

ビルネットワークにおけるセキュリティ連携システムの開発(1) -セキュリティ構築プラットフォームの開発-

三浦健次郎† 金子洋介† 奥村誠司† 桑原直樹‡ 林鋭志‡ 北上眞二†

三菱電機株式会社 †情報技術総合研究所/‡先端技術総合研究所

1. はじめに

社会のセキュリティ管理意識の高まりから、オフィスビル、研究所、工場などでは、外部からの不正侵入を防ぐために、IC カード、指紋認証等による入退管理システム(物理セキュリティ)の導入がすすんでいる。さらに、入退室管理システムに入退場者の映像を監視・記録する映像監視システム(映像セキュリティ)を組み合わせたセキュリティシステムの導入も増加しつつある。

一方、情報システムについては 2000 年頃から、情報セキュリティの管理を強化するため、業務 PC 端末や組織内の Web システム利用を制御するための統合認証システムの導入が進んだ。

しかし、上記の物理セキュリティシステム、映像セキュリティシステム、情報システムは別々に開発されてきたため、各システム間の連携機能の開発にはコストや時間がかかるという課題があった。

近年、組織内への人の出入りと機密情報を統合的に管理したいという要求が多くなってきており、これにこたえるため、上記システムを連携させるためのプラットフォームを開発した。

本稿では、開発したセキュリティシステム構築用プラットフォームの基本アーキテクチャ、機能等について概説する。

2. セキュリティ連携システム

まず、図 1 に想定する連携システムとプラットフォームの全体概要図を示す。プラットフォームを中心に連携させるサブシステムとしては物理セキュリティ、映像セキュリティのセキュリティシステムに情報システムを加えた 3 つをコアサブシステムとして想定している。

これらのサブシステムを連携させる複合型のシステムとして、物理/情報連携システム、物理/映像連携システムを想定している。

実際に、物理/情報連携システムとして①情報システムの(出張)ワークフローの申請・承

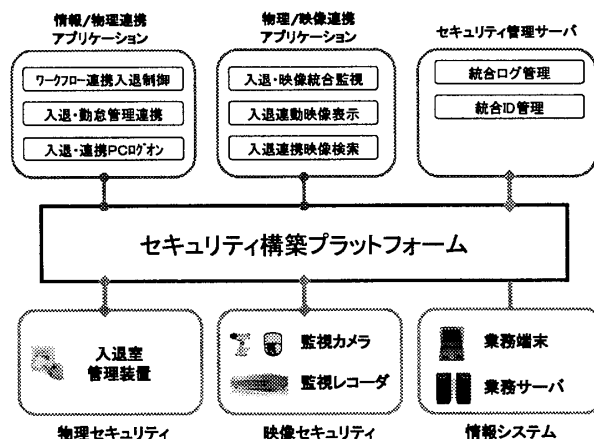


図 1 連携システム概念図

認に連動した入退室管理システム、②入退室管理装置内の出退勤・通行履歴を出勤・退勤時間としてとりこむ勤怠連携システム、③入退室管理装置に連動した業務端末のログオン制御システム等を連携システムとして開発した。

物理・映像連携システムについては、入退室イベントに連動させた監視映像の記録、入退ログからの記録映像の検索機能等の複合型連携機能を強化した統合監視アプリケーションを開発した。

さらに、システム連携で必要となる共通機能を提供するサーバ群も開発した。具体的には、各サブシステムのログ、記録画像を統合的に蓄積し、監査・横断検索を実現する統合ログ管理サーバ、情報システムのユーザ ID と入退室管理装置のカード ID 等を統合的に管理・連携させる統合 ID 管理サーバなどである。

上記システムの具体的な連携機能については連続するセッションで解説するので参照されたい。

3. セキュリティ構築プラットフォーム

次に 2. で説明した連携システムを効率よく構築するための連携プラットフォームについて述べる。プラットフォームは以下のような機能をもつ。

The Integrated Security System on Building Network (1)
- Security Systems Development & Runtime Platform-
†Kenjiro Miura, Yosuke Kaneko, Seiji Okumura, Shinji Kitagami:
Information Technology R&D Center, Mitsubishi Electric Corporation
‡ Naoki Kuwahara, Eiji Hayashi: Advanced Technology
R&D Center, Mitsubishi Electric Corporation

(1)セキュリティ連携システム構築用 API

まずプラットフォーム基本機能として、セキュリティ連携システム構築に必要な API 及びランタイムライブラリを開発した。図2に示すように API は、入退出管理装置、監視カメラ・レコーダ、統合ログ管理サーバ等のサーバ用の API 及び共通 API からなる。共通 API は機器構成管理、通信処理等の機能を持ち、設定により各セキュリティ機器用の通信プロトコルドライバを動的に切り替える。

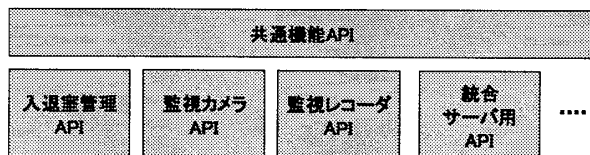


図2 セキュリティ連携 API 概要図

表2に機能セット一覧を示す。

表2. セキュリティ連携API 機能セット一覧

	入退管理	映像カメラ・レコーダ	統合サーバ (ログ/ID)
イベント通知	○	—	—
権限変更	○	—	—
収集・保存	○	○	○
検索	○	○	○
表示/再生	○	○	○

API はオブジェクト指向設計により各セキュリティ機器の抽象化を行い、構成や機能の差異を吸収した。ここで構成の差異とは、例えば、アナログ型カメラの制御はネットワーク接続されたレコーダを通じて間接的に行うが、デジタルネットワークカメラの場合は直接制御する等の通信対象の違いである。このために内部では機器を識別する識別 ID と”関連”を保持している。

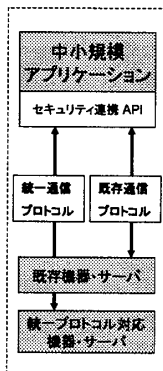
(2)連携システム通信機能

プラットフォームの通信機能については順次統一を進めているところである。ここで通信機能の統一においては、次のように幾つか考慮すべき点がある。

①既存製品との互換性

セキュリティシステムは販売済のシステムも多く、既存セキュリティ機器（入退制御盤、カメラ、レコーダなど）との互換性は確保する必要がある。一方、既存セキュリティ製品の通信プロトコルは LAN 上での利用を想定したものと

①パッケージ型開発



②大規模システム開発

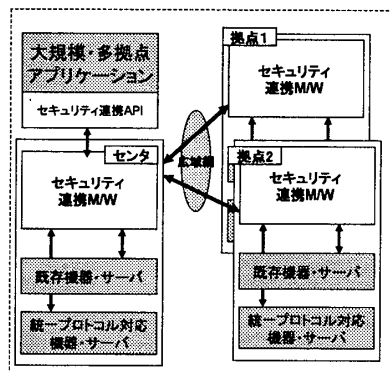


図3. 想定連携システムアーキテクチャ

なっているため、広域網での遠隔監視用途の利用も考慮し、Web サービスベースの (XML-RPC etc) プロトコルを機器側の開発スケジュールにあわせて開発している。なお、接続機器に合わせてプロトコルドライバの設定を切り替えることにより新たなプロトコルに対応することができるのは前述の通りである。

②システム規模対応

セキュリティシステム開発は、図3に示すように中小規模を想定したパッケージ型のセキュリティ連携製品開発と、大規模、顧客情報システムにあわせたカスタマイズシステム開発があり、いずれにも対応できるようにする必要がある。

前者の製品開発はシステム規模が小さいため、図3①のような2層構成のシステムアーキテクチャで開発する。一方、顧客の人事情報システムとの連携等を考慮した大規模なセキュリティシステム開発では、図3②のように情報システムと密接に連携する必要がある。このために標準通信プロトコル（共有ファイル、JMS、HTTP、etc）で顧客情報システムと情報交換/データ変換をするための SOA 型ミドルウェア (G/W) をシステム構築用に利用する。

4. まとめと今後の課題

本稿ではセキュリティシステム、情報システムを連携させるプラットフォームについて概説した。今後は遠隔通信やセキュリティ機能の強化とともに、ビル設備システム（空調・照明等）との連携強化開発も行っていく予定である。参考文献

[1] 原田 篤史, 他:ビルネットワークにおけるセキュリティ連携システムの開発(2)ー物理・情報連携システムの構築ー, 第70回情報処理学会 全国大会講演論文集(予定), Mar 2008