内閣サイバーセキュリティセンター委託調査

平成２９年度企業において育成すべき人材の知識・スキル及びカリキュラムに関する調査

調査研究報告書

平成３０年　３月

みずほ情報総研株式会社

目　次

１．　はじめに 3
１．１ 背景 3
１．２ 略称について 4
２．　企業においてサイバーセキュリティ対策に従事する人材と教育の現状 5
２．１ 想定する組織内の体制モデル 5
２．２ 文献調査 7
２．２．１ 調査概要 7
２．２．２ 調査から得られた知見 10
２．２．３ 調査結果の分析 38
２．３ ヒアリング調査 41
２．３．１ 調査概要 41
２．３．２ ヒアリング調査を通じて把握された事項 41
２．４ 政府会議等における議論の把握 47
３．　課題と方向性 50
３．１ 現状における課題 50
３．２ 課題の解決に関する方向性 54
３．３ 方向性を踏まえた企業における考え方の具体化 56
３．３．１ 組織体制についての検討 56
３．３．２ 役割や人材像に関する検討 58
３．３．３ 戦略マネジメント層の検討に係る考慮事項 60
３．３．４ 戦略マネジメント層向けのカリキュラムについての検討 63
４．　役割と人材像、要求されるスキル、具体的なカリキュラム 65
４．１ 戦略マネジメント層 65
４．１．１ 求められる役割 65
４．１．２ 想定されるキャリアパス 66
４．１．３ 求められる知識・スキル 67
４．１．４ 育成のためのカリキュラム 71
４．２ システム担当（実務者層） 73
４．２．１ 求められる役割 73
４．２．２ 想定されるキャリアパス 75
４．２．３ 求められる知識・スキル 76
４．２．４ 育成のためのカリキュラム 82
４．３ システム構築・運用担当（技術者層） 84
４．３．１ 求められる役割 84
４．３．２ 想定されるキャリアパス 86

４．３．３ 求められる知識・スキル 87
４．３．４ 育成のためのカリキュラム 95
５． 今後の検討事項 97
５．１ 教材の研究開発の推進 97
５．２ 講師の育成 98
５．３ 産学官連携に基づく具体的なプログラムの推進 99
６． おわりに 100

１．はじめに

１．１ 背景

サイバーセキュリティに係る人材を確保し、これらの人材が活躍できるキャリアパスを実現していくことが重要となっている中、サイバーセキュリティ人材の「需要」と「供給」を相応させ、好循環の形成を促進していくためには、需要を産む産業界や、教育・訓練を行う主体（大学など）を含めた産学官が連携し、人材像の正しい認識が共有されていることが必要である。また、既にサイバーセキュリティ人材の育成に関する様々な施策が実施されている中、こうした人材像の共通認識を持ちつつ、個々の施策について連携を強化することによって、より効果的な実施を図ることができるとともに、セキュリティ教育に関わる有限なリソースを効率的に活用できる可能性もある。具体的には、産業界においては、情報通信技術（IT）の利活用の主軸が CIT（コーポレート IT）から BIT（ビジネス IT）に移行し、BIT を前提としたビジネス戦略の推進及びリスクマネジメントの確保にあたり、ビジネスにおけるサイバーセキュリティの重要性が増大している。そして、このような環境の変化に対応したセキュリティ人材の確保及び育成が必要とされている。一方、教育界では、そのようなセキュリティ人材が持つべき知識・スキルを習得するためのモデルとなるカリキュラムが必要とされており、産学官の関係者が一体となった取組が期待されている。

こうした状況を受けて、『サイバーセキュリティ人材育成プログラム』（平成 29 年 4 月 18 日サイバーセキュリティ戦略本部決定）及び『2020 年及びその後を見据えたサイバーセキュリティの在り方について-サイバーセキュリティ戦略中間レビュー-』（平成 29 年 7 月 13 日サイバーセキュリティ戦略本部決定）において、施策間の連携を強化するため、サイバーセキュリティ人材の人材像や必要とされる知識・スキルを明らかにするとともに、モデルとなるカリキュラムの策定が必要であると示された。

このような背景を踏まえ、企業等におけるビジネスモデル、IT 利活用の方法や規模等によって類型化が必要となる可能性を十分に考慮しつつ、

（１）企業内のサイバーセキュリティに関する組織体制
（２）組織体制における、各層の役割・人材像
（３）必要とされる知識・スキル（セキュリティに関する知識・スキルに限らず、IT に関わる基礎的な知識（計算機科学や通信理論など）から社会科学的（経営、法律など）なもの、さらには、トレンド（IT 利活用のモデルやサイバー犯罪動向、国際情勢など））
（４）知識・スキルを習得するための、モデルとなるカリキュラム

の明確化を目的として、本調査研究を実施した。

１．２ 略称について

本報告書で用いる略称は、それぞれ次の意味を示すものとする。

BIT	Business IT
CBK	Common Body of Knowledge
CIO	最高情報責任者
CISO	最高情報セキュリティ責任者
CISSP	Certified Information Systems Security Professional
CIT	Corporate IT
CSIRT	Computer Security Incident Response Team
DB	データベース
ICT	情報通信技術
IoT	Internet of Things
(ISC)²	International Information Systems Security Certification Consortium
IT	情報技術
IPA	独立行政法人情報処理推進機構
ISAC	Information Sharing and Analysis Center
ISMS	情報セキュリティマネジメントシステム
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
MIT	マサチューセッツ工科大学
NACD	National Association of Corporate Directors
NCA	日本コンピュータセキュリティインシデント対応チーム協議会
NICE	National Initiative for Cybersecurity Education
NICT	国立研究開発法人情報通信研究機構
NISC	内閣官房内閣サイバーセキュリティセンター
NIST	米国国立標準技術研究所
OS	オペレーティングシステム
PC	パーソナルコンピュータ
PoC	連絡窓口（Point of Contact）
SOC	セキュリティオペレーションセンター
産業横断検討会	産業横断サイバーセキュリティ人材育成検討会

２．企業においてサイバーセキュリティ対策に従事する人材と教育の現状

２．１　想定する組織内の体制モデル

本調査において想定する、企業等の組織内におけるサイバーセキュリティに関する体制のモデルを次図に示す。

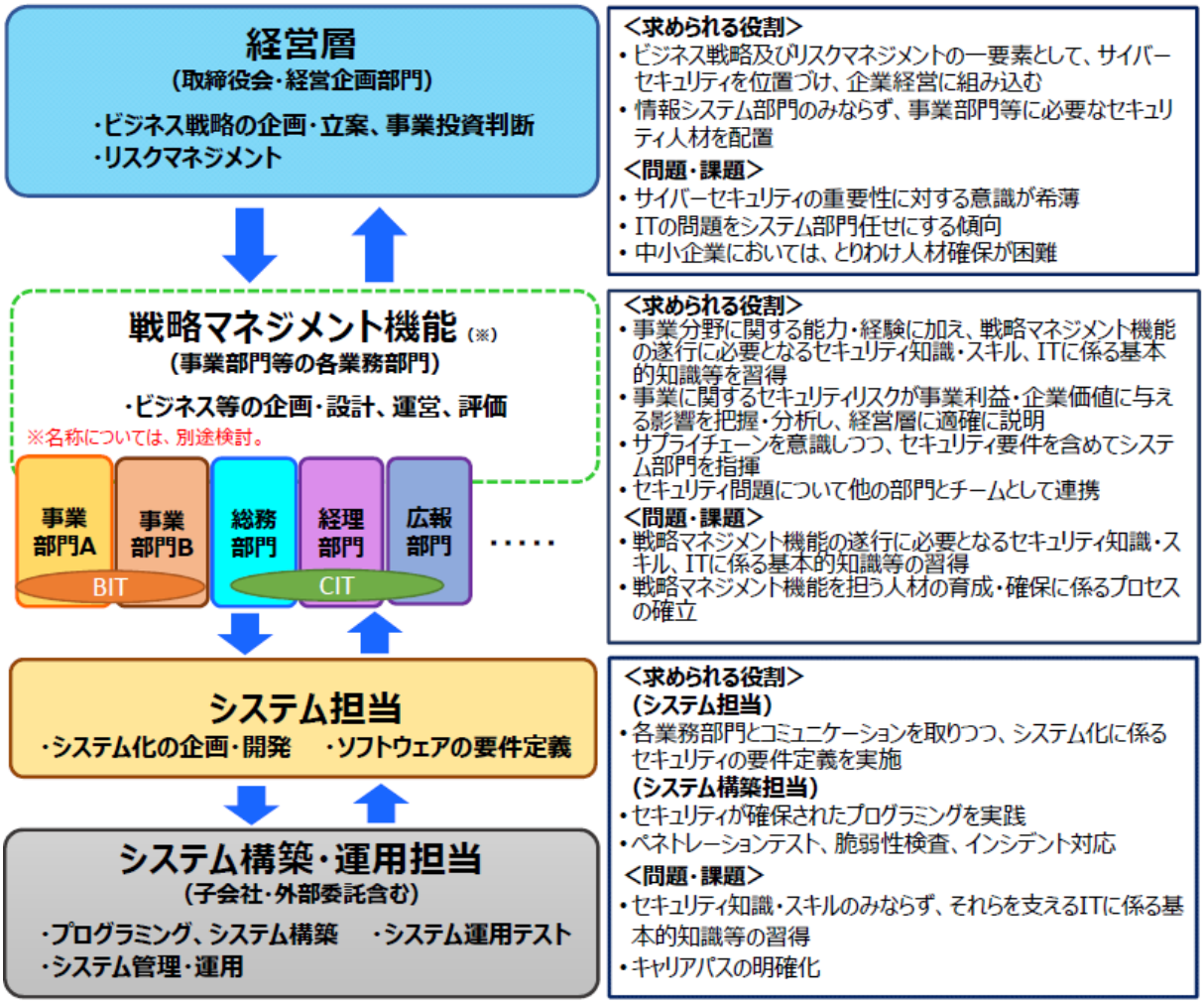

図 １　想定する組織内の体制モデル（出典：脚注参照[1]）

本調査では、上図における「経営層」「戦略マネジメント機能」「システム担当」「システム構築・運用担当」の４種類の人材ごとに１．１に示す（１）～（４）の内容の明確化を図る。このとき、「戦略マネジメント機能」については、サイバーセキュリティ対策を担う人材としてこれまでその人材像が明確化されていないことから、本調査において重点的に扱うこととする。なお、「戦略

[1] サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ第２回会合　資料 1-2 より引用。
https://www.nisc.go.jp/conference/cs/jinzai/wg2/dai02/pdf/02shiryou0102.pdf

マネジメント機能」を担う人材の呼称については、後述のように文献や検討主体ごとに異なる呼称や人材像で扱われており、統一されていない。今後、人材像についての関係機関や専門家における共有が図られていくと見込まれるが、本調査では仮に「戦略マネジメント層」と称することとする。

また、本調査で対象とする「システム担当」「システム構築・運用担当」を担う人材は、それぞれの役割の中でセキュリティ確保のための方策について、経営層や戦略マネジメント層から示される方針をもとに、セキュリティ確保のための方策に関して、その実装方法を検討・立案する役割を担う人材として扱うものとする。

２．２ 文献調査

本調査の実施にあたり、公表されている文献やインターネット上の情報源をもとに収集した情報について整理する。

２．２．１ 調査概要

本調査において調査対象とした文献の一覧は次表の通りである。以降の記述において当該文献を参照する際には、「[文献 2]によると」のように本表における参照用連番を用いて表記することとする。また、１．１にて示した本調査で明確化しようとする 4 種類の内容に関連する記述が当該文献に含まれているかどうかを●印にて表中に示した。

表 1　調査対象文献の一覧

発行国	参照用連番	著者，文献名称，発行機関，発行時期	調査事項との対応（●＝有）			
			(1)	(2)	(3)	(4)
国内	文献1	産業横断サイバーセキュリティ人材育成検討会 第一期最終報告書，産業横断サイバーセキュリティ人材育成検討会, 2016 年 9 月.	●	●	●	－
	文献2	産業横断サイバーセキュリティ人材育成検討会 第二期中間報告書，産業横断サイバーセキュリティ人材育成検討会, 2017 年 11 月.	●	●	●	－
	文献3	CSIRT 人材の定義と確保 Ver.1.5，日本コンピュータセキュリティインシデント対応チーム協議会, 2017 年 3 月.	●	●	－	－
	文献4	鎌田敬介，サイバーセキュリティマネジメント入門，一般社団法人金融財政事情研究会, 2017 年 10 月.	●	●	－	－
	文献5	人生 100 年時代構想会議 中間報告，首相官邸, 2017 年 12 月.	－	●	－	－
	文献6	ITSS＋，独立行政法人情報通信研究機構（IPA）, 2017 年 4 月.	－	●	●	－
	文献7	セキュリティ知識分野（SecBoK）人材スキルマップ 2017 年版, JNSA 教育部会, 2017 年 9 月.	－	●	●	－
	文献8	SOC の役割と人材のスキル 1.0 版，日本セキュリティオペレーション事業者協議会, 2016 年 7 月.	－	●	●	－
	文献9	「管理職に求められる「マネジメント」、管理職が執るべき行動の在り方について」，管理職のマネジメント能力に関する懇談会資料，内閣府人事局, 2016 年.	－	－	●	－
	文献10	平成 28 年度理工系プロフェッショナル教育推進委託事業 工学分野における理工系人材育成の在り方に関する調査研究（情報セキュリティ人材育成に関する調査研究）成果報告書，文部科学省（委託先：学校法人岩崎学園情報セキュリティ大学院大学）, 2017 年 3 月.	－	－	●	●
	文献11	東京電機大学国際化サイバーセキュリティ学特別コース（CySec）[5MG]情報セキュリティマネジメントとガバナンス, 2017 年度	－	－	－	●
米国	文献12	Cybersecurity Framework, NIST, 2014 年 2 月. （邦訳版）重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0 版，独立行政法人情報処理推進機構（IPA）, 2014 年 5 月.	●	●	－	－
	文献13	Cyber-risk Oversight (Director's Handbook Series), National Association of Corporate Directors (NACD), 2017 年.	●	●	－	－

発行国	参照用連番	著者，文献名称，発行機関，発行時期	調査事項との対応（●＝有）			
			(1)	(2)	(3)	(4)
米国	文献14	Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST, 2017 年 8 月.	－	●	●	－
	文献15	Robert L. Katz: Skills of an Effective Administrator, Harvard Business Review, 1974 年 9 月号. （邦訳版）ロバート・L・カッツ: スキル・アプローチによる優秀な管理者への道，ハーバードビジネス 1982 年 6 月号，ダイヤモンド社.	－	－	●	－
	文献16	CISSP8ドメインガイドブック, (ISC)², 2017 年.	－	－	●	－
	文献17	Cybersecurity Curricula 2017 (CSEC2017) Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity version0.95, IEEE, 2017 年.	－	－	●	●
	文献18	MBA コース 2017 年春期科目“Cybersecurity”, MIT Sloan school.	－	－	－	●
EU	文献19	European e-Competence Framework 3.0, EU, 2014 年.	－	●	●	－
	文献20	Status of privacy and NIS course curricula in Member States, ENISA, 2015 年.	－	－	－	●
英国	文献21	SFIA（Skills Framework for the Information Age）Version 6/7 , SFIA Foundation, 2015-7 年.	－	●	●	－
シンガポール	文献22	Skill Framework for Infocomm Technology, シンガポール政府 SkillsFuture プロジェクト, 2017 年.	－	●	●	－
	文献23	Cyber Security Associates and Technologists Programme, CSA, 2017 年.	－	－	－	●
イスラエル	文献24	National Cyber Security Organisation: ISRAEL, CCDCOE / NATO, 2017 年.	●	－	－	－
	文献25	Tabansky, L., & Ben Israel, I.: Cybersecurity in Israel. (Springer Briefs in Cybersecurity Series, Springer International Publishing, ISBN 978-3-319-18985-7, 2015.	●	－	－	－

（各文献のうち、ウェブ上で公表されているもののURL）

[文献1] http://cyber-risk.or.jp/sansanren/xs_20160914_01_Report_1.0.pdf

[文献2] http://cyber-risk.or.jp/cric-csf/report/CRIC-CSF-2nd-Interim-Report.pdf

[文献3] http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf

[文献5] https://www.kantei.go.jp/jp/singi/jinsei100nen/pdf/chukanhoukoku.pdf

[文献6] https://www.ipa.go.jp/jinzai/itss/itssplus.html

[文献7] http://www.jnsa.org/result/2017/skillmap/index.html

[文献8] http://isog-j.org/output/2016/SOC_skill_v1.0.pdf

[文献9] https://www.cas.go.jp/jp/gaiyou/jimu/jinjikyoku/kanri_kondankai/dai1/siryou.html

[文献10] http://www.mext.go.jp/a_menu/koutou/sangaku2/1387701.htm

[文献11] https://cysec.dendai.ac.jp/category/allyear/2017/#tabs-5

[文献12] https://www.nist.gov/cyberframework
（邦訳版） https://www.ipa.go.jp/security/publications/nist/index.html

[文献13] https://isalliance.org/board-auditors/cybersecurity-and-corporate-boards/

[文献14] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

[文献16] https://japan.isc2.org/files/CISSP8_Guidebook_2017_1101.pdf

[文献18] https://sloanbid.mit.edu/resources/15.580.pdf

[文献19] http://www.ecompetences.eu/
[文献20] https://www.enisa.europa.eu/publications/status-of-privacy-and-nis-course-curricula-in-eu-member-states
[文献21] https://www.sfia-online.org/en
[文献22] http://www.skillsfuture.sg/skills-framework/ict
[文献23] https://www.csa.gov.sg/programmes/csat
[文献24] https://ccdcoe.org/multimedia/national-cyber-security-organisation-israel.html

２．２．２ 調査から得られた知見

調査対象文献に記載されている内容のうち、本調査で明確化すべき内容についての検討にあたり考慮すべき事項について、１．に示す（１）～（４）の４種類の内容ごとに整理する。

（１）企業内のサイバーセキュリティに関する組織体制

調査対象文献においてサイバーセキュリティ対策を実施するための組織体制について言及されている内容の概要を以下に示す。

① 産業横断サイバーセキュリティ人材育成検討会における、企業内のサイバーセキュリティ対策を担う体制に関する検討

[文献 1]及び[文献 2]において、産業横断サイバーセキュリティ人材育成検討会（以下、「産業横断検討会」という。）が企業内のサイバーセキュリティ対策を担う体制に関して、次の検討を行っている。

ア）ユーザ企業の類型（[文献 2]による）

産業横断検討会では、セキュリティ人材のキャリアパスの検討に際して、「IT と事業の関係性」をもとに次の類型化を行っている。これは「IT ビジネス企業」においてはビジネス開発が IT システム開発を伴うことが多いことから、DevOps あるいは DevSecOps などと呼ばれるように開発と運用とセキュリティ対策がサイクル的に同時並行的に行われていると見込まれることによる。この結果、こうした企業におけるセキュリティ人材のキャリアパスは通常の人事制度として確立され、「伝統的な企業」との間でセキュリティ人材のキャリアパスと大きく異なると想定されている。表 2　産業横断検討会によるユーザ企業の類型（[文献 2]をもとに作成）

IT ビジネス企業	ビジネス自体がインターネット上にある企業、または、IT を駆使してビジネスを行う企業 ● 業界：E-コマース、金融、各種クラウドサービス事業者等 ● サイバーセキュリティがビジネスに直結していることに自覚的であり、サイバーセキュリティに関して経営層の理解も高い。
伝統的な企業	ものづくり的な部分がビジネスの根幹である企業 ● 業界：電力、ガス、水道、石油、化学、自動車、航空、鉄道、その他製造メーカ等（多くの重要インフラ関連企業が含まれる。） ● 情報だけでなく、物理的なプラントや人などの安全（セーフティ）も含めたセキュリティ[2]。 ● サイバーセキュリティの重要性を認識しつつも、その優先度は必ずしも高くない。

[2] 物理的なプラント等における IT 化の進展により、サイバーセキュリティの問題が保安の問題につながるようなケースを想定。

イ）サイバーセキュリティ専門部署の必要性（[文献 1]による）

前項で「伝統的な企業」として類型化された企業において、外部からの脅威や攻撃者への対応が必要なサイバーセキュリティの分野を扱うには、企業に既にある機能を分化して部門を設置するだけでは対応が難しいことが判明した旨が示されている。産業横断検討会に参加している企業でもサイバーセキュリティ対応部門を新設している事例が多いことから、今後同様にサイバーセキュリティ対応部門の保有／設置が必須になることが想定されている。

ウ）セキュリティ統括（室等）の定義について（[文献 2]による）

「セキュリティ統括（室等）」とは、「伝統的な企業」において、情報システム部門とは別に、企業活動の全体に跨がってサイバーセキュリティ対応を担う部署を指す。産業横断検討会への参加企業において、徐々に業務系 IT 以外のシステムにおいて IT を利活用する事例が多くなり、それに伴い従来の情報システム部門だけではセキュリティに関しての企画・戦略・管理が難しく、それらをとりまとめる部門が必要との議論に基づいて打ち出されたものである。このセキュリティ統括は、後述の人材の役割に関する検討の中で「エキスパート人材（セキュリティ統括人材）として提案されている人材キャリアと対応するものである。

② NIST によるサイバーセキュリティを対象とするフレームワークの提示

[文献 12]は、重要インフラ事業者を主たる対象として、サイバーセキュリティへの取組を企業にとってのビジネス上のモチベーションにつながるものとし、サイバーセキュリティリスクを企業のリスク管理プロセスの一環として扱えるようにするためのフレームワークとして、米国 NIST が 2014 年 2 月に公表したものである。本フレームワークの特徴は次の通りである。

- フレームワークコアとして、企業におけるサイバーセキュリティリスクの管理機能を、「特定」「防御」「検知」「対応」「復旧」の 5 種類に大別し、さらに複数のカテゴリに整理している。企業ではこれを参照することで、対策の立案を効率的に進めたり、取引先や連携先等とのコミュニケーションを円滑にしたりする効果が得られる。
- フレームワークインプリメンテーションティアとして、企業におけるサイバーセキュリティ対策プロセスの成熟度に関する指標を提供。この指標についても顧客や連携先等とのコミュニケーションの円滑化や組織における改善への取組に活用可能である。
- フレームワークに適合さえた形で提供されるプロファイルを参照することで、企業における「ビジネス要件」「リスク許容度」「リソース」「プライバシー保護」等のニーズに応じたサイバーセキュリティ対策の検討を支援。

なお、本調査の実施時点で NIST において改訂版（Version 1.1）の検討が進められている。

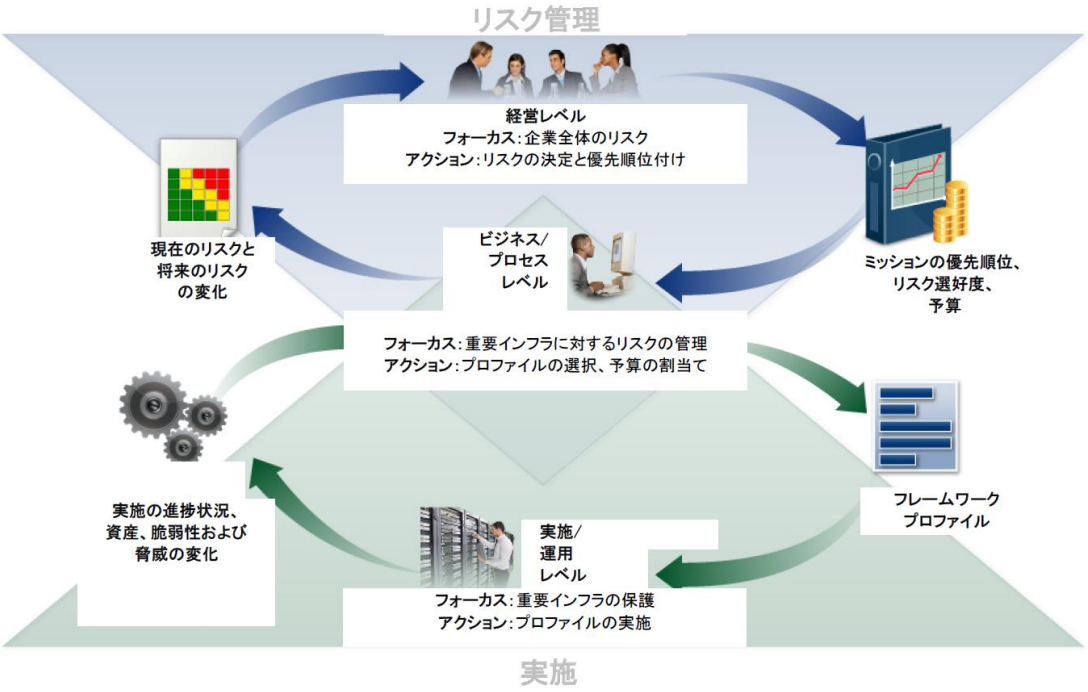

図 2　NIST サイバーセキュリティフレームワークにおける企業内の情報と意思決定の流れ(概念図)[3]

③ NACD による経営層が理解しておくべきサイバーセキュリティ５原則

[文献 13]では、企業の経営層が理解しておくべき、サイバーセキュリティに関する次の 5 種類の原則を軸に、サイバーセキュリティ対策に関する考え方を提示している。

1) 経営層は、サイバーセキュリティを IT のみの問題ではなく、企業全体のリスクマネジメントの問題として理解し、対処する必要がある。
2) 経営層は、企業特有の状況に関連づけてサイバーセキュリティの法的遂行について理解すべきである。
3) 役員はサイバーセキュリティの専門家と適切に連絡を取り、役員会の議題として定期的かつタイムリーにサイバーリスクの管理について議論すべきである。
4) 経営層は、適切な人材と予算を用いた企業全体のサイバーリスクマネジメントフレームワークの構築への期待を示すべきである。
5) サイバーリスクについての役員会では、どのリスクを除去し、どのリスクを需要するか、さらにどのリスクについて緩和したり保険に移転したりするかの区別について、それぞれのアプローチに応じた計画と併せて論ずるべきである。

本調査に関連した内容としては、経営層に対して上記の 5 原則の実施を求めているほか、第 4 の原則に関連して、経営層に対しサイバーリスクをマネジメントするためのチーム（サイバー

[3] 独立行政法人情報処理推進機構（IPA）によるセキュリティ関連 NIST 文書の翻訳資料より引用。
『重要インフラのサイバーセキュリティを向上させるためのフレームワーク　1.0 版』
https://www.ipa.go.jp/security/publications/nist/index.html

リスクチーム）の編成を求めている点が注目される。また付録として、経営層向けのサイバーリテラシーに関するセルフチェックリスト、M&A におけるリスク、計量の考え方、参考とすべき情報源等が添付されている。

④ NCA による企業内体制の３類型

[文献 3]では、企業における専門人材の在籍状況等をもとに、外部のベンダへの委託の度合いに応じた CSIRT の実装例の分類として、次の３種類のモデルを提示している。

表 3　CSIRT の実装モデル（[文献 3]を参考に作成）

モデル	定義	CSIRT の特徴
A	ユーザ企業で総務部門等を主体として構築・運用されている CSIRT	自警団として最低限の機能のみを有し、システム維持はベンダに委託
B	ユーザ企業で IT 系子会社、または情報セキュリティに関する専門部門を主体として構築・運用されている CSIRT	自組織のコア事業以外の部分をベンダにアウトソーシング
C	IT 系、セキュリティベンダ系企業において構築・運用されている CSIRT	CSIRT 機能のほとんどすべてを自組織にて保有

調査結果からの考察

①～④の文献より、企業内のサイバーセキュリティに関する組織体制について、次のことが考察される。

- 米国においては、情報システム部門、ビジネス部門の業務に関わらず、サイバーセキュリティ対策を含む IT 利活用に関する指揮監督は経営層の責任で行うべきとの認識のもと、ビジネスにおけるリスク管理の観点からもサイバーセキュリティ対策を担う組織体制の構築が進められている。
- 一方、日本ではこれまでサイバーセキュリティ対策は情報システム部門等を中心として実施され、ビジネス部門におけるサイバーセキュリティ対策を担う組織体制の構築はこれからの課題である。
- 日米でこうした違いが生ずる背景としては、米国では次図に示すようにユーザ企業に IT 人材が数多く存在し、かつその流動性が高いことから、企業のニーズに応じて必要な体制の構築が容易であるのに対し、日本の IT 人材はベンダに偏在しており、「伝統的な企業」におけるサイバーセキュリティ対策はベンダへの委託が前提となってきたことに起因する可能性が高い。

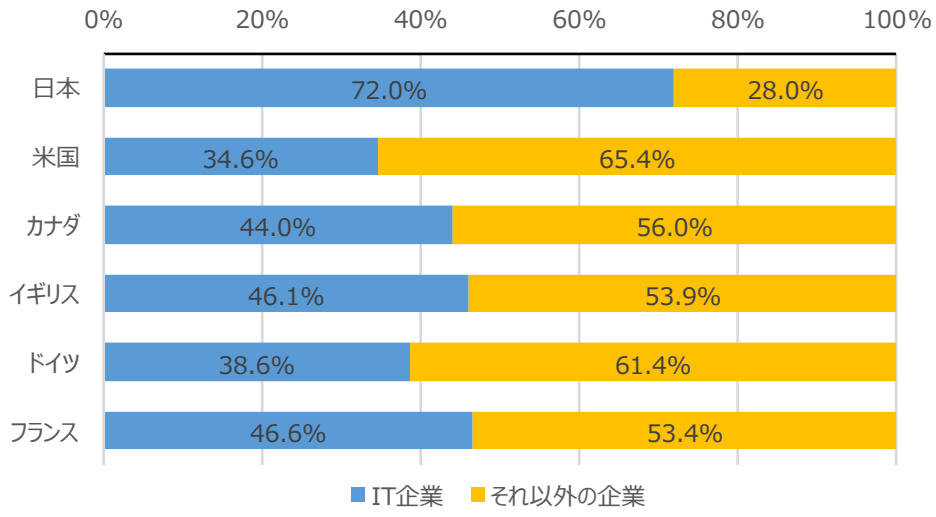

図 3　IT 企業とそれ以外の企業に所属する情報処理・通信に携わる人材の割合

出典:IT 人材白書(独立行政法人情報処理推進機構(IPA), 2017 年)図表 1-1-1 をもとに作成

（２）組織体制における、各層の役割・人材像

調査対象文献においてサイバーセキュリティ対策を実施するための組織体制における、各層の役割・人材像等に関して言及されている内容の概要を以下に示す。なお区分に用いられる名称については、「人材像」という用語が「ある専門性に特化した人材」という印象を与えることから、兼務を前提としたり、非常時のみの業務を担うような人材に対して「役割」（ロール）が、特定の人材像や役割との対応関係を前提としない場合について「専門分野」が、それぞれ用いられることがある。

① 産業横断検討会（第１期最終報告書）による人材定義リファレンス

[文献 1]において、企業のセキュリティ関連活動を機能として洗い出し、それぞれの機能を実施していくために必要な 30 の役割として、次表の定義を行っている。表中に示されている通り、「監査・個人情報保護」を除き、これらの役割はいずれも情報システム部門に所属している人材が担う役割として想定されている。

表 4　サイバーセキュリティ機能を担う役割一覧（[文献 1]より引用）

カテゴリ		役割（担当）	適応力・態度（■＝チームワークや作業遂行に必要）											
			問題発見力	問題分析力	仮説設定力	論理思考力	概念化力	俯瞰力	深耕力	革新力	継続力	相手の考えを理解する力	自分の考えを伝える力	共感を呼ぶ力
情報システム部門におけるサイバーセキュリティ機能を担う役割（担当）	管理職	CISO/CRO.CIO 等		■	■	■	■	■		■	■			■
		サイバーセキュリティ統括（室等）	■	■	■	■		■	■	■	■	■	■	
		システム部門責任者		■		■	■	■			■	■	■	
		システム管理者	■	■		■		■			■	■	■	
		ネットワーク管理者	■	■		■		■			■	■	■	
		CSIRT 責任者	■	■		■		■	■	■		■	■	
	セキュリティ担当職	サイバーセキュリティ事件・事故担当	■	■	■	■		■	■	■		■	■	
		セキュリティ設計担当	■	■	■	■	■	■	■	■	■		■	
		構築系サイバーセキュリティ担当	■	■	■	■		■		■		■	■	
		運用系サイバーセキュリティ担当	■	■		■			■		■	■	■	
		CSIRT 担当	■	■	■	■		■	■		■	■	■	■
		SOC 担当	■	■		■			■		■		■	
		ISMS 担当	■	■		■		■			■	■	■	
	担当職	システム企画担当		■	■	■	■	■	■	■	■	■	■	
		基幹システム構築担当	■	■		■	■	■			■	■	■	
		基幹システム運用担当	■	■		■	■	■			■	■	■	
		WEB サービス担当		■	■		■		■	■	■	■	■	
		業務アプリケーション担当		■	■		■		■	■	■	■	■	
		インフラ担当		■	■		■		■	■	■	■	■	
		サーバ担当		■	■		■		■	■	■	■	■	
		DB 担当		■	■		■		■	■	■	■	■	

カテゴリ		役割(担当)	適応力・態度(■＝チームワークや作業遂行に必要)											
			問題発見力	問題分析力	仮説設定力	論理思考力	概念化力	俯瞰力	深耕力	革新力	継続力	相手の考えを理解する力	自分の考えを伝える力	共感を呼ぶ力
	担当職	ネットワーク担当		■	■		■		■	■	■	■	■	
		サポート・教育担当		■	■		■	■		■	■	■	■	■
		ヘルプデスク担当		■	■	■			■	■	■	■	■	■
情報システム部門以外のセキュリティ担当職	監査・個人情報保護	監査責任者	■	■		■		■			■	■	■	
		監査担当	■	■		■		■	■		■	■	■	
		特定個人情報取扱責任者	■	■		■		■			■	■	■	
		特定個人情報取扱担当	■	■		■			■		■	■	■	
		個人情報取扱責任者	■	■		■		■			■	■	■	
		個人情報取扱担当	■	■		■			■		■	■	■	

② 産業横断検討会（第 2 期中間報告書）によるエキスパート人材（セキュリティ統括人材）の定義

[文献 2]は産業横断検討会による第二期検討の中間報告を示したものであるが、この中で①に示した人材リファレンスの見直しが行われている。具体的にはユーザ企業において内部的に育成すべき人材キャリアとして、「エキスパート人材」を定義するとともに、セキュリティ統括（室等）に所属するべき人材ではないかという仮説が設定されている。セキュリティ統括（室等）に所属することから、エキスパート人材と呼ぶ代わりに「セキュリティ統括人材」と呼ぶことも検討されている。[文献 2]において、エキスパート人材は次のように定義されている。

- セキュリティを行うべき対象があるところで、対策責任を担った部署に必要。
- 対象システムに必要なセキュリティ対策を設計する役割を担う。

サイバーセキュリティ対策として必要なタスクをもとに整理された①の人材定義リファレスにおける 30 種類の役割のうち、このエキスパート人材が担うべき役割と最も重なるものは何かを産業横断検討会にて検討した結果をもとに、「セキュリティ設計担当」がエキスパート人材のモデルの中心になるものと仮定されている。

③ 鎌田による、サイバーセキュリティに関する危機管理体制を担う３層の役割

[文献 4]では、サイバーセキュリティマネジメントにおける経営層・管理層・技術層の役割として、平常時・非常時それぞれ次表に示すような内容を担う必要があることが示されている。このうち管理層については、『現場と経営層の間に立って、経営層への適切な報告のほか、リソース獲得のための努力、現時点の認識の報告や現状の説明、セキュリティ啓発活動といった、経営層に向けた仕事を背負う責任ある立場となる。それらに加え、現場のセキュリティ運用の管理やリスク管理をしながら、セキュリティ対策の実装などの企画もこなしていく、サイバーセキュリティマネジメントの中核をなす、組織にとっての司令塔であり参謀』（[文献 4]より引用）として重要な役割に位置付けられている。

表 5　経営層・管理層・技術層の、平常時・非常時それぞれの役割（[文献 4]より引用）

モデル	平常時	非常時
経営層	・リスクの認識 ・リスクの決定と優先順位づけ ・リソースの割当	組織としての意思決定
管理層 （企画）	・ガバナンス（PPP、PPT） ・コンプライアンス ・リスク管理 ・演習や訓練の実施 ・経営層への報告 ・現場との連携	インシデント対応の司令塔 （トリアージ）
技術層 （現場・運用）	・インフラの保護（監視／検知） ・リスク管理策の実行	インシデント対応の技術的対応・現場対応

注）PPP=Policy, Process, Procedure、PPT=Policy, Process, Technology

④ NIST によるサイバーセキュリティ人材の役割定義

[文献 14]は、米国政府機関向けを含むサイバーセキュリティ専門家の育成・活用、サイバーセキュリティの国民意識の向上、教育機関におけるサイバーセキュリティ教育の推進などを目指して策定された、サイバーセキュリティ人材に関するフレームワークである。同文献は 2011 年に策定された初版に基づく政府機関等における実践結果を踏まえ、タスクやスキルに関する定義範囲を拡大した上で新たに公表されたものである。全体で 52 種類の役割が定義されているが、米国ではこれらの役割をジョブディスクリプションとして人材の採用・育成・キャリアパス形成等に活用されており、日本の企業等におけるジョブローテーションとは異なる意味合いを持つことに留意する必要がある。

「Oversee and Govern（監督・統制）」領域における役割として同文献に示されている 14 種類の役割の一覧を次表に示す。このうち②③の文献で定義している「エキスパート（セキュリティ統括）人材」や「管理層」を担う人材に相当する役割としては、「Program Manager（事業計画マネージャー）」が近いものと考えられる。

表 6　「Oversee and Govern（監督・統制）」領域における役割一覧（[文献 14]を和訳）

分類	役割名	定義
Legal Advice and Advocacy 法的助言・弁護	Cyber Legal Advisor サイバーリーガルアドバイザー	サイバー法に関するトピックについて、法的な助言や勧告を行う。
	Privacy Officer/Compliance Manager プライバシーオフィサー/コンプライアンス管理者	プライバシーコンプライアンスプログラムとプライバシープログラムスタッフを開発、監督し、プライバシーコンプライアンス、ガバナンス/ポリシー、プライバシーとセキュリティの役員とそのチームのインシデント対応のニーズを支援する。
Training, Education, and Awareness 訓練・教育・啓発	Cyber Instructional Curriculum Developer サイバー教育カリキュラム開発者	教育上の必要に基づき、サイバーセキュリティを対象とする訓練・教育に関するコース、手法及び技術について開発、立案、調整及び評価する。
	Cyber Instructor サイバーセキュリティインストラクター	サイバーセキュリティ領域における要員の訓練または教育を開発及び主導する。

分類	役割名	定義
Cybersecurity Management サイバーセキュリティマネジメント	Information Systems Security Manager 情報システムセキュリティ管理者	プログラム、組織、システム等におけるサイバーセキュリティ対策に責任を負う。
	Communication Security (COMSEC) Manager 通信セキュリティ管理者	組織の通信リソースまたは暗号鍵管理システムの鍵を管理する。
Strategic Planning and Policy 戦略立案と方針	Cyber Workforce Developer and Manager サイバーセキュリティ要員の育成者・管理者	サイバー空間の人材、人材、訓練、教育の要件をサポートし、サイバー関連のポリシー、原則、教材、編成、教育訓練の要件に対する変化を扱うためのサイバー空間を対象とする労働力の計画、戦略、指針を開発する。
	Cyber Policy and Strategy Planner サイバーセキュリティ対策方針・戦略の立案者	組織のサイバーセキュリティに関するイニシアチブおよび規制遵守をサポートし、それと整合するようなサイバーセキュリティ計画、戦略、およびポリシーを策定し維持する。
Executive Cyber Leadership 幹部によるサイバーリーダーシップ	Executive Cyber Leadership 幹部によるサイバーリーダーシップ	組織のサイバーおよびサイバー関連の資源及び/又は運用に関する意思決定を行うとともに、ビジョンと方向性を確立する。
Program/Project Management and Acquisition 事業計画/プロジェクトの管理と調達	Program Manager 事業計画マネージャー	プログラムの主導、調整、コミュニケーション、統合を担い、全体の責任を負う。機関や企業における優先度との整合性を確保する。
	IT Project Manager IT プロジェクトマネージャー	情報技術関連プロジェクトを直接管理する。
	Product Support Manager 製品サポートマネージャー	システムと構成要素の準備と運用上の機能を整備し維持するために必要なサポート機能のパッケージを管理する。
	IT Investment/Portfolio Manager IT 投資/ポートフォリオ管理者	ミッションと企業の優先度に関する全体的なニーズに合わせた IT 投資のポートフォリオを管理する。
	IT Program Auditor IT プログラム監査者	標準への準拠状況を判断するため、IT プログラムまたはその個々の構成要素を評価する。

⑤ NCA による CSIRT 役割定義

[文献 3]において示されている、組織が保有すべき CSIRT の役割として定義されている内容は次の通りである。

表 7　NCA による CSIRT の役割（[文献 3]より引用）

分類	役割名称	業務内容
情報共有	PoC	社外窓口として、JPCERT/CC、NISC、警察、監督官庁、NCA、他 CSIRT 等との連絡窓口となり、情報連携を行う。社内窓口として、IT 部門、法務、渉外、IT 部門、広報、各事業部等との連絡窓口となり、情報連携を行う。
	リーガルアドバイザー	情報技術やサイバーセキュリティなどにおける法課題やコンプライアンス問題が発生した時に法的アドバイスを行う。法務部が IT スキルに乏しい場合には IT 担当が法務部向けに翻訳して橋渡しする形でもよい。
	ノーティフィケーション担当	自組織内を調整し、各関連部署への情報発信を行う。自組織システムに影響を及ぼす場合には IT 部門と調整を行う。
情報収集・分析	リサーチャー	セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メディア情報などを収集し、キュレーターに引き渡す。単独機器の分析は行うが、相関的な分析はしない。
	キュレーター	リサーチャーの収集した情報を分析し、その情報を自組織に適用すべきかの選定を行う。リサーチャーと合わせて SOC（セキュリティオペレーションセンター）で実施することが多い。
	脆弱性診断士	OS、ネットワーク、ミドルウェア、アプリケーションが安全かどうかの検査を行い、診断結果の評価を行う。

分類	役割名称	業務内容
	セルフアセスメント担当	自組織環境や情報資産の現状分析を行う。平常時の際にアセスメントを実施しておき、インシデント発生時にはアセスメント結果に基づいて影響範囲を特定する。
	ソリューションアナリスト	自組織の事業計画に合わせてセキュリティ戦略を策定する。現在の状況とあるべき姿の Fit&Gap 分析からリスク評価を行い、ソリューションマップを作成して導入を推進する。導入されたソリューションの有効性を確認し、経営層と情報共有を行い、改善計画に反映する。
インシデント対応	コマンダー	自組織で起きているセキュリティインシデントの全体統制を行う。重大なインシデントに関しては CISO や経営層との情報連携を行う。また、CISO や経営者が意思決定する際の支援を行う。
	インシデントマネージャー	インシデントハンドラーに指示を出し、インシデントの対応状況を把握する。対応履歴を管理するとともにコマンダーへ状況を報告する。
	インシデントハンドラー	インシデントの処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。状況はインシデントマネージャーに報告する。
	インベスティゲーター	外部からの犯罪、内部犯罪を捜査する。セキュリティインシデントはシステム障害とは異なり、悪意のある者が存在する。通常の犯罪捜査と同様に、動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に捜査対象を絞っていくことが要求される。
	トリアージ担当	発生している事象に対して優先順位を決定する。被害がある場合の復旧優先順位や、拡散している場合にはどのシステムから停止していくべきか等の判断を行う。
	フォレンジック担当	システム的な鑑識、精密検査、解析、報告を行う。悪意のある者は証拠隠滅を図ることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求される。
自組織内教育	教育担当	主に役職員向けの教育を実施し、リテラシーの向上を図る。CSIRT 向けの専門トレーニングについては別担当にしてもよい。

⑥ JNSA のセキュリティ知識分野（SecBoK）2017 における役割定義

[文献 7]において定義されているサイバーセキュリティに関する 16 種類の役割のうち、CSIRT 業務に関するものは表 7 と整合性を確保している。それ以外の役割は次の通りである。

表 8　SecBoK 2017 における役割定義（[文献 7]より引用）

役割（ロール）	役割定義（ユーザ企業におけるおもな役割）	セキュリティベンダ職種
CISO（最高情報セキュリティ責任者）	社内の情報セキュリティを統括する。セキュリティ確保の観点から、CIO（最高情報セキュリティ責任者）、CFO（最高財務責任者）と必要に応じて対峙する。	（外部委託しないことを前提とする）
IT企画部門	社内のIT利用に関する企画・立案を行う。必要に応じて、ITの利用状況の調査・分析等を行う。	コンサルタント
IT システム部門	社内のITプロジェクトを推進するとともに、アプリケーションシステムの設計、構築、運用、保守等を担当する。	ネットワークアナリスト
情報セキュリティ監査人	情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、もって保証を与えあるいは助言を行う。	情報セキュリティ監査人

⑦ IPA の ITSS＋（セキュリティ領域）にて定義されている専門分野

[文献 6]において定義されているサイバーセキュリティに関する 13 種類の専門分野一覧は次の通りである。これらは平成 29 年度から IPA にて運用を開始したサイバーセキュリティ分野を対象とする専門資格である情報処理安全確保支援士（登録セキスペ）の登録者の活躍分野としての利用が想定されている。

表 9　ITSS+（セキュリティ領域）の専門分野一覧（[文献 6]より引用）

専門分野	説明
情報リスクストラテジ	自組織または受託先における業務遂行の妨げとなる情報リスクを認識し、その影響を抑制するための、組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定等を推進する。自組織または受託先内の情報セキュリティ対策関連業務全体を俯瞰し、アウトソース等を含むリソース配分の判断・決定を行う。
情報セキュリティデザイン	「セキュリティバイデザイン」の観点から情報システムのセキュリティを担保するためのアーキテクチャやポリシーの設計を行うとともに、これを実現するために必要な組織、ルール、プロセス等の整備・構築を支援する。
セキュア開発管理	情報システムや製品に関するリスク対応の観点に基づき、機能安全を含む情報セキュリティの側面から、企画・開発・製造・保守などにわたる情報セキュリティライフサイクルを統括し、対策の実施に関する責任をもつ。
脆弱性診断	ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行い、診断結果の評価を行う。
情報セキュリティアドミニストレーション	組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むとともに、対策の立案や実施（指示・統括）、その見直し等を通じて、自組織または受託先における情報セキュリティ対策の具体化や実施を統括する。また、利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する。
情報セキュリティアナリシス	情報セキュリティ対策の現状に関するアセスメントを実施し、あるべき姿とのギャップ分析をもとにリスクを評価した上で、自組織または受託先の事業計画に合わせて導入すべきソリューションを検討する。導入されたソリューションの有効性を確認し、改善計画に反映する。
CSIRT キュレーション	情報セキュリティインシデントへの対策検討を目的として、セキュリティイベント、脅威や脆弱性情報、攻撃者のプロファイル、国際情勢、メディア動向等に関する情報を収集し、自組織または受託先に適用すべきかの選定を行う。
CSIRT リエゾン	自組織外の関係機関、自組織内の法務、渉外、IT 部門、広報、各事業部等との連絡窓口となり、情報セキュリティインシデントに係る情報連携及び情報発信を行う。必要に応じて IT 部門と CSIRT の間での調整の役割を担う。
CSIRT コマンド	自組織で起きている情報セキュリティインシデントの全体統制を行うとともに、事象に対する対応における優先順位を決定する。重大なインシデントに関しては CISO や経営層との情報連携を行う。また、CISO や経営者が意思決定する際の支援を行う。
インシデントハンドリング	自組織または受託先におけるセキュリティインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携する。情報セキュリティインシデントへの対応状況を管理し、CSIRT コマンドのタスクを担当する者へ報告する。
デジタルフォレンジクス	悪意をもつ者による情報システムやネットワークを対象とした活動の証拠保全を行うとともに、消されたデータを復元したり、痕跡を追跡したりするためのシステム的な鑑識、精密検査、解析、報告を行う。
情報セキュリティインベスティゲーション	情報セキュリティインシデントを対象として、外部からの犯罪、内部犯罪を捜査する。犯罪行為に関する動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に捜査対象の絞り込みを行う。
情報セキュリティ監査	情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、もって保証を与えあるいは助言を行う。

⑧ 人生 100 年時代構想会議中間報告におけるリカレント教育の提唱

[文献 5]では、『これまでのような、高校・大学まで教育を受け、新卒で会社に入り、定年で引退して現役を終え、老後の暮らしを送るという単線型の人生を送るのではなく、個々人が人生を再設計し、一人一人のライフスタイルに応じたキャリア選択を行い、新たなステージで求められる能力・スキルを身につける機会が提供されることが重要である』との指摘を通じてリカレント教育の重要性を提唱している。この一環として、社会人の学び直し向け教育の一環として、サイバーセキュリティ人材育成に関する教育機会の提供が期待される。

調査結果からの考察

①～④の文献より、企業内のサイバーセキュリティに関する各層の役割・人材像について、次のことが考察される。

- 本調査の実施と並行して、平成 29 年度後半頃より国内でも企業のビジネス戦略に応じたサイバーセキュリティ対策を担う役割（２．１における「戦略マネジメント機能」に相当）の必要性が指摘されるようになりつつあるが、具体的な役割や人材像は明確になっていない。
- これに対して米国では、④の NICE サイバーセキュリティ人材フレームワークにおいて政府機関・企業を横断するものとしてこうした役割がジョブディスクリプションとして定義されるだけでなく、そうした役割を担うために必要となる知識・スキル・能力もあわせて明確化されているなど、先行して整備が進んでいる。
- 一方、２．１において「システム担当」「システム構築・運用担当」としてサイバーセキュリティ対策を担うエンジニアに相当する役割については、日本国内でも SecBoK や ITSS＋などで役割や専門分野として多くの種類が定義されており、米国との比較においても見劣りするものではない。ただし、日本においては IT 人材がベンダに偏在することが以前から指摘されており、ユーザ企業においてこうした「システム担当」や「システム構築・運用担当」に相当する役割の多くが外部委託されていることに留意する必要がある。

（３）必要とされる知識・スキル

調査対象文献においてサイバーセキュリティ対策を実施するために必要な知識・スキルに関して言及されている内容について、２．１の分類における「戦略マネジメント機能」に求められるものを中心に概要を以下に示す。

① 産業横断検討会による、「エキスパート（セキュリティ統括）人材」や「セキュリティ設計担当」が持つべき／育成すべき能力

[文献 2]において、エキスパート（セキュリティ統括）人材に必要な能力については、中間報告とりまとめの段階で明確に洗い出せておらず、検討を続けている状況にあることが報告されている。この中で、特にエキスパート人材に必要な能力として、“リスクセンス”が挙げられている。これは、『何かの脅威に対応しなければならない場合、完璧な情報がそろっていない状況で、事業へのインパクト、脅威への対抗手段の選択、必要なコスト・リソースなどの様々な要因を勘案し、限られた時間の中で判断し対応していく』ための対応能力として定義されている。

一方、人材定義リファレンスで定義される 30 種類の役割のうち、エキスパート（セキュリティ統括）人材と重なる要素の多い「セキュリティ設計担当」が持つべき能力／育成すべき能力として、下表が挙げられている。

表 10　セキュリティ人材育成の考え（[文献 2]より引用）

能力		具体的な例	育成に必要な条件
個人の行動力	適応力・態度	リスクセンス・コミュニケーション	環境により醸成されるもの
	プロフェッショナルスキル	人材定義リファレス:機能（業務区分）	自主的に学習可能なもの
	知識	人材定義リファレス:機能（要求区分）	
	経験	キャリアパスやこれまでの業務経験（人生経験）	環境によって醸成されるもの
	倫理観・信条等	仕事に対するスタンス	
プロジェクト管理能力	活動	人材定義リファレス:機能に対する「実際の業務」	学習と環境の両面から育成されるもの
	プロジェクト管理	業務の優先順位付けや、達成基準の設定と評価	

② 鎌田による、サイバーセキュリティ対策を担う人材に必要な能力

[文献 4]において、鎌田は管理系人材に求められるスキルとして、『米国におけるサイバーセキュリティ人材の教育カリキュラムをみると、最近ではクリティカルシンキング（批判的思考）、情報の取捨選択方法、的確なレポーティング能力、問題解決能力など、いわゆるビジネススキルの基礎といわれるようなものの説明に結構な時間が割かれているようである。これらは実は組織経営における意思決定のトレーニングで行われるようなコンテンツに酷似しており、サイバーセキュリティのマネジメント人材に求められる素質は経営人材に求められる素質と極めて近いことがわかっている。』とした上で、国内での経験をもとに、管理系人材にとって重要なヒューマンスキルとして次表の内容を挙げている。

表 11　管理系人材にとって重要なヒューマンスキル（[文献 4]をもとに編集）

スキルの種類	求められる内容
対人能力	● 各種セキュリティ関係の取組みを円滑に進めるために、効果的なコミュニケーションができることが必要 ● 通知文やポリシーの策定などの文書作成にあたることもあるため、執筆能力も重要。
組織内調整力	● サイバー攻撃対応は一部門のみで対応する問題ではなく、組織内の各部門が横断的に対応する必要性がある。サービスを担当する業務部門、広報部門、法務部門等、多数にわたる部門との調整力が求められる。
構造化能力	● サイバーセキュリティの仕事においては、さまざまな情報を何らかの意味のある軸でとらえて、全体と部分の関係を明らかにし、全体の中で抜け・漏れがないように考える能力が重要となる。構造的、網羅的に対策を考え、状況を俯瞰的に見て進める能力がなければ、本来守るべきものが疎かになってしまう。
抽象化能力	● 技術的・専門的な内容を理解するための十分な知識を持たない人に対して、「間違っていない」範囲で抽象的に説明することが必要となる。特に経営層とのやりとりにおいては、うまく要点のみをとらえて抽象的に物事を説明することが重要になる。

一方技術系人材については、すべての人材の必要な観点として、サイバーセキュリティを理解するために必要な IT に関する「知識」と実際に手を動かす「経験」、上級レベルの人材に求められる観点として、これらに加えて、高度な専門性を培うのに欠かせない「やる気」と、多様な観点から物事を分析したり、重要なポイントをとらえる「センス」がそれぞれ挙げられている。

③ ロバート・L・カッツの提唱する、管理職に求められる能力

①②の調査結果より、管理系人材に求められる能力と共通要素が多いと見込まれることから、ここではこうした人材のスキル分析に関する古典として知られるロバート・L・カッツの著作（[文献 15]）について調査した。同文献において、カッツは管理者像として（a）他人の行動を指揮し、（b）こうしたことに力を入れることを通じて、特定の目標を達成する責任を負うこととし、これを実現するための能力として、「テクニカル・スキル」（業務遂行能力）、「ヒューマン・スキル」（対人関係能力）、「コンセプチュアル・スキル」（概念化能力）の 3 種類を示している。この学説を紹介する[文献 9]では、3 種類のスキルはそれぞれ次表のように整理されている。

表 12　管理者に求められる能力（[文献 9]を参考に作成）

スキル名	定義	相対的な重要性
コンセプチュアル・スキル	企業を総合的にとらえることができる能力のこと。組織の諸機能がいかに相互に依存しあっているか、またその内のどれか1つが変化したとき、どのように全体の機能に影響が及ぶかを認識することであり、個別の事業が産業、地域社会、さらには国全体の政治的、社会的、経済的な力とどのように関係しているかを明確に描けることにまで及ぶ。	最上階層において特に重要
ヒューマン・スキル	グループの一員として手際よく仕事を行い、自分の率いるチーム内で力を合わせて努力する場を作り上げることや、グループ間で関係を構築すること。他人との対応能力であるヒューマン・スキルは、どの階層においても効果的管理を行うための基本となるもの。	すべての階層において重要
テクニカル・スキル	特定の活動、特に手法、プロセス、手順、あるいはテクニックと関わり合う活動を理解し、それに熟達していること。	下位階層において特に重要

カッツは同文献において、次図のように上位階層の管理者ほど「コンセプチュアル・スキル」が占める割合が高まることを示している。

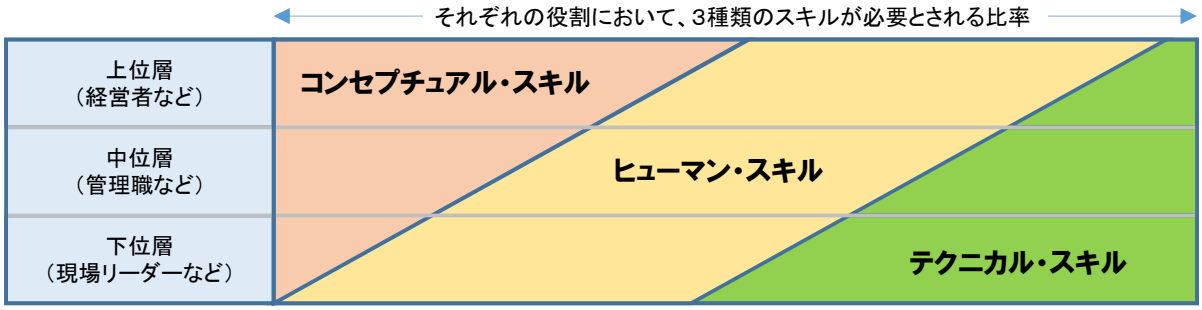

図 4　管理者としての階層に応じて求められるスキルの相違（[文献 15]をもとに作成）

なお、[文献 15]ではカッツが 1955 年に最初の論考を発表してから約 20 年後のコメントとして、コンセプチュアル・スキルについて、『いまではこの思考方法がどの程度オン・ザ・ジョブで育成され得るか、これまでほど楽観的にはなれなくなっている。人生の初期にこの思考方法を学ばない限り、経営者の地位に到達するに当たって、大きな変化を起こすことを期待することは非現実的である。ジョブ・ローテーション、特別な部門をまたがる任務、ケース問題との取組みは事前に育成済みのコンセプチュアル・スキルを高める機会であることは確かである。しかし、青年期を過ぎた人が、この思考方法をどの程度身につけることができるかについては疑問に思っている。したがって、この意味で、コンセプチュアル・スキルは生得の能力と見るべきものであるかもしれない。』として、管理職になってからの能力の習得の可能性については限界があることを示唆している。

④ NIST による NICE サイバーセキュリティ人材フレームワークを構成するタスクと知識・スキル・能力に関するリスト

[文献 14]では、米国の政府機関をはじめとする組織においてサイバーセキュリティ関連業務に従事する人材が担うタスクと、それらのタスクを遂行する上で求められる知識・スキル・能力の一覧をそれぞれリストとして提示した上で、表 6 に抜粋を示した 52 種類の役割におけるタスクと知識・スキル・能力との対応関係を個別に示している。このうち「Program Manager（事業計画マネージャー)」に求められる知識・スキルを抜粋したものを次ページ表に示す。

なお、⑤にて示すように本文献にて示される知識・スキル・能力の一覧を日本国内におけるサイバーセキュリティ関連業務に必要な知識やスキルと比較すると、一部が不足することが JNSA における検討を通じて明らかになっており、日本国内での活用にあたっては留意が必要である。

表 13　役割「事業計画マネージャー」に求められる知識・スキル（[文献 14]をもとに作成）

役割名	事業計画マネージャー Program Manager		カテゴリ	監督・統制
			専門領域	調達及び事業計画／プロジェクトの管理
定義	事業計画の主導、調整、コミュニケーション、統合を担い、全体の責任を負う。機関や企業における優先度との整合性を確保する。			
必要な知識・スキル（抜粋）	IT 系	• コンピュータネットワークのコンセプトとプロトコル、及びネットワークセキュリティ手法に関する知識 • サイバーセキュリティとプライバシーの原理に関する知識 • サイバー脅威と脆弱性に関する知識 • 情報技術のアーキテクチャコンセプトとフレームワークに関する知識 • ソフトウェアのセキュリティとユーザビリティを含む、システムライフサイクルマネジメントの原理に関する知識 • セキュリティ、ガバナンス、調達及び管理に関するクラウドベースのナレッジマネジメント技術とコンセプトに関する知識		
	ビジネス系	• リスクマネジメントプロセスに関する知識、リスクマネジメントフレームワークの要件に関する知識 • サイバーセキュリティの失効がもたらす運用上のインパクトの特定に関する知識 • リソースマネジメントの原理と技法に関する知識 • 組織のエンタープライズ IT のゴールと目的に関する知識 • サプライチェーンのリスクマネジメントに関する実践（NIST SP 800-161）に関する知識 • 組織のコアビジネスとミッションのプロセスに関する知識 • IT 調達要件に関する知識 • システムの目標に関して、システムパフォーマンスの手段や指標、及びパフォーマンスの向上または是正に必要となるアクションの特定に関するスキル • 連携先を含む企業全体にわたって情報に関するニーズとインテリジェンスの収集要件を解釈、追跡及び優先順位づけるスキル • サプライチェーンのリスクマネジメント標準の適用に関する能力 • 開発を監督し、ライフサイクルコストの見積を更新する能力 • 供給者及び/又は製品の信頼性を評価/確保する能力 • 調達プロセスを通じてセキュリティが確実に実践されるようにする能力		
	社会系 人間系	• サイバーセキュリティとプライバシーに関連する、法律、規制、方針及び倫理に関する知識 • 暗号及びその他のセキュリティ技術に関する輸出入規制に関する知識		

⑤ IPA による新たなスキル標準 ITSS＋（セキュリティ領域）

[文献 6]では、IT 人材を対象とする表 9 に示した 13 種類の専門分野ごとに、それぞれの専門分野に相当する業務を遂行する上で想定されるタスクや、習得しておくと望ましいスキルについて、IPA が公表している i コンピテンシディクショナリ（iCD）のタスクリスト、スキルリストをベースに明示している。このうち、専門分野「情報リスクストラテジ」に求められる知識・スキルを抜粋したものを次表に示す。

表 14　専門分野「情報リスクストラテジ」に求められる知識・スキル（[文献 6]をもとに作成）

<table>
<tr><td>専門分野名</td><td colspan="2">情報リスクストラテジ</td><td>想定業務</td><td>経営課題</td></tr>
<tr><td></td><td colspan="2"></td><td>レベル範囲</td><td>レベル4～7</td></tr>
<tr><td>定義</td><td colspan="4">自組織または受託先における業務遂行の妨げとなる情報リスクを認識し、その影響を抑制するための、組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定等を推進する。自組織または受託先内の情報セキュリティ対策関連業務全体を俯瞰し、アウトソース等を含むリソース配分の判断・決定を行う。</td></tr>
<tr><td rowspan="3">必要な知識・スキル（抜粋）</td><td>IT 系</td><td colspan="3">• セキュリティの基礎技術（情報保証、セキュリティアーキテクチャ、プラットフォームセキュリティ、暗号技術、保証・信用・信頼のメカニズム）に関する知識・スキル
• セキュリティの構築技術（方針・基準・計画の策定、要件定義、情報セキュリティ管理、情報セキュリティ分析、セキュリティの見直し）に関する知識・スキル
• システム企画立案手法、ソリューション提案手法に関する知識・スキル
• ソフトウェアエンジニアリング手法（セキュリティ実装、セキュリティ品質）に関する知識・スキル
• サポートセンター基盤技術（インシデント管理システム等）に関する知識・スキル</td></tr>
<tr><td>ビジネス系</td><td colspan="3">• 市場機会の評価と選定（ビジネス環境分析、経営管理システム、経営戦略手法）に関する知識・スキル
• システム戦略立案手法（システム活用推進・評価、業務プロセス、事業戦略・分析、情報システム戦略）に関する知識・スキル
• コンサルティング手法に関する知識・スキル
• 業務動向把握手法に関する知識・スキル
• リスクマネジメント手法に関する知識・スキル
• IT ガバナンス、内部統制に関する知識・スキル
• 事業継続計画（BCP 策定、災害対策管理）に関する知識・スキル
• チェンジマネジメント手法（協働の管理、ビジネスソリューション変更管理、業界固有の要件・事例）に関する知識・スキル
• システムアーキテクティング技術（システム要件定義、障害時運用方式、災害対策）に関する知識・スキル
• ビジネスインダストリ（エンジニアリングシステム、ビジネスシステム、産業機器、民生機器）に関する知識・スキル
• 企業活動（経営・組織論、会計・財務、情報セキュリティ監査、ビジネスプロセスマネジメント）に関する知識・スキル
• 標準化に関する知識・スキル</td></tr>
<tr><td>社会系人間系</td><td colspan="3">• 技術者の社会的責任と倫理に関する知識
• 情報倫理に関する知識
• セキュリティ関連法規及びその他の法律・ガイドライン・技術者倫理に関する知識・スキル</td></tr>
</table>

⑥ JNSA によるセキュリティ知識分野（SecBoK）人材スキルマップ

[文献 7]において示されているスキルマップでは、表 7 及び表 8 に示した 16 種類の役割について、NICE サイバーセキュリティ人材フレームワークで示される知識・スキル・能力のリストの項目の和訳との対応関係を示している。ただし、本文献で用いているフレームワークは、③として改訂される前の内容に基づいていることに留意する必要がある。また、JNSA において、NICE サイバーセキュリティ人材フレームワークを日本国内におけるサイバーセキュリティ関連業務に必要と考えられる内容と比較した結果、次に例示する内容について不足することがわかり、SecBoK の知識・スキル項目として追加されている。

- システム開発のコンセプトに関するスキル
- システム運用のコンセプトに関するスキル
- ITSS レベル 2 程度の基礎的な IT リテラシー
- 情報を適切に判断する能力
- 英語で書かれた文書を正確に読解する能力
- 英語で書かれた文書を素早く読解する能力
- メディアリテラシー（すべての情報をうのみにしてはいけないという批判的視点など）
- 各メディアの特性に関する知識（情報発信の素早さ、正確さ、スタンス、信ぴょう性など）
- レポーティングスキル（難しい内容を、読み手に合わせて書き砕く能力）
- 国家間の関係に関する知識（歴史、政治、地理、経済、軍事、文化、宗教など）
- 尋問に関するコミュニケーション能力と知識
- 捜査(不正かどうかの判断、業務時間外の行動調査、借金などの収支状況調査)に関する能力
- 自社のセキュリティポリシー、規則、実施方法等に関する知識
- 自社の実施するセキュリティ対策、セキュリティ技術に関する知識
- 脆弱性診断に関する基礎知識
- 日本国のサイバーセキュリティに関わる刑法、民法および自社における人事、コンプライアンス、セキュリティポリシーなど各種規程に関する知識

⑦ (ISC)² が定める CISSP 共通知識分野

[文献 16]は、(ISC)² が CISSP（Certified Information Systems Security Professional）資格制度のための認定試験の作成に資することを目的として、情報セキュリティ分野の専門家が理解すべき知識を国際規模で収集し、職務の軸（ドメイン）別に体系的にまとめた CBK（Common Body of Knowledge）である。このうち、各ドメインに盛り込まれている知識に関するキーワードを次ページ表に示す。CBK は世界各国の専門家へのヒアリング調査を通じて、毎年内容が更新されている。

表 15　CISSP8 ドメインごとのキーワード（[文献 16]より引用）

ドメイン	キーワード
1. セキュリティとリスクマネジメント	• 機密性、完全性および可用性の概念の理解と適用 • セキュリティガバナンスの原則の適用 • コンプライアンス • グローバルなコンテキストにおける情報セキュリティに関連する法規制の問題の理解 • 職業倫理の理解 • 文書化されたセキュリティポリシー、スタンダード、プロシージャ、およびガイドラインの策定と実施 • 事業継続要件の理解 • 人的セキュリティポリシーへの貢献 • リスクマネジメントの概念の理解と適用 • 脅威のモデリングの理解と適用 • セキュリティリスク考慮事項と取得戦略および実践への統合 • セキュリティ教育・訓練・意識啓発の確立と管理
2. 資産のセキュリティ	• 情報分類および資産サポート • 所有権の決定・維持 • プライバシー保護 • 適切な保持の確認 • データセキュリティ制御の決定 • 処理要件の確立
3. セキュリティエンジニアリング	• セキュリティ設計原則を使用したエンジニアリングライフサイクルの実装および管理 • セキュリティモデルの基本的概念の理解 • 情報システムセキュリティ基準に基づく制御と対策の選択 • 情報システムのセキュリティ機能の理解 • セキュリティのアーキテクチャ、設計、およびソリューションの要素における脆弱性の評価と軽減 • ウェブベースシステムにおける脆弱性の評価と軽減 • モバイルシステムにおける脆弱性の評価と軽減 • 組込みデバイスおよびサイバーフィジカルシステムにおける脆弱性の評価と軽減 • 暗号の適用 • 施設と設備の設計に対するセキュアな原則の適用 • 施設のセキュリティの設計と実装
4. 通信とネットワークセキュリティ	• セキュアな設計原理をネットワークアーキテクチャに適用する • ネットワークコンポーネントのセキュリティ保護 • セキュアな通信チャネルの設計・確立 • ネットワーク攻撃の防止または軽減
5. アイデンティティとアクセスの管理	• 資産への物理的および論理的なアクセスの制御 • 人及びデバイスの識別と認証の管理 • サービスとしてのアイデンティティ（IDaaS）の統合 • サードパーティのアイデンティティサービスの統合 • 認可メカニズムの実装と管理 • アクセス制御攻撃の防止または軽減 • アイデンティティおよびアクセスのプロビジョニングにおけるライフサイクルの管理

ドメイン	キーワード
6. セキュリティの評価とテスト	• 評価・テスト戦略の設計および検証 • セキュリティ制御テストの実施 • セキュリティプロセスデータの収集 • 内部監査および第三者監査の実施または促進
7. セキュリティの運用	• 調査の理解、サポート • 調査タイプごとの要件の理解 • ログ記録と監視活動の実施 • 構成管理によるリソースのプロビジョニングの確保 • 基本的なセキュリティ運用概念の理解、適用 • リソース保護技術の採用 • インシデント対応の実施 • 予防措置の運用および維持 • パッチおよび脆弱性管理の実装とサポート • 変更管理プロセスへの関与と理解 • 復旧戦略の実装 • 災害復旧プロセスの実装 • 災害復旧計画のテスト • 事業継続計画の演習への参加 • 物理的セキュリティの実装と管理 • 従業員の安全への関与
8. ソフトウェア開発セキュリティ	• ソフトウェア開発ライフサイクル（SDLC）におけるセキュリティの理解と応用 • 開発環境におけるセキュリティ管理策の実行 • ソフトウェア保護の有効性の評価 • ソフトウェア調達上のセキュリティの評価

調査結果からの考察

①～⑥の文献より、必要とされる知識・スキルについて、次のことが考察される。

- 「戦略マネジメント機能」に求められるスキル・能力は、管理系セキュリティ人材に求められる能力と概ね共通し、次のようなものと想定される。
  - 対人能力（ヒューマンスキル）
  - 組織内調整力（ヒューマンスキル）
  - 構造化能力（コンセプチュアルスキル）
  - 抽象化能力（コンセプチュアルスキル）
  - IT・サイバーセキュリティを理解するための基本的なテクニカルスキル
  - リスクセンス
- 一方、知識については国内を対象とする文献調査を通じて、「戦略マネジメント機能」に求められる知識は明らかになっていない。米国の NICE サイバーセキュリティ人材フレームワークにて類似の役割として示されている内容や、CISSP の CBK を参考に、次に挙げるような知識が必要と考えられる。
  - IT のアーキテクチャとフレームワーク
  - インターネットの仕組み、基盤技術及びサイバー空間のステークホルダー
  - 脅威と脆弱性
  - リスクマネジメント
  - 法律/制度/基準/セキュリティに関するフレームワーク
  - 委託先管理

（4）知識・スキルを習得するための、モデルとなるカリキュラム

① 情報セキュリティ大学院大学によるモデル・コア・カリキュラム

[文献 10]では、国内の高等教育機関において情報セキュリティを学んでいる人材の数、これまでに国内で実施された情報セキュリティ人材の育成プロジェクト、海外における情報セキュリティ人材の育成動向、産業界における高等教育機関での情報セキュリティ人材育成への期待等に関する調査結果をもとに、「情報セキュリティ分野の高度人材の育成」、「一般の技術者向けの情報セキュリティ関連知識の教育」、「情報セキュリティに関する一般向けのリテラシー教育」の 3 種類の人材のカテゴリについて、表 16 に示す合計 10 種類のモデル・コア・カリキュラムを作成している。このうち「一般の技術者向けの情報セキュリティ関連知識の教育」については、同様の趣旨で同文献の公表時期に実施された文部科学省による「成長分野を支える情報技術人材の育成拠点の形成」プロジェクト（enPiT、enPiT2）におけるセキュリティ分野での成果を踏まえた内容を活用している。

表 16　モデル・コア・カリキュラムの構成（[文献 10]より引用）

区分	例示ごとの定義	育成しようとする情報セキュリティ人材像	対象者（凡例参照）		
			専門人材	技術者	一般
区分1 学士課程4年間で卒業し社会に出ることを想定した区分	①一般教養としての情報セキュリティに関する講義を対象とするもの	日常の社会生活を営む上で必要なセキュリティに関する知識を備えた人材	○	○	◎
	②学士課程卒業後就職を予定している広く理工系に近い学生を対象とするもの	情報セキュリティに関する基礎的な知識を備えた人材（セキュリティ分野への就職は前提としない）	○	○	○
	③情報セキュリティを専門とする学科等を対象とするもの	情報セキュリティに関する基礎的な知識・経験と意識を備えた人材（セキュリティ分野への就職は前提としない）	○	○	△
区分2 学士課程4年間＋修士課程2年間の6年間の課程を経て社会に出ることを想定し、リテラシー教育が終了した学生（主に学部3年～修士1年）を想定した区分	④修士課程に進学予定の情報系学士課程の学生を対象とするもの	情報セキュリティを本格的に学ぶ上で必要となる基盤的知識を習得した人材	◎	○	－
	⑤情報セキュリティに関する単独の科目を対象とするもの	情報セキュリティに関する基本的な知識を備えた人材（セキュリティ分野への就職は前提としない）	△	○	○
	⑥専門とは別に情報セキュリティを学ぶコース等を対象とするもの	習得した知識・実践的経験を自らの専門分野のセキュリティ対策に活かせる人材	△	◎	－
	⑦情報セキュリティを専門とする専攻等を対象とするもの	情報セキュリティに関する専門的な知識と実践的な経験、及び意識を備えた人材（セキュリティの専門性をある程度発揮できる環境への就職等を想定）	◎	○	－
区分3 情報セキュリティに関して体系的に学び直したいと考える現役IT技術者（就職後10	⑧短期（2週間程度）集中コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	○	◎	○
	⑨中期（3～6ヶ月程度）コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	○	◎	△

区分	例示ごとの定義	育成しようとする情報セキュリティ人材像	対象者（凡例参照）		
			専門人材	技術者	一般
～15年程度（30代中～後半）の技術者）を想定した区分	⑩長期（1年程度）コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	◎	△	－

凡例：専門人材＝情報セキュリティ分野を専門とする人材、
技術者＝情報セキュリティを理解する技術者やマネージャ、一般＝一般の社会人
◎＝主たる育成対象、○＝育成対象、△＝条件により活用可能、－＝対象外

上表に示すモデル・コア・カリキュラムのうち、社会人学び直し向けのカリキュラムとして中期コースの例（例示⑨）を次表に示す。

表 17　モデル・コア・カリキュラム（例示⑨）（[文献 10]より引用）

社会人学び直し：中期（3～6ヶ月程度）コース向けモデル・コア・カリキュラム（例示⑨）		
想定する受講者	情報セキュリティの学び直しをしたい現役IT技術者（30代中～後半）	
受講者の知識・スキル	産業界で情報系業務に従事している技術者を想定する	
育成する人材像	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	
到達目標	下記の複数テーマに関する業務遂行に必要な知識を習得し、複合的な領域で構成される業務や脅威への対策に関する能力を得る。 （テーマ例） ・組織における標的型攻撃対策 ・ソフトウェアの設計・開発段階におけるセキュリティ対策 ・情報セキュリティマネジメントと情報セキュリティ監査 ・CSIRT運営 ・デジタルフォレンジック	
関連科目との関係	以下の領域のうち、当該コース内容を理解する上で必要なものについて基本的な知識を有することを前提とする（募集要項等で明示） ・コンピュータネットワーク（TCP/IP、無線LAN） ・コンピュータアーキテクチャ ・オペレーティングシステム（Windows及びUNIX系） ・プログラミング言語（C言語、アセンブラ）	
実施方法	講義及び演習	
科目	講義名・コマ数	解説
基礎講義1	セキュアシステム構成論・15コマ（各90分）	• 情報セキュリティ概論 • さまざまな事例から見るシステムの脆弱性 • 情報システムに到達する不正経路という視点で「セキュアな情報システムとは何か」について考察 • セキュリティポリシーという視点で、情報システム全体の構成要素について見ていくことで、セキュアなシステムをどのように構成するか整理する
基礎講義2	セキュアプログラミングとセキュアOS・15コマ（各90分）	• ソフトウェアの脆弱性 • 設計レベルの問題と実装レベルの問題 • バッファオーバーフロー攻撃の仕組みと防御策 • Webアプリケーションの脆弱性 • 隔離実行、サンドボックス

		• セキュアOSとアクセス制御
基礎講義3	ネットワークシステム設計・運用管理・15コマ（各90分）	• ネットワーク設計のための理論（待ち行列理論、トラヒック理論、グラフ理論、信頼性理論） • ネットワークサービス • VLANとVPN • 企業ネットワーク構築と運用管理の概要 • ネットワークセキュリティ対策技術 • 仮想ネットワーク技術とクラウド、SDN
基礎講義4	インターネットテクノロジ・15コマ（各90分）	• インターネットの生い立ちと発展の経緯、標準化 • ネットワークアーキテクチャ、ネットワークトポロジ、ネットワークの分類 • LAN技術（イーサネット、衝突制御、誤り制御、フロー制御） • 無線LAN、ダイヤルアップ接続 • IPアドレス、アドレス変換、アドレス解決、IPv4パケット • ルーティング • TCPとUDP、再送制御、輻輳制御 • DHCP、DNS、FTP • WWW、電子メール、P2Pファイル交換 • セキュリティプロトコル（IPsec、SSL） • 監視・管理（ICMP、SNMP） • IPv6（IPv6パケット、IPv4からの移行） • IP電話（SIP、音声品質） • QoS（Intserv、Diffserv、キューイング） • マルチキャスト
演習	CSIRT構築と運営	• CSIRT構築の手引き (2日間・8コマ・各90分) • ネットワークとWebセキュリティ技術演習 （3日間・12コマ・各90分） • デジタルフォレンジック演習（4日間・16コマ・各90分）
応用講義1	ハッキングとマルウェア・15コマ（各90分）	• 偵察とソーシャルエンジニアリング • スキャンと脆弱性識別 • システムハッキング • トロイの木馬，バックドア，ウィルス，ワーム • スニッファ • マルウェアの概要と作成 • マルウェア解析環境構築、マルウェア収集、表層解析 • アセンブラの基礎とプログラミング • バイナリファイルの構成 • 動的解析、静的解析、アンチ解析技術
応用講義2	組織行動と情報セキュリティ・15コマ（各90分）	• 組織の定義と組織行動論の枠組み • モチベーションと組織への貢献 • 組織コミットメントと組織の成果 • 集団のダイナミクス • リーダーシップの役割 • 組織文化の概念と機能、形成と変革 • 組織学習：不完全な組織学習をもたらす要因 • 意思決定のバイアス • 意思決定の課題と改善 • 危機管理組織のマネジメント • 企業事故・不正行動の事例研究 • 組織変革の立案と策定

② 東京電機大学国際化サイバーセキュリティ特別コース

[文献 11]は企業における情報セキュリティを統括する CISO や、セキュアな情報システムの開発において主導的役割を果たす上級セキュリティエンジニアを育成すべき人材像として 2017 年度に実施された大学院修士レベルの教育コースのうち、マネジメント系の内容を集約した科目である。講師はそれぞれの講義内容を専門とする大学教員及び産業界講師が務め、3 ヶ月にわたって開催される 15 回の講義のうちうち 3 回は演習形式とするなど、実践的なカリキュラムとする工夫がなされている。

表 18 「情報セキュリティマネジメントとガバナンス」カリキュラム（[文献 11]より引用）

5MG：情報セキュリティマネジメントとガバナンス	
科目概要	情報セキュリティの計画、設計・導入、運用・保守、見直しのPDCAサイクルを実施する方法論として、国際基準にもなっている情報セキュリティマネジメネントシステム(ISMS)がある。本科目では、企業の事業継続における情報セキュリティマネジメントとガバナンスについて、ISMSを中心としたケーススタディ（演習）で学ぶ。本科目の目標は、企業における情報セキュリティを統括するCISOに必要な基本的な知識と能力を修得することにある。※一部英語資料を用いて講義を行う。
習得できる能力	企業における情報セキュリティを統括するCISOとして必要な基礎知識と能力 ISMSの継続維持を可能とする社員教育の基本的能力 コンプライアンスならびに監査に関する基本的能力
履修資格 （前提）	[1PF]サイバーセキュリティ基盤の先修を推奨する。 [3IN]セキュリティインテリジェンスと心理・倫理・法の先修、または同時履修を推奨する。 学部卒業程度の情報セキュリティに関する基礎知識を前提とする。

回数	講義内容
第1回	暗号の危たい化リスク
第2回	制御システム、組み込み機器のセキュリティ
第3回	内部統制及びIT統制
第4回	セキュリティ監査技法
第5回	情報セキュリティマネジメントにおける標準化動向
第6回	リスクマネジメントとリスク分析
第7回	暗号技術①
第8回	暗号技術②
第9回	認証技術
第10回	ホワイトリストによるサイバー攻撃対策
第11回	CSIRT起点による組織マネジメントとセキュアデザイン技法①
第12回	CSIRT起点による組織マネジメントとセキュアデザイン技法②
第13回	インシデントレスポンス演習①
第14回	インシデントレスポンス演習②
第15回	まとめ学力考査

③ MIT スローンスクールによるサイバーセキュリティ科目

[文献 18]はマサチューセッツ工科大学スローン校の MBA コースにおけるカリキュラム内で提供されているサイバーセキュリティ科目のシラバスである。技術系の専門家育成用のカリキュラムと異なり、サイバーセキュリティによるリスクを把握するために必要最小限の知識を習得するための構成となっている点が特徴的である。なお、[文献 18]によれば、本科目はビジネススクールの教員と MIT で国際関係を専門とする教員が責任者となり、コンピュータサイエンスを専門とする教員がサポートに入る体制で講義が行われており、経営視点でサイバーセキュリティの知識・スキルを身に付けるための実践的な内容になっていることが観察される。

表 19　MIT スローン校 MBA コース“Cybersecurity”科目シラバス（[文献 18]をもとに作成）

大学名等		MIT（マサチューセッツ工科大学）スローンスクール MBA コース	
科目名		サイバーセキュリティ（2017 年春期開講、12 週）	
概要		サイバーセキュリティに関する総合的なアプローチを提供する。脅威、運用及び影響の原因と挙動に焦点を置くとともに、技術、経済、政治及び戦略の観点からのソリューション戦略を扱う。	
講義テーマ（同大学シラバスより抜粋）	パート 1：コンテクスト、コンセプト、論点（サイバーセキュリティの概要を示す。多面的な視点から、脅威、意図、能力、不確実性を含む多様性にフォーカスする。）		
	1	導入＝コンテクスト、意味、インパクト、不確実性	脅威としてのサイバーセキュリティに関するフレーミング
	2	新しいグローバルチャレンジ＝我々は何を知っていて、何を知らないか	グローバルな変化と新たなルール、サイバー環境と実環境との相違
	3	サイバースペース＝インターネットアーキテクチャとセキュリティの複雑性	レイヤー毎の官民アクターの行動を含むアーキテクチャのレビュー
	4	サイバー脅威を扱う国際機関	FIRST, IMPACT, ITU などの国際機関の役割と課題
	パート2：比較展望－場面と条件（サイバーセキュリティの地政学、政治学及び経済学的な「実態」について説明する。新興の活動にともなう新しいマーケットに関する内容を含む。ケーススタディ、データとその測定、関係者とその損得について考察する。）		
	5	ナショナルセキュリティ＝サイバー脅威とサイバー戦争の可能性	国家安全保障におけるサイバーセキュリティの位置付け
	6	障害ポイントと制御範囲	ケーススタディによる制御ポイントの分析
	7	サイバーセキュリティに関する保険と他の原則	サイバーセキュリティに関する対策と保険による保護、その可能性と課題
	8	サイバーセキュリティにおける経営の役割：TJX の事例におけるサイバーセーフティ分析	新規事業による新たなサイバーセキュリティ上の脅威とその対処についての事例毎の分析
	パート 3：政策対応＝戦略と意味（国内・国際的な方針について、変化し続けるサイバーエコロジーにおける代替ソリューション戦略を含めて、公式・非公式の内容を扱う。）		
	9	方針と予想＝コンピュータサイエンスからの視点	コンピュータサイエンスの観点に基づくツール、プロセス、意思決定
	10	マルウェアと脆弱性に関する市場	マルウェアに関する市場、アクターと収益構造

	11	組織のサイバーセキュリティ文化の役割についての理解	メトリクス、サービス、アクター、関心を踏まえたサイバーセキュリティ政策
	12	もうひとつの未来:次は何か？	地政学、国際政治学等を踏まえたインターネットとサイバー領域

調査結果からの考察

①～③の文献より、知識・スキルを習得するための、モデルとなるカリキュラムについて、次のことが考察される。

- 現在国内におけるサイバーセキュリティ人材育成のためのカリキュラムは、IT 人材としての情報セキュリティ人材の育成を主眼とした、IT に関する知識・スキルとその延長上にあるものであり、米国の一部の例に見られるような、ビジネス戦略の視点でサイバーセキュリティの実践力を磨くようなアプローチでのカリキュラムは確認されていない。

２．２．３ 調査結果の分析

前項での調査結果をもとに、サイバーセキュリティ人材育成に係る傾向の分析を行う。

（１）「戦略マネジメント層」に期待される知識・スキル

調査結果をもとに、２．１において定義した「戦略マネジメント層」に相当する役割や専門分野として、調査対象文献で定義されている内容を比較した結果を次表に示す。「戦略マネジメント層」に期待される知識・スキルは、技術系にとどまらず、ビジネス系、社会系、人間系などに拡がっている。ただし、米国では技術系以外について、日本よりも幅広い知識・スキルを持つことが期待されていることがわかる。

表 20　「戦略マネジメント層」に期待される知識・スキル

分類			国内事例				米国事例	
文献番号			文献 6		文献 10	文献 11	文献 14	文献 18
記号凡例 （必要な知識・スキル／教育内容） ◎=高度、○=中間、△=初級、 －=不要、？=不明			ITSS+		情セ大報告書例示⑤「単独科目」	東京電機大 CySec 情報セキュリティマネジメントとガバナンス	NICE 人材フレームワーク "Program Manager"	MIT スローン校 MBA コース “Cybersecurity”
			情報リスクストラテジ	情報セキュリティデザイン				
技術系	IT	システム構築	－	◎	－	－	○	？
		運用・保守	－	－	○	◎	△	？
		ハード・ソフト	－	－	－	－	○	？
		ネットワーク	－	○	－	－	○	◎
		セキュリティ	○	◎	○	◎	◎	◎
	OT（安全管理、プラント運用等）		－	－	－	－	△	？
	基礎	情報学・コンピュータ科学	？	？	－	※	－	◎
		工学基礎	？	？	－	－	－	◎
ビジネス系	マネジメント	プロジェクト	－	－	－	－	○	◎
		セキュリティ	◎	◎	△	◎	◎	◎
		クライシス	－	○	△	◎	－	◎
		リスクセンス	？	？	？	？	○	◎
	ガバナンス		◎	○	－	◎	○	◎
	戦略	コンセプト	－	－	－	－	－	◎
		企画	◎*	◎*	－	－	○	◎
	ファイナンス		○	－	－	－	○	◎
社会系	国際関係		？	？	－	※	△	◎
	経済学		？	？	－	－	－	◎
	法学		○	○	－	－	○	◎
人間系	心理学・行動科学		？	？	－	－	－	◎
	倫理		○	－	－	－	○	◎
トレンド			○	○	－	※	○	◎

*：システム系の戦略・企画に限定　　※：受講の前提知識

（２）セキュリティ人材育成の取組に関する我が国における人材像の定義とカリキュラム

調査結果をもとに、サイバーセキュリティ人材の分類毎の人材像等の定義例とカリキュラム例を整理した結果を次表に示す。「システム担当」「システム構築担当」といったいわゆる IT エンジニアに相当するセキュリティ人材については、既に国内でもカリキュラムを含めて整理されているが、「戦略マネジメント層」についてはそのような人材を端的にターゲットにするようなカリキュラムが存在しない。一方、米国では、MBA プログラムにおけるサイバーセキュリティコースをはじめとして具体的なカリキュラムが存在する。また、カリキュラムの内容も、単なる教科書的な「知識の詰め込み」ではなく、ビジネスにおいてサイバーセキュリティをどうフレーミングするのかの議論や、ケースに基づく意思決定の議論など、発想や意思決定における「考え方」に重きが置かれている。

表 21　サイバーセキュリティ人材の分類毎の人材像等の定義例とカリキュラム例

人材分類	日本		米国	
	人材像等の定義例	カリキュラム例	人材像等の定義例	カリキュラム例
戦略マネジメント層	●産業横断検討会（第2期にて検討中） ●ITSS+（情報リスクストラテジ）	（なし）	●NICE 人材フレームワーク（プログラムマネージャー）	●MBA プログラムにおけるサイバーセキュリティコース
システム担当	●産業横断検討会 ●SecBoK ●ITSS+（情報セキュリティアドミニストレーション等）	●情セ大モデル・コア・カリキュラム ●enPiT 1/2/Pro ●情報処理学会 J07/J17 ●情報処理安全確保支援士シラバス	●NICE 人材フレームワーク（システムアドミニストレーション、システムアナリシス等）	●SANS コース（Managing Security Operations: Detection, Response, and Intelligence 等） ●大学等におけるインフォメーションシステム系プログラムにおける各種コース等
システム構築担当	●産業横断検討会 ●SecBoK ●ITSS+（セキュア開発管理）	●情セ大モデル・コア・カリキュラム ●enPiT 1/2/Pro ●情報処理学会 J07/J17 ●情報処理安全確保支援士シラバス	●NICE 人材フレームワーク（システムアーキテクチャ、ソフトウェアデベロップメント等）	●SANS コース（Web Application Pentesting Hands-On Immersion 等） ●大学等におけるソフトウェアエンジニアリング系プログラムにおける各種コース等

なお、現状では未実施のため調査結果には含めていないが、文部科学省の平成 29 年度「成長分野を支える情報技術人材の育成拠点の形成（enPiT）情報セキュリティプロ人材育成短期集中プ

ログラム」（enPiT Pro Security）[4]において、企業内のセキュリティに責任を負う経営層、最先端のセキュリティ研究者あるいは Fintech や IoT、ビッグデータなどの最先端の技術分野におけるセキュリティマインドを持つシステム開発技術者といった多様なサイバーセキュリティ人材の育成を目的とする、社会人を対象とした産学連携による人材育成の取り組みが実施されている。

調査結果からの考察

本項での分析結果より、サイバーセキュリティ人材の育成を対象とする取り組みについて、次のことが考察される。

- 米国ではサイバーセキュリティに関する多様な役割に応じたカリキュラムが提供されており、中には MIT スローン校の MBA コースのように、戦略マネジメント層に求められる知識・スキルに近いカリキュラムを提供している例もみられる。一方、国内においては調査の結果、戦略マネジメント層に求められる知識・スキルを総合的に扱うような既存のカリキュラムは存在しないことが明らかとなった。
- これに対し、システム担当やシステム構築・運用担当に相当するカリキュラムは複数例が存在しており、こうした人材の育成に活用することが可能である。

[4] http://www.seccap.pro/

２．３ ヒアリング調査

本項では、本調査において実施した企業へのヒアリング調査を通じて把握した内容について整理する。

２．３．１ 調査概要

企業においてサイバーセキュリティ対策を担っている人材の実態や直面している課題など、文献調査では把握することが困難な内容の調査を目的として、国内企業へのヒアリング調査を実施した。対象企業の概要は次の通りである。

- 鉱業系企業の IT 子会社
- 製造業（化学）系企業
- 物流業系企業
- 金融業系企業
- 情報サービス系企業
- ISAC 運営団体

さらに、本調査と並行して同様の問題意識をもとに人材像等についての検討を行っていた産業横断サイバーセキュリティ人材育成検討会の事務局メンバーと２回にわたって意見交換を実施した。本項ではそれらの意見交換の場にて指摘された事項についても併せて示す。

２．３．２ ヒアリング調査を通じて把握された事項

（１）企業内のサイバーセキュリティ対応のための組織体制に関する内容

企業内のサイバーセキュリティ対応のための組織体制に関してヒアリング調査で挙げられた事項を次表に示す。

表 22　企業内のサイバーセキュリティ対応のための組織体制に関するヒアリング調査結果

● サイバーセキュリティを含む IT リスクについては、全社の IT 部門で評価を行っている。この際、対象業務の内容も踏まえて行っている。
● サイバーセキュリティ対策に関する「戦略マネジメント機能」は本部の IT 管理部門で担っており、各事業部門では個別商品・サービスに関する対策を検討している。
● サイバーセキュリティに関するリスク評価をフレームワークやスコープを含めて的確に行い、その結果について経営層を含む社内で共有することの重要性を感じている。
● 現場を知る課長で構成される「制御システムセキュリティ連絡会」で合意した結果を全社で推進している。業界で策定した安全基準をもとに、自社の制御システム向けの対策要領を作成し、さらにこの内容を各工場の工場長に周知してもらった上で、工場運営の基本ルールである工場則に反映させた。
● SOC 業務を想定したとき、そのログ解析を外注することは多くの企業で行うだろうが、その解析結果を判断するアナリスト業務まで外に出して良いかはよく検討する必要がある。事業との距離感から、社内に置きたいと考える企業が多いのではないか。

- 組織内の必要なところに統括人材がいることは重要だが、その人に力がないと厳しい。必要な力を与えるような組織体制にすべきであって、人がいればよいということではない。組織的対策、人的対策ならびに制度的対策が相まってやらないと、統括人材を生かし切れず、全体としてリスクマネジメントができないのではないか。
- 米国の金融機関などでは、サイバーセキュリティ対策の担当部署を IT 部門内からリスク管理部門に移管する動きがある。牽制効果を期待している面もあるだろう。
- IT 部門とビジネス部門のバランスをとる人材がどちらかの部署にいたほうがよいのか、第三者的な立場の部署にいたほうがよいのかは、組織内のパワーバランスによって異なる。
- 日本の企業において IT 部門の力が弱いのは、サイバーセキュリティにおける問題のひとつである。
- IT ベンチャーの事業が IT に立脚しているのは間違いないが、顧客に IT サービスを提供している企業と、自社で IT を使うのが主体で顧客には提供しない企業とを区別すべき。
- 日本企業の多くはPDCAといいながらセキュリティポリシーの適切な見直しを怠ってきたところが多く、クラウド利用や委託先管理などに関するルールが現在の効率的な IT 利用の障害となってしまっている。

（2）組織体制における、各層の役割・人材像に関する内容

企業内のサイバーセキュリティに関する組織体制に関してヒアリング調査で挙げられた事項を次表に示す。

表 23　組織体制における、各層の役割・人材像に関するヒアリング調査結果

- IT を活用した業務は今後も増えると見込まれることから、そのサイバーセキュリティ対策を含む IT 活用を担う人材の必要性は高まると考えられるが、現状では専門性を有する人材のパイが少なく、直ちに期待に応えるのは難しい。
- サイバーセキュリティに関する脅威や対策技術のトレンドは欧米発が多く、これらをしっかり把握できる人材の必要性を感じている。またインテリジェンスについても同様である。
- 戦略マネジメント層は、CIT と BIT を組み合わせて活用していくにあたり、関連する内容を幅広く把握する必要がある。自分ですべて把握していなくても、誰に聞けばわかるかを知っておくなど、共有のための仕組みがあればよい。
- 戦略マネジメント層に事業上の投資判断を求めるかどうかは今後の課題。投資判断が入ってくるとスペシャリストではなくなる。
- 戦略マネジメント層が必ず事業部門に必要とは限らないのではないか。企業によっては本部機能で同様の役割を担うのが適切な場合も想定される。
- セキュリティ統括は、情報を単に流すのではなく、経営トップの意向を受けて、リソースの割当やサポートする、実際の判断をする、意思決定をするといった役割を想定する。
- セキュリティ統括人材のキャリアパスの例としては、ビジネス部門から IT 部門を経験して統括を担当するパスが想定される。
- 重要インフラや製造部門内でのキャリアパスはすでにあり、別にサイバーセキュリティのキャリアパスを考える必要はない。既存のキャリアパスにセキュリティの要素をどう組み込むかの問題である。
- 「セキュリティ統括人材」を考えていく中で、その内部に階層があると感じるようになってきた。「全社レベル」を統括する人と「ドメイン（プラントや事業部等）単位」で統括する人の両方が必要で、一人で全てを担うことはできず、両者が有機的にネットワーク化し、チ

ームとして連携して動くことで組織を支える形になる。特に、大企業、重要インフラ企業ではほぼそうならざるを得ないのではないか。ドメイン固有の事情もあり、組織によっても全社とドメインの分担範囲は異なるだろう。

- IT 系で育ってきた人材をいきなり経営に近いところに回すのは難しい。経営者が何を求めているかに応じて自分で対応しなくても、ベンダを紹介するなど適切な対応がとれるようにする必要がある。反面、IT はスコープが広いので、事業部毎に閉じた狭い世界で育ってきた人材よりも視野を拡げられる機会がある。
- Strategist よりも Supervisor のほうが近いのではないか。Supervisor を和訳すると「統括」が一番近いように思う。
- OT 系のセキュリティを IT 系人材で担うことはできない。IT 機器の対策のようにアドオンのセキュリティ対策ソフトウェアを動かそうとしても、OT 側の機器では性能に影響してしまうためできない。こうした OT の事情に通じた人材がセキュリティを習得する必要があるが、教えられる先生はほとんどいない。OT を研究しているのは、いずれも制御工学や信頼性工学を専門とする先生方で、いわゆるサイバーセキュリティ分野と重ならない。
- ユーザ企業におけるセキュリティ人材は技術のオペレーションに関する部分はベンダにアウトソーシングしてよい。マネジメントリスクや問題へのレスポンスをしっかり扱えることが重要。
- IT 人材が成長してリスク管理を担ったり経営判断をしたりするようになるというキャリアパスは、技術を収益源とする企業ならあり得る。
- 残念ながら業務知識、セキュリティに関する知識、AI などの最先端技術に関する知識をすべて把握している人材はいない。
- 複数のサービスを利用している環境では、そのサイバーセキュリティ対策を担う人材はアーキテクチャを見通せることが必要。ただしそうした人材を確保することは多くの企業にとっては難しいので、現実的には社外に相談できる相手をもっている人材がいればよい。さもないと、ベンダの言いなりになるしかなくなってしまう。
- 情報システム部門であっても外部委託や調達で対応していたため、専門性を身につけた人材が少なく、今後育成していかなければいけないのが課題である。
- セキュリティ黎明期から活躍している人材は全てをやってきたので生き残っているが、今からこれをやれといってもなかなかできない。昔は技術の幅が広がるのに応じて学んでいけばよかった。
- 法的に統括人材を設置することを求めるのは難しいかもしれないが、設置することが望ましいというトーンを打ちだした上で、今後企業の中でサイバーセキュリティに関してどこまでやるかについての基準づくりの方向性がサイバーセキュリティ戦略の中で示されるとよい。

（3）必要とされる知識・スキルに関する内容

必要とされる知識・スキルに関してヒアリング調査で挙げられた事項を次表に示す。

表 24　必要とされる知識・スキルに関するヒアリング調査結果

- 「もしかしたらこれがあるかも」、「これがやられているからこうなっていのかも」というのが我々の考えるリスクセンスである。それをどう磨くかに取り組んでいるが、「環境に突っ込むしかない」という結論になりそうである。
- コンセプチュアルスキルと同様の概念の必要性は感じている。状況に応じて抽象度を上げたり下げたりできる、トップ層の思いを大枠でつかんだ上で、具体化するときにどうすればできるかを考える、自分でできなくても、専門家をどう使えばできるかを考える、といった能

力について議論したことがある。その結論として、まず必要なのはコミュニケーション能力であり、「自分が何がわかっていて何がわからないのかを把握した上で、何をやらないといけないかを大掴みに把握する能力がいる」という結論に至った。

- セキュリティは幅広いため、ネットワークの仕組みを理解していないと苦しい。規程の整備担当者であればこうした知識はそれほど必要ではないが、実務を知らないと現実性のない規程を定めてしまう恐れがある。
- 経営企画部門での経験はあったほうがよい。セキュリティは詰まるところ経営の一要素なので、投資対効果に関するマインドは絶対に必要。
- 制御系に関しては、IT 担当に制御システムを教えるのは無理なので、エンジニアリング（工務・計装系）の経験者にセキュリティを教えている。
- リスク管理はたいへん難しい業務である。経営視点では、リスクを最終的に「被害の大きさ」×「発生確率」に帰着させなければならない。これを含み損とみることで初めて経営との共通認識を確立することができる。こうしたスキルについてはリスク管理に関する研修を通じて素養を身につける必要がある。
- リスクマネジメントについては、業界ごとにフレームワークや標準があるので、ジェネリックに教えることは難しい。リスクアセスメントとは何かを理解してもらった上で、自分達にマッチするフレームワークを探してきて、それを使うことを教えればよいのではないか。NIST のフレームワークが合わなければ別のものを使ってもよい。
- 日本の IT 人材の多くがディテールに注目しがちであるが、統括業務を扱う人材には全体を包括的に見ることができる能力が求められる。さらに、経営者が何を考えているかを把握した上で、わかりやすく伝えるコミュニケーション能力が必要となる。その他、コミュニティ調整能力なども求められ、多彩な人でないと回せない。
- 経営者に対する説明では、単に疑問に答えるのではなく、「ここで対策しないということは、～のリスクを受容するという判断をしたことになるがよいか」という、一種の脅しに近い言い方も必要になる。自らも経営マインドを身につけておくことが望ましい。
- 事業部門側に無理をいってやってもらうような交渉能力も必要である。
- 監査の知識・スキルはリスク管理を行う上でも有用である。
- モチベーションは「マクレランドの氷山モデル」を参考に考えるとよい。
- OS の仕組みを理解していないと、脆弱性が生ずる原理や、なぜ権限を奪われるかがわからない。
- IT 知識のうち何を教えるべきかについては、「脆弱性情報を読む上で知っておくべきことかどうか」で判断すべき。
- 「今日発生した問題に、今日対処できるスキル」が必要。
- これまでのセキュリティは「イントラネットをどう守るか」を中心に考えられていたが、現在クラウド上のサービス利用に移行してしまった企業ではイントラネットそのものが存在しないので、これまでのガイドラインでは守れない。
- 日本の企業における IT の活用が「文房具レベル」であることが、サイバーセキュリティを何のためにやるのかを理解してもらえない原因と感じている。IT が事業のために重要な位置づけにあることを理解しないと、サイバーセキュリティの必要性も認識できない。
- IoT のサイバーセキュリティは、これまでの情報システムを対象とするセキュリティとは全く異なる次元の話である。製品開発時の対策と、インシデント時のフォレンジックをどうするかが気になっている。セキュリティ対策というとサーバとデバイス程度しか考えていない人が多いが、実際には 16 種類のドメインが関与している。そうした IoT セキュリティのモデルが十分議論されていない。

（4）育成方法やカリキュラムに関する内容

人材の育成方法やカリキュラムに関してヒアリング調査で挙げられた事項を次表に示す。

表 25　育成方法やカリキュラムに関するヒアリング調査結果

- 中途採用で専門家を採用し、専門性の高い内容をベンダへの委託で補うと同時に、プロパー職員の育成に取り組んでいる。最終的には専門的な一部の内容を除き、社内の人間同士でセキュリティに関するコミュニケーションができることを目標としている。リスクについては第三者のセキュリティベンダに評価してもらい、その評価結果に関してベンダとコミュニケーションできる、さらに経営層への報告としてのコミュニケーションができるようにするというのが最低限の目標である。
- システム部門においては、特定のシステムのみを知っていても成長しないとの観点からベンダに出向させ、システムに関するとらえ方を身につけるための経験を積ませることはある。
- セキュリティ統括人材を育てる方法として、IT 系出身者に経営を教えるのと、総務・経営企画系出身者にサイバーリスクを教えるのとどちらが簡単かといえば後者である。これは意思決定者に適切に情報提供するスキルは、経営に近いところでの業務経験がないと難しいためではないかと考えている。「ポジションで人を育てる」という発想は重要。ただし誰でもよいわけではなく、アサインしてもなかなか理解できない人もいるので、資質がある人を割り当てる必要がある。もっとも、現状で総務や企画を担っている人材を対象にセキュリティ対策を教えるような研修は存在しない。
- 「自分が知っていることを相手の知識レベルに応じて話せるようなスキル」を磨く研修をピックアップしている。
- 現在の現場人材にセキュリティを教える際には、単純に技術を教えればよいわけではない。まず世の中が変わってきていることを認識してもらった上で、リスクセンスをどう教えるかを考える必要がある。
- 「脅威の関係主体をあらかじめ理解しておかないと、何が起きるかの想像がつかない」ということをまず本質的に理解してもらう必要があるが、経年劣化や設計ミスさえなければよい、という考えの中にどのようにカリキュラムとして入れるかは難しい。
- セキュリティ人材育成のためのカリキュラムから、インターネットそのものについての説明が抜けがちである。IP アドレスやドメインはどのような団体が管理しているのか、インターネットの構造やいろいろな関係団体などを理解していないと、インシデント対応のときに攻撃元の分析もできない。
- 現実のインシデントはそれとわかるように発生しないのが普通であり、それを理解するにはシナリオ演習の形でやるのがよい。
- 教育内容をもっと定式化し、幅広く教育できるようなカリキュラムを作れないか。
- 受講者が理解したつもりになっても、実際には理解できていないことがよくある。したがって、正しく理解できているかどうかを検証する目的で、受講者に実際に手を動かしてもらうこと（ハンズオン）が非常に重要である。
- 短期間で内容を詰め込んでも、すべてを記憶できるわけではない。一定の間隔を置いて定着させていくことが必要である。
- 本を読めば理解できる内容については、詳しく教えなくてもよい。
- IT ベンチャーのように IT に精通した人がマネジメントを行っている企業に対して、サイバーセキュリティを教えるのは簡単である。従来型の企業の人材に 1 日かけて教える内容を 1 時間で理解してもらえる。一方で、そうした IT ベンチャーを在来のユーザ企業向けのセキ

ュリティのコミュニティに参加しても合わないので、新たに IT ベンチャーに特化したセキュリティのコミュニティを作るべきではないか。

- IT ベンチャーのようにクラウド主体で運用している場合のサイバーセキュリティ対策のポイントは次の 5 点である：
  1) ID と認証機構の適切な管理
  2) ID に紐付いたアクセス権限の明確化
  3) クラウドサービスで提供されているセキュリティ機能の活用
  4) アプリケーション開発時の、セキュリティ対策上有利な言語・ツール等の利用
  5) 適切なログ管理

調査結果からの考察

本調査で実施したヒアリング調査において収集された意見から示される事項は次のとおりである。

- 全ての企業にとって理想的な体制は存在せず、企業のビジネスモデルや指揮・命令の方法、慣習などに応じて合理的に機能するような体制を検討すべきである。
- サイバーセキュリティ対策を担う人材の役割やキャリアパスについても体制と同様、企業によって異なるものになる。一方で現行の情報システム管理を行う人材がそのまま戦略マネジメント機能を担うのは難しい。
- 知識やスキルについては、文献調査を通じて重要性が示された、コミュニケーションスキルやコンセプチュアルスキルなどが必要との意見のほか、サイバーセキュリティの基盤となる IT への理解の必要性も指摘されている。
- 育成方法やカリキュラムについては、既存の内容が人材育成上のニーズを満たしていないことが産業界から指摘されている。

２．４ 政府会議等における議論の把握

サイバーセキュリティ人材の育成に関する検討を進めるにあたり、関連する会議体としてサイバーセキュリティ戦略本部の普及啓発・人材育成専門調査会に設置された「セキュリティマインドを持った企業経営ワーキンググループ」及び「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ」における議論の内容を本項にて示す。

（１）企業内のサイバーセキュリティ対応のための組織体制に関する内容

企業内のサイバーセキュリティ対応のための組織体制に関する発言の要旨を次表に示す。

表 26　企業内のサイバーセキュリティ対応のための組織体制に関する発言要旨

- 企業として重要と認めたリスクの１つにサイバーセキュリティがあるという二重構造を前提とすべきであり、サイバーセキュリティのリスクマネジメントのみを扱っても効果がない。
- リスクマネジメントにおいて、業態の差は無視し得ない。企業経営者の訴求力は、業界固有のリスクの性質によるところが大きい。企業規模の違いはむしろ、大企業が先行して、中小企業が業界として追従する程度である。
- 企業それぞれにおいて、危機管理のメカニズムの中でサイバーセキュリティを位置付けるように指向しているかが重要。
- 米国の銀行からは、自社をセキュリティのユーザ企業でなく、先端企業として認識しているとの表明がなされている。その企業では実際にリスクを定量化して経営判断に活かしているようである。
- 業種で見ると、金融業は明らかに他業種とは異なる。特に人材育成を働きかけなくても業務上の必要性から自ら取り組むと考えてもよい。
- 中小企業においてどうすればよいかを考えることで、問題の本質が見えてくることがある。
- グループ企業や地方の支社において、本社と比べてセキュリティレベルが格段に落ちるようなことが現実に見られる。
- 対策すべき基準が不明というのは、基準が多すぎることの裏返しの場合がある。
- 経営層を動かそうとしても難しい場合は、制度論で進めて行かざるを得ないこともある。
- サイバーセキュリティ対策が投資でなくコストに見えるのは、ICT システムがもともと安全という前提に立っているからではないか。
- 企業のセキュリティ対応の型を決めないと、各社が独自に同じようなことを検討することになり負担が大きい。ある程度の部分を標準化することで、型を活用した対応ができるのではないか。
- 米国はすでに経営層がかなりビジネス戦略、戦略マネジメント機能を意識した経営を行っている。
- インシデントのリスクも理解した上で事業設計がなされると、情報システムの側も非常にわかりやすくなる。

（２）組織体制における、各層の役割・人材像に関する内容

企業内のサイバーセキュリティに関する組織体制に関する発言の要旨を次表に示す。

表 27　組織体制における、各層の役割・人材像に関する発言要旨

- セキュリティ人材の育成というと、これまでシステム系の人に知識を付けてなるべく経営層に近づけることにフォーカスしがちだったが、戦略マネジメント機能は事業部門側が IT の知識を習得すべきことをイメージしているのではないか。
- 育成した人材が活躍できるような場所がないという声をよく聞く。セキュリティ人材のキャリアパスがあると回答した企業の比率も低い。
- これまでのセキュリティ人材の対象は情報システム部門のような部署であったが、それが事業部本体のほうに移りつつあるのは確かである。
- セキュリティの技術はどんどん代わっており、数年前までの ISMS 技術者はもうほとんどいない状況である。
- ジョブディスクリプションに基づいて採用と業務遂行が行われる米国と、新卒中心で明確なジョブディスクリプションのない日本との違いは大きく影響すると思う。
- 人材の流動性がもっと確保され、フレームワークをもとに業務についての共通認識ができると今後変わってくる可能性もある。
- NIST のフレームワークは、雇用や教育訓練と連動している点が優れている。

（３）必要とされる知識・スキルに関する内容

必要とされる知識・スキルに関する発言の要旨を次表に示す。

表 28　必要とされる知識・スキルに関する発言要旨

- 「セキュリティの基礎」というとき、セキュリティスペシャリストになるための基礎（例：暗号理論）と Excel や電子メールを安全に使うための基礎的なセキュリティ対策という２つの意味があり、両者は全く異なることに注意すべき。
- リスクマネジメントについて検討する際は、どの規格で定められた用語を用いるかが重要。最新の ISO 規格では、リスクとしてポジティブな概念も扱っている。
- セキュリティ分野では多くの場合、コントロールとしての議論が多いが、経営層まで巻き込む際はマネジメントが必要となる。議論をする際には考え方の違いを整理すべき。
- サイバーセキュリティとしての項目で、マネジメントシステム全体を支配するような概念を出されると、マネジメントシステムが混乱してしまう。
- 情報セキュリティのみがリスクの考え方が違っても、他の分野ではその考え方を使っていないので、マネジメントとして困ることになる。
- リスクマネジメントはマネジメントを支援するものに過ぎない。発生確率が不明であったり、不確定であっても、ある前提で評価したという条件があれば、マネジメントはそれをもとに判断することになる。
- 海外での実態を踏まえ、国際基準イコール ISO でないことに留意すべきである。

（４）育成方法やカリキュラムに関する内容

人材の育成方法やカリキュラムに関する発言の要旨を次表に示す。

表 29　必要とされる知識・スキルに関する発言要旨

● 組織において実践力の高い人材を高校や大学で育成するのは難しい。大学などでできることと企業でできることを明確に分けて議論しないとミスリードになる恐れがある。 ● 大学での教育は、人材として後々長持ちすることを心がけている。更新頻度が短い資格制度と絡める考えには違和感がある。 ● リスクマネジメントやリスクセンスなどの判断ができる人材を育成しようとすると、大学でも教える側の教員の枠を拡げて考えないと要求に応えられない。

調査結果からの考察

政府会議等における議論において示された事項は次のとおりである。

- 組織体制に関しては、企業規模の相違よりも業種の違いによる影響が大きいことが指摘されている一方、グループ企業や地方拠点などではレベルが落ちるとの意見もある。
- 役割に関しては、セキュリティ人材の役割が、業務効率化を目的とした文書作成やメールによる連絡、会計管理などに関わるシステムのセキュリティの問題への対応から、ビジネスにおける挑戦のために不可欠な IT 利活用を支えるためのセキュリティの問題に変化しつつあることが示されている。
- 知識・スキルに関しては、経営視点での考え方を基本として、サイバーセキュリティのリスクマネジメントに取り組んでいく必要があることが指摘されている。
- 育成方法やカリキュラムに関しては、大学等でサイバーセキュリティ人材を育成しようとする場合に、ビジネスと学校教育間の考え方の乖離をはじめとして、様々な問題があることが示されている。

３．課題と方向性

３．１ 現状における課題

文献調査、企業を対象とするヒアリング調査、及び政府会議等における議論についての調査結果をもとに、現在の国内企業におけるサイバーセキュリティ人材育成の課題について整理する。なお、以下の記述における「企業」とは、顧客に対して IT 関連サービスを提供する事業を営んでいない、いわゆる「ユーザ企業」を指すものとする。

（１）事業上のサイバーセキュリティ関連リスクの取扱いに関する課題

① ビジネス部門におけるサイバーセキュリティ関連リスクを考慮する体制がない

多くの企業において、自社のサイバーセキュリティ対策に関する立案・検討は社内の特定の１部署（情報セキュリティ管理部署、情報システムの企画・運用部署、リスクマネジメント担当部署等）に集約して行われている。全社共通の IT 基盤を対象とした対策の立案であれば、このような体制は効率的である。しかしながら、コスト削減や市場ニーズへの迅速な対応等の観点に優れるクラウドコンピューティングサービス（以下、「クラウドサービス」という。）や、スマートフォンやタブレット端末など、業務における PC 以外の IT 機器の活用が進む現状において、複数のビジネス部門がそれぞれ異なる独自の IT 利活用に基づいた事業戦略を展開しているケースが増えているものと推察される。こうした状況において、サイバーセキュリティ対策の立案・検討を担う部署において、各ビジネス部門における IT 利活用形態の相違に起因するサイバーセキュリティ関連のリスクを適切に把握できないことが懸念される。

② ビジネス部門に IT やセキュリティの専門家とコミュニケーションできる人材がいない

①と同様、企業におけるサイバーセキュリティ対策の運用についても、多くの企業において特定の部署に集約して行われており、この結果、サイバーセキュリティ関連の知識・スキルを備えた人材が当該部署に偏っていることが推察される。

一方で、上述したようにビジネス部門における独自の IT 利活用が進む中、ビジネス部門が直接クラウドサービスベンダ等の専門家と交渉する機会が増えている。しかしながら、このような環境においてビジネス部門内部でサイバーセキュリティの確保のためにどのような対策を講じるべきかの検討を行うことができる人材がいない場合、クラウドサービスやセキュリティの専門家との適切な調整・交渉ができず、必要な対策が講じられなかったり、場合によっては、ベンダ等の専門家の提案をうのみにして、過剰な対策を講じてしまったりするなどの状態に陥る恐れがある。それだけではなく、インシデント発生時の対応においても、こうした人材がいない状態では被害の拡大防止と事業継続の観点から最適な判断を行うことが困難になることが想定される。

③ 事業内容とサイバーセキュリティの双方に通じた人材がいない

我が国ではこれまで、サイバーセキュリティ人材はIT人材の専門分野の1つとしてとらえられてきた。インシデントの原因究明や、システムにおける脆弱性の検知など対策に関わる様々な活動にITの専門知識が求められることから、これは当然の経緯と言える。一方で、企業におけるIT利活用が進展し、ITへの依存度が高まる中で、次のような問題が生じている。

- サイバーセキュリティ対策の重要性が高まる中、対策を担う人材による経営層への説明、協議、ならびに関係部署とのコミュニケーションの機会が増えているが、これまでのIT人材育成がコミュニケーションスキルよりもテクニカルスキル主体で行われている場合、コミュニケーションが成立しないことで、企業の事業活動に必要な対策への投資がなされなかったり、適切なインシデント対応ができずに被害が拡大したりする原因となる恐れがある。
- ビジネス部門にこうした対策の立案・検討を担う人材がおらず、例えば情報システム部門の人材にサイバーセキュリティ対策を委ねる場合、情報システム部門に所属する人材がビジネスの特性を詳細に把握することは一般に難しいことから、こうした特性に応じた適切な対策が講じられず、必要な性能が得られなかったり、柔軟な対応が実現されなかったりすることで、サービスの競争力が低下することが懸念される。

④ 事業のリスクマネジメントとサイバーセキュリティ対策の乖離

国内の企業において、事業のリスクマネジメントを担う役割と、サイバーセキュリティ対策を担う役割とは、これまで独立して人材を割当て、それぞれの専門業務として運用されている場合が多いと考えられる。しかしながら、経営課題としてサイバーセキュリティをとらえようとする場合、サイバーセキュリティに起因するリスクを事業リスクのひとつとして管理することが欠かせない。こうした事業リスクマネジメントを通じて、サイバーセキュリティに起因するリスクをコントロールすることが、今後の企業における事業価値の創造における前提条件となる。

そこで、両者を同一の人材が担うか、両者が密接な情報交換や共有をおこなうことが必要となるが、前者については両方のスキルセットを身につけるような人材の育成が行われておらず、後者については相手が求めている情報を提供するようなコミュニケーションの経験が不足するなどの理由により、事業リスクとしてサイバーセキュリティを管理できている企業が少ないことが見込まれる。

（２）情報システム部門を中心としたサイバーセキュリティ組織体制に関する課題

① 今後の社会の変化に合わせた、組織体制や役割設定の見直しの必要性

今後、「Society 5.0」として提唱されているように、サイバー空間と現実の空間を高度に融合させたシステムが社会に展開されていくことが見込まれている。これにあわせて、サイバーセキュリティ関連のリスクも変化することから、企業におけるサイバーセキュリティ対策を担う組織体制や役割において、こうした変化に伴う次のような動きに対応させていく必要がある。

- IoT や AI、ブロックチェーンなどの先進的技術のアグレッシブな導入に伴うセキュリティの重点の変化、
- アジャイル型や DevOps など、システム構築・運用モデルの変化
- 顧客や関係者とのコラボレーション、コミュニケーションや情報共有に関する形態の変化

仮に、企業の情報システム部門でサイバーセキュリティ対策を担っている環境において、当該部門が組織として、あるは当該部門内でサイバーセキュリティ対策を担う人材において、こうした変化への対応が十分にできない場合、事業上の新たなリスクとなる恐れがある。ビジネス部門においてこうした変化が生じていることを情報システム部門が認識していない場合も、同様にリスクとなる。

② クラウドコンピューティングサービスへの移行の影響

前述のようなクラウドサービスへの移行が進むことで、情報システム部門にはすでに次のような影響が生じており、今後この傾向が強まることが見込まれる。

- ビジネス部門が主導して導入され、情報システム部門が把握していないクラウドサービス（いわゆる「シャドーIT」に相当）が生じることで、組織としての IT ガバナンスが不完全なものとなる。この結果、ある脅威に対して情報システム部門で施策を講じても、シャドーIT が対策漏れとなることで、企業による事業活動に大きな被害が生ずる。
- クラウドサービスへの移行により、企業内の情報システム部門が担うべき IT ハードウェア・ソフトウェアの管理負荷が減少することで、情報システム部門が従来よりも小規模化することが見込まれる。一方で、企業における IT 利活用は以前と変わらないか、むしろ拡大する可能性もあり、企業としてそのサイバーセキュリティ対策を講じる必要性は依然として存在する。このとき、経営層にその認識が不足している場合、自社で管理する IT の削減分に比例して情報システム部門の要員数も削減してしまうと、サイバーセキュリティ対策を担う要員数も減ることとなるため、全社の対策に手が回らない事態が生ずる恐れがある。社外のセキュリティサービスベンダへの委託はその解決策になるが、自社内に適した対策を判断する要員を社内に確保できない場合、ベンダに丸投げといった状態になりがちであり、結果として自社に最適なサイバーセキュリティ対策が実現されない可能性が高い。

（３）その他の課題

① 人材に関する日米間の相違に起因する課題

上記のほか、日本固有の事情に起因する課題も存在する。すなわち、国際的な視点に立つと、日本企業における人材のキャリアパスは、次表に示すように米国をはじめとする海外とは異なる傾向を有している。そこで、米国における人材育成に関するベストプラクティスを国内で適用しても、十分な効果が発揮されない恐れがあり、日本の事情に応じた人材の育成・活用方法について検討する必要がある。

表 30　専門性の高い人材のキャリアパスに関する日米の相違

	典型的なキャリアパス	左記がもたらす影響
米国	業界で共有されるジョブディスクリプションで定められた業務について、複数の企業での勤務経験を通じてスキルと経験を蓄積。	● 役割に応じた専門性を有する人材の確保が容易。 ● 担当業務以外の業務内容には一般に精通していない。
日本	終身雇用体制を前提に、単一の企業内でのジョブローテーションを通じて、業務に必要なスキルと経験を蓄積。	● 役割に応じた専門性を有する人材を確保できるとは限らない。 ● ローテーションを通じて企業内での業務に精通したり人的ネットワークを有する人材も存在。

調査結果からの考察

調査結果から明らかとなった、現在の国内におけるサイバーセキュリティ人材育成の課題は次の通りである。

- 企業が事業のリスクマネジメントの一環としてサイバーセキュリティを扱おうとする場合、現状ではそれに必要な知識・スキルを備えた人材の不足から、ビジネス部門におけるサイバーセキュリティ関連リスクを考慮する体制がない、ビジネス部門でセキュリティサービスベンダとの対話ができない、事業内容を理解した上で対策を講じることができないといった課題があり、結果として事業のリスクマネジメントとサイバーセキュリティ対策の乖離が生じてしまう。
- 一方、サイバーセキュリティ組織体制に関しては、今後のビジネスモデルとそれに伴う IT の利活用の変化に合わせた見直しが欠かせない一方で、これまでのオンプレミス型のシステムとは異なるクラウドサービスを利活用したシステムに必要な知識・スキルが組織に根付く対応がなされないなど、ビジネス部門が利用する IT によるトラブルの発生を招いたり、全社の対策に手が回らなくなったりするなどの問題が生ずる恐れがある。

３．２ 課題の解決に関する方向性

前述の課題を踏まえ、その解決の方針を次のように検討する。

（１）事業リスクマネジメントの一部としてのサイバーセキュリティの位置付け

前述の課題に共通するのは、次の２点である。

- **企業のビジネス部門における事業戦略として IT 利活用が進展する中で、サイバーセキュリティが企業における事業リスクとなりつつあること**
- **この事業リスクをマネジメントできる人材の不足**

そこで、これらの課題を解決するには、企業における事業リスクマネジメントの一部として、サイバーセキュリティを位置付けることが欠かせない。経営層はサイバーセキュリティを経営課題として認識した上で、市場動向、競合、法規制対応、レピュテーション対策や防災など、他の経営上のリスクとともにサイバーセキュリティに関する事業リスクマネジメントが可能となるような組織体制と役割、並びにこれを担う人材の育成に関する経営方針を定める必要がある。

上述の方針のもとで、全社的なサイバーセキュリティ施策を立案・実施することを通じて、課題において指摘したような、ビジネス部門における不適切なサイバーセキュリティ対策の実施などのリスクを防ぐ効果が期待される。

（２）企業の類型化

組織体制の検討に先立ち、次のように企業を２種類に類型化する。これは産業横断検討会における類型化を参考に、事業における IT の位置付けの大きさがサイバーセキュリティ対策への取組姿勢にも影響することを踏まえたものである。一般的に、類型１の企業は、先端的な情報通信技術を積極的に取り入れ、新たな価値創造を図ることが主なミッションとなっている。一方、類型２に分類される企業は、企業における基幹システムなどのいわゆるコーポレート IT を円滑に運用し、事業継続を確保することが主なミッションとなる。政府会議における議論においては、業種によってこうした姿勢の違いが異なっていることが指摘されている。近年の企業活動は多様化しているため、厳密に分類することは困難な場合もあるが、本調査における役割の想定に関しては、類型１の企業だけでなく、類型２の企業についても対象として想定することとする。

① 類型１：IT が事業の柱になっている企業（IT ビジネス企業：ビジネス自体がインターネット上にある企業、または、IT を駆使してビジネスを行う企業）

本類型に該当する企業の特徴は次の通りである。

- リスクの高い IT の使い方をしている可能性が高く、サイバーセキュリティ対策の品質がそのままサービスの価値となる。
- セキュリティ技術の専門知識をもちながらリスクマネジメントが出来る人材を確保し、事業のプロセスと一体となって取り組むことが必要。具体的には、セキュリティ対策を担う組織または役割を事業部の中に置くことが想定される。

- サイバーセキュリティを価値（競争力の源泉）として、事業戦略そのものに必要なセキュリティを組み込む（例えば、セキュリティを考慮したビジネス設計や適切な外部委託）ための知識・スキルが必要となる。
- 業種としては、E コマース、クラウドサービス事業者などが該当する。金融業はインターネットや IT への依存度が高まる中、類型２から類型１に移行しつつある。

② 類型２：IT を重要なツールとして位置付けている企業（伝統的な企業：ものづくり的な部分がビジネスの根幹である企業）

本類型に該当する企業の特徴は次の通りである。

- IT をツールとして使う際のリスクマネジメントに取り組むことが前提となる。
- 事業内容に依存するが、事業部の中にリスクマネジメントとサイバーセキュリティを担う人材を置くケースもあれば、事業部の求めに応じて統括部門がリスクマネジメントとサイバーセキュリティの機能をサポートできる体制をつくるケースも考えられる。
- 外部専門家を積極的に活用することが想定される。
- 業種としては電力・ガス。石油、化学、運輸等の重要インフラ企業、自動車その他製造業の多くが該当する。

調査結果からの考察

調査結果をもとに示されている、課題の解決に関する方向性は次の通りである。

- 経営層はサイバーセキュリティを経営課題として認識した上で、他の経営上のリスクとともにサイバーセキュリティに関する事業リスクマネジメントが可能となるような組織体制と役割、並びにこれを担う人材の育成に関する経営方針を定める必要がある。
- 企業の事業における IT の位置付けの大きさの違いがサイバーセキュリティ対策への取組姿勢に影響しており、サイバーセキュリティを担う組織体制の在り方や人材像の検討においてこれを考慮する必要がある。

３．３ 方向性を踏まえた企業における考え方の具体化

前項に示した方向性をもとに、１．１で挙げた本調査で明確化の対象とする４点について個別に検討する。

３．３．１ 組織体制についての検討

サイバーセキュリティ関連リスクのマネジメントを行う組織体制を企業で検討するにあたり、考慮すべき事項を示す。

（１）サイバーセキュリティに関するリスクをどの部署で扱うべきか

ビジネス部門におけるサイバーセキュリティに関するリスクマネジメントは、理想的には当該ビジネス部門内に担当部署ないし担当者を設置し、部門内でリスクの分析や対策の立案等の対応を行うことが、事業リスクを正確に把握し、タイムリーかつ柔軟にその対応をする観点で有効である。一方で、経営層によるガバナンスを支えつつ、企業内で整合性のあるリスクマネジメントを実現するには、本社機能において全社を対象にリスクマネジメントを行う担当部署ないし担当者（情報システム管理部署等がサイバーセキュリティ対策を担当する場合も含む）も必要であって、両者の協調のもとでマネジメントを行うことが望ましい。

しかしながら、以下のようなケースの場合、企業のビジネス部門には、サイバーセキュリティの機能が無いことも想定される。このようなケースにおいては、組織内のサイバーセキュリティを担う統一的な部署において、ビジネス部門に係るサイバーセキュリティも含めて対応をすることになるが、そのような場合には、統一的な部署であっても、ビジネス部門とのコミュニケーションを密にし、ビジネス部門の関心やプライオリティなどを十分に理解した上で取り組む姿勢が不可欠である。

① サイバーセキュリティを理解できる人材が、企業のビジネス部門で確保できない

ビジネス部門を担う人材が直接サイバーセキュリティを実践することが有効とはいえ、サイバーセキュリティに関する知識・スキルを備えていない担当者がリスクマネジメントを行ったところで適切な取組にはなり得ない可能性が高い。人材育成には一定の時間を必要とすることから、各ビジネス部門に、必要な知識・スキルを備えた人材を確保できない状況においては、知識・スキルを備えた人材を部門横断的にみる部署に置き、サイバーセキュリティのリスクマネジメント業務を集約することが適切な可能性がある。

② ビジネス部門内で、当該ビジネス以外のリスクマネジメントを行っていない

当該ビジネス以外のリスクに関するマネジメントをビジネス部門でなく、本社機能で行っている場合、例えば、

- 全社を通じて単一の事業のみを実施している。

- 本社機能でほとんどの施策を決定しており、ビジネス部門に与えられている権限が小さい。
- ビジネス部門が販売機能に特化しているなどして、マネジメント機能を有さない。

のようなケースが想定されるが、このような場合には、リスク管理部門などの統一的な部署が企業全体のサイバーセキュリティのガバナンスを担うことになる。

（2）リスクマネジメントに関する権限の考え方について

IT を利活用する部署とは別部署でリスクマネジメントを行う場合、他部署における IT 利活用に対して強制力を発揮させる必要が生ずることがある。他の事業リスクと異なる、サイバーセキュリティ特有の対応が必要となるケースとして、例えば、次のような状況が想定される。

- 新たな脅威の発生により被害が生ずる恐れがある場合に、前例のない条件でサービスの停止や制限の実施を求める。
- インシデント対応に際して、被害の拡大防止の観点から優先度の高いサービス以外の停止を求める。
- 攻撃の証跡を保存するために、サービスに用いている IT 機器やクラウドサービスにおけるデータの保全を求める。

このような状況が発生した場合の危機管理対応について、部署間であらかじめコミュニケーションを行い、合意を得ておかない限り、迅速かつ適切な対応が困難となる恐れがある。

３．３．２ 役割や人材像に関する検討

前項における組織体制のもとで、サイバーセキュリティ対策を担う人材の役割や人材像を企業にて検討するにあたり、考慮すべき事項について整理する。

（１）リスクマネジメント機能の明確化

本調査では、３．２（１）に示すように、企業における事業リスクマネジメントの一部として、サイバーセキュリティを位置付けることとする。このとき、企業におけるリスクマネジメント機能を定義する手段として、本調査では ISO 31000:2009 が定めるプロセスをもとに、機能の定義を行う。ISO/IEC 27000 シリーズなど情報セキュリティに重点を置いた規格でなく、ISO 31000 を選択したのは、企業における事業リスクを統括的に管理することができる方法論を用いることが、今後「Society 5.0」で提唱されているようなサイバー空間と現実の空間を高度に融合させたシステムの展開が見込まれる社会において、サイバーセキュリティ対策を効果的に実現するには適切であると判断されることによる[5]。

こうした考え方のもとで、サイバーセキュリティを包含するリスクマネジメント機能は、次図のように想定される。

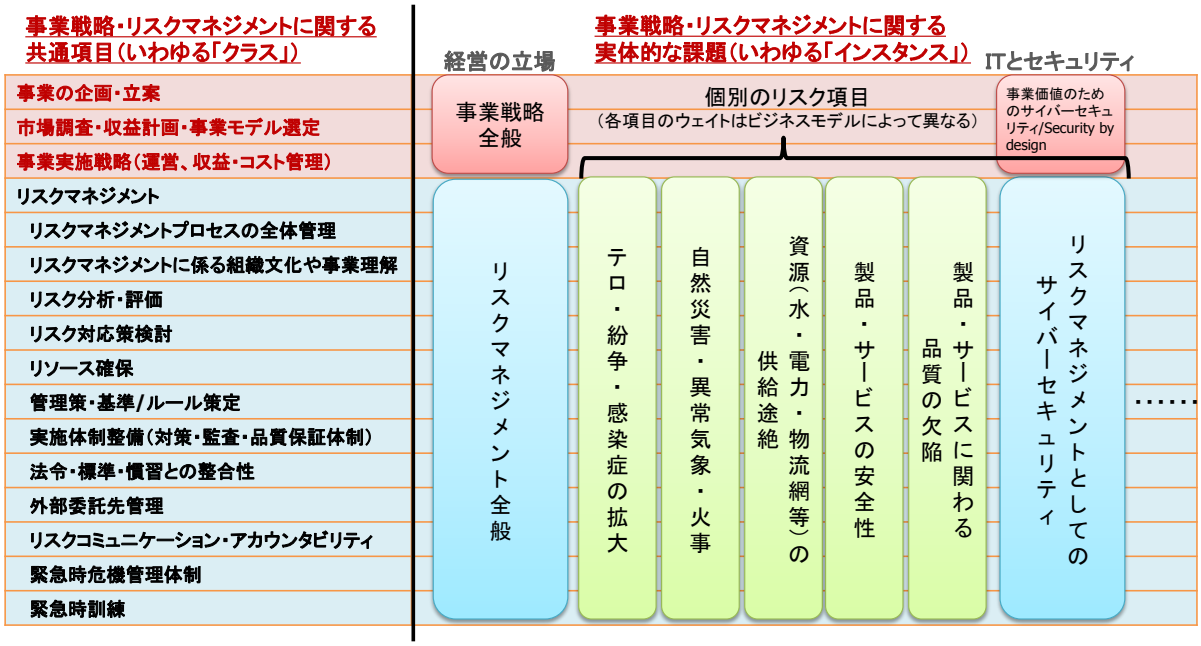

図 5　サイバーセキュリティを包含するリスクマネジメント機能の考え方

図の左側に示されているのは、リスクマネジメント及び事業戦略に関する一般的なプロセス、図の右側に示されているのは、リスクマネジメント及び事業戦略に関する実体的な課題にそれぞ

[5] なお、リスクマネジメントに関する標準やフレームワークとしては、上述した ISO 31000 や ISO/IEC 27000 シリーズのほか、業種ごとに定められているものもあり、業種によってはそれら業種固有のリスクマネジメントに関する標準やフレームワークを活用するほうが効率のよいマネジメントができる可能性もある。

れ相当する。企業が直面する様々な実体的課題に関わる事業戦略とリスクマネジメントのプロセスを進めていく中で、サイバーセキュリティがその一つの課題として組み込まれることを示している。

（2）サイバーセキュリティ対策を担う人材の役割定義

（1）に示した方針のもとに、企業における事業リスクマネジメントの一部としてサイバーセキュリティを扱うことを前提に、２．１において示した「経営層」「戦略マネジメント層」「システム担当」「システム構築・運用担当」の４種類の人材が担うべき役割を、それぞれ次表のように定義する。

表 31　サイバーセキュリティ対策を担う人材の役割定義

	通常時	緊急時対応
経営層	・経営視点から組織のリスクマネジメントに関する判断を行う。	・インシデント対応体制の確保や事業継続等について必要な経営判断を行う。 ・企業としての社会的責任を果たすための必要な対応を行う。
戦略マネジメント層	・経営戦略、事業戦略におけるサイバーセキュリティリスクを把握し、価値創造とリスクマネジメントの中核を担う。 ・マネジメントの範囲におけるサイバーセキュリティリスクを認識し、そのリスクに対し、経営層の方針を踏まえた対策を立案、様々な役割を担う実務者・技術者を指揮し、経営層に報告する役割を担う。	・システム担当等との情報共有をもとに発生したインシデントの経営・事業に対する影響範囲と影響の内容について概括的な把握を行う。 ・インシデントへの対応案を作成し、経営層による判断を支援する。
システム担当 （実務者層）	・組織で利用する情報システムの潜在的なサイバーセキュリティリスクを把握し、関係者で共有する。 ・戦略マネジメント層による方針のもと、前項のリスクを抑制するためのセキュリティ対策の企画・検討を行う。	・インシデントの組織内システムへの影響について特定し、各システムにおける対応案を立案して関係者と協議する。
システム構築・ 運用担当 （技術者層）	・組織で利用する情報システムの構築に際し、セキュリティ要件を満たすように設計・開発・実装を行う。 ・脆弱性情報を収集し、組織内の情報システムがその影響を受けないように必要な対策を講じる。 ・インシデントに備えた技術的対策を整備する。	・個別のインシデント対応を行う。 ・個別のシステムへの影響を調査し、関係者に報告する。

表中に示す役割のポイントを以下に示す。

- 「戦略マネジメント層」は「経営層」とのマネジメントに関する協議と、「システム担当」等との対策のコーディネーション（調整）の双方に関与し、事業リスクマネジメントの中核的な役割を担う。
- 「システム担当」（実務者層を想定）及び「システム構築・運用担当」（技術者層を想定）は「戦略マネジメント層」の指揮のもと、情報システムの利活用における技術的な専門性を前提としたサイバーセキュリティ対策の実務推進を担う。

３．３．３ 戦略マネジメント層の検討に係る考慮事項

本項では、前項に示した人材のうち、特に重要性が高く、サイバーセキュリティ対策において、中核的役割を果たす戦略マネジメント層が習得すべき知識・スキルについて検討するにあたり、考慮すべき事項を示す。なお具体的な知識・スキルの詳細については第４章において示す。

（１）戦略マネジメント層に必要な知識・スキルの想定

２.２.２（３）③で紹介したロバート・L・カッツの著作において管理者に求められる能力として示された整理の中で、戦略マネジメント層は、このうち、中位層の管理職に位置付けられると考えられる。この層においては、図 4（24 ページ）に示されるように、経営層の視点をもってマネジメントを行い、経営層との円滑なコミュニケーションを行うための「コンセプチュアル・スキル」が不可欠となると同時に、現場の実務者や専門人材を動かすために「テクニカル・スキル」も求められる。また、２.２.３の表 20（38 ページ）に示したように、戦略マネジメント層に求められる知識・スキルは、技術系にとどまらず、ビジネス系、社会系、人間系など幅広い内容が求められていることが事例により示されている。

そこで、こうした知見を踏まえ、戦略マネジメント層に必要なスキルとして、次に示すような内容を想定することとする。

① 事業継続を確保するためのリスクマネジメントを行うために必要な知識・スキル

- サイバーセキュリティに関するコミュニケーションや調整、実施体制とその運営に必要な知識・スキル
- サイバーセキュリティに関する法令やガイドライン、リスクマネジメントの手法に関する知識・スキル
- サイバーセキュリティに関するリスクアセスメントを理解するために必要な知識・スキル
- サイバーセキュリティリスクへの対応策（技術的な対応策、マネジメントによる対応策、それを提供する事業者を含む）に関する知識・スキル

② 新しい価値を創造するための事業戦略の推進に必要な知識・スキル

- 事業に対する不正行為を想定するための知識・スキル
- セキュリティに対する顧客の期待を把握するために必要な知識・スキル
- 事業計画において、サイバーセキュリティ投資、ランニングコスト等を適切に見積もり（費用対効果の分析などが想定される）、事業モデルに対して適切なセキュリティ対策を選定するための判断に関わる知識・スキル

（2）企業の類型に応じた求められる知識・スキルの相違

３．２（２）における企業の類型化をもとに、戦略マネジメント層に求められる知識・スキルを次のように整理する。まず、すべての企業においてサイバーセキュリティに関するリスクマネジメントを行うために必要な知識・スキルとして、ISO 31000 をもとに次表①の項目が想定される。さらに類型１（IT が事業の柱になっている企業）の企業では、サイバーセキュリティ対策が競争力の源泉となることから、戦略マネジメント層が事業戦略に関する役割にも関与することが想定される。このため、表内②のようなスキルを①と併せて有することが企業として有利となる。

表 32　類型に応じた知識・スキルの種類

① すべての企業に共通して必要な知識・スキル	● リスクマネジメントプロセスの全体管理 ● リスクマネジメントに係る組織文化や事業理解 ● リスク分析・評価 ● リスク対応策検討 ● リソース確保 ● 管理策・基準/ルール策定 ● 実施体制整備（対策・監査・品質保証体制） ● 法令・標準・慣習との整合性 ● 外部委託先管理 ● リスクコミュニケーション・アカウンタビリティ ● 緊急時危機管理体制 ● 緊急時訓練
② 類型１の企業のみで求められる知識・スキル	● 事業の企画・立案 ● 事業に関する開発・マーケティング ● 事業運営、収益・コスト管理

（３）役割の遂行に求められる知識・スキルの程度

いわゆるユーザ企業において、戦略マネジメント層に求められるサイバーセキュリティに関する知識・スキルの程度としては、業務実態を把握すると概ね次のような要件として整理できる。

- 事業との関係で必要なセキュリティ対策を理解し、経営層に対し、分かりやすく説明することができる
- 事業において必要なシステム開発や運用を担う実務者やベンダの専門家、セキュリティの担当者や専門的なサービスを提供するベンダの技術者等と必要なコミュニケーションをとることができる
- 事業影響が生じうるシステムやセキュリティに関わる外部委託が適切に実施されているか確認することができる
- サイバーセキュリティに関する脅威や深刻な脆弱性に関する情報について、内容を理解し、事業影響について必要な推定をすることができる
- インシデント発生等の非常時において、リスクマネジメントの立場から必要な情報収集、分析を行った上で、経営層による判断の支援、インシデントハンドリング等を行う担当者との連携等、必要な活動をタイムリーに行うことができる

こうした知識・スキルの習得には、組織内での OJT、外部の講習・トレーニングサービスの利用、大学等教育機関が提供する学び直し講座の受講、専門家コミュニティによる勉強会への参加等、様々な方法を活用することができる。業務遂行に必要な知識・スキルが獲得できているかどうかの判断は容易ではないが、次に示す資格のうち、上記の役割に関連する部分の内容については、参考となり得る。

① 情報処理安全確保支援士

独立行政法人情報処理推進機構が運営する国家資格であり、情報セキュリティ分野においてスペシャリストとして活躍できる知識・スキルを保有することを筆記試験で確認した上で、資格維持のために定期的な参加が義務づけられている集合研修を含む更新教育により、専門性の維持が担保されている。

② CISSP（Certified Information Systems Security Professional）

(ISC)² が運営する、２．１（３）⑦に示した情報セキュリティ分野を対象とする共通知識（CBK）の内容を理解している情報セキュリティプロフェッショナルを対象とするグローバルな認定資格である。①と同様、継続教育の受講を要求することで専門性の維持を担保している。

３．３．４ 戦略マネジメント層向けのカリキュラムについての検討

前項に示した知識・スキルを習得するためのコースとして、教育機関において提供されるカリキュラムに関して、考慮すべき事項を示す。

（１）教育コースの要件について

サイバーセキュリティに関する業務遂行に必要な知識・スキルは多様な分野にまたがることもあり、その習得には可能な範囲で多くの時間を費やすことが望ましい。一方で、企業の第一線でマネジメントを行う立場の人材が教育のために割くことのできる時間は限られており、両者のバランスの中でカリキュラムを設計する必要がある。

本調査では第４章に示すカリキュラムについて、次の条件のもとで設計することとした。

- 短時間での集中講座としても受講者が多くの内容を習得することが困難と見込まれることから、週１回、１回あたり 90 分～120 分程度の講座を 1～3 か月にわたって実施することを前提とする。
- 講義については予習・復習として各 2 時間程度の自習を組み合わせることを前提とすることで、限られた講義で多くの内容を学べるように配慮する。
- 独学での習得が相対的に難しいと考えられる内容を中心に構成する。特に、今後戦略マネジメント層を担うことが見込まれる人材において、業務遂行の上で十分に理解されていないと想定される IT の基礎知識や脆弱性の理解などに関する内容を積極的に盛り込むこととする。
- 座学形式の講義のほかに、受講者に実際に手を動かしてもらうことで学習効果を高めるハンズオン形式の演習を組み合わせる。

（２）到達目標と他カリキュラムとの組み合わせについて

（１）の要件をもとに作成されたカリキュラムは、いずれも３．３．３（２）に示したサイバーセキュリティに関する知識・スキルに関する要件を満たすことを目的としている。しかしながら、サイバーセキュリティに関する知識・スキルの習得の難易度は、前提としての IT に関する知識・スキルを受講者がどの程度保有しているかに依存すると見込まれるため、受講者の IT に関する知識・スキルがカリキュラムの前提を満たすほど高くない場合は、カリキュラムを受講し、必要な予復習を行ったとしても期待する到達目標に至らない可能性もある。このような場合は、あらかじめ IT についての知識・スキルを高めるカリキュラムと組み合わせることが考えられる。具体的には、サイバーセキュリティに関する教育内容との関連から、次のような内容が想定される。

- OS の動作原理
- システム管理技術
- インターネットの仕組みと関係機関

調査結果からの考察

戦略マネジメント層の人材像や知識・スキル、カリキュラムの検討において考慮すべき事項は次の通りである。

- 組織体制：
  サイバーセキュリティに関するリスクマネジメントをどの部署で扱うべきか
- 役割や人材像：
  採用する基準、人材がどのような役割を担うべきか、企業に適した兼務の方法など
- 習得すべき知識・スキル：
  企業の類型や求める知識・スキルの程度
- カリキュラム：
  到達目標と他カリキュラムとの組み合わせ

４．役割と人材像、要求されるスキル、具体的なカリキュラム

前章までの検討結果をもとに、企業においてサイバーセキュリティ対策に従事する人材を対象に、役割、人材像、要求されるスキル及び具体的なカリキュラムについて、２．１に示す 4 種類の層別に整理する。ただし、このうち経営層については、NISC において別途 WG での議論を通じて検討を進めていることから、本項における検討の対象外とする。

４．１ 戦略マネジメント層

４．１．１ 求められる役割

企業の特徴に応じて、次のような役割を担う人材として想定する。

（１）通常時

① サイバーセキュリティリスクの把握

経営戦略、事業戦略におけるサイバーセキュリティリスクを把握し、価値創造とリスクマネジメントの中核を担う。

② リスクへの対策の立案・指揮

マネジメントの範囲におけるサイバーセキュリティリスクを認識し、そのリスクに対し、経営層の方針を踏まえた対策を立案、様々な役割を担う実務者・技術者を指揮し、経営層に報告する役割を担う。

（具体的な役割のイメージ）
- ・事業影響が生ずるサイバーセキュリティリスクの洗い出しの指示
- ・適切なセキュリティ対策予算の確保
- ・ベンダーの選定の判断
- ・外部委託先との契約時におけるセキュリティ対策の確認
- ・法令・諸制度対応の確認
- ・セキュリティルールの策定指示、確認
- ・セキュリティ対策の状況を経営層にわかりやすく報告

（２）緊急時対応

① インシデントの事業影響についての推定

システム担当等との情報共有をもとに発生したインシデントの経営・事業に対する影響範囲と影響の内容について概括的な把握を行う。

② 対策の立案、経営層への報告・協議

インシデントへの対応案を作成し、経営層による判断を支援する。

４．１．２ 想定されるキャリアパス

戦略マネジメント層については、経営企画部門や事業部門等のマネジメントラインにおいて、キャリアパスを歩み、現時点でそれらの部門でマネジメントに携わっている人材を対象としている。そういった人材が、様々な課題に対するマネジメントを行う中でのひとつの要素として、サイバーセキュリティ関連のリスクに起因する脅威に対するマネジメントも行うことが期待される。なお、一般的に類型２の企業によく見られる傾向として、事業部門等を含めたサイバーセキュリティのマネジメントに関し、IT 部門（情報システム部門）が集約して担当するケースがある。その場合においては、少なくとも経営企画部門や各事業部門との緊密な連携・コミュニケーションや、それらの部門に対するガバナンスの確保が必要である。さらに、IT 部門（情報システム部門）の当該人材は、その部門だけの経験ではなく、経営企画部門や事業部門の経験を有していることが望ましい。

現在国内企業等でリスクマネジメント関連の業務に従事する人材のうち、IT リスクマネジメントの担当者を除くと IT に関する知識・スキルが十分でない人材が多いと見込まれることから、現状では上述したようなキャリアパスはあまり存在しないと想定されるが、企業におけるリスクマネジメントを統合的に実施する上ではこうしたキャリアを有する人材は有用であり、当該業務を担う人材にとっても事業戦略に携わる経験から有望なキャリアになると考えられる。企業ヒアリング調査の結果、サイバーセキュリティに専門性を有する要員とのチームワークにより必要な要件を満たすことは可能との意見も得られている。ただし、こうした専門性を有する人材と情報交換や共有を図るために必要な IT に関する最低限の知識については、第 4 章に示すようなカリキュラムの受講等を通じてあらかじめ習得する必要がある。

４．１．３ 求められる知識・スキル

３.３.３における検討結果をもとに、戦略マネジメント層に求められる具体的な知識・スキルの一覧を表 33 及び表 34 に示す。これらの表に示した知識・スキルは、同人材がサイバーセキュリティを含むリスクマネジメントを担うために必要となるものを、第２章及び第３章における検討結果に基づいて抽出したものである。

３.２（２）に示す企業の類型との対応関係は次の通りである。

- 類型１の企業：表 33 及び表 34 の両方の知識・スキルが必要
- 類型２の企業：表 33 の知識・スキルが必要

類型１に相当する、IT を事業の柱としている企業においては、事業戦略の立案を担う人材が併せてサイバーセキュリティのリスクも検討できる知識・スキルを備えることが望ましいことから、表 34 に整理する事業戦略のための知識・スキルを追加する形となっている。

表 33　すべての企業において戦略マネジメント層に求められる知識・スキル

プロセス（ISO 31000 項目抜粋）			サイバーセキュリティ関連スキル（①～⑤は対応する講義回）	外部委託先に求める役割	ITSS+専門分野
リスクマネジメント	コミュニケーション及び協議	異なる領域の専門知識の収集	・サイバーセキュリティに関する脅威や対策一般についての情報収集に関するスキル② ・専門家とのサイバーセキュリティに関するコミュニケーションスキル④	（外部委託を想定しない）	・情報リスクストラテジ ・CSIRT リエゾン
		多様なステークホルダの見解の考慮	・ユーザがシステムやサービスに求める機能要件の理解①	（外部委託を想定しない）	
		組織内外との継続的協議	・同業他社のセキュリティレベルについて情報収集し、自社レベルと比較できるスキル（①～⑤の総合力） ・関係する部署や外部機関の把握、関係構築及び維持に関するスキル ・持続的な連絡体制の構築・維持に関するスキル④	（外部委託を想定しない）	
	組織の状況の確定	考慮すべき外部要因の確定	・サイバーセキュリティの関連法令・規格・ガイドライン等の理解③	（外部委託を想定しない）	・情報リスクストラテジ
		考慮すべき内部要因の確定	・組織におけるビジネスモデル、ビジネス上のプライオリティ、経営層の関心事項並びに IT 利活用状況の理解	（外部委託を想定しない）	
		リスクマネジメントプロセスの全体管理・調整	・サイバーセキュリティに関連したリスクマネジメントの手法に関する理解④ ・サイバーセキュリティ対策実施に伴う組織内調整に関するスキル④	（外部委託を想定しない）	
		リスクに関する許容レベルの設定	・サイバーセキュリティリスクが組織にもたらす影響についての理解④	（外部委託を想定しない）	
	リスクアセスメント	リスクの特定	・組織の目的についての理解 ・組織のビジネスモデル及びそれを実現するための仕組みの理解 ・サイバーセキュリティをとりまく最新の脅威についての理解②	・リサーチャー	・情報セキュリティアナリシス
		リスクの分析	・脅威、脆弱性、対策の有効性についての理解② ・業務プロセスの分析と標準化に関するスキル ・リスク分析のフレームワークに関する理解④	・ソリューションアナリスト ・脆弱性診断士	
		リスクの評価	・脅威が組織にどのような影響を及ぼすかの評価に関するスキル②	・ソリューションアナリスト ・コンサルタント	
	リスク対応	リスク対応策の選定	・選択し得る対策についての情報収集に関するスキル② ・対策についての費用対効果も含めた評価に関するスキル⑤ ・関連法令・規格・ガイドライン等との整合性確保に関するスキル③	・ソリューションアナリスト ・キュレーター	・情報リスクストラテジ ・情報セキュリティデザイン ・CSIRT キュレーション
		対応計画の準備及び実践	・対策が有効に機能する環境や条件についての理解②	（外部委託を想定しない）	
			・自社要員にて行うべき対応と外部委託が可能な対応の違いについての理解	（外部委託を想定しない）	
			・外部委託先において対策を遵守させるための実践に関するスキル	（外部委託を想定しない）	
	意思決定への適用*	記録を通じた明示	・意思決定者が理解できるようにリスクを可視化するスキル④	（外部委託を想定しない）	・情報リスクストラテジ

プロセス（ISO 31000 項目抜粋）			サイバーセキュリティ関連スキル（①～⑤は対応する講義回）	外部委託先に求める役割	ITSS+専門分野
	アカウンタビリティ*	役割及び責任の明確化	・サイバーセキュリティ対策を担う要員の役割定義に関するスキル④	（外部委託を想定しない）	
リスクマネジメント	モニタリング 及びレビュー	リスクの監視	・監視結果からインシデントの発生可能性を判断するスキル②	・ソリューションアナリスト	・情報セキュリティアナリシス
		リスクの変化や新リスクの検出	・サイバーセキュリティ分野を対象とするリスクセンス ・サイバーセキュリティのトピックスの収集に関するスキル②	・リサーチャー	
		リスクマネジメントの監査	・ルールの遵守状況についての監査に関するスキル④	・情報セキュリティ監査人	・情報セキュリティ監査
	継続的改善*	組織のパフォーマンス到達目標を用いた改善	・モニタリング結果に基づく改善可能箇所の検出に関するスキル ・改善案の策定と組織内合意形成に関するスキル④	・コンサルタント	・情報リスクストラテジ
	統治体制への統合*	組織の方針への反映	・事業リスクの一部としてサイバーセキュリティに関するリスクを包括的に管理するためのスキル④⑤	（外部委託を想定しない）	
	緊急時対応への 事前の備え	対応手順の策定及び準備	・インシデント対応手順に反映すべき内容についての理解④	・コンサルタント	・CSIRT コマンド ・CSIRT キュレーション
		緊急時実行組織の整備	・組織に求められる CSIRT の要件に関する理解④	（外部委託を想定しない）	
		緊急時対策及び復旧対策の評価	・インシデント対応の実績の把握と評価を行うスキル④	・ソリューションアナリスト	

*：ISO 31000 にて「高度リスクマネジメント」に定義されているプロセス

表 34　類型 1 の企業において戦略マネジメント層に求められる知識・スキル

プロセス		サイバーセキュリティ関連スキル（①～⑤は対応する講義回）	外部委託先に求める役割	ITSS+専門分野
事業戦略	事業の企画・立案	・企画している事業に対し、犯罪者や不正を意図する者がどのような行為を企てるかを想定するスキル② ・企画している事業を遂行する上での影響が見込まれるサイバーセキュリティ関連リスクの洗い出し、影響評価に関するスキル④	・コンサルタント	・情報リスクストラテジ
	市場調査（顧客ニーズ調査、需要予測、競合分析等）	・需要等を踏まえたサイバーセキュリティ関連リスクの定量的評価に関するスキル④ ・サイバーセキュリティに関する市場ニーズの把握に関するスキル⑤ ・競合企業におけるサイバーセキュリティ対策の実施状況の調査、推定に関するスキル	・コンサルタント	・情報リスクストラテジ
	収益計画策定（マネタイズモデル、収益予測、投資計画等）	・事業計画に応じたサイバーセキュリティ対策の初期投資、ランニングコスト等の概算に関するスキル⑤	・コンサルタント	・情報リスクストラテジ
	事業モデル策定（実施体制、内部化・外部化、パートナー選定、連携計画等）	・事業の実施モデルに応じたサイバーセキュリティ対策の選定に関するスキル②	・コンサルタント ・ソリューションアナリスト	・情報セキュリティアドミニストレーション
	事業実施戦略策定（実現方式・運用方針等）	・実現方式に応じた適切なサイバーセキュリティ対策の選定に関するスキル② ・対策を通じたリスクの低減、移転等の効果の評価に関するスキル④ ・サイバーセキュリティ対策の費用対効果分析に関するスキル⑤	・コンサルタント ・ソリューションアナリスト	・情報セキュリティアドミニストレーション

４．１．４ 育成のためのカリキュラム

前項に示した知識・スキルを習得するためのカリキュラムとして、４．１．２（１）の「リスクマネジメントの業務経験を有する人材がサイバーセキュリティ対策を担当」する場合に必要な知識・スキルを習得する場合に受講することを想定した全５回のカリキュラムを次表に示す。

表 35　戦略マネジメント機能を担う人材育成のためのカリキュラム例

目的	企業等における事業戦略の企画・立案責任者が、事業戦略そのものに必要なサイバーセキュリティ対策を組み込む（例えば、セキュリティを考慮したビジネス設計や適切な外部委託）ために求められる、専門ベンダとのコミュニケーションやリスク評価及び対応体制の構築のための知識・スキルを習得する。		
前提知識・経験	企業等において事業やプロジェクトの管理経験を有する者。ITリテラシーは一般ユーザレベルで可。企業経営に近い部署や業務の経験を有することが望ましい。		
	スクーリング内容	説明	実施方法
第１回	サイバー空間を理解するための基礎知識（基礎知識がある場合にはスキップしても構わない）	サイバーセキュリティの全体像を把握するとともに、サイバーセキュリティ上のリスクを理解するために必要となる、以下の基礎知識を理解することで、サイバーセキュリティの専門家とのコミュニケーションに必要なリテラシーを習得する。 (1) 人類とIT（腕木通信から5G、量子コンピューティングまで） (2) サイバー空間と社会（国家、政治、企業、テクノロジー、国民） (3) コンピュータ理論（OSを中心に）、情報通信ネットワーク理論 (4) インターネットの基本原理（ウェブ、電子メール、eコマース、クラウド） (5) サイバーセキュリティの要素技術（暗号と電子署名、認証、アクセス制御）	予習 2 時間 講義 90 分 宿題 2 時間
第２回	サイバー空間における脅威と対策	サイバー空間における主要な脅威を事業上のリスクとして適切に把握することができるよう、脅威及び脆弱性とその対策に関する以下の事項について学ぶ。 (1) 脅威の関係主体（利用者過失、犯罪組織等） (2) 不正・悪用の歴史・トレンドと考え方、犯罪心理 (3) 脅威と対策に関する情報収集の考え方と方法論・基本動作 (4) 脅威のトレンド（サイバーセキュリティに関わる過去の主要な事故やトラブル） (5) 脆弱性と対策（脆弱性の原理と対策方法、性能や利便性とのトレードオフ）	予習 2 時間 講義 90 分 （場合によっては、90×2 分） 宿題 2 時間
第３回	サイバーセキュリティに関連する法令・規格・諸制度	サイバーセキュリティ確保のために事業者が遵守すべき事項や、効果的な対策実現のために参照すべき制度等について学ぶ。 (1) 法令・規格・諸制度対応の考え方と方法論・基本動作 (2) 関連法令（不正アクセス禁止法、不正競争防止法、個人情報保護法、EU 一般データ保護規則（GDPR）等） (3) 規格・標準・ガイドライン（ISO 31000、ISO/IEC 27000 シリーズ、SP-800.171 等） (4) その他（クラウドサービスにおける約款、サイバーセキュリティ保険、インターネットの関係機関）	予習 2 時間 講義 90 分 宿題 2 時間
第４回	サイバーセキュリティに関連するリスクマネジメントの方法	リスクマネジメントを行う上でのサイバーセキュリティ分野の特殊性について認識した上で、リスクを許容レベル以下に抑制するための方法について、グループワークによる演習を通じて学ぶ。 (1) リスクマネジメントの基本的考え方と方法論・基本動作 (2) サイバーセキュリティリスクに関連するリスクの評価方法 (3) (2)で評価したリスクについての低減、回避、保有、移転の方法 (4) 体制構築（組織内での連絡・共有体制の整備・維持、外部専門家の活用等） (5) インシデント対応プロセス（異常検知、サービス停止の判断、復旧等）	予習 2 時間 講義 30 分＋ 演習 60 分 宿題 2 時間
第５回	企業価値向上とサイバーセキュリティ	事業においてITが担う役割が大きな企業ほど、サイバーセキュリティ対策を含めた形で適切にリスク管理されたサービスを提供することが企業価値の向上につながることを認識し、サイバーセキュリティ対策が予め組み込まれた事業戦略を企画立案するための方法について、グループワークによる演習を通じて学ぶ。 (1) 企業価値とサイバーセキュリティの基本的考え方と方法論・基本動作 (2) 企業価値への影響を考慮した費用対効果分析に基づくサイバーセキュリティ投資の考え方 (3) セキュリティ品質とブランド戦略・顧客との信頼醸成 (4) セキュリティ対策の証明と情報発信	予習 2 時間 講義 30 分＋ 演習 60 分 宿題 2 時間

実施にあたっての条件を次に示す。

- 予習・宿題のボリュームが大きいことから、１～２日での集中開催は困難であり、週１回以上の間隔を開け、１～２か月での開催が適切である。各回の開催日を連続させないことで、受講者が学習した内容を記憶に定着させる効果が期待できる。
- 想定する受講者のポジションとして、自ら経営判断をする立場にはないが、経営者に対して説明したり、経営者が判断するための資料を作成したりする必要があり、経営課題について十分な認識を行う必要があることを想定する。
- １回目と２回目の講義においては、板書形式の講義は一切行わない（必要な知識は予習で身に付けることを前提とする）。講義においては、コンピュータとネットワークを実際に使い、手を動かし、目で見ながら身に付けることを基本とする。
- ３回目～５回目の講義においても、板書形式の講義は一切行わない（必要な知識は予習で身に付けることを前提とする）。講義においては実際のケースを使いながら、ディスカッションないしは共同作業形式を中心として実施するものとする。
- 第１回の「サイバー空間を理解するための基礎知識」の講義では、サイバーセキュリティに関する脅威と対策の基本的事項を理解するために必要な情報技術に関する知識を集中的に学習させるものである。情報系の学習経験のない受講者を対象とする場合、「コンピュータの原理」などから入るのではなく、日常目にするサービスやアプリケーションの説明を導入とした上で、その原理を説明するなどの工夫が必要と想定される。５．１において示すように、我が国では情報技術に関する基礎知識を大学等で習得している人材が少ないと見込まれることから、第１回講義で用いる教材に海外の類似内容のものを用いることはできず、今後新たに作成することが必要である。
- 第２回以降については、企業におけるリスクマネジメントについてある程度の経験を有することを前提に、サイバーセキュリティ固有の事情について説明するものである。
- 第４～５回では、リスクマネジメントの実践に必要なスキルについて、演習形式を併用して学習するものであり、受講者が関心をもつテーマで演習を行うことで効果が高まることが期待される。

４．２ システム担当（実務者層）

４．２．１ 求められる役割

企業の特徴に応じて、次のような役割を担う人材として想定する。

（１）通常時

① 情報システムの潜在的なリスクの把握・共有

組織で利用する情報システムの潜在的なサイバーセキュリティリスクを把握し、関係者で共有する。

② セキュリティ対策の企画・検討

戦略マネジメント層による方針のもと、①で把握したリスクを許容範囲内で抑制するためのセキュリティ対策案の企画・検討を行う。

（２）緊急時対応

① インシデントの組織内システムへの影響についての特定

戦略マネジメント層やシステム運用担当等との情報共有をもとに、発生したインシデントの影響範囲と影響の内容について特定する。

② 各システムにおける対応案に関する関係者との協議

ワークアラウンドでの対策を含め、①で特定したインシデントへの対応案を作成し、戦略マネジメント層やシステム運用担当、外部ベンダ等関係者等と協議する。

（３）既存の役割・専門分野との対応

「システム担当」を担う人材の役割は、次ページ表に挙げる過去に定義された役割や専門分野に相当するが、企業の IT 活用状況、業種、規模、事業部の構成等によって変わってくる。共通するのは、組織で管理する IT 基盤やサービスの利用に伴うリスクへの対策に関する責任を担うことと考えられる。

表 36　システム担当に相当する役割・専門分野

文献	役割・専門分野名称	業務内容
産業横断検討会 [文献 1]	システム部門責任者	情報システム部門におけるサイバーセキュリティ機能を担う。（詳細な内容は、[文献 1]において人材定義リファレンスにおける機能との対応表として定義されている）
	システム管理者	
	ネットワーク管理者	
	CSIRT 責任者	
	ISMS 担当	
	システム企画担当	
SecBoK [文献 7]	IT企画部門	社内のIT利用に関する企画・立案を行う。必要に応じて、ITの利用状況の調査・分析等を行う。
ITSS+ [文献 6]	情報セキュリティデザイン	「セキュリティバイデザイン」の観点から情報システムのセキュリティを担保するためのアーキテクチャやポリシーの設計を行うとともに、これを実現するために必要な組織、ルール、プロセス等の整備・構築を支援する。
	情報セキュリティアドミニストレーション	組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むとともに、対策の立案や実施（指示・統括）、その見直し等を通じて、自組織または受託先における情報セキュリティ対策の具体化や実施を統括する。また、利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する。
	情報セキュリティアナリシス	情報セキュリティ対策の現状に関するアセスメントを実施し、あるべき姿とのギャップ分析をもとにリスクを評価した上で、自組織または受託先の事業計画に合わせて導入すべきソリューションを検討する。導入されたソリューションの有効性を確認し、改善計画に反映する。
NCA [文献 3]	ソリューションアナリスト	自組織の事業計画に合わせてセキュリティ戦略を策定する。現在の状況とあるべき姿の Fit&Gap 分析からリスク評価を行い、ソリューションマップを作成して導入を推進する。導入されたソリューションの有効性を確認し、経営層と情報共有を行い、改善計画に反映する。
NICE 人材フレームワーク [文献 13]	情報システムセキュリティ管理者	プログラム、組織、システム等におけるサイバーセキュリティ対策に責任を負う。
	ITプロジェクトマネージャー	情報技術関連プロジェクトを直接管理する。

さらに、３．１で課題として示した内容を踏まえ、システム担当の役割を定義するにあたり、今後は次のような役割も求められていくと考えられる。

- IoT ほか新たな技術について理解するとともに、その導入に伴うサイバーセキュリティ関連のリスクと対策について検討する（最新の IT 技術の把握）
- DevOps など新たなシステム開発の形態に対応したサイバーセキュリティ対策を検討する（最新のシステム構築・運用技術の把握）
- ビジネス部門での IT 利活用に関するサイバーセキュリティ対策やインシデント対応体制の構築の支援を行う（専門人材以外とのコミュニケーション）

４．２．２ 想定されるキャリアパス

「システム担当」を担う人材については、いわゆるユーザ系の企業の場合、次のようなキャリアパスが想定される。

① 情報システム部門内での実践を通じたスキル向上

概ね情報システム部門内での OJT を通じて、業務に必要となるサイバーセキュリティ関連の知識・スキルを向上させていくキャリアパスである。自社内であまり経験する機会のなく、スキル向上が図りにくい分野については、外部の研修やトレーニング等を活用することも必要となる。

② 情報システムベンダや情報セキュリティサービスベンダで経験を積んだ人材

企業が利用する IT 基盤のサイバーセキュリティ対策に関して、ベンダの立場で経験を積んだ上でユーザ企業に活躍の場を移すキャリアパスである。現状では国内において専門性の高い人材がベンダに偏る傾向があり、こうしたキャリアパスを経ている人材は少ないが、ユーザ企業における専門人材の必要性が意識されることで、今後比率が高まる可能性がある。

４．２．３ 求められる知識・スキル

システム担当に求められるスキルとして、文献調査において調査対象とした ITSS＋及び SecBoK におけるシステム担当相当の専門分野・役割として定められている知識・スキル項目を示す。

表 37　ITSS+におけるシステム担当人材に求められる知識・スキル（[文献 6]より抜粋）

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S110010060	メソドロジ	（戦略） 市場機会の評価と選定	最新技術動向把握の手法	◎		
S110050030			技術開発計画	○		
S110050040			技術開発戦略の立案	○		
S110060010		（戦略） システム戦略立案手法	システム化戦略手法	◎	○	
S110060020			システム活用促進・評価	◎	○	
S110060030			ソリューションビジネス	◎	○	
S110060040			業務プロセス	◎	○	
S110060050			現行システムの調査・分析手法	◎	○	
S110060060			事業戦略の把握・分析の手法	◎	○	
S110060070			情報システム戦略	◎	○	
S110080010		（戦略） 業務動向把握手法	業務動向の把握手法	◎	◎	
S120010010		（企画） システム企画立案手法	システム化計画	◎		
S120010020			システム企画立案手法	◎	○	
S120010030			ソリューション提案手法		○	
S120010040			技術問題解決手法	◎		
S120010050			調達計画・実施	◎		
S120020020		（企画） セールス事務管理手法	契約事務手法		○	
S120030010		（企画） 要求分析手法	要求の抽出手法	◎		○
S120030020			要求の整理手法	◎		○
S120030030			要求の仕様化手法	◎		○
S120030040			要求の評価手法	◎		○
S120030050			要件定義	◎		○
S120040010		（企画） 非機能要件設計手法	プラットフォーム要件定義手法	◎		
S120040020			システム基盤の非機能要件設計	◎		
S130010010		（実装） アーキテクチャ設計手法	アーキテクチャ設計手法	◎		○
S130010020			アプリケーションアーキテクチャ設計手法	◎		
S130010030			インダストリパッケージ設計・開発手法	◎		
S130010040			インフラストラクチャアーキテクチャ設計手法	◎		○
S130010050			データアーキテクチャ設計手法	◎		
S130020010		（実装） ソフトウェアエンジニアリング手法	セキュリティ実装手法	◎		
S130020020			ソフトウェアデザイン手法	◎		
S130020030			ソフトウェアのモデリング手法	◎		
S130020040			ソフトウェア開発手法	◎		○
S130020050			ソフトウェア製作手法	◎		○

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S130020060			ソフトウェア設計の表記手法	◎		
S130020090			ソフトウェア設計手法	◎		
S130060010		（実装） 業務パッケージ活用手法	業務パッケージ適用手法		◎	
S130060020			業務パッケージ導入手法		◎	
S130090010		（実装） 見積り手法	規模の見積手法	◎		
S140020020			サービス移行手法			○
S140040010		（利活用） サービスの運用	サービスの運用手法		○	○
S140040020			システム運用管理手法		○	○
S140040040			運用オペレーション手法		○	
S140040050			運用支援ツール手法		○	○
S150010010		（支援活動） 品質マネジメント手法	テスト技術・手法	◎		○
S150010020			テストのマネジメント手法	◎		○
S150010030			品質レビュー手法	◎		
S150010040			検査のマネジメント手法	◎		○
S150010050			品質マネジメント手法	◎		○
S150010060			品質に関する基礎	◎		○
S150010070			セキュリティ品質に関する手法	◎	◎	◎
S150010080			ユーザビリティ品質に関する手法	◎		
S150010090			セーフティ品質に関する手法	◎		
S150010100			法的権利・法的責任のマネジメント手法	◎		
S150010110			品質要求分析手法	◎		○
S150010120			品質マネジメントシステム構築手法	◎		
S150010130			品質改善に関する手法			○
S150010140			品質管理に関する手法	◎		○
S150010150			品質計画に関する手法			○
S150010160			品質保証に関する手法	◎		○
S150010170			品質測定・評価手法	◎		○
S150010180			品質分析・評価手法	◎		○
S150030010		（支援活動） リスクマネジメント手法	リスク管理手法	○	◎	○
S150030020			情報セキュリティ管理手法	◎	◎	○
S150040010		（支援活動） IT ガバナンス	IT ガバナンス手法	○	◎	
S150040020			内部統制	○	◎	○
S150070010		（支援活動） ファシリティマネジメント手法	ファシリティマネジメント		○	
S150080010		（支援活動） 事業継続計画	BCP 策定手法		◎	
S150080020			災害対策管理手法		◎	
S150100010		（支援活動） 標準化・再利用手法	ソフトウェア開発プロセスの標準化手法	◎		
S150100020			ソフトウェアエンジニアリングの標準化手法	◎		
S150120050		（支援活動） 情報セキュリティ	リスク分析手法	◎	◎	◎
S150120060			情報セキュリティポリシー策定手法	○	◎	◎
S150130010		（支援活動） チェンジマネジメント手法	協働の管理手法	◎		
S150130020			ビジネスソリューション変更管理手法	◎		
S150130030			ソリューション価値測定手法	◎		
S210010010	テクノロジ	（システム） ソフトウェアの基礎技術	ソフトウェア工学			○
S210010020			ソフトウェアの標準化			○

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S210010030			ソフトウェアエンジニアリングツール・開発技術			○
S210010040			ソフトウェア構築の基礎知識			○
S210010100			オープンソースソフトウェア			○
S210010110			テスティング			○
S210010120			ソフトウェア品質			○
S210020010		（システム） ソフトウェアの構築技術	システム開発の概念と方法論			○
S210020020			システム開発のアプローチ			○
S210020030			ソフトウェア要件定義			○
S210020040			ソフトウェア方式設計・ソフトウェア詳細設計			○
S210020050			アプリケーション方式設計手法			○
S210020070			リアルタイムシステム設計			○
S210020080			ソフトウェア開発のフォールトトレランス			○
S210020090			ソフトウェア構築			○
S210020100			ソフトウェア結合・ソフトウェア適格性確認テスト			○
S210020110			受入れ支援			○
S210020140			構築品質			◎
S210020150			テスティングツール			◎
S210020160			セキュアプログラミング技法	◎		◎
S210020170			セキュアプログラミング技法（データベース）	◎		◎
S210030030		（システム） ソフトウェアの利用技術	ソフトウェアの進化や保守			○
S210160010		（システム） ネットワークの基礎技術	ネットワーク	○	○	○
S210160020			ネットワークコンピューティング	○	○	○
S210160030			ネットワークシステムの技術動向	○	○	○
S210160040			ネットワーク標準	○	○	○
S210160050			ネットワーク方式	○	○	○
S210160060			通信プロトコル	○	○	○
S210160070			データ通信と制御		○	○
S210180010		（システム） ネットワークの利用技術	ネットワーク管理	○	○	
S210180020			ネットワーク応用	○	○	
S210180030			ネットワーク製品知識	○	○	
S210180040			業界固有のセキュリティ要件、事例	◎	○	○
S210180050			ネットワークシステムの評価	○	○	○
S210180060			テレコミュニケーション	○		
S210190010		（システム） クラウドコンピューティングの基礎技術	クラウドコンピューティング基礎	◎	○	○
S210200010			クラウドデータベース技術	◎		
S210200020			クラウド構築技術	◎		
S210200030			クラウドアプリケーション実装技術	◎		
S210200040			仮想マシンゲストのセキュリティ		○	○
S210210010		（システム） クラウドコンピューティングの利用技術	インタークラウド技術		○	○
S210210020			クラウドコンピューティング利用	◎	○	○
S210210030			クラウドシステムの監視技術	◎	○	○

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S220010010		（開発） システムアーキテクティング技術	システム要件定義	◎	○	○
S220010020			システムインテグレーションとアーキテクチャ	◎	○	○
S220010030			アプリケーション共通基盤要件定義手法	◎		○
S220010040			アプリケーション共通基盤設計手法	◎		
S220010050			IT 基盤構築プロセス	◎		○
S220010060			システム間連携技術	◎		
S220010070			システム方式設計	◎		
S220010100			オブジェクト指向技術	○		
S220020010		（開発） システム開発管理技術	開発プロセス・手法	○		
S220020020			開発環境管理	○		
S230020080			システムの監視			◎
S230020090			稼働状況管理			◎
S230030050		（保守・運用） システム保守・運用・評価	アプリケーションシステムの受け入れ			○
S230030060			システム運用管理要件定義	○		
S230030070			システム運用管理設計	○		
S230030080			システム運用方式技法	○	○	○
S230030090			システムの投資評価技法	○		
S230030100			システム管理計画	○	○	○
S230030110			システム管理技術	○	○	○
S230030120			システム保守基準	○		○
S230030140			システム管理製品		○	○
S230030150			運用管理ソフト製品		○	○
S230030170			運用システムの改善		○	○
S230030180			運用に関するシステム評価		○	○
S230030190			性能管理		○	
S230030200			障害時運用方式	○	○	
S230030210			災害対策	○	○	
S230030230			保守技術			○
S230030240			メンテナンス			○
S230060040			信頼性、可用性、保守性	○	○	
S230060050			耐震安全確保	○	○	
S230060060			物理ネットワーク（通信ネットワーク）の設計	○	○	
S230060070			防災防犯設備設計	○	○	
S230060100			品質管理の知識	○	○	
S230070010		（保守・運用） サポートセンター基盤技術	インシデント管理システム	○	○	
S240010010		非機能要件（可用性、性能・拡張性）	非機能要件の基礎	○		○
S240010020			負荷分散と可用性の設計	○		
S240010030			システム信頼性、性能設計	○		
S240010040			高信頼性システムの設計	○		
S240010050			データベースシステムの信頼性設計	○		
S240020010		（非機能要件） セキュリティの基礎技術	情報セキュリティ	◎	◎	◎
S240020020			情報保証と情報セキュリティ	◎	◎	◎
S240020030			情報倫理とセキュリティ	◎	◎	○

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティデザイン	情報セキュリティアドミニストレーション	情報セキュリティアナリシス
S240020040			セキュリティ・アーキテクチャ技術	◎	○	○
S240020050			アプリケーションセキュリティ	◎	◎	◎
S240020060			情報プラットフォームのセキュリティ技術	◎	◎	◎
S240020070			ネットワークのセキュリティリスク	◎	◎	◎
S240020080			暗号技術	◎	○	○
S240020090			セキュリティと個人情報	◎	◎	◎
S240020100			保証、信用、信頼のメカニズム	◎	○	
S240020110			セキュリティ技術の理解と活用	◎	◎	◎
S240030010		（非機能要件） セキュリティの構築技術	セキュリティ方針の策定	○	◎	○
S240030020			セキュリティ対策基準の策定	○	◎	○
S240030030			情報セキュリティ対策	◎	◎	○
S240030040			セキュリティ実装技術	◎	◎	○
S240030050			セキュリティシステムの計画策定		◎	○
S240030060			セキュリティシステムの要件定義	◎	◎	○
S240030070			セキュリティシステムの設計	◎	◎	○
S240030080			セキュリティシステムの実装、検査	◎	◎	○
S240030090			コンピュータ・フォレンジクス（証拠保全追跡）		○	○
S240040010		（非機能要件） セキュリティの利用技術	セキュリティシステムの運用管理	○	◎	○
S240040020			セキュリティシステム導入支援		◎	○
S240040030			システム運用・保守技術（セキュリティ）	○	◎	◎
S240040040			セキュリティ障害（事件事故/インシデント）管理	○	◎	◎
S240040050			情報セキュリティ管理	○	◎	○
S240040060			情報セキュリティ監査の実施・支援	○	◎	○
S240040070			セキュリティ技術評価	○	◎	◎
S240040080			セキュリティの分析	○	◎	◎
S240040090			セキュリティの見直し（セキュリティシステムの評価と改善）	○	◎	○
S240040100			コンテンツセキュリティ技術		◎	○
S310020050	関連知識	企業活動	情報セキュリティ監査			○
S310020060			ビジネスプロセスマネジメント	○		
S310030010		法規・基準・標準	セキュリティ関連法規	○	◎	○
S310030020			その他の法律・ガイドライン・技術者倫理	○	◎	○
S310030050			標準化関連	◎		

表 38　SecBoK 2017 におけるシステム担当人材に求められる知識・スキル（[文献 7]より抜粋）

分野	大項目	中項目	小項目
基礎	ICT 基礎	データ構造	適切な情報基盤がもつ性質及び機能に関する知識
		システム開発	システム開発のコンセプトに関するスキル
		システム運用	システム運用のコンセプトに関するスキル
		エンタープライズアーキテクチャ	エンタープライズ IT アーキテクチャに関する知識
			組織のエンタープライズ IT のゴールと目的に関する知識
	工学基礎		技術トレンドデータの妥当性を決定する能力
	ビジネス基礎		関連する情報構造の状態と機能に関する知識
			組織のコアビジネスとミッションの原理に関する知識
			サプライチェーンリスクの削減のための輸出管理規制と責任機関に関する知識
セキュリティ基礎	総論		機密性、完全性、可用性、認証及び否認防止に関連する情報保証の原理と組織要件に関する知識
			サイバーセキュリティ問題に関する外部組織と学術機関に関する知識
セキュリティマネジメント	総論		IT サプライチェーンのセキュリティ/リスクマネジメントのポリシー、要求事項および手続きに関する知識
ネットワークセキュリティ	脆弱性診断		コンピュータネットワーク防御（CND）と脆弱性評価ツール（オープンソースツールとその能力を含む）に関する知識
システムセキュリティ	総論		システムとアプリケーションのセキュリティ上の脅威と脆弱性（例： バッファオーバフロー、モバイルコード、クロスサイトスクリプティング、PL/SQL 及びインジェクション、競合状態、隠れチャネル、リプレイ、リターン指向攻撃、悪意のあるコード）に関する知識
セキュアシステム設計・構築	総論		安全、パフォーマンスおよび信頼性の観点から局所固有となるシステムの要件（例： 標準的な IT を使えない重要インフラシステム）に関する知識
セキュリティ運用	総論		新興の情報技術と情報セキュリティ技術に関する知識
			リスク脅威の評価に関する知識
サイバー攻撃手法	総論		攻撃者に悪用される可能性のある新興のコンピュータベースの技術に関する知識
法・制度・標準	総論		技術トレンドを識別するために有用な業界の指標に関する知識
			活動に影響を及ぼす技術的及び法的なトレンドの追跡と解析に関するスキル
			実施する作業に関する適用法、行政機関のガイドラインおよび/または行政/犯罪に関する法的ガイドラインおよび手続きに関する知識
			重要インフラに影響を及ぼす作業に関連する法律、ポリシー、手続きまたはガバナンスに関する知識

４．２．４ 育成のためのカリキュラム

[文献 10]において提示されているモデル・コア・カリキュラムのうち、例示⑤で示されているものをベースにシステム担当人材向けに調整したものを次表に示す。

表 39　システム担当人材育成のためのカリキュラム例

目的	企業等における IT 基盤の企画管理責任者が、必要なサイバーセキュリティ対策を組み込んだ（例えば、セキュリティを考慮したビジネス設計や適切な外部委託）事業計画を立案するために求められる、サイバーセキュリティの最新動向、リスクマネジメントの考え方及び対応体制の構築などに関する知識・スキルを習得する。
前提知識・経験	企業等における情報システムや IT 基盤の運用実務経験者。情報セキュリティマネジメント試験に合格できる程度のサイバーセキュリティに関する知識を有することが望ましい。

	講義内容	解説	実施方法
第1回	情報セキュリティ基礎知識	情報セキュリティの基本的な概要を学び、現在社会が直面する情報セキュリティ課題と企業活動におけるセキュリティの重要性を理解するために実社会におけるサイバー攻撃の脅威と要因、およびサイバー攻撃対策に必要な考え方について学ぶ。サイバー攻撃への対策では、技術的・物理的な対策から人的・組織的対策まで総合的に取り組むことの重要性を学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第2回	情報セキュリティを支える暗号技術の基礎と応用	暗号技術の基礎として、共通鍵暗号、ハッシュ関数、公開鍵暗号とその応用である電子署名とPKIについて学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第3回	ネットワークを守る認証技術とシステム技術	不正なネットワーク接続を防御するための要素技術を学ぶ。「なりすまし」を防ぐために用いられる認証技術や「なりすまし対策」について紹介し、その効果を理解する。また、広く利用が普及している無線LANとスマートフォンのセキュリティ対策についても学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第4回	企業の情報ネットワークシステムのセキュリティ	企業の情報ネットワークのセキュリティ課題と対応する防御技術としてネットワークの仮想化、侵入検知技術、セキュリティ管理業務と支援システムについて学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第5回	ソフトウェアのセキュリティ課題と対策	ソフトウェアに潜む脆弱性について学ぶ。マルウェアの侵入の手口となるバッファオーバーフローを例に攻撃の仕組みやOSやシステム・ソフトウェアによる対策技術の概要について学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第6回	情報セキュリティマネジメントのフレームワーク	情報セキュリティマネジメントにおける事故事例から情報セキュリティマネジメントの重要性とそのフレームワーク（PDCAサイクル）、インシデント対応時の基本的な考え方等について学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第7回	情報セキュリティのリスクマネジメントとリスクコントロール	情報セキュリティマネジメントにおけるリスクマネジメント手法の概要を学びリスクの分析方法、リスクの評価方法、さらにリスクコントロールについて事例をベースに学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第8回	情報セキュリティの関わる法律と標準化動向の基礎知識	最新のセキュリティ関連の法律について焦点を当てサイバーセキュリティ基本法、不正アクセス禁止法などセキュリティに関係する主要な法律の内容について学ぶ。また情報セキュリティに関連する国際標準とガイドラインの概要とソフトローの役割について学ぶ。	予習 2 時間 講義 90 分 宿題2時間

実施にあたっての条件を次に示す。

- 予習・宿題のボリュームが大きいことから、３～２日での集中開催は困難であり、週１回以上の間隔を開け、２～３か月での開催が適切である。
- 想定する受講者のポジションとして、企業の情報システムや IT 基盤の運用に関して豊富な実績を有する者が、それらのサイバーセキュリティ対策に関する企画・管理を担うために必要な知識・スキルを習得することを想定する。よって、４．１．４とは異なり、カリキュラムに IT の基礎に関する内容は含めていない。
- 本カリキュラムは、CSIRT においてインシデント対応の責任を有するような人材を対象としたものではない。こうした役割を兼ねる人材を対象とする場合は、インシデントレスポンスに関する演習等の時間をカリキュラムに追加することが考えられる。

４．３ システム構築・運用担当（技術者層）

４．３．１ 求められる役割

企業の特徴に応じて、次のような役割を担う人材として想定する。なお、「技術者」層としているが、「主として技術者が担うことを想定している」ことを意味するものであり、企業における技術者が担うべき役割を本担当に限定するものではない。

（１）通常時

① 情報システムの構築におけるセキュリティ要件の設計・開発・実装

「セキュリティバイデザイン」の観点から、組織で利用する情報システムにおけるサイバーセキュリティ対策機能を担保するための要件設計を行うとともに、システム構築時に要件が確実に実装されるように必要な確認を行う。

② 情報システムの脆弱性対応

脆弱性情報を収集し、組織内の情報システムがその影響を受けないように必要な対策を講じる。また情報システムの利用者における脆弱性対策の励行等の啓発を行う。

③ インシデント対応に備えた技術的対策の整備

企業内で検知される攻撃の予兆となる事象や軽微なインシデントへの対処を行い、自社の事業や基盤運用への影響を抑制する。また、大規模なインシデント発生に備えて影響を局所化できるようにするなどの対策を行う。

（２）緊急時対応

① 個別のインシデント対応

戦略マネジメント層やシステム担当等との情報共有をもとに、発生したインシデントによる被害を抑制するために必要な対応を行う。

② 個別のシステムへの影響の調査、関係者への報告

企業内情報システムへの広範囲な影響が避けられないインシデントの場合、今後どのような影響が生ずる恐れがあるか、システム毎の影響を調査し、戦略マネジメント層など関係者に報告する。

（３）既存の役割・専門分野との対応

「システム構築・運用担当」を担う人材の役割は、過去に定義された次表の役割や専門分野に

相当するが、企業における情報システムの運用・管理業務のアウトソーシング状況、業種、規模等によって変わってくる。

表 40　システム構築・運用担当に相当する役割・専門分野

文献	役割・専門分野名称	業務内容
産業横断検討会 [文献 1]	サイバーセキュリティ事件・事故担当	情報システム部門におけるサイバーセキュリティ機能を担う。 （詳細な内容は、[文献 1]において人材定義リファレンスにおける機能との対応表として定義されている）
	セキュリティ設計担当	
	構築系サイバーセキュリティ担当	
	運用系サイバーセキュリティ担当	
	CSIRT 担当	
	SOC 担当	
	基幹システム構築担当	
	基幹システム運用担当	
	WEB サービス担当	
	業務アプリケーション担当	
	インフラ担当	
	サーバ担当	
	DB 担当	
	ネットワーク担当	
	サポート・教育担当	
	ヘルプデスク担当	
SecBoK [文献 7]	ITシステム部門	社内のITプロジェクトを推進するとともに、アプリケーションシステムの設計、構築、運用、保守等を担当する。
ITSS+ [文献 6]	セキュア開発管理	情報システムや製品に関するリスク対応の観点に基づき、機能安全を含む情報セキュリティの側面から、企画・開発・製造・保守などにわたる情報セキュリティライフサイクルを統括し、対策の実施に関する責任をもつ。
	脆弱性診断	ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行い、診断結果の評価を行う。
	CSIRT キュレーション	情報セキュリティインシデントへの対策検討を目的として、セキュリティイベント、脅威や脆弱性情報、攻撃者のプロファイル、国際情勢、メディア動向等に関する情報を収集し、自組織または受託先に適用すべきかの選定を行う。
	インシデントハンドリング	自組織または受託先におけるセキュリティインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携する。情報セキュリティインシデントへの対応状況を管理し、CSIRT コマンドのタスクを担当する者へ報告する。
NCA [文献 3]	リサーチャー	セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メディア情報などを収集し、キュレーターに引き渡す。単独機器の分析は行うが、相関的な分析はしない。
	キュレーター	リサーチャーの収集した情報を分析し、その情報を自組織に適用すべきかの選定を行う。リサーチャーと合わせて SOC（セキュリティオペレーションセンター）で実施することが多い。
	脆弱性診断士	OS、ネットワーク、ミドルウェア、アプリケーションが安全かどうかの検査を行い、診断結果の評価を行う。
	セルフアセスメント担当	自組織環境や情報資産の現状分析を行う。平常時の際にアセスメントを実施しておき、インシデント発生時にはアセスメント結果に基づいて影響範囲を特定する。

文献	役割・専門分野名称	業務内容
	インシデントマネージャー	インシデントハンドラーに指示を出し、インシデントの対応状況を把握する。対応履歴を管理するとともにコマンダーへ状況を報告する。
	インシデントハンドラー	インシデントの処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。状況はインシデントマネージャーに報告する。
NICE 人材フレームワーク [文献 13]	セキュアソフトウェア査定者	新規または既存のコンピュータアプリケーション、ソフトウェア、または特殊ユーティリティプログラムのセキュリティを分析し、実用的な結果を提供する。
	システムセキュリティアナリスト	システムセキュリティの統合、テスト、運用、保守の分析と開発を担当する。
	サイバー防衛インシデント対応者	ネットワーク環境またはエンクレーブ内のサイバーインシデントを調査、分析、および対応する。
	脆弱性診断アナリスト	ネットワーク環境内のシステムとネットワークの評価を実施し、それらのシステム/ネットワークが受け入れ可能な構成、特殊又はローカルなポリシーから逸脱している場所を特定する。既知の脆弱性に対する多層防御アーキテクチャの有効性を評価する。

４．３．２ 想定されるキャリアパス

「システム」を担う人材については、いわゆるユーザ系の企業の場合、次のようなキャリアパスが想定される。

① 情報システム部門内での実践を通じたスキル向上

概ね情報システム部門内での OJT を通じて、構築・運用に必要となるサイバーセキュリティ関連の知識・スキルを向上させていくキャリアパスである。自社内であまり経験する機会のなく、スキル向上が図りにくい分野については、外部の研修やトレーニング等を活用することも必要となる。

② 情報システムベンダや情報セキュリティサービスベンダで経験を積んだ人材

企業が利用する IT 基盤のサイバーセキュリティ対策に関して、ベンダの立場で経験を積んだ上でユーザ企業に活躍の場を移すキャリアパスである。現状では国内において専門性の高い人材がベンダに偏る傾向があり、こうしたキャリアパスを経ている人材は少ないが、ユーザ企業における専門人材の必要性が意識されることで、今後比率が高まる可能性がある。

４．３．３ 求められる知識・スキル

システム構築・運用担当に求められるスキルとして、文献調査において調査対象とした ITSS＋及び SecBoK におけるシステム担当相当の専門分野・役割として定められている知識・スキル項目を示す。

表 41　ITSS+におけるシステム構築・運用に求められる知識・スキル（[文献 6]より抜粋）

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRTキュレーション	インシデントハンドリング
S110010060	メソドロジ	（戦略） 市場機会の評価と選定	最新技術動向把握の手法	◎		◎	
S110050010		（戦略） 製品・サービス開発戦略	顧客環境分析手法	○			
S110050020			製品開発戦略手法	○			
S110050030			技術開発計画	○			
S110050040			技術開発戦略の立案	○			
S110060010		（戦略） システム戦略立案手法	システム化戦略手法	◎			
S110060020			システム活用促進・評価	◎			
S110060030			ソリューションビジネス	◎			
S110060040			業務プロセス	◎			
S110060050			現行システムの調査・分析手法	◎			
S110060060			事業戦略の把握・分析の手法	◎			
S110060070			情報システム戦略	◎			
S110080010		（戦略） 業務動向把握手法	業務動向の把握手法			◎	
S120010020		（企画） システム企画立案手法	システム企画立案手法	○			
S120010030			ソリューション提案手法	○			
S120010040			技術問題解決手法	◎			
S120020020			契約事務手法	○			
S120030010		（企画） 要求分析手法	要求の抽出手法			○	
S120030020			要求の整理手法	○		○	
S120030030			要求の仕様化手法			○	
S120030040			要求の評価手法			○	
S120030050			要件定義			○	
S120040010		（企画） 非機能要件設計手法	プラットフォーム要件定義手法	◎		○	
S120040020			システム基盤の非機能要件設計	◎		○	
S130010010		（実装） アーキテクチャ設計手法	アーキテクチャ設計手法	○		○	
S130010020			アプリケーションアーキテクチャ設計手法	○			
S130010030			インダストリパッケージ設計・開発手法	○			
S130010040			インフラストラクチャアーキテクチャ設計手法	○		○	
S130010050			データアーキテクチャ設計手法	○			
S130020010		（実装） ソフトウェアエンジニアリング手法	セキュリティ実装手法	◎			
S130020020			ソフトウェアデザイン手法	◎			
S130020030			ソフトウェアのモデリング手法	◎			
S130020040			ソフトウェア開発手法	◎			
S130020050			ソフトウェア製作手法	◎			
S130020060			ソフトウェア設計の表記手法	◎			
S130020070			開発プロセス設定手法	◎			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRTキュレーション	インシデントハンドリング
S130020080			開発環境設計手法	◎			
S130020090			ソフトウェア設計手法	◎			
S130060010		（実装） 業務パッケージ活用手法	業務パッケージ適用手法			◎	
S130060020			業務パッケージ導入手法			◎	
S130100010		（実装） プロジェクトマネジメント手法	プロジェクトマネジメント	◎			
S130100020			プロジェクト統合マネジメント	◎			
S130100030			プロジェクトコストマネジメント	◎			
S130100040			プロジェクトコミュニケーションマネジメント	◎			
S130100050			プロジェクトスコープマネジメント	◎			
S130100060			プロジェクトステークホルダマネジメント	◎			
S130100070			プロジェクトタイムマネジメント	◎			
S130100080			プロジェクトリスクマネジメント	◎			
S130100090			プロジェクト資源マネジメント	◎			
S130100100			プロジェクト調達マネジメント	◎			
S130100110			プロジェクト品質マネジメント	◎			
S140020010		（利活用） サービスの設計・移行	サービスの設計手法	○			
S140020020			サービス移行手法	○		○	
S140030010		（利活用） サービスマネジメントプロセス	サービス提供プロセス遂行手法	○			
S140030020			解決プロセス遂行手法	○			
S140030030			統合的制御プロセス遂行手法	○			
S140030040			関係プロセス遂行手法	○			
S140040010		（利活用） サービスの運用	サービスの運用手法			○	○
S140040020			システム運用管理手法			○	○
S140040050			運用支援ツール手法			○	○
S150010010		（支援活動） 品質マネジメント手法	テスト技術・手法	◎	◎	○	
S150010020			テストのマネジメント手法	◎	◎	○	
S150010030			品質レビュー手法	◎			
S150010040			検査のマネジメント手法	◎	◎	○	
S150010050			品質マネジメント手法	◎	○	○	
S150010060			品質に関する基礎	◎	○	○	
S150010070			セキュリティ品質に関する手法	◎	○	◎	
S150010080			ユーザビリティ品質に関する手法	◎			
S150010090			セーフティ品質に関する手法	◎			
S150010100			法的権利・法的責任のマネジメント手法	◎			
S150010110			品質要求分析手法	◎	○	○	
S150010120			品質マネジメントシステム構築手法	◎			
S150010130			品質改善に関する手法	◎	○	○	
S150010140			品質管理に関する手法	◎	○	○	
S150010150			品質計画に関する手法	◎	○	○	
S150010160			品質保証に関する手法	◎	○	○	
S150010170			品質測定・評価手法	◎	○	○	
S150010180			品質分析・評価手法	◎	○	○	
S150030010		（支援活動） リスクマネジメント手法	リスク管理手法	◎	○	○	
S150030020			情報セキュリティ管理手法	◎	○	○	
S150100010		（支援活動） 標準化・再利用手法	ソフトウェア開発プロセスの標準化手法	◎			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRTキュレーション	インシデントハンドリング
S150100020			ソフトウェアエンジニアリングの標準化手法	◎			
S150120050		（支援活動） 情報セキュリティ	リスク分析手法	◎	◎	◎	
S150120060			情報セキュリティポリシー策定手法	○		○	
S210010010	テクノロジ	（システム） ソフトウェアの基礎技術	ソフトウェア工学	◎			
S210010020			ソフトウェアの標準化	◎			
S210010030			ソフトウェアエンジニアリングツール・開発技術	◎			
S210010040			ソフトウェア構築の基礎知識	◎			
S210010050			ソフトウェア設計の基礎知識	◎			
S210010060			プログラミング基礎技術	◎			
S210010070			プログラミング	◎			
S210010080			プログラム言語	◎			
S210010090			その他の言語	◎			
S210010100			オープンソースソフトウェア	◎			
S210010110			テスティング	◎			
S210010120			ソフトウェア品質	◎			
S210020010		（システム） ソフトウェアの構築技術	システム開発の概念と方法論	◎			
S210020020			システム開発のアプローチ	◎			
S210020030			ソフトウェア要件定義	◎			
S210020040			ソフトウェア方式設計・ソフトウェア詳細設計	◎			
S210020050			アプリケーション方式設計手法	◎			
S210020060			アプリケーション設計	◎			
S210020070			リアルタイムシステム設計	◎			
S210020080			ソフトウェア開発のフォールトトレランス	◎			
S210020090			ソフトウェア構築	◎			
S210020100			ソフトウェア結合・ソフトウェア適格性確認テスト	◎			
S210020110			受入れ支援	◎			
S210020120			開発ツール	◎	○		
S210020130			再利用のための構築	◎			
S210020140			構築品質	◎	◎	○	
S210020150			テスティングツール	◎	◎		
S210020160			セキュアプログラミング技法	◎	◎		
S210020170			セキュアプログラミング技法（データベース）	◎	◎		
S210030010		（システム） ソフトウェアの利用技術	アプリケーション計画	○			
S210030020			既存ソフトウェアの把握技法	○			
S210030030			ソフトウェアの進化や保守	○			
S210030040			業務パッケージ最新動向	○			
S210030050			インテリジェントシステム	○			
S210040010		（システム） Web システムの基礎技術	Web システムとその技術	○			
S210040020			サーバ技術	○			
S210040030			インターネットアプリケーション基盤技術	○			
S210040040			アプリケーションサービス	○			
S210040050			アプリケーション実行方式	○			
S210050010		（システム） Web システムの構築	Web アプリケーション技術	○			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRTキュレーション	インシデントハンドリング
S210050020		技術	分散コンピューティング開発環境	○			
S210060010		（システム） Web システムの基礎技術	Web システムとその技術	○			
S210070010		（システム） データベースの基礎技術	データベース	○			
S210070020			リレーショナルモデル	○			
S210070030			データベース方式	○			
S210070040			データ操作	○			
S210070050			トランザクション処理	○			
S210070060			SQL	○			
S210070070			情報管理	○			
S210080010		（システム） データベースの構築技術	データベースの要件定義	○			
S210080020			データベース設計	○			
S210080030			データベースマネジメントシステム（DBMS）の選定・導入	○			
S210080040			データベースシステムの受け入れ	○			
S210080050			データベースマネジメントシステム（DBMS）への実装とテスト	○			
S210080060			データベース開発における重要技術	○			
S210090010		（システム） データベースの利用技術	データのオペレーション管理技術	○			
S210090020			データのセキュリティ管理技術	○			
S210090030			データベースシステム管理	○			
S210090040			データベース運用技術	○			
S210090050			データベース運用設計	○			
S210090060			データアクセスサービス設計技術	○			
S210090070			データクオリティ管理技術	○			
S210090080			データと情報の管理	○			
S210090090			データベース応用	○			
S210090100			データベース関連製品の利用技術	○			
S210090110			データベースの周辺技術	○			
S210090120			データベース診断技術とチューニング技術	○			
S210090130			データ移行	○			
S210090140			データ移行設計	○			
S210090150			データ統合サービス設計技術	○			
S210090160			マスタデータ管理技術	○			
S210090170			ドキュメントとコンテンツ管理技術	○			
S210090180			情報製品の設計技術	○			
S210090190			データ照会・加工・クレンジング技術	○			
S210090200			データマイニングツールの利用技術	○			
S210100010		（システム） プラットフォームの基礎技術	オペレーティングシステム	○			
S210100020			ミドルウェア	○			
S210100030			プラットフォーム技術	○			
S210110010		（システム） プラットフォームの構築技術	IT アーキテクチャ（ソフトウェア）	○			
S210110020			プラットフォーム実装技術	○			
S210110030			共通基盤としてのプラットフォーム設計構築	○			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRTキュレーション	インシデントハンドリング
S210120010		（システム） プラットフォームの利用技術	システムプラットフォームの受け入れ	○			
S210120020			システム診断技術と障害対策技術	○			
S210120030			プラットフォームシステム管理	○			
S210120040			製品知識（プラットフォーム）	○			
S210130010		（システム） ハードウェアの基礎技術	ハードウェア	○			
S210140010		（システム） ハードウェアの構築技術	IT アーキテクチャ（ハードウェア）	○			
S210160010		（システム） ネットワークの基礎技術	ネットワーク	○		○	
S210160020			ネットワークコンピューティング	○		○	
S210160030			ネットワークシステムの技術動向	○		○	
S210160040			ネットワーク標準	○		○	
S210160050			ネットワーク方式	○		○	
S210160060			通信プロトコル	○		○	
S210160070			データ通信と制御			○	
S210180010		（システム） ネットワークの利用技術	ネットワーク管理			○	
S210180020			ネットワーク応用			○	
S210180030			ネットワーク製品知識			○	
S210180040			業界固有のセキュリティ要件、事例	○		○	
S210180050			ネットワークシステムの評価			○	
S210190010		（システム） クラウドコンピューティングの基礎技術	クラウドコンピューティング基礎	○		○	
S210200010		（システム） クラウドコンピューティングの構築技術	クラウドデータベース技術	○			
S210200020			クラウド構築技術	○			
S210200030			クラウドアプリケーション実装技術	○			
S210200040			仮想マシンゲストのセキュリティ	○	○	○	○
S210210010		（システム） クラウドコンピューティングの利用技術	インタークラウド技術	○		○	
S210210020			クラウドコンピューティング利用	○		○	
S210210030			クラウドシステムの監視技術	○		○	
S220010010		（開発） システムアーキテクティング技術	システム要件定義	◎		○	
S220010020			システムインテグレーションとアーキテクチャ	◎		○	
S220010030			アプリケーション共通基盤要件定義手法	◎		○	
S220010040			アプリケーション共通基盤設計手法	◎			
S220010050			IT 基盤構築プロセス	◎		○	
S220010060			システム間連携技術	◎			
S220010070			システム方式設計	◎			
S220010080			システム結合・システム適格性確認テスト	◎			
S220010090			導入	◎			
S220010100			オブジェクト指向技術	◎			
S220010110			ファイルシステム	◎			
S220010120			フレームワーク要素技術	◎			
S220020010		（開発） システム開発管理技術	開発プロセス・手法	◎			
S220020020			開発環境管理	◎			
S220020030			知的財産適用管理	◎			

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRTキュレーション	インシデントハンドリング
S220020040			構成管理・変更管理	◎			
S230020080		（保守・運用） IT サービスオペレーション技術	システムの監視			○	○
S230020090			稼働状況管理			○	
S230030010		（保守・運用） システム保守・運用・評価	移行設計	◎		○	
S230030020			移行	◎		○	
S230030030			プラットフォーム移行設計	◎		○	
S230030040			プラットフォーム移行	◎		○	
S230030050			アプリケーションシステムの受け入れ	◎		○	
S230030060			システム運用管理要件定義	◎			
S230030070			システム運用管理設計	◎			
S230030080			システム運用方式技法	◎		○	○
S230030090			システムの投資評価技法	◎			
S230030100			システム管理計画	◎		○	○
S230030110			システム管理技術	◎		○	○
S230030120			システム保守基準	◎		○	
S230030130			運行管理	○		○	
S230030140			システム管理製品	○		○	○
S230030150			運用管理ソフト製品			○	○
S230030160			運用システムの構築			○	
S230030170			運用システムの改善			○	○
S230030180			運用に関するシステム評価			○	○
S230030190			性能管理	○		○	
S230030200			障害時運用方式	○		○	○
S230030210			災害対策	○		○	○
S230030220			構成管理	○		○	
S230030230			保守技術	○		○	
S230030240			メンテナンス	○		○	
S230030250			保守・廃棄			○	
S230060040		（保守・運用） ファシリティ設計技術	信頼性、可用性、保守性			○	
S230060050			耐震安全確保			○	
S230060060			物理ネットワーク（通信ネットワーク）の設計			○	
S230060070			防災防犯設備設計			○	
S230060100			品質管理の知識			○	
S230070010		（保守・運用） サポートセンター基盤技術	インシデント管理システム	○		○	○
S240010010		非機能要件（可用性、性能・拡張性）	非機能要件の基礎	○		○	
S240010020			負荷分散と可用性の設計	○		○	
S240010030			システム信頼性、性能設計	○		○	
S240010040			高信頼性システムの設計	○			
S240010050			データベースシステムの信頼性設計	○			
S240020010		（非機能要件） セキュリティの基礎技術	情報セキュリティ	◎	◎	◎	◎
S240020020			情報保証と情報セキュリティ	◎	○	◎	○
S240020030			情報倫理とセキュリティ	○	○	○	○
S240020040			セキュリティ・アーキテクチャ技術	◎	○	◎	
S240020050			アプリケーションセキュリティ	◎	◎	◎	○
S240020060			情報プラットフォームのセキュリティ技術	◎	◎	◎	○

スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	セキュア開発管理	脆弱性診断	CSIRTキュレーション	インシデントハンドリング
S240020070			ネットワークのセキュリティリスク	◎	◎	◎	○
S240020080			暗号技術	○	◎	◎	○
S240020090			セキュリティと個人情報	◎	○	◎	○
S240020100			保証、信用、信頼のメカニズム	○		○	○
S240020110			セキュリティ技術の理解と活用	◎	○	◎	○
S240030010		（非機能要件） セキュリティの構築技術	セキュリティ方針の策定	◎		○	○
S240030020			セキュリティ対策基準の策定	◎	○	○	○
S240030030			情報セキュリティ対策	◎	○	○	○
S240030040			セキュリティ実装技術	◎	◎	◎	
S240030050			セキュリティシステムの計画策定	◎	○	◎	○
S240030060			セキュリティシステムの要件定義	◎	○	◎	○
S240030070			セキュリティシステムの設計	◎	○	◎	
S240030080			セキュリティシステムの実装、検査	◎	◎	◎	
S240030090			コンピュータ・フォレンジクス（証拠保全追跡）	○	○	○	○
S240040010		（非機能要件） セキュリティの利用技術	セキュリティシステムの運用管理	○	○	◎	◎
S240040020			セキュリティシステム導入支援	○	○	◎	
S240040030			システム運用・保守技術（セキュリティ）	○	○	◎	○
S240040040			セキュリティ障害（事件事故/インシデント）管理	○	○	◎	◎
S240040050			情報セキュリティ管理	○	○	◎	○
S240040060			情報セキュリティ監査の実施・支援	○	○	○	○
S240040070			セキュリティ技術評価	○	○	◎	○
S240040080			セキュリティの分析	○	○	◎	○
S240040090			セキュリティの見直し（セキュリティシステムの評価と改善）	○	○	◎	○
S240040100			コンテンツセキュリティ技術	○	○	◎	○
S310020050	関連知識	企業活動	情報セキュリティ監査	○		○	○
S310030010		法規・基準・標準	セキュリティ関連法規	○		○	
S310030020			その他の法律・ガイドライン・技術者倫理	○		○	
S310030030			知的財産権	○			
S310030040			労働関連・取引関連法規	◎			
S310030050			標準化関連	◎		◎	

表 42　SecBoK 2017 における IT システム部門に求められる知識・スキル（[文献 6]より抜粋）

分野	大項目	中項目	小項目
基礎	ICT 基礎	ネットワークインフラ	通信方式（例： Bluetooth、RFID、赤外線通信、Wi-Fi、ポケットベル、携帯電話、衛星受信アンテナ）および好ましくない情報の通信を可能とする、またはインストールされたシステムの正しい運用を妨げるジャミング技術に関する知識
		通信プロトコル・サービス	ネットワークプロトコル（例： TCP/IP、DHCP）およびディレクトリサービス（例; DNS）に関する知識
			ネットワークを通じてトラフィックがどのように流れるか（例： TCP/IP、OSI、ITIL）に関する知識
			VoIP に関する知識
		システム開発	システム開発のコンセプトに関するスキル
		システム運用	システム運用のコンセプトに関するスキル
			データバックアップ、バックアップの種類（フル、インクリメンタル）及び復元コンセプトとツールに関する知識
	工学基礎		全5レベルにおける CMMI に関する知識
セキュリティ基礎	総論		機密性、完全性、可用性、認証及び否認防止に関連する情報保証の原理と組織要件に関する知識
セキュリティマネジメント	総論		コンピュータネットワーク防御（CND）のポリシー、手続きおよび規制に関する知識
ネットワークセキュリティ	総論		ネットワーク通信のセキュア化に関するスキル
			何がネットワーク攻撃及び脅威と脆弱性の双方への関係を構成するかに関する知識
			トポロジー、プロトコル、構成要素及び原理を含むネットワークセキュリティアーキテクチャのコンセプト（例：深層防御のアプリケーション）に関する知識
	トラフィック解析		ネットワークトラフィック解析手法に関する知識
			パケットレベル解析に関する知識
	侵入検知		IDS ツールとアプリケーションに関する知識
			IDS のハードウェアとソフトウェアの種類に関する知識
			センサのチューニングに関するスキル
	フィルタリング		ウェブフィルタリング技術に関する知識
	アクセス制御		ホスト／ネットワークのアクセス制御（例：アクセス制御リスト）に関する知識
			ホスト／ネットワークアクセス制御（例： アクセス制御リスト）の適用に関するスキル
	VPN		VPN セキュリティに関する知識
			VPN 装置と暗号化の利用に関するスキル
システムセキュリティ	総論		システムとアプリケーションのセキュリティ上の脅威と脆弱性（例： バッファオーバフロー、モバイルコード、クロスサイトスクリプティング、PL/SQL 及びインジェクション、競合状態、隠れチャネル、リプレイ、リターン指向攻撃、悪意のあるコード）に関する知識
セキュリティ運用	インシデント対応		インシデントレスポンスとハンドリングの方法論に関する知識
			インシデントハンドリング手法の利用に関するスキル
			インシデントに関連したネットワークセキュリティの報告のためのプロセスに関する知識
サイバー攻撃手法	マルウェア		マルウェアからのネットワークの保護に関するスキル

４．３．４ 育成のためのカリキュラム

[文献 10]において提示されているモデル・コア・カリキュラムのうち、例示⑤で示されているものをベースにシステム構築とシステム運用をそれぞれ担う人材向けに調整したものを示す。

（１）システム構築担当向け

主にシステム構築を担う人材向けに調整したものを次表に示す。

表 43　システム構築担当人材育成のためのカリキュラム例

目的	企業等における情報システムの構築担当者が、必要なサイバーセキュリティ対策を組み込んだ情報システムの設計・構築を行うために求められる、サイバーセキュリティの最新動向、リスクマネジメントの考え方及び対応体制の構築などに関する知識・スキルを習得する。
前提知識・経験	企業等における情報システムの構築実務経験者。情報セキュリティマネジメント試験に合格できる程度のサイバーセキュリティに関する知識を有することが望ましい。

	講義内容	解説	実施方法
第１回	情報セキュリティ基礎知識	情報セキュリティの基本的な概要を学び、現在社会が直面する情報セキュリティ課題と企業活動におけるセキュリティの重要性を理解するために実社会におけるサイバー攻撃の脅威と要因、およびサイバー攻撃対策に必要な考え方について学ぶ。サイバー攻撃への対策では、技術的・物理的な対策から人的・組織的対策まで総合的に取り組むことの重要性を学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第２回	セキュリティ要件定義とセキュア開発	セキュリティバイデザインの考え方に基づく企画・設計段階での要件定義の方法、DevSecOpsの考え方、脆弱性を生じにくくするためのセキュアコーディング技術について学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第３回	マルウェア感染及び不正侵入と対処	情報システムの脆弱性を悪用したマルウェア感染や不正侵入について、インシデントの過程においてどのような対策を講じれば影響を抑制できるか等の内容を講義と演習で学ぶ。	予習 2 時間 講義 30 分＋ 演習 60 分 宿題2時間
第４回	企業リスクとリスクマネジメント	情報システムの構築に関わるサイバーセキュリティ事象を対象とするリスクマネジメントについて、グループワークを通じて学ぶ。	予習 2 時間 講義 30 分＋ 演習 60 分 宿題2時間

実施にあたっての条件を次に示す。

- 予習・宿題のボリュームが大きいことから、３～２日での集中開催は困難であり、週１回以上の間隔を開け、２～３か月での開催が適切である。
- 想定する受講者のポジションとして、企業の情報システムや IT 基盤の構築に関して豊富な実績を有する者が、それらのサイバーセキュリティ対策に関する実務を担うために必要な知識・スキルを習得することを想定する。

（２）システム運用担当向け

主にシステム運用を担う人材向けに調整したものを次表に示す。

表 44　システム運用担当人材育成のためのカリキュラム例

目的	企業等における情報システムの運用担当者が、必要なサイバーセキュリティ対策を組み込んだ情報システムの運用やインシデント対応を行うために求められる、サイバーセキュリティの最新動向、リスクマネジメントの考え方及び対応体制の構築などに関する知識・スキルを習得する。
前提知識・経験	企業等における情報システムの運用実務経験者。情報セキュリティマネジメント試験に合格できる程度のサイバーセキュリティに関する知識を有することが望ましい。

	講義内容	解説	実施方法
第1回	情報セキュリティ基礎知識	情報セキュリティの基本的な概要を学び、現在社会が直面する情報セキュリティ課題と企業活動におけるセキュリティの重要性を理解するために実社会におけるサイバー攻撃の脅威と要因、およびサイバー攻撃対策に必要な考え方について学ぶ。サイバー攻撃への対策では、技術的・物理的な対策から人的・組織的対策まで総合的に取り組むことの重要性を学ぶ。	予習 2 時間 講義 90 分 宿題2時間
第2回	セキュリティ監視と運用	情報システムやサービスの運用に関して、異常や不正アクセスを検知するための技術やサービスについて学ぶとともに、運用上の誤検知や検知漏れなどが生ずることを前提に適切に運用する方法について理解する。	予習 2 時間 講義 90 分 宿題2時間
第3回	CSIRT 業務とインシデント対応	CSIRTの実務について事例をもとに学習した上で、インシデント対応演習をグループワークで実施する。	予習 2 時間 講義 30 分＋ 演習 60 分 宿題2時間
第4回	企業リスクとリスクマネジメント	情報システムの構築に関わるサイバーセキュリティ事象を対象とするリスクマネジメントについて、グループワークを通じて学ぶ。	予習 2 時間 講義 30 分＋ 演習 60 分 宿題2時間

実施にあたっての条件を次に示す。

- 予習・宿題のボリュームが大きいことから、３～２日での集中開催は困難であり、週１回以上の間隔を開け、２～３か月での開催が適切である。
- 想定する受講者のポジションとして、企業の情報システムや IT 基盤の運用に関して豊富な実績を有する者が、それらのサイバーセキュリティ対策に関する実務を担うために必要な知識・スキルを習得することを想定する。

５．今後の検討事項

本章では、本調査で明らかにした内容を踏まえて、今後検討すべき事項について示す。

５．１ 教材の研究開発の推進

今後解決すべき、最も重要な課題は戦略マネジメント層の育成に適した教材が存在しないことである。通常、IT 人材育成のためのテキストは国内に適切な教材がない場合は海外の同種の教材の翻訳によって提供されていた。しかしながら本調査で示したように、今後国内で戦略マネジメント層を担うことが見込まれる人材は、海外で同様の役割を担う人材と比較して、IT を支える技術的バックグラウンドについての知識・スキルが十分ではないという特徴がある。ゆえにこうした分野に専門性を有するベンダとの分担で対策を検討することになるが、そのためのベンダ側の専門人材とのコミュニケーションに必要となる知識・スキルを学ぶことが優先的な課題となる。また、サイバーセキュリティに関する新たな脅威について把握するために、公的機関から公表される脅威や脆弱性に関する情報について、自分で理解することも必要である。こうした知識・スキルを学ぶ上で、有識者より以下の２点について把握しておくことが重要との指摘がある。

- インターネットの動作に関する基本原理
- ソフトウェアの実行に関する基本原理

これらについてはこれまで十分な背景知識をもたない人材であっても、基本的な知識を習得できるように工夫する必要があり、条件の異なる海外の教材の翻訳では対応できない。そこで、こうした内容を効率的に学習できるような教材の開発を推進する必要がある。

一方、こうした技術の基礎に関する教育とは別に、サイバーセキュリティに関するリスクマネジメントを行うために必要な知識についても学習することが求められる。リスクマネジメントについては対象分野ごとに用語や考え方、準拠するフレームワークなどが異なるため、情報セキュリティ分野に特化して学ぶことが効果的である。理想的には業種毎に簡易な教材を整備することが望まれる。

５．２ 講師の育成

本調査で設定した人材を育成するための教育コース等を設置する場合、その講師の確保も必要となるが、現状では次のような問題がある。

- 大学教員の場合、技術の基礎を教えることには優れているが、実務に直結した内容については経験をもとに教育を行うことができないため、本調査で例示したカリキュラムをすべてカバーすることが困難である。
- IT 系の教育サービスを担当する講師の場合、IT 関連の最新サービスに関する教育等には長けているが、リスクマネジメントにおいて経営上考慮すべき事項については一般論的な内容を教えるにとどまることから、受講者側からすると「本当に知りたいことを教えてもらえない」といった不満が感じられることになりやすい。

そこで、例示したカリキュラムに基づく教育を行う場合、サイバーセキュリティに関する実務経験を豊富に有する産業界講師を活用することが欠かせないと考えられる。一方で、前述のように、リスクマネジメントの手法が産業ごとに異なるような状況では、講師も受講者と同じ業種の方であることが望ましく、結果的にサイバーセキュリティ対策を行う必要のあるすべての業種において、サイバーセキュリティ人材育成のために、現場で活躍している人材に講師としての活動を依頼することになる。講師としての要件を備えたシニア人材が確保可能であればこうした活用が想定されるが、それが難しい場合は多忙な現役の人材に負担を求めることになり、ボランタリーに近い形での依頼では必要数の確保も難しいと見込まれることから、産業界講師本人とその所属企業における講師負担のインセンティブをどうするかについて検討する必要がある。

５．３ 産学官連携に基づく具体的なプログラムの推進

産業界講師が講義の多くを担当する場合、市場で競合している企業が参加する形態も増えることから、教育の場は特定の企業に関連するところではないことが望ましく、産学連携により教育機関において実施することが必然的に求められる。また、前項で示したように講師を提供する企業へのインセンティブ等を考えた場合、官による支援も必要と考えられる。ゆえに今後の人材育成は産学官の連携をもとに推進することが適切と見込まれる。

大学等の高等教育機関は本来、受講者が長期にわたって活用可能な基礎学力を習得させることを目的としているが、最近では「社会人学び直し」など、社会人を対象に実証的教育を行う機会も増えている。本調査で実施する教育も実践的な側面を強化することで効果が高まると期待されることから、産学官の連携環境のもとでこうした実践的教育のノウハウを活用することが望まれる。

なお、本調査において示したカリキュラムにおいて、戦略マネジメント層向けに IT やネットワークに関する基礎知識の教育を含めているが、今後初等中等教育におけるプログラミング教育の実践等を通じて IT に関する基礎的な知識やスキルの習得が若年層の段階でなされていくことが見込まれる。これはサイバーセキュリティの背景となる技術や仕組みを理解する上で有益であり、こうした基礎知識やスキルを習得した人材向けに、より高度な要求に応えることのできる人材の育成を行うことが可能となることが期待される。一方で、サイバーセキュリティに関する理解を高めるための知識・スキルは、単なるツールやプログラミング言語の使い方を身につけるのみといった内容では不十分である。学習指導要領を硬直的に運用するのではなく、コンピュータの動作原理などサイバーセキュリティや IT を司る物事の原理を理解し、論理的思考ができる能力を育てることが重要である。また、サイバーセキュリティに有用な知識や技術を教える際には、興味本位で悪用に走ることのないよう、同時に倫理やモラルに関する教育を行うことが望ましい。

６．おわりに

本調査では、文献調査や企業ヒアリング調査の結果をもとに、企業におけるサイバーセキュリティ対策を効果的に実現する観点から、企業の事業リスクマネジメントの一環としてサイバーセキュリティを管理できるような人材として「戦略マネジメント機能を担う人材」（戦略マネジメント層）を定義し、その人材像や役割を中心に、今後の企業において育成すべき人材の人材像や育成方法に関する明確化を行った。

「Society 5.0」として提唱されている、イノベーションが生み出す人間中心の社会に向け、今後 IT 利活用のモデルがいっそう変化し、それに伴い情報システムやサービスの開発モデルもアジャイル型や DevOps などの動きにとどまらず、大きく変化していくことが見込まれる。これに併せて、サイバー空間における脅威のすがたも変化し、そのセキュリティ対策も現状の延長線上にはない可能性が高い。こうした中で、サイバーセキュリティ人材もよりクリエイティブで、コラボレーションを活発化し、より新技術に貪欲になっていく必要がある、ただし、そのような人材モデルは本調査では整理しきれなかった部分であり、今後の課題である。