特集　デジタル時代の攻めと守りのIT戦略

迫り来るサイバー攻撃の脅威
今、企業に求められる新たなセキュリティマネジメント

木下雅史

CONTENTS

要　約

1　サイバー攻撃の標的は、社内の情報システムから、生産設備などの制御システムや、機械・電子機器に組込まれたITにまで拡大している。これらのITが攻撃を受けた場合、多大な経済損失や人命に繋がる危険性を孕む。企業は、サイバー攻撃への対策を社会的責務として捉え直す必要がある。

2　大規模化・巧妙化するサイバー攻撃に対し、すべての攻撃を未然に防ぐことは現実的ではない。今後は、防御策に偏重せず、侵入前提でどう被害を抑止するかを考える必要がある。従来より講じてきた技術的な対策に加え、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が鍵を握る。

3　近年、サイバー攻撃の標的拡大に伴い、IT部門のトップであるCIOが、全社のセキュリティ統括者であるCISOの役割を兼ねることは難しくなっている。今後は、CISOの役割をCIOの役割から分離し、新たなセキュリティリーダーとして明確化することが望ましい。

4　CISOの確立と同時に、CISOの直下に全社横断的なセキュリティ管理組織を確立し、セキュリティに係る業務、権限を集中化することが必要となる。理想形としては、IT部門と別組織としてセキュリティ専門組織を新設する形を提言する。

5　企業がセキュリティ人材を確保するためには、自社で育成すべき専門人材の人材像やキャリアパスの明確化が必要である。また、企業全体としてサイバー攻撃への対抗力を高めるためには、全従業員のスキル、マインドの底上げも不可欠である。

Ⅰ サイバー攻撃の脅威

1 サイバー攻撃の現状

昨今、パソコンやスマートフォンなどの情報端末だけでなく、自動車や医療機器、電気・水道・ガスなどのライフライン、交通インフラといった生きるために欠かせない機器やシステムまでもが、インターネット経由で管理・制御されつつある。

サイバー攻撃は、これらの新しいIT領域（IoTシステムや制御システム）へと標的を拡大し、猛威をふるっている。サイバー攻撃の件数は、IoTシステムや制御システムを対象にしたものを中心に、2010年から３年で約３倍まで増加（JPCERT/CC「インシデント報告対応レポート」より試算）している。同時に、サイバー攻撃が企業に与える影響や社会的影響も甚大なものとなっている。たとえば、ライフラインを支える発電所などがサイバー攻撃を受けた場合は、電力の安定供給が阻害され、国民生活に多大な影響を及ぼしかねない。自動車や医療機器のシステムが乗っ取られた場合は、人命をも脅かす危険性を孕む。もはや、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。

また、サイバー攻撃は日々進化しており、標的型攻撃やゼロデイ攻撃など、従来には無かった巧妙な手口を用いて、企業のセキュリティ対策の隙を突いてくる。従来と変わらない対策では、もはや太刀打ちできなくなっている。

2 サイバー攻撃の手口の変化

サイバー攻撃の変化を捉える特徴の一つとして、攻撃者の動機の変化がある。2010年以前は、「自己顕示」や「いたずら」を目的として不特定多数に向けたばらまき型の攻撃が多く見られたが、近年は「金銭」や「活動阻害」を目的として、特定の企業、組織に狙いを定めた巧妙な攻撃が増えている。

攻撃者の動機が変わると、攻撃の手口も変わる。DDos攻撃[注1]やリスト型攻撃[注2]など、さまざまな新しいタイプの手口が続発している。中でも、標的型攻撃は最も留意すべき代表的な手口である。この手口の最大の特徴は、攻撃者が標的としたネットワークへ侵入するために、人間心理の隙を突いた実に巧妙な手法を利用している点である。その最たる例が、組織のごく少数の構成員のみを対象に偽装した電子メールを送りつける標的型メールの手法であり、中にはメール受信者の警戒心を解くために個人的なメールのやり取りを数回繰り返すような事例も存在するという。ネットワークの入口をいくら強固に守っていたとしても、ヒトの脆弱性という新たな隙を突いてくるのである。

Ⅱ 事故事例から見えてくる対策の方向性

このようなサイバー攻撃の脅威に対して、企業はどのような対策を講じればよいだろうか。以降では、サイバー攻撃に対する企業の対応を考えるためのケーススタディとして、米国小売大手のターゲット・コーポレーションの事故事例を紹介する。

ターゲット社は2013年11月から12月にかけて不正アクセスを受け、約１億1000万件にも及ぶ顧客のクレジットカード情報やデビット

カード情報などが流出するという、史上最大規模の被害を被った。事故発生後、株価が急落、CIO（情報システム担当役員）、CEO（最高経営責任者）が相次ぎ辞任に追い込まれる事態となった。同社が事故発生後に投じた対応費用は6100万ドル、損害賠償額は1000万ドルにも上ると報じられている。

サイバー攻撃は、ターゲット社の取引先である空調業者が使用する認証情報を標的型攻撃で盗み取るところから始まった。攻撃者は、認証情報を用いることで、ターゲット社のネットワークに不正侵入した。そこで攻撃の基盤を築き、多数のPOS端末に、BlackPOSというPOS端末に特化したマルウェア（不正プログラム）を感染させ、大量のクレジットカード情報などを入手したという（図１）。

この事例は、標的型攻撃というサイバー攻撃に対する事前対策の難しさを知らしめたと同時に、ターゲット社のセキュリティ対策の不備、欠陥を浮き彫りにした。ターゲット社は「PCI DSS」というクレジットカード業界のセキュリティ基準の認証を事故発生の１年前に取得していたが、それでも被害の発生、拡大を防げなかった。

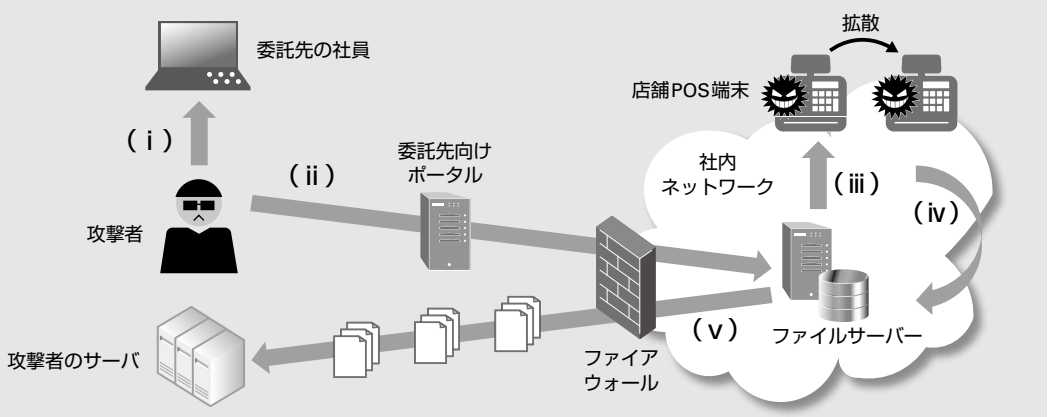
さまざまな調査機関によるレポートから、被害が発生し、拡大した原因について、以下のような事実が明らかとなっている。

①攻撃の侵入経路となった空調業者のPCには、ウイルス対策ソフトさえ搭載されておらず、攻撃者へ簡単に認証情報の搾取を許した

②最新のセキュリティ監視ツールが整備されていたにもかかわらず、ツールが発したアラートを見落としていたため、ウイルス感染範囲の拡大や情報漏洩の拡大を許した

③情報漏洩が始まってから10日後の社外通知を受けるまで、同社は攻撃を受けた事実に気付くことができなかった。同社は通知を受けた後、影響範囲の特定や対策

図1　米国小売 ターゲット社へのサイバー攻撃の概要



（攻撃の概要）
（ｉ）委託先の空調業者へ標的型攻撃を仕掛け、ターゲット社の社内ネットワークへの認証情報を入手
（ii）盗んだ認証情報を用いて、社内ネットワークに不正侵入
（iii）社内ファイルサーバーを踏み台に、多数のPOS端末にBlackPOSというマルウェア（POS端末への攻撃に特化した不正プログラム）を拡散
（iv）POS端末で利用された大量のクレジットカード情報などをファイルサーバーに不正転送
（v）社外にデータを不正転送

にさらに3日もの時間を要した

④事故発生に関する社外への公表が遅れ、情報漏洩した顧客情報の件数を幾度となく変更するなど、後手で不適切な対応が世間の不信を招いた

上記4点はいずれも、企業が取るべき今後の対策を考える上で、重要なヒントとなる。

①の原因は、たとえ自社において最新の対策を講じていたとしても、委託先までもが同様に対策を講じていなければ、攻撃者の侵入経路を断つことができないということを明らかにした。委託先のみならず、企業を取り巻くすべてのステークホルダーへ目を配り、セキュリティ対策を徹底することは容易ではない。攻撃者は事前の綿密な調査から、このような弱点を実に巧妙に突いてくる。

②の原因は、最新のセキュリティ監視ツールを導入していても、それを使いこなせるヒトがいなければ効果的な対策にはならないということを示した。セキュリティ監視ツールの検知の精度を高めるには、監視ログの設定など、細かい調整が必要となる。また、アラートが上がっても、最終的にはヒトがログの振る舞いパターンなどからシステムの異常を迅速に判断しなければならない。

③、④の原因は、有事における経営層と社外の間でのコミュニケーションの難しさを露呈させた。経営層が把握する事故の影響範囲や対応状況などの情報は時々刻々と変化し、不確実性の高い情報となる。経営層がこのような不確実性の高い情報に基づいて迷いなく判断し、社外とコミュニケーションを取ることは簡単ではない。経営層が、日頃からサイバーセキュリティへの意識を持ち、有事に備えておくことが必要となる。

以上の考察から、近年のサイバー攻撃に対し、従来の技術的対策に頼った対策で守りきることは不可能と考えられる。企業は従来の考え方を改め、プロセス・ヒトに重点を置いた対策のあり方を検討する必要がある。

Ⅲ 発生前提に立った対策に重点を

ターゲット社の事例が示す通り、大規模化・巧妙化するサイバー攻撃に対抗するには、すべての攻撃を防ぐことができるという従来の考え方から転換することが不可欠である。

また、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）が企業に与えるダメージが大きいことを理解しなければならない。

このような考えに基づき、企業は、サイバー攻撃の侵入を防御することに偏重するのではなく、侵入された場合に、いかに被害を未然に防ぐか、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である。これまでと同様、引き続き技術的な対策も講じていく必要があるが、それに加えて、プロセス・ヒトを中心とした対策が鍵を握ることになる。

以降では、これらを踏まえ、プロセス・ヒトを中心とした3つのセキュリティマネジメント強化策を紹介する。

①新たなセキュリティリーダー（CISO）の確立

②全社横断のセキュリティ管理組織の確立

③セキュリティ人材育成の仕組み作り

企業ごとにセキュリティ対策に充てられる人材リソースや投資余力、社会的に求められ

る責務の大きさなどが異なるため、最適解は個社ごとに異なるが、一つの指針として提言する。

Ⅳ 強化策①新たなセキュリティリーダー（CISO）の確立

新たなセキュリティマネジメントの確立には、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、サイバー攻撃の標的が拡大し、企業経営上のセキュリティリスクが増大する現況に鑑みると、従来のCIO（情報システム担当役員）を中心とした責任・権限では、対応が難しくなっていると考えられる。

1 CIOがセキュリティリーダーの役割を兼務し得るか

元来、実質的にIT部門のトップに立つCIOがセキュリティ管理の最高責任者の役割を兼務する形が主流であり、多くの企業は旧態依然とした形を維持してきた。CIOが、情報システムの最適化や事業利益の最大化と、セキュリティ確保の役割を一手に担い、そのバランスを取ってきたのである。

しかし、サイバー攻撃が新たに標的としている制御システムやIoTシステムに対して、CIOが従来通りセキュリティマネジメントの権限を発揮するのは難しい。なぜなら制御システムやIoTシステムの開発、運用は各事業部門のCxO（各事業担当役員の総称）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、サイバーセキュリティを経営上の重要なリスクと捉え、CIOとは別にCISO（情報セキュリティ管理担当役員）という専任ポストを設ける形が一般的となっている。制御システムやIoTシステムを含む全社のセキュリティマネジメントの権限をCISOに集中させることで、CISOが経営内での発言権を持ち、全社横断的にセキュリティ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役割を担うのである。

これにより、セキュリティリスクを経営層の間で共有し、経営と一体となって統率を図ることが可能となる。また、情報システムの最適化や事業利益の最大化の目的と相反することもあるセキュリティ確保の役割を分割し、CIOと相互に協調・牽制し合うことが可能となるという利点もある。

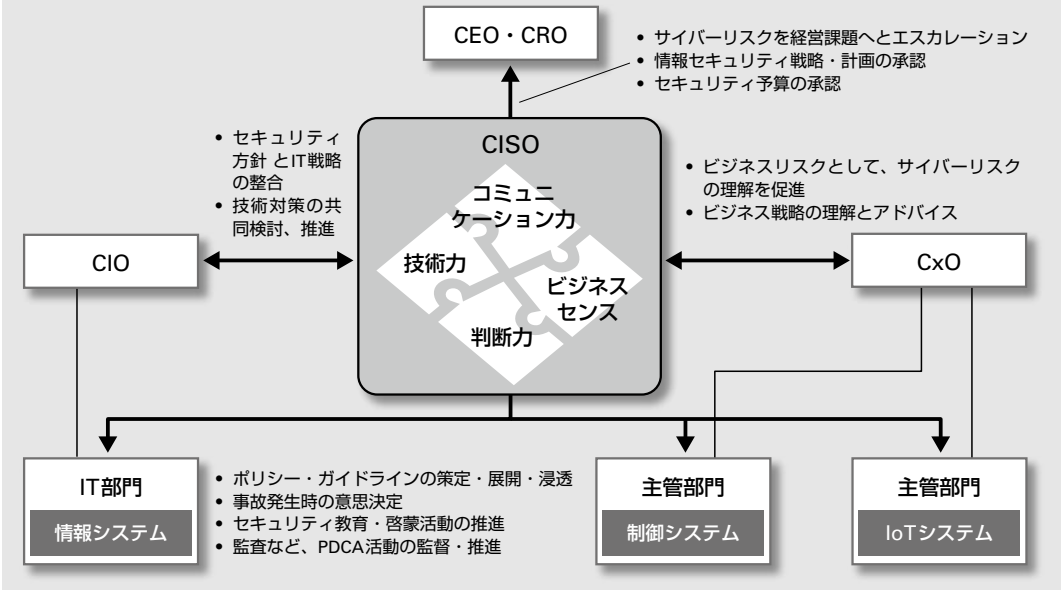
2 セキュリティリーダーに求められる役割

昨今、深刻さを増しているサイバー攻撃に対して、セキュリティリーダーに求められる役割は以前にも増して専門的なスキルが必要となっている。

CEOら経営層に対して直接コミュニケーションを取り、サイバーリスクを説明することが求められるため、ビジネス視点も必要となる。

また、セキュリティマネジメントを行うには、予防・被害最小化・早期復旧・再発防止などのリスク管理プロセスに沿って現場を統率し、活動を推進していかなければならない。IT部門、主管部門とポリシーを策定し、現場に落とし込む役割や、有事の際に迅速かつ正確な判断を行う役割を果たすためには、セキュリティに関するリスクや対策の内容に

図2　新たなセキュリティリーダー（CISO）に求められる役割



深い理解が必要となる。CISOはいわば「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2）。

このような専門的なスキルを、どのように身に付けていくかについては、課題が残る。CIOが兼務する形ではなく、セキュリティリーダーを独立したポストとすることで、確立を目指すことが望ましい。

3　CISOとほかの経営ポストの関係

セキュリティリーダーの役割をCISOとして設置した場合の、ほかのポストとの関係についても、米国の例が参考になる。

金融機関においては日米問わず、リスクマネジメントが重要であることから、ビジネスリスク全体をコントロールするCRO（リスク管理担当役員）を設置する形が一般的である。米国の金融機関においては、CISOをCIOの配下に位置づける形から、近年はCROの配下に位置づける形にシフトしているという。これは、セキュリティリスクの管理を、リスク管理や企業統制の一環と位置づけて推進する狙いがある。CIOやCxOの管理下である情報システムや制御システム、IoTシステムに対し、セキュリティ対策の十分性や妥当性を客観的な立場から評価し、牽制することが可能となる。

CISOの確立に関して、サイバーセキュリティが産業として発達しており、数多くのセキュリティ専門人材を輩出している米国と比べ、日本においては困難さが付きまとう。しかしながら、サイバー攻撃の脅威の甚大さに鑑みると、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であろう。

経済産業省は、日本企業の経営層に対してサイバーセキュリティへの積極的な参画を催すため、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（図3）。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発揮につながるこ

図3　サイバーセキュリティ経営ガイドライン

同ガイドラインは、経営者が認識する必要がある「3原則」に加え、
以下、担当幹部（CISOなど）に指示すべき「重要10項目」の具体的な内容、対策例などを提供している

情報セキュリティ対策を実施する上での責任者となる担当幹部（CISOなど）に
指示すべき「重要10項目」

1　リーダーシップの表明と体制の構築
(1) サイバーセキュリティリスクの認識、組織全体での対応の策定
(2) サイバーセキュリティリスク管理体制の構築

2　サイバーセキュリティリスク管理の枠組み決定
(3) サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
(4) サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
(5) 系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握

3　リスクを踏まえた攻撃を防ぐための事前対策
(6) サイバーセキュリティ対策のための資源（予算、人材等）確保
(7) ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
(8) 情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備

4　サイバー攻撃を受けた場合に備えた準備
(9) 緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施
(10) 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

とを期待したい。

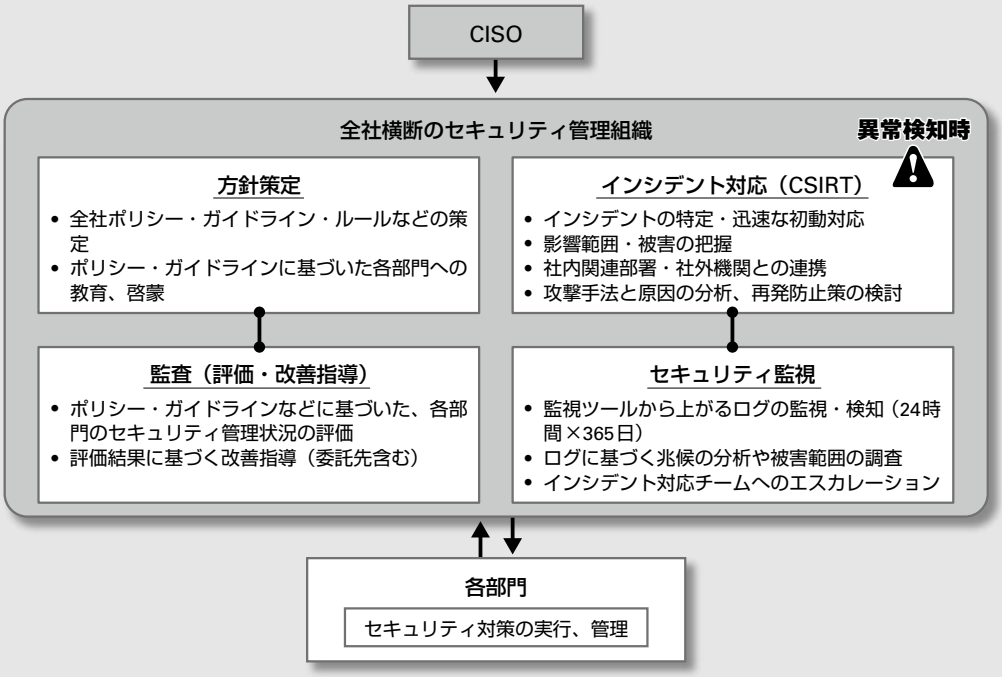
V　強化策②全社横断のセキュリティ管理組織の確立

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おざなりになっているケースも少なくない。こうしたセキュリティ管理体制のサイロ化は、事故発生時の対応における情報集約や初動対応の判断など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。セキュリティマネジメントを全社一体で行うための「方針策定」「監査（評価・改善指導）」、事故発生時の対応を迅速に行うための「インシデント対応（一般的なCSIRTにあたる機能）」「セキュリティ監視」の機能を集約する形である（図４）。

具体的な機能配置としては、CISO直下のセキュリティ専門組織を新規に設置し、権限を集中化する形が最も理想的である。リソース・ノウハウを一元化することで、専門性を高めることができ、事故発生時の全社横断での調整・連携も円滑に進めることができる。また、IT部門と独立した体制とすることで、サイバーセキュリティの領域はIT部門に閉じた活動ではないということを外形的にも示すことができ、セキュリティ管理の統制を働

図4　全社横断のセキュリティ管理組織



かせやすい。

米国では、こうした形態を取る企業が増えているものの、日本ではまだ例が少ない。この形態には新たな人的リソースの調達や、既存体制との役割・権限設定が複雑となり、実行には経営層の強いイニシアティブが必要となることが障壁となるためである。このような場合には、セキュリティ専門組織の立ち上げを最終形として見据えつつ、IT部門に全社横断のセキュリティ管理にかかわる役割を付与する形が考えられる。

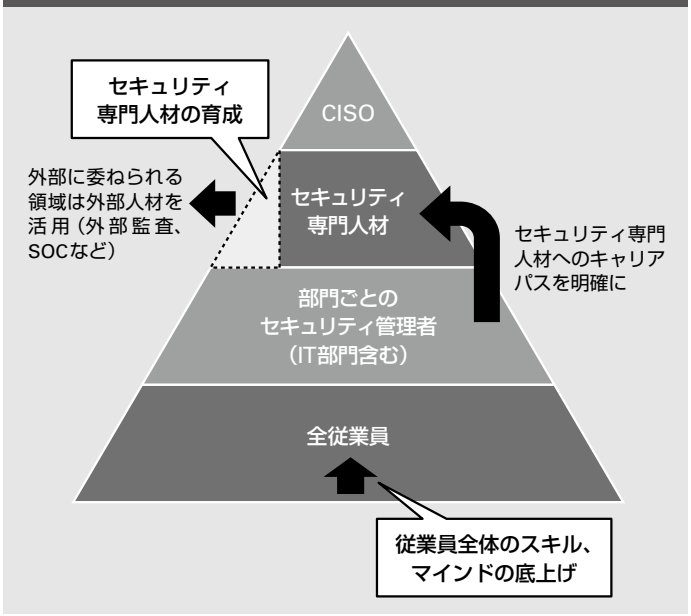
社会インフラ企業A社では、IT部門に全社のセキュリティ管理の旗振りをする権限を与え、以降約３年の期間を経て、全社共通の仕組みを構築した。具体的には、社長制定のセキュリティポリシーから部門単位のルールに至るまで全社の規程の再整備を実施。組織自体は従来通りの体制であるため、セキュリティに充てられる人的リソースやコストが限られるという課題は残るものの、部門横断での管理レベルの底上げや連絡体制の一本化など、一定の効果を得ている。

最初から最終形の前者を目指すか、第一歩として後者の形態を選択するかは、企業各々が自社の事情を踏まえて検討していく必要がある。「監査」や「セキュリティ監視」の機能の一部を、外部の専門企業に委託することも考えられる。自社にとってどのような形が良いのか、さまざまな要素を踏まえた熟慮が必要である。

Ⅵ 強化策③セキュリティ人材育成の仕組み作り

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

図5　セキュリティ人材の類型



に精通した人材の育成・確保が不可欠である。しかし、これが最大の難問でもある。なぜならば、一企業に限られた問題ではないからである。

情報処理推進機構（IPA）の調べによると、日本企業におけるセキュリティ人材の不足は8.1万人、スキル不足が15.9万人にも及ぶ[注3]とされており、国内全体での人材難の問題も根深い。企業は、このような厳しい状況下で、セキュリティに精通した人材をどう育成・確保するべきかについて再考し、手を打たなければならない。

以降では、セキュリティ人材を類型化し、セキュリティ専門人材と従業員全体に関する人材育成のポイントを提言する（図５）。

1　セキュリティ専門人材の育成

前述した、全社横断的なセキュリティ専門組織を確立するには、それを担う高度なスキルを有する人材の育成･確保が不可欠となる。

これらの人材すべてを、企業が自前で育成することは容易ではない。そのため、まずは、外部を活用する領域と自社内の人材でカバーするべき領域の境界を見極めることが重要となる。

セキュリティマネジメントの頭脳となるマネジメント人材は自社で育成しなければならない。経営の意思を踏まえたセキュリティの方針・仕組みをデザインできる人材は、外部から調達することは困難である。

加えて、セキュリティ事故発生後の的確な判断を司る重要な役割を担う人材もまた、内部人材で賄われることが望ましい。ログ監視・検知の業務は外部に委託することが可能だが、ログに基づく兆候の分析や被害範囲の調査などには、自社のシステム・業務の全体像に関する深い理解が必要となるためである。これらの人材を内部人材で賄い、それ以外を外部人材で賄う、といった思い切った対応が求められる。

次に、企業はこれら専門人材のキャリアパスを明確化する必要がある。従来、「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を想像しづらい状況にあった。企業は、セキュリティ専門人材の役割を事業運営上、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、育成に努めなければならない。

2　従業員全体のスキル、マインドの底上げ

企業のサイバー攻撃に対する対応力を高め

るためには、セキュリティ事故の発生源となり得る従業員全体のスキル、マインドの底上げも不可欠である。

従業員が保有するパソコンがウイルス感染し、踏み台とされれば、被害者の立場であると同時に加害者の立場にもなり得る。このようなマインドの転換を図るため、標的型メール訓練をはじめとした取り組みを通じて、従業員の心に働きかけるような工夫が必要である。

昨今、増える内部犯罪に対して、抑止力を働かせるための工夫も取り入れたい。小さいミス（ヒヤリハット）を見過ごし続けると、その積み重ねが従業員の悪意を引き出すきっかけとなる。未然に「監視の目があること」を知らせる仕掛けを取り入れた対策を講じておきたい。

Ⅶ 今こそ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の問い合わせからも、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。

電力業界では電力小売の自由化に伴うスマートメーターと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技術活用、製造業では工場の自動化など、さまざまな業界においてITのさらなる活用が進み、新たなセキュリティ管理体制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難しくなっている今、事故発生後の対応を含め、セキュリティ管理体制において具体化すべきことは多い。また、2016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、サイバー攻撃の増加も懸念されている。つまり、今こそが、セキュリティ管理体制を支える「プロセス」「ヒト」を一から考える契機だといえる。

NRIは、企業のIT活用力を支援するサービスを提供するとともに、企業が直面するセキュリティマネジメントの問題についても、NRIグループのセキュリティ専門会社「NRIセキュアテクノロジーズ」と連携して、貢献していきたいと考えている。

注

1 DDos攻撃：多数のコンピュータ群を踏み台に、標的となるコンピュータに対して大量の処理負荷を与えることでサービスを機能停止状態に追い込む手法

2 リスト型攻撃：攻撃者が何らかの手法によりあらかじめ入手したリスト化したID・パスワードを利用してウェブサイトにアクセスを試み、利用者のアカウントで不正にログインする攻撃

3 2014年7月30日「情報セキュリティ人材不足数等に関する追加分析について（概要）」

著者

木下雅史（きのしたまさし）
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
専門はIT組織改革、セキュリティマネジメント