〔２．建築における ICT 技術〕

建物の入退室管理システムにおける技術動向と運用例

安 田 直 明
NAOAKI YASUDA
（アズビル㈱*1 ビルシステムカンパニー セキュリティ・システム本部企画部
企画グループ グループマネージャ）

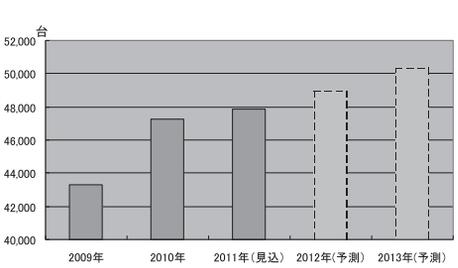
はじめに

近年，建物用途を問わず入退室管理システムが設計・導入されている。10年ほど前までは，金融機関や研究所，データセンターなど機密情報や重要情報を多く所有している企業／業種に導入されるのが主であった。その後，同時多発テロなどの事件や個人情報保護法，日本版SOX法などの法整備の社会的変化も受けて，テナント誘致を有利にするためにビルの付加価値を上げる目的で，テナントビルを中心に入退室管理システムが導入されてきた。最近ではテナントビルだけではなく，自社ビル，工場，病院，福祉施設，大学，百貨店などあらゆる建物に導入されてきており，その件数も年々増加傾向にある（**図－１**）。ここでは，セキュリティシステムの主となっている入退室管理システムに関して，システム内の通信方式や暗号化技術，ここ数年ニーズが高まっている多拠点管理の運用とその事例について解説する。

１．入退室管理システムにおける通信方式

１．１　システム構成

入退室管理システムの一般的なシステム構成は，**図－２**のようになる。一般的な機器構成は，出入ユーザ（カードデータ）や出入履歴など，システムにとって最も重要な情報の管理を行うサーバ（セキュリティ・データ・サーバ），ドアやカードリーダ，電気錠，防犯センサなどの状態監視や警報監視などを行う監視機能サーバ（システム・マネジメント・サーバ），これらサーバ群を操作／管理するための監視用PC（複数台設置可能），カードリーダや電気錠，防犯センサ，鍵管理ボックス，フラッパーゲート（自動改札に似た開閉ゲート）などの制御を行う制御装置（アクセス・コア・コントローラ），所有しているカードデータが正常か否かを判別するカードリーダである。各構成機器は専用線で接続されており，定められた通信プロトコルで通信を行っている。

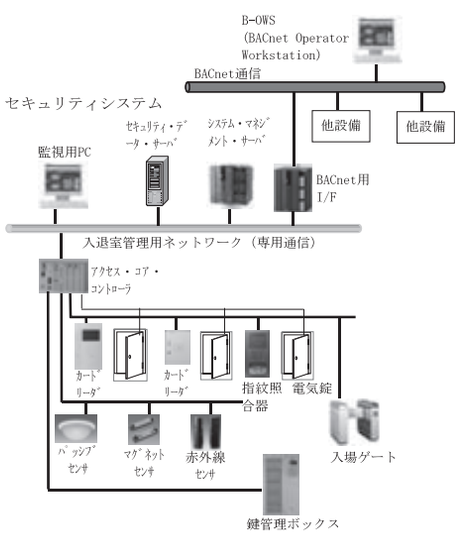


図－１　カードリーダ出荷台数推移

１．２　入退室管理システムの通信方式

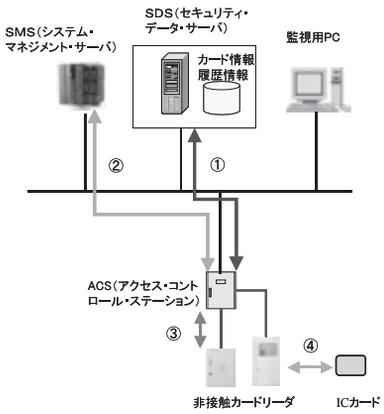
入退室管理システムの通信方式は，ベンダーごとに独自プロトコルを構築しているケースがほとんどである。その背景としては，空調設備や電気・衛生設備などと比べて，通信上を流れるデータの機密性が高いためである。他設備の場合，流れるデータの種類は機器の発停信号や警報信号，状態信号などであるが，セキュリティシステムの場合は，個人を識別するカード情報や氏名などの個人情報，電気錠の施解錠信号などが流れる。これらの情報や信号は，万一ネットワーク盗聴などで情報が漏れた場合に，カードの偽造や扉への不正アクセスなどに繋がる危険性がある。

よってベンダー独自の通信方式を採用し非公開とすることで，ネットワーク盗聴や不正アクセスなどからネットワーク上を流れるセキュリティ情報の機密性を保っている。参考までに，弊社入退室管理システムにおける，



図－２　入退室管理システム構成図

＊１　2012年４月１日，㈱山武 は アズビル㈱へ社名を変更しました。



図－3　デバイス間通信例

表－1　デバイス間通信仕様

対象モジュール	通信方式など
① SDS⇔ACS間	・独自プロトコル ・伝送されるカードデータ（カード内個人データ）は暗号化
② SMS⇔ACS間	・独自プロトコル ・データフォーマットは非公開
③ACS⇔カードリーダ間	・独自プロトコル ・データフォーマットは非公開
④カードリーダ⇔ ICカード間	後述

各デバイス（モジュール）間の通信仕様を記述する（**図－3**，**表－1**）。

1．3　オープン化プロトコル（BACnet（IEIEJ-G-006：2006））

図－2において，他設備と連携（警備状態に連動した他設備の発停／停止，防災信号受信による電気錠の解錠や空調設備の停止など）する場合，各ベンダーの専用プロトコル同士ではフォーマットを合わせるなどのI/F機能が必要となる。現場ごとに多くの設備とフォーマットを取決めしていたのでは，工数や手間が多大にかかってしまう。このようなケースでは，共通化されたプロトコルを使用して連携を構築する。それがBACnet（Building Automation and Control Networking protocol）通信プロトコルである。

BACnetの利点は，マルチベンダー対応を実現するための「オープンな」通信プロトコルであり，文字通り伝送されるメッセージ仕様が公開されているため，事前打合せや設備ごとのI/Fを用意するなどが不要になることであるが，一方，カード情報や電気錠の施解錠操作など，漏洩するとセキュリティ上問題となりうる可能性も含んでいる。よって，入退室管理システムのようなセキュリティシステムでは，共通プロトコルで通信することは望ましいとは言えない。IEIEJ-G-0006：2006はあくまで「ガイドライン」であり，自システム内の通信においても適用を強制するものではないため，「他社デバイスとの通信を妨げない」という前提のもと，自システム内の通信は各社独自の通信仕様を使用することでリスク回避が可能である。

表－2　現行FeliCaと新FeliCaの認証方式と暗号方式の比較

	現行FeliCaカード	新FeliCaカード
カードリーダ（リーダ／ライタ）との相互認証方式	2-key Triple DES（鍵長112ビット）	2-key Triple DES（鍵長112ビット）あるいはAES（鍵長128ビット）
通信路の暗号化方式	DES暗号方式	DES暗号方式あるいはAES暗号方式

1．4　非接触ICカードとカードリーダ間の情報の暗号化

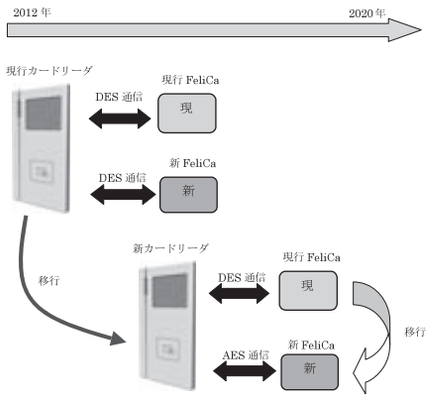
国内で最も多く利用されている非接触ICカードは，FeliCaチップ*2が搭載されたICカードである。入手がし易いことや利用範囲が広いこと，携帯電話にも搭載されていることなどから生活にも密着しており，入退室管理システムにおいても大多数でFeliCaカードが使用されている。

カードにアクセスして入退室情報を読み出す際，システムコードとサービスコードを指定してデータ領域にアクセスすることになるが，さらに暗号鍵を設定して情報漏洩を防ぐことも可能である。現在のFeliCaでは，カードリーダとの相互認証方式に鍵長112ビットの2-key Triple DES（Data Encryption Standard）を，通信路の暗号化にDES暗号方式を採用している。しかし，NIST（米国立標準技術研究所）が，容易に解読される暗号技術の使用を2010年に停止する方針を発表したことをきっかけに，前述の方式が停止対象になったことからFeliCaにおいても暗号方式の見直しが行われている。

具体的には新FeliCaチップは，カードリーダとの相互認証方式に鍵長112ビットの2-key Triple DESあるいは鍵長128ビットAES（Advanced Encryption Standard）を，通信路の暗号化にDES暗号方式あるいはAES暗号方式を採用する（**表－2**）。これにより，認証と暗号のセキュリティ性を向上させて，なりすましや盗聴の防止がより強化される。

この新チップは2012年夏よりサンプル版が提供される予定で，2019年までは移行期間として新旧カードが共存しているが，2020年以降は新カードのみの運用になる予定である。2012年～2019年までの移行期間中については，新旧カードならびに新旧のカードリーダが共存しているわけだが，各ベンダーのカードリーダ（リーダ／ライタ）がすぐには新カードに対応できないため，現行のカードリーダでは，現行カード／新カードともDES通信を行う。一方，カードリーダがAESに対応したのちは，現行カードとはDES通信で，新カードとはAES通信を行う（**図－4**）。さらに移行期間終了後，カード内にDES通信機能が残存しているとセキュリティ性が向上したとは言いがたいため，カードリーダ（リーダ／ライタ）からカードに対してDES

＊2　FeliCa：ソニー㈱の登録商標。



図－4　新旧リーダと新旧カードの暗号通信方法

を停止するコマンドを発行して，DES通信機能を停止することが可能で，AES通信のみに切替えることができる。

1．5　生体認証データの暗号化

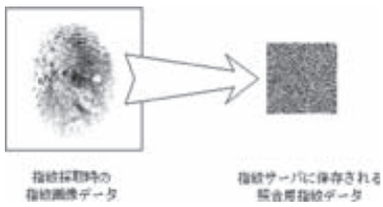
入退室管理システムでは，多くの場合は非接触ICカードリーダが扉付近に設置されてICカードによる入退室が行われるが，サーバルームや機密保管庫，危険物保管室などの重要または危険な居室においては，指紋や静脈，顔といった生体を使った認証装置が設置されるケースが多い。生体認証装置の大きなメリットは，カードなどの物理的な識別デバイスを携帯しなくてよいことである。本人の「体」の一部が識別デバイス代わりとなるため，紛失や盗難のリスクがほとんど無い。

この生体情報は「個人情報」そのものであるため，カード情報と比べて取扱いやデータ伝送に注意を払わなければならない。そのために，生体データを個人を特定する照合に使用する場合は，データを暗号化する必要がある。弊社の指紋照合装置の例でいうと，登録される指紋データは，指紋の画像データそのものではなく，フーリエ変換を用いて位相化し，暗号的に圧縮したバイナリデータである。指紋データそのものを指紋のイメージで表示認識することはできない。これにより，指紋を登録したユーザのプライバシーへの配慮と，万が一指紋データが盗難にあった場合でも，指紋画像として表示認識できないため，なりすましで認証されることも防止できる（**図－5**）。

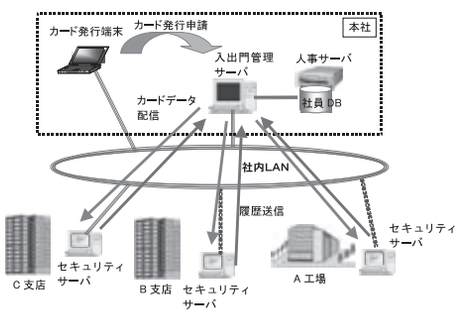
2．多拠点管理によるユーザ情報／入退場履歴の一元管理とその運用例

2．1　多拠点管理

多くの支店や営業所，工場などを所有する企業では，事業所ごとに入退室管理システムを導入しているが，ユーザ情報管理や入退室履歴管理は事業所ごとの対応となっていることが多く，管理や作業が手間となっている。これを解決するために，人事・総務系の部署では，各拠点のユーザ通行許可設定や通行履歴の収集を本社などで一元管理することで，勤怠管理システムと連携したり，従業員の健康管理やBCP（Business Continuity Plan：



図－5　照合用指紋データのイメージ



図－6　多拠点管理のシステム構成例

事業継続計画）対策などに活用したりできる。このように各拠点のユーザ情報や履歴管理を一元管理する多拠点管理は，労働基準法が平成22年４月１日に改正されたことを受けて，時間外労働や社員の健康管理を適正に管理していく上でも注目されている。

2．2　システム構成

多拠点管理のシステム構成は，各拠点を社内LANなどのネットワークで接続し，本社の入出門管理サーバと拠点の入退室管理システムとの間でデータの送受信が行えるように構成する。情報は，本社の入出門管理サーバからカード情報の配信を行い，また各拠点からは入退室履歴情報を取得して一元管理を行う（**図－6**）。

2．3　入退場履歴の活用

社員がいつ出社し，いつ退社したかを知るためには，入退室用のカードリーダの一部を出退勤専用にすることで，必要な履歴のみを抽出することができる。そのデータは次の用途で活用できる。

⑴　労働時間の適正管理

各自が申請する勤怠データと入退場データを比較し，大幅な時間の乖離があった場合などに状況確認をすることで，サービス残業の防止や不要な残留者の把握などを行うことができる。たとえば，履歴上の退場時刻が20：00であるにもかかわらず勤怠上は18：00までの勤務と申請している場合は，サービス残業の可能性がある。

⑵　深夜在館者の管理

指定した時刻以降に在館している人だけをリストアップすることで，申請せずに在館している人や，事故や急病等で動けなくなっている人がいないかなどの確認／管理を行うことができる。

⑶　在館者の安全管理

BCP対策として，有事の際の在館状況把握や災害時の

非難状況の確認などを，その時点での在館者リストを出力することで管理を行うことができる。また，来訪者管理システムと連携することで，来訪者に貸出した来訪者用カードの履歴を収集することにより，社員と同様に有事の際の在館情報をBCP対策として活用できる。

2．4　多拠点管理の運用例

多拠点管理の運用例として，弊社で実施しているユーザ情報と入退場履歴の一元管理を紹介する。

弊社では，入退室管理システムとして各事業所（支店含）にsavic-netFXセキュリティシステム*3を導入している。ユーザ情報（カード情報）は本社総務部門で行い，カード管理端末からカードの追加／変更／削除を行うと，入出門管理サーバに申請情報が反映される。この入出門管理サーバから各拠点のセキュリティサーバに，通行許可情報が１日１回自動展開される。この方法により，たとえば本社勤務の社員が出張で関西支社に行った場合でも，入室許可情報が支社に展開されているため，日常使用しているセキュリティカードで入室することができるようになる。

また，社員の出退勤履歴情報は，各拠点のセキュリティサーバで取得した履歴情報を，１日１回入出門管理サーバに自動送信されるので，勤怠管理システムと連携することで，この出退勤履歴情報を個人の勤怠画面で確認することが可能となる。さらに，午前中は本社勤務，午後は移動して近隣事業所勤務という場合でも，その事業所に何時に出社し何時に退社したかを履歴として反映している。

具体的な運用例として弊社藤沢事業所での事例を紹介する。

ここでは，入退場門付近にカードリーダを設置し，入退場時にカードをかざすことで出勤と退勤時間を把握している。（**写真－１～写真－３**）。

また，入場できる対象者の登録は，図－６にあるように，本社にある入出門管理サーバから変更が発生した差分情報が，社内LAN経由で毎日深夜に藤沢のセキュリティサーバに配信される。一方，入出門ポールの通行履歴は，毎日深夜に本社の入出門管理サーバに送信され，勤怠管理システムに個人ごとの参考データとして反映される。

３．今後のセキュリティシステムの方向性

非接触ICカードが主流となっている現在ではあるが，今後の認証デバイスとしては，ICカードの代わりに無線タグを所有し，人がゲートに近づいたときに入室権限を確認し入退室が可能となったり，あるいは人体通信による入退室管理が普及してくる。さらに，人だけではなく物（PC，医療機器，書類等）にID情報を持たせて，位置情報管理（ロケーション管理）を使った物品管理も注目される。

また，セキュリティ情報を使った，今までとは異なった他設備機器との連携による省エネ／節電も考えられる。たとえば，執務しているエリアの人数カウント（在／不在情報含）を行うことにより，人数に合わせた空調や照明の制御（暑く／寒く，明るく／暗くなど）やOA機器の入／切（手元の電気スタンドやコンセントなど）が求められてくる。また在／不在情報はID情報のみならず，映像情報によりそのエリアに何人在室しているかを解析して，設備機器と連携する運用も実現性が高まってくる。ユビキタス社会が広まってくるのに合わせて，セキュリティシステム側も技術動向に追従していくことが必要となる。

写真－１　人用ポール

（拡大）

写真－２　車両用ポール

写真－３　バス乗降用ポール

おわりに

セキュリティシステムであるが故に，システムで取り扱っている情報はデリケートなものが多い。機器間でやり取りしている情報は，漏洩してはならないという機密性が重要であり，かつ改ざんされてはならないというデータの完全性も求められる。加えて，可用性が保てなければ入室／退室ができないなどの運用上の不具合を発生させてしまう。それゆえに，他設備に比べて通信技術を含めたセキュアなシステム構築が重要になる。今後新しい技術が採用された場合でも，セキュリティシステムに求められる安全性は，常に考慮していかねばならない。

参考文献

１）黒川，月刊CardWave Jul-Aug 2011 Pick up Topics p28-29

２）2011セキュリティ関連市場の将来展望，富士経済

３）竹中，中島，新フレンドタッチ入退室統合システムにおけるアーキテクチャと照合技術，SavemationReview 2004

４）安田，オフィス，工場のセキュリティシステム動向，月刊「建築設備と配管工事」2009年

（平成23年12月26日　原稿受理）

＊3　savic-net：アズビル㈱の登録商標。