社内における情報セキュリティ対策

1 持ち出しのルール

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伴います。不要な持ち出しは行わないようにし、持ち出す際は許可を得て、記録を残すようにしましょう。持ち出す可能性のあるパソコン等に日頃から必要のない情報を入れないことも大切です。

事　例

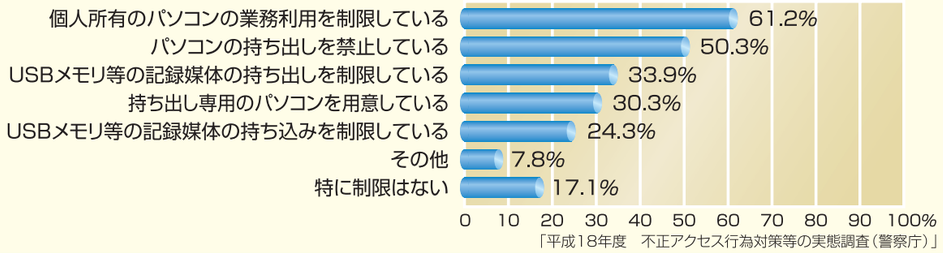
ノートパソコンの持ち出し・盗難

N病院の医師Xは、論文の執筆を行うためにパソコンを持ち出し、帰宅途中に出席したパーティ会場にて、そのパソコンを盗まれた。パソコンには、20数名の患者の個人情報が含まれていた。

記録媒体の持ち出し・盗難

T社では、販売代理店の従業員が社用で使用した自動車が車上ねらいに遭い、個人情報数万人分を記録したUSBメモリーが盗まれた。

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18年度　不正アクセス行為対策等の実態調査（警察庁）」

2 パソコンや記録媒体の廃棄／再利用

パソコンや記録媒体の廃棄に際しては、情報の流出を防ぐために、データ消去が確実に行われるよう専用のソフトウェアを利用し、処理してください。データ消去の証明書を発行してくれる専門業者を活用してもよいでしょう。

事　例

パソコンの廃棄

X市の職員がごみ収集場に捨てたパソコンから、市道用地買収に絡む地権者名や保証金額などの個人情報を含む文書100件が流出した。市職員は、パソコンを道路に数回叩き付け廃棄したが、ハードディスク内の情報は消えていなかった。通行人がパソコンを持ち帰り、情報が流出した。

3 委託先管理

システム構築や運営を外部委託する際には、委託先に対しても社内と同様に情報セキュリティ対策を確実に行うよう監督する必要があります。

事　例

委託先による情報漏えい

A社のクレジットカード会員約56万人の個人情報が漏えいした。情報漏えいは、信販会社のシステム構築及び運営を委託されていた委託先業者によるものであった。

4 物理的なセキュリティ

■情報セキュリティ対策の基礎となるのが、物理的なセキュリティです。内外部からの不正な行為から組織を守るために、物理的な区画を設け、重要度に応じた管理を行いましょう。

■外部との出入りに関しては定められた手順を守り、機器の導入や保守作業などには担当者を同伴させ、必要なセキュリティ機能や設定が確実に実施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エリアには、施錠を行い、入退室の記録を取りましょう。

5 悪意のあるソフトウェア

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を「悪意のあるソフトウェア」と呼びます。ウイルス、ワーム、スパイウェアなどが含まれます。ウイルス被害が増大していることから、ウイルスを作成したり、送信することなどを罰するため刑法の改正が国会で審議されています。一方、ウイルス対策ソフトウェアの導入とこまめな更新は、もはや常識です。

ウイルス被害に遭わないために次のサイトを参考にして、ウイルス対策ソフトウェアやIT機器のベンダーの提供する情報を確認し、対応してください。

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/

検 挙 事 例

フィッシングを利用した詐欺

無職の男（34）らは、インターネットオークションの偽のログイン画面を設置し、その偽ログイン画面へ誘導する電子メールを利用者に送信し、これを本物のログイン画面と誤信した会員が入力した識別符号を不正に入手した。
そして、当該識別符号を使用して同社のコンピュータに不正アクセス行為を行い、同社オークションにおいて商品を売ると偽り多数の落札者から代金をだまし取った。平成19年1月、不正アクセス禁止法違反、詐欺罪で検挙した。
（警視庁、熊本、岡山、広島）

フィッシング

フィッシングとは、銀行等の実在する企業を装って電子メールを送り、その企業のウェブサイトに見せかけた偽のウェブサイトに誘導し、金融情報や個人情報を入力させ、不正に入手する行為のことです。

スパイウェア

スパイウェアとは、ウイルスのようにパソコンに侵入し、打鍵（タイピング）、画面表示、ハードディスク等から個人情報等を盗んで悪意のある者に送信するプログラムのことです。こうして盗まれた個人情報等が悪用されて銀行口座から預金を引き出される被害が発生しています。2005年7月には、インターネットバンキングの利用者をターゲットとしたスパイウェアが出回りました。インターネットバンキング用のID・パスワードを盗まれ、これを利用した不正送金の被害も出ています。スパイウェアの対策としては、不審なCD-ROMやソフトウェアを使用しないこと、スパイウェア検出機能付ウイルス対策ソフトを使用すること等が挙げられます。

6 ネットワーク接続

情報通信のリスクを特定し、ファイアウォールや侵入検知システムの導入・運用など必要な管理策を行ってください。インターネットの普及により社外から部内LANに接続するリモートアクセスが幅広く活用されるようになりました。リモートアクセスを行う利用者を認証・識別し、社内ネットワークの保護を行いましょう。

ファイアウォール

ファイアウォールとは、社内コンピュータネットワークと外部ネットワークとの間に置かれ、外部から社内、又は社内から外部への通信を制御し、不正な通信は遮断するなどにより社内ネットワークの安全を維持する装置又はソフトウェアです。

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です。