FVR-100 セキュリティターゲット

バージョン：1.15

発行日： 2009 年 3 月 16 日

作成者：富士フイルム株式会社

更新履歴

バージョン	変更概要	変更箇所		変更日	変更者
		章･節･項	内容		
1.0	新規作成	全体	－	2008 /10/31	富士フイルム株式会社
1.1	レビューによる修正	全体	－	2008 /10/31	富士フイルム株式会社
1.2	レビューによる修正	全体	－	2008 /11/26	富士フイルム株式会社
1.3	レビューによる修正	全体	－	2009 /1/9	富士フイルム株式会社
1.4	CC パート2,3の翻訳第2版に対応	全体	－	2009 /1/13	富士フイルム株式会社
1.5	レビューによる修正	全体	－	2009 /1/16	富士フイルム株式会社
1.6	指摘による修正	全体	－	2009 /1/21	富士フイルム株式会社
1.7	指摘による修正	全体	－	2009 /1/23	富士フイルム株式会社
1.8	指摘による修正	全体	－	2009 /2/4	富士フイルム株式会社
1.9	レビューによる修正	全体	－	2009 /2/13	富士フイルム株式会社
1.10	指摘による修正	全体	－	2009 /2/16	富士フイルム株式会社
1.11	指摘による修正	全体	－	2009 /2/18	富士フイルム株式会社
1.12	指摘による修正	全体	－	2009 /2/25	富士フイルム株式会社
1.13	指摘による修正	全体	－	2009 /3/2	富士フイルム株式会社
1.14	指摘による修正	全体	－	2009 /3/10	富士フイルム株式会社

バージョン	変更概要	変更箇所		変更日	変更者
		章･節･項	内容		
1.15	指摘による修正	全体	ー	2009 /3/16	富士フイルム株式会社

目次

用語・略語

用語	定義内容
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。

1. ST 概説

1.1 ST 参照

本 ST の識別情報は以下のとおりである。

ST タイトル：	FVR-100 セキュリティターゲット
ST バージョン：	1.15
ST 作成者：	富士フイルム(株)
ST 作成日：	2009 年 3 月 16 日

1.2 TOE 参照

本 TOE の識別情報は以下のとおりである。

TOE 名称：	機能特定（FVR-100）
TOE バージョン：	1.0
TOE 開発者：	富士フイルム(株)

1.3 TOE 概要

1.3.1 TOE の種別

本 TOE の種別は「その他」である。

1.3.2 主要なセキュリティ機能

本 TOE は、富士フイルム株式会社の映像監視システムの 1 製品 FVR-100 である。FVR-100 は、ネットワークビデオレコーダーのアプリケーションであり、Linux のプラットホーム上で動作する。TOE をインストールした機器の動作概要は以下の通りである。

・FVR-100 は監視カメラとネットワークを経由して接続する。
・監視カメラから送信される映像データは FVR-100 に集約される。
・利用者はネットワークに接続されている端末からブラウザを介して映像データを閲覧することができる。

TOE の主要なセキュリティ機能を以下に示す。

1)認証機能

利用者によって入力されたユーザーID とパスワードを使用して、識別と認証を行なう機能。

2)アクセス制御機能

TOE に保存された映像データの参照できる者を、TOE に認証された利用者のみに制限するための機能。

3)ユーザー管理機能

TOE のユーザーID を登録・削除すること（アカウントを登録・削除すること）、利用者のパスワードを変更（登録、改変）すること、アカウントロックした際にアカウントロックフラグを解除すること、映像データ格納領域 ACL を登録・削除すること、ユーザー権限を登録・改変することを管理者及びシステム管理者に制限するための機能。また、一般ユーザーは、自身のパスワードのみ改変できるように制限するための機能。

1.3.3 TOE の動作環境

■ TOE が動作するための機器（サーバ）

本 TOE で利用される機器構成を以下に示す。

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

なお、FVR-100 サーバーは、上記コンポーネントをあらかじめ内蔵しているオールインワンモデルのため、設置時に TOE 以外の各種ソフトを操作する運用はない。

■ 監視カメラ

本 TOE で利用する、監視カメラとその型番を以下に示す。

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

本 TOE で利用する、閲覧端末の環境を以下に示す。

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 ブラウザ	Internet Explorer 6 及び 7

1.4 TOE 記述

1.4.1 TOE の構成

本 TOE の構成要素は以下のとおり。

(1) TOE 本体

本章では、TOEの物理的な範囲、TOEの論理的な範囲、役割の定義について記述する。

■　TOE の物理的範囲

この TOE は、FVR-100 サーバーで稼動するアプリケーションである。この TOE は図 2 に示す様に TOE（FVR-100）を含む FVR-100 サーバー、監視カメラ、閲覧端末、IP ネットワーク（LAN）から構成される FVR-100 映像監視システムにおいて動作する。

図 1　FVR-100 サーバー

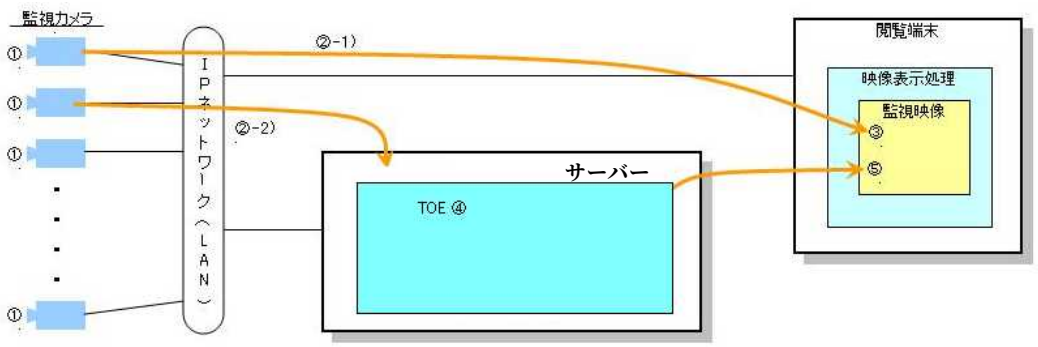

図 2　FVR-100 映像監視システム構成図

TOE は監視カメラが撮影した映像データを受信し、蓄積する機能を持つ装置である。通常は監視カメラが設置される同一の拠点に置かれる。TOE は主に以下の機能を持つ。

・監視カメラからの映像データ取得
・映像取得の制御（撮影スケジュール、撮影の開始／終了）
・監視カメラから取得した映像データの圧縮
・監視カメラから取得した映像データの保管
・閲覧端末への映像データ転送

FVR-100 映像監視システム構成図を用いて映像データの流れを以下に説明する（図中の丸枠番号は以下の番号の説明である）。

①監視カメラが映像を捉える。
②撮影された映像データは、二つの方法でシステムに転送される。
　１）リアルタイムに閲覧端末に転送される
　２） TOE（FVR-100）が予め設定されたスケジュールに従い映像データを取得する
③リアルタイムに閲覧端末に転送された映像データ（図の②-1)）は閲覧端末上のアプリケーションプログラムにより再生・表示される。
④TOE に転送された映像データ（図の②-2)）は TOE 内で保存される。このとき、製品の特徴の一つである、特殊な圧縮技術を用いて保存することも可能である。
⑤TOE に保存された映像データは閲覧端末に転送され再生・表示される。

TOE の物理的な範囲を図 3 に示す。TOE はプラットホームを Linux とし、諸機能を Linux のアプリケーションプロラグラムとして構成している。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。

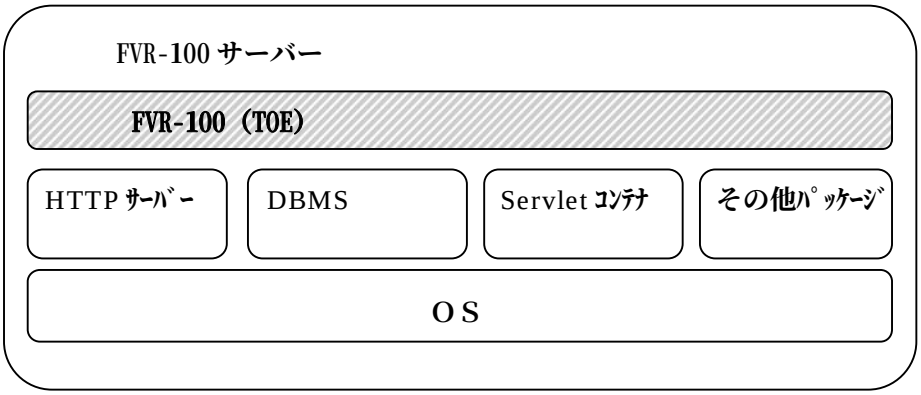

図 3　TOE の物理的範囲

■　TOE の論理的範囲

TOE の論理的範囲を図 4 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。

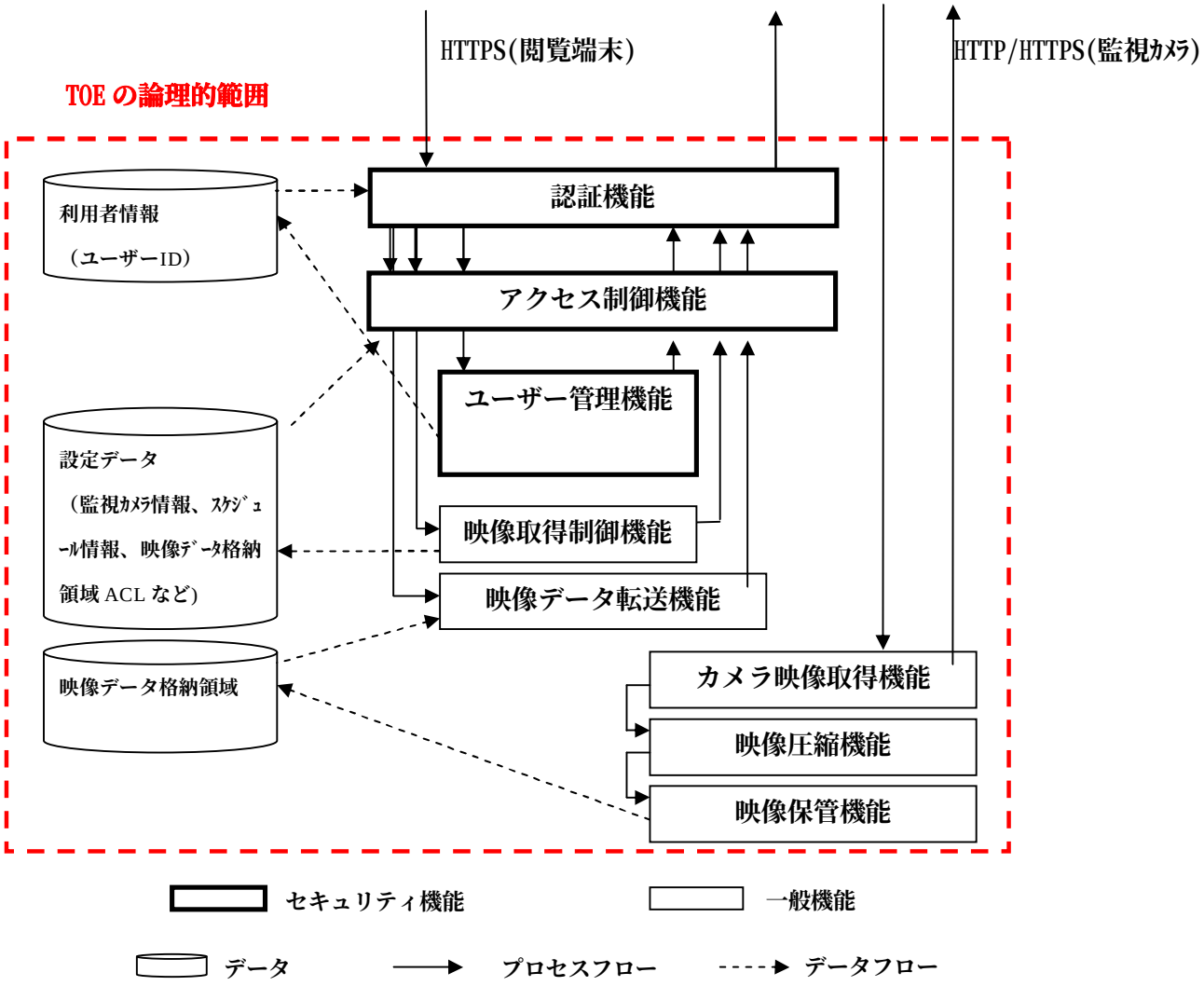

図 4　TOE の論理的範囲

TOE の範囲におけるセキュリティ機能を以下に説明する。

- 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認証識別を行う。利用者は閲覧端末の Viewer(ブラウザ)によって https で FVR-100 にアクセスし、以降の利用者との通信は全て https によりやりとりされる。利用者によって入力されたユーザーID とパスワードが、FVR-100 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。

- アクセス制御機能

利用者からの映像データ格納領域へのアクセス要求に対し、識別・認証された全ての利用者のアクセスを許可する。

その際 TOE は、映像データ格納領域 ACL（全ての識別・認証された利用者の Read を許可するように設定されている）と、ユーザーID の値を比較し、マッチするかどうかをチェックしている。

- 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。

・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　：　利用者の操作を許可された範囲に制限させるためのフラグ。

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。

- 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、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設定変更が可能である。

- 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である。

- 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。

- 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。

- 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。

TOE の範囲におけるデータについて以下に説明する。

- **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（映像データ格納領域 ACL）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。**

■ **役割の定義**

- **一般ユーザー**

  監視カメラの映像データを閲覧することが出来る役割である。

- **管理者**

  一般ユーザーの出来ることに加えて、以下を実行可能である。

  ・「パスワード」を登録・改変する
  ・「アカウントロックフラグ」を解除する
  ・「ユーザーID」を登録・削除する
  ・「映像データ格納領域 ACL」**を登録・削除する**

- **システム管理者**

  管理者の出来ることに加えて、システムログの取得、システムのアップデートが行える役割である。

(2)**添付されるガイダンス文書**

- 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**

1.4.2 TOE **のセキュリティ機能**

1)認証機能

利用者によって入力されたユーザーID とパスワードを使用して、識別と認証を行なう機能。

2)アクセス制御機能

TOE に保存された映像データの参照できる者を、TOE に認証された利用者のみに制限するための機能。

3)ユーザー管理機能

TOE のユーザーID を登録・削除すること（アカウントを登録・削除すること）、利用者のパスワードを変更（登録、改変）すること、アカウントロックした際にアカウントロックフラグを解除すること、映像データ格納領域 ACL を登録・削除すること、ユーザー権限を登録・改変することを管理者及びシステム管理者に制限するための機能。また、一般ユーザーは、自身のパスワードのみ改変できるように制限するための機能。

2. 適合主張

2.1 CC 適合主張

本 ST は、以下の通り CC 適合を主張する。

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　2006 年 9 月　バージョン 3.1　改訂第 1 版　[翻訳第 1.2 版]
パート 2:セキュリティ機能コンポーネント　2007 年 9 月　バージョン 3.1　改訂第 2 版 [翻訳第 2.0 版]
パート 3:セキュリティ保証コンポーネント　2007 年 9 月　バージョン 3.1　改訂第 2 版 [翻訳第 2.0 版]
CC パート 2 適合
CC パート 3 適合

2.2 PP 主張、パッケージ主張

本 ST は、以下の通り PP、パッケージ適合を主張する。

PP：　　PP への適合を主張しない。
パッケージ：　EAL1 適合

3. セキュリティ対策方針

3.1 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。

4. 拡張コンポーネント定義

本 ST には、拡張コンポーネントはない。

5. セキュリティ要件

5.1 セキュリティ機能要件

（1）ログイン制限

FIA_UID.2	**アクション前の利用者識別**
下位階層:	FIA_UID.1 識別のタイミング
依存性:	なし
FIA_UID.2.1	TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

FIA_UAU.2	**アクション前の利用者認証**
下位階層:	FIA_UAU.1 認証のタイミング
依存性:	FIA_UID.1 識別のタイミング
FIA_UID.2.1	TSF は、その利用者を代行する他の TSF 仲介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。

FIA_UAU.7	**保護された認証フィードバック**
下位階層:	なし
依存性:	FIA_UAU.1 認証のタイミング
FIA_UAU.7.1	**TSF は、認証を行っている間、[割付: *フィードバックのリスト*]だけを利用者に提供しなければならない。** [割付: *フィードバックのリスト*] *入力した文字数と同じ数の‘＊’*

FIA_AFL.1	**認証失敗時の取り扱い**
下位階層:	なし
依存性:	FIA_UAU.1 認証のタイミング
FIA_AFL.1.1	**TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付: 正の整数値]*、*[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]回の不成功認証**

	試行が生じたときを検出しなければならない。 [割付: *認証事象のリスト*] *過去 1 時間以内における、前回の認証成功後以降に連続した不成功認証試行回数* [選択: *[割付: 正の整数値]* [割付: 正の整数値] *3*
FIA_AFL.1.2	**不成功の認証試行が定義した回数[選択：*に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。** [選択：*に達する、を上回った*] に達する [割付: *アクションのリスト*] *アカウントロックを解除するまでアカウントをロックする*

（3）ファイルに対するアクセス制御

FDP_ACC.1	**サブセットアクセス制御**
下位階層:	なし
依存性:	FDP_ACF.1 セキュリティ属性によるアクセス制御
FDP_ACC.1.1	**TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。** [割付: *アクセス制御 SFP*] *映像データアクセス制御規則* [割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]

サブジェクトのリスト	利用者プロセス
オブジェクトのリスト	映像データ格納領域
操作のリスト	Read

FDP_ACF.1	**セキュリティ属性によるアクセス制御**
下位階層:	なし
依存性:	FDP_ACC.1 サブセットアクセス制御 FMT_MSA.3 静的属性初期化
FDP_ACF.1.1	**TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、また***

***は SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。**

[割付: *アクセス制御 SFP*]
映像データアクセス制御規則

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

サブジェクト	セキュリティ属性
利用者プロセス	*ユーザーID*

オブジェクト	セキュリティ属性
映像データ格納領域	*映像データ格納領域 ACL*

FDP_ACF.1.2 **TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。**

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

利用者プロセスに対応付けられたユーザーID と映像データ格納領域 ACL に存在するユーザーID と一致した場合、映像データ格納領域への Read を許可する。

FDP_ACF.1.3 **TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。**

[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]
なし

FDP_ACF.1.4 **TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。**

[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]
なし

FIA_USB.1 利用者-サブジェクト結合

下位階層: なし
依存性: FIA_ATD.1 利用者属性定義

FIA_USB.1.1 **TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサ**

	ブジェクトに関連付けなければならない。:[割付: *利用者セキュリティ属性のリスト*] [割付: *利用者セキュリティ属性のリスト*] ***ユーザーID***
FIA_USB.1.2	**TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: *属性の最初の関連付けの規則*]** [割付: *属性の最初の関連付けの規則*] ***なし***
FIA_USB.1.3	**TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: *属性の変更の規則*]** [割付: *属性の変更の規則*] ***なし***

FIA_ATD.1	**利用者属性定義**
下位階層:	なし
依存性:	なし
FIA_ATD.1.1	**TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。:[割付: *セキュリティ属性のリスト*]** [割付: *セキュリティ属性のリスト*] ***ユーザーID***

（5）アカウント管理

FMT_MTD.1(1)	**TSF データの管理(1)**
下位階層:	なし
依存性:	FMT_SMR.1 セキュリティの役割 FMT_SMF.1 管理機能の特定
FMT_MTD.1.1(1)	**TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付: 許可された識別された役割]に制限しなければならない。** [選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*] *[割付: その他の操作]* *以下のリストの“操作”* [割付: *TSF データのリスト*] *以下のリストの“TSF データ”*

TSF データ	操作
パスワード	登録、改変
アカウントロックフラグ	解除
ユーザー権限	登録、改変

[割付: 許可された識別された役割]
管理者、システム管理者

FMT_SMR.1(1) **セキュリティの役割(1)**

下位階層: なし
依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1(1) **TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。**

[割付: *許可された識別された役割*]
管理者、システム管理者

FMT_SMR.1.2(1) **TSF は、利用者を役割に関連付けなければならない。**

（6）認証データの保護

FMT_MTD.1(2) **TSF データの管理(2)**

下位階層: なし
依存性: FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1.1(2) **TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付: 許可された識別された役割]に制限しなければならない。**

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

[割付: *TSF データのリスト*]
自身のパスワード
[割付: 許可された識別された役割]
一般ユーザー

FMT_SMR.1(2) **セキュリティの役割(2)**

下位階層: なし
依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1(2) **TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。**

	[割付: *許可された識別された役割*] *一般ユーザー*
FMT_SMR.1.2(2)	**TSF は、利用者を役割に関連付けなければならない。**

FIA_SOS.1	**秘密の検証**
下位階層:	なし
依存性:	なし
FIA_SOS.1.1	**TSF は、秘密が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。** [割付: *定義された品質尺度*] *以下の条件を満たすパスワード* ・ *パスワード長：６～15* ・ *文字種：半角英小文字【a～z】、半角英大文字【A～Z】、半角数字【0～9】* ・ *上記文字種の範囲において３つ以上の異なる文字を混在させること* ・ *アルファベットと数字を混在させること*

（７）アクセス制御に関わる属性値の設定と保護

FMT_MSA.1(1)	**セキュリティ属性の管理**
下位階層:	なし
依存性:	[FDP_ACC.1 サブセットアクセス制御、または FDP_IFC.1 サブセット情報フロー制御] FMT_SMR.1 セキュリティの役割 FMT_SMF.1 管理機能の特定
FMT_MSA.1.1(1)	**TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]をする能力を[割付: *許可された識別された役割*]に制限する[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。** [割付: *アクセス制御 SFP、情報フロー制御 SFP*] *映像データ管理アクセス制御規則* [選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*] *削除* *[割付: その他の操作]* 登録 [割付: *セキュリティ属性のリスト* *ユーザーID* [割付: *許可された識別された役割*] *管理者、システム管理者*

FMT_MSA.1(2)	**セキュリティ属性の管理**
下位階層:	なし
依存性:	[FDP_ACC.1 サブセットアクセス制御、または FDP_IFC.1 サブセット情報フロー制御] FMT_SMR.1 セキュリティの役割 FMT_SMF.1 管理機能の特定
FMT_MSA.1.1(2)	**TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]をする能力を[割付: *許可された識別された役割*]に制限する[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。** [割付: *アクセス制御 SFP、情報フロー制御 SFP*] *映像データ管理アクセス制御規則* [選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*] *削除* *[割付: その他の操作]* 登録 [割付: *セキュリティ属性のリスト* *映像データ格納領域 ACL* [割付: *許可された識別された役割*] *管理者、システム管理者*

（8）セキュリティ管理機能の定義

FMT_SMF.1	**管理機能の特定**
下位階層:	なし
依存性:	なし
FMT_SMF.1.1	**TSF は、以下の管理機能を実行することができなければならない。: [割付: *TSF によって提供される管理機能のリスト*]** [割付: *TSF によって提供される管理機能のリスト*] ・*FVR-100 セキュリティ管理機能（アカウント管理）* ・*FVR-100 セキュリティ管理機能（アカウント管理制限）* ・*FVR-100 セキュリティ管理機能（パスワードポリシー）* ・*FVR-100 セキュリティ管理機能（アカウント登録削除制限）*

5.2 セキュリティ保証要件

本 TOE の評価保証レベルは EAL1 であり、CC パート 3 に規定された EAL1 の保証要件コンポーネントを使用する。

5.3 セキュリティ要件根拠

FDP_ACF.1 から FMT_MSA.3 への依存性が除去できる理由を以下に示す。

FMT_MSA.3 はセキュリティ属性のデフォルト値に制限的、許可的、またはその他の特性を付与すること、付与されたデフォルト値を代替する初期値を指定することを規定している。

しかし、本 TOE ではセキュリティ属性（ユーザーID）のデフォルト値はなく、また、セキュリティ属性（映像データ格納領域 ACL）のデフォルト値の変更は行えない仕様であるため、FDP_ACF.1 から FMT_MSA.3 への依存性は不要である。

6. TOE 要約仕様

「FVR-100 ログイン機能（認証）:（識別認証（１）ログイン制限（a））」（FIA_UID.2/FIA_UAU.2）

TOE 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」によって認証・識別を行う。利用者は、閲覧端末の Viewer（ブラウザ）によって、https で FVR-100 にアクセスし、以降の利用者との通信は全て https によりやりとりされる。利用者によって入力された「ユーザーID」と「パスワード」が、FVR-100 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。

なお、TOE への識別・認証前には、何もすることができない。

「FVR-100 ログイン機能（パスワード隠蔽）:（識別認証（１）ログイン制限（b））」（FIA_UAU.7）

TOE は、利用者が「パスワード」を入力する際に、1 文字入力する毎に画面に「*」を表示する。

「FVR-100 ログイン機能（アカウントロック）:（識別認証（１）ログイン制限（c））」（FIA_AFL.1）

認証機能は、利用者の識別・認証において、過去 1 時間以内において前回の認証成功後以降に 3 回の連続不成功を検知すると、当該利用者のアカウントをロックする。アカウントのロック状態は、管理者及びシステム管理者によりアカウントロックを解除するまで継続される。

「FVR-100 アクセス制御機能 :（アクセス制御（３）ファイルに対するアクセス制御（a））」（FDP_ACC.1/ FDP_ACF.1/ FIA_USB.1/ FIA_ATD.1）

利用者からの映像データ格納領域へのアクセス要求を TOE が受信した際、映像データ管理アクセス制御規則に従い、TOE は利用者プロセスの「ユーザーID」と映像データ格納領域 ACL に存在する「ユーザーID」とを比較検証し、両者が一致した場合のみ映像データ格納領域への Read を許可する。

「FVR-100 セキュリティ管理機能（アカウント管理）:（セキュリティ管理（５）アカウント管理（a））」（FMT_MTD.1(1)/ FMT_SMR.1(1)）

TOE は、識別･認証され、ユーザー権限に「システム管理者」あるいは「管理者」と設定されている利用者のみ、以下の操作を行うことを許可する。

- 利用者の「パスワード」を登録、改変する。
- 利用者の「アカウントロックフラグ」を解除する。

- 利用者の「ユーザー権限」を登録、改変する。
  （「ユーザー権限」には、「システム管理者」か「管理者」か「一般利用者」を識別するためのコードが設定される。）

「FVR-100 セキュリティ管理機能（アカウント管理制限）:（セキュリティ管理（６）認証データの保護（a））」（FMT_MTD.1(2)/ FMT_SMR.1(2)）

TOE は、識別･認証され、ユーザー権限に「一般利用者」と設定されている利用者のみ、以下の操作を行うことを許可する。

- 自身の「パスワード」の改変のみ許可される

「FVR-100 セキュリティ管理機能（パスワードポリシー）:（セキュリティ管理（６）認証データの保護（b））」（FIA_SOS.1）

TOE は、利用者の「パスワード」を登録・改変する際に、以下のパスワードポリシーに適合した場合のみ登録・改変を許可する。

- パスワード長　：　6～15
- 文字種　：　半角英小文字[a～z]、半角英大文字[A～Z]、半角数字[0～9]
- 上記文字種の範囲において３つ以上の異なる文字を混在させること
- アルファベットと数字を混在させること

「FVR-100 セキュリティ管理機能（アカウント登録削除制限）:（セキュリティ管理（７）アクセス制御に関わる属性値の設定と保護（c））」（FMT_MSA.1(1)/ FMT_MSA.1(2)）

TOE により管理者またはシステム管理者として識別・認証された利用者のみ、映像データアクセス制御規則で利用される「ユーザーID」の登録・削除を行うことが許可される。

また、TOE により管理者またはシステム管理者として識別・認証された利用者のみ、「映像データアクセス制御規則」で利用される「映像データ格納領域 ACL」の登録・削除を行うことが許可される。

「FVR-100 セキュリティ管理機能（セキュリティ管理（８）セキュリティ管理機能の定義（a））」（FMT_SMF.1）

FVR-100 は以下のセキュリティ管理機能を有する。

・FVR-100 セキュリティ管理機能（アカウント管理）
・FVR-100 セキュリティ管理機能（アカウント管理制限）
・FVR-100 セキュリティ管理機能（パスワードポリシー）
・FVR-100 セキュリティ管理機能（アカウント登録削除制限）