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

申請受付日（受付番号）	**平成19年5月2日** (IT**認証**7149)
認証番号	C0135
認証申請者	**株式会社 日立製作所**
TOE**の名称**	**証明書検証サーバ**
TOE**のバージョン**	03-00
PP**適合**	**なし**
適合する保証パッケージ	EAL2
開発者	**株式会社 日立製作所**
評価機関の名称	**有限責任中間法人　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12月26日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

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

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「証明書検証サーバ 03-00」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「証明書検証サーバ 03-00」（以下「本TOE」という。）について有限責任中間法人　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株式会社日立製作所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。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

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

1.2.2 製品概要

TOEは一般利用者からの証明書検証要求に対して、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（以降、証明書検証サーバ）であり、以下の2種類のサービスを提供する（TOE運用者は以下のサービスのどちらかを選択し、一般利用者に提供する）。

・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）

また、TOEは以下のセキュリティ機能を提供する。

・データ保護機能
・データ改ざんチェック機能
・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

1.2.3 TOEの範囲と動作概要

(1) TOE動作環境

図1-1にTOEを利用したシステム構成を示す。

なお、以降使用されるCVS（Certificate Validation Server）はTOEである証明書検証サーバを示す。

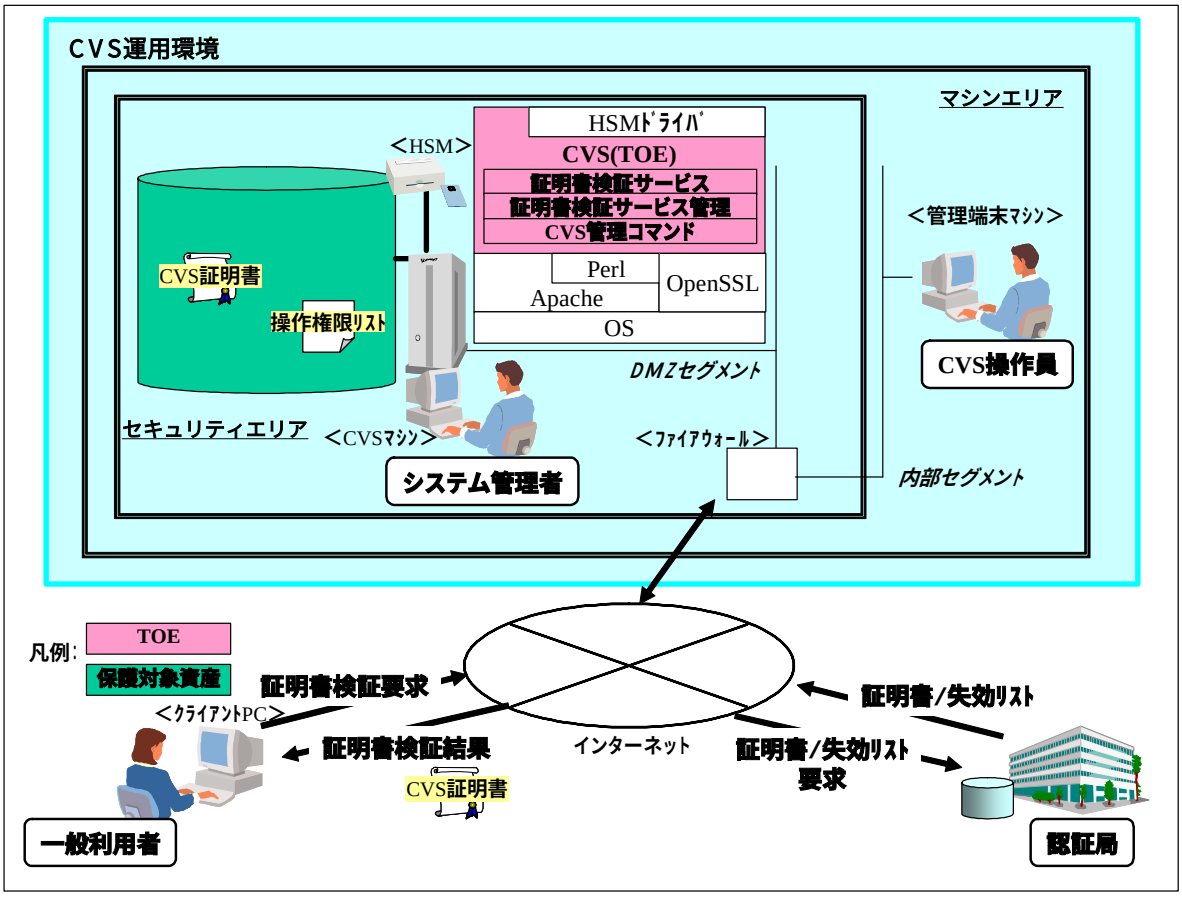


図1-1　TOEを利用したシステム構成

以下に、システムを構成する各要素について説明する。

【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。また、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。

【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。

【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。CVSマシンはセキュリティエリア内に設置される。

また、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。

【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。

【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。

【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。

【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。

図1-1のシステムにおける証明書検証サービスの動作概要について示す。証明書検証サービスは以下の3段階のフェーズにより実現される。

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、クライアントPCからCVSに依頼する。

②証明書検証

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証明書検証結果応答

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。

(2) TOEの範囲

図1-1に示すとおり、TOEはCVSマシン上に実装されるアプリケーションソフトウェアであり、同様にCVS上に構築される他のソフトウェア（OS、Apache、HSMドライバ等）と共に、証明書検証サービス及びセキュリティ機能を提供する。

1.2.4 TOEの機能

TOEである証明書検証サーバは、図1-1に示すように、証明書検証サービス、証明書検証サービス管理、及びCVS管理コマンドの３つの論理モジュールにより構成される。以下では各構成モジュールが提供する機能について述べる。

【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。

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セキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[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「証明書検証サーバ (Certificate Validation Server) 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]のいずれか) 附属書B、CCパート2（[6][9][12]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]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、「株式会社 日立製作所 証明書検証サーバ 03-00 Linux版およびSolaris版 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]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12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、EAL2適合である。

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、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に対抗することが意図されているため、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。

(1) データ保護機能

TOEが生成した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、予めCVSに登録されている署名検証のためのCVS証明書を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TOE外のモジュールであるHSMを用いる。

証明書検証結果を受信した一般利用者は、クライアントPC上のクライアントプログラムを使用して証明書検証結果署名を検証し、証明書検証結果が改ざんされていないことを確認できる。

(2) データ改ざんチェック機能

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。

なお、署名検証に必要な処理の一部である暗号操作にはTOE外のモジュールであるHSMを用いる。

(3) 識別・認証機能

管理端末マシンからCVSに対してアクセスし、各種管理機能を使用する際には、CVS操作員に対して下記の手順で識別認証を実施する。

① 管理端末マシン上で、予め登録されたCVS操作員秘密鍵（CVS操作員毎に登録）に対するPIN認証を実施する
② 管理端末マシンから送付されたCVS操作員証明書を使用し、SSLクライアント認証を実施する
③ 管理端末マシンから送付されたCVS操作員証明書のSubject DN が、TOEが管理する操作権限リスト内に記録されたCVS操作員証明書のSubject DNと一致することの確認を行い、CVS操作員の識別を行う
④ 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

なお、上記①、②の認証機能は、それぞれTOE外である管理端末マシンOS、及びApacheにより実施される。

また、上記識別・認証機能（以降、SSLクライアント認証を利用した識別認証と記す）以外にも、IT環境であるApacheが提供するベーシック認証による識別・認証機能（以降、ベーシック認証を利用した識別認証と記す）を選択することも可能であり、運用者はTOEのインストール時にどちらの機能を使用するか決定し、それ以降は変更が不可能となる。ベーシック認証を利用した識別認証機能を選択した場合は、識別認証に関するTOEのセキュリティ機能として、後述するCVS操作員情報管理機能のみ提供される。

(4) CVS操作員情報管理機能

使用される識別・認証機能の方式によって、下記機能を提供する。

SSLクライアント認証を利用した識別認証機能の場合：

TOEによるCVS操作員識別処理において使用されるCVS操作員証明書のSubject DNを、TOEが管理する操作権限リストに登録するための、CVS操作員登録、削除機能を提供する。

ベーシック認証を利用した識別認証機能の場合：

Apacheによるベーシック認証で使用されるユーザID、パスワードをTOEが管理する操作権限リストに登録するための、CVS操作員登録、削除、パスワード変更機能を提供する。またパスワード変更時に入力されたパスワードが、TOEが要求する品質尺度を満たしているかどうかの検証を行い、満たさない場合は再度パスワードの設定を要求する。

(5) CVS証明書管理機能

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

(6) 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。

(7) 監査機能

TOE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。

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.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。

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はない。

1.5.7 構成条件

TOEは図1-1の環境において必要となるハードウェア構成を表1-2に、ソフトウェア構成を表1-3に示す。なお、TOEがサポートする動作プラットフォームとしてLinux、及びSolarisの2種類が存在するため、プラットフォーム毎に表記する。

表1-2 ハードウェア構成

（Linux環境）

名称	ハードウェア仕様
CVSマシン	Red Hat Enterprise Linux ES 4.0 (x86版)
	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OpenSSL0.9.7m以降が稼動するマシン
	インタプリタとしてPerl5(jcode.pl v2.0及びCGI.pmを含む)が稼動するマシン
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
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)
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
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

（Solaris環境）

名称	ハードウェア仕様
CVSマシン	Sun Solaris 9(SPARC版)
	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OpenSSL0.9.7m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
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
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)
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
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1-3 ソフトウェア構成

（Linux環境）

搭載マシン	ソフトウェア種別	名称
CVSマシン	OS	Red Hat Enterprise Linux ES4.0 (x86版)
	Webサーバ	Apache 2.0.58 以降
	暗号ライブラリ	OpenSSL 0.9.7m以降
	インタプリタ	Perl 5(jcode.pl v2.0及びCGI.pmを含む)
	証明書検証サーバ	証明書検証サーバ 03-00 (Linux版)
	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
管理端末マシン	Webブラウザ	Microsoft Internet Explorer 6.0
	OS	Microsoft Windows XP
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

[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

（Solaris環境）

搭載マシン	ソフトウェア種別	名称
CVSマシン	OS	Sun Solaris 9 (SPARC版)
	Webサーバ	Apache 2.0.58以降
	暗号ライブラリ	OpenSSL 0.9.7m以降
	インタプリタ	Perl 5(jcode.pl v2.0及びCGI.pmを含む)
	証明書検証サーバ	証明書検証サーバ 03-00(Solaris版)
	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
管理端末マシン	Webブラウザ	Microsoft Internet Explorer 6.0
	OS	Microsoft Windows XP
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

[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

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1-4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1-4 TOE使用の前提条件

識別子	前提条件
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。

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。

- 証明書検証サーバ操作の手引き

J-A-793-80 (Solaris版)
J-A-919-60 (Linux版)

- ソフトウェア添付資料

C-940R-11 証明書検証サーバ 03-00 ソフトウェア添付資料 (Solaris版)
C-940R-19 証明書検証サーバ 03-00 ソフトウェア添付資料 (Linux版)

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19年5月に始まり、平成19年12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19年8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19年8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において使用された構成を表2-1に示す。

表2-1 開発者テスト構成

（Linux環境）

搭載マシン	ハードウェア/ソフトウェア構成
CVSマシン	HITACHI FLORA 310
	OS : Red Hat Enterprise Linux ES4.0 (x86版)
	Apache 2.0.58
	OpenSSL 0.9.7m
	Perl 5.8.5(jcode.pl v2.0及びCGI.pm3.29)
	TOE： 証明書検証サーバ 03-00 (Linux版)
	HSMドライバ: nCipher Support Software for Linux 10.15 Luna SA Security Software for Linux 4.0
管理端末マシン	HITACHI FLORA 310
	Microsoft Internet Explorer 6.0
	Microsoft Windows XP
HSM	nCipher netHSM SafeNet Luna SA
ファイアウォール	＊テスト環境ではファイアウォールを使用しない
クライアントPC	HITACHI FLORA 310
	証明書検証クライアントライブラリ for Java 02-30

（Solaris環境）

搭載マシン	ハードウェア/ソフトウェア構成
CVSマシン	Sun Ultra 10
	OS : Sun Solaris 9 (SPARC版)
	Apache 2.0.58
	OpenSSL 0.9.7m
	Perl 5.8.5(jcode.pl v2.0及びCGI.pm3.29)
	TOE： 証明書検証サーバ 03-00 (Solaris版)
	HSMドライバ: nCipher Support Software for Linux 10.15 Luna SA Security Software for Linux 4.0
管理端末マシン	HITACHI FLORA 310
	Microsoft Internet Explorer 6.0
	Microsoft Windows XP
HSM	nCipher netHSM

	SafeNet Luna SA
ファイアウォール	＊テスト環境ではファイアウォールを使用しない
クライアントPC	HITACHI FLORA 310
	証明書検証クライアントライブラリ for Java 02-30

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表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構成と同等のハードウェア及びソフトウェア構成のテスト環境で実施された。以下は、テスト構成がSTにおいて識別されている構成と完全には一致しない部分について、同等であるとみなせる理由である。

表2-1に示したテスト構成では、STにおいて識別されているファイアウォールによるパケットフィルタリングが実施されていない。しかしファイアウォールはCVSマシン、及び管理端末マシンのセキュリティ確保のために必要な装置であるため、外部ネットワークから切り離されたLAN環境で構築された本テスト環境においては必要ない。従って本テスト環境はSTで識別されるTOE構成環境と同等であるとみなすことができる。

b.テスト手法

テストとして、実際の運用により使用されるユーザインタフェース（クライアントからの証明書検証要求、管理端末からのコマンド入力、CVS操作端末からのWebインタフェース操作）を刺激し、セキュリティ機能のふるまいを下記の手段により確認する手法が使用された。

- 操作画面上（クライアントソフト、コンソール、Web画面）での出力結果、動作結果の確認
- インタフェース出力データの解析（証明書検証結果等）
- ログ出力データでの確認

c.実施テストの範囲

テストは開発者によって656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。

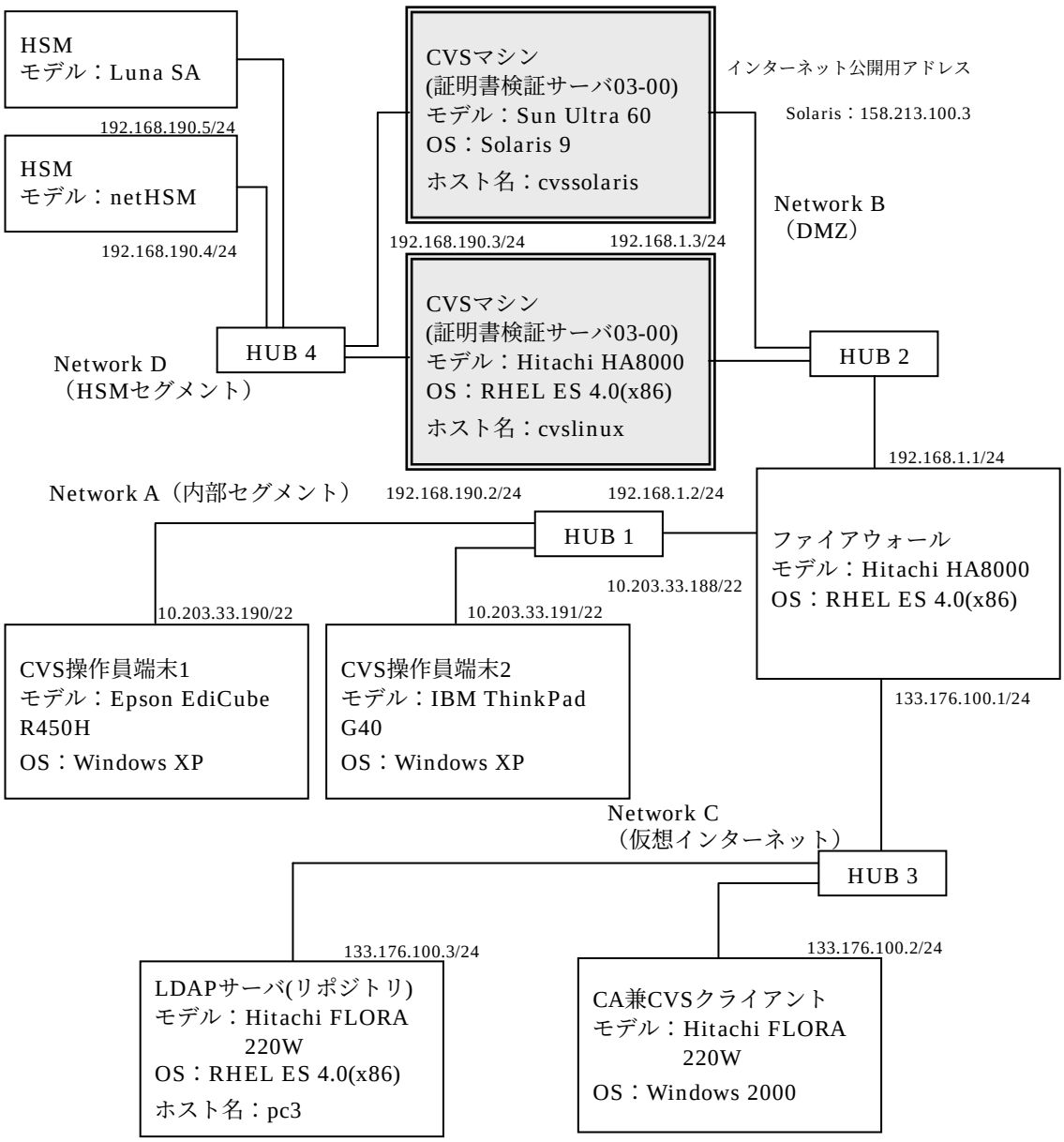
d.結果

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図を図2-1に示す。



注　CVSマシンについてLinux版CVSのテスト時にはSolaris用のCVSマシンを物理的に切り離し、Solaris版CVSのテスト時にはLinux用のCVSマシンを物理的に切り離している

図2-1　評価者テスト構成

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2-1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

テストとして、実際の運用により使用されるユーザインタフェース（クライアントからの証明書検証要求、管理端末からのコマンド入力、CVS操作端末からのWebインタフェース操作）を刺激し、セキュリティ機能のふるまいを下記の手段により確認する手法が使用された。

・操作画面上（クライアントソフト、コンソール、Web画面）での出力結果、動作結果の確認
・インタフェース出力データの解析（証明書検証結果等）
・ログ出力データでの確認
・キャプチャしたパケットデータの解析

c.実施テストの範囲

評価者が独自に考案したテストを48項目、開発者テストのサンプリングによるテストを182項目、侵入テストを12項目、計242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。

① TOEの重要なセキュリティ機能（認証パス検証、OCSP有効性検証、サービス管理、監査ログ参照）を網羅する
② 開発者テストにおいて不足していると判断される項目（特に異常系に関する項目）のテストの実施
③ 脆弱性分析において懸念される事項に関するテストの実施

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

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

① 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EAL2に対する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。
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していることを確認している。
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。
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。
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。
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。
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。
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。
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、前提条件のいずれかへ遡

	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。
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。
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。
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。
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すべてのTOE及びIT環境のセキュリティ要件の記述が、正当であること、客観的に、明確に、曖昧さなく表現されていること、及び保証要件でサポートされるのに適切で妥当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あらゆるITセキュリティ要件の依存性のすべてが識別されてい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。

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。
構成管理	**適切な評価が実施された**
ACM_CAP.2.1E	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。
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。
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。
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。
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。

ADV_HLD.1.1E	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環境としてのハードウェア、ソフトウェア、ファーム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。
ADV_HLD.1.2E	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。
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。
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。
テスト	**適切な評価が実施された**
ATE_COV.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機能仕様に正確に対応していることを確認している。

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。
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。
脆弱性評定	**適切な評価が実施された**
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。
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主張が正しい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。

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。

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。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用された用語を以下に示す。

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（TOE）
CVS証明書	CVSの公開鍵の正当性を保証するものであり、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。RFC3280で定めるX.509形式の電子証明書である。
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Subject DNのこと。
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。

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。
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。
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。RFC2560として公開されている。
PKI	(Public Key Infrastructure) 公開鍵暗号技術を利用したセキュリティ基盤。
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	OCSPに関する技術仕様が記載されたRFCのこと。
RFC3280	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。
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.509	ITU(国際電気通信連合)が定めた電子鍵証明書及び証明書失効リスト(CRL)の標準仕様。
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。

6 参照

[1] 証明書検証サーバ（Certificate Validation Server）セキュリティターゲット Version 1.09（2007年11月1日）株式会社 日立製作所

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

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

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

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

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

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

[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2.3 2005年8月 CCMB-2005-08-001　(平成17年12月翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002　(平成17年12月翻訳第1.0版)

[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2.3 2005年8月 CCMB-2005-08-003　(平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月　(平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] 株式会社 日立製作所 証明書検証サーバ 03-00 Linux版およびSolaris版 評価報告書 第1.5版 2007年12月7日　有限責任中間法人　ITセキュリティセンター