PP を用いない認証申請における

TOE 決定に係る指針

第 2.0 版

本「TOE 決定に係る指針」は、IT セキュリティ評価及び認証制度(JISEC)において評価を行うにあたり、評価対象(TOE)の範囲を決定する際、どのようなことに留意すべきかについて述べたものです。また本制度として、関連する評価手法において評価対象の範囲の適切性をどのように判断するかにも言及しています。

本指針は、特に PP を用いない評価において、申請者が自ら TOE の範囲を決定する際の範囲の妥当性の検討、及び ST 作成者が ST を作成する際の TOE 調達者である ST 読者に関する記述の妥当性の確認のための指針として用いることを目的としています。

IPA 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　　2014 年 4 月 7 日発行

目次

はじめに

国際セキュリティ評価基準 CC(Common Criteria)に基づくセキュリティ評価では、セキュリティ要件は調達者(一般的には政府機関)が作成した PP(Protection Profile)により指定され、その要件に基づき IT 製品の評価が行われます。一方、JISEC では調達者が要求仕様を示さず製品開発者自らが仮想的に要件を決定し、独自の ST を作成するような評価も、調達基準の整備の過渡期(政府 PP 提供の立ち遅れ)として認めてきました。このような PP を用いない評価の場合でも、開発者は調達者の要件を想定し、評価対象(TOE)の範囲やセキュリティ機能が、TOE の調達者にとって意味がありかつ明瞭であるように決定をすることが前提となります。

セキュリティ評価の出発点として、TOE が明確に特定される必要があります。また、この TOE の範囲はセキュリティターゲット(ST)によりその読者（つまり開発者が提供する TOE の「調達者」であり、その TOE が提供するセキュリティ機能の利用者である「消費者」）に正しく認識される必要があります。TOE 範囲の特定や、ST 上での TOE 範囲の記述が曖昧であるために、評価の過程で TOE の開発者および評価・認証者との認識が異なり、多くの工数がその誤解を解くために無駄に浪費されることがあります。また TOE の消費者が、期待するセキュリティ機能が評価の対象となっているかを ST から正確に判断することが困難な場合、本制度の意図するセキュリティ評価の目的は達成されません。

上記の主な原因として、「評価の対象となる製品と評価の範囲」、「製品の主要なセキュリティ機能と評価対象のセキュリティ機能」、「TOE の消費者と ST の読者」、「TOE 名称と TOE の実態」それぞれの乖離が挙げられます。これらの観点から、TOE 範囲の決定や ST における TOE の記述において留意すべき事項をまとめています。

1. TOE と製品

TOE の物理的範囲と製品が一致することが基本となります。製品の一部を TOE 範囲とすることは、独立しかつ相互に影響しない完結した機能性[1]の範囲で評価する場合を除き、消費者にとって評価保証の意味が希薄となります。たとえば、ファイアウォール製品においてユーザインタフェースを含めた NAT 機能全体を評価することは、NAT のみを用いる消費者にとっては有用です。一方、フィルタリングモジュールの一部のみを評価することは、そのモジュール以外の評価されない部分も含めたフィルタ

[1] 本書では、ひとつあるいは複数のセキュリティ機能の組み合わせにより達成される利用者に提供する最小単位のセキュリティサービスを示す。

リング機能を利用する消費者にとって、なにがその評価によって保証されたのか判断できません。

実際には、個々の機能性に対する操作（管理や設定）がお互いのセキュリティ機能に影響し合わないことはほとんどありません。このことから、本制度では開発者の責任範囲全てを含む「製品」を TOE の範囲とすることを基本とします。製品の一部を評価の対象とする場合には調達者にとってどのような評価保証を与えることができるかを ST において論証できない場合、制度として申請を受け付けません。「製品」とは、TOE の外部インタフェースの利用者から見た TOE を含む認識可能なひとつの単位であり、多くの場合商業上の作成された調達可能な商品を示します。

特定の商品のための部品として開発サイト間で取引される「製品」を示す場合もあります。この場合の消費者とはその TOE を部品として利用し商品を開発する開発者であり、ST の読者もこの開発者となります。最終的な商品の利用者は、ここには登場しないことになります。

このような特殊なケースとしては、調達者が既存の特定用途向け IC カード上にのる新機能を実現するファームウェアを調達する場合であり、最終的には IC カードとの連携を想定したコンポジット評価と呼ばれる形式です。

繰り返しとなりますが、消費者は購入した製品を利用する際に、一般的に製品の内部の個々の部品やモジュールの設計や役割を意識することはありません。つまり、開発者側が提供する製品の特定の部品やモジュールのみを評価範囲としても、消費者が利用するセキュリティ機能性が評価対象外のその他の部品やモジュールを使用するのであれば、このような評価は消費者にとってなんら保証を与えないことになります。本制度では、消費者にとって意味のあるセキュリティ評価を推進する観点から、TOE 範囲を製品の一部ではなく製品全体とすることを推奨しています。

上記とは逆に、開発者が自ら提供するセキュリティ機能を超えた範囲を TOE としてはなりません。より正確に言うならば申請者は、自らの責任範囲(主張した評価保証レベルで保証可能な範囲)を超えてセキュリティ機能性を保証するような TOE 範囲を設定してはなりません。TOE の動作環境に必須な製品等が評価するセキュリティ機能の一部を担うのであれば、その評価されるセキュリティ機能の範囲（つまりどこまでが TOE として責任を持ち、どこからが環境が実施しているか）を開発者は明確にして評価に臨む必要があります。責任範囲とは、評価の時にその評価保証レベルを満たす証拠資料等を提供でき、かつ評価における懸念事項に対応できることを意味します。また、調達者が TOE とそれ以外の動作環境のそれぞれの製品調達の境界が識別できるという重要な側面もあります(3.1 章参照)。

2. TOE とセキュリティ機能性

TOE に含まれるセキュリティ機能性については、すべてセキュリティ評価の対象となることが望まれます。その製品の主体的セキュリティ機能と考えられるにもかかわらず、評価の対象からはずれている機能性が存在すること、特に TOE が提供する機能性から当然期待されるセキュリティ機能が評価の対象とならないことは、消費者の誤解を招くとともに、消費者にとって評価保証の意味が希薄となります。たとえば、ファイアウォール製品において、パケットやプロトコルフィルタリングに関する機能は評価対象とせず管理機能（フィルタリング設定等）のみを評価対象とするケースなどです。

本制度では TOE の論理的範囲において、セキュリティ機能要件として表すことのできる機能性すべてを、評価の対象のセキュリティ機能とすることを推奨しますが、特に想定する消費者が期待するセキュリティ機能性については、評価の対象としてください。

これってセキュリティ機能？

CC の評価で対象となるセキュリティ機能の「セキュリティ」とは、一般的に機密性（Confidentiality）、可用性（Availability）、完全性（Integrity）を維持することをいいます。さらに否認防止性(Non Repudiation)、責任追跡性(Accountability)、真正性(Authenticity)などを含めることもあります。これらの多くは CC part2 の機能要件パッケージとして用意されていますので、こられの要件に合致すればセキュリティ機能といえます。しかし、既存の要件に合致しない要件があった場合、既存の要件の解釈を無理に曲げずに新たな要件を考案しましょう。ここで気をつけていただきたいのは、セキュリティ機能としての要件と設計上や実装上の論理的な特性[2]とを混同しないことです。また、セキュリティ機能を呼び出すだけ、セキュリティ機能の結果を加工するだけといった範囲を TOE としたとき、そこには先述のような「セキュリティ」とよばれる特性はありません。またセキュリティ機能が他のプロセスから干渉されたりバイパスされたりせずに呼び出されるという類の概念は、TOE の設計によって達成されるべきすべてのセキュリティ機能に必要な特性です。このような特性は ST で示される明示的なセキュリティ機能とは別に、開発証拠資料などをもとに共通的に評価される事項です。

TOE のセキュリティ機能性を実現するためのいくつかの支援的な機能が、TOE の論理的範囲外に依存する場合があります。その場合も、セキュリティ評価の意義から、

[2] 調達要件では、具体的な暗号アルゴリズムやプロトコルを指定することもある。

少なくともセキュリティ機能要件の実施機能はTOEが保持していなければなりません。たとえば、実際のセキュリティ機能要件を実現している TOE 外の関数(SSL ライブラリ等)を呼び出し、その結果を加工するような機能を実現している範囲のみを TOE とした場合、TOE はセキュリティ機能要件(セキュア通信等)を実施しているとは言えません。これは TOE として評価すべきセキュリティ機能ではなく、あるいは TOE の範囲が不適切と判断できます。

TOE のセキュリティ機能を支援するための機能 が TOE 外にある場合は、一般的には TOE 動作に必要な環境とされ、調達者が独自にそれらを調達することになります。これらの支援機能が、開発者が提供する製品内にあり TOE とともに提供されるような場合、この支援機能も評価範囲として含まれなければなりません。開発者自らが提供する製品のセキュリティ機能性を構成する一部の機能だけを評価しても、最終的なセキュリティ機能性の利用者には意味のない評価となるためです。

ただし、TOE のセキュリティ機能と TOE 外の支援機能間のインタフェースが可視的であり、かつ調達者がその支援機能を含む部分（製品）を調達者の責任で調達できる場合は、分離した評価も可能な場合があります。セキュリティ機能性の実現に直接係るセキュリティ機能実施部とそれらの支援部が分離可能であるということは、その間のインタフェースが完全に公開され、支援機能の交換が可能（調達あるいは自製が可能）ということです。汎用的なよく知られた製品(well-known products)として認知されている OS などがこの例になります。

一方、セキュリティ機能性の支援機能を提供する組み込み OS に依存するアプリケーションを評価する場合、そのセキュリティ機能性の利用者は組み込み OS を自分の責任において選択し、調達することができません。このような場合、評価範囲をアプリケーションのみとすることはできません。支援機能を開発者自身が提供する場合でも、それらがオプション製品に搭載されており、その製品を用いるインタフェースが公開されている場合（XY 標準準拠・W99API 完全互換など）、調達者は自製を含め他の選択が可能となるため、これらの支援機能を前提とした評価をすることができます。現実的には、製品開発者が第三者の提供する支援機能製品等をサポートしていなかったり、非公開の独自インタフェースが存在していたりするため、提供するすべての機能を TOE 範囲とすることがほとんどとなります。

3. TOE と ST 読者（ST における記述）

TOE の範囲を決定すると、TOE の利用者が規定され ST の読者が決定されます。多くの場合、ST の読者は TOE の消費者であり具体的には政府機関の調達者となります。

ここでは、決定したTOEの範囲に対して、STが本来のTOEの消費者に向けて書かれていないために、ST評価のみならずその後のTOE評価においても多大な時間とコストが費やされた事例から、注意すべきSTでの記述について示します。

3.1. 評価外の機能や環境の記述

TOEの範囲に係らず、評価対象とならないセキュリティ機能をTOEの論理的範囲に含めるような記述をSTで行なってはいけません。ST上の具体的な記載としては、

- 「TOE概要」には、評価されるセキュリティ機能性に係らないセキュリティ機能を述べることは許されない。
- 「TOE記述」には、「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は許されない。
- 「TOE記述」で記載しているセキュリティ機能が「TOE要約仕様」で述べられていないことは許されない。
- 「TOE要約仕様」の記述に対応するセキュリティ機能要件がないことは許されない。

評価されているセキュリティ機能性は、「TOE概要」、「TOE記述」、「TOE要約仕様」およびセキュリティ機能要件で一貫していなければなりません。

STにおいて評価されないセキュリティ機能性の説明を含めることは、ST読者に対しあたかもそのセキュリティ機能が保証されているかのような誤解を与えるおそれがあります。多くの場合、評価されないセキュリティ機能性は、評価対象とは独立し、影響を与えないセキュリティ機能により構成されているはずであり、STでの説明を不可欠とする必要はないはずです（もし、評価されないセキュリティ機能性について言及しなければ、評価対象が理解できないのであれば、TOE範囲の決定に問題がある可能性が大きいことになります)。にもかかわらず、評価されないセキュリティ機能性をSTに記述するのであれば、開発者がST読者に対し評価されていないその他のセキュリティ機能においても保証が与えられているような誤解を意図的に与えようとしていると理解されてもしかたがないでしょう。

同じようなことは、製品構成や評価構成についてもいえます。製品としてサポートしている多くの構成がSTに記述されており、実際に評価された構成あるいは認証の対象となる構成や環境が曖昧となるような場合、セキュリティ基本設計書としてのSTの目的は達成されません。ST作成者はSTにおいて不要な製品説明の記述を避け、ST読者に評価された対象が明確に伝わるよう実直に記載しなければなりません。

本制度では、消費者にとって意味のあるセキュリティ評価を推進する観点から、TOE が提供する機能性に含まれるすべてのセキュリティ機能については ST 上にセキュリティ機能要件として規定し、評価の対象とすることを強く推奨しています。ただし、ST 上に示されないセキュリティ機能性の存在により（それが評価対象のセキュリティ機能性とはまったく独立し、ST 読者が製品種別から期待するセキュリティ機能ではなく、評価対象外として ST 読者に理解されるかぎり）、評価を否定するものではありません。

3.2. 製品部品としての TOE の記述

TOE が製品やシステムの一部（XXX モジュールや XXX 機能など）であるにもかかわらず、ST ではその TOE を含む製品やシステムの最終利用者に対する説明を記述することは、ST の読者に TOE の範囲に混乱をもたらします。

この場合 ST では、その TOE の実際の利用者、つまりその TOE を用いて製品やシステムを開発する開発者に対する説明を記述しなければなりません。TOE が製品の一部である場合、当然「TOE の外部インタフェース」と「製品の利用者インタフェース」には乖離があります。それにも係らず、ST において製品の利用者インタフェースをあたかも TOE の外部インタフェースのように記述してはなりません。一般的には TOE がどのようにそれらの製品で扱われるかは TOE 評価の範疇ではありません。よって ST 作成者は、TOE が使われる最終製品の利用イメージを ST に含めることは極力避けるべきです。開発者の責任範囲が製品をカバーできないにも係らず、ST の記述として製品の利用形態から TOE の説明をすることは、セキュリティ評価として無保証の部分をも保証されていると ST の読者に偽ることになりかねません。

TOE が特定の製品の一部品であり、製品のセキュリティ機能性実現の一部を担う場合、製品の利用を TOE の利用として扱えるのは以下の 1.と 2.が満たされた場合のみです。

1. TOE の外部インタフェースが製品の利用者インタフェースと同じである。
   （あるいは TOE の外部インタフェースと製品の利用者インタフェースの対応が自明であり、その間の一切の改ざんや干渉から免れることが、前提条件や運用環境から明確である場合）
2. 製品のセキュリティ機能が、すべて TOE のセキュリティ機能要件により実施されている場合。

上記 1.のインタフェース間の対応が自明であるとは、論理的処理を伴わないハードウェア(ボタンなど)を介する場合などが考えられます。しかし多くの場合、製品インタフ

ェースの入力を論理的に処理した結果が TOE の入力となるため、製品インタフェースを TOE と同等と扱うことはできないでしょう。

過去には、TOE を含む最終製品のマニュアルを TOE 評価の証拠資料として提出するものがありましたが、これは TOE の証拠資料が明らかに欠落しているか、認証取得の便宜上、TOE 範囲を無理に狭めたことに起因するものです。このような認証製品について、本制度では政府調達の対象として推奨しません。

4. TOE 名称

TOE の名称（ST では「TOE 参照」の項で記述される）には、その TOE が関連する製品名称を反映することができます。TOE の名称は、TOE とその製品との関わりが消費者に正しく伝わるように定義しなければなりません。

特に TOE 範囲と製品が一致しておらず、TOE が製品の一部のセキュリティ機能性しか対象としていないような場合(制度としてはそのような製品の部分的なセキュリティ機能性を TOE とすることを推奨していません)、製品全体あるいは TOE 以外のセキュリティ機能性が評価されたと誤解させないよう、TOE 名称で製品との関連を明確に示す必要があります。

ST 作成者は、TOE 参照として使用する TOE 名称に製品名称を用いる場合、製品カタログやマニュアルなどの記述から読者が想定する TOE の範囲やセキュリティ機能性と、実際の TOE の範囲やセキュリティ機能性が異ならないことを保証しなければなりません。

TOE 範囲確認チェックリスト

PP 適合ではない ST で申請する際は、このチェックリストを用いて TOE 範囲を確認してください。

□	TOE と製品は一致しているか。
□	TOE と製品が一致していない場合、 ・調達者が TOE 境界と製品を明確に区別でき、かつ ・消費者にとって意味のある TOE 範囲となっているか。
□	TOE に評価対象とならないセキュリティはないか。 製品カタログやマニュアルに掲げられたセキュリティ機能はすべて評価されるか。
□	TOE に評価対象とならないセキュリティがある場合、 ST の「TOE 概要」「TOE 記述」に対象となるセキュリティについて明確に調達者に伝えているか。
□	TOE の外部インタフェースが製品のインタフェースの場合、 TOE 開発者は製品のインタフェースまで責任を負うか。
□	TOE の外部インタフェースが製品のインタフェースでない場合、 ST で製品の消費者と TOE の消費者を混同していないか。
□	セキュリティ機能性はすべて TOE の範囲か。
□	セキュリティ機能性のすべてが TOE の範囲ではない場合、 ・TOE で実施される機能はセキュリティ要件として定義ができ、かつ ・TOE と TOE 外のセキュリティインタフェースは可視的か。
□	TOE の名称が製品名を引用している場合、 ・調達者は名称から TOE と製品の関係を理解でき、かつ ・製品カタログやマニュアルの内容と異ならないか。