平成 25 年第 1 号

広島県警察本部
サイバー犯罪対策課
082-228-0110

～　セキュリティ・インシデント（情報事故）に備えましょう　～

社長！大変です。噂では同業者の「凸凹金属」から，メールアドレスが流出して，それを使った標的型メールが送られ，被害を受けた親会社から契約を解約されたそうです。

何だって！　メールアドレスが流出しただけでどうして解約なんだ？

それだけじゃなかったんです。製品販売先の住所，氏名，性別，電話番号が入ったファイルも盗まれて，顧客から「身の覚えのない請求が来た。」という，抗議の電話がジャンジャン入っているそうです。

そうか，凸凹社長，「セキュリティに金をかける余裕が無い」と言っていたなあ。

今後の対応を誤ると，凸凹社は倒産する可能性もありますね。

そうだな・・・
我が社のセキュリティはどうなっているのかな。M 君

えーっ　去年社長が経費節減しろって言ったんで，ウイルス対策ソフトの契約更新は切れたままです・・・

こういった事例は数多く発生しています。

- セキュリティの重要性は目に見えにくいのですが，重要なシステムにはしっかり対策をとりましょう。
- 会社の情報資産を見直して，インシデント（情報事故）が起きた際の対策を事前に立てましょう。
  3,000 人の顧客情報流出で 4,500 万円の損害が出るとの試算もあります。また，一部企業では取引相手のセキュリティにランク付けをし，ランクが低い場合は取引停止する例もあるようです。
- セキュリティに対する考えを明記した「セキュリティポリシー」を定め，実行しましょう。
- 次頁の「セキュリティチェック表」を活用して，自社のセキュリティ診断をしてみましょう。

■■■■■■■■■■■　セ キ ュ リ テ ィ チ ェ ッ ク 表　■■■■■■■■■■■

次の質問に[○：実施済み　△：一部実施　×：未実施/不明]で記入してください。

採点は，○が 4 点　△が 2 点　×が 0 点で 100 点満点です。

	重要な情報を鍵がかかる場所へ保管していますか。
	重要ファイルを社外へ持ち出す際にパスワードロック等をかけていますか。
	USB メモリや CD 等を廃棄する際に物理的に破壊するなどしていますか。
	パソコンを廃棄する際に専用ソフトで内容を完全消去したり，業者委託していますか。
	事務所へ無関係な人が出入りできない習慣や仕組みがありますか。
	退社時にパソコンを鍵のかかるロッカーに入れたりワイヤーで固定するなどしていますか。
	最終退社する人が鍵を返却・保管する際に，記録を残すなどの管理をしていますか。
	WindowsUpdate などでパソコンのソフトを常に最新の状態に保っていますか。
	Winny などのファイル共有ソフトを業務用パソコンで使わせない禁止規定がありますか。
	業務に個人のパソコンを使うための規定（または禁止規定）が定められていますか。
	退社時にパソコンの電源を切るなど他人が使えない運用としていますか。
	パスワードは他人から推測されにくいものにしてありますか。
	パスワードを書いた紙片をパソコンに貼り付けないなど適切に管理されていますか。
	パスワードは定期的に変更するようにしていますか。
	ウイルス対策ソフトはインストールされていますか。
	ウイルス対策ソフトのパターンファイルは適切に更新されていますか。
	メール送信直前に宛先を再度確認するなど誤送信回避策を徹底していますか。
	メール一斉配信をする際に Bcc を使うなど個人情報に配意していますか。
	メールに重要ファイルを添付する際にパスワード保護をかけていますか。
	重要ファイルは定期的にバックアップする運用としていますか。
	従業員に守秘義務があることを教養するなど機密保護対策をとっていますか。
	従業員にセキュリティ教養を定期的に実施するなど意識付けをしていますか。
	契約書に守秘義務を盛り込むなど取り引き先に機密を守ることを求めていますか。
	情報インシデント発生時の対応マニュアルを事前に作成してありますか。
	情報セキュリティ上の守るべきことを文書化するなど明確にしていますか。

独立行政法人　情報処理推進機構(IPA)　「情報セキュリティ対策のしおり」を元に作成

■　セキュリティポリシーの策定と実施

- 一般的に，自社の情報システムの内容を棚卸しし，重要性に応じて数段階に分類します。
- そのランクに応じた対策を組織決定し，これをセキュリティ・ポリシーとして明確にした後，責任者・担当者を決めて実行していきます。
- セキュリティ対策システムの導入費用は，業者の言いなりにならず，必要な場所に適切な投資をするよう充分検討しましょう。スーパーのチラシを受注するメールシステムに過大な侵入検知システム等を導入したなどの話もあります。

■　社員教育

いくら高価なシステムや立派なポリシーを定めシステム診断の結果が 100 点であっても，たった一人の社員の「ま，いいか」でセキュリティはゼロになってしまいます。

事故発生時に会社や個人がどのような責任を問われるかなど，具体的事例を中心に，繰り返し，心に響くよう教養することが大切です。