JISEC-PROC-2019-B01

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

第1版

独立行政法人情報処理推進機構
入退管理システムセキュリティ要件検討WG

目　　次

1. はじめに 3
2. 入退管理システムのセキュリティ 4
2.1. 入退管理システムに用いる ID について注意すべき事項 4
2.2. システムの設計構築において注意すべき事項 5
2.3. システムの運用において注意すべき事項 6
2.4. システムの廃棄時に注意すべき事項 7
3. チェックリストについて 8
3.1. 対象とする利用形態 8
3.2. 前提条件 11
4. チェックリスト 12
4.1. チェックリストの使い方（調達時の例） 12
4.2. 設計構築フェーズ 13
4.3. 運用フェーズ 17
4.4. 保守フェーズ 18
4.5. 廃棄フェーズ 18
5. 付録 19
5.1. 想定する脅威について 19
5.2. 用語集 20

改版履歴

版数	発行年月日	備考
第 1 版	20190507	初版

1. はじめに

本書「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」は、「政府機関等の情報セキュリティ対策のための統一基準」[1]において調達・運用時のセキュリティ要件を求められている IoT 機器を含む特定用途機器のひとつである「入退管理システム」について、想定される脅威に対策を講ずる情報セキュリティ対策の要件を列挙した資料です。敷地や建屋の物理セキュリティを確保するためにどのような入退管理を設計するかといった、システムそのものの要件は定義していません。本書は政府機関や自治体の調達仕様書への転記目的に限らず、「3.1 対象とする利用形態」に該当するシステムであればどなたでも参照可能です。

本書に記載したチェックリストの各項目は、現行の入退管理システムで使われている機器の機能性を考慮した上で、現実的に適用可能なセキュリティ対策要件を具体的に記載したものです。本書が調達仕様策定時[2]や、運用において参照されることにより、入退管理を始めとする IoT システムの情報セキュリティが向上することを期待します。

1 https://www.nisc.go.jp/active/general/ 「政府機関等の情報セキュリティ対策のための統一基準群」参照

2 本書は調達者が本書の目的を理解した上で調達仕様書に転記し易い形で作成しています。設計構築を発注する業者向けに適したチェックリスト部分のみを抜き出した表も公開しています（4.1 節参照）。

2. 入退管理システムのセキュリティ

2.1. 入退管理システムに用いる ID について注意すべき事項

一般的な入退管理システムでは、利用者に紐づいた一意の値を ID として利用し、その ID がシステムに登録されている ID と一致するか否かにより、利用者の入退権限の有無を判断しています。そのため、ID が漏えいすると不正な入退に悪用されてしまう可能性があります。例えば、IC カードを用いた入退管理システムでは以下の様な注意が必要です。

例： カード固有の ID の利用

IC カードはそれぞれカード固有の値[3]を持っています。これらの値は IC カードを発行するベンダによってカード毎に一意に付与されているため、利用者を特定する ID として使うことが考えられます。しかしこれらのカード固有の値は市販のカードリーダーやスマートフォンで簡単に読み出せるため、情報セキュリティの観点から言えば入退管理システムで用いる ID としては適していません。

高い情報セキュリティが求められる区域においては、入退管理に用いる ID として利用する値はカード内の保護された領域に保存し、入退管理システムと事前共有された暗号鍵を用いた暗号化や MAC 認証を行って通信することにより、漏えいや複製を防止することも検討しましょう。

[3] TypeA(MIFARE)であれば UID、TypeF(Felica)であれば IDm が該当します。

2.2. システムの設計構築において注意すべき事項

入退管理システムにおいて、設計構築時に注意しなければならない情報セキュリティ上の事項があります。詳しくは「4.2 設計構築フェーズ」を参照して、調達仕様に転記してください。

例：　購入時のままのパスワード設定

2019 年には入退管理の管理サーバのソフトウェアにおいて識別認証情報（ユーザ ID とパスワード）が書かれていたことが脆弱性として公開[4]されました。攻撃者はこれらの情報を元に認証機能の突破を試みます。パスワードが製品出荷時の値になっていると、簡単に突破されてしまいます。パスワードは、システムを導入する組織の**情報セキュリティ対策基準や実施手順**[5]に則った値に必ず変更して運用しなければなりません。（4.2 節の要件 a03-3 参照。以降[対応する 4 章の要件番号]とする）

例：　不要なサービスの放置

IoT 機器は利用者が意識していない通信サービスが動いている場合があります。入退管理システムの脆弱性にはデータベースへアクセスするための識別認証情報がソフトウェアの中に記載されていたケースも報告されました。もし、データベースへ接続するためのサービスが動いていると、攻撃者はネットワーク経由でデータベースにアクセスして、登録されている ID 一覧など様々な情報を不正に入手、および改ざんすることができます。更にこの識別認証情報は利用者が書き換えられない場合があります。不要な通信サービスは構築のタイミングで停止しましょう。[a02-1]

---

4 脆弱性情報は CVE (https://cve.mitre.org/)、JVN (https://jvndb.jvn.jp/)等で検索することができます。

5 組織のセキュリティポリシーの下位文書（参照 https://www.ipa.go.jp/security/manager/protect/pdca/policy.html）

2.3. システムの運用において注意すべき事項

入退管理システムにおいて、運用時に注意しなければならない情報セキュリティ上の事項があります。詳しくは「4.3 運用フェーズ」を参照して、調達仕様に転記してください。

例：　ログの定期的な確認

システムのログは、不正アクセス、システムを構成する機器の停止や切断といった、攻撃や異常が発生したことを管理者が検知するために必要です。

入退管理システムではこれらに加えて、利用者の管理を委託しているオペレータが正しく登録や削除を行っているか、入退権限の無くなった ID を消し忘れていないかといった棚卸が必要かもしれません。このような正規の権限内での誤りは、システムが自動的に検知することが難しため、管理者が定期的にログを確認する必要があります。

定期的な確認によって、通常運用時からの変化による攻撃の予兆に気づける場合があり、また確認をしているという運用方針自体が、内部不正の抑止に繋がるかもしれません。[f01, f03]

例：　時間設定の定期的な確認

運用時は、システムの時刻設定を定期的にズレがないよう管理することが大切です。入退管理システムの特徴として決まった時間に警戒モードへ移行するシステムや、出退勤システムと連携しているシステムがあるため、時刻のズレが誤報や、遅刻や早退といった誤った記録に繋がるかもしれません。ログと同様に管理者が定期的に確認することが大切です。

2.4. システムの廃棄時に注意すべき事項

入退管理システムにおいて、その役目を終えてシステムを構成していた機器を廃棄する際にも、情報セキュリティの観点で考慮しなければならない事項があります。詳しくは「4.5 廃棄フェーズ」を参照してください。

例： 廃棄後の制御装置等からの情報漏洩

入退管理システムでは、システムを構成する一部の機器において利用者に紐づいた ID やログを保存しています。システムによっては ID に加えて個人を識別する情報を保持しているかもしれません。組織のセキュリティポリシーに照らし合わせて、それらの情報が漏えいすると問題となる場合は、リース、レンタルの返却や廃棄処理を外部委託する際の処置について調達仕様で要件化（復元不能な電磁的フォーマットや物理的破壊を行い、消去証明書を提出するなどと記載）しておくべきです。[h01-1]

一般的には管理サーバ、制御装置及び鍵管理盤など IP ネットワークに接続された機器に ID やログは保持されます。あらかじめシステム内のどの機器に漏えいしては困る情報が保存されるのかを確認し、廃棄処理の対象とする機器をリストアップしておきましょう。

3. チェックリストについて

本書のチェックリストはフェーズ（設計構築時、運用時、保守時、及び廃棄時）単位で節を分けて記載しています。入退管理システムを調達する際は委託する事業範囲に合わせて、チェックリストの内容を仕様書に転記してください。チェックリストは、2019 年現在の入退管理システムを構成する機器が持つ機能を踏まえ、IoT 機器に対する一般的な脅威[6]への現実的な情報セキュリティ対策要件を記載しています。機器やシステムの安全性や性能的要件、入退に利用する IC カードの要件や取扱いについては言及していません。

3.1. 対象とする利用形態

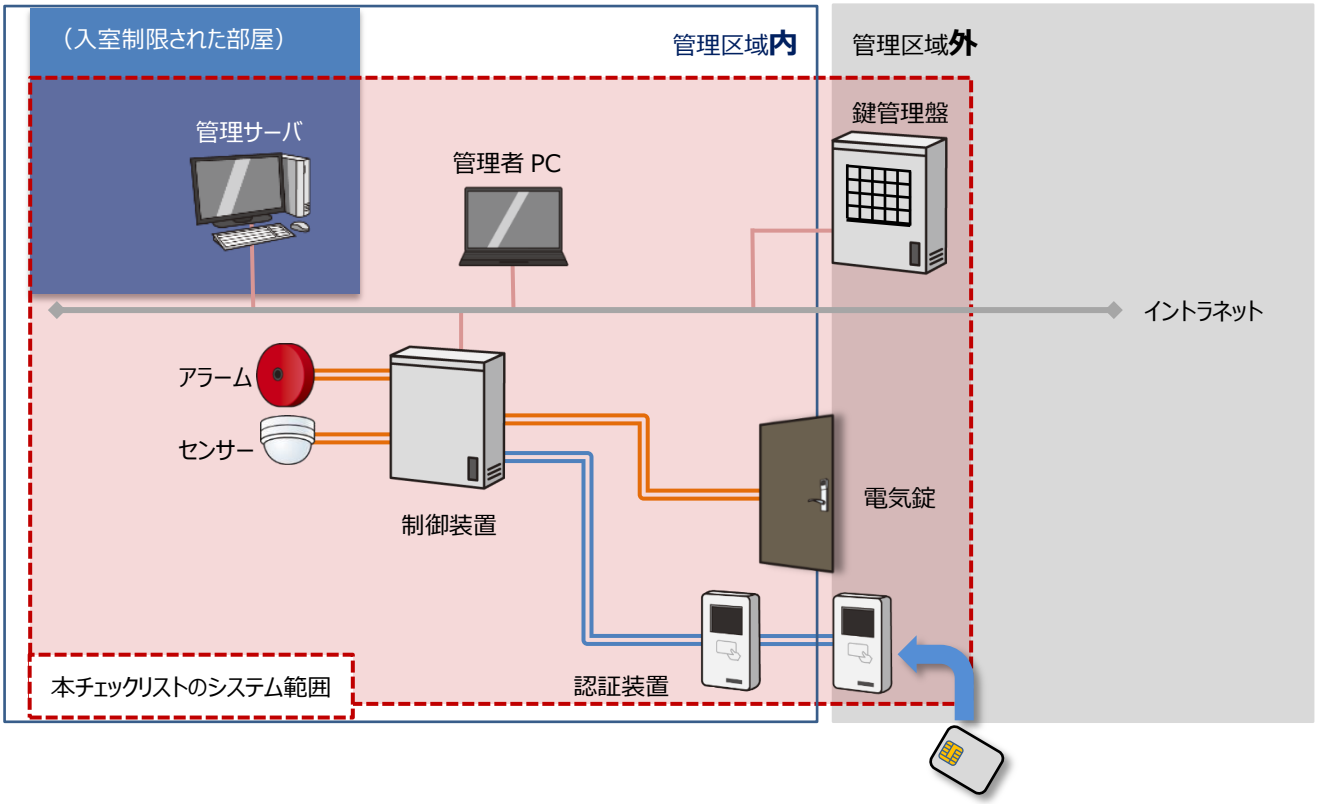


図 1　入退管理システム概要及びシステム範囲

[6] 本チェックリストで対策する脅威は「5.1 想定する脅威について」に例示しています。

本書は IP ネットワークに接続される入退管理システムを対象とし、入退管理の主要機能を担うに示した範囲を対象としています。

本書では整理のために、カード内の値や指紋情報など利用者に紐づいた一意の識別情報を「ID」と呼びます。システムを構成する機器への管理機能（Web サーバなど）へのログインに用いる情報は、「識別認証情報」とし、個別に記載する場合は「ユーザ ID」、「パスワード」とします。（図 2 参照）

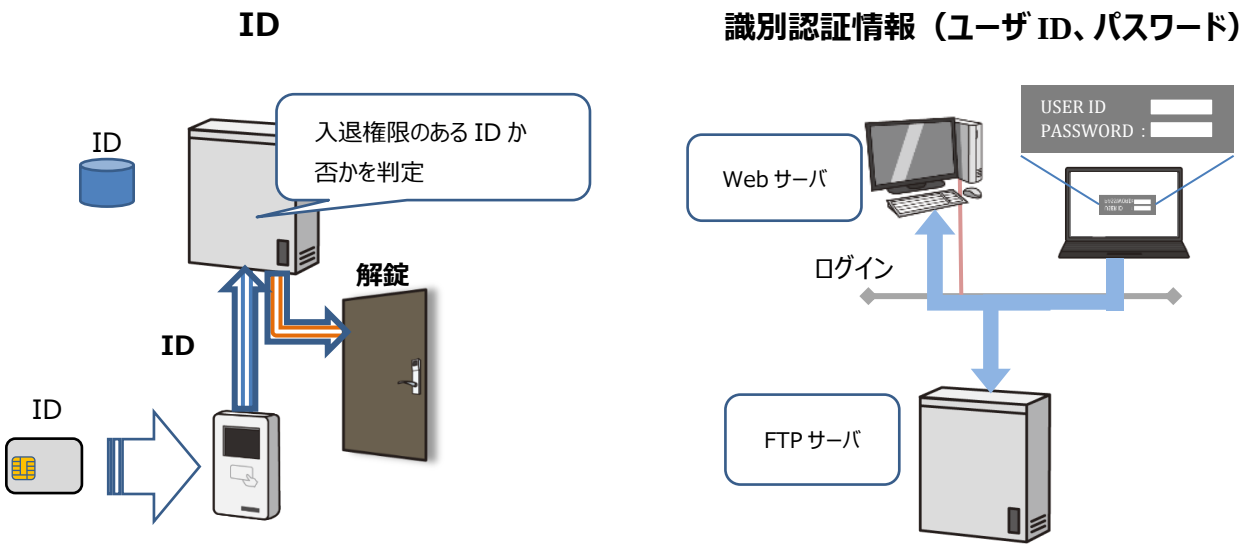


図 2　本書で用いる識別情報の用語

入退管理システムはその規模と利用用途により、スタンドアローンモデル、統合管理モデル、及びクラウドモデルに分類できます。4 章ではそれぞれのモデル毎に必須要件を記載しています。

統合管理モデル

複数の居室からなるオフィスにおいて複数の出入り口を入退管理するシステム。各利用者の出入口毎の入退権限を管理する管理サーバがシステム内に存在する。図 1 に示したモデル。

スタンドアローンモデル

サテライトオフィスの入退管理など、出入口毎に単独で管理するシステム。運用時には IP ネットワークへの接続が無く、管理サーバが存在しないシステム。

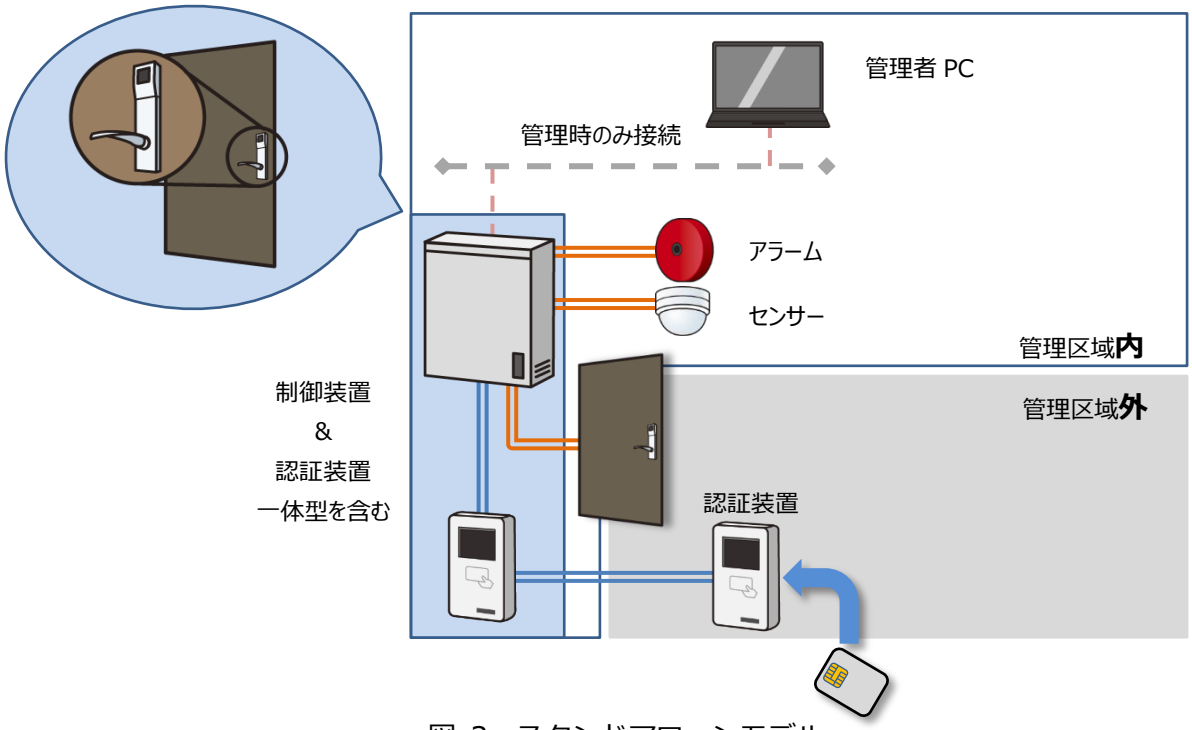


図 3　スタンドアローンモデル

クラウドモデル

統合管理モデルにおける管理サーバの機能を外部に委託しているモデル。管理者は委託先が提供している Web ベース等の管理サイトを利用して入退管理システムの ID 登録やログの確認を行う。

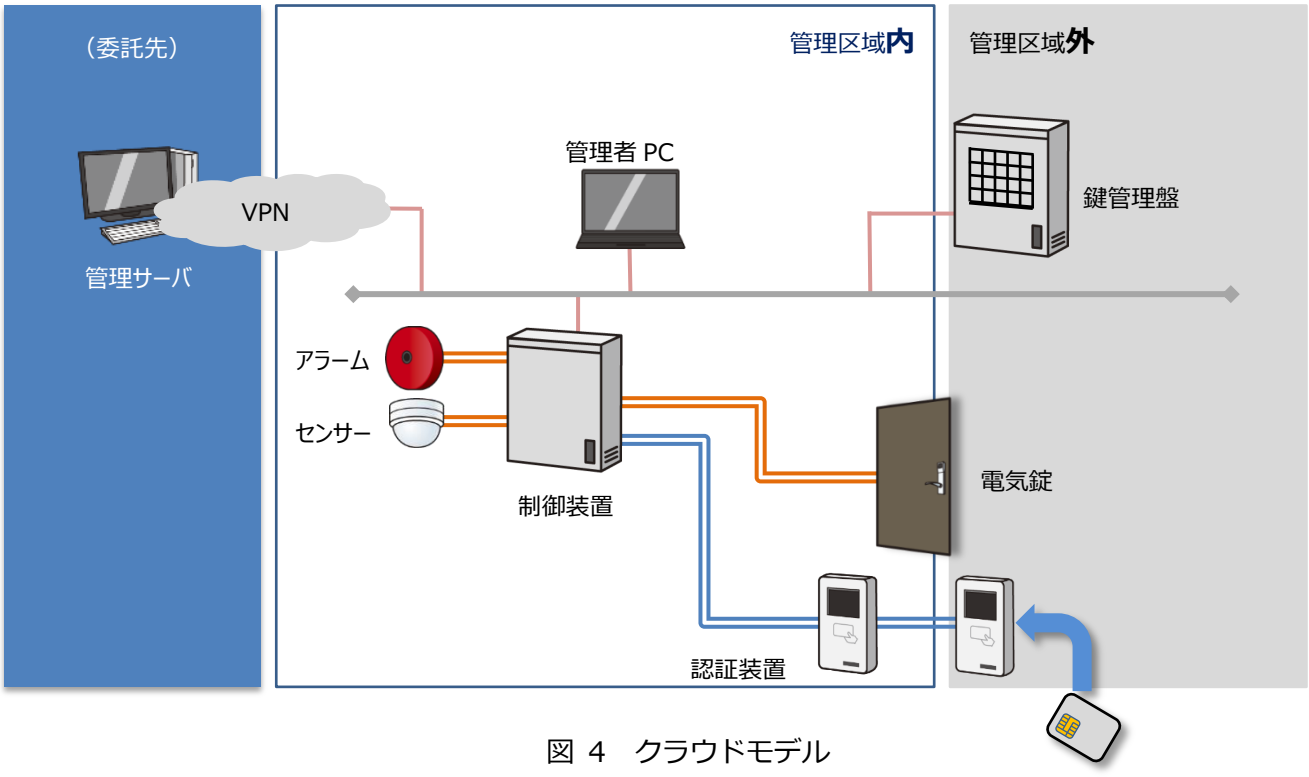


図 4　クラウドモデル

3.2. 前提条件

本書では、以下の役割を定義します。攻撃者として「第三者」と「利用者」を想定します。オペレータは権限内での不正操作のみ脅威として想定します。

役割		想定する攻撃機会
名称	説明	
第三者	入退権限が無く、入退管理システム内のいずれの機器にも正当なアクセス権を所有しない者	管理区域外に設置された機器への物理的な接触 （認証装置、電気錠、及び鍵管理盤）
		ネットワークへの接続 （上記機器に接続されているケーブルへの接触）
利用者	管理者により権限を付与され、入退権限を持つ者 機器の管理機能へのアクセス権は持たない	管理区域内に設置された機器への接触 （第三者が行う攻撃に加え、制御装置に接触可能）
		ネットワークへの接続 （IP ネットワーク線への接触、通信が可能）
オペレータ	管理者より利用者の管理に関する一部管理機能へのアクセス権を付与された者	アクセス権内の利用者の操作（登録、編集、削除） 権限外の操作、接触は行わない
管理者	利用者登録やログ監査等を行う入退管理システムの運用管理者	本書では攻撃者として考慮しない
保守員	ファームウェアのアップデート、アラームの受信を管理者に代行して請け負う者、IoT 機器ベンダや SIer	本書では攻撃者として考慮しない

また、本書では入退管理システムに存在する各種データを以下の通り分類します。

データ		具体例
名称	説明	
保護資産	入退権限に紐づいた利用者の情報や、入退管理システム管理機能へアクセスするためのパスワードや証明書といった漏えいや改ざんが問題となるデータ	ID、ログ
		識別認証情報（ユーザIDとパスワード）、サーバ証明書、暗号鍵
設定・制御データ	管理者や保守員が機器に設定するデータの中で漏えいした時点では問題とならないが、改ざんや再利用されると問題となる場合があるデータ	利用者の入退権限に関する設定値（時刻、扉やゲートの識別子、モード、経路）、監視に関する設定値（ログの設定、アラーム）、IoT や機器の設定値
		電気錠の解錠や施錠、火災などのアラーム、IoT 機器のリブートなどのために生成・発信される制御データ
その他	本書では保護対象としないデータ。人事情報を紐づけるためにシステム外に送信されたデータ、システム外で ID を保持する IC チップ上のデータやその保護のためのデータなど。	

4. チェックリスト

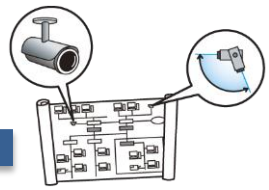
以下の「必須要件」は、2019 年現在の IoT 機器が持つ機能及び導入事例を踏まえた最低限の要件です。スタンドアローンモデルは「a. 必須要件（スタンドアローンモデル）」のみを、統合管理モデル、クラウドモデルは必須要件に加えてそれぞれ「b. 追加要件（統合管理モデル）」、または「c. 追加要件（クラウドモデル）」を追記してください。

全てのモデルにおいて、入退管理システムが他のシステムと接続されている場合、または独立していても利用者が IP ネットワークに接続できる環境の場合は「d. IP ネットワークに接触可能な環境における追加要件」を追加してください。またシステム内の一部に無線 LAN による通信区間が存在する場合は「e.無線 LAN を用いている入退管理システムの追加要件」を追加してください。

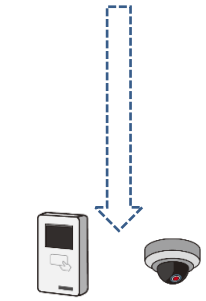
4.1. チェックリストの使い方（調達時の例）

チェックリストは、調達仕様に従ってシステムを構築するシステムインテグレーター（SIer）が参照する要件と、その要件を満たすために SIer が調達する各機器に求める機能性の要件を分けて記載しています。[7] 各機器が単体で機能性を満たせない場合は、他の機器やネットワーク構成で代替してください。

a. 必須要件　（スタンドアローンモデル）			
No.	入退管理システムの基本要件		
	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
a01	【物理的攻撃への対策】 システムを構成する機器は物理的な不正行為を想定した対策をすること	a01-2. 独立した制御装置は管理区域内の利用者が接触困難な場所に設置すること a01-3. 制御線やセンサー線は機器への接続部分も含め壁面等に隠ぺいし敷設すること	■独立した制御装置は管理区域内の EPS など利用者の接触が困難な場所に設置する ■認証装置、制御装置の接続線は壁面から機器まで[redacted]で露出しないよう配線する
a02	【論理的攻撃機会の低減】 サービスの意図しない利用や妨害を防ぐこと	a02-1. IP 線を持つ機器の IP の物理インタフェースはシステムの運用、及び管理操作に必要なサービスのみ動作させ、不要なサービスは全て停止（またはポートを閉鎖）すること a02-2. 接続元を限定できる場合は、接続元の IP アドレス等による制限を行うこと	■[redacted]用に必要なサービス（HTTPS や機器間の通信に使うサービス）のみを許可し、他のサービスは必要なければ停止する ■接続元を限定できる場合は、ソース IP アドレス等による接続元の制限を設定する
a03	【管理者とオペレータの設定】 保護資産や設定データへのアクセスや機器の制御をできる役割を限定すること	a03-1. IP 線から管理操作ができる機器は、保護資産や設定データへのアクセス前に管理者・オペレータを識別認証すること a03-2. 管理者がオペレータのアクセス可能な機能と情報について管理できること a03-3. IP 線に接続される機器は、パスワードを出荷設定値から推測困難な値へ変更すること	■IP 線に接続する機器や管理ソフトウェアでは以下の設定を行う ・ 管理操作の前に識別認証を必須とする設定を行い、適切なアクセス制御の設定を行う ・ 管理者及びオペレータ以外の不要なアカウントは削除する ・ 可能であれば個人毎に異なるユーザ ID で識別する
上記対策要件を満たすためには、下記機能を持つ機器の選定が必要です			
	制御装置の機能要件		
a21	【物理的攻撃への対策】	a21-1. 機器に接続されている全ての線とその接続口、及び USB やシリアルポート等の接続口はケースを閉じた状態では露出しないこと	
a22	【論理的攻撃機会の低減】	a22-1. IP 線では管理者 PC からの接続に用いるサービス以外のサービスは停止できること a22-2. IP 線では IP アドレス等による接続元制限を行う機能を有すること	
a23	【管理者とオペレータの設定】	a23-1. 管理接続時に識別認証を実施できること a23-2. パスワードを出荷設定値から変更する機能があること	



調達者はこの要列を調達仕様の追加要件として SIer に提示する



SIer はこの機能を持つ機器を手配して、要件に従った入退管理システムを設計構築する

図 5　チェックリストの使い方

[7] チェックリストを抜き出した編集可能なシートを以下からダウンロードできます。
https://www.ipa.go.jp/security/jisec/choutatsu/ecs/checklist_ecs.xlsx

4.2. 設計構築フェーズ

設計構築フェーズでは、管理者は以下のセキュリティ対策要件を満たすように、「仕様書へ記述する要件」に記載された事項を情報セキュリティに対する要件として仕様書に転記してください。設計構築の一部を組織が実施する場合は、「組織における対策／運用」を参照してください。

統合管理モデルの場合は以下の必須要件に「b. 追加要件　（統合管理モデル）」を追記してください。

クラウドモデルの場合は以下の必須要件に「c. 追加要件　（クラウドモデル）」を追記してください。

a. 必須要件　（スタンドアローンモデル）			
No.	入退管理システムの基本要件		
	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
a01	【物理的攻撃への対策】 システムを構成する機器は物理的な不正行為を想定した対策をすること	a01-1. 制御装置は管理区域内の利用者が接触困難な場所に設置すること a01-2. 制御線やセンサー線は機器への接続部分も含め壁面等に隠ぺいし敷設すること	■制御装置は管理区域内の EPS など利用者の接触が困難な場所に設置する ■認証装置、制御装置、及び鍵管理盤の接続線は壁面から機器までの間で露出しないよう配線する
a02	【論理的攻撃機会の低減】 サービスの意図しない利用や妨害を防ぐこと	a02-1. IP ネットワークに接続する機器は組織と相談の上、システムの管理や運用に必要なサービスのみ動作させ、不要なサービスは全て停止（またはポートを閉鎖）すること a02-2. 接続元を限定できる場合は、接続元の IP アドレス等による制限を行うこと	■管理サーバ、制御装置、及び鍵管理盤は管理や運用に必要なサービス（HTTPS や機器間の通信に使うサービス）のみを許可し、他のサービスは必要なければ停止する ■接続元を限定できる場合は、ソース IP アドレス等による接続元の制限を設定する
a03	【管理者とオペレータの設定】 保護資産や設定データへのアクセスや機器の制御をできる役割を限定すること	a03-1.管理操作ができる機器は、保護資産や設定データへのアクセス前に管理者・オペレータを識別認証すること a03-2. 管理者がオペレータのアクセス可能な機能と情報について管理できること a03-3. 管理操作ができる機器は、パスワードを出荷設定値から推測困難な値へ変更すること a03-4. 設定可能な機器は、一定回数（5 回程度）の連続した接続試行によるユーザ ID の一定時間のロック、及びパスワードの最低長（8 文字以上）等パスワードの複雑さを上げる設定を行うこと	■管理操作ができる機器や管理サーバでは以下の設定を行う ・ 管理操作の前に識別認証を必須とする設定を行い、適切なアクセス制御の設定を行う ・ 不要なアカウントは削除する ・ 可能であれば個人毎に異なるユーザ ID で識別する ・ 管理者は自身及びオペレータのパスワードを組織の「情報セキュリティ対策基準」に従って設定し、出荷設定値の使用は禁止する ・ 設定可能な場合、一定回数（5 回程度）の連続した接続試行によるユーザ ID の一定時間ロックを有効にする
a04	【不正アクセスの検知】 システムを構成する機器への不正アクセスやなりすましを検知すること	a04-1. システムを構成する機器との通信断を管理者が検知できること a04-2. 制御装置、認証装置、存在する場合は鍵管理盤のケース開けを管理者が検知できること a04-3. 識別認証やシステムからの接続の失敗、及び／または成功を検知し、確認する手段を管理者に提供すること a04-4. 入退、ID 追加などの管理操作、及びセンサーからの通信の履歴を管理者に提供でき	■利用者が接触可能な機器の回線切断、及びケース開け（タンパ―応答）を管理者が検知できる設定とする ■IP 通信を行う機器のログやアラームにおいて識別認証や機器からの接続の失敗、及び／または成功を、管理者が検知できる設定を行う ■入退、ID 追加の管理操作の記録をログに残す設定を行う ■ログの閲覧は必要に応じてオペレータに提供する設定を行っても良いが、ログの削除や設定は管理者

		ること a04-5．システムの時刻は正しく設定でき、構築後に時刻データの変更やズレを管理者が検知できること	に限定する ■管理者はシステムの時刻を正しく設定し、維持する
a05	【既知脆弱性への対応】 システムを構成する機器は公知の脆弱性に対応済みであること	a05-1．IP ネットワークに接続される機器は、機器調達時にベンダから公開されている最新バージョンとすること 構築中に重大な脆弱性が公開された場合は、管理者に相談すること	■システム稼働前に、ベンダの情報を確認し、システムを構成する機器が脆弱性対策を含めた最新のバージョンであることを確認する。
a06	【障害発生への対応】 障害の発生に対する対応が明確であること	a06-1．システムを構成する機器が無応答、もしくはサービス停止した時に、復旧（リブート）する手順を示すこと	■機器の障害発生時に再起動する手順を運用開始前に確認する
上記対策要件を満たすためには、下記機能を持つ機器の選定が必要です			
	制御装置の機能要件		
a21	【物理的攻撃への対策】	a21-1．機器に接続されている全ての接続線とその接続口、及び USB やシリアルポート等の接続口は設置してケースを閉じた状態では露出しないこと	
a22	【論理的攻撃機会の低減】	a22-1．管理者 PC からの接続に用いるサービス以外のサービスは停止できること	
a23	【管理者とオペレータの設定】	a23-1．管理接続時に識別認証を実施できること a23-2．パスワードを出荷設定値から変更する機能があること	
a24	【不正アクセスの検知】	a24-1．管理接続時に認証成功及び／または認証失敗をログやアラームとして出力できること a24-2．ケース開けを検知できること a24-3．認証装置、電気錠との通信断を検知できること a24-4．ID と紐づいた入退や登録／削除を検知できること a24-5．ログは事象発生の時刻とともに記録できること	
a25	【既知脆弱性への対応】	a25-1．動作しているファームウェアのバージョン確認手段が提供されていること	
	認証装置の機能要件		
a31	【物理的攻撃への対策】	a31-1．機器に接続されている全ての接続線とその接続口、及び USB やシリアルポート等の接続口は設置してケースを閉じた状態では露出しないこと	
a32	【不正アクセスの検知】	a32-1．ケース開けを検知できること	

統合管理モデルの場合は以下を必須要件として「a．必須要件　（スタンドアローンモデル）」に以下を追記してください。

b．追加要件　（統合管理モデル）			
	入退管理システムの基本要件		
No.	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
b01	【物理的攻撃への対策】 システムを構成する機器は物理的な不正行為を想定した対策をすること	b01-1．管理サーバは第三者や利用者から物理的に隔離して設置すること b01-2．管理区域外に敷設する IP ネットワークは機器への接続部分も含め壁面等に隠ぺいすること	■組織は管理サーバを入室制限された区域に設置する

上記対策要件を満たすためには、下記機能を持つ機器の選定が必要です		
	管理サーバの機能要件	
b11	【論理的攻撃機会の低減】	b11-1．制御装置や鍵管理盤からの通信に用いるサービス、及び管理者端末からの管理接続に用いるサービス以外は停止できること b11-2．IP アドレス等による接続元制限を行う機能を有すること
b12	【管理者とオペレータの設定】	b12-1．識別認証機能を持ち、少なくても役割単位のアカウントが管理できること b12-2．管理接続時に識別認証を実施できること b12-3．パスワードを出荷設定値から変更する機能があること
b13	【不正アクセスの検知】	b13-1．認証成功及び／または認証失敗をログやアラームとして出力できること b13-2．制御装置、鍵管理盤の通信断を検知できること b13-3．ログは事象発生の時刻とともに記録できること
b14	【既知脆弱性への対応】	b14-1．動作しているファームウェアのバージョン確認手段が提供されていること

クラウドモデルの場合は以下を必須要件として「a．必須要件　（スタンドアローンモデル）」に以下を追記してください。追加される機能要件はありません。

c．追加要件　（クラウドモデル）			
	入退管理システムへの追加要件		
No.	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
c01	【物理的攻撃への対策】 システムを構成する機器は物理的な不正行為を想定した対策をすること	c01-1．VPN 装置は第三者や利用者から物理的に隔離して設置すること c01-2．クラウドサービス業者のデータセンターのセキュリティポリシーが組織のポリシーを満たしていることを示すこと c01-3．管理区域外に敷設する IP ネットワークは機器への接続部分も含め壁面等に隠ぺいすること	■組織は VPN 装置を入室制限された区域に設置する ■クラウドサービス業者のデータセンターのセキュリティポリシーが組織のポリシーを満たしていることを確認する
c02	【論理的攻撃機会の低減】 サービスの意図しない利用や妨害を防ぐこと	c02-1．クラウドサービス上の管理サーバのセキュリティポリシーが組織のポリシーを満たしていることを示すこと	■クラウドサービス業者の管理サーバのセキュリティポリシーが組織のポリシーを満たしていることを確認する

監査のポイント！

- 本システムのセキュリティに関する役割や手順が規定された文書は存在しますか？
- システムの受入れ時に仕様書で定められたセキュリティ要件が満たされていることを確認しましたか？
- システムを構成する機器やソフトウェアにセキュリティ侵害につながる重要な脆弱性が発見された場合、それを認識して修正（を依頼）できるようになっていますか？
- 管理者パスワードは出荷時のものや簡単に推定可能なものを設定していませんか？
- 時刻は正しく設定されていますか？

入退管理システムのネットワークが、他のシステムや基幹ネットワークに接続されている場合、接続されていなくても HUB やケーブルに利用者が接触可能な場合は以下の要件を追加してください。

d. IP ネットワークに接触可能な環境における追加要件			
	入退管理システムへの追加要件		
No.	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
d01	【通信路の保護】 ネットワークを流れるデータを保護すること	d01-1. 保護資産を含む IP 通信は平文で行わないこと d01-2. 可能な場合は IP 通信の確立時に接続先が正しい相手であることを確認すること	■IP ネットワークを流れる通信は暗号化する ・管理接続や保護資産を含む機器間の通信は暗号化される設定にする ・可能な場合は接続時に接続先の証明書を確認する手順を示す
上記対策要件を満たすためには、下記機能を持つ機器の選定が必要です			
	管理サーバの機能要件		
d11	【通信路の保護】	d11-1. HTTPS サーバの機能を持ち、サーバ証明書をインストールする機能を持つこと d11-2. 平文で（暗号化せずに）送信されるログやアラームに保護資産を含まないこと	
	制御装置、鍵管理盤の機能要件		
d21	【通信路の保護】	d21-1. 管理サーバが正しい接続先であることを確認する手段を提供していること（通信手順の中でも可） d21-2. 平文で（暗号化せずに）送信されるログやアラームに保護資産を含まないこと	

入退管理システム内の機器間の通信の一部に無線を利用している場合は、以下の要件も追加してください。

e. 無線 LAN を用いている入退管理システムの追加要件			
	入退管理システムへの追加要件		
No.	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
e01	【無線通信路の保護】 無線 LAN 上のデータの盗聴・改ざんや無線ＬＡＮの不正利用を防ぐこと	e01-1. 無線 LAN の認証・暗号方式は WPA2-AES を使用すること e01-2. SSID は隠ぺいし、可能であれば接続元の MAC アドレス制限を行うこと e01-3. 無線通信 AP のパスワードは推測困難な値を設定すること	■無線 LAN の認証・暗号方式は WPA2-AES を設定する ■SSID は公開しない設定とし、システムの利便性に問題がなければ接続可能な機器を MAC アドレスにより制限する ■無線通信 AP のパスワードは推測困難な値を設定する
上記対策要件を満たすためには、下記機能を持つ機器の選定が必要です			
	管理サーバ、制御装置、鍵管理盤の追加機能要件		
e11	【無線通信路の保護】	e11-1. 無線通信機能を有する場合には、WPA2-AES 方式をサポートすること。 e11-2. 無線通信 AP 機能を有する場合には、SSID の隠ぺい及び MAC アドレスによる接続制限ができること	

監査のポイント！

・　無線 LAN の認証・暗号方式は安全なものを使用していますか？　SSID は公開されていませんか？

4.3. 運用フェーズ

入退管理システムを導入した組織は、下表の「組織における対策／運用」を参照の上、組織の「情報セキュリティ対策基準」に伴うガイダンスや、組織のインシデント対応マニュアルに従い運用してください。運用業務を委託している場合は、組織における対策／運用の項目をそのまま運用の要件に加えてください。

f. 入退管理システム　運用フェーズ必須要件		
No.	入退管理システムの基本要件	
	対策要件	対策方法
		組織における対策／運用
f01	【物理攻撃への対策】 システムを構成する機器は物理的な不正行為を想定した対策をすること	■(f01-1) アラーム（機器間の通信断、ケース開け、電気錠の異常、火災検知）に応じてインシデント対応を行う ■(f01-2) 定期的に機器に物理的な変化が無いかを確認するため、棚卸しを行う
f02	【管理者とオペレータの設定】 保護資産や設定データへのアクセスや機器の制御をできる役割を限定すること	■(f02-1) 機器やソフトウェアで設定したパスワードは、管理者や利用者の変更に伴い、組織の基準や方針に従って（削除、追加、変更など）運用する。必要な場合は利用者への指導を行う
f03	【不正アクセスの検知】 システムを構成する機器への不正アクセスやなりすましを検知すること	■(f03-1) 以下の事象を検知した場合、インシデント対応を行う ・ 連続したログイン試行、覚えのないログイン ・ 大幅な時刻の変更 ・ 不正な ID 登録、削除 ■(f03-2) 定期的にログを監査し、上記以外の不正なアクセスと考えられるログが無いことを確認する ■(f03-3) システムを構成する機器の時刻のズレを補正する
f04	【既知脆弱性への対応】 システムを構成する機器は公知の脆弱性に対応済みであること	■(f04-1) ベンダからの連絡を受けるか、ベンダサイトや公知脆弱性情報によりシステムを構成する機器が該当する脆弱性を確認した場合は、組織の基準や方針に従い脆弱性対応済のソフトウェアへの更新の要否を判断して計画停止時などに対応（を依頼）する
f05	【可用性への対応】 システムが継続的に稼働でき、データ消失から免れること	■(f05-1) 計画停止、及び保守作業を要すると判断した場合は、実施する日時を決めて保守フェーズを実施する ■(f05-2) アラームや管理者の操作により機器のサービス停止を検出した場合で、f01【物理攻撃への対策】または f03【不正アクセスの検知】に該当しない場合は、障害発生時の手順に従って機器の再起動を行う

監査のポイント！

- システムの運用手順書は整備されていますか？　運用業務を委託している場合、セキュリティ対策が適切に運用されていることを確認していますか？
- 定期的な機器の時刻の確認はなされていますか？
- 定期的なログの確認はなされていますか？
- 定期的な公知脆弱性情報の確認はなされていますか？
- インシデントが発生した場合の、対応手順を定めていますか？　インシデントの記録が残っていますか？

4.4. 保守フェーズ

管理者は、入退管理システムの運用を委託する場合は「仕様書へ記述する要件」の要件を仕様書に追記してください。

g. 入退管理システム　保守フェーズ必須要件			
	運用フェーズへの移行に必要な要件		
No.	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
g01	【安全な再稼働】 保守後のシステムは設計された機能が再現できていること	g01-1. 保守フェーズ完了後に、追加（交換）された機器やソフトウェアが更新された製品が設計・構築フェーズの要件通りに設定され接続されたことを確認し、管理者に報告すること	■管理者は保守フェーズの前後で、稼働しているサービスや識別認証情報に相違が無いことを確認し、不備があれば設計構築フェーズに従い設定する（可能な場合はフェーズ前の状態への復旧も検討する）

監査のポイント！

- 保守作業の記録を残していますか？

4.5. 廃棄フェーズ

管理者は、入退管理システムの運用を委託する場合は「仕様書へ記述する要件」の要件を仕様書に追記してください。

h. 入退管理システム　廃棄フェーズ必須要件			
	入退管理システムの基本要件		
No.	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
h01	【安全なデータの廃棄】 廃棄された機器から保護資産が漏えいしないこと	h01-1. 保護資産が格納されている機器をリースやレンタルから返却、または廃棄する場合には復元不可能な方法で消去し、かつデータ消去の証明書を発行すること	■管理者はリースやレンタルから返却時または廃棄時、機器に格納された保護資産を論理的に消去すること ■組織はリース返却した機器の保護資産が全て安全に廃棄されたことをデータ消去証明書にて確認する

監査のポイント！

- リースやレンタルからの返却時あるいは廃棄時のデータ処理手順が存在し、実施記録がありますか？

5. 付録

5.1. 想定する脅威について

本書のチェックリストにおいて対策を講じた入退管理システムの主な脅威は以下となります。

・機器のケース開けや切断

攻撃者が不正に入退するためには入退権限のある ID を入手するか電気錠を解錠することが考えられます。

認証装置はドアやゲートの横に設置されるため誰でも触ることができます。装置の取り外しや、ケース開けにより、制御線に推測した ID を流す[8]ことができれば電気錠を開けることができます。

鍵管理盤や制御装置は ID の一覧を保持し、ケースを開ければ他の機器と通信を行うことができます。また装置内の端子に電圧をかければ電気錠を回すことが可能です。

通信の暗号化や機器内のデータの保護が一般的ではない機器では、ケース開けや機器の切断を管理者が検知できることが重要です。【必須要件】[a01,a04]にて対応します。

・管理操作のアクセス権の取得

入退管理システムは、他のシステムとの連携や配線の都合で基幹ネットワークに接続される場合があります。攻撃者は管理サーバや制御装置の管理機能にアクセスしてデフォルトパスワードや、辞書攻撃を行って識別認証機能の突破を試みます。【必須要件】[a03]にて対応します。IP ネットワークの盗聴による管理接続のパスワード漏えいが懸念される場合は【選択要件】[d01]にて対応します。

・デフォルトサービスの利用

一部の IoT 機器では、通常の運用時に必要としないサービスが開いている場合があります。攻撃者は公開されているそれらのサービスの識別認証情報を用いて、管理機能や機器の OS へのアクセスを試みます。【必須要件】[a02] にて対応します。

・公知脆弱性の利用

公知脆弱性の中には上記対策では防げない攻撃があります。例えば管理用 Web サイトの不備を悪用して、攻撃者はログイン画面を迂回したり工場出荷時のパスワードに戻すことによって、管理機能を奪うことができます。【必須要件】[a05]、[f04]で対応しますが、ベンダとの調整を要する保守には時間を要するため、可能な機器は【必須要件】[a02]により接続元を限定してください。

本書は、IoT 機器を標的としたマルウェアへの感染や公知脆弱性の悪用、入退管理システムや制御用の通信の性質上発生する問題に、一定の対策を行うことを目的として、2018 年度時点で入手可能な機器が実装している機能を適切に設定し、運用することを要件としています。攻撃者がリスクを負う攻撃や、長い時間を要するような高度な攻撃への対策は含めていません。

8 攻撃には認証装置と制御装置間の通信フォーマットの理解を要します。

5.2. 用語集

本書で使用している主な用語を解説します。

EPS ： ビルや建物の内部にある電気設備の配管を通す区画です。管理区域内から出入りできます

HTTPS ： 暗号化して Web ページの情報をやりとりするプロトコルです。入退管理では ID 管理の登録・削除設やログの確認に利用します。システム内で対応している最新のバージョンと強固なアルゴリズムに限定します

ID ： 本書では入退する利用者を識別するための値です。指紋の特徴点も含みます

MAC アドレス ： IP ネットワークの接続口単位で持つ固有の値です。無線 LAN の接続元制限として補助的に利用される値ですが、詐称可能です

MAC 認証 ： Message Authentication Code （メッセージ認証コード）メッセージの受信者と事前に共有した暗号鍵と送付するメッセージの両方を使って計算した値を使った認証方式です。

SSID ： 無線 LAN のアクセスポイントを識別する値です。任意に設定することができるため、正しい SSID であれば正しいアクセスポイントであるとは言えません

VPN ： 仮想的な閉域網です。本書では VPN は閉域網と同等に扱います

VPN 装置 ： VPN を構築する機器です。上記の前提のために、装置は入室制限された部屋に設置され、インターネット側のネットワーク回線からの装置の管理はできないこととします

アクセス権 ： 識別認証された後の管理者や利用者に付与する権限です。識別認証される前は一般的に「ログイン画面」へのアクセス権しかありません

アラーム ： いたずらや不正アクセスを検知した際のメッセージです。管理者へのメール送信や画面上への表示など通知方法はシステムに合わせて設定します

暗号鍵 ： 暗号化されたデータを復号する際の計算に用いる値です

管理区域（内／外） ： 入退管理システムにより権限を付与された利用者のみが入れる物理的な区域を管理区域内、その外側を管理区域外とします。伴連れや、ゲートの飛び越え、扉の破壊は本書では考慮しません

基幹ネットワーク ： 組織から許可された特定の第三者が組織の制限に従って接続しているネットワークです。そのため、組織内の第三者からの攻撃を受けます

ケース開け ： 機器が保存している保護資産を物理的に保護しているカバーや蓋を開けること。一般的な制御装置や認証装置は、ケース開けに対してログやアラームを流すタンパ―応答の機能を持ちます

サーバ証明書 ： HTTPS サーバには必ず存在する値で、暗号鍵とその持ち主の情報が含まれています。サーバ自体で作成することも、外で作成したものをインストールすることもできます

サービス ： ネットワーク経由で提供するサーバ機能で、ポート番号（HTTP であれば 80 番、UPnP であれば 81 番など）を持ちます。不要なサービスは全て止めます

識別認証 ： 管理者や利用者の役割ごとに、本当にその人物かを、その人物しか知り得ない情報（ユーザ ID とパスワードの組み合わせ）を用いて確認することです

識別認証情報 ： 本書では、識別認証に用いるユーザ ID とパスワードの値のことです

制御線 ： IP 通信ではない独自のプロトコルによる通信線です。一般的にシリアル通信のため電圧から信号を読み取ることが可能です

センサー線 ： 通電しているか否かの ON/OFF 判断のみの電線です。電気錠への線も該当します

ハブ（HUB） ： 複数のネットワーク回線を接続することにより、お互いの通信を可能とする機器です

ログ ： ID の登録や削除、ログインに成功や失敗した際に残る記録です。この記録を元にアラームを送る設定をします

著作・制作	独立行政法人情報処理推進機構（IPA）
編集責任	山里 拓己
イラスト制作	株式会社 創樹
執筆協力者	入退管理システムセキュリティ要件検討ワーキンググループ 手塚 悟　大久保 隆夫　吉岡 克成 根本 直樹　福田 次郎　稲生 秀和 三宅 敏之　小川 信吾　前田 卓志 河合 洋亮 内閣官房 内閣サイバーセキュリティセンター 総務省 サイバーセキュリティ統括官室 経済産業省 商務情報政策局 サイバーセキュリティ課 JPCERT コーディネーションセンター 横浜市
IPA 執筆者	飛田 孝幸

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

2019年5月7日　第1版発行

[事務局・発行]　独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目28番8号

文京グリーンコートセンターオフィス

https://www.ipa.go.jp/security/jisec/choutatsu/


セキュアな
製品調達のために