IPA　特定用途機器情報セキュリティ対策検討委員会　参考資料

ネットワークカメラシステムにおける情報セキュリティ対策要件に関する調査

調査実施報告書

2017 年 11 月

株式会社三菱総合研究所
社会 ICT イノベーション本部

本報告書は、2016 年 3 月 31 日公示「ネットワークカメラシステムにおける情報セキュリティ対策要件に関する調査」に係る一般競争入札の納品物です。本報告書は株式会社三菱総合研究所が作成し、公開のため一部 IPA が修正しています。

本報告書にはネットワークカメラシステムに関する公開情報を調査し、利用形態に応じた脅威とその対策に関する調査を行った結果が記載されています。本報告書の内容は IPA の「特定用途機器情報セキュリティ対策検討委員会」へ入力され、当該委員会が 12 月 7 日に公開したチェックリストの参考情報として議論されました。

なお、本報告書が引用している全ての文献や図の利用許諾は本報告書作成者である株式会社三菱総合研究所により確認済です。

■ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト

https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/index.html

■上記チェックリストに関する問い合わせ先

IPA セキュリティセンター 情報セキュリティ認証室 JISEC 担当 飛田/山里

Tel: 03-5978-7538 E-mail: jisec-proc@ipa.go.jp

目 次

1. はじめに

1.1 調査背景・目的

内閣サイバーセキュリティセンターは 2014 年に改定した「政府機関の情報セキュリティ対策のための統一基準」において、テレビ電話会議システム、IP 電話システム、ネットワークカメラシステム等を特定用途機器と呼び、使用される環境や取り扱う情報により想定される脅威への対策を講ずることを求めている。中でもネットワークカメラは広く公共の場に設置され、政府機関においてもその使用が定着している。その一方で、ネットワークカメラシステムを構成する製品に関する脆弱性の悪用や、安易な設置によるインターネットからの映像の流出によるセキュリティやプライバシに関する問題が懸念されており、安全なネットワークカメラシステムの構築を考える際の、機能あるいは運用におけるセキュリティ上の対策については十分に議論されていない。

このような状況を受け、本調査では、IT 製品の安全な政府調達の推進の一環として、ネットワークカメラシステムの利用において考慮すべきセキュリティ上の要件を明確にし、調達者がネットワークカメラシステムの構築や利用に際してセキュリティ対策を確認するための情報を提供することにより、安全な国民サービスを提供可能とするための調査を実施した。

1.2 調査の実施概要

本調査では、調達者が安全なセキュリティカメラシステムを調達する際に利用できる、具体的なセキュリティ要件のチェックリストを作成することを目的とし、以下の手順で調査を計画した。

1) ネットワークカメラシステムの利用形態の調査
2) 利用形態における情報セキュリティ課題の調査分析
3) 情報セキュリティ課題に対応するセキュリティ機能や運用の調査・分析
4) 調査実施報告書等の作成
5) セキュリティ対策チェックリストの作成
6) 本調査に関する委員会の運営

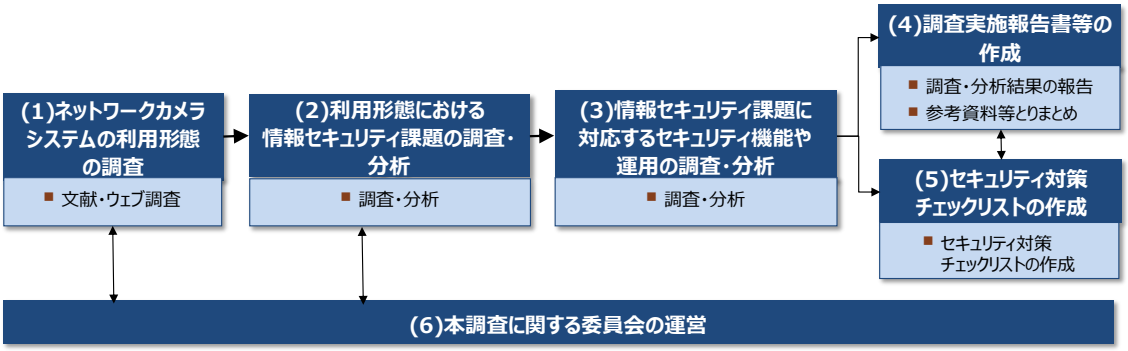
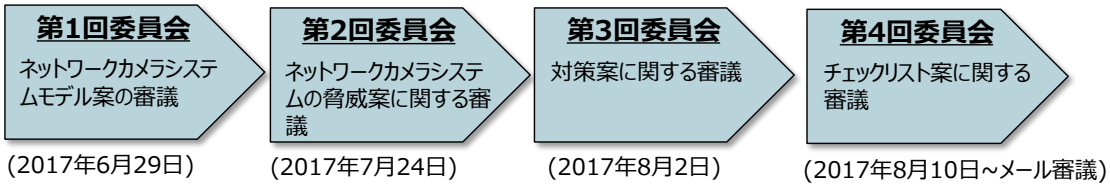


図 1-1　本調査のフロー

1.3 委員会での検討

本調査に関して、独立行政法人情報処理推進機構（以下「IPA」という。）が設置した「特定用途機器情報セキュリティ対策検討委員会」にて 1.2 の調査に関する議論を行った。

委員会は以下のスケジュールで実施した。



2. ネットワークカメラシステムの利用形態の調査

2.1 調査概要

公共施設等でネットワークカメラの利用が広がりつつある。その利用形態は多様であり、ネットワークカメラシステムのセキュリティ上の課題は、カメラが設置される場所や使用する回線等、いくつかの要素によって異なることが想定される。そのため、セキュリティ上の課題の洗い出しに先立って、ネットワークカメラの利用事例を調査し、システムモデルを作成した。

ネットワークカメラの利用事例の調査にあたっては**表 2-1** の文献やウェブサイトを調査対象とした。

表 2-1　ネットワークカメラの利用事例調査の対象一覧

文書種類	番号	発行機関	文書題名	利用用途
国内外のネットワークカメラの導入傾向や事例に関する調査レポート	1	IPA	IoT 開発におけるセキュリティ設計の手引き	個人住宅･事業所向け遠隔監視
	2	電気設備学会	電気設備学会誌「インターネットを支える電気設備，電気設備を支えるインターネット技術 7　監視カメラ」	複合オフィスビル向け内部監視/外部公開
	3	電気設備学会	電気設備学会誌「インターネットを支える電気設備，電気設備を支えるインターネット技術 7　監視カメラ」	河川･道路向け広域監視/道路状況・気象状況・水位等の河川状況･交通渋滞状況等の外部公開
	4	日本防犯設備協会	防犯カメラシステムネットワーク構築ガイドⅡ	遠隔監視
製品カタログ	5	TOA	「TRIFORA シリーズ」カタログ	マンション向け内部監視
	6	TOA	「TRIFORA シリーズ」カタログ	工場･物流倉庫向け内部監視
	7	NEC ネッツエスアイ	「オンデマンド防犯カメラ」カタログ	オンデマンド用記録
	8	三菱電機	「ネットワークカメラ・システム MELOOK3」カタログ	複数拠点向け集中遠隔監視
	9	CANON	ネットワークカメラ総合カタログ	大規模(的確な状況認識とインシデントへの対処が必要とされるシステム) 向け検知
	10	システム・ケイ	株式会社システム・ケイ　ホームページ	道路等向けモニタリング
	11	システム・ケイ	株式会社システム・ケイ　ホームページ	教育機関向け内部監視/授業の外部公開
	12	システム・ケイ	株式会社システム・ケイ　ホームページ	小売店向け内部監視
	13	Axis	IP-Surveillance design guide	内部監視/外部公開

	14	SIMENS	Video Surveillance	小規模店舗･美術館向け内部監視
	15	SIMENS	Video Surveillance	銀行･交通向け遠隔監視
	16	Panasonic	ネットワークカメラ総合カタログ	モーション検知･アラーム通知
	17	Axis	IP-Surveillance design guide	モーション検知･アラーム通知
調達仕様書	18	秋田県由利本荘市	「由利・ネットワークカメラ」公示書	（記載無し）
	19	独立行政法人国立美術館	「国立新美術館　監視映像録画サーバー及びネットワークカメラ調達」仕様書	国立新美術館の監視
	20	関東管区警察局山梨県情報通信部	「ＩＰネットワークカメラほか２件」見積もり依頼書	（記載無し）
	21	独立行政法人水資源機構阿木川ダム管理所	「阿木川ダムネットワークカメラ設備工事」仕様書	ダム現地及び監視室及び管理所の監視
	22	高知市消防局	「高知市消防局高所監視カメラ（カメラネットワーク網）整備事業業務委託」仕様書	マンション及び山及び消防署の遠隔監視
	23	地方独立行政法人　広島市立病院機構	広島市立安佐市民病院　監視カメラシステム賃貸借	広島市立安佐市民病院における監視
	24	公立大学法人三重県立看護大学	ネットワーク防犯カメラシステム整備仕様書	三重県立看護大学における防犯用
	25	独立行政法人国立美術館東京国立近代美術館	東京国立近代美術館フィルムセンター監視カメラ更新工事仕様書	東京国立近代美術館フィルムセンターの各フロアの監視
	26	日本原子力研究開発機構（JAEA）	「情報セキュリティ用監視カメラの更新」仕様書	情報センターの建屋への侵入及び入退室の監視
	27	広島市立大学	「広島市立大学監視カメラ システム（２０１３）賃貸借」仕様書	学内監視カメラシステム
	28	独立行政法人 日本芸術文化振興会	「国立能楽堂防犯カメラ及び録画装置等の調達（配線・取付・調整・既存機器の撤去を含む）」仕様書	国立能楽堂防犯カメラシステム
	29	公立大学法人和歌山県立医科大学	「監視カメラ」仕様書	学内向け内部監視
	30	神戸市	神戸市河川モニタリングシステム第 2 回情報提供招聘仕様書案	河川モニタリングシステム

ネットワークシステムモデルは図 2-1 に示す方法で作成した。

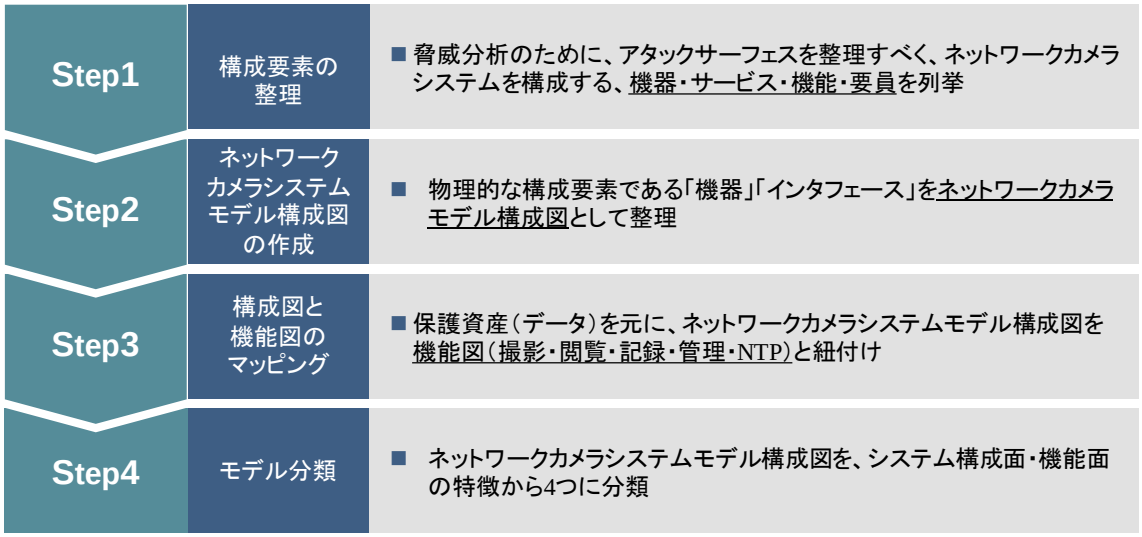


図 2-1　ネットワークカメラシステムモデルの作成手順

2.2 ネットワークカメラシステムに関する文献・ウェブサイトの調査

本調査で対象とするネットワークカメラシステムは、文献・ウェブサイトの事例調査を元に、以下の通り定義する。

- 映像・音声取得装置（カメラ・マイク）と映像・音声の利用者・記録装置間をデジタルデータ転送にて行うシステム
- デジタル転送にはインターネットの基盤技術である「IP」を利用

ネットワークカメラシステムの主な目的は、遠隔からのリアルタイム監視（工場・倉庫等の施設、防災、防犯、交通）と分析用の記録採取であり、情報提供や観光・集客目的で映像をインターネットで公開するケースもある。

なお、相互運用性を確保するため、Web Service としてのインタフェースを規定する「Open Network Video Interface Forum（ONVIF）」が規格化されている（Web Service は HTTP 上で SOAP メッセージを利用するサービスの規格）。

IPA 発行「IoT 開発におけるセキュリティ設計の手引き」では、個人の住宅や事業所に設置したカメラを用いて、遠隔から監視対象区域の静止画像等を監視するネットワークカメラのシステムとして以下の図 2-2 を掲載している。

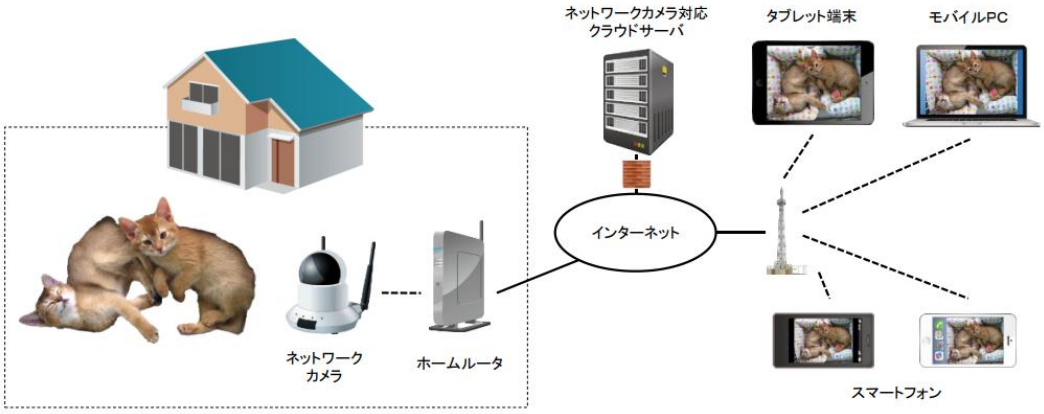


図 2-2　ネットワークカメラのシステム構成

（出所）IPA 発行「IoT 開発におけるセキュリティ設計の手引き」

その他の各ネットワークカメラシステムにおける構成機器の一覧は**別紙 1** に示す。

2.3 ネットワークシステムモデルの作成

2.3.1 ネットワークカメラシステムの構成要素の整理

本調査では、脅威分析のために、ネットワークカメラシステムの構成要素として、前節のネットワークカメラの利用事例調査結果を基に、「機器」「サービス」「要員」「機能」を整理した。

はじめに、ネットワークカメラシステムを構成する機器を列挙した。（**表 2-2**）

表 2-2　ネットワークカメラシステムを構成する機器

機器	説明
IP カメラ	機器自体が音声・映像をデジタルデータとして IP 出力可能な機器 機器自体は音声・映像をアナログデータとして出力し、エンコーダでデジタル変換したのち IP 出力可能なシステムや、音声・映像記録蓄積、ウェブ経由での制御・配信機能を持ち、単体で機能するモデルもある
ビデオレコーダー	本システムでは NVR（Network Video Recorder）のことを指す IP ネットワーク経由で音声・映像デジタルデータを受信、ハードディスク等に蓄積 映像のモニタ出力、音声のスピーカ出力、カメラ制御（パン、チルト、ズーム、フォーカス等）などを行う 他に、FTP サーバ機能、SNMP 機能、SSL 通信機能、NTP 利用による時刻同期、UPS 制御、アラート等のメール送信機能、システムログの外部出力機能などを持つ
管理 PC・管理ソフトウェア	IP カメラ、ビデオレコーダーの統合管理を行うソフトウェア 多拠点の場合、拠点単位でビデオレコーダーを配置し、中央監視センターに設置した PC に管理ソフトウェアをインストールする 全拠点の IP カメラ制御、映像閲覧、異常検知などの集中管理を行う OS としては Windows が主流
ネットワークスイッチ	IP 通信機器・ネットワーク同士を接続する装置。L2 スイッチ、L3 スイッチが主流
無線アクセスポイント	無線 LAN クライアント（本システムでは IP カメラ）から接続し、有線 LAN への転送を行う装置。接続時認証・通信の暗号化などの機能を持つ
ルータ・ファイアウォール	本システムでは LAN とインターネットの境界に設置し、経路制御及びインバウンド・アウトバウンドフィルタリング、コンテンツフィルタリング、VPN といったセキュリティ機能を提供する装置
UPS	電源異常による機能中断が許されないビデオレコーダー、バックアップ装置などに接続し、停電時などの機能継続、正常終了を支援する無停電電源装置（Uninterruptible Power Supply）
ネットワークサービスサーバ	IP 通信に必要な DNS サーバ（ホスト名を IP アドレスに変換）、正確な時刻同期に必要な NTP サーバ、アラームなどを電子メールで配信するための SMTP サーバなどを稼働するサーバ群
バックアップ装置	障害に備え、ビデオレコーダーの内部ストレージに蓄積された音声・映像データ等を外部保存する装置 SATA・USB などのインタフェースで直接ビデオレコーダーに接続する装置（DAS, Direct Attached Storage）、IP 通信経由で接続する装置（NAS, Network Attached Storage）が主流 大容量・広帯域・高可用性を必要とする場合には、高性能な SAN（Storage Area Network）

	を利用する
WAN・インターネット	遠隔監視センターと拠点、または外部を接続するネットワーク

次に、ネットワークカメラシステム内のサービスを列挙した。（**表 2-3**）

表 2-3　ネットワークカメラシステム内のサービス

サービス	内容
ウェブサービス	IP カメラ及びビデオレコーダー上でウェブサービスが稼働、 PC 等のウェブブラウザから HTTP/HTTPS プロトコルでアクセスし外部からストリーミング・制御等が可能
アップデート配信	IP カメラでは、メーカーのウェブサイト・FTP サーバなどでアップデートファイルが公開される IP カメラ自身でアップデートファイルをダウンロード可能な製品と、PC 等でダウンロード・SD カード経由で IP カメラにコピーする製品がある
DNS サービス	DNS サービスは、ホスト名と IP アドレスの相互変換を行う。
NTP サービス	防犯用に証拠として音声映像を記録する際には記録時間が正確であることが求められる。NTP（Network Time Protocol）サービスは、ネットワーク上の時刻配信サーバと同期を行うためのサービス インターネット上でもサービスが提供されているが、GPS や標準電波のレシーバを使った時刻サーバを設置することも可能
SMTP サービス	IP カメラに対するイタズラ（設置角の変更、レンズにフタをするなど）検知時、不審者の侵入検知時など、電子メールを発してアラームとする機能を持つ場合にメール配信サービスを利用する
プロキシサービス	IP カメラ・ビデオレコーダーからインターネット上の Web サーバ（アップデート提供）にアクセスする際に利用する中継サービス
Syslog サービス	IP カメラ、ビデオレコーダーには機器が出力するログをネットワーク経由で外部送信する機能を持つものがある。外部送信の際に用いられる Syslog プロトコルに対応してログを受信するサービス Syslog 自体に暗号化・改ざん検知といったセキュリティ機能がないので、オープンネットワーク上で利用する場合には、SSL-VPN などのセキュリティ通信を併用する必要がある

次にネットワークカメラシステムに関わる要員を整理した。（**表 2-4**）

表 2-4　ネットワークカメラシステムにおける要員

場所	区分	説明
各拠点、 遠隔監視センター（中央管理センター）	利用者	システムの管理者により、システムへの特定のアクセス権限が付与された者 （例） 監視オペレータ 運用オペレータ 外部公開映像の閲覧者

	管理者	各拠点において、システムの管理を行う者 （例） システムマネージャ
IP カメラベンダや保守業者	保守員	ファームウェアアップデート、アラームの受信を管理者に代行して請け負う者 （例） ベンダ、SIer、保守業者　等
場所問わず	第三者	システムへの正当なアクセス権を所有しない者

ネットワークカメラシステムが有する機能は、「撮影」「閲覧」「記録」「管理」「NTP」の 5 つに分類した。各機能の説明を**表 2-5** に示す。

表 2-5　ネットワークカメラシステムが有する機能

機能	説明
撮影	撮影対象となる画像（音声）データを入力すること
閲覧	撮影した画像（音声）データを見ること、確認すること 閲覧した結果により、カメラを制御すること
記録	撮影した画像（音声）データを保存すること
管理	撮影した画像（音声）データの撮影・閲覧・記録の管理や、機器の設定変更等の管理を行うこと
NTP	機器が持つ時刻データを正しい時刻へ同期すること

脅威分析においては、システムが有する保護資産を特定することが必要であるが、ネットワークカメラシステムにおける保護資産としてシステムで取り扱われるデータを対象とすると、データは特定の機器と常に紐付けられる訳ではなく、システム構成により異なる機器に紐付けられてしまう。そこで、脅威分析において漏れなく脅威を分析するために、保護資産は機能と紐付けることとした。各機能が保持するデータ、及び各機能における入出力データを整理したのが図 2-3～図 2-7 である。

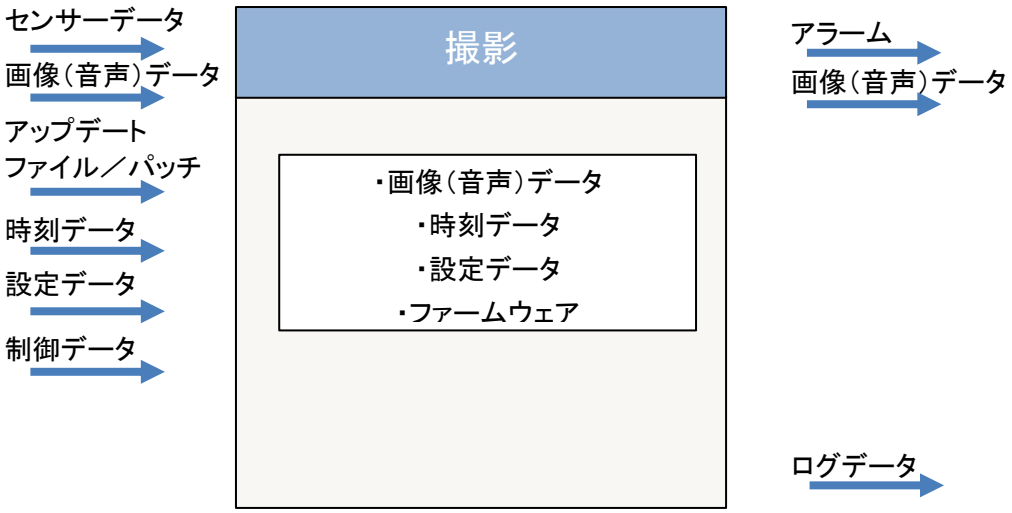


図 2-3　「撮影」機能で保持するデータ・入出力するデータ

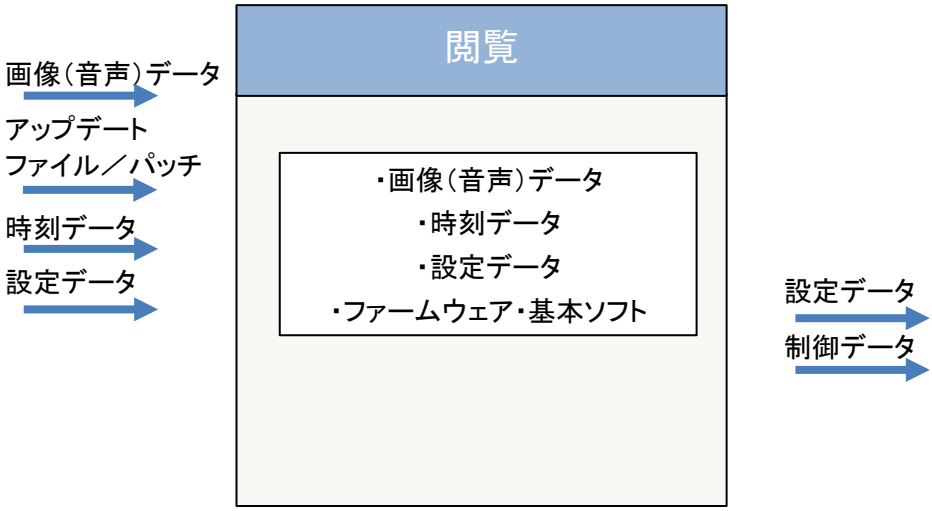


図 2-4　「閲覧」機能で保持するデータ・入出力するデータ

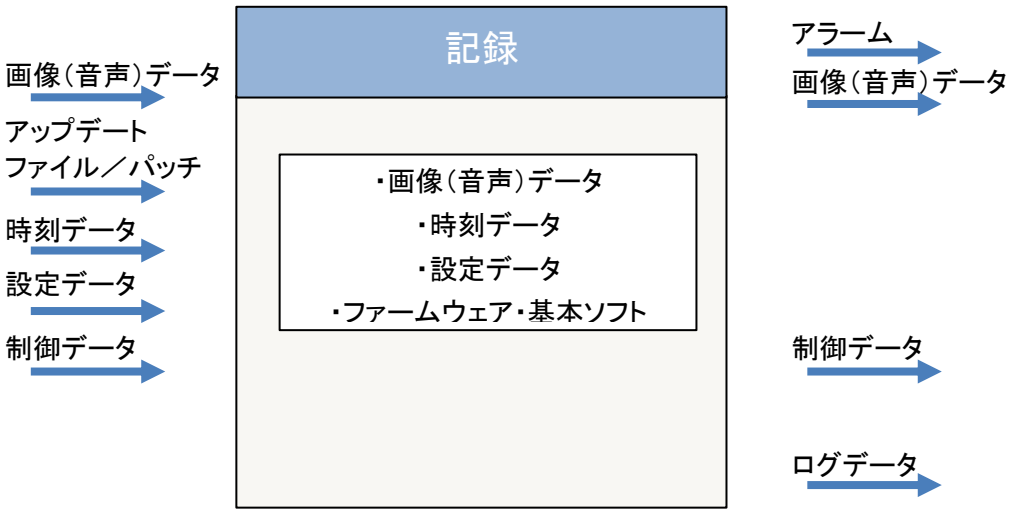


図 2-5　「記録」機能で保持するデータ・入出力するデータ

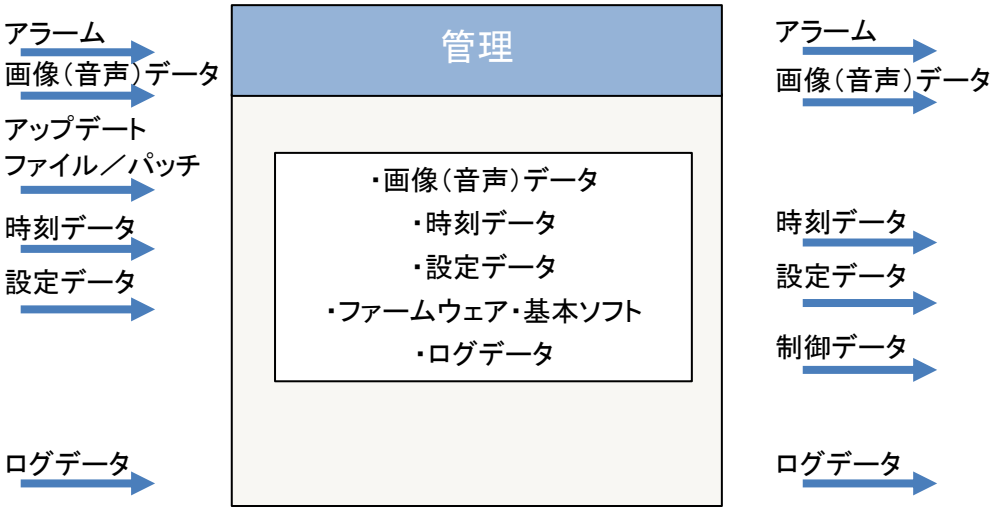


図 2-6　「管理」機能で保持するデータ・入出力するデータ

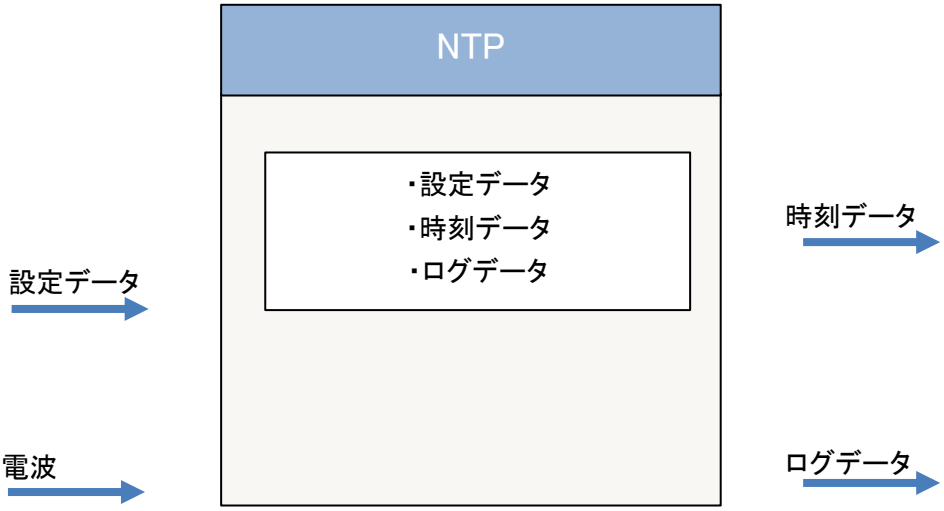


図 2-7　「NTP」機能で保持するデータ・入出力するデータ

なお、ログやアラーム等を受信するサーバ／装置は、本調査におけるネットワークカメラシステムの範囲外とする。ネットワークカメラシステムは、外部システムからの入力データが正しいかどうかの確認を行い、ログやアラーム等の出力データが正しく出力されるよう保護を行うものとする。

また、ベンダ等によるカメラのファームウェアアップデートは、ベンダ等他者による対策が必要であるため、本調査におけるネットワークカメラシステム範囲外とする。

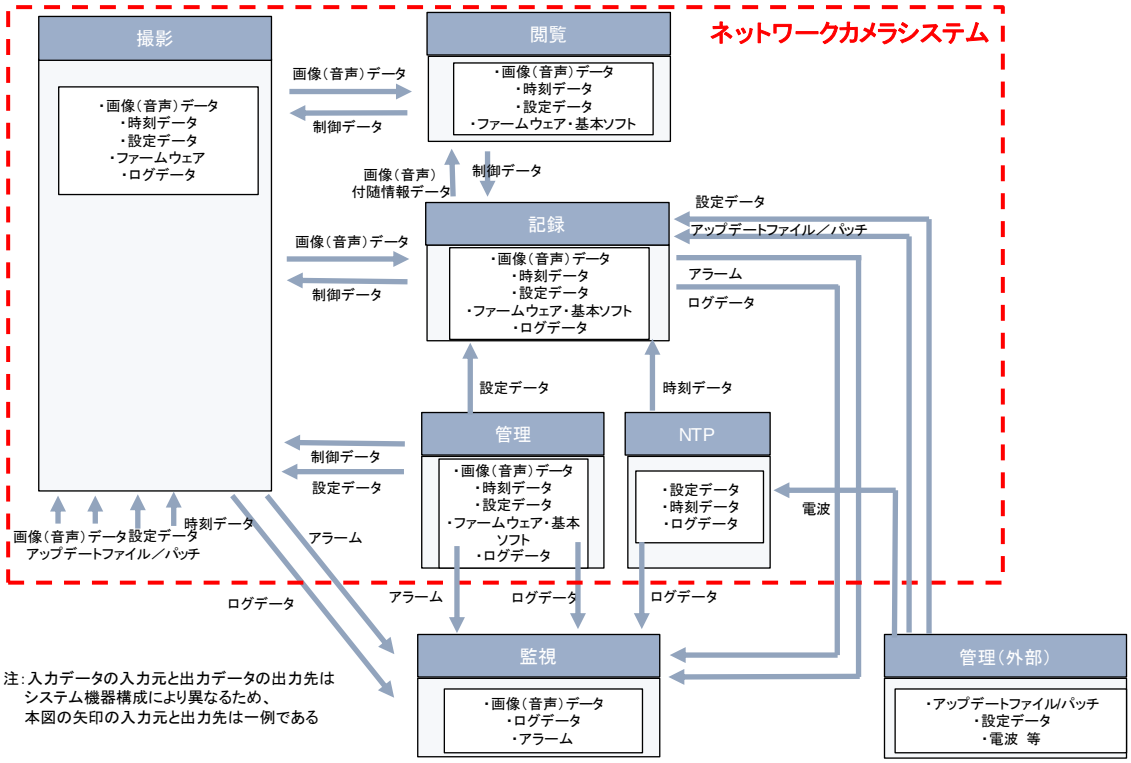


図 2-8　ネットワークカメラシステムモデル図

2.3.2 ネットワークカメラシステムモデル構成図の作成

2.3.1 で整理したネットワークシステムの構成要素を踏まえ、ネットワークカメラシステムモデル構成図を作成した。（図 2-9）

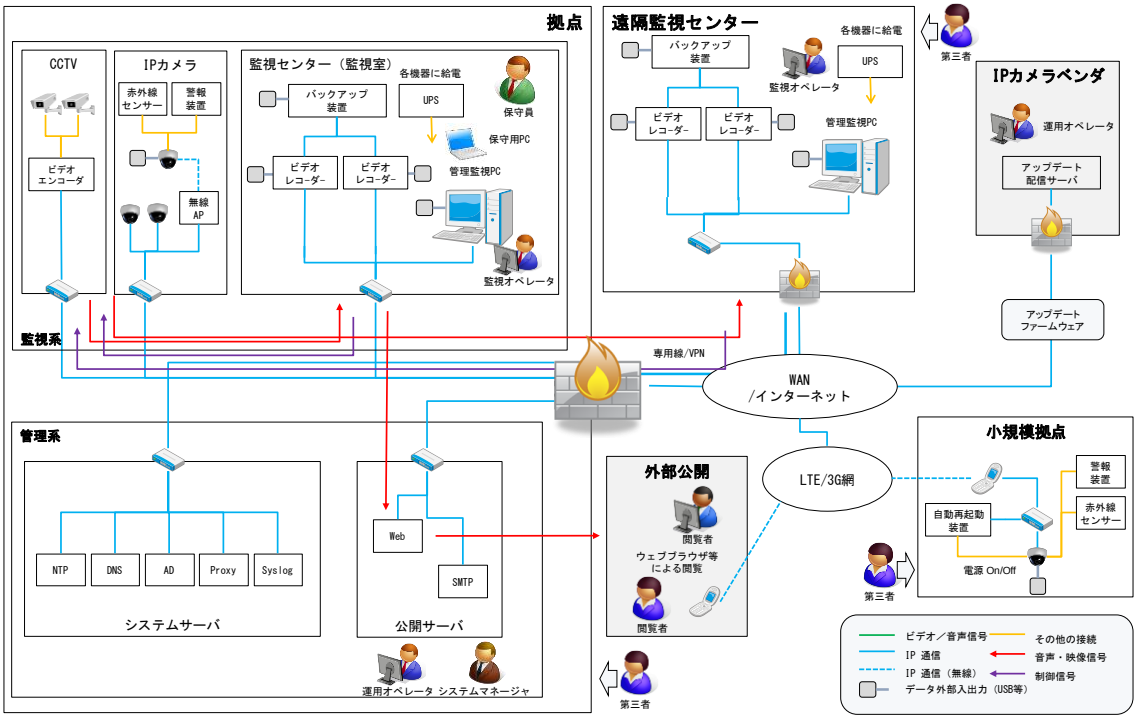


図 2-9　ネットワークカメラシステムモデル構成図

2.3.3 構成図と機能図のマッピング

ネットワークカメラシステムモデル構成図を機能図と紐付けると、図 2-10 の通りとなる。

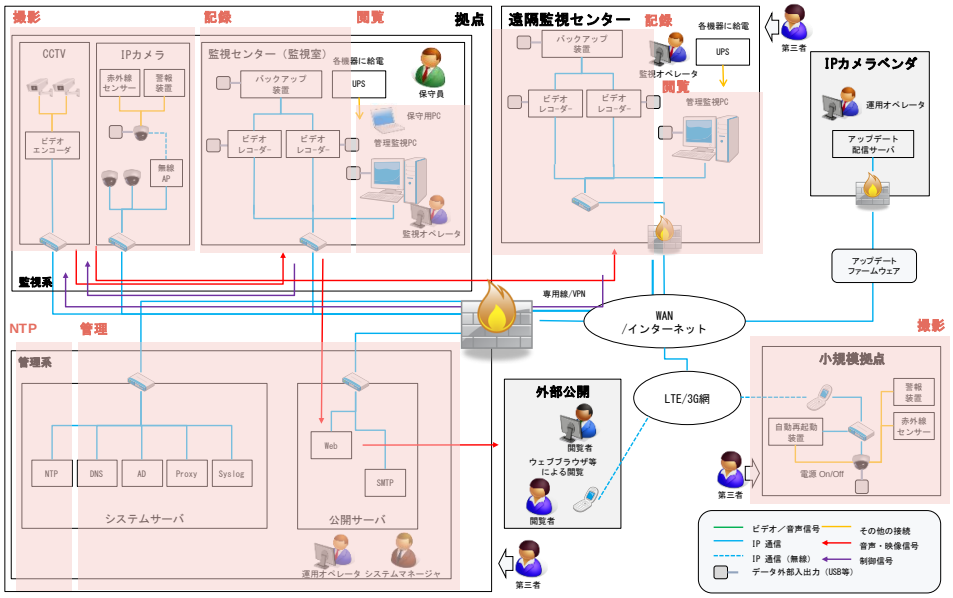


図 2-10 ネットワークカメラシステム構成図と機能図のマッピング

2.3.4 モデル分類

ネットワークカメラシステムモデル構成図は、脅威及び対策の差違を明確化するために定めた。しかしながら、脅威の差違については、保護資産となる重要な機器やデータが保護可能な場所にあるかどうかで異なるため、保護資産が拠点や監視センター等管理可能な区域にあるかどうか、保護されたネットワーク接続形態かどうかについて、製品カタログ等におけるネットワークカメラシステムモデル構成図を調査した。

その結果、ネットワークカメラシステムモデル構成図は以下の 4 つに分類されることがわかった。

(A) 単体拠点モデル

単体の拠点に、カメラシステムと監視センターがあり、拠点内の監視員が監視する形態

（例）　役所、美術館や複数のテナント等が入居するビル、工場・倉庫　等

(B) 複数拠点モデル

複数の拠点にカメラが存在し、主拠点の監視センター内の監視員が監視する形態

（例）　出先機関を持つ役所・教育機関、複数拠点を持つ工場・倉庫　等

(C) 小規模モデル

複数の拠点にカメラが存在し、ネットワーク経由で独立した監視センターが監視する形態

（例）　マンションや小さなビル　等

(D) 大規模モデル

大量の拠点にカメラが存在し、主拠点に管理機能を持ち、ネットワーク経由で独立した監視センターが監視する形態

（例）　防災モニタリングシステム、交通監視　等

製品カタログ等の各利用事例と分類の対応は**別紙 2** に示す。

ネットワークカメラシステムの類型を A～D の 4 分類に分け、ネットワークカメラシステムモデル図を作成したものが**図 2-11～図 2-14** になる。

A のモデルは、単体の拠点内にシステムが構築されるため、ネットワークは LAN となり、拠点も物理的に保護されている。

B のモデルは、外部拠点との接続として、ネットワークに WAN が利用される。

C のモデルは、外部拠点との接続として、ネットワークに WAN が利用されることに加え、外部拠点に遠隔監視センターが含まれた場合、監視人員が委託事業者となる。

D のモデルは、インターネットに接続され、接続先には閲覧者が存在する。

A・B・C のモデルは、通信キャリアが運用する WAN や委託事業者という外部を利用することによる脅威が存在すると考えられるが、本調査では、通信キャリアや委託事業者は調達者による契約において管理可能であるとし、保護資産及び保護資産が保存された機器が、調達者が管理可能な拠点・監視センター内で構築・運用されているとする。ただし、D のモデルは保護資産及び保護資産が保存された機器が調達者の管理可能な拠点・監視センター外にも存在している点が特徴的である。

本調査のアウトプットであるチェックリスト案は、調達者自身がこれから調達しようとするシステムの特性を判断することが容易となるような分類とするため、以下の条件でシステムモデルを「閉域網」（A・B・C モデル）と「広域網」（D モデル）で分類し作成した。

- 閉域網

保護資産及び保護資産が保存された機器が、調達者の管理可能な拠点・監視センター内で構築・運用されている

- 広域網

保護資産及び保護資産が保存された機器が調達者の管理可能な拠点・監視センター外にも存在している

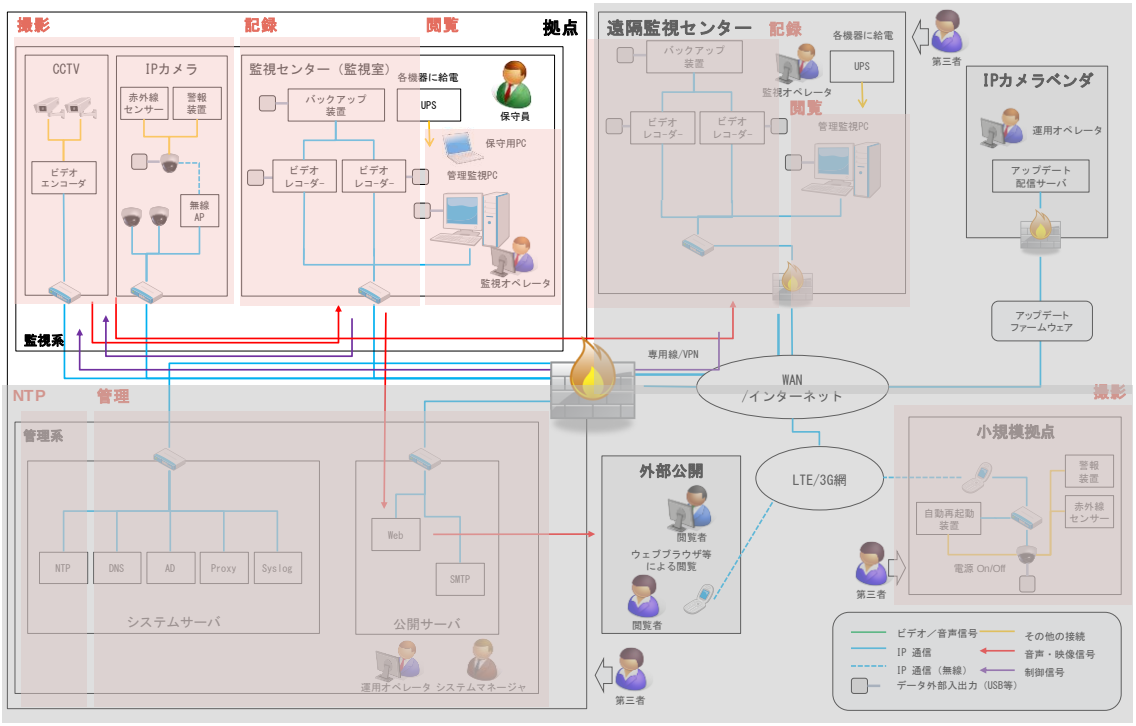


図 2-11　単体拠点モデル

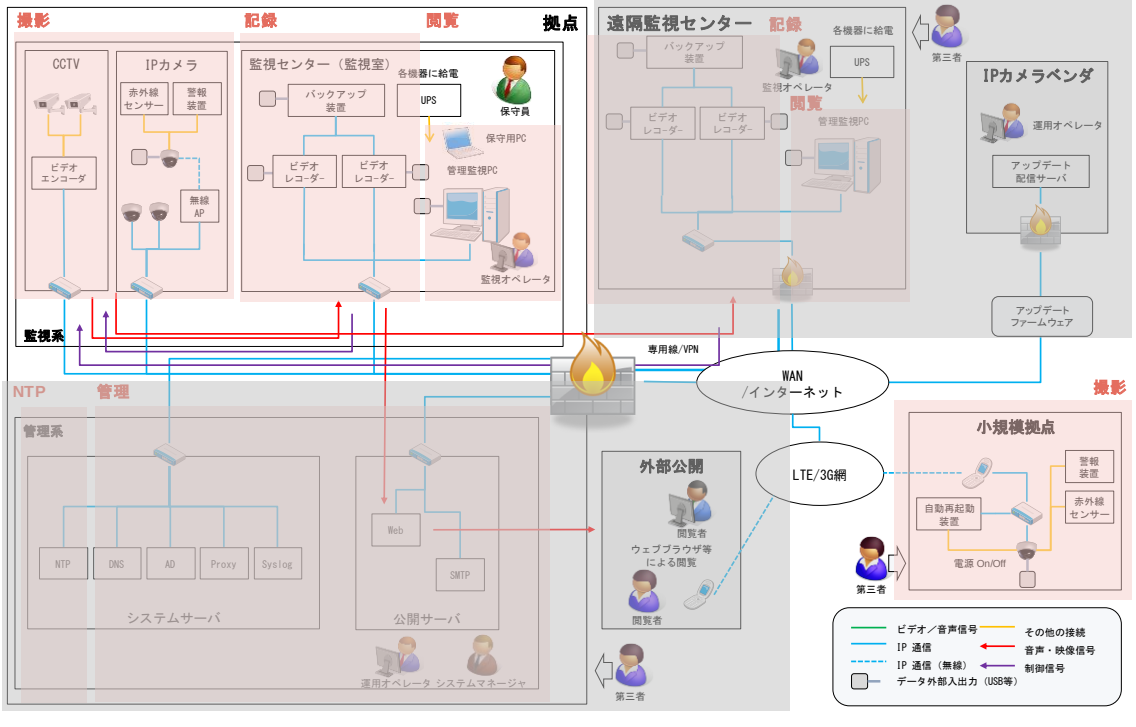


図 2-12　複数拠点モデル

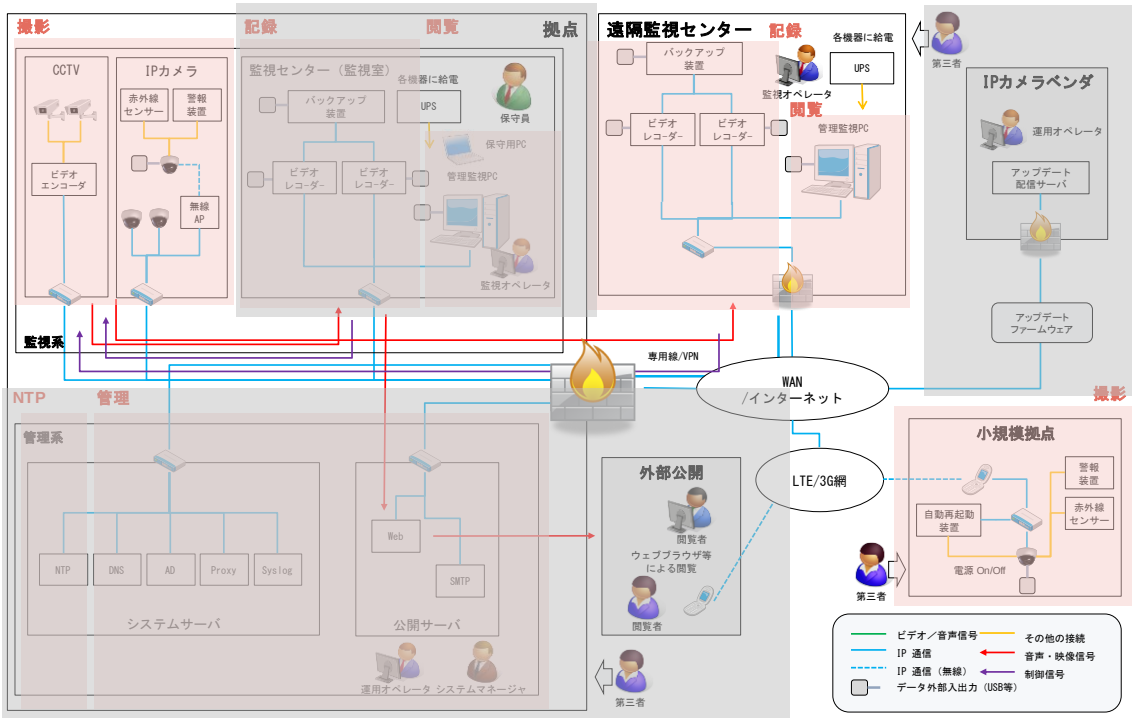


図 2-13　小規模モデル

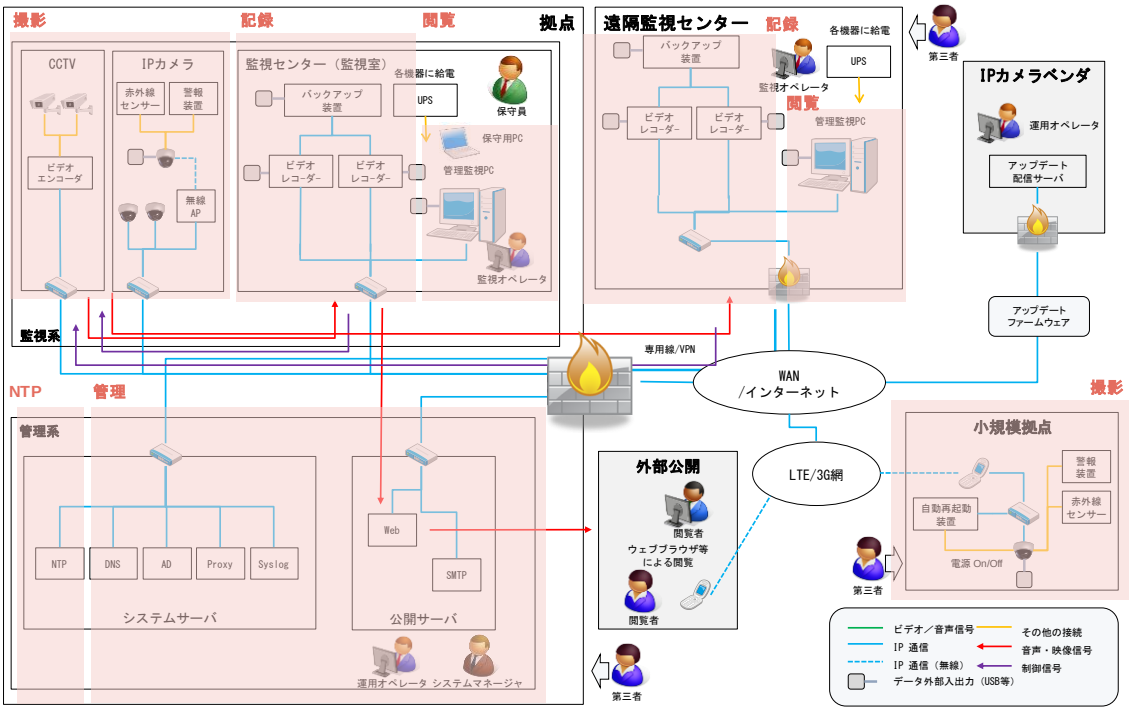


図 2-14　大規模モデル

3. 利用形態における情報セキュリティ課題の調査・分析

3.1 調査概要

ネットワークカメラシステムが安全に利用されるための要件を明確にするため、システムモデル毎に想定される情報セキュリティ上の脅威について分析した。

脅威分析は、機能で分類した「機能図」と、構成機器を整理した「ネットワークカメラシステム構成図」を用いて、以下の手順で実施した。

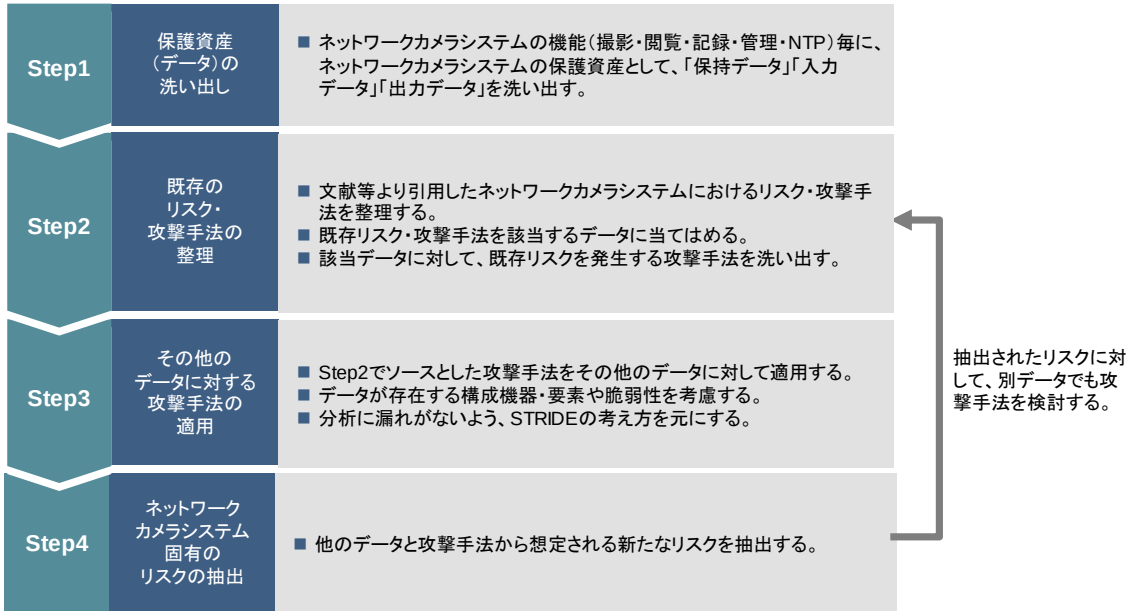


図 3-1　脅威分析方法

3.2 システムモデルにおける保護すべき資産

はじめに、ネットワークカメラに存在する各種データを、製品カタログ等を元に**表 3-1** の通り整理した。なお、各データに含まれる詳細なデータは**別紙 3** に示す。

表 3-1　ネットワークカメラシステムが有するデータ

分類	説明
画像（音声）データ	
画像データ	画像データ
音声データ	音声データ
付随データ	画像（音声）から生成された付加情報
分析データ	動態検知、対象物特定等のために、画像（音声）データを画像処理・分析して得られるデータ
時刻データ	時刻データ
設定データ	（動きの制限値等、機器に設定され保存されるデータ）
識別認証情報	端末、管理者、利用者等を識別・認証する情報
ネットワーク情報	ネットワーク接続のための管理情報
画像情報	画像に関する管理情報
音声情報	音声に関する管理情報
動画配信情報	動画配信に関する情報
録画情報	録画に関する情報
アラーム設定	アラームを出すための条件
通知設定	通知を出すための条件
スケジュール情報	撮影・記録・画像送信等の定期的な作動時間
ロギング設定	ログ取得時の条件
サービス設定	サービスの起動/停止に関する管理情報
時刻設定	時刻設定に関する管理情報
カメラ設定	カメラに関する設定
外部機器設定	外部機器に関する設定
表示設定	表示・ビューワーに関する設定
ファームウェア（・基本ソフト）データ	機器に搭載されるファームウェア、ソフトウェアに搭載される OS 等基本ソフトウェア
ログデータ	操作、アラーム発生、データの変更などのイベント内容と発生時刻
センサーデータ	センサーから得られたデータ
アラーム	アラーム
アップデートファイル／パッチ	ファームウェアや基本ソフトのアップデートするためのデータ、パッチ
制御データ	（機器に対する動きの指令等、機器に保存されないデータ）
パン・チルト	カメラの上下・左右の動きを制御するデータ
ズーム	カメラのズーム等の動きを制御するデータ
再起動	機器の再起動を制御するデータ
電波	時刻のソースとなる電波

また、前述の通り、保護資産をデータとするとシステム構成により異なる機器にデータが紐付けられてしまうことから、脅威分析において漏れなく脅威を洗い出すために、保護資産を機器ではなく機能と紐付けた。データを各機能と紐付けた結果が**表 3-2** である。

表 3-2　データと機能の対応

分類	撮影			閲覧			記録			管理			NTP		
	入力	保持	出力	入力	保持	出力	入力	保持	出力	入力	保持	出力	入力	保持	出力
画像（音声）データ															
画像データ	○	○	○	○	○		○	○	○	○	○	○			
音声データ	○	○	○	○	○		○	○	○	○	○	○			
付随データ		○	○	○	○		○	○	○	○	○	○			
分析データ								○	○		○	○			
時刻データ	○	○		○	○		○	○		○	○	○			○
設定データ															
識別認証情報	○	○		○	○	○	○	○		○	○	○	○	○	
ネットワーク情報	○	○		○	○		○	○		○	○	○	○	○	
画像情報	○	○		○	○		○	○		○	○				
音声情報	○	○		○	○		○	○		○	○				
動画配信情報	○	○													
録画情報							○	○		○	○	○			
アラーム設定	○	○					○	○		○	○				
通知設定	○	○					○	○		○	○				
スケジュール情報	○	○		○	○		○	○		○	○				
ロギング設定	○	○					○	○		○	○		○	○	
サービス設定							○	○		○	○				
時刻設定	○	○		○	○		○	○		○	○				
カメラ設定	○	○													
外部機器設定	○	○													
表示設定				○	○										
ファームウェア（・基本ソフト）データ		○			○			○			○				
ログデータ		○	○					○	○	○	○	○		○	○
センサーデータ	○														
アラーム			○						○	○		○			
アップデートファイル／パッチ	○			○			○			○					
制御データ															
パン・チルト	○			○		○	○		○			○			
ズーム	○			○		○	○		○			○			
再起動	○											○			
電波													○		

3.3 システムモデルにおける想定される攻撃者及び攻撃機会

本調査における脅威分析において想定する攻撃者は、保護資産（機器及びデータ）及びデータが存在する機器間のネットワークへの攻撃機会があるものとして、**表 2-4** で整理したネットワークカメラシステムに関わる要員のうち、第三者（利用者）を対象とするものとする。

表 3-3　攻撃者及び攻撃機会

攻撃者		攻撃機会
名称	説明	
利用者	システムの管理者により、システムへの特定のアクセス権限が付与された者	権限を越えた操作や閲覧
管理者	各拠点において、システムの管理を行う者	攻撃を行わない
保守員	ファームウェアアップデート、アラームの受信を管理者に代行して請け負う者	攻撃を行わない
第三者	システムへの正当なアクセス権を所有しない者	機器への物理的な接触 ネットワークへの接続

なお、本調査では管理者や保守員等による内部犯行については対象としないが、内部犯行への対策については、IPA「組織における内部不正防止ガイドライン」が参考となる。

3.4 システムモデルにおける攻撃手法

ネットワークシステムにおける攻撃手法は、ネットワークカメラシステムで想定される脆弱性に対して、STRIDE の考え方を元に検討し、抽出を行った。

STRIDE はマイクロソフトが提唱する脅威の分類手法であり、「なりすまし」「データの改ざん」「否認」「情報の暴露」「サービス不能」「権限の昇格」の 6 項目に分類している（**表 3-4**）。STRIDE を元に抽出した攻撃手法が**表 3-5** である。

本調査で整理した脆弱性は、以下の通りである。

＜脆弱性一覧＞

【1】脆弱な管理者・利用者パスワード
【2】脆弱なアカウント認証機構または不備
【3】脆弱な機器間の認証機構または不備
【4】ファイル等アクセス制御の不備
【5】ネットワークアクセス管理の不備
【6】外部記憶デバイスの物理ポートの管理不備
【7】脆弱な送信元検証機構や検証機構の不備
【8】web アプリケーションの脆弱性
【9】ネットワークサービスの脆弱性管理の不備・ゼロデイ脆弱性
【10】利用者権限で利用できるコマンド等の脆弱性管理の不備・ゼロデイ脆弱性
【11】通信セッションの管理不備
【12】通信データ保護（暗号化等）の不備
【13】ユーザーのリテラシー不足
【14】ファームウェア更新時の署名の不備または検証の不備

表 3-4　STRIDE の考え方

なりすまし	なりすましとは、コンピュータに対し、他のユーザーを装うことです。なりすましにより、攻撃者は不法にアクセスを行い、ユーザー名やパスワードなど、他のユーザーの認証情報を使用します。
データの改ざん	データの改ざんとは、データを意図的に操作することです。データベースに保持されている永続データを承認を受けずに変更したり、インターネットなどのオープンなネットワークを介してコンピュータ間で伝送されるデータを改ざんすることなどがこれにあたります。
否認	否認とは、ユーザーがあるアクションを行ったこと否認し、相手はこのアクションを証明する方法がないことを意味します。たとえば、禁止された操作をトレースする能力がないシステムで、ユーザーが不法な操作を行うことを言います。 同様に、否認防止とは否認に対抗するシステムの機能を意味します。たとえば、ユーザーが商品を購入した場合、商品の受領に際して署名が必要な場合などです。販売元は、署名入りの受領書をユーザーが商品を受け取った証拠として使用できます。
情報の暴露	情報の暴露とは、アクセス権限を持たない個人に情報が公開されることです。たとえば、あるユーザーが、アクセスを許可されていないファイルを読むことができたり、侵入者がコンピュータ間で伝送されているデータを読むことができる場合です。
サービス不能	DoS （サービス不能） 攻撃により、正規のユーザーへのサービスが中断されます。Web サーバを一時的に使用できない状態にするなどが DoS 攻撃です。システムの可用性および信頼性を高めるには、特定の DoS 攻撃に対してシステムを保護する必要があります。
権限の昇格	権限の昇格とは、権限のないユーザーがアクセス権限を得ることです。システム全体を使用不可にしたり、破壊するために十分なアクセス権限を得ることになります。また、権限の昇格により、攻撃者がシステムの防御をすべて破り、信頼されたシステムの一部となることも考えられます。

（出所）マイクロソフト「セキュリティ上の脅威の評価」[1]

[1] 2017 年 12 月時点では引用元が存在しない。同様の概要は Microsoft の The STRIDE Threat Model のページで確認できる。

表 3-5　攻撃手法

脆弱性（具体的な例）	脅威分類	攻撃手法	
【V1】脆弱な管理者・利用者パスワード	なりすまし	【A1-1】	管理者・利用者になりすまして構成要素に不正アクセス
・短時間で推測可能な単純なパスワード（password, abcdefg）	データ改ざん	【A1-2】	アクセス可能なデータの不正な閲覧・改ざん・消去が行われる
・機器の初期パスワードを変更せずに使用	否認	【A1-3】	管理者権限で侵入・攻撃の痕跡をログ等から消去する
・利用者IDと同じパスワード	情報の暴露	【A1-4】	管理者権限・使用者権限で構成要素に保存された情報を不正に入手する
・パスワードを設定しない（空）	サービス不能	【A1-5】	管理者権限でサービスを不正に停止する
	権限の昇格	【A1-6】	利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手
【V2】脆弱なアカウント認証機構または不備	なりすまし	【A2-1】	力任せの攻撃（ブルートフォースアタック）で管理者・利用者になりすます
・パスワード認証の試行回数上限を設定していない	データ改ざん	【A2-2】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
・不特定多数がアクセス可能な環境で単一要素認証（パスワードのみ）	否認	【A2-3】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	情報の暴露	【A2-4】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	サービス不能	【A2-5】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	権限の昇格	【A2-6】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
【V3】脆弱な機器間の認証機構または不備	なりすまし	【A3-1】	他機器になりすまして中間者攻撃を行う
・通信相手の真正性を確認しない	データ改ざん	【A3-2】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
・通信相手の真正性をIPアドレス等なりすまし可能な情報で判断	否認	【A3-3】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
・通信相手の真正性確認手順に中間者攻撃・リプレイ攻撃等の問題がある	情報の暴露	【A3-4】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	サービス不能	【A3-5】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	権限の昇格	【A3-6】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
【V4】ファイル等アクセス制御の不備	なりすまし	【A4-1】	（なりすます必要はない）
・システム設定ファイル等、管理者が利用するファイルが利用者全員に公開されている	データ改ざん	【A4-2】	アクセス可能なデータの不正な閲覧・改ざん・消去が行われる
・ウェブサーバが管理者権限で稼動していてすべてのファイルにアクセス可能	否認	【A4-3】	侵入・攻撃の痕跡をログ等から消去する
	情報の暴露	【A4-4】	構成要素に保存された情報を不正に入手する
	サービス不能	【A4-5】	設定ファイルを書き換えてサービスを不正に停止する
	権限の昇格	【A4-6】	（権限昇格を行う必要はない）
【V5】ネットワークアクセス管理の不備	なりすまし	【A5-1】	（なりすます必要はない）
・ネットワークアクセスをアクセスが必要な機器に限定していない	データ改ざん	【A5-2】	（アクセス可能であることは攻撃のチャンスが大きくなるだけでデータ改ざんには他の脆弱性が必要）
・不要なネットワークポートへのアクセスを制限していない	否認	【A5-3】	（アクセス可能であることは攻撃のチャンスが大きくなるだけでデータ改ざんには他の脆弱性が必要）
	情報の暴露	【A5-4】	サービスに接続してサービスプログラム名・バージョンなどを不正に入手（攻撃に悪用する）
	サービス不能	【A5-5】	開いているネットワークポートに大量の通信データを送り通信を妨害
	権限の昇格	【A5-6】	（アクセス可能であることは攻撃のチャンスが大きくなるだけでデータ改ざんには他の脆弱性が必要）
【V6】外部記憶デバイスの物理ポートの管理不備	なりすまし	【A6-1】	（なりすます必要はない）
・USBポート等、外部記憶デバイスを接続できるポートへのアクセスを制限していない	データ改ざん	【A6-2】	攻撃者が不正に外部記憶デバイス等をUSBポート等に直接挿入して、システム内にマルウェアを注入
	否認	【A6-3】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	情報の暴露	【A6-4】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	サービス不能	【A6-5】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	権限の昇格	【A6-6】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
【V7】脆弱な送信元検証機構や検証機構の不備	なりすまし	【A7-1】	（脆弱な機器間の認証機構または不備を悪用した攻撃と同じ）
・通信相手の識別手段をIPアドレスのみとしている（偽装可能）	データ改ざん	【A7-2】	（脆弱な機器間の認証機構または不備を悪用した攻撃と同じ）
・そもそも通信相手を識別していない	否認	【A7-3】	（脆弱な機器間の認証機構または不備を悪用した攻撃と同じ）
	情報の暴露	【A7-4】	（脆弱な機器間の認証機構または不備を悪用した攻撃と同じ）
	サービス不能	【A7-5】	（脆弱な機器間の認証機構または不備を悪用した攻撃と同じ）
	権限の昇格	【A7-6】	（脆弱な機器間の認証機構または不備を悪用した攻撃と同じ）
【V8】webアプリケーションの脆弱性	なりすまし	【A8-1】	管理インタフェース等の脆弱性を悪用して管理者・利用者になりすます
・Webアプリとして実装される機器の管理インタフェースに様々な脆弱性が残っている	データ改ざん	【A8-2】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
・ウェブサーバが管理者権限で稼動していて管理者として任意のアクセスが可能	否認	【A8-3】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	情報の暴露	【A8-4】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	サービス不能	【A8-5】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	権限の昇格	【A8-6】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
【V9】ネットワークサービスの脆弱性管理の不備・ゼロデイ脆弱性	なりすまし	【A9-1】	ネットワークサービスの脆弱性を悪用して管理者・利用者権限を奪取
・HTTP・DNSサービスなど内蔵サービスを更新しない（ファームウェア更新を行わない）	データ改ざん	【A9-2】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
・サービスに未知の脆弱性が存在する	否認	【A9-3】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	情報の暴露	【A9-4】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	サービス不能	【A9-5】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	権限の昇格	【A9-6】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
【V10】利用者権限で利用できるコマンド等の脆弱性管理の不備・ゼロデイ脆弱性	なりすまし	【A10-1】	コマンド等の脆弱性を悪用して管理者・利用者権限を奪取
・機器に内蔵されるコマンド類を更新しない（ファームウェア更新を行わない）	データ改ざん	【A10-2】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
・コマンド類に未知の脆弱性が存在する	否認	【A10-3】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	情報の暴露	【A10-4】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	サービス不能	【A10-5】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	権限の昇格	【A10-6】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
【V11】通信セッションの管理不備	なりすまし	【A11-1】	通信を盗聴・再利用することで管理者・利用者になりすます
・セッションシーケンスの整合性を検証していない（順序が間違った指令を受け入れる）	データ改ざん	【A11-2】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
・セッションIDが推測可能・盗聴可能（第三者の割込みを受ける）	否認	【A11-3】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
・セッションIDが推測可能・盗聴可能（第三者の割込みを受ける）	情報の暴露	【A11-4】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	サービス不能	【A11-5】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
	権限の昇格	【A11-6】	（脆弱な管理者・利用者パスワードを悪用した攻撃と同じ）
【V12】通信データ保護（暗号化等）の不備	なりすまし	【A12-1】	通信を盗聴・再利用することで管理者・利用者になりすます
・機密性の高い情報を通信する際にデータの暗号化・改ざん検知を行わない	データ改ざん	【A12-2】	平文のデータあるいは強度の弱い暗号化を解除して通信を改ざんする
・通信相手の真正性検証を行わない	否認	【A12-3】	（この脆弱性単独では否認につながる攻撃はできない）
・脆弱な暗号アルゴリズムが有効になっている	情報の暴露	【A12-4】	暗号強度が低い通信を解読する
・暗号鍵を保護していない	サービス不能	【A12-5】	（この脆弱性単独ではサービス不能状態にはできない）
	権限の昇格	【A12-6】	（この脆弱性単独では権限昇格はできない）
【V13】ユーザのリテラシー不足	なりすまし	【A13-1】	メール・電話等で管理者になりすまして利用者をだます
・不正な第三者が試みる攻撃手法・被害に関する知識が不足している	データ改ざん	【A13-2】	標的型攻撃によりマルウェア感染をひきおこす
・パスワード管理・情報管理に関する意識が低い	否認	【A13-3】	メール・電話等で管理者になりすまして他管理者に不正な動作（ログファイルの削除・設定変更等）を行わせる
	情報の暴露	【A13-4】	メール・電話等で関係者になりすまし情報を引き出す
	サービス不能	【A13-5】	メール・電話等で管理者になりすまして他管理者に不正な動作（サービス停止・設定変更等）を行わせる
	権限の昇格	【A13-6】	メール・電話等で管理者になりすまして他管理者に不正な動作（管理者権限を必要とする）を行わせる
【V14】ファームウェア更新時の署名の不備または検証の不備	なりすまし	【A14-1】	改ざんしたファームウェアを正式なファームウェアと信じ込ませる
・ファームウェア更新データに電子署名が行われていない	データ改ざん	【A14-2】	ファームウェアを改ざんすることで必要な権限を問わず任意の動作を行わせることができる
・ファームウェア更新データの電子署名を検証していない	否認	【A14-3】	ファームウェアを改ざんすることで必要な権限を問わず任意の動作を行わせることができる
・ファームウェア更新データの電子署名証明書の有効性を検証していない	情報の暴露	【A14-4】	ファームウェアを改ざんすることで必要な権限を問わず任意の動作を行わせることができる
	サービス不能	【A14-5】	ファームウェアを改ざんすることで必要な権限を問わず任意の動作を行わせることができる
	権限の昇格	【A14-6】	ファームウェアを改ざんすることで必要な権限を問わず任意の動作を行わせることができる

3.5 攻撃による影響

ネットワークカメラシステムにおける攻撃の影響として考慮すべきものは、攻撃によるリスクが大きいものである。本調査では、リスクとは脅威と脆弱性によって発生する影響とする。すなわち、ネットワークシステムにおいて保護すべき資産が脅かされること、ネットワークカメラシステムの機能が脅かされること、ネットワークカメラシステムが接続する他のシステムの機能に影響を与えることとした。攻撃のリスク分類及び、そのリスク分類の具体例を**表 3-6** に示す。

表 3-6　攻撃によるリスク

分類	リスク（例）
保護資産が脅かされること	・画像データが改ざんされる ・画像データの流出する、不正に閲覧される ・画像データが閲覧不能となる
機能が脅かされること	・カメラの設定データの改ざん、消失等により、撮影・記録ができなくなる
他のシステムに影響を与えること	・機器がボット化され、DoS 攻撃などの踏み台となったり、他のカメラをボットネットに取り込んだりする

3.6 脅威

前述したネットワークカメラシステム（**図 2-3**～**図 2-7**）における脅威分析を、機能を踏まえてデータ毎に行った。データ毎に対応するリスクを示したものが**表 3-7** であり、発生するリスクとリスクを発生する元となるデータを有する機器の対応を示したものが表 3-8 である。

表 3-7　リスク一覧

分類	1．漏えい	2．改ざん	3．消去
A．画像（音声）データ			
画像データ 音声データ	【A-1-1】 画像（音声）データが不正に閲覧される	【A-2-1】 画像（音声）データが改ざんされる → 信頼性が失われる	【A-3-1】 画像（音声）データが不正に消去される
付随データ	–	【A-2-2】 付随データ（保存時のタイムスタンプ等）が改ざんされる → 信頼性が失われる	–
分析データ	–	【A-2-3】 分析データ（検知用データ等）が改ざんされる → 検知ができない	【A-3-2】 分析データ（検知用データ等）が不正に消去される → 検知ができない
B．時刻データ	–	【B-2-1】 時刻データが改ざんされる（なりすましにより、偽の時刻データを出力される） → カメラの機能（撮影、記録等）が果たせない 【B-2-2】 時刻データが改ざんされる（なりすましにより、偽の時刻データを出力される） → 信頼性・証拠性が失われる	–
C．設定データ			
識別認証情報	【C-1-1】 ユーザID・PWが漏えいする → 不正アクセスを引き起こす 【C-1-2】 ユーザID・PWが漏えいする → 機器がボット化され、DoS攻撃などの踏み台として利用される 【C-1-3】 ユーザID・PWが漏えいする → 管理者権限を不正に奪取され、踏み台として利用される 【C-1-4】 ユーザID・PWが漏えいする → 管理者権限を不正に奪取され、サービスを不正に利用される	【C-2-1】 ユーザID・PWを改ざんされる → 対象機器にアクセスが不可能となる 【C-2-2】 ユーザID・PWを改ざんされる → 管理者権限を不正に奪取され、踏み台として利用される 【C-2-3】 ユーザID・PWを改ざんされる → 管理者権限を不正に奪取され、サービスを不正に利用される	–
ネットワーク情報	【C-1-5】 ネットワーク情報が漏えいする → カメラやルーター等への攻撃等により、カメラの機能（撮影、記録等）が果たせない	【C-2-4】 ネットワーク情報が改ざんされる → 画像（音声）データにアクセスできず、閲覧できない 【C-2-5】 ネットワーク情報が改ざんされる → 不正サイトへ誘導される	【C-3-1】 ネットワーク情報が不正に消去される → 画像（音声）データにアクセスできず、閲覧できない
画像情報	–	【C-2-6】 画像情報が改ざんされる → カメラの機能（撮影、記録等）が果たせない（解像度設定が改ざんされ撮影・記録できない等）	【C-3-2】 画像情報が不正に消去される → カメラの機能（撮影、記録等）が果たせない（解像度設定が消去され撮影・記録できない等）
音声情報	–	【C-2-7】 音声情報が改ざんされる → カメラの機能（撮影、記録等）が果たせない（音量設定が改ざんされ撮影・記録できない等）	【C-3-3】 音声情報が不正に消去される → カメラの機能（撮影、記録等）が果たせない（音量設定が消去され撮影・記録できない等）
動画配信情報	–	–	–

分類	1．漏えい	2．改ざん	3．消去
C．設定データ			
録画情報	【C-1-6】 設定データが漏えいする → 内部状態が推測され、ネットワーク構造や各機能情報が漏えいする	【C-2-8】 設定データ（スケジュール情報等）が改ざんされる → カメラの機能（撮影、記録等）が果たせない（指定した時刻にカメラが起動しない 等） 【C-2-9】 設定データ（カメラ設定等）が改ざんされる → 不正な機器の制御・操作が行われる（撮影のための設定（プライベートゾーンやカメラ位置等）や条件（明るさ等）を改ざんし、対象物が撮影できないようにする、等） 【C-2-10】 設定データ（サービス設定等）が改ざんされる → サービス機能が果たせない（アラーム条件や通知先情報が改ざんされ、アラームが鳴らない等） 【C-2-11】 設定データ（サービス設定等）が改ざんされる → 要求を大量に送りつけ、通信帯域を圧迫し、サービスを妨害する 【C-2-12】 設定データ（スケジュール情報、録画に関する情報等）が改ざんされる → 機器（あるいはシステム全体）の記録容量を低下させる	【C-3-4】 設定データ（スケジュール情報等）が不正に消去される → カメラの機能（撮影、記録等）が果たせない（指定した時刻にカメラが起動しない 等） 【C-3-5】 設定データ（カメラ設定等）が不正に消去される → 不正な機器の制御・操作が行われる（撮影のための設定（プライベートゾーンやカメラ位置等）や条件（明るさ等）を不正に消去し、対象物が撮影できないようにする、等） 【C-3-6】 設定データ（サービス設定等）が不正に消去される → サービス機能が果たせない（アラーム条件や通知先情報が不正に消去され、アラームが鳴らない等）
アラーム設定			
通知設定			
スケジュール情報			
ロギング設定			
サービス設定			
時刻設定			
カメラ設定			
外部機器設定			
表示設定			
D．ファームウェア（・基本ソフト）データ	－	【D-2-1】 ファームウェアの機能・データが改ざんされる → パッチが当てられなくなり、脆弱性対処ができなくなる 【D-2-2】 ファームウェアの機能・データが改ざんされる → ボットネットに取り込まれる	－
E．ログデータ	【E-1-1】 ログデータが漏えいする → 内部状態が推測され、ネットワーク構造や各機能情報が漏えいする	【E-2-1】 ログデータが改ざんされる → 攻撃者の行動が分析不可となる	【E-3-1】 ログデータが不正に消去される → 攻撃者の行動が分析不可となる
センサーデータ	－	－	－
アラーム	－	－	－
F．アップデートファイル／パッチ	－	【F-2-1】 アップデートファイル/パッチが改ざんされる → システムが想定通りに動作せず、カメラの機能（撮影、記録等）が果たせない	－
制御データ			
パン・チルト	－	－	－
ズーム			
再起動			
電波	－	－	－
機器全体	【G-1-1】 盗難 → リバースエンジニアリングやサービスの不正利用が行われる → 内部情報が推測され、機器構造、ネットワーク構造、各機能情報が漏えいする	－	【G-3-1】 破壊 → カメラの機能（撮影、記録等）が果たせない

表 3-8　リスクと対象機器

リスク	IPカメラ	レコーダー	エンコーダー	管理PC	保守PC	各種サーバ	VPN装置	PoEハブ	無線AP
【A-1-1】 画像（音声）データが不正に閲覧される	○	○	○	○	○				
【A-2-1】 画像（音声）データが改ざんされる → 信頼性が失われる	○	○	○	○	○				
【A-2-2】 付随データ（保存時のタイムスタンプ等）が改ざんされる → 信頼性が失われる	○	○	○	○	○				
【A-2-3】 分析データ（検知用データ等）が改ざんされる → 検知ができない	○	○	○	○	○				
【A-3-1】 画像（音声）データが不正に消去される	○	○	○	○	○				
【A-3-2】 分析データ（検知用データ等）が不正に消去される → 検知ができない	○	○	○	○	○				
【B-2-1】 時刻データが改ざんされる（なりすましにより、偽の時刻データを出力される） → カメラの機能（撮影、記録等）が果たせない	○	○	○	○	○	○	○	○	○
【B-2-2】 時刻データが改ざんされる（なりすましにより、偽の時刻データを出力される） → 信頼性・証拠性が失われる	○	○	○	○	○	○	○	○	○
【C-1-1】 ユーザID・PWが漏えいする → 不正アクセスを引き起こす	○	○	○	○	○	○	○	○	○
【C-1-2】 ユーザID・PWが漏えいする → 機器がボット化され、DoS攻撃などの踏み台として利用される	○	○	○	○	○	○	○	○	○
【C-1-3】 ユーザID・PWが漏えいする → 管理者権限を不正に奪取され、踏み台として利用される	○	○	○	○	○	○	○	○	○
【C-1-4】 ユーザID・PWが漏えいする → 管理者権限を不正に奪取され、サービスを不正に利用される	○	○	○	○	○	○	○	○	○
【C-1-5】 ネットワーク情報が漏えいする → カメラやルーター等への攻撃等により、カメラの機能（撮影、記録等）が果たせない	○	○	○	○	○	○	○	○	○
【C-1-6】 設定データが漏えいする → 内部状態が推測され、ネットワーク構造や各機能情報が漏えいする	○	○	○	○	○	○	○	○	○
【C-2-1】 ユーザID・PWを改ざんされる → 対象機器にアクセスが不可能となる	○	○	○	○	○	○	○	○	○
【C-2-2】 ユーザID・PWを改ざんされる → 管理者権限を不正に奪取され、踏み台として利用される	○	○	○	○	○	○	○	○	○
【C-2-3】 ユーザID・PWを改ざんされる → 管理者権限を不正に奪取され、サービスを不正に利用される	○	○	○	○	○	○	○	○	○
【C-2-4】 ネットワーク情報が改ざんされる → 画像（音声）データにアクセスできず、閲覧できない	○	○	○	○	○	○	○	○	○

リスク	IPカメラ	レコーダー	エンコーダー	管理PC	保守PC	各種サーバ	VPN装置	PoEハブ	無線AP
【C-2-5】 ネットワーク情報が改ざんされる → 不正サイトへ誘導される	○	○	○	○	○	○	○	○	○
【C-2-6】 画像情報が改ざんされる → カメラの機能（撮影、記録等）が果たせない（解像度設定が改ざんされ撮影・記録できない 等）	○	○	○	○	○				
【C-2-7】 音声情報が改ざんされる → カメラの機能（撮影、記録等）が果たせない（音量設定が改ざんされ撮影・記録できない 等）	○	○	○	○	○				
【C-2-8】 設定データ（スケジュール情報等）が改ざんされる → カメラの機能（撮影、記録等）が果たせない（指定した時刻にカメラが起動しない 等）	○	○	○	○	○	○	○	○	○
【C-2-9】 設定データ（カメラ設定等）が改ざんされる → 不正な機器の制御・操作が行われる（撮影のための設定（プライベートゾーンやカメラ位置等）や条件（明るさ等）を改ざんし、対象物が撮影できないようにする、等）	○	○	○	○	○	○	○	○	○
【C-2-10】 設定データ（サービス設定等）が改ざんされる → サービス機能が果たせない（アラーム条件や通知先情報が改ざんされ、アラームが鳴らない等）	○	○	○	○	○	○	○	○	○
【C-2-11】 設定データ（サービス設定等）が改ざんされる → 要求を大量に送りつけ、通信帯域を圧迫し、サービスを妨害する	○	○	○	○	○	○	○	○	○
【C-2-12】 設定データ（スケジュール情報、録画に関する情報等）が改ざんされる → 機器（あるいはシステム全体）の記録容量を低下させる	○	○	○	○	○	○	○	○	○
【C-3-1】 ネットワーク情報が不正に消去される → 画像（音声）データにアクセスできず、閲覧できない	○	○	○	○	○	○	○	○	○
【C-3-2】 画像情報が不正に消去される → カメラの機能（撮影、記録等）が果たせない（解像度設定が消去され撮影・記録できない 等）	○	○	○	○	○				
【C-3-3】 音声情報が不正に消去される → カメラの機能（撮影、記録等）が果たせない（音量設定が消去され撮影・記録できない 等）	○	○	○	○	○				
【C-3-4】 設定データ（スケジュール情報等）が不正に消去される → カメラの機能（撮影、記録等）が果たせない（指定した時刻にカメラが起動しない 等）	○	○	○	○	○	○	○	○	○
【C-3-5】 設定データ（カメラ設定等）が不正に消去される → 不正な機器の制御・操作が行われる（撮影のための設定（プライベートゾーンやカメラ位置等）や条件（明るさ等）を不正に消去し、対象物が撮影できないようにする、等）	○	○	○	○	○	○	○	○	○
【C-3-6】 設定データ（サービス設定等）が不正に消去される → サービス機能が果たせない（アラーム条件や通知先情報が不正に消去され、アラームが鳴らない等）	○	○	○	○	○	○	○	○	○
【D-2-1】 ファームウェアの機能・データが改ざんされる → パッチが当てられなくなり、脆弱性対処ができなくなる	○	○	○	○	○	○	○	○	○
【D-2-2】 ファームウェアの機能・データが改ざんされる → ボットネットに取り込まれる	○	○	○	○	○	○	○	○	○
【E-1-1】 ログデータが漏えいする → 内部状態が推測され、ネットワーク構造や各機能情報が漏えいする	○	○	○	○	○	○	○	○	○
【E-2-1】 ログデータが改ざんされる → 攻撃者の行動が分析不可となる	○	○	○	○	○	○	○	○	○
【E-3-1】 ログデータが不正に消去される → 攻撃者の行動が分析不可となる	○	○	○	○	○	○	○	○	○
【F-2-1】 アップデートファイル/パッチが改ざんされる → システムが想定通りに動作せず、カメラの機能（撮影、記録等）が果たせない	○	○	○	○	○	○	○	○	○

4. 情報セキュリティ課題に対応するセキュリティ機能や運用の調査・分析

4.1 調査概要

前章で識別された情報セキュリティ課題に関して対抗・回避可能なネットワークカメラシステムのセキュリティ機能や運用策について分析し、攻撃手法に紐付けて整理した。

4.2 システムモデルの機能及び運用に関する要件

脅威分析の結果、3.4 で示したネットワークカメラシステムにおける脆弱性においては、**表 3-5** の攻撃手法を適用すると、ネットワークカメラシステムに対して**表 3-6** のリスクが発生することが示された。

ネットワークカメラシステムにおける脆弱性、ライフサイクルのフェーズ（設計・構築時、運用時、廃棄時）毎の一般的な対策、攻撃手法を整理した。（**別紙 4**）

5. まとめ

本調査では、ネットワークカメラシステムの利用において考慮すべきセキュリティ上の要件を明確にし、調達者がネットワークカメラシステムの構築や利用に際してセキュリティ対策を確認するためのチェックリスト案を策定した。

脅威分析においては、ネットワークカメラに特徴的な脅威として、最も重要な保護資産である画像データ改ざん・漏えい・閲覧不可に加え、カメラの設定機能（撮影スケジュール、カメラ動作等）や時刻データの改ざん等により撮影・記録機能が脅かされる点や、DoS の踏み台となる点が想定された。特にカメラやレコーダー等、保護資産を有する機器、管理 PC 等設定機能を持つ機器、及びこれらを接続するネットワークに対する不正アクセス、接続元の詐称、ファームウェア等の脆弱性を突いた攻撃等が抽出された。

これらの脅威に対して、対策要件について整理を行い整理した。ネットワークカメラシステムでは、一般的な IT 環境で利用するセキュリティ対策ソフトや IDS/IPS 等のセキュリティ製品の導入が難しく、またソフトウェアの更新が困難であることを踏まえ、ユーザーの識別認証、機器や接続点の物理的な保護、最低限守るべき機器（カメラとレコーダー）間の通信の保護が重要であることが示された。

用語集・略語集

ARP スプーフィング	IP アドレスを MAC アドレスに変換する際の ARP リクエストに対する応答を偽装することにより、LAN 上の通信機器になりすます攻撃手法
DoS 攻撃	ネットワークにおいてサービスの提供を不能にさせる攻撃。攻撃手法の例として、攻撃対象となるルータに不正なパケットを大量に送信して、そのパケット処理によりルータを過負荷にしてサービスを停止させる
HTTPS	SSL/TLS プロトコルで暗号化したセキュアな通信路上で HTTP 通信を行うこと
NTP サーバ	ネットワーク上で時刻データを配信するサーバ
Syslog サーバ	ログの外部送信の際に用いられる Syslog プロトコルに対応してログを受信するサーバ
TELNET	インターネットなどの TCP/IP ネットワークを通じて別のコンピュータを遠隔操作するための通信プロトコル
VLAN	ネットワーク機器などの機能により、物理的には一つの LAN（Local Area Network）において、論理的に複数の LAN を構成する技術
サーバ証明書	認証局事業者が発行する、サーバのサイト運営組織が実在していることを証明するもの。クライアントに対して、情報を送受信するサーバが意図する相手（サーバの運営組織等）によって管理されるサーバであることを確認する手段を提供することと、SSL/TLS による暗号通信を行うために必要なサーバの公開鍵情報をクライアントに正しく伝えること、の 2 つの役割を持っている。
ステルス機能	無線アクセスポイントを区別するための SSID を見えないようにする機能
ファイアウォール	外部ネットワークから内部ネットワーク、もしくは内部ネットワークから外部ネットワークへの情報の出入を制限するセキュリティシステム
ボット	コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク （インターネット）を通じて外部から操ることを目的として作成されたプログラム。感染すると、自らネットワークを通じて外部の指令サーバと通信を行い、外部からの指示により指定された処理（スパムメール送信活動・ DoS 攻撃などの攻撃活動･ネットワーク感染活動・ ネットワークスキャン活動など）を実行する
リバースエンジニアリング	ソフトウェアやハードウェアなどを分解、または解析し、その設計や仕様などを明らかにすること
ルート証明書	サーバ証明書の署名検証を行うために用いる、クライアントに登録されている認証局（CA）の証明書

以上

別紙１　文献調査対象システムの構成機器一覧

文書種類	番号	発行機関	文書題名	利用用途	IPカメラ	アナログカメラ	HD-SDI	エンコーダー（ネットワークビデオトランスミッター）	カメラ側音声集音マイク	カメラ側音声出力スピーカー	赤外線投光器	センサー	警告装置（アラームライト等）	SIM	SDカード	無線アクセスポイント	PoEインジェクター	L2スイッチ（スイッチングハブ、PoEスイッチ等）	LAN/シリアル変換器	レコーディングサーバー	管理コンソール（モニター、キーボード等）	管理ソフト（ビューアーソフト）	映像切り替えシステム（マトリクススイッチャ）	管理PC	管理サーバー	SQLサーバー	アクセスコントロールシステム（active directory等）	FTPサーバー	ダウンコンバーター	分配器	バックアップサーバー（外付けHDD等）	UPS（無停電電源装置）	自動再起動装置	GPSタイムサーバー	NTPサーバー	接点入力ユニット	メディアコンバーター	L3スイッチ	ゲートウェイ（ルーター、ファイアウォール）	管理側マイク	管理側スピーカー	クラウド	保守用PC	閲覧専用端末（タブレット等）
国内外のネットワークカメラの導入傾向や事例に関する調査レポート	1	IPA	IoT開発におけるセキュリティ設計の手引き	個人住宅・事業所向け遠隔監視	○																																	○			○		
	2	電気設備学会	電気設備学会誌「インターネットを支える電気設備，電気設備を支えるインターネット技術7　監視カメラ」	複合オフィスビル向け内部監視/外部公開	○	○												○		○	○			○													○	○					
	3	電気設備学会	電気設備学会誌「インターネットを支える電気設備，電気設備を支えるインターネット技術7　監視カメラ」	河川・道路向け広域監視/道路状況・気象状況・水位等の河川状況・交通渋滞状況等の外部公開	○			○												○		○	○			○																		
	4	日本防犯設備協会	防犯カメラシステムネットワーク構築ガイドⅡ	遠隔監視	○													○		○	○			○								○				○							
製品カタログ	5	TOA	「TRIFORAシリーズ」カタログ	マンション向け内部監視	○	○		○										○		○	○																						
	6	TOA	「TRIFORAシリーズ」カタログ	工場・物流倉庫向け内部監視	○												○	○		○	○	○										○		○		○							
	7	NECネッツエスアイ	「オンデマンド防犯カメラ」カタログ	オンデマンド用記録	○									○	○																								○				
	8	三菱電機	「ネットワークカメラ・システム MELOOK3」カタログ	複数拠点向け集中遠隔監視	○				△（カメラに内蔵）											○	○	○									○									○				
	9	CANON	ネットワークカメラ総合カタログ	大規模（的確な状況認識とインシデントへの対処が必要とされるシステム）向け検知	○															○					○	○	○																
	10	システム・ケイ	株式会社システム・ケイ　ホームページ	道路等向けモニタリング	○									○						○	○			○															○				
	11	システム・ケイ	株式会社システム・ケイ　ホームページ	教育機関向け内部監視/授業の外部公開	○													○		○				○															○				
	12	システム・ケイ	株式会社システム・ケイ　ホームページ	小売店向け内部監視	○													○		○																			○				○
	13	Axis	IP-Surveillance design guide	内部監視/外部公開	○	○		○														○		○															○				○
	14	SIMENS	Video Surveillance	小規模店舗・美術館向け内部監視	○							○										○	○		○		○																
	15	SIMENS	Video Surveillance	銀行・交通向け遠隔監視	○															○				○																			○
	16	Panasonic	ネットワークカメラ総合カタログ	モーション検知・アラーム通知	○								○		○									○				○															
	17	Axis	IP-Surveillance design guide	モーション検知・アラーム通知	○							○	○							○				○																			○
調達仕様書	18	秋田県由利本荘市	「由利・ネットワークカメラ」公示書	—	○																																						
	19	独立行政法人国立美術館	「国立新美術館　監視映像録画サーバー及びネットワークカメラ調達」仕様書	国立新美術館の監視	○															○	○											△（本調達外）											
	20	関東管区警察局山梨県情報通信部	「IPネットワークカメラほか2件」見積もり依頼書	—	○																○	○																					
	21	独立行政法人水資源機構阿木川ダム管理所	「阿木川ダムネットワークカメラ設備工事」仕様書	ダム現地及び監視室及び管理所の監視	○											○		○		○	○																○						
	22	高知市消防局	「高知市消防局高所監視カメラ（カメラネットワーク網）整備事業業務委託」仕様書	マンション及び山及び消防署の遠隔監視	○		○	○								○	○	○		○	○	○	○	○					○	○			○			○			○			○		
	23	地方独立行政法人　広島市立病院機構	広島市立安佐市民病院　監視カメラシステム賃貸借	広島市立安佐市民病院における監視	○				△（カメラに内蔵）									△（本調達外）		○	○			○								△（カメラに内臓）											△（本調達外）
	24	公立大学法人三重県立看護大学	ネットワーク防犯カメラシステム整備仕様書	三重県立看護大学における防犯用	○													○		○	○																						
	25	独立行政法人国立美術館東京国立近代美術館	東京国立近代美術館フィルムセンター監視カメラ更新工事仕様書	東京国立近代美術館フィルムセンターの各フロアの監視	○				△（本調達外）	△（本調達外）										○	○			○							△（本調達外）	○										
	26	日本原子力研究開発機構（JAEA）	「情報セキュリティ用監視カメラの更新」仕様書	情報センターの建屋への侵入及び入退室の監視	○							△（本調達外）			○					○											○											
	27	広島市立大学	「広島市立大学監視カメラ システム（2013）賃貸借」仕様書	学内監視カメラシステム	○							○								○	○	○	○																				
	28	独立行政法人 日本芸術文化振興会	「国立能楽堂防犯カメラ及び録画装置等の調達（配線・取付・調整・既存機器の撤去を含む）」仕様書	国立能楽堂防犯カメラシステム	○													○		○	○	○	○																				
	29	公立大学法人和歌山県立医科大学	「監視カメラ」仕様書	学内向け内部監視	○												○			○	○																						
	30	神戸市	神戸市河川モニタリングシステム第2回情報提供招聘仕様書案	河川モニタリングシステム	○						○									○		○											○	○						○				

別紙２　文献調査対象システムとシステムモデルの対応表

文書種類	番号	発行機関	文書題名	利用用途	モデル	広域 OR 閉域
国内外のネットワークカメラの導入傾向や事例に関する調査レポート	1	IPA	IoT 開発におけるセキュリティ設計の手引き	個人住宅・事業所向け遠隔監視	C	閉域
	2	電気設備学会	電気設備学会誌「インターネットを支える電気設備，電気設備を支えるインターネット技術 7 監視カメラ」	複合オフィスビル向け内部監視/外部公開	B	閉域
	3	電気設備学会	電気設備学会誌「インターネットを支える電気設備，電気設備を支えるインターネット技術 7 監視カメラ」	河川・道路向け広域監視/道路状況・気象状況・水位等の河川状況・交通渋滞状況等の外部公開	D	広域
	4	日本防犯設備協会	防犯カメラシステムネットワーク構築ガイドⅡ	遠隔監視	C	閉域
製品カタログ	5	TOA	「TRIFORA シリーズ」カタログ	マンション向け内部監視	C	閉域
	6	TOA	「TRIFORA シリーズ」カタログ	工場・物流倉庫向け内部監視	A	閉域
	7	NEC ネッツエスアイ	「オンデマンド防犯カメラ」カタログ	オンデマンド用記録	B	閉域
	8	三菱電機	「ネットワークカメラ・システム MELOOK3」カタログ	複数拠点向け集中遠隔監視	B	閉域
	9	CANON	ネットワークカメラ総合カタログ	大規模（的確な状況認識とインシデントへの対処が必要とされるシステム）向け検知	D	広域
	10	システム・ケイ	株式会社システム・ケイ　ホームページ	道路等向けモニタリング	D	広域
	11	システム・ケイ	株式会社システム・ケイ　ホームページ	教育機関向け内部監視/授業の外部公開	A	閉域
	12	システム・ケイ	株式会社システム・ケイ　ホームページ	小売店向け内部監視	A	閉域
	13	Axis	IP-Surveillance design guide	内部監視/外部公開	A	閉域
	14	SIMENS	Video Surveillance	小規模店舗・美術館向け内部監視	C	閉域
	15	SIMENS	Video Surveillance	銀行・交通向け遠隔監視	C	閉域
	16	Panasonic	ネットワークカメラ総合カタログ	モーション検知・アラーム通知	C	閉域
	17	Axis	IP-Surveillance design guide	モーション検知・アラーム通知	C	閉域
調達仕様書	18	秋田県由利本荘市	「由利・ネットワークカメラ」公示書	（記載無し）	B	閉域
	19	独立行政法人国立美術館	「国立新美術館　監視映像録画サーバー及びネットワークカメラ調達」仕様書	国立新美術館の監視	B	閉域
	20	関東管区警察局山梨県情報通信部	「ＩＰネットワークカメラほか２件」見積もり依頼書	（記載無し）	B	閉域
	21	独立行政法人水資源機構阿木川ダム管理所	「阿木川ダムネットワークカメラ設備工事」仕様書	ダム現地及び監視室及び管理所の監視	C	閉域
	22	高知市消防局	「高知市消防局高所監視カメラ（カメラネットワーク網）整備事業業務委託」仕様書	マンション及び山及び消防署の遠隔監視	D	広域
	23	地方独立行政法人広島市立病院機構	広島市立安佐市民病院　監視カメラシステム賃貸借	広島市立安佐市民病院における監視	D	広域
	24	公立大学法人三重県立看護大学	ネットワーク防犯カメラシステム整備仕様書	三重県立看護大学における防犯用	B	閉域
	25	独立行政法人国立美術館東京国立近代美術館	東京国立近代美術館フィルムセンター監視カメラ更新工事仕様書	東京国立近代美術館フィルムセンターの各フロアの監視	A	閉域
	26	日本原子力研究開発機構(JAEA)	「情報セキュリティ用監視カメラの更新」仕様書	情報センターの建屋への侵入及び入退室の監視	A	閉域
	27	広島市立大学	「広島市立大学監視カメラ システム（２０１３）賃貸借」仕様書	学内監視カメラシステム	B	閉域
	28	独立行政法人日本芸術文化振興会	「国立能楽堂防犯カメラ及び録画装置等の調達（配線・取付・調整・既存機器の撤去を含む）」仕様書	国立能楽堂防犯カメラシステム	A	閉域
	29	公立大学法人和歌山県立医科大学	「監視カメラ」仕様書	学内向け内部監視	A	閉域
	30	神戸市	神戸市河川モニタリングシステム第 2 回情報提供招聘仕様書案	河川モニタリングシステム	D	広域

別紙 3　モデル図機能別の詳細データ一覧

分類	説明	データ（撮影）	データ（閲覧）	データ（記録）	データ（管理）	データ（NTP）
画像（音声）データ						
画像データ	画像データ	画像データ、アラーム画像	画像データ、アラーム画像	画像データ、アラーム画像	画像データ、アラーム画像	
音声データ	音声データ	音声データ	音声データ	音声データ	音声データ	
付随データ	画像（音声）から生成された付加情報	カメラ名、時間情報、オブジェクトの位置、大きさ、撮影場所、カメラ設定、編集ソフトウェア Iフレーム挿入間隔変更・強制挿入 キープアライブ、ケイパビリティ 録画情報（CPU使用率、録画ビットレート、再生ビットレート）	カメラ名、時間情報、オブジェクトの位置、大きさ、撮影場所、カメラ設定、編集ソフトウェア Iフレーム挿入間隔変更・強制挿入 キープアライブ、ケイパビリティ 録画情報（CPU使用率、録画ビットレート、再生ビットレート）	カメラ名、時間情報、オブジェクトの位置、大きさ、撮影場所、カメラ設定、編集ソフトウェア Iフレーム挿入間隔変更・強制挿入 キープアライブ、ケイパビリティ 録画情報（CPU使用率、録画ビットレート、再生ビットレート）	カメラ名、時間情報、オブジェクトの位置、大きさ、撮影場所、カメラ設定、編集ソフトウェア Iフレーム挿入間隔変更・強制挿入 キープアライブ、ケイパビリティ 録画情報（CPU使用率、録画ビットレート、再生ビットレート）	
分析データ	動態検知、対象物特定等のために、画像（音声）データを画像処理・分析して得られるデータ			検知用データ（背景映像）	検知用データ（背景映像）	
時刻データ	時刻データ	時刻データ	時刻データ	時刻データ	時刻データ	時刻データ
設定データ						
識別認証情報	端末、管理者、利用者等を識別・認証する情報	端末情報（機器名称、ホスト名、グループ） 管理者・ユーザID・PW、認可情報	端末情報（機器名称、ホスト名、グループ） 管理者・ユーザID・PW、認可情報	端末情報（機器名称、ホスト名、グループ） 管理者・ユーザID・PW、認可情報	端末情報（機器名称、ホスト名、グループ） 管理者・ユーザID・PW、認可情報	端末情報（機器名称、ホスト名、グループ） 管理者・ユーザID・PW、認可情報
ネットワーク情報	ネットワーク接続のための管理情報	接続先、プロトコル、証明書 LAN（インターフェース、最大パケットサイズ）、 IPv6（アドレス、プレフィックス長、デフォルトゲートウェイアドレス、自動設定（RA、DHCPv6））、IPv4（アドレス設定方式、サブネットマスク、デフォルトゲートウェイアドレス） DNS（ネームサーバーアドレス、自動設定、DHCP/DHCPv6、ホスト名、DDNS設定、サーチドメイン）、mDNS SNMP カメラへのFTPアクセス、FTPサーバ プロキシ HTTP、UPnP、DDNS メール通知先アドレス、通知先メールサーバ（IPアドレス、識別認証情報）、サーバ証明書 ホストアクセス制限（IPv4、IPv6） SSL/TLS、802.1X（認証方式、証明書）、IPsec（設定方法、自動鍵交換）	接続先、プロトコル、証明書 LAN（インターフェース、最大パケットサイズ）、 IPv6（アドレス、プレフィックス長、デフォルトゲートウェイアドレス、自動設定（RA、DHCPv6））、IPv4（アドレス設定方式、サブネットマスク、デフォルトゲートウェイアドレス） DNS（ネームサーバーアドレス、自動設定、DHCP/DHCPv6、ホスト名、DDNS設定、サーチドメイン）、mDNS SNMP カメラへのFTPアクセス、FTPサーバ プロキシ HTTP、UPnP、DDNS メール通知先アドレス、通知先メールサーバ（IPアドレス、識別認証情報）、サーバ証明書 ホストアクセス制限（IPv4、IPv6） SSL/TLS、802.1X（認証方式、証明書）、IPsec（設定方法、自動鍵交換）	接続先、プロトコル、証明書 LAN（インターフェース、最大パケットサイズ）、 IPv6（アドレス、プレフィックス長、デフォルトゲートウェイアドレス、自動設定（RA、DHCPv6））、IPv4（アドレス設定方式、サブネットマスク、デフォルトゲートウェイアドレス） DNS（ネームサーバーアドレス、自動設定、DHCP/DHCPv6、ホスト名、DDNS設定、サーチドメイン）、mDNS SNMP カメラへのFTPアクセス、FTPサーバ プロキシ HTTP、UPnP、DDNS メール通知先アドレス、通知先メールサーバ（IPアドレス、識別認証情報）、サーバ証明書 ホストアクセス制限（IPv4、IPv6） SSL/TLS、802.1X（認証方式、証明書）、IPsec（設定方法、自動鍵交換）	接続先、プロトコル、証明書 LAN（インターフェース、最大パケットサイズ）、 IPv6（アドレス、プレフィックス長、デフォルトゲートウェイアドレス、自動設定（RA、DHCPv6））、IPv4（アドレス設定方式、サブネットマスク、デフォルトゲートウェイアドレス） DNS（ネームサーバーアドレス、自動設定、DHCP/DHCPv6、ホスト名、DDNS設定、サーチドメイン）、mDNS SNMP カメラへのFTPアクセス、FTPサーバ プロキシ HTTP、UPnP、DDNS メール通知先アドレス、通知先メールサーバ（IPアドレス、識別認証情報）、サーバ証明書 ホストアクセス制限（IPv4、IPv6） SSL/TLS、802.1X（認証方式、証明書）、IPsec（設定方法、自動鍵交換）	接続先、プロトコル、証明書 LAN（インターフェース、最大パケットサイズ）、 IPv6（アドレス、プレフィックス長、デフォルトゲートウェイアドレス、自動設定（RA、DHCPv6））、IPv4（アドレス設定方式、サブネットマスク、デフォルトゲートウェイアドレス） DNS（ネームサーバーアドレス、自動設定、DHCP/DHCPv6、ホスト名、DDNS設定、サーチドメイン）、mDNS SNMP カメラへのFTPアクセス、FTPサーバ プロキシ HTTP、UPnP、DDNS メール通知先アドレス、通知先メールサーバ（IPアドレス、識別認証情報）、サーバ証明書 ホストアクセス制限（IPv4、IPv6） SSL/TLS、802.1X（認証方式、証明書）、IPsec（設定方法、自動鍵交換）
画像情報	画像に関する管理情報	解像度、フレームレート、明るさ、カラー/モノクロ、画質 バックフォーカス、逆光補正、画像埋め込み クロッピング画像、クロッピングエリア、スマートコーディング、画像回転 パノラマ ADSR	解像度、フレームレート、明るさ、カラー/モノクロ、画質 バックフォーカス、逆光補正、画像埋め込み クロッピング画像、クロッピングエリア、スマートコーディング、画像回転 パノラマ ADSR	解像度、フレームレート、明るさ、カラー/モノクロ、画質 バックフォーカス、逆光補正、画像埋め込み クロッピング画像、クロッピングエリア、スマートコーディング、画像回転 パノラマ ADSR	解像度、フレームレート、明るさ、カラー/モノクロ、画質 バックフォーカス、逆光補正、画像埋め込み クロッピング画像、クロッピングエリア、スマートコーディング、画像回転 パノラマ ADSR	
音声情報	音声に関する管理情報	マイクボリューム	マイクボリューム	マイクボリューム	マイクボリューム	
動画配信情報	動画配信に関する情報	JPEG設定、MPEG-4設定、配信量制御（ビットレート）、目標ビットレート、使用ch、ストリーム設定、優先ストリーム、 動画配信方式（CGI制御/RTSP制御）、映像セッション管理、撮像モード、最大パケット長、VIQS、ベストエフォート配信 RTPパケット最大送信サイズ／HTTP最大セグメントサイズ、H.264エントロピー符号化方式、H.264プロファイル、圧縮方式、バナー				
録画情報	録画に関する情報			対象機器、一時保存画像数・画像タイプ、録画ファイル情報 録画モード（映像受信サイズ、映像フォーマット、最大フレームレート、録画ストリーム使用有無、カメラ位置、画質調整、フォーカス、外部デバイス出力、録画オプション） ディスク容量、最大・最小保存期間	対象機器、一時保存画像数・画像タイプ、録画ファイル情報 録画モード（映像受信サイズ、映像フォーマット、最大フレームレート、録画ストリーム使用有無、カメラ位置、画質調整、フォーカス、外部デバイス出力、録画オプション） ディスク容量、最大・最小保存期間	
アラーム設定	アラームを出すための条件	センサー閾値、トリガー事象の発生間隔、アラーム通知先・通知先認証情報、入出力の設定情報、アラームON/OFF、 アラーム連動動作、アラーム入力端子の状態変化、アラームマスク期間		センサー閾値、トリガー事象の発生間隔、アラーム通知先・通知先認証情報、入出力の設定情報、アラームON/OFF、 アラーム連動動作、アラーム入力端子の状態変化、アラームマスク期間	センサー閾値、トリガー事象の発生間隔、アラーム通知先・通知先認証情報、入出力の設定情報、アラームON/OFF、 アラーム連動動作、アラーム入力端子の状態変化、アラームマスク期間	
通知設定	通知を出すための条件	XML通知、顔検出、音検知、CGI検知、ショック検知 イベント、イベント連結、イベント優先度 検知感度、検知閾値、インジケータ		XML通知、顔検出、音検知、CGI検知、ショック検知 イベント、イベント連結、イベント優先度 検知感度、検知閾値、インジケータ	XML通知、顔検出、音検知、CGI検知、ショック検知 イベント、イベント連結、イベント優先度 検知感度、検知閾値、インジケータ	
スケジュール情報	撮影・記録・画像送信等の定期的な作動時間	スケジュール	スケジュール	スケジュール	スケジュール	
ロギング設定	ログ取得時の条件	ロギングレベル、容量、上書き設定、エラーログ、アラームログ		ロギングレベル、容量、上書き設定、エラーログ、アラームログ	ロギングレベル、容量、上書き設定、エラーログ、アラームログ	ロギングレベル、容量、上書き設定、エラーログ、アラームログ
サービス設定	サービスの起動/停止に関する管理情報			録画条件（センサー録画、動き検知、インテリジェント録画、音量検知、悲鳴検知、連結イベント）	録画条件（センサー録画、動き検知、インテリジェント録画、音量検知、悲鳴検知、連結イベント）	
時刻設定	時刻設定に関する管理情報	日付・時刻、時刻設定方法、NTPサーバ（DHCP・DHCPv6）、タイムゾーン、サマータイム	日付・時刻、時刻設定方法、NTPサーバ（DHCP・DHCPv6）、タイムゾーン、サマータイム	日付・時刻、時刻設定方法、NTPサーバ（DHCP・DHCPv6）、タイムゾーン、サマータイム	日付・時刻、時刻設定方法、NTPサーバ（DHCP・DHCPv6）、タイムゾーン、サマータイム	
カメラ設定	カメラに関する設定	パン・チルト制御範囲、プライバシーゾーン、可視範囲、カメラ動作、 VMDエリア、VMD付加情報、VMD感度タイプ、パトロール機能 同軸設定、RS-485設定、EXズーム、プリセットポジション、IR LED Light、 撮像モード（アスペクト比）、初期位置、スキャンモード、デイナイト、鮮明IRモード パノラマ レンズ歪み補正、電動バリフォーカルレンズのズーム/フォーカス ADSR 設置条件、位置制御、ワイパー／ウォッシャー制御、 リレー出力、外部入出力デバイス、電源周波数 自動追尾				
外部機器設定	外部機器に関する設定	SDメモリーカード設定				
表示設定	表示・ビューワーに関する設定		ビューワー設定（ユーザ認証・認可情報、） 表示方法（オンスクリーン表示、表示レイアウト、映像表示の回転）			
ファームウェア（・基本ソフト）データ	機器に搭載されるファームウェア、ソフトウェアに搭載されるOS等基本ソフトウェア	ファームウェア、バージョン	ファームウェア、バージョン	ファームウェア、バージョン	ファームウェア、バージョン	
ログデータ	操作、アラーム発生、データの変更などのイベント内容と発生時刻	システムログ、アクセスログ、アラームログ、エラーログ アクティビティログ、イベントログ		システムログ、アクセスログ、アラームログ、エラーログ アクティビティログ、イベントログ	システムログ、アクセスログ、アラームログ、エラーログ アクティビティログ、イベントログ	システムログ、アクセスログ、アラームログ、エラーログ アクティビティログ、イベントログ
センサーデータ	センサーから得られたデータ	センサーデータ				
アラーム	アラーム	アラーム		アラーム	アラーム	
アップデートファイル／パッチ	ファームウェアや基本ソフトのアップデートするためのデータ、パッチ	アップデートファイル、バッチ	アップデートファイル、バッチ	アップデートファイル、バッチ	アップデートファイル、バッチ	
制御データ						
パン・チルト	カメラの上下・左右の動きを制御するデータ	パン、チルト、旋回、絶対角度、ポジション、連続PTZ	パン、チルト、旋回、絶対角度、ポジション、連続PTZ	パン、チルト、旋回、絶対角度、ポジション、連続PTZ	パン、チルト、旋回、絶対角度、ポジション、連続PTZ	
ズーム	カメラのズーム等の動きを制御するデータ	ズーム、フォーカス、ドラッグ＆ズーム、クリック＆センタリング、自動追尾、速度	ズーム、フォーカス、ドラッグ＆ズーム、クリック＆センタリング、自動追尾、速度	ズーム、フォーカス、ドラッグ＆ズーム、クリック＆センタリング、自動追尾、速度	ズーム、フォーカス、ドラッグ＆ズーム、クリック＆センタリング、自動追尾、速度	
再起動	機器の再起動を制御するデータ	再起動			再起動	
電波	時刻のソースとなる電波					GPS、FM

別紙４　攻撃手法に対する対策一覧

機器	攻撃手法	悪用する脆弱性	一般的な対策 （設計・構築）	一般的な対策 （運用）	一般的な対策 （廃棄）
IP カメラ レコーダー 管理 PC 各種サーバ	・管理者・利用者になりすまして構成要素に不正アクセス - 管理者になりすまして構成要素（ファームウェア）に不正アクセス【A1-1】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A1-6 他】 - 力任せの攻撃（ブルートフォースアタック）で管理者・利用者になりすます【A2-1】 - 管理インタフェース等の脆弱性を悪用して管理者・利用者になりすます【A8-1】 - アクセス可能なデータ（ファームウェア）の不正な閲覧･改ざん･消去が行われる【A1-2 他】【A4-2】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A1-4 他】 - 管理者権限でサービスを不正に停止する【A1-5 他】 - 改ざんしたファームウェアを正式なファームウェアと信じ込ませる【V14-1】 - ファームウェアを改ざんすることで必要な権限を問わず任意の動作を行わせることができる【A14-2 他】 - サービスに接続してサービスプログラム名・バージョンなどを不正に入手（攻撃に悪用する）【A5-4】 - 開いているネットワークポートに大量の通信データを送り通信を妨害【A5-5】	【V1】脆弱な管理者・利用者パスワード	・ネットワーク経由での操作については強固な認証機構を導入する	・機器操作用の管理者・利用者認証に公開鍵を用いる場合 ・秘密鍵は平文で保管せず、パスフレーズでの暗号化、ハードウェアトークンの利用といった不正アクセス対策を施す	・認証情報をすべて確実に削除する ・画像（音声）データ等やカメラの設定データを削除する
		【V2】脆弱なアカウント認証機構または不備	・ネットワーク経由での操作については強固な認証機構を導入する	・機器操作用の管理者・利用者認証に公開鍵を用いる場合 ・秘密鍵は平文で保管せず、パスフレーズでの暗号化、ハードウェアトークンの利用といった不正アクセス対策を施す	↑
		【V4】ファイル等アクセス制御の不備	・管理者・利用者といったアカウント（ロール）にもとづくファイルアクセス制御を実装する	・ファイル・フォルダーごとに管理者・利用者のアクセス権限を設定する ・管理者アカウントを乱用しない	↑
		【V5】ネットワークアクセス管理の不備	・IP アドレス、ホスト名等にもとづくネットワークアクセス制御を実装する	・ネットワークサービスには適切なアクセス設定を行う	↑
		【V8】web アプリケーションの脆弱性	・管理者インタフェースに対して脆弱性テスト（ペネトレーションテスト）を実施する ・IPA のサイトで紹介されているツール等を利用して、よく知られた脆弱性の対応状況を確認し、未対応の脆弱性に対策を施す。	・新たに発見された攻撃手法に対応するため定期的に脆弱性テストを実施する	↑
		【V14】ファームウェア更新時の署名の不備または検証の不備	・ファームウェア・OS 等のアップデート配信サーバは TLS で通信路を保護し、クライアント側はサーバ証明書を検証 ・ファームウェア・OS・アプリケーションのアップデートファイルに電子署名を付与、クライアント側は電子署名を検証した上でインストール ・可能であれば機器側にもクライアント証明書を導入し、相互認証を実施 ・ファームウェアの改ざん検知・工場出荷状態への復帰機能を実装	・ファームウェアや OS のアップデート時は、配布サーバのサーバ証明書を検証する ・ダウンロードしたアップデートファイルの電子署名を検証する	↑
IP カメラ レコーダー 管理 PC 各種サーバ	・OS の脆弱性を悪用して利用者から管理者に昇格 - コマンド等の脆弱性を悪用して管理者・利用者権限を奪取【A10-1】 - 力任せの攻撃（ブルートフォースアタック）で管理者・利用者になりすます【A2-1】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A2-6】 - アクセス可能なデータ（ファームウェア）の不正な閲覧・改ざん・消去が行われる【A2-2】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A2-4】 - 管理者権限でサービスを不正に停止する【A2-5】 - 改ざんしたファームウェアを正式なファームウェアと信じ込ませる【V14-1】 - ファームウェアを改ざんすることで必要な権限を問わず任意の動作を行わせることができる【A14-2 他】	【V10】利用者権限で利用できるコマンド等の脆弱性管理の不備・ゼロデイ脆弱性	・導入する OS に対して脆弱性情報を精査する ・導入する OS に関してセキュリティパッチが提供された場合に機器側にパッチを提供する手段を検討する ・開発したプログラムに対して脆弱性テスト（ペネトレーションテスト）を実施する ・IPA のサイトで紹介されているツール等を利用して、よく知られた脆弱性の対応状況を確認し、未対応の脆弱性に対策を施す。 ・不正アクセスの痕跡をログに出力する ・ログの改ざんに備え、ログをリモートサーバに転送する機能を実装する ・特権コマンドの実行を検知できる仕組みを構築 ・機器と外部とのネットワーク境界に UTM F/W を設置し脆弱性攻撃を防ぐ	・ベンダ等から提供される機器の脆弱性情報を収集する ・セキュリティパッチが提供された際は速やかに適用できる体制を整える ・マルウェア感染時、侵入検知時に当該機器・重要機器をネットワークから切り離す	↑
		【V14】ファームウェア更新時の署名の不備または検証の不備	・ファームウェア・OS 等のアップデート配信サーバは TLS で通信路を保護し、クライアント側はサーバ証明書を検証 ・ファームウェア・OS・アプリケーションのアップデートファイルに電子署名を付与、クライアント側は電子署名を検証した上でインストール ・可能であれば機器側にもクライアント証明書を導入し、相互認証を実施 ・ファームウェアの改ざん検知・工場出荷状態への復帰機能を実装	・ファームウェアや OS のアップデート時は、配布サーバのサーバ証明書を検証する ・ダウンロードしたアップデートファイルの電子署名を検証する	↑
		【V2】脆弱なアカウント認証機構または不備	・ネットワーク経由での操作については強固な認証機構を導入する	・機器操作用の管理者・利用者認証に公開鍵を用いる場合 ・秘密鍵は平文で保管せず、パスフレーズでの暗号化、ハードウェアトークンの利用といった不正アクセス対策を施す	↑

別紙４　攻撃手法に対する対策一覧

IP カメラ レコーダー 管理 PC 各種サーバ	・利用者になりすまし、システムへ不正アクセス - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A1-6 他】 - コマンド等の脆弱性を悪用して管理者・利用者権限を奪取【A10-1】 - アクセス可能なデータの不正な閲覧・改ざん・消去が行われる【A1-2 他】【A4-2】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A1-4 他】 - サービスに接続してサービスプログラム名・バージョンなどを不正に入手（攻撃に悪用する）【A5-4】 - 開いているネットワークポートに大量の通信データを送り通信を妨害【A5-5】	【V1】脆弱な管理者・利用者パスワード	・パスワードの品質設定を実装する（パスワードに含まれる文字種・文字数等の制約） ・パスワードロックアウトを実装（一定回数のパスワード試行失敗時にログイン不可）	・機器操作用の管理者・利用者認証にパスワードを用いる場合 ・パスワード未設定（または空を設定）を許容しない ・IPA のガイドライン等を参考に推測困難なパスワードを設定する ・他サービス等で利用するパスワードを再利用しない（使いまわしの禁止）	↑
		【V4】ファイル等アクセス制御の不備	・管理者・利用者といったアカウント（ロール）にもとづくファイルアクセス制御を実装する	・ファイル・フォルダーごとに管理者・利用者のアクセス権限を設定する ・管理者アカウントを乱用しない	↑
		【V5】ネットワークアクセス管理の不備	・IP アドレス、ホスト名等にもとづくネットワークアクセス制御を実装する	・ネットワークサービスには適切なアクセス設定を行う	↑
		【V10】利用者権限で利用できるコマンド等の脆弱性管理の不備・ゼロデイ脆弱性	・導入する OS に対して脆弱性情報を精査する ・導入する OS に関してセキュリティパッチが提供された場合に機器側にパッチを提供する手段を検討する ・開発したプログラムに対して脆弱性テスト（ペネトレーションテスト）を実施する ・IPA のサイトで紹介されているツール等を利用して、よく知られた脆弱性の対応状況を確認し、未対応の脆弱性に対策を施す。 ・不正アクセスの痕跡をログに出力する ・ログの改ざんに備え、ログをリモートサーバに転送する機能を実装する ・特権コマンドの実行を検知できる仕組みを構築 ・機器と外部とのネットワーク境界に UTM F/W を設置し脆弱性攻撃を防ぐ	・ベンダ等から提供される機器の脆弱性情報を収集する ・セキュリティパッチが提供された際は速やかに適用できる体制を整える ・マルウェア感染時、侵入検知時に当該機器・重要機器をネットワークから切り離す	↑
IP カメラ レコーダー 管理 PC 各種サーバ	・外部記憶デバイス等を USB ポート等に挿入して、システム内にマルウェアを注入 - 攻撃者が不正に外部記憶デバイス等を USB ポート等に直接挿入して、システム内にマルウェアを注入【A6-2】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A6-4】 - 管理者権限でサービスを不正に停止する【A6-5】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A6-6】	【V6】外部記憶デバイスの物理ポートの管理不備	・外部記憶デバイス接続用ポート（USB など）が第三者にアクセスできないように金属製のゲージで囲み施錠可能とする ・外部記憶デバイス接続用ポートを露出せざるを得ない場合はソフトウェア的に有効・無効を設定可能とする ・あらかじめ登録した外部記憶デバイスのみ利用可能とする ・未登録の外部記憶デバイスが接続された際に警告を発信する ・外部記憶デバイス上のファイルについては電子署名を検証し、不正なプログラム、データを受け付けない	・外部記憶デバイス接続用ポートにデバイスが接続された際に、デバイス上のプログラムを自動的に実行しないよう設定する	↑
IP カメラ	・カメラの脆弱性を用いて、カメラへ不正アクセス - 力任せの攻撃（ブルートフォースアタック）で管理者・利用者になりすます【A2-1】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A2-6 他】 - 管理インタフェース等の脆弱性を悪用して管理者・利用者になりすます【A8-1】 - ネットワークサービスの脆弱性を悪用して管理者・利用者権限を奪取【A9-1】 - アクセス可能なデータ（ファームウェア）の不正な閲覧・改ざん・消去が行われる【A1-2 他】【A4-2】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A2-4 他】	【V2】脆弱なアカウント認証機構または不備	・ネットワーク経由での操作については強固な認証機構を導入する	・機器操作用の管理者・利用者認証に公開鍵を用いる場合 ・秘密鍵は平文で保管せず、パスフレーズでの暗号化、ハードウェアトークンの利用といった不正アクセス対策を施す	↑
		【V4】ファイル等アクセス制御の不備	・管理者・利用者といったアカウント（ロール）にもとづくファイルアクセス制御を実装する	・ファイル・フォルダーごとに管理者・利用者のアクセス権限を設定する ・管理者アカウントを乱用しない	↑

別紙４　攻撃手法に対する対策一覧

	- 管理者権限でサービスを不正に停止する【A2-5 他】 - サービスに接続してサービスプログラム名・バージョンなどを不正に入手（攻撃に悪用する）【A5-4】 - 開いているネットワークポートに大量の通信データを送り通信を妨害【A5-5】	【V5】ネットワークアクセス管理の不備	・IP アドレス、ホスト名等にもとづくネットワークアクセス制御を実装する	・ネットワークサービスには適切なアクセス設定を行う	↑
		【V8】web アプリケーションの脆弱性	・管理者インタフェースに対して脆弱性テスト（ペネトレーションテスト）を実施する ・IPA のサイトで紹介されているツール等を利用して、よく知られた脆弱性の対応状況を確認し、未対応の脆弱性に対策を施す	・新たに発見された攻撃手法に対応するため定期的に脆弱性テストを実施する	↑
		【V9】ネットワークサービスの脆弱性管理の不備・ゼロデイ脆弱性	・導入する OS に対して脆弱性情報を精査する ・導入する OS に関してセキュリティパッチが提供された場合に機器側にパッチを提供する手段を検討する ・開発したプログラムに対して脆弱性テスト（ペネトレーションテスト）を実施する ・IPA のサイトで紹介されているツール等を利用して、よく知られた脆弱性の対応状況を確認し、未対応の脆弱性に対策を施す ・不正アクセスの痕跡をログに出力する ・ログの改ざんに備え、ログをリモートサーバに転送する機能を実装する ・特権コマンドの実行を検知できる仕組みを構築 ・機器と外部とのネットワーク境界に UTM F/W を設置し脆弱性攻撃を防ぐ	・ベンダ等から提供される機器の脆弱性情報を収集する ・セキュリティパッチが提供された際は速やかに適用できる体制を整える ・管理者ではない利用者による特権コマンドの実行を検知できる仕組みを構築 ・マルウェア感染時、侵入検知時に当該機器・重要機器をネットワークから切り離す	↑
IP カメラ	・管理者・利用者になりすまして動画撮影・音声記録機能に不正アクセス - 管理者になりすまして構成要素（動画撮影・音声記録機能等）に不正アクセス【A1-1】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A1-6 他】 - アクセス可能なデータの不正な閲覧・改ざん・消去が行われる【A1-2 他】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A1-4 他】 - 管理者権限でサービスを不正に停止する【A1-5 他】	【V1】脆弱な管理者・利用者パスワード	・パスワードの品質設定を実装する（パスワードに含まれる文字種・文字数等の制約） ・パスワードロックアウトを実装（一定回数のパスワード試行失敗時にログイン不可）	・機器操作用の管理者・利用者認証にパスワードを用いる場合 ・パスワード未設定（または空を設定）を許容しない ・IPA のガイドライン等を参考に推測困難なパスワードを設定する ・他サービス等で利用するパスワードを再利用しない（使いまわしの禁止）	↑
IP カメラ	・カメラデバイスの破壊、撮影機能の物理的妨害	（物理的な脆弱性）	（物理的な保護）	（物理的な保護）	
IP カメラ	・カメラデバイスの持ち去り、オフラインでの解析（内部ストレージの解析、デバイスのリバースエンジニアリングなど）	（物理的な脆弱性）	（物理的な保護）	（物理的な保護）	
IP カメラ	・管理者・利用者になりすましてデータ保存機能に不正アクセス - 管理者になりすまして構成要素（データ管理機能等）に不正アクセス【A1-1】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A1-6 他】 - アクセス可能なデータの不正な閲覧・改ざん・消去が行われる【A1-2 他】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A1-4 他】 - 管理者権限でサービスを不正に停止する【A1-5 他】	【V1】脆弱な管理者・利用者パスワード	・パスワードの品質設定を実装する（パスワードに含まれる文字種・文字数等の制約） ・パスワードロックアウトを実装（一定回数のパスワード試行失敗時にログイン不可）	・機器操作用の管理者・利用者認証にパスワードを用いる場合 ・パスワード未設定（または空を設定）を許容しない ・IPA のガイドライン等を参考に推測困難なパスワードを設定する ・他サービス等で利用するパスワードを再利用しない（使いまわしの禁止）	↑

別紙４　攻撃手法に対する対策一覧

IP カメラ レコーダー 管理 PC	・正当な通信機器になりすまして IP カメラに不正アクセス（IP アドレス偽装, ARP スプーフィング） - 他機器になりすまして中間者攻撃を行う【A3-1 他】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A3-6 他】 - アクセス可能なデータの不正な閲覧・改ざん・消去が行われる【A3-2 他】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A3-4 他】 - 管理者権限でサービスを不正に停止する【A3-5 他】	【V3】脆弱な機器間の認証機構または不備	・アプリケーションレイヤーでの相互認証を導入する。 ・第三者によるなりすましが発生しないよう物理的・論理的に独立したネットワークとする ・ネットワーク内に不正な機器が接続されたことを検知するシステムを導入する		↑
IP カメラ レコーダー 管理 PC	・中間者攻撃により、他機器からの通信データを盗聴・改ざん - 他機器になりすまして中間者攻撃を行う【A3-1 他】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A1-6 他】 - 通信を盗聴・再利用することで管理者・利用者になりすます【A12-1】 - アクセス可能なデータの不正な閲覧・改ざん・消去が行われる【A1-2 他】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A1-4 他】 - 管理者権限でサービスを不正に停止する【A1-5 他】 - 平文のデータあるいは強度の弱い暗号化を解除して通信を改ざんする【A12-2】 - 暗号強度が低い通信を解読する【A12-4】	【V7】脆弱な送信元検証機構や検証機構の不備	・HTTP 通信については TLS を導入し機器間で相互認証を行う ・複数のプロトコルに対処する必要がある場合には IPsec を導入し機器間で相互認証を行う ・第三者による不正中継が発生しないよう物理的・論理的に独立したネットワークとする ・ネットワーク内に不正な機器が接続されたことを検知するシステムを導入する		↑
		【V12】通信データ保護（暗号化等）の不備	・安全な認証・暗号プロトコルを導入する ・HTTP 通信については TLS を導入し通信データを保護する ・複数のプロトコルに対処する必要がある場合には IPsec を導入し通信データを保護する		↑
IP カメラ レコーダー 管理 PC	・通信路上に存在する攻撃者が通信データを盗聴して通信データを流出・改ざん - 通信を盗聴・再利用することで管理者・利用者になりすます【A12-1】 - 平文のデータあるいは強度の弱い暗号化を解除して通信を改ざんする【A12-2】 - 暗号強度が低い通信を解読する【A12-4】	【V12】通信データ保護（暗号化等）の不備	・安全な認証・暗号プロトコルを導入する ・HTTP 通信については TLS を導入し通信データを保護する ・複数のプロトコルに対処する必要がある場合には IPsec を導入し通信データを保護する		↑
IP カメラ レコーダー 管理 PC	・開いているネットワークポートに大量の通信データを送り通信を妨害 - アクセス可能なデータ（ファームウェア）の不正な閲覧・改ざん・消去が行われる【A4-2】	【V4】ファイル等アクセス制御の不備	・管理者・利用者といったアカウント（ロール）にもとづくファイルアクセス制御を実装する	・ファイル・フォルダーごとに管理者・利用者のアクセス権限を設定する ・管理者アカウントを乱用しない	↑

	- 構成要素に保存された情報を不正に入手する【A4-4】 - 設定ファイルを書き換えてサービスを不正に停止する【A4-5】 - サービスに接続してサービスプログラム名・バージョンなどを不正に入手（攻撃に悪用する）【A5-4】 - 開いているネットワークポートに大量の通信データを送り通信を妨害【A5-5】	【V5】ネットワークアクセス管理の不備	・IP アドレス、ホスト名等にもとづくネットワークアクセス制御を実装する	・ネットワークサービスには適切なアクセス設定を行う	↑
IP カメラ レコーダー 管理 PC	・ネットワークサービスの脆弱性を悪用して管理者・利用者権限を奪取（不正ログイン、不正コードの実行、バックドアの設置など） - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A8-6 他】 - 管理インタフェース等の脆弱性を悪用して管理者・利用者になりすます【A8-1】 - ネットワークサービスの脆弱性を悪用して管理者・利用者権限を奪取【A9-1】 - アクセス可能なデータ（ファームウェア）の不正な閲覧・改ざん・消去が行われる【A8-2 他】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A8-4 他】 - 管理者権限でサービスを不正に停止する【A8-5 他】	【V8】web アプリケーションの脆弱性	・管理者インタフェースに対して脆弱性テスト（ペネトレーションテスト）を実施する ・IPA のサイトで紹介されているツール等を利用して、よく知られた脆弱性の対応状況を確認し、未対応の脆弱性に対策を施す	・新たに発見された攻撃手法に対応するため定期的に脆弱性テストを実施する	↑
		【V9】ネットワークサービスの脆弱性管理の不備・ゼロデイ脆弱性	・導入する OS に対して脆弱性情報を精査する ・導入する OS に関してセキュリティパッチが提供された場合に機器側にパッチを提供する手段を検討する ・開発したプログラムに対して脆弱性テスト（ペネトレーションテスト）を実施する ・IPA のサイトで紹介されているツール等を利用して、よく知られた脆弱性の対応状況を確認し、未対応の脆弱性に対策を施す ・不正アクセスの痕跡をログに出力する ・ログの改ざんに備え、ログをリモートサーバに転送する機能を実装する ・特権コマンドの実行を検知できる仕組みを構築 ・機器と外部とのネットワーク境界に UTM F/W を設置し脆弱性攻撃を防ぐ	・ベンダ等から提供される機器の脆弱性情報を収集する ・セキュリティパッチが提供された際は速やかに適用できる体制を整える ・管理者ではない利用者による特権コマンドの実行を検知できる仕組みを構築 ・マルウェア感染時、侵入検知時に当該機器・重要機器をネットワークから切り離す	↑
IP カメラ 管理 PC	・再送攻撃により、カメラ制御のコマンドの送信を不正に繰り返す - 他機器になりすまして中間者攻撃を行う【A3-1 他】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A1-6 他】 - 力任せの攻撃（ブルートフォースアタック）で管理者・利用者になりすます【A2-1】 - 通信を盗聴・再利用することで管理者・利用者になりすます【A11-1】 - アクセス可能なデータの不正な閲覧・改ざん・消去が行われる【A1-2 他】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A1-4 他】	【V7】脆弱な送信元検証機構や検証機構の不備	・HTTP 通信については TLS を導入し機器間で相互認証を行う ・複数のプロトコルに対処する必要がある場合には IPsec を導入し機器間で相互認証を行う ・第三者による不正中継が発生しないよう物理的・論理的に独立したネットワークとする ・ネットワーク内に不正な機器が接続されたことを検知するシステムを導入する		↑
		【V11】通信セッションの管理不備	・HTTP 通信については TLS を導入し不正な通信の割り込みを防止する ・正常と認められる制御シーケンスの遷移パターンを規定し、そこから逸脱する制御シーケンスについての対応を実装する（例えば、短時間のうちにカメラの向きを過剰に変更することで動作不良を発生させるような攻撃を想定し、単位時間あたりの制御受付回数に閾値を設けるなど）		↑

	- 管理者権限でサービスを不正に停止する【A1-5 他】	【V2】脆弱なアカウント認証機構または不備	・ネットワーク経由での操作については強固な認証機構を導入する	・機器操作用の管理者・利用者認証に公開鍵を用いる場合 ・秘密鍵は平文で保管せず、パスフレーズでの暗号化、ハードウェアトークンの利用といった不正アクセス対策を施す	↑
レコーダー	・管理者になりすまして画像（音声）データを不正に閲覧、改ざん、消去 - 管理者になりすまして構成要素（画像・音声データ操作機能）に不正アクセス【A1-1】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A1-6 他】 - 力任せの攻撃（ブルートフォースアタック）で管理者・利用者になりすます【A2-1】 - アクセス可能なデータの不正な閲覧・改ざん・消去が行われる【A1-2 他】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A1-4 他】 - 管理者権限でサービスを不正に停止する【A1-5 他】	【V1】脆弱な管理者・利用者パスワード	・ネットワーク経由での操作については強固な認証機構を導入する	・機器操作用の管理者・利用者認証に公開鍵を用いる場合 ・秘密鍵は平文で保管せず、パスフレーズでの暗号化、ハードウェアトークンの利用といった不正アクセス対策を施す	↑
		【V2】脆弱なアカウント認証機構または不備	・ネットワーク経由での操作については強固な認証機構を導入する	・機器操作用の管理者・利用者認証に公開鍵を用いる場合 ・秘密鍵は平文で保管せず、パスフレーズでの暗号化、ハードウェアトークンの利用といった不正アクセス対策を施す	↑
管理 PC	・カメラ機器管理（アプリケーション）の利用者・管理者になりすましてカメラに不正アクセス - 管理者になりすまして構成要素（カメラ管理機能）に不正アクセス【A1-1】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A1-6 他】 - 力任せの攻撃（ブルートフォースアタック）で管理者・利用者になりすます【A2-1】 - アクセス可能なデータの不正な閲覧・改ざん・消去が行われる【A1-2 他】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A1-4 他】 - 管理者権限でサービスを不正に停止する【A1-5 他】	【V1】脆弱な管理者・利用者パスワード	・ネットワーク経由での操作については強固な認証機構を導入する	・機器操作用の管理者・利用者認証に公開鍵を用いる場合 ・秘密鍵は平文で保管せず、パスフレーズでの暗号化、ハードウェアトークンの利用といった不正アクセス対策を施す	↑
		【V2】脆弱なアカウント認証機構または不備	・ネットワーク経由での操作については強固な認証機構を導入する	・機器操作用の管理者・利用者認証に公開鍵を用いる場合 ・秘密鍵は平文で保管せず、パスフレーズでの暗号化、ハードウェアトークンの利用といった不正アクセス対策を施す	↑
管理 PC	・物理的に管理 PC にアクセスし、画像（音声）データを不正に閲覧・消去する ・物理的に管理 PC にアクセスし、制御データを改ざんする	（物理的な脆弱性）	（物理的な保護）	（物理的な保護）	↑
管理 PC	・標的型攻撃などのマルウェア感染 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A10-6 他】	【V4】ファイル等アクセス制御の不備	・管理者・利用者といったアカウント（ロール）にもとづくファイルアクセス制御を実装する	・ファイル・フォルダーごとに管理者・利用者のアクセス権限を設定する ・管理者アカウントを乱用しない	↑

別紙４　攻撃手法に対する対策一覧

	- コマンド等の脆弱性を悪用して管理者・利用者権限を奪取【A10-1】 ・管理者になりすまして、不正な動作を行わせる【A13-1～A13-6】 - アクセス可能なデータの不正な閲覧・改ざん・消去が行われる【A10-2】【A4-2】 - 構成要素に保存された情報を不正に入手する【A4-4】 - 設定ファイルを書き換えてサービスを不正に停止する【A4-5】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A10-4】 - 管理者権限でサービスを不正に停止する【A10-5】	【V10】利用者権限で利用できるコマンド等の脆弱性管理の不備・ゼロデイ脆弱性	・導入する OS に対して脆弱性情報を精査する ・導入する OS に関してセキュリティパッチが提供された場合に機器側にパッチを提供する手段を検討する ・開発したプログラムに対して脆弱性テスト（ペネトレーションテスト）を実施する ・IPA のサイトで紹介されているツール等を利用して、よく知られた脆弱性の対応状況を確認し、未対応の脆弱性に対策を施す ・不正アクセスの痕跡をログに出力する ・ログの改ざんに備え、ログをリモートサーバに転送する機能を実装する ・特権コマンドの実行を検知できる仕組みを構築 ・機器と外部とのネットワーク境界に UTM F/W を設置し脆弱性攻撃を防ぐ	・ベンダ等から提供される機器の脆弱性情報を収集する ・セキュリティパッチが提供された際は速やかに適用できる体制を整える ・マルウェア感染時、侵入検知時に当該機器・重要機器をネットワークから切り離す	↑
		【V13】ユーザーのリテラシー不足		・管理者・利用者に対して標的型攻撃対策を含めた情報セキュリティ教育を定期的に実施する	
無線 AP	・無線信号を妨害する電波を流す	（電波）		・無線 LAN の電波状況を定期的に調査し、電場妨害を行っている機器を排除する	
無線 AP	・通信を中継して、通信先へ再送攻撃を行うことで、不正な制御を行う - 他機器になりすまして中間者攻撃を行う【A7-1】 - 利用者で不正アクセスを行い脆弱性を悪用して管理者権限を入手【A7-6】 - アクセス可能なデータの不正な閲覧・改ざん・消去が行われる【A7-2】 - 管理者権限・使用者権限で構成要素に保存された情報を不正に入手する【A7-4】 - 管理者権限でサービスを不正に停止する【A7-5 他】	【V7】脆弱な送信元検証機構や検証機構の不備	・HTTP 通信については TLS を導入し機器間で相互認証を行う ・複数のプロトコルに対処する必要がある場合には IPsec を導入し機器間で相互認証を行う ・第三者による不正中継が発生しないよう物理的・論理的に独立したネットワークとする ・ネットワーク内に不正な機器が接続されたことを検知するシステムを導入する		
全て	・管理者になりすまして、不正な動作を行わせる【A13-1～A13-6】	【V13】ユーザーのリテラシー不足		・管理者・利用者に対して標的型攻撃対策を含めた情報セキュリティ教育を定期的に実施する	
全て	ー	（外部ネットワークとの接続による脅威）	・他のネットワークの分離を行い、不要なアクセス経路を防ぐ ・ルータやファイアウォールの設置により、外部へのアクセスを制限する ・ファイアウォールの設置や VPN の利用により、外部からのアクセスを制限する		