Against Cybercrime 2009

企業における情報セキュリティの具体策

① 持ち出しルールの構築

パソコンや記録媒体の持ち出しには、情報流出のリスクがともないます。持ち出しには責任者の許可を必要とし、持ち出しの記録は一定期間保存するルールを定めてください。

また、不必要な持ち出しを許可しないこと、必要のなくなったデータは直ちに削除することなども、持ち出し対応の媒体（モバイルメディア）を利用する際のガイドラインとして定める必要があります。

被害実例

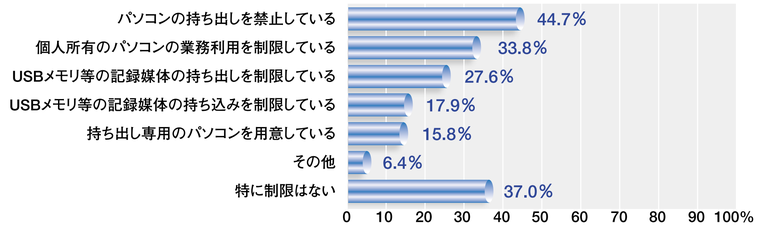
ノートパソコン持ち出し中の盗難

A中学校の教師が帰宅途中に飲食店に立ち寄ったところ、車上荒らしにより生徒の個人情報が保存されたノートパソコンを盗まれた。

記録媒体持ち出し中に紛失

B社の従業員が電車内で居眠りをしていたところ、顧客の個人情報が保存されたUSBメモリを鞄ごと紛失した。

パソコン等の事務所への持ち込み、持ち出し制限の実施状況



「平成19年度　不正アクセス行為対策等の実態調査（警察庁）」

② 廃棄・再利用の際のデータ消去

パソコン・記憶媒体を廃棄するときは、記録データを完全に消去することのできる専用ソフトを使用してください。あるいは、消去作業の信頼性を保証するために消去済の証明書を発行してくれる専門業者に委託してください。

被害実例

C研究所が、リース契約満了後、個人情報や機密情報を消去せずにパソコンをリース会社に返却したところ、同パソコンがインターネット・オークションで売買された。

③ 委託業者の管理

システムの構築・運営を外部委託した場合は、委託業者に対しても、社内と同様の情報セキュリティ対策をとるように監督する必要があります。

被害実例

D社から業務委託を受けた会社の社員が自宅のパソコンに顧客情報を保存していたところ、ウィルスに感染し、顧客情報が流出した。

④ 建物・オフィスのセキュリティ対策

情報セキュリティ対策の基礎となるのが、建物・オフィスのセキュリティ対策です。外部からの侵入や社員の不正行為などによる被害を防ぐため、各室の重要度に基づいてセキュリティレベルを設定し、レベルに応じた入退室管理や防犯設備の設置を行いましょう。

- **社員・部外者の出入りに際して、入退室手順を定めましょう。**
- **機器の設置・保守作業の際には担当社員が常に付き添い、必要なセキュリティ機能が適正に設定されることを確認しましょう。**
- **セキュリティレベルの高い部屋には常に施錠を行い、入退室の記録をとりましょう。**

⑤ “悪意のあるソフトウェア”への対策

コンピュータやシステムに被害をもたらす不正なプログラムは「悪意のあるソフトウェア」と呼ばれ、ウィルス、ワーム、スパイウェアなどがこれに含まれます。これらは、企業活動を停滞させるばかりでなく、情報漏えい等によって社会的信用を失墜するなど、深刻なダメージを企業に与える可能性があります。ウィルス対策ソフトをはじめとするセキュリティソフトの導入は、今や企業にとって必須のものとなっています。

悪意のあるソフトウェアやその他のサイバー犯罪に関する以下のサイトを参考にして、悪意のあるソフトウェアへの対策を検討してください。

- **警察庁 / サイバー犯罪対策**
  http://www.npa.go.jp/cyber/index.html
- **独立行政法人情報処理推進機構（IPA）/ セキュリティセンター**
  http://www.ipa.go.jp/security/index.html
- **有限責任中間法人JPCERT / コーディネーションセンター（JPCERT/CC）**
  http://www.jpcert.or.jp/

用語解説

ウィルス・ワーム

ユーザーが意図しない動作を行うプログラムを（広義の）ウィルスといい、次のいずれか一つ以上の機能を持つ。多くの場合は何らかの被害を及ぼすように悪意を持って作られる。

- 感染：他のファイルやホストに自分自身をコピーする。
- 潜伏：特定の発病条件（時刻など）が成立するまで待つ。
- 発病：ファイルを破壊したり、他サイトのホストに攻撃を開始したりする。

狭義のウィルスは、単体で動作することなく、プログラムや文書ファイルなどに感染する。また、ネットワークを利用して、他のホストに自分自身のコピーを送り込んで自己増殖し、ファイルには感染せずに単独のプログラムで動作するものはワームと呼ばれる。

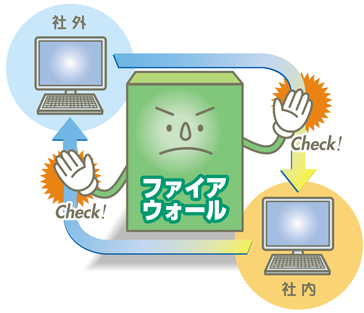
スパイウェア

ウィルスのようにパソコンに侵入し、キー入力、画面表示、ハードディスクの保存データ等から個人情報等を盗み、悪意のある者に送信するプログラムです。

スパイウェアへの対策としては、不審なCD-ROMやソフトを使用しないこと、スパイウェア検出機能付きのセキュリティソフトを使用すること等が挙げられます。

⑥ ネットワークのセキュリティ対策

情報通信のリスクを回避するため、ファイアウォールの設定や侵入検知システムの導入など、必要な安全対策を実施してください。また、外部からインターネットによって社内LANに接続できるリモートアクセスが普及していますが、利用者の認証を厳格にして社内のネットワークを保護してください。



用語解説

ファイアウォール

インターネット上からの不正なアクセスを遮断し、パソコンや社内LANなどのネットワークを保護するためのシステム（ソフトウェアまたはハードウェア）。

侵入検知システム

ネットワークを監視し、ネットワークへの不正なアクセスを検知し、ネットワーク管理者に知らせるシステム。