トピックス

求められる経営起点のセキュリティ対策
―プロセス・ヒトを中心としたセキュリティマネジメント―

サイバー攻撃の対象範囲が情報システムから制御システム、IoT（Internet of Things）システムへと拡大する中、企業には今まで以上の対策が求められている。必要となるのは経営層の強いリーダーシップだ。本稿では、システムコンサルティングの視点から、新たなセキュリティマネジメントの在り方を提言する。

野村総合研究所 システムコンサルティング事業本部
ITマネジメントコンサルティング部 主任システムコンサルタント
木下（きのした） 雅史（まさし）
専門はIT組織改革やセキュリティマネジメントに関するコンサルティング

企業のセキュリティ対策は社会的責務

2015年5月に日本年金機構を襲ったサイバー攻撃は、それらがもたらす被害の甚大さをあらためて世間に印象付けた。同時に、標的型攻撃といわれる実に巧妙な攻撃手法の前では、侵入検知などの防御中心の考え方だけでは限界であることが露呈された。

サイバー攻撃の標的は、社内の情報システムだけでなく、生産設備などの制御システムや、機械・電子機器に組み込まれたITにまで拡大している。これらITが攻撃を受けた場合、その被害はシステムにとどまらず企業活動全体、さらには、インフラを含めた国民生活全体にまで大きく影響を及ぼす危険性がある。このように今やサイバー攻撃への対策は、一企業に閉じたものではなく、社会的責務として捉えるべき問題である。

大規模化・巧妙化するサイバー攻撃に対抗するには、これまでの考え方を転換することが不可欠である。防御策に偏重するのではなく、万が一侵入された場合でも、いかに被害を最小限にとどめるかということにも重点を置くべきだろう。

また、近年の事故を分析すると、復旧や損害賠償などの直接的な被害以上に、事故発生後の対応の不手際による間接的な被害（信頼性の失墜による顧客離れや株価低迷など）の方が企業に与えるダメージは大きい。こうした観点からも、いかに侵入を早期に検知し、被害が出る前、または被害が拡大する前に対応するかが、対策のポイントとなる。そのためには技術的対策に加えて、何が必要となるのか？ここではプロセス・ヒトを中心としたセキュリティマネジメント体制の確立を提言したい。

セキュリティマネジメントの確立に求められるもの

このプロセス・ヒトを中心としたセキュリティマネジメント体制の確立には、3つの方策が考えられる。（1）新たなセキュリティリーダー（CISO）の確立と経営層の強いリーダーシップ、（2）全社横断のセキュリティ

管理組織の確立、(3) 専門人材を育成する仕組みの再整備である。企業の規模や事業特性などによって、最適解は個社ごとに異なるが、1つの指針として考えていただきたい。

(1) 新たなセキュリティリーダー（CISO）の必要性

強固なセキュリティマネジメント体制の確立には、経営層の強いリーダーシップ・コミットメントが不可欠である。しかし、セキュリティマネジメントの領域が制御システムやIoTシステムへと拡大することに伴い、従来のCIO（最高情報責任者）を中心とした責任・権限の配置では対応が難しくなっている。なぜなら制御システムやIoTシステムの開発、運用はCxO（各事業の最高責任者）の責任下であり、CIOの権限が及ぶことは少ないからである。

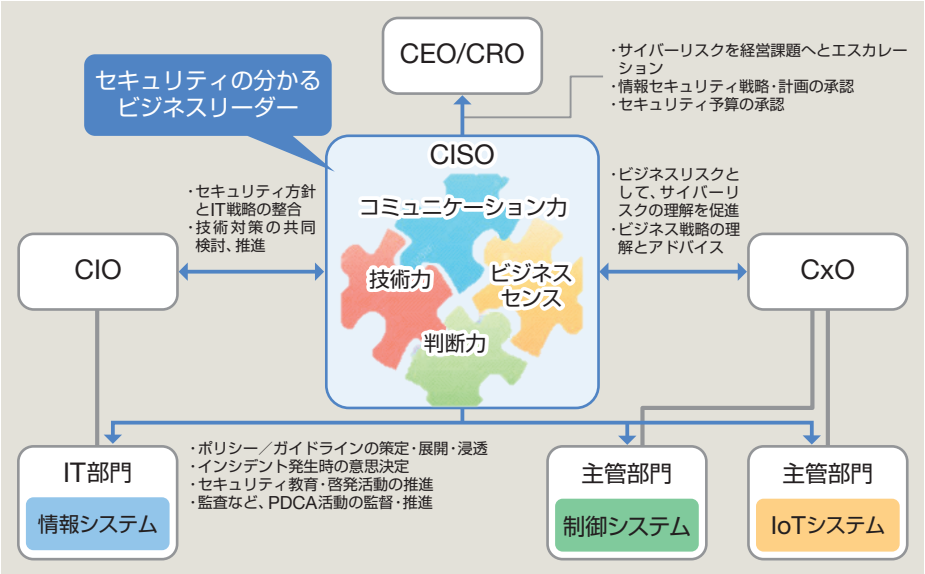
サイバーセキュリティで一歩先を行く米国では、サイバー攻撃を経営上の重要なリスクと捉え、CIOとは別にCISO（最高情報セキュリティ責任者）という専任ポストを設けることが一般的となっている。この形をとることで、制御システムやIoTシステムを含む全社のセキュリティリスクを経営層の間で共有し、経営一体となって統率を図ることが可能となる。さらにCISOが全社横断でのリソースコントロールや事故発生時の対応を統率することもできる。また、この形は、セキュリティ確保と相反することもある情報システムの最適化や事業利益の最大化の役割を分割し、CIOやCxOと相互に協調・けん制し合うことが可能となる利点もある。

CISOを担う人材には、大きく2つの役割が求められる。1つはCEOやCRO（最高リスク管理責任者）に対してビジネス視点でサイバーリスクを直接説明し、相談を受けるという経営と現場をつなぐ役割。2つ目はIT部門、主管部門など現場に対して、ポリシー策定、事故発生時の対応判断など、横断的に現場を統括する役割である。いわばCISOは「セキュリティの分かるビジネスリーダー」でなければならない。(図1参照)

CISOの確立に関して、サイバーセキュリティ分野で一歩先を行く米国と比べ、日本においては困難な側面もある。しかしながら、サイバー攻撃の脅威の甚大さを鑑みると、日本企業も米国の例を参考に経営における責任・権限の配置を再考すべきだろう。

経済産業省は、日本企業の経営層に対して

図1　新たなセキュリティリーダー（CISO）に求められる役割



サイバーセキュリティへの積極的な対策を促すため、2015年12月に「サイバーセキュリティ経営ガイドライン」を公開した。今後、こうした取り組みが浸透し、CISOなど経営層のリーダーシップの発揮につながることを期待したい。

(2) 全社横断のセキュリティ管理組織の確立

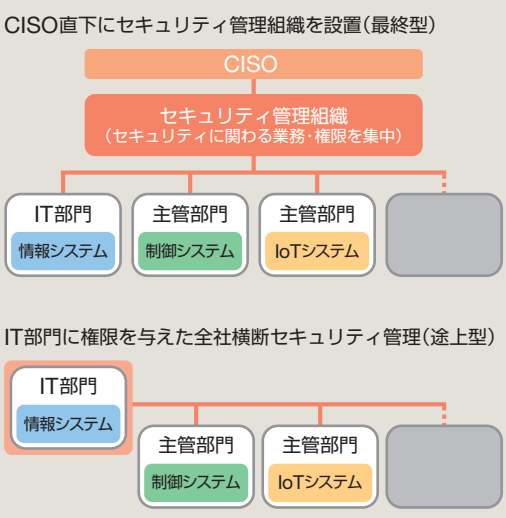
多くの企業では、情報システムはIT部門、制御システムは製造・生産部門、IoTシステムは製品開発部門やサービス部門というように、各部門が個別にセキュリティ管理に取り組んでいる。その結果、セキュリティ管理レベルが部門によってまちまちであり、セキュリティ管理のミッションが曖昧な個別の事業部門では管理が手薄になったり、部署間の連携がとられていなかったりというケースも少なくない。こうした管理体制のサイロ化は、事故発生時の情報集約や初動対応のスピードを妨げるだけでなく、自社の限られたリソース・ノウハウを分散させる原因となっている。

ここでは、全社横断の「セキュリティ管理組織」を確立することを提言したい。具体的には、CISO直下にセキュリティ管理組織を新設し、セキュリティに関わる業務・権限を集中化する形を目指すべきと考える。現場におけるセキュリティ対策の実行・管理業務は個別の事業部門の業務から切り離すことはできないが、セキュリティの「ポリシー策定」、「監査」、事故発生時の対応を迅速に行うための「セキュリティ監視」、「インシデント対応(一般的なCSIRTに当たる機能)」の機能を集約するメリットは大きい。リソース・ノウハウの一元化により、専門性を高めることができ、インシデント発生時の全社横断での調整・連携も円滑に進めることが可能となる。また、IT部門から独立した体制とすることで、セキュリティの領域がIT部門に閉じた活動ではないということを外形的に示し、セキュリティ管理を統制しやすい。(図2上図参照)

米国では、こうした形態をとる企業が増えているものの、日本ではまだ例が少ない。この組織形態は、既存体制との役割・権限設定が複雑となり、新たな人的リソースの調達も必要になることから、実行には経営層の強いイニシアチブが必要となるためである。そこで、組織の新設に向けた障壁が多い場合には、前述の管理組織を最終型として見据え、当面の対応としてIT部門に全社横断のセキュリティ管理の役割を付加する形が考えられる。(図2下図参照)

ある会社を例に挙げてみよう。社会インフラ企業A社では、IT部門に全社のセキュリティ管理の旗振りをする権限を与え、以降約3年間で、全社共通の仕組みを構築した。具

図2　全社を横断するセキュリティ組織の必要性



体的には、社長制定のセキュリティポリシーから部門単位のルールに至るまで全社の規定の再整備を実施。組織自体は従来通りであるため、セキュリティに充てられる人的リソースやコストが限られるという課題は残るものの、部門横断での管理レベルの底上げや連絡体制の一本化など一定の効果を得ている。

最初から最終型の前者を目指すか、第一歩として後者の形態を選択するかは、企業おのおのが自社の事情を踏まえてさまざまな要素を踏まえた熟慮が必要である。

(3) 専門人材を育成する仕組みの再整備

経営層のリーダーシップの下、セキュリティ組織を機能させていくには、セキュリティに精通した人材の育成・確保が不可欠である。

前述したセキュリティ管理組織には、特に2つの専門人材が必要になる。経営の意思を踏まえたセキュリティの方針・仕組みがデザインできる人材と、ログに基づく兆候の分析や被害範囲の調査などを行える人材である。

しかし、この人材確保が最大の難問でもある。情報処理推進機構（IPA）の調べによると、日本企業における人材不足が8.1万人、スキル不足が15.9万人（2014年7月「情報セキュリティ人材不足数などに関する追加分析について（概要）」より）にも及ぶとされている。従って、まずは自社内の人材でどこまでカバーすべきかを見極めることが重要となる。前述した2つの専門人材は内部で育成することが望ましいが、それ以外の作業を外部人材が担う、といった対応が考えられる。

次に、このような専門人材のキャリアパスを明確にすることが重要となる。以前から“IT部門のセキュリティ担当”というと、企画担当らを舞台裏で支えるいわば“縁の下の力持ち”と見られがちで、専門性を高めていった先にマネジメント力を発揮できるキャリアパスが想像しにくい状況にあった。企業は、セキュリティ専門人材の役割を重要かつ魅力的なキャリアとして明示しなくてはならない。そして、社内外の教育・訓練などへの参加を通じて、専門的な人材の育成に努める必要がある。

今こそ自社のセキュリティマネジメントの総点検を

近年、野村総合研究所（NRI）のシステムコンサルティングへ問い合わせいただくお客さまの声からも、サイバー攻撃への危機感が広がっていることは明確である。

今後、電力業界ではスマートメーターの普及による情報システムの連係、自動車業界ではスマートカーへのIT技術の活用、製造業では工場の自動化といったさまざまな業界、場面においてITのさらなる活用が進み、新たなセキュリティマネジメントの確立が急務となっている。

繰り返しとなるが、サイバー攻撃を完全に防ぐことが事実上困難となっている今、事故発生後の対応を含め、セキュリティマネジメントにおいて具体化すべきことは多い。また、サイバー攻撃の増加も懸念される今年6月の伊勢志摩サミットや2020年の東京オリンピックに向け、今こそが、セキュリティマネジメントを支える「プロセス」「ヒト」をいちから考える契機ではないだろうか。 ■