資料３－５

サイバーセキュリティ人材育成に向けた産業界としての取り組み

～第二期中間報告書等のご紹介～

- 「産業横断サイバーセキュリティ人材育成検討会」のご紹介
- 「第二期中間報告書」のご紹介
- 「トップ層会合」（2017年11月21日）のご紹介

一般社団法人 サイバーリスク情報センター

産業横断サイバーセキュリティ人材育成検討会

2017年10月30日(月)

本検討会発足の経緯と活動概要

- **経団連配下の「サイバーセキュリティに関する懇談会」の参加メンバー、及び重要インフラ企業を中心とし、2015.6.9に発足。**
- **フェース・トゥ・フェースでの思いや悩みの交換が参加者の意識を醸成。**
- **「信頼の輪」を築きながら人材定義リファレンス等の成果を創出・発信。**
- **活動を通じて関係省庁とも緊密に連携。**

2015.2.17　**経団連から国へ「サイバーセキュリティ対策の強化に向けた提言」**
経団連配下の「サイバーセキュリティに関する懇談会」での議論をインプット

2015.6.9　**「産業横断サイバーセキュリティ人材育成検討会」を立上げ**
重要インフラ分野を中心とした重要な業界に関わる企業約30社

2016.1.14　**「第一期中間報告」を公表**
産業横断 でのサイバーセキュリティ人材育成 に向けた課題を抽出

2016.9.14　**「第一期最終報告」を公表**
産業横断の人材定義リファレンス等を作成

2016.10.17　**「トップ層会合」開催**
経営層の理解・支持を得、産業界主導活動の推進へ

業界横断での取り組みの推進

- 産業横断の取り組みを推進するためには、「信頼の輪」の構築が重要。
- 検討会参加メンバー間（中間層）では構築されつつあり、おおきな成果のひとつ。

ＫＤＤＩ株式会社
JXアイティソリューション株式会社
住友化学株式会社
全日本空輸株式会社
ソニー株式会社
大日本印刷株式会社
株式会社竹中工務店
株式会社ＴＢＳテレビ
株式会社 東芝
トヨタ自動車株式会社
日本生命保険相互会社
日本通運株式会社
日本テレビ放送網株式会社
日本電気株式会社
日本電信電話株式会社

日本放送協会
日本郵政株式会社
株式会社パソナグループ
パナソニック株式会社
株式会社日立製作所
富士通株式会社
株式会社みずほ銀行
三菱重工業株式会社
三菱商事株式会社
三菱電機株式会社
ヤマトホールディングス株式会社
他

本検討会の理念（2017.4.1～）

- 2020年を見据えながら、参加企業ならびに日本のセキュリティ対応力向上に貢献する。
- 相互扶助の精神のもと、重要インフラ企業、ユーザー企業を中心に業界横断の「信頼の輪」を築き、中核に据える人材育成に加え、情報共有や産学連携を推進する。
- 産業界を代表する組織となり、産学官連携により、セキュリティ人材育成・維持のエコシステムの実現を目指す。

本検討会のビジョン（2017.4.1～）

重要インフラをはじめとする社会インフラを支えるIT環境を（局所的な脆弱性のない）統一的なセキュリティ水準とするために！

- 産業界の知恵と経験を結集して（産業界しか創り得ない）サイバーセキュリティ対策のベストプラクティクス※を発信したい。
  ※産業界の視点から実効的な対策と水準を網羅したガイドライン
- 産業界を代表する組織となり、関係省庁等と連携しながら情報を共有するとともに、産業界の視点から意見を発信したい。
- 産業界の視点から、必要な人材像を定義し、育成に必要なカリキュラムやツールを紹介・共有したい。
- 産学連携により、産業界の次代を担う人材の育成に貢献したい。

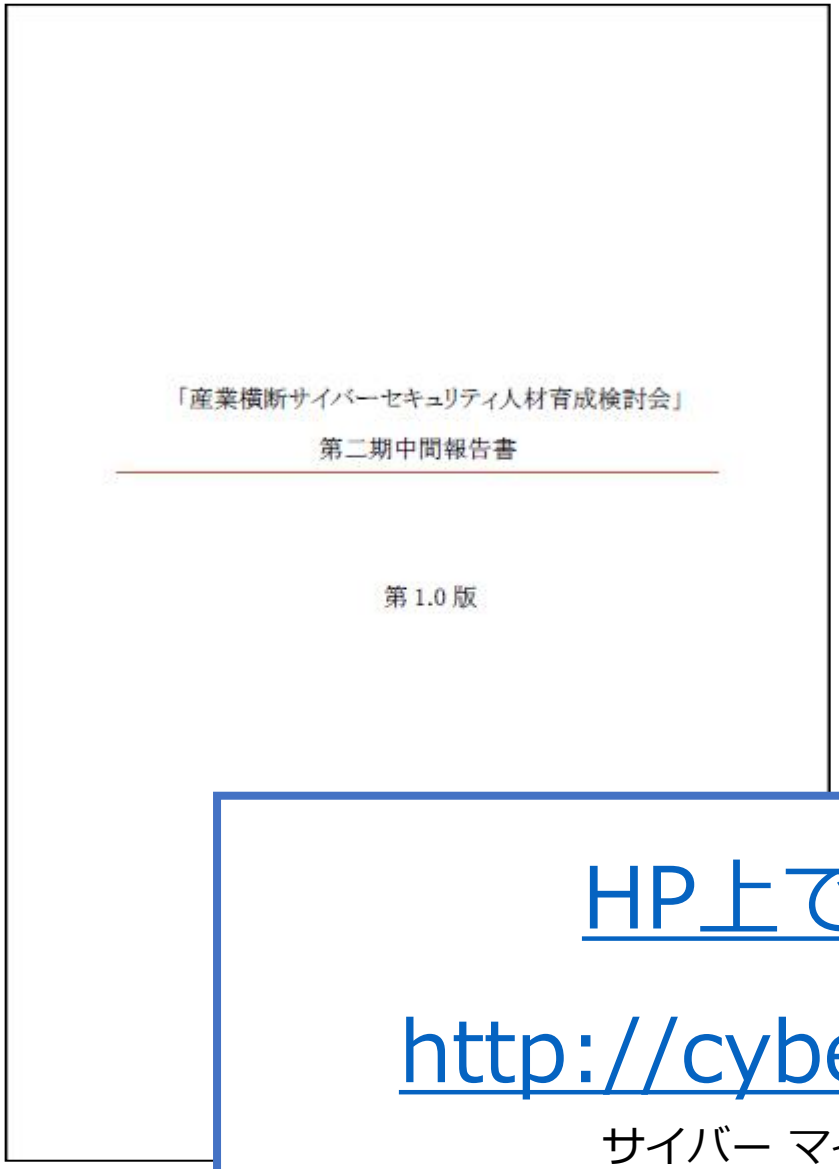
ユーザ企業主導の新体制へ移行（2017.4.1～）

- **制御系含むユーザ企業が活動を牽引する施策を加え、産業横断としての今後の活動方針を刷新。**
- **2017.4.1より、法人格を有するコンソーシアム（既存団体「一般社団法人サイバーリスク情報センター（CRIC）」内に設置）体制に移行**

- **昨年までの成果（人材定義等）を実装展開するWGを立ち上げ（6月）**
  - 必要人材を育成する既存の研修プログラムを収集・共有（DB化し試用中）
  - 業界が必要とする人材（制御系等）への定義拡大
- **“業界横断”を重視した情報共有を推進する新たなWGも立ち上げ（6月）**
  - これまでに築かれた信頼の輪を活用、参加企業の課題解決につながる場を提供
  - 参加企業の知恵を整理・蓄積し、産業界のベストプラクティス策定へつなげる
- **関連団体との関係性も強化、産学官連携エコシステムの具体化に向け加速**
  - 一般社団法人日本経済団体連合会様（賛同団体）
  - 内閣サイバーセキュリティセンター（オブザーバ）

- **これまでの活動を「第二期中間報告書」として公表予定（11月21日）**
  - **経団連様の第三次提言、NISC様の次期サイバーセキュリティ戦略へインプット**
  - **当検討会のトップ層会合（11/21）において、参加企業、招待企業、来賓団体へご紹介**

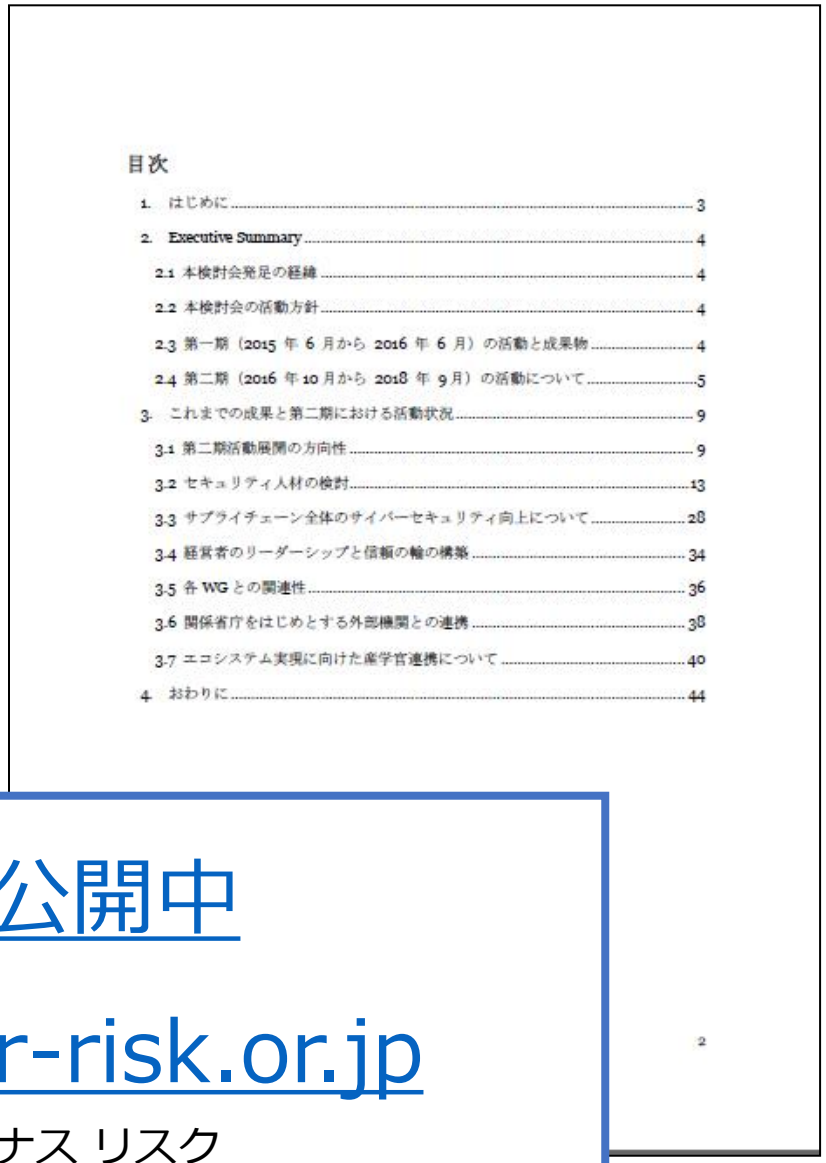
第二期中間報告書



「産業横断サイバーセキュリティ人材育成検討会」

第二期中間報告書

第 1.0 版



目次

2

[HP上で公開中](http://cyber-risk.or.jp)

http://cyber-risk.or.jp

サイバー マイナス リスク

経営層を対象とした「トップ層会合」の開催

サイバーセキュリティの推進には**トップ層、経営層の強いリーダーシップが必須**と考え、**トップ層、経営層の意識醸成**と業界横断の**「信頼の輪」を設ける**べく「トップ層会合」を開催。
（第一回：2016年10月17日、第二回：2017年11月21日）。

#	時刻	時間	議題	発表者（敬称略）
第一部：16:00-17:30				
1	16:00-16:10	10分	●開会の挨拶 ・産業横断活動の必要性、理念、信頼の輪構築・深化・継続	・会長　上野 耕司
2	16:10-16:25	15分	●来賓の紹介（経団連、文科省、JUAS、IPA） ●来賓の挨拶	・司会者 ・NISC 内閣参事官　吉田 恭子
3	16:25-16:40	15分	●活動紹介（計画含む） ・活動内容・成果、活動計画など	・副会長　古田 朋司
4	16:40-17:20	40分	●講演（テーマ：「経営とサイバーセキュリティ」など） 事例①「経営課題としてのサイバーセキュリティ」 事例②「デジタル化の推進とサイバーセキュリティ」	事例①：株式会社日立製作所 情報セキュリティリスク統括本部 サイバーセキュリティ技術本部 本部長 村山 厚 事例②：住友化学株式会社 理事　ＩＴ推進部 土佐 泰夫
5	17:20-17:35	15分	●質疑応答	
6	17:35-17:45	10分	●ラップアップ	・副会長　土佐 泰夫
7	17:45-18:00	15分	トイレ休憩・会場移動	
第二部：18:00-19:30				
8	18:00-19:30	90分	●乾杯	・日本郵政株式会社 執行役副社長　小松 敏秀
			●挨拶	・NISC 内閣審議官　三角 育生
			●中締めの挨拶	・ＪＸアイティソリューション株式会社 代表取締役社長 内田 悟

参考：第一回「トップ層会合」開催模様（2016年10月17日）

- 2016年10月17日、於 経団連館。当検討会メンバ企業38社より計84名が参加。
- 当検討会事務局より、トップ層、経営層幹部に対する活動報告、成果の活用推進に関するお願い、および、今後の取り組み計画を説明。
- メンバ企業代表2社の幹部より、経営課題としてのセキュリティ対策や、重要インフラを担うユーザ系企業としてのサイバーセキュリティに関する取り組みについてプレゼンし、懇親会の場も含め活発な意見交換を行った。

産業横断サイバーセキュリティ人材育成検討会懇談会＆懇親会

2016.10.17（月）於：経団連会館 経団連ホール南/北 開催レポート

産業横断サイバーセキュリティ人材育成検討会　事務局

日本電信電話株式会社
日本電気株式会社
株式会社日立製作所
【事務局組織：一般社団法人サイバーリスク情報センター】

産業横断サイバーセキュリティ人材育成検討会（以下、検討会）は、2015 年 2 月 17 日に日本経済団体連合会から発表された「サイバーセキュリティ対策の強化に向けた提言」を受け、日本電信電話株式会社、日本電気株式会社、株式会社日立製作所の事務局 3 社が、重要インフラ分野を中心とした各業界の主要企業に声掛けし、2015 年 6 月 9 日に発足しました。

本懇談会＆懇親会は、約 1 年間の活動を総括し、より積極的な活動を推し進めるべく、検討会参加企業の経営幹部を集めた情報共有と懇親の機会として開催しました。

【懇談会】

1.開会の挨拶

開会に先立ち、本検討会の立ち上げを行った、日本電信電話株式会社 代表取締役副社長 CTO 兼CISO の篠原より開会の挨拶を行いました。

本懇談会では、2020 年も見据え、
① 産業横断で取り組む必要性（全てがつながる IoT 時代への対応として業種の垣根を越えた連携が必要など）
② 業界横断での取り組みの推進（「信頼の輪」の構築の重要性など）
③ 経営層の理解とリーダーシップ（経営層による産業横断の Trusted Network 立ち上げへ発奮など）
の点を訴求しました。

産業横断サイバーセキュリティ人材育成検討会　事務局

また、業界横断での取り組み推進を行ってきた本検討会に参加されている企業様を一覧にしたプレゼンテーションにより、2015.6.9 に発足して 1 年 3 ヶ月間の活動継続、48 社の参加に対し、感謝の言葉を述べました。

2.活動報告

続いて、事務局の 1 社である日本電信電話株式会社、川村より本検討会のこれまでの活動に関する報告を行いました。
具体的な活動として、
① 民主導でボトムアップに丁寧な議論と情報を推進
② 信頼の輪を産業横断で構築
③ 官や学にも提示できる幾つかの成果物の公表
の点を挙げ、参加企業の継続的な協力に対し、その志に深く感謝を述べました。

本検討会の成果物として「人材定義リファレンス」を中心としたシート類の解説を行い、参加された経営幹部へ次の 2 点をお願いしました。
① 「人材定義リファレンス」等のツール類は、人材の十分性評価、育成や採用の目標設定に役立つ先進的なツールであり、経営マネジメントの一環として導入・活用を推進してほしい。
② 10 月からの新たなステージ（第二期）の開始に際し、検討会メンバの継続的な参加と経営マネジメントとしても支持してほしい。

（配布された第 1 期最終報告書を手に取る参加者の皆さま）
各種リファレンス、ツール類↓

産業横断サイバーセキュリティ人材育成検討会　事務局

↑トップ層会合の会場風景

←メンバ企業各社の全関係者に共有するためのレポートを作成（左図は会合の導入部に関するページ）

別　紙

「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

第 1.0 版

2017 年 11 月 21 日

一般社団法人サイバーリスク情報センター

産業横断サイバーセキュリティ人材育成検討会

本報告書について

本報告書は「産業横断サイバーセキュリティ人材育成検討会」（以下、「本検討会」）の活動に関する 2016 年 7 月から 2017 年 9 月までの内容を纏めた第二期中間報告です。

本検討会に関心のある方々に向けて、本検討会の目的や意義、活動内容等についてご理解いただくことを主な目的としています。

本報告書をお読みいただくにあたり、全体の概要を先ず知りたいという方は第 2 章 Executive Summary を、本検討会の取り組みの全体像を知りたい方は、第 3 章以降をご覧ください。さらには、本検討会に興味のある方は別紙に各 WG の活動アウトプットをご参照ください。

名称　　：一般社団法人サイバーリスク情報センター
　　産業横断サイバーセキュリティ人材育成検討会
英名　　：Cyber Risk Intelligence Center - Cross Sectors Forum
略称　　：CRIC CSF
URL　　：http://cyber-risk.or.jp/

本検討会の第二期中間報告書は、以下の URL からダウンロードが可能です。

http://cyber-risk.or.jp/cric-csf/report/index.html

本報告書についてのお問い合わせは、以下のアドレスまでお願いします。

office@cyber-risk.or.jp

今後とも本検討会の活動に対する継続的なご支援、ご理解を、何卒宜しくお願い申し上げます。

目次

1. はじめに

交通、エネルギー、金融など国民の生活と経済活動の根幹を支える重要インフラは、今や大きく IT に依存している。その一方で、システムの脆弱性や人の心理的な隙をついて攻撃を仕掛けるサイバー攻撃の脅威は、おおきな社会的問題としてクローズアップされている。

本検討会は、第一期（2015 年 6 月から 2016 年 6 月）には日本企業（特にユーザ系企業）における重要インフラ業務に共通するセキュリティ業務と組織構造との関係を把握しながらサイバーセキュリティに係る人材の定義に取り組み「産業横断人材定義リファレンス（機能と業務に基づくセキュリティ人材定義）」等の成果物を策定した。

第二期（2016 年 10 月から 2018 年 9 月）においては、環境の変化として IoT 時代の本格的な到来に伴うサイバー攻撃等の影響の拡大を意識し、以下の 5 つの点を主要な検討ポイントとして丁寧な議論を進めている。

- ✓ *産業界の知恵を結集したベストプラクティクス*
- ✓ *経営者の強いリーダーシップを支える「トップ層会合」と「セキュリティ統括人材」*
- ✓ ***IoT 社会の到来をにらんだ OT（Operational Technology）人材***
- ✓ *関係省庁をはじめとする外部機関との連携*
- ✓ *産学官セキュリティ人材育成エコシステムの実現*

2.Executive Summary

2.1 本検討会発足の経緯

2014 年 10 月、経団連傘下に「サイバーセキュリティに関する懇談会（座長：梶浦敏範氏）」が発足した。そのメンバーでもある日本電信電話株式会社、日本電気株式会社、株式会社日立製作所の 3 社が発起人・事務局となり、2015 年 6 月 9 日に重要インフラ分野を中心とした企業 48 社が結集して本検討会を発足した。

2.2 本検討会の活動方針

2020 年の東京オリンピック・パラリンピックを乗り切り、その先も頑張り続ける産業界としての主体的な活動として推進する。「学」と「官」との連携・協調を含め、あくまでも「産（産業界）」が自主的・主体的に取り組み、自助と共助で様々なセキュリティ問題を乗り越えていく。

2.3 第一期（2015 年 6 月から 2016 年 6 月）の活動と成果物

本検討会は、主にユーザ系企業に共通するセキュリティ業務と組織構造との関係を整理した。その結果、セキュリティ業務（機能）は企業組織内で広範囲に分散している。従って、人材育成のスコープは CSIRT などのセキュリティ専門組織だけでは不十分であるとの結論にいたった。そのうえでサイバーセキュリティに係る人材の定義に取り組み、以下の成果物を設けた。

- ✓ ***産業横断 人材定義リファレンス～機能と業務に基づくセキュリティ人材定義～***
- ✓ ***産業横断 セキュリティ対策カレンダー～セキュリティ対策 A to Z～***
- ✓ ***産業横断 セキュリティオペレーション アウトソーシングガイド***
- ✓ ***産業横断 人材定義リファレンスに基づくスキルマッピング***

2.4 第二期（2016 年 10 月から 2018 年 9 月）の活動について

2.4.1 サイバーセキュリティを取り巻く状況の変化

（1）東京オリンピック・パラリンピックを見据えた横断的なセキュリティ水準確保の必要性

2020 年の東京オリンピック・パラリンピックが成功するには、競技スケジュールの管理や競技の動画配信などの大会運営に加えて、世界中から訪れる観光客を輸送する航空や鉄道、それらを支える電力、ガス、石油などの重要インフラが適切に運営されなくてはならない。一方で、安全管理の分野で盛んに用いられる“The strength of the chain is in the weakest link.「鎖は、もっとも弱いリングで切れる」”のことわざにあるように、大会運営や重要インフラを支える IT に脆弱な部分があると、サイバー攻撃によりおおきなダメージを受けるおそれがある。そうなれば社会的な混乱や不安を引き起こし、ひいては大会運営をおおきく揺るがしかねない。

このような理由から大会運営を支える IT のみならず重要インフラを担う IT には横断的かつ統一的なサイバーセキュリティ水準を確保すべきである。

（2）IoT（Internet Of Things）社会の到来

IDC Japan によると国内の IoT（Internet Of Things）市場は、年率 17%の成長が予想[1]されるという。一方で、あらゆるものがインターネットにつながる IoT 社会が到来すれば、あらゆる機器がインターネットに繋がれ、例えば最適な設備運転を自動的に制御するなど、おおきな利便性や効率化をもたらすであろう。しかしながら IoT を介して制御系システムなどがサイバー攻撃を受ければ、生産計画が狂うのみならず破壊など、人の身体や生命に影響を及ぼす事故につながりかねず、十分な対策を行うのは急務である。

2.4.2 活動の概要

本検討会では、IoT 時代の到来に伴うサイバー攻撃の影響をも意識し、全体会議配下に 4 つの WG のほかトップ層会合、オープンセミナーを配置し、サイバーセキュリティに関する情報共有及び人材育成を進めている。

[1] https://www.idcjapan.co.jp/Press/Current/201704101Apr.html

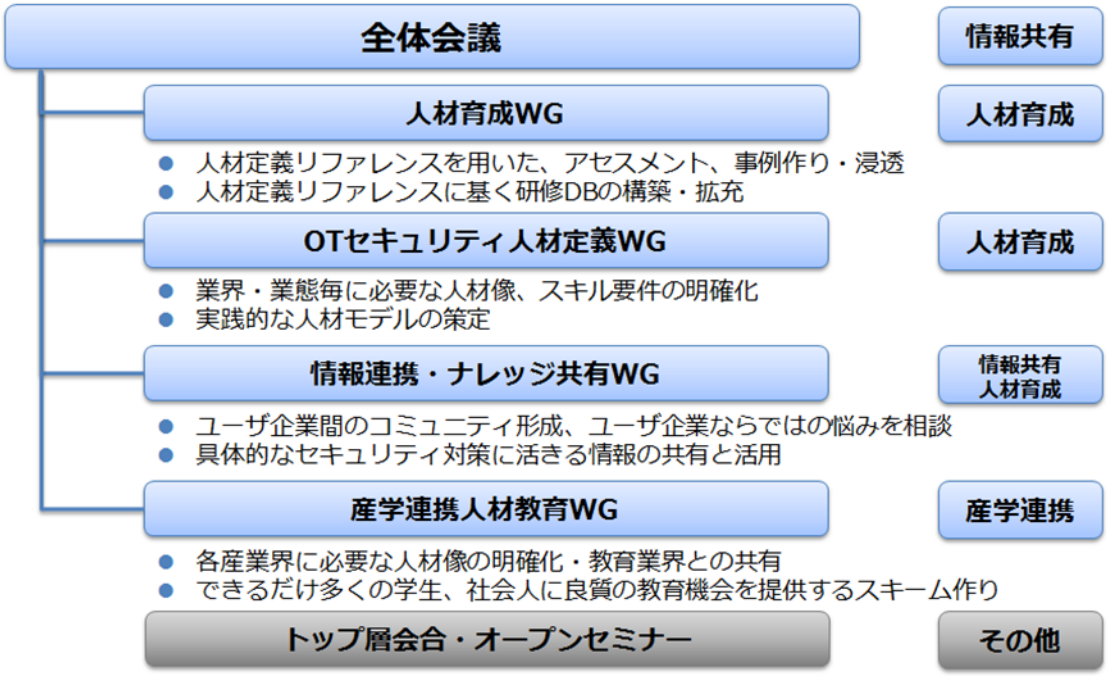


図 2-1　活動の構成

2.4.3 主要検討ポイントそれぞれが活動から得られた方向性

(1) ベストプラクティス策定と経営者のリーダーシップ・信頼の輪の構築

2020 年の東京オリンピック・パラリンピックをにらみ大会運営ならびに重要インフラを担う IT には、横断的かつ統一的なセキュリティ水準を確保する事が求められる。そのためには、「目指すべきセキュリティ水準」を社会的に共有し、個々の経営者が強いリーダーシップを発揮して、系列企業ならびにサプライチェーンのビジネスパートナー等を含めたセキュリティ対策を推進しなくてはならない。

本検討会は、その一助とすべく参加企業のセキュリティ対策の具体的な内容を整理・蓄積したものを産業界のベストプラクティクスとして策定・公開するとともに、経営者自らがセキュリティ対策を「協創領域」という共有価値の創造に向け、経営者を対象とした「トップ層会合」を開催して先進的な事例などを紹介するとともに経営者間の情報・意識交換の推進をはかりたい。

(2) セキュリティ統括人材像の明確化と育成に向けた研修プログラムの整備

前述のように適切なサイバー攻撃対策を推進するには、経営者の強いリーダーシップが不可欠である。しかしながら、その専門的な障壁からセキュリティ方針を設け現

場の納得を得ながら、これをリードするのは難しい。そこで、経営的な知見とサイバー攻撃やネットワークインフラ等の専門的な知見を有して、経営を支援しながら関係部署をリードする「セキュリティ統括人材」の育成が急務である。

このような認識のもとで、その人物像やスキルを明確化するとともに研修データベースの構築などをはかり、実践的な人材育成環境の整備を進めている。

（3）OT（Operational Technology）人材の定義の策定

今後の「あらゆるものがインターネットにつながる」IoT（Internet Of Things）社会が到来すれば、あらゆる機器がインターネットに繋がれ工場内の設備の稼働状況を一元的に入手し、部材の故障予見や最適な装置運転の在り方を検討する事も可能となる。しかしながら、例えば設備を制御するシステムが改ざんされれば、生産計画が狂うのみならず設備自体の破壊など、人の身体や生命に影響を及ぼす事故につながりかねない。

これに加え、前述したような IoT 社会の到来をにらみ、併せて IoT を介した設備などへのサイバー攻撃が及ぼす影響を踏まえると、係る対策の整備は急務である。そこで、本検討会の検討範囲を従来の IT（Information Technology）人材に加えて、社会インフラ・制御システムを担う OT（Operational Technology）人材に拡大した検討第二期より開始し、実績のある OT 活動事例を集めるなど、人材モデルの検証を進めている。

（4）政府機関や関連団体との情報共有を推進する枠組みの策定

今般のサイバー攻撃には、個人による愉快犯的なものから国や組織が政治的動機から標的となる企業等を定めて行うものに変化している。このようななか、個々の企業が逼く政治的動機を持つ国や組織の意図、具体的な手口を知り「これから襲来するおそれのあるサイバー攻撃」に備えるには限界があろう。また過去には特定の業界全体が標的になった事例が多いことから、米国では各業界の ISAC（Information Sharing and Analysis Center：情報共有分析センター）において対策に直結する有益な情報を活発に交換している。

以上を踏まえ、内閣サイバーセキュリティセンターをはじめとする政府機関や関連団体に働きかけ実務的な情報や意見を交換できる枠組みを広げたい。

（5）エコシステム実現に向けた産学連携人材教育の推進

セキュリティ脅威に対抗できる人材の育成スキームを確立し産学官セキュリティ人材育成エコシステム実現を目指すべく、先ずは産業界が求める人材像を明らかにした。そのうえで大学などと連携して、「寄附講座」や企業側から教材と講師を派遣する「出張授業」など多彩な支援のあり方を検討しながら教育機関と密接に連携して、できる限り多くの学生や社会人に良質の教育機会を提供する枠組みを推進する所存である。

2020 年の東京オリンピック・パラリンピックをにらみ、サイバー攻撃は社会的なリスクと認識して「オールジャパン」の観点から推進すべきである。そこで企業の壁を越えた「信頼の輪」のもとに各企業が連携して、互いに知り得た情報や自らの取り組みを交換すべきである。本検討会は産業界の知恵と経験を結集して“産業界しか創り得ない”サイバーセキュリティ対策のガイドラインを発信すると共に、産業界を代表する組織となり、関係省庁等と連携しながら産業界の視点から様々の発信につなげる所存である。引き続き関係各位のご理解とご支援を賜りたい。

3.これまでの成果と第二期における活動状況

3.1 第二期活動展開の方向性

本検討会の第一期活動においては、主として IT 分野のセキュリティ人材の定義を行い、ユーザ企業が IT セキュリティ人材の育成を行うにあたっての目安（ものさし）を成果とした。

第二期活動においては、定義したセキュリティ人材を充足し、また活躍してもらうことがユーザ企業のセキュリティレベルの向上、ひいては自社ビジネスへのサイバー攻撃の影響を最小化することに繋がるという認識のもと、充足・活躍に向けてユーザ企業が具体的な行動に移すことにできるアクションプランの検討に着手した。

さらには、従来の IT（Information　Technology）人材に加えて、社会インフラ・制御システムを担う OT（Operational　Technology）人材に拡大した検討を開始した“セキュリティ人材の充足”という観点においては、育成と併せて雇用やアウトソースをバランスよく行うことが現実的なアプローチとなる。（図 3-1-1）

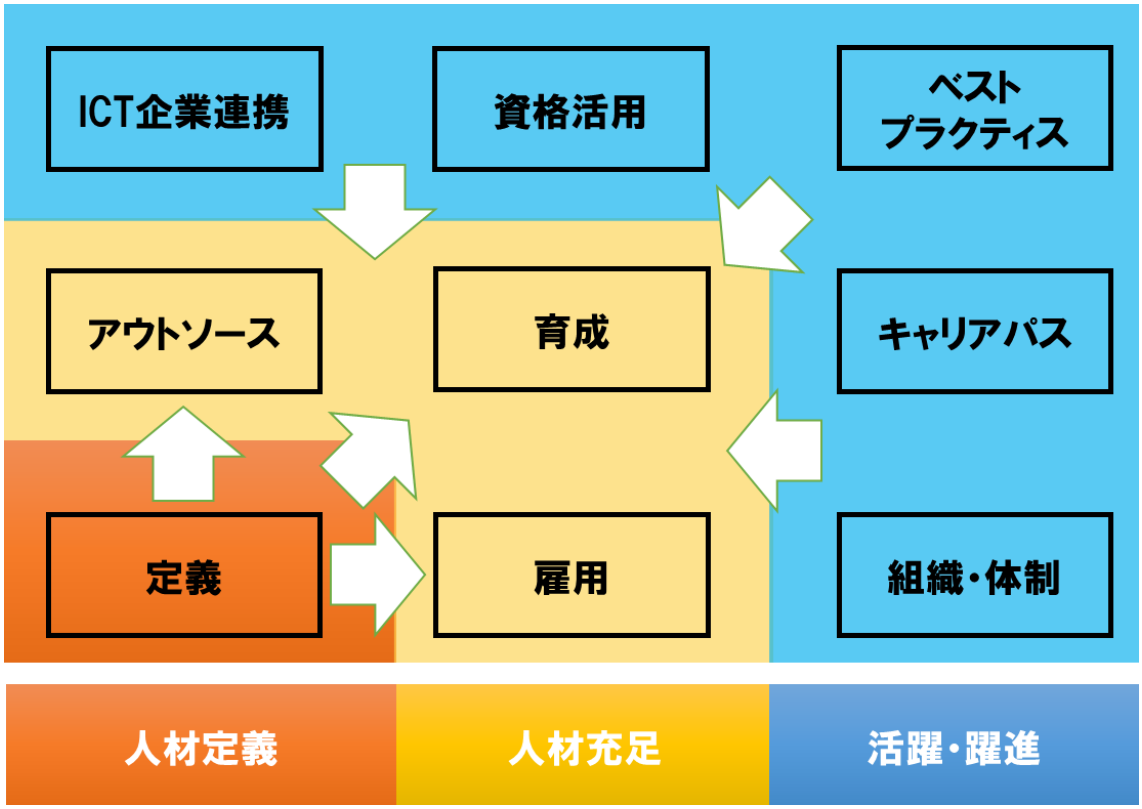


図 3-1-1. 第二期活動展開の方向性

まず育成の観点では、セキュリティ人材のキャリアパスとそれを実現する研修プログラムについて検討する必要がある。キャリアパスが存在することにより、企業は効率的・効果的に人材を育成することができる。どのようなキャリアが次のステップとして考えられ、そのキャリアに必要なスキルがどのようなもので、それをどのような研修プログラムによって身につけるのか、という育成のプロセスは、その企業のキャリアパスを基本として検討・推進されるべきものである。依って立つべきキャリアパスの無いセキュリティ人材育成は、散発的かつ逐次的にならざるをえず、自社に擁すべきセキュリティ人材を計画的・組織的に充足させることは難しい。一方、このキャリアパスを実現する研修プログラムについても検討すべき課題がある。

現在提供されているセキュリティ研修プログラムを概観すると、マルウェアハンドリングやフォレンジックスなどのセキュリティ分析官・オペレータとしての能力を向上させるプログラムが充実している。これらの能力は、セキュリティベンダにて顧客のセキュリティ対処を行うようなセキュリティ専門家向けのプログラムであり、ユーザ企業のセキュリティ人材が受講するようなプログラムでは無い。

ユーザ企業が必要とする研修プログラムを検討し、その開発・提供をセキュリティベンダに要求することが必要である。また、進化し続けるサイバー攻撃に対応可能な研修プログラムの提供においては教育機関への期待も大きい。日進月歩ならぬ秒進分歩であるサイバーセキュリティにおいては、ユーザ企業で活躍する社員に対する学び直しの場を提供することも重要である。

雇用については 2 つの視点で考えることができる。一つは、セキュリティの広範な知識を体系的に取得することができる教育機関の役割の重要性である。進化し続けるサイバー攻撃に対抗するためには、基礎となる広範なセキュリティ知識を体系的に修得したうえで自社のビジネス形態、ワークフローに合わせて最適化することが求められる。そのため、特にユーザ企業においては、自社のビジネス形態やワークフローを深く理解・実践可能な人材が求められ、そのような人材が“セキュリティも”理解することが期待されている。

このような経営に基づいたセキュリティに関する意思決定およびその実行を支援することのできる“セキュリティ統括人材”の重要性はますます増している。セキュリティ統括人材は、企業経営にかかわる全ての側面についてのセキュリティ設計・実行の支援が求められる。セキュリティ統括人材およびそれに至るキャリアパスをたどるための基礎となる広範かつ体系的な知識を身につけた人材の育成には教育機関の貢献が必要不可欠である。

もう一つの視点は、即戦力としてのセキュリティ人材の雇用である。知識と経験を備えた人材を雇用することで、ユーザ企業は短い時間でセキュリティ能力を向上させることができる。様々な経験を積んだセキュリティ人材には、進化し続ける攻撃に対してより適切に対処可能であることが期待できる。

自社の経営の深い理解を元にセキュリティに関する意思決定およびその実行を支援するセキュリティ統括人材と、セキュリティの現場で様々なセキュリティイベントに対して適切かつ迅速にチームを率いて対処を行うことのできる即戦力たるセキュリティ人材とのハイブリッドによって、自社のセキュリティ能力を向上させることがユーザ企業にとってのひとつの形態であろう。

とは言え現実問題として、ユーザ企業が必要となる全てのセキュリティ人材を自社内に保有することは困難であり、アウトソースという選択肢についても考慮する必要がある。

第一期においては、アウトソーシング可能なセキュリティ業務についてガイドラインを示した。セキュリティ対策に割くことのできるリソースが有限である以上、アウトソースを含めたセキュリティ対策の優先度付け、取捨選択は必須となる。この意思決定は自社の経営の深い理解に基づいて行うことが求められる。自社にとってのビジネスリスクの優先度を理解したうえで、その中でのセキュリティの位置づけを明確化し、リスクに対する費用対効果を勘案した要件・レベルに基づいたアウトソースが必要である。このような意思決定はアウトソースすることができない。ユーザ企業自らが意思決定をする必要があり、セキュリティ統括人材がその意思決定を支援することが求められる。育成、雇用、アウトソースというアプローチによって充足されたセキュリティ人材が具体的な行動を起こすことによって、ユーザ企業のセキュリティレベルが向上する。

本検討会では、このセキュリティ人材の活動を支援することも、実効的にセキュリティレベルを向上させるために重要なことと考えている。

ひとつは、組織的・体制的な支援である。サイバーセキュリティが経営課題である以上、セキュリティ人材の活動は企業の様々な側面と関係するため、セキュリティ人材だけで対処することは不可能である。権限やレポートラインを含めた組織的・体制的なバックアップがあることで、セキュリティ人材のスキルを活かすことができる。

いまひとつは、参考となるベストプラクティスの充実である。進化し続けるサイバー攻撃に対し、一企業のセキュリティ人材だけで対処することは非現実的である。他社・他業界の経験やノウハウを積極的に活用することが効果的である。しかしながら、断片的な知識としての経験やノウハウはユーザ企業にとっては、読み解き、実施することは容易では

ない。実例（ストーリー）としてのベストプラクティスはその理解や適用が容易なように作られている。ユーザ企業がそれぞれのセキュリティ能力に応じた具体的なアクションを取るうえで、ベストプラクティスは有効な道しるべとなると考える。そのような、ユーザ企業が活用することのできるベストプラクティスの充実もまた求められている。

一方、前節でも言及した通り、サイバー攻撃の対象はもはや IT だけではない。サイバー攻撃の被害は情報詐取にとどまらず、事業継続そのものに多大なインパクトを与える脅威になってきている。そのようなユーザ企業を取り巻く環境の変化を考えると、ユーザ企業が擁すべきセキュリティ人材のスコープを IT にとどめることはできない。

ビジネス価値を生み出す源泉となる製造・操業・運用などを支える OT へのサイバー攻撃被害を最小化する OT セキュリティや、顧客に提供する製品（Product）に関するセキュリティを管理する製品セキュリティの重要性が喫緊の課題となってきていることを認識すべきである。ユーザ企業を取り巻く環境の変化に応じ、セキュリティ人材が活躍する領域を拡大していく必要がある。（表 3-1-1）

表 3-1-1. 第二期活動展開の進捗状況

	人材定義	人材充足			活躍・躍進				
		育成	雇用	アウトソース	キャリアパス	ﾍﾞｽﾄﾌﾟﾗｸﾃｨｽ	資格活用	組織体制	ICT企業連携
IT領域	○（リファレンス）	活動中（研修DB）	活動中（人材像検討）	○（リファレンス）	活動中（モデル検討）	活動中（事例共有）	検討中	検討中	検討中
OT領域	活動中（事例共有）	今後	今後	今後	今後	今後	今後	今後	今後
PT？	–	–	–	–	–	–	–	–	–
…	–	–	–	–	–	–	–	–	–

3.2 セキュリティ人材の検討

本章では、第一期にセキュリティ人材定義 WG として活動し、第二期途中で人材育成 WG としてリニューアルして議論された内容を報告する。

第一期では、企業におけるセキュリティ人材の定義を検討するにあたって、IT における企業のセキュリティ関連活動を機能として洗い出した。（図 3-2-1）

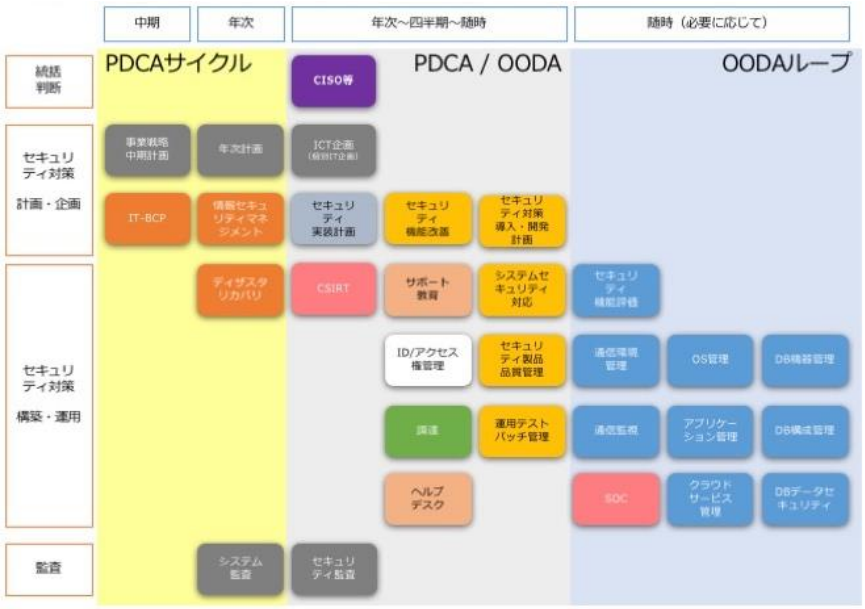


図 3-2-1 サイバーセキュリティ対策の機能定義（関係図）

さらに、それぞれの機能を実施していくために必要な 30 の役割を抽出し、セキュリティ人材定義とした。（表 3-2-1）

セキュリティ人材定義リファレンスは、企業においてサイバーセキュリティ関連活動のある瞬間において必要な役割を示しているが、それらの役割に至るキャリアパスは示していない。

セキュリティ人材に優秀な人材を惹き付けるためには、セキュリティに関わる仕事をしようとする人たちにどのようなキャリアパスがあるのかを示していく必要があるが、本検討会に参加しているユーザ企業の現状から推測すると、ユーザ企業でのセキュリティ関連するキャリアは明確とはなっていない。

表 3-2-1 サイバーセキュリティ機能を担う役割一覧

カテゴリ		役割（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
		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

ユーザ企業がキャリアパスを構築し内部で育成するセキュリティ人材を明確にすることが望まれている。また、そのようなセキュリティ人材を育成するために、どのような教育が必要で、また、どのような経験を踏めばよいかを検討する必要がある。

第二期の人材育成 WG では、企業におけるセキュリティ人材のキャリアパス[2] を 3 つにモデル化し、特に、ユーザ企業のセキュリティ人材の中核として「エキスパート人材（セキュリティ統括人材）」に関する検討を行った。

3.2.1 検討の前提:ユーザ企業の類型

検討の対象となる企業は業態、業界、規模など様々な要因で、その状況は異なっており、キャリアパスもそれに応じて検討する必要がある。今回、全ての企業におけるセキュリティ人材のキャリアパスを一緒に検討することは困難なため、「規模」ならびに「IT と事業の関係性」から企業を分類して議論することとした。第二期のこれまでの議論では、「IT と事業の関係性」で企業を大きく 2 つ類型として検討を行った。それぞれの特性は以下のとおり。

① 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*
- ✓ *情報を主に取り扱い、情報漏洩や改ざんなど、機密性・整合性・可用性（Confidentiality, Integrity, Availability）の順でセキュリティを検討する。*
- ✓ *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*

② 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であり、可用性・整合性・機密性（Availability , Integrity, Confidentiality）の順で検討する。*
- ✓ *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] 3.2 節では、検討の際に実際に使われた「キャリアパス」という用語をそのままの形で使用している。検討を進める中で、キャリアパスは様々なパターンがあり、検討の中で使われている「キャリアパス」という用語は、セキュリティ人材のキャリアとして考えられる 3 つのおおきな領域を示す「キャリア領域」と呼ぶべきではないかと議論があった。本報告書では、検討の際に使われていた「キャリアパス」という用語をそのまま使うこととしたが、将来的には「キャリア領域」に変更する可能性もある。

本検討会では重要インフラ企業からの参加が多く 3.2.1(2)の企業を検討の対象とした。

3.2.1(1)の企業においては、ビジネス開発は IT システム開発を伴うことが多く、DevOps あるいは DevSecOps などといわれるように、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おり、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ていると考え、対象としないこととした。

なお、今回の議論においては、「規模」による企業分類に基づくセキュリティ人材とそのキャリアパスに関しては検討が及ばなかった。「規模」に基づく企業類型では、主に中小企業に対しての検討が主になる。ただし、上記「IT と事業性の関係」、「グループ会社かどうか」、「サプライチェーンへの帰属度合い」などによって、いくつかの類型に分類した上で検討をすることが必要であると考えている。

中小企業の多くでは、セキュリティに専属の人材を設置することや、既存の人材にセキュリティ教育をすることもままならない状況である。セキュリティ人材のキャリアパス以前に、セキュリティ人材不在を前提に、セキュリティ対策を検討すべきという見解もあった。そのため、中小企業におけるサイバーセキュリティ対策については、今後の課題として、別途検討を行うこととした。

3.2.2 セキュリティ人材のキャリアについての考察

本検討会に参加する企業でのセキュリティ人材育成を議論する中で、企業におけるキャリアパスとして、次の 3 つを想定した。

表 3-2-2 セキュリティ人材のキャリアパス

議論での名称	人材のイメージ	現状のキャリアパスとの関係
ゼネラリスト	企業における （ライン）マネジメントを行う人材	管理職のキャリアパス
エキスパート[3]	自社事業とセキュリティ活動をよく 知り、現場と経営をつなぐ人材	技術系企業の技師や技術職などの キャリアパスに類似
スペシャリスト	専門的技術を持った人材	IT/セキュリティベンダ、情報子会社の キャリアパス

3 「エキスパート」という名称については、WG の中でも様々な意見があり、必ずしも適切であるかどうかについては、結論が出ていない。議論を進める上で、ゼネラリストとスペシャリストと区別するための名称が必要であるため、検討の際に利用した名称をそのまま使用している。名称に関する考察は 3.2.3（5）を参照のこと

現状多くの企業においては、複線型人事制度[4]により、ラインマネージャーへの昇格を前提としたキャリアパスのみでなく、専門職としての役割・業務に呼応した職種を設定し、例えば、技術系企業における技師、研究など職種ごとに異なった評価を行い処遇することが行われている。

企業におけるセキュリティ人材も、各部門の管理者として組織運営においてセキュリティ対策に責務を負う役割と、セキュリティと事業の両面についての専門性を持ってセキュリティ関連活動を統括する人材の役割を異なるキャリアパスとすれば、セキュリティ人材に対する複線型人事制度として、現在の各企業における人事制度とうまく整合が取れるのではないかと考えた。また、一方でセキュリティ監視オペレータやフォレンジック技術者などのセキュリティの深い知識と技術を持った人材を、一般のユーザ企業の中で育成し、保持していくことは容易ではなく、その部分については、内製するのではなく、サービスや人的支援を外部から調達することで対応することのほうが現実的であると考えた。

以上の検討から、企業におけるセキュリティ人材のキャリアパスを“**ゼネラリスト**”、“**エキスパート**”、“**スペシャリスト**”の３つとして考えることとした。

これを一般に確立している経理人材のキャリアで例えると、次のようになる。

- ✓ ***経理人材は経理のエキスパートであり、経営者になるキャリアパスがある。***
- ✓ ***スペシャリストとしては会計士がいる。***
- ✓ ***経理部門以外の営業部門も工場も上級管理者は経理の基礎知識は持っていないと困るため、ゼネラリストとして、経理のことは知っていることが求められる。***
- ✓ ***同様に、セキュリティ人材を同じ枠組みで考えられる。***

経理のキャリアパスが当然のように確立しているのは昔から経営上その専門性の必要性が認識されているからであり、セキュリティも同じ認識で考えれば、セキュリティ人材は専門職だけでなく、当然ライン職階においてもセキュリティの基礎知識を持った職として必要である。

ゼネラリストのキャリアパスは、どの企業においてもラインマネージャーとして確立されている。またスペシャリストのキャリアパスは、IT/セキュリティベンダあるいは情報子

---

4 「複線型人事制度とは、全社共通の画一的な人事制度ではなく、同一企業内に複数のキャリアコースが並立する多元的な人事管理システムのことです。ラインとスタッフ、総合職と一般職、全国社員と地域限定社員などの区分を設定し、区分ごとに採用、昇進・昇格、賃金、教育研修などを管理します」（『日本の人事部』 より引用 https://jinjibu.jp/keyword/detl/243/ ）

会社において、別途キャリアパスとして人事制度に取り入れられている。そのため、ユーザ企業としてセキュリティ人材としてキャリアパスを考え育成することが必要な人材はエキスパート人材であると考えるともに、経営上のセキュリティの専門性が必要であることを認識することが必要であると考えた。

この 3 つのキャリアパスと第一期で検討した「人材定義リファレンス」との関係を、次の図に表現した。

図 2-2-2 人材定義リファレンスに対する「エキスパート」の関係

ただし 3 つのキャリアパスが明確に 3 つに分かれるわけではなく、それぞれのキャリアパスを渡り歩く人材も多くいると考えている。重要なのは一般のユーザ企業（3.2.1(2)の企業）において、セキュリティ人材として内製するべき人材のキャリアパスがエキスパート人材という形で顕在化され認識されることである。

3.2.3 セキュリティ統括（室等）とセキュリティ統括人材

第一期の人材定義 WG での議論で、一般企業において通常見られる業務系 IT システムにおける 30 の役割を定義した。このうち、本検討会に参加する企業からのアンケート結果ではなく、議論をした結果として追加した役割が「セキュリティ統括（室等）」である。

これは本検討会参加企業において、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になってきているという事情を反映した結果である。事実、その後、企業活動の全体に跨ってセキュリティ統括を行う部署が参加企業において設置されている。

第二期の人材育成 WG での議論で、ユーザ企業（3.2.1(2)の企業）おいて内部的に育成すべき人材キャリアとして、エキスパート人材が必要であると考え、またエキスパート人材はセキュリティ統括（室等）に所属すべき人材ではないかという仮説に基づき検討を行った。エキスパート人材をセキュリティ統括人材と呼ぶ方向で検討を継続している[5]。第二期の OT セキュリティ人材定義 WG での事例紹介で、複数の工場を所有する製造メーカにおけるセキュリティ対応に関する議論から、エキスパート人材は組織として一カ所に存在するのではなく、セキュリティ対策を行うべき対象があるところで対応責任を担った部署に必要であるという認識を得た。今後、「セキュリティ統括（室等）」についても検討を継続していく。

またエキスパート人材の検討において、次のような点を重要視した。

- ✓ ***セキュリティ対策の実施内容の決定者と承認者の状況***

  本検討会参加各社の多くで、セキュリティ対策を「何を、どこまで、どのように」に実施するかを決める人材は、セキュリティ部署・セキュリティチームに所属している。その内容を承認するのが CISO 相当の役職者であり、その役割は「説明責任」と「予算執行承認」である。

- ✓ ***セキュリティ対策は、セキュリティ製品・サービス導入だけでは不十分***

  サイバーセキュリティ対策が経営課題として重要視されてきており、企業における IT 利活用が単にオフィス環境におえる業務支援だけではなく、生産現場等の業務そのものに浸透してきているため、セキュリティを自社の事業を念頭に置いた上で考える人が重要になってきている。

- ✓ ***日本国内における IT 従事者の 75％はベンダに所属***

  ユーザ企業の IT 部門は、事業運営に必要になる IT システムを守る立場にありシステム企画を担当するが、構築及び運用の実務は情報システム子会社や IT ベンター

[5] 名称に関しての考察は 3.2.3（5）を参照のこと。

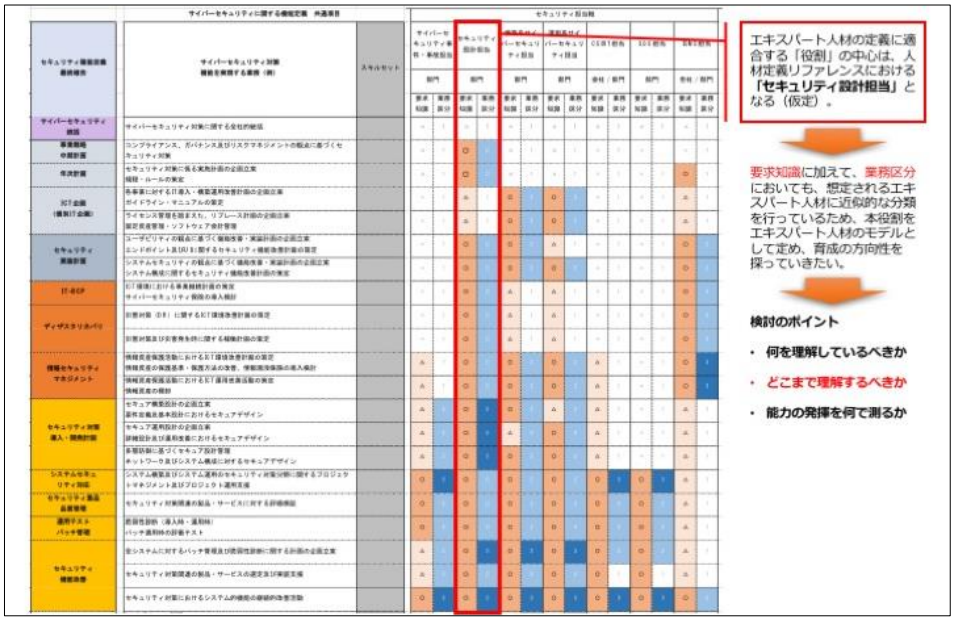
に委託している。その際、委託先がセキュリティ人材を確保していない場合、セキュリティ対策の不十分なシステムが提供され運用されることになる。

(1) 人材定義リファレンスとエキスパート人材

エキスパート人材の検討を進めるにあたり、第一期で検討したセキュリティ人材定義リファレンスで定義した 30 の役割と重なるのかを検討した。

前の章でも述べたように、エキスパート人材（セキュリティ統括人材）はセキュリティ対策を行うべき対象があるところで、対応責任を担った部署に必要であり、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であるとして人材定義リファレンスの“セキュリティ設計担当”の役割がエキスパート人材のモデルの中心になると仮定した。（表 3-2-4）

表 3-2-4 人材定義リファレンスとエキスパート人材の関係（仮説）



検討のポイントとしては、“セキュリティ設計担当”の役割をこなすために、「何を理解しているべきか」、「どこまで理解するべきか」、「能力の発揮を何で測るか」などを中心に議論を進めた。

(2) 持つべき能力/育成すべき能力

“セキュリティ設計担当”の役割として、持つべき能力、あるいは、育成すべき脳力はどのようなものであるかについて、第一期でも使用した「氷山モデル」で検討し

た。「倫理観・信条」などを基礎として、知識や技術だけではない様々な能力が必要である。（図 3-2-3）

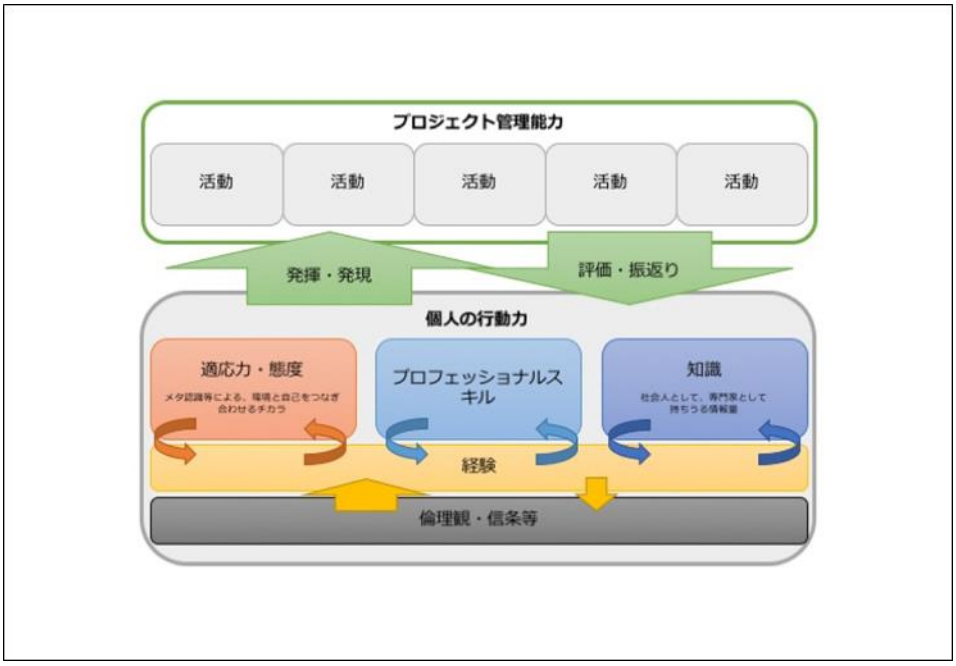


図 3-2-3 持つべき能力／育成すべき能力

表 3-2-5 に、それらの能力の具体的な例とそれらがどのように育成されるのかについて、“育成に必要な条件”としてまとめている。

表 3-2-5 セキュリティ人材育成の考え

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	人材定義リファレンス：機能（業務区分）	自主的に学習可能なもの
	知識	人材定義リファレンス：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	人材定義リファレンス：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	

人材定義リファレンスでは、役割として必要な能力に関して、個人の行動力として“プロフェッショナルスキル”と“知識”、プロジェクト管理能力の部分では“活動”に該当する能力についてのみ言及している。これら能力に関しては、かなりの部分、自主的な学習で育成可能であり、理解しやすく評価も比較的行いやすい能力であるため、人材定義リファレンスに取り入れた形となっている。

第二期ではエキスパート人材に必要な能力として、その他の能力を加えて育成に向けてどのようにすべきかを検討している。本中間報告の時点では、これらの能力に関して明確に洗い出せている状況ではなく、検討を続けている状況である。今の時点での検討内容を図示したものが、図 3-2-4 である。

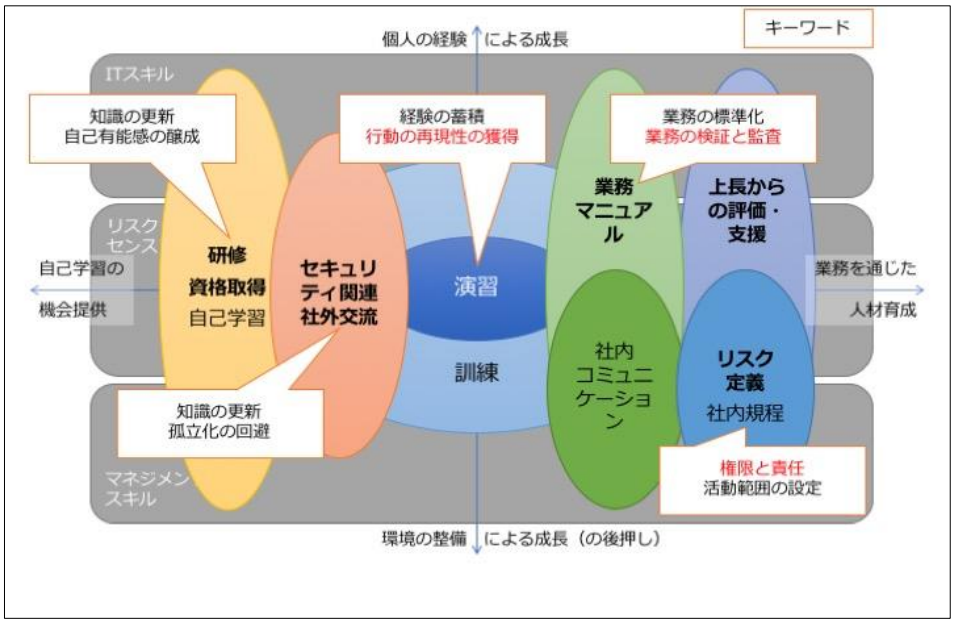


図 3-2-4 エキスパート人材育成のポイント（検討中）

経験に関して、実経験のみでは時間や機会を得ることが難しいため演習や訓練で補う必要がある。育成のポイントでは演習・訓練を育成の中心として考えている。

知識の獲得・更新には、自己学習が有用であるが、自己能力のレベル感を実感するためには、研修・資格取得などが必要である。また、組織内で孤立してしまい、独りよがりの偏った知識や判断になってしまわないために、セキュリティ関連社外交流を行うことも必要である。組織として活動を進めていく為に必要なプロジェクト管理能力や社内の業務を知るためには、業務に関する様々な文書（業務マニュアル、社内規

定）などが整備され、それらに精通する必要がある。特に、上長からの評価・支援が最も大事ではないかと議論があった。

また、現在、議論の中でエキスパート人材にとって必要だと考えられているのが、“リスクセンス”と呼ばれる能力である。

例えば、エキスパート人材が何かの脅威に対応を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、限られた時間のなかで判断し対応をしていくことになる。このような対応能力が“リスクセンス”である。

“リスクセンス”をどのように育成していくかは、検討中である。様々な過去の事例を分類整理し、それらへの対応策を検討し体系的に知識にまとめること。さらに、それら事例集をベースとして、サイバーレンジなどを活用した実際的な演習・訓練を行うことは必要であろう。

今後、さらに議論を重ね、社内のセキュリティ業務で求められる能力と内製すべきポイント（つまりエキスパート人材に求められる能力）および、修得すべきノウハウ（経験を積むための知識・前提）を洗い出していく。

(3) エキスパート人材の配置と環境

エキスパート人材の組織内での配置に関しては、セキュリティ統括（室等）として、組織全体のセキュリティに関しての企画・戦略・管理をとりまとめる部署に配置することを想定した。役割の観点から考えると図 3-2-5 に示すようになると考えられる。

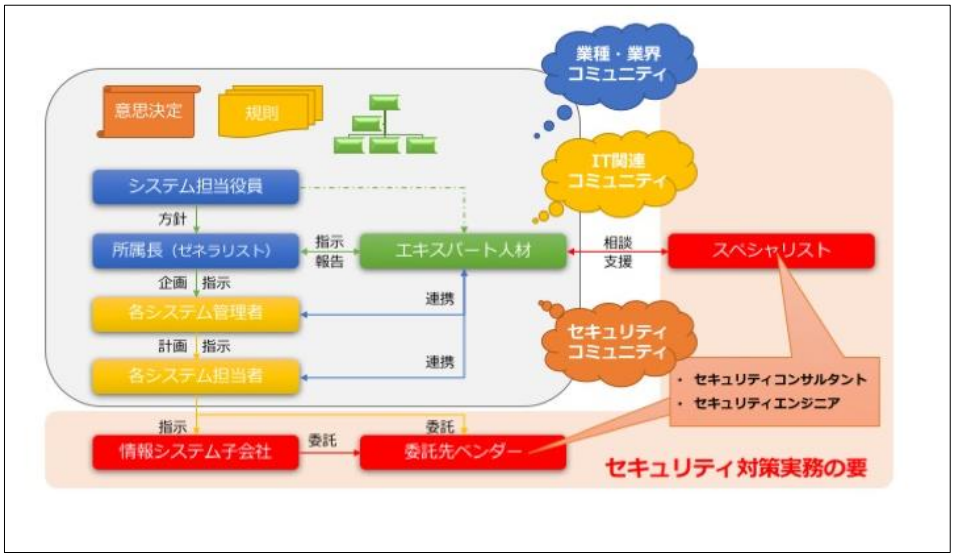


図 3-2-5 エキスパート人材の配置と環境

一般的な情報システムに関しては、情報システム部門が担当し、システム担当役員から最終的な構築を行う情報子会社、あるいは委託先ベンダという流れが存在すると考えられる。それに対して、エキスパート人材は企画を行う立場の所属長と同列かつ独立した形で位置づけられる。

エキスパート人材は外部のセキュリティベンダのスペシャリストの支援を受けつつ、情報システム部門の所属長（ゼネラリスト）へセキュリティに関しての指示・報告を行う。また、より具体的な計画についてはシステム管理者やシステム担当者と連携しつつ、セキュリティレベル確保に努めるような働きをする。

その際、様々なコミュニティ（業種・業界、IT 関連、セキュリティ）とも連携して、自組織にとって有用な情報を得る役割も担う必要がある。

図 3-2-6 は、日米の IT 技術者がどのような企業に分布しているかの比率を示している。米国と異なり、日本では多くの IT 技術者がベンダ（IT サービス企業）に在籍しており、日本のユーザ企業が内製で全ての IT システムの設計/構築/運用まで行うことは難しい状況であることが分かる。セキュリティに関しても同様と考えられ、エキスパート人材は組織全体のセキュリティをとりまとめるために、情報システム子会社、委託先ベンダ、セキュリティベンダなどセキュリティ対策実務者（セキュリティコンサルタント、セキュリティエンジニアなど）の支援を得る必要がある。

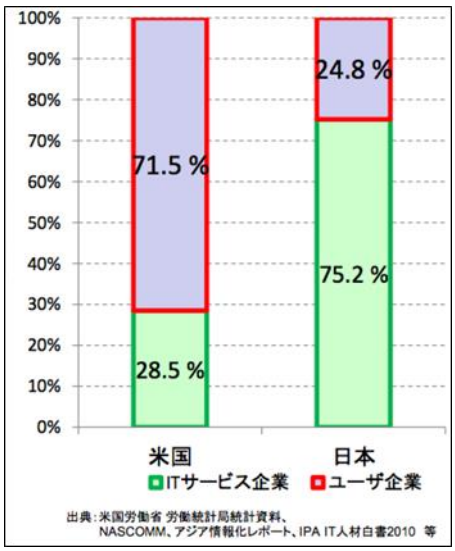


図 3-2-6　日米 IT 企業比較

セキュリティ要件を十分満たすシステムを構築するためには、構築を行うベンダに能力の高いセキュリティ対策実務者が必須である。経済産業省（2016 年 6 月 10 日）発表の「IT 人材の最新動向と将来推計に関する調査結果」[6]によると、セキュリティコンサルティング会社は 194 社であり、アンケート調査から推計したセキュリティコンサルタントは全国で 1330 人（2015 年現在）となっている。（図 3-2-7）

6　http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_4_2.pdf

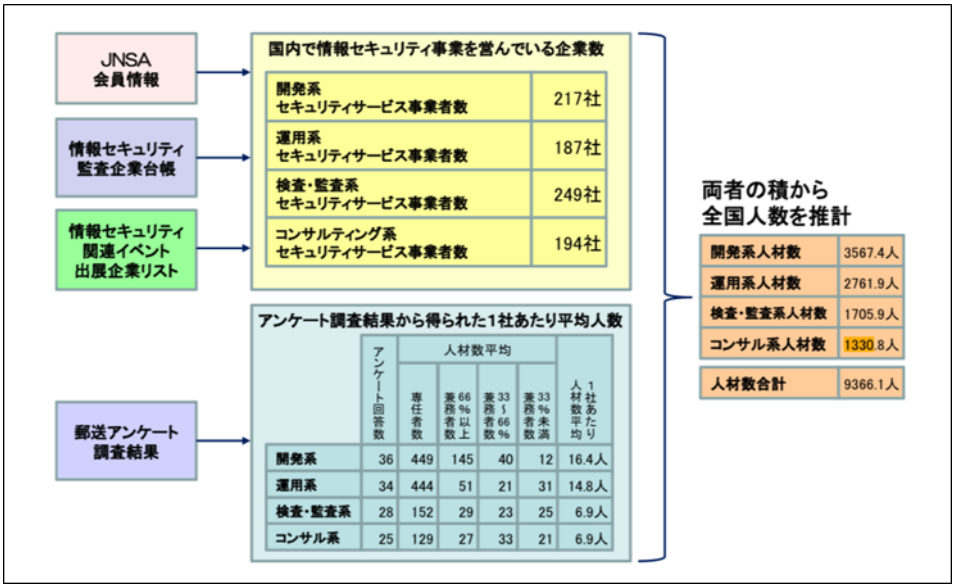


図 3-2-7　1社あたりのセキュリティ人材数

現在、東京証券取引所に上場している企業だけでも 3500 社以上あることを考えれば、ベンダ側のセキュリティ対策実務者も不足していると考えられる。エキスパート人材がユーザ企業において活躍するためには、情報システム子会社、委託先ベンダ、セキュリティベンダなどのセキュリティ対策実務者を育成することも非常に重要である。

（4）CISO とエキスパート人材の役割分担 - 説明責任と意思決定について

サイバーセキュリティが経営課題となってきている状況では、セキュリティ対策に関わる意思決定とそれに対する説明責任は様々なレベルで必要とされている。本検討会では、エキスパート人材が組織の中で、どのような説明責任と意思決定の任を持つべきかについて議論した。（図 3-2-8）

NISC では、*『経営層の示す経営方針に基づき、組織全体のサイバーセキュリティ対策を提示し、さらに、組織内の関係部局間の総合調整や実務者層をまとめ、指揮することができる「橋渡し人材層」を置くとともに、「橋渡し人材層」がその役割を十分に遂行できるよう「権限」と「責任」を明示することが必要である』*[7]としている。

[7] https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf

図 3-2-8 の左側部分は、本検討会が考える普及している意思決定プロセスを説明している。

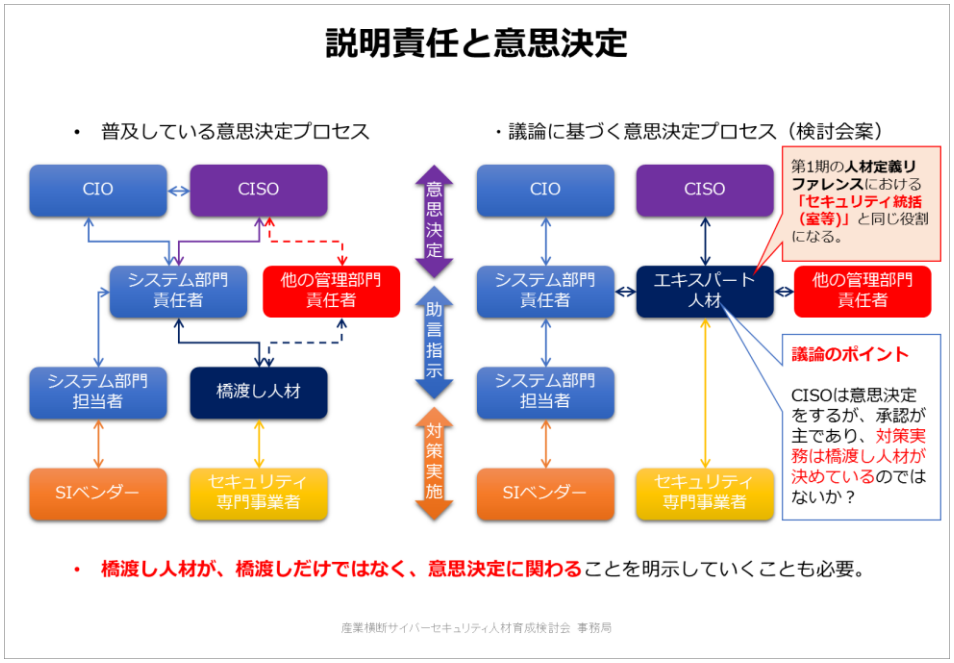


図 3-2-8　CISO とエキスパート人材の役割分担

橋渡し人材は CISO を直接補佐するのではなく、様々な部門の責任者（特に、システム部門責任者）とセキュリティ専門事業者の間に位置して、セキュリティの専門的な表現を分かりやすく各部門長に説明するような役割を担っていることが多いと想定している。

本検討会では、本来あるべき意思決定プロセスは、図 3-2-8 の右側部分に示したようになった。エキスパート人材（セキュリティ統括人材）は CISO の直下で他部門の責任者と同レベルに位置し、連携しながらセキュリティ対策実務を検討し決める役割を担い、CISO がその内容の承認を行う。エキスパート人材の「対策実務決定」と CISO の「承認」を合わせて、「意思決定」と考えることができる。CISO の役割は「説明責任」と「予算執行承認」であり、現在の意思決定プロセスと大きく異なるのは、エキスパート人材（セキュリティ統括人材）がセキュリティの意思決定に関わることである。

（5）人材定義の呼称

3.2 では、ユーザ企業においてセキュリティ対策企画・戦略・計画をとりまとめる中核人材の呼称として、「エキスパート人材」、「セキュリティ統括人材」の両方を用い、また NISC の「橋渡し人材」も同様に扱っている。複数の人材定義の呼称を使い分けるのか同等のものとして扱うかについては、現時点では検討しているところである。

- ✓ *橋渡し人材*

  NISC では、「経営陣と技術者を繋ぐ立場」を担う人材とし普及しており、企業におけるセキュリティに関する意思決定に強く関与する立場であることが想定されている。ただし本検討会の議論では、“橋渡し”という言葉が、単なる情報の橋渡しという印象を与えるとの意見もある。

- ✓ *エキスパート人材*

  経営陣を支えるセキュリティ人材を定めるために、人材育成 WG の議論の中で登場した呼称であり、ゼネラリストとスペシャリストに対比させるために活用している。日本特有な年功序列型人事制度に基づくゼネラリスト、資格や専門分野に基づくスペシャリストに対応し、ユーザ企業の中で人材を確保し育成するために仮置きした呼称である。

- ✓ *セキュリティ統括人材*

  人材育成 WG において、中核となるセキュリティ人材の役割は「セキュリティ対策を決定し、CISO の承認を受ける（「対策決定」と「承認」を合わせて「意思決定」とする）」人材であるとの議論があり、その呼称とした。本検討会に参加しているメンバーの多くが、対象となると考えている。エキスパート人材の後継の用語として、活用を検討している。

以上、第二期の人材育成 WG で検討された内容について説明した。今後は、「セキュリティ統括人材」育成のための実践的手法が必要である。人材育成 WG で引き続き検討を進めていく。

3.3 サプライチェーン全体のサイバーセキュリティ向上について

企業におけるセキュリティ人材の確保という観点では、前述の通り自社を守る PDCA マネジメントサイクルを推進すると共に、セキュリティリスクを自社の事業リスクに置き換えた上で幹部への適切な説明を行うことができる「セキュリティ統括人材」の存在が、円滑かつ安全・安心なビジネスの継続のためにも重要である。

ここで企業のセキュリティマネジメントを支えるのは PDCA サイクルであるが、これと合せて必要となるのが、実業が大きく依存している「IT」自体の健全性である。ここでいう IT とは大きく以下の二つに大別される。

- ✓ *ビジネスを支える受発注や生産管理等の「企業システム」*
- ✓ *顧客へ提供する製品・サービスを構成する「IoT 系の部品やソフトウェア/サービス(モノ)*

実業で利用する部品やサービス（モノ）、IoT 系部品やソフトウェア/サービス（IT 機器）については外部調達により手配されるケースが殆どであり、当該業務のフロントとなるのが調達部門である。

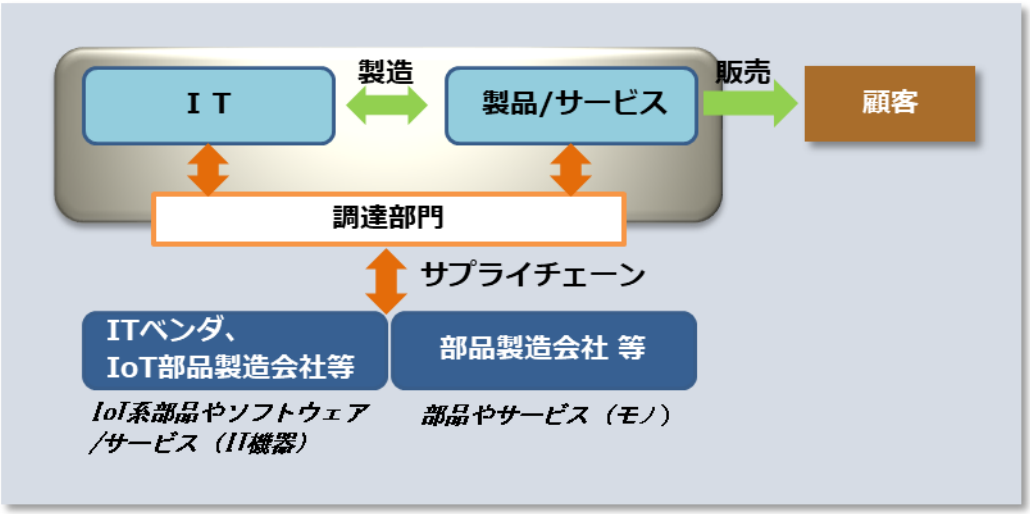


図 3-3-1 調達部門を取り巻く環境

IT 機器やモノを調達する際に必要とされる要件は発注元の事業（担当）部門が策定し、それを元に調達部門が発注先企業と折衝することになるが、セキュリティ要件も例外ではない。従って事業部門は言うまでもなく、調達部門においても、ある程度のセキュリティ知識がないと要件内容を理解できず、発注先企業からの納品時の検収もスムースに実行されない可能性が高い。

本節では上記を踏まえて、サプライチェーンの中でセキュリティ要件を如何に策定し運用するのか、合せてそれを円滑に廻すスキルを有する人材を如何に確保/育成していくのかとの課題認識に基づき、検討内容を記載する。

3.3.1 発注元企業におけるセキュリティ課題

IT 要員を自社で抱え自社でシステムを開発することが多い米国企業と比べ、日本企業では企業内システムの開発や保守を IT ベンダに依存することが多い。また顧客へ提供する製品・サービスにおいて、サプライチェーンから調達する IT が自社の製品・サービスの一部となっている場合は、調達品自体のセキュリティ確保が急務である。

従って、IT ベンダを含むサプライチェーンへの調達基準としてサイバーセキュリティ要件を盛り込むことは、企業組織は言うまでもなく実業であるビジネスの円滑な推進のためには必要不可欠である。

IT の調達だけでなくモノの調達においても、サプライチェーンを構成する企業に潜在するサイバーセキュリティリスクが自社の製品やサービスの安定的な提供を脅かすリスクに直結するようになってきている昨今、サプライチェーンへの調達基準にセキュリティ対策レベルを設定する等の施策も、今後重要となってくる。

加えて、昨今のランサムウェア等によるサイバー攻撃に伴う業務停止リスクは、WannaCry 以降頻繁に現実化しており、しかもそれは大企業だけの問題ではなくサプライチェーンを構成する中小企業においてより切実な問題となっている。

（1）セキュリティ要件策定における課題

ここで、調達時に関するセキュリティ要件に関する役割分担は、以下のように考えられる。

- ✓ ***事業部門*** ： *システム、IoT 機器類、サービス等のセキュリティ実装方針を検討し、具体的な要件として記述する。必要に応じて、会社として具備すべきセキュリティ実装レベルを規定し要件として既述する。*
- ✓ ***調達部門*** ： *当該要件に基づき製品選定、会社選定を実施し発注する。納品時には納品時には事業部門と連携し当該要件を満たしているかの検証を行う。*

①　個々のセキュリティ要件に対応すべき企業側の負担増

サイバーセキュリティに関する調達基準については 米国政府のクラウド調達の基準である FedRAMP に見られるように、自国企業との取り引き時に国境を越えて採用を求める等の国際的な枠組みが作られつつある。

一方、我が国では国際調達は元より、国内取引であっても各企業で採用する標準的なセキュリティ基準がない。従って各企業は自社の個別の基準に基づきセキュリティ要件を策定し、受注者側に要求するのが一般的である。しかし、これは受注企業にとっては複数の相異なる要件への対応を求められ、対応の重複やコストの増加が発生することとなる。さらにグローバルにビジネスを展開する企業にとっては、国際標準との重複も考えられ、ビジネス展開上の障壁ともなりかねない。

②　非機能要求グレードの存在

元々セキュリティは非機能要件として位置付けられ、「どこまで」対応すべきかが曖昧な性質といわれている。それに対して、独立行政法人情報処理推進機構（以下、IPA と略す）では、「非機能要求グレード」[8]を定義している。

非機能要求グレードは発注者と受注者との認識上のアンマッチを防ぐためのツールとの位置付けであるが、例えば IT ベンダ以外の企業で上記について十分に認識されているかというと、残念ながら NO である。これは、内容的に基本的知識がないと理解が難しいこともあるが、それよりもグレードの存在そのものを関知している企業担当者が希少である事の方が大きい。

（2）セキュリティ要件「ベストプラクティス」の策定

①　共通雛形モデル策定検討

そこで本検討会に参画する一般企業の活動としてセキュリティ実装の雛形モデルを議論する場を設け、そこに IT ベンダが意見を出し合いながら受発注時の「セキュリ

---

8 ― 非機能要求グレード

情報システムの開発では、業務機能に関する要求以外のいわゆる「非機能要求」について、発注者と受注者との認識の行き違いや、互いの意図と異なる理解をしたことに気づかないまま開発が進んでしまうことがあります。「非機能要求グレード」は、このような状態を防止することを目的とし、重要な項目から段階的に詳細化しながら非機能要求の確認を行うツール群です。

出典　IPA https://www.ipa.go.jp/sec/softwareengineering/reports/20100416.html

ティ標準要件定義モデル」を策定することを計画している。第一期では、企業の IT 部門におけるセキュリティ担当者の役割定義を策定したが、それに続く実務レベルでの円滑な継続を目指したセキュリティモデル策定の第二弾である。さらに、サプライチェーンの裾野が広がるのに伴い、素材やインフラ産業を中心として業界を跨いだ取引が多く発生するため業界を横断した基準の作成が求められている。産業界として一枚岩となり上記モデルを策定する一方で、政府には調達基準に関するグローバル標準との連携も要望していきたい。

② 企業としてのセキュリティマネジメント標準モデル検討

一方、企業としてどこまでセキュリティマネジメントを実装するか、というのも悩ましい問題である。セキュリティマネジメントのモデルでは ISMS に代表される ISO27000 シリーズが知られており、多くの企業が認証を取得している。また、システムの品質という観点では ISO9001 があり、システム品質に関する一定レベルの維持・確保をアピールできる。

また昨今では、リスクマネジメントの標準規格である ISO31000 シリーズが着目されている。これは組織体のどのレベル・規模であっても適用可能な「リスクマネジメントの考え方」を示したものであり、従来は災害や事故等を想定した対応が一般的であったが、最近はセキュリティリスクについてもマネジメントに含むケースが増えている。

加えて、事業継続計画（以下、Business Continuity Plan：BCP と略す）の策定は、昨今の企業では一般的となりつつあるが、災害やパンデミックに加えてサイバーセキュリティに関する BCP 策定の重要性、必要性が叫ばれている。前者は非常時に如何に事業を継続するかの方策を掲げるが、後者は事業を継続するためにシステムの停止を含めた判断を為すための方策が必要であり、対処の方向性が逆といえる。双方を予め策定することが望ましい。

サプライチェーンを構成する企業として、良質な受注を獲得するためにも企業ポリシーとして、どこまでセキュリティマネジメントを実装するべきかを検討し定める必要がある。それを行うに当たっても、セキュリティ要件標準モデルと同様推奨すべき雛形モデルを策定し、共有する事のメリットは大きい。但し、これについては業界ごとにレベル、内容の相違があると想定され、本検討会における幅広い業種の企業の知恵を結集して検討していきたい。

③　事業部門、調達部門におけるセキュリティ教育の推進

前述の標準モデルを活用すべき環境が整備されたとしても、一定の知識は必要である。セキュリティ要件を検討するに足るセキュリティ知識を確保するためには、セキュリティに関する基礎レベルの教育受講等でスキルを身に着ける地道な努力が求められるが、現状では一般企業向けのセキュリティ講座が極めて希少である。

第二期では、人材育成 WG において、現在開講されているセキュリティ教育講座を調査し、本検討会公式ホームページに掲示している。しかし、IT ベンダ向けやセキュリティ専門家向けがその大多数を占め、しかも関東圏での開催に限られているものが多い。今後は本検討会としても、人材育成 WG の活動を通じて企業向けセキュリティ基礎教育環境の整備を急ぎたいところである。

3.3.2 受注企業側のセキュリティ課題

（1）IT システム構築時のセキュリティ実装レベル

①　仕様書上にない要件の取扱い

企業から IT システムの発注を受けて製品・サービスを提供する IT ベンダ側からみると、元々提示されたシステム仕様書にセキュリティ上の具体的な記述が乏しい中で、仕様書にはないセキュリティ機能を何処まで実装すべきかとの悩みがある。

仕様書上の要求のないセキュリティ機能を実装することは、システムの安全性は確保できるがその分コストが高くなり、入札等においては失注の原因にもなりかねない。しかし特に IT ベンダの場合は、記述がないから何もしない、というのは IT 企業としてのモラルを問われかねない昨今である。加えて中小のベンダでは、かかる対応を行う企業体力に乏しい場合も少なくない。

②　発注側との標準要求定義モデルの共有

そこで、3.3.1 でも記載した「セキュリティ標準要件定義モデル」の策定が、その解決策の一つとなり得る。IT、IoT 等のシステム製品に実装すべきセキュリティ標準モデルが規定され、それを業界共通のテンプレートとして IT ベンダ間、及び発注企業側の双方と共有することは、発注側の企業、受託開発すべきベンダ企業の双方の悩みを解決し、かつ日本国における IT システムのサイバーセキュリティ耐性を高める効果が期待される。

かかる成果物である標準モデルは、CRIC CSF 共通リファレンス[9] として公開し、例えば調達時の仕様書上で、「CRIC CSF 共通リファレンスの№＊＊を参照のこと」と記載することで、解釈のゆらぎを回避し受発注企業双方の共通の理解の下での的確な運用が可能になると考えられる。

③ IT ベンダ側技術者のレベル均質化

IT ベンダ側の SE 等の技術者においても、セキュリティの知識レベルにはまだまだばらつきがあり、担当者によって当たり外れが大きい、との意見も散見される。特に要件やレベルが曖昧なセキュリティにおいては、ユーザ企業の意図を的確に汲み取ることが求められ、例えば技術者としてのセキュリティスキルの可視化方策を検討する事も必要である。

必要とされる知識や経験をポイント化し、当該ポイントに応じたレベルを定義し認定する事で、どのベンダであっても当該レベルに応じたセキュリティ技術が提供可能な技術者であることを示す制度等は有用である。かかる IT ベンダ業界共通のセキュリティ認定資格制度の創設等は、その方策の一つである。

併せて、当該スキルを学習するためのベンダ向け専用セキュリティ講座や、実際に手を動かし頭を使う演習環境の整備も必要と考える。今後、本検討会としても検討していきたい。

---

9 「CRIC CSF 共通リファレンス」は、CCR（CRIC CSF Reference）として検討中

3.4 経営者のリーダーシップと信頼の輪の構築

企業の事業がおおきく IT に依存する一方で、サイバー攻撃の手口は巧妙化・高度化する傾向にある。サイバー攻撃により顧客情報等が詐取される、あるいは生産活動がストップする、さらには重大な事故を引き起こすような事態になると企業の社会的責任を問われ事業継続に甚大な影響を及ぼしかねない。従って経営者はサイバー攻撃を重大なリスクと捉えて適切な対策を講じる必要がある。

一方でサイバー攻撃は、サイバー空間に存在する攻撃者が金銭取得や政治的な目的を持って行うものであるため、特定の業種や企業に特化したリスクというよりも社会的なリスクと認識して、社会全体の耐性を向上させる取り組みが不可欠である。すなわち「競争領域」ではなく、企業が協調して社会的な付加価値を設ける（CSV : Creating Shared Value）すなわち「協創領域」と認識すべきである。

経営者はサイバー攻撃対策が「協創領域」との認識のもとで、他社と積極的に交流して「信頼の輪」を築きながら自らの取り組みを積極的に提供し、また他社の有益な対策を自社に取り組むべきである。本検討会は、その一助とすべく継続的にトップ層会合を設けるとともに、会員企業間の知恵を交換した「サイバーセキュリティ対策のベストプラクティクス集」を設ける所存である。

さて、一般的に「リスク」という言葉は自然災害や事故など損害を被るもの、すなわち「危険」という意味で捉えられることが多いようである。しかし、あらゆる投資にはリスクは付きものであり「ノーリスク・ノーリターン」ともいわれるように、経営者はリスクを事業に付きものの「不確実性」と捉えるべきである。「不確実性」とは、経営判断がもたらす結果が不確実であるということである。想定通りの結果が出ることも悪い方向に振れることも、良い方向に振れることもある。このような不確実性を管理（マネジメント）することこそ、経営者が行うべきリスクマネジメントである。

すなわち事業の大半が IT に大きく依存する今般、サイバー攻撃は、おおきなリスク＝不確実性であり、経営者は、これを強いリーダーシップを発揮してマネジメントすべきである。しかしながら、その理解に要する専門性の高さや経営者を対象とした情報提供の不足が、その理解を遠ざけ様々なサイバー攻撃の被害を拡大している可能性がある。

一方でリスクマネジメントは、リスクが発生する可能性と、その影響度合いを勘案して対策を講じるのが一般的である。例えばリスクが発生する可能性が高く、かつ、その影響度が極めて大きいものは、インターネットの接点を自社で保有せず他社に委託するなど

「リスクを回避」すべきである。またリスクが顕在化する可能性が極めて低く、その影響度が極めて低いものは「リスクを受忍する」という選択もある。

リスク対策は、不正な通信のフィルタリングなどリスクの発生頻度を下げる「事前の対策」とサイバー攻撃を受けた場合にインターネットから切り離すなど、リスクが発生した場合に被害を極小化する「事後の対応」を講じる必要がある。従前のサイバー攻撃対策は「事前の対策」が主流であったが、今般のサイバー攻撃の手口は多様化・巧妙化しており、あらゆるサイバー攻撃を防ぐことはできないという前提に基づき「事後の対応」を講じる必要がある。

このようにリスクを不確実性と捉えて、その発生の可能性と影響度合いに対する考課を深めることで、夫々のリスクに対する具体的な対策をつかむことができよう。そして、リスクの影響範囲、すなわち影響を被る顧客や取引先など協働で対策を講じるべきステークホルダーも明らかとなろう。

しかしながら、サイバー攻撃の手口は常に向上するため、対策の陳腐化は極めて早い。そのためサイバー対策の鮮度を保つには、あらゆる最新の情報に眼を配り必要に応じて対策の改善を行わねばならないが、個々の企業が知り得る情報には限界があるうえに、サイバー攻撃対策は収益すなわちリターンを得るために行うものではない。従って「どこまで対策を講じるべきか」を判断するのは難しい。

繰り返しにはなるが、この課題を解決するためには、経営者自らが、サイバー攻撃対策を「協創領域」との認識のもとで他社との「信頼の輪」を設け、互いの対策等を交換できる関係を構築すべきである。

なお、本検討会では経営者間の「信頼の輪」を設けるべく継続的にトップ層会合を設けるとともに、経営判断の一助とする会員企業の知恵を結集した「サイバーセキュリティ対策のベストプラクティクス集」の発信に向けた活動を行うこととした。

3.5 各 WG との関連性

本検討会は、重要インフラ事業者を中心としたユーザ企業及びその委託先企業に求められるサイバーセキュリティ人材の育成要件をより深く検討するため、以下の図 3-5-1 に示す４つの WG を置き、人材定義や人材育成に対するあるべき姿の検討、判断の基準となる情報共有、高等専門学校、大学・大学院への育成環境の支援等を視野に入れて活動している。

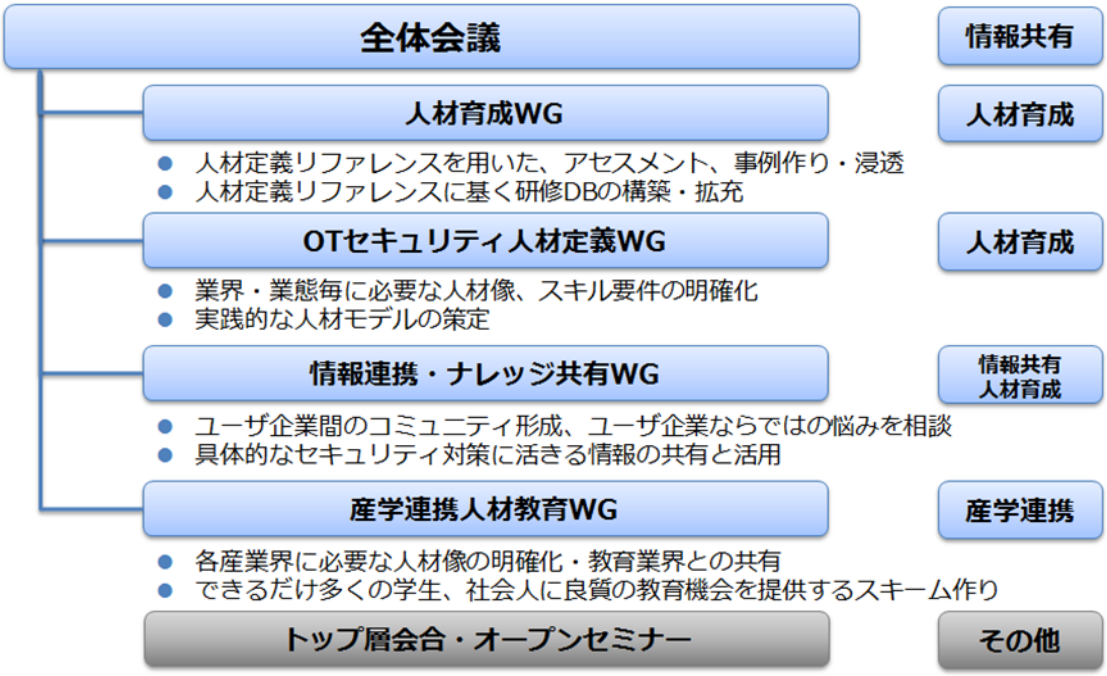


図 3-5-1　本検討会の活動形態

ここでは、以下に各 WG の目的・目標・活動方針について概要を示す。

3.5.1 人材育成 WG

人材育成 WG では第一期で策定、公開した「人材定義リファレンス」の有効活用に向け、ユーザ企業に求められるセキュリティ人材育成の高度化・効率化を目的とし活動している。活動目標は、エコシステム実現に向けた人材定義・人材育成・採用活動の包括的な対策モデルを策定することであり、引き続き第一期同様の成果物の公開を目指して「人材定義リファレンス」の改訂、リファレンスの 30 の役割に対応した育成プログラムの検

証、効率的な人材育成に向けた「研修データベース」の構築運用、産学連携に求められる「採用基準」の確立を行うこととしている。

3.5.2 OT セキュリティ人材定義 WG

OT セキュリティ人材定義 WG では、第一期の検討課題として残していた OT（Operational　Technology：制御・運用技術）に関するセキュリティ人材の育成方法を明確にするため、重要インフラ事業者である参加企業の事例共有を通じて OT 領域を明確化し、タイプ･スキルと言った人材像を定義することを目的と定めている。

また、実践的な OT セキュリティの人材モデルを策定することを目標とし、OT 領域における業務プロセスや業務要件を特定の粒度で明確に具体化し、OT 領域における「わかりやすい」セキュリティ人物像・人材モデルの策定、主要な業務単位を意識した成果物のパッケージ化・実際に人材を育成するためのロードマップ素案作成（人材育成 WG への継承）の方針を実現すべく活動している。

3.5.3 情報連携･ナレッジ共有 WG

情報連携・ナレッジ共有 WG では、ユーザ企業を中心とした産業横断連携により、参加企業の課題解決に貢献できること、情報共有と情報活用の場を作ることを目的とし、産業界全体のサイバーレジリエンス向上・効率化を目標とする。具体的には、ユーザ企業間のコミュニティ形成や共通化される課題の検討、情報共有・活用のための勉強会開催、情報共有、活用に関する事例集・ベストプラクティスの作成等を実現すべく活動している。

3.5.4 産学連携人材教育 WG

産学連携人材教育 WG では、高度化するセキュリティ脅威に対抗できる人材の育成スキームを確立し、産学官が連携したセキュリティ人材育成エコシステムの実現を目的とし、2020 年までに可能な限り多くの学生、社会人に良質の教育機会を至便な形態で提供することを目標として、既存の寄付講座等の取組みにおける連携（教材・講師等の提供）に加えて、e ラーニング等を活用した学習機会の創造（受講対象者、学習領域、地域等の拡大）を実現していくことにより、質的にも量的にも充実した教育機会の創造を方針として活動している。

なお以上紹介した４つの WG に加え、トップ層会合・オープンセミナーを含めた活動内容を別紙にて記載しているので、詳細はそちらをご覧頂ければ幸いである。

3.6 関係省庁をはじめとする外部機関との連携

本検討会における外部機関との連携については、公式 WEB（http://cyber-risk.or.jp）にて公開している。以下は、その一部を紹介する。

内閣サイバーセキュリティセンター（NISC）	
普及啓発・人材育成専門調査会 （会長：東京電機大　安田学長）	第 7 回「普及啓発・人材育成専門調査会」へ参加。 「施策間連携 WG」において本検討会の活動状況を報告。
人材育成に関する施策間連携 WG （主査：情セ大 後藤学長）	第 2 回「サイバーセキュリティ人材の育成に関する施策間連携 WG」へ参加。本検討会から「企業でのセキュリティ人材育成に関する議論状況」を説明し、意見交換。 なお、本 WG に対し、本検討会は委員メンバーとして参加し、本検討会における人材育成に関する活動を円滑に進めるため各種情報を提供し連携中。 ※情セ大：情報セキュリティ大学院大学
基本戦略グループ （吉田内閣参事官）	第 1 回 CRIC CSF セミナーにて来賓としてご挨拶を頂く。 本検討会公式 WEB に賛同団体（オブザーバ）として NISC ロゴ掲載を許諾頂く。

文部科学省	
サイバーセキュリティ人材育成検討チーム （主査：冨岡前副大臣）	産学連携のあり方「モデルコアカリキュラム」策定に関する意見交換を実施。「モデルコアカリキュラム」に対する産業界からの要望を提示。
高等教育局専門教育課 （松永課長）	第 1 回 CRIC CSF セミナーにて来賓としてご挨拶を頂く。 成長分野を支える情報技術人材の育成拠点の形成（enPiT）enPiT-Pro 選定状況が公表され、本検討会の親団体となる CRIC が連携する情セ大のセキュリティテーマが採択。

経済産業省/独立行政法人情報処理推進機構（IPA）	
IPA　HRD イニシアティブセンター （秋元センター長）	第 1 回 CRIC CSF セミナーにて来賓としてご参加を頂く。 情報処理安全確保支援士（通称：登録セキスペ）の活用や講習に関する情報交換を行い、連携強化に向けての会合を定期的に開催。 経済産業省が掲げる情確士 3 万人（2020 年）に向けて、普及に向けた意見交換を継続中。
産業サイバーセキュリティセンター （細川部長）	産業サイバーセキュリティセンターの取り組みについて、本検討会の会合にて説明会を実施頂く。 本検討会で運用する研修 DB において紹介するサイバーレンジの 1 つとして公開していくことで合意。 「産業サイバーセキュリティセンター」卒業生のキャリアパスの検証等について継続的に協議するを決定。

一般社団法人日本経済団体連合会（経団連）	
サイバーセキュリティに関する懇談会 （座長：梶浦氏）	第 1 回 CRIC CSF セミナーにて来賓としてご挨拶を頂く。 「サイバーセキュリティに関する懇談会」へ本検討会としてオブザーバ参加。第三次提言の発表に向けて、本検討会の活動を説明し、継続的に協議を継続中。 本検討会公式 WEB に賛同団体（オブザーバ）として経団連ロゴ掲載を許諾頂く。

一般社団法人日本システム・ユーザー協会（JUAS）	
セキュリティセンター （宮下常務理事）	第 1 回 CRIC CSF セミナーにて来賓としてご挨拶を頂く。 日本を代表するユーザ企業団体として、今後拡大するセキュリティ関連活動に関する説明を頂く。相互のアウトプットの連携を視野に情報交換を継続中。

3.7 エコシステム実現に向けた産学官連携について

日本におけるセキュリティ人材育成の取り組みとして、大学等の教育機関（以下、「学」）では若年層のみならず社会人も対象とし、セキュリティの基礎から高度な実践教育を行うためのカリキュラム策定や講座の開設等に力を入れるようになってきており、企業からの協力による産学連携の教育環境も増えつつある。また NISC や各省庁等、国の機関（以下、「官」）においては、「学」におけるセキュリティ人材教育を支援しつつ、セキュリティ人材としての種別やレベルの指標となる資格制度の運営や OT 領域も含めた特殊で高度な人材を養成するための取り組み等、日本の各界を統制する「官」だからこそ実現可能な各種施策を立ち上げている。そのような中で産業界としても主体的にセキュリティ人材の育成に取り組む必要があり、本検討会はその一助をなすべく活動を進めている。

本検討会では産業界として求められるセキュリティ人材の定義、および、その定義に基づく人材の育成・維持のための手段や施策を、産業界として主体的に推進すべく検討・議論を進めている。その際、育成された人材がそれぞれの企業に適切に雇用され、活躍し続けることができる仕組みが整っていることが重要となる。我々は、その仕組みをセキュリティ人材のための「エコシステム」と捉え、必要となる様々な機能や役割を「産」、「学」、「官」がそれぞれ相応の責任を持って担い合い、全体が有機的に繋がって様々なリソースを活用した施策を行うことで、継続的な人材（学生、社会人、教師、講師等）の育成と維持が効果的に循環（スパイラルアップ）する状況を目指している。

なおセキュリティ人材が必要となるのは、必ずしも「産」だけでなく「官」や「学」の領域にでも同様であるが、現段階では「官」や「学」で必要なセキュリティ人材が育成、雇用されて活躍し続けることに関しては、便宜上、言及・明示するのを省略する。

第一期では、「産」、「学」、「官」がそれぞれ担うべき役割や機能を並べ、想定される相互の関係を描いたエコシステムのイメージを図 3-7-1 のように示した。その後、エコシステム具現化のための議論をする上での重要ポイントが色々と明らかになりなってきており、第二期では 2020 年の東京オリンピック・パラリンピックも見据えた短期的なエコシステム実現に向けた取り組みを推進しつつ、将来的なエコシステムの理想像に向けた取り組みの提言を行いたい。いずれも、「あるべき姿（ToBe 像）」、「ToBe 像に向けて産業界が取り組むべきこと」、「本検討会が取り組むべきこと」の３つの観点を持って進める。

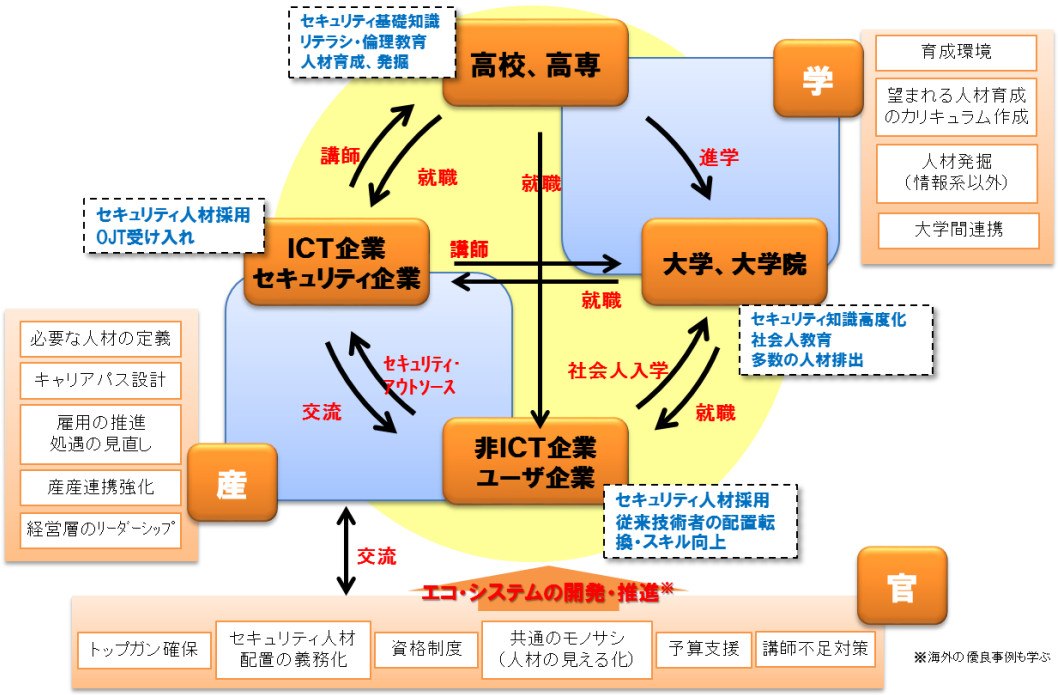


図 3-7-1. 第一期で示した人材育成のためのエコシステムイメージ

【エコシステム議論の重要ポイント】

第二期に入って明らかになってきた重要なポイントを以下に示す。

- ✓ *産業界として主体的にセキュリティ人材を充足するための策は、「育成」、「雇用」、「アウトソース」の３つの手段に大別される。*
- ✓ *セキュリティ人材が活躍し続けるためのキャリアパスとの関係（エコシステムを構成する様々な要素が、キャリアパス上のどの部分に寄与するものなのか）を明確にする。*
- ✓ *IT/OT、ユーザ/ベンダ、インソース/アウトソースなどの対比軸で人材像が大きく異なり、育成の要件も手段も主体も異なってくる。*
- ✓ *コスト投下の是非論がある中、エコシステムを機能させるための制度、マネーフローを支える枠組み等の基盤の構築が必要である。*
- ✓ *国の指針や制度との関係を明確にする。*
  - 「サイバーセキュリティ 2017」2017.8.2（セキュリティマインドを持った企業経営の推進 など）
  - 「重要インフラの情報セキュリティ対策に係る 第４次行動計画」2017.4.18（重要インフラを守るための取組 など）

- 「サイバーセキュリティ人材育成プログラム」2017.4.18　　etc.
- 「学」、「官」による様々な人材育成施策（教育、演習、環境、制度、予算、企業連携）の位置付け。
- 官：各省庁施策における育成対象（主に社会人、ユーザ企業の経営層から IT/セキュリティ企業の実務者層まで）
- 学：学単独、産学連携、産官連携（若年学生～社会人まで、就職を意識したコース/カリキュラム策定・提供）
- エコシステムの早期実現に向けた本検討会の活動成果（アウトプット）による貢献。

前述の議論ポイントを踏まえて、産学官連携を前提としたセキュリティ人材のエコシステム実現に向けて本検討会の活動成果を各種リファレンスとしてまとめ、産業界に展開することで、それぞれの企業の実状にあった人材育成のための具体的な施策として実装が可能となり、サイバーセキュリティ水準向上の実績が広がることを期待している。

また本検討会による各種リファレンスは、産業界に向けてだけでなく「官」や「学」にも様々な機会を通して提示していくことで、産業界としての要件や期待を「官」や「学」から参照できるようになり、より効果的な産学官連携の実現につながるものと考えている。エコシステム実現に向けた産学連携について、本検討会の活動を含めた産業界の目線によるイメージを図 3-7-2 に示す。

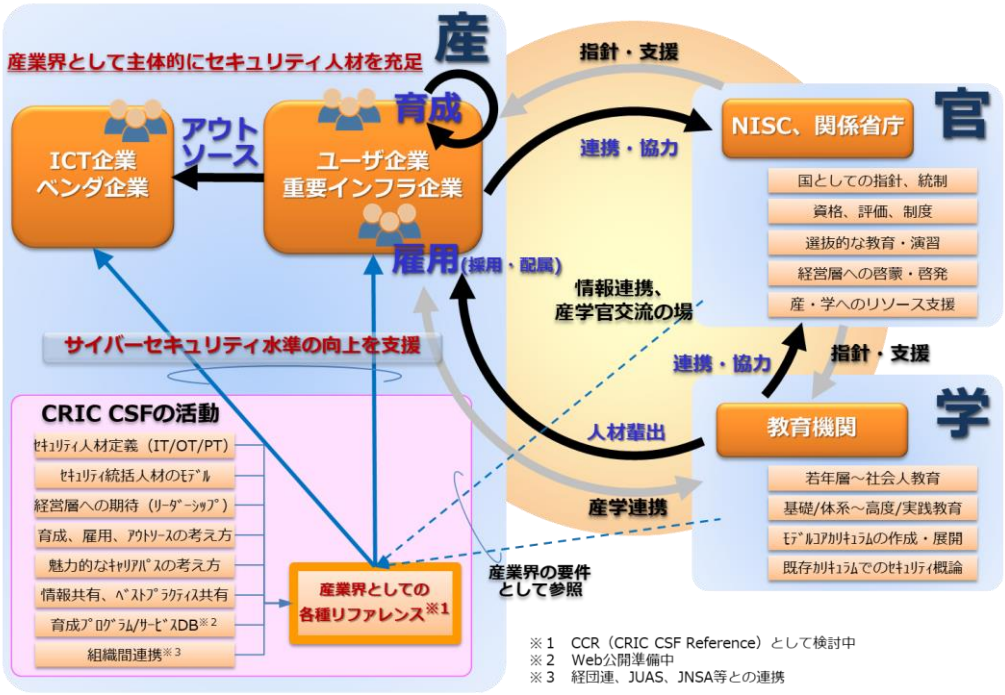


図 3-7-2. エコシステム実現に向けた産学官連携イメージ

4.おわりに

2020 年の東京オリンピック・パラリンピックでは、大会運営すなわち競技スケジュールの管理や競技の動画配信はもちろん、来場する要人警護や競技場の監視、さらには選手村の管理など、あらゆる運営が IT におおきく依存するであろう。そればかりか世界中から訪れる観光客を輸送する航空や鉄道、そのインフラとなる電力、ガス、石油、水道、さらには金融やクレジットなど重要インフラ業種の運営も同じように IT や IoT におおきく依存するだろう。

一方で安全管理の分野では “The strength of the chain is in the weakest link. 「鎖は、もっとも弱いリングで切れる」” という「ことわざ」が頻繁に用いられる。これは大会運営や重要インフラに脆弱な部分があると、サイバー攻撃のダメージを受けて社会全体の不安や混乱につながりかねないことを意味する。このような事態を避けるには、大会運営を支える IT のみならず重要インフラを担う IT や IoT を運営する関係省庁ならびに企業が緊密に連携して、横断的かつ統一的なサイバーセキュリティ水準を確保すべきである。

さらに今般のサイバー攻撃は個人による不特定多数をターゲットにした愉快犯的なものから、国や組織が政治的動機から標的となる企業等を定めて、企業の重要システム停止や重要データの詐取などに変化しているといわれる。もちろん、個々の企業が攻撃に備える「事前の対策」の一環として情報を収集すべきは自明だが、個々の企業が逼く政治的動機を持つ国や組織の意図、具体的な手口を知り得るには限界があろう。また過去には特定の業界全体が標的になった事例は数多く、米国では各業界の ISAC[10] （Information Sharing and Analysis Center、情報共有分析センター）において対策に直結する有益な情報を活発に交換している。

このような状況を踏まえ「これから襲来するおそれのあるサイバー攻撃」を予見し、確度の高い「事前の対策」を講じるには、内閣サイバーセキュリティセンターをはじめとする政府機関や関連団体との実務的な情報・意見交換を定期的に行う必要がある。

もうひとつ、今般のサイバー攻撃を完全に防御するのは困難との観点から、サイバー攻撃を被った場合の「事後の対応」を定める必要がある。これをより充実度の高い内容とす

---

[10] 1998 年 5 月 22 日に当時のクリントン米国大統領によって署名された、大統領令 63（PDD 63：Presidential Decision Directive-63）に基づき重要インフラ業種を中心に 19 業種の ISAC （Information Sharing and Analysis Center）が設立した。業種内の情報共有を推進し、ISAC の活動を監視する役割として、所管省庁（Sector-Specific Agency）が定められている。

べく、重要インフラ企業などが業界の壁を越えて被害状況や復旧方法の具体的な情報を共有するなど、「オールジャパンで共助する」枠組みが求められている。

本検討会は、このような考え方のもと関係省庁や重要インフラを担う企業に協力・賛同を呼びかけ、業界の壁を越えた情報共有と支援を軸とする「事後の対応」の具体的な枠組みや、各企業が具体的な対策を実施する際の判断基準となる「産業界のベストプラクティス」を検討する所存である。

以上のようにサイバー攻撃に対する社会的な枠組みのもとで得られた貴重な情報は、各企業の経営陣と実務担当者が共有するとともに直ちに対応の是非を検討する必要がある。そのためにはサイバー攻撃に関する情報収集に加えて、経営陣と実務担当者をつなぐ組織を明示して、本検討会等が発信する情報の受け皿を設けて頂くよう強く提言したい。

さらに各企業において、この中核的な役割を担うのが、本書で必要性を説く「セキュリティ統括人材」である。「セキュリティ統括人材」は、経営方針に基づいてセキュリティ方針を設け、さらに、これを実現すべく関係部署をリードしながら実行上の課題を経営に伝え、次なるアクションプランを設ける必要がある。

「セキュリティ統括人材」には、現場を納得させられる IT や IoT の高度な専門的な知見に加え、経営的な知見が不可欠である。このような高度な専門的知見を要する「セキュリティ統括人材」の育成には様々のアプローチが考えられるが、育成の対象者を多数の識者が参加する本検討会に積極的に参加させることも実効的かつ有効なアプローチのひとつである。

最後にサイバー攻撃を社会的なリスクと認識して、社会的な視点から企業の壁を越えて、互いに知り得た情報や自らの取り組みを交換する具体的なアクションプランを設け、社会全体の耐性を向上させる取り組みが急務である。本検討会は重要インフラを担う企業等との丁寧な意見交換を経て、様々の社会的な発信につなげ、関係省庁とも連携を拡げていく所存である、引き続き関係各位のご理解とご支援を賜りたい。

以上