Special
“情報＝資産”価値に応じた情報漏洩対策とは？

インタビュー／NTTデータ経営研究所

権限を持つ人間による不正利用を防ぐことが情報漏洩対策のポイントになる

── 2005年４月に個人情報保護法が完全施行されましたが、企業や自治体における「情報保護」の現状についてお聞かせください。

小野寺　施行前は、ノートPC等の盗難や置忘れ、紛失による個人情報の漏洩が目立っていましたが、施行後は、どの企業や団体においても情報セキュリティ対策を経営課題として考えるようになり、注意深く管理するようになりましたので、置き忘れなどのケアレスミスによる情報漏洩はかなり減ったと思います。その一方で、以前から存在していたワームやトロイの木馬などのスパイウェア（悪意のあるプログラム。海外では「マルウェア」と呼ばれている）による情報漏洩が目立ってきています。代表的なものとして、米国のクレジットカード処理会社のケースがあげられます。本件では、全世界で4,000万件以上のクレジットカード番号が流出した可能性があり、その不正利用による被害は、日本だけで１億５千万円以上になると言われています。日本においても、メールに添付されたスパイウェアをクリックしたために、PC上のインターネットバンキング口座の口座番号やパスワードが流出し、口座から不正に現金が引き出されるなどの被害が出ています。また、通販の購入者を装った巧妙な手口で、写真に擬態したスパイウェアをクリックさせるというものもありました。

── このような事件が何故起こるのでしょうか。また、現状の対策に何か問題がありますか。

小野寺　情報漏洩は、個人情報のニーズがある限り、根絶することはできません。したがって、制度面はもちろんですが、技術的対策、物理的対策は必須と言えます。ただ、気をつけなければならないのは、対策の中には、結構、落とし穴があることです。例えば、暗合化ツールは、暗合化・複合化作業を運用に頼る場合が多いため、操作ミスを起こしてしまう場合があります。また、業務上の権限を有する人間が、正当な行為で引き出した個人情報を、不正に利用することを事前に阻止することは極めて困難です。また、これまでのスパイウェア対策では、アンチウイルスソフトとファイアウォールによる対策が主流でした。しかし、アンチウイルスソフトは、ウイルスパターンによるウイルス検出に依存する場合が多く、パターンファイルが作成されていない、未知もしくは特定企業を狙ったスパイウェアにはほとんど効果がありません。またファイアウォールは、企業内部からの通信が正規の通信であるのか、スパイウェアによる不正な通信であるのかを判断することが困難なため、内部からの情報漏洩を防ぐことができません。さらに、今後、どのような攻撃が起こるかは誰にも想像できません。

㈱NTTデータ経営研究所
ITマネジメント本部長
シニアコンサルタント
小野寺　清人氏

── スパイウェアによる情報漏洩を防ぐためには、どのような対策を行えばいいのでしょうか。

小野寺　対策を行う上で「スパイウェアやウイルスに感染しない」という視点だけはなく、「スパイウェアやウイルスに感染しても発病させない」との視点を持つことが必要です。スパイウェアを入り口で発見するとともに、万一内部に入り込んだ場合は、システム内のアプリケーションの動作を制限することで、犯行を内部に封じ

込めるのです。まず、未登録のアプリケーションの起動を禁止します。さらに、スパイウェアが登録済みのアプリケーションを装った場合は、ファイルをメールに添付して送信する／許可されていないフォルダへのファイルの移動または書き込み／ファイルを外部のサイトへアップロードする、といった、本来のアプリケーションの動作と異なるスパイウェア特有の不審な動作を制限することで、情報漏洩のリスクを軽減することができます。

――昨今、情報漏洩を防止するために、既存のPCをシンクライアント化する企業が増えていますが。

小野寺　情報漏洩事件の多くは、PCの盗難や紛失によるものや、PCに保存された機密情報がUSBメモリ等の媒体やメール、印刷物により流失したケースがほとんどです。これまで、このようなケースへの対策は、暗号化が主流でしたが、暗合化ツールは管理・運用が難しく、情報漏洩のリスクに対しては、いくつかの課題を残したままです。そのため、社外に持ち出すことが多く、管理が行き届かないノートPCを使用する企業では、抜本的な対策が求められています。PCのシンクライアント化への動きは、このようなニーズが影響しています。シンクライアント化されることで、これまでPC上にあったアプリケーションやデータをサーバで一元管理するこができます。また、コピーや印刷、メール送信などの情報漏洩につながる恐れのある機能を制限することができ、操作ログの取得を行うことで、情報漏洩の抑止効果が高まります。さらにシンクライアント化は、企業および団体における内部統制の充実にも結びつきます。

――内部統制が図られることで、情報セキュリティ対策はどのように変わりますか。

小野寺　内部統制の充実を図るためには、現在のビジネスプロセスを可視化して、その上で、内部統制が的確かつ効率良く機能するためのマネジメントシステムを構築することが必要です。このマネジメントシステムの運用を通して収集されたログ分析により、ビジネスプロセス上の不具合や課題が抽出されます。この可視化されたビジネスプロセスを分析することで、潜在するセキュリティホールを発見することができます。内部からの情報漏洩の原因は、情報そのものにあるのではなく、ビジネスプロセス上に存在しているからです。

――情報漏洩をはじめとした情報セキュリティ対策を進めていく上で、どのようなことがポイントになるのでしょうか。

小野寺　情報セキュリティ対策には、おおまかに3種類あります。生体認証などの「使用者の識別」、ハッキング、クラッキングなどへの「外部からの攻撃への防御」、個人情報保護法で注目を集めている「内部からの情報漏洩対策」です。ここで言う内部からの情報漏洩対策とは、特に有権限者による情報漏洩の防御を指しています。先ほども述べましたが、有権限者の犯罪行為を未然に防止することは困難です。したがって、不正行為をやりにくい環境、例えば、印刷、メール添付・送信、外部媒体書き出しの制限、オープンスペース化による衆人環視を実現する必要があります。さらに、操作ログの収集、分析による抑止効果も重要です。ただ、セキュリティの最後の砦は人間であり、「人間への対策」も実施すべきです。セキュリティ・ポリシーの徹底や教育の実施とともに、待遇面などを含めた“不満を持たれない”職場環境を築き上げることが大切です。