これからのオフィスセキュリティ強化対策のあり方を考える

大日本印刷株式会社 IPS 事業部
主席研究員　半田　富己男

個人情報保護法が 2005 年 4 月に施行された後にも、個人情報取扱事業者からの漏えい事案報告が続いています。内閣府が国民生活審議会個人情報保護部会へ提出した報告によると、平成 17 年度に個人情報取扱事業者が公表した個人情報の漏えい※1事案は、合計 1,556 件にのぼります。これらの個人情報漏えい事案のうち特段の情報保護措置を講じていなかった件数が全体の 51.7% を占めており、漏えい後の改善措置についてみると、全体の 96.5% の事業者が何らかの安全管理対策を講じています。事件が起きてからでないと、セキュリティ対策への投資の必要性が経営層に理解されにくいという、各企業の情報セキュリティ担当者の悩みは、この数字にも表れています。
こうした事案で、個人情報が漏えいしたとされる人数は、500 人以下の事案が全体の 71.6% と比較的小規模な事案が多くなっています。しかし、PC や記憶媒体の紛失・盗難による事案や、不正アクセスによる漏えい事案では、1 件あたりの漏えい人数が多くなり、重大な 2 次被害につながる恐れもあり、深刻な事態となることが多くなっています。大規模な個人情報漏えい事案を引き起こしてしまった企業は、損害賠償、社会的信用の失墜、顧客や取引先からの取引停止などという大きなダメージをこうむることにより、事業そのものを継続できないという重大な危機を迎えてしまいます。リスク管理の面から見ても、事件を起こしてしまってからの対応は難易度が高いばかりでなく、対応が完了する迄の期間のリスクを考慮すると、事前に適切な対応策をとっておくことが望ましいといえます。
本稿では、物理的セキュリティ対策と技術的セキュリティ対策の両面で効果的なキーデバイスとなる IC カードの使い方を軸にオフィスセキュリティ強化対策のあり方を考察します。

1. 物理的セキュリティ対策

個人情報保護法第20条は、個人情報取扱事業者に対して、その取り扱う個人データの漏えい、滅失又はき損の防止、その他の個人データの安全管理のために必要かつ、適切な措置を講じることを義務付けています。これを受けた経済産業省のガイドライン「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」では、組織的、人的、物理的及び技術的な安全管理措置を講じることを求めています。企業は利潤の追求にとどまらず、社会的責任(CSR)を果たすことが求められるようになり、法令遵守(コンプライアンス)と企業統治(コーポレート・ガバナンス)への関心が急速に高まっています。こうした背景から、今年に入って物理的セキュリティ対策に注目が集まり、オフィスセキュリティに特化した展示会(オフィスセキュリティ EXPO)が初めて開催されたり、オフィスの物理的セキュリティ対策を中心に第三者機関が評価・認証する制度(オフィスセキュリティマーク認証制度)が創設される等の動きが見られます。

(社)ニューオフィス推進協議会(NOPA)では、オフィスセキュリティマーク認証基準を定め、これに基づいたオフィスセキュリティマーク認証制度を2006年10月から開始しようとしています。この制度は、認証内容、取得費用及び期間等において、中堅・中小規模のSMB※2にとって比較的取得・継続しやすい認証制度となっています。ISMS適合性評価制度の認証基準JIS Q 27001でも、管理目的及び管理策として、セキュリティを保つべき領域を規定しています。こうした評価・認証制度では、機密性、完全性、可用性をバランス良く維持し改善していくためにPDCAサイクルを継続的に繰り返して、セキュリティ・レベルの維持・改善を図ることが要求されます。

※1「漏えい」の他、「滅失」、「き損」の事案を含む。　※2 Small and Medium Business

物理的セキュリティ対策の中でも、最初に着手されるのは、物理的セキュリティ境界のゾーニングと、それによって作られたセキュリティ領域への入退館(室)管理です。磁気カードやICカード等をセキュリティ領域のゲートに設置されたカードリーダにスキャンすることにより本人確認を行い、ゲートの電気錠を解錠する方法や、身体的特徴をセンサーで識別・認証して本人確認を行い、解錠する生体認証方式などが用いられています。

一方、従業員と来訪者を識別するために、氏名・顔写真入りのIDカードを貸与して着用させる方法が広く行われています。そのため､従業員識別用のIDカードと入退館(室)管理システム用カードを共通化しようと考えるのは自然な展開といえます。こうした用途のIDカードとして従来の社員証・職員証カードを新規に切り替える際には、磁気カードではなくICカードを採用する事例が増えています。ICカードは磁気カードより大きなメモリ容量を持ち、カード所持者を認証する機能や格納データに対するアクセス制御機能を持っているため、磁気カードに比べてセキュリティを向上させることが可能となります。ICカードには、リーダ・ライタとの通信方式により、接触型と非接触型がありますが、非接触型の場合、リーダ・ライタにカードを通す代わりに「かざす」だけでよいので入退館(室)管理での利用では、利便性の面から非接触型の人気が、最近特に高くなっています。

2. 技術的セキュリティ対策

技術的セキュリティ対策には、情報資産及びそれを取り扱う情報システムへの、アクセス制御、不正ソフトウェア対策、情報システムの監視等、情報資産に対するIT技術的な対策等があります。中でも、識別と認証は、情報システム利用者の身元を特定し、真正性を確認する技術で、情報システムへの不正アクセスを試みる者を入口で拒否する重要な防御機能です。認証技術を分類すると、パスワードなど利用者本人の記憶(知識)に基づく認証、ICカードや認証トークンなど本人のみが所持しているものに基づく認証、本人の身体的特徴に基づくバイオメトリクス認証の3種類があります。利用者IDとパスワードだけによる識別・認証では、利用者本人が覚えやすく簡単で短いパスワードを設定してしまうために、他人にパスワードを推測されてしまったり、逆に、長くて複雑なパスワードに設定したために利用者本人が覚えきれずに紙に書いてしまうところから他人にパスワードが漏えいしたりするなどの問題点があります。そこで、パスワードを知っていることと、ICカードを持っていることなど、複数の要素を組み合わせた多要素認証が注目を集めています。また、公開鍵基盤(PKI)のデジタル証明書等の暗号クレデンシャルを用いた認証でも、暗号クレデンシャルをセキュアに格納し、携帯性に優れた媒体として、ICカードが注目されています。これは、ICカードが耐タンパー性を持っていること、すなわち、ICカード自身がICカード内に格納された機密情報へのアクセスを制限し、機密情報の不正な読出し・複製を防ぐ機能を備えているからです。このため、ICカードを利用して、パソコンのログイン、起動制御、スクリーン・ロック等を実現するPCセキュリティ・ソフトウェアがさまざまなベンダーから提供されています。

PCセキュリティの分野だけでなく、最近では、プリンタ出力時に、プリンタキューにプリント・データを保持し、プリンタ出力命令をかけた者のICカードを認証した後に、印刷出力を開始するというセキュリティプリンタシステムも登場しています。一般に、オフィスでは共有プリンタが利用されているので、プリンタ出力の取り忘れや、印刷出力物を他人に持っていかれたりするといった経験は誰にでもあることでしょう。このように機密文書を共有プリンタに出力するオフィス環境では、セキュリティプリンタシステムが情報管理に非常に有効です。

3. IC カード化に際して

これまで見てきたように、物理的セキュリティ対策においても、技術的セキュリティ対策においてもICカードは重要な役割を果たしています。近年、ICカードはますます記憶容量が増加しつつあり、これら複数の機能を1枚のICカードに搭載することも可能になってきました。

ただし、複数の機能を1枚のICカードに搭載する場合には、ICカードを初期発行するまでに、あらかじめ、導入予定のICカード利用システムの各々について仕様を詰めておく必要があります。その理由は、ICカードを発行する際には、カード内のファイル・レイアウトを決めたうえで発行しなければならないからです。

企業の社員証・職員証カードといったIDカードは、一般に5年間程度の有効期間のカードとして発行されます。企業を取り巻く社会的要求・技術的環境が変化のスピードを、加速度的に速めている時代に、あらかじめ5年先までを見据えたセキュリティ・システム設計は困難です。結果的に、社員証ICカードを発行してから2年後には、セキュリティプリンタシステムの導入により、社員証とは別に、もう一枚のICカードを持たされることになったりしかねません。配付済の社員証ICカードを回収して破棄し、作り直しをすることは現実的ではないからです。同じ社内であっても、部門ごとに異なるベンダーのゲート管理システムが導入されることもあり、それぞれのゲート管理システム独自のカードを社員証ICカードとは別に持たなければならないケースも今後ますます生じることでしょう。

4. IC カードを核とした物理的セキュリティと技術的セキュリティの融合

このように、新たなセキュリティ・サービスを追加するたびにICカードを保有しなければならない枚数が増えてしまい、結果として利用者の利便性を損ねるという課題がありました。これを解決しようとして生まれた企業連合がSSFCアライアンス(Shared Security Formats Cooperation)です。SSFCアライアンスには入退館(室)管理システム、プリンタ・FAX・コピー機、オフィス什器、監視カメラ等、セキュリティ・システム各分野の主要ベンダーと、システム・インテグレータ等、合計100社以上が参加しています。SSFCアライアンスでは、これら複数のセキュリティ・システム分野のベンダーが共有できるICカード内のフォーマット仕様を策定し、ハードウェアベンダー系のメンバー企業は、このフォーマットに対応した機器を製品化します。

SSFC仕様に準拠したICカードとSSFC仕様アプライアンス製品機器の連携イメージの一例を述べましょう。SSFCカードを使ってゲートを通過すると、ゲートシステムはログを出力し、同時に監視カメラに対してゲートを通過した人物のSSFCカード内情報(ID番号など)を通知します。監視カメラは人物の画像をSSFCカード内情報(ID番号など)でインデックス化して録画します。ゲート内の執務室ではゲートを正しく通過した人物だけがパソコン、プリンタ、書類キャビネットを使うことができます。プリンタ等の各種機器は、ID番号付でログを出力しますので、セキュリティ管理者はインデックス化された画像から瞬時にID検索が可能となり、各機器から出力されるログ情報と合わせセキュリティ運用監視に目を光らせることが可能となります。

SSFC仕様の特長の一つに、カード所持者の所在場所情報を、ICカードを介してSSFC仕様セキュリティ機器に伝達する機能があります。SSFC仕様のゲートを通過したという情報がSSFCカードに記録されるので、この在室情報を利用すると、SSFCカード所持者に様々なセキュリティ・ソリューションを与えることが可能になります。

誰が、いつ、どこで、何をしたかを1枚のIDカードで、権限を与え、監査証跡を残すことが可能となります。

初期導入時に将来を見据えたセキュリティ・システムの設計が必要な従来のICカードと異なり、1枚のSSFCカードの導入運用から始めれば、SSFCアライアンスに参加する多数の有力ベンダーの製品群の中から、適切なタイミングで、適切な機器の導入が可能となります。

本稿で考察したセキュリティ・システムは、以下の点において優れています。

- セキュリティ対策への投資に対する経営層の理解が、得られやすい仕組みである
- 継続的なセキュリティ投資が可能な仕組みとなっている
- マルチベンダーでセキュリティ・システムを構築できるので、コストダウンが見込める
- 確実なログ情報が、ID番号付で収集できる
- 物理的セキュリティ対策と技術的セキュリティ対策を融合できる仕組みであるため、より高いセキュリティ効果を得ることが可能な仕組みとなっている

参　考

平成17年度 個人情報の保護に関する法律施行状況の概要、平成18年6月 内閣府
第20次 国民生活審議会 個人情報保護部会 第8回(平成18年6月30日) 資料6
http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20bukai-index.html

個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン、平成16年10月、経済産業省
http://www.meti.go.jp/feedback/data/i41013bj.html