「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

第 1.0 版

2016 年 9 月 14 日

産業横断サイバーセキュリティ人材育成検討会　事務局

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 2015 年 6 月から 2016 年 6 月までの内容を纏めた第一期最終報告です。本検討会に関心のある方々に向けて、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おります。

本報告書をお読みいただくに当り、全体の概要を先ず知りたいという方は第 2 章を、本検討会の取り組みの全体像を知りたい方は第 2 章から第 4 章を、今後のサイバーセキュリティ対策へのヒントを探されている方は第 4 章から第 6 章をご覧ください。さらには、本取り組みの成果を自社内に展開することを検討される場合は、appendix を参照いただくことをお勧めします。

また、2015 年 6 月から 2015 年 12 月までの討議経過については、中間報告として、「産業横断サイバーセキュリティ人材育成検討会」中間報告書第 1.0 版を公開しておりますので、詳細を確認したい場合は、そちらをご参照ください。

「産業横断サイバーセキュリティ人材育成検討会」中間報告第 1.0 版は、以下の URL からダウンロードが可能です。

http://cyber-risk.or.jp/sansanren/index.html

本検討会または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 まで。

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

2020 年のオリンピック・パラリンピックを控え、大会運営に関わる施設やそれを取り巻く様々な環境、特に重要インフラシステムに対するサイバーセキュリティ対策は喫緊の課題である。また、情報システムだけでなく制御系システムや各種デバイスを含むあらゆるモノがネットワークにつながる IoT 時代の到来により、サイバー脅威から守るべき対象が拡大している。それらは、世界中の攻撃者のさらなる興味を惹き攻撃の動機を与えており、産業界全体にとって、危険度が急激に増大しつつある。

2014 年 10 月、一般社団法人 日本経済団体連合会 (以下、経団連)において「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、約 30 社の主要企業による議論を経て、2015 年 2 月 17 日に経団連から国に対し、「サイバーセキュリティ対策の強化に向けた提言」が公開された。同提言において重要視された活動の 1 つである人材育成の実行を推進すべく、「サイバーセキュリティに関する懇談会」のメンバ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「産業横断サイバーセキュリティ人材育成検討会」を発足した。重要インフラ分野を中心とした企業 48 社（2016 年 8 月末現在）が結集し、産業界として取り組まなければ実現し得ないサイバーセキュリティ対策の各種課題において、最初に問題となる「人材の確保（育成と雇用)」に焦点を当て、日本の産業界・企業の実態に対する理解を深めながら「丁寧な議論」を進めてきた。

本検討会では、人材の確保（育成と雇用）を主テーマとしながら、そのために重要となる業界ごと、業界間の情報共有の仕組みの醸成、各企業・各業界に必要なセキュリティ能力の明確化、各社の社内教育プログラム／ツール等の共有、学生教育・社会人教育の支援策の検討等に取り組んできた。

また、「サイバーセキュリティ基本法」の成立（2014 年 11 月）や「サイバーセキュリティ経営ガイドライン」策定（2015 年 12 月、経済産業省）等もあり、サイバーセキュリティは国家戦略としての認識も高まってきている。サイバーセキュリティは企業のコストではなく企業価値向上のための「経営課題」と捉え、経営者のリーダシップが重要視されるようになっている。このような状況の下、セキュリティ対応力向上に向けた産業横断での「信頼の輪」の構築にも努めてきた。

第一期（2015 年 6 月から 2016 年 6 月）は、上記のスタンスで、日本企業（特にユーザ企業）の組織構造とセキュリティ業務との関係に関する実態把握と、主に産業界共通の情報システム部門領域を対象とした人材定義に取り組んできており、具体的な成果の一つとして、「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)」等のツール一式を完成させた（詳細は次章以降参照)。

これまでの活動では、経団連の支持の下、国（NISC[1]、文科省、経産省、総務省等）との継続的な意見交換、情報交換、各種セキュリティ関連組織との交流を行っており、官・学の各所から期待されていた産業界として求める人材像について一定の整理を提示できたこともあり、サイバーセキュリティ人材育成に関する産業界の代表組織として認識されつつある。

今後、第二期(2016 年 10 月以降）として、人材定義に関しては業界ごとの違いに着目した展開の検討を進めながら、人材育成・維持のエコシステム実現に向けた具施策を検討、実行推進に注力する予定である。

[1] NISC 内閣サイバーセキュリティセンター

2. 概要

2.1. 「サイバーセキュリティ人材育成検討会」の目的と意義

＜本検討会の目的＞

これまでの手法では解決できないサイバー脅威の急増に対し、新しい課題に対応できるセキュリティ人材（サイバーセキュリティ人材[2]）が圧倒的に不足する日本の産業界において、それぞれの企業が必要最小限の人材を確保できるようにするためには、IT 企業もユーザ企業も含めた業界横断の協力体制が必須である。本検討会は、産業界として取り組まなければ実現し得ないサイバーセキュリティ対策の各種課題において、まずは最初に問題となる「人材確保（育成と雇用）の在り方」に焦点を当て、重要インフラ分野を中心とした日本の企業が結集し協力し合い一丸となって取り組むことを目的とする。

＜本検討会の意義＞

本検討会では、産業横断の協力体制により、日本の産業界・企業の実態に対する理解を深めながら「丁寧な議論」を進め、産業界に必要な真の人材像（人材要件）を日本の標準的なサイバーセキュリティ対応組織体制のモデルとして定義・見える化し、それに基づく具体的な人材育成施策を立案・推進し、最終的には、セキュリティ人材育成のエコシステム（人材を育成・雇用・活用し続ける循環）の実現に資する活動を目指す。

また、「人材確保（育成と雇用）の在り方」を含むあらゆるサイバーセキュリティ対応は、経済競争力に大きくかかわるサイバー空間での企業活動において、企業のコストではなく企業価値向上のための「経営課題」との認識が浸透し始めている昨今、サイバーセキュリティに関する諸問題に対して産業界が一丸となって対処することを支援・リードし、日本企業のサイバー空間での競争力向上を狙った産業横断での「信頼の輪」の構築も目指している。

2.2. これまでの主な活動

本検討会で、最初に取り組むべき目標は①社内人材育成の推進、②次世代に向けた人材育成、③情報共有の推進の 3 つとした。

[2] サイバーセキュリティ人材：サイバー空間におけるセキュリティ対策を実践できる人材。ICT 関連の技術に明るい人材と想定されたが、ユーザ企業の経営活動において ICT 技術が不可欠になり、かつ情報資産がインターネット網を通じてサイバー空間と密接につながっている現状を踏まえ、技術のみならず幅広いセキュリティ人材や、ISMS 等の情報セキュリティ人材との比較を行いながらサイバーセキュリティ人材の定義を検証していくこととした。

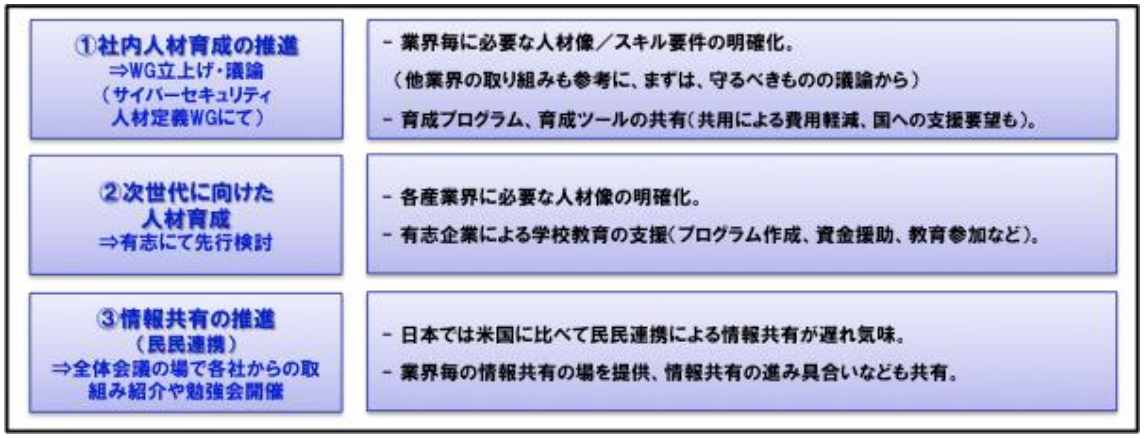

図 1 産業横断サイバーセキュリティ人材育成検討会の目標

また、本検討会では、下図のように配下に３つのグループを作成し、上記「情報共有」、「人材育成」、「産学連携」を推進してきた（詳細は 3 章、4 章参照）。

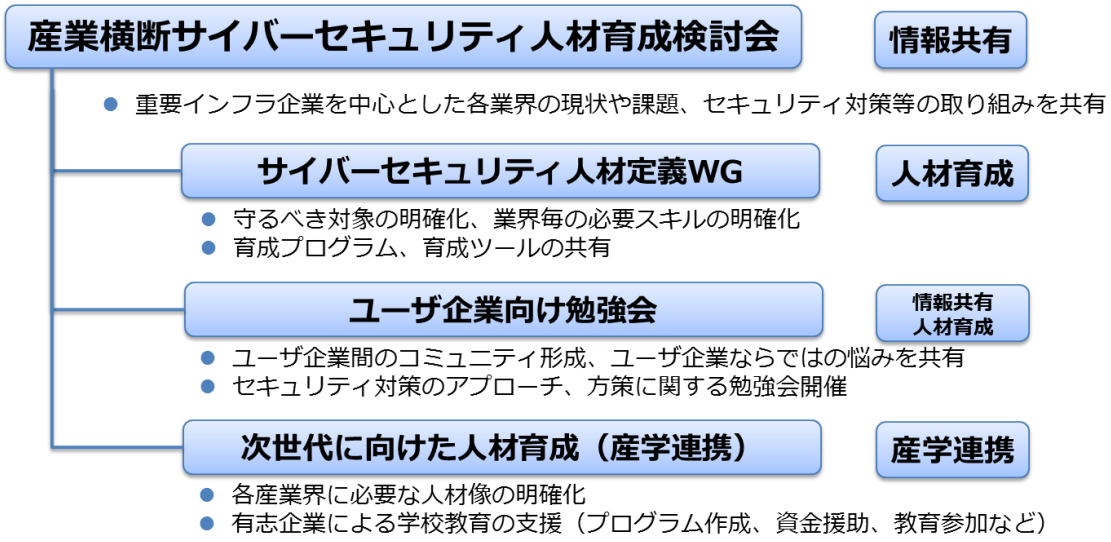

図 2 産業横断サイバーセキュリティ人材育成検討会の会議体

活動スケジュールは、2016 年 6 月までを第一期（Stage1）とし、第一期を前半と後半に分割した。前半では、想定された課題に関して参加者からの意見を広く集め、解くべき課題を出来るだけ具体的に定義した。後半では、前半の提示課題を踏まえ、企業の情報システム部門を対象としたセキュリティ人材の定義を実施した（図 3）。

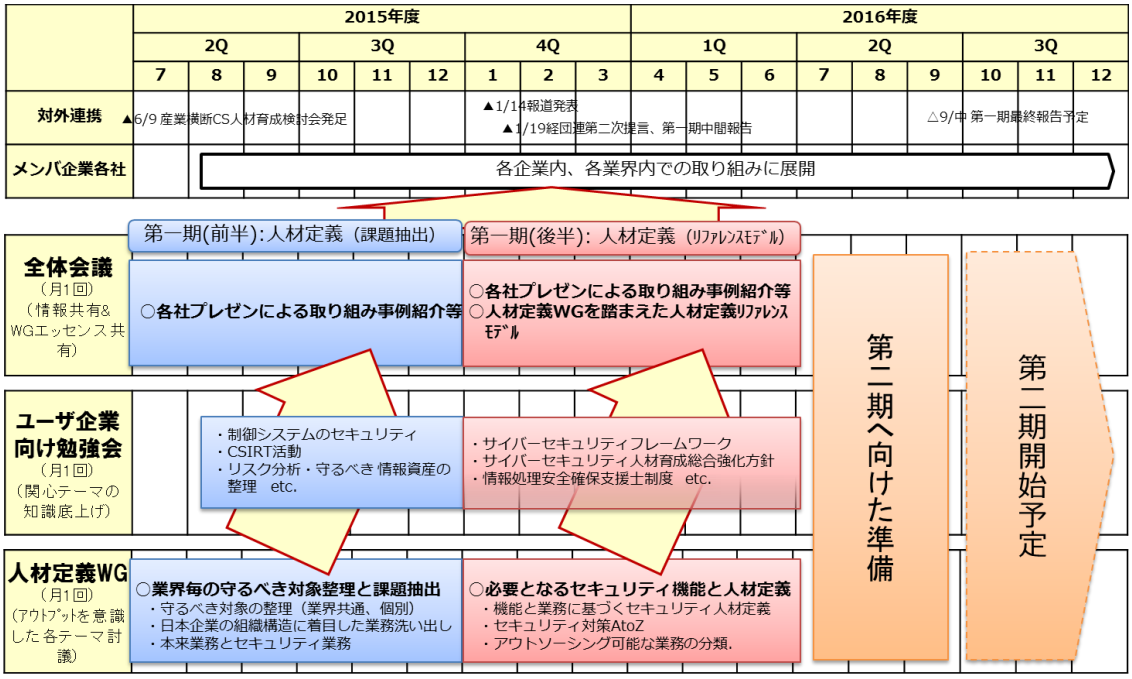

図 3 本検討会の活動スケジュール

2.3. 第一期検討会の成果（概要）

前述の 3 つの目標に対する第一期の取り組み成果を以下に記す。

① 「社内人材育成の推進」に対する成果

各業界・各企業の守るべきものを踏まえた人材像定義に向け、まずは「情報システム領域」をスコープに、日本企業におけるセキュリティ業務の実態把握、人材配置・機能分布のリファレンスモデルを作成。その上で、必要となるサイバーセキュリティ機能を洗い出し、それら機能を実現する要求知識と業務区分で人材を定義した。その成果として、幾つかの有効策（案）が知見として得られた。

まず、第一期前半（2015 年 6 月から 2015 年 12 月）においては、日本企業（特にユーザ企業）の組織構造とセキュリティ業務との関係についての実態分析を行った結果、以下のような課題が得られた。

- 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おり、CSIRT 等のセキュリティ専門組織の人材育成だけでは不十分であること。
- ユーザ企業としてセキュリティ人材を育成または採用し、企業として活用・維持し続けることが可能な仕組みが必須であり、そのための産学官連携の在り方の議論が急務であること。

次に、第一期後半（2016 年 1 月から 2016 年 6 月）においては、第一期前半で得られた上記課題を踏まえ、日本のユーザ企業における情報システム部門をスコープに、必要となるサイバーセキュリティ機能を洗い出し、それら機能を実現する要求知識と業務区分で人材

を定義した。

具体的な成果物は、以下の 4 点（詳細は 3 章を参照）。

(i) 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～
サイバーセキュリティ対策機能を実現する業務とそれを担う各種役割（担当）ごとの要求知識＆業務区分

(ii) 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～
ユーザ企業の情報システム部門等に勤務するエンジニア及び非エンジニア出身者の業務バイブル

(iii) 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
自社内で管理監督すべき業務（インソース）とアウトソーシング可能な業務の分類（一考）

(iv) 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
要求知識と業務区分に基づく人材定義を、iCD／i コンピテンシ ディクショナリ[3]によるスキルディクショナリ等にマッピング（一考）

② 「次世代に向けた人材育成の推進」に対する成果

有志企業メンバにより、教育機関（大学、高専）との産学連携方法の具体化に向けた議論を行い、３件の実案件へ結実した。

・東京工業大学と野村総合研究所が連携協定を締結
https://www.nri.com/jp/news/2016/160510_1.aspx
・九州大学サイバーセキュリティセンターにサイバーセキュリティ人材育成のための寄附研究部門を設置
http://pr.fujitsu.com/jp/news/2016/06/1.html
・国立高専機構殿と若手セキュリティ人材育成に関するディスカッションを実施、今年度から具体的施策についての検討を開始

③ 「情報共有の推進」に対する成果

参加企業が抱える課題や取り組み、さらには、各社のインシデント対応状況等、もう一歩踏み込んだ情報を含めての相互共有を継続的に行っており、その活動自体が各社の人材育成に活かされた。

[3] i コンピテンシ ディクショナリ：情報処理推進機構発行

2.4. 考察（概要）

第一期検討会の最大の成果は前述のとおり、人材定義に関する前述の各種成果物であり、それらを作成する過程において様々な考察を行った。以下、特筆すべき 3 点についてその概要を記す（詳細は 3 章を参照）。

① CISO に関する考察

海外企業と日本企業の CISO の相違点、日本企業における CISO の役割、CISO は役員であるべきか、CISO と CIO/CSO/CRO 等との関係／位置づけ等の話題で議論が行われた。

日本企業の場合、CISO がサイバーセキュリティに関する専門的な知識や実務経験が豊富なケースは少なく、CISO の役割自体が米国のようなサイバーセキュリティ先進国のそれとは異なるため、日本固有の状況を前提としたサイバーセキュリティ対応体制の構築を行っている組織が多いことが分かった。また、サイバーセキュリティ経営ガイドラインには、CISO という記述があり、今後のセキュリティの経営に対する重要度を考慮すると役員であることが望ましいが、日本の現状を考慮すると実際に役員であることよりも、任務を果たすための権限を経営トップから委譲されていることが重要であり、任務を果たすための権限を経営トップから委譲されているかが重要であり、本検討会では、”サイバーセキュリティ対策統括”機能に責任を負う役割として「CISO / CRO / CIO 等」を位置づけた。

② サイバーセキュリティ対応体制の様々な形

本検討会での情報共有により、企業ごとにサイバーセキュリティ対応体制は異なることが判ってきた。体制構築はその会社の業態、組織構成、また、企業文化によって、それぞれの企業の特有事情を加味して行われている（具体的な事例は第 3 章を参照）。しかし、いずれの企業も、会社組織運営の中での位置づけ（責任や権限に関する経営層との関係等）やインシデント発生事での対応体制に関しては留意して検討されていた。

③ サイバーセキュリティ専門部署の必要性

今回、本検討会では、人材定義を考える際に、総務部からの機能分化モデル（第 3 章参照）を作成し、必要な機能・役割を洗い出したが、常に進化する外部からの脅威や攻撃者を想定しなければならないサイバーセキュリティに関しては、既に存在する機能を分化してできた部門だけでは対応が困難という考えに至り、サイバーセキュリティを担当する専門部署（本検討会での人材定義においては「サイバーセキュリティ統括室」と仮称）の保有／設置がどの企業、組織にも重要となってくると思われる。

2.5. 今後の予定（概要）

今後は、人材育成・維持のエコシステム実現に向け、産業界としての具体的な施策を検討・実行推進する次のステージに進む。

以下について 2016 年 10 月以降取り組む予定である。

- セキュリティ人材定義の拡張：プロダクション（システム／業務）編
- 人材定義に基づく、産業界の人材不足の現状把握、および産業界のニーズ（育成が急務な人材）を具体化
- 取り扱う情報の種類・量・質の向上と信頼の輪の拡大を目指す情報共有の活性化（業界ごとの ISAC 設立を促す）
- 日本の産業界・企業の特性・実状に即した人材育成・雇用・活用（維持）が効果的に連携するエコシステムの具体案を検討・推進
- 先行している産学連携（寄附講座）の水平展開および拡張（マネジメント系、制御系等）を推進
- 2020 年に向けたセキュリティ人材の量的不足とトップガン人材育成に関する検討

3. 活動成果

サイバー脅威の急増に対してセキュリティ人材が圧倒的に不足する日本の産業界において、それぞれの企業が必要最小限の人材を確保できるようにするためには、IT 企業もユーザ企業も含めた業界横断の協力体制が必須である。本検討会は、産業界として取り組まなければ実現し得ないサイバーセキュリティ対策の各種課題において、まずは最初に問題となる「人材確保（育成と雇用）の在り方」に焦点を当て、重要インフラ分野を中心とした日本の企業が結集し協力し合い一丸となって取り組むことを目的とする。

本検討会では、産業横断の協力体制により、日本の産業界・企業の実態に対する理解を深めながら「丁寧な議論」を進め、産業界に必要な真の人材像（人材要件）を日本の標準的なサイバーセキュリティ対応組織体制のモデルとして定義・見える化し、それに基づく具体的な人材育成施策を立案・推進し、最終的には、セキュリティ人材育成のエコシステム（人材を育成・雇用・活用し続ける循環）の実現に資する活動を目指す。

また、「人材確保（育成と雇用）の在り方」を含むあらゆるサイバーセキュリティ対応は、経済競争力に大きくかかわるサイバー空間での企業活動において、企業のコストではなく企業価値向上のための「経営課題」との認識が浸透し始めている昨今、サイバーセキュリティに関する諸問題に対して産業界が一丸となって対処することを支援・リードし、日本企業のサイバー空間での競争力向上を狙った産業横断での「信頼の輪」の構築も目指している。

主な活動は、①育成プログラムの共用等による各社の人材育成、②有志企業による大学教育支援等将来の人材育成、③サイバー攻撃対策の取り組み等企業や業界ごとの情報共有化の 3 つとし、それぞれの活動において、産業界としての明確な意思を持ってスピード感ある具体的な施策に取り組むものである（詳細は後述）。

官や学の先行する取り組みに追従するだけではなく、日本の産業界が提供する重要インフラや様々な社会基盤、および、その上で営まれる国民の生活を、深刻化するサイバー脅威から守るための人材育成を産業界自らが連携し、先導する姿勢を見せて臨むことが極めて重要と考える。また、合わせてサイバーセキュリティの取り組みを推進していくためには、サイバーセキュリティは経営課題と捉える、経営者の理解が必要不可欠である。

上記を踏まえ、本検討会が重要インフラ事業者を中心としたユーザ企業により構成されていることから、日本企業に特有の組織運営、人事管理や定期人事異動、業務分担におけるセキュリティ関連業務の割合等を踏まえた、サイバーセキュリティ人材のあり方を検討すべく討議を重ねることとした。本章では、第一期（2015 年 6 月～2016 年 6 月）での成果を説明し、検討会の議論によって得られたいくつかの考察を述べる。検討会で活発に行われた議論の経緯については、別紙 1 産業横断 第一期報告書_人材定義 WG を参照いただきたい。

3.1. 課題設定、論点、アプローチ

3.1.1.　初期の課題設定

ユーザ企業におけるサイバーセキュリティ人材の育成を考えていくにあたり、もっとも重要なテーマは、セキュリティ専門の人材を実際に「配置」できるのか、との課題を検討することにあった。

この「配置」とは、配属されるポジションの有無という意味だけではなく、実際に社内で発生しているサイバーセキュリティ対策の取り組みの量及び質、それら対策に見合う人材（能力や人数の観点での明確化）の必要性、業種・業界により異なる事業環境を踏まえたサイバーセキュリティ対策の重要度の違い等の業態固有の内容が考慮される。更には、社内で専任者として担当するほどの継続的な業務が存在するか否か、またユーザ企業が（1 社又はグループ会社単位において）必要とする採用数と効率的な育成が可能な規模感との兼ね合い、他の職種とのバランス、評価基準の有無等多くの意味合いを含み、検証すべき項目が多数存在した。

特に、検討会発足当時は、サイバーセキュリティ事件・事故が発生すると、セキュリティ専門事業者やセキュリティ製品ベンダによる情報提供や積極的な売り込みも行われており、ユーザ企業内部に各社からの提案内容の有効性を判断できる人材が少ないことや、経営層が自社にも「ハッカー」と呼ばれる専門家を配置しなければならないのではないかと不安を抱くことも少なくなかったため、まずはユーザ企業に求められるサイバーセキュリティ人材像を早急に検証していく必要性に迫られていた。

3.1.2.　主な論点

①　守るべきものに関する議論

企業におけるセキュリティ人材について検討するために、企業がサイバーセキュリティへの対応をどのように行っているかについて知る必要がある。また、企業としてサイバー攻撃から守るべき対象とするものについて、業界ごと、企業ごとの違いの有無を意識しながら把握する必要がある。

②　企業活動としてのセキュリティ対策のリファレンスモデル

現時点では、企業として行うべきセキュリティ対策についてのリファレンスモデルが存在していない。しかし、セキュリティ人材を定義する上でも、企業における典型的なモデルを想定する必要がある。

③　セキュリティ人材定義方法・表現手法

セキュリティ人材には様々な種類や職種や能力があり、それぞれが具体的にどのような人材であるのかを明確に定義しなければならない。

④　育成の対象となる人材がどこに存在するのか

セキュリティ人材育成の施策を考える際に、どこに育成対象が存在するかを正確に把握する必要がある。

⑤　「サイバーセキュリティ経営ガイドライン」

ユーザ企業として社内に構築すべきサイバーセキュリティ対応体制についても、早急に検討していく必要性がある。

3.1.3.　検討会でのアプローチ

①　サイバーセキュリティ対策のあるべき姿の共有

サイバーセキュリティ人材の定義を進める上で、そもそも、サイバーセキュリティ対策のあるべき姿を共有することが必要と考えられ、複数の視点から、対策の在り方を検討することが求められた。

参加企業においては、既に ISO/IEC27001 に基づく ISMS に準じた情報セキュリティ対策が実施されているケースが多く、加えて個人情報保護法に対応する取り組み、更には特定個人情報保護法への対応も進んでいる。そのような背景の中で、サイバーセキュリティ対策をどの基準でどこまで実施すべきか、との共有がなされていなければ、そもそも求められる人材を定義し、更に育成することは困難になると考えられた。

そこで、米国 NIST の発行する「サイバーセキュリティフレームワーク」や「NICE」に基づくサイバーセキュリティ対策の在り方を検討しつつ、検討会においても各社の取り組みの紹介や情報共有に基づく、現在の対策状況を共有する必要があった。

②　サイバーセキュリティ人材育成に関する検討スコープ

「サイバーセキュリティ人材育成」に関する検討を進めるにあたって、以下のような観点を検討スコープと考えた。

・セキュリティ人材の育成とは、どのような人材をどこまで育成するものなのか

これまでセキュリティ対策は ISO/IEC27001 認証や P マークの取得が主流となっており、これらの標準や基準、法令対応ではシステム基盤から業務システム、エンドポイント対するセキュリティや、ユーザに対するリテラシ等、各々のセキュリティ対策手法は明示してこなかった。

サイバーセキュリティ対策に求められる人材の育成に対しては、サイバーセキュリティ対策に必要となる個々の手段、タスクやスキル、育成対象となる人材レベル設定等、育成のあり方や人材の定義から協議していく必要があった。

・セキュリティ人材とは、そもそもどのような人材なのか

サイバーセキュリティ対策に必要とされる人材を定義するためには、まずはサイバーセキュリティ対策の全体像を理解する必要があり、更には組織としてどのような構成、体制に基づいて対処していくのかを協議・共有していく必要があった。

・ユーザ企業におけるセキュリティ対策はどこまでやるべきなのか

セキュリティ対策として求められるレベルを共有し、最低限の対策レベルとあるべき姿を明確にする必要があった。

・セキュリティ対策はユーザ企業自身でどこまで対応可能なものなのか

「サイバーセキュリティ経営ガイドライン」が発表される以前は、ISO/IEC27001 や個人情報保護法、特定個人情報保護法や経済産業省発行のガイドラインが求める安全管理措置が一般的に指標として使われており、システムのセキュリティ対策は IPA 発行の各種ガイドライン及び製品ベンダが発表する脆弱性情報に基づく運用対応が主となっている。

③　セキュリティインシデントへの現実的対応

サイバー攻撃やセキュリティ事故は毎月どこかの法人組織で発生しており、上場企業約 4000 社、グループ企業を含め数万社という法人に対して、セキュリティ専門事業者及びそこに従事する人員の数では不十分であることが想定された。

さらには、「サイバーセキュリティ経営ガイドライン」が発表されたことで、サプライチェーンを意識した取引先への対策の実施を含めて考えていくと、「アウトソーシング」を主体とした体制構築と対応の現状においては、対策が必要となる企業数とセキュリティ専門事業者の数を比較しても実質的に意味がないのではと考えられた。

そこで、本検討会では、ユーザ企業としてどのような人材を配置し、何を理解し、どのような対策を取れるのかという点と、アウトソーシング先となる ICT 企業、製品・サービスベンダ、セキュリティ専門事業者に何を求めていくべきなのかという点を分解して、日々の業務に則した体制の構築を検討していくこととした。

④　サイバーセキュリティ関連の基準の活用

中間報告の実施後、更なる人材定義の検討を進めるにあたり、これまでの組織分化の観点から、役割の種別の選定及び人材の能力定義に移行していくこととなった。

これは、検討会において各社の対応状況に関する情報共有を進めたことにより、参加企業におけるサイバーセキュリティ人材育成の取り組みに違いがあることが確認できたためであり、各社が参考としている情報源に対応した、網羅的な全体像の策定が必要になることが想定されたためである。

特に、以下の基準、モデル等を活用することとしたのは、参加企業が現在の取り組みを継続していく後押しとしての成果物が求められる、と考えたことによる。

・サイバーセキュリティ経営ガイドライン[4]　：経済産業省
・i コンピテンシ ディクショナリー[5]　：IPA
・サイバーセキュリティフレームワーク[6]　：NIST（米国）
・SP-800 シリーズ[7]　：NIST（米国）
・National Cybersecurity Workforce Framework[8]　：NICE（米国）[9]
・CSIRT 人材定義[10]　：日本シーサート協議会
・SOC 人材定義[11]　：日本セキュリティオペレーション事業者連絡会
・Secbok[12]　：NPO 日本ネットワークセキュリティ協会

⑤　人材定義における要件の非 ICT 分野への拡大

人材定義における要件としては、非 ICT 分野における知識や経験の必要性も加味するために、中間報告で発表した人材定義のモデル「**氷山モデル**[13]」を引き続き活用することとした。

この試みは、ユーザ企業における全社リスクマネジメント（ERM）への対応、人事管理や人事異動との関係、新たなキャリアパスの設計等を想定し、人事評価制度に組み込みやすい人材定義を策定することを目的としている。更には、重要なテーマとなっている「セキュリティ人材不足」に対応するため、サイバーセキュリティ対策の経験が無い社員が配属された場合でも率先して対策を講じることができるための後押しとなる要件を策定することを目指した。

⑥　サイバーセキュリティ人材定義の前提を考える

本検討会での討議において、当初サイバーセキュリティ人材をどのように定義していくのかというテーマに対し、国内にある様々なサイバーセキュリティ人材定義に関連する発表資料を参考としてきた。

しかしながら、これまで日本国内で発表されてきた ICT 業界及びセキュリティ専門事業者からの目線で作成されてきたスペシャリストの定義や育成計画は、日々サイバーセキュリティに関するインシデント対応を実践している人材を前提とする取り組みであったため、ユーザ企業の組織運営や人事管理の中に浸透させることが難しいと考えられた。

---

[4] サイバーセキュリティ経営ガイドライン　http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf
[5] i コンピテンシ ディクショナリー　https://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/
[6] サイバーセキュリティフレームワーク　http://www.nist.gov/cyberframework/index.cfm
[7] SP-800 シリーズ　http://csrc.nist.gov/publications/PubsSPs.html
[8] National Cybersecurity Workforce Framework　http://csrc.nist.gov/nice/framework/
[9] NICE（米国）　The National Initiative for Cybersecurity Education　http://csrc.nist.gov/nice/
[10] CSIRT 人材定義　http://www.nca.gr.jp/imgs/recruit-hr20151116.pdf
[11] SOC 人材定義　http://isog-j.org/output/2016/SOC_skill_v1.0.pdf
[12] Secbok　http://www.jnsa.org/result/2016/skillmap/
[13] 氷山モデル　Spencer, L. M. & Spencer, S. M.が 1993 年に提唱したコンピテンシーの評価方法の 1 つ。
海水面に浮かぶ氷山に見立て、水面より上にある可視的な部分をスキルや知識として育成が容易なものと理解し、水面の下にある潜在的な部分を自己概念や動機、性格等育成が困難であると考えるモデル。

そもそもユーザ企業におけるシステム運用においては、ユーザ企業自身が単独で実施することは少なく、システムベンダとの連携や協力の下で実現されている。従って、セキュリティ対策における開発、運用、インシデント対応と様々なフェーズにおいても、担当する人材の配置方式が異なることが想定された。この流れから「アウトソーシング」の在り方についても議論が必要になった。

また、サイバーセキュリティ対策の事項について、典型的な活動パターンを見い出す必要があるとの参加企業からの意見を受け「年間カレンダー」という形式に基づく「業務一覧」の策定を目指すこととなった。

この「業務一覧」は、ユーザ企業では一般的に行われている「人事異動」に着目し、業務手順に対する専門性と企業内における人事異動の基準が別々に運用される、という日本企業の特性に合わせたリファレンスとしての位置づけを持たせたものである。これは、サイバーセキュリティ対策や情報システムの管理等を経験していない（可能性がある）CISO 等及び CSIRT メンバが、日々何を確認し、どのような業務を遂行するべきかを明確にするものである。

3.2. 第一期検討会の成果

3.2.1. 企業におけるセキュリティ人材（機能・定義等のリファレンス）

本検討会の全体会議においては、企業のサイバーセキュリティ対応における様々な問題を解決するために、参加各社での取組状況の共有を行い、各組織においての問題を把握することを行った。その結果、あらゆる問題において最初に挙げられるセキュリティ人材に関する課題について取り組む「**人材定義 WG**」を設置することとした。

(1) 人材定義 WG の活動内容

一般的に、セキュリティ人材不足を解決する必要があるとは認識されているが、個々の企業においてそれを解決するためにどうするべきかが明確になっていない状況であった。そこで、人材定義 WG では、企業のセキュリティ人材が不足しているという理由を分析し、より深く原因を追及した。

我が国の公的なセキュリティ関連組織・団体で行われているセキュリティ人材の定義で多く見受けられるのは、必要とされるセキュリティ技術を用いて、セキュリティの人材を定義する方法である。今回、我々はこのようなスキルセットによる人材定義方式を敢えて行わなかった。

また、従来の人材定義では、セキュリティの専門技術中心のアプローチのため、ユーザ企業の人事部等では、かかるセキュリティ人材を採用し活用することは、業務の専門性やキャリアパス上から非常に困難と考えたからである。

そこで、セキュリティ人材定義 WG では、企業におけるサイバーセキュリティ対策に必要とされる機能を明らかにし、それらの機能を遂行するために必要な人材が果たす

べき役割を定める事で人材を定義するやり方を選択した。

その理由は、企業のセキュリティ対策として、行うべき機能を把握し、必要な人材像を明確にすることで、セキュリティ人材の教育や採用が容易かつ的確に実施できるようになることを目指したものである。

その結果、主に以下の点について検討を行った。

① 企業におけるサイバーセキュリティ対策の機能
企業におけるセキュリティ対策関連活動にはどのようなものがあり、何を行わなければならないのか。

② 企業におけるセキュリティ人材定義
セキュリティ対策関連活動を行うためにどのような人材が必要で、能力を規定する項目としてどのようなものが適当であるのか。

③ インソースとアウトソースのバランス
企業内部の人材で行わなければならない活動（インソース）と外部サービス等を利用（アウトソース）することが可能な活動のバランスをどうするべきか。

(2) 検討の成果物

検討の結果として、この第一期では、以下の成果を導出した。(表 1)

表 1 第一期検討会成果：人材定義関連

No.	名称	概要	成果物
1	**企業におけるサイバーセキュリティ対策の機能**		
2	**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～**	サイバーセキュリティ対策機能を実現する業務とそれを担う各種役割（担当）ごとの要求知識&業務区分	別添 A1-A3
3	**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～**	ユーザ企業の情報システム部門等に勤務するエンジニア及び非エンジニア出身者の業務バイブル	別添B
4	**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**	自社内で管理監督すべき業務（インソース）とアストソーシング可能な業務の分類（一考）	別添C
5	**産業横断 人材定義リファレンスに基づく**	要求知識と業務区分に基づく人材定義を、iCD／ｉコンピテンシ ディクショナリによるスキルデ	別添D

	スキルマッピング	ィクショナリ等にマッピング(一考)	

① 企業におけるサイバーセキュリティ対策の機能

まず第一期においては、様々な業態のユーザ企業においても現状はその存在が必須と想定され、かつ企業におけるセキュリティ対策を先導するであろう「情報システム部門」を対象とした。当該部門における運用を分化していくことで、どのような機能が必要とされているかを検討した。

機能分化を検討する具体的な方法としては、参加各社へのアンケートを実施した。この現状調査により、各社でどのような機能から情報システム部門が成り立っているかを把握した上で、人材定義 WG での議論を経て共通性と特異性を選別し、結果検討会として、29 個の機能を一般的な機能として定義した。(表 2)

表 2 セキュリティ機能定義一覧

セキュリティ機能定義	サイバーセキュリティ対策の機能を実現する業務例
サイバーセキュリティ統括	サイバーセキュリティ対策に関する全社的統括
事業戦略 **中期計画**	コンプライアンス、ガバナンス及びリスクマネジメントの観点に基づくセキュリティ対策
年次計画	セキュリティ対策に係る実施計画の企画立案 規程・ルールの策定
ICT 企画（個別 IT 企画）	各事業に対する IT 導入・構築運用改善計画の企画立案 ガイドライン・マニュアルの策定
	ライセンス管理を踏まえた、リプレース計画の企画立案 固定資産管理・ソフトウェア会計管理
セキュリティ実装計画	ユーザビリティの観点に基づく機能改善・実装計画の企画立案 エンドポイント及び UI に関するセキュリティ機能改善計画の策定
	システムセキュリティの観点に基づく機能改善・実装計画の企画立案 システム構成に関するセキュリティ機能改善計画の策定
IT-BCP	ICT 環境における事業継続計画の策定 サイバーセキュリティ保険の導入検討
ディザスタリカバリ	災害対策（DR）に関する ICT 環境改善計画の策定
	災害対策及び災害発生時に関する稼働計画の策定
情報セキュリティ **マネジメント**	情報資産保護活動における ICT 環境改善計画の策定 情報資産の保護基準・保護方法の改善、情報漏洩保険の導入検討
	情報資産保護活動における ICT 運用改善活動の策定 情報資産の棚卸
セキュリティ対策導入・	セキュア構築設計の企画立案

開発計画	要件定義及基本設計におけるセキュアデザイン
	セキュア運用設計の企画立案 詳細設計及び運用改善におけるセキュアデザイン
	多層防御に基づくセキュア設計管理 ネットワーク及びシステム構成に対するセキュアデザイン
システムセキュリティ対応	システム構築及びシステム運用のセキュリティ対策分野に関するプロジェクトマネジメント及びプロジェクト運用支援
セキュリティ製品品質管理	セキュリティ対策関連の製品・サービスに対する評価検証
運用テスト **パッチ管理**	脆弱性診断（導入時・運用時） パッチ適用時の評価テスト
セキュリティ機能評価/改善	全システムに対するパッチ管理及び脆弱性診断に関する計画の企画立案
	セキュリティ対策関連の製品・サービスの選定及び実装支援
	セキュリティ対策におけるシステム的機能の継続的改善活動
ID 管理 **アクセス権管理**	ActiveDirectry 管理、シングルサインオン管理
	システム、フォルダ等アクセス権管理
サポート **教育**	社内の ICT リテラシ向上のためのユーザ支援 リスク対応教育の企画・計画・実施
CSIRT	コマンダー ： インシデント発生時の全社対応及び CISO 等補佐
	インシデントハンドリング・トリアージ ： インシデント発生時の初動対応及び収束対応
	脅威情報収集、対策情報収集 ： 日常のインシデント情報収集及び社内共有活動
	フォレンジックス ：機器の保全、被害拡大抑止、証跡保全活動
	トレーニング ： インシデント対応能力向上に向けた教育の企画・計画・実施
SOC	セキュリティオペレーション業務における導入・構築
	セキュリティオペレーション業務における運用管理
	セキュリティオペレーション業務におけるインシデント対応
OS 管理	OS・プラットフォーム・ミドルウェア等に対するバージョン管理
アプリケーション管理	基幹システム等のアプリケーションに関するバージョン管理
クラウドサービス管理	クラウドサービス選定及び利用管理、セキュリティ対策
DB 機器管理	DB 機器等に関するバージョン管理
DB 構成管理	データマネジメントに必要な DB 管理（データ特性に合わせた DB 構成管理）
DB データセキュリティ	DB 設定及び格納されるデータに対するセキュリティ対策
通信環境管理	ファイアウォール設定 プロキシ設定
	WAF 設定　（WEB サービスセキュリティ対策）

通信監視	通信監視（死活監視・パケット監視等）
	通信遮断管理（IPS/IDS 機能管理） スレット・インテリジェンス（脅威情報）の対策活用
ヘルプデスク	インシデント発生時の問合せ窓口 端末・機器異常（インシデント発生以前）の相談窓口
セキュリティ監査	情報セキュリティ監査、物理的セキュリティ監査
システム監査	システム監査
セキュリティ 調達管理	取引先選定
	製品・サービス調達

これらの機能の関係性を表現するために、横軸に機能が発動する時間軸、縦軸に当該機能を大きく 4 つに分類した。機能相互の関係性を図 4 に示す。

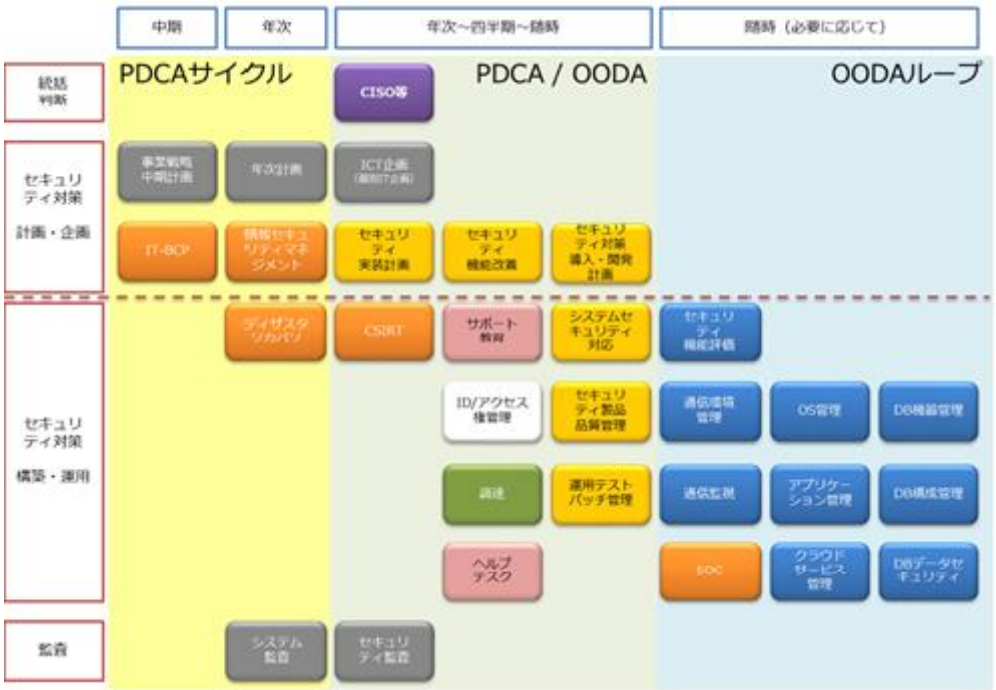

図 4 サイバーセキュリティ対策の機能定義（関係図）

今回の議論の中で、計画・企画に関わる機能は、中期から年次等の長期にわたって PDCA サイクルによって実施されるものが多く、その一方で運用に関わるものは、インシデント発生や日々の活動等必要に応じて実施される特性があることから OODA（ウーダ）ループ[14]によって実施される、という分類を行った。

14 OODA ループは Observe(観察)→Orientation(方向性の決定)→Decision (判断)→Action(行動)の頭文字を取ったもので、人間が行動を起こす際の思考を模式化したもの。

OODA ループで実施される機能を担当する組織では、少ない情報で即座に判断し対応することが要求されることを考え、体制や権限委譲等をどのように設計するかを検討する必要がある。

サイバーセキュリティ対策に関連する機能を、各参加組織で実際に実施されている活動から抽出することで、現実に即した機能を定義することが出来たと考える。加えて、今回定義した 29 の機能の多くがサイバーセキュリティに特化したものではなく、既存の固有業務の中での実施事項であることから、現状の企業組織においては、通常の技術者や数少ないセキュリティ技術者が、複数の部署で複数の役割を掛け持ちで担わされている実態が想起されるものであり、セキュリティ人材不足の具体的な姿が見えたともいえる。

② 産業横断 人材定義リファレンス

人材定義 WG では、定義された 29 の機能を実施する役割（担当）として、情報システム部門におけるセキュリティ機能を担う 24 の役割（担当）と、情報システム部門以外のセキュリティ担当職として 6 つを定義した。（表 3）

機能を担う役割を細かく検討していけば、より多くの役割（担当）に分類することが可能であるし、曖昧さもなくなる。しかしながら、役割を細分化するにより、当初の目的の一つである企業でのセキュリティ人材の採用や教育を行うための利活用することは難しくなると考え、できるだけ少ない役割（担当）に留めることを心がけた。

表 3 サイバーセキュリティ機能を担う役割（担当）一覧

	カテゴリ	*役割（担当）*	*設置粒度*
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**	全社
		サイバーセキュリティ統括（室等）	全社
		システム部門責任者	部門
		システム管理者	部門 / システム
		ネットワーク管理者	部門 / システム
		CSIRT 責任者	部門
	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**	部門
		セキュリティ設計担当	部門
		構築系サイバーセキュリティ担当	部門
		運用系サイバーセキュリティ担当	部門
		CSIRT 担当	会社 / 部門
		SOC 担当	部門
		ISMS 担当	全社 / 部門
	担当職	**システム企画担当**	部門 / システム
		基幹システム構築担当	部門 / システム
		基幹システム運用担当	部門 / システム

OODA ループを敵より早く回す事により、相手に先んじて行動し、敵に勝つ事が出来るという考え方。情報が部分的にしか得られず、敵が存在して直ぐに対応する必要がある場面に適した考え方。

		WEB サービス担当	部門 / システム
		業務アプリケーション担当	部門 / システム
		インフラ担当	部門 / システム
		サーバ担当	部門 / システム
		DB 担当	部門 / システム
		ネットワーク担当	部門 / システム
		サポート・教育担当	会社 / 部門
		ヘルプデスク担当	会社 / 部門
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**	会社
		監査担当	部門
		特定個人情報取扱責任者	会社
		特定個人情報取扱担当	会社
		個人情報取扱責任者	会社
		個人情報取扱担当	会社

情報システム部門以外のセキュリティ担当者とは、法律等（例：個人情報保護法）で設置が義務付けられている役職と、監査等別途設置すべき役割等を追加したものである。

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）は、6 つの管理職、7 つのセキュリティ担当職、11 の担当職に分かれている。管理職は統括・判断機能や、セキュリティ対策計画・企画に対して業務責任を持ったり、業務責任者を支援したりする立場の人である。セキュリティ担当職は、セキュリティ固有の業務を担当する。担当職は、システム開発・運用やネットワーク運用等、情報システムに必要な通常の職務の中でセキュリティに関わる業務を行う立場の人たちである。

人材定義は、これら 30 の役割（担当）それぞれが、先の 29 の機能に対して、次の 2 つの軸で行った。

I. 業務区分：その役割（担当）が、それぞれの機能において持つべき責任や権限を 5 段階（数字：1～5）で表現したもの。

表 4 人材定義リファレンス：業務区分一覧

業務区分	業務役割
5	業務責任を負う
4	業務責任者を支援・補佐する
3	業務を担当する
2	業務担当者を支援・補佐する
1	業務内容を理解する

II. 要求知識：その役割（担当）において、それぞれの機能に関してどれくらいの（ICT 分野における）知識を持つべきかを 3 段階（◎△×）で表現したもの。

表 5 人材定義リファレンス：要求知識レベル

（ICT 分野における）要求知識	要求レベル
○	必須
△	あると良い
×	なくても良い

具体的には、図 5 で説明する。

「CISO/CRO/CIO 等」の役割（担当）では、 “サイバーセキュリティ統括”機能に対しては、業務区分 5 で「業務責任を負う」となっており、“事業戦略・中期計画”、“年次計画”、“ICT 企画（個別 IT 企画)”等については、業務区分 4 で「業務責任者を支援・補佐する」ことが求められている。

また、「システム部門責任者」が業務区分 4 で“サイバーセキュリティ統括“機能においては、「CISO/CRO/CIO 等」を支援・補佐するとなっている。

また、要求知識としては図 6 人材定義リファレンス - 要求知識のみ（抜粋）で示すように「CISO/CRO/CIO 等」の役割（担当)、「システム部門責任者」ともに、“サイバーセキュリティ統括”機能から、“情報セキュリティマネジメント”までの知識が必須となっている。

セキュリティ機能定義最終報告	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
	全社	全社	部門	部門／システム	部門／システム	部門
	業務区分	業務区分	業務区分	業務区分	業務区分	業務区分
サイバーセキュリティ統括	5	4	4	1	1	4
事業戦略中期計画	4	4	5	4	4	4
年次計画	4	4	5	4	4	4
ICT企画（個別IT企画）	4	4	5	4	4	1
	4	1	5	4	4	1
セキュリティ実装計画	4	1	5	4	4	1
	4	4	5	4	4	1
IT-BCP	4	1	5	4	4	1
ディザスタリカバリ	4	1	5	4	4	1
	4	1	5	4	4	1
情報セキュリティマネジメント	4	4	5	4	4	1
	4	4	5	4	4	1

図 5 人材定義リファレンス - 業務区分のみ（抜粋）

セキュリティ機能定義最終報告	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
	全社	全社	部門	部門／システム	部門／システム	部門
	要求知識	要求知識	要求知識	要求知識	要求知識	要求知識
サイバーセキュリティ統括	○	○	○	×	×	○
事業戦略中期計画	○	○	○	△	△	○
年次計画	○	○	○	△	△	○
ICT企画（個別IT企画）	○	○	○	△	△	△
	○	△	○	△	△	△
セキュリティ実装計画	○	△	○	△	△	△
	○	○	○	△	△	△
IT-BCP	○	△	○	△	△	△
ディザスタリカバリ	○	△	○	△	△	△
	○	△	○	△	△	△
情報セキュリティマネジメント	○	○	○	○	○	△
	○	○	○	○	○	△

図 6 人材定義リファレンス - 要求知識のみ（抜粋）

③　産業横断 セキュリティ対策カレンダー

日本の企業の多くは、4 月を年度初めとして一年間の年度計画を立案し、ビジネス活動を行っていくことが通常行われる。多くの組織で年間計画表等の名前で一年間どのような活動やイベントがあるかを示した一覧が作られている。それと同様に、サイバーセキュリティに関して、多くの企業で年間を通じてどのような行事や作業が行われるのかを俯瞰して、見られるようにしたのが、このセキュリティ対策カレンダーである。

図 7 に示すように、“リスクマネジメント委員会”は、毎月定常的に開催されるであろうし、年次計画方針発表は年度の初めに行われ、年度末には、その年の総括が発表される。当然、日々の運用は定常的に行われ、インシデント対応等は不定期に発生時に随時実施するものもある。

AtoZ 共通項目

セキュリティ機能定義 最終報告	月例	定常（日次）業務	インシデント発生時	第１四半期（例：4月～6月）			第２四半期（例：7月～9月）		
サイバーセキュリティ統括	リスクマネジメント委員会 経営会議								
事業戦略 中期計画	リスクマネジメント委員会 経営会議								
年次計画	経営会議	CIO/CISO支援 規程・ルール策定・改定	CIO/CISO支援	方針発表		年次計画進捗確認			年次計画進捗確認 規程改定
ICT企画 （個別IT企画）	IT戦略会議	CIO/CISO支援 ガイドライン・マニュアル改定	インシデント対応判断（全体）			年次計画進捗確認			年次計画進捗確認 ガイドライン
	セキュリティ対応進捗会議	セキュリティ対応進捗評価	インシデント対応状況評価						システム運用におけるKPI評価
セキュリティ 実装計画		システム運用に対するセキュリティ対策評価	インシデント対応状況評価						システム機能改善計画評価
		システム・機器等に対するセキュリティ対策評価	インシデント対応状況評価						
IT-BCP	リスクマネジメント委員会 CIO/CISO支援	バックアップ体制維持 システム更新対応	システム更新評価	方針発表			IT-BCP内部監査	IT-BCP是正措置	IT-BCP訓練計画
ディザスタリカバリ	リスクマネジメント委員会 CIO/CISO支援	災害関連情報収集 災害対策ツール情報収集							防災訓練計画
			インシデント対応判断（災害）						
情報セキュリティ マネジメント	ISMS委員会			方針発表			ISMS内部監査		
	教育計画策定 インシデント注意喚起		インシデント対応判断（情報資産）	新規入社社員教育				ISMS是正措置	
セキュリティ対策 導入・開発計画	構築PJ セキュリティ対応	構築PJ セキュリティ対応	構築PJ セキュリティ対応						
		セキュリティ対策 運用状況監視	運用PJ セキュリティ対応	運用改善 設計支援			運用改善 設計支援		
		インシデント情報収集	OSI7レイヤー整合性評価				運用改善評価		

図 7 産業横断 セキュリティ対策カレンダー（抜粋）

各社ごとに活動内容は異なるため、本カレンダーをベースに自社向けにアレンジして適用することを想定している。今回、検討会に参加している各社でどのような活動が行われているかを集めてカレンダーとしてまとめたことにより、他社が実施していた活動を、自社の活動として取り入れる等、実際的に活用した事例も既に現れている。

また、新たに就任した CISO が、全体としてどのような事項を実行しなければならないのか、を把握するために活用するような使い方も可能である。

④　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

アウトソースはセキュリティ人材を自社内に抱えることが難しいユーザ企業にとって、セキュリティ対策を実装するために非常に有用な手段である。しかしながら、全てを外部委託事業者に丸投げし、いざインシデント発生時に対応が取れないという事態に陥らないようにすることが肝要である。

具体的には、セキュリティ対策において自社で保有すべき機能を明確に意識し、適正に計画し、内部の役割と外部の役割のすりあわせを行い、外部サービスを有効かつ効率的に利用することが求められる。

検討会では、29 のサイバーセキュリティ対策の機能に対して、インソースとアウトソースのバランスをどのように取るべきかを検討したが、アウトソースに関する考え方はそれぞれの組織で異なっており、何をアウトソースすべきかという結論には至らなかった。そこで、何らかのサービスを外部に業務委託する場合に、少なくとも、管理監督業務は、自社内部（インソース）で行うべきであり、それらについての 3 種類の担当（表 6）ごとに記述した。

表 6 管理監督業務（インソース）担当一覧

所属／勤務形態	担当
情報システム部門（情報システム子会社を含む）	管理者
	担当者
常駐者	技術派遣／コンサルタント

また、アウトソース可能業務を次の 3 つの委託先に分類して記述した。

- 構築・運用委託先インテグレータ
- 製品・サービスベンダ
- セキュリティ専門事業者

なお、“CSIRT”機能と“SOC”機能に関しては、各々日本シーサート協議会（NCA）[15]と日本セキュリティオペレーション事業者協議会（ISOG-J）[16]で詳細に検討されており、本検討会としては、両団体から発行されているドキュメントを参照することとした。

⑤　産業横断 人材定義とスキルセットの関係

人材定義 WG では、29 の機能において、30 の役割（担当）の業務区分と要求知識を定

15 CSIRT 人材の定義と確保 Ver.1.0　http://www.nca.gr.jp/imgs/recruit-hr20151116.pdf

16 SOC の役割と人材のスキル v1.0 http://isog-j.org/output/2016/SOC_skill_v1.0.pdf

めることで人材定義を行った。これにより、それぞれの役割（担当）に求められる要件が定まった。

次に必要となるのは、各役割（担当）を担う人が役割を遂行できる能力を持つかどうかを評価することである。その為には、各役割（担当）を遂行するために必要な能力を定義しなければならない。そこで、検討会では、人材の能力の基準として、「氷山モデル」を念頭に置き、人材のスキルを単に技術的なスキル（プロフェッショナルスキル）ではなく、適応力・態度、（技術以外の）知識、業務経験等を加味し、最も重要な要素として倫理観・信条を加えたものとした。（表 7）

表 7 スキルセット項目（氷山モデル）

基準項目	要素	参照先等
適応力・態度	チームワークや作業遂行に必要	i コンピテンシ ディクショナリ[17]（IT ヒューマンスキル）を参照
プロフェッショナルスキル	対策実務に必要	i コンピテンシ ディクショナリ（大分類及び中分類）を参照
知識	対策の企画や対応、未知の領域での作業遂行に必要	NIST サイバーセキュリティフレームワークを基準とし、国内のビジネスに必要な知識を記載
経験	習熟度に関連し、結果から作業を紐解くために必要	
倫理観・信条	信頼性を担保し、善悪の判断を促す	コンプライアンス等

現在、適応力・態度、プロフェッショナルスキルの 2 項目については、IPA[18]の協力の下、さらにブラッシュアップを行っていく予定である。

3.2.2. 産学連携推進活動

本検討会では、サイバーセキュリティ人材育成に関する有効な産官学連携の施策の一つとして、まずは産業界と教育機関の連携を進める必要があることを共有していた。事務局 3 社及びいくつかの検討会メンバ企業では、既にサイバーセキュリティに関する寄付講座（産学連携講座）の開講や人材育成の支援を実施しており、そこで得られた知見や育成された人材の採用等、様々な検討課題が提起されている。

図 8 は、産学連携において、企業の集まりである「産」と、教育の場を提供・運営する「学」との間の相互連携のイメージを示す。サイバーセキュリティに対する取り組みに直面している企業、あるいは、そのための人材の育成を喫緊の重要課題と認識している企業であるからこそ可能となる先端的実践ノウハウの提供やリソース支援（「産」）、それら

[17] i コンピテンシ ディクショナリ https://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/

[18]独立行政法人情報処理推進機構(IPA) https://www.ipa.go.jp/index.html

を受けてこそ実現できる産業界を指向した人材育成の実施（「学」）、この双方向の関係が成立し全国に広く展開されるための仕組み作りが重要となる。

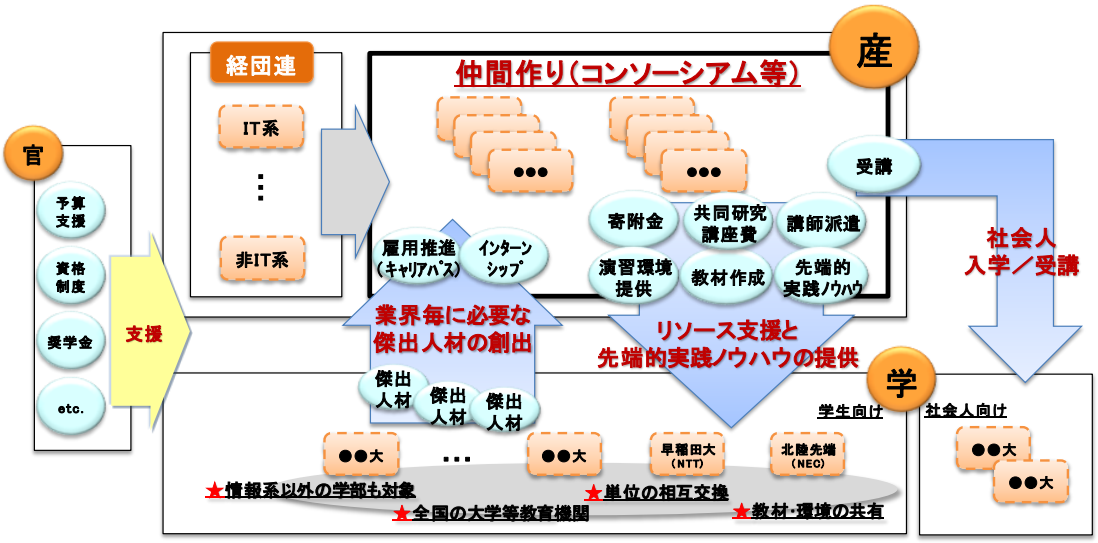

図 8 産学連携のイメージ

検討会では、「次世代に向けた人材育成の推進」の具体的な推進活動として、有志企業メンバ８社により、教育機関（大学、高専）との産学連携方法の具体化に向けて以下のような議論を行った。

① 現状の仕組みの下での各大学、および高専等との契約方法と関連する課題の抽出
② 実質的な連携方法（連携講座設置、講師派遣、教育資料提供等）の検討
③ 将来に向けての産学連携のスキームの検討

これらの議論の中で、企業が求める人材のあり方を踏まえた教育機関としての人材育成の必要性とその方策、及び学校を卒業し ICT 業界への就職を経て経験を積んだ上で、ユーザ企業におけるサイバーセキュリティ担当を担うようなキャリアパスの制定も、一つの方向性として検討課題となっている。また、キャリアパスを考えていくためには、人材定義と人材育成を更に深耕し、採用基準、育成プランの標準化、評価基準等の整備が求められると考える。

2016 年 1 月の本検討会中間報告以降、大学関係者からの確認相談も増えてきたため、事務局として適宜情報共有を進めていくこととなった。また、全国各地域に対して、広くセキュリティ教育を受講可能とするために、各地方における中心となる大学をハブとしてその地域をカバーするような方法を検討した。いくつかのハブ候補の大学に打診し、良い反応を得ている。

本検討会では、各社の負担軽減とより広く教育機関との連携を実現するために、各社が供出した資金を予めプールし、それをベースに複数の大学と契約を行う方式の実現を想定しているが、初年度においては体制の整備等の準備が整わなかったこと等から、1 社 1 校の形態で連携協定を締結した。第二期以降では、産業界と教育機関の関係強化を踏まえ、前述の形態の実現を目指していく（図 9)。

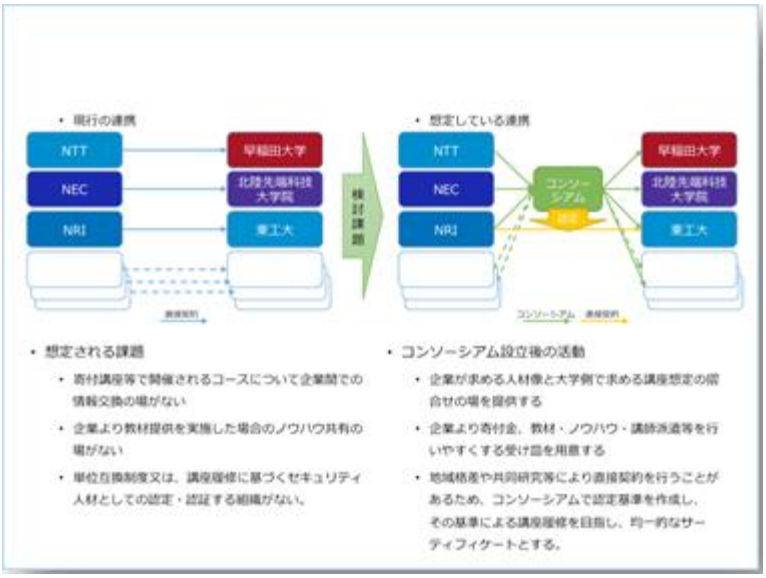

図 9　大学連携の形態

なお、第一期における教育機関との連携活動での協定締結状況を、表 8 に示す。

表 8 教育機関との連携活動での協定状況

連携教育機関	連携企業
早稲田大学	日本電信電話株式会社
北陸先端科学技術大学院大学	日本電気株式会社
東京工業大学	野村総合研究所[19]
九州大学	富士通株式会社[20]

今後は先行している産学連携（寄附講座）活動の水平展開を複数の大学にして実施していくと共に、コンソーシアム的な活動に昇華させ、産学連携の輪を拡大していきたい。

また、今後第二期で行う予定の、プロダクション領域での人材定義モデルの策定結果をベースに、新たにマネジメント系や safety の概念を取り入れた制御システム系における人材育成を、教育機関との連携推進活動に取り入れていく。

[19] https://www.nri.com/jp/news/2016/160510_1.aspx

[20] http://pr.fujitsu.com/jp/news/2016/06/1.html

3.2.3. 人材育成・維持のためのエコシステム

サイバーセキュリティ人材の育成という喫緊の社会的課題に対し、本検討会では前述の通り、産業界として求められる人材の定義とその定義に基づく理想的な状況（それぞれの企業が必要最小限の人材を確保できている状況）へ向かうために必要となる育成・教育の手段や施策の在り方について検討し、実際にその実現・実行を産業界としての立場から推進するものと考えている。

その際、サイバーセキュリティ人材を育成するだけではなく、育成された人材が産業界におけるそれぞれの企業に適切に受け入れられ、さらに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。より正確に言えば、サイバー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」の領域に人材が雇用されそこで活躍することもそれぞれの観点から極めて重要といえる。

人材育成のみならず、それに関係する周辺の様々な機能や役割を産学官がそれぞれ相応の責任を担って実現し、円滑な運用の下に全体が有機的に繋がって効果的に働くような人材育成・以上のための仕組みをここでは「エコシステム」と呼ぶこととする。

本検討会で想定している「エコシステム」全体像（イメージ）を図 10 に示す。以下、同図を参照しながら「エコシステム」の構成について説明する。なお、同図中に記す個々の要素、事項については、あくまでも暫定的なものであり、今後、「官」や「学」と連携しながらの検討や議論を通して精査していきたいと考えている。

＜全体構成（産学官それぞれの位置付け）＞

- 産学官がそれぞれの役割を担いながら連携してこそ成り立つエコシステムである。
- 「産」は、主に人材を雇用・維持する主体であるが、必ずしもセキュリティや ICT に通じた業界だけでなく、今後のサイバーセキュリティ人材の必要性が極めて高くなるであろうユーザ企業の位置付けが重要となる。
- 「学」は、主に人材を教育する主体であるが、大学や大学院のみならず、リテラシ面を含む基礎的な知識や経験の重要性を鑑みて、より若い世代が学ぶ高校や高専の位置付けも重要となる。
- 「官」は、エコシステム自体の開発を牽引・推進し、エコシステムにおける「産」や「学」を制度運用等により下支えする位置付けとなる。

＜「産」の役割＞

サイバーセキュリティに関する知識や技術をある程度保有している ICT 分野の企業、あるいは、セキュリティに関するサービスやソリューションをビジネスとして提供しているセキュリティ企業は、ICT を直接的なビジネスの対象とすることのみなら

ず、サイバーセキュリティに関する対応力が不足するユーザ企業を支援すべき関係性を構築していく必要がある。

具体的には、ユーザ企業が自社のサイバーセキュリティ対応の一部をセキュリティ企業にアウトソースすることや、ユーザ企業だけでなく ICT/セキュリティ企業にとってもメリットのある異業種間の人事交流（ユーザ企業の人材を ICT/セキュリティ企業が OJT として受け入れる形態等）実現が考えられる。

このほか、図中には、「産」として責任を持って行うべき、あるいは、牽引すべき事項として、「必要な人材の定義（本検討会による最優先事項)」、「キャリアパス設計」、「雇用の推進」、「処遇の見直し」、「産産連携強化」、「経営層のリーダシップ」を示したが、過不足を含め詳細は今後、「官」や「学」の識者方も交えての検討・議論としたい。

＜「学」の役割＞

これまで、サイバーセキュリティ人材の育成の場としては、主に大学や大学院において、現役の学生、および一部社会人を対象としたセキュリティ知識・経験の向上のための教育や産官学連携による施策が試みられてきた。

それに対して、今後はより若年層を対象に、セキュリティに関する基礎知識やリテラシ・倫理から学ぶ場、あるいは、人材発掘の場として、高校や高専（高等専門学校）の位置付けも重要となってくる。

このほか、図中には、「学」として責任を持って行うべき、あるいは、牽引すべき事項として、「(健全で充実した）育成環境の提供」、「臨まれる人材育成のカリキュラム作成」、「(情報系の以外の）人材発掘」、「大学間連携」を示したが、過不足を含め詳細は、「産」の役割同様に、今後、産学官それぞれの識者方を交えての検討・議論としたい。

＜「官」の役割＞

産業界が求めるサイバーセキュリティ人材（実際には、「学」や「官」が求める人材も含む）を育成・維持するためのエコシステムに必要で、「産」や「学」が主体となって実現することが難しい機能や仕組みが幾つかある。

具体的には、図中にも示したが、人材定義に基づき人材の質やレベルを客観的に評価するための尺度となる「共通のモノサシ（人材の見える化)」、それによって評価されたことの証を作る「資格制度」、育成の場から排出された人材がスムーズに企業等に雇用されるための一施策としての「セキュリティ人材配置の義務化」、育成する側の人材不足への対策（「講師不足対策」)、必ずしも育成できるものではないと言われているトップガン人材（トップガンという言葉の定義は曖昧であり本来は使うべきではないが）の確保（「トップガン確保」)、これら全ての実現に必要となる予算の確

保（「予算支援」）等が考えられ、やはり、今後、産学官それぞれの識者方を交えての検討・議論としたい。

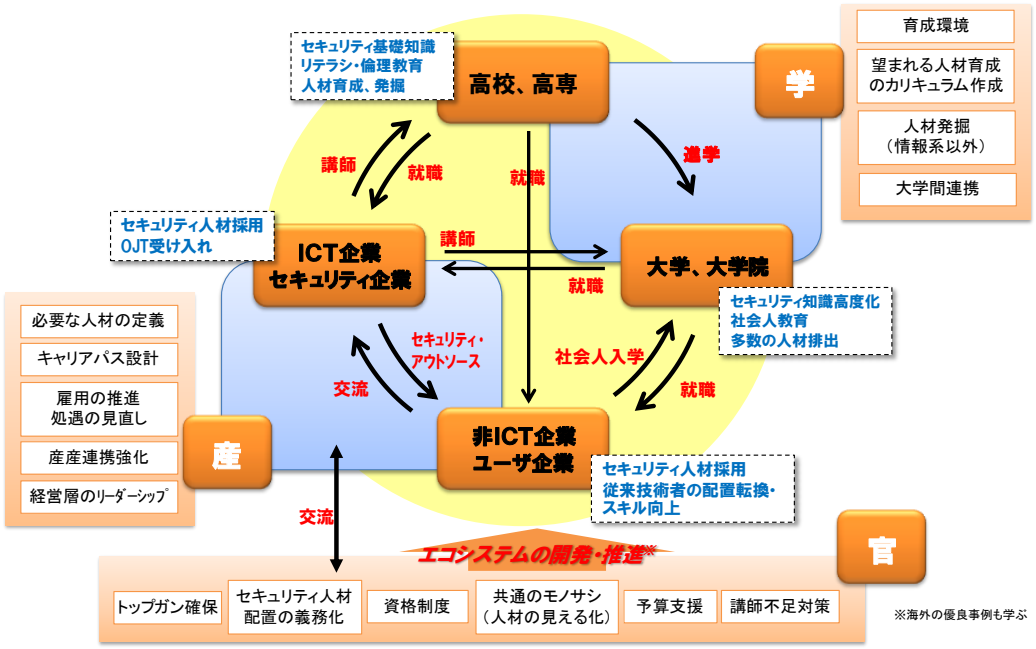

図 10 人材育成・維持のためのエコシステム

3.3. CISO についての考察

サイバーセキュリティ経営ガイドラインにおいても、

「･･･経営者とセキュリティ担当者、両者をつなぐ仲介者としての CISO 等からなる適切な管理体制を構築すること。 その中で、責任を明確化すること。」

と指示されていることもあり、CISO を設置するところは増えている。

本検討会､特に人材定義 WG で CISO について､海外企業と日本企業の CISO の相違点、日本企業における CISO の役割、CISO は役員であるべきか、CISO と CIO/CSO/CRO 等との関係／位置づけ等の話題で議論が行われた。検討会の成果というわけではないが、議論のいくつかの観点を以下に述べる。

- 日本企業での CISO と組織体制

日本企業の場合､CISO となった役員がサイバーセキュリティに関する専門的な知識や見識を持っていて、インシデント対応等の経験も豊富な人である場合は、現時点ではかなり少ないものと想定される。また、日本の場合には、数年で役員が交代し、CISO も交代することが多い。一方、海外企業（特に米国）の場合は、CISO はその道のプロフェッショナルとして、複数の企業を渡り歩いて来た人物の場合が多い。CISO がその企業のサイバーセキュリティ体制を文字通りリードしていく。

そのような日本の状況下においての CISO の役割は、米国のそれとは当然違っており、それを前提にサイバーセキュリティ対応体制の構築を行っている組織が少なくないものと想定される。

- CISO は役員であるべきか

サイバーセキュリティ経営ガイドラインにも、「CISO(最高情報セキュリティ責任者:企業内で情報セキュリティを統括する担当役員)」という記述があるため、CISO という名称のイメージでは、少なくとも執行役員以上である必要があると考えがちである。

実際は、その企業の情報セキュリティ対策を実施する上での責任者であればよいので役員である必要はない。検討会メンバの非常に大きな企業の CISO でも役員ではない例もあるようで、CISO がその任務を果たすことが出来る権限が経営トップから委譲されていればよいということである。

企業により考え方は異なるので、CISO をどのような人が務めるのかは一概には言えないが、検討会では、“サイバーセキュリティ対策統括”機能に責任を負う役割として「CISO / CRO / CIO 等」を位置づけている。

- CISO と CIO との関係

CIO と CISO の関係ならびに上下関係についても企業ごと様々であったが、印象的な事例として、ある製造業メーカでの CISO の位置づけを紹介する。

その企業では、CIO は情報システム部門にて企業の ICT システムについて権限を持っており、その部門のセキュリティにおいては、特に CISO を設置する必要はなかった。しかし、近年製造部門においても、IoT 等 ICT をフル活用した製造ラインを計画しており、その場合のセキュリティを考える必要性が生じてきた。

従って、今後、従来の情報システム部門の掌握範囲以外での ICT 利活用がますます広がることを想定し、企業全体のセキュリティを統括する位置に CISO の設置を検討しているとのことであった。今後同様な事例が増えてくるものと想定される。

3.4. サイバーセキュリティ対応体制の様々な形

検討会での情報共有により、様々な企業のサイバーセキュリティ対応体制は個々に異なるものであることが判ってきた。体制構築はその会社の業態、組織構成、また、企業文化によって、それぞれの企業の特有事情を加味して行われる。例えば、以下のような事例である。

(企業 A の場合)

・グループ全体のセキュリティ方針検討やグループの全体最適に向けた施策等を実行するため、持株会社内に戦略委員会として、「グループ CISO 委員会」を設置。

・持株会社の CISO が委員長を務め、主要各社の CISO にて構成。

・主な検討事項としては、
「グループにおける情報セキュリティマネジメント戦略の策定」等。
・本委員会主導により、グループ全体・分野横断の情報セキュリティマネジメント実現を図っている。

（企業 B の場合）
・委員会は、トータルリスク・内部統制委員会配下に IT 統制部会（含む情報セキュリティ委員会）を設置。
・執行自体は、CISO（経営企画担当　常務執行役員・取締役）と　経営企画部内に情報セキュリティ推進室を設置
・情報セキュリティ推進室配下に、SOC を配置　SOC は、外部委託と内部（実質は IT 子会社）にて実施
・インシデント発生時は、CSIRT として代表取締役を委員長とする「特別危機管理委員会」を準備

企業 A は ICT 企業のため、サイバーセキュリティ対策関連活動は自ビジネスに関わりが深く、また技術人材も多いことから、それ自身を独立した形での位置付けを採用したものと想定される。また、ホールディング体制で、グループ会社全体を統率するための委員会を設置する体制をとっており、セキュリティ対策のために、戦略委員会として「グループ CISO 委員会」を新たに位置付けている。

また、企業 B では、既存の内部統制の枠組み配下にサイバーセキュリティ対応体制をおくことで、経営幹部への報告等が行える体制を整えており、さらに、インシデント発生時には、代表取締役を長とする特別体制を設置することで迅速な対応を可能としている。

それぞれの組織により、サイバーセキュリティ対応体制は異なるものの、特に以下の点に留意した検討が為されていた。

(1) 会社組織運営のなかでの位置づけ

「サイバーセキュリティは経営課題である」という認識は、検討会に参加している企業ではかなり浸透しており、その一端として、検討会参加メンバには、CEO あるいは経営層から、自社のサイバーセキュリティ対応を検討する責務を負っているメンバが多い。当該メンバは、経営層に無理なく報告等が行えるように、会社組織の活動にあったポジションを得ていることが重要となっていた。

いざという時の迅速な対応を実現するためにも、会社の活動として組織内にしっかり組み込まれた体制を確保・維持することが重要な点である。

(2) 組織体制

先の事例に見るように、組織上のトップにセキュリティ管理組織を置く事例もあれば、既存の内部統制等のマネジメントをベースに枠組みを踏襲する事例もある。要は、他組織の例を参考とするも、自社で最も運用しやすく、かつ効果を発揮する体制を構築すべきである。当該組織の有効性評価は、監査等の定期審査により実施され、適宜見直しを図るものとする。

(3) インシデント発生時における対応

CISO の位置づけや各セキュリティ関連部署の構成は、各社の業態や組織構成によって異なるものである。それに応じ、インシデント発生時にその対応の中核を担う SOC/CSIRT の位置付けも異なるが、不変的に最も重要なことは、SOC 等の技術部門が行ったインシデント解析結果を、如何に迅速かつ的確に経営判断に供するかである。

日本企業においては、CIO や CISO が必ずしもセキュリティの専門性を有していないケースが多いことは前述した。従って、セキュリティの技術的特性を自社の業務に置き換えてリスクを明確化する組織が、換言すれば、経営判断のための「翻訳機能」を担う組織（本書では「サイバーセキュリティ統括機能」と呼称）と人物（いわゆる「橋渡し人材」）の存在が重要といえる。

3.5. サイバーセキュリティ専門部署の必要性

今回、人材定義を考える際には、総務部からの機能分化モデルを作成し、必要とされる機能・役割を見出した。しかしながら、それらの検討／議論を実施するうちに、外部からの脅威や攻撃者を想定しなければならないサイバーセキュリティでは、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ってきた。それを裏付けるように、検討会の各社体制の発表でも、サイバーセキュリティ対応部門を新しく設けている事例が多く見受けられた。

今後、企業・官公庁ともに守るべき秘密、知財を保有する組織では、それらの情報やそれを扱うための ICT システム等の資産を防衛するために、その役割を担当する専門部署の保有／設置が必須となるものと想定される。それは、ある程度の規模を持った組織に、総務部、人事部、経理部等の部署があるのと同じように、どの組織においても必ず設置されることが求められる。

3.6. セキュリティ人材の必要人数の試算

本検討会では、NISC が平成 28 年 3 月 31 日に発表した「サイバーセキュリティ人材育成総合強化方針」を踏まえ、人材定義 WG により定義されているサイバーセキュリティ人材が、国内全体ではどれくらいの必要人数となるかの試算に取り組むこととなった。

3.6.1. 「サイバーセキュリティ人材育成総合強化方針」との関係

「サイバーセキュリティ人材育成総合強化方針」には、「はじめに」において、以下の通り示されている。

はじめに

平成 27 年９月、「サイバーセキュリティ戦略」（以下「戦略」という。）を閣議決定した。戦略は、「自由、公正かつ安全なサイバー空間」を創出するため、３つの政策分野（「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」）と１つの分野横断的施策（研究開発や人材育成を含む基礎体力の強化）で構成されており、各施策を着実に推進していく必要がある。

（中略）

本方針は、第１章において、社会で活躍できる人材の育成に向け、サイバーセキュリティを専門とする人材のみならず、ユーザ企業等も含めた幅広い立場でのサイバーセキュリティに係る人材育成に向けた各種施策を加速させていくための方針を示す。次に、第２章では、政府機関における専門人材育成、一般職員のリテラシ向上等についての取組方針を示す。そして、第３章において、今後の検討の枠組みを示す。

第３章にある『３．産学官が連携した人材育成の循環システムの構築』において、『（１）求められる人材像の明示』では、『*産業界においても業種・業界毎に求められる必要規模も含めた人材像の明確化等 を目標として検討する動きがあり、*』として、本検討会の活動及びグループ活動における一考察についても記述されている。

3.6.2. サイバーセキュリティ人材不足に関する発表等

これまで各省庁からサイバーセキュリティ人材不足に関する調査研究や発表、更にそれを受けたマスコミ報道がなされている。

ＩＴ人材新たに 100 万人　総務省、専門資格創設へ

総務省が 20 日の情報通信審議会に示す報告書に、ＩＴに関する専門的な技術者を現在の約 103 万人から 25 年に約 202 万人に倍増させる目標を盛り込む。

平成 28 年 6 月 18 日　日本経済新聞　電子版

IT 人材の最新動向と将来推計に関する調査報告書

情報セキュリティ人材は、現在約 28 万人、不足数は約 13 万人であるが、2020 年には不足数が 20 万人弱に拡大。

平成 28 年 6 月 10 日　経済産業省　商務情報政策局情報処理振興課

サイバー防衛人材、５万人育成　五輪に向け総務省

総務省は 2020 年の東京五輪に向け、サイバー攻撃を防ぐための総合対策をまとめた。大規模なサイバー攻撃演習の実施などを通じ、政府や自治体、企業などで５万人のサイバー人材を育成する。

平成 27 年 7 月 16 日　日本経済新聞　電子版

「情報セキュリティ人材の育成に関する基礎調査」報告書

国内の従業員 100 人以上の企業において情報セキュリティに従事する技術者は約 23 万人、不足人材数は約 2.2 万人と推計されました

平成 26 年 7 月 30 日（最終更新）　独立行政法人情報処理推進機構

3.6.3.　セキュリティ人材の必要人数を考えるにあたり

人材定義 WG では、セキュリティ人材の育成に向けて、まずは日本の産業界が求める人材の定義に向けた議論を進めてきた。その中では、ユーザ企業においては、専任者・兼任者・常駐者・派遣スタッフ・委託従業者等の様々な勤務形態があり、更にサイバーセキュリティ機能に対する担当範囲が広範囲に存在しているため、セキュリティ人材を「人数」で明確化することは難しいと考えてきた。

ユーザ企業が抱える課題として、セキュリティ対策そのものの有効性や実効性がテーマに上がるだけではなく、日々対策が進むことによって、高度な専門性を持つ人材を社員として雇用しておくほどの機微なインシデントが発生しにくくなり、採用人数や育成人数を単純な計算で求めることが困難な状況にあることが共有された。

そこで、人材定義 WG における人材の定義の種類と、その業務内容に基づく 1 社あたりの必要人数をモデル化し、日本国内の企業数や事業所数を「経済センサス」から導き出し、それらを掛け合わせることによって、不足人数ではなく、現在の日本に必要と想定され得る人数を試算することにした。

このような考えに至ったのは、特定のセキュリティ業務に関し、複数の事業所を跨って一人で担うようなケースや、一つの事業所（または一企業）の中でも、複数のセキュリティ業務を掛け持つケースがあり、これらのケースにおいて一事業所あたり、あるいは、一業務あたりの必要人材の人数を表現しようとすると１人以下（例えば、0.5 人）となるためである。更には、ICT 業種・職種では「人月計算」により業務が行われており、プロジェクト型の業務の場合、半常駐等の勤務であっても、企業内における１人のセキュリティ人材としてカウントされるケースが考えられた。

この試算においては、情報システム部門における人材配置が中央集権的な考え方に基づいている点と、制御システムや製品・サービスに ICT を活用する場合の人員配置が分散型で機動的（流動的）になっている点を踏まえて検討することとした。特に、製造現場や製品

に対するセキュリティ人材は、専任者ではなく、製造や保守業務と紐づく兼任者が多くなる傾向が考えられた。

以上の点を踏まえると、セキュリティ人材の定義のみならず、必要人数の試算についても慎重な姿勢が求められると考え、本検討会における今回の必要人数試算は、あくまでも政府・各省等が表明している数値や規模感との整合性を検証する目的での一考（参考指標）と位置付ける。

3.6.4. セキュリティ人材の必要人材の試算

セキュリティ人材の必要人数を試算するにあたり、試算の前提となる法令等の要求事項および主に情報システム部門になる担当部署を想定し、組織構成と人材配置を念頭に、妥当な必要人数を割り当てることとし、その枠組みの中からセキュリティ人材を絞り込む方法を採用した。なお、制御システムや製品・サービスのセキュリティを担当する人材は情報システム部門以外に配置されていることが想定されるため、経済センサスでいう「事業所」に該当する場所での勤務を想定している。

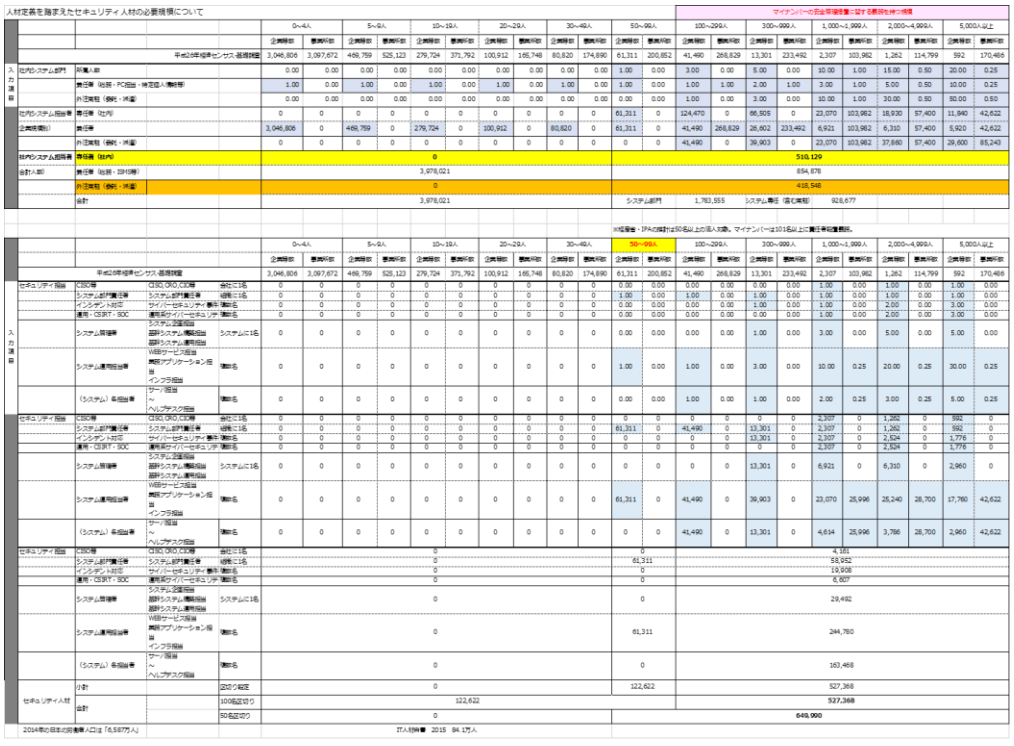

図 11 人材定義を踏まえたセキュリティ人材の必要規模(全体像)

図 12 人材定義を踏まえたセキュリティ人材の必要規模(情報システム分野)

ここでは、横軸に経済センサスに基づく企業数と事業所数、縦軸には、情報システムを司る担当者（専任者・兼任者・外注者）でマトリクスを作成し、どれくらいの企業規模に何名程度が配属されるのが理想なのかについて考察し、総規模を試算した。ただし、製造業、運輸業、WEB サービス業等における情報システム部門や現業部門における IT 人材及びセキュリティ人材の配置には業界ごとの違いがあると想定されるため、あくまでも参考値として試算した。

なお、今回の試算においては、一般社団法人サイバーリスク情報センター（CRIC）の保有する知見も活用し検証を進めた。

注意すべき点として、平成 28 年より稼働している「マイナンバー制度」により、法令対応としての「特定個人情報取扱責任者」及び「担当者」が必要となっていることが挙げられる。これらの役割に対しては「安全管理措置」が求められることから、少なくとも 101 名以上の規模を持つ企業には、技術的安全管理措置を理解できる人材が 1 名は存在することを前提としている。

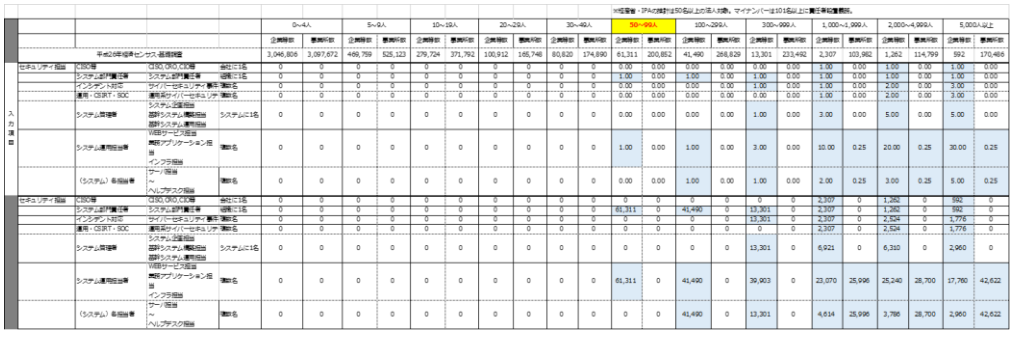

図 13 人材定義を踏まえたセキュリティ人材の必要規模(専門人材)

次に、セキュリティ人材の配置人数に関する試算を行った。ここでは、横軸は同様に経済センサスに基づく企業数と事業所数としたが、縦軸には、人材定義 WG で検討してきたセキュリティ人材の 30 役割から、近い業務を統合した 7 分類を活用した。この考察においては、情報システム部門を中心とした中央集権型の組織構成に該当する人材と、現業部

門におけるセキュリティ人材を踏まえて、企業数に該当する部分に中央集権型、事業所数に該当する部分に現業部門に在籍されている人材とに、セキュリティ人材を配置することを試みた。

ただし、事業所数は拠点数であり、大手製造業のように工場を 1 拠点としている場合、また小売卸業のように数名～10 数名の営業拠点を事業所としているところもあり、一概に 1 事業所に何名のセキュリティ人材が配置されているかは確認が難しいと考えられた。今後、より詳細な数値を試算していく場合には、経済センサスの地域別・人数別の事業所に関するデータを活用したいが、今後の課題としてとどめておく。

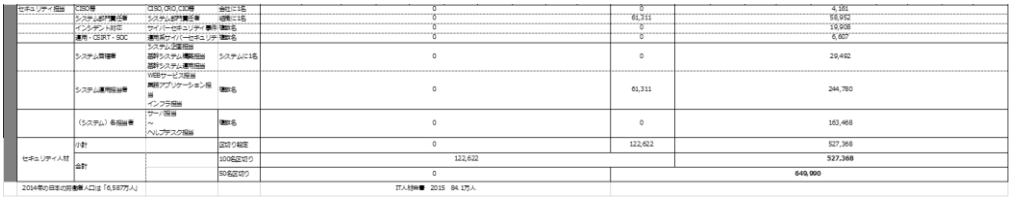

図 14 人材定義を踏まえたセキュリティ人材の必要規模(想定人数)

上記プロセスに基づき、人材定義 WG にて作成した人材定義リファレンスに基づく試算を行ったが、役割が細分化され過ぎることを避けるため、まずはセキュリティを担当する役割の 7 分類を提示し、それぞれの分類において求められるであろう人数を試算した。
この試算においては、事業所（支社・支店・工場等）におけるセキュリティ人材の配置は、業種・業態や企業規模で大きく左右されるため、あくまでも参考値としての試算（一考）としている。

3.6.5. 「情報処理安全確保支援士」との関係性

本試算を通じて得られた数値において、セキュリティ人材の 7 分類を踏まえて来年 4 月より施行される「情報処理安全確保支援士」の候補ゾーンの検証も実施した。「情報処理安全確保支援士」は、最新のセキュリティに関する知識・技能を備えた高度かつ実践的な人材に関する国家資格として 2016 年度後半から運用が開始される新制度で、2020 年までに 30,000 人の有資格者確保を目標としている。

本試算における 7 分類の中では、経済産業省発表の資格制度の説明資料に基づき、インシデント対応、運用・CSIRT・SOC に分類されている役割群が該当すると想定され、試算人数は約 27,000 名となっている。更に業務上必要になる可能性がある範囲を広げていくと、システム部門責任者とシステム管理者との合計 90,000 人超が、次の候補になると考えられる。

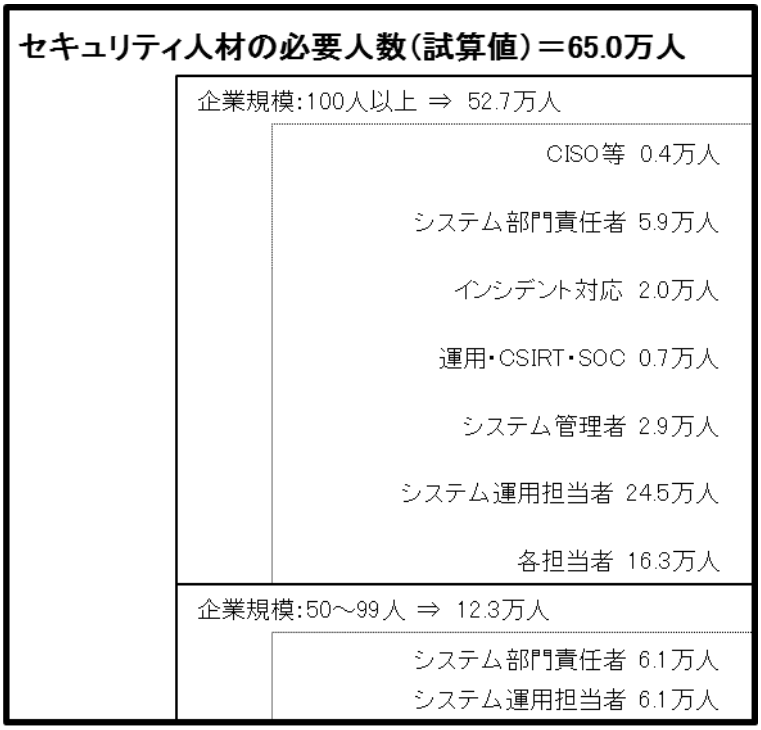

図 15 セキュリティ人材定義に基づく必要人数の試算数(2016 年)

4. 活動過程

4.1. 目標

本検討会で取り組むべき目標は、①社内人材育成の推進、②次世代に向けた人材育成、③情報共有の推進の３つとした。

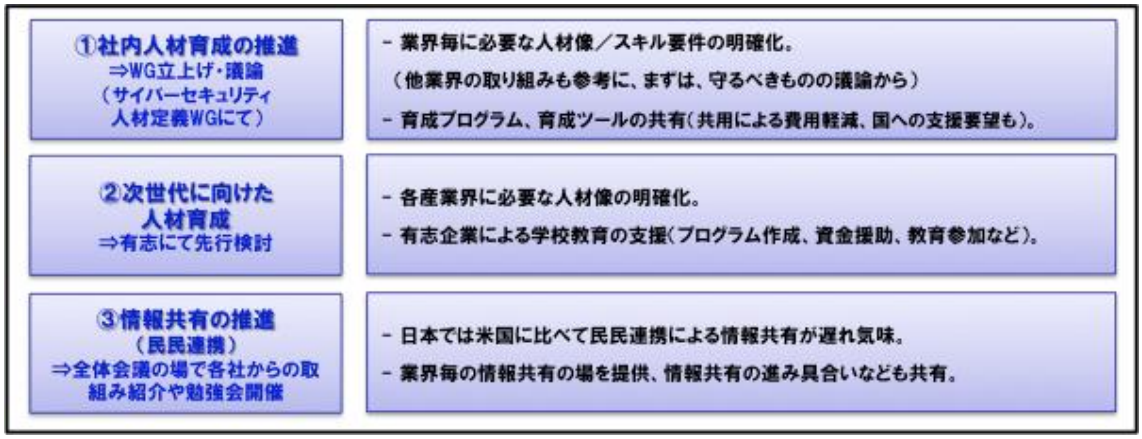

図 16 産業横断サイバーセキュリティ人材育成検討会の目標

4.2. 会議体

本検討会では、配下に３つのグループを作成し、「情報共有」、「人材育成」、「産学連携」を推進した。

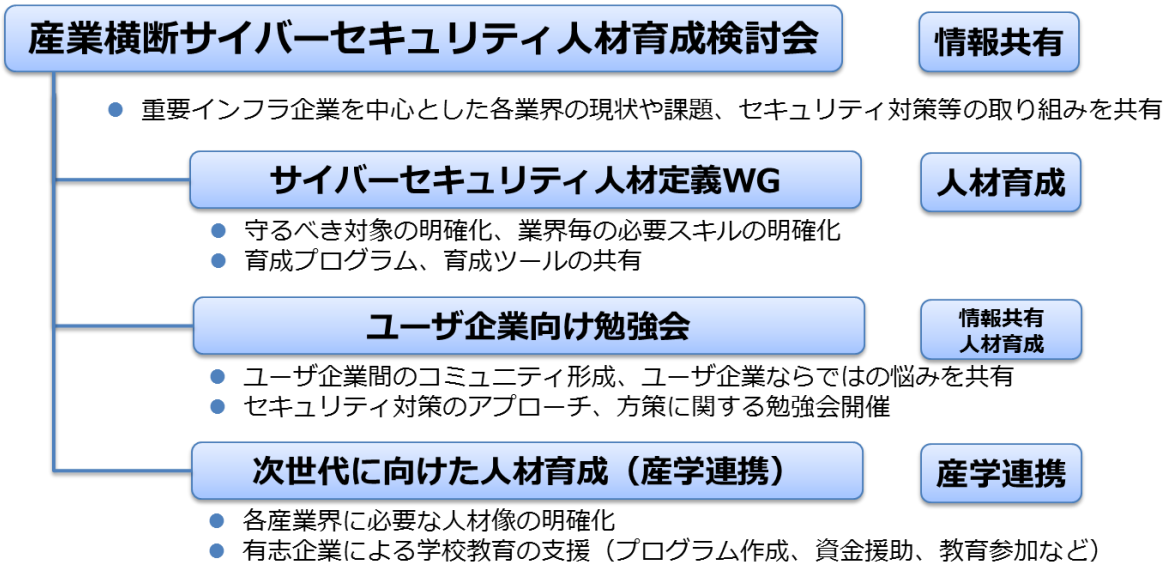

図 17 産業横断サイバーセキュリティ人材育成検討会の会議体

4.3. スケジュール

スケジュールは、2016 年 6 月までを第一期（Stage1）とした。また、第一期を前半と後半に分けた。前半では、想定された課題に関して参加者からの意見を広く集め、解くべき課題を出来るだけ具体的に定義した。後半では、前半の課題を踏まえ、人材を定義した。

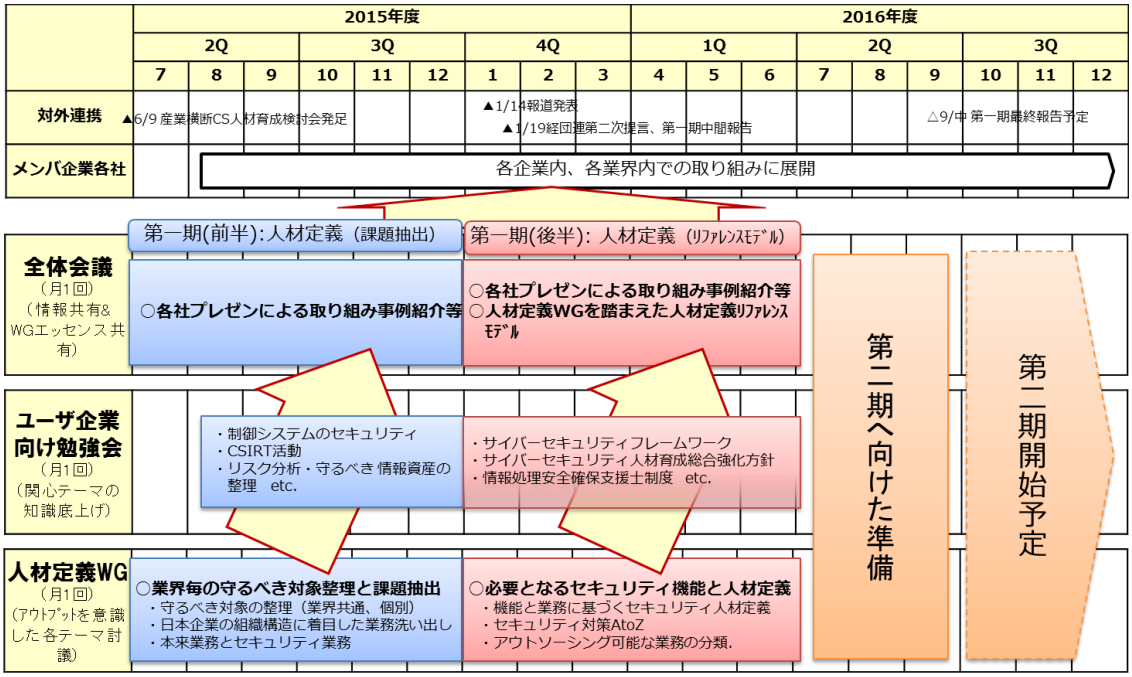

図 18 本検討会の活動スケジュール

それぞれの 3 つの会議体の開催状況は以下の通りである。

表 9 会議体の開催状況

日付	サイバーセキュリティ人材育成検討会（全体会議）	サイバー人材定義 WG	ユーザ企業向け勉強会	
				勉強会テーマ
6 月 9 日（火）	○			
6 月 25 日（木）		○		
7 月 7 日（火）	○	○		
7 月 29 日（水）		○		
8 月 4 日（火）	○			
8 月 26 日（水）		○		
9 月 14 日（月）	○			
9 月 29 日（火）		○		
10 月 9 日（金）	○		○	大学における人材育成の取り組み紹介
10 月 20 日（火）		○	○	制御システムに関するセキュリティ動向
11 月 12 日（木）	○	○	○	CSIRT 最前線
11 月 25 日（水）		○	○	CSIRT 時代の SOC との付き合い方」/「150 分でわかるセキュリティ対応できる組織にする 10 のコツ
12 月 8 日（火）	○		○	オリンピック関連
12 月 21 日（月）		○	○	情報共有関連
1 月 19 日（火）	○			-
1 月 21 日（木）		○		-
2 月 10 日（水）	○		○	Information Sharing in the US - Communication Sector -
2 月 15 日（月）		○	○	サイバーセキュリティ経営ガイドライン
3 月 4 日（金）		○	○	最近のサイバー攻撃の動向
3 月 22 日（火）	○		○	制御システムのセキュリティに関する最新の話題
3 月 25 日（金）		○		-
4 月 13 日（水）	○	○		-

5月10日（火）		○	○	NISTのサイバーセキュリティフレームワーク（日本語版）　解説
5月16日（月）	○		○	NISTのサイバーセキュリティフレームワーク（英語版）　講演
6月2日（木）		○	○	J-CSIPの最近の活動状況やインシデントの動向
6月8日（水）	○		○	情報処理安全確保支援士制度等の解説
6月20日（月）	○			-
7月7日（木）		○	○	CSIRTの動向について
7月11日（月）	○			

4.4. 全体会議

検討会の方向性を話し合うと共に、情報共有活動として各社のセキュリティ対策事例を順次発表してする場として全組織が参加する。具体的には、以下の活動を実施。

・検討会の方向性検討や各グループ等の承認

検討会の目標、方針、取組内容、運営形態等を検討・議論する。アンケート等も適宜活用し、参加各社の声を収集・反映した地に足のついた活動となるよう努めている。また、サイバーセキュリティ人材定義 WG 等の各グループの内容を全体会議で報告・承認し、参加各社が足並みを揃えている。

・産業横断における議論や情報共有の場の提供

各社が取り組みを紹介することで、自社の取り組み等への気づきが発生する点、プレゼン会社自体も良い相談ができる点となっており、検討会自体が産業横断での情報共有の場となっている。業界ごとでの情報共有の場は、各 ISAC 等あるが、産業界主導による産業横断での情報共有の場は他にないと思われる。今後、本検討会の参加各社が、各業界のリーダ役となり、各業界内の情報共有の活性化に昇華できることができれば幸いである。

4.5. ユーザ企業向け勉強会

サイバーセキュリティ情報共有活動の 1 つとして、ユーザ企業向けにサイバーセキュリティ関わる話題を取り上げ、外部講演者による勉強会形式で開催。本勉強会は、ユーザ企業のみで構成しており、ユーザ企業が抱える課題等を“この場限り”で、意見交換する場として活用している。また、意見交換するテーマとして、「人材育成」、「情報共有」、「産学連携」に関連する幅広いものを取り上げ、各種最新動向やフレームワーク等の基本知識を習得し、本検討会の活発な議論へも生かすようにしている。

また、次世代に向けた人材育成として、有志による産学連携の検討も先行的に着手しており、各社ごとの連携講座の設置等、成果も出つつある。今後は、コンソーシアム的な活動に昇華させ、産学連携の輪を拡大していきたい。

4.6. 人材定義 WG

人材定義 WG では、本検討会の方針に沿い、サイバーセキュリティ人材とはどのような人材を指すのかを定義し、育成の方向性や、産官学との連携の在り方について検証していくことを目的として活動を行ってきた。

ユーザ企業におけるサイバーセキュリティ人材とは、日々高度化していく ICT 環境及びサイバーインシデント事案と日々対峙していくことだけではなく、事業運営を支える社員及び外注スタッフとしての日々の業務、情報システム部門の構成メンバとしての役割や、情報システム部門に属していなくてもサイバーインシデント事案発生時には、事態の収束に立ち上がる関係部門・部署の構成メンバとしての役割も必要となることから、ICT 環境や情報セキュリティといった今までの考え方を一度外して、企業における組織と業務の在り方から、その存在意義を再確認することとした。

特に、サイバーセキュリティ人材の育成を考える時、日々日本国内で流通しているサイバーセキュリティ対策に関する情報が、ICT 業界の製品サービスに関する情報と直接的に紐づいているものが多く、ユーザ企業における ICT 利用環境や ICT の構成の全体像を見えにくくしている課題を踏まえて、日本企業の独自性として考えられる社内システムの構築運用における外注比率の高さや、定期人事異動によるゼネラリストの育成方針等を踏まえた、有意義なサイバーセキュリティ人材の定義及び育成が求められるものと合意した。

人材定義の活動骨子としては、以下に集約される。

① サイバーセキュリティ対策には、4 つのフィールド（情報システム、生産・制御システム、IoT、CSIRT）があり、第一期としては、情報システムにおけるサイバーセキュリティ人材を定義する。
② 日本におけるユーザ企業では、情報システムに関する外注比率が高いため、企業内におけるサイバーセキュリティ人材と、外注先に要求するサイバーセキュリティ人材については分けて検討を行う。
③ 「サイバーセキュリティ経営ガイドライン」が、本検討会の活動途中に発表され、CISO 等という役割の重要性が問われるようになったため、ユーザ企業にとって必要とされる CISO の機能を討議する。

④ NISC の発表資料では、橋渡し人材という言葉が定義され、ユーザ企業内にこの橋渡し人材を配置することについて検証し、必要となる人材要件を検討する。
⑤ 日本企業の事業運営の特徴である「定期人事異動」に対応し、サイバーセキュリティ対策を俯瞰できる成果物を作成し、人事異動や組織の新設に伴う活動の立ち上がりの停滞を回避し、効率的な対策を側面から支援する。
⑥ サイバーセキュリティ人材の高度化を検討していく中で、ユーザ企業内で実施しなければならない業務、外注しコストダウンや対策の高度化を行う業務の切り分けが求められてきたため、インソースとアウトソースの業務分担例を策定する。

以上の目的に対し、下記合計 17 回という討議プロセスを経て、サイバーセキュリティ人材の定義を行った。

なお、人材定義 WG に関する活動履歴については、報告書紙面の関係で、別紙として添付する。

5.　まとめ・提言

5.1. まとめ（第一期の到達点）

約一年間にわたる本検討会の活動（第一期：2015 年 6 月～2016 年 6 月）を経て、日本の産業界におけるサイバーセキュリティ事情について、様々な観点からの分析、議論を重ね、産業界としてのサイバーセキュリティ人材育成のあり方として、まずは、産業界が求める人材像の定義に焦点を当ててきた。

現在の到達点としては、以下の 2 点がある。一つは、概ね産業界共通に存在すると思われる情報システム部門領域を対象としたサイバーセキュリティ人材像について定義したこと（下記（1））、もう一つは、人材育成・維持のエコシステム実現に向けた今後の取り組みに関する基本方針を策定したこと（下記（2））である。

（1）産業界共通の情報システム部門領域を対象としたサイバーセキュリティ人材定義

日本のユーザ企業における情報システム部門をスコープに、必要となるサイバーセキュリティ機能を洗い出し、それら機能を実現する要求知識と業務区分で人材を定義した。

人材定義としては、主たる定義と、それに先立つ各種情報整理があり、全体像は以下のようになる。

・「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）人材育成・維持のエコシステム実現に向けた今後の取り組み方針策定

新たに「人材育成 WG」を立ち上げ、人材育成の手段に対する産業界としての要件定義や各種教育プログラム、教育施策等について共有する環境の構築、人材育成関連ビジネス主体との連携検討等を検討会一丸となって推進する。

また、このような活動を行ない易くすることを目的に、第一期成果物（上記（1））の知財、および権利関係の整理、組織間で利用契約可能な組織形態の見直しを行う。

5.2. 提言

本検討会の第一期活動、および本報告書の執筆作業を通して、サイバーセキュリティ人材育成に関する産業界としての様々な理解・見識が深まり、また、産業界として取り組むべき数々の施策についても明らかになってきた。以下、本検討会における合意事項、および活動を通して再認識したことを本検討会からの提言として列挙する。

＜サイバーセキュリティ人材育成のスコープ＞

日本の産業界におけるサイバーセキュリティ人材育成を考える際、少数のサイバーセキュリティ専門職を育成していくことだけにとらわれずに、個々の企業が有する重要な各種資産を守るセキュリティ対策全般の向上に資する人材育成と定め、効率的かつ効果的に、広くそのノウハウを蓄積する機会を準備・提供できるかという視点で取り組むべきである。

＜サイバーセキュリティ専門部署の必要性＞

企業の差別化要因の源泉となる知財・営業の秘密等の重要情報を、意図的なサイバー攻撃から守る体制を日本の組織が積極的に整えることにより、将来の日本の産業競争力がいま以上に高められる（幾分、現時点では行き過ぎと評価されるであろうことが予測されるが敢えて)。そのためには、CISO や CSO に代表されるセキュリティの全体統括を所掌するトップ層、およびそれを支える役割を担う専門部署（本検討会の成果物上は「サイバーセキュリティ統括（室等)」と呼称する組織）の設置が必要、かつ重要になってくる。産業界として、経営者の理解を得ながら設置に向けての取り組みを推進していく。

＜業界固有の人材定義＞

第一期では、概ね産業界共通と思われる「情報システム部門」領域を対象としたサイバーセキュリティ人材像の定義を行ってきたが、加えてモノの製造や運行を行う企業・業界に固有の人材定義についても一定のレベルでは必須と考える。

ここで重要なのは、業界ごとの違いについて『丁寧に議論する』場を設定することである。また、業界ごとにその業務に関する深い知見を持ち、牽引力（リーダシップ）を有するリーダ役が必要である。

業界（事業）ごとの違いが議論になりそうな観点としては、組織的対策面（方針、体制、連携、規約等)、人的対策面（育成・教育、雇用等)、物理的対策（区画、管理等)、技術的対策（適用可能技術等)、および職務の違い（管理者、運用者、技術者）等が挙げられる。また、ユーザ企業の業種専門技術者がセキュリティ知見を有すると共

に、彼らを支援すべきセキュリティを得意とするICT企業との連携関係構築も必要である。

これらを実現していく環境の構築と、人材を定義する作業を引き続き推進していく。

＜2020年東京オリンピック・パラリンピックに向けて＞

2020年の東京オリンピック・パラリンピック開催におけるセキュリティリスク対策が本検討会発足の契機であることは、冒頭述べた通りである。しかし、議論を深めるにつれ、セキュリティ人材育成実現においては、「人材の定義」を実施し「その育成施策を提供」することが必要不可欠であり、そのためには『丁寧な議論』が必要であると説いた。

その一方で、『丁寧な議論』を進めていては2020年に間に合わないというジレンマも感じており、2020年に向けて如何に加速化を図るかを議論している。

次説にその議論の一端を記述することで、第二期への課題提示の一端としたい。

5.3. 残された課題と今後の方向性

本検討会では、セキュリティ人材の役割の明確化とその業務に必要なスキル定義を行い、次は育成施策に転じていく。ここで、人材の育成方策や育成場所は一組織に閉じるべきではなく、社会全体で共有することが必要、かつ重要である。それが本検討会のように40社を超える企業が業種・業界の壁を越えて結集している理由の一つでもある。

3.2項の「図10 人材育成・維持のためのエコシステム」でも示したように、今後、産業界は中上級人材の育成と活用のための組織構造を見直していくことで、個々のセキュリティ対策に当たっていくことになるが、必ずしもその必要な人材全てを育成できるわけではないこともまた認識している。また、教育機関との連携は、多数の初中級人材育成を効果的に行う目的で進めているが、そのスキーム構築と人材の輩出までにはある程度の時間を要する。加えて、未知の強力なサイバー攻撃や、同時多発的インシデント発生時には、対策作業を的確かつ迅速に牽引するリーダの存在が望まれるが、かかるリーダ役をこなすべきサイバーセキュリティにおけるいわゆる「トップガン」と称される最上級人材の育成検討までは、残念ながら取り組めていない。

2020年を考慮した場合、この量的不足への対応、および少数ではあってもトップガンの育成に如何に対処すべきかが、今後の検討課題の一つと考える。

なお、上記考察の詳細については、参考資料として記載した「トップガンも含めたサイバー人材の育成・活用についての一考察」を参照されたい。

5.3.1. セキュリティ人材の量的不足への対応施策

(1) 既存IT技術者のセキュリティ人材への転換

本検討会での人材定義の議論を行う過程において、参加企業からの重要な気付きが得られている。サイバーセキュリティというと技術者を連想しがちだが、企業の日常業務においても緊急時の対応においても、非技術的な事項が実は少なくない。その一方で、サイバー攻撃への対応には守備側に十分な ICT の知識と技術力が要求される。

従って、人材を育成・活用し、維持・確保するためには、以下の観点が重要である。

i) 守備側の技術レベルは攻撃側の技術レベルに均衡する必要がある

ii) さらには、非技術的なことを扱う人材も育成対象である

i）については、サイバーセキュリティ人材の基本素養として IT 技術が不可欠だとすると、IT 利用の進んだ日本企業といえども、人材に関しては予想外の現実を抱えている。元々日本企業の IT 技術者は ICT ベンダにほぼ集約しており、セキュリティ分野へ投入可能な技術者の数には限界がある。

・一般のユーザ企業では、そもそも IT 技術者の採用自体が極めて希少である。
・重要インフラを担う企業ではそれなりの専門技術者を採用するが、その配置先は当然のことながら概ね業務の根幹を担う制御系システム部門であり、IT ではない。
・ICT ベンダは最も多くの IT 技術者を採用するが、製造部門や運用部門での配置も多く、加えて近年は人工知能(AI)やデータ解析等の新規分野への投入も必要であり、複数の分野で取り合いの状態が続く。

上記から言えることは、サイバーセキュリティ技術者の育成においては、これら数少ない ICT 企業の IT 技術者を対象にするしかない、ということである。自社の対策のみならず、一般のユーザ企業のセキュリティ防御に貢献する人材の輩出には、ICT 企業が率先してセキュリティ分野での採用増を含めた人材育成を行うと共に、他分野での IT 技術者をセキュリティ技術者に転換を図っていく施策が必要である。また、そのためには、当該人材をコアとした新たなセキュリティビジネス、産業創生が可能となるような社会の実現が企業経営の観点からも必要不可欠となる。

一方 ii）については、今回の成果物である「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～」でも示したように事業継続計画(BCP)やコンプライアンスを背景に、サイバーセキュリティに関する管理業務担当が必要であり、実際多くの企業で当該業務を担う組織が存在する。

日本では 3,500 社を数える上場企業が存在するが、管理業務担当は共通して存在するにも係らず、一般的に人事ローテーションの対象になりがちな職種であることは、今回検討会参画企業をサンプルとしてみても一般的な傾向であることが判った。今後、専門職として認定していく等の、継続して育成すべき施策も必要と考える。

これらの現実を見据えて、産業界として一気通貫で横断的に実施可能な具体的、かつ現実的なセキュリティ人材育成の道筋を決めていく必要がある。

(2) 企業間連携を踏まえたサイバートレーニングの必要性

（1）で述べた施策により、本検討会参加企業が 2020 年までに一定レベルのサイバー攻撃対応力を、自社保有、または企業間連携等によって確保するという目標を共有し、実現に努力することは重要である。

それと併行して行うべきことは、確保した人材をサイバー攻撃に対する防御に有効的に活用するための恒常的な訓練の実施である。参加企業が人材育成に取り組み、小さくても CSIRT を保有することになり、すべての CSIRT を集めてサイバー攻撃対応演習を行うことは、活用施策の候補の一つとして上がっている。

たとえば、ある企業がサイバー攻撃を検知した場合、速やかにすべての CSIRT に連絡が行き、連絡を受けた CSIRT はガイドラインに沿った調査を行い然るべき対応を取り、その結果がすべての CSIRT で一定時間以内に共有されるようにする、といった所作が演習を行うことで 2020 年にスムーズに実行出来るようになっていれば、被害を最小限にとどめることも現実のこととなり得る。

5.3.2. トップガン人材の育成について

(1) 産官学連携による育成環境の構築と人材の共有

準備、訓練されたサイバー攻撃を、一企業で凌ぎ続けることは難しい。どこかで攻撃を検知したなら、多くの企業が短時間で連携し協力することで、被害を水際で食い止めるか最小限にする横断活動が必要であることは前に述べた。

本報告書では、産業界においては、サイバーセキュリティ統括（室等）を設置し効率的な対処が望まれるとしているが、高度化するサイバー攻撃に対しては、いわゆるトップガンと呼ばれる人材との連携も必要、かつ有用である。そのための人材育成施策も今後必要不可欠であると考える。

トップガンの役割は、一人であっても連携を統率し、被害を最小限に食い止めることである。そのために必要な知識、力量、リーダとしての統率力を備えていなければならない。政府や自治体が攻撃対象となることも多い。産業界と同じくトップガンの役割は公共機関においても重要である。

しかし、高度な育成環境（たとえば OJD[21]）を企業内に用意することは困難であると

[21] OJD　On the Job Development の略。新入社員や若手社員が職場での日常業務の遂行を通じて、直属の上司からの指導・支援を受けながら、将来必要となる能力の開発を行うこと。

共に、当該最上級人材の育成を指導できる人材を有していることは稀である。また、もしトップガン人材が確保できたとしても、世間相場に見合った処遇を行うことは他の社員との関係上困難が伴い、結果的に外資企業に引き抜かれる、という事態も散見される。これは企業がトップガンを必要としていないということではないが、企業内にトップガンを留保することは難しいことを示唆している。

かかる状況に対処するためには、産官学連携でのトップガン育成施策、および効果的に活動できる体制作りの検討が必要であり、今後、各業界の有識者を交えた具体的な議論の場を設けていきたい。

(2) 高度なサイバーセキュリティ技術の研究環境確保

日本の企業や大学に高度なサイバーセキュリティ技術を研究できる人材がいない訳ではないが、研究結果を活用する場が企業側に確保できないため人材が育たないという現実がある。他国と比べても企業側の技術力が相対的に高いにも関わらず、である。

これはトップガン人材の育成、活躍の仕方と絡めて考えるのが建設的だと言える。

海外のトップガン人材は多く企業に属すると考えられ、当該海外企業と日本の研究者が交流、連携することで育成の場を確保すると共に、当該人材を CSIRT やセキュリティ統括等の組織に迎え入れることで、企業としてはセキュリティ体制が有効なものとなり、研究者としても研究成果を活用する場を得ることができる。

これまで述べてきた事項のみが残課題というわけではないが、セキュリティ対策を実効化するためには最も重要と認識され、かつ何らかの取り組みを進めなければ将来に禍根を残すと考えている課題を指摘した。本検討会が出来るだけ早くそのイニシアチブを取り、実現に向けての推進役となることが必要と考えている。

6.　今後の活動について

本検討会の第一期の活動成果を踏まえ、これらを産業界としての具体的な施策として、教育機関や官の関係者との連携の下で実行していくのが第二期である。本検討会としては、2016 年 10 月以降を第二期の取組み開始とし、以下の活動を予定している。

（1）育成手段等の具体策の提示と、実現加速化のための官や学との連携実現
（2）産業界としてのセキュリティ人材活用を促進するキャリアパスの設計と実現
（3）産官学連携のエコシステム実現に向けた施策、制度設計の実施

6.1. 育成手段等の具体策の提示と、実現加速化のための官や学との連携実現

6.1.1.　セキュリティ人材の育成手段の提示

第一期の成果物である「人材定義リファレンス」に基づき、組織における当該役割を担う人材を育成するための施策を推進・実行していく。具体的には、人材育成・維持のエコシステム実現に向けた施策を検討する組織として、従来の人材定義 WG の後継として新たに『人材育成 WG』を立上げ、下記施策を実行する。

なお、施策実行に当り、他組織との NDA 締結等の契約行為の実施や、活動費用の確保と管理が必要不可欠な状況であることから、2016 年度の早い段階で組織の法人化を目指し、必要な施策を迅速かつ的確に実行可能な体制に移行することとしたい。

(1) 育成のための実施項目

① 教育体系の検討（講座、研修、演習等　ISO22398、DHS；HSEEP 等を参考）
- ・講座等のカリキュラム要件・内容の検討／設計
- ・クラウド等の活用による地域に限定されない実行策の検討

② トレーニング/教育のための「カタログ」構築
- ・各種教育プログラム（無償／有償問わず）リストアップ
- ・リファレンス定義の職種との適合性検証と評価
- ・育成ポータルサイト等の構築による、検討会メンバ各社を含む教育プログラムや教育ツールの掲載、および利活用可能な環境の整備

⇒ 既存の商用教育プログラムを展開しているベンダに対しても、積極的に掲載を依頼すると共に、検討会として利用しやすい条件の交渉を実施

③ サイバーレンジ整備
- ・演習環境概要、仕様等の検討と要件定義
- ・産業界での利活用を前提に上記に基づく演習プログラムの策定

⇒ 既存の官製演習教材の活用も視野に入れた実効性のある活動実施

(2) プロダクション領域での人材定義の実施

日本の重要インフラを支える産業分野の多くは、モノの生産や運行と管理を行うことで企業活動を維持し、日々の国民の暮らしを支えている。この、いわゆるプロダクション[22]（システム／業務）領域においても、セキュリティ人材の必要性と、その為すべき役割は重要である。

第二期では、この生産や運用の領域までフォーカスを広げ、当該業界でのセキュリティ人材の必要性と現状の把握、および育成が急務な人材の具体的モデルを策定していく。

(3) 次世代に向けた人材育成の推進

大学や高専における学生を対象とした人材育成活動は、近い将来における産業界での適切なセキュリティ人材の確保と配置のためにも必要不可欠である。

本検討会では、先行している産学連携（寄附講座）活動の水平展開を複数の大学や教育機関に対して実施していくと共に、(2) に示すプロダクション領域での人材定義モデルの策定結果をベースに、新たにマネジメント系や、safety の概念を取り入れた制御システム系における人材育成活動を推進する。

(4) 各種セキュリティ制度面との連携

官が今後展開する各種セキュリティ施策との具体的な連携も、産業界でのセキュリティ人材育成を円滑に推進していく上では非常に重要な位置付けとなる。

例えば、「情報処理安全確保支援士制度」の開始に伴い、企業はセキュリティ人材を如何に登用し活用し得るのか。経済産業省が推進する「サイバーセキュリティ経営ガイドライン」に基づき、企業はセキュリティを経営の根幹と据えた際に、セキュリティ人材の的確な配置と処遇を如何に実現していくべきか。

また、NISC の「サイバーセキュリティ人材育成総合強化方針」や総務省の「サイバーセキュリティ演習に関する取り組み」、文科省の「enPIT」等についても、今後の人材育成計画を策定する上では常に注視が必要である。

これらの官が提供する各種制度との連携と、産業界の代表である経団連の動向を踏まえた推進計画策定が、本検討会の活動推進にとっても非常に重要な位置付けとなる。

6.2. セキュリティ人材活用を促進するキャリアパスの設計と実現

学の分野でのセキュリティ人材育成施策と併行して、産業界としてセキュリティ人材を雇用し受け入れ、所定のキャリアパス制度の下で育成すること、およびその実力を評価する

[22] プロダクション：本文章では、各企業のビジネスに直接的に関わるシステム/業務をさす(製造業における製造ラインのシステム等)

尺度を作り、実力に応じた適正な処遇を実現する責任が産業界にはある。

これは企業一社では出来るものではなく、まさに産業界の横断的連携組織である本検討会で率先して制度設計を実施し、経団連や国に提言することでその実現を推進していくことが求められる。

米国等では、優秀な学生を官のセキュリティ組織の現場で訓練し、一定期間を経て産業界での起業や優秀な技術者として雇用する方式が一般化している。日本国においても 産官学が一体化したセキュリティキャリアパス制度の実現に向け、引き続き対応していく。

6.3. 産官学連携のエコシステム実現

日本の産業界・企業の特性・実情に即した人材育成・雇用・活用（維持）が効果的に連携することで、IT 企業のみならずユーザ企業においても活用が可能なエコシステムの具体案を 2016 年中に検討・提唱する。

その上で、産業界としての活動は、本検討会あるいは本検討会のメンバ企業が主体的に取り組んでいく。将来的には、このエコシステムを基盤とした新たな産業界としてのビジネスを振興し、育成に寄与するスキームを実現していきたい。

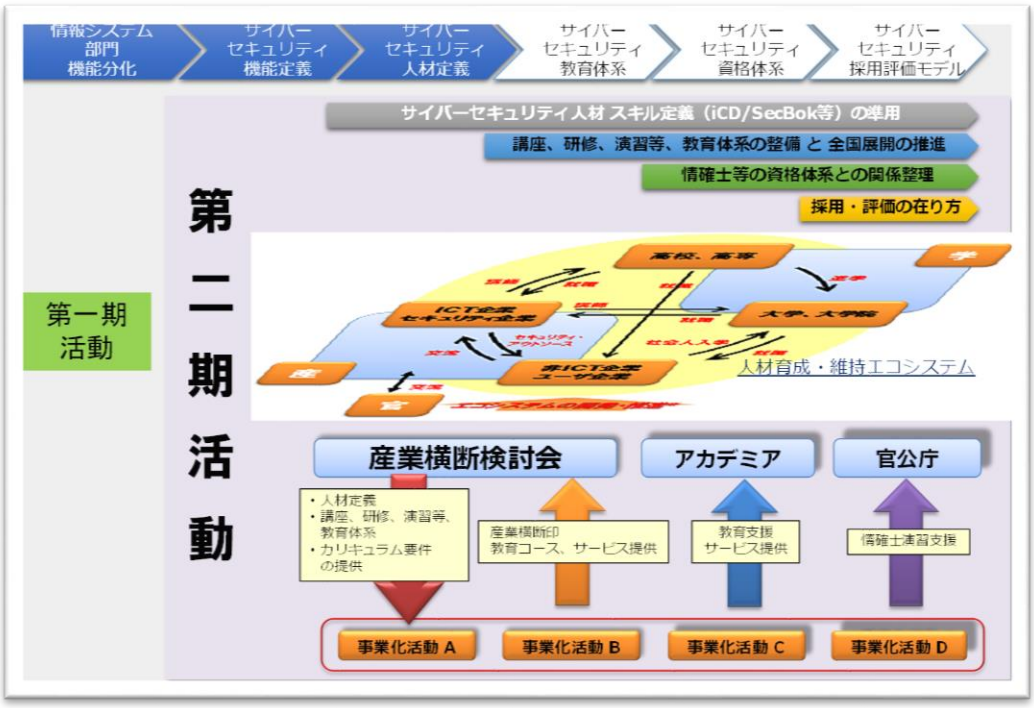

図 19 セキュリティ人材育成ビジネススキームの構築

7. 成果物

①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～

別添 A1- A3 参照

②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～

別添 B 参照

③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

別添 C 参照

④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

別添 D 参照

⑤産業横断サイバーセキュリティ人材育成検討会 人材定義 WG 報告書

別添 E 参照