企業における情報セキュリティ実態調査

金子洋平

CONTENTS

要 約

1　NRIセキュアテクノロジーズでは、毎年「企業における情報セキュリティ実態調査」を実施している。2016年の調査結果からは、情報セキュリティ人材の不足、巧妙化するサイバー攻撃への対策の遅れ、IoTセキュリティの関心の高さ、の3点に関して、特徴的な傾向が見られた。

2　情報セキュリティ人材の不足を感じている企業の割合は89.5％と過去4年間で最も多かったが、人材確保・強化のための施策を実施していない企業も約3割に上ることが分かった。

3　標的型メール攻撃やランサムウエアによる金銭要求などの新しい攻撃が、急速に広がっている。一方で、企業におけるセキュリティ対策は、それらに追いついていない状況である。セキュリティ対策高度化のため、継続的な情報収集と、自社のセキュリティ状況の定期的な評価・可視化・分析が必要である。

4　IoTに多くの企業が関心を寄せている一方で、自社ビジネスへの活用は進んでいない。その一因として、情報セキュリティ対策の困難さを挙げる企業も多い。IoTは、ビジネスに合わせてさまざまな形態がある。このため、自社のノウハウを活かしたセキュリティ対策を推進することが重要である。

5　情報セキュリティの推進を前提とした各種施策が必須であるにもかかわらず、縦割り組織による部門間連携の不足、継続したセキュリティ施策の実施不足などの課題が浮き彫りになった。各社の経営トップがセキュリティをしっかりと意識し、これらの改善に努めることが必要と考える。

Ⅰ 企業における情報セキュリティ実態調査について

本稿では、NRIセキュアテクノロジーズが毎年実施している「企業における情報セキュリティ実態調査（以下、本調査）」の分析結果について述べる。

本調査は、企業の情報セキュリティに関する取り組みの実態を明らかにし、企業の情報システム・情報セキュリティ関連業務に携わる人への有益な参考情報を提供するために、2002年に開始して以来、最新の16年調査に至るまで計15回実施している。最新の調査は、調査期間を16年９月５日から10月14日までとし、上場企業および従業員数の多い非上場企業3000社を対象に実施し、回答をいただいた671社からのアンケート結果を基に分析を行った。

最新調査の結果からは、以下の３つの注目すべき課題が明らかになった。１つ目は、情報セキュリティ人材・経営に関して、９割近くの企業がセキュリティ人材の不足を唱えている。また、最高情報セキュリティ責任者（Chief Information Security Officer：CISO）が未設置である企業が半数以上となっている点である。２つ目は、標的型メール攻撃、ランサムウエアなど巧妙化したサイバー攻撃が急速に増加しているにもかかわらず、それらの攻撃への対策実施企業は、実施率が高い対策でも３割程度となっている点である。17年度に入ってからもWannaCryやApache Struts2などの攻撃が世間を騒がせており、巧妙な攻撃への対策実施の必要性が急速に高まっている。３つ目は、昨今の新技術について調査したところ、５割以上の企業がIoTに関心を持ち、そのうち４割以上の企業がIoTに関する課題としてサイバー攻撃リスクを挙げ、IoTへの関心の高さとサイバー攻撃に対する懸念の高さとの関連の大きさがうかがえた点である。

本稿では、最新調査の結果から、特に注目すべき３テーマを中心として、分析結果の詳細と課題に対する提言を行う。

Ⅱ 情報セキュリティ人材の不足

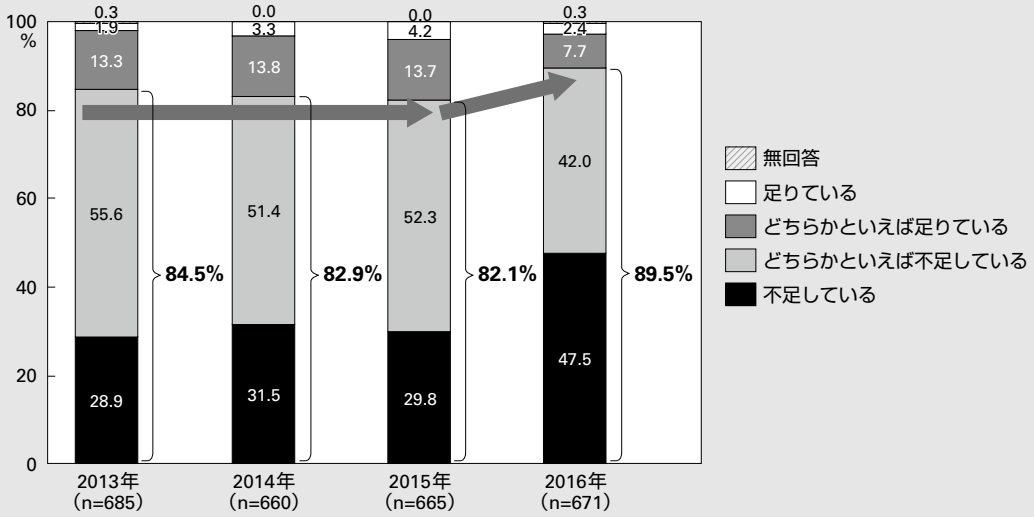
1 情報セキュリティ人材の充足状況

図１は、2013年から16年までの情報セキュリティ人材の充足状況の結果を示している。４年連続で「どちらかといえば不足している」と「不足している」の合計が80％を超えており、セキュリティ人材が一貫して不足していることがうかがえる。特に、最新の16年調査においては89.5％に増えており、過去最も高い割合であった。これは、15年度前後で起きた巧妙なサイバー攻撃、内部不正による情報漏洩事故が多発していることや、サイバーセキュリティ経営ガイドラインでセキュリティ人材を各企業が確保すべきという指針を打ち出されたことなどによる人材確保の重要性の高まりなどが一因になっていると考えられる。

社会からの情報セキュリティ人材確保の要請だけでなく、セキュリティ業務の需要自体も近年大きく増えている。理由としては、昨今企業の業務や提供するサービスの多角化・効率化のためにITを活用する場面が多くなり、情報セキュリティの脅威を考慮しなければならない範囲が格段に広がっている。さら

図1　情報セキュリティ人材の充足状況

Q.貴社の情報セキュリティの管理や、社内システムのセキュリティ対策に従事する人材の充足状況はいかがですか



注）小数第2位で四捨五入したため、合計が100にならない場合がある
出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査」（2013~2016年）

に、セキュリティの脅威は年々高度化・巧妙化してきており、従前の対策では防げない手法が日々増えてきているためである。

このような背景の中、情報セキュリティに関する対策は、量の増加はもちろんのこと、質の向上も求められている。しかし、幅広い知識を持ち、かつ日々進化する脅威に対して常に高度かつ最新の専門性を持ったセキュリティ人材は極めて少ない。

2　人材の獲得・強化のための実施施策

セキュリティ人材不足を解消するために、人材を獲得・育成するには3つの施策が考えられる。

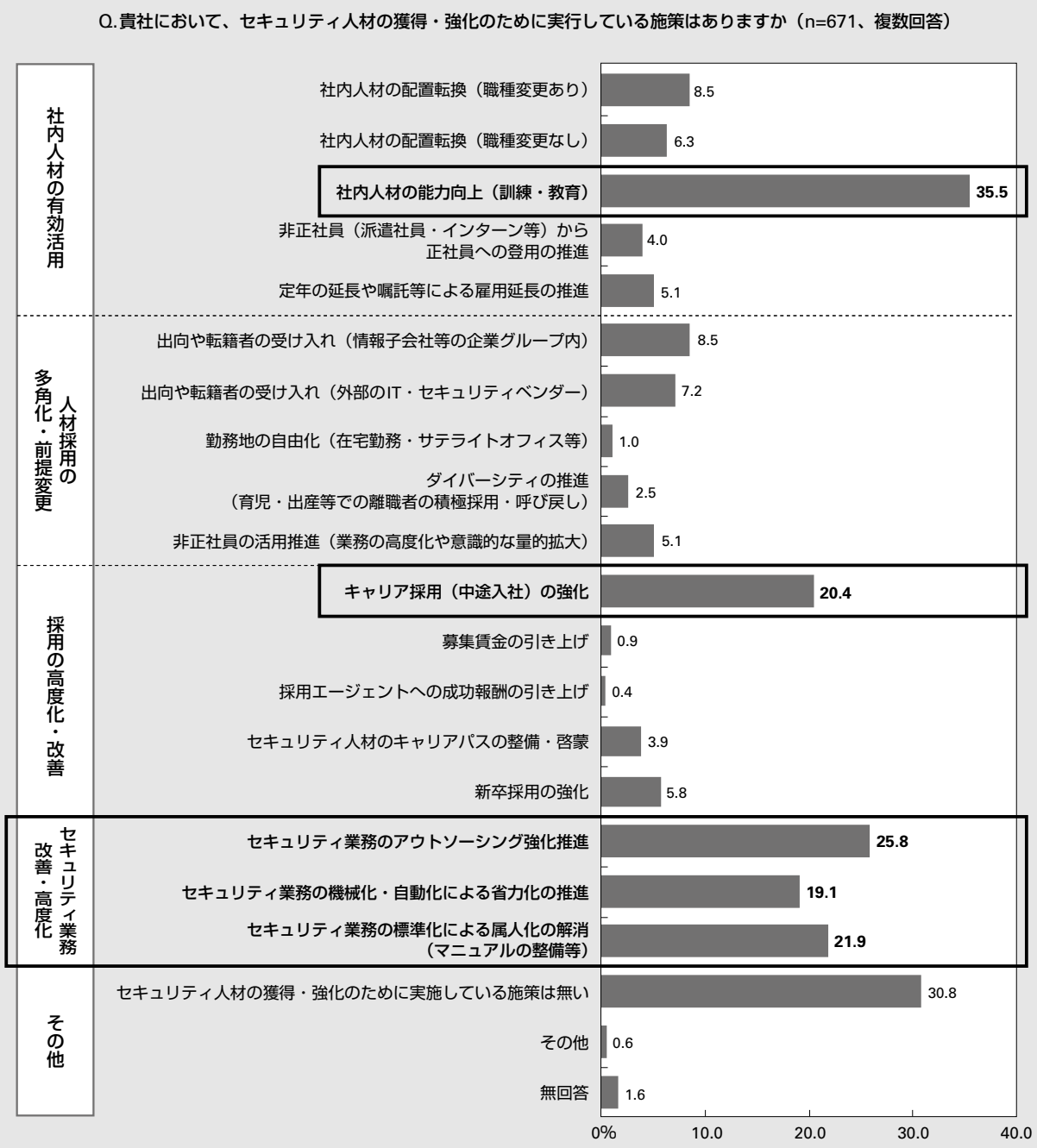
1つ目は、社内人材の有効活用である。配置転換や教育などにより、通常の組織・人事施策の中で人材を確保する方法である。2つ目は、人材の採用や転籍者の受け入れといった外部からの人材受け入れである。3つ目は、業務の自動化や改善、アウトソーシングを活用して社員一人当たりの生産性を高める方法である。

図2は、情報セキュリティ人材の獲得・強化のために各社が実施している施策の実施割合を示した結果である。全体を通して、3つ目の施策に当たる業務の自動化、改善やアウトソーシングといった「セキュリティ業務改善・高度化」の割合は20%前後となっており比較的高いことが分かる。

「社内人材の有効活用」では、社内人材の能力向上（訓練・教育）割合が35.5%と最も高く、外部からの人材調達と比べて、情報セキュリティ人材を自社育成している企業の割合が高いことも分かった。

採用に関する項目（「人材採用の多角化・前提変更」および「採用の高度化・改善」）では、キャリア採用の強化の割合が20.4%と

図2　情報セキュリティ人材の獲得・強化のために実施している施策



出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査」（2016年）

最も高く、人材の多くを新卒採用で調達する日本企業においても、情報セキュリティ人材は、キャリア採用によって即戦力として確保したいという企業の本音が表れている。これは、今まで多くの企業で、情報セキュリティ人材の確保・育成を意識した人事・教育制度

の確立が不足しており、昨今の急激な情報セキュリティ対策の要請を、自社の人材育成だけでまかなうことが困難であるためだと考えられる。

一方で、社内人材の有効活用に関して、教育・訓練以外の「正社員登用」「配置転換」や「雇用延長」といった人材の雇用形態や配置変更を伴う施策については、どの項目も実施率が10％を下回った。これは、経済産業省の「IT人材の最新動向と将来推計に関する調査」でも言及されている通り、情報セキュリティ人材が需要数から13万人以上不足していること、さらに部門を超えた異動や雇用形態の変更が難しい日本の組織独特の事情が、社員登用や配置転換といった施策の実施率を押し下げていると考えられる。また、「募集賃金の引き上げ」「採用エージェントへの成功報酬の引き上げ」の実施率は１％にも満たなく極めて低い。ところが、米国やシンガポールではこれらの施策の実施率も20～30％[注1]であり、人材獲得の主要な選択肢となっている。

これにより、日本企業は金銭を用いた人材獲得施策の割合が低いことが分かる。これは単純な雇用慣習や国民性の違いだけではなく、サイバー攻撃被害件数や規模、それに付随する経営者の情報セキュリティそのものへの関心の高さに違いがあると筆者は考えている。

さらに、「セキュリティ人材の獲得・強化のために実施している施策は無い」と答えた企業が30.8％であり、人材不足を認識しているものの具体的な人材の獲得・育成に向けて動けていない企業が多いことも明らかになった。

3　人材の獲得・強化が推進できない理由

情報セキュリティ人材の獲得・強化が進まない理由として、組織の中に全社的な情報セキュリティ戦略を推進する役割が不在であることが挙げられる。情報セキュリティを推進するに当たり、まずは推進するための計画を策定し、それに基づく自社の情報セキュリティ業務の棚卸しと、今後必要になる業務の明確化が必要である。そして明確化されたセキュリティ業務に沿った人材強化施策や人材獲得施策を実施する必要がある。

しかし、現状では多くの企業で自社の目指すセキュリティの姿が明確化されていないため、強化すべき人材像や獲得すべき人材像を明確化できず、そのための施策が実施できない状況にあると考えられる。さらに、施策の推進には社内の他部署との調整も多く必要となるが、その調整を行う全社的な情報セキュリティを推進する役割が不在であるため、他部署との調整が多く必要な、配置転換や正社員登用、採用時の募集賃金の引き上げなどの施策を実施できなくなっているのが現状である。

4　人材の獲得・強化の推進方法

全社的な情報セキュリティ施策を推進する役割を担うのは、通常CISOである。今回のアンケート結果では、兼任も含めたCISOの設置率は46.8％となっており、半数以上の企業がCISOを設置していない。各企業は情報セキュリティをしっかりと守っていく必要があるわけだが、社内に情報セキュリティを推進するリーダーが不在のため、他部署との連携が必要な人材の強化や獲得を思うように行えていない。まずは、情報セキュリティ経営

ガイドラインなどを参照し、企業経営において情報セキュリティが極めて重要であることを経営層が意識した上で、全社的な情報セキュリティ施策を推進するリーダーの設置が急務である。

Ⅲ 巧妙なサイバー攻撃への対策状況

1 サイバー攻撃の被害状況

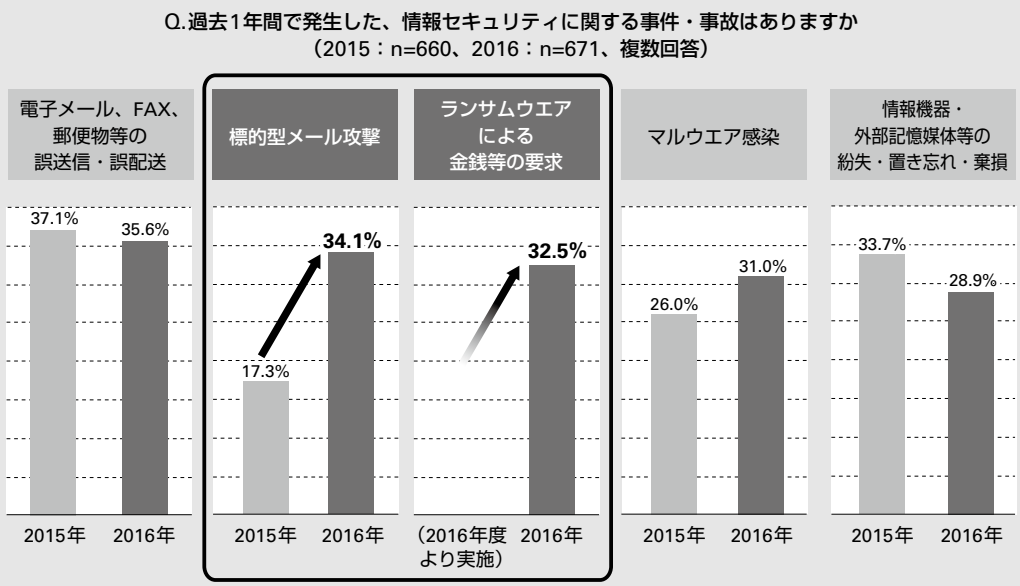
第Ⅲ章では、昨今のサイバー攻撃の傾向と、企業の対策状況について述べる。図3は、企業で2016年に発生した各情報セキュリティに関する事件・事故のうち、割合が高い上位5つの事件・事故に対して、15年と16年の遷移を整理した。

15年に起きたセキュリティ事件・事故で最も多かったのは37.1％の企業で発生している「電子メール、FAX、郵便物等の誤送信・誤配送」である。16年においても35.6％と最も割合が高い。次いで、15年に多かったのは33.7％の「情報機器・外部記憶媒体等の紛失・置き忘れ・棄損」であり、16年でも28.9％の企業で発生しており、5位であった。このことから、15年はヒューマンエラーなど人為的ミスによる事件・事故の発生割合が高かったことが分かる。ただし、上記2つの事件・事故とも、15年に比べて16年は減少している。誤送信・誤配送については、度重なる大規模情報漏洩事故の発生などにより誤送信防止ソフトなどによってある程度防ぐことや、運用で誤送信・誤配送を防ぐ対策を実施している企業が増えてきていると考えられる。

また、紛失・置き忘れ・棄損については、情報セキュリティのポリシー・ルールが整備・浸透され、会社としてのセキュリティ意識が徐々に向上していることが考えられる。

一方、16年の「標的型メール攻撃」の割合は、15年の17.3％から34.1％と2倍近くに増えた。また、「ランサムウエアによる金銭等の要求」は16年から追加した選択肢であるが、32.5％と全体の中で3番目に多い割合となってい

図3　2016年に発生した事件・事故のうち割合が高い上位5種類と2015年からの遷移



出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査」（2015年、2016年）

る。16年は、ばら撒き型と呼ばれるマルウエアの大量配信が猛威を振るった年であった。そのため、15年に比べて16年は、企業が「標的型メール攻撃」と「ランサムウエア」の被害を受けた割合が、大幅に増加したと考えられる。

ヒューマンエラーなどに起因する事件・事故は微減傾向であるが、標的型攻撃、ランサムウエアなど巧妙なサイバー攻撃の割合は大幅に伸びており、企業にとってそれらの攻撃への対策を行うことが急務であるといえる。

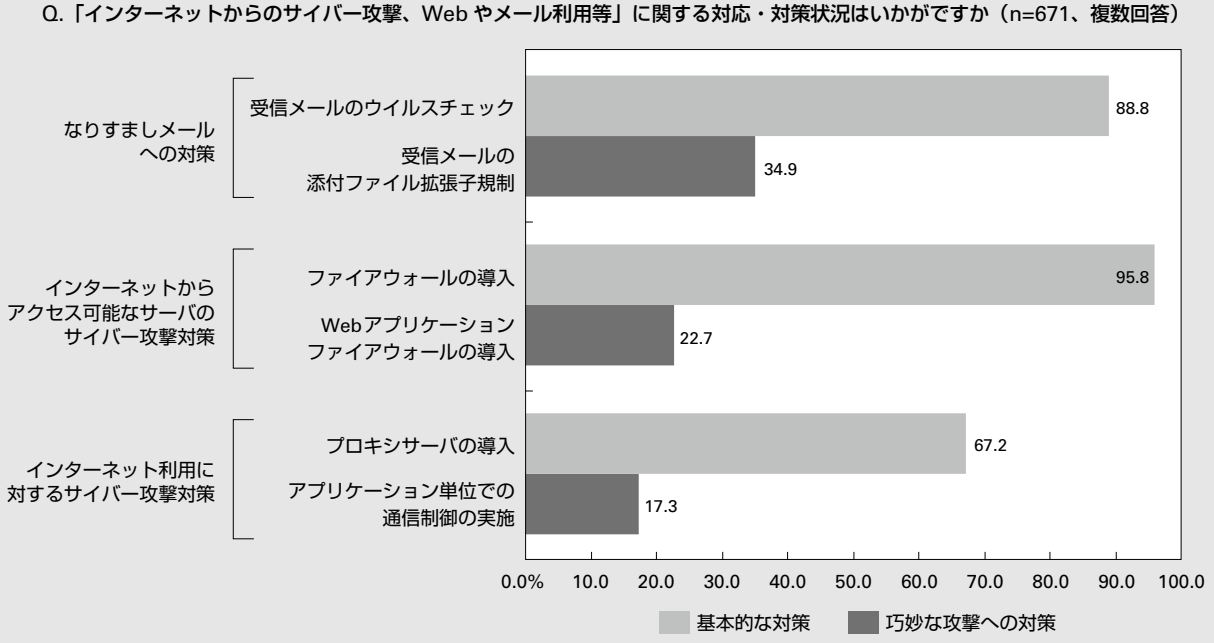
2　追いつかない対策の高度化

図４の企業におけるセキュリティ対策の状況を整理した結果から、多くの企業の対策は昨今の巧妙なサイバー攻撃の増加傾向に対して、追いついていないことが分かる。

まず、「なりすましメールへの対策」については、「受信メールのウイルスチェック」が88.8％の企業で行われているが、「受信メールの添付ファイル拡張子規制」の実施割合は34.9％にとどまっている。 巧妙化する標的型メールによる攻撃は、既存のウイルスチェックでは発見できない未知のパターンのウイルスやあえて暗号化して送付するようなものも多いため、「受信メールの添付ファイル拡張子規制」などの対策で、怪しいメールは未然に防ぐ対策を行うことが望まれる。さらに、最近の巧妙化するなりすましメール対策のトレンドとしては、ウイルスの振る舞いをチェックして駆除する方法も増えてきている。

次に、「インターネットからアクセス可能なサーバのサイバー攻撃対策」については、「ファイアウォール（FW）の導入」は95.8％とほとんどの企業が導入しているが、「Webアプリケーションファイアウォール（WAF）の導入」は22.7％程度にとどまっている。FWは外部からのすべての通信を制御する重要な機器であるが、WAFについては対外的に動的なWebサイト（ECサイトなど）を多

図4　サイバーセキュリティ対策状況（代表例）



出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査」（2016年）

く提供していない場合、Webサイト個別の対策（セキュアなWeb開発、脆弱性診断・ペネトレーションテストなどによる脅威への対応）により対応することも多いため、需要が少ない。

ただし、WAFは、Webサイトを狙う代表的な攻撃（SQLインジェクションやクロスサイトスクリプティングなど）への対策に有効なだけでなく、ゼロデイ脆弱性への攻撃を防ぐことも期待できる。脆弱性が発見された場合でも、Webサイトへ脆弱性プログラムのパッチを当てるまでには時間を要するため、その間のゼロデイ攻撃への緩和策としてECサイトを多く持つ企業のWAFでの対策需要が多い。

「インターネット利用に対するサイバー攻撃対策」については、「プロキシサーバの導入」が67.2％とさほど高くなく、さらに「アプリケーション単位での通信制御の実施」については17.3％しか実施していない。インターネットからのメールやWebなど通信のアクセスについてはある程度セキュリティ対策を行っているが、内部からインターネットへのアクセスに対するセキュリティについては、外部からの脅威に対する対策より割合が低いことが分かる。

Ⅳ IoTセキュリティ

1 IoTへの関心と課題認識

本調査では、毎年のトレンドとなっている技術や製品の導入、関心状況も調査している。2016年は、「IoT」を含む５項目（IoT、人工知能、VR・AR、FinTech・ブロックチェーン、STIX・TAXII）、について導入、関心状況の調査を行った。IoTについては、「導入済み・利用している」「検討中・関心がある」の合計が52.3％となっており、調査を行った５項目の中で最も関心が高いことが分かった。IoTは、今までインターネットにつなげていなかったモノがインターネットに接続されることで相互に制御する仕組みのことで、スマート工場や電力供給などをはじめとしてさまざまな分野での活用が期待されており、既にIoTの技術を活用したサービスや生産ラインの効率化に力を入れている企業が増加傾向にある。

しかし、IoTに関心のある企業が半数を超えている一方で、実際にIoTを導入・利用している企業の割合は５％程度となっている。本調査では、IoTを導入するに当たっての課題についても調査しており、その結果として、企業が挙げる主な課題は「IoTを活用したビジネスモデルの策定」が59.8％と最も多いが、「機器をインターネットに接続することによるサイバーリスクの増大」も41.9％と続き、IoTを導入・利用するに当たりセキュリティ課題が足かせとなり、導入・利用に踏み込めない企業も多いということも分かった。

2 IoTとセキュリティ脅威

IoTでは、概念が普及し始めた当初から、システムの構成要素の多さ、セーフティとセキュリティを考慮する必要性、インシデント発生時の被害の大きさなどから、セキュリティ対策の重要性とその対応の難しさが指摘されていた。対策の不備を突かれて、実際にドイツの製鉄所で制御システムが不正操作され高炉が損傷する事故[注2]や、実証研究ではあるが、空調機器の不正操作[注3]、リモートか

らの自動車への不正操作[注4]などの攻撃・事故事例がある。

IoTはデバイス、ネットワーク、クラウドなど多くの構成要素を持ち、IoTシステムではそれらが一体となって１つのシステムを提供しており、構成要素の一つ一つに対してセキュリティを考慮する必要がある。構成要素の１つに脆弱性などの問題があると、すべてのモノに対して脆弱性を突いた攻撃を受けるリスクが高まり、IoTシステム全体としてセキュリティを維持することができなくなってしまうからである。また、その脆弱性などの問題に対応する場合、多く提供しているデバイスやネットワークすべてに対して対応する必要があり、その対応への影響も大きい。

IoTシステムは、ここまで述べてきた通り、多くの構成要素に対して一つ一つ確実なセキュリティ対策を施さなくてはならない。また、新たな脅威に対する対応（脆弱性への対応など）を膨大なデバイスに対して行わなければならない点から情報系システムに比べ、セキュリティの初期対策だけでなく、新たな脅威に対して継続したセキュリティ維持管理を行うことが困難である。このような背景の中でIoTシステムにおけるセキュリティを担保するためには、デバイス、ネットワーク、クラウド、システム（サーバなど）などの構成要素で切り分けを行った上で、各構成要素に対して、網羅的な対策を施すだけでなく、継続してセキュリティを担保できるようにすることが肝要である。

3　自社IoTに合ったガイドライン作成が重要

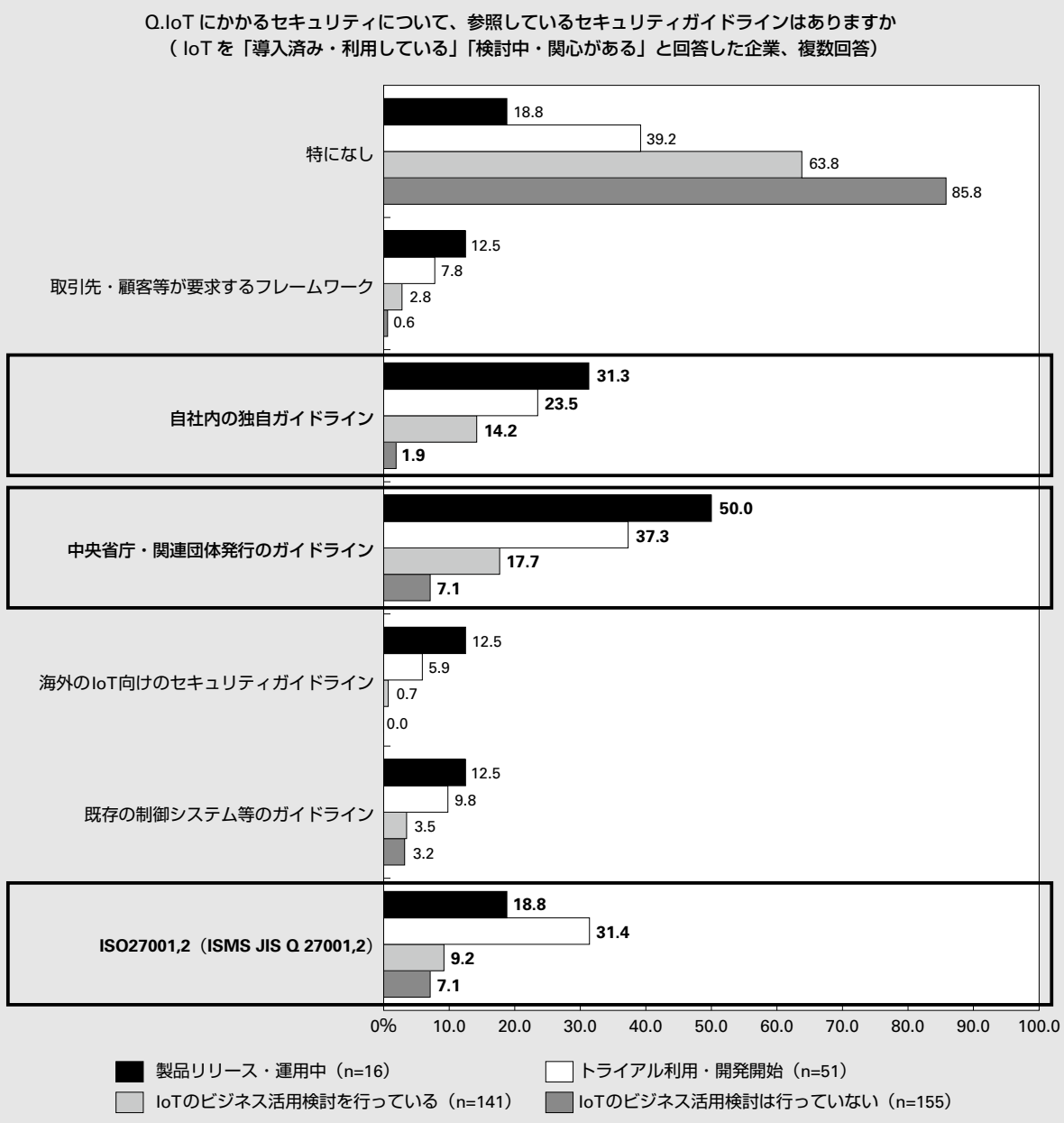
システムのセキュリティを担保する上で、どのような対策を実施するべきかを考えるときには、まず、各種団体が公開しているガイドラインを参考にすることを推奨する。情報系システムのセキュリティガイドラインは、官公庁や業界団体などが多くのガイドラインを発行しており、広く利用されている。IoTシステムのセキュリティガイドラインについても、2015年頃から国内外のいくつかの団体から発行され始めている。しかし、情報系システムのガイドラインとは異なり、標準的に活用されているものや業種などに特化したものがいまだ整備されていない状況である。

図５は、IoTに関心を持つ企業のうち、IoTシステムの検討、開発段階別に参照しているガイドラインの種別をまとめた図である。IoTに興味を持っている企業は、「中央省庁、関連団体発行のガイドライン」「自社内の独自のガイドライン」「ISO27001,2」の３種類の利用率が高いことが分かった。その中でも、特に注目するべき点が２つある。

１つ目はISO27001,2を参照する企業は、検討段階の初期で利用されている割合が高く、IoTシステムの開発段階が進むにつれて増えてきているが、実際にIoT製品をリリースしている企業・運用フェーズの企業では、直前のフェーズよりも割合が減少している点である。これは、ISO27001,2が広く情報セキュリティのガイドラインとして使われているため、検討段階の初期で参照される割合が高いが、情報セキュリティを対象とした規格であり、実際にIoTシステムへ適用する場合、要件をIoTシステムに直接適用することが困難であるため割合が下がっていると推測できる。

２つ目は、検討段階初期では極めて割合の

図5　IoTシステムの検討、開発段階ごとに参照しているセキュリティガイドラインの割合



出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査」（2016年）

低い「自社内の独自のガイドライン」や「中央省庁・関連団体発行のガイドライン」は検討段階が進むにつれて急激に参照する割合が増加する点である。先にも述べた通りIoTは、社内ITシステムのようなコモディティ化された情報系システムと比較すると、個社ごとのビジネスに沿った多様な利用形態、システム構成が存在する。たとえば、ビル管理システムにIoTを活用した事例では、ビルのさまざまな場所に配置したセンサの情報をリ

アルタイムに解析し、空調、ゲートなどを制御することで省エネ・快適性や防犯・防災に役立てている。農業に活用した事例では、気温、湿度や土壌の状態などをセンサで計測しその情報を解析することで放水などを行う。

このように、ビル管理の事例と農業の事例では同じIoTという概念ではあるが、利用するセンサ、制御するデバイス、ネットワークなどの構成やソフトウエアがまちまちで利用場面も異なるため、それぞれに要求されるセキュリティ水準や要件も異なる。このため、IoTセキュリティという括りで一律のセキュリティ基準を適用することは極めて困難である。

このことから、IoT先行企業は、公開されている既存の中央官庁・関連団体が発行しているガイドラインを参考にしつつ、自社のビジネス種別や事業規模などを考慮した上で、独自にガイドラインを作成している場合が多い。このため、IoT製品をリリースしている企業・運用フェーズの企業では「自社内の独自のガイドライン」や「中央省庁・関連団体発行のガイドライン」の参照割合が高くなっていると考えられる。

現在、政府や業種団体によって業界ごとのIoTセキュリティに関するガイドラインの検討は行われているが、自社のIoTシステムへのローカライズは今後も必須となると考えられる。たとえば、製造業のスマート工場などのIoT活用事例では、自社工場のセキュリティを担保するために、情報系システムのガイドライン（ISO27001,2など）、IoT推進コンソーシアムの発行している「IoTセキュリティガイドライン」、OWASP、NISTなど海外団体が発行しているガイドライン、IEC62443-2-1など、制御システム向けのガイドラインを組み合わせたフレームワークを活用し、スマート工場の各要素（デバイス・端末、サーバ、ネットワーク、組織）のセキュリティ評価を行い、その上で、自社の工場に適したガイドラインの策定などを行っている。

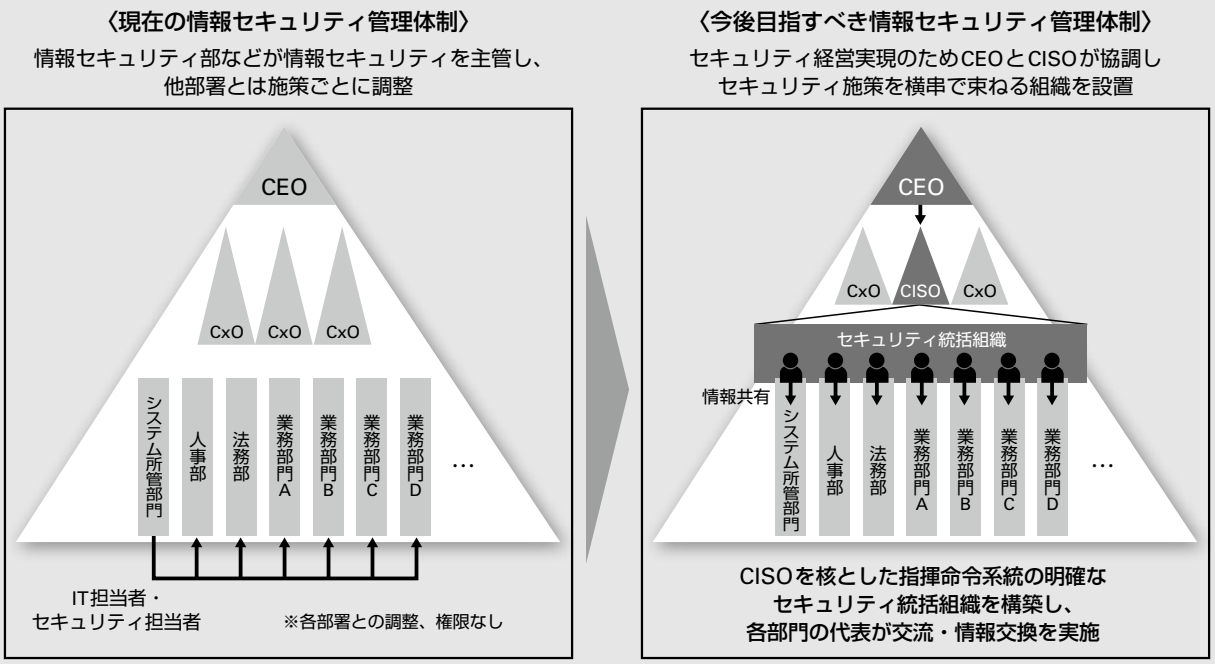
IoTガイドラインを先行して策定しているグローバル製造業では、このようなガイドラインの策定をIoTシステムを保有している生産管理部門とシステムを所管する部門が組織横断的に協調し合い、自社ガイドラインの策定やノウハウの共有を進めている。IoTにおいては、セキュリティ担当は本社、システムの保有主体は現場事業部となっている場合が多いので、IoTセキュリティを推進する組織横断的な新たな責任主体を配置することが望ましい。今後、IoTの活用を検討している企業は、先行事例を参考に組織横断的なIoTセキュリティ推進組織を作り、自社ビジネスに合ったセキュリティガイドラインを策定することがベストプラクティスになると考えられる。

V 総括と提言

1 セキュリティ前提の組織体制の整備

ここまで述べてきた通り、サイバー攻撃は年々巧妙化しており、特に2016年は新たな攻撃による被害が大幅に増えていることが本調査で分かった。さらに、これまでITが積極的に活用されてこなかった分野において、IoTという形でビジネスを高度化する機運も高まっており、情報セキュリティが適用されるべき範囲が増えていくことは確実である。

図6　今後目指すべき情報セキュリティ管理体制



このような背景から、必要とされる情報セキュリティ人材の数も年々増加し、求められる能力も高度化しているため、情報セキュリティ人材の不足感は高まっている。この課題を解決するためには、各企業によるセキュリティ組織体制の整備と、巧妙なサイバー攻撃などに対する継続したセキュリティ対策の推進が必要である。

多くの企業では、社内に組織横断で情報セキュリティを推進する役割が設置されておらず、組織横断的なセキュリティ施策の実施が難しいと考えられる。現在の情報セキュリティ推進の一般的な体制は図６の左にあるように、システムを所管する部門（情報システム部・情報セキュリティ部など）が、本社機構や業務部門と調整しつつ個別の情報セキュリティ施策ごとに推進することが一般的である。また、情報セキュリティを推進する上でシステムを所管する部門は、他の部門に対する情報セキュリティを推進するための権限が弱く、調整窓口が設置されていないことも多いため、個別施策ごとに調整に多くの労力、時間を要してしまう。

たとえば、人材の獲得においては、第Ⅱ章で述べた通り、日本企業は米国やシンガポールの企業に比べ金銭を用いた人材確保施策の割合が極めて低い。さらに、人員の配置転換などによる自社内での情報セキュリティ人材の確保も実施割合が低い。人材の獲得や教育は、通常、人事部門に裁量があるため、人事部門との調整の上実施する必要がある。しかし、現状ではセキュリティ人材獲得施策の推進主体が存在しない企業が多く、存在しても人事部門との交渉の必要性を認識していないケースが大半である。そのため、人事部門と連携した人材獲得以外の手段で人材不足を補

おうと考えるので、効率化やアウトソーシングの実施割合は高いが、人材の採用や強化については実施割合が低いという調査結果につながっている。

情報セキュリティを担保するためには、全社の経営戦略を理解した上で、自社のビジネス推進に必要十分なセキュリティ施策を過不足なく実施する必要があり、それに伴い、それぞれの施策に最適化した人材の確保が必要となっている。多くの企業は縦割り組織で部門間のコミュニケーションが希薄なため、セキュリティ人材確保のための調整が難しい。このような課題への1つの解として、図6の右のような、CISOを中心とした全社のセキュリティ施策を横串で推進するためのセキュリティ統括組織を設置する取り組みがある。本社機構や業務部門の各部署から情報セキュリティ担当者を選出し、統括組織の活動に参加してもらい、各部署との連携を推進する。このような統括組織を設置するためには、最初に会社の中心である経営のトップが情報セキュリティの重要性を認識する必要がある。

昨今では情報セキュリティ経営ガイドラインなどの経営層に向けたガイドラインも発行されており、経営層が情報セキュリティ意識を高める機運が高まっている。各社は自社の情報セキュリティ高度化のために、全社的なセキュリティ統括組織の設置を検討するべきである。

2 継続したセキュリティ対策の推進

第Ⅲ章で述べた通り、情報セキュリティの脅威は日々進化しており、特に2016年はサイバー攻撃が増加・巧妙化した年であった。各セキュリティベンダーはそれらの脅威に対して、対策ソリューションを提供し続けているが、守るべき範囲の増加や、脅威の進化のスピードが速いことから、新たにセキュリティ製品を導入し、脅威の巧妙化についていくことが難しくなってきている。企業としてどの資産やシステムを守るべきかを整理し、その上でどのような脅威に対してどう対応すべきかを明確にする必要がある。

そのためには、国内だけでなく海外を含めたセキュリティ脅威の最新情報や動向を収集し、自社対策へ反映することが大切である。情報収集の対象としては、たとえば、公共情報として企業の各種所轄官庁のセキュリティ情報やガイドライン、IPAやJPCERT/CCなどのセキュリティ専門組織の発信する情報などがある。業界におけるセキュリティの横断組織（ISACなど）があれば、その横断組織に所属してセキュリティ情報連携を共有・収集することも重要である。自社内にCSIRT（Computer Security Incident Response Team：コンピュータセキュリティにかかわるインシデントに対処するための組織の総称）を持つ場合は、日本シーサート協議会などCSIRTを運営する企業の情報共有組織に入り、各社の情報セキュリティ対応態勢を平時と有事の観点から収集することも有効である。また、セキュリティ専門ベンダーによっては、脅威動向などの情報提供をしているベンダーもあり、セキュリティ情報提供サービスを利用することも情報収集の選択肢の1つである。このように多様な情報収集方法が存在するため、企業の需要に応じて複数の方法を選択し、使い分けることが肝要である。

また、継続した脅威への対応としては、定

期的に企業の実状を把握するための点検を行い、点検結果から必要な対策を実施し、改善していくことが必要である。具体的には、業界や企業特性に応じたセキュリティチェック項目を策定し、その上で現状のセキュリティ対策を網羅的に整理する。さらに、チェック項目と現状の対策を突合し、収集した情報を考慮した上で、次に行うべき対策を可視化することが必要である。このような調査・現状評価・分析・可視化は一過性のものとせず、常に高度化・巧妙化する攻撃に対応していくために、定期的に実施することが重要である。さらに、グループ会社が複数存在する企業においては、単体での対応だけではなく、グループガバナンスを利かせ、全体でセキュリティの底上げを行うために、調査・現状評価・分析・可視化をグループ全体に広げて実施することを推奨する。

注

1 NRIセキュアテクノロジーズ「NRI Secure Insight 2017 企業における情報セキュリティ実態調査 グローバル編」2017年
2 「サイバー攻撃で、ドイツの製鋼所が甚大な被害を被っていた」 http://www.newsweekjapan.jp/tsuchiya/2015/09/post-2.php、2015
3 「Hackers Make the First-Ever Ransomware for Smart Thermostats」 https://motherboard.vice.com/en_us/article/internet-of-things-ransomware-smart-thermostat、2016
4 Blackhat2015内での研究発表、2015年

著者

金子洋平（かねこようへい）
NRIセキュアテクノロジーズ ストラテジーコンサルティング部
専門は情報セキュリティに関する調査・コンサルティング