住民基本台帳カード Version 2
組込みソフトウェア
プロテクションプロファイル

第1.00版

2011年1月21日

LASDEC 財団法人 地方自治情報センター
Local Authorities Systems Development Center

株式会社電子商取引安全技術研究所

認証番号: C0284

(空白ページ)

このPPについて

PPの背景とPPを満たす住基カード製品開発について説明する。

次世代の住民基本台帳カード

住民基本台帳カード (以下、「住基カード」という) は、住民基本台帳ネットワークシステムで使用するICカードである。

本人確認の円滑化にとどまらず、公的個人認証サービス、条例利用など、多目的の公的ICカードとして利用されている。

平成15年の住基ネット二次施行で交付が開始されており、住民基本台帳カードType I (以下、「Type Iカード」という) 、住民基本台帳カードType II (以下、「Type IIカード」という) の2種類の仕様を規定している。

住民基本台帳法の一部を改正する法律 (平成21年7月15日公布) により、他の市町村へ住所を移した場合でも引き続き住民基本台帳カードを使用することができるようになったこと、Type Iカード、Type IIカードで実装されている暗号アルゴリズムのセキュリティ強化、新たな行政サービスへの拡張性向上等の対応として、住民基本台帳カードVersion 2として次世代の住基カード仕様書を策定した。

住基カードのセキュリティ要件

本PPでは、住基カードVersion 2の組込みソフトウェアに対するセキュリティ要件を規定する。住基カードVersion 2は、セキュリティ評価の国際規格であるCC (Common Criteria; ISO/IEC 15408規格と同一) に基づいて評価し、適切なセキュリティ対策が施されていることを確認する。住基カードの開発・製造者は、本PPの要件をすべて満たす住基カードを提供しなければならない。

住基カードのセキュリティ評価

住基カードは、プラスチックカードの中にICチップ、無線アンテナ (非接触通信用) 、ソフトウェアが搭載され、ハードウェアとソフトウェアが一体化された製品である。住基カードのセキュリティ評価は、製品全体を評価対象として実施することとなろう。

製品全体を評価する際、ソフトウェアを搭載するハードウェア部分が既に評価済みの場合と、未評価の場合の二つのケースがある。前者の場合、コンポジット評価と呼ぶ評価手法を適用できる。これについては、次節「コンポジット評価」で説明する。

後者の場合、製品全体をTOEとし、住基カードが満たすべきセキュリティ要件を明らかにした新たなSTを作成しなくてはならない。本PPは、住基カードのソフトウェアに関わるセキュリティ要件だけを規定するので、本PPでカバーしないセキュリティ要件の追加が必要である。

製品に対するSTは、本PPに準拠するため、本PPの要件をすべて満たさねばならない。さらにハードウェアで対応すべきセキュリティ要件と、ハードウェア・ソフトウェアの協働で実現するセキュリティ機能のソフトウェア側追加要件を含めねばならない。このSTが満たすべき評価保証レベルは、本PPの評価保証レベルと同等か、それ以上のものでなければならない。

住基カード製品としてハードウェアを評価対象に含めることで、ハードウェアに関わるセキュリティ上のリスクを考慮しなくてはならない。このリスクとは、ハードウェアに関わる物理的特性を利用し、ソフトウェアで実現したセキュリティ機能の正常な動作を妨害しようとする攻撃である。例えば、ICチップの消費電力変化を観測して暗号演算を分析し、演算に使用された秘密鍵を暴露する、ICチップ内部を物理的に操作し、ソフトウェアのセキュリティ機能をバイパスして秘密データにアクセスする、などの攻撃がある。これらの攻撃から、住基カード内の情報資産を保護しなくてはならない。

コンポジット評価

ソフトウェアとハードウェアを一体化した住基カード全体のセキュリティ評価を実施する際、ハードウェアであるICチップ部分のセキュリティ評価が実施済みなら、コンポジット評価を適用し、評価の重複部分を省略できる。

コンポジット評価は、セキュリティ評価基準のCCを提供するCCRA (The Common Criteria Recognition Arrangement) が発行する補助文書によって規定される。その評価結果は、CCRAに加盟するすべての制度下で有効である。コンポジット評価への対応を以下に説明する。

住基カード全体に対するセキュリティ要件への対応は、以下のように分類される。

(a) ハードウェア単体のセキュリティ機能で対応

(b) ソフトウェア単体のセキュリティ機能で対応

(c) ハードウェアとソフトウェアの組み合わせによるセキュリティ機能で対応

(a) に相当する部分は既に評価済みなので、(b) と (c) に該当する部分を評価すれば、住基カード全体に対するセキュリティ機能を評価したことになる。(b) に対するセキュリティ要件は、本PPに規定される。 (c) に関わるセキュリティ要件は、両者を組み合わせたことであらたに発生するものである。

(c) に関わるものは、主として、物理的特性に関わる攻撃に対し、ソフトウェアの機能を併用して対処する場合に生じる。例えば、消費電力分析による秘密鍵暴露攻撃に対し、ソフトウェアの暗号演算手順を工夫して消費電力変化を減少させるような対処である。あるいは、乱数生成において、物理的生成とソフトウェアによる決定論的生成を組み合わせるハイブリッド方式で対処するかもしれない。これらは、ICチップ仕様とソフトウェアのプラットフォーム部の実装に依存するので、住基カード開発者が具体的な対処方針を選択することになる。

コンポジット評価の適用にあたり、ハードウェア評価を実施したスキーム (国ごとのCC評価・認証制度) とコンポジット評価を実施するスキームが異なるケースでは注意が必要である。コンポジット評価では、評価済みハードウェアに対するST及びST・TOE評価の詳細情報 (評価報告書) が必要になる。ハードウェア評価・認証を実施した評価機関及び認証機関から必要な情報提供を受けられるよう、事前調整が必須である。

コンポジット評価の詳細は、上記CCRAが公開する補助文書を参照されたい。ICチップの物理的特性を利用する攻撃も、この文書で具体的に提示される。

目次

1 PP概説

1.1 PP参照

タイトル: 住民基本台帳カード Version 2 組込みソフトウェア プロテクションプロファイル

版数: 1.00

発行: 2011年1月21日

発行者: 財団法人 地方自治情報センター

作成者: 株式会社 電子商取引安全技術研究所

登録: C0284

キーワード: ICカード、住民基本台帳、住民基本台帳ネットワークシステム、住基カード

1.2 TOE概要

1.2.1 TOE種別

TOEは、ICカードに搭載される組込みソフトウェアである。プラットフォームとして動作する基本ソフトウェア部分と、TOE固有のアプリケーションプログラム (以下、「AP」という) である住基APから構成される。

1.2.2 TOEの用途と主要セキュリティ機能

TOEは、住民基本台帳カード (以下、「住基カード」という) 内のICチップ上で動作する、住基カード向け組込みソフトウェアである。住基カードを媒体としてサービスを提供するシステムは、住民基本台帳ネットワークシステム (以下、「住基ネット」という) と呼ばれる。住基カードは、住基ネットにおける主要構成要素の一つである。住基カードの利用者は、居住地の市町村から住基カードを交付され、住基ネットのサービスを受ける際に住基カードを使用する。

TOEは、プラットフォームと、その上で動作する住基APから構成される。住基APは、住基カード発行主体であるすべての市町村に共通するAPであり、すべてのTOEに搭載される。プラットフォームには他のAPを追加搭載できるが、住基AP以外のAPは、TOEの構成要素に含まれない。

追加搭載されるAPの例は、券面事項確認AP、公的個人認証サービスAP、あるいは住基カード発行者である市町村の条例に基づくものなどである。それ以外のAPも、住基カード発行者によって追加搭載できる。AP搭載は、開発フェーズで実施されることもあり、住基カード発行者へ納入後、発行者の管理下で行われることもある。すべてのAPの搭載は、セキュアな環境において、正規の権限を持つ者の管理下で実施される。権限を持たない者が任意にAPを追加することはできない。

TOEには、利用者データ保護のためのセキュリティ機能が備えられる。TOEが持つ主要なセキュリティ機能は、以下のようなものである。

- 通信チャネル保護　住基カードと外部装置間の通信チャネルを盗聴・改ざんから保護する機能。プラットフォーム部及び住基AP部のそれぞれが通信チャネル保護機能を持つ。
- 相互認証　住基カードと通信相手の外部装置の双方において、互いに相手が適正なものであることを確認する機能。プラットフォーム部及び住基AP部のそれぞれが相互認証機能を持つ。 (相互認証機能のうち、外部装置がTOEを認証する機能は外部装置のセキュリティ機能であり、TOEのセキュリティ機能に含まれない。)
- カード保持者の本人確認　住基カードを保持する者が正しい保持者であることを確認する機能。住基APの機能であり、TOEに追加搭載される他のAPからは利用できない。
- 格納データの保護　TOEの管理下にある格納データを不正な攻撃から保護する機能。プラットフォーム部及び住基AP部のそれぞれが格納データ保護機能を持つ。

TOEは、住基カードに埋め込まれたICチップ上で動作する。ICチップを含むハードウェアは、TOEが動作するために必要なIT環境であるが、TOE範囲外である。TOEの動作に必要なIT環境は、以下のものである。

- ICチップ　ソフトウェアであるTOEを動作させるICチップ。本PPでは、特定のICチップを指定しない。

  [注釈]　住基カード全体のCC評価が行われる場合、評価対象は、本PPが規定するソフトウェア部分のTOEに加え、ソフトウェアの動作に必要なハードウェアを含むものになると想定される。プラスチックカードに通信アンテナとともにICチップが埋め込まれ、ICチップには、本PPの要件を満たすソフトウェアが搭載される。

住基カード全体の評価では、まずハードウェア部分を独立して評価[1]し、次のステップでソフトウェアを含む住基カード全体を評価する、コンポジット評価が適用されるかもしれない。ICカードを対象とするコンポジット評価では、CCRAが定める補助文書[2]が使用される。

コンポジット評価に適用される評価保証レベルは、本PPが要求するものと同一である。一方、コンポジット評価に使用されるハードウェア部分は、本PPが要求するのものと同一かそれ以上の評価保証レベルで評価・認証されたものでなければならない。

コンポジット評価を適用せず、ハードウェア、ソフトウェアを含めたものを一つの製品として評価することもできる。この場合も、評価される対象がICチップであるから、評価において、CCRAが定める補助文書(コンポジット評価の文書を除く) が適用される。

- 通信アンテナ　ICチップが外部装置と非接触通信を行う際に必要。ICチップに外付けされ、ICチップとともにプラスチックカードに埋め込まれる。
- プラスチックカード　住基カードの仕様を満たすプラスチックカード。表面に外部接続電気端子を持つ。住基カードとしての必要事項が券面に印刷される。

---

[1] ICチップハードウェアのPPとして、 “Security IC Platform Protection Profile Version 1.0 15.06.2007 BSI-PP-0035” が広く使用されている。このPPは、評価保証レベルをEAL4+（追加保証要件は、ALC_DVS.2とAVA_VAN.5）としており、本PPのTOE（ソフトウェア）を搭載するICチップハードウェアのセキュリティ要件定義に使用できる。

[2] CCDB-2009-03-001: Application of Attack Potential to Smartcards, March 2009, Version 2.7 Revision 1

CCDB-2009-03-002: The Application of CC to Integrated Circuits, March 2009, Version 3.0 Revision 1

CCDB-2007-09-001: Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0 Revision 1

1.2.3 TOEの構成

図1-1にTOEの構成を示す。TOEは、ICチップ (ハードウェア) 上で動作するソフトウェアであり、プラットフォーム部と住基AP部の二層で構成される。

プラットフォームは、APの実行環境を提供する。複数のAPが搭載される場合、プラットフォームは、各APの実行領域を分離し、AP間の相互干渉を防止する。APとプラットフォームの動作領域も分離され、APからプラットフォームへの干渉が防止される。前章で記したとおり、住基APはプラットフォーム上に初期搭載され、TOEの一部となる。

図1-1には、TOEを構成するプラットフォームと住基APのほか、追加APが示される。追加APはすべての住基カードに共通のものではなく、TOE構成要素に含めない。追加APの例は、券面事項確認AP、公的個人認証サービスAP、市町村の条例に基づいて追加搭載される条例利用APなどである。

追加APは、住基カードを発行する市町村によって、それぞれ異なるものを搭載できる。TOE製造時に搭載されることもあり、TOEの運用環境で搭載されることもある。TOEの運用環境におけるAP追加搭載は、TOEプラットフォーム部の管理機能の制御下で行われる。

すべてのAP、すなわち住基APと追加APは、プラットフォーム上のプロセス (TOE内プロセス) として動作する。プラットフォームと住基APの一部がTSFを構成する (図1-1にTSFは表示されていない) 。追加APはTOEの構成要素ではないが、運用環境における追加APの搭載・削除・実行・終了等は、TSFの制御下で実行されるTOE内部の動作である。図1-1に示すTOEの境界は、TOE構成要素の範囲ではなく、TSFの制御範囲を示すものである。

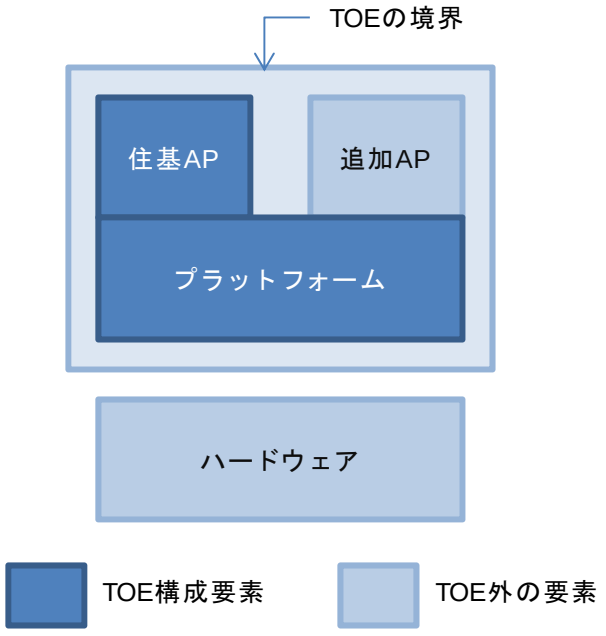

図1-1 TOEの構成

1.2.4 TOEのライフサイクル

TOEのライフサイクルは、以下のように定義される。ここに示す定義は、本PPにおけるTOE説明の一環として示すものであり、開発方法特定などの意図を持つものではない。本PPを参照してPP/STを開発する者は、本節の記述に関わらず、実際の環境に応じたライフサイクル記述を行うことができる。

(1) ICチップ (ハードウェア) 開発

ICチップ開発者によって、住基カードに埋め込まれるICチップが開発される。ICチップ製造に使用されるフォトマスク開発、ICチップ専用ソフトウェア/ファームウェア開発もこの工程に含まれる。本PPでは、ICチップ開発は評価範囲に含まれない。しかし、住基カード製品の評価においては、これらの開発に携わる者は、すべて開発者に相当する。これらの開発環境に対し、本PPのTOEに対するものと同等の高レベルの攻撃に対抗する開発セキュリティが要求される。

ICチップへのソフトウェア組込み (ソフトウェア開発は、(2) に示すフェーズで行われる) は、このフェーズか、あるいは (3) のフェーズで実施される。

ハードウェア開発に関わるこのフェーズでは、開発が複数サイトに分散することが多い。ハードウェア回路設計、ICチップ製造のためのマスク設計・製造、ICチップ製造など、多様な工程が各所の開発サイトで実施されるかもしれない。

(2) TOE (プラットフォーム及び住基AP) 開発

本PPのTOEに相当するソフトウェア (プラットフォーム及び住基AP) が開発される。これらソフトウェア開発は、(1) に示すハードウェア開発と独立して行うことができる。

(3) 住基カード製造

本PPのTOEに相当するソフトウェアがICチップに埋め込まれ (あるいは、ハードウェア製造の一環でソフトウェアが埋め込まれるかもしれない) 、さらにICチップと非接触通信用アンテナがプラスチックカードに埋め込まれて住基カードが製造される。追加APがこの段階で搭載されることもある。この段階までがライフサイクル上の開発フェーズに相当する。製造された住基カードは、住基カード発行者となる市町村へ納付される。

(4) 発行時のパーソナライゼーション

市町村は、住民に住基カードを発行する。住基カード発行に際し、管理者によって住民の固有情報が書き込まれる。この手続きは、住基カードのパーソナライゼーションと呼ばれる。本PPのTOEのライフサイクルにおいて、(4) 以降が運用フェーズに相当する。市町村において住基カード発行に携わる者は、CC評価の観点ではTOEの利用者に該当し、本PPでは、TOEの管理者と呼ばれる。

(5) 市町村における条例利用AP等の追加

住基カード発行者である市町村において、納付された住基カードに対し、市町村独自の条例利用AP、あるいはそれ以外のAPが追加APとして搭載される。追加APは市町村によるオプションであり、必ず搭載されるものではない。

(6) 住基カード保持者による利用

住基カード発行を受けた住民 (保持者) は、住基カードに搭載されたAPを用い、住基ネットの提供するサービスを利用する。住基カード保持者は、TOEの利用者である。CC評価上、住基カード保持者としての利用者は、発行者側の利用者 (管理者) と区別される。

住基カードは、住基ネットを利用するためのツールである。住基カードが悪用されると、住基ネットに脅威が生じる。住基カードには、住基ネットへの脅威に対抗するセキュリティ機能が必要である。

2 適合主張

2.1 CC適合主張

- 本PPは、CC V3.1 (JISEC公開の日本語版) 適合を主張する。
- 本PPは、CC パート2 (セキュリティ機能コンポーネント 改訂第3版 最終版 [翻訳第1.0版] 2009年7月 CCMB-2009-07-002) 適合を主張する。

  拡張するセキュリティ機能コンポーネントを第5章に定義する。
- 本PPは、CCパート3 (セキュリティ保証コンポーネント 改訂第3版 最終版 [翻訳第1.0版] 2009年7月 CCMB-2009-07-003) 適合を主張する。

2.2 PP主張

本PPは、他のPPへの適合を主張しない。

2.3 パッケージ主張

本PPにおいて、TOEに対して適用する保証パッケージは、EAL4追加である。

追加する保証要件は、AVA_VAN.5である。

2.4 適合根拠

本PPは、他のPPへの適合を主張しないので、適合根拠の記述を行わない。

2.5 適合ステートメント

本PPへの適合を主張するPP/STは、論証適合を主張しなくてはならない。

3 セキュリティ課題定義

本章では、TOEに関わるセキュリティ課題を定義する。セキュリティ課題は、脅威 (TOE及び/または環境で対抗する) 、組織のセキュリティ方針 (TOE及び/または環境で対処する) 、前提条件 (環境で満たす) の三つの側面から定義される。これらの課題は、TOEのライフサイクルにおける運用フェーズに関わるものである (1.2.4参照) 。TOE及び環境は、これらのセキュリティ課題に適切な形で対応しなければならない。

脅威、組織のセキュリティ方針、前提条件は、それぞれ、先頭が “T.”、“P.”、“A.” で始まる識別名が付与される。それぞれの内容記述において、必要に応じて [注釈] を付記する。[注釈] は、本PPの参照時に内容を誤解なく理解してもらうためのものであり、セキュリティ課題の定義文の一部ではない。

3.1 保護資産

TOEのセキュリティ機能によって保護される情報資産は、住基ネットが提供するサービスとTOEの内部データである。内部データにおいては、利用者データに該当するものが主たる保護対象である。例えば、住基APでは、住民票コードが利用者データに該当する。追加APの利用者データについては明示的に保護資産には含めないが、プラットフォームのセキュリティ機能で保護できるものは、暗黙的に保護対象となる (3.2に示すT.AP_abuseを参照) 。追加AP自身のセキュリティ機能で保護すべきものは、TOEの保護資産に該当しない。

TOEでは、利用者データ以外にも多様なデータが扱われる。これらのデータは、TOEのセキュリティ機能に利用され (TSFデータと呼ばれる) 、あるいは、それ以外の管理のために使用される。TSFデータは、それが暴露・改ざんされることで、結果的に、利用者データの暴露・改ざんにつながることがある。このため、主たる保護対象を一次資産とし、それと区別するため、TSFデータを二次資産と呼ぶことがある。二次資産の保護が必要なことは言うまでもないが、一次資産と異なり、必ずしも本PPの脅威中には明示されない。

3.2 脅威

本TOEに関して、対抗すべき脅威を示す。これらの脅威は、TOE、その運用環境、あるいは両者の組み合わせによって対抗されねばならない。

T.Fraud

攻撃者が他人の住基カードを使用して住基ネットのサービスを不正に利用する。

T.Illegal_attack

正当な利用権限を持たない攻撃者がTOEの外部インタフェースを介してTOEにアクセスし、TOE内部のプログラムやデータを許可なく暴露したり改ざんしたりする。TOEへのアクセスには、住基カードとの通信機能を持つ外部装置が使用される。本脅威に関しては、正規の外部装置だけに限らず、スキミングツールと呼ばれるような攻撃ツールが使用されるかもしれない。住基カードの電気端子、あるいは非接触通信インタフェースを経由して、TOEへのアクセスが行われる。

[注釈]　この脅威は、TOEが発行者の管理下にあるとき、あるいはTOEが住基カード保持者へ発行されたのち、それぞれの運用環境で生じる。「プログラムの改ざん」には、許可なく新規プログラムを追加する攻撃も含む。

TOEの正当な利用者とは、TOEを搭載した住基カードの保持者、及び住基カードを管理・運用する市町村における許可された権限者である (本PPでは、管理者と称する) 。住基カード保持者は、その住基カード (あるいはTOE) と一対一に対応づけられる。一方、管理者は、複数のTOEを管理する。

T.AP_abuse

TOEのAP利用者がそのAPを介して、他のAPで管理される利用者データを暴露したり改ざんしたりする。

[注釈]　このAPには、TOEの一部である住基APと、TOEに含まれない追加APの両方が該当する。

T.Eavesdrop

攻撃者がTOEと外部装置間の非接触通信に干渉し、通信データを傍受して通信データに含まれる個人情報を暴露したり、通信データを改ざんしたりする。

T.Replay

攻撃者がTOEと外部装置間の非接触通信における認証手順を傍受・記録し、記録した手順を繰り返すことで認証に成功して外部装置になりすまし、TOE内部データを暴露したり改ざんしたりする。

3.3 組織のセキュリティ方針

TOEあるいは運用環境に適用される組織のセキュリティ方針を示す。この「組織」に該当するのは、住基カードの運用・管理主体である市町村である。

P.Delivery

製造者から発行者 (市町村) へ納入される住基カードは、TOEのセキュリティ機能であるInitial Key及び輸送鍵によって内部データへの不正アクセスを防止する。Initial Keyはプラットフォームの保護に、輸送鍵は住基APの保護に使用する。

[注釈] TOE配付過程は、TOEセキュリティ機能による保護ではなく、配付手続きによるセキュリティ保護の対象になるものである。しかしながら、本TOEでは、Initial Key及び輸送鍵というTOEのセキュリティ機能 (認証メカニズムに相当) を輸送時の保護手段として併用する。このセキュリティ機能は、TOE運用環境において、輸送時にセキュリティ侵害がなかったことを確認するために使用される。さらに、輸送時だけでなく運用環境で不正使用からTOEを保護する手段としても有効である。本PPで使用するInitial Keyと輸送鍵の用語は、ICカード一般用語として用いられる輸送鍵に相当するものである。P.Deliveryは、TOEが利用者 (市町村) の管理下にあるときに適用される組織のセキュリティ方針であり、TOEが住基カード保持者へ発行されたのちは、P.Deliveryは適用されない。

P.Cryptography

TOEの暗号操作において、表3-1に示す暗号アルゴリズム及び鍵を使用する。これらの暗号アルゴリズムは、プラットフォーム、住基AP (いずれもTOEに含まれる) 、あるいは追加AP (TOE外) によって使用される。

使用する暗号アルゴリズムは、危殆化対応前と危殆化対応後の2群に大別される。どの暗号アルゴリズムを使用するかは、プラットフォーム、住基AP、追加APごとに要求が異なる。暗号アルゴリズムの選択は、住基カードを使用するシステム仕様に依存するので、TOEは、必要とされる暗号アルゴリズムを提供できるようにしなければならない。

プラットフォームが使用する暗号アルゴリズムにおいては、RSA暗号鍵をインポートする場合、既に格納されている暗号鍵をそれよりも短い暗号鍵で置き換えてはならない。

住基APが使用する暗号アルゴリズムは、危殆化対応前、あるいは対応後のいずれか片方の組み合わせが設定される。住基カード調達時に住基AP用として危殆化対応前の暗号アルゴリズムが設定されている場合、管理者による危殆化対応後の暗号アルゴリズムへの変更が可能でなければならない。

表3-1　暗号アルゴリズムと鍵

暗号アルゴリズム	暗号鍵長 (ビット)	標準名	暗号操作	危殆化対応
T-DES	192	NIST SP 800-67	・ 暗号化/復号 ・ MAC生成/検証	危殆化対応前
RSA	1024	PKCS#1 v2.1	・ 暗号化/復号 ・ 署名生成/検証	
SHA-1	-	FIPS PUB 180-2	ハッシュ演算	
AES	128	NIST FIPS PUB 197	・ 暗号化/復号 ・ MAC生成/検証	危殆化対応後
RSA	2048	PKCS#1 v2.1	・ 暗号化/復号 ・ 署名生成/検証	
SHA-256	-	FIPS PUB 180-2	ハッシュ演算	

[注釈]　暗号アルゴリズム危殆化に関わる対処

プラットフォームと住基APは、すべての住基カードに共通搭載される。まず、住基APに関わる暗号アルゴリズム選択について述べる。

以前のバージョンの住基APでは、表3-1に危殆化対応前として示した暗号アルゴリズムが使用されている。一方、暗号アルゴリズムの危殆化に伴い、将来は、危殆化対応後の欄に示した暗号アルゴリズムへ移行することが計画されている。この移行は、全国すべての住基APシステムが危殆化対応後の暗号アルゴリズムに対応したのち、一斉に実施される。移行以前の住基APは、危殆化対応前の暗号アルゴリズムを使用する。

住基カード開発者 (納入者) は、住基APの暗号アルゴリズムを、危殆化対応前のものから対応後のものに切り替えられるTOEを提供しなければならない。すなわち、住基AP向けに危殆化対応前の暗号アルゴリズムを設定したTOEを納入する場合、カード発行時に危殆化対応後の暗号アルゴリズムへ切り替えが必要になることがあり、カード発行者が切り替えを行えねばならない。なお、納入時に危殆化対応後の暗号アルゴリズム設定がなされているケースでは、危殆化対応前のものへの変更が必要になることはない。

プラットフォーム及び追加APが使用する暗号アルゴリズムは、住基APが使用する暗号アルゴリズムに依存しない。プラットフォームは、表3-1に示した危殆化対応前、対応後の両方の暗号アルゴリズムを提供しなくてはならない。なお、追加APがプラットフォームの暗号アルゴリズム演算機能を利用する場合、暗号鍵管理は、そのAP内で行われる。

次に、TOEが実装する暗号アルゴリズムとCC評価・認証制度の関係を述べる。

暗号アルゴリズム自体はCC評価の対象でないが、必要なセキュリティ特性を確保できない暗号アルゴリズムは、CC評価・認証制度 (日本では、JISEC) によって、認証対象として不適と判断されることがある。個々の暗号アルゴリズムに対する判断は各国のCC評価・認

証制度によって異なる。本PPを参照してPP/STを作成する者は、TOE評価に際し、対応するCC評価・認証制度における暗号アルゴリズムの扱いを確認すべきである。

TOEが使用する暗号アルゴリズムは、想定する攻撃に対抗できるものでなければならない。本PPは高レベルの攻撃を想定する。そのような攻撃に対抗できない暗号アルゴリズム (すなわち、危殆化した暗号アルゴリズム) を使用すると、TOEのセキュリティ機能が侵害されるかもしれない。もし、本PPに示した危殆化対応前の暗号アルゴリズムがCC評価・認証制度において不適と判断される場合、ST作成者は、危殆化対応後の暗号アルゴリズムをTOEのセキュリティ要件にするとともに、危殆化対応前の暗号アルゴリズムのうち不適とされたものについて、既存システムとの相互運用性維持のために必要だが、高レベルの攻撃に対するセキュリティ特性を主張するものではないことをSTに明示すべきである。

3.4 前提条件

TOEの運用環境で対処されるべき前提条件を示す。これらの前提条件は、TOEのセキュリティ機能性が効果を発揮するために必要である。

A.PKI

TOEは、その公開鍵暗号システム用鍵 (公開鍵・秘密鍵のペア) が有効に動作できるようなPKIシステムにおいて使用される。

A.Administrator

TOE内のデータあるいはAPの新規設定、変更もしくは削除を行う管理者は、許可された権限に基づき、正しくTOEを操作する。

A.AP

TOEに搭載される追加APは、プログラム中に悪意あるコードを含まず、かつ、プラットフォームや他のAPが使用するTOE資源を侵害しない。

4 セキュリティ対策方針

3章に示したセキュリティ課題に対して、TOE及びその運用環境におけるセキュリティ対策方針を示す。セキュリティ対策方針は、TOEによって対処するものを4.1に、その運用環境によって対処するものを4.2に記載する。さらに、これらのセキュリティ対策方針がセキュリティ課題に対して適切であることの根拠を4.3に示す。

TOEのセキュリティ対策方針、運用環境のセキュリティ対策方針は、それぞれ、先頭に“O.”、“OE.” を付与した識別名で表す。

4.1 TOEのセキュリティ対策方針

セキュリティ課題として定義された脅威と組織のセキュリティ方針に関して、課題解決のためにTOEが対処すべきセキュリティ対策方針を示す。

O.I&A

TOEは、外部インタフェース利用者を識別・認証し、正当な権限を持つ利用者だけに、その利用者に許可されたサービスを提供しなければならない。TOEの外部インタフェース利用者に相当するのは、住基カード発行者、住基カード利用者 (保持者) 、及び外部装置である。TOEは、これら利用者の真正性を確認した場合に限り、その利用者に許可されるサービスを提供しなくてはならない。

TOEは、上記利用者の真正性を確認するため、表4-1に示す認証メカニズムを使用する。認証メカニズムが暗号アルゴリズムを使用する場合、表3-1の公開鍵暗号アルゴリズム (RSA) を使用する。認証メカニズムの実行プロセスにおいては、表3-1に含まれるハッシュ演算が行われる。

暗号アルゴリズムが使用する暗号鍵に関わるTOEのセキュリティ対策方針は、O.Cryptographyに示される。なお、暗号鍵の選択に関して、表3-1の注釈を参照されたい。

表4-1 TOEの認証メカニズム

認証メカニズムの名称	認証メカニズムの規則	用途
住基カード発行者認証 (プラットフォーム)	Initial Keyによる照合(鍵長は調達仕様で指定される)	プラットフォーム部における住基カード発行者の認証

住基カード発行者認証(住基AP)	輸送鍵(8バイト)による照合	住基AP部における住基カード発行者の認証
利用者(住基カード保持者) 認証	4桁の暗証番号による照合 (住基カード交付前は16バイトの仮パスワードを設定し、照合を行う。交付時に利用者の暗証番号で置き換える)	住基AP部における利用者認証 ・住基カード保持者の認証 ・住基カード交付前の不正使用防止
外部装置認証(プラットフォーム)	公開鍵暗号方式による認証対象の真正性確認	プラットフォーム部における外部装置の認証
外部装置認証(住基AP)	公開鍵暗号方式による認証対象の真正性確認	住基AP部における外部装置の認証

O.Access_control

TOEは、利用者データのアクセスを正当な権限を持つものだけに許可し、権限外のアクセスを禁止しなければならない。

O.Secure_messaging

TOEは、外部装置間との非接触通信データが第三者に傍受され、通信データに含まれる個人情報の暴露、あるいは通信データ改ざんが行われるのを防ぐため、表3-1に示す共通鍵暗号アルゴリズム (T-DESあるいはAES) による通信データの保護 (セキュアメッセージング) を行わねばならない。プラットフォームにおけるセキュアメッセージングでは、暗号化及びMAC付与による通信データ保護を行う。住基APにおけるセキュアメッセージングでは、暗号化による通信データ保護を行う。使用される暗号鍵、MAC鍵の交換には、表3-1に示すRSA暗号アルゴリズムを使用する。セッション確立手順での署名検証には、表3-1に示すSHA関数を使用する。

O.Replay

TOEは、外部装置の認証手順において、攻撃者によって認証データが複製され再使用されるのを防ぐため、同一の認証データを再使用してはならない。

O.Delivery

製造者から発行者 (市町村) へ納入される住基カードは、Initial Key及び輸送鍵によって内部データへの不正アクセスを防止しなければならない。Initial Keyはプラットフォーム、輸送鍵は住基APをそれぞれ保護する。

O.Cryptography

TOEは、プラットフォーム、住基AP (いずれもTOEに含まれる) 、あるいは追加AP (TOE外) が、表3-1に示す暗号アルゴリズムを選択し、使用できるようにしなければならない。

プラットフォームが使用する暗号アルゴリズム向けRSA暗号鍵をインポートする場合、既に格納されている暗号鍵をそれよりも短い暗号鍵で置き換えてはならない。

住基カード調達時、TOEにおける住基AP向け暗号アルゴリズムが表3-1の危殆化対応前の組み合わせに設定されている場合、管理者によって危殆化対応後の組み合わせに変更できねばならない。

4.2 運用環境のセキュリティ対策方針

セキュリティ課題として定義された脅威、組織のセキュリティ方針及び前提条件に関して、課題解決のためにTOEの運用環境において対処すべきセキュリティ対策方針を示す。なお、ここに記載するセキュリティ対策方針は、すべて前提条件に由来する。

OE.PKI

市町村において住基カードの管理・運用に責任を持つ者は、TOEの使用環境において、TOEに搭載された公開鍵暗号システム用鍵 (公開鍵・秘密鍵のペア) が有効に動作できるようなPKIシステムを準備する。

OE.Administrator

市町村において住基カードの管理・運用に責任を持つ者は、TOE内のデータあるいはAPの新規設定、変更あるいは削除を担当する管理者について、TOEを正しく操作できるとともにTOEの保護資産に対して悪意ある行為をしない者を選定し、それらの行為を行う権限を付与する。

OE.AP

市町村において住基カードの管理・運用に責任を持つ者、あるいはTOEの管理者は、TOEに追加APを搭載する際、そのAPがTOEを熟知した信頼できる開発者によって開発されたものであることを確認し、信頼できない追加APが搭載されないようにする。

4.3 セキュリティ対策方針根拠

本章では、上述のセキュリティ対策方針がセキュリティ課題定義の各項目に対して有効であることの根拠を示す。4.3.1では、各々のセキュリティ対策方針がいずれかのセキュリティ課題にさかのぼれること、4.3.2では、各々のセキュリティ課題が対応するセキュリティ対策方針によって有効に対処されることを説明する。

4.3.1 セキュリティ課題定義とセキュリティ対策方針の対応

セキュリティ課題定義とセキュリティ対策方針の対応を表4-2に示す。ここに示すとおり、すべてのセキュリティ対策方針は、一つ (以上) のセキュリティ課題定義の項目にさかのぼることができる。

表4-2 セキュリティ課題定義とセキュリティ対策方針の対応

セキュリティ課題定義 ＼ セキュリティ対策方針	O.I&A	O.Access_control	O.Secure_messaging	O.Replay	O.Delivery	O.Cryptography	OE.PKI	OE.Administrator	OE.AP
T.Fraud	x								
T.Illegal_attack	x	x							
T.AP_abuse		x							
T.Eavesdrop			x						
T.Replay				x					
P.Delivery	x				x				
P.Cryptography	x		x			x			
A.PKI							x		
A.Administrator								x	

A.AP									x

4.3.2 セキュリティ対策方針の根拠説明

TOE及び環境に対するセキュリティ対策方針によって、識別された脅威がすべて十分に対抗され、組織のセキュリティ方針が実施され、さらに、前提条件が適切に満たされることの根拠を示す。

T.Fraud

O.I&AによってTOEの利用者を識別・認証し、TOEの正当な保持者以外の者がTOEを使用して住基ネットサービスを利用することを防止できる。O.I&Aは、T.Fraudの脅威を十分に軽減できる。

T.Illegal_attack

O.I&Aによって、TOEの外部インタフェース利用者を識別・認証し、正当な権限を持たない者にTSFを介するサービス提供を行わない。さらに、O.Access_controlによって、権限外のTOE内利用者データへのアクセスを許可しない。これによって、権限を持たない攻撃者はTOE内部の利用者データにアクセスできず、利用者データを暴露したり改ざんしたりすることができない。これらのセキュリティ対策方針によって、T.Illegal_attackの脅威を十分に軽減できる。

T.AP_abuse

O.Access_controlによって、それぞれのAP上で利用者を代行して動作するサブジェクトが、異なるAPに属するアクセス権限を持たないオブジェクトにアクセスすることが禁止される。これによって、T.AP_abuseの脅威を十分に軽減できる。

T.Eavesdrop

O.Secure_messagingによってTOEと外部装置間の非接触通信データが盗聴・改ざんから保護される。プラットフォームにおけるセキュアメッセージングでは、暗号化とMAC付与を併用することで、T.Eavesdropの脅威を十分に軽減する。住基APにおけるセキュアメッセージングでは、暗号化によって通信データ暴露の脅威を十分に軽減する。さらに、住基APに関

わる暗号化された通信データが改ざんされた場合、改ざんデータは有効な住基APデータとして復元されなくなるので、改ざんに対する脅威の影響が十分に緩和される。

T.Replay

O.Replayによって、攻撃者が外部装置による認証手順を傍受・記録し、外部装置になりすましてTOEに認証を試みても、傍受した認証データは既に無効になっており、認証に成功できない。これによって、T.Replayに示した同一の認証手順再使用によるなりすましの脅威が除去される。

P.Delivery

O.Deliveryは、P.Deliveryが求める輸送中の攻撃に対する保護手段を提供する。輸送中のセキュリティ保護は本来保証要件の対象であるが、本TOEでは、輸送中及び発行者管理下の両方に適用できる保護メカニズムとして、発行者が特定するInitial Key及び輸送鍵を使用する。このため、TOEセキュリティ対策方針の対象とする。O.I&Aは、Initial Key及び輸送鍵による認証メカニズムに関わる側面を規定し、保護手段の実現方法として有効である。これらのセキュリティ対策方針によって、P.Deliveryを適切に実施できる。

P.Cryptography

O.Cryptographyは、P.Cryptographyが規定する暗号アルゴリズムへの対応をカバーする。O.I&AとO.Secure_messagingは、P.Cryptographyの暗号アルゴリズムの適用を規定する。これらのセキュリティ対策方針によって、P.Cryptographyを適切に実施できる。

A.PKI

OE.PKIは、A.PKIの内容に直接対応しており、A.PKIを適切に満たす。

A.Administrator

OE.Administratorは、TOE内のデータあるいはAPの新規設定、変更あるいは削除を担当する者について、TOEを正しく操作でき、かつTOEの保護資産に対して悪意ある行為をしない者を選定し権限を付与することを示しており、A.Administratorに記述された内容を適切に満たす。

A.AP

OE.APは、追加APが悪意あるコードを内包したり、あるいはプラットフォームや他のAPの使用するTOE資源を侵害したりしないものであることを確認する手段として、追加AP開発者の信頼性の確認を求めている。このセキュリティ対策方針によって、A.APが適切に満たされる。

5 拡張コンポーネント定義

本PPでは、拡張コンポーネント定義を行わない。

6 セキュリティ要件

6.1 セキュリティ機能要件

本PPで規定するSFRは、すべてCCパート2に含まれるコンポーネントを使用する。表6-1にSFRのリストを示す。

表6-1 SFRリスト

章番号	識別名	
6.1.1	FCS_CKM.4	暗号鍵破棄
6.1.2	FCS_COP.1	暗号操作
6.1.3	FDP_ACC.1	サブセットアクセス制御
6.1.4	FDP_ACF.1	セキュリティ属性によるアクセス制御
6.1.5	FDP_ITC.1	セキュリティ属性なし利用者データのインポート
6.1.6	FIA_AFL.1(1)	認証失敗時の取り扱い(1)
6.1.7	FIA_AFL.1(2)	認証失敗時の取り扱い(2)
6.1.8	FIA_AFL.1(3)	認証失敗時の取り扱い(3)
6.1.9	FIA_UAU.1	認証のタイミング
6.1.10	FIA_UAU.4	単一使用認証メカニズム
6.1.11	FIA_UAU.5	複数の認証メカニズム
6.1.12	FIA_UID.1	識別のタイミング
6.1.13	FMT_MOF.1	セキュリティ機能のふるまいの管理
6.1.14	FMT_MSA.3	静的属性初期化
6.1.15	FMT_MTD.1	TSFデータの管理
6.1.16	FMT_SMF.1	管理機能の特定
6.1.17	FMT_SMR.1	セキュリティの役割
6.1.18	FTP_ITC.1	TSF間高信頼チャネル

それぞれのセキュリティ機能コンポーネントに必要な操作を施すことによってSFRを規定する。操作内容は、各SFRにおいて、以下の表記方法で示される。

- 割付あるいは選択操作の箇所を[割付: ×××*(斜体)*]、[選択: ×××*(斜体)*]の形式で示す。
- 選択操作において、選択対象外の項目を抹消線 (~~*抹消線*~~) で示す。
- 詳細化部分をSFR中に***斜体・太字***で示す。

- 繰返し操作は、SFR識別名の後ろに (1) 、(2) のように番号を付けて示す。
- 本PPでは、一部の操作が未了であり、その個所を[割付: *×××(斜体・下線)*]のように下線で示す。ST作成者は、未了部分の操作を完了せねばならない。

以下、本PPで規定するSFRを示す。

6.1.1 FCS_CKM.4 暗号鍵破棄

下位階層: なし

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または

FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4.1 TSFは、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵破棄方法[割付: *暗号鍵破棄方法*]に従って、暗号鍵を破棄しなければならない。

[注釈] ST作成者は、暗号鍵破棄に適用する標準名と破棄方法を具体的に記述する。

6.1.2 FCS_COP.1 暗号操作

下位階層: なし

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または

FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1 TSFは、[割付: *表6-2(a)、表6-2(b)に示す標準のリスト*]に合致する、特定された暗号アルゴリズム[割付: *表6-2(a)、表6-2(b)に示す暗号アルゴリズム*]と暗号鍵長[割付: *表6-2(a)、表6-2(b)に示す暗号鍵長*]に従って、[割付: *表6-2(a)、表6-2(b)に示す暗号操作のリスト*]を実行しなければならない。

表6-2(a) 暗号アルゴリズムと鍵 (危殆化対応前)

暗号アルゴリズム	*標準名*	*暗号鍵長 (ビット)*	*暗号操作*	*備考 (用途)*
T-DES	*NIST SP 800-67*	*192*	*・ 暗号化/復号* *・ MAC生成/検証*	*・セキュアメッセージング* *・秘密鍵設定機能(秘密鍵の復号)*
RSA	*PKCS#1 v2.1*	*1024*	*・ 暗号化/復号* *・ 署名生成/検証*	*・トークン検証* *・外部認証/内部認証* *・署名生成/検証* *・セキュアメッセージング用セッションキー共有*
SHA-1	*FIPS PUB 180-2*	*-*	*ハッシュ演算*	

表6-2(b) 暗号アルゴリズムと鍵 (危殆化対応後)

暗号アルゴリズム	*標準名*	*暗号鍵長*	*暗号操作*	*備考 (用途)*
AES	*NIST FIPS PUB 197*	*128*	*・暗号化/復号* *・MAC生成/検証*	*・セキュアメッセージング* *・秘密鍵設定機能(秘密鍵の復号)*
RSA	*PKCS#1 v2.1*	*2048*	*・暗号化/復号* *・署名生成/検証*	*・トークン検証* *・外部認証/内部認証* *・署名生成/検証* *・セキュアメッセージング用セッションキー共有*
SHA-256	*FIPS PUB 180-2*	*-*	*ハッシュ演算*	

[注釈] TOEである住基AP及びプラットフォーム、あるいはTOE外である追加APが外部装置と通信するため、表6-2(a)、表6-2(b) に示す暗号アルゴリズムが使用される。

住基APが使用する暗号アルゴリズムは、表6-2(a)、表6-2(b) のどちらか一方の組み合わせが選択的に使用される (本SFRで選択する必要はない) 。この選択に関わる要件は、FMT_MOF.1/FMT_SMF.1で規定される。

6.1.3 FDP_ACC.1 サブセットアクセス制御

下位階層: なし

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1 TSFは、[割付: *サブジェクト <利用者を代行して動作するTOE内プロセス> 、オブジェクト <TOE内ファイル> 、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト <ファイル生成・削除、ファイル内データ書き込み・読出し・更新・消去、実行可能ファイルの実行・停止>*]に対して[割付: *住基カードアクセス制御SFP*]を実施しなければならない。

6.1.4 FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

依存性: FDP_ACC.1 サブセットアクセス制御

FMT_MSA.3 静的属性初期化

FDP_ACF.1.1 TSFは、以下の[割付: *示されたSFP下において制御されるサブジェクト <利用者を代行して動作するTOE内プロセス> とオブジェクト <TOE内ファイル> 、及び各々に対応する、SFP関連セキュリティ属性 <サブジェクト: 認証ステータス、オブジェクト: サブジェクトに要求する認証ステータス、サブジェクトに許可する操作>*]に基づいて、オブジェクトに対して、[割付: *住基カードアクセス制御SFP*]を実施しなければならない。

FDP_ACF.1.2 TSFは、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: *オブジェクトに設定されたサブジェクトの「認証ステータス」条件をサブジェクトが満たすとき、サブジェクトは、「サブジェクトに許可する操作」を実行できる*]。

FDP_ACF.1.3 TSFは、次の追加規則、[割付: *なし*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

FDP_ACF.1.4 TSFは、次の追加規則、[割付: *なし*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

6.1.5 FDP_ITC.1 セキュリティ属性なし利用者データのインポート

下位階層: なし

依存性: [FDP_ACC.1 サブセットアクセス制御、または

FDP_IFC.1 サブセット情報フロー制御]

FMT_MSA.3 静的属性初期化

FDP_ITC.1.1 TSFは、SFP制御下にある利用者データをTOEの外部からインポートするとき、

[割付:*住基カードアクセス制御SFP*]を実施しなければならない。

FDP_ITC.1.2 TSFは、TOE外からインポートされるとき、利用者データに関連付けられたいかなるセキュリティ属性も無視しなければならない。

FDP_ITC.1.3 TSFは、TOE外部からSFPの下で制御される利用者データをインポートするとき、[割付: *利用者データがプラットフォーム部の使用するRSA暗号アルゴリズム鍵の場合、そのデータ長が既に格納済みの鍵データよりも短い鍵データのインポートを拒否*]の規則を実施しなければならない。

6.1.6 FIA_AFL.1 認証失敗時の取り扱い (1)

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 TSFは、[割付: *表6-3に示すInitial Keyによる認証*]に関して、[選択: *[割付: 3]*~~*、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*~~]回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2 不成功の認証試行が定義した回数[選択：~~*に達する、*~~*を上回った*]とき、TSFは、[割付: *表6-3に示すInitial Keyによる認証機能の恒久的閉塞*]をしなければならない。

6.1.7 FIA_AFL.1 認証失敗時の取り扱い (2)

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 TSFは、[割付: *表6-3に示す暗証番号照合あるいは仮パスワード照合による認証*]に関して、[選択: *[割付: 3]*、~~*[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*~~]回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2 不成功の認証試行が定義した回数[選択：~~*に達する、*~~*を上回った*]とき、TSFは、[割付: *表6-3に示す暗証番号照合あるいは仮パスワード照合による認証機能を閉塞し、管理者によって閉塞解除されるまで閉塞状態の継続*]をしなければならない。

6.1.8 FIA_AFL.1 認証失敗時の取り扱い (3)

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 TSFは、[割付: *表6-3に示す輸送鍵照合による認証*]に関して、[選択: *[割付: 3]*、~~*[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*~~]回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2 不成功の認証試行が定義した回数[選択：~~*に達する、*~~ *を上回った*]とき、TSFは、[割付: *表6-3に示す輸送鍵照合による認証機能の恒久的閉塞*]をしなければならない。

6.1.9 FIA_UAU.1 認証のタイミング

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.1.1 TSFは、利用者が認証される前に利用者を代行して行われる[割付: *TSF仲介アクションのリスト*]を許可しなければならない。

FIA_UAU.1.2 TSFは、その利用者を代行する他のすべてのTSF仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

[注釈] ST作成者は、利用者認証なしに利用できるTSF仲介アクションのリストを記載しなければならない。アクションリストでは、ISO/IEC 7816等で定義されるコマンド名称でなく、「×××情報の読出し」のように、サービス内容を明確に定義できる情報を記載する。該当するサービスが存在しない場合、「なし」と記載することはできず、FIA_UAU.1の代わりにFIA_UAU.2を使用する。なお、認証のために一連のコマンドセットを使用するケースでは、そのコマンドセット全体を認証サービスに必要なアクションとみなせるので、一部を認証前に許可するアクションリストに含める必要はない。

6.1.10 FIA_UAU.4 単一使用認証メカニズム

下位階層: なし

依存性: なし

FIA_UAU.4.1 TSFは、[割付: *外部装置認証*]に関係する認証データの再使用を防止しなければならない。

6.1.11 FIA_UAU.5 複数の認証メカニズム

下位階層: なし

依存性: なし

FIA_UAU.5.1 TSFは、利用者認証をサポートするため、[割付: *表6-3に示す複数の認証メカニズムのリスト*]を提供しなければならない。

FIA_UAU.5.2 TSFは、[割付: *表6-3に示す複数の認証メカニズムがどのように認証を提供するかを記述する規則*]に従って、利用者が主張する識別情報を認証しなければならない。

表6-3 認証メカニズム

認証メカニズムの名称	*認証メカニズムの規則*	*用途**
住基カード発行者認証(プラットフォーム)	*Initial Keyによる照合(鍵長は調達仕様で指定される)*	*プラットフォーム部における住基カード発行者の認証*
住基カード発行者認証(住基AP)	*輸送鍵(8バイト)による照合*	*住基AP部における住基カード発行者の認証*
利用者(住基カード保持者)認証	*4桁の暗証番号による照合* *(住基カード交付前は16バイトの仮パスワードを設定し、照合を行う。交付時に利用者の暗証番号で置き換える)*	*住基AP部における利用者認証* *・住基カード保持者の認証* *・住基カード交付前の不正使用防止*
外部装置認証(プラットフォーム)	*公開鍵暗号方式による認証対象の真正性確認*	*プラットフォーム部における外部装置の認証*
外部装置認証(住基AP)	*公開鍵暗号方式による認証対象の真正性確認*	*住基AP部における外部装置の認証*

* 用途欄は、SFRの一部ではなく、SFR内容理解のための参考情報である。

6.1.12 FIA_UID.1 識別のタイミング

下位階層: なし

依存性: なし

FIA_UID.1.1 TSFは、利用者が識別される前に利用者を代行して実行される[割付: *TSF仲介アクションのリスト*]を許可しなければならない。

FIA_UID.1.2 TSFは、その利用者を代行する他のTSF仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

[注釈] 利用者識別は、一般的には利用者がID情報を入力することで行う。一方、ICカードの場合、利用者が認証データを格納したファイルを選択することで、TSFは、そのファイルに関わる利用者が認証対象と識別できる。つまり、認証データファイルを選択するアクションが識別アクションに相当する。

ST作成者は、利用者識別なしに利用できるTSF仲介アクションのリストを記載しなければならない。アクションリストでは、ISO/IEC 7816等で定義されるコマンド名称でなく、「×××情報の読出し」のように、サービス内容が明確になる情報を記載する。該当するサービスが存在しない場合、「なし」と記載することはできず、FIA_UID.1の代わりにFIA_UID.2を使用する。なお、識別のために一連のコマンドセットを使用するケースでは、そのコマンドセット全体を識別サービスに必要なアクションとみなせるので、識別前に許可するアクションリストに含める必要はない。

6.1.13 FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

FMT_MOF.1.1 TSFは、機能[割付: *住基APが使用する暗号アルゴリズムを、表6-2(a)に示す危殆化対応前の暗号アルゴリズムから表6-2(b)に示す危殆化対応後の暗号アルゴリズムに変更することで、暗号操作に関わるセキュリティ機能*][選択: ~~*のふるまいを決定する、を停止する、を動作させる、*~~*のふるまいを改変する*]能力を[割付: *管理者*]に制限しなければならない。

[注釈] 本SFRは、住基APが使用する暗号アルゴリズムとして、FCS_COP.1.1の表6-2(a)に示す危殆化対応前の暗号アルゴリズムがTOEに設定されているとき、管理者によって、表6-2(b)に示す危殆化対応後の暗号アルゴリズムに変更可能なことを要求する。

TOEの住基APが初めから (例えば、住基カード発行者に納入された時点で) 危殆化対応後の暗号アルゴリズムに設定される場合、そのTOEでは本SFRによるセキュリティ機能のふるまい改変が完了したものとみなせるので、ST作成者は、根拠を正当化した上で、本SFRを削除できる。

本注釈に関連し、FMT_SMF.1の注釈を併せて参照のこと。

6.1.14 FMT_MSA.3 静的属性初期化

下位階層: なし

依存性: FMT_MSA.1 セキュリティ属性の管理

FMT_SMR.1 セキュリティの役割

FMT_MSA.3.1 TSFは、そのSFP を実施するために使われるセキュリティ属性に対して[選択: *制限的、許可的、[割付: その他の特性]: から一つのみ選択*]デフォルト値を与える[割付: *住基カードアクセス制御SFP*]を実施しなければならない。

FMT_MSA.3.2 TSFは、***追加APの***オブジェクトや情報が生成されるとき、[割付: *管理者*]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

[注釈] FMT_MSA.3.1では、追加APに関わるファイル生成時のセキュリティ属性デフォルト値の特性を規定する。デフォルト値の特性とは、ファイル生成の際、管理者がファイルのセキュリティ属性を設定する以前のアクセス制御の特性である。「制限的」とは、アクセスを許可しない特性を示す。このデフォルト値は、管理者がファイルのセキュリティ属性を設定することによって、その新しい値に置き換わる。

本SFRは、TOE運用環境におけるファイル生成に関わる要件であることに注意すること。例えば、運用環境でAPを追加する場合がこれに該当する。住基AP用ファイルのようにTOE納入時に開発者によって生成済みのファイルは、本SFRの対象ではない。

追加AP用ファイル生成時にセキュリティ属性を初期設定する権限者は、管理者である。本SFRの意味するところは、市町村の職員である管理者が追加APに関わるセキュリティ属性初期値の設定権限を持つということである。

管理者がTOEを操作して追加APをインストールし、ファイルを生成するのであれば、ファイルのセキュリティ属性デフォルト値がSFRを満たし、かつ管理者だけがデフォルト値を書き換えられるセキュリティメカニズムが要求される。

あるいは、追加APインストール時に、インストーラによってプログラム、ファイル、及びセキュリティ属性初期データが一括してTOEに書き込まれるかもしれない。その場合、TOEへの書き込みを管理者権限で行うセキュリティメカニズムが要求される。セキュリティ属性が初めから管理者の意図するセキュアな値に設定されるときは、デフォルト値を与えたり、それを置き換えたりするメカニズムは不要である。このような実装によっても、本SFRが満たされる。

6.1.15 FMT_MTD.1 TSFデータの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

FMT_MTD.1.1 TSFは、[割付: *住基AP部の利用者認証に用いるデータ*]を[選択: ~~*デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*~~]する能力を[割付: *管理者*]に制限しなければならない。

6.1.16 FMT_SMF.1 管理機能の特定

下位階層: なし

依存性: なし

FMT_SMF.1.1 TSFは、以下の管理機能を実行することができなければならない。: [割付: *オブジェクトのセキュリティ属性初期値設定、住基APが使用する暗号アルゴリズムの変更、住基AP部の利用者認証に用いるデータの改変*]

[注釈] 割付第1項の [オブジェクトのセキュリティ属性初期値設定] は、TOEの運用環境でファイル生成が行われる際の要件である。関連するFMT_MSA.3の注釈を併せて参照のこと。

割付第2項の [住基APが使用する暗号アルゴリズムの変更] を説明する。表6-2(b)に示す危殆化対応後の暗号アルゴリズム設定済みTOEが納入される場合、6.1.13の注釈に示したとおり、管理者が暗号アルゴリズムを変更することはない。このケースに該当するとき、ST作成者は、根拠を正当化したうえで、本SFRの割付から[住基APが使用する暗号アルゴリズムの変更]を削除することができる。

[住基APが使用する暗号アルゴリズムの変更] 管理機能は、FMT_MOF.1に対応する要件である。管理者が暗号アルゴリズムを変更するためのTSFメカニズムを要求する。SFRは実装を特定しないので、暗号アルゴリズム変更手段は、開発者による実装に依存する。例えば、TOEプログラムを一部変更することでアルゴリズム変更が可能だが、その場合、管理者だけがセキュアにプログラムを書き換えられるメカニズムが必要であり、書き換え前、書き換え後の両プログラムがTSFの一部として評価対象に含まれることに注意すること。

6.1.17 FMT_SMR.1 セキュリティの役割

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1 TSFは、役割[割付: *管理者*]を維持しなければならない。

FMT_SMR.1.2 TSFは、利用者を役割に関連付けなければならない。

[注釈] 管理者とは、住基カード発行者の総体としての組織ではなく、組織の中で住基カード発行、及び発行後の管理において、権限と責任を持って住基カードを取り扱う役割を意味する。

6.1.18 FTP_ITC.1 TSF間高信頼チャネル

下位階層: なし

依存性: なし

FTP_ITC.1.1 TSFは、それ自身と他の高信頼IT製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別、及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

FTP_ITC.1.2 TSFは、[選択: ~~*TSF、*~~*他の高信頼IT製品*]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。

FTP_ITC.1.3 TSFは、[割付: *外部装置との間で実施する保護資産データの送受信 (ex. 住民票コード読出し、秘密鍵インポートなど)*]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。

6.2 セキュリティ保証要件

本TOEに適用するセキュリティ保証要件は、表6-4に示す保証コンポーネントで定義される。これらは、すべて、CC パート3に含まれる。

表6-4に示すすべてのコンポーネントにおいて、本PPでは、操作を適用しない。

表6-4 保証コンポーネント

保証クラス	保証コンポーネント
セキュリティターゲット評価	ASE_CCL.1
	ASE_ECD.1

	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
開発	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
ガイダンス文書	AGD_OPE.1
	AGD_PRE.1
ライフサイクルサポート	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1
テスト	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
脆弱性評定	AVA_VAN.5

6.3 セキュリティ要件根拠

6.3.1 セキュリティ機能要件根拠

本章では、定義されたSFRがTOEのセキュリティ対策方針を適切に達成することの根拠を示す。6.3.1.1では、各々のSFRがいずれかのTOEのセキュリティ対策方針にさかのぼれること、6.3.2.2では、各々のTOEのセキュリティ対策方針が対応する有効なSFRによって適切に満たされることを説明する。

6.3.1.1 セキュリティ対策方針とセキュリティ機能要件の対応

TOEのセキュリティ対策方針に対応するSFRを表6-5に示す。この表は、すべてのSFRが少なくとも一つのTOEのセキュリティ対策方針にさかのぼれることの根拠となる。

表 6-5　TOE セキュリティ対策方針と SFR の対応

TOEセキュリティ対策方針 / SFR	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_ITC.1	FIA_AFL.1(1)	FIA_AFL.1(2)	FIA_AFL.1(3)	FIA_UAU.1	FIA_UAU.4	FIA_UAU.5	FIA_UID.1	FMT_MOF.1*	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FTP_ITC.1
O.I&A		x				x	x	x	x	x	x	x			x	x	x	
O.Access_control			x	x	x									x		x	x	
O.Secure_messaging	x	x	x	x	x													x
O.Replay										x								
O.Delivery									x		x	x						
O.Cryptography	x	x			x								x			x*	x*	x

[注釈]　*: 6.1.13の注釈に示した理由によってFMT_MOF.1を削除する場合、ST作成者は、表6-5からFMT_MOF.1を削除するとともに、O.CryptographyとFMT_SMF.1/FMT_SMR.1の対応を削除すること。

6.3.1.2 対応関係の根拠説明

TOEのセキュリティ対策方針がそれに対応づけられるSFRによって満たされることの根拠を示す。個々のSFRがTOEのセキュリティ対策方針を満たす上での有効性を持つことも同時に示される。

O.I&A

正当な権限を持つ利用者にサービスを提供する要件を、FIA_UAU.1、FIA_UID.1で規定する。セキュリティ対策方針O.I&Aの表4-1にTOEが提供すべき認証メカニズムとその規則、認証メカニズムの用途が示されており、これらはすべてFIA_UAU.5の表6-3で規定される。外部装置の認証には公開鍵暗号方式を使用する。乱数に施した電子署名の検証によって認証を行う。これに対応するSFRは、FCS_COP.1のRSA公開暗号方式及びSHAハッシュ演算である。さらに乱数使用に関して、同一認証データの再使用防止を規定するFIA_UAU.4を適用する。各認証メカニズムにおける認証失敗時のTSFアクションをFIA_AFL.1(1)、FIA_AFL.1(2)、FIA_AFL.1(3)で規定する。住基APの利用者認証に使用する認証データの管理要件として、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1を用いる。これらSFRによって、O.I&Aが十分に達成される。

O.Access_control

セキュリティ対策方針O.Access_controlは、利用者データに対し、正当な権限を持つものだけが許可されたアクセスを実行できることを求める。この要件は、FDP_ACC.1/FDP_ACF.1で規定される。FDP_ACF.1で使用されるセキュリティ属性を管理するため、FMT_MSA.3、FMT_SMF.1、FMT_SMR.1が用いられる。アクセスの範囲には、TOE外からの利用者データインポートが含まれる。このケースに対応するため、FDP_ITC.1を用いる。FDP_ITC.1は、追加AP搭載や暗号鍵インポートに適用される。これらのSFRによって、O.Access_controlが十分に達成される。

O.Secure_messaging

セキュアメッセージングで使用するセッション鍵 (T-DES/AES) は、外部装置においてRSA暗号化され、TOEにインポートされたのち復号される。暗号操作に関する規定はFCS_COP.1に示される。セキュアメッセージングによる利用者データのTOEへのインポートはFDP_ITC.1で規定される。利用者データインポート時のアクセス制御は、FDP_ACC.1/FDP_ACF.1で規定される。使用されたセッション鍵の破棄は、FCS_CKM.4で規定される。セキュアメッセージング自体の要件は、FTP_ITC.1で規定される。これらのSFRによって、O.Secure_messagingが十分に達成される。

O.Replay

FIA_UAU.4は、認証データの単一使用を規定するSFRで、セキュリティ対策方針O.Replayに合致する。

O.Delivery

セキュリティ対策方針O.Deliveryが要求するInitial Key及び輸送鍵による保護は、それぞれの鍵による認証機能をTOEに要求することで達成できる。識別・認証の要求はFIA_UAU.1とFIA_UID.1で規定し、それぞれの認証メカニズムはFIA_UAU.5で規定される。これらのSFRによって、O.Deliveryが十分に達成される。

O.Cryptography

セキュリティ対策方針O.Cryptographyが要求する暗号アルゴリズムと暗号操作は、FCS_COP.1で規定される。暗号操作に必要な暗号鍵には、セキュアメッセージング用セッション鍵 (T-DESまたはAES) とRSA暗号鍵がある。これら暗号鍵のインポートは

FDP_ITC.1で規定される。RSA暗号鍵インポート時は鍵長制限の規則が適用され、これもFDP_ITC.1に規定される。暗号鍵インポート時の通信路保護は、FTP_ITC.1で規定される。不要になった暗号鍵の破棄はFCS_CKM.4で規定される。住基AP向け暗号アルゴリズムの危殆化対応後への変更は、FMT_MOF.1、FMT_SMF.1、FMT_SMR.1で規定される。これらのSFRによって、O.Cryptographyが十分に達成される。

[注釈]　6.1.13の注釈に示した理由によってFMT_MOF.1を削除した場合、ST作成者は、本根拠から「住基AP向け暗号アルゴリズムの危殆化対応後への変更は、FMT_MOF.1、FMT_SMF.1、FMT_SMR.1で規定される。」の記述を削除する必要がある。

6.3.1.3　セキュリティ機能要件の依存性

各SFRに規定された依存性とその対応を表6-6に示す。

表において、「依存性の要求」欄にはCCパート2のコンポーネントに規定された依存性を示す。「依存性の対応」欄には、規定された依存性がPP中のどのSFRによって満たされるか、あるいは満たされない場合の正当性を示す根拠が記述される。

表6-6　SFRの依存性

SFR	依存性の要求	依存性の対応
FCS_CKM.4	[FDP_ITC.1または FDP_ITC.2または FCS_CKM.1]	FDP_ITC.1が対応し、依存性が満たされる。
FCS_COP.1	[FDP_ITC.1または FDP_ITC.2または FCS_CKM.1] FCS_CKM.4	FDP_ITC.1及び FCS_CKM.4が対応し、依存性が満たされる。
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1が対応し、依存性が満たされる。
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1及び FMT_MSA.3が対応し、依存性が満たされる。
FDP_ITC.1	FDP_ACC.1または FDP_IFC.1 FMT_MSA.3	FDP_ACC.1及び FMT_MSA.3が対応し、依存性が満たされる。
FIA_AFL.1(1)	FIA_UAU.1	FIA_UAU.1が対応し、依存性が満たされる。
FIA_AFL.1(2)	FIA_UAU.1	FIA_UAU.1が対応し、依存性が満たされる。
FIA_AFL.1(3)	FIA_UAU.1	FIA_UAU.1が対応し、依存性が満たされる。
FIA_UAU.1	FIA_UID.1	FIA_UID.1が対応し、依存性が満たされる。
FIA_UAU.4	なし	不要
FIA_UAU.5	なし	不要

FIA_UID.1	なし	不要
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1、FMT_SMF.1が対応し、依存性が満たされる。
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	運用上、オブジェクト生成後のセキュリティ属性操作を行わないので、FMT_MSA.1は要求されない。FMT_SMR.1は要件に含まれ、依存性が満たされる。
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1、FMT_SMF.1が対応し、依存性が満たされる。
FMT_SMF.1	なし	不要
FMT_SMR.1	FIA_UID.1	FIA_UID.1が対応し、依存性が満たされる。
FTP_ITC.1	なし	不要

6.3.2 セキュリティ保証要件根拠

本TOEは、ハードウェアであるICチップに埋め込まれるソフトウェアである。TOEのセキュリティは、ICチップのセキュリティ機能に多くを依存する。ICチップに対する典型的な攻撃は、ICチップのハードウェアを物理的に攻撃し、メモリ内の暗号鍵を読み出そうというものである。この物理的攻撃手法は高度に発達しており、内部に機密情報を持つICチップは、高レベルの攻撃に対抗することを求められる。すなわち、住基カード全体のセキュリティを考える際、ICチップ部分は、高レベルの攻撃力に対抗できることが必要である。

ICチップに高レベルの攻撃が想定されるため、そのICチップに埋め込まれるソフトウェアも、同様に高レベルの攻撃力に対抗することが望まれる。そのため、本PPのTOEにおいても、高レベルの攻撃者を想定し、脆弱性評定における保証要件としてAVA_VAN.5を要求する。

一方、ICチップとそのソフトウェアのセキュリティに限った場合、高レベルの攻撃を想定しても、使用される攻撃手法や評価上の確認ポイントは明確で、限定的である。このため、すべての保証要件を高レベルの攻撃に対応させる必要はなく、脆弱性評定以外の保証要件としては、商用製品として最高レベルではあるがEAL5ほどの厳密性を必要としないEAL4を設定する。

AVA_VAN.5に規定される依存性はAVA_VAN.3 (EAL4) と同一である。従って、依存性に関してEAL4保証パッケージと変わる部分がないため、表6-4に示す各保証コンポーネント間の依存性はすべて満たされる。

7 用語

7.1 CC関連

PP	Protection Profile: TOEの調達者あるいは開発に関わる業界などが共通仕様として定めるセキュリティ要件定義書。
CC	Common Criteria; IT装置のセキュリティ評価基準。ISO/IEC 15408規格は、CCをISO/IEC JTC1/SC27で審議し、ISO/IEC規格としたもの。
CCRA	The Common Criteria Recognition Arrangementの略。CC承認アレンジメントと訳される。CCRAに加盟する各国のCC評価・認証制度間で、他国の制度下での評価・認証結果を相互に承認し受け入れることを協定する。
ST	Security Target: 個々のIT製品に対するセキュリティ要件定義書。
TOE	Target of Evaluation; 評価対象。IT製品を構成するソフトウェア、ハードウェア、ファームウェア、ガイダンスが評価対象になる。IT製品全体をTOEと定義することもあり、IT製品の一部をTOEと定義することもある。TOEの範囲は、STによって厳密に定義する。

7.2 TOE関連

住基カード	住民基本台帳カード。 住民基本台帳ネットワークシステムで使用するICカードである。 本人確認の円滑化にとどまらず、公的個人認証サービス、条例利用など、多目的の公的ICカードとして利用されている。 平成15年の住基ネット二次施行で交付が開始されており、住民基本台帳カードType I (以下、「Type Iカード」という) 、住民基本台帳カードType II (以下、「Type IIカード」という) の2種類の仕様を規定している。 本PPの住基カードは、住民基本台帳法の一部を改正する法律 (平成21年7月15日公布) により、他の市町村へ住所を移した場合でも引き続き住民基本台帳カードを使用することができるようになったこと、Type Iカード、Type IIカードで実装されている暗号アルゴリズムの

	セキュリティ強化、新たな行政サービスへの拡張性向上等の対応として策定された住民基本台帳カードVersion 2である。
住基AP	住民基本台帳ネットワークシステム用カードアプリケーション。 住基APは、住基カード保持者の住民票コード管理に使用される。全ての住基カードに搭載され、正当なカード保持者だけが安全に住基APを使用できるよう、住基AP専用のセキュリティ機能が組み込まれる。
コンポジット評価	ICカードは、ハードウェア (ICチップや非接触通信用アンテナなどから構成される) とソフトウェアが一体化されたIT製品である。同一のハードウェアにさまざまなソフトウェアを組み合わせてICカード製品とする場合、まずハードウェア部分を評価し、その後にソフトウェアを搭載したICカードとして追加部分を評価すれば、時間のかかるハードウェア評価を共通化でき、トータルの評価コストを減らせる。このように、初めに基本部分を評価し、その後、追加部分を含めたIT製品全体の評価を行う方式をコンポジット評価と言う。 上記ICカードの例では、後から搭載されるソフトウェア部分及びソフトウェアとハードウェアの協働部分がコンポジット評価の対象となる。既に評価が実施されたハードウェア部分については、評価済みのSTと評価報告書を再利用できる。しかしながら、評価報告書は公開資料ではなく、再利用には評価報告書を作成した評価機関、評価を監督した認証機関の了承が必要になる。特に、基本部分の評価とコンポジット評価とを各々異なる認証機関のもとで行う場合、了承を得るための関係者が多くなり、十分な事前調整が必要である。