特集「エンタープライズ・セキュリティ」の発刊に寄せて

平 岡 昭 良

相次ぐ情報漏えい事件と，2005 年 4 月の個人情報保護法の全面施行により，情報セキュリティに対する社会の関心や認識は高まり，それにともなって企業の情報セキュリティへの取り組みに対する社会的要請が強まってきている．

情報セキュリティをめぐる事件・事故は，事業活動の一時停止や株価低下にとどまらず，これまで培ってきた信用を一瞬にして失うことにもなる極めて重要なビジネスリスクとして捉えられるようになってきている．

さらに加えて，金融商品取引法（J-SOX 法）の施行により，コンプライアンスや内部統制も求められるようになり，企業にはますます多岐に亘る取り組みが必要となってきている．

実際，多くの企業・組織が情報セキュリティに関する取り組みを行い，情報セキュリティ・マネジメント・システムの構築に取り組んできた．しかし，そうした取り組みの推進にも拘わらず，個人情報や機密情報の流出，インターネットを経由した不正アクセスなどの情報セキュリティ事件・事故があとを絶たず，頻繁にメディアで報じられている．

一方で，情報セキリュティ対策を過剰に優先させるあまり，モバイル PC の使用禁止など，せっかくの ICT の利便性を犠牲にせざるを得ないケースや，運用負荷の増大や情報共有・交換の制限など，業務の効率性を阻害するケースも増えてきている．情報セキュリティ対策を年々厳しくしてきた結果，企業の ICT 鎖国，ガラパゴス化といった現象が生じてきた．

グローバル化の波は，閉じた組織，企業から競争力を奪うと言われている．ICT をビジネス基盤として利活用することで，グローバルレベルでの横断的な情報共有・活用を図り，企業が持つバリューチェーンの最適化を図ることが競争力につながることになる．単純に情報セキュリティを強化するだけではなく，企業グループを超えたオープンなサプライチェーンや顧客サービスの強化に，いかにセキュリティ対策を組み込み，競争力を高めていくかが問われている．

また，近年，ワーク・ライフ・バランスが注目を集めるようになってきている．人材を確保するための福利厚生という狭い観点ではなく，働き方や働く環境，いわゆるワークスタイルの変革が，企業の競争優位と，社員の仕事と生活の調和をもたらすという考え方である．テレワーク（在宅勤務）やモバイルワークが代表的な手法だが，制度と職場の風土，それを支える ICT の環境，特に十分な情報セキュリティ対策がないと実施できない．

さらには，企業の社会的責任という観点から，企業には，適法性と適正性の遵守，透明性や情報開示を求める声が高まり，企業によるリスクなどの情報開示，説明責任が求められるようになってきている．社会的責任を考慮した，情報資産の有効活用と管理の高度化，事業継続対応への取り組みをさらに強化する必要がある．

ICT の技術革新もまだまだ続いている．SaaS やクラウドコンピューティングと呼ばれるソ

フトウェアからサービスの流れは，今後さらに加速すると言われる．コンシューマ向けのサービスに目を転じてみると，メールや検索サイト，ブログ，SNS などのネットサービスは，無料もしくは低価格での競争が激化しており，ますますサービスレベルが高くなり，利便性も増してきている．企業では，情報セキュリティ面での不安から，業務上有効と思われるこうしたサイトさえ利用を禁止しているケースが多く，企業の ICT 鎖国とも言われる一因になっている．実際，企業で使える ICT とコンシューマとして使う ICT を比べてもどかしく思われている方も多いのではなかろうか．

この流れは，当然企業にも影響を与えつつある．コンピュータ・システムを「所有する」から「利用する」という形態が普及してきており，自社で所有するシステムと，外部システムをサービスとして利用するものが企業に共存するようになりつつある．自社で閉じた情報セキュリティ対策から，外部のサービスと連携できる情報セキュリティ管理が求められ始めてきている．さらに，情報セキュリティ対策そのものが，サービスとして提供されるようになるであろう．

このような環境にあって，企業が情報セキュリティ管理を継続的に維持していく重要性はますます高まっていくであろう．しかしながら，前述したような環境変化が加速する中で，情報セキュリティが持つ三つの特性「多様性と変化」「運用負荷（業務効率の低下）」「投資対効果の不透明さ」が，さらに情報セキュリティ管理を困難なものにしていく可能性は否定できない．

全体最適な視点で，情報セキュリティ管理を経営戦略や社会，取引先などからのセキュリティ要求と整合性が保たれた状態で統制していく必要がある．リスク管理，ポリシー，管理の仕組み，技術面の対策，人的対策，BCP，コンプライアンス，効果測定などを体系的な枠組みでとして捉える ESA（エンタープライズ・セキュリティ・アーキテクチャ）による活動がそろそろ求められる時代になりつつある．

日本ユニシスグループでも，2004 年，2006 年と「情報セキュリティ総合戦略」を策定し，主に情報資産をしっかり守り抜くということに重きを置いて活動してきた．2008 年には，「守りから攻めの情報セキュリティ対策」をキーワードに，新たな「情報セキュリティ総合戦略 2008」を策定し，環境の変化に対応できる活動を推進中である．

本号では，エンタープライズ・セキュリティ・アーキテクチャを取り上げ，さらに重要な構成要素であるセキュリティポリシー，情報セキュリティ技術，人材，効果測定についての考察を試みた．また，実際の日本ユニシスグループの取り組み事例として，情報セキュリティ・マネジメントへの取り組み，事業継続計画への取り組み，情報システム開発におけるセキュリティ対策を紹介させていただいた．読者の一助になれば幸いである．

（CIO　CISO　CPO　上席常務執行役員）