日本の安全安心考えます！

セキュリティ研究 112

March
2008

特集　2008年春 注目のセキュリティプロダクト

アクシスコミュニケーションズ　アムテックス　池上通信機　エア・ブラウン
クマヒラ　ＣＢＣ　スタンダード　スリーディー　セントラル警備保障
タムロン　チェックポイントシステムジャパン　ティービーアイ　ドッドウエル ビー・エム・エス
日本通信エレクトロニック　日本ビクター　ビデオテクニカ　朋　栄
松下電器産業　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

しあわせ通信　まだまだもっと、いい騎手になりたいですね

日本中央競馬会 騎手　武　豊

巻末特集　SECURITY BUSINESS INFORMATION

通信とヒトにおける通信傍受対策の考え方

特定非営利活動法人 日本情報安全管理協会
技術課長 槇　良

通信の歴史

情報通信の歴史は、狼煙、枕木通信、旗旒信号、手信号、郵便と様々な方法が使われていた。中には現在でも使われているものもある。電気通信は、18 世紀に電信・電話が発明され、離れた者同士の疎通は高速化を増した。その利用は国内外に渡り時には争いにも用いられてきた。

また、通信内容も電信電報から音声通話、伝送模写（ファクシミリ）、電子メール、画像・動画伝送と、この百数十年に目まぐるしく発展していった。伝送方式にあっても銅線から光を利用した有線通信、時間や場所を選ばない無線通信と変化させていった。現在の利用者は個人まで広がり、誰もが公私問わず 24 時間 365 日間自由に疎通を図ることが可能である。

今更ではあるが、「通信（Communication）」とは、「人がその意思を他人に知らせること」又は「離れた人と人が意思疎通を図る」とある。

企業活動においては「意思」や「疎通」の中には「情報」が含まれていると同時に「価値」が生成される。

「価値」即ち「利益」あるものには、必ず不正に入手しようとする者がいることを認識しなければならない。その対象は有形無形を問ないと言っても過言ではない。情報窃盗がそれに該当する。我が国では「窃盗」とは有形物に対するものしか適用されなかったのが現状である。

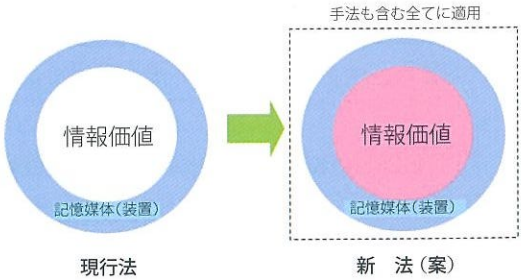
法律の規制

法の規制について、近年多発している事例を参考にすると、ハードディスクや外部記憶媒体などの物理的記憶装置の窃盗で適用していた。

例えば、数億円の価値のある経営情報が保存された記憶装置が持ち出されたとしても、容疑は原価償却で換算した装置の数千円程度を窃盗したものとして罰せられているのが現状であった。これは、我が国にとって国益に関わる深刻な問題であった。また、情報そのものだけではなく、手法についても適用されることになる。

現在審議中である「情報窃盗罪」「産業スパイ罪」等は無形も適用することが盛り込まれている。

このことから、今までの認識で社外に仕事を持ち出し外から連絡、書類の作成をしたことによって、その行為が罰せられる恐れがある。無論、既に社内規定で定めている法人もある。しかし、未整備であるところでは、取り扱う事業によって異なるが、場合によっては社内規定違反ではなく、法によって罰せられることが予測される。



法による情報保護

日常の留意事項

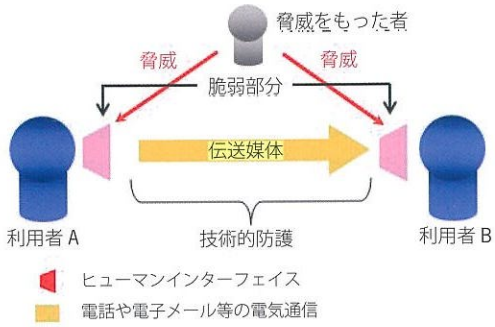
日常業務においても、一見気に留めないような些細なところに脅威があることを認識しなければならない。以下の例を挙げてみる。

- 会議・日常会話
  - (1) 第三者の入り込む余地のある場所
  - (2) 他の部署に隣接する場所
  - (3) 静粛な場所
- 電話連絡
  - (1) 大声での送話
  - (2) 私用の携帯電話機
  - (3) 事業用アナログコードレスフォンの使用
- 電子メール
  - (1) 無暗号のメール
  - (2) フリーアカウントの使用
  - (3) 私用アカウントメール
- 就業後
  - (1) アルコール類の摂取できる店舗での反省会
  - (2) 家族に職場内の状況報告
  - (3) 同期への近況報告（特に同業職での従事者）

傾向として、個人の防護基準意識が低下しやすい場所や場面として社内より社外、就業時間より就業後の時間、取引相手より同僚、物品については公用備品より私物と気持ちが切り替わることを経験した方も多いのではないだろうか。先に述べた事例ではあえて、電気的なもの以外についても触れている。理由としては、システムの技術的防護だけではない。それらに介在する人間が自身についても防護手段（意識・認識）をもたなければならない。よって、パーソナルコンピュータにウィルス対策ソフトウェアをインストールするように、個々自身にも第三者からの脅威に対する対策意識を持つことが必要となる。

危機管理としての通信傍受対策について

通信とは、電気通信だけではなく、かつての手振り身振りで行っていた、生身での通信も含まれるのではないだろうか。少々大げさな表現ではあるが、いつ何時に狙われるか分からないのである。情報窃取者は常にその隙を伺っている。



ヒューマンインターフェイスの脆弱部分

危機管理とは、経営責任者に課せられたものだけではなく、組織の末端まで心得なければならい。少々息苦しいが、高度高速化された現代社会の中で戦う人間にとっては致しかたない。かつての日本では隣人同士の環境が近いところにあり、相互監視や秩序の維持が無意識に行われていた。

この考えを少し活用してみてはどうだろうか。同じ利益を追求する者同士、意識して注意喚起することによって、一人ひとりの負担軽減や軽微な事故を防止できるものと考える。

やはりヒトとヒトの意思（情報）疎通における「と」にあたる部分が電気や電気以外の方法であっても末端はヒトの視聴覚によるものである。情報媒体の種類に関わらずそれらを取り扱うヒューマンインターフェイスにも視野を広げた通信傍受対策につい考えてみるのも良いでのではなかろうか。

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
〒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