IPA　入退管理システムセキュリティ要件検討 WG　参考資料

IoT システムにおける情報セキュリティ対策要件策定に関する調査

調査実施報告書

2019 年 1 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、2018年6月1日公示「IoTシステムにおける情報セキュリティ対策要件策定に関する調査」に係る一般競争入札の納品物の一部である「入退管理システム」に関する調査結果の抜粋です。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。

本報告書には入退管理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「入退管理システムセキュリティ要件検討WG」へ入力され、当該ワーキンググループが5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。

■入退管理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/ecs/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

独立行政法人情報処理推進機構（以下「IPA」という。）は 2017 年度、「政府機関の情報セキュリティ対策のための統一基準 」（以下「政府統一基準」という。）における特定用途機器の政府調達や、自治体及び民間組織における IoT を含んだ情報システム（以下「IoT システム」という。）の調達時に参照することで具体的な情報セキュリティ対策を可能とする「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 」を公開した。

一方で、ネットワークカメラシステム以外の IoT システムに関しては、調達担当者が参照できる具体的な情報セキュリティ対策の資料として有効なものは多くない。IoT システムに対するインシデントが問題視されている現在において、安全な国民サービスを提供可能にするために、IoT システム毎の具体的な要件を早急に整備する必要がある。

そこで今回の調査では、ネットワークカメラシステム以外の IoT システムを調査対象として、考慮すべき情報セキュリティの要件を明確にし、政府機関・自治体等の調達担当者が IoT システムの調達・運用に際し利用できる情報として提供する。調査対象は政府機関・自治体等において利用実績があり、今後調達時の情報セキュリティ対策の必要性が見込まれる IoT システムとする。

1.2 調査の実施概要

本調査では、政府機関・自治体等の調達担当者が IoT システムの調達・運用に際し利用できる情報をするため、以下の手順で調査を行った。

1) IoT システムのユースケースの調査
2) ユースケース毎の脅威の洗い出し
3) 脅威に対抗する情報セキュリティ要件の調査

なお、調査にあたっては、IPA が別途設置する委員会及び有識者に対して上記の調査結果の報告を行い、承認を得ている。

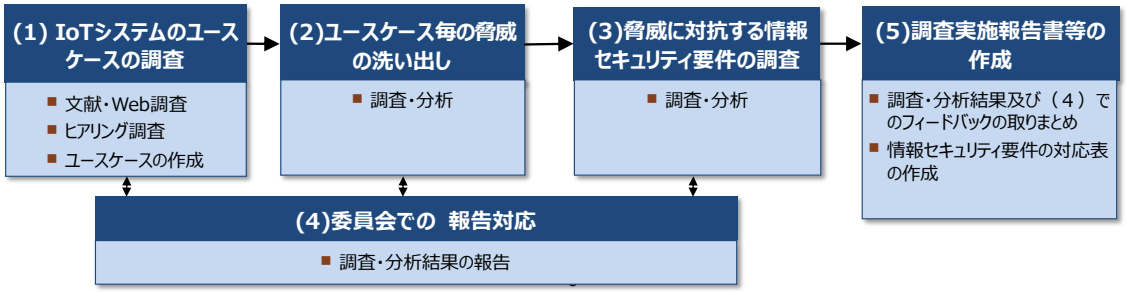

図 1-1　本調査のフロー

2. 入退管理システム

2.1 ユースケースの調査

2.1.1 調査概要

政府機関や自治体等で利用される入退管理システムの利用形態は一つではなく、情報セキュリティ上の脅威や対策は、入退管理システムが設置される場所や IoT システムを構成する要素によって異なることが想定される。そのため、情報セキュリティ上の脅威の洗い出しに先立って、入退管理システムの利用事例を調査し、ユースケースを作成した。

利用事例の調査では、入退管理システムに関する公開資料の調査及びベンダや SIer へのヒアリングを実施した。

ユースケースでは利用目的を明確にし、入退管理システムとそれらの接続状態、データの流れや利用者、設置される物理的な環境とその境界線を図表化した。

2.1.2 入退管理システムに関する公開資料の調査及びベンダ・SIer へのヒアリング

(1) 公開資料の調査

入退管理システム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　入退管理システムの利用事例調査の対象一覧

文献番号	発行組織	資料名
a	新潟市病院事業管理者	新潟市民病院公告第 50 号　入札公告
b	中国四国農政局	平成 30 年度岡山第２合同庁舎　入退館ゲート管理システム保守業務仕様書（案）
c	中国四国農政局	平成 27 年度岡山第２合同庁舎　入退館管理サーバー等更新
d	第八管区海上保安本部	舞鶴港湾合同庁舎入退館管理システム等保守業務仕様書
e	鹿児島市教育委員会学習情報センター	学習情報センターサーバー室入退室管理システム設置業務委託　仕様書
f	北本市	電算区画入退室管理システム更新事業に係る導入及び運用保守業務委託仕様書
g	三菱電機	三菱統合セキュリティーシステム MELSAFETY カタログ（大規模向け）

h	三菱電機	三菱統合セキュリティーシステム MELSAFETY カタログ（1 扉のスタンドアロン運用）
i	日立ビルシステム	統合型ファシリティマネジメントソリューション BIVALE　ウェブサイト
j	日立情報通信エンジニアリング	入退管理システム CyberGatevision 5　ウェブサイト

(2) ベンダ・SIer へのヒアリング

入退管理システムの利用事例調査では､3 社のベンダ･SIer にヒアリング協力いただいた。ヒアリング概要については以下の通り。

＜システム構成＞

- 入退管理システムの構成､機器･ケーブルの種別等はメーカーによって大幅に異なり、業界で統一されたものがない。
- 通常､入退管理は制御装置で行う。各制御装置に通知を送る連動制御用の制御装置が設置される場合もある。
- 管理端末から各種情報の登録を行うが､設置しない場合は制御装置にそのまま登録も可能である。
- 管理サーバは Windows が多い。導入先に既にある仮想環境に乗せることもある。
- 制御線は国内で独自のプロトコルが多いが、専用 LAN の場合もある。
- 認証装置はカードリーダーが一般的だが、QR コードリーダー等もある。カードと静脈等、複合認証もある。
- サーバまで戻って認証するケースはほとんどない。データは一元管理して､制御装置で認証するケースが多い｡顔認証はデータ量が多く､認証速度の面でサーバを立てる。生体情報専用のサーバは外に立てて別管理を行いたい面もある。
- 空調、照明との連動制御もある。サーバから上位は BACNet での接続が一般的。
- ファームウェアは機器にそのままアップデートする場合､センター側で書き換え機能を持つ場合のいずれもある。

＜脅威と対策＞

- ローカルネットワークでは、スタンドアローンか VLAN で分離する。ゲートウェイで切り分ける場合もある。最近は共用 LAN を使う場合もある。拠点間を繋ぐケースはインターネット VPN を使うことが多い。
- 認証装置の物理的な破壊に備え、認証装置と制御装置を別にするメーカーが増えている。
- 管理区域外にはデータを置かず､最近は制御装置を EPS に置くケースも増えている。
- ランサムウェアもあり、ここ数年は制御装置側もパッチを当てる必要性が言われている。昔は専用 OS だったが、最近は Linux、メーカーによっては Windows を使う。
- 端末群への USB 差し込みからマルウェアを流し込まれるリスクはある。
- デフォルトの ID・PW が利用されている場合もある。

・　端末の盗難や回線の切断等では、通信異常が検知される。
・　EPS で一括管理するものと複数分散するものがあるが、停電等が発生しても単独で動けるような形式を基本としている。
・　上位の管理サーバに様々な機能を持つケースもあるが、データに触れる部分と機能を分け、全体をコントロールされる箇所を作らないことでリスクを低減する。
・　異常が発生しても、ドアが開放される、停電しても鍵を物理的に回して開けられる等の安全設計は行っている。

(3) 入退管理システムの整理

脅威分析のために、入退管理システムの構成要素として、前節の入退管理システムの利用事例調査結果を基に、「機能」「機器」「利用に関わる要員」「機器の接続」を整理した。

対象とする入退管理システムは、利用事例の調査を元に、以下の通り定義する。

- 入退管理システム（Access Control System, ACS）とは、システム・環境・施設への物理的なアクセス制御・監視を行うシステム
- ID カード番号（身分証）・生体情報（指紋、声紋、虹彩、顔等）・暗証番号等を認証情報として受け取り、主体を識別、アクセス制御リスト（Access Control List, ACL）に基づき、要求されるアクセスの承認・拒否といった判断を行う

はじめに、“ISO/IEC 10181-3:1996” に示されるアクセス制御フレームワークと入退管理システムの関係を参考に、入退管理システムを構成する機能を列挙した。（表 2-2）
アクセス制御に加え入退履歴、在室状態等の管理も重要な機能である。

表 2-2　入退管理システムを構成する機能

要素	入退管理システムでの実体
アクセス要求主体	セキュリティゲートを通過しようとする従業員・来訪者
アクセス制御執行機能	アクセス要求主体の認証情報を入力として受け取る認証装置及び制御装置
アクセス制御決定機能	ユーザデータベース、アクセス制御リストなどを用いてアクセス要求の承認・拒否を行う制御装置
アクセス対象	入退管理システムではセキュリティゲート

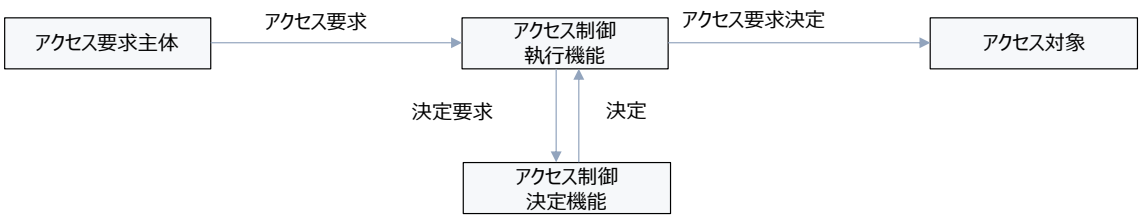

図 2-1　入退管理システムを構成する機能の関係

次に、入退管理システムを構成する機器を整理した。（表 2-3）

表 2-3　入退管理システムを構成する機能

要素	概要
制御装置（コントローラ）	「アクセス制御執行機能」及び「アクセス制御決定機能」としてシステムの中核となる装置。認証装置から認証情報を受け取り、照合認証の結果、セキュリティゲート類を操作する装置。
管理サーバ（サーバ・ソフトウェア）	制御装置の諸設定、カード登録、履歴取得・保管、認証情報保管、利用者管理等を行う。
管理端末（PC・ソフトウェア）	管理サーバの操作用クライアント（小規模システムでは管理サーバとクライアントを 1 台とする）。 認証情報の初期化・登録等も行う。
認証装置（リーダー）	ID カード、生体情報、暗証番号等を読取る装置等（制御装置が組み込まれたスタンドアローンタイプあり）。
認証デバイス	アクセス要求主体（利用者）の認証情報が格納され、認証装置でその情報を読取られるデバイス。ID カード（Felica, MIFARE 等、交通系カード、買物系カードも利用可能）、スマートフォン（専用アプリ）、RFID タグ等。
生体認証サーバ	生体認証の場合、認証装置ではなくサーバ側で照合認証を行う場合に設置される。
セキュリティゲート	制御装置から制御可能な電気錠を備えた扉、フラッパーゲート等。
各種センサー	動体の接近、火災の発生等を検知するセンサー（赤外線、パッシブセンサー）等。
キーボックス	「鍵」を収容する装置。入退管理システムと連携して認証デバイスによる利用が可能。
連携システム	入退管理システムと連携する外部システム。勤怠管理、エレベーター、防犯設備等。

上記のうち、制御装置、管理サーバ・管理端末、認証装置、セキュリティゲートの詳細は以下の通り。

表 2-4　制御装置の詳細

概要	認証装置、セキュリティゲート（電気錠）を接続し、認証装置からの読取り情報と装置内部で記憶している利用者情報（認証情報）を照合し認証の結果、アクセスが承認された場合にゲートを解錠する装置。 パッシブセンサーや、マグネットスイッチなど警備センサーを接続することで機械警備が可能。
外部インターフェース	LAN ポート、認証端末ポート（UTP）、電気錠制御ポート、USB ポート

主な機能	● セキュリティゲート制御 各ゲートに対して入室用・退室用認証装置を設定。 1 回解錠（通常動作、照合 OK 後に一定時間解錠・施錠）、連続解錠（施錠するまで解錠状態を維持）モードを備える ● 照合レスポンス 認証装置と連動して照合を実施、照合に成功した場合に電気錠解錠及び認証装置の解錠ブザーが鳴る。 認証情報はカード番号・暗証番号・生体情報等。 通信プロトコルは、汎用プロトコル（LonTalk 等）、独自プロトコル等、様々な種類がある。 ● イベント管理 正常操作・エラー・設定操作イベント等の履歴記録、履歴データのエクスポート。 ● 利用者登録管理 従業員・来訪者等の利用者情報（ID・氏名・開始日・有効期間・カード番号・カード世代・暗証番号等）を登録。 登録作業は、本体直接操作、ウェブブラウザまたはユーティリティソフト経由で実施（ネットワークあるいは外部記憶媒体経由）。
他機能	照合ペナルティ機能（暗証番号を連続失敗した場合の無効期間設定）、在室管理機能（アンチパスバック）、カレンダー保持機能、ルートチェック（入室経路制限）、インターロック（二重扉）、機械警備機能、ツーパーソン照合機能（2 名が連続照合することで解錠・施錠）、エレベーター連動制御機能（登録階のみ停止）、ファームウェア更新機能、スケジュール設定機能、設定・履歴書出機能、設定読込機能、等。

表 2-5　管理サーバ・管理端末

概要	制御装置の諸設定、カード登録、履歴取得・保管、認証情報保管、ユーザ管理等を行う。 認証装置に入力された ID カード、RFID タグの照合・認証は認証装置または制御装置、生体情報の場合は認証装置、制御装置、認証サーバのいずれかで実行され、管理サーバは関与しない。
外部インターフェース	LAN ポート、USB ポート（カードリーダー、外部記憶媒体）
主な機能	● 制御装置監視 制御装置の動作状況をモニタ、異常発生時には管理端末に表示、設定されたメールアドレスにアラートメール発信等を行う。 ● 利用者登録管理 入退を行う従業員・来訪者の情報をデータベースに登録・削除・変更とい

	った編集機能を持つ。 利用者は所属部署、役職、アクセスレベル等でのグルーピングが可能。 ● 認証情報登録 ID カードを用いる場合はカードリーダー経由でカード番号を読取り利用者と紐づける。RFID についても同様。 生体情報の場合は認証装置または認証サーバにデータを登録する。 ● 入退履歴管理 制御装置で記録される入退履歴情報を取得し管理サーバ上に保管する。 外部記憶媒体等への書き出しが可能。 ● 認証装置アップデート アップデート機能を持つ制御装置・認証装置については、管理端末からアップデートファイルを管理サーバ経由または直接、装置に送ることができる。
他機能	―

表 2-6　認証装置

概要	セキュリティゲートを通過しようとするアクセス主体（人）の認証情報（ID、ID カード内の認証データ、暗証番号、RFID タグ、生体情報等）を読取り、制御装置に送信。照合結果を装置上に表示する。 認証装置内に制御装置の機能を持ち単独で動作する装置もある。
外部インターフェース	制御装置接続ポート
主な機能	● 認証情報読取り機能 ID カード内の認証情報、生体情報、暗証番号（テンキー入力）等を読みだす。 ID カードのみ、暗証番号のみ、ID カード＋暗証番号といった照合方式の設定が可能。 ● 状況表示機能 認証装置（正常・異常）・セキュリティゲート（施錠・解錠）の状態、照合結果等を装置上に表示、スピーカを鳴動する等。 ● 各種設定機能 読取りカードタイプ、照合方法（登録カードを許可または不許可）等の設定を行う。 ● 認証情報登録機能（スタンドアローンタイプ） ID カード・生体情報等の登録。
他機能	―

表 2-7　セキュリティゲート

概要	居室内の場合は扉にとりつける電気錠、ビルの入退館の場合はフラッパーゲートが相当する。
外部インターフェース	● 電気錠入出力 解錠・施錠用ソレノイド入力 扉開閉信号出力 施錠・解錠信号出力 異常信号出力（ピッキング・破壊時の異常開錠） ● フラッパーゲート入出力 機能としては認証装置と電気錠・扉がセットになっている。 制御装置接続ポート
主な機能	● 電気錠 施錠・解錠機能：電圧により施錠・解錠状態を切り替える。 扉・錠の状態を信号出力する。 異常検知機能：ピッキング・破壊時の異常開錠を検知し信号を出力する。 ● フラッパーゲート 認証情報読取り機能：ID カード内の認証情報、生体情報等を読みだす。 状況表示機能：装置（正常・異常）の状態、照合結果等を装置上に表示、スピーカを鳴動する等。 扉開閉機能：照合結果に基づきゲートを開閉する。緊急時の動作として全開放・全閉鎖のいずれかを設定する。 人体検知機能：挟みこみ防止及び共連れ入場防止のため、ゲート内を通過中の人体を検知する機能。
他機能	飛び越え検知機能、挟みこみ防止機能、等。

次に、入退管理システムに関わる要員を列挙した。（表 2-8）

表 2-8　入退管理システムに関わる要員

要素	概要
管理者	管理端末から管理サーバを操作する者のこと。複数拠点にわたるシステムの場合、全体を管理する全体管理者、支社・支店等の部分的な管理を行うサブ管理者と、階層的な構成をとる。
保守員	入退管理システム（制御装置、認証装置、管理サーバ等）の保守要員
利用者	管理対象の施設を保有する組織の職員または来訪者。事前に登録され、ID カード等で入退室・入退館を行う（来訪者には一時利用可能なゲストカードを発行）。
外部委託事業者	入退管理システム設定構築運用等を委託された外部事業者及び警備

	員等
サービス提供事業者	クラウドサービスモデルの場合、サービスを提供運用する事業者。
第三者	どれにも当てはまらない部外者。脅威分析の際には、システムを攻撃する者、不正入室・入館を試みる者。

次に、管理サーバ、制御装置、認証装置に登録する利用者（ユーザ）情報を整理する。（表 2-9）

表 2-9　機能管理サーバ、制御装置、認証装置に登録する利用者（ユーザ）情報

データ項目	概要
利用者番号	ユーザを一意に識別するユニークな番号。
名前	利用者の氏名。
所属組織名称	利用者の所属組織、所属組織単位でアクセスレベルを設定し、利用者の検索を行う際に利用できる。
発行回数	利用者番号に対するカード発行回数。紛失したカードの不正利用を識別するために使われる。
操作レベル	利用者に許可される入退管理システムの操作レベル（警備モード設定可能等）。
アクセスレベル	セキュリティゲートで区切られた領域（ゾーン）にアクセスレベルを付与、利用者が入退可能なレベルを設定。
暗証番号	設定することによりテンキー入力による認証が可能となる。
有効・無効フラグ	ID カード等を紛失した場合に無効とするフラグ（無効なカードが使用された際に不正使用の履歴が残る）。
有効期限	認証可能となる期間を指定する（開始日時～終了日時）。
カード種別	Felica, MIFARE 等、ID カードの種類
カード番号	ID カード特有の番号（Felica IDm、MIFARE UID 等）。
生体情報	生体情報から特徴を抽出しデータ化した「登録特徴データ」。

表 2-3 で整理した機器の関係を以下に示す。（図 2-2）

入退管理システムの中心は制御装置であり、管理サーバは制御装置の設定、データ（ユーザ情報、入退履歴等）の管理が役割となっている。

生体認証を用いる場合、生体情報を認証装置側に持ち装置上で照合を行うケース（制御装置が認証装置に組み込まれている）（図 2-3）と、認証装置では読取りだけを行い照合はサーバ側で行うケースがある（図 2-4）。前者では、認証装置で読取った生体情報を制御装置で受け取り、制御装置上で認証を実施する。認証結果に応じて解錠操作を実施し、認証サーバで登録された生体情報を制御装置に送信、制御装置からは照合履歴を認証サーバに送信する。後者では、認証装置で読取った生体情報を認証サーバに送り、認証サーバ上で認証が行われる形態となっている。

キーボックスと制御装置の接続は CPEV 線（図 2-5）または LAN 接続（図 2-6）が利用されている。

入退管理システムとしての保守の対象は、制御装置、認証装置、管理サーバ、認証サーバ、キーボックス等になる。

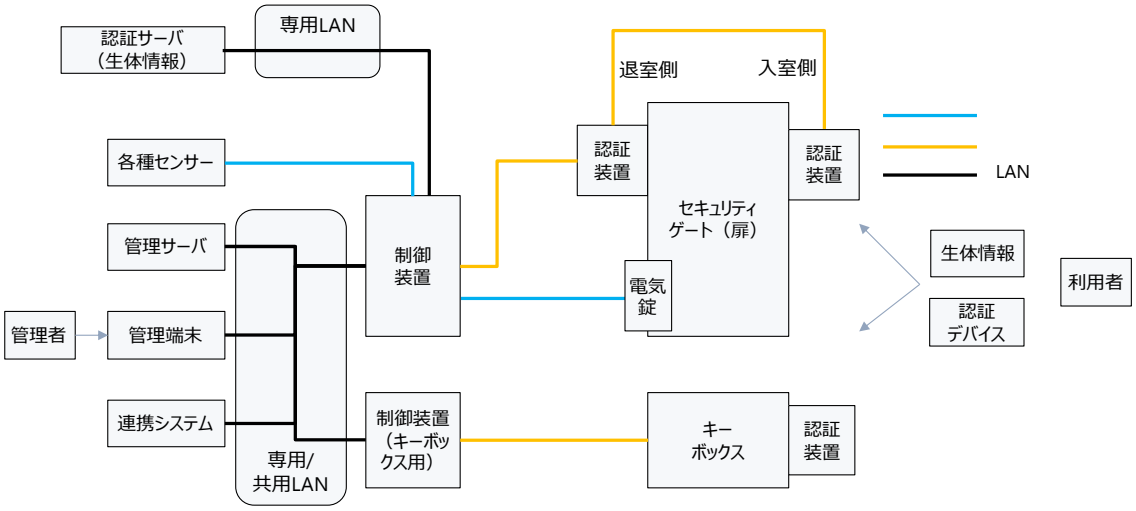

図 2-2　機器の接続関係

図 2-3　生体情報を認証装置側で照合する場合の流れ

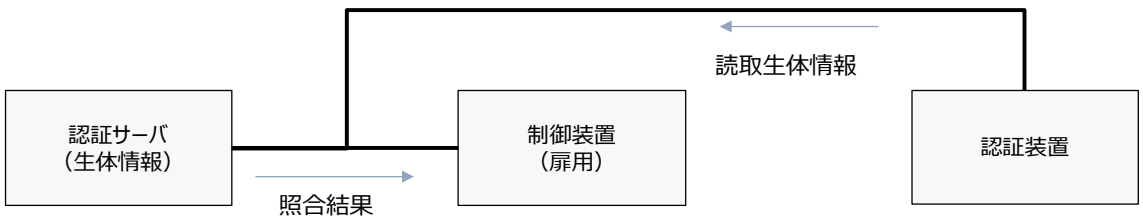

図 2-4　生体情報を認証サーバで照合する場合の流れ

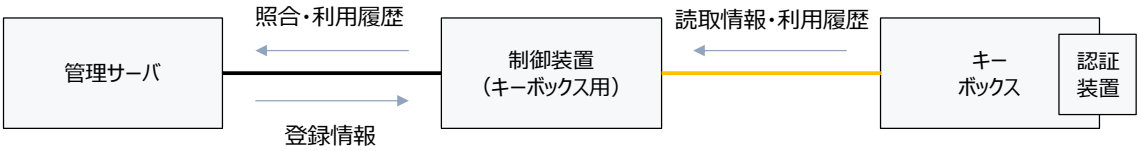

図 2-5　キーボックスと制御装置の接続（CPEV 線）

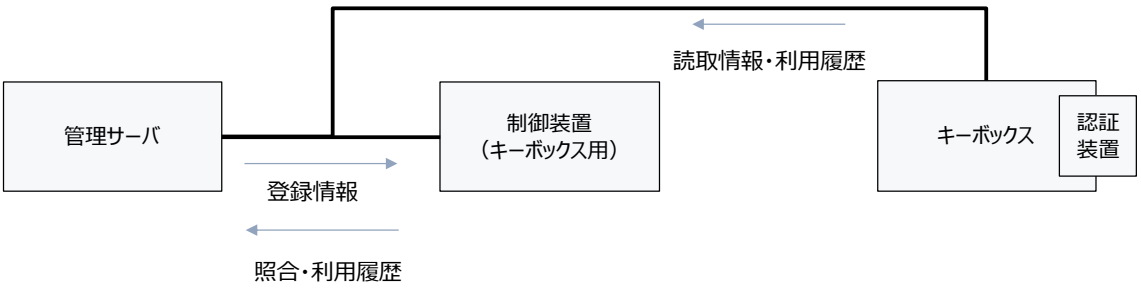

図 2-6　キーボックスと制御装置の接続（LAN 接続）

2.1.3 ユースケースの作成

入退管理システムは認証装置に制御装置が組み込まれたスタンドアローンタイプのものから、複数拠点・数百のゲートを制御し、様々な周辺システムと連携する大規模なものまで存在する。2.1.2 で整理した入退管理システムの構成要素を踏まえ、以下の 3 種類のユースケースに整理した。

- スタンドアローンモデル（SA）
  数部屋分の出入り口ドアの電気錠を管理する形態を想定。小規模のため管理サーバを設置せず、制御装置と認証装置のみで構成される。入退管理システムの主要な要素が含まれており基本となる。
- 統合管理モデル（TM）
  複数ビルにオフィスを展開する企業等を想定。WAN（専用回線）を介した外部拠点との分散管理を行う。また、入退館から各部屋の入退室までを統合制御を行い、他システムとの連携が含まれる。脅威分析においてはネットワーク境界への攻撃、他システムからの影響、他システムへの影響等が含まれる。社内システム（人事管理・勤怠管理）やエレベーター・防犯システム・火災警報等との連携がある。
- クラウドサービスモデル（CS）
  管理サーバ機能・制御装置機能が SaaS サービスとして提供される形態を想定。スタンドアローンモデルと同じく一体化した制御装置を設置。認証装置からのインターネット接続が必要となる。管理サーバのメンテナンスが不要となる。インターネット上に管理サーバが存在するため拠点外においても設定作業等が可能となる。

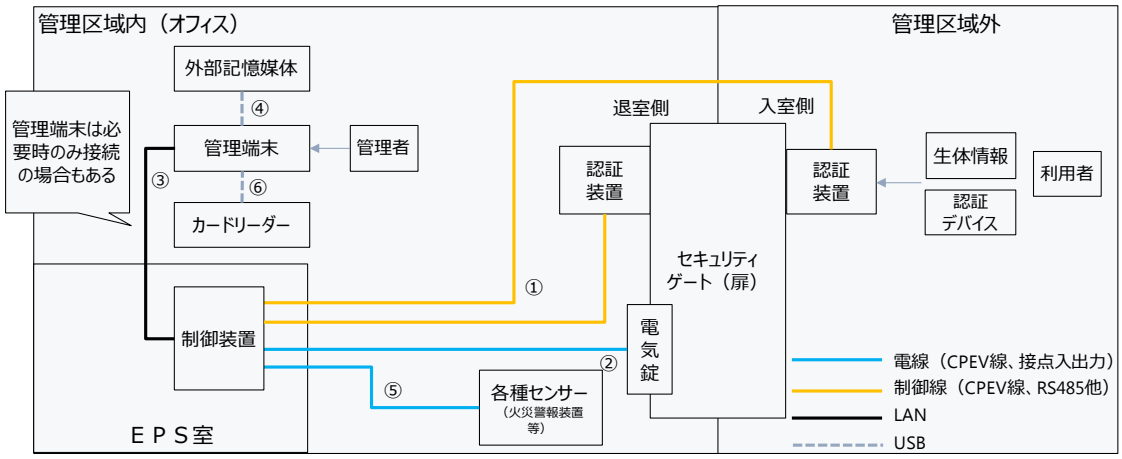

図 2-7　ユースケース①スタンドアローンモデル（SA）[1]

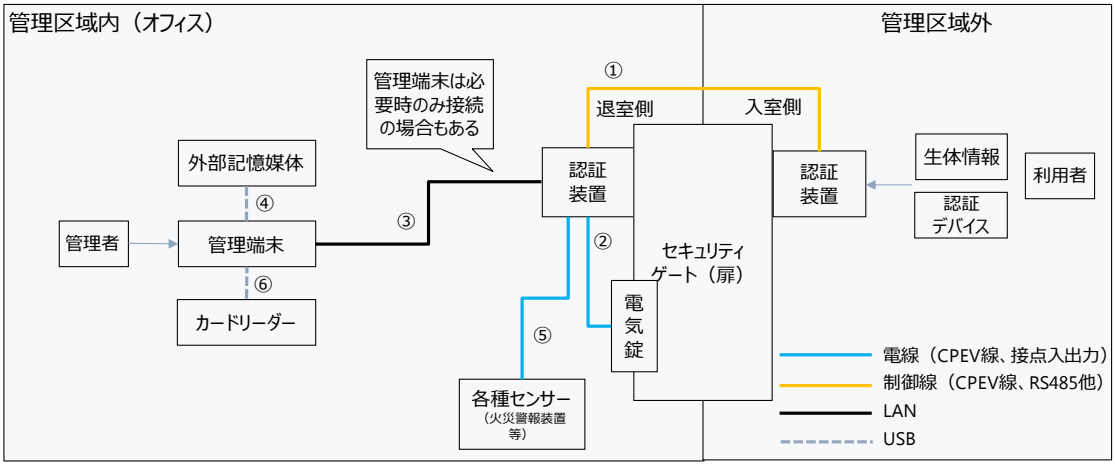

図 2-8　ユースケース①スタンドアローンモデル（SA）（認証装置機能と制御装置機能の一体型製品の場合）

[1] 接続線毎の通信の目的　：　認証装置から制御装置に読取った認証情報を送信、制御装置にて照合認証を実施（①）。制御装置は認証結果に基づき電気錠を解錠・施錠（②）。制御装置・認証装置の設定管理、データ取得は管理端末からウェブブラウザ・専用アプリケーションで実施（③）。入退履歴情報・設定情報・ファームウェアアップデートファイルは外部記憶媒体経由で入出力することが可能（④）。火災警報装置等と連動し、災害発生時は全解錠／全施錠（⑤）。カード情報の登録は管理端末にカードリーダーを接続して行う（⑥）。

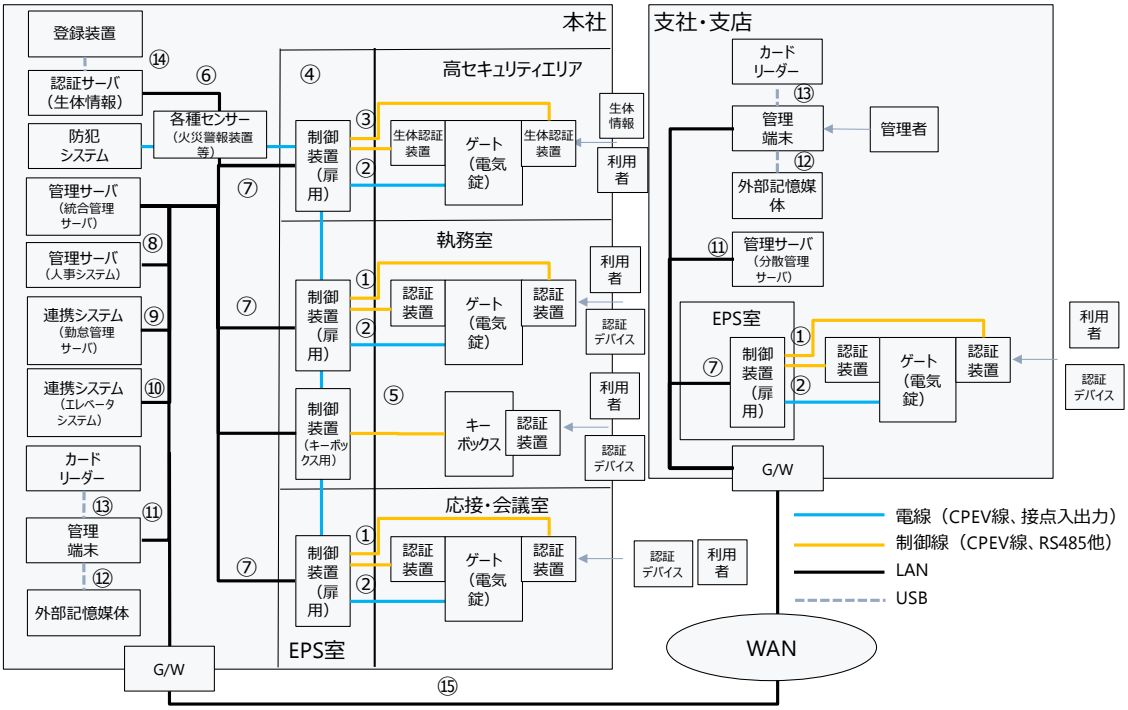

図 2-9　ユースケース②統合管理モデル（TM）[2]

[2] 接続線毎の通信の目的　：　認証装置から制御装置に読取った認証情報を送信（①）、制御装置にて照合認証を実施して電気錠を解錠・施錠（②）。生体認証の場合は認証装置内で照合・認証を行う場合と、認証サーバで行う場合がある（③④）。登録の際は認証サーバに接続された登録装置を用いる（⑬）。キーボックスアクセスと入退管理システムが連携している場合は、キーボックスの認証装置（カードリーダ等）から制御装置に読取った認証情報を送信 、制御装置にて照合認証を実施してキーボックスに結果及びアクセス可能キー番号等を送信（⑤）。火災警報装置等と連動し、災害発生時は全解除／全施錠、接点接続を連携するため各制御装置間を接続（⑥）。制御装置の設定管理、データ取得は管理端末から統合管理サーバ経由で実施（⑦、⑪）。利用者情報登録管理に用いる従業員情報は人事システムから取得（⑧）。従業員の照合情報（入室／入館、退室／退館時刻）を勤怠管理サーバに送信（⑨）。利用者のアクセスレベル、操作レベル等に応じ、エレベーターの停止階を制御するため、エレベータシステムと連携（⑩）。入退履歴情報・設定情報・ファームウェアアップデートファイルは外部記憶媒体経由で入出力することが可能（⑫）。ID カードは USB 接続のカードリーダーを用いて実施する（⑬）。統合管理サーバで利用者情報を作成し各分散管理サーバに配布、分散管理サーバから入退管理履歴を集約する（⑭）。

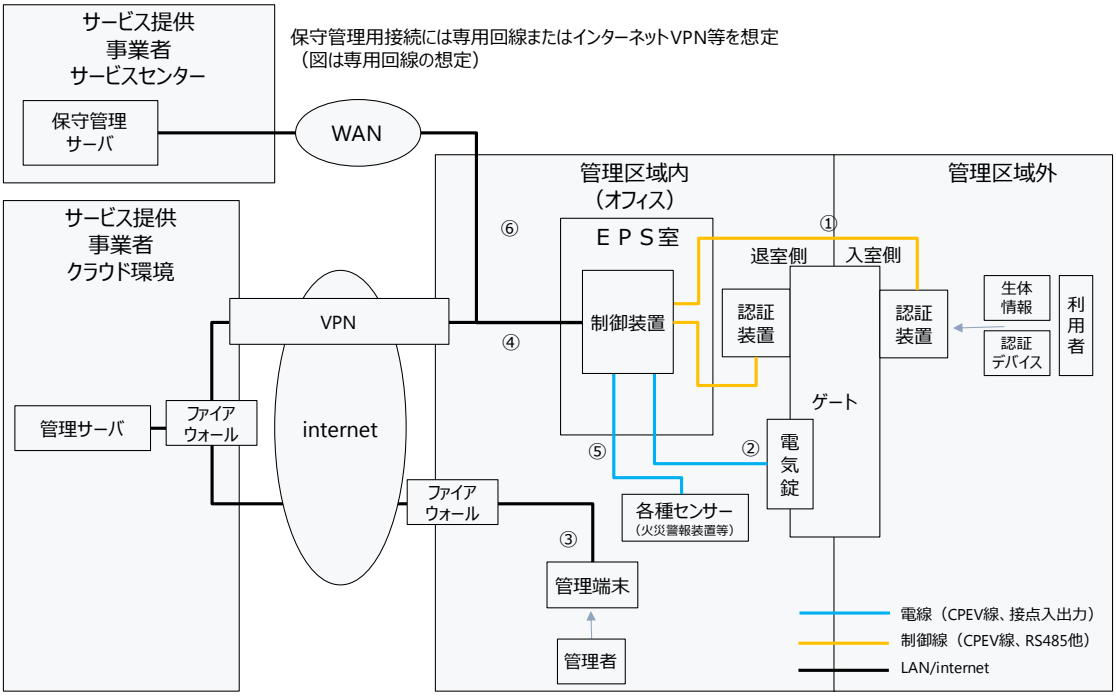

図 2-10　ユースケース③クラウドサービスモデル（CS）[3]

2.2 ユースケース毎の脅威の洗い出し

2.2.1 調査概要

入退管理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､ユースケース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、「ユースケース」及び「フェーズ」をベースとし、以下の手順で実施した。（図 2-11）

なお、フェーズは以下の 5 パターンを設定した。

- 登録：利用者の認証データやスケジュール等の設定データの登録時
- 運用：通常の運用時
- 警備：警備員が巡回する警備時
- 異常：建物内で火災が発生し火災警報装置の鳴動や移報が伝達された場合や、入退室の異常発生時で扉を開閉する必要がある場合
- 保守：機器の保守時（ファームウェアアップデートも含む）

[3] 接続線毎の通信の目的　：　認証装置間で同期等を行い（①）、電気錠を解錠・施錠（②）。認証装置の設定管理は管理端末上のウェブブラウザからクラウドサービスとしての管理サーバに対して実施（③）、管理サーバ上に保管された設定情報はインターネット経由で認証装置に送信（④）認証装置上の入退履歴情報はインターネット経由でクラウド上の管理サーバに保管（④）、ウェブブラウザを用いて取得（③）。火災警報装置等と連動し、災害発生時は全解除／全施錠（⑤）。サービス提供事業者の保守管理サーバからは認証装置の動作監視、ファームウェアアップデート等が実施される。保守管理を行う接続については、インターネットを用いる場合と専用回線が用いられる場合が想定される（⑥）　。

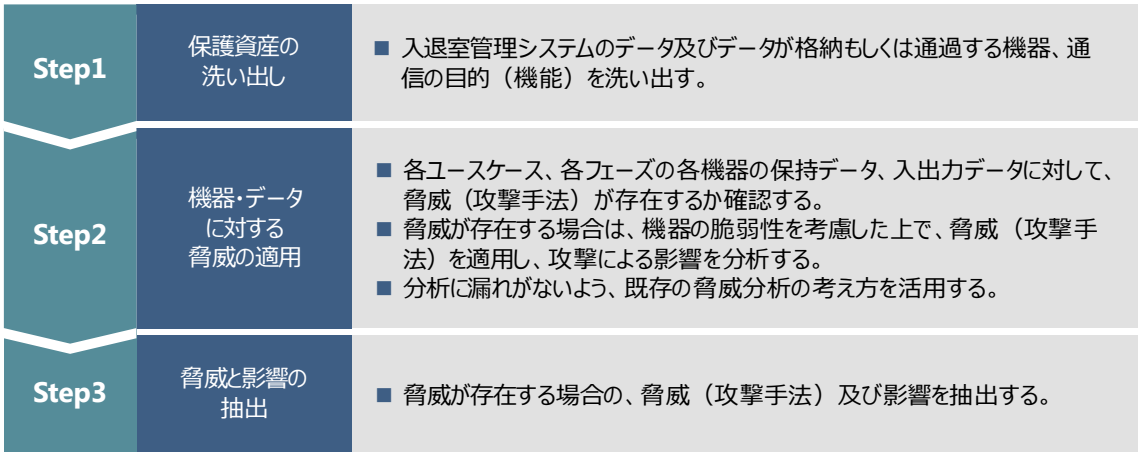

図 2-11　脅威分析方法

2.2.2

2.2.3 ユースケースにおける保護資産の洗い出し

はじめに、入退管理システムに存在するデータを製品カタログ等から抽出し、保護資産として**表 2-10** の通り整理した。その後、各ユースケースにおいて保有するデータをマッピングした（**図 2-12**、**図 2-13**、**図 2-14**）。

表 2-10　保護資産（データ）一覧

名称	含まれる情報	モデル		
		SA	TM	CS
認証データ	カード情報、暗証番号情報、生体情報	○	○	○
登録データ	利用者情報、組織情報、扉情報	○	○	○
状態データ	鍵情報、扉情報、警備情報、発報情報、機器情報	○	○	○
分析データ	在室者データ	○	○	○
時刻データ		○	○	○
識別認証データ（機器や、ソフトウェア等にログインするための認証情報）		○	○	○
設定データ	ネットワーク情報、スケジュール情報、カレンダー情報、制御対象情報、機器認証情報、各種管理情報、認証方法設定情報	○	○	○
ファームウェア（・基本ソフト）データ		○	○	○

ログデータ	入退ログ、認証装置ログ、スケジュール設定ログ、システムログ、操作・警報・故障ログ	○	○	○
センサーデータ	火報	○	○	○
移報	盗難警報、異常信号	○	○	○
アップデートファイル		○	○	○
制御データ	システム制御、認証装置制御、電気錠制御、入力制御、出力制御、部屋制御、警備ブロック制御、機器制御、コントローラ制御	○	○	○
連携システムデータ	映像監視システム、車両入退場システム、エレベーター、ビル管理システム、勤怠システム、人事システム	―	○	―

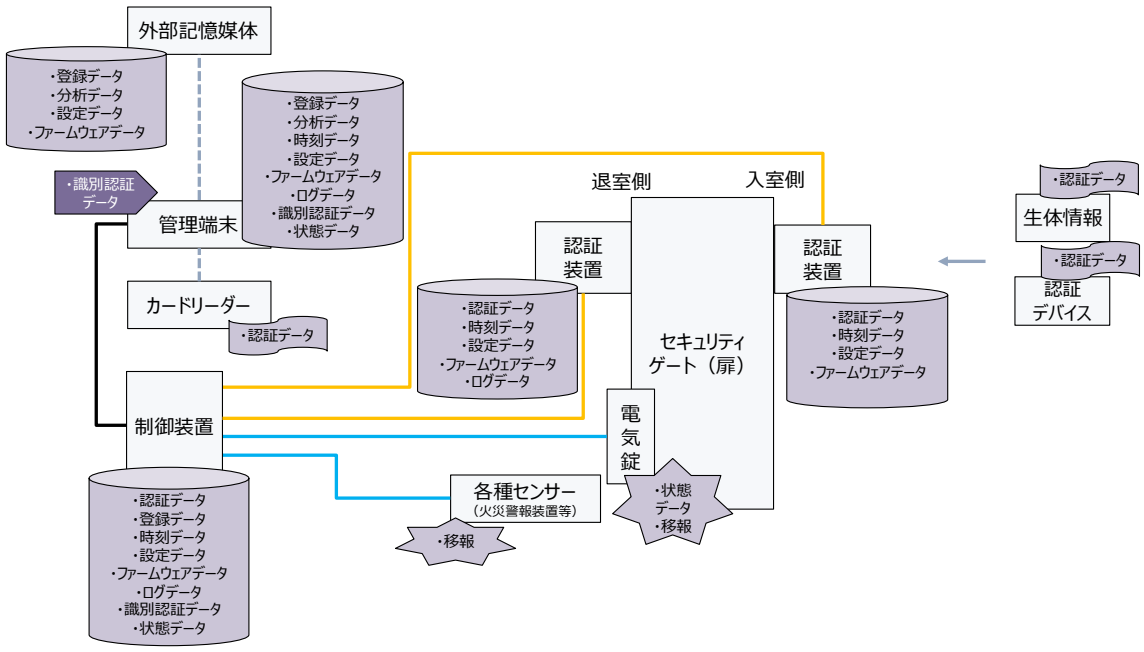

図 2-12　スタンドアローンモデル（SA）の保有データ

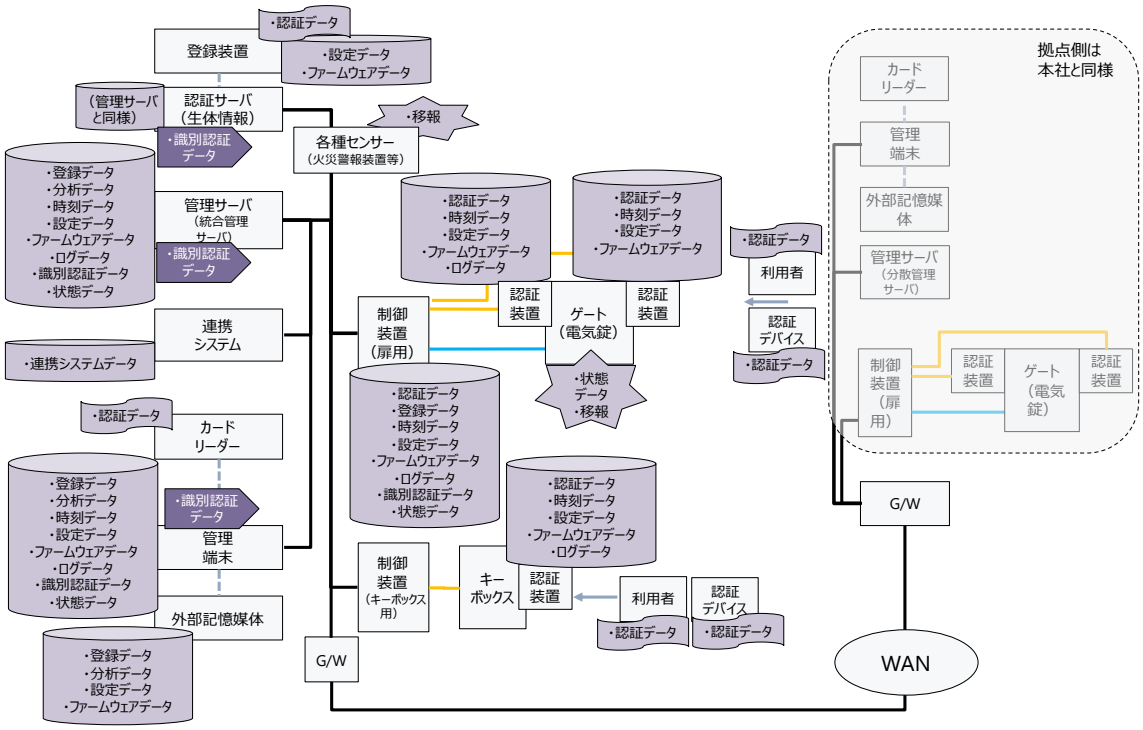

図 2-13　統合管理モデル（TM）の保有データ

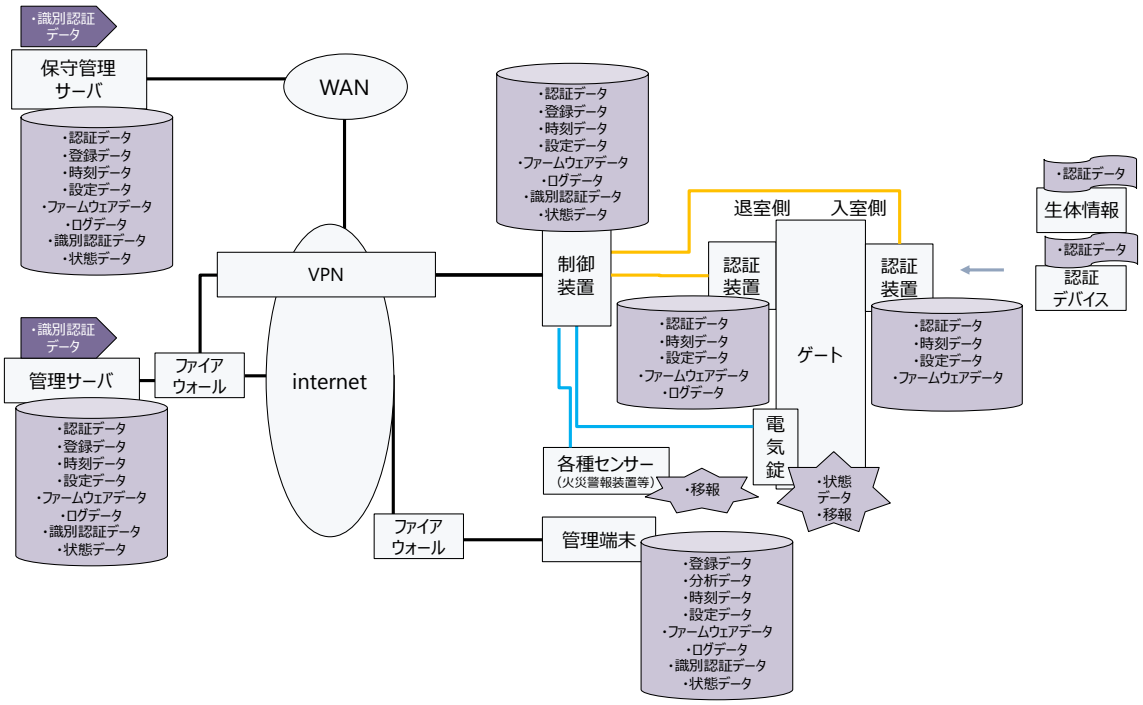

図 2-14　クラウドサービスモデル（CS）の保有データ

次に、保護資産として機器を整理した（表 2-11）。機器の整理にあたっては、設置場所を設定した。

表 2-11　保護資産（機器）一覧

		スタンドアローンモデル	統合管理モデル	クラウドサービスモデル
A-1	認証装置（入室側）	管理区域外	管理区域外	管理区域外
A-2	認証装置（退室側）	管理区域内	管理区域内	管理区域内
A-3	制御装置	管理区域内	管理区域内	管理区域内
A-4	管理サーバ	－	サーバ室	提供事業者環境
A-5	管理端末	管理区域内	管理区域内	管理区域内
A-6	認証デバイス	管理区域外	管理区域外	管理区域外
A-7	生体認証サーバ	－	サーバ室	－
A-8	生体認証装置	－	管理区域内	－
A-9	セキュリティゲート	管理区域外	管理区域外	管理区域外
A-10	電気錠	管理区域外	管理区域外	管理区域外
A-11	各種センサー	管理区域内	管理区域内	管理区域内
A-12	キーボックス	－	管理区域外	－
A-13	連携システム	－	サーバ室	－
A-14	防犯システム	－	サーバ室	－
A-15	外部記憶媒体	管理区域内	管理区域内	－
A-16	カードリーダー	管理区域内	管理区域内	－
A-17	登録装置	－	管理区域内	－
A-18	保守管理サーバ	－	－	提供事業者環境
A-19	ファイアウォール	－	サーバ室	サーバ室
A-20	ゲートウェイ	－	サーバ室	サーバ室
A-21	LAN	管理区域内	管理区域内	管理区域内
A-22	WAN	－	サーバ室	サーバ室
A-23	インターネット	－	－	管理区域外

2.2.4 機器・データに対する脅威の適用

本調査における脅威分析において想定する脅威（攻撃手法）は IPA「制御システムのセキュリティリスク分析ガイド」より以下の 21 項目を利用した（表 2-12）。

表 2-12　脅威（攻撃手法）一覧

脅威(攻撃手法)	説明
不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。
物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。
不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。
過失操作	内部関係者（社員や協力者の内、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。
不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVDやUSB機器等）を接続し、攻撃を実行する。
プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。
マルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。
情報窃取	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を窃取する。
情報改ざん	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を改ざんする。
情報破壊	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を破壊する。
不正送信	他の機器に対して、不正な制御コマンド（設定値変更、電源断等）や不正なデータを送信する。
機能停止	機器の機能を停止する。
高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。
窃盗	機器を窃盗する。
盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）が窃取される。
経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。
通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。
無線妨害	無線通信を妨害する。
盗聴	ネットワーク上を流れる情報を盗聴する。
通信データ改ざん	ネットワーク上を流れる情報を改ざんする。
不正機器接続	ネットワーク上に不正機器を接続する。

次に、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 2-8 で整理した入退管理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 2-13　攻撃者と攻撃機会

名称	攻撃機会
管理者	攻撃者として想定しない
保守員	攻撃者として想定しない
利用者	アクセス権を越えた操作や閲覧が可能
外部委託事業者	攻撃者として想定しない
サービス提供事業者	攻撃者として想定しない
第三者	機器への物理的な接触、及びネットワークへの接続が可能

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。

また、製造者については、攻撃者として想定せず、「機器の正当性を確認」との対策として整理する。工事者についても、攻撃者として想定せず、「システムの構築・施工に関する

要件を明記」との対策として整理する。

2.2.5 脅威と影響の抽出

整理した情報に基づき、ユースケース・フェーズ毎のデータ・機器から、脅威（攻撃手法）及び影響を抽出する。

脅威分析は、攻撃ポイント×攻撃目標機器・データ×攻撃ゴールの組み合わせから、現実に発生しうるガイドワード（脅威 21 項目）の絞り込みを行った。

影響は、ガイドワード（脅威 21 項目）×攻撃ポイント×攻撃目標機器・データ×攻撃ゴールの組み合わせとして整理した。

まず、脅威及び影響の絞り込みにあたって、NIST SP800-30 “Guide for Conducting Risk Assessments”（表 2-14）と ENISA “Threat Taxonomy: A tool for structuring threat information”（表 2-15）を参考に攻撃ゴールを設定した（表 2-16）。ここで、攻撃ゴール 1・2 は各フェーズで異なる攻撃ゴールであり、攻撃ゴール 3～8 は全てのフェーズで共通の攻撃ゴールである。

表 2-14　NIST SP800-30 “Guide for Conducting Risk Assessments”内で示されている潜在的な攻撃脅威/攻撃目標の分類[4]

1. 偵察を行い、情報を収集する
2. 攻撃に用いるツールを作成する
3. 悪意あるツール（マルウェア等）を挿入する
4. 脆弱性を利用し、情報やシステムを侵害する
5. 実質的な攻撃を実施する
6. システム機能を攻撃に気づかれることなく維持する
7. 攻撃活動を他の攻撃と連携させる

表 2-15　ENISA “Threat Taxonomy: A tool for structuring threat information” 内で示されている潜在的な攻撃脅威/攻撃目標の分類[5]

1. 物理的な攻撃（デバイスの窃盗や破壊など）
2. 故意ではない攻撃（誤使用による情報流出など）
3. 自然災害
4. 攻撃による機能停止

[4] 3. はその後の攻撃のための過程であるため、除外。

[5] 2. 3. はスコープ外の影響であるため、除外。８．は攻撃による影響であるため、除外。

5. 停電やネットワークの切断
6. 情報の盗聴/傍受/ハイジャック
7. 実質的な攻撃活動
８．違法行為への誘導（及び顧客信頼の損失）

表 2-16　各フェーズにおける攻撃ゴール一覧

	登録フェーズ	運用フェーズ	警備フェーズ	異常フェーズ	保守フェーズ
【G-1】	不正な登録が実行される	不正な入退室が実行される	不正な入退室が実行される	不正な移報の伝送や、それに伴う不正な扉の開閉が実行される	不正なアップデートが実行される
【G-2】	適切な登録が実行されない（利用者や設定が登録できなくなる）	適切な入退室が実行されない（利用者が入退室できなくなる）	適切な入退室が実行されない（警備員が入退室できなくなる）	適切な移報が伝送されず、適切な扉の開放が実行されない	適切なアップデートが実行されない
【G-3】	重要な情報が漏洩する[6]				
【G-4】	重要な情報が消去される[7]				
【G-5】	他攻撃のための攻撃の踏み台とされる/他の攻撃を実行するための補助攻撃が実行される				
【G-6】	機器の破壊など、物理的に悪意ある影響を及ぼす				
【G-7】	攻撃の証拠を消去する				
【G-8】※	連携システムへと悪意ある影響を及ぼす				

※　【G-8】「連携システムへと悪意ある影響を及ぼす」は統合管理モデルにのみ存在する攻撃ゴールである。

次に、各フェーズでの攻撃ゴールを達成するために攻撃目標となるデータを検討するために、各データが改ざん/破壊された場合に、各フェーズの主要機器に影響があるデータを以下の表において×と表記し、整理した。

[6] 【G-3】「重要な情報が漏洩する」における「重要な情報」とは、保護資産（データ）における時刻データ以外のデータを指す。

[7] 【G-4】「重要な情報が消去される」における「重要な情報」とは、時刻データを含んだ全ての保護資産（データ）を指す。これは、時刻データがタイムスタンプの役割として機能する場合、時刻データが消去されることで適切なログが保存されないなど、様々な影響を及ぼすことに起因する。

表 2-17　各データにおける攻撃による影響

	①登録フェーズ	②運用フェーズ	③警備フェーズ	④異常フェーズ	⑤保守フェーズ
各フェーズの主な実施事項	利用者情報の登録	利用者の入退室	警備員の入退室	移報の伝達・火災報知器の鳴動・ゲートの停止	ファームウェア等アップデート
各フェーズにおける主要機器[8]	管理端末・管理サーバ	制御装置・認証装置	制御装置・認証装置	各種センサー・認証装置	全端末・全装置・全サーバ
認証データ	×	×	×		×
登録データ	×	×	×	×	×
状態データ		×	×	×	×
分析データ		×			
時刻データ	×	×	×	×	×
識別認証データ	×	×	×	×	×
設定データ	×	×	×		×
ファームウェアデータ					×
ログデータ	攻撃目標 7「攻撃の証拠を消去する」において影響				
センサーデータ				×	
移報				×	
アップデートファイル					×
制御データ		×	×	×	
連携システムデータ	統合管理モデルにおいて影響				

[8] 主要機器とは、各フェーズの主な実施事項を実質的に実行する機器であり、その機器が侵害されることで各フェーズの主な実施事項を達成できないものと定義している。

次に、各フェーズでの攻撃ゴールを達成するための、入退室管理システムの攻撃ポイントを下記 A.~G.の 7 つに分け整理した。（表 2-18）

表 2-18　攻撃ポイント別の脅威と影響

<table>
<tr><th></th><th>機器例</th><th>データ例</th><th colspan="5">各フェーズにおける、攻撃による影響例</th></tr>
<tr><th></th><th></th><th></th><th>①登録フェーズ</th><th>②運用フェーズ</th><th>③警備フェーズ</th><th>④異常フェーズ</th><th>⑤保守フェーズ</th></tr>
<tr><td>A.USB 等を利用した攻撃</td><td>外部記憶端末</td><td>登録データ
設定データ</td><td>利用者データが登録できない</td><td></td><td></td><td></td><td>管理端末がアップデートされない</td></tr>
<tr><td>B.端末・装置に対する攻撃</td><td>管理端末･管理サーバ
制御装置
認証装置</td><td>登録データ
設定データ
ログデータ
状態データ</td><td rowspan="2">利用者情報が登録できない</td><td rowspan="3">利用者が入退室できない</td><td rowspan="3">警備員が入退室できない</td><td rowspan="3">異常時に扉が開閉されない</td><td>装置・端末がアップデートされない</td></tr>
<tr><td>C.ネットワーク上のデータに対する攻撃</td><td>管理端末と制御装置間のネットワーク</td><td>登録データ
設定データ
ログデータ
状態データ</td><td rowspan="2"></td></tr>
<tr><td>D.電線・制御線に対する攻撃</td><td>制御装置から電気錠への電線</td><td>認証データ
状態データ</td><td></td></tr>
<tr><td>E.情報入力を利用した攻撃</td><td>管理端末への入力</td><td>識別認証データ
認証データ</td><td>利用者情報が登録できない</td><td></td><td></td><td></td><td>装置・端末がアップデートされない</td></tr>
<tr><td>F.情報出力を利用した攻撃</td><td>管理端末からの出力</td><td>認証結果</td><td colspan="5">利用者の認証結果（個人情報を含む可能性あり）が第三者に漏洩する。</td></tr>
<tr><td>G.各種センサーに対する攻撃</td><td>火災センサー等</td><td>移報</td><td></td><td></td><td></td><td>異常時に扉が開閉されない</td><td></td></tr>
</table>

各ユースケース及びフェーズ毎に攻撃ポイント別脅威を図示すると以下のようになる。（図 2-15～図 2-29）

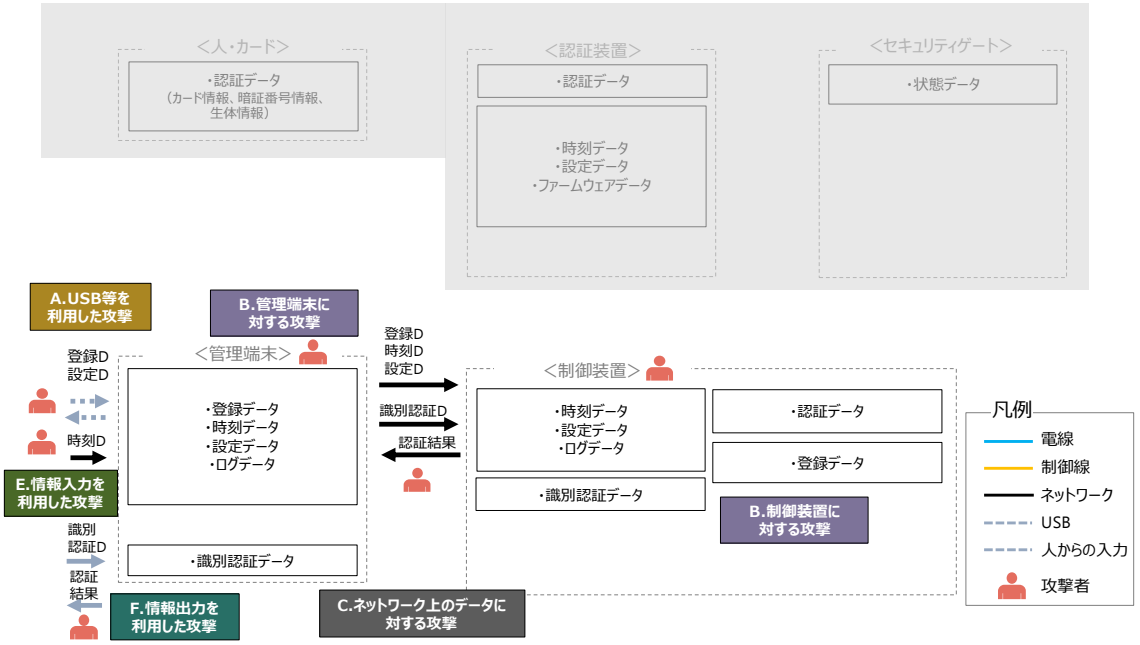

図 2-15　スタンドアローンモデル ①登録フェーズ

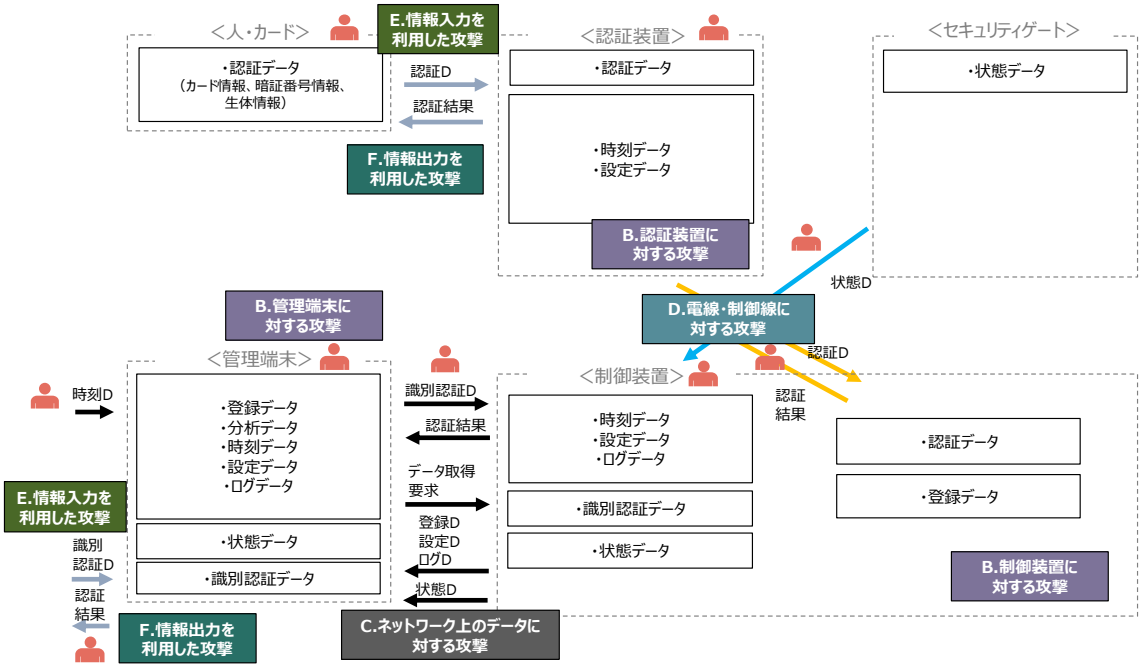

図 2-16　スタンドアローンモデル ②運用フェーズ

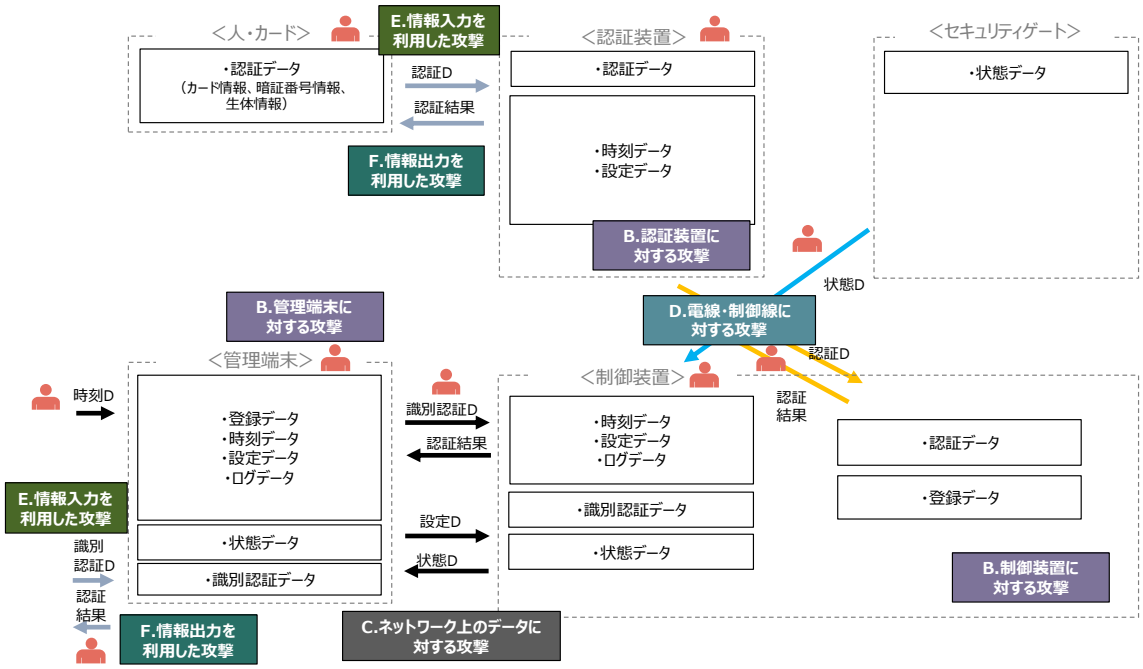

図 2-17　スタンドアローンモデル ③警備フェーズ

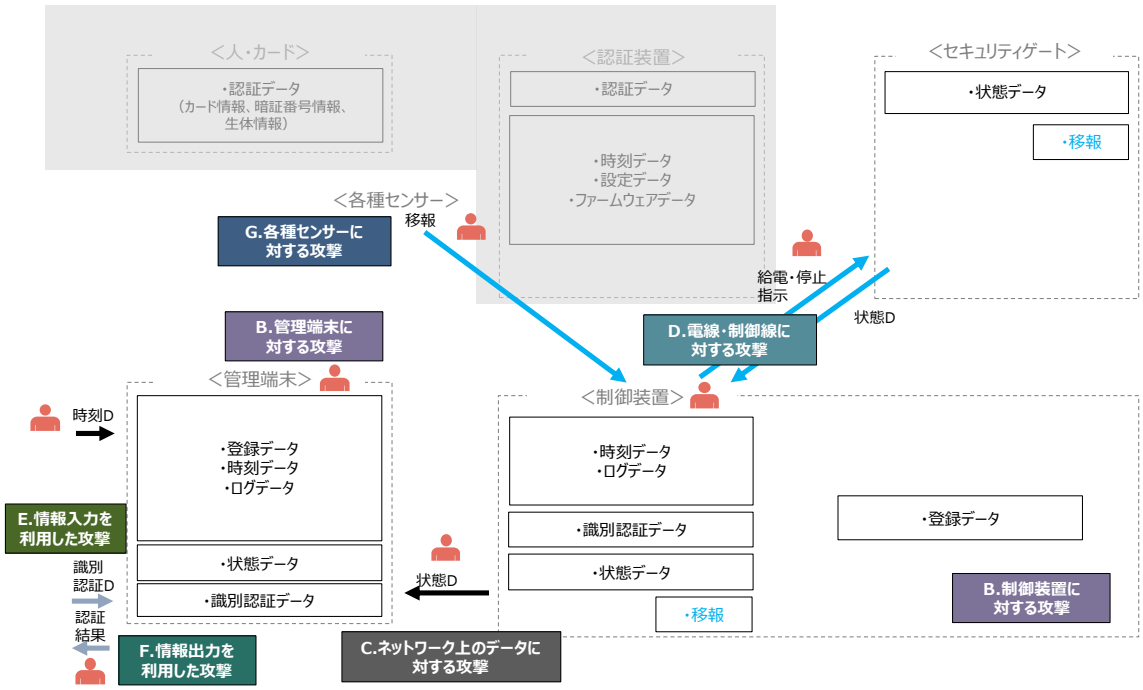

図 2-18　スタンドアローンモデル ④異常フェーズ

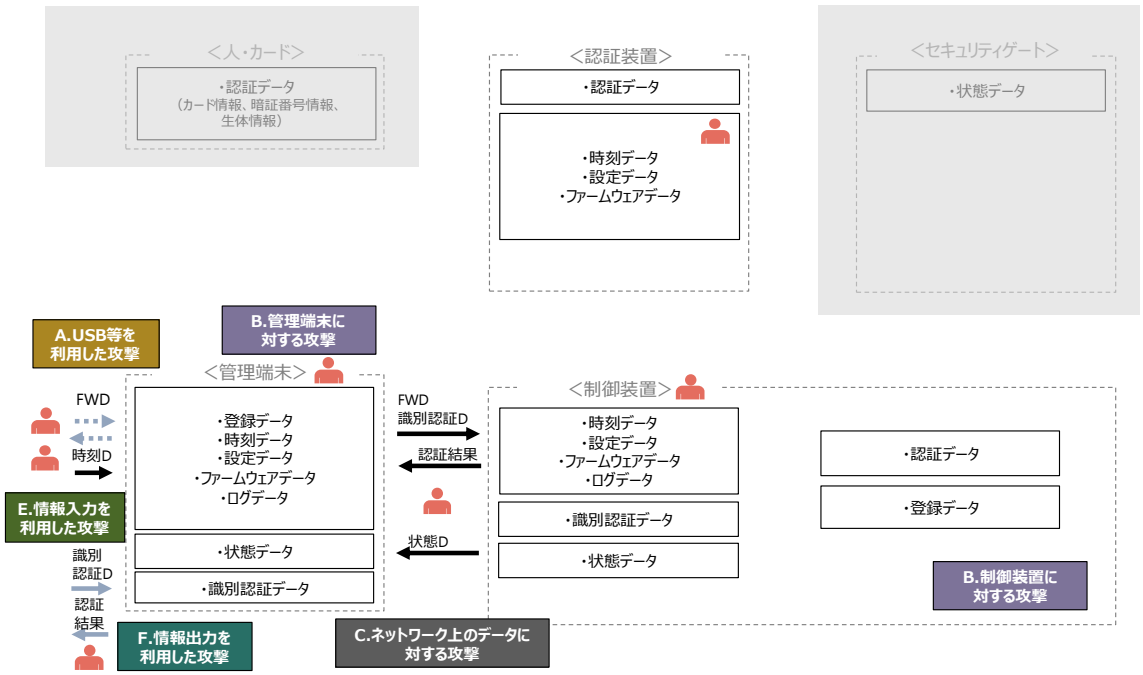

図 2-19　スタンドアローンモデル ⑤保守フェーズ

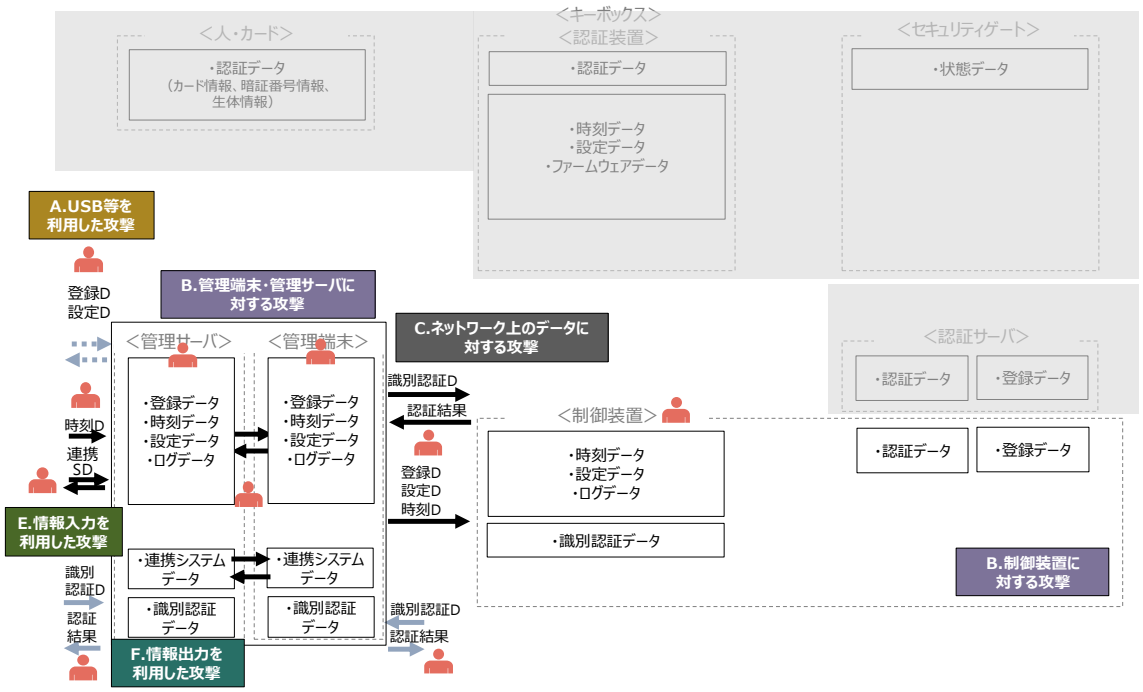

図 2-20　統合管理モデル ①登録フェーズ

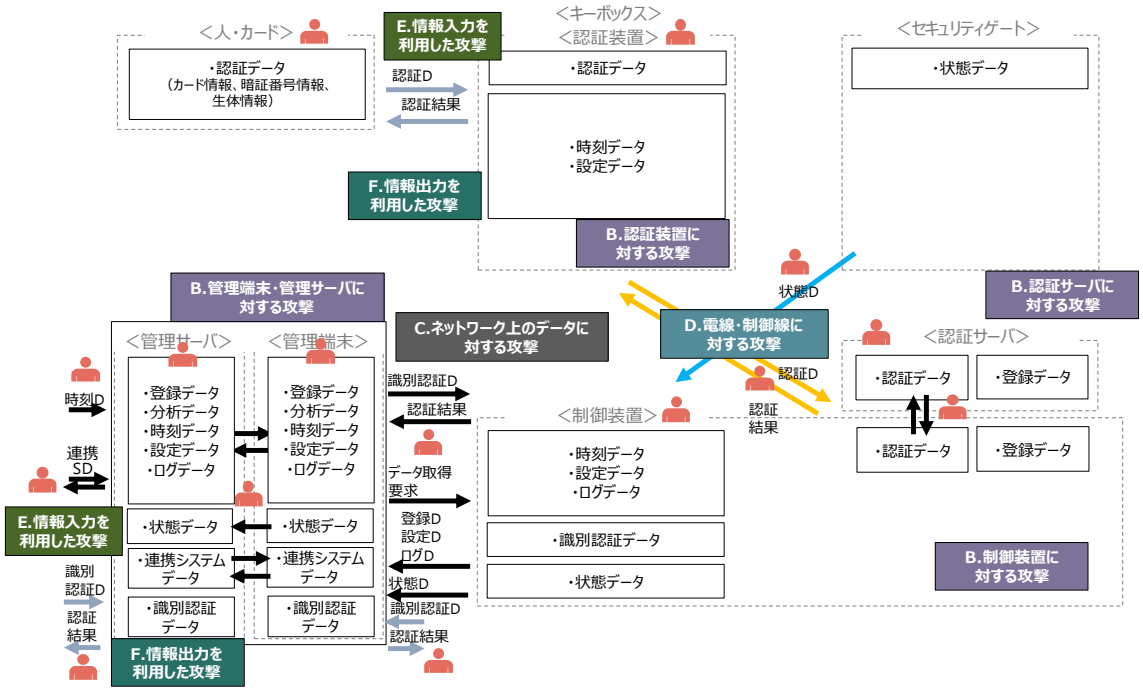

図 2-21　統合管理モデル ②運用フェーズ

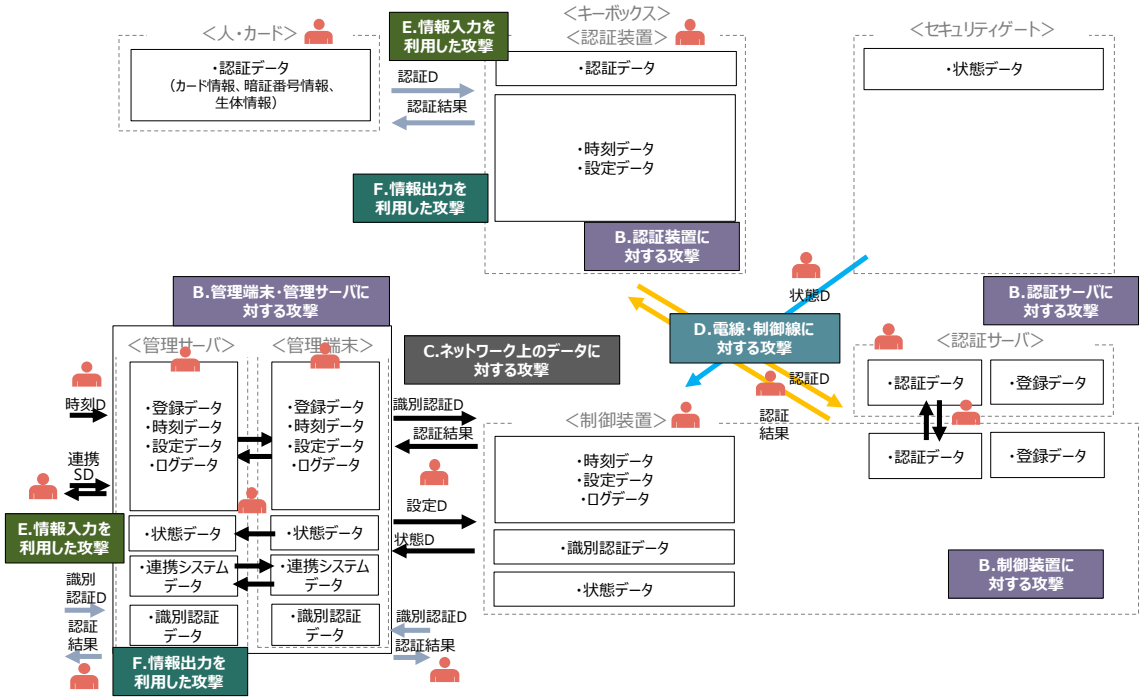

図 2-22　統合管理モデル ③警備フェーズ

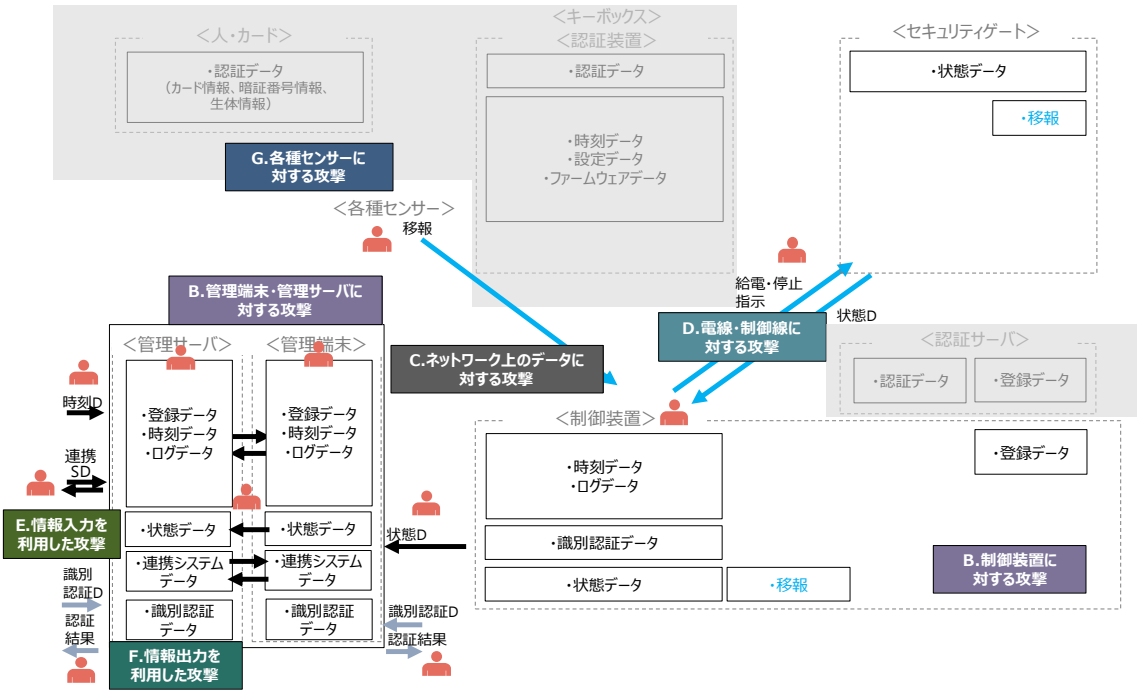

図 2-23　統合管理モデル ④異常フェーズ

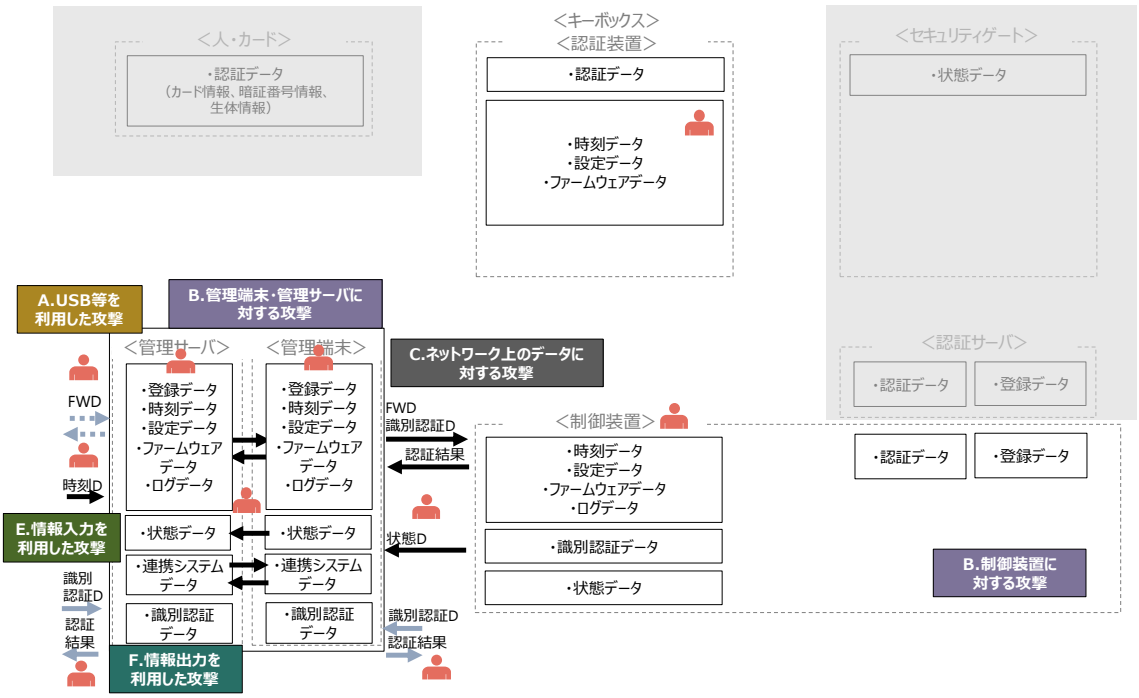

図 2-24　統合管理モデル ⑤保守フェーズ

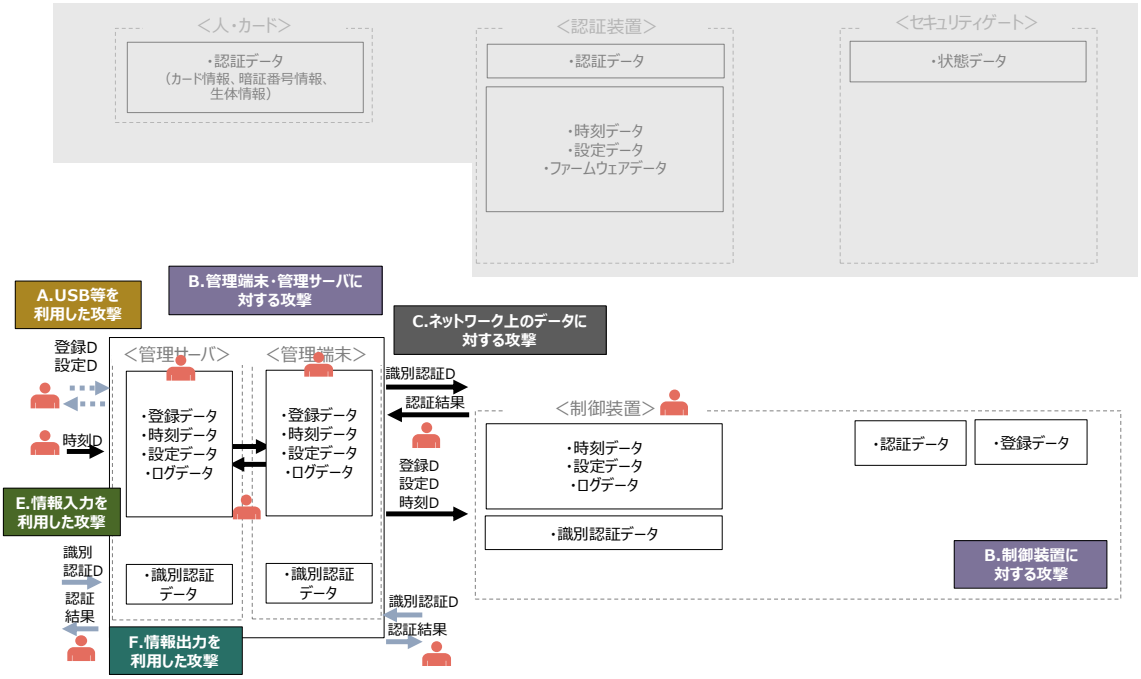

図 2-25　クラウドサービスモデル ①登録フェーズ

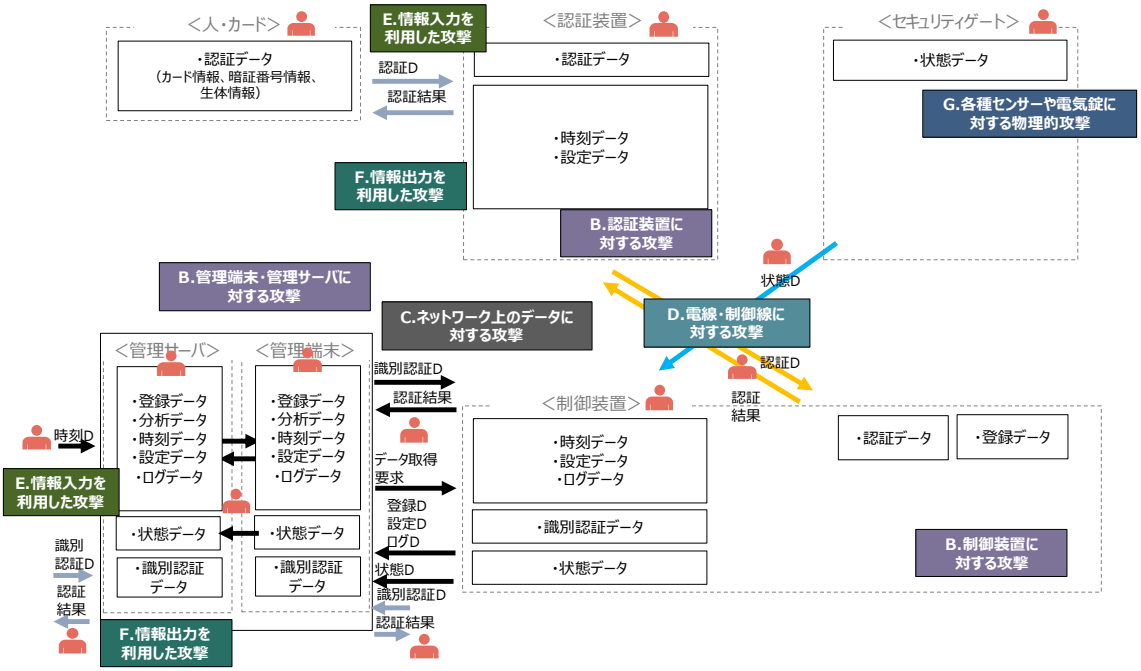

図 2-26　クラウドサービスモデル ②運用フェーズ

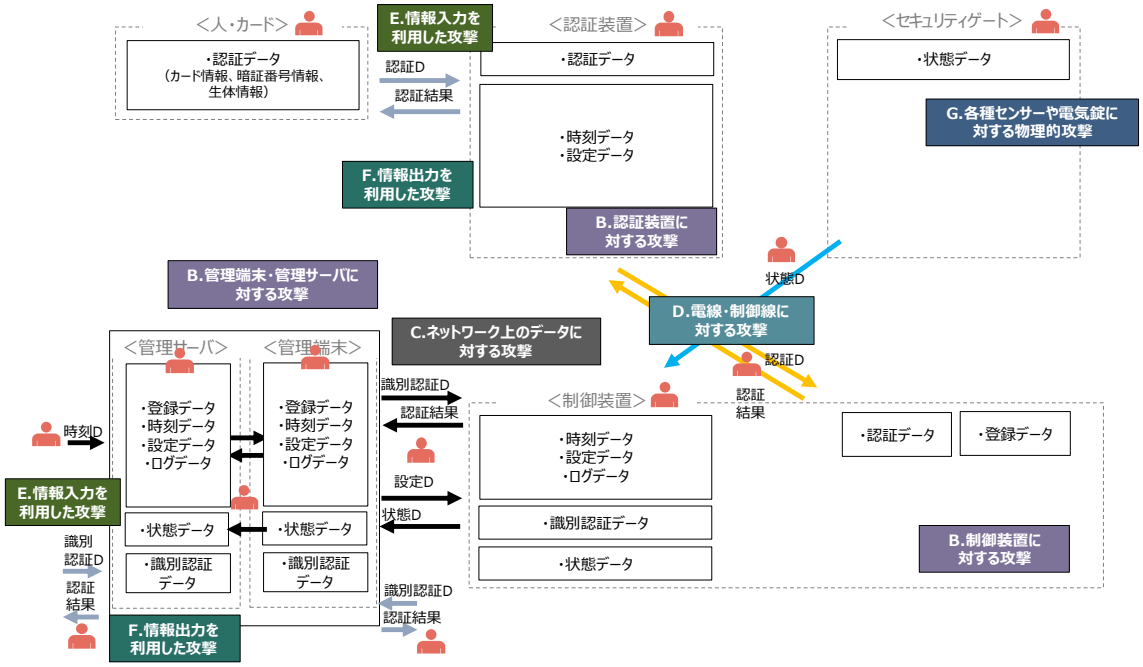

図 2-27　クラウドサービスモデル ③警備フェーズ

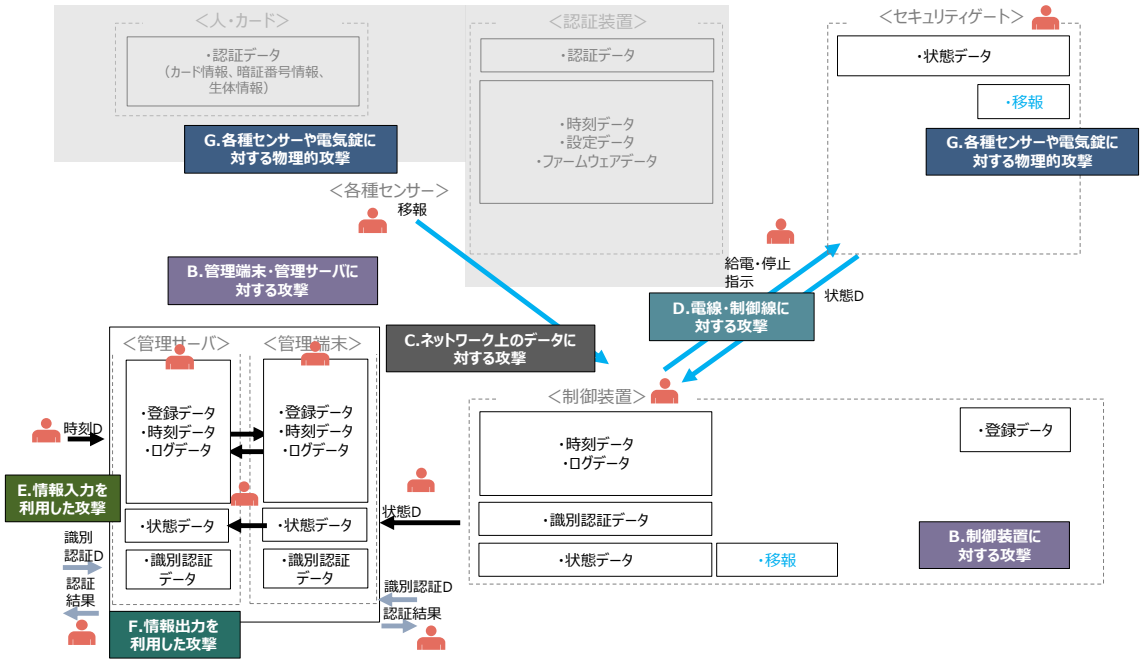

図 2-28　クラウドサービスモデル ④異常フェーズ

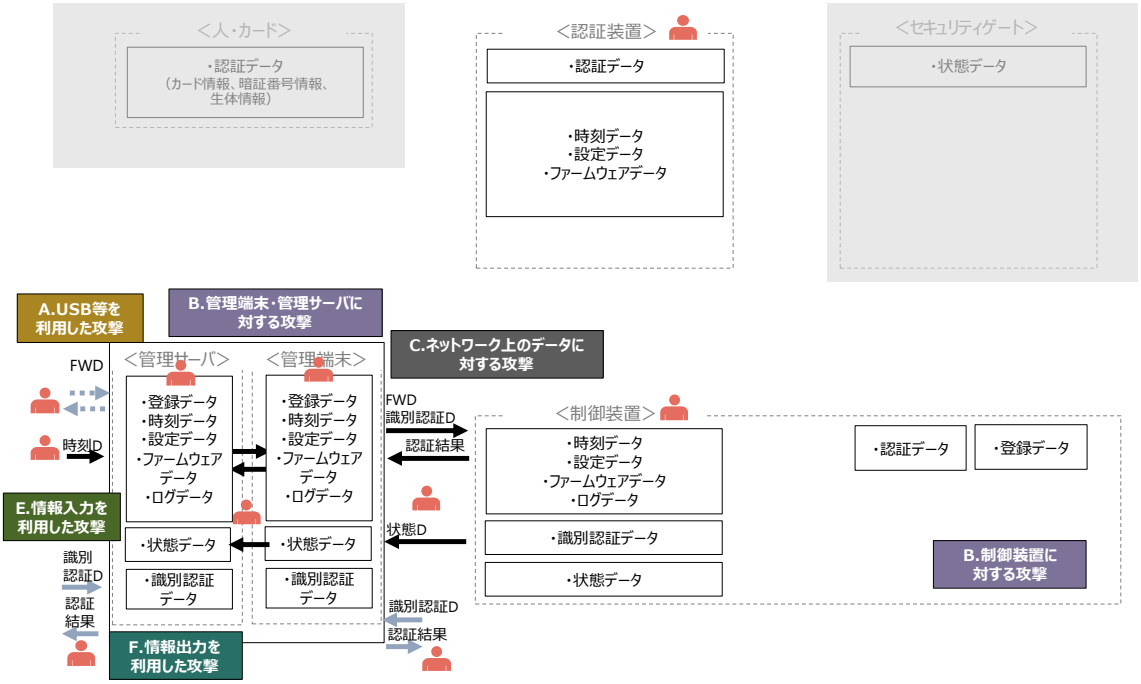

図 2-29　クラウドサービスモデル ⑤保守フェーズ

これらのユースケースに基づき、各機器に対する脅威分析を行った。まず、網羅性を担保する目的で各ユースケース・フェーズにおいて存在する全ての機器・データに対して、表 2-16 で示した攻撃ゴールへと繋がる脅威 21 項目（ガイドワード）を全て抽出した。これらの脅威 21 項目は、独立的な脅威ではなく、相互に作用する脅威であるため[9]、攻撃のステップを明確にするために、最終的な攻撃ゴールに達するための脅威の実施ステップを、攻撃ゴール毎に整理した。各機器は、表 2-18 で示した攻撃ポイントに分類可能であり、これにより後に示す脆弱性との対応が可能である。

2.3 脅威に対抗する情報セキュリティ要件の調査

2.3.1 調査概要

前章で識別された脅威に関して、入退管理システムのどのような機能により対抗・回避できるか、または入退管理システムの運用上どのようなことで対抗・回避ができるかを分析し、脅威に紐づけて整理した。

具体的には、入退管理システムの利用形態を想定したユースケース毎の各脅威に対抗するために具備すべき情報セキュリティ機能または運用要件を分析し、整理した。次に、整理した対抗策について、機能及び運用に関する必須要件の項目を作成した。作成した機能及び運用に関する必須要件の妥当性を委員会において確認し、決議された内容を基に、入退管理システムが現実的に対策できるセキュリティ要件にまとめた。

[9] 相互作用の例として、攻撃者が「物理的侵入」を行った後に機器の「機能停止」を行うなどが挙げられる。

2.3.2 ユースケース毎の各脅威に対抗するために具備すべき情報セキュリティ機能または運用要件

前章で整理した脅威を発生しうる脆弱性を整理し、取り得る対策（情報セキュリティ機能または運用要件）を検討した。

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
【15】物理的保護の不備

脅威分析において各機器に存在した脅威のそれぞれに対して、その脅威に起因する脆弱性を分析し整理した。

対策の検討にあたっては、ライフサイクルのフェーズ（設計・構築時、運用時、保守時、廃棄時）毎に各脆弱性に対する対策を検討した。各対策において、赤字は必須対策要件、黒字は条件付き必須対策要件を示す。ただし、各対策を入退管理システムに講じる際は、その運用を大幅に阻害しない範囲で適用する必要がある。

以上で示した、脅威分析資料、脆弱性分析資料及び対策資料について、脅威分析資料と脆弱性分析資料は全ての機器に存在する脅威による紐づけが可能であり、脆弱性分析資料と対策資料は各脅威に起因する脆弱性による紐づけが可能であるため、各脅威に対応した対策が示される。

3. まとめ

本調査では、IoT システムとして入退管理システムを利用する際に考慮すべきセキュリティ上の要件を明確にした。

脅威分析においては、入退管理システムに対する特徴的な脅威として、利用者の情報や扉情報の改ざん・破壊によって、利用者の入退室が脅かされる他、第三者が不正に入退室する可能性が想定された。特に保護資産を有する認証装置や、管理端末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、DoS 攻撃等の高負荷攻撃、ファームウェア等の脆弱性をつ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した。入退管理システムでは、一般的な IT 環境で利用するセキュリティや IDS/IPS 等のセキュリティ製品の導入が困難であり、またソフトウェアの更新範囲が限定的であることを踏まえ、適切なユーザ識別認証機構の導入、適切なファイル等アクセス制御の実装、機器や接続点の物理的保護、通信ネットワークの保護が重要であることが示された。

本調査による対策が調達時に活用されることで、入退管理システムの構築や利用に際してセキュリティ対策が進展することが望ましい。

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
BACNet	Building Automation and Control Networking protocol の略で、インテリジェントビル用ネットワークのための通信プロトコル規格。 ANSI や ISO での標準規格とされており、空調や照明、アクセス制御、火気検出などの総合的な制御に用いられる。
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
NAT	プライベート IP アドレスとグローバル IP アドレスを相互に変換する機能
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

IoT システムにおける情報セキュリティ対策要件策定に関する調査　調査実施報告書

2019 年 1 月

株式会社三菱総合研究所
社会 ICT イノベーション本部