JEITA

情産－18－技標－2

平成29年度情報セキュリティ調査報告書

－経営とセキュリティに関する調査－

平成３０年３月

一般社団法人 電子情報技術産業協会
情報セキュリティ調査専門委員会

はじめに

ビジネスの現場において、IT の利活用は企業の収益性向上に不可欠であり、それを脅かすサイバー攻撃は、企業にとって経営リスクとなっている。サイバー攻撃のリスクの対処には、セキュリティへの投資が必要となる。企業戦略として、IT に対する投資をどの程度行うか、その中で、事業継続性の確保やサイバー攻撃に対する防衛力の向上という企業価値増進にどう取り組むか、経営判断が求められる。

このような背景に、経済産業省、独立行政法人情報処理推進機構（以下、IPA とする）は「サイバーセキュリティ経営ガイドライン」を策定し、経営者が認識する必要がある「サイバーセキュリティの 3 原則」、CISO 等が着実に実施すべき「サイバーセキュリティ経営の重要 10 項目」を公表している。

こうした政府等の公表を受け、サイバーセキュリティ対策を進める上で経営層の関与が求められている。企業において経営とセキュリティの観点で現状を認識し課題を検討することは、企業の経営リスクマネジメントや事業戦略の策定に役立つと考えられる。

本年度の活動として情報セキュリティ調査専門委員会では、経営とセキュリティの観点から、企業におけるセキュリティ対策の推進方策及び事業展開の方向性について調査を行った。主に、企業におけるセキュリティ体制構築に関する取組みや、セキュリティ支援組織からの経営層や現場へのアプローチについて、企業視察と有識者ヒアリングにより事例を調査した。その結果を、JEITA 会員企業のビジネスや事業戦略の策定に役立てていただくことを目的として、調査報告書として取りまとめた。

本調査報告書の作成にあたり、視察及びヒアリングにご協力いただいた企業や有識者の方々、そして当専門委員会の関係の皆様に深く感謝の意を表すとともに、本報告書が関係の方々に活用され、今後のセキュリティ対策の躍進に寄与できれば幸いである。

2018 年 3 月

情報セキュリティ調査専門委員会
委員長　佐藤　淳

情報セキュリティ調査専門委員会名簿

（敬称略・順不同）

委員長	佐藤　淳	㈱リコー
副委員長	對馬　孝高	㈱日立製作所（2017年4月～7月）
〃	武本　敏	㈱日立製作所（2017年8月～9月）
〃	森安　隆	㈱日立製作所（2017年10月～2018年3月）
委員	福島　孝文	東芝テック㈱
〃	水島　九十九	日本電気㈱
〃	増田　佳弘	富士ゼロックス㈱
〃	白石　節男	富士通㈱
〃	池田　恵一	富士通㈱
オブザーバ	田中　清一	エム・アール・アイ リサーチアソシエイツ㈱
〃	村木　由利香	エム・アール・アイ リサーチアソシエイツ㈱
〃	牧野　夏葉	エム・アール・アイ リサーチアソシエイツ㈱
事務局	長岡　勉	(一社)電子情報技術産業協会
〃	内田　光則	(一社)電子情報技術産業協会

目 次

1. 現状認識

1.1 セキュリティ分野における経営リスクを生み出す要因

企業を取り巻くリスクは、多種多様かつ複雑多岐にわたっている。犯罪の被害、事故や災害、法制度の改定、訴訟の提起など、企業に損失を与える要因は数限りない。また、ICT 技術などの環境変化が進むことで、これまでとは異なる複合的なリスクの可能性も生じてくる。

技術革新や IoT の進展は経済活動や社会生活に大きな便益をもたらす。しかしながら、イノベーションの源としてそれらが普及することで、従来以上にセキュリティリスクが深刻化してくる。また、サイバー攻撃の手口が多様化・巧妙化しており、もはや防御だけではサイバー攻撃に対処しきれなくなっている。さらに、サイバーセキュリティリスクの脅威に対して、全ての攻撃を防御するのは困難な時代になってきている。

このような社会環境変化において、セキュリティ分野における経営リスクを生み出す要因を以下に概観する。

1.1.1 サイバーセキュリティリスクの認識不足

サイバーセキュリティにおいて、リスクが十分に認識されておらず対策が不十分な場合には、サイバー攻撃により企業秘密や個人情報が漏えいするリスクが高まる。また、サイバー攻撃によりインフラ等のサービスが停止すると社会に大きな損害を与え、社会問題に発展することもある。

セキュリティ対策を「コスト」と考えるのではなく、事業活動に必須なものと位置付けて「投資」と考えるべきある。サイバーセキュリティ対策は、何も起きていない時期に行う必要があるものの後手に回る傾向がある。

セキュリティ投資をどの程度行うかは、経営課題であり経営者の役割となる。しかしながら日本では、サイバーセキュリティ対策において、経営者が十分リーダーシップを発揮して対策を進めているとは言えない状況である。サイバーセキュリティ対策は企業経営にとって不可欠な課題であり、経営者がリーダーシップを取って対応策を推進していくことが求められる。

さらに、経営者がセキュリティ対応を社内外へ提示しない場合、セキュリティ対策の実行において会社方針と一貫性が取れなくなる。社内外へ提示することで、ステークホルダーの信頼性を高めブランド価値向上につながるのである。逆に提示されない場合には、サイバーセキュリティへの取組みがステークホルダーに伝わらず、企業における信頼性を高めることが難しくなるのである。

1.1.2 サイバーセキュリティ対策のためのリソース不足

サイバーセキュリティ対応を図るためには、質と量ともに従来を遥かに超える取組みが必要になっている。サイバーセキュリティの対策においては、積極的にリソースを充当することが求められ、それを支える人材の育成と確保が急務となっている。

しかしながら、サイバー空間を取り巻くセキュリティリスクが急激に進展し深刻化してお

り、更には人材育成が長期的な課題のため、未だ十分な成果が出ていない状況である。人材育成は、産業活性化や研究開発及びリテラシー向上とともに、サイバー空間の創造力や知識力の強化を目指す方策の一つと考えられている。セキュリティ人材の不足解消に向けた積極的取組みとして、サイバーセキュリティを担当する技術者のスキルアップが最重要となる。突出した人材の発掘や育成を通して、グローバル水準で活躍できる人材を増やすことが求められている。また、適切な処遇の維持や改善が図れない場合、有能なサイバーセキュリティ人材を自社に留めておくことが困難になる。

さらに、サイバーセキュリティ対策において適切な予算確保が十分でない場合には、企業において対策実施やリソース確保が困難となるほか、外部ベンダへの関連業務を委託することも困難になるリスクが生じる。

1.1.3 サイバーセキュリティリスク対応における PDCA 実施が不十分

各企業の状況に応じて、適切なセキュリティ対応を実施しなければ日常の業務遂行に支障をきたす可能性が残る。また、受容できないリスクが残る場合には、想定外の損失を被る可能性が高まる。

セキュリティ関連の環境変化に対応し、新たに発生した脅威に対応することが極めて重要となる。適切なセキュリティ対応を実施するためにも、PDCA を実施する体制を構築できないと実行計画が確実に推進できない。新たな脅威への対応が可能かといった視点も踏まえて、サイバーセキュリティ対策を定期的に見直す必要がある。

さらに、サイバーセキュリティに応じた適切な対策が実行されないと、サイバー攻撃が発生し被害が拡大するリスクが生じる。適切な対策と運用が不十分な場合には、サイバー攻撃の状況を正確に把握できず、組織内の重要情報が漏えいするなどの致命的な被害に発展する可能性が残る。

1.1.4 インシデント発生時の緊急体制整備が不十分

企業秘密や個人情報の漏えいが発生した際には、従来以上に実ビジネスに与えるインパクトが大きくなっている。特にサイバー攻撃で情報が漏えいした場合、企業が被る被害は計り知れず大きなインパクトを受けることになる。重要な顧客情報や大規模な情報漏えいが発生すれば、顧客からの信用や企業が育てたブランドは大きく毀損する。法令上の罰則を受ける場合もあり、損害賠償などで膨大な金銭的損失を招くもリスクも高まっている。

また、緊急時の対応体制が整備されていないと、組織内外の関係者間のコミュニケーションが円滑に行われないことが懸念される。迅速に対処することができず情報開示が遅延すると、顧客や取引先等にも被害が及ぶリスクが増大する。そして、損害賠償請求など責任を問われる可能性につながる。所管官庁等への報告が義務付けられている場合には、報告が遅延すると更なる罰則等を受けるリスクが高まる。

さらに、日常的にインシデント報告の訓練を実施していないと、不測の事態が起こった際に担当者が適切に必要な行動をとることができない。重要なサービスが適切な時間内に復旧できないと、企業経営に致命的な影響を与える可能性が増大するのである。

1.1.5 ビジネスパートナーを含めたサプライチェーン全体の対策が不十分

ビジネスプロセスにおいては、自社だけではなくサプライチェーン上に存在するセキュリティリスクにも対処することが必要になる。自社だけでなくグループ会社や、サプライチェーンのビジネスパートナーや業務委託先を含め、セキュリティ対策を実施することが非常に重要となっている。

グループ会社やサプライチェーンのビジネスパートナーにおいて、適切なサイバーセキュリティ対策が行われていないと、これらの企業が踏み台にされ攻撃されるリスクが生じる。その結果、他社への二次被害を誘発し加害者となる可能性が高まる。また、緊急時の原因究明においては、これらの企業からの協力を得られないことでインシデント対応が遅延することにつながる。

さらに業務委託においては、自社で対応する内容と委託先が実施する内容の境界線が不明確となり対策漏れが生じるリスクがある。委託元としては、サプライチェーン上の全企業を管理することは困難である。そのため、再委託先以降へのセキュリティ対策は、直接取引のある委託先に大きく依存せざるを得ないこととなるのである。

1.1.6 情報共有活動による攻撃情報の利活用が不十分

サイバー攻撃手法を解析した情報など、セキュリティ関連情報を社内外で共有することにより、同様の被害を未然に防止できる可能性が高まる。しかし、情報共有ができていない場合には、常に新たな攻撃に独自に対応することとなり企業における対応コストを低減することが困難になる。

2000 年代までは、サイバー攻撃はほとんどが個人の愉快犯によるものであった。しかし、徐々にウイルスが高度化し、ソフトウェアの機能の盲点や脆弱性を突いて自動的に感染を拡大するウイルスが登場した。さらに攻撃者は効率を求めて企業を標的とするようになり、ウイルスメールをばらまく大量感染型が主流になった。その後、サイバー攻撃を請け負うようなグループが登場し、ボットネットワークを使った「DDoS 攻撃」を仕掛けて事業運営を妨害するようになった。そして、サイバー犯罪者が組織化するとともにブラックマーケットも形成され、ウイルスをはじめ機密情報や個人情報などが売買されるようになった。

こうした中でランサムウェアなど悪質で強力なウイルスが登場するようになり、関連情報の早期入手が有効な手立てとなる。情報共有活動へ参加することにより、関連情報を活用して同様の被害を未然に防止する必要性が高まっているのである。

1.1.7 スマートシティ等における近未来の脅威

スマートシティでは、エネルギーや生活インフラの管理に IoT などを活用し、その導入により生活レベルの向上や都市の運用及びサービスの効率化などが期待されている。しかしながら、サイバーセキュリティのリスクも増大しており対策が急がれている。

スマートグリッドでは、電力網において IoT デバイスであるスマートメーターにより、設置場所のエネルギー消費が記録され、供給元である電力会社にデータが自動的に送られている。しかし、関連する装置などにセキュリティリスクがあると、様々な形で攻撃者に悪用される可能性が高まる。スマートメーターの通信が妨害されると、電力需要に対する供給が不能になるリスクがある。また、DDoS 攻撃を仕掛けられて、大規模都市で電力システムが停

止し、重要なサービスに影響を及ぼすことも考えられる。

交通業界では、日常的に起こる交通システム管理の問題解決が求められている。高度道路交通システムでは、信号機を自動的に認識し、交差点における遅延や歩行者の待ち時間を削減することが期待されている。しかし、これらの装置などにセキュリティリスクがあると、システムが復旧するまで利用者に多大な影響を与えることになる。また、スマート信号機をハッキングされた場合、コネクテッドカーが攻撃の影響を受けるリスクがある。また、コネクテッドカーの機能を乗っ取ったり、コネクテッドカーをランサムウェアで攻撃したり、誤情報をドライバーに送信する可能性が高まるのである。

通信インフラにおいては、信頼できる無線通信インフラがなければスマートシティなどは意図した機能を実行できなくなる。DDoS 攻撃によりネットワークやスマートデバイス等が利用不能になるリスクを生じる。また、通信を傍受することで、企業秘密や認証情報などを盗み出す可能性もあり、更なる個人情報漏えいやプライバシーを侵害する問題にも発展する可能性が増大する。

1.1.8 まとめ

IoT や AI の市場は、世界規模で大きく拡大することが見込まれている。企業のシステムがネットワークでつながり、ネットワーク連携が急速に進んでいる。そのため、ネット家電や制御システムなどあらゆるネット機器において、サイバー攻撃への対応が必須となっている。

しかしながら、その対応は企業にとっては容易なことではない。サイバー攻撃を受けても社内で気付くのは困難な状況になっており、多くの企業は外部から指摘されて初めてインシデントに気付くことも少なくない。企業にとっては、様々なセキュリティリスクに対処することが従来以上に重要となってきている。直面している環境が複雑かつ急激に変化することから、経営課題と捉え経営者のリーダーシップにより対応することが求められているのである。

1.2 セキュリティへの経営層の関与の必要性及びセキュリティ推進体制

1.2.1 サイバーセキュリティ経営ガイドライン

経済産業省では IPA とともに、大企業及び中小企業のうち、IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下でサイバーセキュリティ対策を推進するため、「サイバーセキュリティ経営ガイドライン」を 2015 年 12 月 28 日に策定、公表した。その後、2017 年 11 月 16 日に「サイバーセキュリティ経営ガイドライン Ver2.0」が公表された。

本項では、サイバーセキュリティ経営ガイドラインの概要を紹介する。

(1) サイバーセキュリティは経営問題

IT の利活用は企業の収益性向上に不可欠なものとなっている一方、こうしたビジネスを脅かすサイバー攻撃は避けられないリスクとなっている。その防衛策には、セキュリティへの投資が必要となる。企業戦略として、事業継続性の確保やサイバー攻撃に対する防衛力の向上という企業価値のためにどの程度セキュリティ投資をすべきか、経営判断が求められる。

(2) 経営者が認識すべき 3 原則

サイバーセキュリティ経営ガイドラインでは、セキュリティ対策を進めるにあたって認識すべき 3 原則をまとめている。3 原則の内容は以下のとおり。

表 1.2-1 サイバーセキュリティ経営の 3 原則

サイバーセキュリティ経営の３原則
① 経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
② 自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要
③ 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

出所）経済産業省、IPA「サイバーセキュリティ経営ガイドライン　Ver 2.0」より作成

(3) サイバーセキュリティ経営の重要 10 項目

また、ガイドラインでは、経営者がサイバーセキュリティ対策を実施する責任者（セキュリティ関連組織・役職含む。以下、CISO 等とする。）に対して指示すべき重要 10 項目についても、整理している。重要 10 項目の内容は以下のとおりである。

表 1.2-2 サイバーセキュリティ経営の重要 10 項目

サイバーセキュリティ経営の重要１０項目		
経営者がリーダシップをとったセキュリティ対策の推進	1. サイバーセキュリティリスクの管理体制構築	①サイバーセキュリティリスクの認識、組織全体での対応方針の策定 ②サイバーセキュリティリスク管理体制の構築 ③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
	2. サイバーセキュリティリスクの特定と対策の実装	④サイバーセキュリティリスクの把握とリスク対応に関する計画の策定 ⑤サイバーセキュリティリスクに対応するための仕組みの構築 ⑥サイバーセキュリティ対策におけるPDCAサイクルの実施
	3. インシデント発生に備えた体制構築	⑦インシデント発生時の緊急対応体制の整備 ⑧インシデントによる被害に備えた復旧体制の整備
4. サプライチェーンセキュリティ対策の推進		⑨ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
5. ステークホルダーを含めた関係者とのコミュニケーションの推進		⑩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及び提供

出所）経済産業省、IPA「サイバーセキュリティ経営ガイドライン　Ver 2.0」より作成

1.2.2 セキュリティ推進体制

サイバーセキュリティ経営ガイドラインに記載されている対策を実現するためには、経営者をトップとした体制の整備が不可欠となる。

特定非営利活動法人日本ネットワークセキュリティ協会（以下、JNSA とする）で公開しているセキュリティ推進体制例を図 1.2-1 に示す。また、それぞれのプレイヤーの役割を表 1.2-3 に示す。

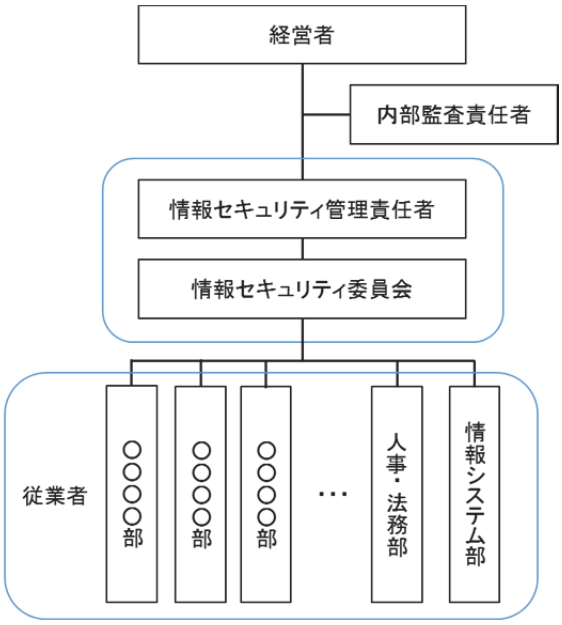

図 1.2-1 一般的な情報セキュリティ組織体制

出所）JNSA「特定非営利活動法人日本ネットワークセキュリティ協会 HP　「情報セキュリティ体制」をたずねられたら」　http://www.jnsa.org/ikusei/info_security/01_01.html より作成

表 1.2-3 体制のプレイヤーと役割

プレイヤー	役割
経営者	・情報セキュリティ基本方針を策定する ・CISOからの報告を踏まえ、改善指示を行う ・セキュリティ対策を検討する際、担当者任せにせず、積極的に関わる
情報セキュリティ管理責任者（CISO）	・検討した対策を実施する ・社内の指導を行う ・事故・緊急時の対応を指示する ・必要に応じて、社員の招集や経営者へ報告する
内部監査責任者	・方針通り対策が運用されているか、確認する ・客観的な視点で点検する
情報セキュリティ委員会	・各部門の課題を提出する ・部門内の指導・管理を行う ・部門の代表者により構成し、相互理解を得る
従業者	・事故を起こさないように業務を遂行する ・組織が定めたルールを遵守する

出所）JNSA「特定非営利活動法人日本ネットワークセキュリティ協会 HP「情報セキュリティ体制」をたずねられたら」 http://www.jnsa.org/ikusei/info_security/01_01.html より作成

1.2.3 セキュリティ推進体制構築事例

本項では、これらの動きを受け、経営層が情報セキュリティの推進に関与できる体制を構築している企業の事例を紹介する。

(1) 富士ゼロックス株式会社

富士ゼロックスでは、社長をトップとする情報セキュリティ推進体制を構築している。情報セキュリティ担当役員配下に、全社の情報セキュリティを統括・推進する情報セキュリティセンターを設置し、その情報セキュリティセンターとサイバーセキュリティ対応チーム（サイバー攻撃担当）、情報通信システム部（IT ガバナンス担当）、富士ゼロックス情報システム（FXIS IT インフラ構築・運用担当）が連携し、全社の情報セキュリティを推進している。

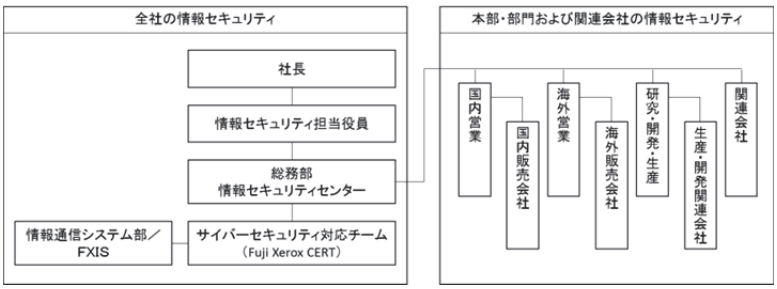

図 1.2-2 富士ゼロックスの情報セキュリティ推進体制

出所）富士ゼロックス株式会社「富士ゼロックス 情報セキュリティ報告書 第 10 版」
https://www.fujixerox.co.jp/company/public/i_security/doc/i_security2016.pdf より作成

(2) 株式会社日立製作所

日立製作所は、執行役社長が任命する情報セキュリティ統括責任者と情報セキュリティ監査責任者を中心に情報セキュリティを推進する体制を構築している。情報セキュリティ統括責任者は、情報セキュリティ委員会を組織する。情報セキュリティ委員会では、情報セキュリティに関する各種方針、教育計画、各種施策を決定し、その決定事項は、全事業所実務者が出席する情報セキュリティ推進会議を通じて、各事業所に周知される。

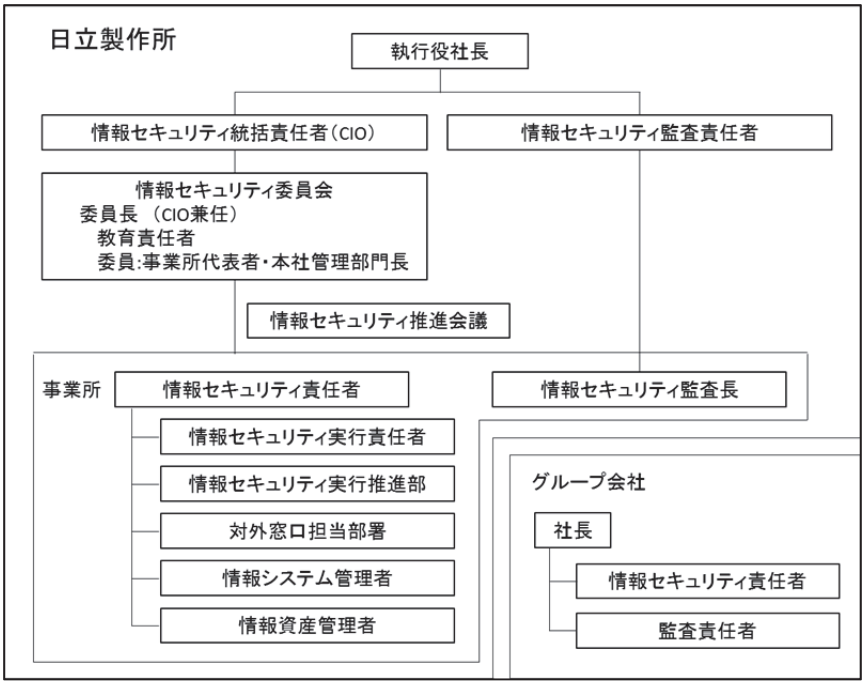

図 1.2-3 日立製作所の情報セキュリティ推進体制

出所）株式会社 日立製作所「情報セキュリティ報告書 2017 日立グループ」
http://www.hitachi.co.jp/csr/download/pdf/securityreport.pdf より作成

(3) 富士通株式会社

富士通は、取締役会直属の組織であるリスク・コンプライアンス委員会の下に最高情報セキュリティ責任者（CISO）を設置している。最高情報セキュリティ責任者は、情報セキュリティ管理に専任・特化した責任者である。また、グローバルな情報セキュリティマネジメント体制を強化することを目的として、最高情報セキュリティ責任者傘下に世界各リージョンの最高情報責任者（リージョナル CISO）を設置し、グローバルな情報セキュリティガバナンスの強化を図っている。

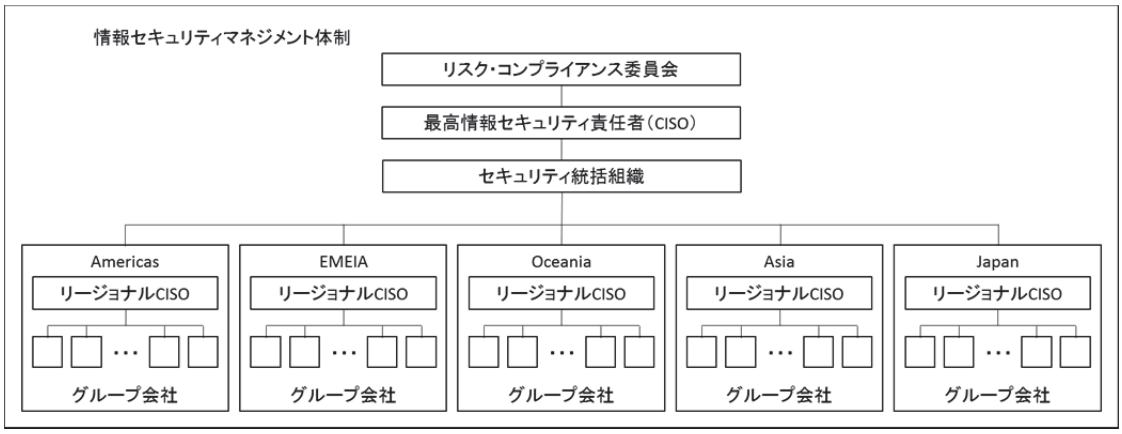

図 1.2-4 富士通の情報セキュリティ推進体制

出所）富士通株式会社「富士通グループ情報セキュリティ報告書 2017」
http://www.fujitsu.com/jp/documents/about/resources/reports/securityreport/security-2017.pdf より作成

1.3 CISO 等の役割

現在、様々なビジネスの現場においてITが活用されており、そこでは個人情報、プライバシー情報、企業情報などの多くの機微情報が利用されている。これらを狙うサイバー攻撃は増加してきており経営者としては対応が必須になってきている。サイバーセキュリティ経営ガイドラインの公表により、CISO等の設置が求められるようになってきた。しかし、CISO等の役割などは企業や日米欧でそれぞれ異なっている。

1.3.1 日本企業の実態

日本のCISO等の設置状況を業種毎にみると、金融及び情報サービス・通信プロバイダにおいて設置率が高くなっている[1]。これは情報やデータそのものが重要な価値を持ち、企業として利益を得る事業を展開している企業がCISO等を設置している状況と言える。一方、製造業のように事業に付随するが情報やデータから利益を生み出さない事業形態ではCISO等の設置率が低くなっている。

このようなことから日本のCISO等が管理責任を負う範囲は「社内情報システム」が中心となり84.4%と高い割合となっている。次いで「事業部門が保有する情報システム・制御システム」の62.2%、「自社製品・サービスのセキュリティ品質の確保」に至っては29.8%と低くなっている[2]。

情報やデータが直接的な利益を生む企業は情報漏えいや改ざんを防ぎ、事業を安定して運用するために可用性を重要視する。このため、セキュリティインシデント等への迅速な対応が必要となっている。迅速な対応の先頭に立って指揮するのがCISO等であり、サイバーセキュリティ体制が早い時期から構築されてきた。

製造業は情報やデータが直接的な利益を生まないことと、製造現場で培ってきた現場力によって問題が現場で解決される土壌などがあったため、これまでCISO等の指示による特別なサイバーセキュリティ体制は構築されてこなかった。しかし、昨今では製造の現場でもICT/IoTを活用した製造・制御システムが増加してきており、セキュリティインシデントが製造現場に与える影響が増えており、全社的な指示をだせるCISO等の関与が必要となってきている。

また、ビジネスシステムや製造・制御システムなどで利用する情報機器を選定する場合には、セキュリティ機能とともに、セキュリティインシデントが発生した場合にも迅速な対応が実施でき、セキュリティインシデントの被害や影響が少ない機器を選ぶことが必要である。

このように、製造現場でのセキュリティ脅威・リスクを分析して対応方針も定めるのもCISO等の役割である。

1.3.2 日米での比較

CISO等が有する権限・役割として、2016年は、日本、米国、欧州ともに「情報セキュリティの方針、戦略の立案・計画」が最も高くなっている。米国では「情報セキュリティ対

[1] 警察庁生活安全局情報技術犯罪対策課：「不正アクセス行為対策等の実態調査　調査報告書」、平成28年11月、https://www.npa.go.jp/cyber/research/h28/h28countermeasures.pdf

[2] IPA：「企業のCISOやCSIRTに関する実態調査2017―調査報告書―」、平成29年4月13日、https://www.ipa.go.jp/files/000058850.pdf

策実施組織の管理・監督」も高い割合となっていた。さらに 2017 年になると「セキュリティ技術分析・評価」も役割に加えられている[3]。これは、サイバーセキュリティ攻撃が高度化しており従来の対策方法が適応し難くなってきたことにより、対策立案の前に分析をしなければならないからである。このように CISO 等の役割としては、セキュリティ分析と対策立案と実行管理と広い範囲の司令塔となることである。

日本の企業の多くで CISO 等の職務範囲は「社内情報システム」が 84.4%と高い割合となっており、次いで「事業部門が保有する情報システム・制御システム」の 62.2%、「自社製品・サービスのセキュリティ品質の確保」に至っては 29.8%と低くなっている[4]ことは前述のとおりである。

これらを日米欧で比較すると、各々で何についてサイバーセキュリティを重要視しているのかは明確な差がある。日本では CISO 等の職務範囲として「社内情報システム」が中心になっているが、米国、欧州では「自社部門が保有する情報システム・制御システム」と「自社製品・サービスのセキュリティ品質の確保」が日本より割合が高い。特に、欧州では「自社製品・サービスのセキュリティ品質の確保」が日本と米国よりも高い割合となっている。「自社製品・サービスのセキュリティ品質の確保」で判るとおり、欧米ではセキュリティは製品の品質として捉えられていることがわかる[5]。

ICT/IoT 機器が製造ラインやオフィスシーンなど様々な場所で利用されることを考えると、「自社部門が保有する情報システム・制御システム」のサイバーセキュリティ対策として、セキュリティを考慮されセキュリティ品質の高い ICT/IoT 機器を導入する必要がある。また、ICT/IoT ベンダ側の立場としては、セキュリティ品質が確保された製品やサービスを提供していかなければならない。セキュリティ要件を満たさないベンダ／事業者、製品、サービスはグローバルサプライチェーンからはじき出される恐れがある。このことを含め、自社の事業に対して何がリスクとなるのかを認識した上で CISO 等の職務範囲を定めることが望ましい。

このようにサイバーセキュリティは経営に直結しているが、CISO 等の組織内での位置付けは、米国では「経営層」が 46.8%、欧米では「経営層直下」が 43.4%である一方、日本では「情報システム部門のトップ（非経営層）」が 38.7%と低く[6]、更なる経営層の関与が必要となっている。これらを改善するために「サイバーセキュリティ経営ガイドライン」が IPA により公表されたが、情報セキュリティ対策を実施する際に「サイバーセキュリティ経営ガイドライン」を参照している企業は、2 割以下と少ない[7]。

1.3.3 有能な人材の海外流出の可能性

サイバーセキュリティはビジネスリスクであり、それを理解して経営トップを支える人材

[3] IPA：「企業の CISO や CSIRT に関する実態調査 2017―調査報告書―」、平成 29 年 4 月 13 日、https://www.ipa.go.jp/files/000058850.pdf

[4] 同上

[5] 同上

[6] 同上

[7] 経済産業省：「平成 28 年度我が国におけるデータ駆動型社会に係る基盤整備（情報処理実態調査の分析及び調査設計等事業）調査報告書」、平成 29 年 3 月、http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H28_report.pdf

の育成が鍵となる。特に求められる人材として、ビジネスや技術を理解した上で、サイバーセキュリティのリスクを把握し、経営トップともコミュニケーションがとれるような人材が重要である。そしてこのような人材が CISO 等に必要である。

CISO 等がどんな仕事をする人で、求められるスキルやキャリアパスがどんなものかということは、まだ一般に広く理解されているとは言い難い。一方で、企業に対するサイバー攻撃が増え続ける中、求人ニーズは日増しに高まっている。世界的なサイバーセキュリティの人材不足により米国では高い報酬で求人されている。CISO 等をキャリアパスの頂点とできるような、企業における CISO 等の位置付け、地位の再定義が行われないのであれば、情報セキュリティに関する有能な人材は海外に流出してしまう恐れがある。

欧米では、CISO 等のキャリアパスに必要な能力として、セキュリティポリシーやシステムの設計/運用から、経営層/社員への伝達や教育まで、情報セキュリティに関係する多岐に亘る分野のマネジメント、そしてビジネスの知識が挙げられている。また、情報セキュリティに関するルールが異なる業界の場合は、業界の知識や資格が必要となる。

このようなことから、欧米における CISO 等のキャリアパスには、情報システム分野の学位及び職務履歴が必須とされ、さらに、CISO 等は全社における横断的な情報セキュリティの統括のために、社内外に対する調整能力（コミュニケーション能力等）や組織の統率力が必要になる。このように、理想的な CISO には多くの能力が必要となる。特に、情報セキュリティは「利益を生まないコスト」と捉えられる傾向が強く、そのような中で情報セキュリティ管理を組織内で推進するためのコミュニケーション能力や内部調整力が必要となっている。

また、CISO 等のキャリアパスは重要となっており、人材育成も必要である。日本では、情報セキュリティ大学院大学が 2007 年に情報セキュリティ管理者（CISO）コースを開講して、経営層と実務層の橋渡しとなる人材の育成を実施している。また、IPA 産業サイバーセキュリティセンターでは、将来、企業などの経営層と現場担当者を繋ぐ中核を担う人材を対象とした「中核人材育成プログラム」を開講して人材育成を行っている。

人材育成においては、情報セキュリティ分野の幅広い技術的な知識・設計技術、ビジネス戦略を踏まえた各種計画の策定、情報セキュリティに係る体制の構築、法的視点、組織全体における IT の教育プログラムの設計に関する知識等を学べるような、幅広い項目からなる教育カリキュラムの設定が必要である。また、経営者クラス向けの教育としては、ビジネスにおける情報セキュリティの必要性を再確認させることを目的としたロールプレイングやケーススタディ等、より実践的な内容を学べるような教育プログラムが考えられる。

これらの教育プログラムにより、知識と実務が身に付くとともに、情報セキュリティの必要性を再確認させることができる。そして、CISO 等の役割や地位の向上に繋がり、情報セキュリティに必要な有能な人材の海外流出を防ぐことができる。

2. 課題と提言

本章では、第 1 章で述べた現状分析に基づき、セキュリティ人材、及び経営層と現場における体制とコミュニケーションに関する課題と提言について述べる。

2.1 セキュリティ人材の育成と確保

本項目では、CISO 等の育成に向けた課題と提言として、CISO に必要とされるスキルセットとそれらスキルを形成するための教育プログラム、及び、CISO へのキャリアパスを描けるようにするための人材を確保するための施策について述べる。

2.1.1 CISO に必要とされるスキルセット

CISO を育成する上で、CISO に必要とされるスキルや経験を明確に定義することができないという課題がある。

JNSA が作成した「セキュリティ知識分野（SecBoK）人材スキルマップ 2017 年版」[8]では、情報セキュリティに関わる 16 種類の人材に必要とされる前提スキルと必須スキルがまとめられている。ここでは、CISO に必要とされる前提スキルとして、コミュニケーションスキル、コンプライアンスや組織ガバナンスのスキル、必須スキルとして、ネットワークやセキュリティに関する技術的な知識が挙げられている。

また、IPA が実施したアンケート調査「企業の CISO や CSIRT に関する実態調査 2017」[9]では、CISO 等に必要とされるスキル・経験として「コミュニケーションスキル（経営層や現場、ステークホルダー等）」や「ICT スキル（セキュリティ技術や ICT に関する知識等）」、「リーダーシップ（プロジェクトマネジメントスキル）」等の回答割合が高いことが示されている。

[8] JNSA：「セキュリティ知識分野（SecBoK）人材スキルマップ 2017 年版」、平成 29 年 8 月 21 日、http://www.jnsa.org/result/2017/skillmap/

[9] IPA：「企業の CISO や CSIRT に関する 実態調査 2017」、平成 29 年 4 月 13 日、https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html

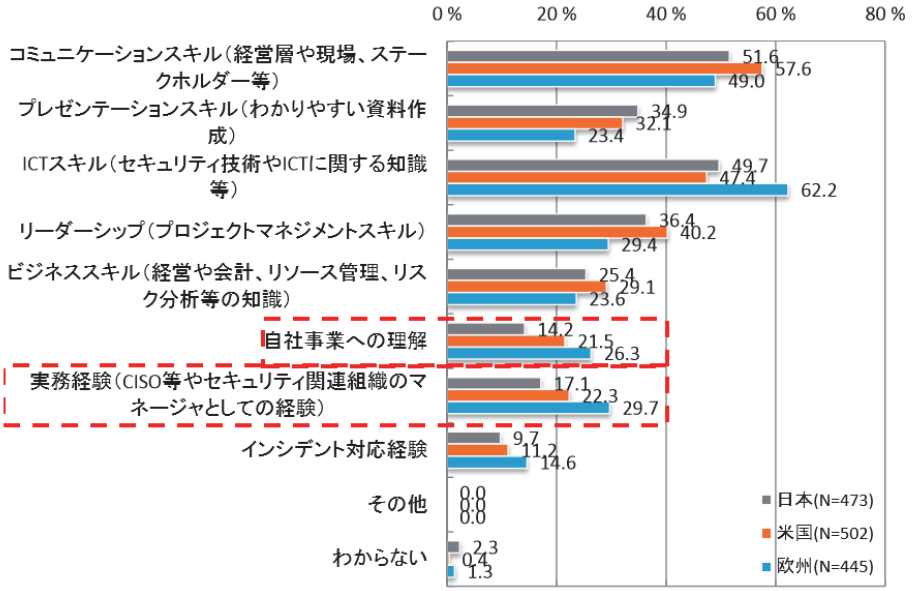

図 2.1-1　CISO 等に求めるスキル・経験

出所）IPA「企業の CISO や CSIRT に関する 実態調査 2017」，
https://www.ipa.go.jp/files/000058850.pdf より取得

さらに、海外における CISO に必要とされるスキルセットについては、NIST（National Institute of Standards and Technology）の SP800-39 Managing Information Security Risk Organization, Mission, and Information System View で触れられている。ここでは、CISO の役割は、セキュリティに関する責任を負い、CIO と関連各所との橋渡し役を担うことであり、セキュリティプログラムを管理するための専門的な知識と、リーダーシップが必要であることが記載されている。

またさらに、CISO に必要とされるスキルセットに関する研究として、Kansas 大学と IBM による「Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers」[10]がある。ここでは、CISO に必要とされる重要スキルとして、以下に示すような 10 項目が挙げられている。

- コミュニケーションとプレゼンテーションスキル
- ポリシー策定とアドミニストレーション
- 政治的手腕
- 州政府に関する知識
- コラボレーションとコンフリクト管理
- 計画と戦略的管理スキル
- 管理監督者としての手腕
- インシデント管理
- 法律や標準に準拠する知識
- リスクアセスメントとリスク管理

[10] University of Kansas, IBM：「Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers」、https://www.a51.nl/storage/pdf/CybersecurityManagementintheStatesIBMKansasUreportMay2010.pdf

上記の国内外の調査にみられるように、CISO に求められるスキルセットは、非常に広範に亘る。しかしながら、これらのスキルセットを全て満たす CISO を育成することは難しいと考えられる。特に、セキュリティベンダや IT ベンダではない国内のユーザ企業の場合、専任の CISO を設置することは稀であり、多くの場合、リスクマネジメント領域を管掌する総務系部門の役員や社内 IT 基盤の運用を管掌する情報システム系部門の役員が、管掌領域の一部として担う場合がほとんどである。このため、セキュリティ以外の業務比率が高い役員に、セキュリティに特化した専門知識やスキルの向上を求めていくことは非常に難しいと考えられる。

このような現状を踏まえ、多くの国内企業においては、CISO を補佐する役割を担う部門が、上述の CISO に必要とされるスキルセットを満たせるように支援することが重要になると考えられる。

2.1.2 CISO 育成のための教育プログラム

前章で述べたような、CISO に必要とされるスキルや経験が明確にできたとしても、それらスキルを育成するためのトレーニングをどのようにして行うかという課題がある。

現在、国内の CISO の育成を目的とした教育プログラムとして、情報セキュリティ大学院大学の CISO コース、IPA 産業サイバーセキュリティセンターが主催する短期プログラム（2 日間）などがある。また、海外では、カーネギーメロン大学の大学院 Heinz College の教育プログラム（6 か月）や、CISO に必要とされる知識（以下に示す 5 つの知識ドメインで構成される）を備えたことを認定する資格 CCISO（Certified Chief Information Security Officer）を取得のためのトレーニングコースなどがある。

Domain 1 – Governance
Domain 2 – Security Risk Management, Controls, and Audit Management
Domain 3 – Security Program Management & Operations
Domain 4 – Information Security Core Concepts
Domain 5 – Strategic Planning, Finance, & Vendor Management

また、上記のように体系的な知識の習得を目的とした教育プログラムの受講には受講時間を要するため、実務の中で CISO のスキルを育成していく方法を実践している例もある。例えば、CISO への定例報告の際に、同業他社でのインシデント事例について解説することや、経営者にインシデント対応訓練に参加してもらうなどして、スキル向上を図っている実施事例もある。

2.1.3 CISO へのキャリアパス

前章までで述べたようなスキルを備えたセキュリティ人材を効果的に育成し、CISO や CISO を補佐する人材を確保するためには、セキュリティに従事する担当者がキャリアアップしていくためのパスを描けるようにすることが課題となる。

IPA が 2012 年に発行した「情報セキュリティ人材の育成に関する基礎調査」では、情報セキュリティ人材のキャリアパスについての調査結果が示されている。ここでは、以下のような情報セキュリティに関わる人材の 6 つのキャリアパスモデルが事例研究に基づいてま

とめられており、CISO（図 2.1-2 左上）へのステップアップのパスが事例データに基づいて示されている。

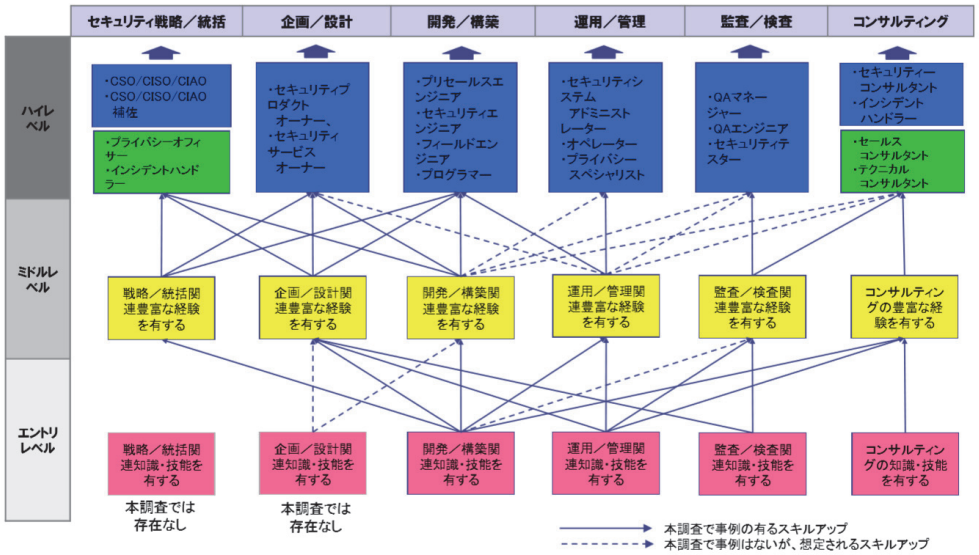

図 2.1-2　情報セキュリティ関連人材のキャリアアップモデル

出所）IPA「情報セキュリティ人材の育成に関する基礎調査 2012」
https://www.ipa.go.jp/security/fy23/reports/jinzai/index.html より取得

また、2016 年に経済産業省がまとめた「情報セキュリティ人材の育成・確保について」では、企業におけるセキュリティ人材の全体像として、ベンダ企業とユーザ企業という区別でセキュリティ人材のピラミッド構造が示され、ユーザ企業の最上位に CISO が位置付けられている（図 2.1-3）。

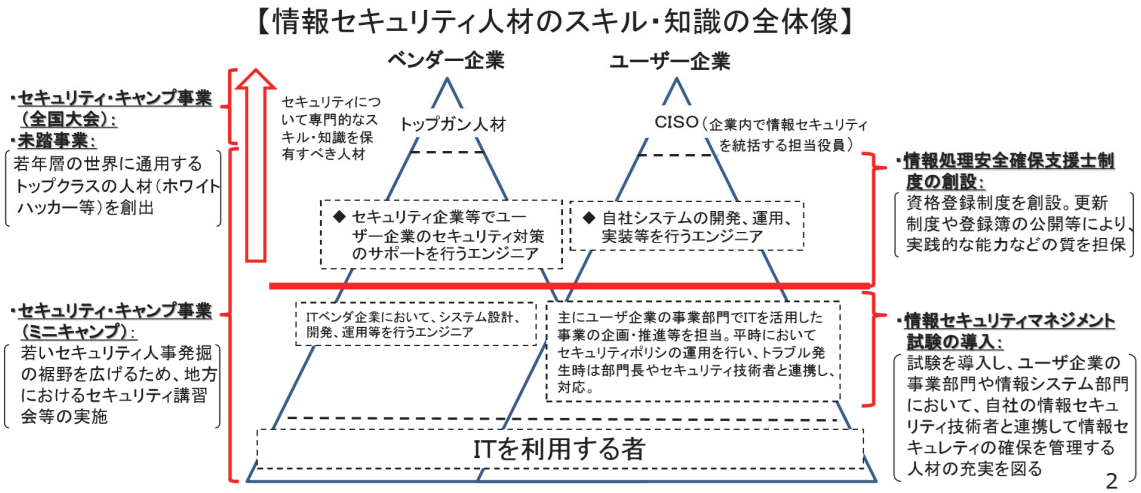

図 2.1-3　情報セキュリティ人材のスキル・知識の全体像

出所）経済産業省「情報セキュリティ人材の育成・確保について」，
https://www.nisc.go.jp/conference/cs/jinzai/dai01/pdf/01shiryou0503.pdf より取得

ここでのベンダ企業は、ユーザ企業のサポートをする立場として位置付けられているが、この役割を、CISO を支援する専門職のキャリアパスとして捉え、将来、専任 CISO が必要になった場合にセキュリティ専門職として培ったスキルや経験に基づいて社内から任用できるようにすることが望ましいと考えられる。

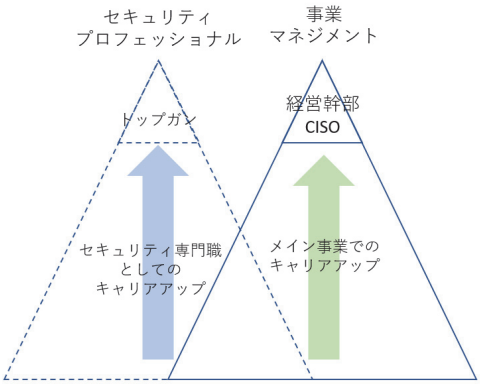

図 2.1-4　ユーザ企業に望まれるキャリアパス

また、国内の先進的な企業では、社内のセキュリティ人材を発掘・育成するための、セキュリティに特化した独自の社内認定制度やキャリア形成プログラムを運用している例がある。

富士通では、2019 年度末までに社内 1 万人のセキュリティマイスターを養成することを目標にした「セキュリティマイスター認定制度」を運用しており、3 領域（フィールド、エキスパート、ハイマスター）に 15 種類の人材像モデルを定義し、社内セキュリティコンテストの実施、社内認定制度の実施、セキュリティマイスターコミュニティにおける情報交換の場の提供等を通じて、社内におけるセキュリティ技術者の発掘と育成を進めている。

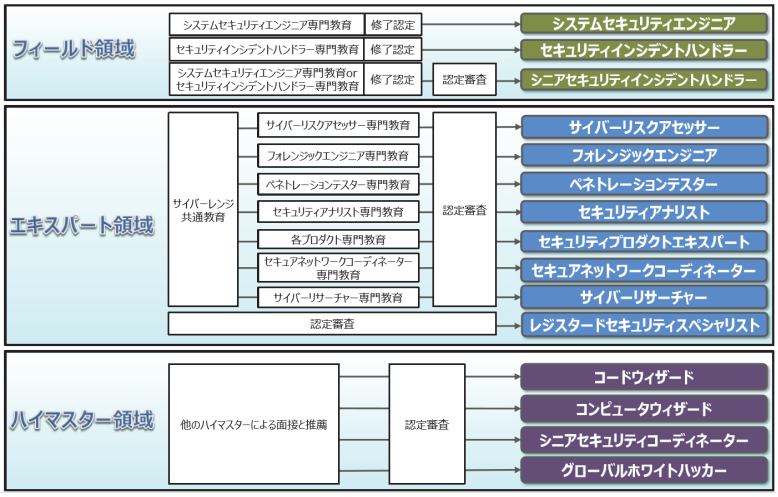

図 2.1-5　富士通のセキュリティマイスター認定制度

出所）富士通株式会社「セキュリティ人材育成の取り組み」，
http://www.fujitsu.com/jp/solutions/business-technology/security/secure/concept/security-initiative/security-meister/securitymeister-certification-system.pdf より取得

日立グループでは、「情報セキュリティ人財育成活動」を運用しており、IT スキル標準（ITSS）のレベルと専門性（管理系、技術系）に応じた人材育成とキャリアパスの構築を支援しており、情報セキュリティスペシャリスト審査による社内人材の可視化、情報セキュリティ業務、情報セキュリティコミュニティによる「学びの場」といった活動で構成される育成サイクルにより、階層に分かれたセキュリティ人材ピラミッドを運用している。

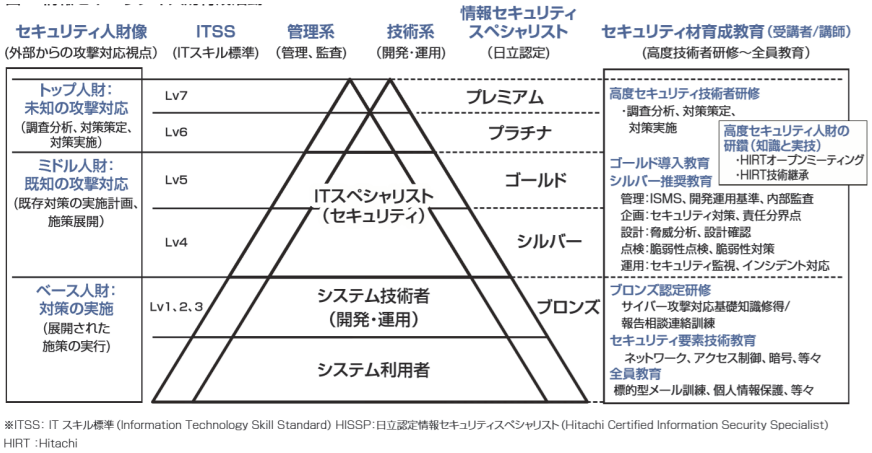

図 2.1-6　日立の情報セキュリティ人財育成活動

出所）株式会社日立製作所「情報セキュリティ報告書 2017」
http://www.hitachi.co.jp/csr/download/pdf/securityreport.pdf より取得

日本電気では、3 段階のレベルの「NEC プロフェッショナル認定制度（NEC Certified Professional）」（NCP 認定制度）を運用している。高度な専門性を活かせる人材の育成が重要と捉え、専門性を市場価値に照らして人材カテゴリーごとに人材タイプを設定し、達成目標となるスキルや業績の水準を詳細に定義している。

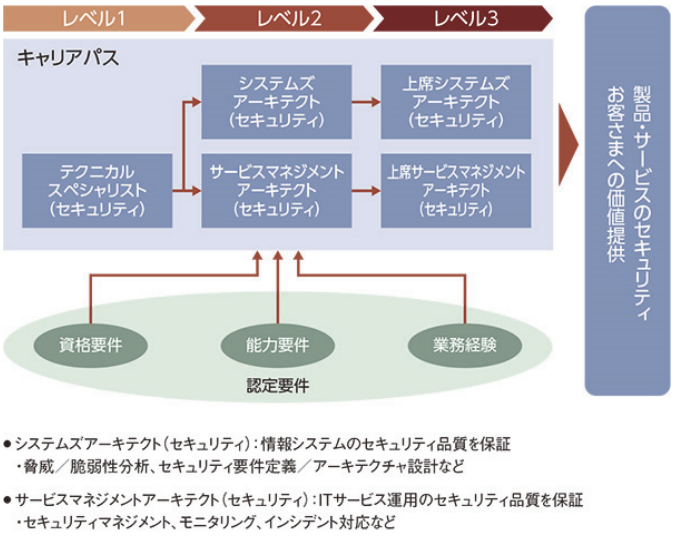

図 2.1-7　NEC プロフェッショナル認定制度（NCP 認定制度）- セキュリティ

出所）日本電気株式会社「NEC HP プロフェッショナルな人材の育成」
http://jpn.nec.com/cybersecurity/jinzai/index.html より取得

さらに、上記 3 社は、2017 年 12 月に「サイバーセキュリティ人材育成スキーム策定共同プロジェクト」を発足し、①統合セキュリティ人材モデルの策定、②人材育成シラバス・教材ガイドラインの作成、③サイバーレンジ連携インターフェースの策定、④演習を実施するための運用ルール・マニュアルの整備などを進めている。

これら、先進企業にみられるように、情報セキュリティ人材のキャリアパスを形成するには、社内のセキュリティ人材の発掘と把握、社内認定制度や専門職としての職位の設定、セキュリティ人材による社内コミュニティの形成などが必要であると考えられる。

2.2 経営層と現場における体制とコミュニケーション

2.2.1 経営層と現場とのコミュニケーション

現場と経営層の情報セキュリティに対する意識や考え方の乖離により、組織としてのセキュリティ対策がなかなか進まないといった課題が多少の差はあれ、どこにも存在しているのが実情である。今般、そのギャップを埋め、円滑なコミュニケーションを実現するべく、先述にもあったように、CISO 等という「橋渡し」的な役職を設置しているのが世界的な潮流である。

ここで、一口にコミュニケーションといっても、CISO 等と経営層とのコミュニケーションは「平常時」と「事故時」の大きく二つに分けることができる。

前者は、主にセキュリティ対策への予算化についてであり、リスクを可能な限り、定量的な数値で明確化した上で、問題意識を共有するとともにその対応策（例えば、製品やサービス）を調査・比較・評価し、最終的に経営者に判断してもらうことが望ましいと考えられる。

他方、後者は自組織における情報システムへの攻撃時や情報漏えい時等に、CISO 等がどのような情報を経営層にエスカレーションし、報告・共有するのか、また、効率的なコミュニケーション手段は何か、に関して予め検討しておく必要がある。例えば、実際に被害を受けた際は、経営者として、本当に意図的な攻撃であったのか、証拠として出せるものがあるのか、法的措置に意味があるのか、といった事項を弁護士等と検討する必要があるため、判断に資する、ログ等の証拠を保全・整理しておき、CISO 等として説明できるようにしておくことが肝要である。また、事業継続が可能か否かを検討・判断するための情報として、代替運用についても示すことができるよう準備しておくことが望ましい。さらに、被害の規模が甚大であり、かつそれによる影響が大きい場合は、経営者自らによる記者会見等、マスコミへの対応に関するセキュリティ視点における助言（又は必要に応じた同席）もコミュニケーションの形態として有り得る。

2.2.2 情報セキュリティ統制

特定非営利活動法人日本ネットワークセキュリティ協会によると、情報セキュリティに係る体制として、経営者を組織のトップに置き、その下に情報セキュリティ管理責任者である CISO 等や情報セキュリティ委員会を設置する体制を一般的な例として挙げている。しかし、実際の体制は様々であり、例えば、企業によっては、執行役社長をトップに情報セキュリティ担当役員、総務部情報セキュリティセンター、サイバーセキュリティ対応チーム、本部・部門及び関連会社の情報セキュリティ組織から構成されているところもあれば、執行役社長を筆頭に情報セキュリティ統括責任者、情報セキュリティ委員会、事業所における責任者・管理者等で構成している企業もある。なお、いずれの体制の運用においても、誰が責任者であるのかも含め、体制を構成する個々の組織の役割やレポートライン等が不明確又は煩雑であれば、全体としてうまく機能しない可能性が高いため、これらを明確化しておくことが重要である。

近年、情報セキュリティは経営課題とすべきと論じられている。例えば、「重要インフラ

の情報セキュリティ対策に係る第 4 次行動計画」[11]においては、情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むとともに、重要インフラ事業者等が取り組む内部ステークホルダー相互間のリスクコミュニケーション及び協議の推進への必要に応じた支援の必要性等が謳われている。また、前述の「サイバーセキュリティ経営ガイドライン」では、経営層が、経営者によるサイバー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である CISO 等に指示すべき「重要 10 項目」を示しており、その中に、「3．1．サイバーセキュリティリスクの管理体制構築」が示されている。

本節に関連する指示は以下のとおりである。

- 指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定
- 指示 2 サイバーセキュリティリスク管理体制の構築
- 指示 3 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

上記の指示に対し、企業として如何に取り組むかは、それぞれの企業の実態によるものと考えられ、正解は存在しない。経営層からのトップダウンで事業を推進する組織と現場からのボトムアップで事業を推進する組織、過去に大きな情報セキュリティインシデントを体験した組織と未体験の組織、組織における IT 部門の力の強弱等によっても、その組織体制は変わってくるものと考えられる。

その一方で、共通する部分も考えられる。情報セキュリティの統制は、全社に対して実現されるべきものであり、独立した組織によって担当すべきものと考えられる。統制する部門と、その統制に基づいて執行する部門が独立することで、より効果的な情報セキュリティ対策を実現できることが期待される。ここで、情報セキュリティを統制する部門と、IT を統制する部門があるときに、その力関係が重要な要素となることが考えられる。それぞれの組織の実態等に合わせて、適切に組織を構築・運用することが望ましい。

2.2.3 組織間の情報共有

情報共有は、組織間の連携のため、作業効率向上のため、その他様々な場面で利用される。しかしながら、やみくもにフレームワークのみを先に構築したとしても、どのような場面で誰とどのような内容の情報を共有するのか、共有主体にとって、どのようなメリットが期待できるのか、などが事前に詰められていなければ、真に有効な情報共有は実現できない。

情報セキュリティ確保のための情報共有は、いくつかの類型に分けられる。例を挙げると、緊急度の高い情報、機密度の高い情報、自然言語による情報、機械可読な形式による情報、脆弱性や不正アクセスに関する情報、地政学的な情報、得られた"Information"に対し、必要性・信頼性に基づき選択を行い、内容について分析を実施することによって、その解釈や経営者にとって必要な価値判断を与える、いわゆる"Intelligence"の性格をもつ情報等、それぞれの性質や組合せ等に合わせた情報共有を行うことが重要となる。例えば、公開された脆弱性情報と、自社をターゲットにした標的型攻撃を検知した場合では、誰と何をどうやって共

[11] サイバーセキュリティ戦略本部：「重要インフラの情報セキュリティ対策に係る　第 4 次行動計画」、平成 29 年 4 月 18 日、https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf

有するかは変わってくると考えられる。

加えて、情報共有はステータスによっても分類できる。脆弱性情報であって攻撃コードが既知であるか否か、自社に不正アクセスが届いているか否か、既に自社内で被害が発生しているか否かによっても、誰と何をどうやって共有するかは変わってくる。特に、自社に被害が及んでしまっている場合、自社内で情報共有環境を構築していると、情報共有が機能しなくなる可能性があるため、様々な場面に備えた情報共有体制を構築する必要がある。

情報の性質とステータスを類型化し、それぞれの類型に基づく情報共有のルール作りとその訓練を実施することが重要であると考えられる。どのような場合に、いつ、誰と、何を、どのように共有するのかについて一覧化し、事前準備することが重要である。

情報共有の対象に国外の組織が含まれる場合には、さらに注意を要する。時間（時差）に加え、言葉や文化の壁はもちろん、各国法制度等へのガバナンスについても留意する必要があると考えられる。そのため、国外の者と情報共有する場合には、担当者を明確化し、現地の者と連携して検討する、三極あるいはそれ以上との共有については自組織がハブの役割になる、などのリスクを勘案した上で対応する必要がある。

なお、情報共有体制も、従前からの情報セキュリティリスクに対応する CSIRT 機能を有する体制の他に IoT の普及に伴う製品に係るセキュリティリスクに対応するための PSIRT（Product Security Incident Response Team）機能の必要性も改めて議論されているなど、今後様々な態様が考えられるが、まずは、情報セキュリティを統制する組織が中心となって、国内外各組織との連携を図ることが、統制を実現する上でも重要ではないかと考えられる。

おわりに

本報告書では、経営とセキュリティに関し、委員会で得た現状の情報を認識し、調査した結果を課題と提言としてまとめた。主に、セキュリティ人材の育成やセキュリティのコミュニケーションに関する提言を通じて、企業の経営とセキュリティを確保するために必要となる事柄を明確にした。

サイバーセキュリティの優れたガバナンスを活用する努力を続け、サイバーセキュリティの難題に立ち向かっている企業は、攻撃を受けても秩序を取り戻すことができるだろう。脅威の全てを取り除くことは不可能だが、抵抗力を備えた企業は自らをどのように守り、問題が生じたときにその問題をどのように早期に検知し、どのようにすれば効果的に対応できるかを知ることができる。

情報セキュリティ調査専門委員会では、情報セキュリティ技術とビジネスの方向に関する調査を行い、これまでの情報セキュリティ技術とビジネス環境や社会制度の変化を整理し、情報セキュリティに関する今後の技術開発やビジネス展開の方向について分析を行うことを目的として活動している。本委員会としては、今後の日本における、IT の活用を通じた産業界の発展と国際競争力強化のために、本書が活用されることを期待する。

平成 29 年度情報セキュリティ調査報告書
ー経営とセキュリティに関する調査ー

発　行　日　　平成30年3月
編集・発行　　一般社団法人 電子情報技術産業協会
　　情報・産業システム部
　　〒100-0004　東京都千代田区大手町1丁目1番3号
　　大手センタービル
　　TEL　(03)5218-1057
印　　刷　　株式会社 オガタ印刷