CyberCrime Control Project

～　個人情報流出への備えは大丈夫ですか　～

平成 26 年 9 月

広島県警察本部
サイバー犯罪対策課
082-228-0110

■　個人情報漏洩事件の発生とその影響

本年 7 月に発生した大手企業の個人情報流出事件では，約 2,000 万件の住所・氏名・生年月日・性別・電話番号などの顧客情報が流出し，当時補償費用として 200 億円が用意されたことなどが報じられました。

ネット上の損害賠償要求に関する試算の一つに，3,000 人の個人情報が流出した場合，保障や対策費用に約 4,500 万円がかかるとも言われているようです。

一度情報流出事案が発生すると，企業の信用の失墜はもとより，取引の停止，賠償請求などにより甚大なダメージを被ることになります。

報道によれば，今回の事件の直接原因は，導入していたセキュリティシステムの設定ミスあるいは不備ではないかと推察されています。

また，高いデータベースアクセス権限を持つ人物に対する監査が，充分に機能していなかったことも考えられます。

情報流出を完全に防止できる対策というものは存在しないと言われていますが，多数の対策を組み合わせていくこと（多層防御）が，リスクを減らすことは間違いないところです。今一度，自社のシステムを再確認してみてください。

■　情報漏洩対策

こういった情報漏洩に対する対策としては，大きく次の２点が考えられます。

１　自社のセキュリティ体制の確立

(1) セキュリティポリシーの作成と実施

情報システムを危機管理の立場からどのように運用していくかを具体的に定めたものが「セキュリティポリシー」です。

今回の事案であれば，単独による高機密情報へのアクセスはできないようなポリシーの導入も有効と思われます。（入出力担当者と開発者の分離など）

当然，データへのアクセス権は必要最小限に限定し，随時アクセス記録を監査する体制と知識が必要で，たとえ社長であっても不必要な場合はアクセス権を与えないという姿勢が必要です。

また，物理的に機密情報へアクセスできる端末を限定したり，設置場所を考慮するなどの対策も有効です。

(2) セキュリティ体制と責任所在の明確化

自社情報資産の棚卸しにより，重要機密情報とその流出時のリスクを明確にし，管理体制や責任所在を明確にしておく必要があります。

(3) 事案発生時対応の事前策定

万が一，事案が発生した場合に備えて，対応マニュアルを予め作成しておくことが，事業継続に大きく影響します。

また，個人情報漏洩保険などを掛けておくとも検討しておくべきでしょう。

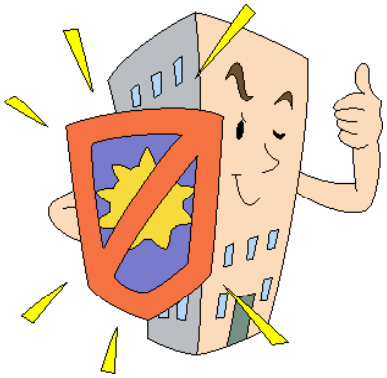
(4) PDCA サイクルによるポリシーの推進と社員教育
定期的に，画一的にならない具体的事例を示した教育が必要です。
（PDCA とは事業活動の管理業務を効率的に推進する手法の一つ）

(5) 委託先管理の徹底
システム開発・運用を外注する場合は，下請け・孫請け，派遣社員など委託（再委託）先への秘密保持に関する契約は必須です。
また，開発に必要なデータの利用制限をかけると共に，その利用記録に係る検証を他人任せにしないことが重要です。

(6) セキュリティ知識を有する社員の育成
本来は，自社内に情報セキュリティに関する幅広い知見を持つ人物を育成するのが望ましいところですが，それが困難な場合は，部外コンサルティング等にセキュリティ診断や監査を委託することも可能です。また，委託すると，最新のセキュリティリスクに対し，柔軟に対応することが可能となります。

2　セキュリティシステムの導入

今回の事件を防止する具体的なシステムとしては，



- ○　入出力装置接続制限システム
  未登録の USB メモリなどを接続できなくする機能
- ○　入出力履歴記録システム
  入出力を行った履歴を記録する機能
- ○　アクセス権管理システム
  データベースや機密ファイルへのアクセス権等を一括管理する機能
- ○　ファイルアクセス履歴記録システム
  ファイルの生成，変更，改名，印刷，削除，読み込み等を記録する機能
  情報システムへのログイン記録だけでは不十分です。
- ○　暗号化システム
  ファイルを入出力する際に自動的に暗号化するなどの機能

などが考えられますが，単にシステム導入するだけでは意味が無く，導入したシステムについて管理者自らが知識を持ち，各種の操作履歴から不審な動作を発見できる能力が必要となります。

また，投資費用を軽減するためには，従来からあるシステムを組み合わせた多層防御手法や OS 標準搭載機能の活用なども有効です。

3　その他

意外に忘れがちなのは，WindowsXp などの古い OS の利用です。インターネットに直接接続していなくても，多くの脆弱性を抱える端末が１台でもあると，情報流出のリスクが非常に高くなります。

～　企業向けインターネットバンキング口座からの不正送金事件　～

コンピュータウイルスに感染し遠隔操作されることで，金融口座から勝手に送金されるというインターネットバンキングに係る不正送金事案が，平成 26 年 9 月 4 日現在，全国で 1,254 件，総額 18 億 5,200 万円の被害が発生しています。

被害にあわないためには，OS やウイルス対策ソフトを最新の状態に保つことはもちろんですが，新たに，送金承認者制の導入や電子認証用の暗号鍵複製機能の停止措置，翌日送金システムの導入などの対策をとることができます。

口座を置く金融機関に問い合わせるなどして，被害防止につとめてください。