TOEセキュリティ機能の脆弱性識別とその対策事例

2005.07版　IPA

関連工程	種別	NO	脆弱性	攻撃例	対策事例
マニュアル	前提	1	前提条件が正確に運用者や利用者に伝わらないため、セキュリティが確保されない環境で、TOEが動作する。	・前提条件が満足されない環境でTOEを使用し、保護資産を不正に利用する。	・前提条件を正確にガイダンス文書に記載し、運用者や利用者に認識させる。（「xxの条件を満足しないと、セキュリティが確保されない。」と記載する。多数の注意書きの中に、単に「xxすること。」と記載しただけでは、その重要性を読者は認識できないことがある。）
基本設計	前提	1	TOEの想定する運用環境では、前提条件を満足させるには無理があり、セキュリティが確保されない環境で、TOEが動作する。 （製品によっては、利用者がガイダンス文書を読まないで、機能を使用する場合がある。）	・前提条件が満足されない環境でTOEを使用し、保護資産を不正に利用する。	・前提条件が満たされていることを、TOEがチェックし、満たされていなければ、TOEの処理を中断して、警告メッセージを表示する。
	エラー処理	1	エラー処理（ハード障害、他機能からのエラーリターン、操作ミス、入力パラメタのミス、暗号秘密鍵の取得/参照不可、などへの対処）の不備で、セキュリティ機能が動作不能になる。	・誤操作、異常なパラメタ値の設定、ハード障害などを誘発し、セキュリティ機能を動作不能にして、保護資産を不正に利用する。	・エラーによって、セキュリティ機能の正常な動作が不可ならば、TOEの処理を安全サイド（保護資産の利用は禁止など）で行う。
	警告	1	不正利用に係わる警告メッセージを表示しても、知見されないため、セキュリティが確保されない環境で、必要な対処がなされないまま、TOEの処理を継続する。	・不正アクセスが検知されないので、不正な利用を継続する。	・警告のためのメッセージが、関係者によって認識されたことを確認する処理を、TOEに組み込む。確認された後に、TOEの処理を継続する。
		2	法律上、不正アクセスは禁止されている旨の警告が表示されない。	・保護資産を不正に利用する。	・TOEを不正に使用することは禁止されている旨の警告を、TOE処理の先頭で表示する。
	メッセージ	1	メッセージのテキストに、秘密情報（パスワードなど）の推測、セキュリティ属性（役割、権限、グループIDなど）の暴露、攻撃対象（ファイル名称、所有者、当該製品やオペレーティングシステムの識別情報など）の識別などを容易にする情報が含まれている。	・テキストの内容を手がかりに秘密情報の推測、セキュリティ属性の把握、攻撃対象の特定を行い、保護資産を不正に利用する。	・関連者の行為に不必要な情報は、表示(通知）しない。 ・メッセージテキストには、攻撃者にとって有益な情報を含めない。
		1	セキュリティ機能をバイパスできる操作が存在する。	・セキュリティ機能をバイパスする操作をした後、保護資産を不正に利用する。 ・権限付与者による当該操作を誘発（ソーシャルエンジニアリングなど）し、保護資産を不正に利用する。	・セキュリティ機能のバイパス操作の実施は、権限付与者に制限する。 ・セキュリティ機能のバイパスが操作された時には、当該操作の再確認（誤操作でないことの確認）を行なう。

関連工程	種別	NO	脆弱性	攻撃例	対策事例
	操作	2	セキュリティ機能を非稼動に（停止）できる操作が存在する。	・セキュリティ機能を非稼動にした後に、保護資産を不正に利用する。 ・権限付与者による当該操作を誘発（ソーシャルエンジニアリングなど）し、保護資産を不正に利用する。	・セキュリティ機能の非稼動（停止）操作の実施は、権限付与者に制限する。 ・セキュリティ機能の非稼動が操作された時には、当該操作の再確認（誤操作でないことの確認）を行なう。
		3	セキュリティ機能が起動されていない状態で、TOEは保護資産の処理を実施できる。	・セキュリティ機能が起動されていない時に、保護資産を不正に利用する。	・TOEの初期設定の段階で、自動的にセキュリティ機能を起動する。 ・セキュリティ機能が動作していなければ、保護資産に対するTOEの処理は行わない。
	共用データ	1	保護資産が共用の記憶領域(媒体）に格納されているため、当該保護資産の処理に無関係の人（非許可者）からも、利用される。	・共用域にある保護資産を不正に利用する。	・保護資産に対するアクセス制御を行う。 ・保護資産を暗号化して格納する。
		2	保護資産が不揮発性の記憶領域(媒体）に格納されているため、処理が終了(ファイルはデリート）しても、データそのものは、記憶領域(媒体）に残留する。	・記憶媒体を取り出し、その媒体にアクセスできる環境で、格納されている保護資産を暴露する。 ・記憶領域を表示機能で暴露する。	・記憶媒体上の保護資産を暗号化する。 ・処理が終了したならば、記憶媒体上から、データそのものをイレーズする。
	共用サービス		複数の利用者がTOE機能を利用できようになっているため、当該機能に係わる業務に無関係の人（非許可者）からも利用される。	・TOE機能を利用して、保護資産を不正に利用する。	・TOE機能の実行に係わるアクセス制御（許可者のみ当該機能の実行を可）を行う。
	利用者識別	1	グループIDが利用できるため、個人の責任追跡ができない。	・グループIDを使用し、不正利用者個人の特定を困難または、不可にする。このため、即時の対処が困難になる。	・グループIDの使用は監視する。 ・個人が識別できる場合のみ、グループIDでTOEの使用を許可する。
	認証	1	容易に推測できるパスワードを設定することができる。	・辞書攻撃。 ・暗号化されているパスワードファイルを入手後、制限されない環境で、パスワードを推測する。	・推測を困難にするように、パスワードの長さや構文の規則を設定する。 ・パスワードファイルを保護する。
		2	利用者が直接、クライアントを操作する場合には、利用者の認証を行っているが、関連のサーバからAPIで呼ばれた場合は、利用者の認証は行なっていない。	・不正なクライアントから、関連サーバ経由で、TOEを利用し（認証なしで）、保護資産を不正に利用する。	・API経由でもクライアントの認証を行う。
		3	TOE機能の実行中は、個々のサービスの単位で利用者を認証することはできない。	・正当な利用者が利用端末から離席したスキに、保護資産を不正に利用する。	・クライアントからの未入力時間を監視し、タイムオーバ後の処理再開時には、再認証する。

関連工程	種別	NO	脆弱性	攻撃例	対策事例
機能設計		4	不正者が、他人の認証を連続して失敗させることによって、当該利用者は失効状態にさせられる。	・規定回数、連続して不当なパスワードを入力する。	・監査ログを採取して、不正者を識別できるようにする。 ・失効者の復旧。 ・不正者の端末を識別し、端末をブロックする。
	セキュリティ属性値	1	セキュリティ属性値（アクセス権限、フィルタリングルール、など）の設定値を誤ると、セキュリティ機能が有効に動作しない。	・誤った値が設定されている間に、保護資産を不正に利用する。 ・誤った値が設定されるように誘導する（ソーシャルエンジニアリング）	・セキュリティ属性値の妥当性をチェックする。
		2	セキュリティ属性値（アクセス権限、フィルタリングルール、など）のデフォルト値が不適切であるため、セキュリティ機能が有効に動作しない。	・製品の導入直後に、保護資産を不正に利用する。	・セキュリティ属性値のデフォルトを、TOEが安全サイドで機能するように設定する。
	利用権限	1	TOEの機能上、必要でない情報資産が利用できる。（機能の処理内容から見て、情報資産の利用単位/範囲が不適切。）	・アクセス権限の範囲で得た保護資産を暴露する。	・アクセスできる情報の単位を、TOEの個々の機能で必要最小限のものにする。
		2	複数の管理機能を単一の権限（役割分担）で実施している。	・単一の権限を取得して、他の多数の管理機能を不正に利用する。	・TOEの管理権限（役割分担）の分散化を図る。
	管理データ	1	TOEの管理ファイル（アクセス規則、登録利用者のIPアドレス、通信データあて先アドレス、セキュリティ機能管理データ、などが格納）が他のファイルに置換あるいは、中のデータが変更された場合でも、TOEはその管理データに基いて実行する。	・TOEの管理ファイルを偽造し、保護資産を不正に利用する。 ・TOEの管理データを改ざんし、保護資産を不正に利用する。	・TOE管理ファイルの更新権限を、権限付与者に制限する。 ・TOE管理ファイル（あるいは、データ）の改ざん検出を行う。
		2	TOEの管理ファイルの名称（ディレクトリー名称）から、、容易に、秘密データ（構成パラメタ、アクセスルール、暗号鍵、など）が格納されていることが推測できる。	・短期間に攻撃対象ファイルを絞り込んで、秘密情報を暴露し、保護資産を不正に利用する。	・格納データが推測できるような名称を、ディレクトリーやファイルに付与しない。
	情報資産管理	1	保護資産（ファイルなど）の作成時には、初期値（デフォルト）として、誰でも、その保護資産を利用できる。	・利用許可が無いにもかかわらず、保護資産を不正に利用する。	・保護資産の作成時の初期アクセス権は、所有者のみアクセス可とする。
		1	ネットワーク回線上のデータが平文のため、データを参照することができる。	・プロトコルアナラーザなどのツールによって、ネットワーク上の通信データを盗聴する。	・データを暗号化する。

関連工程	種別	NO	脆弱性	攻撃例	対策事例
	通信データ	2	無線通信データが平文のため、データを参照することができる。	・無線通信用の盗聴（傍受）装置によって、通信データを盗聴する。	・データを暗号化する。
		3	データを送受信しているエンティティの識別は、パケットに設定されているIPアドレスに基づいている。	・パケットのIPアドレスを改ざん（送信元IPアドレスの詐称など）して、不正にデータを入手する。	・データを暗号化する。 ・送信元IPアドレスのフィルタリングを行なう。
	隠れチャネル	1	正当に存在する通信チャネルを利用して、保護資産を転送できる。（例：通信パケットの制御用の領域にデータを混入させると、そのデータを取り出すことは可能。）	・正当に存在するチャネルを使用して、保護資産を暴露する。	・保護資産を暴露できるチャネルを閉塞（あるいは、通信可能量を最小化）する。
	添付ファイル	1	利用者の添付ファイルを無条件にOPENする。	・添付ファイルに不正なプログラム（実行マクロ）を挿入して、自動的に実行させることによって、保護資産を不正に利用する。	・添付ファイルのOpenの可否を利用者に問い合わせる。
	プログラムコード	1	特定のファイルに登録されているプログラムを、TOEが実行している。	・特定のファイルに不正プログラムを登録し、そのプログラムの実行によって、保護資産を不正に利用する。	・特定ファイルへのアクセスを制限する。 ・プログラムの認証を行う。
		2	Webサイトからプログラムをダウンロードして、TOEが実行している。	・不正なWebに不正なプログラムを登録し、そのプログラムの実行によって、保護資産を不正に利用する。	・プログラムの認証を行う。
		3	利用者が実行プログラムを作成（マクロの作成など）できるため、不正なプログラムでも実行される。	・不正なマクロを作成し、、そのプログラムの実行によって、保護資産を不正に利用する。	・利用者作成プログラムの内容の正当性確認を行わない限り、実行できないようにする。
		4	利用者がコマンドを送信できるため、不正なコマンドでも実行される。	・不正なコマンドを送信する。	・コマンドの内容の正当性確認を行わない限り、実行できないようにする。
	監査	1	大量のログデータが一度に採取されるため（監査ログとメッセージーログの共用などによる）、有用なログデータをタイムリーに検出することは困難である。	・APIを利用して、大量のダミーメッセージを発生させ、不正アクセスの検出を困難にする。	・監査データのロギング機能は専用の機能とする。
		2	監査用のログデータを変更できる。	・不正利用に係わるデータが格納されている監査用ログデータを改ざんする。	・監査ログデータは参照のみ可とする。
		3	監査用のログデータを採取していないので、保護資産のアクセス履歴が記録されない。	・不正利用しても、証拠が無い。	・保護資産のアクセスに係る監査ログを採取する。

関連工程	種別	NO	脆弱性	攻撃例	対策事例
		4	監査ログデータにより、個人の利用状況を把握できる。	・監査ログデータの内容を暴露する。	・監査者以外はアクセスできないように監査ログを保護する。
	バックアップデータ	1	バックアップデータを参照や変更することができる。	・バックアップデータを使用して、保護資産を不正に利用する。	・バックアップ時に、暴露防止や改ざん検出の処理を行う。
	サービス否認	1	利用者がTOEへサービスを依頼したり、TOEからのサービス受領の事実を否認した場合、それらの事実を証明する（否認を拒否する）手段が無い。	・TOEへのサービスの依頼や提供の事実を拒否することによって、TOEのサービスを妨害する。	・否認拒否機能（プロトコル）を導入する。
		2	TOEが保管している利用者データが変更されたり、置換されたりしていないことを証明する手段が無い。	・TOEが保管しているデータに対して、改ざんや置換をクレームして、サービスを妨害する。	・TOEが保管しているデータに対して、電子署名を施す。
	暗号鍵	1	暗号鍵は参照や作成できる。	・鍵解読攻撃を行う。 ・暗号鍵の格納域に不正にアクセスする。	・十分な強度の暗号鍵を生成する。 ・不正アクセスを拒否できる領域、方法で暗号鍵を保管/配布する。
	秘密情報	1	確率や統計的な手法で秘密情報（例えば、パスワード）を生成している場合、同じ手法によって、同じ秘密情報を生成することが可能である。	・TOEが使用している手法（文字の組み合わせなど）で、秘密情報を生成する。	・秘密情報の生成が、実時間内には困難となるような生成の規則を導入する。
	非公開機能	1	TOEの保護資産を利用できる、非公開のインタフェースが存在している。	・非公開のインタフェースを使用して、TOEの保護資産を不正に利用する。	・利用者（当該インタフェース公開対象プログラム）の認証を行う。 ・インタフェース情報を保護する。
	処理回路	1	物理的な干渉によって、TOEの処理回路の変更や参照ができる。	・配線加工装置などを使用して処理回路を改ざんし、セキュリティ機能を無効にする。 ・物理的プロービング（探針）により、処理回路を暴露して、同等の機器を偽造する。 ・電子顕微鏡などで回路構成を解析し、機器を偽造する。 ・機器の樹脂や絶縁膜を除去して、回路構成を暴露して、機器を偽造する。	・探針検出機能を装備する。 ・改ざん検出機能を装備する。 ・物理的ストレスの検知機能を装備する。

関連工程	種別	NO	脆弱性	攻撃例	対策事例
論理設計		2	TOEの処理に係わる物理的な特性を解析すると、処理論理や制御用のデータが推測できる。	・処理時間、消費電力、出力データなどを解析して、処理論理や制御用のデータ（暗号鍵など）を推測し、セキュリティ機能を無効にする。	・物理的特性の冗長化（推測できないように）を図る。
		3	環境のストレスによって、TOEの回路動作に異常が発生する。	・振動、温度などの環境ストレスを与えて、回路に誤動作を発生させ、セキュリティ機能を無効にする。	・異常発生時には、TOEを安全サイドで動作させる。
	エラー処理	1	TOEのエラー処理（ハード障害、タイムアウト、他モジュールからのエラーリターン、管理情報の破壊、異常な入力データ、バッファオーバフロー、暗号秘密鍵参照エラー、不正な再送、などへの対処）の不備で、セキュリティ機能が動作不能になる。	・エラーの発生を誘発し、セキュリティ機能を動作不能にして、保護資産を不正に利用する。	・エラーによって、セキュリティ機能の正常な動作が不可ならば、TOEの処理を安全サイド（保護資産の利用は禁止など）で行う。。
	監査	1	監査ログデータ用のバッファがオーバフローした際、以前の記録データを上書きして、消してしまう。	・保護資産を不正に利用した後、ダミーのアクセスを大量に行って、そのログデータを上書きさせて、不正利用の痕跡を消す。	・バッファがオーバフローする以前に、システム運用者に通知する。 ・バッファがオーバフローした場合には、情報資産へのアクセスを中断する。
保守	配付	1	TOEの実行コードを利用者に配付している。	・リバースエンジニアリングによって、コード情報を取得し、ソフトウェアやハードウェアを偽造して、保護資産を不正に利用する。	・ハードウェアに対しては、耐タンパー性を装備する。 ・正当な機能であることを認証する。
		2	追加の機能やパッチを、保護しないで利用者に配付している。	・不正プログラムを、追加機能やパッチとして配布し、保護資産を不正に利用する。	・追加機能やパッチに電子署名を添付し、適用側で検証する。
		3	TOEに係わるセキュリティ問題とその対処のためのパッチ情報が、すべての利用者に、タイムリー、かつ、正確に伝えられない。	・パッチを分析して、攻撃方法を見つける。	・利用者にパッチを速やかに適用させる。
	認証	1	運用システムにデフォルトパスワード（テスト、インストール、保守用など）が残留する。	・推測して使用する。 ・開発者や保守者が、一般利用者として使用する。	・作業後は、デフォルトパスワードは抹消する。 ・運用開始時に、残留が無い事を確認する。 ・保守時の都度、管理者により設定、完了後は抹消する。

関連工程	種別	NO	脆弱性	攻撃例	対策事例
運用	利用者登録	1	長期間、未使用（非使用）の利用者が登録されたままの状態で残る。	・未検出の状態で、不正な利用を継続する。	・長期未使用利用者の検出機能を導入する。 ・頻繁に利用者登録状況の確認と更新を行う。 ・人事部門と連携する。
	不正なプログラムコード	1	TOEにプログラムを追加し、TOE機能の一部として、動作させることができる。	・実行コードの一部を、不正コードで置換する。 ・コードをcall命令に置き換えて、不正コードを呼び出す。 ・ソースコードを改ざんする。	・機能専用のプログラム実行領域を確保し、他からの干渉を阻止する。 ・ソースコードライブラリーを保護する。
	共用資産	1	保護資産が共用の記憶領域(媒体）に格納されているため、他のシステム（開発システムなど）からもアクセスできる。	・当該資産を共有している環境から、TOEの保護資産を不正に利用する。	・共有している他の環境に対して、アクセス制御。
	内部不正	1	権限付与者が保護資産を不正に利用する。	・内部不正。 ・権限付与者を脅迫する。	・権限付与者の行為を監視する。 ・権限付与者と個別に契約する。
	資源枯渇	1	セキュリティ機能が動作するために必要な資源が枯渇すると、そのタイムリーな動作が保証できなくなる。	・Ｄｏｓ攻撃	・セキュリティ機能の動作に必要な資源（各種のバッファ領域など）は、動作環境に応じて、必要な量を確保できるようにしておく。 ・枯渇した場合には、TOEの処理を安全サイド（保護資産の利用は禁止など）で行う。
	電磁波放射	1	電磁波の放射により情報が流出する。	・放射する電磁波を解析する。	・情報機器に電磁波放射シールドを付ける。 ・建屋に電磁波の遮蔽を施す。
	特殊機能	1	デバックツールやユーティティプログラムなどの、特殊目的の機能が、TOEの保護資産を利用できる。	・デバックツールやユーティティプログラムなどの、特殊目的の機能を使用して、TOEの保護資産を不正に利用する。	・特殊プログラムの利用を管理する。 ・特殊プログラムは運用環境では利用できないようにしておく。 ・特殊プログラムの利用に際しても、利用者の認証を行う。