2014.4

情報セキュリティニュース ＜2014 No.1＞

中小企業における情報漏えい防止対策

近年発生している情報漏えい事件では、1 件あたりの情報流出件数が非常に多くなっている。2013 年度において国内では一度に数万件から数十万件の情報が流出する事件がたびたび発生している。一方、海外に目を向けると、例えばアメリカでは約 4000 万人分のクレジットカード情報が流出する史上最大級ともいわれる情報漏えい事件が発生している。

この背景にはサイバー攻撃が増加しているという事情がある。情報セキュリティ対策に多額の投資を行い、人材を投入し、社内体制を強化することができる企業は大企業など一部にとどまる。中小企業の多くは、対策への必要性を感じながらも投入できる資源が限られていたり、システム担当者がいても、十分な対応をとるための知識が不足しているなど、企業間でも大きな格差が存在する。

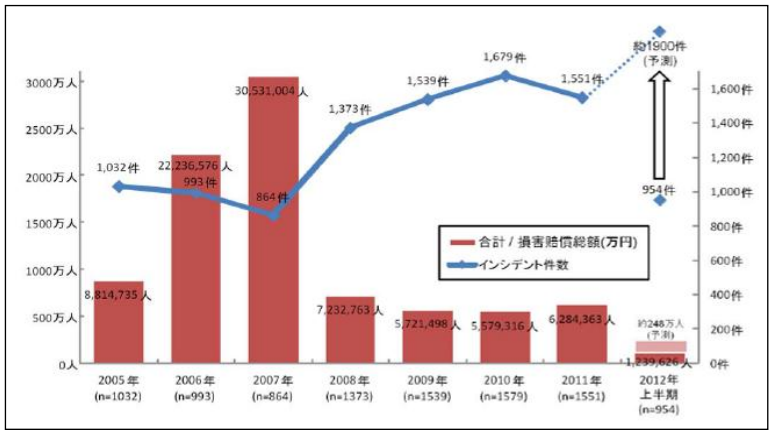
詳細は後述するが、今年は「Windows XP」などのサポート終了に伴う、いわゆる 2014 年問題があり、中小企業がサイバー攻撃のターゲットとなる可能性が高まると考えられる。セキュリティ対策が万全である大企業よりも、その業務委託先や取引先、関連会社などのセキュリティが脆弱な部分から入り込み、最終目的を達成する方が容易であるからである。中小企業にとって、行うべきシステム対策はあまりに広範囲に及び、どこから手をつけてよいのか、非常に悩ましい問題であるが、情報漏えい事件は単純なミスによるものも多く、基本的な対策を確実に行うだけでも防止効果は高い。

ここでは、発生件数の多い「内部の人間のミス（ヒューマンエラー）」による漏えいと、漏えいする情報量が多い「不正アクセスなどの外部からの攻撃」による漏えいについて、原因と主な対策について記載するとともに、2014 年問題について説明する。

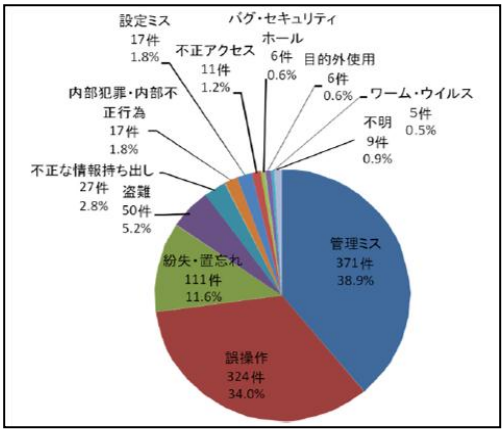
1. 個人情報漏えいの現状

1.1　個人情報漏えいの傾向

NPO 日本ネットワークセキュリティ協会の調べによると、漏えい事件は 2011 年（通年）に 1,551 件発生したが、2012 年は上半期だけで 954 件発生しており、年々増加する傾向にある（図 1 を参照）。漏えい原因は、「管理ミス」「誤操作」「紛失・置忘れ」といった内部の人間のミス（ヒューマンエラー）が約 85%を占めている（図 2 を参照）。



【図 1：漏えい人数とインシデント件数】



【図 2：原因別の漏えい件数】

出典：特定非営利活動法人日本ネットワークセキュリティ協会
「2012 年情報セキュリティインシデントに関する調査報告書（上半期速報版）」

一方、図 3 の漏えい件数(インシデント件数)で見てみると、「不正アクセス」などの外部からの攻撃の場合、漏えい件数が非常に多い。

これらの結果から、企業が情報漏えい防止対策を行う際には、ヒューマンエラーを減らすことと不正アクセス対策を実施することの双方が重要であるといえる。

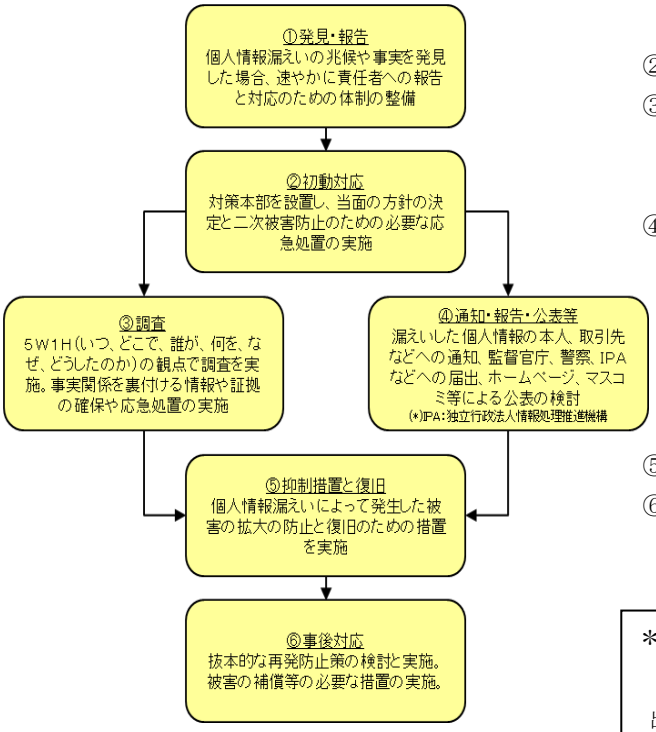
発生月（もしくは公表月）	業種等	漏えい件数（件）	漏えいした情報	原因
7月	情報通信業	4,000,000（最大）	メールアドレス、パスワード（暗号化）など	不正アクセス
7月	情報通信業	1,692,496	メール、アカウント名、パスワード（ハッシュ化）など	不正アクセス
6月	自治体	426,064	氏名、住所、生年月日、性別、転出表示など	盗難
2月	情報通信業	250,000	ユーザー名、メールアドレス、セッションID、パスワード（暗号化）	不正アクセス
8月	サービス業	243,266	氏名、ニックネーム、メールアドレス、生年月日、居住地域、性別、仮想通貨の履歴情報など	不正アクセス
8月	情報通信業	175,297	ユーザー名やパスワード（平文）、メールアドレス、登録日時、ホスト名、IPアドレスなど	不正アクセス
10月	小売業	150,165	氏名、住所、電話番号、クレジットカードのカード番号、有効期限など	不正アクセス
9月	銀行業	131,888	氏名、口座番号、取引金額、クレジットカード番号、有効期限、電話番号、振込先の氏名、取引銀行名、支店名、預金科目、口座番号、ATMの利用限度額など	管理ミス
7月	銀行業	124,471	氏名、住所、電話番号、預金金額、生年月日、勤務先など	管理ミス
11月	信用保証業	120,616	氏名、住所、電話番号、生年月日、年齢、勤務先、年収など	管理ミス

【図 3：2013 年に発生した主な情報漏えい事件】
（参考：Security NEXT「個人情報漏洩事件・事故一覧」）

1.2　個人情報漏えい時の影響

個人情報が漏えいした場合、一般的には以下のような手順に従って対応がなされる。漏えい事件の規模にもよるが、これらの対応は通常業務と並行して実施されるため、大企業においては大きな負荷が掛かるとともに、その対応費用も高額に上ると考えられる。

これに対し、中小企業の場合、大企業と比べて保有する情報量が少ない場合が多く、損害賠償額を含めた対応費用は相対的には高額にはならない場合が多いと考えられる。



【図 4：個人情報漏えい対応の基本的な流れ】
出典：特定非営利活動法人日本ネットワークセキュリティ協会

＜図 4 における各対応時の想定コスト＞

②初動対応：体制構築に関する費用

③調査：

漏えい原因究明・ログ解析等システム分析に関する費用（数百万円）等

④通知・報告・公表等：

コールセンター開設費用・それに伴う人件費（数百万円）、電話代(数十万円)、お詫び状の作成・発送費用（100 円程度/人）、新聞広告出稿費用（全国紙 4 紙に 1/3 面で約 800 万円）等

⑤抑制措置と復旧：再発防止対策費用（数百万円） 等

⑥事後対応：

金券等のお詫び対応費用（義務ではないが、500 円/人程度が支払われるケースも見受けられる） 等

＊平均損害賠償額：

漏えい事件 ： 3,787 万円／件、 5 万 7,710 円／人

出典：特定非営利活動法人日本ネットワークセキュリティ協会「2012 年情報セキュリティインシデントに関する調査報告書（上半期速報版）」

2. 情報漏えいの原因と対策

2.1　ヒューマンエラー

マスコミにおいては、サイバー攻撃による個人情報の漏えいが大きく報じられるが、研究情報や製品情報ならびに取引先の情報などの重要情報が、ヒューマンエラーやサイバー攻撃を受け漏えいするケースも存在する。これらの情報も個人情報と同様、社外に流出すると、自社への信用を失墜させたり、取引停止や新規事業の断念などの危機的事態にも陥りかねない。

以下で、ヒューマンエラーのパターン別にとるべき対策について述べるが、情報セキュリティ対策という観点からは、個人情報とその他の重要情報において大きな差異はなく、企業が保有する情報に共通してあてはまるものとしてお読みいただきたい。

原因１：管理ミス

「管理ミス」による情報漏えいとは、作業手順の誤りや、情報の公開・管理ルールが明確化されていなかったために漏えいすることをいう。例えば、情報の受け渡し確認が不十分で紛失した、適切な管理がなされず誤って情報を廃棄したなどのケースが挙げられる。

＜対策＞

- 事務所へ無許可の人が立ち入りできないようにする。
- 情報の受け渡しの際には、台帳を作成し、受け渡し確認を取るとともに記録を保管する。
- 取り扱う情報に保管期間を決め、定期的に情報の棚卸を実施し、不要な情報は廃棄する。
- 起動中のPCを他の人が利用できる状態で席を離れない(離席時はパスワードロックをする)。
- 各端末にはウィルス対策ソフトを導入のうえ、常にソフトウェアを更新する。
- 各端末にはログイン時のパスワードを設定し、利用者はパスワードを定期的に更新する。
- 情報管理に関する教育（従業員の意識付け）を定期的に実施する。　など

原因２：誤操作

「誤操作」による情報漏えいとは、あて先の書き間違えや操作ボタンの押し間違えなど、人間のオペレーションミスにより生じる情報の漏えいのことをいう。例えば、あて先間違いによる電子メール・ファクシミリの誤送信、郵便の誤送付、などが挙げられる。

＜対策＞

- 郵便物の発送に関わる作業は、一定の広さがある作業台等で実施する。また、作業中の割り込み作業を禁止する。
- 拠点間のファクシミリ通信は内線化するか、番号を短縮登録する（登録時に、テスト通信を実施する)。
- ファクシミリ送信時は、複数人立会いのもと送信する。
- 電子メール（Outlook使用時）のあて先入力を行う場合は、オートコンプリート機能は利用しない（設定を無効にする)。または、連絡帳の「表示名」を利用し、送信前のあて先チェックを容易にする。
- 送信ボタンを押した後、数分間は送信ボックスに留まった後に発信されるよう設定する。
- メールで送付する添付ファイルはパスワード設定や暗号化を行う。　など

原因３：紛失・置忘れ

「紛失・置忘れ」による情報漏えいとは、「持ち出し許可を得た情報を、個人のミスにより持ち出し先や移動中に忘れたり、紛失したりすることで生じる情報漏えい」のことをいう。例えば、電車、飲食店など外部の場所において、設計図・PC・情報媒体等を紛失する、などが挙げられる。

「紛失・置忘れ」については、個人の危機感や性格によるところが大きく、事件を発生させないためには情報を持ち出させない、という方法が最も効果的であるが、その一方で、日常業務を遂行する上での妨げになるため、一律持ち出させないということはなかなか難しい。このため、万一紛失・置忘れが発生した場合も、第三者がその情報にアクセスできないように、以下のような対策を講じることが考えられる。

＜対策＞

- PCやデータを持ち出す際には承認制とする。
- 従業員におけるＵＳＢメモリの使用禁止または使用制限を行う。

➢ 持ち出し用 PC には BIOS パスワード、システムパスワード、ハードディスクの暗号化ならびにファイルの暗号化を行う。　など

2.2　外部からの攻撃

近年、外部からの不正アクセス・Web サイト改ざん等のサイバー攻撃が高度化しており、これを防ぐためには、さまざまなシステム対策を継続的に講じる必要がある。とはいえ、中小企業では、システム対策にかけられる人と資金が限られており、大企業と同様な対応をとることが難しいことも事実である。

ここでは、コストをかけずに実施可能な対策を記載するので、参考にしていただきたい。

＜対策＞

① PC にはウィルス対策ソフトを必ずインストールし、常に最新版を利用するとともに、定期的に PC 内のスキャンを実行する。
② OS やアプリケーションソフトのアップデートや、脆弱性を修正するためのセキュリティパッチは最新のものをインストールする。
③ インターネットと内部ネットワークの境界線上にファイアウォールを設置する。
④ 従業員ごとにユーザーアカウントを付与し、情報のアクセス制限を行う。
⑤ システムへのアクセスログを取得・保存する。
⑥ 個人用 PC の持ち込みを禁止する。禁止できない場合は、許可制とする。
⑦ 業務用 PC へのソフトのインストールを制限する。
⑧ 離席時のパスワードロックの実施、退社時の電源オフを徹底する。
⑨ 従業員が退職した際は、パスワードのリセットを実施し、在職者は定期的にパスワードを変更する。
⑩ 重要情報のバックアップを定期的に行う（週 1 回を推奨）。
⑪ 不審なサイトへのアクセスや不審なメールの対応等、従業員への定期的な注意喚起を行うとともに教育を実施する。　など

3. ビジネス PC の 2014 年問題

3.1　2014 年問題とは何か

2014 年 4 月 9 日（日本時間）、世界各国で利用されてきた「Windows XP」のサポートが終了する。また、「Microsoft Office 2003」ならびに「Internet Explorer6」も、同日をもってサポートを終了する。これに伴い、情報漏えい事件が多発することが懸念されており、PC の「2014 年問題」と呼ばれている。

4 月 9 日以降、これらを搭載する PC が直ちに使用できなくなるわけではないが、脆弱性を修正するための更新プログラムが提供されなくなるため、ウィルスへの感染リスクが非常に高まるとともに、周辺機器についても新たな不具合が見つかった場合、対応がとれず利用できなくなる可能性が考えられる。

また、図 5 からもわかるように過去 5 年間において、「Windows XP」の脆弱性は継続的に発見されており、今後も発見される可能性は高いと考えられる。これらの脆弱性に対する対策を実施することなく使用し続けることは極めて危険である。

【図 5:Windows XP の既知の脆弱性の件数】
出典：独立行政法人情報処理推進機構「Windows XP のサポート終了に伴う注意喚起」(2014 年 1 月 29 日)
(注 1) JVN（Japan Vulnerability Notes）は、日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供している情報ポータルサイト。

今回のサポート終了は、数年前より公表されていたが、製造業における生産管理システム・在

庫管理システムや、医療現場の検査装置等の制御端末など、今もなお「Windows XP」上でしか稼働しない業務アプリケーションを利用している場合があろう。

また、多数の端末を使用している場合、一度にすべての端末を新しいOSに移行することは、時間や費用の観点から非常に難しく、現時点においても、対応が完了していない企業が一定数残っているとみられている。

3.2 対策

サポートが継続している後継または代替OSに移行することがベストであるが、やむをえず「Windows XP」を使用せざるを得ない場合、以下の方法が独立行政法人情報処理推進機構より公表されているので参照していただきたい。

＜オフラインでの利用に切り替えられる場合＞

① 「Windows XP」の使用は、オフラインに限定する。

② ＵＳＢメモリなど外部情報媒体の自動実行機能を無効化する等、ネットワーク以外からの攻撃リスクを低減するための対策を行う。

＜オンラインで使用する場合＞

① サポートが継続しているウィルス対策ソフト、マイクロソフト社の無償ツールEMET(注2)等の攻撃対策ツールを活用し、攻撃の検知・回避を行う。

② サポートが継続しているアプリケーションを最新に保ち、サポートが終了したアプリケーションは代替アプリケーションに切り替える。

(注2)EMET：マイクロソフト社が提供しているWindows用の脆弱性緩和ツール。

上記の対策以外に、Windows XPから新しいOSへの移行をサポートする上で、現システムの延命サービスを提供している企業もあるので、各社においてベストな対策を検討のうえ選択することをお勧めする。

4. おわりに

2001年の発売開始後、十分な性能と安定性により使用され続けてきたWindows XPのサポート期間が終了を迎え、まだWindows XPを使用している企業のシステム担当者の中にはどのように対応するか頭を悩ませている方もいるのではないかと思われる。

ウィルス感染については、インターネットに接続されたWindows XP端末に目が行きがちだが、複合機、テレビ会議システムや防犯カメラ等がインターネットに接続されている場合においても、ウィルス感染や攻撃の道具として利用されるなどの問題が発生する可能性がある。企業によっては、システム端末と複合機等の什器備品の担当部門が違うことから、それぞれの部門で万全な対策を講じていると思っていたにも関わらず、セキュリティホールが発見されることも考えられるので、注意したい。

一方で、システム対策に力を入れ、不正アクセスを防止できる体制を構築したとしても、ヒューマンエラーによる情報漏えいを防ぐことができなければ、企業としての信用を維持することはできない。個人情報や重要情報などの漏えい事件に巻き込まれないよう、投入できる人的・物的資源も踏まえながら、情報漏えい防止の観点からの自社の弱点を分析したうえで、外部による情報漏えい対策と内部からの情報漏えい対策の双方をバランスよく講じることが重要である。

インターリスク総研 事業リスクマネジメント部　事業継続マネジメントグループ
アソシエイト　沖　　歩　（オキ　アユミ）

株式会社インターリスク総研は、ＭＳ＆ＡＤインシュアランスグループに属する、リスクマネジメントについての調査研究およびコンサルティングに関する専門会社です。
弊社では情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問い合わせ先、または、あいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
㈱インターリスク総研　事業リスクマネジメント部　統合リスクマネジメントグループ
TEL.03-5296-8914　　http://www.irric.co.jp/

本誌は、マスコミ報道など公開されている情報に基づいて作成しております。
また、本誌は、読者の方々が企業の情報セキュリティへの取り組みを推進する際に、役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。