プレスリリース
2019 年 5 月 20 日
独立行政法人情報処理推進機構

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を公開

～ 調達仕様書に記述すべき要件が明記されており、民間組織でも活用可能 ～

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）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（以下、政府統一基準）」の要件に従い、入退管理システムの調達者が情報セキュリティ上の要件や対策を確認するための「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」を公開しました。

家電や自動車、事務機器をはじめとした様々な機器がインターネットに接続するモノのインターネット（IoT）が普及するなか、IoT 機器にも適切なセキュリティ対策を講じることが重要となっています。ビルや工場の物理セキュリティを担う入退管理システムは、複数の扉やゲートに設置された機器がネットワーク経由で統合管理されています。また、勤怠管理などの社内システムと接続されるケースもあります。そのため、「政府統一基準」において情報セキュリティ対策が必要とされる IoT 機器を含む特定用途機器に指定されています。

そこで、IPA はより安全な国民サービスを提供するための政府調達推進の一環として、「入退管理システム」の機能と運用におけるセキュリティ上の対策を確認できるチェックリストを公開しました。これは、2017 年 12 月に公開した「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」に続くものです。

本チェックリストで要件を示している機器等は以下の通りです。

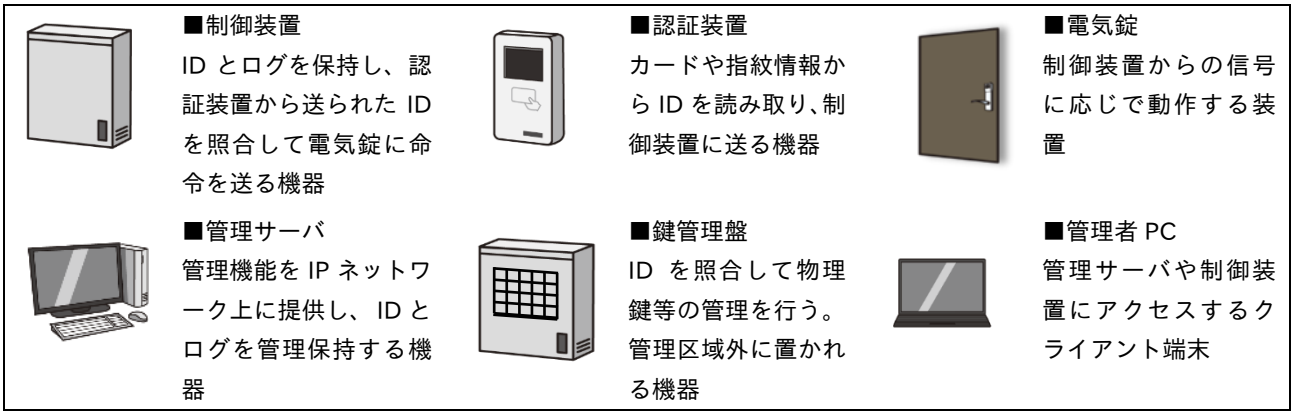

図 1：対象とする機器等

要件の策定にあたっては、既存の入退管理システムに関わる警備会社やベンダー等の協力のもと、情報セキュリティに関する機能の実態調査を行い、①保護すべきデータや想定される脅威の分析、②脅威への対策の洗い出し、③委員会 (*1) による対策の具体的な要件化を行いました。

(*1) 入退管理システムセキュリティ要件検討 WG：政府機関や自治体の調達者、有識者、警備会社、及びベンダーで構成。

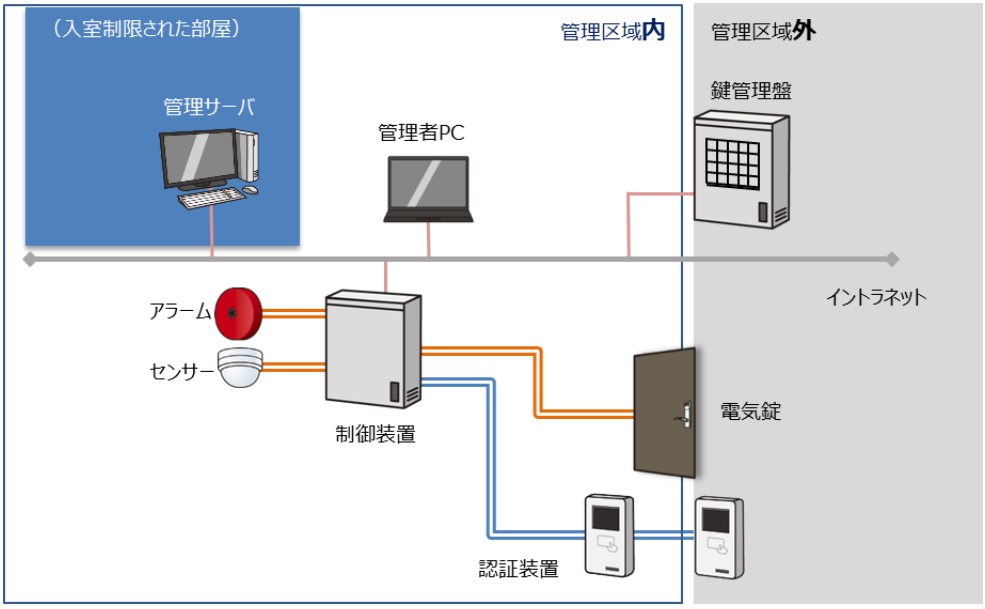

図２：対象とするネットワーク構成の一例

本チェックリストは、設計構築・運用・保守・廃棄といったフェーズ毎に構成され、それぞれ仕様書へ記述すべき要件と組織における対策・運用方法が明記されているため、政府組織に限らず自治体や民間組織においても調達仕様の策定時や日常の運用における情報セキュリティ向上に役立てることができます。例えば「不正アクセスの検知」という要件に対し、「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」といった仕様書に適した形式での記述とともに、「機器の回線切断およびケース開けを管理者が検知できる設定とする」といった対策などを示しています。（別紙１：要件表記の一例）

なお、本チェックリストは、製品のセキュリティ機能の向上や、攻撃手法の変化に伴い更新する予定です。調達時には以下の URL からダウンロードし、最新のチェックリストを利用してください。
https://www.ipa.go.jp/security/jisec/choutatsu/ecs/index.html

IPA では、今後も IT 製品の安全な政府調達のための情報提供を行っていきます。

■本件に関するお問い合わせ先
IPA セキュリティセンター セキュリティ技術評価部　飛田／山里
Tel: 03-5978-7538　Fax: 03-5978-7548　E-mail: jisec-proc@ipa.go.jp
■報道関係からのお問い合わせ先
IPA 戦略企画部 広報戦略グループ　伊藤／白石
Tel: 03-5978-7503　Fax:03-5978-7510　E-mail: pr-inq@ipa.go.jp