http://www.tokiorisk.co.jp/

TRC EYE Vol. 138

東京海上日動リスクコンサルティング（株）
情報グループ　主席研究員　下島 和彦
開発グループ　主任研究員　本田 祐嗣
開発グループ　　研究員　岡田 陽子
情報グループ　　河野 幸子

情報漏洩リスクと対峙するオフィス環境

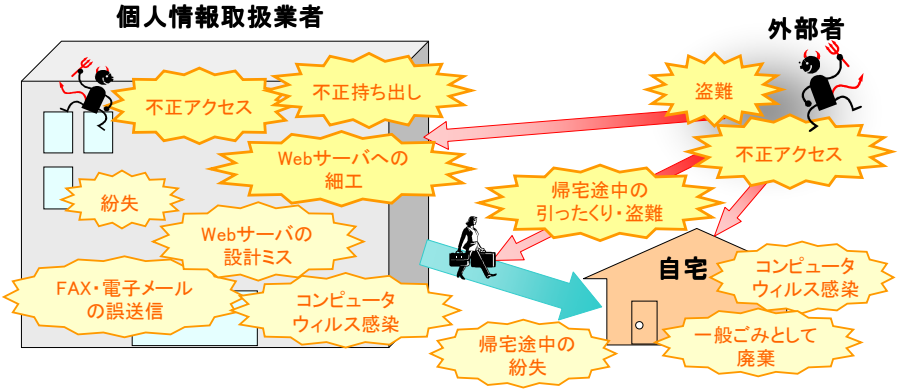
【『安全と管理』2007 年 3 月号から 8 月号に連載されたものを日本実務出版社の許可を得て転載しています。】

国際的な情報流通の拡大、急速な IT 化に伴い、企業における情報セキュリティ対策は、いまや当たり前のように取り組まれています。また、頻発するテロや凶悪犯罪の影響により、企業のオフィスにおける警備体制が強化されています。しかし、こうした取り組みは、外部の人間による犯行を想定したものがほとんどであり、内部者の不正アクセスあるいは不正持ち出しなどによる情報漏洩は、あまり想定されていません。本稿は、物理的セキュリティ対策を中心に、内部からの脅威を含む情報漏洩リスクを減らすオフィス環境づくりの基本について解説します。

１．事例からみるオフィスセキュリティの穴

新聞やインターネットニュースに公開される情報漏洩事件の件数は、年々増加傾向にあります。JNSA（NPO　日本ネットワークセキュリティ協会）の「2005 年　情報セキュリティインシデントに関する調査報告書」によると、2005 年の件数は 1032 件、前年の約 2.8 倍となっています。個人情報保護法の施行によって自主的に公表する企業が増えたこともありますが、個人情報の悪用が多発していることは事実です。詐欺電話や迷惑メールに加え、個人情報をネット上で公開されて精神的苦痛を受けたり、クレジットカード番号などの情報が流出して経済的被害を受けたりする事件が報告されています。

【情報漏洩の主な要因】



情報漏洩事件というと、悪意を持った外部の人間が、ネットワークを経由してアクセス制御を破って侵入したり、鍵を破ってあるいは社員や出入業者になりすまして事務所内に侵入したりして盗んでいくというイメージがあるかもしれません。しかし、実際には、内部者の管理意識の低さから発生するケースが多いのが現状です。電子メールや FAX の誤送信といった「うっかりミス」のほか、自宅などで作業するために持ち出した個人情報が流出する事件が多発しています。Winny をインストールした自宅のパソコンがウィルスに冒されネット上に流出する、持ち出した情報を電車内に置き忘れるあるいは車上荒らしに遭い盗まれるなど、同様の事件が繰り返されています。大量の個人情報を紙で持ち出すのは大変ですが、USB メモリーや CD-ROM で持ち出すのは簡単ですし、「いままでもやってきたが問題なかった」「この程度の情報なら漏れたとしても大したことにはならないだろう」という意識がまだ蔓延していることも問題のようです。

http://www.tokiorisk.co.jp/

また、コピーを取ろうとしたらそこに重要そうな書類が置いてあった、お金になりそうな名簿が机上に放置されていた、という状況で衝動的に持ち去るケースも考えられます。不満あるいは悪意をもった内部者が特定の目的をもって特定の情報を狙い、企業や顧客に損害を与えようとすれば防御も発見も困難なケースがありますが、多くの場合は「持ち出そうと思えば簡単に持ち出せる」状況をなくすことで防ぐことができます。

プライバシーマークや ISMS 認証などを取得して情報管理体制を整えたとしても、取り扱う人間の意識が低ければ「仏つくって魂入れず」になってしまいます。ルールを守りやすい環境、ルール違反を起こさせない環境を作ることが重要です。

２．トップダウンのセキュリティ対策を

近年、情報漏洩のみならず、自動車のリコール問題や瞬間ガス湯沸し器の一連の事故、食品メーカーにおける賞味期限切れ原料の使用など、国民の安全・安心を損なうような不祥事が相次いでいます。終身雇用制が崩壊し、雇用形態も多様化、企業間を個人が自由に移動するようになり、企業への帰属意識や従業員同士の信頼関係も希薄になってきている中、従業員一人ひとりの倫理観や社会に対する責任意識を徹底し、誠実な組織文化を醸成していくことは、多くの企業で喫緊の課題となっています。

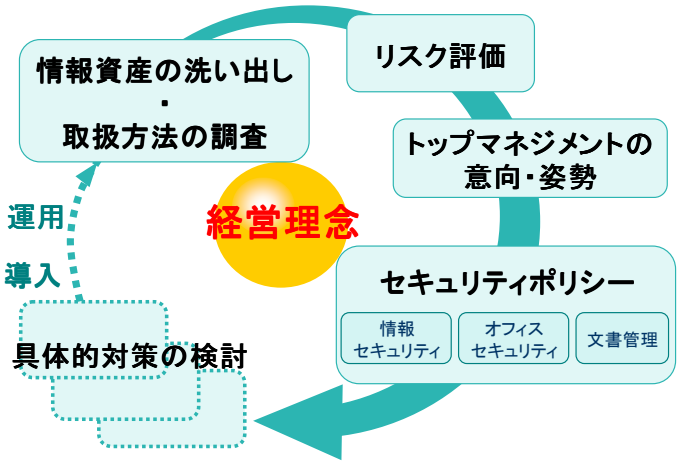
社会的信用の失墜は企業のブランド価値に大きなダメージを与えます。コンプライアンスを実践できない企業が市場からの撤退を余儀なくされるケースも増えました。コンプライアンスはいまや世界的な流れとなっており、内部統制システムを筆頭に、様々な方面でマネジメントシステムの構築が求められています。情報セキュリティ対策についても、IT が急速に普及する中で国民生活や社会経済活動の安全・安心を脅かす事態が発生している状況を鑑み、内部統制の一環として重点的に取り組みが進んでいます。

一方、オフィス環境のセキュリティ対策については、コストがかかる割に投資効果が見えにくいため、「やらなきゃいけないのはわかるが、まだ何も起こっていない」と後回しにされがちなのが現状です。これだけ頻繁に個人情報流出の報告がされているにもかかわらず、侵入しようと思えば簡単に侵入できるオフィス、あるいは一度侵入してしまえば重要な情報を簡単に持ち出せるオフィスが多々見られます。内部統制機能の強化の要請が日増しに高まる中、当然予測できたであろうリスクに対策を講じず「このような事態になり、誠に遺憾です」などと言い訳する企業は今後淘汰されていきます。大量の個人情報が流出し、苦情や訴訟に対応しながらオフィスを移転するコストを考えてみてください。

ただし、必要なセキュリティ対策は個々の企業で異なります。まず、企業内にある情報資産をリストアップし、情報を取り扱う局面毎のリスクを洗い出してみてください。そして、アクセス権限を持たない者にアクセスさせない、アクセスを許可した者を監視する、内部者のルール違反を防ぐという視点で IT 環境、オフィス環境を見直してみてください。必要な対策が見えてくるはずです。情報セキュリティ対策は IT 部門、オフィス環境のセキュリティ対策は管財部門、文書管理は総務部門、と情報資産がばらばらな観点で管理されている企業が多いと思いますが、それらを包括したセキュリティの方針と対策が必要です。

こうした検討を怠り、システム事業者や防犯設備のベンダー、警備会社などに丸投げしてしまう企業もあります。それでは体裁は整えることはできても、運用上の支障が出てくるおそれがあります。一人ひとりの従業員の意識やそれに基づく行動に影響を与え得るのは、トップマネジメントのリーダーシップであり、コミットメントです。経営理念と連動したセキュリティポリシーを策定し、具体的対策を検討していくことが重要です。

【情報漏洩対策の検討手順】



http://www.tokiorisk.co.jp/

３．アクセスコントロールの基本

具体的対策を検討するには、オフィスセキュリティの基本的なポイント押さえておく必要があります。

通常、財物の盗難を狙った侵入者は、人に姿を見られることや犯行に時間がかかることを嫌がります。これまでのオフィスにおける侵入盗をみると、人目の少ない時間帯に、死角となりやすい開口部から侵入し、パソコンや金庫を盗み出すのが通常の手口でした。しかし、そうした時間帯、侵入経路となりやすい場所にはセンサや監視カメラなど防犯設備が厳重に設置されており、相当入念な下見と技術なしに侵入するのは至難の業です。そのため、近年ではプロの窃盗団による犯行と思われる巧妙かつ大胆な手口が多くみられます。

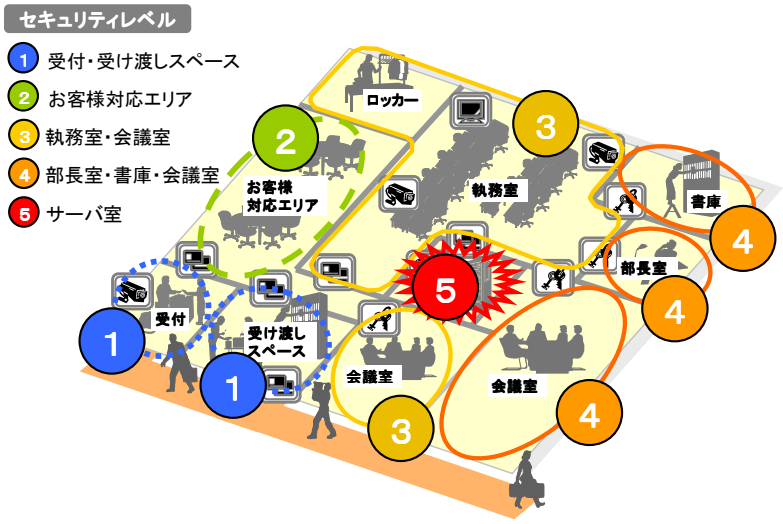
一方、情報資産を持ち出す場合は、大抵そのような危険を冒す必要はありません。書類や電子媒体の社外持ち出しが日常的に行われているオフィスで、情報を取り扱う人が多い時間帯に、内部者に紛れて情報にアクセスすることができれば、人に姿を見られても、時間がかかっても、全く怪しまれずに持ち出すことが可能です。アクセス頻度が高く、アクセスログ（記録）が残らなければ、追跡も困難です。悪意がなくても、作業のために持ち帰って車内に置き忘れる、あるいは「ほんの出来心」から持ち出して売却してしまうという事態になりかねません。

そこで、アクセスコントロールがキーとなります。情報資産を守るには、権限をもたない者にアクセスさせないこと、アクセスした場合は記録を残すことが必要です。具体的には、次の４つの対策が基本となります。

① ゾーニング

強固な壁で仕切り、エリアのセキュリティ区分を明確にします。仕切り方は、基本的に入れ子状にし、内部に行くほどセキュリティレベルが高くなる構造にします。

【フロアゾーニングの一例】



② 入退室管理

個人認証機能のついた電気錠を出入口毎に設置します。個人単位でアクセス権限を付与し、ゲート毎のアクセス権限者の設定を細分化すれば、セキュリティレベルは高まります。また、アクセスログ（記録）を残すことで、流出経路の究明、責任の追及が可能になり、抑止効果も得られます。

③ 情報資産の分類・管理ルール

「個人情報」「顧客情報」「営業秘密情報」「公開情報」など情報の分類、「関係者外秘」「社外秘」「公開」など機密区分、取得・開示・複製・保管・持ち出し・廃棄など取扱方法について、全社的なルールを策定することで、保護しなければいけない情報資産だけを適切に守ることができます。アクセスコントロールを的確かつ効率的に行うことができます。

④ 鍵の管理

キャビネットなどの鍵は、机の引き出しなどに放置せず、アクセス制限できる鍵収納ボックスに収納します。

オフィスのリスクは建物用途や保有する資産、人の出入り状況などにより様々ですが、こうした基本を踏まえると、必要となる対策のポイントがみえてきます。次に、一般事務オフィスと専門施設（研究所・データセンター等）について、もう少し詳しく解説します。

４．一般事務オフィスにおける物理的セキュリティ対策

企業が事業活動を行ううえで「情報」の活用は不可欠です。そのため重要な情報資産が個人のパソコンやキャビネットの中など、オフィスのいたるところに置かれています。

また、オフィスでは派遣やアルバイトといった多様な雇用形態が混在し、メンバーは流動的です。日中、来客もあるほか、宅配便、事務機器のメンテナンス、清掃など、従業員以外の人が頻繁に出入するのが通常です。

このような場所では、しっかりとした対策が必要な一方、そこで働く一人ひとりのセキュリティに対する意識を高め、業務効率に配慮したバランスの良い対策を立てる事が重要となります。以下、具体的な物理的セキュリティ対策を見ていきます。

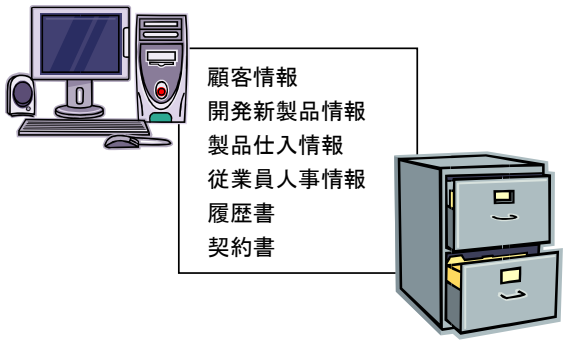
情報資産を守る一番の方法は、必要のない人間を情報にアクセスさせないことです。まず、情報を利用・保管するエリアは外部と壁で隔て、境界を明確にします。出入口は施錠するか、または有人の受付を設け、権限者のみが執務エリアに入れるようにします。

さらに執務エリア内はセキュリティレベルごとにゾーニングし、重要度の高い情報資産は出入口から遠い、高セキュリティエリア内で施錠保管します。物理的に情報資産にアクセスできないように、またはアクセスしにくくすることが基本的な対策です。

アクセスを制限すると同時に、全てのアクセスを記録することが望まれます。特にサーバールームなどの高セキュリティエリアでは、入室を許された権限者による犯行も想定し、漏れのない入退記録はもちろん、生体認証システム、監視カメラの設置、複数名での入室の義務化など、きめ細かい対策が必要です。アクセスログの取得は内部犯行の抑止にもつながり、また、実際に事故が発生した際の原因究明に役立ちます。

一方、業務効率とのバランスをとることも重要です。情報資産と一言でいっても様々な様式、種類の情報があり、使用頻度も異なります。全てを一律に施錠保管するのではなく、情報資産のライフサイクル、重要度、使用頻度を考え分類し、本当に守るべき情報資産を見極め、優先順位に応じた守りやすいルールを策定します。また、外部と内部の緩衝地帯として DMZ（DeMilitarized Zone：「非武装地帯」の意）を設け、そこで受渡や応接のみの来訪者に対応します。重要な情報資産に部外者を近づけることなく、無駄な入退室記録も行わなくて済みます。

【一般オフィスの情報資産】



物理的セキュリティには様々な対策がありますが、その効果は情報資産に対する直接のリスクだけにとどまりません。例えば物理的に「入館証がないとオフィスに入れない」という事実は、オフィスで働く人達に「執務エリアには部外者を入れてはいけない」と無意識のうちに理解させ、セキュリティを向上させる効果もあります。様々な立場の人達が働く一般事務オフィスにおいてこのような象徴的な対策は、大変分かりやすく、有効な手段であるといえます。

５．専門施設における物理的セキュリティ対策

次に、専門施設の物理的セキュリティついて解説します。

ここでいう「専門施設」とは、特定の業務を専門に行う施設のことで、かつ個人情報や営業秘密、知的財産などの重要な情報資産を、大量に利用、保管している施設を指すこととします。例えば、企業の研究所、情報システム（事務）センター、コールセンターなどがこの「専門施設」に該当します。

一般事務オフィスでは、セキュリティ対策と同時に、多様な来訪客に効率よく対応するための便宜性も求められましたが、専門施設では、その情報資産の重要性から、多少の便宜を犠牲にしてでもセキュリティを確保する必要があります。そこで本稿ではまず、専門施設の特徴とそのリスクを概観し、次にリスクに見合ったセキュリティ対策を検討していきます。

専門施設は、高度な営業秘密や知的財産、大量の顧客データベースなどを駆使して業務を実施することが多いため、施設内で従事する人員は、これらの情報資産に直接アクセスできる権利を持っています。また、一般事務オフィスに比べ人員の外出や外部からの来客は少なく、施設への出入りに便宜を図る必要性は小さいと考えられます。加えて、情報システムの開発・保守を委託している事業者やコールセンターのコミュニケータを派遣している事業者など、自社の社員以外の人員が多人数､従事している場合もあります。こうした人員は、自社社員に比べて就業形態や雇用形態等が流動的で、一人ひとりの管理が困難な場合もあります。

したがって、専門施設の物理的セキュリティ対策を検討するにあたっては、アクセス権限を持たない人員を絶対に入場・入室させないようアクセスコントロールを厳しく行うこと、および情報資産にアクセス可能な権限者が不正に情報資産を持ち出さないようにすることの 2 面からの対策が重要であるといえます。

【一般事務オフィスと専門施設における情報リスクの違い】

	一般事務オフィス	専門施設
立地	テナントとして入居している場合が多い	専用の敷地や建物を占有している場合もある
就業形態	派遣、アルバイトなど多様	外部委託先が一部スペースを占有している場合もある
就業時間	ビジネスアワー中心	深夜、休日も就業している場合もある
来客	多様な来客が多数訪れる	一定の決まった来客の場合が多い
荷物の搬入・搬出	郵便など限定的	物資の大量搬入や印刷帳票の大量搬出もある
情報資産	重要情報も存在するが限定的である	高度な営業秘密や大量の顧客データベースが存在している
人的管理のしやすさ	日中出入りが多く管理しづらい	比較的出入りが少ないため、多少の手数も受け入れられやすい

アクセスコントロールは、情報資産の保管場所や情報システムだけでなく、専門施設の敷地や建物の境界線も、防犯カメラや防犯センサによって死角のないように管理します。実際の入場にあたっては、警備員等、人による受付によって、従業者以外の入場、退場は全て記録することが望ましいでしょう。正面玄関のセキュリティを強固にしても、地下駐車場や荷物搬入口等でのセキュリティチェックが甘い場合があります。全ての出入り口のセキュリティレベルは同一に維持する必要があります。また、建物や部屋のセキュリティレベルをきめ細かく設定し、従業者や委託先従業員の入場資格も、レベルに応じてきめ細かく設定します。単発の来訪者の入館カードは、１日で無効になるようにするなど、アクセス権の見直しもなるべく短い周期で行います。

特に重要な情報資産がある建物や部屋への入場、退場は、アクセス権のある従業者であっても記録しておきます。一人ひとりの入退場を正確に記録するためには、共連れ防止機能のある入退管理装置やアンチパスバックシステムの導入が効果的です。また重要なエリアには、前室を設けロッカーを設置し、身の回りの必要なものだけを透明バッグに入れて持ち込み、私物や鞄を持ち込ませない、端末操作のみが必要なコールセンターなどでは、机に引き出しを設けないなど、権限者が情報資産を持ち出さないようにする徹底した対策を検討する必要もあります。

６．オフィスセキュリティの課題と展望

本稿では、初めに情報漏洩事例を紹介し、各企業がトップダウンでオフィスのセキュリティ対策に取り組むことを提案。その後、一般事務オフィスと専門施設の違いを考慮しながら、対策の基本を解説してきました。

オフィスのセキュリティという話題は、特に違和感なく読者の皆様に受け入れられたのではないでしょうか。しかし、オフィスセキュリティという概念は、意外にも、比較的最近になってから本格的に広まり始めたものです。以降では、この新しい概念の現状と課題、今後の展望を述べます。

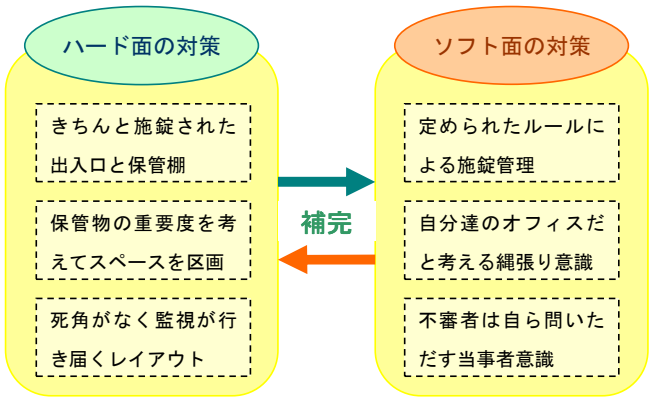
オフィス等の空間を対象としたセキュリティは、物理的セキュリティ（Physical Security）という分野に属し、米国ではその体系をマネジメントの視点で整理した解説書が多数出版されています。

わが国では､洋書の邦訳版も含めて､セキュリティマネジメントを取り扱う標準的なテキストがなく､実務者が参考にできる情報が乏しかったのが実情でした。しかし、オフィスセキュリティの考え方が広まるにつれて、状況が変わりつつあります。社団法人ニューオフィス推進協議会がオフィスセキュリティの考え方と実践法を体系化し、実務に適用できるガイドブックを刊行するところまで進んできました。

http://www.tokiorisk.co.jp/

オフィスセキュリティの成否を左右する重要なポイントは、ハード面の対策とソフト面の対策のバランスです。経済産業省によると、個人情報の漏洩事案の６割程度は、書類の紛失や盗難、パソコンの盗難が占めているそうです。また、はじめに指摘したように、内部者の不正行為や管理意識不足に起因する情報漏洩も頻発しています。セキュリティ機器は年々進歩しているとはいえ、機器の導入だけに活路を求めても、根本的な問題解決には至らないケースは少なくないと思われます。機械警備には必ず穴があります。現場では、その穴を意識の向上や衆人環視などで補うマネジメントを展開することが課題になります。

【ハード面の対策とソフト面の対策】



セキュリティ強化だけが目的では、企業の現場は前向きに取り組みにくいかも知れません。しかし、オフィスセキュリティへの取り組みから、侵入や盗難の防止以外の副次的な効果も期待できます。前出の社団法人ニューオフィス推進協議会によると、書類等をきちんとファイリングし、重要度別に保管する作業が、オフィススペースの効率活用につながるケースが多いそうです。従業員にとっても、無駄な手間が減って効率が上がり、以前よりも快適に仕事ができるようになる例が少なくないそうです。

規模の大小を問わず、企業は漏らすことができない情報を抱えています。また、情報漏洩リスクが完全になくなることはありません。ならば、上手に付き合う方法を考えるべきです。昨年から、オフィスセキュリティマーク認証制度が始まりました。要員や知識の面で不安がある企業でも、認証取得を通じて、比較的手軽にセキュリティ対策に取り組めるようになりました。オフィスセキュリティへの取り組みは、今後ますます広がっていくことが期待されています。

（了）

※　本文中の図表はすべて執筆者が独自に作成したものです。