業務プロセスの視点からの情報セキュリティ

飯塚佳代

情報セキュリティマネジメントにおいて重要なポイントは、リスクとの兼ね合いを考えながら情報をどう守るかということである。そのためにさまざまな観点でリスクを分析し、施策を行うことが重要である。重要な情報が存在している場所とその場所へのアクセスに焦点を当てた技術的な対策も必要であるが、それとともに業務プロセスに焦点を当てた分析と対策も有効な方法である。個人情報などの重要情報を、業務プロセスを流れる情報の１つとして位置づけて分析することで、業務効率とリスク管理の両面からの改善が可能となり得るからである。

情報を守る

情報セキュリティ対策の重要な視点は、ヒト、モノ、カネに続く経営資源である「情報」を活用しつつ、それを適切な状態に保ち、守ることである。たとえば、「JIS Q15001：個人情報保護に関するコンプライアンス・プログラムの要求事項」に準拠する文書の１つとして、個人情報資産管理台帳があげられる。これは、必要なポリシーや体制を整えるとともに、守るべき情報とそのありかを明らかにすることが重要だからと考えられる。

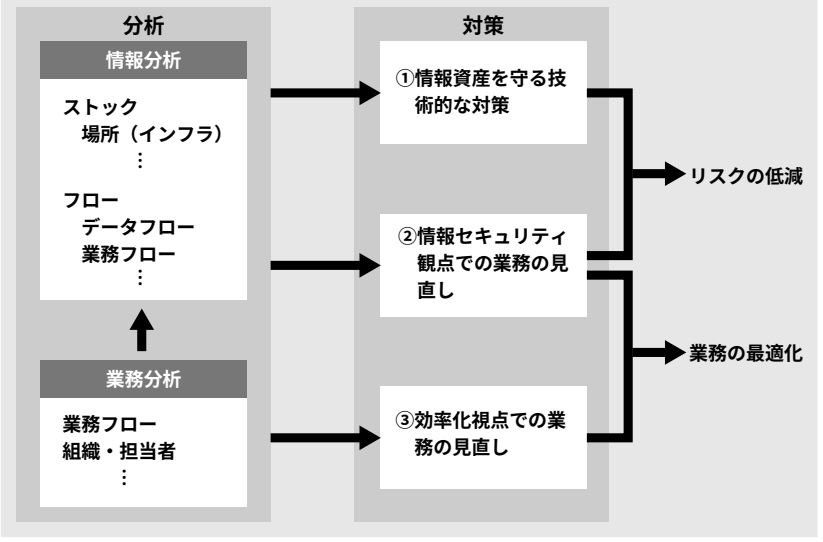
情報そのものに焦点を絞ってセキュリティ上の脆弱性の分析を行う場合、情報およびその情報が属するインフラを中心に、機密性、完全性、可用性の観点で行うのが一般的である。

不正な手段でアクセスされないか、情報が正確な状態を保てているか、そして適切な利用者が必要な時にアクセスできているかを検証するために、インタビューや、実機による技術的な評価などを行う。加えて、業務プロセスの視点で個人情報などの重要情報の流れを分析することが、リスク削減への有効な施策となる（図１）。

業務プロセスを流れる重要情報

たとえば、一般消費者に対して財やサービスの直販を行う企業などでは、受注情報、在庫情報、個人情報などさまざまな情報が、商品やサービスの提供に関する業務プロセスを流れている。SCM（サプライチェーンマネジメント）やERP（統合基幹業務システム）

図１　業務プロセス分析の位置づけ



当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2005 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

パッケージの導入などに伴って業務プロセスを整理する場合には、在庫情報や会計情報などに焦点を絞って、それらが業務プロセス（手作業の業務を含む）の中でどのように生成され、やりとりされ、処理されるかという視点で整理・分析を行う。

同じように、個人情報が業務プロセスのどこで収集・生成、やりとりされて、処理されるかという点を改めて整理してみると、次のような課題が発覚することが少なくない。

①必要以上に情報のやりとりが発生している業務プロセス
②プロセス間が滞りがちだったり、断絶が発生したりしている業務プロセス
③担当が不明な（誰であるかわからない）業務プロセス
④実際は不要な業務プロセス

個人情報の管理には留意しているつもりの組織であっても、業務プロセスは不断に変化するものであり、上記のような状態が気づかないうちに発生していることも珍しくはない。

業務プロセスの視点で考えることの意義

SCMプロセスの改善では、在庫やそれにかかわる受発注・生産の情報の流れを分析することにより、その流れの中の問題個所を発見し、これを改善することで、供給リードタイムの短縮やコスト削減などを実現する。

これと同様に、個人情報を含む業務プロセスでも、上記の①～③のような問題点が原因となって、顧客を待たせていたり、業務の処理コストがかさんでいたりすることがあり、こうした問題は、業務の効果と効率の面から改善の余地がある。

それだけでなく、これらの問題は、業務プロセスにセキュリティ上の脆弱性が潜む危険性があることも意味している。たとえば、組織をまたがるプロセスにおいて、必要以上の数の個人情報が外部を含むさまざまな部署に存在したままになり、それが「処理中」であることすら把握されていない、といったケースもある。

また、業務上で実際に必要とされる以上の情報のやりとりが定型業務として行われ、担当者のローカルパソコンに個人情報を含むファイルが残っている、といったことも少なくない。担当者間の確認プロセスなどでは、同報アドレスあてのメール添付の形でやりとりされ、そうした状態が放置されているケースもある。

このような場合、汎用的な削除ルールなどを決めておくことはもちろん必要である。しかし、業務プロセスそのものを見直し、中間に介在する余分なファイルに関するリスクと、それらを管理する工数を減らすことが、より本質的な対処方法である。工数そのものの削減という業務効率的な観点と、情報セキュリティ対策の両面からの解決策となり得るからである。

統合的な視点でのセキュリティ対策へ

企業には、組織をまたがるさまざまな業務機能をもつ業務プロセスがある。このような業務プロセスを分析することで、潜在するセキュリティの脆弱性を明確にし、リスク管理と業務効率の両面から改善を図ることが、今後ますます重要になると考えられる。

『ITソリューションフロンティア』2005年５月号より転載

飯塚佳代（いいづかかよ）
NRIセキュアテクノロジーズ(株)情報セキュリティ調査室主任情報セキュリティコンサルタント

当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2005 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.