2008年3月1日発行 毎月1回1日発行 通巻463号 Vol.43 NO.3 1972年2月28日 第3種郵便物認可

ビル メンテナンス

月刊

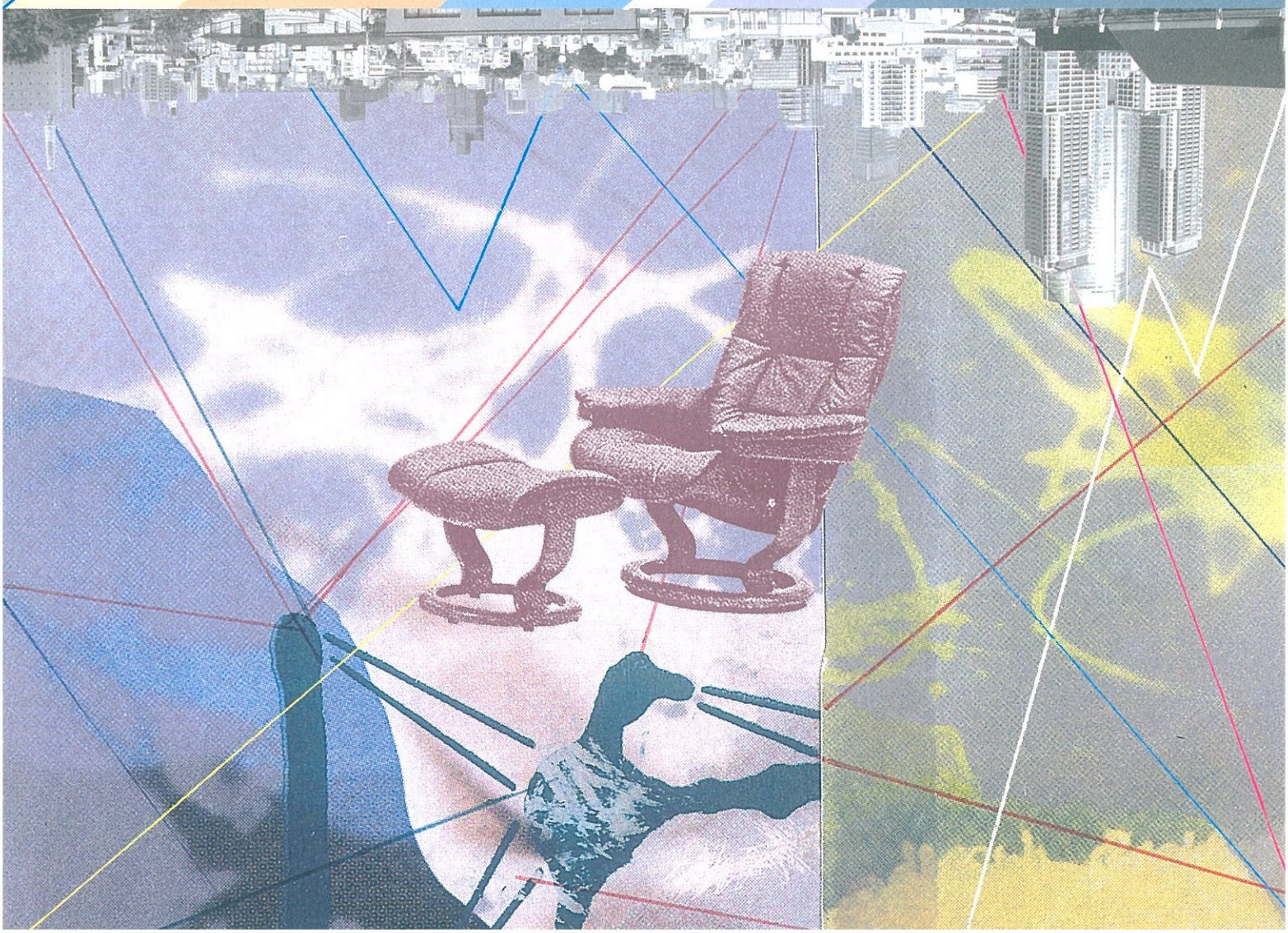
清掃・衛生
設備
保全・保安の
管理総合誌

盗聴防止対策とビルメンテナンス業界

〈別冊付録〉
・建築物環境衛生維持管理要領
・建築物における維持管理マニュアル

編集・発行
㈳全国ビルメンテナンス協会

2008 3



通信傍受（盗聴）防止対策とビルメン業界の今後の対応について

特定非営利活動法人　日本情報安全管理協会
専務理事・事務局長　**佐藤　健次**

情報セキュリティ意識の高まる日本企業

近年、ICT（情報通信技術）の進展により、企業間の競争は激化を極め、日本国内においては、新会社法の改正、さらに2007年５月には三角合併が解禁されたことにより、より企業間の自由競争は加速し、外資系企業に狙われることを脅威に感じている企業も少なくないと思われる。

日本企業は、経済面ではグローバル化が叫ばれて久しいが、一方でセキュリティ面では、まだまだセキュリティ先進国の外資系企業に肩を並べているとは言いがたく、特に国際競争力の源泉として誇れる先端技術および知的所有権を所有する日本企業にとっては、今まで以上に情報セキュリティにおける予防・予知の重要性を認識していく必要がある。

IT革命以後、日本においても内閣官房を中心とし、法制面では個人情報保護法や不正アクセス禁止法、日本版SOX法の制定、それらを運用するための基準として、ISMS認証評価制度、プライバシーマーク制度により、ITを中心としたセキュリティに関しては、対策が進み始めている。

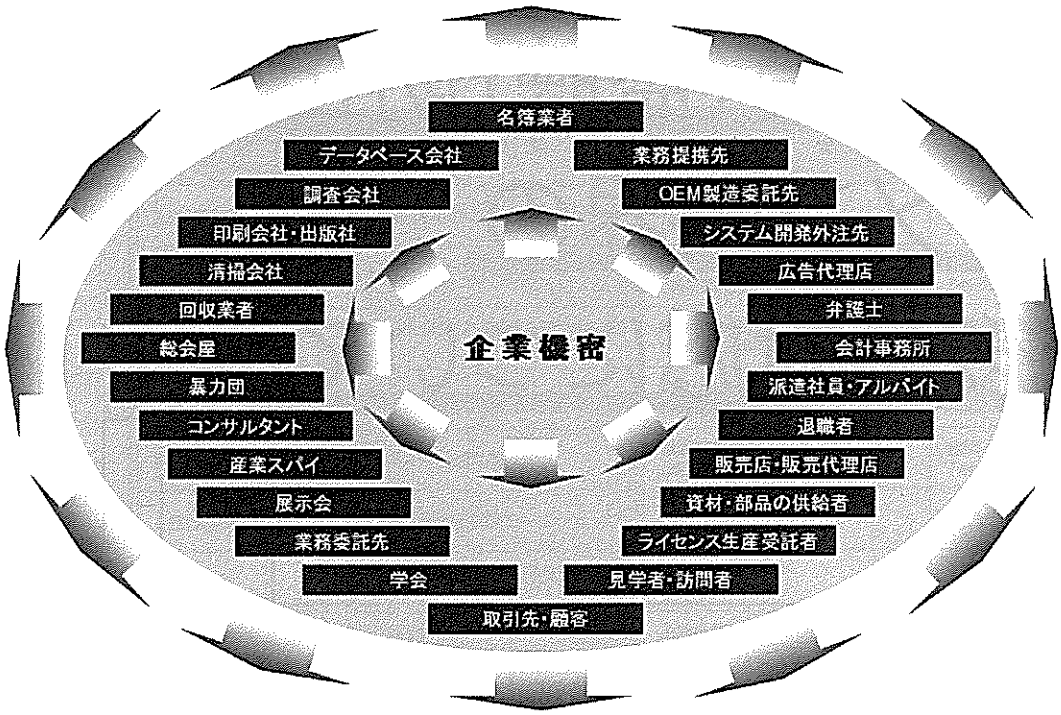
このように、日常的な情報セキュリティ対策が進む一方で、情報窃取のターゲットにされた場合の対策については脆弱性を隠せない。ターゲット企業のネットワークなどに侵入し、財務状況や、株主に関するデータを盗み、新製品開発などの技術情報や海外進出などの経営戦略に関する情報を窃取し、その情報を企業戦略や買収のための重要情報として活用することは、日本では想像もつかないが、欧米ではもはや常識に近い状況である。

もちろん、このようにターゲットに特定されたことを想定して、セキュリティ対策を実施している企業もある。それらは日本企業の中でもグローバル化している企業に多い。

日本でも懸念される情報窃取の手法

情報窃取者は、さまざまな手段や高度な技術に裏づけ

図1　企業機密漏洩のルート



された情報収集方法を用いて企業情報を狙っている。海外では情報漏洩の原因の上位にハッカー（クラッカー）などによる外部からの攻撃が挙げられているが、日本では、外部からの攻撃による情報漏洩については報告が少なく、社内の関係者、つまりは内部犯行による情報漏洩の報告が非常に多い。

例えば、ネットワーク管理者や利用者などから盗み聴き、盗み見などの手段によってパスワードなどのセキュリティ上重要な情報を入手したり、また、オフィスから出る書類のゴミをあさってパスワードや手がかりとなるメモを探し出したり、ネットワーク利用者や顧客になりすまして、電話でパスワードなどを聞き出す方法がとられることもある。本人確認が不十分な場合や、組織内部での機密情報の管理ルールが不完全な場合は、これらの手法によって機密情報が漏洩してしまう。これらの手法は、ある程度ターゲットとなる会社の基礎情報がなければ難しい。

このように、情報漏洩はネットワークシステム（IT）の問題のみならず、ヒューマンファクターに起因する問題も、本来重要視されなければならない。終身雇用の崩壊、人材派遣システムの定着化などによる現在の日本の状況下では、今後ますます内部告発者、退職社員、派遣社員、アルバイトなどによる情報流出が続発していくことが予想される。

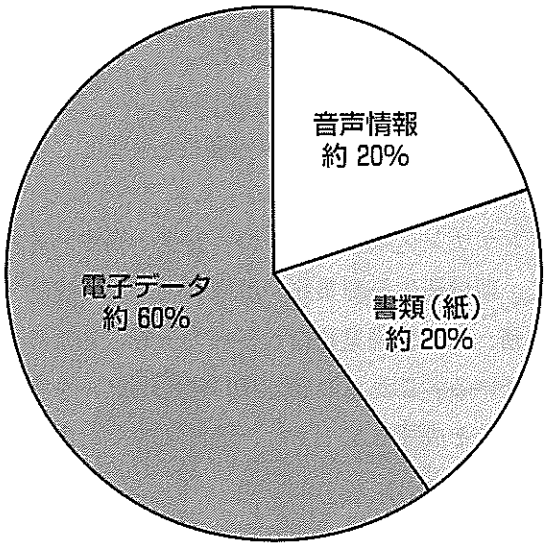
ビルメン業者になりすますこともある産業スパイ

近年、個人情報保護法やISMS認証評価制度などにより、業務委託先への情報管理は徹底されつつあるが、それも十分であるとは言えない。例えば、必ずある程度のデータを共有しなければならない印刷業、コンサルタント、OEM製造委託業者などは、常に厳正な管理が求められる。

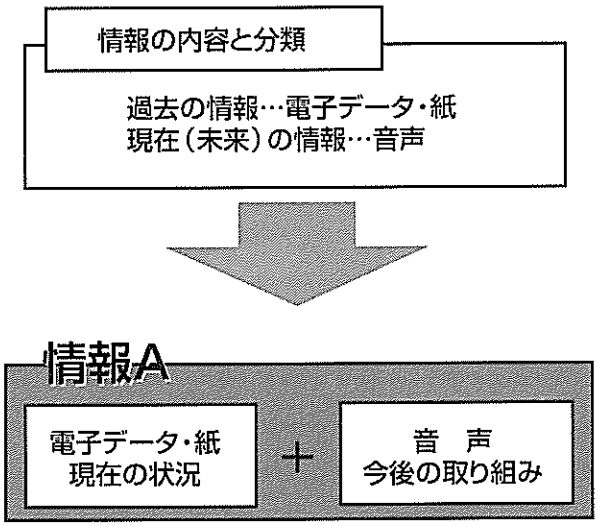
それらとともに、清掃や警備、設備管理を行うビルメンテナンス業者は、クライアントの社内情報に触れる機会が非常に多い。つまり、情報セキュリティ対策の考え方に基づいた場合、機密情報に触れる可能性が十分にある立場と見られている。

ある大手企業では、情報漏洩のリスクを削減させるために、ビルメンテナンス業者と契約する際、機密保持に関する条項を盛り込むようにしているという。

図2　情報の分類



情報の形式は、「電子データ」「紙」「音声」に分類されます。



情報管理者は、1つの管理を得る為に、目的の情報を部分的に把握し、最終的に1つの情報として統合・分析する。

ビルメンテナンス業者は、ビルが無人になる夜間に作業する場合や、アクセスコントロールがなされているビルであっても電球交換等のため、ある程度どこの部屋にも入っていくことができる。

また、日中に作業が行われる場合も、社内の人が常時監視できない作業も多く、その中には機密に触れる作業もかなり多く含まれている。特にゴミ箱に企業の重要情報が捨てられていた場合、その収集過程において意図があるなしに関わらず、情報漏洩の危険が生じる。

そのような理由から、俗に産業スパイといわれる情報窃取者がなりすます職業の一つとして、ビルメンテナンスが挙げられることが多い。ある海外の雑誌では、高度に組織化された情報窃取集団が、ビル清掃の職に応募していた事例が報告されている。

ビルメンテナンス業者には、作業現場で知り得た機密情報等が外部に漏洩しないよう従業員教育を徹底したり、また、情報窃取者が従業員になりすますことを防止する対策をとるなどの努力が求められている。

一方で、ビルメンテナンス業界の清掃担当者が、不審物(情報収集装置など)を発見したという事例も報告されている。もし、ビルメンテナンス業の1サービスとして、通信傍受対策の日常点検が取り入れられるのであれば、クライアントのセキュリティ強度は非常に高まるであろう。

音声情報管理の必要性

通信傍受（盗聴）とは、会話や通話などで話し合われている情報をリアルタイムで窃取できる唯一の方法である。情報は一般的に、「電子データ」「紙」「音声」の3つの媒体に分類することができる。

日本企業の通信傍受（盗聴）による情報漏洩の脅威は、情報窃取者の多くが、情報機関等に在籍したことがある“情報のプロフェッショナル”という点である。プロの情報窃取者から見れば、ターゲットとなる企業のどこにウィークポイントがあるのかが、一目瞭然となるためである。

また、海外の情報窃取者の情報収集能力は非常に高いとされ、会議で発表されるはずの経営トップの決定事項を事前に盗聴によって窃取したり、取引先と取り交わす会話の内容からヒントを得て新規事業の情報を窃取することもある。これらの音声情報に対する管理も、通信傍受対策として、欧米ではごく一般的・定期的に実施されている。

情報窃取者は当然、ターゲットのセキュリティが脆弱なところから情報を窃取しようとするため、情報保全す

るためには、それぞれの情報（電子データ、書類、音声）の形式に合った対策を講じていくことが最重要課題となる。

例えば、海外の大手企業のCEO等のVIPが来日する際には、各VIPが宿泊するスィートルーム、重要な会議が行われる会議室、さらにそれらの部屋に隣接する部屋には、盗聴探査を実施する必要がある。これは情報セキュリティにおける予防・予知の管理という意味で、音声情報の管理の面からも綿密な計画を立てる必要があるということである。

情報セキュリティ・コンプライアンスの重要性

これまで述べてきたように、セキュリティ意識が高まってきている現在では、企業活動に携わる人すべてが、情報セキュリティについて、ある一定の知識を持っていることが求められており、クライアントの信頼を得られる重要なキーワードと考えられている。

セキュリティのノウハウを取得し、サービスの一環として展開することも事業の一つとして考えられるが、先に優先されるべきは、クライアント企業のセキュリティを理解し、それに合わせて、これまで提供していたサービスなどに付加していくことであろう。

我々は、これらを「情報セキュリティ・コンプライアンス」と位置付け、教育プログラムを提供している。受講することによって、現場の担当者のレベルで、「なぜセキュリティを考えることが必要なのか」といった問題から、「ここまで意識して実施すれば、クライアントに信頼される」といった内容までが身につくように設定されている。

ビルメンテナンス業の業務によっては、専門的な資格等が必要とされるものもあるが、これらの情報セキュリティ・コンプライアンスについては、業務内容によってクライアントとの携わり方のレベルが違うため、それぞれの業務によって必要とされる項目と、そうでない項目が分かれる。

つまり一般論だけ勉強しても、なかなか理解するのは難しく、業務内容に合った形のケーススタディを学んでいくことが重要となる。

ビルメンテナンス業界と通信傍受対策

（通信傍受（盗聴）防止対策の必要性と差別化）

ビルメンテナンス業は、ビルの「安全・衛生」をキーワードに、環境衛生管理業務、設備管理業務、建物・設備保全業務、保安警備業務など多岐の分野にわたり、業が営まれている。これらの分野は日常的にビルを管理しているからこそ成せる業であり、他の業界では考えられないほど多様である。

同時に、情報セキュリティの理想的な運用を考えてみると、日常的な運用管理が重要なキーワードの一つであり、これはまさにビルメンテナンス業務と通じるものがあるのではないかと考えられる。

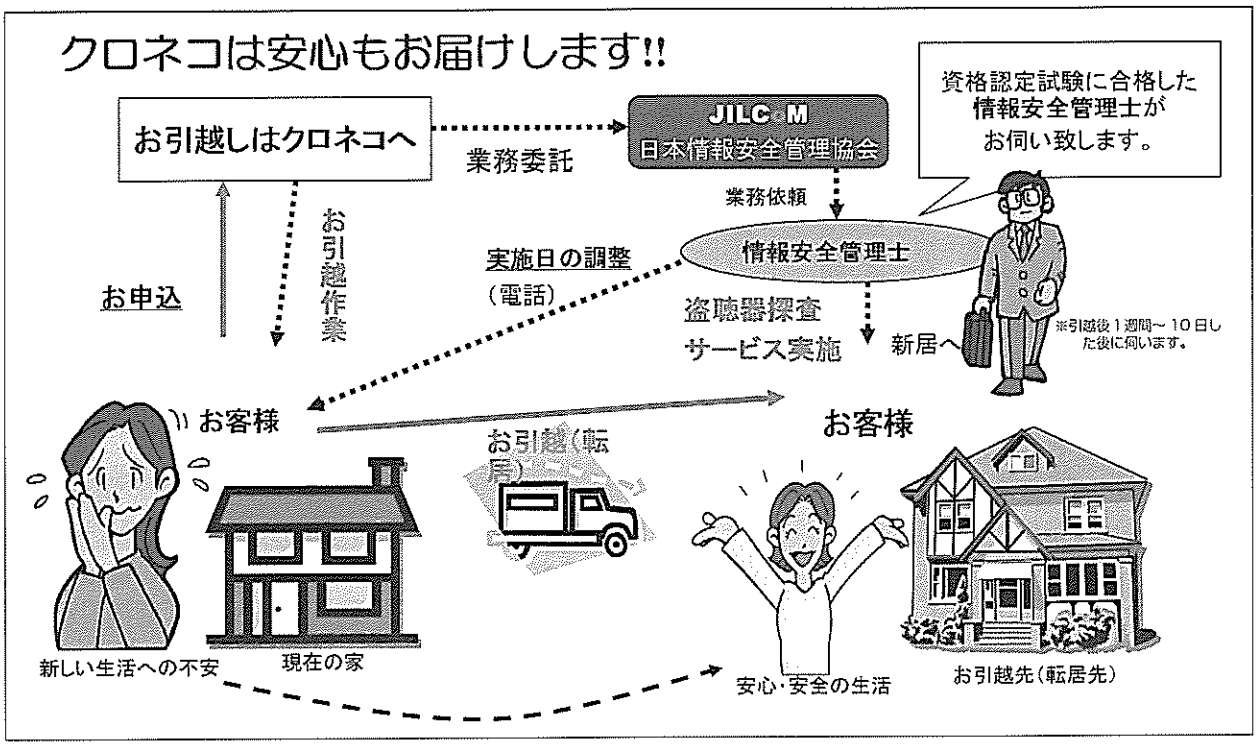
実際に日常清掃業務の中で、担当者が不審物（盗聴器など）を発見したという例も挙げられている。例えばこのような事象において、担当者が専門的な講習または訓練を受けていた場合、適切な対応をとることができ、クライアントのリスク削減に大きく貢献できることは間違いないであろう。

情報セキュリティにおいても、日本では未だに弱い分野であるといわれている通信傍受対策をはじめ、フィジカルセキュリティ（入退室管理）をサービスの一環として取り入れることによって、近年の高まる情報セキュリティのニーズに応えることができ、競合との差別化の一要因になり得るのではなかろうか。特に、通信傍受対策に関しては、ビルメンテナンス業において保安警備業務と電気通信設備などの設備管理業務の中間に位置づけられると考えられる。

我々が察するに、ビルメンテナンス企業の新規事業として、通信傍受対策サービスは十分成立し得るのではないかと考える。

また、常にクライアントのビルに担当者がいるため、日常の目視点検や簡易的な探査作業など、一般的な盗聴探査会社では実施が難しいサービスが提供できると考えられる。通信傍受対策事業におけるサービスの多様化が進むのではないかと推察される。

図３　引越に伴う盗聴探査ビジネスモデル



事例研究：引越（移転）業界と通信傍受対策

日本情報安全管理協会では、物流会社大手のクロネコヤマトの引越部門であるヤマトホームコンビニエンス株式会社と業務委託契約を締結し、「引越に伴う盗聴探査サービス」をスタートさせた。

過当競争業界であると言われている引越（移転）業界においては、引越（移転）そのものだけではなく、それに伴う付帯サービスが、顧客の意思決定を左右すると言っても過言ではない状況にある。その付帯サービスの一つとして、弊協会が提案する「盗聴器探査サービス」が選ばれた。

スタート当初は、細かいサービス内容をいかにエンドユーザまで伝えるかということに重点を絞ってプロモーション展開を実施した。現在では、繁忙期（３月）になると、月間の受注件数が100件（個人向け）を超えるほどで、年間にして250件程度のサービスを展開するに至っている。

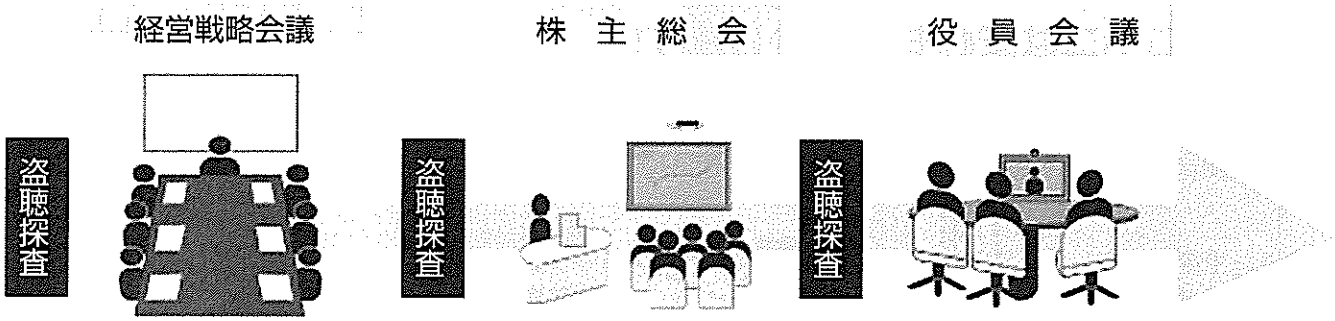
また弊協会では、物流会社の大手である日本通運株式会社の引越・移転部門と業務提携を行い、法人顧客についても移転終了時の安全確認として、「盗聴器探査サービス」を展開している。

これらは、一般的な法人はもちろんのこと、官公庁からも依頼があとを絶たない。

大規模な企業、官公庁の移転は、莫大な費用を要するうえ、オフィスレイアウトやネットワーク通信設備の構築・設計をはじめ、現場鍵管理、養生、情報機器の解体・梱包、電気工事、通信配線工事、内装工事、電気工事、新規購入物搬入・設置、引取・廃棄処理、家具クリーニング、情報機器移設、運搬・設置、運搬物チェック、養生撤去・清掃・建物傷確認等、さまざまな業者が必要となることが多く、これらの調整も含め、一手にどこかにお願いしたいというのがクライアントのニーズである。移転事業者も、これに対応するべくサービスを展開している。

一方で、これらの業務形態は多くの業者が関係してくるため、盗聴器をはじめとする情報収集装置が非常に設置されやすい環境にある。移転後、施設を安心安全にして使用していくためには、移転後の盗聴対策サービスは必要不可欠なサービスであるといえる。これまでの案件については、クライアントから非常に高い評価をいただいている。

図４　通信傍受（盗聴）防止対策実施のタイミングの例



事例研究：警備業界と通信傍受対策

ALSOK綜合警備保障株式会社、株式会社全日警も、弊協会と業務提携をし、通信傍受（盗聴）防止対策サービスを展開している。

警備会社として、常駐警備業務、防災点検業務など、ビルの総合的な警備業務を主業務として展開している両社は、年間を通したクライアントとの商談の中で、盗聴防止対策のニーズの高まっていることを認識し、警備業務の新たな１分野として「情報警備」に取り組むに至っている。

特に、社内における重要会議の前や、大規模な株主総会などに使用する前の施設点検などのニーズが多い。また、セキュリティ対策の一環として常時（年に２回、もしくは４半期に１回）、探査を実施する必要性を十分認識して依頼してくるクライアントも多く、これらは本来の警備業務と同様に、年間で業務契約を締結し対応している。

日本情報安全管理協会の活動

（人材育成・新規ビジネスに関する相談業務）

弊協会では、情報セキュリティに関する啓発活動を主体におき、情報セキュリティの専門資格である情報安全管理士資格認定制度を実施している。

その中でも通信傍受対策の専門資格である通信傍受対策技士は、二種・一種・特殊・総合監理の４段階に分かれており、現在、全国で約200名の有資格者が活躍している。また有資格者の活躍の場として、大手企業との業務提携により通信傍受（盗聴）防止対策サービスを全国的に展開している。

また、コンサルティング事業として、情報セキュリティ・コンプライアンス講習の実施や、弊協会会員企業とのコラボレーションによる情報セキュリティ商品・サービスの開発も行っている。

これまで述べてきたように、情報セキュリティの一環としての通信傍受（盗聴）防止対策は今、注目されている分野の一つである。先日も弊協会の活動が全国紙の新聞の一面に取り上げられるなど、さらなるニーズの高まりを見せている。

このようにニーズが急速に高まっている中、大手企業が参入してくる可能性が出てきており、ますます市場の広がりが期待されている分野である。

この機会に、ぜひ情報セキュリティ、通信傍受対策という分野を新規事業として開拓されることを期待し、また、これらの事業展開により、ビルメンテナンス業界がますます活発化されれば、我々としてはこの上ない喜びである。

（さとう　けんじ／特定非営利活動法人 日本情報安全管理協会
専務理事・事務局長）

■この記事に関するお問い合わせは
特定非営利活動法人（NPO法人）
日本情報安全管理協会
〒108-0073　東京都港区三田2-14-5-712
TEL 03-5765-7677　　FAX 03-5765-3181
URL http://www.jilcom.or.jp