

平成 19 年 7 月 2 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

CC Version 3.1 の ST 作成および評価に関するお願い

第 2 版

表題の件につきまして、申請者及び評価者は、下記の事項に留意し ST 作成あるいは評価実施をしていただきますようお願いいたします。

- 記 -

CC Version 3.1 の評価基準または評価方法について、JISEC の運用として以下に示す ST 上の記載または評価の実施をすべてのケースにおいて必須としますので、注意をしてください。

1. CC 適合主張の翻訳版規格の記載

1.1. ST 上の記載

CC の翻訳版を用いる場合、同じ CC のバージョンに対し複数の版数が存在する可能性があるため、ST 作成者は ST 中の「CC 適合主張」の記載にて使用する翻訳版に対するバージョンの識別をする必要があります。

2007 年 4 月 18 日時点で公開されている翻訳版での記載例は以下のとおりです。

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

パート 1:概説と一般モデル 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版

パート 2:セキュリティコンポーネント 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版

パート 3:セキュリティ保証コンポーネント 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版

翻訳版の内容等が修正された場合、版数が更新されます。更新された場合、版数の取り扱いについてホームページ等に掲載します。CC 適合主張の記載も、申請時においてホームページ等を参照して有効な翻訳版の版数を用いてください。

1.2. 評価の実施

評価者は CEM の以下のワークユニットの評価において、翻訳版の識別について検査をします。

ASE_CCL.1-1 評価者は、STとTOEが適合を主張するCCのバージョンを識別するCC適合主張が適合主張に含まれていることをチェックしなければならない。

335 評価者は、このSTを開発するために使用されたCCのバージョンをCC適合主張が識別することを決定する。これには、CCのバージョン番号を含めるべきであり、また、CCの国際的な英語バージョンが使用されなかった場合は、使用されたCCのバージョンの言語も含めるべきである。

(解説)

CCの翻訳版を用いた場合、CCのバージョンを一意に識別する情報としてその翻訳版のバージョンの識別も含まれます。「使用されたCCのバージョンの言語」については、引用された翻訳版のバージョンの識別から明らかな場合、言語を特定して記載しなくても許容されます。

2. TOE 記述、TOE 要約仕様および SFR の対応

2.1. ST 上の記載

ST作成者は、TOE概要、TOE記述、TOE要約仕様及びセキュリティ機能要件(SFR)の対応がなされるようにそれぞれを記述する必要があります。このため以下のような、読者に誤解等を与えるような記述がないようにしてください。

- (1)ST中の「TOE記述」に、「TOE概要」に述べられていないTOEのセキュリティ機能を述べること。
- (2)TOE(あるいはそれを含む製品)のガイダンスやパンフレットにおいてTOEのセキュリティ機能として識別されている機能が、「TOE記述」で記載されているにも係らず、「TOE要約仕様」に示されない(つまり評価の対象とならない)こと。
- (3)「TOE要約仕様」に記述されているにもかかわらず、対応するSFRが示されないこと。

2.2. 評価の実施

評価者はCEMの以下のワークユニットに基づいて、それぞれ「TOE概要」、「TOE記述」、「TOE要約仕様」、SFRの一貫性評価を行います。

ASE_INT.1-11 評価者は、TOE 参照、TOE 概要、及び TOE 記述が相互に一貫していることを決定するために、その TOE 参照、TOE 概要、及び TOE 記述を検査しなければならない。

(解説)

ASE_INT.1-11 の検査では、TOE 概要に記述された以外のセキュリティ機能が TOE 記述に書かれていた場合、評価者は TOE 概要と TOE 記述の一貫性がないと判断します。

また、TOE 記述に明示的にセキュリティ機能が示されていない場合でも、TOE の論理的範囲内にセキュリティ要件が想定される(たとえば、TOE 記述から TOE がデータを保護する必要があると想定される)場合、評価者は TOE の消費者がそれらのセキュリティ機能を期待する必要がない合理的な理由が示されないかぎり、TOE 概要と TOE 記述の一貫性が満たされないと判断すべきです。

ASE_TSS.1-1 評価者は、TOE がどのように各 SFR を満たすかを TOE 要約仕様が記述することを決定するために、その TOE 要約仕様を検査しなければならない。

498 評価者は、セキュリティ要件のステートメントにある各 SFR に対し、その SFR がどのように満たされるかについての記述を TOE 要約仕様が提供することを決定する。

(解説)

ASE_TSS.1-1 では、SFR に結びつかない記述が TOE 要約仕様にも検査します。

3. 明確な組織のセキュリティ方針(OSP)の記述

3.1. ST 上の記載

(1)ST 中の「セキュリティ課題定義」に記述される OSP は、対応する SFR がその操作の完了も含め正当性を実証できる程度の明確な提示が必要です。

たとえば、OSP において「十分な強度」を持つことが提示されているが、対応する SFR において具体的な割付の値の正当性が示せない、あるいは特定できない場合は、OSP が明確でないことを意味します。TOE が従うべき規則に「十分な」と示されていた場合、ST 作成者は SFR までの詳細化の過程でその「十分な」ことの実証ができなくてはなりません。ST 作成者は、使用される環境や TOE の目的を加味し、

OSP の記述が SFR の「十分な」ことが実証可能かどうか明確であることを確認してください。

(2)ST 作成者は、「十分な強度」のような OSP が、暗に想定される脅威からでなく、TOE が課せられる規則やガイドラインから導かれたものであるかを十分吟味すべきです。

もし、TOE が対抗すべき脅威であれば、OSP としてではなく脅威として ST で記述されるべきです。また、それらの OSP が特定のセキュリティ規則や脅威にも係らない場合、ST においてそれらの OSP を述べる必要があるか（ST の読者に有用であり、誤解を与える冗長なものではないか）を検討する必要があります。

安易な OSP を規定することで、それを実現する SFR の実施を損なう脆弱性により評価が不合格となることがあります。

3.2. 評価の実施

評価者は CEM の以下のワークユニットにおいて、セキュリティ対策方針が OSP を実施すること、セキュリティ対策方針根拠が、SFR がセキュリティ対策方針を満たすことについて、セキュリティ要件根拠が実証していることを検査します。

ASE_OBJ.2-5 評価者は、各 OSP について、セキュリティ対策方針がその OSP を実施するために適していることをセキュリティ対策方針根拠が正当化していることを決定するために、その根拠を検査しなければならない。

ASE_REQ.2-11 評価者は、TOE の各セキュリティ対策方針について、SFR がその TOE セキュリティ対策方針を満たすために適していることをセキュリティ要件根拠が実証することを決定するために、そのセキュリティ要件根拠を検査しなければならない。

(解説)

ASE_OBJ.2-5 で、各セキュリティ対策方針が、その OSP を実施するのに十分であり、各セキュリティ対策方針が OSP の実施に寄与することを決定します。

ASE_REQ.2-11 において、評価者は各 SFR が、そのセキュリティ対策方針を十分満たしていることと、各 SFR がセキュリティ対策方針の達成に不可欠であることを決定します。セキュリティ対策方針は、SFR の必要性及び十分なことが判断できる記述でなければ、評価は不合格となります。

評価者は、これらのワークユニットで OSP から SFR までの詳細化の過程で不要な

条件が紛れ込んでいないこと、すべての条件が SFR から OSP へさかのぼれることを
検査します。

ASE_SPD.1-3 評価者は、セキュリティ課題定義が OSP を記述していることをチェック
しなければならない。

384 評価者は、各 OSP が明確に理解できるように十分な詳細が説明及び/
または解釈が行われていることを決定する。セキュリティ対策方針の追
跡を許可するために方針ステートメントの明確な提示が必要である。

(解説)

セキュリティ対策方針や SFR の十分なこと及び必要性が実証できない場合、それらに関連する OSP が曖昧性を含んだまま記述されていることがあります。評価者は、セキュリティ対策方針や SFR の対応で矛盾を生じた OSP の記述が、明確に理解できる十分な詳細をもって説明されているかを、ASE_SPD.1-3 のワークユニットでチェックします。

OSP を実現する SFR の脆弱性分析は、脅威に対抗する SFR に対するそれと同等に扱われなくてはなりません。OSP から詳細化された SFR が、TOE の運用環境で侵害される可能性について、評価者は十分な検証が必要です。

以上

改版履歷

2007年6月6日 第1版

2007年7月2日 第2版 3章追加