認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙 押印済

評価対象

申請受付日（受付番号）	**平成20年12月16日** (IT**認証**8241)
認証番号	C0213
認証申請者	**富士フイルムソフトウエア株式会社**
TOE**の名称**	**機能特定**（FVR-100）
TOE**のバージョン**	1.0
PP**適合**	**なし**
適合する保証パッケージ	EAL1
開発者	**富士フイルム株式会社**
評価機関の名称	**一般社団法人** IT**セキュリティセンター 評価部**

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21年4月21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　山里　拓己

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 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3.1 改訂第2版 (翻訳第2.0版)
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 改訂第2版　(翻訳第2.0版)

評価結果：合格

「FVR-100」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、「FVR-100」（以下「本TOE」という。）について一般社団法人 ITセキュリティセンター 評価部（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富士フイルムソフトウエア株式会社に報告するとともに、本TOEに関心を持つ利用者や運用者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威への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、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、市販される本TOEを購入する一般消費者を読者と想定している。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。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL1適合である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称： FVR-100
バージョン： 1.0
開発者： 富士フイルム株式会社

1.2.2 製品概要

本製品は、富士フイルム株式会社の映像監視システムを構成する製品である、ネットワークビデオレコーダーFVR-100サーバーであり、本TOEは、FVR-100サーバーに搭載される。

本TOEを含めた画像監視システムの構成図を図1-1に示す

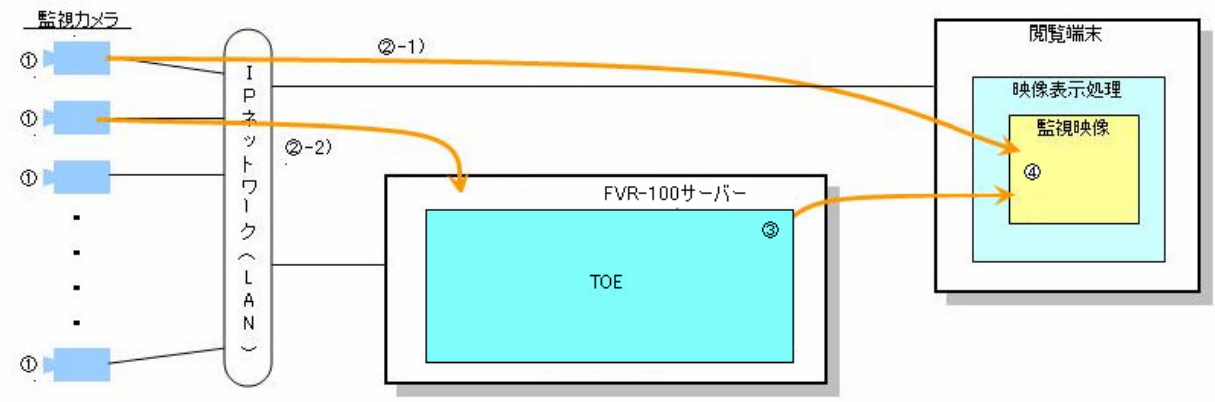

図1-1 映像監視システム構成図

本製品を含む画像監視システム及び本TOEの動作概要を以下に示す。

①監視カメラが撮影を行い、映像データを作成する。
②監視カメラにより作成された映像データは、IPネットワーク（LAN）を経由し、以下の二つの方法で画像監視システムを構成する端末へ渡される。
1）監視カメラが、映像データを閲覧可能な閲覧端末へリアルタイムで転送する。
2）映像データを集約・管理する、本TOEを含むFVR-100サーバーが、あらかじめ設定されたスケジュールに従い、監視カメラから映像データを取得する。
③閲覧端末からFVR-100サーバーに格納された画像データを参照する場合、本TOEが提供する認証機能、アクセス制御機能により制限を行う。
④利用者は閲覧端末のViewer（ブラウザ）を利用して、リアルタイムに転送された画像データやFVR-100サーバーで集約管理された映像データを参照する。

本TOEの主要なセキュリティ機能を以下に示す。
・認証機能
・アクセス制御機能
・ユーザー管理機能

1.2.3 TOE範囲とセキュリティ機能

1.2.3.1 TOEの物理的範囲

本TOEの物理的範囲を図1-2に示す。

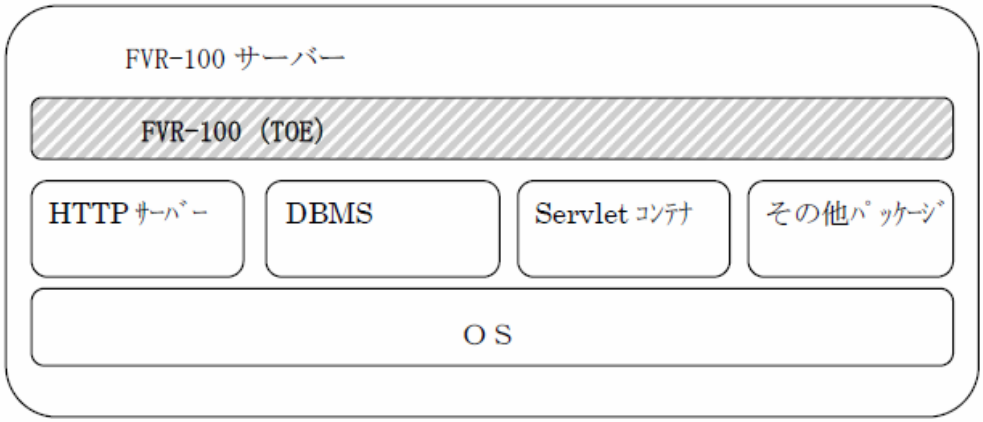

図1-2　TOEの物理的範囲

本TOE は、Linux OS 上で動作するソフトウェアであり、Linux OS に標準搭載されるソフトウェアや、Linux OS 上で動作する別のソフトウェアと連携して動作する。

閲覧端末からのアクセスはHTTPサーバーが受け付ける。本TOEは、Servletコンテナ上で動作し、HTTPサーバーが受け付けた通信はServletコンテナを介して本TOEが受け取り、その内容に応じた処理を行う。本TOEが取り扱う画像データは、DBMSに登録、管理される。その際、画像データはその他のパッケージにより特殊な圧縮技術を用いて保存することも可能である。

1.2.3.2 TOE の論理的範囲

TOE の論理的範囲を図1-3に示す。

TOE におけるセキュリティ機能は「認証機能」、「アクセス制御機能」、「ユーザー管理機能」である。

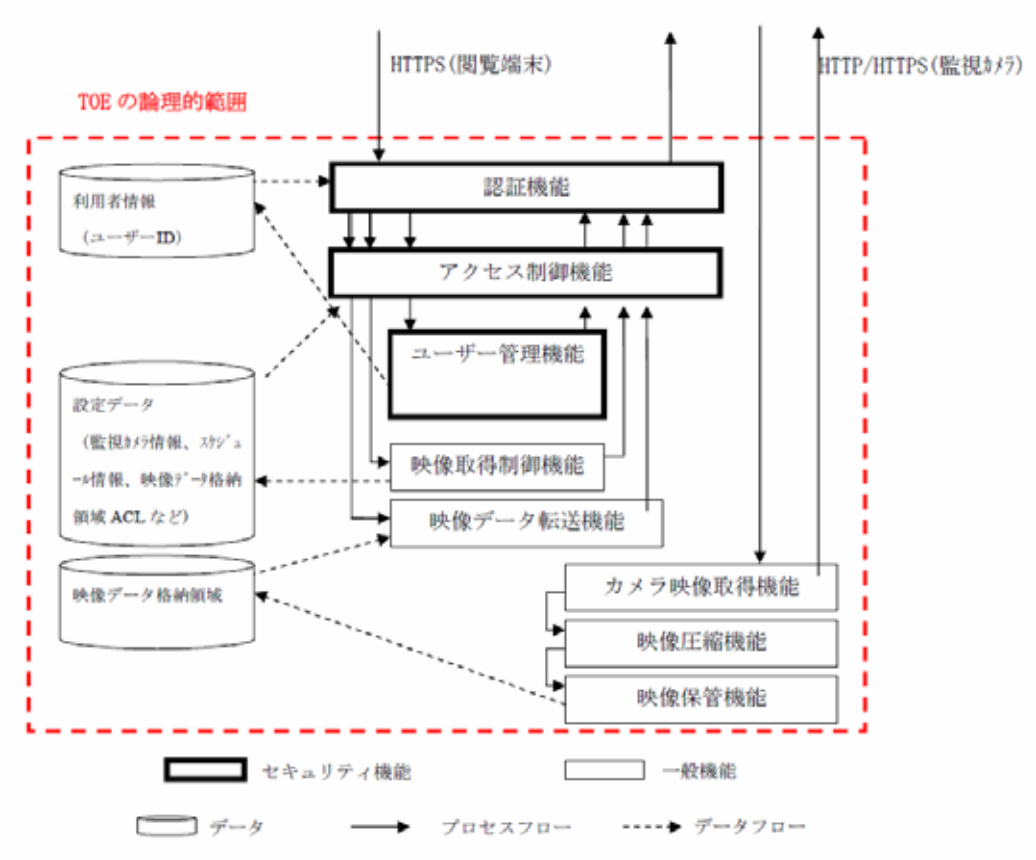

図1-3　TOEの論理的範囲

本TOEの範囲におけるセキュリティ機能を以下に説明する。

(1) 認証機能

認証機能は、利用者が全ての操作を行う前に必ず、ユーザーID、パスワードによって識別認証を行う。

利用者は閲覧端末のViewer（ブラウザ）によってHTTPSで本TOEへアクセスし、以降の利用者との通信は全てHTTPSに送受信される。

利用者によって入力されたユーザーID とパスワードが、本TOEの利用者情報（ユーザーIDとパスワード）と一致した場合、処理を後続の機能に引き渡す。

(2) アクセス制御機能

利用者からの映像データ格納領域に格納された映像データへのアクセス要求に対し、本TOEは識別認証されたユーザーIDと映像データ格納領域ACLが一致している場合に映像データの閲覧を許可する。

(3) ユーザー管理機能

以下の情報を管理者及びシステム管理者のみ管理することを許可する機能である。

・ユーザーID：利用者を識別するための情報。

・パスワード： 利用者を認証する際のパスワード。

※ 利用者は自身のパスワードのみ変更できる

・アカウントロックフラグ： ユーザーID の使用を禁止するフラグ。

・ユーザー権限： 識別された利用者ごとに一般ユーザー、管理者、システム管理者のいずれかの権限が付与され、ユーザー管理操作を許可された範囲に制限させるためのフラグ。

本TOEの範囲におけるセキュリティ機能以外の機能を以下に説明する。

(4) 映像取得制御機能

監視カメラから映像を取得するための機能で、本TOEにより識別・認証された管理者及びシステム管理者により監視カメラのIPアドレス等の設定変更が可能である。

(5) 映像データ転送機能

監視カメラから取得した映像データをファイル形式で閲覧端末に転送する機能。

(6) カメラ映像取得機能

映像取得制御機能で設定した監視カメラを対象に、定期的に映像データを取得する機能。取得された映像データは、映像圧縮機能へ渡される。

(7) 映像圧縮機能

監視カメラから取得した映像データを圧縮する機能。圧縮した映像データは、映像保管機能へ渡される。

(8) 映像保管機能

監視カメラから取得し、圧縮されたデータを映像データ格納領域へ保管する機能。

本TOEが取り扱うデータについて以下に説明する。

(1) 利用者情報

利用者の性質を現す情報である。「ユーザーID」、「パスワード」、「ユーザー権限」、「アカウントロックフラグ」がある。

(2) 設定データ

アクセス制御リスト（映像データ格納領域ACL）や、監視カメラのIPアドレス等の設定情報など、各種機能の設定情報のこと。

(3) 映像データ格納領域

本TOEが監視カメラから映像データを取得する際に、映像データを格納するための論理的な領域のことである。属性として「映像データ格納領域ACL」を持つ。

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「FVR-100セキュリティターゲット」（以下「本ST」という。）[1] 及び本TOE開発に関連する評価用提供物件を調査し、本TOEがCCパート1 ([5][8]のいずれか) 附属書A、CCパート2（[6][9]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の開発がCCパート3（[7][10]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、「富士フイルム株式会社 FVR-100 Ver.1.0 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

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21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。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEでは、セキュリティ課題定義は評価対象外である。

2.1.2 組織のセキュリティ方針

本TOEでは、セキュリティ課題定義は評価対象外である。

2.1.3 操作環境の前提条件

本TOEでは、セキュリティ課題定義は評価対象外であるが、操作環境の前提となる運用環境のセキュリティ対策方針を表2-1に示す。

これらの運用環境のセキュリティ対策方針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2-1 TOEの運用環境のセキュリティ対策方針

識別子	運用環境のセキュリティ対策方針
OE.Environment	システム管理者は、TOE の実装された機器を、システム管理者以外物理的に触れられない場所に設置しなければならない。
OE.Administrator	組織の責任者は、セキュリティ意識が高く、責任を持って管理できる者を管理者、システム管理者として任命し、それらのセキュリティ意識のレベルを高く維持し続けるよう監督しなければならない。
OE.Password	全ての利用者は、自身のパスワードが漏洩しないように管理し、推測可能なパスワード（人の名前や“password”などの辞書にある単語など）を設定しないようにしなければならない。

2.1.4 製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。TOEの利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

・FVR-100 取扱説明書　第１版

・FVR-100 設置マニュアル　第１版
・FVR-100 簡単操作ガイド　第１版

2.1.5　構成条件

本評価は以下のハードウェア及びソフトウェア上での動作を対象とする。なお、本構成に示されるハードウェア及びソフトウェアの信頼性は本評価の範囲外である。

■　本TOEが動作するための機器（FVR-100サーバー）

コンポーネント名	スペック
機器名	NEC製品　Express5800/110Gd-S
OS	CentOS 4.6
HTTPサーバー	Apache 2.2.10
Servletコンテナ	Tomcat 5.5.27
DBMS	Postgresql8.3.5-1
その他パッケージ	MainConcept社 H.264/AVCコーデックパッケージ

■　監視カメラ

メーカー名	型番
Axis	Axis241Q　ビデオサーバー（アナログ）
Vivotek	IP-7138
Basler	BIP-1000C

■　閲覧端末

コンポーネント名	スペック
OS	WindowsXP SP2 ： Internet Explorer 6 の場合 WindowsXP SP3 ： Internet Explorer 7 の場合
Webプラウザ	Internet Explorer 6 及び 7

2.2　セキュリティ対策

本TOEでは、セキュリティ対策は評価対象外である。

3 評価機関による評価実施及び結果

3.1 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。

3.2 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20年12月に始まり、平成21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21年1月および2月に開発者サイトで開発者のテスト環境を使用し、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。

3.3 製品テスト

評価者は、評価の過程で示された証拠を検証した結果から、必要と判断された評価者テスト及び脆弱性評定に基づく侵入テストを実施した。

3.3.1 開発者テスト

本TOEでは、開発者テストは評価対象外である。

3.3.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成を図3-1および表3-1に示す。評価者テストは本STにおいて識別されているTOE構成と同一の環境で実施されている。

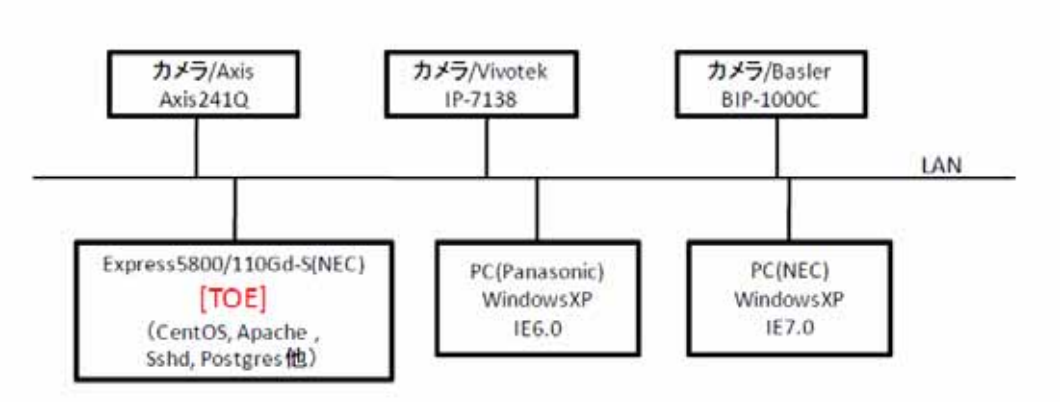

図3-1　評価者独立テスト環境

表3-1　評価者独立テスト環境

テスト環境	内容
TOE が稼動するサーバー	Express5800/110Gd-S(NEC) CentOS 4.6 Apache 2.2.10 Tomcat 5.5.27 Postgresql8.3.5-1 MainConcept社 H.264/AVC コーデックパッケージ
監視カメラ	Axis製 Axis241Q　ビデオサーバー(アナログ) Vivotek製 IP-7138 Basler製 BIP-1000C
閲覧端末	WindowsXP SP2：Internet Explorer 6あるいは WindowsXP SP3：Internet Explorer 7

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a.　独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

＜テストの観点＞

①テストの効率性・種別を踏まえ、より多くのセキュリティ機能をテスト

する。
②確率的・順列的メカニズムをテスト対象とする。
③インタフェースの重要性・複雑性を踏まえ、必要と判断されるバリエーションをテストする。
④革新的・一般的でない機能はテスト対象とする。

b. テスト概要

評価者が実施した独立テストの概要は以下のとおり。

＜テスト手法＞
画面上から入力可能なテストデータは、その外部インタフェースを使用してふるまいを観察することにより実施し、画面上から入力ができないテストデータについては、画面上から入力されたデータをキャプチャし、編集できるツールを使用することで実施した。

＜テストで使用したツール等＞
プロキシ型脆弱性スキャナ「Paros」：
Webブラウザからの HTTP リクエストを参照、改ざんして脆弱性を確認するツール

＜テストの観点とテスト概要＞
評価者は、TOEのTSFI（全4個）をすべて対象とし、18項目の独立テストを実施した。
独立テストの観点ごとのテスト概要を表3-2に示す。

表3-2　独立テストのテスト概要

独立テストの観点	テスト概要
観点①	評価者が追加して確認する必要があると判断したテストを実施した。
観点②	一般ユーザー、管理者、システム管理者それぞれについて、識別認証等の確率的・順列的メカニズムに着目し、文字桁数及び文字種類を変化させたテストを実施した。
観点③	評価者が重要と判断したユーザー権限の管理を行う、ユーザー管理画面におけるふるまいを確認するため、ユーザーの登録・削除機能、パスワード変更機能、アカウントロックフラグ解除機能、ユーザー権限の変更機能の状況を確認するテストを実施した。
観点④	圧縮オプション設定機能は、革新的または一般的でない機能と

	判断し、動作を確認するテストを実施した。

c. 結果

実施したすべての評価者独立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。

3.3.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、懸念される脆弱性の可能性について必要な侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

a. 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

探索した公知情報からWebアプリケーションで一般的によく知られている潜在的な脆弱性17件（ディレクトリトラバーサル、クロスサイトスクリプティング、クッキーの不適切な設定、セッションハイジャック、SQLインジェクション等）を識別し、また提供された証拠資料から本TOE運用における潜在的な脆弱性2件（起動されたサービス等に対する不正アクセス）を識別した。

b. 実施テストの範囲

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。

侵入テストは、証拠資料に記載さているセキュリティ機能のふるまいを基に、Webブラウザからの侵入テスト、操作中におけるネットワーク切断等のテスト、ポートスキャン、サーバーへの不正アクセスの確認テスト、認証機能の迂回テスト等、全7項目のテストを実施した。

＜テスト手法とツール＞

使用目的	ツール名	手法
ポートスキャン	Nmap	閲覧端末でFVR-100サーバーのポートスキャンを実施し、悪

		用可能なサービスが存在するかどうか確認した。
パケットアナライザ	Wireshark	閲覧端末でFVR-100サーバーへのパケットの確認を実施し、フォーマット解析が可能かどうか確認した。
プロキシ型脆弱性スキャナ	Paros	Webブラウザからの HTTP リクエストを参照、改ざんして脆弱性を確認した。
Cookie参照、編集ツール	Cookie Editor	IEのキャッシュ情報を参照してキャッシュ内Cookieを参照、編集できるツールを用いて、Cookieを参照できるかどうか確認した。
リモートターミナル	TeraTermPro	開放されているTCPポートに対して不正アクセスが可能かどうか確認した。

＜テスト環境＞
侵入テストは、図3-1及び表3-1に示す、評価者独立テスト環境と同一のテスト環境にて実施した。

c. 結果

実施した評価者侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

3.4 評価結果

3.4.1 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。

3.4.2 評価者コメント/勧告

特になし。

4 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 所見報告書でなされた指摘内容が妥当であること。
② 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、本ST及び評価報告書において、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、本認証報告書を発行した。

5 結論

5.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL1に対する保証要件を満たすものと判断する。

5.2 注意事項

評価範囲の機能は、Viewer（ブラウザ）からのHTTPSを用いた本TOEへのアクセスにおける認証機能、アクセス制御機能、ユーザー管理機能のみである。

6 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation(セキュリティ評価基準)
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用されたTOEに関する略語を以下に示す。

DBMS	DataBase Management System
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Security
IE	Internet Explorer

本報告書で使用された用語の定義を以下に示す。

FVR-100 映像監視システム	TOEを含め、FVR-100のサービスを利用者に提供するために必要なシステム構成のことである。
FVR-100 サーバー	TOEをインストールしたハードウェアや連携するソフトウェアを含めた機器のことである。
Viewer	閲覧端末からTOEへアクセスし、設定変更や映像データを閲覧する際に利用するブラウザのこと。
閲覧端末	利用者が映像データを閲覧する際に利用するパーソナルコンピュータである。
利用者	TOE が提供するサービスを利用する人。利用者は権限により、一般ユーザーと管理者、システム管理者に分かれる。なお、システム管理者の権限を付与される者は、TOE の設置や初期設定など、TOE のサービスを利用可能にするための役割を担うことを想定している。
ユーザー権限	利用者の役割によって行える操作を制限すること。ユーザー権限には、一般ユーザー、管理者、システム管理者、の権限がある。

利用者情報	利用者の性質を現す情報である。「ユーザーID」、「パスワード」、「ユーザー権限」、「アカウントロックフラグ」がある。
設定データ	アクセス制御の制御に関する情報や、監視カメラから映像を取得するための設定情報など、各種機能の設定情報のこと。
映像データ格納領域	FVR-100が監視カメラから映像データを取得する際に、FVR-100が映像データを格納するための論理的な領域のことである。属性として「映像データ格納領域ACL」を持つ。
ユーザーID	利用者を一意に識別するためのID である。
アカウントロックフラグ	利用者が使用するユーザーID を利用不可とするフラグである。
映像データ格納領域ACL	映像データ格納領域への利用者のReadを許可するかどうかを判断するためにTOEが保持する、Read許可者のユーザーID を管理するリストのことである。

7 参照

[1] FVR-100 セキュリティターゲット バージョン1.15 2009年3月16日 富士フイルム株式会社

[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 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003

[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3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3月翻訳第1.2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: セキュリティ機能コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-002 (平成20年3月翻訳第2.0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: セキュリティ保証コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-003 (平成20年3月翻訳第2.0版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004

[12] 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3.1 改訂第2版 2007年9月 CCMB-2007-09-004 (平成20年3月翻訳第2.0版)

[13] 富士フイルム株式会社 FVR-100 Ver.1.0 評価報告書 第1.6版 2009年3月27日 一般社団法人 ITセキュリティセンター 評価部