ウェブブラウザのプロテクションプロファイル

本書は、米国政府 DoD 傘下の NSA 情報保証局で作成したプロテクションプロファイルの一部を調達要件の検討のため、参考として日本語に直訳したものです。IT セキュリティ評価及び認証制度における適合 PP として利用する場合は、正式な文書である英語版のみとなります。

正式な文書は、以下の URL よりダウンロード可能です。

https://www.niap-ccevs.org/pp/pp_webbrowser_v1.0.pdf

2014 年 3 月 31 日

バージョン 1.0

平成 26 年 12 月 5 日　翻訳 暫定第 0.1 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

目次

改版履歴

バージョン	日付	内容
1.0	2014 年 3 月 31 日	ウェブブラウザクライアント PP

1 概論

ウェブブラウザは、主にハイパーテキスト転送プロトコル (HTTP) または HTTP セキュア (HTTPS) を用いて、ウェブサーバにより提供されるコンテンツを取り込み、表示するクライアントアプリケーションである。ブラウザは年々複雑さを増し、当初は単純で変化しないウェブページの表示に用いられるツールだったものが、ウェブコンテンツの洗練された実行環境となってきた。アカウントやサーバ、あるいは組み込みシステムをリモート管理するためのブラウザ利用には、秘密情報をセキュアに取り扱うことが要求される。タブや拡張機能､HTML5 のようなイノベーションによりブラウザの機能が強化されるだけでなく、新たなセキュリティ上の懸念ももたらされた。ブラウザはインターネットへアクセスする主要な手段であり、またその複雑さと処理する情報のため、攻撃者のターゲットとなるのは自然の理である。結果として、ウェブブラウザのセキュリティを向上させ、クライアントマシン及びエンタープライズネットワークへのリスクを低減させることが至上命令となる。

本文書では、ウェブブラウザクライアントのセキュリティ機能要件 (SFR) のベースラインセットを提供する。オペレーティングシステムのセキュリティサービスの利用を推奨し、基盤となるプラットフォームにより提供されるサンドボックス化技術と環境緩和効果の利用を要求することにより、ブラウザのセキュリティを向上させることを意図している。さらに､これらの要件はブラウザが提供しなければならない (must) セキュリティ機能を定義している。

本文書中の要件は、基盤となるプラットフォームの構成にかかわらず、任意のオペレーティングシステム上で動作するすべてのウェブブラウザに適用される。

1.1 TOE の概要

本文書の評価対象 (TOE) は､任意のオペレーティングシステムまたはプラットフォーム上で動作可能な､主に HTTP 及び HTTPS を用いてウェブコンテンツの表示に用いられる､任意のウェブブラウザクライアントである。

1.2 TOE の利用方法

ウェブブラウザは多くのタスクの実行に利用されるが、それらは 3 つの主要なユースケースに分類できる。

[ユースケース 1] ウェブサーフィン

ブラウザは､ウェブページ､ストリーミングメディア､画像及び専用フォーマット (例えば、Java、Flash、Word、PDF) など、ウェブ上のコンテンツを取り込み表示するために用いられる。ブラウザはまた、ウェブサイトへコンテンツを書き込むためにも用いることができる (web 2.0 — 例えば、Facebook)。ウェブサーフィンは、インターネットまたはイントラネット上で行われる可能性がある。

[ユースケース 2] リモート管理クライアント

ブラウザは、サーバ、ネットワークデバイス、ならびに SCADA、スマート TV、及びサーモスタットなどの組み込みシステムをはじめとしたシステムにリモート管理インタフェースを提供するために用いられる。ブラウザが未知のサーバと対話するウェブサーフィンの場合とは異なり、リモート管理クライアントとして動作するブラウザは、利用者が信頼するサーバと接続する。

[ユースケース 3] コンテンツ作成

ブラウザは、利用者データ及び記録がオンラインで保存される、Microsoft Office 365、Google Drive、及び Adobe Creative Cloud など、次第に数を増しつつある、サービスとしてのソフトウェア (SaaS) を用いてコンテンツを作成するために用いられる。

2 セキュリティ課題記述

以下に、適合 TOE が対処する課題を記述する。

2.1 脅威

2.1.1 悪意や欠陥のある更新

最もよく利用される攻撃ベクトルは、既知の欠陥を含むソフトウェアのパッチされていないバージョンへの攻撃を利用するものであるため、ブラウザを更新して脅威環境の変化へ確実に対処することが必要となる。パッチを適宜適用することによりクライアントが「攻略しにくい目標 (ハードターゲット)」であることが確実となり、その製品がセキュリティ方針を維持管理し実施できる可能性が増大する。しかし、製品へ適用されるべき更新は何らかの形で信頼できなければならない (must)。そうでなければ、攻撃者がルートキットやボット、あるいはその他のマルウェアなど、自分たちの選択した悪意のあるコードを含んだ独自の「更新」を作成することができてしまう。このような「更新」が一度インストールされると、その後そのシステムとそのデータすべての制御権は攻撃者に握られてしまう。

[T.UNAUTHORIZED_UPDATE]

2.1.2 悪意や欠陥のあるアドオン

ウェブブラウザの機能は、サードパーティ製のユーティリティやツールの統合により拡張可能である。このような能力の拡張されたセットは、ブラウザのプラグイン及び拡張機能の利用により可能となる。基本的なブラウザのコードとプラグインや拡張機能の提供する新しい能力とが緊密に統合されているため、攻撃者により悪意を持って、または開発者により意図されずに、深刻な欠陥をブラウザアプリケーションへ注入できるリスクが増大する。これらの欠陥により、望ましくないふるまいが起こり得る。これには、ブラウザ中の秘密情報への不正アクセスや、そのデバイスのファイルシステムへの不正アクセスを可能とすること、あるいは他のアプリケーションまたはオペレーティングシステムへの不正アクセスを可能とする特権昇格さえもが含まれるが、これらに限定されるものではない。

[T.UNAUTHORIZED_ADD-ON]

2.1.3 ネットワークの盗聴

ネットワークの盗聴には、何らかの潜在的に秘密データの意図された送信先とシステムとの間の送信を監視するため、攻撃者がネットワーク上の位置を手に入れることが必要となる。ウェブブラウザに関しては、例えば公共料金を支払おうとしている利用者とその公共料金のウェブサイトとの間の送信など、ブラウザと 1 つまたは複数のウェブサーバとの間のトランザクションの監視が必要とされる。

[T.NETWORK_EAVESDROP]

2.1.4 ネットワーク攻撃

ネットワーク攻撃は、攻撃者がネットワーク上の位置を手に入れることが必要であるという点で、ネットワークの盗聴と同様である。ネットワークの盗聴と異なる点は、攻撃者がターゲットシステムとの通信を開始すること、あるいはターゲットシステムとデータの正当な送信先との間のデータを改変することが必要となることである。ブラウザに関しては、そのふるまいに影響を与え得る脆弱性を悪用するために、あるいはウェブサーバへ送信されるアカウント情報を改変するために、悪意のあるデータをブラウザへ送信することがネットワーク攻撃に必要となるかもしれない。

ブラウザ攻撃は、一般的にはインターネットに接続されたブラウザへ行われるが、閉じた

ネットワーク内で行われることもないとは言えない。攻撃者は、フィッシングなどのソーシャルエンジニアリングテクニックを用いて、利用者が悪意のあるサイトを訪れるよう仕向けることができる。また利用者は、ウェブブラウジングの途中で意図せず、あるいは意図して悪意のあるサイトを訪れるかもしれない。そしてそのサイトは悪意のあるコンテンツを利用者のブラウザへ提示し、多くの場合には利用者へ何の表示もされずに、ブラウザを悪用してマルウェアのインストールが行われる。これらの攻撃は、ブラウザまたはブラウザ拡張機能の脆弱性に依存する。

ネットワーク攻撃の例をいくつか挙げる。

- セショントークンの不十分な保護により、セションのハイジャックが行われ、トークンが取り込まれてそのセションを開始した利用者の特権を得るために再利用されるおそれがある。
- クロスサイトスクリプティング (XSS) 及びクロスサイトリクエストフォージェリ (CSRF) 攻撃は、ウェブサイトへの利用者クレデンシャルを危殆化する (通常はその利用者のセショントークンを盗み出すことにより) ために用いられる手法である。これらの攻撃はサーバのセキュリティ問題に起因することが多いが、この攻撃の検出を試行する技術を採用しているブラウザもある。
- ブラウザのタブ／ウィンドウの不十分なサンドボックス化またはクロスドメイン通信モデルの欠陥により、1 つのタブ／ウィンドウ中の 1 つのドメイン (例えば、cnn.com) から別のタブ／ウィンドウ中の別のドメイン (例えば、google.com) へのコンテンツの漏えいが引き起こされるおそれがある。これは、複数ドメインからのコンテンツをブラウザが同時に表示できる能力の悪用であり、スクリプトにより実行可能である。

[T.NETWORK_ATTACK]

2.1.5 データアクセス

実行中のウェブブラウザへのアクセスにより、ウェブブラウザにより保存される利用者データの機密性または完全性、あるいはその両方の損失が引き起こされるかもしれない。クッキーキャッシュ、履歴、ウェブフォームデータなどのブラウザデータが、これらの攻撃によりアクセスされるおそれがある。

[T.DATA_ACCESS]

2.2 前提条件

TOE の前提条件は、附属書 A.1.1 に定義される。

3 セキュリティ対策方針

適合 TOE は、以下に列挙されるセキュリティ対策方針に対応し、また TOE への新たな脅威に対応する方針を実装するセキュリティ機能を提供することになる。以下のセクションでは、上に列挙した脅威を考慮しつつ、この機能の記述を提供する。

3.1 TOE のセキュリティ対策方針

3.1.1 O.COMMS 保護された通信

ネットワーク攻撃及びネットワーク盗聴の脅威に対応するため、TOE はブラウザと所与のウェブサーバとの間の保護ネットワークを、そのような保護された通信が望ましい場合には提供しなければならない (must)。運用環境におけるこれら 2 つのエンティティの間のデータは、以下の標準プロトコル : HTTPS、トランスポート層セキュリティ (TLS) 及びデータグラムトランスポート層セキュリティ (DTLS) の 1 つ以上を用いて実装される高信頼パスにより保護される。

FCS_CKM.1(*),FCS_CKM_EXT.4, FCS_COP.1(*), FCS_DTLS_EXT.1, FCS_HTTPS_EXT.1, FCS_TLSC_EXT.1, FCS_STS_EXT.1, FDP_STR_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FPT_INT_EXT.3, FTP_ITC.1

3.1.2 O.ISOLATION ドメイン隔離

ブラウザにより表示される異なるウェブドメイン間のコンテンツ漏えいに関連したネットワーク攻撃に対応するため、TOE は異なるドメインに由来するコンテンツ (例えば、タブまたは iFrame 中の) が適切に隔離されアクセスが許可されないことを確実にしなければならない (must)。

FDP_ACF_EXT.1, FDP_SBX_EXT.1, FDP_SOP_EXT.1

3.1.3 O.CONFIG TOE の構成

ブラウザにより (一時的または永続的に) 保存され、あるいは処理される秘密データを保護するため、適合 TOE は管理者により定義されたセキュリティポリシーを定義、構成、及び適用する能力を提供する。エンタープライズのポリシーが管理者により TOE に構成される場合、これらはいかなる利用者の定義する設定よりも優先されなければならない (must)。

FDP_ACC_EXT.1, FDP_TRK_EXT.1, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1

3.1.4 O.INTEGRITY TOE の完全性

ブラウザの完全性が保たれていることを確実にするため、適合 TOE はセルフテストを行ってソフトウェア及びデータの完全性が保たれていることを確実にする。

悪意または欠陥のあるブラウザのソフトウェア、プラグインまたは拡張機能に関連した課題に対応するため、適合 TOE はブラウザのソフトウェア、プラグイン及び拡張機能の完全性を保証し、またそれらが正当な情報源に由来するものであることを保証するメカニズムを実装しなければならない (must)。TOE は、任意のブラウザソフトウェア、プラグイン及び拡張機能が、その後それらに適用される任意の更新と共に、インストール時及び実行時に検証されることを可能とするメカニズムを提供し、またそのようなポリシーを実施しなければならない (must)。さらに、TOE は実行可能形式のダウンロードと起動を制御しなけ

ればならない (shall)。

FAU_GEN.1, FAU_SEL.1, FCS_COP.1(2), FCS_COP.1(3), FPT_DNL_EXT.1, FPT_DNL_EXT.2, FPT_INT_EXT.1, FPT_INT_EXT.2, FPT_MCD_EXT.1, FPT_TUD_EXT.1, FPT_TUD_EXT.2, FPT_TUD_EXT.3

3.1.5 O.STORAGE 秘密情報のセキュアなストレージ

ブラウザは、数多くの種別の潜在的に秘密利用者情報 (例えば、パスワード、ウェブフォームデータ、暗号鍵) を取り扱う。この情報を保存の際にブラウザが保護することは、必須である。ブラウザは、ブラウザ自身の一部であるメカニズムやライブラリではなく、プラットフォームの暗号及び認証のメカニズムやライブラリを利用して、この情報を保護しなければならない (shall)。

FCS_COP.1(1), FCS_CKM_EXT.1, FCS_CKM_EXT.4, FCS_COP.1(4), FDP_COO_EXT.1, FDP_DEL_EXT.1, FDP_DEL_EXT.2, FDP_DEL_EXT.3, FDP_PBR_EXT.1, FDP_PST_EXT.1

4 セキュリティ要件

このセクションに含まれるセキュリティ機能要件の一部は、*情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 改定第 4 版*のパート 2 から導出されたものに、拡張機能コンポーネントを追加したものである。

4.1 表記

CC では、割付、選択、選択中の割付、及び詳細化という、セキュリティ機能要件に関する操作を定義している。本文書では、以下のフォント規則を用いて、CC により定義される操作を識別する。

- 割付：*イタリック体*のテキストで示す。
- PP 作成者によりなされた詳細化：エレメント番号の後に**太字**で表記された「詳細化」という単語と、**太字**の追加されたテキスト及び必要に応じて取り消し線で表記された削除により示される。
- 選択：下線付きテキストで示す。
- 選択中の割付：*イタリック体の下線付き*テキストで示す。
- 繰返し：例えば (1), (2), (3) など、繰返し回数を括弧内に付記して示す。

拡張 SFR は、TOE SFR の要件名の後にラベル「EXT」を付けることにより識別される。

4.2 セキュリティ機能要件

このセクションは、TOE により満たされ得るセキュリティ機能要件に対応する。

4.2.1 クラス：利用者データ保護 (FDP)

アクセス制御機能

FDP_ACF_EXT.1 拡張：ローカル及びセションストレージの分離

FDP_ACF_EXT.1 TOE は、ローカル (永続的) 及び短期的 (ephemeral) ストレージを、ドメイン、プロトコル及びポートに基づいて分離しなければならない (shall)：

- セションストレージは、それが由来するタブまたはウィンドウからのみアクセス可能でなければならない (shall)；
- ローカルストレージは、同一のウェブアプリケーションが動作するウィンドウ及びタブからのみアクセス可能でなければならない (shall)。

適用上の注意：

ローカル及びセションストレージの分離は、World Wide Web Consortium (W3C) Proposed Recommendation: “Web Storage” に記述されている。

この文脈において、ドメインとはインターネット上の管理主体、権威または監督の領域である (例えば、cnn.com、ietf.org)。サブドメインは、トップレベルのドメイン名の前にプリフィックスをつけることにより示される (例えば、news.cnn.com)。プロトコルは、コンピュータ内またはコンピュータ間データ交換のデジタル的なルールの体系である。ウェブ環境において、典型的なプロトコルは HTTP 及び HTTPS である。ポートは、コンピュータのホスト OS において通信エンドポイントとして機能するアプリケーション特有の構成物である。ウェブ環境において、ポート 80 が HTTP 通信のデフォルトポートであるが、他のポートを用いることもできる。ウェブアドレスにおいては、ポートはドメインまたはサブド

メインの後に指定される (例えば、http://www.cnn.com:80)。

保証アクティビティ

TSS

評価者は、TSF がローカル及びセションストレージを分離する方法が記述されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、ローカルストレージに用いられるファイルシステム上の場所及びセションストレージに用いられる場所が文書化されていることを検証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、ローカル及びセションストレージから情報を保存及び取り込む JavaScript ベースのスクリプトを取得または作成しなければならず (shall)、また異なるプロトコルまたはポートあるいはその両方を用いる 2 つ以上のウェブページを持つウェブサーバをセットアップしなければならない (shall)。評価者は、そのスクリプトをウェブページへ取り込まなければならない (shall)。評価者は 2 つ以上のブラウザウィンドウをオープンし、同一のウェブページへナビゲートしなければならない (shall)。評価者は、1 つのウィンドウで動作しているセションストレージへアクセスするスクリプトが、異なるウィンドウと関連付けられたセションストレージへアクセスできないことを検証しなければならない (shall)。
- テスト 2 : 同一のウェブサーバを用いて、評価者は 2 つ以上のブラウザタブをオープンし、同一のウェブページへナビゲートしなければならない (shall)。評価者は、1 つのタブで動作しているセションストレージへアクセスするスクリプトが、異なるタブと関連付けられたセションストレージへアクセスできないことを検証しなければならない (shall)。
- テスト 3 : 同一のウェブサーバを用いて、評価者は 2 つ以上のブラウザウィンドウをオープンし、同一のウェブページへナビゲートしなければならない (shall)。評価者は、1 つのウィンドウで動作しているローカルストレージへアクセスするスクリプトが、異なるウィンドウと関連付けられたローカルストレージへアクセスできないことを検証しなければならない (shall)。
- テスト 4 : 同一のウェブサーバを用いて、評価者は 2 つ以上のブラウザタブをオープンし、同一のウェブページへナビゲートしなければならない (shall)。評価者は、1 つのタブで動作しているローカルストレージへアクセスするスクリプトが、異なるタブと関連付けられたローカルストレージへアクセスできないことを検証しなければならない (shall)。
- テスト 5 : 同一のウェブサーバを用いて、評価者は複数のウィンドウと複数のタブをオープンし、異なるウェブページへナビゲートしなければならない (shall)。評価者は、1 つのウィンドウまたはタブ中の 1 つのドメイン／プロトコル／ポートの文脈で動作しているスクリプトが、異なるウィンドウまたはタブ中の異なるドメイン／プロトコル／ポートの文脈と関連付けられた情報へアクセスできないことを検証しなければならない (shall)。

クッキーの取り扱い

FDP_COO_EXT.1 拡張：クッキーのブロック

FDP_COO_EXT.1.1 TOE は、ウェブサイトによるサードパーティクッキーの保存をブロックする能力を提供しなければならない (shall)。

保証アクティビティ：

TSS

評価者は、TSF がサードパーティクッキーをブロックする方法と、そのブロックが行われる時点 (例えば、自動的に、ブロックが許可された際) が記述されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、サードパーティクッキーをブロックするための構成オプションの記述が提供されていることを検証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者はすべてのクッキーをクリアした後、サードパーティクッキーの保存が許可されるよう TOE を構成しなければならない (shall)。評価者は、サードパーティクッキーを保存するウェブページをロードしなければならない (shall)。評価者はクッキーが保存される場所へナビゲートしなければならず (shall)、そしてクッキーが存在することを検証しなければならない (shall)。
- テスト 2 : 評価者はすべてのクッキーをクリアした後、サードパーティクッキーの保存がブロックされる (すなわち、許可されない) よう TOE を構成しなければならない (shall)。評価者は、サードパーティクッキーの保存を試行するウェブページをロードしなければならず (shall)、そしてそのクッキーが保存されなかったことを検証しなければならない (shall)。

情報の削除

FDP_DEL_EXT.1 拡張：ブラウザデータの削除

FDP_DEL_EXT.1.1 TOE は、利用者により呼び出された際に TOE から [選択：ブラウザキャッシュ、履歴、パスワード、ウェブフォーム情報、クッキー、拡張機能、プラグイン] を削除する能力を提供しなければならない (shall)。

FDP_DEL_EXT.1.2 TOE は、ブラウザが終了する際に TOE から [選択：ブラウザキャッシュ、履歴、パスワード、ウェブフォーム情報、クッキー、拡張機能、プラグイン] を削除する能力を提供しなければならない (shall)。

適用上の注意：

上記の拡張機能またはプラグインが選択される場合、附属書 C から該当する選択に基づく要件もまた ST の本文に含まれなければならない (must)。

保証アクティビティ：

TSS

評価者は、すべてのブラウザコンテンツがどこに保存されるか、どのブラウザコンテンツ

が削除可能か、文書化されていることを保証するため、TSS を検査しなければならない (shall)。また TSS には、ブラウザ終了の際のブラウザコンテンツの削除も記述されなければならない (shall)。

ガイダンス

評価者は、どのようにすれば利用者が保存されたコンテンツを削除できるか、及びどの種別の保存されたコンテンツが削除できるか選択するための指示が含まれることを検証するため、操作ガイダンスを検査しなければならない (shall)。また操作ガイダンスには、ブラウザ終了時にコンテンツが確実に削除されるための指示も含まれなければならない (shall)。

テスト

評価者は、保存されたコンテンツの各種別について、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、保存されるコンテンツの作成と保存をプロンプトするウェブサーバとのウェブセションをセットアップしなければならない (shall)。評価者は、サポートされる種別のコンテンツが文書化された場所へ保存されることを検証しなければならない (shall)。評価者は次にブラウザからコンテンツを削除しなければならず (shall)、また保存されたコンテンツが文書化された場所から削除されていることを検証しなければならない (shall)。
- テスト 2 : 評価者は、ブラウザコンテンツが指定された場所にあることを検証しなければならない (shall)。評価者は TOE を起動し、コンテンツを削除するよう設定し、そして TOE を終了しなければならない (shall)。評価者は文書化されたコンテンツの場所へナビゲートし、保存されたコンテンツが削除されていることを検証しなければならない (shall)。

サンドボックス化

FDP_SBX_EXT.1 拡張 : 表示プロセスのサンドボックス化

FDP_SBX_EXT.1.1 TOE は、ウェブページの表示が以下のように制限されたプロセスにおいて行われることを保証しなければならない (shall) :

- 表示プロセスは直接 TOE プラットフォームのファイルシステムへアクセスできない ;
- 表示プロセスは非 TOE プロセスとプロセス間通信メカニズムを直接起動できない ;
- 表示プロセスは [選択 : [割付 : *最小特権の原則が表示プロセスに実装される手法*]、その他の方法なし] 他の TOE プロセスに関して低減された権限を持つ。

適用上の注意 :

ウェブブラウザは、処理している HTML または JavaScript により表示プロセスが損なわれるリスクを低減するために、HTML を表示し JavaScript を解釈するプロセスが制約された環境において動作することを確実にする、さまざまな手法を実装している。このコンポーネントは、表示プロセスがホストのファイルシステムへ直接アクセスできず、またホスト上の非 TOE プロセスと通信するためにホストにより提供される IPC メカニズムを使用できないことを確実にすることにより、表示プロセスの特権を低下させることを TSF に要求している。典型的には、表示プロセスがファイルへのアクセスや非 TOE プロセスとの通信を必要とする場合、表示プロセスは TSF を介してそのようなアクセスを要求 (これは要件により許可される) しなければならない (must)。

要求される 2 つの手段に加えて、TOE 及びホストプラットフォームに応じた他の手段を実装することもできる。これらには、表示プロセスの所有者を低い特権のアカウントへ変更することや、表示プロセス中のプラットフォームにより定義される特権を破棄するなどのアクションが必要とされるかもしれない。ST 作成者は、TOE により実装される追加的手段を記入する。

保証アクティビティ：

TSS

評価者は、HTML の表示と JavaScript の解釈が TOE によりどのように行われるか、関連するプラットフォームプロセス (この「プロセス」とはコードを実行するアクティブなエンティティである) の観点から記述されていることを保証するため、TSS を検査しなければならない (shall)。HTML の表示または JavaScript の解釈を行うプロセスに関して、評価者は、これらのプロセスによるプラットフォームファイルシステムへのアクセスがどのように防止されるか、記述されていることをチェックするため、TSS を検査しなければならない (shall)。評価者は、あらゆるプラットフォームの提供する IPC メカニズムが記述されていること、そして各メカニズムについて、それを用いて表示プロセスが非 TOE プロセスとの通信を行うことが不可能である理由が詳述されていることを保証するため、TSS をチェックしなければならない (shall)。また評価者は、IPC 及びファイルシステムへのアクセスがどのように有効化されるか TSS に記述されていることを確認しなければならない (shall) (この能力が実装されている場合)。例えば、ウェブページの表示を行わない、より高い特権を持った TOE プロセスを介して。評価者は、これらの記述が ST に主張されるすべてのプラットフォームについて存在することを保証しなければならない (shall)。

ST 作成者によりこのコンポーネントの 3 番目の丸印に列挙された追加の各メカニズムについて、評価者は、1) そのメカニズムが記述されていること ; 2) そのメカニズムの記述が、最小特権の法則の表示プロセスへの実装に役立っていると決定できるほど十分に詳細であること ; そして 3) 主張される最小特権メカニズムを理解するための文脈を提供する適切な支援情報が TSS に提供されている (または、そのような情報への参照が提供されている) ことを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、表示プロセスに関して利用可能な制約の記述が提供されていることを決定するため、操作ガイダンスを検査しなければならない (shall)。また、そのようなメカニズムが構成可能である (例えば、利用者がどのメカニズムを「オンにする」か選べる) 場合、評価者は、そのメカニズムを有効化及び無効化する手法が提供されていること、そしてそのようなアクションの影響が記述されていることを保証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

注意：以下のテストには、消費者向けプラットフォームには通常含まれないデバッグ及びテストツールを評価者へ提供するテストプラットフォームへのアクセスを、開発者が提供することが要求される。

評価者は、ST に主張される各プラットフォームについて、以下のテストを行わなければならない (shall) :

- テスト 1 : 評価者はデバッグまたはテスト設備を用いて、評価者はプラットフォームのファイルシステムへの直接アクセスを試行するコードを表示プロセスへ導入し、その後直接それを実行しなければならない (shall)。評価者は、このコードの実行により TOE

ファイルシステムへのアクセスができないことを保証しなければならない (shall)。

- テスト 2 : TSS に記述される各 IPC メカニズムについて、評価者はデバッグまたはテスト設備を用いてプラットフォーム上の他の非 TOE プロセスとの直接通信を試行するコードを表示プロセスへ導入し、その後直接それを実行しなければならない (shall)。評価者は、この試行が失敗することを保証しなければならない (shall)。
- テスト 3 : ST に主張される追加の各メカニズムについて、評価者はそのメカニズムが TSS に記述されるとおりに機能することを示すテストを考案しなければならない (shall)。そのようなテストが作成できない場合、評価者はそのメカニズムがテストできない理由の正当化をテスト報告中に提供しなければならない (shall)。
- テスト 4 : 構成もしくはオンまたはオン可能な各メカニズムについて、評価者はそのメカニズムの構成が操作ガイダンスに指定されるとおりふるまうことを保証するテストを行わなければならない (shall)。

同一生成元ポリシー

FDP_SOP_EXT.1 拡張：同一生成元ポリシー

FDP_SOP_EXT.1.1 TOE は、1 つの生成元から取り込まれたコンテンツが、他の生成元から取り込まれたコンテンツと、コンテンツが取り込まれた生成元からの同意なしに相互作用できないことを確実にしなければならない (shall)。

FDP_SOP_EXT.1.2 TOE は、異なるドメインについて同一生成元ポリシーの例外を許可してはならない (shall not)。

適用上の注意：

同一生成元ポリシー (The Same Origin Policy) の概念は、RFC 6454, "The Web Origin Concept" に記述されている。

生成元は、ドメイン、プロトコル及びポートの組み合わせとして定義される。同一のドメイン、プロトコル及びポートを共有する 2 つの URI は、同一生成元を持つとみなされる。

保証アクティビティ：

TSS

評価者は、同一生成元ポリシーの実装が記述され、またどのように RFC 6454 に準拠しているか説明されていることを保証するため、TSS を検査しなければならない (shall)。異なるタブまたはウィンドウ中のサブドメインに関して同一生成元ポリシーの緩和を TSF が許可している場合、TSS にはこれらの例外がどのように実装されているか記述されなければならない (shall).

ガイダンス

N/A

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、指定された場所からコンテンツを取り込むことのできるスクリプトを取得または作成しなければならず (shall)、また異なるドメインを表現する 2 つ以上のウェブページを持つウェブサーバをセットアップしなければならない (shall)。評価者は、そのスクリプトをウェブページへ取り込まなければならない (shall)。評価者

は、各ページに異なるプロトコルまたはポートあるいはその両方を関連付けなければならない (shall)。評価者は 2 つ以上のブラウザウィンドウをオープンし、各ウィンドウでウェブサイト上の異なるページへナビゲートしなければならない (shall)。評価者はスクリプトを実行しなければならず (shall)、また 1 つのウィンドウで動作しているそのスクリプトが異なるウィンドウで取り込まれたコンテンツへアクセスできないことを検証しなければならない (shall)。

- テスト 2 : 同一のウェブサーバを用いて、評価者は 2 つ以上のブラウザタブをオープンし、各タブでそのウェブサイトの異なるページへナビゲートしなければならない (shall)。評価者はスクリプトを実行しなければならず (shall)、1 つのタブで動作しているそのスクリプトが異なるタブで取り込まれたコンテンツへアクセスできないことを検証しなければならない (shall)。
- テスト 3 : TSF がサブドメインに関して同一生成元ポリシーの緩和をサポートしている場合、評価者はウェブサーバにサブドメインを構成しなければならず (shall)、またテスト 1 及び 2 を繰り返さなければならない (shall)。評価者は、スクリプトが異なるサブドメインの別のウィンドウ／タブからコンテンツを取り込むことができることを検証しなければならない (shall)。

セキュアなデータの送信

FDP_STR_EXT.1 拡張 : セキュアなクッキーデータの送信

FDP_STR_EXT.1.1 TOE は、set-cookie ヘッダに“secure”属性を含むクッキーが HTTPS 上で送信されることを確実にしなければならない (shall)。

適用上の注意 :

set-cookie ヘッダの機能は、RFC 6265“HTTP State Management Mechanism”に記述されている。

保証アクティビティ :

TSS

評価者は、TOE が RFC 6265 に従って set-cookie ヘッダの“secure”属性をサポートしていることが、この属性を含むクッキーの HTTPS 上での送信が要求されることを含め、記述されていることを検証するため、TSS を検査しなければならない (shall)。

ガイダンス

N/A

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は TOE を、HTTPS を実装したクッキーが有効化されたテストウェブサイトへ接続し、そのウェブサイトが TOE へ“secure”クッキーを提示するようにしなければならない (shall)。評価者は、そこに secure クッキーが含まれることを検証し、TOE のクッキーキャッシュを検査しなければならない (shall)。
- テスト 2 : 評価者はセキュアでないチャネル上でクッキーが有効化されたウェブサイトへ再接続し、“secure”クッキーが送信されないことを検証しなければならない (shall).

利用者追跡情報

FDP_TRK_EXT.1 拡張：追跡情報の収集

FDP_TRK_EXT.1.1 TOE は、ウェブサイトが TOE 利用者に関して [選択：アクセスしたウェブサイト、位置情報、システムの構成、システムの状態、エラー条件、クラッシュ条件、[割付：*その他の追跡情報*]] を収集する能力をサポートしなければならない (shall)。

FDP_TRK_EXT.1.2 TOE は、追跡情報がウェブサイトにより要求された際、利用者へ通知を行わなければならない (shall)。

保証アクティビティ：

TSS

評価者は、TSF が追跡情報をサポートしていることが記述され、TOE がウェブサイトに収集を許した TOE 利用者に関する追跡情報が指定されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、追跡情報がウェブサイトにより要求された際に利用者が受け取る任意の通知と、通知を受け取る際に利用者に与えられる選択肢が記述されていることを保証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、TSS に列挙された追跡情報の種別について、次のテストを行わなければならない (shall)：

- テスト 1：評価者は利用者に関する追跡情報を要求するウェブサイトを構成しなければならず (shall)、そしてそのウェブサイトへナビゲートしなければならない (shall)。評価者は、追跡情報の要求に関して利用者が通知されること、そして合意の上で、ウェブサイトが追跡情報を取り込むことを検証しなければならない (shall)。

4.2.2 クラス：TSF の保護 (FPT)

TOE へのダウンロード

FPT_DNL_EXT.1 拡張：ダウンロードされた実行可能形式の起動

FPT_DNL_EXT.1.1 TOE は、ダウンロードされた実行可能形式が自動的に起動されることを防止しなければならない (shall)。

FPT_DNL_EXT.1.2 TOE は、実行可能形式をダウンロードするか、破棄するかの選択肢を利用者へ提示しなければならない (shall)。

適用上の注意：

これに関連して、実行可能形式とはソフトウェアプログラムのコンパイルされたコードを含むファイルであって、起動された際にプログラムのインストールを開始するものである。これは、TOE とは独立して、また TOE とは無関係に起動される。これにはモバイルコード、スクリプト、あるいはプラグインは含まれない。

本要件には、TOE プラットフォーム上にすでにインストールされた任意のプログラムの起動は含まれない。

本要件は、利用者が意図的に (リンクをクリックすることにより) あるいは意図せずに実行可能形式のダウンロードを開始した場合、TSF が、例えば実行可能形式をファイルシステムへ保存するか実行可能形式をダウンロードしないかの選択肢を利用者へ提示するダイアログボックスをオープンすることにより、介入することを確実にしている。

保証アクティビティ：

TSS

評価者は、利用者が実行可能形式のダウンロードを開始した際の TSF のふるまいが記述されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、ダウンロードが開始された際に表示されるダイアログボックスと、そのダイアログボックスにより提示されるオプションの影響が記述されていることを保証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は実行可能形式をホストするウェブサイトへナビゲートしなければならず (shall)、そしていくつかの実行可能形式のダウンロードと起動を試行しなければならない (shall)。評価者は、実行可能形式をファイルシステムへダウンロードするか実行可能形式を破棄するかの選択肢を持つダイアログボックスを、TOE が常に提示することを検証しなければならない (shall)。

FPT_DNL_EXT.2 拡張：ダウンロードの場所

FPT_DNL_EXT.2.1 TOE は、ダウンロードが保存される場所を指定する能力を持たなければならない (shall)。

保証アクティビティ：

TSS

N/A

ガイダンス

評価者は、ダウンロードのデフォルトの場所と、その場所を変更するための指示が記述されていることを保証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、ファイルを提供するウェブサイトへナビゲートしなければならず (shall)、そしてファイルのダウンロードを行わなければならない (shall)。評価者は操作ガイダンスに指定されたデフォルトの場所を検査しなければならず (shall)、そしてダウンロードが存在することを検証しなければならない (shall)。
- テスト 2 : 評価者は、ダウンロードされたファイルが保存される場所を変更しなければならない (shall)。評価者はファイルを提供するウェブサイトからファイルのダウンロードを試行しなければならず (shall)、そして構成された場所へファイルが保存されることを検証しなければならない (shall)。

外部との対話

FPT_INT_EXT.1 拡張：バックグラウンドプロセスとの対話

FPT_INT_EXT.1.1 TOE は、TOE が終了する際、TOE の子プロセスとして生成されたバックグランドプロセスがあれば、それをシャットダウンしなければならない (shall)。

保証アクティビティ：

TSS

評価者は、TOE の動作中に動作する TOE の子プロセスがすべて記述されており、また TOE が終了する際にこれらのプロセスを終了させる能力について記述されていることを保証するため、TSS を検査しなければならない (shall)。TSS には、バックグランドプロセスの性質、それらが子プロセスとして実行される状況、それらと関連付けられるプロセス／イメージ名（もしあれば）及びそれらに期待される寿命についても記述されるべきである (should)。

ガイダンス

N/A

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1：評価者は、TOE のインスタンスをスタートさせなければならない (shall)。評価者は TOE プラットフォームの実行中プロセスを検査して、TOE のインスタンスと関連するものを識別しなければならない (shall)。評価者は TOE のインスタンスをシャットダウンし、TOE のバックグラウンドプロセスが終了していることを検証しなければならない (shall)。

モバイルコード

FPT_MCD_EXT.1 拡張：モバイルコード

FPT_MCD_EXT.1.1 TOE は、署名された [選択：ActiveX、Flash、Java、JavaScript、[割付：*TOE によりサポートされるその他のモバイルコードの種別*]] モバイルコードを実行する能力をサポートしなければならない (shall)。

FPT_MCD_EXT.1.2 TOE は、署名されていない [選択：ActiveX、Flash、Java、JavaScript、[割付：*TOE によりサポートされるその他のモバイルコードの種別*]] モバイルコードを実行する能力をサポートしなければならない (shall)。

FPT_MCD_EXT.1.3 TOE は、信頼されない、または未検証の情報源からの [選択：ActiveX、Flash、Java、JavaScript、[割付：*TOE によりサポートされるその他のモバイルコードの種別*]] モバイルコードを実行する能力をサポートしなければならない (shall)。

FPT_MCD_EXT.1.3 TOE は、署名されていない、信頼されない、または未検証のモバイルコードに遭遇した際、利用者へ通知しなければならない (shall)。

FPT_MCD_EXT.1.4 TOE は、署名されていない、信頼されない、または未検証のモバイルコードを実行することなく破棄する選択肢を利用者へ提供しなければならない (shall)。

適用上の注意：

ST 作成者は、ブラウザによりサポートされるすべてのモバイルコードの種別を指定しなければならない (must)。列挙されていないものがあれば、ST 作成者は欠けているモバイルコードの種別を割付へ記入しなければならない (must)。

権限のある署名者がコードそのものへ直接署名してもよいし、あるいは権限のあるエンティティとの認証された HTTPS 接続上でコードが配付されてもよい。

署名されたモバイルコードの実行は、FIA_X509_EXT.2 により指定される。

保証アクティビティ：

TSS

評価者は、TSF がサポートする署名されたモバイルコードの種別が列挙されていることを保証するため、TSS を検査しなければならない (shall)。TSS には、署名されていないモバイルコード、信頼されない情報源からのモバイルコード、及び未検証の情報源からのモバイルコードを TSF がどのように取り扱うか、記述されなければならない (shall)。

ガイダンス

評価者は、サポートされるモバイルコードの各種別について、構成指示が提供されていることを検証するため、操作ガイダンスを検査しなければならない (shall)。また操作ガイダンスには、署名されていない、信頼されない、または未検証のモバイルコードに遭遇した際に TOE が利用者へ表示する警報と、利用者が取ることのできるアクションも記述されなければならない (shall)。

テスト

評価者は、TSS に指定されたモバイルコードの各種別について、次のテストを行わなければならない (shall) :

- テスト 1 : 評価者は、署名されていない、正しく認証された、及び不正に認証されたモバイルコードを含むウェブページを構築し、認証に失敗するモバイルコードに TOE が遭遇した際に TOE が利用者へ警報を行うこと、実行することなくそのモバイルコードを破棄する選択肢を利用者へ提供すること、しかし適切に認証されるモバイルコードは実行することを保証しなければならない (shall)。

4.3 TOE または TOE プラットフォームのセキュリティ機能要件

このセクションは、TOE そのものにより、TOE プラットフォームにより、あるいは TOE と TOE プラットフォームの組み合わせにより満たされ得るセキュリティ機能要件に対応する。

4.3.1 クラス：暗号サポート (FCS)

暗号鍵の管理

FCS_CKM.1 暗号鍵の生成

FCS_CKM.1(1) 暗号鍵生成 (鍵確立に関して)

FCS_CKM.1.1(1) 詳細化： [選択：TOE、TOE プラットフォーム] は、以下に従って**鍵確立に用いられる**非対称暗号鍵を生成しなければならない (shall)。

- 楕円曲線ベースの鍵確立スキームならびに「NIST 曲線」 P-256、P-384 及び [選択：

P-521、その他の曲線なし] (FIPS PUB 186-4, “Digital Signature Standard” の定義による) の実装については、NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”

- RSA ベースの鍵確立スキームについては、NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”

[選択：

- 有限体ベースの鍵確立スキームについては、NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”、
- その他のスキームなし

]

また、指定された暗号鍵サイズは 112 ビットの対称鍵強度と同等、またはそれよりも大きくなければならない。

適用上の注意：

このコンポーネントは、TOE により用いられるさまざまな暗号プロトコル (例えば高信頼チャネル) の鍵確立の目的で用いられる公開鍵/プライベート鍵ペアを TSF または TOE プラットフォームが生成できることを要求する。複数のスキームがサポートされている場合には、ST 作成者は本要件を繰り返してこの機能を取り込むべきである (should)。用いられるスキームは、ST 作成者により選択の中から選ばれることになる。用いられるべきドメインパラメタは本 PP のプロトコル要件により指定されているため、TOE がドメインパラメタを生成することは期待されておらず、従って本 PP に指定されたプロトコルに TOE が準拠する際には追加的なドメインパラメタの検証は必要とされない。

2048 ビットの DSA 及び RSA 鍵の生成鍵強度は、112 ビットの対称鍵強度と同等、またはそれよりも大きくなければならない。同等の鍵強度に関する情報については、NIST Special Publication 800-57, “Recommendation for Key Management” を参照されたい。

RSA 及び楕円曲線ベースのスキームは、FCS_TLSC_EXT.1 に要求される暗号スイートへ適合するため要求される。

保証アクティビティ：

TSS

TOE プラットフォームにより満たされる要件：評価者は、そのプラットフォームの ST に主張される鍵確立にウェブブラウザの ST における鍵確立要件が含まれていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。また評価者は、、(サポートされる各プラットフォームについて) 鍵確立機能が呼び出される方法が記述されていることを検証するため、ウェブブラウザの ST の TSS を検査しなければならない (shall) (これはウェブブラウザにより実装されないメカニズムにより行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムはこの保証アクティビティの一部として TSS 中に識別されることになる)。

ガイダンス

N/A

テスト

TOE により満たされる要件：

評価者は、TOE 上で用いられる鍵生成及び鍵確立スキームの実装を検証しなければならない (shall)：

鍵生成：

評価者は、下記から該当するテストを用いて、サポートされるスキームの鍵生成ルーチンの実装を検証しなければならない (shall)。

RSA ベースの鍵確立スキーム向け鍵生成：

評価者は、鍵生成テストを用いて TOE による RSA 鍵生成の実装を検証しなければならない (shall)。このテストは、公開鍵検証指数 e、プライベート素因数 p 及び q、公開モジュラス (modulus) n 及びプライベート署名指数 d の計算を含めた鍵コンポーネントの値を正しく求める TSF の能力を検証する。

鍵ペア生成では、素数 p 及び q を生成するための 5 とおりの方法 (または手法) を指定している。これには、以下のものが含まれる。

- ランダム素数：
  - 証明可能素数
  - 確率的素数
- 条件付き素数：
  - 素数 p1、p2、q1、q2、p 及び q を、すべて証明可能素数とする (shall)
  - 素数 p1、p2、q1 及び q2 を証明可能素数とし、p 及び q を確率的素数とする (shall)
  - 素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数とする (shall)

ランダム証明可能素数手法とすべての条件付き素数手法の鍵生成手法をテストするため、評価者は決定論的に RSA 鍵ペアを生成するために十分なデータをシードとして TSF 鍵生成ルーチンに与えなければならない (shall)。これには、1 つまたは複数の乱数シード、RSA 鍵の公開鍵指数、及び望ましい鍵の長さが含まれる。サポートされている各鍵長について、評価者は 25 個の鍵ペアを TSF に生成させなければならない (shall)。評価者は、TSF により生成された値を既知の良好な実装から生成された値と比較することにより、TSF の実装の正しさを検証しなければならない (shall)。

有限体暗号 (FFC) ベースの 56A スキーム向け鍵生成

FFC ドメインパラメタ及び鍵生成テスト

評価者は、パラメタ生成及び鍵生成テストを用いて TOE による FFC 向けパラメタ生成及び鍵生成の実装を検証しなければならない (shall)。このテストは、フィールド素数 p、暗号素数 q (p-1 を割り切る)、暗号群生成元 g、ならびにプライベート鍵 x 及び公開鍵 y の計算の値を正しく求める TSF の能力を検証する。

パラメタ生成では、暗号素数 q 及びフィールド素数 p を生成するための 2 とおりの方法 (または手法)：

- 暗号素数及びフィールド素数：
  - 素数 q 及び p を両方とも証明可能素数とする (shall)
  - 素数 q 及びフィールド素数 p を両方とも確率的素数とする (shall)

そして、暗号群生成元 g を生成するための 2 とおりの方法を指定している。

- 暗号群生成元：
  - 検証可能プロセスにより構築された生成元 g
  - 検証不可能プロセスにより構築された生成元 g

鍵生成では、プライベート鍵 x を生成するための 2 とおりの方法を指定している。

- プライベート鍵：
  - RBG の len(q) ビットの出力、ここで 1 <=x <= q-1
  - RBG の len(q) + 64 ビットの出力に、q-1 を法とする剰余演算を行ったもの、ここで 1<= x<=q-1

RBG のセキュリティ強度は、少なくとも FFC パラメタセットにより提供されるセキュリティの強度と同じでなければならない (must)。

証明可能素数手法の暗号素数及びフィールド素数生成手法、または検証可能プロセスの群生成元 g、あるいはその両方をテストするため、評価者は決定論的にパラメタセットを生成するために十分なデータをシードとして TSF パラメタ生成ルーチンに与えなければならない (must)。

サポートされている各鍵長について、評価者は 25 個のパラメタセットと鍵ペアを TSF に生成させなければならない (shall)。評価者は、TSF により生成された値を既知の良好な実装から生成された値と比較することにより、TSF の実装の正しさを検証しなければならない (shall)。検証では、以下

- g != 0,1
- q が p-1 を割り切ること
- g^q mod p = 1
- g^x mod p = y

もまた、各 FFC パラメタセットと鍵ペアについて、確認されなければならない (must)。

楕円曲線暗号 (ECC) ベースの 56A スキーム向け鍵生成

ECC 鍵生成テスト

サポートされている各 NIST 曲線、すなわち P-256、P-284 及び P-521 について、評価者は 10 個のプライベート鍵／公開鍵ペアを試験対象実装 (IUT) に生成させなければならない (shall)。プライベート鍵は、承認済みランダムビット生成器 (RBG) を用いて生成されなければならない (shall)。正しさを決定するため、評価者は生成された鍵ペアを既知の良好な実装の公開鍵検証 (PKV) 機能へ提出しなければならない (shall)。

ECC 公開鍵検証 (PKV) テスト

サポートされている各 NIST 曲線、すなわち P-256、P-284 及び P-521 について、評価者は既知の良好な実装の鍵生成機能を用いて 10 個のプライベート鍵／公開鍵ペアを生成し、5 個の公開鍵を不正な値となるように変更し、5 個を未変更の (すなわち、正しい) 値のままにしなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

鍵確立スキーム

評価者は、以下から該当するテストを用いて、TOE によりサポートされる鍵確立スキームの実装を検証しなければならない (shall)。

SP800-56A 鍵確立スキーム

評価者は、以下の機能及び検証テストを用いて、SP800-56A 鍵共有スキームの TOE の実装を検証しなければならない (shall)。各鍵共有スキーム向けのこれらの検証テストは、勧告中の仕様にしたがった鍵共有スキームのコンポーネントが TOE に実装されていることを検証するものである。これらのコンポーネントには、DLC プリミティブ (共有秘密の値 Z) の計算と、鍵導出関数 (KDF) による導出鍵マテリアル (DKM) の計算が含まれる。鍵確認がサポートされる場合、評価者はまた以下に記述されるテスト手順を用いて、鍵確認のコンポーネントが正しく実装されていることも検証しなければならない (shall)。これには、DKM の解析、MAC データの生成、及び MAC タグの計算が含まれる。

機能テスト

機能テストは、鍵共有スキームを正しく実装する TOE の能力を検証する。このテストを行うために評価者は、TOE のサポートするスキームの既知の良好な実装からテストベクトルを生成または取得しなければならない (shall)。サポートされている鍵共有スキーム・鍵共有役割の組み合わせ、KDF タイプと (サポートされている場合には) 鍵確認役割・鍵確認タイプの各組み合わせについて、試験者は 10 セットのテストベクトルを生成しなければならない (shall)。このデータセットは、10 セットの公開鍵あたり 1 セットのドメインパラメタ値 (FFC) または NIST 承認の曲線 (ECC) からなる。これらの鍵は、テストされるスキームにより静的鍵であるか、短期鍵であるか、あるいはその両方である。

評価者は、DKM、対応する TOE の公開鍵 (静的鍵または短期鍵あるいはその両方)、1 つまたは複数の MAC タグ、及びその他の情報フィールド (OI) や TOE id フィールドなど KDF において用いられる任意の入力を取得しなければならない (shall)。

TOE が SP 800-56A に定義される KDF を利用しない場合、評価者は公開鍵と共有秘密のハッシュ値のみを取得しなければならない (shall)。

評価者は、既知の良好な実装を用いて共有秘密の値を計算し、鍵マテリアル DKM を導出し、そしてこれらの値から生成されるハッシュまたは MAC タグを比較することにより、所与のスキームの TSF の実装の正しさを検証しなければならない (shall)。

鍵確認がサポートされている場合、実装された各承認 MAC アルゴリズムについて、TSF は上記を行わなければならない (shall)。

検証テスト

検証テストは、相手方の有効及び無効な鍵共有結果を、鍵確認と共に、または鍵確認なしで、認識する TOE の能力を検証する。このテストを実施するため評価者は、SP800-56A 鍵共有実装に含まれるサポートする暗号機能のリストを取得し、どのエラーを TOE が認識可能であるべきか (should) を決定しなければならない (shall)。評価者は、ドメインパラメタ値または NIST 承認の曲線、評価者の公開鍵、TOE の公開鍵／プライベート鍵ペア、MAC タグ、及びその他の情報フィールドや TOE id フィールドなど KDF において用いられる任意の入力を含むデータセットから構成される 24 個 (FFC) または 30 個 (ECC) のテストベクトルのセットを生成する。

評価者はテストベクトルの一部にエラーを注入し、以下のフィールドが不正であるために生じる無効な鍵共有結果を TOE が認識することをテストしなければならない (shall) : 共有秘密の値 Z、DKM、その他の情報フィールド OI、MAC 対象データ、または生成された MAC タグ。完全な、または部分的な (ECC のみ) 公開鍵検証が TOE に含まれる場合、評価者は

また両者の静的公開鍵、両者の短期公開鍵及び TOE の静的プライベート鍵へ個別にエラーを注入し、公開鍵検証機能または部分的な鍵検証機能 (ECC のみ) あるいはその両方におけるエラーを TOE が検出できることをも保証する。少なくとも 2 個のテストベクトルは未変更のままでなければならず (shall)、従って有効な鍵共有結果をもたらすべきである (should) (これらのテストベクトルは合格すべきである (should))。

TOE は、これらの改変されたテストベクトルを利用して、対応するパラメタを用いた鍵共有スキームをエミュレートしなければならない (shall)。評価者は TOE の結果を既知の良好な実装を用いた結果と比較して、TOE がこれらのエラーを検出することを検証しなければならない (shall)。

SP800-56 鍵確立スキーム

現時点では、RSA ベースの鍵確立スキーム向けの詳細なテスト手順は利用できない。行われた選択に応じて TSF が 800-56A または 800-56B あるいはその両方に準拠していることを示すため、評価者は TOE が準拠する 1 つまたは複数の適切な 800-56 標準のすべてのセクションが TSS に列挙されていることを保証しなければならない (shall)。

FCS_CKM_EXT.1 拡張：暗号ストレージ

FCS_CKM_EXT.1.1 [選択：TOE、TOE プラットフォーム] は、永続的秘密、プライベート鍵、[割付：*秘密ウェブフォームデータ*]、及びセキュアクッキーを使用していない際には、プラットフォームにより提供される鍵ストレージに保存しなければならない (shall)。

適用上の注意：

本要件により、永続的秘密 (パスワード、その他のクレデンシャル、秘密鍵) 、プライベート鍵、秘密ウェブオームデータ、及びセキュアクッキーが使用されていない際、セキュアに保存されることが確実となる。

秘密ウェブフォームデータには、個人が識別可能な情報 (例えば、社会保障番号、住所、生年月日) や金融情報 (例えば、クレジットカード番号、銀行口座番号) が含まれるかもしれない。ST 作成者は TSS に、TOE がどのウェブフォームデータをサポートするか、そしてそれがどのように保護されるかを指定する。

セキュアクッキーは、“set-cookie”ヘッダに“secure”属性を持つクッキーである。

上記のいずれかが TOE により操作され、その他がプラットフォームにより操作される場合には、両方の選択が ST 作成者により指定されることが可能であり、また ST 作成者は TOE により操作される鍵とプラットフォームにより操作される鍵とを TSS 中に識別しなければならない (must)。

本要件は、ウェブブラウザにより用いられる永続的秘密、プライベート鍵、秘密ウェブフォームデータ、及びセキュアクッキーがプラットフォームにより保存されることを義務付けている。

保証アクティビティ：

TSS

本要件が TOE と TOE プラットフォームのどちらにより満たされる場合であっても、評価者は、ST 中の要件を満たすことが必要とされる各永続的秘密 (パスワード、クレデンシャル、または秘密鍵) とプライベート鍵が列挙されていることを保証するため、TSS を検査する。上記のいずれかが TOE により、その他がプラットフォームにより操作される場合、

評価者はどの鍵が TOE により、どれがプラットフォームにより操作されるのか検証しなければならない (shall)。評価者は、どのウェブフォームデータが保存され、どれが秘密ものと取り扱われ、そしてどれが保護されるのか、TSS に識別されていることを検証しなければならない (shall)。評価者は、クッキーがセキュアであると識別される方法が TSS に識別されていることを検証しなければならない (shall)。これらの各項目について、評価者はその項目がどのように識別されるか、何の目的に用いられるか、そしてどのように保存されるか TSS に列挙されていることを確認する。次に評価者は、以下のアクションを行う。

TOE プラットフォームにより操作される永続的秘密及びプライベート鍵 : ST 中に列挙された各プラットフォームについて、評価者は、ウェブブラウザの ST にプラットフォームにより保存されるものとして列挙される永続的秘密、プライベート鍵、秘密ウェブフォームデータ、及びセキュアクッキーが、そのプラットフォームの ST 中で保護されるものとして識別されていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。

TOE により操作される永続的秘密及びプライベート鍵 : 評価者は、TOE により操作されるものとして列挙される各項目について、暗号化されずに永続的メモリへ書き込まれることはなく、またその項目がプラットフォームにより保存される、ということが立証されていることを決定するため、TOE の TSS を検査しなければならない (shall)。

ガイダンス

N/A

テスト

N/A

FCS_CKM_EXT.4 拡張 : 暗号鍵のゼロ化

FCS_CKM_EXT.4.1 [選択 : TOE、TOE プラットフォーム] は、すべての平文の秘密及びプライベート暗号鍵ならびに CSP を、もはや必要とされなくなった際にゼロ化しなければならない (shall)。

適用上の注意 :

ウェブブラウザプラットフォームが平文の秘密、秘密暗号鍵、及び CSP を用いる一切の操作を行わない場合、ST 作成者はプラットフォームを選択すべきである (should)。

あらゆるセキュリティ関連情報 (鍵や認証データ、そしてパスワードなど) は、セキュリティ上重要なデータの開示または改変を防止するため、もはや使われなくなった際にはゼロ化されなければならない (must)。

上述のゼロ化は、平文鍵及び暗号サービスプロバイダ (CSP) のすべての中間ストレージ領域 (すなわち、メモリバッファなど任意のストレージであって、そのようなデータの経路中に含まれるもの) に、その鍵／CSP が別の場所へ転送された際に適用される。

保証アクティビティ :

TSS

TOE プラットフォームにより満たされる要件 : 評価者は、、各秘密鍵 (対称鍵暗号化に用いられる鍵)、プライベート鍵、及び TOE に課される要件 FCS_CKM_EXT.4 に扱われていない鍵の生成に用いられる CSP が TSS に記述されていることを保証するためにチェックしなければならない (shall)。ST で列挙された各プラットフォームについて、評価者は、上記

に列挙された秘密鍵、プライベート鍵、及び鍵の生成に用いられる CSP が扱われていることを保証するため、プラットフォームの ST の TSS を検査しなければならない (shall)。

TOE により満たされる要件：評価者は、鍵の生成に用いられる CSP；いつ鍵がゼロ化されるか (例えば、使用後すぐに、システムのシャットダウン時等)；実行されるゼロ化処理の種別 (ゼロで上書き、ランダムパターンで三回上書き等) と同様に、各秘密鍵 (対称鍵暗号化用の鍵)とプライベート鍵が TSS に記述されていることを保証するために、チェックしなければならない (shall)。異なる種別のメモリが保護すべき材料の保存に用いられる場合、評価者はデータが保存されるメモリに対応したゼロ化処理 (例えば、「揮発性メモリ上に保存される秘密鍵はゼロで一回上書きでゼロ化するが、内部ハードドライブ上に保存される秘密鍵は書き込みごとに変化するランダムパターンを三回上書きでゼロ化する」) が TSS に記述されていることを保証するため、チェックしなければならない (shall)。ゼロ化を検証するためにリードバック（復唱）が行われる場合、このことも記述されなければならない (shall)。

ガイダンス

N/A

テスト

保証アクティビティの注意*：以下のテストには、消費者向けプラットフォームには通常含まれないツールを評価者へ提供するテストプラットフォームへのアクセスを、開発者が提供することが要求される。*

TOE により満たされる要件：TSS に記述される鍵クリアの各状況について、評価者は以下のテストを繰り返さなければならない (shall)。

- テスト 1：評価者は、TOE 及び計測機能を備えた TOE ビルドに適切な専用の運用環境と開発ツール (デバッガ、シミュレータなど) の組み合わせを利用して、鍵 (その鍵に関する通常の暗号処理中に TOE により内部的に作成される可能性のある鍵の中間コピーのすべてを含む) が正しくクリアされることをテストしなければならない (shall)。

  ソフトウェア中の暗号 TOE 実装は、デバッガの下でロード及び行使され、そのようなテストが行われなければならない (shall)。評価者は、TOE により永続的に暗号化される鍵の中間コピーを含め、クリア対象となる各鍵について、以下のテストを行わなければならない (shall)。

  - 計測機能を備えた TOE ビルドをデバッガへロードする。
  - クリア対象となる TOE 内の鍵の値を記録する。
  - #1 の鍵に関する通常の暗号処理を TOE に行わせる。
  - TOE に鍵をクリアさせる。
  - TOE に実行を停止させるが、終了はさせない。
  - TOE に、TOE の全メモリフットプリントをバイナリファイルへダンプさせる。
  - #4 で作成されたバイナリファイルの内容から、#1 の既知の鍵の値のインスタンスを検索する。

  このテストは、ステップ#7 で#1 の鍵のコピーが見つからなかった場合に成功し、それ以外の場合に失敗する。

  評価者はこのテストを、暗号化された形態で永続するものを含めたすべての鍵に関し

て行い、中間コピーがクリアされることを保証しなければならない (shall)。

- テスト 2：TOE がファームウェアに実装されておりデバッガを用いることができない制限された運用環境で動作している場合、評価者は汎用オペレーティングシステム上で TOE のシミュレータを利用しなければならない (shall)。評価者は、シミュレートされたテスト環境という計測設備を説明し、得られたテスト結果を正当化する根拠を提供しなければならない (shall)。

暗号操作

FCS_COP.1(1) 暗号操作 (データの暗号化／復号に関して)

FCS_COP.1.1(1) [選択：TOE、TOE プラットフォーム] は、以下の指定された暗号アルゴリズム

- (NIST SP 800-38A に定義される) AES-CBC モード、

[選択：

- (NIST SP 800-38D に定義される) AES-GCM
- その他のモードなし]

及び暗号鍵サイズ 128 ビット、256 ビットに従って *[暗号化／復号]* を行わなければならない (shall)。

適用上の注意：

128 及び 256 ビットの鍵サイズは、FCS_TLSC_EXT.1 へ適合するため義務付けられる

保証アクティビティ：

TSS

TOE プラットフォームにより満たされる要件：ST 中に列挙された各プラットフォームについて、評価者は、そのプラットフォームの ST に主張される 1 つまたは複数の暗号化／復号機能にウェブブラウザの ST における 1 つまたは複数の暗号化／復号機能が含まれていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。また評価者は、、 (サポートされる各プラットフォームについて) 暗号化／復号機能が呼び出される方法が、ウェブブラウザの ST 中に選択されたモードと鍵サイズごとに記述されていることを検証するため、ウェブブラウザの ST の TSS を検査しなければならない (shall) (これはウェブブラウザにより実装されないメカニズムにより行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムはこの保証アクティビティの一部として TSS 中に識別されることになる)。

ガイダンス

N/A

テスト

TOE により満たされる要件：

AES-CBC テスト

AES-CBC 既知解テスト

既知解テスト (KAT) には、以下に記述される 4 つがある。すべての KAT において、平文、

暗号文、及び IV の値は 128 ビットのブロックとする (shall)。各テストの結果は、直接評価者により、あるいは入力を実装者へ供給しその結果を受領することにより、取得され得る。正しさを決定するため、評価者は結果の値を、同一の入力を既知の良好な実装へ与えることにより得られた値と比較しなければならない (shall)。

KAT-1。AES-CBC の暗号化機能をテストするため、評価者は 10 個の平文の値のセットを供給し、すべてゼロの鍵の値とすべてゼロの IV を用いて所与の平文の AES-CBC 暗号化から得られる暗号文の値を取得しなければならない (shall)。5 個の平文の値は 128 ビットのすべてゼロの鍵で暗号化されるものとし (shall)、それ以外の 5 個は 256 ビットのすべてゼロの鍵で暗号化されるものとする (shall)。

AES-CBC の復号機能をテストするため、評価者は 10 個の暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを行わなければならない (shall)。

KAT-2。AES-CBC の暗号化機能をテストするため、評価者は 10 個の鍵の値のセットを供給し、所与の鍵の値とすべてゼロの IV を用いてすべてゼロの平文の AES-CBC 暗号化から得られる暗号文の値を取得しなければならない (shall)。5 個の鍵は 128 ビットの鍵とし (shall)、それ以外の 5 個は 256 ビットの鍵とする (shall)。

AES-CBC の復号機能をテストするため、評価者はすべてゼロの暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを行わなければならない (shall)。

KAT-3。AES-CBC の暗号化機能をテストするため、評価者は以下に記述する 2 セットの鍵の値を供給し、所与の鍵の値とすべてゼロの IV を用いてすべてゼロの平文の AES 暗号化から得られる暗号文の値を取得しなければならない (shall)。第 1 の鍵のセットは 128 個の 128 ビットの鍵からなるものとし (shall)、第 2 のセットは 256 個の 256 ビットの鍵からなるものとする (shall)。[1,N] の範囲の i について、各セットの鍵 i の左端の i ビットは 1、右端の N-i ビットは 0 とする (shall)。

AES-CBC の復号機能をテストするため、評価者は以下に記述する 2 セットの鍵と暗号文の値のペアを供給し、所与の鍵の値とすべてゼロの IV を用いて所与の暗号文の AES-CBC 復号から得られる平文の値を取得しなければならない (shall)。第 1 の鍵／暗号文のペアのセットは 128 個の 128 ビットの鍵／暗号文のペアからなるものとし (shall)、第 2 のセットは 256 個の 256 ビットの鍵／暗号文のペアからなるものとする (shall)。[1,N] の範囲の i について、各セットの鍵 i の左端の i ビットは 1、右端の N-i ビットは 0 とする (shall)。各ペアの暗号文の値は、それに対応する鍵で復号された際にすべてゼロの平文が得られるような値とする (shall)。

KAT-4。AES-CBC の暗号化機能をテストするため、評価者は以下に記述する 128 個の平文の値のセットを供給し、2 種別の暗号文の値 (、すべてゼロの 128 ビットの鍵の値とすべてゼロの IV、及びすべてゼロの 256 ビットの鍵の値とすべてゼロの IV を用いて、所与の平文の AES-CBC 暗号化から得られる) を取得しなければならない (shall)。[1,128] の範囲の i について、各セットの平文の値 i の左端の i ビットは 1、右端の N-i ビットは 0 とする (shall)。

AES-CBC の復号機能をテストするため、評価者は暗号化テストにおける平文と同一の形式の暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを行わなければならない (shall)。

AES-CBC 複数ブロックメッセージテスト

評価者は、i 個のブロックからなるメッセージ (ここで 1 < i <=10) を暗号化することにより、暗号化機能をテストしなければならない (shall)。評価者は鍵、IV 及び長さ i ブロックの平文メッセージを選び、選んだ鍵及び IV により、試験すべきモードを用いてメッセージを暗

号化しなければならない (shall)。暗号文は、同一の平文メッセージを同一の鍵と IV により既知の良好な実装を用いて暗号化した結果と比較されなければならない (shall)。

また評価者は、i 個のブロックからなるメッセージ (ここで 1< i <=10) を復号することにより、各モードについて復号機能をテストしなければならない (shall)。評価者は鍵、IV 及び長さ i ブロックの暗号文メッセージを選び、選んだ鍵及び IV により、試験すべきモードを用いてメッセージを復号しなければならない (shall)。平文は、同一の暗号文メッセージを同一の鍵と IV により既知の良好な実装を用いて復号した結果と比較されなければならない (shall)。

AES-CBC モンテカルロテスト

評価者は、200 個の平文、IV、及び鍵の 3 つ組のセットを用いて、暗号化機能をテストしなければならない (shall)。これらのうち 100 個は 128 ビットの鍵を用いるものとし (shall)、100 個は 256 ビットの鍵を用いるものとする (shall)。平文と IV の値は、128 ビットのブロックとする (shall)。各 3 つ組について、以下のように 1000 回の反復処理が実行されるものとする (shall)。

```
# 入力：PT, IV, Key
for i = 1 to 1000:
        if i == 1:
                CT[1] = AES-CBC-Encrypt(Key, IV, PT)
                PT = IV
        else:
                CT[i] = AES-CBC-Encrypt(Key, PT)
                PT = CT[i-1]
```

1000 回目の反復処理において計算された暗号文 (すなわち、CT[1000]) が、その試行の結果となる。この結果は、既知の良好な実装を用いて同一の値により 1000 回反復処理を実行した結果と比較されなければならない (shall)。

評価者は、暗号化と同一のテストを用い、CT と PT とを入れ替え、AES-CBC-Encrypt を AES-CBC-Decrypt で置き換えて、復号機能をテストしなければならない (shall)。

AES-GCM モンテカルロテスト

評価者は、以下の入力パラメタ長の各組み合わせについて、AES-GCM の認証済み暗号化機能をテストしなければならない (shall)。

- 128 ビット及び 256 ビットの鍵
- 2 とおりの平文の長さ。平文の長さの一方は、128 ビットのゼロ以外の整数倍とする (shall) (サポートされる場合)。他方の平文の長さは、128 ビットの整数倍であってはならないものとする (shall not) (サポートされる場合)。
- 3 とおりの AAD の長さ。1 つの AAD の長さは 0 とする (shall) (サポートされる場合)。1 つの AAD の長さは、128 ビットのゼロ以外の整数倍とする (shall) (サポートされる場合)。1 つの AAD の長さは、128 ビットの整数倍であってはならないものとする (shall not) (サポートされる場合)。
- 2 とおりの IV の長さ。96 ビットの IV がサポートされる場合、テストされる 2 とおり

の IV の長さの一方を 96 ビットとする (shall)。

評価者は、上記のパラメタ長の各組み合わせについて、10 個の鍵、平文、AAD、及び IV の組のセットを用いて暗号化機能をテストし、AES-GCM 認証済み暗号化から得られた暗号文とタグを取得しなければならない (shall)。サポートされている各タグ長は、10 個のセットにつき少なくとも一回はテストされなければならない (shall)。IV の値は、それが既知である限り、評価者により供給されても、テストされている実装により供給されてもよい。

評価者は、上記のパラメタ長の各組み合わせについて、10 個の鍵、平文、暗号文、タグ、AAD、及び IV の 5 つ組のセットを用いて復号機能をテストし、認証に関する合格／不合格結果を取得して、合格の場合には平文を復号しなければならない (shall)。セットには、合格となる 5 組と不合格となる 5 組が含まれなければならない (shall)。

各テストの結果は、直接評価者により、あるいは入力を実装者へ供給しその結果を受領することにより、取得され得る。正しさを決定するため、評価者は結果の値を、同一の入力を既知の良好な実装へ与えることにより得られた値と比較しなければならない (shall)。

FCS_COP.1(2) 暗号操作 (暗号ハッシュに関して)

FCS_COP.1.1(2) [選択：TOE、TOE プラットフォーム] は、以下の指定された暗号アルゴリズム

- SHA-1;
- SHA-256;
- SHA-384;
- [選択：SHA-512、その他のアルゴリズムなし]

及びメッセージダイジェストのサイズが 160、256、384 及び [選択：512、その他のサイズなし] であって、以下：FIPS PUB 180-4 を満たすものに従って暗号ハッシュを行わなければならない (shall)。

適用上の注意：

本 PP の将来の版では、SHA-1 は選択肢から削除されるかもしれない。SHA-1 によるデジタル署名の生成はもはや許可されず、また SHA-1 によるデジタル署名の検証は、これらの署名の受容に存在する可能性のあるリスクのため、強く非推奨とされる。SHA-1 は現在、FCS_TLSC_EXT.1 に適合するため要求されている。SHA-256 及び SHA-384 は、FCS_TLSC_EXT.1 へ適合するため義務付けられる

本要件の意図は、高信頼更新及び高信頼チャネルと関連したデジタル署名生成及び検証に用いられるハッシュ機能を指定することである。ハッシュの選択は、メッセージダイジェストサイズの選択をサポートしなければならない (must)。ハッシュの選択は、FCS_COP.1(1) に用いられるアルゴリズムの全体的な強度と一貫しているべきである (should)。

保証アクティビティ：

TSS

プラットフォームにより満たされる要件：本要件の意図は、高信頼更新及び高信頼チャネルと関連したデジタル署名生成及び検証に用いられるハッシュ機能を指定することである。ハッシュの選択は、メッセージダイジェストサイズの選択をサポートしなければならない (must)。ハッシュの選択は、FCS_COP.1(1) に用いられるアルゴリズムの全体的な強度と一

貫しているべきである (should)。

TOE により満たされる要件 : 評価者は AGD 文書をチェックして、必要とされるハッシュのサイズに機能を構成するために行われることが必要とされる構成があれば、それが存在することを決定しなければならない (shall)。評価者は、ハッシュ機能と他の TSF 暗号機能 (例えば、デジタル署名検証機能) との関連が TSS に文書化されていることをチェックしなければならない (shall)。

ガイダンス

N/A

テスト

TOE により満たされる要件 :

TSF ハッシュ関数は、2 つのモードのいずれかで実装できる。第 1 のモードは、バイト指向モードである。このモードでは、TSF は長さがバイトの整数倍であるメッセージのみをハッシュする。すなわち、ハッシュされるべきメッセージのビット長が 8 で割り切れる必要がある。第 2 のモードは、ビット指向モードである。このモードでは、TSF は任意の長さのメッセージをハッシュする。各モードについて異なるテストが存在するため、ビット指向とバイト指向のテストについて、以下のセクションで指示を与える。

評価者は、TSF により実装され、本 PP の要件を満たすために用いられる各ハッシュアルゴリズムについて、以下のテストをすべて行わなければならない (shall)。

ショートメッセージテスト—ビット指向モード

評価者は m+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは、0 から m ビットまでシーケンシャルに変化する。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、各メッセージのメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

ショートメッセージテスト—バイト指向モード

評価者は m/8+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは 0 から m/8 バイトまでシーケンシャルに変化し、各メッセージは整数個のバイトとなる。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、各メッセージのメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

選択されたロングメッセージテスト—ビット指向モード

評価者は m 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。i 番目のメッセージの長さは 512 + 99*i となる (ここで $1 \leq i \leq m$)。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、各メッセージのメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

選択されたロングメッセージテスト—バイト指向モード

評価者は m/8 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。i 番目のメッセージの長さは 512 + 8*99*i となる (ここで $1 \leq i \leq m/8$)。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、各メッセージのメッセージダイジェストを計算し、メッセージが TSF へ提供された

際に正しい結果が得られることを保証する。

疑似ランダム的に生成されたメッセージテスト

このテストは、バイト指向の実装にのみ行われる。評価者は、n ビットの長さのシードをランダムに生成する。ここで n はテストされるハッシュ関数により作成されるメッセージダイジェストの長さである。次に評価者は、[SHAVS] の図 1 に示されるアルゴリズムに従って 100 個のメッセージと関連するダイジェストのセットを作成する。次に評価者は、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

FCS_COP.1(3) 暗号操作 (暗号署名に関して)

FCS_COP.1.1(3) [選択：TOE、TOE プラットフォーム] は、以下に指定された暗号アルゴリズムに従って暗号署名サービスを行わなければならない (shall)。

- 2048 ビット以上の鍵サイズ (モジュラス) を用いる RSA デジタル署名アルゴリズム (rDSA) であって FIPS PUB 186-2 または FIPS PUB 186-4, “Digital Signature Standard” を満たすもの、
- 256 ビット以上の鍵サイズを用いる楕円曲線デジタル署名アルゴリズム (ECDSA) であって FIPS PUB 186-4, “Digital Signature Standard”と (FIPS PUB 186-4, “Digital Signature Standard”に定義される)「NIST 曲線」 P-256、P-384 及び [選択：P-521、その他の曲線なし] を満たすもの、

[選択：

- 2048 ビット以上の鍵サイズ (モジュラス) を用いるデジタル署名アルゴリズム (DSA) であって FIPS PUB 186-4, “Digital Signature Standard”を満たすもの、
- その他の暗号署名サービスなし

]。

適用上の注意：

TOE は、FCS_TLSC_EXT.1 に従って RSA 及び ECDSA デジタル署名を行わなければならない (must)。また TOE プラグイン及び拡張機能上の署名を検証してもよい。

複数のスキームがサポートされている場合、ST 作成者は本要件を繰り返し、この機能を取り込むべきである (should)。使用するスキームは、ST 作成者により選択肢から選択される。

保証アクティビティ：

TSS

TOE プラットフォームにより満たされる要件：ST 中に列挙された各プラットフォームについて、評価者は、そのプラットフォームの ST に主張されるデジタル署名機能にウェブブラウザの ST におけるデジタル署名機能が含まれていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。また評価者は、、 (サポートされる各プラットフォームについて) デジタル署名機能が呼び出される方法が、ウェブブラウザ中に用いられる操作ごとに記述されていることを検証するため、ウェブブラウザの ST の TSS を検査しなければならない (shall) (これはウェブブラウザにより実装されないメカニズムにより行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムはこの保証アクティビティの一部として TSS 中に識別されることになる)。

ガイダンス

N/A

テスト

TOE により満たされる要件：

鍵生成：

RSA 署名スキームの鍵生成

評価者は、鍵生成テストを用いて TOE による RSA 鍵生成の実装を検証しなければならない (shall)。このテストは、公開鍵検証指数 e、プライベート素因数 p 及び q、公開モジュラス (modulus) n 及びプライベート署名指数 d の計算を含めた鍵コンポーネントの値を正しく求める TSF の能力を検証する。

鍵ペア生成では、素数 p 及び q を生成するための 5 とおりの方法 (または手法) を指定している。これには、以下のものが含まれる。

- ランダム素数：
  - 証明可能素数
  - 確率的素数
- 条件付き素数：
  - 素数 p1、p2、q1、q2、p 及び q を、すべて証明可能素数とする (shall)
  - 素数 p1、p2、q1 及び q2 を証明可能素数とし (shall)、p 及び q を確率的素数とする (shall)
  - 素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数とする (shall)

ランダム証明可能素数手法とすべての条件付き素数手法の鍵生成手法をテストするため、評価者は決定論的に RSA 鍵ペアを生成するために十分なデータをシードとして TSF 鍵生成ルーチンに与えなければならない (must)。これには、1 つまたは複数の乱数シード、RSA 鍵の公開鍵指数、及び望ましい鍵の長さが含まれる。サポートされている各鍵長について、評価者は 25 個の鍵ペアを TSF に生成させなければならない (shall)。評価者は、TSF により生成された値を既知の良好な実装から生成された値と比較することにより、TSF の実装の正しさを検証しなければならない (shall)。

ECDSA 鍵生成テスト

FIPS 186-4 ECDSA 鍵生成テスト

サポートされている各 NIST 曲線、すなわち P-256、P-284 及び P-521 について、評価者は 10 個のプライベート鍵／公開鍵ペアを試験対象実装 (IUT) に生成させなければならない (shall)。プライベート鍵は、承認済みランダムビット生成器 (RBG) を用いて生成されなければならない (shall)。正しさを決定するため、評価者は生成された鍵ペアを既知の良好な実装の公開鍵検証 (PKV) 機能へ提出しなければならない (shall)。

FIPS 186-4 公開鍵検証 (PKV) テスト

サポートされている各 NIST 曲線、すなわち P-256、P-284 及び P-521 について、評価者は既知の良好な実装の鍵生成機能を用いて 10 個のプライベート鍵／公開鍵ペアを生成し、5 個の公開鍵を不正な値となるように変更し、5 個を未変更の (すなわち、正しい) 値のままにしなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

ECDSA アルゴリズムテスト

ECDSA FIPS 186-4 署名生成テスト

サポートされている NIST 曲線 (すなわち、P-256、P-284 及び P-521) と SHA 関数の各ペアについて、評価者は 10 個の 1024 ビットの長さのメッセージを生成し、各メッセージについて公開鍵ならびに得られた署名の値 R 及び S を取得しなければならない (shall)。正しさを決定するため、評価者は既知の良好な実装の署名検証機能を利用しなければならない (shall)。

ECDSA FIPS 186-4 署名検証テスト

サポートされている NIST 曲線 (すなわち、P-256、P-284 及び P-521) と SHA 関数の各ペアについて、評価者は 10 個の 1024 ビットの長さのメッセージ、公開鍵及び署名の組のセットを生成し、10 組のうち 5 組で値のいずれか (メッセージ、公開鍵または署名) を変更しなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

RSA 署名アルゴリズムテスト

署名生成テスト

評価者は、署名生成テストを用いて TOE による RSA 署名生成の実装を検証しなければならない (shall)。このテストを行うために評価者は、TSF のサポートするモジュラスのサイズ／SHA の各組み合わせについて、高信頼リファレンス実装から 10 個のメッセージを生成または取得しなければならない (must)。評価者は、TOE に自分のプライベート鍵とモジュラスの値を用いてこれらのメッセージへ署名させなければならない (shall)。

評価者は、既知の良好な実装及び関連付けられた公開鍵を用いて署名を検証することにより、TSF の署名の正しさを検証しなければならない (shall)。

署名検証テスト

評価者は、署名検証テストを行って、相手方の有効及び無効な署名を認識する TOE の能力を検証しなければならない (shall)。評価者は、公開鍵 e、メッセージ、IR フォーマット、または署名、あるいはこれらのうち 2 つ以上にエラーを導入することにより、署名検証テスト中に作成されたテストベクトルへエラーを注入しなければならない (shall)。TOE は署名の検証を試行し、成功または失敗を返す。

評価者はこれらのテストベクトルを利用して、対応するパラメタを用いた署名検証テストをエミュレートし、TOE がこれらのエラーを検出することを検証しなければならない (shall)。

FCS_COP.1(4) 暗号操作 (鍵付きハッシュによるメッセージ認証)

FCS_COP.1.1(4) [選択：TOE、TOE プラットフォーム] は、以下の指定された暗号アルゴリズム

- HMAC- SHA-256

[選択：

- SHA-1
- SHA-384
- SHA-512

- その他のアルゴリズムなし

]、

鍵サイズが [割付 : *HMAC に用いられる (ビット単位の) 鍵サイズ*]、そしてメッセージダイジェストのサイズが 256 及び [選択 : 160、384、512、その他のサイズなし] ビットの、以下 : FIPS Pub 198-1, The Keyed-Hash Message Authentication Code”, と FIPS Pub 180-4, “Secure Hash Standard”を満たすものに従って、鍵付きハッシュによるメッセージ認証を行わなければならない (shall)。

適用上の注意 :

本要件の意図は、TOE により用いられるさまざまな暗号プロトコル (例えば高信頼チャネル) の鍵確立の目的で用いられる際に用いられる鍵付きハッシュによるメッセージ認証機能を指定することである。ハッシュの選択は、メッセージダイジェストサイズの選択をサポートしなければならない (must)。ハッシュの選択は、FCS_COP.1(1) に用いられるアルゴリズムの全体的な強度と一貫しているべきである (should)。HMAC-SHA256 は、FCS_TLSC_EXT.1 に要求される暗号スイートへ適合するため要求される。

保証アクティビティ :

プラットフォームにより満たされる要件:ST 中に列挙された各プラットフォームについて、評価者は、そのプラットフォームの ST に主張される 1 つまたは複数の鍵付きハッシュ機能にウェブブラウザの ST における 1 つまたは複数の鍵付きハッシュ機能が含まれていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。また評価者は、、 (サポートされる各プラットフォームについて) 鍵付きハッシュ機能が呼び出される方法が、ウェブブラウザの ST 中に選択されたモードと鍵サイズごとに記述されていることを検証するため、ウェブブラウザの ST の TSS を検査しなければならない (shall) (これはウェブブラウザにより実装されないメカニズムにより行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムはこの保証アクティビティの一部として TSS 中に識別されることになる)。

TOE により満たされる要件 : 評価者は、HMAC 機能により利用される以下の値が指定されていることを保証するため、TSS を検査しなければならない (shall) : 鍵の長さ、用いられるハッシュ関数、ブロックサイズ、そして用いられる出力 MAC 長。

ガイダンス

N/A

テスト

TOE により満たされる要件 :

サポートされている各パラメタセットについて、評価者は 15 セットのテストデータを構成しなければならない (shall)。各セットは、1 つの鍵とメッセージデータから構成されるものとする (shall)。評価者は、テストデータのこれらのセットについて TSF に HMAC タグを生成させなければならない (shall)。得られた MAC タグは、同一の鍵と IV により既知の良好な実装を用いて生成された HMAC タグと比較されなければならない (shall)。

Hypertext Transport Protocol Secure (HTTPS)

FCS_HTTPS_EXT.1 拡張 : HTTPS の実装

FCS_HTTPS_EXT.1.1 [選択 : TOE、TOE プラットフォーム] は、RFC 2818 に準拠する

HTTPS プロトコルを実装しなければならない (shall)。

FCS_HTTPS_EXT.1.2 [選択：TOE、TOE プラットフォーム] は、FCS_TLSC_EXT.1 に指定される TLS を用いて HTTPS を実装しなければならない (shall)。

保証アクティビティ：

評価者は、ウェブサーバとの HTTPS 接続を試行し、パケットアナライザでトラフィックを確認し、そして接続が成功しトラフィックが TLS または HTTPS と識別されることを検証しなければならない (shall)。他のすべてのテストは、FCS_TLSC_EXT.1 と組み合わせて行われる。

ランダムビット生成

FCS_RBG_EXT.1 拡張：ランダムビット生成

FCS_RBG_EXT.1.1 [選択：TOE、TOE プラットフォーム] は、 [選択、1 つを選択：[選択：Hash_DRBG (任意) 、HMAC_DRBG (任意) 、CTR_DRBG (AES) 、Dual_EC_DRBG (任意)] を用いる NIST Special Publication 800-90A、FIPS Pub 140-2 附属書 C：AES を用いる X9.31 附属書 2.4] に従って、すべての決定論的ランダムビット生成サービスを行わなければならない (shall) 。

FCS_RBG_EXT.1.2 決定論的 RBG は、鍵とそれが生成するハッシュとの (NIST SP 800-57 による) セキュリティ強度の大きいほうと少なくとも等しい、最小で [選択：128 ビット、256 ビット] のエントロピーを持つ、 [選択：ソフトウェアベースの雑音源、プラットフォームベースの RBG] からエントロピーを蓄積するエントロピー源によりシードが供給されなければならない (shall)。

適用上の注意：

FCS_RBG_EXT.1.1 の最初の選択に関しては、ST 作成者は TOE か TOE のインストールされるプラットフォームのどちらが RBG サービスを提供するか選択すべきである (should)。

NIST Special Pub 800-90B の附属書 C には、FIPS-140 の将来のバージョンでおそらく必要とされることになる最小エントロピー量が記述されている。可能であれば直ちにこれを用いるべきであり (should)、また本 PP の将来のバージョンでは要求されることになる。

FCS_RBG_EXT.1.1 の 2 番目の選択に関しては、ST 作成者は RBG サービスが適合する標準 (800-90 または 140-2 附属書 C のいずれか) を選択すべきである (should)。

SP 800-90A には、4 つの異なる乱数生成手法が含まれる。これらは、基盤となる暗号プリミティブ (ハッシュ関数／暗号) に依存している。ST 作成者は利用される関数を選択し (800-90A が選択されている場合)、要件または TSS に用いられる具体的な基盤となる暗号プリミティブを取り込む。識別されたハッシュ関数はいずれも Hash_DRBG または HMAC_DRBG に許可されるが、CTR_DRBG には AES ベースの実装のみが許可される。800-90A に定義された任意の曲線が Dual_EC_DRBG に許可される一方で、ST 作成者は選択された曲線だけではなく、利用されるハッシュアルゴリズムも取り込まなければならない (must)。

FCS_RBG_EXT.1.2 の 2 番目の選択に関しては、ST 作成者はエントロピー源がソフトウェアベースであるか、プラットフォームベースであるか、あるいはその両方であるかを示す。エントロピーの源が複数存在する場合には、ST には各エントロピー源について、それがソフトウェアベースであるかプラットフォームベースであるかを含めて説明する。プラットフォームベースの雑音源が望ましい。

プラットフォームベースのRBG 源は、プラットフォームにより提供される検証済みのRBG の出力であり、これはFCS_RBG_EXT.1.1 に従ってTSF の提供するDRBG のエントロピー源として利用される。このようにして、開発者はNIST SP800-90C に記述されているようにRBG を連鎖する。

FIPS Pub 140-2 の附属書 C については、現在のところ NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション3 に記述される手法のみが有効であることに注意されたい。ここで用いられるAES 実装の鍵の長さが利用者データの暗号化に用いられるものと異なる場合には、FCS_COP.1 を調整するか繰り返して異なる鍵の長さを反映する必要があるかもしれない。FCS_RBG_EXT.1.2(1) の選択については、ST 作成者はRBG にシードを供給するために用いられるエントロピーの最小ビット数を選択する。

またST 作成者は、任意の基盤となる機能がTOE のベースライン要件に確実に含まれるようにする。

保証アクティビティ：

TSS

プラットフォームにより満たされる要件:ST 中に列挙された各プラットフォームについて、評価者は、そのプラットフォームの ST に主張される RBG 機能にウェブブラウザの ST における RBG 機能が含まれていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。また評価者は、、 (サポートされる各プラットフォームについて) RBG 機能が呼び出される方法が、ウェブブラウザ中に用いられる操作ごとに記述されていることを検証するため、ウェブブラウザの ST の TSS を検査しなければならない (shall) (これはウェブブラウザにより実装されないメカニズムにより行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムはこの保証アクティビティの一部として TSS 中に識別されることになる)。

TOE により満たされる要件 : 附属書 E に従って、文書が作成されなければならない (shall) (そして評価者はアクティビティを行わなければならない (shall))。

ST 作成者がプラットフォームベースの雑音源を選択した場合、評価者は、プラットフォームの RBG が検証されていることを検証するため、プラットフォームの ST を検査しなければならない (shall)。評価者は、少なくともこのプロファイルに関して ST 作成者により選択されたエントロピー量が、プラットフォームの RBG に供給されていることを検証しなければならない (shall)。この場合、ST 作成者はプラットフォームの RBG の附属書 E 文書に責任を負わない。

ガイダンス

N/A

テスト

TOE により満たされる要件 :

評価者は、RBG が準拠する標準に従って、以下のテストを行わなければならない (shall)。

FIPS 140-2 の附属書 C に準拠する実装

このセクションに含まれるテストの参照情報は、The Random Number Generator Validation System (RNGVS) である。評価者は、以下の 2 つのテストを実施しなければならない (shall)。「期待値」は、正しいことが知られているアルゴリズムの参照実装により作成されることに注意されたい。正しさの証明は、各スキームに任される。

評価者は、可変シードテストを行わなければならない (shall)。評価者は (Seed, DT) ペア (128 ビット) の 128 個のセットを TSF の RBG 機能に提供しなければならない (shall)。また評価者は、128 ペアの (Seed, DT) すべてについて一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなければならない (shall)。DT の値は、各セットについて 1 ずつ増やされる。シードの値は、セットの中で繰り返されてはならない (shall not)。評価者は、TSF により返される値が期待値と一致することを保証する。

評価者は、モンテカルロテストを行わなければならない (shall)。このテストについては、評価者がシード及び DT の初期値 (128 ビット) を TSF の RBG 機能に提供する。また評価者は、テストを通して一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなければならない (shall)。次に評価者は、繰返しのたびに DT の値を 1 ずつ増やしながら、そして NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション 3 に指定されるように次回の繰返しの際の新たなシードを作成して、TSF の RBG を 10,000 回呼び出す。評価者は、得られた 10,000 番目の値が期待値と一致することを保証する。

NIST Special Publication 800-90A に準拠する実装

評価者は、RBG 実装の 15 回の試行を行わなければならない (shall)。RBG が構成可能な場合、評価者は各構成について 15 回の試行を行わなければならない (shall)。また評価者は、RBG 機能を構成するための適切な指示が操作ガイダンスに含まれていることも確認しなければならない (shall)。

RBG が有効な予測困難性を持つ場合、各回の試行は (1) DRBG をインスタンス化し、 (2) ランダムなビットの最初のブロックを生成し、 (3) ランダムなビットの 2 番目のブロックを生成し、 (4) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成しなければならない (shall)。最初はカウント (0〜14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして個別化文字列である。次の 2 つは、最初の生成呼び出しへの追加的入力とエントロピー入力である。最後の 2 つは、2 番目の生成呼出しへの追加的入力とエントロピー入力である。これらの値は、ランダムに生成される。「ランダムなビットのひとつのブロックを生成」とは、返されるビット数が (NIST SP 800-90A に定義される) Output Block Length と等しいランダムなビットを生成することを意味する。

RBG が予測困難性を持たない場合、各回の試行は (1) DRBG をインスタンス化し、 (2) ランダムなビットの最初のブロックを生成し、 (3) シードを再供給し、 (4) ランダムなビットの 2 番目のブロックを生成し、 (5) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成しなければならない (shall)。最初はカウント (0〜14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして個別化文字列である。5 番目の値は、最初の生成呼出しへの追加的入力である。6 番目と 7 番目は、シードを再供給する呼出しへの追加的入力とエントロピー入力である。最後の値は、2 回目の生成呼出しへの追加的入力である。

以下のパラグラフには、評価者により生成／選択されるべき入力値のいくつかについて、より多くの情報が含まれている。

エントロピー入力: エントロピー入力値の長さは、シードの長さと等しくなければならない (must)。

ノンス: ノンスがサポートされている場合 (導出関数 (df) なしの CTR_DRBG はノンスを

利用しない)、ノンスのビット長はシードの長さの半分となる。

個別化文字列：個別化文字列の長さは、シードの長さ以下でなければならない (must)。実装が 1 とおりの個別化文字列の長さしかサポートしていない場合には、両方の値に同一の長さが使用できる。2 とおり以上の文字列の長さがサポートされている場合、評価者は 2 つの異なる長さの個別化文字列を用いなければならない (shall)。実装が個別化文字列を用いない場合、値を供給する必要はない。

追加的入力：追加的入力のビット長は、個別化文字列の長さと同一のデフォルトと制約を持つ。

トランスポート層セキュリティ (Transport Layer Security)

FCS_TLSC_EXT.1 拡張：TLS

FCS_TLSC_EXT.1.1 [選択：TOE、TOE プラットフォーム] は、以下の暗号スイートをサポートして TLS 1.2 (RFC 5246) を実装しなければならない (shall)：

必須暗号スイート：

- RFC 3268 に定義される TLS_RSA_WITH_AES_128_CBC_SHA
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
-

オプションの暗号スイート：

[選択：

- RFC 3268 に定義される TLS_RSA_WITH_AES_256_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- その他の暗号スイートなし

]。

適用上の注意：

評価される構成に用いられる暗号スイートは、本要件により制限される。ST 作成者は、サポートされるオプションの暗号スイートを選択すべきである (should)。必須スイート以外にサポートされる暗号スイートが存在しない場合には、「なし」が選択されるべきである (should)。テスト環境中のサーバ上で評価される構成において管理的に用いられることが可能な暗号スイートを制限することは必要である。上に列挙した Suite B アルゴリズム (RFC 6460) は、実装に望ましいアルゴリズムである。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 との適合を確実にするため要求されている。

FCS_TLSC_EXT.1.2 TOE は、証明書に含まれる識別名 (DN) がピアに期待される DN にマッチしない場合、高信頼チャネルを確立してはならない (shall not)。

適用上の注意：

DN は、証明書の Subject Name フィールドまたは Subject Alternative Name 拡張に存在するかもしれない。期待される DN は、構成されてもよいし、あるいはピアにより用いられるドメイン名または IP アドレスと比較されてもよい。

高信頼通信チャネルには、TSF または TOE プラットフォームにより実施される TLS、HTTPS、または DTLS のいずれかが含まれる。高信頼チャネルを確立するための有効性チェックは、FIA_X509_EXT.1 と組み合わせて行われる。

FCS_TLSC_EXT.1.3 TOE は、Client Hello 中の signature_algorithm 拡張に以下のハッシュアルゴリズムを提示しなければならない (shall)： [選択：SHA256、SHA384、SHA512] 及びその他のハッシュアルゴリズムなし。

適用上の注意：

本要件は、クライアントによるデジタル署名検証の目的でサポートされるハッシュアルゴリズムを制限すると共に、サーバによるデジタル署名生成の目的でサポートされるハッシュにサーバを制限する。signature_algorithm 拡張は、TLS 1.2 のみによりサポートされる。

FCS_TLSC_EXT.1.4 TOE は、Client Hello 中の Supported Elliptic Curves Extension 拡張に以下の NIST 曲線を提示しなければならない (shall)： [選択：secp256r1、secp384r1、secp521r1] 及びその他の曲線なし。

適用上の注意：

本要件は、認証及び鍵共有のために許可される楕円曲線を FCS_COP.1(3) 及び FCS_CKM.1(1) からの NIST 曲線に制限する。この拡張は、楕円曲線暗号スイートをサポートするクライアントについて要求される。

保証アクティビティ：

TSS

評価者は TSS 中のこのプロトコルの実装の記述をチェックして、サポートされる暗号スイートが指定されていることを保証しなければならない (shall)。評価者は TSS をチェックして、指定された暗号スイートがこのコンポーネントに列挙されたものを含むことを保証しなければならない (shall)。また評価者は操作ガイダンスをチェックして、TLS が TSS 中の記述と適合するように TOE を構成することに関する指示が含まれることを保証しなければならない (shall)。

評価者は、証明書中の DN が期待される DN と比較される方法が TSS に記述されていることを検証しなければならない (shall)。評価者は、HTTPS 接続について、期待される DN が

ピアのドメイン名または IP アドレスであること、比較が自動的に行われること、そして DN 中のワイルドカードがどのように用いられるか TSS に記述されていることを検証しなければならない (shall)。

評価者は、signature_algorithm 拡張について、そして要求されるふるまいがデフォルトで実施されるのか構成され得るのかのどちらであるか、TSS に記述されていることを検証しなければならない (shall)。

評価者は、Supported Elliptic Curves 拡張について、そして要求されるふるまいがデフォルトで実施されるのか構成され得るのかのどちらであるか、TSS に記述されていることを検証しなければならない (shall)。

ガイダンス

DN が自動的にドメイン名や IP アドレスと比較されない場合、評価者はその接続に期待される DN の構成が AGD ガイダンスに含まれることを保証しなければならない (shall)。

本要件を満たすためには signature_algorithm 拡張が構成されなければならない (must) ことが TSS に示されている場合、評価者は AGD ガイダンスに signature_algorithm 拡張の構成が含まれることを検証しなければならない (shall)。

本要件を満たすためには Supported Elliptic Curves 拡張が構成されなければならない (must) ことが TSS に示されている場合、評価者は AGD ガイダンスに Supported Elliptic Curves 拡張の構成が含まれることを検証しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、要件に指定された暗号スイートのを用いて、TLS 接続を確立しなければならない (shall)。この接続は、より高位のプロトコルの確立の一部として確立されてもよい (例えば、EAP セションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。
- テスト 2 : 評価者は、extendedKeyUsage フィールド中にサーバ認証目的を含むサーバ証明書を持ったサーバを用いて接続を確立する試行を行い、接続が確立されることを検証しなければならない (shall)。次に評価者は、extendedKeyUsage フィールド中にサーバ認証目的を含まないこと以外は有効なサーバ証明書をクライアントが拒否し、接続が確立されないことを検証する。理想的には、2 つの証明書は extendedKeyUsage フィールドを除いて同一であるべきである (should)。
- テスト 3 : 評価者は、構成された期待される DN またはピアのドメイン名／IP アドレスのいずれかに DN がマッチする証明書による接続を試行しなければならない (shall)。評価者は、TSF が接続を成功できることを検証しなければならない (shall)。評価者は、構成された期待される DN またはピアのドメイン名／IP アドレスのいずれにも DN がマッチしない証明書による接続を試行しなければならない (shall)。評価者は、TSF が接続を成功できないことを検証しなければならない (shall)。接続の失敗を示す利用者通知は、FIA_X509_EXT.2.3 に従って受容可能である。
- テスト 4 : 評価者は、TLS 接続中にクライアントの signature_algorithm 拡張にしたがえばサポートされない証明書を送信する (例えば、SHA-1 署名を持つ証明書を送信する) ようにサーバを構成しなければならない (shall)。評価者は、TOE が ServerCertificate ハンドシェイクメッセージを受信した後に切断することを検証しな

ければならない (shall) 。

- テスト 5：評価者は、サポートされない曲線 (例えば P-192) を用いて ECDHE 鍵交換を行うようサーバを構成しなければならず (shall)、そして TOE が ServerKeyExchange ハンドシェイクメッセージを受信した後に切断することを検証しなければならない (shall) 。
- テスト 6：評価者は、サーバにより選択された暗号スイートとマッチしない証明書を TLS 接続中に送信する (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用しているのに ECDSA 証明書を送信したり、ECDSA 暗号スイートのいずれかを使用しているのに RSA 証明書を送信したりする) ようサーバを構成しなければならない (shall)。評価者は、TOE が ServerCertificate ハンドシェイクメッセージを受信した後に切断することを検証しなければならない (shall) 。
- テスト 7：評価者は、TLS_NULL_WITH_NULL_NULL 暗号スイートを選択するようサーバを構成し、クライアントが接続を拒否することを検証しなければならない (shall)。
- テスト 8：評価者は、TOE とサーバとの間に中間者ツールを設定しなければならず (shall)、またトラフィックに以下の改変を行わなければならない (shall)。
    - ServerHello 中のサーバにより選択される TLS バージョンを、サポートされない TLS バージョン (例えば 03 04 の 2 バイトにより表現される 1.3) に変更し、クライアントが接続を拒否することを検証する。
    - ServerHello ハンドシェイクメッセージ中のサーバのノンス中の少なくとも 1 バイトを改変して、ServerKeyExchange ハンドシェイクメッセージをクライアントが拒否すること (DHE または ECDHE 暗号スイートの場合) またはクライアントの Finished ハンドシェイクメッセージをサーバが拒否すること検証する。
    - ServerHello ハンドシェイクメッセージ中のサーバの選択された暗号スイートを、ClientHello ハンドシェイクメッセージ中に提示されない暗号スイートに改変する。評価者は、クライアントが ServerHello を受信した後に接続を拒否することを検証しなければならない (shall) 。
    - サーバの KeyExchange ハンドシェイクメッセージ中の署名ブロックを改変して、クライアントが ServerKeyExchange の受信後に接続を拒否することを検証する。
    - 相互認証を要求するようサーバを構成し、次にサーバの CertificateRequest ハンドシェイクメッセージ中の CA フィールド中の 1 バイトを改変する。改変された CA フィールドは、クライアントの証明書の署名に用いられた CA であってはならない (must not)。評価者は、サーバがクライアントの Finished ハンドシェイクメッセージを受信した後に接続を拒否することを検証しなければならない (shall) 。
    - サーバの Finished ハンドシェイクメッセージの 1 バイトを改変して、受信後にクライアントが fatal alert を送信しアプリケーションデータを全く送信しないことを検証する。
    - クライアントが ChangeCipherSpec メッセージを発行した後にサーバから暗号化されていないパケットを送信し、クライアントが接続を拒否することを検証する。

4.3.2 クラス：識別と認証 (FIA)

X509 証明書

FIA_X509_EXT.1 拡張：X509 有効性確認

FIA_X509_EXT.1.1 [選択：TOE、TOE プラットフォーム] は、以下のルールに従って証明書の有効性を確認しなければならない (shall)：

- RFC 5280 証明書有効性確認及び認証パス検証。
- TSF は、すべての CA 証明書について、basicConstraints 拡張の存在と cA フラグが TRUE にセットされていることを保証することにより、認証パスを検証しなければならない (shall)。
- TSF は、 [選択：RFC 2560 に指定されるオンライン証明書状態プロトコル (OCSP)、RFC 5759 に指定される証明書失効リスト (CRL)] を用いて証明書の失効状態を検証しなければならない (shall)。
- TSF は、以下のルールに従って extendedKeyUsage フィールドを検証しなければならない (shall)。
  - 高信頼更新及び実行可能コードの完全性検証に用いられる証明書は、コード署名目的 (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) を持たなければならない (shall)。
  - TLS に提示されるサーバ証明書は、extendedKeyUsage フィールドにサーバ認証目的 (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) を持たなければならない (shall)。

適用上の注意：

FIA_X509_EXT.1.1 には、証明書有効性確認を行うためのルールが列挙されている。ST 作成者は、失効状態が OCSP か CRL のどちらを用いて検証されるか選択しなければならない (shall)。証明書は、TOE の高信頼更新のため (FPT_TUD_EXT.1.3) 及びプラグインや拡張機能のインストールのため (FPT_TUD_EXT.2.3 及び FPT_TUD_EXT.3.3) にオプションとして用いてもよく、また TOE により実装されている場合には、コード署名目的 extendedKeyUsage を含むことが検証されなければならない (must)。FCS_TLSC_EXT.1 を用いたウェブサーバとの認証を行うには証明書が利用されなければならず (must)、また証明書にサーバ認証目的 extendedKeyUsage が含まれることが検証されなければならない (must)。

TSF あるいは TOE プラットフォームの選択にかかわらず、証明書の有効性確認はプラットフォームにより管理されるルートストア中の信頼済みルート証明書に至ることが期待される。

FIA_X509_EXT.1.1 は TOE プラットフォームに、TLS サーバにより提示される証明書に関して一定のチェックを行うことを要求しているが、クライアントにより提示される証明書に関してサーバが行わなければならない (have to) これに対応するチェックも存在する。すなわち、クライアント証明書の extendedKeyUsage フィールドに "Client Authentication" が含まれ、また鍵共有 (key agreement) ビット (Diffie-Hellman 暗号スイートの場合) または鍵暗号化 (key encipherment) ビット (RSA 暗号スイートの場合) がセットされていることである。TOE による使用のため取得される証明書がエンタープライズ内で使用されるためには、これらの要件に適合しなければならない (have to)。

FIA_X509_EXT.1.2 [選択：TOE、TOE プラットフォーム] は、basicConstraints 拡張が存在し CA フラグが TRUE にセットされている場合にのみ、証明書を CA 証明書として取り扱わなければならない (shall)。

適用上の注意：

本要件は、TOE または TOE プラットフォームにより用いられ処理される証明書に適用される。

保証アクティビティ：

TSS

評価者は、どこで証明書の有効性のチェックが行われるか TSS に記述されていることを保証しなければならない (shall)。また評価者は、認証パス検証アルゴリズムの記述も TSS に提供されていることも確認する。

ガイダンス

N/A

テスト

記述されるテストは、FIA_X509_EXT.2.1 の使用事例を含め、他の証明書サービス保証アクティビティと組み合わせて実行されなければならない (must)。extendedKeyUsage ルールのテストは、これらのルールを要求する用途と組み合わせて実行される。

- テスト 1 : 評価者は、有効な認証パスのない証明書の有効性確認が、その機能 (アプリケーションの検証、高信頼チャネルの設定、あるいは高信頼ソフトウェア更新) において失敗することを実例により示さなければなければならない (shall)。次に、評価者は、その機能で使われた証明書の検証に必要となった証明書または複数の証明書をロードし、その機能が成功することを実例により示さなければなければならない (shall)。次に、評価者は、これらの証明書の一つを削除して、その機能が失敗することを示さなければならない (shall)。
- テスト 2 : 評価者は、有効期限を過ぎた証明書の有効性確認が、その機能において失敗することを実例により示さなければならない (shall)。
- テスト 3 : 評価者は、CRL または OCSP のどちらが選択されているかに応じて、TOE が失効した証明書を適切に処理できることをテストしなければならない (shall)。両方とも選択されている場合には、それぞれの方法についてテストが実行される。評価者は、信頼の連鎖の一つ上位のみをテストする必要がある (将来の版では、上位の連鎖全体について検証が実行されることを保証することが要求されるかもしれない)。評価者は、有効な証明書が用いられること、そして証明書の有効性確認機能が成功することを保証しなければならない (shall)。次に評価者は、失効するはずの証明書 (選択において選択された各方法について) を用いてテストを試行し、もはや証明書が有効ではない場合には証明書の有効性確認機能が失敗することを保証すること。
- テスト 4 : 評価者は、TOE の証明書を発行する CA の証明書に basicConstraints 拡張が含まれないような認証パスを構築しなければならない (shall)。この認証パスの検証は失敗すること。
- テスト 5 : 評価者は、TOE の証明書を発行する CA の証明書の basicConstraints 拡張の cA フラグがセットされていないような認証パスを構築しなければならない (shall)。この認証パスの検証は失敗すること。
- テスト 6 : 評価者は、TOE の証明書を発行する CA の証明書の basicConstraints 拡張中の cA フラグが TRUE にセットされているような認証パスを構築しなければならない (shall)。この認証パスの検証は成功すること。
- テスト 7 : 評価者は、証明書の中間の 1 バイトだけを改変し、その証明書の有効性確認が失敗することを実例で示さなければならない (shall)。

FIA_X509_EXT.2 拡張：X509 認証

FIA_X509_EXT.2.1 [選択：TOE、TOE プラットフォーム] は、RFC 5280 により定義される X.509v3 証明書を用いて HTTPS、TLS、及び [選択：DTLS、その他のプロトコルなし]、ならびに TOE 更新のコード署名、モバイルコードインストールのコード署名、及び [選択：拡張機能インストールのコード署名、プラグインインストールのコード署名、追加用途なし] をサポートしなければならない (shall)。

適用上の注意：

DTLS は、FCS_DTLS_EXT.1 が本文に取り込まれる場合に選択されなければならない (shall)。証明書は、TOE ソフトウェアの高信頼更新に用いられなければならず (must)、またプラグインや拡張機能のインストールにオプションとして用いられてもよい。

TOE 更新及びモバイルコードのコード署名は、FPT_TUD_EXT.1.1 及び FPT_MCD_EXT.1 に指定されるルールに忠実でなければならない (must)。選択された場合、拡張機能及びプラグインのコード署名は、FPT_TUD_EXT.2 及び FPT_TUD_EXT.3 に指定されるルールに忠実でなければならない (must)。

FIA_X509_EXT.2.2 [選択：TOE、TOE プラットフォーム] が証明書の有効性を決定する接続を確立できないとき、[選択：TOE、TOE プラットフォーム] は [選択：このような場合には証明書を受容するかどうかの選択を管理者に許可する、証明書を受容する、証明書を受容しない] ようにしなければならない (shall)。

適用上の注意：

CRL のダウンロードにせよ、OCSP の実行にせよ、証明書の失効状態の検証を行うために接続を確立しなければならない (must) 場合は多々生ずる。この選択は、そのような接続が確立できない場合 (例えば、ネットワークエラーのため) のふるまいを記述するために用いられる。TOE が、証明書は FIA_X509_EXT.1 中の他の全てのルールに従って有効であると決定した場合、2 番目の選択に示されるふるまいにより有効性が決定されなければならない (shall)。証明書が FIA_X509_EXT.1 中の他の有効性確認ルールのいずれかに失敗する場合、TOE はその証明書を受容してはならない (must not)。

FIA_X509_EXT.2.3 [選択：TOE、TOE プラットフォーム] は、高信頼通信チャネルの確立中にピア証明書が不正とみなされる場合には利用者へ通知しなければならない (shall)。

適用上の注意：

高信頼通信チャネルには、TSF または TOE プラットフォームにより実施される TLS、HTTPS、または DTLS のいずれかが含まれる。有効性は認証パス、有効期限、及び RFC 5280 にしたがう失効状態により決定される。

FIA_X509_EXT.2.4 [選択：TOE、TOE プラットフォーム] は、コード署名証明書が無効とみなされる場合にはそのコードをインストールしてはならない (shall not)。

適用上の注意：

証明書は、システムソフトウェアの高信頼更新 (FPT_TUD_EXT.1.3) にオプションとして用いてもよい。

保証アクティビティ：

TSS

評価者は、TOE がどの証明書を使用するか選ぶ方法が記述されていることを保証するため、TSS を検査しなければならない (shall)。

評価者は、高信頼チャネルの確立に用いられる証明書の有効性確認中に接続が確立できな

かった際の TOE または TOE プラットフォームのふるまいが記述されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、TOE が証明書を使用できるように運用環境を構成するため必要な任意の指示が操作ガイダンスに含まれていることを検証しなければならない (shall)。

管理者がデフォルトのアクションを指定できるという要件である場合、この構成アクションを行う方法に関する指示が操作ガイダンスに含まれていることを評価者は保証しなければならない (shall)。

テスト

評価者は、証明書の使用を要求する FIA_X509_EXT.2.1 に列挙される各機能について、テスト 1 を行わなければならない (shall)。

- テスト 1 : 評価者は、有効な認証パスのない証明書を使用すると、その機能が失敗するか、利用者通知が受領されることを例証しなければならない (shall) (エレメント 3 及び 4 により要求されるように)。次に評価者は、その機能で使われる証明書の検証に必要とされる任意の証明書をプラットフォームのルートストアへロードし、その機能が成功することを例証しなければならない (shall)。
- テスト 2 : 評価者は、TOE 以外の IT エンティティとの通信により、有効な証明書の使用には少なくとも一部の証明書有効性確認のチェック実行が必要とされることを例証しなければならない (shall)。次に評価者は、TOE が証明書の有効性を検証できないように環境を操作し、FIA_X509_EXT.2.2 で選択されたアクションが行われることを確認しなければならない (shall)。選択されたアクションが管理者により構成可能である場合には、評価者は操作ガイダンスに従って、サポートされているすべての管理者構成可能オプションが、文書化されているようにふるまうことを決定しなければならない (shall)。

4.3.3 クラス : セキュリティ管理 (FMT)

TSF 内の機能の管理

FMT_MOF.1 機能のふるまいの管理

FMT_MOF.1.1 [選択 : TOE、TOE 及び TOE プラットフォーム] は、以下の機能 :

1. 秘密ウェブフォーム情報のストレージの有効化／無効化 ;
2. モバイルコードの構成 :
    a. モバイルコードをインストールする能力 ;
    b. モバイルコードをアンインストールする能力 ;
    c. モバイルコードを更新する能力 ;
    d. 未署名のモバイルコードを実行する能力 ;
    e. 信頼されない、または未検証の発行者からのモバイルコードを実行する能力

[選択 :

3. サードパーティクッキーのストレージの有効化／無効化 ;

4. 拡張機能の構成：
    a. 拡張機能をインストールする能力；
    b. 拡張機能をアンインストールする能力；
    c. 拡張機能を更新する能力；
    d. 拡張機能を無効化する能力
5. プラグインの構成：
    a. プラグインをインストールする能力；
    b. プラグインをアンインストールする能力；
    c. プラグインを更新する能力；
    d. プラグインを無効化する能力
6. X.509 証明書の失効状態を取得するための OCSP の有効化／無効化；
7. HTTP ヘッダ中のユーザエージェント情報の取り込みの構成；
8. ウェブサイトが利用者に関する追跡情報を収集することを有効化／無効化する能力
9. 保存されたブラウジングデータ (キャッシュ、ウェブフォーム情報) の削除：
    a. どのコンテンツが削除されるべき (should) か指定する能力；
    b. すべての保存されたコンテンツを削除する能力；
    c. ブラウザセションの終了時に自動的にコンテンツを削除する；
10. 永続的ストレージ中に秘密情報を保存することを有効化／無効化；
11. ダウンロードされたファイルがディスクへ保存される場所を指定する能力；
12. クッキーキャッシュのサイズの構成；
13. グラフィック処理ユニット (GPU) との相互作用の有効化／無効化
14. 無効または有効性未確認の X.509 証明書を持つウェブサイトへ進む能力の構成；
15. プライベートブラウジングセションの利用の有効化／無効化；
16. ダウンロード前に悪意のあるアプリケーションを検出するためのアプリケーションレピュテーションサービスの使用の構成；
17. マルウェアまたはフィッシングコンテンツを含むサイトを検出するための URL レピュテーションサービスの使用の構成；
18. ソフトウェア更新及びパッチの自動インストールの有効化／無効化；
19. TSF が証明書の有効性を決定するための接続を確立できなかった場合の高信頼チャネル確立の有効化／無効化；
20. ウェブサイトがプロトコルハンドラを登録する能力の有効化／無効化。

]

を*行う*能力を、管理ポリシーに従って管理者に制限しなければならない (shall)。

適用上の注意：

本要件の意図は、利用者により上書きされ得ないポリシーにより TOE を構成することを TOE プラットフォームの管理者に可能とすることである。管理者が識別の機能向けのポリシーを設定しなかった場合、利用者は依然としてその機能を実行し得る。ポリシーの実施は TOE そのものにより、あるいは TOE と TOE プラットフォームが互いに協調して行われる

保証アクティビティ：

TSS

評価者は、ポリシーに従って構成された際、これらの管理機能が TOE プラットフォーム管理者によりのみ構成可能であること、及び利用者により上書きできないことが、TSS に記述されていることを検証しなければならない (shall)。

ガイダンス

評価者は、TOE プラットフォーム管理者が FMT_MOF.1.1 に列挙される機能を構成するための指示が含まれることを検証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1：評価者は、FMT_MOF.1.1 に定義される、TOE プラットフォーム管理者により制御され利用者により上書きできないすべての管理機能を一括して含むポリシーを作成しなければならない (shall)。評価者は TOE へこれらのポリシーを適用して、利用者として各設定の上書きを試行し、そして TSF がこれを許可しないことを検証しなければならない (shall)。

管理機能の仕様

FMT_SMF.1 管理機能の仕様

FMT_SMF.1.1 [選択：TOE、TOE 及び TOE プラットフォーム] は、以下の管理機能を行えなければならない (shall)：

1. 秘密ウェブフォーム情報のストレージの有効化／無効化；
2. サードパーティクッキーのストレージの有効化／無効化；
3. HTTP ヘッダ中のユーザエージェント情報の取り込みの構成；
4. ウェブサイトが利用者に関する追跡情報を収集することを有効化／無効化する能力
5. ブラウジングデータ (キャッシュ、ウェブフォーム情報) の削除：
    a. どのコンテンツが削除されるべき (should) か指定する能力；
    b. すべての保存されたコンテンツを削除する能力；
    c. ブラウザセションの終了時に自動的にコンテンツを削除する；
6. モバイルコードの構成：
    a. モバイルコードをインストールする能力；
    b. モバイルコードをアンインストールする能力；

c. モバイルコードを更新する能力；

d. 未署名のモバイルコードを実行する能力；

e. 信頼されない、または未検証の発行者からのモバイルコードを実行する能力

7. ダウンロードされたファイルがディスクへ保存される場所を指定する能力；
8. クッキーキャッシュのサイズの構成；
9. 無効または有効性未確認の X.509 証明書を持つウェブサイトへ進む能力の有効化／無効化；
10. ソフトウェア更新及びパッチの自動インストールの有効化／無効化；

[選択：

11. 拡張機能の構成：
    a. 拡張機能をインストールする能力；
    b. 拡張機能をアンインストールする能力；
    c. 拡張機能を更新する能力；
    d. 拡張機能を無効化する能力
12. プラグインの構成：
    e. プラグインをインストールする能力；
    f. プラグインをアンインストールする能力；
    g. プラグインを更新する能力；
    h. プラグインを無効化する能力
13. 永続的ストレージ中に秘密情報を保存することを有効化／無効化；
14. X.509 証明書の失効状態を取得するための OCSP の有効化／無効化；
15. グラフィック処理ユニット (GPU) との相互作用の有効化／無効化
16. プライベートブラウジングセションの利用の有効化／無効化；
17. ダウンロード前に悪意のあるアプリケーションを検出するためのアプリケーションレピュテーションサービスの使用の構成；
18. マルウェアまたはフィッシングコンテンツを含むサイトを検出するための URL レピュテーションサービスの使用の構成；
19. TSF が証明書の有効性を決定するための接続を確立できなかった場合の高信頼チャネル確立の有効化／無効化；
20. ウェブサイトがプロトコルハンドラを登録する能力の有効化／無効化

]。

適用上の注意

管理者がセキュリティ管理機能を構成し、構成情報を TOE へ「プッシュ」するような例もあるかもしれない。これは受容可能な管理形態である。ST 作成者は ST 中に、どの管理機能が TOE で構成されるのか、そしてどれが管理者により構成されるのか、単純に明示しな

ければならない (must)。機能が重複する (すなわち、プラットフォーム上のエンドユーザによりも、管理者によりも行われることが可能な) 場合もあり得るが、ST が明確であってこの機能を行う方法がガイダンス文書に記述されている限り、これは問題ない。

機能 1 は、FCS_CKM_EXT.1 に指定される。

機能 2 は、FDP_COO_EXT.1 に指定される。

機能 3 は、ユーザエージェント文字列中の情報の構成とともに、ユーザエージェント文字列中の任意の情報の送信の有効化／無効化にも対応する。

機能 4 は、FDP_TRK_EXT.1 に指定される。

機能 5 は、FDP_DEL_EXT.1 に指定される。

機能 6 は、FIA_X509_EXT.2.1 及び FPT_MCD_EXT.1 に指定される。

機能 7 は、FPT_DNL_EXT.2.1 に指定される。

機能 8 は、各利用者により保存されるクッキーの数を制御するため、クッキーキャッシュのサイズを構成する能力に対応する。

機能 9 は、FIA_X509_EXT.1 及び FIA_X509_EXT.2 に指定される。

機能 10 は、FPT_TUD_EXT.1 に指定される。

機能 11 は、FDP_DEL_EXT.1 及び FPT_TUD_EXT.1 で拡張機能が選択される場合に選択されるべきである (should)。アンインストールは FDP_DEL_EXT.2 に指定される。インストールと更新は FPT_TUD_EXT.2 に指定される。

機能 12 は、FDP_DEL_EXT.1 及び FPT_TUD_EXT.1 でプラグインが選択される場合に選択されるべきである (should)。アンインストールは FDP_DEL_EXT.3 に指定される。インストールと更新は FPT_TUD_EXT.3 に指定される。

機能 13 は FDP_PST_EXT.1 に指定され、TOE がこれをサポートする場合に選択されるべきである (should)。

機能 14 は FIA_X509_EXT.1.1 に指定され、TOE がこれをサポートする場合に選択されるべきである (should)。

機能 15 において、GPU はコンピュータグラフィックスの操作と表示を非常に効率的に行う専用電子回路である。この能力を有するブラウザは、この機能を取り込むべきである (should)。ブラウザの UI においては、これはグラフィックスの高速化オプションとして表現されるかもしれない。これは、TOE がこれをサポートする場合に選択されるべきである (should)。

機能 16 は FDP_PBR_EXT.1 に指定され、TOE がこれをサポートする場合に選択されるべきである (should)。

機能 17 は FPT_INT_EXT.2 に指定され、TOE がこれをサポートする場合に選択されるべきである (should)。

機能 18 は FPT_INT_EXT.3 に指定され、TOE がこれをサポートする場合に選択されるべきである (should)。

機能 19 は FIA_X509_EXT.2.2 に指定され、TOE がこれをサポートする場合に選択されるべきである (should)。

機能 20 において、プロトコルハンドラは特定のウェブプロトコル (例えば、メール、カレ

ンダー) と関連付けることのできるウェブアプリケーションである。ウェブアプリケーションは、特定プロトコルの潜在的なハンドラとしてブラウザに自分自身の登録を試行できる。この機能は、TOE がこれをサポートする場合に選択されるべきである (should)。

保証アクティビティ

TSS

適用上の注意に言明されているように、TOE はローカルに構成されてもよいし、あるいはリモートに構成されてもよい。評価者は、どの機能がローカル及びリモートに行えるか明確に言明されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、PP により義務付けられるすべての管理機能が操作ガイダンスに記述され、その記述にはその管理機能と関連付けられた管理職務を行うために必要な情報が含まれていることを検証しなければならない (shall)。

操作ガイダンス文書には、各機能の TSS 記述に従って構成をローカルまたはリモートあるいはその両方で行う方法が記述されること。

テスト

評価者は、TOE を構成して上記要件に列挙されるオプションのをテストすることにより、管理機能を提供する TOE の能力、または TOE プラットフォームと組み合わされた TOE の能力をテストしなければならない (shall)。評価者は AGD ガイダンスを参照して以下のテストのを行い、利用者及び管理者の両方がその機能を行い得る場合には各テストを繰返さなければならない (shall)。

機能 1：この機能のテストは、FCS_CKM_EXT.1 と組み合わせて行われる。

機能 2：この機能のテストは、FDP_COO_EXT.1 と組み合わせて行われる。

機能 3：

- テスト 1：評価者は、操作ガイダンス中の指示に従ってユーザエージェント文字列を無効化するオプションを構成しなければならない (shall)。評価者はサーバとの接続を開始し、ネットワークプロトコルアナライザを用いて TOE とサーバとの間のトラフィックをモニターしなければならない (shall)。評価者はキャプチャされたネットワークトラフィックを検査して、ユーザエージェント文字列が HTTP ヘッダ内に存在しないことを検証しなければならない (shall)。
- テスト 2：評価者は、操作ガイダンス中の指示に従ってユーザエージェント文字列の内容を構成しなければならない (shall)。評価者はサーバとの接続を開始し、ネットワークプロトコルアナライザを用いて TOE とサーバとの間のトラフィックをモニターしなければならない (shall)。評価者はキャプチャされたネットワークトラフィックを検査して、ユーザエージェント文字列が構成された値と一致することを検証しなければならない (shall)。

機能 4：評価者は、追跡情報の収集を有効化しなければならず (shall)、そして FDP_TRK_EXT.1 と関連付けられたテストを行わなければならない (shall)。評価者は、追跡情報の収集を無効化してテストを繰り返さなければならず (shall)、そして追跡情報が収集されないことを検証しなければならない (shall)。

機能 5：この機能のテストは、FDP_DEL_EXT.1 と組み合わせて行われる。

機能 6：この機能のテストは、FIA_X509_EXT.2.1 及び FPT_MCD_EXT.1 と組み合わせて

行われる。

機能 7：この機能のテストは、FPT_DNL_EXT.2.1 と組み合わせて行われる。

機能 8：

- テスト 1：評価者は、クッキーが有効化されたウェブサイトへナビゲートして、一度デフォルトクッキーキャッシュサイズ閾値を超えると他のクッキーがクッキーキャッシュへ書き込まれないことを検証しなければならない (shall)。
- テスト 2：評価者は、操作ガイダンスに従ってクッキーキャッシュのサイズを許容される最大サイズに構成しなければならない (shall)。評価者は、最大クッキーキャッシュサイズ閾値を超えるクッキーの保存を試行するウェブサイトへアクセスした際、クッキーがクッキーキャッシュへ書き込まれないことを検証しなければならない (shall)。

機能 9：この機能のテストは、FIA_X509_EXT.1 及び FIA_X509_EXT.2 と組み合わせて行われる。

機能 10：評価者は、更新及びパッチの自動インストールを有効化しなければならず (shall)、そして FPT_TUD_EXT.1.4 と関連付けられたテストを行わなければならない (shall)。次に評価者は自動インストールを無効化し、テストを再実行しなければならず (shall)、そして更新またはパッチがインストールされないことを検証しなければならない (shall)。

機能 11：(条件付き)

- テスト 1。拡張機能のインストール、更新及び削除について、テストは FPT_TUD_EXT.2 及び FDP_DEL_EXT.2 と組み合わせて行われなければならない (shall)。
- テスト 2：評価者は、TOE に多数の拡張機能をロードしなければならない (shall)。評価者は、多数の拡張機能の無効化を試行しなければならない (shall)。次に評価者は、無効化された拡張機能の機能の使用を試行しなければならず (shall)、この機能が作動しないことを検証しなければならない (shall)。また評価者は、TOE の拡張機能インタフェースを検査しなければならず (shall)、そして無効化された拡張機能が無効化されたものとして見えることを検証しなければならない (shall)。

機能 12：(条件付き)

- テスト 1。プラグインのインストール、更新及び削除について、テストは FPT_TUD_EXT.3 及び FDP_DEL_EXT.3 と組み合わせて行われなければならない (shall)。
- テスト 2：評価者は、TOE に多数のプラグインをロードしなければならない (shall)。評価者は、多数のプラグインの無効化を試行しなければならない (shall)。次に評価者は、無効化されたプラグインの機能の使用を試行しなければならず (shall)、この機能が作動しないことを検証しなければならない (shall)。また評価者は、TOE のプラグインインタフェースを検査しなければならず (shall)、そして無効化されたプラグインが無効化されたものとして見えることを検証しなければならない (shall)。

機能 13：(条件付き) この機能のテストは、FDP_PST_EXT.1 と組み合わせて行われる。

機能 14：(条件付き) この機能のテストは、FIA_X509_EXT.1 と組み合わせて行われる。

機能 15：(条件付き)　評価者は TOE の UI へアクセスしなければならず (shall)、そして GPU との相互作用を有効化／無効化する能力が UI で利用可能であることを検証しなければならない (shall)。

機能 16：(条件付き) この機能のテストは、FDP_PBR_EXT.1 と組み合わせて行われる。

機能 17：(条件付き) この機能のテストは、FPT_INT_EXT.2 と組み合わせて行われる。

機能 18：(条件付き) この機能のテストは、FPT_INT_EXT.3 と組み合わせて行われる。

機能 19：(条件付き) この機能のテストは、FIA_X509_EXT.2.2 と組み合わせて行われる。

機能 20：(条件付き)

- テスト 1：評価者は、プロトコルハンドラの登録を許可しなければならない (shall)。評価者は、自分自身をプロトコルハンドラとして登録可能なアプリケーションが動作しているテスト用または実際のウェブサイトへナビゲートしなければならず (shall)、そしてそのアプリケーションが自分自身を登録できることを検証しなければならない (shall)。
- テスト 2：評価者は、テスト 1 のプロトコルハンドラの登録を削除し、プロトコルハンドラの登録を禁止しなければならない (shall)。評価者は同一のサイトへナビゲートしなければならず (shall)、そしてウェブサイトが自分自身を登録することが許可されないことを検証しなければならない (shall)。

FMT_SMR.1 セキュリティ管理役割

FMT_SMR.1.1 [選択：TOE、TOE プラットフォーム] は、以下の役割を維持管理しなければならない (shall)：*管理者*。

FMT_SMR.1.2 [選択：TOE、TOE プラットフォーム] は、利用者を役割と関連付けることができなければならない (shall)。

保証アクティビティ：

TSS

評価者は、管理者の役割と、役割に付与される権限及び役割の制限が記述されていることを検証するため、TSS と利用者文書を検査しなければならない (shall)。

ガイダンス

評価者は、TOE を管理するための指示とどのインタフェースがサポートされるかが含まれることを保証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価のためテストアクティビティを行うにあたって、評価者はすべてのサポートされるインタフェースを利用しなければならない (shall) が、各インタフェースについて管理アクションを伴う各テストを繰り返す必要はない。しかし評価者は、本 PP の要件に適合する TOE 管理のサポートされた手法のがテストされることを確実にしなければならない (shall)。例えば、TOE がローカルなハードウェアインタフェースまたは TLS/HTTPS を介して管理可能な場合には、評価チームのテストアクティビティ中で両方の管理手法が行使されなければならない (must)。

4.3.4 クラス：TSF の保護 (FPT)

TSF のセルフテスト

FPT_TST_EXT.1 拡張：TSF のセルフテスト

FPT_TST_EXT.1.1 [選択 : TOE、TOE プラットフォーム] は、最初の起動中 (電源投入時) に一連のセルフテストを実行し、その実行可能形式及びデータの完全性を保証しなければならない (shall)。

保証アクティビティ：

TSS

評価者は、起動時に行われるセルフテストが指定されていることを保証するため、TSS を検査しなければならない (shall)。この記述には、実際に行われるテストの概要 (例えば、TOE 実行可能形式の完全性を検証する) が含まれるべきである (should)。TSS には、セルフテスト失敗の際に TSF または TOE プラットフォームが入り得る任意のエラー状態、及びそのエラー状態を抜けて通常動作を再開するために必要な条件とアクションが含まれなければならない (must)。評価者は、これらのセルフテストが起動時に自動的に実行されること、そして利用者またはオペレータからの入力やアクションは一切必要とされないことが TSS に示されていることを検証しなければならない (shall)。

ガイダンス

N/A

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、既知の良好な TSF 実行可能形式に関する完全性チェックを行い、そのチェックが成功することを検証しなければならない (shall)。
- テスト 2 : 評価者は、TSF 実行可能形式を改変し、その改変された TSF 実行可能形式に関する完全性チェックを行い、そのチェックが失敗することを検証しなければならない (shall)。
- テスト 3 : 評価者は、既知の良好な TOE データに関する完全性チェックを行い、そのチェックが成功することを検証しなければならない (shall)。
- テスト 4 : 評価者は、TOE 構成データを改変し、その改変された TOE データに関する完全性チェックを行い、そのチェックが失敗することを検証しなければならない (shall)。

高信頼更新

FPT_TUD_EXT.1 拡張 : 高信頼ソフトウェア更新及びパッチ

FPT_TUD_EXT.1.1 [選択 : TOE、TOE プラットフォーム] は、TOE ソフトウェア、 [選択 : 拡張機能、プラグイン、その他のアドオンなし] の現在のバージョンを問い合わせる能力を提供しなければならない (shall)。

FPT_TUD_EXT.1.2 [選択 : TOE、TOE プラットフォーム] は、TOE ソフトウェア、 [選択 : 拡張機能、プラグイン、その他のアドオンなし] の更新及びパッチを開始する能力を提供しなければならない (shall)。

FPT_TUD_EXT.1.3 [選択 : TOE、TOE プラットフォーム] は、TOE へのソフトウェア更新及びパッチ、 [選択 : 拡張機能の更新、プラグインの更新、その他の更新なし] の検証を、デジタル署名メカニズム及び [選択 : 公開ハッシュ、その他の機能なし] を用いて、それらの更新及びパッチをインストールする前に検証する手段を提供しなければならない (shall)。

FTP_TUD_EXT.1.4 [選択：TOE、TOE プラットフォーム] は、TOE へのソフトウェア更新及びパッチ、 [選択：拡張機能、プラグイン、その他のアドオンなし] を、検証後に自動的にインストールする能力を提供しなければならない (shall)。

適用上の注意：

3 番目のエレメントにおいて参照されているデジタル署名メカニズムは、FCS_COP.1(3) に指定されたものである。参照されている公開ハッシュは、FCS_COP.1(2) に指定された関数のいずれかにより生成される。

上記の拡張機能またはプラグインが選択される場合、附属書 C から該当する選択に基づく要件もまた ST の本文に含まれなければならない (must)。

保証アクティビティ：

TSS

TOE への更新は正当な情報源により署名され、またそれと関連付けられたハッシュを持つことがある。正当な情報源の定義は、更新検証メカニズムにより用いられる証明書がシステムへ取り込まれる方法の記述とともに、TSS 中に含まれなければならない (must)。評価者は、この情報が TSS に含まれることを保証しなければならない (shall)。

また評価者は、更新候補が取得される方法、更新のデジタル署名の検証または更新のハッシュの計算に関連した処理、そして成功の (ハッシュまたは署名が検証された) 場合と不成功の (ハッシュまたは署名が検証できなかった) 場合に行われるアクションが、TSS (または操作ガイダンス) に記述されていることを保証しなければならない (shall)。これらのアクティビティが完全に基盤となるプラットフォームにより行われる場合、要求される機能が各プラットフォームについて含まれることを示す各プラットフォームの ST への参照が、評価者により検証されなければならない (shall)。

ガイダンス

評価者は、TOE ソフトウェアの現在のバージョンを検証し、TOE ソフトウェアへの更新及びパッチを開始し、そしてソフトウェア更新及びパッチの検証を構成するためのステップが文書化されていることを検証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、バージョン検証アクティビティを行って製品の現在のバージョンを決定しなければならない (shall)。評価者は、操作ガイダンスに記述されている手順を用いて本物の更新を取得し、その TOE へのインストールが成功することを検証しなければならない (shall)。その後、評価者はその他の保証アクティビティテストのサブセットを行い、更新が期待されたとおり機能していることを例証しなければならない (shall)。更新の後、評価者はバージョン検証アクティビティを再び行って、そのバージョンが更新のものと正しく対応していることを検証しなければならない (shall)。
- テスト 2 : 評価者は、バージョン検証アクティビティを行って製品の現在のバージョンを決定しなければならない (shall)。評価者は、偽物の更新を取得または作成し、その TOE へのインストールを試行しなければならない (shall)。評価者は、その更新を TOE が拒否することを検証しなければならない (shall)。
- テスト 3 : 評価者は、署名されていないパッチまたは更新のインストールを試行しなければならず (shall)、またその更新が失敗することを検証しなければならない (shall)。

- テスト 4：評価者は、無効な証明書でパッチまたは更新に署名しなければならない (shall)。評価者は、そのパッチまたは更新のインストールを試行しなければならず (shall)、またその更新が失敗することを検証しなければならない (shall)。
- テスト 5：評価者は、コード署名 extendedKeyUsage 拡張のない、あるいは無効な証明書でパッチまたは更新に署名しなければならない (shall)。評価者は、そのパッチまたは更新のインストールを試行しなければならず (shall)、またその更新が失敗することを検証しなければならない (shall)。
- テスト 6：評価者は、署名されたパッチまたは更新のインストールを試行しなければならず (shall)、またそのインストールが成功し署名が検証された後自動的に行われることを検証しなければならない (shall)。

4.3.5 クラス：高信頼パス／チャネル (FTP)

高信頼チャネル

FTP_ITC.1 TSF 間高信頼チャネル

FTP_ITC.1 **詳細化：** [選択：TOE、TOE プラットフォーム] は、それ自身と他の高信頼 IT 製品との間に、他の通信パスとは論理的に分離され、その端点の保証された識別、及び**暴露からの**チャネルデータの保護や**チャネルデータの改変の検知**を提供する**高信頼**通信チャネルを提供するため、**[選択：HTTPS、TLS、DTLS]** を利用しなければならない（shall）。

FPT_ITC.1.2 [選択：TOE, TOE プラットフォーム] は、*TSF* が高信頼チャネルを介して通信を開始するのを許可しなければならない (shall)。

FPT_ITC.1.3 [選択：TOE, TOE プラットフォーム] は、*その接続を通過するすべてのトラフィック*にのために、高信頼チャネルを介して通信を開始しなければならない (shall)。

適用上の注意：

上記の要件の意図は、要件に識別された暗号プロトコルを用いて TOE と高信頼サーバとの間の高信頼チャネルを確立し維持することである。

保証アクティビティ：

TSS

評価者は、要件中に指定される暗号プロトコルの観点からウェブサーバへの TOE の接続の詳細が、仕様中に反映されていない可能性のある TOE 特有のオプションまたは手続きと共に、記述されていることを決定するため、TSS を検査しなければならない (shall)。また評価者は、TSS に列挙されたすべてのプロトコルが指定され、ST 中の要件に含まれていることを確認しなければならない (shall)。

ガイダンス

評価者は、アクセスポイント (訳注：ウェブサーバの間違い) への接続を確立するための指示が操作ガイダンスに含まれていることと、万一接続が意図せず切断されてしまった際の回復の指示が含まれていることを確認しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、操作ガイダンスに記述されたように接続の設定を行い、通信が成功することを保証して、TOE または TOE プラットフォームが要件に指定されたプロトコルを用いてウェブサーバとの通信を開始できることを保証しなければならない (shall)。
- テスト 2 : 評価者は、ウェブサーバとの各通信チャネルについて、チャネルデータが平文で送信されないことを保証しなければならない (shall)。

5 セキュリティ保証要件

セクション 3 の TOE に関するセキュリティ対策方針は、セクション 2 で識別された脅威に対抗するために構成された。セクション 4 のセキュリティ機能要件 (SFR) は、セキュリティ対策方針の形式的な具体化である。PP は、CC からセキュリティ保証要件 (SAR) を選び出し、評価者が評価に用いられる文書を評定し、独立テストを実行するための範囲を設定する。

このセクションには、CC からの SAR の完全なセットが含まれている一方で、評価者により行われるべき保証アクティビティは、このセクションと共にセクション 4 の両方に詳述されている。

本 PP に適合するために書かれた ST に対する TOE の評価についての一般的なモデルは以下のようなものである：

ST が評価について承認されると、コモンクライテリアテスト機関 (CCTL、訳注：評価機関) は、TOE 及びその支援 IT 環境へのアクセスを得るとともに、TOE の管理ガイダンスへもアクセスを得る。ST に列挙された保証アクティビティ (これは CCTL により TOE 特有となるように、ST の中または別文書に詳細化される) が、CCTL により実行される。これらのアクティビティの結果は、認証のために (利用した管理ガイダンスにそって) 文書化され提示される。

のファミリについて、開発者が提供する必要のある追加の文書／アクティビティが、もしあれば、それを明確にするため、「開発者への注意」が、開発者アクションエレメントについて提供される。内容／提示及び評価者アクティビティエレメントについては、エレメントごとにではなく、ファミリ全体について追加のアクティビティが記述されている。さらに、このセクションに記述された保証アクティビティは、セクション 4 に指定されたものとは相補的な関係にある。

TOE のセキュリティ保証要件には、本 PP のセクション 4 に識別された脅威に対抗するために必要とされる管理及び評価アクティビティが識別されている。

ADV クラス：開発

TOE に関する情報は、ST の TOE 要約仕様 (TSS) 部分とともに、エンドユーザに利用可能なガイダンス文書にも含まれている。TOE 開発者は TSS に含まれる製品の記述を、機能仕様との関連において一致させなければならない (must)。セクション 4 に含まれる保証アクティビティは、TSS セクションとして適切な内容であることを決定するために十分な情報を ST 作成者へ提供すべきである (should)。

ADV_FSP.1 基本機能仕様

開発者アクションエレメント：

ADV_FSP.1.1D　開発者は、機能仕様を提供しなければならない (shall)。

ADV_FSP.1.2D　開発者は、機能仕様から SFR への追跡を提供しなければならない (shall)。

開発者への注意：このセクションの概論で述べたように、機能仕様は AGD_OPR 及び AGD_PRE 文書に含まれる情報と、ST の TSS に提供される情報との組み合わせで構成される。機能仕様中の保証アクティビティは、文書及び TSS セクションに存在すべき (should) 証拠資料を参照している。これらは SFR と直接関連付けられているため、エレメント ADV_FSP.1.2D 中の追跡は暗黙にはすでにな

されており、追加的な文書は必要とされない。

内容・提示エレメント：

ADV_FSP.1.1C *機能仕様は、SFR 実施及び SFR 支援の各 TSFI の目的と使用手法を記述しなければならない (shall)。*

ADV_FSP.1.2C *機能仕様は、SFR 実施及び SFR 支援の各 TSFI に関連するすべてのパラメタを識別しなければならない (shall)。*

ADV_FSP.1.3C *機能仕様は、暗黙的に SFR 非干渉として分類されているインタフェースについて、その分類の根拠を示さなければならない (shall)。*

ADV_FSP.1.4C *追跡は、機能仕様での TSFI に対する SFR の追跡を実証するものでなければならない (shall)。*

評価者アクションエレメント：

ADV_ FSP.1.1E *評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない (shall)。*

ADV_ FSP.1.2E *評価者は、機能仕様が、SFR の正確かつ完全な具体化であることを決定しなければならない (shall)。*

保証アクティビティ：

これらの SAR に関連付けられた具体的な保証アクティビティは存在しない。機能仕様文書はセクション 4.2 に記述された評価アクティビティと、AGD、ATE、及び AVA SAR に関して記述されたその他のアクティビティをサポートするために提供される。機能仕様情報の内容についての要件は、行われるその他の保証アクティビティの特質により暗黙に評定される。不十分なインタフェース情報しか存在しなかったために評価者がアクティビティを行うことができなかった場合には、十分な機能仕様が提供されていなかったことになる。

AGD クラス：ガイダンス文書

ガイダンス文書は、開発者のセキュリティターゲットと共に提供される。ガイダンスには、運用環境がセキュリティ機能にそれ自身の役割を果たすことができることを正当な利用者が検証する方法の記述が含まれなければならない (must)。本文書は、正当な利用者により読解可能な非形式的なスタイルであるべきである (should)。

製品がサポートすると ST で主張されているすべての運用環境について、ガイダンスが提供されなければならない (must)。このガイダンスには、以下が含まれる。

- その環境への TOE のインストールを成功させるための指示、及び
- 製品として、またより大規模な運用環境のコンポーネントとして、TOE のセキュリティを管理するための指示。

また、特定のセキュリティ機能に関するガイダンスも提供される。そのようなガイダンスに関する具体的な要件は、セクション 4.2 に指定された保証アクティビティに含まれている。

AGD_OPE.1 利用者操作ガイダンス

開発者アクションエレメント：

AGD_OPE.1.1D 開発者は、利用者操作ガイダンスを提供しなければならない (shall)。

開発者への注意： ここで繰返し情報を提示するのではなく、開発者はこのコンポーネントに関する保証アクティビティをレビューして、評価者がチェックすることになるガイダンスの詳細を確認すべきである (should)。これにより、受容可能なガイダンスの作成に必要な情報が提供されることになる。

内容・提示エレメント：

AGD_OPE.1.1C 利用者操作ガイダンスは、適切な警告を含め、セキュアな処理環境で管理するべき (should)、正当な利用者がアクセス可能な機能と権限がどのようなものであるか、記述しなければならない (shall)。

AGD_OPE.1.2C 利用者操作ガイダンスは、TOE により提供された利用可能なインタフェースをセキュアな方法でどのように使用するかを正当な利用者について記述しなければならない (shall)。

AGD_OPE.1.3C 利用者操作ガイダンスは、利用可能な機能とインタフェース、特に利用者の管理下にあるすべてのセキュリティパラメタを、必要に応じてセキュアな値を示し、正当な利用者について記述しなければならない (shall)。

AGD_OPE.1.4C 利用者操作ガイダンスは、TSF の制御下にあるエンティティのセキュリティ特性の変更を含む、利用者がアクセス可能で実行が必要な機能に関連するセキュリティ関連事象の各タイプについて、正当な利用者について明確に提示しなければならない(shall)。

AGD_OPE.1.5C 利用者操作ガイダンスは、TOE の操作のすべての可能なモード (障害や操作誤りの後の操作を含む)、それらの結果、及びセキュアな動作を維持するために必要なことを識別しなければならない (shall)。

AGD_OPE.1.6C 利用者操作ガイダンスは、ST に記述された運用環境のセキュリティ対策方針を満たすために従うべきセキュリティ手段を、正当な利用者について記述しなければならない (shall)。

AGD_OPE.1.7C 利用者操作ガイダンスは、明確で、合理的なものでなければならない (shall)。

AGD_OPE.1.8C 利用者操作ガイダンスは、セキュリティオートメーションをサポートするため、セキュリティ設定チェックリスト記述形式 (XCCDF) で表現されなければならない (shall)。[米国のみの追記] 利用者操作ガイダンスは、XCCDF チェック項目検査方法エレメントとしてレジームの適合チェックを行うために利用できる各設定ガイダンス項目を表現し、またその項目が満たす NIST 800-53 管理策への参照を提供しなければならない (shall)。

評価者アクションエレメント：

AGD_OPE.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない (shall)。

保証アクティビティ：

操作ガイダンスの内容の一部は、セクション 4.2 の保証アクティビティと CEM にしたがっ

たTOE の評価により検証されることになる。

文書には、ハッシュのチェックまたはデジタル署名の検証のいずれかにより、TOE への更新を検証するためのプロセスが記述されなければならない (must)。評価者は、このプロセスに以下の手順が含まれることを検証しなければならない (shall)。

1. *TOE ソフトウェアの現在のバージョンを問い合わせるための指示。*
2. *ハッシュについては、所与の更新についてのハッシュがどこで取得できるかという記述。デジタル署名については、署名された更新が証明書の所有者から受信されていることを保証するために、FCS_COP.1(2) メカニズムにより用いられる証明書を取得するための指示。これは、最初から製品と共に供給されてもよいし、何らかの別の手段により取得されてもよい。*
3. *更新そのものを取得するための指示。これには、更新を TOE からアクセス可能とするための指示 (例えば、特定のディレクトリへの格納) が含まれるべきである (should)。*
4. *更新プロセスを開始するための、そしてそのプロセスが成功したか失敗したかを判別するための指示。これには、ハッシュ／デジタル署名の生成が含まれる。*

AGD_PRE.1 準備手続き

開発者アクションエレメント：

AGD_PRE.1.1D 開発者は、準備手続きを含めて TOE を提供しなければならない (shall)。

開発者への注意：操作ガイダンスと同様に、開発者は準備手続きに関して必要とされる内容を決定するため、保証アクティビティを検査すべきである (should)。

内容・提示エレメント：

AGD_PRE.1.1C 準備手続きには、開発者の配付手続きに従って配付された TOE のセキュアな受入れに必要なすべてのステップを記述しなければならない (shall)。

AGD_PRE.1.2C 準備手続きには、TOE のセキュアな設置、及び ST に記述された運用環境のセキュリティ対策方針に従った運用環境のセキュアな準備に必要なすべてのステップを記述されなければならない (shall)。

評価者アクションエレメント：

AGD_PRE.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない (shall)。

AGD_PRE.1.2E 評価者は、TOE が運用に向けてセキュアに準備されることを確認するために、準備手続きを適用しなければならない (shall)。

保証アクティビティ：

上の概論で述べたように、特に TOE の機能要件をサポートする運用環境の構成にあたっては、文書に関して多大な期待が存在する。評価者は、TOE に提供されたガイダンスが、ST 中に TOE について主張されているすべてのプラットフォーム (すなわち、ハードウェアとオペレーティングシステムの組み合わせ) へ十分に対応していることをチェックして保証しなければならない (shall)。

ALC クラス：ライフサイクルサポート

本 PP に適合する TOE に提供される保証レベルでは、ライフサイクルサポートは TOE ベンダの開発及び構成管理プロセスの検査に限定される。これは、製品の全体的な信頼度の向上に開発者のプラクティスが果たす重要な役割の結果である。

ALC_CMC.1 TOE のラベル付け

開発者アクションエレメント：

ALC_CMC.1.1D　開発者は、TOE 及び TOE の参照情報を提供しなければならない (shall)。

内容・提示エレメント：

ALC_CMC.1.1C　*TOE は、その一意な参照でラベル付けされなければならない (shall)。*

評価者アクションエレメント：

ALC_CMC.1.1E　*評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない (shall)。*

保証アクティビティ：

評価者は、TOE がその一意な参照ラベル付けと共に提供されていることを検証しなければならない (shall)。評価者は、CM 文書が提供されており、またそれに各構成項目を一意に識別するために用いられる手法が記述されていることを検証しなければならない (shall)。評価者は、開発者が CM システムを使用しており、またこのシステムが各構成項目を一意に識別していることを検証しなければならない (shall)。

ALC_CMS.1 TOE の CM カバレージ

開発者アクションエレメント：

ALC_CMS.1.1D　開発者は、TOE の構成リストを提供しなければならない (shall)。

内容・提示エレメント：

ALC_CMS.1.1C　*構成リストには、TOE 事態、及び SAR が要求する評価証拠を含まれなければならない (shall)。*

ALC_CMS.1.2C　*構成リストは、構成要素を一意に識別しなければならない (shall)。*

評価者アクションエレメント：

ALC_CMS.1.1E　*評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない (shall)。*

保証アクティビティ：

評価者は、上記に明示された各項目を含む TOE の構成リストを開発者が提供していることを検証しなければならない (shall)。評価者は、構成リスト中の各項目が一意に識別され、またその開発者が示されていることを検証しなければならない (shall)。

ATE クラス：テスト

テストは、システムの機能的側面と、設計または実装の弱点を利用する側面について指定される。前者は ATE_IND ファミリにより行われるが、後者は AVA_VAN ファミリにより行

われる。本 PP に指定された保証レベルにおいては、テストは通知された機能及びインタフェースに基づき、設計情報の利用可能性に依存して行われる。評価プロセスの主要なアウトプットのひとつは、以下の要件に指定されるテスト報告である。

ATE_IND.1 独立テスト—適合

テストは、TSS と、提供された管理 (構成及び操作を含む) 文書に記述された機能を確認するために行われる。テストで重視されるのは、セクション 4.2 に指定された要件が満たされていることの確認であるが、いくつかの追加的テストがセクション 4.3 中の SAR について指定されている。保証アクティビティは、これらのコンポーネントと関連付けられた追加的テストアクティビティを識別する。評価者は、テストの計画及び結果、ならびに本 PP への適合を主張するプラットフォーム／TOE の組み合わせに焦点を絞ったカバレージの論拠を文書化した、テスト報告を作成する。

開発者のアクションエレメント：

ATE_IND.1.1D *開発者は、テストのための TOE を提供しなければならない (shall)。*

内容及び提示エレメント：

ATE_IND.1.1C *TOE は、テストに適当していなければならない (shall)。*

評価者のアクションエレメント：

ATE_IND.1.1E *評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない (shall)。*

ATE_IND.1.2E *評価者は、TSF が使用どおりに動作することを確認するために TSF のサブセットをテストしなければならない (shall)。*

保証アクティビティ：

評価者は、システムのテストの側面を文書化したテスト計画とテスト報告を作成しなければならない (shall)。テスト計画は、CEM と本 PP の保証アクティビティの本文に含まれるすべてのテストアクションを扱う。保証アクティビティ中に列挙された各テストについて 1 つのテストケースを用意する必要はないが、ST 中の該当する各テスト要件が扱われていることを評価者はテスト計画中に文書化しなければならない (must)。

テスト計画は、テストするプラットフォームを識別し、テスト計画に含まれないが ST に含まれるプラットフォームについては、そのプラットフォームをテストしないことの正当化をテスト計画が提供する。この正当化には、テストされるプラットフォームとテストされないプラットフォームとの違いを取り上げ、行われるべきテストにその違いが影響しないという論拠を示さなければならない (must)。単にその違いが影響しないと主張するだけでは十分ではなく、根拠が提供されなければならない (must)。ST 中に主張されるすべてのプラットフォームがテストされる場合には、根拠は必要とされない。

テスト計画にはテストされるべき各プラットフォームの構成が記述され、また AGD 文書に含まれるもの以外に必要な設定があれば、それも記述される。テストの一部としての、または標準的なテスト前の条件としての、各プラットフォームの設置及び設定について、評価者が AGD 文書にしたがうことが期待されていることには注意すべきである (should)。これには、特別なテストドライバまたはツールも含まれるかもしれない。各ドライバまたはツールについて、そのドライバまたはツールが TOE 及びそのプラットフォームによる機能の実行に悪影響を与えないという、(単なる主張ではなく) 論拠が提供される。またこれには、用いられるべき暗号エンジンの構成が含まれる。このエンジンにより実装される暗号

アルゴリズムは、本 PP により指定され、評価される暗号プロトコル (DTLS, TLS/HTTPS) により用いられるものである。

テスト計画には、高レベルのテスト目的とともに、これらの目的を達成するために行われるべきテスト手順も識別される。これらの手順には、期待される結果も含まれる。テスト報告 (テスト計画へ単に注釈を加えたものであってもよい) には、テスト手順が実施された際に行われたアクティビティが詳述され、またテストの実際の結果が含まれる。これは累積的な記述でなければならない (shall)。従って失敗に終わったテストの実行が存在し、修正がインストールされ、そして次にテストの再実行が成功した場合、報告には単なる「成功」の結果だけではなく、「失敗」及び「成功」の結果 (及びそれを支持する詳細) が示される。

AVA クラス：脆弱性評定

168. このプロテクションプロファイルの第一世代については、、これらの種別の製品にどのような脆弱性が発見されているのかを研究するため、オープンソースの調査を行うことが評価機関に期待される。多くの場合、これらの脆弱性には基本的な攻撃者を超える巧妙さが必要とされる。ペネトレーションツールが作成されて評価機関へあまねく配付されるまでは、評価者には TOE 中のこれらの脆弱性のテストを行うことは期待されない。評価機関には、ベンダにより提供された文書を考慮して、これらの脆弱性の存在する可能性についてコメントすることが期待される。この情報はペネトレーションテストツールの開発と、将来のプロテクションプロファイルの開発のために用いられることになる。

AVA_VAN.1 脆弱性調査

開発者アクションエレメント：

AVA_VAN.1.1D	開発者は、テストのための TOE を提供しなければならない (shall)。

内容・提示エレメント：

AVA_VAN.1.1C	*TOE は、テストに適していなければならない (shall)。*

評価者アクションエレメント：

AVA_VAN.1.1E	*評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない (shall)。*
AVA_VAN.1.2E	*評価者は、TOE の潜在的脆弱性を識別するために、公知の情報源の探索を実行しなければならない (shall)。*
AVA_VAN.1.3E	*評価者は、基本的な攻撃能力を持つ攻撃者からの攻撃に TOE が耐えられることを決定するために、識別された潜在的脆弱性に基づいて侵入テストを実施しなければならない (shall)。*

保証アクティビティ：

ATE_IND と同様に、評価者は報告を作成し、本要件に関連する自分たちの結論を文書化しなければならない (shall)。この報告は、物理的には ATE_IND に言及される全体的なテスト報告の一部であってもよいし、あるいは別個の文書であってもよい。評価者は、公開された情報の検索を行って、MDM 一般に発見されている脆弱性と、特定の TOE に関する脆弱性を決定する。評価者は、参考とした情報源と発見された脆弱性を報告中に文書化する。発見された各脆弱性について、評価者はそれが該当しないことを示す根拠を提供するか、あるいはそのほうが適切であれば脆弱性を確認するためのテストを (ATE_IND に提供されるガイドラインを用いて) 策定するかのどちらかを行う。適切かどうかは、その脆弱性を利

用するために必要とされる攻撃ベクトルの評定により決定される。例えば、ブート時にあるキーの組み合わせを押すことにより脆弱性が検出できる場合、本 PP の保証レベルにおいてはテストが適当であろう。例えば、脆弱性の悪用に専門的なスキルと電子顕微鏡が必要とされる場合には、テストは適当ではなく、適切な根拠が策定されることになるであろう。

根拠

脅威を対策方針へ、そして対策方針を要件へ追跡する根拠は、セクション 2.0 及び 3.0 の本文に含まれている。未解決となっている対応付けは前提条件と組織のセキュリティ方針についてのもののみであり、これらは以下の附属書 A に含まれている。

附属書A： 参考表

このプロテクションプロファイルにおいて、本文書の最初のほうのセクションでは全体的なわかりやすさの向上を重視して、ネットワークデバイスへの脅威、これらの脅威を低減するために用いられる手法、及び適合 TOE により達成される低減の程度について、説明文を提示した。この提示のスタイルは形式化された評価アクティビティにはそのまま適用できないため、本附属書では表形式のアーティファクトを用いて、本文書に関連付けられる評価アクティビティを説明する。

前提条件

以下のサブセクションに列挙する具体的な条件が、TOE の運用環境に存在することが前提となる。これらの前提条件には、TOE セキュリティ要件の開発における実質的な事実と、TOE の使用にあたって不可欠な環境条件の両方が含まれる。

ST 作成者は、自分たちの特有の技術においてもこれらの前提条件が引き続き満たされることを確実にすべきである (should)。表は適宜変更されるべきである (should)。

表 1：TOE の前提条件

前提条件の名称	前提条件の定義
A.PLATFORMS	本文書に記述されるウェブブラウザは、基盤となるプラットフォームにかかわらず、任意のオペレーティングシステム上で動作できるであろう。
A.TRUSTED_ADMIN	TOE 管理者は、すべての管理ガイダンスを遵守し信頼された方法で適用すると信頼されている。
A.TRUSTED_USER	ウェブブラウザの利用者は悪意を持たず、適切な予防措置を講じる。
A.PLATFORM_FUNCTIONS	クライアントをサポートするプラットフォームは、ファイルシステムやその他のオペレーティングシステム機能を提供しなければならない (shall)。

脅威

以下の脅威は、本文書に記述された要件を取り込む際に、PP 作成者により技術に特有の脅威と統合されるべきである (should)。要件の変更、削除、及び追加はこのリストに影響を与えるかもしれないので、PP 作成者は適宜これらの脅威を変更または削除すべきである (should)。

表 2：脅威

脅威の名称	脅威の定義
T.UNAUTHORIZED_ADD-ON	悪意のある、または悪用可能な拡張機能またはプラグインが、開発者により意図的に、あるいは意図せず用いられ、プラットフォームのシステムソフトウェアに対する攻撃能力を生じさせてしまうかもしれない。
T.UNAUTHORIZED_UPDATE	悪意のある、または悪用可能なソフトウェアが、開発者により意図的に、あるいは意図せず用いられ、プラットフォームのシステムソフトウェアに対する攻撃能力を生じさせてしまうかもしれない。
T.NETWORK_EAVESDROP	ワイヤレス通信チャネル上やネットワーク基盤上の他のどこかに位置する場合、攻撃者は、ブラウザと他のエンドポイントとの間で交換されるデータの監視やアクセスの獲得ができてしまうかもしれない
T.NETWORK_ATTACK	攻撃者は、ブラウザとの通信の開始や、ブラウザと他のエンドポイントとの間の通信の改変ができてしまうかもしれない。
T.DATA_ACCESS	利用者データ及びクレデンシャルの機密性の損失が、ブラウザの動作中に攻撃者がブラウザへのアクセスを取得した結果として生じるかもしれない。

TOE のセキュリティ対策方針

表 3：TOE のセキュリティ対策方針

TOE セキュリティ対策方針	TOE 対策方針の定義
O.COMMS	TOE は、TOE の外部へ送信されるデータの機密性を保つ手段として、1 つ (以上) の標準プロトコルを用いて通信を行う能力を提供すること。
O.CONFIG	TOE はセキュリティポリシーを構成し適用する能力を提供すること。これによりブラウザが、その保存または処理し得る利用者及びエンタープライズデータを保護できることが確実となる。
O.INTEGRITY	TOE はセルフテストを行う能力を提供し、重要な機能、ソフトウェア／ファームウェア及びデータの完全性が保たれていることを確実にすること。また TOE は、ダウンロードされた更新の完全性を検証し、実行可能形式のダウンロードと起動を制御する手段をも提供すること。
O.ISOLATION	TOE は、任意の不正なアクセスを防止するため、異なるドメインからのコンテンツを隔離する能力を提供すること。
O.STORAGE	TOE は、すべての利用者及びエンタープライズデータ及び認証鍵を暗号化する能力を提供し、その保存するデータの機密性を確実にすること。

セキュリティ脅威からセキュリティ対策方針への対応付け

以下の表には、セキュリティ脅威から TOE の対策方針への対応付けが含まれている。

表 4：セキュリティ脅威から対策方針への対応付け

脅威	対策方針
T.UNAUTHORIZED_ADD-ON	O.INTEGRITY
T.UNAUTHORIZED_UPDATE	O.INTEGRITY
T.NETWORK_EAVESDROP	O.COMMS
T.NETWORK_ATTACK	O.COMMS; O.ISOLATION
T.DATA_ACCESS	O.STORAGE; O.CONFIG

附属書B： オプションの要件

本 PP の概論で示したように、本 PP の本文にはベースライン要件 (TOE またはその基盤となるプラットフォームにより行われなければならない (must) もの) が含まれている。これに追加して、これ以外の 3 種別の要件が附属書 B、C、及び D に指定されている。

第 1 の種別 (本附属書に含まれる) は、ST に取り込むことができる要件であるが、TOE が本 PP への適合を主張するためには必要とされないものである。第 2 の種別 (附属書 C に含まれる) は、PP の本文中の選択に基づく要件である。特定の選択がなされた場合には、その附属書中の追加的要件が取り込まれることが必要となる。第 3 の種別 (附属書 D に含まれる) は、本 PP へ適合するためには要求されないが、本 PP の将来のバージョンのベースライン要件に取り込まれることになっているコンポーネントである。ST 作成者には、附属書 B、附属書 C、または附属書 D に含まれる要件と関連し得るが列挙されていない要件 (例えば、FMT タイプの要件) もまた、ST へ取り込まれることを確実にする責任があることに注意されたい。

どの時点においても、これらは ST へ取り込むことができ、その場合でも TOE は依然として本 PP に適合する。

B.1 クラス：利用者データ保護 (FDP)

プライベートブラウジングセション

FDP_PBR_EXT.1 拡張：プライベートブラウジングセション

FDP_PBR_EXT.1.1 TOE は、プライベートブラウジングセションをサポートする能力を提供しなければならない (shall)。

適用上の注意：

プライベートブラウジングは、ブラウジング履歴、画像、及びクッキーなどのデータを保存することなく利用者がウェブをブラウズすることを許可するモードである。この能力をサポートするブラウザは、本要件を取り込むべきである (should)。

保証アクティビティ：

TSS

評価者は、TOE がどのようにプライベートブラウジングをサポートするか記述されていることを保証するため、TSS を検査しなければならない (shall)。TSS には、プライベートブラウジングモードにあるときローカルに保存されないデータが指定され、また TOE がこのモードで動作しているときと動作していない時とでウェブサイトと行う相互作用の違いが記述されなければならない (shall)。

ガイダンス

評価者は、プライベートブラウジングを許可または不許可とするためのステップが含まれることを保証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者はブラウジング履歴とクッキーキャッシュをクリアしなければならず (shall)、そしてプライベートブラウジングを有効化しなければならない (shall)。評価者

はテスト用または実際のウェブサイトあるいはその両方へナビゲートしなければならず (shall)、そしてブラウジング履歴とクッキーキャッシュが変更されないことを検証しなければならない (shall)。

- テスト 2：評価者はプライベートブラウジングを無効化しなければならず (shall)、そして同一のウェブサイトを再訪問しなければならない (shall)。評価者は、ブラウジング履歴とクッキーキャッシュが更新され、評価者のブラウジングアクティビティを反映していることを検証しなければならない (shall)。

附属書C： 選択に基づいた要件

本 PP の概論で示したように、本 PP の本文にはベースライン要件 (TOE またはその基盤となるプラットフォームにより行われなければならない (must) もの) が含まれている。これ以外にも PP の本文中の選択に基づく追加的要件が存在し、特定の選択がなされた場合には、以下の追加的要件が取り込まれることが必要となる。

C.1 クラス：暗号サポート (FCS)

データグラムトランスポート層セキュリティ (Datagram Transport Layer Security)

FCS_DTLS_EXT.1 拡張：データグラムトランスポート層セキュリティ

FCS_DTLS_EXT.1.1(2) [選択 : TOE、TOE プラットフォーム] は、DTLS 1.2 (RFC 6347) に従って DTLS プロトコルを実装しなければならない (shall)。

FCS_DTLS_EXT.1.2(2) [選択 : TOE、TOE プラットフォーム] は、RFC 6347 にしたがった変動が許可される場合を除き、DTLS の実装には FCS_TLS_EXT.1 の中の要件を実装しなければならない (shall)。

適用上の注意：

DTLS と TLS との違いは RFC 6347 に概説されている。それ以外の点では、これらのプロトコルは同一である。特に、TOE に定義される適用可能なセキュリティ特性については、2 つのプロトコルに違いはない。従って、FCS_TLSC_EXT.1 に列挙されたすべての適用上の注意と保証アクティビティは、DTLS の実装に適用される。

保証アクティビティ：

TSS

N/A

ガイダンス

N/A

テスト

評価者は、DTLS サーバとの接続を試行し、パケットアナライザでトラフィックを確認し、そして接続が成功しトラフィックが DTLS と識別されることを検証しなければならない (shall)。他のすべてのテストは、FCS_TLSC_EXT.1 に列挙された保証アクティビティと組み合わせて行われる。

C.2 クラス：利用者データ保護 (FDP)

情報の削除

FDP_DEL_EXT.2 拡張：拡張機能情報の削除

FDP_DEL_EXT.2.1 TOE は、拡張機能、構成エレメント、及び保存された情報を含むすべての情報が削除されるように、拡張機能を削除する能力を提供しなければならない (shall)。

保証アクティビティ：

TSS

評価者は、どこに拡張機能が保存されるか、どこに拡張機能が情報を保存することを許可されているか、文書化されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、どのようにすれば利用者が拡張機能を削除できるかの指示が含まれることを検証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、拡張機能と拡張機能データが文書化されたとおり保存されていることを検証するため、TOE 拡張機能をインストールし、そして TOE のファイルシステムを検査しなければならない (shall)。次に評価者は拡張機能と拡張機能データが文書化された場所から削除されていることを検証するため、TOE 拡張機能をアンインストールし、そして TOE のファイルシステムを検査しなければならない (shall)。

FDP_DEL_EXT.3 拡張：プラグイン情報の削除

FDP_DEL_EXT.3.1 TOE は、プラグイン、構成エレメント、及び保存された情報を含むすべての情報が削除されるように、プラグインを削除する能力を提供しなければならない (shall)。

保証アクティビティ：

TSS

評価者は、どこにプラグインが保存されるか、どこにプラグインが情報を保存することを許可されているか、そしてすべてのプラグイン情報を削除するためのオプションが存在するかどうか、文書化されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、どのようにすれば利用者がプラグイン及び関連付けられた内容を削除できるかの指示が含まれることを検証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、プラグインとプラグインデータが文書化されたとおり保存されていることを検証するため、TOE プラグインをインストールし、そして TOE のファイルシステムを検査しなければならない (shall)。次に評価者はプラグインとプラグインデータが文書化された場所から削除されていることを検証するため、TOE プラグインをアンインストールし、そして TOE のファイルシステムを検査しなければならない (shall)。

C.3 クラス：TSF の保護 (FPT)

高信頼更新

FPT_TUD_EXT.2 拡張：高信頼拡張機能更新

FPT_TUD_EXT.2.1 TOE は、拡張機能の現在のバージョンを問い合わせる能力を提供しなければならない (shall)。

FPT_TUD_EXT.2.2 TOE は、拡張機能の更新を開始する能力を提供しなければならない (shall)。

FTP_TUD_EXT.2.3 TOE は、拡張機能または拡張機能の更新をインストールする前に、デジタル署名メカニズムを用いて拡張機能または拡張機能の更新を検証する手段を提供しなければならない (shall)。

FTP_TUD_EXT.2.4 TOE は、ウェブサイトが拡張機能を自動的にインストールすることを防止しなければならない (shall)。

適用上の注意：

拡張機能は、ブラウザがデフォルトでは提供しない特定の機能を追加するために、ブラウザへ追加されるコード群である。拡張機能は、ブラウザベンダーにより、または第三者により開発される可能性があり、またブラウザが見るウェブコンテンツを閲覧し相互作用するためにフルアクセスが許可される。拡張機能は非モバイルプラットフォームによく見られるが、豊富なコンテンツを供給するウェブサイトに HTML5 が用いられる傾向にあるモバイルプラットフォームではサポートされないかもしれない。

保証アクティビティ：

TSS

評価者は、拡張機能と拡張機能の更新が信頼できる情報源からのものであることを検証する TSF の能力が記述されていることを検証するため、TSS を検査しなければならない (shall)。評価者は、承認されていない情報源からの拡張機能を TSF が拒否することが述べられていることを検証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、信頼された拡張機能の情報源を用いて TOE を構成する方法についての指示が操作ガイダンスに含まれていることを検証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1：評価者は、信頼された拡張機能の情報源を用いて TOE を構成しなければならない (shall)。評価者は、信頼された情報源により署名された拡張機能を作成または取得し、インストールを試行しなければならない (shall)。評価者は、拡張機能の署名が有効であることを検証しなければならない (shall)。
- テスト 2：評価者は、信頼されない情報源により署名された拡張機能を作成または取得し、インストールを試行しなければならない (shall)。評価者は、署名された拡張機能が拒否されることを検証しなければならない (shall)。
- テスト 3：評価者は、無効な証明書を用いて署名された拡張機能を作成または取得し、インストールを試行しなければならない (shall)。評価者は、署名された拡張機能が拒否されることを検証しなければならない (shall)。

- テスト 4: 評価者は、信頼された情報源により署名された拡張機能を作成または取得し、再署名することなくその拡張機能を改変し、インストールを試行しなければならない (shall)。評価者は、その署名された拡張機能が拒否されることを検証しなければならない (shall)。

FPT_TUD_EXT.3 拡張：高信頼プラグイン更新

FPT_TUD_EXT.3.1 TOE は、プラグインの現在のバージョンを問い合わせる能力を提供しなければならない (shall)。

FPT_TUD_EXT.3.2 TOE は、プラグイン及びプラグイン更新のダウンロードを開始する能力を提供しなければならない (shall)。

FTP_TUD_EXT.3.3 TOE は、デジタル署名メカニズム及び [選択：公開ハッシュ、その他の機能なし] を用いて、プラグインのインストール前にプラグインを検証する手段を提供しなければならない (shall)。

FTP_TUD_EXT.3.4 TOE は、ウェブサイトがプラグインを自動的にインストールすることを防止しなければならない (shall)。

保証アクティビティ：

TSS

評価者は、承認されていない情報源からのプラグインを TSF が拒否することが述べられていることを検証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、信頼されたプラグインの情報源を用いて TOE を構成する方法についての指示が含まれることを検証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1：評価者は、信頼されたプラグインの情報源を用いて TOE を構成しなければならない (shall)。評価者は、信頼された情報源により署名されたプラグインを作成または取得し、インストールを試行しなければならない (shall)。評価者は、プラグインの署名が有効であることを検証しなければならない (shall)。
- テスト 2: 評価者は、信頼されない情報源により署名されたプラグインを作成または取得し、インストールを試行しなければならない (shall)。評価者は、その署名されたプラグインが拒否されることを検証しなければならない (shall)。
- テスト 3: 評価者は、無効な証明書を用いて署名されたプラグインを作成または取得し、インストールを試行しなければならない (shall)。評価者は、その署名されたプラグインが有効である (訳注:「拒否される」の間違い) ことを検証しなければならない (shall)。
- テスト 4：評価者は、信頼された情報源により署名されたプラグインを作成または取得し、再署名することなくそのプラグインを改変し、インストールを試行しなければならない (shall)。評価者は、その署名されたプラグインが拒否されることを検証しなければならない (shall)。

附属書D： オブジェクティブな要件

本 PP の概論で示したように、本 PP の本文に、はベースライン要件 (TOE またはその基盤となるプラットフォームにより行われなければならない (must) もの) が含まれている。これ以外にも望ましいセキュリティ機能を指定する追加的要件が存在し、これらの要件は本附属書に含まれる。これらの要件は、本 PP の将来のバージョンではオブジェクティブな要件からベースライン要件へ移行することが期待される。

D.1 クラス：セキュリティ監査 (FAU)

セキュリティ監査データの生成

FAU_GEN.1 監査データの生成

FAU_GEN.1.1 [選択 : TOE、TOE プラットフォーム] は、以下の監査対象事象の監査記録を生成できなければならない (shall) :

- 監査機能の開始と終了 ;
- 監査の指定なしのレベルのすべての監査対象事象 ;
- *表 5 に列挙される具体的に定義された監査対象事象*]。

FAU_GEN.1.2 [選択 : TOE、TOE プラットフォーム] は、各監査記録において少なくとも以下の情報を記録しなければならない (shall) :

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、及び事象の結果 (成功または失敗)。

適用上の注意：

ST 作成者は、他の監査対象事象を直接表中に取り込むことができる。監査対象事象は、提示されたリストには限定されない。

保証アクティビティ：

TSS

N/A

ガイダンス

評価者は、操作ガイダンスにすべての監査対象事象が列挙され、監査記録のフォーマットが提供されていることを保証するため、操作ガイダンスを検査しなければならない (shall)。各監査記録フォーマット種別は、各フィールドの簡潔な記述とともに扱われなければならない (must)。評価者は、PP により義務付けられるすべての監査事象種別が TSS に記述され、またフィールドの記述には FAU_GEN.1.2 に要求される情報が含まれることを保証しなければならない (shall)。

テスト

評価者は、FAU_GEN.1.1 に列挙された事象に対して TOE に監査記録を生成させることにより、TOE の正しく監査記録を生成する能力をテストしなければならない (shall)。これには、事象のすべてのインスタンスが含まれるべきである (should)。評価者は、ST 中に含ま

れる各暗号プロトコルについて、チャネルの確立と終了に関して監査記録が生成されることをテストしなければならない (shall)。管理アクションについて評価者は、本 PP の文脈においてセキュリティ関連であると上記のように評価者により決定された各アクションが監査対象であることをテストしなければならない (shall)。テスト結果を検証する際に、評価者はテスト中に生成された監査記録が操作ガイダンスに指定されたフォーマットと一致すること、そして各監査記録のフィールドが適切なエントリを有すること及び監査記録が解釈に適した方法で提供されることを保証しなければならない (shall)。また評価者は、事象の種別、事象を引き起こした責任のある利用者、及び適用される証明書の識別情報に基づき、監査データの検索を行う能力をも保証しなければならない (shall)。

ここでのテストは、セキュリティメカニズムの直接的なテストと組み合わせて達成できることに注意すること。例えば、提供された操作ガイダンスが正しいことを保証するために行われるテストは、AGD_OPE.1 が満たされることを検証するため、監査記録が期待どおり生成されたことの検証に必要な管理アクションの呼び出しに対応しているはずである (should)。

表 5. 監査対象事象

要件	監査対象事象	追加監査記録の内容
FAU_GEN.1	なし。	なし。
FAU_SEL.1	監査収集機能が動作している間に生じたすべての監査構成への変更。	なし。
FCS_CKM.1(*)	鍵生成アクティビティの失敗。	なし。
FCS_CKM_EXT.1	なし。	なし。
FCS_CKM_EXT.4	鍵ゼロ化プロセスの失敗。	クリアされるオブジェクトまたはエンティティの識別情報。
FCS_COP.1(1)	暗号化または復号の失敗。	操作の暗号モード、暗号化／復号されるオブジェクトの名称／識別子。
FCS_COP.1(2)	ハッシュ機能の失敗。	操作の暗号モード、ハッシュされるオブジェクトの名称／識別子。
FCS_COP.1(3)	暗号署名の失敗。	操作の暗号モード、署名／検証されるオブジェクトの名称／識別子。
FCS_COP.1(4)	非データ完全性暗号ハッシュの失敗。	操作の暗号モード、ハッシュされるオブジェクトの名称／識別子。
FCS_DTLS_EXT.1	DTLS セションの確立失敗。	なし。
FCS_HTTPS_EXT.1	HTTPS セションの確立失敗。	
FCS_RBG_EXT.1	ランダム化プロセスの失敗。	なし。
FCS_STS_EXT.1	なし。	なし。
FCS_TLSC_EXT.1	TLS セションの確立失敗。	なし。
FDP_ACC_EXT.1	なし。	なし。

FDP_ACF_EXT.1	なし。	
FDP_COO_EXT.1	サードパーティクッキーのブロック失敗。	なし
FDP_CSP_EXT.1	なし。	なし。
FDP_DEL_EXT.1	なし。	なし。
FDP_DEL_EXT.2	なし。	なし。
FDP_DEL_EXT.3	なし。	なし。
FDP_PBR_EXT.1	なし。	なし。
FDP_PST_EXT.1	なし。	なし。
FDP_SBX_EXT.1	プロセス制限のすべての違反。	なし。
FDP_SOP_EXT.1	同一生成元ポリシーのすべての例外。	なし。
FDP_STR_EXT.1	なし。	なし。
FDP_TRK_EXT.1	なし。	なし。
FIA_X509_EXT.1	X.509 証明書有効性確認の失敗。	有効性確認失敗の理由。
FIA_X509_EXT.2	なし。	なし。
FMT_MOF.1	任意のセキュリティに関連した TOE の構成への変更。	なし。
FMT_SMF.1	なし。	なし。
FMT_SMR.1	なし。	なし。
FPT_DNL_EXT.1	なし。	なし。
FPT_DNL_EXT.2	なし。	なし。
FPT_INT_EXT.1	なし。	なし。
FPT_INT_EXT.2	なし。	なし。
FPT_INT_EXT.3	なし。	なし。
FPT_MCD_EXT.1	未署名のモバイルコード実行のすべてのインスタンス。信頼されない、または未検証の情報源からのモバイルコード実行のすべてのインスタンス。	証明書の主体
FPT_TST_EXT.1	TSF セルフテストのこのセットの実行。検出された完全性違反。	完全性違反については、その完全性違反を引き起こした TSF コードファイル。
FPT_TUD_EXT.1	更新の開始。更新の完全性の検証のあらゆる失敗。	なし。
FPT_TUD_EXT.2	更新の開始。更新の完全性の検証のあらゆる失敗。	なし。
FPT_TUD_EXT.3	更新の開始。更新の完全性の検証のあらゆる失敗。	なし。
FTP_ITC.1	高信頼チャネルを確立しようとするすべての試行。チャネルデータの改変の検出。	

セキュリティ監査事象の選択

FAU_SEL.1 選択的監査

FAU_SEL.1.1 [選択：TOE、TOE プラットフォーム] は、以下のような属性に基づいて、すべての監査対象事象のセットから監査される事象のセットを選択することができなければならない (shall)：

a) 事象種別、

b) 監査対象セキュリティ事象の成功、

c) 監査対象セキュリティ事象の失敗、及び

d) [割付：*その他の属性*]。

適用上の注意：

本要件の意図は、監査事象を引き起こすために選択可能なすべての基準を識別することである。これは、利用者／管理者が呼び出すクライアント上のインタフェースを介して構成できる。ST 作成者は、割付を用いて任意の追加基準を列挙するか、あるいは「なし」とする。監査対象事象の種別は、表 5 に列挙されている。

保証アクティビティ：

TSS

N/A

ガイダンス

評価者は、ガイダンスにすべての事象の種別が列挙されていることと、要件に従って選択可能であるべきすべての属性が (割付中に列挙された属性を含め) 記述されていることを保証するため、操作ガイダンスを検査しなければならない (shall)。また操作ガイダンスには、現在実施されている選択基準に関わらず、常に記録される監査記録も識別されなければならない (shall)。

テスト

テストは、FAU_GEN.1.1 のテストと組み合わせて達成されるべきである (should)。

D.2 クラス：暗号サポート (FCS)

Strict Transport Security

FCS_STS_EXT.1 拡張：Strict Transport Security

FCS_STS_EXT.1.1 [選択：TOE、TOE プラットフォーム] は、RFC 6797 に従って HTTP Strict-Transport-Security を実装しなければならない (shall)。

FCS_STS_EXT.1.2 [選択：TOE、TOE プラットフォーム] は、max-age ディレクティブ中でウェブサイトにより宣言されたタイムスパンの間､HSTS 有効化をシグナリングする永続的データを保持しなければならない (shall)。

FCS_STS_EXT.1.3 [選択：TOE、TOE プラットフォーム] は、最も新鮮な Strict Security ポリシー情報をキャッシュしなければならない (shall)。

適用上の注意：

ブラウザがウェブサイトから HSTS ヘッダを受け取った場合、TOE とそのウェブサイトのドメインまたはスーパードメインとの間のすべての将来の HTTP セションは、HTTPS (RFC 2818) を利用することにより TLS 1.2 (RFC 5246) 以上の上で行われなければならない (must)。

保証アクティビティ：

TSS

評価者は、TOE がどのように HSTS をサポートするか文書化されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、HSTS を利用する方法に関する指示が含まれることを保証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、ネットワークプロトコルアナライザを動作させてトラフィックを監視しながら、HSTS に準拠したウェブサイトへ接続しなければならない (shall)。評価者はキャプチャされたネットワークトラフィックを検査して、Strict Transport Security ヘッダが受信されていること、そして HSTS 関係の max-age ディレクティブが存在することを検証しなければならない (shall)。
- テスト 2 : 評価者は、HTTP 上で再び HSTS ウェブサイトへ再接続しなければならず (shall)、そしてそのセションが HTTPS へリダイレクトされることを検証しなければならない (shall)。
- テスト 3 : 評価者は、max-age の有効期限が過ぎた後に HSTS ウェブサイトへ再接続し、そしてそのウェブサイトと TOE が HSTS 関係を再確立することを検証しなければならない (shall)。
- テスト 4 : 評価者は、ウェブサイトの HSTS 情報を更新し、そして TOE がそのウェブサイトへ再接続した際、その情報が TOE により更新されることを検証しなければならない (shall)。

D.3 クラス：利用者データ保護 (FDP)

アクセス制御ポリシー

FDP_ACC_EXT.1 拡張：ドメインによるアクセス制御

FDP_ACC_EXT.1.1 TOE は、ドメインをグループ化し、ドメインの特定のセットへアクセス制限を適用する能力を提供しなければならない (shall)。

適用上の注意：

この機能の例は、インターネットエクスプローラーのゾーンの概念である。

保証アクティビティ：

TSS

評価者は、ドメインのグループ化とそれらへのアクセス制限の適用とを TSF がどのようにサポートしているか記述されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、ドメインをグループ化しアクセス制限を適用する能力を構成するステップが文書化されていることを保証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- 評価者はドメインのグループを作成し、そのグループへ特定の制限を適用しなければならない (shall)。評価者は制限されたグループに含まれるドメイン内のウェブサイトへナビゲートしなければならず (shall)、そしてその制限が機能することを検証しなければならない (shall)。評価者は制限されたグループに含まれないドメイン内のウェブサイトへナビゲートしなければならず (shall)、そしてその制限が適用されないことを検証しなければならない (shall)。

永続的情報の保存

FDP_PST_EXT.1 拡張：永続的情報の保存

FDP_PST_EXT.1.1 TOE は、永続的データをファイルシステムへ保存することなく動作する能力を提供しなければならない (shall)。

適用上の注意：

本要件の例外となるのは、クレデンシャル及び構成情報である。

保証アクティビティ：

TSS

評価者は、どのように TOE が永続的利用者データをファイルシステムへ保存することなく動作するのか記述されていることを検証するため、TSS を検査しなければならない (shall)。

ガイダンス

N/A

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1：評価者は、幅広い TOE 機能が確実に行使されるよう、TOE をある期間動作させなければならない (shall)。次に評価者は、クレデンシャルまたは構成情報以外に、ファイルシステムへ書き出されたファイルがないことを保証するため、TOE と基盤となるプラットフォームを検査しなければならない (shall)。

D.4 クラス：TSF の保護 (FPT)

外部エンティティとの TOE の相互作用

FPT_INT_EXT.2 拡張：アプリケーションレピュテーションサービスとの相互作用

FPT_INT_EXT.2.1 TOE は、悪意のあるアプリケーションのダウンロードを防止するためにアプリケーションレピュテーションサービスを利用しなければならない (shall)。

適用上の注意：

アプリケーションレピュテーションサービスは、悪意のあるアプリケーションを識別するオンラインサービスであって、ダウンロード前にそのようなアプリケーションを検出するために用いられる。

保証アクティビティ：

TSS

評価者は、TOE が悪意のあるアプリケーションの検出にアプリケーションレピュテーションサービスを利用することが記述されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、TOE がどのサービスをデフォルトでサポートするか (もしあれば) と、追加的サービスが構成可能であるかどうかを含め、アプリケーションレピュテーションサービスを利用するための TOE のサポートが記述されていることを保証するため、操作ガイダンスを検査しなければならない (shall)。操作ガイダンスには、アプリケーションレピュテーションサービスを構成するためのステップが含まれなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1 : 評価者は、操作ガイダンスに従って 1 つ以上のアプリケーションレピュテーションサービスの利用を有効化するように TOE を構成しなければならない (shall)。評価者は、ネットワークプロトコルアナライザを用いてネットワークトラフィックをスニッフしながら、TOE へのアプリケーションのダウンロードを試行するウェブサイトとの接続を開始しなければならない (shall)。評価者はキャプチャされたネットワークトラフィックを検査しなければならず (shall)、TOE がダウンロード開始前に 1 つまたは複数の構成されたアプリケーションレピュテーションサービスへの接続を開始することを検証しなければならない (shall)。

FPT_INT_EXT.3 拡張：URL レピュテーションサービスとの相互作用

FPT_INT_EXT.3.1 TOE は、悪意のあるウェブサイトとの接続を防止するために URL レピュテーションサービスを利用しなければならない (shall)。

適用上の注意：

URL レピュテーションサービスは、悪意のある、またはフィッシングコンテンツアプリケーションを伴うウェブサイトを識別するオンラインサービスであって、利用者のアクセスを許可する前にそのようなウェブサイトを検出するために用いられる。

本要件の目的は、インターネット上のマルウェアの既知の情報源との接続を TOE が確立す

ることを確実に防止することである。ブロック決定前に取られる特定の一連のアクションは、TOE の特定の実装により異なるかもしれない。例えば、URL レピュテーションサービスによりリアルタイムで提供される不良 URL のリストをチェックすることにより悪意のあるコンテンツのチェックを実装する TOE もあるかもしれない。また TOE 起動時に不良 URL の更新されたリストをダウンロードし、TOE が終了するまで 1 つまたは複数の URL レピュテーションサービスから周期的にリストを更新する TOE もあるかもしれない。最終的に、不良 URL への接続を TOE がブロックする結果となるべきである (should)。

保証アクティビティ：

TSS

評価者は、TSF が悪意のあるウェブサイトの検出に URL レピュテーションサービスを利用することが記述されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、TOE がどのサービスをデフォルトでサポートするか (もしあれば) と、追加的サービスが構成可能であるかどうかを含め、URL レピュテーションサービスを利用するための TOE のサポートが記述されていることを保証するため、操作ガイダンスを検査しなければならない (shall)。操作ガイダンスには、URL レピュテーションサービスを構成するためのステップが含まれなければならない (shall)。

テスト

評価者は、以下のテストを行わなければならない (shall)。

- テスト 1：評価者は、操作ガイダンスに従って 1 つ以上の URL レピュテーションサービスの利用を有効化するように TOE を構成しなければならない (shall)。評価者は、ネットワークプロトコルアナライザを用いてネットワークトラフィックをスニッフしながら、既知の良好なウェブサイトとの接続を開始しなければならない (shall)。評価者はキャプチャされたネットワークトラフィックを検査しなければならず (shall)、TOE が 1 つまたは複数の構成された URL レピュテーションサービスへの接続を開始することを検証しなければならない (shall)。
- テスト 2：評価者は、操作ガイダンスに従って 1 つ以上の URL レピュテーションサービスの利用を有効化するように TOE を構成しなければならない (shall)。評価者は、ネットワークプロトコルアナライザを用いてネットワークトラフィックをスニッフしながら、1 つ以上の URL レピュテーションサービスにより識別されている既知の悪意のあるウェブサイトとの接続を開始しなければならない (shall)。評価者は、そのウェブサイトは悪意のあることが知られているため TOE の接続が許可されないことを警報する警告が表示されることを検証しなければならない (shall)。評価者はキャプチャされたネットワークトラフィックを検査しなければならず (shall)、TOE が 1 つまたは複数の構成された URL レピュテーションサービスへの接続を開始すること、及びテストされたウェブサイトが掲載された悪意のある URL の更新されたリストを取り込んだことを検証しなければならない (shall)。

附属書E： 用語集と略語

E.1 技術的定義

アクティブコンテンツ (Active Content)	利用者と対話することなく、ネイティブにあるいはプラグインを介して、ブラウザ中で実行されるコード
管理者 (Administrator)	管理者は、エンタープライズによりブラウザへ適用されるポリシーの設定を含めた、管理アクティビティに責任を負う。この管理は、リモートで行われることが多い。デバイスがエンタープライズに接続されていない場合、利用者が管理者となる。
アプリケーション (Application)	オペレーティングシステム上で動作するソフトウェアであって、そのプラットフォームの利用者または所有者の代理としてタスクを実行するもの
CSRF	クロスサイトリクエストフォージェリ (Cross Site Request Forgery) — 攻撃者が、標的となる利用者に、その利用者の特権でスクリプトを実行させる脆弱性
DTLS	データグラムトランスポート層セキュリティ (Datagram Transport Layer Security)
拡張機能 (Extension)	ブラウザがデフォルトでは提供しない特定の機能を追加するために、ブラウザへ追加されるコード群
GPU	Graphics Processing Unit (グラフィックス処理ユニット)
HTML	ハイパーテキストマークアップ言語 (HyperText Markup Language) — ブラウザへコンテンツを提示するためにウェブサーバにより用いられる言語
HTML5	ハイパーテキストマークアップ言語バージョン 5 (HyperText Markup Language version 5)、ブラウジング経験を豊かにする多くの新規機能を取り込んだ HTML の新バージョン
HTTP	ハイパーテキスト転送プロトコル (HyperText Transfer Protocol) — ウェブ上で通信を行うためのプロトコル
HTTPS	ハイパーテキスト転送プロトコルセキュア (HyperText Transfer Protocol Secure)；暗号化されたチャネル (SSL/TLS) 上で動作する、HTTP のセキュアなバージョン
JavaScript	コンピュータオブジェクトへのプログラム的アクセスを可能とする、ウェブブラウザの一部としてよく使われるプログラム言語
プラグイン (Plug-in)	特定の種別のウェブコンテンツを取り扱うためのブラウザのアドオン

ポップアップ (Pop-up)	ブラウザウィンドウを、現在フォーカスのあるブラウザインスタンスの外部でオープンさせる、ウェブコード
サンドボックス化 (Sandbox)	プログラムの実行を分離するためのセキュリティメカニズムで、悪意のあるコードを含むかもしれない未検証のプログラムを、そのプログラムがホストシステムに害を与えることを許可せずにテストまたは実行するためによく利用される
タブ (Tabs)	ブラウザの別のインスタンスをスタートさせずに複数のウェブサイトからのコンテンツを表示することをブラウザに可能とする
ウェブブラウザ利用者 (Web Browser User)	非特権モードで TOE を動作させる利用者
ウェブアプリケーション (Web Application)	ウェブ技術 (例えば、Flash、Java、HTML) を利用するソフトウェアアプリケーションであって、ウェブブラウザやその他のクライアントアプリケーション中で動作するもの
ウェブブラウザ (Web Browser)	ウェブサーバにより提供されるコンテンツを取り込んで表示するアプリケーション
ホワイトリスト (Whitelist)	何かを行うことを許可されたドメインのリストを指定するメカニズム
XSS	クロスサイトスクリプティング (Cross Site Scripting) — 後にブラウザで表示されるスクリプトを攻撃者がウェブサイトへ注入することを可能とする、特殊文字の不十分なフィルタリングに起因する脆弱性；ウェブサイトを改ざんしたり、セション情報を盗んだりする攻撃を可能とする

E.2 コモンクライテリア定義

保証 (Assurance)	TOE が SFR を満たしているという確信の根拠 [CC1]。
CC	コモンクライテリア (Common Criteria)
PP	プロテクションプロファイル (Protection Profile)
SAR	セキュリティ保証要件 (Security Assurance Requirement)
SFR	セキュリティ機能要件 (Security Functional Requirement)
セキュリティターゲット (Security Target) (ST)	具体的な識別された TOE に関する、実装に依存したセキュリティの必要性の言明。
評価対象 (Target of Evaluation) (TOE)	評価にゆだねられるソフトウェア、ファームウェア及びハードウェアのセットで、ガイダンスが伴うことがある。

TOE セキュリティ機能 (TSF)	TOE のすべてのハードウェアとソフトウェア、そしてファームウェアの結合した機能であって、SFR の正しい実施のために信頼されなければならない (must) もの
TOE 要約仕様 (TOE Summary Specification) (TSS)	評価者に、TOE における SFR の実装の記述を提供する文書。

E.3 略語

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CRL	証明書失効リスト (Certificate Revocation List)
CSP	暗号サービスプロバイダ (Cryptographic Service Provider)
CSRF	クロスサイトリクエストフォージェリ (Cross Site Request Forgery)
DHE	Diffie-Hellman 鍵交換 (Diffie-Hellman Key Exchange)
DN	識別名 (Distinguished Name)
DSA	デジタル署名アルゴリズム (Digital Signature Algorithm)
DTLS	データグラムトランスポート層セキュリティ (Datagram Transport Layer Security)
ECC	楕円曲線暗号 (Elliptic Curve Cryptography)
ECDSA	楕円曲線デジタル署名アルゴリズム (Elliptic Curve Digital Signature Algorithm)
FFC	有限体暗号 (Finite-Field Cryptography)
FIPS	連邦情報処理規格 (Federal Information Processing Standards)
GCM	Galois/Counter Mode
GPU	Graphics Processing Unit (グラフィックス処理ユニット)
HMAC	Keyed Hash Message Authentication Code
HTML	ハイパーテキストマークアップ言語 (HyperText Markup Language)

HTML5	ハイパーテキストマークアップ言語バージョン 5 (HyperText Markup Language version 5)
HTTP	ハイパーテキスト転送プロトコル (HyperText Transfer Protocol)
HTTPS	ハイパーテキスト転送プロトコルセキュア (HyperText Transfer Protocol Secure)
IETF	インターネットエンジニアリングタスクフォース (Internet Engineering Task Force)
IV	初期化ベクトル (Initialization Vector)
KAT	既知解テスト (Known Answer Test)
KDF	鍵導出関数 (Key Derivation Function)
NIST	国立標準技術研究所 (National Institute of Standards and Technology)
OCSP	オンライン証明書状態プロトコル (Online Certificate Status Protocol)
OID	オブジェクト識別子 (Object Identifier)
PDF	ポータブル文書フォーマット (Portable Document Format)
rDSA	RSA デジタル署名アルゴリズム (RSA Digital Signature Algorithm)
RFC	Request for Comment (IETF)
RGB	ランダムビット生成器 (Random Bit Generator)
RSA	Rivest Shamir Adelman
SaaS	サービスとしてのソフトウェア (Software as a Service)
SHA	セキュアハッシュアルゴリズム (Secure Hash Algorithm)
SSL	Secure Sockets Layer
TLS	トランスポート層セキュリティ (Transport Layer Security)
W3C	World Wide Web Consortium
XSS	クロスサイトスクリプティング (Cross Site Scripting)