# 認　証　報　告　書

独立行政法人 情報処理推進機構
理事長　藤原　武平太　原紙押印済

評価対象

| | |
|---|---|
| **申請受付年月日(受付番号)** | **平成17年9月20日（IT認証5062）** |
| **認証番号** | C0091 |
| **認証申請者** | **横河電機株式会社** |
| **TOEの名称** | SecureTicket Core |
| **TOEのバージョン** | 5.0.0.0.0 |
| **PP適合** | **なし** |
| **適合する保証要件** | EAL3 + ADV_SPM.1 |
| **TOE開発者** | **横河電機株式会社** |
| **評価機関の名称** | **社団法人　電子情報技術産業協会　ITセキュリティセンター** |

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成19年4月27日

独立行政法人 情報処理推進機構
セキュリティセンター 情報セキュリティ認証室
技術管理者　田渕　治樹

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

① Common Criteria for Information Technology Security Evaluation Version 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0407

**評価結果：合格**

「SecureTicket Core 5.0.0.0.0」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証手続規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

# 目次

1 全体要約 ..... 1
1.1 はじめに ..... 1
1.2 評価製品 ..... 1
1.2.1 製品名称 ..... 1
1.2.2 製品概要 ..... 1
1.2.3 TOEの範囲と動作概要 ..... 1
1.2.4 TOEの機能 ..... 4
1.3 評価の実施 ..... 7
1.4 評価の認証 ..... 7
1.5 報告概要 ..... 8
1.5.1 PP適合 ..... 8
1.5.2 EAL ..... 8
1.5.3 セキュリティ機能強度 ..... 8
1.5.4 セキュリティ機能 ..... 8
1.5.5 脅威 ..... 9
1.5.6 組織のセキュリティ方針 ..... 10
1.5.7 構成条件 ..... 11
1.5.8 操作環境の前提条件 ..... 12
1.5.9 製品添付ドキュメント ..... 13
2 評価機関による評価実施及び結果 ..... 14
2.1 評価方法 ..... 14
2.2 評価実施概要 ..... 14
2.3 製品テスト ..... 14
2.3.1 開発者テスト ..... 14
2.3.2 評価者テスト ..... 16
2.4 評価結果 ..... 18
3 認証実施 ..... 19
4 結論 ..... 19
4.1 認証結果 ..... 19
4.2 注意事項 ..... 26
5 用語 ..... 27
6 参照 ..... 31

# 1 全体要約

## 1.1 はじめに

この認証報告書は、「SecureTicket Core 5.0.0.0.0」（以下「本TOE」という。）について社団法人　電子情報技術産業協会　ITセキュリティセンター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である横河電機株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

## 1.2 評価製品

### 1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

| | |
|---|---|
| 名称: | SecureTicket Core |
| バージョン: | 5.0.0.0.0 |
| 開発者: | 横河電機株式会社 |

### 1.2.2 製品概要

本製品は、Webサーバの代理としてWebクライアントからの要求を受け付け、WebクライアントとWebサーバ間のHTTP通信を中継するリバースプロキシソフトウェア製品である。

本製品は、WebクライアントとWebサーバ間に設置される中継サーバ上で動作するサーバモジュール、Webクライアント上で動作するクライアントモジュール、SecureTicket Core管理用のツールに組み込まれるライブラリから構成されており、これらが連携して、利用者の識別認証、Webサーバに格納された保護すべき情報へのアクセス制御、ファイルや通信データの暗号化などを行うことにより、保護すべき情報を漏洩や不正アクセスなどから保護する。

### 1.2.3 TOEの範囲と動作概要

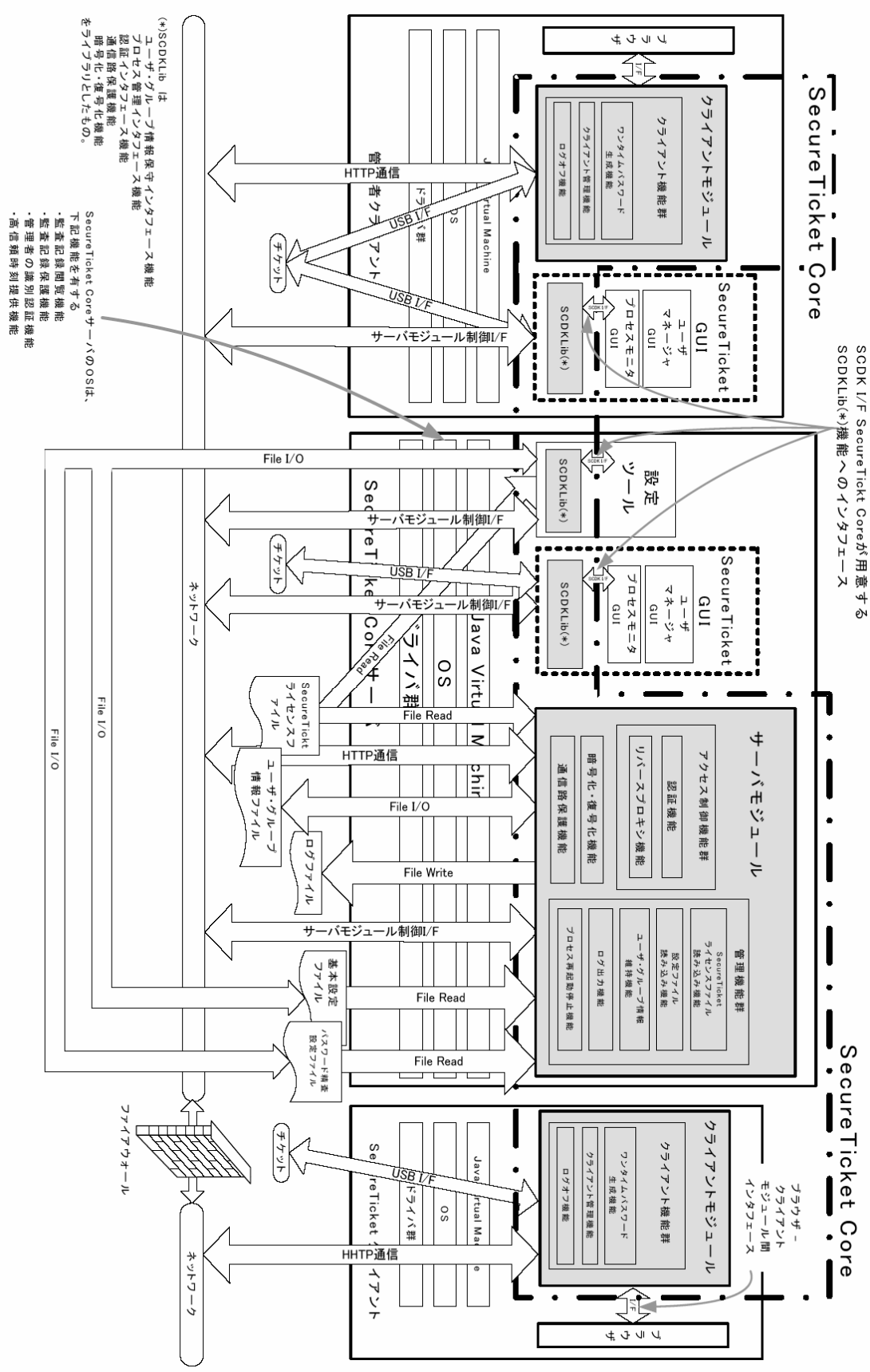


**図**1-1　SecureTicket Core **構成図**

TOEは、中継サーバ（以下「SecureTicket Coreサーバ」という。）上で動作するサーバモジュールと、Webクライアント（以下「SecureTicketクライアント」という。）上で動作するクライアントモジュールと、SecureTicket CoreサーバまたはSecureTicket Core管理用クライアント（以下「管理者クライアント」という。）上で動作する管理用ツール（設定ツール、SecureTicket GUI）に組み込まれるライブラリ（以下「SCDKLib」という。）から構成される（図1-1参照）。

サーバモジュールはSecureTicket Coreサーバ上にJavaアプリケーションとしてインストールされ、SCDKLibはSecureTicket Coreサーバ及び管理者クライアントにJava共有ライブラリとしてインストールされる。一方、クライアントモジュールは、Webクライアント上のブラウザからサーバモジュールにアクセスすることによりJavaアプレットとして読み込まれる。

各部分の主要な動作を以下に示す。なお、各部分が提供する機能のより詳細な説明は「1.2.4 TOEの機能」を参照のこと。

(1) サーバモジュール

保護したい情報を格納するWebサーバ（以下「保護サーバ」という。）の代理として、保護サーバ上のURLを代替する公開用URLを提供し、Webクライアントからのリクエストを受け付けて保護サーバとのHTTP通信を中継する。このとき、あらかじめ登録されたURLにアクセスできる利用者を制限する。（アクセス制御機能群(図1-1)）

また、一般利用者によるクライアントモジュールからの認証情報（パスワード、チケットデータ）の変更・発行要求や管理者による設定ツール・SecureTicket GUIからの各種のTOE管理用の要求を受け付けて、TOEの動作に反映させる。（管理機能群(図1-1)）

さらに上記の各処理に伴うネットワーク経由の情報の送受信ではSSLプロトコルまたは独自通信プロトコルによる通信を行い、ハードディスク上のファイルの読み書きでは暗号化・復号を行う。（通信路保護機能、暗号化・復号化機能(図1-1)）

(2) クライアントモジュール

一般利用者から認証情報（パスワード、チケットデータ）を受け付け、これらの認証情報からワンタイムパスワードを生成した後、サーバモジュールに送信する。また、一般利用者からの認証情報（パスワード、チケットデータ）の変更・発行要求をサーバモジュールに送信する。（クライアント機能群(図1-1)）

(3) SCDKLib

管理者から受け付けた認証情報（チケットデータ）をサーバモジュールに送信する。サーバモジュールでの認証成功後、設定ツール・SecureTicket GUIのユーザインタフェースを介して管理者から受け付けた各種のTOE管理用の要求をサーバモジュールに送信する。

これらの処理に伴うサーバモジュールとの情報の送受信では独自通信プロトコルによる通信を行う。（SCDKLib(図1-1)）

### 1.2.4 TOEの機能

TOEは、サーバモジュール、クライアントモジュール、及びSCDKLibから構成される（図1-1参照）。各部分が提供する機能の概要を以下に示す。なお、TOE固有の用語の説明は「5 用語」を参照のこと。

(1) サーバモジュール

大別すると、以下のアクセス制御機能群、管理機能群、通信路保護機能、暗号化・復号化機能を提供する。

(a) アクセス制御機能群

SecureTicketクライアントからのHTTPリクエストを受け付けて利用者のアクセス権限を吟味した上で保護サーバとのHTTP通信を中継するリバースプロキシ機能と利用者の本人確認のための認証機能を提供する。

・リバースプロキシ機能

SecureTicketクライアントから公開保護URLの取得要求を受け付けると、許可された利用者のみにそのURLの情報を送信するように、クライアントモジュールと保護サーバとの間のHTTP通信を中継する。SecureTicketクライアント及び保護サーバとの送受信は、下記(c)の通信路保護機能を使用した通信を行う。

・認証機能

SecureTicketクライアントから公開保護URLまたはパスワード変更用/チケット発行用のURLの取得要求を受け付けると、当該URLに基づくコンテンツ情報の送信またはパスワード変更/チケット更新を実行する前に一般利用者の識別認証を行う。さらに、最初の認証後にアクセスを続けている一般利用者を所定のタイミングで再認証する。また、設定ツール・SecureTicket GUIからの各種のTOE管理の要求を受け付ける前に管理者の識別認証を行う。これらのために行われるSecureTicketクライアント、設定ツール・SecureTicket GUIとの送受信には、下記(c)の通信路保護機能を使用した通信を行う。

(b) 管理機能群

TOEの管理・運用に必要な以下の5つの機能を提供する。

なお、設定ツール・SecureTicket GUIからの各種のTOE管理の要求に対しては、情報の送受信は下記(c)の通信路保護機能を使用した通信を行い、各種要求に伴うハードディスク上の各種設定ファイルへのアクセスは下記(d)の暗号化・復号化機能を使用した書き込み・読み取りを行う。

・SecureTicketライセンスファイル読み込み機能

サーバモジュールの起動時に、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取り、ライセンスの妥当性を判定する。

・基本設定ファイル読み込み機能
サーバモジュールの起動時に、基本設定ファイルを読み取る。
・ユーザ・グループ情報維持機能
サーバモジュールの起動時に、ユーザ・グループ情報ファイルを読み取る。
また、SecureTicket GUI（下記(3)SCDKLib(a)のユーザ・グループ情報保守インタフェース機能）を使用して要求されたユーザ・グループ情報ファイルの変更要求を受け付けて、その変更内容をユーザ・グループ情報ファイルに書き込む。
・ログ出力機能
サーバモジュールの監査証跡をログファイルに出力する。
・プロセス再起動停止機能
SecureTicket GUI（下記(3)SCDKLib(a)のプロセス管理インタフェース機能）を使用して要求された停止・再起動要求を受け付けて、サーバモジュールプロセスの停止と再起動を行う。

(c) 通信路保護機能

SecureTicketクライアント上のSSL機能を備えたブラウザとの間、及び保護サーバとの間でSSLプロトコルによる通信を行う。

また、SCDKLibを呼び出すことにより、設定ツール・SecureTicket GUIとの間で独自通信プロトコルによる通信を行う。

(d) 暗号化・復号化機能

SCDKLibを呼び出すことにより、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の書き込みと読み取りを行うときにファイル内容の暗号化と復号を行う。

(2) クライアントモジュール

サーバモジュールと連携して以下の機能を提供する。

なお、下記の機能に必要なクライアントモジュールは、SecureTicketクライアントのブラウザからサーバモジュールが提供する所定のURLへアクセスがあったときにダウンロードされる。

(a) ワンタイムパスワード生成機能

公開保護URLまたはパスワード変更用のURLの取得要求をサーバモジュールが受け取ると、当該機能を含むクライアントモジュールが要求元のSecureTicketクライアントにダウンロードされる。

このクライアントモジュールが、一般利用者から認証情報（パスワード、チケットデータ）を受け付け、これらをもとにワンタイムパスワードを生成し、サーバモジュールに送信する。ワンタイムパスワードメカニズムの認証に成功した場合、チケットデータを更新する。

(b) クライアント管理機能

パスワード変更用のURLまたはチケット発行用のURLの取得要求をサーバモジュールが受け取ると、当該機能を含むクライアントモジュールが要求元のSecureTicketクライアントにダウンロードされる。

パスワード変更の場合、ワンタイムパスワード生成機能による認証成功後に、サーバモジュールの応答に従って一般利用者から入力された新パスワードをサーバモジュールに送信する。

チケット発行の場合、一般利用者から受け付けたユーザ名とパスワードをサーバモジュールに送信し、ユーザ名・パスワードメカニズムの認証に成功した場合、サーバモジュールの応答に従ってチケットデータを作成し、チケットに格納する。

(c) ログオフ機能

ログアウト用のURLの取得要求をサーバモジュールが受け取ると、当該機能を含むクライアントモジュールが要求元のSecureTicketクライアントにダウンロードされる。

このクライアントモジュールが、サーバモジュールとのセッションを明示的に切断する（セッションIDを廃棄する）ためのログアウト要求をサーバモジュールに送信する。

(3) SCDKLib

設定ツール、SecureTicket GUI、及びサーバモジュールから呼び出される共有ライブラリであり、以下の機能を提供する。

(a) インタフェース機能

設定ツール及びSecureTicket GUIに対して、サーバモジュールの機能を利用するための以下のインタフェースを提供する。

- 認証インタフェース機能
  サーバモジュールと連携して管理者を識別認証するためのAPIを提供する。
- ユーザ・グループ情報保守インタフェース機能
  サーバモジュールを介してユーザ・グループ情報ファイルを読み書きするためのAPIを提供する。
- プロセス管理インタフェース機能
  サーバモジュールのプロセスを管理するためのAPIを提供する。

(b) 通信路保護機能

設定ツール・SecureTicket GUIとサーバモジュールとの間で独自通信プロトコルによる通信を行うための機能を提供する。この機能は、上記(a)のインタフェース機能及びサーバモジュールから呼び出される。

(c) 暗号化・復号化機能

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の書き込みと読み取りを行うときにファイル

内容の暗号化と復号を行う機能と暗号化・復号機能付きのファイル書き込み・読み取りAPIを提供する。この機能は、サーバモジュール及び設定ツールが各ファイルにアクセスするときに呼び出される。

## 1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証手続規程」[3]、「評価機関承認手続規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。

(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。

(3) 本TOEがセキュリティ設計に基づいて開発されていること。

(4) 上記(1)、(2)、(3)を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「SecureTicket Core セキュリティターゲット」（以下「ST」という。）[1]及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11][14]のいずれか) 附属書C、CCパート2（[6][9][12][15]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13][16]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「横河電機株式会社 SecureTicket Core 評価報告書」（以下「評価報告書」という。）[22]に示されている。なお、評価方法は、CEMパート2（[17][18][19]のいずれか）に準拠する。また、CC及びCEMの各パートは補足（[20][21]のいずれか）の内容を含む。

## 1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成19年3月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

## 1.5 報告概要

### 1.5.1 PP適合

適合するPPはない。

### 1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL3追加である。

追加されるコンポーネントはADV_SPM.1である。

### 1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、高度な専門知識を持たず公開インタフェースのみを悪用する低レベルの攻撃能力を備えた脅威エージェントを想定している。よって、SOF-基本で十分である。

### 1.5.4 セキュリティ機能

本TOEのセキュリティ機能は以下のとおりである。なお、各機能の詳細についてはST[1]を参照のこと。

(1) 識別認証機能

SecureTicketクライアントからサーバモジュールが提供する公開保護URLへのアクセス時、SecureTicketクライアントからサーバモジュールが提供する一般利用者向けのパスワード変更用/チケット発行用のURLへのアクセス時、または、設定ツール・SecureTicket GUIを使用したサーバモジュールへのアクセス時に、アクセスしてきた利用者を識別認証する。

このときに使用する認証メカニズムは、認証対象とアクセス目的に応じて、ワンタイムパスワードメカニズムとユーザ名・パスワードメカニズムを切り替える。また、管理者によって設定された認証の有効時間を越えてアクセスする認証済み利用者に対して再認証を行う。

(2) アクセス制御機能

SecureTicketクライアントからサーバモジュールが提供する公開保護URLへのアクセスに対して、管理者によってあらかじめ登録されたアクセスルールに従ったアクセス制御を行う。

また、SecureTicketクライアントとSecureTicket Coreサーバ上のサーバモジュール間、及びSecureTicket Coreサーバ上のサーバモジュールと保護サーバ間で行う通信をSSLプロトコルにより保護する。

(3)　監査機能

TOEの利用・運用に伴うセキュリティ機能の動作に関連する所定の事象を記録する。

(4)　管理機能

設定ツール・SecureTicket GUIのSCDKLib(1.2.4節(3)参照)を介してTOE管理機能を提供し、その機能の使用を管理者のみに制限する。このときのSCDKLibとサーバモジュールとの間の情報の送受信を独自通信プロトコルにより保護する。

また、一般利用者のパスワード変更とチケット発行の各機能を提供し、その機能の使用を当該一般利用者のみに制限する。

さらに､これらの機能を使用してTSFデータやセキュリティ属性を各種設定ファイルに書き込む場合とサーバモジュールの起動時にTSFデータやセキュリティ属性をそのファイルから読み取る場合に、その内容の暗号化・復号を行う。

### 1.5.5　脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

**表1-1　想定する脅威**

| 識別子 | 脅　威 |
|---|---|
| T.IllAccess | 実体保護URLへの不許可アクセス<br>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<br>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<br>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<br><br>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<br><br>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<br><br>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<br><br>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。 |

### 1.5.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表1-2に示す。

**表1-2　組織のセキュリティ方針**

| 識別子 | 組織のセキュリティ方針 |
|---|---|
| P.UsrCrtTckt | 一般利用者のチケット発行<br>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<br>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。 |

### 1.5.7　構成条件

評価された構成のTOEは、セキュリティ強化モードに設定された状態であり、その動作環境が以下のハードウェア／ソフトウェアで構成されている。

**表1-3　SecureTicket Core サーバの構成**

| ソフトウェア | |
|---|---|
| OS | Windows 2003 Server SP1 以降、または<br>Red Hat Enterprise Linux ES v.4 以降 |
| JVM | JRE 5.0 Update 7 以降 |
| ハードウェア | |
| CPU | Pentium 500 MHz 以上、または<br>Celeron 500 MHz 以上 |
| メモリ | 512 MB 以上 |
| HDD | 10 GB 以上 |
| 周辺機器 | CD-ROMドライブ |

**表1-4　SecureTicket クライアントの構成**

| ソフトウェア | |
|---|---|
| OS | Windows 2000 SP2 以降、または<br>Windows XP |

| | |
|---|---|
| JVM | Sun Java Plug-in 5.0 Update 7 以降、または<br>Microsoft VM 5.0 Release 5.0.0.3810 以降 |
| ブラウザ | IE 5.5 以降、または<br>Firefox 1.5.0.7 以降（この場合のJVMは、Sun Java Plug-in 5.0 Update 7 以降のみ） |
| ハードウェア | |
| 周辺機器 / インタフェース | USBトークン(製品名: ePass1000) / USBポート |

**表1-5　管理者クライアントの構成**

| | |
|---|---|
| ソフトウェア | |
| OS | Windows 2000 または<br>Windows XP |
| JVM | Sun Java Plug-in 5.0 Update 7 以降 |
| ハードウェア | |
| 周辺機器 / インタフェース | USBトークン(製品名: ePass1000) / USBポート |

### 1.5.8　操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-6に示す。

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

**表1-6　TOE使用の前提条件**

| 識別子 | 前提条件 |
|---|---|
| A.TOENetPos | TOEのネットワーク設置条件<br>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<br>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<br>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<br>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<br><br>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。 |

### 1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

- SecureTicket Core ユーザーズガイド 一般利用者編（BA-SM-0001）Rev7
- SecureTicket Core ユーザーズガイド 導入編（BA-SM-0002）Rev11
- SecureTicket Core ユーザーズガイド 応用編（BA-SM-0003）Rev12
- SecureTicket Core ユーザーズガイド セキュリティ編(BA-SM-0004)Rev9
- SecureTicket Core ユーザーズガイド プログラム編[1]（BA-SM-0005）Rev4

[1] このドキュメントの配付には秘密保持契約が必要になります。

# 2 評価機関による評価実施及び結果

## 2.1 評価方法

評価は、CCパート3の保証要件について、CEMパート2に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMパート2のワークユニットごとに評価した内容及び判断が記載されている。

## 2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成17年10月に始まり、平成19年3月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成18年11月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用・ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成18年11月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

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

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

## 2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

### 2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を図2-1に示す。

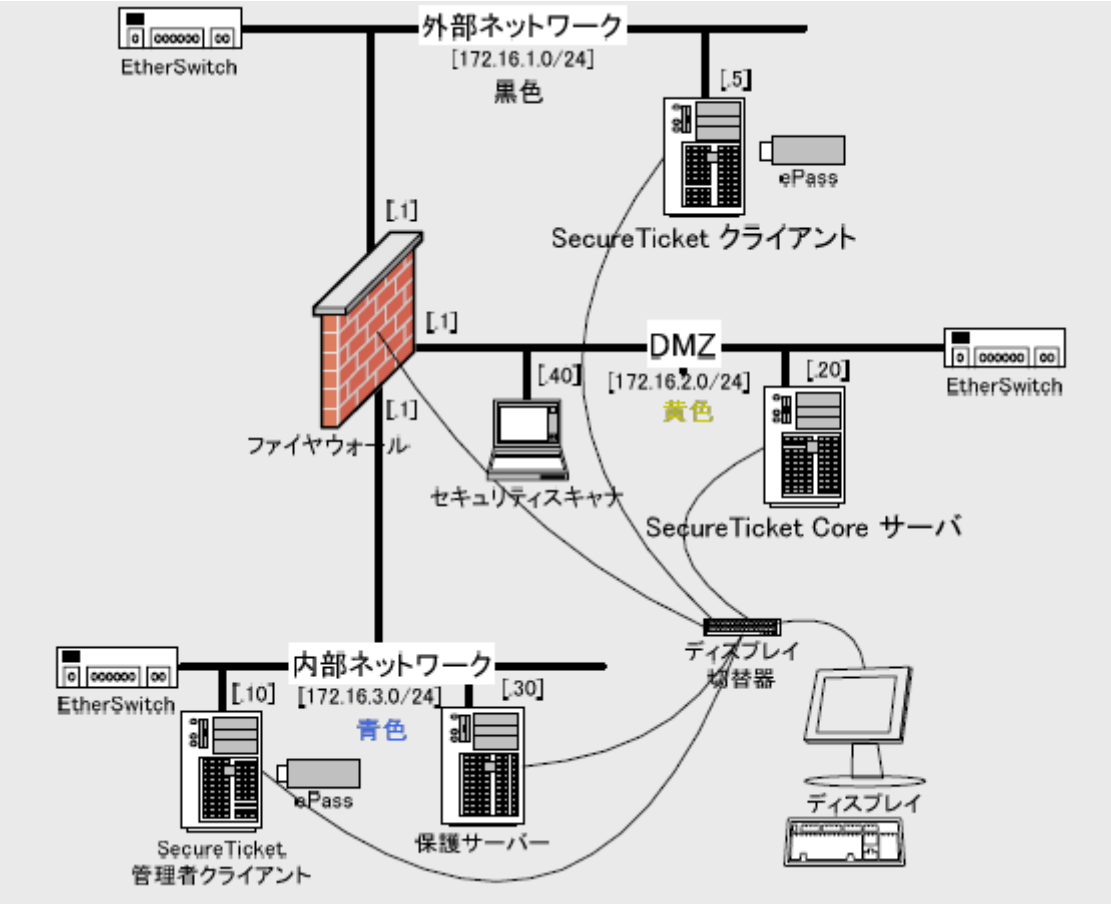


**図2-1　開発者テストの構成図**

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を図2-1に示す。開発者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。なお、STに識別されていない装置（セキュリティスキャナ、ディスプレイ、ディスプレイ切替器）が追加されているが、これらは特定のテスト時のみ使用するテストツールとテスト結果観察用の装置であり、セキュリティ機能のふるまいに影響しないため、テスト結果には影響しない。

b.テスト手法

テストには、以下の手法が使用された。

①SecureTicket クライアント上のブラウザを操作することにより、セキュリティ機能の外部インタフェースを刺激する。

②管理者クライアント上のSecureTicket GUIまたはSecureTicket Coreサーバ上の設定ツールを操作することにより、セキュリティ機能の外部インタフェースを刺激する。

③上記①②に伴うディスプレイやログファイルへの出力内容を観察すること

により、セキュリティ機能のふるまいを確認する。

④上記①②に伴うネットワーク上の通信内容や各種設定ファイルへの出力内容をツールを使用して観察することにより、セキュリティ機能のふるまいを確認する。

c.実施テストの範囲

テストは開発者によって175項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証されている。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

### 2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成である。

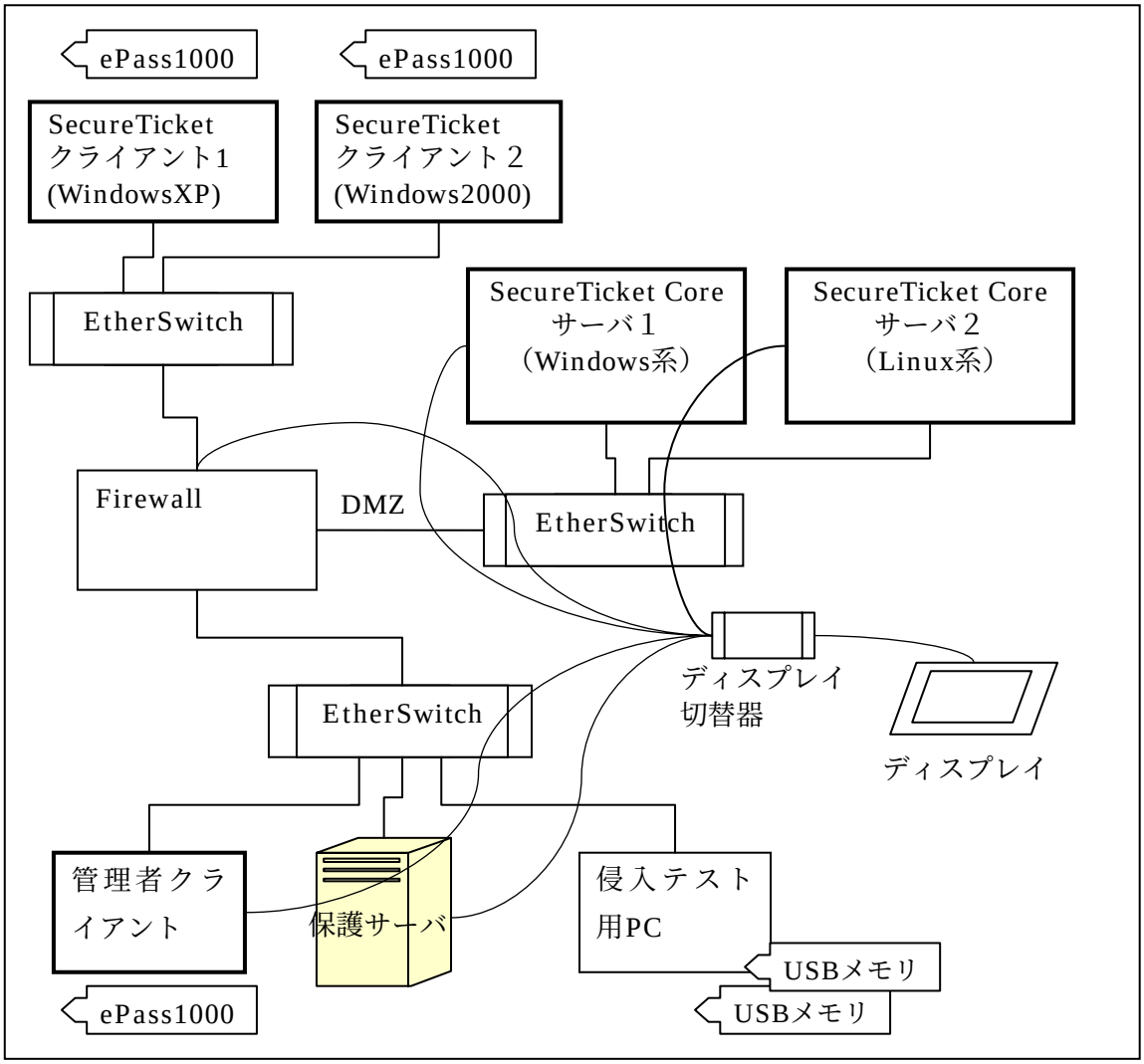


**図2-2　評価者テストの構成図**

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を図2-2に示す。評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

①SecureTicket クライアント上のブラウザを操作することにより、セキュリティ機能の外部インタフェースを刺激する。

②管理者クライアント上のSecureTicket GUIまたはSecureTicket Coreサーバ上の設定ツールを操作することにより、セキュリティ機能の外部インタフェースを刺激する。

③上記①②に伴うディスプレイやログファイルへの出力内容を観察することにより、セキュリティ機能のふるまいを確認する。
④上記①②に伴うネットワーク上の通信内容や各種設定ファイルへの出力内容をツールを使用して観察することにより、セキュリティ機能のふるまいを確認する。

c.実施テストの範囲

評価者は、独自に考案したテストを15項目、開発者テストのサンプリングによるテストを41項目、侵入テストを9項目、計65項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

【独自に考案した独立テスト】
① すべてのセキュリティ機能をテスト対象にすること
② セキュリティ機能のふるまいに影響を与えるパラメータで、開発者テストに含まれていないパラメータを指定したテスト
③ セキュリティ機能に対するパラメータの境界条件を考慮したテスト
④ 機能仕様から想定できる積極的、消極的なテスト
⑤ 機能強度の対象となるセキュリティ機能の品質尺度のテスト

【開発者テストのサンプリングによるテスト】
① 開発者テスト項目数の20%以上を確保すること
② すべてのセキュリティ機能を網羅すること

【侵入テスト】
①　識別認証機能の迂回・無効化の脆弱性の確認
②　不要ポートの悪用可能性の確認

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

## 2.4　評価結果

評価報告書をもって、評価者は本TOEがCEMパート2のワークユニットすべてを満たしていると判断した。

# 3 認証実施

評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。

② 当該所見報告書でなされた指摘内容が正しく反映されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

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

認証機関は、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

# 4 結論

## 4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL3+ADV_SPM.1保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

**表4-1 評価者アクションエレメント検証結果**

| 評価者アクションエレメント | 検証結果 |
|---|---|
| **セキュリティターゲット評価** | **適切な評価が実施された。** |
| ASE_DES.1.1E | 評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_DES.1.2E | 評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫性していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |

| | |
|---|---|
| ASE_DES.1.3E | 評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_ENV.1.1E | 評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_ENV.1.2E | 評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_INT.1.1E | 評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_INT.1.2E | 評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_INT.1.3E | 評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_OBJ.1.1E | 評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_OBJ.1.2E | 評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_PPC.1.1E | 評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。 |

| | |
|---|---|
| ASE_PPC.1.2E | 評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。 |
| ASE_REQ.1.1E | 評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_REQ.1.2E | 評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_SRE.1.1E | 評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。 |
| ASE_SRE.1.2E | 評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。 |
| ASE_TSS.1.1E | 評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_TSS.1.2E | 評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| **構成管理** | **適切な評価が実施された** |
| ACM_CAP.3.1E | 評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |

| | |
|---|---|
| ACM_SCP.1.1E | 評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。 |
| **配付と運用** | **適切な評価が実施された** |
| ADO_DEL.1.1E | 評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ADO_DEL.1.2D | 評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。 |
| ADO_IGS.1.1E | 評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。 |
| ADO_IGS.1.2E | 評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| **開発** | **適切な評価が実施された** |
| ADV_FSP.1.1E | 評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ADV_FSP.1.2E | 評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |

| | |
|---|---|
| ADV_HLD.2.1E | 評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのソフトウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ADV_HLD.2.2E | 評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。 |
| ADV_RCR.1.1E | 評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ADV_SPM.1.1E | 評価はワークユニットに沿って行われ、セキュリティ方針モデルが非形式的でありSTにおいて明示的方針をもつこと、ST中のセキュリティ機能要件で表されたすべてのセキュリティ方針がモデル化されていること、セキュリティ方針モデルの規則や特性がモデル化されたTOEのセキュリティふるまいを明確に表していること、モデル化されたふるまいがセキュリティ方針と一貫し完全であること、セキュリティ方針を実装している機能仕様にてすべてのセキュリティ機能を識別していること、機能仕様の内容とセキュリティ方針モデルの実装として識別された機能の内容が一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| **ガイダンス文書** | **適切な評価が実施された** |
| AGD_ADM.1.1E | 評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |

| | |
|---|---|
| AGD_USR.1.1E | 評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| **ライフサイクルサポート** | **適切な評価が実施された** |
| ALC_DVS.1.1E | 評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ALC_DVS.1.2E | 評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| **テスト** | **適切な評価が実施された** |
| ATE_COV.2.1E | 評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ATE_DPT.1.1E | 評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |

| | |
|---|---|
| ATE_FUN.1.1E | 評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ATE_IND.2.1E | 評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。 |
| ATE_IND.2.2E | 評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。 |
| ATE_IND.2.3E | 評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| **脆弱性評定** | **適切な評価が実施された** |
| AVA_MSU.1.1E | 評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| AVA_MSU.1.2E | 評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。 |

| | |
|---|---|
| AVA_MSU.1.3E | 評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| AVA_SOF.1.1E | 評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| AVA_SOF.1.2E | 評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しことを確認している。 |
| AVA_VLA.1.1E | 評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| AVA_VLA.1.2E | 評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |

## 4.2 注意事項

特になし。

# 5 用語

本報告書で使用された略語を以下に示す。

| | |
|---|---|
| API | Application Program Interface |
| CC | Common Criteria for Information Technology Security Evaluation |
| CEM | Common Methodology for Information Technology Security Evaluation |
| DMZ | Demilitarized Zone |
| EAL | Evaluation Assurance Level |
| HTTP | HyperText Transfer Protocol |
| JVM | Java Virtual Machine |
| PP | Protection Profile |
| SOF | Strength of Function |
| SSL | Secure Socket Layer |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |
| USB | Universal Serial Bus |

本報告書で使用された用語を以下に示す。

| | |
|---|---|
| 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。 |
| SCDKLib | SecureTicket Core Developers'Kit Library。設定ツール及びSecureTicket GUIに組み込んで使用するライブラリ。 |
| SecureTicket | 本TOEを組み込んだエンドユーザ向け製品の名称。 |
| SecureTicket Core | SecureTicketの基本機能部分であり、本TOE のこと。 |
| SecureTicket Core サーバ | サーバモジュールを動作させるサーバ。 |

| | |
|---|---|
| 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。 |
| 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。許可利用者用に発行されたチケットを装着している。 |
| SecureTicketライセンスファイル | 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。 |
| USBトークン | USBデバイスの一種で、一般に暗号処理を行うICチップを搭載している。ただし、メモリ(EEPROMなど)のみを搭載したものもUSBトークンと呼ぶことがある。 |
| 外部ネットワーク | 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。 |
| 管理者クライアント | 管理者がSecureTicket GUI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。 |
| 基本設定ファイル | リンク設定情報などを格納したファイル。 |
| クライアントモジュール | 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。 |
| グループ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。 |
| グループ名 | 一般利用者の所属するグループの名前。 |
| グループ情報 | 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。 |
| 公開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。 |
| 公開保護URL | TOEが保護する公開URL。 |
| サーバモジュール | SecureTicket Coreサーバで動作するTOEのJavaアプリケーション。 |
| サーバモジュール制御 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。 |
| 実体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に関係付けられる。 |
| 実体保護URL | TOEが保護する実体URL。公開保護URLと関係付けられる。 |
| セキュリティ強化モード | 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。 |
| セッション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。 |
| 設定ツール | 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。 |
| チケット | 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。 |
| チケットデータ | 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。 |
| 独自通信プロトコル | SecureTicket Coreで用いられる独自の通信プロトコル。 |
| 内部ネットワーク | 組織内のネットワーク |
| 認証情報 | 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。 |
| 認証の有効時間 | 発行されたセッションIDが有効である期間（秒数）。セッション有効期限(認証成功日時または最後に保護対象資産にアクセスした日時に認証の有効時間を加えた日時)を決定するために使用される。 |
| パスワード精査設定ファイル | 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。 |
| プロセスモニタGUI | SecureTicket GUI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。 |
| 保護サーバ | TOEの保護対象資産が格納されるサーバ。 |
| ユーザ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。 |
| ユーザ情報 | 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。 |
| ユーザマネージャGUI | SecureTicket GUIのうち、ユーザ・グループ情報を保守するためのGUI。 |
| ユーザ名 | 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。 |
| ユーザ・グループ情報 | 上記のユーザ情報とグループ情報の総称。 |
| ユーザ・グループ情報ファイル | ユーザ情報、グループ情報を格納したファイルの総称。 |
| リンク設定情報 | 公開URLと実体URLとを対応づけるためのリンク情報及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。 |

# 6 参照


[1] SecureTicket Core セキュリティターゲット Rev21（2007年3月14日）
横河電機株式会社

[2] ITセキュリティ評価及び認証制度の基本規程　平成17年7月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成17年7月　独立行政法人 情報処理推進機構　EC-03

[4] 評価機関承認手続規程　平成17年7月　独立行政法人 情報処理推進機構　EC-05

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン2.1 1999年8月 CCIMB-99-031

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 バージョン2.1 1999年8月 CCIMB-99-032

[10] 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 バージョン2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

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

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

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

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論

バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0407

[21] 補足-0210 第2版、補足-0407

[22] 横河電機株式会社 SecureTicket Core 評価報告書 第5.6版 2007年3月14日
社団法人　電子情報技術産業協会　ITセキュリティセンター