証明書検証サーバ

(Certificate Validation Server)

セキュリティターゲット

2007/11/1

Version 1.09

株式会社 日立製作所

「証明書検証サーバ (Certificate Validation Server) **セキュリティターゲット」**

－ 変更歴 －

変更番号	作成／変更年月日	バージョン	更新理由	作成者	承認者
1	2006/4/27	0.930	新規作成	佐藤 油利 古屋	古屋
2	2007/5/8	0.940	「認証局から取得した証明書/失効リスト」を保護対象資産として追加するための変更を反映	佐藤 油利	古屋
3	2007/5/15	0.950	Solaris 版 TOE 及び Linux 版 TOE を同一 ST で記述するための変更を反映	佐藤 油利	古屋
4	2007/5/23	0.960	ASE 所見報告書 (所見報告書番号: ASE001-01) のご指摘を反映	佐藤 油利	古屋
5	2007/6/4	0.965	IT 環境として HSM を追加するための変更を反映	佐藤 油利	古屋
6	2007/6/11	0.970	ASE 所見報告書 (所見報告書番号: ASE002-01) のご指摘を反映	油利	古屋
7	2007/6/12	0.975	「TOE の範囲・境界に関わる論理的構成要素」について詳細を追記	油利	古屋
8	2007/6/14	0.980	SSL クライアント秘密鍵の生成について詳細を追記	佐藤 油利	古屋
9	2007/6/15	0.990	論理構成要素を示す図に「CVS マシンの操作端末」を追加	油利	古屋
10	2007/6/19	0.995	ASE 所見報告書 (所見報告書番号: ASE003-01) のご指摘を反映	油利	古屋
11	2007/6/25	1.00	CVS 操作員認証に SSL クライアント認証を利用する場合について改訂	油利	古屋
			ASE 所見報告書(所見報告書番号: ASE004-01) のご指摘を反映	油利 佐藤 古屋	古屋
			ベーシック認証時のユーザ ID・パスワードの認証機能を IT 環境のセキュリティ要件として記述	佐藤	古屋
12	2007/7/2	1.01	全体の一環性に関わる修正及びエディトリアルな修正	佐藤 油利	古屋
13	2007/7/11	1.02	ベーシック認証機能を TOE のセキュリティ機能から除外	油利	古屋
			セキュリティ管理機能に関する記述の一貫性に関わる修正およびエディトリアルな修正		
14	2007/7/11	1.03	監査機能に関するエディトリアルな修正	油利	古屋
15	2007/8/21	1.04	ASE 所見報告書(所見報告書番号: ASE006-01) のご指摘を反映	古屋	古屋
			エディトリアルな修正		
16	2007/9/3	1.05	所見報告書 (所見報告書番号: ADV002-01) のご指摘を反映	佐藤 古屋	古屋
			エディトリアルな修正		
17	2007/9/4	1.06	エディトリアルな修正	古屋	古屋

18	2007/9/7	1.07	**エディトリアルな修正**	**佐藤**	**古屋**
19	2007/9/18	1.08	**エディトリアルな修正**	**古屋**	**古屋**
20	2007/11/1	1.09	ASE **所見報告書(所見報告書番号**: ASE007-01) **のご指摘を反映**	**佐藤**	**古屋**
			エディトリアルな修正		

＜商標類＞

Ethernet は、米国 Xerox Corp.の商品名称です。

PC/AT は、米国 International Business Machines Corp.の商品名称です。

RedHat (R)は米国その他の国で RedHat, Inc.の登録商標もしくは商標です。

Sun Solaris は、米国 Sun microsystems,Inc. の米国及びその他の国における登録商標です。

Microsoft は、米国及びその他の国における米国 Microsoft Corp.の登録商標です。

Windows は、米国及びその他の国における米国 Microsoft Corp.の登録商標です。

Microsoft Internet Explorer は、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。

nCipher netHSM は、nCipher Corporation Limited. の登録商標です。

SafeNet Luna SA は、SafeNet, Inc. の登録商標です。

＜著作権＞

「証明書検証サーバ (Certificate Validation Server) **セキュリティターゲット」**

－ 目次 －

－ 図 目次 －

－ 表 目次 －

1 ST 概説

1.1 ST 識別

1.1.1 ST 識別情報

名称:	証明書検証サーバ (Certificate Validation Server) セキュリティターゲット
バージョン:	Version 1.09
識別名:	CVS-ST-1.09
作成日:	2007 年 11 月 1 日
作成者:	株式会社 日立製作所
キーワード:	PKI、公開鍵基盤、証明書検証
CC のバージョン:	CC v2.3、補足-0512 適用

1.1.2 TOE 識別情報

名称:	証明書検証サーバ
バージョン:	03-00
作成者:	株式会社 日立製作所

※ なお、本 TOE は Linux 及び Solaris で動作する。

1.2 ST 概要

本 ST は、株式会社 日立製作所のソフトウェア製品「証明書検証サーバ (Certificate Validation Server、以降 CVS と略記)」が提供する機能について記述する。CVS は、国際標準 X.509 に準拠した証明書の検証を行うサーバ用のソフトウェア製品であり、一般利用者に対して以下のサービスを提供する。

- RFC3280 に記載の認証パス検証アルゴリズムに準拠した証明書の検証 (以降、認証パス検証と記す)
- RFC2560 に記載の OCSP に準拠した証明書の有効性検証 (以降、OCSP 有効性検証と記す)

CVS が想定する消費者は CVS を運用する組織である。CVS を運用する組織は上記 2 つのサービスのどちらか一方を一般利用者へ提供し、2 つの方式を同時には提供できない。上記のサービスを適用する上では、適切な権限を有した CVS 操作員による、適切な設定及び運用が重要となるが、そのために CVS は以下のセキュリティ機能を提供する。

- データ保護
- データ改ざんチェック
- 識別･認証機能

- CVS 操作員情報管理機能
- CVS 証明書管理機能
- 失効リスト取得機能
- 監査機能

1.3 CC 適合

- CC v2.3 パート 2 拡張
- CC v2.3 パート 3 適合
- EAL2 適合
- 適合する PP は存在しない

1.4 参考資料

(IPA 翻訳文書)

- 情報技術セキュリティ評価のためのコモンクライテリア バージョン 2.3
  パート 1: 概説と一般モデル［翻訳第 1.0 版］
  パート 2: セキュリティ機能要件［翻訳第 1.0 版］
  パート 3: セキュリティ保証要件［翻訳第 1.0 版］
- 補足-0512

1.5 用語及び略語

1.5.1 用語集

用語	説明
CVS 証明書	CVS の公開鍵の正当性を保証する。RFC3280 で定める X.509 形式の電子証明書である。
CVS 秘密鍵	CVS が証明書検証結果署名に用いる鍵。HSM で管理を行う。CVS 秘密鍵による署名は、CVS 証明書に記載された公開鍵で検証を行える。
CVS 操作員秘密鍵	CVS 操作員が管理し、SSL クライアント認証に使用する SSL クライアント証明書に対応した秘密鍵のこと。
CVS 操作員証明書	CVS 操作員が管理し、SSL クライアント認証に使用する SSL クライアント証明書のこと。
CVS 操作員証明書 ID	CVS 操作員証明書に記載してある SubjectDN のこと。
トラストアンカ証明書	検証依頼者が信頼する認証局の電子証明書のこと。
証明書検証結果署名	証明書検証結果に CVS が付与する署名のこと。
リポジトリ	認証局が発行した証明書及び失効リストを格納して公開するデータベース。

1.5.2 略語集

略語	正式名称	説明
C		
CVS	Certificate Validation Server	RFC3280 及び、RFC2560 に準拠した証明書の検証を行うサーバ製品。
D		
DMZ	DeMilitarized Zone	組織の内部ネットワークと外部のネットワーク（一般的にインターネット）の間に設置されている隔離されたネットワーク領域。
H		
HSM	Hardware Security Module	秘密鍵の生成、保管及び、暗号操作を行うハードウェア。
HTTP	Hypertext Transfer Protocol	Web サーバと Web ブラウザ間で HTML などのコンテンツをやり取りする際に使用するプロトコル。
HTTPS	Hypertext Transfer Protocol Security	HTTP に、SSL 等によるデータの暗号化機能を付加したプロトコル。
L		
LDAP	Lightweight Directory Access Protocol	ディレクトリサービスにアクセスするためのプロトコル。
O		
OCSP	Online Certificate Status Protocol	証明書の状態(失効していないかどうか)をオンラインで問い合わせるプロトコル。RFC 2560 として公開されている。
P		
PKI	Public Key Infrastructure	公開鍵暗号技術を利用したセキュリティ基盤。
R		
RFC	Request for Comments	IETF (Internet Engineering Task Force) による技術仕様の保存、公開形式のこと。
RFC2560	Request for Comments 2560	OCSP に関する技術仕様が記載された RFC のこ

		と。
RFC3280	Request for Comments 3280	公開鍵証明書と証明書失効リストのプロファイルが記載された RFC のこと。
S		
SSL	Secure Socket Layer	Web サーバと Web ブラウザ間の双方向認証とデータ暗号を行うプロトコル。
SubjectDN	Subject Distinguished Name	証明書内に記載される、その証明書の所有者の識別情報。
X		
X.509	X.509	ITU(国際電気通信連合)が定めた電子鍵証明書および証明書失効リスト(CRL)の標準仕様。

2 TOE 記述

2.1 TOE **種別**

TOE は、国際標準 X.509 に準拠した証明書の検証機能を提供する CVS というサーバ用のソフトウェア製品である。

2.2 TOE **概要**

CVS は、RFC3280 及び、RFC2560 に準拠した証明書の検証を行うサーバ用のソフトウェア製品である。

CVS が提供する証明書検証サービスには次の 2 つの方式がある。

- 認証パス検証
- OCSP 有効性検証

CVS が想定する消費者は CVS を運用する組織である。 CVS を運用する組織は上記 2 つのサービスのどちらか一方のみを一般利用者へ提供し、2 つの方式を同時には提供できない。

CVS は、Linux、Solaris の 2 種類のプラットフォームで動作するが、TOE 名称及び TOE バージョンは同一のものであり、したがって以後同一 ST(本 ST)で記述する。Linux、Solaris 間で共通の機能・コンポーネントに関しては本 ST 中でプラットフォームを区別せずに記述し、プラットフォーム間で差異がある場合に関してのみ Linux、Solaris のプラットフォームを区別して記述する。

2.2.1 認証パス検証

RFC 3280 に則った認証パスの構築と検証により、証明書の信頼性の検証を行うサービスを提供する。

認証パス検証の流れを図 1に示す。

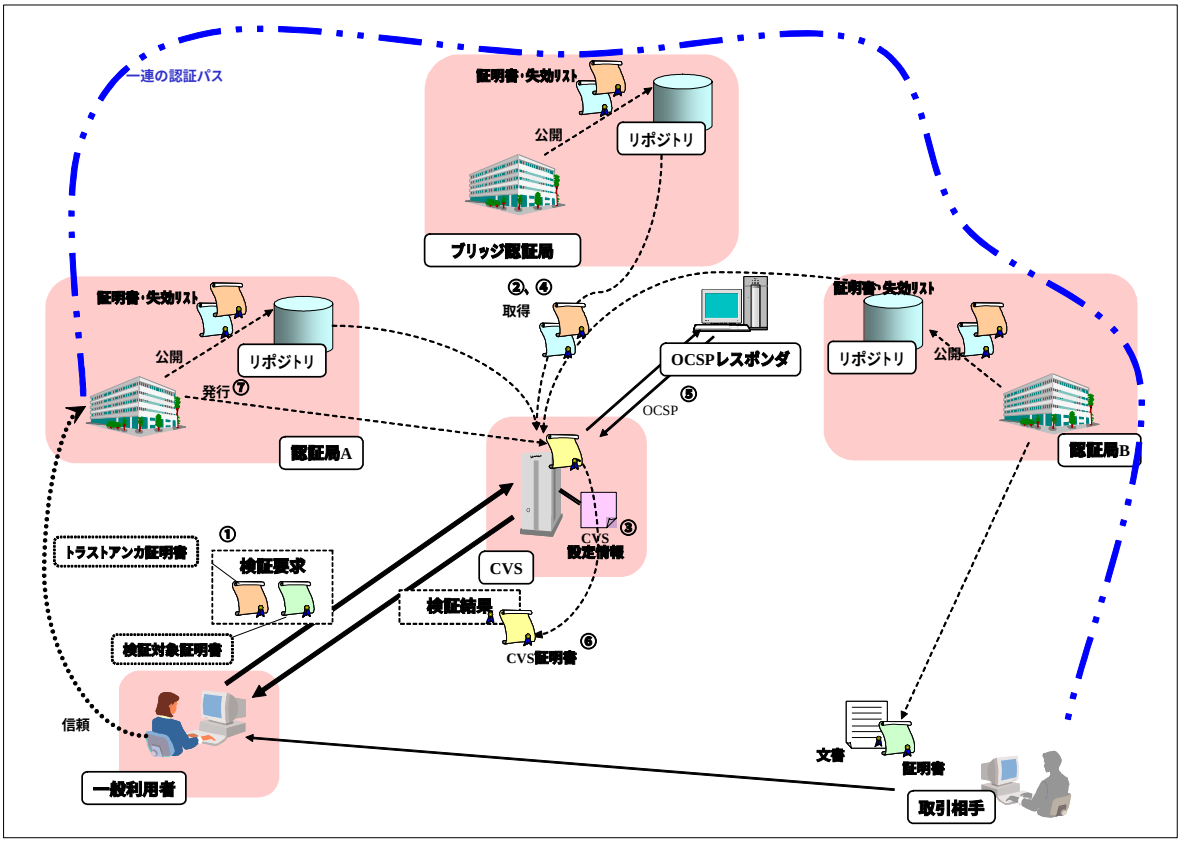

図 1 認証パス検証

(1) 証明書検証要求

一般利用者は、電子申請、電子取引等を行った際に、取引相手から受け取った証明書の検証を CVS に依頼する。この証明書検証要求には、以下の情報を含む（図 1 内､①)。

- 検証対象証明書
- トラストアンカ証明書

(2) 証明書検証

証明書検証要求を受けた CVS は、RFC3280 に則った認証パスの構築と検証を行う。認証パスとは、トラストアンカ証明書から、検証対象証明書までの一連の証明書の繋がりを指す。認証パスの構築において、CVS は、認証局が公開しているリポジトリに LDAP を用いてアクセスを行い、必要な証明書を取得する（図 1 内､②)。このとき、アクセスを行うリポジトリは、事前に CVS 操作員が登録した CVS 設定情報（図 1 内､③）に基づいて決定する。

認証パスの構築に成功した場合、構築した認証パスに対して、以下の項目を検証する。

- 認証パスを構成している証明書の署名の検証
- 認証パスを構成している証明書の有効期間の検証
- 認証パスを構成している証明書の制約事項の検証
- 認証パスを構成している証明書の有効性検証

認証パスの検証において、CVS は、認証局が公開しているリポジトリに、LDAP、HTTP または HTTPS を用いてアクセスし、有効性検証に必要な失効リストを取得する（図 1 内､④)。なお、このとき取得した失効リストについても署名の検証を実施する。また、有効性検証の対象となる証明書に、失効情報の取得先として OCSP レスポンダのロケーションが記載されている場合は、OCSP を用いて、この OCSP レスポンダへ問い合わせることで有効性検証を行う（図 1 内､⑤)。

(3) 証明書検証結果応答

CVS は、検証対象証明書の検証結果を、検証を依頼した一般利用者に返却する。証明書検証結果には CVS の秘密鍵を用いた署名(証明書検証結果署名)と、この署名を検証するために必要となる CVS 証明書を付与する（図 1 内､⑥)。CVS 証明書は、認証局から発行（図 1 内､⑦）され、CVS 操作員が CVS に登録する。CVS 証明書が証明書検証結果に付与されていることにより、検証を依頼した一般利用者は CVS の検証結果を信頼できる。証明書検証結果応答には、以下の情報を含む。

- 証明書検証結果
- 証明書検証結果署名
- CVS 証明書

2.2.2 OCSP 有効性検証

RFC 2560 に則った証明書の有効性の検証を行うサービスを提供する。

OCSP 有効性検証の流れを図 2に示す。

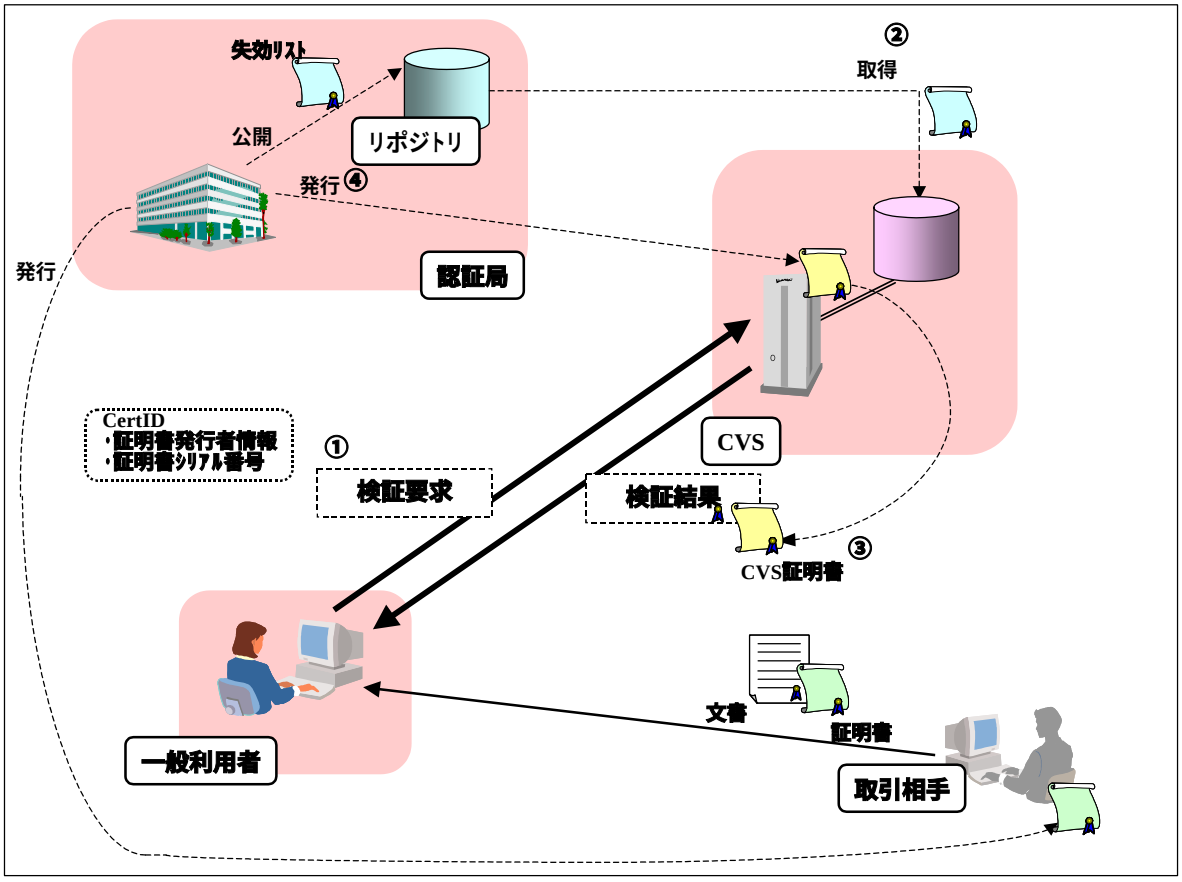

図 2 OCSP 有効性検証

(1) 証明書検証要求

一般利用者は、電子申請、電子取引等を行った際に、取引相手から受け取った証明書の検証を CVS に依頼する。この証明書検証要求には、検証対象証明書を一意に特定するための以下の情報を含む（図 2 内、①）。

- 証明書の発行者
- 証明書のシリアル番号

(2) 証明書検証

証明書検証要求を受けた CVS は、検証対象証明書の有効性検証を行う。有効性検証は、認証局が公開しているリポジトリから CVS 管理コマンドにより事前に取得した失効リスト

（図 2 内､②）の情報に基づく。

(3) 証明書検証結果応答

CVS は、検証対象証明書の検証結果を、検証を依頼した一般利用者に返却する。証明書検証結果には､CVS 操作員が生成した CVS の秘密鍵を用いた署名(証明書検証結果署名)と、この署名を検証するために必要となる CVS 証明書を付与する（図 2 内､③)。CVS 証明書は、認証局から発行（図 2 内､④）されており、CVS 操作員が CVS に登録する。検証対象証明書を発行した認証局が発行した CVS 証明書が付与されていることにより、検証を依頼した一般利用者は CVS の検証結果を信頼できる。

証明書検証結果応答には、以下の情報を含む。

- 証明書検証結果
- 証明書検証結果署名
- CVS 証明書

2.3 TOE 範囲

CVS を適用したシステムの基本構成を図 3に示す。

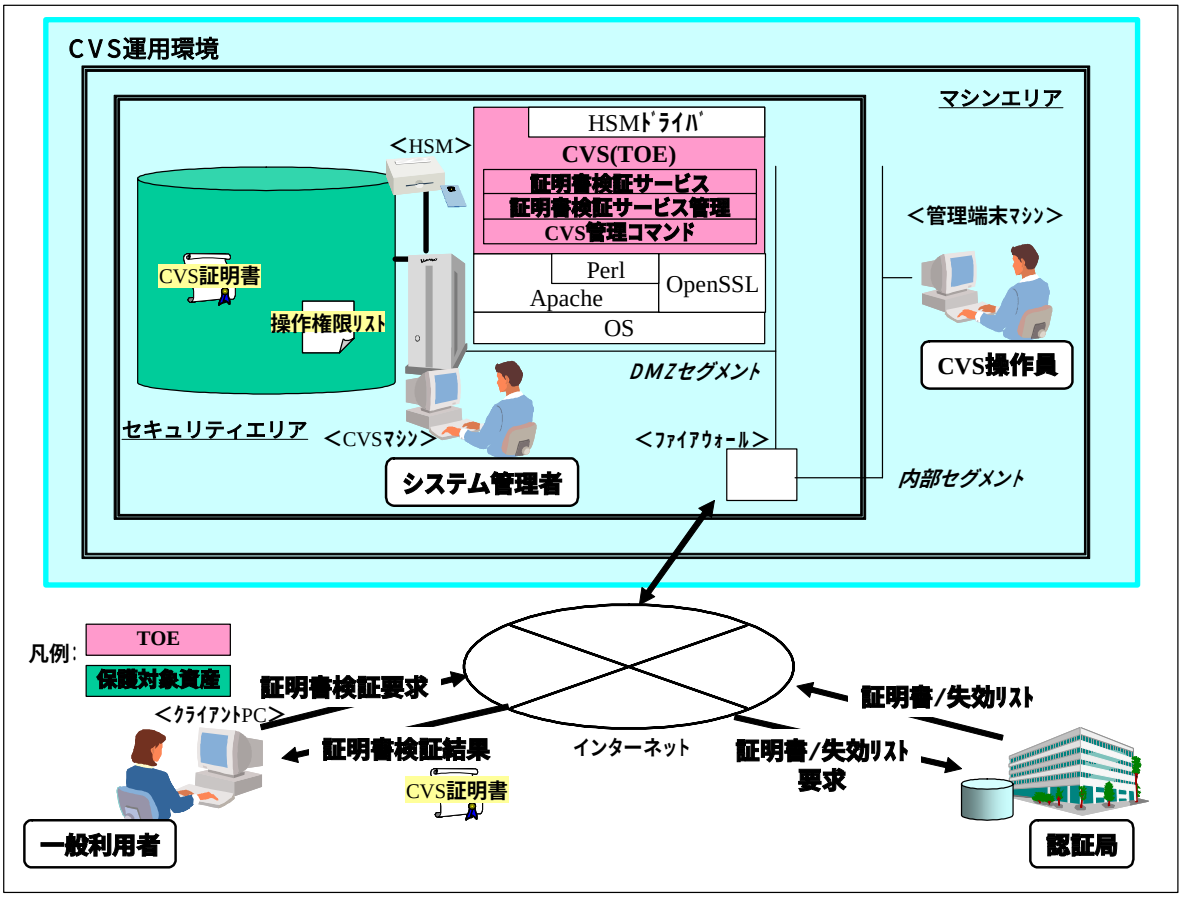

図 3 CVS を適用したシステム構成

図 3に示した CVS 運用環境を構成する論理エリア及び物理エリアについて以下に説明する。

(1) 論理エリア

① DMZ セグメント

CVS マシンが Ethernet を使用して接続する。内部セグメント及びインターネットとは、ファイアウォールを介して接続される。

② 内部セグメント

管理端末マシンが Ethernet を使用して接続する。DMZ セグメントとは、ファイアウォールを介して接続される。

(2) **物理エリア**

① セキュリティエリア

CVS マシン、HSM 及びファイアウォールが設置される。入退室管理が行われ、不正な物理的アクセスから保護されている。セキュリティエリアには、システム管理者のみ入室することができる。

② マシンエリア

CVS 運用環境内に設置されたマシン室であり、管理端末マシンが設置される。マシンエリアには、システム管理者、CVS 操作員及びその他の CVS を運用する組織に属する者が入室できる。

2.3.1 ハードウェア構成

図 3に示した環境で使用されるハードウェアの構成について以下に説明する。

IT 環境を構成するマシンの一覧を、Linux 版 CVS については表 1、Solaris 版 CVS については表 2に示す。

表 1 IT 環境を構成するマシンの一覧(Linux 版 CVS)

No	名称	ハードウェア仕様	備考
1	CVS マシン	Red Hat Enterprise Linux ES 4.0 (x86 版)	操作端末を持つ
		Web サーバとして Apache 2.0.58 以降が稼動するマシン	
		暗号ライブラリとして OpenSSL 0.9.7m 以降が稼動するマシン	
		インタプリタとして Perl 5 (jcode.pl v2.0 及び CGI.pm を含む)が稼動するマシン	
2	管理端末マシン	Web ブラウザとして Microsoft Internet Explorer 6.0 が稼働する Microsoft Windows XP が稼動するマシン	
3	HSM	下記のうち、いずれかの HSM 製品 nCipher netHSM (nCipher 社製 ハードウェア暗号装置) SafeNet Luna SA (SafeNet 社製 ハードウェア暗号装置)	
4	ファイアウォール	ファイアウォール製品が稼働するマシン	
5	クライアント PC	利用者側クライアントプログラムが稼動するマシン	

表 2 IT 環境を構成するマシンの一覧(Solaris 版 CVS)

No	名称	ハードウェア仕様	備考
1	CVS マシン	Sun Solaris 9 (SPARC 版)	操作端末を持つ
		Web サーバとして Apache 2.0.58 以降が稼動するマシン	
		暗号ライブラリとして OpenSSL 0.9.7m 以降が稼動するマシン	
		インタプリタとして Perl 5 (jcode.pl v2.0 及び CGI.pm を含む)が稼動するマシン	
2	管理端末マシン	Web ブラウザとして Microsoft Internet Explorer 6.0 が稼働する Microsoft Windows XP が稼動するマシン	
3	HSM	下記のうち、いずれかの HSM 製品 nCipher netHSM (nCipher 社製 ハードウェア暗号装置) SafeNet Luna SA (SafeNet 社製 ハードウェア暗号装置)	
4	ファイアウォール	ファイアウォール製品が稼働するマシン	
5	クライアント PC	利用者側クライアントプログラムが稼動するマシン	

表 1、表 2に示したマシンについて以下に説明する。

(1) CVS **マシン**

CVS が動作し、証明書検証サービスを提供する。また、システム管理者が CVS のインストール及び CVS に関する管理を行う際に使用する操作端末を持つ。

セキュリティエリア内に設置される。

証明書検証サービス用ポートと証明書検証サービス管理機能用ポートを持ち、CVS 運用環境のネットワークの DMZ セグメントに Ethernet を使用して接続される。

(2) **管理端末マシン**

CVS の管理を行うための端末として動作する。管理端末マシンは CVS 操作員によって利用され、CVS と通信することによって、CVS の設定や CVS 証明書の管理及び CVS 秘密鍵の生成・破棄の指示を行う。

CVS 運用環境のネットワークの内部セグメントに、Ethernet を使用して接続される。

(3) HSM

CVS 秘密鍵の生成と破棄及び暗号操作を行う。CVS 秘密鍵は HSM 内に格納されており、HSM 外に漏洩することはない。

セキュリティエリア内に設置される。

(4) **ファイアウォール**

CVS 運用環境のネットワークのインターネット、DMZ セグメント及び内部セグメントを論理的に分離する。

セキュリティエリア内に設置される。

(5) **クライアント** PC

一般利用者が証明書検証要求を送信する。また、利用者側クライアントプログラムを用いて CVS からの証明書検証結果応答の正当性の検証を行う。

2.3.2 ソフトウェア構成

図 3に示した CVS 運用環境で使用されるソフトウェアの構成について以下に説明する。

TOE 及び IT 環境で使用されるソフトウェアの一覧を、Linux 版 CVS については表 3、Solaris 版 CVS については表 4に示す。

表 3 TOE 及び IT 環境で使用されるソフトウェアの一覧(Linux 版 CVS)

No	搭載マシン	ソフトウェア種別	名称	TOE／TOE 外
1	CVS マシン	OS	Red Hat Enterprise Linux ES 4.0 (x86 版)	×
2		Web サーバ	Apache 2.0.58 以降	×
3		暗号ライブラリ	OpenSSL 0.9.7m 以降	×
4		インタプリタ	Perl 5 (jcode.pl v2.0 及び CGI.pm を含む)	×
5		証明書検証サーバ	証明書検証サーバ 03-00 (Linux 版)	○
6		HSM ドライバ［注 1］	nCipher Support Software for Linux 8.20 以降 Luna SA Security Software for Linux 2.2.1 以降	×
7	管理端末マシン	Web ブラウザ	Microsoft Internet Explorer 6.0	×
		OS	Microsoft Windows XP	×
8	クライアント PC	プログラム	利用者側クライアントプログラム	×

凡例:○…TOE、×…TOE 外

［注 1］CVS マシンに接続する HSM 製品に適合するものを選択して使用する。

表 4 TOE 及び IT 環境で使用されるソフトウェアの一覧(Solaris 版 CVS)

No	搭載マシン	ソフトウェア種別	名称	TOE／TOE 外
1	CVS マシン	OS	Sun Solaris 9 (SPARC 版)	×
2		Web サーバ	Apache 2.0.58 以降	×
3		暗号ライブラリ	OpenSSL 0.9.7m 以降	×
4		インタプリタ	Perl 5 (jcode.pl v2.0 及び CGI.pm を含む)	×
5		証明書検証サーバ	証明書検証サーバ 03-00 (Solaris 版)	○
6		HSM ドライバ［注 1］	nCipher Support Software for Solaris 8.20 以降 Luna SA Security Software for Solaris 2.2.1 以降	×
7	管理端末マシン	Web ブラウザ	Microsoft Internet Explorer 6.0	×
		OS	Microsoft Windows XP	×
8	クライアント PC	プログラム	利用者側クライアントプログラム	×

凡例:○…TOE、×…TOE 外

［注 1］CVS マシンに接続する HSM 製品に適合するものを選択して使用する。

2.3.3 TOE の範囲・境界に関わる論理的構成要素

図 3における TOE の範囲・境界に関わる論理的構成要素を図 4に示す。

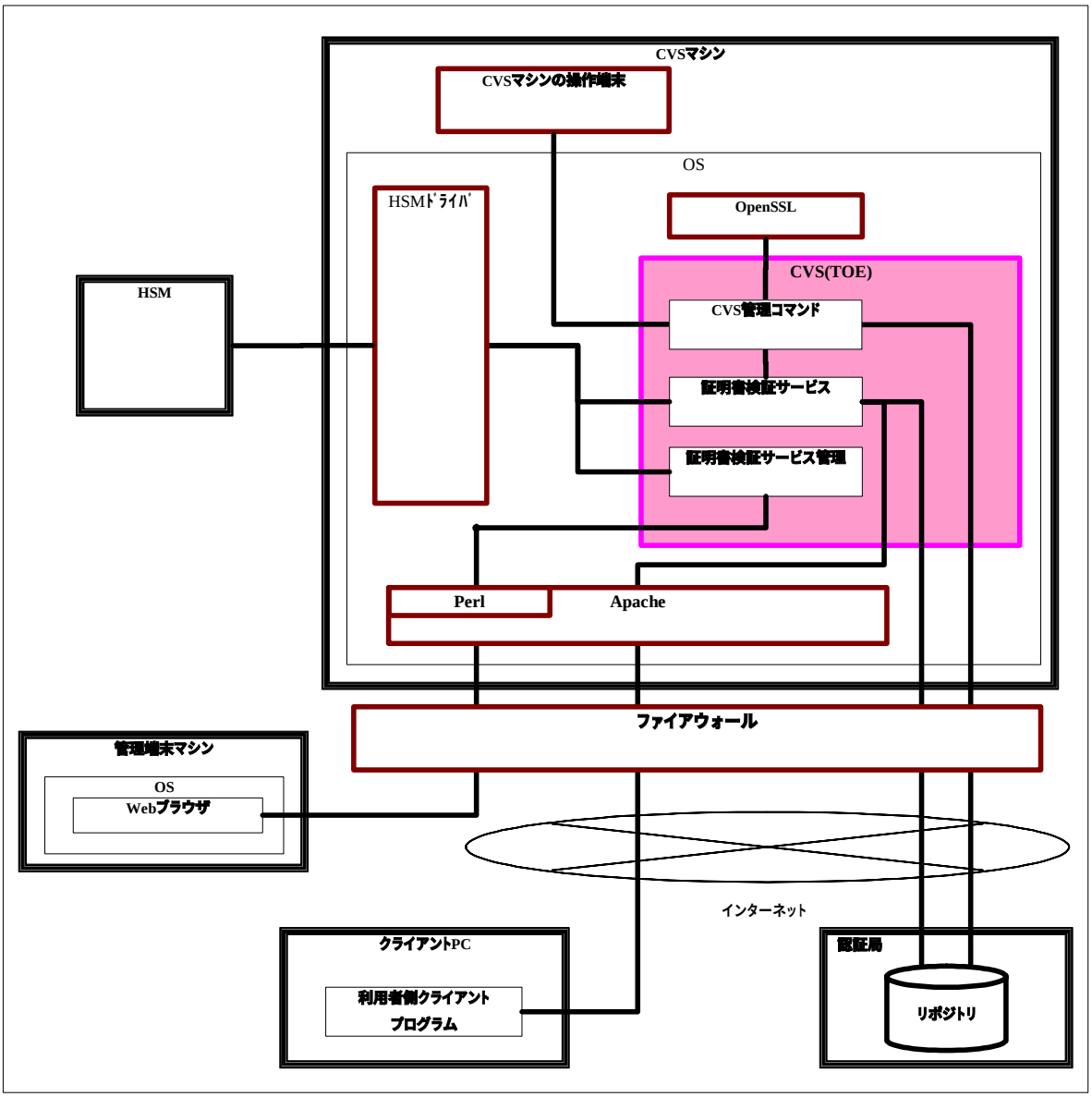

図 4 TOE の範囲・境界に関わる論理的構成要素

(1) CVS **マシン上の論理的構成要素**

① CVS

TOE であり、以下の論理的構成要素からなる。

証明書検証サービス

一般利用者が利用者側クライアントプログラムを利用して送信した証明書検証要求に基づいて証明書検証を行い、検証を依頼した一般利用者の利用者側クライアントプログラムに証明書検証結果応答を送信する。

証明書検証サービスには認証パス検証と OCSP 有効性検証の 2 種類がある。

証明書検証サービス管理

CVS 操作員が管理端末マシン上の Web ブラウザを通して利用する。

証明書検証サービス管理では、証明書検証に必要となる以下の処理を行う。

- CVS 証明書の登録・削除
- HSM ドライバへの CVS 秘密鍵の生成・破棄操作の指示
- 監査ログの検索・参照・削除

また、CVS 操作員の認証にベーシック認証を利用する場合は、以下の処理を行う。

- CVS 操作員の登録・削除・CVS 操作員のパスワード変更

CVS 管理コマンド

システム管理者に提供されるコマンド群であり、システム管理者により CVS マシンの操作端末から実行される。

CVS 管理コマンドは以下の処理を行う。

- CVS 操作員証明書登録コマンド
  - CVS 操作員認証に SSL クライアント認証を利用するとき、CVS 操作員証明書 ID を操作権限リストへ登録する。
- CVS 操作員証明書削除コマンド
  - CVS 操作員認証に SSL クライアント認証を利用するとき、CVS 操作員証明書 ID を操作権限リストから削除する。
- 失効リスト取得コマンド
  - OCSP 有効性検証サービス提供時に、検証対象証明書の有効性検証に利用する失効リストの登録及び、既に取得している失効リストの更新を行う。
  - システム管理者によって事前に登録されている認証局証明書を使用して、取得した失効リストの署名検証を行う。

② HSM **ドライバ**

HSM の操作を行うためのインタフェース群である。CVS の指示により HSM を操作し、CVS 秘密鍵の生成と破棄及び暗号操作を実行する。

HSM ベンダより提供される。

③ Apache

証明書検証サービス及び証明書検証サービス管理を動作させるための Web サーバである。

証明書検証サービスにおいては、証明書検証要求の受信と証明書検証結果の送信を行う。

証明書検証サービス管理においては、Perl を利用した証明書検証サービス管理の操作画面の送信と、CVS 操作員が操作画面で行った操作の受信を行う。

CVS 操作員認証にベーシック認証を利用する場合は、CVS 操作員から送信されたユーザ ID・パスワードと、操作権限リストに登録されているユーザ ID・パスワードの照合を行う。

④ Perl

証明書検証サービス管理を動作させるために必要なソフトウェアである。

証明書検証サービス管理において、CVS 操作員が証明書検証サービス管理で行う処理を指示するための画面を生成し、Apache に受け渡す処理を行う。また、CVS 操作員が画面から入力した情報を CVS に受け渡す処理を行う。

⑤ OpenSSL

CVS 管理コマンドを動作させるために必要なライブラリソフトウェアである。

CVS 操作員証明書登録コマンドにおいて、CVS 操作員証明書を作成するために利用される。

⑥ OS

- CVS、Apache、及び HSM ドライバが動作するために必要なオペレーティングシステムである。システム管理者のみが OS に対する操作を行う。

(2) **管理端末マシン上の論理的構成要素**

① OS

管理端末マシンが動作するために必要なオペレーティングシステムである。CVS 操作員が SSL クライアント認証により証明書検証サービス管理にアクセスする際、CVS 操作員秘密鍵の PIN による識別・認証を行う。

② Web **ブラウザ**

- CVS 操作員が証明書検証サービス管理にアクセスするために利用する。

(3) クライアント PC 上の論理的構成要素

① 利用者側クライアントプログラム

一般利用者がクライアント PC 上で利用するクライアントプログラムである。CVS に対して証明書検証要求を送信し、CVS からの証明書検証結果応答を受信する。また受信した証明書検証結果応答の検証を行う。

(4) その他の論理的構成要素

① リポジトリ

認証局が公開しているファイルサーバで、認証局証明書および認証局が発行した証明書と失効リストを保存している。

2.3.4 証明書検証サービスと関連するエンティティ及びデータ

一般利用者は、利用者側クライアントプログラムを使用して CVS マシンの検証機能用ポートにアクセスし、証明書検証要求の送信を行う。CVS が証明書検証要求を受けて、証明書検証結果応答を送信するまでの処理シーケンスを、各エンティティ及び関連データとの関係を中心に記述する。

(1) 証明書検証要求

CVS の認証パス検証サービス提供時の証明書検証要求には、

- 検証対象証明書
- トラストアンカ証明書

が含まれ、CVS の OCSP 有効性検証サービス提供時の証明書検証要求には、

- 証明書の発行者
- 証明書のシリアル番号

が含まれる。

これらの情報は一般利用者側がその正当性を保護するものとし、CVS は入力された情報をそのまま利用するものとする。したがって、証明書検証要求データの内容の正当性については CVS は積極的に関与しない。

証明書検証要求データは CVS から外部に出力されることのないメモリ情報である。また、証明書検証要求データは、証明書検証が終了した時点で CVS から抹消される。

ただし、CVS は、証明書の形式をとっているデータについては、証明書に付与されている署名を検証することにより改ざんチェックを行える。また、証明書検証要求に署名が付与されていたときには、その署名を検証することにより証明書検証要求の改ざんチェックを行える。

(2) 認証局への証明書／失効リストの要求とその取得データ

CVS は、認証パス検証／OCSP 有効性検証サービスを提供するために、認証局等が公開している認証局証明書及び失効リストが公開されているリポジトリから必要な認証局証明書及び失効リストを取得する。

認証パス検証サービス提供時には証明書検証要求受信時に、認証局証明書及び失効リストを取得する。OCSP 有効性検証サービス提供時には、サービス開始前に失効リストを取得する。

(3) HSM を利用した署名検証

CVS は、リポジトリから取得した認証局証明書及び失効リストの署名を検証することにより、改ざんチェックを行う。なお、署名検証の処理の一部である暗号操作は HSM を利用する。

(4) CVS 秘密鍵と CVS 証明書

CVS は、送信するデータの正当性を示すために、CVS 秘密鍵と CVS 証明書を持つ。CVS 秘密鍵と CVS 証明書は、CVS 操作員が証明書検証サービス管理を使用して管理する。

CVS 秘密鍵の生成及び破棄は、証明書検証サービス管理からの指示に基づいて HSM の内部で行われ、CVS 秘密鍵が HSM の外部に漏洩することはない。

CVS 証明書は、CVS 秘密鍵に対して発行された証明書である。CVS 証明書は、証明書検証結果応答の正当性を検証するための証拠として、証明書検証結果署名とともに証明書検証結果応答に付与される。

(5) 証明書検証結果応答

CVS は、証明書検証要求にしたがって認証パス検証／OCSP 有効性検証サービスによる証明書の検証を行い、証明書検証結果応答を返却する。証明書検証結果には、HSM 内に格納されている CVS 秘密鍵を使用して生成した署名(証明書検証結果署名)と、CVS 証明書を付与する。このデータはインターネットを経由して送信する。

CVS を使用した証明書検証の概要を図 5に示す。

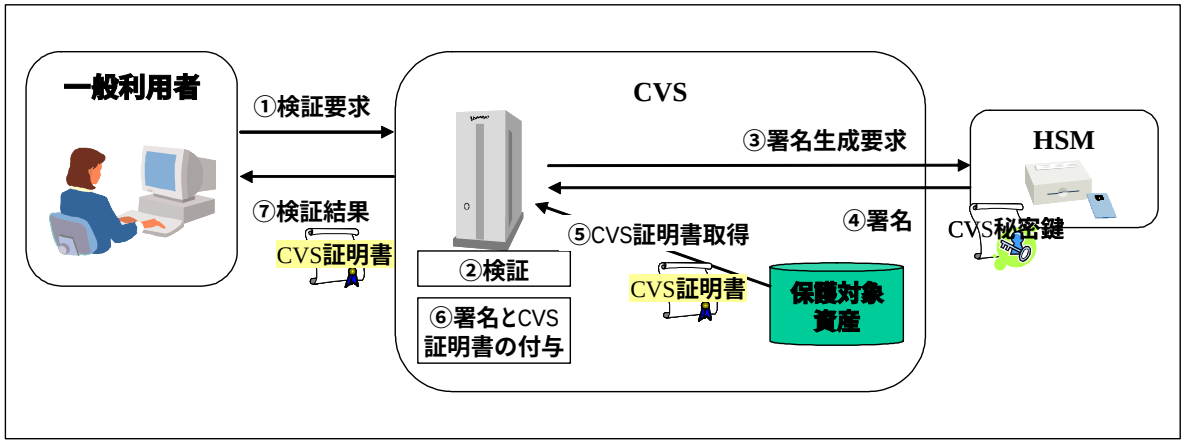

図 5 CVS を使用した証明書検証

2.3.5 証明書検証サービス管理と関連するエンティティ及びデータ

CVS 操作員は、CVS 運用環境において、管理端末マシン上の OS を使用して CVS マシンの証明書検証サービス管理機能にアクセスし、CVS 証明書の管理を行う。

管理端末マシン上の OS から CVS へのアクセスする際には、CVS 操作員に対する認証と識別が行われる。

CVS 操作員に対する認証には以下の 2 通りの方法がある。

① CVS 操作員の CVS 操作員証明書及び CVS 操作員秘密鍵による SSL クライアント認証

② CVS 操作員のユーザ ID とパスワードによるベーシック認証

①の場合は、CVS 操作員が入力した CVS 操作員秘密鍵の PIN による識別･認証を、管理端末マシン上の OS で行い、CVS 操作員証明書 ID と操作権限リスト(SSL クライアント認証用)の照合による識別を CVS で行う。CVS 操作員証明書 ID を記録している操作権限リストへのレコードの登録・削除はシステム管理者が行う。

②の場合は、ユーザ ID とパスワードによる識別･認証は Apache により行うが、ユーザ ID とパスワードを記録した操作権限リスト(ベーシック認証用)へのレコードの登録・削除及び CVS 操作員のパスワード変更は CVS 操作員が行う。

①、②どちらの認証を利用するかについては CVS のインストール時に選択し、CVS 利用開始後の認証方法の変更はできない。また、これらの認証を同時に利用することはできない。

(1) SSL クライアント認証による CVS 操作員認証

システム管理者は、CVS 管理コマンドを利用して CVS 操作員証明書 ID を操作権限リストに登録する。

CVS 操作員は、CVS 操作員秘密鍵に PIN を設定し、CVS 操作員証明書とともに管理端末マシンに登録する。

証明書検証サービス管理機能にアクセスする際には、CVS 操作員が CVS 操作員秘密鍵の PIN を入力することで、管理端末マシン上の OS による CVS 操作員の識別と認証を行う。CVS 操作員であることが確認されると、管理端末マシンより CVS マシンへ CVS 操作員証明書が送られる。CVS マシンへ送られた CVS 操作員証明書をもとに、まず、Apache により SSL クライアント認証が実行される。SSL クライアント認証で問題ない CVS 操作員証明書であることが確認されると Apache は CVS へ CVS 操作員証明書を渡す。CVS は CVS 操作員証明書を受け取り、CVS 操作員証明書 ID と操作権限リストの内容を比較することで CVS 操作員の識別を行う。

SSL クライアント認証による CVS 操作員認証の概要を図 6に示す。

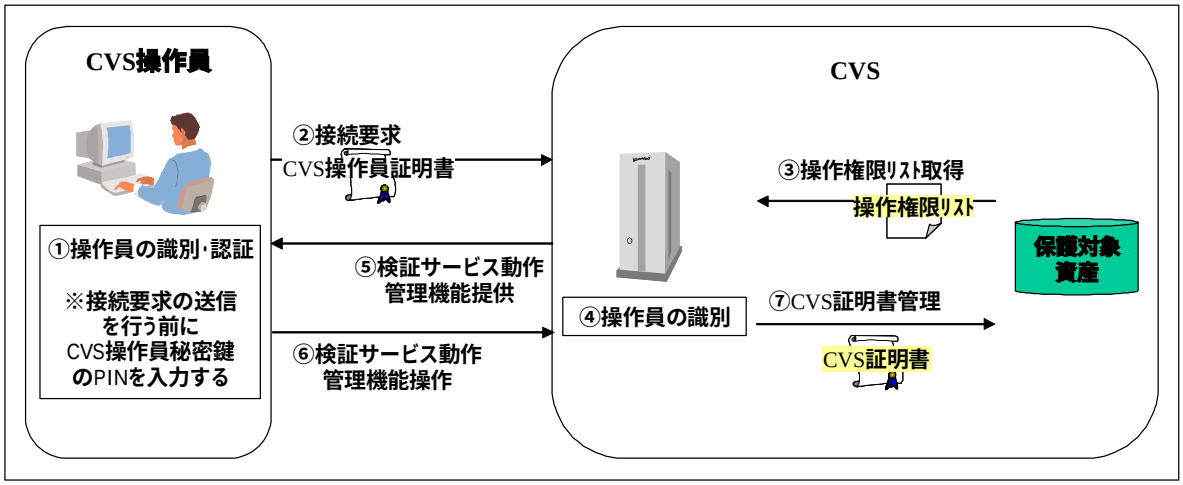

図 6 CVS 操作員認証と証明書検証サービス管理(SSL クライアント認証)

(2) ベーシック認証による CVS 操作員認証

CVS 操作員は、CVS 操作員のユーザ ID とパスワードを操作権限リストに登録する。

証明書検証サービス管理機能にアクセスする際には、CVS 操作員がユーザ ID とパスワードを入力し、これを Apache が識別･認証する。

ベーシック認証による CVS 操作員認証の概要を図 7に示す。

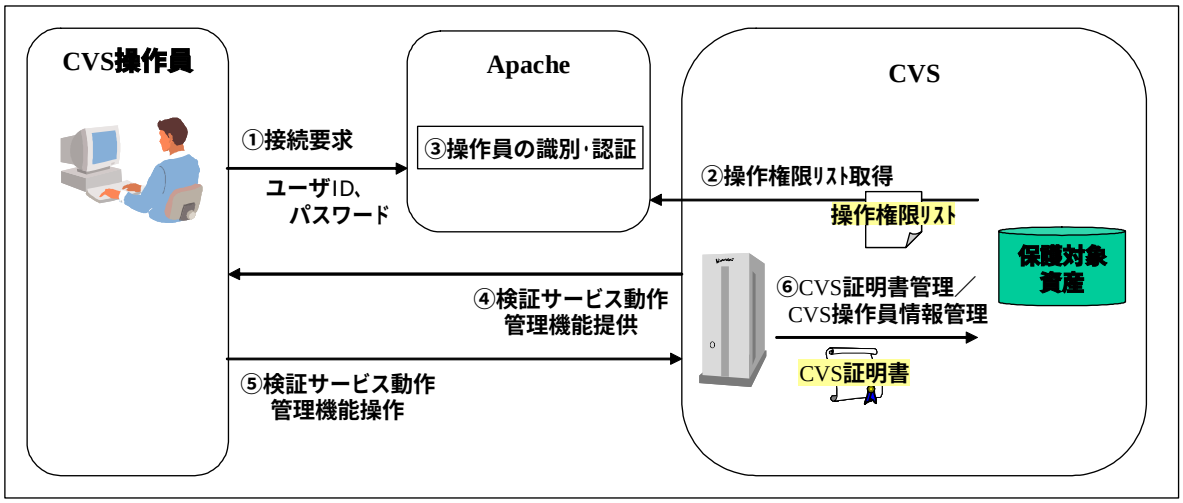

図 7 CVS 操作員認証と証明書検証サービス管理(ベーシック認証)

2.4 TOE の保護対象資産

TOE が提供する証明書検証サービスには 2 つの方式があるが、両方式でセキュリティ上の要件に差異はない。このため、本 ST では以下のデータを両方式での共通の保護対象資産として同様に扱い、区別はしない。

2.4.1 利用者データ

(1) 証明書検証結果応答

TOE のサービスとして提供する証明書検証の結果であり、TOE が証明書検証結果に付与する署名と CVS 証明書によってその信頼性が保証される。

署名の生成に使用する秘密鍵は、IT 環境として提供される HSM が管理する。また、CVS 証明書の信頼性は、CVS 証明書を発行する認証局の運用組織の管理に拠るところである。

(2) 操作権限リスト(ベーシック認証用)

CVS 操作員認証にベーシック認証を利用する場合の、CVS 操作員の情報である。CVS 操作員が証明書検証サービス管理機能にアクセスする際に、Apache によって参照され、識別･認証に使用される。なお、操作権限リスト(ベーシック認証用)は、IT 環境である Apache のセキュリティ機能を実現するための Apache の制御データであるが、TOE においては利用者データである。

CVS マシンの OS の管理下にあるファイルとして保管される。

2.4.2 TSF データ

(1) 認証局から取得した認証局証明書及び失効リスト

CVS のサービスを提供するために、公開されているリポジトリから取得した認証局証明書及び失効リストであり、以下の目的で利用する。

① 認証局証明書

- 認証パス検証において、証明書の検証を依頼した一般利用者が信頼する認証局の証明書から、検証対象の証明書までの一連の証明書の繋がりを構築するため。

② 失効リスト

- 認証パス検証において、認証パスを構成する認証局証明書の有効性検証を行うため。
- OCSP 有効性検証において、検証の対象となる証明書の有効性検証を行うため。

(2) CVS 証明書

CVS が提供する証明書検証結果に、署名とともに付与する証明書である。認証局から発行され、CVS 操作員によって CVS に登録される。CVS 証明書が改ざん・削除された場合

には正当な証明書検証結果応答の送信を行えなくなる。

CVS マシンの OS の管理下にあるファイルとして保管される。

(3) **操作権限リスト**(SSL **クライアント認証用**)

CVS 操作員認証に SSL クライアント認証を利用する場合の、CVS 操作員の情報である。CVS 操作員が、証明書検証サービス管理機能にアクセスする際に CVS 操作員証明書 ID の識別に使用される。

CVS マシンの OS の管理下にあるファイルとして保管される。

2.5 TOE **の関連者**

本 ST では TOE の運用・管理に関わる者として以下を想定する。

2.5.1 **システム管理者**

システム管理者は、セキュリティエリアに立ち入り、CVS マシンの操作端末を使用できる。システム管理者は CVS 操作員との兼務はできず、管理端末マシンの操作は行わない。

システム管理者は以下の作業を行う。

(CVS 操作員認証に SSL クライアント認証を利用する場合)

- ファイアウォールの設定
- CVS のインストール
- HSM の設定
- CVS 操作員の登録
- CVS 操作員の削除
- 失効リストの登録･更新(OCSP 有効性検証サービス利用時のみ)

(CVS 操作員認証にベーシック認証を利用する場合)

- ファイアウォールの設定
- CVS のインストール
- HSM の設定
- 失効リストの登録･更新(OCSP 有効性検証サービス利用時のみ)

2.5.2 CVS **操作員**

CVS 操作員は、セキュリティエリアに立ち入ることはできない。また、CVS 操作員はシステム管理者を兼務することはできない。

CVS 操作員は以下の作業を行う。

(CVS 操作員認証に SSL クライアント認証を利用する場合)

- CVS 証明書の登録・削除

- CVS 秘密鍵の生成・削除
- 監査ログの検索・参照・削除

(CVS 操作員認証にベーシック認証を利用する場合)

- CVS 操作員の登録・削除
- CVS 操作員のパスワード変更
- CVS 証明書の登録・削除
- CVS 秘密鍵の生成・削除
- 監査ログの検索・参照・削除

2.5.3 一般利用者

一般利用者は、利用者側クライアントプログラムを使用して、CVS に証明書検証を依頼する。

2.6 TOE が提供するセキュリティ機能

TOE は、以下のセキュリティ機能を提供する。

2.6.1 データ保護

TOE は、認証パス検証／OCSP 有効性検証サービスにおいて、証明書検証結果署名を証明書検証結果に付与し、検証を依頼した一般利用者の利用者側クライアントプログラムに送信する。検証を依頼した一般利用者の利用者側クライアントプログラムは、証明書検証結果応答の改ざんを検知するために、証明書検証結果署名の検証を行う。

2.6.2 データ改ざんチェック

TOE は、認証パス検証サービスを提供するために認証局から取得した認証局証明書及び失効リストを証明書検証に使用する前に、付与されている署名の検証を行い、データの改ざんチェックを行う。

改ざんを検知した場合は、その証明書を証明書検証に使用しない。

また、TOE は OCSP 有効性検証サービスを開始する前に、システム管理者が CVS 管理コマンドを実行して取得した失効リストに付与されている署名の検証を行い、データの改ざんチェックを行う。

改ざんを検知した場合は、その失効リストを証明書検証に使用しない。

2.6.3 識別･認証機能(CVS 操作員認証に SSL クライアント認証を利用する場合)

CVS の証明書検証サービス管理機能を利用する場合、管理端末マシン上の OS で、CVS 操作員秘密鍵の PIN による識別と認証が行われる。

TOE は、管理端末マシン上の OS によりその正当性が確認できた CVS 操作員証明書 ID に対して、操作権限リストによる識別を行い、その利用者が正当な CVS 操作員であることを確認する。

2.6.4 CVS 操作員情報管理機能(CVS 操作員認証に SSL クライアント認証を利用する場合)

TOE は、CVS 操作員証明書 ID を操作権限リストに登録することにより、CVS 操作員の登録を行う機能をシステム管理者に提供する。なお、CVS 操作員証明書及びそれに対応する CVS 操作員秘密鍵の生成についてはセキュリティ機能外とする。

また、操作権限リストに登録した CVS 操作員証明書 ID を削除することで CVS 操作員を削除する機能をシステム管理者に提供する。システム管理者は、CVS マシンの操作端末から CVS 管理コマンドを入力してこの機能を使用する。

2.6.5 CVS 操作員情報管理機能(CVS 操作員認証にベーシック認証を利用する場合)

TOE は、CVS 操作員の識別・認証を行うために必要となるユーザ ID とパスワードを操作権限リストに登録・削除すること、または CVS 操作員のパスワードを変更することにより、CVS 操作員の登録、削除及び CVS 操作員のパスワード変更を行う機能を CVS 操作員に提供する。

2.6.6 CVS 証明書管理機能

TOE は、CVS を適切に運用するために必要な、CVS 証明書の登録・更新及び削除を行う機能を CVS 操作員に提供する。

2.6.7 失効リスト取得機能

TOE は、OCSP 有効性検証サービスにおいて、検証対象証明書の有効性判定の根拠となる情報を CVS に取り込むために、失効リストの登録及び更新を行う機能をシステム管理者に提供する。

2.6.8 監査機能

TOE は、CVS のセキュリティ機能が適切に運用されていることを監査するために必要な情報を、監査ログとして記録し、監査ログの検索・参照及び削除を行う機能を CVS 操作員に提供する。

3 TOE セキュリティ環境

3.1 前提条件

3.1.1 利用環境

A.CVS_MACHINE (CVS マシンの設置)

CVS マシン、ファイアウォール及び HSM はシステム管理者のみが入退出できるエリアに設置される。

A.OPERATOR (人的資源)

システム管理者及び CVS 操作員は､TOE のセキュリティに対する不正及び秘密情報の漏洩を行わない。

A.CVS_R_ACCESS(CVS マシンへのリモートアクセス)

CVS マシン上の OS へのリモートからのログインはできない。

A.CVS_NETWORK(CVS マシンのネットワーク設定)

DMZ セグメント及び内部セグメントとインターネットそれぞれとの間は、以下の目的としたもの以外のアクセスを全て拒否する。

(インターネットから内部セグメントへのアクセス)

- (全てのアクセスを許可しない)

(内部セグメントからインターネットへのアクセス)

- (全てのアクセスを許可しない)

(インターネットから DMZ セグメントへのアクセス)

- 証明書検証要求を受信する際の CVS マシンの検証サービス用ポートへのアクセス
- CVS がリポジトリから認証局証明書及び失効リストを取得する際の、リポジトリから CVS マシンへデータを返却するためのアクセス

(DMZ セグメントからインターネットへのアクセス)

- CVS がリポジトリから認証局証明書及び失効リストを取得する際の、リポジトリへのアクセス
- CVS が証明書検証結果応答をする際の、一般利用者へのアクセス

(内部セグメントから DMZ セグメントへのアクセス)

- CVS 操作員が証明書検証サービス管理機能を利用する際の CVS マシンの管理機能用ポートへのアクセス

(DMZ セグメントから内部セグメントへのアクセス)

- CVS 操作員が証明書検証サービス管理機能を利用する際の、CVS マシンから管理端末マシンへのアクセス

A.CLIENT(利用者側クライアントプログラムの設置)

一般利用者は、証明書検証結果署名を検証できる利用者側クライアントプログラムを設置する。

A.ADMIN_SSL(CVS 操作員証明書の使用)

SSL クライアント認証の場合、CVS 操作員が管理端末から TOE にアクセスするための CVS 操作員証明書は、CVS 操作員のみが使用できる。

3.2 脅威

3.2.1 脅威エージェント

「3.1 前提条件」より、セキュリティ侵害を試みる脅威エージェントを、以下のように定義する。

- 不正な利用者 (CVS 操作員として TOE に接続することを許可されていない者全てを指す)
- インターネット上の悪意者

上記の脅威エージェントは、いずれも高度な専門知識を持たず、攻撃用の特別なツールを利用することも無い低レベルの攻撃者とする。

3.2.2 脅威の識別

T.MAN_IN_THE_MIDDLE (中間者攻撃)

インターネット上の悪意者が、ネットワーク上で TOE の証明書検証結果応答を取得し、改ざんして一般利用者へ送信することによって、一般利用者が、不正な証明書検証結果応答を受信するかもしれない。

また、インターネット上の悪意者が、認証パス検証/OCSP 有効性検証サービスを提供するために取得する証明書及び失効リストの通信中に、これをインターネット上で不正に取得、改ざんして TOE へ送信することによって正当なデータによる証明書検証が行えなくなるかもしれない。

T.UNAUTH_ACCESS (不正なアクセス)

不正な利用者が、管理端末マシン上の OS から TOE にアクセスし、保護対象資産を改ざんするか、あるいは削除することで、正当な証明書検証結果応答の送信を行うことができなくなるかもしれない。

3.3 組織のセキュリティ方針

組織のセキュリティ方針はない。

4 セキュリティ対策方針

4.1 TOE セキュリティ対策方針

TOE により実現するセキュリティ対策方針を以下に示す。

4.1.1 データ保護

O.SIGNATURE (証明書検証結果署名の付与)

TOE は、利用者側クライアントプログラムが証明書検証結果応答の改ざんを検知できるように、送信する証明書検証結果に対して、証明書検証結果署名と、この署名を検証するための CVS 証明書を付与する。なお、署名の生成に必要な処理の一部である暗号操作については HSM が提供する機能を利用するが、署名の生成機能は TOE が提供する機能である。

O.SIGVERIFY (取得データの署名検証)

TOE は、証明書検証サービスを提供するために取得した認証局証明書及び失効リストを使用する前に、署名の検証を行ってその正当性を確認し、改ざんを検知した場合はその認証局証明書及び失効リストを証明書検証に利用しない。なお、署名の検証に必要な処理の一部である暗号操作については HSM が提供する機能を利用するが、署名の検証機能は TOE が提供する機能である。

4.1.2 識別と認証

O.I&A_SSL (SSL クライアント認証による識別と認証)

CVS 操作員認証に SSL クライアント認証を利用する場合、TOE は、TOE の保護対象資産へのアクセスを許可する前に、管理端末マシン上の OS により識別・認証された CVS 操作員を、CVS 操作員が提示する CVS 操作員証明書 ID によって識別する。

O.I&A_BASIC (ベーシック認証による識別と認証)

CVS 操作員認証にベーシック認証を利用する場合、TOE は、登録された CVS 操作員のみが CVS 操作員のユーザ ID・パスワードを Apache に設定することにより、設定されたユーザ ID・パスワード以外を用いた Apache 上での CVS 操作員の識別・認証を不可能とする。

4.2 環境セキュリティ対策方針

IT 環境または運用・管理規程により実現するセキュリティ対策方針を以下に示す。

4.2.1 IT 環境セキュリティ対策方針

(1) 証明書検証結果署名

OE.HSM (HSM による暗号操作)

以下の処理については、IT 環境として提供される HSM が TOE からの指示によって実現する。

- 証明書検証結果署名を付与する際の暗号操作に利用する CVS 秘密鍵の生成・保持及び破棄
- CVS 秘密鍵を使用した、証明書検証結果に付与する証明書検証結果署名の生成における暗号操作機能の提供
- 証明書検証サービスを提供するために取得した認証局証明書及び失効リストの改ざんを検知するための署名検証における暗号操作機能の提供

(2) 証明書検証結果応答の検証

OE.CLIENT(利用者側クライアントプログラムによる証明書検証結果応答の検証)

以下の処理については、IT 環境として提供される利用者側クライアントプログラムによって実現する。

- 証明書検証結果署名の検証

(3) CVS 操作員秘密鍵の管理

OE.ADMIN_MACHINE(管理端末マシン上の OS による CVS 操作員秘密鍵の管理)

CVS 操作員認証に SSL クライアント認証を利用する場合、以下の処理については IT 環境として提供される管理端末マシン上の OS によって実現する。

- 管理端末マシン上の OS から、指定した CVS 操作員証明書を提示して CVS 管理機能へのアクセスする際、CVS 操作員秘密鍵の PIN の入力要求及び入力された PIN による CVS 操作員の識別と認証

(4) ユーザ ID とパスワードの認証

OE.HTTPD_BASIC (Apache のベーシック認証による識別･認証)

CVS 操作員認証にベーシック認証を利用する場合、Apache は、設定された「CVS 操作員が管理端末から TOE をアクセスするために必要な CVS 操作員のユーザ ID･パスワード」を用いて、Apache 上で、CVS 操作員が管理端末から TOE をアクセスする場合の CVS 操作員の識別･認証を実現する。

4.2.2 運用・管理的セキュリティ対策方針

(1) 設置・生成・立上げ規定

OM.SETTING (設置規定)

CVS マシン、HSM 及びファイアウォールは、セキュリティエリア内に設置しなければならない。

OM.CONNECT (接続規定)

- DMZ セグメントは、ファイアウォールを介してインターネットに接続しなければならない。
- ファイアウォールは、インターネットから内部セグメントへの全てのアクセスを拒否しなければならない。
- ファイアウォールは、内部セグメントからインターネットへの全てのアクセスを拒否しなければならない。
- ファイアウォールは、インターネットから DMZ セグメントへは、以下のアクセスを除いて全て拒否しなければならない。
  - 証明書検証要求を受信する際の CVS マシンの検証サービス用ポートへのアクセス
  - CVS がリポジトリから認証局証明書及び失効リストを取得する際の、リポジトリから CVS マシンへデータを返却するためのアクセス
- ファイアウォールは、DMZ セグメントからインターネットへは、以下のアクセスを除いて全て拒否しなければならない。
  - CVS がリポジトリから認証局証明書及び失効リストを取得する際の、リポジトリへのアクセス
  - CVS が証明書検証結果応答をする際の、一般利用者へのアクセス
- ファイアウォールは、内部セグメントから DMZ セグメントへは、以下のアクセスを除いて全て拒否しなければならない。
  - CVS 操作員が証明書検証サービス管理機能を利用する際の CVS マシンの管理機能用ポートへのアクセス
- ファイアウォールは、DMZ セグメントから内部セグメントへは、以下のアクセスを除いて全て拒否しなければならない。
  - CVS 操作員が証明書検証サービス管理機能を利用する際の、CVS マシンから管理端末マシンへのアクセス

OM.R_LOGIN(CVS マシンへのリモートログイン)

CVS マシン上の OS により提供されるリモートログインのためのサービスである、Rlogin、Telnet、SSH、Rsh、FTP を全て停止した状態で稼動する。

4.2.3 運用・管理規定

OM.OPERATOR(人的資源に関する規定)

CVS を運用する組織の長は、システム管理者及び CVS 操作員に対して TOE のセキュリティに関する教育を十分に実施し、保護対象資産への不正な操作、及び、自身が保持する秘密情報の漏洩を行うことのない信頼できる人物を配置する。

OM.S_AREA_CONTROL (セキュリティエリアの入退室制限)

セキュリティエリアは、システム管理者のみ入室できるよう入退室管理を行い、不正な物理的アクセスから保護しなければならない。

OM.CLIENT(利用者側クライアントプログラムの設置規定)

CVS を運用する組織は、一般利用者に対し、証明書検証結果署名を検証できる利用者側クライアントプログラムの設置を指導する。

OM.I&A_SSL(CVS 操作員認証に SSL クライアント認証を利用する場合の規定)

CVS を運用する組織は、CVS 操作員認証に SSL クライアント認証を利用する場合、CVS 操作員証明書を発行する認証局を１つの認証局に特定する。

OM.ADMIN_SSL(CVS 操作員証明書・CVS 操作員秘密鍵の提供に関する規定)

システム管理者は、CVS 操作員証明書及び CVS 操作員秘密鍵を、CVS 操作員にのみ提供する。CVS 操作員は、以下の条件を満たす PIN を CVS 操作員秘密鍵に付与して、CVS 操作員証明書とともに管理端末に登録する。

＜PIN の条件＞

文字種：半角英数字

文字長：8 文字以上 20 文字以下

5 IT セキュリティ要件

本章では、セキュリティ要件の許可された機能コンポーネントの割付及び選択に関する操作部分を **下線かつ太字** で示す。また、”＜”、”＞”及び”(”、”)”で囲まれた部分は、割付の内容を示す。詳細化に関する操作部分は *斜体かつ下線* で示す。繰り返しに関しては、コンポーネント及びエレメントに対してアルファベットを付与して記述する。

5.1 TOE セキュリティ機能要件

本 ST では、基本データ認証における証拠の生成と証拠の検証に関する機能要件コンポーネントとして CC パート 2 で規定されている機能要件で適合するものが存在しなかったため、CC パート 2 で規定されている **FDP_DAU.1** を拡張し **FDP_DAU_T.1** を設けている。

また、IT 環境のセキュリティ管理に関する機能要件コンポーネントとして CC パート 2 で規定されている機能要件で適合するものが存在しなかったため、CC パート 2 で規定されている **FIA_SOS.1** をベースとして **FIT_SOS.1** を、**FMT_MTD.1** をベースとして **FIT_MTD.1** を設けている。

これら以外の機能要件コンポーネントは、CC パート 2 で規定されているものを直接使用している。

5.1.1 セキュリティ監査

FAU_GEN.1 監査データ生成

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**指定なし**レベルのすべての監査対象事象; 及び
c) **上記以外の個別に定義した監査対象事象**。

＜個別に定義した監査対象事象＞

本節で挙げる各機能要件を選択した場合に、監査対象とすべきアクションと、「6.1.8 監査機能 (SF.AUDIT)」で示す TOE の監査対象事象との対応を表 5に示す。また、TOE で監査対象事象としているアクションを下線で示す。

表 5 機能要件と監査対象の一覧

機能要件	監査対象とすべきアクション	TOE の監査対象事象
TOE セキュリティ機能要件		
FAU_GEN.1	予見される監査対象事象はない。	なし
FAU_GEN.2	予見される監査対象事象はない。	なし
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	なし((1)参照)
FAU_SAR.2	a) 基本: 監査記録からの成功しなかった情報読み出し。	監査ログの読み込み失敗
FAU_SAR.3	a) 詳細: 閲覧に使用されるパラメタ。	なし((2)参照)
FDP_DAU_T.1	a) 最小: 有効性の証拠の生成成功。 b) 基本: 有効性の証拠の生成不成功。 c) 詳細: 証拠を要求したサブジェクトの識別情報。	証明書検証結果応答への署名付与 成功／失敗
FIA_UID.2.T	a) 最小: 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; b) 基本: 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すべての使用。	CVS 操作員の識別成功／失敗
FMT_MTD.1.a	a) 基本: TSF データの値のすべての改変。	CVS 操作員の登録 CVS 操作員の削除
FMT_MTD.1.b	a) 基本: TSF データの値のすべての改変。	CVS 証明書登録 CVS 証明書削除
FMT_MTD.1.c	a) 基本: TSF データの値のすべての改変。	失効リストの登録･更新
FMT_MTD.1.d	a) 基本: TSF データの値のすべての改変。	監査ログの削除
FMT_SMF.1	a) 最小：管理機能の使用	CVS 操作員の登録 CVS 操作員の削除 CVS 証明書登録 CVS 証明書削除
FMT_SMR.1	a) 最小: 役割の一部をなす利用者のグループに対する改変; b) 詳細: 役割の権限の使用すべて。	なし((3)参照)
FPT_ITI.1	a) 最小: 送出 TSF データの改変の検出。 b) 基本: 送出 TSF データの改変の検出において取られるアクション。	取得した証明書または失効リストの改ざん検知
FPT_RVM.1.T	予見される監査対象事象はない	なし
FPT_STM.1	a) 最小: 時間の変更 b) 詳細: タイムスタンプの提供。	なし ((4)参照)
FIT_SOS.1	a) 最小: TSF による、テストされた IT 環境の秘密の拒否 b) 基本: TSF による、テストされた IT 環境の秘密の拒否または受け入れ c) 詳細: 定義された品質尺度に対する変更の識別。	CVS 操作員の登録 CVS 操作員情報の改変
FIT_MTD.1	a) 基本: IT 環境用データの値のすべての改変。	CVS 操作員の登録 CVS 操作員情報の改変 CVS 操作員の削除

(1) **監査対象事象例外の根拠(監査記録の読み出し成功)**

FAU_SAR.1

CVS 操作員は、TOE へのログインに成功すれば必ず監査ログを読み込むことができる。したがって監査ログの読み込み成功を監査対象事象に含めない。

(2) **監査対象事象例外の根拠(閲覧に使用されるパラメタ)**

FAU_SAR.3

CVS 操作員は、TOE へのログインに成功すれば全ての監査ログを読み込むことができる。監査ログを閲覧するには TOE へのログインが必要であり、不正な利用者はログイン時の識別・認証の時点で排除される。

監査ログの閲覧を行う際に使用されるパラメタは、全ての監査ログの中から、閲覧対象を絞り込むための絞込み条件のみである。不正なパラメタが指定された場合は、監査ログの読み込み失敗として監査ログに記録される。

これらのことから、閲覧に使用されるパラメタを監査対象事象として記録する必要はない。

(3) **監査対象事象例外の根拠(グループに対する改変の監査)**

FMT_SMR.1

CVS 操作員は単一のグループである。したがって TOE はグループに対する改変を監査する機能を提供しない。

(4) **監査対象事象例外の根拠(時間の変更)**

FPT_STM.1

TOE は、時間を変更する機能を提供しない。

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、**以下の監査関連情報**

＜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_GEN.2 利用者識別情報の関連付け

下位階層: なし

FAU_GEN.2.1 TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

依存性: FAU_GEN.1 監査データ生成
FIA_UID.1 識別のタイミング

FAU_SAR.1 監査レビュー

下位階層: なし

FAU_SAR.1.1 TSF は、**CVS 操作員**が、**個別に定義した監査対象事象**を監査記録から読み出せるようにしなければならない。

＜個別に定義した監査対象事象＞

個別に定義した TOE の監査対象事象は表 5に示した通りである。

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。

依存性: FAU_GEN.1 監査データ生成

FAU_SAR.2 限定監査レビュー

下位階層: なし

FAU_SAR.2.1 TSF は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

依存性: FAU_SAR.1 監査レビュー

FAU_SAR.3 選択可能監査レビュー

下位階層: なし

FAU_SAR.3.1 TSF は、**監査事象の発生日時及び事象種別**に基づいて、監査データを**検索**する能力を提供しなければならない。

依存性: FAU_SAR.1 監査レビュー

5.1.2 利用者データ保護

FDP_DAU_T.1 基本データ認証(証拠の生成)

下位階層: なし

管理: **FDP_DAU_T.1**

以下のアクションは FMT における管理機能と考えられる:

a) データ認証が適用され得るオブジェクトに対する割付や改変が、システムにおいて設定可能である。

監査: **FDP_DAU_T.1**

FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下の事象を監査対象にすべきである:

a) 最小: 有効性の証拠の生成成功。

b) 基本: 有効性の証拠の生成不成功。

c) 詳細: 証拠を要求したサブジェクトの識別情報。

FDP_DAU_T.1.1 TSF は、**証明書検証結果**の有効性の保証として使用できる証拠を生成する能力を提供しなければならない。

依存性: **FDP_DAU_C.1 基本データ認証 (証拠の検証)**

5.1.3 識別と認証

FIA_UID.2.T アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1.T 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。

依存性: なし

5.1.4 セキュリティ管理

FMT_MTD.1.a TSF データの管理

下位階層: なし

FMT_MTD.1.1.a TSF は、(以下のデータ)を(以下の操作)する能力を(以下の役割)に制限しなければならない。

＜データ＞

- 操作権限リスト(SSL クライアント認証用)

＜操作＞

- その他の操作
  - レコードの追加
  - レコードの削除

＜役割＞

- システム管理者

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.b TSF データの管理

下位階層: なし

FMT_MTD.1.1.b TSF は、(以下のデータ)を(以下の操作)する能力を(以下の役割)に制限しなければならない。

＜データ＞

- CVS 証明書

＜操作＞

- 削除
- その他の操作
  - 登録

＜役割＞

- CVS 操作員

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.c TSF データの管理

下位階層: なし

FMT_MTD.1.1.c TSF は、**(以下のデータ)**を**(以下の操作)**する能力を**(以下の役割)**に制限しなければならない。

＜データ＞

- OCSP 有効性検証に利用する失効リスト

＜操作＞

- その他の操作
  - 登録
  - 更新

＜役割＞

- システム管理者

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.d TSF データの管理

下位階層: なし

FMT_MTD.1.1.d TSF は、**(以下のデータ)**を**(以下の操作)**する能力を**(以下の役割)**に制限しなければならない。

＜データ＞

- 表 5に示した個別に定義した監査事象に対する監査ログ

＜操作＞

- 削除

＜役割＞

- CVS 操作員

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:
：**(以下のセキュリティ管理機能のリスト)。**

＜セキュリティ管理機能＞

本節で挙げる各機能要件を選択した場合に、管理対象とすべきアクティビティと、TOE が持つセキュリティ管理機能を表 6に示す。また、TOE でセキュリティ管理機能を持つアクティビティを下線で示す。

表 6 機能要件と管理対象の一覧

機能要件	管理対象アクティビティ	TOE の管理機能
TOE セキュリティ機能要件		
FAU_GEN.1	予見される管理アクティビティはない。	なし
FAU_GEN.2	予見される管理アクティビティはない。	なし
FAU_SAR.1	a) 監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)。	なし((1)参照)
FAU_SAR.2	予見される管理アクティビティはない。	なし
FAU_SAR.3	予見される管理アクティビティはない。	なし
FDP_DAU_T.1	a) データ認証が適用され得るオブジェクトに対する割付や改変が、システムにおいて設定可能である。	CVS 証明書の設定
FIA_UID.2.T	利用者識別情報の管理。	CVS 操作員の登録、削除
FMT_MTD.1.a	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし ((1)参照)
FMT_MTD.1.b	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし((1)参照)
FMT_MTD.1.c	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし((1)参照)
FMT_MTD.1.d	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし((1)参照)
FMT_SMF.1	予見される管理アクティビティはない。	なし
FMT_SMR.1	役割の一部をなす利用者のグループの管理。	なし((1)参照)
FPT_ITI.1	予見される管理アクティビティは無い。	なし
FPT_RVM.1.T	予見される管理アクティビティは無い。	なし
FPT_STM.1	a) 時間の管理。	なし ((2)参照)
FIT_SOS.1	a) IT 環境の秘密の検証に使用される尺度の管理。	なし ((3)参照)
FIT_MTD.1	IT 環境用データと相互に影響を及ぼし得る役割のグループを管理すること。	なし((1)参照)

(1) 管理対象事象例外の根拠(TOE が保持する役割)

FAU_SAR.1

FMT_MTD.1.a

FMT_MTD.1.b

FMT_MTD.1.c

FMT_MTD.1.d

FMT_SMR.1

FIT_MTD.1

TOE が保持する役割は、各々の機能要件に対し、CVS 操作員、システム管理者のいずれかに固定されているため、管理対象とならない。したがって TOE はグループに対する管理及び改変を行う機能を提供しない。

(2) **管理対象事象例外の根拠(時間の変更)**

FPT_STM.1

TOE は、時間を変更する機能を提供しない。

(3) **管理対象事象例外の根拠(秘密の検証)**

FIT_SOS.1

TOE は、秘密の検証に使用される尺度の管理を行う機能を提供しない。

依存性: なし

FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1 TSF は、役割 **(以下の役割)** を維持しなければならない。

＜役割＞

- CVS 操作員

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

5.1.5 TSF の保護

FPT_ITI.1 TSF 間改変の検出

下位階層: なし

FPT_ITI.1.1 TSF は、以下の尺度の範囲で、TSF とリモート高信頼 IT 製品間で送出中のすべての TSF データの改変を検出する能力を提供しなければならない:**(以下の改変尺度)。**

＜改変尺度＞

リモート高信頼 IT 製品から送信される TSF データに対する任意の改変

FPT_ITI.1.2 TSF は、TSF とリモート高信頼 IT 製品間で送られるすべての TSF データの完全性を検証し、かつ改変が検出された場合には**(以下のアクション)**を実行する能力を提供しなければならない。

＜アクション＞

- 改変が検出された TSF データの不使用

依存性: なし

FPT_RVM.1.T TSP の非バイパス性

下位階層: なし

FPT_RVM.1.1.T TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能

が呼び出され成功することを保証しなければならない。

依存性: なし

FPT_STM.1 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。

依存性: なし

5.1.6 IT 環境のセキュリティ管理(拡張機能要件)

FIT_SOS.1 IT 環境の秘密の検証

下位階層: なし

管理：**FIT_SOS.1**

以下のアクションは FMT における管理機能と考えられる：

a) IT 環境の秘密の検証に使用される尺度の管理

監査：**FIT_SOS.1**

FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである。

a)最小：TSF による、テストされた IT 環境の秘密の拒否；

b)基本：TSF による、テストされた IT 環境の秘密の拒否または受け入れ；

c)詳細：定義された品質尺度に対する変更の識別。

FIT_SOS.1.1 TSF は、IT 環境の秘密が**(以下の品質尺度)**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。

＜品質尺度＞

文字種：半角英数字

文字長：8 文字以上 20 文字以下

依存性： なし

FIT_MTD.1 IT 環境用データの管理

下位階層: なし

管理：**FIT_MTD.1**

以下のアクションは FMT 管理における管理機能と考えられる：

a) IT 環境用データと相互に影響を及ぼし得る役割のグループを管理すること。

監査：**FIT_MTD.1**

FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである。

a) 基本：IT 環境用データの値のすべての改変。

FIT_MTD.1.1 TSF は、**(以下のデータ)**を**(以下の操作)**する能力を**(以下の役割)**に制限しなければならない。

＜データ＞

- 操作権限リスト(ベーシック認証用)

＜操作＞

- レコードの追加
- レコードの改変
- レコードの削除

＜役割＞

- CVS 操作員

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

5.2 IT 環境に対するセキュリティ機能要件

本 ST では、基本データ認証における証拠の生成と証拠の検証に関する機能要件コンポーネントとして CC パート 2 で規定されている機能要件で適合するものが存在しなかったため、CC パート 2 で規定されている **FDP_DAU.1** を拡張し **FDP_DAU_C.1** を設けている。これ以外の機能要件コンポーネントは、CC パート 2 で規定されているものを直接使用している。

5.2.1 **暗号サポート**

FCS_CKM.1 暗号鍵生成

下位階層: なし

FCS_CKM.1.1 *HSM* は、以下の**(暗号鍵生成に関する標準)**に合致する、指定された暗号鍵生成アルゴリズム **(以下の鍵生成アルゴリズム)** と指定された暗号鍵長 **(以下の鍵長)** に従って、暗号鍵を生成しなければならない。

＜暗号鍵生成に関する標準＞
＜鍵生成アルゴリズム＞
＜鍵長＞

各暗号鍵に関する暗号鍵生成に関する標準、鍵生成アルゴリズム、鍵長について表 7に示す。

表 7 暗号鍵生成に関する標準

鍵名称	標準	鍵生成アルゴリズム	鍵長
CVS **秘密鍵**	PKCS#1	RSA	512/768/1024/2048 bit

依存性: 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_CKM.4 暗号鍵破棄

下位階層: なし

FCS_CKM.4.1 *HSM* は、以下の**(暗号鍵破棄方法に関する標準)**に合致する、指定された暗号鍵破棄方法 **(以下の暗号鍵破棄方法)** に従って、暗号鍵を破棄しなければならない。

＜暗号鍵破棄方法に関する標準＞
＜暗号鍵破棄方法＞

各暗号鍵に関する暗号鍵破棄方法に関する標準、暗号鍵破棄方法について表 8に示す。

表 8 暗号鍵破棄方法に関する標準

鍵名称	標準	暗号鍵破棄方法
CVS **秘密鍵**	FIPS 140-2	FIPS 140-2 **準拠**

依存性: FCS_CKM.1 暗号鍵生成
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1.H 暗号操作

下位階層: なし

FCS_COP.1.1.H *HSM*は、**(以下の暗号操作に関する標準)**に合致する、特定された暗号アルゴリズム **(以下の暗号アルゴリズム)** と暗号鍵長 **(以下の鍵長)** に従って、**(以下の暗号操作)**を実行しなければならない。

＜暗号操作＞
＜暗号操作に関する標準＞
＜暗号アルゴリズム＞
＜鍵長＞

暗号操作に対する標準、暗号アルゴリズム、鍵長について、表 9に示す。

表 9 暗号操作に関する標準

暗号操作	標準	暗号アルゴリズム	鍵長
ディジタル署名の暗号化	PKCS#1	RSA	512/768/1024/2048 bit
ディジタル署名の復号	PKCS#1	RSA	**任意の鍵長**

依存性: FCS_CKM.1 暗号鍵生成
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1.C 暗号操作

下位階層: なし

FCS_COP.1.1.C *利用者側クライアントプログラム*は、**(以下の暗号操作に関する標準)**に合致する、特定された暗号アルゴリズム **(以下の暗号アルゴリズム)** と暗号鍵長 **(以下の鍵長)** に従って、**(以下の暗号操作)**を実行しなければならない。

＜暗号操作＞
＜暗号操作に関する標準＞
＜暗号アルゴリズム＞
＜鍵長＞

暗号操作に対する標準、暗号アルゴリズム、鍵長について、表 9に示す。

表 10 暗号操作に関する標準

暗号操作	標準	暗号アルゴリズム	鍵長
ディジタル署名の復号	PKCS#1	RSA	512/768/1024/2048 bit

依存性: 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

5.2.2 利用者データ保護

FDP_DAU_C.1 基本データ認証 (証拠の検証)

下位階層: なし

管理: **FDP_DAU_C.1**

以下のアクションは FMT における管理機能と考えられる:

a) データ認証が適用され得るオブジェクトに対する割付や改変が、システムにおいて設定可能である。

監査: **FDP_DAU_C.1**

FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下の事象を監査対象にすべきである:

a) 最小: 有効性の証拠の生成成功。
b) 基本: 有効性の証拠の生成不成功。
c) 詳細: 証拠を要求したサブジェクトの識別情報。

FDP_DAU_C.1.1 *利用者側クライアントプログラム*は、示された情報の有効性の証拠を検証する能力を**一般利用者**に提供しなければならない。

依存性: **FDP_DAU_T.1 基本データ認証(証拠の生成)**

5.2.3 識別と認証

FIA_AFL.1.BASIC 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1.BASIC *Apache* は、**管理端末からの接続における認証の要求**に関して、**1** 回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2.BASIC 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、*Apache* は、**当該コネクションの切断**をしなければならない。

依存性: FIA_UAU.1 認証のタイミング

FIA_UAU.2.BASIC アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1.BASIC *Apache* は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

依存性: FIA_UID.1 識別のタイミング

FIA_UID.2.BASIC アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1.BASIC *Apache* 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。

依存性: なし

FIA_AFL.1.SSL 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1.SSL *管理端末マシン上の OS* は、**管理端末からの接続における認証の要求**に関して、**1** 回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2.SSL 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、*管理端末マシン上の OS* は、**当該コネクションの切断**をしなければならない。

依存性: FIA_UAU.1 認証のタイミング

FIA_UAU.2.SSL アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1.SSL *管理端末マシン上の OS* は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

依存性: FIA_UID.1 識別のタイミング

FIA_UID.2.SSL アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1.SSL *管理端末マシン上の OS* 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。

依存性: なし

5.2.4 TSF の保護

FPT_RVM.1.BASIC TSP の非バイパス性

下位階層: なし

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

依存性: なし

FPT_RVM.1.SSL TSP の非バイパス性

下位階層: なし

FPT_RVM.1.1.SSL *管理端末マシン上の OS* 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

5.3 最小機能強度レベル

本 ST の TOE セキュリティ機能強度の最小強度レベルは SOF-基本であり、明示された機能強度は下記の通りである。

SOF-基本：**FIT_SOS.1**

5.4 TOE セキュリティ保証要件

TOE の評価保証レベルは EAL2 である。該当する保証コンポーネントを表 11に示す。

表 11 保証コンポーネント一覧 (EAL2)

保証クラス	保証コンポーネント	
構成管理 (ACM)	ACM_CAP.2	**構成要素**
配付と運用 (ADO)	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)	ADV_FSP.1	**非形式的機能仕様**
	ADV_HLD.1	**記述的上位レベル設計**
	ADV_RCR.1	**非形式的対応の実証**
ガイダンス文書 (AGD)	AGD_ADM.1	**管理者ガイダンス**
	AGD_USR.1	**利用者ガイダンス**
テスト (ATE)	ATE_COV.1	**カバレージの証拠**
	ATE_FUN.1	**機能テスト**
	ATE_IND.2	**独立試験 - サンプル**
脆弱性評定 (AVA)	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**

6 TOE 要約仕様

6.1 TOE セキュリティ機能

TOE のセキュリティ機能要件と TOE のセキュリティ機能の対応を表 12に示す。

表 12 セキュリティ機能要件と TOE セキュリティ機能の対応表

TOE セキュリティ機能要件 / TOE セキュリティ機能	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3	FDP_DAU_T.1	FIA_UID.2.T	FMT_MTD.1.a	FMT_MTD.1.b	FMT_MTD.1.c	FMT_MTD.1.d	FMT_SMF.1	FMT_SMR.1	FPT_ITI.1	FPT_RVM.1.T	FPT_STM.1	FIT_SOS.1	FIT_MTD.1
SF.SIGNATURE						○												
SF.SIGVERIFY														○				
SF.I&A_SSL							○						○		○			
SF.CVS_MGT_SSL								○				○	○					
SF.CVS_MGT_BASIC													○				○	○
SF.CVS_MGT_COMMON									○			○						
SF.CVS_MGT_CRL										○				○				
SF.AUDIT	○	○	○	○	○						○					○		

6.1.1 **データ保護** (SF.SIGNATURE)

TOE は証明書検証結果に対して、その有効性を検証するための証拠となる証明書検証結果署名と、CVS 証明書を、証明書検証結果に付与して一般利用者へ送信する。なお、証明書検証結果署名の生成に必要な処理の一部である暗号操作には、HSM を用いる。

一般利用者は証明書検証結果署名を利用者側クライアントプログラムにより検証し、証明書検証結果応答が改ざんされていないことを確認できる。

なお、保護対象資産である CVS 証明書は以下の形式のデータである。

＜CVS 証明書＞

RFC3280 で規定されている X.509 形式の電子証明書

6.1.2 **データ改ざんチェック**(SF.SIGVERIFY)

TOE は、証明書検証サービスを提供するために取得した認証局証明書及び失効リストと、これらのデータに付与された署名に対して、署名検証を行い、改ざんを検知した場合は証明書検証に使用しない。なお、署名検証に必要な処理の一部である暗号操作には HSM を用いる。

この署名検証により、TOE は取得した認証局証明書及び失効リストが改ざんされていないことを確認できる。

6.1.3 SSL **クライアント認証による識別･認証機能** (SF.I&A_SSL)

TOE は、正当な CVS 操作員を確認するために、以下の手順によって CVS 操作員の識別と認証を行う。なお、CVS 操作員証明書と特定の CVS 操作員との一意性は、管理端末マシン上の OS で行われる PIN による CVS 操作員秘密鍵の所有者の識別･認証により保証されている。

(1) TOE により、管理端末マシンの利用者が送信した CVS 操作員証明書 ID が、操作権限リスト内に記録された CVS 操作員証明書 ID と一致することの確認を行い、CVS 操作員の識別を行う。

(2) 以上の識別･認証が成功した後に、TOE は、CVS 操作員の動作を代行するサブジェクトとして、代行プロセスを生成し、当該 CVS 操作員を代行プロセスに関連付ける。

6.1.4 SSL **クライアント認証利用時における** CVS **操作員情報管理機能**(SF.CVS_MGT_SSL)

TOE は、CVS 管理コマンドにより、以下の管理機能をシステム管理者に提供する。

- CVS 操作員の登録

- CVS 操作員の削除

CVS 操作員の登録は、CVS 操作員証明書 ID を 1 レコードとして操作権限リストに登録することで行う。

CVS 操作員の削除は、削除対象の CVS 操作員証明書 ID を記録したレコードを、操作権限リストの中から削除することで行う。

なお、保護対象資産である操作権限リスト(SSL クライアント認証用)は以下の形式のデータである。

＜操作権限リスト(SSL クライアント認証用)＞

＜CVS 操作員レコード＞＜改行＞

＜CVS 操作員レコード＞＜改行＞

・・・

＜CVS 操作員レコード＞

＜CVS 操作員証明書 ID＞

6.1.5 **ベーシック認証利用時における** CVS **操作員情報管理機能** (SF.CVS_MGT_BASIC)

TOE は、管理端末マシン上の OS を経由して、以下の管理機能を CVS 操作員に提供する。

- CVS 操作員のパスワードの変更
- CVS 操作員の登録
- CVS 操作員の削除

CVS 操作員のパスワードの変更では、CVS 操作員の認証に利用するパスワードを設定する。このとき TOE は、パスワードが以下の品質尺度に基づいて設定されていることの検証を行い、設定されたパスワードが品質尺度を満たさない場合は再度パスワードの設定を要求する。なお、インストール時に初期設定されるユーザ ID とパスワードはそのままで使用せず、本機能により CVS 操作員がセキュアな値に設定した後に使用する。

＜品質尺度＞

文字種：半角英数字

文字長：8 文字以上 20 文字以下

CVS 操作員の登録は、CVS 操作員のユーザ ID とパスワードの組を 1 レコードとして操作権限リストに登録することで行う。CVS 操作員の削除は、削除対象の CVS 操作員のユーザ ID 及びパスワードの組を、操作権限リストの中から削除することで行う。なお、操作権限リストは Apache で行われるユーザ ID・パスワードの識別･認証の際に利用される。

保護対象資産である操作権限リスト(ベーシック認証用)は以下の形式のデータである。

＜操作権限リスト(ベーシック認証用)＞

＜CVS 操作員レコード＞＜改行＞

＜CVS 操作員レコード＞＜改行＞

・・・

＜操作員レコード＞

＜CVS 操作員のユーザ ID＞,＜CVS 操作員のパスワード＞

6.1.6 CVS **証明書管理機能** (SF.CVS_MGT_COMMON)

TOE は、以下の管理機能を CVS 操作員に提供する

- CVS 証明書の削除及び登録

CVS 証明書の削除及び登録では、CVS 操作員が管理端末マシン上の OS から CVS マシンの証明書検証サービス管理機能へアクセスし、これらの操作を行う。CVS 証明書の新規作成を行う場合は、CVS 秘密鍵を、HSM を用いて生成し、HSM 内で保持する。CVS 操作員は、CVS 秘密鍵に生成を行った後に、対応する CVS 証明書の登録を行う。

6.1.7 **失効リスト取得機能** (SF.CVS_MGT_CRL)

TOE は、CVS 管理コマンドにより、以下の管理機能をシステム管理者に提供する。

- OCSP 有効性検証に利用する失効リストの登録及び更新

失効リストの登録及び更新は、システム管理者が CVS マシンの操作端末から、失効リスト取得コマンドを実行することで行う。

失効リストの登録は、コマンドの設定ファイルで指定されたリポジトリから、インターネットを介して行う。

失効リストの更新では、取得と同様の処理により、前回登録した失効リストの情報を上書きする。

また TOE は、失効リストの登録および更新を行う際には、それらの失効リストを発行した認証局証明書による失効リストの署名検証を行い、改ざんを検知した場合は証明書検証に使用しない。なお、署名検証の処理の一部である暗号操作には HSM を利用する。

6.1.8 **監査機能** (SF.AUDIT)

(1) 監査ログ生成

TOE は、監査の対象となる事象が発生した場合に、当該事象を監査ログとして記録する。なお、監査機能の起動･終了は、証明書検証サービス管理の起動･停止として記録される。

監査ログには以下の 2 種類が存在する。

- 運用・管理操作のログ(管理ログ・起動停止ログ)
- 証明書検証サービスのログ(システムログ・アクセスログ)

① 運用・管理操作のログ

管理ログ

CVS 操作員が行った、TOE の運用・管理操作および、システム管理者が行った、SSL クライアント認証利用時における CVS 操作員情報管理操作を記録する。

TOE が、管理ログに記録する監査情報の一覧を表 13に示す。

表 13 TOE が記録する監査情報の一覧 (管理ログ)

項目	説明
日時	**事象が発生した年月日時分秒を示すタイムスタンプ情報**
プロセス ID	**事象が発生したプロセスのプロセス** ID
事象種別	**発生事象の種別（標準：**INFO**、エラー：**ERROR**）**
ユーザ ID	**発生事象に関連する操作を行ったシステム管理者または、**CVS **操作員の** ID
メッセージ	**発生事象の内容**

TOE は、監査ログに必要なタイムスタンプを OS から取得して記録する。

システム管理者による操作の場合、TOE は、ユーザ ID の項目に consoleOperator と記録する。

CVS 操作員による操作の場合、TOE は、ユーザ ID の項目に、CVS 操作員の ID を記録する。

TOE は、発生事象の成功及び失敗を、メッセージの内容に記述する。

発生事象が成功の場合、TOE は、事象種別の項目を INFO として記録する。発生事象が失敗の場合、TOE は、事象種別の項目を ERROR として記録する。

TOE は、表 14に示す事象が発生した際に、監査ログを記録する。

表 14 TOE が記録する監査対象事象の一覧 (管理ログ)

No	監査対象事象
1	CVS **操作員の登録**
2	CVS **操作員情報の改変**
3	CVS **操作員の削除**
4	CVS **操作員の識別 成功／失敗**
5	CVS **証明書登録**
6	CVS **証明書削除**
7	**監査ログの読み込み 失敗**
8	**監査ログの削除**

起動停止ログ

システム管理者が行った、証明書検証サービス管理の起動/停止を記録する。

TOE が、起動停止ログに記録する監査情報の一覧を表 15に示す。

表 15 TOE が記録する監査情報の一覧 (起動停止ログ)

項目	説明
日時	**事象が発生した年月日時分秒を示すタイムスタンプ情報**
プロセス ID	**事象が発生したプロセスのプロセス** ID
事象種別	**発生事象の種別（**INFO**）**
ユーザ ID	**発生事象に関連する操作を行ったシステム管理者の** ID (consoleOperator)
メッセージ	**発生事象の内容**

TOE は、監査ログに必要なタイムスタンプを OS から取得して記録する。

TOE は、ユーザ ID の項目に consoleOperator と記録する。

TOE は、発生事象の内容を、メッセージの内容に記述する。

TOE は、事象種別の項目を INFO として記録する。

TOE は、表 16に示す事象が発生した際に、監査ログを記録する。

表 16 TOE が記録する監査対象事象の一覧 (起動停止ログ)

No	監査対象事象
1	**証明書検証サービス管理起動**
2	**証明書検証サービス管理停止**

② 証明書検証サービスのログ

システムログ

TOE が、証明書検証要求にしたがって実行した証明書検証の結果および、システム管理者が行った、TOE の運用・管理操作を記録する。

TOE が、システムログに記録する監査情報の一覧を表 17に示す。

表 17 TOE が記録する監査情報の一覧 (システムログ)

項目	説明
日時	**事象が発生した年月日時分秒を示すタイムスタンプ情報**
プロセス ID	**事象が発生したプロセスのプロセス** ID
事象種別	**発生事象の種別（標準：**INFO**、エラー：**ERROR**）**
機能分類	**エラーが発生した機能**
トランザクション ID	**エラーが発生したトランザクションの** ID **(トランザクション** ID **が出力できない場合は、 ”-”を出力)**

メッセージ	発生事象の内容
エラー番号	オペレーティングシステム（OS）から通知されたエラー番号（項目：事象種別がエラーの場合に出力）

TOE は、監査ログに必要なタイムスタンプを OS から取得して記録する。

TOE は、監査ログのサブジェクト識別情報として、トランザクション ID を記録する。

TOE は、発生事象の成功及び失敗を、メッセージの内容に記述する。

発生事象が成功の場合、TOE は、事象種別の項目を INFO として記録する。発生事象が失敗の場合、TOE は、事象種別の項目を ERROR として記録する。

TOE は、表 18に示す事象が発生した際に、監査ログを記録する。

表 18 TOE が記録する監査対象事象の一覧（システムログ）

No	監査対象事象
1	証明書検証結果署名の付与 失敗
2	取得した証明書または失効リストの改ざん検知
3	失効リスト登録･更新

アクセスログ

証明書検証要求受信および、証明書検証応答送信の発生と、認証パス検証の結果を記録する。

TOE が、アクセスログに記録する監査情報の一覧を表 19に示す。

表 19 TOE が記録する監査情報の一覧（アクセスログ）

項目	説明
日時	事象が発生した年月日時分秒を示すタイムスタンプ情報
プロセス ID	事象が発生したプロセスのプロセス ID
事象種別	発生事象の種別（REQUEST、VALIDATION、RESPONSE）
IP アドレス	証明書検証要求を送信したクライアントマシンの IP アドレス
トランザクション ID	事象が発生したトランザクションの ID
メッセージ	発生事象の内容

TOE は、監査ログに必要なタイムスタンプを OS から取得して記録する。

TOE は、監査ログのサブジェクト識別情報として、証明書検証要求を送信したクライアント PC の IP アドレスを記録する。

TOE は、証明書検証要求を一意に特定する識別情報を、トランザクション ID として記録する。

TOE は、発生事象の成功及び失敗を、メッセージの内容に記述する。

TOE は、事象種別の項目を、証明書検証要求受信時には “REQUEST”、証明書検証応答送信時には “RESPONSE” として記録する。また、認証パス検証サービスの提供時は、認

証パス検証時に “VALIDATION” として記録する。

TOE は、表 20に示す事象が発生した際に、監査ログを記録する。

表 20 TOE が記録する監査対象事象の一覧 (アクセスログ)

No	監査対象事象
1	取得した証明書または失効リストの改ざん検知
2	証明書検証結果署名の付与 成功

(2) 監査ログ参照

TOE は CVS 操作員に対してのみ、管理端末マシン上の OS から監査ログを参照する機能を提供する。なお、TOE が提供する機能を利用して参照できるログは管理ログ、システムログ及びアクセスログである。

監査ログの参照に先立って、CVS 操作員はその参照範囲を、監査事象の発生日時及び事象種別を条件として検索することができる。

CVS 操作員が監査ログの検索により参照範囲を絞り込み、または、監査ログの検索を行わず、参照範囲を絞り込まずに監査ログを参照することによって、TOE は、当該監査ログを表示する。

監査ログの表示に際して TOE は、記録した情報を記録した時刻順に表形式で表示する。

(3) 監査ログ削除

TOE は CVS 操作員に対してのみ、管理端末マシン上の OS から監査ログを削除する機能を提供する。なお、TOE が提供する機能を利用して削除できるログは管理ログ、システムログ及びアクセスログである。

6.2 セキュリティ機能強度

確率的または順列的メカニズムに基づくセキュリティ機能は、**SF.CVS_MGT_BASIC** である。このセキュリティ機能は機能強度レベル SOF-基本を持つ。

6.3 保証手段

本 ST で適用するセキュリティ保証要件と、セキュリティ保証手段の対応を表 21、表 22 に示す。

表 21、表 22に示したドキュメントは、「5.4 TOE セキュリティ保証要件」で記述した保証要件を満たすものである。

表 21 セキュリティ保証要件(EAL2)とセキュリティ保証手段の対応表(Linux 版)

保証要件クラス	保証要件 コンポーネント	保証手段
ACM:構成管理	ACM_CAP.2	証明書検証サーバ 構成管理文書
ADO:配付と運用	ADO_DEL.1	証明書検証サーバ 配付文書
	ADO_IGS.1	証明書検証サーバ 操作の手引き(Linux 版) 、ソフトウェア添付資料(Linux 版)
ADV:開発	ADV_FSP.1	証明書検証サーバ 機能仕様書
	ADV_HLD.1	証明書検証サーバ 構造設計書
	ADV_RCR.1	証明書検証サーバ 対応分析書
AGD:ガイダンス文書	AGD_ADM.1	証明書検証サーバ 操作の手引き(Linux 版)、ソフトウェア添付資料(Linux 版)
	AGD_USR.1	
ATE:テスト	ATE_COV.1	証明書検証サーバ テスト分析書
	ATE_FUN.1	証明書検証サーバ テスト仕様書 証明書検証サーバ テスト報告書
	ATE_IND.2	TOE(Linux 版)
AVA:脆弱性評定	AVA_SOF.1	証明書検証サーバ セキュリティ強度分析書
	AVA_VLA.1	証明書検証サーバ 脆弱性分析書

表 22 セキュリティ保証要件(EAL2)とセキュリティ保証手段の対応表(Solaris 版)

保証要件クラス	保証要件 コンポーネント	保証手段
ACM:構成管理	ACM_CAP.2	証明書検証サーバ 構成管理文書
ADO:配付と運用	ADO_DEL.1	証明書検証サーバ 配付文書
	ADO_IGS.1	証明書検証サーバ 操作の手引き(Solaris 版) ソフトウェア添付資料(Solaris 版)
ADV:開発	ADV_FSP.1	証明書検証サーバ 機能仕様書
	ADV_HLD.1	証明書検証サーバ 構造設計書
	ADV_RCR.1	証明書検証サーバ 対応分析書
AGD:ガイダンス文書	AGD_ADM.1	証明書検証サーバ 操作の手引き(Solaris 版)、ソフトウェア添付資料(Solaris 版)
	AGD_USR.1	
ATE:テスト	ATE_COV.1	証明書検証サーバ テスト分析書
	ATE_FUN.1	証明書検証サーバ テスト仕様書 証明書検証サーバ テスト報告書
	ATE_IND.2	TOE(Solaris 版)
AVA:脆弱性評定	AVA_SOF.1	証明書検証サーバ セキュリティ強度分析書
	AVA_VLA.1	証明書検証サーバ 脆弱性分析書

7 PP 主張

7.1 PP 参照

参照した PP はない。

7.2 PP 修正

PP への修正はない。

7.3 PP 追加

PP への追加はない。

8 根拠

8.1 セキュリティ対策方針根拠

本節では、セキュリティ対策方針が TOE セキュリティ環境に対して必要かつ十分であることを記述する。

セキュリティ対策方針と、対応する前提条件及び脅威の対応関係を表 23に示す。

表 23 セキュリティ対策方針と対応する前提条件及び脅威の対応

前提条件及び脅威 / セキュリティ対策方針	A.CVS_MACHINE	A.OPERATOR	A.CVS_R_ACCESS	A.CVS_NETWORK	A.CLIENT	A.ADMIN_SSL	T.MAN_IN_THE_MIDDLE	T.UNAUTH_ACCESS
O.SIGNATURE							○	
O.SIGVERIFY							○	
O.I&A_SSL								○
O.I&A_**BASIC**								○
OM.OPERATOR		○						
OM.SETTING	○							
OM.S_AREA_CONTROL	○							
OM.CONNECT				○				
OM.R_LOGIN			○					
OM.CLIENT					○			
OM.I&A_SSL								○
OM.ADMIN_SSL						○		
OE.HSM							○	
OE.CLIENT							○	
OE.ADMIN_MACHINE								○
OE.HTTPD_BASIC								○

次に、各前提条件に対して、セキュリティ対策方針で実現できること、ならびに各脅威に対してセキュリティ対策方針で対抗できることを示す。

＜前提条件＞

A.CVS_MACHINE (CVS マシンの操作)

OM.SETTING により、CVS マシン、ファイアウォール、HSM はセキュリティエリア内に配置される。また、**OM.S_AREA_CONTROL** により、セキュリティエリアにはシステム管理者のみが入れるように入退室管理が行われ、不正な物理的アクセスから保護されている。したがって CVS マシン、ファイアウォール及び HSM はシステム管理者のみが入退出できるエリアに設置される。

この対策によって **A._CVS_MACHINE** は実現される。

A.OPERATOR (人的資源)

OM.OPERATOR により、CVS を運用する組織の長は、システム管理者及び CVS 操作員に対して TOE のセキュリティに関する十分な教育を行い、保護対象資産への不正な操作、及び、自身が保持する秘密情報の漏洩を行うことのない信頼できる人物を配置する。

この対策によって **A.OPERATOR** は実現される。

A.CVS_R_ACCESS(CVS マシンへのリモートアクセス)

OM.R_LOGIN により CVS マシン上の OS へのリモートログインが行えなくなる。

この対策によって **A.CVS_R_ACCESS** は実現される。

A.CVS_NETWORK(CVS のネットワーク設定)

OM.CONNECT により、インターネットから DMZ セグメントへの証明書検証要求の送信と、CVS がリポジトリから認証局証明書／失効リストの取得する際の、リポジトリから CVS マシンの検証サービス用ポートへのアクセス以外が拒否され、また DMZ セグメントからインターネットへの、CVS が認証パス検証／OCSP 有効性検証サービスを提供するための認証局証明書及び失効リストを取得する際のアクセスと、検証を依頼した証明書検証結果応答の送信以外のアクセスが拒否される。さらに、内部セグメントからインターネット、インターネットから内部セグメントへの全てのアクセスが拒否される。ならびに、ファイアウォールによって DMZ セグメントにある CVS マシンの管理機能用ポート以外への管理端末マシンからのアクセスは拒否され、また内部セグメントへの CVS マシンの管理機能用ポート以外からのアクセスも拒否される。

この対策によって **A.CVS_NETWORK** は実現される。

A.CLIENT(利用者側クライアントプログラムの設置)

OM.CLIENT により、一般利用者は、CVS を運用する組織の指導に基づいて証明書検証結果署名を検証できる利用者側クライアントプログラムを設置する。

この対策によって **A.CLIENT** は実現される。

A.ADMIN_SSL(CVS 操作員証明書の使用)

OM.ADMIN_SSL により、CVS 操作員証明書及び CVS 操作員秘密鍵は、システム管理者によって CVS 操作員にのみ提供される。CVS 操作員は、一定の品質尺度を満たす PIN を CVS 操作員秘密鍵に付与して、CVS 操作員証明書とともに管理端末に登録するため、CVS 操作員のみが CVS 操作員証明書を使用できる。

この対策によって **A.ADMIN_SSL** は実現される。

以上より、全ての前提条件に対して、何らかのセキュリティ対策方針が十分に実現していることが示される。

＜脅威＞

T.MAN_IN_THE_MIDDLE (中間者攻撃)

OE.HSM により、HSM は、TOE の指示に基づいて CVS 秘密鍵を使用した証明書検証結果署名の生成に必要は暗号操作機能を提供する。そして、**O.SIGNATURE** により、TOE は一般利用者へ送信する証明書検証結果応答に対して、証明書検証結果署名と、この署名を検証するための CVS 証明書を付与する。なお、この時利用する CVS 秘密鍵は、**OE.HSM** により、HSM 内で生成・保存・破棄の管理を実施し、外部に漏洩することはない。

また、**OE.CLIENT** により、一般利用者は利用者側クライアントプログラムによって証明書検証結果署名の検証を行い、インターネット上の悪意者によるネットワーク上での証明書検証結果応答の改ざんを検知することができる。

また、**OE.HSM** により、HSM は、証明書検証サービスを提供するために取得した認証局証明書及び失効リストに付与されている署名の検証に必要な暗号操作機能を提供する。そして、**O.SIGVERIFY** により、TOE は認証局証明書及び失効リストに付与されている署名の検証を行い正当性を確認する。このとき改ざんを検知した場合はその認証局証明書及び失効リストを証明書検証に利用しない。以上により、認証局証明書及び失効リストは、インターネット上の悪意者による改ざんから保護される。

これらの対策により、**T.MAN_IN_THE_MIDDLE** に対抗できる。

T.UNAUTH_ACCESS (不正なアクセス)

(CVS 操作員認証に SSL クライアント認証を利用する場合)

CVS 操作員の TOE の保護対象資産へのアクセスを許可する前に、**OE.ADMIN_MACHINE** により、すべての CVS 操作員に対して、CVS 操作員秘密鍵の PIN による CVS 操作員の識別･認証が管理端末の OS によって行われる。また、**O.I&A_SSL** により、識別認証後に提示される CVS 操作員証明書の CVS 操作員証明書 ID による CVS 操

作員の識別を TOE が実施することで､不正な利用者の TOE へのアクセスに対抗している。

なお、不正な利用者が、正当な CVS 操作員証明書 ID と同じ ID を持つ証明書を不正に作成してアクセスを試みる場合においても、**OM.I&A_SSL** により、CVS 操作員証明書を発行できる認証局は１つに特定されている。したがって不正な利用者が同一認証局発行の同一 CVS 操作員証明書 ID を持つ証明書を作成することは困難である。

この組合せにより、管理端末から TOE への不正なアクセスに対抗し、保護対象資産の改ざんに対抗することができる。

これらの対策によって **T.UNAUTH_ACCESS** に対抗できる。

(CVS 操作員認証にベーシック認証を利用する場合)

O.I&A_BASIC により､Apache 上での識別･認証に使用される CVS 操作員のユーザ ID･パスワードを TOE が設定する。**OE.HTTPD_BASIC** により、TOE に接続を試みるすべての CVS 操作員に対し、CVS 操作員のユーザ ID・パスワードに基づく識別･認証が Apache 上で行われる。この組合せにより、TOE は管理端末からの不正な TOE へのアクセスに対抗し、保護対象資産の改ざんに対抗することができる。

これらの対策によって **T.UNAUTH_ACCESS** に対抗できる。

以上より、全ての脅威に対して、何らかのセキュリティ対策方針が十分に対策していることが示される。

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

本項では、セキュリティ機能要件がセキュリティ対策方針に対して必要かつ十分であることを記述する。

セキュリティ機能要件とセキュリティ対策方針の対応関係を表 24に示す。

表 24 セキュリティ機能要件とセキュリティ対策方針の対応表

セキュリティ機能要件 ＼ セキュリティ対策方針	O.SIGNATURE	O.SIGVERIFY	O.I&A_SSL	O.I&A_**BASIC**	OE.HSM	OE.CLIENT	OE.ADMIN_MACHINE	OE.HTTPD_BASIC
TOE **セキュリティ機能要件**								
FAU_GEN.1	○	○	○	○				
FAU_GEN.2	○	○	○	○				
FAU_SAR.1	○	○	○	○				
FAU_SAR.2	○	○	○	○				
FAU_SAR.3	○	○	○	○				
FDP_DAU_T.1	○							
FIA_UID.2.T			○					
FMT_MTD.1.a			○					
FMT_MTD.1.b	○							
FMT_MTD.1.c		○						
FMT_MTD.1.d	○	○	○	○				
FMT_SMF.1	○		○					
FMT_SMR.1	○			○				
FPT_ITI.1		○						
FPT_RVM.1.T			○					
FPT_STM.1	○	○	○	○				
FIT_SOS.1				○				
FIT_MTD.1				○				
IT **環境セキュリティ機能要件**								
FCS_CKM.1					○			
FCS_CKM.4					○			
FCS_COP.1.H					○			
FCS_COP.1.C						○		
FDP_DAU_C.1						○		
FIA_AFL.1.BASIC								○
FIA_UAU.2.BASIC								○
FIA_UID.2.BASIC								○
FIA_AFL.1.SSL							○	
FIA_UAU.2.SSL							○	
FIA_UID.2.SSL							○	
FPT_RVM.1.BASIC								○
FPT_RVM.1.SSL							○	

表 24より、セキュリティ機能要件が、何らかのセキュリティ対策方針に対応している。

次に、セキュリティ対策方針が、セキュリティ機能要件によって実現できることを以下に説明する。

＜TOE セキュリティ対策方針＞

O.SIGNATURE (保護対象資産への署名付与)

FDP_DAU_T.1 により、TOE は、証明書検証結果が改ざんされていないことの保証として、証明書検証結果署名、及び、この署名を検証するための CVS 証明書を証明書検証結果に付与して一般利用者に提供する。なお、証明書検証結果署名の生成に必要な暗号操作機能は HSM により提供される。

証明書検証結果の有効性を保証する証拠である証明書検証結果署名を生成するためには、CVS 証明書が改ざんされていない事を保証することが必要となる。CVS 証明書に対する管理機能は、**FMT_SMF.1** により CVS 証明書の設定と規定され、CVS 証明書の設定に関する操作は **FMT_MTD.1.b** により、CVS 操作員のみが行えるように制限されている。また、**FMT_SMR.1** により、TOE はセキュリティ役割(CVS 操作員)を割り当てるための機能を提供する。以上により CVS 証明書を改ざんから保護できる。

また、証明書検証結果署名の付与が正しく行われたかを確認するために、TOE は監査対象事象に対応した監査ログを **FAU_GEN.1**、**FAU_GEN.2**、**FPT_STM.1** により生成し、証明書検証結果への署名付与の成否および CVS 証明書の登録･削除が行われたことを検出する。**FAU_SAR.1**、**FAU_SAR.2**、**FAU_SAR.3** により、CVS 操作員のみが監査対象事象に対応した監査ログから監査情報を検索･参照でき、監査ログの不正な参照は行われず、また、**FMT_MTD.1.d** により、CVS 操作員のみが監査ログを削除でき、監査ログの不正な削除は行われない。このため、監査ログのセキュリティを保証できる。

O.SIGVERIFY (取得データの署名検証)

FPT_ITI.1 により、TOE は、認証局から取得した認証局証明書及び失効リストの署名検証を行うことで、取得した認証局証明書及び失効リストの改変(改ざん)を検知する能力を持ち、改変を検知した場合はそのデータを使用しない。署名検証に必要な暗号操作機能は HSM により提供される。なお、OSCP 有効性検証サービスの場合、失効リストをサービス開始前に事前に登録または更新を行っており、不正な失効リストの取得が行われないことを保証する必要があるが、この場合の失効リストは、**FMT_MTD.1.c** によってシステム管理者のみが登録あるいは更新を行えるように制限されている。したがって不正な失効リストの取得は行われない。

また、認証局から取得した認証局証明書及び失効リストの署名検証が正しく行われたかを確認するために、TOE は監査対象事象に対応した監査ログを **FAU_GEN.1**、**FAU_GEN.2**、**FPT_STM.1** により生成し、認証局から取得した認証局証明書及び失効リストの改ざんの検

知および、失効リストの登録･更新の操作が行われたことを検出する。また **FAU_SAR.1**、**FAU_SAR.2**、**FAU_SAR.3** により、CVS 操作員のみが監査対象事象に対応した監査ログから監査情報を検索･参照でき、不正な利用者による監査ログの参照は行われず、また、**FMT_MTD.1.d** により、CVS 操作員のみが監査ログを削除でき、監査ログの不正な削除は行われない。このため、監査ログのセキュリティを保証できる。

O.I&A_SSL (SSL クライアント認証による識別と認証)

FIA_UID.2.T により、CVS 操作員が TOE の保護対象資産にアクセスする前に、CVS 操作員証明書 ID による識別が成功することを要求する。また、**FPT_RVM.1.T** により、この識別が迂回されずに成功することを保証する。

CVS 操作員認証に必要となる管理機能は、**FMT_SMF.1** により CVS 操作員の登録および削除と規定され、CVS 操作員の情報を記録した操作権限リストに対する操作は、**FMT_MTD.1.a** によりシステム管理者に制限されるため、不正な利用者による操作権限リストの改ざんは行われない。

また、操作権限リストに対する操作が問題なく行われているかを確認できるように、**FAU_GEN.1**、**FAU_GEN.2**、**FPT_STM.1** により、TOE は監査対象事象に対応した監査ログを生成し、CVS 操作員の識別の成否、及び、CVS 操作員の登録または削除の操作の結果を検出する。さらに、**FAU_SAR.1**、**FAU_SAR.2**、**FAU_SAR.3** により、CVS 操作員のみが監査対象事象に対応した監査ログから監査情報を検索･参照でき、不正な利用者による監査ログの参照は行われず、また、**FMT_MTD.1.d** により、CVS 操作員のみが監査ログを削除でき、監査ログの不正な削除は行われない。このため、監査ログのセキュリティを保証できる。

O.I&A_BASIC (ベーシック認証による識別と認証)

CVS 操作員認証において Apache が利用する IT 環境用データである操作権限リストに対する操作は、**FIT_MTD.1** により CVS 操作員に制限する。また、**FMT_SMR.1** により、TOE はセキュリティ役割(CVS 操作員)を割り当てるための機能を提供する。さらに、**FIT_SOS.1** により、CVS 操作員のパスワードが所定の品質尺度を確保していることを保証している。以上により、不正な利用者による操作権限リストの改ざんは行われない。

また、操作権限リストに対する操作が問題なく行われているかを確認できるように、**FAU_GEN.1**、**FAU_GEN.2**、**FPT_STM.1** により、TOE は監査対象事象に対応した監査ログを生成し、CVS 操作員の登録･削除または CVS 操作員情報の改変の操作が行われたことを検出する。また **FAU_SAR.1**、**FAU_SAR.2**、**FAU_SAR.3** により、CVS 操作員のみが監査対象事象に対応した監査ログから監査情報を検索･参照でき、不正な利用者による監査ログの参照は行われず、また、**FMT_MTD.1.d** により、CVS 操作員のみが監査ログを削除でき、監査ログの不正な削除は行われない。このため、監査ログのセキュリティを保証でき

る。

＜IT 環境セキュリティ対策方針＞

OE.HSM

FCS_COP.1.H により、HSM は指定されたアルゴリズムと鍵長にしたがって、証明書検証結果に対する署名生成に必要な処理である暗号操作及び証明書検証サービスを提供するために取得した認証局証明書及び失効リストの署名検証に必要な暗号操作を行う。また、**FCS_CKM.1** により、HSM は CVS 証明書の生成に必要となる CVS 秘密鍵の生成を行い、**FCS_CKM.4** により CVS 秘密鍵の破棄を行う。

OE.CLIENT

FDA_DAU_C.1 により、利用者側クライアントプログラムは、証明書検証結果応答の正当性の証拠である証明書検証結果署名について、CVS 証明書を利用して検証する機能を提供する。証明書検証結果署名に対する検証に必要な暗号操作は、**FCS_COP.1.C** により、指定されたアルゴリズムと鍵長にしたがって行う。以上により、利用者側クライアントプログラムは証明書検証結果署名の検証を実現できる。

OE.ADMIN_MACHINE

FIA_UID.2.SSL 及び **FIA_UAU.2.SSL** により、管理端末マシン上の OS は、提示された CVS 操作員証明書と PIN による識別･認証を実行する。**FIA_AFL.1.SSL** により、管理端末マシン上の OS は、識別･認証が 1 回でも失敗した場合、当該管理端末からのコネクションを終了する。また、**FPT_RVM.1.SSL** により、以上の識別･認証が迂回されないことを保証する。以上により、管理端末マシン上の OS は、CVS 操作員秘密鍵の PIN による識別･認証を実現できる。

OE.HTTPD_BASIC

FIA_UID.2.BASIC 及び **FIA_UAU.2.BASIC** により、Apache は、提示されたユーザ ID とパスワードによる識別･認証を実行する。**FIA_AFL.1.BASIC** により、Apache は、識別･認証が 1 回でも失敗した場合、当該管理端末からのコネクションを終了する。**FPT_RVM.1.BASIC** により､以上の識別･認証が迂回されないことを保証する｡以上により、Apache は、CVS 操作員のユーザ ID･パスワードによる識別･認証を実現できる。

8.2.2 セキュリティ機能要件依存性

セキュリティ機能要件のコンポーネントの依存性を表 25に示す。

表 25 セキュリティ機能要件のコンポーネントの依存性

セキュリティ機能要件	選択した依存コンポーネント	除去した依存コンポーネント
TOE セキュリティ機能要件		
FAU_GEN.1	FPT_STM.1	
FAU_GEN.2	FAU_GEN.1、FIA_UID.2(**後述**)	
FAU_SAR.1	FAU_GEN.1	
FAU_SAR.2	FAU_SAR.1	
FAU_SAR.3	FAU_SAR.1	
FDP_DAU_T.1	FDP_DAU_C.1	
FIA_UID.2.T	**なし**	
FMT_MTD.1.a	FMT_SMF.1	FMT_SMR.1 (**後述**)
FMT_MTD.1.b	FMT_SMF.1、FMT_SMR.1	
FMT_MTD.1.c	FMT_SMF.1	FMT_SMR.1 (**後述**)
FMT_MTD.1.d	FMT_SMF.1、FMT_SMR.1	
FMT_SMF.1	**なし**	
FMT_SMR.1	FIA_UID.2 (**後述**)	
FPT_ITI.1	**なし**	
FPT_RVM.1.T	**なし**	
FPT_STM.1	**なし**	
FIT_SOS.1	**なし**	
FIT_MTD.1	FMT_SMF.1、FMT_SMR.1	
IT **環境セキュリティ機能要件**		
FCS_CKM.1	FCS_COP.1、FCS_CKM.4	FMT_MSA.2 (**後述**)
FCS_CKM.4	FCS_CKM.1	FMT_MSA.2 (**後述**)
FCS_COP.1.H	FCS_CKM.1、FCS_CKM.4	FMD_MSA.2(**後述**)
FCS_COP.1.C	FCS_CKM.1、FCS_CKM.4	FMD_MSA.2(**後述**)
FDP_DAU_C.1	FIA_DAU_T.1	
FIA_AFL.1.BASIC	FIA_UAU.2(**後述**)	
FIA_UAU.2.BASIC	FIA_UID.2 (**後述**)	
FIA_UID.2.BASIC	**なし**	
FIA_AFL.1.SSL	FIA_UAU.2(**後述**)	
FIA_UAU.2.SSL	FIA_UID.2(**後述**)	
FIA_UID.2.SSL	**なし**	
FPT_RVM.1.BASIC	**なし**	
FPT_RVM.1.SSL	**なし**	

FIA_UID.2

本 ST では、**FAU_GEN.2**、**FIA_UAU.2.SSL**、**FIA_UAU.2.BASIC**、**FMT_SMR.1** の依存コンポーネントとして、CC で記述されている **FIA_UID.1** ではなく、その上位コンポーネントである **FIA_UID.2** を選択した。

FIA_UAU.2

本 ST では、**FIA_AFL.1.SSL**、**FIA_AFL.1.BASIC** の依存コンポーネントとして、CC で記述されている **FIA_UAU.1** ではなく、その上位コンポーネントである **FIA_UAU.2** を選択

した。

FMT_MSA.2

本 ST では、**FCS_CKM.1**、**FCS_CKM.4**、**FCS_COP.1.H**、**FCS_COP.1.C** の依存コンポーネントとして、**FMT_MSA.2** を取り扱わない。CVS 秘密鍵は、HSM 内部で生成され、HSM 外に漏洩することはない。そのため、**FMT_MSA.2** がなくとも、CVS 秘密鍵は常にセキュアな状態で使用できる。したがって、**FMT_MSA.2** は取り扱わない。

FMT_SMR.1

本 ST では、**FMT_MTD.1.a**、**FMT_MTD.1.c** の依存コンポーネントとして、**FMT_SMR.1** を取り扱わない。TOE は、システム管理者というセキュリティ役割を割り当てる機能を提供しない。したがって、**FMT_SMR.1** は取り扱わない。

8.2.3 セキュリティ機能要件相互補完性

表 26に、TOE セキュリティ機能要件の相互作用の関係について検証する。

表 26 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要件			
TOE セキュリティ機能要件	迂回	改ざん	非活性化	無効化
FAU_GEN.1	N/A	N/A	N/A	N/A
FAU_GEN.2	N/A	N/A	N/A	N/A
FAU_SAR.1	N/A	N/A	N/A	N/A
FAU_SAR.2	N/A	N/A	N/A	FAU_GEN.1
FAU_SAR.3	N/A	N/A	N/A	N/A
FDP_DAU_T.1	N/A	N/A	N/A	FAU_GEN.1
FIA_UID.2.T	FPT_RVM.1.T	N/A	N/A	FAU_GEN.1
FMT_MTD.1.a	N/A	N/A	N/A	FAU_GEN.1
FMT_MTD.1.b	N/A	N/A	N/A	FAU_GEN.1
FMT_MTD.1.c	N/A	N/A	N/A	FAU_GEN.1
FMT_MTD.1.d	N/A	N/A	N/A	FAU_GEN.1
FMT_SMF.1	N/A	N/A	N/A	FAU_GEN.1
FMT_SMR.1	N/A	N/A	N/A	N/A
FPT_ITI.1	N/A	N/A	N/A	FAU_GEN.1
FPT_RVM.1.T	N/A	N/A	N/A	N/A
FPT_STM.1	N/A	N/A	N/A	N/A
FIT_SOS.1	N/A	N/A	N/A	FAU_GEN.1
FIT_MTD.1	N/A	N/A	N/A	FAU_GEN.1
IT **環境セキュリティ機能要件**				
FCS_CKM.1	N/A	N/A	N/A	N/A
FCS_CKM.4	N/A	N/A	N/A	N/A
FCS_COP.1.H	N/A	N/A	N/A	N/A
FCS_COP.1.C	N/A	N/A	N/A	N/A
FDP_DAU_C.1	N/A	N/A	N/A	N/A
FIA_AFL.1.BASIC	FPT_RVM.1.BASIC	N/A	N/A	N/A
FIA_UAU.2.BASIC	FPT_RVM.1.BASIC	N/A	N/A	N/A
FIA_UID.2.BASIC	FPT_RVM.1.BASIC	N/A	N/A	N/A
FIA_AFL.1.SSL	FPT_RVM.1.SSL	N/A	N/A	N/A
FIA_UAU.2.SSL	FPT_RVM.1.SSL	N/A	N/A	N/A
FIA_UID.2.SSL	FPT_RVM.1.SSL	N/A	N/A	N/A
FPT_RVM.1.BASIC	N/A	N/A	N/A	N/A
FPT_RVM.1.SSL	N/A	N/A	N/A	N/A

凡例:N/A･･･Not Applicable

迂回

CVS 操作員が TOE にアクセスする場合は Apache を経由する以外の方法は存在しない。

CVS 操作員認証にベーシック認証を利用している場合、CVS 操作員が TOE を利用する場合は、**FPT_RVM.1.BASIC** により、必ず先に **FIA_UID.2.BASIC**、**FIA_UAU.2.BASIC** が呼び出され、識別･認証を迂回することはできず、認証失敗時にも **FIA_AFL.1.BASIC** が

呼び出される。

CVS 操作員認証に SSL クライアント認証を利用している場合、CVS 操作員が TOE を利用する場合は、**FPT_RVM.1.SSL** により、必ず先に **FIA_UID.2.SSL**、**FIA_UAU.2.SSL** が呼び出され、管理端末マシン上の OS による識別･認証を迂回することはできず、認証失敗時にも **FIA_AFL.1.SSL** が呼び出される。

また、TOE による識別の際にも、**FPT_RVM.1.T** により、必ず先に **FIA_UID.2.T** が呼び出され、TOE による識別を迂回することはできない。

改ざん

システム管理者のインタフェースは、内部に閉じられたものであるため不信なサブジェクトは存在しない。

CVS 操作員のインタフェースは、CVS 操作員に対する識別･認証を迂回されることなく実施しているため、不正な利用者に対してインタフェースの利用を許可することはない。

また、一般利用者のインタフェースは、証明書検証要求の送信および証明書検証結果応答の取得に限定されたインタフェースであり、TOE の改ざんを可能とするインタフェースではない。

したがって、改ざんへの対応を必要としない。

非活性化

本 TOE の TSF データに対するインタフェースはシステム管理者か、認証･識別機能によって特定された CVS 操作員のみに限定して提供される。

したがって、非活性化への対応を必要としない。

無効化

本 TOE の TSF データに対する無効化については、**FAU_GEN.1** により、監査データ生成に関わるセキュリティ機能要件の無効化を狙った攻撃の検出が可能になる。**FAU_GEN.1** により、セキュリティ侵害に繋がる不正行為を抑止する。

8.2.4 拡張セキュリティ機能要件根拠

FDP_DAU_T.1、FDP_DAU_C.1

本 ST では、利用者データ保護におけるデータの真正性確保に係る機能要件コンポーネントとして、既存の基本データ認証(**FDP_DAU.1**)をベースに、その同等の機能を TOE と IT 環境の協調によって実現する機能エレメントに分割した新たな機能要件コンポーネント **FDP_DAU_T.1、FDP_DAU_C.1** を設けている。 その根拠は、以下のとおりである。

- 必要とされる本質的な要件は、利用者データの真正性の確保であり、TSF 保護を取り扱う FPT クラスの既存コンポーネントの適用は適切ではない。

- 対象の利用者データは、TOE から IT 環境に渡されるものであり、その意味で通信上のデータ交換を扱う FCO クラスの既存コンポーネントの適用も考えられるが、FCO クラスは、通信中のデータ交換と送信者・受信者の識別保証が主な目的であるため、受け渡しされる利用者データそのものの真正性確保を、通信中に限定せず、実現する目的への適用は適切ではない。
- 利用者データ保護を取り扱う FDP クラスの中に、類似の機能要件として、**FDP_ETC**、**FDP_UIT** があるが、前者は TSF 外へのエクスポートを対象としている点、後者は TSF 間の転送を対象としている点で、利用者への応答データを保護する場合の適用は相応しくない。

以上から、利用者データの真正性を取り扱う機能要件として、FDP クラスの **FDP_DAU**(データ認証)が最適であると考えられるが、既存のコンポーネントは TSF 内に閉じたデータの真正性を取扱うものであり、今回のように TOE と IT 環境が協調して実現する機能要件としては適用することができないため、既存の機能要件コンポーネント **FDP_DAU.1** の機能エレメントを、各々対応する TOE の機能要件（証拠の生成）、IT 環境の機能要件（証拠の検証）に分離分割して、新たな機能要件コンポーネントとして設定したものである。

なお、この拡張セキュリティ機能要件は、既存の **FDP_DAU.1** を分離分割しただけのものであり、本 TOE の評価保証レベル EAL2 で特定されるセキュリティ保証要件に対して、新たな保証要件や評価方法を必要とするものではなく、EAL2 の保証要件がそのまま適用できる。

FIT_SOS.1、**FIT_MTD.1**

本 ST では、IT 環境の秘密の検証に関する機能要件コンポーネントとして、**FIA_SOS.1** をベースとした新たな機能要件コンポーネントとして **FIT_SOS.1** を設けている。また、IT 環境の識別認証用データの管理に関する機能要件コンポーネントとして、**FMT_MTD.1** をベースとした新たな機能要件コンポーネントとして **FIT_MTD.1** を設けている。その根拠は以下の通りである。

- OE.HTTPD_BASIC が正しく認証を実行できるようにするためには、IT 環境の識別認証用データである操作権限リスト(ベーシック認証用)の管理を CVS 操作員のみに限定する必要があるので、IT 環境の秘密の検証及び IT 環境の識別認証用データを管理するための TOE セキュリティ機能要件が必要となる。
- 操作権限リスト(ベーシック認証用)は、IT 環境である Apache の識別認証用データであるとともに IT 環境の秘密であり、TOE から見れば利用者データである。
- このようなデータを TOE の FIA クラス及び FMT クラスでは扱えない。FDP クラスの適用が考えられるが、本 TOE においては、CVS 操作員にはセキュリティ属性として

管理する TSF データが存在しないため、FDP_ACC 及び FDP_ACF の適用が困難であり、新たな機能要件を定義する必要がある。

- また、IT 環境の識別認証用データである操作権限リスト(ベーシック認証用)は、TOE と IT 環境である Apache で共有される OS 管理のファイルであり、このファイルは OS 環境においてシステム管理者しかアクセスできないため、そのデータ保護については、FMT クラスでの管理要件以上のセキュリティ上の配慮は不要である。以上から、FIA_SOS.1、FMT_MTD.1 をベースに新たな機能要件を設定したものである。

なお、これらの拡張セキュリティ機能要件は、既存の CC パート 2 で規定されているセキュリティ機能要件をベースとしたものであり、本 TOE の評価保証レベル EAL2 で特定されるセキュリティ保証要件に対して、新たな保証要件や評価方法を必要とするものではなく、EAL2 の保証要件がそのまま適用できる。

8.2.5 最小機能強度レベル根拠

「3.2.1 脅威エージェント」で述べたように、脅威エージェントは高度な専門知識を持たず、攻撃用の特別なツールを利用することも無いと想定される。したがって、TOE の最小機能強度は、SOF-基本が妥当である。

8.2.6 セキュリティ保証要件根拠

本 TOE の証明書検証部分は、外部ネットワーク及び物理的なアクセスから保護され、かつ、信頼できる管理者により運用されることを前提としており、運用／管理面で十分なセキュリティが確保できる。残る TOE 部分はクライアント PC との通信機能であり、厳密に機密として管理されるべきデータはない。したがって EAL2 は適当である。

8.3 TOE 要約仕様根拠

8.3.1 TOE セキュリティ機能根拠

表 12より、全ての TOE セキュリティ機能が、何らかの IT セキュリティ機能要件を実現するために必要であることが示される。

FAU_GEN.1 監査データ生成

SF.AUDIT が要件を満たす。

＜根拠＞

SF.AUDIT は、表 13、表 14、表 17、表 18に示した監査対象事象の監査ログを生成する。

「6.1.8 監査機能 (SF.AUDIT)」で述べた通り、各機能要件の監査対象とすべきアクションは、例外を除いて、本 TOE の監査対象事象として記録している。

また、例外に関しても CC パート 2 で規定された監査対象とすべき最小レベルのアクションのうち、本 TOE において監査対象事象に含まれない根拠を説明している。

また、監査機能の起動と終了は、証明書検証サービス管理の起動と停止として記録している。

したがって **SF.AUDIT** により、**FAU_GEN.1** を実現できる。

FAU_GEN.2 利用者識別情報の関連付け

SF.AUDIT が要件を満たす。

＜根拠＞

SF.AUDIT は、監査記録時に、システム管理者あるいは CVS 操作員の ID、またはクライアント PC の IP アドレスあるいはトランザクション ID を記録することによって、当該事象を、その原因となった操作を行ったサブジェクトに関連付けている。

したがって **SF.AUDIT** により、**FAU_GEN.2** を実現できる。

FAU_SAR.1 監査レビュー

SF.AUDIT が要件を満たす。

＜根拠＞

SF.AUDIT は、CVS 操作員に個別に定義した監査対象事象を記録した監査ログの参照を許可する。また、**SF.AUDIT** は、TOE が記録する監査情報を、それぞれ表 13、表 17および表 19で示した形式で表示する機能を提供する。したがって **SF.AUDIT** により、**FAU_SAR.1** を実現できる。

FAU_SAR.2 限定監査レビュー

SF.AUDIT が要件を満たす。

＜根拠＞

SF.AUDIT は、CVS 操作員にのみ個別に定義した監査対象事象を記録した監査ログの参照を許可し、CVS 操作員以外が個別に定義した監査対象事象を記録した監査ログを参照することはできない。

したがって **SF.AUDIT** により、**FAU_SAR.2** を実現できる。

FAU_SAR.3 選択可能監査レビュー

SF.AUDIT が要件を満たす。

＜根拠＞

SF.AUDIT により、TOE は監査事象の発生日時及び事象種別を条件として個別に定義した監査対象事象を記録した監査ログを検索する機能を提供する。

したがって **SF.AUDIT** により、**FAU_SAR.3** を実現できる。

FDP_DAU_T.1 基本データ認証(証拠の生成)

SF.SIGNATURE が要件を満たす。

＜根拠＞

SF.SIGNATURE により、TOE は、証明書検証結果に対して、その有効性の証拠として、証明書検証結果署名を生成し、署名検証に必要となる CVS 証明書とともに証明書検証結果に付与して、一般利用者へ提供する。

したがって **SF.SIGNATURE** により、**FDP_DAU_T.1** を実現できる。

FIA_UID.2.T アクション前の利用者識別

SF.I&A_SSL が要件を満たす。

＜根拠＞

CVS 操作員認証**に** SSL クライアント認証を利用する場合は **SF.I&A_SSL** により、CVS 操作員が識別に成功して TOE に接続しない限り、TOE は、CVS 操作員による TOE の利用を許可することはない。

したがって **SF.I&A_SSL** により、**FIA_UID.2.T** を実現できる。

FMT_MTD.1.a TSF データの管理

SF.CVS_MGT_SSL が要件を満たす

＜根拠＞

SF.CVS_MGT_SSL により、TOE は操作権限リスト(SSL クライアント認証用)に対するレコード追加とレコード削除の操作をシステム管理者に制限する。

したがって **SF.CVS_MGT_SSL** により、**FMT_MTD.1.a** を実現できる

FMT_MTD.1.b TSF データの管理

SF.CVS_MGT_COMMON が要件を満たす

＜根拠＞

SF.CVS_MGT_COMMON により、TOE は CVS 証明書の削除・登録の操作を CVS 操作員に制限する。

したがって **SF.CVS_MGT_COMMON** により、**FMT_MTD.1.b** を実現できる

FMT_MTD.1.c TSF データの管理

SF.CVS_MGT_CRL が要件を満たす

＜根拠＞

SF.CVS_MGT_CRL により、TOE は OCSP 有効性検証に利用する失効リストの登録・更新の操作をシステム管理者に制限する。

したがって **SF.CVS_MGT_CRL** により、**FMT_MTD.1.c** を実現できる

FMT_MTD.1.d TSF データの管理

SF.AUDIT が要件を満たす。

＜根拠＞

SF.AUDIT は、監査ログの削除の操作を CVS 操作員に制限する。

したがって **SF.AUDIT** により、**FMT_MTD.1.d** を実現できる。

FMT_SMF.1 管理機能の特定

SF.CVS_MGT_SSL、**SF.CVS_MGT_COMMON** が要件を満たす。

＜根拠＞

SF.CVS_MGT_SSL、**SF.CVS_MGT_COMMON** は、TSF データに対するセキュリティ管理機能を提供する。

各機能要件の管理対象とすべきアクティビティは､例外を除いて全て **SF.CVS_MGT_SSL**、**SF.CVS_MGT_COMMON** のいずれかで管理している。また、例外に関しても CC パート 2 で規定された管理対象とすべきアクティビティが、本 TOE において管理対象事象に含まれない根拠を説明している。

したがって **SF.CVS_MGT_SSL**、**SF.CVS_MGT_COMMON** により、**FMT_SMF.1** を実現できる。

FMT_SMR.1 セキュリティ役割

CVS 操作員認証のそれぞれのモードで **SF.I&A_SSL** と **SF.CVS_MGT_SSL**、または **SF.CVS_MGT_BASIC** が要件を満たす。

＜根拠＞

CVS 操作員認証に SSL クライアント認証を利用する場合は **SF.CVS_MGT_SSL**、ベーシック認証を利用する場合は **SF.CVS_MGT_BASIC** によって、CVS 証明書を操作する権限を持つ操作員を、CVS 操作員という役割として設定し、維持する。また、CVS 操作員認証に SSL クライアント認証を利用する場合は **SF.I&A_SSL** によって、識別･認証に成功した利用者を CVS 操作員と関連付ける。

したがって、**SF.I&A_SSL** と **SF.CVS_MGT_SSL**、または **SF.CVS_MGT_BASIC** により、**FMT_SMR.1** を実現できる。

FPT_ITI.1 TSF 間改変の検出

SF.SIGVERIFY、**SF.CVS_MGT_CRL** が要件を満たす。

＜根拠＞

SF.SIGVERIFY は、証明書検証サービスを提供するために取得した認証局証明書及び失効リストと、これらのデータに付与された署名に対して、署名検証を行うことで、リモート高信頼 IT 製品であるリポジトリから送信される TSF データである認証局証明書及び失効リストに対する任意の改変を検出する。また改変を検知した場合には、その認証局証明書及び失効リストを証明書の検証に使用しない。

SF.CVS_MGT_CRL は、OCSP 有効性検証サービスを提供するために取得した失効リストと、これらのデータに付与された署名に対して、署名検証を行うことで、リモート高信頼 IT 製品であるリポジトリから送信される TSF データである失効リストに対する任意の改変を検出する。また改変を検知した場合には、その認証局証明書及び失効リストを証明書の検証に使用しない。

したがって **SF. SIGVERIFY**、**SF.CVS_MGT_CRL** により、**FPT_ITI.1** を実現できる。

FPT_STM.1 高信頼タイムスタンプ

SF.AUDIT が要件を満たす。

＜根拠＞

SF.AUDIT は、監査ログの記録に必要なタイムスタンプ情報を提供する。

したがって **SF.AUDIT** により、**FPT_STM.1** を実現できる。

FPT_RVM.1.T TSP の非バイパス性

SF.I&A_SSL が要件を満たす。

＜根拠＞

SF.I&A_SSL は、管理端末マシンの OS 上において CVS 操作員証明書と特定の CVS 操作員との一意性が PIN による識別･認証により保証された後、CVS 操作員証明書 ID が操作権限リストにあることを確認することで CVS 操作員を識別する。この識別の成功後に、TOE は当該 CVS 操作員を代行プロセスに関連付ける。よって、TSC 内の各機能の動作が許可される前に、TSP 実施機能が呼び出されて成功することが保証され、バイパスを防止できる。

したがって **SF.I&A_SSL** により、**FPT_RVM.1.T** を実現できる。

FIT_SOS.1 IT 環境の秘密の検証

SF.CVS_MGT_BASIC が要件を満たす。

＜根拠＞

CVS 操作員認証にベーシック認証を利用する場合は **SF.CVS_MGT_BASIC** により、TOE は Apache が CVS 操作員を認証するためのパスワードを設定する時に、**FIT_SOS.1** で定めた品質尺度を満たしていることの検証を行う。

したがって **SF.CVS_MGT_BASIC** により、**FIT_SOS.1** は実現できる

FIT_MTD.1 IT 環境用データの管理

SF.CVS_MGT_BASIC が要件を満たす

＜根拠＞

SF.CVS_MGT_BASIC により、TOE は IT 環境用データである操作権限リスト(ベーシック認証用)に対する CVS 操作員の登録、CVS 操作員のパスワードの改変、CVS 操作員の削除の操作を CVS 操作員に制限する。

したがって **SF.CVS_MGT_BASIC** により、**FIT_MTD.1** を実現できる

8.3.2 セキュリティ機能強度根拠

本 ST の IT セキュリティ要件における最小機能強度には SOF-基本を指定している。明示された機能強度に指定されたメカニズムは、CVS 操作員の識別･認証機能だけであり、SOF-基本を指定している。

本メカニズムに対する IT セキュリティ機能は **SF.CVS_MGT_BASIC** で実現されており、これらの機能強度は SOF-基本である。したがって、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」の表 21、表 22に示したように、EAL2 で必要とする全ての 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、保証手段によって、本 ST で規定した 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。したがって、EAL2 における TOE セキュリティ保証要件が要求している証拠に合致している。

ACM_CAP.2(構成要素)

証明書検証サーバ構成管理文書は以下の内容を含む。

- TOE を構成する全ての構成要素と、その一意な識別を示した構成リスト

したがって、証明書検証サーバ構成管理文書により **ACM_CAP.2** を実現できる。

ADO_DEL.1(配布手続き)

証明書検証サーバ配布文書は以下の内容を含む。

- TOE を利用者サイトへ配送するときにセキュリティを維持するために必要な全ての手続き

したがって、証明書検証サーバ配布文書により **ADO_DEL.1** を実現できる。

ADO_IGS.1(設置、生成、及び立上げ手順)

証明書検証サーバ操作の手引き(Linux 版、Solaris 版)及びソフトウェア添付資料(Linux 版、Solaris 版)は以下の内容を含む。

- TOE のセキュアな設置、生成、及び立上げのために必要な全てのステップ

したがって、証明書検証サーバ操作の手引き及びソフトウェア添付資料により **ADO_IGS.1** を実現できる。

ADV_FSP.1(非形式的機能仕様)

証明書検証サーバ機能仕様書は以下の内容を含む。

- 非形式的な様式による、全ての外部 TSF インタフェースの目的と使用方法に関する記述

したがって、証明書検証サーバ機能仕様書により **ADV_FSP.1** を実現できる。

ADV_HLD.1(記述的上位レベル設計)

証明書検証サーバ構造設計書は以下の内容を含む。

- TSF が必要とする全てのハードウェア、ファームウェア及びソフトウェアの識別
- TSF が必要とする全てのハードウェア、ファームウェア及びソフトウェアに実装されている補助的な保護メカニズムによって提供される機能
- TSF のサブシステムに対する全てのインタフェース識別

したがって、証明書検証サーバ構造設計書により **ADV_HLD.1** を実現できる。

ADV_RCR.1(非形式対応の実証)

証明書検証サーバ対応分析書は以下の内容を含む。

- 提供された TSF 表現の隣接する各々の組に対するセキュリティ機能性に関する分析

したがって、証明書検証サーバ対応分析書により **ADV_RCR.1** を実現できる。

AGD_ADM.1(管理者ガイダンス)

証明書検証サーバ操作の手引き(Linux 版、Solaris 版)及びソフトウェア添付資料(Linux 版、Solaris 版)は以下の内容を含む。

- TOE の管理者がセキュアに TOE を管理するために利用できる管理機能とインタフェース
- 管理者に関連する、IT 環境での全てのセキュリティ要件

したがって、証明書検証サーバ操作の手引き及びソフトウェア添付資料により **AGD_ADM.1** を実現できる。

AGD_USR.1(利用者ガイダンス)

証明書検証サーバ操作の手引き(Linux 版、Solaris 版)及びソフトウェア添付資料(Linux 版、Solaris 版)は以下の内容を含む。

- TOE の非管理者である利用者が利用できる機能とインタフェース
- TOE により提供された、利用者がアクセスできるセキュリティ機能の使用法

したがって、証明書検証サーバ操作の手引き及びソフトウェア添付資料により **AGD_USR.1** を実現できる。

ATE_COV.1(カバレージの証拠)

証明書検証サーバテスト分析書は以下の内容を含む。

- テスト証拠資料で識別されたテストと機能仕様に記述された TSF との対応

したがって、証明書検証サーバテスト分析書により **ATE_COV.1** を実現できる。

ATE_FUN.1(機能テスト)

証明書検証サーバテスト仕様書、証明書検証サーバテスト報告書は以下の内容を含む。

- テスト計画、テスト手順記述、期待されるテスト結果及び実際のテスト結果

したがって、証明書検証サーバテスト仕様書／報告書により **ATE_FUN.1** を実現できる。

ATE_IND.2(独立試験・サンプル)

TOE(Linux 版、Solaris 版)は以下の内容を含む。

- TSF の開発者機能テストで使用されたものと同等の一連の資源

したがって、TOE により **ATE_IND.2** を実現できる。

AVA_SOF.1(TOE セキュリティ機能強度評価)

証明書検証サーバセキュリティ強度分析書は以下の内容を含む。

- TOE セキュリティ機能強度主張を有する各メカニズムに対する、セキュリティ機能強度の分析結果

したがって、証明書検証サーバ脆弱性分析書により **AVA_SOF.1** を実現できる。

AVA_VLA.1(開発者脆弱性分析)

証明書検証サーバ脆弱性分析書は以下の内容を含む。

- 利用者が TSP を侵害し得る明白な方法を探すために行われた TOE 提供物件の分析

したがって、証明書検証サーバ脆弱性分析書により **AVA_VLA.1** を実現できる。

8.4 PP **主張根拠**

参照した PP はない。