

ITセキュリティ評価・認証業務における判断事例

バージョン 1.4
2007年7月17日

独立行政法人 情報処理推進機構
セキュリティセンター 情報セキュリティ認証室

まえがき

本書の目的

本書は、「IT セキュリティ評価・認証制度」に基づいて実施した評価・認証業務において抽出された問題点およびそれらに対する判断を整理したものである。ST 作成、及び評価作業における参考資料として利用してもらうことを目的に公開するものである。

使用上の注意

本書は、IT セキュリティ評価・認証制度における判断事例を示したものであり、新たな規格を定めるものでも、現規格を補足するものではない。

- 目次 -

1. 暗号アルゴリズムと SOF について	1
2. ST に含まれる秘密情報の扱い	2
3. 単独利用者の識別・認証	3
4. 使用を認める暗号アルゴリズムについて	4
5. セキュリティ機能コンポーネントの依存性の除去について	5
6. セキュリティ監査機能の必要性について	6
7. 前提条件を満たさない SOF のワーストケースは妥当か	7
8. TOE リファレンスの一貫性について	9
9. IT 環境のセキュリティ機能に関連するデータ管理について	10
10. 「以上」や「シリーズ」を用いた動作環境の特定	11
11. 前提条件の記述について	13
12. FAU_GEN.1 における、監査対象事象の妥当性について	15
13. TOE 名称 (TOE 範囲) と製品名称の関係	16
14. OSP における暗黙の脅威の想定	18
15. 意図する使用法・使用環境を直接明示しない前提条件	19
16. FPT_STM.1 が適用可能なケース	21
17. 動作環境の製品指定と動作確認保証について	22

1. 暗号アルゴリズムとSOFについて

問題の概要:

ハッシュ関数を含む暗号アルゴリズムの強度については、CC の適用範囲外である。そのため、暗号が用いられるという根拠をもって、すべての場合において実現される TOE セキュリティ機能を強度分析の対象から外すことが適切であるか。

判断の内容:

暗号化アルゴリズムの強度は CC の適用範囲外である。また、暗号アルゴリズムの制度での運用については、「使用を認める暗号アルゴリズム」(認証レビュー事例 4)として公開されている。よって、「使用を認める暗号アルゴリズム」を適切に使用している場合については、機能強度分析の対象とはしない。

しかしながら、評価者はそれらの暗号アルゴリズムの使用法の適切性や標準とされていない暗号アルゴリズムの安全性については判断をしなければならない。

たとえば、利用者に対し TOE がデータ暗号化に用いる秘密鍵を入力するインタフェースを持ち、その鍵長がそのまま機能強度で考慮されるべきパスワードスペースとして扱われるような場合や、ハッシュ値の衝突を試行可能なインタフェースを持ち、その結果がデータの正当性の検証として用いられるような使用がなされている場合、評価者はその使用法や安全性の見地から、暗号アルゴリズムの評定によらない確率・順列的側面として機能強度を考慮すべきかを判断しなければならない。

備考:

特になし。

2. STに含まれる秘密情報の扱い

問題の概要:

秘密情報が含まれる ST で評価・認証を受け、ST 公開時に評価・認証を受けた ST から秘密情報を削除した ST を作成して公開することができるか。

判断の内容:

評価・認証を受けた ST から秘密情報を削除して ST を公開することはできない。CCRA においては、以下のような形で ST から秘密情報を除去することを求めている。

I.13 Security Target

The Security Target must be included with the Certification/Validation Report. However, it should be sanitised by the removal or paraphrase of proprietary technical information.

(出典: ARRANGEMENT on the Recognition of Common Criteria Certificates)

CCRA の枠組みにおいては、ST は、秘密情報を除去、あるいは問題のない表現に置き換えたものでなければならない。

日本の制度において、公開される ST は、評価に合格し、認証を受けた ST である。CC/CEM で規定された評価・認証に必要な情報は、すべて ST に記述されていなければならない。CC/CEM の規定を満たしていない ST は、評価・認証済みの ST ではなく、認証報告書に含めることはできない。つまり、公開の対象となる ST には、秘密情報が含まれるべきでない。また、評価・認証済みの ST から情報を削除したものを公開対象とすることはできない。なお、公開対象としない ST に秘密情報が含まれることは、特に問題とならない。

一方、評価・認証の参考資料として秘密情報を付加することは可能である。この情報は、評価・認証上必須ではないが、それがあることによって、評価者、認証者の判断の助けとなるものである。この参考資料は、ST 本体の公開を考慮し、ST と分けて提出されるべきである。ST は、ST 本体だけで独立した文書でなければならない。本文中でこの参考資料を参照するのは好ましくない。参考資料の内容は、製品の詳細仕様、設計・製造方法、特定の環境に関わるものなどが考えられる。多くは、ST の TOE 記述や TOE 要約仕様を補足するようなものとなる。あるいは、ST 確認における保証要件への依存性を満たすことの証明資料など、セキュリティ機能要件に関わるものであってもよい。

備考:

特になし。

3. 単独利用者の識別・認証

問題の概要:

TOE の利用者が 1 名しかいない場合、TOE は、利用者を識別する必要がないと考えられる。この場合でも、利用者認証要件の依存性を満たすために利用者識別要件が必要か。

判断の内容:

利用者認証要件の依存性を満たさないことの正当性が根拠として適切に述べられていれば、利用者識別要件は必ずしも必要ではない。

TOE に登録された利用者が 1 名の場合、利用者を一意に特定する必要はない。このため、必ずしも利用者を識別するためのメカニズムが必要とは限らず、TOE は、利用者から認証情報を提示されるだけで認証を実施できる。TOE が利用者識別のメカニズムを実装しないのであれば、それに該当する要件がなくても実質的な問題は生じない。そのため、利用者識別要件を省略した場合でも、利用者認証要件が依存性を満たさないことの正当性を根拠として適切に述べてあれば、利用者識別要件は必要ないと判断する。

なお、利用者が 1 名だけでも、TOE が明示的に利用者に識別行為（例えば ID 入力）を要求してもよい。この場合は、利用者識別要件が必要になる。

備考:

利用者が 1 名だけという TOE の使用環境・使用方法については、TOE セキュリティ環境の前提条件等で明確にされ、適切なセキュリティ対策方針が提示されていなければならない。例えば、何人もの利用者が同一のパスワードを用い、一人の利用者として TOE を利用するような使い方をすると、TOE は、それらの利用者群から特定の個人を識別することができない。利用者は、自分自身が正確に識別されないことから、悪意を持って TOE を利用するかもしれない。TOE の使用方法がセキュリティ上の問題につながらないことについて、十分に吟味される必要がある。

4. 使用を認める暗号アルゴリズムについて

問題の概要:

セキュリティ機能要件に、公知ではない暗号アルゴリズム（ハッシュや乱数生成のアルゴリズムを含む）を使用することができるか。また、電子政府推奨暗号リストに掲載されていない暗号アルゴリズムを使用することができるか。

判断の内容:

安全性について客観的で信頼できる証拠があれば、公知ではないアルゴリズムや電子政府推奨暗号リストに掲載されていない暗号を使用することはできる。

暗号アルゴリズムの評価は、現在のところ CC の評価対象外であり、CEM においては、国ごとの制度で対応するとされている。

日本の制度では、暗号アルゴリズムの扱いについて明文化された規定を公示していないが、現在、以下のような運用をしている。

- ・ 総務省と経済産業省によって定められた電子政府推奨暗号リストに載せられたものは認める
- ・ 信頼できる第三者機関で実績があるものは認める
- ・ 上記以外のものは安全性について客観的で信頼できる証拠資料があれば、それを確認のうえで認めるかどうかの判断をする

「安全について客観的で信頼できる証拠資料」とは、業界標準としての実績を伴う信頼できる資料、信頼できる学会での第三者の客観的な評価を伴う安全性の証拠となる資料などが該当する。

なお、IPA や NIST (National Institute of Standards and Technology : 米国国立標準技術研究所) などの機関から提供されるアルゴリズムの脆弱性に関する情報について十分注意して使用するアルゴリズムを選定すること。

備考:

特になし。

5. セキュリティ機能コンポーネントの依存性の除去について

問題の概要:

自由選択の依存性を持つセキュリティ機能コンポーネントの依存性を除去する場合、自由選択の対象となるすべてのコンポーネントの依存性を満たさない根拠を示さなければならないのか。

判断の内容:

自由選択の対象となるすべてのコンポーネントの依存性を満たさない根拠を示さなければならない。

セキュリティ機能コンポーネントが自由選択の依存性を持つ場合、その依存性を満たさない場合の正当化においては、自由選択の対象となる全てのコンポーネントに対する依存性を満たさなくてもよい適切な正当化が含まなければならない。

例)

FCS_CKM.1 暗号鍵生成

下位階層: なし

FCS_CKM.1.1 TSF は、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵生成アルゴリズム[割付: *暗号鍵生成アルゴリズム*]と指定された暗号鍵長[割付: *暗号鍵長*]に従って、暗号鍵を生成しなければならない。

依存性: [FCS_CKM.2 暗号鍵配付

または

FCS_COP.1 暗号操作]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

この TOE セキュリティ機能要件の依存性を除去する場合、[FCS_CKM.2 暗号鍵配付 または FCS_COP.1 暗号操作]については、FCS_CKM.2 と FCS_COP.1 の両方の機能コンポーネントに対する依存性除去の正当化が提供されなければならない。

依存性除去の正当化の記述において、FCS_CKM.2 だけについて言及しており、FCS_COP.1 について言及していない場合は、正しい正当化とは言えない。

備考:

特になし。

6. セキュリティ監査機能の必要性について

問題の概要:

STにおいてセキュリティ監査機能がセキュリティ機能要件として記述されているが、セキュリティ監査機能の必要性が十分に述べられていないSTが存在する。

判断の内容:

セキュリティ監査機能を要件として記述する場合は、監査要件が対抗する脅威が明確に識別されていて、その対抗根拠が明確に記述されていることが必要である。

なお、一般的にセキュリティ監査機能で対抗することができる脅威は、以下に示すものなどが考えられる。

- ・ TOEの許可利用者による誤操作に対するトレース
- ・ 他のセキュリティ機能と共に動作して脅威に対抗する場合（識別認証の失敗事象を監査することで攻撃者による不正なアクセスの試みを検出して脅威を低減させるなど）

備考:

特になし。

7. 前提条件を満たさないSOFのワーストケースは妥当か

問題の概要:

ワークユニット AVA_SOF.1-3 の SOF 分析で、その分析の正当性を決定する際に用いるワーストケースとは、前提条件が満たされないことを考慮する必要があるのか。

たとえば、パスワードの使用において、TOE 利用者が英数字および特殊文字の組み合わせにおいてパスワードを形成することを保証手段（利用者ガイダンス）により規定しているが、TOE の機能としては英数字および特殊文字の使用可能な文字種のみを判別し、その組み合わせであることを前提としていない。このような場合、SOF 分析におけるワーストケースとは、英数字および特殊文字の組み合わせの範囲で考えることができるか、あるいは機能として除外できないのであれば、数字のみ等前提条件を満たさないワーストケースを考えるべきなのか。

判断の内容:

SOF 分析において、前提条件を満たさないワーストケースを考慮する必要はない。CEM の段落 849 および 850 では、以下のような記述がある。

849 ワーストケースが ST により無効にされない限り、SOF 分析を裏付ける前提条件には、このワーストケースを反映するべきである。多数の異なる可能なシナリオが存在し、これらが人間利用者または攻撃者に依存する場合、すでに述べたように、このケースが無効にされない限り、最小の強度を表すケースが想定されるべきである。

850 例えば、最大の論理的パスワードスペースに基づく強度の主張（すなわち、すべての印刷可能な ASCII 文字）は、自然言語パスワードを使用してパスワードスペース及び関係する強度を効果的に減らすのが人間のふるまいであるために、ワーストケースとはならない。ただし、自然言語パスワードの使用を最小にするパスワードフィルタなど、ST に識別されている IT 手段を TOE が使用する場合、そのような前提条件は、適切となる。

CEM では、ST によりワーストケースが無効にされていない場合、SOF 分析の前提としてこのワーストケースを反映するべきと述べている。つまり、ST により除外されるようなワーストケースは考慮しなくてよいと考える。段落 850 では、ST により除外される例として IT 手段を TOE が用いた場合を述べているが、保証手段であることを制限しているわけではない。

また CC パート 1 の「6.3.1 セキュリティ環境」に以下の記述がある。

- a) TOE がセキュアと見なされるために TOE の環境が満たすべき前提条件のステートメント。このステートメントは、TOE の評価に対する公理として受け入れることができる。

公理とは証明なしに採用される命題である。よって前提条件は SOF 分析を含む TOE 評価の出発点として考えるべきである。前提条件を考慮しないワーストケースを以って、単純な機能としての順列・組み合わせの強度を示すことは、すでに TOE がセキュアと見なせない状態での評価であり意味がない。

よって、SOF 分析のワーストケースとは前提条件が満たされる範囲内でのワーストケースを考慮すればよく、前提条件が満たされない場合までを考慮する必要はない。

備考:

前提条件の適切性について

前提条件の記述内容については、その妥当性、実現性、正確性について十分考慮されなければならない。

前提条件において、利用者がパスワードの規則（安易に推測されやすいパスワードを使用しない等）を遵守するとした場合、その規則を適用したワーストケースを考慮すればよい。しかし、TOE の利用環境として不特定多数かつ資産に特に責任を負わない利用者を想定している場合、パスワード規則を遵守するという前提条件が必ず履行される可能性は低い。一方、TOE の利用環境が特定の利用者を対象とし、また TOE のセキュアな状態が保たれないと利用者自身の資産が危うくなるケースでは、パスワードの規則を遵守するという前提条件の実現性は十分あると考えられる。

8. TOEリファレンスの一貫性について

問題の概要:

TOE のバージョンが「Version 1.1」であり、評価用提供物件として提供されたガイドンス文書に「本ガイドンスが対応する製品のバージョン：Version 1.0 以上」と記述されていた場合、TOE とガイドンス文書の関係付けは正しく行われていると判断できるか。

TOE リファレンスの一貫性については、ACM_CAP.3-3 において要求されている。

ACM_CAP.3-3 評価者は、使用されている TOE リファレンスが一貫していることをチェックしなければならない。

もし、TOE に 2 度以上のラベルが付けられているならば、ラベルは一貫している必要がある。例えば、TOE の一部として提供されるラベルの付いたガイドンス証拠資料を評価される運用可能 TOE に関係付けることができるべきである。これにより消費者は、TOE の評価済みバージョンを購入したこと、このバージョンを設置したこと、ST に従って TOE を運用するためのガイドンスの正しいバージョンを所有していることを確信できる。評価者は、提供された CM 証拠資料の一部である構成リストを使用して識別情報の一貫性のある使用を検証することができる。

判断の内容:

一般的に、「Version 1.0 以上」という表現は「Version 1.1」を含んでいると判断できることから、TOE とガイドンス文書の関係付けは正しく行われていると判断して問題ない（ガイドンス文書の記述を「Version 1.0 以上」から「Version 1.1」に修正する必要はない）。

備考:

特になし。

9. IT環境のセキュリティ機能に関連するデータ管理について

問題の概要:

IT環境が持つセキュリティ機能を利用しているTOEにおいて、そのIT環境のセキュリティ機能が利用するデータの管理(データを管理しているのはTOE)をSTで表現することはできるか。

判断の内容:

IT環境のセキュリティ機能が利用するデータの管理に関する記述方法の例を以下に示す。

IT環境が持つセキュリティ機能は、IT環境に対するセキュリティ要件として定義し、TOEが実施するデータ管理は、TOEセキュリティ機能要件として定義する。この時、TOEが管理するIT環境のセキュリティ機能のためのデータは、利用者データとして扱う。TOEのセキュリティ機能が利用するデータはTSFデータとして扱う必要があるが、IT環境のセキュリティ機能が利用するデータをTSFデータとして扱うことは不適切である。

アクセス制御によりデータの管理を実施するのであれば、TOEセキュリティ機能要件として、FDPクラス(FDP_ACC、FDP_ACFなど)を使用する。FMTクラス(FMT_MTD)は、TSFデータの管理に関する要件なので使用しない。

例) IT環境が提供する識別認証機能を利用し、識別認証データをTOEが管理する場合

IT環境に対するセキュリティ要件として識別認証(FIAクラス)を定義し、TOEセキュリティ機能要件として識別認証データの管理(FDPクラス)を定義する。

備考:

特になし。

10. 「以上」や「シリーズ」を用いた動作環境の特定

問題の概要:

ST において、TOE の動作環境として「オペレーティングシステムに対してサービスパック 3 以上を適用する」と記述した場合、“サービスパック 3 以上”という表現では、TOE が動作するソフトウェア環境が特定されていないのではないか。

判断の内容:

ST 読者が TOE の動作環境を明確に識別することができれば、“以上”という表現を使用しても問題はない。“以上”や“シリーズ”という表現に関わらず、TOE の動作環境が明確に識別できれば、どのような表現を使用しても問題はない。

TOE の動作環境に“以上”という表現を使用した場合の留意点を以下に示す。

- ・ 一般的に“以上”という表現を使用することにより記述内容は曖昧になることが考えられる。従って、ST読者がTOEの動作環境について誤解することがないように、“以上”という表現の使用方法には注意する。
- ・ “以上”という表現により複数の環境がTOEの動作環境に含まれる場合、全ての動作環境が評価の対象になる。例えば、TOEのテストにおいて、全ての動作環境においてテストが行われていない場合は、評価は不合格となる（全ての動作環境でテストをしなくても問題がないことが言及されている場合は除く）。
- ・ “以上”という表現により、認証取得後に提供される動作環境が含まれる場合、開発者は認証取得後に提供される動作環境におけるTOEのセキュリティ機能の動作についても保証することになる。認証取得後に提供されたTOEの動作環境において、TOEのセキュリティ機能が正常に動作しないことが判明した場合、認証が一時停止又は取消しとなる（認証申請に係る規程「ITセキュリティ認証申請手続等に関する規程：CCM-02」を参照）。

例)ST に TOE の動作環境として“ Windows 2000 Professional Service Pack 3 以上 ” と記述されていた場合

ST読者は、この記述から“ Windows 2000 Professional Service Pack 3 ”、“ Windows 2000 Professional Service Pack 4 ” は TOE の動作環境として適しており、“ Windows 2000 Professional(サービスパック未適用)”、“ Windows 2000 Professional Service Pack 1 ”、“ Windows 2000 Professional Service Pack 2 ” は TOE の動作環境として適していないことが判断できる。

認証取得後に“ Windows 2000 Professional ” に対して“ Service Pack 5 ”

が提供された場合、開発者は“ Windows 2000 Professional Service Pack 5 ” の環境における TOE のセキュリティ機能の動作についても保証しなければならない。“ Windows 2000 Professional Service Pack 5 ” の環境において TOE のセキュリティ機能が正常に動作しない場合、認証が一時停止される。

備考:

関連する判断事例: [17. 動作環境の製品指定と動作確認保証について]

11. 前提条件の記述について

問題の概要:

パーソナルコンピュータにインストールして使用する TOE について、ST の前提条件に以下に示すような TOE の動作環境を記述する必要はあるか。なお、TOE が持つセキュリティ機能の動作に関して、TOE はパーソナルコンピュータ及びオペレーティングシステムと関連性を持っていないものとする。

例 1)

A.IT ENVIRONMENT : TOE の動作環境

TOE を使用するために TOE に対応した以下の動作環境を必要とする。

- ・ パーソナルコンピュータ
- ・ オペレーティングシステム

判断の内容:

ST の前提条件は、TOE のセキュアな動作や運用に関わる事項のみを記載する。TOE が意図しない方法で使用されることにより、TOE がセキュアでない状態で動作し、資産が脅威にさらされる場合、前提条件として TOE の使用法や使用環境について記述すべきである。

前提条件「A.IT ENVIRONMENT」は、TOE のセキュアな動作や運用に関する内容ではなく、TOE を動作させるために必要な条件と考えられる。従って、前提条件「A.IT ENVIRONMENT」の内容は、TOE を動作させるために必要な動作条件として TOE に添付されるガイダンス文書などに記載される必要があるが、TOE のセキュアな動作や運用に関する内容として ST の前提条件に記述することは不適切と考えられる。

一般的に前提条件として記述する必要がないと考えられる例を以下に示す。なお、TOE の種別、使用法、使用環境などにより以下の内容も前提条件として適切な場合もあり、以下の内容を前提条件として記述することを否定するものではない。

例 2)

TOE 利用者は、TOE がインストールされていることを確認する。

この前提条件が守られない場合、単に TOE を利用することができないだけと考えられ、TOE のセキュアな動作や運用に関する内容を読み取ることはできない。

例 3)

TOE が動作するために必要なハードウェアやソフトウェアは、仕様どおりに動作する。

仕様どおりに動作しないハードウェアやソフトウェアを使用した場合、単に TOE が動作しないだけと考えられ、TOE のセキュアな動作や運用に関する内容を読み取ることはできない。

備考:

例 1)、例 2)、例 3) で取り上げた内容は、CC や CEM が要求している前提条件の内容とは明らかに異なるものであり、このような内容を前提条件として記述することは、ST 読者の TOE に対する正しい理解を妨げる可能性がある。例 1)、例 2)、例 3) のような内容が ST に記述されていても、評価として不合格になることはないが（当然、前提条件の記述内容が、ST 読者に理解不能な内容や矛盾した内容の場合は不合格になる）、ST の前提条件には、TOE のセキュアな動作や運用に関する記述のみを記載するように十分留意すること。

12. FAU_GEN.1 における、監査対象事象の妥当性について

問題の概要:

脅威や組織のセキュリティ方針に対応するために、TSF の制御下で発生するセキュリティ関連事象を記録する必要がある場合、TOE セキュリティ機能要件「FAU_GEN.1.1」を使用して監査対象の定義を行う。

FAU_GEN.1.1 TSF 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:

- a) 監査機能の起動と終了;
- b) 監査の[選択: 最小、基本、詳細、指定なし: から一つのみ選択]レベルのすべての監査対象事象; 及び
- c) [割付: 上記以外の個別に定義した監査対象事象]。

この時、b)の監査レベルとして「最小」、「基本」、「詳細」を選択した場合、各監査レベルに該当する監査対象事象が全て含まれていることの根拠は述べられているが、その監査レベルを選択したことの妥当性について十分に述べられていないSTが存在する。

判断の内容:

監査レベルの選択として「最小」、「基本」、「詳細」を選択した場合、各監査レベルに該当する監査対象事象を取得することによって、FAU_GEN.1.1 が対応するセキュリティ対策方針が満たされるという適切な正当化（選択した監査レベルの妥当性）を、セキュリティ要件根拠としてSTに記述すべきである。

また、監査レベルの選択として「指定なし」を選択した場合、FAU_GEN.1 c)で明示した監査対象事象を取得することによって、FAU_GEN.1.1 が対応するセキュリティ対策方針が満たされるという適切な正当化を、セキュリティ要件根拠としてSTに記述すべきである。

備考:

特になし。

13. TOE名称（TOE範囲）と製品名称の関係

問題の概要:

評価対象が製品の主要な機能を含んでいない、あるいは製品の一部のパッケージである場合でも、TOE 記述において TOE と製品との関係を述べていれば、TOE を管理・識別するための情報（一般的に TOE 名称と TOE バージョンとして記述される）として製品名称を用いても問題がないか。

判断の内容:

TOE と製品が同一でない場合、ST において物理的、論理的境界、評価された構成を含め消費者に対し適切に説明することが CEM で要求されている。一方 TOE 名称等については、ST 概説に ST が参照する TOE を識別するために必要な情報であることのみを要求しており、ST における評価範囲と TOE 名称についての関係を規定していない。

現在の JISEC 規程においては、運用上 TOE 識別情報と評価された IT 製品・システムの名称を区別しておらず、認証書をはじめ多くの公開情報が TOE 名称と TOE バージョンにより認証済み TOE を識別している。このため、TOE 名称に製品名称を用いた場合、消費者は ST の TOE 記述を読まない限り、その製品における評価範囲を知ることができず、また主要な機能やコンポーネントが評価対象であると誤解する恐れがある。

このため、本制度では、TOE を管理・識別するための情報を TOE 名称とバージョンであることを推奨するとともに、TOE の評価範囲と異なる TOE 名称（評価されていないその他のセキュリティ機能を含む名称等）を使用することは許容しないものとする。

また、TOE の一意な識別に用いるため、TOE 名称あるいはバージョンは、TOE の変更に伴い変更されるべきものであるとともに、TOE 以外の変更により影響を受ける可能性がないかについて注意を払うべきである。

備考:

CC の V3.1 においては、TOE 参照については、CEM の ASE_INT.1-4 にて以下のように規定されている。

製品のごく一部のみが評価された状況で、それにもかかわらず TOE 参照がそのことを反映していないということは許されない。 [ASE_INT.1-4 抜粋]

*ASE_INT.1-4 The evaluator **shall examine** the TOE reference to determine that it is not misleading.*

If the TOE is related to one or more well-known products, it is allowed to reflect this in the TOE reference. However, this should not be used to mislead consumers: situations where only a small part of a product is evaluated, yet the TOE reference does not reflect this, are not allowed.

14. OSPにおける暗黙の脅威の想定

問題の概要:

OSP (組織のセキュリティ方針) で示される TOE が従うべき規則、慣例またはガイドラインが、具体的な記述でない場合 (たとえば、特定のセキュリティ機能の実装を要求しているが、対抗すべき脅威レベルを規定していない場合や、セキュアな値の受け入れを要求しているが、具体的な強度に言及していない場合)、対応するセキュリティ対策方針や機能要件で攻撃能力や機能強度についてどのように言及すべきか。OSP において脅威が明示されていない場合に、ST 作成者は、それ以後のセキュリティ対策方針の記述にて、OSP をカバーするのに適切であれば、想定する脅威を述べてもよい。その場合、機能強度に関わる妥当性根拠については述べる必要はない。

判断の内容:

OSP に暗黙のうちに脅威が想定されていたり、OSP では規定されていない強度主張が OSP を根拠になされていることは、ST の読者にとって誤った判断を導く恐れがある。

ST のセキュリティ環境の脅威として明確に含むことができない場合を除き、脅威を含む OSP を用いることは不適切である [PP/ST 作成のためのガイド]。セキュリティ機能の強度やセキュアな値の特定は、脅威を想定することにより適切に決定することが考えられる。このような OSP は、極力セキュリティ環境の脅威として述べ、資産に対するセキュリティの側面を利用者に明示することが望ましい。

また、上記のような規則、慣行またはガイドラインが TOE に強制的に課せられている場合、ST 作成者は当該 TOE の運用環境を鑑み、機能の強度やパスワード長などを ST の読者に対し具体的あるいは決定可能な形で示し、その妥当性の根拠を述べる必要がある。OSP がいかなる脅威も想定していない場合、ST 作成者はその機能や値が特定の資産に対する特定の攻撃に対抗するものではなく、単純に要件として実装したことを明示的に読者に示さなければならない。

備考:

特になし。

15. 意図する使用法・使用環境を直接明示しない前提条件

問題の概要:

前提条件で、ST 作成者は消費者による具体的な TOE の使用法や使用環境を述べずに、除去すべき脅威やその原因を述べ、具体的対応を読者に任せるようなことは許されるか。

例： TOE がデュアルモード動作時に受信する TOE 管理要求のパケットは、想定しない管理プロトコル SID を持たない。

判断の内容:

前提条件に記されるべき事項は、CEM のワークユニット ASE_ENV.1-1 で述べられているとおり、消費者自らが意図する使用法が前提条件と一致していること、あるいは意図する環境が前提条件と一致していることを決定できる内容でなければならない。

具体的に消費者が意図する使用法や環境を満たせるのであれば、必要がない限りその結果として TOE が免れる脅威や脆弱性について前提条件で説明するべきではない。

上記の例において、対象とする消費者が前提条件から具体的対応が導き出せないと評価者が判断した場合、本ワークユニットは満たされない。また、前提条件を満たす具体的な使用法や使用環境が多様であり特定できない場合も、ワークユニット ASE_ENV.1-1 は満たされないと考えるべきである。たとえば、上記の例の前提条件から、下記のようないくつかの具体的対応を消費者が考えられるのであれば、そのいずれもが相互に矛盾あるいは ST の他の部分に不整合を招くものではなく、前提条件として適切なものとなることを保証しなければならない。また評価者は、消費者がその判断に迷わないことを決定しなければならない。

- ・ 外部ネットワークに接続された環境では TOE をデュアルモードで起動しない。
- ・ TOE をデュアルモードで起動する場合、FW において TCP あるいは先プロトコル番号が XXXX で、かつ XXX バイト目が 0x1 から 0x27 の範囲以外のパケットを遮断する。
- ・ TOE が接続されるネットワーク上のすべての端末は、TOE 対応クライアントソフトウェアがインストールされており、物理的に隔離され、端末管理者のみが操作できる状態にある。

備考:

「管理者は正しく管理する」という前提条件は、管理すべき項目や内容が明記あ

るいは参照されないかぎり、消費者に明確に理解されない場合がある。一方「管理者は不正を行わない」という前提条件に対し、評価者は消費者がいかなる具体的対応を特定したとしても、それらが前提条件に矛盾せず、また想定される消費者がTOEの対策方針に反する行為を不正な行為と明確に理解できることを決定することもできる。

16. FPT_STM.1 が適用可能なケース

問題の概要:

TSF がタイムスタンプを生成する際に、時刻を IT 環境から取得して使用している場合、FPT_STM.1(高信頼タイムスタンプ)は TOE の要件として使用できるか。

判断の内容:

TSF がタイムスタンプを生成する際に時刻を IT 環境から取得して使用している場合でも、FPT_STM.1 を TOE の要件として使用してよい。

CC Part2 の Annex(CC V2.3 Part2 J.13, CC V3.1 Part2 J.11)には、FPT_STM に関して以下のような説明が存在する。

*「高信頼タイムスタンプ」という用語の意味を明確にすること、及び信頼の受入れを決定する責任がどこにあるかを示すことは、PP/ST 作成者の責任である。
(CC V2.3 日本語訳より)*

つまり、FPT_STM.1 における「高信頼タイムスタンプ」の意味と信頼の受入れを決定する責任を CC は規定しておらず、PP/ST 作成者に委ねている。本問題の場合、「高信頼タイムスタンプ」の意味と信頼の受入れを決定する責任は以下のように定めればよい。

- 「高信頼タイムスタンプ」の意味は、特定のIT環境からインポートした時刻を確実にタイムスタンプとして利用することである。
- TSFは特定のIT環境からインポートする日時を全面的に信頼する。」

備考:

「高信頼タイムスタンプ」の意味や信頼の受入れを決定する責任を明確にすることが必要な場合は、以下のいずれかの方法で明確にすることができる。

- FPT_STM.1を詳細化することで明確にする。
- TOE要約仕様の、FPT_STM.1を満たすための箇所で明確にする。

特定の IT 環境が信頼できる時刻を提供することや、その時刻が一定以上の精度を持つことが脅威の除去に必要な場合は、そのことを前提条件に含めることでそのような脅威が除去されることを示すことができる。

本事例は CC V2.3, CC V3.1 の両方に適用する。

17. 動作環境の製品指定と動作確認保証について

問題の概要:

ST 概説の TOE 概要では、TOE が依存するソフトウェアやハードウェアを識別する。この識別において、TOE が直接依存しないレベルの記述を、商業上の観点から記述することは許されるか。またその場合に保証する動作の範囲はどのように変わるか。

たとえば、TOE が特定の OS の上で動くことが前提であるが、OS より下位のハードウェアには依存していない(TOE は OS のレベルのサービス、関数のみを使用している)場合、ST では、その OS に関する識別がなされていればよい。しかし OS が動作するハードウェアを自社製品などの具体的な商品を特定、羅列し、消費者に示すことはどのような意味があるか。

判断の内容:

TOE 概説では、消費者が TOE を使用するために必要なハードウェアやソフトウェアを判断するための十分な安全かつ詳細な識別を提供する必要がある。上記の例で特定の OS を示した場合、消費者は TOE がその特定の OS で動作することを保証したことを確信するが、OS が動作するハードウェアの選択については、消費者の判断であることを理解する。

一方、OS が動作するハードウェアのいくつかが具体的に ST で示されていた場合、消費者は、TOE の動作環境として、識別された OS およびハードウェアが必要であり、またそれらを含めた動作が保証されていることを確信する。

TOE の動作環境の条件として、必ずしも特定する必要がないが、商業上の理由から具体的な製品などを指定し消費者に示すことは可能である。ただし、その場合には指定されたすべての動作環境において TOE のテストがなされていなければならない。

評価においては、ASE_INT.1.6C で TOE に必須となるハードウェア、ソフトウェアの識別が ST でなされていることが検査され、ATE_FUN.1.2C でテスト環境と ST の、ATE_FUN.1.3C で TOE 構成と ST の一貫性が検査される。

備考:

関連する判断事例: [10. 「以上」や「シリーズ」を用いた動作環境の特定]