# 情報システム開発契約のセキュリティ仕様

# 作成のためのガイドライン

# ～Windows Active Directory編～

2020年12月

セキュリティ検討プロジェクトチーム

目次

[I. 概要 1](#_Toc56588711)

[1 はじめに 2](#_Toc56588712)

[1.1 米国国防総省 Security Technical Implementation Guides 2](#_Toc56588713)

[1.2 Center for Internet Security Benchmarks 3](#_Toc56588714)

[1.3 Microsoft Security Baseline 及び Security Configuration Framework 3](#_Toc56588715)

[1.4 本ガイドラインの策定の経緯とスコープ 3](#_Toc56588716)

[1.5 本ガイドラインの改訂について 5](#_Toc56588717)

[1.6 契約等の仕様として使用する際の注意 5](#_Toc56588718)

[1.7 著作権表示、商標、ライセンス 6](#_Toc56588719)

[1.8 本ガイドラインの著作権と保証 7](#_Toc56588720)

[2 対象システムと利用上の注意 8](#_Toc56588721)

[2.1 利用上の注意 8](#_Toc56588722)

[II. サイバー攻撃の実態 10](#_Toc56588723)

[3 攻撃ベクトルの研究 11](#_Toc56588724)

[3.1 サイバーキルチェーンとセキュリティ対策 11](#_Toc56588725)

[3.2 CVE-2017-11882 Officeの数式エディタの脆弱性を使った攻撃 13](#_Toc56588726)

[3.3 ランサムウェア Emotet の攻撃ベクトル 14](#_Toc56588727)

[III. サイバー攻撃に対する防御 17](#_Toc56588728)

[4 最低限検討すべきデフォルト緩和策 端末編 18](#_Toc56588729)

[4.1 教育の実施 19](#_Toc56588730)

[4.2 重要情報資産の暗号化とバックアップの実施 20](#_Toc56588731)

[4.3 管理者権限の制限 21](#_Toc56588732)

[4.4 アンチウイルスソフトの利用 21](#_Toc56588733)

[4.5 脆弱性修正プログラムの適用 22](#_Toc56588734)

[4.6 マクロ・スクリプト禁止と保護ビューの利用 23](#_Toc56588735)

[4.7 メール・ブラウザーの適切な利用 23](#_Toc56588736)

[4.8 多要素認証機能の利用 24](#_Toc56588737)

[4.9 セキュアなネットワークの利用 25](#_Toc56588738)

[4.10 外部記憶媒体の利用制限 26](#_Toc56588739)

[4.11 適切に管理・設定されたパスワードの利用 27](#_Toc56588740)

[5 サイバー攻撃に対する防御 最低限検討すべきデフォルト緩和策 セキュリティ仕様・Webアプリケーション編 29](#_Toc56588741)

[5.1 暗号化 29](#_Toc56588742)

[5.2 脆弱性管理 29](#_Toc56588743)

[5.3 セッション管理 30](#_Toc56588744)

[5.4 属性管理 30](#_Toc56588745)

[5.5 認証・認可 30](#_Toc56588746)

[5.6 ネットワーク構成 32](#_Toc56588747)

[IV. サイバー攻撃に対する防御 詳細なデフォルト緩和策 33](#_Toc56588748)

[6 セキュアコーディング 34](#_Toc56588749)

[6.1 セキュアコーディング 34](#_Toc56588750)

[6.2 OWASP Application Security Verification Standard 4.0.1 JA 34](#_Toc56588751)

[6.3 ASVS 4.0.1 の構成 34](#_Toc56588752)

[6.4 ASVSと契約 35](#_Toc56588753)

[6.5 ASVSのテーラリング 35](#_Toc56588754)

[7 詳細設定対策に必要な措置 36](#_Toc56588755)

[7.1 Windows の 管理者の設定 36](#_Toc56588756)

[8 プロトコル設定（Windows） 42](#_Toc56588757)

[8.1 Windows SMB 42](#_Toc56588758)

[8.2 Windows TLS 42](#_Toc56588759)

[8.3 暗号スイート 43](#_Toc56588760)

[8.4 Linux 44](#_Toc56588761)

[9 管理インターフェースの保護 46](#_Toc56588762)

[9.1 基本的な考え方 46](#_Toc56588763)

[9.2 管理レイヤーの設定と、アカウント・ネットワーク・管理端末の分離 46](#_Toc56588764)

[9.3 最重要資産での物理的アクセス制御 52](#_Toc56588765)

[10 ログとレジストリの保護 55](#_Toc56588766)

[10.1 ログの保護 55](#_Toc56588767)

[10.2 レジストリの保護 56](#_Toc56588768)

[11 電子認証について 59](#_Toc56588769)

[11.1 目的 59](#_Toc56588770)

[11.2 電子認証（本人認証）の方式検討 59](#_Toc56588771)

[11.3 パスワードの要件と課題 63](#_Toc56588772)

[11.4 パスワード認証に関する要求事項（推奨） 66](#_Toc56588773)

[11.5 Windows認証を利用する場合 68](#_Toc56588774)

[11.6 リスクの影響度に応じた認証方式の選択 69](#_Toc56588775)

[11.7 認証に関する用語解説・資料 72](#_Toc56588776)

[12 Windows Group Policyの再読み込み 80](#_Toc56588777)

[12.1 Windows Group Policy設定 80](#_Toc56588778)

[12.2 Windows レジストリー（Windows 10、Windows Server 2016確認済） 80](#_Toc56588779)

[13 レベル1セキュリティ構成（Windows 10） 81](#_Toc56588780)

[13.1 設定による影響 81](#_Toc56588781)

[13.2 レベル1セキュリティ構成（Windows 10） 81](#_Toc56588782)

[13.3 ・L1 アカウントポリシー 83](#_Toc56588783)

[13.4 ・L1 ローカルポリシー ユーザー権利の割り当て 84](#_Toc56588784)

[13.5 ・L1 ローカルポリシー セキュリティ オプション 87](#_Toc56588785)

[13.6 ・L1 監査ポリシーの詳細な構成 92](#_Toc56588786)

[13.7 ・L1 セキュリティが強化されたWindowsファイアウォール 94](#_Toc56588787)

[13.8 ・L1 MS Security Guide 96](#_Toc56588788)

[13.9 ・L1 MSS 98](#_Toc56588789)

[13.10 ・L1 ネットワーク 99](#_Toc56588790)

[13.11 ・L1 システム 100](#_Toc56588791)

[13.12 ・L1 Windows コンポーネント 104](#_Toc56588792)

[13.13 ・L1 Windows コンポーネントｰInternet Explorer 113](#_Toc56588793)

[13.14 ・L1 コントロール 126](#_Toc56588794)

[13.15 ・L1 OFFICE2016の共通設定 127](#_Toc56588795)

[13.16 ・L1 Excel 2016 130](#_Toc56588796)

[13.17 ・L1 Word 2016 134](#_Toc56588797)

[13.18 ・L1 Outlook 2016 138](#_Toc56588798)

[13.19 ・L1 OneDrive 2016 150](#_Toc56588799)

[13.20 ・L1 Google Chrome 151](#_Toc56588800)

[14 ・Windows Server 2016 Domain Controller 160](#_Toc56588801)

[14.1 Windows Server 2016 Domain Controller のセキュリティ構成 160](#_Toc56588802)

[14.2 DC アカウントポリシー 161](#_Toc56588803)

[14.3 ・DC ローカルポリシー ユーザー権利の割り当て 163](#_Toc56588804)

[14.4 ・DC ローカルポリシー セキュリティ オプション 170](#_Toc56588805)

[14.5 ・DC 監査ポリシーの詳細な構成 186](#_Toc56588806)

[14.6 ・DC 管理用テンプレート 191](#_Toc56588807)

[V. サイバー攻撃に対する防御 MITREに基づく緩和対策 208](#_Toc56588808)

[15 MITRE ATT&CK に基づく詳細設定対策 209](#_Toc56588809)

[15.1 MITRE ATT&CKによる設定対策一覧（絞り込み済み） 209](#_Toc56588810)

[16 ・悪意のあるファイルを添付したフィッシングメール 211](#_Toc56588811)

[16.1 戦術：初期侵入 211](#_Toc56588812)

[16.2 概説 211](#_Toc56588813)

[16.3 緩和の方針 211](#_Toc56588814)

[16.4 運用やNetworkが変更された場合の影響の有無 212](#_Toc56588815)

[16.5 優先すべき措置 212](#_Toc56588816)

[16.6 ユーザー運用管理責任 212](#_Toc56588817)

[16.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 214](#_Toc56588818)

[16.8 受託開発ベンダー管理責任 215](#_Toc56588819)

[17 ・コマンドラインインターフェースの悪用 217](#_Toc56588820)

[17.1 戦術：悪意のあるプログラムの実行 217](#_Toc56588821)

[17.2 概説 217](#_Toc56588822)

[17.3 緩和の方針 217](#_Toc56588823)

[17.4 運用やNetworkが変更された場合の影響の有無 217](#_Toc56588824)

[17.5 優先すべき措置 218](#_Toc56588825)

[17.6 ユーザー運用管理責任 218](#_Toc56588826)

[17.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 218](#_Toc56588827)

[17.8 受託開発ベンダー管理責任 219](#_Toc56588828)

[17.9 ・コマンドラインインターフェースの監査 220](#_Toc56588829)

[18 ・PowerShellの悪用 221](#_Toc56588830)

[18.1 戦術:悪意あるプログラムの実行 221](#_Toc56588831)

[18.2 概説 221](#_Toc56588832)

[18.3 緩和の方針 221](#_Toc56588833)

[18.4 運用やNetworkが変更された場合の影響の有無 221](#_Toc56588834)

[18.5 優先すべき措置 221](#_Toc56588835)

[18.6 ユーザー運用管理責任 222](#_Toc56588836)

[18.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 223](#_Toc56588837)

[18.8 受託開発ベンダー管理責任 225](#_Toc56588838)

[18.9 WinRMサービスを無効化/制限 225](#_Toc56588839)

[19 ・Windowsタスクスケジューラ at, schtasks の悪用 227](#_Toc56588840)

[19.1 戦術：悪意あるプログラムの実行 227](#_Toc56588841)

[19.2 概説 227](#_Toc56588842)

[19.3 緩和の方針 227](#_Toc56588843)

[19.4 運用やNetworkが変更された場合の影響の有無 227](#_Toc56588844)

[19.5 優先すべき措置 227](#_Toc56588845)

[19.6 ユーザー運用管理責任 228](#_Toc56588846)

[19.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 228](#_Toc56588847)

[19.8 受託開発ベンダー管理責任 228](#_Toc56588848)

[19.9 ・タスクスケジューラのポリシー設定 229](#_Toc56588849)

[20 ・悪意あるスクリプティングの実行 232](#_Toc56588850)

[20.1 戦術：悪意あるプログラムの実行、永続化、防御の回避 232](#_Toc56588851)

[20.2 概説 232](#_Toc56588852)

[20.3 緩和の方針 232](#_Toc56588853)

[20.4 運用やNetworkが変更された場合の影響の有無 232](#_Toc56588854)

[20.5 優先すべき措置 232](#_Toc56588855)

[20.6 ユーザー運用管理責任 233](#_Toc56588856)

[20.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 233](#_Toc56588857)

[20.8 受託開発ベンダー管理責任 234](#_Toc56588858)

[20.9 コマンドラインインターフェースの監査 235](#_Toc56588859)

[20.10 Windows Script Hostの制御設定 235](#_Toc56588860)

[20.11 Visual Basic for Application（VBA、マクロ） の課題 237](#_Toc56588861)

[21 ・悪意あるWindowsサービスの実行 ・不正なWindowsサービスの追加 239](#_Toc56588862)

[21.1 戦術：悪意あるプログラムの実行 （悪意あるWindowsサービスの実行） 239](#_Toc56588863)

[21.2 戦術：永続性、特権昇格 （不正なWindowsサービスの追加） 239](#_Toc56588864)

[21.3 概説 239](#_Toc56588865)

[21.4 緩和の方針 239](#_Toc56588866)

[21.5 運用やNetworkが変更された場合の影響の有無 239](#_Toc56588867)

[21.6 優先すべき措置 239](#_Toc56588868)

[21.7 ユーザー運用管理責任 240](#_Toc56588869)

[21.8 情報システム設計開発部門・運用部門（ベンダー代行を含む) 240](#_Toc56588870)

[21.9 受託開発ベンダー管理責任 242](#_Toc56588871)

[22 ・メールに添付されたマルウェアファイルやリンクをユーザーが実行する 243](#_Toc56588872)

[22.1 戦術：悪意あるプログラムの実行 243](#_Toc56588873)

[22.2 概説 243](#_Toc56588874)

[22.3 緩和の方針 243](#_Toc56588875)

[22.4 運用やNetworkが変更された場合の影響の有無 243](#_Toc56588876)

[22.5 優先すべき措置 243](#_Toc56588877)

[22.6 ユーザー運用管理責任 243](#_Toc56588878)

[22.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 243](#_Toc56588879)

[22.8 受託開発ベンダー管理責任 243](#_Toc56588880)

[23 ・レジストリRunキーやスタートアップフォルダの悪用 244](#_Toc56588881)

[23.1 戦術：永続化 244](#_Toc56588882)

[23.2 概説 244](#_Toc56588883)

[23.3 緩和の方針 244](#_Toc56588884)

[23.4 運用やNetworkが変更された場合の影響の有無 244](#_Toc56588885)

[23.5 優先すべき措置 244](#_Toc56588886)

[23.6 ユーザー運用管理責任 244](#_Toc56588887)

[23.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 245](#_Toc56588888)

[23.8 受託開発ベンダー管理責任 246](#_Toc56588889)

[24 ・ファイル削除 247](#_Toc56588890)

[24.1 戦術：防御の回避 247](#_Toc56588891)

[24.2 概説 247](#_Toc56588892)

[24.3 緩和の方針 247](#_Toc56588893)

[24.4 運用やNetworkが変更された場合の影響の有無 247](#_Toc56588894)

[24.5 優先すべき措置 247](#_Toc56588895)

[24.6 ユーザー運用管理責任 247](#_Toc56588896)

[24.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 247](#_Toc56588897)

[24.8 受託開発ベンダー管理責任 248](#_Toc56588898)

[25 ・難読化されたファイルまたは情報 249](#_Toc56588899)

[25.1 戦術：防衛回避 249](#_Toc56588900)

[25.2 概説 249](#_Toc56588901)

[25.3 緩和の方針 249](#_Toc56588902)

[25.4 運用やNetworkが変更された場合の影響の有無 249](#_Toc56588903)

[25.5 優先すべき措置 249](#_Toc56588904)

[25.6 ユーザー運用管理責任 250](#_Toc56588905)

[25.7 啓発・教育 250](#_Toc56588906)

[25.8 管理規程 250](#_Toc56588907)

[25.9 情報システム設計開発部門・運用部門（ベンダー代行を含む) 250](#_Toc56588908)

[25.10 受託開発ベンダー管理責任 251](#_Toc56588909)

[26 ・認証情報のダンプ 252](#_Toc56588910)

[26.1 戦術：認証情報アクセス 252](#_Toc56588911)

[26.2 概説 252](#_Toc56588912)

[26.3 緩和の方針 252](#_Toc56588913)

[26.4 運用やNetworkが変更された場合の影響の有無 252](#_Toc56588914)

[26.5 優先すべき措置 252](#_Toc56588915)

[26.6 ユーザー運用管理責任 253](#_Toc56588916)

[26.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 254](#_Toc56588917)

[26.8 受託開発ベンダー管理責任 255](#_Toc56588918)

[27 ・脆弱性を悪用した認証情報アクセス 257](#_Toc56588919)

[27.1 戦術：認証情報アクセス 257](#_Toc56588920)

[27.2 概説 257](#_Toc56588921)

[27.3 緩和の方針 257](#_Toc56588922)

[27.4 運用やNetworkが変更された場合の影響の有無 257](#_Toc56588923)

[27.5 優先すべき措置 257](#_Toc56588924)

[27.6 ユーザー運用管理責任 257](#_Toc56588925)

[27.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 258](#_Toc56588926)

[27.8 受託開発ベンダー管理責任 259](#_Toc56588927)

[28 ・アカウントの探索 260](#_Toc56588928)

[28.1 戦術：情報の探索 260](#_Toc56588929)

[28.2 概説 260](#_Toc56588930)

[28.3 緩和の方針 260](#_Toc56588931)

[28.4 運用やNetworkが変更された場合の影響の有無 260](#_Toc56588932)

[28.5 優先すべき措置 260](#_Toc56588933)

[28.6 ユーザー運用管理責任 260](#_Toc56588934)

[28.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 260](#_Toc56588935)

[28.8 受託開発ベンダー管理責任 262](#_Toc56588936)

[29 ・ファイルとディレクトリの探索 263](#_Toc56588937)

[29.1 戦術：情報の探索 263](#_Toc56588938)

[29.2 概説 263](#_Toc56588939)

[29.3 緩和の方針 263](#_Toc56588940)

[29.4 運用やNetworkが変更された場合の影響の有無 263](#_Toc56588941)

[29.5 優先すべき措置 263](#_Toc56588942)

[29.6 ユーザー運用管理責任 263](#_Toc56588943)

[29.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 264](#_Toc56588944)

[29.8 受託開発ベンダー管理責任 264](#_Toc56588945)

[30 ・ネットワークサービスのスキャン 266](#_Toc56588946)

[30.1 戦術：情報の探索 266](#_Toc56588947)

[30.2 対象プラットフォーム 266](#_Toc56588948)

[30.3 概説 266](#_Toc56588949)

[30.4 緩和の方針 266](#_Toc56588950)

[30.5 運用やNetworkが変更された場合の影響の有無 266](#_Toc56588951)

[30.6 優先すべき措置 266](#_Toc56588952)

[30.7 ユーザー運用管理責任 266](#_Toc56588953)

[30.8 情報システム設計開発部門・運用部門（ベンダー代行を含む) 267](#_Toc56588954)

[30.9 受託開発ベンダー管理責任 267](#_Toc56588955)

[31 ・システム情報の探索 269](#_Toc56588956)

[31.1 戦術：情報の探索 269](#_Toc56588957)

[31.2 概説 269](#_Toc56588958)

[31.3 緩和の方針 269](#_Toc56588959)

[31.4 運用やNetworkが変更された場合の影響の有無 269](#_Toc56588960)

[31.5 優先すべき措置 269](#_Toc56588961)

[31.6 ユーザー運用管理責任 270](#_Toc56588962)

[31.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 270](#_Toc56588963)

[31.8 受託開発ベンダー管理責任 270](#_Toc56588964)

[32 ・システムのネットワーク設定の探索 272](#_Toc56588965)

[32.1 戦術：情報の探索 272](#_Toc56588966)

[32.2 概説 272](#_Toc56588967)

[32.3 緩和の方針 272](#_Toc56588968)

[32.4 運用やNetworkが変更された場合の影響の有無 272](#_Toc56588969)

[32.5 優先すべき措置 272](#_Toc56588970)

[32.6 ユーザー運用管理責任 272](#_Toc56588971)

[32.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 272](#_Toc56588972)

[32.8 受託開発ベンダー管理責任 273](#_Toc56588973)

[33 ・システムユーザーの探索 274](#_Toc56588974)

[33.1 戦術：情報の探索 274](#_Toc56588975)

[33.2 概説 274](#_Toc56588976)

[33.3 緩和の方針 274](#_Toc56588977)

[33.4 運用やNetworkが変更された場合の影響の有無 274](#_Toc56588978)

[33.5 優先すべき措置 274](#_Toc56588979)

[33.6 ユーザー運用管理責任 274](#_Toc56588980)

[33.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 274](#_Toc56588981)

[33.8 受託開発ベンダー管理責任 275](#_Toc56588982)

[34 ・Pass the Hash 276](#_Toc56588983)

[34.1 戦術：水平展開 276](#_Toc56588984)

[34.2 概説 276](#_Toc56588985)

[34.3 緩和の方針 276](#_Toc56588986)

[34.4 運用やNetworkが変更された場合の影響の有無 276](#_Toc56588987)

[34.5 優先すべき措置 276](#_Toc56588988)

[34.6 ユーザー運用管理責任 277](#_Toc56588989)

[34.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 278](#_Toc56588990)

[34.8 受託開発ベンダー管理責任 284](#_Toc56588991)

[35 ・ローカルシステムからのデータ収集 285](#_Toc56588992)

[35.1 戦術：情報の収集 285](#_Toc56588993)

[35.2 概説 285](#_Toc56588994)

[35.3 緩和の方針 285](#_Toc56588995)

[35.4 運用やNetworkが変更された場合の影響の有無 285](#_Toc56588996)

[35.5 優先すべき措置 285](#_Toc56588997)

[35.6 ユーザー運用管理責任 285](#_Toc56588998)

[35.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 286](#_Toc56588999)

[35.8 受託開発ベンダー管理責任 286](#_Toc56589000)

[36 ・ネットワーク共有ドライブからのデータ収集 287](#_Toc56589001)

[36.1 戦術:情報の収集 287](#_Toc56589002)

[36.2 概説 287](#_Toc56589003)

[36.3 緩和の方針 287](#_Toc56589004)

[36.4 運用やNetworkが変更された場合の影響の有無 287](#_Toc56589005)

[36.5 優先すべき措置 287](#_Toc56589006)

[36.6 ユーザー運用管理責任 287](#_Toc56589007)

[36.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 287](#_Toc56589008)

[36.8 受託開発ベンダー管理責任 288](#_Toc56589009)

[37 ・データの圧縮 290](#_Toc56589010)

[37.1 戦術：持ち出し 290](#_Toc56589011)

[37.2 概説 290](#_Toc56589012)

[37.3 緩和の方針 290](#_Toc56589013)

[37.4 運用やNetworkが変更された場合の影響の有無 290](#_Toc56589014)

[37.5 優先すべき措置 290](#_Toc56589015)

[37.6 ユーザー運用管理責任 290](#_Toc56589016)

[37.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 290](#_Toc56589017)

[37.8 受託開発ベンダー管理責任 291](#_Toc56589018)

[38 ・一般的に利用されるポートの悪用 292](#_Toc56589019)

[38.1 戦術：外部からの指令統制 292](#_Toc56589020)

[38.2 概説 292](#_Toc56589021)

[38.3 緩和の方針 292](#_Toc56589022)

[38.4 運用やNetworkが変更された場合の影響の有無 292](#_Toc56589023)

[38.5 優先すべき措置 292](#_Toc56589024)

[38.6 ユーザー運用管理責任 293](#_Toc56589025)

[38.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 293](#_Toc56589026)

[38.8 受託開発ベンダー管理責任 293](#_Toc56589027)

[39 ・標準アプリケーションレイヤプロトコル(HTTP,SMTPなど) 295](#_Toc56589028)

[39.1 戦術：外部からの指令統制 295](#_Toc56589029)

[39.2 概説 295](#_Toc56589030)

[39.3 緩和の方針 295](#_Toc56589031)

[39.4 運用やNetworkが変更された場合の影響の有無 296](#_Toc56589032)

[39.5 優先すべき措置 296](#_Toc56589033)

[39.6 ユーザー運用管理責任 296](#_Toc56589034)

[39.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 296](#_Toc56589035)

[39.8 受託開発ベンダー管理責任 296](#_Toc56589036)

[40 ・データの暗号化 298](#_Toc56589037)

[40.1 戦術：持ち出し、外部からの指令統制 298](#_Toc56589038)

[40.2 概説 298](#_Toc56589039)

[40.3 緩和の方針 298](#_Toc56589040)

[40.4 運用やNetworkが変更された場合の影響の有無 298](#_Toc56589041)

[40.5 優先すべき措置 298](#_Toc56589042)

[40.6 ユーザー運用管理責任 298](#_Toc56589043)

[40.7 情報システム設計開発部門・運用部門（ベンダー代行を含む) 299](#_Toc56589044)

[40.8 受託開発ベンダー管理責任 299](#_Toc56589045)

参考例

OWASP アプリケーションセキュリティ検証標準 4.0

# 概要

## はじめに

本ガイドラインは、重要インフラ、大企業基幹系の受託開発に際して、ユーザーとベンダーがセキュリティ仕様を策定する際の、脅威分析とその対策を検討するためのOS、デスクトップアプリ、ブラウザーのセキュリティ設定を検討するためのガイドラインです。

脅威については、NIST（米国国立標準技術研究所）の委託を受け、世界中のCVEの採番を行っている非営利法人 MITRE の ATT&CK® Matrix for Enterprise をベースに、日本国内で発生したインシデントで実際に使われ、かつ、実績の多いものをセキュリティプロジェクトチームの有識者が抽出したものです。また、脅威に対する対策は、MITRE ATT&CK Matrix for Enterprise の推奨する緩和策に加え、以下のガイドラインの緩和策を参照しています。

* 米国国防総省 Security Technical Implementation Guides (STIG)
* 米国 Center for Internet Security Benchmarks
* Microsoft® Security Baseline 及び Security Configuration Framework

また、OS等のセキュリティ設定ではカバーしきれない、SQLインジェクション攻撃やアプリケーションの構成の不備に起因する脆弱性対策を行うものとして、OWASP の Application Security Verification Standard (ASVS:アプリケーションセキュリティ検証標準) V4 と Java Spring Framework セキュアコーディングガイドラインを参考例として例示しました。 本ガイドラインとセキュアコーディングを合わせることで、より強靭なシステムの要件定義が可能となり、後工程でのセキュリティ実装がより具体的になると期待できます。

重要：攻撃者と彼らが生み出す脅威は日々、進化を遂げています。本ガイドラインは過去の実績のある脅威に対する緩和策の提案であり、このガイドラインを適用することでサイバー攻撃の被害をゼロにすることが保証されるわけではありません。

本ガイドラインを参考に、定期・不定期でシステム固有の脅威に対するリスクを認識し、そのリスクの緩和に向けた検討を続けることを強く推奨します。

### 米国国防総省 Security Technical Implementation Guides

米国国防総省 Security Technical Implementation Guides (STIGs) は、製品の安全な展開の実装を支援するように設計されたガイドラインで、ホームページによると「悪意のあるコンピューター攻撃に対して脆弱な情報システム/ソフトウェアを「ロックダウン」するための技術的なガイダンスが含まれています。」となっています。2020年10月時点で、507製品/ポリシーガイド/ツール（ドラフトを含む）が掲載されており、Network機器、セキュリティ製品、OS、アプリケーションソフト、データベースがバージョンごとに発行されています。また、さまざまなベンダーやコミュニティからの提案を受け、逐次、改訂されています。多くのサードパーティがSTIG Viewerを提供しており、各製品の設定データをXML、JSON、CSVで入手できます。

* 国防総省 STIGs [[1]](#footnote-1)
* サードパーティーのSTIGVIWER[[2]](#footnote-2)

### Center for Internet Security Benchmarks

Center for Internet Security Inc は米国の州、地方、政府機関のサイバー攻撃の防御、対応、回復を担うMulti-State Information Sharing and Analysis Center（MS-ISAC）と、選挙事務所や選挙インフラシステムのサーバーセキュリティを担うElections Infrastructure Information Sharing and Analysis Center (EI-ISAC) の運用を行っている非営利法人です。 CIS Benchmarkはホームページによると「実証済みのガイドラインにより、サイバー攻撃に対して最も脆弱なオペレーティングシステム、ソフトウェア、およびネットワークを保護できます。進化するサイバーセキュリティの課題と闘うために、ボランティアのITコミュニティによって継続的に検証されています。」となっています。STIG同様にハードウェアからOS、アプリケーションに至る各個別製品の具体的な設定方法が掲載されており、NIST Cybersecurity Framework (CSF)、NIST SP 800-53、ISO 27000、PCI DSSなどの規格、枠組みに対応しています。BenchmarkはLevel 1（設定しても弊害がない基本的なセキュリティ要件）、Level 2（機能低下を起こすがより高度なセキュリティ環境向けセキュリティ要件）の2つの設定が提供されています。ツールを除き、実証済みのガイドラインが無償でダウンロードでき、2020年3月段階で、およそ600製品/バージョンが登録されています。STIG同様に、必要に応じて改訂されています。

* Center for Internet Security Benchmarks[[3]](#footnote-3)

### Microsoft Security Baseline 及び Security Configuration Framework

Microsoft Security Baselineは、「一連の Microsoft が推奨する構成設定であり、そのセキュリティに対する影響についても説明しています。 これらの設定は、Microsoft セキュリティのエンジニアリングチーム、製品グループ、パートナー、および顧客のフィードバックに基づいています。」とされています。Windowsおよび関連コンポーネントには数千のグループポリシーがありますが、セキュリティ設定に関連するグループポリシーが集約されたもので、同社のSecurity Compliance Toolkit (SCT) に含まれています。Security Baselineは半年ごとに改訂されており、ブログ で改訂理由などが詳細に表明されています。

Microsoft security configuration framework は、Windows 10 にフォーカスし、エンドポイントの強化作業の優先順位付けを支援するためのものとされています。Level 1からLevel 5 までが規程されており、現在はLeve 2までがリリースされています。Level 1 は、Security Baselineよりは水準が低く見えますが、30日以内に展開できるように設計されているとなっており、既存のアプリケーションへの影響を最小限にする設定となっています。

* Microsoft Security Baseline[[4]](#footnote-4)
* Microsoft security configuration framework[[5]](#footnote-5)

### 本ガイドラインの策定の経緯とスコープ

#### 経緯

2020年4月の改正民法（債権法）施行に伴い、経済産業省の「情報システム・モデル取引・契約書」の改訂作業を独立行政法人情報処理推進機構社会基盤センターモデル取引・契約書見直し検討部会が実施しました。この見直しに際し、セキュリティ関連に特化して、「モデル取引・契約書」改定版あるいは追補版に盛り込むべき内容を検討し、その結果を提案することを目指しセキュリティ検討プロジェクトチームが設置され、その議論においてユーザーとベンダーがセキュリティ仕様を策定する際の、検討のためのたたき台として一定のセキュリティ設定を提示すべきとなり、本ガイドラインが作成されました。

* セキュリティ検討プロジェクトチームメンバー

|  |  |  |
| --- | --- | --- |
| 主査 | 加藤　智巳 | 株式会社ラック |
| 委員 | 阿部 恭一 | ANAシステムズ株式会社 |
| 委員 | 伊藤 昇 | 株式会社大塚商会 |
| 委員 | 江原 悠介 | PwCあらた有限責任監査法人 |
| 委員 | 大谷 和子 | 株式会社日本総合研究所 |
| 委員 | 小川 隆一 | 独立行政法人情報処理推進機構（IPA） |
| 委員 | 垣内 由梨香 | 日本マイクロソフト株式会社 |
| 委員 | 金森 直樹 | 株式会社TKC |
| 委員 | 田上 利博 | サイバートラスト株式会社 |
| 委員 | 坪井 正広 | 株式会社野村総合研究所 |
| 委員 | 中尾 康二 | 国立研究開発法人情報通信研究機構（NICT） |
| 委員 | 萩原 健太 | グローバルセキュリティエキスパート株式会社／Software ISAC |
| 委員 | 板東 直樹 | アップデートテクノロジー株式会社 |
| 委員 | 深津 博 | 愛知医科大学病院 |
| 委員 | 丸山 満彦 | PwCコンサルティング合同会社 |
| 委員 | 山崎 文明 | 情報安全保障研究所合同会社 |
| 委員 | 山根 義則 | 三菱自動車工業株式会社 |

#### 想定している読者とプロセス

* 重要インフラ・大企業基幹系システム開発に携わる方

#### 対象となるプロセス

共通フレーム2013 (SLCP-JCF2013) の以下のプロセス

* 2.2要件定義プロセス
* 2.3システム開発プロセス
* 2.4ソフトウェア実装プロセス
* 2.6保守プロセス
* 3.1運用プロセス

#### スコープ

セキュリティ仕様は、物理的、技術的、人的な側面を持ちます。このガイドラインは情報システム開発契約における、技術的なセキュリティ仕様の検討を支援しますが、情報の物理的保護対策や、データーセンターなどへの侵入の物理的保護については触れていません。また、重要な情報を入力する際のショルダーハッキングを防止するなどの人的な対策についても触れていません。これらの仕様の検討は以下をご参考下さい。

* 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」内閣サイバーセキュリティセンター令和元年版
* 「組織における内部不正防止ガイドライン」IPA 2017年版

### 本ガイドラインの改訂について

日々、攻撃者は脆弱性を発見し、新たな攻撃手法やユーザーを騙すテクニックを開発しています。従って、防御のためのセキュリティ設定も日々、進化することが求められます。MITRE ATT&CKは四半期に1回、主に新たな攻撃手法の追加の改訂がされるため、本ガイドラインもATT&CKの改訂に応じて、対応策や設定値を追加していく予定です。 また、対応策や設定によって、システムへの不具合や運用に影響が及ぼすことがあります。こうした特定環境でのセキュリティ設定に対する不具合の情報は、ITに依存する社会全体にとって有益で重要な情報と考えることができます。こうした観点から、設定における課題や代替策についても改訂版に追加してく予定です。改訂版は、以下のWebサイトで随時公開します。

www.softwareisac.jp/ipa/

改訂作業は、セキュリティプロジェクトチームの事務局を担当した、一般社団法人ソフトウェア協会 Software ISACで実施します。

ご意見、ご提案、改良すべき点などのご提案をお待ちしております。以下までメールにてご連絡ください。皆様のご協力をお願い申し上げます。なお、技術的なご質問については回答いたしかねますので、ご承知おきください。

提案先: secguide@softwareisac.jp

一般社団法人ソフトウェア協会（Software Association of Japan）  
〒107-0052 東京都港区赤坂1-3-6　赤坂グレースビル  
TEL：03-3560-8440／FAX：03-3560-8441  
<https://www.saj.or.jp/activity/project/softwareisac/index.html>

### 契約等の仕様として使用する際の注意

本ガイドラインをシステム開発契約等の仕様として利用する際は、「情報システム開発契約のセキュリティ仕様作成のためのガイドライン～Windows Active Directory編～2020年12月版」と明記した上でご利用下さい。開発に入ったのち、本ガイドラインが改訂された場合で、システムに大きな変更を加えなければならないことが考えられます。こうした際の、開発費用や納期の変更の取扱いについては、必ず、事前に発注者と受注者で取り決めをし、契約書に明記してください。

### 著作権表示、商標、ライセンス

本書でのグループポリシーの説明は、米国Microsoft Corporation. の著作物が含まれています。 Microsoft®、Windows®、Windows® Server 2016、Windows® 10は、米国Microsoft Corporation.の米国およびその他の国における登録商標です。

その他、すべてのページに記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

© 2020 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

### by-sa本ガイドラインの著作権と保証

本ガイドラインのライセンスは、クリエイティブコモンズ 表示-継承 4.0 国際[[6]](#footnote-6) で提供されます。原作者のクレジット（氏名、作品タイトルなど）を表示し、改変した場合には元の作品と同じCCライセンス（このライセンス）で公開することを主な条件に、営利目的での二次利用も許可されるCCライセンス。但し、第三者が著作権を有する部分はその著作者が権利を有します。

本ガイドラインは、現状有姿、無保証で提供されます。ガイドラインの設定によってサイバー攻撃が100%防げるものではありません。本ガイドラインを使用することに関連して利用者及び第三者に生じた直接的な損害及び間接的な損害について一切の責任を負いません。

また、既存のアプリケーションソフトやActive Directoryの動作に制限が加わる可能性があります。ガイドラインの設定は、環境に応じてテストを実施した上で、自己責任で適用してください。

## 対象システムと利用上の注意

本ガイドラインは、以下の環境を対象とします。

* Server OS： Windows Server 2016 以上
* Client OS： Windows 10 (1903) 以上
* ドメイン： Active Directory
* Office： Office 2016/2019 （バージョン16）
* その他：   
  Windows 8.1, Windows Server 2012R2以降に実装されたセキュリティ機能は、Windows 8.1, Windows Server 2012R2で動作しませんが、本ガイドラインの適用で、限定的ではありますが、脅威に対する緩和策となるものもあります。

アンチウイルスソフトの一般的な運用は実施済みであることを前提としています。

* 対象外：   
  サポートが終了している Windows 7、Windows Server 2008/2008R2は本ガイドラインの対象外となります。

**重要** サポートの終了しているOS、アプリケーションの使用は、被害を被るだけでなく、第三者にインシデントを起こす原因となる可能性が高いため、すぐに使用を中止し、ネットワークから切り離すこと検討してください。

### 利用上の注意

本ガイドラインを適用した際に、以下のネットワーク接続や共有ができなくなることがあります。事前の調査、検証をお勧めします。

#### SMBv1 の無効化

SMBv1 の脆弱性が報告されており、2017年にはこの脆弱性を利用した WannaCry と呼ばれるランサムウェアの被害が発生しています。このため本ガイドラインでは、グループポリシーでSMBv1を無効化する設定を推奨しています。この設定を実施した場合、一部のSMBv2以上のプロトコルに対応していない古い NAS やファイルサーバー、複合機などに接続できない場合があります。なお、Windows 10では SMBv1 は廃止されています。

#### SSL3.0、TLS1.0、TLS1.1 の無効化

SSL3.0、TLS1.0、TLS1.1 は脆弱性が報告されており、主要ブラウザーベンダーは2020年にサポートを終了しています。このため、本ガイドラインでは、使用を無効化する設定を推奨しています。 この設定をした場合、組織内、組織外のWebサーバーとの接続ができない場合があります。

#### グループポリシー

本ガイドラインは、Active Directory グループポリシーを利用し、サーバー、端末のポリシー設定を行います。ポリシー適用によって、以下の影響が考えられます。

* Officeマクロの実行制限
* グループポリシーのキャッシュ制限による、ドメインコントローラへの負荷の増大、トラフィックの増加
* ログの増加
* ブラウザーでのパスワード保存の禁止
* 未署名のスクリプトの実行禁止

これ以外にも従来の業務に対して影響を及ぼすものがあるため、ポリシーを全体に適用する前に、テスト用の OU に適用し、業務への影響を調査する必要があります。

一方で、Officeマクロやスクリプトはマルウェアの初期侵入に最も頻繁に利用される手法であり、マルウェア感染のリスク受容が出来ない場合は、これらの利用は厳格に管理されるべきです。安易に現状の業務遂行を優先するのではなく、脅威に対するリスク分析を行い、適切なポリシー設定を行う事を強く推奨します。

# サイバー攻撃の実態

サイバー攻撃の防御のための戦略、戦術立案には、サイバー攻撃の実態を知る必要があります。特に、ソフトウェアの脆弱性やスクリプトを使用し侵入してくるマルウェア対策のためには、攻撃側の手口を理解し、正しい対策を行うことが重要です。Ⅱ部では実際に発生した攻撃の手口を解説します。

## 攻撃ベクトルの研究

攻撃は様々な手法が存在しており、2020年3月現在、MITRE ATT&CK で330もの攻撃手法が確認されています。本項では、代表的なマルウェアの攻撃ベクトルを紹介します。

### サイバーキルチェーンとセキュリティ対策

攻撃は、初期侵入から、実行、認証情報の収集、水平展開と幅広い手法の積み重ねで構成されているため、一部の手法の実施を阻止できれば、大規模な拡散や情報漏洩などの被害をある程度防ぐことが可能となります。

タイムライン

自動的に生成された説明以下の図にもあるように、攻撃にはSQLインジェクションなどのコーディングの不備や、構成の不備などの脆弱性を利用するものと、PC、サーバーのOSやアプリケーションなどの設定の不備を利用するものがあります。

また、攻撃ベクトルの初期で侵入を断ち切らないと、検知以外に攻撃を知る方法がなくなり、検知に成功するまでは、情報漏洩が発生したかすら把握できなくなる可能性がでてきます。本ガイドラインを、ユーザーとベンダーのリスクコミュニケーションのツールとして利用する際は、以下のように切り分けて使うと効果的です。

* コーディングや構成の不備  
  ASVS を開発仕様、開発標準として活用し、受入テストの基準作りに利用する
* OSやアプリケーションの不備  
  詳細な緩和策 を構成仕様として活用し、受入テストでチェックする

### CVE-2017-11882 Officeの数式エディタの脆弱性を使った攻撃

ソフトウェアの脆弱性を利用してマルウェアを侵入させた例です。

パ本稿は、FIREEYE社の脅威調査: https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html を参考にしました。

#### 攻撃に利用された脆弱性

* CVE-2017-11882 : https://warp.da.ndl.go.jp/info:ndljp/pid/11376004/www.ipa.go.jp/security/ciadr/vul/20171129\_ms.html  
  以下に搭載された数式エディタのスタックベースのバッファーオーバーフローを悪用したものです。
* Office 2007 SP3
* Office 2010SP2(32/64bit)
* Office 2013SP1(32/64bit)
* Office 2016(32/64bit)

#### ダイアグラム 自動的に生成された説明 CVE-2017-11882の攻撃ベクトル

#### 攻撃ベクトルで使用されたコンポーネント

|  |  |
| --- | --- |
| **名前** | **役割** |
| PowerShell | 標準スクリプト言語 |
| MSHTA.EXE | Microsoft HTML Application Host、HTAファイルの実行エンジン |
| VBScript Windows | 標準スクリプト言語 |
| CERTUTIL.EXE | Windows標準コマンド：証明書ユーティリティ |
| SCHTASKS.EXE | Windows標準コマンド：タスクスケジューラ |

#### 手口

1. 攻撃者は、リッチテキストフォーマットに細工をした数式を埋め込みターゲットにメールの添付ファイルとして送信します。
2. 受信者が添付ファイルを開くと、受信者の脆弱な数式エディターが起動し数式を読み込みますが、この際、数式エディターがデータ長を正しくチェックしないため、スタックメモリが破壊され、悪意のあるプログラムが実行されます。
3. 悪意あるプログラムは、WinExec関数を呼び出し、受信者のコンテキストで子プロセス「mshta.exe」を呼び出します。「mshta.exe」は外部サイトからテキストファイルに見せかけた悪意あるPowerShellスクリプトをダウンロードし実行します。
4. 悪意あるPowerShellスクリプトは、さらにテキストファイルに見せかけたVBScriptをダウンロードし、実行します。
5. VBScriptは、C:\ProgramData\Windows\Microsoft\java\ に4つのコンポーネントをダウンロードします。
6. このうちBase64でエンコードされた2つのコンポーネントは、証明書関連の正規のユーティリティである Certutil.exe を利用しデコードし、PowerShellスクリプトに変換されます。
7. 残りの2つのファイルの内、バッチファイルが永続化のためのVBScriptをタスクスケジューラに登録します。
8. 定期的に起動されるPowerShell スクリプトは、C&Cサーバーと通信し、追加の悪意あるコンポーネントダウンロードします。

#### 設定対策

本件は、PowerShellの実行ポリシーを禁止にするべきか、署名済みスクリプトのみ許可する、とし、環境評価によって、VBScriptの実行停止、もしくは、コマンドラインのブラックリスト化を行うことで、十分に抑止できたと考えられます。

1. ユーザーにローカル管理者権限を与えない。
2. Officeの数式エディターの脆弱性アップデート。
3. グループポリシーによるPowerShellの実行ポリシーの制御（停止、署名済みのみ許可等）。
4. AppLocker、Defender Application制御を使ったMSHTA.EXE、CERTUTIL.EXE、SCHETASKS.EXEの実行制御。
5. Registry設定によるVBScriptエンジン（WSCRIPT.EXE、CSCRIPT.EXE）の停止、署名のみ許可設定。

### ランサムウェア Emotet の攻撃ベクトル

電子メールに悪意のあるファイルを添付し、ユーザーがそれを開くことでマルウェアを侵入させた例です。

本稿は、cybereason社の脅威調査: https://www.cybereason.co.jp/blog/cyberattack/3613/ を参考にしました。

#### テキスト が含まれている画像 自動的に生成された説明Emotetの攻撃ベクトル

#### 攻撃ベクトルで使用されたコンポーネント

|  |  |
| --- | --- |
| **名前** | **役割** |
| Outlook.Exe | 電子メールクライアントソフト |
| Word.Exe | ワープロソフト |
| Visual Basic for Application | Microsoft Office用マクロ言語 |
| cmd.Exe | Windows コマンドラインインターフェース |
| PowerShell.Exe | Windows スクリプト言語エンジン |

#### 手口

1. Emotet は、Visual Basic for Application （VBA/マクロ) が含まれた Word の文書を電子メールで相手方に送り付けます。
2. 受信者が Word の内容を確認するため保護されたビュー（初期設定）を解除し、文書を閲覧します。
3. この際に、難読化されたVBA が起動し、コマンドラインインターフェースを起動し、コマンドラインインターフェースは、続けて PowerShell.Exe を起動します。
4. PowerShell は難読化されたスクリプトを実行し、Internet からマルウェア本体をダウンロードします。
5. このような手順を踏むのは、  
   ①VBAやスクリプトを難読化することでアンチウイルスソフトの検出を免れること、  
   ②アンチウイルスソフトに正常なプロセスと認識させること、  
   などを狙ったものと考えられます。

#### 設定対策

本件は、信頼できない相手方からのOffice文書は保護ビューを解除しない、Viasual Basic for Application （VBA/マクロ) を禁止する、PowerShellの実行ポリシーを禁止にすることで、抑止できたと考えられます。

1. ユーザーに対面したことがない相手方からのOffice文書は、開かないもしくは保護ビューを解除しないことを教育する。
2. メールで何回かやり取りを行い信頼関係を築いた上で、添付の Word を開かせる、という手口があることに留意する。
3. Emotet は組織内のメールアドレスを窃取し、組織内の従業員をなりすます場合があることに留意し、組織内のファイルのやり取りは、File Server や、他のコミュニケーションツール経由とするなどを検討する。
4. ユーザー権限は標準ユーザーとし、 Built-in Administrators（ローカル管理者グループ）に所属させない。
5. グループポリシーによるPowerShellの実行ポリシーの制御（停止、署名済みのみ許可等）。
6. AppLocker、Defender Application制御、AppLocker を使った PowerShell.exe、PowerShell\_ISE.Exe、System.Management.Automation.dll の実行制御。

# サイバー攻撃に対する防御

サイバー攻撃に対する技術的な防御は、以下のように大別できます。

① セキュアコーディングで脆弱性排除する  
② OSやアプリケーションの設定で脆弱性を排除する  
③ ネットワークやリムーバブルメディアなどの経路設定で脅威を排除する

また、取り扱う情報資産の重要度に応じて様々な組み合わせと設定が考えられます。

Ⅲ部では、最低限取り組むべき事項として、最低限検討すべきデフォルト緩和策について解説します。

## 最低限検討すべきデフォルト緩和策 端末編

本章では、端末に対して最低限検討すべきデフォルト緩和策を解説します。MITREに基づく詳細設定にすぐに取り掛かることができない場合は本緩和策を検討し実施してください。

この緩和策は、ユーザー主体による運用管理および業務ルールによる対策として実施することが想定されますが、システムによる自動化、制限機能、チェック機能等の実装または実施を促すような機能による対策もあるため、必要に応じてシステム開発時のセキュリティ仕様として盛込むことも推奨します。

また、この対策は、ガイドラインによるリスク低減の効果に大きく影響するため、ベンダーはユーザーに対して内容をレクチャーすることを推奨します。

| **項番** | **項目** | **概説** | **期待できる効果** | **考えられる影響** | **影響の緩和策** |
| --- | --- | --- | --- | --- | --- |
| 1 | [教育の実施](https://www.softwareisac.jp/ipa/index.php?%E6%9C%80%E4%BD%8E%E9%99%90%E6%A4%9C%E8%A8%8E%E3%81%99%E3%81%B9%E3%81%8D%E3%83%87%E3%83%95%E3%82%A9%E3%83%AB%E3%83%88%E7%B7%A9%E5%92%8C%E7%AD%96+%E7%AB%AF%E6%9C%AB%E7%B7%A8#c25660aa) | 経営者向け：サイバーセキュリティ経営のリーダーシップをとり、セキュリティマネジメントのための知識を身に着ける。 | 適切な投資（セキュリティ対策費とリスク受容のバランス）の実施 | 具体的な方法がわからない | IPA 中小企業の情報セキュリティ対策ガイドラインの活用 |
| 管理職向け：セキュリティ設定の重要性や運用の必要性を理解し、指示・対応可能な知識を身に着け、継続的に組織に対して脅威情報などのインプットを行う。 | インシデント発生時の対応、社内外への適切な運用の維持、注意喚起の実施 | 具体的な方法がわからない | IPA 中小企業の情報セキュリティ対策ガイドラインの活用 |
| 従業員向け：設定の意味や運用の背景を理解する。 | 最新の攻撃手口の習得、適切な運用と報告 | 集合教育が難しい、コンテンツがない | IPA コンテンツの活用 |
| 2 | [重要情報資産の暗号化とバックアップの実施](https://www.softwareisac.jp/ipa/index.php?%E6%9C%80%E4%BD%8E%E9%99%90%E6%A4%9C%E8%A8%8E%E3%81%99%E3%81%B9%E3%81%8D%E3%83%87%E3%83%95%E3%82%A9%E3%83%AB%E3%83%88%E7%B7%A9%E5%92%8C%E7%AD%96+%E7%AB%AF%E6%9C%AB%E7%B7%A8#vacd6be0) | 重要資産を指定し、暗号化を行い、定期的にバックアップをとる。 | 被害の軽減／復旧 | バックアップシステムの導入コスト | クラウドの活用（OneDrive、GoogleDrive、DropBox） |
| 3 | [管理者権限の制限](https://www.softwareisac.jp/ipa/index.php?%E6%9C%80%E4%BD%8E%E9%99%90%E6%A4%9C%E8%A8%8E%E3%81%99%E3%81%B9%E3%81%8D%E3%83%87%E3%83%95%E3%82%A9%E3%83%AB%E3%83%88%E7%B7%A9%E5%92%8C%E7%AD%96+%E7%AB%AF%E6%9C%AB%E7%B7%A8#ed3bd5c7) | 利用者にローカルの管理者権限を付与しない （特権IDの適切な管理）。 | 特権昇格・永続化の防止／資格情報の窃取の防止 | アプリケーションインストールが不便 | インストール時のID/パスフレーズの付与 |
| 4 | [アンチウイルスソフトの利用](https://www.softwareisac.jp/ipa/index.php?%E6%9C%80%E4%BD%8E%E9%99%90%E6%A4%9C%E8%A8%8E%E3%81%99%E3%81%B9%E3%81%8D%E3%83%87%E3%83%95%E3%82%A9%E3%83%AB%E3%83%88%E7%B7%A9%E5%92%8C%E7%AD%96+%E7%AB%AF%E6%9C%AB%E7%B7%A8#l81f245a) | パターンファイルの更新、クイックスキャン(日次)・完全スキャン (週次)の実施。 | 初期侵入の軽減／マルウェアの実行の防止 | スキャンが重く、PCが遅くなる | SSDもしくはSSD搭載PCへの換装検討（業務効率も向上） |
| 5 | [脆弱性修正プログラムの適用](https://www.softwareisac.jp/ipa/index.php?%E6%9C%80%E4%BD%8E%E9%99%90%E6%A4%9C%E8%A8%8E%E3%81%99%E3%81%B9%E3%81%8D%E3%83%87%E3%83%95%E3%82%A9%E3%83%AB%E3%83%88%E7%B7%A9%E5%92%8C%E7%AD%96+%E7%AB%AF%E6%9C%AB%E7%B7%A8#lff79275) | 脆弱性を修正するプログラムがリリースされた場合は、リリース後速やかに適用する（対応が難しい場合は代替策を用いる）。 | 初期侵入の軽減／マルウェアの実行の防止 | アプリケーションが動かなくなる | ベンダー情報の収集、互換性の低いアプリの運用停止 |
| 6 | [マクロ・スクリプト禁止と保護ビューの利用](https://www.softwareisac.jp/ipa/index.php?%E6%9C%80%E4%BD%8E%E9%99%90%E6%A4%9C%E8%A8%8E%E3%81%99%E3%81%B9%E3%81%8D%E3%83%87%E3%83%95%E3%82%A9%E3%83%AB%E3%83%88%E7%B7%A9%E5%92%8C%E7%AD%96+%E7%AB%AF%E6%9C%AB%E7%B7%A8#j72da14a) | Office、Acrobat製品等のマクロを禁止し、保護ビューを設定し、外部からのファイルは保護ビューを解除しない。 | 初期侵入の軽減／マルウェアの実行の防止 | マクロが使えない | マクロ実行用バッチファイルの設定 |
| 7 | [メール・ブラウザーの適切な利用](https://www.softwareisac.jp/ipa/index.php?%E6%9C%80%E4%BD%8E%E9%99%90%E6%A4%9C%E8%A8%8E%E3%81%99%E3%81%B9%E3%81%8D%E3%83%87%E3%83%95%E3%82%A9%E3%83%AB%E3%83%88%E7%B7%A9%E5%92%8C%E7%AD%96+%E7%AB%AF%E6%9C%AB%E7%B7%A8#z8bc75a0) | メールのファイルやリンクはむやみにクリックしない、リンク先を確認する、HTTPSで始まらないサイトは閲覧しない、パスワード解析ツールがあることからID/パスワードをブラウザーに保存させない、お気に入りは定期的に整理する。 | 初期侵入の軽減／マルウェアの実行の防止 |  | 多要素認証の導入、パスワードマネージャーの導入 |
| 8 | [多要素認証機能の利用](https://www.softwareisac.jp/ipa/index.php?%E6%9C%80%E4%BD%8E%E9%99%90%E6%A4%9C%E8%A8%8E%E3%81%99%E3%81%B9%E3%81%8D%E3%83%87%E3%83%95%E3%82%A9%E3%83%AB%E3%83%88%E7%B7%A9%E5%92%8C%E7%AD%96+%E7%AB%AF%E6%9C%AB%E7%B7%A8#e752d0de) | 顔認証や指紋認証、トークンなどを利用する。 | 資格情報の窃取の防止／水平展開の防止 | 設定がわからない | 専用サイトへの誘導 |
| 9 | [セキュアなネットワークの利用](https://www.softwareisac.jp/ipa/index.php?%E6%9C%80%E4%BD%8E%E9%99%90%E6%A4%9C%E8%A8%8E%E3%81%99%E3%81%B9%E3%81%8D%E3%83%87%E3%83%95%E3%82%A9%E3%83%AB%E3%83%88%E7%B7%A9%E5%92%8C%E7%AD%96+%E7%AB%AF%E6%9C%AB%E7%B7%A8#jd60a8d0) | フリーWi-Fi（特にパスワード設定のないWi-Fi）は利用せず、テザリングを活用する。httpsのみの接続が望ましい。退職者が出た場合、Wi-Fiのパスワードを変更する。 | 初期侵入の軽減／資格情報の窃取の防止／水平展開の防止 | 見分け方がわからない | IPA コンテンツの活用 |
| 10 | [外部記憶媒体の利用制限](https://www.softwareisac.jp/ipa/index.php?%E6%9C%80%E4%BD%8E%E9%99%90%E6%A4%9C%E8%A8%8E%E3%81%99%E3%81%B9%E3%81%8D%E3%83%87%E3%83%95%E3%82%A9%E3%83%AB%E3%83%88%E7%B7%A9%E5%92%8C%E7%AD%96+%E7%AB%AF%E6%9C%AB%E7%B7%A8#n3b7ef9d) | USBメモリやスマートフォンの外部記憶媒体で顧客とデータ交換をしない。利用する場合は最新のアンチウイルスソフトで完全スキャン後に利用する。 | 初期侵入の軽減／マルウェアの実行の防止 | 顧客とのコミュニケーションや対応が悪くなる | 社内規程を整備し、社内ルールであることを周知する |
| 11 | [適切に管理・設定されたパスワードの利用](https://www.softwareisac.jp/ipa/index.php?%E6%9C%80%E4%BD%8E%E9%99%90%E6%A4%9C%E8%A8%8E%E3%81%99%E3%81%B9%E3%81%8D%E3%83%87%E3%83%95%E3%82%A9%E3%83%AB%E3%83%88%E7%B7%A9%E5%92%8C%E7%AD%96+%E7%AB%AF%E6%9C%AB%E7%B7%A8#e4927d57) | 初期パスワードの変更（OS、ネットワーク機器等）を行い、端末・サーバーのローカル管理者のパスワードをユニークにする。またパスフレーズを活用し、設定する。 | 資格情報の窃取の防止／水平展開の防止／被害の軽減 | 設定がわからない | 導入業者に指示し、報告を受ける |

### 教育の実施

#### 実施対策

サイバーセキュリティの維持のためには、IT部門・担当者に依存することなく、全社的な取り組みが必須である。サイバーセキュリティ経営を実現するために組織の役割に応じた教育を実施する。

* 経営者向け：  
  リーダーシップをとってサイバーセキュリティ経営を促進するためにセキュリティマネジメントの知識を身に付ける
* 中間管理職向け：  
  セキュリティ設定の重要性や運用の必要性を理解し、指示・対応可能な知識を身に着け、継続的に組織に対して脅威情報などのインプットを行う
* 従業員向け：　  
  設定の意味や運用の背景を理解する

#### コンテンツ

* IPA映像で知る情報セキュリティ ～映像コンテンツ一覧[[7]](#footnote-7)
  + - 組織の情報資産を守れ！-標的型サイバー攻撃に備えたマネジメント-
    - 見えざるサイバー攻撃 -標的型サイバー攻撃の組織的な対策-
    - そのメール本当に信用してもいいんですか？　-標的型サイバー攻撃メールの手口と対策-
    - 今　制御システムも狙われている！ －情報セキュリティの必要性－

### 重要情報資産の暗号化とバックアップの実施

#### 設定・運用対策

組織内で重要情報資産を定義する。

* 情報の内容の識別：  
  個人情報、機微情報、営業情報、技術情報、財務情報等
* 情報の機密度の識別：  
  極秘、営業秘密、秘密、社外秘
* 情報の共有の識別：  
  社内関係者限り、部門限り、関係部門間限り、社外を含む関係者限り、一般公開可能 定義に応じて、重要情報資産へのアクセス設定を行い、その上で暗号化する、しないを決定する。 情報資産の内容に応じて、バックアップの可否、バックアップの実施タイミング（日次、週次、月次、年次等）を決定し、実施する。

#### 攻撃の手口

ゼロディ攻撃や、修正プログラムリリース前に攻撃コードが公開された場合で、アンチウイルスソフトを始めとする緩和策がまったく有効でない場合がある。  
また、ランサムウェアに感染すると、データを暗号化されてしまうだけでなく、情報を窃取し、身代金を支払わない場合、窃取した情報をインターネットに公開するなどの手口も出現している。

#### 現状の課題

データが窃取された場合、情報公開や悪用される可能性があり、事業継続に多大な影響を及ぼす可能性がある。ランサムウェアの場合、身代金を支払っても、データが復号できる保証はない。

#### **対策の効果**

攻撃されることを前提に措置を講じることは、極めて有効である。 重要資産の暗号化は、情報漏洩の際に実質的な漏洩を軽減する効果があり、Zip暗号化やOffice文書のパスワード設定等で容易に設定が可能である。  
バックアップは、ランサムウェアなどの改ざんを行うマルウェア対策として極めて有効である。

#### リスクの受容

万一、マルウェアに感染し、データの暗号化等が実施された場合の復旧コストに比べ、はるかに低コストで防御が可能となるため、暗号化、バックアップを実施しないというリスク受容は推奨できない。

#### 対策による弊害の緩和

バックアップ先として、Dropbox、Google Drive、OneDrive、VBOX などの、ファイルの世代管理を実施するクラウドシステムがあり、情報資産の機密性、重要に応じて、これらの活用も視野に入れるべきである。（ランサムウェアで暗号化される前の世代のファイルで復旧できる）  
OneDriveの場合、マイドキュメント、デスクトップを自動的に随時、バックアップする機能がある。

### 管理者権限の制限

#### 設定・運用対策

管理業務以外の一般業務に携わる利用者には、管理者権限を付与せず、最小限の権限のみ与える。Windows においては、Built-in Administrators に利用者やドメインユーザーを所属させない。

#### 攻撃の手口

マルウェアが、永続性の確保や、アンチウイルスソフトの無効化、改ざん、情報漏洩といった実害を引き起こすためには、管理者権限が必要となる場合がある。

#### 現状の課題

利用者に管理者権限を与えている場合、マルウェアは侵入と同時に管理者権限で様々な行動が可能になり、新たなマルウェアをインターネットから呼び込んだり、C&Cサーバーと通信し、情報を外部に送信するなどの被害が発生する可能性が高まる。  
また、管理者権限であれば、アンチウイルスソフトの停止や、様々なセキュリティ設定を変更でき、監査証跡も消去が可能で、他の端末への拡散も実行可能となる。

#### 対策の効果

一方、標準ユーザーの場合、アプリケーションのインストール、OS やアプリケーションの設定変更が不可能であり、都度、管理者のID、パスワードが必要である。このため、特権昇格を試みている間に、検出が可能になる可能性が高まり、また、水平展開が困難となるなど、被害拡大を緩和できるメリットが大きい。

#### リスク受容

運用に弊害が発生するとの理由から、リスク受容することは危険であり、推奨できない。

#### 対策による弊害の緩和

アプリケーションのインストール、設定変更のための個別のユニークなBuilt-In Administrators の ID、パスワードを PC に保存しないこと、適切な管理を前提に、標準ユーザーに印刷物で付与し、運用することを強く推奨する。

### アンチウイルスソフトの利用

#### 設定・運用対策

アンチウイルスソフトは端末、サーバー起動時にパターンファイルもしくはアンチウイルスソフト自体のバージョンアップを実施する。  
日次1回は、マイドキュメント等のクイックスキャンを実施する。  
週次1回以上、接続されたメディア全体の完全スキャンを実施する。

#### 攻撃の手口

マルウェアは、アンチウイルスソフトの検知を逃れるために、大量の亜種を作成する。亜種が多ければ多いほど、対応するパターンファイルのリリースに一定の時間がかかるためであり、この間に攻撃を完了しようという戦術に基づく。

#### 現状の課題

未対応のパターンファイルの場合、検出が困難であり、対応するパターンファイルのリリースまでの期間（delta）はマルウェアの侵入を許してしまう。

#### 対策の効果

パターンファイルの更新、日次でのマイドキュメントへのクイックスキャン、週次での完全スキャンを実施することで、最新のパターンファイルでの検出ができる可能性が高まる。

#### リスク受容

完全スキャンについては、動作が遅くなる等の弊害も指摘されるが、最新のパターンファイルですべてをスキャンすることは、極めて重要であり、実施しないことで、マルウェアの活動を許す期間が長くなるため、このリスク受容は推奨できない。

#### 対策による弊害の緩和

ハードディスクなどの低速のI/Oを使用している場合、完全スキャンはシステムの動作が緩慢になり、生産性が落ちる。一方で、SSDに換装することで、完全スキャンの弊害は回避できる上、起動や処理全般の高速化による生産性の向上も期待できる。

### 脆弱性修正プログラムの適用

#### 設定・運用対策

脆弱性修正プログラムは、リリース後、早期に適用する。  
テスト期間中や、適用が早期に行えない場合は、脆弱性の性質に応じた適切な緩和策を実施し、監査を強化する。

#### 攻撃の手口

マルウェアは、OSやアプリケーションソフトの脆弱性を利用し、自身のインストールや永続性の確保を行う。

#### 現状の課題

修正プログラム適用によって、アプリケーションが動作しない等の理由で、修正プログラムの適用を実施できない場合がある。また、テストの工数負担が大きくすぐに適用できない場合や、運用上、システムを再起動できない24/365システムが存在する。

#### 対策の効果

脆弱性情報発表の数日後に、その脆弱性を利用する新種のマルウェアが出現するなどの実績があり、早期適用は強く推奨される。

#### リスク受容

リスク受容する場合は、脆弱性の性質とシステムの特性に応じて、アクセス制限、不要なポートの遮断、脆弱性を有するプロトコルやアプリケーションの使用制限などの緩和策を速やかに実施し、監査を強化し検出に努める。

### マクロ・スクリプト禁止と保護ビューの利用

#### 設定・運用対策

Office のマクロは警告を発して原則禁止とする。保護ビューの設定を行う。  
PDF のスクリプトは原則禁止とする。サンドボックスによる保護（表示は、「保護されたビュー」）の設定を行う。

* Adobe Acrobat Standard DCでの設定例

1. [環境設定]>[Java Script]>[Acrobat JavaScript を使用] のチェックボックスを外す。

2. [環境設定]>[Java Script]>[JavaScript のセキュリティ]>[メニュー項目の JavaScript 実行権限を有効にする] のチェックボックスを外す。

3. [環境設定]>[セキュリティ(拡張)]>[サンドボックスによる保護]>[保護されたビュー]>[すべてのファイル] を選択。

#### 攻撃の手口

ローダーと呼ばれるマルウェアは、Office文書、PDF文書に埋め込まれたマクロやスクリプトであり、文書を開かせることで起動する。起動後、ローダーは外部から新たにマルウェア本体をダウンロードする。このように複雑な手順を踏むのは、アンチウイルスソフトによる検出を避けるためである。

#### 現状の課題

業務でマクロ・スクリプトを実行できる環境では、悪意ある文書の保護ビューを解除すると感染してしまう。

#### 対策の効果

業務でマクロ・スクリプトを実行しない環境では、出荷時規程値であるマクロ・スクリプトの禁止を維持し、保護ビューを解除しないことで、被害を緩和できる。

#### リスク受容

多くのマルウェアは、この攻撃手口を利用することから、リスク受容は推奨できない。また、マクロ・スクリプトの利用許可は、一種の脆弱性の容認であることから、文書化し、監査を強化することを推奨する。

#### 対策による弊害の緩和

業務でマクロ・スクリプトを実行する環境では、通常は、レジストリ設定でマクロ・スクリプトを禁止しておき、マクロ・スクリプト使用時のみ、レジストリを許可設定に変更したのち、マクロ・スクリプトファイルを使用する。使用後は、マクロ・スクリプトを禁止設定とする。一連の手順をバッチファイルにして、バッチファイルの操作で完了するようにする。

### メール・ブラウザーの適切な利用

#### 運用対策

HTTPSで始まらないサイトの閲覧、ダウンロードを禁止する。  
電子メールに埋め込まれたWebサイトのリンクをクリックする場合は、実際のリンクを確認し、フィッシングサイトでないことを確実に確認する。HTTPS で始まらないリンクの場合は、送信者に確認するなどを規程化する。  
相手方の実在を対面で確認した以外のメールの送信者はなりすましである可能性が否定できないため、対面もしくは相手方代表電話を経由し実在の確認ができた相手方に限り、リンク、添付文書の閲覧を実施する。

#### 攻撃の手口

マルウェアの初期侵入は、メールに添付した悪意ある文書ファイルや、悪意あるサイトへ誘導する埋め込みされたリンクである。OSやアプリケーションの脆弱性を利用し、Webサイトを閲覧しただけで、マルウェアが送り込まれる。マルウェアはブラウザーのID/Passwordを窃取し、システムへの攻撃や水平展開に利用する。

#### 現状の課題

攻撃者はユーザーとメールのやり取りを数回し、信頼を得たところで、悪意ある文書やリンクを送付してくる。信頼関係があるため、ファイルやリンクを開き被害にあってしまう。

#### 対策の効果

不審なサイトの閲覧を極力回避することで、被害を軽減できる。特に HTTPS で始まらない、鍵マークが表示されないサイトへの接続を禁止する規程を整備し、周知する。

#### リスク受容

Google Chrome は既に HTTPSでなくHTTPのみ で始まるサイトへの接続に警告を発している。2020年10月からは HTTPのみ で始まるサイトからのダウンロードをブロックする予定である。今後、 HTTPS で始まらない、つまりドメインや組織の存在が確認できないサイトの閲覧は、脅威であると認識すべきであり、リスク受容は推奨できない。

#### 対策による弊害の緩和

Chrome を使用する場合は、安全と考えられる HTTPのみで始まるサイトを登録することで、ブロックを回避できる。

### 多要素認証機能の利用

#### 設定・運用対策

多要素認証を利用する。

システム管理者の場合、多要素認証は必須とする。

#### 攻撃の手口

侵入したマルウェアは、ブラウザーやOSが保存しているID /PWなどの情報を窃取し、特権昇格や他の端末への水平展開を試みる。

#### 現状の課題

パスワードは知識（記憶）に頼った認証方式である。一般的に、複雑で長い桁数のパスワードは記憶が困難なため、パスワードを使いまわすか、多少、変更して使いまわすことが多い。このため、何らかの方法でパスワードが漏洩すると、類似のパスワードを生成され、Webサイトやドメインに侵入されてしまう可能性が高い。また、パスワードの場合、漏洩したこと自体を検知するのが困難なため、定期変更が求められるが、定期変更までに攻撃が完了しているかもしれず脆弱である。このように、定期変更は防御とならず、かつ、類推しやすいパスワードを生み出す温床となっている可能性が指摘されている。

#### 対策の効果

多要素認証は、知識もしくは、生体情報と、所有（ハードウェア）のいずれか2種類以上を組み合わせて認証を行うものである。

| **認証要素** | **代表例** | **想定される攻撃や課題** |
| --- | --- | --- |
| 知識 | PIN 、パスワード、パスフレーズ | 総当たり攻撃、辞書攻撃、漏洩パスワードの悪用 |
| 生体 | 顏、指紋、静脈 | 他人誤認識があり、確率的で確定的でない、漏洩した場合の代替がない |
| 所有 | PKI ハードウェアトークン、ワンタイムパスワード生成トークン | 盗難、紛失の際、失効する仕組みが必要 |

これらを複数組み合わせることで脆弱性を補完できるが、知識＋生体の組合せの場合は、情報が揃って窃取された際の対処が難しい。そのため、所有＋知識もしくは所有＋生体で多要素認証を構成する例が多い。万一、パスワードもしくは生体情報が漏洩しても、所有物がなければ認証が成功しない。所有物を紛失、盗難して、パスワードが試行されても、パスワードのロックアウトが実施され、ブルートフォース攻撃は成功しない。

#### リスク受容

多要素認証は導入にコストがかかることがあり、移行期間中に、既存のシステムの認証方式との整合性が取れない場合がある。多要素認証を導入しない場合、ブルートフォース攻撃、辞書攻撃の耐性が強いとされる、長い桁数のパスフレーズの導入を行い、リスクを受容することが考えられる。この場合、同じフレーズの繰り返しや回文の使用、連続した文字列（123456789、qwerty）を禁止する必要がある。  
システム管理者のリスク受容は推奨できない。

### セキュアなネットワークの利用

#### 設定・運用対策

Free Wi-Fi は利用禁止とし、携帯電話でのテザリングを利用する。  
例外的にセキュアでないネットワークに接続する際は、組織もしくは信頼できるプロバイダーまで VPN 接続を行う。  
Wi-Fiは事前共有鍵方式(PSK)ではなく、802.1X/EAP認証を利用する。

#### 攻撃の手口

攻撃者は通信が暗号化されない Free Wi-Fi などで通信を傍受し、認証情報の窃取、システムへの侵入を試みる。特に、認証情報が暗号化されずに送信された場合、なりすましを許してしまう。また、実在する正規のAPアクセスポイント (AP) と同一のSSID、暗号化キーを設置し、Free Wi-Fiのなりすましを行い、通信を傍受するなどの攻撃が実例として存在する。  
退職者が組織の Wi-Fi の事前共有鍵 (PSK) を利用し、若しくは第三者に暴露し、構外から Wi-Fi に接続する可能性がある。

#### 現状の課題

総務省の調査では、65%がFree Wi-Fi の危険性を認知していながらも、48%が実際にはなんら対策を施していないという調査がある。  
退職者が出た場合に Wi-Fi の PSK を変更する組織は少なく、情報漏洩・窃取の脅威が存在している。

#### 対策の効果

テザリングを利用し Free Wi-Fi に接続しないことで、情報窃取・漏洩のリスクを緩和できる。  
ゲストエリアでの組織内 Wi-Fi の AP を設置しない、月次で Wi-Fi の PSK を変更することで、退職者が出ても、情報窃取・漏洩のリスクを緩和できる。802.1X/EAPの場合、ユーザー個別に認証することから、退職者が出た場合、ユーザーアカウントの無効化で対処できる。  
それぞれ、実効性を担保するため、規程を整備することが望ましい。

#### リスク受容

セキュアでないネットワークの利用は、情報窃取・漏洩のリスクが高く危険で、リスク受容は推奨できない。

#### 対策による弊害の緩和

やむを得ずセキュアでないネットワークを利用する際は、VPNソフトウェアを利用し、組織もしくは信頼できるプロバイダーまで、VPN で接続し、セキュアでないネットワーク内での暗号化通信を実施する。

### 外部記憶媒体の利用制限

#### 設定・運用対策

USBメモリ等のリムーバブルメディアの利用を、職務上、やむを得ない場合を除いて許可しない。

リムーバブルメディアを接続する端末は、自動再生を許可しない、自動実行コマンドの実行しない設定を行う。

可能な限り、リムーバブルメディアはアンチウイルスソフト内蔵のものに限定する。

使用が終わったら初期化する。

使用を禁止する場合は、USBメモリ等の挿入を禁止するUSBポートガード等での物理的禁止設定を施す。

#### 攻撃の手口

マルウェアは常時、リムーバブルメディアの接続を監視しており、接続された段階で、リムーバブルメディアに自分自身をコピーし、自動再生機能、自動実行機能を悪用し他の端末への拡散を行う。

#### 現状の課題

客先等で、大量のデータを交換する際に、電子メールや Web アプリケーションを経由することが阻まれるケースがあり、やむなく、リムーバブルメディアを利用せざるを得ない状況が存在する。

#### 対策の効果

利用制限の内、リムーバブルメディアの接続の際の自動再生を禁止し、かつ、アンチウイルスソフト内蔵のリムーバブルメディアを利用することで、リスクを大幅に緩和することが可能である。

#### リスク受容

自動再生、自動実行の禁止は設定容易であり、再生もワンクリックするだけである。自動再生、自動実行のリスクがはるかに高く、受容すべきではない。

### 適切に管理・設定されたパスワードの利用

#### 設定・運用対策

初期パスワードは必ず変更する。  
ロックアウト可能なシステムの場合は、5回連続して間違ったら15分間、ロックアウトを実施する。  
長いパスフレーズを採用する。ただし、連続、繰り返し、回文は排除する。

* 123456789
* aaaaaaaaaaaaa
* qwertyuiop
* monkeyyeknom

#### 攻撃の手口

ルーター、Firewall、IoT 機器の変更されていない初期パスワードは、Web上で多数公開されている。攻撃者は、ブルートフォースや辞書攻撃でインターネットの接続点を攻撃してくる。また、電子メールやWebサイト経由で侵入したマルウェアは、水平展開を行う際に、それまで収集したID、パスワードをもとに推測したパスワードで侵入を試みる。 IoT 機器や Windows の Built-in Administrator の場合、パスワード試行失敗のアカウントロックアウトができないため、ブルートフォースや辞書攻撃は極めて有効である。

#### 現状の課題

ロックアウトが設定された場合、パスワードは8桁、英大文字、英小文字、記号の組み合わせで十分といえるが、上述のようにロックアウトができないシステムの場合、例えば”Ipa#9801” という英数字（大文字、小文字を含む）と記号を使った8桁のパスワードは、攻撃用システムで解析すれば0.83日で解読可能 となる。

#### 対策の効果

”Ipa ha komagome” (長さ20桁）のような長いパスフレーズの場合、解析は困難である。複雑性を要求するよりも、覚えやすいパスフレーズで長さを要求したほうが安全である。

#### リスクの受容

システムの都合上、長い桁数を受け入れない、かつ、ロックアウトができないシステムが存在する。その場合は、極力、複雑かつ完全にランダムで可能な限り長いパスワードを設定する。総当たり攻撃がないか、定期的に監査を行い、兆候がある場合は、パスワードの有効期間を短く設定し、変更するなどを規程化して受容する。システム更新を早め、長い桁数を受け入れる、もしくは、ロックアウト可能なシステムに入れ替える。

#### 対策による弊害の緩和

辞書に掲載されていない単語を採用することが望ましいが、完全にランダムなパスワードは入力間違えも多く発生する。管理者端末からリモート接続の場合に限ってのみ、管理者のパスフレーズで暗号化保存したパスワードファイルからのコピー&ペーストを許可する。

## サイバー攻撃に対する防御 最低限検討すべきデフォルト緩和策 セキュリティ仕様・Webアプリケーション編

Webアプリケーションのコンポーネントの脆弱性や弱いセキュリティ設定は攻撃の的になります。本項では、最低限検討すべきセキュリティやWebアプリケーションの仕様を解説します。

### 暗号化

#### アプリケーションは、暗号で保護されたパスワードのみを送信すること。

#### パスワードを送信するときにパスワードを暗号化するようにアプリケーションを構成する。

#### アプリケーションは、送信される情報の機密性と整合性を保護すること。 データ保護要件に従ってTLS暗号化を要求するように、すべてのアプリケーションシステムを構成する。

### 脆弱性管理

#### アプリケーションは、オーバーフロー攻撃に対して脆弱であってはいけない。 自動境界チェックを実行する言語またはコンパイラを使用するようにアプリケーションを設計する。 抽象化ライブラリを使用して、危険なAPIを抽象化する。 StackGuard、ProPolice、Microsoft Visual Studio / GSフラグなどのコンパイラベースのカナリアメカニズムを使用する。 OSレベルの保護機能を使用し、ユーザー入力の検証を制御する。 ベンダー製品でオーバーフローが特定された場合、アプリケーションにパッチを適用する。

#### システムの初期化が失敗した場合、シャットダウンが失敗した場合、またはアプリケーション中止処理が失敗した場合、アプリケーションは安全な状態に失敗させる。 初期化、シャットダウン、中止などで、アプリケーションが安全でない状態があった場合、その脆弱性を修正する。

#### アプリケーションは、入**力処理及び出力処理の脆弱性の影響を受けない。 入力を受け入れるときはベ**ストプラクティスに従い、アプリケーションが入力を処理する前にすべての入力が要件に照らし、正しい値か検証されることを確認する。 アプリケーションは出力を処理する前にすべての出力を要件に照らし、正しい値か検証されることを確認する。 特定された脆弱性を修正し、すぐに修正できない問題について文書化されたリスク許容度を取得する。

#### すべての製品は、ベンダーまたは開発チームによってサポートされること。 アプリケーション内のサポートされていないすべてのソフトウェア製品を削除または使用停止にする。

#### メンテナンスまたはサポートが利用できなくなったら、アプリケーションを廃止する。 アプリケーションのメンテナンスが継続されていることを確認する。

#### アプリケーションは、XML指向の攻撃に対して脆弱であってはならない。 XML攻撃に対して脆弱ではないコンポーネントを利用するようにアプリケーションを設計する。 脆弱性が発見されたら、アプリケーションコンポーネントにパッチを適用する。

#### アプリケーションは、SQLインジェクションに対して脆弱であってはならない。 アプリケーションを変更し、SQLインジェクションの脆弱性を削除する。

#### アプリケーションは、コマンドインジェクションから保護する。 特殊文字入力をエスケープ/サニタイズするようにアプリケーションを変更するか、アプリケーションアーキテクチャに基づいてコマンドインジェクション攻撃から保護するようにシステムを構成する。

#### アプリケーションは、クロスサイトスクリプティング（XSS）脆弱性から保護する。 ユーザー入力が検証されていることを確認し、ユーザー入力をエンコードまたはエスケープして、埋め込みスクリプトコードが実行されないようにする。 独自のエスケープロジックを構築するのではなく、Webテンプレートシステムまたは自動エスケープ機能を提供するWebアプリケーション開発フレームワークを使用して、アプリケーションを開発する。

### セッション管理

#### アプリケーションは、ログオフ時またはブラウザーのクローズ時にセッションID値やCookieを破棄する。 アプリケーションセッションが終了したら、セッションID Cookieを破棄するようにアプリケーションを構成する。

#### アプリケーションはセッションIDを公開しない。 セッションIDを傍受または改ざんから保護するようにTLS、VPN等でアプリケーションを構成する。

#### アプリケーションは、非表示フィールドに機密情報を保存しない。 非表示フィールドに機密情報を保存しないようにアプリケーションを設計および構成する。ユーザーセッション管理にサーバー側セッション管理技術を使用する。

### 属性管理

#### アプリケーションには、必要に応じて機密属性を表示する機能が必要。 アプリケーションは、データの機密属性（個人情報、機微情報等）を、画面や印刷物に適切に表示する。

### 認証・認可

#### アプリケーションは、ユーザーによる15分間の無効なログオン試行を3回連続して制限する。 15分間に3回、もしくは5回ログオンに失敗すると、アカウントロックを強制するようにアプリケーションを構成する。回数はシステムの特性に応じて検討する。

#### アプリケーションに埋め込み認証データを含めることはできない。 コード、構成ファイル、スクリプト、HTMLファイル、またはASCIIファイルに、クリアテキストの認証データを埋め込まない。

#### SAMLアサーションでSubjectConfirmation要素を使用する場合、アプリケーションはNotOnOrAfter条件を使用する。 SAMLアサーションで<SubjectConfirmation>要素を使用するときに、<NotOnOrAfter>条件を使用するようにアプリケーションを設計および構成する。

#### WS-SecurityまたはSAMLアサーションを使用して、すべてのアプリケーションメッセージで有効期間を検証する。 すべてのWS-SecurityトークンプロファイルおよびSAMLアサーションで有効期間が検証されるようにする。

#### SAMLアサーションでConditionsエレメントを使用する場合、アプリケーションはNotBeforeエレメントとNotOnOrAfterエレメントの両方、またはOneTimeUseエレメントを使用する。 SAMLアサーションで<Conditions>要素を使用するときに、<NotBefore>および<NotOnOrAfter>または<OneTimeUse>の使用を実装するようにアプリケーションを設計および構成する。

#### WS-Securityで保護されたメッセージは、作成および有効期限付きのタイムスタンプを使用する。 WS-Securityメッセージを使用してアプリケーションを設計および構成し、作成および有効期限のタイムスタンプとシーケンス番号を使用する。

#### アプリケーションは、PKIベースの認証を使用する場合、対応する秘密キーへの承認されたアクセスを強制する。 アプリケーションまたは関連するアクセス制御メカニズムを構成して、アプリケーション秘密鍵への許可されたアクセスを強制する。

#### アプリケーションは、パスワード/ PINをクリアテキストとして表示しない。 入力時にパスワードとPINが難読化され、読み取れないようにアプリケーションを構成する。 難読化されたパスワードをコピーしてクリアテキストとして貼り付けることができないように、アプリケーションを設計する。

#### アプリケーションは、PKIベースの認証を利用する場合、受け入れられたトラストアンカーへの証明書パス（ステータス情報を含む）を構築することにより証明書を検証する。 PKIベースの認証を使用する場合、受け入れられたトラストアンカーへの証明書パスを構築するようにアプリケーションを設計する。

#### アプリケーションは、14文字以上のパスワード長を強制する。 パスワードに14文字を要求するようにアプリケーションを構成する。 アプリケーションは、設定されるパスワードに、IDが含まれておらず、000000、12345678、qwerty、monkeymonkeyなどの連続した文字や繰り返しおよびmonkeyeknomのような回文がないことを検証し、不適切と判断された場合は、不適切である理由をユーザーに通知する。

#### アプリケーションは、過度のアカウント権限なしで実行する。 最小限の特権でアプリケーションアカウントを構成する。アプリケーションが管理者資格情報で動作することを許可しない。

#### デフォルトのパスワードを変更する。 可能な場合、パスワードの代わりに強力な認証システムを使用するようにアプリケーションを構成する。そうでない場合は、デフォルトのパスワードを承認済みの強度のパスワードに変更し、パスワードに関するすべてのガイダンスに従う。 デフォルトのパスワードには、P@ssw0rd、pass、製品名などの推測しやすい弱いパスワードを使用しない。

#### アプリケーションは、アクセス制御ポリシーに従って、情報およびシステムリソースへの論理アクセスに対して承認を実施する。 アプリケーションリソースへのアクセス承認を強制する。

#### アプリケーションは、組織ユーザー（または組織ユーザーに代わって動作するプロセス）を一意に識別して認証する。 ユーザーおよびユーザープロセスを一意に識別および認証するようにアプリケーションを構成する。

#### アプリケーションは、パスワードの暗号表現のみを保存する。 パスワードハッシュ値を作成するときは、強力な暗号化ハッシュ関数を使用する。 パスワードハッシュの作成時にランダムなソルト値を使用する。 認証データを含むデータファイルの強力なアクセス制御許可を確認する。

### ネットワーク構成

#### アプリケーションWebサーバーは、DMZで動作する階層型アプリケーションである場合、アプリケーションサーバーおよびデータベースサーバーとは別のネットワークセグメントに存在する必要がある。 他のアプリケーション層からWebサーバーを分離し、DMZデータアクセス制御要件に従って、アプリケーションサーバーおよびデータベースサーバーとは別のネットワークセグメントに配置する。

# サイバー攻撃に対する防御 詳細なデフォルト緩和策

Ⅳ部では、最低限検討すべきデフォルト緩和策を発展させ、OS、アプリケーションへの詳細な技術的緩和策を解説します。

6章では、OWASP ASVS 4.0.1 による詳細なコーディング基準の概要を解説しています。

7章では、Group Policy を有効に活用するための、事前準備を解説しています。

8章から12章は Windows Group Policy を有効に利用するための事前準備について解説しています。

13章と14章はWindows端末とドメインコントローラーのGroup Policyについて解説しています。

## セキュアコーディング

本章では、アプリケーションソフト開発で、自ら脆弱性を作りこまないための安全なプログラム開発の根底となるセキュアコーディングについて解説します。

### セキュアコーディング

セキュアコーディングは、外部からの侵入や、情報の漏洩、悪意あるサイトへの誘導などを防ぐために必要なプログラムの記述規約です。多くの開発言語は、インジェクション攻撃やクロスサイトスクリプティングなどを防ぐ手法を実装していますが、システム開発での要件定義、開発標準、コーディング規約で要求され、かつ、プログラミングレビュー、単体テスト、結合テスト、運用テストで実際にセキュリティが保たれているかをテストする必要があります。

一方で、脅威の洗い出しと実装対策や、実施すべきテスト項目を網羅的に洗い出すことは、大変難しいといわざるを得ません。そこで、本ガイドラインでは、ソフトウェアの脆弱性を識別するための国際標準であるCommon Weakness Enumeration をベースとして、具体的な対策要求を取りまとめたOpen Web Application Security Project（国際ウェブセキュリティ標準機構）の Application Security Verification Standard 4.0.1 JAをセキュアコーディング仕様として採用しました。

### OWASP Application Security Verification Standard 4.0.1 JA

OWASP Application Security Verification Standard 4.0.1 JAは、Software ISACが本年8月に邦訳し、OWASP ASVSのGitHubに収録されたもので、以下のサイトからそれぞれPDF形式で入手が可能です。本書では、巻末のAppendixに収録しています。

(OWASP GitHub)  
<https://github.com/OWASP/ASVS/blob/master/4.0/OWASP-Application-Security-Verification-Standard-4.0-ja.pdf>

(一般社団法人ソフトウェア協会/Software ISAC)  
<https://www.saj.or.jp/documents/NEWS/pr/20200903_OWASP_ASVS4.0-ja.pdf>

全体の構成は以下の通りで、前文の解説とV1:アーキテクチャからV14:API および Web サービスの検証要件、付録で構成されており、14チャプターに渡って、アプリケーション作成におけるセキュリティ要件を網羅しています。全体を通してWebアプリケーションを対象としていますが、Webアプリケーション以外のシステムでも十分に利活用が可能であり、かつ、CWEや米国国立標準技術研究所の電子認証ガイドライン NIST SP800-63-3 に準拠していることから、脅威分析と網羅性、一貫性が確保されたセキュアコーディング規約として位置づけることが出来ます。

### ASVS 4.0.1 の構成

ASVS 4.0.1は以下のように構成されています。

* ヘッダ、口絵、序文、ASVS の使い方、監査と認定
* V1: アーキテクチャ、設計、脅威モデリング要件
* V2: 認証の検証要件
* V3: セッション管理の検証要件
* V4: アクセス制御の検証要件
* V5: バリデーション、サニタイズ、エンコーディングの検証要件
* V6: 保存時における暗号化の検証要件
* V7: エラー処理およびログ記録の検証要件
* V8: データ保護の検証要件
* V9: 通信の検証要件
* V10: 悪意あるコードの検証要件
* V11: ビジネスロジックの検証要件
* V12: ファイルおよびリソースの検証要件
* V13: API および Web サービスの検証要件
* V14: 構成の検証要件
* 付録 A: 用語集
* 付録 B: 参考情報
* 付録 C: Internet of Things の検証要件

### ASVSと契約

実際の利用に当たっては、ASVSの使い方を参照し、各チャプターの項目が、作成するシステムに当てはまるかを検討し、該当する項目については、具体的な実装方法をユーザーとベンダーが合意し、文書化することが望まれます。また、ソフトウェアサプライチェーンの中で実効性を担保するため、要件定義書、システム設計書、コーディング規約等を契約の内容として定め、ベンダーの協力会社等もその対象とすることが重要です。

### ASVSのテーラリング

ASVSはNIST SP800-63に準拠していますが、一方でSP800-63 と全く同じとはいえません。例えば、パスワードの最低文字数は12文字であり､SP800-63 が規程した8文字とは異なり、厳しい設定値を推奨しています。また、パスワードハッシュの手法についても、SP800-63とは異なる見解をのべていますが、いずれも、SP800-63を最低限の基準とみなし、よりリスクを受容しない方向で規程していると考えられます。

従って、仕様策定の際は、初めにASVSの規程値で標準仕様を検討し、ユーザービリティやシステム特性を加味した上で、SP800-63の基準でもリスク受容できると判断された場合は、テーラリングの理由を文書化し、ダウングレードすることをお勧めします。

## 詳細設定対策に必要な措置

セキュリティ対策は、OS、プロトコル、アプリケーションの設定によって、緩和策が有効であったり、場合によっては無効となっているケースが存在します。そのため、すべての設定対策が効果を発揮するための基本的な措置が必要です。

特に、MITRE に基づく詳細設定対策を実施する際は、本項の設定を実施することを強く推奨します。

|  |  |  |
| --- | --- | --- |
| **項番** | **項目** | **内容** |
| 4.4 | Windows の 管理者の設定 | Windows 管理者の厳格かつ限定的運用 |
| 4.5 | プロトコル設定 | 脆弱なプロトコルの排除 |
| 4.6 | 管理インターフェースの保護 | 管理用端末の分離運用 |
| 4.7 | ログとレジストリの保護 | ログの改ざんの排除、レジストリの権限管理 |
| 4.8 | 電子認証について | 電子認証、特にパスワードに関する推奨事項 |
| 4.9 | Windows Group Policyの再読み込み | Group Policyの改ざん防止 |
| 4.10 | レベル1セキュリティ構成（Windows 10） | Group Policyの推奨設定値 |
| 4.11 | Windows Server 2016 Domain Controller |

### Windows の 管理者の設定

#### Windows Administrator の厳格かつ限定的運用の重要性

Windows に組み込まれている特権管理者である Administrator はすべての管理権限を有しています。従って、Administrator 権限で Windows にログオンしている際に、攻撃者や悪意あるプログラムに侵害されると、管理者特権で、永続化、防御の回避（アンチウイルスソフトの停止等）、資格情報の窃取、水平展開が可能となり、情報漏洩、ログの改ざん、サービス停止などの被害を受け、他の端末、サーバーへの拡散を招きます。

このため、安易な Administrator の運用は避けるべきであり、極めて限定的に使用される必要があります。 反対に、Administrator の厳格かつ限定的な運用は、標的型攻撃を始めとする様々な攻撃を緩和する最も有効な措置であり、あらゆるセキュリティ対策の一丁目一番地といえます。

本項では、Active Directory ドメイン環境における Administrator の特性を解説し、Administrator への攻撃と防御方法を述べます。

#### Windows Administrator の特徴

Windowsには ビルトイン Administrator とビルトイン Administrators があります。それぞれの特徴を述べます。

##### ビルトイン Administrator の特徴

ローカル管理者、ローカルAdministrator などと表現されることがありますが、ここでは、ビルトイン Administrator といいます。ビルトイン Administratorは以下の特徴を有します。

* グラフィカル ユーザー インターフェイス, アプリケーション

  自動的に生成された説明ビルトイン Administrator 以外のユーザーは、Windows に変更を加える場合は、以下のようなユーザーアカウント制御（UAC）が表示されますが、ビルトイン Administrator は UAC の表示がなく完全な管理者権限が実行でき、リモート接続の際も UAC が適用されません。

図 ユーザーアカウント制御

* アカウントロックアウト、アカウントの有効期限、ログオン時間が適用されません。
* ビルトイン Administrators から削除できません。
* Windows 10 はビルトイン Administrator は Default で無効となっており、Install の際の最初のユーザーがビルトイン Administrators に所属します。
* Administrator の ID はグループポリシーで変更が可能です。
* Windows Server では Default で有効となっています。
* ドメインコントローラーの場合は、ビルトイン Administrator は存在せず、代わりにドメイン Administrator がビルトイン Administrator として機能します。

##### ビルトイン Administrators の特徴

* ローカルグループ Administrators 、もしくは Administrators に所属するユーザーを指します。
* UAC が適用されます。
* アカウントロックアウト、アカウントの有効期限、パスワードの有効期限、ログオン時間が適用されます。

#### Windows Administrator への攻撃と緩和策

##### ビルトイン Administrator へのブルートフォース攻撃（総当たり攻撃）

ビルトイン Administrator はアカウントロックアウト設定ができないため、ブルートフォース攻撃が可能です。リモートデスクトップ接続 (RDP)、PowerShell (PsSession)、PSEXECなどのリモート接続で実行されます。また、クラウド上の Public IPを持つ仮想マシンに対する RDP でのブルートフォース攻撃は頻繁に実施されることが知られています。

ビルトイン Administrator 以外のコマンドラインによるリモート接続は、通常、UACが適用されるため、マルウェアによる接続を緩和することができますが、ビルトイン Administrator は UAC が適用されないため危険です。

また、NTLM ハッシュが窃取された場合、オフラインで解析するという手法が知られています。この場合、8桁複雑なパスワードでも、2.5時間で解析可能だとの報告[[8]](#footnote-8) があります。

* 暫定的な緩和策

以下の緩和策を設定する前に、ID として Administrator を使用したタスクスケジューラやバッチジョブへの影響を事前に調査してください。

1. グループポリシーでビルトイン Administrator の ID を変更し、攻撃者から推測困難な ID に変更します。  
   [コンピューターの構成]>[Windows の設定]>[セキュリティの設定]>[ローカル ポリシー]>[セキュリティ オプション]>[アカウント:Administrator アカウント名の変更] で 新たなIDを設定します。  
   新たな ID に組織名や組織の略称を含めることは避けるべきです。また、xxxAdmin、xxxSu などの推測容易な文字列も含めることは避けるべきです。
2. IDを変更したビルトイン Administrator のパスワードを少なくとも14桁以上にして、セキュリティログを定期点検しブルートフォース攻撃を検出するようにしてください。また、オフライン攻撃に備えて20桁を超える長いパスフレーズへの移行を検討します。  
   パスフレーズの例:「Hayabusa2 ha Chikyuu ni# Kikanchuu Desu」(スペースを含み39桁)
3. ポリシーでビルトイン Administrator に対しても UAC の適用を行うよう設定します。  
   参考文書: Your Pa$$word doesn't matter  
   https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

* 根本的な緩和策
* 多要素認証の導入  
  多要素認証の導入を検討してください。多要素認証は攻撃者のコストが高くなるため、被害を大幅に軽減することができます。調査によると、多要素認証を使用するアカウントの侵害率は0.1%未満[[9]](#footnote-9)といわれています。  
  Active Directory の場合、多要素認証としては、Windows Hello for Business（所有＋記憶/所有＋生体）、MS-CA やサードパーティーCA による PKI （所有＋記憶）、Windows Helloの導入などが考えられます。
* ビルトイン Administrator の無効化  
  グループポリシーで端末のビルトイン Administrator を無効化します。（Windows 10では既定で無効化されており、最初にログオンしたユーザーがビルトイン Administrators のメンバーになっています)
  + グループポリシーエディターで以下のポリシーを開きます。  
    [コンピューター構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティオプション]>[アカウント:Administrator アカウントの状態] を [無効] にします。
  + ポリシーの規程値

|  |  |
| --- | --- |
| **サーバーの種類または GPO** | **既定値** |
| 既定のドメインポリシー | 未定義 |
| 既定のドメインコントローラーポリシー | 未定義 |
| スタンドアロンサーバーの既定の設定 | 有効 |
| DC の有効な既定の設定 | 有効 |
| メンバーサーバーの有効な既定の設定 | 有効 |
| クライアントコンピューターの有効な既定の設定 | 無効 |

##### ビルトイン Administrator を使った水平展開

組織で端末やサーバーを初期設定する際に、ローカル Administrator の ID、パスワードを共通にすることがあります。これは、セッティングやサポートの管理負担を軽減するためですが、この慣習を狙い、水平展開を図る攻撃が知られています。共通 ID と共通パスワードが摂取できれば、他の端末、サーバーへのリモートアクセスが可能となります。

* 緩和策

1. ローカル Administrator のパスワードを一台ずつ、すべてユニークにします。リモートでこの作業を一括して展開できるツール LAPS (Local Administrator Password Solution) が、Microsoft から無償で提供されています。  
   ローカル管理者パスワードソリューション（LAPS）導入ガイド（日本語版）  
   <https://msrc-blog.microsoft.com/2020/08/26/20200827_laps/>
2. その上で、ポリシーで [Apply UAC restrictions to local accounts on network logons] を有効にします。これによって、ローカルアカウントにネットワーク経由でログオンする際にUACが適用されます。  
   [コンピューターの構成]>[ポリシー]>[管理用テンプレート]>[MS Security Guide]> [Apply UAC restrictions to local accounts on network logons]  
   参考 ユーザー アカウント制御、Windows Vista でリモートの制限の説明:   
   https://support.microsoft.com/ja-jp/help/951016.
3. ポリシーでビルトイン Administrator に対しても UAC の適用を行うよう設定します。  
   |[コンピューターの構成]>[Windows の設定]>[セキュリティの設定]>[ローカル ポリシー]>[セキュリティ オプション]>[ユーザー アカウント制御: ビルトイン Administrator アカウントのための管理者承認モード] でポリシーを [有効] にします。|

##### ドメインユーザーがビルトイン Administrators に所属している場合の攻撃

ドメインユーザーがビルトイン Administrators に所属している場合、マルウェアが侵入すると、マルウェアはビルトイン Administrators で許可される行動が可能になります。

* 実行可能な戦術

悪意あるプログラムの実行、永続化、防御回避、資格情報へのアクセス、情報の窃取、外部送信、ログ改ざん、破壊

* 緩和策

ドメインユーザーは標準ユーザーで運用し、ビルトイン Administrators にドメインユーザーを登録しないようにします。この措置で、アプリケーションのインストールやWindowsの設定変更のたびに UAC が起動し、管理者のID、パスワードが求められるようになり、マルウェアが外部からダウンロードした新たなマルウェアのインストールを防ぎます。

業務上、アプリケーションのインストールや設定変更が必要な場合は、ビルトイン Administrators にドメインユーザー以外のユーザーを登録し、個別にユニークなパスフレーズを設定し、必要に応じて入力することで回避します。

##### リスク受容する場合の注意点

ユーザーの利便性や業務の遂行を優先し無条件にリスク受容を行った場合、予期せぬインシデント招く可能性が高まります。利用者とともに「正しくリスクを認識し、インシデント発生時の事業への影響を検討」した上でリスク受容を行います。

1. 一般業務でのリスク受容は、まったく推奨できません。メールやWebの閲覧を行わない、インターネットに接続しない完全な閉域網であってもリスク受容は避けるべきです。
2. 開発環境におけるDebugコマンド実行やヘルプデスク業務などでは、管理者権限が必要となることから緩和策の設定が困難な場合があります。  
   このような場合は、対象の端末やシステムを限定し、仮想化、ネットワークセグメントの分離やフィルタリング、メールやWebの閲覧の禁止などの措置を講じた上で文書化し、一定のリスクを受容しつつ、検知に努めることを検討して下さい。また、以下の教育や緩和策は規程にし、実効性を担保してください。

* 利用者への教育

Administrators にドメインユーザーが含まれる環境への脅威を利用者とともに認識します。

* 攻撃手法について理解する（攻撃ベクトルの研究を参照してください）
* 緩和策
* 脆弱性修正プログラムの適用
* アンチウイルスソフトの日次更新とクィックスキャン及び週次での完全スキャンの実施
* リムーバブルメディアの運用制限、自動再生の禁止
* 電子メール、Webブラウザーの閲覧等の運用制限の検討（仮想マシン上で閲覧する、仮想マシンは異なるネットワークセグメントで接続する等）
* インターネットへの接続制限の検討
* 侵入検知システム、Endpoint Detection and Response 等の導入の検討

## プロトコル設定（Windows）

### Windows SMB

SMBv1はランサムウェアの攻撃を受ける脆弱性を持っています。このため、SMBv1を無効にする必要があります。

なお、Linux ベースのNASやSambaをFile Serverとして使用する例は多数あるため、後述の Linux も参照し、SMBv1の存在に注意してください。

* Microsoft Windows と Windows Server で SMBv1、SMBv2、SMBv3 を検出する方法と有効または無効にする方法：   
  https://support.microsoft.com/ja-jp/help/2696547/detect-enable-disable-smbv1-smbv2-smbv3-in-windows-and-windows-server
* 警告  
  SMBv2 または SMBv3 は無効にしないことをお勧めします。 接続不良等の切り分けを行う場合でも、あくまでも "一時的な" トラブルシューティング手段として、SMBv2 または SMBv3 を無効にしてください。 SMBv2 または SMBv3 を無効なままにしないでください。
* SMBの各バージョンと、対応しているWindows OS   
  SMBのバージョン 対応しているWindows OS

|  |  |
| --- | --- |
| **SMBのバージョン** | **対応しているWindows OS** |
| SMB 1.0（SMBv1） | Windows 2000／XP／Vista／7／8／8.1／10、Windows 2000 Server／Windows Server 2003／2003 R2／2008／2008 R2／2012／2012 R2／2016 |
| SMB 2.0 | Windows Vista／7／8／8.1／10、Windows Server 2008／2008 R2／2012／2012 R2／2016 |
| SMB 2.1 | Windows 7／8／8.1／10、Windows Server 2008 R2／2012／2012 R2／2016 |
| SMB 3.0 | Windows 8／8.1／10、Windows Server 2012／2012 R2／2016 |
| SMB 3.02 | Windows 8.1／10、Windows Server 2012 R2／2016 |
| SMB 3.11 | Windows 10、Windows Server 2016 |

出典：https://www.atmarkit.co.jp/ait/articles/1705/17/news043\_3.html

### Windows TLS

SSL3.0、TLS1.0、TLS1.1には脆弱性があります。TLS1.2 以上を使用するようにしてください。製品のDefault のままでは脆弱性のある暗号が使用されてしまい、攻撃や情報漏洩の原因となります。暗号の脆弱性情報を収集し、Windows の半期リリースに合わせて、少なくとも半年に1回は暗号スイートの見直しを行ってください。

また、Webサーバー側では Linux が使用されることが多いため、後述のTLSの設定を実施してください。

| **SSL/TLS攻撃方法に対する耐性** | **TLS1.3** | **TLS1.2** | **TLS1.1** | **TLS1.0** | **SSL3.0** |
| --- | --- | --- | --- | --- | --- |
| ダウングレード攻撃 | 安全 | | 脆弱 | | |
| バージョンロールバック攻撃 | 安全 | | | | 脆弱 |
| BEAST/POODLE攻撃 | 安全 | | | パッチ適用要 | 脆弱 |

出典：IPA TLS 暗号設定ガイドライン Ver.3.0.1 2020年7月

### 暗号スイート

#### 暗号スイートとは

暗号スイートは、キー交換、バルク暗号化、メッセージ認証の暗号アルゴリズムの組み合わせです。

* キー交換アルゴリズム サーバーとクライアント間で共有キーを作成するための情報を保護します。
* バルク暗号化アルゴリズム サーバーとクライアント間のメッセージを暗号化します。
* メッセージ認証アルゴリズム メッセージの整合性を保証し、ハッシュ生成と署名を行います。
* キー交換 バルク暗号化 楕円曲線
* TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SH384\_P384A
* 署名 ハッシュ

#### Group Policy による暗号スイートの設定

グループポリシーで以下の順序となるよう、設定を確認してください。

[ポリシー]>[コンピューターの構成]>[管理用テンプレート]>[ネットワーク]>[SSL 構成設定］

| **暗号スイート文字列** | **SCH\_USE\_STRONG\_CRYPTO で許可** | **TLS / SSL**  **プロトコルバージョン** |
| --- | --- | --- |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 | はい | TLS 1.2 |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 | はい | TLS 1.2 |
| TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 | はい | TLS 1.2 |
| TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | はい | TLS 1.2 |
| TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 | いいえ | TLS 1.2 |
| TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | はい | TLS 1.2 |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 | はい | TLS 1.2 |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 | はい | TLS 1.2 |
| TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 | はい | TLS 1.2 |
| TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | はい | TLS 1.2 |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | はい | TLS 1.2、TLS 1.1、TLS 1.0 |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | はい | TLS 1.2、TLS 1.1、TLS 1.0 |
| TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | はい | TLS 1.2、TLS 1.1、TLS 1.0 |
| TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | はい | TLS 1.2、TLS 1.1、TLS 1.0 |
| TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 | はい | TLS 1.2 |
| TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | はい | TLS 1.2 |
| TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 | はい | TLS 1.2 |
| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | はい | TLS 1.2 |
| TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | はい | TLS 1.2、TLS 1.1、TLS 1.0 |
| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | はい | TLS 1.2、TLS 1.1、TLS 1.0 |
| TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | はい | TLS 1.2、TLS 1.1、TLS 1.0 |
| TLS\_RSA\_WITH\_NULL\_SHA256 | いいえ | TLS 1.2 注 |
| TLS\_RSA\_WITH\_NULL\_SHA | いいえ | TLS 1.2、TLS 1.1、TLS 1.0、SSL 3.0 注 |

注：アプリケーションが明示的に要求する場合にのみ使用されます。

TLS Cipher Suites in Windows 10 v1903, v1909, and v2004:  
https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-cipher-suites-in-windows-10-v1903

### Linux

NAS (Network Attached Storage) にはLinuxがOSとして採用されるケースが多いため、Linuxを使っているNASに対しては、設定の確認が必要です。

#### Samba SMB

/etc/samba/smb.conf の [global] に以下の項目を追記します。

[global]

server min protocol = SMB2

出典：http://www.samba.gr.jp/project/translation/4.1/htmldocs/manpages/smb.conf.5.html

#### TLS1.0とTLS1.1の無効化

TLS1.2 を使うには OpenSSL のバージョンが 1.0.1 以上であることが必要です。

$ openssl version

OpenSSL 1.1.1 11 Sep 2018

* Apache httpd

次の設定は、Apache httpd サーバーで TLS1.0 と TLS1.1 を無効にします。

vi /etc/httpd/conf.d/ssl.conf

…

SSLProtocol -all +TLSv1.2

…

設定後、Apache httpd を再起動してください。

* nginx

次の設定は、nginx サーバーで TLS1.0 と TLS1.1 を無効にします。

vi /etc/nginx/conf.d/virtual.conf~

…

ssl\_protocols TLSv1.2

…

設定後、nginx を再起動してください。

## 管理インターフェースの保護

### 基本的な考え方

Microsoft は、Pass the Hash 攻撃を防御するため、ドメインコントローラーに対して管理目的で接続できる端末のネットワークの分離を提唱しています。これは管理者の露出を制限し、重要資産にアクセスできる特権の窃取を防ぐとともに、ログ監査の負担を軽減し、検出を容易にするという効果があります。

また、重要資産やアカウントの洗い出しを行った上で、ランサムウェアの被害低減策を検討します。これには、侵入時の攻撃ベクトルの遮断、インターネット分離と水平展開の防止、情報の多重バックアップなどが考えられますが、本稿では重要資産にアクセスするアカウントの保護方法について説明します。

### 管理レイヤーの設定と、アカウント・ネットワーク・管理端末の分離

情報資産の管理単位をドメイン、メンバーサーバー、業務端末の3つのレイヤーで分け、各レイヤーごとに管理者アカウント、管理接続用ネットワーク、管理端末の分離を行います。コストやネットワーク設定上、分離が困難な場合は、最低限、アカウントの分離を行います。

Windows の Built-in Administrator は使用せず、ドメインの Administrators に参加している管理者アカウントを利用します。また、ドメインの Administrators に参加しているアカウントは管理業務専用とし、一般業務での使用を規程で禁止します。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tier** | **管理者グループ** | **管理対象** | **接続可能なレイヤー** | | |
| **Tier 0** | **Tier 1** | **Tier 2** |
| Tire 0 | Domain Admin | ドメインコントローラー、RADIUSサーバー | 〇 | × | × |
| Tire 1 | Member Server Admin | 業務サーバー | × | 〇 | × |
| Tire 2 | Workstation Admin | 業務端末 | × | × | 〇 |

このように、ドメイン、メンバーサーバー、端末の管理ネットワークを分離することで、最も重要なドメインの管理者への露出を最低限にすることで、他のレイヤーへの攻撃があっても、安全に管理者を守りながら対処が可能となります。また、管理ネットワークはトラフィックやノイズが少ないことから、ログの監視が容易であり、異常の早期検出が可能となります。

#### 各レイヤーの設定

* 各レイヤーのネットワーク
* 各レイヤーはセグメントで分離し、アクセスコントロールを実施する
* 管理端末は各管理対象と同じ居室に設置するか、VLANで接続する
* 各レイヤーの管理者
* IDはレイヤーごとにすべてユニークにし、一般業務では使用しないように規程する
* 物理的な多要素認証を採用する
* ロール権限を最小にする
* 各レイヤーの管理端末
* 端末緩和設定 を参照

#### システム管理者の資格情報の保護

システム管理者は、アカウント管理、バックアップ、アクセスコントロール管理、ログ保全など、システム運営における重要な業務を担います。攻撃者にシステム管理者の資格情報が窃取された場合、情報漏洩、情報資産の改ざん、ログの消去、踏み台による他への攻撃など、広範囲な被害が予想されます。従って、システム管理者の認証情報は、重要な情報資産や個人情報と同等以上の保護が必要です。

一方で、パスワードという知識要素の認証は、ログ分析以外に危殆化を知ることができません。例え、定期変更を設定したとしても、次に変更される時期までは、攻撃されるリスクが残ります。

そこで、多要素認証をもちいてシステム管理者の資格情報を保護し、資格情報の窃取、漏洩を防ぎ、情報資産の保全を強化することを推奨します。また、多要素認証導入までは、推測が困難な十分な長さを有するパスフレーズの利用と、ブルートフォース（総当たり）攻撃を困難にするアカウントロックアウトの設定を推奨します。

##### 多要素認証の種類

多要素認証では、知識、所有、生体という認証要素を複数、同時に満たす必要があります。NIST SP800-63B [[10]](#footnote-10)では、次の方式、もしくは組み合わせが要求されています。

|  |  |
| --- | --- |
| **Authenticator** | **内容** |
| 多要素OTPデバイス | PIN を入力することでワンタイムパスワードを生成するデバイス |
| 多要素暗号ソフトウェア | PIN を入力することで秘匿エリアに保存された電子証明書が読み出せるソフトウェア |
| 多要素暗号デバイス | PIN を入力することで秘匿エリアに保存された電子証明書が読み出せるデバイス |
| 記憶シークレット＋ルックアップシークレット | パスワードとリカバリコードの組み合わせ |
| 記憶シークレット＋経路外 | パスワードとSMSによるコード送信 |
| 記憶シークレット＋単一要素OTPデバイス | パスワードとワンタイムパスワード生成デバイス |
| 記憶シークレット＋単一要素暗号ソフトウェア | パスワードとOSの秘匿エリアに保存された電子証明書 |
| 記憶シークレット＋単一要素暗号デバイス | パスワードとデバイスの秘匿エリアに保存された電子証明書 |

##### 管理者の資格情報の管理

ドメインの管理者とエンタープライズ管理者の資格情報は、明確に分離されるべきです。もし同一であったとすると、ドメインとエンタープライズの双方に被害が及ぶ可能性があるからです。また、同様の理由で Windows ドメイン以外のシステム管理者の資格情報を他の Linux などのシステムと共通にすることは、大変、危険といえます。

加えて、各管理者の権限でログオンする端末はクリーンセットアップされた専用端末とすべきです。一般業務端末の転用は、すでにマルウェアに感染している可能性があるためです。

各管理者の権限で、以下の行為を行うことは、規程で明確に禁止されるべきです。

* 管理端末での電子メールの閲覧：  
  フィッシングによるマルウェアの侵入を許し、かつ、管理者特権でマルウェアのインストールを許可することとなるため。
* 管理端末でのWeb の閲覧：  
  ドライブバイダウンロード攻撃などによってマルウェアの侵入を許し、かつ、管理者特権でマルウェアのインストールを許可することとなるため。
* 一般の業務端末へのパスワードを使ったログイン:  
  すでにマルウェアが侵入しており、Pass the Hash 攻撃やキーロガーが動作している場合、パスワードの窃取されるため。

#### 管理端末緩和設定

ドメインコントローラー、メンバーサーバーの管理に使用する端末が汚染されないよう、以下の緩和設定を行い、かつ、実効性を担保するために規程を定める必要があります。

* クリーンセットアップされたものに限定する
* BitLockerによる暗号化
* リムーバブルメディア、スマートフォン等の接続の禁止
* 明示的に必要なポート以外はすべて着信接続を拒否する
* Update以外は、すべてのインターネットアクセスをブロックする、もしくはポートを最小限にし、接続先のIPアドレスを制限する
* 管理に不要なアプリケーションのアンインストール
* Web、電子メールの閲覧の禁止、Office、PDFの閲覧の禁止
* グループポリシー の設定
  + ネットワーク経由でのコンピュータへのアクセス拒否
  + バッチジョブとしてログオンを拒否
  + サービスとしてログオンを拒否
  + リモートデスクトップ経由のログオンを拒否

#### 管理端末とサーバーのログ監査

管理端末とドメインコントローラー、メンバーサーバーのログを監査することで、攻撃の実態を把握します。

##### ログ監査の着目点

ログ監査では、以下を着目点として監査します。

* アカウントが使用された場所(発信元または宛先)。
* 認証実行時(ユーザーが休憩中、休暇中、勤務時間外など)。
* 異常なアカウントの作成 (たとえば、プロビジョニング・システムの外部で作成されたドメイン・アカウント、またはサーバー上で作成されたローカル・アカウント)。
* アカウントを使用した異例のアクティビティ (たとえば、設定の変更や認証ポリシーの失敗)。
* 既知または未知の悪意のある実行可能ファイルの検出。
* 同じホストから使用される、無関係な複数の重要なアカウント (たとえば、同じホストから使用されるドメイン管理者認証情報とサービス・アカウント)。
* 異なる所有者の複数のアカウントが、同じセッション内の同じコンピュータから短時間で認証を行う。
* 重要なオブジェクトの修正(たとえば、Domain Admins のメンバーシップの変更)。
* VPN などの境界アクセスに使用されるアカウントと、リソースへのアクセスに使用されるアカウントの不一致。

##### イベントログの設定

以下のイベントログの収集設定を行います。

* グループポリシーによるコマンドラインインターフェースの監査設定

グループポリシーの [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[システム]>[プロセス作成の監査]>[プロセス作成イベントにコマンドラインを含める] を [有効] に設定します。

**注意：**コマンドライン引数には、パスワードや個人情報が含まれます。Security ログを読み取れるユーザーによる個人情報の漏洩に留意してください。

* イベントビューワーによるタスクスケジューラの監査設定（管理端末毎）

[イベントビューワー（ローカル）]>[アプリケーションとサービスログ]>[Microsoft]>[Windows] >[TaskScheduler]>[Operational] で右クリックし [プロパティ] を開きます。[ログを有効にする] をチェックし、最大ログサイズを [10240] KB に設定し、[イベントを上書きしないでログをアーカイブする] をチェックし、[OK] をクリックします。

* リモートデスクトップの監査（管理端末毎）

[イベントビューワー（ローカル）]>[アプリケーションとサービスログ]>[Microsoft]>[Windows] >[TerminalServices-ClientActiveXCore]>[ Microsoft-Windows-TerminalServices-RDPClient/Operational] で右クリックし [プロパティ] を開きます。[ログを有効にする] をチェックし、最大ログサイズを [10240] KB に設定し、[イベントを上書きしないでログをアーカイブする] をチェックし、[OK] をクリックします。

[イベントビューワー（ローカル）]>[アプリケーションとサービスログ]>[Microsoft]>[Windows] >[TerminalServices-LocalSessionManager]>[ Microsoft-Windows-TerminalServices-LocalSessionManager/Operational] で右クリックし [プロパティ] を開きます。[ログを有効にする] をチェックし、最大ログサイズを [10240] KB に設定し、[イベントを上書きしないでログをアーカイブする] をチェックし、[OK] をクリックします。

[イベントビューワー（ローカル）]>[アプリケーションとサービスログ]>[Microsoft]>[Windows] >[TerminalServices-RemoteConnectionManager]>[ Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational] で右クリックし [プロパティ] を開きます。[ログを有効にする] をチェックし、最大ログサイズを [10240] KB に設定し、[イベントを上書きしないでログをアーカイブする] をチェックし、[OK] をクリックします。

##### 監視するEvent ID

* 監視対象のすべてのコンピュータ
* [Windowsログ]>[Security]
  + Event ID 4688 新しいプロセスが作成されました。  
    詳細：  
    https://docs.microsoft.com/ja-jp/windows/security/threat-protection/auditing/event-4688
  + Event ID 4648 明示的な資格情報を使用してログオンが試行されました。  
    詳細：  
    https://docs.microsoft.com/ja-jp/windows/security/threat-protection/auditing/event-4648
  + Event ID 4624 アカウントが正常にログオンしました。  
    詳細：  
    https://docs.microsoft.com/ja-jp/windows/security/threat-protection/auditing/event-4624
  + Event ID 4625 アカウントがログオンに失敗しました。  
    詳細：  
    https://docs.microsoft.com/ja-jp/windows/security/threat-protection/auditing/event-4625
* ドメインコントローラー
* [Windowsログ]>[Security]
  + Event ID 4769 Kerberos サービス チケットが要求されました。  
    詳細：  
    https://docs.microsoft.com/ja-jp/windows/security/threat-protection/auditing/event-4769
  + Event ID 4768 Kerberos 認証チケット (TGT) が要求されました。  
    詳細：  
    https://docs.microsoft.com/ja-jp/windows/security/threat-protection/auditing/event-4768
  + Event ID 4766 SIDの履歴をアカウントに追加できませんでした。  
    詳細：  
    https://docs.microsoft.com/ja-jp/windows/security/threat-protection/auditing/event-4766
* [アプリケーションとサービスログ]>[Microsoft]>[Windows]> [Authentication] >[ProtectedUserFailures-DomainController]
  + Event ID 100 NLTM usage attempted.
  + Event ID 104 DES or RC4 attempted for Kerberos Authentication.  
    詳細：  
    https://docs.microsoft.com/ja-jp/windows-server/security/credentials-protection-and-management/protected-users-security-group
* [アプリケーションとサービスログ]>[Microsoft]>[Windows]>[Authentication]> [AuthenticationPolicyFailures-DomainController]
  + Event ID 101 – NTLM usage attempted.
  + Event ID 105 – Kerberos authentication from a particular device was not permitted.
  + Event ID 106 – The user or device was not allowed to authenticate to the server.
  + Event ID 305 – Kerberos TGT request did not meet access control restrictions.
  + Event ID 306 – User, device or both do not meet the access control restrictions.  
    詳細：  
    https://docs.microsoft.com/ja-jp/windows-server/security/credentials-protection-and-management/authentication-policies-and-authentication-policy-silos
* [アプリケーションとサービスログ]>[Microsoft]>[CodeIntegrity]
* Event ID 3065 プロセス   
  (通常は lsass.exe) が共有セクションのセキュリティ要件を満たしていない特定のドライバーの読み込みを試行したことを、コードの整合性チェックによって特定したことを記録します。 ただし、設定されたシステム ポリシーのために、イメージの読み込みは許可されました。
* Event ID 3066 プロセス   
  (通常は lsass.exe) が Microsoft 署名のレベル要件を満たしていない特定のドライバーの読み込みを試行したことを、コードの整合性チェックによって特定したことを記録します。 ただし、設定されたシステム ポリシーのために、イメージの読み込みは許可されました。  
  詳細：  
  https://docs.microsoft.com/ja-jp/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection

##### 侵害が疑われた場合の対処

侵害が疑われた際は、フォレンジックの専門家に調査を依頼し、専門家の指示以上の措置を講じないでください。場合によっては、原因の究明が困難になり、**他の潜伏しているマルウェアの検出が出来なくなる可能性**があります。必ず、専門家の指示に従って行動してください。

* 禁止事項
* ネットワークの切断によって解析に必要な情報が消去される可能性があるため、メモリ情報、ディスク情報の保全までは切断しない事。
* ファイルの破損など解析の重大な妨げになる場合があるため、アンチウイルスソフトのフルスキャンは絶対に実行しないこと。

#### アカウントの無効化

専門家のアドバイスに従い、以下の項目の実施タイミングを検討します。

* Active Directoryドメインサービスで侵害が考えられるアカウントを無効にします。
* グループのメンバーシップはハードコーディングされたセキュリティトークンです。そのトークンですでに実行されているプロセスは、セキュリティグループから削除された後も、アカウントの元の権限で実行されます。
* 侵害されたアカウントを削除し、新たにアカウントを登録します。これによって、同じアカウント名でも、異なる識別子 (SID) が新たに割り当てられます。新たなアカウントで必要最低限のバックアップ、パスワードの変更等を行った後、アカウントを再度、削除してください。侵害されたアカウント名はすでに攻撃者に知られているため、別な新しいアカウントで運用してください。

#### ドメインコントローラーの復旧措置

* KRNTGTパスワードハッシュが窃取されている可能性があるため、KRBTGTアカウントを2回リセットする必要があります。  
  https://msrc-blog.microsoft.com/2015/07/29/kerberos-krbtgt-account-password-reset-scripts/  
  https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password
* 他のドメインコントローラーの侵害を調査します。
* Administrator、Administrators、Domain Admin、Enterprise Adminへの侵害を調査し、適宜、アカウント、メンバーの削除、再登録を行います。
* レジストリへの常駐、ログの改ざんを確認するため、それぞれのアクセス権限を調査します。
* スケジュールされたタスクとスクリプトを検証します。

### 最重要資産での物理的アクセス制御

極めて重要な情報資産が存在する場合は、物理的な入退出管理を行うとともに、アクセスコントロールを行うとともに、リモート接続をポリシーで禁止し、ローカルでの物理的な対話型ログオンにのみ限定することを検討します。この場合、物理的多要素認証を導入し、管理アカウントと業務アカウントの分離を行うことで、否認ができないようにし、オブジェクトアクセスの監査を適用して内部不正も防止します。ログは、改ざんを防ぐため、リアルタイムで他のシステムに転送します。

#### 管理者、重要資産にアクセスできる関係者

通常の業務での情報資産へのアクセスを特定し、誰がどのようなリソースにアクセスできるかを棚卸します。次に、各アカウントで、資格情報の窃取やランサムウェアの被害を受けた場合を想定し、適切な緩和策を検討します。

##### 厳重に管理すべきセキュリティグループ、管理者、従業員アカウント

システム管理者やシステム管理者が所属するセキュリティグループとして、以下のアカウントが考えられます。

* Domain Admin
* Enterprise Admin
* Schema Admin
* Account Operators
* Backup Operators
* BUILTIN\Administrator
* ハイパーバイザー管理者
* アプリケーション管理システム、アンチウイルスソフト管理システムなどの管理者
* ソフトウェアのインストール、アップデート、バックアップのためのサービスアカウント
* セキュリティスキャンに使用するサービスアカウント
* ローカル管理者アカウント

##### 管理者、重要資産にアクセスできる関係者への緩和策

管理者アカウントを保護するために、以下の緩和策を実施します。

* 多要素認証の導入
* リスクに応じたシステム管理者規程の策定とユーザー教育
  + 最新の手口の共有
  + これらのアカウントを使用する際にインターネットへの接続を必要最小限にする等のアクセス管理
  + これらのアカウントのログオン成功、ログオン失敗等のログ監査

##### 付加価値の高いビジネス資産へのアクセス権を持っているアカウント

システム管理者以外に付加価値の高い資産へのアクセス権を有するアカウントとして、以下のアカウントが考えられます。コンテンツ管理システムなどは部門に管理を委任している場合があり、注意が必要です。

* メールシステムの管理者
* ファイル共有システムの管理者
* SharePoint、DropBox、BOXなどのコンテンツ管理システムの管理者
* File Server、オンラインバンキング端末などの重要なインフラの管理者
* 経営幹部
* 研究者
* 経理・財務担当者
* 知財・法務担当者
* 役員秘書

##### 付加価値の高いビジネス資産へのアクセス権を持っているアカウントへの緩和策

付加価値の高い資産へのアクセス権を有するアカウントを保護するために、以下の緩和策を実施します。

* 多要素認証の導入
* リスクに応じたシステム管理者規程の策定とユーザー教育
  + 最新の手口の共有
  + 電子メールの添付ファイル、組み込みリンクのサンドボックスによる検査
  + これらのアカウントのログオン成功、ログオン失敗等のログ監査
  + クラウドサービスの脆弱性への対処（パスワード漏洩等）
  + 信頼できるパスワードマネージャーの利用

##### 特権アカウントを使用することが想定される端末

以下の端末は特権アカウントを使用するケースが多いため、マルウェアの初期侵入時に特権でマルウェアが動作することから、感染リスクが極めて高い端末といえます。9.3.1.3 付加価値の高いビジネス資産へのアクセス権を持っているアカウントと同様の緩和策を講じて下さい。

* ヘルプデスクなどのサポートに使用されるコンピュータ
* バッチ処理管理サーバー
* セキュリティスキャナ
* RDP を使用する端末
* PS Remoting を使用する端末
* Debugツール、開発環境を使用する端末

## ログとレジストリの保護

### ログの保護

MITRE ATT&CK で、Disable Windows Event Logging（T1562.002）[[11]](#footnote-11) として採番されているように、攻撃者は攻撃の痕跡から検出されることを避けるために、ログの無効化、改ざん、消去を行います。従って、攻撃の検出・分析を行うためのログの保護は極めて重要な防御策といえます。ログの保護は、コンピュータの役割と機能、ログのアクセス権、保存とバックアップの観点から検討します。

#### コンピュータの役割と機能

Windows サーバー と Windows クライアント は非常に多くの機能を有しており、Windows 独自形式の Event Log と、RFC/W3C で定められた形式のログを出力します。そのため、コンピュータに与えられた役割と機能によって、セキュリティ監査の観点から出力されるログを整理する必要があります。

|  |  |  |
| --- | --- | --- |
| **役割・機能** | **ログの有効化** | **保存場所** |
| Domain Controller  File Server | ・DC 監査ポリシーの詳細な構成および・DC管理用テンプレートを参照してください。 | %systemroot%\System32\winevt\Logs\Security.evtx |
| DNS サーバー | DNSログ | %systemroot%\System32\winevt\Logs\DNS Server.evtx |
| DHCPサーバー | DHCPログ | %systemroot%\System32\Dhcp\DhcpSrvLog-\*.log |
| IIS | Webログ、FTPログ | %SystemDrive%\Inetpub\Logs\Logfiles\W3SVC1\\*.log |
| Network Policy Server (RADIUS) | ユーザー認証およびアカウンティング要求ログ（テキスト、SQL） | %systemroot%\System32\LogFiles\IN\*.log |
| Windows ファイアウォール | [・L1 セキュリティが強化されたWindowsファイアウォール](https://www.softwareisac.jp/ipa/index.php?%E3%83%BBL1+%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%81%8C%E5%BC%B7%E5%8C%96%E3%81%95%E3%82%8C%E3%81%9FWindows%E3%83%95%E3%82%A1%E3%82%A4%E3%82%A2%E3%82%A6%E3%82%A9%E3%83%BC%E3%83%AB) | %systemroot%\system32\LogFiles\Firewal\pfirewall.log |

#### Event Log のアクセス権

すべてのEvent Log のアクセス権（ファイルのプロパティのセキュリティタブ）の設定は、以下のユーザー、グループに与えられていなければなりません。これ以外の文書化されていないユーザーやグループが登録されていた場合は、何らかの特権昇格した上での侵害の可能性を疑う必要があります。

|  |  |
| --- | --- |
| **グループ名またはユーザー名** | **アクセス許可** |
| Eventlog | フルコントロール |
| SYSTEM |
| Domain\Administrators |

また、DNS、DHCP等のログのアクセス権は、保守運用のオペレーターを含めて個別に検討する必要がありますが、権限最小化の考え方から、SYSTEM、Domain\Administrators を基本にして、限定的に ServerOperators などに付与することを検討して下さい。

#### ログの保存とバックアップ

Event Log は初期値で 1Mbyte を超えた場合、上書きという設定になっています。このため、サーバーや端末を構築した場合は、すぐにグループポリシーを適用し、既定の容量を超えた場合は、上書きせずに保存するようにしなければなりません。メンバーサーバー等でドメインに参加しない場合は、構築直後に、手動で Event Log のプロパティを設定する必要があります。特に、セキュリティログは認証、認可の情報が書き込まれるため、優先的に設定を施すべきです。

##### リアルタイムでの転送

米国国防総省の Security Technical Implementation Guide (STIG) では、システムの監査レコードをリアルタイムで他のシステムに転送すべき、としています。リアルタイムで転送することで、ログの改ざんを免れ、正しい検知ができるとの判断です。ただし、大規模システムの場合、ネットワークの負荷も高くなることから、SIEM との統合を見据えて検討してください。

##### Event Log の保存サイズ

セキュリティログは大量のログが書き込まれるため、保存サイズを大きくしますが、100GByte を超える設定をすると、イベントビューワーでの閲覧も困難になる場合が出てきます。一方で、小さい Event Log では、全体の流れや事象を判断することが難しくなります。手動で監査を行う場合は、100GByte程度を上限とし、SIEM や専用の分析ツールを使用する場合は分析するシステムに応じたサイズを設定して下さい。

##### Event Log 関連のツール

Event Log はバイナリ形式であり、ツールを使いわない限り内容を確認することはできません。そのため、イベントログ関連のツールもしくはサードパーティーのイベントログビューワーが必要です。また、 .Net もしくは Win32 インターフェースからアクセスが可能です。

* GUI
* Windows イベントビューアー
* Microsoft Log Parser Studio.Exe[[12]](#footnote-12)
* MessageAnalyzer.Exe （現在はダウンロードできません）
* CUI
* wevtutil.Exe
* WMIC.Exe
* Logparser.Exe
* PowerShell Get-EventLogコマンドレット

### レジストリの保護

MITRE ATT&CK では、 Modify Registry : https://attack.mitre.org/techniques/T1112/ として採番されているように、攻撃者にとってレジストリは、様々な利用方法がある魅力的なストレージという事ができます。例えば、永続性を確保するため、悪意のあるプログラムをファイル形式で保存せずに、レジストリにデータとして書き込み、スタートアップでレジストリから自分自身を読み出しメモリ上で実行したり、収集した情報を保存する場合があります。従って、レジストリに対するアクセス権の監査と、変更があった場合の検出の観点から検討します。

#### レジストリハイブのアクセス権の監査

1. 管理者権限で立ち上げたコマンドプロンプトから、regiedit.exe を実行します。

2. [コンピュータ]>[HKEY\_LOCAL\_MACHINE]>[SECURITY] で右クリックし、[アクセス許可] をクリックし、[詳細設定] をクリックします。

3. 次のアクセス許可を確認します。基本的に規程値を維持します。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **種類** | **プリンシパル** | **アクセス** | **継承元** | **適用先** |
| 許可 | SYSTEM | フルコントロール | なし | このキーとサブキー |
| 許可 | Administrators | 特殊 | なし | このキーとサブキー |

4. [コンピュータ]>[HKEY\_LOCAL\_MACHINE]>[SOFTWARE] で右クリックし、[アクセス許可] をクリックし、[詳細設定] をクリックします。

5. 次のアクセス許可を確認します。基本的に規程値を維持します。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **種類** | **プリンシパル** | **アクセス** | **継承元** | **適用先** |
| 許可 | Users | 読み取り | なし | このキーとサブキー |
| 許可 | SYSTEM | フルコントロール | なし | このキーとサブキー |
| 許可 | Administrators | 特殊 | なし | このキーとサブキー |
| 許可 | CREATOR OWNER | フルコントロール | なし | このキーとサブキー |
| 許可 | ALL APPLICATION PACKAGES | 読み取り | なし | このキーとサブキー |

6. [コンピュータ]>[HKEY\_LOCAL\_MACHINE]>[SYSTEM] で右クリックし、[アクセス許可] をクリックし、[詳細設定] をクリックします。

7. 次のアクセス許可を確認します。基本的に規程値を維持します。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **種類** | **プリンシパル** | **アクセス** | **継承元** | **適用先** |
| 許可 | Users | 読み取り | なし | このキーとサブキー |
| 許可 | SYSTEM | フルコントロール | なし | このキーとサブキー |
| 許可 | Administrators | 特殊 | なし | このキーとサブキー |
| 許可 | CREATOR OWNER | フルコントロール | なし | このキーとサブキー |
| 許可 | ALL APPLICATION PACKAGES | 読み取り | なし | このキーとサブキー |

#### リモートレジストリサービスの無効化

リモートレジストリサービスによって、リモートから操作される可能性があります。Windows サービスの Remote Registry が無効になっていることを確認します。

コントロールパネルからサービスを起動し、 RemoteRegistry が無効になっているかを確認するには、以下のコマンドを管理者権限で実行します。

C:\Windows\system32>sc query RemoteRegistry

* SERVICE\_NAME: RemoteRegistry
* TYPE : 20 WIN32\_SHARE\_PROCESS
* STATE : 1 STOPPED
* WIN32\_EXIT\_CODE : 1077 (0x435)
* SERVICE\_EXIT\_CODE : 0 (0x0)
* CHECKPOINT : 0x0

WAIT\_HINT : 0x0

STATE が [1 STOOPED] になっていることを確認します。

STATE が STOPPED になっていない場合は、以下のコマンドを管理者権限で実行します。

C:\Windows\system32>sc stop RemoteRegistry

C:\Windows\system32>sc config RemoteRegistry start= disabled

## 電子認証について

### 目的

情報システムの認証方式設計は非常に重要です。一方で、近年、認証方式各々での課題や脆弱性に関する研究が進み、従来より安全とされていた運用において、脆弱性が存在する可能性があることが分かってきました。例えば、2017年に改訂された米国国立標準技術研究所（NIST）の電子認証ガイドライン (SP800-63B) では、従来、必要とされてきたパスワードの複雑性や定期変更に関しては非推奨（SHOULD NOT）とし、パスワードには、辞書に含まれるワードや繰り返しまたは連続した文字を含ませないことを厳格に要求（SHALL）しています。 本項では、こうした技術動向を踏まえ、システム特性に応じた認証方式を実装するため、認証方式ごとの技術的な課題や研究成果を整理し解説します。

### 電子認証（本人認証）の方式検討

本項では、電子認証の内、特に情報システム開発で重要となる本人認証の方式を検討するための、考え方やプロセスについて解説します。

#### システム構築における電子認証に関する基本的な考え方

電子認証とは、オンライン上の業務システムやサービスに対して、本人とIDに関連付けられた Authenticator（パスワードや証明書などの認証子）を使い、本人に代わって Authenticator が正当な本人であることを認証システム (Verifier) に対して証明します。この Authenticator が適切に管理されず、例えばパスワードが外部に流出すれば成りすましを許すため、以下の点を考慮して、取り扱うデータと Authenticator の適切な組み合わせを検討する必要があります。

1. 取り扱うシステムやデータ資産の重要度や漏洩や改ざんなどのインパクト
2. 取り扱うシステムやデータ資産にアクセスできる人（職務権限や業務上の役割）、もしくはバッチ処理等でアクセスするシステムの特定
3. アクセスする際の Network や物理的領域での制限
4. Authenticator の特性と危殆化（漏洩等）した際のリスク

特に、①と②の明確化がなされた上で、初めて認証方式の検討が行われるべきであるといえます。

#### 電子認証に使用されるAuthenticatorの種類と課題

##### Authenticator の種類

以下に代表的な Authenticator をあげます。[[13]](#footnote-13)

|  |  |  |
| --- | --- | --- |
| **種類** | **認証要素** | **内容** |
| パスワード | 知識 | ユーザーが記憶するもの。PIN（暗証番号）も含まれる。 |
| ルックアップシークレット | 所有 | 乱数表やリカバリコード表。 |
| 経路外デバイス | 所有 | スマートフォンのSMSによるコード送信、QRコードの読み取り。 |
| 単一要素ワンタイムパスワードデバイス | 所有 | ワンタイムパスワード発生器、もしくはソフトウェア。 |
| 多要素ワンタイムパスワードデバイス | 所有+知識/生体 | パスワードなどを入力すると稼働するワンタイムパスワードデバイス。 |
| 単一要素暗号ソフトウェア | 所有 | 端末に保存されたクライアント電子証明書。 |
| 単一要素暗号デバイス | 所有 | FIDO U2FのUSBドングル。 |
| 多要素暗号ソフトウェア | 所有+知識/生体 | 指紋認証などで有効化されるクライアント電子証明書。 |
| 多要素暗号デバイス | 所有+知識/生体 | パスワード、生体認証で有効化されるクライアント電子証明書が納められたUSBトークン。 |

##### Authenticator に対する脅威

以下にAuthenticator ごとの脅威と対策をあげます。パスワードに関する詳細な課題については、第3章で解説します。

|  |  |  |
| --- | --- | --- |
| **種類** | **脅威** | **対策** |
| パスワード | 総当たり攻撃、辞書攻撃による突破。 | ロックアウト設定。Soltを加えたHashデータの保存。 |
| パスワードを書いたメモやファイルの開示。 | ユーザー教育。罰則を伴う運用規程の施行。 |
| キーロギングによる盗聴。 | アンチウイルスソフト、EDR等での検出。 |
| フィッシングサイトでの漏洩。 | サンドボックス、Webフィルタリングの導入。 |
| ショルダーハッキング。 | ユーザー教育。のぞき見防止フィルターの導入。 |
| 上司や管理者を装った攻撃者からの問い合わせによる漏洩。 | ユーザー教育。 |
| Pass the Hash攻撃による盗聴、漏洩。 | Credential Guardの導入。多要素認証の導入。 |
| ルックアップシークレット | 紛失、盗難、複写による漏洩。 | 封緘し、鍵のかかるロッカー、金庫での保管。 |
| 経路外デバイス | 紛失、盗難による漏洩。 | スマートフォン等のアカウント凍結、再発行。 |
| 単一要素ワンタイムパスワードデバイス | 紛失、盗難による漏洩。 | アカウント凍結、再発行。 |
| 多要素ワンタイムパスワードデバイス | 紛失、盗難による漏洩。 | アカウント凍結、再発行。 |
| 総当たり攻撃、辞書攻撃による突破。 | アカウント凍結、再発行。 |
| 単一要素暗号ソフトウェア | 紛失、盗難による秘密鍵の漏洩。 | 秘密鍵のエクスポート禁止設定。P12形式ファイルをCD-ROM等に記録し、封緘の上、金庫で保管する。 |
| 単一要素暗号デバイス | 紛失、盗難による漏洩。 | 公開鍵の失効もしくはアカウント凍結、再発行。 |
| 多要素暗号ソフトウェア | 紛失、盗難による漏洩。 | 公開鍵の失効もしくはアカウント凍結、再発行。 |
| 多要素暗号デバイス | 紛失、盗難による漏洩。 | 公開鍵の失効もしくはアカウント凍結、再発行 |

##### 脅威からAuthenticator を守る手段

Authenticator を脅威から守る手段として、多要素の利用、物理的な制限、ネットワーク制限などが考えられます。これらを複合的に利用することで、脅威を排除します。ここでは、パスワードを利用する際の強化策をあげます。

* スマートカード、スマートフォンのSMSなどの多要素認証の利用
* 社員証などによる物理的な入退出管理が伴う領域での端末、サーバーでの利用
* IPアドレス制限、端末制限
* Windows における Credential GuardなどのPass The Hash 対策の実施
* ATP、EDRの導入によるエンドポイント監視、SIEMでの監視の実施
* ロールベースアクセス制御 に基づくリスクマネジメントの実施

##### パスワード以外の認証方式の課題

* スマートカードログオン

スマートカードは多要素認証の代表格であり、単一認証に比べればはるかに強固な認証ソリューションを提供します。スマートカード（所有）とPIN（知識）という組み合わせが必要なため、たとえPINが漏洩してもスマートカードがなければ攻撃が成功しないとされています。

しかし、スマートカードログオンでも、Windows の場合は NTLM ハッシュを生成されることから、NTLM ハッシュを悪用する[Pass The Hash攻撃](https://www.softwareisac.jp/ipa/index.php?%E3%83%BBPass+the+Hash" \o "・Pass the Hash)に対して万全ではありません。NTLM ハッシュが窃取されてしまえばスマートカードがなくてもログオンは成功します。従って、スマートカードアカウントの定期的なハッシュのローテーションは必須であり、Credential Guard などのソリューションを組み合わせることで、NTLMハッシュを保護しなければ、期待される効果が発揮されません。

また、紛失や盗難があった場合、スマートカード再発行までの期間は代替の認証方式を用意する必要があり、安全な物理的配布と本人確認など運用面での課題があります。

自営で認証局 (CA) を保有する場合、ルート認証局が署名した中間認証局から証明書を発行したうえで、ルート認証局の秘密鍵をハードウェア・セキュリティ・モジュール (HSM) に保管し、オフラインにしておくなど管理が必要です。

証明書の有効期間が短いと更新が頻繁に起こり、管理負担が増加します。一方で、有効期間の長い証明書を大量に発行しかつ失効すると、有効期限が切れるまでCRL（失効リスト）に収録されるため、CRLが大きくなり、ログオンの際のトラフィックの増大につながるため注意が必要です。

* 生体認証

生体認証は顏、指紋、静脈などの生体情報を使った認証であり、スマートカード（所有）やハードウェアワンタイムパスワード（所有）に比べて持ち歩く必要がなく、紛失や盗難などが起こらないというメリットがあります。しかし、生体情報が漏洩した場合、代替が困難なことから、認証側での生体情報の管理を厳重にする必要があります。また、生体認証は誤認識による他人受入や本人拒否の可能性があり、確率に基づく認証方式といえます。ゆえに重要な情報資産を扱う場合は（知識）や（所有）など、他の要素との組み合わせが必須となってきます。以下に生体認証に関する脆弱性の一覧[[14]](#footnote-14)をあげます。

| **脆弱性** | **概要** |
| --- | --- |
| 他人受け入れ | 自分の生体情報をそのまま提示した場合、他の利用者として偶然受け入れられてしまう。 |
| 狼(wolf) | 複数のテンプレートに対して、高確率で他人受入を可能にする生体情報を有する利用者（狼）が存在する。 |
| 子羊(lamb) | 複数の生体情報に対して、高確率で他人受入を可能にするテンプレートを有する利用者（子羊）が存在する。 |
| 類似性 | 双子等、類似の生体情報を有する人が複数存在してしまう。 |
| 偽生体情報 | 生体情報を物理的に偽造し、それが受け入れられてしまう。 |
| 公開 | 生体情報が本人の同意なく容易に他人の手に渡ってしまう。 |
| 推定 | テンプレートや照合結果が生体情報推定の手掛かりとなる。 |
| 利用者状態 | 被認証者の生体情報が自身の事情で変化し、システムに受け入れられない。また、そうした品質の劣る生体情報を登録することによって、他者になりすましされてしまう。 |
| 入力環境 | 被認証者の生体情報の読取データが環境要因で変化し、システムに受け入れられない。また、そうした品質の劣る生体情報を登録することによって、他者になりすましされてしまう。 |
| 認証パラメータ | 不適切な認証パラメータの設定によって他人受入の可能性が高まる。 |

#### そのほか認証に関する留意点

本項では認証全般に関する留意点を解説します。

##### E-Mailは経路外認証とはならない

NIST SP800-63-Bでは、スマートフォンを使った経路外認証は、検討当初は非推奨でしたが、最終的に ”RESTRICTED” となりました。事前登録済の電話番号が物理デバイスと結びついていることを確認した上で、Authenticator ソフトや SMS にワンタイムパスワードを送信することは問題ありませんが、E-Mail を使った場合は、特定デバイスの所有の証明とはならないため経路外認証とはならず、多要素認証を構成できません。

##### ID管理

* デフォルトの弱いID、パスワードの変更

Administrator、Admin、Adm、root、Su などの、OS、データベース、通信機器などのデフォルトのIDは、総当たり攻撃の際に使用されるため、変更可能な場合は、初期設定時に必ず変更しておく必要があります。IDを変更できれば、総当たり攻撃に対する耐性が確保できます。

OS、ルーター等のデフォルトのパスワードは、インターネット上に公開されており、必ず変更しておく必要があります。

* Windows における Administratorの変更

グループポリシーによって、Administratorを異なるIDに変更します。Administrator利用し続けること、共有利用することは、以下の理由から禁止すべきです。

* 攻撃の対象になりやすい
* ログ等でオペレーターを特定できず、改ざんや成りすましの発見が困難となる
* 退職者が出た際にパスワードの変更が必要となり、類推可能なパスワードの変更が発生したり、記憶されるまでメモ書き等の露出の可能性が高まる

##### 開発者のIDは削除する

開発中に使用した開発者のID、テスト用のIDなど、運用に不要なIDは必ず削除してください。

##### 機器間認証 （Machine To Machine）

機器同士の通信の場合、IDやパスワードがハードコードされるケースが散見されますが、危険です。アクセス権限が設定された外部ファイルに暗号化して保存するなど、変更したい場合にはいつでもリモートで変更できるような構成が必要です。また、デフォルトのIDのまま初期設定されると、1.3.2項同様に総当たり攻撃に対して脆弱となりますので、導入設置時には変更を強制する認証システムの実装が必要です。 PKIを使用する際は、証明書の有効期限切れのないように期限管理に留意してください。

##### 特権ID、パスワードの保管・管理

管理者が利用する特権IDとパスワードなどが記載されたドキュメントを保管する場合は、オフラインが原則です。サーバーや端末には保存せず、CD-ROM等の外部メディアに保存し、CD-ROMケースに封緘して鍵のかかる金庫に保管してください。紙に記録した場合も、同様に封筒に入れて封緘し鍵のかかる金庫に保管します。

##### ID、パスワード、センシティブ情報のハードコードの禁止

ID、パスワードやセンシティブな情報をソースコードに直接書き込まないでください。ハードコードされたID、パスワードなどはプロジェクトに参加した開発者全員が知ることとなり、その時点で危殆化していると考えるべきです。開発時の保全が出来たとしても、運用に入った後で、パスワードが危殆化した場合、ソフトウェアをバージョンアップする必要が出ます。攻撃者がバイナリにアクセスできる場合、逆アセンブルすることでID、パスワードなどの漏洩につながります。対策として、JPCERT/CCの実装例[[15]](#footnote-15) を参照してください。

OSSのソースを受け入れる際は、ハードコードされたID、パスワードの存在を確認し、認証ロジックを実装してください。また、ハードコードしたソースをGit Hubなどで公開しないようにしてください。

Windowsの場合、アプリケーションが使用するユーザーやシステムIDは、Service Principal Name (SPN) を使用し、一般ユーザーアカウントを使用しないでください。

### パスワードの要件と課題

パスワードに関する現在の要件と課題を理解するために、「NIST SP800-63B」からパスワードに対する要求事項（抜粋）をあげ、変更の理由となった研究を紹介します。

#### NIST SP800-63-3の記憶シークレット（パスワード）の要求事項

注：SP800-63BではパスワードやPINを「記憶シークレット」と呼んでいますが、ここでは、パスワードに置き換えています。

一般的にはパスワードや、数字ならばPINとして表されているものは、ユーザーによって決められ、記憶されるシークレットである。パスワードは攻撃者が正しい値を推測したり特定できないように、十分に複雑かつ秘密の状態にしておく必要がある。

* ユーザーが指定する場合、最低8文字以上を要求する (SHALL)
* パスワードの設定、変更を処理する際、一般的に利用されているパスワード、予想できるパスワード、セキュリティ侵害を受けたパスワードと比較する (SHALL)
  + 過去にセキュリティ侵害にあったパスワードリスト
  + 辞書に含まれる言葉
  + サービス名や、ユーザー名、そこから派生するようなものなど、文脈によって特定可能な単語
* パスワードがこれらに該当したらユーザーは異なるパスワードを選びなおす必要があることを通知され、異なる値の選択を求められる (SHALL)
* アカウント乗っ取りのために試みた認証失敗の回数を制限する仕組みを実装する (SHALL)
* 例えば異なる文字種の組合せをパスワードに課すべきではない (SHOULD NOT)
* パスワードが侵害されている、もしくはユーザーの変更要求がない限り、パスワードを例えば定期的に変更するよう要求するべきではない (SHOULD NOT)
* パスワード入力時にペースト機能を利用できることを許可すべきである (SHOULD)

「SHALL（するものとする）」及び「SHALL NOT（しないものとする）」というキーワードは、刊行物に厳密に従うことを要求しており、内容と異なってはならない。

「SHOULD（すべきである」」及び「SHOULD NOT（すべきではない）」は、いくつかある選択肢の中で特定の推奨があることを示しており、他の選択肢については選択も除外もしない。ある行動指針を推奨するが、必須であることまでは要求しない。（否定の意味では）ある選択肢または行動指針を非推奨するが、禁止はしない。

「MAY（してもよい）」及び「NEED NOT（しなくてよい）」は、刊行物の範囲において、行動指針が許容できることを示す。

「CAN（できる）」及び「CANNOT（できない）」は、可能性や、能力があることを示す。その対象が物理的か一時的かにはかかわらない。

#### パスワードの課題

本項では、NIST SP800-63Bが要求事項改訂に至ったとする課題について解説します。

##### 長さについて

NISTとカーネギーメロン大学の研究[[16]](#footnote-16)で、5,000人の参加者に、様々なパスワードを生成させ、その強度を比較したところ、「8文字」・「複雑さ」・「辞書に含まれていない」パスワードよりも、何ら制約を課していない16桁のパスワードが優れていたことが判明しました。パスワードの適切な長さについては、システムの特性によるとしていますが、短すぎるパスワードは辞書攻撃や総当たり攻撃に弱いため、最低8文字とされています。また、長いパスワードが使えるように促進されるべきとしています。

##### 複雑さの課題

複雑さとは、以下の複数の文字種の使用を条件とするもので、通常、3種類か4種類の使用を求めます。

* 英大文字
* 英小文字
* 数字
* 記号（特殊文字）

複雑さは攻撃の困難性を高める有効な手段として考えられていましたが、複雑さを求めることで別な弊害が発生することがフロリダ州立大学[[17]](#footnote-17)らの研究で明らかになっています。ユーザーは複雑さを条件とされると、比較的高い確率で以下のような変更をすることが確認されました。そのため、複雑さを強制してもパスワードの推測が可能であり、強度の向上にはつながらないことが判明しています。

* 最初のパスワード password
* 大文字、小文字、数字の要求 Password1
* 大文字、小文字、数字、記号の要求 Password1!

また、長さが8桁で大文字、小文字、数字、記号のすべての使用を条件とした場合、制約から1桁から7けたまでの組み合わせと、大文字・小文字・数字・記号以外の組合せは除外されるため、組み合わせ数を大幅に下げることになるため効果的ではありません。

##### 定期変更の課題

パスワードの定期変更を求めると、多くのユーザーにおいてパスワードの末尾の記号を増やす・減らす、などの推測しやすいパスワードを設定する傾向があることが分かっています。米国での大規模な研究 では、調査したアカウントの11％は、過去に設定されたパスワードが分かれば、5回未満で現在のパスワードを入手できることが確認されました。これは、5回でロックアウトするシステムの場合、11%のユーザーはオンラインでクラックされてしまう、という事を意味します。また、オフラインの場合は数秒で40%を超えるユーザーの、現在のパスワードの割り出しに成功しています。

安易な、つまり攻撃者にとって類推可能なパスワードを増やすだけであれば、定期変更を求めず、パスワードが危殆化した時だけ、変更するのは合理的といえます。

なお、パスワードに有効期限を設けて定期的に変更を強制する理由として、「パスワードが侵害された場合に備える」があります。しかし、パスワードが侵害されたならば即座に変更をするべきであり、次の定期変更日まで待つことはリスクを高めます。

##### パスワードの使い回しの課題

パスワードの使い回しは危険だという指摘は多数ありますが、さまざまなWebサイトごとにパスワードを変えて、それを覚えるのは大変ですし、いざ必要な時に素早くアクセスできないのはさらに苦痛です。こうしたことから、多くのユーザーはパスワードを使い回します。

SP800-63Bではそれを防止させるため、SP800-63B ではパスワード入力の際のペースト行為を許可しています。これは、パスワード管理ツールの利用を促し、強力なパスワードを手軽に利用するため、としています。

##### 長いパスワードを実装する場合

パスワードの組み合わせは、以下の式で得られます。

組み合わせ数＝b2n

ここで、b は利用可能な文字種であり、標準的な101キーボードではスペースを含めると95種類が利用可能です。パスワードの桁数が6桁であれば、735,091,890,625の組合せがあり、8桁ならば6,634,204,312,890,620と格段に多い組み合わせが考えられます。べき乗であることから、1桁増えれば95倍組み合わせが増えるため、桁数を長めにすることで総当たり攻撃を困難にすることが可能となります。

| **桁数** | **組み合わせ数** |
| --- | --- |
| 1 | 95 |
| 2 | 9,025 |
| 3 | 857,375 |
| 4 | 81,450,625 |
| 5 | 7,737,809,375 |
| 6 | 735,091,890,625 |
| 7 | 69,833,729,609,375 |
| 8 | 6,634,204,312,890,620 |
| 9 | 630,249,409,724,609,000 |
| 10 | 59,873,693,923,837,900,000 |
| 12 | 540,360,087,662,637,000,000,000 |
| 14 | 4,876,749,791,155,300,000,000,000,000 |
| 16 | 44,012,666,865,176,600,000,000,000,000,000 |
| 18 | 397,214,318,458,219,000,000,000,000,000,000,000 |
| 20 | 3,584,859,224,085,420,000,000,000,000,000,000,000,000 |

但し、ユーザーに長いパスワードを求めると次のような弊害が発生します。

* 文字列の繰り返し　　　　　　　　　　　12341234、monkeymonkey、monkeyeknom
* 連続した文字列やキーボード配列の利用　111111111、qwerty、1q2w3e

繰り返しや連続した文字列は、機械的に攻撃用の辞書データを作成できることから、好ましくありません。ある程度の長さを要求する場合は、これらの弊害を取り除くロジックの実装が必要になります。これは、パスフレーズを利用する上でも、同様です。

### パスワード認証に関する要求事項（推奨）

本項は、パスワード認証を実装する際の要求事項と、認証に関する留意事項を解説します。

#### パスワード認証を実装する際の要求事項

今後、構築されるアプリケーションのパスワードの要件として以下を推奨します。強度が低くなるテーラリングをする際は、その理由を明確にして文書化し、ユーザーとベンダーで共有し合意してください。

また、テーラリングの際は、「2.2.3 脅威からAuthenticator を守る手段」を参照してください。Windows認証を利用する際は、「4.13 Windows認証を利用する場合」を参照してください。

なお、パスワード認証の実装については、定期的にログ監査と要求事項の見直しを行い、強度の妥当性を検証してください。

#### 長さと評価

長いパスフレーズが推奨されるが、推測容易なパスフレーズは辞書攻撃の対象となるため、長さとともに内容を評価する。システムの環境条件に応じ、適切なリスク評価を行い、強度を高めるようにする。

* 長さの評価
* 8文字以上の設定を要求し、パスワードの切り捨てをせず64文字以上の設定を許可する
* パスワードの切り捨てはしない
* パスワード評価を実装しない場合、14桁以上を求める
* 推測が容易な文字列かの評価
* 使用を拒否する文字列：
* IDが含まれる場合は拒否する。
* 人名、地名、組織名、組織内で使用される略称、ブランド名が含まれる場合は拒否する。
* IDから個人を特定できる場合、生年月日や電話番号は拒否する。
* 特定の文字列の繰り返し “12341234”、“monkeymonkey” などは拒否する。
* キーボード配列や連続した文字列 “qwertyuiop”、”1q2w3e4r”、“11111111” などは拒否する。
* 評価に違反した場合は、理由と改善方法をユーザーに通知する

#### 定期変更

* パスワードの侵害をチェックしている場合は要求しない
* パスワードの侵害をチェックしていない場合は要求する

#### アカウントロックアウト

* 連続失敗回数 3-5回
* ロックアウト期間 15分以上 もしくは経路外認証によるパスワード変更

#### パスフレーズの推奨と注意喚起の表示

* 20桁を超えるパスフレーズを推奨する旨の表示を実装する
* 推測容易なフレーズを使用しない旨の表示を実装する
* 例：長いパスフレーズはなりすましを防ぐ有効な手段です。  
  但し、姓名、生年月日など個人情報の使用や、第三者から推測可能な組織名、  
  地名や家族などの情報などの文字列を含まないようにご注意ください。

#### 重要資産へのアクセス

* 多要素認証もしくはリスクベース認証を強く推奨する

#### 初回アクセス時のパスワード変更要求

* システム発行のパスワードでの初回アクセス時は、必ずパスワードの変更を求める

#### パスワードの変更

* ユーザーがパスワードを変更する場合は、現在のパスワードを要求する。
* ユーザーがパスワードを忘れた場合、スマートフォンの Authenticator や SMSでの経路外デバイス認証を要求する。 なお、経路外でSMS、電子メールを使用する場合、秘密シークレットは送信しない。

#### ID

* 使用を拒否する文字列
  + root、sa、administrator、admin、adm、推測容易と思われる文字列が含まれる場合は拒否する。

#### パスフレーズの注意点

長いパスフレーズは、オンラインでの総当たり攻撃に対して有効な手段であり、利用が推奨されます。一方で、以下のような推測容易な文字列の組合せでの辞書攻撃が考えられるため、十分な注意が必要です。パスワード変更時の注意喚起を推奨します。

* watashino hahano kyuuseiha tanakadesu 私の 母の 旧姓は 田中です
* chichino shusshinnha nagano desu 父の 出身は 長野 です
* aneno namaeha yuka desu 姉の 名前は 由香 です

### Windows認証を利用する場合

Windows の実装はNIST SP800-63-３よりも古いため、パスワード認証に関する要求事項（推奨） をそのまま適合させることができません。将来に向けての変更までの経過措置として、以下の設定を推奨します。

#### 背景と考え方

Active Directory の [複雑さの要件を満たす必要があるパスワード] ポリシー 本ポリシーにより、複雑さを求める設定をすることで、パスワードにIDを含ませることができなくなり、パスワードの安全性が高まります。

一方で、パスワードの長さを8桁かつ複雑さを要求した場合は、全体の組み合わせ数が減り、推測しやすいパスワードを生み出す温床となります。定期変更による弊害を排除し、かつ、安全なパスワードを設定させるためには、複雑かつ長いパスワードの選択が必要です。

多要素認証の導入した場合は、これらの複雑かつ長いパスワードは不要です。但し、多要素認証を導入した場合でも、Pass The Hass 攻撃の影響が考えられる場合は、Credential Guard による防御を検討して下さい。

#### Windows グループポリシーでの設定

Windows のグループポリシー [コンピューターの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[アカウントポリシー]>[パスワードのポリシー]及び[アカウントロックアウトのポリシー] の設定を解説します。

* Windows Hello やハードウェアトークンなどの多要素認証を導入した場合の [パスワードポリシー]
* PIN を使用する場合、6桁以上とする
* PIN の定期変更、履歴、複雑性は求めない、但し、個人から推測可能な誕生日、電話番号等の使用は認めず、これらを規程化する。
* アカウントロックアウトは3-5回に設定する。
* アカウントロックアウト期間は15分以上、もしくは管理者による解除とする。
  + 多要素認証を導入しない場合の [パスワードのポリシー]
* [パスワードの長さ] は14桁以上を推奨する
* [複雑さの要件を満たす必要があるパスワード] を有効にすることで SamAccountName、DisplayName を ID に含ませることができない事から、有効にする。複雑さの要件は、パスワードの変更時または作成時に強制的に適用される。
* ユーザーのアカウント名またはフル ネームに含まれる 3 文字以上連続する文字列を使用しない。
* 複雑性は長さ 6 文字以上で適用される。
* 次の 4 つのカテゴリのうち 3 つから文字を使う。
  + 英大文字 (A から Z)
  + 英小文字 (a から z)
  + 10 進数の数字 (0 から 9)
  + アルファベット以外の文字 (!、$、#、% など)
* 定期的なセキュリティログ監査もしくはパスワードの漏洩・侵害検査の導入を前提に、[パスワードの有効期間]は[0日]（定期変更を求めない）、[パスワードの履歴を記録する]は[0回]（パスワードの履歴は求めない）とする
* ログ監査の対象 セキュリティログ   
  Event ID:4625（アカウントがログオンに失敗しました）  
  Event ID:4776（資格情報の確認）
* 多要素を導入する場合の [アカウント ロックアウトのポリシー]
* [アカウントのロックアウトのしきい値] を[5回ログオンに失敗] とする
* [ロックアウト カウンターのリセット] を [15分後] とする
* [ロックアウト 期間] を [15分] とする

### リスクの影響度に応じた認証方式の選択

基幹系システムやWebサービスの認証システムの強度は、認証情報が侵害された場合の企業や社会に及ぼす影響を考慮に入れて設定されるべきです。本項では、SP800-63を参考にし、リスクの影響度に応じた認証方式の選択方法を解説します。また、Windows 認証を利用する際は、こちらを参照してください。

#### リスクの影響度の検討

今後、構築されるアプリケーションの認証方式の選択の際には、以下の検討ポイントを参考に、文書化することを推奨します。なお、強度が低くなるテーラリングをする際は、その理由を明確にして文書化し、ユーザーとベンダーで共有し合意してください。

また、テーラリングの際は、脅威からAuthenticator を守る手段を参照してください。

#### 認証方式に係る検討ポイント

アプリケーションの認証方式を検討する際には、認証方式を取り巻く様々なリスクポイントを検討する必要があります。但し、認証方式がどのようなシステム環境で実装されるのかによって検討すべきポイントも異なるため、本書で全てのポイントを網羅することはできません。よって、ここではどのシステムにおいても最低限検討することが推奨される3つのポイントに基づき、具体的な検討例を紹介します。

1. 認証によりアクセス可能となるデータの種別   
   認証によりアクセス可能となるデータが漏洩、破壊・改ざんされることに伴うリスクを検討します。例えば、個人情報や知財情報・営業機密等、機微性の高い情報は一般的にリスクが高いと考えられます。また、本番システム環境の設定ファイル等についても、該当ファイルが破壊・改ざんされた場合、システムの継続性が損なわれることが考えられるため、リスクが高いと考えられます。
2. 認証を行う際のアクセス経路   
   認証を行う際のアクセス経路にも様々なパターンが想定されます。例えば、社内ネットワークにおける特定の端末からのみアクセスを行うのか、または不特定多数の端末から社外のネットワークを介してアクセスを行うのかによって、リスクの軽重は異なります。そのため、どのようなアクセス経路のもとで認証が行われるのかという観点から、認証方式に求めるセキュリティ水準（リスクの高低）を検討する必要があります。
3. 認証により付与される権限の種類   
   認証によって付与される権限が具体的にどのような操作を許可されているのかについても検討すべきです。操作を制限された一般権限(Users Group等)のみが付与されるのか、あるいは全ての操作を許可された管理者権限（Administrators Group等）が付与されるのかによっても、認証方式に求められるセキュリティ水準（リスクの高低）は異なると言えます。

#### 検討例

例えば、上記のポイントを以下のように分類し、それぞれスコアリングします。

|  |  |  |
| --- | --- | --- |
| **検討ポイント** | **高リスク** | **低リスク** |
| ①データの種別 | 1点 個人情報や本番環境設定ファイル等、漏洩、破壊・改ざんに伴う影響の大きいデータ | 0点 左記以外の、公開情報や一時ファイル等、漏洩、破壊・改ざんに伴う影響が小さいデータ |
| ②アクセス経路 | 1点 外部ネットワークからの不特定多数によるアクセス | 0点 社内ネットワークからの特定関係者によるアクセス |
| ③権限の種類 | 1点 管理者権限等、全ての操作が許可される権限の付与 | 0点 一般権限等、操作が制限された権限の付与 |

各検討ポイントのスコアを合算した際に、スコアの合計値が高ければ、認証方式を取り巻くリスクが高いことになり、認証方式に求められるセキュリティ水準も高くすべきと判断します。

|  |  |  |
| --- | --- | --- |
| **リスクスコア** | **リスクの程度** | **認証のイメージ（例）** |
| 3点 | 高 | 不特定多数が外部ネットワークを経由して、個人情報等、または本番環境設定ファイル等の高リスクのデータへアクセスできる管理者権限を付与されるケース |
| 2点 | 中 | 個人情報等、高リスクのデータへ管理者権限をもってアクセス可能だが、社内ネットワークにおける特定端末からのみしかアクセスができないケース  外部ネットワークから不特定多数が個人情報等、高リスクのデータへアクセス可能だが、一部の情報のみ参照が可能な、制限された権限が付与されるケース |
| 1点 | 小 | 個人情報等、高リスクへのデータのアクセスはできない一般権限が付与されているが、外部ネットワークから不特定多数のアクセスを許可するケース  管理者権限が付与されているが、社内ネットワークにおける特定端末から、機微性の低い一般情報へのみアクセスが許可されるケース |
| 0点 | 軽微 | 特定の関係者が社内ネットワークを経由して、公開情報、または開発環境の一時ファイル等へアクセスできる一般権限が付与されるケース |

#### 許容される認証方式の決定

前項で得られた点数に基づき、許容される認証を決定します。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **許容される認証方式** | **0点** | **1点** | **2点** | **3点** |
| 単一要素認証 | 許容 | 許容 | 条件付き許容\* | 使用不可 |
| 多要素認証 | 許容 | 推奨 | 推奨 | 必須 |
| リスクベース認証 |  | 許容 | 推奨 | 強く推奨 |

単一要素認証の条件付き許容 単一要素認証でパスワードを認証方式として選択する場合は、「4 パスワード認証に関する要求事項（推奨）」の要求事項のすべてを満たす必要があります。

### 認証に関する用語解説・資料

#### パスワード認証に関するガイダンス

パスワード認証に関するガイダンスを紹介します。

| **タイトル** | **桁数** | **辞書検査** | **複雑さ** | **定期変更** | **使いまわし** | **多要素** |
| --- | --- | --- | --- | --- | --- | --- |
| [内閣サイバーセキュリティセンター インターネットの安心・安全ハンドブック](https://www.nisc.go.jp/security-site/files/handbook-all.pdf) | 10桁以上 | ー | 英大小数字記号 | 必要なし、流出時に速やかに変更 | 不可 | 推奨 |
| [総務省 国民のための情報セキュリティサイト](https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-2.html) | 適切な長さ | 推奨 | 英数 | 必要なし、流出時に速やかに変更 | 不可 | ー |
| [IPA 今、パスワードが危ない！チョコっとプラス パスワード](https://www.ipa.go.jp/security/chocotto/) | 8文字以上 | 推奨 | 英大小数字記号 | ー | 不可 | ー |
| [NIST SP800-63B Digital Identity Guidelines](https://www.jipdec.or.jp/sp/topics/event/u71kba0000009o56-att/nist_sp_800-63b.pdf) | 8文字以上 | 必須 | 不要 | 不要 | 不可 | システム特性に応じて必須 |
| [OWASP Application Security Verification Standard V4](https://owasp.org/www-project-application-security-verification-standard/) | 12文字以上 | 必須 | 不要 | 不要 | 不可 | システム特性に応じて必須 |
| [国防総省 STIG Windows Server 2016](https://www.stigviewer.com/stig/windows_server_2016/) | 15文字以上 | 必須 | 英大小数字記号 | 60日以下 | 不可 | 必須 |
| [Microsoft Password Guidance](https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf) | 8文字以上 | 必須 | 不要 | 不要 | 不可 | 必須 |
| [Google 強力なパスワードとより安全なアカウントを作成する](https://support.google.com/accounts/answer/9094506) | 8文字以上 | 推奨 | 許容 | ー | 不可 | ー |

#### 用語解説

* + アクティブ認証（Active Authentication）：  
    ユーザーの操作を必要とする認証方式。USBトークン、ワンタイムパスワードデバイス・ソフト、生体認証などのユーザーが所有し管理しているAuthenticatorを使い、正当なユーザーかを判断する。  
    ユーザーの操作が必要で、Authenticator内の秘密の値を検証者（Verifier）側で検証し処理が完結する。内部統制でいう、予防的なコントロールに基づく認証。
  + 申請者（Claimant）：  
    1 つ以上の認証プロトコルを使用して身元が確認される対象者。
  + 多段階認証  
    最初にパスワードやPIN（知識認証）などで認証を行い、それらが認証された場合にもう1つ別の要素を組み合わせて認証を行うことを二段階認証や2ステップ認証という。要素が3つ以上にわたる場合、「多段階認証」という。
  + 多要素認証  
    多要素認証は、認証要素の内2つ以上を使用した認証を指す。多要素認証であるスマートカードは、所有するスマートカードを端末に接続し、知識であるPINが整合することで、内部の秘密鍵へのアクセスが許可され、認証に供される。
  + 単一要素認証  
    認証要素のうち、一つの認証方式を使用する場合を指す。パスワード認証だけなら単一要素認証となる。
  + 認証要素  
    認証に用いる要素であり、知識（What you know)、所持（What you have)、生体( What you are) の三要素がある。パスワードは本人だけが知る知識要素である。
  + パッシブ認証（Passive Authentication）：  
    ユーザーの操作を必要としない認証方式。デバイスの種別、IPアドレス、ユーザーの振る舞い、生体情報などから、正当なユーザーかを判断する。ユーザーの操作は必要なく、検証者（Verifier）側で処理が完結する。  
    内部統制でいう、発見的なコントロールに基づく認証。予防的コントロールを強化するために使用されることが多い。
  + Authenticator：  
    申請者が所有し、管理しているもの（認証子：通常は暗号モジュールまたはパスワード）で、申立人のIDを認証するために使用される。
  + Verifier：  
    認証プロトコルを使用して、1 つまたは 2 つの認証子の所有および管理を確認することで、 申請者の身元を検証するシステムおよび組織。

#### 漏洩パスワード TOP200 の特徴

IPA セキュリティプロジェクトチームが調査した漏洩パスワードTOP200の特徴は以下の通りです。

##### データ出典

https://haveibeenpwned.com/ 2020年6月13日 バージョン4 の 漏洩出現順 SHA-1データを逆変換サイトで逆変換したもので、トップ101の内、1個だけ逆変換に成功しなかったものを除いた200個のパスワードを使用しました。

##### 特徴の考え方と発現数

以下のように特徴を定義し分類しました。

* 単語　　　　　　password、iloveyou など
* キーボード配列　qwertyなどのキーボードの配列に由来するもの  
  　　　　　　　　1234などの連続も配列に由来するものとした
* 連続　　　　　　11111 など
* 繰り返し　　　　123123など
* 語順　　　　　　abcなど
* 語頭　　　　　　キーワードの先頭に1文字だけ追加したもの
* 語尾　　　　　　キーワードの最後に1文字だけ追加したもの
* 置換　　　　　　o → 0、a→@、you→u などの置換

最初に出現した特徴を特徴1とし、次に出現した特徴を特徴2としました。

複数の特徴を有するパスワードは200個中42個で、語尾変化が最も多く、複雑さを求めた場合、数値や記号を追加した可能性を示唆するものと考えられます。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **順位** | **パスワード** | **文字種** | **特徴1** | **特徴2** | **その他** |
| 1 | 123456 | 数 | キーボード配列 |  |  |
| 2 | 123456789 | 数 | キーボード配列 |  |  |
| 3 | qwerty | 英 | キーボード配列 |  |  |
| 4 | password | 英 | 単語 |  |  |
| 5 | 111111 | 数 | 連続 |  |  |
| 6 | 12345678 | 数 | キーボード配列 |  |  |
| 7 | abc123 | 英数 | 連続 |  |  |
| 8 | 1234567 | 数 | キーボード配列 |  |  |
| 9 | password1 | 英数 | 単語 | 語頭・語尾 |  |
| 10 | 12345 | 数 | キーボード配列 |  |  |
| 11 | 1234567890 | 数 | キーボード配列 |  |  |
| 12 | 123123 | 数 | キーボード配列 | 繰り返し |  |
| 13 | 0 | 数 | 1文字 |  |  |
| 14 | iloveyou | 英 | 単語 |  |  |
| 15 | 1234 | 数 | キーボード配列 |  |  |
| 16 | 1q2w3e4r5t | 英数 | キーボード配列 |  |  |
| 17 | qwertyuiop | 英 | キーボード配列 |  |  |
| 18 | 123 | 数 | キーボード配列 |  |  |
| 19 | monkey | 英 | 単語 |  |  |
| 20 | dragon | 英 | 単語 |  |  |
| 21 | 123456a | 英数 | キーボード配列 | 語頭・語尾 |  |
| 22 | 654321 | 数 | キーボード配列 |  |  |
| 23 | 123321 | 数 | キーボード配列 |  |  |
| 24 | 666666 | 数 | 連続 |  |  |
| 25 | 1qaz2wsx | 英数 | キーボード配列 |  |  |
| 26 | 121212 | 数 | キーボード配列 | 繰り返し |  |
| 27 | myspace1 | 英数 | 単語 | 語頭・語尾 |  |
| 28 | homelesspa | 英 | 単語 |  |  |
| 29 | 123qwe | 英数 | キーボード配列 |  |  |
| 30 | a123456 | 英数 | キーボード配列 | 語頭・語尾 |  |
| 31 | 1q2w3e4r | 英数 | キーボード配列 |  |  |
| 32 | 123abc | 英数 | 増分 |  |  |
| 33 | qwe123 | 英数 | キーボード配列 |  |  |
| 34 | 7777777 | 数 | 連続 |  |  |
| 35 | qwerty123 | 英数 | キーボード配列 |  |  |
| 36 | 987654321 | 数 | キーボード配列 |  |  |
| 37 | target123 | 英数 | 単語 | キーボード配列 |  |
| 38 | zxcvbnm | 英 | キーボード配列 |  |  |
| 39 | tinkle | 英 | 単語 |  |  |
| 40 | qwerty1 | 英数 | キーボード配列 | 語頭・語尾 |  |
| 41 | 222222 | 数 | 連続 |  |  |
| 42 | 1g2w3e4r | 英数 | キーボード配列 |  |  |
| 43 | gwerty | 英 | キーボード配列 |  |  |
| 44 | zag12wsx | 英数 | キーボード配列 |  | q をgに置き換え |
| 45 | gwerty123 | 英数 | キーボード配列 |  |  |
| 46 | 555555 | 数 | 連続 |  |  |
| 47 | fuckyou | 英 | 単語 |  |  |
| 48 | asdfghjkl | 英 | キーボード配列 |  |  |
| 49 | 112233 | 数 | キーボード配列 | 繰り返し |  |
| 50 | 1q2w3e | 英数 | キーボード配列 |  |  |
| 51 | qazwsx | 英 | キーボード配列 |  |  |
| 52 | 123123123 | 数 | キーボード配列 | 繰り返し |  |
| 53 | princess | 英 | 単語 |  |  |
| 54 | computer | 英 | 単語 |  |  |
| 55 | 12345a | 英数 | キーボード配列 | 語頭・語尾 |  |
| 56 | 159753 | 数 | キーボード配列 |  |  |
| 57 | ashley | 英 | 単語 |  |  |
| 58 | michael | 英 | 単語 |  |  |
| 59 | football | 英 | 単語 |  |  |
| 60 | 1234qwer | 英数 | 増分 | キーボード配列 |  |
| 61 | sunshine | 英 | 単語 |  |  |
| 62 | aaaaaa | 英 | 連続 |  |  |
| 63 | iloveyou1 | 英数 | 単語 | 語頭・語尾 |  |
| 64 | fuckyou1 | 英数 | 単語 | 語頭・語尾 |  |
| 65 | 789456123 | 数 | キーボード配列 |  |  |
| 66 | daniel | 英 | 単語 |  |  |
| 67 | asdfgh | 英 | キーボード配列 |  |  |
| 68 | 777777 | 数 | 連続 |  |  |
| 69 | 123654 | 数 | キーボード配列 |  |  |
| 70 | 11111 | 数 | 連続 |  |  |
| 71 | princess1 | 英数 | 単語 | 語頭・語尾 |  |
| 72 | 999999 | 数 | 連続 |  |  |
| 73 | abcd1234 | 英数 | 連続 |  |  |
| 74 | 11111111 | 数 | 連続 |  |  |
| 75 | passer2009 | 英数 | 単語 |  |  |
| 76 | love | 英 | 単語 |  |  |
| 77 | shadow | 英 | 単語 |  |  |
| 78 | 888888 | 数 | 連続 |  |  |
| 79 | superman | 英 | 単語 |  |  |
| 80 | football1 | 英数 | 単語 | 語頭・語尾 |  |
| 81 | love123 | 英数 | 単語 | キーボード配列 |  |
| 82 | jordan23 | 英数 | 単語 | キーボード配列 |  |
| 83 | jessica | 英 | 単語 |  |  |
| 84 | 12qwaszx | 英数 | キーボード配列 |  |  |
| 85 | baseball | 英 | 単語 |  |  |
| 86 | monkey1 | 英数 | 単語 | 語頭・語尾 |  |
| 87 | killer | 英 | 単語 |  |  |
| 88 | a12345 | 英数 | キーボード配列 | 語頭 |  |
| 89 | 123456789a | 英数 | キーボード配列 | 語頭・語尾 |  |
| 90 | master | 英 | 単語 |  |  |
| 91 | asd123 | 英数 | キーボード配列 |  |  |
| 92 | asdf | 英 | キーボード配列 |  |  |
| 93 | samsung | 英 | 単語 |  |  |
| 94 | charlie | 英 | 単語 |  |  |
| 95 | azerty | 英 | キーボード配列 |  |  |
| 96 | soccer | 英 | 単語 |  |  |
| 97 | q1w2e3r4t5y6 | 英数 | キーボード配列 |  |  |
| 98 | jordan | 英 | 単語 |  |  |
| 99 | 88888888 | 数 | 連続 |  |  |
| 100 | FQRG7CS493 | 英数 | 単語 |  | ボットによるクラウドサイトへの大量登録が漏洩した結果 |
| 101 | michael1 | 英数 | 単語 | 語尾 |  |
| 102 | jesus1 | 英数 | 単語 | 語尾 |  |
| 103 | blink182 | 英数 | 単語 |  |  |
| 104 | 789456 | 数 | キーボード配列 |  |  |
| 105 | qwer1234 | 英数 | キーボード配列 |  |  |
| 106 | linkedin | 英 | 単語 |  |  |
| 107 | babygirl1 | 英数 | 単語 | 語尾 |  |
| 108 | thomas | 英 | 単語 |  |  |
| 109 | q1w2e3r4 | 英数 | キーボード配列 |  |  |
| 110 | Status | 英 | 単語 | 語頭 |  |
| 111 | michelle | 英 | 単語 |  |  |
| 112 | liverpool | 英 | 単語 |  |  |
| 113 | nicole | 英 | 単語 |  |  |
| 114 | 333333 | 数 | 連続 |  |  |
| 115 | asdasd | 英 | キーボード配列 | 繰り返し |  |
| 116 | qwert | 英 | キーボード配列 |  |  |
| 117 | j38ifUbn | 英数 | 単語 |  |  |
| 118 | 131313 | 数 | 繰り返し |  |  |
| 119 | 987654 | 数 | キーボード配列 |  |  |
| 120 | 123456789 | 数 | キーボード配列 |  |  |
| 121 | lovely | 英 | 単語 |  |  |
| 122 | 0 | 数 | 1文字 |  |  |
| 123 | andrew | 英 | 単語 |  |  |
| 124 | gfhjkm | 英 | キーボード配列 |  |  |
| 125 | joshua | 英 | 単語 |  |  |
| 126 | anthony | 英 | 単語 |  |  |
| 127 | hello1 | 英数 | 単語 | 語尾 |  |
| 128 | justin | 英 | 単語 |  |  |
| 129 | angel1 | 英数 | 単語 | 語尾 |  |
| 130 | zxcvbn | 英 | キーボード配列 |  |  |
| 131 | hello | 英 | 単語 |  |  |
| 132 | iloveyou2 | 英数 | 単語 | 語尾 |  |
| 133 | 1111111 | 数 | 連続 |  |  |
| 134 | 1111 | 数 | 連続 |  |  |
| 135 | jennifer | 英 | 単語 |  |  |
| 136 | naruto | 英 | 単語 |  |  |
| 137 | tigger | 英 | 単語 |  |  |
| 138 | hunter | 英 | 単語 |  |  |
| 139 | welcome | 英 | 単語 |  |  |
| 140 | 159357 | 数 | キーボード配列 |  |  |
| 141 | babygirl | 英 | 単語 |  |  |
| 142 | 147258369 | 数 | キーボード配列 |  |  |
| 143 | pokemon | 英 | 単語 |  |  |
| 144 | 101010 | 数 | 繰り返し |  |  |
| 145 | bitch1 | 英数 | 単語 | 語尾 |  |
| 146 | jessica1 | 英数 | 単語 | 語尾 |  |
| 147 | robert | 英 | 単語 |  |  |
| 148 | 987654321 | 数 | キーボード配列 |  |  |
| 149 | 102030 | 数 | キーボード配列 |  |  |
| 150 | parola | 英 | 単語 |  |  |
| 151 | secret | 英 | 単語 |  |  |
| 152 | 5201314 | 数 | キーボード配列 |  |  |
| 153 | fuckyou2 | 英数 | 単語 | 語尾 |  |
| 154 | 696969 | 数 | 繰り返し |  |  |
| 155 | loveme | 英 | 単語 |  |  |
| 156 | 123456q | 英数 | キーボード配列 | 語尾 |  |
| 157 | purple | 英 | 単語 |  |  |
| 158 | mother | 英 | 単語 |  |  |
| 159 | anthony1 | 英数 | 単語 | 語尾 |  |
| 160 | apple | 英 | 単語 |  |  |
| 161 | qazwsxedc | 英 | キーボード配列 |  |  |
| 162 | money1 | 英数 | 単語 | 語尾 |  |
| 163 | trustno1 | 英数 | 単語 | 語尾 |  |
| 164 | matthew | 英 | 単語 |  |  |
| 165 | buster | 英 | 単語 |  |  |
| 166 | baseball1 | 英数 | 単語 | 語尾 |  |
| 167 | 1111111111 | 数 | 連続 |  |  |
| 168 | andrea | 英 | 単語 |  |  |
| 169 | hannah | 英 | 単語 | 回文 |  |
| 170 | basketball | 英 | 単語 |  |  |
| 171 | freedom | 英 | 単語 |  |  |
| 172 | passw0rd | 英数 | 単語 | 置換 |  |
| 173 | soccer1 | 英数 | 単語 | 語尾 |  |
| 174 | abc | 英 | 語順 |  |  |
| 175 | iloveu | 英 | 単語 | 置換 |  |
| 176 | chelsea | 英 | 単語 |  |  |
| 177 | george | 英 | 単語 |  |  |
| 178 | friends | 英 | 単語 |  |  |
| 179 | william | 英 | 単語 |  |  |
| 180 | samantha | 英 | 単語 |  |  |
| 181 | amanda | 英 | 単語 |  |  |
| 182 | golfer | 英 | 単語 |  |  |
| 183 | summer | 英 | 単語 |  |  |
| 184 | chocolate | 英 | 単語 |  |  |
| 185 | asdf1234 | 英数 | キーボード配列 |  |  |
| 186 | qwerty12 | 英数 | キーボード配列 |  |  |
| 187 | number1 | 英数 | 単語 | 語尾 |  |
| 188 | flower | 英 | 単語 |  |  |
| 189 | maggie | 英 | 単語 |  |  |
| 190 | letmein | 英 | 単語 |  |  |
| 191 | charlie1 | 英数 | 単語 | 語尾 |  |
| 192 | pakistan | 英 | 単語 |  |  |
| 193 | batman | 英 | 単語 |  |  |
| 194 | superman1 | 英数 | 単語 | 語尾 |  |
| 195 | asshole1 | 英数 | 単語 | 語尾 |  |
| 196 | butterfly | 英 | 単語 |  |  |
| 197 | 147258 | 数 | キーボード配列 |  |  |
| 198 | marina | 英 | 単語 |  |  |
| 199 | 10203 | 数 | キーボード配列 |  |  |
| 200 | 1 | 数 | 1文字 |  |  |

## Windows Group Policyの再読み込み

MITRE ATT&CKに基づく詳細設定対策では、Windowsの場合、グループポリシーによって予防的設定をレジストリーに適用します。しかし、攻撃者によってレジストリーが改ざんされた場合、例外を許すことになります。そこで、Group Policyに変更がなくても、必ずグループポリシー全体を読み込み直し、改ざんされた場合でもレジストリーを再度上書きすることでポリシーを維持します。

ただし、定時出社の始業時では、ドメインコントローラーへの負荷が増大する恐れがあります。このため、OUごとにグループポリシーの変更を実施して負荷を計測し、必要に応じてサイトの見直しや、ドメインコントローラーを増強するなどの措置をとってください。

### Windows Group Policy設定

グループポリシーで設定する場合は、以下の設定を実施します。

[コンピューターの構成]>[管理用テンプレート]>[システム]>[グループポリシー]>[レジストリポリシー処理の構成] のポリシー値を [有効] に構成し、[グループポリシーオブジェクトが変更されていない場合でも処理する] を選択する。

### Windows レジストリー（Windows 10、Windows Server 2016確認済）

レジストリーで設定する場合は、以下の設定を実施します。

|  |  |
| --- | --- |
| **項目** | **値** |
| レジストリハイブ | HKEY\_LOCAL\_MACHINE |
| レジストリパス | \SOFTWARE\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2} |
| 値の名前 | NoGPOListChanges |
| 値の種類 | REG\_DWORD |
| 値 | 0 |

## レベル1セキュリティ構成（Windows 10）

このセキュリティ構成は、Microsoft が定めた The Security Configuration Framework (SecCon)[[18]](#footnote-18) の Level 1 Enterprise Basic Security をベースとし、Office 2016/2019、Acrobat Reader のポリシーを追加し、Office 文書や PDF を悪用した悪意あるプログラムの初期侵入や実行を防止するために策定されたものです。

### 設定による影響

本設定を実施することで、以下のような影響が考えられます。

* 脆弱性のある危険なプロトコル SMBv1 を禁止しているため、古い互換性のないNASに接続できない場合があります。この場合は、古いNASの更新を検討して下さい。
* 脆弱性のある危険なプロトコル TLS1.0、TLS1.1 を禁止しているため、TLS1.2を有効化していないWebサイトに接続できない場合があります。この場合は、Webサイトの更新、もしくは、接続の禁止を検討して下さい。
* リモート接続や共有へのアクセスの厳格化や防御設定によって、一部、アプリケーションが動作しないなどの影響が考えられます。事前に、テスト用の OU を作成し、設定を検証してください。
* Office 2016/2019/365 ではマクロの実行に影響が出ます。 Office マクロの影響を参考にしてください。
* Acrobat、Chrome、Edgeなどの動作には影響があったとの報告は受けていませんが、Webアプリケーションの動作テストを行ってください。
* 設定によって影響が出た場合   
  影響が発生した端末、サーバー、ドメインコントローラーの、それぞれのOSのバージョン、ビルド番号、ドメインの機能レベル、現象の詳細をメールでご一報ください。ただし、原因究明やサポートは致しかねますので、ご承知おきください。
* Software ISAC 事務局  
  [gpo@softwareisac.jp](mailto:gpo@softwareisac.jp)

### レベル1セキュリティ構成（Windows 10）

#### 前提となるハードウェア構成

* トラステッドプラットフォームモジュール（TPM）2.0
* Bitlockerドライブ暗号化
* UEFIセキュアブート
* Windows Updateを通じて配布されるドライバーとファームウェア

#### グループポリシーの管理用テンプレートの設定

ドメインコントローラーには、すべての管理用テンプレートはインストールされていません。以下のリンクを参照して、グループポリシー管理用テンプレートのセントラルストアを作成[[19]](#footnote-19)してください。なお、Windows 10 の半期リリースごとの機能の更改に伴い、管理用テンプレートも追加、廃止されますので、ご注意ください。

* 適用するポリシーの一覧
* L1 アカウントポリシー
* L1 ローカルポリシー ユーザー権利の割り当て
* L1 ローカルポリシー セキュリティ オプション
* L1 監査ポリシーの詳細な構成
* L1 セキュリティが強化されたWindowsファイアウォール
* L1 MS Security Guide
* L1 MSS
* L1 ネットワーク
* L1 システム
* L1 Windows コンポーネント
* L1 Windows コンポーネントｰInternet Explorer
* L1 コントロール
* L1 OFFICE2016の共通設定
* L1 Excel 2016
* L1 Word 2016
* L1 Outlook 2016
* L1 OneDrive 2016
* L1 Google Chrome

### ・L1 アカウントポリシー

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[アカウント ポリシー]> [パスワードのポリシー]

* + パスワードの漏洩、危殆化の定期的なチェックを**実施している場合**

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| パスワードの長さ | 8 | ユーザーアカウントのパスワードに使用できる最少文字数を示します。 |
| パスワードの履歴を記録する | 無効 | 以前使ったことがあるパスワードをもう一度使用できるようになるまでに、ユーザーアカウントに引き続き必要がある異なる新しいパスワードの数を示します。 |
| 暗号化を元に戻せる状態でパスワードを保存する | 無効 | オペレーティングシステムが可逆暗号化を使用してパスワードを保存するかどうかを決定します。 |
| 複雑さの要件を満たす必要があるパスワード | 無効 |  |

* + パスワードの漏洩、危殆化の定期的なチェックを**実施していない場合**

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| パスワードの長さ | 14 | ユーザーアカウントのパスワードに使用できる最少文字数を示します。 |
| パスワードの履歴を記録する | 24 | 以前使ったことがあるパスワードをもう一度使用できるようになるまでに、ユーザーアカウントに引き続き必要がある異なる新しいパスワードの数を示します。 |
| 暗号化を元に戻せる状態でパスワードを保存する | 無効 | オペレーティングシステムが可逆暗号化を使用してパスワードを保存するかどうかを決定します。 |
| 複雑さの要件を満たす必要があるパスワード | 有効 | パスワードが複雑さの要件を満たす必要があるかどうかを決定します。 1) ユーザーの SAM アカウント名 (アカウント名) 値または表示名 (フルネーム値) 全体を含めないでください。どちらのチェックでも大文字と小文字は区別されません。 SAM アカウント名は、それがパスワードの一部であるかどうかを判別するためにのみ、完全にチェックされます。SAM アカウント名が 3 文字未満の場合、このチェックはスキップされます。表示名は、区切り文字 (コンマ、ピリオド、ダッシュまたはハイフン、アンダースコア、スペース、シャープ記号、タブ) について解析されます。これらの区切り文字のいずれかが見つかると、表示名が分割され、すべての解析済みセクション (トークン) がパスワードに含まれていないことが確認されます。3 文字未満のトークンは無視され、トークンのサブ文字列はチェックされません。 たとえば、「Erin M. Hagens」という名前は 3 つのトークンに分割されます。「Erin」、「M」、「Hagens」です。2 番目のトークンは 1 文字しかないため、無視されます。したがって、このユーザーはパスワード内の任意の場所にサブ文字列として「erin」または「hagen」を含むパスワードを取得できません。 2) 次の 3 つのカテゴリの文字が含まれている必要があります。 - ヨーロッパ言語の大文字 (発音区別符号、ギリシャ文字およびキリル文字を使用した A から Z) - ヨーロッパ言語の小文字 (発音区別符号、ギリシャ文字およびキリル文字を使用した A から Z) - 基数 10 桁 (0 から 9) - 英数字以外の文字 (特殊文字): (~!@#$%^&\*\_-+=`&3x7c;\(){}[]:;"'<>,.?/) ユーロやイギリス ポンドなどの通貨記号は、このポリシー設定の特殊文字としてはカウントされません。 - アルファベット文字として分類されているが、大文字でも小文字でもない任意の Unicode 文字。これには、アジア言語の Unicode 文字が含まれます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[アカウント ポリシー]> [アカウント ロックアウトのポリシー]

| ポリシー設定 | 値 | 説明 |
| --- | --- | --- |
| アカウントのロックアウトのしきい値 | 3-5 | ユーザーアカウントがロックアウトされる原因となるログオン失敗回数を示します。ロックアウトされたアカウントは、管理者がリセットするか、そのアカウントのロックアウト期間が過ぎるまで使用できません。 |
| ロックアウト カウンターのリセット | 15 | ログオン失敗後、ログオン失敗のカウンタが0（不良ログオン試行）にリセットされるまでに必要な時間を分単位で示します。 |
| ロックアウト期間 | 15 | ロックアウトされたアカウントが自動的にロック解除されるまでのロックアウト期間を分単位で示します。アカウントロックアウトのしきい値が定義されている場合は、アカウントロックアウト期間をリセット時間と同じかそれ以上にしてください。 |

### ・L1 ローカルポリシー ユーザー権利の割り当て

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[ユーザー権利の割り当て]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| オペレーティングシステムの一部として機能 | 誰もいない（空白） | このユーザーの権利を使用すると、プロセスは認証なしでどのユーザーを偽装することもできます。したがって、プロセスはそのユーザーと同じローカル リソースにアクセスできるようになります。 |
| グローバルオブジェクトの作成 | Administrators; LOCAL SERVICE; NETWORK SERVICE; SERVICE | このセキュリティ設定は、ユーザーがすべてのセッションで使用可能なグローバルオブジェクトを作成できるかどうかを決定します。 |
| コンピューターとユーザー アカウントに委任時の信頼を付与 | 誰もいない（空白） | このセキュリティ設定は、ユーザー オブジェクトまたはコンピューター オブジェクトに対する [Trusted for Delegation] 設定を設定できるユーザーを決定します。 |
| デバイスドライバーのロードとアンロード | Administrators | デバイスドライバーまたは他のコードをカーネルモードに動的にロードおよびアンロードできるユーザーを決定します。このユーザー権利は、プラグアンドプレイデバイスドライバーには適用されません。 |
| トークンオブジェクトの作成 | 誰もいない（空白） | プロセスが内部アプリケーション プログラミング インターフェイス (API) でアクセス トークンを作成するときに、ローカル リソースへのアクセス用のトークンを作成するプロセスが使用できるアカウントを決定します。 |
| ネットワーク経由でのアクセス | Administrators;Remote Desktop Users | このユーザーの権利は、ネットワーク経由でコンピューターに接続できるユーザーおよびグループを決定します。リモート デスクトップ サービスはこのユーザーの権利には影響されません。 |
| ファームウェア環境値の修正 | Administrators | ファームウェアの環境値を変更できるユーザーを決定します。ファームウェア環境変数は、非 x86 ベースのコンピューターの不揮発性 RAM に格納される設定です。設定の影響は、プロセッサによって異なります。 |
| ファイルとその他のオブジェクトの所有権の取得 | Administrators | Active Directory オブジェクト、ファイルとフォルダ、プリンタ、レジストリ キー、プロセス、スレッドなど、セキュリティが設定可能な任意のオブジェクトの所有権を取得できるユーザーを決定する。 |
| ファイルとディレクトリのバックアップ | Administrators | システムをバックアップするために、ファイルやディレクトリ、レジストリ、およびその他の固定オブジェクトのアクセス許可をバイパスできるユーザーを決定する。 |
| ファイルとディレクトリの復元 | Administrators | バックアップしたファイルやディレクトリを復元するときにファイル、ディレクトリ、レジストリ、およびその他の持続的なオブジェクトのアクセス許可をバイパスできるユーザーと、任意の有効なセキュリティ プリンシパルをオブジェクトの所有者に設定できるユーザーを決定する。 |
| プログラムのデバッグ | Administrators | 任意のプロセスまたはカーネルにデバッガをアタッチできるユーザーを決定します。独自のアプリケーションをデバッグする開発者にこのユーザーの権利を割り当てる必要はありません。新しいシステム コンポーネントをデバッグする開発者には、このユーザーの権利が必要です。このユーザーの権利は、重要なオペレーティング システム コンポーネントに完全なアクセスを提供します。 |
| ページファイルの作成 | Administrators | どのユーザーとグループが内部アプリケーションプログラミングインターフェイス（API）を呼び出してページファイルのサイズを作成および変更できるかを決定します。 |
| ボリュームの保守タスクを実行 | Administrators | このセキュリティ設定は、リモートデフラグなどのボリュームでメンテナンスタスクを実行できるユーザーとグループを決定します。 |
| メモリ内のページのロック | 誰もいない（空白） | プロセスを使用して物理メモリにデータを保持できるアカウントを決定します。これによって、システムはディスク上の仮想メモリにデータをページングできなくなります。この特権を使用すると、使用できるランダム アクセス メモリ (RAM) の量が減るため、システムのパフォーマンスに重大な影響を与える可能性があります。 |
| リモートコンピュータからの強制シャットダウン | Administrators | ネットワーク上のリモート ロケーションからコンピューターをシャットダウンできるユーザーを決定します。このユーザーの権利を誤用すると、サービス拒否 (Denial-Of-Service) を引き起こす可能性があります。 |
| ローカルログオンを許可 | Administrators、Users | このコンピューターにログオンできるユーザーを決定する。 |
| 永続的共有オブジェクトの作成 | 誰もいない（空白） | オブジェクト マネージャを使ってディレクトリ オブジェクトの作成にプロセスが使用するアカウントを決定する。 |
| 監査とセキュリティログの管理 | Administrators | ファイル、Active Directory オブジェクト、レジストリ キーなど個別のリソースに対してオブジェクト アクセスの監査オプションを指定できるユーザーを決定します。 |
| 資格情報マネージャーに信頼された呼び出し側としてアクセス | 誰もいない（空白） | この設定は、バックアップ/復元の処理中に資格情報マネージャーで使用されます。これは Winlogon のみに割り当てられる特権です。いかなるアカウントにも付与しないでください。この特権を他のエンティティに付与すると、資格情報を保存したユーザーのセキュリティが侵害される可能性があります。 |
| 単一プロセスのプロファイル | Administrators | このセキュリティ設定は、パフォーマンス監視ツールを使用して、システム外のプロセスのパフォーマンスを監視できるユーザーを決定します。 |
| 認証後にクライアントを偽装 | Administrators, SERVICE, Local Service, Network Service | ユーザーにこの特権を割り当てると、そのユーザーに代わって実行されるプログラムがクライアントを偽装できるようになります。この種の偽装にこのユーザー権利が必要となるのは、権限のないユーザーが作成したサービスに (たとえばリモート プロシージャ コール (RPC) や名前付きパイプを使用して) クライアントを接続させ、次にそのクライアントを偽装することによって、管理者レベルまたはシステム レベルなど上位のアクセス許可を得ることを防ぐためです。 |

### ・L1 ローカルポリシー セキュリティ オプション

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[Microsoftネットワーククライアント]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 常に通信にデジタル署名を行う | 有効 | このセキュリティ設定を使用して、SMBクライアントコンポーネントがパケット署名を必要とするかどうかを決定します。 |
| サードパーティ SMB サーバーへの接続に、暗号化されていないパスワードを送信する | 無効 | このセキュリティ設定を有効にすると、サーバーメッセージブロック（SMB）リダイレクタは、認証中のパスワード暗号化をサポートしていない、Microsoft以外のSMBサーバーにテキスト形式のパスワードを送信することができます。暗号化されていないパスワードを送信するのはセキュリティ上の危険があります。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[Microsoftネットワークサーバー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 常に通信にデジタル署名を行う | 有効 | このセキュリティ設定を使用して、SMBサーバーコンポーネントがパケット署名を必要とするかどうかを決定します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[アカウント]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ローカル アカウントの空のパスワードの使用をコンソール ログオンのみに制限する | 有効 | このセキュリティ設定は、物理的なコンピューターコンソール以外の場所からログオンするときに、パスワードで保護されていないローカルアカウントを使用できるかどうかを決定します。この設定が有効な場合、パスワードで保護されていないローカルアカウントへのログインするには、そのコンピューターのキーボードを使用する必要があります。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[システムオブジェクト]

| ポリシー設定 | 値 | 説明 |
| --- | --- | --- |
| 内部システムオブジェクトの既定のアクセス許可を強化する（例：シンボリックリンク） | 有効 | このセキュリティ設定は、オブジェクトの既定の随意アクセス制御リスト（DACL）の強度を決定します。Active Directoryは、DOSデバイス名、ミューテックス、セマフォなどの共有システムリソースのグローバルリストを保持します。このようにして、オブジェクトを見つけてプロセス間で共有できます。各タイプのオブジェクトは、オブジェクトにアクセスできるユーザーと許可されるアクセス許可を指定するデフォルトのDACLを使用して作成されます。このポリシーを有効にすると、既定のDACLが強化され、管理者ではないユーザーは共有オブジェクトを読み取ることができますが、これらのユーザーは作成していない共有オブジェクトを変更できなくなります。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ドメインメンバー]

| ポリシー設定 | 値 | 説明 |
| --- | --- | --- |
| コンピュータ アカウント パスワード：定期的な変更を無効にする | 無効 | ドメインメンバーがそのコンピューターアカウントのパスワードを定期的に変更するかどうかを決定します。 |
| 可能な場合、セキュリティで保護されたチャネルのデータをデジタル的に暗号化する | 有効 | このセキュリティ設定は、ドメインメンバーが開始するすべてのセキュリティで保護されたチャネルトラフィックの暗号化をネゴシエートするかどうかを決定します。有効にすると、ドメインメンバーはすべての安全なチャネルトラフィックの暗号化を要求します。ドメインコントローラーがすべてのセキュリティで保護されたチャネルトラフィックの暗号化をサポートしている場合、すべてのセキュリティで保護されたチャネルトラフィックが暗号化されます。それ以外の場合、安全なチャネルを介して送信されるログオン情報のみが暗号化されます。この設定が無効になっている場合、ドメインメンバーはセキュアチャネル暗号化のネゴシエーションを試行しません。 |
| 可能な場合、セキュリティで保護されたチャネルのデータをデジタル的に署名する | 有効 | このセキュリティ設定は、ドメインメンバーが開始するすべてのセキュリティで保護されたチャネルトラフィックの署名をネゴシエートしようとするかどうかを決定します。有効にすると、ドメインメンバーはすべてのセキュアチャネルトラフィックの署名を要求します。ドメインコントローラーがすべてのセキュリティで保護されたチャネルトラフィックの署名をサポートしている場合、すべてのセキュリティで保護されたチャネルトラフィックが署名されるため、送信中に改ざんされることはありません。 |
| 最大コンピュータ アカウントのパスワードの有効期間 | 30 | ドメインメンバーがコンピューターアカウントのパスワードを変更しようとする頻度を決定します |
| ドメインメンバー：強力な（Windows 2000かそれ以降のバージョン）セッションキーを必要とする | 有効 | 暗号化されたセキュアチャネルデータに128ビットキー強度が必要かどうかを決定します |
| 常にセキュリティで保護されたチャネルのデータをデジタル的に暗号化または署名する | 有効 | このセキュリティ設定は、ドメインメンバーによって開始されたすべてのセキュリティで保護されたチャネルトラフィックを署名または暗号化する必要があるかどうかを決定します。この設定は、ドメインメンバーによって開始されたすべてのセキュアチャネルトラフィックが最小セキュリティ要件を満たしているかどうかを決定します。具体的には、ドメインメンバーによって開始されたすべてのセキュリティで保護されたチャネルトラフィックを署名または暗号化する必要があるかどうかを決定します。このポリシーが有効になっている場合、すべてのセキュアチャネルトラフィックの署名または暗号化がネゴシエートされない限り、セキュアチャネルは確立されません。このポリシーを無効にすると、すべてのセキュリティで保護されたチャネルトラフィックの暗号化と署名がドメインコントローラーとネゴシエートされます。この場合、署名と暗号化のレベルはドメインコントローラーのバージョンと次の2つのポリシーの設定によって異なります。-ドメインメンバー：セキュリティで保護されたチャネルデータをデジタルで暗号化する（可能な場合）-ドメインメンバー：セキュリティで保護されたチャネルデータにデジタルで署名する（可能な場合） |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ネットワークアクセス]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| SAM アカウントおよび共有の匿名の列挙を許可しない | 有効 | このセキュリティ設定は、SAMアカウントと共有の匿名列挙が許可されるかどうかを決定します。Windowsでは、匿名ユーザーがドメインアカウントやネットワーク共有の名前を列挙するなど、特定のアクティビティを実行できます。これは、たとえば、管理者が相互信頼を維持していない信頼できるドメインのユーザーにアクセスを許可する場合に便利です。SAMアカウントと共有の匿名列挙を許可しない場合は、このポリシーを有効にします。 |
| SAM アカウントの匿名の列挙を許可しない | 有効 | このセキュリティ設定は、コンピューターへの匿名接続に付与される追加のアクセス許可を決定します。Windowsでは、匿名ユーザーがドメインアカウントやネットワーク共有の名前を列挙するなど、特定のアクティビティを実行できます。これは、たとえば、管理者が相互信頼を維持していない信頼できるドメインのユーザーにアクセスを許可する場合に便利です。このセキュリティオプションを使用すると、次のように匿名接続に追加の制限を設定できます。有効：SAMアカウントの列挙を許可しません。このオプションは、リソースのセキュリティ権限でEveryoneをAuthenticated Usersに置き換えます。 |
| SAMへのリモート呼び出しを許可されたクライアントを制限する | Domain\Administrators にリモートアクセスを許可O:BAG:BAD:(A;;RC;;;BA) | このポリシー設定を使用すると、SAMへのリモートRPC接続を制限できます。選択しない場合、デフォルトのセキュリティ記述子が使用されます。 |
| 匿名の SID と名前の変換を許可する | 無効 | このセキュリティ設定は、匿名ユーザーが別のユーザーのセキュリティ識別子（SID）属性を要求できるかどうかを決定します。このポリシーが有効になっている場合、管理者のSIDを知っているユーザーは、このポリシーが有効になっているコンピューターにアクセスし、SIDを使用して管理者の名前を取得できます。 |
| 名前付きパイプと共有への匿名のアクセスを制限する | 有効 | 有効にすると、このセキュリティ設定により、共有およびパイプへの匿名アクセスが次の設定に制限されます。 -ネットワークアクセス：匿名でアクセスできる名前付きパイプ -ネットワークアクセス：匿名でアクセスできる共有 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ネットワークセキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| LAN Manager 認証レベル | NTLMv2 応答のみを送信 (LMとNTLMを拒否する) | このセキュリティ設定は、ネットワークログオンに使用されるチャレンジ/レスポンス認証プロトコルを決定します。この選択は、クライアントが使用する認証プロトコルのレベル、ネゴシエートされるセッションセキュリティのレベル、およびサーバーが受け入れる認証のレベルに次のように影響します。NTLMv2応答のみを送信\ LMとNTLMを拒否：クライアントはNTLMv2認証のみを使用し、NTLMv2セッションセキュリティを使用サーバーがサポートしている場合;?ドメインコントローラーはLMおよびNTLMを拒否します（NTLMv2認証のみを受け入れます）。 |
| LocalSystem による NULL セッション フォールバックを許可する | 無効 | LocalSystemで使用する場合、NTLMがNULLセッションにフォールバックできるようにします。 |
| 次回のパスワード変更時に LAN Manager のハッシュ値を保存しない | 有効 | このセキュリティ設定は、次回のパスワード変更時に、新しいパスワードのLAN Manager（LM）ハッシュ値が保存されるかどうかを決定します。LMハッシュは、暗号的に強力なWindows NTハッシュと比較して、比較的弱く、攻撃を受けやすいです。LMハッシュはセキュリティデータベースのローカルコンピューターに保存されるため、セキュリティデータベースが攻撃されるとパスワードが危険にさらされる可能性があります。 |
| NTLM SSP ベース (セキュア RPC を含む) のクライアント向け最小セッション セキュリティ | NTLMv2セッションセキュリティが必要  128ビット暗号化が必要 | このセキュリティ設定により、クライアントは128ビット暗号化やNTLMv2セッションセキュリティのネゴシエーションを要求できます。これらの値は、LAN Manager認証レベルのセキュリティ設定値に依存しています。 |
| NTLM SSP ベース (セキュア RPC を含む) のサーバー向け最小セッション セキュリティ | NTLMv2セッションセキュリティが必要  128ビット暗号化が必要 | このセキュリティ設定により、サーバーは128ビット暗号化やNTLMv2セッションセキュリティのネゴシエーションを要求できます。これらの値は、LAN Manager認証レベルのセキュリティ設定値に依存しています。 |
| 必須の署名をしている LDAP クライアント | ネゴシエーション署名 | このセキュリティ設定は、LDAP BIND要求を発行するクライアントに代わって要求されるデータ署名のレベルを次のように決定します。署名のネゴシエート：トランスポート層セキュリティ/ Secure Sockets Layer（TLS \ SSL）が開始されていない場合、LDAP BIND要求は呼び出し元が指定したオプションに加えて、LDAPデータ署名オプションを設定して開始されます。TLS \ SSLが開始されている場合、LDAP BIND要求は呼び出し元によって指定されたオプションで開始されます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ユーザーアカウント制御]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| アプリケーションのインストールを検出し、昇格をプロンプトする | 有効 | 特権の昇格を必要とするアプリケーションインストールパッケージが検出されると、ユーザーは管理ユーザー名とパスワードの入力を求められます。ユーザーが有効な資格情報を入力すると、該当する特権で操作が続行されます。 |
| ビルトイン Administrator アカウントのための管理者承認モード | 有効 | ビルトインAdministratorアカウントは管理者承認モードを使用します-特権の昇格を必要とする操作はすべて、ユーザーにその操作を承認するように促します。 |
| 安全な場所にインストールされている UIAccess アプリケーションの昇格のみ | 有効 | このポリシー設定は、ユーザーインターフェイスアクセシビリティ（UIAccess）整合性レベルでの実行を要求するアプリケーションがファイルシステムの安全な場所に存在する必要があるかどうかを制御します。安全な場所は次のものに制限されます。 -…\Program Files\、サブフォルダーを含む -…\Windows\system32\ -…\ Program Files(x86)\、64ビットバージョンのWindowsのサブフォルダーを含む |
| 各ユーザーの場所へのファイルまたはレジストリの書き込みエラーを仮想化する | 有効 | このポリシー設定は、アプリケーションの書き込みエラーを定義済みのレジストリおよびファイルシステムの場所にリダイレクトするかどうかを制御します。このポリシー設定は、管理者として実行され、ランタイムアプリケーションデータを％ProgramFiles％、％Windir％、％Windir％\ system32、またはHKLM\Softwareに書き込むアプリケーションの問題を緩和します。 |
| 管理者承認モードですべての管理者を実行する | 有効 | このポリシーを有効にし、関連するUACポリシー設定も適切に設定して、ビルトインAdministratorアカウントおよびAdministratorsグループのメンバーである他のすべてのユーザーが管理者承認モードで実行できるようにする必要があります。 |
| 管理者承認モードでの管理者に対する昇格時のプロンプトの動作 | セキュリティで保護されたデスクトップで同意を要求する | 操作に特権の昇格が必要な場合、ユーザーはセキュリティで保護されたデスクトップで特権ユーザー名とパスワードを入力するよう求められます。ユーザーが有効な資格情報を入力すると、ユーザーの利用可能な最高の特権で操作が続行されます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[監査]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 監査ポリシーサブカテゴリ設定（Windows Vista以降）を強制して、監査ポリシー カテゴリ設定を上書する | 有効 | Windows Vista以降のバージョンのWindowsでは、監査ポリシーのサブカテゴリを使用して、より正確な方法で監査ポリシーを管理できます。カテゴリレベルで監査ポリシーを設定すると、新しいサブカテゴリ監査ポリシー機能が上書きされます。グループポリシーでは、監査ポリシーをカテゴリレベルでのみ設定できます。また、既存のグループポリシーは、ドメインへの参加またはアップグレード時に新しいマシンのサブカテゴリ設定をオーバーライドできます。グループポリシーを変更せずにサブカテゴリを使用して監査ポリシーを管理できるようにするため、Windows Vista以降のバージョンには新しいレジストリ値SCENo&3x41;pplyLegacyAuditPolicyがあり、グループポリシーおよびローカルセキュリティからのカテゴリレベルの監査ポリシーの適用を防止します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[対話型ログオン]

| ポリシー設定 | 値 | 説明 |
| --- | --- | --- |
| コンピューターの非アクティブ状態の上限 | 900 | セッションがロックされるまでの非アクティブの秒数 |
| スマート カード取り出し時の動作 | ワークステーションをロックする | このセキュリティ設定は、ログオンしているユーザーのスマートカードがスマートカードリーダーから削除されたときに何が起こるかを決定します。クリックするとワークステーションのロックでプロパティをこのポリシーのスマートカードが取り外されたときに、ワークステーションは、ユーザーが、地域を離れ、彼らと彼らのスマートカードを取り、まだ保護されたセッションを維持することができ、ロックされています。この設定をWindows Vista以降で機能させるには、スマートカード削除ポリシーサービスを開始する必要があります。 |

### ・L1 監査ポリシーの詳細な構成

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[アカウントログオン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 資格情報の確認の監査 | 成功と失敗 | ユーザーアカウントのログオン資格情報の検証テストによって生成された監査イベント。これらの資格情報に対して権限のあるコンピューターでのみ発生します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[アカウント管理]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| セキュリティ グループの管理の監査 | 成功 | セキュリティグループの作成、変更、削除、メンバーの追加または削除、グループタイプの変更など、セキュリティグループの変更によって生成されるイベントを監査します。 |
| ユーザー アカウントの管理の監査 | 成功と失敗 | ユーザーアカウントへの変更を監査します。イベントには、ユーザーアカウントの作成、変更、削除が含まれます。アカウントの名前変更、無効化、有効、ロックアウト、またはロック解除。ユーザーアカウントのパスワードの設定または変更。ユーザーアカウントのSID履歴にセキュリティ識別子（SID）を追加します。ディレクトリサービス復元モードのパスワードの構成。管理ユーザーアカウントのアクセス許可の変更。Credential Manager資格情報のバックアップまたは復元。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[詳細追跡]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| PNP アクティビティの監査 | 成功 | プラグアンドプレイが外部デバイスを検出したときに監査する。 |
| プロセス作成の監査 | 成功 | プロセスの作成時または開始時に生成される監査イベント。プロセスを作成したアプリケーションまたはユーザーの名前も監査されます |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[ログオン/ログオフ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| アカウントロックアウトの監査 | 失敗 | ロックアウトされたアカウントへのログオン試行の失敗により生成された監査イベント。 |
| グループメンバーシップの監査 | 成功 | ユーザーのログオントークンのグループメンバーシップ情報を監査します。このサブカテゴリのイベントは、ログオンセッションが作成されたコンピューターで生成されます。対話型ログオンの場合、ユーザーがログオンしたコンピューターでセキュリティ監査イベントが生成されます。ネットワーク上の共有フォルダーへのアクセスなどのネットワークログオンの場合、リソースをホストしているコンピューターでセキュリティ監査イベントが生成されます。 |
| ログオンの監査 | 成功と失敗 | コンピューターでのユーザーアカウントのログオン試行によって生成された監査イベント。 |
| その他のログオン/ログオフ イベントの監査 | 成功と失敗 | ターミナルサービスセッションの切断、ワークステーションのロックとロック解除、スクリーンセーバーの呼び出しまたは終了、Kerberosの検出など、「ログオン/ログオフ」ポリシー設定に含まれない他のログオン/ログオフ関連イベントを監査するリプレイ攻撃、またはユーザーまたはコンピューターアカウントに付与されたワイヤレスネットワークへのアクセス。 |
| 特殊なログオンの監査 | 成功 | 管理者と同等の特権を持ち、プロセスをより高いレベルに昇格するために使用できるログオンである特別なログオンの使用や、特別なグループのメンバーによるログオンなど、特別なログオンによって生成されたイベントを監査するグループを使用すると、特定のグループのメンバーがネットワークにログオンしたときに生成されたイベントを監査できます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[オブジェクトアクセス]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 詳細なファイル共有の監査 | 失敗 | 共有フォルダー上のファイルおよびフォルダーへのアクセス試行を監査します。詳細なファイル共有設定は、ファイルまたはフォルダーにアクセスするたびにイベントを記録します。 |
| ファイル共有の監査 | 成功と失敗 | 共有フォルダーへのアクセス試行を監査します。共有フォルダーにアクセスしようとすると、監査イベントが生成されます。 |
| その他のオブジェクト アクセス イベントの監査 | 成功と失敗 | タスクスケジューラジョブまたはCOM +オブジェクトの管理によって生成された監査イベント。 |
| リムーバブル記憶域の監査 | 成功と失敗 | 監査ユーザーは、リムーバブルストレージデバイス上のファイルシステムオブジェクトにアクセスしようとします。セキュリティ監査イベントは、要求されたすべてのタイプのアクセスのすべてのオブジェクトに対してのみ生成されます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[ポリシーの変更]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 監査ポリシーの変更の監査 | 成功 | セキュリティ監査ポリシー設定の変更を監査する。 |
| 認証ポリシーの変更の監査 | 成功 | 認証ポリシーの変更によって生成された監査イベント。 |
| MPSSVCルールレベル ポリシー変更の監査 | 成功と失敗 | Microsoft Protection Service（MPSSVC）によって使用されるポリシールールの変更によって生成されたイベントを監査します。このサービスは、Windowsファイアウォールによって使用されます。 |
| その他のポリシー変更イベントの監査 | 失敗 | トラステッドプラットフォームモジュール（TPM）構成の変更、カーネルモード暗号化自己テスト、暗号化プロバイダー操作、暗号化コンテキスト操作または変更、適用された中央アクセスポリシーなど、ポリシー変更カテゴリで監査されないその他のセキュリティポリシー変更によって生成された監査イベント（CAP）の変更、またはブート構成データ（BCD）の変更。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[特権の使用]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 重要な特権の使用の監査 | 成功と失敗 | 機密特権（ユーザー権利）が使用されたときに生成される監査イベント。オペレーティング システムの一部として機能。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[システム]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| その他のシステムイベントの監査 | 成功と失敗 | 次のイベントのいずれかを監査します。Windowsファイアウォールサービスとドライバーの起動とシャットダウン、Windowsファイアウォールサービスによるセキュリティポリシーの処理、暗号化キーファイル、および移行操作。 |
| セキュリティ状態の変更の監査 | 成功 | コンピューターの起動およびシャットダウン、システム時間の変更、CrashOnAuditFailからのシステムの回復など、コンピューターのセキュリティ状態の変化によって生成された監査イベント。エントリが構成されます。 |
| セキュリティシステムの拡張の監査 | 成功 | セキュリティシステムの拡張機能またはサービスに関連する監査イベント。 |
| システムの整合性の監査 | 成功と失敗 | セキュリティサブシステムの整合性に違反する監査イベント。 |

### ・L1 セキュリティが強化されたWindowsファイアウォール

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[セキュリティが強化された Windows ファイアーウォール]>[Windows ファイアウォールのプロパティ]>[ドメイン プロファイル]>[状態]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ファイアウォールの状態 | 有効 | ドメインプロファイルに接続したときにファイアウォールを有効にします。 |
| 受信接続 | ブロック | ドメインプロファイルで接続をブロックすることを許可するルールが存在しない非請求の受信接続。 |
| 送信接続 | 許可する | 接続をブロックするルールがない送信接続は、ドメインプロファイルで許可されます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[セキュリティが強化された Windows ファイアーウォール]>[Windows ファイアウォールのプロパティ]>[ドメイン プロファイル]>[設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 通知を表示する | いいえ | ドメインプロファイルでプログラムが受信接続の受信をブロックされている場合、ユーザーへの通知の表示が有効になります。本設定では表示をしません。 **※注意** 本設定は、ポリシーでプログラムがブロックされた際に、ユーザーに通知を行うことを禁止し、ユーザーがポリシーに反して許可を与えないようにするための措置です。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[セキュリティが強化された Windows ファイアーウォール]>[Windows ファイアウォールのプロパティ]>[ドメイン プロファイル]>[ログ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| サイズ制限 | 16384 | ドメイン接続のファイアウォールログファイルサイズを設定します。 |
| 破棄されたパケットをログに記録する | はい | ドメイン接続の破棄されたパケットのロギングを有効にします。 |
| 正常な接続をログに記録する | はい | ドメイン接続の成功した接続のログを有効にします。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[セキュリティが強化された Windows ファイアーウォール]>[Windows ファイアウォールのプロパティ]>[プライベートプロファイル]>[状態]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ファイアウォールの状態 | 有効 | プライベートプロファイルに接続したときにファイアウォールを有効にします。 |
| 受信接続 | ブロック | プライベートプロファイルで接続をブロックすることを許可するルールが存在しない非請求の受信接続。 |
| 送信接続 | 許可する | 接続をブロックするルールがない送信接続は、プライベートプロファイルで許可されます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[セキュリティが強化された Windows ファイアーウォール]>[Windows ファイアウォールのプロパティ]>[プライベートプロファイル]>[設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 通知を表示する | いいえ | プライベートプロファイルでプログラムが受信接続の受信をブロックされている場合、ユーザーへの通知の表示が有効になります。本設定では表示をしません。 **※注意** 本設定は、ポリシーでプログラムがブロックされた際に、ユーザーに通知を行うことを禁止し、ユーザーがポリシーに反して許可を与えないようにするための措置です。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[セキュリティが強化された Windows ファイアーウォール]>[Windows ファイアウォールのプロパティ]>[プライベートプロファイル]>[ログ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| サイズ制限 | 16384 | プライベート接続のファイアウォールログファイルサイズを設定します。 |
| 破棄されたパケットをログに記録する | はい | プライベート接続の破棄されたパケットのロギングを有効にします。 |
| 正常な接続をログに記録する | はい | プライベート接続の成功した接続のログを有効にします。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[セキュリティが強化された Windows ファイアーウォール]>[Windows ファイアウォールのプロパティ]>[パブリックプロファイル]>[状態]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ファイアウォールの状態 | 有効 | パブリックプロファイルに接続したときにファイアウォールを有効にします。 |
| 受信接続 | ブロック | パブリックプロファイルで接続をブロックすることを許可するルールが存在しない非請求の受信接続。 |
| 送信接続 | 許可する | 接続をブロックするルールがない送信接続は、パブリックプロファイルで許可されます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[セキュリティが強化された Windows ファイアーウォール]>[Windows ファイアウォールのプロパティ]>[パブリックプロファイル]>[設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 通知を表示する | いいえ | パブリックプロファイルでプログラムが受信接続の受信をブロックされている場合、ユーザーへの通知の表示が有効になります。本設定では表示をしません。 **※注意** 本設定は、ポリシーでプログラムがブロックされた際に、ユーザーに通知を行うことを禁止し、ユーザーがポリシーに反して許可を与えないようにするための措置です。 |
| ローカルファイアウォールの規則を適用する | いいえ | ユーザーは新しいファイアウォールルールを作成できません。 |
| ローカル接続のセキュリティ規則を適用する | いいえ | ローカル接続ルールがドメインのグループポリシー設定とマージされないようにします。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[セキュリティが強化された Windows ファイアーウォール]>[Windows ファイアウォールのプロパティ]>[パブリックプロファイル]>[ログ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| サイズ制限 | 16384 | パブリック接続のファイアウォールログファイルサイズを設定します。 |
| 破棄されたパケットをログに記録する | はい | パブリック接続の破棄されたパケットのロギングを有効にします。 |
| 正常な接続をログに記録する | はい | パブリック接続の成功した接続のログを有効にします。 |

### ・L1 MS Security Guide

[コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[MS Security Guide]

MS Security Guide は Microsoft Security Compliance Toolkit 1 に含まれる Windows 10 Version 1909 and Windows Server Version 1909 Security Baseline\Templates に含まれています。日本語化はされていません。

Microsoft Security Compliance Toolkit 1.[[20]](#footnote-20)

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[MS Security Guide]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| [Apply UAC restrictions to local accounts on network logons](https://www.softwareisac.jp/ipa/index.php?Apply+UAC+restrictions+to+local+accounts+on+network+logons) | 有効 | 有効(推奨):UACトークンフィルターをネットワークログオンのローカルアカウントに適用します。Administratorsなどの強力なグループのメンバーシップが無効になり、作成されたアクセストークンから強力な特権が削除されます。これにより、LocalAccountTokenFilterPolicyレジストリ値が0に構成されます。これは、Windowsの既定の動作です。 |
| [Configures SMB v1 client driver](https://www.softwareisac.jp/ipa/index.php?Configures+SMB+v1+client+driver) | 有効 オプション: Configure MrxSmb10 driver&brDisable driver (recommended) | SMBv1プロトコルのクライアント側の処理を無効にするには、[有効]ラジオボタンを選択し、ドロップダウンから[ドライバーを無効にする]を選択します。警告：いかなる状況下でも「無効」なラジオボタンを選択しないでください。 |
| [Configures SMB v1 server](https://www.softwareisac.jp/ipa/index.php?Configures+SMB+v1+server) | 無効 | この設定を無効にすると、SMBv1プロトコルのサーバー側の処理が無効になります。 （推奨）この設定を有効にすると、SMBv1プロトコルのサーバー側の処理が有効になります。 （デフォルト。）この設定の変更を有効にするには、再起動が必要です。 |
| [Enable Structured Exception Handling Overwrite Protection (SEHOP)](https://www.softwareisac.jp/ipa/index.php?Enable+Structured+Exception+Handling+Overwrite+Protection+%28SEHOP%29) | 有効 | この設定を有効にすると、SEHOPが実施されます。 |
| [NetBT NodeType configuration](https://www.softwareisac.jp/ipa/index.php?NetBT+NodeType+configuration) | P-node (recommendes) | NetBT NodeType設定は、NetBTが名前の登録と解決に使用する方法を決定します。 - Bノードコンピューターはブロードキャストを使用します。 - Pノードコンピューターは、ネームサーバー（WINS）へのポイントツーポイントの名前クエリのみを使用します。 - Mノードコンピューターは最初にブロードキャストし、次にネームサーバーに照会します。 - Hノードコンピューターは、最初にネームサーバーに照会し、次にブロードキャストします。LMHOSTSまたはDNSによる解決は、これらの方法に従います。 NodeType値が存在する場合、DhcpNodeType値をオーバーライドします。NodeTypeもDhcpNodeTypeも存在しない場合、コンピューターは、ネットワーク用に構成されたWINSサーバーがない場合はBノードを使用し、少なくとも1つのWINSサーバーが構成されている場合はHノードを使用します。 |
| [WDigest authentication](https://www.softwareisac.jp/ipa/index.php?WDigest+authentication) | 無効 | WDigest認証プロトコルが有効になっている場合、プレーンテキストパスワードはLocal Security Authority Subsystem Service（LSASS）に保存され、盗難にさらされます。Windows 10では、デフォルトでWDigestは無効になっています。この設定により、これが強制されます。 |

※Windows で SMBv1、SMBv2、および SMBv3 を検出、有効化、および無効化する方法[[21]](#footnote-21)

### ・L1 MSS

MSS (Legacy) は Microsoft Security Compliance Toolkit 1 に含まれる Windows 10 Version 1909 and Windows Server Version 1909 Security Baseline\Templates に含まれています[[22]](#footnote-22)。日本語化はされていません。

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[MSS(Legacy)]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| (DisableIPSourceRouting IPv6) | 有効:Hightest protection, source routing is completely disabled | IPソースルーティング保護レベル（パケットスプーフィングに対する保護） |
| (DisableIPSourceRouting) | 有効:Hightest protection, source routing is completely disabled | IPソースルーティング保護レベル（パケットスプーフィングに対する保護） |
| (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | 無効 | ルートのICMPリダイレクトを許可すると、トラフィックが適切にルーティングされない可能性があります。無効にすると、これによりICMPが最初に最短パス経由でルーティングされます。 |
| (NoNameReleaseOnDemand) | 無効 | WINSサーバーに対するサービス拒否（DoS）攻撃を防ぎます。DoSは、サーバーのキャッシュ内のエントリごとにNetBIOS Name Release Requestをサーバーに送信することで構成され、サーバーのWINS解決機能の通常の動作で応答遅延を引き起こします。 |

### ・L1 ネットワーク

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[ネットワーク]>[DNSクライアント]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| マルチキャスト名前解決をオフにする | 有効 | リンク ローカル マルチキャスト名前解決 (LLMNR) がクライアント コンピューターで無効になるように指定します。 LLMNR は補助的な名前解決プロトコルです。LLMNR を使用すると、クエリはクライアント コンピューターから、単一サブネット上のローカル ネットワーク リンクでマルチキャストを使用して、同じサブネット上の LLMNR が有効な別のクライアント コンピューターに送信されます。LLMNR は、DNS サーバーまたは DNS クライアント構成を必要とせず、従来の DNS 名前解決を使用できないときに、名前解決できるようにします。 このポリシー設定を有効にした場合、クライアント コンピューター上の利用可能なすべてのネットワーク アダプターで LLMNR が無効になります。 このポリシー設定を無効にした場合、または構成しなかった場合、利用可能なすべてのネットワーク アダプターで LLMNR が有効になります。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[ネットワーク]>[Lanman ワークステーション]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 安全でないゲスト ログオンを有効にする | 無効 | このポリシー設定では、SMB クライアントが SMB サーバーへの安全でないゲスト ログオンを許可するかどうかを決定します。このポリシー設定を有効にした場合、またはこのポリシー設定を構成しなかった場合、SMB クライアントは安全でないゲスト ログオンを許可します。このポリシー設定を無効にした場合、SMB クライアントは安全でないゲスト ログオンを拒否します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[ネットワーク]>[Windows接続マネージャー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ドメイン認証されたネットワークに接続されているときに、非ドメイン ネットワークへの接続を禁止する | 有効 | このポリシー設定は、コンピューターがドメインベースのネットワークと非ドメインベースのネットワークの両方に同時に接続することを防ぎます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[ネットワーク]>[ネットワークプロバイダー]

| ポリシー設定 | 値 | 説明 |
| --- | --- | --- |
| 強化された UNC パス | 有効 | このポリシー設定は、UNCパスへの安全なアクセスを構成します。このポリシーを有効にすると、Windowsは追加のセキュリティ要件を満たした後、指定されたUNCパスへのアクセスのみを許可します。 |
| 値の名前: \\\*SYSVOL |
| 値: RequireMutualAuthentication = 1, RequireIntegrity = 1 |
| 値の名前: \\\*\NETLOGON |
| 値: RequireMutualAuthentication = 1, RequireIntegrity = 1 |

※値を [有効グラフィカル ユーザー インターフェイス, テーブル

自動的に生成された説明] にすると、以下の画面が表示されます。

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[ネットワーク]>[ネットワーク接続]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| DNS ドメイン ネットワーク上でインターネット接続の共有の使用を禁止する | 有効 | 管理者がインターネット接続のインターネット接続共有（ICS）機能を有効にして構成できるかどうか、およびICSサービスをコンピューターで実行できるかどうかを決定します。 |

### ・L1 システム

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[システム]>[インターネット通信の管理]>[インターネット通信設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Web 発行およびオンライン注文ウィザードのインターネット ダウンロードをオフにする | 有効 | このポリシー設定は、WindowsがWeb公開ウィザードおよびオンライン注文ウィザードのプロバイダーのリストをダウンロードするかどうかを指定します。これらのウィザードを使用すると、ユーザーはオンラインストレージや写真印刷などのサービスを提供する会社のリストから選択できます。デフォルトでは、Windowsは、レジストリで指定されたプロバイダーに加えて、Windows Webサイトからダウンロードされたプロバイダーを表示します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[システム]>[カーネル DMA 保護]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| カーネル DMA 保護と互換性のない外部デバイスの列挙ポリシー | 有効 オプション:列挙ポリシー すべて禁止 | DMA 再マッピングと互換性のない外部 DMA 対応デバイスの列挙ポリシー。このポリシーは、カーネル DMA 保護が有効されていて、かつシステムでサポートされている場合にのみ有効です。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[システム]>[グループポリシー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| レジストリポリシーの処理を構成する | バックグランドで定期的に処理しているときは適用しない＝無効  グループ ポリシー オブジェクトが変更されていなくても処理する＝有効 | このポリシー設定では、レジストリ ポリシーをいつ更新するかを決定します。 このポリシー設定は、[管理用テンプレート] フォルダーにあるすべてのポリシー、およびレジストリに値を格納しているその他のポリシーに影響します。この設定は、インストール時に設定されたレジストリ ポリシーを実装しているプログラムのカスタム設定よりも優先されます。 このポリシー設定を有効にした場合、オプションを変更するためのチェック ボックスが利用できるようになります。このポリシー設定を無効にした場合、または構成しなかった場合は、システムに影響はありません。 [バックグラウンドで定期的に処理しているときは適用しない] オプションを有効にした場合、コンピューターの使用中は関連するポリシーがバックグラウンドで更新されなくなります。バックグラウンドでの更新を無効にすると、再度ユーザーがログオンするか、システムを再起動するまでポリシーへの変更は適用されません。 [グループ ポリシー オブジェクトが変更されていなくても処理する] オプションを使うと、ポリシーが変更されていない場合でも、ポリシーは更新されて再適用されます。変更されたときのみ更新するように指定できるポリシーは複数あります。しかし、ユーザーが変更した場合に備え、変更されていないポリシーであっても、必要なポリシー設定を再適用するなどの方法で更新することをお勧めします。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[システム]>[サービス コントロール マネージャーの設定]>[セキュリティの設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| svchost.exe 軽減オプションを有効にする | 有効 | svchost.exeプロセスのプロセス軽減オプションを有効にします。 このポリシー設定を有効にすると、svchost.exeプロセスでホストされている組み込みシステムサービスで、より厳しいセキュリティポリシーが有効になります。これには、これらのプロセスに読み込まれたすべてのバイナリにマイクロソフトによる署名を要求するポリシーと、動的に生成されたコードを許可しないポリシーが含まれます。 このポリシー設定を無効にした場合、または構成しなかった場合、これらのより厳しいセキュリティ設定は適用されません。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[システム]>[デバイスのインストールの制限]>[デバイスのインストール]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| これらのデバイス ID と一致するデバイスのインストールを禁止します | 有効 [表示ボタン]をクリックし、禁止するハードウェアID、プラグ アンド プレイ互換 IDを入力する すでにインストールされている一致するデバイスにも適用されます= 有効 | このポリシー設定を使用すると、WindowsがインストールできないデバイスのプラグアンドプレイハードウェアIDと互換性IDのリストを指定できます。このポリシー設定は、Windowsによるデバイスのインストールを許可する他のポリシー設定よりも優先されます。 このポリシー設定を有効にすると、作成したリストにハードウェアIDまたは互換性IDが表示されるデバイスをWindowsがインストールできなくなります。 リモートデスクトップサーバーでこのポリシー設定を有効にすると、ポリシー設定は、指定されたデバイスのリモートデスクトップクライアントからリモートデスクトップサーバーへのリダイレクトに影響します。このポリシー設定を無効にするか、未構成にした場合、他のポリシー設定で許可または禁止されているデバイスをインストールおよび更新できます。 |
| これらのデバイス セットアップ クラスのドライバーを使用したデバイスのインストールを禁止する | 有効 [表示]ボタンをクリックし、デバイス セットアップ クラスを表す GUID を入力する 既にインストールされている一致するデバイスにも適用されます=有効 | このポリシー設定を使用すると、Windowsがインストールできないデバイスドライバーのデバイスセットアップクラスのグローバル一意識別子（GUID）の一覧を指定できます。 このポリシー設定は、Windowsによるデバイスのインストールを許可する他のポリシー設定よりも優先されます。このポリシー設定を有効にすると、作成したリストにデバイスセットアップクラスGUIDが表示されるデバイスドライバーのインストールまたは更新がWindowsで禁止されます。リモートデスクトップサーバーでこのポリシー設定を有効にすると、ポリシー設定は、指定されたデバイスのリモートデスクトップクライアントからリモートデスクトップサーバーへのリダイレクトに影響します。 このポリシー設定を無効にした場合、または構成しなかった場合、Windowsは他のポリシー設定で許可または禁止されているデバイスをインストールおよび更新できます。 |

* ※グループポリシーを使用してデバイスのインストールを制御するためのステップバイステップガイド[[23]](#footnote-23)

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[システム]>[リモートプロシージャコール]

| ポリシー設定 | 値 | 説明 |
| --- | --- | --- |
| 認証されていない RPC クライアントを制限する | 有効 [認証済み] | このポリシー設定は、すべての RPC アプリケーションに影響します。 ドメイン環境では、このポリシー設定はグループ ポリシーの処理自体を含む広範な機能に影響する可能性があるため、注意して使用する必要があります。 このポリシー設定の変更を元に戻す場合、影響するコンピューターごとに手動での操作が必要になることがあります。 このポリシー設定は、ドメイン コントローラーには適用しないでください。 このポリシー設定を無効にすると、RPC サーバー ランタイムは Windows クライアントでは [認証済み] の値を使用し、このポリシー設定をサポートする Windows Server バージョンでは [なし] の値を使用します。 このポリシー設定を構成しない場合、設定は無効のままになります。 RPC サーバー ランタイムは、Windows クライアントでは [認証済み] の値の使用が、このポリシー設定をサポートする Server SKU では [なし] の値の使用が有効にされた場合と同じように動作します。 このポリシー設定を有効にすると、コンピューター上の RPC サーバーに接続する、認証されていない RPC クライアントを制限するよう RPC サーバー ランタイムに指示します。サーバーとの通信時に名前付きパイプを使用している場合、または RPC セキュリティを使用している場合に、クライアントは認証済みとして認識されます。このポリシー設定で選択された値によっては、未認証のクライアントがアクセスできるよう明示的に要求した RPC インターフェイスは、この制限から除外される場合もあります。 -- [なし] では、このポリシー設定が適用されるコンピューター上で実行されている RPC サーバーへの、すべての RPC クライアントの接続を許可します。 -- [認証済み] では、このポリシー設定が適用されるコンピューター上で実行されている RPC サーバーへの、認証済み (前の定義による) の RPC クライアントのみの接続を許可します。除外を要求したインターフェイスは除外されます。 -- [認証済み (例外なし)] では、このポリシー設定が適用されるコンピューター上で実行されている RPC サーバーへの、認証済み (前の定義による) の RPC クライアントのみの接続を許可します。 例外は許可されません。 注: このポリシー設定は、システムが再起動されるまで適用されません。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[システム]>[起動時マルウェア対策]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ブート開始ドライバーの初期化ポリシー | 有効 良好、不明、および不良（ブートに不可欠） | 起動時マルウェア対策のブート開始ドライバーによって決定された分類に基づいて、どのブートスタートドライバーを初期化するかを指定できます。起動時マルウェア対策のブート開始ドライバーは、各ブート開始ドライバーについて次の分類を返すことができます。 -良好：ドライバーは署名されており、改ざんされていません。 -不良：ドライバーがマルウェアとして識別されました。既知の不良ドライバーの初期化を許可しないことをお勧めします。 -不良（起動に不可欠）：ドライバーはマルウェアとして識別されましたが、コンピューターはこのドライバーをロードしないと正常に起動できません。 -不明：このドライバーは、マルウェア検出アプリケーションによって証明されておらず、起動時マルウェア対策ブート開始ドライバーによって分類されていません。 このポリシー設定を有効にすると、次回コンピューターを起動するときに初期化するブート開始ドライバーを選択できます。このポリシー設定を無効にした場合、または構成しなかった場合、正常、不明、または不良と判断されたブート開始ドライバーは初期化され、不良と判断されたドライバーの初期化はスキップされます。マルウェア検出アプリケーションに起動時マルウェア対策ブート開始ドライバーが含まれていない場合、または起動時マルウェア対策ブート開始ドライバーが無効になっている場合、この設定は効果がなく、すべてのブートスタートドライバーが初期化されます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[システム]>[資格情報の委任]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| リモートホストでエクスポート不可の資格情報の委任を許可する | 有効 | 資格情報の委任を使用する場合、デバイスはリモートホストに資格情報のエクスポート可能なバージョンを提供します。 これにより、ユーザーはリモートホストの攻撃者からの資格情報の盗難のリスクにさらされます。このポリシー設定を有効にすると、ホストは制限付き管理モードまたはリモート資格情報ガードモードをサポートします。 |
| 暗号化オラクルの修復 | 更新済みクライアントの強制 | 一部のバージョンの CredSSP プロトコルには、クライアントに対する暗号化オラクル攻撃を受けやすい脆弱性があります。 このポリシーは、攻撃を受けやすいクライアントおよびサーバーとの互換性を制御します。このポリシーを使用すると、暗号化オラクル攻撃に対する脆弱性について、望ましい保護レベルを設定できます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[システム]>[電源の管理]>[スリープの設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| コンピューターのスリープ状態の解除時にパスワードを要求する（バッテリー使用時） | 有効 | システムがスリープから再開するときに、ユーザーにパスワードの入力を求めるかどうかを指定します。 |
| コンピューターのスリープ状態の解除時にパスワードを要求する(電源接続時） | 有効 | システムがスリープから再開するときに、ユーザーにパスワードの入力を求めるかどうかを指定します。 |

### ・L1 Windows コンポーネント

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[BitLocker ドライブ暗号化]

|  |  |  |
| --- | --- | --- |
| **[ポリシー設定]** | **[ポリシー値]** | **[説明]** |
| このコンピューターがロックされているときに新しいDMA デバイスを無効にする | [有効] | ユーザーがWindowsにログインするまで、すべてのThunderboltホットプラグ可能なPCIダウンストリームポートのダイレクトメモリアクセス（DMA）をブロックできます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[BitLocker ドライブ暗号化]>[オペレーティングシステムのドライブ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| スタートアップの拡張 PIN を許可する | [有効] | BitLocker で拡張スタートアップ PIN を使用するかどうかを構成できます。 拡張スタートアップ PIN では、大文字と小文字、記号、数字、空白などの文字を使用できます。このポリシー設定は、BitLocker を有効にすると適用されます。 このポリシー設定を有効にした場合、すべての新しい BitLocker スタートアップ PIN のセットが拡張 PIN になります。 注意: コンピューターによっては、プリブート環境で拡張 PIN がサポートされていない場合もあります。BitLocker セットアップでシステム チェックを実行することを強くお勧めします。 |

[Windows コンポーネント]>[Internet Explorer] は、13.13 ・L1 Windows コンポーネントｰInternet Explorer を参照して下さい。

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Microsoft Edge]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Cookie の構成 | 有効 オプション=すべての Cookie をブロックする | この設定を有効にした場合は、次のいずれかを選択する必要があります。 -すべての Cookie を許可する (既定値): すべての Web サイトからのすべての Cookie を許可します。 -すべての Cookie をブロックする: すべての Web サイトからのすべての Cookie をブロックします。 -サード パーティの Cookie のみをブロックする: サード パーティの Web サイトからの Cookie のみをブロックします。 この設定を無効にした場合または構成しなかった場合は、すべての Web サイトからのすべての Cookie が許可されます。 注意: 本設定は運用に影響があるため、設定値はリスク受容も含めて検討してください。 |
| WebRTC での Localhost IP アドレス使用の回避 | 有効 | この設定を有効にした場合、WebRTC プロトコルを使用して電話をかける際に LocalHost IP アドレスは表示されません。 この設定を無効にした場合または構成しなかった場合、WebRTC プロトコルを使用して電話をかける際に LocalHost IP アドレスが表示されます。 |
| Windows Defender SmartScreen を構成します | 有効 | この設定を有効にした場合は、Windows Defender SmartScreen が有効になり、従業員が無効にすることはできません。 この設定を無効にした場合は、Windows Defender SmartScreen が無効になり、従業員が有効にすることはできません。 この設定を構成しなかった場合は、Windows Defender SmartScreen フィルターを使用するかどうかを従業員が選択できます。 |
| サイトに関する Windows Defender SmartScreen プロンプトをバイパスしない | 有効 | この設定を有効にした場合、従業員は Windows Defender SmartScreen の警告を無視できず、サイトへの移動がブロックされます。 この設定を無効にした場合または構成しなかった場合、従業員は Windows Defender SmartScreen の警告を無視して、サイトに移動することができます。 |
| サイトをスタートにピン止めする際にライブ タイル情報の収集を Microsoft Edge に許可しない | 有効 | この設定を有効にした場合、Microsoft Edge ではライブ タイルのメタデータが収集されず、ユーザーがライブ タイルをスタート メニューにピン留めする際に提供されるエクスペリエンスは最小限になります。 この設定を無効にした場合、または構成しなかった場合、Microsoft Edge ではライブ タイルのメタデータが収集され、ユーザーがライブ タイルをスタート メニューにピン留めする際に、より完全なエクスペリエンスが提供されます。 |
| トラッキング拒否の構成 | 有効 | この設定を有効にした場合は、トラッキング情報が要求される Web サイトにはトラッキング拒否要求が常に送信されます。 この設定を無効にした場合は、トラッキング情報が要求される Web サイトにトラッキング拒否要求が送信されません。 この設定を構成しなかった場合は、トラッキング情報が要求される Web サイトにトラッキング拒否要求を送信するかどうかを従業員が選択できます。 |
| パスワードマネージャの構成 | 無効 | この設定を有効にした場合は、パスワード マネージャーを使用して従業員が自分のパスワードをローカル コンピューター上に保存できます。 この設定を無効にした場合は、パスワード マネージャーを使用して従業員が自分のパスワードをローカル コンピューター上に保存することはできません。 この設定を構成しなかった場合は、パスワード マネージャーを使用して自分のパスワードをローカル コンピューター上に保存するかどうかを従業員が選択できます。 |
| ファイルに関する Windows Defender SmartScreen プロンプトをバイパスしない | 有効 | この設定を有効にした場合、従業員は Windows Defender SmartScreen の警告を無視できず、確認されていないファイルのダウンロードがブロックされます。 この設定を無効にした場合または構成しなかった場合、従業員は Windows Defender SmartScreen の警告を無視して、ダウンロード プロセスを続行することができます。 |
| 証明書エラーのオーバーライドを禁止する | 有効 | Web セキュリティ証明書は、ユーザーの移動先サイトが正当であることを確認するために使用され、状況によってはデータが暗号化されます。このポリシーを使用すると、SSL エラーがあるサイトに対するセキュリティ警告をユーザーがバイパスすることを禁止するかどうかを指定できます。 有効にすると、証明書エラーのオーバーライドは許可されません。 無効または未構成の場合は、証明書エラーのオーバーライドが許可されます。 |
| 書籍ライブラリの構成の更新を許可する | 無効 | この設定を有効にするか (既定値)、構成しなかった場合は、Microsoft Edge は自動的に書籍ライブラリの構成データを更新します。 この設定を無効にすると、Microsoft Edge は書籍ライブラリの更新された構成データを自動的にダウンロードしません。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[RSSフィード]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 添付ファイルのダウンロードを禁止する | 有効 | このポリシー設定は、ユーザーがフィードからユーザーのコンピューターに添付ファイルをダウンロードできないようにします。このポリシー設定を有効にすると、ユーザーはフィードのプロパティページから添付ファイルをダウンロードするようにフィード同期エンジンを設定できません。開発者は、Feed APIを使用してダウンロード設定を変更することはできません。このポリシー設定を無効にするか、未構成にした場合、ユーザーは、フィードのプロパティページから添付ファイルをダウンロードするようにフィード同期エンジンを設定できます。開発者は、Feed APIを使用してダウンロード設定を変更できます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windows Defender SmartScreen]>[Microsoft Edge]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Windows Defender SmartScreen を構成します | 有効 | Windows Defender SmartScreenをオンまたはオフにします。 SmartScreenは、インターネットからダウンロードされた潜在的に悪意のあるプログラムを実行する前にユーザーに警告することにより、PCを保護します。この警告は、インターネットからダウンロードされたアプリを実行する前に表示されるインタースティシャルダイアログとして表示され、認識されないか、悪意があることがわかっています。疑わしいと思われないアプリのダイアログは表示されません。この機能が有効になっているPCで実行されるファイルおよびプログラムに関する情報がマイクロソフトに送信されます。このポリシーを有効にすると、すべてのユーザーに対してSmartScreenが有効になります。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windows Defender SmartScreen]>[エクスプローラー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Windows Defender SmartScreen を構成する | 有効 オプション：警告してバイパスを回避 | Windows Defender SmartScreen をオンまたはオフにします。SmartScreen は、インターネットからダウンロードされた潜在的に悪意のあるプログラムを実行する前にユーザーに警告することにより、PCを保護します。この警告は、インターネットからダウンロードされたアプリを実行する前に表示されるインタースティシャルダイアログとして表示され、認識されないか、悪意があることがわかっています。疑わしいと思われないアプリのダイアログは表示されません。この機能が有効になっているPCで実行されるファイルおよびプログラムに関する情報がマイクロソフトに送信されます。このポリシーを有効にすると、すべてのユーザーに対してSmartScreen が有効になります。その動作は、次のオプションで制御できます。 -警告してバイパスを防ぐ -警告 「警告とバイパス回避」オプションを使用してこのポリシーを有効にすると、SmartScreen のダイアログでは、警告を無視してアプリを実行するオプションがユーザーに表示されません。SmartScreen は、アプリを次に実行しようとすると警告を表示し続けます。「警告」オプションを使用してこのポリシーを有効にすると、SmartScreen のダイアログは、アプリが疑わしいとユーザーに警告しますが、ユーザーは警告を無視してアプリを実行できます。ユーザーが SmartScreen にアプリを実行するように指示した場合、SmartScreen はそのアプリについてユーザーに再度警告しません。このポリシーを無効にすると、SmartScreen はすべてのユーザーに対して無効になります。インターネットから疑わしいアプリを実行しようとしても、ユーザーに警告は表示されません。このポリシーを構成しない場合、SmartScreen はデフォルトで有効になりますが、ユーザーは設定を変更できます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windows Defender ウイルス対策]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Windows Defender Antivirusをオフにする | 無効 | Windows Defender Antivirusをオフにします。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windows Defender ウイルス対策]>[MAPS]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Microsoft MAPSに参加する | 高度なマップ | Microsoft MAPSに参加できます。Microsoft MAPSは、潜在的な脅威への対応方法の選択を支援するオンラインコミュニティです。コミュニティは、新しい悪意のあるソフトウェアの感染拡大を阻止するのにも役立ちます。 注意: 本設定は組織、個人の情報が意図せず送信される可能性があるとされています。組織によっては、本設定の便益と情報保護の観点から有効・無効を検討してください。 |
| 詳細な分析が必要な場合はファイルのサンプルを送信する | 有効：安全なサンプルを送信 | MAPSテレメトリのオプトインが設定されている場合のサンプル送信の動作を構成します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windows Defender ウイルス対策]>[Windows Defender Expoit Guard]>[ネットワーク保護]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ユーザーとアプリが危険な Web サイトにアクセスするのを防ぎます | 有効 オプション＝ブロック | Windows Defender Exploit Guard ネットワーク保護を有効または無効にすることで、従業員がアプリケーションを使用して、フィッシング詐欺、不正利用ホスト サイト、およびインターネット上の他の悪意のあるコンテンツをホストする可能性のある危険なドメインにアクセスしないようにします。 有効: [オプション] セクションでモードを指定します。 -ブロック: ユーザーとアプリケーションは危険なドメインにアクセスできません -監査モード: ユーザーとアプリケーションは危険なドメインに接続できますが、ブロック設定ならアクセスをブロックされるようなドメインに接続した場合には、イベント ログにそのイベントの記録が書き込まれます。 無効:ユーザーとアプリケーションは危険なドメインへの接続をブロックされません。 未構成:無効と同じです。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windows Defender ウイルス対策]>[スキャン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 1日にクイックスキャンを実行する間隔を指定する | 24 | クイックスキャンを実行する間隔を指定できます。時間値は、クイックスキャン間の時間数として表されます。有効な値の範囲は、1（1時間ごと）から24（1日1回）です。 |
| リムーバブル ドライブをスキャンする | 有効 | フルスキャンの実行時に、USBフラッシュドライブなどのリムーバブルドライブのコンテンツで悪意のあるソフトウェアや不要なソフトウェアをスキャンするかどうかを管理できます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windows Defender ウイルス対策]>[リアルタイム保護]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| リアルタイム保護を無効にする | 無効 | 既知のマルウェア検出のリアルタイム保護プロンプトをオフにします |
| 動作の監視を有効にする | 有効 | 動作監視を設定できます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windows Inkワークスペース]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Windows Inkワークスペースを許可します | 有効 オプション：オン（ただしロックより上のアクセスは許可しない） | Windows Inkワークスペースを許可する |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windows PowerShell]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| PowerShell スクリプトブロックのログを有効にする | 有効 | このポリシー設定により、Microsoft-Windows-PowerShell / Operationalイベントログへのすべての PowerShell スクリプト入力のログが有効になります。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windowsインストーラー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ユーザーによるインストール制御を有効にする | 無効 | 通常はシステム管理者のみが利用できるインストールオプションをユーザーが変更できるようにします。 |
| 常にシステム特権でインストールする | 無効 | システムにプログラムをインストールするときに、昇格されたアクセス許可を使用するようにWindowsインストーラーに指示します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windowsリモート管理（WinRM）]>[WinRMクライアント]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ダイジェスト認証を許可しない | 有効 | このポリシー設定を使用すると、Windowsリモート管理（WinRM）クライアントがダイジェスト認証を使用するかどうかを管理できます。 |
| 暗号化されていないトラフィックを許可する | 無効 | Windowsリモート管理（WinRM）クライアントがネットワーク上で暗号化されていないメッセージを送受信するかどうかを管理します |
| 基本認証を許可する | 無効 | このポリシー設定を使用すると、Windowsリモート管理（WinRM）クライアントが基本認証を使用するかどうかを管理できます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windowsリモート管理（WinRM）]>[WinRMサービス]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| WinRMがRunAs資格情報を保存することを許可しない | 有効 | このポリシー設定を使用すると、Windowsリモート管理（WinRM）サービスでプラグインのRunAs資格情報を保存できないようにするかどうかを管理できます。 |
| 暗号化されていないトラフィックを許可する | 無効 | Windowsリモート管理（WinRM）サービスが暗号化されていないメッセージをネットワーク経由で送受信するかどうかを管理します。 |
| 基本認証を許可する | 無効 | このポリシー設定を使用すると、Windowsリモート管理（WinRM）サービスがリモートクライアントからの基本認証を受け入れるかどうかを管理できます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[Windowsログオンオプション]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 再起動後に自動的に前回の対話ユーザーでサインインしてロックする | 無効 | Windows Updateがシステムを再起動した後、デバイスが最後の対話ユーザーに自動的にサインインするかどうかを制御します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[アプリ実行時]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Microsoftアカウントをオプションにする | [有効] | サインインにアカウントを必要とするWindowsストアアプリでMicrosoftアカウントがオプションかどうかを制御できます。このポリシーは、それをサポートするWindowsストアアプリにのみ影響します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[イベント ログ サービス]>[アプリケーション]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ログファイルの最大サイズ（KB）を指定する | [有効]：32768 | ログファイルの最大サイズをキロバイト単位で指定します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[イベント ログ サービス]>[システム]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ログファイルの最大サイズ（KB）を指定する | [有効]：32768 | ログファイルの最大サイズをキロバイト単位で指定します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[イベント ログ サービス]>[セキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ログファイルの最大サイズ（KB）を指定する | [有効]：196608 | ログファイルの最大サイズをキロバイト単位で指定します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[エクスプローラー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Windows Defender SmartScreenを構成します | 有効 オプション: 警告してバイパスを防止 | Windows Defender SmartScreenを有効にして警告メッセージを提供するかどうかを構成し、潜在的なフィッシング詐欺や悪意のあるソフトウェアからユーザーを保護します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[リモートデスクトップサービス]>[リモートデスクトップ接続のクライアント]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| パスワードの保存を許可しない | 有効 | リモートデスクトップ接続からこのコンピューターにパスワードを保存できるかどうかを制御します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[検索]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 暗号化されたファイルのインデックス作成を許可する | 無効 | このポリシー設定では、暗号化されたアイテムのインデックスを作成できます。このポリシー設定を有効にすると、インデックス作成はコンテンツの復号化とインデックス作成を試みます（アクセス制限は引き続き適用されます）。このポリシー設定を無効にすると、Search Serviceコンポーネント（Microsoft以外のコンポーネントを含む）は、暗号化されたアイテムまたは暗号化されたストアのインデックスを作成しないことが期待されます。このポリシー設定は、デフォルトでは構成されていません。このポリシー設定を構成しない場合、コントロールパネルで構成されたローカル設定が使用されます。デフォルトでは、コントロールパネルの設定は、暗号化されたコンテンツのインデックスを作成しないように設定されています。この設定を有効または無効にすると、インデックスは完全に再構築されます。暗号化されたファイルのセキュリティを維持するには、インデックスの場所にフルボリューム暗号化（BitLockerドライブ暗号化やマイクロソフト以外のソリューションなど）を使用する必要があります。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[リモートデスクトップサービス]>[リモートデスクトップセッションホスト]>[セキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| クライアント接続の暗号化レベルを設定する | 有効 オプション：高レベル | リモートデスクトッププロトコル（RDP）接続中にクライアントコンピューターとRDセッションホストサーバー間の通信をセキュリティで保護するために、特定の暗号化レベルの使用を要求するかどうかを指定します。このポリシーは、ネイティブ RDP 暗号化を使用している場合にのみ適用されます。ただし、ネイティブの RDP 暗号化（ SSL 暗号化とは対照的に）は推奨されません。このポリシーは SSL 暗号化には適用されません。 |
| セキュリティで保護された RPC 通信を要求する | 有効 | リモートデスクトップセッションホストサーバーがすべてのクライアントとの安全なRPC通信を必要とするか、安全でない通信を許可するかを指定します。 |
| 接続するたびにパスワードを要求する | 有効 | このポリシー設定は、リモートデスクトップサービスが接続時にクライアントにパスワードの入力を常に要求するかどうかを指定します。この設定を使用して、リモートデスクトップ接続クライアントで既にパスワードを提供している場合でも、リモートデスクトップサービスにログオンしているユーザーにパスワードプロンプトを強制できます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[自動再生のポリシー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ボリューム以外のデバイスの自動再生を許可しない | [有効] | カメラや電話などのMTPデバイスの自動再生を禁止します。 |
| 自動再生機能をオフにする | [有効] オプション:すべてのドライブ | 自動再生機能をオフにできます。 |
| 自動実行の規程の動作を設定する | [有効] オプション:自動実行のコマンドを実行しない | 自動実行コマンドのデフォルトの動作を設定します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[生体認証]>[顔特徴]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 拡張スプーフィング対策を構成する | [有効] | この設定を有効にした場合、またはこの設定を構成しない場合は、管理対象デバイスのすべてのユーザーに、Windows Hello 顔認証に対する拡張スプーフィング対策の使用が要求されます。これにより、拡張スプーフィング対策をサポートしていないデバイスでは Windows Hello 顔認証が無効になります。 |

### ・L1 Windows コンポーネントｰInternet Explorer

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ActiveX コントロールのインストールには ActiveX インストーラーサービスの使用を指定する | 有効 | このポリシー設定では、ActiveXコントロールのインストール方法を指定できます。このポリシー設定を有効にすると、ActiveXインストーラーサービスが存在し、ActiveXコントロールのインストールを許可するように構成されている場合にのみ、ActiveXコントロールがインストールされます。このポリシー設定を無効にするか、未構成にした場合、ユーザーごとのコントロールを含むActiveXコントロールは、標準のインストールプロセスでインストールされます。 |
| SmartScreen フィルターの管理を禁止する | 有効 オプション: SmartScreen フィルター モードの選択: オン | ユーザーがSmartScreenフィルターを管理できないようにします。SmartScreenフィルターは、訪問されているWebサイトが「フィッシング」を通じて個人情報を収集しようとする不正な行為であるか、マルウェアをホストしていることがわかっている場合に警告します。 |
| セキュリティ設定チェック機能を無効にする | 無効 | このポリシー設定は、セキュリティ設定チェック機能を無効にします。この機能は、Internet Explorerのセキュリティ設定をチェックして、設定がInternet Explorerを危険にさらすタイミングを判断します。このポリシー設定を有効にすると、機能は無効になります。このポリシー設定を無効にした場合、または構成しなかった場合、機能はオンになります。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 証明書エラーを無視できないようにする | 有効 | このポリシー設定は、Internet Explorerでの参照を中断するSecure Sockets Layer / Transport Layer Security（SSL / TLS）証明書エラー（「期限切れ」、「失効」、「名前の不一致」エラーなど）をユーザーが無視できないようにします。このポリシー設定を有効にすると、ユーザーは閲覧を継続できません。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[詳細設定 ページ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| サーバーの証明書失効を確認する | 有効 | Internet Explorerがサーバーの証明書の失効ステータスをチェックするかどうかを管理できます |
| ダウンロードされたプログラムの署名を確認する | 有効 | このポリシー設定では、実行可能プログラムをダウンロードする前に、Internet Explorerがユーザーコンピューターでデジタル署名（署名されたソフトウェアの発行者を識別し、変更または改ざんされていないことを確認する）をチェックするかどうかを管理できます。 |
| 暗号化サポートを無効にする | 有効 オプション: 安全なプロトコルの組み合わせ: TLS 1.2 のみを使用する | このポリシー設定を使用すると、ブラウザーでトランスポート層セキュリティ（TLS）1.0、TLS 1.1、TLS 1.2、Secure Sockets Layer（SSL）2.0、またはSSL 3.0のサポートをオフにできます。TLSとSSLは、ブラウザとターゲットサーバー間の通信を保護するのに役立つプロトコルです。ブラウザーがターゲットサーバーとの保護された通信を設定しようとすると、ブラウザーとサーバーは使用するプロトコルとバージョンをネゴシエートします。ブラウザとサーバーは、サポートされているプロトコルとバージョンの互いのリストを一致させようとし、最も優先される一致を選択します。 注：TLS1.1は2020年前半にChrome, Edge, FireFox、Safariなどのブラザーがサポートを中止します。使用するブラウザの対応状況を鑑み、早期にTLS1.2のみを使用の設定を検討してください。 |
| 署名が無効であっても、ソフトウェアの実行またはインストールを許可する | 無効 | このポリシー設定を使用すると、署名が無効であっても、ユーザーがActiveXコントロールやファイルダウンロードなどのソフトウェアをインストールまたは実行できるかどうかを管理できます。無効な署名は、誰かがファイルを改ざんしたことを示す場合があります。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[セキュリティ ページ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 証明書アドレスの不一致についての警告を有効にする | 有効 | このポリシー設定を使用すると、証明書アドレスの不一致のセキュリティ警告を有効にできます。このポリシー設定をオンにすると、別のWebサイトアドレスに対して発行された証明書を提示するSecure HTTP（HTTPS）Webサイトにアクセスすると、ユーザーに警告が表示されます。この警告は、なりすまし攻撃の防止に役立ちます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[セキュリティ ページ]>[インターネットゾーン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ActiveX コントロールに対してマルウェア対策プログラムを実行しない | 無効 | Internet Explorer が ActiveX コントロールに対してマルウェア対策プログラムを実行するかどうかを決定し、ページにロードしても安全かどうかを確認します。 |
| Authenticode 署名済みではない .NET Framework コンポーネントを実行する | 無効 | このポリシー設定を使用すると、Authenticodeで署名されていない.NET FrameworkコンポーネントをInternet Explorerから実行できるかどうかを管理できます。これらのコンポーネントには、オブジェクトタグから参照されるマネージコントロールと、リンクから参照されるマネージ実行可能ファイルが含まれます。 |
| Authenticode 署名済みの .NET Framework コンポーネントを実行する | 有効 オプション: Autheticode 署名済みの .NET Framework コンポーネントを実行する: 無効 | このポリシー設定を使用すると、Authenticodeで署名された.NET FrameworkコンポーネントをInternet Explorerから実行できるかどうかを管理できます。これらのコンポーネントには、オブジェクトタグから参照されるマネージコントロールと、リンクから参照されるマネージ実行可能ファイルが含まれます。 |
| IFRAME のアプリケーションとファイルの起動 | 無効 | このポリシー設定を使用すると、アプリケーションを実行できるかどうか、およびこのゾーンのページの HTML の IFRAME 参照からファイルをダウンロードできるかどうかを管理できます。 |
| Internet Explorer WebBrowser コントロールのスクリプトを許可する | 無効 | このポリシー設定は、ページがスクリプトを介して埋め込みWebBrowserコントロールを制御できるかどうかを決定します。 |
| Internet Explorer で VBScript 実行を許可する | 無効 | このポリシー設定を使用すると、Internet Explorerの指定されたゾーンのページでVBScriptを実行できるかどうかを管理できます。 |
| Javaのアクセス許可 | 有効 オプション： Java のアクセス許可: Java を無効にする | このポリシー設定を使用すると、Javaアプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Javaを無効にして、アプレットが実行されないようにします。 |
| SmartScreenフィルター スキャンを有効にする | 有効 オプション: SmartScreen フィルター機能を使う: 有効 | SmartScreenフィルターがこのゾーンのページで悪意のあるコンテンツをスキャンするかどうかを制御します。 |
| TDC ActiveX コントロールの資料を承認済のドメインにのみ許可する | 有効 オプション: TDC ActiveX コントロールの使用を承認済みのドメインにのみ許可する: 有効 | このポリシー設定は、ActiveXコントロールをインストールしたWebサイト以外のWebサイトでActiveXコントロールの実行を許可するようにユーザーに求めるかどうかを制御します。 |
| UserData の常設 | 無効 | このポリシー設定を使用すると、ブラウザーの履歴、お気に入り、XMLストア、またはディスクに保存されたWebページ内での情報の保存を管理できます。ユーザーが永続化されたページに戻ったときに、このポリシー設定が適切に構成されていれば、ページの状態を復元できます。 |
| XAMLファイルの読み込みを許可する | 無効 | このポリシー設定では、XAML（Extensible Application Markup Language）ファイルの読み込みを管理できます。XAMLはXMLベースの宣言型マークアップ言語であり、Windows Presentation Foundationを活用する豊富なユーザーインターフェイスとグラフィックスの作成に一般的に使用されます。 |
| ウィンドウ上の各ドメインからコンテンツをドラッグできるようにします | 無効 | このポリシー設定を使用すると、ソースと宛先が異なるウィンドウにあるときに、あるドメインから別のドメインにコンテンツをドラッグするためのオプションを設定できます。 |
| ウィンドウ内の別のドメインからのコンテンツのドラッグを有効にする | 無効 | このポリシー設定を使用すると、ソースと宛先が同じウィンドウにあるときに、あるドメインから別のドメインにコンテンツをドラッグするためのオプションを設定できます。 |
| クロスサイト スクリプト フィルターを有効にする | 有効 オプション: クロスサイト スクリプト (XSS) フィルターを有効にする: 有効 | クロスサイトスクリプティング（XSS）フィルターがこのゾーンのWebサイトへのクロスサイトスクリプト挿入を検出および防止するかどうかを制御します。 |
| サイズや位置の制限なしにスクリプトでウィンドウを開くことを許可する | 無効 | このポリシー設定を使用すると、スクリプトで起動されるポップアップウィンドウ、およびタイトルバーとステータスバーを含むウィンドウの制限を管理できます。 |
| スクリプトによる切り取り、コピー、またはクリップボードからの貼り付け操作を許可する | 無効 | このポリシー設定を使用すると、指定した領域でスクリプトがクリップボード操作（切り取り、コピー、貼り付けなど）を実行できるかどうかを管理できます。 |
| スクリプトレットを許可する | 無効 | このポリシー設定を使用すると、ユーザーがスクリプトレットを実行できるかどうかを管理できます。 |
| スクリプトを介してステータスバーの更新を許可する | 無効 | このポリシー設定を使用すると、スクリプトがゾーン内のステータスバーを更新できるかどうかを管理できます。 |
| スクリプトを実行しても安全だとマークされていない ActiveX コントロールの初期化とスクリプトの実行 | 無効 | このポリシー設定を使用すると、安全とマークされていないActiveXコントロールを管理できます。このポリシー設定を有効にすると、ActiveXコントロールが実行され、パラメーターが読み込まれ、信頼されていないデータまたはスクリプトのオブジェクトの安全性を設定せずにスクリプトが作成されます。この設定は、セキュリティで保護されたゾーンを除いて推奨されません。この設定により、安全でないコントロールと安全なコントロールの両方が初期化およびスクリプト化され、スクリプトオプションに対して安全とマークされたActiveXコントロールのスクリプトは無視されます。 |
| ドメイン間でデータ ソースのアクセス | 無効 | このポリシー設定を使用すると、Microsoft XML Parser（MSXML）またはActiveX Data Objects（ADO）を使用して、Internet Explorerが別のセキュリティゾーンのデータにアクセスできるかどうかを管理できます。 |
| ファイルのダウンロード時に自動的にダイアログを表示 | 無効 | ファイルのダウンロードがユーザー以外によって開始されたときにユーザーにメッセージを表示するかどうかを管理できます。この設定に関係なく、ユーザーによってダウンロードが開始された場合はファイル ダウンロードのダイアログが表示されます。 この設定を無効にした場合、または構成しなかった場合は、ユーザー以外によって開始されたファイルのダウンロードはブロックされ、ファイル ダウンロードのダイアログの代わりに通知バーがユーザーに表示されます。その後、ユーザーは通知バーをクリックしてファイル ダウンロードのダイアログ表示を許可できます。 |
| ファイルのドラッグ/ドロップ、またはコピー/貼り付けを許可する | 無効 | このポリシー設定を使用すると、ユーザーがゾーン内のソースからファイルをドラッグしたり、ファイルをコピーして貼り付けたりできるかどうかを管理できます。 |
| ポップアップ ブロックの使用 | 有効 オプション：有効 | 不要なポップアップウィンドウが表示されるかどうかを管理できます。エンドユーザーがリンクをクリックしたときに開かれるポップアップウィンドウはブロックされません。 |
| ユーザーがサーバーにファイルをアップロードするときにローカル パスを含める | 無効 | このポリシー設定は、ユーザーがHTMLフォーム経由でファイルをアップロードするときにローカルパス情報を送信するかどうかを制御します。ローカルパス情報が送信されると、一部の情報が意図せずにサーバーに公開される可能性があります。たとえば、ユーザーのデスクトップから送信されたファイルには、パスの一部としてユーザー名が含まれている場合があります。 |
| より権限の少ない Web コンテンツゾーンの Web サイトがこのゾーンに移動できる | 無効 | このポリシー設定を使用すると、制限付きサイトなど、特権の低いゾーンのWebサイトがこのゾーンに移動できるかどうかを管理できます。 |
| ログオンのオプション | 有効 オプション：ユーザー名とパスワードを入力してログオンする | このポリシー設定を使用すると、ログオンオプションの設定を管理できます。ユーザー名とパスワードの入力を求めて、ユーザーにユーザーIDとパスワードを照会します。ユーザーが照会された後、これらの値はセッションの残りの部分でサイレントに使用できます。 |
| 安全でない可能性があるファイルに対するセキュリティ警告を表示する | 有効 オプション：ダイアログを表示する | このポリシー設定は、ユーザーが実行可能ファイルまたはその他の安全でない可能性のあるファイル（たとえば、エクスプローラーを使用してイントラネットファイル共有から）を開こうとしたときに、「ファイルを開く-セキュリティ警告」メッセージを表示するかどうかを制御します。 |
| 異なるドメイン間のウィンドウとフレームの移動 | 無効 | このポリシー設定を使用すると、異なるドメイン間でウィンドウとフレームのオープンとアプリケーションのアクセスを管理できます。 |
| 保護モードを有効にする | 有効 オプション：有効 | 保護モードをオンにできます。保護モードは、Internet Explorerがレジストリおよびファイルシステムに書き込むことができる場所を減らすことにより、悪用された脆弱性からInternet Explorerを保護するのに役立ちます。 |
| 未署名の ActiveX コントロールのダウンロード | 無効 | このポリシー設定を使用すると、ユーザーがゾーンから署名されていない ActiveX コントロールをダウンロードできるかどうかを管理できます。そのようなコードは、特に信頼できないゾーンから来た場合、潜在的に有害です。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[セキュリティ ページ]>[イントラネットゾーン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ActiveX コントロールに対してマルウェア対策プログラムを実行しない | 有効 オプション：無効 | Internet ExplorerがActiveXコントロールに対してマルウェア対策プログラムを実行するかどうかを決定し、ページにロードしても安全かどうかを確認します。 |
| Java のアクセス許可 | 有効: オプション:無効 | このポリシー設定では、Javaアプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム:権限の設定を個別に制御します。Javaを無効にして、アプレットが実行されないようにします。 |
| SmartScreen フィルター スキャンを有効にする | 有効 オプション:有効 | SmartScreenフィルターがこのゾーンのページで悪意のあるコンテンツをスキャンするかどうかを制御します。 |
| スクリプトを実行しても安全だとマークされていない ActiveX コントロールの初期化とスクリプトの実行 | 有効 オプション:無効 | このポリシー設定を使用すると、安全とマークされていないActiveXコントロールを管理できます。このポリシー設定を有効にすると、ActiveXコントロールが実行され、パラメーターが読み込まれ、信頼されていないデータまたはスクリプトのオブジェクトの安全性を設定せずにスクリプトが作成されます。この設定は、セキュリティで保護されたゾーンを除いて推奨されません。この設定により、安全でないコントロールと安全なコントロールの両方が初期化およびスクリプト化され、スクリプトオプションに対して安全とマークされたActiveXコントロールのスクリプトは無視されます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[セキュリティ ページ]>[ローカルマシンゾーン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ActiveX コントロールに対してマルウェア対策プログラムを実行しない | 無効 | Internet ExplorerがActiveXコントロールに対してマルウェア対策プログラムを実行するかどうかを決定し、ページにロードしても安全かどうかを確認します。 |
| Java のアクセス許可 | 有効 オプション：Javaを無効にする | このポリシー設定を使用すると、Javaアプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Javaを無効にして、アプレットが実行されないようにします。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[セキュリティ ページ]>[ロックダウンされたインターネットゾーン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| SmartScreen フィルター スキャンを有効にする | 有効 オプション：有効 | SmartScreenフィルターがこのゾーンのページで悪意のあるコンテンツをスキャンするかどうかを制御します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[セキュリティ ページ]>[ロックダウンされたイントラネットゾーン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Javaのアクセス許可 | 有効 オプション：Javaを無効にする | このポリシー設定を使用すると、Javaアプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Javaを無効にして、アプレットが実行されないようにします。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[セキュリティ ページ]>[ロックダウンされたローカルコンピューターゾーン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Java のアクセス許可 | 有効 オプション：Javaを無効にする | このポリシー設定を使用すると、Javaアプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Javaを無効にして、アプレットが実行されないようにします。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[セキュリティ ページ]>[ロックダウンされた信頼済みサイト]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Java のアクセス許可 | 有効 オプション：Javaを無効にする | 選択したセキュリティレベルのデフォルト（低、中、高など）に応じてポリシー設定を構成できます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[セキュリティ ページ]>[ロックダウンされた制限付きサイトゾーン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Java のアクセス許可 | 有効 オプション：Javaを無効にする | このポリシー設定を使用すると、Javaアプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Javaを無効にして、アプレットが実行されないようにします。 |
| SmartScreen フィルター スキャンを有効にする | 有効 オプション：有効 | SmartScreenフィルターがこのゾーンのページで悪意のあるコンテンツをスキャンするかどうかを制御します。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[セキュリティ ページ]>[信頼済みサイト]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ActiveX コントロールに対してマルウェア対策プログラムを実行しない | 無効 | Internet ExplorerがActiveXコントロールに対してマルウェア対策プログラムを実行するかどうかを決定し、ページにロードしても安全かどうかを確認します。 |
| Java のアクセス許可 | 有効 オプション：安全性-高 | このポリシー設定を使用すると、Javaアプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。安全性が高いため、アプレットをサンドボックスで実行できます。 |
| スクリプトを実行しても安全だとマークされていない ActiveX コントロールの初期化とスクリプトの実行 | 無効 | このポリシー設定を使用すると、安全とマークされていないActiveXコントロールを管理できます。このポリシー設定を有効にすると、ActiveXコントロールが実行され、パラメーターが読み込まれ、信頼されていないデータまたはスクリプトのオブジェクトの安全性を設定せずにスクリプトが作成されます。この設定は、セキュリティで保護されたゾーンを除いて推奨されません。この設定により、安全でないコントロールと安全なコントロールの両方が初期化およびスクリプト化され、スクリプトオプションに対して安全とマークされたActiveXコントロールのスクリプトは無視されます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[インターネットコントロールパネル]>[セキュリティ ページ]>[制限付きサイトゾーン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ActiveXコントロールとプラグインを実行する | 有効 オプション：無効 | このポリシー設定を使用すると、指定したゾーンのページでActiveXコントロールとプラグインを実行できるかどうかを管理できます。 |
| ActiveX コントロールに対してマルウェア対策プログラムを実行しない | 無効 | Internet ExplorerがActiveXコントロールに対してマルウェア対策プログラムを実行するかどうかを決定し、ページにロードしても安全かどうかを確認します。 |
| Authenticode 署名済みではない .NET Framework コンポーネントを実行する | 無効 | このポリシー設定を使用すると、Authenticodeで署名されていない.NET FrameworkコンポーネントをInternet Explorerから実行できるかどうかを管理できます。これらのコンポーネントには、オブジェクトタグから参照されるマネージコントロールと、リンクから参照されるマネージ実行可能ファイルが含まれます。 |
| Authenticode 署名済みの .NET Framework コンポーネントを実行する | 有効 オプション：無効 | このポリシー設定を使用すると、Authenticodeで署名された.NET FrameworkコンポーネントをInternet Explorerから実行できるかどうかを管理できます。これらのコンポーネントには、オブジェクトタグから参照されるマネージコントロールと、リンクから参照されるマネージ実行可能ファイルが含まれます。 |
| IFRAME のアプリケーションとファイルの起動 | 無効 | このポリシー設定を使用すると、アプリケーションを実行できるかどうか、およびこのゾーンのページのHTMLのIFRAME参照からファイルをダウンロードできるかどうかを管理できます。 |
| Internet Explorer WebBrowser コントロールのスクリプトを許可する | 無効 | このポリシー設定は、ページがスクリプトを介して埋め込みWebBrowserコントロールを制御できるかどうかを決定します。 |
| Internet Explorer での VBScript　実行を許可する | 無効 | このポリシー設定を使用すると、Internet Explorerの指定されたゾーンのページでVBScriptを実行できるかどうかを管理できます。 |
| Java アプレットのスクリプト | 無効 | このポリシー設定を使用すると、アプレットがゾーン内のスクリプトに公開されるかどうかを管理できます。 |
| Java のアクセス許可 | 有効 オプション：Javaを無効にする | このポリシー設定を使用すると、Javaアプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Javaを無効にして、アプレットが実行されないようにします。 |
| SmartScreen フィルター スキャンを有効にする | 有効 オプション：有効 | SmartScreenフィルターがこのゾーンのページで悪意のあるコンテンツをスキャンするかどうかを制御します。 |
| TDC ActiveX コントロールの使用を承認済みのドメインにのみ許可する | 有効 | このポリシー設定は、ユーザーがWebサイトでTDC ActiveXコントロールを実行できるかどうかを制御します。 |
| UserData の常設 | 無効 | このポリシー設定を使用すると、ブラウザーの履歴、お気に入り、XMLストア、またはディスクに保存されたWebページ内での情報の保存を管理できます。ユーザーが永続化されたページに戻ったときに、このポリシー設定が適切に構成されていれば、ページの状態を復元できます。 |
| XAML ファイルの読み込みを許可する | 無効 | このポリシー設定では、XAML（Extensible Application Markup Language）ファイルの読み込みを管理できます。XAMLはXMLベースの宣言型マークアップ言語であり、Windows Presentation Foundationを活用する豊富なユーザーインターフェイスとグラフィックスの作成に一般的に使用されます。 |
| アクティブ スクリプトの許可 | 無効 | このポリシー設定を使用すると、ゾーン内のページでスクリプトコードを実行するかどうかを管理できます。 |
| ウィンドウ上の各ドメインからコンテンツをドラッグを有効にする | 無効 | このポリシー設定を使用すると、ソースと宛先が異なるウィンドウにあるときに、あるドメインから別のドメインにコンテンツをドラッグするためのオプションを設定できます。 |
| ウィンドウ内の別のドメインからコンテンツのドラッグを有効にする | 無効 | このポリシー設定を使用すると、ソースと宛先が同じウィンドウにあるときに、あるドメインから別のドメインにコンテンツをドラッグするためのオプションを設定できます。 |
| クロスサイト スクリプティング フィルターを有効にする | 有効 オプション：有効 | クロスサイトスクリプティング（XSS）フィルターがこのゾーンのWebサイトへのクロスサイトスクリプト挿入を検出および防止するかどうかを制御します。 |
| サイズや位置の制限なしにスクリプトでウィンドウを開くことを許可する | 有効 オプション：無効 | このポリシー設定を使用すると、スクリプトで起動されるポップアップウィンドウ、およびタイトルバーとステータスバーを含むウィンドウの制限を管理できます。 |
| スクリプトによる切り取り、コピー、またはクリップボードからの貼り付け操作を許可する | 有効 オプション：無効 | このポリシー設定を使用すると、指定した領域でスクリプトがクリップボード操作（切り取り、コピー、貼り付けなど）を実行できるかどうかを管理できます。 |
| スクリプトレットを許可する | 無効 | このポリシー設定を使用すると、ユーザーがスクリプトレットを実行できるかどうかを管理できます。 |
| スクリプトを介したステータス バーの更新を許可する | 無効 | このポリシー設定を使用すると、スクリプトがゾーン内のステータスバーを更新できるかどうかを管理できます。 |
| スクリプトを実行しても安全だとマークされていない ActiveX コントロールの初期化とスクリプトの実行 | 無効 | このポリシー設定を使用すると、安全とマークされていないActiveXコントロールを管理できます。このポリシー設定を有効にすると、ActiveXコントロールが実行され、パラメーターが読み込まれ、信頼されていないデータまたはスクリプトのオブジェクトの安全性を設定せずにスクリプトが作成されます。この設定は、セキュリティで保護されたゾーンを除いて推奨されません。この設定により、安全でないコントロールと安全なコントロールの両方が初期化およびスクリプト化され、スクリプトオプションに対して安全とマークされたActiveXコントロールのスクリプトは無視されます。 |
| スクリプトを実行しても安全とマークされている ActiveX コントロールのスクリプトの実行 | 無効 | このポリシー設定を使用すると、スクリプトを実行しても安全とマークされたActiveXコントロールがスクリプトと対話できるかどうかを管理できます。 |
| ドメイン間でのデータソースのアクセス | 有効 オプション：無効 | このポリシー設定を使用すると、Microsoft XML Parser（MSXML）またはActiveX Data Objects（ADO）を使用して、Internet Explorerが別のセキュリティゾーンのデータにアクセスできるかどうかを管理できます。 |
| バイナリ ビヘイビアーとスクリプト ビヘイビアーの許可 | 無効 | このポリシー設定を使用すると、動的なバイナリおよびスクリプトの動作を管理できます。これらの動作は、それらが添付されたHTML要素の特定の機能をカプセル化するコンポーネントです。 |
| ファイルのダウンロードの許可 | 無効 | このポリシー設定を使用すると、ゾーンからのファイルのダウンロードを許可するかどうかを管理できます。このオプションは、ファイルの配信元のゾーンではなく、ダウンロードの原因となっているリンクがあるページのゾーンによって決定されます。 |
| ファイルのダウンロード時に自動的にダイアログを表示 | 無効 | このポリシー設定は、ユーザーが開始しないファイルのダウンロードをユーザーに求めるかどうかを決定します。この設定に関係なく、ユーザーは、ユーザーが開始したダウンロードのファイルダウンロードダイアログを受け取ります。 |
| ファイルのドラッグ/ドロップ、またはコピー/貼り付けの許可 | 無効 | このポリシー設定を使用すると、ユーザーがゾーン内のソースからファイルをドラッグしたり、ファイルをコピーして貼り付けたりできるかどうかを管理できます。 |
| ページの自動読み込み | 無効 | このポリシー設定を使用すると、Webページの作成者がMeta Refresh設定（タグ）を使用してブラウザーを別のWebページにリダイレクトする場合に、ユーザーのブラウザーを別のWebページにリダイレクトできるかどうかを管理できます。 |
| ポップアップ ブロックの使用 | 有効 オプション: 有効 | 不要なポップアップウィンドウが表示されるかどうかを管理できます。エンドユーザーがリンクをクリックしたときに開かれるポップアップウィンドウはブロックされません。 |
| ユーザーがファイルをサーバーにアップロードするときにローカルパスを含める | 無効 | このポリシー設定は、ユーザーがHTMLフォーム経由でファイルをアップロードするときにローカルパス情報を送信するかどうかを制御します。ローカルパス情報が送信されると、一部の情報が意図せずにサーバーに公開される可能性があります。たとえば、ユーザーのデスクトップから送信されたファイルには、パスの一部としてユーザー名が含まれている場合があります。 |
| より権限の少ない Web コンテンツ ゾーンの Web サイトがこのゾーンに移動できる | 無効 | このポリシー設定を使用すると、インターネットサイトなど、特権の低いゾーンからのWebサイトがこのゾーンに移動できるかどうかを管理できます。 |
| ログオンのオプション | 有効 オプション：匿名ログオン | このポリシー設定を使用すると、ログオンオプションの設定を管理できます。HTTP認証を無効にし、Common Internet File System（CIFS）プロトコルにのみゲストアカウントを使用する匿名ログオン。 |
| 安全でない可能性があるファイルのセキュリティ警告を表示する | 無効 | このポリシー設定は、ユーザーが実行可能ファイルまたはその他の安全でない可能性のあるファイル（たとえば、エクスプローラーを使用してイントラネットファイル共有から）を開こうとしたときに、「ファイルを開く-セキュリティ警告」メッセージを表示するかどうかを制御します。このポリシー設定を無効にすると、これらのファイルは開きません。 |
| 異なるドメイン間のウィンドウとフレームの移動 | 有効 オプション:無効 | このポリシー設定を使用すると、異なるドメイン間でウィンドウとフレームのオープンとアプリケーションのアクセスを管理できます。 |
| 許可されたドメインにのみ、警告なしで ActiveX を使用することを認める | 有効 オプション:有効 | このポリシー設定は、ActiveXコントロールをインストールしたWebサイト以外のWebサイトでActiveXコントロールの実行を許可するようにユーザーに求めるかどうかを制御します。 |
| 署名済み ActiveX コントロールのダウンロード | 無効 | このポリシー設定を使用すると、ユーザーがゾーン内のページから署名済みActiveXコントロールをダウンロードできるかどうかを管理できます |
| 保護モードをオンにする | 有効 オプション：有効 | 保護モードをオンにできます。保護モードは、Internet Explorerがレジストリおよびファイルシステムに書き込むことができる場所を減らすことにより、悪用された脆弱性からInternet Explorerを保護するのに役立ちます。 |
| 未署名の ActiveX コントロールのダウンロード | 無効 | このポリシー設定を使用すると、ユーザーがゾーンから署名されていないActiveXコントロールをダウンロードできるかどうかを管理できます。そのようなコードは、特に信頼できないゾーンから来た場合、潜在的に有害です。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[セキュリティの機能]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| SSL 3.0 へのフォールバックを許可する（Internet Explorer） | 有効 オプション：サイトなし | SSL 3.0への安全でないフォールバックをブロックできます。このポリシーを有効にすると、Internet Explorerは、TLS 1.0以上が失敗したときにSSL 3.0以下を使用してサイトへの接続を試みます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[セキュリティの機能]>[ActiveXインストールの制限]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Internet Explorer のプロセス | 有効 | このポリシー設定は、Internet ExplorerプロセスのActiveXコントロールインストールプロンプトのブロックを有効にします。このポリシー設定を有効にすると、Internet ExplorerプロセスでActiveXコントロールのインストールのプロンプトがブロックされます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[セキュリティの機能]>[MIME スニッフィングの安全機能]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Internet Explorer のプロセス | 有効 | このポリシー設定は、Internet ExplorerのMIMEスニッフィングが、あるタイプのファイルをより危険なファイルタイプに昇格させないようにするかどうかを決定します。このポリシー設定を有効にした場合、MIMEスニッフィングは、あるタイプのファイルをより危険なファイルタイプに昇格させることはありません。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[セキュリティの機能]>[MK プロトコル セキュリティの制限]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Internet Explorer のプロセス | 有効 | このポリシー設定は、Internet ExplorerのMIMEスニッフィングが、あるタイプのファイルをより危険なファイルタイプに昇格させないようにするかどうかを決定します。このポリシー設定を有効にした場合、MIMEスニッフィングは、あるタイプのファイルをより危険なファイルタイプに昇格させることはありません。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[セキュリティの機能]>[アドオン管理]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Internet Explorer で古い ActiveX コントロールの [今回は実行] ボタンを削除する | 有効 | このポリシー設定を使用すると、ユーザーが[今回実行]ボタンを表示したり、Internet Explorerで特定の古いActiveXコントロールを実行したりするのを停止できます。 |
| Internet Explorer の古い ActiveX コントロールのブロックを無効する | 無効 | このポリシー設定は、Internet Explorerが特定の古いActiveXコントロールをブロックするかどうかを決定します。古いActiveXコントロールがイントラネットゾーンでブロックされることはありません。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[セキュリティの機能]>[スクリプト化されたウィンドウのセキュリティ制限]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Internet Explorer のプロセス | 有効 | Internet Explorerでは、スクリプトを使用して、さまざまな種類のウィンドウをプログラムで開いたり、サイズを変更したり、位置を変更したりできます。ウィンドウ制限セキュリティ機能は、ポップアップウィンドウを制限し、タイトルとステータスバーがユーザーに見えないウィンドウを表示したり、他のWindowsのタイトルとステータスバーを難読化したりするスクリプトを禁止します。このポリシー設定を有効にすると、ポップアップウィンドウとその他の制限がエクスプローラーとInternet Explorerのプロセスに適用されます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[セキュリティの機能]>[ゾーン昇格からの保護]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Internet Explorer のプロセス | 有効 | Internet Explorerは、開く各Webページに制限を設けます。制限は、Webページの場所（インターネット、イントラネット、ローカルコンピューターゾーンなど）に依存します。ローカルコンピューター上のWebページは、セキュリティ制限が最も少なく、ローカルコンピューターゾーンに存在するため、ローカルコンピューターセキュリティゾーンは悪意のあるユーザーの主要な標的になります。ゾーンの高度は、セキュリティコンテキストがない場合、JavaScriptナビゲーションも無効にします。このポリシー設定を有効にすると、Internet Explorerプロセスによるゾーンの昇格からすべてのゾーンを保護できます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[セキュリティの機能]>[ファイルダウンロードの制限]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Internet Explorer のプロセス | 有効 | このポリシー設定は、ユーザーが開始したものではないファイルダウンロードプロンプトのブロックを有効にします。このポリシー設定を有効にすると、ユーザーが開始したものではないファイルのダウンロードプロンプトは、Internet Explorerプロセスに対してブロックされます。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[セキュリティの機能]>[整合性のあるMIME処理]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Internet Explorer のプロセス | 有効 | Internet Explorerは、MIME（Multipurpose Internet Mail Extensions）データを使用して、Webサーバー経由で受信したファイルのファイル処理手順を決定します。このポリシー設定は、Webサーバーが提供するすべてのファイルタイプ情報の一貫性をInternet Explorerで要求するかどうかを決定します。たとえば、ファイルのMIMEタイプがtext / plainであるが、MIMEスニフがそのファイルが実際に実行可能ファイルであることを示している場合、Internet ExplorerはファイルをInternet Explorerキャッシュに保存して拡張子を変更することでファイル名を変更します。このポリシー設定を有効にした場合、Internet Explorerでは、受信したすべてのファイルに対して一貫したMIMEデータが必要です。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント] >[Internet Explorer]>[セキュリティの機能]>[通知バー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Internet Explorer のプロセス | 有効 | このポリシー設定を使用すると、ファイルまたはコードのインストールが制限されている場合に、Internet Explorerプロセスの通知バーを表示するかどうかを管理できます。デフォルトでは、Internet Explorerプロセスの通知バーが表示されます。このポリシー設定を有効にすると、Internet Explorerプロセスの通知バーが表示されます。 |

### ・L1 コントロール

#### コントロールの方針

| **ポリシー設定** | **構成方針** | **説明** |
| --- | --- | --- |
| ローカル管理者パスワードソリューション（LAPS） | すべてのデバイスに展開 | デバイスに対する一意のローカル管理者パスワードを生成し、多くの横方向のトラバーサル攻撃を軽減します。 |
| Windows Defender ATP EDR | すべてのデバイスに展開 | Windows Defender ATP エンドポイント検出および応答（EDR）は、高度な攻撃の実用的でほぼリアルタイムの検出を提供します。EDR はセキュリティアナリストを支援し、同じ攻撃手法でアラートを集約するか、同じ攻撃者に起因するアラートをインシデントと呼ばれるエンティティに集約します。インシデントは、アナリストがアラートに優先順位を付け、違反の範囲全体をまとめて調査し、脅威に対応するのに役立ちます。Windows Defender ATP EDR は、ユーザーやアプリケーションに影響を与えることは想定されておらず、1つの手順ですべてのデバイスに展開できます。 |
| Windows Defender Credential Guard | 互換性のあるすべてのハードウェアで有効化 | Windows Defender Credential Guard は、仮想化ベースのセキュリティを使用してシークレットを分離し、特権システムソフトウェアのみがシークレットにアクセスできるようにします。これらの秘密への不正アクセスは、Pass-the-Hash や Pass-The-Ticket などの資格情報の盗難攻撃につながる可能性があります。Windows Defender Credential Guard は、NTLM パスワードハッシュ、Kerberos チケット許可チケット（TGT）、およびドメイン資格情報としてアプリケーションによって保存された資格情報を保護することにより、これらの攻撃を防ぎます。アプリケーションが NTLMv1、Kerberos DES 暗号化、Kerberos の制約のない委任、または Keberos TGT の抽出を必要とするとアプリケーションが破損するため、アプリケーションの互換性にわずかなリスクがあります。そのため、マイクロソフトでは、リングの方法論を使用して Credential Guard を展開することをお勧めします。 |
| Microsoft Edge | デフォルトブラウザ | Windows 10 の Microsoft Edgeは、Internet Explorer 11（IE11）よりも優れたセキュリティを提供します。一部のサイトとの互換性のために IE11 を活用する必要がある場合もありますが、Microsoft Edge をデフォルトのブラウザーとして構成し、それを必要とするサイトのみに IE11 にリダイレクトするエンタープライズモードサイトリストを作成することをお勧めします。マイクロソフトは、Windows Analytics またはEnterprise Site Discovery のいずれかを活用して初期のエンタープライズモードサイトリストを作成し、その後リング方式を使用してこの構成を徐々に展開することをお勧めします。 |
| Windows Defender Application Guard | 互換性のあるハードウェアで有効化 | Windows Defender Application Guard は、ハードウェア分離アプローチを使用します。従業員が Microsoft Edge または Internet Explorer のいずれかを介して信頼できないサイトにアクセスすると、Microsoft Edge は、ホストオペレーティングシステムとは別の Hyper-V によって有効化された隔離されたコンテナーでサイトを開きます。信頼されていないサイトが悪意のあるサイトであることが判明した場合、隔離されたコンテナがホスト PC を保護し、攻撃者は企業データにアクセスできません。一部のアプリケーションはホスト PC との対話を必要とする場合がありますが、Application Guard の信頼できるWebサイトのリストにはまだ含まれていない可能性があるため、アプリケーションの互換性にはわずかなリスクがあります。マイクロソフトでは、Windows Analytics または Enterprise Site Discovery を活用して初期ネットワーク分離設定を構築し、リング方法論を使用してこの構成を徐々に展開することをお勧めします。 |
| ネットワーク保護 | ネットワーク保護の構成と実施 | ネットワーク保護は、従業員がアプリケーションを使用して、フィッシング詐欺、エクスプロイト、およびインターネット上のその他の悪意のあるコンテンツをホストする可能性のある危険なドメインにアクセスするのを防ぐのに役立ちます。これは、Windows Defender SmartScreen の範囲を拡張して、低レピュテーションソース（ドメインまたはホスト名に基づく）への接続を試みるすべてのアウトバウンド HTTP トラフィックをブロックします。フラグ付きサイトでの誤検知の結果として、アプリケーションの互換性にリスクがあります。Microsoftは、Audit / Enforce Methodologyを使用して展開することをお勧めします。 |

#### アクション

| **項目** | **構成方針** | **説明** |
| --- | --- | --- |
| OSセキュリティアップデート | リリースから7日以内にWindows品質更新プログラムを展開する | パッチのリリースから、そのパッチのリバースエンジニアリングに基づくエクスプロイトまでの期間が短縮されるにつれて、セキュリティ維持の重要な側面は、セキュリティの脆弱性に対処する品質アップデートを迅速に検証して展開するエンジニアリングプロセスを持つことです。 |

### ・L1 OFFICE2016の共通設定

以下のレジストリ設定はポリシーキーに格納されていないため、優先される設定であるとみなされます。そのため、この設定を実装するグループポリシーオブジェクトが削除された場合、このレジストリ設定は残ります。

|  |  |
| --- | --- |
| **項目** | **値** |
| ハイブ | HKLM |
| キー名 | \Software\Microsoft\Internet Explorer\Main\FeatureControl |
| REG DWORD | = 0 無効  = 1 有効 |

値は、各項目の説明にあります。

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Microsoft Office 2016(マシン)]>[セキュリティ設定]>[IEのセキュリティ]

|  |  |  |
| --- | --- | --- |
| **ポリシー設定** | **値** | **説明** |
| ActiveX のインストールを制限する | 有効 使用しているアプリケーションをチェックする | 適切な制限のためにActiveXインストールを設定する必要があります。 \FEATURE\_RESTRICT\_ACTIVEXINSTALL |
| MIME スニッフィングの安全機能 | 有効 使用しているアプリケーションをチェックする | MIMEファイルタイプのなりすましは、組織にとって潜在的な脅威です。ネットワークに感染する可能性のある悪意のあるファイルのダウンロードを防ぐために、これらのファイルが一貫して処理されるようにすることをお勧めします。 \MIME SNIFFING SAFETY FEATURE |
| URL からの保存 | 有効 使用しているアプリケーションをチェックする | 通常、Internet ExplorerがMark of the Web(MOTW)コメントを含むWebページをUniversal Naming Convention(UNC)共有からロードするとき、そのページがインターネット上のサイトから保存されたことを示すと、Internet Explorerは制限の緩いローカルイントラネットセキュリティゾーンではなく、インターネットセキュリティゾーンでページを実行します。この機能は、Officeアプリケーション(たとえば、ユーザーがOfficeドキュメント内のリンクをクリックするか、Webページをロードするメニューオプションを選択した場合)によって起動されるInternet Explorerのインスタンスに対して個別に制御できます。Internet ExplorerがページをMOTWとして評価しない場合、危険なコードの実行が許可される可能性があります。 \FEATURE\_UNC\_SAVEDFILECHECK |
| URL への移動 | 有効 使用しているアプリケーションをチェックする | ユーザーを攻撃から保護するために、Internet Explorerは通常、不正なURLをロードしようとしません。この機能は、Officeアプリケーションによって生成されたInternet Explorerのインスタンスに対して個別に制御できます。 \FEATURE\_VALIDATE\_NAVIGATE\_URL |
| アドオンの管理 | 有効 使用しているアプリケーションをチェックする | アドオン管理機能を許可する必要があります。 \FEATURE\_ADDON\_MANAGEMENT |
| オブジェクト キャッシュ保護 | 有効 使用しているアプリケーションをチェックする | 悪意のあるWebサイトが、他のドメインからのオブジェクト参照を使用しようとする可能性があります。 \OBJECT CACHING PROTECTION |
| オブジェクトにバインドする | 有効 使用しているアプリケーションをチェックする | Internet Explorerは、ActiveXコントロールを初期化する前に、いくつかの安全性チェックを実行します。レジストリにコントロールのKill Bitが設定されている場合、またはコントロールが配置されているゾーンのセキュリティ設定でコントロールの初期化が許可されていない場合、コントロールは初期化されません。 \FEATURE\_SAFE\_BINDTOOBJECT |
| スクリプト化されたウィンドウのセキュリティ制限 | 有効 使用しているアプリケーションをチェックする | この設定を無効にするか、構成しないと、不明なWebサイトで次のことが可能になります。ローカルオペレーティングシステムのブラウザウィンドウを作成します。キーボード入力をキャプチャする画面の表示可能領域の外側に表示されるアクティブなウィンドウを描画します。重要なシステム情報、選択、プロンプトを隠すために、親ウィンドウを独自のブラウザウィンドウでオーバーレイします。 \FEATURE\_WINDOW\_RESTRICTIONS |
| ゾーン昇格からの保護 | 有効 使用しているアプリケーションをチェックする | この設定を無効にするか、構成しないと、インターネットゾーンのページがローカルコンピューターゾーンのページに移動して、コードを実行して特権を昇格させる可能性があります。これにより、悪意のあるコードまたはユーザーがユーザーのコンピューターまたはネットワークでアクティブになる可能性があります。 \FEATURE\_ZONE\_ELEVATION |
| ファイルのダウンロードを制限する | 有効 使用しているアプリケーションをチェックする | この設定を無効にすると、ユーザーが特にダウンロードを開始しなくても、Webサイトでコードを介してファイルのダウンロードプロンプトを表示できます。ユーザー設定により、プロンプトやユーザーとの対話なしでダウンロードを実行することもできます。 \FEATURE\_RESTRICT\_FILEDOWNLOAD |
| ポップアップをブロックする | 有効 使用しているアプリケーションをチェックする | Internet Explorerのポップアップブロッカー機能を使用して、ほとんどの不要なポップアップおよびポップアンダーウィンドウの表示をブロックできます。この機能は、Officeアプリケーションによって生成されたInternet Explorerのインスタンスに対して個別に制御できます（たとえば、ユーザーがOfficeドキュメント内のリンクをクリックするか、Webページを読み込むメニューオプションを選択した場合）。 \FEATURE\_WEBOC\_POPUPMANAGEMENT |
| ユーザー名とパスワードを無効にする | 有効 使用しているアプリケーションをチェックする | URL（Uniform Resource Locator）標準では、ユーザー認証をhttp://username:password@example.comの形式でURL文字列に含めることができます。悪意のあるユーザーは、このURL構文を使用して、正当なWebサイトを開くように見えるが、実際には偽の（なりすまし）Webサイトを開くハイパーリンクを作成する可能性があります。たとえば、URL http://www.wingtiptoys.com@example.comはhttp://www.wingtiptoys.comを開くように見えますが、実際にはhttp://example.comを開きます。ユーザーをこのような攻撃から保護するために、Internet Explorerは通常、この構文を使用してURLをブロックします。 \FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE |
| ローカルコンピュータ ゾーンのロックダウン セキュリティ | 有効 | ローカルマシンゾーンのセキュリティは、すべてのローカルファイルとコンテンツに適用されます。この機能は、ローカルマシンゾーンが悪意のあるHTMLコードをロードするための攻撃ベクトルとして使用される攻撃を軽減するのに役立ちます。 \FEATURE\_LOCALMACHINE\_LOCKDOWN |
| 一貫性のある MIME 処理 | 有効 使用しているアプリケーションをチェックする | ユーザーは、Internet Explorerを使用して、誤ったファイル名拡張子を装った、またはMIMEヘッダーに誤ってマークされた悪意のあるコンテンツを無意識のうちにダウンロードする可能性があります。ダウンロードされると、誤ったハンドラーがファイルを実行し、悪意のあるコンテンツがユーザーのシステムまたはネットワークに損害を与える可能性があります。 \FEATURE\_MIME\_HANDLING |
| 情報バー | 有効 使用しているアプリケーションをチェックする | 情報バーは、悪意のある可能性のあるコンテンツがいつブロックされたかをユーザーが理解するのに役立ちます。一方、一部のユーザーは、バーの外観に混乱したり、応答方法がわからない場合があります。 \FEATURE\_SECURITYBAND |

### ・L1 Excel 2016

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Excel 2016]>[Excelオプション]>[セキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Excel Open XML ブック内の暗号化されたマクロをスキャンする | 無効 | Open XML ブック内の暗号化されたマクロについて、開く前にウイルス対策ソフトウェアによるスキャンが必要かどうかを指定することができます。 このポリシー設定を有効にした場合、以下のオプションのいずれかを選択できます。 - [暗号化されたマクロをスキャンする]: ウイルス対策ソフトウェアがインストールされていない限り、暗号化されたマクロは無効になります。マクロが含まれている暗号化されたブックを開くときに、暗号化されたマクロがウイルス対策ソフトウェアでスキャンされます。 - [ウイルス対策ソフトウェアが利用できる場合はスキャンする]: ウイルス対策ソフトウェアがインストールされている場合、暗号化されたマクロは読み込まれる前にスキャンされます。ウイルス対策ソフトウェアが利用できない場合、暗号化されたマクロの読み込みを許可します。 - [スキャンせずにマクロを読み込む]: ウイルス対策ソフトウェアの確認を行わず、暗号化されたファイル内のマクロの読み込みを許可します。 このポリシー設定を無効にするか、未構成にした場合、[暗号化されたマクロをスキャンする] オプションを選択した場合と同じ動作になります。 |
| WEBSERVICE 関数の通知設定 | 無効 | Excel で WEBSERVICE 関数が存在する場合に、警告が表示される方法を制御します。このポリシー設定を無効にした場合、[通知してすべてを無効にする] が既定の設定になります。 |
| ファイル検証機能をオフにする | 無効 | Office Binary Documents（97-2003）は、開かれる前にファイル形式スキーマに準拠しているかどうかが確認されます。 |

[ユーザーの構成]>[管理用テンプレート]>[Microsoft Excel 2016]>[Excelオプション]>[セキュリティ]>[セキュリティセンター]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| VBA マクロ通知設定 | 有効 通知してすべてを無効にする | Visual Basic for Applications（VBA）マクロが存在する場合に、指定されたアプリケーションがユーザーに警告する方法を制御します。このポリシー設定を有効にすると、指定されたアプリケーションがマクロについてユーザーに警告する方法を決定するための4つのオプションから選択できます。-すべての通知を無効にする：アプリケーションは、署名の有無にかかわらず、すべてのマクロの信頼バーを表示します。このオプションは、Officeの既定の構成を強制します。 |
| Visual Basic プロジェクトへのアクセスを信頼する | 無効 | このポリシー設定では、Microsoft Visual Studio 2005 Tools for Microsoft Office (VSTO) などのオートメーション クライアントから、指定したアプリケーションの Visual Basic for Applications プロジェクト システムへのアクセスを許可するかどうかを指定します。このポリシー設定を無効にした場合、VSTO から VBA プロジェクトへのプログラムによるアクセスができなくなります。また、[VBA プロジェクト オブジェクト モデルへのアクセスを信頼する] チェック ボックスがオフになり、ユーザーはこの設定を変更できません。注意: このポリシー設定を無効にすると、VSTO プロジェクトと、指定したアプリケーションの VBA プロジェクト システムのやり取りが正常に行われなくなります。 |
| アプリケーション アドインには信頼できる発行元による署名が必要 | 有効 | このポリシー設定を有効にした場合、このアプリケーションで各アドインを読み込む前に、デジタル署名がチェックされます。アドインがデジタル署名されていないか、または信頼できる発行元による署名でない場合、そのアドインは無効になり、ユーザーに通知されます。信頼できる発行元による署名がすべてのアドインで必要であると指定した場合は、信頼できる発行元の一覧に証明書を追加する必要があります。 このポリシー設定を無効にするか、または未構成にした場合、Office 2016 アプリケーションでは、アプリケーション アドインを開く前にそのデジタル署名はチェックされません。危険なアドインが読み込まれた場合は、ユーザーのコンピューターに損害を与えたり、データのセキュリティが低下したりする可能性があります。 |
| インターネットから取得した Office ファイルの内のマクロの実行をブロックします | 有効 | このポリシー設定を有効にした場合、セキュリティ センターの [マクロの設定] セクションで [すべてのマクロを有効にする] がオンになっている場合でも、マクロの実行はブロックされます。また、[コンテンツの有効] の選択肢が表示されないで、マクロの実行がブロックされたことを示す通知が表示されます。Office ファイルが信頼できる場所に保存されている場合、または以前にユーザーが信頼した場合は、マクロを実行できます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Excel 2016]>[Excelオプション]>[セキュリティ]>[セキュリティセンター]>[ファイル制限機能の設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| DIF および SYLK ファイル | 有効 開く/保存をブロックする(オープンポリシーを使用） | [開く/保存をブロックする (オープン ポリシーを使用)]: この種類のファイルを開く操作と保存する操作がブロックされます。ファイルは [ファイル制限機能の既定動作] キーで構成されたポリシー設定に基づいて開かれます。 このポリシー設定を無効にするか、未構成にした場合、この種類のファイルはブロックされません。 |
| dBase Ⅲ / Ⅳ ファイル |
| Excel 2 マクロシートとアドイン ファイル |
| Excel 2 ワークシート |
| Excel 3 マクロシートとアドイン ファイル |
| Excel 3 ワークシート |
| Excel 4 マクロシートとアドイン ファイル |
| Excel 4 ブック |
| Excel 4 ワークシート |
| Excel 95-97 ブックとテンプレート | 有効 開く/保存をブロックする(オープンポリシーを使用） |
| Web ページと Excel 2003 XML スプレッドシート |
| ファイル制限機能の規程動作の設定 | 無効 | このポリシー設定を無効にするか、未構成にした場合、[ブロックされたファイルは開くことができない] オプションの設定と同じ動作になります。ユーザーがブロックされたファイルを開くことはできません。 |
| Excel 95 ブック | 有効 編集を許可し、保護ビューで開く | - [保護ビューで開く (編集可)]: この種類のファイルを開く操作と保存する操作がブロックされ、編集のためのオプションが有効になります。 このポリシー設定を無効にするか、未構成にした場合、この種類のファイルはブロックされません。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Excel 2016]>[Excelオプション]>[セキュリティ]>[セキュリティセンター]>[信頼できる場所]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| すべての信頼できる場所を無効にする | 有効 | 管理者は指定したアプリケーションで、すべての信頼できる場所を無効にできます。セキュリティ センターで指定する信頼できる場所は、安全と見なすことができるファイル保存場所を定義するために使用します。信頼できる場所からは、最低限のセキュリティでコンテンツ、コード、およびアドインを読み込むことができます。また、ユーザーにアクセス許可のプロンプトが表示されることもありません。信頼できる場所から危険なファイルが開かれた場合、標準のセキュリティ対策の対象とはならないため、ユーザーのコンピューターやデータに損害を与える可能性があります。 このポリシー設定を有効にした場合、指定したアプリケーションで、すべての信頼できる場所 (セキュリティ センターで指定) が無視されます。これらの信頼できる場所には、セットアップ中に Office 2016 で設定されたもの、グループ ポリシーを使用してユーザーに展開されたもの、およびユーザー自身が追加したものが含まれます。信頼できる場所からファイルを開くときにはプロンプトが再び表示されます。 |
| ネットワーク上の信頼できる場所を許可する | 無効 | このポリシー設定では、ネットワーク上にある信頼できる場所を使用できるようにするかどうかを指定します。 このポリシー設定を有効にした場合、ユーザーは、セキュリティ センターの [信頼できる場所] セクションにある [新しい場所の追加] ボタンをクリックすることによって、ネットワーク共有または直接の管理下にない別のリモートの場所にある信頼できる場所を指定できます。信頼できる場所からは、最低限のセキュリティでコンテンツ、コード、およびアドインを読み込むことができます。また、ユーザーにアクセス許可のプロンプトが表示されることもありません。 このポリシー設定を無効にした場合、選択したアプリケーションでは、セキュリティ センターの [信頼できる場所] セクションの一覧にあるネットワーク上のすべての場所が無視されます。 |

#### ユーザーの構成]>[管理用テンプレート]>[Microsoft Excel 2016]>[Excelオプション]>[セキュリティ]>[セキュリティセンター]>[保護ビュー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Outlook から開かれた添付ファイルで保護ビューをオフにする | 無効 | このポリシー設定では、Outlook に添付された Excel ファイルを保護ビューで開くかどうかを指定できます。 このポリシー設定を有効にした場合、Outlook の添付ファイルは、保護ビューでは開かれません。 このポリシー設定を無効にするか、未構成にした場合、Outlook の添付ファイルは、保護ビューで開かれます。 |
| インターネット ゾーンからダウンロードされたファイルを保護ビューで開かない | 無効 | このポリシー設定を無効にするか、未構成にした場合、インターネット ゾーンからダウンロードされたファイルは、保護ビューで開かれます。 |
| ファイルの検証に失敗した場合のドキュメントの処理の設定 | 無効 | このポリシー設定では、ファイル検証が失敗した場合のドキュメントの処理方法を指定できます。 このポリシー設定を無効にした場合、[ファイルを保護ビューで開く (編集不可)] の処理が適用されます。 このポリシー設定を構成しなかった場合、[ファイルを保護ビューで開く (編集可)] の処理が適用されます。 |
| ローカル イントラネット UNC 上のファイルを保護ビューで開く | 有効 | このポリシー設定を有効にした場合、ローカル イントラネット UNC ファイル共有にあるファイルの UNC パスがインターネット ゾーン内であると考えられれば、ファイルは保護ビューで開かれます。 このポリシー設定を無効にするか、または未構成にした場合、UNC パスがインターネット ゾーン内であると考えられても、ローカル イントラネット UNC ファイル共有上のファイルは、保護ビューで開かれません。 |
| 安全でない可能性のある場所にあるファイルを保護ビューで開かない | 無効 | このポリシー設定では、安全でない可能性のある場所にあるファイルを、保護ビューで開くかどうかを指定できます。安全でない可能性のある場所を指定していない場合は、[ダウンロードしたプログラム ファイル] と [インターネット一時ファイル] フォルダーのみが、安全でない可能性のある場所と見なされます。 このポリシー設定を有効にした場合、安全でない可能性のある場所にあるファイルは、保護ビューでは開かれません。 このポリシー設定を無効にするか、未構成にした場合、安全でない可能性のある場所にあるファイルは、保護ビューで開かれます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Excel 2016]>[Excelオプション]>[保存]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 既定のファイル形式 | 有効 Excel ブック(\*.xlsx) | このポリシー設定では、Excel でブックを保存するときの既定のファイル形式を指定します。このポリシー設定を有効にした場合、以下のオプションから Excel で使用する既定のファイル形式を設定できます。- Excel ブック (.xlsx)。このオプションは、Excel 2016 の既定の構成です。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Excel 2016]>[データの回復]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 破損したブックを開くときにデータ抽出オプションを表示しない | 有効 | このポリシー設定では、ユーザーが修復または抽出モードで破損したブックを開くときに、[開いて修復] 操作に先立ってデータ抽出オプションの一覧を表示するかどうかを指定します。 このポリシー設定を有効にした場合、Safe Load 処理によってファイルが開き、データの修復または抽出を選択するためのメッセージは表示されません。 このポリシー設定を無効にするか、未構成にした場合、データを修復するかまたは抽出するかを確認するメッセージと、値に変換するかまたは数式を回復するかを確認するメッセージが表示されます。 |

### ・L1 Word 2016

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Word 2016]>[Wordオプション]>[セキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ファイル検証機能をオフにする | 無効 | このポリシー設定を有効にした場合、ファイル検証機能はオフになります。 このポリシー設定を無効にするか、未構成にした場合、ファイル検証機能はオンになります。Office バイナリ ドキュメント (97-2003) は、開かれる前に、ファイル形式のスキーマに準拠しているかどうかが確認されます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Word 2016]>[Wordオプション]>[セキュリティ]>[セキュリティセンター]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| VBA マクロ通知 | 有効 通知してすべてを無効にする | Visual Basic for Applications (VBA) マクロが存在する場合に、指定したアプリケーションでユーザーに警告を表示する方法を指定します。- [通知してすべてを無効にする]: 署名の有無にかかわらず、すべてのマクロについてセキュリティ バーを表示します。このオプションでは、Office の既定の構成が適用されます。- [デジタル署名付きのマクロを除くすべてのマクロを無効にする]: デジタル署名付きのマクロについてセキュリティ バーで警告を表示します。ユーザーはこのマクロを有効にするか、または無効のままにできます。署名のないマクロは無効になり、ユーザーには通知されません。- [通知せずにすべてを無効にする]: 署名の有無にかかわらず、すべてのマクロを無効にします。ユーザーには通知されません。- [すべてのマクロを有効にする] (推奨しません): 署名の有無にかかわらず、すべてのマクロを有効にします。このオプションを選んだ場合、危険なコードの実行が検出されなくなるため、セキュリティが大幅に低下します。このポリシー設定を無効にした場合、[通知せずにすべてを無効にする] が既定の設定になります。このポリシー設定を未構成にした場合、指定したアプリケーションで VBA マクロを含むファイルを開くときに、このファイルはマクロが無効にされた状態で開きます。このとき、マクロが存在しており、無効にされたことを示すセキュリティ バーの警告が表示されます。ユーザーは必要に応じてファイルを検査して編集できますが、無効化された機能を使うことはできません。これらの機能を使うには、セキュリティ バーで [コンテンツを有効にする] をクリックして機能を有効にする必要があります。ユーザーが [コンテンツを有効にする] をクリックすると、ドキュメントは信頼済みのドキュメントとして追加されます。重要: [デジタル署名付きのマクロを除くすべてのマクロを無効にする] を選んだ場合、署名のない Access データベースを開くことができなくなります。 |
| Visual Basicプロジェクトへのアクセスを信頼 | 無効 | このポリシー設定を無効にした場合、VSTO から VBA プロジェクトへのプログラムによるアクセスができなくなります。また、[VBA プロジェクト オブジェクト モデルへのアクセスを信頼する] チェック ボックスがオフになり、ユーザーはこの設定を変更できません。注意: このポリシー設定を無効にすると、VSTO プロジェクトと、指定したアプリケーションの VBA プロジェクト システムのやり取りが正常に行われなくなります。 |
| Word Open XML 文書内の暗号化されたマクロをスキャンする | 無効 | このポリシー設定では、Open XML 文書内の暗号化されたマクロについて、開く前にウイルス対策ソフトウェアによるスキャンが必要かどうかを指定することができます。- [暗号化されたマクロをスキャンする]: ウイルス対策ソフトウェアがインストールされていない限り、暗号化されたマクロは無効になります。マクロが含まれている暗号化されたブックを開くときに、暗号化されたマクロがウイルス対策ソフトウェアでスキャンされます。- [ウイルス対策ソフトウェアが利用できる場合はスキャンする]: ウイルス対策ソフトウェアがインストールされている場合、暗号化されたマクロは読み込まれる前にスキャンされます。ウイルス対策ソフトウェアが利用できない場合、暗号化されたマクロの読み込みを許可します。- [スキャンせずにマクロを読み込む]: ウイルス対策ソフトウェアの確認を行わず、暗号化されたファイル内のマクロの読み込みを許可します。このポリシー設定を無効にするか、未構成にした場合、[暗号化されたマクロをスキャンする] オプションを選択した場合と同じ動作になります。 |
| アプリケーション アドインには信頼できる発行元による署名が必要 | 有効 | このポリシー設定を有効にした場合、このアプリケーションで各アドインを読み込む前に、デジタル署名がチェックされます。アドインがデジタル署名されていないか、または信頼できる発行元による署名でない場合、そのアドインは無効になり、ユーザーに通知されます。信頼できる発行元による署名がすべてのアドインで必要であると指定した場合は、信頼できる発行元の一覧に証明書を追加する必要があります。証明書の取得と配布について詳しくは、http://go.microsoft.com/fwlink/?LinkId=294922?をご覧ください。Office 2016 では、信頼できる発行元の証明書は Internet Explorer の信頼できる発行元ストアに格納されます。以前のバージョンの Microsoft Office では、信頼できる発行元の証明書情報 (特に、証明書の拇印) は、Office の特別な信頼できる発行元ストアに格納されていました。Office 2016 でも引き続き Office の信頼できる発行元ストアから証明書情報を読み取りますが、このストアに情報を書き込むことはありません。したがって、以前のバージョンの Office で信頼できる発行元の一覧を作成した後で Office 2016 にアップグレードした場合、その一覧は引き続き認識されます。ただし、信頼できる発行元の証明書を一覧に追加した場合、その情報は Internet Explorer の信頼できる発行元ストアに格納されます。信頼できる発行元の詳細については、Office Resource Kit を参照してください。 |
| インターネットから取得した Office ファイル内のマクロの実行をブロックします | 有効 | このポリシー設定を有効にした場合、セキュリティ センターの [マクロの設定] セクションで [すべてのマクロを有効にする] がオンになっている場合でも、マクロの実行はブロックされます。また、[コンテンツの有効] の選択肢が表示されないで、マクロの実行がブロックされたことを示す通知が表示されます。Office ファイルが信頼できる場所に保存されている場合、または以前にユーザーが信頼した場合は、マクロを実行できます。このポリシーを無効にした場合、または構成していない場合は、セキュリティ センターの [マクロの設定] セクションで構成された設定で、インターネットから取得された Office ファイル内のマクロが実行されるかどうかが決まります。 |
| 署名されていないアプリケーション アドインに関するセキュリティ バーの通知を無効にして、ブロックする | 有効 | このポリシー設定では、指定した Office アプリケーションで、署名のないアプリケーション アドインが読み込まれたときにユーザーに通知するか、またはユーザーに通知せずに自動的に無効にするかを指定します。このポリシー設定は、[アプリケーション アドインには信頼できる発行元による署名が必要] ポリシー設定を有効にした場合にのみ適用されます。このポリシー設定を有効にすると、ユーザーは設定を変更できなくなります。このポリシー設定を有効にした場合、署名のないアドインはユーザーに通知することなく自動的に無効になります。このポリシー設定を無効にした場合、すべてのアドインに信頼できる発行元による署名が必要であるようにアプリケーションが構成されると、アプリケーションによって読み込まれた署名のないアドインはすべて無効になり、アクティブ ウィンドウの上部にセキュリティ バーが表示されます。セキュリティ バーには、署名のないアドインについてユーザーに通知するメッセージが表示されます。このポリシー設定を未構成にした場合、[動作を無効にする] が適用され、またユーザーは、アプリケーションのセキュリティ センターの [アドイン] カテゴリでこの要件を構成できます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Word 2016]>[Wordオプション]>[セキュリティ]>[セキュリティセンター]>[ファイル制限機能の設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Word 2 またはそれ以前のバージョンのバイナリ文書とテンプレート | 有効開く/保存をブロックする(オープンポリシーを使用） | - [開く/保存をブロックする (オープン ポリシーを使用)]: この種類のファイルを開く操作と保存する操作がブロックされます。ファイルは [ファイル制限機能の既定動作] キーで構成されたポリシー設定に基づいて開きます。このポリシー設定を無効にするか、未構成にした場合、この種類のファイルはブロックされません。 |
| Word 6.0 バイナリ文書とテンプレート |
| Word 95 バイナリ文書とテンプレート | 編集を許可し、保護ビューで開く | - [保護されたビューで開く (編集可)]: この種類のファイルを開く操作と保存する操作がブロックされ、編集のためのオプションが有効になります。このポリシー設定を無効にするか、未構成にした場合、この種類のファイルはブロックされません。 |
| Word 97 バイナリ文書とテンプレート |
| Word XP バイナリ文書とテンプレート |
| Word 2000 バイナリ文書とテンプレート |
| ファイル制限機能の既定動作の設定 | 無効 | このポリシー設定では、ユーザーが Word ファイルを開き、表示または編集することができるかどうかを指定できます。このポリシー設定を有効にした場合、以下のオプションのいずれかを設定できます。- ブロックされたファイルは開くことができない- ブロックされたファイルは保護ビューで開く (編集不可)- ブロックされたファイルは保護ビューで開く (編集可)このポリシー設定を無効にするか、未構成にした場合、[ブロックされたファイルは開くことができない] オプションの設定と同じ動作になります。ユーザーがブロックされたファイルを開くことはできません。 |

#### [ユーザーの構成]>[セキュリティ]>[セキュリティセンター]>[信頼できる場所]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| すべての信頼できる場所を無効にする | 有効 | このポリシー設定では、管理者は指定したアプリケーションで、すべての信頼できる場所を無効にできます。セキュリティ センターで指定する信頼できる場所は、安全と見なすことができるファイル保存場所を定義するために使用します。信頼できる場所からは、最低限のセキュリティでコンテンツ、コード、およびアドインを読み込むことができます。また、ユーザーにアクセス許可のプロンプトが表示されることもありません。信頼できる場所から危険なファイルが開かれた場合、標準のセキュリティ対策の対象とはならないため、ユーザーのコンピューターやデータに損害を与える可能性があります。このポリシー設定を有効にした場合、指定したアプリケーションで、すべての信頼できる場所 (セキュリティ センターで指定) が無視されます。これらの信頼できる場所には、セットアップ中に Office 2016 で設定されたもの、グループ ポリシーを使用してユーザーに展開されたもの、およびユーザー自身が追加したものが含まれます。信頼できる場所からファイルを開くときにはプロンプトが再び表示されます。このポリシー設定を無効にするか、未構成にした場合、指定したアプリケーションで、すべての信頼できる場所 (セキュリティ センターで指定) が安全と見なされます。 |
| ネットワーク上の信頼できる場所を許可する | 無効 | このポリシー設定を有効にした場合、ユーザーは、セキュリティ センターの [信頼できる場所] セクションにある [新しい場所の追加] ボタンをクリックすることによって、ネットワーク共有または直接の管理下にない別のリモートの場所にある信頼できる場所を指定できます。信頼できる場所からは、最低限のセキュリティでコンテンツ、コード、およびアドインを読み込むことができます。また、ユーザーにアクセス許可のプロンプトが表示されることもありません。このポリシー設定を無効にした場合、選択したアプリケーションでは、セキュリティ センターの [信頼できる場所] セクションの一覧にあるネットワーク上のすべての場所が無視されます。また、グループ ポリシーを使用して [信頼できる場所] を展開する場合は、これらの場所がリモートの場所かどうかを確認する必要があります。リモートの場所が存在しているが、このポリシー設定でリモートの場所を許可しない場合、リモートの場所を指すポリシー キーはクライアント コンピューターで無視されます。このポリシー設定を無効にしても、ネットワークの場所は [信頼できる場所] の一覧から削除されませんが、ユーザーが [信頼できる場所] の一覧にネットワークの場所を追加する場合に混乱を招く可能性があります。また、セキュリティ センターの [信頼できる場所] の一覧に新しいネットワークの場所を追加できません。[プライベート ネットワーク上にある信頼できる場所を許可する (推奨しません)] チェック ボックスのテキストが示すように、このポリシー設定を有効にすることは推奨されていないため、実際にはこのポリシー設定を無効にしても、ユーザーの利便性に大きな問題が起こることはほとんどありません。このポリシーを有効にしなかった場合、ユーザーは必要に応じて [プライベート ネットワーク上にある信頼できる場所を許可する (推奨しません)] チェック ボックスを選択し、[新しい場所の追加] ボタンをクリックすることにより、信頼できる場所を指定することができます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Word 2016]>[Wordオプション]>[セキュリティ]>[セキュリティセンター]>[保護ビュー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Outlook から開かれた添付ファイルで保護ビューをオフにする | 無効 | このポリシー設定を有効にした場合、Outlook の添付ファイルは、保護ビューでは開かれません。このポリシー設定を無効にするか、未構成にした場合、Outlook の添付ファイルは、保護ビューで開かれます。 |
| インターネットゾーンからダウンロードされたファイルを保護ビューで開かない | 無効 | このポリシー設定を有効にした場合、インターネット ゾーンからダウンロードされたファイルは、保護ビューでは開かれません。このポリシー設定を無効にするか、未構成にした場合、インターネット ゾーンからダウンロードされたファイルは、保護ビューで開かれます。 |
| ファイル検証に失敗した場合のドキュメントの処理の設定 | 無効 | このポリシー設定を有効にした場合、ファイル検証に失敗したファイルに対する次のオプションを構成できます。- ファイルを完全にブロックする: ユーザーはファイルを開くことができません。- ファイルを保護ビューで開く (編集不可): ユーザーはファイルを編集できません。このポリシー設定を無効にした場合も、この方法でファイルが処理されます。- ファイルを保護ビューで開く (編集可): ユーザーはファイルを編集することができます。このポリシー設定を構成しなかった場合も、この方法でファイルが処理されます。このポリシー設定を無効にした場合、[ファイルを保護ビューで開く (編集不可)] の処理が適用されます。このポリシー設定を構成しなかった場合、[ファイルを保護ビューで開く (編集可)] の処理が適用されます。 |
| ローカルイントラネット UNC 上のファイルを保護ビューで開く | 有効 | このポリシー設定を有効にした場合、ローカル イントラネット UNC ファイル共有にあるファイルの UNC パスがインターネット ゾーン内であると考えられれば、ファイルは保護ビューで開かれます。このポリシー設定を無効にするか、または未構成にした場合、UNC パスがインターネット ゾーン内であると考えられても、ローカル イントラネット UNC ファイル共有上のファイルは、保護ビューで開かれません。 |
| 安全でない可能性のある場所にあるファイルを保護ビューで開かない | 無効 | このポリシー設定では、安全でない可能性のある場所にあるファイルを、保護ビューで開くかどうかを指定できます。安全でない可能性のある場所を指定していない場合は、[ダウンロードしたプログラム ファイル] と [インターネット一時ファイル] フォルダーのみが、安全でない可能性のある場所と見なされます。このポリシー設定を有効にした場合、安全でない可能性のある場所にあるファイルは、保護ビューでは開かれません。このポリシー設定を無効にするか、未構成にした場合、安全でない可能性のある場所にあるファイルは、保護ビューで開かれます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Word 2016]>[Wordオプション]>[詳細設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 文書を開いたときにリンクを自動的に更新する | 無効 | ユーザーがドキュメントを開くと、Wordはグラフィック、Excelワークシート、PowerPointスライドなどの外部コンテンツへのリンクを自動的に更新します。ドキュメントが開いているときにWordが自動的にリンクを更新するように構成されている場合、ユーザーの知らないうちにドキュメントの内容が変更される可能性があり、重要な情報が危険にさらされる可能性があります。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Word 2016]>[Wordオプション]>[保存]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 既定のファイル形式 | 有効 Word 文書(\*.docx) | [Word 文書 (\*.docx)]: このオプションは、Word の既定の構成です。 |

### ・L1 Outlook 2016

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[Outlook のオプション]>[その他]>[詳細設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| パブリックフォルダーに対する Outlook オブジェクト モデル スクリプトの実行を許可しない | 有効 | ユーザー設定フォームまたはフォルダーのホーム ページに関連付けられている、共有フォルダー用のスクリプトを Outlook で実行するかどうかを指定します。このポリシー設定を有効にした場合、Outlook では、共有フォルダーに関連付けられているスクリプトを実行できません。この設定は、ユーザーのコンピューター上のどの構成変更よりも優先されます。このポリシー設定を無効にした場合、ユーザー設定フォームまたはフォルダーのホーム ページに関連付けられている、共有フォルダー用の任意のスクリプトが Outlook で自動的に実行されます。このポリシー設定を未構成にした場合、このポリシーを [有効] に設定した場合と同じ動作になります。 |
| 共有フォルダーに対する Outlook オブジェクト モデル スクリプトの実行を許可しない | 有効 | ユーザー設定フォームまたはフォルダーのホーム ページに関連付けられている、共有フォルダー用のスクリプトを Outlook で実行するかどうかを指定します。このポリシー設定を有効にした場合、Outlook では、共有フォルダーに関連付けられているスクリプトを実行できません。この設定は、ユーザーのコンピューター上のどの構成変更よりも優先されます。このポリシー設定を無効にした場合、ユーザー設定フォームまたはフォルダーのホーム ページに関連付けられている、共有フォルダー用の任意のスクリプトが Outlook で自動的に実行されます。このポリシー設定を未構成にした場合、このポリシーを [有効] に設定した場合と同じ動作になります。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[Outlook のオプション]>[ユーザー設定]>[予定表オプション]>[Office.com 共有サービス]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| DAV サーバーに予定表を公開できないようにする | 有効 | このポリシー設定では、Outlook ユーザーが DAV サーバーに公開できるかどうかを指定します。このポリシー設定を有効にした場合、Outlook ユーザーは 予定表を DAV サーバーに公開できません。このポリシー設定を無効にするか、未構成にした場合、Outlook ユーザーは、WebDAV (Web 分散オーサリングとバージョン管理) プロトコルをサポートするサーバーに予定表を公開して、他のユーザーと予定表を共有することができます。 |
| Offiece.com に予定表を公開できないようにする | 有効 | このポリシー設定では、Outlook ユーザーが Office.com 予定表共有サービスに予定表を公開できるかどうかを指定します。このポリシー設定を有効にした場合、Outlook ユーザーは Office.com に予定表を公開できません。このポリシー設定を無効にするか、未構成にした場合、Outlook ユーザーは Microsoft Outlook 予定表共有サービスに予定表を公開して、選択した他のユーザーと予定表を共有することができます。ユーザーは、予定表を表示できるユーザー、および表示できる詳細レベルを指定できます。 |
| ユーザーが公開できる予定表の詳細情報のレベルを制限する | 有効[完全な詳細情報] および [詳細情報の一部] を無効にする | このポリシー設定では、Outlook ユーザーが Microsoft Outlook 予定表共有サービスに公開する予定表の詳細レベルを指定します。このポリシー設定を有効にした場合、以下の 3 つの詳細レベルから選択できます。\* [すべてのオプションを使用可能にする] - この詳細レベルが既定の構成です。\* [[完全な詳細情報] を無効にする]\* [[完全な詳細情報] および [詳細情報の一部] を無効にする]このポリシー設定を無効にするか、未構成にした場合、Outlook ユーザーは、予定表を Microsoft Outlook 予定表共有サービスに公開して、選択した他のユーザーと予定表を共有できます。ユーザーは、以下の 3 つの詳細レベルから選択できます。\* [空き時間情報のみ] - 許可されている訪問者は、[空き時間]、[予定あり]、[仮の予定]、または [外出中] に設定されているユーザーの予定を確認できますが、予定表アイテムの件名や詳細を表示することはできません。\* [詳細情報の一部] - 許可されている訪問者は、ユーザーの空き情報および予定表アイテムの件名のみを確認できます。予定表アイテムの詳細を表示することはできません。ユーザーは、訪問者に非公開アイテムの存在を表示することもできます。\* [完全な詳細情報] - 許可されている訪問者は、予定表アイテムの完全な詳細を確認できます。ユーザーは、訪問者に非公開アイテムの存在を表示することもできます。 |
| 公開予定表へのアクセス | 有効 | このポリシー設定では、Office.com またはサード パーティの WebDAV (Web 分散オーサリングとバージョン管理) サーバーに予定表を公開するユーザーに適用する制限を指定します。このポリシー設定を有効または無効にした場合、Office.com に公開される予定表へのアクセスが制限され (予定表の所有者/公開者以外のユーザーは、予定表の所有者から招待状を受け取っている場合にのみその予定表を表示できます)、ユーザーは自分の予定表をサード パーティの DAV サーバーに公開できません。このポリシー設定を未構成にした場合、ユーザーは、Office.com 予定表共有サービスや、WebDAV プロトコルをサポートするサーバーに予定表を公開することによって、他のユーザーと自分の予定表を共有できます。Office.com では、ユーザーは招待した他のユーザーのアクセスを制限するか、または予定表にアクセスするための URL を知っているすべてのユーザーに制限のないアクセスを許可するかを選択できます。DAV へのアクセスは、サーバーとフォルダーへのアクセス許可を使用してのみ制限することができ、セットアップと保守を行うためにサーバー管理者の支援が必要となる場合があります。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[アカウントの設定]>[Exchange]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Exchange サーバーでの認証方式 | 有効 Kerberos パスワード認証 スマートカードを挿入する | このポリシー設定では、Microsoft Exchange Server を認証する場合に Outlook で使用する認証方法を指定します。注意 - Exchange Server では、Kerberos 認証プロトコルおよび NTLM が認証用としてサポートされています。Kerberos プロトコルはより安全な認証方法であり、Windows 2000 Server およびそれ以降のバージョンでサポートされています。NTLM 認証は、Windows 2000 よりも前の環境でサポートされています。このポリシー設定を有効にした場合、以下の 3 つのオプションから、Outlook での Microsoft Exchange Server の認証方法を選択できます。 - [Kerberos/NTLM パスワード認証]: Kerberos 認証プロトコルを使用した認証を行います。失敗した場合は、NTLM を使用した認証を行います。このオプションが既定の構成です。 - [Kerberos パスワード認証]: Kerberos プロトコルのみを使用して認証を行います。 - [NTLM パスワード認証]: NTLM のみを使用して認証を行います。このポリシー設定を無効にするか、未構成にした場合、Outlook では Kerberos 認証プロトコルを使用して認証を行います。Windows 2000 またはそれ以降のドメイン コントローラーがないため Kerberos 認証プロトコルを使用できない場合は、NTLM を使用して認証を行います。 |
| RPC 暗号化を有効する | 有効 | このポリシー設定では、Microsoft Exchange サーバーと通信するために Outlook でリモート プロシージャ コール (RPC) 暗号化を使用するかどうかを指定します。このポリシー設定を有効にした場合、Exchange サーバーとの通信時に Outlook で RPC 暗号化が使用されます。 注意: RPC 暗号化によって暗号化されるのは、Outlook クライアント コンピューターから Exchange サーバーへのデータのみです。メッセージがインターネットを移動するときに、メッセージ自体は暗号化されません。このポリシー設定を無効または未構成にした場合でも、既定で RPC 暗号化が使用されます。この設定を使用すると、対応するプロファイル単位の設定を上書きできます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[アカウントの設定]>[インターネット予定表]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| インターネット予定表を Outlook に統合しない | 有効 | このポリシー設定では、インターネット予定表を Outlook に統合するかどうかを指定します。Outlook のインターネット予定表機能によって、ユーザーは webcal:// プロトコルを使用して予定表をオンラインで公開することができ、他のユーザーが公開した予定表を購読できます。ユーザーがインターネット予定表を購読すると、Outlook では予定表への照会が定期的に行われ、投稿されたすべての変更内容がダウンロードされます。&brこのポリシー設定を有効にした場合、Outlook のすべてのインターネット予定表機能が無効になります。このポリシー設定を無効にするか、未構成にした場合、ユーザーはインターネット予定表を購読できます。 |
| 添付ファイルを自動的にダウンロードする | 無効 | このポリシー設定では、インターネット予定表の予定に添付されたファイルが Outlook でダウンロードされるかどうかを指定します。このポリシー設定を有効にした場合、Outlook では、インターネット予定表の予定に添付されたすべてのファイルがダウンロードされます。このポリシー設定を無効にするか、未構成にした場合、Outlook では、インターネット予定表の予定を取得するときに添付ファイルはダウンロードされません。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[アカウントの設定]>[RSS フィード]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 記事の全文を HTML 形式の添付ファイルとしてダウンロードする | 無効 | このポリシー設定を無効にするか、未構成にした場合、Outlook では、RSS アイテムのオフライン コピーが HTML 形式の添付ファイルとして自動的に作成されません。 |
| 添付ファイルを自動的にダウンロードする | 無効 | このポリシー設定を無効にするか、未構成にした場合、Outlook では、RSS アイテムの添付ファイルが既定でダウンロードされません。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ActiveX の 1回限りのフォームを許可する | 有効  Outlook のコントロールのみ読み込む | 既定では、サード パーティの ActiveX コントロールは Outlook の 1 回限りのフォームでは実行できません。これを、安全なコントロール (Microsoft Forms 2.0 のコントロールおよび Outlook の受信者/本文コントロール) を 1 回限りのフォームで実行できるように、またはすべての ActiveX コントロールを実行できるように変更することができます。 |
| アドインの信頼レベルを構成する | 有効  読み込まれた COM アドインと組み込み済みの COM アドインをすべて信頼する | 信頼された組み込み済みの COM アドインがすべて信頼されます。アドイン用の Exchange の設定が存在し、このオプションが選択されている場合、Exchange の設定が使用されます。 |
| インターネット 電子メール アカウントの [パスワードを保存する] を無効にする | 有効 | このオプションを使用すると、ユーザーがパスワードをコンピューターのレジストリにローカルで保存できる機能が非表示になります。このポリシーを構成すると、[パスワードを保存する] チェック ボックスが非表示になるため、Outlook にパスワードを記憶させることができなくなります。Outlook では、POP3、IMAP、および HTTP の電子メール アカウントすべてがインターネット 電子メールアカウントと見なされます。電子メール アカウントのオプションは、ユーザーが [ツール] メニューの [アカウント設定] をクリックして、[電子メール] タブの [新規] をクリックすると [新しい電子メール アカウントの追加] ダイアログ ボックスに表示されます。 |
| 既定のセキュリティ設定を適用できない場合はユーザーに設定を選択させる | 無効 | オンにした場合、既定のセキュリティ設定を適用できないときに、ユーザーに設定を選択させます。オフにした場合、自動的に選択します。 |
| 添付ファイルのセキュリティ設定をユーザーが変更できないようにする | 有効 | このポリシー設定では、Outlook によってブロックされた添付ファイルの上書きを禁止します。このポリシー設定を有効にした場合、Outlook によってブロックされた添付ファイルの上書きが禁止されます。また、この設定が指定されている場合、"Level1Remove" レジストリ キーが確認されます。このポリシー設定を無効にするか、未構成にした場合、Outlook によってブロックされた添付ファイルの上書きがユーザーに許可されます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[暗号化]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| S/MIME の外部クライアントとの相互運用性: | 有効 内部で処理する | このポリシー設定では、暗号化されたメッセージを Outlook で復号化するか、外部プログラムに渡して処理するかを指定します。このポリシー設定を有効にした場合、S/MIME の外部クライアントを構成するためのオプションを次の 3 つから選択できます。- [内部で処理する]: Outlook ですべての S/MIME メッセージが復号化されます。- [外部で処理する]: すべての S/MIME メッセージが、構成された外部プログラムに渡されます。- [可能な場合は処理する]: Outlook ですべての S/MIME メッセージの復号化が試行されます。Outlook でメッセージを復号化できない場合、構成された外部プログラムにメッセージが渡されます。このオプションが既定の構成です。このポリシー設定を無効にするか、未構成にした場合、[可能な場合は処理する] を [有効] に設定した場合と同じ動作になります。 |
| S/MIME 確認メッセージ要求の処理 | 有効 S/MIME 確認メッセージを送信しない | このポリシー設定では、Outlook で S/MIME 確認メッセージ要求を処理する方法を指定します。このポリシー設定を有効にした場合、Outlook で S/MIME 確認メッセージ要求を処理する方法のオプションを次の 4 つから選択できます。- [確認メッセージを送信できない場合はメッセージを開く]- [確認メッセージを送信できない場合、メッセージを開かない]- [確認メッセージを送信する前に常に確認する]- [S/MIME 確認メッセージを送信しない]このポリシー設定を無効にするか、未構成にした場合、確認メッセージ要求が添付されているメッセージをユーザーが開くと、Outlook では、メッセージを開いたユーザーの ID とメッセージを開いた時刻に関する情報を含む確認メッセージを送信者に送信するかどうかを決定するためのメッセージが表示されます。Outlook で確認メッセージを送信できない場合でも、ユーザーはメッセージを開くことができます。 |
| すべての署名されたメッセージをクリア署名されたメッセージとして送信する | 有効 | このポリシー設定を有効にした場合、セキュリティ センターの [電子メールのセキュリティ] セクションにある [署名されたメッセージを送信する際は、クリア テキストで送信する] オプションがオンになります。注：これはOutlookのDefaultです。このポリシー設定を無効にするか、未構成にした場合、ユーザーが自分のデジタル署名を使用して電子メール メッセージに署名して送信する際に、Outlook ではその署名の秘密キーを使用してデジタル署名を暗号化します。ただし、メッセージを個別に暗号化しない限り、メッセージはクリア テキストで送信されます。 |
| メッセージ形式 | 有効S/MIME | このポリシー設定では、Outlook で使用できるメッセージの暗号化形式を指定します。Outlook では、メッセージの暗号化および署名用の形式として、S/MIME、Exchange、および Fortezza の 3 つがサポートされています。このポリシー設定を有効にした場合、Outlook で S/MIME (既定)、Exchange、または Fortezza の暗号化を使用できるかどうか、またはこれらのオプションの任意の組み合わせを使用できるかどうかを指定できます。ユーザーがこの構成を変更することはできません。このポリシー設定を無効にするか、未構成にした場合、Outlook は S/MIME のみを使用してメッセージの暗号化および署名を行います。このポリシー設定を未構成にした場合、ユーザーがこの構成を変更することはできません。 |
| 最小暗号化設定 | 有効最小キー サイズ(ビット)168 | このポリシー設定では、暗号化メールのキーの最小の長さを指定します。このポリシー設定を有効にした場合、暗号化メールのキーの最小の長さを設定できます。ユーザーがメールを送信する際に、使用している暗号化キーの長さが設定した最小暗号化キー値より短い場合、警告ダイアログが表示されます。ただし、ユーザーは警告を無視して、当初に選択した暗号化キーを使用してメールを送信できます。このポリシー設定を無効にするか、未構成にした場合、ユーザーが暗号化を使用してメールを送信する際に警告が表示されます。ユーザーは警告を無視して当初に選択した暗号化キーを使用してメールを送信できます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[暗号化]>[署名の状況ダイアログボックス]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| CRL （証明書取り消し一覧）の取得 | 有効オンラインの場合は常に CRL を取得する | このポリシー設定では、証明書の有効性を検証するために Outlook で証明取り消し一覧を取得する方法を指定します。証明取り消し一覧 (CRL) は、デジタル証明書の管理元である証明機関 (CA) によって取り消されたデジタル証明書の一覧です。通常は、証明書の発行が不適切である場合や、関連付けられている秘密キーが侵害された場合に取り消されます。このポリシー設定を有効にした場合、以下の 3 つのオプションから、Outlook で CRL を使用する方法を選択できます。- [既定のシステム設定を使用する]: オペレーティング システムで構成されている CRL ダウンロード スケジュールを Outlook で使用します。- [オンラインになると自動的に CRL を取得する]: このオプションは、Outlook の既定の構成です。- [CRL を取得しない]: オンラインの場合であっても、Outlook で証明書の CRL がダウンロードされません。このオプションによって、セキュリティが低下する場合があります。このポリシー設定を無効にするか、未構成にした場合、Outlook では、CRL をダウンロードできる URL を含む証明書を処理しているときに Outlook がオンラインであれば、その URL から CRL が取得されます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[画像の自動ダウンロード設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| [画像の自動ダウンロード] のセーフゾーンにインターネットを含める | 無効 | このポリシー設定では、インターネット上の信頼できない差出人からの HTML 電子メール内の画像や外部コンテンツを、Outlook ユーザーが明示的にダウンロードを選択しなくてもダウンロードするかどうかを指定します。このポリシー設定を有効にした場合、インターネット経由で送信されたすべての電子メール メッセージの外部コンテンツが自動的にダウンロードされます。ユーザーはこの設定を変更できません。このポリシー設定を無効にするか、未構成にした場合、Outlook ではインターネットはセーフ ゾーンと見なされません。つまり、差出人が [信頼できる差出人のリスト] に含まれていない場合、外部サーバーのコンテンツは自動的にダウンロードされません。受信者は、メッセージごとに、信頼できない差出人からの外部コンテンツをダウンロードするかどうかを選択できます。 |
| 信頼済みゾーンをブロックする | 有効 | このポリシー設定を有効にした場合、Internet Explorer の [信頼済みサイト] ゾーン内の Web サイトのコンテンツは Outlook では自動的にダウンロードされません。受信者は、メッセージごとに外部コンテンツをダウンロードするかどうかを選択できます。このポリシー設定を無効にするか、未構成にした場合、Internet Explorer の [信頼済みサイト] ゾーン内の Web サイトからコンテンツが自動的にダウンロードされます。 |
| [信頼できる差出人のリスト] と [信頼できる宛先のリスト] に登録されエチルユーザーからのコンテンツを自動的にダウンロードする | 無効 | このポリシー設定では、[信頼できる差出人のリスト] または [信頼できる宛先のリスト] の差出人からの電子メールの外部コンテンツを Outlook で自動的にダウンロードするかどうかを指定します。このポリシー設定を有効にした場合、[信頼できる差出人のリスト] または [信頼できる宛先のリスト] に登録されている相手からの電子メールのコンテンツが Outlook で自動的にダウンロードされます。このポリシー設定を無効にした場合、ユーザーの [信頼できる差出人のリスト] または [信頼できる宛先のリスト] に登録されている相手から送信されたメッセージの外部コンテンツは Outlook で自動的にダウンロードされません。受信者は、メッセージごとに、外部コンテンツをダウンロードするかどうかを選択できます。このポリシー設定を未構成にした場合、ユーザーが自分の [信頼できる差出人のリスト] または [信頼できる宛先のリスト] に登録されている相手から電子メールを受信すると、ダウンロードが許可されます。 |
| HTML 形式の電子メールに含まれる画像および外部コンテンツを表示する | 有効 | このポリシー設定では、HTML 電子メール メッセージに含まれる信頼できない画像や外部コンテンツを、ユーザーが明示的にダウンロードを選択しなくても Outlook でダウンロードするかどうかを指定します。このポリシー設定を有効にした場合、差出人が [差出人セーフ リスト] に含まれていないと、Outlook では外部サーバーのコンテンツは自動的にダウンロードされません。受信者は、メッセージごとに、信頼できない差出人からの外部コンテンツをダウンロードするかどうかを選択できます。このポリシー設定を無効にした場合、HTML 電子メールの画像や外部コンテンツは表示されません。このポリシー設定を未構成にした場合、HTML 電子メールや RSS アイテムのコンテンツは、これらのコンテンツが安全であると見なされない限りダウンロードされません。以下のコンテンツは、Outlook で安全なコンテンツとして構成できます。- [差出人セーフ リスト] および [宛先セーフ リスト] で定義されている差出人からの電子メールおよび受信者への電子メールのコンテンツ。- Internet Explorer の [信頼済みサイト] セキュリティ ゾーンの Web サイトのコンテンツ。- RSS アイテムのコンテンツ。- SharePoint ディスカッション掲示板のコンテンツ。ユーザーは、セキュリティ センターの [自動ダウンロード] セクションのオプションを変更して、安全と見なすコンテンツを指定できます。Outlook の既定のブロック構成が上書きされると、セキュリティ センターに、または他の方法によって、すべての HTML 電子メール メッセージの外部コンテンツ (Web ビーコンを含む) が表示されます。 |
| セーフゾーンからのコンテンツのダウンロードを許可しない | 無効 | このポリシー設定では、Outlook でメッセージを表示するときに、セーフ ゾーンのコンテンツを自動的にダウンロードするかどうかを指定します。このポリシー設定を有効にした場合、セーフ ゾーンのコンテンツは自動的にダウンロードされます。このポリシー設定を無効にした場合、セーフ ゾーンのコンテンツは自動的にダウンロードされません。受信者は、メッセージごとに、信頼できない差出人からの外部コンテンツをダウンロードするかどうかを選択できます。このポリシー設定を構成しない場合、Internet Explorer の [インターネット オプション] ダイアログ ボックスの [セキュリティ] タブの定義に基づいて "安全" と見なされるサイトのコンテンツは自動的にダウンロードされます。重要 - このポリシー設定は逆方向に作用することに注意してください。名前とは逆に、このポリシー設定を無効にするとセーフ ゾーンのコンテンツはダウンロードされず、有効にするとダウンロードされます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[セキュリティセンター]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| フィッシング詐欺の疑いがある電子メール メッセージのハイパーリンクを有効にする | 無効 | このポリシー設定では、フィッシング詐欺の疑いのある電子メール メッセージのハイパーリンクを Outlook で有効にするかどうかを指定します。 このポリシー設定を有効にした場合、Outlook では、フィッシング詐欺の疑いがあり迷惑メールにも分類されていないメッセージのハイパーリンクが有効になります。 このポリシー設定を無効にするか、未構成にした場合、Outlook では、迷惑メールとして分類されなくても、フィッシング詐欺の疑いがあるメッセージのハイパーリンクは無効になります。 |
| マクロのセキュリティ設定 | 有効署名されている場合は警告を表示し、署名されていない場合は無効にする | - [署名されている場合は警告を表示し、署名されていない場合は無効にする]: このオプションは、セキュリティ センターの [署名されたマクロに対しては警告を表示し、署名されていないマクロはすべて無効にする] オプションに対応しています。マクロは以下のように扱われます。 - マクロの発行元が信頼されており、その信頼できる発行元によってマクロにデジタル署名が適用されている場合は、マクロを実行できます。 - マクロに発行元によって有効な署名が適用されているが、その発行元が信頼されていない場合、そのマクロのセキュリティに関する警告ダイアログ ボックスが開きます。 ユーザーはこのダイアログ ボックスで、現在のセッションでマクロを有効にするか、現在のセッションでマクロを無効にするか、または今後メッセージを表示せずにマクロを実行できるようにこの発行元を信頼できる発行元の一覧に追加するかを選択できます。- 有効な署名が適用されていないマクロは、信頼できる場所から開いた場合を除き、メッセージを表示せずに無効になります。このオプションは、Outlook の既定の構成です。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[セキュリティ フォーム設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| outlook セキュリティ モード | 有効Outlook セキュリティのグループポリシーを使用する | このポリシー設定では、Outlook で適用されるセキュリティ設定を指定します。このポリシー設定を有効にした場合、Outlook のセキュリティ設定を適用するオプションを、以下の 4 つから選択できます。\* [Outlook の既定のセキュリティ] - このオプションは、Outlook の既定の構成です。ユーザーはセキュリティを自分で構成でき、グループ ポリシーで構成されたセキュリティ関連の設定は無視されます。\* [[Outlook Security Settings] パブリック フォルダーのセキュリティ フォームを使用する] - 指定したパブリック フォルダーに発行されているセキュリティ フォームの設定が使用されます。\* [[Outlook 10 Security Settings] パブリック フォルダーのセキュリティ フォームを使用する] - 指定したパブリック フォルダーに発行されているセキュリティ フォームの設定が使用されます。\* [Outlook セキュリティのグループ ポリシーを使用する] - グループ ポリシーのセキュリティ設定が使用されます。重要 - このガイドで説明されているその他の Outlook セキュリティ ポリシー設定を適用する場合は、このポリシー設定を有効にする必要があります。このポリシー設定を無効にするか、未構成にした場合、Outlook ユーザーはセキュリティを自分で構成でき、グループ ポリシーで構成されたセキュリティ関連の設定は無視されます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[セキュリティ フォーム設定]>[ユーザー設定フォームのセキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 1回限りの Outlook フォームでのスクリプトの使用を許可する | 無効 | このポリシー設定を有効にした場合、スクリプトは 1 回限りの Outlook フォームで実行できます。このポリシー設定を無効にするか、未構成にした場合、メッセージにスクリプトとレイアウトが含まれているフォームでは、スクリプトは実行されません。重要: このポリシー設定は、[Microsoft Outlook 2016]\[セキュリティ]\[セキュリティ フォーム設定] にある [Outlook セキュリティ モード] ポリシー設定が [Outlook セキュリティのグループ ポリシーを使用する] に構成されている場合にのみ適用されます。 |
| Outlook オブジェクト モデルのユーザー設定アクションの実行確認について設定する | 有効自動的に拒否する | このポリシー設定では、ユーザー設定のアクションを実行する前に、Outlook でメッセージを表示するかどうかを指定します。ユーザー設定のアクションによって、ルールの一部としてトリガーできる機能が Outlook に追加されます。ユーザー設定のアクションにはさまざまな機能がありますが、メッセージの返信時に、Outlook モデルのプログラム的な送信に対する保護を解除するアクションを作成できます。このポリシー設定を有効にした場合、Outlook オブジェクト モデルを使用するユーザー設定のアクションを実行するときの Outlook の動作を指定するオプションを、以下の 4 つから選択できます。\* [ユーザーに確認する]\* [自動的に許可する]\* [自動的に拒否する]\* [コンピューターのセキュリティに基づいてユーザーにメッセージを表示する]: このオプションでは、Outlook の既定の構成が適用されます。このポリシー設定を無効にするか、未構成にした場合、Outlook または別のプログラムが Outlook オブジェクト モデルを使用してユーザー設定のアクションを開始すると、そのアクションを許可するか拒否するかを確認するメッセージが表示されます。この構成を変更した場合、悪意のあるコードで Outlook オブジェクト モデルを使用できるため、重要な情報が脅かされたり、データやコンピューティング リソースが危険にさらされる可能性があります。これは、[コンピューターのセキュリティに基づいてユーザーにメッセージを表示する] を [有効] に設定した場合と同じ動作になります。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[セキュリティ フォーム設定]>[プログラムによるセキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| [名前を付けて保存] を実行するときの Outlook オブジェクト モデルに関する確認について構成する | 有効自動的に拒否する | このポリシー設定では、信頼できないプログラムが [名前を付けて保存] コマンドを使用して、プログラム的にアイテムを保存しようとしたときの動作を指定します。このポリシー設定を有効にした場合、信頼できないプログラムが [名前を付けて保存] コマンドを使用してプログラム的にアイテムを保存しようとしたときの動作を次の 4 つのオプションから選択できます。- [ユーザーに確認する] - アクセスが試みられるたびにユーザーに確認します。- [自動的に許可する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に許可します。このオプションは重大な脆弱性の原因となる可能性があるため、お勧めしません。- [自動的に拒否する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に拒否します。- [コンピューターのセキュリティに基づいてユーザーにメッセージを表示する] - ウイルス対策プログラムが最新ではないか、または実行されていない場合のみメッセージが表示されます。これが既定の構成です。このポリシー設定を無効にするか、未構成にした場合、信頼できないアプリケーションが [名前を付けて保存] コマンドを使用しようとしたときに、セキュリティ センターの [プログラムによるアクセス] セクションの設定に従って動作が決定されます。 |
| UserProperty オブジェクト の Formula プロパティにアクセスするときの Outlook オブジェクト モデルに関する確認について構成する | 有効自動的に拒否する | このポリシー設定では、ユーザーが Outlook でユーザー設定フォームをデザインし、アドレス情報フィールドをユーザー設定の組み合わせフィールドまたは式フィールドにバインドしようとしたときの動作を指定します。このポリシー設定を有効にした場合、信頼できないプログラムが Outlook オブジェクト モデルの UserProperties.Find メソッドを使用してアドレス情報にアクセスしようとしたときの動作を次の 4 つのオプションから選択できます。 - [ユーザーに確認する] - アクセスが試みられるたびにユーザーに確認します。 - [自動的に許可する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に許可します。このオプションは重大な脆弱性の原因となる可能性があるため、お勧めしません。 - [自動的に拒否する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に拒否します。 - [コンピューターのセキュリティに基づいてユーザーにメッセージを表示する] - ウイルス対策プログラムが最新ではないか、または実行されていない場合のみメッセージが表示されます。 このポリシー設定を無効にするか、未構成にした場合、ユーザーがアドレス情報フィールドをユーザー設定の組み合わせまたは式フィールドにバインドにようとしたときに、セキュリティ センターの [プログラムによるアクセス] セクションの設定に従って動作が決定されます。 |
| アドレス情報を読み込むときの Outlook オブジェクト モデルにあkンする確認について構成する | 有効自動的に拒否する | このポリシー設定では、信頼できないプログラムが Outlook オブジェクト モデルを使用して、[宛先] フィールドなどの受信者フィールドにアクセスしようとしたときの動作を指定できます。このポリシー設定を有効にした場合、信頼できないプログラムが Outlook オブジェクト モデルを使用して受信者フィールドにアクセスしようとしたときの動作を次の 4 つのオプションから選択できます。 - [ユーザーに確認する] - アクセスが試みられるたびにユーザーに確認します。 - [自動的に許可する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に許可します。 - [自動的に拒否する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に拒否します。 - [コンピューターのセキュリティに基づいてユーザーにメッセージを表示する] - ウイルス対策プログラムが最新ではないか、または実行されていない場合のみメッセージが表示されます。これが既定の構成です。 このポリシー設定を無効にするか、未構成にした場合、信頼できないアプリケーションが受信者フィールドにアクセスしようとしたときに、セキュリティ センターの [プログラムによるアクセス] の設定に従って動作が決定されます。 |
| メール送信時の Outlook オブジェクト モデルに関する確認について構成する | 有効自動的に拒否する | このポリシー設定では、信頼できないプログラムが Outlook オブジェクト モデルを使用してプログラムからメールを送信しようとしたときの動作を指定します。このポリシー設定を有効にした場合、信頼できないプログラムが Outlook オブジェクト モデルを使用してプログラムからメールを送信しようとしたときの動作を、次の 4 つのオプションから選択できます。 - [ユーザーに確認する] - アクセスが試みられるたびにユーザーに確認します。 - [自動的に許可する] - Outlook は、すべてのプログラムからのアクセス要求を自動的に許可します。このオプションは重大な脆弱性の原因となる可能性があるため、お勧めしません。 - [自動的に拒否する] - Outlook は、すべてのプログラムからのアクセス要求を自動的に拒否します。 - [コンピューターのセキュリティに基づいてユーザーにメッセージを表示する] - ウイルス対策プログラムが最新ではないか、または実行されていない場合のみメッセージが表示されます。 重要: このポリシー設定は、[Microsoft Outlook 2016\セキュリティ\セキュリティ フォーム設定] にある [Outlook セキュリティ モード] ポリシー設定が [Outlook セキュリティのグループ ポリシーを使用する] に構成されている場合のみ適用されます。このポリシー設定を無効にするか、未構成にした場合、信頼できないプログラムがメールを送信しようとしたときに、セキュリティ センターの [プログラムによるアクセス] セクションの設定に従って動作が決定されます。 |
| 会議出席依頼およびタスクの依頼に返信するときの Outlook オブジェクト モデルに関する確認について構成する | 有効自動的に拒否する | このポリシー設定では、信頼できないプログラムが、タスクの依頼または会議出席依頼の返信を使用してプログラム的に電子メールを送信しようとしたときの動作を指定します。このポリシー設定を有効にした場合、信頼できないプログラムがタスクの依頼または会議出席席依頼の返信を使用してプログラム的に電子メールを送信しようとしたときの動作を次の 4 つのオプションから選択できます。 - [ユーザーに確認する] - アクセスが試みられるたびにユーザーに確認します。 - [自動的に許可する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に許可します。このオプションは重大な脆弱性の原因となる可能性があるため、お勧めしません。 - [自動的に拒否する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に拒否します。 - [コンピューターのセキュリティに基づいてユーザーにメッセージを表示する] - ウイルス対策プログラムが最新ではないか、または実行されていない場合のみメッセージが表示されます。これが既定の構成です。 このポリシー設定を無効にするか、未構成にした場合、信頼できないプログラムがタスクの依頼または会議出席依頼にプログラム的に返信しようとしたときに、セキュリティ センターの [プログラムによるアクセス] セクションの設定に従って動作が決定されます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[セキュリティ フォーム設定]>[プログラムによるセキュリティ]>[信頼できるアドイン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 信頼できるアドインを構成する | 無効 | このポリシー設定では、Outlook のセキュリティ対策によって制限されることなく実行可能な、信頼できるアドインの一覧を指定できます。このポリシー設定を有効にした場合、信頼できるアドインとハッシュの一覧が使用できるようになり、エントリを追加および削除して変更できるようになります。この一覧は、既定では空です。新しいエントリを作成するには、[値の名前] 列に DLL ファイル名を、[値データ] 列にハッシュの結果を入力します。 このポリシー設定を無効にするか、未構成にした場合、信頼できるアドインの一覧は空になり、使用されないため、EC および SSLF の推奨設定ではユーザビリティの問題は発生しませんが、管理者がこの設定を有効にしてアドインを一覧に追加しない場合には、Outlook オブジェクト モデルにアクセスするアドインを使用しているユーザーに確認メッセージが繰り返し表示されることがあります。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[セキュリティ フォーム設定]>[添付ファイル セキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| レベル 1 のブロック対象であるファイル拡張子を削除する | 無効 | このポリシー設定では、Outlook で配信しない添付ファイルの種類を指定します (ファイルの拡張子で指定)。Outlook では、電子メール メッセージやその他のアイテムに添付されたファイルへのユーザーのアクセスを制限するために、2 つのレベルのセキュリティが使用されています。特定の拡張子を持つファイルは、レベル 1 (ユーザーはファイルを表示できない) またはレベル 2 (ユーザーはファイルをディスクに保存した後に開くことができる) に分類できます。レベル 1 とレベル 2 に分類されない種類のファイルは自由に開くことができます。このポリシー設定を有効にした場合、削除するファイルの種類の拡張子をテキスト フィールドにセミコロンで区切って入力することによって、この拡張子をレベル 1 に分類されるように指定し、配信をブロックできます。このポリシー設定を無効にするか、未構成にした場合、問題を起こす可能性があるいくつかのファイルの種類 (.exe、.reg、.vbs などの拡張子を持つファイル) はレベル 1 に分類され、これらの拡張子を持つファイルの配信がブロックされます。重要: このポリシー設定は、[Microsoft Outlook 2016]\[セキュリティ]\[セキュリティ フォーム設定] にある [Outlook セキュリティ モード] ポリシー設定が [Outlook セキュリティのグループ ポリシーを使用する] に構成されている場合にのみ適用されます。 |
| レベル 1 の添付ファイルを表示する | 無効 | このポリシー設定は、レベル 1 に指定されている潜在的に危険な添付ファイルを Outlook でブロックするかどうかを指定します。Outlook では、電子メール メッセージやその他のアイテムに添付されたファイルへのユーザーのアクセスを制限するために、2 つのレベルのセキュリティが使用されています。特定の拡張子を持つファイルは、レベル 1 (ユーザーはファイルを表示できない) またはレベル 2 (ユーザーはファイルをディスクに保存した後に開くことができる) に分類できます。レベル 1 とレベル 2 に分類されない種類のファイルは自由に開くことができます。このポリシーを有効にした場合、Outlook ユーザーは、添付ファイルをディスクに保存してから開くことで、レベル 1 の種類の添付ファイルにアクセスできます。レベル 2 の添付ファイルについても同様です。このポリシー設定を無効にした場合、レベル 1 の添付ファイルはどのような場合にも表示されることはありません。このポリシー設定が未構成の場合、Outlook ではレベル 1 の種類の添付ファイルへのアクセスを全面的に遮断し、ユーザーがレベル 2 のファイルを開くには、ディスクに保存する必要があります。 |
| レベル2のブロック対象であるファイル拡張子を削除する | 無効 | このポリシー設定では、ユーザーが開く前にディスクに保存しておく必要がある添付ファイルの種類を指定します (ファイルの拡張子で指定)。特定の拡張子を持つファイルは、レベル 1 (ユーザーはファイルを表示できない) またはレベル 2 (ユーザーはファイルをディスクに保存した後に開くことができる) に分類できます。レベル 1 とレベル 2 に分類されない種類のファイルは自由に開くことができます。このポリシー設定を有効にした場合、レベル 2 に分類される添付ファイルの種類の一覧を指定できます。ユーザーは、それらの種類の添付ファイルを表示するためにダウンロードするかどうかを決定する必要があります。このポリシー設定を無効にするか、未構成にした場合、Outlook ではどのファイルの種類の拡張子もレベル 2 に分類されません。重要: このポリシー設定は、[Microsoft Outlook 2016]\[セキュリティ]\[セキュリティ フォーム設定] にある [Outlook セキュリティ モード] ポリシー設定が [Outlook セキュリティのグループ ポリシーを使用する] に構成されている場合にのみ適用されます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]>[会議ワークスペース]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| サーバー リストへのユーザー入力を無効にする | 有効  既定の発行、他のユーザーを許可しない | このポリシー設定では、Outlook ユーザーが会議ワークスペースを作成するときに SharePoint サーバーのリストにエントリを追加できるかどうかを指定します。このポリシー設定を有効にした場合、以下の 2 つのオプションから、発行済みのサーバー リストに Outlook ユーザーがエントリを追加できるかどうかを指定できます。- [既定の発行、他のユーザーを許可する]: このオプションは、Outlook の既定の構成です。- [既定の発行、他のユーザーを許可しない]: このオプションを選択すると、ユーザーは発行済みの既定のサーバー リストにサーバーを追加できません。このポリシー設定を無効にするか、未構成にした場合、ユーザーは会議ワークスペースを作成した後、管理者から提供された既定のリストからサーバーを選択するか、またはリストにないサーバーのアドレスを手動で入力できます。これは、[既定の発行、他のユーザーを許可する] を [有効] に設定した場合と同じ動作になります。 |

### ・L1 OneDrive 2016

OneDrive の管理用テンプレートは、OneDriveがインストールされたクライアント PC の以下のフォルダーに保存されています。[[24]](#footnote-24)

%localappdata%\Microsoft\OneDrive\BuildNumber\adm\

#### [コンピュータの構成]>[管理用テンプレート]>[OneDrive]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ディスク領域が不足しているユーザーに警告する | 有効最小の空きディスク領域:500MB | この設定では、ディスクの空き領域の最小量を指定し、OneDrive 同期クライアント (OneDrive.exe) がファイルをダウンロードすると領域がこの量未満になるときに、ユーザーに通知することができます。ユーザーには、領域を解放するためのオプションが表示されます。 |
| ユーザーのディスクの空き領域が少ない場合にファイルのダウンロードをブロックする | 有効最小の空きディスク領域:200MB | この設定では、ディスクの空き領域の最小量を指定し、OneDrive の同期クライアント (OneDrive.exe) がユーザーがこの値より小さい場合、ファイルをダウンロードすることを禁止することができます。ユーザーは、領域を解放するためにオプションが要求されます。 |
| 大規模な削除操作ではユーザーの確認が必要 | 有効 | この設定により、ユーザーは多数の同期したファイルを削除したときに、クラウド内のファイルを削除することを確認します。この設定を有効にした場合、ユーザーは、多数の同期したファイルを削除するとき警告が表示常にします。ユーザーが 7 日以内の削除操作を確認しない場合、ファイルは削除されません。無効にした場合、またはこの設定を構成しなかった場合は、ユーザーは、警告を非表示にし、常に、クラウド内のファイルを削除できます。 |

#### [ユーザーの構成]>[管理用テンプレート]>[OneDrive]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ユーザーが個人用の OneDrive アカウントを同期できないようにする | 有効 | この設定は、ユーザーが Microsoft アカウントにサインインして個人用の OneDrive ファイルを同期できないようブロックすることができます。この設定を有効にすると、ユーザーは個人用 OneDrive アカウントで同期リレーションシップを設定できなくなります。この設定を有効にしたときに既に個人用 OneDrive アカウントを同期しているユーザーは、引き続き同期することはできなくなりますが (また同期が停止したメッセージが表示されます)、コンピューターと同期されたファイルはコンピューター上に残ります。この設定を無効にするか構成しない場合、ユーザーは個人用 OneDrive アカウントを同期できます。 |

### ・L1 Google Chrome

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Google]>[Google Chrome]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 3D グラフィックス API のサポートを無効にする | 有効 | この設定を有効にした場合、ウェブページはグラフィック処理ユニット（GPU）にアクセスできません。具体的には、ウェブページは WebGL API を使用できず、プラグインは Pepper 3D API を使用できません。この設定を無効または未設定にした場合、ウェブページは WebGL API を使用でき、プラグインは Pepper 3D API を使用できます。ただし、ブラウザのデフォルト設定により、これらの API を使用するにはコマンドライン引数を渡すことが必要になる可能性もあります。HardwareAcceleration&#x4D;odeEnabled が false の場合、Disable3DAPIs は無視されます。これは、Disable3DAPIs が true の場合と同じです。 |
| Chrome クリーンアップから Google へのデータ送信を管理する | 無効 | このポリシーが未設定の場合、Chrome クリーンアップで望ましくないソフトウェアが検出されると、SafeBrowsingUxtendedReportingEnabled で設定されているポリシーに基づいて、スキャンに関するメタデータのレポートが Google に送信される可能性があります。ユーザーは望ましくないソフトウェアをクリーンアップするかどうかを選択できます。また、望ましくないソフトウェアの検出精度を向上するために、クリーンアップの結果を Google と共有するかどうかも選択できます。これらの結果には、Chrome のプライバシー ホワイトペーパーで説明されているとおり、ファイルのメタデータのほか自動インストールされた拡張機能とレジストリキーが含まれます。このポリシーが無効な場合、Chrome クリーンアップで望ましくないソフトウェアが検出されても、スキャンに関するメタデータのレポートは Google に送信されません。この設定は、SafeBrowsingUxtendedReportingEnabled で設定されているポリシーよりも優先されます。ユーザーは望ましくないソフトウェアをクリーンアップするかどうかを選択できます。クリーンアップの結果は Google に送信されず、また送信するようユーザーが選択することもできません。このポリシーが有効な場合、Chrome クリーンアップで望ましくないソフトウェアが検出されると、SafeBrowsingUxtendedReportingEnabled で設定されているポリシーに基づいて、スキャンに関するメタデータのレポートが Google に送信される可能性があります。ユーザーは望ましくないソフトウェアをクリーンアップするかどうかを選択できます。クリーンアップの結果は Google に送信され、送信しないようユーザーが選択することはできません。このポリシーは、Microsoft Active Directory ドメインに追加した Windows インスタンス、またはデバイスの管理対象として登録した Windows 10 Pro あるいは Enterprise インスタンスでのみ使用できます。 |
| Google Chrome を閉じた際にバックグラウンド アプリの処理を続行する | 無効 | Google Chrome プロセスが OS ログインで開始してから最後のブラウザ ウィンドウが閉じるまで動作し続けているかどうかを判断し、バックグラウンド アプリや現在のブラウジング セッション（セッション Cookie を含む）がアクティブな状態を維持できるようにします。このポリシーを True に設定すると、バックグラウンド モードが有効になります。ユーザーがブラウザ設定で変更することはできません。このポリシーを False に設定すると、バックグラウンド モードが無効になります。ユーザーがブラウザ設定で変更することはできません。このポリシーが未設定の場合、バックグラウンド モードは最初は無効の状態です。ユーザーはブラウザ設定で変更することができます。 |
| Google サービスからの WebRTC イベントログの収集を許可する | 無効 | このポリシーが true に設定されている場合、Google Chrome に対して、Google サービス（Google Meet など）からの WebRTC イベントログの収集と、Google へのそれらのログのアップロードが許可されます。このポリシーが false に設定されている場合、Google Chrome によるログの収集とアップロードは行われません。ポリシーが未設定の場合、M76 以下では、Google Chrome によるログの収集とアップロードは行われません。ポリシーが未設定のとき、M77 以降では、ブラウザ プロフィールが管理対象とみなされる場合（プロフィールでクラウドレベルかマシンレベルのポリシーを受信し、子プロフィール、一時プロフィール、ログイン プロフィール、シークレット プロフィールでない場合）には Google Chrome によるログの収集とアップロードがデフォルトで行われます。これらのログには、送受信された RTP パケットの時間とサイズ、ネットワークの輻輳に関するフィードバック、音声および動画フレームの時間と品質に関するメタデータなど、Chrome での音声や動画の呼び出しに関する問題をデバッグする際に役立つ診断情報が含まれます。呼び出された音声や動画のコンテンツは含まれません。Chrome によるこのデータ収集は、Google のウェブサービス（Google ハングアウト、Google Meet など）からのみ行われます。Google は、これらのログと、Google サービス自体により収集される他のログとをセッション ID を使って関連付けることがあります。この関連付けは、デバッグを容易にする目的で行われます。 |
| Google とのデータの同期を無効にする | 有効 | Google でホストされる同期サービスを使用した Google Chrome でのデータ同期を無効にするとともに、ユーザーがこの設定を変更できないようにします。この設定を有効にした場合、ユーザーは Google Chrome でこの設定を変更したりオーバーライドしたりすることができなくなります。このポリシーを未設定のままにした場合、ユーザーは Google Sync を使用するかどうかを選択できます。Google Sync を完全に無効にするには、Google 管理コンソールで Google Sync サービスを無効にすることをおすすめします。RoamingProfileSupportEnabled ポリシーが有効に設定されている場合は、同じクライアントサイドの機能が共有されるため、このポリシーは有効にしないでください。この場合、Google でホストされる同期は完全に無効になります。 |
| URL キーによる匿名化データの収集を有効にする | 無効 | Google Chrome で URL キーによる匿名化データの収集を有効にし、ユーザーがこの設定を変更できないようにします。URL キーによる匿名化データの収集では、検索とブラウジングを改善する目的で、ユーザーがアクセスしたページの URL を Google に送信します。このポリシーを有効にすると、URL キーによる匿名化データの収集は常に有効になります。このポリシーを無効にすると、URL キーによる匿名化データの収集は常に無効になります。このポリシーを未設定のままにすると、URL キーによる匿名化データの収集は有効になりますが、ユーザーはこの設定を変更できます。 |
| URL のリストへのアクセスをブロックする | 有効次の値を入力するJavascript:// \*Chrome://History | このポリシーを有効にすると、ユーザーはブラックリストの URL からウェブページを読み込むことができなくなります。ブラックリストには、ブロックする URL のパターンを指定します。URL のパターンは、https://www.chromium.org/administrators/url-blacklist-filter-format?で示されている形式にする必要があります。URL ホワイトリスト ポリシーで例外を定義できます。このポリシーに指定できる項目数は 1,000 件で、それ以上指定した分は無視されます。内部の「chrome://\*」URL のブロックは、予期しないエラーが発生する可能性があるためおすすめしません。M73 以降では「Javascript://\*」の URL をブロックできます。ただし、ブロックされるのはアドレスバー（またはブックマークレットなど）に入力された Javascript のみです。ページ内 Javascript URL で動的に読み込まれたデータには、このポリシーは適用されません。たとえば、「example.com/abc」をブロックした場合でも、ページ「example.com」では XMLHTTPRequest で「example.com/abc」を読み込むことができます。このポリシーが未設定の場合、ブラウザではどの URL もブラックリスト扱いにはなりません。Chrome://History はブラウザーの履歴を削除できなくするための設定です。これにより、フォレンジックで悪意あるサイトの識別が可能となり、また、不正なWeb閲覧を特定できます。 サンプル値: example.com https://ssl.server.com hosting.com/bad\_path https://server:8080/path .exact.hostname.com file://\* custom\_scheme:\* \* |
| オンライン OCSP / CRL チェックを有効にする | 有効 | オンラインによる証明書取り消しの確認が Soft Fail の場合、セキュリティ上特段の効果がないという点を考慮し、Google Chrome バージョン 19 以降ではデフォルトで無効になっています。このポリシーを true に設定すると、前回の動作を復元し、オンライン OCSP / CRL チェックを実行します。このポリシーが未設定または false に設定された場合、Google Chrome はオンラインによる証明書取り消しの確認を行いません（Google Chrome 19 以降）。 |
| サードパーティの Cookie をブロックする | 有効 | この設定を有効にすると、ブラウザのアドレスバーに表示されているドメイン以外のウェブページ要素による Cookie の設定が禁止されます。この設定を無効にすると、ブラウザのアドレスバーに表示されているドメイン以外のウェブページ要素による Cookie の設定が許可されます。ユーザーはこの設定を変更できません。このポリシーが未設定の場合、サードパーティの Cookie が有効になりますが、ユーザーはその設定を変更できます。 |
| シークレット モードが利用可能かどうかを設定する | 有効 シークレットモードを無効にする | ユーザーが Google Chrome でシークレット モードを使用してページを開くことができるかどうかを指定します。[有効] が選択されている、またはポリシーが未設定の場合、シークレット モードでページを開くことができます。[無効] が選択されている場合、シークレット モードでページを開くことはできません。[強制] が選択されている場合、シークレット モードでのみページを開くことができます。シークレットモードを使用すると、ユーザーは閲覧履歴/アクティビティを記録せずにインターネットを閲覧できます。フォレンジックの観点からは、これは受け入れられません。ベストプラクティスでは、ブラウザの履歴を保持する必要があります。 |
| ダウンロードの制限を許可する | 有効 危険なダウンロードをブロックするもしくは危険なダウンロードをブロックする | Google Chrome で完全にブロックするダウンロードの形式を設定します（ユーザーはセキュリティの判定結果を無視するよう選択することはできません）。このポリシーを設定した場合、Google Chrome では特定形式のダウンロードがブロックされます。その際、ユーザーはセキュリティの警告を無視するよう選択することはできません。[危険なダウンロードをブロックする] オプションを選択すると、セーフ ブラウジングの警告が表示される場合にダウンロードがブロックされ、それ以外の場合はダウンロードが許可されます。[危険性のあるダウンロードをブロックする] オプションを選択すると、ダウンロードの危険性を示すセーフ ブラウジングの警告が表示される場合にダウンロードがブロックされ、それ以外の場合はダウンロードが許可されます。[すべてのダウンロードをブロックする] オプションを選択すると、すべてのダウンロードがブロックされます。[不正なファイルのダウンロードをブロックする] オプションを選択すると、セーフ ブラウジングで不正なファイルの可能性が高いと判断される場合にダウンロードがブロックされ、それ以外の場合はダウンロードが許可されます。ダウンロードの危険性を示す警告とは異なり、ファイルの形式は考慮されませんが、ホストは考慮されます。このポリシーが未設定の場合（または [特別な制限なし] オプションを選択した場合）、ダウンロードの際にはセーフ ブラウジングの解析結果に基づく通常のセキュリティ制限が適用されます。注: こうした通常の制限は、ウェブページのコンテンツやコンテキスト メニューの [リンクをダウンロード] オプションからダウンロードを呼び出す場合に適用されます。現在表示中のページを保存またはダウンロードする場合、あるいは印刷オプションから PDF への保存を選択する場合には適用されません。 |
| ダウンロード前に各ファイルの保存場所を確認する | 有効 | このポリシーが有効な場合、ユーザーはダウンロードの前に各ファイルの保存先を尋ねられます。このポリシーが無効な場合は、ダウンロードが直ちに始まり、ユーザーはファイルの保存先を尋ねられません。このポリシーが未設定の場合、ユーザーはこの設定を変更できます。 |
| ネットワーク予測を有効にする | 有効ネットワーク接続でネットワーク動作を予測しない | Google Chrome でネットワーク予測を有効にして、ユーザーがこの設定を変更できないようにします。これにより、DNS のプリフェッチ、TCP と SSL の事前接続、ウェブページの事前レンダリングが制御されます。このポリシーを設定すると、ユーザーは Google Chrome でこの設定の変更や上書きができなくなります。このポリシーが未設定の場合、ネットワーク予測は有効になりますが、ユーザーはこの設定を変更できます。 |
| ブラウザの履歴の保存を無効にする | 無効 | Google Chrome のブラウザ履歴の保存を無効にし、ユーザーがこの設定を変更できないようにします。 この設定を有効にすると、閲覧履歴は保存されません。また、タブの同期も無効になります。 この設定を無効にした場合、または未設定の場合は、閲覧履歴が保存されます。 |
| 検索キーワード候補を有効にする | 無効 | Google Chrome のアドレスバーで検索キーワード候補の表示を有効にし、ユーザーがこの設定を変更できないようにします。この設定を有効にすると、検索キーワード候補が表示されるようになります。この設定を無効にすると、検索キーワード候補は表示されません。この設定を有効または無効にすると、ユーザーは Google Chrome でこの設定の変更やオーバーライドができなくなります。このポリシーが未設定の場合は有効になりますが、ユーザーはこの設定を変更できます。 |
| 古いプラグインの実行を許可する | 無効 | この設定を有効にした場合、古いプラグインが通常のプラグインとして使用されます。この設定を無効にした場合、古いプラグインは使用されず、ユーザーに実行の許可を求めるメッセージも表示されません。未設定の場合、ユーザーに古いプラグインの実行の許可を求めるメッセージが表示されます。 |
| メディアの自動再生を許可する | 無効 | Google Chrome でユーザーの同意なしに動画の音声コンテンツを自動再生するかどうかを指定します。このポリシーを True に設定した場合、Google Chrome でメディアが自動再生されます。このポリシーを False に設定した場合、Google Chrome でメディアは自動再生されません。デフォルトでは、Google Chrome でメディアは自動再生されません。AutoplayWhitelist ポリシーを使用すると、特定の URL パターンについて、この設定をオーバーライドできます。Google Chrome の実行中にこのポリシーを変更した場合、変更内容は新しく開かれるタブにのみ適用されます。そのため、一部のタブでは変更前の動作が見られる場合があります。 |
| メディアの自動再生を許可する URL パターンのホワイトリストを指定する | ホワイトリストが必要な場合のみ 有効値＝URLパターンのホワイトリスト | 自動再生を常に有効にする URL パターンのホワイトリストを管理します。自動再生が有効な場合、動画は音声コンテンツとともに Google Chrome で自動再生されます（ユーザーの同意は確認されません）。有効な URL パターンの仕様は次のとおりです。- [\*.]domain.tld（domain.tld とすべてのサブドメインに一致）- host（ホスト名に完全一致）- scheme://host:port（サポートされているスキーム: http、https）- scheme://[\*.]domain.tld:port（サポートされているスキーム: http、https）- file://path（パスは絶対パスで「/」から開始する必要があります)- a.b.c.d（IPv4 IP に完全一致）- [a:b:c:d:e:f:g:h]（IPv6 IP に完全一致）AutoplayAllowed ポリシーを「True」に設定した場合、このポリシーは無視されます。AutoplayAllowed ポリシーを「False」に設定した場合、このポリシーに設定されている URL パターンでは再生が許可されます。Google Chrome の起動中にこのポリシーを変更した場合、変更内容は新しく開かれたタブにのみ適用されます。このため、一部のタブで以前の動作が継続される場合があります。サンプル値:https://www.example.com[\*.]example.edu |
| 使用状況とクラッシュ関連データのレポートを有効にする | 無効 | Google Chrome の使用状況とクラッシュに関するデータをGoogle に匿名で送信する設定を有効にするとともに、ユーザーがこの設定を変更できないようにします。この設定を有効にすると、使用状況とクラッシュに関するデータがGoogle に匿名で送信されます。この設定を無効にすると、この情報はGoogle に送信されません。どちらの場合も、ユーザーはこの設定を変更したりオーバーライドしたりすることはできません。このポリシーを未設定のままにした場合は、ユーザーがインストール時または初回実行時に選択した設定が適用されます。このポリシーは、Microsoft Active Directory ドメインに追加した Windows インスタンス、またはデバイスの管理対象として登録した Windows 10 Pro あるいは Enterprise インスタンスでのみ使用できます。 |
| 初回実行時にデフォルトのブラウザから保存したパスワードをインポートする | 無効 | このポリシーを有効にすると、以前の既定のブラウザで保存されたパスワードがインポートされます。有効にすると、このポリシーはインポート ダイアログにも影響します。無効にすると、保存されたパスワードはインポートされません。このポリシーが未設定の場合、インポートするかどうかをユーザーに尋ねるか、自動的にインポートされます。保存したパスワードをインポートすると、別のブラウザからシステムに保存された暗号化されていないアカウントパスワードが表示される可能性があるため、インポートを無効にする必要があります。 |
| 有効な SSL の最小バージョン | 有効TLS 1.2 | このポリシーが未設定の場合、Google Chrome ではデフォルトの最小バージョン（TLS 1.0）が使用されます。このポリシーを設定する場合、「tls1」、「tls1.1」、「tls1.2」のいずれかの値を指定できます。Google Chrome では、指定されたバージョンより小さい SSL / TLS バージョンは使用されません。認識されない値は無視されます。注?2020年上半期に多数のブラウザーがTLS1.0/1.1のサポートを中止します。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Google]>[Google Chrome]>[Google Cast]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Google Cast を有効にする | 無効 | このポリシーが true に設定されているか未設定の場合は、Google Cast が有効になり、ユーザーはアプリメニュー、ページ コンテキスト メニュー、Cast 対応ウェブサイトのメディア コントロール、Cast ツールバー アイコン（表示されている場合）から起動できるようになります。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Google]>[Google Chrome]>[コンテンツの設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 一致する URL からの Cookie を現在のセッションに限定する | 無効 | 指定の URL パターンに一致するページにより設定される Cookie を現在のセッションに限定します（ブラウザを終了するとこれらの Cookie が削除されます）。ここで指定するパターンに一致しない URL（またはこのポリシーが未設定の場合はすべての URL）に対しては、グローバルなデフォルト値（DefaultCookiesSetting」ポリシーで値が設定されている場合はその値、設定されていない場合はユーザーの個人設定の値）が使用されます。Google Chrome が「バックグラウンド モード」で実行されている場合、ブラウザ ウィンドウをすべて閉じてもセッションは閉じられず、ブラウザを終了するまで開かれたままになる可能性があります。この動作の設定について詳しくは、「Background&#x4D;odeEnabled」ポリシーを参照してください。「CookiesAllowedForUrls」ポリシーと「CookiesBlockedForUrls」ポリシーも参照してください。これら 3 つのポリシーの URL パターンが競合しないようにする必要があります。競合する場合にどのポリシーが優先されるかは決まっていません。「Restore&#x4F;nStartup」ポリシーで前のセッションの URL を復元するように設定されている場合、このポリシーは無視され、該当するサイトの Cookie は恒久的に保存されます。サンプル値:https://www.example.com[\*.]example.edu |
| デフォルトの位置情報設定 | 有効すべてのサイトに対してユーザーの物理的な現在地の追跡を許可しない | ウェブサイトに対してユーザーの物理的な現在地の追跡を許可するかどうかを設定できます。ユーザーの物理的な現在地の追跡は、デフォルトで許可または禁止することができます。また、ウェブサイトが物理的な現在地を要求するときに毎回ユーザーに確認することもできます。このポリシーが未設定の場合、「AskGeolocation」が使用され、ユーザーはこの設定を変更できます。 |
| デフォルトの通知設定 | 有効どのサイトにもデスクトップ通知の表示を許可しない | ウェブサイトに対してデスクトップ通知の表示を許可するかどうかを設定できます。デスクトップ通知の表示は、デフォルトで許可または禁止することができます。また、ウェブサイトでデスクトップ通知が表示される前にユーザーが毎回確認することもできます。このポリシーが未設定の場合、「AskNotifications」が使用され、ユーザーはこの設定を変更できます。 |
| デフォルトの Flash 設定 | 有効クリックして再生する | ウェブサイトでの Flash プラグインの自動実行を許可するかどうかを設定します。すべてのウェブサイトに対し、Flash プラグインの自動実行を許可するか拒否するかのいずれかに設定できます。クリックして再生の場合、Flash プラグインの実行は許可されますが、実行にはユーザーがプレースホルダをクリックする必要があります。自動再生は PluginsAllowedForUrls ポリシーで明示的に指定されているドメインでのみ許可されます。すべてのサイトで自動再生を有効にするには、このリストに?http://\*?と?https://\*?を追加します。このポリシーを設定しない場合、ユーザーはこの設定を手動で変更できます。 |
| デフォルトのポップアップ設定 | 有効すべてのサイトに対してポップアップ表示を許可しない | ウェブサイトに対してポップアップ表示を許可するかどうかを設定できます。ポップアップ表示は、すべてのウェブサイトに対して許可または禁止することができます。このポリシーが未設定の場合、「BlockPopups」が使用され、ユーザーはこの設定を変更できます。 |
| WebUSB API の使用を管理する | 有効すべてのサイトに対して WebUSB API 経由での USB デバイスへのアクセスを許可しない | 接続されている USB デバイスへのアクセスをウェブサイトに許可するかどうかを設定します。アクセスを完全にブロックするか、接続されている USB デバイスへのアクセスがウェブサイトからリクエストされたときに毎回ユーザーに確認するように設定することができます。「WebUsbAskForUrls」または「WebUsbBlockedForUrls」ポリシーで指定した URL パターンに該当するサイトには、これらのうちいずれか該当する方のポリシーが適用され、このポリシーは適用されません。このポリシーが未設定の場合は「3」が使用され、ユーザーはこの設定を変更できます。 |
| これらのサイトで Flash プラグインを許可する | 有効許可するサイトのURLを設定 | Flash プラグインの実行を許可するサイトを表す URL パターンのリストを設定します。このポリシーが未設定の場合は、すべてのサイトでグローバルなデフォルト値（「DefaultPluginsSetting」ポリシーで値が設定されている場合はその値、設定されていない場合はユーザーの個人設定の値）が使用されます。サンプル値:https://www.example.com[\*.]example.edu |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Google]>[Google Chrome]>[セーフブラウジングの設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| セーフブラウジングを有効にする | 有効 | Google Chrome のセーフ ブラウジング機能を有効にするとともに、ユーザーがこの設定を変更できないようにします。この設定を有効にすると、セーフ ブラウジングが常に適用されます。この設定を無効にすると、セーフ ブラウジングは適用されません。この設定を有効または無効にした場合、ユーザーは Google Chrome の [フィッシングや不正なソフトウェアからの保護を有効にする] 設定を変更したりオーバーライドしたりできなくなります。このポリシーを未設定のままにした場合、セーフ ブラウジングは有効になりますが、ユーザーがこの設定を変更することもできます。このポリシーは、Microsoft Active Directory ドメインに追加した Windows インスタンス、またはデバイスの管理対象として登録した Windows 10 Pro あるいは Enterprise インスタンスでのみ使用できます。 |
| セーフ ブラウジングの詳細レポートを有効にする | 無効 | Google Chrome のセーフ ブラウジングの詳細レポートを有効にするとともに、ユーザーがこの設定を変更できないようにします。詳細レポートでは、一部のシステム情報とページ コンテンツが Google のサーバーに送信され、危険なアプリやサイトの検出に役立てられます。この設定を true にした場合、レポートは必要なとき（セキュリティ インタースティシャルが表示されたときなど）に毎回作成され、送信されます。この設定を false にした場合、レポートは送信されません。このポリシーが true または false に設定されている場合、ユーザーは設定を変更できません。このポリシーが未設定の場合、ユーザーは設定を変更でき、レポートを送信するかどうかを指定できます。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Google]>[Google Chrome]>[デフォルトの検索プロバイダ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| デフォルトの検索プロバイダの検索 URL | 有効組織が承認した暗号化された検索文字列を指定する。 例：  https://www.google.com/#q={searchTerms}  またはhttps://www.bing.com/search?q={searchTerms }） | デフォルトの検索を行うときに使用される検索エンジンのURLを指定します。インターネット検索を行うときは、https経由の暗号化された接続を使用することが重要です。 |
| デフォルトの検索プロバイダを有効にする | 有効 | デフォルトの検索プロバイダの使用を有効にします。この設定を有効にすると、ユーザーがアドレスバーに URL 以外のテキストを入力したときにデフォルトの検索プロバイダによる検索が実行されます。デフォルトの検索に関する他のポリシーを設定して、使用されるデフォルトの検索プロバイダを指定することもできます。これらの設定を空白のままにすると、ユーザーはデフォルトのプロバイダを選択できます。この設定を無効にすると、ユーザーがアドレスバーに URL 以外のテキストを入力したときに検索は実行されません。この設定を有効または無効にすると、ユーザーは Google Chrome でこの設定の変更やオーバーライドができません。このポリシーを未設定のままにした場合、デフォルトの検索プロバイダが有効になり、ユーザーは検索プロバイダのリストを設定することができます。このポリシーは、Microsoft Active Directory ドメインに追加した Windows インスタンス、またはデバイスの管理対象として登録した Windows 10 Pro あるいは Enterprise インスタンスでのみ使用できます。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Google]>[Google Chrome]>[パスワード マネージャ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| パスワード マネージャへのパスワード保存を有効にする | 無効 | この設定が有効な場合、ユーザーは Google Chrome にパスワードを保存できます。パスワードは、サイトへ次回ログインしたときに自動的に入力されます。この設定が無効な場合、ユーザーは新しいパスワードを保存できませんが、以前保存したパスワードは引き続き使用できます。このポリシーが有効または無効の場合、ユーザーは Google Chrome でこの設定を変更したりオーバーライドしたりすることはできません。このポリシーが未設定の場合、パスワードは保存されます（ただし、ユーザーはパスワードの保存をオフにできます）。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Google]>[Google Chrome]>[リモートアクセス]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| リモート アクセス ホストからのファイアウォール トラバーサルを有効にする | 無効 | リモート クライアントがこのコンピュータへの接続を試行するときに STUN サーバーを使用できるようにします。この設定が有効な場合、リモート クライアントはファイアウォールの有無にかかわらずこのコンピュータを検出して接続できます。この設定が無効な場合で発信 UDP 接続がファイアウォールによって除外されている場合は、ローカル ネットワーク内のクライアント コンピュータのみがこのコンピュータに接続できます。このポリシーが未設定の場合、この設定は有効になります。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Google]>[Google Chrome]>[印刷]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Google Cloud Print プロキシを有効にする | 無効 | Google Cloud Print と、パソコンに接続している従来のプリンタとの間で、Google Chrome がプロキシとして動作できるようにします。この設定が有効な場合または未設定の場合、ユーザーは Google アカウントでの認証によってクラウド プリント プロキシを有効にできます。この設定が無効な場合、ユーザーはプロキシを有効にできず、パソコンはプリンタを Google Cloud Print と共有できません。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Google]>[Google Chrome]>[拡張機能]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 拡張機能インストールのブラックリストを設定する | 有効表示をクリックし値に \* を設定する | ユーザーによるインストールを禁止する拡張機能を指定できます。すでにインストールされている拡張機能をブラックリスト登録した場合、その拡張機能は無効になり、ユーザーが有効にすることはできません。ブラックリスト登録して無効になった拡張機能は、ブラックリストから削除すると自動的に再度有効になります。値「\*」を指定すると、すべての拡張機能をブラックリスト登録することになります（明示的にホワイトリスト登録している拡張機能は除外されます）。このポリシーが未設定の場合、ユーザーは Google Chrome にあらゆる拡張機能をインストールできます。 |
| 拡張機能インストールのホワイトリストを設定する | 有効表示をクリックし値に1を入力する。 | ブラックリストの対象外となる拡張機能を指定できます。ブラックリストの値が「\*」の場合、すべての拡張機能がブラックリストに登録されており、ユーザーはホワイトリストにリストされている拡張機能しかインストールできません。デフォルトでは、すべての拡張機能はホワイトリストに登録されていますが、ポリシーによってすべての拡張機能をブラックリストに登録している場合、ホワイトリストを使ってそのポリシーをオーバーライドできます。有効なポリシー値oiigbmnaadbkfbmpbfijlflahbdbdgdf（または1）注：oiigbmnaadbkfbmpbfijlflahbdbdgdfは、scriptno（一般的に使用されるChrome拡張機能）の拡張IDです。 |

## ・Windows Server 2016 Domain Controller

### Windows Server 2016 Domain Controller のセキュリティ構成

このセキュリティ構成は、米国防総省の Security Technical Implementation Guides をベースとし、悪意あるプログラムの初期侵入や実行を防止するために策定されたものです。

#### 設定による影響

* 脆弱性のある危険なプロトコル (SMBv1) を禁止している関係で、古い互換性のないNASに接続できない可能性があります。
* リモート接続や共有へのアクセスの厳格化や防御設定によって、一部、アプリケーションが動作しないなどの影響が考えられます。事前に、テスト用の OU を作成し、設定を検証してください。
* Office 2019 やAcrobat、Chrome、Edgeなどの動作には影響があったとの報告は受けていません。

#### 前提となるハードウェア構成

* トラステッドプラットフォームモジュール（TPM）2.0
* Bitlockerドライブ暗号化
* UEFIセキュアブート
* Windows Updateを通じて配布されるドライバーとファームウェア

#### 適用するポリシー

* DC アカウントポリシー
* DC ローカルポリシー ユーザー権利の割り当て
* DC ローカルポリシー セキュリティ オプション
* DC 監査ポリシーの詳細な構成
* DC 管理用テンプレート
* DC アカウントポリシー

### DC アカウントポリシー

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[アカウント ポリシー]>[パスワードのポリシー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| パスワードの長さ | 14文字 | このセキュリティ設定は、ユーザー アカウントのパスワードに使用できる最少文字数を決定します。1 から 20 文字に設定するか、文字数を 0 に設定してパスワードを不要にします。 既定値: 7 (ドメイン コントローラーの場合) 0 (スタンドアロン サーバーの場合) 注意: 既定では、メンバー コンピューターはそのドメイン コントローラーの構成に従います。 |
| パスワードの変更禁止期間 | 1日 | このセキュリティ設定は、パスワードが変更可能になるまでの期間 (日数) を決定します。この期間内は、同じパスワードを使わなければなりません。1 から 998 までの日数を指定するか、または日数を 0 に設定してすぐに変更できるようにします。パスワード有効期間が 0 (有効期限が無期限) に設定されている場合を除き、パスワードの変更禁止期間には、パスワード有効期間よりも短い値を設定してください。パスワードの有効期間が 0 に設定されている場合は、パスワード変更禁止期間として 0 から 998 までの日数を指定できます。 [パスワードの履歴を記録する] を有効にする場合は、パスワードの変更禁止期間を 1 以上に設定してください。パスワードの変更禁止期間を指定しない場合、ユーザーはパスワードを繰り返し変更して、以前のパスワードを再度利用することができます。既定の設定はこの推奨事項に従っていません。これは、管理者がユーザーのパスワードを設定しておき、管理者指定のパスワードをログオン時に変更するようユーザーに要求できるようにするためです。パスワードの履歴が 0 の場合、ユーザーは新しいパスワードを設定する必要がありません。このため、[パスワードの履歴を記録する] の既定値は 1 に設定されています。 既定値:1 (ドメイン コントローラーの場合)0 (スタンドアロン サーバーの場合) 注意: 既定では、メンバー コンピューターはそのドメイン コントローラーの構成に従います。 |
| パスワードの有効期間 | 60日間 | このセキュリティ設定は、1 つのパスワードを使用できる期間 (日数) を決定します。この期間を過ぎると、システムから変更するよう要求されます。有効期間として 1 から 999 までの日数を指定するか、日数を 0 に設定してパスワードの有効期限が切れないように指定します。パスワードの有効期間が 1 から 999 日の場合、パスワードの変更禁止期間にはこの有効期間よりも短い日数を指定してください。パスワードの有効期間が 0 に設定されている場合は、パスワードの変更禁止期間として 0 から 998 までの日数を指定できます。 注意: ご使用の環境に応じて、パスワードの有効期間を 30 から 90 日間に設定しておくとセキュリティ上最も効果的です。これにより、攻撃者がユーザー パスワードの解読とネットワーク リソースへのアクセスに使用できる時間が制限されます。 既定値: 42 |
| パスワードの履歴を記録する | 24回 | このセキュリティ設定は、以前使ったことがあるパスワードをもう一度使用できるようになるまでに、ユーザー アカウントに関連付ける必要がある異なる新しいパスワードの数を決定します。0 から 24 までの値を指定してください。このポリシーを使用すると、管理者は古いパスワードの継続使用を防ぐことによってセキュリティを強化できます。既定値:24 (ドメイン コントローラーの場合)0 (スタンドアロン サーバーの場合) 注意: 既定では、メンバー コンピューターはそのドメイン コントローラーの構成に従います。パスワードの履歴の有効性を保つために、パスワードの変更禁止期間セキュリティ ポリシーも有効にして、パスワードを変更した直後にはパスワードを変更できないようにしてください。パスワードの変更禁止期間セキュリティ ポリシーの詳細については、「パスワードの変更禁止期間」を参照してください。 |
| 暗号化を元に戻せる状態でパスワードを保存する | 無効 | このセキュリティ設定は、オペレーティング システムが暗号化を元に戻せる状態でパスワードを保存するかどうかを決定します。 このポリシーは、認証用にユーザーのパスワード情報が必要なプロトコルを使用するアプリケーションをサポートします。暗号化を元に戻せる状態でパスワードを保存するということは、実質的にパスワードをプレーンテキストで保存するのと同じことです。このため、パスワード情報の保護よりもアプリケーションの要件が優先される場合以外は、このポリシーを有効にしないでください。 このポリシーは、リモート アクセスまたはインターネット認証サービス (IAS) でチャレンジ ハンドシェイク認証プロトコル (CHAP) 認証を使用する場合に必要です。また、インターネット インフォメーション サービス (IIS) でダイジェスト認証を使用する場合にも必要です。 既定値: 無効 |
| 複雑さの要件を満たす必要があるパスワード | 有効 | このセキュリティ設定は、パスワードが複雑さの要件を満たす必要があるかどうかを決定します。このポリシーが有効な場合、パスワードは次の最小要件を満たす必要があります。 ユーザーのアカウント名またはフル ネームに含まれる 3 文字以上連続する文字列を使用しない。 長さは 6 文字以上にする。 次の 4 つのカテゴリのうち 3 つから文字を使う。 英大文字 (A から Z)英小文字 (a から z) 10 進数の数字 (0 から 9) アルファベット以外の文字 (!、$、#、% など) 複雑さの要件は、パスワードの変更時または作成時に強制的に適用されます。 既定値: 有効 (ドメイン コントローラーの場合) 無効 (スタンドアロン サーバーの場合) 注意: 既定では、メンバー コンピューターはそのドメイン コントローラーの構成に従います。 |

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[アカウント ポリシー]>[アカウント ロックアウトのポリシー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| アカウントのロックアウトのしきい値 | 3回 | このセキュリティ設定は、ユーザー アカウントがロックアウトされる原因となるログオン失敗回数を決定します。ロックアウトされたアカウントは、管理者がリセットするか、そのアカウントのロックアウト期間が過ぎるまで使用できません。ログオン失敗回数として 0 から 999 までの値を設定できます。この値を 0 に設定すると、アカウントがロックアウトされることはありません。 Ctrl + Alt + Del キーまたはパスワード保護されたスクリーン セーバーを使ってロックされているワークステーションまたはメンバー サーバーの場合、パスワードの失敗はログオンの失敗としてカウントされます。 既定値: 0 |
| ロックアウト カウンターのリセット | 15分 | このセキュリティ設定は、ログオン失敗後、ログオン失敗のカウンターが 0 (不良ログオン試行) にリセットされるまでに必要な時間を分単位で指定します。設定できる時間は、1 から 99,999 分です。 アカウント ロックアウトのしきい値が定義されている場合は、このリセット時間をロックアウト期間と同じかそれ以下にしてください。 既定値: なし。このポリシーの設定は、アカウントのロックアウトのしきい値が指定されている場合のみ有効です。 |
| ロックアウト期間 | 15分 | このセキュリティ設定は、ロックアウトされたアカウントが自動的にロック解除されるまでのロックアウト期間を分単位で指定します。設定できる時間は、0 から 99,999 分です。ロックアウト期間を 0 に設定すると、管理者が明示的にロックを解除するまでアカウントはロックアウトされます。 アカウント ロックアウトのしきい値が定義されている場合は、アカウント ロックアウト期間をリセット時間と同じかそれ以上にしてください。 既定値: なし。このポリシーの設定は、[アカウントのロックアウトのしきい値] が設定されている場合のみ有効です。 |

### ・DC ローカルポリシー ユーザー権利の割り当て

#### [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[ユーザー権利の割り当て]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| オペレーティングシステムの一部として機能 | 誰もいない（空白） | このユーザーの権利を使用すると、プロセスは認証なしでどのユーザーを偽装することもできます。したがって、プロセスはそのユーザーと同じローカル リソースにアクセスできるようになります。 この特権を必要とするプロセスでは、この特権を特別に割り当てられたユーザー アカウントを使用するのではなく、この特権が最初から含まれている LocalSystem アカウントを使用してください。組織内で Windows Server 2003 ファミリのメンバーのサーバーしか使用しない場合、この特権をユーザーに割り当てる必要はありません。ただし、組織内で Windows 2000 または Windows NT 4.0 を実行するサーバーを使用する場合は、この特権を割り当てて、プレーンテキストのパスワードを交換するアプリケーションを使用する必要が生じる場合があります。 注意: このユーザーの権利を割り当てると、セキュリティ上の問題が生じる可能性があります。このユーザーの権利は、信頼できるユーザーのみに割り当ててください。 既定値: なし |
| グローバルオブジェクトの作成 | Administrators LOCAL SERVICE NETWORK SERVICE SERVICE | このセキュリティ設定は、すべてのセッションから利用できるグローバル オブジェクトをユーザーが作成できるかどうかを決定します。このユーザー権利がないユーザーも、自分のセッションに特有のオブジェクトは作成できます。グローバル オブジェクトを作成できるユーザーは、他のユーザーのセッション下で実行されているプロセスに影響を及ぼす可能性があり、そのためアプリケーション エラーやデータの破損を引き起こすことがあります。 注意: このユーザー権利を割り当てると、セキュリティ上の問題が生じる可能性があります。このユーザー権利は、信頼できるユーザーのみに割り当ててください。 既定値: Administrators Local Service Network Service Service |
| コンピューターとユーザー アカウントに委任時の信頼を付与 | Administrators | このセキュリティ設定は、ユーザー オブジェクトまたはコンピューター オブジェクトに対する [Trusted for Delegation] 設定を設定できるユーザーを決定します。この特権を与えられるユーザーまたはオブジェクトは、ユーザー オブジェクトまたはコンピューター オブジェクトのアカウント制御フラグに対する「書き込み」アクセスを与えられている必要があります。クライアントのアカウントに "Account cannot be delegated" アカウント制御フラグ セットがない限り、委任時の信頼を付与されているコンピューター (またはユーザー コンテキスト) で実行されているサーバー プロセスは、クライアントの委任された資格情報を使用して他のコンピューター上のリソースにアクセスできます。このユーザー権利は、既定のドメイン コントローラーのグループ ポリシー オブジェクト (GPO) およびワークステーションとサーバーのローカル セキュリティ ポリシーで定義されます。 注意: このユーザー権利または [Trusted for Delegation] 設定を誤って使用すると、外部から接続するクライアントを偽装し、その資格情報を使用してネットワーク リソースにアクセスするトロイの木馬プログラムによる高度な攻撃に対して、ネットワークが脆弱になる可能性があります。 既定値: ドメイン コントローラー上の Administrators |
| サービスとしてログオン | 誰もいない（空白） | このセキュリティ設定は、セキュリティ プリンシパルがサービスとしてログオンすることを可能にします。Local System、Local Service、Network Service の各アカウントは、サービスとしてログオンするための権利が組み込まれているため、サービスをこれらのアカウントで実行するように構成できます。その他のユーザー アカウントで実行するサービスには適切な権利を割り当てる必要があります。 既定値: なし Windows Server 2012ベースのコンピューターでHyper-V仮想マシンの起動またはライブ移行がエラー0x80070569で失敗する場合がある [https://support.microsoft.com/ja-jp/help/2779204/starting-or-live-migrating-hyper-v-virtual-machines-may-fail-with-erro](https://support.microsoft.com/ja-jp/help/2779204/starting-or-live-migrating-hyper-v-virtual-machines-may-fail-with-erro&br;) この場合、NT Virtual Machine\Virtual Machines を含める。 |
| シンボリックリンクを作成する | Administrators NT Virtual Machine\Virtual Machines （必要に応じて） | この特権は、ユーザーがログオンしているコンピューターからシンボリック リンクを作成できるかどうかを決定します。 既定値: Administrator 警告: この特権は、信頼されるユーザーにのみ付与するようにしてください。シンボリック リンクを処理するように設計されていないアプリケーションでシンボリック リンクを使用すると、セキュリティによる保護が脆弱になります。 注意: この設定は、コンピューター上で許可される symlink の種類を制御するためにコマンド ライン ユーティリティで操作される、symlink ファイル システム設定と組み合わせて使用できます。fsutil とシンボリック リンクの詳細についての情報を得るには、コマンド ラインで「fsutil behavior set symlinkevalution /?」と入力してください。 |
| スケジューリング優先順位の繰り上げ | Administrators | このセキュリティ設定は、他のプロセスに対するプロパティの書き込みアクセスを持つプロセスを使用して、そのプロセスに割り当てられている実行の優先順位を上げることができるアカウントを決定します。この特権を与えられているユーザーは、タスク マネージャー ユーザー インターフェイスを使ってプロセスのスケジュールの優先順位を変更できます。 既定値: Administrator |
| セキュリティ監査の生成 | NETWORK SERVICE、LOCAL SERVICE | このセキュリティ設定は、セキュリティ ログにエントリを追加するためにプロセスが使用できるアカウントを決定します。セキュリティ ログは、システムへの権限のないアクセスの追跡に使用されます。このユーザーの権利を誤用すると、多くの監査イベントが生成され、[監査: セキュリティ監査のログを記録できない場合は直ちにシステムをシャットダウンする] セキュリティ ポリシー設定が有効になっている場合には、攻撃の証拠が隠されたり、サービス拒否 (Denial-Of-Service) を引き起こす可能性があります。詳細については、「監査: セキュリティ監査のログを記録できない場合は直ちにシステムをシャットダウンする」を参照してください。 既定値: Local ServiceNetwork Service |
| デバイスドライバーのロードとアンロード | Administrators | このユーザーの権利は、デバイス ドライバーまたは他のコードをカーネル モードで動的にロードおよびアンロードできるユーザーを決定します。このユーザーの権利は、プラグ アンド プレイ デバイス ドライバーには適用されません。この特権は、他のユーザーに割り当てないことをお勧めします。 注意: このユーザーの権利を割り当てると、セキュリティ上の問題が生じる可能性があります。このユーザーの権利は、システム管理の担当ではないユーザー、グループ、またはプロセスには割り当てないでください。 ワークステーションとサーバーの既定値: Administrators ドメイン コントローラーの既定値:Administrators, Print Operators |
| トークンオブジェクトの作成 | 誰もいない（空白） | このセキュリティ設定は、プロセスが内部アプリケーション プログラミング インターフェイス (API) でアクセス トークンを作成するときに、ローカル リソースへのアクセス用のトークンを作成するプロセスが使用できるアカウントを決定します。 このユーザーの権利はオペレーティング システムによって内部的に使用されます。必要がない限り、このユーザーの権利を Local System 以外のユーザー、グループ、またはプロセスに割り当てないでください。 注意: このユーザーの権利を割り当てると、セキュリティ上の問題が生じる可能性があります。このユーザーの権利を、システム管理の担当ではないユーザー、グループ、またはプロセスには割り当てないでください。 既定値: なし |
| ドメインにワークステーションを追加 | Administrators | このセキュリティ設定は、ドメインにワークステーションを追加できるグループまたはユーザーを決定します。 このセキュリティ設定は、ドメイン コントローラーでのみ有効です。既定では、認証済みのすべてのユーザーにこの権利があり、最大 10 個のコンピューター アカウントをドメインに作成できます。 ドメインにコンピューター アカウントを追加すると、そのコンピューターは Active Directory ベースのネットワークに参加できます。たとえば、ワークステーションをドメインに追加すると、そのワークステーションは Active Directory にあるアカウントとグループを認識できるようになります。 既定値: Authenticated Users (ドメイン コントローラー) 注意: Active Directory コンピューター コンテナーで "コンピューター オブジェクト作成" アクセス許可を持つユーザーは、ドメインにコンピューター アカウントを作成することもできます。コンテナーでのアクセス許可を持つユーザーは、作成できるコンピューター アカウントの数が 10 個に制限されません。また、"ドメインにワークステーションを追加" を使用して作成したコンピューター アカウントの所有者は Domain Administrators になります。一方、コンピューター コンテナーでのアクセス許可を使用して作成したコンピューター アカウントの所有者は、コンピューター アカウントの作成者になります。コンテナーでのアクセス許可を持つユーザーが、"ドメインにワークステーションを追加" ユーザー権利も持っている場合、ユーザー権利ではなくコンピューター コンテナーのアクセス許可に基づいてコンピューターが追加されます。 |
| ネットワーク経由でのアクセス | Administrators Authenticated Users ENTERPRISE DOMAIN CONTROLLERS | このユーザーの権利は、ネットワーク経由でコンピューターに接続できるユーザーおよびグループを決定します。リモート デスクトップ サービスはこのユーザーの権利には影響されません。 注意: リモート デスクトップ サービスは、以前のバージョンの Windows Server でターミナル サービスと呼ばれていました。 ワークステーションとサーバーの既定値:Administrators, Backup Operators, Users, Everyone ドメイン コントローラーの既定値:Administrators, Authenticated Users, Enterprise Domain Controllers, Everyone, Pre-Windows 2000 Compatible Access |
| ネットワーク経由でのアクセスを拒否する | Guests | このセキュリティ設定は、ネットワーク経由でコンピューターにアクセスできないユーザーを決定します。ユーザー アカウントに [ネットワーク経由でのアクセス] と [ネットワーク経由のアクセスを拒否] の両方のポリシーが適用されている場合、このポリシーの設定は、[ネットワーク経由でのアクセス] ポリシーの設定より優先されます。 既定値: Guest |
| バッチ ジョブとしてのログオンを拒否 | Guests | このセキュリティ設定は、バッチ ジョブとしてログオンできないアカウントを決定します。ユーザー アカウントに [バッチ ジョブとしてログオン] と [バッチ ジョブとしてのログオンを拒否] の両方のポリシーが適用されている場合、このポリシーの設定は、[バッチ ジョブとしてログオン] ポリシーの設定より優先されます。既定値 : なし |
| ファームウェア環境値の修正 | Administrators | このセキュリティ設定は、ファームウェアの環境値を変更できるユーザーを決定します。ファームウェア環境変数は、非 x86 ベースのコンピューターの不揮発性 RAM に格納される設定です。設定の影響は、プロセッサによって異なります。 x86 ベースのコンピューターでは、このユーザーの権利を割り当てることで変更できる唯一のファームウェア環境値は、前回正常起動時の構成です。これは、システムによってのみ変更する構成です。 Itanium ベースのコンピューターでは、起動情報が不揮発性 RAM に格納されます。bootcfg.exe を実行し、[システムのプロパティ] の [起動と回復] にある [既定のオペレーティング システム] 設定を変更するには、ユーザーにこのユーザーの権利を割り当てる必要があります。 すべてのコンピューターにおいて、Windows をインストールまたはアップグレードするにはこのユーザーの権利が必要です。 注意: [システムのプロパティ] の [詳細設定] タブに表示されるシステム環境変数とユーザー環境変数を変更できるユーザーに対しては、このセキュリティ設定は影響を及ぼしません。これらの値の変更方法の詳細については、「環境変数の値を追加または変更する」を参照してください。 既定値: Administrators |
| ファイルとその他のオブジェクトの所有権の取得 | Administrators | このセキュリティ設定は、Active Directory オブジェクト、ファイルとフォルダー、プリンター、レジストリ キー、プロセス、スレッドなど、セキュリティが設定可能な任意のオブジェクトの所有権を取得できるユーザーを決定します。 注意: このユーザーの権利を割り当てると、セキュリティ上の問題が生じる可能性があります。オブジェクトの所有者はオブジェクトを完全に制御できるので、信頼されているユーザーのみにこのユーザーの権利を割り当ててください。 既定値: Administrators |
| ファイルとディレクトリのバックアップ | Administrators | このユーザーの権利は、システムをバックアップするために、ファイルやディレクトリ、レジストリ、およびその他の固定オブジェクトのアクセス許可をバイパスできるユーザーを決定します。 具体的には、このユーザーの権利はシステムのすべてのファイルおよびフォルダーに対する次のアクセス許可を、特定のユーザーまたはグループに与えることに似ています。 -フォルダーのスキャンとファイルの実行 -フォルダーの一覧/データの読み取り -属性の読み取り -拡張属性の読み取り -アクセス許可の読み取り 注意: このユーザーの権利を割り当てると、セキュリティ上の問題が生じる可能性があります。ユーザーがデータをバックアップしているのか、データを盗み出しているのか、あるいは配布用にデータをコピーしているのかを判断する方法がないため、信頼されているユーザーのみにこのユーザーの権利を割り当ててください。 ワークステーションとサーバーの既定値:Administrators, Backup Operators ドメイン コントローラーの既定値: Administrators, Backup Operators, Server Operators |
| ファイルとディレクトリの復元 | Administrators | このセキュリティ設定は、バックアップしたファイルやディレクトリを復元するときにファイル、ディレクトリ、レジストリ、およびその他の持続的なオブジェクトのアクセス許可をバイパスできるユーザーと、任意の有効なセキュリティ プリンシパルをオブジェクトの所有者に設定できるユーザーを決定します。 具体的には、このユーザーの権利はシステムのすべてのファイルおよびフォルダーに対する次のアクセス許可を、特定のユーザーまたはグループに与えることに似ています。 -フォルダーのスキャンとファイルの実行 -書き込み 注意: このユーザーの権利を割り当てると、セキュリティ上の問題が生じる可能性があります。このユーザー権利が割り当てられているユーザーは、レジストリ設定を上書きしたり、データを非表示にしたり、システム オブジェクトを所有することができるため、信頼されているユーザーのみにこの権利を割り当ててください。 ワークステーションとサーバーの既定値:: Administrators、Backup Operators ドメイン コントローラー既定値: Administrators、Backup Operators、Server Operators |
| プログラムのデバッグ | Administrators | このユーザーの権利は、任意のプロセスまたはカーネルにデバッガーをアタッチできるユーザーを決定します。独自のアプリケーションをデバッグする開発者にこのユーザーの権利を割り当てる必要はありません。新しいシステム コンポーネントをデバッグする開発者には、このユーザーの権利が必要です。このユーザーの権利は、重要なオペレーティング システム コンポーネントに完全なアクセスを提供します。 注意: このユーザーの権利を割り当てると、セキュリティ上の問題が生じる可能性があります。このユーザーの権利は、信頼できるユーザーのみに割り当ててください。 既定値: Administrators |
| ページファイルの作成 | Administrators | このユーザーの権利は、内部のアプリケーション プログラミング インターフェイス (API) を呼び出してページ ファイルの作成とサイズ変更を実行できるユーザーおよびグループを決定します。このユーザーの権利はオペレーティング システムの内部で使用され、通常はユーザーに割り当てる必要はありません。 特定のドライブのページング ファイルのサイズを変更する方法については、仮想メモリのページング ファイルのサイズ変更に関するページを参照してください。 既定値: Administrators |
| ボリュームの保守タスクを実行 | Administrators | このセキュリティ設定は、リモート最適化などのボリュームの保守タスクを実行できるユーザーおよびグループを決定します。 このユーザーの権利を割り当てるときは、注意が必要です。このユーザー権利が割り当てられたユーザーは、ディスクを参照したり、他のデータが含まれているメモリにファイルを拡張することができます。拡張されたファイルが開かれると、取得したデータをユーザーが参照して変更できる可能性があります。 既定値: Administrators |
| メモリ内のページのロック | 誰もいない（空白） | このセキュリティ設定は、プロセスを使用して物理メモリにデータを保持できるアカウントを決定します。これによって、システムはディスク上の仮想メモリにデータをページングできなくなります。この特権を使用すると、使用できるランダム アクセス メモリ (RAM) の量が減るため、システムのパフォーマンスに重大な影響を与える可能性があります。 既定値: なし |
| リモート コンピュータからの強制シャットダウン | Administrators | このセキュリティ設定は、ネットワーク上のリモート ロケーションからコンピューターをシャットダウンできるユーザーを決定します。このユーザーの権利を誤用すると、サービス拒否 (Denial-Of-Service) を引き起こす可能性があります。このユーザー権利は、既定のドメイン コントローラーのグループ ポリシー オブジェクト (GPO) およびワークステーションとサーバーのローカル セキュリティ ポリシーで定義されます。 ワークステーションとサービスの既定値: Administrators ドメイン コントローラーの既定値: Administrators、Server Operators |
| リモート デスクトップ サービスを使ったログオンを拒否 | Guests | このセキュリティ設定は、リモート デスクトップ サービス クライアントとしてログオンしたときに拒否されるユーザーまたはグループを決定します。 既定値: なし |
| リモート デスクトップ サービスを使ったログオンを許可 | Administrators | このセキュリティ設定は、リモート デスクトップ サービス クライアントとしてログオンするためのアクセス許可が付与されるユーザーまたはグループを決定します。 ワークステーションとサーバーの既定値: Administrators、Remote Desktop Users ドメイン コントローラーの既定値: Administrators |
| ローカルログオンを拒否 | Guests | このセキュリティ設定は、コンピューターでログオンできないユーザーを決定します。アカウントに [ローカル ログオンを許可] と [ローカル ログオンを拒否] の両方のポリシーが適用されている場合、このポリシーの設定は、[ローカル ログオンを許可] ポリシーの設定より優先されます。重要このセキュリティ ポリシーを Everyone グループに適用すると、だれもローカルでログオンできなくなります。既定値: なし |
| ローカルログオンを許可 | Administrators | このコンピューターにログオンできるユーザーを決定します。 重要: この設定を変更すると、クライアント、サーバー、およびアプリケーションとの互換性に影響が生じることがあります。この設定の互換性については、Microsoft の Web サイト (<http://go.microsoft.com/fwlink/?LinkId=24268)> の「ローカル ログオンを許可」の項を参照してください。 ワークステーションおよびサーバーの既定値: Administrators、Backup Operators、Power Users、Users、Guest ドメイン コントローラーの既定値: Account Operators、Administrators、Backup Operators、Print Operators |
| 永続的共有オブジェクトの作成 | 誰もいない（空白） | このユーザーの権利は、オブジェクト マネージャーを使ってディレクトリ オブジェクトの作成にプロセスが使用するアカウントを決定します。 このユーザーの権利はオペレーティング システムによって内部的に使用され、オブジェクトの名前空間を拡張するカーネル モードのコンポーネントで使用できます。カーネル モードで実行されているコンポーネントには既にこのユーザーの権利が割り当てられているため、この権利を明示的に割り当てる必要はありません。 既定値: なし |
| 監査とセキュリティログの管理 | Administrators | このセキュリティ設定は、ファイル、Active Directory オブジェクト、レジストリ キーなど個別のリソースに対してオブジェクト アクセスの監査オプションを指定できるユーザーを決定します。 通常このセキュリティ設定は、ファイルとオブジェクトへのアクセスの監査を有効にすることをユーザーに許可しません。このような監査を有効にするには、コンピューターの構成\Windows の設定\セキュリティの設定\ローカル ポリシー\監査ポリシーで [オブジェクト アクセスの監査] 設定を構成する必要があります。 監査されたイベントは、イベント ビューアーのセキュリティ ログに表示できます。この特権を与えられているユーザーは、セキュリティ ログを表示および消去することもできます。 既定値: Administrators |
| 資格情報マネージャーに信頼された呼び出し側としてアクセス | 誰もいない（空白） | この設定は、バックアップ/復元の処理中に資格情報マネージャーで使用されます。これは Winlogon のみに割り当てられる特権です。いかなるアカウントにも付与しないでください。この特権を他のエンティティに付与すると、資格情報を保存したユーザーのセキュリティが侵害される可能性があります。 |
| 単一プロセスのプロファイル | Administrators | このセキュリティ設定は、パフォーマンス監視ツールを使用して、システム外のプロセスのパフォーマンスを監視できるユーザーを決定します。 既定値: Administrators、Power Users |
| 認証後にクライアントを偽装 | Administrators Local Service Network Service SERVICE | ユーザーにこの特権を割り当てると、そのユーザーに代わって実行されるプログラムがクライアントを偽装できるようになります。この種の偽装にこのユーザー権利が必要となるのは、権限のないユーザーが作成したサービスに (リモート プロシージャ コール (RPC) や名前付きパイプなどを使用して) クライアントを接続させ、次にそのクライアントを偽装することによって、管理者レベルまたはシステム レベルなど上位のアクセス許可を得ることを防ぐためです。 注意: このユーザー権利を割り当てると、セキュリティ上の問題が生じる可能性があります。このユーザー権利は、信頼できるユーザーのみに割り当ててください。 既定値:Administrators, Local Service, Network Service, Service 注意: 既定では、サービス コントロール マネージャーによって開始されるサービスのアクセス トークンにビルトインの Service グループが追加されます。コンポーネント オブジェクト モデル (COM) サーバーが COM インフラストラクチャによって起動され、特定のアカウントで実行するよう構成されている場合も、サーバーのアクセス トークンに Service グループが追加されます。その結果、これらのサービスが開始するときにこのユーザー権利が与えられます。 また、次の条件のいずれかに該当するときは、ユーザーがアクセス トークンを偽装できます。 偽装しようとしているアクセス トークンがそのユーザー用のものである。 このログオン セッションで、明示的な資格情報を使用してネットワークにログオンすることにより、ユーザーがアクセス トークンを作成した。 要求されるレベルが "匿名" や "識別" など、"偽装" より下である。 このような要因があるため、通常はユーザーがこのユーザー権利を必要とすることはありません。 詳細については、Microsoft プラットフォーム ソフトウェア開発キット (SDK) で "SeImpersonatePrivilege" を検索してください。 警告: この設定を有効にすると、以前に偽装の特権があったプログラムはこの特権を失い、実行しなくなる可能性があります。 |

### ・DC ローカルポリシー セキュリティ オプション

#### [セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[Microsoftネットワーククライアント]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| サードパーティ SMB サーバーへの接続に、暗号化されていないパスワードを送信する | 無効 | このセキュリティ設定を有効にすると、サーバー メッセージ ブロック (SMB) リダイレクターは、認証中のパスワード暗号化をサポートしていない、Microsoft 以外の SMB サーバーにテキスト形式のパスワードを送信することができます。 暗号化されていないパスワードの送信はセキュリティ上の危険があります。 既定値: 無効 |
| サーバーが同意すれば、通信にデジタル署名を行う | 有効 | このセキュリティ設定を使用して、SMB クライアントが SMB パケット署名のネゴシエートを試みるかどうかを決定します。 サーバー メッセージ ブロック (SMB) プロトコルは、Microsoft のファイルとプリンターの共有、およびリモート Windows 管理などの多くのネットワーク操作の基盤を提供します。転送中の SMB パケットを改ざんする man-in-the-middle アタックを防止するため、SMB プロトコルは SMB パケットのデジタル署名をサポートしています。このポリシー設定により、SMB クライアント コンポーネントが SMB サーバーに接続する際に、SMB パケット署名のネゴシエートを試みるかどうかが決定されます。 この設定を有効にすると、Microsoft ネットワーク クライアントは、セッション セットアップの際、サーバーに対して SMB パケット署名の実行を要求します。サーバー上でパケット署名が有効にされている場合は、パケット署名がネゴシエートされます。このポリシーを無効にすると、SMB クライアントは SMB パケット署名をネゴシエートしません。 既定値: 有効。 注意: すべての Windows オペレーティング システムにおいて、クライアント サイドの SMB コンポーネントおよびサーバー サイドの SMB コンポーネントの両方がサポートされています。Windows 2000 以降では、クライアント側およびサーバー側の SMB コンポーネントでのパケット署名の有効または要求は、次の 4 つのポリシー設定によって制御されます。 Microsoft ネットワーク クライアント: 常に通信にデジタル署名を行う - クライアント側 SMB コンポーネントがパケット署名を要求するかどうかを制御します。 Microsoft ネットワーク クライアント: サーバーが同意すれば、通信にデジタル署名を行う - クライアント側 SMB コンポーネントでパケット署名を有効にするかどうかを制御します。 Microsoft ネットワーク サーバー: 常に通信にデジタル署名を行う - サーバー側 SMB コンポーネントがパケット署名を要求するかどうかを制御します。 Microsoft ネットワーク サーバー: クライアントが同意すれば、通信にデジタル署名を行う - サーバー側 SMB コンポーネントでパケット署名を有効にするかどうかを制御します。 クライアント側とサーバー側の SMB 署名の両方が有効で、クライアントがサーバーへの SMB 1.0 接続を確立している場合、SMB 署名が試行されます。 SMB パケット署名を行うと、言語バージョン、OS バージョン、ファイル サイズ、プロセッサのオフロード機能、およびアプリケーションの IO 動作によって SMB のパフォーマンスが著しく低下する場合があります。この設定は、SMB 1.0 接続に対してのみ適用されます。 詳細については、<http://go.microsoft.com/fwlink/?LinkID=787136> を参照してください。 |
| 常に通信にデジタル署名を行う | 有効 | このセキュリティ設定を使用して、SMB クライアント コンポーネントがパケット署名を必要とするかどうかを決定します。 サーバー メッセージ ブロック (SMB) プロトコルは、Microsoft のファイルとプリンターの共有、およびリモート Windows 管理などの多くのネットワーク操作の基盤を提供します。転送中の SMB パケットを改ざんする man-in-the-middle アタックを防止するため、SMB プロトコルは SMB パケットのデジタル署名をサポートしています。このポリシー設定により、SMB サーバーとの以降の通信を許可するために SMB パケット署名をネゴシエートする必要があるかどうかが決定されます。 この設定を有効にすると、Microsoft ネットワーク クライアントは、SMB パケット署名を実行することに同意しない Microsoft ネットワーク サーバーとは通信しません。このポリシーを無効にすると、クライアントとサーバーとの間で SMB パケット署名がネゴシエートされます。 既定値: 無効。 重要: Windows 2000 を実行しているコンピューター上でこのポリシーを有効にするには、クライアント側のパケット署名も有効にされている必要があります。クライアント側 SMB パケット署名を有効にするには、"Microsoft ネットワーク クライアント: サーバーが同意すれば、通信にデジタル署名を行う" を設定します。 注意:すべての Windows オペレーティング システムにおいて、クライアント サイドの SMB コンポーネントおよびサーバー サイドの SMB コンポーネントの両方がサポートされています。Windows 2000 以降のオペレーティング システムでは、クライアント側およびサーバー側の SMB コンポーネントでのパケット署名の有効または要求は、次の 4 つのポリシー設定によって制御されます。 Microsoft ネットワーク クライアント: 常に通信にデジタル署名を行う - クライアント側 SMB コンポーネントがパケット署名を要求するかどうかを制御します。 Microsoft ネットワーク クライアント: サーバーが同意すれば、通信にデジタル署名を行う - クライアント側 SMB コンポーネントでパケット署名を有効にするかどうかを制御します。 Microsoft ネットワーク サーバー: 常に通信にデジタル署名を行う - サーバー側 SMB コンポーネントがパケット署名を要求するかどうかを制御します。 Microsoft ネットワーク サーバー: クライアントが同意すれば、通信にデジタル署名を行う - サーバー側 SMB コンポーネントでパケット署名を有効にするかどうかを制御します。 SMB パケット署名を行うと、言語バージョン、OS バージョン、ファイル サイズ、プロセッサのオフロード機能、およびアプリケーションの IO 動作によって SMB のパフォーマンスが著しく低下する場合があります。 詳細については、<http://go.microsoft.com/fwlink/?LinkID=787136> を参照してください。 |

#### [セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[Microsoftネットワークサーバー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| クライアントが同意すれば、通信にデジタル署名を行う | 有効 | このセキュリティ設定では、SMB サーバーが SMB パケット署名を要求するクライアントとの間で、SMB パケット署名のネゴシエートを行うかどうかを指定します。 サーバー メッセージ ブロック (SMB) プロトコルは、Microsoft のファイルとプリンターの共有、およびリモート Windows 管理などの多くのネットワーク操作の基盤を提供します。転送中の SMB パケットを改ざんする man-in-the-middle アタックを防止するため、SMB プロトコルは SMB パケットのデジタル署名をサポートしています。このポリシー設定により、SMB クライアントが SMB パケット署名を要求する場合に、SMB サーバーが SMB パケット署名のネゴシエートを行うかどうかを指定します。 この設定が有効な場合、Microsoft ネットワーク サーバーは、クライアントの要求があった場合に SMB パケット署名のネゴシエートを行います。つまり、クライアント側でパケット署名が有効になっている場合、パケット署名のネゴシエートが行われます。このポリシーが無効な場合、SMB クライアントは SMB パケット署名のネゴシエートを行いません。 既定値: ドメイン コントローラー側のみ有効 重要: Windows 2000 サーバーが Windows NT 4.0 クライアントとの間で署名のネゴシエートを行うには、Windows 2000 を実行するサーバー側で次のレジストリ値を 1 に設定する必要があります。HKLM\System\CurrentControlSet\Services\lanmanserver  \parameters\enableW9xsecuritysignature 注意: すべての Windows オペレーティング システムは、クライアント側 SMB コンポーネントとサーバー側 SMB コンポーネントの両方をサポートしています。Windows 2000 以降では、クライアント側およびサーバー側の SMB コンポーネントでのパケット署名の有効または要求は、次の 4 つのポリシー設定によって制御されます。 Microsoft ネットワーク クライアント: 常に通信にデジタル署名を行う - クライアント側 SMB コンポーネントがパケット署名を要求するかどうかを制御します。 Microsoft ネットワーク クライアント: サーバーが同意すれば、通信にデジタル署名を行う - クライアント側 SMB コンポーネントでパケット署名を有効にするかどうかを制御します。 Microsoft ネットワーク サーバー: 常に通信にデジタル署名を行う - サーバー側 SMB コンポーネントがパケット署名を要求するかどうかを制御します。 Microsoft ネットワーク サーバー: クライアントが同意すれば、通信にデジタル署名を行う - サーバー側 SMB コンポーネントでパケット署名を有効にするかどうかを制御します。 クライアント側とサーバー側の SMB 署名の両方が有効で、クライアントがサーバーへの SMB 1.0 接続を確立している場合、SMB 署名が試行されます。 SMB パケット署名を行うと、言語バージョン、OS バージョン、ファイル サイズ、プロセッサのオフロード機能、およびアプリケーションの IO 動作によって SMB のパフォーマンスが著しく低下する場合があります。この設定は、SMB 1.0 接続に対してのみ適用されます。 詳細については、<http://go.microsoft.com/fwlink/?LinkID=787136> を参照してください。 |
| 常に通信にデジタル署名を行う | 有効 | このセキュリティ設定を使用して、SMB サーバー コンポーネントがパケット署名を必要とするかどうかを決定します。 サーバー メッセージ ブロック (SMB) プロトコルは、Microsoft のファイルとプリンターの共有、およびリモート Windows 管理などの多くのネットワーク操作の基盤を提供します。転送中の SMB パケットを改ざんする man-in-the-middle アタックを防止するため、SMB プロトコルは SMB パケットのデジタル署名をサポートしています。このポリシー設定により、SMB クライアントとの以降の通信を許可するために SMB パケット署名をネゴシエートする必要があるかどうかが決定されます。 この設定を有効にすると、Microsoft ネットワーク サーバーは、SMB パケット署名を実行することに同意しない Microsoft ネットワーク クライアントとは通信しません。この設定を無効にすると、クライアントとサーバーとの間で SMB パケット署名がネゴシエートされます。既定値: メンバー サーバーでは無効。 ドメイン コントローラーでは有効。 注意: すべての Windows オペレーティング システムは、クライアント側 SMB コンポーネントとサーバー側 SMB コンポーネントの両方をサポートしています。Windows 2000 以降では、クライアント側およびサーバー側の SMB コンポーネントでのパケット署名の有効または要求は、次の 4 つのポリシー設定によって制御されます。 Microsoft ネットワーク クライアント: 常に通信にデジタル署名を行う - クライアント側 SMB コンポーネントがパケット署名を要求するかどうかを制御します。 Microsoft ネットワーク クライアント: サーバーが同意すれば、通信にデジタル署名を行う - クライアント側 SMB コンポーネントでパケット署名を有効にするかどうかを制御します。 Microsoft ネットワーク サーバー: 常に通信にデジタル署名を行う - サーバー側 SMB コンポーネントがパケット署名を要求するかどうかを制御します。 Microsoft ネットワーク サーバー: クライアントが同意すれば、通信にデジタル署名を行う - サーバー側 SMB コンポーネントでパケット署名を有効にするかどうかを制御します。 同様に、クライアント側 SMB 署名が要求される場合、クライアントは、パケット署名が有効にされていないサーバーとはセッションを確立できません。既定では、サーバー側 SMB 署名は、ドメイン コントローラー上でのみ有効にされています。 サーバー側 SMB 署名が有効にされている場合、クライアント側 SMB 署名が有効にされているクライアントとの間で SMB パケット署名がネゴシエートされます。 SMB パケット署名を行うと、言語バージョン、OS バージョン、ファイル サイズ、プロセッサのオフロード機能、およびアプリケーションの IO 動作によって SMB のパフォーマンスが著しく低下する場合があります。 重要: Windows 2000 を実行しているコンピューター上でこのポリシーを有効にするには、サーバー側のパケット署名も有効にされている必要があります。サーバー側 SMB パケット署名を有効にするには、次のポリシーを設定します。 Microsoft ネットワーク サーバー: サーバーが同意すれば、通信にデジタル署名を行う Windows 2000 サーバーが Windows NT 4.0 クライアントとの間で署名をネゴシエートするには、Windows 2000 サーバーで次のレジストリ値を 1 に設定する必要があります。 HKLM\System\CurrentControlSet\Services \lanmanserver\parameters\enableW9xsecuritysignature 詳細については、<http://go.microsoft.com/fwlink/?LinkID=787136> を参照してください。 |

#### [セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[アカウント]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Administrator アカウント名の変更 | 定義する "z-admin" などを定義する。 | このセキュリティ設定は、Administrator アカウントのセキュリティ識別子 (SID) に異なるアカウント名を関連付けるかどうかを決定します。既知の Administrator アカウント名を変更すると、承認されていないユーザーが、この特権のユーザー名とパスワードの組み合わせを推測しづらくなります。 既定値: Administrator 注意: 会社名、ドメイン名、それらの略称などの、推測しやすい文字列を含めないようにして下さい。 |
| Guest アカウントの状態 | 無効 | このセキュリティ設定は、Guest アカウントを有効にするか無効にするかを決定します。 既定値: 無効 注意: Guest アカウントが無効でセキュリティ オプション [ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル] に [Guest のみ] が設定されている場合、Microsoft ネットワーク サーバー (SMB サービス) などで実行されるネットワーク ログオンが失敗します。 |
| Guest アカウント名の変更 | 定義する "visitor" などを定義 | このセキュリティ設定は、"Guest" アカウントのセキュリティ識別子 (SID) に異なるアカウント名を関連付けるかどうかを決定します。既知の Guest アカウント名を変更すると、認証されていないユーザーが、このユーザー名とパスワードの組み合わせを推測しづらくなります。 既定値: Guest |
| ローカル アカウントの空のパスワードの使用をコンソールログオンのみに制限する | 有効 | このセキュリティ設定は、パスワードで保護されていないローカル アカウントを、そのコンピューター コンソール以外の場所から使用できるかどうかを決定します。この設定が有効な場合、パスワードで保護されていないローカル アカウントへログオンするには、そのコンピューターのキーボードを使用する必要があります。 既定値: 有効 警告: 物理的に安全でない場所にあるコンピューターでは、すべてのローカル ユーザー アカウントに対して常に強力なパスワード ポリシーを設定してください。そのようにしておかないと、コンピューターに物理的にアクセスできるユーザーが、パスワードが設定されていないユーザー アカウントを使用してログオンできるようになります。これは、ポータブル コンピューターを使用する場合は特に重要です。 このセキュリティ ポリシーを Everyone グループに適用すると、リモート デスクトップ サービスを使用したログオンができなくなります。 注意: この設定は、ドメイン アカウントを使用するログオンには影響しません。 リモートの対話型ログオンを使うアプリケーションでは、この設定を無効にすることができます。 注意: リモート デスクトップ サービスは、以前のバージョンの Windows Server でターミナル サービスと呼ばれていました。 |

#### [セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[システムオブジェクト]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 内部システムオブジェクトの既定のアクセス許可を強化する（例：シンボリックリンク） | 有効 | システム オブジェクト: 内部のシステム オブジェクトの既定のアクセス許可を強化する (例: シンボリック リンク) このセキュリティ設定は、オブジェクトに対する既定の随意アクセス制御リスト (DACL) を強化するかどうかを指定します。 Active Directory は共有システム リソース (例: DOS デバイス名、ミューテックス、セマフォ) のグローバル リストを管理しています。このようにして、プロセスの間オブジェクトの特定と共有が可能となっています。各オブジェクト タイプは、オブジェクトにアクセス可能なユーザーと付与されるアクセス許可を指定する、既定の DACL に基づいて作成されます。 このポリシーが有効な場合、既定の DACL はより強力で、管理者以外のユーザーは共有オブジェクトを読み取ることができますが、自身が作成者ではない共有オブジェクトは修正できません。 既定値: 有効。 |

#### [セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ドメインコントローラー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| LDAP サーバー署名必須 | 定義する[署名を必要とする] | このセキュリティ設定を使用して、LDAP サーバーが LDAP クライアントとの間で署名のネゴシエートを必要とするかどうかを決定します。次のオプションがあります。 なし: サーバーとバインドするためにデータ署名は必要ありません。クライアントがデータの署名を要求した場合はサーバーから提供されます。 署名属性の要求: TLS\SSL が使用される場合以外は、LDAP データ署名オプションをネゴシエートする必要があります。 既定値: このポリシーは定義されていないため、なしとして処理されます。 警告: サーバーに [署名属性の要求] を設定した場合は、クライアントも設定する必要があります。クライアントを設定しないと、サーバーとの接続が失われます。 注意: この設定は LDAP 簡易結合にも SSL 経由 LDAP 簡易結合にも影響しません。Windows XP Professional と共に出荷される Microsoft LDAP クライアントは、ドメイン コントローラーとの対話に LDAP 簡易結合も SSL 経由 LDAP 簡易結合も使用しません。 署名が必要とされる場合、LDAP 簡易結合と SSL 経由 LDAP 簡易結合の要求は拒否されます。Windows XP Professional または Windows Server 2003 ファミリで動作する Microsoft LDAP クライアントは、ディレクトリ サービスへのバインドに LDAP 簡易結合も SSL 経由 LDAP 簡易結合も使用しません。 |
| コンピューター アカウントのパスワードの変更を拒否する | 無効 | このセキュリティ設定を使用して、ドメイン コントローラーがメンバー コンピューターからのコンピューター アカウントのパスワード変更の要求を拒否するかどうかを決定します。既定では、メンバー コンピューターは 30 日ごとにコンピューター アカウントのパスワードを変更します。この設定を有効にすると、ドメイン コントローラーは、コンピューター アカウントのパスワードの変更要求を拒否します。 有効にした場合、ドメイン コントローラーは、コンピューター アカウントのパスワードに対するどのような変更も受け付けることができません。 既定値: このポリシーは定義されていないため、システムにより無効として処理されます。 |

#### [セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ドメインメンバー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| コンピュータ アカウント パスワード：定期的な変更を無効にする | 無効 | ドメイン メンバーがコンピューター アカウントのパスワードを定期的に変更するかどうかを決定します。この設定を有効にすると、ドメイン メンバーはコンピューター アカウントのパスワードの変更を試みません。この設定を無効にした場合、ドメイン メンバーは、"ドメイン メンバー: 最大コンピューター アカウントのパスワードの有効期間" の設定 (既定は 30 日間) に従って、コンピューター アカウントのパスワードの変更を試みます。 既定値: 無効。 注意: このセキュリティ設定は有効にすべきではありません。コンピューター アカウントのパスワードは、メンバーとドメイン コントローラー間、およびドメイン内ではドメイン コントローラーどうしの間で、セキュリティで保護されたチャネルの通信を確立するために使用されます。セキュリティで保護されたチャネルが確立されると、認証と承認の決定を行うために必要な機密情報の送信に使用されます。 この設定は、同じコンピューター アカウントを使用するデュアルブートのシナリオをサポートするために使用しないでください。同じドメインに参加している 2 つのインストールをデュアルブートする場合は、2 つのインストールに異なるコンピューター名を使用してください。 |
| 可能な場合、セキュリティで保護されたチャネルのデータをデジタル的に暗号化する | 有効 | このセキュリティ設定を使用して、ドメイン メンバーが、自身が開始した、セキュリティで保護されたチャネルのすべてのトラフィックの暗号化をネゴシエートするよう試みるかどうかを決定します。 コンピューターがドメインに参加すると、コンピューター アカウントが作成されます。その後システムが開始されると、そのコンピューター アカウントのパスワードを使用して、そのドメインのドメイン コントローラーとの間にセキュリティで保護されたチャネルが作成されます。このセキュリティで保護されたチャネルは、NTLM パススルー認証、LSA SID/名前参照などの操作に使用されます。 この設定により、ドメイン メンバーが、自身が開始したセキュリティで保護されたチャネルのすべてのトラフィックの暗号化をネゴシエートするよう試みるするかどうかが決定されます。有効にした場合、ドメイン メンバーは、セキュリティで保護されたチャネルのすべてのトラフィックの暗号化を要求します。ドメイン コントローラーが、セキュリティで保護されたチャネルのすべてのトラフィックの暗号化をサポートする場合は、セキュリティで保護されたチャネルのすべてのトラフィックが暗号化されます。そうでない場合は、セキュリティで保護されたチャネル上で送信されるログオン情報だけが暗号化されます。この設定を無効にすると、ドメイン メンバーは、セキュリティで保護されたチャネルの暗号化をネゴシエートするよう試みません。 既定値: 有効。 重要: 現在のところ、この設定を無効にする理由はありません。この設定を無効にすると、セキュリティで保護されたチャネルの潜在的な機密性レベルが不必要に低下するだけでなく、セキュリティで保護されたチャネルのスループットも不必要に低下することがあります。これは、セキュリティで保護されたチャネルを使用する同時 API コールは、セキュリティで保護されたチャネルが署名または暗号化されている場合のみ可能であるためです。 注意: ドメイン コントローラーはドメイン メンバーでもあり、同じドメイン内および信頼されるドメイン内のドメイン コントローラーとの間にセキュリティで保護されたチャネルを確立します。 |
| 可能な場合、セキュリティで保護されたチャネルのデータをデジタル的に署名する | 有効 | このセキュリティ設定を使用して、ドメイン メンバーが、自身が開始した、セキュリティで保護されたチャネルのすべてのトラフィックの署名をネゴシエートするよう試みるかどうかを決定します。 コンピューターがドメインに参加すると、コンピューター アカウントが作成されます。その後システムが開始されると、そのコンピューター アカウントのパスワードを使用して、そのドメインのドメイン コントローラーとの間にセキュリティで保護されたチャネルが作成されます。このセキュリティで保護されたチャネルは、NTLM パス スルー認証、LSA SID/名前参照などの操作に使用されます。 この設定により、ドメイン メンバーが、自身が開始したセキュリティで保護されたチャネルのすべてのトラフィックの署名をネゴシエートするよう試みるかどうかが決定されます。有効にした場合、ドメイン メンバーは、セキュリティで保護されたチャネルのすべてのトラフィックの署名を要求します。ドメイン コントローラーが、セキュリティで保護されたチャネルのすべてのトラフィックの署名をサポートする場合は、セキュリティで保護されたチャネルのすべてのトラフィックが署名され、それにより送信中の改ざんを防止できます。 既定値: 有効 注意: "ドメイン メンバー: 常にセキュリティで保護されたチャネルのデータをデジタル的に暗号化または署名する" ポリシーが有効にされている場合、このポリシーは、実際の設定に関係なく、有効にされていると見なされます。 ドメイン コントローラーはドメイン メンバーでもあり、同じドメイン内および信頼されるドメイン内のドメイン コントローラーとの間にセキュリティで保護されたチャネルを確立します。 |
| 最大コンピュータ アカウントのパスワードの有効期間 | 30 | このセキュリティ設定を使用して、ドメイン メンバーがコンピューター アカウントのパスワードの変更を試みる頻度を決定します。 既定値: 30 日間。 重要:この設定は Windows 2000 コンピューターにも適用されますが、それらのコンピューターで使用しているセキュリティの構成マネージャー ツールを通じて使用することはできません。 |
| 常にセキュリティで保護されたチャネルのデータをデジタル的に暗号化または署名する | 有効 | このセキュリティ設定は、ドメインメンバーによって開始されたすべてのセキュリティで保護されたチャネルトラフィックを署名または暗号化する必要があるかどうかを決定します。この設定は、ドメインメンバーによって開始されたすべてのセキュアチャネルトラフィックが最小セキュリティ要件を満たしているかどうかを決定します。具体的には、ドメインメンバーによって開始されたすべてのセキュリティで保護されたチャネルトラフィックを署名または暗号化する必要があるかどうかを決定します。このポリシーが有効になっている場合、すべてのセキュアチャネルトラフィックの署名または暗号化がネゴシエートされない限り、セキュアチャネルは確立されません。このポリシーを無効にすると、すべてのセキュリティで保護されたチャネルトラフィックの暗号化と署名がドメインコントローラーとネゴシエートされます。この場合、署名と暗号化のレベルはドメインコントローラーのバージョンと次の2つのポリシーの設定によって異なります。 -ドメインメンバー：セキュリティで保護されたチャネルデータをデジタルで暗号化する（可能な場合） -ドメインメンバー：セキュリティで保護されたチャネルデータにデジタルで署名する（可能な場合） |
| 強力な（Windows 2000かそれ以降のバージョン）セッションキーを必要とする | 有効 | このセキュリティ設定を使用して、セキュリティで保護されたチャネル データの暗号化に、128 ビット キーの強度を必要とするかどうかを決定します。 コンピューターがドメインに参加すると、コンピューター アカウントが作成されます。その後システムが開始されると、そのコンピューター アカウントのパスワードを使用して、そのドメインのドメイン コントローラーとの間にセキュリティで保護されたチャネルが作成されます。このセキュリティで保護されたチャネルは、NTLM パススルー認証、LSA SID/名前参照などの操作に使用されます。 ドメイン メンバーの通信相手であるドメイン コントローラーで実行されている Windows のバージョンと、パラメーターの設定に依存します: ドメイン メンバー: 常にセキュリティで保護されたチャネルのデータをデジタル的に暗号化または署名する ドメイン メンバー: 可能な場合、セキュリティで保護されたチャネルのデータをデジタル的に暗号化する セキュリティで保護されたチャネル上で送信される情報の一部またはすべてが暗号化されます。このポリシー設定により、暗号化される、セキュリティで保護されたチャネルの情報に 128 ビット キーの強度が必要とされるかどうかが決定されます。 この設定を有効にすると、128 ビットの暗号化が実行可能でない限りセキュリティで保護されたチャネルは確立されません。この設定を無効にすると、キーの強度はドメイン コントローラーとの間でネゴシエートされます。既定値: 有効。 重要: メンバーのワークステーションとサーバーでこのポリシーの利点を活用するには、メンバーのドメインを構成するすべてのドメイン コントローラーで Windows 2000 以降を実行している必要があります。 ドメイン コントローラーでこのポリシーの利点を活用するには、同じドメイン内とすべての信頼されるドメイン内のすべてのドメイン コントローラーで Windows 2000 以降を実行している必要があります。 |

#### [セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ネットワークアクセス]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Everyone のアクセス許可を匿名ユーザーに適用する | 無効 | このセキュリティ設定は、このコンピューターへの匿名接続に対して与える、追加のアクセス許可の内容を指定します。 Windows では、ドメイン アカウントやネットワーク共有の名前の列挙など、一定の操作が匿名ユーザーに許可されます。これは、たとえば、相互の信頼が維持されていない、信頼されるドメインのユーザーに対して管理者がアクセスを許可したい場合に便利です。既定では、匿名接続に対して作成されたトークンから、Everyone セキュリティ識別子 (SID) が削除されます。そのため、Everyone グループに与えられたアクセス許可は、匿名ユーザーには適用されません。このオプションが設定されている場合、匿名ユーザーは、明示的にアクセス許可が与えられているリソースのみアクセスできます。 このポリシーを有効にすると、匿名接続に対して作成されたトークンに Everyone の SID が追加されます。この場合、Everyone グループにアクセス許可が与えられているリソースであれば、匿名ユーザーはアクセスできます。 既定値: 無効。 |
| SAM アカウントおよび共有の匿名の列挙を許可しない | 有効 | このセキュリティ設定は、SAM アカウントおよび共有の、匿名による列挙を許可するかどうかを指定します。 Windows では、ドメイン アカウントやネットワーク共有の名前の列挙など、一定の操作が匿名ユーザーに許可されます。これは、たとえば、相互の信頼が維持されていない、信頼されるドメインのユーザーに対して管理者がアクセスを許可したい場合に便利です。SAM アカウントおよび共有の匿名による列挙を許可したくない場合は、このポリシーを有効にしてください。 既定値: 無効。 |
| SAM アカウントの匿名の列挙を許可しない | 有効 | このセキュリティ設定は、このコンピューターへの匿名接続に対して与える、追加のアクセス許可の内容を指定します。 Windows では、ドメイン アカウントやネットワーク共有の名前の列挙など、一定の操作が匿名ユーザーに許可されます。これは、たとえば、相互の信頼が維持されていない、信頼されるドメインのユーザーに対して管理者がアクセスを許可したい場合に便利です。 このセキュリティ オプションでは、匿名の接続に対して、次に示す制限を追加できます。 有効: SAM アカウントの列挙を許可しない。このオプションでは、リソースに関するセキュリティのアクセス許可について、Everyone ではなく Authenticated Users の設定が使用されます。 無効: 制限を追加しません。既定のアクセス許可に依存します。 ワークステーション側の既定値: 有効 サーバー側の既定値: 無効重要: このポリシーは、ドメイン コントローラーには影響を与えません。 |
| 匿名の SID と名前の変換を許可する | 無効 | このポリシー設定は、匿名ユーザーが他のユーザーのセキュリティ識別子 (SID) 属性を要求できるかどうかを指定します。 このポリシーが有効な場合、匿名ユーザーは別のユーザーの SID 属性を要求できます。管理者の SID を知っている匿名ユーザーは、このポリシーが有効になっているコンピューターにアクセスして、管理者の名前を取得することが可能になります。この設定は、SID から名前への変換にも、名前から SID の変換にも影響します。 このポリシー設定が無効な場合、匿名ユーザーは他のユーザーの SID 属性を要求することはできません。 ワークステーションおよびメンバー サーバーの既定値: 無効 Windows Server 2008 またはそれ以降を実行するドメイン コントローラーの既定値: 無効 Windows Server 2003 R2 またはそれ以前を実行するドメイン コントローラーの既定値: 有効 |
| 名前付きパイプと共有への匿名のアクセスを制限する | 有効 | このセキュリティ設定を有効にすると、次に示す設定に関して、共有およびパイプに対する匿名アクセスを制限します。 ネットワーク アクセス: 匿名でアクセス可能な名前付きパイプ ネットワーク アクセス: 匿名でアクセス可能な共有 既定値: 有効。 |

#### [セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ネットワークセキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Kerberos で許可する暗号化の種類を構成する | DES\_CBC\_CRC:無効DES\_CBC\_MD5:無効RC4\_HMAC\_MD5:無効AES128\_HMAC\_SHA1:有効AES256\_HMAC\_SHA1:有効将来使用する暗号化の種類:有効 | このポリシー設定を使用すると、Kerberos での使用を許可する暗号化の種類を設定できます。 選択していない暗号化の種類は許可されません。この設定はクライアント コンピューターまたはサービスとアプリケーションの互換性に影響することがあります。暗号化の種類は複数選択することもできます。 このポリシーは、Windows 7 および Windows Server 2008 R2 以降でサポートされます。 |
| LAN Manager 認証レベル | NTLMv2 応答のみを送信 (LMとNTLMを拒否する) | このセキュリティ設定は、ネットワーク ログオンに使用するチャレンジ/レスポンス認証プロトコルを指定します。この設定の選択肢は、クライアントが使用する認証プロトコルのレベル、ネゴシエーションが行われるセッション セキュリティのレベル、およびサーバーが受け付ける認証のレベルに影響します。選択肢は次のとおりです。 LM と NTLM 応答を送信する: クライアントは LM 認証および NTLM 認証を使用し、NTLMv2 セッション セキュリティは使用しません。ドメイン コントローラーは、LM 認証、NTLM 認証、および NTLMv2 認証を受け付けます。 LM と NTLM を送信する - ネゴシエーションの場合、NTLMv2 セッション セキュリティを使う: クライアントは LM 認証と NTLM 認証を使用し、サーバーでサポートされている場合は NTLMv2 セッション セキュリティを使用します。ドメイン コントローラーは、LM 認証、NTLM 認証、および NTLMv2 認証を受け付けます。 NTLM 応答のみ送信する: クライアントは NTLM 認証のみを使用し、サーバーでサポートされている場合は NTLMv2 セッション セキュリティを使用します。ドメイン コントローラーは、LM 認証、NTLM 認証、および NTLMv2 認証を受け付けます。 NTLMv2 応答のみ送信する: クライアントは NTLMv2 認証のみを使用し、サーバーでサポートされている場合は NTLMv2 セッション セキュリティを使用します。ドメイン コントローラーは、LM 認証、NTLM 認証、および NTLMv2 認証を受け付けます。 NTLMv2 応答のみ送信\ (LM を拒否する): クライアントは NTLMv2 認証のみを使用し、サーバーでサポートされている場合は NTLMv2 セッション セキュリティを使用します。ドメイン コントローラーは、LM を拒否し、NTLM 認証と NTLMv2 認証のみを受け付けます。 NTLMv2 応答のみ送信 (LM と NTLM を拒否する): クライアントは NTLMv2 認証のみを使用し、サーバーでサポートされている場合は NTLMv2 セッション セキュリティを使用します。ドメイン コントローラーは、LM と NTLM を拒否し、NTLMv2 認証のみを受け付けます。 重要: この設定は、ネットワークを経由して Windows NT 4.0 またはそれ以前を実行するコンピューターとネットワークを経由して通信する場合に、Windows 2000 Server、Windows 2000 Professional、Windows XP Professional、および Windows Server 2003 ファミリを実行するコンピューターの性能に悪影響を及ぼす場合があります。たとえば、現時点では Windows NT 4.0 SP4 またはそれ以前を実行するコンピューターは NTLMv2 をサポートしていません。Windows 95 または Windows 98 を実行するコンピューターは NTLM をサポートしていません。 既定値: Windows 2000 および Windows XP: LM と NTLM 応答を送信する Windows Server 2003: NTLM 応答のみ送信するWindows Vista、Windows Server 2008、Windows 7 および Windows Server 2008 R2: NTLMv2 応答のみ送信する |
| LocalSystem による NULL セッション フォールバックを許可する | 無効 | NTLM を LocalSystem で使用する場合に NULL セッションへのフォールバックを許可します。既定値は、Windows Vista 以前の場合は TRUE、Windows 7 の場合は FALSE です。 |
| NTLM SSP ベース (セキュア RPC を含む) のクライアント向け最小セッション セキュリティ | NTLMv2セッションセキュリティが必要、128ビット暗号化が必要 | このセキュリティ設定では、128 ビット暗号化と NTLMv2 セッション セキュリティのどちらかまたはその両方のネゴシエーションを、クライアントが要求することができます。必要なネゴシエーションは、LAN Manager 認証レベルのセキュリティ設定値によって決まります。次のオプションがあります: NTLMv2 セッション セキュリティが必要: NTLMv2 プロトコルでネゴシエーションが行われなければ、接続が失敗します。 128 ビット暗号化が必要: 強力な暗号化 (128 ビット) によるネゴシエーションが行われない場合は、接続が失敗します。 既定値: Windows XP、Windows Vista、Windows 2000 Server、Windows Server 2003、および Windows Server 2008: 必要なし Windows 7 および Windows Server 2008 R2: 128 ビット暗号化が必要 |
| NTLM SSP ベース (セキュア RPC を含む) のサーバー向け最小セッション セキュリティ | NTLMv2セッションセキュリティが必要、128ビット暗号化が必要 | このセキュリティ設定では、128 ビット暗号化と NTLMv2 セッション セキュリティのどちらかまたはその両方のネゴシエーションを、クライアントが要求することができます。必要なネゴシエーションは、LAN Manager 認証レベルのセキュリティ設定値によって決まります。次のオプションがあります: NTLMv2 セッション セキュリティが必要: メッセージの整合性でネゴシエーションが行われない場合は、接続が失敗します。 128 ビット暗号化が必要: 強力な暗号化 (128 ビット) によるネゴシエーションが行われない場合は、接続が失敗します。 既定値: Windows XP、Windows Vista、Windows 2000 Server、Windows Server 2003、および Windows Server 2008: 必要なし Windows 7 および Windows Server 2008 R2: 128 ビット暗号化が必要 |
| NTLM で Local System によるコンピューター ID の使用を許可する | 有効 | このポリシー設定を使用すると、Negotiate を使用するローカル システム サービスが NTLM 認証にフォールバックするときにコンピューター ID を使用することを許可できます。 このポリシー設定を有効にした場合、Local System として実行され、Negotiate を使用するサービスは、コンピューター ID を使用します。その結果、Windows オペレーティング システム間で行われる一部の認証要求が失敗し、エラーが記録される可能性があります。 このポリシー設定を無効にした場合、Local System として実行され、NTLM 認証にフォールバックするときに Negotiate を使用するサービスは、匿名で認証されます。 Windows 7 以降では、このポリシーは既定で有効になっています。 Windows Vista では、このポリシーは既定で無効になっています。 このポリシーは、Windows Vista および Windows Server 2008 以降でサポートされます。 注意: Windows Vista または Windows Server 2008 では、この設定はグループ ポリシーに公開されていません。 |
| オンライン ID を使用するためのこのコンピューターへの PKU2U 認証要求を許可する | 無効 | このポリシーは、ドメインに参加しているコンピューターでは既定でオフになります。オフの場合、ドメインに参加しているコンピューターに対してオンライン ID による認証は実行されません。 注意: Windows Serverでは、KU2Uはデフォルトで無効になっています。ハイブリッドAzure ADに参加したサーバーからAzure ADに参加したWindows 10デバイス、またはハイブリッドAzure ADに参加したドメインメンバーWindows 10デバイスへのリモートデスクトップ接続が失敗します。これを解決するには、サーバーでPKU2Uを有効にします。 [[25]](#footnote-25) |
| 必須の署名をしている LDAP クライアント | 定義する ネゴシエーション署名 | このセキュリティ設定は、LDAP BIND 要求を発行するクライアントの代わりに要求されているデータ署名のレベルを指定します。設定できるレベルは次のとおりです。 なし: LDAP BIND 要求は、呼び出し側が指定したオプションで発行されます。 ネゴシエーション署名: Transport Layer Security/Secure Sockets Layer (TLS\SSL) が開始されていない場合、LDAP BIND 要求は、呼び出し側が指定したオプションに加え、LDAP データ署名オプション セットを指定して開始されます。TLS\SSL が既に開始されている場合、LDAP BIND 要求は、呼び出し側が指定したオプションで開始されます。 署名属性の要求: [ネゴシエーション署名] と同じですが、LDAP トラフィック署名が必要であることを LDAP サーバーの中間 saslBindInProgress 応答が示していない場合、呼び出し側には LDAP BIND コマンド要求が失敗したことが通知されます。 警告: サーバーに [署名属性の要求] を設定した場合は、クライアントの設定も必要です。クライアントを設定しないと、サーバーとの接続が失われます。 注意: この設定は、ldap\_simple\_bind および ldap\_simple\_bind\_s には影響ありません。Windows XP Professional に含まれている Microsoft LDAP クライアントは、ドメイン コントローラーとの通信には、ldap\_simple\_bind および ldap\_simple\_bind\_s を使用しません。 既定値: ネゴシエーション署名。 |
| 次回のパスワード変更時に LAN Manager のハッシュ値を保存しない | 有効 | このセキュリティ設定は、次回パスワードを変更するときに、変更後のパスワードに対する LAN Manager (LM) のハッシュ値を保存するかどうかを指定します。LM ハッシュは、暗号化の面でより強力な Windows NT のハッシュと比較すると、ぜい弱で攻撃に弱いという性質があります。LM ハッシュはローカル コンピューターのセキュリティ データベースに保存されるため、セキュリティ データベースが攻撃されると、パスワードが漏えいするおそれがあります。Windows Vista 以降の既定値: 有効 Windows XP の既定値: 無効 重要: Windows 2000 Service Pack 2 (SP2) 以降では、認証方法について、Microsoft Windows NT 4.0 など、旧バージョンの Windows との互換性が確保されています。 この設定は、Windows 95 または Windows 98 を実行するコンピューターと通信する場合、Windows 2000 Server、Windows 2000 Professional、Windows XP、および Windows Server 2003 ファミリを実行するコンピューターの性能に悪影響を及ぼす場合があります。 |

#### [セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ユーザーアカウント制御]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| UIAccess アプリケーションで、セキュリティで保護されたデスクトップを使用せずに昇格のプロンプトを表示できるようにする | 無効 | このポリシー設定は、標準ユーザーによって使用される、セキュリティで保護されたデスクトップによる昇格時のプロンプトを、ユーザー インターフェイス アクセシビリティ (UIAccess または UIA) プログラムが自動的に無効にできるかどうかを決定します。 有効: Windows リモート アシスタンスなどの UIA プログラムにより、セキュリティで保護されたデスクトップでの昇格時のプロンプト表示が自動的に無効にされます。[ユーザー アカウント制御: 昇格のプロンプト時にセキュリティで保護されたデスクトップに切り替える] ポリシー設定を無効にしていない場合、セキュリティで保護されたデスクトップではなく、対話ユーザーのデスクトップにプロンプトが表示されます。 無効: (既定値) セキュリティで保護されたデスクトップは、対話型デスクトップのユーザーによって、または [ユーザー アカウント制御: 昇格のプロンプト時にセキュリティで保護されたデスクトップに切り替える] ポリシー設定を無効にすることによってのみ無効にできます。 |
| アプリケーションのインストールを検出し、昇格をプロンプトする | 有効 | このポリシー設定は、コンピューターへのアプリケーションのインストールを検出したときの動作を決定します。次のオプションがあります。 有効: (既定値) インストールするために特権の昇格を必要とするアプリケーションのインストール パッケージを検出した場合、管理ユーザーの名前とパスワードの入力を求めるプロンプトを表示します。有効な資格情報が入力された場合は、その管理ユーザーに適用される特権で操作を実行します。 無効: アプリケーションのインストール パッケージを検出せず、昇格を求めるプロンプトも表示しません。標準ユーザー デスクトップを実行し、Group Policy Software Install や Systems Management Server (SMS) のような委任されたインストール技術を使用する企業では、このポリシー設定を無効にしてください。そのような場合には、インストーラーの検出は必要ありません。 |
| ビルトイン Administrator アカウントのための管理者承認モードを使用する | 有効 | このポリシー設定は、ビルトイン Administrator アカウントのための管理者承認モードの動作を決定します。次のオプションがあります。 有効: ビルトイン Administrator アカウントは管理者承認モードを使用します。既定では、特権の昇格を必要とする操作が試みられた場合はすべて、ユーザーに操作の承認を求めるメッセージを表示します。 無効: (既定値) ビルトイン Administrator アカウントはすべてのアプリケーションを完全な管理者特権で実行します。 |
| 安全な場所にインストールされている UIAccess アプリケーションの昇格のみ | 有効 | このポリシー設定は、ユーザー インターフェイス アクセシビリティ (UIAccess) 整合性レベルでの実行を必要とするアプリケーションが、ファイル システム内の安全な場所に存在する必要があるかどうかを決定します。安全な場所は、次のディレクトリに限定されます。 - …\Program Files\、サブディレクトリを含む - …\Windows\system32\ - …\Program Files (x86)\、64 ビット バージョンの Windows のサブディレクトリを含む 注意: Windows は、このセキュリティ設定の状態にかかわらず、UIAccess 整合性レベルでの実行を必要とする対話型アプリケーションすべてにおいて、公開キー基盤 (PKI) 署名チェックを強制します。 次のオプションがあります。有効: (既定値) アプリケーションは、ファイル システム内の安全な場所に存在する場合のみ、UIAccess 整合性レベルで実行されます。 無効: アプリケーションは、ファイル システム内の安全な場所に存在していなくても、UIAccess 整合性レベルで実行されます。 |
| 各ユーザーの場所へのファイルまたはレジストリの書き込みエラーを仮想化する | 有効 | このポリシー設定は、アプリケーションによる書き込みエラーが、定義されたレジストリおよびファイル システムの場所にリダイレクトされるかどうかを決定します。このポリシー設定は、管理者として実行される、実行時アプリケーション データを %ProgramFiles%、%Windir%、%Windir%\system32、または HKLM\Software に書き込むアプリケーションの問題を緩和します。次のオプションがあります。 有効: (既定値) ファイル システムとレジストリについて、アプリケーションの実行時の書き込みエラーを定義済みのユーザーの場所へリダイレクトします。 無効: 保護された場所にデータを書き込むアプリケーションは失敗します。 |
| 管理者承認モードですべての管理者を実行する | 有効 | このポリシー設定は、コンピューターのユーザー アカウント制御 (UAC) ポリシー設定の動作を決定します。このポリシー設定を変更した場合は、コンピューターを再起動する必要があります。次のオプションがあります。 有効: (既定値) 管理者承認モードが有効になっています。ビルトイン Administrator アカウントと、Administrators グループに属するその他のすべてのユーザーを管理者承認モードで実行できるようにするには、このポリシーが有効になっていること、関連する UAC ポリシー設定が適切に設定されていることが必要です。 無効: 管理者承認モードと、関連する UAC ポリシーの設定すべてが無効になっています。 注意: このポリシー設定が無効な場合、オペレーティング システムの全体的なセキュリティが低下したことが、セキュリティ センターから通知されます。 |
| 管理者承認モードでの管理者に対する昇格時のプロンプトの動作 | 有効セキュリティで保護されたデスクトップで同意を要求する | このポリシー設定は、管理者承認モードでの管理者に対する昇格時のプロンプトの動作を決定します。次のオプションがあります。 確認を要求しないで昇格する: 特権のあるアカウントに対して、特権の昇格を必要とする操作を、同意または資格情報を要求せずに実行することを許可します。 注意: このオプションは、最も制約の厳しい環境でのみ使用するようにしてください。 セキュリティで保護されたデスクトップで資格情報を要求する: 特権の昇格を必要とする操作が試みられた場合、セキュリティで保護されたデスクトップに、特権のあるユーザーの名前とパスワードの入力を求めるプロンプトを表示します。有効な資格情報が入力された場合は、そのユーザーが利用できる最高の特権で操作を続行します。 セキュリティで保護されたデスクトップで同意を要求する: 特権の昇格を必要とする操作が試みられた場合、セキュリティで保護されたデスクトップに、[許可] または [拒否] を選択するように求めるプロンプトを表示します。[許可] が選択された場合は、そのユーザーが利用できる最高の特権で操作を続行します。 資格情報を要求する: 特権の昇格を必要とする操作が試みられた場合、管理ユーザーの名前とパスワードの入力を求めるプロンプトを表示します。有効な資格情報が入力された場合は、その管理ユーザーに適用される特権で操作を実行します。 同意を要求する: 特権の昇格を必要とする操作が試みられた場合、[許可] または [拒否] を選択するように求めるプロンプトを表示します。[許可] が選択された場合は、そのユーザーが利用できる最高の特権で操作を続行します。 Windows 以外のバイナリに対する同意を要求する: (既定値) Windows 以外のアプリケーションで特権の昇格を必要とする操作が試みられた場合、セキュリティで保護されたデスクトップに、[許可] または [拒否] を選択するように求めるプロンプトを表示します。[許可] が選択された場合は、そのユーザーが利用できる最高の特権で操作を続行します。 |
| 標準ユーザーに対する昇格時のプロンプトの動作 | 昇格の要求を自動的に拒否する | このポリシー設定は、標準ユーザーに対する昇格時のプロンプトの動作を決定します。次のオプションがあります。 資格情報を要求する: (既定値) 特権の昇格を必要とする操作が試みられた場合、管理ユーザーの名前とパスワードの入力を求めるプロンプトを表示します。有効な資格情報が入力された場合は、その管理ユーザーに適用される特権で操作を実行します。 昇格の要求を自動的に拒否する: 特権の昇格を必要とする操作が試みられた場合、構成可能なアクセス拒否エラー メッセージを表示します。デスクトップを標準ユーザーとして実行している企業は、ヘルプ デスクへの電話の数を削減するために、このオプションを選択した方がよい場合があります。 セキュリティで保護されたデスクトップで資格情報を要求する: 特権の昇格を必要とする操作が試みられた場合、セキュリティで保護されたデスクトップに、別のユーザーの名前とパスワードの入力を求めるプロンプトを表示します。有効な資格情報が入力された場合は、そのユーザーに適用される特権で操作を続行します。 |

#### [セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[監査]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 監査ポリシーサブカテゴリ設定（Windows Vista以降）を強制して、監査ポリシー カテゴリ設定を上書する | 有効 | Windows Vista 以降の Windows バージョンでは、監査ポリシーのサブカテゴリを使用して、より厳密に監査ポリシーを管理できます。カテゴリ レベルで監査ポリシーを設定すると、この新しいサブカテゴリ監査ポリシー機能が上書きされます。グループ ポリシーではカテゴリ レベルにおいてのみ監査ポリシーを設定できるため、新しいコンピューターがドメインに参加したときや Windows Vista 以降のバージョンにアップグレードしたときには、それらのコンピューターのサブカテゴリ設定よりも既存のグループ ポリシーが優先される可能性があります。グループ ポリシーを変更することなく、サブカテゴリを使用して監査ポリシーを管理できるようにするには、Windows Vista 以降のバージョンでは、新しいレジストリ値 SCENoApplyLegacyAuditPolicy を使用します。これにより、グループ ポリシーおよびローカル セキュリティ ポリシー管理ツールによってカテゴリ レベルの監査ポリシーが適用されるのを防ぐことができます。ここで設定されたカテゴリ レベルの監査ポリシーが、現在生成されているイベントと矛盾する場合、原因としてこのレジストリ キーが設定されていることが考えられます。 既定値: 有効 |

#### [セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[対話型ログオン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| キャッシュする過去のログオン数 (ドメイン コントローラーが使用できない場合) | 10 | 一意なユーザーのログオン情報をそれぞれローカルにキャッシュし、その後のログオン試行中にドメイン コントローラーが使用できない場合でもログオンできるようにします。キャッシュされるログオン情報は過去のログオン セッションから保存されます。ドメイン コントローラーが使用できない場合、ユーザーのログオン情報がキャッシュされていないと、ユーザーに次のようなメッセージが表示されます。現在、ログオン要求を処理できるログオン サーバーはありません。 このポリシーに 0 を設定すると、ログオン情報はキャッシュされません。50 より大きな値を設定しても、キャッシュされるログオン試行情報は 50 回までです。Windows では、最大 50 のキャッシュ エントリをサポートし、各ユーザーによって使用されるエントリの数は、資格情報によって異なります。たとえば、Windows システムではユーザーごとに最大 50 の一意のパスワードをキャッシュできますが、スマート カードのユーザー アカウントの場合は、パスワード情報とスマート カード情報の両方が保存されるため、25 のスマート カード ユーザー アカウントしかキャッシュできません。キャッシュされたログオン情報を持つユーザーがもう一度ログオンすると、ユーザーの個々のキャッシュ情報が置き換えられます。 既定値: Windows Server 2008: 25 他のすべてのバージョン: 10 |
| コンピューターの非アクティブ状態の上限 | 900 | Windows ではログオン セッションの非アクティブ状態が通知され、非アクティブ状態の時間が非アクティブ状態の上限を超えると、スクリーン セーバーが作動し、セッションがロックされます。 既定値: 適用しない。 |
| スマート カード取り出し時の動作 | ワークステーションをロックする | このセキュリティ設定を使用して、ログオンしているユーザーのスマート カードがスマート カード リーダーから取り外されたときの動作を決定します。次のオプションがあります。 何もしない ワークステーションをロックする ログオフを強制する リモート デスクトップ サービスのセッションである場合に切断する このポリシーの [プロパティ] ダイアログ ボックスで [ワークステーションをロックする] をクリックすると、スマート カードが取り外されたときにワークステーションがロックされます。これによりユーザーは、その場を離れるときにスマート カードを取り外して持ち歩くことで、保護されたセッションを維持できます。このポリシーの [プロパティ] ダイアログ ボックスで [ログオフを強制する] をクリックすると、スマート カードが取り外されたときにユーザーが自動的にログオフされます。[リモート デスクトップ サービスのセッションである場合に切断する] をクリックすると、スマート カードが取り外されたときに、ユーザーをログオフせずにセッションが切断されます。これにより、ユーザーは後で、または別のスマート カード リーダーが装備されたコンピューターで、再びログオンする必要なくスマート カードを挿入してセッションを再開することができます。セッションがローカルの場合、このポリシーは [ワークステーションをロックする] と同様に機能します。 注意: リモート デスクトップ サービスは、以前のバージョンの Windows Server でターミナル サービスと呼ばれていました。 既定値: このポリシーは定義されておらず、[何もしない] が設定されているものとして扱われます。 Windows Vista 以降: この設定が動作するには、スマート カードの取り出しポリシー サービスが開始されている必要があります。 |

### ・DC 監査ポリシーの詳細な構成

#### [監査ポリシーの詳細な構成]>[監査ポリシー]>[アカウントログオン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 資格情報の確認の監査 | 成功、失敗 | このポリシー設定を使用すると、ユーザー アカウント ログオン資格情報に対する検証テストによって生成されたイベントを監査できます。 このサブカテゴリのイベントは、その資格情報に対する権限を持つコンピューター上でのみ発生します。ドメイン アカウントの場合は、ドメイン コントローラーが権限を持ちます。ローカル アカウントの場合は、ローカル コンピューターが権限を持ちます。 ボリューム: ドメイン コントローラーでは "高"。 クライアント エディションの既定値: 監査なし サーバー エディションの既定値: 成功 |

#### [監査ポリシーの詳細な構成]>[監査ポリシー]>[アカウント管理]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| コンピューター アカウントの管理 | 成功 | このポリシー設定を使用すると、コンピューター アカウントの作成、変更、または削除など、コンピューター アカウントの変更によって生成されるイベントを監査できます。 このポリシー設定を構成すると、コンピューター アカウントの変更操作が試みられた場合に監査イベントが生成されます。成功の監査では成功した操作が、失敗の監査では成功しなかった操作が記録されます。 このポリシー設定を構成しないと、コンピューター アカウントが変更された場合に、監査イベントは生成されません。 ボリューム: 低 クライアント エディションの既定値: 監査なし サーバー エディションの既定値: 成功 |
| その他のアカウント管理イベント | 成功 | このポリシー設定を使用すると、次のような、このカテゴリに含まれないその他のユーザー アカウントの変更によって生成されるイベントを監査できます。 ユーザー アカウントのパスワード ハッシュへのアクセス。これは通常、Active Directory 管理ツールのパスワードの移行中に発生します。 パスワード ポリシー確認 API の呼び出し。この関数の呼び出しは、悪意のあるアプリケーションが、パスワード辞書攻撃中の操作数を削減するためにポリシーをテストする場合に、攻撃の一環として実行される可能性があります。 |
| セキュリティ グループの管理の監査 | 成功 | セキュリティグループの作成、変更、削除、メンバーの追加または削除、グループタイプの変更など、セキュリティグループの変更によって生成されるイベントを監査します。 |
| ユーザー アカウントの管理の監査 | 成功と失敗 | このポリシー設定を使用すると、ユーザー アカウントの変更を監査できます。イベントは次のとおりです。 ユーザー アカウントの作成、変更、削除、名前の変更、無効化、有効、ロックアウト、またはロック解除 ユーザー アカウントのパスワードの設定または変更 ユーザー アカウントの SID 履歴へのセキュリティ識別子 (SID) の追加 ディレクトリ サービス復元モードのパスワードの構成 管理者ユーザーのアクセス許可の変更 資格情報マネージャーの資格情報のバックアップまたは復元 このポリシー設定を構成すると、ユーザー アカウントの変更操作が試みられた場合に監査イベントが生成されます。成功の監査では成功した操作が、失敗の監査では成功しなかった操作が記録されます。このポリシー設定を構成しないと、ユーザー アカウントが変更された場合に、監査イベントは生成されません。 ボリューム: 低 既定値: 成功 |

#### [監査ポリシーの詳細な構成]>[監査ポリシー]>[詳細追跡]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| PNP アクティビティの監査 | 成功 | このポリシー設定を使用すると、プラグ アンド プレイが外部デバイスを検出したときに監査できます。 このポリシー設定を構成すると、プラグ アンド プレイが外部デバイスを検出するたびに監査イベントが生成されます。成功した監査だけが、このカテゴリに記録されます。 このポリシー設定を構成しないと、プラグ アンド プレイによって外部デバイスが検出されても監査イベントは生成されません。 ボリューム: 低 |
| プロセス作成の監査 | 成功 | このポリシー設定を使用すると、プロセスの作成または開始時に生成されるイベントを監査できます。そのプロセスを作成したアプリケーションまたはユーザーの名前も監査されます。このポリシー設定を構成すると、プロセスの作成時に監査イベントが生成されます。成功の監査では成功したプロセス作成が、失敗の監査では成功しなかったプロセス作成が記録されます。 このポリシー設定を構成しないと、プロセスの作成時に監査イベントは生成されません。 ボリューム: コンピューターの使用状態に依存。 |

#### [監査ポリシーの詳細な構成]>[監査ポリシー]>[オブジェクトアクセス]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| その他のオブジェクト アクセス イベントの監査 | 成功、失敗 | このポリシー設定を使用すると、タスク スケジューラ ジョブまたは COM+ オブジェクトの管理により生成されるイベントを監査できます。 スケジューラ ジョブの場合の監査対象: ジョブの作成 ジョブの削除 ジョブの有効 ジョブの無効化 ジョブの更新 COM+ オブジェクトの場合の監査対象: カタログ オブジェクトの追加 カタログ オブジェクトの更新 カタログ オブジェクトの削除 ボリューム: 低 |
| リムーバブル記憶域の監査 | 成功、失敗 | このポリシー設定を使用すると、ユーザーによるリムーバブル記憶域デバイス上のファイル システム オブジェクトへのアクセス試行を監査できます。セキュリティ監査イベントは、要求されたすべての種類のアクセスのすべてのオブジェクトに対してのみ生成されます。 このポリシー設定を構成すると、アカウントがリムーバブル記憶域上のファイル システム オブジェクトにアクセスするたびに監査イベントが生成されます。成功の監査では成功したアクセス試行が、失敗の監査では成功しなかったアクセス試行が記録されます。 このポリシー設定を構成しないと、アカウントがリムーバブル記憶域上のファイル システム オブジェクトにアクセスした場合に監査イベントは生成されません。 |

#### [監査ポリシーの詳細な構成]>[監査ポリシー]>[ポリシー変更]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 監査ポリシーの変更 | 成功、失敗 | このポリシー設定を使用すると、次のようなセキュリティ監査ポリシー設定の変更を監査できます。 監査ポリシー オブジェクトのアクセス許可設定および監査設定 システム監査ポリシーの変更 セキュリティ イベント ソースの登録 セキュリティ イベント ソースの登録解除 ユーザーごとの監査設定の変更 CrashOnAuditFail の値の変更 ファイル システムまたはレジストリ オブジェクトのシステム アクセス制御リストの変更 特殊グループの一覧の変更 注意: システム アクセス制御リスト (SACL) の変更の監査は、オブジェクトの SACL が変更され、このポリシー変更のカテゴリが有効にされている場合に実行されます。随意アクセス制御リスト (DACL) および所有権の変更は、オブジェクト アクセスの監査が有効にされていて、DACL/所有者の変更を監査するようにオブジェクトの SACL が構成されている場合に、監査されます。 このポリシー設定を構成すると、リモート RPC 接続が操作された場合に監査イベントが生成されます。成功の監査では成功した操作が、失敗の監査では成功しなかった操作が記録されます。 このポリシー設定を構成しないと、リモート RPC 接続が操作された場合に、監査イベントは生成されません。 ボリューム: 低 既定値: 成功 |
| 認証ポリシーの変更 | 成功 | このポリシー設定を使用すると、次のような認証ポリシーの変更によって生成されるイベントを監査できます。 フォレスト間およびドメイン間の信頼の作成 フォレスト間およびドメイン間の信頼の変更 フォレスト間およびドメイン間の信頼の削除 コンピューターの構成\Windows の設定\セキュリティの設定\Account ポリシー\Kerberos ポリシー以下の Kerberos ポリシーの変更 ユーザーまたはグループへの次のユーザー権利の付与: ネットワーク経由でコンピューターへアクセス ローカル ログオンを許可する ターミナル サービスを使ったログオンを許可する バッチ ジョブとしてログオン サービスとしてログオン 名前空間の競合。たとえば、新しい信頼に既存の名前空間名と同じ名前が付けられた場合です。 このポリシー設定を構成すると、認証ポリシーの変更操作が試みられた場合に監査イベントが生成されます。成功の監査では成功した操作が、失敗の監査では成功しなかった操作が記録されます。 このポリシー設定を構成しないと、認証ポリシーが変更された場合に、監査イベントは生成されません。 注意: セキュリティ監査イベントは、グループ ポリシーが適用された時点で記録されます。設定が変更された時点では、発生しません。 ボリューム: 低 既定値: 成功 |
| 承認ポリシーの変更 | 成功 | このポリシー設定を使用すると、次のような承認ポリシーの変更によって生成されるイベントを監査できます。 "認証ポリシーの変更" サブカテゴリによって監査されない SeCreateTokenPrivilege などのユーザー権利 (特権) の割り当て "認証ポリシーの変更" サブカテゴリによって監査されない SeCreateTokenPrivilege などのユーザー権利 (特権) の削除 暗号化されたファイル システム (EFS) のポリシーの変更 オブジェクトのリソース属性に対する変更 オブジェクトに適用された集約型アクセス ポリシー (CAP) に対する変更 このポリシー設定を構成すると、承認ポリシーの変更操作が試みられた場合に監査イベントが生成されます。成功の監査では成功した操作が、失敗の監査では成功しなかった操作が記録されます。 このポリシー設定を構成しないと、承認ポリシーが変更された場合に、監査イベントは生成されません。 ボリューム: 低 既定値: 監査なし |

#### [監査ポリシーの詳細な構成]>[監査ポリシー]>[特権の使用]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 重要な特権の使用の監査 | 成功、失敗 | このポリシー設定を使用すると、次のような重要な特権 (ユーザー権利) の使用時に生成されるイベントを監査できます。 特権サービスの呼び出し 次の特権のいずれかの呼び出し: オペレーティング システムの一部として機能 ファイルとディレクトリのバックアップ トークン オブジェクトの作成 プログラムのデバッグ コンピューターとユーザー アカウントに委任時の信頼を付与 セキュリティ監査の生成 認証後にクライアントを偽装 デバイス ドライバーのロードとアンロード 監査とセキュリティ ログの管理 ファームウェアの環境値の修正 プロセス レベル トークンの置き換え ファイルとディレクトリの復元 ファイルとその他のオブジェクトの所有権の取得 このポリシー設定を構成すると、重要な特権が要求された場合に監査イベントが生成されます。成功の監査では成功した要求が、失敗の監査では成功しなかった要求が記録されます。 このポリシー設定を構成しないと、重要な特権が要求された場合に、監査イベントは生成されません。 ボリューム: 高 |

#### [監査ポリシーの詳細な構成]>[監査ポリシー]>[システム]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| IPsec ドライバーの監査 | 成功、失敗 | このポリシー設定を使用すると、次のような IPsec フィルター ドライバーによって生成されるイベントを監査できます。 IPsec サービスの開始とシャットダウン 整合性チェックの不合格が原因のネットワーク パケットの破棄 リプレイ チェックの不合格が原因のネットワーク パケットの破棄 プレーンテキストであることが原因のネットワーク パケットの破棄 セキュリティ パラメーター インデックス (SPI) が正しくないネットワーク パケットの受信。ネットワーク カードが正しく動作していないか、ドライバーを更新する必要がある可能性があります。 IPsec フィルターの処理不能 このポリシー設定を構成すると、IPsec フィルター ドライバーの操作が発生した場合に監査イベントが生成されます。成功の監査では成功した操作が、失敗の監査では成功しなかった操作が記録されます。 このポリシー設定を構成しないと、IPsec フィルター ドライバーの操作が発生した場合に、監査イベントは生成されません。 ボリューム: 低 既定値: 監査なし |
| その他のシステム イベントの監査 | 成功、失敗 | このポリシー設定を使用すると、次のようなイベントを監査できます。 Windows ファイアウォール サービスおよびドライバーの開始とシャットダウン Windows ファイアウォール サービスによるセキュリティ ポリシーの処理 暗号化キー ファイルおよび移行操作 ボリューム: 低 既定値: 成功、失敗 |
| セキュリティ状態の変更 | 成功 | このポリシー設定を使用すると、次のイベントのようなコンピューターのセキュリティ状態の変更によって生成されるイベントを監査できます。 コンピューターの起動およびシャットダウン システム時刻の変更 CrashOnAuditFail からのシステムの回復。これは、セキュリティ イベント ログがいっぱいで、CrashOnAuditFail レジストリ エントリが構成されている場合に、システムの再起動後に記録されます。 ボリューム: 低 既定値: 成功 |
| セキュリティ システムの拡張 | 成功 | このポリシー設定を使用すると、次のようなセキュリティ システムの拡張またはサービス関連のイベントを監査できます。 セキュリティ システムの拡張。認証、通知、またはセキュリティ パッケージが読み込まれ、ローカル セキュリティ機関 (LSA) に登録された場合など。これは、ログオンの認証、ログオン要求の送信、アカウントやパスワードの変更に使用されます。セキュリティ システムの拡張の例としては、Kerberos や NTLM が挙げられます。 サービスのインストールおよびサービス コントロール マネージャーへの登録。監査ログには、サービスの名前、バイナリ、種類、開始の種類、およびサービス アカウントが含まれます。 このポリシー設定を構成すると、セキュリティ システムの拡張を読み込む操作が実行された場合に監査イベントが生成されます。成功の監査では成功した操作が、失敗の監査では成功しなかった操作が記録されます。 このポリシー設定を構成しないと、セキュリティ システムの拡張を読み込む操作が実行された場合に、監査イベントは生成されません。 ボリューム: 低。セキュリティ システムの拡張関連のイベントは、クライアント コンピューターやメンバー サーバーよりもドメイン コントローラー上で、より頻繁に生成されます。 既定値: 監査なし |
| システムの整合性 | 成功、失敗 | このポリシー設定を使用すると、次のようなセキュリティ サブシステムの整合性に違反するイベントを監査できます。  監査システムの問題のために、イベント ログへの書き込みができなかったイベント クライアント アドレス空間へのまたはクライアント アドレス空間からの応答、読み取り、または書き込みによるクライアントの偽装の操作において無効なローカル プロシージャ コール (LPC) ポートを使用するプロセス システムの整合性を損なうリモート プロシージャ コール (RPC) の検出 コードの整合性により無効とされた実行可能ファイルのハッシュ値の検出 システムの整合性を損なう暗号化操作 ボリューム: 低 既定値: 成功、失敗 |

### ・DC 管理用テンプレート

[コンピュータの構成]>[ポリシー]>[管理用テンプレート]

MS Security Guide は Microsoft Security Compliance Toolkit 1 に含まれる Windows 10 Version 1909 and Windows Server Version 1909 Security Baseline\Templates [[26]](#footnote-26)に含まれています。日本語化はされていません。

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[MS Security Guide]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Apply UAC restrictions to local accounts on network logons | 有効 | ローカルアカウントにネットワークログオンする際にUACを適用します。 This setting controls whether local accounts can be used for remote administration via network logon (e.g., NET USE, connecting to C$, etc.). Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Enabling this policy significantly reduces that risk. Enabled (recommended): Applies UAC token-filtering to local accounts on network logons. Membership in powerful group such as Administrators is disabled and powerful privileges are removed from the resulting access token. This configures the LocalAccountTokenFilterPolicy registry value to 0. This is the default behavior for Windows. Disabled: Allows local accounts to have full administrative rights when authenticating via network logon, by configuring the LocalAccountTokenFilterPolicy registry value to 1. For more information about local accounts and credential theft, see "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques":  http://www.microsoft.com/en-us/download/details.aspx?id=36036. For more information about LocalAccountTokenFilterPolicy, see [[27]](#footnote-27) |
| Configure SMB v1 client driver | 有効 オプション Configure MrxSmb10 driver [Disable driver (recommended)] | SMB v1 ドライバーを無効にします。 Configures the SMB v1 client driver's start type. To disable client-side processing of the SMBv1 protocol, select the "Enabled" radio button, then select "Disable driver" from the dropdown. WARNING: DO NOT SELECT THE "DISABLED" RADIO BUTTON UNDER ANY CIRCUMSTANCES! For Windows 7 and Servers 2008, 2008R2, and 2012, you must also configure the "Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)" setting. To restore default SMBv1 client-side behavior, select "Enabled" and choose the correct default from the dropdown: \* "Manual start" for Windows 7 and Windows Servers 2008, 2008R2, and 2012; \* "Automatic start" for Windows 8.1 and Windows Server 2012R2 and newer. Changes to this setting require a reboot to take effect. For more information, see [[28]](#footnote-28) |
| Configure SMB v1 server | 無効 | SMB v1 サーバーを無効にします。 Disabling this setting disables server-side processing of the SMBv1 protocol. (Recommended.) Enabling this setting enables server-side processing of the SMBv1 protocol. (Default.) Changes to this setting require a reboot to take effect. For more information, see[[29]](#footnote-29) |
| WDigest Authentication (disabling may require KB2871997) | 無効 | Windows ダイジェスト認証を無効にします。 When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. Microsoft recommends disabling WDigest authentication unless it is needed. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server. Update KB2871997 must first be installed to disable WDigest authentication using this setting in Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012. Enabled: Enables WDigest authentication. Disabled (recommended): Disables WDigest authentication. For this setting to work on Windows 7, Windows 8, Windows Server 2008 R2 or Windows Server 2012, KB2871997 must first be installed. For more information, see [[30]](#footnote-30) . |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[MSS (Legacy) ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) | 有効 オプション DisableIPSourceRoutingIPv6 [Highest protection, Source routing is completely disabled] | IPv6のパケットスプーフィングに対する保護を設定します。ソースルーティングは完全に無効になります。 |
| MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) | 有効 オプション DisableIPSourceRoutingIP [Highest protection, Source routing is completely disabled] | IPv4のパケットスプーフィングに対する保護を設定します。ソースルーティングは完全に無効になります。 |
| MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | 無効 | ICMPリダイレクトによるOSPF生成ルートのオーバーライドを無効化します。 |
| MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | 有効 | WINSサーバーを除き、コンピュータがNetBIOS名の開放要求を無視することを許可します。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[RSS フィード ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 添付ファイルのダウンロードを禁止する | 有効 | このポリシー設定は、添付ファイルをフィードからユーザーのコンピューターにダウンロードできないようにします。 このポリシー設定を有効にすると、フィードのプロパティ ページで、フィード同期エンジンが添付ファイルをダウンロードするように設定できません。開発者は、フィードの API を使用してダウンロード設定を変更できません。 このポリシー設定を無効にするか、構成しない場合、フィードのプロパティ ページで、フィード同期エンジンが添付ファイルをダウンロードするように設定できます。開発者は、フィードの API を使用してダウンロード設定を変更できます。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[Windows PowerShell]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| PowerShell スクリプト ブロックのログ記録を有効にする | 有効 スクリプト ブロックの呼び出し開始/停止イベントをログに記録する: [無効] | このポリシー設定を使用して、すべての PowerShell スクリプト入力を Microsoft-Windows-PowerShell/操作イベント ログに記録することができます。このポリシー設定を有効にした場合、 Windows PowerShell のコマンド処理、スクリプト ブロック、関数、スクリプトが記録されます。対話的に呼び出された場合も、自動的に呼び出された場合もすべて記録されます。 このポリシー設定を無効にした場合、PowerShell スクリプト入力のログ記録が無効になります。 スクリプト ブロックの呼び出しのログ記録を有効にした場合、コマンド、スクリプト ブロック、関数、スクリプトの開始/停止を呼び出したときも イベントがログ記録されます。呼び出しのログ記録を有効にすると、大量のイベント ログが生成されます。 注: このポリシー設定は、グループ ポリシー エディターの [コンピューターの構成] と [ユーザーの構成] の両方にあります。[コンピューターの構成] のポリシー設定は、[ユーザーの構成] のポリシー設定よりも優先されます。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[Windows インストーラー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ユーザーによるインストール制限を有効にする | 無効 | このポリシー設定を使用すると、通常はシステム管理者のみが使用できるインストールのオプションをユーザーが変更できるようになります。 このポリシー設定を有効にした場合、Windows インストーラーの一部のセキュリティ機能がバイパスされます。このポリシーを使用すると、通常はセキュリティ違反のため強制的に中止されるインストールを完了させることができます。 このポリシー設定を無効にした場合、または構成しなかった場合、Windows インストーラーでは、通常システム管理者のみに許可されているインストールのオプション (たとえば、ファイルのインストール先の指定) をユーザーが変更することはできません。 保護されているオプションをユーザーが変更しようとすると、インストールは中止されエラー メッセージが表示されます。このセキュリティ機能は、インストール プログラムが特権付きセキュリティ コンテキストで実行されており、ユーザーがアクセス許可を持っていないディレクトリにプログラムがアクセスできるときに機能します。 このポリシー設定は、規制を緩和するためのものです。ソフトウェアのインストールを妨げるようなインストールのエラーを回避するためにも使用できます。 |
| 常にシステム特権でインストールする | 無効 | このポリシー設定を使用すると、Windows インストーラーを使ってシステムにプログラムをインストールするときに管理者特権のアクセス許可が使用されます。 このポリシー設定を有効にすると、管理者特権がすべてのプログラムに適用されます。通常、この特権はユーザー (デスクトップ上で提供されている) またはコンピューター (自動的にインストールされている) に割り当てられているプログラム、またはコントロール パネルの [プログラムの追加と削除] で利用できるプログラム用に予約されています。このプロファイル設定を使うと、ユーザーはアクセス許可が与えられていないため表示も変更もできないディレクトリ (厳しく制限されているコンピューター上のディレクトリを含む) へのアクセスを必要とするプログラムをインストールできます。 このポリシー設定を無効にした場合、または構成しなかった場合は、システム管理者から配布または提供されていないプログラムのインストール時にはユーザーの現在のアクセス許可が適用されます。 注: このポリシー設定は [コンピューターの構成] フォルダーおよび [ユーザーの構成] フォルダーにあります。このポリシー設定を有効にするには、両方のフォルダーでこのポリシー設定を有効にする必要があります。 警告: 上級ユーザーは、このポリシー設定で付与されるアクセス許可を使って特権を変更し、制限付きのファイルおよびフォルダーに継続してアクセスできます。このポリシー設定の [ユーザーの構成] バージョンのセキュリティ保護は必ずしも安全ではないことに注意してください。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[Windows リモート管理(WinRM)]>[WinRM クライアント]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ダイジェスト認証を許可しない | 有効 | このポリシー設定を使用して、Windows リモート管理 (WinRM) クライアントでダイジェスト認証を使用するかどうかを管理できます。 このポリシー設定を有効にすると、WinRM クライアントでダイジェスト認証は使用されません。 このポリシー設定を無効にした場合、または構成しなかった場合は、WinRM クライアントでダイジェスト認証が使用されます。 |
| 暗号化されていないトラフィックを許可する | 無効 | このポリシー設定を使用して、Windows リモート管理 (WinRM) クライアントで、暗号化されていないメッセージをネットワーク経由で送受信するかどうかを管理できます。 このポリシー設定を有効にすると、WinRM クライアントは、暗号化されていないメッセージをネットワーク経由で送受信します。 このポリシー設定を無効にした場合、または構成しなかった場合は、WinRM クライアントは、暗号化されたメッセージのみをネットワーク経由で送受信します。 |
| 基本認証を許可する | 無効 | このポリシー設定を使用して、Windows リモート管理 (WinRM) クライアントで基本認証を使用するかどうかを管理できます。 このポリシー設定を有効にすると、WinRM クライアントで基本認証が使用されます。WinRM が HTTP トランスポートを使用するように構成されている場合は、ユーザー名とパスワードがクリア テキストとしてネットワーク経由で送信されます。 このポリシー設定を無効にした場合、または構成しなかった場合は、WinRM クライアントで基本認証は使用されません。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[Windows リモート管理(WinRM)]>[WinRM サービス]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| WinRM で RunAs 資格情報の保存を許可しない | 有効 | このポリシー設定を使用すると、Windows リモート管理 (WinRM) サービスでプラグインに対して RunAs 資格情報の保存を許可しないかどうかうかを管理できます。 このポリシー設定を有効にする場合、WinRM サービスではプラグインに対して RunAsUser または RunAsPassword の構成値の設定を許可しません。 既にプラグインで RunAsUser および RunAsPassword の構成値を設定している場合、このコンピューターの資格情報ストアから RunAsPassword の構成値が消去されます。 このポリシー設定を無効にする場合、または構成しない場合、WinRM サービスではプラグインに対して RunAsUser および RunAsPassword の構成値の設定を許可し、RunAsPassword 値が安全に保存されます。 このポリシー設定を有効にした後、無効にした場合、それまでに RunAsPassword に構成済みの値があれば、リセットする必要があります。 |
| 暗号化されていないトラフィックを許可する | 無効 | このポリシー設定を使用して、Windows リモート管理 (WinRM) サービスで、暗号化されていないメッセージをネットワーク経由で送受信するかどうかを管理できます。 このポリシー設定を有効にすると、WinRM クライアントは、暗号化されていないメッセージをネットワーク経由で送受信します。 このポリシー設定を無効にした場合、または構成しなかった場合は、WinRM クライアントは、暗号化されたメッセージのみをネットワーク経由で送受信します。 |
| 基本認証を許可する | 無効 | このポリシー設定を使用して、Windows リモート管理 (WinRM) サービスでリモート クライアントからの基本認証を受け付けるかどうかを管理できます。 このポリシー設定を有効にすると、WinRM サービスはリモート クライアントからの基本認証を受け付けます。 このポリシー設定を無効にした場合、または構成しなかった場合は、WinRM サービスはリモート クライアントからの基本認証を受け付けません。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[Windows ログオンのオプション]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 再起動後に自動的に前回の対話ユーザーでサインインしてロックする | 無効 | このポリシー設定では、システムの再起動後、またはシャットダウンとコールド ブートの後に、デバイスに自動的に前回の対話ユーザーでサインインしてロックするかどうかを制御します。 これは、前回の対話ユーザーが再起動またはシャットダウンの前にサインアウトしなかった場合にのみ発生します。 デバイスが Active Directory または Azure Active Directory に参加している場合、このポリシーは Windows Update による再起動のみに適用されます。それ以外の場合は、Windows Update による再起動と、ユーザーによって開始された再起動およびシャットダウンの両方に適用されます。 このポリシー設定を構成しなかった場合は、既定で有効になります。このポリシーを有効にすると、デバイスの起動後、ユーザーは自動的にサインインし、そのユーザー用に構成されたすべてのロック画面アプリを使用してセッションが自動的にロックされます。 このポリシーを有効にした後、ConfigAutomaticRestartSignOn ポリシーを使用して設定を構成できます。それにより、再起動またはコールド ブート後に前回の対話ユーザーで自動的にサインインしてロックするモードを構成します。 このポリシー設定を無効にすると、デバイスでは自動サインインが構成されません。システムの再起動後、ユーザーのロック画面アプリは再起動されません。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[アプリケーションの互換性]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| インベントリ コレクターをオフにする | 有効 | このポリシー設定では、インベントリ コレクターの状態を制御します。 インベントリ コレクターは、システム上のアプリケーション、ファイル、デバイス、およびドライバーのインベントリを作成し、その情報を Microsoft に送信します。 この情報は、互換性の問題の診断に役立てられます。 このポリシー設定を有効にした場合、インベントリ コレクターは無効になり、Microsoft にデータが送信されなくなります。プログラム互換性アシスタントによるインストール データの収集も無効になります。 このポリシー設定を無効にした場合、または構成しなかった場合は、インベントリ コレクターは有効になります。 注: カスタマー エクスペリエンス向上プログラムが無効になっている場合、このポリシー設定による効果はありません。インベントリ コレクターは無効になります。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[イベントログサービス]>[アプリケーション]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ログ ファイルの最大サイズ(KB)を指定する | 有効 最大ログサイズ(KB): 32768 | このポリシー設定では、ログ ファイルの最大サイズを KB 単位で指定します。 このポリシー設定を有効にした場合、ログ ファイルの最大サイズを KB 単位で 1 MB (1024 KB) から 2 TB (2147483647 KB) までの範囲で構成できます。 このポリシー設定を無効にするか、未構成にした場合、ログ ファイルの最大サイズはローカルで構成された値に設定されます。この値は、ローカル管理者が [ログのプロパティ] ダイアログ ボックスを使用して変更でき、既定では 1 MB になります。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[イベントログサービス]>[システム]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ログ ファイルの最大サイズ(KB)を指定する | 有効 最大ログサイズ(KB): 32768 | このポリシー設定では、ログ ファイルの最大サイズを KB 単位で指定します。 このポリシー設定を有効にした場合、ログ ファイルの最大サイズを KB 単位で 1 MB (1024 KB) から 2 TB (2147483647 KB) までの範囲で構成できます。 このポリシー設定を無効にするか、未構成にした場合、ログ ファイルの最大サイズはローカルで構成された値に設定されます。この値は、ローカル管理者が [ログのプロパティ] ダイアログ ボックスを使用して変更でき、既定では 1 MB になります。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[イベントログサービス]>[セキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ログ ファイルの最大サイズ(KB)を指定する | 有効 最大ログサイズ(KB): 196608 | このポリシー設定では、ログ ファイルの最大サイズを KB 単位で指定します。 このポリシー設定を有効にした場合、ログ ファイルの最大サイズを KB 単位で 1 MB (1024 KB) から 2 TB (2147483647 KB) までの範囲で構成できます。 このポリシー設定を無効にするか、未構成にした場合、ログ ファイルの最大サイズはローカルで構成された値に設定されます。この値は、ローカル管理者が [ログのプロパティ] ダイアログ ボックスを使用して変更でき、既定では 1 MB になります。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[エクスプローラー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| Windows Defender SmartScreen を構成します | 有効 オプション: [警告してバイパスを回避] | このポリシーを使用すると、Windows Defender SmartScreen を有効または無効にできます。SmartScreenは、インターネットからダウンロードされた悪意のある可能性のあるプログラムを実行する前にユーザーに警告することで、PC の保護に役立ちます。認識できないアプリまたは悪意があるとわかっているアプリがインターネットからダウンロードされ実行される前に、この警告がスポット ダイアログとして表示されます。不審であると見なされていないアプリの場合、ダイアログは表示されません。 この機能を有効にした PC で実行されたファイルおよびプログラムについて、Microsoft に情報が送信されます。 このポリシーを有効にすると、すべてのユーザーに対して SmartScreen がオンになります。その動作は、次のオプションを使用して制御できます: ・警告してバイパスを回避 ・警告 [警告してバイパスを回避] オプションを指定してこのポリシーを有効にした場合、SmartScreen のダイアログでは、警告を無視してアプリを実行するオプションがユーザーに提示されません。その後アプリを実行しようとすると、引き続き SmartScreen から警告が表示されます [警告] オプションを指定してこのポリシーを有効にした場合、SmartScreen のダイアログで、アプリが不審だと思われるという警告がユーザーに提示されますが、ユーザーは警告を無視してすぐにアプリを実行することもできます。ユーザーがアプリの実行を SmartScreen に指定した場合、そのアプリについては SmartScreen から再度ユーザーに警告されることはありません。 このポリシーを無効にすると、すべてのユーザーに対して SmartScreen が無効になります。ユーザーがインターネットから不審なアプリを実行しようとしても、警告は表示されません。 このポリシーを構成しなかった場合、既定では SmartScreen が有効になりますが、ユーザーは独自に設定を変更できます。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[データの収集とプレビュー ビルト]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 利用統計情報の許可 | 有効 オプション: [1 - 基本] | このポリシー設定では、マイクロソフトに送信される Windows 診断データの最大レベルを決定します。この設定を構成した場合、ユーザーは製品利用統計情報の設定を変更できますが、組織に対して設定されたレベルよりも上のレベルに変更することはできません。Windows 10 診断データの設定は、Windows オペレーティング システムと Windows の付属アプリだけに適用されます。Windows 10 で実行されるサードパーティのアプリには適用されません。 この設定を有効にすると、どのレベルの診断データをマイクロソフトに送信するかを決定できます。次のレベルがあります。 - 0 (セキュリティ)。Windows の安全性を維持するために必要な最小限の量のデータだけをマイクロソフトに送信します。悪意のあるソフトウェアの削除ツール (MSRT) や Windows Defender などの Windows セキュリティ コンポーネントにより (有効であれば)、このレベルでマイクロソフトにデータが送信されることもあります。値 0 の設定は、Enterprise、Education、IoT、Windows Server のいずれかのエディションを実行しているデバイスだけに適用されます。その他のエディションで値 0 を設定した場合は、値 1 を設定した場合と同じ結果になります。 - 1 (基本)。値が 0 の場合と同じデータに加えて、ごく限られた量の診断データ (基本的なデバイス情報、品質に関連するデータ、アプリの互換性情報など) が送信されます。値を 0 または 1 に設定すると、デバイスで特定のエクスペリエンスが低下することにご注意ください。 - 2 (拡張)。値が 1 の場合と同じデータに加えて、Windows、Windows Server、System Center、アプリの使用状況、パフォーマンス、詳細な信頼性データなどの追加データが送信されます。 - 3 (完全)。値が 2 の場合と同じデータに加えて、デバイスの診断と問題解決に使用される詳細な診断データが送信されます。これには、デバイスでの問題の原因となった可能性があるファイルやコンテンツが含まれます。 このポリシー設定を無効にした場合または構成しなかった場合、製品利用統計情報の設定は [設定] で個別に構成することができます。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[リモートデスクトップ サービス]>[リモート デスクトップ セッション ホスト]>[セキュリティ]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| クライアント接続の暗号化レベルを設定する | 有効 暗号化レベル: [高レベル] | リモート デスクトップ プロトコル (RDP) 接続時に、クライアント コンピューターと RD セッション ホスト サーバー間の通信をセキュリティで保護するために、特定の暗号化レベルの使用を必要とするかどうかを指定します。このポリシーは、ネイティブの RDP 暗号化を使用しているときにのみ適用されます。ただし (SSL 暗号化と比べ) ネイティブ RDP 暗号化は推奨されません。SSL 暗号化にこのポリシーは適用されません。 このポリシー設定を有効にした場合、リモート接続時のクライアントと RD セッション ホスト サーバー間のすべての通信で、この設定で指定された暗号化方法を使用する必要があります。既定では、暗号化レベルは [高] に設定されています。次の暗号化方法を利用できます。 \* 高: [高] 設定では、強力な 128 ビット暗号化を使ってクライアントとサーバー間で送受信されるデータを暗号化します。この暗号化レベルは、128 ビット クライアント (リモート デスクトップ接続クライアントなど) のみが含まれる環境で使用します。この暗号化レベルをサポートしていないクライアントは RD セッション ホスト サーバーに接続できません。 \* クライアント互換: [クライアント互換] 設定では、クライアントとサーバーの間で送信されるデータは、クライアントでサポートされている最高のキー強度で暗号化されます。この暗号化レベルは、128 ビット暗号化をサポートしていないクライアントが含まれる環境で使用します。 \* 低: [低] 設定では、56 ビット暗号化を使ってクライアントからサーバーへ送信されるデータのみを暗号化します。 この設定を無効にするか、または構成しない場合は、RD セッション ホスト サーバーへのリモート接続に使用される暗号化レベルは、グループ ポリシーを通じて強制されません。 重要: FIPS 準拠は、システム暗号化を通じて構成できます。グループ ポリシーの [暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う] 設定 (場所: "コンピューターの構成\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション")。[FIPS 準拠] 設定では、Microsoft 暗号化モジュールを使用して、Federal Information Processing Standard (FIPS) 140 暗号化アルゴリズムによって、クライアントとサーバー間で送受信されるデータを暗号化および暗号化解除します。この暗号化レベルは、クライアントと RD セッション ホスト サーバー間の通信で最高レベルの暗号化が必要な場合に使用します。 |
| セキュリティで保護された RPC 通信を要求する | 有効 | リモート デスクトップ セッション ホスト サーバーに、クライアントすべてとのセキュリティで保護された RPC 通信が必要か、またはセキュリティで保護されていない通信を許可するかどうかを指定します。 この設定を使って、認証されて暗号化された要求のみを許可することで、クライアントとの RPC 通信のセキュリティを強化できます。 状態が有効に設定されている場合、リモート デスクトップ サービスは、セキュリティで保護された要求をサポートする RPC クライアントからの要求を受け入れて、信用されていないクライアントとのセキュリティで保護されていない通信を許可しません。 状態が無効に設定されている場合は、リモート デスクトップ サービスは RPC トラフィックすべてのセキュリティを常に要求します。しかし、要求に応答しない RPC クライアントにはセキュリティで保護されていない通信が許可されます。 状態が未構成に設定されている場合は、セキュリティで保護されていない通信は許可されます。 注: RPC インターフェイスがリモート デスクトップ サービスの管理または構成に使用されています。 |
| 接続するたびにパスワードを要求する | 有効 | このポリシー設定は、接続時にクライアントが、リモート デスクトップ サービスによって常にパスワードの入力を要求されるかどうかを指定します。 リモート デスクトップ サービスにログオンしているユーザーが、リモート デスクトップ接続のクライアントでパスワードを既に提供していても、この設定を使ってパスワードの入力を強制できます。 既定では、リモート デスクトップ サービスによりユーザーはリモート デスクトップ接続のクライアントにパスワードを入力して自動的にログオンできます。 このポリシー設定を有効にすると、ユーザーはリモート デスクトップ接続のクライアントでパスワードを供給しても、リモート デスクトップ サービスに自動的にログオンできません。ユーザーは、ログオンするためにパスワードを要求されます。 このポリシー設定を無効にすると、ユーザーは常にリモート デスクトップ接続のクライアントでパスワードを供給することでリモート デスクトップ サービスに自動的にログオンできます。 このポリシー設定を構成しなかった場合、自動ログオンはグループ ポリシー レベルでは指定されません。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[リモートデスクトップ サービス]>[リモート デスクトップ セッション ホスト]>[デバイスとリソースのリダイレクト]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ドライブのリダイレクトを許可しない | 有効 | このポリシー設定は、リモート デスクトップ サービス セッションで、クライアント ドライブのマッピングをしないようにするかどうかを指定します (ドライブ リダイレクト)。 既定では、RD セッション ホスト サーバーは接続時に自動的にクライアント ドライブをマップします。マップされたドライブは、エクスプローラーまたは [コンピューター] のセッション フォルダー ツリーに、<コンピューター名> の <ドライブ文字> という形式で表示されます。このポリシー設定を使ってこの動作を上書きできます。 このポリシー設定を有効にすると、クライアント ドライブのリダイレクトはリモート デスクトップ サービス セッションでは許可されません。また、クリップボードでのファイル コピーのリダイレクトは、Windows Server 2003、Windows 8、および Windows XP を実行しているコンピューターでは許可されません。 このポリシー設定を無効にすると、クライアント ドライブのリダイレクトは常に許可されます。さらに、クリップボードのリダイレクトを許可すると、クリップボードでのファイル コピーのリダイレクトは常に許可されます。 このポリシー設定を構成しなかった場合、クライアント ドライブのリダイレクトおよびクリップボードでのファイル コピーのリダイレクトはグループ ポリシー レベルでは指定されません。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[リモートデスクトップ サービス]>[リモート デスクトップ接続のクライアント]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| パスワードの保存を許可しない | 有効 | リモート デスクトップ接続からこのコンピューター上でパスワードを保存できるようにするかどうかを制御します。 この設定を有効にすると、リモート デスクトップ接続のパスワードを保存するためのチェック ボックスが使用できなくなり、以降、ユーザーはパスワードを保存できなくなります。ユーザーがリモート デスクトップ接続で RDP ファイルを開いて設定を保存した場合、RDP ファイルに以前から存在していたパスワードはすべて削除されます。 この設定を無効または未構成にする場合、ユーザーはリモート デスクトップ接続でパスワードを保存できるようになります。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[検索]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 暗号化されたファイルのインデックス作成を許可する | 無効 | このポリシー設定を使用すると、暗号化されたアイテムのインデックスを作成できます。このポリシー設定を有効にすると、内容に対して暗号化の解除とインデックスの作成が行われます (アクセス制限は引き続き適用されます)。このポリシー設定を無効にすると、検索サービスのコンポーネント (Microsoft 製以外のコンポーネントを含む) は、暗号化されたアイテムのインデックス作成は行わず、暗号化されたストアのインデックス作成も行いません。このポリシー設定は、既定では構成されていません。このポリシー設定を構成しない場合は、コントロール パネルを使用して構成されたローカル設定が使用されます。既定では、コントロール パネルの設定は、暗号化された内容のインデックスを作成しないように設定されています。 この設定の有効/無効を切り替えるたびに、インデックス全体が最初から再構築されます。 インデックスの場所にフルボリューム暗号化 (BitLocker ドライブ暗号化や Microsoft 製以外のソリューションなど) を使用して、暗号化されたファイルのセキュリティを維持する必要があります。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[資格情報のユーザーインターフェース]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 昇格時に管理者アカウントを列挙する | 無効 | このポリシー設定により、ユーザーが実行中のアプリケーションの昇格を試みたときに、管理者アカウントが表示されるかどうかを制御します。既定では、ユーザーが実行中のアプリケーションの昇格を試みたときに、管理者アカウントは表示されません。 このポリシー設定を有効にした場合、PC 上のローカル管理者アカウントがすべて表示され、ユーザーがその 1 つを選択して、正しいパスワードを入力できます。 このポリシー設定を無効にした場合、ユーザーは、昇格時にユーザー名とパスワードを常に入力するよう要求されます。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[Windows コンポーネント ]>[自動再生のポリシー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ボリューム以外のデバイスの自動再生を許可しない | 有効 | このポリシー設定では、カメラや電話などの MTP デバイスの自動再生を許可しません。 このポリシー設定を有効にした場合、カメラや電話などの MTP デバイスの自動再生が許可されません。 このポリシー設定を無効にした場合、または構成しなかった場合、ボリューム以外のデバイスに対する自動再生が有効になります。 |
| 自動再生機能をオフにする | 有効 自動再生機能をオフにする: [すべてのドライブ] | このポリシー設定では、自動再生機能をオフにできます。 自動再生とは、ドライブにメディアを挿入すると同時にドライブからの読み込みを開始する機能です。この機能によって、プログラムのセットアップ ファイルやオーディオ メディアの音楽などがすぐに開始されます。 Windows XP SP2 より前は、自動再生は、フロッピー ディスク ドライブなどのリムーバブル ドライブ (CD-ROM ドライブは除く) およびネットワーク ドライブ上では既定で無効になっています。 Windows XP SP2 以降では、自動再生は Zip ドライブや一部の USB 大容量記憶装置デバイスなどのリムーバブル ドライブでも有効になっています。 このポリシー設定を有効にした場合、CD-ROM およびリムーバブル メディア ドライブの自動再生を無効にするか、すべてのドライブの自動再生を無効にすることができます。 このポリシー設定によって、これ以外の種類のドライブでの自動再生を無効にすることができます。この設定を使用して、既定で無効になっているドライブ上の自動再生を有効にすることはできません。 このポリシー設定を無効にした場合、または構成しなかった場合、自動再生が有効になります。 注: このポリシー設定は [コンピューターの構成] フォルダーおよび [ユーザーの構成] フォルダーにあります。ポリシー設定が競合する場合、[コンピューターの構成] にあるポリシー設定が [ユーザーの構成] にあるポリシー設定より優先されます。 |
| 自動実行の既定の動作を設定する | 有効 既定の自動実行の動作: [自動実行コマンドを実行しない] | このポリシー設定では、自動実行コマンドの既定の動作を設定します。 通常、自動実行コマンドは autorun.inf ファイルに保存されています。多くの場合、インストール プログラムや他のルーチンを起動します。 Windows Vista 以前の場合、自動実行コマンドを含むメディアを挿入すると、ユーザーによる手動操作がなくてもプログラムが自動的に実行されます。 この場合、ユーザーが知らずにコードが実行される可能性があるため、重大なセキュリティ上の問題が発生することがあります。Windows Vista 以降の既定の動作では、自動実行コマンドを実行するかどうかをユーザーに確認するメッセージが表示されます。自動実行コマンドは、[自動再生] ダイアログ ボックスでハンドラーとして表示されます。 このポリシー設定を有効にした場合、管理者は Windows Vista 以降の自動実行の既定の動作を次のように変更することができます。 a) 自動実行コマンドを完全に無効にする。または b) 自動実行コマンドを Windows Vista 以前の自動実行の動作に戻す。 このポリシー設定を無効にした場合、または構成しなかった場合、Windows Vista 以降では、自動実行コマンドを実行するかどうかをユーザーに確認するメッセージが表示されます。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[コントロールパネル ]>[個人用設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ロック画面スライドショーを有効にできないようにする | 有効 | PC 設定でロック画面スライド ショー設定を無効にし、ロック画面でスライド ショーを再生できないようにします。 既定では、ユーザーは、コンピューターのロック後に実行されるスライド ショーを有効にできます。 この設定を有効にした場合、ユーザーは、PC 設定でスライド ショー設定を修正できなくなり、スライド ショーが開始されることもなくなります。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[システム]>[インターネット通信の設定]>[インターネット通信の設定]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| HTTP経由の印刷をオフにする | 有効 | このポリシー設定では、このクライアントの HTTP 経由の印刷を許可するかどうかを指定します。 HTTP 経由の印刷では、イントラネットおよびインターネット上のプリンターで印刷できます。 注: このポリシー設定によって影響を受けるのは、インターネット印刷のクライアント側のみです。このポリシー設定が有効になっている場合でも、このコンピューターはインターネット プリント サーバーとして機能し、共有プリンターを HTTP 経由で利用可能にすることができます。 このポリシー設定を有効にした場合、このクライアントは HTTP 経由でインターネット プリンターに出力することはできません。 このポリシー設定を無効にした場合、または構成しなかった場合、ユーザーは HTTP 経由でインターネット プリンターに出力することを選択できます。 "コンピューターの構成/管理用テンプレート/プリンター" の "Web ベース印刷" ポリシー設定も参照してください。 |
| プリンター ドライバーの HTTP 経由でのダウンロードをオフにする | 有効 | このポリシー設定では、クライアントが HTTP 経由でプリンター ドライバー パッケージをダウンロードするかどうかを指定します。 HTTP 経由の印刷をセットアップするには、付属していないドライバーを HTTP 経由でダウンロードする必要があります。 注: このポリシー設定が有効になっている場合でも、クライアントはイントラネットやインターネットのプリンターに HTTP 経由で出力できます。 ローカルにインストールされていないドライバーのダウンロードのみを禁止します。 この設定を有効にした場合、プリンター ドライバーは HTTP 経由でダウンロードできません。 このポリシー設定を無効にした場合、または構成しなかった場合、ユーザーは HTTP 経由でプリンター ドライバーをダウンロードできます。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[システム]>[グループポリシー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| レジストリ ポリシーの処理を構成する | 有効 オプション バックグラウンドで定期的に処理しているときは適用しない: [無効] グループポリシー オブジェクトが変更されていなくても処理する: [有効] | このポリシー設定では、レジストリ ポリシーをいつ更新するかを決定します。 このポリシー設定は、[管理用テンプレート] フォルダーにあるすべてのポリシー、およびレジストリに値を格納しているその他のポリシーに影響します。この設定は、インストール時に設定されたレジストリ ポリシーを実装しているプログラムのカスタム設定よりも優先されます。 このポリシー設定を有効にした場合、オプションを変更するためのチェック ボックスが利用できるようになります。このポリシー設定を無効にした場合、または構成しなかった場合は、システムに影響はありません。 [バックグラウンドで定期的に処理しているときは適用しない] オプションを有効にした場合、コンピューターの使用中は関連するポリシーがバックグラウンドで更新されなくなります。バックグラウンドでの更新を無効にすると、再度ユーザーがログオンするか、システムを再起動するまでポリシーへの変更は適用されません。 [グループ ポリシー オブジェクトが変更されていなくても処理する] オプションを使うと、ポリシーが変更されていない場合でも、ポリシーは更新されて再適用されます。変更されたときのみ更新するように指定できるポリシーは複数あります。しかし、ユーザーが変更した場合に備え、変更されていないポリシーであっても、必要なポリシー設定を再適用するなどの方法で更新することをお勧めします。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[システム]>[プロセス作成の監査]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| プロセス作成イベントにコマンドラインを含める | 有効 | このポリシー設定では、新しいプロセスの作成時にセキュリティ監査イベントのログに記録する情報を決定します。 この設定は、プロセス作成の監査ポリシーが有効な場合にのみ適用されます。このポリシー設定を有効にした場合、このポリシー設定が適用されているワークステーションやサーバーでは、各プロセスのコマンド ライン情報が、プロセス作成の監査イベント 4688 "新しいプロセスの作成" の一部としてテキスト形式でセキュリティ イベント ログに記録されます。 このポリシー設定を無効にした場合、または構成しなかった場合、プロセスのコマンド ライン情報はプロセス作成の監査イベントに含まれません。 既定: 未構成 注: このポリシー設定を有効にした場合、セキュリティ イベントの読み取りアクセス権を持つユーザーは、正常に作成されたプロセスのコマンド ライン引数を読み取ることができます。コマンド ライン引数には、パスワードやユーザー データなどの機密性の高い情報や個人情報を含めることができます。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[システム]>[リモートプロシージャコール]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 認証されていない RPC クライアントを制限する | 有効 適用する RPC ランタイム未認証クライアント制限: [認証済み] | このポリシー設定は、RPC サーバーに接続する認証されていない RPC クライアントを RPC サーバー ランタイムが処理する方法を制御します。 このポリシー設定は、すべての RPC アプリケーションに影響します。 ドメイン環境では、このポリシー設定はグループ ポリシーの処理自体を含む広範な機能に影響する可能性があるため、注意して使用する必要があります。 このポリシー設定の変更を元に戻す場合、影響するコンピューターごとに手動での操作が必要になることがあります。 このポリシー設定は、ドメイン コントローラーには適用しないでください。 このポリシー設定を無効にすると、RPC サーバー ランタイムは Windows クライアントでは [認証済み] の値を使用し、このポリシー設定をサポートする Windows Server バージョンでは [なし] の値を使用します。 このポリシー設定を構成しない場合、設定は無効のままになります。 RPC サーバー ランタイムは、Windows クライアントでは [認証済み] の値の使用が、このポリシー設定をサポートする Server SKU では [なし] の値の使用が有効にされた場合と同じように動作します。 このポリシー設定を有効にすると、コンピューター上の RPC サーバーに接続する、認証されていない RPC クライアントを制限するよう RPC サーバー ランタイムに指示します。サーバーとの通信時に名前付きパイプを使用している場合、または RPC セキュリティを使用している場合に、クライアントは認証済みとして認識されます。このポリシー設定で選択された値によっては、未認証のクライアントがアクセスできるよう明示的に要求した RPC インターフェイスは、この制限から除外される場合もあります。 -- [なし] では、このポリシー設定が適用されるコンピューター上で実行されている RPC サーバーへの、すべての RPC クライアントの接続を許可します。 -- [認証済み] では、このポリシー設定が適用されるコンピューター上で実行されている RPC サーバーへの、認証済み (前の定義による) の RPC クライアントのみの接続を許可します。除外を要求したインターフェイスは除外されます。 -- [認証済み (例外なし)] では、このポリシー設定が適用されるコンピューター上で実行されている RPC サーバーへの、認証済み (前の定義による) の RPC クライアントのみの接続を許可します。 例外は許可されません。 注: このポリシー設定は、システムが再起動されるまで適用されません。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[システム]>[ログオン]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| ドメインに参加しているコンピューターのローカル ユーザーを列挙する | 無効 | このポリシー設定は、ドメインに参加しているコンピューターのローカル ユーザーを列挙します。 このポリシー設定を有効にした場合、ログオン UI に、ドメインに参加しているコンピューターのすべてのローカル ユーザーが列挙されます。 このポリシー設定を無効にした場合、または構成しなかった場合、ログオン UI に、ドメインに参加しているコンピューターのローカル ユーザーは列挙されません。 |
| ネットワークの選択の UI を表示しない | 有効 | このポリシー設定を使用すると、ログイン画面で使用可能なネットワークの UI をだれでも操作できるかどうかを制御できます。 このポリシー設定を有効にした場合、Windows にサインインしないと PC のネットワーク接続の状態を変更できません。 このポリシー設定を無効にした場合、または構成しなかった場合、すべてのユーザーは、Windows にサインインしなくても、PC をネットワークから切断したり、別の使用可能なネットワークに接続したりすることができます。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート] >[システム]>[電源の管理]>[スリープの設定]

|  |  |  |
| --- | --- | --- |
| **ポリシー設定** | **値** | **説明** |
| コンピュータのスリープ状態の解除時にパスワードを要求する(バッテリ使用時) | 有効 | このポリシー設定では、システムのスリープ状態を解除するときに、ユーザーにパスワードを要求するかどうかを指定します。 このポリシー設定を有効にした場合、または構成しなかった場合、ユーザーはシステムのスリープ状態を解除するときにパスワードを要求されます。 このポリシー設定を無効にすると、ユーザーはシステムのスリープ状態を解除するときにパスワードを要求されません。 |
| コンピュータのスリープ状態の解除時にパスワードを要求する(電源接続時) | 有効 | このポリシー設定では、システムのスリープ状態を解除するときに、ユーザーにパスワードを要求するかどうかを指定します。  このポリシー設定を有効にした場合、または構成しなかった場合、ユーザーはシステムのスリープ状態を解除するときにパスワードを要求されます。  このポリシー設定を無効にすると、ユーザーはシステムのスリープ状態を解除するときにパスワードを要求されません。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[ネットワーク]>[Lanman ワークステーション]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 安全でないゲスト ログオンを有効にする | 無効 | このポリシー設定では、SMB クライアントが SMB サーバーへの安全でないゲスト ログオンを許可するかどうかを決定します。 このポリシー設定を有効にした場合、またはこのポリシー設定を構成しなかった場合、SMB クライアントは安全でないゲスト ログオンを許可します。 このポリシー設定を無効にした場合、SMB クライアントは安全でないゲスト ログオンを拒否します。 安全でないゲスト ログオンがファイル サーバーによって使用されるのは、共有フォルダーに対する認証されていないアクセスを許可することが目的です。エンタープライズ環境では一般的ではありませんが、ファイル サーバーとして動作しているコンシューマー NAS (ネットワーク接続ストレージ) アプライアンスでは、安全でないゲスト ログオンが頻繁に使用されています。Windows ファイル サーバーでは認証を要求し、既定では安全でないゲスト ログオンを使用しません。安全でないゲスト ログオンは認証されていないため、SMB 署名、SMB 暗号化などの重要なセキュリティ機能が無効になります。結果として、安全でないゲスト ログオンを許可するクライアントは、さまざまな man-in-the-middle 攻撃に対して脆弱になり、データ損失、データの破損、マルウェアに対するリスクにつながる可能性があります。また、安全でないゲスト ログオンを使用してファイル サーバーに書き込まれたデータには、ネットワーク上のすべてのユーザーからアクセスできる可能性があります。Microsoft では、安全でないゲスト ログオンを無効にして、認証されたアクセスが要求されるようにファイル サーバーを構成することをお勧めします。 |

#### [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[ネットワーク]>[ネットワークプロバイダー]

| **ポリシー設定** | **値** | **説明** |
| --- | --- | --- |
| 強化された UNC パス | 有効 値の名前: \\\*SYSVOL 値: RequireMutualAuthentication = 1, RequireIntegrity = 1 値の名前: \\\*\NETLOGON 値: RequireMutualAuthentication = 1, RequireIntegrity = 1 | このポリシー設定は、UNCパスへの安全なアクセスを構成します。このポリシーを有効にすると、Windowsは追加のセキュリティ要件を満たした後、指定されたUNCパスへのアクセスのみを許可します。 |

グラフィカル ユーザー インターフェイス, テーブル

自動的に生成された説明

# サイバー攻撃に対する防御 MITREに基づく緩和対策

Ⅴ部では、MITRE ATT&CK に登録された攻撃手法の中から、実際に日本国内で発生し、かつ、頻繁に利用されている攻撃手法を絞り込み、それぞれの脅威に対して、効果的かつ具体的な設定対策を解説しています。

攻撃は、初期侵入→悪意あるプログラムの実行→C&C→永続化→防御回避→探索→水平展開→情報漏洩、破壊といったベクトルを持ちますが、「初期侵入」や「悪意あるプログラムの実行」段階で食い止めることが最も重要です。永続化され防御回避されてしまうと、検出が難しくなり、大規模な被害を受ける可能性が高まります。また、ベクトル後半の攻撃手法の多くは、OSの標準機能を使用するため、技術的な防御設定が困難になります。

緩和対策は、「初期侵入」、「悪意あるプログラムの実行」の各攻撃手法を最優先し対策して下さい。

## MITRE ATT&CK に基づく詳細設定対策

本項では、MITRE ATT&CK で分類された攻撃手法の内、日本国内でもっとも使用されたと考えられる手法を有識者によって絞り込み、DoD STIG、CIS Benchmark、MS Security Base Line、Security Configration Framework を参考に、有効な緩和策を取りまとめたものです。

### MITRE ATT&CKによる設定対策一覧（絞り込み済み）

| **戦術** | **手法** | **緩和策** |
| --- | --- | --- |
| 初期侵入 | ・悪意のあるファイルを添付したフィッシングメール | 特権アカウント管理 |
| ユーザートレーニング |
| 電子メール、ブラウザの厳格運用 |
| 検知システム |
| 悪意あるプログラムの実行 | ・コマンドラインインターフェースの悪用 | 特権アカウント管理 |
| ホワイトリスト、ブラックリスト |
| 監査（イベントログ） |
| 開発業務と一般業務の分離 |
| ・PowerShellの悪用 | 機能やプログラムの無効化または削除 |
| コード署名 |
| ホワイトリスト |
| [・Windowsタスクスケジューラ at, schtasks の悪用](https://www.softwareisac.jp/ipa/index.php?%E3%83%BBWindows%E3%82%BF%E3%82%B9%E3%82%AF%E3%82%B9%E3%82%B1%E3%82%B8%E3%83%A5%E3%83%BC%E3%83%A9+at%2C+schtasks+%E3%81%AE%E6%82%AA%E7%94%A8) | 監査(イベントログ） |
| [・悪意あるスクリプティングの実行](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E6%82%AA%E6%84%8F%E3%81%82%E3%82%8B%E3%82%B9%E3%82%AF%E3%83%AA%E3%83%97%E3%83%86%E3%82%A3%E3%83%B3%E3%82%B0%E3%81%AE%E5%AE%9F%E8%A1%8C) | 電子署名 |
| 保護されたビュー |
| [・悪意あるWindowsサービスの実行](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E6%82%AA%E6%84%8F%E3%81%82%E3%82%8BWindows%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E3%81%AE%E5%AE%9F%E8%A1%8C) | 特権アカウント管理 |
| 監査(イベントログ） |
| 脆弱性の排除 |
| [・メールに添付されたマルウェアファイルやリンクをユーザーが実行する](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%A1%E3%83%BC%E3%83%AB%E3%81%AB%E6%B7%BB%E4%BB%98%E3%81%95%E3%82%8C%E3%81%9F%E3%83%9E%E3%83%AB%E3%82%A6%E3%82%A7%E3%82%A2%E3%83%95%E3%82%A1%E3%82%A4%E3%83%AB%E3%82%84%E3%83%AA%E3%83%B3%E3%82%AF%E3%82%92%E3%83%A6%E3%83%BC%E3%82%B6%E3%83%BC%E3%81%8C%E5%AE%9F%E8%A1%8C%E3%81%99%E3%82%8B) | 特権アカウント管理 |
| ユーザートレーニング |
| 電子メール、ブラウザの厳格運用 |
| 検知システム |
| 永続化 | [・不正なWindowsサービスの追加](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E4%B8%8D%E6%AD%A3%E3%81%AAWindows%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E3%81%AE%E8%BF%BD%E5%8A%A0) | 特権アカウント管理 |
| 監査(イベントログ） |
| 脆弱性の排除 |
| [・レジストリRunキーやスタートアップフォルダの悪用](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%AC%E3%82%B8%E3%82%B9%E3%83%88%E3%83%AARun%E3%82%AD%E3%83%BC%E3%82%84%E3%82%B9%E3%82%BF%E3%83%BC%E3%83%88%E3%82%A2%E3%83%83%E3%83%97%E3%83%95%E3%82%A9%E3%83%AB%E3%83%80%E3%81%AE%E6%82%AA%E7%94%A8) | 監査(イベントログ） |
| 防御の回避 | [・ファイル削除](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%95%E3%82%A1%E3%82%A4%E3%83%AB%E5%89%8A%E9%99%A4) | 侵入検知システム |
| [・難読化されたファイルまたは情報](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E9%9B%A3%E8%AA%AD%E5%8C%96%E3%81%95%E3%82%8C%E3%81%9F%E3%83%95%E3%82%A1%E3%82%A4%E3%83%AB%E3%81%BE%E3%81%9F%E3%81%AF%E6%83%85%E5%A0%B1) | AMSI対応アンチウイルスソフトの適用 |
| 侵入検知システム |
| [・悪意あるスクリプティングの実行](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E6%82%AA%E6%84%8F%E3%81%82%E3%82%8B%E3%82%B9%E3%82%AF%E3%83%AA%E3%83%97%E3%83%86%E3%82%A3%E3%83%B3%E3%82%B0%E3%81%AE%E5%AE%9F%E8%A1%8C) | 電子署名 |
| AppLocker |
| 認証情報アクセス | [・認証情報のダンプ](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E8%AA%8D%E8%A8%BC%E6%83%85%E5%A0%B1%E3%81%AE%E3%83%80%E3%83%B3%E3%83%97) | 特権アカウント管理 |
| Active Directoryの構成 |
| 多要素認証 |
| [・脆弱性を悪用した認証情報アクセス](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E8%84%86%E5%BC%B1%E6%80%A7%E3%82%92%E6%82%AA%E7%94%A8%E3%81%97%E3%81%9F%E8%AA%8D%E8%A8%BC%E6%83%85%E5%A0%B1%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9) | 脆弱性管理 |
| 情報の探索 | [・アカウントの探索](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%82%A2%E3%82%AB%E3%82%A6%E3%83%B3%E3%83%88%E3%81%AE%E6%8E%A2%E7%B4%A2) | ポリシー設定 |
| 監査(イベントログ） |
| [・ファイルとディレクトリの探索](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%95%E3%82%A1%E3%82%A4%E3%83%AB%E3%81%A8%E3%83%87%E3%82%A3%E3%83%AC%E3%82%AF%E3%83%88%E3%83%AA%E3%81%AE%E6%8E%A2%E7%B4%A2) | ダイナミックアクセス制御 |
| サーバーへの集約 |
| 監査(イベントログ） |
| [・ネットワークサービスのスキャン](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%8D%E3%83%83%E3%83%88%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E3%81%AE%E3%82%B9%E3%82%AD%E3%83%A3%E3%83%B3) | 脆弱性管理 |
| 侵入防止システム |
| ポート管理 |
| [・システム情報の探索](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E6%83%85%E5%A0%B1%E3%81%AE%E6%8E%A2%E7%B4%A2) | 脆弱性管理 |
| [・システムのネットワーク設定の探索](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E3%81%AE%E3%83%8D%E3%83%83%E3%83%88%E3%83%AF%E3%83%BC%E3%82%AF%E8%A8%AD%E5%AE%9A%E3%81%AE%E6%8E%A2%E7%B4%A2) | 監査(イベントログ） |
| [・システムユーザーの探索](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E3%83%A6%E3%83%BC%E3%82%B6%E3%83%BC%E3%81%AE%E6%8E%A2%E7%B4%A2) | ポリシー設定 |
| 監査(イベントログ） |
| 水平展開 | [・Pass the Hash](https://www.softwareisac.jp/ipa/index.php?%E3%83%BBPass+the+Hash) | Hashの取得阻止 |
| 水平展開の防止 |
| 垂直展開の防止 |
| 情報の収集 | [・ローカルシステムからのデータ収集](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%AD%E3%83%BC%E3%82%AB%E3%83%AB%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E3%81%8B%E3%82%89%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86) | 暗号化 |
| 監査(イベントログ） |
| 侵入防止システム |
| [・ネットワーク共有ドライブからのデータ収集](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%8D%E3%83%83%E3%83%88%E3%83%AF%E3%83%BC%E3%82%AF%E5%85%B1%E6%9C%89%E3%83%89%E3%83%A9%E3%82%A4%E3%83%96%E3%81%8B%E3%82%89%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86) | 簡単に軽減できない |
| [・データの圧縮](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E5%9C%A7%E7%B8%AE) | 監査(イベントログ） |
| 外部からの指令統制 (C&C) | [・一般的に利用されるポートの悪用](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E4%B8%80%E8%88%AC%E7%9A%84%E3%81%AB%E5%88%A9%E7%94%A8%E3%81%95%E3%82%8C%E3%82%8B%E3%83%9D%E3%83%BC%E3%83%88%E3%81%AE%E6%82%AA%E7%94%A8) | 監査(イベントログ） |
| ポート管理 |
| [・標準アプリケーションレイヤプロトコル(HTTP,SMTPなど)](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E6%A8%99%E6%BA%96%E3%82%A2%E3%83%97%E3%83%AA%E3%82%B1%E3%83%BC%E3%82%B7%E3%83%A7%E3%83%B3%E3%83%AC%E3%82%A4%E3%83%A4%E3%83%97%E3%83%AD%E3%83%88%E3%82%B3%E3%83%AB%28HTTP%2CSMTP%E3%81%AA%E3%81%A9%29) | 監査(イベントログ） |
| ポート管理 |
| [・データの暗号化](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E6%9A%97%E5%8F%B7%E5%8C%96) | 監査(イベントログ） |
| 持ち出し | [・データの暗号化](https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E6%9A%97%E5%8F%B7%E5%8C%96) | 監査(イベントログ） |

## ・悪意のあるファイルを添付したフィッシングメール

### 戦術：初期侵入

MITRE ATT&CK T1566.001 Phishing: Spearphishing Attachment[[31]](#footnote-31)

### 概説

攻撃者は、取引先や関係者を装い悪意あるプログラム（マルウェア）を電子メールに添付して送信します。本文には、添付ファイルの内容確認を促す内容が書かれています。添付ファイルを開くと、マルウェアが端末に送り込まれ、情報漏洩や改ざんなどの被害を受けます。

差出人は、eコマースサイト、宅配便業者、銀行、保険会社、クラウドサービス事業者、組織の上司、同僚、部下などさまざまですが、これらに限りません。また、同様の手法で、悪意のあるリンクを埋め込んだフィッシングメールがありますが、本対策を参考にしてください。

マルウェアの初期侵入の経路として、この手法は最も多用されており、被害を軽減するために対策を行う必要があります。攻撃側は、以下のような件名や巧みな文面で、心理的な圧迫を与え添付ファイルを開かせようとする特徴があります。

* ご意見をおねがいします
* アンケートのお願い
* 緊急
* 口座を封鎖
* アカウントが凍結されました
* 履歴書送付

### 緩和の方針

「悪意のあるファイルを添付したフィッシングメール」は、初期侵入で最も使われる手法であるため、多角的な緩和策の検討が必要です。

* 管理者特権を最小化し、原則的に標準ユーザーで運用します。
* 侵入には利用者の操作が伴うため、利用者のリテラシーを高めることを検討します。
* 電子メールやブラウザーの閲覧ができるセグメントと、重要資産にアクセスできるセグメントの分離を検討します。
* 添付ファイルのスキャンなどの検知システムの導入を検討します。

### 運用やNetworkが変更された場合の影響の有無

後述する重要資産を保有するコンピューターでのWebや電子メールの閲覧は極めてリスクを高くすることから、運用規程の整備と遵守が重要です。

### 優先すべき措置

緩和の方針に基づき、以下を優先します。

* 管理者特権の限定運用の適用。  
  端末/サーバーの利用者権限が管理者権限で実行されている場合、悪意のあるプログラムは管理者特権で実行されるため、極めて危険です。このため、利用者の権限を標準ユーザーにすることは、大変効果的かつ侵入以降の攻撃の緩和に役立ちます。

業務で管理者特権が必要な端末/サーバーは文書化し、検出を強化します。

* ユーザートレーニング。  
  Office文書、PDF文書の保護ビューの重要性の理解を得ます。また、最新のフィッシングメールに関する情報共有や、アンチウイルスソフトのアップデート、完全スキャンの実施方法、OS、アプリケーションのアップデートの実施、確認方法等のユーザートレーニングを検討します。
* 電子メール、Web閲覧が許可される端末と、重要資産を有するシステム・端末の厳格な分離の検討。   
  インターネットセグメントに接続可能な端末と、インターネットセグメントに接続できない重要資産を有するコンピュータの分離、アクセスコントロールの厳格化を検討します。
* インターネットセグメント接続可能端末は、添付ファイルの無害化、組み込みリンクの無害化の実施。  
  アンチウイルスソフト、Endpoint Detection and Response、侵入検知システムの導入の検討を検討します。アプリケーションポリシーによる危険な拡張子（ .scr、 .exe、 .pif、 .cplなど）の排除、圧縮ファイルや本文に埋め込まれたリンクの分析を行うサンドボックス等による添付ファイルの無害化、組み込みリンクの無効化を検討します。

### ユーザー運用管理責任

#### リスクの受容

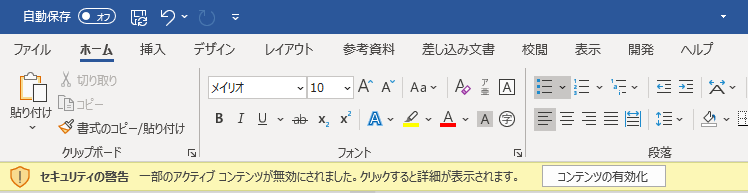
守るべき資産が電子メールやWebサイトから適切に分離されており、守るべき資産が暗号化されていて、情報の漏洩、改ざんを受けても実質的な情報漏洩や暴露等の被害が軽微と想定される場合は受容します。

ただし、経営者、秘書、取締役、執行役、研究者、システム管理者など、日常的に重要資産に接している職務に対しては、リスクを受容すべきではありません。

また、プログラム開発担当者はデバッグのために管理者権限が必要であり、悪用されやすいDebug用のコマンドを利用すること、Help Desk担当者は、ドメイン管理者権限を有することがあることから、最もリスクが高いといえます。

|  |  |  |
| --- | --- | --- |
| **業務** | **特権** | **リスク受容のための条件例** |
| プログラム開発担当者 | Local Administrator | メールやWeb閲覧の分離、侵入監視、ログ監査、開発/Help Desk業務で使用するアカウントと一般業務アカウントの分離、定期的なトレーニング、厳格な脆弱性管理 |
| Help Desk 担当者 | Domain/Local Administrator |
| システム管理者 | Enterprise/Domain/Local Administrator | 管理業務端末の分離、メールやWeb閲覧の分離、侵入監視、ログ監査、管理業務で使用するアカウントと一般業務アカウントの分離、定期的なトレーニング、厳格な脆弱性管理 |
| 部門管理者（OUの委任） | OUのパスワードリセット、グループ管理、ドメイン参加等 |
| VBA/スクリプト利用者 | 標準ユーザー | VBA/スクリプト署名、侵入監視、ログ監査、定期的なトレーニング、Local Administrators に含めない、厳格な脆弱性管理 |
| 役職者、研究者、秘書 | 標準ユーザー | 侵入監視、ログ監査、定期的なトレーニング、Local Administrators に含めない、厳格な脆弱性管理 |
| 上記以外の一般業務担当者 | 標準ユーザー | 定期的なトレーニング、Local Administrators に含めない、厳格な脆弱性管理 |

#### 啓発・教育

* すべての端末利用者   
  フィッシング対策協議会から最新の手口を入手し、理解を求めてください。  
  知らない・不明な・不審な・日本語がおかしいファイルを開かない、セキュリティの警告が出た場合は開かない・印刷せず、場合によっては、電話で発信者に確認を取るよう求めてください。  
  Office、PDF ビューワーの保護されたビュー（サンドボックス）の重要性の理解を求めてください。

図：Word セキュリティの警告 右下の [コンテンツの有効化] をクリックすることでOfficeマクロが実行される。

* 開発者、ヘルプデスク担当者   
  "初期侵入" から "悪意あるプログラムの実行" までの攻撃ベクターでの攻撃阻止の重要性の理解を求めてください。  
  管理者権限でのインターネット接続、メール受信などのリスクを正しく認識させます。
* 重要資産にアクセスする経営者、秘書、研究者など

"初期侵入" から "悪意あるプログラムの実行" までの攻撃ベクターでの攻撃阻止の重要性の理解を求めてください。重要資産保護のための暗号化の重要性について理解を求めてください。

#### 管理規程

実効性を担保するため、以下の管理規程の整備を検討して下さい。

* 電子メールクライアント、Webブラウザの使用禁止する端末・サーバーの厳格な定義、これらの監査規程。
* 確実なアップデートの実施と完全スキャンの強制のための、脆弱性アップデート及びアンチウイルスソフト運用規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

* 13 ・レベル1セキュリティ構成（Windows 10）及び14 ・Windows Server 2016 Domain Controller の適用を検討して下さい。
* Microsoft Outlook 2016 の場合、マクロを悪用するフィッシングメール対策として以下のポリシーが存在します。
  + [ユーザーの構成]>[ポリシー>管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[セキュリティフォーム設定]>[Outlook セキュリティモード] を [有効] に設定し、オプション [Outlook セキュリティポリシー] を [Outlook セキュリティのグループ ポリシーを使用する] に設定します。
  + [ユーザーの構成]>[ポリシー>管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[セキュリティセンター]>[マクロのセキュリティ設定] を [有効] に設定し、オプション [セキュリティレベル] を [署名されている場合は警告を表示し、署名されていない場合は無効にする] に設定します。
  + [ユーザーの構成]>[ポリシー>管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[添付ファイルのセキュリティ設定をユーザーが変更できないようにする] を [有効] に設定します。
  + [ユーザーの構成]>[ポリシー>管理用テンプレート]>[Microsoft Outlook 2016]>[セキュリティ]>[セキュリティセンター]>[フィッシング詐欺の疑いがある電子メールメッセージのハイパーリンクを有効にする] を [無効] に設定します。

#### モニタリング

権限に応じて、以下のモニタリングを検討します。

* 電子メールクライアント、Webブラウザを使用禁止する端末・サーバーで、以下の状況を確認します。
  + 電子メールクライアントがインストールされていない。
  + Webブラウザが使用できない設定となっている。
* OS、アプリケーションのアップデートの状況を確認します。
* アンチウイルスソフトのアップデートの状況を確認します。
* アプリケーションソフトのインストールの状況を確認します。
* コマンドライン、スクリプトの実行、セキュリティ権限の変更、ログオン成功・失敗のログを監査します。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

情報資産の重要度に応じて以下を検討します。

* メール閲覧端末と重要資産システムとのネットワークセグメントの分離。
* 管理用端末と一般業務用端末のネットワークセグメントの分離。
* 状況に応じ重要資産システムセグメント及びそのセグメントに接続する端末等でのPOP、SMTP、IMAP、HTTP、HTTPS等のメール関連プロトコルの停止。
* Office文書、PDF文書の保護されたビューの設定。
* 侵入検知システム、メールフィルタリングシステムの導入により、.scr、.exe、.pif、.cpl、   
  .ps1、.vbs などの実行形式やスクリプトの拡張子の添付ファイルを排除する。
* サンドボックスを導入し、上記ファイルや、.zip、.rarなどの圧縮されたファイルを展開し、悪意のある添付ファイルを排除する。

#### 仮想端末運用

プログラム開発者、HelpDesk担当者、システム管理者については、電子メール、Web閲覧などの一般業務を行う端末と、重要資産システムの管理端末へのアクセスや開発業務を行う端末を、仮想端末で分離し、また、ネットワークセグメントの分離を検討します。

#### ゲートウェイ及びエンドポイント対策

以下のエンドポイント対策の実施を検討します。

* 脆弱性アップデートの実施と監査。
* アンチウイルスソフトの日次パターンファイルの更新、日次クィックスキャン、週次完全スキャンの実施。
* Endpoint Detection and Response もしくは、侵入検知システムの導入を検討してください。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施してください。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施する。

## ・コマンドラインインターフェースの悪用

### 戦術：悪意のあるプログラムの実行

MITRE ATT&CK T1059.003 Command and Scripting Interpreter: Windows Command Shell[[32]](#footnote-32)

### 概説

OSの標準機能であるコマンドラインインターフェースを悪用することで、悪意あるプログラムを実行します。リモートデスクトップやリバースシェルセッションなどを介してローカルもしくはリモートで操作します。

コマンドラインインターフェースは、多くの場合、ログオンしているユーザーのセキュリティ権限で動作するため、ユーザーに管理者権限を与えている場合は厳重な防御が必要となります。

開発用のデバッグコマンドの一部には、外部からプログラムを読み込む機能や、ユーザーアカウント制御 (UAC) をバイパスして悪意あるプログラムを実行させることができるため、一般業務と開発業務を厳重に分離することは、リスク低減に役立ちます。

### 緩和の方針

OSの標準機能を悪用するため、完全な防御は困難な場合があります。

* 端末の利用者権限が管理者権限で実行されている場合、コマンドは特権で実行されるため、極めて危険です。このため、利用者の権限を標準ユーザーにすることは、大変効果的で、この攻撃の緩和に役立ちます。
* Windows Defenderアプリケーション制御、Windows AppLocker（要ライセンス）、などで、ホワイトリスト管理、ブラックリスト管理を実施し、不要なコマンドの実行制御を検討します。
* アプリケーション制御が困難な場合は、ログの定期監査を実施し、不審なコマンド実行を検知します。
* 開発で使用するデバッグコマンドは、外部からコードやプログラムを読み込み実行する機能を持つものがあります。このため、これらのデバッグコマンドを利用する開発業務端末と一般業務端末のネットワーク、サーバーの論理的な分離は、拡散防止の観点から有効です。

### 運用やNetworkが変更された場合の影響の有無

重要資産を有する端末、サーバーで、管理者権限でデバッグコマンドなどが利用許可されると、マルウェアにコマンドを実行されるリスクが高まります。不用意な開発環境 (SDK) の展開を防止する必要があります。

### 優先すべき措置

* 管理者権限は極めて限定的に付与し、一般業務では標準ユーザーで運用する。
* 管理者権限が必要な場合は、Windows Defenderアプリケーション制御、もしくは AppLocker の導入の検討をする。
* コマンドライン実行ログの取得と監査を実施する。

### ユーザー運用管理責任

#### リスクの受容

防御の方式によって実行の阻止、実行後の検知とリスクの性質が異なりますので、詳細な検討が必要です。

|  |  |  |
| --- | --- | --- |
| **業務** | **特権** | **リスク受容のための条件例** |
| プログラム開発担当者 | Local Administrator | 侵入監視、コマンドラインログ監査、定期的なトレーニング |
| Help Desk 担当者 | Domain/Local Administrator |
| システム管理者 | Enterprise/Domain/Local Administrator |
| 部門管理者（OUの委任） | OUのパスワードリセット、グループ管理、ドメイン参加等 |
| 役職者、研究者、秘書 | 標準ユーザー | 侵入監視、定期的なトレーニング、Local Administrators に含めない |
| 上記以外の一般業務担当者 | 標準ユーザー | 定期的なトレーニング、Local Administrators に含めない |

#### 啓発・教育

* + 対象：開発者、ヘルプデスク担当者
* 開発・ヘルプデスク端末のリスクの認識、管理規程の正しい理解を求めます。
* 開発環境やSDKを端末に展開した場合は、文書化し、管理対象として監査することの重要性の理解を求めます。
* "初期侵入" から "悪意あるプログラムの実行" までの攻撃ベクターで攻撃を阻止しないと、情報窃取、送信、漏洩等のリスクが高まることを理解させます。
* 管理者権限でのインターネット接続、メール受信、添付ファイルを開くなどのリスクを正しく認識させます。

#### 整備すべき規程

以下の規程の整備を検討します。

* 開発端末、ヘルプデスク端末のログ取得及び監査規程

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

以下のポリシーの適用を検討します。

* [13 ・レベル1セキュリティ構成（Windows 10）] 及び [14 ・Windows Server 2016 Domain Controller] の適用。
* 後述の [17.9・コマンドラインインターフェースの監査] の適用。

#### モニタリング

以下の監査の実施を検討します。

* 重要資産が保存されているサーバー、端末でのセキュリティログ Event ID 4688 の監査。
* ホワイトリスト、ブラックリストによるアプリケーション制御を実施している場合は、違反の状況の分析を実施する。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

開発端末、ヘルプデスク端末と重要資産を有する端末、サーバーの厳格なセグメント分離を検討します。

以下を参考にWindows Defender アプリケーション制御 もしくは Windows AppLocker でコマンドの実行を制限します。  
※Windows AppLocker は Windows 10 はEnterprise Editionが必要です。

* WDAC または AppLocker のどちらを使用するかを選ぶ:https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control
* Microsoft が推奨するブロックの規則:https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

Endpoint Detection and Response もしくは、侵入検知システムの導入を検討してください。

### 受託開発ベンダー管理責任

#### セキュアコーディング

Task Scheduler の設定や、プログラムや子プロセスの実行権限については文書化してユーザーと共有します。この際、最小特権原則で実行されているかを明確にしてください。~

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じる。 例外はすべて文書化し、適切な監査を実施します。

### ・コマンドラインインターフェースの監査

#### 設定方法

以下のグループポリシーを設定します。

* 監査ポリシー カテゴリの設定を上書きする
  + [コンピューターの構成]>[ポリシー]>[Windows の設定]>[セキュリティ設定]>[ローカルポリシー]>[セキュリティオプション]>[監査: 監査ポリシー サブカテゴリの設定 (Windows Vista 以降) を強制して、監査ポリシー カテゴリの設定を上書きする] の [このポリシーの設定を定義する] をチェックし、[有効] をクリックします。
* 監査プロセス作成の監査
  + [コンピューターの構成]>[ポリシー]>[Windows の設定]>[セキュリティ設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[詳細追跡]>[プロセス作成の監査]の [成功]、[失敗] を構成します。
* プロセス作成の監査にコマンドラインを含める
  + [コンピューターの構成] >> [管理用テンプレート] >> [システム] >> [プロセス作成の監査] >> [プロセス作成イベントにコマンドラインを含める]のポリシー値を [有効] に設定します。

#### 監査方法

イベントビューワーで [Windows ログ]>[セキュリティ] からEvent ID 4688 等を検索し、不審なコマンドの実行を調査します。

JPCERT/CCの「インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書」を参考にしてください。[[33]](#footnote-33)

## ・PowerShellの悪用

### 戦術:悪意あるプログラムの実行

MITRE ATT&CK T1059.001 Command and Scripting Interpreter: PowerShell[[34]](#footnote-34)

### 概説

Windowsの設定管理を行うスクリプト言語であるPowerShellを悪用し、悪意あるプログラム(マルウェア）を実行します。PowerShell は、Windows の API にアクセス可能であり、かつ、インターネットアクセスなどの機能も提供されているため、攻撃の中核となるテクノロジーともいえます。そのため、外部との通信（新たなプログラムのダウンロード）や端末情報や認証情報の窃取など、多種多様なコマンドの実行が考えられます。

スクリプトは難読化されることが多く、侵入検知システムやアンチウイルスソフトでの検知が困難な場合があり注意が必要です。

DefaultではPowerShellの実行は無効に制限されていますが、実行が有効となっている端末では攻撃を受ける可能性が高く、慎重な運用が必要です。

古いバージョンである PowerShell2.0 は、ログ機能などのセキュリティ機能がないため、検出を免れるためにダウングレード攻撃が発生しています。また、制限設定を回避する手法も多数研究されていることから、緩和策設定後も、定期的に新たなバイパス手法の情報入手と対策を講じる必要があります。

### 緩和の方針

さまざまな緩和策をバイパスする方法が研究されています。完全な防御は困難ですが、多角的な緩和措置が必要です。

* 管理端末以外はPowerShellスクリプトを無効（Default)にします。
* PowerShell が許可された端末、サーバーでは、PowerShellスクリプトに電子署名を実施し、署名付きPowerShellスクリプトのみ実行許可とするか、 AppLocker 等でのホワイトリストの導入を検討します。

### 運用やNetworkが変更された場合の影響の有無

PowerShellの実行が有効とした端末では、メール添付のファイルの実行、Webサイトの閲覧などで、悪意あるプログラムの実行のリスクが高まります。

### 優先すべき措置

* ダウングレード攻撃を阻止するため、役割と機能の削除ウィザードで Windows PowerShell 2.0 エンジン を削除します。
* PowerShell スクリプトの実行可能端末・サーバーを限定し、文書化した上で、PowerShell スクリプトに電子署名を実施します。その他の端末・サーバーではグループポリシーで PowerShell スクリプトの実行を禁止します。
* 管理上、PowerShell を必要とするサーバー、端末のログの取得と監査を実施します。
* AppLocker もしくは、Windows Defender アプリケーション制御による、以下のモジュールの制御、スクリプト制御の併用を検討します。
  + - powershell.exe、powershell\_ise.exe (32bit, 64bit)
    - System.Management.Automation.dll (32bit, 64bit)
    - System.Management.Automation.ni.dll (32bit, 64bit)
* [18.9 WinRMサービスを無効化/制限] を参照して、リモート実行でPowerShellが使用されないようにします。

### ユーザー運用管理責任

#### リスクの受容

PowerShellスクリプトの実行可能端末・サーバーは、設定されたセキュリティポリシーだけでなく、端末・サーバーのネットワーク構成、運用方法によって影響が異なるため、慎重なリスクの見極めが必要です。

##### ドメインコントローラー、DHCPサーバー、開発用端末、管理用端末

これらはシステム設定管理上、PowerShell は必須といえます。従って、ホワイトリストの導入、PowerShell スクリプトの署名やログ監査による早期検出でのリスク受容を検討します。

##### アプリケーションサーバー、ファイルサーバー、業務端末

これらは PowerShell は必須といえないので、AppLocker等での実行制御をするか、Office VBA（マクロ）の厳格運用とVBScript の運用停止による初期侵入から悪意のあるプログラムの実行までのベクトルの遮断とログ監査による早期検出でリスク受容することが考えられます。

| **実行ポリシー** | **署名付き** | **署名なし ローカル** | **署名なし 非ローカル** | **概要** |
| --- | --- | --- | --- | --- |
| Restricted | × | × | × | 全てのスクリプトが実行禁止。PowerShellまたはWindows OSインストール直後のデフォルト設定（Windows Server 2012 R2を除く） |
| AllSigned | ○ | × | × | 署名されているスクリプトのみが実行可能。署名されていないスクリプトは実行禁止 |
| RemoteSigned | ○ | ○ | × | ローカルに保存されているスクリプトは実行可能。インターネットからダウンロードしたスクリプト（非ローカルのスクリプト）は、署名されているもののみが実行可能。Windows Server 2012 R2では、この設定がデフォルト |
| Unrestricted | ○ | ○ | △ | 全てのスクリプトが実行可能。ただしインターネットからダウンロードしたスクリプトは、実行するかどうかが確認されるので、ユーザーが明示的に許可した場合のみ実行される |
| Bypass | ○ | ○ | ○ | 警告やユーザーへの確認なしに、全てのスクリプトが実行可能 |

出典：atmarkIT WindowsでPowerShellスクリプトの実行セキュリティポリシーを変更する[[35]](#footnote-35)

|  |  |  |
| --- | --- | --- |
| **業務** | **特権** | **リスク受容のための条件例** |
| プログラム開発担当者 | Local Administrator | PowerShell スクリプト開発環境の分離（リリース後は署名する）  AllSigned適用、侵入監視・Endpoint Detection and Response の導入、PowerShell スクリプトログ監査、定期的なトレーニング |
| Help Desk 担当者 | Domain/Local Administrator |
| システム管理者 | Enterprise/Domain/Local Administrator |
| 部門管理者（OUの委任） | OUのパスワードリセット、グループ管理、ドメイン参加等 |
| 役職者、研究者、秘書 | 標準ユーザー | Restricted適用、Local Administrators に含めない |
| 上記以外の一般業務担当者 | 標準ユーザー | Restricted適用、Local Administrators に含めない |

##### 啓発・教育

* 対象：ローカル Administrator メンバー、開発者   
  PowerShell を利用した攻撃方法の理解を求め、PowerShell 利用端末の危険性の認識、管理規程の正しい理解を求めます。

##### 管理規程

以下の規程の整備を検討してください。

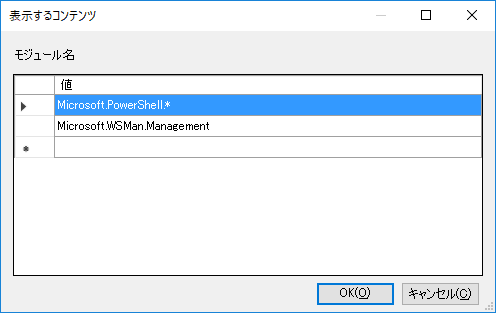
* 業務上、PowerShellの実行環境が必要な端末、サーバーの文書化及び監査規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

以下のポリシーの適用を検討します。

* [13章 ・レベル1セキュリティ構成（Windows 10）] 及び [14章 ・Windows Server 2016 Domain Controller] の適用。
* PowerShell 2.0 の無効化。PowerShell 2.0 を無効化することで、PowerShell 5.0 スクリプトブロックのログ機能を回避するダウングレード攻撃を緩和する。
  + [コントロールパネル]>[プログラム]>[プログラムと機能]>[Windows の機能の有効化または無効化]>[Windows PowerShell 2.0] のチェックボックスを外す。
* グループポリシーで PowerShellのログを有効にする。
  + [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Windowsコンポーネント]>[Windows PowerShell]>[モジュールログを有効にする] を **[有効]** に設定し、[オプション]>[モジュール名]>[表示] をクリックする。
  + [モジュール名] の入力画面で、[値] に [Microsoft.PowerShell.\*] [Microsoft.WSMan.Management] の2行を入力し、[OK] をクリックする。（以下の図を参照。）



#### モニタリング

ポリシーを設定した上で、PowerShell スクリプト実行のログを有効化します。

* [イベントビューアー]-[アプリケーションとサービス ログ]-[Microsoft]-[Windows]-[PowerShell]-[Operational] を右クリックし、[プロパティ] をクリックし、[ログを有効にする] にチェックを入れる。
* 最大ログサイズを10048KB以上にし、[イベントを上書きしないでログをアーカイブする]をチェックする。
* 定期的に [イベントビューアー]-[アプリケーションとサービス ログ]-[Microsoft]-[Windows]-[PowerShell]-[Operational] を監査する。

攻撃者はレジストリを書き換え、PowerShell のログを無効にすることがあります。

* [12章・Windows Group Policyの再読み込み] を設定していない場合は、定期的に以下のレジストリの値をチェックする。

|  |  |
| --- | --- |
| **項目** | **値** |
| レジストリハイブ | HKEY\_LOCAL\_MACHINE |
| キー | \SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging |
| 名前 | EnableScriptBlockLogging |
| 種類 | REG\_DWORD |
| データ | 0x00000001(1) （有効） |

#### ネットワークデザイン、アクセスコントロール、フィルタリング

以下を参考にWindows Defender アプリケーション制御 もしくは Windows AppLocker でコマンドの実行を制限します。※Windows AppLocker は Windows 10 はEnterprise Editionが必要です。

* WDAC または AppLocker のどちらを使用するかを選ぶ:  
  https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control  
  Microsoft が推奨するブロックの規則:  
  https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules  
  ただし、PowerShell without PowerShell などの Bypass 方法が研究されているため検討が必要。[[36]](#footnote-36)
* PowerShell Constrained Language Mode [[37]](#footnote-37)(制約付き言語モード）の導入を検討する。
* WinRMサービスを無効化する。（WinRMサービスを無効化/制限を参照）

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

Endpoint Detection and Response もしくは、侵入検知システムの導入を検討してください。

### 受託開発ベンダー管理責任

#### セキュアコーディング

* 作成したPowerShellスクリプトへのタイムスタンプ付き署名の実施。
* 実行運用環境に限定した実行ポリシーの適用（対象端末・サーバーはAllSigned、対象外はRestricted）。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

### WinRMサービスを無効化/制限

#### グループ ポリシーを使用してリモート管理を無効にする

ローカルグループポリシーエディターを開くには、次のいずれかの操作を行います。

1. Windows Server 2016、Windows Server 2012 R2、または Windows Server 2012 を実行しているサーバーで、「グループポリシーの管理」を起動します。
2. ポリシーオブジェクトを選択し、右クリックして編集をクリックします。
3. グループポリシー管理エディターで、[コンピューターの構成]>[管理用テンプレート]>[Windows コンポーネント]>[windows リモート管理 (winrm)]>[Winrm サービス] を開きます。
4. コンテンツ ウィンドウで [WinRM によるリモート サーバー管理を許可する] をダブルクリックします。
5. [WinRM によるリモート サーバー管理を許可する] ポリシー設定のダイアログ ボックスで、[無効] をクリックしてリモート管理を無効にします。[OK] をクリックして変更内容を保存し、ポリシー設定のダイアログ ボックスを閉じます。

#### WinRM が使用するポートをパーソナルFirewallで閉じる

PowerShell を管理者モードで起動し、以下のコマンドを実行します。

Set-NetFirewallRule -name WINRM-HTTP-In-TCP -Enabled False

Set-NetFirewallRule -Name WINRM-HTTP-In-TCP-PUBLIC -Enabled False

#### WinRM機能を無効化する

PowerShell を管理者モードで起動し、以下のコマンドを実行します。

Disable-PSRemoting -Force

## ・Windowsタスクスケジューラ at, schtasks の悪用

### 戦術：悪意あるプログラムの実行

MITRE ATT&CK T1053.002 Scheduled Task/Job: At (Windows)[[38]](#footnote-38)  
 T1053.005 Scheduled Task/Job: Scheduled Task[[39]](#footnote-39)

### 概説

at コマンド(Windows 8.1まで）や、schtasks コマンド(windows10) は、予め定めた時刻にプログラムを実行させるOS標準のツールです。これらを使い悪意あるプログラム（マルウェア）を密かに起動することが可能です。

また、schtasks コマンドは、リモートコンピュータに対しても設定が可能なため、AdministratorsのメンバーのID/Passwordが窃取されていた場合、ネットワーク上の他の端末、サーバーに対してタスクの設定が可能です。但し、リモートコンピュータ上のパーソナルファイアーウォールで「ファイルとプリンターの共有」が閉じている場合はリモート設定が不可能になりますので、必要に応じて、パーソナルファイアーウォールの「ファイルとプリンターの共有」を無効にすることも検討してください。同様に、ローカルのAdministratorのID/Passwordが全社共通の場合は、大規模な水平展開が可能となります。この手法の防御については、Pass The Hash、LAPSを参照してください。

### 緩和の方針

新たなタスクの登録の検出に努めます。

### 運用やNetworkが変更された場合の影響の有無

アカウントの認証情報が漏洩すると、悪用されるリスクが非常に高くなります。極力、限定された権限のアカウントを利用します。

### 優先すべき措置

検出を優先します。

* タスクスケジューラの登録を監査する。詳細は18.9 タスクスケジューラのポリシー設定を参照。
  + イベントログ「Microsoft-Windows-TaskScheduler/Operational」で、イベントID 106 [タスクが登録されました] を調査し、文書化された登録タスク以外のタスクを検索する。
* 認証済みアカウントのコンテキストでタスクを実行するようにスケジュールされたタスクの設定を構成する。

### ユーザー運用管理責任

#### リスクの受容

ドメインコントローラー、メンバーサーバーと特権管理者の端末に対して新たなTaskが追加されているかを監査します。

|  |  |  |
| --- | --- | --- |
| **業務** | **特権** | **リスク受容のための条件例** |
| プログラム開発担当者 | Local Administrator | ドメインコントローラー、メンバーサーバー、担当者端末のTask Scheduler ログ監査。 |
| Help Desk 担当者 | Domain/Local Administrator |
| システム管理者 | Enterprise/Domain/Local Administrator |
| 部門管理者（OUの委任） | OUのパスワードリセット、セキュリティグループ管理、ドメイン参加等 |
| 役職者、研究者、秘書 | 標準ユーザー | Local Administrators に含めない |
| 上記以外の一般業務担当者 | 標準ユーザー | Local Administrators に含めない |

#### 啓発・教育

特権管理者に対し Task Scheduler の危険性の理解を求めます。

#### 管理規程

以下の規程の整備を検討します。

* タスク登録を文書化します。
* ドメインコントローラー、メンバーサーバー、特権管理者の端末のタスクスケジューラの監査規程を策定します。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

後述の[19.9 タスクスケジューラのポリシー設定] を参照してください。

#### モニタリング

後述の[19.9 タスクスケジューラのポリシー設定] を参照してください。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

該当しません。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

Endpoint Detection and Response もしくは、侵入検知システムの導入を検討してください。

### 受託開発ベンダー管理責任

#### セキュアコーディング

タスクスケジューラが起動するプログラム、スクリプトの権限を最小化し、文書化し、ユーザーと合意してください。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

### ・タスクスケジューラのポリシー設定

MITRE ATT&CK では、緩和策として「ドメイン コントローラー: Server Operators がタスクのスケジュールを割り当てるのを許可する」の設定を推奨していますが、このポリシーはATコマンドに対してのみ有効です。一方で、ATコマンドはWindows 10/Windows Server 2012以降廃止されているため、効果が期待できません。このため、システムの特性に応じて、監査を強化し検出に努めます。

#### タスクスケジューラ ジョブの作成、有効化の監査（グループポリシー）

グループポリシーで [その他のオブジェクトアクセス イベントの監査のプロパティ] を設定します。

[コンピュータの構成]>[ポリシー]>[Windowsの設定]>[セキュリティの設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[オブジェクトアクセス]>[その他のオブジェクトアクセス イベントの監査のプロパティ] で [次の監査イベントを構成する] にチェックをいれ、[成功] と [失敗] にチェックを入れます。

これにより、新規にタスクが作成されると、[イベントビューアー]>[Windowsログ]>[セキュリティ] に [4698]-[その他のオブジェクト アクセス イベント] が登録されます。

また、[イベントビューアー]>[アプリケーションとサービスログ]>[Microsoft]>[Windows]> [TaskScheduler] >[Operational] で [106]-[タスクが登録されました] 、[142]-[タスクが無効になりました] が登録されます。 スケジューラ ジョブの監査対象は以下の通りです。

* タスクの登録 Event ID 106
* タスクの更新 Event ID 140
* タスクの削除 Event ID 141
* タスクの無効化 Event ID 142

#### タスクスケジューラ ジョブの作成、有効化の監査（ローカル）

[イベントビューアー]>[アプリケーションとサービスログ]>[Microsoft]>[Windows]> [TaskScheduler]>[Operational] で右クリックし、[プロパティ] をクリックします。[ログを有効にする] をチェックし、最大ログサイズを [10240KB]以上に設定し、[イベントを上書きしないでログをアーカイブする] をチェックします。

[TaskScheduler]>[Operational] を有効にすると、[セキュリティログ] に [4698] および [4702] [その他のオブジェクト アクセス イベント] が発生します。

* [4698]-[その他のオブジェクト アクセス イベント]-[スケジュールされたタスクが作成されました。]
* [4702]-[その他のオブジェクト アクセス イベント]-[スケジュールされたタスクがアップデートされました。]

#### タスクスケジューラー Event ID

|  |  |  |
| --- | --- | --- |
| **Event ID** | **Task Category** | |
| 100 | タスクの開始 | |
| 101 | タスクの開始が失敗しました | |
| 102 | タスクが完了しました | |
| 103 | 操作の開始が失敗しました | |
| 106 | タスクが登録されました | |
| 107 | スケジューラによってトリガーされるタスク | |
| 108 | イベントによってトリガーされるタスク | |
| 110 | ユーザーによってトリガーされるタスク | |
| 111 | タスクが終了しました | |
| 114 | 実行されなかったタスクが起動されました | |
| 118 | コンピューターの起動によってトリガーされるタスク | |
| 119 | ログオンによってトリガーされるタスク | |
| 129 | タスクのプロセスが作成されました | |
| 135 | Launch condition not met, machine not idle | |
| 140 | タスクの登録が更新されました | |
| 141 | タスクの登録が削除されました | |
| 142 | タスクが無効になりました | |
| 200 | | 開始された操作 |
| 201 | | 操作が完了しました |
| 202 | | 操作に失敗しました |
| 203 | | Action failed to start |
| 301 | | Task engine properly shut down |
| 310 | | Task Engine started |
| 311 | | Task Engine failed to start |
| 314 | | Task Engine idle |
| 317 | | Task Engine started |
| 318 | | Task engine properly shut down |
| 319 | | Task Engine received message to start task |
| 322 | | Launch request ignored, instance already running |
| 329 | | Task stopping due to timeout reached |
| 332 | | Launch condition not met, user not logged-on |
| 400 | | Service started |
| 411 | | Service signaled time change |
| 700 | | Compatibility module started |

## ・悪意あるスクリプティングの実行

### 戦術：悪意あるプログラムの実行、永続化、防御の回避

MITRE ATT&CK T1059 Command and Scripting Interpreter[[40]](#footnote-40)   
T1059.001 Command and Scripting Interpreter: PowerShell  
T1059.003 Command and Scripting Interpreter: Windows Command Shell  
T1059.005 Command and Scripting Interpreter: Visual Basic  
T1059.006 Command and Scripting Interpreter: Python  
T1059.007 Command and Scripting Interpreter: JavaScript/JScript  
T1037.001 Boot or Logon Initialization Scripts: Logon Script (Windows)

### 概説

Windowsの場合は、VBScript、PowerShell、コマンドラインバッチがスクリプティングに該当します。また、開発環境やサーバーでは、Python、JavaScript/JScriptも該当します。それぞれ、コマンドの実行や条件判断が可能で、複雑な管理処理を容易にするためのOSの標準的なプログラミング機能ともいえます。

脅威の多くは、Word、Excelなどのデスクトップアプリケーションで利用が可能なVisual Basic for Application (VBA)や、VBScriptを初期の侵入に使い、侵入に成功すると、PowerShellやコマンドラインインターフェースを使用して、マルウェア本体のダウンロードや情報の収集、水平展開を図ります。

### 緩和の方針

スクリプトが必要な端末を特定し、電子署名されたスクリプトのみ実行許可とします。もしくはAppLockerによるスクリプト制御を検討します。但し、スクリプトを使ったファームアップデートなどがあることから注意が必要です。

VBAが不要な端末には Office のグループポリシーでVBAの実行を Default で禁止設定し、必要な端末では電子署名されたVBAのみ実行許可とし、全端末で保護されたビューを有効にします。

### 運用やNetworkが変更された場合の影響の有無

管理されていない端末でスクリプトの実行が許可されると、検知が困難になりリスクが高くなります。新たにスクリプトを許可する場合は、必ず文書を改訂し、監査対象とする必要があります。

### 優先すべき措置

以下の措置を優先します。

* Windowsの場合、VBA、PowerShellに電子署名を実施し、電子署名された Script だけを実行許可にする。電子署名証明書は秘密鍵のエクスポートが出来ないように設定する。
* アジャイル開発等で電子証明書の導入が困難な場合は、AppLocker 等の導入を検討する。
* 端末の特定と文書化、ログ監査を実施する。

### ユーザー運用管理責任

#### リスクの受容

一般的にスクリプトはOSの標準機能のため、動作を完全に停止することが困難な場合があります。スクリプトを実行する端末、サーバーには重要資産を保存しないことで、この脅威を受容し、他の防御方法を検討します。

|  |  |  |
| --- | --- | --- |
| **業務** | **特権** | **リスク受容のための条件例** |
| プログラム開発担当者 | Local Administrator | スクリプトへの署名。スクリプトの使用の文書化と監査。  ドメインコントローラー、メンバーサーバー、担当者端末のスクリプト実行のログ監査。 |
| Help Desk 担当者 | Domain/Local Administrator |
| システム管理者 | Enterprise/Domain/Local Administrator |
| 部門管理者（OUの委任） | OUのパスワードリセット、セキュリティグループ管理、ドメイン参加等 |
| VBAを利用する業務担当者 | 標準ユーザー | スクリプトへの署名、担当者端末のスクリプト実行ログの監査。Local Administrators に含めない。 |
| 役職者、研究者、秘書 | 標準ユーザー | Local Administrators に含めない。 |
| 上記以外の一般業務担当者 | 標準ユーザー | Local Administrators に含めない。 |

#### 啓発・教育

* 対象：すべての端末利用者
  + インターネットからダウンロードした、もしくは、電子メールに添付された Office 文書、PDF は保護されたビューで閲覧するようにし、編集・印刷する際は、信頼できるダウンロード先か、信頼できる送信元かを確認した上で編集・印刷するように理解を求めます。
* 対象：Office VBA利用者
  + マクロの実行許可された端末はマルウェア攻撃の可能性が高いことを理解させます。
  + マクロファイル利用中の電子メール、Web閲覧のリスクを理解させます。
  + 署名が出来ない場合は、通常はマクロの実行を禁止しておき、マクロ付きファイルを開く際にマクロ実行を許可し、処理が終了したら、マクロの実行を禁止するバッチファイルの作成、利用を義務付け、もしくは代替措置を講じます。

#### 管理規程

以下の規程の整備を検討します。

* 管理上、スクリプティングが必要な端末、サーバーの監査規程。
* 電子署名用証明書の管理規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

以下のポリシー設定を検討して下さい。

* [17章・コマンドラインインターフェースの悪用]、[18章・PowerShellの悪用] を参考にして、コマンド、スクリプト実行のログ取得を設定する。
* [20.11 Visual Basic for Application（VBA、マクロ） の課題] を参考にして、VBA使用が必要な端末の制御設定をする。

#### モニタリング

以下の監査の実施を検討します。

* コマンドラインインターフェースの監査
  + 前項のポリシーを設定の上、[イベントビューアー]-[Windowsログ]-[セキュリティ]-[Event ID 4688] を検索し、不審な msinfo32、systeminfo等の実行を監査します。なお、上記コマンドをPowerShellで実行しても、セキュリティログに記録されます。
* PowerShellスクリプトの監査
  + [イベントビューアー]-[アプリケーションとサービスログ]-[Microsoft]-[Windows]-[PowerShell/Operational] で不審なスクリプトの実行を監査します。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

攻撃者はメールやWebサイトを通じて、悪意あるスクリプトをダウンロードすることから、重要資産が保存されている端末、サーバーのネットワーク分離と電子メール、Web接続の禁止を検討します。

以下のアクセスコントロールを検討します。

* PowerShell  
  17章・PowerShellの悪用 の設定を検討します。
* Windows Script Hostの制御設定   
  19.10 Windows Script Hostの制御設定 の設定を検討します。  
  なお、本設定は、JScript、VBScript のホストエンジンである、Windows Script Host の動作設定を停止もしくは署名されたスクリプトのみ許可にするため、WSHを活用しているシステムの場合、運用に影響を及ぼします。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

アンチウイルスソフトのパターンファイルの日次更新、クイックスキャンの日次実施、完全スキャンの週次実施をします。

Endpoint Detection and Response もしくは、侵入検知システムの導入を検討してください。

### 受託開発ベンダー管理責任

#### セキュアコーディング

スクリプトへの署名を実施します。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

### コマンドラインインターフェースの監査

グループポリシーを利用し、コマンドラインインターフェースの実行履歴をイベントログに出力します。

#### 設定方法

以下のグループポリシーを設定します。

* 監査ポリシー カテゴリの設定を上書きする  
  [コンピューターの構成]>[ポリシー]>[Windows の設定]>[セキュリティ設定]>[ローカルポリシー]>[セキュリティオプション]>[監査: 監査ポリシー サブカテゴリの設定 (Windows Vista 以降) を強制して、監査ポリシー カテゴリの設定を上書きする] の [このポリシーの設定を定義する] をチェックし、[有効] をクリックします。
* 監査プロセス作成の監査  
  [コンピューターの構成]>[ポリシー]>[Windows の設定]>[セキュリティ設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[詳細追跡]>[プロセス作成の監査]の [成功]、[失敗] を構成します。
* プロセス作成の監査にコマンドラインを含める  
  [コンピューターの構成] >> [管理用テンプレート] >> [システム] >> [プロセス作成の監査] >> [プロセス作成イベントにコマンドラインを含める]のポリシー値を [有効] に設定します。

#### 監査方法

イベントビューワーもしくは Message Analyzer で Event ID 4688 を検索します。

#### 参考

コマンド ライン プロセスの監査:   
https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing

### Windows Script Hostの制御設定

レジストリを修正しWindows Script Hostの実行制御を設定します。設定にあたっては、VBScriptの停止をした場合の影響を調査します。

#### レジストリ設定

以下のレジストリを設定します。

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings

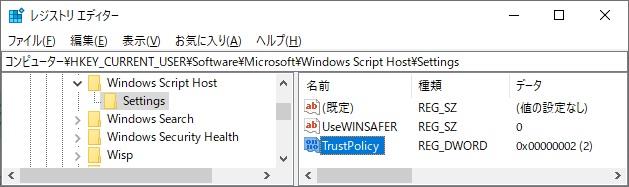
HKEY\_CURRENT\_USER\Software\Microsoft\Windows Script Host\Settings

| **レジストリキー** | **種類** | **値** | **動作** |
| --- | --- | --- | --- |
| Enabled | REG\_SZ | 0 | Windows Script Hostは無効 |
| 1 | Windows Script Hostは有効 |
| Remote | REG\_SZ | 0 | リモートスクリプトは無効 |
| 1 | リモートスクリプトは有効 |
| UseWINSAFER | REG\_SZ | 0 | TrustPolicyは有効 |
| 1 | TrustPolicyは無効 |
| TrustPolicy | REG\_DWORD | 0 | TrustPolicyが有効、スクリプト署名がなくても許可 |
| 1 | TrustPolicyは有効、スクリプト署名がないと警告 |
| 2 | TrustPolicyは有効、スクリプト署名がないと警告して終了 |

#### 設定例

CurrentUser に TrustPolicyを有効にし、スクリプト署名を必須とした場合

* 名前： REG\_DWORD
* 値： 2（16進）

Enable、TrustPolicyがない場合は作成してください。

上記設定でVBScriptをダブルクリックすると、以下のようなメッセージが表示されます。

### Visual Basic for Application（VBA、マクロ） の課題

Office のマクロは文書を開いた際に自動実行させることができます。また、マクロはコマンドラインインターフェースや PowerShell を呼び出せるため、これらを組み合わせて、Office文書を開いた瞬間に、外部から悪意のあるプログラムを呼び込む「ダウンローダー」と呼ばれる機能が実装できます。この手口は攻撃者に好んで使われており、2019年12月から急拡大している Emotet でも、Word のマクロを悪用して大きな被害をもたらしています。  
この Emotet の出現以降、悪意あるプログラムをメールに添付して送信する際に、組織内の送信者になりすまして、被害者を安心させマクロ付きOffice文書を開かせるという手口は、今後、さらに巧妙化し主流となってくると予想できます。

#### ・L1 Word 2016 のグループポリシーでの対策

・L1 Word 2016 などでは、[ユーザーの構成]>[ポリシー]>[管理用テンプレート]>[Microsoft Word 2016]>[Word のオプション]>[セキュリティ]>[セキュリティセンター]>[VBA マクロ通知設定] が [有効:通知してすべてを無効にする] としており、マクロの実行はできない設定となっています。この設定は Excel などの他のOfficeアプリケーションでも同様です。

#### 業務で必要なマクロを実行したい場合

一方で、業務を効率よくするためにマクロが欠かせない業務も存在します。このため、このポリシーが全社に展開されると、業務に支障をきたすことになります。しかし、マルウェアの被害を軽減することも重要です。そこで、通常は、マクロ禁止の設定をしておき、マクロを含むファイルを開くときだけマクロを有効にする設定を行うことで、万一、メールに添付された悪意あるマクロ付き Office 文書を開いても、マクロの実行を停止することができます。

##### 設定手順

1. マクロを実行する端末を特定し、コンピュータグループを作成、登録します。
2. [AllowMacro] などの わかりやすい OU を作成し、コンピュータのセキュリティグループ を登録します。
3. セキュリティグループが登録された OU の グループポリシー で [VBA マクロ通知設定] で [すべてのマクロを有効にする（推奨しません）] を設定します。
4. 端末ごとに以下のバッチファイルを作成します。このバッチは、レジストリでマクロを有効にしてマクロが登録されたExcelファイルを開き、Excelの終了後、再びレジストリでマクロを禁止する設定を行います。これによって、メールやインターネットからダウンロードされたマクロ付きExcelファイルを開いても、マクロが実行されず、被害が緩和されます。

@echo off

REM すべての Excel マクロを有効にする

reg add "HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Security" /v "VBAWarnings" /t REG\_DWORD /d "1" /f

REM マクロを実行したい Excel 文書のファイルパス

"C:\Users\User\_Name\Documents\abc.xlsm"

REM 警告を表示してすべての Excel マクロを無効にする

reg add "HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Security" /v "VBAWarnings" /t REG\_DWORD /d "2" /f

exit

##### 関連レジストリ

| **Office アプリ** | **レジストリキー** | **値の名前** | **型** | **値** |
| --- | --- | --- | --- | --- |
| Access 2016/2019 | HKCU\SOFTWARE\Microsoft \Office\16.0\Access\Security | VBAWarnings | REG\_DWORD | 1 → すべてのマクロを有効にする 2 → 警告を表示してすべてのマクロを無効にする【既定】 3 → デジタル署名されたマクロを除き、すべてのマクロを無効にする 4 → 警告を表示せずにすべてのマクロを無効にする |
| Excel 2016/2019 | HKCU\SOFTWARE\Microsoft \Office\16.0\Excel\Security |
| PowerPoint 2016/2019 | HKCU\SOFTWARE\Microsoft \Office\16.0\Excel\Security |
| Word 2016/2019 | HKCU\SOFTWARE\Microsoft \Office\16.0\Excel\Security |

他のバージョンは [\16.0] を適宜、置き換えてください。なお、Office 2019 のメジャーバージョンは 2016と同じで、同じ \16.0を使用します。

#### トレーニング

従業員には、マクロが有効になっている端末がマルウェアの侵入口であることに、十分な理解を得てください。外部から、関係者を装った悪意のある添付ファイルをみだりに開かず、必ず保護ビュー（サンドボックスなどともいいます）で開き、マクロを実行しないように注意を呼び掛けてください。

## ・悪意あるWindowsサービスの実行 ・不正なWindowsサービスの追加

### 戦術：悪意あるプログラムの実行 （悪意あるWindowsサービスの実行）

MITRE ATT&CK T1569.002 System Services: Service Execution

### 戦術：永続性、特権昇格 （不正なWindowsサービスの追加）

MITRE ATT&CK T1543.003 Create or Modify System Process: Windows Service

### 概説

MITRE ATT&CKでは、悪意あるプログラムの実行と永続性、特権昇格を異なる戦術として定義し解説していますが、防御対策等は同じといえるため、本稿では二つの戦術を同一として扱います。

Windowsサービスとは、ユーザーインターフェイスを持たずにバックグラウンドで常駐して動作するプログラムで、最も高い権限で機能を実行できます。Windowsが起動した際に自動起動するように設定できるため、初期侵入後、悪意あるプログラム（マルウェア）をWindows サービスとしてインストールに成功すれば、最上位の権限での実行が可能となります。

新しいWindowsサービスをインストールするか、既存のサービスを改ざんすることでこの手法は実現されますが、Windowsサービスの操作には管理者権限が必要です。

### 緩和の方針

一般業務端末を操作するユーザーアカウントを標準ユーザーとして設定し、ローカル管理者であるビルトインAdministratorsグループのメンバーから除外し、Windowsサービスのインストールを失敗させることで緩和します。ドメインコントローラー、メンバーサーバーは検出に努めます。

CWE-428（引用符で囲まれていないプログラムパス）の脆弱性を排除します。

### 運用やNetworkが変更された場合の影響の有無

標準ユーザーアカウントを、ビルトインAdministratorsグループのメンバーにした場合、リスクが非常に高まります。

### 優先すべき措置

以下の設定を検討します。

* 一般業務は標準ユーザーアカウントで実行し、ビルトインAdministratorsグループのメンバーから除外します。
* 管理者業務を行う端末、サーバーでは [Windows ログ]-[システムログ]-[Event ID 7045] を監査し、不審なWindowsサービスのインストールを検知します。
* CWE-428（引用符で囲まれていないプログラムパス）の脆弱性を排除します。

### ユーザー運用管理責任

#### リスクの受容

アプリケーションのインストール権限をユーザーに委ねた場合、この手法のリスクが高くなります。対象端末の文書化と監査による検知を強化し緩和します。

|  |  |  |
| --- | --- | --- |
| **業務** | **特権** | **リスク受容のための条件例** |
| プログラム開発担当者 | Local Administrator | スクリプトへの署名と実行ポリシーの設定。  ドメインコントローラー、メンバーサーバー、担当者端末のWindowsサービスインストールのログ監査。  侵入検知システムの導入。 |
| Help Desk 担当者 | Domain/Local Administrator |
| システム管理者 | Enterprise/Domain/Local Administrator |
| 部門管理者（OUの委任） | OUのパスワードリセット、セキュリティグループ管理、ドメイン参加等 |
| VBAを利用する業務担当者 | 標準ユーザー | スクリプトへの署名と実行ポリシーの設定。担当者端末のスクリプト実行ログの監査。Local Administrators に含めない。 |
| 役職者、研究者、秘書 | 標準ユーザー | Local Administrators に含めない。 |
| 上記以外の一般業務担当者 | 標準ユーザー | Local Administrators に含めない。 |

#### 啓発・教育

* すべての端末利用者
* 組織のアプリケーションのインストール規程（評価済みアプリケーション以外をインストールしない等）の理解と遵守を求めます。
  + ローカル Administrators メンバー
* アプリケーションをインストールできる権限を持つユーザーに対して、"初期侵入" から "悪意あるプログラムの実行" までの攻撃ベクターで攻撃を阻止しないと、情報窃取、送信、漏洩等のリスクが高まることを理解させます。
* アプリケーションのインストールや保守以外での管理者権限でのインターネット接続、メール受信などのリスクを正しく認識させます。

#### 管理規程

運用規程に以下を追加することを検討します。

* ローカル管理者権限を業務ユーザーに付与した場合の文書化
* 監査による不正なWindowsサービスのインストールの検出。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

該当しません。

#### モニタリング

以下の監査の実施を検討します。

1. 管理対象の端末、サーバー、ドメインコントローラーで以下のイベントログを監査します。

* [イベントビューアー]-[Windows ログ]-[システム]   
  ソース： Service Control Manager  
  イベントID： 7045 サービスがシステムにインストールされました。

1. 不審なサービスのインストールが疑われた際は、次のドキュメントを参照し、必要に応じて専門家の支援を得ます。  
   JPCERT/CC インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書[[41]](#footnote-41)
2. Windowsサービスのインストールをイベントログで検出した際は、以下のコマンドを実行し、CWE-428の脆弱性を検知します。

* 引用符で囲まれていないWindowsサービスの検知（管理者権限のコマンドプロンプトで実行する）

wmic service get name,pathname,displayname,startmode | findstr /i auto | findstr /i /v "C:\Windows\\" | findstr /i /v """

なお、C:\Windows 以下のWindowsサービスはデフォルトで引用符で囲まれていないため除外しています。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

以下の設定を検討します。

* 標準ユーザー  
  ビルトインAdministratorsグループのメンバーに標準ユーザーアカウントを含めないようにします。
* Windowsサービスのインストールの制限  
  Windowsサービスはログインしているユーザーのセキュリティコンテキストとは異なるセキュリティコンテキストで実行される特徴を有します。そこで、ドメインの管理者でないユーザーにアプリケーションをインストールできる権限を与えた場合を考えてみます。

このような場合、アプリケーションがLocal Systemで動作するサービスをインストールできてしまうと、本来、特権を有しないユーザーが特権を有するアプリケーションを使って、レジストリを変更するなどして永続性の確保や、権限昇格が可能となります。

Windowsサービスのセキュリティコンテキストは以下の表の通りです。システムの特性に合わせて、アプリケーションのインストール権限を付与できるユーザーを限定し、限定されたユーザーの端末のサービスを監査する事を検討します。

| **セキュリティコンテキスト** | **与えられる権限** |
| --- | --- |
| User | システムは、サービスのインストール時に有効なユーザー名とパスワードの指定を要求し、ネットワーク上の 1 人のユーザーによって指定されたアカウントのコンテキストで実行します。 |
| LocalService | ローカル コンピューター上で非特権ユーザーとして機能し、リモート サーバーに匿名の資格情報を提示するアカウントのコンテキストで実行します。 |
| LocalSystem | 広範なローカル特権を提供し、リモート サーバーにコンピューターの資格情報を提示するアカウントのコンテキストで実行します。 |
| NetworkService | ローカル コンピューター上で非特権ユーザーとして機能し、リモート サーバーにコンピューターの資格情報を提示するアカウントのコンテキストで実行します。 |

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

侵入検知システム、Endpoint Detection and Responseの導入を検討します**。**

### 受託開発ベンダー管理責任

#### セキュアコーディング

最小限のセキュリティコンテキストでWindowsサービスを設計し、文書化して、ユーザーと共有します。

Windowsサービスを作成する場合は、CWE-428（引用符で囲まれていないプログラムパス）の脆弱性の排除を行います。サービスはイベントログに、起動、エラー、終了等のログを出力するようにします。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・メールに添付されたマルウェアファイルやリンクをユーザーが実行する

### 戦術：悪意あるプログラムの実行

MITRE ATT&CK T1204.001 User Execution: Malicious Link[[42]](#footnote-42)  
 T1204.002 User Execution: Malicious File[[43]](#footnote-43)

### 概説

悪意あるプログラム（マルウェア）の侵入経路の大半は電子メールです。メールの添付ファイルを開くか、メール本文に埋め込まれたリンクをクリックすることで、マルウェアがPC本体のメモリにダウンロードされ活動を開始します。 この攻撃はユーザーがファイルやリンクをクリックするところから始まるため、定期的な教育は非常に有効です。最新の手口をフィッシング対策協議会[[44]](#footnote-44)などから入手し、最新の手口などを共有してください。

### 緩和の方針

最新のフィッシングメールのユーザートレーニング、その他は、・悪意のあるファイルを添付したフィッシングメール を参考にして下さい。

### 運用やNetworkが変更された場合の影響の有無

重要な情報資産があるサーバーや端末でメールに添付されたOffice文書やPDF文書の閲覧を行うと、この攻撃のリスクが高まります。

### 優先すべき措置

最新の手口をフィッシング対策協議会から入手し、組織全体で共有してください。

### ユーザー運用管理責任

13章・悪意のあるファイルを添付したフィッシングメールを参照してください。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

13章・悪意のあるファイルを添付したフィッシングメールを参照してください。

### 受託開発ベンダー管理責任

13章・悪意のあるファイルを添付したフィッシングメールを参照してください。

## ・レジストリRunキーやスタートアップフォルダの悪用

### 戦術：永続化

MITRE ATT&CK T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder[[45]](#footnote-45)

### 概説

Windowsには、OSが起動した際に自動的にプログラムを起動させる機能の例として、レジストリやスタートアップフォルダなどを使用するものがあります。これは、①端末やサーバーが起動した際と、②特定のユーザーがログオンした際に、それぞれ分けて設定が可能です。攻撃者はこの機能を悪用し、端末やサーバーが再起動した際やユーザーがログオンした際に、悪意のあるプログラムを起動させ活動を永続化します。

この攻撃手法は、侵入後にWindowsの基本機能を悪用するため簡単に軽減できません。

### 緩和の方針

この手法は、管理者権限を使われて初期侵入された、もしくはOS、プログラムの脆弱性を利用して悪意あるプログラムが実行された後の結果であるということができます。従って、重要資産に対してはツールを使い自動起動するアプリケーション定期的に監査し、検出に努めます。 Microsoft の純正ツールである Sysinternals の Autoruns[[46]](#footnote-46) の使用が監査に有効です。

### 運用やNetworkが変更された場合の影響の有無

脆弱性対策ができていない、不用意に管理者権限を使用すると、この手法のリスクが高まります。

### 優先すべき措置

重要な情報資産にアクセスする端末やサーバーに対して、Autoruns を使い自動起動アプリケーションとレジストリ、ファイルを監査し、検出に努めます。

レジストリを操作することから、レジストリのアクセス権限を監査します。

Endpoint Detection and Response もしくは、侵入検知システムの導入を検討してください。

### ユーザー運用管理責任

#### リスクの受容

この攻撃手法は、システム機能の悪用に基づいているため、簡単に軽減できません。初期侵入や悪意あるプログラムの実行などでの阻止を検討し、重要資産の暗号化、管理者権限の厳格な運用を実施し、リスクを受容します。

#### 啓発・教育

* すべての端末利用者
  + 組織のアプリケーションのインストール規程（評価済みアプリケーション以外をインストールしない等）の理解と遵守を求めます。
  + 最新のフィッシングメールの事例、手口の理解を深めます。
* ローカル Administrtors メンバー
  + "初期侵入" から "悪意あるプログラムの実行" までの攻撃ベクターで攻撃を阻止しないと、情報窃取、送信、漏洩等のリスクが高まることを理解させます。
  + アプリケーションのインストールや保守以外での管理者権限でのインターネット接続、メール受信などのリスクを正しく認識させます。

#### 管理規程

以下の規程の整備を検討します。

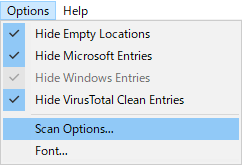
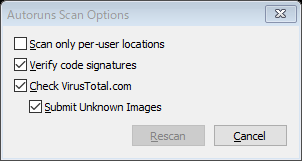
* 重要な情報資産にアクセスする端末、サーバーに対する監査規程。
* レジストリのアクセス権の監査。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

該当しません。

#### モニタリング

1. Autoruns64.exeを入手し、対象となるコンピュータのデスクトップにコピーします。
2. アイコンを右クリックし、[管理者として実行] をクリックし起動します。
3. 起動したら、[Options] で [Hide Empty Locations]、[Hide Microsoft Entries]、[Hide VirusTotal Clean Entries] をチェックし、続いて [Scan Options] をクリックします。
4. 以下のチェックボックスにチェックを入れます。  
   [Verify code signatures]  
   [Check VirusTotal.com]  
   [Submit Unknown Images]

この設定により、Googleが運営するマルウェアの総合サイトVirusTotal[[47]](#footnote-47) でClean と判断されたファイル以外のエントリが表示されます。VirusTotal の列で「指定されたファイルが見つかりません」、「指定されたパスが見つかりません」以外の行に着目します。

黄色の行はレジストリもしくはタスクスケジューラに起動のエントリが残っているが、ファイルがない場合を指します。多くは、アンインストールが不完全か削除を失敗している場合ですが、マルウェアの痕跡の可能性もあります。

VirusTotalの列に赤字で表示されている場合は、マルウェアの可能性があります。1/57 となっている場合は、セキュリティベンダーの57社中1社が当該行のファイルをマルウェアと判定していることを意味します。分子が数件以上あった場や、分子の数が増加傾向にある場合は、専門家の助言を受けます。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

レジストリのアクセス権を Administrators に設定します。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

アンチウイルスソフトのパターンファイルの日次更新と、日次クイックスキャン、週1回以上の完全スキャンを実施します。

侵入検知システム、Endpoint Detection and Responseの導入を検討します**。**

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・ファイル削除

### 戦術：防御の回避

MITRE ATT&CK T1070.004 Indicator Removal on Host: File Deletion[[48]](#footnote-48)

### 概説

攻撃者はダウンロードしたファイルや、自身が作成したファイルを削除し、痕跡を残さないようにするため、ファイル削除ツールやWindowsのコマンド機能を使用します。

### 緩和の方針

この手法は、OSの標準機能の悪用に基づくものが多く、予防制御では簡単に軽減できません。不審なコマンド実行を監査し、検出に努めます。

### 運用やNetworkが変更された場合の影響の有無

初期侵入、悪意のあるプログラム実行後のため、該当しません。

### 優先すべき措置

コマンドラインインターフェースのログ監査。不正なコマンド、引数の検知を優先します。

Endpoint Detection and Response もしくは、侵入検知システムの導入を検討してください。

### ユーザー運用管理責任

#### リスクの受容

初期侵入、悪意のあるプログラム実行後であり、標準機能を使うことが多く、この手法のリスクは受容せざるを得ません。

#### 啓発・教育

該当しません。

#### 管理規程

以下の規程の整備を検討します。

* コマンドラインインターフェース、スクリプトのログ監査規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

以下のポリシーの適用を検討します。

* [17章・コマンドラインインターフェースの悪用]、[18章・PowerShellの悪用]を参考にしてコマンド、スクリプト実行のログを取得します。

#### モニタリング

以下の監査を検討して下さい。

* コマンドラインインターフェースの監査
  + 前項のポリシーを設定の上、[イベントビューアー]-[Windowsログ]-[セキュリティ]-[Event ID 4688] を検索し、不審なdelet、replacee等の実行を監査します。なお、上記コマンドをPowerShellで実行しても、セキュリティログに記録されます。
* PowerShellスクリプトの監査
  + [イベントビューアー]-[アプリケーションとサービスログ]-[Microsoft]-[Windows]-[PowerShell/Operational] で不審なスクリプトの実行を監査します。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

該当しません。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

侵入検知システム、Endpoint Detection and Responseの導入を検討します。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・難読化されたファイルまたは情報

### 戦術：防衛回避

MITRE ATT&CK T1027 Obfuscated Files or Information[[49]](#footnote-49)

### 概説

攻撃者は悪意あるプログラムを隠ぺいするため、難読化や暗号化を行うことがあります。難読化はスクリプトなどの命令文を無意味な変数に置き換えたり、16進数に変換するなどして、どのような機能かの分析を困難にさせ、かつ、アンチウイルスソフトの解析を免れることを目的としています。ただし、正規の正常な製品でも、リバースエンジニアリングを避けるために、難読化を実施することがあるため、難読化＝悪意とは限りません。

Windows では外部からマルウェアをダウンロードする際に、難読化させたPowerShell スクリプトを使用[[50]](#footnote-50)することが知られています。

### 緩和の方針

Windows 10で実装されたマルウェア対策スキャンインターフェイス（AMSI）に対応したアンチウイルスソフトの採用もしくは同等機能を有するアンチウイルスソフトの採用を検討します。

侵入検知システム、Endpoint Detection and Responseの導入を検討します。

### 運用やNetworkが変更された場合の影響の有無

該当しません。

### 優先すべき措置

AMSI に対応したアンチウイルスソフトの導入を検討します。AMSI対応のアンチウイルスソフトは以下の難読化されたスクリプトの攻撃コードを検出します。

* PowerShell（スクリプト、インタラクティブな使用、および動的なコード評価）
* Windows Script Host（wscript.exeおよびcscript.exe）
* JavaScriptとVBScript
* OfficeVBAマクロ

但し、AMSI 機能を改ざんすることで AMSI 機能をバイパスする実証実験が報告[[51]](#footnote-51)されています。

侵入検知システム、Endpoint Detection and Responseの導入を検討します。

### ユーザー運用管理責任

#### リスクの受容

難読化はPowerShellスクリプトに限ったものではありませんが、多くはPowerShell に施されるため、「18章・PowerShellの悪用」のリスク受容を援用します。

|  |  |  |
| --- | --- | --- |
| **業務** | **特権** | **リスク受容のための条件例** |
| プログラム開発担当者 | Local Administrator | PowerShell スクリプト開発環境の分離。なお、スクリプトはリリース後に署名する。  ポリシーでAllSigned適用、侵入監視・Endpoint Detection and Response・AMSI対応アンチウイルスソフトの導入、PowerShell スクリプトログ監査、定期的なトレーニング。 |
| Help Desk 担当者 | Domain/Local Administrator |
| システム管理者 | Enterprise/Domain/Local Administrator |
| 部門管理者（OUの委任） | OUのパスワードリセット、グループ管理、ドメイン参加等 |
| 役職者、研究者、秘書 | 標準ユーザー | Restricted適用、Local Administrators に含めない。 |
| 上記以外の一般業務担当者 | 標準ユーザー | Restricted適用、Local Administrators に含めない。 |

### 啓発・教育

* 対象：すべての端末利用者
  + アンチウイルスソフトの更新方法、更新の確認方法を理解させます。
  + 万一、動作していない、更新されていない、記憶にない設定変更がなされていた場合は、インシデントのおそれがあることから、報告させるようにします。

### 管理規程

以下の規程の整備を検討します。

* アンチウイルスソフトの運用規程の文書化、監査。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

「18章・PowerShellの悪用」を参照してください。

#### モニタリング

「18章・PowerShellの悪用」を参照してください。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

該当しません。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

AMSI対応アンチウイルスソフト、侵入検知システム、Endpoint Detection and Responseの導入を検討します。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・認証情報のダンプ

### 戦術：認証情報アクセス

* MITRE ATT&CK T1003 OS Credential Dumping[[52]](#footnote-52)
* T1003.001 OS Credential Dumping: LSASS Memory
* T1003.002 OS Credential Dumping: Security Account Manager
* T1003.003 OS Credential Dumping: NTDS
* T1003.004 OS Credential Dumping: LSA Secrets
* T1003.005 OS Credential Dumping: Cached Domain Credentials

T1003.006 OS Credential Dumping: DCSync

### 概説

認証情報のダンプは、OSに保存されているアカウントのIDとパスワードを取得するプロセスです。その後、窃取した資格情報を利用して、情報の収集や水平展開を図ります。このため、認証情報のダンプを阻止することは、被害の拡大を防ぐ重要なポイントとなります。

認証情報はOSによってHashされ安全な状態で保管され、AdministratorやSYSTEM権限でアクセスされますので、一般的な標準ユーザー権限でログオンしている状態では脆弱性がない限り、悪意あるプログラム（マルウェア）は、認証情報にアクセスできません。しかし、Administrator権限でログオン中に悪意あるプログラムの実行を招くと、認証情報のアクセスを許してしまうこととなります。

また、既定ではダイジェスト認証は無効となっているため、平文の資格情報がキャッシュされることはありませんが、侵入を許した場合、攻撃者はレジストリを書き換え平文の資格情報を窃取する場合があります。これはグループポリシーの再読み込みで排除できますが、重要資産に対しては監査が必要となります。

MITRE ATT&CKでは、主にWindowsからの認証情報の窃取にフォーカスしていますが、これ以外にも、DBへの接続情報やアプリケーションの認証情報などが探索される可能性もあることから、本項では、セキュアコーディングで注意事項を加えてあります。

### 緩和の方針

認証情報の窃取は管理者権限が必要なため、利用者の権限を標準ユーザーにすることは大変効果的で、この攻撃の緩和に役立ちます。管理者に対しては、厳重な保護が必要です。システム管理者、もしくは管理者特権が必要な業務には多角的な防御を検討します。重要資産に対しては、監査を実施します。

### 運用やNetworkが変更された場合の影響の有無

意図しない管理者権限でのアプリケーションのインストールや、電子メール、Webサイトの閲覧は悪意あるプログラムに高位の権限を与えるため、十分な管理が必要です。

### 優先すべき措置

多角的な防御が必要です。以下のすべての措置を優先的に検討して下さい。

* 一般業務を行う場合
  + 標準ユーザーでの運用とする。
* システム管理者、もしくは管理者特権が必要な業務
  + 多要素認証の導入を検討する。
  + 重要な情報資産を有する端末、サーバー、それらの管理用端末へはハードウェアトークンの導入を検討する。
  + Windows Defender Credential Guard の導入を検討する。
  + Protected Users のグループメンバーに追加し、資格情報のキャッシュを禁止[[53]](#footnote-53)する。但し、NTLM認証が無効となるため、適用においては十分なテストを行う。
    - オフラインサインインはサポートされなくなる。
    - IPアドレスを指定してログオンすることはできなくなる。
* ローカル Administrators
  + ドメインユーザーはローカル Administratorsのメンバーから除外する。
  + ローカル Administrators のメンバーを監査する。
  + LAPSの導入を検討する。
* 管理者端末、重要資産を有する端末、メンバーサーバー、ドメインコントローラー
  + WDigest認証の無効化と監査を行う。
* その他の事項  
  互換性維持のための弱いハッシュ、暗号方式、平文パスワードの使用を禁止する。  
  LSASSプロセスを保護する。 「26.7.3ネットワークデザイン、アクセスコントロール 、フィルタリング」を参照。

### ユーザー運用管理責任

#### リスクの受容

このリスクの回避は困難です。慎重な検討を行ってください。

|  |  |  |
| --- | --- | --- |
| **業務** | **特権** | **リスク受容のための条件例** |
| すべて | Local Administrator | LAPSを導入し、すべての端末、サーバーのLocal Administratorのパスワードをユニークにする。  ドメインユーザーはLocal Administrators から除外する。 |
| プログラム開発担当者 | Local Administrator | Windows Defender Credential Guardの導入。多要素認証の導入。Protected Usersグループへの参加。WDigest認証の無効化と監査。 定期的なトレーニング。 |
| Help Desk 担当者 | Domain/Local Administrator |
| システム管理者 | Enterprise/Domain/Local Administrator |
| 部門管理者（OUの委任） | OUのパスワードリセット、グループ管理、ドメイン参加等 |
| 役職者、研究者、秘書 | 標準ユーザー | 標準ユーザーでの運用。Local Administrators に含めない。 |
| 上記以外の一般業務担当者 | 標準ユーザー |

Windows Defender Credential Guard はWindows 10 Enterprise Editionが必要ですが、Windows Defender Credential Guard は管理者特権のWindows で実行されるマルウェアに対して、仮想化ベースのセキュリティで資格情報を保護するため、リスク受容に対しては有効な手段といえます。

#### 啓発・教育

* 対象：システム管理者   
  認証情報のダンププロセスと攻撃プロセスを理解させるとともに、管理者の認証情報の適切な保護や、運用について検討させます。

#### 管理規程

以下の規程の整備を検討します。

* ローカル Administrator 権限を有するドメインユーザーの管理規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

以下のポリシーの適用を検討します。

1. ローカルAdministratorの無効化する。Windows 10、Windows Server 2016以降ではDefaultでローカルAdministratorは無効になっているが、Windows 8.1、Windows Server 2012R2以前は有効となっている。グループポリシーで以下の設定を行う。

[コンピュータの構成]>[Windowsの設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティオプション]>[アカウント: Administrator アカウントの状態] を [無効] に設定する。

なお、ビルトインローカルAdministratorを有効にし、AdministratorのIDを変更する方法があるが、ローカルのAdministratorの識別子（Security Identifier：SID）は変更されず、SIDが公知の情報なため、攻撃側からは容易にIDを特定できる。このため、他のIDに設定する方法は推奨しない。

1. LSASSプロセスを保護します。 資格情報を管理するLSASSプロセスへの攻撃を防御する。  
   [グループポリシー]-[コンピュータの構成]-[基本設定]-[Windowsの設定]-[レジストリ] で [\HKLM\SYSTEM\CurrentControlSet\Control\Lsa] に値を新規に設定[[54]](#footnote-54)する。
2. WDigest認証プロトコルを無効化する。

[コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[MS Security Guide] を [無効] に設定する。（13.8・L1 MS Security Guide を参照。）

1. MITRE ATT&CKの緩和策では、Protected Users や NTLM認証の無効が提案されているが、特に、NTLMの無効化は広範な影響が出るため、慎重なテストを実施する。

#### モニタリング

以下の監査を検討して下さい。

* 管理者端末、重要資産を有する端末、メンバーサーバー、ドメインコントローラー
  + 「17章・コマンドラインインターフェースの悪用」、「18章・PowerShellの悪用」を参照し、監査を実施する。
  + セキュリティイベントログ Evenmt ID 4624[[55]](#footnote-55) でWDigestのプロセスの使用を監査する。存在する場合は、侵害が疑われるため、専門家の助言を得る。
    - ログオンプロセス：WDigest
    - 認証パッケージ：WDigest
* ドメインコントローラー
  + セキュリティイベントログ:イベントEvent ID 4776[[56]](#footnote-56) でWDigestパッケージの使用を監査する。存在する場合は、侵害が疑われるため、専門家の助言を得る。
    - 認証パッケージ：WDigest
* Protected User
  + [イベントログ]-[アプリケーションとサービスログ]-[Microsoft]-[Windows]-[Authentication]-[PrtectedUsersFailures-DomainController] のログを有効化する。  
    ホスト名を使用せず明示的にIPアドレスを指定してアクセスした場合、WindowsはKerberos認証を試行せず、NTLM認証にフォールバックされる。このようなNTLM認証、AES以外の暗号を使用したKerberos認証が存在する場合、侵害が疑われるため、専門家の助言を得る。  
    100 NLTM usage attempted.  
    104 DES or RC4 attempted for Kerberos Authentication

#### ネットワークデザイン、アクセスコントロール 、フィルタリング

以下の設定を検討して下さい。

* クレデンシャルガードを導入し、資格情報を仮想化ベースのセキュリティ[[57]](#footnote-57)で保護する。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

侵入検知システム、Endpoint Detection and Responseの導入を検討します。

### 受託開発ベンダー管理責任

#### セキュアコーディング

以下を開発規約とすることを検討して下さい。

* 特権が必要なサービスに対する認証を行う場合は、システムの認証ダイアログ(またはOSが提供する仕組み)を使用する。
* アプリケーション自身に認証情報等をハードコーディングしてはならない。app.configなどに認証情報や接続文字列を記述する場合は、暗号化を行う。（必須）
* プレーンテキストで認証情報をメモリ、ディスクに格納する事を禁止する。（必須）
* 物理メモリから機密情報がスワップされディスクに書き出されないようにする。（推奨：権限によりロックできない場合がある。）
* JPCERT/CC Java コーディングスタンダード MSC03-J. センシティブな情報をハードコードしない [[58]](#footnote-58) を参照。
* JPCERT/CC CERT C コーディングスタンダード MSC18-C. プログラムコードの中でパスワードなどの機密情報を扱うときは注意する[[59]](#footnote-59) を参照。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・脆弱性を悪用した認証情報アクセス

### 戦術：認証情報アクセス

MITRE ATT&CK T1212 Exploitation for Credential Access[[60]](#footnote-60)

### 概説

脆弱性を悪用した認証情報アクセスは、OS、アプリケーション、プロトコルの脆弱性を利用して、認証情報を窃取するものです。攻撃者は何らかの資格情報を得て、ユーザーと認証機関のやり取りを窃取し、脆弱性を利用して特権昇格や永続的な資格を得ます。脆弱性が利用されるため、攻撃であっても正規のプロセスとみなされることがあり、発見が困難となる場合があります。資格を取得されると、それ以降、自由に資格情報を使って攻撃ができるため危険です。

### 緩和の方針

攻撃者は脆弱性を狙うためセキュリティ更新プログラムの適用や、脆弱なプロトコルの利用停止が最優先となります。

一方で、セキュリティ更新プログラムの適用によって、ごくまれに特定の環境でシステムの動作に影響を及ぼす場合があります。可用性の観点から、システムの重要度に応じてセキュリティ更新プログラムのリリースに合わせて、動作テストを実施し、適用の可否の判定、適用できない場合は回避策の適用を行う運用体制を作る、もしくは、セキュリティ更新プログラム適用前のバックアップを保存しておき、セキュリティ更新プログラムをアンインストールする、もしくはバックアップから復元し、回避策を適用する運用体制を作ることが重要となります。

### 運用やNetworkが変更された場合の影響の有無

セキュリティ更新プログラムが適切に適用されていない場合に、リスクが高まります。

### 優先すべき措置

セキュリティ更新プログラムの適用をテストし速やかに適用します。特に、プロトコルに起因する脆弱性はネットワークからの攻撃に利用されるため、優先します。

### ユーザー運用管理責任

#### リスクの受容

システムの特性上、速やかなパッチ適用が困難な場合は、以下を検討します。

* ログ監査を強化する。
* 当該システムを Internet から切り離す、当該システムでの電子メールやWebの閲覧を禁止し、関連するポートを閉じる。
* 脆弱なプロトコルの使用を停止する。

|  |  |  |
| --- | --- | --- |
| **業務** | **特権** | **リスク受容のための条件例** |
| すべて | － | 脆弱なプロトコルの使用停止。 |
| プログラム開発担当者 | Local Administrator | ドメインコントローラー、メンバーサーバー、担当者端末のコマンドライン、スクリプト実行、Windowsサービスインストールのログ監査。スクリプトへの署名と実行ポリシーの設定。侵入検知システムの導入。Internet接続の停止。 |
| Help Desk 担当者 | Domain/Local Administrator |
| システム管理者 | Enterprise/Domain/Local Administrator |
| 部門管理者（OUの委任） | OUのパスワードリセット、セキュリティグループ管理、ドメイン参加等 |
| VBAを利用する業務担当者 | 標準ユーザー | コマンドライン、スクリプト実行、Windowsサービスインストールのログ監査。スクリプトへの署名と実行ポリシーの設定。Local Administrators に含めない。 |
| 役職者、研究者、秘書 | 標準ユーザー | Local Administrators に含めない。 |
| 上記以外の一般業務担当者 | 標準ユーザー | Local Administrators に含めない。 |

#### 啓発・教育

* 対象：すべての端末利用者
  + 脆弱性修正プログラムの重要性と適用方法をトレーニングする。

#### 管理規程

以下の規程および文書の整備を検討します。

* セキュリティ更新プログラム適用の手順書の作成。
* 速やかにセキュリティ更新プログラムができないシステムの文書化、必要な監査の実施規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

脆弱性を利用するマルウェアの場合、コマンドラインインターフェース、PowerShell、悪意あるWindowsサービスの悪用が考えられます。「17章・コマンドラインインターフェースの悪用]、「18章・PowerShellの悪用」、「20章・悪意あるスクリプティングの実行」、「21章・悪意あるWindowsサービスの実行」を参照してください。[Windows 10 のセキュリティ機能を使用して脅威を軽減する][[61]](#footnote-61)を参照してください。

#### モニタリング

前項を参照してください。

#### ネットワークデザイン、アクセスコントロール 、フィルタリング

速やかにセキュリティ更新プログラムが適用できないシステムは、インターネットの分離を検討します。

脆弱なプロトコルの運用停止を検討して下さい。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

侵入検知システム、Endpoint Detection and Responseの導入を検討します。

### 受託開発ベンダー管理責任

#### セキュアコーディング

コンパイラ/リンカにおける保護機能の利用を強制して下さい。

* Visual Studio GS Protection (/GS)

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・アカウントの探索

### 戦術：情報の探索

MITRE ATT&CK T1087 Account Discovery

### 概説

攻撃者はローカル、ドメイン、クラウド、電子メールのアカウントを取得する場合があります。いずれも、OSのコマンドもしくはシェルを利用しアカウントの情報を取得できます。なお、この手法はクラウドシステムのアカウントの探索も含まれることから、クラウド管理システムも対象となります。

### 緩和の方針

ローカル管理者アカウントが列挙されないようにポリシー設定をします。

クラウドの制御に使用するコマンドラインインターフェースやスクリプトがインストールされた端末を特定し、監査を強化します。

* Azure PowerShell コマンド、Azure CLI コマンド、AWS CLIコマンドなど

### 運用やNetworkが変更された場合の影響の有無

ローカル管理者アカウント列挙のポリシーが有効にされると、攻撃者は容易にローカル管理者のIDを入手でき、クレデンシャルアクセスなどのリスクが増大します。

### 優先すべき措置

Windowsのローカル管理者アカウントが列挙されないようにポリシーを設定します。

スクリプト、コマンドラインインターフェースの実行ログの取得を取得し検出に努めます。

### ユーザー運用管理責任

#### リスクの受容

グループポリシーで容易に設定でき、設定しない場合は攻撃者に情報を提供するため、このリスクは受容すべきではありません。

#### 啓発・教育

該当しません。

#### 管理規程

該当しません。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

以下のポリシー設定を検討します。

[コンピューターの構成]> [ポリシー]> [管理用テンプレート]> [Windowsコンポーネント]> [資格情報ユーザーインターフェイス]> [昇格時に管理者アカウントを列挙する] を [無効] にします。

* 潜在的な影響：ユーザーアカウント制御（UAC）で、管理者への昇格時に管理者アカウントが表示されないだけで、影響はありません。[[62]](#footnote-62)

[コンピューターの構成]>[ポリシー]>[Windowsの設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティオプション]>[ネットワーク アクセス:Everyone アクセス許可を匿名ユーザーに適用する] を [無効] にします。

* 潜在的な影響:Windowsの規程値で影響はありません。[[63]](#footnote-63)

[コンピューターの構成]>[ポリシー]>[Windowsの設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティオプション]>[ネットワーク アクセス:SAMアカウントの匿名列挙を許可しない ] を [有効] にします。

* 潜在的な影響: 信頼する側のドメインの管理者が、他のドメインのアカウントの一覧を列挙できないため、1方向の信頼を越えて別のドメインのユーザーにアクセスを許可することはできません。 ファイルやプリントサーバーに匿名でアクセスしたユーザーは、それらのサーバー上の共有ネットワークリソースを一覧表示することはできません。共有フォルダーとプリンターの一覧を表示するには、ユーザーが認証されている必要があります。[[64]](#footnote-64)

[コンピューターの構成]>[ポリシー]>[Windowsの設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティオプション]>[ネットワーク アクセス: SAM アカウントおよび共有の匿名の列挙を許可しない] を [有効] にします。

* 潜在的な影響: 信頼する側のドメインの管理者が、他のドメインのアカウントの一覧を列挙できないため、1方向の信頼を越えて別のドメインのユーザーにアクセスを許可することはできません。 ファイルやプリントサーバーに匿名でアクセスしたユーザーは、それらのサーバー上の共有ネットワークリソースを一覧表示することはできません。共有フォルダーとプリンターの一覧を表示するには、ユーザーが認証されている必要があります。[[65]](#footnote-65)

[コンピューターの構成]>[ポリシー]>[Windowsの設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティオプション]>[ネットワーク アクセス: SAM へのリモート呼び出しを許可するクライアントを制限する] を [定義する] にチェックし、[セキュリティの編集] で [Domain\Administrators] を指定し、[リモートアクセス] を [許可] します。[セキュリティ記述子]を[O:BAG:BAD:(A;;RC;;;BA)] が設定されることを確認します。

* 潜在的な影響: Windows 10、Windows 8.1、Windows Server 2012R2/2016の2017年3月の月例品質ロールアッププログラムを適用されたコンピュータとWindows Server 2019では、既定でローカル Administrators のメンバーにリモート呼び出しが許可されています。このロールアッププログラムを適用していない、もしくはローカル Administratorsが、ユーザー、グループ、グループメンバーシップを列挙する管理ツールやソフトウェアが影響を受けます。[[66]](#footnote-66)

#### モニタリング

以下の監査の実施を検討します。

* ポリシー設定の変更の有無を定期的に監査する。
* クラウドコマンドラインインターフェースのログを監査する。

#### ネットワークデザイン、アクセスコントロール 、フィルタリング

該当しません。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

該当しません。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・ファイルとディレクトリの探索

### 戦術：情報の探索

MITRE ATT&CK T1083 File and Directory Discovery

### 概説

悪意のあるプログラム（マルウェア）や攻撃者はファイルやディレクトリ、ネットワーク共有を探索し、特定の情報を検索する場合があります。また、ターゲットとなる端末やサーバーに感染するか、他の行動を試みる場合があります。これは複合機の蓄積文書や文書共有なども含まれます。

### 緩和の方針

この手法は、システムの標準機能を悪用しているため、予防的設定が困難なため、多角的な緩和策を講じる必要があります。

### 運用やNetworkが変更された場合の影響の有無

脆弱なプロトコルの許可や、ポートの公開は、攻撃を受けるリスクを高めます。

重要な情報資産が不適切なセグメントに設置することで、攻撃者に検知されるリスクが高めます。

### 優先すべき措置

以下の設定を検討して下さい。

* ダイナミックアクセス制御[[67]](#footnote-67)の導入を検討します。
* 端末のドライブの共有を停止し、ファイルサーバー、NAS等に集約し、アクセス権を設定しログの取得と分析をします。
* 重要な情報資産を暗号化し、特定のユーザーだけがアクセスできるように権限を設定します。
* 不要なポートを閉じ、脆弱なプロトコルの使用を禁止します。
* ログの監査によって探索の検出を検討します。
* 複合機のファイル共有機能には、ID、パスワードを設定します。

### ユーザー運用管理責任

#### リスクの受容

ログ保存、分析コストが高い場合は、重要な情報資産の暗号化を行い受容します。なお、端末でのディレクトリ共有、ファイル共有は水平展開のリスクが高いため受容は推奨できません。

#### 啓発・教育

* 対象：重要な情報資産にアクセスできる担当者
  + 誤操作や運用変更によって発生するリスクと防御策を共有します。

#### 管理規程

以下の規程の整備を検討します。

* 重要資産管理規程。
* ログ監査を行う場合  
  コマンドラインインターフェース、スクリプトの監査規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

[17章・コマンドラインインターフェースの悪用]、[18章・PowerShellの悪用]、[20章・悪意あるスクリプティングの実行] を参考にしてコマンド、スクリプト実行のログを取得します。

#### モニタリング

前項のポリシーを設定の上、以下の監査の実施を検討します。

* コマンドラインインターフェースの監査
  + [イベントビューアー]-[Windowsログ]-[セキュリティ]-[Event ID 4688] を検索し、不審なdir、tree等の実行を監査します。なお、上記コマンドをPowerShellで実行しても、セキュリティログに記録されます。
* PowerShellスクリプトの監査
  + [イベントビューアー]-[アプリケーションとサービスログ]-[Microsoft]-[Windows]-[PowerShell/Operational] で、Get-Childitem等の不審なスクリプトの実行を監査します。

#### ネットワークデザイン、アクセスコントロール 、フィルタリング

* 重要情報資産を特定セグメントに設置し、必要最低限のプロトコルだけを許可し、不要なポートはすべて閉じます。
* 重要資産にアクセスできるユーザーの権限（読み取り、書き込み、実行、削除等）を設定し、文書化します。
* 重要資産に対するロール管理を設計し設定します[[68]](#footnote-68)。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

該当しません。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・ネットワークサービスのスキャン

### 戦術：情報の探索

MITRE ATT&CK T1046 Network Service Scanning

### 対象プラットフォーム

* Windows
* Amazon Web Services (AWS)、Google Cloud Platform (GCP)、Microsoft Azure

### 概説

攻撃者はリモートホストで実行されているサービスのリストを取得しようとする場合があります。併せて、リモートホストで実行されているソフトウェアの脆弱性を狙い侵入を試みることもあります。ネットワークサービスのスキャンは攻撃の前兆ともいえます。

### 緩和の方針

スキャンは日常的に実施される可能性があることから、脆弱性の是正とスキャンの検出の観点から緩和を実施します。

### 運用やNetworkが変更された場合の影響の有無

脆弱性対策を怠ることで、攻撃のリスクが高まります。不要なポートの公開は、脆弱性攻撃を受けるリスクが高まります。

### 優先すべき措置

以下の措置の実施を検討して下さい。

* 重要資産が保存されている端末、サーバーに関連する脆弱性情報の収集と、脆弱性修正プログラムを適切に適用します。
* 侵入検知システムを使用しスキャンを検出、防止を検討します。
* 不要なポートとサービスを閉じ、定期的に監査します。

### ユーザー運用管理責任

#### リスクの受容

脆弱性修正プログラムの早期適用や、侵入検知システムの導入が困難な場合は、情報資産の暗号化などの軽減策を講じ、攻撃のリスクを受容することを検討します。

#### 啓発・教育

該当しません。

#### 管理規程

以下の規程の整備を検討します。

* 脆弱性情報管理、脆弱性修正プログラム適用規程。
* 重要情報資産の監査規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

該当しません。

#### モニタリング

以下の監査の実施を検討します。

* コマンドラインインターフェースから以下のコマンドを実行し、ListeningのTCPポートとプロセスを監査し、不要なポートは閉じます。

c:\Windows\system32>netstat -ano

* -a すべての接続とリッスン ポートを表示  
  -nアドレスとポート番号を数値形式で表示  
  -o 各接続に関連付けられたそれらを所有するプロセス ID を表示

#### ネットワークデザイン、アクセスコントロール 、フィルタリング

* 重要情報資産を特定セグメントに設置し、必要最低限のプロトコルだけを許可し、不要なポートはすべて閉じます。
* 重要情報資産へのアクセスは必要最小限の許可されたユーザーとし、データは適切に暗号化、バックアップがなされている必要があります。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

侵入検知システム、Endpoint Detection and Responseの導入を検討します。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・システム情報の探索

### 戦術：情報の探索

MITRE ATT&CK T1082 System Information Discovery[[69]](#footnote-69)

### 概説

攻撃者は、バージョン、パッチ・修正プログラムの適用、サービスパックの適用など、オペレーティングシステムとハードウェアに関する詳細情報を収集する場合があります。取得した情報によって、永続的な感染を試みたり、他の行動をとることがあります。以下はシステム情報を取得するためのコマンドやプログラムの例です。

* Windows コマンドラインインターフェース
  + msinfo32、systeminfo
  + wmic
* Windows PowerShell
  + Get-wmiobject、Get-CimInstance、Get-ComputerInfo
* Amazon Web Services
  + Application Discovery Service
* Google Cloud Platform
  + GET /v1beta1/{{parent=organizations/}}/assets
  + POST /v1beta1/{{parent=organizations/}}/assets:runDiscovery
* Microsoft Azure
  + GET https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Compute/virtualMachines/{vmName}?api-version=2019-03-01

### 緩和の方針

この手法はシステムの標準機能を悪用するため予防的設定が困難です。システム情報から、脆弱性更新プログラムの適用状況が窃取され、脆弱性を検出された場合は悪用される可能性があるため、脆弱性情報の取得と脆弱性修正プログラムの適用を適切に行い、検出に努めます。

### 運用やNetworkが変更された場合の影響の有無

該当しません。

### 優先すべき措置

以下の措置の実施を検討して下さい。

* 脆弱性情報の取得と脆弱性修正プログラムの適用を適切に行います。
* システム情報の取得に伴うコマンド実行の検出に努めます。

### ユーザー運用管理責任

#### リスクの受容

脆弱性修正プログラムを適宜適用できない場合は、この攻撃は受容し、情報資産の暗号化、アクセス制御等の設定を検討します。

#### 啓発・教育

該当しません。

#### 管理規程

以下の規程の整備を検討します。

* 脆弱性修正プログラム適用規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

[17章・コマンドラインインターフェースの悪用]、[18章・PowerShellの悪用]を参考にして、コマンド、スクリプト実行のログ取得を設定します。

#### モニタリング

以下の監査の実施を検討します。

* コマンドラインインターフェースの監査
  + 前項のポリシーを設定の上、[イベントビューアー]-[Windowsログ]-[セキュリティ]-[Event ID 4688] を検索し、不審な msinfo32、systeminfo等の実行を監査します。なお、上記コマンドをPowerShellで実行しても、セキュリティログに記録されます。
* PowerShellスクリプトの監査
  + [イベントビューアー]-[アプリケーションとサービスログ]-[Microsoft]-[Windows]-[PowerShell/Operational] で不審なスクリプトの実行を監査します。

#### ネットワークデザイン、アクセスコントロール 、フィルタリング

該当しません。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

該当しません。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・システムのネットワーク設定の探索

### 戦術：情報の探索

MITRE ATT&CK T1016 System Network Configuration Discovery

### 概説

攻撃者は、OSの標準コマンドを使用して、システムやリモートシステムのネットワーク構成と設定に関する詳細な情報を探索する可能性があります。これらの情報を利用して、ターゲットに感染するか、他のアクションを起こす場合があります。使用されるコマンドは、Arp、ipconfig、nbtstat、route、nslookup などが考えられます。

### 緩和の方針

この手法はシステムの標準機能を悪用するため予防的設定が困難です。ログ分析による検出を検討します。

### 運用やNetworkが変更された場合の影響の有無

該当しません。

### 優先すべき措置

コマンド実行のログ分析による検出を検討します。

### ユーザー運用管理責任

#### リスクの受容

ログの保存、分析にコストがかかる場合は、この攻撃は受容し、情報資産の暗号化、アクセス制御等の設定を検討します。

#### 啓発・教育

該当しません。

#### 管理規程

該当しません。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

[17章・コマンドラインインターフェースの悪用]、[18章・PowerShellの悪用]を参考にしてコマンド、スクリプト実行のログを取得します。

#### モニタリング

以下の監査の実施を検討します。

* + コマンドラインインターフェースの監査
* 前項のポリシーを設定の上、[イベントビューアー]-[Windowsログ]-[セキュリティ]-[Event ID 4688] を検索し、不審なArp、ipconfig、nbtstat、route、nslookup等の実行を監査します。なお、上記コマンドをPowerShellで実行しても、セキュリティログに記録されます。
  + PowerShellスクリプトの監査
* [イベントビューアー]-[アプリケーションとサービスログ]-[Microsoft]-[Windows]-[PowerShell/Operational] で不審なスクリプトの実行を監査します。

#### ネットワークデザイン、アクセスコントロール 、フィルタリング

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

該当しません。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・システムユーザーの探索

### 戦術：情報の探索

MITRE ATT&CK T1033 System Owner/User Discovery

### 概説

攻撃者は、現在ログインしているユーザーやシステムを使用するユーザーを識別する場合があります。net userコマンドなどでログインしているユーザーのIDを取得したり、資格情報をダンプを試みます。実行中のプロセスの所有権やファイル/ディレクトリの所有権、セッション情報、ログなどを様々な方法で収集します。取集した情報によっては、システムに感染するか、他のアクションを起こす場合があります。

### 緩和の方針

この手法はシステムの標準機能を悪用するため予防的設定が困難です。一般業務端末においては、ローカル Administrators にドメインユーザーを所属させないことでnet userコマンド等を使った情報収集を阻止できます。[28章・アカウントの探索のポリシー] の設定を参考にします。

### 運用やNetworkが変更された場合の影響の有無

該当しません。

### 優先すべき措置

コマンド、スクリプトの監査を行い検出に努めます。

### ユーザー運用管理責任

#### リスクの受容

この手法はシステムの標準機能を悪用するため、ポリシー設定、監査ができない場合は受容します。

#### 啓発・教育

該当しません。

#### 管理規程

該当しません。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

[17章・コマンドラインインターフェースの悪用]、[18章・PowerShellの悪用]を参考にしてコマンド、スクリプト実行のログを取得します。

#### モニタリング

以下の監査の実施を検討します。

* + コマンドラインインターフェースの監査
* 前項のポリシーを設定の上、[イベントビューアー]-[Windowsログ]-[セキュリティ]-[Event ID 4688] を検索し、不審なnet user、net localgroup、net group等の実行を監査します。なお、上記コマンドをPowerShellで実行しても、セキュリティログに記録されます。
  + PowerShellスクリプトの監査
* [イベントビューアー]-[アプリケーションとサービスログ]-[Microsoft]-[Windows]-[PowerShell/Operational] で不審なスクリプトの実行を監査します。

#### ネットワークデザイン、アクセスコントロール 、フィルタリング

該当しません。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

該当しません。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・Pass the Hash

### 戦術：水平展開

MITRE ATT&CK T1550.002 Use Alternate Authentication Material: Pass the Hash

### 概説

Windowsには、Kerberos認証、NTLM認証があります。このうちNTLM認証は、Kerberos認証が使えないドメインに参加していないメンバーサーバーやNASでの認証、ローカルアカウントなどで利用される認証方法です。

このNTLM認証は端末のメモリ、レジストリにパスワードのNTLMハッシュ値を保存します。攻撃者はこのNTLMハッシュ値をツールを利用して窃取し、ログオンの際に、NTLMハッシュ値をベースにした認証情報を送信します。サーバー側も同様の情報を保有しているため、NTLMハッシュ値をベースに送られた認証情報をサーバー側でも計算し、合致すれば正しい資格情報が入力されたとしてログオンを許可します。

攻撃者は、ツールを使いメモリ上やレジストリのSecurity Account Manager（SAM：アクセスには管理者権限が必要）のNTLMハッシュ値を取得し、正規のユーザーをなりすましパスワードを利用せず認証情報を計算してサーバーに送信し、ログオンします。

ローカル Administrator は端末の管理を容易にするため、全社的に統一されている場合が多く見受けられますが、ローカルのAdministratorのNTLMハッシュ値が取得されると、全社的な水平展開が可能となり、非常に危険です。

### 緩和の方針

Pass the Hash 対策は拡散を防止する観点から、最も重要な防御、緩和策のひとつです。

Mimikatz、PWDump7などの攻撃ツールが公開されており、保存されているパスワードやパスワードのハッシュ値を窃取するために、多角的な攻撃が存在します。このため、多重防御が必要です。

資格情報管理する LSASS プロセスへの攻撃を防ぎ、資格情報を極力保持しないことが重要です。

### 運用やNetworkが変更された場合の影響の有無

各端末において、ローカルのAdministratorのパスワードが同一の場合、拡散のリスクが高まります。

ドメインユーザーがビルトイン Administrators に所属している場合、攻撃のリスクが高まります。

### 優先すべき措置

**Hashの取得阻止**、**取得された場合の水平展開の阻止**、**垂直展開（特権アカウントに対する侵入）の阻止**の観点で防御を講じます。

#### Hashの取得阻止

以下の措置の実施を検討します。

* Windows Defender Credential Guard の設定。  
  （Windows 10 の場合、Enterprise Edition のライセンスが必要です。Windows Server 2016/2019はライセンスが付与されています。なお、ドメインコントローラーでの Credential Gurad の有効化はサポートされていません。）
* LSA 保護モードの有効化。
* 一般ユーザーをローカル Administrators に所属させません。

#### 水平展開の阻止

以下の措置の実施を検討します。

* 既定の Local Administrator を無効化します。
* ローカルアカウントのネットワーク越しの操作とログオンを制限します。

#### 垂直展開の阻止

以下の措置の実施を検討します。

* 組織内の権限を分離します。ドメインコントローラー、メンバーサーバー、端末の管理者IDを分け、厳格な運用をします。
* 管理者権限を最小化し、特権アカウントの露出を最小限に抑えます。

### ユーザー運用管理責任

#### リスクの受容

Pass The Hash は攻撃者にとって水平展開を図る最も有効な攻撃手法であり、拡散防止の観点からリスク受容はまったく推奨できません。

#### 啓発・教育

* 対象：すべての端末利用者
  + 「一般ユーザーをローカル管理者グループから外す」ことで、アプリケーションのインストールや各種設定の際に手間が増えますが、最も安価かつ最も攻撃の耐性が高くなることについて、理解を求めてください。
  + 「一般ユーザーをローカル管理者グループから外す」を実施しないことで、コストの高いシステム監査が必要になることについても理解を得てください。

#### 管理規程

以下の規程の整備を検討します。

* 端末管理規程に「一般ユーザーをローカル管理者グループから外す」措置を実施しない端末の文書化を追加し、措置を実施しない理由と定期監査を明確化させます。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー ①LSASS保護 + 認証情報の削減

|  |  |  |  |
| --- | --- | --- | --- |
| **対策** | **目的** | **対策の効果** | **対策作業量** |
| Windows Defender Credential Guard | 独立した仮想領域に資格情報を隔離します。LSASS プロセスに対する正当なRPC呼び出し以外のアクセスを不可能とすることで、資格情報の窃盗を防ぎます。[[70]](#footnote-70)※Windows 10 Enterprise エディションが必要 | 非常に高い | 高 |
| [LSA 保護モードの有効化](https://www.softwareisac.jp/ipa/index.php?LSA+%E4%BF%9D%E8%AD%B7%E3%83%A2%E3%83%BC%E3%83%89%E3%81%AE%E6%9C%89%E5%8A%B9%E5%8C%96) | LSASS プロセスに対する悪意のあるプラグインやコードの挿入を防止し、プロセスが保持している資格情報の窃盗を防ぎます。(レジストリで有効化） | 高 | 高 |
| [ビルトイン Administrator の無効化](https://www.softwareisac.jp/ipa/index.php?%E3%83%BBWindows+%E3%81%AE+%E7%AE%A1%E7%90%86%E8%80%85%E3%81%AE%E8%A8%AD%E5%AE%9A) | 既知のアカウントを狙った攻撃を防ぎます。 | 高 | 低 |
| [一般ユーザーをローカル管理者グループから外す](https://www.softwareisac.jp/ipa/index.php?%E3%83%BBWindows+%E3%81%AE+%E7%AE%A1%E7%90%86%E8%80%85%E3%81%AE%E8%A8%AD%E5%AE%9A) | 資格情報窃取やシステムへの攻撃を防ぎます。 | 非常に高い | 高 |
| セキュリティ更新プログラムの適用 | 脆弱性を悪用する攻撃を防ぎます。※特に特権昇格、情報漏洩、バイパスの脆弱性 | 中 | 中 |
| [平文パスワードを保存しない](https://www.softwareisac.jp/ipa/index.php?%E3%83%BBL1+MS+Security+Guide#e6cd5e70) | LSASSメモリに平文パスワードを保存しないことで、攻撃者の窃盗を防ぎます。グループポリシーで[管理用テンプレート]>[MS Security Guide]>[WDigest authentication]を無効にします。  ※Windows 8.1, Windows Server 2012 R2 以降は既定で有効 | 中 | 低 |
| [LM ハッシュを保存しない](https://www.softwareisac.jp/ipa/index.php?%E3%83%BBL1+%E3%83%AD%E3%83%BC%E3%82%AB%E3%83%AB%E3%83%9D%E3%83%AA%E3%82%B7%E3%83%BC+%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3+%E3%82%AA%E3%83%97%E3%82%B7%E3%83%A7%E3%83%B3#pd3ec705) | LM ハッシュは総当たり攻撃などに対して脆弱であるため、パスワード解析のリスクを減らします。※Vista、Windows Server 2008R2 以降は既定で有効 | 中 | 低 |
| [ログオフ後の資格情報消去](https://www.softwareisac.jp/ipa/index.php?%E3%83%AD%E3%82%B0%E3%82%AA%E3%83%95%E5%BE%8C%E3%81%AE%E8%B3%87%E6%A0%BC%E6%83%85%E5%A0%B1%E6%B6%88%E5%8E%BB) | ユーザーのログオフ後に LSASS メモリから消去します。※Windows 8.1, Windows Server 2012 R2 以降は既定で有効 | 低 | 高 |
| NTLMプロトコルを無効にする | NTLM 認証を利用しないことで、NTLM ハッシュを悪用する攻撃を防ぎます。※NTLM認証に依存する実装は多数あることから、事前に十分な検証と使用実態の監査が必要です。[[71]](#footnote-71) | 低 | 高 |
| [ARSO 無効化](https://www.softwareisac.jp/ipa/index.php?ARSO+%E7%84%A1%E5%8A%B9%E5%8C%96) | Windows 8.1 以降の Automatic Restart Sign-On (ARSO) による資格情報保持を無効化します。 | 中 | 低 |

##### LSA 保護モードの有効化

* 機能   
  LSASS プロセス (Lsass.exe) に読み込まれるプラグインは認定された署名を必要とすることで、プロセスを保護します。
* 効果  
  LSASS プロセスに対する悪意のあるプラグインやコードの挿入を防止し、プロセスが保持している資格情報の窃盗を防ぎます。
* 注意事項  
  LSASS プロセスへの攻撃すべてが防げるわけではありません。LSASS 以外に保持されている資格情報の保護は対象外です。  
  また、現在利用中のプラグインがエラーになる可能性があります。対象はスマートカードドライバー、暗号化プラグイン、パスワードフィルターなどです。事前に監査ログを設定し、利用中のプラグインをイベントから確認し、障害を回避します。
* 関連情報   
  追加の LSA の保護の構成[[72]](#footnote-72) を参考にしてください。
* 設定方法：単独のコンピューターに LSA の保護を有効にする
  + レジストリ エディター (RegEdit.exe) を開き、次の場所にあるレジストリ キーに移動します。HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
  + レジストリ キーに次の値を設定します。"RunAsPPL"=dword:00000001
  + コンピューターを再起動します。
* 設定方法：グループ ポリシーを使用して LSA の保護を有効にする
  + グループ ポリシー管理コンソール (GPMC) を開きます。
  + GPO を右クリックし、 [編集] をクリックしてグループ ポリシー管理エディターを開きます。
  + [コンピューターの構成]>[基本設定]>[Windows の設定]>[レジストリ] を右クリックし、 [新規] をポイントして、 [レジストリ項目] をクリックします。 [新しいレジストリのプロパティ] ダイアログ ボックスが表示されます。
  + [ハイブ] の一覧で、HKEY\_LOCAL\_MACHINE をクリックします。
  + キー パス 一覧の SYSTEM\CurrentControlSet\Control\Lsaを参照してください。
  + [値の名前] ボックスに「RunAsPPL」と入力します。
  + [値の種類] ボックスで、 [REG\_DWORD] をクリックします。
  + [値のデータ] ボックスに「00000001」と入力します。
  + [OK] をクリックします。
  + LSA の保護の確認
* [イベントビューワー]> [Windows ログ]>[System] ログで次の WinInit イベントを検索し ます。
  + 12: LSASS.exe がレベル 4 で保護されたプロセスとして起動されました
  + 追加の LSA の保護の構成 を参考にしてください。[[73]](#footnote-73)

##### ビルトイン Administrator の無効化

[7章・Windows の管理者の設定] の [7.1.3.1ビルトイン Administrator へのブルートフォース攻撃（総当たり攻撃）] を参照してください。

##### [一般ユーザーをローカル管理者グループから外す](https://www.softwareisac.jp/ipa/index.php?%E3%83%BBWindows+%E3%81%AE+%E7%AE%A1%E7%90%86%E8%80%85%E3%81%AE%E8%A8%AD%E5%AE%9A)

[7章・Windows の管理者の設定] の [7.1.3.3ドメインユーザーがビルトイン Administrators に所属している場合の攻撃] を参照してください。

##### 平文パスワードを保存しない

WDigest認証は平文パスワードが保存されます。グループポリシーで設定を変更するには、「13.8・L1 MS Security Guide」の [[WDigest authentication](https://www.softwareisac.jp/ipa/index.php?WDigest+authentication)] を参照してください。Windows 8.1 と Windows Server 2012 R2 以降のバージョンの既定では、メモリ内に資格情報を取得する WDigest の設定は無効です (レジストリ エントリが存在しない場合、UseLogonCredential 値の既定は 0 です)が、攻撃によって改ざんされないように、グループポリシーを設定して下さい。

なお、Windows 8、Windows Server 2012は、KB2871997を適用することで、WDigest認証を無効にできます。後述の [35.7.1.6 ログオフ後の資格情報消去] を参照してください。

* KB2871997適用後、レジストリで修正する場合
  + HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest-UseLogonCredential
  + UseLogonCredential 値が 0 に設定されている場合、WDigest は資格情報をメモリに保存しません。
  + UseLogonCredential 値が 1 に設定されている場合、WDigest は資格情報をメモリに保存します。

##### [LM ハッシュを保存しない](https://www.softwareisac.jp/ipa/index.php?%E3%83%BBL1+%E3%83%AD%E3%83%BC%E3%82%AB%E3%83%AB%E3%83%9D%E3%83%AA%E3%82%B7%E3%83%BC+%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3+%E3%82%AA%E3%83%97%E3%82%B7%E3%83%A7%E3%83%B3#pd3ec705)

Lan Manager認証のLMハッシュは脆弱なため、グループポリシーでLMハッシュの保存を無効にします。Vista以降は既定で無効になっています。

[13.5.7 [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ネットワークセキュリティ]] の [[次回のパスワード変更時に LAN Manager のハッシュ値を保存しない]] を参照してください。

##### ログオフ後の資格情報消去（Windows 8、Windows Server 2012）

* 機能  
  Windows 8.1より前のバージョンのWindowsの場合、KB2871997[[74]](#footnote-74)がインストールされていることを確認します。この更新プログラムはユーザーのログオフ後に LSASS メモリから消去します。(平文パスワード、NT/LM ハッシュ, Kerberos TGT, セッションキー)Windows 8.1以降はデフォルトで有効になっています。
* 効果  
  ユーザーのログオフ後に行われる資格情報の窃盗を防ぎます。
* 注意事項  
  LSASS メモリ以外に保存されている資格情報は機能の対象外です。
* 設定方法
  + HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\TokenLeakDetectDelaySecs DWORD:30

##### NTLMプロトコルを無効にする

NTLM 認証を利用しないことで、NTLM ハッシュを悪用する攻撃を防ぎます。

※NTLM認証に依存する実装は多数あることから、事前に十分な検証と使用実態の監査が必要です。

ネットワーク セキュリティ: NTLM を制限する: 着信 NTLM トラフィックを監査する:

https://docs.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-audit-incoming-ntlm-traffic

802.1X認証を使ったWi-Fiの接続等に影響が出る場合がありますので、十分、ご注意ください。

##### [ARSO 無効化](https://www.softwareisac.jp/ipa/index.php?ARSO+%E7%84%A1%E5%8A%B9%E5%8C%96)

* 機能  
  ARSOは、デバイスが Active Directory または Azure Active Directory に参加している場合、ユーザーの不在時にデバイスが自動的にアップデートをインストールして再起動した場合に、Windowsのロック画面通知（デバイスのロック画面に表示される目覚まし時計やカレンダーの通知など）が機能し続けるように設計されています。この体験を実現するために、Windows は、ログオンしたユーザーの暗号化された資格情報をデバイスの再起動中にローカル ストレージに一時的に保存し、その後、それらを使用してユーザーを再びログオンしてデバイスをロックする必要があります。この方法では、ユーザーがデバイスに戻ってきたときに、重要な通知がすぐに見えるようになります。しかし、攻撃者は、クレデンシャルが保存されている間にクレデンシャルにアクセスできる可能性があります。

この機能は、BitLockerが有効になっているWindows 8.1ではデフォルトで有効になっています

* 効果  
  Windows Update後の資格情報の窃盗を防ぎます。
* 注意  
  本設定は、[・L1 Windows コンポーネント] のポリシー設定には含まれていません。
* 設定方法
  + [コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Windows コンポーネント]>[Windows ログオンのオプション]>[再起動後に自動的に前回の対話ユーザーでサインインしてロックする] 値：[無効] にします。

#### ポリシー ②水平展開の阻止

|  |  |  |  |
| --- | --- | --- | --- |
| **策** | **目的** | **対策の効果** | **対策作業量** |
| [・LAPS](https://www.softwareisac.jp/ipa/index.php?%E3%83%BBLAPS)  Local Administrator Password Solution[[75]](#footnote-75) | 攻撃者がドメイン内の異なる端末へ侵入を広げる機会を減らす | 高 | 中～高 |
| [ローカルアカウントのネットワーク越しの操作制限、ログオン防止](https://www.softwareisac.jp/ipa/index.php?%E3%83%AD%E3%83%BC%E3%82%AB%E3%83%AB%E3%82%A2%E3%82%AB%E3%82%A6%E3%83%B3%E3%83%88%E3%81%AE%E3%83%8D%E3%83%83%E3%83%88%E3%83%AF%E3%83%BC%E3%82%AF%E8%B6%8A%E3%81%97%E3%81%AE%E6%93%8D%E4%BD%9C%E5%88%B6%E9%99%90%E3%80%81%E3%83%AD%E3%82%B0%E3%82%AA%E3%83%B3%E9%98%B2%E6%AD%A2) | 遠隔地にいる攻撃者がローカル管理者を悪用することを防ぐ  ※新しい well-known SIDs の活用 | 高 | 中 |

##### LAPS

ローカル Administrator のパスワードを一台ずつ、すべてユニークにします。リモートでこの作業を一括して展開できるツール LAPS (Local Administrator Password Solution) が、Microsoft から無償で提供されています。

* 機能
  + セキュリティ  
    管理対象マシンで自動的に変更されるパスワードをランダムに生成します。  
    Kerberosバージョン5プロトコルを使用した暗号化による転送中のパスワード保護の強化。  
    アクセス制御リスト（ACL）を使用してActive Directoryのパスワードを保護し、詳細なセキュリティモデルを簡単に実装します。
  + 管理機能  
    複雑さ、長さなどのパスワードパラメータを設定します。  
    マシンごとにパスワードを強制的にリセットします。  
    Active DirectoryのACLと統合されたセキュリティモデルを使用します。  
    コンピューターアカウントの削除から保護します。  
    最小限の設置面積でソリューションを簡単に実装します。  
    ドメインコントローラー、LAPSツールをインストールした端末、PowerShell（適切な権限が必要）から、ランダムに設定されたローカル Administrator のパスワードを確認できます。
* 効果  
  同一のローカルアカウントパスワードに依存するPass The Hash攻撃を効果的に軽減します。  
  多数の端末のローカルAdministrator のパスワードをランダムに設定でき、かつ、管理者はそのパスワードを適切に確認できます。  
  Active Directory に保存されているパスワードを閲覧したユーザーを監査できます。
* 設定方法
  + ローカル管理者パスワードソリューション（LAPS）導入ガイド（日本語版）[[76]](#footnote-76) を参考にしてください。

##### ローカルアカウントのネットワーク越しの操作制限、ログオン防止

ローカルアカウントやGuest、Anonymous がネットワーク越しに端末やサーバーを操作するのを防止します。グループポリシーで設定を実施します。

* 機能  
  ローカルアカウントに対する新しい Well-Known SID の割り当てを利用しローカルアカウントへの制限を実施します。
  + S-1-5-113 ローカル アカウント
  + S-1-5-114 ローカル アカウントと Administrators グループのメンバー
* 効果  
  グループポリシーを利用することで、ローカルアカウントへの制限が容易になります。
* 注意事項  
  LSASS メモリ以外に保存されている資格情報は機能の対象外です。
* 設定方法：ネットワーク経由のアクセスを拒否
  + [コンピュータの構成]>[ポリシー]>[Windowsの設定]>[セキュリティの設定]>[ユーザー権利の割り当て]>[ネットワーク経由のアクセスを拒否] をクリックし、[これらのポリシーの設定を定義する] にチェックボックスを入れます。
  + [ユーザーまたはグループの追加] をクリックします。
  + [参照]をクリックします。
  + [場所]をクリックします。
  + ドメイン名ではなくローカルサーバーをクリックし、[OK] をクリックます。
  + "ローカル" と入力し、[名前の確認] をクリックします。
  + "ローカル アカウント" と "ローカル アカウントと Administrators グループのメンバー" を指定し、[OK] をクリックします。
  + "Guests” と入力し、[名前の確認] をクリックします。
  + "ANONYMOUS LOGON" と入力し、[名前の確認] をクリックします。
  + [OK] をクリックします。
  + [OK] をクリックします。
* 設定方法：リモート デスクトップ サービスを使ったログオンを拒否
  + [コンピュータの構成]>[ポリシー]>[Windowsの設定]>[セキュリティの設定]>[ユーザー権利の割り当て]>[リモートデスクトップサービスを使ったログオン拒否] をクリックし、 [これらのポリシーの設定を定義する] にチェックボックスを入れます。
  + [ユーザーまたはグループの追加] をクリックします。
  + [参照]をクリックします。
  + [場所]をクリックします。
  + ドメイン名ではなくローカルサーバーをクリックし、[OK] をクリックます。
  + "ローカル" と入力し、[名前の確認] をクリックします。
  + "ローカル アカウント" と "ローカル アカウントと Administrators グループのメンバー" を指定し、[OK] をクリックします。
  + "Guests” と入力し、[名前の確認] をクリックします。
  + [OK] をクリックします。
  + [OK] をクリックします。

#### ポリシー ③縦展開防止対策

|  |  |  |  |
| --- | --- | --- | --- |
| **対策** | **目的** | **対策の効果** | **対策作業量** |
| 組織内の権限を分離する | 攻撃者がドメイン内の異なる端末へ侵入を広げる機会を減らす | 非常に高い | 高 |
| 特権アカウントの保護 | 特にドメイン管理権限を保護 | 非常に高い | 中 |
| 高い権限を持つ端末の要塞化 | 高い権限を扱う端末を要塞化することで攻撃者の機会を減らす | 高 | 中～高 |
| リモートセッション資格情報保護 | 侵害にあっている端末へ接続をしてくるユーザーの資格情報を盗まれないようにする | 高 | 中 |

[9章 管理インターフェースの保護] を参照してください。

#### ネットワークデザイン、アクセスコントロール 、フィルタリング

以下の設定を検討して下さい。

* LSA保護を構成する方法[[77]](#footnote-77)
* [9章 管理インターフェースの保護] を参照して、管理端末と一般業務端末のネットワーク分離する。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

侵入検知システム、Endpoint Detection and Responseの導入を検討します。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・ローカルシステムからのデータ収集

### 戦術：情報の収集

MITRE ATT&CK T1005 Data from Local System

### 概説

攻撃者は、ローカルシステムから機密データを収集することがあります。コマンドラインインターフェースを使い、目的のファイルを探します。収集したデータは外部にアップロードしたり、バックドアを設置しファイルを窃取します。

### 緩和の方針

この手法はシステム機能の悪用に基づいているため、予防的設定は困難です。そのため、暗号化やライツマネジメントなどを用いて、漏洩等の影響を最小限にすることを検討します。

### 運用やNetworkが変更された場合の影響の有無

ファイルやフォルダーのアクセス権限が Everyone であると窃取されるリスクが高まります。定期的に重要資産に対するアクセス権の監査を実施してください。

### 優先すべき措置

重要資産の暗号化、ライツマネジメントの導入を検討します。

コマンドラインインターフェースの実行ログ、PowerShell のスクリプトブロックのログを取得し、検出を強化します。

侵入検知システム、Endpoint Detection and Response の導入を検討します。

### ユーザー運用管理責任

#### リスクの受容

基本的に防御が困難なため、重要資産の暗号化、ライツマネジメント等の導入をした上で、この手法のリスクは受容し、漏洩しても実質的に情報が悪用されないことを検討します。

#### 啓発・教育

* 対象：すべての端末利用者
  + 重要な情報資産に対しては、パスフレーズを使った暗号化設定などに対する理解を求めてください。

#### 管理規程

以下の管理規程の整備を検討して下さい。

* 重要資産に対する監査規程
* コマンドラインインターフェースの監査規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

[17章・コマンドラインインターフェースの悪用]、[18章・PowerShellの悪用]を参考にしてコマンド、スクリプト実行のログを取得します。

#### モニタリング

以下の監査の実施を検討します。

* コマンドラインインターフェースの監査
  + 前項のポリシーを設定の上、[イベントビューアー]-[Windowsログ]-[セキュリティ]-[Event ID 4688] を検索し、不審なdir、copy等の実行を監査します。なお、上記コマンドをPowerShellで実行しても、セキュリティログに記録されます。
* PowerShellスクリプトの監査
  + [イベントビューアー]-[アプリケーションとサービスログ]-[Microsoft]-[Windows]-[PowerShell/Operational] で不審なスクリプトの実行を監査します。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

重要資産のフォルダー、ファイルのアクセス権を適切に設定します。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

侵入検知システム、Endpoint Detection and Responseの導入を検討します。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・ネットワーク共有ドライブからのデータ収集

### 戦術:情報の収集

MITRE ATT&CK T1039 Data from Network Shared Drive

### 概説

攻撃者はネットワーク上のファイルサーバーや、端末のネットワーク共有ドライブなどから機密データを窃取します。コマンドラインインターフェースを介してネットワーク共有を探します。

### 緩和の方針

この手法はシステムの標準機能を悪用することから予防的設定が困難です。管理されていない端末のドライブ・フォルダー共有や、部門が独自に設置したNAS等は運用を停止し、管理されたファイルサーバーに集約し、適切なアクセス権を設定します。

### 運用やNetworkが変更された場合の影響の有無

アクセス権が設定されていない [Everyone] がアクセスできる共有フォルダーに機密データが保存された場合、リスクが高まります。機密データは、アクセス権が適切に設定されたフォルダーに適切な強度の暗号を設定して保存してください。

### 優先すべき措置

コマンドラインインターフェースの実行ログを取得し、検出を強化し、重要な情報資産に対するコントロールを検討します。

### ユーザー運用管理責任

#### リスクの受容

基本的に防御が困難なため、この手法のリスクは受容します。

#### 啓発・教育

* 対象：すべての端末利用者
  + サーバー以外の端末での共有フォルダーによる共有を禁止し、アクセス権の設定されたファイルサーバー等の利用を促します。
  + 機密データの暗号化を促します。

#### 管理規程

以下の管理規程の整備を検討します。

* 端末運用規程でのローカル共有ドライブの利用禁止規程。
* ファイルサーバー、NAS、クラウドストレージサービス等の管理規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

[17章・コマンドラインインターフェースの悪用]、[18章・PowerShellの悪用]を参考にしてコマンド、スクリプト実行のログを取得します。

#### モニタリング

以下の監査の実施を検討します。

* コマンドラインインターフェースの監査
  + 前項のポリシーを設定の上、[イベントビューアー]-[Windowsログ]-[セキュリティ]-[Event ID 4688] を検索し、不審なnet、dir等の実行を監査します。なお、上記コマンドをPowerShellで実行しても、セキュリティログに記録されます。
* PowerShellスクリプトの監査
  + 前項のポリシーを設定の上、[イベントビューアー]-[アプリケーションとサービスログ]-[Microsoft]-[Windows]-[PowerShell/Operational] で不審なスクリプトの実行を監査します。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

以下のコントロールを検討します。

* 重要資産が保存されたファイルサーバーなどのアクセス権の設定を監査し、問題があれば再設定します。
* ファイルサーバー、NAS、端末の共有フォルダー等のアクセス権限が Everyone となっているフォルダーの検出と、適切なアクセス権を再設定します。
* ファイルサーバー等に情報資産を保存する際の、管理者と利用者のロール設定を検討します。
* 個人情報、クレジットカード情報、営業情報、財務情報など、企業内での重要情報の棚卸を実施します。
* セキュリティ設定管理者の権限、利用者の権限を検討します。
* 重要な資産に対する暗号化、パスワード設定等のルールも併せて検討します。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

侵入検知システム、Endpoint Detection and Responseの導入を検討します。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・データの圧縮

### 戦術：持ち出し

MITRE ATT&CK T1560.001 Archive Collected Data: Archive via Utility

### 概説

攻撃者は窃取した情報の送信量を最小限に抑えるため、データを圧縮することがあります。圧縮はカスタムプログラム、もしくは、7zip、RAR、ZIP、zlibなどの一般的な圧縮ライブラリまたはユーティリティを使用します。

### 緩和の方針

ネットワーク侵入防止システムで、特定のファイル形式の送信を検知することができます。ただし、暗号化された通信の場合、検知できない場合があります。

圧縮は様々な業務端末では日常的に実行されますが、ドメインコントローラーやアプリケーションサーバーなどでの圧縮プログラムの実行は限定的です。このため、重要資産が配置されているサーバーでの検出を検討します。

### 運用やNetworkが変更された場合の影響の有無

該当しません。

### 優先すべき措置

重要資産が配置されているサーバーでのコマンドラインインターフェースのログの取得と分析を検討します。

### ユーザー運用管理責任

#### リスクの受容

暗号化された通信の場合、圧縮されたデータを検知することが困難です。従って、重要資産の暗号化を実施し、暗号化通信のリスクは受容し、事後的な検出に努めることを検討します。

#### 啓発・教育

該当しません。

#### 管理規程

以下の管理規程の整備を検討します。

* 重要資産の監査規程。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

[17章・コマンドラインインターフェースの悪用]、[18章・PowerShellの悪用]を参考にしてコマンド、スクリプト実行のログを取得します。

#### モニタリング

以下の監査の実施を検討します。

* コマンドラインインターフェースの監査
  + 前項のポリシーを設定の上、[イベントビューアー]-[Windowsログ]-[セキュリティ]-[Event ID 4688] を検索し、不審なnet、dir等の実行を監査します。なお、上記コマンドをPowerShellで実行しても、セキュリティログに記録されます。
* PowerShellスクリプトの監査
  + [イベントビューアー]-[アプリケーションとサービスログ]-[Microsoft]-[Windows]-[PowerShell/Operational] で不審なスクリプトの実行を監査します。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

以下のコントロールを検討します。

* 重要資産が保存されたファイルサーバーなどのアクセス権の設定を監査し、問題があれば再設定します。
* ファイルサーバー、NAS、端末の共有フォルダー等のアクセス権限が Everyone となっているフォルダーの検出と、適切なアクセス権を再設定します。
* ファイルサーバー等に情報資産を保存する際の、管理者と利用者のロール設定を検討します。
* 個人情報、クレジットカード情報、営業情報、財務情報など、企業内での重要情報の棚卸を実施します。
* セキュリティ設定管理者の権限、利用者の権限を検討します。
* 重要な資産に対する暗号化、パスワード設定等のルールも併せて検討します。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

該当しません。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

## ・一般的に利用されるポートの悪用

### 戦術：外部からの指令統制

MITRE ATT&CK T1001.003 Data Obfuscation: Protocol Impersonation

### 概説

攻撃者は一般的に使用されるポートを介して通信し、ファイアウォールまたはネットワーク検出システムをバイパスし、通常の通信にまぎれて、詳細な検査を回避します。次のような一般的に開いているポートを使用する場合がありますが、これに限りません。

|  |  |  |
| --- | --- | --- |
| **プロトコル、ポート** | **名称** | **用途** |
| TCP:20 | FTP | ファイル転送(データ) |
| TCP:21 | FTP | ファイル転送(制御) |
| TCP/UDP:22 | SSH | Secure Shell |
| TCP:25 | SMTP | 電子メール送信 |
| TCP/UDP:53 | DNS | ドメインの名前解決 |
| TCP:80 | HTTP | Webアクセス |
| TCP:110 | POP | 電子メール受信 |
| TCP/UDP:135 | RPC | RPC |
| TCP:443 | HTTPS | Webアクセス |
| TCP:445 | SMB | ファイル共有 |
| TCP/UDP:3389 | RDP | リモートデスクトップ |

### 緩和の方針

一般的に使用される通信プロトコルを悪用するため、完全な防御は困難な場合があります。

* 重要な情報資産があるネットワークセグメントに不要なポートをブロックします。
* 監査を強化し検出に努めます。

### 運用やNetworkが変更された場合の影響の有無

重要資産を有する端末、サーバーがあるネットワークセグメントに不要なポートが公開された場合、侵入、情報漏洩、改ざん、他のシステムへの感染などのリスクが高まります。

### 優先すべき措置

重要な情報資産があるネットワークセグメントに不要なポートをブロックします。

侵入検知システムの導入を検討します。

### ユーザー運用管理責任

#### リスクの受容

一般的に使用される通信プロトコルを悪用するため、重要な情報資産を暗号化するなどし、外部流出しても内容の暴露の可能性が低いと判断できる場合などは、リスクを受容します。

#### 啓発・教育

* 対象：開発者、Web作成者
  + FTP、SSHなどのポートを使用する、開発者端末の危険性の認識を共有します。
  + パーソナルファイアーウォールを利用し、接続先のIPを制限するなどの端末管理の正しい理解を求めます。

#### 管理規程

以下の管理規程の整備を検討します。

* 開発端末のログ取得及び監査規程を整備します。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

該当しません。

#### モニタリング

以下の監査の実施を検討します。

* 侵入検知システムを導入した場合は、重要資産が保存されているサーバー、端末でのアクセスログの分析を実施します。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

重要資産を有する端末、サーバーの厳格なセグメント分離、不要なポートの停止を実施します。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

侵入検知システム、Endpoint Detection and Responseの導入を検討します。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じる。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じる。 例外はすべて文書化し、適切な監査を実施します。

## ・標準アプリケーションレイヤプロトコル(HTTP,SMTPなど)

### 戦術：外部からの指令統制

MITRE ATT&CK T1071 Application Layer Protocol

### 概説

一般的に利用されるポートの悪用と同様に、攻撃者は標準アプリケーションレイヤプロトコル（HTTP、SMTP)などを介して通信し、ファイアウォールまたはネットワーク検出システムをバイパスし、通常の通信にまぎれて、詳細な検査を回避します。次のような一般的に開いているポートを使用する場合があります。

* 外部通信の場合

|  |  |  |
| --- | --- | --- |
| **プロトコル、ポート** | **名称** | **用途** |
| TCP:20 | FTP | ファイル転送(データ) |
| TCP:21 | FTP | ファイル転送(制御) |
| TCP:25 | SMTP | 電子メール送信 |
| TCP/UDP:53 | DNS | ドメインの名前解決 |
| TCP:80 | HTTP | Webアクセス |
| TCP:110 | POP | 電子メール(受信) |
| TCP:443 | HTTPS | Webアクセス |
| TCP:993 | IMAPS | 電子メール |
| TCP:995 | POPS | 電子メール(受信) |
| TCP/UDP:989 | FTPS | ファイル転送(データ) |
| TCP/UDP:990 | FTPS | ファイル転送(制御) |

* 組織内通信の場合

|  |  |  |
| --- | --- | --- |
| **プロトコル、ポート** | **名称** | **用途** |
| TCP/UDP:22 | SSH | Secure Shell |
| TCP/UDP:69 | TFTP | ファイル転送 |
| TCP:445 | SMB | ファイル共有 |
| TCP/UDP:3389 | RDP | リモートデスクトップ |

### 緩和の方針

一般的に使用される通信プロトコルを悪用するため、完全な防御は困難な場合があります。

* 重要な情報資産があるネットワークセグメントに不要なポートをブロックします。
* 監査を強化し検出に努めます。

### 運用やNetworkが変更された場合の影響の有無

重要資産を有する端末、サーバーがあるネットワークセグメントに不要なポートが公開された場合、侵入、情報漏洩、改ざん、他のシステムへの感染などのリスクが高まります。

### 優先すべき措置

重要な情報資産があるネットワークセグメントに不要なポートをブロックします。

侵入検知システムの導入を検討します。

### ユーザー運用管理責任

#### リスクの受容

一般的に使用される通信プロトコルを悪用するため、重要な情報資産を暗号化するなどし、外部流出しても内容の暴露の可能性が低いと判断できる場合などは、リスクを受容します。

#### 啓発・教育

該当しません。

#### 整備すべき規程

該当しません。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

該当しません。

#### モニタリング

以下の監査の実施を検討します。

* 侵入検知システムを導入した場合は、重要資産が保存されているサーバー、端末でのアクセスログの分析の実施。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

重要資産が保存されているサーバー、端末では、不要なアプリケーションレイヤーポートを閉じます。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

侵入検知システムの導入を検討してください。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じる。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じる。 例外はすべて文書化し、適切な監査を実施します。

## ・データの暗号化

### 戦術：持ち出し、外部からの指令統制

* MITRE ATT&CK T1048 Exfiltration Over Alternative Protocol[[78]](#footnote-78)  
   T1573 Encrypted Channel[[79]](#footnote-79)

### 概説

攻撃者は外部にデータを持ち出す際に、検出を免れるためデータを暗号化して外部に送信する場合があります。暗号化は、JCE（Java 暗号化拡張機能）やWindows CNG(Cryptography Next Generation) APIを使ったり、悪意あるプログラムオリジナルのアルゴリズムで暗号化されます。RAR、Zipなどのアーカイブも利用されます。

* 利用された暗号形式 出典: https://attack.mitre.org/techniques/T1022/
  + AES、3DES、DES、RC4
  + BASE64エンコード
  + AESで暗号化の後、BASE64でエンコード
  + XOR
  + 単純置換暗号+XOR
  + XOR+Zip

### 緩和の方針

この攻撃手法はシステム機能の悪用に基づいているため、予防的設定では緩和できません。

コマンドラインインターフェース、PowerShellの監査など事後的な検出に努めますが、必ずしも検出できるとは限りません。

### 運用やNetworkが変更された場合の影響の有無

該当しません。

### 優先すべき措置

侵入検知システムの導入を検討します。

コマンドラインインターフェース、PowerShellの監査の実施を検討します。

### ユーザー運用管理責任

#### リスクの受容

暗号化されたデータを検知することは困難です。従って、重要資産の暗号化を実施し、暗号化通信のリスクは受容し、事後的な検出に努めることを検討します。

#### 啓発・教育

該当しません。

#### 管理規程

該当しません。

### 情報システム設計開発部門・運用部門（ベンダー代行を含む)

#### ポリシー

[17章・コマンドラインインターフェースの悪用]、[18章・PowerShellの悪用]を参考にしてコマンド、スクリプト実行のログを取得します。

#### モニタリング

以下の監査の実施を検討します。

* コマンドラインインターフェースの監査
  + 前項のポリシーを設定の上、[イベントビューアー]-[Windowsログ]-[セキュリティ]-[Event ID 4688] を検索し、不審なnet、dir等の実行を監査します。なお、上記コマンドをPowerShellで実行しても、セキュリティログに記録されます。
* PowerShellスクリプトの監査
  + [イベントビューアー]-[アプリケーションとサービスログ]-[Microsoft]-[Windows]-[PowerShell/Operational] で不審なスクリプトの実行を監査します。

#### ネットワークデザイン、アクセスコントロール、フィルタリング

該当しません。

#### 仮想端末運用

これは将来のためのプレースフォルダーです。

#### ゲートウェイ及びエンドポイント対策

該当しません。

### 受託開発ベンダー管理責任

#### セキュアコーディング

該当しません。

#### 開発環境管理

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

#### サプライチェーン正常性維持

ユーザー運用管理責任、情報システム設計開発部門・運用部門責任に準じます。 例外はすべて文書化し、適切な監査を実施します。

参考例



アプリケーションセキュリティ検証標準 4.0 Application Security Verification Standard 4.0

1. 最終版

2019 年 3 月

邦訳：Software ISAC 2020 年 8 月

目次

[アプリケーションセキュリティ検証標準 4.0 Application Security Verification Standard 4.0 1](#_Toc56782123)

[1. 最終版 1](#_Toc56782124)

[口絵 8](#_Toc56782125)

[2. 本標準について 8](#_Toc56782126)

[3. 著作権とライセンス 8](#_Toc56782127)

[4. プロジェクトリーダー 8](#_Toc56782128)

[5. 執筆者およびレビュー担当者 8](#_Toc56782129)

[序文 10](#_Toc56782130)

[6. 4.0 の更新内容 10](#_Toc56782131)

[ASVS の使い方 13](#_Toc56782132)

[7. アプリケーションセキュリティ検証レベル 13](#_Toc56782133)

[8. この標準の使い方 15](#_Toc56782134)

[9. 実際にASVS を適用する 16](#_Toc56782135)

[監査と認証 17](#_Toc56782136)

[10. ASVS 認証と認証マークに対する OWASP の見解 17](#_Toc56782137)

[11. 認証機関のためのガイダンス 17](#_Toc56782138)

[12. ASVS のその他の用途 19](#_Toc56782139)

[V1: アーキテクチャ、設計、脅威モデリング要件 21](#_Toc56782140)

[13. 管理目標 21](#_Toc56782141)

[14. V1.1 セキュアソフトウェア開発ライフサイクル要件 22](#_Toc56782142)

[15. V1.2 認証アーキテクチャ要件 23](#_Toc56782143)

[16. V1.3 セッション管理アーキテクチャ要件 23](#_Toc56782144)

[17. V1.4 アクセス制御アーキテクチャ要件 24](#_Toc56782145)

[18. V1.5 入力および出力アーキテクチャ要件 24](#_Toc56782146)

[19. V1.6 暗号アーキテクチャ要件 25](#_Toc56782147)

[20. V1.7 エラー、ロギング、監査アーキテクチャ要件 26](#_Toc56782148)

[21. V1.8 データ保護とプライバシーアーキテクチャ要件 26](#_Toc56782149)

[22. V1.9 通信アーキテクチャ要件 26](#_Toc56782150)

[23. V1.10 悪意あるソフトウェアのアーキテクチャ要件 27](#_Toc56782151)

[24. V1.11 ビジネスロジックアーキテクチャ要件 27](#_Toc56782152)

[25. V1.12 セキュアファイルアップロードアーキテクチャ要件 27](#_Toc56782153)

[26. V1.13 API アーキテクチャ要件 28](#_Toc56782154)

[27. V1.14 コンフィギュレーションアーキテクチャ要件 28](#_Toc56782155)

[28. 参考情報 29](#_Toc56782156)

[V2:認証の検証要件 30](#_Toc56782157)

[29. 管理目標 30](#_Toc56782158)

[30. NIST 800-63 - 最新のエビデンスベースの認証標準 30](#_Toc56782159)

[31. 凡例 31](#_Toc56782160)

[32. V2.1 パスワードセキュリティ要件 31](#_Toc56782161)

[33. V2.2 一般的なオーセンティケータの要件 34](#_Toc56782162)

[34. V2.3 オーセンティケータライフサイクルの要件 35](#_Toc56782163)

[35. V2.4 クレデンシャルの保管要件 36](#_Toc56782164)

[36. V2.5 クレデンシャルリカバリ要件 37](#_Toc56782165)

[37. V2.6 ルックアップシークレット検証者(Verifier)の要件 38](#_Toc56782166)

[38. V2.7 経路外 (Out of Band) 検証者(Verifier) の要件 39](#_Toc56782167)

[39. V2.8 単一または多要素のワンタイム検証者の要件 40](#_Toc56782168)

[40. V2.9 暗号化ソフトウェアおよびデバイス検証者の要件 41](#_Toc56782169)

[41. V2.10 サービス認証要件 42](#_Toc56782170)

[42. 追加の米国政府機関要件 43](#_Toc56782171)

[43. 用語集 43](#_Toc56782172)

[44. 参考情報 43](#_Toc56782173)

[V3: セッション管理の検証要件 45](#_Toc56782174)

[45. 管理目標 45](#_Toc56782175)

[46. セキュリティ検証要件 45](#_Toc56782176)

[47. V3.1 基本セッション管理要件 45](#_Toc56782177)

[48. V3.2 セッションバインディング要件 45](#_Toc56782178)

[49. V3.3 セッションログアウトおよびタイムアウト要件 46](#_Toc56782179)

[50. V3.4 クッキーベースのセッション管理 47](#_Toc56782180)

[51. V3.5 トークンベースのセッション管理 48](#_Toc56782181)

[52. V3.6 フェデレーションまたはアサーションからの再認証 48](#_Toc56782182)

[53. V3.7 セッション管理の悪用に対する防御 49](#_Toc56782183)

[54. 参考情報 50](#_Toc56782184)

[V4: アクセス制御検証要件 51](#_Toc56782185)

[55. 管理目標 51](#_Toc56782186)

[56. セキュリティ検証要件 51](#_Toc56782187)

[57. V4.1 一般的なアクセス制御デザイン 51](#_Toc56782188)

[58. V4.2 オペレーションレベルアクセス制御 52](#_Toc56782189)

[59. V4.3 他のアクセス制御の考慮 52](#_Toc56782190)

[60. 参考情報 52](#_Toc56782191)

[V5: バリデーション、無害化とエンコーディング検証要件 53](#_Toc56782192)

[61. 管理目標 53](#_Toc56782193)

[62. V5.1 入力バリデーション要件 53](#_Toc56782194)

[63. V5.2 無害化とサンドボックス化要件 55](#_Toc56782195)

[64. V5.3 出力エンコーディングとインジェクション防御の要件 56](#_Toc56782196)

[65. V5.4 メモリ、文字列、アンマネージドコードの要件 57](#_Toc56782197)

[66. V5.5 デシリアライゼーション防御の要件 58](#_Toc56782198)

[67. 参考情報 58](#_Toc56782199)

[V6: 保存時の暗号化の検証要件 60](#_Toc56782200)

[68. 管理目標 60](#_Toc56782201)

[69. V6.1 データ分類 60](#_Toc56782202)

[70. V6.2 アルゴリズム 60](#_Toc56782203)

[71. V6.3 乱数値 61](#_Toc56782204)

[72. V6.4 シークレット管理 62](#_Toc56782205)

[73. 参考情報 62](#_Toc56782206)

[V7: エラー処理およびログ記録の要件 63](#_Toc56782207)

[74. 管理目標 63](#_Toc56782208)

[75. V7.1 ログ内容の要件 63](#_Toc56782209)

[76. V7.2 ログ処理の要件 64](#_Toc56782210)

[77. V7.3 ログ保護の要件 65](#_Toc56782211)

[78. V7.4 エラー処理 65](#_Toc56782212)

[79. 参考情報 66](#_Toc56782213)

[V8: データ保護の要件 67](#_Toc56782214)

[80. 管理目標 67](#_Toc56782215)

[81. V8.1 一般的なデータ保護 67](#_Toc56782216)

[82. V8.2 クライアントサイドのデータ保護 68](#_Toc56782217)

[83. V8.3 機密性の高い個人データ 68](#_Toc56782218)

[84. 参考情報 70](#_Toc56782219)

[V9: 通信の検証要件 71](#_Toc56782220)

[85. 管理目標 71](#_Toc56782221)

[86. V9.1 通信のセキュリティ要件 71](#_Toc56782222)

[87. V9.2 サーバ通信のセキュリティ要件 72](#_Toc56782223)

[88. 参考情報 72](#_Toc56782224)

[V10: 悪性コードの検証要件 74](#_Toc56782225)

[89. 管理目標 74](#_Toc56782226)

[90. V10.1 コード整合性コントロール 74](#_Toc56782227)

[91. V10.2 悪意コード検索 74](#_Toc56782228)

[92. V10.3 デプロイ済アプリケーションの整合性コントロール 75](#_Toc56782229)

[93. 参考情報 76](#_Toc56782230)

[V11: ビジネスロジックの検証要件 77](#_Toc56782231)

[94. 管理目標 77](#_Toc56782232)

[95. V11.1 ビジネスロジックのセキュリティ要件 77](#_Toc56782233)

[96. 参考情報 78](#_Toc56782234)

[V12: ファイルとリソースの検証要件 79](#_Toc56782235)

[97. 管理目標 79](#_Toc56782236)

[98. V12.1 ファイルアップロード要件 79](#_Toc56782237)

[99. V12.2 ファイルの完全性の要件 79](#_Toc56782238)

[100. V12.3 ファイル実行の要件 80](#_Toc56782239)

[101. V12.4 ファイル保存の要件 80](#_Toc56782240)

[102. V12.5 ファイルダウンロードの要件 81](#_Toc56782241)

[103. V12.6 SSRF からの保護要件 81](#_Toc56782242)

[104. 参考情報 81](#_Toc56782243)

[V13: API、Web サービスの検証要件 82](#_Toc56782244)

[105. 管理目標 82](#_Toc56782245)

[106. V13.1 一般的な Web サービスセキュリティの検証要件 82](#_Toc56782246)

[107. V13.2 RESTful Web サービスの検証要件 83](#_Toc56782247)

[108. V13.3 SOAP Web サービスの検証要件 84](#_Toc56782248)

[109. V13.4 GraphQL や他の Web サービスデータレイヤのセキュリティ要件 84](#_Toc56782249)

[110. 参考情報 85](#_Toc56782250)

[V14: 構成の検証要件 86](#_Toc56782251)

[111. 管理目標 86](#_Toc56782252)

[112. V14.1 ビルド 86](#_Toc56782253)

[113. V14.2 依存関係 87](#_Toc56782254)

[114. V14.3 意図しないセキュリティの開示の要件 88](#_Toc56782255)

[115. V14.4 HTTP セキュリティヘッダの要件 89](#_Toc56782256)

[116. V14.5 HTTP リクエストヘッダのバリデーションの要件 89](#_Toc56782257)

[117. 参考情報 90](#_Toc56782258)

[Appendix A: 用語集 91](#_Toc56782259)

[Appendix B: 参考情報 95](#_Toc56782260)

[118. OWASP 主要プロジェクト 95](#_Toc56782261)

[119. Mobile Security Related Projects 95](#_Toc56782262)

[123. OWASP Internet of Things related projects 95](#_Toc56782263)

[124. OWASP Serverless projects 95](#_Toc56782264)

[125. Others 95](#_Toc56782265)

[Appendix C: IoT 検証要件 97](#_Toc56782266)

[126. 管理目標 97](#_Toc56782267)

[127. セキュリティ検証要件 97](#_Toc56782268)

[128. 参考情報 100](#_Toc56782269)

口絵

1. 本標準について

OWASP アプリケーションセキュリティ検証標準はアーキテクト、開発者、テスター、セキュリティ専門家、ツールベンダ、アプリケーション利用者がセキュアなアプリケーションの定義、ビルド、テスト、検証に使用できるアプリケーションセキュリティ要件またはテストのリストです。

1. 著作権とライセンス

Version 4.0.1, March 2019

|  |  |
| --- | --- |
| license | Copyright © 2008-2019 The OWASP Foundation. 本書は Creative  Commons Attribution ShareAlike 3.0 license に基づいてリリースされています。再利用または配布する場合には、他者に対して本著作物のライセンス  条項を明らかにする必要があります。 |

1. プロジェクトリーダー

* Andrew van der Stock
* Daniel Cuthbert
* Jim Manico

1. 執筆者およびレビュー担当者

* Josh C Grossman
* Mark Burnett
* Osama Elnaggar
* Erlend Oftedal
* Serg Belkommen
* David Johansson
* Tonimir Kisasondi
* Ron Perris
* Jason Axley
* Abhay Bhargav
* Benedikt Bauer
* Elar Lang
* ScriptingXSS
* Philippe De Ryck
* Grog's Axle
* Marco Schnüriger
* Jacob Salassi
* Glenn ten Cate
* Anthony Weems
* bschach
* javixeneize
* Dan Cornell
* hello7s
* Lewis Ardern
* Jim Newman
* Stuart Gunter
* Geoff Baskwill
* Talargoni
* Ståle Pettersen
* Kelby Ludwig
* Jason Morrow
* Rogan Dawes

アプリケーションセキュリティ検証標準は 2008 年の ASVS 1.0 から 2016 年の 3.0 に至る関係者の責任の下で作成されています。今日の ASVS にまだ残っている構成と検証項目の多くはもともと MikeBoberski, Jeff Williams, Dave Wichers によって書かれましたが、もっと多くの執筆者がいます。以前に関わりのあったすべての人々に感謝します。以前のバージョンに貢献したすべての人の包括的なリストについては、以前の各バージョンを確認してください。

クレジットが上記のクレジットリストにない場合は、 [vanderaj@owasp.org](mailto:vanderaj@owasp.org) に連絡するか、将来の 4.x

アップデートで認識されるように GitHub のチケットを記録してください。

序文

アプリケーションセキュリティ検証標準 (ASVS) バージョン 4.0 へようこそ。ASVS は現代の Web アプリケーションおよび Web サービスを設計、開発、テストする際に必要となる、機能的および非機能的なセキュリティ管理策の定義に焦点を当てた、セキュリティ要件および管理策のフレームワークを確立するコミュニティ主導の取り組みです。

ASVS v4.0 は長年にわたるコミュニティの取り組みと業界のフィードバックの集大成です。セキュアなソフトウェア開発ライフサイクルを通して、さまざまなユースケースに ASVS をより簡単に採用できるようにしました。

ASVS を含むあらゆる Web アプリケーション標準の内容に 100% 合意できるとは考えていません。リスク分析は常にある程度主観的なものであり、さまざまな場面に対応する規格で一般化しようとすることは困難が伴います。しかし、このバージョンで行われた最新の更新が正しい方向への一歩であり、この重要な業界標準に導入されたコンセプトの強化を願っています。

1. 4.0 の更新内容

このバージョンでの最も重要な変更は NIST 800-63-3 デジタルアイデンティティガイドラインの導入であり、最新で、エビデンスをベースとする、高度な認証管理を紹介しています。高度な認証規格との整合については多少の相違が考えられますが、主に他のよく知られているアプリケーションセキュリティ標準規格がエビデンスベースの場合には、標準規格との調整が不可欠と考えています。

準拠する組織が競合する管理策や相反する管理策を決定する必要がないように、情報セキュリティ標準は固有の要件の数を最小限に抑えるように努めるべきです。OWASP Top 10 2017 と現在の OWASP アプリケーションセキュリティ検証標準は認証とセッション管理に関して NIST 800-63 に準拠しています。セキュリティを最大化しコンプライアンスコストを最小化するために、他の標準化団体が私たち、NIST、および他の人たちと協力して、一般に認められている一連のアプリケーションセキュリティ管理策に取り組むことを歓迎します。

ASVS 4.0 は最初から最後まで全面的に番号が付け替えられました。新しい採番スキームにより長期間消えていた章からのギャップを埋めることができ、開発者やチームが順守しなければならない管理策の数を最小限に抑えるために長い章をセグメント化できました。たとえば、アプリケーションが JWT を使用しない場合、セッション管理における JWT のセクション全体が適用されません。

4.0 での新規項目は、近年長期にわたり最もよく求められていた機能要求のひとつです、Common Weakness Enumeration (CWE) への包括的なマッピングです。CWE マッピングにより、ツール開発業者と脆弱性管理ソフトウェアを使用しているユーザは、他のツールおよび以前の ASVS バージョンの結果を 4.0 およびそれ以降に一致させることができます。CWE エントリのためのスペースを確保するために、「導入バージョン」列を廃止しなければなりませんでした。「導入バージョン」列は完全に番号を付け替えたため、以前のバージョンの ASVS のものより意味がありません。ASVS のすべての項目に関連する CWE があるわけではありませんし、CWE には多くの重複があるため、必ずしも近いものではなく最も一般的に使用されているものを使用しようとしています。検証管理は常に同等の脆弱性にマップできるわけではありません。私たちはこのギャップをより一般的なものに埋めることに関して CWE コミュニティおよび情報セキュリティ分野との継続的な議論を歓迎します。

私たちは OWASP Top 10 2017 および OWASP Proactive Controls 2018 に対応する要件を包括的に満たし、上回るように努めてきました。OWASP Top 10 2017 は過失を回避するための最低限のもののた

め、特定のログ記録を除き意図的にすべての Top 10 要件をレベル 1 管理策とし、OWASP Top 10 の採用者が具体的なセキュリティ標準に容易にステップアップできるようにしています。

ASVS 4.0 レベル 1 は、アプリケーション設計、コーディング、テスト、セキュアコードレビュー、ペネトレーションテストのための PCI DSS 3.2.1 セクション 6.5 の包括的なスーパーセットであることを確認することに着手しました。これには、既存の業界をリードするアプリケーションおよび Web サービスの検証要件に加えて、V5 ではバッファオーバーフローと危険なメモリ操作、V14 では危険なメモリ関連のコンパイラフラグを含める必要がありました。

ASVS はモノリシックなサーバサイドのみの管理策から、現代のすべてのアプリケーションおよび API に対するセキュリティ管理策を提供することへの移行を完了しました。関数型プログラミング、サーバレス API 、モバイル、クラウド、コンテナ、CI/CD および DevSecOps 、フェデレーションなどの時代には、現代のアプリケーションアーキテクチャを無視し続けることはできません。現代のアプリケーションはオリジナルの ASVS が 2009 年にリリースされたときに構築されたものとは全く異なるように設計されています。私たちの主要なオーディエンスである開発者に適切なアドバイスを提供するために、ASVS は常に遠い将来を見据えたものでなければなりません。アプリケーションが単一の組織により所有されているシステム上で実行されることを前提としている要件を明確化または廃止しました。

ASVS 4.0 のサイズ、および他のすべての ASVS の取り組みのためのベースライン ASVS になりたいという私たちの願いのために、OWASP モバイルアプリケーションセキュリティ検証標準(MASVS) に賛同

し、モバイルの章を削除しました。Internet of Things の付録は OWASP Internet of Things Project のもとで将来 IoT ASVS として現れるでしょう。付録 C に IoT ASVS の早期プレビューがあります。これらの

ASVS をサポートしてくれた OWASP Mobile Team と OWASP IoT Project Team の双方に感謝し、将来彼らが補完的な標準を提供することを楽しみにしています。

最後に、影響の少ない管理策を重複削減および廃止しました。時間とともに、ASVS は包括的な管理策のセットになり始めましたが、すべての管理策がセキュアなソフトウェアを生み出すうえで同等というわけではありません。影響の少ない項目を排除するこの取り組みはさらに進むかもしれません。ASVS の将来のエディションでは、Common Vulnerability Scoring System (CVSS) が真に重要な管理策と廃止すべき管理策の優先順位付けに役立つでしょう。

バージョン 4.0 では、ASVS は従来および現在のアプリケーションアーキテクチャ、アジャイルセキュリティプラクティス、DevSecOps カルチャーをカバーする、主要な Web アプリおよびサービス標準であることにのみフォーカスしています。

ASVS の使い方

ASVS には主な目標が 2 つあります。

* 組織がセキュアなアプリケーションを開発および保守するのに役立つこと。
* セキュリティサービスベンダ、セキュリティツールベンダ、および利用者が、各々の要件とプロダクトを調整できるようにすること。

1. アプリケーションセキュリティ検証レベル

アプリケーションセキュリティ検証標準では 3 つのセキュリティ検証レベルを定義しており、レベルごとに深くなっていきます。

* ASVS レベル 1 は低保証レベル向けであり、すべてがペネトレーションテスト可能です。
* ASVS レベル 2 は機密データを含むアプリケーション向けであり、保護を必要とし、ほとんどのアプリに推奨されるレベルです。
* ASVS レベル 3 は極めて重要なアプリケーション向けであり、高額取引を行うアプリケーション、機密性の高い医療データを持つアプリケーション、最高レベルの信頼性を必要とするアプリケーションのためのものです。

各 ASVS レベルはセキュリティ要件のリストを含みます。これらの各要件はセキュリティ固有の機能や開発者がソフトウェアに組み込む必要のある機能にもマップできます。

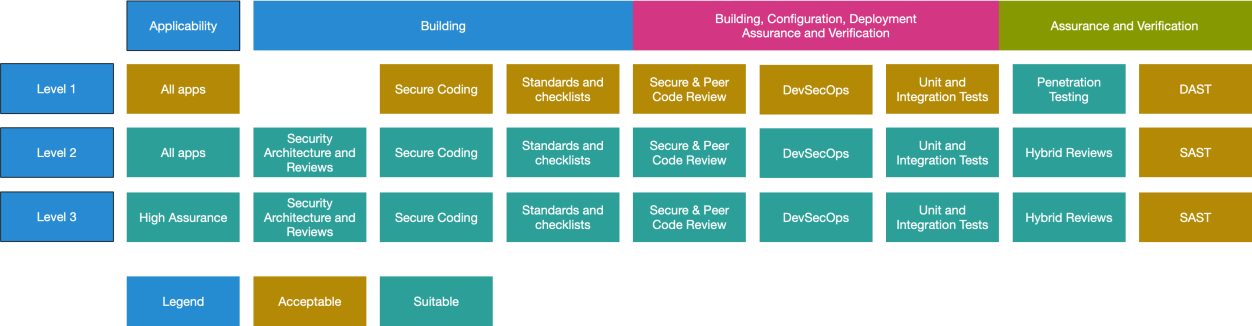


図 1 - OWASP アプリケーションセキュリティ検証標準 4.0 レベル

レベル 1 は人間によりすべてがペネトレーションテスト可能な唯一のレベルです。それ以外のものはすべてドキュメント、ソースコード、設定、開発プロセスに携わる人々へのアクセスを必要とします。但し、たとえレベル 1 が「ブラックボックス」 (ドキュメントなし、ソースなし) テストを行うことができたとしても、それは有効な保証活動ではなく積極的に阻止すべきです。悪意のある攻撃者にはかなりの時間があり、ほとんどのペネトレーションテストは数週間以内に終了します。防御する者はセキュリティ管理策を組み入れ、すべての弱点を保護、発見、解決し、悪意のある行為を行う者を妥当な時間内に検出および対応する必要があります。悪意のある行為を行う者は本質的に無限の時間があり、成功するためにはひとつの侵入しやすい防御、ひとつの弱点、または見逃した検出のみで足ります。ブラックボックステストは開発の最後に行われることが多く、あわただしく行われるか、全く行われず、このような不均衡に完全に対処することはできません。

過去 30 年以上にわたり、ブラックボックステストはさらに深刻な侵害に直接つながる重大なセキュリティ問題を見逃していることが何度も繰り返し証明されてきました。開発プロセス全体を通して開発者とドキュメントへのフルアクセスを伴い、レベル 1 でのペネトレーションテストをソースコード主導 (ハイブリッド) ペネトレーションテストに置き換えるなど、幅広いセキュリティ保証と検証の使用を強く推奨します。金融規制当局は財務記録、サンプル取引、管理を実行する人々にアクセスできない外部の財務監査を認めません。産業界および政府機関はソフトウェア工学の領域で同じ標準の透明性を要求しなければなりません。

開発プロセス自体の中でセキュリティツールを使用することを強く推奨します。DAST および SAST ツールはビルドパイプラインで継続的に使用して、存在してはならないセキュリティ問題を簡単に見つけることができます。

自動ツールとオンラインスキャンは人間による支援なしでは ASVS の半分以上を完了することができません。ビルドごとに包括的なテスト自動化が必要な場合には、カスタムの単体テストと統合テストの組み合わせをビルド開始時のオンラインスキャンとともに使用します。ビジネスロジックの欠陥とアクセ

ス制御のテストは人間による支援でのみ可能です。これらは単体テストと統合テストに変えるべきです。

1. この標準の使い方

アプリケーションセキュリティ検証標準を使用する最善の方法の 1 つは、アプリケーション、プラットフォーム、組織に固有のセキュアコーディングチェックリストを作成するための青写真として使用することです。ユースケースに合わせて ASVS を仕立て直すことで、プロジェクトや環境にとって最も重要なセキュリティ要件に焦点を当てるでしょう。

レベル 1 - ファーストステップ、自動化、ポートフォリオビュー全体

検出が容易で、OWASP Top 10 や他の同様のチェックリストに含まれているアプリケーションセキュリティ脆弱性に対して適切に防御されていれば、アプリケーションは ASVS レベル 1 を達成します。

レベル 1 はすべてのアプリケーションが目指すべき必要最低限のレベルです。複数フェーズの作業での

最初のステップとして、またはアプリケーションが機密データを格納や処理しないためレベル 2 や 3 の

より厳しい管理策を必要としない場合にも役立ちます。レベル 1 管理策はツールにより自動的にチェックすることも、ソースコードにアクセスすることなく手動でチェックすることもできます。私たちはレベル 1 をすべてのアプリケーションに最低限必要なものと考えています。

アプリケーションに対する脅威は、発見が容易で悪用が容易な脆弱性を特定するために簡単で手間のかからない技法を使用している攻撃者からのものがほとんどです。これはアプリケーションを明確にターゲットとすることに集中的にエネルギーを費やす、確固たる攻撃者とは対照的です。アプリケーションにより処理されたデータが高い価値を持つ場合には、レベル 1 レビューで止めたくないでしょう。

レベル 2 - 大半のアプリケーション

今日のソフトウェアに関連するリスクのほとんどを適切に防御できれば、アプリケーションは ASVS レベル 2 (または Standard) を達成します。

レベル 2 ではセキュリティ管理策が適用され、効果的であり、アプリケーション内で使用されていることを確認します。ヘルスケア情報の処理、ビジネスに不可欠なまたは機密性の高い機能の実装、他の機密性の高い資産の処理などを含む、重要な企業間取引を処理するアプリケーションや、チートやゲームハックを阻止するゲーム業界などの、ビジネスを保護するために完全性が重要な要素となる業界に対して、通常、レベル 2 が適用されます。

レベル 2 アプリケーションの脅威は、通常、アプリケーション内の弱点を発見および悪用するために高度に実践され効果的なツールや技法を用いて特定のターゲットに集中する、熟練した動機のある攻撃者です。

レベル 3 - 高い価値、高い保証、高い安全性

ASVS レベル 3 は ASVS 内での最高レベルの検証です。このレベルは通常、軍事、安全衛生、重要インフラなどの分野で見られるような、重大なレベルのセキュリティ検証を必要とするアプリケーション向けに予定されています。

故障が組織の業務に、またその存続可能性にさえ大きく影響する可能性のある、重要な機能を実行するアプリケーションに対して、組織は ASVS レベル 3 を要求する可能性があります。ASVS レベル 3 のアプリケーションに関するガイダンスの例を以下に示します。高度なアプリケーションセキュリティ脆弱性に対して適切に防御し、優れたセキュリティ設計の原則を実証している場合、そのアプリケーションは ASVS レベル 3 (または Advanced) を達成します。

ASVS レベル 3 のアプリケーションは他のすべてのレベルよりもアーキテクチャ、コーディング、テストの詳細な分析を必要とします。セキュアなアプリケーションは (耐性、スケーラビリティ、そして何よりもセキュリティの層を促進するために) 意味のある方法でモジュール化され、各モジュール (ネットワーク接続や物理インスタンスで分離されている) はそれ自身のセキュリティ責任 (多層防御) を管理し、適切に文書化される必要があります。責任には機密性 (暗号化など) 、完全性 (トランザクション、入力検証など) 、可用性 (負荷の適切な処理など) 、認証 (システム間を含む) 、否認防止、認可、監査 (ログ記録) を確保するための管理策が含まれます。

1. 実際にASVS を適用する

脅威が異なれば動機も異なります。一部の業界では独自の情報資産と技術資産があり、ドメイン固有の規制順守要件があります。

組織はそのビジネスの性質に基づく独自のリスク特性を詳細に検討し、そのリスクとビジネス要件に基づいて適切な ASVS レベルを決定することを強く推奨します。

監査と認証

1. ASVS 認証と認証マークに対する OWASP の見解

OWASP はベンダ中立の非営利組織であり、現在、ベンダ、検証者、ソフトウェアの認証は行っていません。

そのような保証の表明、認証マーク、認証はいずれも OWASP によって公式に検査、登録、認証されたものではありません。そのような見解に依存している組織は ASVS 認証を主張する第三者や認証マークについて、その信頼性に注意する必要があります。

これは、OWASP の公式な認証であると主張しない限り、組織がこのような保証サービスを提供することを妨げるものではありません。

1. 認証機関のためのガイダンス

アプリケーションセキュリティ検証標準はアプリケーションの検証内容が明確化された検証として利用できます。特にレベル 2 とレベル 3 の検証には、設計者や開発者、プロジェクト文書、ソースコード、(役割ごとにひとつ以上のアカウントへのアクセスを含む) テストシステムへの認証されたアクセスといった、主要リソースへのオープンで自由なアクセスを含みます。

歴史上、ペネトレーションテストとソースコードレビューは「例外による」問題を含んでいました。つまり、不合格のテストのみが最終レポートに示されます。認証機関は (特に SSO 認証などの主要コンポーネントがスコープ外の場合) 検証のスコープ、合格および不合格のテストを含む検証結果の要約、不合格のテストへの解決法の明確な指示をレポートに含める必要があります。

特定の検証要件はテスト中のアプリケーションに適用されない場合があります。例えば、クライアント実装なしで顧客にステートレスサービス層 API を提供する場合、V3 セッション管理の要件の多くは直接適用されません。そのような場合、認証機関は依然として ASVS の完全な順守を主張することができますが、そのような除外された検証要件が適用されない理由を明確にレポートに示さなければなりませ

ん。

詳細な調書、スクリーンショットやムービー、問題を確実かつ繰り返し利用するためのスクリプト、傍受したプロキシログなどのテストの電子記録、クリーンアップリストなどの関連メモを保持することは標準的な業界の慣行と考えられます。そして、最も疑わしい開発者の発見の証拠として本当に役に立ちます。単にツールを実行して不合格を報告するだけでは十分ではありません。認証レベルのすべての問題がテストされ、余すところなくテストされている十分な証跡を (まったく) 提供していません。異議申

し立てがあった場合に備えて、それぞれすべての検証要件が実際にテストされたことを実証するのに十分な証跡が必要となります。

テスト手法

認証機関は適切なテスト手法を自由に選択できますが、レポートに記載する必要があります。

テスト対象のアプリケーションと検証要件に応じて、結果に均一な信頼性を得るためにさまざまなテスト手法を使用できます。例えば、アプリケーションの入力検証メカニズムの有効性を妥当性確認するには、手動ペネトレーションテストで分析するかソースコード解析を用います。

*自動セキュリティテストツールの役割*

自動ペネトレーションテストツールの使用は、できるだけ多くの範囲をカバーするために推奨されています。

自動ペネトレーションテストツールだけを使用して ASVS 検証を完全に完了することはできません。レベル 1 の要件の大部分は自動テストを使用して実行できますが、要件全体の大半は自動ペネトレーションテストには適していません。

アプリケーションセキュリティ業界が成熟するにつれて、自動テストと手動テストの境界があいまいになっていることに注意してください。自動ツールは専門家により手動で調整されることが多く、手動テスト担当者はさまざまな自動テストツールを活用することがよくあります。

*ペネトレーションテストの役割*

バージョン 4.0 では、ソースコード、ドキュメント、開発者にアクセスすることなく レベル 1 を完全に

ペネトレーションテストできるようにしました。OWASP Top 10 2017 A10 に準拠するための必要な二

つのログ記録の項目は、OWASP Top 10 2017 の場合と同様に、インタビュー、スクリーンショット、その他の証跡収集が必要になります。しかし、必要な情報にアクセスせずにテストすることは、ソースのレビュー、脅威の特定、管理策の欠如、そしてより短期間での十分なテスト実行の可能性を見逃すため、セキュリティ検証の理想的な方法ではありません。

可能であれば、開発者、ドキュメント、コードへのアクセス、および本番用ではないデータでのテストアプリケーションへのアクセスが、レベル 2 またはレベル 3 アセスメントを実行する際に必要です。これらのレベルで行われるペネトレーションテストには、「ハイブリッドレビュー」や「ハイブリッドペネトレーションテスト」と呼ぶ、このレベルのアクセスが必要です。

1. ASVS のその他の用途

アプリケーションのセキュリティを評価するために使用される以外に、ASVS のその他の潜在的な用途がいくつか考えられています。

詳細なセキュリティアーキテクチャガイダンスとして

アプリケーションセキュリティ検証標準のより一般的な用途のひとつはセキュリティアーキテクトのためのリソースです。Sherwood Applied Business Security Architecture (SABSA) にはアプリケーションセキュリティアーキテクチャの十分なレビューを完了するための必要な多くの情報が欠けています。ASVS を使用して、セキュリティアーキテクトがデータ保護パターンや、入力バリデーション戦略などの一般的な問題に対してより適切な管理策を選択できるようにすることで、これらのギャップを埋めることができます。

画一的なセキュアコーディングチェックリストの代わりとして

多くの組織は ASVS を採用することでメリットがあります。3 つのレベルのいずれかを選択するか、ASVS をフォークし、各アプリケーションのリスクレベルに必要なものをドメイン固有の方法で変更します。トレーサビリティが維持されている限りこのタイプのフォークをお勧めします。アプリが要件 4.1 をパスした場合、これはフォークされたコピーについても標準としてそれが進化したものとして同じことを意味します。

自動ユニットテストおよび自動統合テストのガイドとして

多くの組織は ASVS を採用することでメリットがあります。3 つのレベルのいずれかを選択するか、ASVS をフォークし、各アプリケーションのリスクレベルに必要なものをドメイン固有の方法で変更します。トレーサビリティが維持されている限りこのタイプのフォークをお勧めします。アプリが要件 4.1 をパスした場合、これはフォークされたコピーについても標準としてそれが進化したものとして同じことを意味します。

セキュア開発トレーニングのために

ASVS はセキュアソフトウェアの特性を定義するためにも使用できます。多くの「セキュアコーディング」コースはコーディングのヒントがわずかにあるだけの単なるエシカルハッキングコースです。これは開発者がよりセキュアなコードを書くのに必ずしも役に立つとは限りません。代わりに、セキュア開発コースでは、してはいけないことの Top 10 ネガティブ項目ではなく、ASVS にある予防的管理策に重点を置いて ASVS を使用できます。

アジャイルアプリケーションセキュリティの牽引役として

ASVS は、セキュアな製品を開発するためにチームが実装する必要がある特定のタスクを定義するためのフレームワークとして、アジャイル開発プロセスで使用できます。ひとつのアプローチとして、レベル 1 から始めて、指定されたレベルの ASVS 要件に従い特定のアプリケーションやシステムを検証し、どの管理策が欠けているかを見つけ、バックログに特定のチケットやタスクを上げます。これは特定のタスクの優先度付け (または調整) に役立ち、アジャイルプロセスでセキュリティを可視化します。これはまた、特定の ASVS 要件が特定のチームメンバーのレビュー、リファクタリング、監査の牽引役とな

り、バックログでいずれ行う必要がある「負債」として可視化され、組織内の監査タスクおよびレビュータスクの優先度付けにも使用できます。

セキュアなソフトウェアの調達をガイドするためのフレームワークとして

ASVS は、セキュアなソフトウェアの調達やカスタム開発サービスの調達を支援する優れたフレームワークです。調達者は単に入手したいソフトウェアを ASVS レベル X で開発しなければならないという要件を設定し、そのソフトウェアが ASVS レベル X を満たすことを販売者に証明するよう要求できます。これは OWASP Secure Software Contract Annex と組み合わせると効果的です。

V1: アーキテクチャ、設計、脅威モデリング要件

1. 管理目標

セキュリティアーキテクチャは多くの組織で失われた技術となっています。エンタープライズアーキテクトの時代は DevSecOps で過去のものとなりました。アプリケーションセキュリティの分野では、最新のセキュリティアーキテクチャの原則をソフトウェア実務者に再導入しながら、アジャイルセキュリティの原則をキャッチアップし採用する必要があります。アーキテクチャは実装ではなく、潜在的に多くの異なる答えがある可能性があり、唯一の「正しい」答えがない問題について考える方法です。多くの場合、開発者がその問題を解決するはるかに優れた方法を知っている可能性がある場合には、セキュリティは柔軟性がなく、開発者が特定の方法でコードを修正することを要求するものとみなされます。アーキテクチャに対して唯一で単純な解決策はありません。そして、そうではないフリをすることはソフトウェアエンジニアリング分野への害となります。

Web アプリケーションの特定の実装はそのライフタイムを通じて継続的に改訂される可能性がありますが、全体的なアーキテクチャはほとんど変更されず、ゆっくりと進化します。セキュリティアーキテクチャも同様です。私たちは今日認証が必要ですし、明日も認証が必要でしょうし、五年後にも必要でしょう。今日、妥当な判断を下して、アーキテクチャに準拠したソリューションを選択して再利用すれ

ば、多くの労力、時間、費用を節約できます。例えば、一昔前には、多要素認証はほとんど実装されていませんでした。

開発者が SAML フェデレーションアイデンティティなどの単一のセキュアなアイデンティティプロバイダモデルに注力した場合、元のアプリケーションのインタフェースを変更することなく、NIST 800-63 コンプライアンスなどの新しい要件を組み込むためにそのアイデンティティプロバイダを更新できることでしょう。多くのアプリケーションが同じセキュリティアーキテクチャ、つまり同じコンポーネントを共有している場合、すべてのアプリケーションが同時にこのアップグレードの利を得られます。但し、SAML は常に最良ないし最適な認証ソリューションとして残るわけではありません。要件変更に応じて他のソリューションと交換する必要があるかもしれません。このような変更は互いに入り組んでおり、完全な書き直しが必要になるほどコストがかかるか、セキュリティアーキテクチャなしではまったく不可能となります。

本章では、ASVS は妥当なセキュリティアーキテクチャの主要な側面である可用性、機密性、処理の完全性、否認防止、プライバシーをカバーしています。これらの各セキュリティ原則はすべてのアプリケーションに組み込まれ、本質的に備わったものでなければなりません。「シフトレフト」が重要です。セ

キュアコーディングチェックリスト、メンタリングとトレーニング、コーディングとテスティング、構築、展開、構成、運用で開発者の強化を開始します。そして、すべてのセキュリティ管理策が存在し機能していることを保証するために、フォローアップの独立テストで終了します。かつては業界として私たちが行うすべての作業が最後のステップでしたが、開発者が一日に数十回または数百回コードをプロダクションにプッシュするようになると、それだけでは不十分です。アプリケーションセキュリティの専門家はアジャイル技法に遅れずついていく必要があります。つまり、開発者ツールを採用し、コードを学び、開発者と協力することを意味します。他の全員が異動してから何か月も後にプロジェクトを批判するのではありません。

1. V1.1 セキュアソフトウェア開発ライフサイクル要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.1.1** | 開発すべての段階でセキュアソフトウェア開発ライフサイクルを用いている。 ([C1](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ |  |
| **1.1.2** | 脅威を特定し、対策を計画し、適切なリスク対応を促進し、セキュリティテストを進めるため、すべての設計変更またはスプリントプランニングに対する脅威モデリングが用いている。 |  | ✓ | ✓ | 1053 |
| **1.1.3** | すべてのユーザストーリーおよび機能に、「ユーザが、自分のプロフィールを表示および編集できるようにする。他のユーザのプロフィールを表示または編集するができない」などのセキュリティ上の制限機能が含まれる。 |  | ✓ | ✓ | 1110 |
| **1.1.4** | すべてのアプリケーションの信頼境界線、コンポーネントおよび重要なデータフローの文書化と正当性がある。 |  | ✓ | ✓ | 1059 |
| **1.1.5** | アプリケーションの高レベルアーキテクチャおよびすべてのリモート接続サービスの定義とセキュリティ分析がなされている。 ([C1](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 1059 |
| **1.1.6** | 重複や欠落がある、非効果的な、もしくはセキュアでない管理策を回避するために、集中管理され簡潔（エコデザイン）で徹底調査され、セキュアで、再利用可能なセキュリティ管理策が実装されている。 ([C10](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 637 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.1.7** | セキュアコーディングチェックリスト、セキュリティ要件、ガイドラインまたはポリシーを、すべての開発者およびテスターが利用可能。 |  | ✓ | ✓ | 637 |

1. V1.2 認証アーキテクチャ要件

認証を設計する際、攻撃者がコールセンターを呼び出して一般的に知らせている質問に答えることでアカウントをリセットできる場合、強力なハードウェア対応の多要素認証があるかどうかは問題なりません。身元を証明するときは、すべての認証経路が同じ強度を持つ必要があります。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.2.1** | すべてのアプリケーションコンポーネント、サービスおよびサーバに対して一意の、または特別な低特権の OS アカウントが使用されている。([C3](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 250 |
| **1.2.2** | API、ミドルウェア、データ層などのアプリケーションコンポーネント間の通信が認証されている。 コンポーネントには必要最小限の権限が設定されている。([C3](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 306 |
| **1.2.3** | セキュアであることが知られており、強力な認証を含むよう拡張できる単一で徹底調査された認証機構をアプリケーションが使用しているこ と、アカウントの悪用や侵害を検出するのに十分なログ記録と監視をアプリケーション実装している。 |  | ✓ | ✓ | 306 |
| **1.2.4** | アプリケーションのリスクごとに、弱い代替の認証が存在しないよう  に、すべての認証経路と ID 管理 API が一貫した認証セキュリティ制御強  実装している。 |  | ✓ | ✓ | 306 |

1. V1.3 セッション管理アーキテクチャ要件

これは将来のアーキテクチャ要件のためのプレースホルダです。

1. V1.4 アクセス制御アーキテクチャ要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.4.1** | アクセス制御ゲートウェイ、サーバ、サーバレス機能などの信頼できる強制ポイントでアクセス制御が実施されている。クライアント上でアクセス制御を実施してはなりません。 |  | ✓ | ✓ | 602 |
| **1.4.2** | 選択したアクセス制御ソリューションがアプリケーションのニーズを満たすのに十分柔軟性がある。 |  | ✓ | ✓ | 284 |
| **1.4.3** | 機能、データファイル、URL、コントローラ、サービス、およびその他のリソースにおける最小特権の原則が実施されている。これにより、なりすましや特権昇格に対する保護が可能となります。 |  | ✓ | ✓ | 272 |
| **1.4.4** | 保護されたデータやリソースにアクセスするために、アプリケーションが 1 つの十分に検証されたアクセス制御機構を使用している。コピー& ペーストまたは安全でない代替パスを回避するため、すべてのリクエストがこの単一の機構をパスする必要があります。 ([C7](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 284 |
| **1.4.5** | 属性または機能ベースのアクセス制御が使用されており、コードは単にユーザのロールではなくむしろ、機能/データ項目に対するユーザの権限を確認します。それでも、権限はロールを利用して割り当てる必要があ  ります。 ([C7](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 275 |

1. V1.5 入力および出力アーキテクチャ要件

4.0 では、意味のある信頼境界線の用語として「サーバサイド」という用語をなくしました。信頼境界線は依然として重要です。信頼できないブラウザやクライアントデバイスでの決定はバイパス可能です。しかし、今日の主流のアーキテクチャ展開では、信頼の実行点が劇的に変わりました。したがって、ASVS で「信頼できるサービスレイヤ」という用語が使用されている場合、マイクロサービス、サーバレス API、サーバサイド、セキュアブートを備えたクライアントデバイス上の信頼された API、パートナーAPI や外部 API など、場所に関係なく、信頼された実行点を意味します。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1.5.1** | 入出力要件が、データの種類や内容および適用法、規制、その他のポリシー準拠に基づいて、取り扱い手順を明確に定義している。 | ✓ | ✓ | 1029 |
| **1.5.2** | 信頼できないクライアントと通信するときにシリアライゼーションが使用されていない。これが不可能な場合は、オブジェクトインジェクションを含むデシリアライゼーション攻撃を防ぐために、適切な完全性制御  （および機密データが送信される場合はできる限り暗号化）を実施する。 | ✓ | ✓ | 502 |
| **1.5.3** | 信頼できるサービスレイヤで入力の妥当性確認が実施されている。 ([C5](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | 602 |
| **1.5.4** | アウトプットエンコーディングが意図されているインタプリタもしくはその近くで生成される。([C4](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | 116 |

1. V1.6 暗号アーキテクチャ要件

アプリケーションは分類に従ってデータ資産を保護するために、強力な暗号化アーキテクチャで設計する必要があります。すべてを暗号化することは無駄であり、なにも暗号化しないことは法的な過失となります。通常、アーキテクチャ設計や高レベル設計、デザインスプリントやアーキテクチャスパイクの際に、バランスをとる必要があります。暗号を自ら設計したり追加導入したりすることは、最初から単純に組み込むよりも、セキュアに実装するために必然的により多くのコストがかかります。

アーキテクチャ要件はコードベース全体に内在するため、単体テストや統合テストは困難です。アーキテクチャ要件はコーディングフェーズを通じてコーディング標準を考慮する必要があり、セキュリティアーキテクチャ、ピアレビューやコードレビュー、振り返りの際にレビューする必要があります。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.6.1** | 暗号鍵の管理に関する明示的なポリシーがあり、暗号鍵のライフサイクルが NIST SP 800-57 などの鍵管理標準に従っている。 |  | ✓ | ✓ | 320 |
| **1.6.2** | 暗号化サービスの利用者が、Key Vault または API ベースの代替手段を使用して、キーマテリアルおよびその他の秘密情報を保護している。 |  | ✓ | ✓ | 320 |
| **1.6.3** | すべての鍵とパスワードが置き換え可能であり、機密データを再暗号化するため明確に定義されたプロセスの一部となっている。 |  | ✓ | ✓ | 320 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.6.4** | クライアントによって生成されたまたはクライアントと共有された対称鍵やパスワードまたは API 秘密情報が、ローカルストレージの暗号化などの低リスクの秘密情報の保護、またはパラメータ難読化などの一時的な用途にのみ使用される。クライアントと秘密情報を共有することは、平文と同等であり、アーキテクチャ的にはそのように扱われる必要があ  ります。 |  | ✓ | ✓ | 320 |

1. V1.7 エラー、ロギング、監査アーキテクチャ要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.7.1** | システム全体で共通のログ形式とアプローチが使用されている。 ([C9](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 1009 |
| **1.7.2** | 分析、検出、警告、およびエスカレーションのために、できればリモートシステムにログがセキュアに送信されている。 ([C9](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ |  |

1. V1.8 データ保護とプライバシーアーキテクチャ要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.8.1** | すべての機密データが識別され、保護レベルごとに分類されている。 |  | ✓ | ✓ |  |
| **1.8.2** | 暗号化要件、完全性要件、保存期間、プライバシー、その他の機密保持要件などの関連する保護要件一式がすべての保護レベルにあり、それらがアーキテクチャに適用されている。 |  | ✓ | ✓ |  |

1. V1.9 通信アーキテクチャ要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.9.1** | 特にコンポーネントが異なるコンテナ、システム、サイトまたはクラウドプロバイダにある場合は、アプリケーションがコンポーネント間の通信を暗号化している。 ([C3](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 319 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1.9.2** | 中間者攻撃を防ぐために、アプリケーションコンポーネントが通信リンクの両側の信頼性を検証している。例えば、アプリケーションコンポー  ネントは TLS 証明書とチェーンを検証する必要があります。 | ✓ | ✓ | 295 |

1. V1.10 悪意あるソフトウェアのアーキテクチャ要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.10.1** | チェックインが、イシューや変更チケットによることを保証するため、手続きを定めてソースコード管理システムが利用されている。ソースコード管理システムは、アクセス制御と識別可能なユーザのみ登録され、  どんな変更もトレースできるようにする必要がある。 |  | ✓ | ✓ | 284 |

1. V1.11 ビジネスロジックアーキテクチャ要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.11.1** | 提供するビジネスまたはセキュリティ機能の観点で、すべてのアプリケーションコンポーネントの定義と文書化がされている。 |  | ✓ | ✓ | 1059 |
| **1.11.2** | 認証、セッション管理、アクセス制御を含むすべての重要なビジネスロジックフローが非同期状態で共有しない。 |  | ✓ | ✓ | 362 |
| **1.11.3** | 認証、セッション管理、アクセス制御などを含む重要度の高いすべてのビジネスロジックフローがスレッドセーフであり、チェック時間  （TOC）や使用時間（TOU）の競合状態に対して耐性がある。 |  |  | ✓ | 367 |

1. V1.12 セキュアファイルアップロードアーキテクチャ要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.12.1** | ユーザがアップロードしたファイルが Web ルートの外部に保存される。 |  | ✓ | ✓ | 552 |
| **1.12.2** | ユーザがアップロードしたファイル（表示またはアプリケーションからダウンロードする必要がある場合）が、オクテットストリームによるダウンロード、またはクラウドファイルストレージバケットなどの無関係 |  | ✓ | ✓ | 646 |

なドメインからダウンロードされる。XSS ベクターまたはアップロードされたファイルによる他の攻撃リスクを軽減するため、適切なコンテンツセキュリティポリシー（Content Security Policy）が実装されている。

1. V1.13 API アーキテクチャ要件

これは将来のアーキテクチャ要件のためのプレースホルダです。

1. V1.14 コンフィギュレーションアーキテクチャ要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **1.14.1** | すべてのアプリケーションコンポーネント、サービス、サーバに対して、一意または特別な低権限のオペレーティングシステムアカウントが使用されている。 |  | ✓ | ✓ | 923 |
| **1.14.2** | 信頼できないデバイスにバイナリを展開する場合は、バイナリ署名、信頼できる接続および検証済みのエンドポイントを使用する。 |  | ✓ | ✓ | 494 |
| **1.14.3** | ビルドパイプラインが、古いまたはセキュアでないコンポーネントについて警告し、かつ適切な措置が取られる。 |  | ✓ | ✓ | 1104 |
| **1.14.4** | 特にクラウド環境のビルドスクリプトなどアプリケーションインフラストラクチャがソフトウェアで定義されている場合、ビルドパイプラインにアプリケーションの安全なデプロイを自動的に構成および検証するビルドステップが含まれている。 |  | ✓ | ✓ |  |
| **1.14.5** | 特に機密性が高い、またはデシリアライゼーションなど危険な動作を実行している場合は、攻撃者が他のアプリケーションを攻撃するのを遅らせたり阻止したりするために、アプリケーションのデプロイがネットワークレベルで適切にサンドボックス化、コンテナ化および/または隔離されている。 ([C5](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 265 |
| **1.14.6** | NSAPI プラグイン、Flash、Shockwave、ActiveX、Silverlight、  NACL、またはクライアントサイドの Java アプレットなど、サポート |  | ✓ | ✓ | 477 |

がされておらずセキュアでない、または非推奨のクライアント側技術をアプリケーションが使用していない。

1. 参考情報

詳しくは以下の情報を参照してください。

* [OWASP Threat Modeling Cheat Sheet](https://www.owasp.org/index.php/Threat_Modeling_Cheat_Sheet)
* [OWASP Attack Surface Analysis Cheat Sheet](https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet)
* [OWASP Threat modeling](https://www.owasp.org/index.php/Application_Threat_Modeling)
* [OWASP Secure SDLC Cheat Sheet](https://www.owasp.org/index.php/Secure_SDLC_Cheat_Sheet)
* [Microsoft SDL](https://www.microsoft.com/en-us/sdl/)
* [NIST SP 800-57](https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final)

V2:認証の検証要件

1. 管理目標

認証とは、誰か (あるいは何か) を真正であるとして確立または確認する行為であり、個人またはデバイスの要求は正しく、なりすましに耐性があり、パスワードのリカバリや傍受を防ぐことです。

ASVS が最初にリリースされたとき、ユーザ名 + パスワードは高度なセキュリティシステム以外で最も一般的な認証形式でした。多要素認証 (MFA) はセキュリティサークルで一般的に受け入れられていますが、他ではほとんど必要とされていませんでした。パスワード侵害の数が増加するにつれ、ユーザ名は何かしらの形で機密情報であり、パスワードは不明であるという考えでは、多くのセキュリティ管理策は維持できなくなりました。例えば、NIST 800-63 はユーザ名とナレッジベース認証 (KBA) を公開情報、SMS および電子メール通知を「[制限された](https://pages.nist.gov/800-63-FAQ)」オーセンティケータタイプ、パスワードをすでに侵害されたものと考えています。この現実は、知識ベースのオーセンティケータ、SMS および電子メールでのリカバリ、パスワード履歴、複雑さ、ローテーション管理が役に立たないと言っています。これらの管理はまったく役に立たず、ユーザは数か月ごとに脆弱なパスワードを考えてきましたが、50 億を超えるユーザ名とパスワード侵害が公表されています。今が前進するときです。

ASVS のすべての章の中で、認証とセッション管理の章が最も変更されています。効果的で、エビデンスベースのリーディングプラクティスの採用は多くの人にとって挑戦となるでしょうが、それはまったくいいことです。今ここでポストパスワードの未来へ、移行を始める必要があります。

1. NIST 800-63 - 最新のエビデンスベースの認証標準

NIST 800-63b は最新のエビデンスベースの標準であり、適用可能性とは関係なく、利用可能な最適なアドバイスを表しています。この標準は世界中のすべての組織に役立ちますが、特に米国の代理店および米国の代理店を扱う組織に関連します。

NIST 800-63 の用語は、特にユーザ名 + パスワードの認証にしか慣れていない場合には、最初は少しわかりにくいかもしれません。最新の認証には進歩が必要であるため、将来一般的になるであろう用語を導入する必要がありますが、業界がこれらの新しい用語に落ち着くまで理解が難しいことを承知しています。この章の最後に参考のための用語集があります。要件の文字どおりの意味よりも、むしろ要件の目的を満たすために、多くの要件を言い換えました。例えば、NIST が「記憶された秘密 (memorized secret)」を使用する場合、ASVS では「パスワード」という用語を使用します。

ASVS V2 認証、V3 セッション管理、および範囲は狭いですが、V4 アクセス制御は選択された NIST 800- 63b 管理策の準拠サブセットに適応し、一般的な脅威と一般的に悪用される認証の脆弱性に焦点を当てています。NIST 800-63 に完全に準拠する必要がある場合には、NIST 800-63 を確認してください。

適切な NIST AAL レベルの選択

アプリケーションセキュリティ検証標準は ASVS レベル 1 を NIST AAL1 要件に、レベル 2 を AAL2 に、レベル 3 を AAL3 にマップしようとしました。しかし、「必須」管理策としての ASVS レベル 1 のアプローチはアプリケーションや API を検証するための正しい AAL レベルとは限りません。例えば、アプリケーションがレベル 3 アプリケーションである場合や AAL3 とする規制要件がある場合には、セクション V2 および V3 セッション管理でレベル 3 を選択すべきです。NIST 準拠の認証アサーションレベル(AAL) の選択は NIST-63b ガイドラインに従って実行すべきです。[NIST 800-63b Section 6.2](https://pages.nist.gov/800-63-3/sp800-63-3.html) のSelecting AAL に記載されています。

1. 凡例

特に、最新の認証がアプリケーションのロードマップ上にある場合には、アプリケーションは常に現在のレベルの要件を超える可能性があります。以前は、ASVS には必須の MFA を要求していました。NIST は必須の MFA を要求しません。したがって、この章では ASVS が推奨するが管理策を要求しない場所を示すために、オプションの指定を使用しました。この標準では以下の凡例が使用されています。

|  |  |
| --- | --- |
| 記号 | 説明 |
|  | 必須ではない |
| o | 推奨（必須ではない） |
| ✓ | 必須 |

1. V2.1 パスワードセキュリティ要件

NIST 800-63 により「暗記された秘密」と呼ばれるパスワードには、パスワード、PIN、ロック解除パターン、正しい子猫や他の画像要素の選択、およびパスフレーズがあります。それらは一般に「あなたが知っているもの（something you know）」と、みなされ多くの場合に一要素オーセンティケータとして使用されます。インターネットで公開されている数十億の有効なユーザ名とパスワード、デフォルトパスワードや脆弱なパスワード、レインボーテーブル、最も一般的なパスワードの順序付き辞書など、一要素認証の継続使用には大きな課題があります。

アプリケーションはユーザに多要素認証への登録を強く推奨し、ユーザが FIDO や U2F トークンなどすでに所有しているトークンを再利用できるようにするか、多要素認証を提供する資格情報プロバイダへのリンクを許可する必要があります。

資格情報プロバイダ (CSP) はユーザにフェデレーション ID (federated identity) を提供します。ユーザは一般的な選択肢として Azure AD, Okta, Ping Identity, Google を使用するエンタープライズ ID や、Facebook, Twitter, Google, WeChat を使用するコンシューマ ID など、複数の CSP で複数の ID を持つことがよくあります。このリストはこれらの企業やサービスを支持するものではなく、多くのユーザが多くの ID をすでに持っているという現実を、開発者が検討することを推奨するものです。組織は CSP の ID プルーフィングの強度のリスクプロファイルに従って、既存のユーザ ID との統合を検討すべきです。例えば、政府機関がソーシャルメディア ID を機密システムのログインとして受け入れることはまずありません。偽の ID を作成、ID を破棄することが簡単なためです。一方、モバイルゲーム会社はアクティブなプレイヤベースを拡大するために、主要なソーシャルメディアプラットフォームと統合する必要があると考えるかもしれません。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.1.1** | ユーザが設定するパスワードは、最低 12 文字となっている。  ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 521 | 5.1.1.2 |
| **2.1.2** | 64 文字以上のパスワードが使用できる。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 521 | 5.1.1.2 |
| **2.1.3** | パスワードにスペースを含めることができ、切り捨てが行われない。 任意で、連続した複数のスペースは 1 つにまとめてもよい。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 521 | 5.1.1.2 |
| **2.1.4** | パスワードに Unicode 文字が使用できる。単一の Unicode 符号点は文字と見なされるため、12 文字の絵文字や 64 文字の漢字が有効に使用できる必要があります。 | ✓ | ✓ | ✓ | 521 | 5.1.1.2 |
| **2.1.5** | ユーザは自身のパスワードを変更できる。 | ✓ | ✓ | ✓ | 620 | 5.1.1.2 |
| **2.1.6** | パスワード変更機能には、ユーザの現在のパスワードと新しいパスワードが必要とされる。 | ✓ | ✓ | ✓ | 620 | 5.1.1.2 |
| **2.1.7** | アカウント登録、ログインおよびパスワード変更中に送信されるパスワードが、ローカル（システムのパスワードポリシーに | ✓ | ✓ | ✓ | 521 | 5.1.1.2 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
|  | 一致する上位 1,000 または 10,000 個の最も一般的なパスワードなど）または外部 API を使用して、侵害されたパスワードと照合される。 API を使用する場合は、平文のパスワードが送信されたりパスワードの侵害状況を確認する際に使用されたりしないように、ゼロ知識証明またはその他の仕組みを使用する必要があります。 パスワードが侵害された場合、アプリケーションはユーザに新しい侵害されていないパスワードの設定を要求する必要があります。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  |  |  |  |  |
| **2.1.8** | ユーザがより強力なパスワードを設定できるように、パスワード強度メータが用意されている。 | ✓ | ✓ | ✓ | 521 | 5.1.1.2 |
| **2.1.9** | 使用可能な文字の種類を制限するパスワード規則がない。大文字、小文字、数字、特殊文字を要求する必要はない。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 521 | 5.1.1.2 |
| **2.1.10** | 定期的なクレデンシャル変更またはパスワード履歴に関する要件がない。 | ✓ | ✓ | ✓ | 263 | 5.1.1.2 |
| **2.1.11** | パスワード入力に対して、ペースト、ブラウザのパスワードヘルパー、および外部パスワードマネージャが使用できる。 | ✓ | ✓ | ✓ | 521 | 5.1.1.2 |
| **2.1.12** | ユーザがマスクされたパスワード全体を一時的に表示するか、またはネイティブ機能としてこれを備えていないプラットフォームではパスワードの最後に入力した文字を一時的に表示する  かを選択できる。 | ✓ | ✓ | ✓ | 521 | 5.1.1.2 |

注: ユーザにパスワードの表示または最後の一文字の一時的な表示を許可する目的は、特に長いパスワード、パスフレーズ、およびパスワードマネージャの使用に関して、資格情報エントリの使いやすさを向上させることです。この要件を含めるもう一つの理由は、この最新のユーザフレンドリなセキュリティエクスペリエンスを削除するよう要求するようなテストレポートを阻止または防止するためです。

1. V2.2 一般的なオーセンティケータの要件

オーセンティケータの柔軟性は将来も使い続けるアプリケーションにとって不可欠です。アプリケーションの検証をリファクタリングして、ユーザの好みに応じて追加のオーセンティケータを許可し、非推奨のオーセンティケータや安全でないオーセンティケータを規則正しく廃止できるようにします。

NIST は電子メールや SMS を 「制限された」オーセンティケータタイプ ("[restricted" authenticator](https://pages.nist.gov/800-63-FAQ/) [types](https://pages.nist.gov/800-63-FAQ/)”) と考えており、将来のある時点で NIST 800-63 および ASVS から削除される可能性があります。アプリケーションは電子メールや SMS の使用を必要としないロードマップを計画すべきです。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.2.1** | 耐自動化コントロールが流出したクレデンシャルテスト攻撃、ブルートフォース攻撃、およびアカウントロックアウト | ✓ | ✓ | ✓ | 307 | 5.2.2 /  5.1.1.2 /  5.1.4.2 / |
|  | 攻撃の軽減に効果的となっている。このようなコントロール |  |  |  |  | 5.1.5.2 |
|  | には最も一般的な流出パスワードのブロック、ソフトロック |  |  |  |  |  |
|  | アウト、レート制限、CAPTCHA、試行間の遅延増加、IP ア |  |  |  |  |  |
|  | ドレスの制限、または場所、デバイスへの最初のログイン、 |  |  |  |  |  |
|  | アカウントロック解除の最近の試行などのリスクベースの制 |  |  |  |  |  |
|  | 限があります。一つのアカウントで一時間あたり 100 回以 |  |  |  |  |  |
|  | 上の試行失敗が可能ではない。 |  |  |  |  |  |
| **2.2.2** | 弱いオーセンティケータ (SMS や電子メールなど) の使用がよりセキュアな認証方式の代わりとしてではなく、二次検証とトランザクション承認に限定されている。より強い方式が弱い方式の前に提示されていること、ユーザがリスクを承知していること、またはアカウント侵害のリスクを制限するために適切な対策が講じられている。 | ✓ | ✓ | ✓ | 304 | 5.2.10 |
| **2.2.3** | クレデンシャルのリセット、電子メールやアドレスの変更、不明な場所や危険な場所からのログインなどの認証詳細の更新後に、セキュアな通知がユーザに送信される。SMS や電子メールではなく、プッシュ通知の使用が推奨されますが、プッシュ通知がない場合、通知に機密情報が開示されていな  い限り SMS や電子メールは受け入れられます。 | ✓ | ✓ | ✓ | 620 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.2.4** | 多要素認証、目的別暗号化デバイス (プッシュして認証する接続キーなど) 、またはより高い AAL レベルのクライアント側証明書の使用など、フィッシングに対するなりすまし耐性がある。 |  |  | ✓ | 308 | 5.2.5 |
| **2.2.5** | クレデンシャルプロバイダ (CSP) と認証を検証するアプリケーションが分離されている場合、2 つのエンドポイント間で相互に認証された TLS が設定されている。 |  |  | ✓ | 319 | 5.2.6 |
| **2.2.6** | OTP デバイス、暗号化オーセンティケータ、またはルックアップコードを強制的に使用して、リプレイ耐性をつける。 |  |  | ✓ | 308 | 5.2.8 |
| **2.2.7** | OTP トークンの入力や、FIDO ハードウェアキーのボタンを押すなどのユーザ始動のアクションを要求することにより、認証の意思を検証する。 |  |  | ✓ | 308 | 5.2.9 |

1. V2.3 オーセンティケータライフサイクルの要件

オーセンティケータにはパスワード、ソフトトークン、ハードウェアトークン、生体認証デバイスがあります。オーセンティケータのライフサイクルはアプリケーションのセキュリティにとって重要です。任意の人が身分証明のないアカウントを自己登録できる場合、ID アサーションに対する信頼はほとんどありません。Reddit のようなソーシャルメディアサイトでは、それはまったく問題ありません。銀行システムでは、クレデンシャルやデバイスの登録と発行にフォーカスすることが、アプリケーションのセキュリティにとって重要です。

注: パスワードの最大有効期間をもつべきではありません。パスワードローテーションの原因となります。パスワードは定期的に入れ替えるのではなく、侵害されているかどうかを確認する必要があります。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.3.1** | システムが生成した初期パスワードまたはアクティベーションコードは、セキュアでランダムに生成されており、6 文字以上  であり、文字と数字を含むことができ、短期間で有効期限が切 | ✓ | ✓ | ✓ | 330 | 5.1.1.2  / A.3 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
|  | れる。これらの初期の秘密情報が長期間有効なパスワードになることを許可してはいけない。 |  |  |  |  |  |
| **2.3.2** | U2F や FIDO トークンなど、サブスクライバ(Subscriber)が提供する認証デバイスの登録と使用がサポートされている。 |  | ✓ | ✓ | 308 | 6.1.3 |
| **2.3.3** | 期限付きのオーセンティケータを更新するとき、十分な時間をとって更新指示が送信される。 |  | ✓ | ✓ | 287 | 6.1.4 |

1. V2.4 クレデンシャルの保管要件

アーキテクトおよび開発者はコードをビルドまたはリファクタリングする際にこのセクションを順守すべきです。このセクションはソースコードレビューを使用するか、セキュア単体テストまたはセキュア統合テストを通してのみ、完全に検証できます。ペネトレーションテストではこれらの問題を特定できません。

承認された一方向鍵生成関数のリストは NIST 800-63 B section 5.1.1.2 および [BSI Kryptographische](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf) [Verfahren: Empfehlungen und Schlussellängen (2018)](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf) で詳しく説明されています。これらの選択の代わりに、最新の国内または地域のアルゴリズムおよび鍵長標準を選択できます。

このセクションはペネトレーションテストができないため、管理策は レベル 1 に該当しません。ただし、このセクションはクレデンシャルが盗まれた場合に、セキュリティにとって非常に重要であるた め、アーキテクチャ、コーディングガイドライン、コードレビューチェックリストに対して ASVS をフォークする場合は、これらの管理策を内部バージョンでは レベル 1 に戻してください。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.4.1** | パスワードがオフライン攻撃に強い形式で保存されている。承認済みの一方向鍵生成またはパスワードハッシュ関数を使用して、パスワードをソルト化およびハッシュ化しなければなりません。 鍵生成およびパスワードハッシュ関数は、パスワードハッシュを生成するときに入力として、パスワード、ソルト、お  よびコストファクターを受け取ります。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 916 | 5.1.1.2 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2.4.2** | ソルトの長さが少なくとも 32 ビットであり、保存されているハッシュ間のソルト値の衝突を最小限に抑えるために任意に選択されている。クレデンシャルごとに、固有のソルト値とその結果のハッシュを保管しなければなりません。([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | 916 | 5.1.1.2 |
| **2.4.3** | PBKDF2 が使用されている場合、反復回数は検証サーバの性能が許す限り大きくすべきであり、通常少なくとも 100,000 回イテレーションする。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | 916 | 5.1.1.2 |
| **2.4.4** | bcrypt が使用されている場合、ワークファクターは検証サーバの性能が許す限り大きくする必要があり、通常少なくとも 13 とする。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | 916 | 5.1.1.2 |
| **2.4.5** | 秘密であり検証者のみが知っているソルト値を使用して、鍵生成関数の追加のイテレーションが実行される。承認された乱数ビット生成器 [SP 800-90Ar1] を使用してソルト値を生成し、少なくとも SP 800-131A の最新リビジョンで指定されている最小セキュリティ強度を提供します。秘密のソルト値はハッシュされたパスワードとは別に (例えば、ハードウェアセキュリティ  モジュールのような専用デバイスに) 保存すべきです。 | ✓ | ✓ | 916 | 5.1.1.2 |

米国標準が言及されている場合、必要に応じて米国標準の代わりに、またはそれに加えて、地域またはローカルの標準を使用できます。

1. V2.5 クレデンシャルリカバリ要件

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.5.1** | システムによって生成された初期アクティベーションまたはリカバリ用の秘密情報が平文でユーザに送信されていない。([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 640 | 5.1.1.2 |
| **2.5.2** | パスワードのヒントや知識ベースの認証（いわゆる「秘密の質問」）が存在しない。 | ✓ | ✓ | ✓ | 640 | 5.1.1.2 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.5.3** | パスワードクレデンシャルのリカバリによって現在のパスワードが明らかにならない。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 640 | 5.1.1.2 |
| **2.5.4** | 共有アカウントまたはデフォルトアカウントが存在しない  （例えば "root", "admin", "sa"）。 | ✓ | ✓ | ✓ | 16 | 5.1.1.2 / A.3 |
| **2.5.5** | 認証要素が変更または置き換えられた場合、ユーザにこのイベントが通知される。 | ✓ | ✓ | ✓ | 304 | 6.1.2.3 |
| **2.5.6** | パスワードを忘れた場合や他のリカバリパスは、 TOTP またはその他のソフトトークン、モバイルパス、または別のオフラインリカバリ機構などのセキュアなリカバリ機構を使用する。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 640 | 5.1.1.2 |
| **2.5.7** | OTP または多要素認証要素が失われた場合、登録時と同じレベルで同一性証明の証拠が実行される。 |  | ✓ | ✓ | 308 | 6.1.2.3 |

1. V2.6 ルックアップシークレット検証者(Verifier)の要件

ルックアップシークレットはトランザクション認証番号 (TAN) 、ソーシャルメディアリカバリーコードなどの、事前に生成されたシークレットコードのリスト、またはランダム値のセットを含むグリッドです。これらはユーザにセキュアに配布されます。これらのルックアップコードは一度使用され、すべて使用されると、ルックアップシークレットリストは破棄されます。このタイプのオーセンティケータは

「持っているもの (something you have)」とみなされます。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.6.1** | ルックアップシークレットは一度だけしか使用されない。 |  | ✓ | ✓ | 308 | 5.1.2.2 |
| **2.6.2** | ルックアップシークレットが十分なランダム性（112 ビットのエントロピー）を持っていること、または、112 ビットのエントロピー以下の場合に、一意でランダムな 32 ビットでソルト  され、承認された一方向ハッシュでハッシュ化されている。 |  | ✓ | ✓ | 330 | 5.1.2.2 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2.6.3** | ルックアップシークレットは予測可能な値などのオフライン攻  撃に対して耐性がある。 | ✓ | ✓ | 310 | 5.1.2.2 |

1. V2.7 経路外 (Out of Band) 検証者(Verifier) の要件

過去において、一般的な経路外オーセンティケータはパスワードリセットリンクを含む電子メールまたは SMS でした。攻撃者はこの脆弱なメカニズムを使用して、ある人物の電子メールアカウントを乗っ取り、発見されたリセットリンクを再利用するなど、まだ制御していないアカウントをリセットします。経路外の検証を処理するためのより良い方法があります。

セキュアな経路外オーセンティケータはセキュアなセカンダリチャネルを介して検証者と通信できる物理デバイスです。例えばモバイルデバイスへのプッシュ通信がそうです。このタイプのオーセンティケータは「持っているもの (something you have)」とみなされます。ユーザが認証したいとき、検証アプリケーションは認証者への接続を介して直接もしくは間接的にサードパーティサービスを通じて経路外オーセンティケータにメッセージを送信します。メッセージには認証コード（通常はランダムな六桁の番号またはモーダル承認ダイアログ）が含まれます。検証アプリケーションはプライマリチャネルを通じて認証コードを受信することを待ち、受信した値のハッシュを元の認証コードのハッシュと比較します。それらが一致する場合、経路外オーセンティケータはユーザが認証されたと想定できます。

ASVS はプッシュ通知などの新たな経路外オーセンティケータを開発する開発者はごく少数であると想定しているため、認証 API 、アプリケーション、シングルサインオン実装などの件奏者に次の ASVS 管理策が適用されます。新しい経路外オーセンティケータを開発する場合には、NIST 800-63B § 5.1.3.1 を参照してください。

電子メールや VOIP などの安全でない経路外オーセンティケータは許可されていません。PSTN およびSMS 認証は現在 NIST により「制限」され、廃止対象であり、プッシュ通知などを推奨しています。電話または SMS の経路外認証を使用する必要がある場合には、§ 5.1.3.3 を参照してください。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.7.1** | SMS や PSTN などの平文経路外（NIST で制限されている）オーセンティケータがデフォルトで提供されておらず、プッシュ通知などの強力な代替が最初に提供されている。 | ✓ | ✓ | ✓ | 287 | 5.1.3.2 |
| **2.7.2** | 経路外検証者が 10 分後に、帯域外認証リクエスト、コード、またはトークンが期限切れにさせる。 | ✓ | ✓ | ✓ | 287 | 5.1.3.2 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.7.3** | 経路外検証者の認証リクエストやコード、またはトークンが 1 回しか使用できず、元の認証リクエストに対してのみ使用可能となっている。 | ✓ | ✓ | ✓ | 287 | 5.1.3.2 |
| **2.7.4** | 経路外オーセンティケータおよび検証者はセキュアで独立したチャネルを介して通信する。 | ✓ | ✓ | ✓ | 523 | 5.1.3.2 |
| **2.7.5** | 経路外検証者がハッシュ化されたバージョンのオーセンティケーションコードのみを保持している。 |  | ✓ | ✓ | 256 | 5.1.3.2 |
| **2.7.6** | 初期オーセンティケーションコードは少なくとも 20 ビットのエントロピーを含む (通常、6 デジタル乱数で十分です) セキュ  アな乱数生成器により生成されている。 |  | ✓ | ✓ | 310 | 5.1.3.2 |

1. V2.8 単一または多要素のワンタイム検証者の要件

単一要素ワンタイムパスワード（OTP）は継続的に変化する疑似ランダムワンタイムチャレンジを表示する物理トークンまたはソフトトークンです。これらのデバイスはフィッシング (なりすまし) を困難にしますが、不可能ではありません。このタイプのオーセンティケータは「持っているもの (something you have)」とみなされます。多要素トークンは単一要素 OTP と似ていますが、有効な PIN コード、生体認証ロック解除、USB 挿入または NFC ペアリングまたは追加の値（トランザクション署名計算機など）を入力して最終 OTP を作成する必要があります。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.8.1** | 時間ベースの OTP は期限切れまでの有効期間が定義されている。 | ✓ | ✓ | ✓ | 613 | 5.1.4.2 / 5.1.5.2 |
| **2.8.2** | 送信された OTP を検証するために使用される対称鍵は、ハードウェアセキュリティモジュールまたはセキュアなオペレーティングシステムベースのキーストレージなどを使用して、高度に保護されている。 |  | ✓ | ✓ | 320 | 5.1.4.2 / 5.1.5.2 |
| **2.8.3** | 承認済みの暗号化アルゴリズムが生成、シード、検証に使用されている。 |  | ✓ | ✓ | 326 | 5.1.4.2 / 5.1.5.2 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2.8.4** | 時間ベースの OTP が有効期間内に 1 回しか使用できない。 | ✓ | ✓ | 287 | 5.1.4.2 / 5.1.5.2 |
| **2.8.5** | 時間ベースの多要素 OTP トークンが有効期間中に再利用された場合、それがログに記録され、セキュアな通知がデバイスの所有者に送信されるとともにリジェクトされる。 | ✓ | ✓ | 287 | 5.1.5.2 |
| **2.8.6** | 盗難やその他の損失が発生した場合は、物理的な単一要素のOTP ジェネレータを無効にすることができる。場所に関係なく、ログインしたセッション全体で失効がすぐに反映されるようにします。 | ✓ | ✓ | 613 | 5.2.1 |
| **2.8.7** | 生体認証システムが、自分が持っているものと自分が知っているものの、両方と組み合わせて二次的要素としてのみ使用  されるよう制限されている。 | o | ✓ | 308 | 5.2.3 |

1. V2.9 暗号化ソフトウェアおよびデバイス検証者の要件

暗号化セキュリティキーはスマートカードまたは FIDO キーであり、ユーザは認証を完了するために暗号化デバイスをコンピュータに接続するかペアリングする必要があります。検証者はチャレンジナンスを暗号化デバイスまたはソフトウェアに送信し、デバイスまたはソフトウェアはセキュアに保存された暗号化キーに基づいてレスポンスを計算します。

単一要素暗号化デバイスとソフトウェア、および多要素暗号化デバイスとソフトウェアの要件は同じです。これは暗号化オーセンティケータの検証が認証要素の所有を証明するためです。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.9.1** | 検証に使用される暗号化キーは、TPM や HSM またはこのセキュアなストレージを使用できる OS サービスを使用するなど、セキュアに保存され、漏えいから保護されている。 |  | ✓ | ✓ | 320 | 5.1.7.2 |
| **2.9.2** | チャレンジノンスは少なくとも 64 ビットの長さがあり、統計的に一意か、暗号化デバイスの有効期間を通じて一意となっている。 |  | ✓ | ✓ | 330 | 5.1.7.2 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2.9.3** | 承認された暗号化アルゴリズムが生成、シード、および検証に  使用されている。 | ✓ | ✓ | 327 | 5.1.7.2 |

1. V2.10 サービス認証要件

このセクションはペネトレーションテスト可能ではないため、レベル 1 要件はありません。ただし、アーキテクチャ、コーディングまたはセキュアコードレビューで使用する場合、ソフトウェアは (Java Key Store と同様に) レベル 1 の最小要件と考えてください。どのような状況でも秘密情報の平文での保存は受け入れられません。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST § |
| **2.10.1** | 統合シークレットが、API キーや共有特権アカウントなどの不変のパスワードに依存していない。 |  | OS  assisted | HSM | 287 | 5.1.1.1 |
| **2.10.2** | パスワードが必要な場合は、クレデンシャルがデフォルトアカウントではない。 |  | OS  assisted | HSM | 255 | 5.1.1.1 |
| **2.10.3** | ローカルシステムアクセスを含むオフラインリカバリ攻撃を防ぐために、パスワードは十分保護された状態で保存されている。 |  | OS  assisted | HSM | 522 | 5.1.1.1 |
| **2.10.4** | パスワード、データベースおよびサードパーティシステムとの統合、シードおよび内部シークレット、およ |  | OS  assisted | HSM | 798 |  |
|  | び API キー がセキュアに管理され、ソースコードに |  |  |  |
|  | 含まれていないこと、またはソースコードリポジトリ |  |  |  |
|  | に保存されていない。このようなストレージはオフラ |  |  |  |
|  | イン攻撃に耐える必要があります。パスワードストレ |  |  |  |
|  | ージにはセキュアなソフトウェアキーストア (L1) 、 |  |  |  |
|  | ハードウェアトラステッドプラットフォームモジュー |  |  |  |
|  | " (TPM) 、またはハードウェアセキュリティモジュ |  |  |  |
|  | ール(L3) の使用を推奨します。 |  |  |  |

1. 追加の米国政府機関要件

米国政府機関には NIST 800-63 に関する必須要件があります。アプリケーションセキュリティ検証標準は常に、アプリのほぼ 100%に適用される管理策の約 80%であり、高度な管理策や適用が制限される管理策の残りの 20%ではありません。そのため、ASVS は特に IAL1/2 および AAL1/2 分類では NIST 800- 63 の厳密なサブセットですが、特に IAL3/AAL3 分類に関しては十分に包括的ではありません。

米国政府機関には NIST 800-63 全体をレビューし実装することを強くお勧めします。

1. 用語集

|  |  |
| --- | --- |
| 用語 | 意味 |
| CSP | クレデンシャルサービスプロバイダ (Credential Service Provider) は ID プロバイダ (Identity Provider) とも呼ばれます。 |
| オーセンティケータ  (Authenticator) | パスワード、トークン、MFA、フェデレーションアサーションなどを認証するコード。 |
| 検証者(Verifier) | 「認証プロトコルを使用して 1 つまたは 2 つのオーセンティケータの認証要求者の所有と制御を検証することにより、認証要求者の身元を検証するエンティティ。これを行うために、検証者はオーセンティケータをサブスクライバ(Subscriber)のオーセンティケータにリンクし、そのステータスを確認するクレデンシャルをバリデートする必要がある場合があります。」 |
| OTP | ワンタイムパスワード (One-time password) |
| SFA | 単一要素オーセンティケータ (Single-factor authenticators) 。知っているもの (記憶された秘密、パスワード、パスフレーズ、PIN) 、持っている特徴 (生体情報、指紋、顔スキャン) 、または持っているもの (OTP トークン、スマートカードなどの暗号化デバイス) など。 |
| MFA | 多要素オーセンティケータ (Multi-factor authenticator)。2 つ以上の単一要素のものを含む。 |

1. 参考情報

詳しくは以下の情報を参照してください。

* [NIST 800-63 - Digital Identity Guidelines](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf)
* [NIST 800-63 A - Enrollment and Identity Proofing](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf)
* [NIST 800-63 B - Authentication and Lifecycle Management](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf)
* [NIST 800-63 C - Federation and Assertions](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf)
* [NIST 800-63 FAQ](https://pages.nist.gov/800-63-FAQ/)
* [OWASP Testing Guide 4.0: Testing for Authentication](https://www.owasp.org/index.php/Testing_for_authentication)
* [OWASP Cheat Sheet - Password storage](https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet)
* [OWASP Cheat Sheet - Forgot password](https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet)
* [OWASP Cheat Sheet - Choosing and using security questions](https://www.owasp.org/index.php/Choosing_and_Using_Security_Questions_Cheat_Sheet)

V3: セッション管理の検証要件

1. 管理目標

Web ベースのアプリケーションやステートフルAPI の中核となるコンポーネントのひとつは、それと対話するユーザやデバイスの状態を制御および保守するメカニズムです。セッション管理はステートレスプロトコルをステートフルに変更します。これはさまざまなユーザやデバイスを区別するために重要で す。

検証されるアプリケーションが以下の上位レベルのセッション管理要件を満たしていることを確認します。

* セッションは、各個人に固有のものであり、推測や共有することはできません
* セッションは、不要になったときや非アクティブ期間内にタイムアウトしたときに無効になります

前述のように、これらの要件は、一般的な脅威や一般的に悪用される認証の脆弱性にフォーカスした、選択された NIST 800-63b 管理策の準拠サブセットとなるように適合されています。以前の検証要件は廃止、重複削除、またはほとんどの場合、必須の [NIST 800-63b](https://pages.nist.gov/800-63-3/sp800-63b.html) 要件の意図と厳密に一致するように調整されています。

1. セキュリティ検証要件
2. V3.1 基本セッション管理要件

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST  § |
| **3.1.1** | アプリケーションが URL パラメータやエラーメッセージ内にセッショントークンを漏洩しない。 | ✓ | ✓ | ✓ | 598 |  |

1. V3.2 セッションバインディング要件

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST  § |
| **3.2.1** | アプリケーションがユーザ認証時に新しいセッショントークンを生成する。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 384 | 7.1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **3.2.2** | セッショントークンに少なくとも 64 ビットのエントロピーがある。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 331 | 7.1 |
| **3.2.3** | 適切に保護された Cookie (セクション 3.4 を参照) や HTML 5 セッションストレージなどのセキュアな方法を使用して、アプリケーションがブラウザにセッショントークンのみを保存する。 | ✓ | ✓ | ✓ | 539 | 7.1 |
| **3.2.4** | セッショントークンが承認済みの暗号化アルゴリズムを使用して生成されている。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 331 | 7.1 |

TLS や他のセキュアなトランスポートチャネルはセッション管理の必須要件です。これは通信セキュリティの章でカバーされています。

1. V3.3 セッションログアウトおよびタイムアウト要件

セッションタイムアウトは NIST 800-63 と整合しています。これはセキュリティ標準で旧来許可されているよりもはるかに長いセッションタイムアウトを許可します。組織は以下の表をレビューする必要があります。また、アプリケーションのリスクに基づいてより長いタイムアウトが望ましい場合には、NIST 値をセッションアイドルタイムアウトの上限にすべきです。

このコンテキストでのレベル 1 は IAL1/AAL1, レベル 2 は IAL2/AAL3, レベル 3 は IAL3/AAL3 です。 IAL2/AAL2 および IAL3/AAL3 では、アイドルタイムアウトはより短くなり、ログアウトやセッションを再開するための再認証にはアイドルタイムの下限とします。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST  § |
| **3.3.1** | 「戻る」ボタンや下流の依拠当事者(Relying Parties)が、依拠当事者(Relying Parties)間を含め認証済みセッションを再開しないよう に、ログアウトおよび有効期限によってセッショントークンが無効になる。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 613 | 7.1 |
| **3.3.2** | オーセンティケータがユーザにログインしたままでいることを許可する場合、アクティブに使用されているときと、アイドル期間後の  両方で、定期的に再認証が行われる。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | 30  日 | 12 時間 or  30 分のアイドル状態、 | 12 時間 or  15 分のアイドル状 | 613 | 7.2 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | 2FA はオプ  ショナル | 態、 2FA  を利用 |  |  |
| **3.3.3** | パスワードが正常に変更された後、アプリケーションが他のすべてのアクティブセッションを終了している。および、これがアプリケーション、フェデレーションログイン（存在する場合）、依拠当事者(Relying Parties)すべてに有効となっている。 | ✓ | ✓ | 613 |  |
| **3.3.4** | ユーザがすべての現在のアクティブなセッションまたはデバイスを表示、ログアウトでき  る。 | ✓ | ✓ | 613 | 7.1 |

1. V3.4 クッキーベースのセッション管理

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST  § |
| **3.4.1** | クッキーベースのセッショントークンに Secure 属性が設定されている。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 614 | 7.1.1 |
| **3.4.2** | クッキーベースのセッショントークンに HttpOnly 属性が設定されている。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 1004 | 7.1.1 |
| **3.4.3** | クロスサイトリクエストフォージェリ攻撃を抑制するために、クッキーベースのセッショントークンが SameSite 属性を利用している。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 16 | 7.1.1 |
| **3.4.4** | セッションクッキーの機密性を確保するために、クッキーベースのセッショントークンが" Host-"プレフィックス（参考文献を参照）を使用している。 | ✓ | ✓ | ✓ | 16 | 7.1.1 |
| **3.4.5** | セッションクッキーを上書きまたは開示する可能性があるセッションクッキーを設定または使用する他のアプリケーションを持つ  ドメイン名配下でアプリケーションが公開されている場合は、最 | ✓ | ✓ | ✓ | 16 | 7.1.1 |

も正確なパスを使用してクッキーベースのセッショントークンに

path 属性を設定している。 ([C6](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering))

1. V3.5 トークンベースのセッション管理

トークンベースのセッション管理には JWT, OAuth, SAML, API キーが含まれます。これらのうち、API キーは脆弱なことが分かっているため、新しいコードでは使用すべきではありません。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST  § |
| **3.5.1** | アプリケーションが、サブスクライバ(Subscriber)として、OAuth および Refresh Token を自ら処理せず、ユーザがリンクされたアプリケーションとの信頼関係を終了できるようにしている。 |  | ✓ | ✓ | 290 | 7.1.2 |
| **3.5.2** | レガシーな実装を除いて、アプリケーションが静的な API シークレットや API キーではなくセッショントークンを使用している。 |  | ✓ | ✓ | 798 |  |
| **3.5.3** | ステートレスセッショントークンがデジタル署名、暗号化、およびその他の対策を使用して、改ざん、エンベローピング、リプレイ、ヌル暗号、鍵置き換え攻撃から保護されている。 |  | ✓ | ✓ | 345 |  |

1. V3.6 フェデレーションまたはアサーションからの再認証

このセクションは依拠当事者（Relying Parties）またはクレデンシャルサービスプロバイダ（CSP）のコードを書いている人に関係するものです。これらの機能を実装するコードに依存する場合には、これらの問題が正しく処理されていることを確認します。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST  § |
| **3.6.1** | 依拠当事者(Relying Parties)が CSP に最大認証時間を指定していること、および CSP がその期間内にセッションを使用していない場合は、CSP がサブスクライバ(Subscriber)を再認証する。 |  |  | ✓ | 613 | 7.2.1 |
| **3.6.2** | CSP がユーザを再認証する必要があるかどうかを依拠当事者(Relying Parties)が決定できるように、CSP が依拠当事者(Relying Parties)に最後の認証イベントを通知する。 |  |  | ✓ | 613 | 7.2.1 |

1. V3.7 セッション管理の悪用に対する防御

数は少ないがセッション管理に対する攻撃があり、そのいくつかはセッションのユーザエクスペリエンス（UX）に関連しています。以前は、ISO 27002 要件に基づいて、ASVS は複数の同時セッションをブロックすることを要求していました。最近のユーザは多くのデバイスを使用しているだけでなく、アプリはブラウザセッションを使用しない API であるため、同時セッションのブロックはもはや適切ではありません。これらの実装のほとんどでは、最終認証者が勝利します。それはおおよそ攻撃者です。このセクションでは、コードを使用したセッション管理に対する攻撃の阻止、遅延、検出に関する主要なガイダンスを提供します。

ハーフオープン攻撃の説明

2018 年初頭、攻撃者が「ハーフオープン攻撃」と呼ぶものを使用して、いくつかの金融機関が侵害されました。この用語は業界に受け入れられています。攻撃者はさまざまな独自のコードベースを使用して複数の機関を攻撃しました。実際、同じ機関内でもコードベースが異なるようです。ハーフオープン攻撃は、多くの既存の認証、セッション管理、およびアクセス制御システムで一般的にみられる設計パターンの欠陥を悪用しています。

攻撃者は、クレデンシャルをロック、リセット、リカバリしようと試みることにより、ハーフオープン攻撃を開始します。一般的なセッション管理デザインパターンは、未認証、半認証 (パスワードリセット、ユーザ名忘れ) 、完全認証コードの間でユーザプロファイルセッションオブジェクトやモデルを再利用します。このデザインパターンは、パスワードハッシュやロールなど、被害者のプロファイルを含む 有効なセッションオブジェクトやまたはトークンを入力します。コントローラまたはルータのアクセス制御チェックでユーザが完全にログインしていることを正しく検証していない場合、攻撃者はそのユーザとして行動できるかもしれません。攻撃には、ユーザのパスワードを既知の値に変更する、有効なパスワードリセットを実行するために電子メールアドレスを更新する、多要素認証を無効にする、新しいMFA デバイスを登録する、API キーを公開または変更する、などがあります。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE | NIST  § |
| **3.7.1** | 機密性の高いトランザクションやアカウントの変更を許可する前に、アプリケーションが完全で有効なログインセッションを確保  していること、または再認証や二次検証を必要としている。 | ✓ | ✓ | ✓ | 778 |  |

1. 参考情報

詳しくは以下の情報を参照してください。

* [OWASP Testing Guide 4.0: Session Management Testing](https://www.owasp.org/index.php/Testing_for_Session_Management)
* [OWASP Session Management Cheat Sheet](https://www.owasp.org/index.php/Session_Management_Cheat_Sheet)
* [Set-Cookie Host- prefix details](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie#Directives)

V4: アクセス制御検証要件

1. 管理目標

認可 (Authorization) とは、リソースへのアクセスを、その使用を許可されたユーザのみに制限する概念です。検証対象のアプリケーションが次の高次の要件を満たすことを確認します。

* リソースにアクセスするユーザが有効なクレデンシャルを持つ
* ユーザには、正しく定義された一連のロールと権限が割り当てられている
* ロールとアクセス許可のメタデータがリプレイや改ざんから保護されている

1. セキュリティ検証要件
2. V4.1 一般的なアクセス制御デザイン

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **4.1.1** | 特に、クライアント側のアクセス制御が存在し、それが迂回される可能性がある場合には、アプリケーションは信頼できるサービスレイヤに対してアクセス制御ルールを適用する。 | ✓ | ✓ | ✓ | 602 |
| **4.1.2** | アクセス制御で使用されるすべてのユーザ属性とデータ属性およびポリシー情報は、特に認可されていない限りエンドユーザーによって操作されない。 | ✓ | ✓ | ✓ | 639 |
| **4.1.3** | 最小権限の原則が導入されている。ユーザは認可されているものについてのみ、機能やデータファイル、URL、コントローラ、サービス、他のリソースにアクセスできる。これは、なりすましや権限昇格に対する防御となる。 ([C7](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 285 |
| **4.1.4** | デフォルト拒否の原則が存在する。これにより新規のユーザやロールは 最小限の権限または権限なしで開始し、アクセスが明示的に割り当てら れるまで新しい機能へのアクセスができません。 ([C7](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 276 |
| **4.1.5** | 例外が発生した場合も含めて、アクセス制御がセキュアに失敗する。  ([C10](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 285 |

1. V4.2 オペレーションレベルアクセス制御

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **4.2.1** | 機密データおよび API が、他人のレコードの作成や更新、全員のレコードの閲覧、すべてのレコードの削除など、レコードの作成、読み取り、更新、削除を目的とするダイレクトオブジェクト攻撃に対して保護されている。 | ✓ | ✓ | ✓ | 639 |
| **4.2.2** | 認証済みの機能を保護するために、アプリケーションやフレームワークが強力な CSRF 対策メカニズムを実施していること、および有効な自動  化対策や CSRF 対策が未認証機能の保護を実施している。 | ✓ | ✓ | ✓ | 352 |

1. V4.3 他のアクセス制御の考慮

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **4.3.1** | 管理インタフェースが、不正使用を防ぐために、適切な多要素認証を使用している。 | ✓ | ✓ | ✓ | 419 |
| **4.3.2** | ディレクトリリスティグは、意図して許可されない限り、無効となっている。また、ファイルやディレクトリのメタデータ  (Thumbs.db、.DS\_Store、.git、.svn フォルダなど) の検出や開示が許可されていない。 | ✓ | ✓ | ✓ | 548 |
| **4.3.3** | アプリケーションが、低価値のシステムを対象とした追加の認可 (ステップアップ認証または適応認証など)や高価値アプリケーションを対象とした職務分掌を備えており、アプリケーションのリスクや過去に行われた  不正行為に基づき、不正行為対策の管理策を必須とする。 |  | ✓ | ✓ | 732 |

1. 参考情報

詳しくは以下の情報を参照してください。

* [OWASP Testing Guide 4.0: Authorization](https://www.owasp.org/index.php/Testing_for_Authorization)
* [OWASP Cheat Sheet: Access Control](https://www.owasp.org/index.php/Access_Control_Cheat_Sheet)
* [OWASP CSRF Cheat Sheet](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)
* [OWASP REST Cheat Sheet](https://www.owasp.org/index.php/REST_Security_Cheat_Sheet)

V5: バリデーション、無害化とエンコーディング検証要件

1. 管理目標

最も一般的な Web アプリケーションのセキュリティ上の弱点は、クライアントや環境からの入力を、出力エンコーディングなしで直接使用する前に適切に検証できないことです。この弱点は、クロスサイトスクリプティング(XSS)、SQL インジェクション、インタプリタインジェクション、ロケール/Unicode 攻撃、ファイルシステム攻撃、バッファオーバーフローなど、Web アプリケーションの重要な脆弱性のほとんどすべてにつながっています。

検証するアプリケーションが、以下の高レベルの要件を満たすことを確認してください。

* 入力のバリデーションと出力エンコーディングのアーキテクチャは、インジェクション攻撃を防ぐために合意されたパイプラインを持っています
* 入力データは強力に型付けされ、バリデーションされ、範囲や長さがチェックされ、最悪の場合、サニタイズされ、フィルタリングされていること
* 出力データは、データのコンテキストに応じて、可能な限りインタプリタに近い形でエンコード、エスケープされること

モダンな Web アプリケーションのアーキテクチャにおいては、出力エンコーディングはこれまで以上に重要です。特定のシナリオでは、堅牢な入力バリデーションを行うことは難しく、パラメータ化されたクエリ、テンプレートフレームワークによる自動エスケープ、または慎重に選択された出力エンコーディングのようなより安全な API を使用することは、アプリケーションのセキュリティにとって非常に重要です。

1. V5.1 入力バリデーション要件

ポジティブホワイトリストと強力なデータ型付けを使用して適切に実装された入力バリデーション制御は、すべてのインジェクション攻撃の 90%以上を排除することができます。長さと範囲のチェックは、これをさらに減らすことができます。アプリケーションのアーキテクチャ、設計スプリント、コーディング、ユニットテストと統合テストの間に安全な入力バリデーションの組み込みが要求されます。これらの項目の多くは、ペネトレーションテストでは発見できませんが、実装しなかった場合の結果は、通常、V5.3(出力エンコーディングとインジェクション防止要件)に記載されています。開発者やセキュアコーディングのレビュー担当者は、インジェクションを防ぐためにすべての項目に L1 が必要であるのと同じように、このセクションを扱うことが推奨されます。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **5.1.1** | アプリケーションが HTTP 変数汚染攻撃に対する防御策を備えている。特にアプリケーションフレームワークが、リクエストパラメータのソース(GET、POST、Cookie、ヘッダ、環境など)を区別しない場合はこの防御が必要。 | ✓ | ✓ | ✓ | 235 |
| **5.1.2** | フレームワークが大量のパラメータ割り当て攻撃から保護している、またはフィールドを非公開にするなど安全でないパラメータの代入を防ぐための対策が行われている。 ([C5](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 915 |
| **5.1.3** | すべての入力データがバリデーションされている。入力データには、HTML のフォームのフィールド、REST 呼び出し、クエリパラメータ、HTTP ヘッダ、Cookie、バッチファイル、RSS フィードなども含む。バリデーションはホワイトリスト方式で行う。 ([C5](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 20 |
| **5.1.4** | 構造化データが強く型付けされており、使用可能な文字、長さ、パターン等の定義されたスキーマに基づいてバリデーションされる。（例：クレジットカード番号や電話番号などのバリデーションや、地区名と郵便番号等 2 つの関連するフィールドのデータが妥当なことのバリデーション）([C5](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 20 |
| **5.1.5** | URL のリダイレクト先と転送先がホワイトリストに登録された宛先のみ許可されている、または信頼できない可能性のあるコンテンツにリダイ  レクトするときに警告を表示する。 | ✓ | ✓ | ✓ | 601 |

1. V5.2 無害化とサンドボックス化要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **5.2.1** | WYSIWYG エディタ等から取得した信頼できない HTML 入力が、HTML サニタイザライブラリもしくはフレームワークの機能によって適切に無害化され、入力バリデーションやエンコードにより適切に処理されてい  る。 ([C5](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 116 |
| **5.2.2** | 非構造化データが無害化され、使用可能な文字や長さなど一般的な対策が適用されている。 | ✓ | ✓ | ✓ | 138 |
| **5.2.3** | SMTP または IMAP インジェクションから保護するため、アプリケーションがメールシステムに渡す前にユーザ入力を無害化する。 | ✓ | ✓ | ✓ | 147 |
| **5.2.4** | eval()もしくは動的コード実行機能を使用しない。代替方法がない場合は、実行前に含まれるユーザ入力の無害化もしくはサンドボックス化する。 | ✓ | ✓ | ✓ | 95 |
| **5.2.5** | テンプレートインジェクション攻撃に対して、ユーザ入力の無害化もしくはサンドボックス化によってアプリケーションが保護されている。 | ✓ | ✓ | ✓ | 94 |
| **5.2.6** | 信頼できないデータやファイル名やURL 入力フィールドなど HTTP ファイルメタデータのバリデーションまたは無害化や、プロトコル、ド メイン、パス、ポートにホワイトリストを使用することで、アプリケーションが SSRF 攻撃から保護されている。 | ✓ | ✓ | ✓ | 918 |
| **5.2.7** | ユーザの指定した SVG スクリプト化可能コンテンツ（特に XSS に関連するインラインスクリプトや foreignObject）に対して、アプリケーションが無害化またはサンドボックス化している。 | ✓ | ✓ | ✓ | 159 |
| **5.2.8** | ユーザ指定の Markdown、CSS、XSL スタイルシート、BBCode のようなスクリプト可能もしくは式のテンプレート言語コンテンツに対して、アプリケーションが無害化、無効化またはサンドボックス化されてい  る。 | ✓ | ✓ | ✓ | 94 |

1. V5.3 出力エンコーディングとインジェクション防御の要件

使用しているインタプリタの近くまたは隣接している出力エンコーディングは、アプリケーションのセキュリティにとって非常に重要です。通常、出力エンコーディングは永続化されず、適切な出力コンテキストで出力を安全にレンダリングして、すぐに使用されます。出力エンコードに失敗すると、安全ではなくインジェクション可能で危険なアプリケーションになります。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **5.3.1** | 出力エンコーディングがインタプリタとコンテキストが要求するものに関連している。例えば特に信頼できない入力("ねこ" や "O'Hara" など、Unicode 文字やアポストロフィを含む名前など) に対して、HTML 値、HTML 属性、JavaScript、URL パラメータ、HTML ヘッダ、SMTP、その他コンテキストが必要とするものに対して個別のエンコードを使用する。([C4](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 116 |
| **5.3.2** | どの Unicode 文字でも有効かつ安全に処理されるように、出力エンコーディングがユーザが選択した文字コードセット、ロケールが保持されている。 ([C4](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 176 |
| **5.3.3** | HTML や他の Web クライアントコード中に存在するすべての文字列変数が、コンテキストに応じて適切に手動でエンコードされる、もしくはコンテキストに応じて自動的にエンコードを行うテンプレートを使用しており、アプリケーションが、反射型、格納型、および DOM ベースクロスサイトスクリプティング (XSS) 攻撃の影響を受けない。 ([C4](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 79 |
| **5.3.4** | データ選択またはデータベースクエリ（例、SQL、HQL、ORM、NoSQL）がクエリのパラメータ化、ORM、エンティティフレームワークもしくは他の方法により保護されており、データベースインジェクション攻撃の影響を受けない。 ([C3](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 89 |
| **5.3.5** | パラメータ化もしくはより安全な機構が存在しない場合、SQL インジェクションから保護するための SQL エスケープの使用など、コンテキスト固有の出力エンコーディングによりインジェクション攻撃から保護さ  れている。 ([C3, C4](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 89 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **5.3.6** | eval 攻撃、リモート JavaScript インクルード、CSP バイパス、DOM XSS、JavaScript の式の評価を含む JavaScript もしくは JSON インジェクション攻撃からアプリケーションが保護されている。 ([C4](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 830 |
| **5.3.7** | アプリケーションが LDAP インジェクションの影響を受けない、またはセキュリティ管理策によって LDAP インジェクションが防止される。([C4](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 943 |
| **5.3.8** | OS コマンドインジェクションに対して保護していること、およびオペレーティングシステムコールがパラメータ化された OS クエリを使用、もしくはコンテキストコマンドライン出力エンコーディングを使用する。 ([C4](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 78 |
| **5.3.9** | アプリケーションが、リモートファイルインクルード (RFI) やローカルファイルインクルード(LFI) の影響を受けない。 | ✓ | ✓ | ✓ | 829 |
| **5.3.10** | アプリケーションが XPath インジェクション攻撃や XML インジェクション攻撃から保護されている。 ([C4](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 643 |

注:クエリのパラメータ化や SQL のエスケープだけでは必ずしも十分ではありません。テーブル名やカラム名、ORDER BY などはエスケープできません。これらのフィールドにエスケープされたユーザ作成データが含まれていると、クエリの失敗や SQL インジェクションが発生します。

注: SVG フォーマットは、ほとんどすべてのコンテキストで ECMA スクリプトを明示的に許可しているため、すべての SVG XSS ベクターを完全にブロックすることは不可能かもしれません。SVG のアップロードが必要な場合は、アップロードされたファイルをtext/plane として提供するか、別のユーザ指定コンテンツドメインを使用して、アプリケーションから引き継がれた XSS を防止します。

1. V5.4 メモリ、文字列、アンマネージドコードの要件

以下の要件は、アプリケーションがシステム言語またはアンマネージドコードを使用している場合にのみ適用されます。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **5.4.1** | メモリセーフな文字列、安全なメモリコピー、ポインタ演算を使って、スタック、バッファ、ヒープのオーバーフローをアプリケーションが検出または防止する。 | ✓ | ✓ | 120 |
| **5.4.2** | フォーマット文字列は悪意のある入力を受け取らず、定数となっている。 | ✓ | ✓ | 134 |
| **5.4.3** | 整数オーバーフローを防ぐために符号、範囲および入力のバリデーションが使用されている。 | ✓ | ✓ | 190 |

1. V5.5 デシリアライゼーション防御の要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **5.5.1** | シリアライズされたオブジェクトが整合性チェックを使用しているこ と、または悪意のあるオブジェクトの作成やデータの改ざんを防ぐために暗号化されている。 ([C5](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 502 |
| **5.5.2** | アプリケーションが XML パーサを可能な限り最も制限の厳しい構成のみを使用するように正しく制限し、外部エンティティの解決などの危険な機能を無効にして XXE を防ぐようにしている。 | ✓ | ✓ | ✓ | 611 |
| **5.5.3** | 信頼できないデータのデシリアライズが回避されている、またはカスタムコードとサードパーティのライブラリ（JSON、XML、YAML パーサなど）の両方で保護されている。 | ✓ | ✓ | ✓ | 502 |
| **5.5.4** | ブラウザもしくは JavaScript ベースのバックエンドで JSON をパースするときは JSON.parse を使用する。eval() を使用しない。 | ✓ | ✓ | ✓ | 95 |

1. 参考情報

詳しくは以下の情報を参照してください。

* [OWASP Testing Guide 4.0: Input Validation Testing](https://www.owasp.org/index.php/Testing_for_Input_Validation)
* [OWASP Cheat Sheet: Input Validation](https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet)
* [OWASP Testing Guide 4.0: Testing for HTTP Parameter Pollution](https://www.owasp.org/index.php/Testing_for_HTTP_Parameter_pollution_%28OTG-INPVAL-004%29)
* [OWASP LDAP Injection Cheat Sheet](https://www.owasp.org/index.php/LDAP_Injection_Prevention_Cheat_Sheet)
* [OWASP Testing Guide 4.0: Client Side Testing](https://www.owasp.org/index.php/Client_Side_Testing)
* [OWASP Cross Site Scripting Prevention Cheat Sheet](https://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet)
* [OWASP DOM Based Cross Site Scripting Prevention Cheat Sheet](https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet)
* [OWASP Java Encoding Project](https://www.owasp.org/index.php/OWASP_Java_Encoder_Project)
* [OWASP Mass Assignment Prevention Cheat Sheet](https://www.owasp.org/index.php/Mass_Assignment_Cheat_Sheet)
* [DOMPurify - Client-side HTML Sanitization Library](https://github.com/cure53/DOMPurify)
* [XML External Entity (XXE) Prevention Cheat Sheet](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet))

自動エスケープの詳細な情報はこちらをご覧ください。

* [Reducing XSS by way of Automatic Context-Aware Escaping in Template Systems](https://googleonlinesecurity.blogspot.com/2009/03/reducing-xss-by-way-of-automatic.html)
* [AngularJS Strict Contextual Escaping](https://docs.angularjs.org/api/ng/service/%24sce)
* [AngularJS ngBind](https://docs.angularjs.org/api/ng/directive/ngBind)
* [Angular Sanitization](https://angular.io/guide/security#sanitization-and-security-contexts)
* [Angular Template Security](https://angular.io/guide/template-syntax#content-security)
* [ReactJS Escaping](https://reactjs.org/docs/introducing-jsx.html#jsx-prevents-injection-attacks)
* [Improperly Controlled Modification of Dynamically-Determined Object Attributes](https://cwe.mitre.org/data/definitions/915.html)

デシリアライゼーションの詳細情報はこちらをご覧ください。

* [OWASP Deserialization Cheat Sheet](https://www.owasp.org/index.php/Deserialization_Cheat_Sheet)
* [OWASP Deserialization of Untrusted Data Guide](https://www.owasp.org/index.php/Deserialization_of_untrusted_data)

V6: 保存時の暗号化の検証要件

1. 管理目標

検証されたアプリケーションが以下の高レベルの要件を満たしていることを確認します。

* すべての暗号モジュールが安全な方法で失敗し、エラーが正しく処理されること
* 適切な乱数発生器が使用されていること
* 鍵へのアクセスが安全に管理されていること

1. V6.1 データ分類

最も重要な資産は、アプリケーションによって処理、保存、または送信されたデータです。保存されているデータのデータ保護の必要性を正しく分類するために、常にプライバシー影響評価を実施してください。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **6.1.1** | 個人を特定できる情報（PII）、センシティブな個人情報、または EU のGDPR の対象となる可能性が高いと判断されたデータなど、規制対象の非公開データが暗号化されて保管されている。 |  | ✓ | ✓ | 311 |
| **6.1.2** | 医療記録、医療機器の詳細、匿名化されていない調査記録など、規制対象の医療データが暗号化されて保存されている。 |  | ✓ | ✓ | 311 |
| **6.1.3** | 金融口座、債務不履行やクレジットの履歴、税務記録、支払い履歴、受益者、匿名化されていない市場や調査記録など、規制対象の財務データが暗号化されて保管されている。 |  | ✓ | ✓ | 311 |

1. V6.2 アルゴリズム

最近の暗号技術の進歩は、以前は安全だったアルゴリズムや鍵の長さが、データを保護するためにはもはや安全でも十分でもないことを意味しています。したがって、アルゴリズムを変更することは必要です。

このセクションはペネトレーションテストが難しく、ほとんどの項目で L1 が含まれていませんが、開発者はこのセクション全体を必須項目と考えてください。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **6.2.1** | すべての暗号化モジュールにおいて、処理に失敗した場合の安全対策が施されており、オラクルパディング攻撃を許さない方法でエラーが処理される。 | ✓ | ✓ | ✓ | 310 |
| **6.2.2** | 独自実装された暗号化方式ではなく、業界で実績のある、または政府が承認した暗号化アルゴリズム、モード、およびライブラリが使用されている。 ([C8](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 327 |
| **6.2.3** | 最新の勧告を使用して、暗号初期化ベクトル、暗号設定およびブロックモードが安全に構成されている。 |  | ✓ | ✓ | 326 |
| **6.2.4** | 暗号の破壊から保護するため、乱数、暗号化またはハッシュアルゴリズム、鍵の長さ、ラウンド、暗号方式またはモードが、いつでも再構成やアップグレードもしくは入れ替えられる。 ([C8](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 326 |
| **6.2.5** | 既知の安全でないブロックモード（ECB など）、パディングモード  （PKCS#1 v1.5 など）、ブロックサイズが小さい暗号（Triple-DES、Blowfish など）、および弱いハッシュアルゴリズム（MD5、SHA1 など）が、下位互換のために要求されない限り使用されていない。 |  | ✓ | ✓ | 326 |
| **6.2.6** | ノンス、初期化ベクトル、およびその他の使い捨ての数字が、特定の暗号化鍵で複数回使いまわしされていない。生成方法は、使用しているアルゴリズムに適切となっている。 |  | ✓ | ✓ | 326 |
| **6.2.7** | 暗号化されたデータが署名、認証された暗号モード、または HMAC によって認証され、暗号文が権限のない者によって変更されない。 |  |  | ✓ | 326 |
| **6.2.8** | 情報の漏洩を防ぐために、すべての暗号化操作が、比較や計算または返戻の際にショートカット操作がなく、一定時間となっている。 |  |  | ✓ | 385 |

1. V6.3 乱数値

真の疑似乱数生成(PRNG)を正しく行うことは非常に困難です。一般的にシステム内のエントロピーの良いソースは使い過ぎるとすぐに枯渇してしまいますが、ランダム性の少ないソースは予測可能な鍵や秘密情報につながる可能性があります。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **6.3.1** | すべての乱数、ランダムなファイル名、ランダムな GUID、ランダムな文字列は、攻撃者が推測できないことを意図している場合、暗号化モジュールが許可する乱数生成器を用いて生成する。 |  | ✓ | ✓ | 338 |
| **6.3.2** | ランダムな GUID が GUID v4 アルゴリズムと暗号的に安全な疑似乱数ジェネレータ（CSPRNG）を使用して作成されている。他の疑似乱数ジェネレータを使用して作成された GUID は予測可能な場合がある。 |  | ✓ | ✓ | 338 |
| **6.3.3** | アプリケーションの負荷が高い状態であっても、乱数が適切なエントロピーを使って生成される、あるいはアプリケーションがそのような環境で適切にデグレードする。 |  |  | ✓ | 338 |

1. V6.4 シークレット管理

このセクションはペネトレーションテストが難しく、ほとんどの項目で L1 が含まれていませんが、開発者はこのセクション全体を必須項目と考えてください。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **6.4.1** | 鍵保管庫のような秘密情報管理ソリューションを、秘密情報の作成、保存、アクセス制御および秘密情報の破壊に使用している。 ([C8](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 798 |
| **6.4.2** | 鍵マテリアルがアプリケーションに公開されていない。代わりに暗号化操作用の金庫のように隔離されたセキュリティモジュールを使用してい  る。 ([C8](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 320 |

1. 参考情報

詳しくは以下の情報を参照してください。

* [OWASP Testing Guide 4.0: Testing for weak Cryptography](https://www.owasp.org/index.php/Testing_for_weak_Cryptography)
* [OWASP Cheat Sheet: Cryptographic Storage](https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet)
* [FIPS 140-2](https://csrc.nist.gov/publications/detail/fips/140/2/final)

V7: エラー処理およびログ記録の要件

1. 管理目標

エラー処理とログ記録の主な目的は、ユーザ、管理者、インシデント対応チームに有用な情報を提供することです。目的は、大量のログを作成することではなく、廃棄されるノイズよりも多くのシグナルを含む高品質のログを作成することです。

高品質のログには機密データが含まれていることが多く、現地のデータプライバシー法や指令に従って保護されなければなりません。これには以下が含まれます。

* 特に必要とされない限り、機密情報の収集やロギングを行わないこと
* すべてのログ情報が安全に処理され、データ分類に従って保護されていること
* ログは永久に保存せず、可能な限り短い絶対的な寿命を持つようにすること

定義は国によって異なりますが、ログに個人情報や機密性の高いデータが含まれている場合、ログはアプリケーショ ンによって保持される最も機密性の高い情報の一部となり、攻撃者にとって非常に魅力的なものとなります。

また、アプリケーションが安全に失敗し、エラーが不必要な情報を開示しないようにすることも重要です。

1. V7.1 ログ内容の要件

機密情報をログに記録するのは危険です。ログそのものが機密情報に分類されるため、暗号化する必要が生じ、保存ポリシーの対象となり、セキュリティ監査で開示する必要があります。必要な情報のみをログに保存し、支払い、資格情報（セッショントークンを含む）、機密情報または個人を特定できる情報は絶対に含めないでください。

V7.1 は OWASP Top 10 2017:A10 をカバーしています。2017:A10 とこのセクションはペネトレーションテストが不可能なため、以下の点が重要です。

* 開発者は、このセクションで L1 とマークされているすべての項目に完全準拠すること
* ペネトレーションテスターは、インタビューやスクリーンショットまたはアサーションを介して

V7.1 のすべての項目への完全準拠を検証すること

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **7.1.1** | アプリケーションがクレデンシャルまたは支払い情報をログに保存していない。セッショントークンは、不可逆的なハッシュ形式でのみログに保存する。 ([C9, C10](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 532 |
| **7.1.2** | 現地のプライバシー法または関連するセキュリティポリシーで定義されているその他のセンシティブなデータをログに記録していない。 ([C9](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 532 |
| **7.1.3** | 成功および失敗した認証イベント、アクセス制御の失敗、デシリアライゼーションの失敗、および入力検証の失敗を含むセキュリティへの影響が考えられるイベントについてログを保存する。 ([C5, C7](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 778 |
| **7.1.4** | 各ログのイベントには、イベント発生時のタイムラインを詳細に調査するために必要な情報が含まれている。 ([C9](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 778 |

1. V7.2 ログ処理の要件

タイムリーなログ記録は、監査イベント、トリアージおよびエスカレーションにとって重要です。アプリケーションのログが明確で、ローカルまたはリモートの監視システムに送信されたログのいずれかで簡単に監視および分析できることを確認してください。

V7.2 は OWASP Top 10 2017:A10 をカバーしています。2017:A10 とこのセクションはペネトレーションテストが不可能なため、以下の点が重要です。

* 開発者は、このセクションで L1 とマークされているすべての項目に完全準拠すること
* ペネトレーションテスターは、インタビューやスクリーンショットまたはアサーションを介して

V7.2 のすべての項目への完全準拠を検証すること

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **7.2.1** | センシティブなセッション ID やパスワードを保存せずに、すべての認証判定がログに記録されている。これには、セキュリティ調査に必要な関連メタデータを含むリクエストを含める。 |  | ✓ | ✓ | 778 |
| **7.2.2** | すべてのアクセス制御判定がログに記録され、失敗したすべての判定がログに記録される。これには、セキュリティ調査に必要な関連メタデータを含むリクエストを含める。 |  | ✓ | ✓ | 285 |

1. V7.3 ログ保護の要件

簡単に変更や削除が可能なログは、調査や訴追には使えません。ログの公開により、アプリケーションまたはアプリケーションに含まれるデータに関する内部の詳細が明らかになる可能性があります。不正な開示、変更、削除からログを保護する際には注意が必要です。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **7.3.1** | ログインジェクションを防ぐためにユーザ指定のデータを適切にエンコードする。 ([C9](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 117 |
| **7.3.2** | ログ閲覧ソフトウェアで表示したときに、すべてのイベントがインジェクションから保護されている。 ([C9](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 117 |
| **7.3.3** | セキュリティログが不正なアクセスや改変から保護されている。 ([C9](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 200 |
| **7.3.4** | 時刻源が正しい時間と正しいタイムゾーンに同期されている。システムがグローバルである場合は、インシデント後のフォレンジック分析を支  援するために UTC でのみログを記録することを強く検討する。 ([C9](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ |  |

注：ログのエンコーディング（7.3.1）は、自動化された動的ツールやペネトレーションテストによるテストやレビューは困難ですが、設計者、開発者、ソースコードレビュー者はログのエンコーディングをL1 の要件と考える必要があります。

1. V7.4 エラー処理

エラー処理の目的は、アプリケーションが監視やトリアージおよびエスカレーションのためにセキュリティ関連のイベントを提供できるようにすることです。目的はログを作成することではありません。セキュリティ関連のイベントをログに記録するときは、ログに目的があること、および SIEM または分析ソフトウェアによって区別できることを確認してください。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **7.4.1** | 予期しないエラーまたはセキュリティ上重要なエラーが発生したとき  に、サポート担当者が調査に使用できる一意の ID とともに一般的なメッ  セージが表示される。 ([C10](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 210 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **7.4.2** | 予期されるエラーおよび予期されないエラー状態を説明するために、例外処理（または機能的に同等なもの）がコードベース全体で使用されている。 ([C10](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | 544 |
| **7.4.3** | 未処理の例外をすべて捕捉する「最後の手段」となるエラーハンドラが定義されている。 ([C10](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | 460 |

注：Swift や Go のような特定の言語や（および一般的な設計手法を通して）多くの関数型言語は、例外や最終手段イベントハンドラをサポートしていません。このような場合、設計者と開発者は、パター

ン、言語またはフレームワークで簡単に使える方法を使用して、例外や予期しないイベントまたはセキュリティ関連のイベントをアプリケーションが安全に処理できるようにする必要があります。

1. 参考情報

詳しくは以下の情報を参照してください。

* [OWASP Testing Guide 4.0 content: Testing for Error Handling](https://www.owasp.org/index.php/Testing_for_Error_Handling)

V8: データ保護の要件

1. 管理目標

データ保護を適切に行うには次の 3 つの要素を考慮する必要があります。機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の CIA です。この標準ではデータ保護が、強固かつ十分な保護を備えるサーバなど信頼できるシステム上でデータ保護が行われていることを想定しています。

アプリケーションは「ユーザデバイスはどれも完全には信頼できない」ことを前提にする必要があります。共有コンピュータや電話、タブレット等の安全でないデバイスに対してセンシティブなデータの送信や保存を行う場合、アプリケーション側が責任を持って、デバイス上に保存するデータを暗号化し、不正な取得や変更、開示が容易にはできないよう保護する必要があります。

検証対象のアプリケーションが次の高次のデータ保護要件を満たすことを確認します。

* 機密性：送信と保存の両方で認可されていない監視や開示からデータが保護されている
* 完全性：攻撃者による悪意のある作成，変更，削除からデータが保護されている
* 可用性：必要なときにデータが許可されたユーザに提供される

1. V8.1 一般的なデータ保護

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **8.1.1** | アプリケーションは機密データをロードバランサやアプリケーションキャッシュなどのサーバコンポーネントにキャッシュされないように保護している。 |  | ✓ | ✓ | 524 |
| **8.1.2** | サーバ上に保存されている機密データの、すべてのキャッシュや一時コピーが、認証されていないアクセスから保護されているか、認証されたユーザが機密データにアクセスした後に削除または無効化される。 |  | ✓ | ✓ | 524 |
| **8.1.3** | 1 リクエスト中に含まれるパラメータの数（非表示フィールド、Ajax 変数、Cookie、ヘッダ値など）を最小限にしている。 |  | ✓ | ✓ | 233 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **8.1.4** | アプリケーションが、IP 、ユーザ、1 時間または 1 日あたりの総数、またはアプリケーションにとって重要なリクエストなど、異常な数のリクエストを検出および警告できる。 | ✓ | ✓ | 770 |
| **8.1.5** | 重要なデータの定期的なバックアップが実行され、データのリストアテストが実行されている。 |  | ✓ | 19 |
| **8.1.6** | データの盗難や破損を防ぐために、バックアップがセキュアに保存されている。 |  | ✓ | 19 |

1. V8.2 クライアントサイドのデータ保護

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **8.2.1** | 最新のブラウザで機密データがキャッシュされないように、アプリケーションは十分なキャッシュ防止ヘッダを設定する。 | ✓ | ✓ | ✓ | 525 |
| **8.2.2** | クライアントの記憶域（HTML5 のローカルストレージ、セッションストレージ、IndexedDB、通常の Cookie、FlashCookie など）に保存されるデータにセンシティブなデータや PII が含まれていない。 | ✓ | ✓ | ✓ | 922 |
| **8.2.3** | セッションの終了後、ブラウザの DOM など認証されたデータがクライアントの記憶域から消去される。 | ✓ | ✓ | ✓ | 922 |

1. V8.3 機密性の高い個人データ

このセクションは、特に大量の場合、センシティブなデータを認証なく作成、読み取り、更新、削除することから保護するのに役立ちます。

このセクションへの準拠は V4 アクセス制御、特に V4.2 への準拠を意味します。例えば、認証のない更新やセンシティブな個人情報の開示から保護するには V4.2.1 を順守する必要があります。完全に網羅するにはこのセクションと V4 に従ってください。

注: オーストラリアのプライバシー原則 APP-11 や GDPR などのプライバシー規制や法令は、センシティブな個人情報の保存、使用、および転送の実装にアプリケーションがどのようにアプローチする必要があるかに直接影響します。これには厳しいペナルティから簡単なアドバイスまであります。地域の法令や規制を調べ、必要に応じて資格のあるプライバシーの専門家または弁護士に相談してください。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **8.3.1** | センシティブなデータが HTTP メッセージボディまたはヘッダでサーバに送信される。どんな HTTP verb のクエリストリングパラメータにもセンシティブなデータが含まれない。 | ✓ | ✓ | ✓ | 319 |
| **8.3.2** | ユーザが自身のデータをオンデマンドで、削除またはエクスポートできる。 | ✓ | ✓ | ✓ | 212 |
| **8.3.3** | 個人情報の収集および利用に関する明確なポリシーが、ユーザに提供されている。個人情報が何らかの方法で使用される前に、オプトイン方式で個人情報利用に関する同意を得ている。 | ✓ | ✓ | ✓ | 285 |
| **8.3.4** | アプリケーションにより作成および処理される、すべてのセンシティブなデータを特定している。センシティブなデータを処理する方法に関するポリシーが、策定されている。 ([C8](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 200 |
| **8.3.5** | データが関連するデータ保護規制の下で収集されている場合や、アクセスログ記録が必要な場合、センシティブなデータへのアクセスが（センシティブなデータ自体がログに記録されることなく）監査されている。 |  | ✓ | ✓ | 532 |
| **8.3.6** | メモリダンプ攻撃を軽減するため、メモリに保持されたセンシティブな情報は、不要になればすぐに、ゼロまたはランダムデータを使用して上書きする。 |  | ✓ | ✓ | 226 |
| **8.3.7** | 暗号化を必要とするセンシティブなもしくは個人情報は、機密性と完全性の双方を提供する承認済みアルゴリズムを使用して暗号化する。 ([C8](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 327 |
| **8.3.8** | センシティブな個人情報は、古いデータや期限切れのデータが、自動 的、定期的、または状況に応じて削除されるなど、データ保持分類の対  象となっている。 |  | ✓ | ✓ | 285 |

データ保護を検討する際には、主に一括抽出、一括変更、過度の使用について考慮すべきです。例え ば、多くのソーシャルメディアシステムではユーザは 1 日に新しい友人を 100 人しか追加できませんが、これらのリクエストがどのシステムから来たのかは重要ではありません。銀行のプラットフォームでは、1000 ユーロを超える資金を外部の機関に転送することは、1 時間当たり 5 つの取引まででブロッ

クすることが期待されています。各システムの要件は大きく異なることがあるため、「異常」を判断するには脅威モデルとビジネスリスクを考慮する必要があります。重要な基準はそのような異常な大量のアクションを検出、阻止、または可能であればブロックする能力です。

1. 参考情報

詳しくは以下の情報を参照してください。

* [Consider using Security Headers website to check security and anti-caching headers](https://securityheaders.io/)
* [OWASP Secure Headers project](https://www.owasp.org/index.php/OWASP_Secure_Headers_Project)
* [OWASP Privacy Risks Project](https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project)
* [OWASP User Privacy Protection Cheat Sheet](https://www.owasp.org/index.php/User_Privacy_Protection_Cheat_Sheet)
* [European Union General Data Protection Regulation (GDPR) overview](https://edps.europa.eu/data-protection_en)
* [European Union Data Protection Supervisor - Internet Privacy Engineering Network](https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en)

V9: 通信の検証要件

1. 管理目標

検査対象のアプリケーションが次の高次の要件を満たすことを確認します。

* 送信されるデータの機密性に関係なく、TLS または強力な暗号が常に使用されている
* 構成に関する最新の先導的な勧告が、優先アルゴリズムおよび暗号の有効化と順序づけに使用されている
* 脆弱または近い将来廃止予定のアルゴリズムや暗号は、最後の手段として順序付けされている
* 非推奨または既知のセキュアでないアルゴリズムや暗号が無効になっている

セキュアな TLS 構成に関する業界の主要な勧告は、既存のアルゴリズムや暗号の壊滅的な破綻が原因で頻繁に変更されます。常に最新のバージョンの TLS 設定レビューツール（SSLyze や他の TLS スキャナなど）を使用して、優先順位とアルゴリズム選択を設定してください。設定を定期的にチェックして、セキュアな通信設定が常に存在し有効であることを確認します。

1. V9.1 通信のセキュリティ要件

すべてのクライアント通信は、暗号化された通信経路を介してのみ行われる必要があります。特に、最新のブラウザや検索エンジンでは、TLS1.2 以降の使用が必須とされています。オンラインツールを使用して定期的に構成を見直し、最新の先進的な手法が採用されていることを確認する必要があります。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Description | L1 | L2 | L3 | CWE |
| **9.1.1** | 安全な TLS がすべてのクライアント接続に使用されており、安全でないプロトコルや非暗号化プロトコルにフォールバックしない。 ([C8](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 319 |
| **9.1.2** | オンラインまたは最新の TLS テストツールを使用して、強力なアルゴリズム、暗号、プロトコルのみが有効であり、最も強力なアルゴリズムと暗号が優先的に設定されている。 | ✓ | ✓ | ✓ | 326 |
| **9.1.3** | 古いバージョンの SSL や TLS プロトコル（SSLv2、SSLv3、TLS 1.0、TLS 1.1）、アルゴリズム、暗号および構成が無効になっている。最新バージ  ョンの TLS を優先する暗号スイートに設定する。 | ✓ | ✓ | ✓ | 326 |

1. V9.2 サーバ通信のセキュリティ要件

サーバ通信は HTTP だけではありません。監視システム、管理ツール、リモートアクセスや SSH、ミドルウェア、データベース、メインフレーム、パートナーまたは外部ソースシステムなど、他のシステムとの安全な接続が必要です。「外部は堅牢だが、内部が傍受しやすい」ことを防ぐために、これらの通信はすべて暗号化する必要があります。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **9.2.1** | サーバ接続（外向き、内向きの両方）において、信頼できる TLS 証明書が使用されている。内部で生成された証明書または自己署名証明書を使用する場合、サーバは特定の内部認証局や特定の自己署名証明書のみを信頼するように構成し、それ以外の証明書はすべて拒否する。 |  | ✓ | ✓ | 295 |
| **9.2.2** | 管理ポート、監視、認証、API、または Web サービスの呼び出し、データベース、クラウド、サーバレス、メインフレーム、外部やパートナー間の接続など、すべての外向き／内向きの接続に TLS などの暗号化通信が使用されている。サーバは、安全でないプロトコルや暗号化されていないプロトコルにフォールバックしてはいけない。 |  | ✓ | ✓ | 319 |
| **9.2.3** | センシティブな情報や機能を持つ外部システムとの暗号化接続がすべて認証されている。 |  | ✓ | ✓ | 287 |
| **9.2.4** | Online Certificate Status Protocol (OCSP) Stapling など証明書の失効を適切にチェックできる機能を設定し、有効にしている。 |  | ✓ | ✓ | 299 |
| **9.2.5** | バックエンドの TLS 通信に関するエラーがログに記録されている。 |  |  | ✓ | 544 |

1. 参考情報

詳しくは以下の情報を参照してください。

* [OWASP – TLS Cheat Sheet](https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet)
* 「認定された TLS のモード」に関する注記。これまで、ASVS は米国標準 FIPS 140-2 を参照してきましたが、この米国標準をグローバル標準として適用することは困難であったり、矛盾が生じたり、あるいは混乱を招く可能性があります。要件 9.1.3 に準拠するためのより良い方法は、<https://wiki.mozilla.org/Security/Server_Side_TLS>などのガイドを参照したり、[https://ssl-](https://ssl-config.mozilla.org/)

[config.mozilla.org/](https://ssl-config.mozilla.org/) で既知の適切な構成をつくり、sslyze などの既存の TSL 評価ツールや脆弱性スキャナ、信頼できるオンラインの TLS アセスメントサービスを使用して、望ましいレベルのセキュリティを確保することです。本セクションに準拠しない例としては、旧式または安全性の低い暗号やアルゴリズムの使用、Perfect Forward Secrecy の欠如，旧式または安全性の低い SSL プロトコル、脆弱な推奨暗号などが一般に見られます。

V10: 悪性コードの検証要件

1. 管理目標

検査対象のコードが次の高次の要件を満たすことを確認します。

* アプリケーションの他の部分に影響が及ばないよう、悪性活動がセキュアな方法で適切に処理される
* time bomb や他の time based 攻撃に繋がる問題を作り込んでいない
* 悪性サイトや許可されていないサイトとの秘密の通信 (“phone home”)を行わない
* 攻撃者が制御可能なバックドア、イースターエッグ、サラミ攻撃、ルートキット、不正コードが作り込まれていない

悪性コードを完全に見つけることは不可能です。コードの中に悪性コードや不要な機能が含まれていないことを確認するために、最善の努力を払う必要があります。

1. V10.1 コード整合性コントロール

悪性コードに対する最良の防御策は、「信頼はするが、検証もする」ことです。 不正なコードや悪性コードを取り込むことは、多くの管轄で犯罪行為となっています。そして 悪性コードを無くすためにガイドラインを設ける必要があります。

リード開発者による定期的なコードチェック（特に時間、I/O、またはネットワーク機能にアクセスする可能性があるコード）を行う必要があります。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **10.1.1** | 時間関数、危険なファイル操作、ネットワーク接続など、悪性コードを検出できるコード分析ツールが使用されている。 |  |  | ✓ | 749 |

1. V10.2 悪意コード検索

悪性コードが作り込まれることは極めてまれです。また検出は困難です。コードを 1 行 1 行レビューするのはロジックボムを見つける助けにはなるでしょうが、最も経験を積んだコードレビュアをもってしても、存在すると分かっていても悪性コードを見つけることは容易ではありません。

このセクションに準拠するには、サードパーティのライブラリを含むソースコードに完全にアクセスする必要があります。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **10.2.1** | アプリケーションのソースコードおよびサードパーティライブラリに、不正な通信 (“phone home”) またはデータ収集機能が含まれていないようにする。このような機能がある場合は、データを収集する前にユーザの許可を受ける。 |  | ✓ | ✓ | 359 |
| **10.2.2** | アプリケーションが連絡先、カメラ、マイク、ロケーションなど、プライバシー関連の機能に対して不要な権限または過剰な権限を要求しない。 |  | ✓ | ✓ | 272 |
| **10.2.3** | アプリケーションのソースコードおよびサードパーティのライブラリにバックドアが含まれていない。（ハードコードされたアカウントや鍵、文書化されていないアカウントや鍵、コードの難読化、文書化されていないバイナリ BLOB、ルートキット、アンチデバッグ、危険なデバッグ機能、古い機能、隠された機能） |  |  | ✓ | 507 |
| **10.2.4** | 日付と時刻関連の機能を検索して、アプリケーションのソースコードとサードパーティのライブラリに時限爆弾(time bomb)が含まれていない。 |  |  | ✓ | 511 |
| **10.2.5** | アプリケーションのソースコードとサードパーティのライブラリに、サラミ攻撃、ロジックバイパス(logic bypasses)、ロジックボム(logic bombs)などの悪意のあるコードが含まれていない。 |  |  | ✓ | 511 |
| **10.2.6** | アプリケーションのソースコードとサードパーティのライブラリにイースターエッグやその他の望ましくない機能が含まれていない。 |  |  | ✓ | 507 |

1. V10.3 デプロイ済アプリケーションの整合性コントロール

アプリケーションがデプロイされた後も、悪性コードが挿入される可能性があります。 アプリケーションは、信頼されていないソースからの未署名のコードの実行やサブドメインテイクオーバ（subdomain takeover）などの一般的な攻撃から自身を保護する必要があります。

このセクションに準拠するには運用上、持続的に進める必要があります。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **10.3.1** | アプリケーションにクライアントまたはサーバの自動更新機能がある場合は、安全なチャネルを経由して、デジタル署名がされていることを確 認する。インストールまたは実行する前に、アップデートするコード のデジタル署名を検証する必要がある。 | ✓ | ✓ | ✓ | 16 |
| **10.3.2** | アプリケーションで、コード署名やサブリソースの完全性などの保護が使用されている。加えて、信頼できない場所やインターネットから取得したモジュール、プラグイン、コード、ライブラリなどをロードまたは実行しない。 | ✓ | ✓ | ✓ | 353 |
| **10.3.3** | 期限切れドメイン名、期限切れ DNS ポインタまたは CNAME、パブリックソースコードリポジトリでの期限切れプロジェクト、一時的なクラウド API、サーバレス機能、ストレージバケット（autogen-bucket- id.cloud.example.com）など、DNS エントリまたは DNS サブエントリに依存している場合、アプリケーションがサブドメイン奪取  （subdomain takeover）から保護されている。アプリケーションの保護は使用する DNS 名の有効期限または変更を定期的にチェックするこ  とを含めます。 | ✓ | ✓ | ✓ | 350 |

1. 参考情報

* [Hostile Sub-Domain Takeover, Detectify Labs](https://labs.detectify.com/2014/10/21/hostile-subdomain-takeover-using-herokugithubdesk-more/)
* [Hijacking of abandoned subdomains part 2, Detectify Labs](https://labs.detectify.com/2014/12/08/hijacking-of-abandoned-subdomains-part-2/)

V11: ビジネスロジックの検証要件

1. 管理目標

検証対象のアプリケーションが次の高次の要件を満たすことを確認します。

* ビジネスロジックが正しい順序で処理
* ビジネスロジックに自動攻撃を検知し防止する制限が実装されている。自動攻撃の例としては，連続的な少額の送金や 1 度に 100 万人の友人を追加する，などがある
* 高い価値を持つビジネスロジックにおいて悪用ケースや悪用する人を想定している。また，なりしまし (spoofing)，改ざん (tampering)，否認 (repudiation)，情報の漏えい (information disclosure)，権限昇格 (elevation of privilege) 攻撃の対策を行っている

1. V11.1 ビジネスロジックのセキュリティ要件

ビジネスロジックセキュリティは、すべてのアプリケーションごとに固有なため、どのチェックリストも適用はできません。そして外部からの脅威から保護するように設計されている必要がありますが、それは Web アプリケーションファイアウォール(firewalls)や安全な通信を使用しても保護することはできません。OWASP Cornucopia などのツールを使用して、デザインスプリント中に脅威モデリングを使用することを推奨します。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **11.1.1** | アプリケーションが同じユーザのビジネスロジックフローを手順通り、省略せずに処理する。 | ✓ | ✓ | ✓ | 841 |
| **11.1.2** | アプリケーションは、すべてのステップが人間の実際に処理する時間で処理されたビジネスロジックフローのみ処理する。（送信されるのが早すぎるトランザクションは処理されない。） | ✓ | ✓ | ✓ | 779 |
| **11.1.3** | アプリケーションに適切な制限が実装されており、特定のビジネス活動やトランザクションに対し、ユーザごとに適用されている。 | ✓ | ✓ | ✓ | 770 |
| **11.1.4** | データの流出、ビジネスロジック要求、過剰なファイルのアップロード、DoS 攻撃(denial of service attacks)を検出および保護するため  に、アプリケーションに充分な自動攻撃を検知し防止する制限がある。 | ✓ | ✓ | ✓ | 770 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **11.1.5** | アプリケーションは脅威モデリング(threat modelling)または類似の方法を使用して特定されたビジネスリスクから保護するために、ビジネスロジックの制限またはバリデーションがある。 | ✓ | ✓ | ✓ | 841 |
| **11.1.6** | アプリケーションの機密性の高い処理が「Time of Check to Time of Use」TOCTOU 問題や、その他の競合状態の影響を受けない。 |  | ✓ | ✓ | 367 |
| **11.1.7** | アプリケーションはビジネスロジックの観点から異常なイベントまたはアクティビティを監視している。例えば、順序がおかしい行為や通常のユーザが決して試みない行為の試行が該当する。 ([C9](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 754 |
| **11.1.8** | アプリケーションは、自動攻撃または異常なアクティビティが検出されたときにアラートする設定機能がある。 |  | ✓ | ✓ | 390 |

1. 参考情報

詳しくは以下の情報を参照してください。

* [OWASP Testing Guide 4.0: Business Logic Testing](https://www.owasp.org/index.php/Testing_for_business_logic)
* [OWASP Cheat Sheet](https://www.owasp.org/index.php/Business_Logic_Security_Cheat_Sheet)
* 対自動処理はこれらを含む、多くの方法で対応できる。[OWASP AppSensor](https://www.owasp.org/index.php/OWASP_AppSensor_Project)、[OWASP Automated Threats to Web Applications](https://www.owasp.org/index.php/OWASP_Automated_Threats_to_Web_Applications)
* [OWASP AppSensor](https://www.owasp.org/index.php/OWASP_AppSensor_Project) は、攻撃検知と対応に役立つ。
* [OWASP Cornucopia](https://www.owasp.org/index.php/OWASP_Cornucopia)

V12: ファイルとリソースの検証要件

1. 管理目標

検査対象のアプリケーションが次の高次の要件を満たすことを確認します。

* 信頼できないファイルのデータがセキュアな方法で適切に処理される
* 信頼できない情報源から取得したデータは，Web ルート(webroot) の外に保存され，アクセスが制限される

1. V12.1 ファイルアップロード要件

高圧縮ファイル爆弾（zip bombs）はペネトレーションテスト技法を用いて充分テスト可能ですが、慎重な手動テストによる設計と開発の配慮を奨励し、かつ自動または不十分な手動ペネトレーションテストによるサービス運用妨害状態（DoS）を回避するために、L2 以上と見なされます。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **12.1.1** | ストレージを圧迫させたり、DoS 攻撃を引き起こしたりする可能性のある大きなファイルをアプリケーションが受け付けない。 | ✓ | ✓ | ✓ | 400 |
| **12.1.2** | 圧縮ファイルが「高圧縮ファイル爆弾(zip bombs)」でないことを確認する。（高圧縮ファイル爆弾(zip bombs)：小さい入力ファイルが解凍されて巨大なファイルになり、ファイルの保存容量の限界を超えて、ストレージを使用不能にする悪意のある圧縮ファイル。） |  | ✓ | ✓ | 409 |
| **12.1.3** | 1 人のユーザがあまりにも多くのファイルまたは極端に大きいファイルでストレージを圧迫させることができないように、ユーザあたりのファ  イルサイズクォータと最大ファイル数が適用されている。 |  | ✓ | ✓ | 770 |

1. V12.2 ファイルの完全性の要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **12.2.1** | 信頼できない場所から取得したファイルが、期待されるファイルである ことをファイルの内容に基づいて判断する。 |  | ✓ | ✓ | 434 |

1. V12.3 ファイル実行の要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **12.3.1** | パストラバーサルから保護するために、ユーザが送信したファイル名の メタデータがシステムまたはフレームワークファイルや URL API で直接使用されていない。 | ✓ | ✓ | ✓ | 22 |
| **12.3.2** | ローカルファイル（LFI）の漏えい、作成、更新、または削除を防止す るために、ユーザが送信したファイル名のメタデータをバリデートもしくは無視する。 | ✓ | ✓ | ✓ | 73 |
| **12.3.3** | SSRF にも繋がる可能性があるリモートファイル(RFI)の漏えいまたは実行を防ぐために、ユーザが送信したファイル名のメタデータをバリデートもしくは無視する。 | ✓ | ✓ | ✓ | 98 |
| **12.3.4** | アプリケーションを反射型ファイルダウンロード（RFD）から保護するため、ユーザが送信したファイル名（JSON、JSONP または URL パラメータの中にある）をバリデートまたは無視し、レスポンスのContent-Type ヘ ッ ダ は text/plain に 設 定 、 お よ び Content- Disposition ヘッダは固定ファイル名を指定する。 | ✓ | ✓ | ✓ | 641 |
| **12.3.5** | OS コマンドインジェクションから保護するために、信頼できないファイルメタデータをシステム API またはライブラリで直接使用しない。 | ✓ | ✓ | ✓ | 78 |
| **12.3.6** | アプリケーションは、未検証のコンテンツ配信ネットワーク、  JavaScript ライブラリ、ノード npm ライブラリ、サーバサイド DLL  などの信頼できない場所からの機能を含まず、かつ実行されない。 |  | ✓ | ✓ | 829 |

1. V12.4 ファイル保存の要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **12.4.1** | 信頼できない場所から取得したファイルは、Web ルート以外にパーミッションを制限した上で保存し、可能な限り厳密なバリデーションを行  う。 | ✓ | ✓ | ✓ | 922 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **12.4.2** | 信頼できない場所から取得したファイルが、アプリケーションが想定する種類であることを検証し、既知の悪性コンテンツがアップロードされ  るのを防止するためにアンチウイルスソフトで検査する。 | ✓ | ✓ | ✓ | 509 |

1. V12.5 ファイルダウンロードの要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **12.5.1** | 意図しない情報やソースコードの漏えいを防ぐために、特定のファイル 拡張子を持つファイルのみを処理するように Web 層が構成されている。例えば、バックアップファイル（.bak など）、一時作業ファイル  （.swp など）、圧縮ファイル（.zip、.tar.gz など）およびエディタで一般的に使用されるその他の拡張子は、必要ない限り処理しない。 | ✓ | ✓ | ✓ | 552 |
| **12.5.2** | アップロードされたファイルへの直接のリクエストが  HTML/JavaScript コンテンツとして実行されない。 | ✓ | ✓ | ✓ | 434 |

1. V12.6 SSRF からの保護要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **12.6.1** | Web サーバまたはアプリケーションサーバが、リクエストを送信したりデータ/ファイルをロードしたりできるように、リソースまたはシス  テムにホワイトリストが構成されている。 | ✓ | ✓ | ✓ | 918 |

1. 参考情報

詳しくは以下の情報を参照してください。

* [File Extension Handling for Sensitive Information](https://www.owasp.org/index.php/Unrestricted_File_Upload)
* [Reflective file download by Oren Hafif](https://www.trustwave.com/Resources/SpiderLabs-Blog/Reflected-File-Download---A-New-Web-Attack-Vector/)
* [OWASP Third Party JavaScript Management Cheat Sheet](https://www.owasp.org/index.php/3rd_Party_Javascript_Management_Cheat_Sheet)

V13: API、Web サービスの検証要件

1. 管理目標

信頼されたサービスレイヤ API（一般的に JSON や XML、または GraphQL）を使用する検証対象アプリケーションが以下を備えていることを確認します。

* すべての Web サービスで適切な認証、セッション管理および認可
* 低信頼レベルから高信頼レベルに移行する全てのパラメータの入力正当性確認
* クラウドやサーバレス API を含む全ての API の種類に対して有効なセキュリティ管理策の実施

この章を他の全ての章と組み合わせて同じレベルで読んでください。 認証や API セッション管理の課題については重複しません。

1. V13.1 一般的な Web サービスセキュリティの検証要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **13.1.1** | SSRF 攻撃や RFI 攻撃で使用される可能性があるような、異なる URI またはファイルのパーサを悪用する攻撃を回避するために、すべてのアプリケーションコンポーネントが同じエンコードおよびパーサを使用する。 | ✓ | ✓ | ✓ | 116 |
| **13.1.2** | Web サービスアプリケーション内の管理機能にアクセスできるのは、アクセスが許可された 管理者のみとなっている。 | ✓ | ✓ | ✓ | 419 |
| **13.1.3** | API URL が API Key やセッショントークンなどの機密情報を公開していない。 | ✓ | ✓ | ✓ | 598 |
| **13.1.4** | 認可の判定が、URI とリソースレベルの両方で行われている（URI ではコントローラまたはルータで実施するプログラム型または宣言型のセキュリティによって、リソースレベルではモデルベースの許可によって実  施される）。 |  | ✓ | ✓ | 285 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **13.1.5** | 予期しないまたは欠落している Content Type を含むリクエストが、適切なヘッダ（HTTP レスポンスステータス 406 Unacceptable または  415 Unsupported Media Type）でリジェクトされる。 | ✓ | ✓ | 434 |

1. V13.2 RESTful Web サービスの検証要件

JSON schema のバリデーションの標準化のドラフト段階にあります（リファレンスを参照）。SOAP Web サービスのベストプラクティスである JSON schema バリデーションの使用を検討するときは、JSON schema バリデーションと組み合わせ以下の追加のデータ検証の戦略を使用することを検討してください。

* 不足している要素や余分な要素があるかなど、JSON オブジェクトの解析検証
* データタイプ、データ形式、長さなどの標準入力検証メソッドを使用した JSON オブジェクト値のバリデーション
* そして、正式な JSON schema のバリデーション

JSON schema のバリデーション標準が正式化されると、ASVS はこの領域でのアドバイスを更新します。使用中の JSON schema バリデーションのライブラリを注意深く監視します。標準が正式になり、バグがリファレンス実装から解決されるまで、定期的に更新する必要があります。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **13.2.1** | 保護された API またはリソースに対して通常ユーザが DELETE またはPUT を使用するのを防ぐなど、有効化されている RESTful HTTP メソッドが、ユーザまたはアクションにとって妥当となっている。 | ✓ | ✓ | ✓ | 650 |
| **13.2.2** | JSON スキーマバリデーションが設定され、入力を受け付ける前に確認されている。 | ✓ | ✓ | ✓ | 20 |
| **13.2.3** | Cookie を使用する RESTful Web サービスが、次のうち少なくとも 1 つ以上を使って、クロスサイトリクエストフォージェリから保護されている。三重または二重送信クッキーパターン（[参考文献](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)）、CSRF ノン  ス、ORIGIN リクエストヘッダのチェック。 | ✓ | ✓ | ✓ | 352 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **13.2.4** | 特に API が認証不要な場合、過剰な呼び出しから保護するための耐自動化管理策が REST サービスにある。 | ✓ | ✓ | 779 |
| **13.2.5** | 受信した Content-Type が application/xml や application/JSON などの予期されるものであることを、REST サービスが明示的に検査している。 | ✓ | ✓ | 436 |
| **13.2.6** | メッセージヘッダとペイロードが信頼でき、転送中に変更されていない。機密性、完全性の保護のため、転送に強力な暗号化（TLS のみ）を要求することは、多くの場合これで十分です。メッセージごとのデジタル署名は、高度なセキュリティを必要とするアプリケーションに対して、転送保護に加えて追加の保証を提供することができますが、複雑さ  やリスクをもたらす可能性があります。 | ✓ | ✓ | 345 |

1. V13.3 SOAP Web サービスの検証要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **13.3.1** | 適切に形成された XML 文書を確保するために、XSD スキーマバリデーションに続いて、そのデータの処理が行われる前に各入力フィールドのバリデーションが実施されている。 | ✓ | ✓ | ✓ | 20 |
| **13.3.2** | クライアントとサービス間の信頼できる転送を確保するために、メッセージペイロードが WS-Security を使用して署名されている。 |  | ✓ | ✓ | 345 |

注：DTD に対する XXE 攻撃の問題があるため、DTD 検証は使用しないでください。また、V14 構成で設定された要件に従って、フレームワーク DTD 評価を無効にしてください。

1. V13.4 GraphQL や他の Web サービスデータレイヤのセキュリティ要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **13.4.1** | 高コストで、ネストされたクエリの結果として GraphQL またはデータレイヤエクスプレッションがサービス運用妨害（DoS）となることを防  止するために、クエリホワイトリストまたは、Depth 制限と量の制限 |  | ✓ | ✓ | 770 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | の組み合わせを使用している。より高度なシナリオでは、クエリコスト  分析を使用する必要があります。 |  |  |  |
| **13.4.2** | GraphQL または他のデータレイヤの認可ロジックが、GraphQL レイヤではなくビジネスロジックレイヤに実装されている。 | ✓ | ✓ | 285 |

1. 参考情報

詳しくは以下の情報を参照してください。

* [OWASP Serverless Top 10](https://www.owasp.org/images/5/5c/OWASP-Top-10-Serverless-Interpretation-en.pdf)
* [OWASP Serverless Project](https://www.owasp.org/index.php/OWASP_Serverless_Top_10_Project)
* [OWASP Testing Guide 4.0: Configuration and Deployment Management Testing](https://www.owasp.org/index.php/Testing_for_configuration_management)
* [OWASP Cross-Site Request Forgery cheat sheet](https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.md#triple-submit-cookie)
* [OWASP XML External Entity Prevention Cheat Sheet - General Guidance](https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.md#general-guidance)\* [JSON Web Tokens (and Signing)](https://jwt.io/)
* [REST Security Cheat Sheet](https://www.owasp.org/index.php/REST_Security_Cheat_Sheet)
* [JSON Schema](https://json-schema.org/specification.html)
* [XML DTD Entity Attacks](https://www.vsecurity.com/download/publications/XMLDTDEntityAttacks.pdf)
* [Orange Tsai - A new era of SSRF Exploiting URL Parser In Trending Programming Languages](https://www.blackhat.com/docs/us-17/thursday/us-17-Tsai-A-New-Era-Of-SSRF-Exploiting-URL-Parser-In-Trending-Programming-Languages.pdf)

V14: 構成の検証要件

1. 管理目標

検証済みのアプリケーションに以下が含まれていることを確認します。

* 安全で、再現性があり、自動化可能なビルド環境
* サードパーティのライブラリ、依存関係、構成管理を強化し、アプリケーションに古いコンポーネントや安全でないコンポーネントが含まれないようにします
* 管理者とユーザが既定のセキュリティ体制を弱める必要がある、セキュアバイデフォルト構成

既定のアプリケーションを構成することは、インターネット上で安全である必要があり、安全に構成する必要があります。

1. V14.1 ビルド

ビルドパイプラインは再現性のあるセキュリティの基盤です。安全でない何かが発見されるたびに、それをソースコード、ビルドまたはデプロイスクリプトで解決し、自動的にテストが可能。既知のセキュリティの問題が本番環境に展開されないようにビルドを警告または中断する自動セキュリティおよび依存関係のチェックを備えたビルドパイプラインの使用を強く勧めます。不規則に実行される手動手順は、回避可能なセキュリティのミスに直結します。

業界として DevSecOps モデルに移行するにつれ、「Known good（既知の良好な）」状態を実現するには、デプロイメントと構成の継続的な可用性と整合性を確保することが重要。以前はシステムがハッキングされた場合に、それ以上の侵害が生じていないことを証明するのに数日から数か月かかりまし

た。今日では、ソフトウェア定義のインフラストラクチャ、ダウンタイム無しでの迅速な A/B デプロイメント、そして自動化コンテナ化されたビルドでは、侵害された「既知の良好な」代替品を自動的かつ継続的にビルド、強化、デプロイすることができます。

もし従来のモデルがまだ存在する場合は、その構成を強化してバックアップするために手動の手順を実行し、侵害されたシステムを整合性の高い妥協のないシステムに迅速に交換できるようにする必要があります。

このセクションに準拠するには、自動ビルドシステムと、ビルドおよびデプロイスクリプトへのアクセ スが必要です。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **14.1.1** | アプリケーションのビルドおよびデプロイプロセスが、CI / CD の自動化、自動構成管理、自動デプロイスクリプトなどの安全で再現性のある方法で実行されている。 |  | ✓ | ✓ |  |
| **14.1.2** | コンパイラフラグが、スタックのランダム化、データ実行防止などの利用可能なすべてのバッファオーバーフローの保護と警告を有効にし、安全でないポインタ、メモリ、フォーマット文字列、整数、または文字列操作が見つかった場合にビルドを中断するように構成されている。 |  | ✓ | ✓ | 120 |
| **14.1.3** | 使用しているアプリケーションサーバとフレームワークの推奨事項に従って、サーバ構成が強化されている。 |  | ✓ | ✓ | 16 |
| **14.1.4** | アプリケーション、構成、およびすべての依存関係が、自動でデプロイスクリプトを使用して再度デプロイできるか、文書化およびテストされた Runbook から妥当な時間で構築できるか、またはバックアップからタイムリーに復元できる。 |  | ✓ | ✓ |  |
| **14.1.5** | 許可された管理者が、セキュリティ関連のすべての構成の整合性を検証して改ざんを検出できる。 |  |  | ✓ |  |

1. V14.2 依存関係

依存関係の管理は、あらゆる種類のあらゆるアプリケーションの安全な運用に欠かせません。 古くなった、または安全でない依存関係で最新の状態を維持できないことは、これまでで規模が大きく、とても高くつく攻撃の根本的な原因です。

注：レベル 1 では、14.2.1 の準拠は、より正確なビルド時の静的コード分析または依存関係分析では なく、クライアント側およびその他のライブラリとコンポーネントの観察または検出に関係します。 これらのより正確な手法は、必要に応じてインタビューによって発見できる場合があります。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **14.2.1** | すべてのコンポーネントが最新となっている。できればビルド時またはコンパイル時にディペンデンシチェッカを使用する。 ([C2](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) | ✓ | ✓ | ✓ | 1026 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **14.2.2** | サンプルアプリケーション、プラットフォームのドキュメント、デフォルトまたはサンプルのユーザなど、不要な機能、ドキュメント、サンプ ル、コンフィギュレーションがすべて削除されている。 | ✓ | ✓ | ✓ | 1002 |
| **14.2.3** | JavaScript ライブラリ、CSS スタイルシート、Web フォントなどのアプリケーション資産がコンテンツ配信ネットワーク（CDN）または外部プロバイダで外部的にホストされている場合、資産の整合性を検証するためにサブリソース完全性（SRI）が使用されている。 | ✓ | ✓ | ✓ | 714 |
| **14.2.4** | サードパーティのコンポーネントが、事前に定義され、信頼され、継続的に維持されるリポジトリからのものとなっている。 ([C2](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 829 |
| **14.2.5** | 使用しているすべてのサードパーティライブラリのインベントリカタログが維持されている。 ([C2](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ |  |
| **14.2.6** | サードパーティのライブラリをサンドボックス化またはカプセル化して、必要な動作だけをアプリケーションに公開することで、攻撃対象領  域を最小化する。 ([C2](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab%3DFormal_Numbering)) |  | ✓ | ✓ | 265 |

1. V14.3 意図しないセキュリティの開示の要件

本番環境の構成を強化して、デバッグコンソールなどの一般的な攻撃から保護し、クロスサイトスクリプティング（XSS）とリモートファイルインクルード（RFI）攻撃の基準を引き上げ、歓迎されない多 くのペネトレーションテストの報告の特徴である発見された些細な脆弱性を排除します。

これらの問題の多くはめったに重大なリスクとして評価されませんが、他の脆弱性と連鎖します。これらの問題がデフォルトで存在しない場合、ほとんどの攻撃が成功する前にレベルが引き上げられます。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **14.3.1** | Web またはアプリケーションサーバとフレームワークのエラーメッセージが、意図しないセキュリティ情報の開示を排除するために、ユーザが実行可能なカスタマイズされた応答を返すように構成されている。 | ✓ | ✓ | ✓ | 209 |
| **14.3.2** | Web またはアプリケーションサーバとアプリケーションフレームワークのデバッグモードが運用環境で無効になっていることを確認して、デ | ✓ | ✓ | ✓ | 497 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | バッグ機能、開発者コンソール、および意図しないセキュリティ開示を  排除する。 |  |  |  |  |
| **14.3.3** | HTTP ヘッダまたは HTTP レスポンスの一部がシステムコンポーネントの詳細なバージョン情報を公開していない。 | ✓ | ✓ | ✓ | 200 |

1. V14.4 HTTP セキュリティヘッダの要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |
| **14.4.1** | すべての HTTP レスポンスに、安全な文字セット（例：UTF-8、ISO 8859-1）を指定するコンテントタイプヘッダが含まれている。 | ✓ | ✓ | ✓ | 173 |
| **14.4.2** | す べ て の API レ ス ポ ン ス に Content-Disposition:attachment; filename="api.json"が含まれている（または他のコンテントタイプの 適切なファイル名）。 | ✓ | ✓ | ✓ | 116 |
| **14.4.3** | HTML、DOM、JSON、JavaScript インジェクションの脆弱性などのXSS 攻撃の影響を軽減するのに役立つ Content Security Policy (CSPv2) が配置されている。 | ✓ | ✓ | ✓ | 1021 |
| **14.4.4** | すべてのレスポンスに X-Content-Type-Options：nosniff が含まれている。 | ✓ | ✓ | ✓ | 116 |
| **14.4.5** | HTTP Strict Transport Security ヘッダがすべてのレスポンスとすべてのサブドメインに含まれている。例えば、Strict-Transport-Security： max-age = 15724800; | ✓ | ✓ | ✓ | 523 |
| **14.4.6** | 「no-referrer」や「same-origin」のような、適切な「Referrer- Policy」ヘッダが含まれている。 | ✓ | ✓ | ✓ | 116 |
| **14.4.7** | サードパーティのサイトに埋め込むべきではないサイトで、適切なヘッダが（X-Frame-Options または Content-Security-Policy：frame-  ancestors）が、サイトで使用されている。 | ✓ | ✓ | ✓ | 346 |

1. V14.5 HTTP リクエストヘッダのバリデーションの要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | CWE |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **14.5.1** | アプリケーションサーバが、pre-flight OPTIONS を含む、アプリケーションまたは API で使用されている HTTP メソッドのみを受け入れる。 | ✓ | ✓ | ✓ | 749 |
| **14.5.2** | 提供された Origin ヘッダは、攻撃者によって簡単に変更できるため、認証やアクセス制御の判断に使用されていない。 | ✓ | ✓ | ✓ | 346 |
| **14.5.3** | オリジン間リソース共有（CORS）の Access-Control-Allow-Origin ヘッダが信頼できるドメインの厳密なホワイトリストを使用して照合し、  「null」オリジンをサポートしていない。 | ✓ | ✓ | ✓ | 346 |
| **14.5.4** | 信頼できるプロキシまたは bearer トークンのような SSO デバイスによって追加された HTTP ヘッダがアプリケーションによって認証されている。 |  | ✓ | ✓ | 306 |

1. 参考情報

詳しくは以下の情報を参照してください。

* [OWASP Testing Guide 4.0: Testing for HTTP Verb Tampering](https://www.owasp.org/index.php/Testing_for_HTTP_Verb_Tampering_%28OTG-INPVAL-003%29)
* Content-Disposition の API レスポンスへの追加はクライアントとサーバ間の MIME タイプの誤認識におよびファイル名オプションによる多くの攻撃から防御するのに役立つ。[Reflected File Download attacks.](https://www.blackhat.com/docs/eu-14/materials/eu-14-Hafif-Reflected-File-Download-A-New-Web-Attack-Vector.pdf)
* [Content Security Policy Cheat Sheet](https://www.owasp.org/index.php?title=Content_Security_Policy_Cheat_Sheet)
* [Exploiting CORS misconfiguration for BitCoins and Bounties](https://portswigger.net/blog/exploiting-cors-misconfigurations-for-bitcoins-and-bounties)
* [OWASP Testing Guide 4.0: Configuration and Deployment Management Testing](https://www.owasp.org/index.php/Testing_for_configuration_management)
* [Sandboxing third party components](https://www.owasp.org/index.php/3rd_Party_Javascript_Management_Cheat_Sheet#Sandboxing_Content)

Appendix A: 用語集

* **二要素認証(2FA) –** 2 要素認証は、アカウントログインに第 2 レベルの認証を追加したもの
* **アドレス空間配置のランダム化(ASLR) –** メモリ破損のバグ悪用をより困難にする手法
* **アプリケーションセキュリティ(Application Security)** – OS やネットワークではなく，OSI 参照モデルのアプリケーション層を構成するコンポーネントの分析に重点をおく、アプリケーションレベルのセキュリティ
* **アプリケーションセキュリティ検証(Application Security Verification)** – OWASP ASVS に沿って実施するアプリケーションの技術的評価
* **アプリケーションセキュリティ検証報告書(Application Security Verification Report)** – 対象となるアプリケーションの分析と検証結果をまとめた報告書
* **認証(Authentication)** – アプリケーションのユーザが正当であることの検証
* **自動検証(Automated Verification)** – シグネチャを使って脆弱性を見つける自動ツール(動的解析ツール、静的解析ツール、その両方)を用いた検査
* **ブラックボックステスト(Black box testing)** – アプリケーションの内部構造や仕組みを調べずにアプリケーションの機能を調べるソフトウェアテストの方法
* **コンポーネント(Component)** – 独立したコード単位。ディスクや他のコンポーネントと通信するネットワークインターフェイスとの関連をもちます
* **クロスサイトスクリプティング(Cross-Site Scripting (XSS))** – クライアントからコンテンツへのスクリプトの注入を可能にする、Web アプリケーションに典型的なセキュリティ上の脆弱性
* **暗号モジュール(Cryptographic module)** – 暗号アルゴリズムを実装し、暗号鍵を生成する、ハードウェアやソフトウェア、ファームウェア
* **CWE** - Common Weakness Enumeration（CWE）は、コミュニティが開発した一般的なソフトウェアセキュリティの弱点一覧。共通言語、ソフトウェアセキュリティツールの測定基準、および脆弱性の特定・軽減・防止の取り組みのベースラインとして機能します
* **DAST** – 動的アプリケーションセキュリティテスト（DAST）技術は、実行状態にあるアプリケーションのセキュリティの脆弱性を示す状況を検出するように設計されています
* **設計検証(Design Verification)** – アプリケーションのセキュリティアーキテクチャに関する技術的評価
* **動的検証(Dynamic Verification)** – アプリケーションの実行中に脆弱性のシグネチャを用いて問題点を検出する自動化ツールを使用すること
* **グローバル一意識別子（GUID）** – ソフトウェアで識別子として使用される一意の照会番号
* **HTTP** – 分散、コラボレーション、ハイパーメディア情報システム用のアプリケーションプロトコル．World Wide Web におけるデータ通信の基盤
* **ハードコードされた鍵(Hardcoded keys)** – コード、コメント、ファイルなど、ファイルシステムに格納されている暗号化鍵
* **入力バリデーション(Input Validation)** – 信頼できないユーザ入力を正規化およびバリデーションします
* **悪性コード(Malicious Code)** – アプリケーションの開発時にアプリケーションのオーナに気付かれることなく導入されるコードであり，アプリケーションのセキュリティポリシーを回避します。ウイルスやワームなどのマルウェアとは異なります！
* **マルウェア(Malware)** – アプリケーションの実行時に、ユーザや管理者に気付かれることなくアプリケーションに侵入する実行コード
* **Open Web Application Security Project (OWASP)** – The Open Web Application Security Project (OWASP) は、アプリケーションソフトウェアのセキュリティ向上に注力する、自由でオープンなコミュニティ。OWASP のミッションは、アプリケーションのセキュリティを"見える化" することで、人や組織が、アプリケーションセキュリティのリスクについて十分な情報に基づいた決断を下すことができることです。<http://www.owasp.org/>を参照
* **個人を特定できる情報 Personally Identifiable Information (PII)** - 単独または他の情報と共に使用して、1 人の人物を識別したり、連絡したり、居場所を特定したり、または状況に応じて個人を識別したりできる情報
* **位置独立実行形式(PIE)** – 位置独立実行可能ファイル（PIE）は、1 次メモリのどこかに配置されて、絶対アドレスに関係なく適切に実行される機械語
* **公開鍵暗号基盤(PKI)** – 公開鍵暗号基盤（PKI）は、公開鍵をエンティティのそれぞれの ID にバインドする取り決めです。バインディングは、認証局（CA）での証明書の登録および発行のプロセスを通じて確立
* **SAST** – 静的アプリケーションセキュリティテスト（SAST）は、アプリケーションのソースコー

ド、バイトコード、セキュリティの脆弱性を示すコーディングおよびバイナリを分析するために設計された一連の技術。SAST ソリューションは、実行されていない状態の「インサイドアウト」からアプリケーションを分析

* **SDLC** – ソフトウェア開発ライフサイクル
* **セキュリティアーキテクチャ(Security Architecture)** – アプリケーションの設計を抽象化したも の。どこでどのようにセキュリティ管理策を使用しているか、また、ユーザデータとアプリケーションデータを保持する場所とデータの機密性について記述します
* **セキュリティ設定(Security Configuration)** – アプリケーションにおけるセキュリティの管理を左右するランタイム設定
* **セキュリティ管理(Security Control)** – セキュリティチェック(例:アクセス制御の検査など)を実行する、あるいは呼出し結果がセキュリティに影響を与えうる(例：監査レコードの生成など)、機能や構成要素
* **SQL インジェクション(SQL Injection)** – データ駆動型アプリケーションに対する攻撃に使用されるコードインジェクション技法の 1 つ。悪性 SQL 文がデータの入力箇所に挿入されます
* **SSO アプリケーション(SSO Application)** – シングルサインオン（SSO）は、ユーザが 1 つのアプリケーションにログインした後に、再認証を必要とせずに自動的に他のアプリケーションにログインする。例えば、Google にログインすると、Youtube、Google Docs、Gmail などの他のGoogle サービスにアクセスすると、自動的にログインします
* **脅威モデリング(Threat Modelling)** - 脅威の主体、セキュリティゾーン、セキュリティ管理、重要な技術資産やビジネス資産を明らかにするための、精緻なセキュリティアーキテクチャの構築に基づく手法
* **Transport Layer Security** – ネットワークの通信セキュリティを提供する暗号プロトコル
* **URI/URL/URL フラグメント(URI/URL/URL fragments)** – Uniform Resource Identifier (URI) は、名前または Web リソースを識別するために使用される文字列。多くの場合リソースへの参照として使用されます
* **検証者(Verifier)** – OWASP ASVS の要件に基づいてアプリケーションをレビューする個人またはグループ
* **ホワイトリスト(Whitelist)** – アプリケーションにおいて許可されているデータまたは操作のリスト

(例：入力バリデーションで許可されている文字のリストなど)

* **X.509 証明書(X.509 Certificate)** – X.509 証明書は、広く受け入れられている国際的な X.509 公開鍵暗号基盤（PKI）標準を使用して、公開鍵が証明書に含まれるユーザやコンピュータまたはサービス ID に属していることを確認するデジタル証明書

Appendix B: 参考情報

以下の OWASP プロジェクトは、この基準のユーザや採用者に役立つ可能性が高い:

1. OWASP 主要プロジェクト
2. OWASP Top 10 Project: https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project
3. OWASP Testing Guide: <https://www.owasp.org/index.php/OWASP_Testing_Project>
4. OWASP Proactive Controls: <https://www.owasp.org/index.php/OWASP_Proactive_Controls>
5. OWASP Security Knowledge Framework:<https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework>
6. OWASP Software Assurance Maturity Model (SAMM):<https://www.owasp.org/index.php/OWASP_SAMM_Project>
7. Mobile Security Related Projects
8. OWASP Mobile Security Project:<https://www.owasp.org/index.php/OWASP_Mobile_Security_Project>
9. OWASP Mobile Top 10 Risks: [https://www.owasp.org/index.php/Projects/OWASP\_Mobile\_Security\_Project\_-](https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks)

[\_Top\_Ten\_Mobile\_Risks](https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks)

1. OWASP Mobile Security Testing Guide:<https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide>
2. OWASP Internet of Things related projects

1. OWASP Internet of Things Project:<https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project>

1. OWASP Serverless projects

1. OWASP Serverless Project:<https://www.owasp.org/index.php/OWASP_Serverless_Top_10_Project>

1. Others

同様に、次の Web サイトは、この標準のユーザ/採用者にとって有用である可能性が最も高い

1. SecLists Github: <https://github.com/danielmiessler/SecLists>
2. MITRE Common Weakness Enumeration: <https://cwe.mitre.org/>
3. PCI Security Standards Council: [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org/)
4. PCI Data Security Standard (DSS) v3.2.1 Requirements and Security Assessment Procedures:<https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf>
5. PCI Software Security Framework - Secure Software Requirements and Assessment Procedures: [https://www.pcisecuritystandards.org/documents/PCI-Secure-Software- Standard-v1\_0.pdf](https://www.pcisecuritystandards.org/documents/PCI-Secure-Software-Standard-v1_0.pdf)
6. PCI Secure Software Lifecycle (Secure SLC) Requirements and Assessment Procedures:<https://www.pcisecuritystandards.org/documents/PCI-Secure-SLC-Standard-v1_0.pdf>

Appendix C: IoT 検証要件

このセクションは元々メインブランチにありましたが、OWASP IoT チームが行った作業によって、このテーマに関する 2 つの異なる基準を維持することは意味がありません。4.0 リリースでは、これを付録に移動し、これを必要とするすべての人に、メインの [OWASP IoT プロジェクト](https://owasp.org/www-project-internet-of-things/)を使用することを推奨します。

1. 管理目標

組み込み/IoT 機器は、

* 信頼できる環境でセキュリティ管理を実施することによって、サーバ内と同じレベルのセキュリティ管理をデバイス内でも行う
* デバイスに保存されている機密データは、セキュアエレメントなどのハードウェアに保護されたストレージを使用して、安全な方法で実行する必要があります
* デバイスから送信されるすべての機密データは、TLS を利用する必要があります

1. セキュリティ検証要件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 説明 | L1 | L2 | L3 | Since |
| **C.1** | USB、UART、そして他のシリアルバリアントのような、アプリケーション層のデバッグインターフェイスが無効になっているか、複雑なパスワードによって保護されている。 | ✓ | ✓ | ✓ | 4.0 |
| **C.2** | 暗号鍵と証明書が各デバイスに固有となっている。 | ✓ | ✓ | ✓ | 4.0 |
| **C.3** | ASLR や DEP などのメモリ保護制御が、組み込み/ IoT オペレーティングシステムによって有効になっている（該当する場合）。 | ✓ | ✓ | ✓ | 4.0 |
| **C.4** | JTAG や SWD などのオンチップデバッグインターフェイスが無効になっている、または使用可能な保護メカニズムが有効になっていて適切に構成されている。 | ✓ | ✓ | ✓ | 4.0 |
| **C.5** | SoC デバイスまたは CPU で利用可能な場合、Trusted Execution が実装および有効になっている。 | ✓ | ✓ | ✓ | 4.0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **C.6** | 機密データ、秘密鍵、そして証明書が、セキュアエレメント、TPM、TEE  （Trusted Execution Environment）に安全に保存されていること、または強力な暗号化を使用して保護されている。 | ✓ | ✓ | ✓ | 4.0 |
| **C.7** | ファームウェアアプリが Transport Layer Security（トランスポートレイヤセキュリティ）を使用して伝送中のデータを保護している。 | ✓ | ✓ | ✓ | 4.0 |
| **C.8** | ファームウェアアプリがサーバ接続のデジタル署名を検証する。 | ✓ | ✓ | ✓ | 4.0 |
| **C.9** | ワイヤレス通信が相互に認証されている。 | ✓ | ✓ | ✓ | 4.0 |
| **C.10** | ワイヤレス通信が暗号化されたチャネルを介して送信される。 | ✓ | ✓ | ✓ | 4.0 |
| **C.11** | 禁止された C 関数の使用が適切な安全な同等の関数に置き換えられている。 | ✓ | ✓ | ✓ | 4.0 |
| **C.12** | 各ファームウェアがサードパーティのコンポーネント、バージョン、および公開された脆弱性をカタログ化するソフトウェア部品表を維持している。 | ✓ | ✓ | ✓ | 4.0 |
| **C.13** | サードパーティのバイナリ、ライブラリ、フレームワークを含むすべてのコードがハードコードされたクレデンシャル（バックドア）についてレビューされている。 | ✓ | ✓ | ✓ | 4.0 |
| **C.14** | シェルコマンドラッパー、スクリプトを呼び出して、アプリケーションおよびファームウェアコンポーネントが OS コマンドインジェクションの影響を受けないこと、またはセキュリティ制御により OS コマンドインジェクションが阻止されている。 | ✓ | ✓ | ✓ | 4.0 |
| **C.15** | ファームウェアのアプリが信頼できるサーバを固定化している。 |  | ✓ | ✓ | 4.0 |
| **C.16** | 耐タンパ性または、改ざん検知機能が存在する。 |  | ✓ | ✓ | 4.0 |
| **C.17** | チップ製造者による、有用な知的財産権保護技術が有効化されている。 |  | ✓ | ✓ | 4.0 |
| **C.18** | ファームウェアのリバースエンジニアリングを防止するためのセキュリティ管理策（デバッグ情報の除去など）が実施されている。 |  | ✓ | ✓ | 4.0 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **C.19** | デバイスが、ブートイメージのロード前に署名の検証を行う。 | ✓ | ✓ | 4.0 |
| **C.20** | ファームウェアの更新処理が TOCTOU 攻撃に対して脆弱でない。 | ✓ | ✓ | 4.0 |
| **C.21** | デバイスがコード署名を利用し、インストール前にファームウェアのアップグレードファイルの検証を行う。 | ✓ | ✓ | 4.0 |
| **C.22** | デバイスが、古いバージョンのファームウェアにダウングレードしない。 | ✓ | ✓ | 4.0 |
| **C.23** | 暗号論的に安全な擬似乱数生成器が、組込み機器上で使用されていること（例えば、チップが提供する乱数生成器を使用している等）。 | ✓ | ✓ | 4.0 |
| **C.24** | ファームウェアが事前設定のスケジュールに従って、ファームウェアの自動更新を実行する。 | ✓ | ✓ | 4.0 |
| **C.25** | 改ざんを検知、不正なメッセージを受信した際に、デバイスがファームウェアおよび機密データをワイプする。 |  | ✓ | 4.0 |
| **C.26** | デバッグ用インターフェース（JTAG/SWD など）を無効化できるマイクロコントローラだけが使用されている。 |  | ✓ | 4.0 |
| **C.27** | デキャップやサイドチャネル攻撃から防御できるマイクロコントローラを使用する。 |  | ✓ | 4.0 |
| **C.28** | 機微な痕跡がプリント基板の外部レイヤに漏えいしない。 |  | ✓ | 4.0 |
| **C.29** | チップ間の通信（メインボードからドーターボードへの通信など）を暗号化している。 |  | ✓ | 4.0 |
| **C.30** | デバイスがコード署名を使用し、実行前にコードの妥当性の検証を行う。 |  | ✓ | 4.0 |
| **C.31** | メモリ内に保持される機密な情報が、不要になったら直ちにゼロで上書きされる。 |  | ✓ | 4.0 |
| **C.32** | ファームウェアアプリがアプリ分離のため、カーネルコンテナを利用している。 |  | ✓ | 4.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **C.33** | ファームウェアが -fPIE、-fstack-protector-all、-Wl、-z、noexecstack、-Wl、-z、noexecheap などの安全なコンパイルフラグでビルドされている。 | ✓ | 4.0 |
| **C.34** | （該当する場合）マイクロコントローラが、コードプロテクションを利用している。 | ✓ | 4.0 |

1. 参考情報

詳しくは以下の情報を参照してください。

* [OWASP Internet of Things Top 10](https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf)
* [OWASP Embedded Application Security Project](https://www.owasp.org/index.php/OWASP_Embedded_Application_Security)
* [OWASP Internet of Things Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project)
* [Trudy TCP Proxy Tool](https://github.com/praetorian-inc/trudy)

1. https://public.cyber.mil/stigs/ [↑](#footnote-ref-1)
2. https://www.stigviewer.com/ https://cyber.trackr.live/stig [↑](#footnote-ref-2)
3. https://www.cisecurity.org/cis-benchmarks/ [↑](#footnote-ref-3)
4. https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-security-baselines [↑](#footnote-ref-4)
5. https://github.com/microsoft/SecCon-Framework/blob/master/windows-security-configuration-framework.md [↑](#footnote-ref-5)
6. https://creativecommons.org/licenses/by-sa/4.0/legalcode.ja [↑](#footnote-ref-6)
7. https://www.ipa.go.jp/security/videos/list.html [↑](#footnote-ref-7)
8. https://www.theregister.co.uk/2019/02/14/password\_length/ [↑](#footnote-ref-8)
9. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/all-your-creds-are-belong-to-us/ba-p/855124 [↑](#footnote-ref-9)
10. NIST SP800-63-3 の OpenID ファウンデーション・ジャパンによる邦訳: https://openid-foundation-japan.github.io/800-63-3-final/index.ja.html [↑](#footnote-ref-10)
11. https://attack.mitre.org/techniques/T1562/002/ [↑](#footnote-ref-11)
12. https://www.microsoft.com/ja-jp/download/details.aspx?id=24659 [↑](#footnote-ref-12)
13. NIST SP800-63-3翻訳版63-Bパートの紹介を参考にしました。https://www.slideshare.net/kthrtty/20171027-nist-sp80063bkthrtty-81333156 [↑](#footnote-ref-13)
14. 出典：生体認証システムの脆弱性の分析と生体検知技術の研究動向   
    <https://www.imes.boj.or.jp/research/papers/japanese/kk28-3-4.pdf> [↑](#footnote-ref-14)
15. JPCERT/CC Java コーディングスタンダード CERT/Oracle版 https://www.jpcert.or.jp/java-rules/msc03-j.html [↑](#footnote-ref-15)
16. Of Passwords and People:Measuring the Effect of Password-Composition Policies : https://users.ece.cmu.edu/~lbauer/papers/2011/chi2011-passwords.pdf [↑](#footnote-ref-16)
17. Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords : http://www.cs.umd.edu/~jkatz/security/downloads/passwords\_revealed-weir.pdf [↑](#footnote-ref-17)
18. Windows 堅牢化のためのセキュリティ構成フレームワーク https://aka.ms/SecconJP [↑](#footnote-ref-18)
19. Windows でグループ ポリシー管理用テンプレート用のセントラル ストアを作成および管理する方法https://support.microsoft.com/ja-jp/help/3087759/how-to-create-and-manage-the-central-store-for-group-policy-administra [↑](#footnote-ref-19)
20. https://www.microsoft.com/en-us/download/confirmation.aspx?id=55319 [↑](#footnote-ref-20)
21. https://docs.microsoft.com/ja-jp/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3 [↑](#footnote-ref-21)
22. Microsoft Security Compliance Toolkit 1.: https://www.microsoft.com/en-us/download/confirmation.aspx?id=55319 [↑](#footnote-ref-22)
23. https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/bb530324(v=msdn.10)?redirectedfrom=MSDN [↑](#footnote-ref-23)
24. https://docs.microsoft.com/ja-jp/onedrive/use-group-policy [↑](#footnote-ref-24)
25. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-pku2u-authentication-requests-to-this-computer-to-use-online-identities> [↑](#footnote-ref-25)
26. Microsoft Security Compliance Toolkit 1.: https://www.microsoft.com/en-us/download/confirmation.aspx?id=55319 [↑](#footnote-ref-26)
27. http://support.microsoft.com/kb/951016. [↑](#footnote-ref-27)
28. https://support.microsoft.com/kb/2696547 [↑](#footnote-ref-28)
29. https://support.microsoft.com/kb/2696547 [↑](#footnote-ref-29)
30. http://support.microsoft.com/kb/2871997,  
     <http://blogs.technet.com/b/srd/archive/2014/06/05/an-overview-of-kb2871997.aspx> [↑](#footnote-ref-30)
31. https://attack.mitre.org/techniques/T1543/003/ [↑](#footnote-ref-31)
32. https://attack.mitre.org/techniques/T1059/003/ [↑](#footnote-ref-32)
33. https://www.jpcert.or.jp/research/20160628ac-ir\_research.pdf [↑](#footnote-ref-33)
34. https://attack.mitre.org/techniques/T1059/001/ [↑](#footnote-ref-34)
35. https://www.atmarkit.co.jp/ait/articles/0805/16/news139.html [↑](#footnote-ref-35)
36. https://www.ired.team/offensive-security/code-execution/powershell-without-powershell [↑](#footnote-ref-36)
37. https://devblogs.microsoft.com/powershell/powershell-constrained-language-mode/ [↑](#footnote-ref-37)
38. https://attack.mitre.org/techniques/T1053/002/ [↑](#footnote-ref-38)
39. https://attack.mitre.org/techniques/T1053/005/ [↑](#footnote-ref-39)
40. https://attack.mitre.org/techniques/T1059/ [↑](#footnote-ref-40)
41. https://www.jpcert.or.jp/research/20160628ac-ir\_research.pdf [↑](#footnote-ref-41)
42. https://attack.mitre.org/techniques/T1204/001/ [↑](#footnote-ref-42)
43. https://attack.mitre.org/techniques/T1204/002/ [↑](#footnote-ref-43)
44. https://www.antiphishing.jp [↑](#footnote-ref-44)
45. https://attack.mitre.org/techniques/T1547/001/ [↑](#footnote-ref-45)
46. https://docs.microsoft.com/ja-jp/sysinternals/downloads/autoruns [↑](#footnote-ref-46)
47. https://www.virustotal.com/gui/ [↑](#footnote-ref-47)
48. https://attack.mitre.org/techniques/T1070/004 [↑](#footnote-ref-48)
49. https://attack.mitre.org/techniques/T1027/ [↑](#footnote-ref-49)
50. https://www.cyberfortress.jp/2020/03/25/blog-powershell-obfuscation/ [↑](#footnote-ref-50)
51. F-Secure Hunting for AMSI bypasses: https://blog.f-secure.com/hunting-for-amsi-bypasses/  
    Bypass AMSI by manual modification: https://s3cur3th1ssh1t.github.io/Bypass\_AMSI\_by\_manual\_modification/ [↑](#footnote-ref-51)
52. https://attack.mitre.org/techniques/T1003/ [↑](#footnote-ref-52)
53. https://docs.microsoft.com/ja-jp/windows-server/security/credentials-protection-and-management/protected-users-security-group  
    https://msrc-blog.microsoft.com/2014/06/05/an-overview-of-kb2871997/ [↑](#footnote-ref-53)
54. <https://docs.microsoft.com/ja-jp/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection#BKMK_HowToConfigure>

    追加の LSA の保護の構成: https://docs.microsoft.com/ja-jp/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection [↑](#footnote-ref-54)
55. https://docs.microsoft.com/ja-jp/windows/security/threat-protection/auditing/event-4624 [↑](#footnote-ref-55)
56. https://docs.microsoft.com/ja-jp/windows/security/threat-protection/auditing/event-4776 [↑](#footnote-ref-56)
57. Windows Defender Credential Guard の要件:https://docs.microsoft.com/ja-jp/windows/security/identity-protection/credential-guard/credential-guard-requirements [↑](#footnote-ref-57)
58. https://www.jpcert.or.jp/java-rules/msc03-j.html [↑](#footnote-ref-58)
59. https://www.jpcert.or.jp/sc-rules/c-msc18-c.html [↑](#footnote-ref-59)
60. https://attack.mitre.org/techniques/T1212/ [↑](#footnote-ref-60)
61. https://docs.microsoft.com/ja-jp/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10#understanding-windows-10-in-relation-to-the-enhanced-mitigation-experience-toolkit [↑](#footnote-ref-61)
62. https://news.mynavi.jp/article/win10tips-368/ [↑](#footnote-ref-62)
63. https://docs.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/network-access-let-everyone-permissions-apply-to-anonymous-users [↑](#footnote-ref-63)
64. https://docs.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts [↑](#footnote-ref-64)
65. https://docs.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts-and-shares [↑](#footnote-ref-65)
66. https://docs.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls [↑](#footnote-ref-66)
67. ダイナミック アクセス制御:シナリオの概要: https://docs.microsoft.com/ja-jp/windows-server/identity/solution-guides/dynamic-access-control--scenario-overview [↑](#footnote-ref-67)
68. 日本ネットワークセキュリティ協会 エンタープライズロール管理解説書: https://www.jnsa.org/result/2013/Role-Management-v1.pdf [↑](#footnote-ref-68)
69. https://attack.mitre.org/techniques/T1082/ [↑](#footnote-ref-69)
70. Windows Defender Credential Guard によるドメインの派生資格情報の保護:https://docs.microsoft.com/ja-jp/windows/security/identity-protection/credential-guard/credential-guard [↑](#footnote-ref-70)
71. ネットワーク セキュリティ: NTLM を制限する: 着信 NTLM トラフィックを監査する:https://docs.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-audit-incoming-ntlm-traffic [↑](#footnote-ref-71)
72. https://msdn.microsoft.com/ja-jp/library/dn408187(v=ws.11).aspx [↑](#footnote-ref-72)
73. https://docs.microsoft.com/ja-jp/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection [↑](#footnote-ref-73)
74. https://support.microsoft.com/kb/2871997 [↑](#footnote-ref-74)
75. マイクロソフト セキュリティ アドバイザリ 3062591 Local Administrator Password Solution (LAPS) の提供を開始：https://docs.microsoft.com/ja-jp/security-updates/securityadvisories/2015/3062591?redirectedfrom=MSDN [↑](#footnote-ref-75)
76. https://msrc-blog.microsoft.com/2020/08/26/20200827\_laps/ [↑](#footnote-ref-76)
77. https://docs.microsoft.com/ja-jp/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection#BKMK\_HowToConfigure [↑](#footnote-ref-77)
78. https://attack.mitre.org/techniques/T1048/ [↑](#footnote-ref-78)
79. https://attack.mitre.org/techniques/T1573/ [↑](#footnote-ref-79)