アダプタ対応型高速版住基カードソフトウェア

セキュリティターゲット

バージョン：　1.92

発行者：　日本電信電話株式会社
サービスインテグレーション基盤研究所

発行日：　2008 年 10 月 10 日

作　成：　NTT エレクトロニクス株式会社

注意：本製品は、外国為替及び外国貿易法が定める許可申請対象貨物に該当いたします。本製品は、国内でのご利用を前提としたものでありますので、日本国外へ持出す場合は、同法に基づく輸出許可等必要な手続きをお取り下さい。

変更記録

Ver.	発行日	作成者	変更の理由と内容
1.00	03.06.26	大須賀	ST 評価用
1.10	03.07.29	大須賀	指摘事項の反映
1.20	03.07.30	大須賀	指摘事項の修正
1.30	05.12.05	大須賀	対象チップ変更に伴う変更，および適応する CC 補足資料のバージョンアップに伴う変更
1.40	05.12.21	大須賀	指摘事項の修正
1.50	07.03.12	大須賀	CC 評価に向けた最新化
1.60	07.08.01	大須賀	根拠の記述に対するコメント反映
1.70	07.08.29	大須賀	本評価における指摘事項への対応
1.80	07.09.14	大須賀	本評価における指摘事項への対応
1.81	07.09.20	大須賀	本評価における指摘事項への対応
1.82	07.10.05	大須賀	誤記等の修正
1.83	07.10.26	大須賀	本評価における指摘事項への対応
1.84	07.12.06	大須賀	機能設計書との整合性の観点からの修正
1.85	07.12.11	大須賀	機能設計書との整合性の観点からの修正
1.86	08.02.22	大須賀	誤記等の修正
1.87	08.03.28	大須賀	実装との整合性の観点からの修正、参照資料の追加
1.88	08.05.26	大須賀	実際の運用との整合性の観点からの修正
1.89	08.06.03	大須賀	指摘事項への対応、誤記等の修正
1.90	08.07.25	大須賀	指摘事項への対応
1.91	08.08.22	大須賀	カード交付時の状態に関する記述の追加
1.92	08.10.10	大須賀	TOE の動作環境に関する記述の一部削除

目　次

1. ST 概説

本章では、ST の識別と概要および CC への適合性について記述する。

1.1 ST 識別

タイトル ： アダプタ対応型高速版住基カードソフトウェア
セキュリティターゲット
バージョン： 1.92
発行日 ： 2008 年 10 月 10 日
発行者 ： 日本電信電話株式会社　サービスインテグレーション基盤研究所
作成者 ： 大須賀 勝美（NTT エレクトロニクス株式会社）

対象 TOE ： アダプタ対応型高速版住基カードソフトウェア
TOE のバージョン： 2.00

適用する CC のバージョン： CC Version 2.3 part1,2,3 (2005) および 補足-0512

保証レベル： EAL4 追加（追加される保証要件：AVA_MSU.3）

キーワード： 住民基本台帳カード、IC カード、組み込みソフトウェア、
住民票コード、認証、証明書、機密保護

1.2 ST 概要

本 ST が対象としている TOE は、住民基本台帳カード(以下、住基カードと表記)に搭載される組み込みソフトウェアであり、暗号処理のための演算機能をハードウェア化した高速版住基カードに搭載される。TOE は利用者の識別と認証、カード内に保存されるデータの保護のためのアクセス制御、外部との通信における機密漏洩の防止のための暗号通信、利用者の識別と認証の結果に基づいて実行できる機能を制御するための実行管理、カード上に複数搭載されるアプリケーションのドメイン分離、電源断発生に対するデータの保全のためのデータ復元と言ったセキュリティ機能を提供する。なお、暗号通信はハードウェア化した演算機能の支援により高速に実行される。

TOE が搭載された住基カードは、住民基本台帳ネットワークシステム(以下、住基ネットと表記)の業務で利用される。

本 ST は、TOE が対抗する脅威とその脅威に対する対策方針を明確にし、提供するセキュリティ機能要件と保証要件、実装された TOE の要約仕様およびそれらの根拠説明を記述する。

1.3 CC 適合の主張

本 ST の CC への適合性は以下の通りである。

1) CC Version 2.3 Part 2　適合
2) CC Version 2.3 Part 3　適合　EAL4　追加
   追加された保証要件は AVA_MSU.3 である。
   AVA_MSU.3 に対する保証方法として、参照資料[JIL]と[AIS]も用いる。

本 ST の TOE に対するセキュリティ機能強度は SOF-基本である。

また、本 ST が適合する PP はないが、以下の PP を参照する。
「住民基本台帳用 IC カードのセキュリティ要求仕様(プロテクションプロファイル)　ver. 2.0」

2. TOE 記述

本章では、TOE の種別、利用、構成、機能、メカニズムについて記述する。

2.1 TOE の種別

本 ST の対象とする TOE は、住基ネットにおいて使用される住基カードに搭載される組み込みソフトウェアであり、住基カードに記録されるデータや搭載されるアプリケーション(以下、AP と表記)を管理するために利用され、住基カードとしての要求仕様を満足するものである。

2.2 TOE の利用

2.2.1 TOE の利用目的

本 TOE は、住基カードに搭載され、カード発行者からカード所有者への安全な交付、カード所有者の本人確認、カードに格納されたカード所有者の情報に対する保護を実現することを目的とする。

住基ネットは、各市町村で管理する住民基本台帳を基にし、全国の市町村システムを電気通信回線で接続し、住民基本台帳の事務処理を効率化するために導入するものである。住基カードは、住民票の写しの広域交付、転入転出の特例および本人確認の業務に利用される。住基カードは、市町村の窓口に設置された住基ネットへ接続された市町村システムの業務用端末に接続されている住基カード用のカードリーダ・ライタに挿入され、カードリーダ・ライタを通じて市町村の業務用端末と通信して各業務を実現する。本 TOE は、上記のような要求を実現する際に、利用者の認証、アクセス制御、暗号化通信、アプリケーションの独立性確保などのセキュリティ機能を提供することを目的とする。

2.2.2 TOE に関係する存在

ここでは、TOE の製造から利用において TOE に関わる人または装置の役割を明確にする。TOE に関係するのは、カード製造者、カード発行者、カード所有者、業務用端末、AP 搭載管理者である(以下、単に製造者、発行者、所有者、業務用端末、搭載管理者と表現する場合がある)。製造者以外の TOE に関係する存在を総称して TOE 関係者と呼ぶ。また、TOE に搭載される AP の利用者も存在するが、TOE とは直接関係しないため、本 ST では TOE 関係者に含めない。

TOE 製造者

カード製造者：TOE の製造者であり、TOE 利用開始前の製造段階でしか TOE と関与しない。

TOE 関係者

カード発行者:製造者から TOE が搭載されたカードを調達し、住基カードの発行と交付を行なう。
カード所有者：住基カードの交付を受け、カードを所有する。
業務用端末：住基カードへ各種処理を要求するコマンドを発行する。
AP 搭載管理者：住基カードの AP 管理領域において AP の搭載全般を管理する。

2.2.3 TOE の利用方法

カードの利用

TOE 関係者はあらかじめ設定された認証データを提示することにより、TOE により正当性が確認された後、許可されたデータへのアクセスおよび機能を実行することが可能となる。

カードの発行

TOE は、あらかじめカード製造者によって住基カード上に搭載され、安全な配送手順に基づきカード発行者に納入される。カード発行者である市町村は、TOE のデータ領域に利用者データ、認証で必要となる認証データ、および TOE の動作で必要となる情報を設定する。発行時はカード発行者によって仮の認証データが設定され、カードの機能を一部利用できない状態とする。仮の認証データは市町村のポリシに基づき設定され、設定された内容は秘密情報として市町村において正しく管理される。

カードの交付

住基カードが住民に交付される際に、交付される住基カードの仮の認証データを知っている市町村職員による正当性の確認後、カードの発行を受ける住民により本人性を確認するための認証データが設定される。カード所有者により認証データが設定されると、カード所有者は住基カードを利用することが可能となる。

AP の搭載と削除

カード発行者はアプリケーションが搭載される領域を管理し、管理する領域におけるアプリケーションの搭載と削除の可否に関するセキュリティ属性を設定する。TOE は、カード発行者が設定したセキュリティ属性に基づき、アプリケーションを利用者データとして扱い、カード発行者またはカード発行者から権限を委譲された AP 搭載管理者によるアプリケーションの搭載と削除に関わるアクセス制御を実施する。カード所有者はカードに搭載されたアプリケーションが利用可能となる。

カードの廃止

カード発行者によってカードが廃止状態にされた場合、TOE はすべての要求を受け付けなくなり、カードのすべての機能が利用不可能となる。

2.3 TOE を含む構成

2.3.1 ハードウェアとソフトウェアの構成

TOE を構成するソフトウェアおよび周辺のハードウェアとソフトウェアは**図 1**のようであり、網掛け部分が TOE である。外部とのインタフェースはカードリーダ・ライタを経由して送受信されるコマンドメッセージとレスポンスメッセージによって実現される。

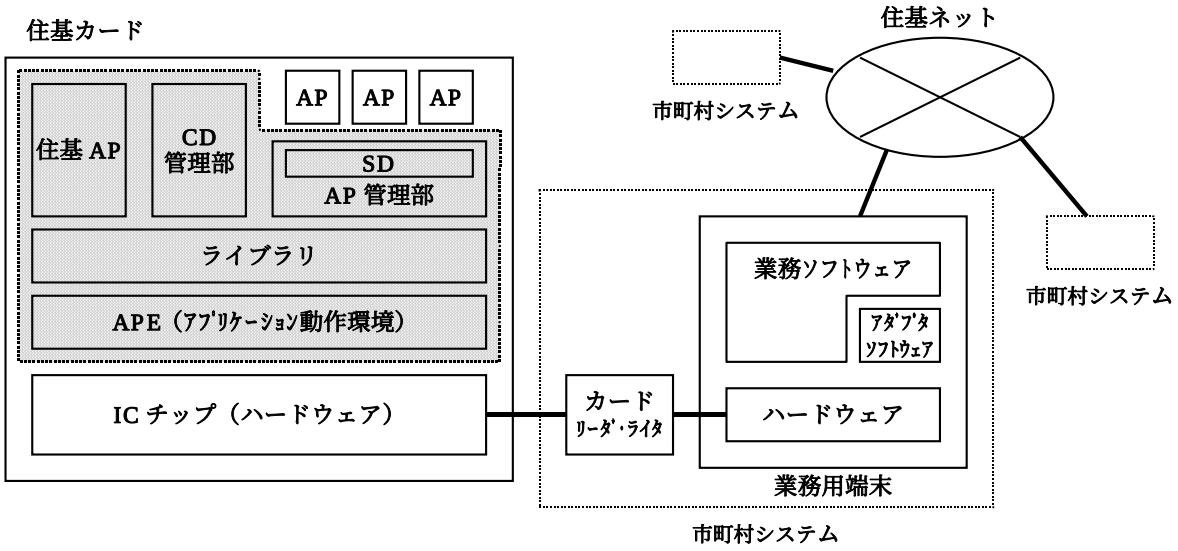

図 1　TOE の構成

TOE は、IC チップ上のメモリに組み込まれ、アプリケーションの動作環境を提供する AP 実行環境(APE)、ミドルウェアとして共通的な処理を行なうライブラリ、住基カードの発行や状態遷移の管理に関連する機能を実現する CD 管理部、アプリケーションの搭載と削除を管理する AP 管理部、住基ネットの業務への利用に必要な機能を実現する住基 AP の各モジュールから構成される。更にライブラリは、セキュリティライブラリ、RAM 管理ライブラリ、Flash 管理ライブラリから構成される。住基 AP はアプリケーションの１つであるが、製造段階であらかじめカード上に搭載され、AP 管理部の管理対象外である。また、AP 管理部には SD と呼ばれる領域が創生されてその上に AP が搭載できる。TOE によって搭載される AP は利用者データとして搭載と削除に対するアクセス制御が実施され、更に搭載された AP 間でのドメイン分離が実施される。SD 上に搭載された AP が提供するセキュリティ機能は本 TOE の外部に存在する。

住基カードはカードリーダ・ライタを通じて業務用端末に接続され、業務用端末は住基ネットに接続される。住基ネットには同様にして各市町村のシステムが接続されている。住基カードは、IC チップの通信機能によりカードリーダ・ライタを通じて業務用端末から送信されたコマンドメッセージを受け取り、コマンドメッセージの内容に基づいた処理を実施し、その結果をレスポンスメッセージとして返却する。

業務用端末上では業務ソフトウェアと呼ばれるソフトウェアが動作し、住基ネットに必要な業

務を処理する。業務用端末上には更にアダプタと呼ばれるソフトウェアが存在し、住基仕様で規定されたコマンド仕様に基づき住基カードの実装に対応したコマンドメッセージを生成する。アダプタは業務ソフトウェアから呼び出され、製造者毎に異なる住基カードの実装の差を吸収して共通のコマンド仕様で住基カードを利用できるようにする。

2.3.2 TOE の範囲

TOE の物理的な範囲は、**図 1**の網掛け部分であり、5 つのモジュールからなり、ソフトウェアとして IC チップのメモリ上に搭載される。外部とのインタフェースはすべてコマンドメッセージとレスポンスメッセージによって行なわれる。

また、TOE の論理的な範囲は、**2.4.1** でセキュリティ機能として記述されている部分である。

2.3.3 TOE の動作環境

TOE の動作環境および TOE 周辺装置の仕様は、以下の通りである。

＜IC チップ＞
製造元： シャープ株式会社
型式： SM4148 IC カード LSI

＜カードリーダ・ライタ＞

ISO/IEC 14443 および JIS X 6322 に規定される非接触型のインタフェース、または ISO/IEC 7816 および JIS X 6304 に規定される接触型のインタフェースを有するカードリーダ・ライタとする。

＜アダプタソフトウェア＞
住基カードの要求仕様に基づき住基カードの実装に対応して作成されたソフトウェア

＜業務ソフトウェア＞
要求仕様に基づいた住基カードの動作に見合った対応するように作成されたソフトウェア

2.4 TOE および環境の機能

本節では、TOE および TOE 環境の機能について記述する。

2.4.1 TOE の機能

TOE である**図 1**における APE、ライブラリ、CD 管理部、AP 管理部および住基 AP のモジュールで実現される TOE のセキュリティ機能を記述する。

《 TOE のセキュリティ機能 》

2.4.1.1 識別と認証機能

(1) 識別機能

TOE は、セレクトコマンドによりモジュールを切り替える際に利用者を識別し、選択されてカード上で動作しているモジュールをプロセスと呼ぶ。識別された利用者とプロセスが関連付けられ、プロセスは利用者を代行して動作し、受信したコマンドメッセージは現在選択されているプロセスへ引き渡される。

(注釈) 本 ST において、モジュールはカード上に搭載されたソフトウェアのプログラム単位での構成要素を表し、プロセスはモジュールがサブジェクトとして動作している状態の時のプログラムを表す。CD 管理部、住基 AP および AP 管理部の各モジュールが動作した場合、それぞれ CD 管理プロセス、住基 AP プロセスおよび AP 管理プロセスとなる。

(2) PIN 照合機能

TOE は、外部から送られた PIN をあらかじめカード内に設定されたデータと照合し、TOE 関係者を認証する。

(3) 外部認証機能

TOE は、生成した乱数を外部へ送り、外部から送られた暗号化データをあらかじめカード内に設定された公開鍵、または検証された公開鍵証明書の公開鍵を使用して復号し、外部ノードを認証する。

2.4.1.2 アクセス管理機能

(4) ファイル管理機能

TOE は、Flash メモリ上にデータを格納するための各ファイル領域の確保および管理を行ない、ファイルに設定されたデータへのアクセスを制御する。

(5) SD 管理機能

TOE は、AP 管理領域として AP を搭載する SD と呼ばれる領域を有する。

(6) アプリケーション管理機能

TOE は、SD において AP を管理し、アクセス制御に基づき AP の搭載と選択と削除を管理する。

(7) 鍵管理機能

TOE は、TOE の管理する鍵格納用ファイルへの鍵データの設定、更新を行なう。

2.4.1.3 暗号通信機能

(8) セキュアメッセージング機能

TOE は、外部との通信にセキュアメッセージング機能として送信データの暗号化と受信データの復号を行なう。IC カード LSI が持つ DES 暗号処理のための演算機能により高速な動作を実現している。

2.4.1.4 実行管理機能

(9) 認証ステータス管理機能

TOE は、PIN 照合と外部認証の結果を認証ステータスとして管理する。CD 管理部、AP 管理部および住基 AP のいずれかのモジュールがカレントプロセスとして選択された際に認証ステータスをクリアまたは維持し、各プロセスにおいて PIN 照合および外部認証が行われた際に認証ステータスを更新する。

(10) 状態遷移管理機能

TOE は、CD 管理部、AP 管理部および住基 AP の各モジュールにおける状態を管理し、コマンドにより各モジュールの状態を遷移させる。

(注釈) 各モジュールの状態はプロセスとして動作中に遷移し、モジュールとして搭載されている非動作時にも状態は維持される。

(11) コマンド実行制御機能

TOE は、状態遷移の状態に応じて認証されている TOE 関係者の役割でコマンドの実行が可能かどうかを判断し、コマンド実行を制御する。

2.4.1.5 ドメイン分離機能

(12) ドメイン分離機能

TOE は、カードに搭載されるモジュール間が相互に干渉しないようにそれぞれの動作領域を分離する。

2.4.1.6 データ復元機能

(13) 電源断異常検出機能

TOE は、データの書込み中または消去中に電源断異常が発生したかどうかを起動時に検査する。

(14) 障害回復機能

TOE は、処理実行前に、トランザクション処理を開始し、正常終了した場合にはトランザクション処理中の書込み内容を有効にして終了し、異常終了した場合には、トランザクション処理中の書込み内容を無効にして終了し、カードを正常状態に回復する。

《 TOE のセキュリティ以外の機能 》

セキュリティには直接関係ないが、TOE が有する機能を以下に記述する。

(1) 通信機能

TOE は、実行要求であるコマンドメッセージの受信および処理結果であるレスポンスメッセージの送信を行なう。

(2) コマンド解析機能

TOE は、受信したコマンドメッセージを解析し、要求された処理を行なう。

(3) メモリ制限機能

TOE は、カード上に搭載されたアプリケーションが利用可能なメモリ領域の大きさを制限する。

2.4.2 TOE 環境の機能

2.4.2.1 IC チップの機能

(1) 耐タンパー機能

TOE 環境は、チップ上に搭載されたプログラムおよびデータを物理的な攻撃から防御する。

(2) DES 演算機能

TOE 環境は、DES 暗号化のための演算機能をハードウェアで実現する。

2.4.2.2 カードリーダ・ライタの機能

(1) 残存情報保護機能

TOE 環境は、TOE 関係者の入力した情報が装置内に残存して漏洩しないように、残存情報を消去する。

2.4.2.3 業務用端末の機能

業務用端末は市町村の庁舎内に設置され、市町村職員により運用される。業務用端末上で業務ソフトウェアが動作し、カード発行、AP 搭載、PIN 設定、住民票コード読出しが行なわれる。業務ソフトウェアは、カード発行者や AP 搭載管理者を認証後にアクセス制御を実施し、カード発行者である正規の職員によって起動された場合にのみ業務用端末の秘密鍵を利用できるようにアクセス制御される。また、住基カードへ送信するためにカード所有者が入力した PIN および住

基カードから読出された住民票コードを漏洩から保護するため、これらの残存情報は利用後に業務用端末から消去される。

(1) 残存情報保護機能

業務用端末は、TOE 関係者の入力した情報が装置内に残存して漏洩しないように、残存情報を消去する。

(2) 認証機能

業務用端末は、操作する TOE 関係者および業務用端末がネットワークを通じて接続される他の業務用端末の正当性を認証する。

(3) アクセス制御機能

業務用端末は、端末の上で管理されている端末の秘密鍵に対してアクセス制御を実施する。

(4) 実行管理機能

業務用端末は、セキュリティ属性の設定およびセキュリティ機能の管理を実行できる TOE 関係者の役割を制限する。

2.5 TOE のセキュリティメカニズム

本節では、TOE が提供する認証、アクセス管理、状態遷移、暗号操作のセキュリティ機能について、実装する上でのメカニズムに対する説明を記述する。

2.5.1 TOE の認証メカニズム

TOE 関係者の役割に対するプロセスにおける認証メカニズムを**表 2-1**に示す。同じ役割に対して認証メカニズムが複数ある場合、操作に応じて 1 つのメカニズムで認証される必要がある。

表 2-1 TOE 関係者と認証のメカニズム

関係者の役割	認証のメカニズム	対応する人・物
カード発行者	CD 管理部輸送 PIN による PIN 照合 CD 管理部仮 PIN による PIN 照合 CD 管理部独自利用 PIN による PIN 照合 住基 AP 仮 PIN による PIN 照合 CD 管理部における発行市町村公開鍵による外部認証 AP 管理部輸送 PIN による PIN 照合 AP 管理部におけるカード発行者公開鍵による外部認証	市町村
カード所有者	CD 管理部所有者 PIN による PIN 照合 住基 AP 所有者 PIN による PIN 照合	住民
業務用端末	住基 CD における証明書検証用公開鍵により証明書が検証されたテンポラリ公開鍵による外部認証 住基 AP における鍵管理用公開鍵により証明書が検証されたテンポラリ公開鍵による外部認証	市町村に設置されて運用されるシステム
AP 搭載管理者	AP 管理部における AP 搭載管理者の公開鍵による外部認証	市町村

(注釈) TOE 関係者ではないが、AP 管理部におけるカード発行者と AP 搭載管理者の公開鍵に対して証明書を発行する証明書発行局が存在する。証明書発行局は市町村内に設置され、市町村による運営の下で証明書を発行する。カード発行時に AP 管理領域に証明書発行局の公開鍵を設定し、カード発行者または AP 搭載管理者の認証の際に利用する。

認証で利用される PIN は TSF データの管理規則に基づき、許可された TOE 関係者の役割によって設定、変更ができる。カード発行者により仮 PIN が設定され、カード所有者により所有者 PIN が設定される。仮 PIN は市町村におけるポリシに基づき設定され、設定された仮 PIN の内容は秘密情報として市町村において正しく管理される。カード発行者は、TOE の状態によって新たに値を再設定できる。また、許可された業務端末からは認証データを再設定できる。

PIN 照合および外部認証において 3 回連続で認証が失敗することにより、該当する認証データはそれ以降の認証に利用できなくなる。認証データ毎に失敗の回数が管理され、認証が成功すると失敗回数は 0 に戻される。ひとたび認証できなくなると、認証データを改めて設定しなおさなければならない。新しく設定された段階で失敗回数は 0 である。

CD 管理部輸送 PIN および AP 管理部輸送 PIN は TOE 関係者によって再び設定することができないため、3 回連続で認証が失敗すると、各輸送 PIN による認証が必要な機能は利用できなくなる。

2.5.2 TOE のアクセス管理

TOE が利用するデータは**図 2**のように住基 AP 領域、CD 管理領域、AP 管理領域の 3 つに分かれ、それぞれ住基 AP、CD 管理部、および AP 管理部だけがアクセスできるように APE によってドメインが分離されている。各ドメインには実行形式のモジュールとモジュールが扱うデータのための領域が割り当てられる。各ドメインに存在するモジュールからドメイン内のデータはアクセス可能であるが、他のドメインのデータへのアクセスはできない。分離された各ドメインに CD 管理部、住基 AP、AP 管理部の 3 つのモジュールがそれぞれ搭載され、それぞれ独立して TOE 関係者の認証を行ない、各ドメインに存在する利用者データへのアクセス制御を実施する。また、他のドメインからもアクセス可能な共有ドメインを設定することもでき、ライブラリは共有ドメインに搭載されて各ドメインから利用が可能である。

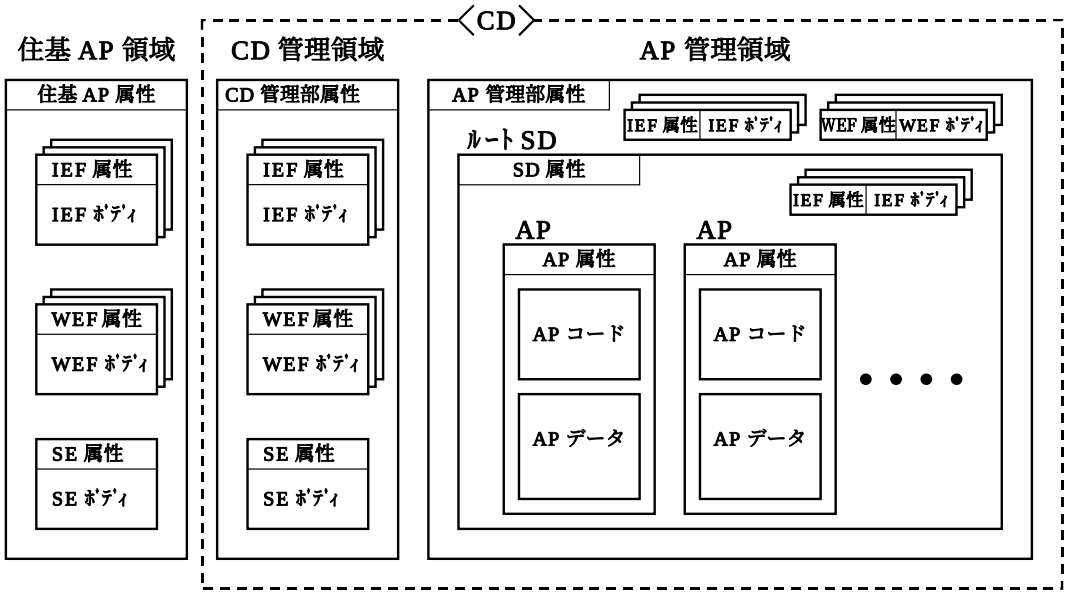

図 2　データ領域の構成

住基カードにおいて､データを格納する領域として EF と呼ばれる基礎ファイルが創生できる。EF には、PIN または鍵の認証データが格納される IEF と呼ばれるデータ格納領域と、作業で利用するデータを格納する WEF と呼ばれるデータ格納領域が存在する。認証や暗号化で利用する鍵を指定するためのセキュリティ属性の 1 つとして、SE と呼ばれるデータ格納領域が存在する。また、住基カードには、CD と呼ばれる領域が 1 つだけ存在してカード全般に関わる情報を管理し、CD は CD 管理領域と AP 管理領域の 2 つの領域で構成される。AP 管理領域の中にはルート SD と呼ばれる領域が製造者によって創生され、カードに搭載されるすべての AP を管理する。AP の格納領域には AP のプログラムコードが格納される領域と、AP の利用するデータが格納される領域が存在する。各データの格納領域にはデータの管理情報である属性を格納する領域がそれぞれ存在する。ルート SD には、SD 属性と呼ばれる AP 搭載に関する設定をするためのセキュリティ属性が存在する。

CD 管理領域には IEF と WEF がそれぞれ複数存在し、SE が 1 つ存在する。AP 管理領域には SD が 1 つだけ創生され、その配下に複数の AP が搭載される。AP 管理領域と SD にはそれぞれ IEF が複数存在する。住基 AP 領域には IEF と WEF がそれぞれ複数存在し、SE が 1 つ存在する。

TOE の実施するアクセス制御の概念は図 3の通りである。業務用端末からカードリーダ・ライタを通じて送られたコマンドは、まず TOE の通信部へ引き渡される。「セレクト」コマンドにより CD 管理部、AP 管理部、または住基 AP の 1 つが選択され、選択されたモジュールが CD 管理プロセス、AP 管理プロセス、または住基 AP プロセスとして動作し、サブジェクトとして利用者を代行する。利用者とサブジェクトとして動作しているプロセスはカレントプロセスの識別情報で関連付けられ、コマンドディスパッチ部によって CD 管理プロセス、AP 管理プロセス、または住基 AP プロセスの内、現在選択されているプロセスへコマンドが送られて処理される。「セレクト」コマンドによりカレントプロセスの識別情報は変更され、カード起動時の最初のカレントプロセスは AP 管理プロセスとなる。サブジェクトとして動作しているプロセスにおいてコマンドが処理される中でデータ領域へのアクセスが実行されるが、利用者データへのアクセスに対してアクセス制御が実施される。

「セレクト」コマンドにより 3 つのモジュールの内のひとつを選択できるが、モジュールを切り替える際に利用者の識別が行なわれ、プロセスとして動作するときに識別した利用者を代行したサブジェクトとなる。「セレクト」コマンドだけは他のコマンドと区別され、利用者の識別なしに実行が可能である。

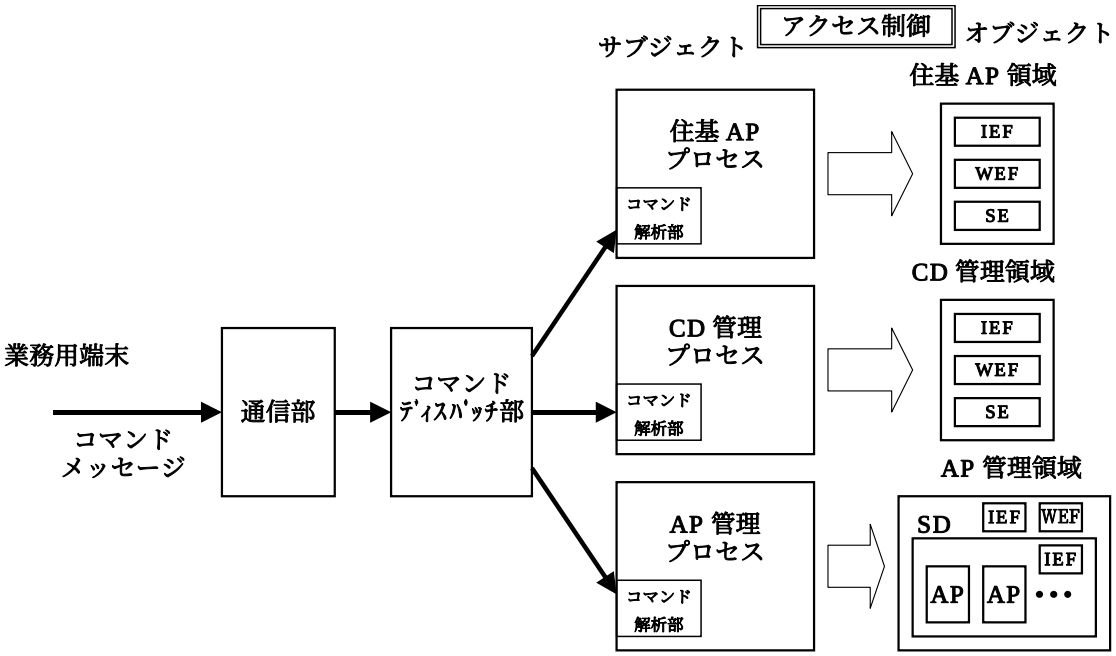

図 3　アクセス制御におけるサブジェクトとオブジェクトの関係

アクセス制御の仕組みは、アクセス管理属性と呼ばれるセキュリティ属性によってアクセス制御の操作に対するアクセス権を規定する。認証ステータスと呼ばれるセキュリティ属性によってTOE 関係者に対する認証結果が保持され、アクセス管理属性の条件を満足した場合に、オブジェクト内の情報へのアクセスが許可される。各モジュールのアクセス制御は状態遷移図における状態に応じて規則が異なり、状態遷移ステータスと呼ばれるセキュリティ属性によって現在の状態が管理される。アクセス管理属性は製造時に製造者によって IEF 属性または WEF 属性の領域に設定され、TOE 利用時に変更することはできない。認証ステータスおよび状態遷移ステータスは各モジュールの動作に応じて変化し、**図 2**における CD 管理部属性、住基 AP 属性、AP 管理部属性の領域にそれぞれ保持される。

アクセス制御におけるサブジェクトと利用者と役割の関係を**表 2-2**に示す。**表 2-2**において、利用者は TOE 外に存在する人または装置で、各サブジェクトが代行する利用者をまとめた総称である。

表 2-2アクセス制御におけるサブジェクトと利用者と役割の関係

サブジェクト	利用者	役割
CD 管理プロセス	CD 管理部利用者	カード発行者 カード所有者
住基 AP プロセス	住基 AP 利用者	カード発行者 カード所有者 業務用端末
AP 管理プロセス	AP 管理部利用者	カード発行者 AP 搭載管理者

2.5.3 TOE の状態遷移

CD 管理部、AP 管理部、および住基 AP の各モジュールは、TOE 関係者による操作実行に伴って**図 4**に示す状態遷移を行なう。**図 4**における四角い枠が状態を表し、3 つのモジュールそれぞれで状態遷移ステータスと呼ばれるセキュリティ属性によって現在の状態が管理され、状態の遷移に伴い状態遷移ステータスの値が変化する。状態遷移ステータスはモジュールがプロセスとして動作している際に変化するが、プロセスが切り替わった場合およびカードが非活性化の場合にも値は保持されてモジュールの状態を管理する。

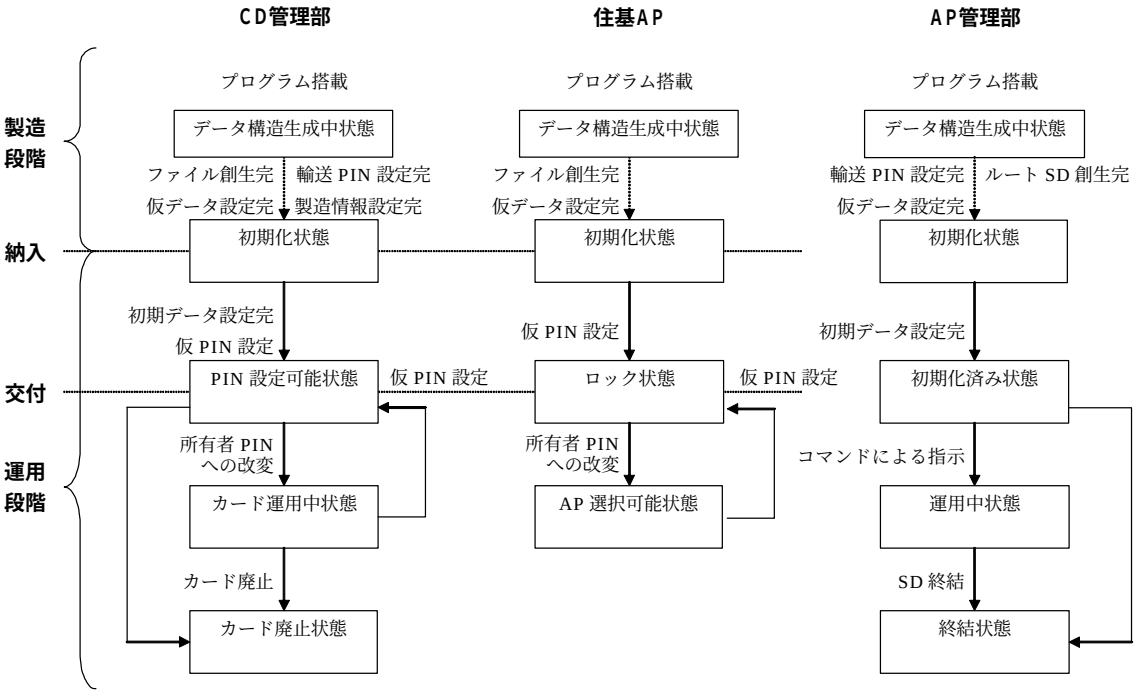

図 4　TOE の状態遷移図

まず、APE、ライブラリも含め TOE を構成するすべてのプログラムを製造者が IC チップのメモリ上に搭載する。その後、ファイル創生、輸送 PIN 設定、仮データ設定までは、製造者が処理を行ない、各モジュールの輸送 PIN および仮データの設定完の状態で発行者である市町村へ安全な配送手順に基づき納入される。各モジュールのドメインは分離されているため、納入後の各モジュールの状態遷移は独立して個別に遷移することができるが、利用方法としては複数のモジュールの状態遷移を同期させてそれぞれ遷移させる。具体的には、発行者が仮 PIN を設定の後、CD 管理部と住基 AP の各モジュールがそれぞれ PIN 設定可能状態、ロック状態となった状態で所有者となる住民へカードが交付される。AP 管理部の状態遷移はカード発行者の処理に基づいて発生し、市町村の AP 搭載に対する管理方針に応じて遷移される。運用段階において AP 搭載管理者による AP 搭載や AP 削除を実施する場合、AP 管理部は運用中状態に遷移して交付される。また、運用段階において AP 搭載管理者による AP 搭載や AP 削除を実施しない場合、AP 管理部が初期化済み状態で交付される。CD 管理部がカード廃止状態に遷移した場合、カードとしてすべてのコマンドを受け付けなくなりカードは利用できなくなる。

本 ST の TOE が TOE 関係者によって利用されるのは**図 4**における運用段階の範囲であり、製造段階は利用の対象外である。

以下に各モジュールにおける状態遷移の関係を説明する。

2.5.3.1 CD 管理部の状態遷移

(1) データ構造生成中状態

製造者により住基カードに必要なファイルの創生と IEF 中の仮データを設定している最中の状態で、仮データの設定完了後、初期化状態に移行する。

(2) 初期化状態

製造者からカードが納入される際の状態で、住基カードの要求仕様を満たし、初期データの設定が可能な状態。

(3) PIN 設定可能状態

カードの初期化や運用に必要な情報をカードへ登録するための初期データの設定が完了し、仮 PIN が設定された状態。カード所有者へのカード交付が可能な状態。

(4) カード運用中状態

カード所有者へのカード交付後、カード所有者による PIN の設定が完了することにより移行し、住基システムでの利用が可能な状態。

(5) カード廃止状態

カードが恒久的に利用できないようにされている状態。

表 2-3 CD 管理部における状態遷移

状態の遷移	遷移の条件
データ構造生成中状態 ⇒ 初期化状態	製造者による作業完
初期化状態 ⇒ PIN 設定可能状態	カード発行者による CD 管理部仮 PIN の設定
PIN 設定可能状態 ⇒ カード運用中状態	カード発行者によるCD管理部所有者PINの設定※
カード運用中状態 ⇒ カード廃止状態	カード発行者からのコマンドによる指示
PIN 設定可能状態 ⇒ カード廃止状態	カード発行者からのコマンドによる指示
カード運用中状態 ⇒ PIN 設定可能状態	カード発行者による CD 管理部仮 PIN の設定

※：CD 管理部において、CD 管理部仮 PIN と CD 管理部所有者 PIN は同じ場所に格納され、PIN 設定可能状態からカード運用中状態へ遷移する場合、CD 管理部所有者 PIN の設定とは、CD 管理部仮 PIN から CD 管理部所有者 PIN への改変を意味する。

2.5.3.2 AP 管理部の状態遷移

(1) データ構造生成中状態

AP 管理部に必要な初期データを設定中の状態。輸送 PIN の設定完了後、CD 内に直接ルート SD が創生され、カード管理データが設定された状態で製造者から納入される。

(2) 初期化状態

AP 管理部の運用に必要な初期データの設定が可能な状態。

(3) 初期化済み状態

カード発行者が証明書発行局の公開鍵、カード発行者の公開鍵、鍵配送用暗号鍵、鍵配送用復号鍵を設定した状態。

(4) 運用中状態

AP 管理部運用中の状態で、AP の搭載が可能な状態。

(5) 終結状態

AP 管理部終結の状態で、AP 管理部のコマンドを受け付けない状態。

表 2-4　AP 管理部における状態遷移

状態の遷移	遷移の条件
データ構造生成中状態　⇒　初期化状態	製造者による作業完
初期化状態　⇒　初期化済み状態	カード発行者からのコマンドによる指示
初期化済み状態　⇒　運用中状態	カード発行者からのコマンドによる指示
運用中状態　⇒　終結状態	カード発行者からのコマンドによる指示
初期化済み状態　⇒　終結状態	カード発行者からのコマンドによる指示

2.5.3.3 住基 AP の状態遷移

(1) データ構造生成中状態

住基カードに必要なファイル等を生成中、また IEF 中の仮データ等を設定中の状態。データ設定完了後、初期化状態に移行する。

(2) 初期化状態

住基 AP に対する初期データの設定に必要な処理が可能な状態

(3) ロック状態

運用に必要な情報をカードへ登録する初期データの書込みが完了し、住基 AP 仮 PIN が設定された状態。カード所有者へのカード交付が可能であるが、実施できる機能が PIN の設定と照合に制限される。

(4) AP 選択可能状態

カード所有者へのカード交付後、カード所有者による PIN 設定が完了し、住基 AP を利用した処理が実施でき、住基システムでの利用が可能な状態。

表 2-5 住基 AP における状態遷移

状態の遷移	遷移の条件
データ構造生成中状態 ⇒ 初期化状態	製造者による作業完
初期化状態 ⇒ ロック状態	カード発行者による住基 AP 仮 PIN の設定
ロック状態 ⇒ AP 選択可能状態	カード発行者による住基AP所有者PINの設定※
AP 選択可能状態 ⇒ ロック状態	カード発行者による住基 AP 仮 PIN の設定

※：住基 AP において、住基 AP 仮 PIN と住基 AP 所有者 PIN は同じ場所に格納され、ロック状態から AP 選択可能状態へ遷移する場合、住基 AP 所有者 PIN の設定とは、住基 AP 仮 PIN から住基 AP 所有者 PIN への改変を意味する。

2.5.3.4 PIN および公開鍵の状態遷移

認証で利用する PIN および公開鍵(但し、テンポラリ公開鍵は除く)は各データ領域にそれぞれ複数存在し、それぞれ**図 5**および**図 6** に示す状態遷移図において状態を遷移する。PIN または公開鍵の状態遷移は個別に管理され、該当する PIN または公開鍵の認証への利用可否を決定し、**図 4**の TOE の状態遷移とは独立である。

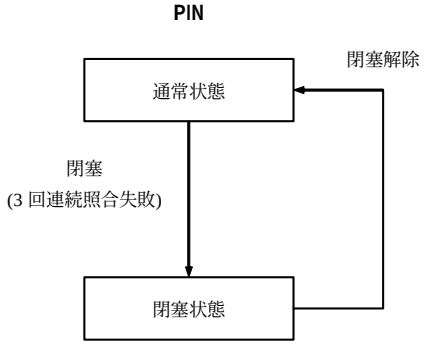

図 5 PIN の状態遷移図

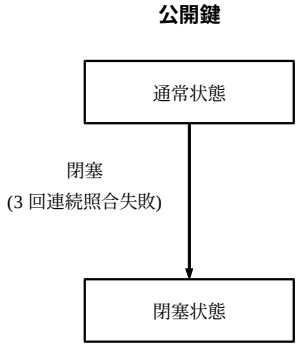

図 6 公開鍵の状態遷移図

(1) 通常状態

PIN については PIN 照合、また、公開鍵については外部認証において認証に利用できる状態。

(2) 閉塞状態

PIN については PIN 照合、また、公開鍵については外部認証において連続的に認証に失敗し、再び認証に利用できない状態。PIN 照合時の状態遷移と閉塞状態からの解除方法を**表 2-6**に示す。公開鍵はひとたび閉塞状態になると通常状態へは戻せない。

表 2-6　PIN 照合時の状態遷移と閉塞状態からの解除方法

モジュール	状態、＜役割＞	通常状態 ⇒ 閉塞状態	閉塞状態からの解除方法
CD 管理部	初期化状態、 ＜カード発行者＞	輸送 PIN 照合連続失敗	なし
	PIN 設定可能状態、 ＜カード発行者＞	CD 管理部仮 PIN 照合連続失敗	なし
	カード運用中状態、 ＜カード所有者＞	CD 管理部所有者 PIN 照合連続失敗	カード発行者による CD 管理部仮 PIN の設定
住基 AP	初期化状態、 ＜カード発行者＞	輸送 PIN 照合連続失敗	なし
	ロック状態、 ＜カード発行者＞	住基 AP 仮 PIN 照合連続失敗	なし
	AP 選択可能状態、 ＜カード所有者＞	住基 AP 所有者 PIN 照合連続失敗	カード発行者による住基 AP 仮 PIN の設定
AP 管理部	初期化状態、 ＜カード発行者＞	AP 管理部輸送 PIN 照合連続失敗	なし
	初期化済み状態 ＜カード発行者＞	AP 管理部輸送 PIN 照合連続失敗	なし
	運用中状態	該当 PIN なし	対象外

2.5.4 TOE の暗号操作

TOE で利用される暗号操作の内容と利用箇所と利用目的と利用する鍵は以下の通りである。

表 2-7 TOE の暗号操作と利用方法

アルゴリズム	鍵長	暗号操作	利用目的	使用する鍵
RSA	1024 ビット	外部認証時､認証の検証のため､関係者の秘密鍵により暗号化された認証コードの復号	関係者の認証	発行市町村公開鍵、AP 管理部カード発行者公開鍵、AP 搭載管理者公開鍵
RSA	1024 ビット	セキュアメッセージングで使用するため配送(インポート)されたセッション鍵の復号	暗号通信鍵の配送	住基 AP 鍵配送用復号鍵、AP 管理部鍵配送用復号鍵
RSA	1024 ビット	カード所有者に対する内部認証における認証コード作成のため暗号化	認証コードの作成	CD 管理部カード秘密鍵、AP 管理部カード秘密鍵
RSA	1024 ビット	テンポラリ公開鍵に対する証明書の検証	証明書の検証	鍵管理用公開鍵、証明書検証用公開鍵
RSA	1024 ビット	AP 管理部におけるカード発行者と AP 搭載管理者の公開鍵に対する証明書の検証	証明書の検証	証明書発行局の公開鍵
RSA	1024 ビット	業務用端末の外部認証のため業務用端末の秘密鍵で暗号化された認証コードの復号	業務用端末の認証	テンポラリ公開鍵
Triple-DES	168 ビット	インポートされた CD 管理部カード秘密鍵の復号	データの秘匿	インポート用鍵
Triple-DES	168 ビット	セキュアメッセージングにおけるコマンドの復号およびレスポンスの暗号化	データの秘匿	住基 AP セッション鍵
Triple-DES	112 ビット	セキュアメッセージングにおけるコマンドの復号およびレスポンスの暗号化	データの秘匿	固定鍵、AP 管理部セッション鍵

(注釈) 鍵配送用暗号鍵と鍵配送用復号鍵は、それぞれ RSA 暗号における公開鍵と秘密鍵に対応し、住基 AP と AP 管理部で別の鍵を利用する。また、カード秘密鍵は TOE 外部からカード所有者の認証における認証コード作成のために使用され、TOE はカード秘密鍵を使用した暗号操作の機能を持っているが、本 ST において TOE の想定する資産保護のために何らセキュリティ機能を提供するものではない。AP 管理部カード秘密鍵は、AP 管理部鍵配送用復号鍵と同一である。

3. TOE セキュリティ環境

本章では、TOE のセキュリティ環境として、資産、前提条件、脅威と組織のセキュリティ方針について記述する。

3.1 資産

住基カードは、種々の生産工程を経て作られる。本 ST では、市町村に納入される住基カード内の TOE が守るべきデータおよび守るための手段となるデータを資産として以下に定義する。

TOE が守る利用者データは、以下の通りである。

・市町村が個別に設定する市町村データ
・製造者が設定するカード種別識別データおよびカード管理データ
・本人確認の業務で使われる住民票コード
・外部からのカード認証で利用される CD 管理部カード秘密鍵
・鍵配送でインポートされる住基 AP セッション鍵および AP 管理部セッション鍵
・住基 AP セッション鍵の配送に先立ち外部へ配付される住基 AP 鍵配送用暗号鍵
・AP 管理部セッション鍵の配送に先立ち外部へ配付される AP 管理部鍵配送用暗号鍵
・住基カードに市町村が搭載するアプリケーション

(注釈) 市町村データにはカード種別識別子、カード発行番号、市町村コード、有効期限が含まれる。カード種別識別データにはソフトウェア種別識別データ、OS 種別データが含まれる。カード管理データにはカード種別、ハードウェア種別、最大利用可能サイズが含まれる。

また、これらのデータを守るため、TOE は以下の TSF データ(認証データやセキュリティ属性等)を利用する。

・TOE 関係者を認証（本人認証）するために利用される CD 管理部輸送 PIN、CD 管理部仮 PIN、CD 管理部所有者 PIN、CD 管理部独自利用 PIN、住基 AP 仮 PIN、住基 AP 所有者 PIN、および AP 管理部輸送 PIN
・外部ノードを認証するための利用される発行市町村公開鍵、AP 管理部カード発行者公開鍵、AP 搭載管理者公開鍵
・テンポラリ公開鍵に対する証明書の検証で利用される証明書検証用公開鍵および鍵管理用公開鍵
・AP 管理部におけるカード発行者と AP 搭載管理者の公開鍵に対する証明書の検証で利用される証明書発行局の公開鍵
・業務用端末の外部認証のため業務用端末の秘密鍵で暗号化された認証コードの復号で利用されるテンポラリ公開鍵
・インポートされた CD 管理部カード秘密鍵の復号で利用されるインポート用鍵

・配付されたセッション鍵を復号するための住基 AP 鍵配送用復号鍵および AP 管理部鍵配送用復号鍵
・セキュアメッセージングの暗号化と復号で利用される固定鍵

3.2 前提条件

本節では、TOE がセキュリティ機能を発揮できるために、前提となる事柄について記述する。前提条件は、以下の通りである。

1) **A.CARD_SET_Data**：

TOE がカード所有者に渡されるまでに、カード発行者または AP 搭載管理者である市町村は、利用者データや認証データおよび TOE の動作で必要となる情報を、TOE に設定する。それらのデータは人的側面において、市町村の責任で安全な値が指定され、教育と訓練を受けた職員により正しく設定され、安全に管理されるものとする。また、物理的側面として、TSF データの設定/利用時には、TSF データを安全に管理できる IT 装置(カードリーダ・ライタや業務用端末)を市町村は調達し、市町村の安全な環境で使用するものとする。また、カード所有者である住民は、推測されにくい適切な PIN を設定するものとする。

3.3 脅威

TOE を利用する上で想定される脅威は、以下の通りである。

住基カードを交付された住民は、そこに格納された住民票コードを基に、市町村が管理している個人情報（本人確認情報：氏名、生年月日、性別、住所、住民票コード、付随情報）へアクセスし、各種の行政サービスを受ける。このような便利なカードは、様々な動機を持った人から、以下に示すような様々な攻撃を受けると想定され、カード発行を受けた住民はプライバシー侵害だけでなく、財産的な損害を受ける恐れがある。

1) **T.Logical_Attack**：

市町村に納入された住基カードは、住基カードの記憶素子へ、発行市町村データや住民票コード設定、住基カードへの券面印刷等の工程を経て、市町村から住民に交付され、利用される。この一連の過程の住基カードに対し、IC カードの技術に詳しい攻撃者が、住民基本台帳カード仕様で規定する論理的インタフェース(コマンド/レスポンス)を悪用し、利用者データや TSF データを改ざんしたり、盗んだりする。

2) **T.Illegal_Term_Use**：

住民基本台帳ネットワークで使われる業務用端末の操作に詳しい正規の職員以外の攻撃者が業務用端末を悪用したり、業務用端末に改造を行なったりして、住基カードとやり取りされるデータへ不正にアクセスし、利用者データや TSF データを改ざんしたり、盗んだりする。

3) **T.Disturb_APL**：
住基カードには多くのアプリケーションが存在する。即ち、本人確認業務アプリケーション、市町村によってロードされる市町村独自のアプリケーションである。このような複数のアプリケーションが存在する住基カード内で、市町村独自のアプリケーションが利用者データを改ざんしたり、盗んだりする。

4) **T.Environment**：
住基カードを使っている時に電源断が発生し、データの書換えが中断されることがある。その後、再度、住基カード使おうとした時、住基カード内の利用者データや TSF データが正しく書換わっていないことがある。

5) **T.Incomplete**：
市町村に納入された住基カードが住民に交付されるまでに、様々な利用者データや TSF データの設定が行われる。このような利用者データや TSF データが設定された、交付前の住基カードを不正に入手した攻撃者が、正規に発行された住基カードとして、悪用する。

6) **T.Hardware**：
半導体や暗号の技術に詳しい攻撃者は､以下に述べるハードウェア攻撃手段を使い TOE の資産の盗聴や改ざんもしくは秘密(Secret)の推測を行なうかも知れない。

・FIB(Focused Ion Beam) workstation, EBP(Electron Beam Prober), AFM(Automatic Force Microscope)を利用し、演算回路、記憶素子の物理的改ざん、盗聴（i.e. TOE 自体や TSF データの改ざん、TSF データの盗聴）
・ハードウェアの処理状況を分析することで、TSF データを推定
・IC カードを異常な状態で動作させ、その結果を分析し、TSF データを推定

3.4 組織のセキュリティ方針

TOE を利用する組織に対する組織のセキュリティ方針は、以下の通りである。

住民基本台帳カード仕様書 第 2.3 版（**[住基仕様 23]**）は、住基カードの仕様書であるが、組織のセキュリティポリシと捉えるべき記述があるので、それらの要件を以下に引用する。

(注釈) **[住基仕様 23]**における「セキュリティアトリビュート」および「パスワード」は、本 ST における「アクセス管理属性」および「PIN」にそれぞれ相当する。また、SC3、SC4 は、本 ST における P-5 または P-6、N-4 にそれぞれ相当する。

1) **P.Authentication**：

[住基仕様 23]には、住民票コードの読出条件について、ポリシ的な記述は無い。しかし、7 章 住民カードアプリケーション仕様編 表 8.9 住基カード AP のセキュリティアトリビュート設定から、以下の条件が暗黙的にポリシとして設定されていると考えられる。

・PIN による本人認証が終わっていること(SC3)

・全国センター発行の証明書による市町村認証が終わっていること(SC4)

注) 表 8.9 にはアクセス権限が表されている。住民票コードへのアクセス権は、SC3：PIN による本人認証済で、かつ、SC4：全国センター発行の証明書による市町村認証済が条件になっている。

2) **P.Secret_Setting**：

1 章 概要 2.3 節 住民基本台帳カードの業務要件の(1)に、「カードに秘密鍵を設定する際に、安全な発行方式を採用する」との規定があり、TOE の実装に反映する必要がある。

3) **P.PIN_Initialize**：

1 章 概要 2.3 節 住民基本台帳カードの業務要件の(3)に、「パスワード忘却時にカード再利用に資する目的で、暗証番号初期化の後、利用者の新たなパスワード設定に対応する方式を採用する」との規定があり、TOE の実装に反映する必要がある。

4) **P.Secure_Path**：

7 章 住基カードアプリケーション仕様編 3.4 セキュアメッセージング機能について、「セキュアメッセージング機能は、IC カードと外部装置との間で授受される APDU を不正な盗聴から保護するための暗号化通信を行なう機能である。住基カード AP において、本機能は住民票コード読み出し処理において利用される」との規定があり、TOE の実装に反映する必要がある。

(注釈) APDU(Application Protocol Data Unit)とは、住基カードとカードリーダ・ライタ間でやり取りされるデータの単位で、本 ST では、カードリーダ・ライタから住基カードへの APDU をコマンドメッセージ、住基カードからカードリーダ・ライタへの APDU をレスポンスメッセージと呼んでいる。

4. セキュリティ対策方針

本章では、TOE および TOE 環境に対するセキュリティ対策方針を記述する。
本 ST の TOE および TOE 環境に対するセキュリティ対策方針は、以下の通りである。

4.1 TOE セキュリティ対策方針

本節では、TOE に対するセキュリティ対策方針について記述する。TOE に対するセキュリティ対策方針は、以下の 6 つである。

1) **O.Identification**：
TSF は、CD 管理部利用者、住基 AP 利用者、および AP 管理部利用者を識別する機構を装備しなければならない。

2) **O.AccessManagement**：
TSF は、外部からのコマンドに基づく TOE 内の利用者データと TSF データへのアクセス手段を限定し、TOE が認証したカード発行者、カード所有者、業務用端末、AP 搭載管理者のみがそれぞれの役割に許可された資産へだけアクセスできる機構を備えなければならない。

3) **O.Domain**：
TSF は、市町村独自のアプリケーションから TSF を保護する機構を装備し、また、他のアプリケーション管理下にあるファイルへのアクセスを防止しなければならない。

4) **O.Secure_Path**：
TSF は、カードリーダ・ライタとの通信データに対し、データフォーマットの分析を妨げる機構を備えなければならない。

5) **O.Retention**：
TSF は、住基カード使用中の電源断に対して再起動された時、使用中であった利用者データ、TSF データを復元する機構を備えなければならない。

6) **O.Forgery**：
TSF は、認証された TOE 関係者から指示(住民がパスワードを設定することを含む)があるまで、行政サービスに使えない機構を備えなければならない。

4.2 環境セキュリティ対策方針

本節では、環境に対するセキュリティ対策方針について記述する。

環境に対するセキュリティ対策方針は、以下の 4 つである。

1) **OE.CARD_SET_Data**：

TOE がカード所有者に渡されるまでに、カード発行者または AP 搭載管理者である市町村は、安全な値を TOE に正しく設定し､安全に管理することができるように職員の教育と訓練を実施しなければならない。また、市町村は、カード所有者である住民が適切な PIN を設定するように指導しなければならない。

2) **OE.Term_TSF**：

カードリーダ・ライタおよび業務用端末は、住基カードが認証で用いる TSF データを安全に管理するため、認証の際に入力された PIN を処理が終わると消去し、住基カードから読み出された住民票コードを漏洩から保護するため、利用後に消去する。

3) **OE.Term_Mgt**：

業務用端末は市町村の安全な環境で使用され、業務用端末上で動作するソフトウェアは、TOE 関係者を認証してアクセス制御を実施し、正規の職員によって起動された場合にのみ業務用端末の秘密鍵を利用可能とする。

4) **OE.Hardware**：

TOE は、半導体や暗号の技術に詳しい攻撃者が行なう以下に示す攻撃に耐えうる安全なハードウェア上で動作する。ハードウェアはこれらを保証するシャープ(株)製の SM4148 IC カード LSI を利用する。

・FIB(Focused Ion Beam) workstation, EBP(Electron Beam Prober), AFM(Atomic Force Microscope)を利用し、演算回路、記憶素子の物理的改ざん、盗聴（i.e. TOE 自体や TSF データの改ざん、TSF データの盗聴）
・ハードウェアの処理状況を分析することで、TSF データを推定
・IC カードを異常な状態で動作させ、その結果を分析し、TSF データを推定

5. IT セキュリティ要件

本章では、セキュリティ機能要件とセキュリティ保証要件を記述する。これらの要件は、それぞれ、CC Version 2.1 Part2 の機能コンポーネントと Part 3の保証コンポーネントから成っている。

5.1 TOE セキュリティ要件

本節では、TOE に対するセキュリティ機能要件とセキュリティ保証要件について記述する。

5.1.1 TOE セキュリティ機能要件

5.1.1.1 暗号サポート(FCS)

本節は、TOE の暗号サポートセキュリティ要件を規定する。

FCS_CKM.2 暗号鍵配付

下位階層： なし

FCS_CKM.2.1 TSF は、以下の［割付：***住基カードに対する要求仕様 ver.2.3 および AP 管理部に対する要求仕様***］に合致する、指定された暗号鍵配付方法［割付：***セッション鍵設定プロトコル***］に従って、[詳細化：***セッション鍵を配送するための***]暗号鍵を配付しなければならない。

依存性：[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 または
FDP_ITC.2 セキュリティ属性付き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
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4 暗号鍵破棄

下位階層： なし

FCS_CKM.4.1 TSF は、以下の［割付：***標準なし***］に合致する、指定された暗号鍵廃棄方法［割付：***ゼロクリア***］に従って、[詳細化：***揮発性メモリ上にあるインポート用鍵、固定鍵、セッション鍵、鍵配送用復号鍵、およびカード秘密鍵***]を破棄しなければならない。

(注釈) 発行市町村公開鍵、住基 AP 鍵配送用暗号鍵と AP 管理部鍵配送用暗号鍵、鍵管理用公開鍵、証明書検証用公開鍵、テンポラリ公開鍵、証明書発行局の公開鍵、AP 管理部カード発行者公開鍵、AP 搭載管理者公開鍵について、公開鍵のためゼロクリアに従って破棄

する必要はない。

依存性：[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 または
FDP_ITC.2 セキュリティ属性付き利用者データのインポート または
FCS_CKM.1 暗号鍵生成]
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1/T-DES 暗号操作
下位階層： なし

FCP_COP.1.1/T-DES TSF は、［割付：***ANSI X9.52***］に合致する、特定された暗号アルゴリズム［割付：***Triple-DES 暗号***］と暗号鍵長［割付：***112 ビット、168 ビット***］に従って、［割付：***表 5-1で示される暗号操作***］を実行しなければならない。

(注釈) T-DES 暗号処理を実現するための DES 演算機能は TOE の動作する IC カード LSI により提供される。

表 5-1 Triple-DES 暗号の操作

暗号操作	使用する鍵	鍵長
インポートされた CD 管理部カード秘密鍵の復号	インポート用鍵	168 ビット
セキュアメッセージングにおけるコマンドの復号およびレスポンスの暗号化	住基 AP セッション鍵	168 ビット
	固定鍵、 AP 管理部セッション鍵	112 ビット

依存性：[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 または
FDP_ITC.2 セキュリティ属性付き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
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1/RSA 暗号操作
下位階層： なし

FCP_COP.1.1/RSA TSF は、［割付：***PKCS#1***］に合致する、特定された暗号アルゴリズム［割付：***RSA 暗号***］と暗号鍵長［割付：***1024 ビット***］に従って、［割付：***表 5-2で示される暗号操作***］を実行しなければならない。

表 5-2 RSA 暗号の操作

暗号操作	使用する鍵
外部認証時、認証の検証のため、関係者の秘密鍵で暗号化された認証コードの復号	発行市町村公開鍵､AP 管理部カード発行者公開鍵､AP 搭載管理者公開鍵
セキュアメッセージングで使用するため配送(インポート)されたセッション鍵の復号	住基 AP 鍵配送用復号鍵、AP 管理部鍵配送用復号鍵
カード所有者に対する内部認証における認証コード作成のため暗号化	CD 管理部カード秘密鍵、AP 管理部カード秘密鍵
テンポラリ公開鍵に対する証明書の検証	鍵管理用公開鍵、証明書検証用公開鍵
AP 管理部におけるカード発行者と AP 搭載管理者の公開鍵に対する証明書の検証	証明書発行局の公開鍵
業務用端末の外部認証のため業務用端末の秘密鍵で暗号化された認証コードの復号	テンポラリ公開鍵

依存性：[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 または
FDP_ITC.2 セキュリティ属性付き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
FMT_MSA.2 セキュアなセキュリティ属性

5.1.1.2 利用者データ保護 (FDP)

本節は、TOE の利用者データ保護セキュリティ要件を規定する。

FDP_ACC.1 サブセットアクセス制御

下位階層： なし

FDP_ACC.1.1 TSF は、［割付：***表 5-3に示されるサブジェクトとオブジェクトとそれらの間の操作リスト***］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。

表 5-3 TOE におけるサブジェクトとオブジェクトと操作

サブジェクト	オブジェクト	操　作
CD 管理プロセス AP 管理プロセス 住基 AP プロセス	EF(WEF および IEF)	読出し、書込み、書換え
	SD	AP 搭載、AP 選択、AP 削除

《 住基カードアクセス制御 SFP 》

あらかじめ定義されたサブジェクトとオブジェクトと操作に対してのみアクセス制御を実施する。

(注釈) 「書込み」とはデータ領域に初めて値を書込むことを意味し、「書換え」とは既に値

の書込まれたデータ領域の値を書換えることを意味する。

依存性：FDP_ACF.1 セキュリティ属性によるアクセス制御

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

FDP_ACF.1.1 TSF は、以下の［割付：***状態遷移ステータス、認証ステータス、アクセス管理属性***］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。

(注釈) アクセス管理属性は、オブジェクトに対するセキュリティ属性であり、オブジェクト毎にそのオブジェクトに対する各操作で要求される認証ステータスが規定される。

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：***表 5-4～表 5-14 のアクセス制御規則に定義されたサブジェクトからオブジェクトに対して操作を許可される TOE 関係者の認証ステータスに基づき、許可された認証ステータスを満足する TOE 関係者にのみ操作を限定する***］。

(注釈) **表 5-4**～**表 5-14**のアクセス制御規則において、「なし」とはアクセスを許可する認証ステータスが存在せず、「任意」とはどんな認証ステータスでもアクセスが許可されることを意味する。また、「P-x」や「N-x」とはアクセスの許可に必要な認証ステータスを表す。また、「&」は 2 つの認証ステータスが同時に必要なことを表し、「／」はどちらかの認証ステータスだけが必要なことを表す。具体的には**表 5-4**において、サブジェクト(CD 管理プロセス)は状態遷移ステータスが初期化状態の時、認証ステータスが P-1(CD 管理部輸送 PIN による PIN 照合済み)ならば、オブジェクト(市町村データ)に対して読出し、書込みはできるが、書換えは許可されない。オブジェクト(カード種別識別データ)に対してはすべての認証ステータスで読出しできるが、書込みと書換えは許可されない。また、オブジェクト(CD 管理部カード秘密鍵)に対しては認証ステータスが P-1 ならば、読出し、書込み、書換えができる。

表 5-4 CD 管理部におけるアクセス制御規則（初期化状態の場合）

サブジェクト：CD 管理プロセス

オブジェクト(EF)	読出し	書込み	書換え
市町村データ	P-1	P-1	なし
カード種別識別データ	任意	なし	なし
CD 管理部カード秘密鍵	P-1	P-1	P-1

P-1：CD 管理部輸送 PIN による PIN 照合済み(カード発行者)

表 5-5 CD 管理部におけるアクセス制御規則（PIN 設定可能状態の場合）

サブジェクト：CD 管理プロセス

オブジェクト(EF)	読出し	書込み	書換え
市町村データ	なし	なし	なし
カード種別識別データ	任意	なし	なし
CD 管理部カード秘密鍵	なし	なし	なし

表 5-6 CD 管理部におけるアクセス制御規則（カード運用中状態の場合）

サブジェクト：CD 管理プロセス

オブジェクト(EF)	読出し	書込み	書換え
市町村データ	任意	なし	なし
カード種別識別データ	任意	なし	なし
CD 管理部カード秘密鍵	任意	なし	なし

表 5-7 CD 管理部におけるアクセス制御規則（カード廃止状態の場合）

サブジェクト：CD 管理プロセス

オブジェクト(EF)	読出し	書込み	書換え
市町村データ	なし	なし	なし
カード種別識別データ	なし	なし	なし
CD 管理部カード秘密鍵	なし	なし	なし

表 5-8 住基 AP におけるアクセス管理規則（初期化状態の場合）

サブジェクト：住基 AP プロセス

オブジェクト(EF)	読出し	書込み	書換え
住民票コード	P-1	P-1	なし
住基 AP 鍵配送用暗号鍵	P-1	P-1	なし
住基 AP セッション鍵	P-1	なし	P-1

P-1：CD 管理部輸送 PIN による PIN 照合済み(カード発行者)

表 5-9 住基 AP におけるアクセス管理規則（ロック状態の場合）

サブジェクト：住基 AP プロセス

オブジェクト(EF)	読出し	書込み	書換え
住民票コード	なし	なし	なし
住基 AP 鍵配送用暗号鍵	なし	なし	なし
住基 AP セッション鍵	なし	なし	N-4

N-4：住基 AP における鍵管理用公開鍵により証明書が検証された
テンポラリ公開鍵による外部認証済み(業務用端末)

表 5-10 住基 AP におけるアクセス管理規則（AP 選択可能状態の場合）

サブジェクト：住基 AP プロセス

オブジェクト(EF)	読出し	書込み	書換え
住民票コード	P-6 & N-4	なし	なし
住基 AP 鍵配送用暗号鍵	N-4	なし	なし
住基 AP セッション鍵	P-6 & N-4	なし	N-4

P-6：住基 AP 所有者 PIN の照合済み(カード所有者)

N-4：住基 AP における鍵管理用公開鍵により証明書が検証された
テンポラリ公開鍵による外部認証済み(業務用端末)

表 5-11 AP 管理部におけるアクセス制御規則（初期化状態の場合）

サブジェクト：AP 管理プロセス

オブジェクト(SD)	AP 搭載	AP 選択	AP 削除
ルート SD	P-7	任意	P-7
オブジェクト(EF)	読出し	書込み	書換え
カード管理データ	任意	なし	なし
AP 管理部鍵配送用暗号鍵	なし	P-7	P-7
AP 管理部セッション鍵	なし	なし	なし

P-7：AP 管理部輸送 PIN の PIN 照合済み(カード発行者)

表 5-12 AP 管理部におけるアクセス制御規則（初期化済み状態の場合）

サブジェクト：AP 管理プロセス

オブジェクト(SD)	AP 搭載	AP 選択	AP 削除
ルート SD	P-7	任意	P-7
オブジェクト(EF)	読出し	書込み	書換え
カード管理データ	任意	なし	なし
AP 管理部鍵配送用暗号鍵	なし	P-7	P-7
AP 管理部セッション鍵	なし	なし	なし

P-7：AP 管理部輸送 PIN の PIN 照合済み(カード発行者)

表 5-13 AP 管理部におけるアクセス制御規則（運用中状態の場合）

サブジェクト：AP 管理プロセス

オブジェクト(SD)	AP 搭載	AP 選択	AP 削除
ルート SD	N-2／N-5	任意	N-2／N-5
オブジェクト(EF)	読出し	書込み	書換え
カード管理データ	任意	なし	なし
AP 管理部鍵配送用暗号鍵	任意	なし	なし
AP 管理部セッション鍵	N-2／N-5	なし	N-2／N-5

N-2：AP 管理部におけるカード発行者の公開鍵による外部認証済み(カード発行者)

N-5：AP 管理部における AP 搭載管理者の公開鍵による外部認証済み(AP 搭載管理者)

表 5-14 AP 管理部におけるアクセス制御規則（終結状態の場合）

サブジェクト：AP 管理プロセス

オブジェクト(SD)	AP 搭載	AP 選択	AP 削除
ルート SD	なし	なし	なし
オブジェクト(EF)	読出し	書込み	書換え
カード管理データ	なし	なし	なし
AP 管理部鍵配送用暗号鍵	なし	なし	なし
AP 管理部セッション鍵	なし	なし	なし

FDP_ACF.1.3 TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない***：***［割付：***なし***］。

FDP_ACF.1.4 TSF は、［割付：***なし***］に基いて、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。

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_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

FDP_ITC.1.1 TSF は、SFP に従って制御され、TSC 外から利用者データ[詳細化：***である CD 管理部カード秘密鍵、住基 AP セッション鍵、AP 管理部セッション鍵、住基 AP 鍵配送用暗号鍵、および AP 管理部鍵配送用暗号鍵***]をインポートするときは、［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、TSC 外からインポートされるとき、利用者データ[詳細化：***である CD 管理部カード秘密鍵、住基 AP セッション鍵、AP 管理部セッション鍵、住基 AP 鍵配送用暗号鍵、および AP 管理部鍵配送用暗号鍵***]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、SFP に従って制御され、TSC 外から利用者データ[詳細化：***である CD 管理部カード秘密鍵、住基 AP セッション鍵、AP 管理部セッション鍵、住基 AP 鍵配送用暗号鍵、および AP 管理部鍵配送用暗号鍵***]をインポートするときは、以下の規則を実施しなければならない：
［割付：***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

5.1.1.3 識別と認証(FIA)

本節は、TOE の識別と認証セキュリティ要件を規定する。

FIA_AFL.1/VERIFY 認証失敗時の取り扱い

下位階層： なし

FIA_AFL.1.1/VERIFY TSF は、［割付：***PIN 照合***］に関して、［割付：***連続 3***］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/VERIFY 不成功の認証試行が定義された回数に達するか上回ったとき、TSF は、［割付：***対象の PIN の状態遷移ステータスを閉塞状態に変更して認証への利用の停止し、カード発行者により CD 管理部仮 PIN または住基 AP 仮 PIN が設定されたとき、CD 管理部仮 PIN または住基 AP 仮 PIN の状態遷移ステータスを通常状態に変更して認証への利用停止の解除し、それ以外では PIN の利用の停止は解除することはできない***］をしなければならない。

依存性：FIA_UAU.1 認証のタイミング

FIA_AFL.1/EXT_AUTH 認証失敗時の取り扱い

下位階層： なし

FIA_AFL.1.1/EXT_AUTH TSF は、［割付：***外部認証***］に関して、［割付：***連続 3***］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/EXT_AUTH 不成功の認証試行が定義された回数に達するか上回ったとき、TSF は、［割付：***外部認証に用いた公開鍵(但し、テンポラリ公開鍵は除く)の状態遷移ステータスを閉塞状態に変更して認証への利用の停止をし、利用の停止は解除することはできない***］をしなければならない。

(注釈) 認証失敗により公開鍵の認証への利用が停止された場合、解除することはできない。

(注釈) テンポラリ公開鍵を用いた外部認証に失敗した場合、テンポラリ公開鍵に対する証明書を検証した公開鍵による認証失敗として取り扱う。

依存性：FIA_UAU.1 認証のタイミング

FIA_ATD.1 利用者属性定義

下位階層： なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリスト［割付：***カレントプロセスの識別情報、認証ステータス***］を維持しなければならない。

依存性：なし

(注釈) カレントプロセスの識別情報とは、現在選択されている動作しているプロセスを識別するための情報である。

FIA_UAU.1 認証のタイミング
下位階層： なし

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：***表 5-4～表 5-14において認証ステータスが「任意」で許可される操作を利用するコマンド(セレクト、輸送 PIN 情報取得、カード種別識別情報取得、カード状態取得、乱数取得、証明書交換)***］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 TSF 調停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。

依存性：FIA_UID.1 識別のタイミング

(注釈) 上記[割付]部分の記述は TOE とのインタフェースにおけるコマンドメッセージのコマンド名であり、各コマンドは以下のような機能の実行を要求する。
セレクト：カード上で動作するプロセスを切り替えるためのコマンド
輸送 PIN 情報取得：輸送 PIN を識別する情報を取得するためのコマンド、
カード種別識別情報取得：カード種別を識別するデータを取得するためのコマンド、
カード状態取得：カードの状態遷移における現在の状態を取得するためのコマンド、
乱数取得：外部認証で利用する乱数を取得するためのコマンド
証明書交換：外部認証で利用する証明書を交換するためのコマンド

FIA_UAU.4 単一使用認証メカニズム
下位階層： なし

FIA_UAU.4.1 TSF は［割付：***外部認証***］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。

依存性：なし

FIA_UAU.5 複数の認証メカニズム

下位階層： なし

FIA_UAU.5.1 TSF は、利用者認証をサポートするため、［割付：***関係者の役割に応じて表 5-15に示す 12 種類の認証メカニズム***］を提供しなければならない。

FIA_UAU.5.2 TSF は、［割付：***表 5-15に示す TOE 関係者の役割に応じた利用者の認証メカニズムの規則***］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 5-15 役割と対応する利用者の認証メカニズムの規則

関係者の役割	対応する利用者の認証メカニズム	認証ｽﾃｰﾀｽ
カード発行者	CD 管理部輸送 PIN による PIN 照合	P-1
	CD 管理部仮 PIN による PIN 照合	P-2
	CD 管理部独自利用 PIN による PIN 照合	P-4
	住基 AP 仮 PIN による PIN 照合	P-5
	CD 管理部における発行市町村公開鍵による外部認証	N-1
	AP 管理部輸送 PIN による PIN 照合	P-7
	AP 管理部におけるカード発行者公開鍵による外部認証	N-2
カード所有者	CD 管理部所有者 PIN による PIN 照合	P-3
	住基 AP 所有者 PIN による PIN 照合	P-6
業務用端末	CD 管理部における証明書検証用公開鍵により証明書が検証されたテンポラリ公開鍵による外部認証	N-3
	住基 AP における鍵管理用公開鍵により証明書が検証されたテンポラリ公開鍵による外部認証	N-4
AP 搭載管理者	AP 管理部における AP 搭載管理者の公開鍵による外部認証	N-5

依存性：なし

(注釈) 認証ステータスとして N-3 が定義されているが、アクセス制御や TSF データの管理においては使用されず、CD 管理部のセキュリティ属性の読出しの許可に使用される。

FIA_UAU.6 再認証

下位階層： なし

FIA_UAU.6.1 TSF は、条件［割付：***他のプロセスから再び住基 AP プロセスがセレクトされた場合：住基 AP の PIN 照合と外部認証について、他のプロセスから再び AP 管理プロセスがセレクトされた場合：AP 管理プロセスの外部認証について、住基 CD プロセスと AP 管理プロセス以外から住基 CD プロセスが再びセレクトされた場合：住基 CD の輸送 PIN、仮 PIN、または所有者 PIN による PIN 照合または発行市町村公開鍵による外部認証以外について、の 3 条件***］のもとで利用者を再認証しなければならない。

依存性：なし

FIA_UID.1 識別のタイミング
下位階層： 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：***セレクト***］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 調停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。

依存性：なし

(注釈) 「セレクト」は TOE とのインタフェースにおけるコマンドメッセージのコマンド名を表し、カード上で動作するプロセスの切り替えを要求するコマンドである。

FIA_USB.1 利用者・サブジェクト結合
下位階層： なし

FIA_USB.1.1 TSF は、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない：［割付：***カレントプロセスの識別情報***］

FIA_USB.1.2 TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない：［割付：***カード起動時の最初のカレントプロセスの識別情報は AP 管理プロセスとする。***］

FIA_USB.1.3 TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない：［割付：***セレクトコマンドによりプロセスが切り替わるときにカレントプロセスの識別情報を変更する。***］

依存性：FIA_ATD.1 利用者属性定義

5.1.1.4 セキュリティ管理（FMT）

本節は、TOE のセキュリティ管理セキュリティ要件を規定する。

FMT_MSA.1/STATUS セキュリティ属性の管理
下位階層： なし

FMT_MSA.1.1/STATUS TSFは、セキュリティ属性［割付：***CD管理部、AP管理部、お***

よび住基APにおける状態遷移ステータス、また、認証で利用されるPINの状態遷移ステータス］に対し［選択：***改変***］をする能力を［割付：***カード発行者***］に制限するために［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。
(注釈) **表 5-16**～**表 5-22**において、「＊」印が付された状態遷移が伴う操作に対して許可された役割に状態遷移ステータスの「改変」する能力を制限する。

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_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MTD.1/IEF　TSF データの管理
下位階層： なし

FMT_MTD.1.1/IEF　TSF は、［割付：***IEF に格納される PIN または鍵***］を［選択：***改変***、［割付：***設定***］］する能力を、［割付：***表 5-16～表 5-26の規則に基づき許可された TOE 関係者の役割***］に制限しなければならない。

(注釈) **表 5-16**～**表 5-26**の管理規則において、「なし」とは操作を許可する認証ステータスが存在しないことを意味する。また、「P-x」や「N-x」とは操作を許可する認証ステータスを表す。また、「／」は 2 つの認証ステータスのどちらかの認証ステータスだけが必要なことを表し、「＊」印は状態遷移を伴う操作を意味する。具体的には**表 5-16**において、状態遷移ステータスが初期化状態の時、認証ステータスが P-1(CD 管理部輸送 PIN による PIN 照合済み)ならば、TSF データ(CD 管理部仮 PIN)に対して改変と設定ができ、TSF データ(独自利用 PIN、発行市町村公開鍵、証明書検証用公開鍵、テンポラリ公開鍵)に対して改変ができるが、それ以外の操作は許可されない。TSF データ(CD 管理部仮 PIN)に対して設定が操作される際に CD 管理部の状態が遷移する。

(注釈) 「改変」は既に設定されている値を変更すること、「設定」は未設定の状態へ戻し新しく値を確定することをそれぞれ意味する。**表 5-16**および**表 5-20**の管理規則において、初期化状態でも「設定」が許可されない TSF データが存在するが、製造者によって IEF 創生時に仮データが設定されているため、「改変」と考える。

(注釈) CD 管理部輸送 PIN、インポート用鍵、固定鍵、および AP 管理部輸送 PIN は、製造時に製造者によってあらかじめ設定されており、AP 管理部輸送 PIN の改変を除き、TOE 関係者によって設定、改変はできない。CD 管理部仮 PIN と CD 管理部所有者 PIN は、CD 管理部 PIN として同じ領域に格納されて管理され、住基 AP 仮 PIN と住基 AP 所有者 PIN は、住基 AP PIN として同じ領域に格納されて管理される。

表 5-16 CD 管理部における IEF の管理規則（初期化状態の場合）

TSF データ(IEF)	改変	設定
CD 管理部 PIN	P-1	P-1＊
独自利用 PIN	P-1	なし
発行市町村公開鍵	P-1	なし
証明書検証用公開鍵	P-1	なし
テンポラリ公開鍵	P-1	なし

P-1：CD 管理部輸送 PIN による PIN 照合済み(カード発行者)

表 5-17 CD 管理部における IEF の管理規則（PIN 設定可能状態の場合）

TSF データ(IEF)	改変	設定
CD 管理部 PIN	P-2＊	なし
独自利用 PIN	なし	なし
発行市町村公開鍵	なし	なし
証明書検証用公開鍵	なし	なし
テンポラリ公開鍵	なし	なし

P-2：CD 管理部仮 PIN による PIN 照合済み(カード発行者)

表 5-18 CD 管理部における IEF の管理規則（カード運用中状態の場合）

TSF データ(IEF)	改変	設定
CD 管理部 PIN	P-3	N-1＊
独自利用 PIN	なし	なし
発行市町村公開鍵	なし	なし
証明書検証用公開鍵	P-4	なし
テンポラリ公開鍵	任意	なし

P-3：CD 管理部所有者 PIN による PIN 照合済み(カード所有者)

P-4：CD 管理部独自利用 PIN による PIN 照合済み(カード発行者)

N-1：CD 管理部における発行市町村公開鍵による外部認証済み(カード発行者)

表 5-19 CD 管理部における IEF の管理規則（カード廃止状態の場合）

TSF データ(IEF)	改変	設定
CD 管理部所有者 PIN	なし	なし
独自利用 PIN	なし	なし
発行市町村公開鍵	なし	なし
証明書検証用公開鍵	なし	なし
テンポラリ公開鍵	なし	なし

表 5-20 住基 AP における IEF の管理規則（初期化状態の場合）

TSF データ(IEF)	改変	設定
鍵管理用公開鍵	P-1	なし
テンポラリ公開鍵	P-1	なし
住基 AP PIN	P-1	P-1＊
住基 AP 鍵配送用復号鍵	P-1	なし

P-1：CD 管理部輸送 PIN による PIN 照合済み(カード発行者)

表 5-21 住基 AP における IEF の管理規則（ロック状態の場合）

TSF データ(IEF)	改変	設定
鍵管理用公開鍵	なし	なし
テンポラリ公開鍵	任意	なし
住基 AP PIN	P-5＊	なし
住基 AP 鍵配送用復号鍵	なし	なし

P-5：住基 AP 仮 PIN の照合済み(カード発行者)

表 5-22 住基 AP における IEF の管理規則（AP 選択可能状態の場合）

TSF データ(IEF)	改変	設定
鍵管理用公開鍵	なし	なし
テンポラリ公開鍵	任意	なし
住基 AP PIN	P-6	N-1＊
住基 AP 鍵配送用復号鍵	なし	なし

N-1：CD 管理部における発行市町村公開鍵による外部認証済み(カード発行者)

P-6：住基 AP 所有者 PIN の照合済み(カード所有者)

表 5-23 AP 管理部における IEF の管理規則（初期化状態の場合）

TSF データ(IEF)	改変	設定
AP 管理部輸送 PIN	P-7	なし
証明書発行局の公開鍵	なし	P-7
AP 管理部カード発行者公開鍵	P-7	P-7
AP 管理部鍵配送用復号鍵	P-7	P-7

P-7：AP 管理部輸送 PIN の PIN 照合済み(カード発行者)

表 5-24 AP 管理部における IEF の管理規則（初期化済み状態の場合）

TSF データ(IEF)	改変	設定
AP 管理部輸送 PIN	P-7	なし
証明書発行局の公開鍵	なし	P-7
AP 管理部カード発行者公開鍵	P-7	P-7
AP 管理部鍵配送用復号鍵	P-7	P-7

P-7：AP 管理部輸送 PIN の PIN 照合済み(カード発行者)

表 5-25 AP 管理部における IEF の管理規則（運用中状態の場合）

TSF データ(IEF)	改変	設定
AP 管理部輸送 PIN	なし	なし
証明書発行局の公開鍵	なし	なし
AP 管理部カード発行者公開鍵	なし	なし
AP 管理部鍵配送用復号鍵	なし	なし

表 5-26　AP 管理部における IEF の管理規則（終結状態の場合）

TSF データ(IEF)	改変	設定
AP 管理部輸送 PIN	なし	なし
証明書発行局の公開鍵	なし	なし
AP 管理部カード発行者公開鍵	なし	なし
AP 管理部鍵配送用復号鍵	なし	なし

依存性：FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MTD.1/STATUS　TSF データの管理
下位階層： なし

FMT_MTD.1.1/STATUS　TSF は、［割付：***CD 管理部、住基 AP、および AP 管理部のそれぞれにおける状態遷移ステータス***］を［選択：***改変***］］する能力を、［割付：***表 5-27～表 5-29の規則に基づき認証ステータスを有する TOE 関係者の役割***］に制限しなければならない。

(注釈) **表 5-27**～**表 5-29**において、表中の記号は状態の遷移に必要な認証ステータスを表す。例えば**表 5-27**において、CD 管理部では現在の状態が「初期化状態」の場合、認証ステータス「P-1」による役割で CD 管理部仮 PIN を設定すると「PIN 設定可能状態」へ遷移することを意味する。

表 5-27　CD 管理部における状態遷移ステータスの管理規則

現在の状態	遷移後の状態	必要な認証ステータス	遷移の条件
初期化状態	PIN 設定可能状態	P-1	CD 管理部仮 PIN の設定
PIN 設定可能状態	カード運用中状態	P-2	CD 管理部所有者 PIN への改変
PIN 設定可能状態	カード廃止状態	P-2	コマンドによる指示
カード運用中状態	PIN 設定可能状態	N-1	CD 管理部仮 PIN の設定
カード運用中状態	カード廃止状態	N-1	コマンドによる指示

P-1：CD 管理部輸送 PIN による PIN 照合済み(カード発行者)
P-2：CD 管理部仮 PIN による PIN 照合済み(カード発行者)
N-1：CD 管理部における発行市町村公開鍵による外部認証済み(カード発行者)

表 5-28　住基 AP における状態遷移ステータスの管理規則

現在の状態	遷移後の状態	必要な認証ステータス	遷移の条件
初期化状態	ロック状態	P-1	住基 AP 仮 PIN の設定
ロック状態	AP 選択可能状態	P-5	住基 AP 所有者 PIN への改変
AP 選択可能状態	ロック状態	N-1	住基 AP 仮 PIN の設定

P-1：CD 管理部輸送 PIN による PIN 照合済み(カード発行者)

P-5：住基 AP 仮 PIN の照合済み(カード発行者)

N-1：CD 管理部における発行市町村公開鍵による外部認証済み(カード発行者)

表 5-29　AP 管理部における状態遷移ステータスの管理規則

現在の状態	遷移後の状態	必要な認証ステータス	遷移の条件
初期化状態	初期化済み状態	P-7	コマンドによる指示
初期化済み状態	運用中状態	P-7	コマンドによる指示
初期化済み状態	終結状態	P-7	コマンドによる指示
運用中状態	終結状態	N-2	コマンドによる指示

P-7：AP 管理部輸送 PIN の PIN 照合済み(カード発行者)

N-2：AP 管理部におけるカード発行者の公開鍵による外部認証済み(カード発行者)

依存性：FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定

下位階層： なし

FMT_SMF.1.1 TSFは、以下のセキュリティ管理機能を行なう能力を持たなければならない。：[割付:***表 5-30の一覧に示されるセキュリティ管理機能***]。

表 5-30　管理機能の一覧

機能要件	管理機能と考えられるアクション	実現する機能要件
FCS_CKM.2	a) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	a) なし
FCS_CKM.4	同上	a) なし
FCS_COP.1/T-DES	予見される管理アクティビティはない。	不要
FCS_COP.1/RSA	予見される管理アクティビティはない。	不要
FDP_ACC.1	予見される管理アクティビティはない。	不要
FDP_ACF.1	a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	a) FMT_MTD.1/IEF
FDP_ITC.1	a) インポートに対して使用される追加の制御規則の改変。	a) なし
FIA_AFL.1/VERIFY	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	a) なし b) なし
FIA_AFL.1/EXT_AUTH	同上	a) なし　b) なし
FIA_ATD.1	a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	a) FMT_MTD.1/STATUS
FIA_UAU.1	a) 管理者による認証データの管理	a) FMT_MTD.1/IEF b) FMT_MTD.1/IEF

	b) 関係する利用者による認証データの管理 c) 利用者が認証される前にとられるアクションリストの管理	c) なし
FIA_UAU.4	予見される管理アクティビティはない。	不要
FIA_UAU.5	a) 認証メカニズムの管理 b) 認証に対する規則の管理	a) なし b) なし
FIU_UAU.6	a) 許可管理者が再認証を要求できる場合、管理に再認証要求を含める。	a) なし
FIA_UID.1	a) 利用者識別情報の管理 b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストの管理	a) なし b) なし
FIA_USB.1	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 b) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を変更できる。	a) なし b) なし
FMT_MSA.1/STATUS	a) セキュリティ属性と相互に影響を及ぼし得る役割のグループの管理	a) なし
FMT_MTD.1/IEF	a) TSF データと相互に影響を及ぼし得る役割のグループの管理	a) なし
FMT_MTD.1/STATUS	同上	a) なし
FMT_SMF.1	予見される管理アクティビティはない。	不要
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理	a) なし
FPT_RCV.2	a)メンテナンスモードにおける修復能力に誰がアクセスできるかの管理 b) 自動的な手順で処理される障害/サービス中断のリストの管理	a) なし b) なし
FPT_RVM.1	予見される管理アクティビティはない。	不要
FPT_SEP.1	予見される管理アクティビティはない。	不要
FTP_ITC.1	a) もしサポートされていれば、高信頼チャネルを要求するアクションの設定	a) なし

依存性：なし

FMT_SMR.1 セキュリティ役割

下位階層： なし

FMT_SMR.1.1 TSFは、役割［割付：***カード発行者、カード所有者、業務用端末、AP搭載管理者***］を維持しなければならない。

FMT_SMR.1.2 TSF は、[詳細化：***表 5-15の認証メカニズムによる認証結果に基づき、***]利用者を役割に関連付けなければならない。

依存性：FIA_UID.1 識別のタイミング

5.1.1.5 TSF の保護(FPT)

本節は、TSF の保護セキュリティ要件を規定する。

FPT_RCV.2 自動回復

下位階層： FPT_RCV.1

FPT_RCV.2.1 ［割付：***データ書込み時の電源断発生、コマンド中断、または通信異常の理由による異常終了***］からの自動回復が不可能な場合、TSF はセキュアな状態に戻す能力が提供されるメンテナンスモードに移らなければならない。

(注釈) TSF は、自動化された手順により必ずセキュアな状態へ回復されるため、メンテナンスモードに移ることはない。

FPT_RCV.2.2 ［割付：***データ書込み時の電源断発生、コマンド中断、または通信異常の理由による異常終了***］に対し、TSF は、自動化された手順による TOE のセキュアな状態への復帰を保証しなければならない。

依存性：AGD_ADM.1 管理者ガイダンス
ADV_SPM.1 非形式的 TOE セキュリティ方針モデル

FPT_RVM.1 TSP の非バイパス性

下位階層： なし

FPT_RVM.1.1 TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性：なし

FPT_SEP.1 TSF ドメイン分離

下位階層： なし

FPT_SEP.1.1 TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2 TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性：なし

5.1.1.6 高信頼パス／チャネル(FTP)

本節は、高信頼パス／チャネルセキュリティ要件を規定する。

FTP_ITC.1 TSF 間高信頼チャネル

下位階層： なし

FTP_ITC.1.1 TSF は、それ自身とリモート高信頼 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：***リモート高信頼 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：***セキュアメッセージングが要求される機能、CD 管理部カード秘密鍵のインポート、個人識別情報の読み出し、AP 搭載***］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。

依存性：なし

5.1.2 最小機能強度宣言

本 ST の TOE に対する最小機能強度を SOF-基本とする。TOE セキュリティ機能要件で順列的または確率的なメカニズムを含む機能が対象となる。なお、暗号アルゴリズムの機能強度は評価対象外である。

5.1.3 TOE セキュリティ保証要件

本節では、TOE セキュリティ保証要件について記述する。

TOE に要求されるセキュリティ保証要件のコンポーネントを表 5-31に示す。EAL4 のセキュリティ保証要件に AVA_MSU.3 が追加されている。

表 5-31 TOE 保証要件

クラス	コンポーネント	名前
構成管理	ACM_AUT.1	部分的な CM 自動化
	ACM_CAP.4	生成の支援と受入手続き
	ACM_SCP.2	問題追跡の CM 範囲
配付と運用	ADO_DEL.2	改変の検出
	ADO_IGS.1	設置、生成、及び立上げ手順
開発	ADV_FSP.2	完全に定義された外部インタフェース
	ADV_HLD.2	セキュリティ実施上位レベル設計
	ADV_IMP.1	TSF の実装のサブセット
	ADV_LLD.1	記述的下位レベル設計
	ADV_RCR.1	非形式的対応の実証
	ADV_SPM.1	非形式的なセキュリティ方針モデル
ガイダンス文書	AGD_ADM.1	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ライフサイクルサポート	ALC_DVS.1	セキュリティ手段の識別
	ALC_LCD.1	開発者によるライフサイクルモデルの定義
	ALC_TAT.1	明確に定義された開発ツール
テスト	ATE_COV.2	カバレージの分析
	ATE_DPT.1	テスト：上位レベル設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト－サンプル
脆弱性分析	AVA_MSU.3	セキュアでない状態の分析とテスト
	AVA_SOF.1	TOE セキュリティ機能強度評価
	AVA_VLA.2	独立脆弱性テスト

5.2 IT 環境セキュリティ要件

5.2.1 IT 環境セキュリティ機能要件

IT 環境に対するセキュリティ機能要件は存在しない。

6. TOE 要約仕様

本章では、TOE の要約仕様について記述する。

6.1 IT セキュリティ機能

表 6-1に**5.1.1** 節で記述した TOE のセキュリティ機能要件を実現するための TOE セキュリティ機能仕様との対応付けを示す。対応する部分を○で示している。

表 6-1 セキュリティ機能要件と TOE 要約仕様の対応

	セキュリティ機能要件 ＼ TOE 要約仕様	SF.ACCESS_MANAGEMENT	SF.AUTHENTICATE	SF.SECURE_MESSAGING	SF.MANAGEMENT	SF.DOMAIN	SF.RETENTION
1	FCS_CKM.2			○			
2	FCS_CKM.4			○			
3	FCS_COP.1/T-DES			○			
4	FCS_COP.1/RSA		○	○			
5	FDP_ACC.1	○					
6	FDP_ACF.1	○					
7	FDP_ITC.1	○					
8	FIA_AFL.1/VERIFY		○				
9	FIA_AFL.1/EXT_AUTH		○				
10	FIA_ATD.1	○	○		○		
11	FIA_UAU.1		○				
12	FIA_UAU.4		○				
13	FIA_UAU.5		○				
14	FIA_UAU.6		○				
15	FIA_UID.1		○				
16	FIA_USB.1	○	○				
17	FMT_MSA.1/STATUS	○			○		
18	FMT_MTD.1/IEF	○					
19	FMT_MTD.1/STATUS				○		
20	FMT_SMF.1	○			○		
21	FMT_SMR.1	○	○		○		
22	FPT_RCV.2						○
23	FPT_RVM.1	○	○	○	○	○	○
24	FPT_SEP.1	○	○		○	○	
25	FTP_ITC.1			○			

6.1.1 アクセス管理機能

SF.ACCESS_MANAGEMENT

TOE の資産は CD 管理領域、住基 AP 領域、AP 管理領域の 3 つのいずれかに置かれ、それぞれ CD 管理部、住基 AP、および AP 管理部だけがアクセスできるように **SF.DOMAIN** によりドメインが分離されている。各ドメインには実行形式のモジュールとモジュールが扱うデータ領域が割り当てられる。各ドメインに存在するモジュールからは同一ドメイン内のデータはアクセス可能であるが、他のドメインのデータへのアクセスはできない。

CD 管理部、住基 AP、および AP 管理部は、データの格納領域として、**表 6-2**のようなファイル構造をとる。

表 6-2 データの格納領域

EF	WEF	レコード構造のデータ
	IEF	PIN／鍵

基礎ファイル EF の中に、作業で利用するデータをレコード構造で格納する WEF ファイルと PIN や鍵を格納する IEF ファイルが存在し、各ファイルにアクセス管理属性などの属性情報が設定される。SE と呼ばれる認証や暗号化で利用する鍵を指定するためのセキュリティ属性は WEF に格納される。

SF.ACCESS_MANAGEMENT は、WEF および IEF に格納されたすべての利用者データに対するアクセス制御とすべての TSF データに対する管理を実施する。利用者データに対するアクセス制御と TSF データに対する管理を合わせてここではアクセス管理と表現する。

TOE におけるアクセス管理の仕組みは、アクセス管理属性で定義され、認証条件と状態と操作からなる。アクセス管理属性はカード製造者によって設定され、TOE 利用時に変更することはできない。

アクセス管理属性

1) アクセス管理に必要な認証条件を認証ステータスと呼ぶセキュリティ属性で定義する。
   利用者の認証による TOE 関係者の認証条件を規定する。
2) TOE 関係者の認証条件を満たす役割が実行可能な状態を定義する。

SF.ACCESS_MANAGEMENT は、このアクセス管理属性を独立した CD 管理領域、住基 AP 領域、AP 管理領域において、利用者の認証条件と状態を満たすか確認し、満たす場合は利用者データが格納されるオブジェクトまたは TSF データに対する規定された操作を実行する。また、**SF.ACCESS_MANAGEMENT** に先立ち、**SF.AUTHENTICATE** により TOE の利用者の識別と認証が行われ、カレントプロセスの識別情報が利用者とサブジェクトを関連付け、認証ステータスが利用者の役割を特定する。

SF.MANAGEMENT により CD 管理部、住基 AP、および AP 管理部の各モジュールの独立した状態が維持され、定義した状態において許可された役割により特定の制御がおこなわれると状態が遷移する。

利用者データに対するアクセス制御の操作は「読出し」、「書込み」、「書換え」の 3 種類である。「書込み」とはデータ領域に初めて値を書込むことを意味し、「書換え」とは既に値の書込まれた

データ領域の値を書換えることを意味する。

IEF に格納された TSF データの管理の操作は「改変」、「設定」の 2 種類である。「改変」は既に設定されている値を変更すること、「設定」は未設定の状態へ戻し新しく値を確定することをそれぞれ意味する。

AP 管理部は、AP の搭載領域として SD の構造をとる。SD に対する操作は「AP 搭載」、「AP 選択」、「AP 削除」の 3 種類である。

以上のアクセス管理に関する規則をまとめたものを**表 6-3**～**表 6-5**に示す。表は各モジュールの各状態における利用者データの格納されたオブジェクトと TSF データに対し、表中の認証ステータスを得た TOE 関係者の役割によって許可される操作を表す。ただし、「－」は許可される操作がないことを表す。例えば、**表 6-3**において、初期化状態の CD 管理部において、認証ステータス「任意」によりすべての TOE 関係者はカード種別識別データに対して「読出し」操作ができ、認証ステータス P-1 を得たカード発行者は、市町村データに対して「読出し」と「書込み」、カード種別識別データに対して「読出し」、CD 管理部カード秘密鍵に対して「読出し」、「書込み」、「書換え」ができ、CD 管理部 PIN に対して「設定」と「改変」、そして独自利用 PIN、発行市町村公開鍵、証明書検証用公開鍵、テンポラリ公開鍵に対して「改変」の操作ができることを表す。

表 6-3　CD 管理部におけるアクセス管理

			オブジェクト			TSF データ				
状態	関係者の役割	認証ｽﾃｰﾀｽ	市町村データ	ｶｰﾄﾞ種別識別ﾃﾞｰﾀ	CD 管理部カード秘密鍵	CD 管理部 PIN	独自利用 PIN	発行市町村公開鍵	証明書検証用公開鍵	テンポラリ公開鍵
初期化状態	TOE 関係者	任意	－	読出し	－	－	－	－	－	－
	カード発行者	P-1	読出し 書込み	読出し	読出し 書込み 書換え	CD 管理部仮 PIN の設定と改変	改変	改変	改変	改変
PIN 設定可能状態	TOE 関係者	任意	－	読出し	－	－	－	－	－	－
	カード発行者	P-2	－	読出し	－	CD 管理部所有者 PIN への改変	－	－	－	－
カード運用中状態	TOE 関係者	任意	読出し	読出し	読出し	－	－	－	－	改変
	カード所有者	P-3	読出し	読出し	読出し	CD 管理部所有者 PIN の改変	－	－	－	改変
	カード発行者	P-4	読出し	読出し	読出し	－	－	－	改変	改変
	カード発行者	N-1	読出し	読出し	読出し	CD 管理部仮 PIN の設定	－	－	－	改変
カード廃止状態	TOE 関係者	任意	－	－	－	－	－	－	－	－

P-1：CD 管理部輸送 PIN による PIN 照合済み(カード発行者)

P-2：CD 管理部仮 PIN による PIN 照合済み(カード発行者)

P-3：CD 管理部所有者 PIN による PIN 照合済み(カード所有者)

P-4：CD 管理部独自利用 PIN による PIN 照合済み(カード発行者)

N-1：CD 管理部における発行市町村公開鍵による外部認証済み(カード発行者)

表 6-4　住基 AP におけるアクセス管理

			オブジェクト			TSF データ			
状態	関係者の役割	認証ｽﾃｰﾀｽ	住民票コード	住基 AP 鍵配送用暗号鍵	住基 AP ｾｯｼｮﾝ鍵	鍵管理用公開鍵	テンポラリ公開鍵	住基 AP PIN	住基 AP 鍵配送用復号鍵
初期化状態	TOE 関係者	任意	－	－	－	－	－	－	－
	カード発行者	P-1	読出し書込み	読出し書込み	読出し書換え	改変	改変	住基 AP 仮 PIN の設定と改変	改変
ロック状態	TOE 関係者	任意	－	－	－	－	改変	－	－
	カード発行者	P-5	－	－	－	－	改変	住基 AP 所有者 PIN への改変	－
	業務用端末	N-4	－	－	書換え	－	改変	－	－
AP 選択可能状態	TOE 関係者	任意	－	－	－	－	改変	－	－
	カード発行者	N-1	－	－	－	－	改変	住基 AP 仮 PIN の設定	－
	業務用端末	N-4	－	読出し	書換え	－	改変	－	－
	カード所有者	P-6	－	－	－	－	改変	住基 AP 所有者 PIN の改変	－
	業務用端末とカード所有者	N-4 & P-6	読出し	読出し	読出し書換え	－	改変	住基 AP 所有者 PIN の改変	－

P-1：CD 管理部輸送 PIN による PIN 照合済み(カード発行者)

P-5：住基 AP 仮 PIN の照合済み(カード発行者)

P-6：住基 AP 所有者 PIN の照合済み(カード所有者)

N-1：CD 管理部における発行市町村公開鍵による外部認証済み(カード発行者)

N-4：住基 AP における鍵管理用公開鍵により証明書が検証されたテンポラリ公開鍵による外部認証済み(業務用端末)

表 6-5　AP 管理部におけるアクセス管理

			オブジェクト				TSF データ			
状態	関係者の役割	認証ｽﾃｰﾀｽ	ルート SD	カード管理データ	AP 管理部鍵配送用暗号鍵	AP 管理部ｾｯｼｮﾝ鍵	AP 管理部輸送 PIN	証明書発行局の公開鍵	AP 管理部カード発行者公開鍵	AP 管理部鍵配送用復号鍵
初期化状態	TOE 関係者	任意	AP 選択	読出し	－	－	－	－	－	－
	カード発行者	P-7	AP 搭載 AP 選択 AP 削除	読出し	書込み 書換え	－	改変	設定	設定 改変	設定 改変
初期化済み状態	TOE 関係者	任意	AP 選択	読出し	－	－	－	－	－	－
	カード発行者	P-7	AP 搭載 AP 選択 AP 削除	読出し	書込み 書換え	－	改変	設定	設定 改変	設定 改変
運用中状態	TOE 関係者	任意	AP 選択	読出し	読出し	－	－	－	－	－
	カード発行者	N-2	AP 搭載 AP 選択 AP 削除	読出し	読出し	読出し 書換え	－	－	－	－
	AP 搭載管理者	N-5	AP 搭載 AP 選択 AP 削除	読出し	読出し	読出し 書換え	－	－	－	－
終結状態	TOE 関係者	任意	－	－	－	－	－	－	－	－

P-7：AP 管理部輸送 PIN の PIN 照合済み(カード発行者)

N-2：AP 管理部におけるカード発行者の公開鍵による外部認証済み(カード発行者)

N-5：AP 管理部における AP 搭載管理者の公開鍵による外部認証済み(AP 搭載管理者)

6.1.2　識別と認証機能

SF.AUTHENTICATE

SF.AUTHENTICATE は、セレクトコマンドにより CD 管理部、AP 管理部、または住基 AP の内の 1 つが選択される際に、利用者を識別する。識別された利用者と利用者を代行して動作するプロセスはカレントプロセスの識別情報で関連付けられ、カレントプロセスの識別情報はセレクトコマンドで変更され、カード起動時の最初は AP 管理プロセスとなる。**SF.AUTHENTICATE** は、CD 管理プロセス、住基 AP プロセス、および AP 管理プロセスの各プロセスが代行している利用者を認証するため、PIN 照合および外部認証を行なう。また、**SF.AUTHENTICATE** は、利用者の識別なしにセレクトコマンドの実行だけを許可し、利用者の認証なしにセレクト、輸送 PIN 情報取得、カード種別識別情報取得、カード状態取得、乱数取得、証明書交換のコマンドの実行を許可する。

PIN 照合：

業務用端末から TOE 内の PIN 情報格納 IEF を指定し、利用者の PIN を送信する。**SF.AUTHENTICATE** は、受信した利用者の PIN と指定された PIN 情報格納 IEF の PIN と照合し、一致した場合には、認証ステータスを対象の PIN による PIN 照合済とする。なお、PIN 照合は 3～16[byte]の PIN を取り扱う。(PIN 情報格納 IEF に PIN をインポートするのは **SF.ACCESS_MANAGEMENT** にて行なう。)

外部認証：

利用者の公開鍵と秘密鍵ペアを使用し、TOE が生成した乱数を業務用端末において利用者の秘密鍵で正しく暗号化することを、TOE 内の IEF に保管された公開鍵を利用し、利用者を以下のように認証する。

(1) TOE は乱数を生成し業務用端末に送信する。

(2)業務用端末は、対応する秘密鍵により乱数を暗号化して認証コードとして TOE に送信する。

(3) **SF.AUTHENTICATE** は、受信した認証コードを CD 管理プロセスあるいは住基 AP プロセスにおいて、秘密鍵に対応する公開鍵で復号し乱数と比較し、一致した場合、認証ステータスを復号に用いた公開鍵による外部認証済とする。

外部認証において TOE 内の公開鍵には、あらかじめ IEF に格納された関係者に対応する公開鍵を使用する場合と、業務用端末が業務用端末の公開鍵に署名を付した証明書を TOE に送信し（証明書検証コマンド）、TOE は受信した証明書を検証後公開鍵（テンポラリ公開鍵）として使用する場合がある。（鍵管理用公開鍵やテンポラリ公開鍵の改変は **SF.ACCESS_MANAGEMENT** にて行なう。）

証明書を検証するため業務用端末は秘密鍵を持ち、住基 CD では秘密鍵に対応する証明書検証用公開鍵を利用し、住基 AP では秘密鍵に対応する鍵管理用公開鍵を利用する。

SF.AUTHENTICATE の外部認証において行なわれる暗号操作と使用される鍵を**表 6-6**に示す。

表 6-6 外部認証において行なわれる暗号操作と使用される鍵

暗号操作	使用する鍵	アルゴリズム	鍵長
外部認証時、認証の検証のため、関係者の秘密鍵により暗号化された認証コードの復号	発行市町村公開鍵、AP管理部カード発行者公開鍵、AP搭載管理者公開鍵	RSA	1024ビット
テンポラリ公開鍵に対する証明書の検証	鍵管理用公開鍵、証明書検証用公開鍵	RSA	1024ビット
業務用端末の外部認証のため業務用端末の秘密鍵で暗号化された認証コードの復号	テンポラリ公開鍵	RSA	1024ビット

暗号化および復号で利用する暗号機能として、PKCS#1 に合致した RSA 暗号を提供する。

各 PIN および公開鍵(但し、テンポラリ公開鍵は除く)には、試行回数許容値が設定されており、またカード内に格納されている PIN あるいは公開鍵を用いた PIN 照合および外部認証に対し、正常終了するまでの連続失敗回数をエラーカウンタとして保持する。テンポラリ公開鍵を用いた

外部認証に失敗した場合、テンポラリ公開鍵に対する証明書を検証した公開鍵による認証失敗として取り扱う。試行回数許容値には、試行可能回数の上限値、あるいは上限値なしが設定される。試行回数許容値として製造者によってあらかじめ「3 回」が設定され、TOE 関係者による変更は不可能である。そして、エラーカウンタの値がこの上限値に達した場合に対象の鍵あるいは PIN を閉塞状態とする。閉塞状態となった鍵による認証は不可能となる。PIN および公開鍵の状態遷移はそれぞれ独立して管理され、カード発行時におけるデフォルトの値は通常状態であり、エラーカウンタのデフォルトの値は 0 である。CD 管理部のカード運用中状態においてカード発行者が CD 管理部仮 PIN を設定した時、および住基 AP の AP 選択可能状態においてカード発行者が住基 AP 仮 PIN を設定した時、該当する CD 管理部仮 PIN または住基 AP 仮 PIN の状態遷移ステータスは通常状態へ戻され、認証への利用が可能となる。それ以外の PIN および公開鍵がひとたび閉塞状態となると、通常状態へ戻すことはできない。

CD 管理部、住基 AP、および AP 管理部における認証ステータスは、PIN 照合あるいは外部認証の結果を保持する情報で、表 6-7の規則に従って管理する。認証ステータスは状態が遷移した場合も維持する。結果として、住基 AP 部が再選択された場合、PIN 照合と外部認証に対して再認証が必要となり、AP 管理部が再選択された場合、外部認証に対して再認証が必要となる。

表 6-7 認証ステータスの管理規則

1.	CD 管理部における輸送 PIN、仮 PIN、または所有者 PIN による PIN 照合または発行市町村公開鍵による外部認証により確立した認証ステータスは、カードが非活性化されるまで有効である。それ以外の PIN 照合または外部認証により確立した認証ステータスは、CD 管理部または AP 管理部が選択されている間有効である。
2.	住基 AP における PIN 照合または外部認証により確立した認証ステータスは、住基 AP が選択されている間有効である。
3.	AP 管理部における PIN 照合により確立した認証ステータスは、カードが非活性化されるまで有効であり、外部認証により確立した認証ステータスは、AP 管理部が選択されている間有効である。
4.	上記以外の AP 間で切り替わる場合、認証ステータスを継承しない。
5.	既に確立した認証ステータスであっても、AP 管理部の外部認証を再び開始するとクリアし、他のものは PIN 照合または外部認証に失敗するとクリアする。

AP 管理部における外部認証の手順は、まずカードと業務用端末との間でお互いに生成した乱数と証明書を交換し、相互の証明書を検証した後に、業務用端末で生成したセッション鍵と乱数のハッシュ値を業務用端末の秘密鍵で暗号化したデータを送信し、AP 管理部はあらかじめ検証された業務用端末の証明書に対応する公開鍵でデータ復号することにより認証を行なう。

表 6-8 認証のメカニズムと関係者の役割との対応付け

関係者の役割	認証のメカニズム
カード発行者	CD 管理部輸送 PIN による PIN 照合 CD 管理部仮 PIN による PIN 照合 CD 管理部独自利用 PIN による PIN 照合 住基 AP 仮 PIN による PIN 照合 CD 管理部における発行市町村公開鍵による外部認証 AP 管理部輸送 PIN による PIN 照合 AP 管理部におけるカード発行者の公開鍵による外部認証

カード所有者	CD 管理部所有者 PIN による PIN 照合 住基 AP 所有者 PIN による PIN 照合
業務用端末	住基 CD における証明書検証用公開鍵により証明書が検証されたテンポラリ公開鍵による外部認証 住基 AP における鍵管理用公開鍵により証明書が検証されたテンポラリ公開鍵による外部認証
AP 搭載管理者	AP 管理部における AP 搭載管理者の公開鍵による外部認証

6.1.3 暗号通信機能

SF.SECURE_MESSAGING

SF.SECURE_MESSAGING は、CD 管理部、住基 AP、および AP 管理部と業務用端末との通信において、セキュアメッセージングを実施し、業務用端末との間で送受信されるコマンドおよびレスポンスを暗号化する。

CD 管理部において、業務用端末からセキュアメッセージングの利用を指定したコマンドを受信した時、セキュアメッセージングを実施する。TOE と業務端末の通信の暗号化と復号には共通の鍵を使用する。CD 管理部の共通鍵はカード製造者があらかじめ設定した固定鍵を暗号通信鍵として利用する。

住基 AP において、業務用端末から本人確認情報読出しコマンドを受信した時、セキュアメッセージングが実施され、読出した住民票コードを暗号化する。

AP 管理部において、業務用端末からセキュアメッセージングの利用を指定したコマンドを受信した時、セキュアメッセージングを実施する。TOE と業務端末の通信の暗号化と復号には共通の鍵を使用する。

住基 AP および AP 管理部において業務用端末との通信の暗号化と復号の共通鍵として、それぞれ住基 AP セッション鍵および AP 管理部セッション鍵を使用する。これらのセッション鍵は、業務用端末で生成され、暗号通信により TOE 内へ配送する。**[住基仕様 23]**および AP 管理部に対する要求仕様で規定されたセッション鍵設定プロトコルに従い、配送で利用される鍵配送用暗号鍵を業務用端末へ配付する。鍵配送用暗号鍵はカード発行時に属性情報なしの利用者データとしてインポートする。(TOE へのインポートは **SF.ACCESS_MANAGEMENT** にて行なう。)

業務用端末は、TOE から配付された鍵配送用暗号鍵(住基 AP 鍵配送用暗号鍵または AP 管理部鍵配送用暗号鍵)を利用することにより、セッション鍵を暗号化して鍵配送を行なう。住基 AP または AP 管理部は、暗号化されたセッション鍵を、セッション鍵配送用復号鍵(住基 AP 鍵配送用復号鍵または AP 管理部鍵配送用復号鍵)を利用することにより復号し、セッション鍵を取得する。復号後、揮発性メモリ上におかれたセッション鍵配送用復号鍵はゼロクリアされる。

AP 管理部において認証後に共有されたセッション鍵(AP 管理部セッション鍵)は AP 管理領域内に保持され、その後の処理でセッション鍵(AP 管理部セッション鍵)を利用する。

SF.SECURE_MESSAGING の暗号通信において行なわれる暗号操作と使用される鍵を**表 6-9** に示す。

表 6-9 暗号通信において行なわれる暗号操作と使用される鍵

暗号操作	使用する鍵	アルゴリズム	鍵長
セキュアメッセージングにおけるコマンドの復号およびレスポンスの暗号化	住基AP部：住基APセッション鍵	Triple-DES	168 ビット
	CD管理部：固定鍵 AP管理部：AP管理部セッション鍵	Triple-DES	112 ビット
セキュアメッセージングで使用するため配送(インポート)されたセッション鍵の復号	住基 AP 鍵配送用復号鍵 AP 管理部鍵配送用復号鍵	RSA	1024 ビット

暗号化および復号で利用する暗号機能として、ANSI X.9.52 に合致した Triple-DES 暗号と PKCS#1 に合致した RSA 暗号を提供する。ハードウェアにより DES 暗号の演算機能が実現され、TOE であるソフトウェアが被演算データと暗号鍵をセットして Triple-DES 暗号として利用し、演算後、ハードウェアの揮発性メモリ上にセットした暗号鍵をゼロクリアして破棄する。

CD 管理部で利用された揮発性メモリ上の固定鍵は、演算直後にゼロクリアして破棄される。住基 AP で利用された揮発性メモリ上のセッション鍵は、セレクトコマンドでプロセスが切り替わる時にゼロクリアして破棄される。AP 管理部で利用された揮発性メモリ上のセッション鍵は**表 6-10**の管理規則に基づきゼロクリアして破棄される。

表 6-10 AP 管理部におけるセッション鍵の管理規則

1.	セレクトコマンドでプロセスが切り替わる時にゼロクリアする。
2.	次の外部認証コマンド開始時にゼロクリアする。
3.	暗号通信の復号が失敗した場合にゼロクリアする。

業務用端末で生成された CD 管理部カード秘密鍵を、**[住基仕様 23]**で規定されたカード秘密鍵設定プロトコルに従いカード内へインポートする。(TOE へのインポートは **SF.ACCESS_MANAGEMENT** にて行なう。) CD 管理部カード秘密鍵を、インポート用鍵と呼ばれる鍵を利用して暗号化する。CD 管理部は、あらかじめカード内に設定されているインポート用鍵を読み出し、揮発メモリ上において復号に利用する。復号後、揮発性メモリ上におかれたインポート用鍵をゼロクリアする。

SF.SECURE_MESSAGING においてカード秘密鍵に関連して行なわれる暗号操作と使用される鍵を**表 6-11**に示す。

表 6-11 カード秘密鍵に関連して行なわれる暗号操作と使用される鍵

暗号操作	使用する鍵	アルゴリズム	鍵長
インポートされたCD管理部カード秘密鍵の復号	インポート用鍵	Triple-DES	168 ビット
カード所有者に対する内部認証における認証コード作成のため暗号化	CD管理部カード秘密鍵、 AP管理部カード秘密鍵	RSA	1024 ビット

CD 管理部カード秘密鍵は、属性情報なし利用者データとしてインポートされ、インポートされた CD 管理部カード秘密鍵は **SF.ACCESS_MANAGEMENT** によるアクセス制御が実施され、「読出し」操作で取り出した後、カード所有者に対する「内部認証」コマンドにおいて認証コード作成のための暗号化で利用する。AP 管理部カード秘密鍵は、AP 管理部鍵配送用復号鍵と同一であり、**SF.ACCESS_MANAGEMENT** により TSF データとして管理され、AP 管理部の内部認証における認証コード作成のための暗号化で利用する。利用された揮発性メモリ上の CD 管理部カード秘密鍵および AP 管理部カード秘密鍵を利用後にゼロクリアして破棄する。TOE は RSA の秘密鍵を使用した暗号操作を実装しているが、本 ST の TOE が想定している資産保護のために何らセキュリティ機能を提供するものではない。

6.1.4 実行管理機能

SF.MANAGEMENT

TOE は、CD 管理部、住基 AP、および AP 管理部の各モジュールの独立した状態を定義し、資産に対して定義した状態において TOE が認証し、許可した役割に操作ができるように制御する。

SF.MANAGEMENT は、状態の遷移を管理し、**SF.ACCESS_MANAGEMENT** は各状態における実行可能な操作を制限する。**SF.MANAGEMENT** は、CD 管理部、AP 管理部および住基 AP の各モジュールの状態遷移ステータスを持ち、状態遷移を伴う操作を許可された TOE 関係者が実行した場合のみ状態を遷移させる。

表 6-12に各モジュールの状態遷移における状態遷移ステータスの管理規則を示す。**表 6-12**において、各モジュールにおける状態の遷移に必要な認証ステータスと条件を表す。例えば、CD 管理部において、初期化状態から PIN 設定可能状態へ遷移する場合、認証ステータスが P-1 であるカード発行者が仮 PIN を設定する必要があることを意味する。

表 6-12　状態遷移ステータスの管理規則

モジュール	状態の遷移	認証ｽﾃｰﾀｽ	遷移の条件
CD 管理部	初期化状態　⇒　PIN 設定可能状態	P-1	仮 PIN の設定
	PIN 設定可能状態　⇒　カード運用中状態	P-2	所有者 PIN への改変
	カード運用中状態　⇒　カード廃止状態	N-1	コマンドによる指示
	PIN 設定可能状態　⇒　カード廃止状態	P-2	コマンドによる指示
	カード運用中状態　⇒　PIN 設定可能状態	N-1	仮 PIN の設定
AP 管理部	初期化状態　⇒　初期化済み状態	P-7	コマンドによる指示
	初期化済み状態　⇒　運用中状態	P-7	コマンドによる指示
	運用中状態　⇒　終結状態	N-2	コマンドによる指示
	初期化済み状態　⇒　終結状態	P-7	コマンドによる指示
住基 AP	初期化状態　⇒　ロック状態	P-1	仮 PIN の設定
	ロック状態　⇒　AP 選択可能状態	P-5	所有者 PIN への改変
	AP 選択可能状態　⇒　ロック状態	N-1	仮 PIN の設定

P-1：CD 管理部輸送 PIN による PIN 照合済み(カード発行者)

P-2：CD 管理部仮 PIN による PIN 照合済み(カード発行者)

P-5：住基 AP 仮 PIN の照合済み(カード発行者)

P-7：AP 管理部輸送 PIN の PIN 照合済み(カード発行者)

N-1：CD 管理部における発行市町村公開鍵による外部認証済み(カード発行者)
N-2：AP 管理部におけるカード発行者の公開鍵による外部認証済み(カード発行者)

CD 管理部、AP 管理部および住基 AP の各モジュールがプロセスとして動作している場合、状態遷移ステータスにて利用者データや TSF データに対して許可される操作を制御する。その結果各モジュールに対応する状態遷移ステータスに応じて TOE は業務端末からのコマンドの実行可否を制御する。コマンドに伴う操作が許可されない場合、コマンドの実行は拒否する。

6.1.5 ドメイン分離機能

SF.DOMAIN

ドメイン分離の機能としてカード上に搭載されるアプリケーションとアクセス可能なデータ領域に制限を設け、CD 管理部からのみ CD 管理領域をアクセスし、AP 管理部からのみ AP 管理領域をアクセスし、住基 AP からのみ住基 AP 領域をアクセスするように制御する。

SF.DOMAIN は、住基カード上のメモリ領域を複数の領域に分割してメモリ領域への読み書きを制御する。現在動作しているプログラムの搭載されているメモリ領域のアドレスと、動作しているプログラムからアクセスされるデータが格納されているメモリ領域のアドレスを把握し、分割されたどのメモリ領域に該当するかを判断する。プログラムの搭載されているメモリ領域からデータの格納されているメモリ領域への読み書きの可否はテーブルで管理され、そのテーブルの値に基づき読み書きを制御する。読み書き可否を管理するテーブルの設定は、製造段階で製造者によってプログラム搭載と合わせて実施され、住基カードとして利用時には設定を変更できない。

6.1.6 データ復元機能

SF.RETENTION

SF.RETENTION は、CD 管理部、AP 管理部および住基 AP において、セキュリティ機能の動作を要求するすべてのコマンドの処理に対して、データの書込み処理を行なう際にトランザクション処理を開始し、正常終了した場合には、トランザクション処理中の書込み内容を有効にして終了し、コマンド中断または通信異常の理由により異常終了した場合、トランザクション処理中の書込み内容を無効にして終了する機能を持つ。

SF.RETENTION は、Flash メモリに対するすべてのアクセスを管理し、Flash メモリの書込みまたは消去による変更中に電源断異常が発生したかどうかを常に監視する。初期立ち上げ中にメモリへのアクセス状態フラグを検査し、前回終了時にアクセスしていた領域のデータ種別および異常の状態に応じて正しい状態へ自動的に回復する。必ず自動的に回復できるため、手動回復のためのメンテナンスモードは用意されていない。

利用者データおよび TSF データについては、変更時には元の値を保持しておくことにより、変更が正常に終了しなかった場合、保持している値でデータを復元する。

6.2 セキュリティ機能強度

本 ST の TOE において、確率的または順列的なメカニズムによって実現されるセキュリティ機能は **SF.AUTHENTICATE** によって実現する PIN 照合と外部認証の機能、**SF.SECURE_MESSAGING** によって実現するセキュアメッセージング機能および利用者データインポート時の暗号化機能である。

セキュアメッセージングとインポート時の暗号化の機能は暗号アルゴリズムによって実現され、暗号アルゴリズムはセキュリティ機能強度の評価の対象外であり、これら 2 つの機能は対象とならない。

PIN 照合については確率的なメカニズムを含み、攻撃者による確率的な試行が可能であるが、製造段階で製造者により試行回数は 3 回と設定され、すべての TOE 関係者により変更することはできない。PIN は 3～16[byte]で設定でき、3 回連続で照合が失敗すると対象となっている PIN または公開鍵は閉塞状態となり新たな認証に利用できなくする。

外部認証については、認証において暗号アルゴリズムが使用されるが、暗号アルゴリズムはセキュリティ機能強度の評価の対象外である。しかし、認証において乱数が使用されるため確率的なメカニズムを含み、攻撃者による確率的な試行が可能であるが、使用される乱数の長さは、住基CD部と住基APにおいては 127[byte]でAP管理部においては 16[byte]である。セキュリティ機能強度が弱いAP管理部の方を考えても、リプレイ攻撃に対して平均 2^{127}の試行が必要であり、SOF-基本を満足する。

したがって、本 ST の TOE に含まれる確率的または順列的なメカニズムは PIN 照合と外部認証であり、PIN 照合と外部認証のどちらにおいてもセキュリティ機能強度 SOF-基本を実現する。

6.3 保証手段

表 6-13に示す保証手段のドキュメントを作成することにより EAL4 追加の保証要件を満足する。また、ASE クラスの保証要件および下記の保証要件を保証する際に参照されるドキュメントとして、本 ST「アダプタ対応型高速版住基カードソフトウェアセキュリティターゲット」も存在する。

表 6-13 保証手段

保証要件コンポーネント		保証方法（参照ドキュメント）
ACM_AUT.1	部分的な CM 自動化	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 構成管理規定 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 バージョン管理規定 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 構成リスト ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 構成管理記録 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 バージョン管理記録
ACM_CAP.4	生成の支援と受入手続き	
ACM_SCP.2	問題追跡の CM 範囲	
ADO_DEL.2	改変の検出	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 ガイダンス統括文書 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 配付と運用統括文書 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 モジュール管理簿
ADO_IGS.1	設置、生成、及び立上げ手順	
ADV_FSP.2	完全に定義された外部インタフェース	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 機能仕様書
ADV_HLD.2	セキュリティ実施上位レベル設計	AP 実行環境 取扱説明書 住基 CD 部 機能仕様書 CM 部 機能仕様書 住基 AP 部 機能仕様書 ｾｷｭﾘﾃｨﾗｲﾌﾞﾗﾘ CC 認証対応版 機能仕様書 共通 RAM 管理ﾗｲﾌﾞﾗﾘ CC 認証対応版 機能仕様書 Flash 管理ﾗｲﾌﾞﾗﾘ CC 認証対応版 機能仕様書
ADV_IMP.1	TSF の実装のサブセット	AP 実行環境 ソースコード 住基 CD 部 ソースコード CM 部 ソースコード 住基 AP 部 ソースコード ｾｷｭﾘﾃｨﾗｲﾌﾞﾗﾘ CC 認証対応版 ソースコード 共通 RAM 管理ライブラリ CC 認証対応版 ソースコード Flash 管理ライブラリ CC 認証対応版 ソースコード
ADV_LLD.1	記述的下位レベル設計	AP 実行環境 詳細設計書 住基 CD 部 詳細設計書 CM 部 詳細設計書 住基 AP 部 詳細設計書

		ｾｷｭﾘﾃｨﾗｲﾌﾞﾗﾘ CC 認証対応版 詳細設計書 共通 RAM 管理ﾗｲﾌﾞﾗﾘ CC 認証対応版 詳細設計書 Flash 管理ﾗｲﾌﾞﾗﾘ CC 認証対応版 詳細設計書
ADV_RCR.1	非形式的対応の実証	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 対応表 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 セキュリティ機能要件対応表 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 TOE 要約仕様各段落対応表 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 詳細設計書
ADV_SPM.1	非形式的なセキュリティ方針モデル	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 セキュリティポリシモデル
AGD_ADM.1	管理者ガイダンス	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 カード発行者ガイダンス文書 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 AP 搭載管理者ガｲﾀﾞﾝｽ文書
AGD_USR.1	利用者ガイダンス	
ALC_DVS.1	セキュリティ手段の識別	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 開発セキュリティ管理規定 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 文書管理規定
ALC_LCD.1	開発者によるライフサイクルモデルの定義	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 ライフサイクルモデル
ALC_TAT.1	明確に定義された開発ツール	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 開発ツール管理規定 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 ツール管理記録
ATE_COV.2	カバレージの分析	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 試験項目対応表
ATE_DPT.1	テスト：上位レベル設計	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 試験深さ分析書
ATE_FUN.1	機能テスト	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 試験項目書 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 試験手順書 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 試験成績書
ATE_IND.2	独立テスト－サンプル	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 テスト環境 ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 テストプログラム ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 テストデータ アダプタ対応型高速版住基カードソフトウェア ver.2.00
AVA_MSU.3	セキュアでない状態の分析とテスト	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 開発者誤使用防止分析報告書
AVA_SOF.1	TOE セキュリティ機能強度評価	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 開発者セキュリティ機能強度評価報告書
AVA_VLA.2	独立脆弱性テスト	ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 開発者脆弱性分析報告書

7. PP 主張

本章では、PP に対する参照、詳細化、追加について記述する。

7.1 PP 参照

本 ST が適合する PP は存在しない。

7.2 PP 修整

本 ST において、PP に対する修整は存在しない。

7.3 PP 追加

本 ST において、PP に対する追加は存在しない。

8. 根拠

本章では、前章までに述べた内容の根拠について記述する。

8.1 セキュリティ対策方針根拠

本 ST における、脅威と前提条件と組織のポリシに対する TOE および環境のセキュリティ対策方針の対応付けは表 8-1の通りである。

表 8-1 セキュリティ環境とセキュリティ対策方針との対応

セキュリティ環境 ＼ セキュリティ対策方針		TOE の対策方針						環境の対策方針			
		1) O.Identification	2) O.AccessManagement	3) O.Domain	4) O.Secure_Path	5) O.Retention	6) O.Forgery	1) OE.CARD_SET_Data	2) OE.Term_TSF	3) OE.Term_Mgt	4) OE.Hardware
脅威	1) T.Logical_attack	○	○								
	2) T.Illegal_Term_use								○	○	
	3) T.Distub_APL			○							
	4) T.Environment					○					
	5) T.Incomplete						○				
	6) T.Hardware										○
前提条件	1) A.CARD_SET_Data							○	○	○	
組織のポリシ	1) P.Authentication	○	○								
	2) P.Secret_Setting	○	○								
	3) P.PIN_Initialize	○	○								
	4) P.Secure_Path				○						

6 つの脅威に対する根拠は以下の通りである。

1) **T.Logical_Attack** は、**O.Identification**、**O.AccessManagement** で対抗している。

O.Identification により、TOE 外からアクセスしてくる利用者(CD 管理部利用者、住基 AP 利用者および AP 管理部利用者)は識別される。

更に、**O.AccessManagement** により、役割に対応付けられた利用者が認証され、カード発行者、カード所有者と認証された TOE 関係者のみがアクセス可能な利用者データと TSF データが明確になるので、利用者データと TSF データの悪用が防止できる。また、TOE 外部から TOE 内の利用者データと TSF データへのアクセス手段は **O.AccessManagement** により、正規のコマンドに

基づく操作に限定されている。

2) **T.Illegal_Term_Use** は、**OE.Term_TSF**、**OE.Term_Mgt** で対抗している。
TOE 関係者を認証する際、外部から認証のためのデータがカードリーダ・ライタを経由して、TOE へ送られてくる。このようなデータは **OE.Term_TSF** により処理が終わると消去され、漏洩から保護され、このような機器が盗難にあっても、**OE.Term_Mgt** で装備される不正使用防止機構により悪用を防止できる。

3) **T.Disturb_APL** は、**O.Domain** で対抗している。
O.Domain により、アプリケーションの管理下にあるファイルは明確になり、他のアプリケーションの管理するファイルへのアクセス(読出し、書込みなど)は防止される。

4) **T.Environment** は、**O.Retention** で対抗している。
O.Retention により、住基カード使用中の電源断に対し、利用者データ、TSF データを復元する機構が用意される。

5) **T.Incomplete** は、**O.Forgery** で対抗している。
O.Forgery により、住民へ交付前の住基カードが盗まれても、TOE によって認証された TOE 関係者以外、行政サービスに使えなくなっている。

6) **T.Hardware** は、**OE.Hardware** で対抗している。
OE.Hardware により、TOE が動作するハードウェアの安全性が確保される。

1 つの前提条件に対する根拠は以下の通りである。

1) **A.CARD_SET_Data** は、**OE.CARD_SET_Data** と **OE.Term_TSF** と **OE.Term_Mgt** で対抗している。
TOE 外で TSF を知っている TOE 関係者は、カード発行者、カード所有者、業務用端末、AP 搭載管理者である。カード発行者、カード所有者に関する TSF データは **OE.CARD_SET_Data** により適切な値が設定されるように教育や指導が行われ、業務用端末は **OE.Term_TSF** により秘密の漏洩から保護され、**OE.Term_Mgt** により正規の職員により処理されることを確実にする。

4 つの組織のセキュリティ方針に対する根拠は以下の通りである。

1) **P.Authentication** は、**O.Identification**、**O.AccessManagement** で対抗している。
O.Identification により、TOE 外からアクセスしてくる利用者(CD 管理部利用者、住基 AP 利用者および AP 管理部利用者)は識別され、**O.AccessManagement** により、利用者データ(住民票コード)へのアクセス(読出し)は、本人(住民)の認証、発行者(市町村)の認証が終わった TOE 関係者に限定される。

2) **P.Secret_Setting** は、**O.Identification**、**O.AccessManagement** で対抗している。

O.Identification により、TOE 外からアクセスしてくる利用者(CD 管理部利用者、住基 AP 利用者および AP 管理部利用者)は識別され、**O.AccessManagement** により、TSF データ(鍵)の設定は、カード発行者に限定される。

3) **P.PIN_Initilize** は、**O.Identification**、**O.AccessManagement** で対抗している。

[住基仕様 23]には、PIN 初期化の権限が誰にあるかは明示されていないので、**P.PIN_Initialize** の権限はカード発行者にあると考えた。**O.Identification**、**O.AccessManagement** により、認証された発行者のみがアクセス(住基カードに TSF データである仮 PIN 設定)可能なことを保証している。

4) **P.Secure_Path** は、**O.Secure_Path** で対抗している。

O.Secure_Path により、住基カードとカードリーダ・ライタの間の通信データは、データフォーマット分析防止対策が施されるので、通信データを盗んでも利用者データや TSF データを推定することはできない。

8.2 セキュリティ要件根拠

8.2.1 TOE セキュリティ機能要件根拠

表 8-2にセキュリティ機能要件とセキュリティ対策方針との対応を示す。TOE のセキュリティ機能要件によってすべてのセキュリティ対策方針は満足され、すべてのセキュリティ機能要件は 1 つ以上のセキュリティ対策方針に寄与している。

表 8-2 セキュリティ対策方針とセキュリティ要件との対応

セキュリティ機能要件 ＼ セキュリティ対策方針	TOE の対策方針					
	O.Identification	O.AccessManagement	O.Domain	O.Secure_Path	O.Retention	O.Forgery
FCS_CKM.2				○		
FCS_CKM.4				○		
FCS_COP.1/T-DES				○		
FCS_COP.1/RSA		○				
FDP_ACC.1		◎		△		◎
FDP_ACF.1		◎		△		◎
FDP_ITC.1		◎		○		
FIA_AFL.1/VERIFY		○				
FIA_AFL.1/EXT_AUTH		○				
FIA_ATD.1	◎	◎				◎
FIA_UAU.1		◎				
FIA_UAU.4		○				
FIA_UAU.5		◎				
FIA_UAU.6		○				
FIA_UID.1	○	△				△
FIA_USB.1	◎	◎				
FMT_MSA.1/STATUS		◎				
FMT_MTD.1/IEF		◎				◎
FMT_MTD.1/STATUS		◎				◎
FMT_SMF.1		◎				◎
FMT_SMR.1		◎				◎
FPT_RCV.2					◎	
FPT_RVM.1	◎	◎	◎	◎	◎	◎
FPT_SEP.1	◎	◎	◎			◎
FTP_ITC.1				◎		
AGD_ADM.1					△	
ADV_SPM.1					△	

注) 表中の記号は以下の意味を表す。空欄は関連がないことを示す。

◎：対策方針に対する主要なセキュリティ機能要件

○：対策方針に対する主要なセキュリティ機能要件を強化するセキュリティ機能要件
△：◎または○のセキュリティ機能要件の依存性から必要となるセキュリティ要件

各セキュリティ対策方針に対するセキュリティ機能要件による充足性の根拠は、以下の通りである。また、環境に対するセキュリティ対策方針として 4 つの対策方針を挙げているが、IT 環境に関するものは存在しない。

1) **O.Identification** は、TSF が利用者を識別するための対策方針であり、**O.Identification** の主要なセキュリティ機能は、以下の 5 つの機能要件で実現される。
FIA_ATD.1(利用者属性定義)
FIA_UID.1(識別のタイミング)
FIA_USB.1(利用者・サブジェクト結合)
FPT_RVM.1(TSP の非バイパス性)
FPT_SEP.1(TSF ドメイン分離)
FAI_USB.1 により、セレクトコマンドを送信して識別された利用者と、セレクトされてサブジェクトとして利用者を代行してカード上で動作するプロセスとが、カレントプロセスの識別情報で関連付けられる。**FIA_ATD.1** により、TOE へアクセスしてくる利用者、すなわち CD 管理部利用者、住基 AP 利用者、AP 管理部利用者を代行して、サブジェクトとしてカード内で動作するカレントプロセスの識別情報が維持される。
また、識別前に、TSF が行なえる調停アクションは **FIA_UID.1** で定義されるセレクトのみに限定される。
さらに、各機能要件の迂回を防止するために、**FPT_RVM.1** によって他の TOE 機能を動作させる前に必ず識別機能を呼び出す構造にするとともに、各機能要件を不正な干渉から保護するために、**FPT_SEP.1** によって TSF とサブジェクトのドメインを分離・維持する。

2) **O.AccessManagement** は、TSF が利用者を認証し、資産へのアクセスを限定するための対策方針であり、**O.AccessManagement** の主要なセキュリティ機能は、以下の 14 の機能要件で実現される。
FIA_ATD.1(利用者属性定義)
FIA_UAU.1(認証のタイミング)
FIA_UAU.5(複数の認証メカニズム)
FIA_USB.1(利用者・サブジェクト結合)
FDP_ACC.1(サブセットアクセス制御)
FDP_ACF.1(セキュリティ属性によるアクセス制御)
FDP_SMF.1(管理機能の特定)
FMT_MSA.1/STAUTS(セキュリティ属性の管理)
FMT_MTD.1/IEF(TSF データの管理)
FMT_MTD.1/STATUS(TSF データの管理)
FMT_SMR.1(セキュリティ役割)

FPT_RVM.1(TSP の非バイパス性)
FPT_SEP.1(TSF ドメイン分離)
FAI_USB.1 により、セレクトコマンドを送信して識別された利用者と、セレクトされてサブジェクトとして利用者を代行してカード上で動作するプロセスとが、カレントプロセスの識別情報で関連付けられる。**FIA_ATD.1** により、TOE へアクセスしてくる利用者、すなわち CD 管理部利用者、住基 AP 利用者、AP 管理部利用者を代行して、サブジェクトとしてカード内で動作するプロセスの識別情報と利用者の役割に対する認証結果である認証ステータスが維持される。**FIA_UAU.1** により、TOE の識別、認証処理を行なわないで提供される TSF 調停アクションが明確になる。すなわち、**FIA_UAU.1** の割付に記述された以外の TSF 調停アクションは識別、認証が必須となる。具体的な TOE 関係者(カード発行者、カード所有者、業務用端末、AP 搭載管理者)、操作可能な操作と資産の一覧は **FDP_ACC.1** で明確になり、その時に適用される規定は **FDP_ACF.1** で示される。
FIA_UAU.5 により、TOE のサポートする利用者認証の認証メカニズムが明確になる。**FIA_UAU.5** で規定された認証メカニズムに基づき認証された TOE 関係者の役割は、**FMT_SMR.1** により維持され、住基カードの TOE に対する管理的役割(鍵設定、仮 PIN 設定、行政サービスに利用可能な状態に設定)が明確になる。**FMT_SMF.1** により、**FDP_ACF.1** と **FIA_ATD.1** と **FIA_UAU.1** のセキュリティ機能要件に対する管理機能と考えられるアクションを **FMT_MTD.1/IEF** と **FMT_MTD.1/STATUS** が実現することが明確になる。また、**FMT_MTD.1/IEF** により、管理的役割と TSF データの関係が明確になり、**FMT_MTD.1/STATUS** により、オブジェクトへの操作に伴う状態遷移が管理される。また、**FMT_MSA.1/STATUS** により、セキュリティ属性に対する管理方法が明確になる。これらの要件は、TOE のセキュリティ対策方針に対応する要件が、効率的に運用されるために必要な要件である。
さらに、各機能要件の迂回を防止するために、**FPT_RVM.**1 によって他の TOE 機能を動作させる前に必ずアクセス制御機能を呼び出す構造にするとともに、各機能要件を不正な干渉から保護するために、**FPT_SEP.1** によって TSF とサブジェクトのドメインを分離・維持する

以下は、**O.AccessManagement** を強化する 6 つの支援的な要件である。
FIA_AFL.1/VERIFY、**FIA_AFL.1/EXT_AUTH**(認証失敗時の取り扱い)
FIA_UAU.4(単一使用認証メカニズム)
FIA_UAU.6(再認証)
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)
FCS_COP.1/RSA(暗号操作)
FIA_AFL.1/VERIFY と **FIA_AFL.1/EXT_AUTH** により、認証失敗時の TSF 動作が明確になり、攻撃者の攻撃チャンスを少なくする。住基カードの発行／サービス業務に使われる業務用端末の認証メカニズムには、**FIA_UAU.4** により、チャレンジなどの再利用のできない認証データの生成を要求しているので、発行を行なう業務用端末になりすますことを難しくしている。**FIA_UAU.6** により、再認証を行なうタイミングが明確になり、作業域へ展開した資産の漏洩が防止される。
FIA_UAU.5 で規定された認証メカニズムの中に含まれる、住基カードの発行／サービス業務に

使われる業務用端末の外部認証メカニズムには、**FCS_COP.1/RSA** で指定されるアルゴリズムが使われる。また、鍵の初期設定には **FDP_ACC.1** および **FDP_ACF.1** で規定され **FDP_ITC.1** で指定されるポリシに則り、外部から TOE 内にインポートされる。
FIA_UID.1 は、**FIA_UAU.1** と **FMT_SMR.1** からの依存性で必要となる要件であり、利用者の識別のタイミングを明確にする。**FMT_MSA.3** も依存性から必要となるが、すべてのオブジェクトは製造時に既に作られており、デフォルトの値を上書きすることはできないため、依存性から除去される。

3) **O.Domain** は、アプリケーションから TSF を保護するためと、TSF が他のアプリケーション管理下のファイルへのアクセスを防止するため対策方針であり、**O.Domain** は、以下の 2 つの機能要件で実現される。
FPT_RVM.1(TSP 非バイパス性)
FPT_SEP.1(TSF ドメイン分離)
FPT_SEP.1 は、アプリケーションが搭載されたりデータが格納されたりしている領域に基づき市町村独自のアプリケーションから TSF を保護する。TSF を CD 管理部、住基 AP および AP 管理部に分離することで、これらのドメインも保護される。また、**FPT_RVM.1** は、各機能要件の迂回を防止するために、TOE 機能を動作させる前に必ず識別機能を呼び出し、不正な干渉から保護する。

4) **O.Secure_Path** は、TSF が通信データのフォーマットの分析を妨げるための対策方針であり、**O.Secure_Path** の主要なセキュリティ機能は、以下の 2 つの機能要件で実現される。
FTP_ITC.1(TSF 間高信頼チャネル)
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)
FTP_ITC.1 により、TOE とリモートにある IT 製品との通信経路において、通信データの改ざんや機密漏洩に対する対策が施される。また、その際に使用される暗号化の鍵は **FDP_ACC.1** および **FDP_ACF.1** で規定され **FDP_ITC.1** で指定されるポリシに則り、外部から TOE 内にインポートされる。

以下は、**O.Secure_Path** を強化する 4 つの支援的な要件である。
FCS_CKM.2(暗号鍵配付)
FCS_CKM.4(暗号鍵破棄)
FCS_COP.1/T-DES(暗号操作)
FPT_RVM.1(TSP の非バイパス性)
改ざん、漏洩対策には、**FCS_COP.1/T-DES** で指定されるアルゴリズム、鍵サイズの暗号操作、**FCS_CKM.2** の鍵配送、**FCS_CKM.4** の鍵破棄が使われ、**FTP_ITC.1** を補強している。また、鍵の初期設定には **FDP_ACC.1** および **FDP_ACF.1** で規定され **FDP_ITC.1** で指定されるポリシに則り、外部から TOE 内にインポートされる。
FDP_ACC.1、**FDP_ACF.1** は依存性で必要となる要件である。通信経路の暗号で使われる鍵の設定、鍵の配付、鍵の破棄に関するポリシは、**FDP_ACC.1** 、**FDP_ACF.1** で規定される。また、

依存性から **FMT_MSA.3** が必要となるが、鍵の初期設定においてデフォルト値を上書きする代替の初期値を指定できないため依存性から除去する。
さらに、通信データの暗号化に関する機能が迂回されるのを防止するために、**FPT_RVM.1** によって通信を開始する前に必ず暗号処理に使用する鍵を共有しておく構造にする

5) **O.Retention** は、TSF が電源断に対して使用中のデータを復元するための対策方針であり、**O.Retention** の主要なセキュリティ機能は、以下の 2 つの機能要件で実現される。
FPT_RCV.2(自動回復)
FPT_RVM.1(TSP の非バイパス性)
FPT_RCV.2 により、データ書込み時に電源断が発生した場合、カード活性化後に前回のデータ書込み中断が検出され、そのとき書込み中であった利用者データや TSF データは中断の状況に応じて正しいデータに復元される。
AGD_ADM.1 と **ADV_SPM.1** は依存性で必要となる要件である。**AGD_ADM.1** において機能要件のメンテナンスモードについて記述され、**ADV_SPM.1** においてセキュアな状態が何かについて記述される。
FPT_RVM.1 によって障害発生時には必ず **FPT_RCV.2** の機能要件を呼び出し、正しいデータへ復元処理を可能とする。

6) **O.Forgery** は、TSF が認証された TOE 関係者から指示があるまで実行できる機能を制限するための対策方針であり、**O.Forgery** の主要なセキュリティ機能は、以下の 9 つの機能要件で実現される。
FIA_ATD.1(利用者属性定義)
FDP_ACC.1(サブセットアクセス制御)
FDP_ACF.1(セキュリティ属性によるアクセス制御)
FMT_MTD.1/IEF(TSF データの管理)
FMT_MTD.1/STATUS(TSF データの管理)
FMT_SMR.1(セキュリティ役割)
FMT_SMF.1(管理機能の特定)
FPT_RVM.1(TSP の非バイパス性)
FPT_SEP.1(TSF ドメイン分離)
FIA_ATD.1 により、TOE へアクセスしてくる利用者、すなわち CD 管理部利用者、住基 AP 利用者、AP 管理部利用者を代行して、サブジェクトとしてカード内で動作するプロセスの識別情報と利用者の役割に対する認証結果である認証ステータスが維持される。**FMT_MTD.1/STATUS** で TOE の状態遷移における状態が管理される。TOE 関係者(カード発行者、カード所有者、業務用端末、AP 搭載管理者)、操作可能な操作と資産の一覧は **FDP_ACC.1** で明確になり、**FMT_MTD.1/STATUS** で管理された各状態で適用される規定は **FDP_ACF.1** および **FMT_MTD.1/IEF** で示される。**FMT_SMR.1** により、行政サービスを可能とする役割が定義され、**FMT_SMF.1** により、**FDP_ACC.1** と **FIA_ATD.1** のセキュリティ機能要件に対する管理機能と考えられるアクションを **FMT_MTD.1/IEF** と **FMT_MTD.1/STATUS** が実現することが明確になる

ので、発行前のカードが盗まれても、悪用はできない。
さらに、各機能要件の迂回を防止するために、**FPT_RVM.1** によって他の TOE 機能を動作させる前に必ず識別機能を呼び出す構造にするとともに、各機能要件を不正な干渉から保護するために、FPT_SEP.1 によって TSF とサブジェクトのドメインを分離・維持する
FIA_UID.1 は識別のタイミングを明確にするために依存性で必要となる要件である。

8.2.2 セキュリティ機能要件の依存性の検証

表 8-3に TOE に対するセキュリティ機能要件の対応関係を示す。根拠の部分は依存する機能要件の同表での行番号(#)または該当する説明が記述された本 ST の項番を示す。依存性が存在しないものについては「－」で示してある。[ ]内で／で区切られているコンポーネントは依存性が「または」で要求され、選択可能なものを示す。選択可能なコンポーネントのうち、依存性として TOE のセキュリティ機能要件で対応していないものは、根拠欄において非選択と示している。

#1, #2, #3, #4, #6 および#7 のコンポーネントにおいては CC の Part2(**[CC-2]**)で規定された依存性は満足されていないが、**8.2.3** 項において依存性除去の理由を述べている。それ以外のについてはすべて依存性を満足している。#22 の **FPT_RCV.2** の依存性は、5.1.3 項で示されるセキュリティ保証要件によって満足されている。

表 8-3 セキュリティ機能要件の依存性

#	コンポーネント	名　　称	依存性	根拠
1	**FCS_CKM.2**	暗号鍵配付	[FDP_ITC.1 ／FDP_ITC.2 ／FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	# 7 非選択 非選択 # 2 8.2.3 項
2	**FCS_CKM.4**	暗号鍵破棄	[FDP_ITC.1 ／FDP_ITC.2 ／FCS_CKM.1] FMT_MSA.2	# 7 非選択 非選択 8.2.3 項
3	**FCS_COP.1/T-DES**	暗号操作	[FDP_ITC.1 ／FDP_ITC.2 ／FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	# 7 非選択 非選択 # 2 8.2.3 項
4	**FCS_COP.1/RSA**	暗号操作	[FDP_ITC.1 ／FDP_ITC.2 ／FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	# 7 非選択 非選択 # 2 8.2.3 項
5	**FDP_ACC.1**	サブセットアクセス制御	FDP_ACF.1	# 6
6	**FDP_ACF.1**	セキュリティ属性によるアクセス制御	FDP_ACC.1 FMT_MSA.3	# 5 8.2.3 項
7	**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	[FDP_ACC.1 ／FDP_IFC.1] FMT_MSA.3	# 5 非選択 8.2.3 項
8	**FIA_AFL.1/VERIFY**	認証失敗時の取扱い	FIA_UAU.1	# 11
9	**FIA_AFL.1/EXT_AUTH**	認証失敗時の取扱い	FIA_UAU.1	# 11
10	**FIA_ATD.1**	利用者属性定義	なし	－
11	**FIA_UAU.1**	認証のタイミング	FIA_UID.1	# 15
12	**FIA_UAU.4**	単一使用認証メカニズム	なし	－
13	**FIA_UAU.5**	複数の認証メカニズム	なし	－
14	**FIA_UAU.6**	再認証	なし	－
15	**FIA_UID.1**	識別のタイミング	なし	－
16	**FIA_USB.1**	利用者・サブジェクト結合	FIA_ATD.1	# 10

17	**FMT_MSA.1/STATUS**	セキュリティ属性の管理	[FDP_ACC.1 ／FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	# 6 非選択 # 21 # 22
18	**FMT_MTD.1/IEF**	TSF データの管理	FMT_SMF.1 FMT_SMR.1	# 21 # 22
19	**FMT_MTD.1/STATUS**	TSF データの管理	FMT_SMF.1 FMT_SMR.1	# 21 # 22
20	**FMT_SMF.1**	管理機能の特定	なし	―
21	**FMT_SMR.1**	セキュリティ役割	FIA_UID.1	# 15
22	**FPT_RCV.2**	自動回復	AGD_ADM.1 ADV_SPM.1	5.1.3 項 5.1.3 項
23	**FPT_RVM.1**	TSP 非バイパス性	なし	―
24	**FPT_SEP.1**	TSF ドメイン分離	なし	―
25	**FTP_ITC.1**	TSF 間高信頼チャネル	なし	―

表 8-4は、機能コンポーネントに対する依存性を表し、それらの直接的、間接的、あるいは自由選択の依存性を示す。ある機能コンポーネントが依存する各々のコンポーネントは、列に配置され、各機能コンポーネントは、行に配置される。表のセルにおける値は、列に書かれたコンポーネントが、行に書かれたコンポーネントによって、直接的に要求されるか(「×」で表示)、あるいは自由選択的に要求されるか(「○」で表示)を示す。選択されたものを「◎」で表示する。行に何も記号が存在しないコンポーネントは、他のコンポーネントに依存しないものである。TOE に要求されている機能コンポーネントは太字で表す。根拠説明により除去されたコンポーネントを「＊」で表す。すべての機能コンポーネントの依存性を満足するためには、列に配置されたすべてのコンポーネントが TOE の要件となっている必要があるが、要件となっていない部分(細字のコンポーネント)は、選択上他のコンポーネントが選択されて不要であるか、根拠説明により除去されたコンポーネントである。したがって、TOE で要求する依存性で不足しているものは存在しない。

表 8-4 セキュリティ機能要件の依存性

	依存するセキュリティ要件 / セキュリティ機能要件	FCS_CKM.1	**FCS_CKM.4**	**FDP_ACC.1**	**FDP_ACF.1**	FDP_IFC.1	**FDP_ITC.1**	FDP_ITC.2	**FIA_ATD.1**	**FIA_UAU.1**	**FIA_UID.1**	**FMT_MSA.1**	FMT_MSA.2(*)	FMT_MSA.3(*)	**FMT_SMF.1**	**FMT_SMR.1**	**AGD_ADM.1**	**ADV_SPM.1**
1	**FCS_CKM.2**	○	×				◎	○					×					
2	**FCS_CKM.4**	○					◎	○					×					
3	**FCS_COP.1/T-DES**	○	×				◎	○					×					
4	**FCS_COP.1/RSA**	○	×				◎	○					×					
5	**FDP_ACC.1**				×													
6	**FDP_ACF.1**			×										×				
7	**FDP_ITC.1**			◎		○								×				
8	**FIA_AFL.1/VERIFY**									×								
9	**FIA_AFL.1/EXT_AUTH**									×								
10	**FIA_ATD.1**																	
11	**FIA_UAU.1**										×							
12	**FIA_UAU.4**																	
13	**FIA_UAU.5**																	
14	**FIA_UAU.6**																	
15	**FIA_UID.1**																	
16	**FIA_USB.1**								×									
17	**FMT_MSA.1/STATUS**			◎		○									×	×		
18	**FMT_MTD.1/IEF**														×	×		
19	**FMT_MTD.1/STATUS**														×	×		
20	**FMT_SMF.1**																	
21	**FMT_SMR.1**										×							
22	**FPT_RCV.2**																×	×
23	**FPT_RVM.1**																	
24	**FPT_SEP.1**																	
25	**FTP_ITC.1**																	

8.2.3 依存性除去の理由

表 8-3に示すように、TOE セキュリティ機能要件の依存性において、**FCS_CKM.2**、**FCS_CKM.4**、**FCS_COP.1/T-DES**、**FCS_COP.1/RSA** から **FMT_MSA.2** が、また、**FDP_ACF.1**、**FDP_ITC.1** から **FMT_MSA.3** が、それぞれ必要であるが、本 TOE では提供していない。

本 ST では、業務用端末の認証とセキュアメッセージングの機能を実現するため、FCS_COP.1 で暗号アルゴリズムの使用を要求している。しかし、そのアルゴリズムで必要な鍵は住基カードの発行者が生成したもので、発行する市町村が安全と確認した値が入力される。TOE の外部で安全な鍵が生成されるため、TOE として安全性を確認する必要はなく、**FMT_MSA.2** をセキュリティ機能要件から除外している。

また、本 ST のアクセス制御の対象となるオブジェクトのうち、すべてのオブジェクトは製造時に既に生成されており、デフォルトの値を上書きすることはできない。したがって、**FMT_MSA.3** をセキュリティ機能要件から除外している。

FCS_COP.1/RSA の依存性から、**FDP_ITC.1** または **FDP_ITC.2** または **FCS_CKM.1** が必要である。外部認証に使用される公開鍵と暗号化されたセッション鍵を復号するための鍵配送用復号鍵については、TOE の外部で生成されて与えられるが、これらの鍵は TSF データと考えており、利用者データのインポートではなく TSF データの管理規則に従い「設定」または「改変」される。

8.2.4 セキュリティ機能要件の相互補完

8.2.2 項で示した TOE セキュリティ機能要件の依存関係において、依存性のあるセキュリティ機能は片方のセキュリティ機能を補完する。
また、**FDP_ACC.1** と **FDP_ACF.1** および **FMT_MTD.1/IEF** で提供される利用者データおよび TSF データに対するアクセス制御を実現するために、**FPT_RVM.1** の非バイパス機能および **FPT_SEP.1** のドメイン分離機能が補完する

8.2.5 セキュリティ機能要件の競合

TOE の提供するセキュリティ機能要件として、識別と認証の機能要件群、アクセス制御の機能要件群、暗号通信の機能要件群、実行管理の機能要群、ドメイン分離の機能要件、データ復元の機能要件が存在するが、TOE が動作する環境はシングルプロセスの LSI であり、処理のシーケンスはあらかじめ定まっており、これらの機能要件に対して競合が生じることはない。

8.2.6 最小機能強度レベルの妥当性

本 ST の TOE は、個人情報を取り扱うため安全性を重要視しており、更に全国規模で多くの住民に配られ、本人確認業務だけでなく、市町村が提供する様々な行政サービスの中で使われる。住基カードには、正当な役割に関連付けられた利用者を識別･認証する機能が必要である。住基カードは個人情報を取り扱うが、金融系のカードのように資産的な価値を取り扱う訳ではない。
したがって、TOE の認証における安全性を確保する機構には、低位の攻撃力を持つ攻撃者からの攻撃にも耐えうる SOF-基本が妥当である。

8.2.7 セキュリティ保証要件の妥当性

住基カードに格納される様々な行政サービスの関する情報は犯罪者にとって魅力的である。また、一旦、住基カードの技術的欠陥を付き、偽造が発生すると、その社会的影響は非常に大きいため、住基カードには高い信頼度が要求される。一般的に信頼度を高くするためには、開発やセキュリティ評価にそれなりの費用がかかり、カードの価格に影響を及ぼしてしまう。

したがって、民間製品に対する最高の保証レベルである EAL4 は、下位設計書とソースコードの評価を含み TOE の細部まで評価され、高い信頼度が得られるので、妥当な選択である。

また、住基カードは、住民に交付され各住民が使用するため、誤使用されることが想定される。したがって、開発段階で様々な観点から TOE の誤使用によりセキュアでない状態に対する分析をしておく必要があり、AVA_MSU.3 を追加することにより誤使用に対する保証を強化している。AVA_MSU.3 を追加することにより、ADO_IGS.1、ADV_FSP.1、AGD_ADM.1、AGD_USR.1 が依存性として要求されるが、すべて同じ保証要件または上位の保証要件が選択済みとなっており、保証要件の依存性は満たされている。

8.2.8 相互補完のセキュリティ機能要件

各対策方針に対して相互的に補完するセキュリティ機能要件を**表 8-5**に示す。

表 8-5 対策方針に対する相互補完のセキュリティ要件

対策方針		相互補完のセキュリティ要件
TOE	1) O.Identification	FIA_ATD.1, FIA_UID.1, FIA_USB.1, FPT_RVM.1, FPT_SEP.1
	2) O.AccessManagement	FCS_COP.1/RSA, FDP_ACC.1, FDA_ACF.1, FDP_ITC.1, FIA_AFL.1/VERIFY, FIA_AFL.1/EXT_AUTH, FIA_ATD.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UID.1, FIA_USB.1, FMT_MSA.1/STATUS, FMT_MTD.1/IEF, FMT_MTD.1/STATUS, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1
	3) O.Domain	FIA_ATD.1, FPT_RVM.1, FPT_SEP.1
	4) O.Secure_Path	FCS_CKM.2, FCS_CKM.4, FCS_COP.1/T-DES, FDP_ACC.1, FDA_ACF.1, FDP_ITC.1, FTP_ITC.1, FPT_RVM.1
	5) O.Retention	FPT_RCV.2, FPT_RVM.1
	6) O.Forgery	FDP_ACC.1, FDA_ACF.1, FIA_UID.1, FMT_MTD.1/STATUS, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1

TOE の外部インタフェースは論理的インタフェースのみであり、住基カード外から**表 8-5**で挙げた相互補完的な機能要件の実行部分を迂回させたり、実行部分の処理状況を見たり、実行部分を停止させるようなインタフェースはない。また、住民の希望でロードされる市町村独自のアプリケーションは TOE 外であるが、TSF は FPT_RVM.1 と FPT_SEP.1 で守られているので、TOE 内の処理を迂回／覗き見／停止することはできない。TOE を構成するプログラムは、FPT_SEP.1 により TOE 内の信頼できないサブジェクトによる動作中の干渉およびプログラムコードの改変に対して保護されている。

住基カードの TOE はセキュリティ機能実行の記録は行なっていないので、記録機能の防衛手段は有していない。TOE における機能の実行はコマンドとして TOE 外のシステムから送られ、外部のシステム側で送信したコマンドのログを記録として残しているため、監査に使用できる。

8.3 TOE 要約仕様根拠

8.3.1 TOE セキュリティ機能の根拠

表 6-1はセキュリティ機能要件と TOE 要約仕様との対応付けを示し、すべてのセキュリティ機能要件はひとつ以上の TOE 要約仕様によって実現され、セキュリティ機能要件の十分性は満足されている。また、TOE 要約仕様にもひとつ以上のセキュリティ機能要件が対応し、実装の必要性が満足されている。

以下に、個々のセキュリティ機能要件に対する実現の正当性を説明する。

8.3.1.1 暗号サポート(FCS)

FCS_CKM.2 暗号鍵配付
FCS_CKM.2 は、鍵配送用暗号鍵の配付に対する機能要件である。
SF.SECURE_MESSAGING は、業務用端末側で生成されたセッション鍵の配送を受けるに当たり、鍵配送用暗号鍵を配付する。したがって、**SF.SECURE_MESSAGING** により、**FCS_CKM.2** は実現される。

FCS_CKM.4 暗号鍵破棄
FCS_CKM.4 は、鍵のゼロクリアによる破棄に対する機能要件である。
SF.SECURE_MESSAGING は、暗号通信で利用した固定鍵およびセッション鍵、セッション鍵の配送で利用した鍵配送用復号鍵、秘密鍵のインポートで利用したインポート用鍵、および暗号操作で利用したカード秘密鍵を、揮発性メモリ上において使用した後にゼロクリアして破棄する。
したがって、**SF.SECURE_MESSAGING** により、**FCS_CKM.4** は実現される。

FCS_COP.1 暗号操作
FCS_COP.1/T-DES は、Triple-DES 暗号に対する機能要件である。
SF.SECURE_MESSAGING は、セキュアメッセージングのデータ暗号化および CD 管理部カード秘密鍵のインポートにおいて Triple-DES 暗号を利用する。
したがって、**SF.SECURE_MESSAGING** により、**FCS_COP.1/T-DES** は実現される。

SF.AUTHENTICATE は、外部認証で利用する RSA 暗号の機能を提供する。
FCS_COP.1/RSA は、RSA 暗号に対する機能要件である。
SF.SECURE_MESSAGING は、セキュアメッセージングで利用されるセッション鍵の配送およびカード秘密鍵に対して行なわれる RSA 暗号を利用する。
したがって、**SF.AUTHENTICATE** および **SF.SECURE_MESSAGING** により、**FCS_COP.1/RSA** は実現される。

8.3.1.2 利用者データ保護 (FDP)

FDP_ACC.1 サブセットアクセス制御

FDP_ACC.1 は、アクセス制御の操作に対する機能要件である。

SF.ACCESS_MANAGEMENT は、CD 管理プロセス、AP 管理プロセス、および住基 AP プロセスのそれぞれのプロセスにおいて**表 6-3**～**表 6-5**の規則に基づきサブジェクトとオブジェクトとそれらの間の操作に対してアクセス制御を実施する。

したがって、**SF.ACCESS_MANAGEMENT** により、**FDP_ACC.1** は実現される。

FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1 は、アクセス制御の実施に対する機能要件である。

SF.ACCESS_MANAGEMENT は、CD 管理プロセス、AP 管理プロセス、および住基 AP プロセスのそれぞれのプロセスにおいて**表 6-3**～**表 6-5**の規則に従いセキュリティ属性の状態に基づきアクセス制御を実施する。

したがって、**SF. ACCESS_MANAGEMENT** により、**FDP_ACF.1** は実現される。

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

FDP_ITC.1 は、利用者データのインポートに対する機能要件である。

SF.ACCESS_MANAGEMENT は､セキュアメッセージングの暗号化で利用されるセッション鍵、セッション鍵の配送で利用される鍵配送用暗号鍵、およびカード所有者に対する CD 管理部カード秘密鍵をセキュリティ属性なしでインポートする。

したがって、**SF.ACCESS_MANAGEMENT** により、**FDP_ITC.1** は実現される。

8.3.1.3 識別と認証(FIA)

FIA_AFL.1 認証失敗時の取り扱い

FIA_AFL.1/VERIFY は、PIN 照合における認証失敗時の取り扱いに対する機能要件である。

SF.AUTHENTICATE は、PIN 照合においてあらかじめ設定された試行回数を連続して照合が失敗すると、対応する IEF に格納されている照合 PIN を閉塞状態にして認証への利用を停止し、カード発行者による利用停止の解除を実施する。

したがって、**SF.AUTHENTICATE** により、**FIA_AFL.1/VERIFY** は実現される。

FIA_AFL.1/EXT_AUTH は、外部認証における認証失敗時の取り扱いに対する機能要件である。

SF.AUTHENTICATE は、外部認証においてあらかじめ設定された試行回数を連続して認証が失敗すると、対応する IEF に格納されている公開鍵を閉塞状態にして認証への利用を停止し、利用停止の解除はできなくする。

したがって、**SF.AUTHENTICATE** により、**FIA_AFL.1/EXT_AUTH** は実現される。

FIA_ATD.1 利用者属性定義

FIA_ATD.1 は、利用者属性の定義に対する機能要件である。

SF.ACCESS_MANAGEMENT は、CD 管理部、AP 管理部および住基 AP で維持されている照合された PIN あるいは外部認証された公開鍵の格納されていた IEF に対応する当事者番号またはノード番号をアクセス制御に利用する。

SF.MANAGEMENT は、CD 管理部、AP 管理部および住基 AP で維持されている照合された PIN あるいは外部認証された公開鍵の格納されていた IEF に対応する当事者番号またはノード番号を実行管理に利用する。

SF.AUTHENTICATE は、照合された PIN あるいは外部認証された公開鍵の格納されていた IEF に対応する当事者番号またはノード番号を維持する。

したがって、**SF.ACCESS_MANAGEMENT**、**SF.MANAGEMENT** および **SF.AUTHENTICATE** により、**FIA_ATD.1** は実現される。

FIA_UAU.1 認証のタイミング

FIA_UAU.1 は、認証のタイミングに対する機能要件である。

SF.AUTHENTICATE は、認証の有無にかかわらず、セレクト、輸送 PIN 情報取得、カード種別識別情報取得、カード状態取得、乱数取得、証明書交換の実行を許可する。

したがって、**SF.AUTHENTICATE** により、**FIA_UAU.1** は実現される。

FIA_UAU.4　単一使用認証メカニズム

FIA_UAU.4 は、単一使用の認証メカニズムに対する機能要件である。

SF.AUTHENTICATE は、外部認証において認証毎に新しく生成した乱数を利用する。

したがって、**SF.AUTHENTICATE** により、**FIA_UAU.4** は実現される。

FIA_UAU.5　複数の認証メカニズム

FIA_UAU.5 は、複数の認証メカニズムに対する機能要件である。

SF.AUTHENTICATE は、CD 管理部において CD 管理部輸送 PIN、CD 管理部仮 PIN、CD 管理部所有者 PIN のいずれかとの照合を行ない、TOE 関係者を認証する。

SF. AUTHENTICATE は、住基 AP において住基 AP 仮 PIN または住基 AP 所有者 PIN との照合を行い、TOE 関係者を認証する。

SF.AUTHENTICATE は、AP 管理部において AP 管理部輸送 PIN との照合を行ない、TOE 関係者を認証する。

SF.AUTHENTICATE は、CD 管理部において発行市町村公開鍵を利用してカード発行者を認証し、証明書検証用公開鍵により証明書が検証されたテンポラリ公開鍵を利用して業務用端末を認証する。

SF.AUTHENTICATE は、住基 AP において発行市町村公開鍵を利用してカード発行者を認証し、鍵管理用公開鍵により証明書が検証されたテンポラリ公開鍵を利用して業務用端末を認証する。

SF.AUTHENTICATE は、AP 管理部においてカード発行者の公開鍵を利用してカード発行者を認証する。

SF.AUTHENTICATE は、AP 管理部において AP 搭載管理者の公開鍵を利用して AP 搭載管理者を認証する。
したがって、**SF.AUTHENTICATE** により、**FIA_UAU.5** は実現される。

FIA_UAU.6 再認証
FIA_UAU.6 は、再認証に対する機能要件である。
SF.AUTHENTICATE は、住基 AP 部が再選択された場合、PIN 照合と外部認証に対して再認証を要求し、AP 管理部が再選択された場合、外部認証に対して再認証を要求する。
したがって、**SF.AUTHETICATE** により、**FIA_UAU.6** は実現される。

FIA_UID.1 識別のタイミング
FIA_UID.1 は、識別のタイミングに対する機能要件である。
SF.AUTHENTICATE は、利用者を識別することなくすべての利用者に対してセレクトコマンドの実行だけを許可する。
したがって、**SF.AUTHENTICATE** により、**FIA_UID.1** は実現される。

FIA_USB.1 利用者・サブジェクト結合
FIA_USB.1 は、利用者とサブジェクトの関連付けに対する機能要件である。
SF.ACCESS_MANAGEMENT は、識別された利用者とサブジェクトとして利用者を代行して動作しているプロセスを関連付けるカレントプロセスの識別情報をアクセス制御に利用する。
SF.AUTHENTICATE は、セレクトコマンドを送信した利用者とセレクトされてサブジェクトとして利用者を代行して動作しているプロセスをカレントプロセスの識別情報により関連付ける。
したがって、**SF.ACCESS_MANAGEMENT** および **SF.AUTHENTICATE** により、**FIA_USB.1** は実現される。

8.3.1.4 セキュリティ管理（FMT）

FMT_MSA.1 セキュリティ属性の管理
FMT_MSA.1/STATUS は、セキュリティ属性である状態遷移ステータスの管理に対する機能要件である。
SF.ACCESS_MANAGEMENT は、CD 管理部および住基 AP において**表 6-3**と**表 6-4**の規則に基づき認証で利用される PIN のセキュリティ属性である状態遷移ステータスに対する管理を実行する。**表 6-3**と**表 6-4**において、新しく仮 PIN を設定して状態遷移ステータスを改変できるのはカード発行者だけである。
SF.MANAGEMENT は、CD 管理部、住基 AP、および AP 管理部において**表 6-12**の管理規則に基づき各モジュールのセキュリティ属性である状態遷移ステータスに対する管理を実行する。**表 6-12**において、状態遷移ステータスを改変できるのはカード発行者だけである。
したがって、**SF.ACCESS_MANAGEMENT** および **SF.MANAGEMENT** により、

FMT_MSA.1/STATUS は実現される。

FMT_MTD.1 TSF データの管理

FMT_MTD.1/IEF は、TSF データである PIN と鍵の管理に対する機能要件である。

SF.ACCESS_MANAGEMENT は、CD 管理部、AP 管理部および住基 AP において**表 6-3**～**表 6-5**の規則に基づき TSF データである PIN と鍵を管理する。**表 6-3**の規則は、**表 5-16**～**表 5-19**の CD 管理部における IEF の管理規則を実現し、**表 6-4**の規則は、**表 5-20**～**表 5-22**の住基 AP における IEF の管理規則を実現し、**表 6-5**の規則は、**表 5-23**～**表 5-26**の AP 管理部における IEF の管理規則を実現する。

したがって、**SF.ACCESS_MANAGEMENT** により、**FMT_MTD.1/IEF** が実現される。

FMT_MTD.1/STATUS は、TSF データである状態遷移ステータスの管理に対する機能要件である。

SF.MANAGEMENT は、CD 管理部、AP 管理部および住基 AP において**表 6-12**の管理規則に基づき TSF データである状態遷移ステータスを管理する。**表 6-12**の管理規則は、**表 5-27**～**表 5-29**の状態遷移ステータスの管理規則を実現する。

したがって、**SF.MANAGEMENT** により、**FMT_MTD.1/STATUS** が実現される。

FMT_SMF.1 管理機能の特定

FMT_SMF.1 は、管理機能の特定に対する機能要件である。

表 8-6に管理機能を実現するセキュリティ機能の一覧と実現するセキュリティ機能がない場合の根拠の説明を示す。

SF.ACCESS_MANAGEMENT は、**FDP_ACF.1** のアクセス制御におけるアクセス許可の決定に使われる規則と **FIA_UAU.1** の認証で使用される認証データである PIN と公開鍵に対する管理機能を実現する。

SF.MANAGEMENT は、**FIA_ATD.1** で使用される利用者に属するセキュリティ属性であるカレントプロセスの識別情報と認証ステータスに対する管理機能を実現する。

したがって、**SF.ACCESS_MANAGEMENT** および **SF.MANAGEMENT** により、**FMT_SMF.1** は実現される。

表 8-6 管理機能の一覧と根拠の説明

機能要件	管理機能と考えられるアクション	実現するセキュリティ機能
FCS_CKM.2	a) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	a) なし(暗号鍵属性を変更することはできない)
FCS_CKM.4	同上	a) なし(暗号鍵属性を変更することはできない)
FCS_COP.1/T-DES	予見される管理アクティビティはない。	不要
FCS_COP.1/RSA	予見される管理アクティビティはない。	不要
FDP_ACC.1	予見される管理アクティビティはない。	不要
FDP_ACF.1	a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	a) SF.ACCESS_MANAGEMENT
FDP_ITC.1	a) インポートに対して使用される追加の制御規則の改変。	a) なし(規則を改変することはできない)
FIA_AFL.1/VERIFY	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	a) なし(閾値は固定である) b) なし(とられるアクションは固定である)
FIA_AFL.1/EXT_AUTH	同上	a) なし(閾値は固定である) b) なし(とられるアクションは固定である)
FIA_ATD.1	a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	a) SF.MANAGEMENT
FIA_UAU.1	a) 管理者による認証データの管理 b) 関係する利用者による認証データの管理 c) 利用者が認証される前にとられるアクションリストの管理	a) SF.ACCESS_MANAGEMENT b) SF.ACCESS_MANAGEMENT c) なし(とられるアクションは固定である)
FIA_UAU.4	予見される管理アクティビティはない。	不要
FIA_UAU.5	a) 認証メカニズムの管理 b) 認証に対する規則の管理	a) なし(認証メカニズムは固定である) b) なし(認証に対する規則は固定である)
FIU_UAU.6	a) 許可管理者が再認証を要求できる場合、管理に再認証要求を含める。	a) なし(許可利用者であっても再認証を要求できない)
FIA_UID.1	a) 利用者識別情報の管理 b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストの管理	a) なし(利用者識別情報は固定である) b) なし(アクションは変更できない)
FIA_USB.1	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 b) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を変更できる。	a) なし(デフォルトのサブジェクトは固定である) b) なし(デフォルトのサブジェクトは変更できない)
FMT_MSA.1/STATUS	a) セキュリティ属性と相互に影響を及ぼし得る役割のグループの管理	a) なし(グループは存在しない)
FMT_MTD.1/IEF	a) TSF データと相互に影響を及ぼし得る役割のグループの管理	a) なし(グループは存在しない)

FMT_MTD.1/STATUS	同上	a) なし(グループは存在しない)
FMT_SMF.1	予見される管理アクティビティはない。	不要
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理	a) なし(グループは存在しない)
FPT_RCV.2	a) メンテナンスモードにおける修復能力に誰がアクセスできるかの管理 b) 自動的な手順で処理される障害/サービス中断のリストの管理	a) なし(メンテナンスモードになることはない) b) (障害/サービス中断のリストは固定である)
FPT_RVM.1	予見される管理アクティビティはない。	不要
FPT_SEP.1	予見される管理アクティビティはない。	不要
FTP_ITC.1	a) もしサポートされていれば、高信頼チャネルを要求するアクションの設定	a) なし(高信頼性チャネルを要求するアクションは固定である)

FMT_SMR.1 セキュリティ役割

FMT_SMR.1 は、セキュリティ役割に対する機能要件である。

SF.ACCESS_MANAGEMENT は、アクセス制御において維持されているセキュリティ役割を利用する。

SF.AUTHENTICATE は、照合および外部認証によって認証された利用者のセキュリティ役割を維持する。

SF.MANAGEMENT は、各モジュールの状態遷移の管理において維持されているセキュリティ役割を利用する。

したがって、**SF.ACCESS_MANAGEMENT**、**SF.AUTHENTICATE** および **SF.MANAGEMENT** により、**FMT_SMR.1** は実現される。

8.3.1.5 TSF の保護(FPT)

FPT_RCV.2　自動回復

FPT_RCV.2 は、自動回復に対する機能要件である。

SF.RETENTION は、データ書込み時に電源断が発生した場合、再起動時に利用者データと TSF データを正常なデータに復元する。

したがって、**SF.RETENTION** により、**FPT_RCV.2** は実現される。

FPT_RVM.1　TSP の非バイパス性

FPT_RVM.1 は、TSP の非バイパスに対する機能要件である。

SF.ACCESS_MANAGEMENT は、CD 管理部、AP 管理部および住基 AP が管理するファイルへのアクセスが実行される前に、アクセス制御機能を実行する。

したがって、**SF.ACCESS_MANAGEMENT** により、**FPT_RVM.1** は実現される。

SF.AUTHENTICATE は、CD 管理部利用者、AP 管理部利用者および住基 AP 利用者のアクセスがあった際にアクセスが実行される前に、識別認証機能を実行する。
したがって、**SF.AUTHENTICATE** により、**FPT_RVM.1** は実現される。

SF.SECURE_MESSAGING は、暗号通信を実行する前に暗号処理に使用する暗号鍵をカードと運用端末の間で共有する。
したがって、**SF.SECURE_MESSAGING** により、**FPT_RVM.1** は実現される。

SF.MANAGEMENT は、状態遷移の管理の管理を行い、許可した役割に応じた制御の実行を行う。この制御を実施する前に識別認証機能を実行する。
したがって、**SF.MANAGEMENT** により、**FPT_RVM.1** は実現される。

SF.DOMAIN は、識別・認証機能を実行し、ドメインのアクセスに関する制御を行う。
したがって、**SF.DOMAIN** により、**FPT_RVM.1** は実現される。

SF.RETENTION は、障害発生時に必ず障害検知機能が動作し、障害時に異常が発生したデータの復旧を行う。
したがって、**SF.RETENTION** により、**FPT_RVM.1** は実現される。

FPT_SEP.1　TSF ドメイン分離
FPT_SEP.1 は、TSF ドメイン分離に対する機能要件である。

SF.ACCESS_MANAGEMENT は、CD 管理部、AP 管理部および住基 AP が管理するファイルへのアクセス制御を実行する際に、アクセス制御機能は、他の機能から分離される。
したがって、**SF.ACCESS_MANAGEMENT** により、**FPT_SEP.1** は実現される。

SF.AUTHENTICATE は、CD 管理部利用者、AP 管理部利用者および住基 AP 利用者の識別認証を実行する際に、識別認証機能は、他の機能から分離されている。
したがって、**SF.AUTHENTICATE** により、**FPT_SEP.1** は実現される。

SF.MANAGEMENT は、状態遷移の管理の管理を行い、許可した役割に応じた状態遷移を実施する機能は、他の機能から分離されている。
したがって、**SF.MANAGEMENT** により、**FPT_SEP.1** は実現される。

SF.DOMAIN は、カードに搭載されたカード AP 相互のプログラム領域およびデータ領域を不正にアクセスしないように動作環境を分離する。
したがって、**SF.DOMAIN** により、**FPT_SEP.1** は実現される。

8.3.1.6 高信頼パス／チャネル(FTP)

FTP_ITC.1　TSF 間高信頼チャネル

FTP_ITC.1 は、TSF 間高信頼性チャネルに対する機能要件である。

SF.SECURE_MESSAGING は、セキュアメッセージングによりカードと業務用端末との間に高信頼性パスを確立する。

したがって、**SF.SECURE_MESSAGING** により、**FTP_ITC.1** は実現される。

8.3.2 セキュリティ機能強度の根拠

5.1.2 項で TOE セキュリティ要件における最小機能強度レベルとして SOF-基本を宣言しているが、**6.2** 節のセキュリティ機能強度で述べられているように、本 TOE は SOF-基本を実現しており、最小機能強度レベルと同じであり、TOE に要求されている最小のセキュリティ機能強度を満足している。

8.3.3 セキュリティ機能の組み合わせ根拠

いくつかのセキュリティ機能要件は、TOE 要約仕様において複数のセキュリティ機能で実現され、1 つのセキュリティ機能要件を実現するために複数のセキュリティ機能が組み合わされる必要がある。次に示すセキュリティ機能要件は、複数のセキュリティ機能によって実現される。

FCP_COP.1/RSA は、**SF_AUTHENTICATE** と **SF.SECURE_MESSAGING** の 2 つのセキュリティ機能で実現される。

FIA_ATD.1 は、**SF_ACCESS_MANAGEMENT** と **SF_AUTHENTICATE** と **SF.MANAGEMENT** の 3 つのセキュリティ機能で実現される。

FIA_USB.1 は、**SF_ACCESS_MANAGEMENT** と **SF_AUTHENTICATE** の 2 つのセキュリティ機能で実現される。

FMT_MSA.1/STATUS は、**SF_ACCESS_MANAGEMENT** と **SF_MANAGEMENT** の 2 つのセキュリティ機能で実現される。

FMT_SMF.1 は、**SF_ACCESS_MANAGEMENT** と **SF_MANAGEMENT** の 2 つのセキュリティ機能で実現される。

FMT_SMR.1 は、**SF_ACCESS_MANAGEMENT** と **SF_AUTHENTICATE** と **SF.MANAGEMENT** の 3 つのセキュリティ機能で実現される。

FPT_RVM.1 は、**SF_ACCESS_MANAGEMENT**、**SF_AUTHENTICATE**、**SF.SECURE_MESSAGING**、**SF_MANAGEMENT**、**SF_DOMAIN** および **SF_RETENTION** の 6 つのセキュリティ機能で実現される。

FPT_SEP.1 は、**SF_ACCESS_MANAGEMENT**、**SF_AUTHENTICATE**、**SF_MANAGEMENT** および **SF_DOMAIN** の 4 つのセキュリティ機能で実現される。

8.3.4 保証手段の根拠

表 6-13に保証要件に対応する参照ドキュメントが示されているが、以下に個々の保証要件に対する参照ドキュメントの正当性を説明する。

ACM_AUT.1（部分的な CM 自動化）
「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 構成管理規定」は、TOE の開発全般に関する構成要素の改変および承認に関する管理方法を規定している。
「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 バージョン管理規定」は、TOE の各構成要素に対するバージョンの付与と記録に関する管理方法を規定している。
したがって、上記規定類により **ACM_AUT.1** を実現できる。

ACM_CAP.4（生成の支援と受入手続き）
「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 構成リスト」は、TOE の開発に関する構成要素のリストおよび各要素間の依存関係を記述している。
「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 構成管理記録」は、構成リストの改変履歴および承認結果を記録している。
「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 バージョン管理記録」は、バージョン管理規定に基づき管理された各構成要素の改変履歴を記録している。
したがって、上記文書類により **ACM_CAP.4** を実現できる。

ACM_SCP.2（問題追跡の CM 範囲）
「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 構成リスト」は、TOE の開発に関する構成要素のリストおよび各要素間の依存関係を記述している。
「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 構成管理記録」は、構成リストの改変履歴および承認結果を記録している。
「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 バージョン管理記録」は、バージョン管理規定に基づき管理された各構成要素の改変履歴を記録している。
したがって、上記記録類の内容から問題が発生した TOE の構成要素を追跡することにより **ACM_SCP.2** を実現できる。

ADO_DEL.2（改変の検出）
「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 配付と運用統括文書」は、モジュールの適切な配付手順が記述されている。
「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 モジュール管理簿」は、TOE の製造時における搭載されたモジュールと出荷に関する内容を記録する。
したがって、上記文書類により **ADO_DEL.2** を実現できる。

ADO_IGS.1（設置、生成、及び立上げ手順）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 配付と運用統括文書」は、製造時における TOE のソフトウェアをハードウェアであるカード上へ搭載するための手順と注意事項が記述されている。
「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 ガイダンス統括文書」は、納品後の TOE の利用方法が記述されている。
したがって、上記文書類から TOE の設置および初期データの設定方法が明確になり **ADO_IGS.1** を実現できる。

ADV_FSP.2（完全に定義された外部インタフェース）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 機能仕様書」は、非形式的な様式で TOE が提供するすべてのセキュリティ機能の仕様および外部インタフェースを記述する。
したがって、上記仕様書により **ADV_FSP.2** を実現できる。

ADV_HLD.2（セキュリティ実施上位レベル設計）

「AP 実行環境 取扱説明書」は、APE に対する非形式的な上位レベルの設計内容を記述する。
「住基 CD 部 機能仕様書」は､CD 管理部に対する非形式的な上位レベルの設計内容を記述する。
「CM 部 機能仕様書」は、AP 管理部に対する非形式的な上位レベルの設計内容を記述する。
「住基 AP 部 機能仕様書」は、住基 AP に対する非形式的な上位レベルの設計内容を記述する。
「ｾｷｭﾘﾃｨﾗｲﾌﾞﾗﾘ CC 認証対応版 機能仕様書」は、ｾｷｭﾘﾃｨﾗｲﾌﾞﾗﾘに対する非形式的な上位レベルの設計内容を記述する。
「共通 RAM 管理ライブラリ CC 認証対応版 機能仕様書」は、RAM 管理ライブラリに対する非形式的な上位レベルの設計内容を記述する。
「Flash 管理ライブラリ CC 認証対応版 機能仕様書」は、Flash 管理ライブラリに対する上位レベルの設計内容を記述する。
したがって、上記設計書類により **ADV_HLD.2** を実現できる。

ADV_IMP.1（TSF の実装のサブセット）

「AP 実行環境 ソースコード」は、APE に対する実装を記述する。
「住基 CD 部 ソースコード」は、CD 管理部に対する実装を記述する。
「CM 部 ソースコード」は、AP 管理部に対する実装を記述する。
「住基 AP 部 ソースコード」は、住基 AP に対する実装を記述する。
「ｾｷｭﾘﾃｨﾗｲﾌﾞﾗﾘ CC 認証対応版 ソースコード」は、ｾｷｭﾘﾃｨﾗｲﾌﾞﾗﾘに対する実装を記述する。
「共通 RAM 管理ライブラリ CC 認証対応版 ソースコード」は、RAM 管理ライブラリに対する実装を記述する。
「Flash 管理ライブラリ CC 認証対応版 ソースコード」は、Flash 管理ライブラリに対する実装を記述する。
上記により TOE に実装されるすべてのセキュリティ機能に対する実装を記述している。
したがって、上記ソースコードにより **ADV_IMP.1** を実現できる。

ADV_LLD.1（記述的下位レベル設計）

「AP 実行環境 詳細設計書」は、APE に対する非形式的な機能仕様を記述する。

「住基 CD 部 詳細設計書」は､CD 管理部に対する非形式的な下位レベルの設計内容を記述する。

「CM 部 詳細設計書」は、AP 管理部に対する非形式的な下位レベルの設計内容を記述する。

「住基 AP 部 詳細設計書」は、住基 AP に対する非形式的な下位レベルの設計内容を記述する。

「ｾｷｭﾘﾃｨﾗｲﾌﾞﾗﾘ CC 認証対応版 詳細設計書」は、ｾｷｭﾘﾃｨﾗｲﾌﾞﾗﾘに対する非形式的な下位レベルの設計内容を記述する。

「共通 RAM 管理ライブラリ CC 認証対応版 詳細設計書」は、RAM 管理ライブラリに対する非形式的な下位レベルの設計内容を記述する。

「Flash 管理ライブラリ CC 認証対応版 詳細設計書」は、Flash 管理ライブラリに対する非形式的な下位レベルの設計内容を記述する。

したがって、上記設計書類により **ADV_LLD.1** を実現できる。

ADV_RCR.1（非形式的対応の実証）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 TOE 要約仕様各段落対応表」は、ST における TOE 要約仕様と機能仕様書における機能との対応付けを記述する。

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 セキュリティ機能要件対応表」は、機能仕様書と上位レベルの設計書の機能との対応付けを記述する。

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 詳細設計書」は、上位レベルの設計書の機能と下位レベルの設計書の機能との対応付けを記述する。

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 対応表」は、下位レベルの設計書の機能とソースコードとの対応付けを記述する。

したがって、上記対応表により **ADV_RCR.1** を実現できる。

ADV_SPM.1（非形式的なセキュリティ方針モデル）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 セキュリティポリシモデル」は、TOE の利用方法としてセキュリティ方針に対して開発者によって想定されるモデルを記述している。また、**FPT_RCV.2** の自動回復におけるセキュアな状態が何かについて記述している。

したがって、上記文書により **ADV_SPM.1** を実現できる。

AGD_ADM.1（管理者ガイダンス）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 カード発行者ガイダンス」は、TOE を運用するためのガイドラインが記述されており、ガイダンス文書として要求される中身が含まれた文書である。また、**FPT_RCV.2** の自動回復におけるメンテナンスモードについて記述している。

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 AP 搭載管理者ガイダンス」は、TOE を運用するためのガイドラインが記述されており、ガイダンス文書として要求される中身が含まれた文書である。また、**FPT_RCV.2** の自動回復におけるメンテナンスモードについて記述している。

したがって、上記文書により **AGD_ADM.1** を実現できる。

AGD_USR.1（利用者ガイダンス）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　カード発行者ガイダンス」は、TOE を利用するためのガイドラインも記述されており、ガイダンス文書として要求される中身が含まれた文書である。

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　AP 搭載管理者ガイダンス文書」は、TOE を利用するためのガイドラインも記述されており、ガイダンス文書として要求される中身が含まれた文書である。

したがって、上記仕様書により **AGD_USR.1** を実現できる。

ALC_DVS.1（セキュリティ手段の識別）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　開発セキュリティ管理規定」は、TOE の開発環境に対する管理方法が規定されている。

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　文書管理規定」は、開発で利用される文書類の管理方法が規定されている。

したがって、上記規定で TOE 開発の環境および手順が明確になり **ALC_DVS.1** を実現できる。

ALC_LCD.1（開発者によるライフサイクルモデルの定義）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　ライフサイクルモデル」は、開発者によって意図された TOE のライフサイクルに関するモデルを定義してある。

したがって、上記文書により **ALC_LCD.1** を実現できる。

ALC_TAT.1（明確に定義された開発ツール）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 開発ツール管理規定」は、開発で利用するツールに対する管理方法が規定されている。

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 ツール管理記録」は、上記規定に基づいて実施されたツールの管理記録を含んでいる。

したがって、上記文書類により **ALC_TAT.1** を実現できる。

ATE_COV.2（カバレージの分析）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 試験項目対応表」は、TOE の開発者によって実施された試験項目と設計書で記述された機能との対応付けとそのカバレージに対する分析結果を含んでいる。

したがって、上記対応表により **ATE_COV.2** を実現できる。

ATE_DPT.1（テスト：上位レベル設計）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 試験深さ分析書」は、TOE の開発者によって実施された試験項目の深さに対する分析結果を含んでいる。

したがって、上記文書類により **ATE_DPT.1** を実現できる。

ATE_FUN.1（機能テスト）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 試験項目書」は、高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 に対して開発者によって実施された試験の項目が記述されている。

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　試験手順書」は、高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 に対して開発者によって実施された試験の手順が記述されている。

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　試験成績書」は、高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0 に対して開発者によって実施された試験の結果が記述されている。

したがって、上記成績書により **ATE_FUN.1** を実現できる。

ATE_IND.2（独立テストーサンプル）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　テスト環境」は、開発者によって実施された試験の環境を含んでいる。

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　テストプログラム」は、開発者によって実施された試験で利用されたプログラムを含んでいる。

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　テストデータ」は、開発者によって実施された試験に必要なデータを含んでいる。

「アダプタ対応型高速版住基カードソフトウェア ver.2.00」は、開発者によって開発された TOE そのものである。

したがって、上記提供物を利用することで評価者による独立テストの実施を助け、開発者の実施した試験結果と比較することにより **ATE_IND.2** を実現できる。

AVA_MSU.3（セキュアでない状態の分析とテスト）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　開発者誤使用防止分析報告書」は、開発者によって実施された TOE の誤使用を防止する対策とセキュアでない状態に対する分析の結果を含んでいる。

したがって、上記報告書により **AVA_MSU.3** を実現できる。

AVA_SOF.1（TOE セキュリティ機能強度評価）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　開発者セキュリティ機能強度評価報告書」は、開発者によって実施された TOE のセキュリティ機能強度に対する評価の結果を含んでいる。

したがって、上記報告書により **AVA_SOF.1** を実現できる。

AVA_VLA.2（独立脆弱性テスト）

「ｱﾀﾞﾌﾟﾀ対応型高速版住基ｶｰﾄﾞｿﾌﾄｳｪｱ ver.2.0　開発者脆弱性分析報告書」は、開発者によって実施された TOE の脆弱性に対する分析の結果を含んでいる。

したがって、上記報告書により **AVA_VLA.2** を実現できる。

付録 A　用語集

本 ST で利用される略号および用語の定義を以下に整理する。

＜CC に関連する略語＞
以下の用語は、CC part1 において定義されている通りに利用する。

CC：　コモンクライテリア(Common Criteria)
EAL：　評価保証レベル(Evaluation Assurance Level)
IT：　情報技術(Information Technology)
PP：　プロテクションプロファイル(Protection Profile)
SOF：　機能強度(Strength of Function)
ST：　セキュリティターゲット(Security Target)
TOE：　評価対象(Target of Evaluation)
TSF：　TOE セキュリティ機能(TOE Security Functions)

＜標準に関連する略語＞
以下の標準に関する略号の定義は、以下の通りである。

ANSI：American National Standerds Institute
PKCS：Public-Key Cryptography Standards

＜カード全般に関連する略号および用語＞
以下の略号および用語は、本 ST において以下の定義に基づいて利用される。

住基カード：住民基本台帳用 IC カード
住基ネット：住民基本台帳ネットワークシステム
CD：　カードドメイン(Card Domain)、カードに一つだけ存在し、カード発行者が管理する領域。
AP：アプリケーション、ここではカードに搭載されるプログラムを表す。カードに複数存在し、発行後のカードに搭載が可能である。
SD：セキュリティドメイン、カードに搭載される AP を管理する領域。
製造者：TOE をカードに搭載し、発行市町村へカードを納入する役割で、製造ベンダに対応する。
発行者：TOE の搭載されたカードを発行する役割で、市町村に対応する。
所有者：TOE の搭載されたカードの交付を受けてカードを所有する役割で、住民に対応する。
APE：　アプリケーション実行環境、チップに搭載される AP のドメイン分離を管理する。
CD 管理部：CD のセキュリティに関する設定を管理する。
AP 管理部：カードにロードして搭載される AP を管理する。

住基 AP：住基カード AP、住基カード用の市町村業務のための AP
EF： 基礎ファイル、データを格納する領域である。
IEF： PIN または鍵の認証で利用するデータを格納する領域である。
WEF： 作業で利用するデータを格納する領域である。
SE： 認証や暗号化で利用する鍵を決定するための属性で、セキュリティ属性の 1 つである。
アクセス管理属性：アクセス管理の操作に対する条件を管理するセキュリティ属性。
認証ステータス：認証結果を保持するセキュリティ属性。
アダプタ：業務用端末上で動作するソフトウェアで、住基仕様で規定されたインタフェースに基づき、住基カードの実装に対応したコマンドメッセージを生成する。製造者毎に異なる住基カードの実装の差を吸収して共通のインタフェースで住基カードを利用できるようにするソフトウェアであり、業務ソフトウェアから呼び出される。
モジュール： カード上に搭載されたソフトウェアのプログラム単位での構成要素である。
プロセス： カード上に存在するモジュールがサブジェクトとして動作している状態である。

＜AP 管理部に関連する用語＞

証明書発行局：公開鍵に対する証明書を発行するシステム。
AP 搭載管理者：AP 管理領域において AP の搭載全般を管理する。

付録 B　参照資料

本 ST で参照している資料を以下に示す。**[ ]**は各資料に対する引用識別子を表す。

[JIS-1]　JIS X 5070-1:2000 セキュリティ技術－情報技術セキュリティの評価基準－
第１部：総則及び一般モデル

[JIS-2]　JIS X 5070-2:2000 セキュリティ技術－情報技術セキュリティの評価基準－
第２部：セキュリティ機能要件

[JIS-3]　JIS X 5070-3:2000 セキュリティ技術－情報技術セキュリティの評価基準－
第３部：セキュリティ保証要件

[CC-1]　情報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
2005 年 8 月 バージョン 2.3 CCMB-2005-08-001　（IPA 翻訳文書 第 1.0 版）

[CC-2]情報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 ：セキュリティ機能要件
2005 年 8 月 バージョン 2.3 CCMB-2005-08-002　（IPA 翻訳文書 第 1.0 版）

[CC-3]情報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 ：セキュリティ保証要件
2005 年 8 月 バージョン 2.3 CCMB-2005-08-003　（IPA 翻訳文書 第 1.0 版）

[CEM]　情報技術セキュリティ評価のための共通方法：評価方法
2005 年 8 月 バージョン 2.30 CCMB-2005-08004　（IPA 翻訳文書 第 1.0 版）

[住基 PP]　住民基本台帳用 IC カードのセキュリティ要求仕様(プロテクションプロファイル)
バージョン 2.0　2003 年 4 月 16 日 財団法人地方自治情報センター発行

[補足-0512]　補足-0512　2005年12月

[住基仕様 23]　住民基本台帳ネットワークシステム住民基本台帳カード仕様書　第 2.3 版
2003 年 7 月 15 日 財団法人地方自治情報センター発行

[CC-1E]　Common Criteria for Information Technology Security Evaluation
Part1:Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[CC-2E]　Common Criteria for Information Technology Security Evaluation
Part2:Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[CC-3E] Common Criteria for Information Technology Security Evaluation
Part3:Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[CEM-E] Common Methodology for Information Technology Security Evaluation (CEM)
Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[CCMB-0512] Interpretations-0512

[JIL] Application of Attack Potential to Smartcards, Version 2.5, Revision 1,
April 2008 CCDB-2008-04-001

[AIS] Application Notes and Interpretation of the Scheme, 01 June 2004, Version 1.00