認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤江　一正　原紙押印済

プロテクションプロファイル（PP）

申請受付日（受付番号）	平成22年10月25日 (IT認証0312)
認証番号	C0284
認証申請者	財団法人地方自治情報センター
PPの名称	住民基本台帳カード Version2 組込みソフトウェア プロテクションプロファイル
PPのバージョン	1.00
PP適合	なし
保証パッケージ	EAL4 及び追加の保証コンポーネントAVA_VAN.5
開発者	財団法人地方自治情報センター
評価機関の名称	株式会社電子商取引安全技術研究所　評価センター

上記のPPについての評価は、以下のとおりであることを認証したので報告します。
平成23年2月28日

セキュリティセンター 情報セキュリティ認証室
技術管理者　山里　拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 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 バージョン3.1 リリース3
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース3

評価結果：合格

「住民基本台帳カードVersion2 組込みソフトウェアプロテクションプロファイル」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、財団法人地方自治情報センターが開発した「住民基本台帳カード Version2 組込みソフトウェア プロテクションプロファイル、 バージョン1.00」（以下「本PP」という。）について株式会社電子商取引安全技術研究所　評価センター（以下「評価機関」という。）が平成23年1月に完了したITセキュリティ評価に対し、その内容の認証結果を申請者である財団法人地方自治情報センターに報告するとともに、本PPに関心を持つ消費者や調達者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応するPPを併読されたい。本PPに適合するTOEの動作条件や運用のための前提についての詳細、TOEが対抗する脅威へのセキュリティ対策方針とその実施のためのセキュリティ機能要件、及び保証要件の十分性の根拠は、PPにおいて詳述されている。

本認証報告書は、本PPに準拠した住民基本台帳カードを開発・納入する開発者を読者と想定している。本認証報告書は、本PPが適合する保証要件に基づいた認証結果を示すものである。

1.1 評価PP

本PPが要求するセキュリティ機能性の概要を以下に示す。詳細は2章以降を参照のこと。

1.1.1 保証パッケージ及び適合主張

本PPにおいて要求される評価保証レベルは、EAL4追加である。追加の保証コンポーネントは、AVA_VAN.5である。

また、本PPへの適合を主張するPP、及びSTは論証適合を主張しなければならない。

1.1.2 PP概要

本PP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。）における主要構成要素の１つである、住民基本台帳カード（以下「住基カード」という。）の次世代の仕様である住基カードVersion2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。

本PPにおいて、TOEは住基カード内の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り、アプリケーション動作環境を提供するプラットフォームと、その上で動作する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。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（追加AP）は評価の対象外である。図1-1にTOE構成を示す。

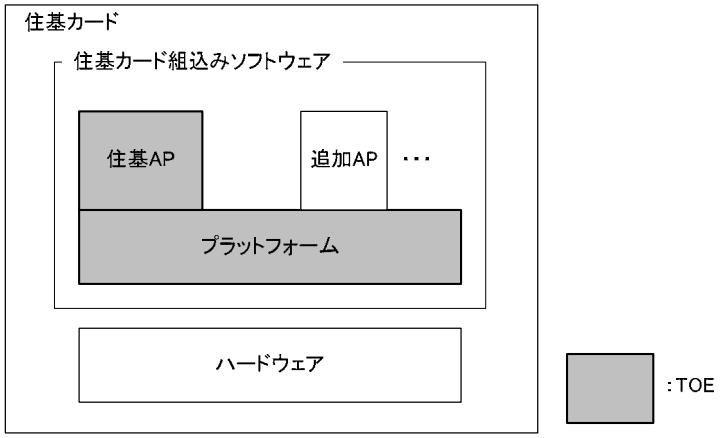

図1-1　TOE構成

開発者によって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。市町村は住民に住基カードを発行するが、その際各住基カードに住民の固有情報が書き込まれる（住基カードのパーソナライゼーション）。また必要に応じて住基カードに住基AP以外の追加APが搭載される。市町村において住基カード発行に携わるものはTOE管理者となる。

住基カード発行を受けた住民（住基カード保持者）は、住基カードに搭載された住基APを用い、住基ネットの提供するサービスを利用する。

1.1.2.1　セキュリティ機能概要

本PPでは、住基カードの利用者が、安全に住基APを利用して住基ネットが提供するサービスを利用できるように、セキュリティ機能を要求する。その主要なものを以下に示す。

(1) 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、及び住基APのそれぞれが通信チャネル保護機能を持つ。

(2) 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、及び住基AP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。）

(3) 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。

(4) 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、及び住基APのそれぞれが格納データ保護機能を持つ。

1.1.3 免責事項

本PPは住基カードの組込みソフトウェア部分をTOEとしており、ハードウェアを含めた住基カード全体のセキュリティ要件を規定するものではない。

1.2 評価の実施

認証機関が運営するITセキュリティ評価・認証制度に基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[1]、「ITセキュリティ認証申請手続等に関する規程」[2]、「ITセキュリティ評価機関承認申請手続等に関する規程」[3]に規定された内容に従い、評価機関によって本PPに関わる機能要件及び保証要件に基づいてITセキュリティ評価が実施され、平成23年1月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本PPの評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、本PPの評価がCC（[4][5][6]または[7][8][9]）及びCEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 PP識別

本PPは、以下のとおり識別される。

PP名称：	住民基本台帳カード Version2 組込みソフトウェア プロテクションプロファイル
バージョン：	1.00
開発者：	財団法人 地方自治情報センター

3 セキュリティ方針

本章では、本PPに適合するTOEが脅威に対抗するために採用するセキュリティ機能方針や組織のセキュリティ方針を説明する。

本PPでは、住基カード内の格納データに対する不正なアクセスを防ぐためのセキュリティ機能、及び組織のセキュリティ方針を満たすためのセキュリティ機能を要求する。

3.1 セキュリティ機能方針

本PPに適合するTOEは、3.1.1に示す脅威に対抗し、3.1.2に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本PPに適合するTOEは、表3-1に示す脅威を想定し、これに対抗する機能を備える。

表3-1 想定する脅威

識別子	脅 威
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。 【補足】 住基APを用いての不正利用の脅威である。追加APからの住基ネットサービスの利用は住基ネット側により対抗する。
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無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。
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。

	【補足】 前提条件A.APを満たすAPの誤使用、改ざんを想定した脅威である。また本脅威におけるAPは、全てのAP（住基AP、及び追加AP）が含まれる。
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。

3.1.1.2 脅威に対するセキュリティ機能方針

本PPに適合するTOEは、表3-1に示す脅威に対し、主に以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.Fraud」に対抗するためのセキュリティ機能

本脅威は、TOEの正当な保持者以外の者がTOEの住基APを使用して住基ネットサービスを不正に利用することを想定している。

この脅威に対して、TOEでは住基カード保持者の正当性を確認するための利用者認証機能を提供する。認証を行う際は、住基カード交付時に仮パスワードから置き換えられた4桁の暗証番号の照合を行い、3回以内に成功した場合に正当な住基カード保持者として住基APの使用が許可される。

(2) 脅威「T.Illegal_attack 」及び「T.Replay」に対抗するためのセキュリティ機能

脅威「T.Illegal_attack」は、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経由でTOE内部のプログラム、及びデータに不正にアクセスされることを想定している。また、「T.Replay」では外部装置の非接触通信における認証手順を再利用して、TOEに不正アクセスすることを想定している。

これらの脅威に対して、TOEでは住基カードと通信を行う外部装置の認証を行うことで正当性を確認し、正当な権限を持つことが確認された場合のみ、その権限の範囲でデータへのアクセスを許可する。外部装置の認証を行う際は、表3-3に示す暗号アルゴリズム（RSA）を用いた、公開鍵暗号方式による真正性確認を行う。また、その際の認証データは再利用せず、毎回異なるデータが使用される。これにより正当な外部装置のみがTOEの内部データにアクセスすることができる。

(3) 脅威「T.AP_abuse」に対抗するためのセキュリティ機能

本脅威は、TOEのプラットフォーム上で実行されるAPを介して、他のAPの資源に不正にアクセスすることを想定している。

この脅威に対して、TOEでは利用者データに対して、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することができる。これにより異なるAPに属する利用者データへの不正なアクセスを防ぐことができる。

(4) 脅威「T.Eavesdrop」に対抗するためのセキュリティ機能

本脅威は、TOEと外部装置間の非接触通信における通信データを傍受し、機密情報を暴露、もしくは通信データを改ざんすることを想定している。

この脅威に対して、TOEでは表3-3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を行う。使用される暗号鍵の交換には、表3-3に示す暗号アルゴリズム（RSA）を使用し、セッション確立手順での署名検証には、表3-3に示すSHA関数を使用する。これによりTOEと外部装置間の非接触通信を安全に行うことができる。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

本PPに適合するTOEの利用に当たって要求される組織のセキュリティ方針を表3-2に示す。

表3-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
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。 【補足】 本方針はTOEが市町村の管理下にあるときに適用される方針であり、TOEが住基カード保持者へ発行された後は適用されない。
P.Cryptography	TOEの暗号操作において、表3-3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3-3　暗号アルゴリズム及び鍵

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	

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

本PPに適合するTOEは、表3-2に示す組織のセキュリティ方針を満たす機能を具備する。

(1) 組織のセキュリティ方針「P.Delivery」を満たすためのセキュリティ機能

本組織のセキュリティ方針は、住基カード発行者である市町村の管理下にあるTOEに対して、正当な利用者のみがTOEの内部データへアクセスできることを規定している。

TOEの内部データへアクセスする前に、Initial Key、輸送鍵による認証を要求し、認証が成功した場合のみ、それぞれの鍵の認証に基づくTOEの内部データへアクセスできる。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。

(2) 組織のセキュリティ方針「P.Cryptography」を満たすためのセキュリティ機能

本組織のセキュリティ方針は、TOEが使用する暗号アルゴリズム、及び鍵を規定している（表3-3）。

TOEは、プラットフォーム、住基AP（いずれもTOEに含まれる）、及び追加AP（TOE外）が、表3-3に示す暗号アルゴリズムを選択し、使用できるようにする。表3-3の暗号アルゴリズムは、危殆化対応前、及び対応後の２群に大別され、住基APが使用する暗号アルゴリズムは、いずれか片方の組み合わせが管理者によって設定される（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この設定に影響されない）。

3.2 使用及び環境に関する前提条件

本PPに適合するTOEを運用する際の前提条件を表3-4に示す。

これらの前提条件が満たされない場合、本PPに適合するTOEのセキュリティ機能が有効に動作することは保証されない。

表3-4　前提条件

識別子	前提条件
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。 【補足】 本前提条件は、AP開発者及びAP自身の挙動が信頼できないAPがカードに追加されることを防ぐためのものである。この条件を満たすために、TOEの管理者がAPを追加する際に、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することが求められる。

4 評価機関による評価実施及び結果

4.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、本PPの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

4.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成22年11月に始まり、平成23年1月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

4.3 評価結果

評価者は、評価報告書をもって本PPがCEMのワークユニットすべてを満たしていると判断した。

評価では以下について確認された。

- PP適合：なし
- セキュリティ機能要件：　コモンクライテリア　パート２適合
- セキュリティ保証要件：　コモンクライテリア　パート３適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

- APE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.2、APE_ECD.1、APE_REQ.2

4.4 評価者コメント/勧告

消費者に喚起すべき評価者勧告は、特にない。

5 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。
② 所見報告書でなされた指摘内容が解決されていること。
③ 提出された証拠資料の内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、本PP及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

5.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3の保証コンポーネントAPE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.2、APE_ECD.1、及びAPE_REQ.2に対する保証要件を満たすものと判断する。

5.2 注意事項

1.1.3にもあるとおり、本PPでは住基カードの組込みソフトウェア単体で実現するセキュリティ機能について規定している。

住基カードとしてのセキュリティ評価を行う場合は、本PPで規定するセキュリティ機能に加えて、ハードウェア単体で実現するセキュリティ機能、及びハードウェアとソフトウェアの組み合わせにより実現するセキュリティ機能を含めた全体の評価・認証が必要になり、本PPに準拠したSTの作成者は、それら機能に関するセキュリティ課題、対策方針、機能要件等の定義が必要になることに注意する必要がある（住基カード全体の評価方法の詳細についてはPPの説明内容を参照のこと）。

また、本PPで規定する暗号アルゴリズムについては、本PPに適合するTOEの評価を行う時点での有効性を保証するものではない。従って、本PPに適合するTOE

の評価を行う際には、本PPが規定する暗号アルゴリズムの有効性の確認、及び危殆化についての評価が必要になる。

6 附属書

特になし。

7 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された用語の定義を以下に示す。

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カードであり、本人確認の円滑化にとどまらず、公的個人認証サービス、条例利用等、多目的の公的ICカードとして利用されている。 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、カードに実装され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Version2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。
危殆化対応	本PPではTOEが提供する暗号アルゴリズムの組み合わせとして危殆化対応前、危殆化対応後のセットが定義されている。以前のバージョンの住基カードでは、危殆化対応前のアルゴリズムセットが使用されており、今後危殆化対応後の暗号アルゴリズムへの切り替えが予定されている。切り替えのタイミングは暗号アルゴリズムの危殆化の状況、及び住基ネットワークシステム側の対応

状況により、住基ネットワークシステム全体で一斉に行なわれることとなり、設定の変更はTOEの管理者である市町村の担当者が実施する。

8 参照

[1] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[2] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[3] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 3 July 2009 CCMB-2009-07-003

[7] 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 バージョン3.1 改訂第3版 2009年7月 CCMB-2009-07-001 (平成21年12月翻訳第1.0版)

[8] 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2: セキュリティ機能コンポーネント バージョン3.1 改訂第3版 2009年7月 CCMB-2009-07-002 (平成21年12月翻訳第1.0版)

[9] 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3: セキュリティ保証コンポーネント バージョン3.1 改訂第3版 2009年7月 CCMB-2009-07-003 (平成21年12月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 3 July 2009 CCMB-2009-07-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン3.1 改訂第3版 2009年7月 CCMB-2009-07-004 (平成21年12月翻訳第1.0版)

[12] 住民基本台帳カード Version2 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　財団法人 地方自治情報センター

[13] 住民基本台帳カード Version2 組込みソフトウェア プロテクションプロファイル 評価報告書 第1.1版 2011年1月31日　株式会社電子商取引安全技術研究所 評価センター