技術解説

出入管理システムの運用面から見た課題とその解決策

株式会社アート 技術センター　技術本部 開発部　部長　田村　和寛

この度の東日本大震災におきまして被災された皆様に心よりお見舞い申し上げますと共に、一日も早い復興を心よりお祈り申し上げます。

はじめに

出入管理システムという市場はこの10年間でＩＴ市場の拡大、個人情報保護法という社会的情勢の変化の追い風を受け、成長を続けていました。

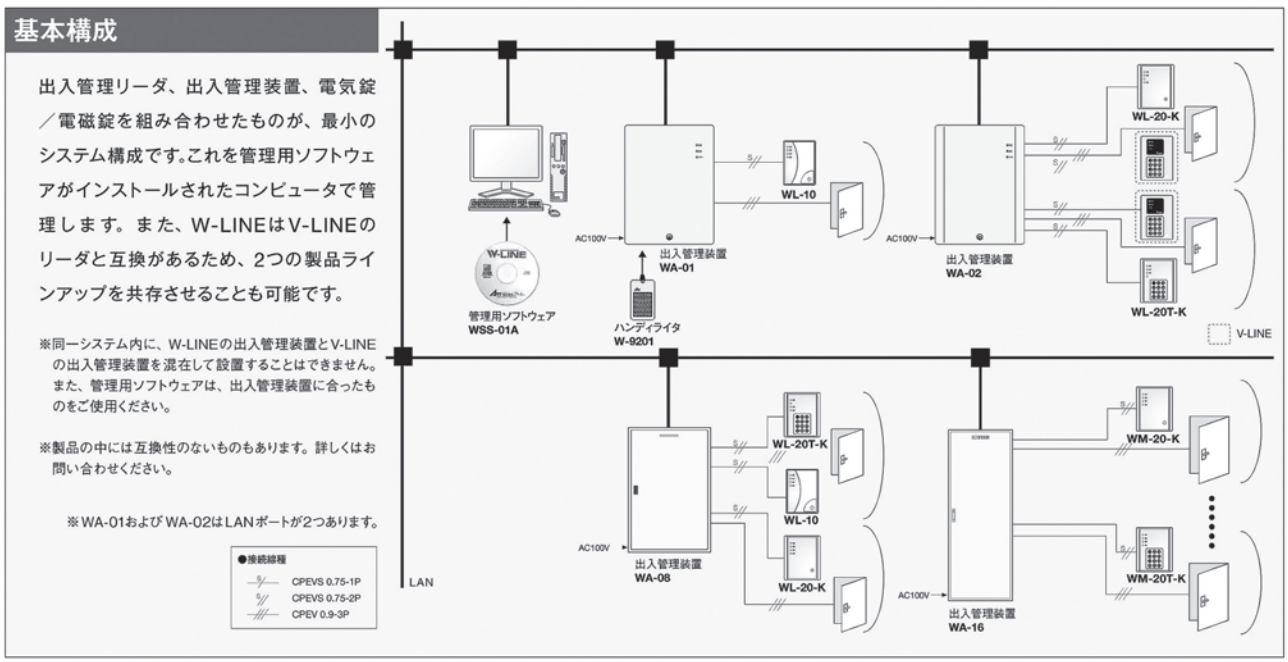
出入管理システムは、主にオフィスビル・研究所・工場を中心として企業向けに導入が進んでおり、「部外者の侵入を防ぐ」＝「許可者のみを入室（入館）」するということから、許可者しか持ち得ない「カード」、許可者しか知り得ない「暗証番号」を利用した出入管理が行われてきております。

企業以外では学校・病院・図書館等の公共施設にも出入管理システムの導入事例が増えてきております。導入目的は防犯がメインではありますが、利用者の利便性向上を目的としたシステムとして導入が進んできています。

本解説では、出入管理システムのハード的な技術解説にも触れますが、システムを導入する企業・利用者の運用的面から見た解説を中心に説明をさせていただくことと致します。

出入管理システムのシステム構成について

出入管理システムを導入する場合、電気錠をコントロールする制御装置、入室（退室）の操作を行う端末装置（リーダ・テンキー）、登録データの管理・操作履歴の管理を行うための管理装置（上位コンピュータ）にて構成されることが一般的であります。(図1)



（図1）

また、複数の扉を管理することから、１台の制御装置で複数台の端末装置を接続することができる多ゲート制御装置が一般的です。

出入管理システムで扱うデータ量は防犯カメラなどの設備機器よりも比較的少量のデータ配信で済むこと、また、通信処理能力の高い方式を積極的に採用する必要はなかったことから、シリアル通信を採用しているシステムが多くあります。

徐々にではありますがLAN方式に移行していますが、セキュリティシステムの特性上CLOSEされたネットワークが必要ということから、専用のネットワーク網でシステムが構築されています。

しかしながら、ネットワークの世界では暗号技術が一般的になってきており、徐々にOPENなネットワークを利用したシステムに組み込むことも増えてきました。

さらに、企業内にセキュリティシステムが導入される場合、セキュリティシステム単独のネットワークを敷設するのではなく、社内インフラとしてのネットワーク網を利用することを導入側から求められてきております。

照合媒体の変化

セキュリティシステムの多くは、磁気カードを利用したシステムが主流でした。磁気カードは複製の懸念からICタイプのカードへ切り替えようという動きがありましたが、端末装置のコスト及びカードコストが高く、国内では普及が進みませんでした。

ご承知の通りSuicaなどの交通系カード・おサイフケータイ・電子マネー・IC免許証・住民基本台帳カードなどに代表される非接触カードの普及が進み、カードコストが劇的に下がり、ICカードを飛び越えて一気に非接触カードを利用したシステムに切り替わってきております。

今後は、Androidに代表されるスマートフォンにNFCチップが標準搭載されることから、国内のみならず世界的な規模で非接触ICカードというインフラが普及され、誰もが意識することなく、非接触カードを持つことになっていくことは明らかです。

セキュリティシステム専用のカードを用意するのではなく、既に個人が所有しているカードを出入管理システムで利用される状況に変わりつつあります。

市場の変化

出入管理システムを導入する側は、利用者がモラルを持ってアクセスを行い、許可された人は正しい運用を行っていることを前提とした性善説をベースにシステムを運用してまいりました。

しかし、本人が所有する「カード」、本人しか知り得ない「暗証番号」がカードの貸し借りや紛失・盗難などにより、許可された本人が正しく使っているのかを判断することができなくなってきております。

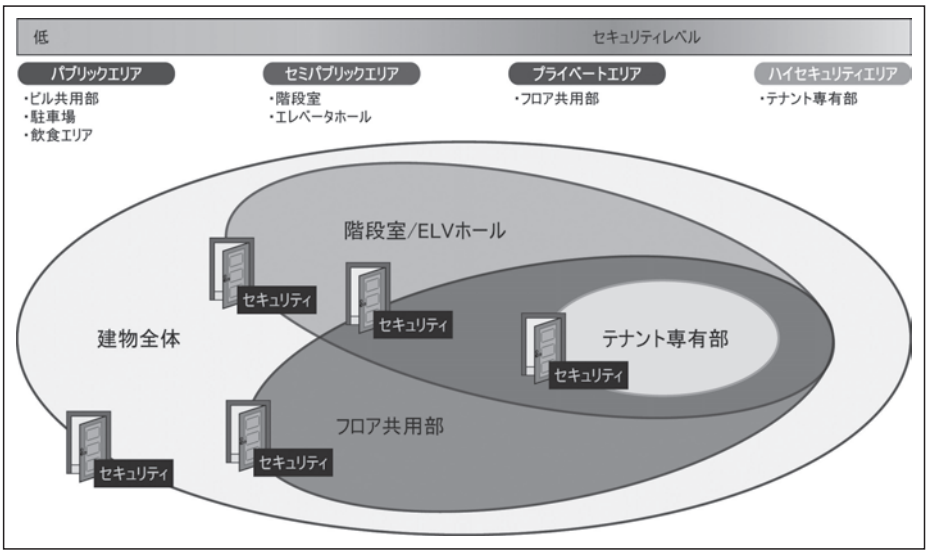
個人情報保護法など法体系も確立され、企業・団体では関係者に対して管理を徹底するように指導をしていますが、雇用体系の変化、賃金格差などによる社会情勢・雇用状況が不安定になることにより、カードの不正利用、悪意を持った行為、うっかりミス、等による情報流出が社会的な問題となってきております。

導入側としても厳密なシステムを求めており、バイオメトリクス技術を利用した生体認証装置が採用され始めました。(図2)

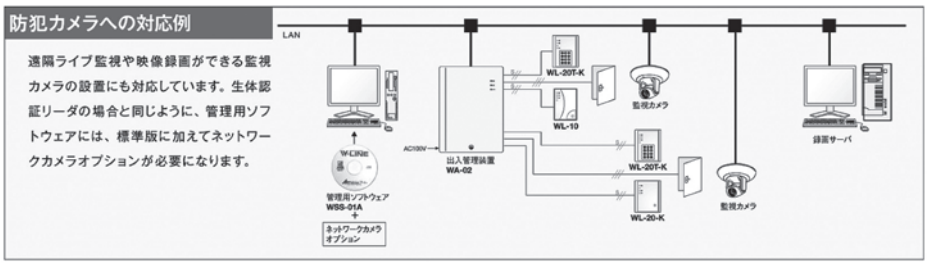
生体認証リーダ

(図2)

全てのエリア・扉にバイオメトリクス認証装置が設置することが理想的だが、一般的な非接触カードと比較すると端末装置の費用が数倍することから、重要度の高い部屋のみに設置しているというのが実情であります。



（図3）



（図4）

このような背景から、「セキュリティレベル」という概念が生まれました。(図3)

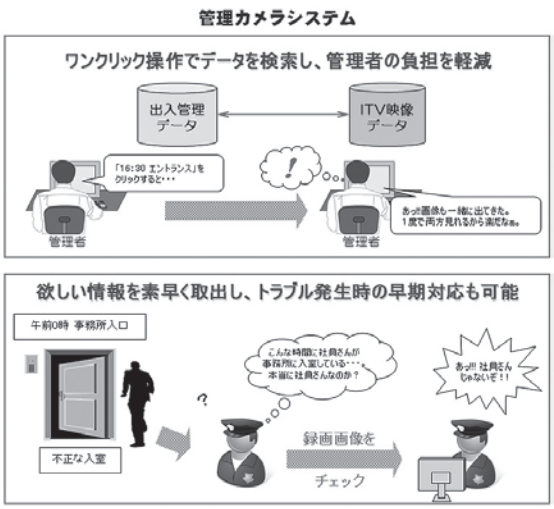
パブリックエリア・セミパブリックエリア・プライベーエリア・ハイセキュリティエリアというように、セキュリティレベルを決め、レベルに合わせてテンキー・カードリーダ・バイオメトリクス認証装置、物理的なフラッパーゲートや電気錠扉などを設置するようになり、利用シーン・レベルに合わせて最適なシステムを構築できるようになりました。

導入側の変化

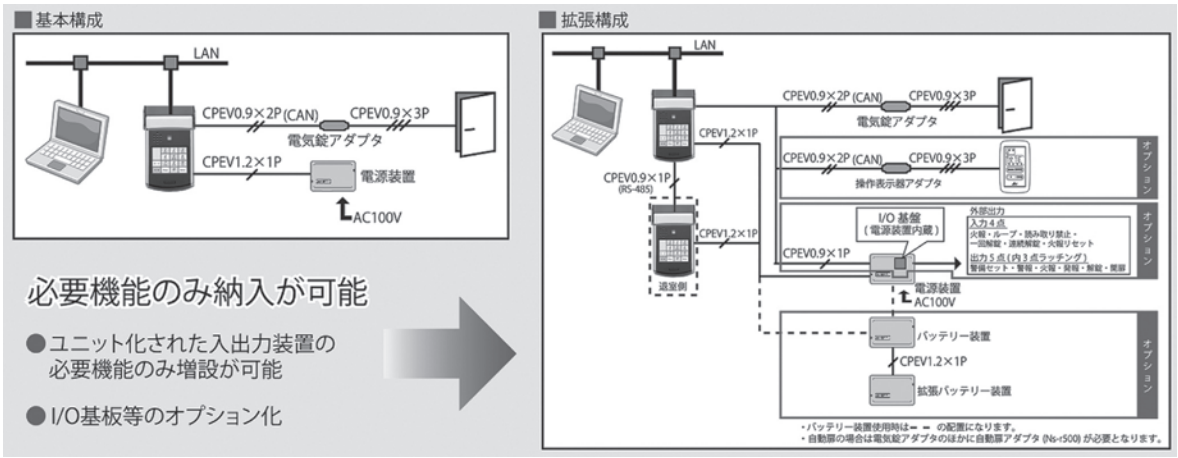
利用者のモラル向上を図ることを目的の一つとして、防犯カメラのシステム導入を実施している企業も多数見られます。(図4)

「人に見られている」という意識を利用者が持つことにより、セキュリティ性を向上させようということです。

出入管理ゲートの設置場所は、パーティションの区切りや執務スペースへの出入口、サーバールーム、書庫に多く設置されております。その部屋へ部外者・不正者・許可されていない人が入室するということは、勤務中に在席・在室している人たちの監視の目があり、既にセキュリティ性は確保されているという意識があります。休日・夜間等は人も少なくなり、無人になることも多いことから、室内側に防犯カメラを設置し、リーダ操作のログと同時に映像データを記録し、相互システムでデータをリンクしてログを確認できる仕組みが普及しはじめています。(図5)



（図5）



（図6）

出入管理システムと防犯カメラのシステムを導入するためには、それぞれのシステムを導入し、上位ソフトにより連携統合する必要があり、コスト的に非常に高価なシステムになってしまう問題があります。

パーティション変更や部署異動・オフィス内の模様替え等により、セキュリティレベルは日常的に変化しており、ダウンタイムの軽減も求められてきています。しかし、システムの移設に伴う費用・時間も多大になることから、導入時のままで実態に合わない運用形態になっている場合も多く見られます。

今後の出入管理システムについて

出入管理システムは高価な付加価値的なシステムであり、安全を守るためにはそれなりの設備投資と、運用コストが必要であると言われ続けていました。

今後は、セキュリティの仕様・機能面だけでなく、コスト面でも導入しやすく、かつ運用コストも軽減できるシステムが求められてくると考えられます。

ハード面は従来通り端末装置・制御装置・管理装置という構成が主流です。将来設置するかもしれない予備ゲート部分を確保する構成ではなく、必要なゲートにのみ設置することが求められるようになってきており（図6）、端末装置と制御装置の一体型の１ゲート用装置が主流になっていくと考えられます。

カードについては非接触カードは現状から大きな変化はみられる要素は少ないものの、コスト面から見ると大きな変化が見られます。セキュリティ専用の社員証・職員証を貸与・付与するのではなく、利用者が既に所有する非接触カード媒体を利用することがで、初期導入コスト・追加発行等の運用コストの軽減につながることができます。また、個人所有の非接触カード媒体は携帯電話内蔵であったり、電子マネー等が一体になったカードであることから安易な貸し借りを防止でき、所持忘れや紛失への懸念も少なくなるであろうと考えられています。

利用者のモラル向上もセキュリティを確保するためには必要な要素であることから、防犯カメラを設置するか、出入管理システムを設置するかという選択を迫られる場面も出てくることと思われます。

端末装置にカメラを内蔵させ、入室操作時の画像データと操作時の履歴を一元管理できるシステムを採用することで、導入コストも抑えることができるようなると考えています。（図7、8）

さらに、既設ビルへの導入が多くなってきていることから、無線技術を利用した出入管理システムも今後期待されていると言われています。セキュリティシステムだから、無線は好ましくないという認識は、今やセキュアな無線通信が一般的になってきている以上、変わらざるを得ない状況になっているとも言われています。

今後、無線技術を利用した出入管理システムが市場に登場することで機器のコストではなく、設置コスト・移設コストも大幅に削減できるという期待が持たれています。

（図7）

（図8）

最後に

セキュリティシステムは、誰から何を守るのか？という定義は「外部の侵入者」から「財産・生命」を守る。という人的・物理的なことから、「内部の関係者」から「情報」を守る。という技術的なことへ大きく変化していることは周知の事実であります。

物理的に強固なセキュリティシステムを導入し、セキュリティ性を確保することも重要ではありますが、操作する人のモラルも同時に向上させることが必要不可欠であると考えております。

日本国内においても、「安全と空気と水はただ」という常識が変わってきており、「電気」も必要な分を使う時代から、必要最低限の使用量をコントロールするシステムに変わる必要に直面しております。出入管理システムならではの省エネルギーへの取り組み・システムアップが今後の課題であると考えております。

株式会社アートは、セキュリティシステムの専業メーカとして時代の流れより一歩先を見ながら、製品の開発を続けて参りました。今後劇的なスピードで変化していくであろうセキュリティシステムの市場に対し、先駆者として時代の要請に応えられるシステムを提供し続けていきたいと考えております。

※「Suica」は東日本旅客鉄道 株式会社の登録商標です。
※「おサイフケータイ®」は株式会社NTTドコモの登録商標です。
※「Android」は、Google Inc.の商標または登録商標です。