必要性高まる 安全なIT環境

情報漏洩対策と内部統制対応

IT（情報技術）の活用が日々拡大・高度化する一方で、ウイルス感染や情報漏洩（ろうえい）などの被害は年々増加している。企業はこうした脅威から身を守り、内部統制の一環として安全なセキュリティー環境を構築する必要がある。先に開催された日経産業フォーラム「ガバナンス時代のセキュリティー」では、政府の情報セキュリティー政策をはじめ、実際の企業が抱える課題やその解決策などが紹介された。

基調講演

金谷　学氏
経済産業省
商務情報政策局情報経済課
情報セキュリティ政策室
総括係長

IT戦略本部の下に設置された「情報セキュリティ政策会議」において決定された基本戦略に基づき、各府省庁は所管領域の情報セキュリティー政策を立案、実施している。同会議は日本の情報セキュリティー問題の根幹に関する事項を策定する母体となっている。

本省では一九九〇年の「コンピュータウイルス対策基準」に始まり、九六年の「コンピュータ不正アクセス対策基準」、九九年の「不正アクセス行為の禁止等に関する法律」、二〇〇三年の「情報セキュリティ管理基準」などの関連所管法令を制定。併せてコンピューターウイルス・不正アクセスに関する届け出制度や、フィッシング対策事業、ボット対策推進事業などの情報セキュリティー問題による被害の未然防止・抑制を図るための事業を推進している。

〇三年には産業構造審議会の「情報セキュリティ部会」で我が国で初めての総合的な情報セキュリティー戦略として「情報セキュリティ総合戦略」を策定した。経済・文化国家としての日本の強みを生かした「世界最高水準の高信頼性社会の構築」を戦略の基本目標と位置付け、その要となる情報セキュリティーについて提言している。また〇七年には産業構造審議会「情報セキュリティー基本問題委員会」で、「グローバル情報セキュリティ戦略」を取りまとめた。ITが我が国だけではなく世界の隅々に行きわたり、経済社会システムに融合した密接不可分なものと化していくことを見据えている。

企業の経営者が抱える経営課題は多様化・複雑化しており、情報セキュリティー意識に基づく業務活動を組織内に徹底させる仕組みや、経営者が組織内の状況をモニタリングし、方針を決定する仕組み、市場に対する開示と市場による評価の仕組みが必要である。

本省では〇六年度までに「情報セキュリティ対策ベンチマーク」「情報セキュリティ報告書モデル」「事業継続計画策定ガイドライン」などを策定してきた。〇八年六月には「情報セキュリティ基本問題委員会」で戦略的かつ適正な情報セキュリティーガバナンスの確立のための環境整備に関する提言を行うべく中間の取りまとめを行ったが、〇九年以降に完全な取りまとめを公表する予定だ。

〇八年度の確立促進活動では、各種法律における情報セキュリティー上の要求事項に関する調査、アウトソーシングに関する情報セキュリティー対策ガイドライン策定、情報セキュリティーガバナンスの構築事例に関する調査、情報セキュリティー格付けのあり方に関する調査研究などが予定されており、継続して活動を行っていく考えである。

ガバナンスの確立を

情報セキュリティー

セッション1

麻地　徳男氏
アルプス システム インテグレーション
代表取締役社長

一九九〇年代半ば以降米国では、インターネット上での検索エンジンの利用が進み検索が容易になったことで、青少年が犯罪に巻き込まれるケースが増えてきた。日本でも規制が立て続けに発効したが、子どもたちが巻き込まれる事件は激増している。

そこで注目されているのが、ウェブページの内容をチェックし、業務などに不適切なサイトへのアクセスを遮断するウェブフィルタリングソフトだ。当社のウェブフィルタリングソフト「インターセーフ」は、当社子会社のネットスターで専任のリサーチャーが収集したURLをすべて目視で確認しており、五年連続で国内シェアナンバーワンを誇っている。最近では、内部統制対策や情報漏洩対策に不可欠なインターネットのアクセスマネジメントも実現している。

企業活動がグローバル化するなかで、情報セキュリティーのリスクは国際的に広がっている。日本の企業は情報に関するリスクの意識が低く、これまでのやり方では重要な情報は守りきれない。そこで基本となるのが、まず守るべき情報は何かという情報資産の洗い出しと整理を行うこと。そして的確な侵入防止・情報漏洩対策を立てることである。

日本の企業ではこれまで、性善説を基に外部からの侵入・攻撃に備えてきたが、悪意ある情報の持ち出しや漏洩についてを誘っている。最近では、内部統制対策や情報漏洩対策に不可欠なインターネットのアクセスマネジメントも実現している。

企業活動がグローバル化するなかで、

全拠点の端末や利用権限を中央集権型で一括管理

は、性悪説の観点で情報セキュリティー策を検討する必要がある。

グローバルな環境では、規定やルールだけでは情報を守れない。悪意を持って情報を持ち出そうと思ってもできない仕組みを、世界規模で構築することが必要だ。

グローバルセキュリティー展開モデルとしては、最低限順守するべき具体的なルールを示して全拠点へ準拠を求める「中央集権型」、抽象度の高い方針を示して各拠点が独自のルールを策定・運用する「連邦型」、拠点を階層化して配下の企業を統治する「権限委譲型」の三タイプに分かれる。当社としては、本社側の負担は重いが、グループで一貫性のある管理ができる中央集権型を勧めている。

グローバルセキュリティー構築のポイントは、全世界の端末や利用者の権限の変更などの運用、管理が容易で、海外拠点の情報セキュリティーを一括管理できること。当社の「ドキュメントセキュリティ」はこうしたニーズを満たし、現在、親会社のアルプス電気が世界十四カ国で活用していることを含め、二十八万以上のユーザーがいる。

ファイル保存・閲覧などに暗号化や解除が自動で行われるなど、現状の使い勝手を変更せずに対策を行える点、七カ国八言語の多言語基本ソフト（OS）に対応している点などが評価されている。

重要な情報は、セキュリティーレベルの低いところから漏洩する。企業には、グローバル展開にふさわしい対策が求められている。

セッション2

山倉　直氏
NRIセキュアテクノロジーズ
ソリューション事業部
統合セキュリティ管理
チームリーダー

セキュリティーといえば、一昔前はウイルス対策を行ったり、ファイアウオールを導入したりすることだった。しかしの手口は日々巧妙化し、次々と新たな脅威が出てきている。それに合わせてたくさんのツールを導入しなければならず、管理はますます複雑になる。やればやるほど「対策疲れ」になるという悪循環に陥っている。

そこで求められるのが、個別の対策や個別最適化ではなく、全体を統合した戦略、つまり全体最適化だ。ゴールが見えないという問題に対してはセキュリティー管理業務のベストプラクティスを活用した「セキュリティーBPR（業務改善）」を提案している。

セキュリティーBPRで管理業務の効率化を促進

BPRは、他社のベストプラクティスのモデルをそのまま使い、セキュリティー管理業務を変えていこうという発想である。セキュリティー管理業務は組織・対象・管理策という三つの軸により、誰が、何を・どうするという形で表せる。

ID管理を例に取ると、「セキュリティー管理部門が」「ファイルサーバーのアクセスパスワードを」「八文字以上に設定する」のように定義することで、業務全体を具体的に表せる。

が、効果が見えないという問題に対しては定量評価による動機付けが、解決策として考えられる。

セキュリティーBPRや定量評価による動機付けを実現するセキュリティーソリューションとして、「SecureCube／Central」という製品を提供している。

また定量評価による動機付けは、効果が目に見えるように数値化して表す。例えば部門ごとに、A部署は何点、B部署は何点というのが分かると、競争心理が働いて自然とセキュリティーの対策が促進される。全社的にも、現状が何点で、今後の目標として来期は何点にするという目標が描ければ、インセンティブが働く。実際に、このやり方でセキュリティーレベルの向上に成功している企業がある。

こうしたセキュリティーBPRや定量評価による動機付けを実現するセキュリティーソリューションとして、「SecureCube／Central」という製品を提供している。

セキュリティーポータルとして利用するもので、セキュリティー管理部門だけでなく、多数の一般ユーザーがアクセスするための画面・機能を備え、効率的なセキュリティー管理業務の効率化を可能にするものである。

セッション3

梅澤　泉氏
新日本有限責任監査法人
TSRS部
シニアマネージャー
公認会計士

情報セキュリティー関連の基準として は、経済産業省の「情報セキュリティー管理基準」をはじめ、「情報セキュリティーマネジメントシステム（ISMS）」の要求事項を定めた規格「ISO／IEC 27001：2005」などがある。

一方、内部統制については「財務報告に係る内部統制の評価及び監査に関する実施基準」「情報セキュリティー管理基準追補版」、そしてIT統制の国際的な指針「COBIT／for／SOX」などがある。

マネジメントシステムとしての情報セキュリティーと内部統制には共通点がある。一つ目は、基本的にPDCAサイクルの流れの中で仕組みが構築され、運用されているということ。二つ目は、要素として機密性、完全性、可用性が組み込まれていること。三つ目は、リスクへの取り組みだ。制度面から言うと、情報セキュリティーと内部統制は同じ考え方の下に作られており、それぞれバラバラに活動するのは非効率的である。

内部統制の推進と連携を潜在リスクの予防も大切

また実際の運用面では、内部統制（IT全般統制）の情報セキュリティー関連の要求事項として挙げられる①プログラム開発・変更時の検証②アクセスコントロール③適切な障害対応④データ直接修正時の承認、検証⑤スプレッドシートに対するコントロール⑥外部委託先の管理――を十分に機能させる必要がある。内部統制の求める情報セキュリティーとしては、フレームワークを確立し、アクセス管理策を構じるとともに、インシデント（事件・事故など）の管理や外部委託先の管理がポイントになる。

情報セキュリティーマネジメントを内部統制に生かすには、企業全体で取り組む内部統制の中に情報マネジメントを組み込み、一体として評価・改善活動を実施することが必要だ。情報セキュリティー担当部門と内部統制推進部門とが連携を図り、双方向で情報を共有するのが望ましい。情報セキュリティーは機密性だけではなく、完全性・可用性をバランスよく取り入れることが重要。また、顕在化した情報セキュリティーインシデントに対してのみ事後的に対策に取り組むのではなく、潜在的なリスクについての予防的コントロールを考える視点を持つことが大切だ。

広　告
企画・制作＝
日本経済新聞社クロスメディア営業局