みんなで考えよう日本の安全！

月刊セキュリティ研究

急速に拡大するセキュリティ事業を勝ち抜く

パナソニック SSマーケティング株式会社 代表取締役社長 **森永 洋一郎**

緊急地震速報 **気象庁 地震火山部**

地震の強い揺れが“ここ”に届くまでの秒数を速報

特 集 **危機管理プロダクト 2007**

三井物産エアロスペース　三菱電機インフォメーションテクノロジー
東芝産業システム社　日本SGI　竹中エンジニアリング　美和ロック
アイ・ティー・エス　日本通信エレクトロニック　ポニー工業

2007 10
Security Specialist Association

■ **注目の企業紹介**

ノーネスユニバーシティー　　アラビアンブリッジ株式会社

■ **しあわせ通信**

答えはいつもイエス（Always Say Yes !）

Info
特定非営利活動法人 NBCR対策推進機構
特定非営利活動法人 日本情報安全管理協会
特定非営利活動法人 日本防犯学校
学術社団 日本安全保障・危機管理学会
ASIS International 日本支部

連載 ニーモニックNEWS
ザ・ボディーガード

巻末特集 セキュリティ業界有力企業一覧

日本企業に求められる空間情報セキュリティの意義

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

三角合併解禁により予測される情報戦争

2007年5月より三角合併が解禁された。海外投資ファンドが続々と日本に進出してきている現在では、これまでも日本企業は含み資産が大きい割には株価が安いとされ、M&A（企業の合併・買収）のターゲットとされてきた企業も少なくない。実際、多数の外資系企業が日本企業に対して、活発な攻勢をかけ始めている。

そのような現状の中、日本企業の買収防衛策として、企業価値を向上し株価を上げていくことこそが、基本的対応であるが、一方で、企業間の情報活動への対策も重要な要因であると考えられる。弊協会顧問である宮脇磊介氏は、一般的な買収防衛策を「表のゲーム」、情報戦争のことを「裏のゲーム」と表現（讀賣新聞2007年5月31日「論点」）している。

企業間の競争が激しい欧米では、約20年前より、競合企業間での情報活動が活発かつ日常的に行われている。これは、東西冷戦の終焉により、情報機関に所属していた情報活動の専門家の多くが民間企業に入り、企業情報活動およびその防衛の中核を担っているためであるとも考えられる。

ターゲット企業のネットワーク等に侵入して、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為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のである。

日本の企業は自社が、国際的に広範にわたり繰り広げられている企業間情報活動のターゲットになっていることを認識し、早急に対策を講じることが必要である。日本の企業経営者が先述の三角合併の解禁に臨み、買収防衛策を用意するに当たって、こうした国際標準の情報窃取手法に対する無関心・無用心は、今後の日本企業全体の競争力に関する懸案事項及び危険性を感じざるを得ない現状である。

ITセキュリティの整備だけでは不十分

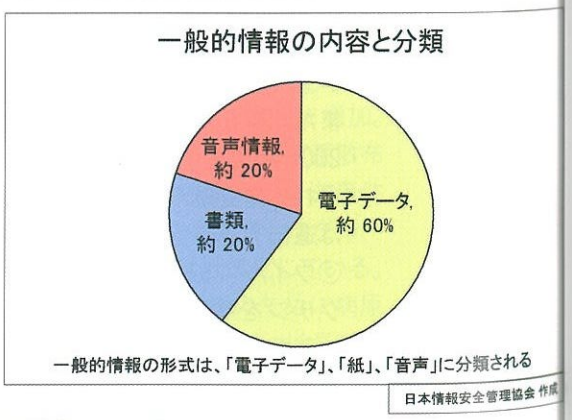
日本では情報窃取のさまざまな対策の中でも、特にITやネットワークシステムの侵入等（パソコン周辺）に対策が集中している。しかしながら、電話・FAXの傍受、オフィスや会議での情報窃取（盗聴）は、海外の情報窃取者にとってみれば、ごくごく一般的な手法である。しかし、日本ではこうした活動に関する知識が乏しく、警戒心も薄いのが現状であり、このような状態では、外資系企業との企業間における情報活動に勝てるはずはない。

なぜ情報安全対策が重視されないのかについては、前述の宮脇氏は同紙において「日本では文系出身の企業経営者が多くITを使いこなす知識に欠けている上、技術者、それもネットワークの技術者に丸投げしているところに原因がある。」と日本の経営文化の歴史的な背景まで原因があると指摘している。

また、現在では多くの認証・規格等を多くの企業が取得しようとしているが、かれらの多くは、認証を取得することが目的となってしまい、情報セキュリティ対策を運用していく重要性の認識が薄くなってしまっている。尚且つ、それらの認証等の基準は、ITやネットワークによるものが中心であることが多く、日本の企業では、ネットワークシステム管理に関する国際標準規格の認証を受けさえすれば、情報安全対策が講じられたと認識する傾向があるからであると考えられる。

しかしながら、情報窃取はITの技術によるものだけではなく、物理的に書類を持ち出すことや会話を盗み聞くこと（盗聴）による情報窃取も行われる。

物理的セキュリティについては、書類の管理は行われているが、音声情報窃取に対する対策は不十分であると思われる。



日本企業のセキュリティに不足している空間情報セキュリティ

通信傍受（盗聴）は会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。

日本企業の通信傍受（盗聴）による情報漏洩の脅威は、情報機関に在籍したことがあるプロフェッショナルな情報窃取者によって、情報が窃取されるという点にあるであろう。彼らから見れば、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為である。

また、海外の情報窃取者の情報収集能力はとても高いとされ、経営トップの決定事項、新商品開発情報、取引先と取り交わす内容をはじめ、新規事業情報、資金運用情報、取引先や顧客情報、役員や社員の情報など、情報が窃取された場合、事業継続が困難となることもあり得る。

これら音声情報に対する管理も通信傍受(盗聴防止)対策として、欧米では定期的に実施されている。国内における意識と対策は欧米諸国のそれとはだいぶ開きがあるようである。

情報窃取者は、セキュリティの脆弱なところから、情報を窃取する為、情報を保全するには、それぞれの情報(電子データ・書類・音声)の型式に合った対策を講じていくことが必要となる。

本来、情報セキュリティが適用されるべき範囲は、情報が発生してから廃棄されるまでであり、その間は情報が窃取されないよう保全対策をとることが必要である。

情報は発生から、保管、活用、廃棄のサイクルを踏む。一般的には、情報を保管する際には電子媒体や紙媒体が用いられ管理されるのであるが、発生時や活用している際の会話(打ち合わせ、会議等)については、充分な管理がなされているとは言えない。

会話を聞かれたとしても同じ情報が窃取されてしまう危険性があり、その情報を保全し、有効的に活用する為にも、会話をする上で安全な空間なのか確認する(盗聴対策=音声による情報窃取対策)対策を行うことが重要となる。

第17回　通信傍受対策技士二種 資格認定試験ご案内

通信傍受対策技士とは、盗聴器・盗撮機器の探査を実施するための技術、知識、コンプライアンスを有し、そのセキュリティに関する水準が認められた方を言います。

1. 情報安全管理士・通信傍受対策技士の業務
   - 盗聴器・盗撮機器の探索・発見業務
   - TSCM(テクニカル・サーベランス・カウンター・メジャー:電子的監視対抗措置)
   - 盗聴・盗撮対策のセキュリティコンサルティング
   - 建物内の情報漏洩ルートの分析・レポート
   - 新盗聴技術に関する対策技術研究・開発
2. 資格取得のメリット
   - これまで、ガイドラインのなかった通信傍受対策技術を一元化された基準において、資格認定を受けることによって、顧客からの信用をより一層深めます。
   - 経験者もこれまで自己流だった技術・知識を客観的に試すことができるチャンスです。
3. こんな方に適しています
   - 盗聴器の探査・発見業務に従事している方
   - 盗聴対策技術に興味のある方
   - 一般住居の防犯関連の仕事をされている方
   - 企業内情報セキュリティのご担当者
   - 盗聴器・盗撮機器に対して自分自身で防衛したい方
4. 開催予定

資格種別	回次	開催日	開催地(受験会場)	定員	受験申請受付期間
二種	第17回	2007年11/11(日)	東京会場	50名	9/3(月)～10/31(水)

5. お申込について

   募集期間の間、当協会のホームページ上にて「受験申込書」をダウンロードして必要事項を記入の上、FAXまたは郵送にてお申込み下さい。受験申込書を受付次第、受験票等の関係書類を送付させて頂きますので、受験申請手続きを行ってください。詳しくは協会事務局までお問合せ下さい。

   URL:http://www.jilcom.or.jp
   TEL:03-5765-7677　FAX:03-5765-3181
   郵送:日本情報安全管理協会 事務局宛
   〒108-0073　東京都港区三田2-14-5　7F

6. 試験当日のタイムテーブル

※時間割は会場の都合などにより、一部変更することもございます。

第17回　二種　　2007年11月11日

10:00	会場受付開始
10:15～10:30	協会挨拶・連絡事項
10:30～12:00	筆記試験(90分)
12:00～13:00	休憩
13:00～17:00	技能試験(実技)
	面接試験

お問い合わせ先
特定非営利活動法人 日本情報安全管理協会 事務局　担当:槇
〒108-0073　東京都港区三田2-14-5　7F
TEL:03-5765-7677　FAX:03-5765-3181
URL:http://www.jilcom.or.jp　E-MAIL:jilcom@aioros.ocn.ne.jp