SecureTicket Core
セキュリティターゲット
(ASE)
BA-DA-0001
Rev21

2007年3月14日

横河電機株式会社
YOKOGAWA ◆

― 修正履歴 ―

発行年月日	版数	変更内容	作成者	チェック者	承認者
2005/7/12	1.00	初版作成	武部 達明	橋口 昌弘	武部 達明
2005/7/21	1.10	レビュー指摘事項反映	武部 達明	高松 家廣	武部 達明
2005/9/12	1.11	レビュー指摘事項反映、誤記訂正	武部 達明	橋口 昌弘	武部 達明
2005/10/11	1.12	レビュー指摘事項反映、誤記訂正	武部 達明	橋口 昌弘	武部 達明
2005/11/4	1.13	レビュー指摘事項反映、誤記訂正	武部 達明	高松 家廣	武部 達明
2006/1/30	1.20	レビュー指摘事項反映、誤記訂正	武部 達明	高松 家廣	武部 達明
2006/4/7	1.30	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/5/15	1.40	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/5/24	1.41	誤記訂正	武部 達明	星野 浩志	武部 達明
2006/5/31	1.42	誤記訂正	武部 達明	星野 浩志	武部 達明
2006/6/16	1.43	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/7/11	1.44	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/7/12	1.45	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/7/13	1.50	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/7/14	2	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/7/20	3	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/7/21	4	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/7/24	5	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/7/27	6	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/7/28	7	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/9/2	8	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/9/6	9	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/9/12	10	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/9/13	11	誤記訂正	武部 達明	星野 浩志	武部 達明
2006/9/15	12	誤記訂正	武部 達明	星野 浩志	武部 達明
2006/9/26	13	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/10/16	14	レビュー指摘事項反映、誤記訂正	武部 達明	星野 浩志	武部 達明
2006/10/20	15	誤記訂正	武部 達明	星野 浩志	武部 達明
2006/10/23	16	誤記訂正	武部 達明	星野 浩志	武部 達明
2006/10/31	17	誤記訂正	武部 達明	星野 浩志	武部 達明
2006/12/1	18	誤記訂正	武部 達明	星野 浩志	武部 達明
2006/12/11	19	誤記訂正	武部 達明	星野 浩志	武部 達明
2007/3/12	20	誤記訂正	武部 達明	高松 家廣	武部 達明
2007/3/14	21	誤記訂正	武部 達明	高松 家廣	武部 達明

― 目次 ―

― 図目次 ―

― 表目次 ―

― リスト目次 ―

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合、参考資料、及び表記規則、用語、略語について記述する。

1.1. ST 識別

1.1.1. ST の識別と管理

ST 名称： SecureTicket Core セキュリティターゲット
ST バージョン： 第 21 版
発行日： 2007 年 3 月 14 日
作成者： 横河電機株式会社

1.1.2. TOE の識別と管理

TOE 名称： SecureTicket Core
TOE バージョン： 5.0.0.0.0

1.1.3. 使用する CC のバージョン

CC バージョン 2.1
補足-0210 第 2 版
補足-0407

1.2. ST 概要

本 ST は、横河電機株式会社製 製品「SecureTicket Core」について記述している。「SecureTicket Core」は、ネットワーク環境において、運用されているサーバ群を情報漏洩や不正アクセスなどから保護するための統合セキュリティソフトウェアである。

1.3. CC 適合

本 ST は、以下の CC に適合する。

①. CC バージョン 2.1 パート 2 適合
②. CC バージョン 2.1 パート 3 適合
③. EAL3 追加 追加コンポーネント ADV_SPM.1

1.4.参考資料

略　称	資　　料　　名
[CC_Part1_J]	情報技術セキュリティ評価のためのコモンクライテリア パート１：概説と一般モデル　1999 年８月 バージョン 2.1 CCIMB-99-031 2003-12-31 付け解釈組込み
[CC_Part2_J]	情報技術セキュリティ評価のためのコモンクライテリア パート２：セキュリティ機能要件　1999 年８月 バージョン 2.1 CCIMB-99-032 2003-12-31 付け解釈組込み
[CC_Part3_J]	情報技術セキュリティ評価のためのコモンクライテリア パート３：セキュリティ保証要件　1999 年８月 バージョン 2.1 CCIMB-99-033 2003-12-31 付け解釈組込み
[CEM_Part1_J]	情報技術セキュリティのための共通評価方法論 CEM-97/017 パート１：概説と一般モデル バージョン 0.6 97/01/11
[CEM_Part2_J]	情報技術セキュリティ評価のための共通評価方法論 CEM-99/045 パート２:評価方法論 バージョン１．０ 1999 年８月 2003-12-31 付け解釈組込み
[Int-0210_2_J]	補足-0210 第２版
[Int-0407_J]	補足-0407
[CC_Part1_E]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model August 1999 version 2.1 CCIMB-99-031 Annotated with interpretations as of 2003-12-31
[CC_Part2_E]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements August 1999 version 2.1 CCIMB-99-032 Annotated with interpretations as of 2003-12-31
[CC_Part3_E]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements August 1999 version 2.1 CCIMB-99-033 Annotated with interpretations as of 2003-12-31
[CEM_Part1_E]	Common Evaluation Methodology for Information Technology Security CEM-97/017 Part 1：Introduction and general model Version 0.6 97/01/11

[CEM_Part2_E]	Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2 : Evaluation Methodology Annotated with interpretations as of 2003-12-31 version 1.0 August 1999
[Int_0407_E]	CCIMB Interpretations-0407

1.5.表記規則、用語、略語

1.5.1.表記規則

第3章の前提条件、脅威、組織のセキュリティ方針、及び第4 章のセキュリティ対策方針では、それぞれのラベルを**ボールド体フォント**で記述し、続けてその定義を通常フォントで記述する。
第5章のセキュリティ機能要件では、操作内容を***ボールド斜体フォント***で記述する。

1.5.2.用語

本ST では、各用語を以下の意味で用いる。

認証（authentication）
　情報の提供元が、それに対するアクセスを試みる者に対して、本当に当人であるかを検査する作業。

パスワード（password）
　特定のサービスの利用や、特定のデータのアクセスを試みるときに、その利用権利・アクセス権利のある利用者であることを検査するために使われる、文字列。

IT（Information Technology）
　コンピュータやデータ通信に関する技術を総称的に表す語。

ネットワーク（network）
　複数のコンピュータ間で情報通信が行なえるように接続すること。そのための設備。

サーバ（server）
　ネットワークにおいて、クライアントに対し、自身の持っている機能やデータを提供するコンピュータのこと。

クライアント（client）
　ネットワークにおいて、サーバの提供する機能やデータを利用するコンピュータのこと。

悪用（exploitation）
　本来の用途とは違った不正な目的のために用いること。

インターネット（internet）
　通信プロトコルTCP/IPという機種に依存しない標準化されたプロトコルを用いて全世界のネットワークを相互に接続した巨大なコンピュータネットワークを指す。

イントラネット（intranet）

通信プロトコルTCP/IPを初めとするインターネット標準の技術を用いて構築された組織内ネットワークを指す。

ファイアウォール（firewall）

組織内のコンピュータネットワークへ外部から侵入されるのを防ぐシステム。また、そのようなシステムが組みこまれたコンピュータ。

脆弱性（vulnerability）

コンピュータやネットワークなどの情報システムにおいて、第三者が脅威となる行為（機密情報の漏洩、情報の改竄、システムの乗っ取りなど）に利用できる可能性のあるシステム上の欠陥や仕様上の問題点。

SSL（secure socket layer）

インターネット上で情報を暗号化して安全に送受信するプロトコル。WWWやFTPなどのデータを暗号化し、プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信することができる。

ワンタイムパスワード（OTP、 One Time Password）

端末からネットワークを通じてサーバコンピュータを利用する際に、アクセスしてくる人間が許可利用者かどうかを検証する認証技術のひとつ。通常の認証方式では、通信経路上でパスワードが「盗み聞き」されてしまう可能性がある。ワンタイムパスワードは、利用者のパスワードが毎回異なった文字列としてサーバに送信されるため、通信経路上でサーバと端末のやり取りを盗み聞きされても、同じパスワードが二度と使われないため、サーバが不正使用されることはない。

DMZ (Demilitarized Zone)

「非武装地帯」の略。インターネットに接続されたネットワークにおいて、ファイアウォールにより外部ネットワークからも内部ネットワークからも隔離された区域のこと。

IETF

TCP/IP などのインターネットで利用される技術を標準化する組織。

HTTP

Web サーバとクライアント(Web ブラウザなど)がデータを送受信するのに使われるプロトコル。HTML 文書や、文書に関連付けられている画像、音声、動画などのファイルを、表現形式などの情報を含めてやり取りできる。IETF によって、規格化されている。

プロキシ（proxy）

企業内ネットワークとインターネットの境界に置かれ、直接インターネットに接続できない内部ネットワークのコンピュータに代わって「代理」としてインターネットとの接続を行うコンピュータのこと。またはその機能を実現するソフトウェア。

Java Virtual Machine (JVM)

Java バイトコードを、解釈し、実行するマシンのマシンコードに変換して実行するソ

フトウェア。

Java バイトコード

Java 言語で記述されたソースコードをコンパイラが実行用に生成する中間コードの一種である。

セッション（session）

Web サイトを訪れるユーザのアクセスを数える単位の一つ。サイト内で行なう一連の行動をまとめて 1 セッションという。

USB（Universal Serial Bus）

キーボード、マウス、モデムなどの周辺機器とパソコン、ワークステーションなどのコンピュータを結ぶデータ転送路の規格。あまり高速でない（12Mbps）USB1.1 という規格と高速な USB2.0 とがある。

USB ポート（USB port）

USB ケーブルを差し込む接続口（コネクタ）。

認証データ（Authentication Data）

利用者の識別情報を検証するために使用されるデータである。

1.5.3.略語

CC : Common Criteria
EAL : Evaluation Assurance Level
IT : Information Technology
OS : Operating System
PC : Personal Computer
PP : Protection Profile
SOF : Strength of Function
TOE : Target of Evaluation
TSC : TSF Scope of Control
TSF : TOE Security Function
TSP : TOE Security Policy

2. TOE 記述

2.1. TOE 種別

TOE の種別は ネットワーク環境で使用される 認証機能付きリバースプロキシ ソフトウェア製品である。

2.2. 用語定義

本STで使用する用語の定義を以下に示す。

表 2-1 用語定義

番号	用　語	定　　義
1	セキュアチケット SecureTicket	本 TOE 製品を組み込んだエンドユーザ向け製品の名称
2	セキュアチケットコア SecureTicket Core	SecureTicket の基本機能部分であり、本 TOE のこと
3	サーバモジュール Server Module	SecureTicket Core サーバで動作する TOE の Java アプリケーション
4	クライアントモジュール Client Module	SecureTicket クライアントで動作する TOE の Java アプレット。SecureTicket クライアントがブラウザを使ってサーバモジュールにアクセスすることでダウンロードされる。
5	チケットデータ Ticket Data	許可利用者が TOE に認証されるために必要な認証データを生成するために使われる固有情報
6	内部ネットワーク Internal Network	組織内のネットワーク
7	外部ネットワーク External Network	内部ネットワーク以外のネットワークで、通常はインターネットを指す。内部ネットワークとはファイアウォールを介して接続される。
8	SecureTicket Core サーバ SecureTicket Core Server	サーバモジュールを動作させるサーバ。
9	保護サーバ Protected Server	TOE の保護対象資産が格納されるサーバ。

10	公開 URL Public URL	保護サーバへアクセスするために TOE 上に用意された URL。公開 URL は、公開保護 URL か公開非保護 URL のいずれかである。
11	公開保護 URL Protected Public URL	TOE が保護する公開 URL
12	公開非保護 URL Unprotected Public URL	TOE が保護しない公開 URL
13	実体 URL Actual URL	保護サーバに存在する実際の URL で、TOE が用意する公開 URL に関係づけられる。実体 URL は、実体保護 URL か実体非保護 URL のいずれかである。
14	実体保護 URL Actual Protected URL	TOE が保護する実体 URL
15	実体非保護 URL Actual Unprotected URL	TOE が保護しない実体 URL
16	リンク設定情報 Link Attribute Information	公開 URL と実体 URL とを対応づけるためのリンク情報およびそのリンクに対応づける保護属性などが設定された情報。
17	基本設定ファイル Configuration File	リンク設定情報などを格納したファイル
18	リバースプロキシ機能 Reverse Proxy Function	保護サーバの代理でクライアントからの http プロトコルのリクエストを受けてその結果をクライアントに応答する機能。
19	チケット Ticket	TOE への認証に使用するために一般利用者が取得し、所持するメディア（媒体）のことで、チケットデータが格納されている。
20	ePass	USB トークンの一種で、チケットとして使用することができるデバイス。
21	ePass ドライバ ePass driver	ePass に対して SecureTicket Core サーバやクライアントから USB ポートを経由して読み書きするドライバ。
22	SecureTicket クライアント	一般利用者が公開 URL にアクセスを行うために内部ネットワークまたは外部ネットワークに接続された PC。許可利用者用

	SecureTicket Client	に発行されたチケットを装着している。
23	パスワード精査設定ファイル Password scrutinization specification file	利用者が選択してしまう恐れがある『推測されやすいパスワード』、『弱いパスワードの仕様』を登録するデータベースで、管理者によって編集される。この辞書に載っているパスワードを設定しようとしても、設定できない。
24	ユーザ名 User Name	許可利用者が TOE に自分を認識させるために用いる名前などの文字列。
25	ユーザ ID User ID	TOE が許可利用者を識別するために内部的に用いるハッシュ値。
26	グループ名 Group Name	一般利用者の所属するグループの名前。
27	グループ ID Group ID	TOE がグループ名を識別するために内部的に用いるハッシュ値。
28	ユーザ情報 User Information	ユーザ情報は、TOE に登録される許可利用者のユーザ名、ユーザ ID、パスワードなどを示す。
29	グループ情報 Group Information	グループ情報は、TOE に登録されるグループの　グループ名、グループ ID、ユーザ ID とグループ ID の関係、複数グループ ID 間の関係などを示す。
30	ユーザ・グループ情報 User Group Information	上記のユーザ情報とグループ情報の総称。
31	ユーザ・グループ情報ファイル User Group Information File	ユーザ情報、グループ情報を格納したファイルの総称。
32	設定ツール Configuration Tool	管理者が基本設定ファイルやパスワード精査設定ファイルを編集するために使うツール。TOE の範囲対象外である。
33	SecureTicket GUI	管理者が作成する管理用の GUI。TOE の範囲対象外である。
34	ユーザマネージャ GUI	上記 33 のうち、ユーザ・グループ情報を保守するための GUI
35	プロセスモニタ GUI	上記 33 のうち、サーバモジュールのプロセスを再起動・停止する GUI
36	管理者クライアント Administrator	管理者が、上記 33 を動作させることができる PC。管理者用に発行されたチケットを装着している。

	Client	
37	セッション ID Session ID	一般利用者が公開保護 URL にアクセスする際、TOE が識別・認証に成功した一般利用者を識別するために生成した識別番号。ハッシュ値である。
38	連続失敗認証検出回数 Limit of successive authentication errors	TSP 侵害の可能性があると考えられる、一般利用者または管理者の TOE への連続失敗認証回数。
39	SecureTicket ライセンスファイル SecureTicket License File	SecureTicket Core の購入者に対してソフトウェアを使用することを許諾することを認める情報を記述したファイル。
40	SCDKLib	SecureTicket Core Developers’ Kit Library 設定ツールおよび SecureTicket GUI に使用されるライブラリ。
41	SCDK I/F	設定ツールおよび SecureTicket GUI が SCDKLib の機能を使用するときに用いられるインタフェース。
42	独自通信プロトコル Proprietary Communication Protocol	SecureTicket Core で用いられる独自の通信プロトコル。
43	認証情報 Authentication Information	利用者の認証データを生成するために使われる利用者固有のデータ。パスワードやチケットデータなど。
44	SecureTicket Core 暗号運用標準 SecureTicket Core Cryptography Operational Standards	横河電機株式会社の「SecureTicket Core」開発において使用する暗号方式を定めた基準。
45	SecureTicket Core 共通鍵生成アルゴリズム SecureTicket Core	AES 暗号鍵のために用いられる横河電機株式会社独自のアルゴリズムであり、「SecureTicket Core 暗号運用標準」に定められている。

	Symmetric Key Generation Algorithm	
46	サーバモジュール制御 I/F Server Module Control I/F	サーバモジュールが、独自通信プロトコルで行う通信のインタフェース。
47	シード Seed	ワンタイムパスワードを生成するときに使われる文字列。
48	セキュリティ強化モード Security Enforcement Mode	SecureTicket Core を TOE として運用するとき、接続環境や各種動作設定をよりセキュアにするために配慮したモード。
49	セッション有効期限 Sessin Time Limit	認証成功日時（時刻）または最後に保護対象資産にアクセスした日時（時刻）から認証の有効時間を加えた日時（時刻)。

2.3. TOE 概要

2.3.1. TOE の概要動作

TOEは、内部ネットワーク外部ネットワークを分離するファイアウォールのDMZまたは内部ネットワークに配置され、予め登録した実体URLを、予め登録した利用者のみに、アクセス許可する機能を提供する。同時に、一般利用者および管理者に対して管理機能を提供する。
TOE を利用する環境は『図 2-1 SecureTicket Core の利用環境 1』または『図 2-2 SecureTicket Core の利用環境２』に示されるものを想定する。

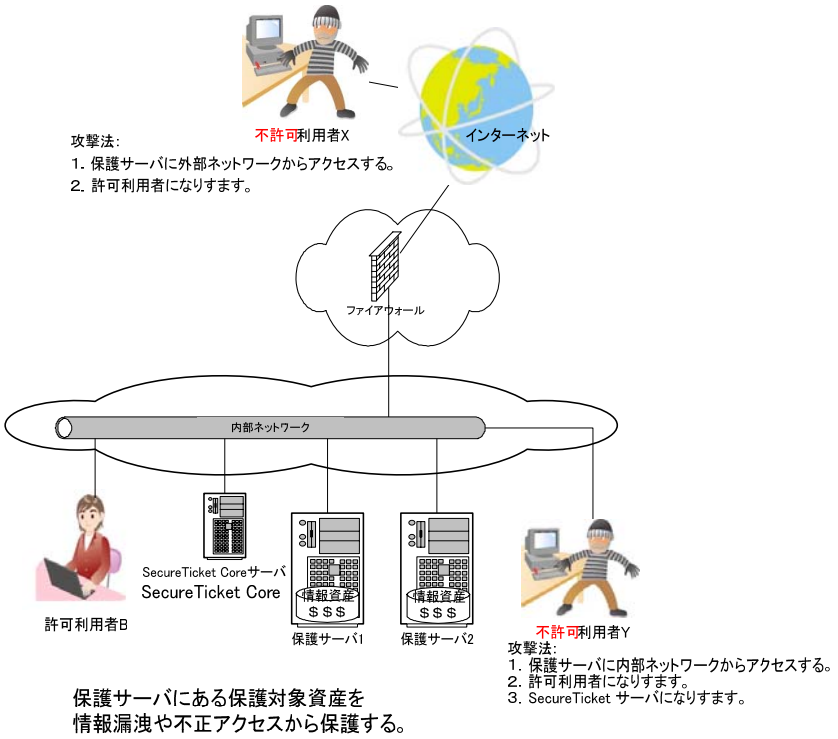

図 2-1 SecureTicket Core の利用環境 1

図 2-1 では、SecureTicket Core サーバが内部ネットワークに配置されている。

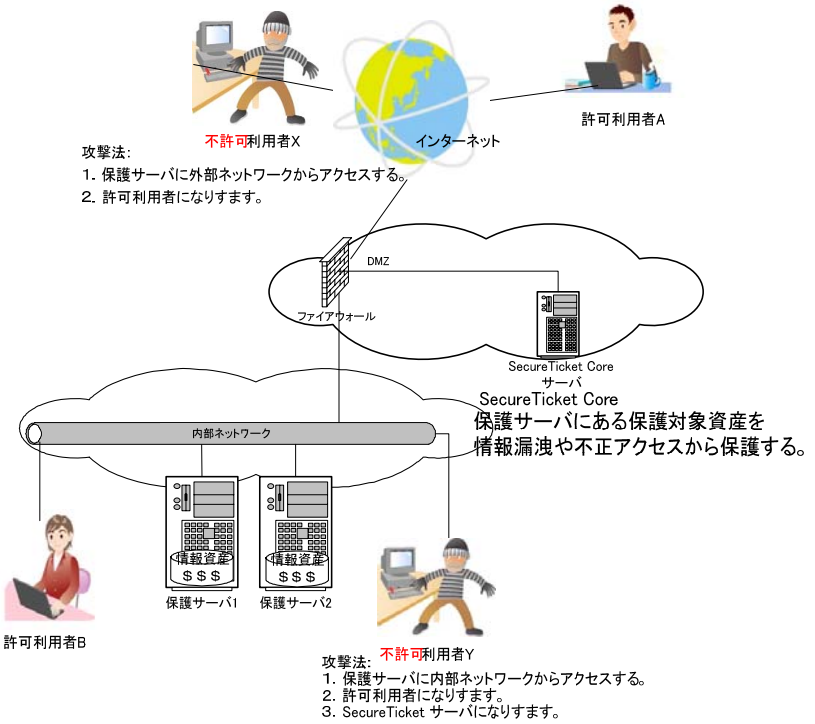

図 2-2 SecureTicket Core の利用環境２

図 2-2 では SecureTicket Core サーバが DMZ に配置されている。

TOE は、外部ネットワークまたは内部ネットワークのクライアントから公開 URL へのアクセスリクエストを受け取った場合、以下の『規則 1 公開 URL へのアクセスルール』のルールセット１もしくはルールセット２が満たされることを確かめる。

公開 URL へのアクセスを許可するか、拒否するかは、『規則 3 アクセス許可・アクセス拒否ルール』に従うように、管理者が設定を行う。

ルールセット１：

1. リクエストは、公開非保護 URL に対するアクセスである。

または、

ルールセット２：

1. リクエストは、公開保護 URL に対するアクセスである。 かつ
2. リクエスト発信者は、一般利用者として TOE に登録されている。 かつ
3. リクエスト発信者は、『規則 2 一般利用者の公開 URL へのアクセス時の識別・認証ルール』に従って TOE に正しく認証された。 かつ

4. 当該 公開保護 URL のリンク設定情報は以下のいずれかに合致する。
   - リクエスト発信者が『アクセス許可』の対象になっている　　または、
   - リクエスト発信者が『アクセス拒否』の対象になっていない　　または、
   - リンク設定情報が何も登録されていない。

規則 1 公開 URL へのアクセスルール

一般利用者が公開 URL にアクセスするときの認証のルール：

1. 当該利用者のアカウントはロックされていない。　　かつ
2. 当該利用者の認証は、当該利用者にアクセスが許されている日時に行われている。かつ
3. 本人のパスワードを提示できる。　かつ
4. 本人のチケットを有している。

規則 2 一般利用者の公開 URL へのアクセス時の識別・認証ルール

上記『規則 1 公開 URL へのアクセスルール』のルールセット１もしくはルールセット２の結果が満たされたとき、当該アクセスリクエストを保護サーバに渡す。上記ルールセット１もルールセット２も満たされない場合、TOE は、エラーか認証リクエストで応答する。

アクセス許可・アクセス拒否のルール：

1. 保護サーバ上の実体保護 URL を TOE 上の公開保護 URL に関連づけ、保護サーバ上の実体非保護 URL を TOE 上の公開非保護 URL に関連づける。
2. TOE に登録されている一般利用者に、アクセス規則を適用できるようにグループ名を関連付ける。
3. 公開保護 URL に対して、グループからのアクセスについての許可・拒否の属性を設定する。
   (ア) 公開保護 URL に許可属性を設定した場合、そのグループに属している一般利用者は『アクセス許可』され、それ以外のグループの一般利用者は『アクセス拒否』される。
   (イ) 公開保護 URL に拒否属性を設定した場合、そのグループに属している一般利用者は『アクセス拒否』され、それ以外のグループの一般利用者は『アクセス許可』される。
4. 公開非保護 URL　はすべての一般利用者のアクセスを許可する。

規則 3 アクセス許可・アクセス拒否ルール

TOE は、外部ネットワークまたは内部ネットワークのクライアントから一般利用者のクライアント管理機能へのアクセスリクエストを受け取った場合、以下の『規則 4 一般利用者のクライアント管理機能へのアクセスルール』が満たされることを確かめる。

また TOE は、外部ネットワークまたは内部ネットワークのクライアントから管理者用管理機能へのアクセスリクエストを受け取った場合、以下の『規則 6 管理者用管理機能へのアクセスルール』が満たされることを確かめる。

当該規則が満たされている場合、アクセスを許可し、それ以外の場合は、エラーで応答する。

ルールセット３：

1. リクエスト発信者は、一般利用者として TOE に登録されている。　　かつ
2. リクエスト発信者は、『規則 5 一般利用者のクライアント管理機能へのアクセス時の識別・認証ルール』に従って TOE に正しく認証された。

規則 4 一般利用者のクライアント管理機能へのアクセスルール

一般利用者がクライアント管理機能にアクセスするときの認証のルール：

1. 当該利用者のアカウントはロックされていない。　　かつ
2. リクエストは、リクエスト発信者にアクセスが許されている日時に行われている。かつ次のいずれかに該当する。
3. 一般利用者がクライアント管理機能（パスワード変更）を使用するときの認証ルール
   - 本人のパスワードを提示できる。　かつ
   - 本人のチケットを有している。
4. 一般利用者がクライアント管理機能（チケット発行）を使用するときの認証ルール
   - 本人のユーザ名と本人のパスワードを提示できる。　かつ
   - 当該一般利用者がチケット発行可能状態である。（これは、管理者が一般利用者に本人のチケットを発行してもらうため、「2.6.2 管理機能群」を用いて発行可能状態とする。）

規則 5 一般利用者のクライアント管理機能へのアクセス時の識別・認証ルール

ルールセット４：

1. リクエスト発信者は、管理者として TOE に登録されている。　かつ
2. リクエスト発信者は、『規則 7 管理者の識別・認証ルール』に従って TOE に正しく認証された。

規則 6 管理者用管理機能へのアクセスルール

管理者が管理機能にアクセスするときの認証のルール：

1. 当該利用者のアカウントはロックされていない。　　かつ
2. リクエストは、当該利用者にアクセスが許されている日時に行われている。　　かつ
3. 本人のチケットを有している。

規則 7 管理者の識別・認証ルール

『規則 2 一般利用者の公開 URL へのアクセス時の識別・認証ルール』、『規則 5 一般利用者のクライアント管理機能へのアクセス時の識別・認証ルール』、『規則 7 管理者の識別・認証ルール』の『許可利用者に許可する日時の指定』は、管理者が TOE に設定する規則である。

2.3.2.TOE の動作の設定

管理者は、TOE の動作を決定するための各種設定を行う。この際、管理者は各種設定をセキュリティ強化モードの設定にする。TOE の動作を規定する各種設定情報は、

1. SecureTicket ライセンスファイル
2. 基本設定ファイル
3. ユーザ・グループ情報ファイル
4. パスワード精査設定ファイル

に格納され、SecureTicket Core サーバに格納される。これらのファイルについては『2.5.1.1TOE の物理的環境』を参照のこと。

SecureTicket ライセンスファイルは、販売元から提供される。

基本設定ファイルとパスワード精査設定ファイルは、管理者が、設定ツールを用いて作成する。

ユーザ・グループ情報ファイルは、管理者が作成するユーザマネージャ GUI を使って編集する。

TOE は電源投入時にこれらの値を読み込んで、動作する。

2.4.TOE の関連者と役割

TOE の関連者と役割を以下に示す。

表 2-2 関連者と役割

番号	役　　割	説　　明
1	利用者	TOE にアクセスする役割。
2	一般利用者	TOE に登録されている利用者。本人認証のためのパスワードとチケットを所有する。
3	未登録利用者	TOE に一般利用者として登録されていない利用者で、公開非保護 URL をアクセスする役割。
4	管理者	TOE の導入サイトで、SecureTicket Core サーバに TOE をインストールし、GUI ツールを作成し、保護サーバ、保護すべき URL および利用者の登録などを行い、TOE の管理を担当する役割。本人認証のためのチケットを所有する。 SecureTicket Core サーバの管理も同時に行う。
5	責任者	TOE の導入サイトで、管理者を選任する役割。

6	許可利用者	TOE に登録されており、あるデータにアクセスすることが許される一般利用者または管理者を、そのデータに対する許可利用者と呼ぶ。
7	攻撃者 不許可利用者	TOE に一般利用者として登録されていないのに、保護サーバの実体保護 URL にアクセスを試みる役割。 または、 TOE に一般利用者として登録されてはいるが、アクセス権限を持たない保護サーバの実体保護 URL にアクセスを試みる役割。 または、 TOE に一般利用者として登録されてはいるが、権限を越えた管理機能の使用を試みる役割。 または、 一般利用者や管理者が TOE にアクセスを行っているときの通信内容を傍受・改竄したり、TOE の持つサーバモジュールインタフェースを利用して基本設定ファイル、パスワード精査設定ファイル、ユーザ・グループファイルを漏洩・改竄したりする役割。

2.5. TOE の構成

本 TOE の構成を『図 2-3 SecureTicket Core 構成図』に示す。

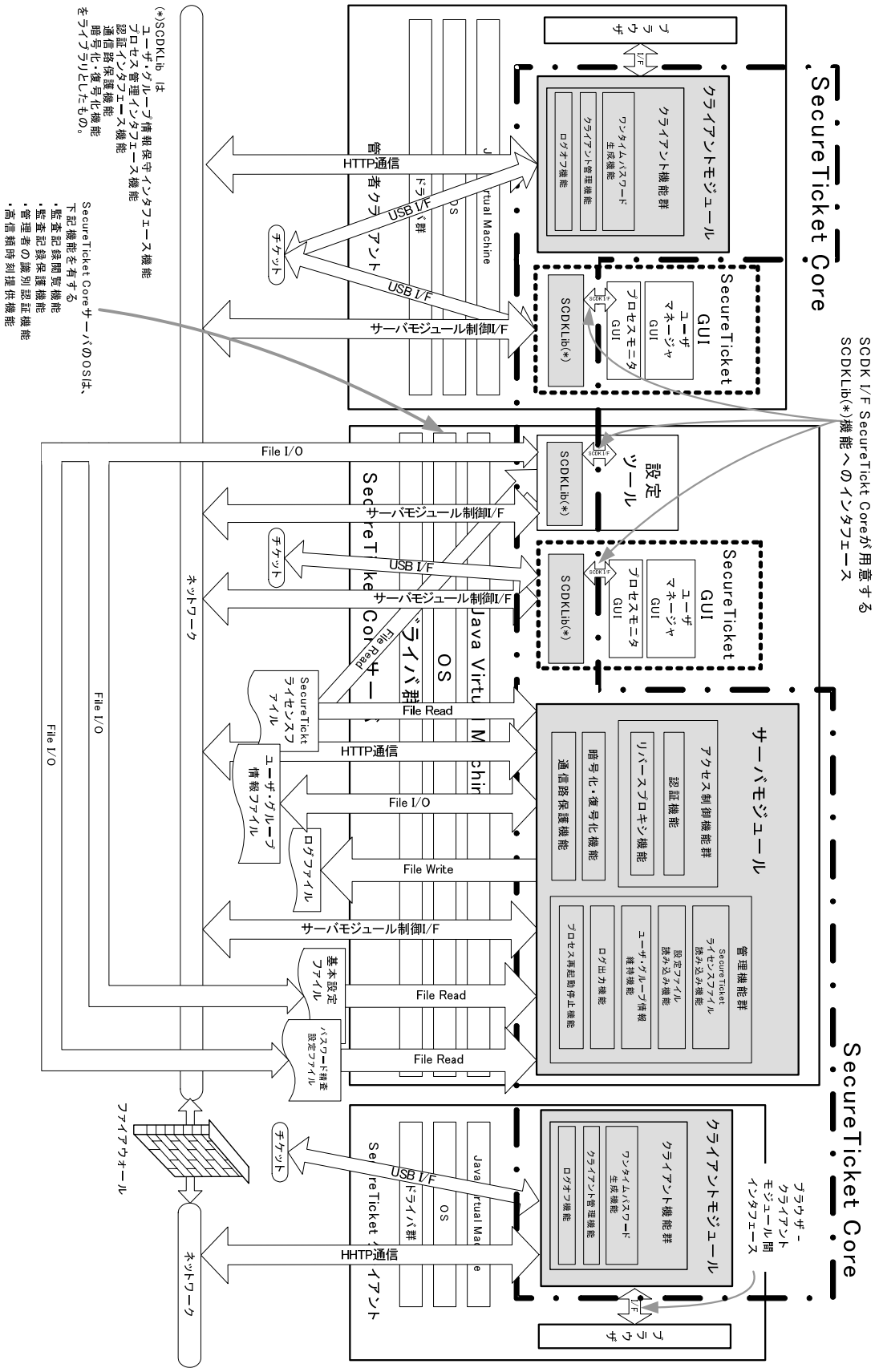
SecureTicket Core
SCDK I/F SecureTickt Coreが用意する
SCDKLib(*)機能へのインタフェース
(*)SCDKLib は
ユーザ・グループ情報保守インタフェース機能
プロセス管理インタフェース機能
認証インタフェース機能
通信路保護機能
暗号化・復号化機能
をライブラリとしたもの。
SecureTicket Coreサーバの OSは、
下記機能を有する
・監査記録閲覧機能
・監査記録保護機能
・管理者の識別認証機能
・高信頼時刻提供機能
ブラウザ
クライアントモジュール
ワンタイムパスワード生成機能
クライアント管理機能
ログオフ機能
クライアント機能群
SecureTicket GUI
ユーザマネージャ GUI
プロセスモニタ GUI
SCDKLib(*)
管理者クライアント
HTTP通信
USB I/F
チケット
サーバモジュール制御I/F
File I/O
設定ツール
ネットワーク
ドライバ群
OS
Java Virtual Machine
File Read
File Write
サーバモジュール
アクセス制御機能群
認証機能
リバースプロキシ機能
暗号化・復号化機能
通信路保護機能
管理機能群
SecureTicket ライセンスファイル読み込み機能
設定ファイル読み込み機能
ユーザ・グループ情報維持機能
ログ出力機能
プロセス再起動停止機能
SecureTickt ライセンスファイル
ユーザ・グループ情報ファイル
ログファイル
基本設定ファイル
パスワード禁止設定ファイル
ファイアウォール
HHTP通信
ブラウザ - クライアントモジュール間インタフェース

図 2-3 SecureTicket Core 構成図

サーバモジュールは、負荷を分散するため、複数の SecureTicket Core サーバにインストールして実行することができる。

2.5.1.TOE の物理的範囲

TOE は、サーバモジュール、クライアントモジュールおよび SCDKLib の３つで構成される。すなわち、これらが TOE の物理的範囲であり、それは『図 2-3 SecureTicket Core 構成図』で色づけされている部分と一致する。

サーバモジュールは、SecureTicket Core サーバで動作し、TOE の主要なセキュリティ機能であるアクセス制御機能群および管理機能群を実現する。クライアントモジュールはクライアント上で動作し、クライアント機能群を実現する。SCDKLib は、SecureTicket GUI および設定ツールにライブラリとして組み込まれ、アクセス制御機能および管理機能群へのインタフェースを提供する。

2.5.1.1. TOE の物理的環境

クライアントモジュールは、クライアント上で動作するブラウザからサーバモジュールにアクセスすることでその内部に取り込まれる。

サーバモジュールは SecureTicket Core サーバ上で実行される。SecureTicket Core サーバには、JVM が含まれる。SecureTicket Core サーバ上の OS は、ハードウェア及びネットワークドライバを制御する。

『図 2-3 SecureTicket Core 構成図』で、SecureTicket ライセンスファイルは、TOE のライセンス情報を格納しているファイルであり、基本設定ファイルは、保護サーバの実体 URL とそれに関連づけられる公開 URL、その種別（公開保護 URL か公開非保護 URL）、公開 URL へのアクセス権限としてのグループ名が記述されている。ユーザ・グループ情報ファイルは、TOE に登録されたユーザ ID、パスワード、アクセス権限を示すグループ ID とユーザ ID との関係を示す。

2.5.2.TOE の制御範囲

TOE の制御範囲は『図 2-3 SecureTicket Core 構成図』で色づけされている部分に以下の制御範囲リストの要素群を加えた範囲である。

制御範囲リスト

1. SecureTicket ライセンスファイル
2. 基本設定ファイル
3. ユーザ・グループ情報ファイル

4. パスワード精査設定ファイル
5. チケット

2.5.3.TOE のインタフェース

TOE は、以下のインタフェースを持つ。

1. File I/O I/F
   TOE とユーザ・グループ情報ファイル、パスワード精査設定ファイル、および基本設定ファイルとのインタフェースである。このインタフェースは、管理者がユーザマネージャ GUI を使ってユーザ・グループ情報を読み書きするとき、または設定ツールを使ってパスワード精査設定ファイルおよび基本設定ファイルを編集するときに使用される。
2. File Read I/F
   SecureTicket ライセンスファイルの内容、パスワード精査設定ファイルの内容、基本設定ファイルの内容を TOE に読み込ませるときに使用される。
3. File Write I/F
   TOE が運用中に生成するログの内容を書き込むときに使用される。管理者が SecureTicket Core サーバの OS を使ってログ情報を読む。
4. HTTP 通信 I/F
   一般利用者が SecureTicket クライアントから TOE 経由で保護サーバにアクセスするときに使われるインタフェース。
5. クライアントモジュールとブラウザの I/F
   一般利用者が SecureTicket クライアントでブラウザを使ってクライアントモジュールにリクエストを出したり、リクエストの結果を表示させたりするときに使われるインタフェース。
6. サーバモジュール制御 I/F
   管理者が SecureTicket Core サーバもしくは内部ネットワーク上の管理者クライアントから、SecureTicket GUI を用いてサーバモジュールを制御する。複数のサーバモジュール間で通信を行う。
   TCP/IP プロトコルを利用した独自通信プロトコル（ソケット通信）が使われる。
7. USB I/F
   一般利用者が所有するチケットを SecureTicket クライアントがクライアントモジュールで読み書きする。管理者が所有するチケットを管理者クライアントが SecureTicket GUI で読み書きする。
8. SCDK I/F
   SecureTicket GUI や設定ツールが、サーバモジュールと通信を行うために、設定ツールが基本設定ファイルやパスワード精査設定ファイルにアクセスする

ために、開発者向けに用意されたプログラミングインタフェース。

2.5.4.TOE の運用

管理者は、運用にあたって、TOE の SCDKLib を使う SecureTicket GUI を作成し、SecureTicket Core サーバもしくは管理者クライアントにインストールしていなければならない。

1． 準備

① 管理者の準備作業

『2.3.2 TOE の動作の設定』で述べたように、管理者は、TOE をインストールした SecureTicket Core サーバに対して、以下の作業を行う。この作業は SecureTicket Core サーバ、管理者クライアントから行う。SecureTicket Core サーバでしか行えない作業は、設定ツールでの作業である。

✓ TOE を運用するための準備作業

1. 管理者は、SecureTicket Core サーバにログインする。
2. 管理者は、設定ツールを使って、
   ① 基本設定ファイルに公開保護 URL、実体保護 URL およびアクセス許可・拒否するグループなどを登録して保護対象資産にアクセスを許す対象を決定する。
   ② パスワード精査設定ファイルにパスワードに使用させない単語を登録する。
3. 管理者はサーバモジュールを再起動し、登録した基本設定ファイルおよびパスワード精査設定ファイル内容を TOE に読み込ませる。

✓ 一般利用者を登録する作業

1. 管理者はユーザマネージャ GUI を使用して、ユーザ・グループ情報を登録する。ここで、管理者は TOE を使用することができる一般利用者と、一般利用者がアクセスできる公開保護 URL、アクセスできない公開保護 URL を決定して、グループを割り付ける。これにより、一般利用者には保護対象資産へのアクセス権が設定される。
2. 管理者は、一般利用者が TOE を利用できるように、次のいずれかの作業を行う。
   (ア) ePass ドライバをインストールしてから、ユーザマネージャ GUI を使って発行した一般利用者のチケットデータを、ePass に格納して一般利用者に渡す。一般利用者には、パスワードを教える。
   (イ) 一般利用者に ePass ドライバをインストールさせる。一般利用者にユーザ名とパスワードを教え、当該一般利用者のアカウントをチケット発行可能状態とした上で、一般利用者にブラウザでチケットを発行するページを表

示させて、チケットデータを生成させ、それを ePass に格納させる。

② 一般利用者の準備作業

一般利用者は、ePass ドライバを SecureTicket クライアントにインストールしてから、下記のいずれかの方法で、チケットを受け取り、パスワードを教えてもらい、チケットを使用できるようにする。

- ✓ 管理者から、本人に発行されたチケットを受け取り、パスワードを教えてもらう。
- ✓ 自分でチケットを発行する。すなわち、
  - ① 一般利用者は、管理者にチケット発行可能状態としてもらう。
  - ② 一般利用者は、管理者から空の ePass をもらう。
  - ③ 一般利用者は、そのチケット（ePass）を、SecureTicket クライアントの USB ポート に装着する。
  - ④ 一般利用者は、ブラウザを使って、チケット発行機能のあるページを表示し、自分のユーザ名とパスワードを打ち込んで、TOE に認証させて、チケットデータを生成させ、チケットに格納させる。

2. 運用

一般利用者、および未登録利用者は、公開 URL にアクセスする。

① 一般利用者は、チケットを SecureTicket クライアントに装着し、アクセスしたい実体 URL に対応する公開 URL をブラウザで指定する。

② 当該公開 URL が公開保護 URL の場合は、

- ✓ 最初にアクセスする場合、TOE が一般利用者にパスワードを入力するように促すページを表示するので、一般利用者はパスワードを打鍵することで認証が行われ、ブラウザに入力した公開保護 URL に対応した実体保護 URL にアクセスできる。
- ✓ 以降は、一般利用者は直ちに、ブラウザに入力した公開保護 URL に対応する実体 URL にアクセスできる。

③ 当該公開 URL が公開非保護 URL である場合は、未認証で対応する実体 URL にアクセスできる。

3. 保守

① 管理者の保守作業

- ✓ 管理者は、運用中、一般利用者の追加、変更、削除の必要が生じたときは、ユーザマネージャ GUI を使って、対応する。
- ✓ 公開 URL の追加、変更、削除や禁止ワードの変更が必要となったとき、
  1. 設定ツールを使って基本設定ファイルやパスワード精査設定ファイルを保守する。
  2. プロセスモニタ GUI を使って、サーバモジュールの再起動を行って SecureTicket Core サーバに反映する。

② 一般利用者の保守作業

- ✓ 一般利用者は、ブラウザを使用して、自分自身のパスワードを変更するページを表示し、パスワードを変更できる。
- ✓ 一般利用者が、万一チケットを破損するようなことがあった場合は、管理者に連絡した上で、上記の『1．②一般利用者の準備作業』と同じ手順に従って、本人のチケットを再発行することができる。

2.5.5.TOE の動作環境

TOE は、次の環境で動作する。

1． サーバマシン

(ア) JVM JRE 5.0 Update 7 以降

(イ) OS 下記のいずれか

① Windows 2003 Server SP1 以降

② Red Hat Enterprise Linux ES v.4 以降

(ウ) ハードウェア

① CPU： Pentium 500MHz 以上 又は Celeron 500MHz 以上

② メモリ ５１２MB 以上

③ HDD １０GB 以上

④ CD-ROM ドライブ

2． 一般利用者クライアント

(ア) JVM Sun Java Plug-in 5.0 Update 7 以降 または Microsoft VM 5.0 Release 5.0.0.3810 以降

(イ) OS 下記のいずれか

① Windows 2000 SP2 以降

② Windows XP

(ウ) ハードウェア

① USB ポートがあるもの

(エ) ブラウザ 下記のいずれか

① IE 5.5 以降

② Firefox 1.5.0.7 以降（このブラウザを使用する場合、JVM は Sun Java Plug-in 5.0 Update 7 以降 を使用する）

3． 管理者クライアント

(ア) JVM Sun Java Plug-in 5.0 Update 7 以降

(イ) OS 下記のいずれか

① Windows 2000
② Windows XP

(ウ) ハードウェア
① USB ポートがあるもの

4. チケット
(ア) USB トークン ePass として、下記を使用する。
① ePass1000

2.6.SecureTicket Core の機能構成

TOE は以下に記述する機能のうち、『2.6.1 ライブラリ機能群』『2.6.2 管理機能群』『2.6.3 アクセス制御機能群』『2.6.4 クライアント機能群』の機能を有する。すなわち、TOE の論理的範囲は、『2.6.1 ライブラリ機能群』『2.6.2 管理機能群』『2.6.3 アクセス制御機能群』『2.6.4 クライアント機能群』の集合であり、TOE の範囲外となるものは『2.7 その他』に記載される機能群である。上記の４つの機能はすべて TOE のセキュリティ機能であり、TOE の論理的範囲と一致する。

2.6.1.ライブラリ機能群（SCDKLib）

これらは、以下に示す５つの機能である。管理者は SecureTicketGUI を作成するとき、SCDKLib を使用する。

2.6.1.1. ユーザ・グループ情報保守インタフェース機能

これは、ユーザ・グループ情報を保守するためのインタフェース機能である。

2.6.1.2. プロセス管理インタフェース機能

これは、サーバモジュールのプロセスを管理するためのインタフェース機能である。

2.6.1.3. 認証インタフェース機能

この機能は、チケットデータやパスワードを使って、認証を行うためのインタフェース機能である。

2.6.1.4. 通信路保護機能

この機能は、サーバモジュールおよび管理者クライアントが行う通信を保護するとき使われる。

2.6.1.5. 暗号化・復号化機能

この機能は、SecureTicket ライセンスファイル、基本設定ファイル、パスワード精査設定ファイル、ユーザ・グループ情報ファイルにアクセスするとき、ファイル内容の暗号化・復号化を行うとき使われる。暗号鍵の生成はサーバモジュールの起動時に行われ、暗号鍵の保持は揮発性メモリで行われ、暗号鍵の破棄は、SecureTicket Core サーバの停止時に揮発性メモリが消去されることで物理的に破棄される。

2.6.2.管理機能群

これらは、以下に示す５つの機能である。これらは、必要に応じ、SCDKLib と同一の暗号化・復号化機能、通信路保護機能を利用する。

2.6.2.1. SecureTicket ライセンスファイル読み込み機能

この機能は、サーバモジュールが(再)起動するとき、TOE の使用許諾情報を書き込んだ SecureTicket ライセンスファイルを読み込んで、ライセンスの妥当性の判定を行う。

2.6.2.2. 基本設定ファイル読み込み機能

この機能は、サーバモジュールが(再)起動するとき、または、プロセスモニタ GUI から出されたサーバモジュール再起動リクエストによって、基本設定ファイルを読み込む。

2.6.2.3. ユーザ・グループ情報維持機能

この機能は、TOE が(再)起動するとき、ユーザ・グループ情報ファイルを読み込む。
また、ユーザマネージャ GUI を使って管理者はユーザ・グループ情報を更新し、ユーザ・グループ情報ファイルに反映する。TOE が利用者のアクセス権限を把握するため、ユーザとグループの関連づけ、チケットデータの更新、チケット発行可能状態管理などユーザ固有情報の管理を行う。
これは、後述の『2.7.2.2 ユーザマネージャ GUI』からのリクエストを受け付けるインタフェースを持つ。

2.6.2.4. ログ出力機能

この機能は、TOE が監査証跡をファイル（ログファイル）に出力する。管理者がログファイルを閲覧する場合は、SecureTicket Core サーバの OS のツールを利用する。

2.6.2.5. プロセス再起動停止機能

この機能は、サーバモジュールの プロセスを再起動・停止する。

2.6.3.アクセス制御機能群

2.6.3.1. リバースプロキシ機能

一般利用者が SecureTicket クライアントから公開 URL にアクセスを行ったとき、リンク設定情報に基づき一般利用者のアクセス権限を吟味して代理応答する。
このとき、アクセス先が公開保護 URL の場合、一般利用者の認証を『**2.6.3.2 認証機能**』で行う。
　このリバースプロキシ機能では、一般利用者が SecureTicket クライアントから TOE 経由で保護サーバにアクセスを行うとき、SecureTicket クライアント⇔TOE 間の通信路および TOE ⇔保護サーバ間の通信路を SSL によって保護する。ただし、TOE⇔保護サーバ間の通信を盗聴される恐れが無い場合は、TOE⇔保護サーバ間通信路の保護を省略することもできる。
　また、このリバースプロキシ機能では、一般利用者がクライアントモジュールの『2.6.4 クライアント機能群』にアクセスを行うとき、SecureTicket クライアント⇔TOE 間の通信路を SSL によって保護する。

2.6.3.2. 認証機能

認証機能は、一般利用者または管理者が TOE にアクセスを行ったとき、許可利用者およびアク

セス先に応じて『規則 2 一般利用者の公開 URL へのアクセス時の識別・認証ルール』、『規則 5 一般利用者のクライアント管理機能へのアクセス時の識別・認証ルール』、『規則 7 管理者の識別・認証ルール』のいずれかを満たすことを確認する。

2.6.4.クライアント機能群

2.6.4.1. ワンタイムパスワード生成機能

一般利用者がSecureTicketクライアントから公開保護URLや『2.6.4.2クライアント管理機能』のパスワード変更を行うURLにアクセスすると、サーバモジュールからクライアントモジュールがダウンロードされる。クライアントモジュールはチケットデータと一般利用者のパスワードからワンタイムパスワードを生成して、サーバモジュールに送信する。送信後、サーバモジュールの認証機能により一般利用者が識別され、認証されると、クライアントモジュールはチケットデータを更新し、公開URLの取得要求を送信する。

2.6.4.2. クライアント管理機能

一般利用者が SecureTicket クライアントからチケット発行するための URL にアクセスすると、サーバモジュールからクライアントモジュールがダウンロードされる。クライアントモジュールは一般利用者が入力したユーザ名とパスワードをサーバモジュールに送信する。送信後、サーバモジュールの応答に従って、一般利用者のチケットデータを作成し、チケットに格納する。チケットを発行する機能は、管理者が一般利用者を登録し、一般利用者自身にチケットを発行する許可を管理ツールにて行うことで、初めて一般利用者が使えるようになる。一度チケットが発行されると、この機能は管理者がチケット発行可能状態とするまで使用不能となる。

一般利用者が SecureTicket クライアントからパスワード変更するための URL にアクセスすると、『2.6.4.1 ワンタイムパスワード生成機能』にて作成したワンタイムパスワードをサーバモジュールに送信する。送信後、サーバモジュールの応答に従って、一般利用者が入力した新パスワードをサーバモジュールに送信して一般利用者のパスワードを変更する。

2.6.4.3. ログオフ機能

一般利用者が SecureTicket クライアントからログアウト URL にアクセスすると、サーバモジュールからクライアントモジュールがダウンロードされる。クライアントモジュールは一般利用者のチケットを読み込み、ログアウト要求をサーバモジュールに送信する。なお、本機能は非セキュリティ機能である。

2.7.その他

TOE へのインタフェースを持つ機能として、以下がある。

2.7.1.設定ツール

管理者が基本設定ファイルおよびパスワード精査設定ファイルを編集するために使うツールである。リンク設定情報の登録、削除、変更などを行う。

2.7.2.SecureTicketGUI

TOE の範囲外である SecureTicketGUI は以下の機能を有する。これは管理者が SCDKLib を用いて作成する機能で、SecureTicket Core サーバもしくは管理者クライアントで動作する。

2.7.2.1. 管理者クライアント通信路保護機能

『2.7.2.2 ユーザマネージャ GUI』および『2.7.2.3 プロセスモニタ GUI』が SCDKLib を用いて通信を保護する機能である。

2.7.2.2. ユーザマネージャ GUI

この機能は、『2.6.2.3 ユーザ・グループ情報維持機能』で定義されるユーザ・グループ情報の管理機能を操作するための管理者向け GUI インタフェースツールである。一般利用者のユーザ名、パスワードの登録・削除、チケットの発行・無効化、一般利用者のチケット発行許可、グループ登録・削除などを行う。

2.7.2.3. プロセスモニタ GUI

この機能は、『2.6.2.5 プロセス再起動停止機能』で定義されるサーバモジュールのプロセス起動・停止機能を操作するための GUI インタフェースツールである。設定ツールで基本設定ファイルやパスワード精査設定ファイルを編集した後、その内容を TOE に反映するために、管理者が使用する。

2.7.3.ログファイルビューア

SecureTicket Core サーバの OS のテキストエディタが、TOE のログファイルビューアとして使用される。

2.8.保護対象となる資産

TOE の保護対象となる資産は実体保護 URL 上の情報、およびユーザ・グループ情報ファイル、基本設定ファイル、パスワード精査設定ファイルであり、ＴＯＥはそれらデータへのアクセスを制御する。

3. TOE セキュリティ環境

本章では、TOEの前提条件、脅威、組織のセキュリティ方針、攻撃者の攻撃能力について述べる。

3.1. 前提条件

A.TOENetPos　TOE のネットワーク設置条件
　SecureTicket Core サーバは、DMZ または内部ネットワークで動作する。

A.NetCfg　　TOE のネットワーク構成条件
　保護サーバがクライアントと通信を行う際は、必ず SecureTicket Core サーバを中継して通信を行う。

A.Admin　　信頼できる管理者
　管理者は、不正な行為を行わない。

A.STSvrAcct　SecureTicket Core サーバのアカウント管理
　SecureTicket Core サーバの OS は、識別認証機能を持つ。SecureTicket Core サーバにアカウント登録されているのは管理者だけであり、管理者のみが SecureTicket Core サーバにログインし、管理を行う。

A.TcktPwUsr　一般利用者認証同時紛失
　一般利用者のチケットとパスワードが同時に攻撃者の手に渡ってしまうことはない。

3.2. 脅威

T.IllAccess　　実体保護 URL への不許可アクセス
　外部ネットワークや内部ネットワーク上のクライアントから攻撃者が、ブラウザを使って、実体保護 URL にアクセスする、または、実体保護 URL の許可利用者になりすまして実体保護 URL にアクセスする恐れがある。

T.EvsDropX　　外部ネットワークでの盗聴
　SecureTicket クライアントと TOE 間を流れる通信内容（一般利用者が読み取っている実体保護 URL の内容や許可利用者が変更・発行している認証情報）を、攻撃者が外部ネットワークで盗聴ツールを用いて漏洩させる恐れがある。

T.EvsDropI　内部ネットワークでの盗聴

クライアント（SecureTicket クライアントもしくは管理者クライアント）と TOE 間を流れる通信内容（一般利用者が読み取っている実体保護 URL の内容や一般利用者が変更・発行している認証情報、管理者が管理している管理情報）を、攻撃者が内部ネットワークで盗聴ツールを用いて漏洩させる恐れがある。

T.EvsDropS　内部ネットワークや DMZ でのサーバ間通信の盗聴

SecureTicket Core サーバと保護サーバ間を流れる通信内容（一般利用者が読み取っている実体保護 URL の内容）を、攻撃者が内部ネットワークや DMZ から盗聴ツールを用いて漏洩させる恐れがある。

T.MsqrdAdm　管理者へのなりすまし

攻撃者が、管理者になりすまして、内部ネットワークからユーザマネージャ GUI を悪用することによって、ユーザ・グループ情報を改竄したり、一般利用者のチケットを不正に発行したりして、保護サーバの実体保護 URL にアクセスする恐れがある。

T.StolenUsrAthDt　一般利用者認証データを使ってのなりすまし

攻撃者からの不正アクセスを防ぐために実体保護 URL の許可利用者を識別･認証するように対策をしたとき、その二次脅威として、攻撃者が許可利用者の認証データをクライアントからの盗聴などの手段で不正に傍受し、その認証データの所有者である一般利用者になりすまして実体保護 URL にアクセスする恐れがある。

T.StolenUsrTckt　管理不備の一般利用者チケットを使ってのなりすまし

攻撃者からの認証データの不正傍受を防ぐために実体保護 URL の許可利用者に対して毎回異なる認証データで識別・認証するようにしたとき、その二次脅威として、攻撃者が毎回異なる認証データを生成する元データを格納したチケットを窃盗などの手段で不正に取得して、そのチケットの所有者になりすまして、保護サーバの実体保護 URL にアクセスする恐れがある。

3.3.組織のセキュリティ方針

P.UsrCrtTckt　一般利用者のチケット発行

一般利用者の利便性のために、管理者に許可された一般利用者自身によって本人のチケットを発行できるようにする。その際には、管理者がチケット発行可能状態とした上でユーザ名とパスワードによる識別・認証を行うこととする。

P.HDDTsfProtect　TOE のハードディスク内容の保護

TOE のユーザ・グループ情報ファイル、基本設定ファイル、パスワード精査設定ファイルの内容は暗号化して格納することとする。

3.4.攻撃者の攻撃能力

攻撃者は攻撃能力として高度な専門知識を持たないものとする。

4. セキュリティ対策方針

4.1. TOE のセキュリティ対策方針

O.IAUsr　一般利用者の識別認証機能
TOE は、実体保護 URL にアクセスを試みる一般利用者に対して、識別・認証を行う。

O.OTAthDtUsr　一般利用者のワンタイムパスワード
TOE は、実体保護 URL にアクセスを試みる一般利用者に対して、毎回異なる認証データで識別・認証を行う。

O.DblAthDtUsr　一般利用者の二要素認証
TOE は、実体保護 URL にアクセスを試みる一般利用者に対して、複数のデータをもとにした認証データで識別・認証を行う。

O.IAUsrCrTckt　一般利用者のチケット発行時識別認証機能
TOE は、自身のチケット発行を試みる一般利用者に対して、ユーザ名とパスワードによる識別・認証を行う。

O.IAAdm　管理者の識別認証機能
TOE は、TOE の保守を行う管理者に対して、識別・認証を行う。

O.Manage　管理機能
TOE は、一般利用者が本人のチケットを発行できる状態とする機能を管理者のみに提供する。

O.UMaint　一般利用者向け保守機能
TOE は一般利用者自身のチケットを発行する機能を一般利用者本人のみに提供する。

O.RvsProxy　保護サーバアクセス制御
TOE は、実体保護 URL にアクセスを試みる要求のうち、アクセス許可を持っている要求を保護サーバに渡し、許可を持っていない要求を棄却する。

O.ComProtect クライアント-TOE 間通信経路の保護
TOE は、SecureTicket Core サーバと通信を行うクライアントとの通信内容を保護する。

O.SComProtect　　TOE-保護サーバ間通信経路の保護
TOE は、SecureTicket Core サーバと通信を行う保護サーバとの通信内容を保護する。

O.TsfProtect　基本設定ファイル、ユーザ･グループ情報ファイル、パスワード精査設定ファイルの保護
TOE は、基本設定ファイル、ユーザ･グループ情報ファイル、パスワード精査設定ファイルの内容を暗号化する。

O.Audit　　監査情報の記録
TOE は、セキュリティ関連事象を監査証跡として記録し、管理する。

4.2. 環境のセキュリティ対策方針

OE.STSvrAcct　　SecureTicket Core サーバの管理者アカウント
SecureTicket Core サーバの OS は、TOE の管理者を識別・認証する機能を提供する。管理者は、当該 OS に対するアカウントとして管理者のみ登録し、管理者だけが SecureTicket Core サーバにログインできるようにして TOE の運用管理を行う。

OE.TOENetPos　　TOE のネットワーク設置
管理者は、SecureTicket Core サーバを、DMZ もしくは内部ネットワークに接続する。

OE.NetCfg　　TOE のネットワーク構成条件
管理者は、保護サーバが SecureTicket Core サーバとのみ通信を行うようネットワーク設定を行う。すなわち、管理者は、すべてのクライアントが必ず SecureTicket Core サーバを中継して保護サーバと通信を行い、保護サーバは SecureTicket Core サーバとのみ通信を行うようネットワーク設定を行う。

OE.Admin　　管理者の条件
責任者は、不正を行わない人物を管理者として選任する。

OE.TcktPwDstr　　管理者の安全なチケット/パスワードの配布
管理者は、一般利用者に、一般利用者のチケットおよびパスワードを安全に配布する。

OE.IAStolen　　一般利用者の認証データの管理
管理者は、一般利用者の認証情報の入ったチケットとパスワードが決して同時に他人の手に渡らないよう一般利用者を教育・指導する。

OE.Audit IT 環境の監査支援

SecureTIcket Core サーバの OS は、高信頼タイムスタンプを提供し、また監査証跡を保護し、読み出す機能を提供する。

5. IT セキュリティ要件

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

5.1.1.1. クラス FAU： セキュリティ監査

FAU_GEN.1 監査データの生成

下位階層：なし

FAU_GEN.1.1

TSFは、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了;

b) 監査の[選択: 最小、基本、詳細、指定なし: から一つのみ選択]レベルのすべての監査対象事象; 及び

[選択：最小、基本、詳細、指定なし: から一つのみ選択]

- *指定なし*

c) [割付: 上記以外の個別に定義した監査対象事象]。

[割付：上記以外の個別に定義した監査対象事象]

- 監査の対象を『表 5-1監査対象となる事象一覧』に記す。

表 5-1 監査対象となる事象一覧

セキュリティ機能要件	CC の Part2 が規定する最小レベルの監査対象事象	実際の監査対象事象
FAU_GEN.1	無し。	無し。
FAU_STG.4	無し。	無し。
FCS_CKM.1	動作の成功と失敗	AES:暗号鍵生成の失敗。
FCS_COP.1	成功と失敗及び暗号操作の種別	AES: 『リスト 5-1 AES で暗号化・復号化されるデーター覧』の暗号化、復号化時の失敗。 SHA-256: 『リスト 5-2 SHA-256 で生成されるデーター覧』で規定されるハッシュ値生成

		の失敗。
FDP_ACC.1	無し。	無し。
FDP_ACF.1	SFP で扱われるオブジェクトに対する操作の実行における成功した要求。	公開保護 URL に対してアクセスが成功した要求
FIA_AFL.1	不成功認証が閾値に達したこと。アカウントがロックされたこと。アカウントが管理者により正常に復帰されたこと。	不成功認証が閾値に達したこと。アカウントがロックされたこと。
FIA_ATD.1	監査対象にすべき識別されたアクションはない。	無し。
FIA_SOS.1	TSF による、テストされた秘密の拒否	検査されたパスワードが『リスト 5-4 パスワードの品質尺度』を満たさなかったこと。
FIA_SOS.2	TSF による、テストされた秘密の拒否	無し
FIA_UAU.2	認証メカニズムの不成功になった使用	パスワードメカニズムによる認証の不成功 ワンタイムパスワードメカニズムによる認証の不成功
FIA_UAU.4	認証データを再使用する試み。	無し
FIA_UAU.5	認証の最終決定	最終的に不成功になった認証
FIA_UAU.6	再認証の失敗	無し
FIA_UAU.7	無し。	無し
FIA_UID.2	提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用	一般利用者、管理者の認証の不成功時の識別情報
FIA_USB.1	利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。	無し
FMT_MOF.1	TSF の機能のふるまいにおけるす	無し

	べての改変	
FMT_MSA.1	セキュリティ属性の値の改変すべて	無し
FMT_MSA.2	セキュリティ属性に対して提示され、拒否された値すべて	無し
FMT_MSA.3	許可的あるいは制限的規則のデフォルト設定の改変	無し
FMT_MTD.1[1]	TSF データの値のすべての改変	ユーザ・グループ情報の登録、改変、削除
FMT_MTD.1[2]	TSF データの値のすべての改変	一般利用者のパスワードの改変
FMT_MTD.1[3]	TSF データの値のすべての改変	一般利用者のパスワードの改変
FMT_MTD.1[4]	TSF データの値のすべての改変	管理者によるチケットの発行
FMT_MTD.1[5]	TSF データの値のすべての改変	一般利用者による本人のチケット発行
FMT_MTD.1[6]	TSF データの値のすべての改変	無し
FMT_MTD.1[7]	TSF データの値のすべての改変	無し
FMT_MTD.1[8]	TSF データの値のすべての改変	無し
FMT_MTD.1[9]	TSF データの値のすべての改変	無し
FMT_MTD.1[10]	TSF データの値のすべての改変	無し
FMT_MTD.1[11]	TSF データの値のすべての改変	無し
FMT_SMF.1	管理機能の使用	無し
FMT_SMR.1[1]	役割の一部をなす利用者のグループに対する改変	無し
FMT_SMR.1[2]	役割の一部をなす利用者のグループに対する改変	無し
FPT_RVM.1	無し	無し
FTA_TSE.1[1]	セション確立メカニズムによるセション確立の拒否	無し
FTA_TSE.1[2]	セション確立メカニズムによるセション確立の拒否	無し
FTP_ITC.1	高信頼チャネル機能の失敗	通信エラー
FTP_TRP.1[1]	高信頼パス機能の失敗	通信エラー

FTP_TRP.1[2]	高信頼パス機能の失敗	通信エラー

詳細化：「監査機能の起動と終了」→ 「*サーバモジュールの起動と終了*」

FAU_GEN.1.2

TSFは、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗); 及び

b) 各監査事象種別に対して、PP/STの機能コンポーネントの監査対象事象の定義に基づいた、[割付: その他の監査関連情報]

[割付：その他の監査関連情報]

- *なし*

依存性：FPT_STM.1 高信頼タイムスタンプ

FAU_STG.4 監査データ損失の防止

下位階層： FAU_STG.3

解釈注：解釈-202の結果として以下のエレメントを変更する。

FAU_STG.4.1

TSFは、監査証跡が満杯になった場合、[選択: 監査対象事象の無視、特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き: から一つのみ選択]及び[割付:監査格納失敗時にとられるその他のアクション]を行わねばならない。

[選択: 監査対象事象の無視、特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き: から一つのみ選択]

- ***最も古くに格納された監査記録への上書き***

[割付:監査格納失敗時にとられるその他のアクション]

- ***監査対象事象のSecureTicket Coreサーバ・コンソールへの出力***

依存性: FAU_STG.1 保護された監査証跡格納

5.1.1.2. クラス FCS： 暗号サポート

FCS_CKM.1　暗号鍵生成

下位階層：なし

FCS_CKM.1.1

TSFは、以下の[割付: 標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付: 暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付: 暗号鍵長]に従って、暗号鍵を生成しなければならない。

[割付: 標準のリスト]

- *AES： SecureTicket Core 暗号運用標準*

[割付: 暗号鍵生成アルゴリズム]

- *AES： SecureTicket Core 共通鍵生成アルゴリズム*

[割付: 暗号鍵長]

- *AES： 256bit*

依存性：[FCS_CKM.2 暗号鍵配付
または
FCS_COP.1 暗号操作]
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　暗号操作

下位階層：なし

FCS_COP.1.1

TSFは、[割付: 標準のリスト]に合致する、特定された暗号アルゴリズム[割付: 暗号アルゴリズム]と暗号鍵長[割付: 暗号鍵長]に従って、[割付: 暗号操作のリスト]を実行しなければならない。

[割付: 標準のリスト]

- *AES： FIPS PUB 197*
- *SHA-256： FIPS PUB 180-2*

[割付: 暗号アルゴリズム]

- *AES*
- *SHA-256*

[割付: 暗号鍵長]

- *AES： 256bits*
- *SHA-256： N/A*

[割付: 暗号操作のリスト]

- *AES:『リスト 5-1 AES で暗号化・復号化されるデータ一覧』で示されるデータのNIST SP 800-38Aで定義されるOFBモードでの暗号化および暗号化された同リストデータのNIST SP 800-38Aで定義されるOFBモードでの復号。*

リスト 5-1 AES で暗号化・復号化されるデータ一覧

1	*サーバモジュール制御 I/F で送受信する内容全て*
2	*『表 5-5リバースプロキシSFPのオブジェクトのセキュリティ属性』に記述されるセキュリティ属性*
3	*『リスト 5-6 TSFデータリスト その1』*
4	*『リスト 5-7 TSFデータリストその2』*
5	*『リスト 5-9 TSFデータリスト その4』*
6	*『リスト 5-11 TSFデータリスト その6』*
7	*『リスト 5-12 TSFデータリスト その7』*

8	*『リスト 5-13 TSFデータリストその8』*
9	*『リスト 5-14 TSFデータリストその9』*
10	*『リスト 5-15 TSFデータリストその１０』*
11	*『リスト 5-16 TSFデータリストその１１』*

- ***SHA-256：『リスト 5-2 SHA-256で生成されるデーター覧』で示されるデータの生成***

リスト 5-2 SHA-256 で生成されるデーター覧

1	*ワンタイムパスワード*
2	*セッションID*

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
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

5.1.1.3. クラス FDP： 利用者データ保護

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: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御SFP]を実施しなければならない。

[割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]

- *サブジェクト：リバースプロキシ受付プロセス :一般利用者の公開保護 URL へのアクセスの依頼を受け付けるプロセス*
- *オブジェクト：公開保護 URL*
- *操作：*
  公開保護 URL への一般利用者のアクセス

[割付: アクセス制御SFP]

- *リバースプロキシSFP*

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: 示されたSFP下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御SFP]を実施しなければならない。

[割付: 示されたSFP下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ]

- *サブジェクト： リバースプロキシ受付プロセス*
- *オブジェクト： 公開保護URL*
- *SFP関連セキュリティ属性（サブジェクト）： グループID*
- *SFP関連セキュリティ属性（オブジェクト）： グループID、グループ有効開始日時、グループ有効期限、グループの許可・拒否属性（「許可」、「拒否」がある。）*
- *SFP関連セキュリティ属性の名前付けされたグループ： 無し*

[割付: アクセス制御SFP]

- *リバースプロキシSFP*

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: 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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

[割付: 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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

- *ユーザIDによって識別される一般利用者を代行する「リバースプロキシ受付プロセス」（サブジェクト）と「公開保護URL」（オブジェクト）の間で、それらの持つセキュリティ属性同士で「表 5-2 リバースプロキシSFPアクセス規則」のよう*

な関係があるとき、アクセスは、○のとき許可され、×のとき拒否される。

- *オブジェクトのセキュリティ属性であるグループIDに、「グループ有効開始日時」、「グループ有効期限」があるときは、現在有効なグループIDのみをリバースプロキシSFPのセキュリティ属性とする。*
- *（ここでは、便宜上、選別されたオブジェクトのセキュリティ属性であるグループIDを、OGIDOK、OGIDNOなどとし、選別されたサブジェクトのセキュリティ属性であるグループIDとして、SGIDとして説明する。）*

表 5-2 リバースプロキシ SFP アクセス規則

オブジェクト	*サブジェクト*			*アクセスの可否*
公開保護 URL	*リバースプロキシ受付プロセス*			
セキュリティ属性	*セキュリティ属性*			
（グループ ID、許可･拒否属性）	*グループ ID*	*属性の関係*	*説明*	
（OGIDOK、許可）	*SGID*	*SGID= OGIDOK*	*OGIDOK に一致するグループ ID(SGID)を一つでもサブジェクトが持つ*	*○*
	SGID	*SGID≠ OGIDOK*	*OGIDOK に一致するグループ ID(SGID)を一つもサブジェクトが持たない*	*×*
	無し		*グループ ID が無い*	*×*
（OGIDNO、拒否）	*SGID*	*SGID= OGIDNO*	*OGIDNO に一致するグループ ID(SGID)を一つでもサブジェクトが持つ*	*×*
	SGID	*SGID≠ OGIDNO*	*OGIDNO に一致するグループ ID(SGID)を一つもサブジェクトが持たない*	*○*
	無し		*グループ ID が無い*	*○*
（無し、無し）	*SGID*		*オブジェクトにグループ ID が無い*	*○*
	無し			*○*

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: セキュリティ属性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する規則]。

[割付: セキュリティ属性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する規則]

- *無し*

FDP_ACF.1.4

TSFは、[割付: セキュリティ属性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拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付: セキュリティ属性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拒否する規則]

- *無し*

依存性：FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

5.1.1.4. クラス FIA： 識別と認証

FIA_AFL.1 認証失敗時の取り扱い

下位階層：なし

FIA_AFL.1.1

TSFは、[割付: 認証事象のリスト]に関して、[選択: [割付:正の整数値], 「[割付: 許容可能な値の範囲］内における管理者設定可能な正の整数値]」]回の不成功認証試行が生じたときを検出しなければならない。

[割付：認証事象のリスト]

- *パスワードとチケットデータによる認証*
- *チケットデータのみによる認証*
- *ユーザ名とパスワードによる認証*

[選択: [割付:正の整数値], 「[割付: 許容可能な値の範囲］内における管理者設定可能な正の整数値]」]

- *「[割付: 許容可能な値の範囲］内における管理者設定可能な正の整数値]」*

[割付: 許容可能な値の範囲]

- *１～１００（「連続失敗認証検出回数」）*

FIA_AFL.1.2

不成功の認証試行が定義した回数に達するか上回ったとき、TSFは、[割付: アクションのリスト]をしなければならない。

[割付：アクションのリスト]

- *認証不成功となった一般利用者、管理者に対して、アカウントをロックする。（ロックの解除は管理者が FMT_MTD.1[9］を用いて 一般利用者のセキュリティ属性「Ticket認証エラーステータス」をリセットすることで行う。）*

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:セキュリティ属性のリスト]を維持しなければならない。

[割付:セキュリティ属性のリスト]

リスト 5-3 利用者のセキュリティ属性

ユーザID
グループID（）*

（）複数のグループをセキュリティ属性として持つ場合もある。*

依存性：なし

FIA_SOS.1　秘密の検証

下位階層：なし

FIA_SOS.1.1

TSF は、秘密が[割付: 定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[割付：定義された品質尺度]

- *パスワードの品質尺度を以下のように定義する。*

リスト 5-4 パスワードの品質尺度

パスワード長	*8バイト～128バイト*
構成文字種	*英数字、"0" ~ "9"、"A" ~ "Z"、"a" ~" z"* *特殊文字、"@"、"_"、"~"、"#"、"("、")"、"."*
許容条件	*一世代前と同一のパスワードを禁止する* *管理者が登録した使用禁止ワードと一致しない*

詳細化：「秘密」→ 「*パスワード*」

依存性：なし

FIA_SOS.2　　TSF 秘密生成

下位階層：なし

FIA_SOS.2.1

TSF は、[割付: 定義された品質尺度]に合致する秘密を生成するメカニズムを提供しなければならない。

[割付：定義された品質尺度]

- *ワンタイムパスワードの品質尺度を以下のように定義する。*

リスト 5-5 ワンタイムパスワードの品質尺度

ワンタイムパスワード長	*６４バイト*
構成文字種	*十六進数字、“0”～“9”、“A”～“F”(大文字のみ)*

FIA_SOS.2.2

TSF は、[割付: TSF 機能のリスト]に対し、TSF 生成の秘密の使用を実施できなければならない。

[割付：TSF 機能のリスト]

- *一般利用者、管理者の識別・認証*

詳細化：「秘密」→ 「*ワンタイムパスワード*」

依存性：なし

FIA_UAU.2　　アクション前の利用者認証

下位階層：FIA_UAU.1

FIA_UAU.2.1

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。

詳細化：「認証」→「*ユーザ名とパスワードによる認証 または*
チケットデータのみによる認証 または
パスワードとチケットデータによる認証」

依存性：FIA_UID.1 識別のタイミング

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: 識別された認証メカニズム]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。

[割付: 識別された認証メカニズム]

- *ワンタイムパスワードメカニズム*

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: 複数の認証メカニズムのリスト]を提供しなければならない。

[割付: 複数の認証メカニズムのリスト]

- *パスワードメカニズム*
- *ワンタイムパスワードメカニズム*

FIA_UAU.5.2

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

[割付: 複数の認証メカニズムがどのように認証を提供するかを記述する規則]

下記の「表 5-3複数の認証メカニズムが認証を提供する規則」に従い、認証される主体と、主体がアクセスを試みるものの組合せに従って、適用される認証メカニズムが決定される。

表 5-3 複数の認証メカニズムが認証を提供する規則

認証される主体	*主体がアクセスを試みるもの*	*認証メカニズム*
		初回認証および再認証
一般利用者	*公開保護 URL*	*ワンタイムパスワードメカニズム*
	クライアント管理機能（パスワード変更機能）	*ワンタイムパスワードメカニズム*
	クライアント管理機能（一般利用者本人のチケット発行機能）	*パスワードメカニズム*
管理者	*管理機能*	*ワンタイムパスワードメカニズム*

依存性：なし

FIA_UAU.6 再認証

下位階層：なし

FIA_UAU.6.1

TSFは、条件[割付: 再認証が要求される条件のリスト]のもとで利用者を再認証しなければならない。

[割付: 再認証が要求される条件のリスト]

- *セッション有効期限後に一般利用者が行う公開保護URLへのアクセス*
- *セッション有効期限後に一般利用者が試みる一般利用者本人のパスワードの改変*
- *セッション有効期限後に管理者が行う管理者機能へのアクセス*

依存性：なし

FIA_UAU.7　保護された認証フィードバック

下位階層：なし

FIA_UAU.7.1

TSFは、認証を行っている間、[割付: フィードバックのリスト]だけを利用者に提供しなければならない。

[割付: フィードバックのリスト]

- *パスワード桁数分の“*”*

詳細化　：「認証」→ *ユーザ名とパスワードによる認証 または パスワードとチケットデータによる認証*

依存性：FIA_UAU.1 認証のタイミング

FIA_UID.2　　アクション前の利用者識別

下位階層：FIA_UID.1

FIA_UID.2.1

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、各利用者に自分自身を識別することを要求しなければならない。

詳細化　：「利用者」→***一般利用者、管理者***

依存性：なし

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、適切な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。

詳細化：「適切な利用者セキュリティ属性」
『リスト 5-3 利用者のセキュリティ属性』で定義したセキュリティ属性

依存性：FIA_ATD.1 利用者属性定義

5.1.1.5. クラス FMT： セキュリティ管理

FMT_MOF.1　セキュリティ機能のふるまいの管理

下位階層：なし

FMT_MOF.1.1

TSFは、機能[割付：機能のリスト][選択：のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]能力を[割付：許可された識別された役割]に制限しなければならない。

表 5-4 TSF のふるまい決定についての役割

[割付: 機能のリスト]
TOE － 保護サーバ間 通信保護機能
一般利用者、管理者の識別と認証機能
監査情報の記録機能

[選択: のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]

- *のふるまいを決定する、のふるまいを改変する*

[割付: 許可された識別された役割]

- *管理者*

詳細化　：「TOE － 保護サーバ間通信 保護機能のふるまいを決定する」→
「TOE－保護サーバ間 通信を　SSL通信路とするか、平文通信路とするかの決定をする」
詳細化　：「認証機能のふるまいを改変する」→
「一般利用者の認証機能として、チケットのみの認証とする」
「パスワードの品質尺度として１～１２８バイトを認める」
詳細化　：「監査情報の記録機能のふるまいを改変する」→
「監査情報の出力レベルを改変する」

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_MSA.1　　セキュリティ属性の管理

下位階層：なし

FMT_MSA.1.1

TSFは、セキュリティ属性[割付: セキュリティ属性のリスト]に対し[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]をする能力を[割付: 許可された識別された役割]に制限するために[割付: アクセス制御SFP、情報フロー制御SFP]を実施しなければならない。

表 5-5 リバースプロキシ SFP のオブジェクトのセキュリティ属性

[割付: セキュリティ属性のリスト]
公開保護 URL に対するグループ名
公開保護 URL に対する許可・拒否属性
グループ有効開始日時
グループ有効期限

[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]

- *問い合わせ、削除、[割付: その他の操作]*

[割付: その他の操作]

- *登録*

[割付: 許可された識別された役割]

- *管理者*

[割付: アクセス制御SFP、情報フロー制御SFP]

- *リバースプロキシSFP*

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_MSA.2　セキュアなセキュリティ属性

下位階層：なし

FMT_MSA.2.1

TSFは、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。

依存性： ADV_SPM.1 非形式的TOEセキュリティ方針モデル
[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.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティ役割

FMT_MSA.3　静的属性初期化

下位階層：なし

FMT_MSA.3.1

TSFは、そのSFPを実施するために使われるセキュリティ属性として、[選択: 制限的、許可的 : から一つのみ選択、[割付 : その他の特性]]デフォルト値を与える[割付: アクセス制御SFP、情報フロー制御SFP]を実施しなければならない。

[選択: 制限的、許可的 : から一つのみ選択、[割付 : その他の特性]]

- *許可的*

[割付: アクセス制御SFP、情報フロー制御SFP]

- *リバースプロキシSFP*

FMT_MSA.3.2

TSFは、オブジェクトや情報が生成されるとき、[割付: 許可された識別された役割]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

[割付: 許可された識別された役割]

- *管理者*

依存性：FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティ役割

FMT_MTD.1[1] TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付: TSFデータのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]

リスト 5-6 TSF データリスト その1

*ユーザ情報レコード(*注 1)*
*グループ情報レコード(*注 2)*

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- *[割付: その他の操作]*

[割付: その他の操作]

- *レコード全体の登録、削除*
- *ユーザ情報の問い合わせ*
- *グループ情報の問い合わせ*

[割付:許可された識別された役割]

- *管理者*

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

(***注 1**) ユーザ情報レコードは、許可利用者の「ユーザ名」、「ユーザ ID」、「Ticket 認証エラーステータス」、「所属グループ ID」 などのユーザ情報よりなる。
(***注 2**) グループ情報レコードは、「グループ名」、「グループ ID」、「グループ有効開始日時」、「グループ有効期限」などのグループ情報よりなる。

FMT_MTD.1[2] TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付: TSFデータのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]

リスト 5-7 TSF データリストその2

一般利用者のパスワード

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- ***改変、[割付: その他の操作]***

[割付: その他の操作]

- ***登録***

[割付:許可された識別された役割]

- ***管理者***

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_MTD.1[3] TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付: TSFデータのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]

リスト 5-8 TSF データリストその3

一般利用者本人のパスワード

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- ***改変***

[割付:許可された識別された役割]

- ***一般利用者本人***

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[4] TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付: TSFデータのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]

リスト 5-9 TSF データリスト その4

チケットデータ

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- *[割付: その他の操作]*

[割付: その他の操作]

- *生成してチケットを発行する*

[割付:許可された識別された役割]

- *管理者*

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_MTD.1[5] TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付: TSFデータのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]

リスト 5-10 TSF データリスト その5

一般利用者本人のチケットデータ

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- *[割付: その他の操作]*

[割付: その他の操作]

- *生成して、本人のチケット発行許可フラグが「発行可能」であるときに限り、本人のチケットを発行し、直ちにチケット発行許可フラグを「発行禁止」(一般利用者自身が本人のチケットを発行することを禁止する状態）とする。*

[割付:許可された識別された役割]

- *一般利用者本人*

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[6] TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付: TSFデータのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]

リスト 5-11 TSF データリスト その6

使用禁止ワード

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- ***問い合わせ、改変、削除、[割付: その他の操作]***

[割付: その他の操作]

- ***登録***

[割付:許可された識別された役割]

- ***管理者***

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_MTD.1[7] TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付: TSFデータのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]

リスト 5-12 TSF データリスト その7

チケット発行許可フラグ

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- *[割付: その他の操作]*

[割付: その他の操作]

- *「発行可能」(一般利用者本人に本人のチケットを発行することを許可する状態)にする。*
- *「発行禁止」(一般利用者本人に本人のチケットを発行することを禁止する状態)にする。*

[割付:許可された識別された役割]

- *管理者*

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_MTD.1[8] TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付: TSFデータのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]

リスト 5-13 TSF データリストその8

パスワードの有効期限
Ticket 認証許可時間帯
Ticket 認証有効開始日時
Ticket 認証有効期限

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- ***問い合わせ、改変、削除、[割付: その他の操作]***

[割付: その他の操作]

- ***登録***

[割付:許可された識別された役割]

- ***管理者***

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_MTD.1[9] TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付: TSFデータのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]

リスト 5-14 TSF データリストその9

Ticket 認証エラーステータス

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- *問い合わせ、[割付: その他の操作]*

[割付: その他の操作]

- *リセット*

[割付:許可された識別された役割]

- *管理者*

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_MTD.1[10] TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付: TSFデータのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]

リスト 5-15 TSF データリストその１０

連続失敗認証検出回数

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- *問い合わせ、改変、[割付: その他の操作]*

[割付: その他の操作]

- *登録*

[割付:許可された識別された役割]

- *管理者*

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_MTD.1[11] TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付: TSFデータのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]

リスト 5-16 TSF データリストその１１

認証の有効時間

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

- *問い合わせ、改変*

[割付:許可された識別された役割]

- *管理者*

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う能力を持たねばならない：[割付：TSF によって提供されるセキュリティ管理機能のリスト]

[割付：TSF によって提供されるセキュリティ管理機能のリスト]

- 次の『表 5-6 管理要件項目一覧』に示す。

表 5-6 管理要件項目一覧

セキュリティ機能要件	管理要件	管理項目
FAU_GEN.1	なし	監査情報の出力レベル
FAU_STG.4	監査格納失敗時にとられるアクションの維持(削除、改変、追加)。	監査格納失敗時に取られる下記の二つのアクションの管理。 ● 最も古くに格納された監査記録への上書き ● 監査対象事象のSecureTicket Coreサーバ・コンソールへの出力
FCS_CKM.1	暗号鍵属性の変更の管理	暗号鍵の属性は固定であり、変更されないため、管理項目は無い
FCS_COP.1	なし	
FDP_ACC.1	なし	
FDP_ACF.1	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	明示的にアクセス許可または拒否に基づく決定に使われる属性は存在しないので、管理項目はない。
FIA_AFL.1	不成功の認証試行に対する閾値の管理	連続失敗認証検出回数
	認証失敗の事象においてとられるアクションの管理	アクションは決まっており、変更されないため、管理項目は無い。
FIA_ATD.1	許可管理者が利用者に対して追加定義するセキュリティ属性	セキュリティ属性は決まっており、変更されないため、管理項目はない。

FIA_SOS.1	秘密の検証に使用される尺度の管理	秘密の検証に使用される尺度。「8～128文字」か「１～１２８文字」か。使用禁止ワード。
FIA_SOS.2	秘密の生成に使用される尺度の管理	秘密の生成に使用される尺度は、固定であり、変更されないため、管理項目は無い。
FIA_UAU.2	管理者による認証データの管理	一般利用者のパスワード、チケットデータ、一般利用者に対する認証方式（「パスワードとチケットデータによる認証」か「チケットデータのみによる認証」）の管理
	このデータに関係する利用者による認証データの管理	一般利用者のパスワード、チケットデータ
FIA_UAU.4	なし	
FIA_UAU.5	認証メカニズムの管理	認証メカニズムは、パスワードメカニズムとワンタイムパスワードの２種類であり固定であるため管理項目はない。
	認証に対する規則の管理	保護対象資産と役割で、認証のメカニズムが決まり、その規則は変更されないため、管理項目はない。
FIA_UAU.6	許可管理者が再認証を要求できる場合、再認証要求の管理。	認証の有効時間
FIA_UAU.7	なし	
FIA_UID.2	利用者識別情報の管理	ユーザ名
FIA_USB.1	許可管理者の定義する、デフォルトのサブジェクトのセキュリティ属性。	デフォルトのセキュリティ属性は固定であるため、管理項目は無い。
FMT_MOF.1	TSF の機能と相互に影響を及ぼし得る役割グループの管理	TSF の機能に影響を及ぼし得る役割グループは管理者のみに固定されているため、管理項目は無い
FMT_MSA.1	セキュリティ属性と相互に影響を及ぼし得る役割グループの管理	役割は管理者のみに固定されているため、管理項目は無い
FMT_MSA.2	なし	

FMT_MSA.3	初期値を特定できる役割グループの管理	役割は管理者のみに固定されているため、管理項目は無い
FMT_MTD.1[1]	TSF データと相互に影響を及ぼし得る役割グループの管理	役割は管理者のみに固定されているため、管理項目は無い
FMT_MTD.1[2]	TSF データと相互に影響を及ぼし得る役割グループの管理	役割は管理者のみに固定されているため、管理項目は無い
FMT_MTD.1[3]	TSF データと相互に影響を及ぼし得る役割グループの管理	役割はパスワードを有する一般利用者のみに固定されているため、管理項目は無い
FMT_MTD.1[4]	TSF データと相互に影響を及ぼし得る役割グループの管理	役割は管理者のみに固定されているため、管理項目は無い
FMT_MTD.1[5]	TSF データと相互に影響を及ぼし得る役割グループの管理	役割はパスワードを有する一般利用者のみに固定されているため、管理項目は無い
FMT_MTD.1[6]	TSF データと相互に影響を及ぼし得る役割グループの管理	役割は管理者のみに固定されているため、管理項目は無い
FMT_MTD.1[7]	TSF データと相互に影響を及ぼし得る役割グループの管理	役割は管理者のみに固定されているため、管理項目は無い
FMT_MTD.1[8]	TSF データと相互に影響を及ぼし得る役割グループの管理	役割は管理者のみに固定されているため、管理項目は無い
FMT_MTD.1[9]	TSF データと相互に影響を及ぼし得る役割グループの管理	役割は管理者のみに固定されているため、管理項目は無い
FMT_MTD.1[10]	TSF データと相互に影響を及ぼし得る役割グループの管理	役割は管理者のみに固定されているため、管理項目は無い
FMT_MTD.1[11]	TSF データと相互に影響を及ぼし得る役割グループの管理	役割は管理者のみに固定されているため、管理項目は無い
FMT_SMF.1	なし	
FMT_SMR.1[1]	役割の一部をなす利用者グループの管理	管理者の役割は固定されているため、管理項目は無い
FMT_SMR.1[2]	役割の一部をなす利用者グループの管理	一般利用者の役割は固定されているため、管理項目は無い
FPT_RVM.1	なし	
FTA_TSE.1[1]	許可管理者によるセション確立条件の管理	一般利用者のパスワードの有効期限

FTA_TSE.1[2]	許可管理者によるセション確立条件の管理	Ticket 認証許可時間帯 Ticket 認証有効開始日時 Ticket 認証有効期限
FTP_ITC.1	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。	TOE－保護サーバ間の通信をSSL通信とするか平文通信とするかの管理。
FTP_TRP.1[1]	もしサポートされていれば、高信頼パスを要求するアクションの設定	無し。（サポートされていないため、管理項目は無い）
FTP_TRP.1[2]	もしサポートされていれば、高信頼パスを要求するアクションの設定	無し。（サポートされていないため、管理項目は無い）

依存性：なし

FMT_SMR.1[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: 許可された識別された役割]を維持しなければならない。

[割付: 許可された識別された役割]

- ***管理者***

FMT_SMR.1.2

TSFは、利用者を役割に関連づけなければならない。

依存性：FIA_UID.1 識別のタイミング

FMT_SMR.1[2] セキュリティ役割

下位階層：なし

FMT_SMR.1.1

TSFは、役割[割付: 許可された識別された役割]を維持しなければならない。

[割付: 許可された識別された役割]

- ***一般利用者***

FMT_SMR.1.2

TSFは、利用者を役割に関連づけなければならない。

依存性：FIA_UID.1 識別のタイミング

5.1.1.6. クラス FPT： TSF の保護

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

5.1.1.7. クラスFTA： TOEセション確立

FTA_TSE.1[1] TOEセション確立

下位階層：なし

FTA_TSE.1.1

TSFは、[割付: 属性]に基づきセション確立を拒否できなければならない。

[割付: 属性]

- *一般利用者のパスワードの有効期限*

依存性：なし

FTA_TSE.1[2] TOEセション確立

下位階層：なし

FTA_TSE.1.1

TSFは、[割付: 属性]に基づきセション確立を拒否できなければならない。

[割付: 属性]

- *許可利用者のTicket認証許可時間帯*
- *許可利用者のTicket認証有効開始日時*
- *許可利用者のTicket認証有効期限*

依存性：なし

5.1.1.8. クラスFTP： 高信頼パス/チャネル

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。

詳細化：「高信頼IT製品」→「*保護サーバ*」

FTP_ITC.1.2

TSFは、[選択: TSF、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。

[選択: TSF、リモート高信頼IT製品]

- *TSF*

FTP_ITC.1.3

TSFは、[割付: 高信頼チャネルが要求される機能のリスト]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。

[割付: 高信頼チャネルが要求される機能のリスト]

- *TOE－保護サーバ間 通信保護機能*

依存性：なし

FTP_TRP.1[1] 高信頼パス

下位階層：なし

FTP_TRP.1.1

TSFは、それ自身と[選択: リモート、ローカル]利用者間に、他の通信パス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通信データの保護を提供する通信パスを提供しなければならない。

[選択: リモート、ローカル]

- *リモート*

FTP_TRP.1.2

TSFは、[選択: TSF、ローカル利用者、リモート利用者]が、高信頼パスを介して通信を開始することを許可しなければならない。

[選択: TSF、ローカル利用者、リモート利用者]

- *リモート利用者*
  詳細化 ：「リモート利用者」→*リモート一般利用者*

FTP_TRP.1.3

TSFは、[選択: 最初の利用者認証、[割付: 高信頼パスが要求される他のサービス]]に対して、高信頼パスの使用を要求しなければならない。

[選択: 最初の利用者認証、[割付: 高信頼パスが要求される他のサービス]]

- *最初の利用者認証、[割付: 高信頼パスが要求される他のサービス]*
  詳細化 ：「利用者」→*一般利用者*

[割付: 高信頼パスが要求される他のサービス]

- *TOEが要求する一般利用者再認証*
- *TOEが提供するリバースプロキシサービス*
- *TOEが提供するクライアントモジュール経由の管理サービス（一般利用者本人のパスワード変更機能、一般利用者本人のチケット発行機能）*

依存性：なし

FTP_TRP.1[2] 高信頼パス

下位階層：なし

FTP_TRP.1.1

TSFは、それ自身と[選択: リモート、ローカル]利用者間に、他の通信パス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通信データの保護を提供する通信パスを提供しなければならない。

[選択: リモート、ローカル]

- *リモート、ローカル*

FTP_TRP.1.2

TSFは、[選択: TSF、ローカル利用者、リモート利用者]が、高信頼パスを介して通信を開始することを許可しなければならない。

[選択: TSF、ローカル利用者、リモート利用者]

- *TSF、ローカル利用者、リモート利用者*

詳細化 ：「利用者」→*管理者*

FTP_TRP.1.3

FTP_TRP.1.3 TSFは、[選択: 最初の利用者認証、[割付: 高信頼パスが要求される他のサービス]]に対して、高信頼パスの使用を要求しなければならない。

[選択: 最初の利用者認証、[割付: 高信頼パスが要求される他のサービス]]

- *最初の利用者認証、[割付: 高信頼パスが要求される他のサービス]*

詳細化 ：「利用者」→*管理者*

[割付: 高信頼パスが要求される他のサービス]

- *TOEが要求する管理者再認証*
- *TOEがサーバモジュール制御/Fで提供するすべての管理サービス（管理者が行う管理機能）*

依存性：なし

5.1.2.TOE セキュリティ保証要件

本 TOE は、商用の製品において、十分なレベルの品質保証レベルである EAL3+ADV_SPM.1 を主張する。EAL3+ADV_SPM.1 に対応する TOE セキュリティ保証要件を『表 5-7 TOE セキュリティ保証要件一覧』に示す。

表 5-7 TOE セキュリティ保証要件一覧

保証クラス	保証要件
構成管理	ACM_CAP.3 許可の管理
	ACM_SCP.1 TOE の CM 範囲
配付と運用	ADO_DEL.1 配付手続き
	ADO_IGS.1 設置、生成、及び立上げ手順
開発	ADV_FSP.1 非形式的機能仕様
	ADV_HLD.2 セキュリティ実施上位レベル設計
	ADV_RCR.1 非形式的対応の実証
	ADV_SPM.1 非形式的な TOE 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
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
脆弱性評定	AVA_MSU.1 ガイダンスの検査
	AVA_SOF.1 TOE セキュリティ機能強度評価
	AVA_VLA.1 開発者脆弱性分析

5.2.IT 環境に対するセキュリティ要件

5.2.1.IT 環境に対するセキュリティ機能要件

5.2.1.1. クラスFAU： セキュリティ監査

FAU_SAR.1[E] 監査レビュー

下位階層: なし

FAU_SAR.1.1

TSFは、[割付: 許可利用者]が、[割付: 監査情報のリスト]を監査記録から読み出せるようにしなければならない。

[割付: 許可利用者]

- *管理者*

[割付: 監査情報のリスト]

- *FAU_GEN.1 で規定する「表 5-1 監査対象となる事象一覧」に示す監査情報*

詳細化 ：「TSF」→*IT環境としてのOS*

FAU_SAR.1.2

TSFは、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

詳細化 ：「TSF」→*IT環境としてのOS*
「利用者」→*管理者*

依存性: FAU_GEN.1 監査データ生成

FAU_STG.1[E] 保護された監査証跡

下位階層: なし

FAU_STG.1.1

TSFは、格納された監査記録を不正な削除から保護しなければならない。

解釈注：解釈-141及び202の結果として以下のエレメントを変更する。

FAU_STG.1.2

TSFは、監査証跡内の監査記録への不正な改変を[選択: 防止、検出: から一つのみ選択]できねばならない。

[選択: 防止、検出: から一つのみ選択]

- *防止*

詳細化 ：「TSF」→*IT環境としてのOS*

依存性: FAU_GEN.1 監査データ生成

5.2.1.2. クラス FIA： 識別と認証

FIA_UAU.2[E] アクション前の利用者認証

下位階層：FIA_UAU.1

FIA_UAU.2.1

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。

詳細化 ：「TSF」→ *IT環境としてのSecureTicket Coreサーバ'のOS*
詳細化 ：「TSF調停アクション」→ *IT環境としてのSecureTicket Coreサーバ'OSの調停アクション*

依存性：FIA_UID.1 識別のタイミング

FIA_UAU.7[E] 保護された認証フィードバック

下位階層：なし

FIA_UAU.7.1

TSFは、認証を行っている間、[割付: フィードバックのリスト]だけを利用者に提供しなければならない。

[割付: フィードバックのリスト]

- *桁数分のダミー文字*

詳細化 ：「TSF」→ *IT環境としてのSecureTicket Coreサーバ'のOS*

依存性：FIA_UAU.1 認証のタイミング

FIA_UID.2[E]　アクション前の利用者識別

下位階層：FIA_UID.1

FIA_UID.2.1

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、各利用者に自分自身を識別することを要求しなければならない。

詳細化　：「TSF」→*IT環境としてのSecureTicket Coreサーバ*の*OS*
「TSF調停アクション」→ *IT環境としてのSecureTicket Coreサーバ*の*OS調停アクション*
「利用者」→*管理者*

依存性：なし

5.2.1.3. クラス FPT： TSF の保護

FPT_STM.1 [E] 高信頼タイムスタンプ

下位階層：なし

FPT_STM.1.1

TSFは、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

詳細化 ：「TSF」→ *IT環境としてのSecureTicket Coreサーバ*のOS、
「それ自身」→*TSF*

依存性：なし

5.3.TOE 最小機能強度

TOE 機能強度主張が対象とするのは以下のワンタイムパスワードメカニズムとパスワードメカニズムであり、本 ST において対象とする TOE の機能コンポーネントはそれらのメカニズムに対するセキュリティ機能要件 10 個である。

- ワンタイムパスワードメカニズム
  FCS_COP.1、FIA_AFL.1、FIA_SOS.2、FIA_UAU.2、FIA_UAU.4、FIA_UAU.5、FIA_UAU.6、FIA_UID.2
- パスワードメカニズム
  FIA_AFL.1、FIA_SOS.1、FIA_UAU.2、FIA_UAU.4、FIA_UAU.5、FIA_UAU.6、FIA_UAU.7、FIA_UID.2

TOE セキュリティ機能コンポーネント

FCS_COP.1（暗号操作）SHA-256 による乱数生成
FIA_AFL.1（認証失敗時の取り扱い）
FIA_SOS.1（秘密の検証）
FIA_SOS.2（TSF 秘密生成）
FIA_UAU.2（アクション前の利用者認証）
FIA_UAU.4（単一使用認証メカニズム）
FIA_UAU.5（複数の認証メカニズム）
FIA_UAU.6（再認証）
FIA_UAU.7（保護された認証フィードバック）
FIA_UID.2（アクション前の利用者識別）

上記 10 個の TOE 機能要件に対して、SOF一基本を主張する。また、TOE の最小機能強度に対して、SOF一基本を主張する。

6. TOE 要約仕様

6.1. TOE セキュリティ機能

6.1.1. 識別認証機能

識別認証機能は、以下のセキュリティ機能を備える。

⑷ 一般利用者、管理者の識別と認証（F.IA.AUTH）

以下に、セキュリティ機能について述べる。

6.1.1.1. 一般利用者、管理者の識別と認証（F.IA.AUTH）

6.1.1.1.1. セキュリティ機能

【概要】

一般利用者が保護対象資産である公開保護 URL やクライアント管理機能にアクセスする前に、また、管理者が管理者機能にアクセスする前に、TOE に登録されていることを識別し、本人であることを、クライアントモジュール、サーバモジュールを使って認証する。

【詳細】

1. F.IA.AUTH に対する TOE のインタフェースは次の４つである。
   ⑷ 一般利用者が保護対象資産（公開保護 URL またはクライアント管理機能としてのパスワード変更ページ、）にアクセスすると表示される認証ページ。
   ⑹ 一般利用者用の Ticket 発行ページ。
   ⑹ 一般利用者が上記『⑷』で認証済みとなったのち、セッション有効期限が過ぎ、保護対象資産（公開保護 URL やクライアント管理機能であるパスワード変更ページ）に、再び行ったアクセス。
   ⑹ 管理者用の管理機能としてのユーザマネージャ GUI、プロセスモニタ GUI。
2. 一般利用者のクライアントは、認証ページ、パスワード変更ページ、または Ticket 発行ページからクライアントモジュールをクライアントにダウンロードし、次のように異なる認証メカニズムを用いて {FIA_UAU.5} 識別・認証を行う。F.IA.AUTH が動作するときは、F.REVPROXY により、SSL 通信路が確立されている。
   ⑷ 認証ページ
      ① F.IA.AUTH は、一般利用者の認証をパスワードとチケットにより行う。この認証ではワンタイムパスワードメカニズムが適用される。但し、管理者の設定によりチケットのみの認証とすることが可能（「6.1.4.2 管理者機能（F.MNG.ADMIN)」参照）である。
      ② 認証ページは、本人にパスワードを入力させる。パスワードのエコーバックには、文字数分の‘＊’を表示させ、パスワードの漏洩を防ぐ。{FIA_UAU.7}
      ③ クライアントモジュールは、クライアントに装着されているチケットからチケット

データを読み取り、パスワードを加えて２５６ビットのビット幅で、ハッシュ値生成アルゴリズム SHA-256 に従って、バイナリのハッシュ値を生成し{FCS_COP.1}、『リスト 6-1 クライアントモジュールのワンタイムパスワードの仕様』に変換したものをワンタイムパスワードとして{FIA_SOS.2}、サーバモジュールに送信する。

リスト 6-1 クライアントモジュールのワンタイムパスワードの仕様

✓ ASCII 文字（‘0’～‘9’、‘A’～‘F’）で構成される６４文字長の文字列

④ サーバモジュールは、認証を行えるか下記『リスト 6-2 許可利用者の認証を行えるかの検査』のチェックを行う。

リスト 6-2 許可利用者の認証を行えるかの検査

1	当該アカウントの一般利用者は登録されている。
2	当該アカウントはロックされていない。
3	現在時刻が、Ticket 認証許可時間帯に入っている。{FTA_TSE.1[2]}
4	現在時刻は、Ticket 認証有効開始日時以降である。{FTA_TSE.1[2]}
5	現在時刻は、Ticket 認証有効期限より前である。{FTA_TSE.1[2]}

⑤ 上記のチェックが通り、受信したワンタイムパスワードの値と、管理しているデータから生成した『リスト 6-3 サーバモジュールでのワンタイムパスワードの仕様』を満たすワンタイムパスワードの値と一致したとき、本人であると認証する{FIA_UID.2、FIA_UAU.2}。それ以外、すなわち、『リスト 6-2 許可利用者の認証を行えるかの検査』の検査を通らなかった場合は、セッション確立を拒否して認証失敗とし、エラーページを表示して、下記の『５．(b) 認証失敗時の処理』に進む。

リスト 6-3 サーバモジュールでのワンタイムパスワードの仕様

✓ ASCII 文字（‘0’～‘9’、‘A’～‘F’）で構成される６４文字長の文字列 ✓ 検査時に一致しない場合でも、一世代前のワンタイムパスワードと一致する場合には認証成功とする。

⑥ サーバモジュールは、パスワード有効期限が過ぎていないことを確認する。過ぎている場合は、F.MNG.CLNT にてクライアントモジュールにパスワード変更画面を表示させ、一般利用者にパスワード変更を促す。

1. 一般利用者がパスワード変更画面を強制終了するなどしてパスワード変更しない場合は、セッション確立を拒否して未認証状態とし、エラーページを表示し

{FTA_TSE.1[1]}、『５．(b) 認証失敗時の処理』に進む。

2. 変更パスワード入力欄に何も入力しない場合や、「リスト 6-17 パスワードに対する条件」を満足しない場合は、パスワード無効のエラーを表示し、パスワード入力画面を再表示する。（上記、『⑥ サーバモジュールは、…』に戻る。）
3. パスワード変更画面の指示に従ってパスワードを変更した場合、次に進む。

⑦ クライアントモジュールは、パスワード変更後、『４．チケットデータの更新』に進む。

(b) Ticket 発行ページまたはパスワード変更ページ

① F.IA.AUTH は、ユーザ名とパスワードの入力をそれぞれ、次のように行う。このとき、パスワードのエコーバックには、文字数分の‘＊’を表示させ、パスワードの漏洩を防ぐ。{FIA_UAU.7}

1. Ticket 発行ページでは、一般利用者に、ユーザ名とパスワードを入力させる。この認証ではパスワードメカニズムが適用される。
2. パスワード変更ページでは、ユーザにパスワードのみを入力させる。ユーザ名は、クライアントモジュールが一般利用者のチケットから自動的に読み取る。この認証ではワンタイムパスワードメカニズムが適用される。

② クライアントモジュールは、ユーザ名とパスワードをサーバモジュールに送信する。

③ サーバモジュールは、認証を行えるか下記『リスト 6-4 チケットの発行を行えるかの検査』のチェックを行う。

リスト 6-4 チケットの発行を行えるかの検査

1	当該アカウントの一般利用者は登録されている。
2	当該アカウントのチケットは発行可能状態である。
3	現在時刻は、Ticket 認証有効期限より前である。{FTA_TSE.1[2]}

④ 上記全てのチェックが通り、ユーザ名とパスワードが、登録済みの一般利用者のものと一致していれば、本人であると認証する。{FIA_UID.2、FIA_UAU.2}。それ以外は、セッション確立を拒否して、認証失敗として扱い、下記の『５．(b) 認証失敗時の処理』に進む。認証成功した場合、次に進む。

⑤ クライアントモジュールは、『４．チケットデータの更新』に進む。

(c) 一般利用者の再認証

① F.IA.AUTH は、一旦認証済みとなった一般利用者が、セッション有効期限後に、保護対象資産（公開保護 URL やクライアント管理機能であるパスワード変更ページ）から離れて、再びアクセスを行ったとき、次のように再認証を行なう。

② 上記の『(a) ２．(a) 認証ページ』の『①』に進む。

３． 管理者の場合、次のように識別・認証を行う。（セッション有効期限後に管理機能に再ア

クセスする場合も同じように識別・認証を行う。）

① F.IA.AUTH は、SecureTicketGUI の SCDKLib を介して、クライアントに装着されているチケットからチケットデータを読み取り、２５６ビットのビット幅で、ハッシュ値生成アルゴリズム SHA-256 に従ってバイナリのハッシュ値を生成し{FCS_COP.1}、『リスト 6-1 クライアントモジュールのワンタイムパスワードの仕様』に変換したものをワンタイムパスワードとして{FIA_SOS.2}、サーバモジュールに送信する。この認証ではワンタイムパスワードメカニズムが適用される。

② サーバモジュールは、認証を行えるか下記『リスト 6-2 許可利用者の認証を行えるかの検査』のチェックを行う。

③ 上記のチェックが通り、受信したワンタイムパスワードの値と、管理しているデータから生成した『リスト 6-3 サーバモジュールでのワンタイムパスワードの仕様』を満たすワンタイムパスワードの値と一致したとき、本人であると認証する{FIA_UID.2、FIA_UAU.2}。それ以外は、セッション確立を拒否して、認証失敗として扱い、下記の『５．(b) 認証失敗時の処理』に進む。認証成功した場合、『４．チケットデータの更新』に進む。

４． チケットデータの更新

(a) 一般利用者（認証ページまたはパスワード変更ページ）の場合も、管理者の場合も、サーバモジュールは、次回の認証に備えて、現在のチケットデータと異なるチケットデータを生成し、クライアントモジュールに送信する。

(b) クライアントモジュールは、その値をチケットに書き込む。このため、認証ごとに使用されるワンタイムパスワードは一世代前と異なったものとなる{FIA_UAU.4}。このときセッション ID を生成し、維持する。

５． 認証成功の場合と認証失敗の場合で次のように処理が異なる。

(a) 認証成功時の処理

認証に成功した場合は、サーバ側の認証情報を更新し、２５６ビットのビット幅で、ハッシュ値生成アルゴリズム SHA-256 に従ってバイナリのハッシュ値として生成し{FCS_COP.1}、セッション ID を発行して、認証機能の呼び出し元である、次の①～④に渡す。

① 一般利用者の認証ページ

② 一般利用者のパスワード変更ページ

③ 一般利用者の Ticket 発行ページ

④ 管理者用の管理機能としてのユーザマネージャ GUI、プロセスモニタ GUI を構築する SCDKLib

(b) 認証失敗時の処理

認証に失敗した場合、サーバモジュールは認証エラー回数を更新し、連続して失敗した回数が、『連続失敗認証検出回数』以上となった場合は、当該利用者のアカウントをロ

ックし {FIA_AFL.1}、チケットを無効にする。エラーメッセージ（場合によっては、ロックした旨のメッセージ）は、下記の①～④に渡す。

① 一般利用者の認証ページ
② 一般利用者のパスワード変更ページ
③ 一般利用者の Ticket 発行ページ
④ 管理者用の管理機能としてのユーザマネージャ GUI、プロセスモニタ GUI を構築する SCDKLib

ロックされたアカウントの解除（ユーザの Ticket 認証エラーステータスをリセット）、チケットの有効化は、管理者しかできない。

一般利用者が公開保護 URL や管理機能にアクセスする前、また、管理者が管理者用の保守機能にアクセスする前には、TOE は必ず認証ページを表示するため、識別認証が迂回されることはない {FPT_RVM.1}。認証機能の振る舞いを変更する能力は管理者のみに限定されている。

6.1.1.1.2. IT セキュリティ機能要件

以下に、当該セキュリティ機能の満たす TOE セキュリティ機能要件を述べる。

FCS_COP.1、FIA_AFL.1、FIA_SOS.2、FIA_UAU.2、FIA_UAU.4、FIA_UAU.5、FIA_UAU.7、FIA_UID.2、FPT_RVM.1、FTA_TSE.1[1]、FTA_TSE.1[2]

6.1.2.アクセス制御機能

アクセス制御機能は、以下のセキュリティ機能を備える。

(a) リバースプロキシのアクセス制御（F.REVPROXY）
(b) TOE－保護サーバ間 通信保護機能（F.TOESVRPRT）

以下に、そのセキュリティ機能について述べる。

6.1.2.1. リバースプロキシのアクセス制御（F.REVPROXY）

6.1.2.1.1. セキュリティ機能

【概要】

一般利用者および未登録利用者が、公開 URL へアクセスを行ったとき、予め利用者ごとに登録されたアクセスルールに従ったアクセス制御をする。

【詳細】

1. F.REVPROXY に対するインタフェースは、利用者がブラウザで公開 URL にアクセスを行うことである。
2. F.REVPROXY は、SSL プロトコルにてクライアントと SecureTicket Core サーバ間通信路を確立する {FTP_TRP.1[1]}。これにより、後続の識別・認証機能（F.IA.AUTH）は、最初の一般利用者の認証機能、および一般利用者の再認証のために、通信データの保護を行う通信パスを保証する {FTP_TRP.1[1]}。

3. F.REVPROXY は、HTTP リクエストから、アクセスを試みる公開 URL を得る。
4. 当該公開 URL が公開非保護 URL、公開保護 URL の場合で処理が異なる。
   (ア) 当該公開 URL が公開非保護 URL である場合、直ちにアクセスを許す。
   (イ) 当該公開 URL が公開保護 URL である場合、下記の通りアクセス制御する。
      ① 識別・認証機能 F.IA.AUTH を次の条件のとき実行する。
         1. 識別・認証が完了していない場合
         2. 識別・認証後、セッション ID の有効期限が切れている場合 {FIA_UAU.6}
      ② F.REVPROXY は、リンク設定情報から公開保護 URL のグループ ID、許可・拒否属性を求め、ユーザ・グループ情報から当該グループの有効開始日時、有効期限を取り出す。その情報を基に、現時点で公開保護 URL に有効なグループ ID と許可・拒否属性をセキュリティ属性とする。{FDP_ACF.1}
      ③ 次に、F.REVPROXY はセッション ID からリクエストをした一般利用者のユーザ ID を求め、ユーザ ID を基にユーザ・グループ情報からそのユーザ ID とリンクされたグループ ID を求め {FIA_ATD.1、FIA_USB.1}、さらにグループの有効開始日時、有効期限を取り出す。その情報を基に、現時点で一般利用者に有効なグループ ID をセキュリティ属性とする。{FDP_ACF.1}
      ④ F.REVPROXY は、上述のセキュリティ属性をリバースプロキシ SFP に適用して次のいずれかの条件が成り立つとき、一般利用者は公開保護 URL へアクセス権限を持つと判断する。{FDP_ACC.1、FDP_ACF.1}
         1. 公開保護 URL がそのセキュリティ属性として許可属性を持つとき、一般利用者は公開保護 URL のグループ ID と一致するグループ ID をセキュリティ属性として最低ひとつ持つ。
         2. 公開保護 URL がそのセキュリティ属性として拒否属性を持つとき、一般利用者は、公開保護 URL のグループ ID と一致するグループ ID をセキュリティ属性としてひとつも持たない。
         3. 公開保護 URL はそのセキュリティ属性として何も持たない。
      ⑤ アクセス権限の有無に従って、下記を行う。
         1. 一般利用者がアクセス権限を持つ場合には、
            (ア) サーバモジュールと保護サーバ間通信路を F.TOESVRPRT を使って用意する。
            (イ) 保護サーバの代理でクライアントからの http プロトコルのリクエストを受けてその結果をクライアントに応答する。
         2. 一般利用者がアクセス権限を持たない場合には、エラーページを返す {FDP_ACC.1、FDP_ACF.1}。

リバースプロキシ機能は、一般利用者に対して必ず動作しているため、迂回されることはない {FPT_RVM.1}。

6.1.2.1.2. IT セキュリティ機能要件

以下に、当該セキュリティ機能の満たす TOE セキュリティ機能要件を述べる。

FDP_ACC.1 、FDP_ACF.1 、FIA_ATD.1 、FIA_UAU.6 、FIA_USB.1 、FPT_RVM.1 、FTP_TRP.1[1]

6.1.2.2. TOE－保護サーバ間 通信保護機能（F.TOESVRPRT）

6.1.2.2.1. セキュリティ機能

【概要】

TOE と保護サーバ間で行う通信を保護する。

【詳細】

1. F.TOESVRPRT に対するインタフェースは、利用者がブラウザで公開 URL にアクセスするとき、F.REVPROXY を呼び出すことである。
2. F.TOESVRPRT は、管理者によって決定された TOE－保護サーバ間 通信保護機能のふるまい にしたがって、サーバモジュールと保護サーバ間通信を SSL 通信路{FTP_ITC.1}、平文通信路のいずれかを用意する。

TOE－保護サーバ間 通信保護機能は、迂回されることはない {FPT_RVM.1}。

6.1.2.2.2. IT セキュリティ機能要件

以下に、当該セキュリティ機能の満たす TOE セキュリティ機能要件を述べる。

FTP_ITC.1、FPT_RVM.1

6.1.3.監査機能

監査機能は、以下のセキュリティ機能を備える。

⑷ 監査情報の記録（F.AUDIT）

以下に、セキュリティ機能について述べる。

6.1.3.1. 監査情報の記録（F.AUDIT）

6.1.3.1.1. セキュリティ機能

【概要】

一般利用者、管理者のセキュリティ機能に関する事象を記録し、セキュリティ侵害の検出に備える。

【詳細】

1. F.AUDIT に対するインタフェースは、『サーバモジュールを（再）起動する。』『サーバモジュールを停止する。』ことである。
2. F.AUDIT は、管理者の指定に従って、監査事象の出力レベルを改変する。{FMT_MOF.1}
3. F.AUDIT は、サーバモジュールの起動と停止、セキュリティ機能の動作に関する監査事象をその発生日時、ユーザ名とともに生成して記録する {FAU_GEN.1}。

4. F.AUDIT は、監査証跡エリアが満杯になった場合、最も古くに格納された監査記録へ上書きを行い、監査記録の失敗時には SecureTicket Core サーバのコンソールに出力する{FAU_STG.4}。
5. 監査対象となるイベントを以下に示す。(監査対象の出力レベル＝４)

リスト 6-5 F.AUDIT の監査事象一覧

1	サーバモジュールの起動と終了
2	公開保護 URL に対して成功したアクセス要求
3	AES 暗号鍵生成の失敗
4	ユーザ・グループ情報、リンク設定情報、禁止ワード辞書内容、セキュリティ属性、独自通信プロトコルを用いてやりとりされる通信内容の暗号化・復号化の失敗
5	ワンタイムパスワード生成の失敗
6	ハッシュ値（セッション ID）生成の失敗
7	不成功認証が閾値（連続失敗認証検出回数）に達したこと。アカウントがロックされたこと。
8	パスワードの仕様『リスト 6-17 パスワードに対する条件』に合わないパスワードが入力されたこと
9	パスワードメカニズムによる認証の不成功およびワンタイムパスワードメカニズムによる認証の不成功 （一般利用者、管理者の認証の不成功時の識別情報）
10	ユーザ・グループ情報に対する登録、削除。[ユーザ名、グループ名]
11	管理者によるパスワードの改変
12	一般利用者による一般利用者自身のパスワードの改変
13	管理者による一般利用者のチケット発行
14	一般利用者による一般利用者自身のチケット発行
15	通信エラー

この条件のもとで、監査情報の記録機能は、TOE が動作しているとき、動作しているため、迂回されることはない {FPT_RVM.1}。

6.1.3.1.2. IT セキュリティ機能要件

以下に、当該セキュリティ機能の満たす TOE セキュリティ機能要件を述べる。

FAU_GEN.1、FAU_STG.4、FPT_RVM.1

6.1.4.管理機能

管理機能は、以下のセキュリティ機能群を備える。

⑷ TSF データファイル読み込み・書き込み機能（F.MNG.FILEIO）
⑸ 管理者機能（F.MNG.ADMIN）
⑹ クライアント管理機能（F.MNG.CLNT）

これらが、どのように、管理を行うのかの概略を述べる。

管理者は、保護サーバ上の保護対象資産（公開保護 URL）、公開資産（公開非保護 URL）を決定し、それらを、TOE 経由で外部からアクセスできるように、登録する。このとき、アクセス制御できるよう、グループ、許可・拒否属性をつける。この作業を管理者機能の設定ツールで行う。また、パスワードとして好ましくないワードを追加する。

管理者は、SecureTicketGUI のひとつであるユーザマネージャ GUI を使って、一般利用者を登録する。一般利用者の所属するグループも同時に登録しておく。

管理者は、SecureTicketGUI のひとつであるプロセスモニタ GUI を使って、サーバモジュールを停止・再起動する。

サーバモジュールが再起動するときは、TSF データファイル読み込み・書き込み機能が、基本設定ファイル、ユーザ･グループ情報ファイル、パスワード精査設定ファイルの内容を TOE に読み込む。

一般利用者はクライアント管理機能を使って自分のパスワードの変更などを行える。

以下に、各セキュリティ機能について述べる。

6.1.4.1. TSF データファイル読み込み・書き込み機能（F.MNG.FILEIO）

6.1.4.1.1. セキュリティ機能

【概要】

TSF データ、セキュリティ属性を格納するファイル『リスト 6-6 F.MNG.FILEIO の読み込むファイル』の内容を読み込む。『リスト 6-14 F.MNG.FILEIO の書き込むファイル』に対しては内容を更新する。

【詳細】

1. F.MNG.FILEIO に対するインタフェースは、次の４つである。
   ⑴ 管理者が SecureTicket GUI のプロセスモニタ GUI から SCDKLib 経由でサーバモジュールを再起動するとき
   ⑵ 管理者がユーザマネージャ GUI でユーザ・グループ情報を変更するとき
   ⑶ 一般利用者がクライアント管理機能で自分のパスワードを変更するとき
   ⑷ SecureTicket Core サーバが電源投入などによってサーバモジュールが（再）起動するとき
2. F.MNG.FILEIO は、以下の『リスト 6-6 F.MNG.FILEIO の読み込むファイル』に記載されるファイルを読み込む。

リスト 6-6 F.MNG.FILEIO の読み込むファイル

1	(a)SecureTicket ライセンスファイル
2	(b)基本設定ファイル
3	(c)ユーザ・グループ情報ファイル
4	(d)パスワード精査設定ファイル

3. F.MNG.FILEIO は、256 ビット長の AES 暗号鍵を 『SecureTicket Core 暗号運用標準』の『SecureTicket Core 共通鍵生成アルゴリズム』に従って生成する {FCS_CKM.1}。暗号鍵に係るセキュリティ属性（特定の文字列からなるシード）は、セキュリティ方針モデルに記載された品質基準に従ってセキュアな値のみ受け入れる {FMT_MSA.2}。
4. ファイルから読み込んだ内容を FIPS PUB 197 標準に従う AES 暗号アルゴリズムで２５６ bit 鍵長の AES アルゴリズムを用いて NIST SP 800-38A で定義される OFB モードで復号する {FCS_COP.1}。
5. F.MNG.FILEIO が復号した内容は TSF データも含む。

- 各ファイルに格納されているデータは次のとおりである。

(a) SecureTicket ライセンスファイル

「SecureTicket ライセンス情報」がこのファイルに含まれるがこれは TSF データではない。

(b) 基本設定ファイル

リスト 6-7 基本設定ファイルに含まれるデータ

• TOE－保護サーバ間通信 SSL 機能の動作・停止指定
• 連続失敗認証検出回数
• 認証の有効時間
• 実体 URL
• 実体 URL と公開 URL のリンク
• 公開保護 URL に対するグループ名
• 公開保護 URL に対する許可・拒否属性

(c) ユーザ・グループ情報ファイル

リスト 6-8 ユーザ・グループ情報ファイルに含まれるデータ

• ユーザ名
• パスワード
• ユーザ ID

• パスワードの有効期限
• Ticket 認証許可時間帯
• Ticket 認証有効開始日時
• Ticket 認証有効期限
• Ticket 認証エラーステータス
• グループ名
• グループ ID
• グループ開始有効日時
• グループ有効期限
• グループ ID とユーザ ID のリンク

(d) パスワード精査設定ファイル

リスト 6-9 パスワード精査設定ファイルに含まれるデータ

• 使用禁止ワード

- 上記のファイル内容（『リスト 6-7 基本設定ファイルに含まれるデータ』『リスト 6-8 ユーザ・グループ情報ファイルに含まれるデータ』『リスト 6-9 パスワード精査設定ファイルに含まれるデータ』）のうち、『リスト 6-10 TOE 起動時の TSF データ』が TSF データである。

リスト 6-10 TOE 起動時の TSF データ

• TOE－保護サーバ間通信 SSL 機能の動作・停止指定
• 連続失敗認証検出回数
• 認証の有効時間
• 公開 URL
• 公開 URL と実体 URL のリンク
• ユーザ情報
• グループ情報
• 使用禁止ワード

- 上記ファイルのうちセキュリティ属性は次のとおりである。
  (ア) 公開 URL に対してのセキュリティ属性は、『リスト 6-11 公開保護 URL のセキュリティ属性』である。
  (イ) ユーザに対してのセキュリティ属性は、『リスト 6-12 ユーザのセキュリティ属性』で

ある。

(ウ) グループに対してのセキュリティ属性は、『リスト 6-13 グループのセキュリティ属性』である。

リスト 6-11 公開保護 URL のセキュリティ属性

• 公開保護 URL に対するグループ ID
• 公開保護 URL に対する許可・拒否属性

リスト 6-12 ユーザのセキュリティ属性

• ユーザ ID
• パスワードの有効期限
• Ticket 認証許可時間帯
• Ticket 認証有効開始日時
• Ticket 認証有効期限
• Ticket 認証エラーステータス

リスト 6-13 グループのセキュリティ属性

• グループ ID
• グループ有効開始日時
• グループ有効期限
• グループ ID とユーザ ID のリンク

- F.MNG.FILEIO は、ユーザ・グループ情報（『リスト 6-8 ユーザ・グループ情報ファイルに含まれるデータ』）に関しては、F.MNG.ADMIN よりリクエストがかかれば、アップデートされた内容を FIPS PUB 197 標準に従う AES 暗号アルゴリズムで２５６bit 鍵長の AES アルゴリズムを用いて NIST SP 800-38A で定義される OFB モードで暗号化して{FCS_COP.1}、ファイルに書き込む。
- また、F.MNG.FILEIO は、設定ツールから呼ばれる SCDKLib よりリクエストがかかれば、設定ツールが編集した基本設定ファイル内容（『リスト 6-7 基本設定ファイルに含まれるデータ』）やパスワード精査設定ファイル内容（『リスト 6-9 パスワード精査設定ファイルに含まれるデータ』）を FIPS PUB 197 標準に従う AES 暗号アルゴリズムで２５６bit 鍵長の AES アルゴリズムを用いて NIST SP 800-38A で定義される OFB モードで暗号化して

{FCS_COP.1}、それぞれのファイルに書き込む。

リスト 6-14 F.MNG.FILEIO の書き込むファイル

1	(b)基本設定ファイル
2	(c)ユーザ・グループ情報ファイル
3	(d)パスワード精査設定ファイル

F.MNG.FILEIO は、TOE が（再）起動されるとき、必ず動作するため、迂回されることはない{FPT_RVM.1}。ユーザ・グループ情報ファイルへの書き込み機能は、TOE がユーザ・グループ情報を更新するとき、必ず動作するため、迂回されることはない{FPT_RVM.1}。

6.1.4.1.2. IT セキュリティ機能要件

以下に、当該セキュリティ機能の満たす TOE セキュリティ機能要件を述べる。

FCS_CKM.1、FCS_COP.1、FMT_MSA.2、FPT_RVM.1

6.1.4.2. 管理者機能（F.MNG.ADMIN）

6.1.4.2.1. セキュリティ機能

【概要】

管理者にのみユーザ・グループ情報を登録、変更する機能およびプロセス再起動・停止機能を提供する。これは、ユーザマネージャ GUI、プロセスモニタ GUI によって呼ばれる機能である。

【詳細】

1. F.MNG.ADMIN に対するインタフェースは、管理者向けの管理機能を起動することである。実際のインタフェースは、設定ツール、ユーザマネージャ GUI、またはプロセスモニタ GUI より呼ばれる、SCDKLib インタフェースである。
2. F.MNG.ADMIN は、FIPS PUB 197 標準に従う AES 暗号アルゴリズムで２５６bit 鍵長の AES アルゴリズムを用いて NIST SP 800-38A で定義される OFB モードで通信内容にチェックサム値を加えて暗号化・復号化{FCS_COP.1}する独自通信プロトコルにて通信路を確立する{FTP_TRP.1[2]}。この暗号化・復号には、F.MNG.FILEIO で生成した暗号鍵を用いる。
3. F.MNG.ADMIN は、管理者の識別・認証機能 F.IA.AUTH を次の条件のとき実行する。
   (ア) 識別・認証が完了していない場合
   (イ) 識別・認証後、セッション有効期限が切れている場合{FIA_UAU.6}
4. F.MNG.ADMIN は、認証のステータスにより、次のいずれかを行う。
   (ア) 識別・認証が失敗していたら、エラー表示して終了する。
   (イ) 下記の『(a)基本設定ファイル、パスワード精査設定ファイル管理機能』『(b)ユーザ・グ

ループ管理機能』『(c)**プロセス再起動停止機能**』で、管理者から送られるリクエストを受付け、その処理を実行する。

(a) 基本設定ファイル、パスワード精査設定ファイル管理機能（設定ツールより呼ばれる SCDKLib 機能）

基本設定ファイル、パスワード精査設定ファイル管理機能は、リンク設定情報などの管理機能を管理者のみに提供する。この機能は『**リスト 6-15 管理者に提供される管理機能 その1**』で記述される管理機能よりなる。公開保護 URL を作成する場合、そのセキュリティ属性は、許可的となる {FMT_MSA.3}。

リスト 6-15 管理者に提供される管理機能 その1

• TOE ― 保護サーバ間 通信保護機能 のふるまい（これは、「TOE ― 保護サーバ間 通信保護機能」を有効とするか･無効とするか）を決定する。{FMT_MOF.1} • 認証機能のふるまい（これは、一般利用者がパスワードとチケットを併用した認証とするか、チケットのみの認証とするかの指定、パスワードの品質尺度を８～１２８バイトとするか１～１２８バイトとするかの指定）を決定する。{FMT_MOF.1} • 監査情報の出力レベルの改変を１～５の範囲で許可する。ただし、セキュリティ強化モードのときは、監査対象出力レベルとして、４以上を設定する。初期値は“４”。{FMT_MOF.1}
• 公開保護 URL に対するグループ名、許可・拒否属性、登録、削除を行う。{FMT_MSA.1}
• 使用禁止ワードの問い合わせ、変更、削除、登録を行う {FMT_MTD.1[6]}
• 連続失敗認証検出回数の問い合わせ、“１～１０００”の範囲で登録と改変が可能 {FMT_MTD.1[10]}。ただし、セキュリティ強化モードのときは、“１～１００”の範囲で登録・改変を行う。初期値は“3”。
• 認証の有効時間（識別・認証後に発行されるセッション ID の有効秒数）の問い合わせおよび改変。“30～86400” の範囲で改変が可能 {FMT_MTD.1[11]}。ただし、セキュリティ強化モードのときは、“30～3600”の範囲で改変を行う。初期値は“60”。

(ア) 基本設定ファイル、パスワード精査設定ファイル管理機能は、管理者から送られるリクエストを受付け、基本設定ファイルおよびパスワード精査設定ファイルに対して、登録・削除・変更等を行う。管理者が、この作業の後、サーバモジュールを停止・再起動することにより、ファイルの内容が TOE に反映される。

(b) ユーザ・グループ管理機能（ユーザマネージャ GUI より呼ばれる SCDKLib 機能）

ユーザ・グループ管理機能は、許可利用者、グループの登録、管理などの管理機能を管理者のみに提供する。この機能は『**リスト 6-16 管理者に提供される管理機能 その2**』で記述される管理機能よりなる。許可利用者、グループを作成する場合、そのセキュリティ属性は、許可的となる {FMT_MSA.3}。

リスト 6-16 管理者に提供される管理機能 その2

• 一般利用者の一覧を取得する（全てのユーザ名を取得する。）{FMT_MTD.1[1]}
• 一般利用者の問い合わせを行う（当該利用者のユーザ情報を取得する。）{FMT_MTD.1[1]}
• 一般利用者の登録、削除を行う。{FMT_MTD.1[1]}
• 一般利用者のパスワードを登録、変更する {FMT_MTD.1[2]}
• 一般利用者のチケットを発行する {FMT_MTD.1[4]}
• チケット発行許可フラグを「発行可能」（一般利用者本人に本人のチケットを発行することを許可する状態）にする。{FMT_MTD.1[7]}
• チケット発行許可フラグを「発行禁止」（一般利用者本人に本人のチケットを発行することを禁止する状態）にする。{FMT_MTD.1[7]}
• グループの一覧を取得する（全てのグループ名を取得する。）{FMT_MTD.1[1]}
• グループの問い合わせを行う（当該グループ情報を取得する。）{FMT_MTD.1[1]}
• グループに対する、グループ有効開始日時、グループ有効期限 の問い合わせ、登録、削除を行う。{FMT_MSA.1}
• グループに属するユーザの問い合わせ、登録、削除を行う {FMT_MTD.1[1]} ✓ グループに属する許可利用者の問い合わせ、グループへの許可利用者の登録
• 一般利用者のパスワードの有効期限、Ticket 認証時間帯、Ticket 認証有効開始日時、Ticket 認証有効期限の問い合わせ、登録、変更、削除を行う。{FMT_MTD.1[8]}
• 一般利用者のアカウントロック状態の問い合わせ（Ticket 認証エラーステータスの問い合わせ）、アカウントロック解除（Ticket 認証エラーステータスのリセット）を行う。{FMT_MTD.1[9]}

✓ **パスワードに対する検査**

パスワードに対して、TSF は以下の『リスト 6-17 パスワードに対する条件』規則で検証し、規則を満たさないものの登録、規則を満たさないものへの変更は行わない {FIA_SOS.1}。但し、特殊な設定では、パスワードの桁数として、１～１２８文字とすることもできる。この変更は管理者だけに許可されている {FMT_MOF.1}。

リスト 6-17 パスワードに対する条件

• パスワードは半角英数文字（大文字、小文字を含む）、特殊文字「“@”、“_”、“~”、“#”、“(”、“)”、“.”」で構成する８文字～１２８文字長
• パスワードは一世代前のパスワードと同一の値を禁止する
• パスワード精査設定ファイルに登録されている使用禁止ワードとは一致しない

(ア) ユーザ・グループ管理機能 は、許可された識別された役割のみが設定または更新を行える {FMT_MTD.1[8]} ようにする。

(イ) ユーザ・グループ管理機能 は、管理者がユーザ・グループ情報をファイルに反映させる場合、『6.1.4.2.1 セキュリティ機能』の『(b)**ユーザ・グループ管理機能**』で変更した内容を F.MNG.FILEIO にてファイルに反映させる。

(c) プロセス再起動停止機能（プロセスモニタ GUI より呼ばれる SCDKLib 機能）

プロセス再起動停止機能は、サーバモジュールの停止、再起動を行う機能である。これは、管理者が、設定ツールにて編集した『リスト 6-18 設定ツールにて編集するファイル』の内容を TOE に反映するときに使用する。

リスト 6-18 設定ツールにて編集するファイル

1	(b)基本設定ファイル
2	(d)パスワード精査設定ファイル

プロセス再起動停止機能は、停止要求または再起動要求を管理者より受けとり、サーバモジュールを停止、再起動する。このリクエストは、SCDKLib を通して、サーバモジュールに伝達する。

F.MNG.ADMIN で、管理者が基本設定ファイル、パスワード精査設定ファイルに問い合わせ、改変、削除、登録するインタフェース、および管理者がユーザを登録するインタフェースは、SCDKLib のみに限定され、動作するため、迂回されることはない {FPT_RVM.1}。
F.MNG.ADMIN の管理機能は特定されており {FMT_SMF.1}、セキュリティ役割は維持されている {FMT_SMR.1[1]}。

6.1.4.2.2. IT セキュリティ機能要件

以下に、当該セキュリティ機能の満たす TOE セキュリティ機能要件を述べる。

FCS_COP.1、FIA_SOS.1、FIA_UAU.6、FMT_MOF.1、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1[1]、FMT_MTD.1[2]、FMT_MTD.1[4] 、FMT_MTD.1[6]、FMT_MTD.1[7]、FMT_MTD.1[8]、FMT_MTD.1[9]、FMT_MTD.1[10]、FMT_MTD.1[11]、FMT_SMF.1、FMT_SMR.1[1]、FPT_RVM.1、FTP_TRP.1[2]

6.1.4.3. クライアント管理機能（F.MNG.CLNT）

6.1.4.3.1. セキュリティ機能

【概要】

一般利用者に自分自身のパスワードを変更する機能、自分自身のチケットを発行する機能を提供する。

【詳細】

1. F.MNG.CLNT へのインタフェースは、一般利用者に許される管理機能を利用する（パスワード変更ページ、または Ticket 発行ページにアクセスする）ことである。

2. F.MNG.CLNT は、リバースプロキシ機能の SSL 暗号化機能を用いて、TOE が提供するクライアントモジュール経由の管理サービスに通信データの保護を行う通信パスを保証する。これにより、後続の識別・認証機能（F.IA.AUTH）で、最初の一般利用者の認証機能、および一般利用者の再認証機能に対して、通信データの保護を行う通信パスを保証する。
3. F.MNG.CLNT は、一般利用者の識別・認証機能 F.IA.AUTH を次の条件のとき実行する。
   (ア) 識別・認証が完了していない場合
   (イ) 識別・認証後、セッション有効期限が切れている場合 {FIA_UAU.6}
4. F.MNG.CLNT は、認証された一般利用者に対して、下記の機能を提供する。

(a) 一般利用者に提供する機能

クライアント管理機能は、パスワードとチケットデータまたは、ユーザ名とパスワードで識別・認証された一般利用者のみに対して下記『**リスト 6-19 認証された一般利用者に提供される機能**』を提供する。

リスト 6-19 認証された一般利用者に提供される機能

● 一般利用者自身のパスワードの変更機能 ➢ パスワードとチケットデータで識別・認証された一般利用者に対して下記の機能を提供する。 ➢ パスワード変更画面をブラウザに表示し、認証された一般利用者から入力されたパスワードを受け取って、『リスト 6-17 パスワードに対する条件』で記述される検査を行い {FIA_SOS.1}、検査をパスしたらパスワードを変更し {FMT_MTD.1[3]}、検査にパスしなければエラー表示する。
● チケットの発行 ➢ ユーザ名とパスワードで識別・認証された一般利用者に対して下記の機能を提供する。 ➢ 当該一般利用者のチケット発行許可フラグが「発行可能」となっている場合、一般利用者は、自身のチケットデータを生成し、チケット発行することができる。TOE は、一般利用者がチケット発行すると直ちに、当該一般利用者のチケット発行許可フラグを「発行禁止」にする。{FMT_MTD.1[5]}。

F.MNG.CLNT で、一般利用者がパスワードを変更するときまたはチケットを発行するとき、必ず動作するため迂回されることはない {FPT_RVM.1}。F.MNG.CLNT の管理機能は特定されており {FMT_SMF.1}、セキュリティ役割は維持されている {FMT_SMR.1[2]}。

6.1.4.3.2. IT セキュリティ機能要件

以下に、当該セキュリティ機能の満たす TOE セキュリティ機能要件を述べる。

FIA_SOS.1、FIA_UAU.6、FMT_MTD.1[3]、FMT_MTD.1[5]、FMT_SMF.1、FMT_SMR.1[2]、FPT_RVM.1

6.2. セキュリティ機能強度

本 TOE は、パスワードメカニズムおよび、ワンタイムパスワードメカニズムに対し SOF-基本のセキュリティ機能強度を主張する。該当するパスワードメカニズムおよびワンタイムパスワードメカニズムを用いているセキュリティ機能は、識別認証機能（F.IA.AUTH）及び管理支援機能（F.MNG.ADMIN および F.MNG.CLNT.）である。

6.3. 保証手段

開発者は、セキュリティ保証要件及び開発組織が規定した開発規約に従って開発する。EAL3 を満たすセキュリティ保証要件のコンポーネント及び保証要件に対応する関連文書を『表 6-1 EAL3+ADV_SPM.1 の保証要件と関連文書』に示す。

表 6-1 EAL3+ADV_SPM.1 の保証要件と関連文書

保証要件項目	コンポーネント	関連文書
構成管理	ACM_CAP.3	文書管理方針と手順 SecureTicket Core 構成管理計画書 SecureTicket Core ソースコード管理手順書
	ACM_SCP.1	SecureTicket Core 文書一覧 SecureTicket Core ソースコード一覧
配付と運用	ADO_DEL.1	SecureTicket Core 配付手順書
	ADO_IGS.1	SecureTicket Core ユーザーズガイド 導入編 SecureTicket Core ユーザーズガイド セキュリティ編
開発	ADV_FSP.1	SecureTicket Core 機能仕様書・上位レベル設計書 SecureTicket Core 機能仕様書別冊 SecureTicket Core 暗号運用標準書
	ADV_HLD.2	SecureTicket Core 機能仕様書・上位レベル設計書 SecureTicket Core 機能仕様書別冊 SecureTicket Core 暗号運用標準書

	ADV_RCR.1	SecureTicket Core 表現対応書
	ADV_SPM.1	SecureTicket Core セキュリティ方針モデル仕様書
ガイダンス文書	AGD_ADM.1	SecureTicket Core ユーザーズガイド 導入編 SecureTicket Core ユーザーズガイド 応用編 SecureTicket Core ユーザーズガイド セキュリティ編 SecureTicket Core ユーザーズガイド プログラム編
	AGD_USR.1	SecureTicket Core ユーザーズガイド 一般利用者編 SecureTicket Core ユーザーズガイド セキュリティ編
ライフサイクルサポート	ALC_DVS.1	セキュリティ規定書
テスト	ATE_COV.2	SecureTicket Core テスト網羅率分析書
	ATE_DPT.1	SecureTicket Core テスト深さ分析書
	ATE_FUN.1	SecureTicket Core 機能テスト計画書 SecureTicket Core 機能テスト手順書 SecureTicket Core 機能テスト結果報告書
	ATE_IND.2	TOE
脆弱性評定	AVA_MSU.1	SecureTicket Core ユーザーズガイド 一般利用者編 SecureTicket Core ユーザーズガイド 導入編 SecureTicket Core ユーザーズガイド 応用編 SecureTicket Core ユーザーズガイド セキュリティ編 SecureTicket Core ユーザーズガイド プログラム編
	AVA_SOF.1	SecureTicket Core 機能強度分析書
	AVA_VLA.1	SecureTicket Core 脆弱性分析書

7. PP 主張

本 ST が準拠する PP はない。

8. 根拠

8.1. セキュリティ対策方針根拠

脅威に対するセキュリティ対策方針の関係を『表 8-1 脅威とセキュリティ対策方針の対応』に、前提条件と組織のセキュリティ方針に対するセキュリティ対策方針の関係を『表 8-2 前提条件、組織のセキュリティ方針とセキュリティ対策方針の対応』に示す。

表 8-1 脅威とセキュリティ対策方針の対応

脅威、前提条件、組織のセキュリティ方針 / 対策方針	T.IllAccess	T.EvsDropX	T.EvsDropI	T.EvsDropS	T.MsqrdAdm	T.StolenUsrAthDt	T.StolenUsrTckt
O.IAUsr	○						
O.OTAthDtUsr						○	
O.DblAthDtUsr							○
O.IAUsrCrTckt							
O.IAAdm					○		
O.Manage							
O.UMaint							
O.RvsProxy	○						
O.ComProtect		○	○				
O.SComProtect				○			
O.TsfProtect							
O.Audit	○				○	○	○
OE.STSvrAcct							
OE.TOENetPos							
OE.NetCfg							
OE.Admin							
OE.TcktPwDstr							○
OE.IAStolen							
OE.Audit	○				○	○	○

表 8-2 前提条件、組織のセキュリティ方針とセキュリティ対策方針の対応

脅威、前提条件、組織のセキュリティ方針 / 対策方針	A.TOENetPos	A.NetCfg	A.Admin	A.STSvrAcct	A.TcktPwUsr	P.UsrCrtTckt	P.HDDTsfProtect
O.IAUsr							
O.OTAthDtUsr							
O.DblAthDtUsr							
O.IAUsrCrTckt						○	
O.IAAdm							
O.Manage						○	
O.UMaint						○	
O.RvsProxy							
O.ComProtect							
O.SComProtect							
O.TsfProtect							○
O.Audit						○	
OE.STSvrAcct				○			
OE.TOENetPos	○						
OE.NetCfg		○					
OE.Admin			○				
OE.TcktPwDstr						○	
OE.IAStolen					○		
OE.Audit						○	

以下に、『表 8-1 脅威とセキュリティ対策方針の対応』『表 8-2 前提条件、組織のセキュリティ方針とセキュリティ対策方針の対応』の根拠を示す。

T.IllAccess　保護サーバ上の URL への不許可アクセス

TOE は、**O.RvsProxy** にて、保護サーバ上の URL へのアクセス許可を決定する。このとき、

URL の許可利用者へのなりすましができないように、O.IAUsr にて一般利用者を識別・認証する。
従って、TOE は、実体保護 URL へのアクセスを、予め設定した許可利用者のみに制限できる。
もし、アクセス許可を持たない利用者が当該許可利用者に成りすまそうと、強引にアクセスを試みた場合、O.Audit および OE.Audit によってアクセス不成功がログに残るため、後の調査で対抗できる。
よって、TOE は T.IllAccess に対抗できる。

T.EvsDropX　外部ネットワークでの盗聴
TOE は、O.ComProtect により、外部ネットワークを流れる SecureTicket Core サーバとクライアント間の通信内容を保護する。通信内容が保護されているので、情報の漏洩、すなわち一般利用者が読み取っている実体保護 URL の内容や許可利用者が変更・発行している認証情報は漏洩しない。
これにより、TOE は、外部ネットワークでの盗聴 T.EvsDropX に対抗できる。

T.EvsDropI　内部ネットワークでの盗聴
TOE は、O.ComProtect により、内部ネットワークを流れる SecureTicket Core サーバとクライアント間の通信内容を保護する。通信内容が保護されているので、情報の漏洩、すなわち一般利用者が読み取っている実体保護 URL の内容や許可利用者が変更・発行している認証情報、管理者が管理している管理情報は漏洩しない。
これにより、TOE は、内部ネットワークでの盗聴 T.EvsDropI に対抗できる。

T.EvsDropS　TOE と保護サーバ間での通信内容の盗聴
TOE は、O.SComProtect により、SecureTicket Core サーバと保護サーバ間を流れる情報を保護する。通信内容が保護されているので、情報の漏洩、すなわち一般利用者が読み取っている実体保護 URL の内容は漏洩しない。
これにより、TOE は、TOE と保護サーバ間での通信内容の盗聴 T.EvsDropS に対抗できる。

T.MsqrdAdm　管理者へのなりすまし
TOE は、O.IAAdm により管理者の識別・認証を行う。TOE は O.Audit および OE.Audit により不成功認証のログを残すため、後の調査で対抗できる。
よって、以上により TOE は、T.MsqrdAdm に対抗できる。

T.StolenUsrAthDt　一般利用者認証データを使ってのなりすまし
TOE は O.OTAthDtUsr により、毎回異なる認証データで認証するため、たとえ一般利用者の認証データが攻撃者の手に渡ってしまっても、TOE は攻撃者の入手した認証データと異なる認証データを使って認証することになるので対抗できる。

また、TOE は O.Audit および OE.Audit により不成功認証のログを残すため、後の調査で対抗できる。

よって、以上により TOE は、T.StolenUsrAthDt に対抗できる。

T.StolenUsrTckt　　管理不備の一般利用者チケットを使ってのなりすまし

TOE は、O.DblAthDtUsr により一般利用者の識別・認証を行う。これは、チケットデータとパスワードをもとにしたデータを認証に使っているため、たとえ攻撃者が毎回異なる認証データを生成する元データが格納されたチケットを取得しても TOE の認証データはチケットデータだけでは生成されないので、対抗できる。管理者は OE.TcktPwDstr に従って、一般利用者に安全な方法でチケットとパスワードを配布するので、一般利用者は安全にチケットとパスワードを入手する。TOE は O.Audit および OE.Audit により不成功認証のログを残すため、後の調査で対抗できる。

よって、以上により TOE は、T.StolenUsrTckt に対抗できる。

A.TOENetPos　TOE のネットワーク設置条件

OE.TOENetPos により、管理者は、すべての TOE が動作する SecureTicket Core サーバを、DMZ または内部ネットワークに接続する。これにより、A.TOENetPos は満たされる。

A.NetCfg　　TOE のネットワーク構成条件

OE.NetCfg により、管理者は、すべてのクライアントが必ず SecureTicket Core サーバを中継して保護サーバと通信を行い、保護サーバは SecureTicket Core サーバとのみ通信を行うようネットワーク設定を行う。これにより、A.NetCfg は満たされる。

A.Admin　　信頼できる管理者

OE.Admin により、責任者は、不正を行わない人物を管理者として選任する。これにより、A.Admin は満たされる。

A.STSvrAcct　SecureTicket Core サーバのアカウント管理

OE.StSvrAcct により、SecureTicket Core サーバの OS は識別・認証機能を持ち、当該 OS に対して管理者アカウントのみ作成する。これにより、A.STSvrAcct は満たされる。

A.TcktPwUsr　一般利用者認証情報同時紛失

OE.IAStolen により、一般利用者は、管理者から認証情報の入ったチケットとパスワードが決して同時に他人の手に渡らないよう教育・指導を受ける。これにより、A.TcktPwUsr は満たされる。

P.UsrCrtTckt　一般利用者のチケット発行

TOE は、O.Manage により管理者のみに、チケット発行を行う一般利用者のアカウント状態を「チケット発行可能状態」とする機能を提供する。管理者は「一般利用者本人に対してチケットを発行できる状態」にすると同時に、OE.TcktPwDstr に従って、一般利用者に安全な方法でパスワードを配布する。TOE は、O.IAUsrCrTckt によって自身のチケット発行を試みる一般利用者をユーザ名とパスワードにより識別認証し、O.UMaint によって、一般利用者自身のチケットを発行する機能を一般利用者本人のみに提供するので、一般利用者は自分自身でチケットの発行を行える。攻撃者が一般利用者に成り済ましを試みた場合、TOE は O.Audit および OE.Audit によって認証不成功のログを残すため、後の調査時に利用できる。

以上により、P.UsrCrtTckt は満たされる。

P.HDDTsfProtect　TOE のハードディスク内容の保護

TOE は、O.TsfProtect によりハードディスクに格納されている基本設定ファイル、ユーザ・グループ情報ファイル、パスワード精査設定ファイルの内容を暗号化する。P.HDDTsfProtect は、TOE のユーザ・グループ情報ファイル、基本設定ファイル、パスワード精査設定ファイルの内容を暗号化して格納することとするという組織の方針である。

O.TsfProtect により、組織のセキュリティ方針で列挙されているファイルはすべて暗号化されるため、TOE は P.HDDTsfProtect を達成できる。

8.2. セキュリティ要件根拠

8.2.1. セキュリティ機能要件根拠

8.2.1.1.　セキュリティ対策方針と IT セキュリティ機能要件の対応

セキュリティ対策方針に対する TOE セキュリティ機能要件の対応を以下の『表 8-3 セキュリティ対策方針と IT セキュリティ機能要件の対応』に示す。

表 8-3 セキュリティ対策方針と IT セキュリティ機能要件の対応

セキュリティ対策方針 / セキュリティ機能要件	O.IAUsr	O.OTAthDtUsr	O.DblAthDtUsr	O.IAUsrCrTckt	O.IAAdm	O.Manage	O.UMaint	O.RvsProxy	O.ComProtect	O.SComProtect	O.TsfProtect	O.Audit	OE.STSvrAcct	OE.Audit
FAU_GEN.1												○		
FAU_STG.4												○		
FCS_CKM.1									○		○			

FCS_COP.1		○			○				○		○			
FDP_ACC.1								○						
FDP_ACF.1								○						
FIA_AFL.1	○			○	○									
FIA_ATD.1								○						
FIA_SOS.1			○	○										
FIA_SOS.2		○			○									
FIA_UAU.2	○			○	○									
FIA_UAU.4		○			○									
FIA_UAU.5		○		○	○									
FIA_UAU.6	○				○									
FIA_UAU.7			○	○										
FIA_UID.2	○			○	○									
FIA_USB.1								○						
FMT_MOF.1			○	○						○		○		
FMT_MSA.1								○						
FMT_MSA.2									○		○			
FMT_MSA.3								○						
FMT_MTD.1[1]			○	○										
FMT_MTD.1[2]			○	○										
FMT_MTD.1[3]			○											
FMT_MTD.1[4]			○											
FMT_MTD.1[5]							○							
FMT_MTD.1[6]			○	○										
FMT_MTD.1[7]						○								
FMT_MTD.1[8]			○	○										
FMT_MTD.1[9]	○			○										
FMT_MTD.1[10]	○			○										
FMT_MTD.1[11]	○				○									
FMT_SMF.1	○		○	○	○					○		○		
FMT_SMR.1[1]	○		○	○	○	○		○		○		○		
FMT_SMR.1[2]			○				○							
FPT_RVM.1	○	○	○	○	○	○	○	○	○	○	○	○		
FTA_TSE.1[1]			○	○										
FTA_TSE.1[2]			○											

FTP_ITC.1										○				
FTP_TRP.1[1]									○					
FTP_TRP.1[2]									○					
FAU_SAR.1[E]														○
FAU_STG.1[E]														○
FIA_UAU.2[E]													○	
FIA_UAU.7[E]													○	
FIA_UID.2[E]													○	
FPT_STM.1[E]														○

以下に、『表 8-3 セキュリティ対策方針と IT セキュリティ機能要件の対応』の根拠を示す。

O.IAUsr： 一般利用者の識別認証機能

FIA_UID.2 により、一般利用者を識別し、FIA_UAU.2 により一般利用者の認証が行われる。このとき、FIA_UAU.6 により、セッション有効期限が過ぎている場合、保護対象資産へのアクセス時に、再度、認証を促す。FIA_AFL.1 により、N（管理者により選択される 1～１００）回の認証失敗で、アカウントがロックされるため、総当り攻撃に対抗できる。

FMT_MTD.1[9]により、Ticket 認証エラーステータスのリセットを管理者のみに許可し、FMT_MTD.1[10]により、連続失敗認証検出回数の問い合わせ、登録、改変を管理者のみに許可し、FMT_MTD.1[11]により、認証の有効時間の問い合わせ、改変を管理者のみに許可する。FMT_SMF.1 により、管理機能は特定されており、この管理者役割は FMT_SMR.1[1]により維持される。

FPT_RVM.1 によりこれらの機能は必ず実行される。よって、O.IAUsr は実現できる。

O.OTAthDtUsr：一般利用者のワンタイムパスワード

FCS_COP.1 によりハッシュ値を生成し、それを基に FIA_SOS.2 により、ワンタイムパスワードを生成し、その品質尺度を保証する。このワンタイムパスワードは、FIA_UAU.4 により、再利用が防止されている。FIA_UAU.5 により、複数の認証メカニズムが用意され、一般利用者が公開保護 URL やパスワード変更機能にアクセスする場合には、ワンタイムパスワードメカニズムを提供する。

FPT_RVM.1 によりこれらの機能は必ず実行される。よって、O.OTAthDtUsr は実現できる。

O.DblAthDtUsr：一般利用者の二要素認証

FIA_UAU.7 により一般利用者が入力するパスワードはフィードバックされない。FIA_SOS.1 により、パスワードの品質尺度は保証される。FTA_TSE.1[1]によりパスワードの有効期限が切れている場合、TOE はセッションの確立を拒否し、パスワード変更を促す。FTA_TSE.1[2]に

より、Ticket 認証許可時間帯、Ticket 認証有効開始日時、Ticket 認証有効期限の条件に合わない場合はセッションの確立を拒否することが保証される。

FMT_MOF.1 により、パスワードの品質尺度を変更することおよび一般利用者の認証をチケット認証のみに変更することは、管理者にのみ制限することができる。FMT_MTD.1[1]により、ユーザ情報レコード、グループ情報レコードの登録、削除を管理者にのみ許可し、FMT_MTD.1[2]により、一般利用者のパスワードの登録、改変を管理者のみに許可し、FMT_MTD.1[3]により、一般利用者本人のパスワードの変更を識別・認証された一般利用者本人にのみ許可し、FMT_MTD.1[4]により、一般利用者のチケットの発行を管理者のみに許可し、FMT_MTD.1[6]により、使用禁止ワードの登録を管理者のみに許可し、FMT_MTD.1[8]により、パスワードの有効期限、Ticket 認証許可時間帯、Ticket 認証有効開始日時、Ticket 認証有効期限の登録、削除、改変を管理者のみに許可する。FMT_SMF.1 により、管理機能は特定されており、管理者役割は FMT_SMR.1[1]により維持される。一般利用者役割は FMT_SMR.1[2]により維持される。

FPT_RVM.1 によりこれらの機能は必ず実行される。よって、O.DblAthDtUsr は実現できる。

O.IAUsrCrTckt： 一般利用者のチケット発行時識別認証機能

FIA_UID.2 により、一般利用者が本人であることを識別し、FIA_UAU.2 により一般利用者の認証が行われる。FIA_UAU.7 により一般利用者が入力するパスワードはフィードバックされない。このとき、FIA_SOS.1 により、パスワードの品質尺度は保証される。FTA_TSE.1[1]によりパスワードの有効期限が切れている場合、TOE はセッションの確立を拒否し、パスワード変更を促す。FIA_UAU.5 により、複数の認証メカニズムが用意され、一般利用者が一般利用者本人のチケット発行機能にアクセスする場合には、パスワードメカニズムを提供する。FIA_AFL.1 により、N（管理者により選択される 1～１００）回の認証失敗で、アカウントがロックされるため、総当り攻撃に対抗できる。

FMT_MOF.1 により、パスワードの品質尺度の変更は、管理者にのみ制限することができる。FMT_MTD.1[1]により、ユーザ情報レコード、グループ情報レコードの登録、削除を管理者にのみ許可し、FMT_MTD.1[2]により、一般利用者のパスワードの登録、改変を管理者のみに許可し、FMT_MTD.1[6]により、使用禁止ワードの登録を管理者のみに許可し、FMT_MTD.1[8]により、パスワードの有効期限、Ticket 認証許可時間帯、Ticket 認証有効開始日時、Ticket 認証有効期限の登録、削除、改変を管理者のみに許可し、FMT_MTD.1[9]により、Ticket 認証エラーステータスのリセットを管理者のみに許可し、FMT_MTD.1[10]により、連続失敗認証検出回数の問い合わせ、登録、改変を管理者のみに許可する。FMT_SMF.1 により、管理機能は特定されており、この管理者役割は FMT_SMR.1[1]により維持される。

FPT_RVM.1 によりこれらの機能は必ず実行される。よって、O.IAUsrCrTckt は実現できる。

O.IAAdm： 管理者の識別認証機能

FIA_UID.2 により、管理者が本人であることを識別し、FIA_UAU.2 により管理者の認証が行われる。FCS_COP.1 によりハッシュ値を生成し、それを基に FIA_SOS.2 により、ワンタイムパスワードを生成し、その品質尺度を保証する。このワンタイムパスワードは、FIA_UAU.4 により、再利用が防止されている。FIA_UAU.5 により、複数の認証メカニズムが用意され、管理者が管理機能にアクセスする場合には、ワンタイムパスワードメカニズムを提供する。FIA_AFL.1 により、N（管理者により選択される 1～１００）回の認証失敗で、アカウントがロックされるため、総当り攻撃に対抗でき、FIA_UAU.6 により、セッション有効期限が過ぎている場合、再度、認証を促す。また、FMT_MTD.1[11]により、認証の有効時間の問い合わせ、改変を管理者のみに許可する。FMT_SMF.1 により、管理機能は特定されており、この管理者役割は FMT_SMR.1[1]により維持される。

FPT_RVM.1 によりこれらの機能は必ず実行される。よって、O.IAAdm は実現できる。

O.Manage：管理機能

FMT_MTD.1[7]により、チケット発行許可フラグを「発行可能」または「発行禁止」に改変する機能を、識別・認証された管理者のみに許可する。

この管理者役割は FMT_SMR.1[1]により維持される。

FPT_RVM.1 によりこれらの機能は必ず実行される。

よって、以上より、O.Manage は実現できる。

O.UMaint：一般利用者向け保守機能

TSF は、FMT_MTD.1[5]により、識別・認証された一般利用者にのみ、本人のチケット発行許可フラグが「発行可能」であるときに限り、本人のチケットを発行し、直ちにチケット発行許可フラグを「発行禁止」（一般利用者自身が本人のチケットを発行することを禁止する状態）とすることを許可する。

FMT_SMR.1[2]により、この識別・認証された一般利用者役割は維持される。

FPT_RVM.1 によりこれらの機能は必ず実行される。

よって、以上より、O.UMaint は実現できる。

O.RvsProxy：保護サーバアクセス制御

FIA_USB.1 により、利用者を代行するサブジェクトに、FIA_ATD.1 により定義された個々の利用者に属するセキュリティ属性（ユーザ ID およびグループ ID）が関連づけられ、維持される。

FDP_ACC.1 と FDP_ACF.1 によって、公開保護 URL に対して、その時点でグループ有効開始日時、グループ有効期限で指定される時間帯で有効なグループ ID、許可・拒否属性を求めることができる。これをもとに、利用者に関連付けられるグループ ID と合わせて、利用者が公開保護 URL にアクセスを許されるか否かを確認する。公開保護 URL は、TOE で実体保護 URL に一対一で対応づけられているので、サブジェクトの公開保護 URL に対するアクセス許可で、対応する

実体保護 URL へのアクセスを許可する。

FMT_MSA.1 により、公開保護 URL のセキュリティ属性であるグループ名、許可・拒否属性、グループ有効開始日時、グループ有効期限を、問い合わせ、登録、削除することを管理者にのみ制限し、FMT_MSA.3 により、公開保護 URL の許可的属性であるセキュリティ属性のデフォルト値を上書きすることを管理者にのみ制限している。この管理者役割は FMT_SMR.1[1]により維持される。

FPT_RVM.1 によりこれらの機能は必ず実行される。

よって、O.RvsProxy は実現できる。

O.ComProtect：クライアント ー TOE 間通信経路の保護

FTP_TRP.1[1]、FTP_TRP.1[2]により、信頼できる通信路が提供される。

FTP_TRP.1[2]は、FCS_CKM.1 で生成した暗号鍵を使って FCS_COP.1 にて暗号化・復号することで、実現している。このとき、FMT_MSA.2 により暗号鍵に関するセキュリティ属性としてセキュアな値のみ受け付ける。

FPT_RVM.1 によりこれらの機能は必ず実行される。

よって、O.ComProtect は実現できる。

O.SComProtect：TOE ー 保護サーバ間通信経路の保護

FTP_ITC.1 により、信頼できる通信路が提供される。

FMT_MOF.1 により、信頼できる通信路を提供する「TOEー保護サーバ間通信 保護機能」の管理を管理者に制限することができる。FMT_SMF.1 により、管理機能は特定されており、この管理者役割は FMT_SMR.1[1]により維持される。また、FPT_RVM.1 によりこれらの機能は必ず実行される。

よって、O.SComProtect は実現できる。

O.TsfProtect：基本設定ファイル、ユーザ・グループ情報ファイル、パスワード精査設定ファイルの保護

FCS_CKM.1 により、AES の暗号鍵が生成され、その鍵を使って、FCS_COP.1 により、ユーザ・グループ情報ファイル、基本設定ファイルおよびパスワード精査設定ファイルに格納されている、暗号化された情報が、復号される。このとき、FMT_MSA.2 により暗号鍵に関するセキュリティ属性としてセキュアな値のみ受け付ける。また、FCS_COP.1 により、ユーザ・グループ情報を暗号化してユーザ・グループ情報ファイルに書き込む。

同様に、FCS_COP.1 により、基本設定ファイル内容、パスワード精査設定ファイル内容を暗号化してそれぞれのファイルに書き込む。

FPT_RVM.1 によりこれらの機能は必ず実行される。

よって、O.TsfProtect は実現できる。

O.Audit：監査情報の記録

FAU_GEN.1 により、監査情報が生成される。FAU_STG.4 により、監査証跡が満杯になった場合、最も古くに格納された監査記録へ上書きを行い、監査記録の失敗時には、SecureTicket Core サーバのコンソールに監査データを出力する。

FMT_MOF.1 により、監査情報の出力レベルの変更能力を管理者のみに制限することができる。FMT_SMF.1 により、管理機能は特定されており、この管理者役割は FMT_SMR.1[1]により維持される。FPT_RVM.1 によりこれらの機能は必ず実行される。

「表 5-1 監査対象となる事象一覧」に示した事象を監査対象にすることで、不正アクセスや成りすましの脅威に十分対抗できる。

よって、O. Audit は実現できる。

OE.STSvrAcct：SecureTicket Core サーバの管理者アカウント

IT 環境としての SecureTicket Core サーバの OS は、IT 環境のセキュリティ機能要件 FIA_UID.2[E]により、管理者が本人であることを識別し、FIA_UAU.2[E]により管理者の認証を行える。また、FIA_UAU.7[E]により、管理者が入力するパスワードはフィードバックしない。

よって、OE.STSvrAcct を実現できる。

OE.Audit：IT 環境の監査支援

IT 環境としての SecureTicket Core サーバの OS は、IT 環境のセキュリティ機能要件 FAU_STG.1[E]により、格納された監査記録を保護し、FPT_STM.1[E]により、高信頼タイムスタンプを TSF に提供し、FAU_SAR.1[E]により、監査記録「表 5-1 監査対象となる事象一覧」に示した事象を読み出すことができる。

よって、OE.Audit を実現できる。

8.2.1.2. セキュリティ要件セットの内部的一貫性

チケットによるワンタイムパスワードでの認証の対策方針（O.OTAthDtUsr、O.IAAdm）、二要素認証の対策方針（O.DblAthDtUsr）に関連するセキュリティ機能要件は、互いに協調しあってこれらの対策方針を実現しているので、対応するセキュリティ機能要件間での競合は発生しない。これらのセキュリティ対策方針は他のセキュリティ対策方針（O.IAUsrCrTckt）と互いに異なる事象である。当該セキュリティ対策方針に対する各セキュリティ機能要件は、それぞれのセキュリティ対策方針を実現するために相互補完的に働いているので、セキュリティ機能要件間で競合は発生しない。

8.2.2.IT セキュリティ機能要件間の依存関係

TOE セキュリティ機能要件間および IT 環境のセキュリティ機能要件間の依存関係は『表 8-4

IT セキュリティ機能要件間の依存関係』に示すように、暗号鍵生成（FCS_CKM.1）、暗号操作（FCS_COP.1）、およびセキュアなセキュリティ属性（FMT_MSA.2）以外、すべての必要な依存関係を満たしている。暗号鍵の破棄は、揮発性メモリに格納されているデータがサーバモジュールの停止と共に破棄されるため、それを悪用するインタフェースはないため、明示的に破棄する機能要件は不要である。

表 8-4 IT セキュリティ機能要件間の依存関係

セキュリティ機能要件	CC Part 2 での依存先	ST での実際の依存先	備考
FAU_GEN.1	FPT_STM.1	FPT_STM.1[E]	OK
FAU_STG.4	FAU_STG.1	FAU_STG.1[E]	OK
FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1] FCS_CKM.4 FMT_MSA.2	FCS_COP.1 FMT_MSA.2	暗号鍵は、揮発性メモリに格納されており、SecureTicket Core サーバが停止するとき、破棄されるため、FCS_CKM.4 は必要ない。
FCS_COP.1	[FDP_ITC.1 または FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1 FMT_MSA.2	AES の暗号鍵は、揮発性メモリに格納されており、SecureTicket Core サーバが停止するとき、破棄されるため、FCS_CKM.4 は必要ない。 SHA-256 はハッシュ関数であり、暗号鍵を持たず、暗号鍵の生成・破棄およびセキュアのセキュリティ属性の管理が不要であるから依存性は不要。
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	OK
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	OK
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	高位レベルのコンポーネントで依存先を満たしている。
FIA_ATD.1	なし	なし	OK

FIA_SOS.1	なし	なし	OK
FIA_SOS.2	なし	なし	OK
FIA_UAU.2	FIA_UID.1	FIA_UID.2	高位レベルのコンポーネントで依存先を満たしている。
FIA_UAU.4	なし	なし	OK
FIA_UAU.5	なし	なし	OK
FIA_UAU.6	なし	なし	OK
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2	高位レベルのコンポーネントで依存先を満たしている。
FIA_UID.2	なし	なし	OK
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	OK
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]	OK
FMT_MSA.1	[FDP_ACC.1 または FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1[1]	OK
FMT_MSA.2	ADV_SPM.1 [FDP_ACC.1 または FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	ADV_SPM.1 FDP_ACC.1	FMT_MSA.2 から FMT_MSA.1 および FMT_SMR.1 への依存性は次の理由から不要である。暗号鍵に係る属性は、AES または SHA-256 で定められた方式や鍵長などであり、固定であるから、管理する必要はない。
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1[1]	OK
FMT_MTD.1[1]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]	OK

FMT_MTD.1[2]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]	OK
FMT_MTD.1[3]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]	OK
FMT_MTD.1[4]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]	OK
FMT_MTD.1[5]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]	OK
FMT_MTD.1[6]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]	OK
FMT_MTD.1[7]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]	OK
FMT_MTD.1[8]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]	OK
FMT_MTD.1[9]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]	OK
FMT_MTD.1[10]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]	OK
FMT_MTD.1[11]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]	OK
FMT_SMF.1	なし	なし	OK
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2	高位レベルのコンポーネントで依存先を満たしている。
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2	高位レベルのコンポーネントで依存先を満たしている。
FPT_RVM.1	なし	なし	OK
FTA_TSE.1[1]	なし	なし	OK
FTA_TSE.1[2]	なし	なし	OK
FTP_ITC.1	なし	なし	OK
FTP_TRP.1[1]	なし	なし	OK
FTP_TRP.1[2]	なし	なし	OK
FAU_SAR.1[E]	FAU_GEN.1	FAU_GEN.1	OK
FAU_STG.1[E]	FAU_GEN.1	FAU_GEN.1	OK

FIA_UAU.2[E]	FIA_UID.1	FIA_UID.2[E]	高位レベルのコンポーネントで依存先を満たしている。
FIA_UAU.7[E]	FIA_UAU.1	FIA_UAU.2[E]	高位レベルのコンポーネントで依存先を満たしている。
FIA_UID.2[E]	なし	なし	OK
FPT_STM.1[E]	なし	なし	OK

8.2.3.IT セキュリティ保証要件間の依存関係

IT セキュリティ保証要件間の依存関係は、本 TOE の保証要件として、EAL3 保証要件パッケージに ADV_SPM.1 を追加している。ADV_SPM.1 は、EAL3 に含まれる ADV_FSP.1 に依存しているため、IT セキュリティ保証要件の依存関係は満たされる。

8.2.4.TOE セキュリティ機能要件の相互作用

TOE セキュリティ機能要件間の相互作用について、『表 8-5 TOE セキュリティ機能要件の相互作用』に示す。

表 8-5 TOE セキュリティ機能要件の相互作用

セキュリティ機能要件	防御を提供している機能		
	迂回	破壊	非活性化
FAU_GEN.1	FPT_RVM.1	N/A	FMT_MOF.1
FAU_STG.4	FPT_RVM.1	N/A	
FCS_CKM.1	FPT_RVM.1	N/A	
FCS_COP.1	FPT_RVM.1	N/A	
FDP_ACC.1	FPT_RVM.1	N/A	
FDP_ACF.1	FPT_RVM.1	N/A	
FIA_AFL.1	FPT_RVM.1	N/A	
FIA_ATD.1	FPT_RVM.1	N/A	
FIA_SOS.1	FPT_RVM.1	N/A	FMT_MOF.1
FIA_SOS.2	FPT_RVM.1	N/A	
FIA_UAU.2	FPT_RVM.1	N/A	
FIA_UAU.4	FPT_RVM.1	N/A	
FIA_UAU.5	FPT_RVM.1	N/A	

FIA_UAU.6	FPT_RVM.1	N/A	
FIA_UAU.7	FPT_RVM.1	N/A	
FIA_UID.2	FPT_RVM.1	N/A	
FIA_USB.1	FPT_RVM.1	N/A	
FMT_MOF.1	N/A	N/A	
FMT_MSA.1	N/A	N/A	
FMT_MSA.2	FPT_RVM.1	N/A	
FMT_MSA.3	N/A	N/A	
FMT_MTD.1[1]	N/A	N/A	
FMT_MTD.1[2]	N/A	N/A	
FMT_MTD.1[3]	N/A	N/A	
FMT_MTD.1[4]	N/A	N/A	
FMT_MTD.1[5]	N/A	N/A	
FMT_MTD.1[6]	N/A	N/A	
FMT_MTD.1[7]	N/A	N/A	
FMT_MTD.1[8]	N/A	N/A	
FMT_MTD.1[9]	N/A	N/A	
FMT_MTD.1[10]	N/A	N/A	
FMT_MTD.1[11]	N/A	N/A	
FMT_SMF.1	N/A	N/A	
FMT_SMR.1[1]	N/A	N/A	
FMT_SMR.1[2]	N/A	N/A	
FPT_RVM.1		N/A	
FTA_TSE.1[1]	FPT_RVM.1	N/A	
FTA_TSE.1[2]	FPT_RVM.1	N/A	
FTP_ITC.1	FPT_RVM.1	N/A	FMT_MOF.1
FTP_TRP.1[1]	FPT_RVM.1	N/A	
FTP_TRP.1[2]	FPT_RVM.1	N/A	

上記の N/A は適用外を意味する。

【迂回】　FPT_RVM.1
TOE の管理機能及びリバースプロキシ機能を使用するにあたり、管理者及び一般利用者への識別認証(FIA_AFL.1、FIA_ATD.1、FIA_SOS.1、FIA_SOS.2、FIA_UAU.2、FIA_UAU.4、FIA_UAU.5、FIA_UAU.6、FIA_UAU.7、FIA_UID.2、FIA_USB.1)は必ず実施されるため、迂回されない。
識別・認証を経た後、実体保護 URL へアクセスする時は、かならずアクセス制御(FDP_ACC.1 と FDP_ACF.1)を元にアクセスされるため、迂回されない。
FCS_CKM.1 および FMT_MSA.2 は TOE 起動時に暗号鍵が必ず生成され、セキュアなものだけが受け入れられるため、迂回されない。
FCS_COP.1 は各種ファイルへの読み込み/書き込み時および独自通信プロトコルでの通信時に、必ず暗号化/復号が実行されるため迂回されない。また、FCS_COP.1 は識別・認証の処理時にも必ずハッシュ値が生成されるため、迂回されない。
FTA_TSE.1[1]はおよび FTA_TSE.1[2]は、識別認証の処理に当たり必ず実行され、セッションは特定された条件に合致した場合は拒否されるため迂回されない。
FTP_ITC.1 は、TOE と保護サーバとの通信にあたり、管理者が指定した場合は必ず、通信路を保護する機能が実行されるため、迂回されない。
FTP_TRP.1[1]は、一般利用者クライアントと SecureTicket Core サーバ間との通信において、必ず SSL プロトコルにて通信路を保護する機能が実行されるため、迂回されない。
FTP_TRP.1[2]は、管理者クライアントと SecureTicket Core サーバ間との通信において、必ず独自通信プロトコルにて通信路を保護する機能が実行されるため、迂回されない。
監査機能は、ディスク領域がある限り、必ず監査証跡に残る。(FAU_GEN.1、FAU_STG.4)
FPT_RVM.1 により、以上が確実に実行されるため、迂回を防止する。

【非活性化】　FMT_MOF.1
TOE－保護サーバ間通信 保護機能の有効/無効を指定する能力（FTP_ITC.1)、パスワードの品質尺度を変更する能力、一般利用者認証をパスワードとチケットを併用した認証とするかチケットのみの認証とするか指定する能力（FIA_SOS.1）および監査情報の出力レベルを変更する（FAU_GEN.1）能力は、管理者のみに制限されている。他のセキュリティ機能については、非活性化する機能がない。

【改竄】　FPT_SEP.1
セキュリティ機能を実現するサブジェクトは、信頼される JVM（Java Virtual Machine）上で動作するが、JVM は、それらのサブジェクトが動作するためのメモリ空間を管理保護し、他サブジェクトからの干渉を防ぐ。したがって、サブジェクトの干渉と改竄が防止されているので、FPT_SEP.1 は必要ない。
よって、改竄は防止できる。

【検出】　FAU_GEN.1
『表 5-1 監査対象となる事象一覧』に示すように監査対象のセキュリティ機能要件の侵害事象を検出する。

8.2.5.セキュリティ対策方針に対するセキュリティ機能強度の一貫性

本 ST が主張する TOE の最小機能強度は SOF-基本である。
TOE は、以下のような環境にて運用されることが想定されている。

- TOE の動作する SecureTicket Core サーバは、管理者以外がログインすることは無い。
- TOE は DMZ 上または内部ネットワーク上に設置された SecureTicket Core サーバ上で動作する。
- TOE は、『2.5.5 TOE の動作環境』で定義された環境で利用される。
- 不正行為は公開インタフェースを利用した攻撃である。

よって、脅威エージェントを以下の人物に特定できる。
　攻撃能力 ： 低レベル
以上により、上記の攻撃能力を有した脅威エージェントに対して十分な対抗性があることからセキュリティ対策方針に対する最小機能強度として SOF-基本が適切であり、一貫している。

8.2.6.保証要件根拠

本 TOE は、商用利用される製品であり、低レベルの攻撃能力を有する脅威　に対抗するために、TOE の機能と外部インタフェースの仕様、開発者テストの結果、明らかな脆弱性に対する開発者の分析及び機能強度分析などが必要となる。したがって、評価保証レベルは EAL3＋ADV_SPM.1 が妥当である。この評価保証レベルの保証要件コンポーネントに対応する保証手段となるドキュメントは『表 6-1 EAL3+ADV_SPM.1 の保証要件と関連文書』で定義されるとおりであり、これらの文書により、要求されるすべての保証要件コンポーネントが満たされる。
以上の理由により、保証要件は満たされる。

8.3.TOE 要約仕様根拠

8.3.1.TOE 要約仕様に対するセキュリティ機能要件の適合性

TOE 要約仕様に適合するセキュリティ機能要件の関係を『表 8-6　IT セキュリティ機能とセキュリティ機能要件の対応』に示す。

表 8-6　IT セキュリティ機能とセキュリティ機能要件の対応

IT セキュリティ機能 / セキュリティ機能要件	F.IA.AUTH	F.REVPROXY	F.TOESVRPRT	F.AUDIT	F.MNG.FILEIO	F.MNG.ADMIN	F.MNG.CLNT
FAU_GEN.1				○			
FAU_STG.4				○			
FCS_CKM.1					○		
FCS_COP.1	○				○	○	
FDP_ACC.1		○					
FDP_ACF.1		○					
FIA_AFL.1	○						
FIA_ATD.1		○					
FIA_SOS.1						○	○
FIA_SOS.2	○						
FIA_UAU.2	○						
FIA_UAU.4	○						
FIA_UAU.5	○						
FIA_UAU.6		○				○	○
FIA_UAU.7	○						
FIA_UID.2	○						
FIA_USB.1		○					
FMT_MOF.1						○	
FMT_MSA.1						○	
FMT_MSA.2					○		
FMT_MSA.3						○	
FMT_MTD.1[1]						○	
FMT_MTD.1[2]						○	
FMT_MTD.1[3]							○
FMT_MTD.1[4]						○	
FMT_MTD.1[5]							○
FMT_MTD.1[6]						○	
FMT_MTD.1[7]						○	
FMT_MTD.1[8]						○	
FMT_MTD.1[9]						○	

FMT_MTD.1[10]						○	
FMT_MTD.1[11]						○	
FMT_SMF.1						○	○
FMT_SMR.1[1]						○	
FMT_SMR.1[2]							○
FPT_RVM.1	○	○	○	○	○	○	○
FTA_TSE.1[1]	○						
FTA_TSE.1[2]	○						
FTP_ITC.1			○				
FTP_TRP.1[1]		○					
FTP_TRP.1[2]						○	

以下に、『表 8-6　IT セキュリティ機能とセキュリティ機能要件の対応』の根拠を示す。

FAU_GEN.1

F.AUDIT では、サーバモジュール監査機能の起動と終了および『リスト 6-5 F.AUDIT の監査事象一覧』を発生日時、ユーザ名とともに記録している。監査機能の起動と終了はサーバモジュールの起動と終了に連動しているので、F.AUDIT では監査機能の起動と終了を記録している。

『リスト 6-5 F.AUDIT の監査事象一覧』で記載される内容は、TOE セキュリティ機能要件コンポーネント FAU_GEN.1 の記述に示す『表 5-1 監査対象となる事象一覧』で規定される内容を具体化している。

『表 5-1 監査対象となる事象一覧』で、最小レベルの監査対象事象を監査証跡に生成しないことの正当性根拠については、『表 8-7 最小レベルの監査対象事象を満たさないことの正当性根拠』に示すとおりである。

以上により、F.AUDIT を実装することで FAU_GEN.1 を実現できる。

表 8-7 最小レベルの監査対象事象を満たさないことの正当性根拠

セキュリティ機能要件	最小レベルの監査対象事象	最小レベルを満たさないことの正当性根拠
FIA_SOS.2	TSF による、テストされた秘密の拒否	ワンタイムパスワードは、SHA-256 によるハッシュ値生成に成功していれば、必ず、指定の秘密の規定になる。これが満たされないときは、SHA-256 のハッシュ値生成で失敗しているときでありそのときは、FCS_CKM.1 で検出されるから監査証跡の生成は不要である。

FIA_UAU.4	認証データを再使用する試み。	認証データを再使用した場合、単なる認証失敗として監査証跡を残すため監査証跡の生成は不要である。
FIA_UAU.5	認証の最終決定。	最終的に失敗したときの認証を記録しているため、セキュリティ侵害は起こらず、認証成功時の監査証跡の生成は不要である。
FIA_UAU.6	再認証の失敗	再認証に失敗した場合、単なる認証失敗として監査証跡を残すため監査証跡の生成は不要である。
FIA_USB.1	利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。	利用者セキュリティ属性のサブジェクトに対する結合が不成功であったら、公開保護 URL にアクセスするとき、再認証が発生するためセキュリティ侵害は起こらず監査証跡の生成は不要である。
FMT_MOF.1	TSF の機能のふるまいにおけるすべての改変	TSF のふるまい変更は管理者にのみ許可されているため、監査証跡の生成は不要である。
FMT_MSA.1	セキュリティ属性の値の改変すべて	セキュリティ属性の変更は管理者にのみ許可されているため、監査証跡の生成は不要である。
FMT_MSA.2	セキュリティ属性に対して提示され、拒否された値すべて	暗号鍵に関するセキュリティ属性は、セキュリティ方針モデル仕様書で規定されるセキュリティ属性で、固定のため拒否されることが無いため監査証跡の生成は不要である。
FMT_MSA.3	許可的あるいは制限的規則のデフォルト設定の改変	オブジェクト、サブジェクトが生成されるときのデフォルト値は固定であるため、監査証跡の生成は不要である。
FMT_MTD.1[4]	TSF データの値のすべての改変	この機能要件で TSF データは変更されないため、監査証跡の生成は不要である。
FMT_MTD.1[5]	TSF データの値のすべての改変	この機能要件で TSF データは変更されないため、監査証跡の生成は不要である。
FMT_MTD.1[6]	TSF データの値のすべての改変	使用禁止ワードを登録、変更、削除できるのは管理者のみであり、管理者はこのデータの変更・削除が、TOE のセキュリティポリシーにどのような影響を与えるかよく理解しているため不要である。

FMT_MTD.1[7]	TSF データの値のすべての改変	管理者のみが、チケットを必要としている一般利用者のためにだけ、本人のチケット発行許可フラグの改変を行い、一般利用者がチケットをセキュアに発行できるよう運用を行うため、監査証跡の生成は不要である。
FMT_MTD.1[8]	TSF データの値のすべての改変	TSF データの変更は管理者にのみ許可されているため、監査証跡の生成は不要である。
FMT_MTD.1[9]	TSF データの値のすべての改変	TSF データの変更は管理者にのみ許可されているため、監査証跡の生成は不要である。
FMT_MTD.1[10]	TSF データの値のすべての改変	TSF データの変更は管理者にのみ許可されているため、監査証跡の生成は不要である。
FMT_MTD.1[11]	TSF データの値のすべての改変	TSF データの変更は管理者にのみ許可されているため、監査証跡の生成は不要である。
FMT_SMF.1	管理機能の使用	管理者のみが、管理機能を使用することができ、その内容を把握できるため、監査証跡の生成は不要である。
FMT_SMR.1[1]	役割の一部をなす利用者のグループに対する改変	管理者は固定であるため、改変は起こらず、監査証跡の生成は不要である。
FMT_SMR.1[2]	役割の一部をなす利用者のグループに対する改変	一般利用者は固定であるため、改変は起こらず、監査証跡の生成は不要である。
FTA_TSE.1[1]	セション確立メカニズムによるセション確立の拒否	セッション確立が拒否された場合、一般利用者は、再度認証を要求される。このため、認証失敗でセッション確立の拒否を検出できるため、監査証跡の生成は不要である。
FTA_TSE.1[2]	セション確立メカニズムによるセション確立の拒否	セッション確立が拒否された場合、一般利用者は、再度認証を要求される。このため、認証失敗でセッション確立の拒否を検出できるため、監査証跡の生成は不要である。

FAU_STG.4

F.AUDIT では、監査証跡エリアが満杯になった場合、最も古くに格納された監査記録へ上書きを行い、監査記録の失敗時には SecureTicket Core サーバのコンソールに出力するとしているので、FAU_STG.4 で規定する内容を過不足なく具体化している。

以上により、F.AUDIT を実装することで FAU_STG.4 を実現できる。

FCS_CKM.1

FCS_CKM.1 では、AES の暗号鍵が、指定された暗号鍵生成アルゴリズムと指定された暗号鍵長で生成されることを要求している。

F.MNG.FILEIO では、２５６ビットの AES 暗号鍵を 『SecureTicket Core 暗号運用標準』の 『SecureTicket Core 共通鍵生成アルゴリズム』に従って生成するので、FCS_CKM.1 の内容を過不足なく実現している。

以上により、F.MNG.FILEIO を実装することで FCS_CKM.1 を実現できる。

FCS_COP.1

F.IA.AUTH では、SHA-256 で生成したバイナリのハッシュ値をワンタイムパスワードに用い、認証成功後、SHA-256 で生成したバイナリのハッシュ値をセッション ID として生成する。

F.MNG.FILEIO では、『リスト 6-6 F.MNG.FILEIO の読み込むファイル』、『リスト 6-7 基本設定ファイルに含まれるデータ』『リスト 6-9 パスワード精査設定ファイルに含まれるデータ』を AES 暗号アルゴリズム、OFB モードで復号し、『リスト 6-14 F.MNG.FILEIO の書き込むファイル』を AES 暗号アルゴリズム、OFB モードで暗号化して書き込んでいる。

F.MNG.ADMIN では AES 暗号アルゴリズム、OFB モードで通信内容を暗号化・復号化している。

これらは、FCS_COP.1 の内容を過不足なく実現している。

以上により、F.IA.AUTH、F.MNG.FILEIO、F.MNG.ADMIN を実装することで FCS_COP.1 を実現できる。

FDP_ACC.1

F.REVPROXY は、リバースプロキシ受付プロセスとして、公開保護 URL との間でアクセス制御を行う。

これは、FDP_ACC.1 で規定するリバースプロキシ SFP を実施した内容となっている。

以上により、F.REVPROXY を実装することで FDP_ACC.1 を実現できる。

FDP_ACF.1

F.REVPROXY は、リバースプロキシ受付プロセスとして、公開保護 URL との間で、アクセス時点でそれぞれに有効なグループ ID を基にしてアクセス制御を行う。このアクセス制御は、公開保護 URL のセキュリティ属性として、許可である場合、拒否である場合、許可・拒否属性が無い場合の３つのケースに分けて記述してある。これらの記述は、FDP_ACF.1 の『表 5-2 リバースプロキシ SFP アクセス規則』の記述内容と一致している。すなわち、これは、FDP_ACF.1 で規定する内容を実現している。

以上により、F.REVPROXY を実装することで FDP_ACF.1 を実現できる。

FIA_AFL.1

F.IA.AUTH では、認証に失敗した場合、TOE は認証エラー回数を更新し、これが、規定値（連続失敗認証検出回数）を超えた場合は、当該利用者のアカウントをロックするとしている。これは、FIA_AFL.1 で規定する内容を過不足なく具体化している。

以上により、F.IA.AUTH を実装することで FIA_AFL.1 を実現できる。

FIA_ATD.1

F.REVPROXY では、TOE は認証に成功した許可利用者ごとに利用者属性としてユーザ ID およびグループ ID を維持している。これは、FIA_ATD.1 で規定する内容を過不足なく具体化している。

以上により、F.REVPROXY を実装することで FIA_ATD.1 を実現できる。

FIA_SOS.1

F.MNG.ADMIN、F.MNG.CLNT では、管理者およびパスワードを所有する一般利用者に、『リスト 6-17 パスワードに対する条件』を満たすパスワードを登録、変更する機能を実装している。

このリストは、『リスト 5-4 パスワードの品質尺度』を過不足なく満たしている。

以上により、F.MNG.ADMIN、F.MNG.CLNT を実装することで FIA_SOS.1 を実現できる。

FIA_SOS.2

F.IA.AUTH は、クライアントモジュールで、バイナリのハッシュ値を生成し、それをもとに『リスト 6-1 クライアントモジュールのワンタイムパスワードの仕様』に変換したものをワンタイムパスワードにし、検査時は『リスト 6-3 サーバモジュールでのワンタイムパスワードの仕様』とするよう定めている。

これは、『リスト 5-5 ワンタイムパスワードの品質尺度』を満たすワンタイムパスワードであり、FIA_SOS.2 で規定する内容を具体化している。

以上により、F.IA.AUTH を実装することで FIA_SOS.2 を実現できる。

FIA_UAU.2

F.IA.AUTH では、一般利用者が保護対象資産である公開保護 URL にアクセスする前に、管理者や一般利用者が管理機能にアクセスする前に、TOE が許可利用者として認証していることを確認している。

これは、FIA_UAU.2 で規定する内容を過不足なく具体化している。

以上により、F.IA.AUTH を実装することで FIA_UAU.2 を実現できる。

FIA_UAU.4

F.IA.AUTH では、チケットデータとパスワードを使ってワンタイムパスワードを生成するが、一回の認証ごとに、チケットの値を現在とは違う値に更新している。

これは、FIA_UAU.4 で規定する内容を具体化している。

以上により、F.IA.AUTH を実装することで FIA_UAU.4 を実現できる。

FIA_UAU.5

F.IA.AUTH では、一般利用者が公開保護 URL、パスワード変更機能およびチケット発行機能にアクセスするとき、管理者が管理機能にアクセスするとき、それぞれの場合の認証において、ワンタイムパスワードメカニズムまたはパスワードメカニズムのどちらの認証メカニズムが使用されているかが規定されている。

これは、FIA_UAU.5 で規定する内容を具体化している。

以上により、F.IA.AUTH を実装することで FIA_UAU.5 を実現できる。

FIA_UAU.6

F.REVPROXY では、一般利用者が公開保護 URL にアクセスするとき、セッション有効期限が切れていたら、再認証を要求している。

F.MNG.ADMIN では、管理者が管理機能にアクセスするとき、セッション有効期限が切れていたら、再認証を要求している。

F.MNG.CLNT では、一般利用者が管理機能にアクセスするとき、セッション有効期限が切れていたら、再認証を要求している。

これらは、FIA_UAU.6 で規定する内容を具体化している。

以上により、F.REVPROXY、F.MNG.ADMIN、F.MNG.CLNT を実装することで FIA_UAU.6 を実現できる。

FIA_UAU.7

F.IA.AUTH では、パスワードのエコーバックには、文字数分の‘*’を表示させ、パスワードの漏洩を防いでいる。これは、FIA_UAU.7 で規定する内容を過不足なく具体化している。

以上により、F.IA.AUTH を実装することで FIA_UAU.7 を実現できる。

FIA_UID.2

F.IA.AUTH では、一般利用者が保護対象資産である公開保護 URL にアクセスする前に、管理者や一般利用者が管理機能にアクセスする前に、TOE が本人を識別している。

これは、FIA_UID.2 で規定する内容を過不足なく具体化している。

以上により、F.IA.AUTH を実装することで FIA_UID.2 を実現できる。

FIA_USB.1

F.REVPROXY では、TOE は認証に成功した許可利用者を代行するサブジェクトに利用者属性としてユーザ ID およびグループ ID を関連づける。これは、FIA_USB.1 で規定する内容を過不足なく具体化している。

以上により、F.REVPROXY を実装することで FIA_USB.1 を実現できる。

FMT_MOF.1

F.MNG.ADMIN では TOE － 保護サーバ間 通信保護機能 の有効/無効設定、一般利用者認証をパスワードとチケットを併用した認証とするかチケットのみの認証とするかの指定、パスワードの品質尺度を８～１２８バイトとするか１～１２８バイトとするかの指定、監査事象出力レベルの１～５の範囲での改変を管理者のみに制限している。

これは、FMT_MOF.1 で要求している内容である。

以上により、F.MNG.ADMIN を実装することで FMT_MOF.1 を実現できる。

監査事象の出力レベルを１～５の範囲で改変する

FMT_MSA.1

F.MNG.ADMIN では、公開保護 URL に対するセキュリティ属性（グループ名、許可・拒否属性、グループ有効開始日時、グループ有効期限）の操作（問い合わせ、登録、削除）を管理者に制限している。

これは、FMT_MSA.1 で要求している内容を実現したものになっている。

以上により、F.MNG.ADMIN を実装することで FMT_MSA.1 を実現できる。

FMT_MSA.2

F.MNG.FILEIO では、暗号鍵に係るセキュリティ属性（特定の文字列からなるシード）として、セキュリティ方針モデルに記載された品質基準に従ってセキュアな値のみ受け入れている。

これは FMT_MSA.2 で規定される内容を実現している。

以上により、F.MNG.FILEIO を実装することで FMT_MSA.2 を実現できる。

FMT_MSA.3

F.MNG.ADMIN では、一般利用者を作成したとき、デフォルトではグループは登録されていない。このため、サブジェクトのセキュリティ属性としてグループが存在しない。オブジェクトを生成するとき、公開保護 URL は、グループも、許可・拒否属性も設定せずに生成できる。このことから、サブジェクトはオブジェクトにアクセスできるため、許可的である。F.MNG.ADMIN は、デフォルト値に対して、FMT_MSA.1 の登録操作で代替の初期値を管理者が設定できるので、FMT_MSA.3.2 の要求を満たしている。

これは、FMT_MSA.3 で規定される内容を実現している。

以上により、F.MNG.ADMIN を実装することで FMT_MSA.3 を実現できる。

FMT_MTD.1[1]

F.MNG.ADMIN では、一般利用者の一覧取得、問い合わせ、登録、削除、グループの一覧取得、問い合わせ、登録、削除、グループに属するユーザの問い合わせ、登録、削除を行う機能を管理者のみに提供している。

これは、FMT_MTD.1[1]を実現したものになっている。

以上により、F.MNG.ADMIN を実装することで FMT_MTD.1[1]を実現できる。

FMT_MTD.1[2]

F.MNG.ADMIN では、一般利用者のパスワードの変更、登録を行う機能を管理者のみに提供している。

これは、FMT_MTD.1[2]を実現したものになっている。

以上により、F.MNG.ADMIN を実装することで FMT_MTD.1[2]を実現できる。

FMT_MTD.1[3]

F.MNG.CLNT では、一般利用者自身のパスワードの変更を、パスワードとチケットデータで識別・認証された一般利用者のみに提供している。

これは、FMT_MTD.1[3]を実現したのになっている。

以上により、F.MNG.CLNT を実装することで FMT_MTD.1[3]を実現できる。

FMT_MTD.1[4]

F.MNG.ADMIN では、一般利用者のチケットを発行する機能を管理者に提供している。

これは、FMT_MTD.1[4]を実現したものになっている。

以上により、F.MNG.ADMIN を実装することで FMT_MTD.1[4]を実現できる。

FMT_MTD.1[5]

F.MNG.CLNT では、ユーザ名とパスワードで識別・認証された一般利用者に対して、本人のチケット発行許可フラグが「発行可能」であるときに限り、本人のチケットを発行し、直ちにチケット発行許可フラグを「発行禁止」とする機能を提供している。

これは、FMT_MTD.1[5]を実現したものになっている。

以上により、F.MNG.CLNT を実装することで FMT_MTD.1[5]を実現できる。

FMT_MTD.1[6]

F.MNG.ADMIN では、使用禁止ワードの問い合わせ、変更、削除、登録を行う機能を管理者のみに提供している。

これは、FMT_MTD.1[6]を実現したものになっている。
以上により、F.MNG.ADMIN を実装することで FMT_MTD.1[6]を実現できる。

FMT_MTD.1[7]
F.MNG.ADMIN では、一般利用者のチケット発行許可フラグを「発行可能」または「発行禁止」とし、一般利用者本人に本人のチケットを発行することを許可／禁止する管理機能を管理者のみに提供している。
これは、FMT_MTD.1[7]を実現したものになっている。
以上により、F.MNG.ADMIN を実装することで FMT_MTD.1[7]を実現できる。

FMT_MTD.1[8]
F.MNG.ADMIN では、パスワードの有効期限、Ticket 認証許可時間帯、Ticket 認証有効開始日時、Ticket 認証有効期限を登録、変更、削除する管理機能を管理者のみに提供している。
これは、FMT_MTD.1[8]を実現したものになっている。
以上により、F.MNG.ADMIN を実装することで FMT_MTD.1[8]を実現できる。

FMT_MTD.1[9]
F.MNG.ADMIN では、一般利用者のアカウントロックを解除する管理機能を管理者のみに提供している。
これは、FMT_MTD.1[9]を実現したものになっている。
以上により、F.MNG.ADMIN を実装することで FMT_MTD.1[9]を実現できる。

FMT_MTD.1[10]
F.MNG.ADMIN では、連続失敗認証検出回数の問い合わせ、変更、登録する管理機能を管理者のみに提供している。
これは、FMT_MTD.1[10]を実現したものになっている。
以上により、F.MNG.ADMIN を実装することで FMT_MTD.1[10]を実現できる。

FMT_MTD.1[11]
F.MNG.ADMIN では、認証の有効時間の問い合わせ、改変する管理機能を管理者のみに提供している。
これは、FMT_MTD.1[11]を実現したものになっている。
以上により、F.MNG.ADMIN を実装することで FMT_MTD.1[11]を実現できる。

FMT_SMF.1
F.MNG.ADMIN では『リスト 6-15 管理者に提供される管理機能 その１』『リスト 6-16 管

理者に提供される管理機能 その２』に記述されるセキュリティ機能を管理する。

F.MNG.CLNT では『リスト 6-19 認証された一般利用者に提供される機能』に記述されるセキュリティ機能を管理する。

これは、FMT_SMF.1 で規定する内容を実現している。

以上により、F.MNG.ADMIN および F.MNG.CLNT を実装することで FMT_SMF.1 を実現できる。

FMT_SMR.1[1]

F.MNG.ADMIN では管理者役割を維持している。これは、FMT_SMR.1[1]で規定する内容を実現している。

以上により、F.MNG.ADMIN を実装することで FMT_SMR.1[1]を実現できる。

FMT_SMR.1[2]

F.MNG.CLNT ではユーザ名、パスワード、チケットを所有する一般利用者を維持している。これは、FMT_SMR.1[2]で規定する内容を実現している。

以上により、F.MNG.CLNT を実装することで FMT_SMR.1[2]を実現できる。

FPT_RVM.1

F.REVPROXY では、公開保護 URL に対するアクセスがあると、F.IA.AUTH によって、識別・認証を行い、一般利用者を代行するプロセスを割り当てる。

管理機能 F.MNG.ADMIN に対するアクセスがあると、F.IA.AUTH によって、識別・認証を行い、管理者を代行するプロセスを割り当てる。

一般利用者の管理機能 F.MNG.CLNT に対するアクセスがあると、F.IA.AUTH によって、識別・認証を行い、一般利用者を代行するプロセスを割り当てる。

F.TOESVRPRT は F.REVPROXY が保護サーバに通信を行うとき、必ず呼び出される。

F.AUDIT は、サーバモジュールが起動・再起動されるとき、必ず呼び出され、上記プロセスが動作中に監査事象が発生したとき、必ず呼び出される。

F.MNG.FILEIO はサーバモジュールが起動・再起動されるとき、必ず呼び出される。

これは、FPT_RVM.1 で規定する内容を実現している。

以上により、F.IA.AUTH、F.REVPROXY、F.TOESVRPRT、F.AUDIT、F.MNG.FILEIO、F.MNG.ADMIN、F.MNG.CLNT を実装することで FPT_RVM.1 を実現できる。

FTA_TSE.1[1]

F.IA.AUTH は、一般利用者の認証時に、パスワード有効期限が過ぎていないことを確認し、過ぎている場合は、パスワード変更を要求し、パスワード変更しない場合はセッションを拒否する。

これは、FTA_TSE.1[1]で規定する内容を実現している。

以上により、F.IA.AUTH を実装することで FTA_TSE.1[1]を実現できる。

FTA_TSE.1[2]

F.IA.AUTH は、一般利用者の認証時に、認証日時が、Ticket 認証許可時間帯であり、Ticket 認証有効開始日時以降であり、Ticket 認証有効期限より前であることを確認し、それらのひとつでも満たさない場合、セッションを拒否する。

これは、FTA_TSE.1[2]で規定する内容を実現している。

以上により、F.IA.AUTH を実装することで FTA_TSE.1[2]を実現できる。

FTP_ITC.1

F.TOESVRPRT は、SecureTicket Core サーバと保護サーバ間通信を管理者の設定に応じて SSL 通信によって保護する。

これは、FTP_ITC.1 で規定する内容を実現している。

以上により、F.TOESVRPRT を実装することで FTP_ITC.1 を実現できる。

FTP_TRP.1[1]

F.REVPROXY で、SSL プロトコルにてクライアントと SecureTicket Core サーバ間通信路を確立する。

これは、FTP_TRP.1[1]で規定する内容を実現している。

以上により、F.REVPROXY を実装することで FTP_TRP.1[1]を実現できる。

FTP_TRP.1[2]

F.MNG.ADMIN では、独自通信プロトコルにて通信路を確立する。独自通信プロトコルは、平文にチェックサムを加えた上で AES 暗号アルゴリズムを用いて OFB モードで暗号化し、復号時、AES 暗号アルゴリズムを用いて OFB モードで復号しチェックサムを確認しており、チェックサムエラーの検出時は通信内容が再送され、情報改竄を防ぐことができる。すなわち、情報漏洩や改竄の発生しない通信路となっている。

これは、FTP_TRP.1[2]で規定する内容を実現している。

以上により、F.MNG.ADMIN を実装することで FTP_TRP.1[2]を実現できる。

8.3.2. セキュリティ機能強度根拠

『5.3 TOE 最小機能強度』では、TOE セキュリティ機能要件に対して最小機能強度は SOF-基本を主張している。

『6.2 セキュリティ機能強度』では、パスワードメカニズムおよび、ワンタイムパスワードメカニズムに対し SOF-基本のセキュリティ機能強度を主張している。

よって、主張するセキュリティ機能強度は一貫している。

8.3.3.保証手段根拠

『6.3 保証手段』において、EAL3＋ADV_SPM.1 で必要とするすべての TOE セキュリティ保証要件に対して、保証手段を対応付けている。また、保証手段に示すドキュメントによって、本 ST が規定した TOE セキュリティ保証要件が要求する証拠を網羅している。

それは、次のとおりである。

1. ACM_CAP.3 許可の管理

保証手段：

文書管理方針と手順、
SecureTicket Core 構成管理計画書、
SecureTicket Core ソースコード管理手順書

内容：

構成要素を一意に識別し、また利用者がTOE のどの段階のものを使用しているかを知ることができることを保証するための手段、手続きを規定している。

2. ACM_SCP.1 TOE の CM 範囲

保証手段：

SecureTicket Core 文書一覧、
SecureTicket Core ソースコード一覧

内容：

TOEの構成管理下に置かれている構成要素リストを明示的に規定している。

3. ADO_DEL.1 配付手続き

保証手段：

SecureTicket Core 配付手順書

内容：

TOE のセキュリティ維持のため、TOE が開発元から利用者までの配付に関し、使用される手段、手続きについて規定している。

4. ADO_IGS.1 設置、生成、及び立上げ手順

保証手段：

SecureTicket Core ユーザーズガイド 導入編、
SecureTicket Core ユーザーズガイド セキュリティ編

内容：

購入者が行うTOE の設置手段、手続きについて規定している。

5. ADV_FSP.1 非形式的機能仕様

保証手段：

SecureTicket Core 機能仕様書・上位レベル設計書
SecureTicket Core 機能仕様書別冊
SecureTicket Core 暗号運用標準書

内容：

TSF のふるまいと、利用者から見えるインタフェースについて規定している。

6. ADV_HLD.2 セキュリティ実施上位レベル設計

保証手段：

SecureTicket Core 機能仕様書・上位レベル設計書
SecureTicket Core 機能仕様書別冊
SecureTicket Core 暗号運用標準書

内容：

TOE 機能要件の実装に適したアーキテクチャを、TOE が提供することの保証を、TOE の主要な構成単位（サブシステム）及びこれらの単位をこれらが提供する機能と関係付ける観点から規定している。

7. ADV_RCR.1 非形式的対応の実証

保証手段：

SecureTicket Core 表現対応書

内容：

TOE 要約仕様、機能仕様、上位レベル設計の対応について規定している。

8. ADV_SPM.1 非形式的な TOE セキュリティ方針モデル

保証手段：

SecureTicket Core セキュリティ方針モデル仕様書

内容：

機能仕様、セキュリティ方針モデルとTSP の方針の間の対応を規定し、またセキュアな値だけがセキュリティ属性として受け入れられることの保証を提供している。

9. AGD_ADM.1 管理者ガイダンス

保証手段：

SecureTicket Core ユーザーズガイド 導入編、
SecureTicket Core ユーザーズガイド 応用編、
SecureTicket Core ユーザーズガイド セキュリティ編、
SecureTicket Core ユーザーズガイド プログラム編

内容：

TOE の管理者に対し、TOE を正しい方法で保守し管理することを目的として書かれた資料（取扱説明書）である。

10. AGD_USR.1 利用者ガイダンス

保証手段：

SecureTicket Core ユーザーズガイド 一般利用者編、
SecureTicket Core ユーザーズガイド セキュリティ編

内容：

TOE 利用者に対し、TOE をセキュアに使用してもらうことを目的とした資料（取扱説明書）である。

11. ALC_DVS.1 セキュリティ手段の識別

保証手段：

セキュリティ規定書

内容：

TOE の開発環境で使用されている物理的、手続き的、人的セキュリティ手段を規定している。

12. ATE_COV.2 カバレージの分析

保証手段：

SecureTicket Core テスト網羅率分析書

内容：

機能テスト仕様書記述のテストにおいて、TSF が機能仕様通りに動作することを実証するに十分であることを記述したものである。

13. ATE_DPT.1 テスト:上位レベル設計

保証手段：

SecureTicket Core テスト深さ分析書

内容：

機能テスト仕様書記述のテストにおいて、TSF が上位レベル設計書通りに動作することを実証するに十分であることを記述したものである。

14. ATE_FUN.1 機能テスト

保証手段：

SecureTicket Core 機能テスト計画書
SecureTicket Core 機能テスト手順書
SecureTicket Core 機能テスト結果報告書

内容：

全てのセキュリティ機能の実行が、仕様通りであることを実証するテストについて記述したものである。

15. ATE_IND.2 独立テスト - サンプル

保証手段：

TOE

内容：

テストに適したTOE。

16. AVA_MSU.1 ガイダンスの検査

保証手段：

SecureTicket Core ユーザーズガイド 一般利用者編、
SecureTicket Core ユーザーズガイド 導入編、
SecureTicket Core ユーザーズガイド 応用編、
SecureTicket Core ユーザーズガイド セキュリティ編、
SecureTicket Core ユーザーズガイド プログラム編

内容：

TOE の管理者に対するTOE を正しい方法での保守管理方法と、TOE 利用者に対するTOE のセキュアな使用について書かれた資料（取扱説明書）である。

17. AVA_SOF.1 TOE セキュリティ機能強度評価

保証手段：

SecureTicket Core 機能強度分析書

内容：

確率的順列的メカニズムに対する機能強度分析を実施したものである。

18. AVA_VLA.1 脆弱性分析

保証手段：

SecureTicket Core 脆弱性分析書

内容：

TOE の明白なセキュリティ脆弱性の存在と、TOE の意図する環境においてそれらが悪用され得ないことの分析を実施したものである。

したがって、EAL3＋ADV_SPM.1 における TOE セキュリティ保証要件を実現できる。

8.3.4.PP 主張根拠

本 ST が準拠する PP はない。