入退場と情報セキュリティのシステム連携

早野 慎一郎・谷川 忠・北風 二郎

要　旨

本稿では、高まる情報漏えいのリスクに対応して、エリア管理の考え方を取り入れた新しい方向を示します。従来、個別に導入されていた、人、物、PC、ネットワーク、情報コンテンツの管理について統合ID管理を中心として連携させることにより、いつ誰がどこで情報に対して何をするのかを管理できることを述べます。具体例として、PCと入退場の連携などにより、情報アクセス場所を限定し、それを記録できること、映像処理により入退場セキュリティをさらに高め、管理を効率的に行えることを紹介します。

キーワード

●入退場　●セキュリティ　●フィジカルセキュリティ　●IC カード　●情報漏えい

1. はじめに

情報化の進展によりICT (Information Communication Technologies)を活用し、ビジネスを改革しようという動きが進んでいます。一方、大量の情報を容易に運ぶことができるようになり、情報漏えいのリスクも高まっています。さらに、個人情報を保護し、企業秘密の漏えい防止につとめ、内部統制の基礎固めをして法規制に対応し、ビジネスを支えるためにも情報セキュリティの強化が重要になっています[1)]。

本稿では、情報の管理に加え、それを運ぶ人、物についても管理を行い、人、物、情報の管理をお互いに連携させ、情報の安全性をさらに高め、効率的に運用を行うことができる新しいセキュリティシステムについて述べます。

2. 情報セキュリティ管理の動向

旧来の情報セキュリティ管理は外部の人が会社などの組織から情報を持ち出すことを防止するモデルが一般的であり、情報を会社外へ漏らさないとか、外部の人をオフィスエリアに入れない、ウイルスを会社内ネットワークに入れないといった侵入防御がセキュリティ対策の中心でした。しかし、情報が漏れる原因を分析してみると、PCの盗難、紛失、また、社員が自宅に情報を持ち帰り、自宅のPCからファイル交換ソフトを介して情報が漏れる例など、社員が情報漏えいに関与している例が多いことが分かります。また、社内でも個人情報を大量に扱う部門や会社の基幹データを統合して扱うデータセンターなどは特に情報にアクセスできる人を制限し、アクセスした人の記録を残すといった管理が必要となり、通常のオフィスエリアとは異なるセキュリティ管理を行う必要があります。

こうしたことから、**図1**に示すように、今後はオフィスを必要とされるセキュリティレベルに応じて複数のエリアに分け、フィジカルセキュリティと呼ばれる入退場管理の仕組みをエリアごとに導入し、いつ、どこに人がいるかを管理し、エリアに対応したセキュリティ対策を行うことが重要となります。また、セキュリティを高め、事故が起こったときに追跡を行いやすくするため、人と扱う情報を結びつけ、いつ誰がどこで情報に対して何をするのかを管理できるようにすることが重要

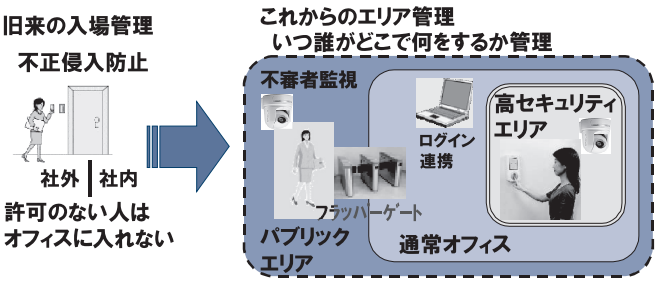

図1　これからのセキュリティ管理

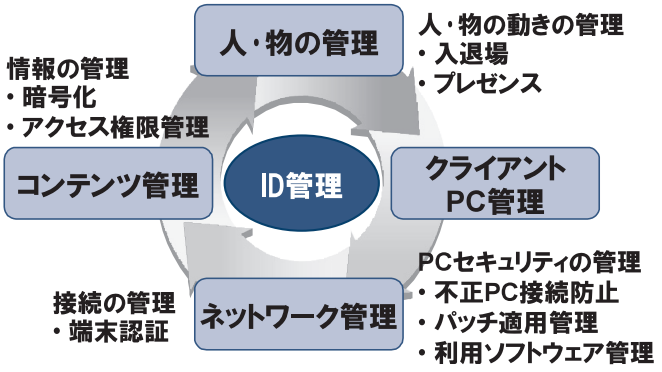

図2　人、物とネットワークを一体化したセキュリティ管理

となってきます。

そのような管理を行うために必要な項目を整理したのが**図2**になります。まず、ビル、オフィスだけではなく各種エリアへの入退場、プレゼンス(人、物の位置情報、状態情報)を管理することにより、人、物の動きを管理できるようにします。2番目に、情報を操作するのに使われるクライアントPCの管理を行うようにし、私有PC、ファイル交換ソフトの入ったPCの接続を禁止します。3番目のネットワークの管理では、端末認証を行い、どこで、どの端末が使われるかを管理します。4番目のコンテンツ管理では、暗号化とアクセス権限管理を用いて、情報を操作、読み取りできる人を管理します。最後に、人の特定を行い、権限の設定を行うID管理により、全体を統合し、いつだれがどこで何をしたかが分かる仕組みを構築します。また、このようなシステムを導入することにより、不正な利用を何段にもわたって防止することができるようになります。たとえば、管理エリア外から不正に内部情報にアクセスするとか、データを不正にコピーするような装置をネットワークにつなぐことを不可能にできます。

このような管理システムを導入することにより、情報漏えいに結びつく行動を抑止し、事故を早期に発見し、事故の追跡、探査が容易にできるようになります。

3. 人、物とネットワーク、情報に関するセキュリティの連携

本章ではどのように人・物と情報に関するセキュリティを連携させ、高度な管理システムを構築するかを述べます。人、物、情報に関する管理システムは従来から導入されていましたが、それぞれが別々に管理されていました。たとえば、入退場管理は勤務管理のために導入されており、入場していない人が社内システムにアクセスしているといったことを検出するのは困難でした。

情報の管理システムもシステムごとに個別になっていて、あるシステムは使えるのに、別のシステムを使うためには新たに申請してIDをとらないといけないといったことが起こっていました。また、個人を特定するIDもシステムごとに個別に管理されており、同じAさんであっても、IDはシステムによって異なり、同一人物が異なったシステムで行ったことを関連付けるのは簡単ではありませんでした。

このような状況では同じ人に関するID、権限が複数のシステムで管理されており、管理の手間が大きくなること、さらに、連携が取れていないために、異なるシステムの間でミスマッチを起こしやすくなり、事故が起こる原因となっていました。たとえば、退職者のデータがあるシステムでは退職前の状態で残っているということが起こり得ました。

これらのシステムの連携を取るためには、**図3**に示すように、まず、統合ID管理システムを導入し、人事システムなどと連携をとり、人の認証を統一的に行うことのできる環境を作る必要があります。統合ID管理システムを中核に、全体をIPネットワークで結び、入退場などの人、物に関するセキュリティシステムとの連携、情報アクセス管理などの情報、ネットワークに関するセキュリティとの連携を図っていきます。この際、非接触型のICカードを用いるのが最近の動向となっています。このようにシステムを連携させ、セキュリティポリシーの管理を統合ID管理システムで行うため、変更が一ヵ所で済み、全体として効率的で、間違いの少ない運用管理が可能となります。また、すべての認証を連携させることができるため、ユーザはICカードをかざすだけで、どのシステムでも認証を行うことができます。さらに、認証の受け渡し機能を利用し、居室

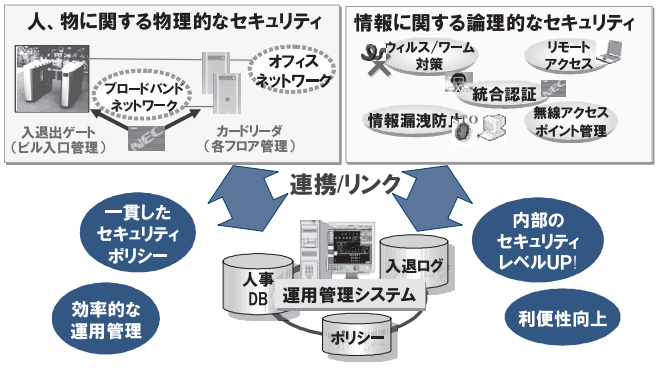

図3　人・物と情報に関するセキュリティの連携

を出たら、PCをログオフするといったセキュリティの強化もユーザに負担をかけることなく行うことができます。

4. 人、物と情報のセキュリティ連携具体例

人、物と情報を連携させる具体例としては、**図4**に示したようなものがあります。基本となるのは、ICカードによる入退場管理になります。エリアごとに共連れを防止するフラッパーゲート、自動ドアとカードリーダなどによる入退場制限により、だれが、いつ、どこにいるのかを管理します。入退場管理は統合ID管理と連携して行われ、人事異動などで生じた変更は即時に入退場管理に反映されます。これにより、セキュリティエリアへの職責による入場制限や入社、退職者の適切な入場管理、さらには勤務時間管理などを効率よく行うことができます。

ITシステムや、ネットワークの認証と連携させることにより、情報に対するアクセスを管理することができるようになり、それらのセキュリティを高めることも可能となります。PCへの認証情報の受渡しを入退場管理情報で制限することにより、オフィスエリアに在籍する人だけにPCのアクセスを許可するとか、エリアから退場した場合にはPCを自動ログオフするとか、部屋への入室した人のみ無線LANへのアクセスを許可し、アクセスしたエリアを記録するということが可能になります。これにより、情報にアクセスした場所を記録できるようにもなります。逆に、共連れによって入場しても、PCへのアクセスをすることはできなくなります。また、プリンタと連携させることにより、ICカードをかざした時にその場所のプリンタに出力するといったことも可能になります。これらにより、不要な人が情報にふれることを防止し、不正な情報アクセスを防止することができます。

導入に当たっては、すべてのシステムを一度に入れ替える必要はありません。必要に応じて、また、システムの更新時期に応じて部分的に導入することができます。ポイントは統合ID管理システムとICカードの選択となります。いずれも、将来の拡張に対応した機能を検討し、具備しておくことが必要となります。逆に統合ID管理システムまたはICカードの変更を計画する場合には、どこまで連携させるのかを検討しておくことにより、将来のシステム変更コストを小さくすることができます。

5. 映像を使った連携例

映像による監視は以前から行われていましたが、近年、映像のディジタル化、IP化により、セキュリティ強化で映像を活用できる場面が増えています。また、映像処理により、動体検知、不動体検知、エリア監視、顔認証といったことが可能

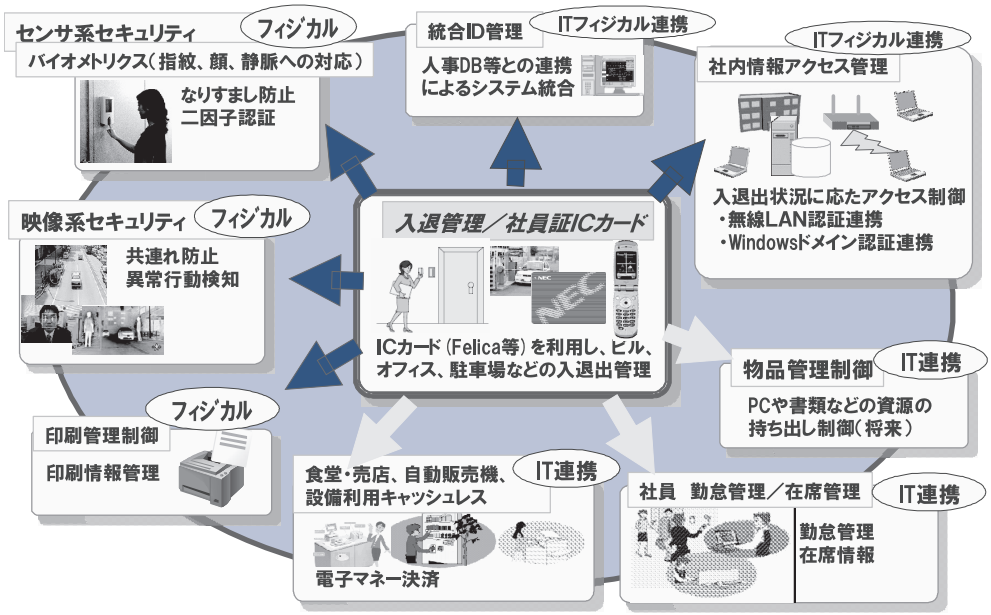

図4　社員証ICカードを中心としたセキュリティ連携

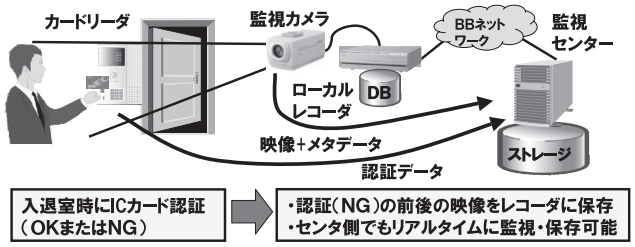

図5　動画像を使ったセキュリティ強化

になっており、他のシステムと連携してセキュリティ機能の向上、監視コストの低減を行うことができるようになっています。**図5**に示したのは入退場との連携です。入退場で検出されるカード認証の情報 (ID、OK、NGなど)とそれに連動して撮影された映像を共に記録しておくことにより、不審者の特定、事故の分析などを効率的に行うことができます。従来は映像のみが記録されていたため、確認したいことがあると、すべての映像を人手で確認する必要があり、カメラの台数が多いと非常に多くの人手、時間が必要でタイムリーな対応が困難でした。映像にID、入退場の情報が加わることにより、その情報で確認する映像を事前に絞り込むことができるようになり、確認に必要な人手、時間を大幅に削減することができます。

さらに、映像処理を用いた顔認証によりICカードによる認証に加えて本人認証を行うとか、フラッパーゲートの設置が難しい部分で映像分析により共連れの検出を行い、アラームを出すとか、不審者、不審物の検出、記録を行うといったセキュリティ強化をできるようになります。

システム構成上では、従来、サーバで行っていた映像処理の一部をカメラ側で行うことができるようになっています。カメラ側で映像処理した結果をメタ情報として映像とともにサーバに送り、サーバではメタ情報によって絞込みを行った映像だけをさらに詳細に分析を行うことができ、カメラの台数が増えたときのサーバへの負荷集中を避けることができます。

6. おわりに

人、物と情報のセキュリティについて統合ID管理システムを中心として連携させ、いつ、どこで、だれが、何をしたのか管理することにより、情報セキュリティを高度化し、運用管理を効率化する方法について述べてきました。今後はRFIDなどによるIDの遠隔検出の技術が進展し、情報を大量に運ぶことのできるPCや記録媒体の移動まで含めたセキュリティ管理へと進展することが期待されます。

参考文献

1）情報通信白書平成17年版、総務省、2005年6月

執筆者プロフィール

早野 慎一郎
企業ソリューション企画本部
グループマネージャー

谷川 忠
エンタープライズソリューション事業本部
UNIVERGEソリューション推進本部
ブロードバンドセキュリティ推進部
マネージャー

北風 二郎
エンタープライズソリューション事業本部
UNIVERGEソリューション推進本部
ブロードバンドセキュリティ推進部
部長

●本論文に関する詳細は下記をご覧ください。

関連URL: http://www.nec.co.jp/univerge/solution/pack/index.html