みんなで考えよう日本の安全！

月刊セキュリティ研究

警戒心が希薄な「丸裸の国」の構造的な危機

財団法人世界平和研究所 研究顧問　宮脇磊介

危機管理体制

三重県　危機管理の先進的な取組「リスク把握取組」

特集 Event Watching

第2回 オフィス セキュリティEXPO

2007 8
Security Specialist Association

■注目の企業紹介
株式会社 ヘルシー・ワークス

■しあわせ通信
教育にとって大切なこと

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
防犯・防災グッズ

巻末特集 セキュリティ業界有力企業一覧

多様化する情報窃取の脅威

～狙われるディジタル情報社会に埋もれる重要アナログ情報～

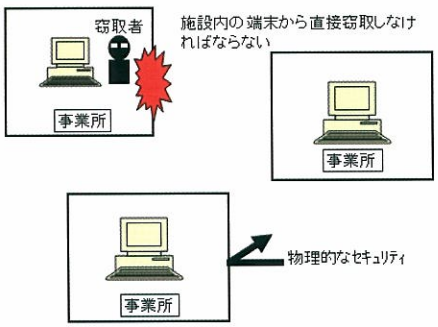
特定非営利活動法人 日本情報安全管理協会
技術課長代理　槇　良

電子計算機が国内で個人情報を取扱、処理し始めたのは1960年代で東京・大阪・名古屋の三大都市から導入が始まり、他の地方都市においても順次導入が開始された。これにより膨大な情報を瞬時に処理できるようになり飛躍的に処理速度を向上させた。当時、各拠点で処理していたが、1980年代頃からそれらの処理は専用線によって接続され、点から線となりネットワークが構築された。また、閉鎖的ネットワークから公衆網であるインターネットに接続され現在に至る。これらの経緯から個人情報が取り扱われる経路はより大衆の間を通ることになる。

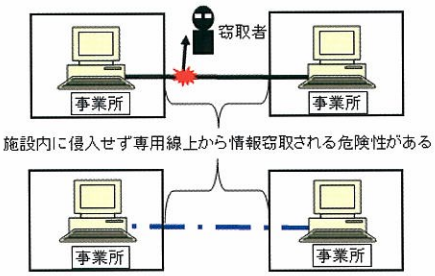
例えば、これらの情報を窃取しようと考えた場合、電子計算機を導入した当初であれば、その施設内に侵入し直接情報を窃取しに出向く必要があった。しかし、これはある意味物理的なセキュリティとして強固であったと考えることができる。無論、当時のソフトウェア技術を考えると現在の認証システムと比較にならないであろう。

しかし、施錠された施設は現在のハイテクとは劣るものの間接的に情報セキュリティ対策がされていたといえる。

よって、情報を窃取しようとした場合、施設内に不法侵入する他に、間者（スパイ）を従業員から取得するか、本人が成りすましなどして職場に採用されなければ、電子計算機に近づくことは出来なかったのである。

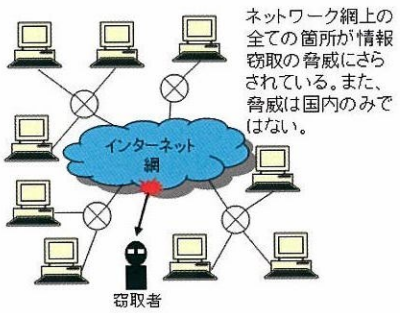


各拠点での情報処理システム



専用線に接続された端末

現在はどうだろうか。先に述べたように拠点間を結ぶ通信網は公衆網であるインターネット網に接続され多くの人々が便利に携帯電話端末や自宅のパーソナルコンピュータで自由に届出や申請、照会が可能となり利便性は飛躍的に向上している。しかし、言い換えれば、個人情報は一般の人々の端末まで広がっているといえる。これは先に述べたように、わざわざ対象となる施設へ侵入することなく、自宅や外出先などで情報を窃取できるということである。1980年初期のマルチメディアという言葉が出てきたキャッチフレーズである「いつでも　どこでも」といった具合である。その後、企業をはじめ個人利用者まで、その需要は拡大していった。しかし、人間の性とも言うべきなのか、利便性を感じるあまり、多くの利用者は、安易に個人（企業）の識別情報を入力する傾向にある。無論、各利用者も危険であることは認識していないわけではない。また、このことは各関係機関から喚起されていることも、承知の上であるが、今一度、書面上の規定だけではなく利用者単位で考え直す必要があるといえる。



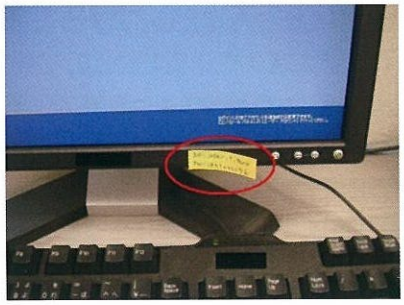
ネットワーク化した通信網

例を一つ挙げると、ある職場内の特定従業員に対して勧誘販売員を装い施設内に入り、個人情報取扱の担当者の机まで行く。そこには情報通信システム課（室など）から支給されたパーソナルコンピュータが置かれ、機械にあまり明るくない職員は、覚えにくい数字と英字のログイン名とパスワードはディスプレイの画面横に付箋紙で書かれている。それを販売員に装った窃取者が暗記し持ち帰る。そして、ネットワーク上にデータを公衆網に接続するための装置や機器を混入させ、あとは、空いた時間にインターネットカフェなど不特定多数の人間が出入りするところから情報を窃取する。例え不正アクセスのログが上がったとしても情報を最終的に抜いた場所まで特定できたとしても犯人の素性まではたどり着くことは困難である。

このように情報を引き出すという行為に必ずしも機械だけを使用して窃取するとは限らないことである。ここでは、パスワードを入手する際に人間の目によるアナログ的手法で盗まれている点である。確かにセキュリティソフトウェアは人間に代わり 24 時間常時休むことなく監視をしているが、それはあくまでも対象は、ディジタルデータのみでしかないことである。

情報とは何も活字だけではなく肉声や行動なども含まれている。確かにディジタルデータはアナログ情報と違い品質の劣化はほとんどなく、瞬時に複製が可能であること、ネットワークに重畳することにより情報が瞬時に伝わる（流出）ことで、被害の拡大を食い止めることは非常に難しく、追跡も著しく困難であることは事実である。

セキュリティの一部を強固にしてその他の部分については、丸腰状態では、歪なセキュリティホールとなりせっかく巨額な投資を無駄にしてしまう恐れがある。



ID とパスワードの書かれた付箋紙

セキュリティホールを小さくするためには、ディジタルデータだけに注視するのではなく、アナログ情報にあるような音声（肉声情報）や映像（行動情報）などにも目を向けなければならないのではないだろうか。　バランスの取れた統合情報管理の見直しが急務と感じられる。

繰り返すが窃取者は、常に手法を変えて脆弱部分を狙ってくる。

セキュリティに関する法律や制度などあっても情報窃取には決まった方法がないことをここで再度認識、意識することを求めていきたい。

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