「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

2016/01

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」の活動に関する 2015 年 12 月までの中間報告であり、本検討会に関心のある方々に、検討会の目的や意義、活動内容等について理解いただくことを目的としたものである。

本検討会または本報告書についてのお問い合わせは、cyber-jinzai-ml@hco.ntt.co.jp まで。

目次

1. はじめに

1.1. 概要

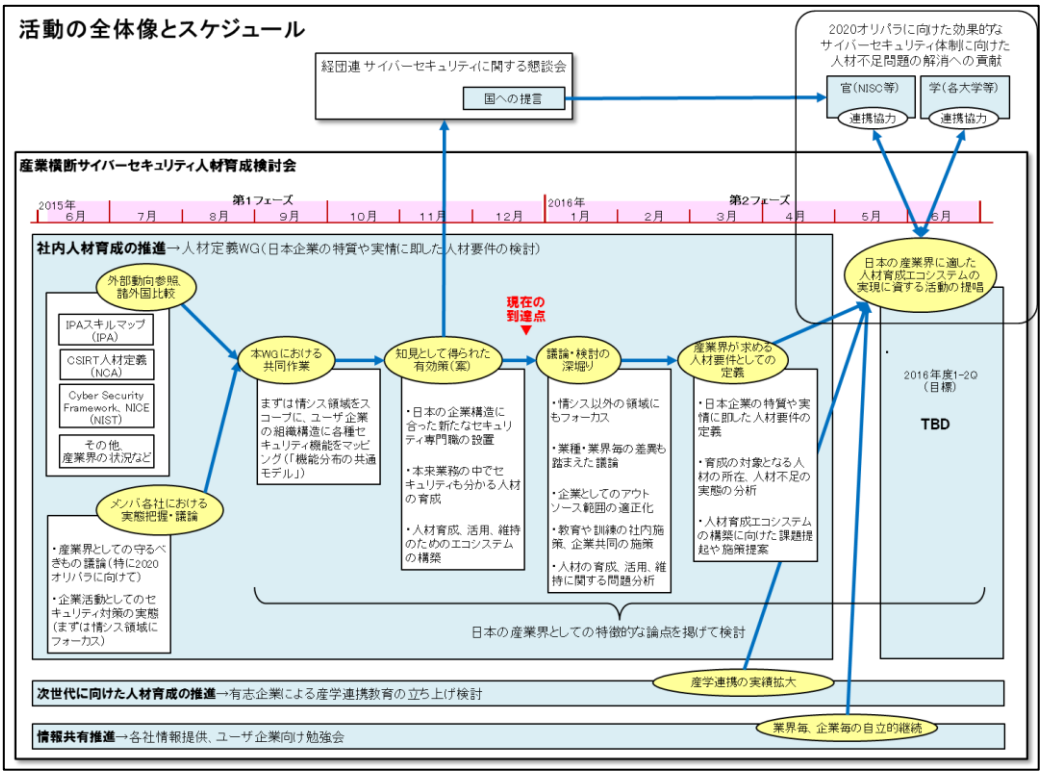
2015 年 2 月 17 日に発表された経団連から国への提言において重要視された活動の 1 つである人材育成の実行・加速を目的として、2015 年 6 月 9 日に「産業横断サイバーセキュリティ人材育成検討会」が発足。重要インフラ分野を中心とした重要な業界に関わる企業 40 社以上が結集し、サイバーセキュリティに関する人材育成について議論を行った。

これまでのところ、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。また、その結果、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

上記を踏まえ、今後は、以下について 2016 年 6 月目途で取り組む予定である。

- 業種・業界毎に求められる人材像の明確化
- 企業毎に有する育成プログラムの共用等による効率的な育成の推進
- 産学官連携した人材育成のためのエコシステム構築に向けた声掛け



1.2. 背景

2020 年東京オリンピック・パラリンピック競技大会を控え、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、世界中の攻撃者の興味を惹き攻撃の動機を与えることになり、日本の各業界や企業にとってサイバー脅威から守るべき対象と危険度が急激に拡大しつつある。(別紙 1 「日本企業における人材不足と産学官連携による対策の必要性」参照)

折しも 2014 年 10 月、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「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。同提言においては、重要視された課題の一つである人材育成について、産業界として具体的な取り組みを進める意思が表明されており、同懇談会にも関わった日本電信電話株式会社（以下、「NTT」とする)、日本電気株式会社（以下、「NEC」とする)、株式会社日立製作所（以下、「日立製作所」とする）の 3 社が、実際の活動をどう具体化しどう推進していくべきか検討するための場が必要と考え、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て

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」（以降、「本検討会」とする）を発足させた。本検討会の参加企業は当初の約 30 社から、40 社以上にまで拡大している（2016 年 1 月現在）。

1.3. 「サイバーセキュリティ人材育成検討会」の目的と意義

本検討会では、サイバー脅威の急増に対して圧倒的に不足するセキュリティ人材の問題を踏まえ、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、産業界における協力体制を構築し、産業界に必要な人材像（人材要件）を定義・見える化し、産業界のための人材育成を推進し、最終的には、サイバー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提唱する。

主な活動は、「社内人材育成の推進」、「次世代に向けた人材育成の推進」、「情報共有の推進」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先導する姿勢を見せて臨むことが極めて重要と考える。

1.4. これまでの活動と今後の予定

これまでの活動では、以下を実施してきた。

- 社内人材育成の推進

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・機能分布の共通モデルを作成し、幾つかの有効策（案）が知見として得られた。

- 次世代に向けた人材育成の推進
  有志企業メンバーにより、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っている。
- 情報共有の推進
  参加企業が抱える課題や取り組みを相互に共有しており、その活動自体が各社の人材育成に活かされている。

今後は次のような活動を予定している。

- 社内人材育成の推進
  情報システム以外の領域にもフォーカスを広げ、業種・業界毎の差異も踏まえた議論等を行いながら、日本の産業界が求める人材要件としての具体的な定義をまとめ、前述のようなサイバーセキュリティ人材育成のためのエコシステム実現を目指した、産、学、官が相互に連携する施策として、2016 年度上期中に提唱する。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ー企業が主体的に取り組んでいく。
- 次世代に向けた人材育成の推進
- 情報共有の推進
  適宜、前述の「社内人材育成の推進」とのシナジーにつなげる取り組みとして継続する。

2. 「サイバーセキュリティ人材育成検討会」活動概要

前章で述べたように、サイバーセキュリティ人材不足が、広く一般に認知され、セキュリティ人材育成が今後社会にとって大きな課題であることは多くの人にとって共通認識となった。また、経団連の提言によって、サイバーセキュリティに関して、産業界として検討していくことが示され、実際の活動としてどのように進めていくべきかが重要となった。そういった状況を受け、少しでも具体化しようと、2014 年末に有志が集まり活動が開始され、以下のような点を話し合った。。

- 最初に取り組むべきは人材育成

  企業におけるセキュリティ対応に関して検討しなければならない項目は多岐にわたっており、さらに広がりつつあるが、全ての項目において実施・実行を阻害している要因となるのは人材不足との認識から、産業界として最初に取り組むべきは人材育成とする。

- セキュリティ人材育成は企業が共同して取り組むべき

  セキュリティ人材不足は、それぞれの企業が個々に取り組んで解決できる状況ではない。また、セキュリティ専門企業を除いた多くの一般の企業においては、セキュリティに関する活動はそれぞれのビジネス差別化要因ではないことが多く、共同で対応することが可能である。

- セキュリティ人材育成は社会貢献であり、その認識を醸成すべき

  セキュリティ人材の育成は、産業界のみならず、社会全体の課題である。人材育成を社会的価値の創出（＝社会課題の解決）と捉え、産業界として、社会貢献しているという認識を持つことが必要である。

- 産業界として意思を明確にする

  産業界としてどのような人材が必要なのかを声を上げて明確に示していくことが必要である。と同時に、セキュリティ人材が企業で活躍できる環境を提供することも検討する必要がある。

- スピード感を持って具体的な活動を行う

  2020 年東京オリンピック・パラリンピック競技大会に向けて、時間があまりない中で、どのように進めていくのかを考えなければならない。きちんと形式立てて進めようとすると施策を開始させるまでに数年を要してしまう。十分でなくても何らかの形で始められることから進めるようにする。

その活動が契機となり、2015 年 6 月 9 日に本検討会を設立した。

検討会メンバーに関しては、経団連の「サイバーセキュリティに関する懇談会」で発表をした 15 社のうち、セキュリティ人材に関して積極的な印象を受けた企業から声がけをすることにした。

また、重要インフラ企業は必要不可欠であると考え、重要インフラ 13 分野のそれぞれより、少なくとも 1 社は参加していただくことを想定した。ただし、現時点での重要インフラ 13 分野以外にも、サイバーセキュリティを考える上で重要と思われる事業分野も対象とすることとした。(例えば、自動車業界。現時点では重要インフラ分野にはなっていないが、将来自動運転や IoT 技術等の発展により交通管制システムが広く活用される可能性は十分考えられ、将来の重要インフラ分野になることは予想に難くない。)

産業界全体を考慮し、経団連といった枠も越えて産々連携することも視野に入れている。ただし、議論を活発に進めていく上で、ある程度の参加者に絞ることも必要と考え、現在の 40 数社のメンバー構成となっている。メンバー拡大については、今後より具体的な施策を行っていく際など、必要と思われる場合にその都度検討することが検討会の現時点の合意である。

2.1. 検討会の位置づけと計画概要

2.1.1. 検討会の位置づけ

本検討会の位置づけ（意義）は、以下のように認識している。

① 産業界の情報・意見を明確に出していく場としての位置づけ
産業界が必要とするセキュリティ人材定義を明確にするなど、企業におけるサイバーセキュリティ対応に関わる事項を広く外部に対して、産業界視点で発信する場である。

② 産業横断で連携をする場としての位置づけ（産々連携活動・情報共有活動）
広い業種にわたり企業のみで構成されているため、産業界としてのセキュリティ人材育成ならびに各社のセキュリティ対策について話し合うことができる。人的つながりを信頼の基盤として、情報共有活動を行う場である。

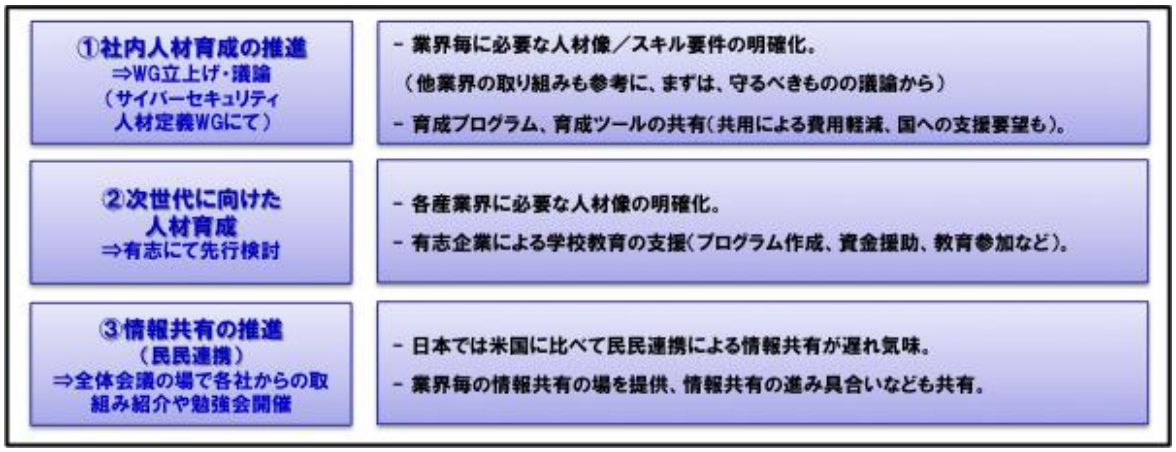
③　産業界としての共通の意識を醸成する場としての位置づけ（産官学連携の推進とエコシステム構築）

セキュリティ人材不足を解決することは社会的課題であり、産業界として社会全体に向けての共通価値を創造することを目指す活動であるとの意識を醸成し、その意識の下、必要と思われる産官学連携の推進ならびにセキュリティ人材育成のためのエコシステム構築を推進する場である。

2.1.2. 目標・会議体等

- 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。



- 会議体

会議体としては、全体会議、ユーザ企業向け勉強会、人材定義ワーキンググループ（以後、「人材定義 WG」とする）の 3 つを設置した。

①　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。

②　ユーザ企業向け勉強会

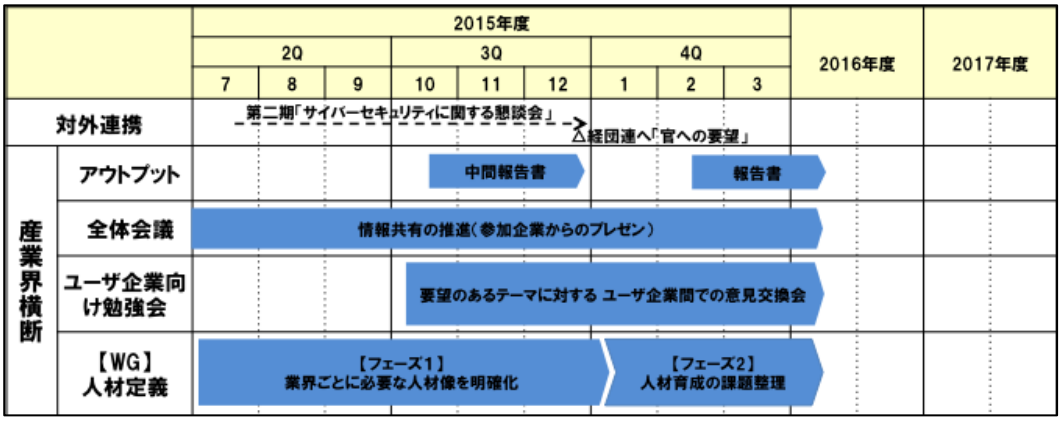
サイバーセキュリティ情報共有活動の 1 つとして、ユーザ企業向けにサイバーセキュリティ関わる話題を取り上げて、外部講演者による勉強会形式で開催する。

③　人材定義 WG

産業界が必要とするセキュリティ人材像を明確にするために人材定義を行う。人材定義に関して集中的な議論を行うために、人材定義に積極的に貢献できるメンバーを募集した。活動を 2 つのフェーズに分け、産業界全体で共通的と考えられる部分に関しては第 1 フェーズで、個々の業界毎で異なっている部分については第 2 フェーズ以降で検討することになった。

- スケジュール

スケジュールは、当面の活動期間として、2016 年 6 月までを第 1 期とした。また、第 1 期を第 1 フェーズと第 2 フェーズに分けた。第 1 フェーズでは、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。



- 開催状況

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。

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	
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）		○		勉強会テーマ
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」

なお、前述の 3 つの会議体の他、大学連携については、2020 年東京オリンピック・パラリンピック競技大会が間近に控えているため、出来るだけ早くに体制を整えることが必要との認識から、全体ではなくスモールスタートとして大学連携に積極的な有志企業での検討を行っている。活発な議論が行われ、具体的な施策の検討が進んでいるが、現時点では報告すべきではないとの判断から、本中間報告には含めていない。

2.1.3. 想定された議論項目（守るべきものの明確化～必要な人材像の定義）

第 1 フェーズにおいて、解くべき課題を具体的にしていく活動を行った。具体化を進める中で、以下のような議論項目を想定した。

- 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、サイバー攻撃から守るべきものとして企業が対象とするものを把握する必要がある。

  どの企業においても情報システムにおける情報資産は守る対象として共通して持っていると考えられるが、それ以外にも、例えば、製造業における工場ラインなどのプロダクションシステム、重要インフラ業者のサービスインフラなど、サイバー攻撃から守るべき対象がある。

  将来的には情報システムと物理的な対象が相互に連携していくことが予想されるため、企業におけるサイバーセキュリティを検討していく中で、守るべき対象を広く考えるべきである。その際に、業種・業態による差異は当然のことながら、詳細に検討していけば、企業毎に異なっていると思われるが、詳細になりすぎて一般性を失わず、なおかつ、産業界としての特徴を踏まえた議論を行うべきとの認識が得られた。

- 企業活動としてのセキュリティ対策の共通モデル

  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共通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。

  ここ数年、CSIRT の設置の必要性が広く言われているが、企業のセキュリティに関連する活動全体にわたってどのような人材が必要であるかを検討することが求められており、CSIRT に加えてどのようなセキュリティ関連活動が企業で行われているのかを把握する必要があるとの認識に至った。

  これは、企業としてセキュリティ対策をどこまで講じればよいのかということを示すことにもなる。

  企業活動に際して、法律、商習慣、人材の流動性などそれぞれの国によって事情が異なっていることを踏まえれば、企業におけるサイバーセキュリティ対応についても同様に、日本の独自性を考慮することが必要になってくる。米国では企業がサイバーセキュリティ対策を行う際の共通のフレームワークとして NIST の Cyber Security Framework を企業に採用するよう働きかけている。さらに、他国に対しても、同フレームワークの採用を働きかけている。したがって、日本における独自性を考慮した日本企業におけるサイバーセキュリティに関するフレームワークについ

ても議論が必要である。

- 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。

  産業界で必要なセキュリティ人材定義の表現方法は、採用活動や組織体制整備など企業においてセキュリティ人材を扱う場面で、それらを行う人が使いやすいものとなっていなければならないが、例えば人事部がセキュリティ人材を募集する際に一般的に認知されている職種の表現が確立されていないため、人材のミスマッチが起きている現状がある。

  また、業種・業界毎に必要とされるセキュリティ人材が異なっており、その点を考慮したセキュリティ人材定義を行う必要がある。今回の検討会では、まずは、共通に必要とされるセキュリティ人材について検討し、典型的なモデルとして明確にすることを優先するが、最終的には、業種・業界による差異も踏まえてセキュリティ人材の定義を行う必要がある。

- 育成の対象となる人材がどこに存在するのかについて

  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。ユーザ企業（非 ICT 企業を想定）には直ぐにセキュリティ人材となれるような人は少なく、大手 ICT 企業には、セキュリティ人材に転換可能な ICT 人材はある程度いると想定したが、具体的な数字は把握できていない。育成の対象となる人材がどこに存在するのかを検討する必要がある。

  また、学生に視点を向けると、大学の学部生や大学院生が育つには 2016 年度からスタートするとしても、早くて 2 年経たないと社会に出てこないことを考えると 2020 年東京オリンピック・パラリンピック競技大会には間に合わない。発想を切り替えて、学生については長期的視野でどう育てていくかを考える必要がある。また、対象を大学・大学院だけではなく、高等専門学校まで含めるか否かを検討することとした。

2.1.4. 産業界としての論点について

参加者からの意見を聞く中で、上記議論項目を検討するに当たって考慮すべき特徴的な論点について述べる。

- ICT 企業とユーザ企業

  セキュリティ専門人材のキャリアパスをユーザ企業で構築することは、現状では非常に難しい。例えば、証券会社の人材は、通常、証券などの金融に関わる仕事をするために入社してきた人が中心であり、そのためのキャリアパスはある。しかし、セキュリティを専門に扱う人材を採用して、ずっとセキュリティの専門性を生かしつつ昇進していくようなキャリアパスを構築することは難しい。したがって、今いる人材をどのように育てるかが課題となる。

  今後、ユーザ企業においてもサイバーセキュリティへの対応が経営的な課題として取り上げられるのであれば、人材を確保し長期的に取り組まなければならなくなる。その際に、ユーザ企業のセキュリティ人材のキャリアパスをどのように構築するのかは検討課題である。

- 企業規模（大手企業と中小企業）

  検討会に参加している企業は大企業が多いが、産業界全体として考えれば、中小企業でのサイバーセキュリティ対応は非常に重要である。

  最近の標的型サイバー攻撃は、もっとも弱いところを突破口として、徐々に目的とする組織に侵入してくる。大企業も数多くの中小企業と取引しており、システム連携も頻繁に行われていることを考えると、連携している中小企業でもセキュリティ対策をしっかり行うことが必要となってくる。

  中小企業では情報システム規模や運用管理している組織の有無など状況は様々である。また、サイバーセキュリティ対応を行うためのリソース不足が顕著であり、大企業から比べれば予算も少ない。そのため、セキュリティ専門で対応する人員を配置できず、多くの役割を兼任する場合が多いが、そのような小さい規模の企業におけるサイバーセキュリティ対応も産業界として検討する必要がある。

- ICT システムと制御システム

  一般にサイバーセキュリティ対策として検討するべき対象は、企業の構成員が利用する情報システムが中心であるが、産業界としては、製品を製造する工場のシステム、顧客にサービスを提供するためのサービスシステムおよびそのインフラ、製造して販売した製品自身、顧客システムに提供するサービスなどのサイバーセキュリティ対策を考えなければならない。

  また、最近、工場等システムへのサイバーセキュリティなどをまとめて、“制御シ

ステムセキュリティ”と呼ばれてマスコミ等で取り扱われることが多い。制御システムには様々なもの（例えば、石油精製、紙・パルプ製造や製鉄などのプロセス制御や、自動車などの組み立てラインなどのファクトリ制御は異なる。また、制御機器としてもDCS、SCADA、PLCなどがある。）があるため、検討会では、その点も考慮し、どこまで、制御システムセキュリティに踏み込むべきかを見極めることが必要になってくる。

- 業種による特徴

  本検討会は、産業横断ということで様々な業種からの企業が参加しており、それぞれ異なったビジネス環境、背景を持っている。サイバーセキュリティへの対応も業種による特徴を考慮する必要がある。同時に、企業活動という面では共通な活動もあるため、それを上手く一般化し、抽出して汎用的な形にまとめることが必要である。

- 単一ビジネス企業と複合ビジネス企業

  企業の特徴として、単一ビジネスのみを行っている企業と、一つの企業ではあるが複数の異なったビジネスを展開している企業とが存在する。後者には、一般には製造業として知られているが、金融事業、住宅事業、エンターテインメント事業等複数のビジネスを展開しており、売上なども各事業でバランスしているような例がある。このような企業の場合、事業毎で人材の特性も異なっており、サイバーセキュリティ対策の実施方法も適宜変更が必要となる。サイバーセキュリティ対応体制をどのように構築するのかに関して、業種・業態として分類するだけでなく、企業の経営形態に考慮することが求められるということである。

- 国内と海外展開

  国内のみで事業展開している企業と海外展開している企業が存在する。後者の場合、組織体制にも複数のパターンがあり、それぞれに応じた考慮が必要となる。また、展開している国毎にセキュリティに関わる法律等が異なることも考慮すべきであり、どのように整理し取り扱うか検討する必要がある。

- 情報システム系子会社の有無とグループ会社の関係

  企業のサイバーセキュリティ対応を考えていく中で、どこまでインソースで行うのか、アウトソースできる機能としてはどのようなものがあるのかを検討する必要があるが、その際に、情報システム系子会社を持っている企業とそうでない企業によって、大きく対応が異なることがわかってきた。また、グループ会社に対するガバナンスの違いも、サイバーセキュリティ対応体制に大きく影響することがわかっ

てきた。例えば、サイバーセキュリティ対策を実施する際（特にインシデント対応）に、対策実施部門に対して他部署への指示権限を持たせることが可能となるように、各企業の特性に応じて体制設計に工夫が必要となる。

- マネージメント層の専門性（CISO/CSO 等の特性）

  2015 年から、サイバーセキュリティは経営問題であるとの認識が高まり、CISO あるいは CSO の設置が必要であることが「サイバーセキュリティ経営ガイドライン」などで政府からも提言されている。CISO/CSO あるいは、CEO 自らがサイバーセキュリティへの対応を意識してリードすることが必要であることは、検討会の議論でも異論がない。

  欧米では、役員レベルでも人材の流動性が高く、CISO/CSO に就く人材も、専門性を持った人が企業を渡り歩く例が多く見受けられる。日本では、人材の流動性はあまり高くないため、CISO/CSO に任命された役員にセキュリティの専門性を求めることが難しい場合が多いことが予想される。そのため、日本的な CISO/CSO を想定したサイバーセキュリティ対応体制を考える必要がある。これは、企業経営の欧米との習慣・文化の相違であり、良い・悪いの問題ではなく、日本型のあり方を検討すべきということである。

- セキュリティ人材の要件：スキルセットと役割

  多くの一般企業におけるセキュリティ人材採用において、必要な人材の要件をどのように表現するかについて見直す必要がある。

  現状では、スキルセットを用いて人材の要件を表現することが多い。しかしながら、セキュリティのことをよくわかっていない人事担当では、スキルセットだけによる要件では、本当の求められている人材像を理解しにくく、また、人材派遣会社や人材リクルート会社においても的確な人材を供給できていないという状況が見受けられる。

  これは、世の中に共通に受け入れられるセキュリティ関連職種の定義がないため、技術者から人事関係者にまで広く受け入れられるセキュリティ関連の役割に関する職種ラベルが必要ということである。

  例えば、病院の中では、医者、看護士、レントゲン技師、薬剤師などの様々な職種・役割が明確に認知され、一般にも認識されており、人員の募集の際には、どのような人材が求められているのかが誰にでも明確であることと対比して考えれば理解がしやすい。（これはあくまでも、理解を助けるための例としてあげているだけで

あり、医療とは状況も対象領域も異なっているので、単純な比較をするつもりはない。）

2.2. 人材育成の取り組み

2.2.1. 人材定義 WG

人材定義 WG（以下「本 WG」とする）では、以下の 2 つの目的を達成するための基準及び導入運用プロセスを策定するべく、産業横断で本 WG に参加した重要インフラ分野を中心とした企業（以下、「ユーザ企業」とする）により、サイバーセキュリティ人材の定義に必要となる「サイバーセキュリティ対策に求められる機能定義」（以下、「機能定義」とする）の検討を進めてきた。

① サイバーセキュリティ人材不足を解消し効率的な教育訓練を実施する
② サイバーセキュリティに関連する業務を定義し、適切にアウトソーシングすることにより、2020 年東京オリンピック・パラリンピック競技大会に向けて効果的なサイバーセキュリティ体制を構築運用する

なお、「機能定義」とは、サイバーセキュリティ人材を定義する一つ前の段階のものであり、ユーザ企業に求められるサイバーセキュリティ対策の各機能を規定し、業種業界に拠らず必要とされるサイバーセキュリティ対策の機能分布の共通モデルを策定することを指す。更に、これら機能を担う人材を定義することを「人材定義」とする関係にある。

現在、セキュリティ人材（情報セキュリティ人材）の定義は、政府機関や様々な ICT 関連団体を通して実施されており ICT 企業を中心に積極的に人材育成が進められている。

しかしながら、現在公開されているサイバーセキュリティ対策に関する人材定義やスキルセットは、既に ICT 関連業務に従事する情報セキュリティ技術者にとってのキャリア形成に主眼が置かれているため、日本企業の特殊性を考慮したユーザ企業に適用できるサイバーセキュリティ人材のあり方というものが別に存在するのではないかという仮説に立ち、参加企業による討議に基づく「機能定義」について検討を行うこととした。

これまで日本国内の多くの企業では、情報セキュリティすなわち情報資産を保護するための「情報システム」を中核としたセキュリティ対策を重点的に実施しているが、ユーザ企業の ICT 利用環境を考えるとき、事業活動に求められるセキュリティ対策は「情報システム」だけではなく、生産活動や各種制御にかかるシステム、IoT に代表される製品やその開発プロセス等、守るべき対象が多種多様に存在しており、更にはインシデントハンドリ

ングを担うCSIRTがそれらのサイバーセキュリティ対策を横断的に共有連携していることから、情報漏洩対策だけではなく、サイバー攻撃への対処や漏洩後のレピュテーションリスク等幅広い対策を想定していく必要があることを共有確認した。

以上のことから、サイバーセキュリティ人材を定義するためには、まずはICT利用環境におけるセキュリティ対策と、CSIRT活動を含むセキュリティ対策に求められる要件の両面から考察した「機能定義」を定める必要があり、ユーザ企業各社のIT戦略に基づき、効率的な人材配置を行う指標とできるものを策定するに至った。

本WGにおいては、その限られた時間において一定の成果を策定すべく、まずは対応の急がれる「情報システム」に関するサイバーセキュリティ対策に必要となる機能定義について帰納的な検討を実施した。また、その他の守るべき対象についてのサイバーセキュリティ対策の検討は今後の課題として規定するにとどめた。

現段階での本WGの成果物は、情報システム部門に求められる機能定義及び、それら機能に対するサイバーセキュリティ対策の要件を例示している。これら要件の策定にあたっては日本独自の事情を踏まえた「機能定義」を目指すと同時に、グローバル展開するユーザ企業が海外拠点においても共通言語として活用可能とするため、検討の初期段階からThe National Initiative for Cybersecurity Education（通称 NICE）及び Framework for Improving Critical Infrastructure Cybersecurity Version 1.0（NIST発行）との相関を整理している。

さらに、「機能定義」ではユーザ企業におけるサイバーセキュリティ対策に求められる社内業務とアウトソーシングの活用を分類整理することにより、2015年12月28日に経済産業省から発表された「サイバーセキュリティ経営ガイドライン」の「3原則」に対応し、当該ガイドラインにある指示（特に、2、7、8、9、10）を実現するための機能も考慮するものとした。

2.2.2. 次世代に向けた人材育成

有志企業による教育機関との連携方法の具体化に向けた議論を実施している。

2.2.3. 情報共有の推進

参加企業が抱える課題や取り組みを相互に共有しており、その活動自体が人材育成に活かされている。

3. 人材定義 WG の活動と到達点

人材定義 WG では、2.2.1 に示した通り、サイバーセキュリティ人材を定義するにあたり、産業横断で本 WG に参加したユーザ企業において活用することができる人材の定義を策定することを目指し、サイバーセキュリティ対策の機能定義から、該当する人材の採用や育成を考えることができる基準を定めることを目的として討議を重ねてきた。

そこでは、ユーザ企業がサイバーセキュリティ人材を取り合うための基準を明確化するのではなく、ユーザ企業としてサイバーセキュリティ対策のあるべき姿を描き、かつ共有しながら、その姿を実現するために必要となる取り組みを「機能」として定義し、ユーザ企業ごとの規模や事業形態、情報システム子会社の有無や、委託先との連携等の現状を踏まえた、サプライチェーンの視点を持ったサイバーセキュリティ機能の定義と、それら機能を担う人材の配置や連携等をイメージできる全体像を生み出す作業を行ってきた。
この前提に基づき、ユーザ企業の知見と実績を踏まえての成果物とした。

3.1. 検討プロセス

先に述べた ICT 利用環境を前提とする広範なセキュリティ対策の必要性をユーザ企業間で共有し、更には人材定義として共通化できると考えられるセキュリティ機能を明確化することにより、より効率的なセキュリティ対策を講ずる一助になるという想定の下に協議を進めた。

当初の課題認識として、現在公開されている様々な情報セキュリティ技術者に対するスキルセットでは ICT 領域における「技」にその力点が置かれていることから、長期的キャリア形成を前提とした人事制度を持つ多くのユーザ企業においては、人事評価項目としての活用が困難であり、またシステム構築や運用保守を担う SI 企業においても、開発運用を担う人材の育成は盛んではあるがセキュリティ対策の専門家育成がなかなか進んでいない現状にあって、個人のスキルアップを前提とした情報システム部門のサイバーセキュリティ対策の強化には様々な制約があると想定された。
そのため、サイバーセキュリティ対策に求められる機能定義（以下、「機能定義」という）を検討していくにあたり、組織体、機能、人材及び評価の 3 つの観点から整理し、機能を定めていくこととした。

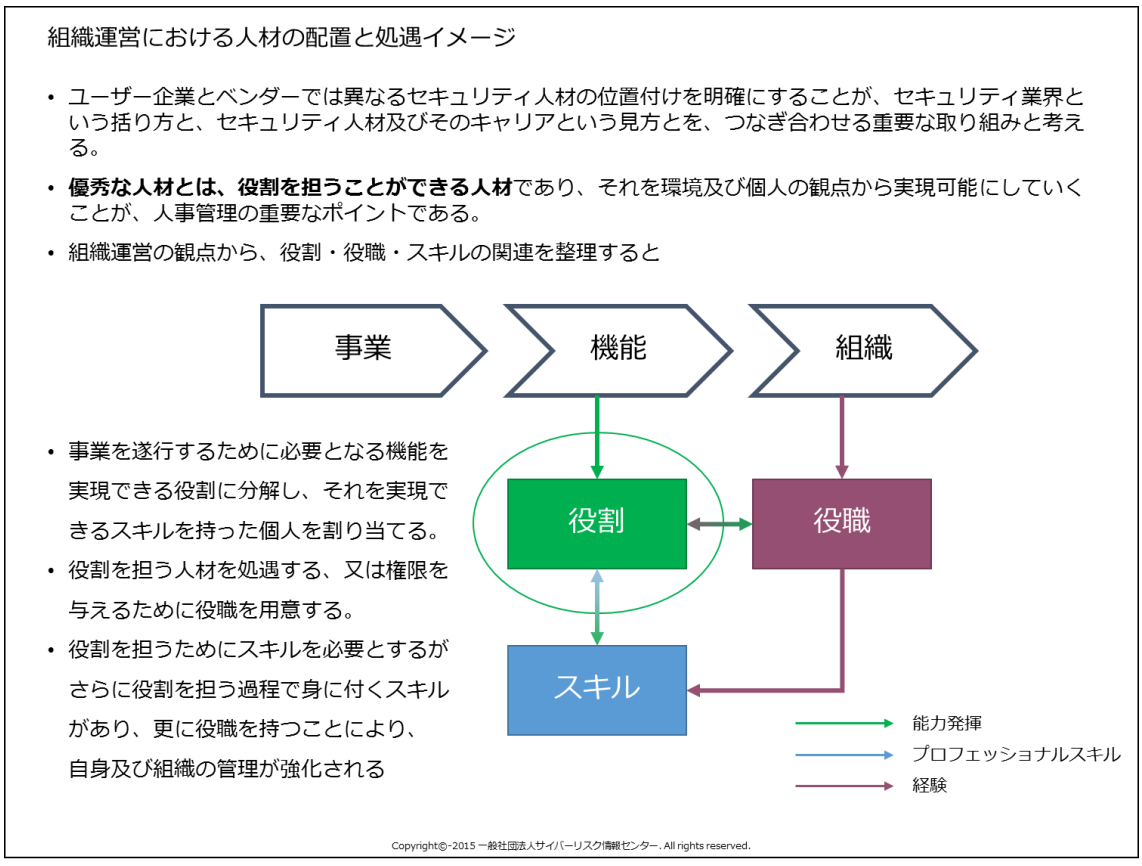
3.1.1. 第 1 回 WG における検討

第 1 回の WG において、現在のサイバーセキュリティ人材不足の改善に向けた討議の方向性の確認を行った。まずは以下 2 点について討議を進めた。

① セキュリティ専門家に何を委託し、自社として何を管理していくのか

② セキュリティ人材は引き抜くのか、育てるのか

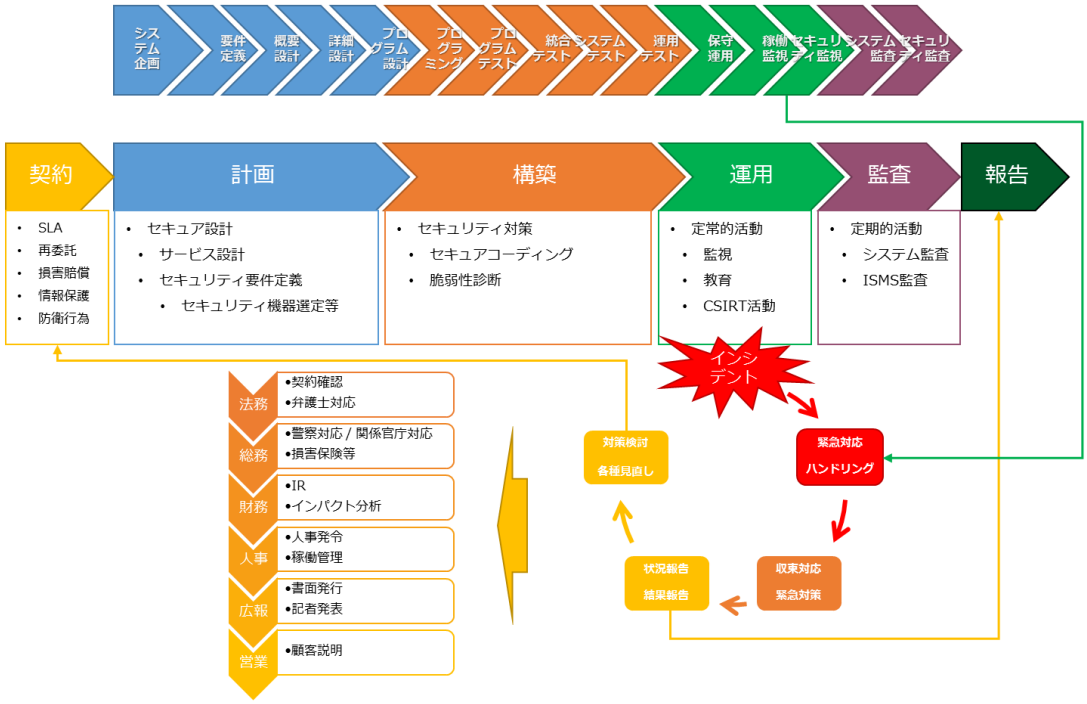
更に、本 WG における検討の範囲を絞り込むため、下記のモデルを提示し、検討の方向性が拡散しないように配慮することとした。



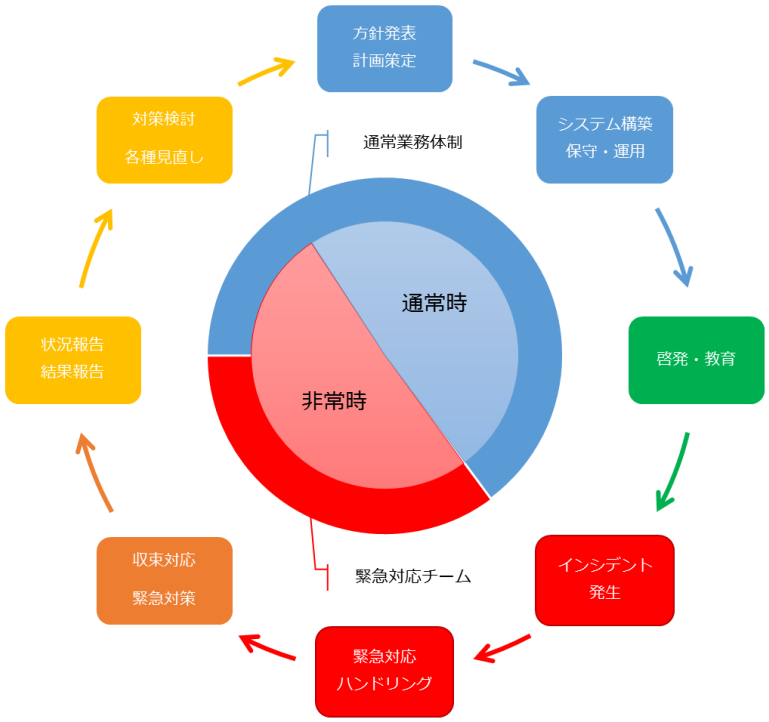
更に、本 WG 参加者が、人材育成に向けての機能定義を意識して討議できるよう、システム開発プロセス及びインシデントハンドリングプロセスのモデルを確認し、現在、自社社内ではどのような部門・部署、委託先が、サイバーセキュリティ対策に関する業務を担当しているのかを確認する機会とした。

システム開発プロセスから考える通常時と非常時の活動

- システム開発・運用プロセス



インシデントハンドリング（CSIRT活動）から考える通常時と非常時の考え方

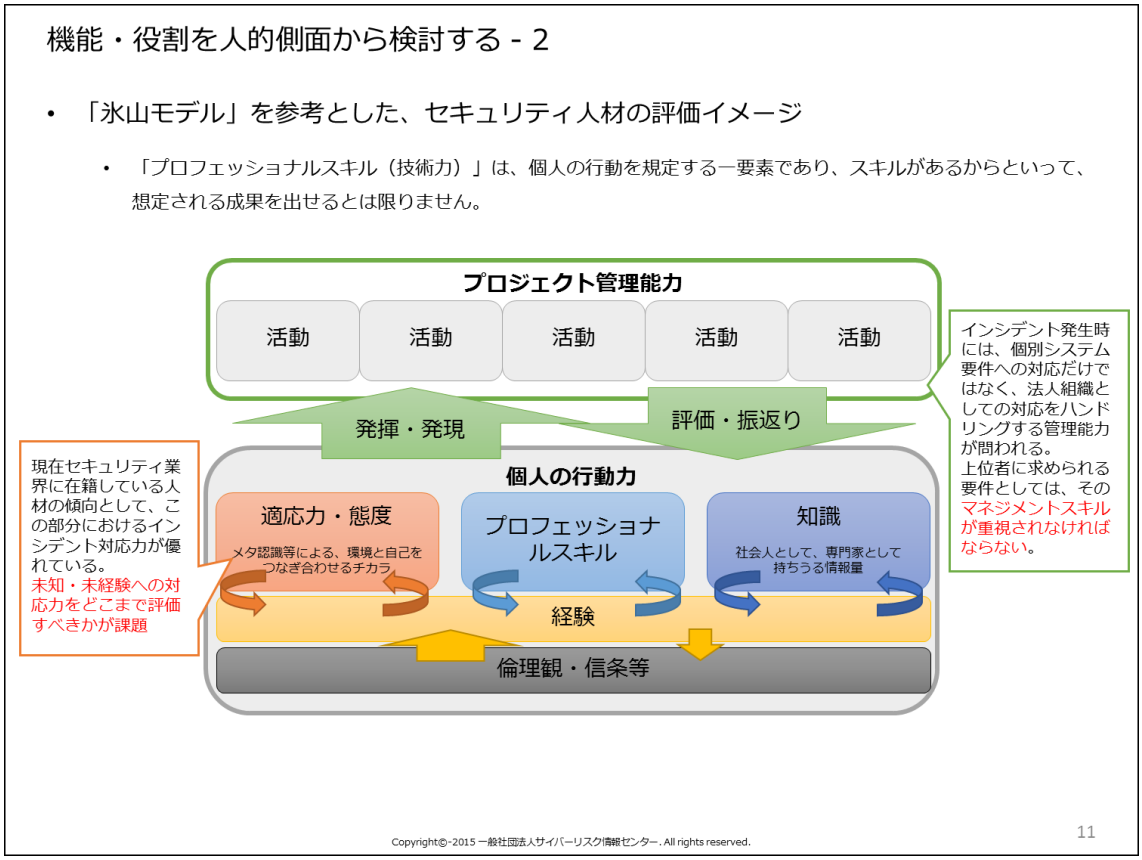


3.1.2. 第 2 回 人材定義 WG における検討

第 2 回での討議は、第 1 回の全体像の共有を経て、人材的側面、組織的側面から検討を深め、更に、内部統制に絡む全社リスクマネジメントとの関係性について確認した。

ここでは、サイバーセキュリティ人材に求められるスキルセットの検証作業に入り込んでしまうと、最終的には採用時の「募集要項」のようなものが出来上がってしまう恐れがあったため、まずは機能や役割を検討するための人的側面について確認した。

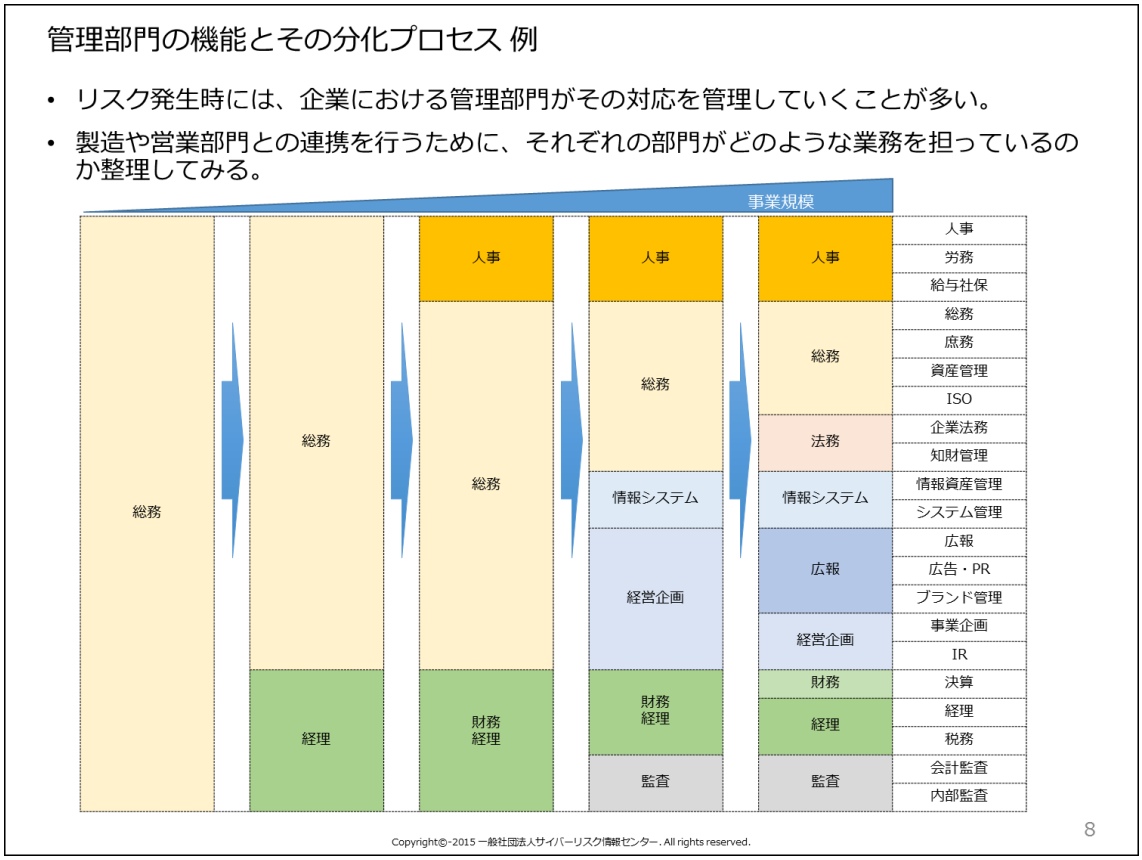
まずは、下記資料に基づき、第 1 回で確認した「機能」を定義するためには、サイバーセキュリティ対策に明るい人材像を掘り下げるのではなく、サイバーセキュリティ対策に詳しく、社内の業務に精通し、チームで業務が遂行できる人材を想定していることを再確認するものとした。



更に、情報システム部門におけるサイバーセキュリティ対策に必要となる機能を定義するにあたり、機能を担う人材を企業内だけではなく、関係会社や取引先 SI 企業、セキュリ

ティ専門事業者等との分担により実現することを模索するための機能一覧を目指すこととした。

その機能の分担を検討していくにあたり、まずは管理部門における機能分化プロセス（下図）を用いて、現在の自社の部門の在り方について振り返ることとした。



加えて、ユーザ企業においては J-SOX 対応によるリスクマネジメント委員会の機能強化及び、東日本大震災後に BCP 対策を強化している企業が多いため、既存のリスクマネジメントを実行する部門・部署を確認することにより、既存のリスクマネジメントに関する取り組みとサイバーセキュリティ対策を比較できるようにした。この検討プロセスは、サイバーセキュリティ対策が目新しいものではなく、現業の延長にあるものであるという共有に繋がった。

法令要件としてのリスクマネジメント（対応組織の運用）

- 既存の事業リスクマネジメント体制に、サイバーセキュリティ対策を組み込む
  - サイバーセキュリティに関する機能及び役割を定義するためには、社内ルールとしてその責任者及び担当範囲、発動のポイントや定期的な監査内容について定義されている必要がある。

	サイバーセキュリティ対策	情報セキュリティ管理	個人情報管理	文書管理	防火管理	労働安全衛生
規程		情報セキュリティ管理規程	個人情報取扱規程	文書管理規程	防火管理規程	労働安全衛生管理規程
担当範囲		情報システムに関するセキュリティ対策	個人情報取扱いに関する体制構築及び運用	社内にある情報・文書の取扱いに関する体制及び運用	施設・設備の防火管理に関する体制及び運用	労働安全衛生法に基づく労働環境管理体制及び運用
責任者		CIO又は情報システム部門責任者	主に人事担当役員又は人事部長	主に総務担当役員又は総務部長	主に総務担当役員又は総務部長	主に人事担当役員又は人事部長
担当者		情報システム部門担当者	個人情報取扱い部署の責任者又は指名された担当者	文書取扱い部署の責任者又は、指名された担当者	総務部門所属社員及び各拠点・フロアの担当者	人事部門所属社員及び各事業拠点で指名された担当者
運用方法		対策基準が定めてあり、業務上必要な対策を講じることを確認	運用ルールが定めてあり、業務が従っていることを確認	運用ルールが定めてあり、業務が従っていることを確認	運用ルールが定めてあり、発動条件により対応する	定期的な会合に必要となる確認を実施し、報告承認のプロセスを実施

  - ルール化することで形骸化することもあるため、機能及び役割が決定した段階で、年度における各タスクおよび必要となるトレーニングについても記載しておくことが望ましい。

法令要件としてのリスクマネジメント（対応プロセス）

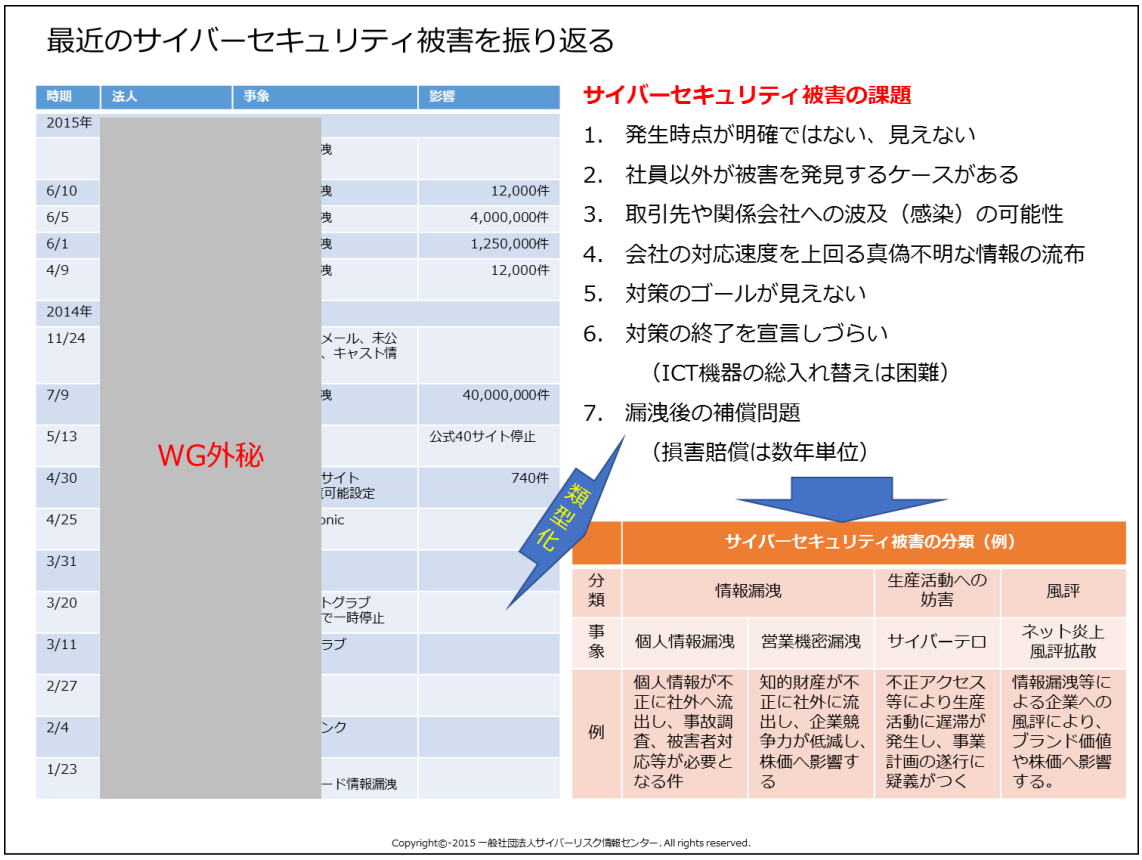
- リスクマネジメント規程（リスク管理規程）の一般的な意思決定プロセス・フロー

- 主なケース（目に見える脅威とその対応）

リスク	事象	発覚	経過	対応
信用危機	社員が顧客の免許証のコピーを持ち帰る 個人情報1名の漏洩	ネットで炎上していることを社員が知り、会社へ報告	Twitterで炎上。 株式に売りが入り時価総額460億円下落	顧客への謝罪 広報対応
財政危機	取引先の倒産	取引銀行から注意喚起 営業担当が確認訪問	発注済み原料の停滞 入金予定金額の未入金	取引先変更 貸倒引当金の適用
人的危機	海外拠点でストライキによる社員の監禁	現地大使館から連絡	本社スタッフを派遣し、解放交渉	操業再開に向けてベアを含む労働争議
	台風接近による河川の増水による拠点浸水	気象庁による警報 拠点社員からの報告	社員の帰宅・自宅待機 数名の社員による泊込み	浸水被害の報告 取引先への説明
外部危機	海外拠点周辺での反日デモによる操業停止	現地大使館から連絡 現地社員から連絡	社員の自宅待機 サプライチェーンの見直し	代替拠点の稼働率向上 株主説明
	生産拠点に対する事業活動への妨害活動	• 設備への破壊工作 • 異物混入等の問い合わせ	• 警察による事態収拾 • 警察と消費者庁と連携した事態把握	• 記者会見・プレスリリース • 謝罪会見 • 再発防止策の発表
その他				

次回 WG より実際にサイバーセキュリティ対策に求められる「機能定義」を討議していくため、まずは、サイバーセキュリティ事件・事故事例を振り返りながら、なぜ今サイバーセキュリティ人材が不足しているのか、なぜサイバーセキュリティ対策に予算を割くことが難しいのかといった点について共有した。

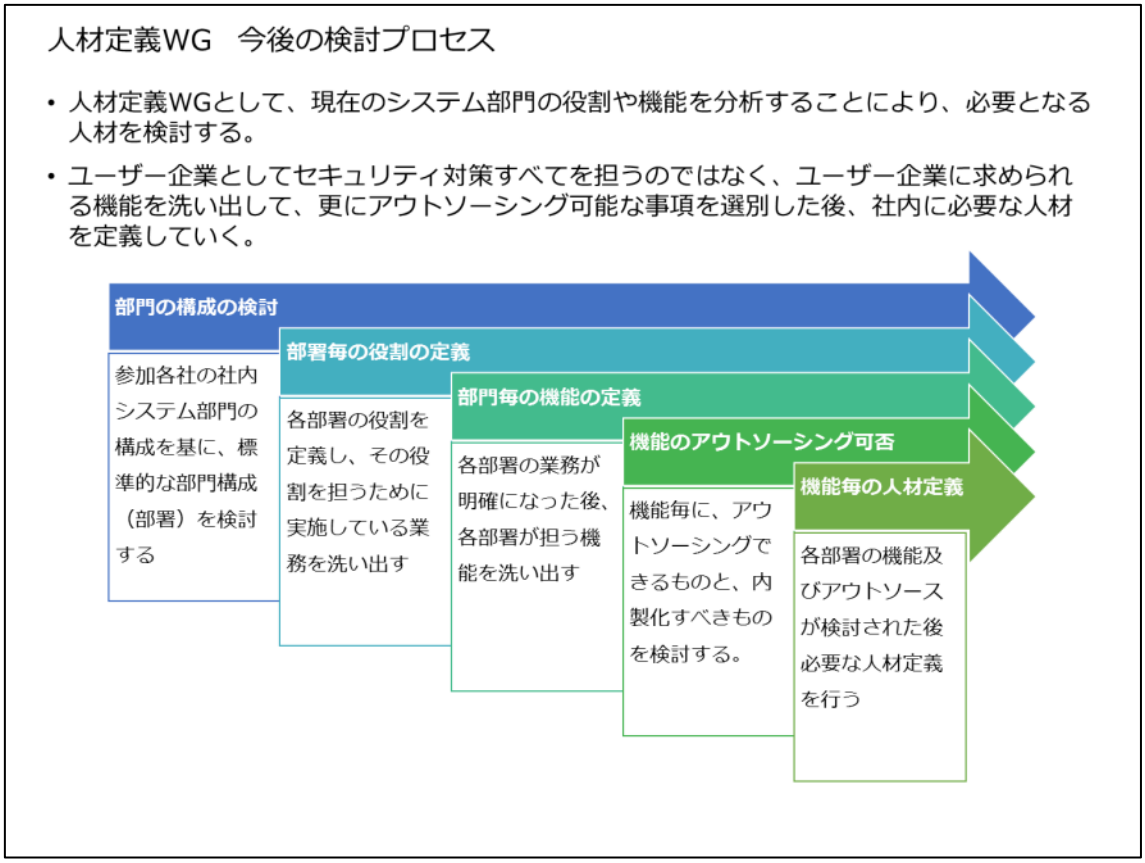
サイバーセキュリティ被害の類型を共有しながら、サイバーセキュリティ対策の方向性すなわち必要となる機能毎の活動の前提条件について討議確認をした。



サイバーセキュリティ対策をどの被害の段階において、誰が、どのような権限で、どこまで対処すべきかを検討するため、サイバーセキュリティ被害の分類を 4 つに分け、それぞれにどのように対応していくべきかを自社に振り返り検討して頂くことで、必要となる機能についての検証を進めることとした。

3.1.3. 第 3 回 人材定義 WG における検討

第 3 回では、人材定義 WG において確認してきたサイバーセキュリティ人材の定義における課題や背景に基づき、今後の検討プロセスを共有することとした。



更に、機能定義における粒度を模索するため、簡易的な整理軸を定めることとした。討議の中で、ユーザ企業各社の情報システムの構築運用の体制には大きな差があり、その中でサイバーセキュリティ対策に求められる機能定義を共通化していくことが重要であるということを、今後の討議の重要事項として提起した。

加えて、アウトソーシング（自社以外への委託）を行う分野・業務に関する分析を進めることを目的として、検討例を提示し、検証を進めた。

機能一覧 アウトプット 検討例

- サイバーセキュリティ人材育成の基準となる、ITシステム部門における機能の定義を検討していくたたき台の例

	大分類	中分類	小分類	機能	社内対応	アウトソース	部署名例
1	戦略・企画	事業戦略	• IT投資 • 人員計画 • セキュリティ方針		○	×	
2		システム企画	• システム導入計画 • システム仕様計画		○	△	
3	調達	システム調達	• システム調達 • IT資産管理		○	○	
		ベンダー調達	• ベンダー調達・管理		○	△	
4	構築	実装	• プロジェクト管理		○	○	
5		品質管理	• 開発テスト		○	○	
6	運用	運用	• システム運用 • アクセス権管理 • バージョンテスト • DR	• 機器管理 • システム管理 • アクセス管理 • DR対策	○	△	
7		監視	• ネットワーク監視 • セキュリティ監視		○	○	
8		インシデント ハンドリング	• 予兆監視、トリアージ • 危機対応		○	△	
9	ユーザー サポート		• ユーザーサポート • 教育		○	△	
10	監査		• システム監査 • セキュリティ監査		○	△	

機能のアウトソーシング可否の検討例

- セキュリティに関する「機能」を洗い出す過程で、ユーザー企業におけるセキュリティ対策をどこまで自社内の人材で対応していくべきかを検討するためには、既にどのような業務をアウトソーシングしているのかを検討しておくことが重要。

【アウトソーシングの例】

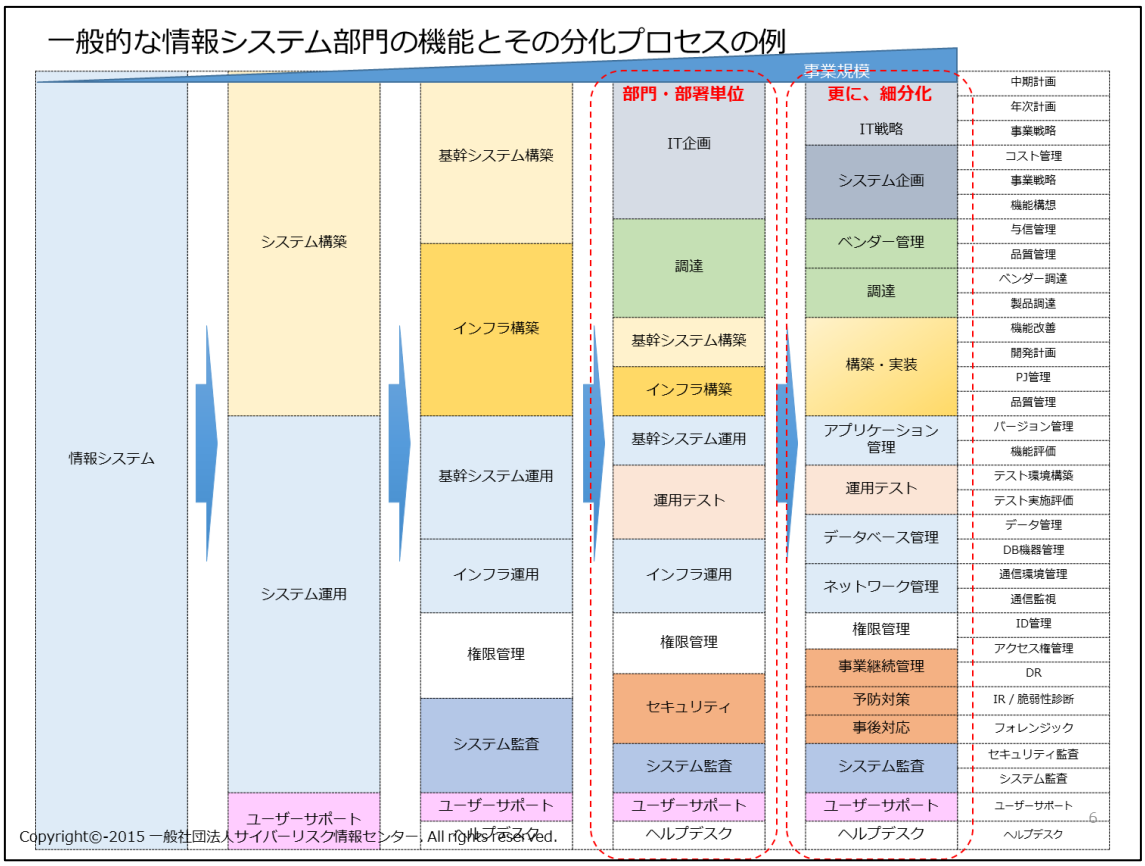
- 調達部門
  - 信用調査
- システム運用
  - 基幹システム運用
  - ネットワーク運用
- ネットワーク監視
  - SOC
- 脆弱性診断
  - WEB脆弱性診断
  - ネットワーク脆弱性診断
  - スマホアプリ脆弱性診断
- フォレンジックス

【委託内容の例】

- 調達部門
  - 信用調査会社のランキングを社内基準に適用
- システム運用
  - 開発会社へバージョン管理を委託
  - トラフィックや稼働率の監視を委託
- ネットワーク監視
  - インシデント管理やログ解析、レポートを委託
- 脆弱性診断
  - 基幹システムのカットオーバー前診断を委託
  - 外部接続環境の診断を委託
  - 顧客向けアプリの診断を委託
- フォレンジックス
  - 訴訟対応やデータ復旧等を委託

3.1.4. 第 4 回 人材定義 WG について

第 4 回では、前回の WG により共有された、サイバーセキュリティ対策に求められる機能定義を進める上で重要となる、ユーザ企業における共通モデルの策定に向けて、これまで管理部門の機能分化プロセスとして共有していたものから、情報システム部門における組織の成立からの機能分化プロセスについて確認を行うこととした。



特に、本機能分化プロセスは、日本企業における情報システム部門の発展を前提として例示したが、同時に、海外の基準も俯瞰することにより、機能定義がグローバル展開している場合であっても共通言語として活用できることを想定し、討議を進めた。

ここで活用した海外における基準は以下の 2 つによる。
Framework for Improving Critical Infrastructure Cybersecurity Version 1.0（NIST 発行）
the National Initiative for Cybersecurity Education（通称 NICE）

NIST　サイバーセキュリティフレームワーク

機能の一意の識別子	機能	カテゴリーの一意の識別子	カテゴリー	機能分化例における部門の例
ID	特定	ID.AM	資産管理	調達
		ID.BE	ビジネス環境	IT企画
		ID.GV	ガバナンス	IT企画
		ID.RA	リスクマネジメント	各部門
		ID.RM	リスク管理戦略	IT企画
PR	防御	PR.AC	アクセス制御	権限管理・基幹システム運用
		PR.AT	意識向上およびトレーニング	ユーザーサポート
		PR.DS	データセキュリティ	基幹システム運用・インフラ運用
		PR.IP	情報を保護するためのプロセスおよび手順	IT企画・セキュリティ・監査
		PR.MA	保守	基幹システム運用・インフラ運用
		PR.PT	保護技術	基幹システム運用・インフラ運用
DE	検知	DE.AE	異常とイベント	セキュリティ・インフラ運用
		DE.CM	セキュリティの継続的なモニタリング	セキュリティ・インフラ運用
		DE.DP	検知プロセス	セキュリティ・インフラ運用
RS	対応	RS.RP	対応計画の作成	セキュリティ
		RS.CO	伝達	セキュリティ
		RS.AN	分析	セキュリティ
		RS.MI	提言	セキュリティ・監査
		RS.IM	改善	セキュリティ・IT企画
RC	復旧	RC.RP	復旧計画の作成	セキュリティ・IT企画
		RC.IM	改善	セキュリティ・IT企画
		RC.CO	伝達	IT企画・監査・ユーザーサポート

NICE WORKFORCE / The National Cybersecurity Framework

1	**Security Provision**	Information Assurance Compliance	Software Assurance and Security Engineering	Systems Development	Systems Requirements Planning	System Security Architecture	Technology Research and Development	Test and Evaluation
	セキュリティ(概念の)提供	情報保証コンプライアンス	ソフトウェア保証とエンジニアリング	システム開発	システム要件計画	システム セキュリティ アーキテクチャ	技術研究開発	試験と評価
2	**Operate and Maintain**	Customer & Tech Support	Data Administration	Knowledge Management	Network Services	System Administration	Systems Security Analysis	
	運用・保守	カスタマーサポート & 技術サポート	データ アドミニストレーション	ナレッジ マネジメント	ネットワークサービス	システム アドミニストレーション	システム セキュリティ分析	
3	**Protect and defend**	Computer Network Defense（CND）Analysis	CND Infrastructure Support	Incident Response	Vulnerability Assessment & Management			
	守備・防衛	コンピューター ネットワーク防御分析	コンピューターネット ワーク防御インフラ支援	インシデント レスポンス	脆弱性アセスメントと管理			
4	**Investigate**	Digital Forensics	Investigation					
	捜査	デジタルフォレンジック	捜査					
5	**Collect and Operate**	Collection Operations	Cyber Operations	Cyber Operational Planning				
	運用・情報収集	情報収集オペレーション	サイバーオペレーション	サイバーオペレーション計画				
6	**Analyze**	All-source Intelligence	Exploitation Analysis	Targets	Cyber Threat Analysis			
	分析	全情報源の諜報活動	エクスプロイト分析	ターゲット	脅威分析			
7	**Oversight and Development**	Education & Training	Information Systems Security Operations	Legal Advice & Advocacy	Security Program Management（CISO）	Strategic Planning & Policy Development		
	監督と開発	教育と訓練	情報システム セキュリティオペレーション	法的助言と弁護	セキュリティ プログラム管理	戦略的な計画とポリシー策定		

NICEは、セキュリティから見たフレームワーク

3～6にCSIRT活動を規定しているため、セキュア設計やセキュア運用等については大きな単位でまとめられている。

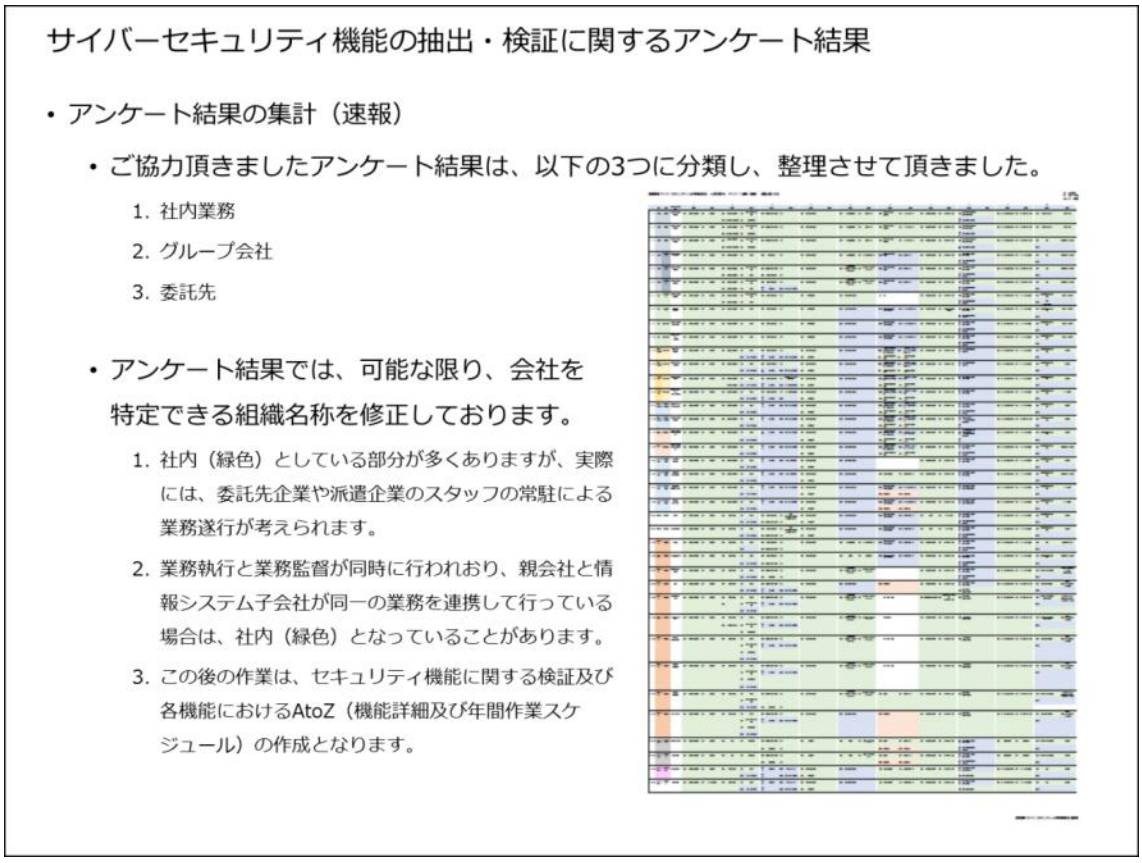
10

3.1.5. 第 5 回～第 7 回 人材定義 WG について

第 5 回から第 7 回における本 WG の討議は、ユーザ企業におけるサイバーセキュリティ対策に求められる機能定義に、共通モデルを策定するためのアンケートを実施した。
これまで、ユーザ企業におけるサイバーセキュリティ対策の機能定義を進めてきたが、実際に、各社の実情とどの程度整合性があり、また乖離しているのかについて確認を行うこととした。

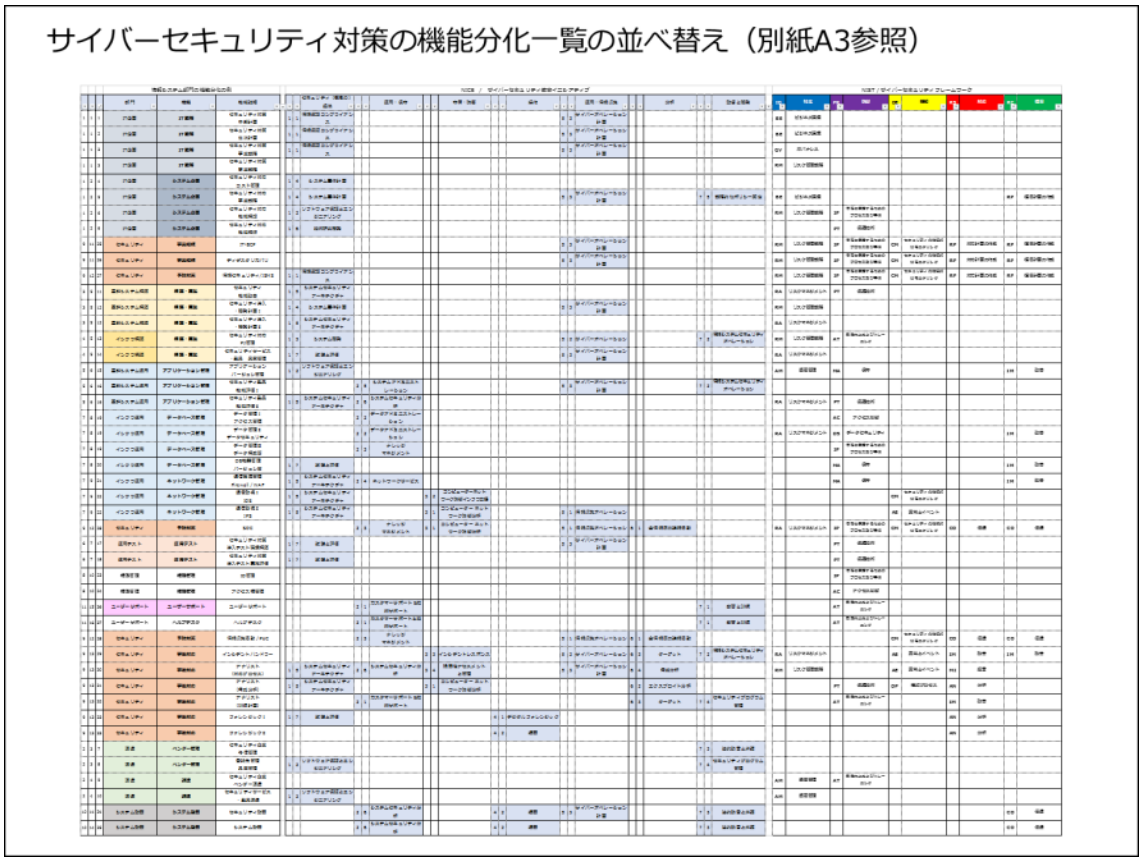
アンケートの目的は 2 つあり、1 つめは、WG 参加企業におけるセキュリティ対策がどのような単位で分担されているのか、2 つめは、社内対応と社外（子会社や専門事業者等）の分担はどのように行われているのか、を確認することとした。

このアンケートにより、人材の定義の前に、まずはユーザ企業がどのようなサイバーセキュリティ対策の体制を構築し、専門事業者を活用し、また非 IT 部門との連携を進めているのかについて確認することで、サイバーセキュリティ対策に必要となる機能定義に対する共通認識を醸成することとした。



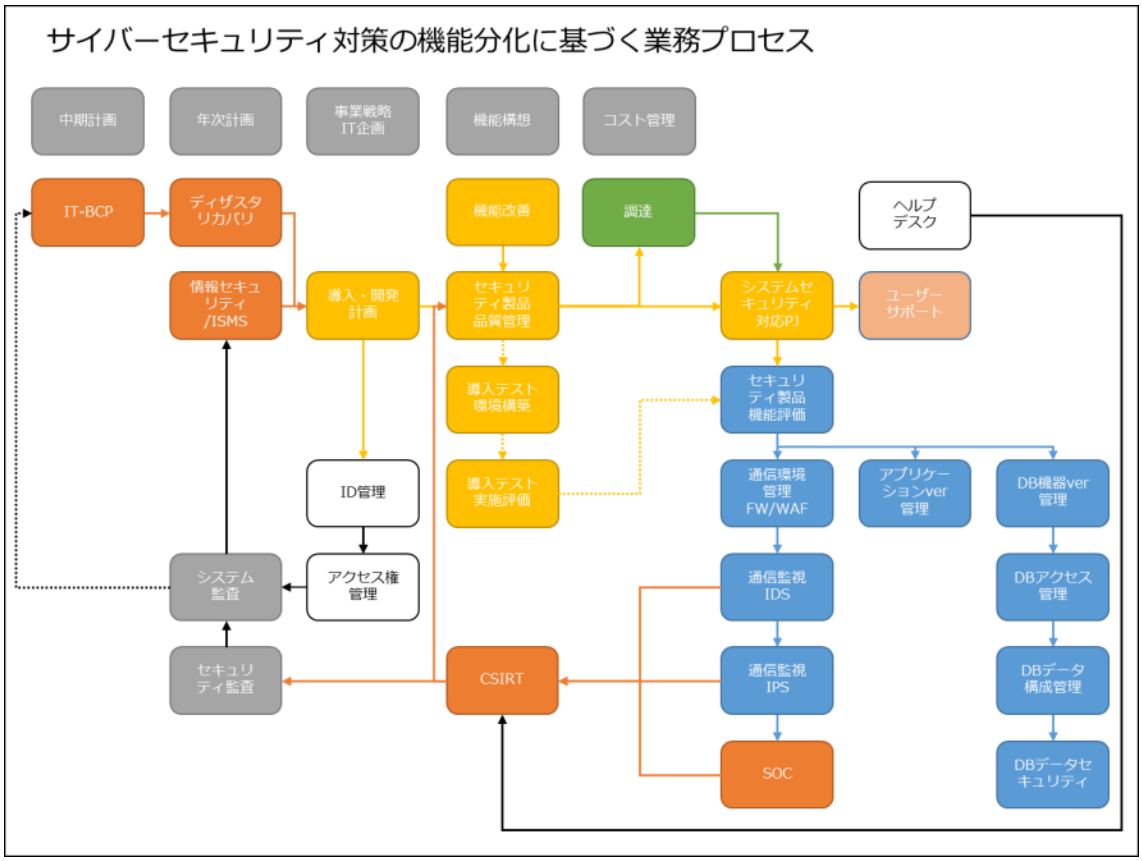
3.1.6. 第 8 回 人材定義 WG

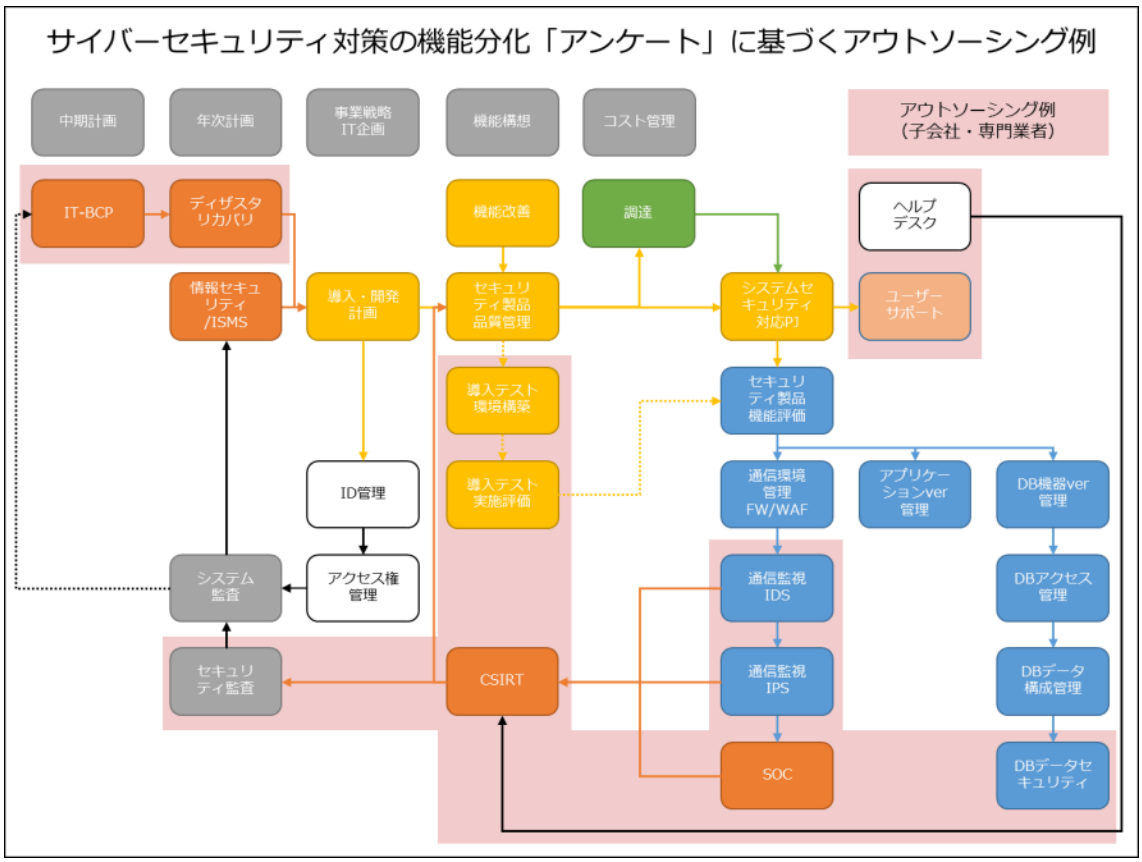
本 WG においては、これまでの討議により策定された「機能定義」案に対して、アンケート結果に基づく機能の配列の修正を実施した。



更に、機能定義の一覧を前提とし、ユーザ企業での運用に対応できるよう、サイバーセキュリティ対策の機能一覧を土台としたサイバーセキュリティ対策業務のプロセスモデルを導き出し、兼務を想定した必要となる機能の繋がりを明示することとした。

加えて、機能別に対するアウトソーシングの実施例及び適用可能性を明示し、ユーザ企業の社員が役割として担うべき機能と、管理監督を主体としてセキュリティ専門事業者及び ICT 事業者へアウトソーシング可能であると判断できるものを整理した。

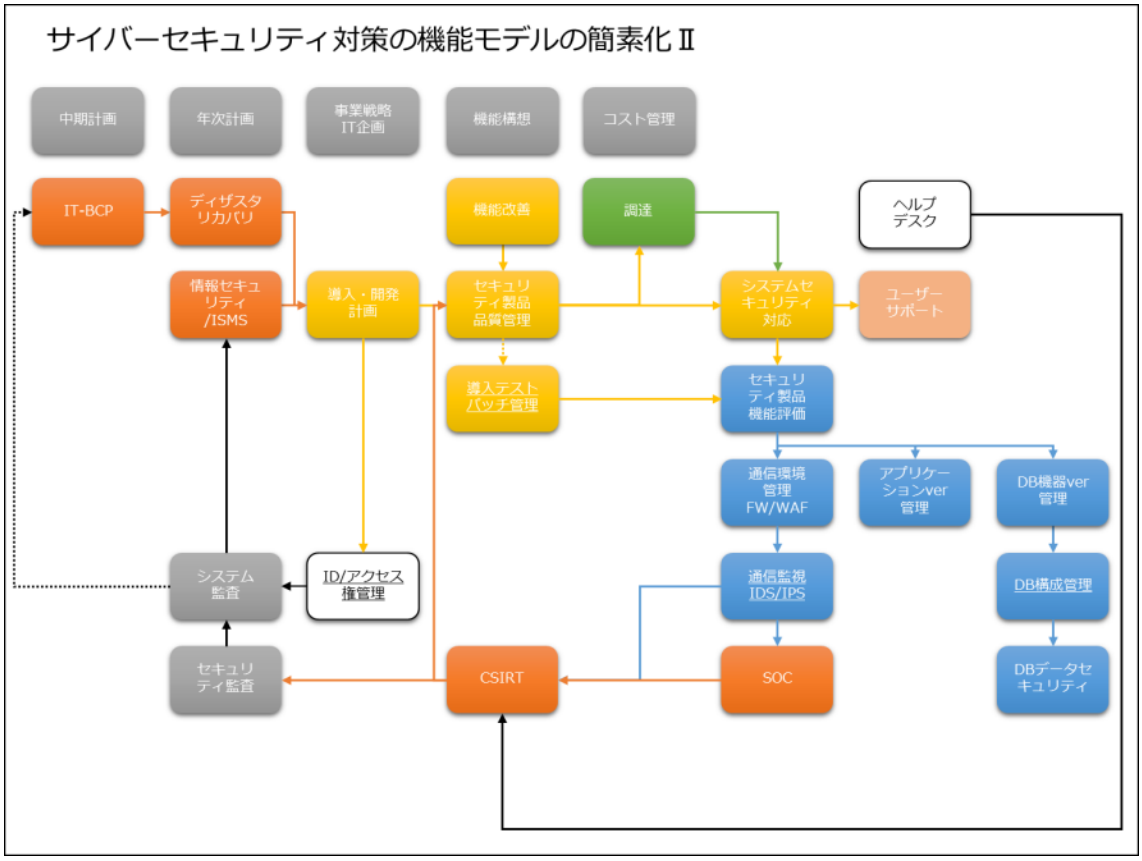

サイバーセキュリティ対策の機能分化に基づく業務プロセス
中期計画
年次計画
事業戦略
IT企画
機能構想
コスト管理
IT-BCP
ディザスタ
リカバリ
機能改善
調達
ヘルプ
デスク
情報セキュ
リティ
/ISMS
導入・開発
計画
セキュリ
ティ製品
品質管理
システムセ
キュリティ
対応PJ
ユーザー
サポート
導入テスト
環境構築
セキュリ
ティ製品
機能評価
ID管理
導入テスト
実施評価
通信環境
管理
FW/WAF
アプリケー
ションver
管理
DB機器ver
管理
システム
監査
アクセス権
管理
通信監視
IDS
DBアクセス
管理
セキュリ
ティ監査
CSIRT
通信監視
IPS
DBデータ
構成管理
SOC
DBデータセ
キュリティ


サイバーセキュリティ対策の機能分化「アンケート」に基づくアウトソーシング例
中期計画
年次計画
事業戦略
IT企画
機能構想
コスト管理
アウトソーシング例
（子会社・専門業者）
IT-BCP
ディザスタ
リカバリ
機能改善
調達
ヘルプ
デスク
情報セキュ
リティ
/ISMS
導入・開発
計画
セキュリ
ティ製品
品質管理
システムセ
キュリティ
対応PJ
ユーザー
サポート
導入テスト
環境構築
セキュリ
ティ製品
機能評価
ID管理
導入テスト
実施評価
通信環境
管理
FW/WAF
アプリケー
ションver
管理
DB機器ver
管理
システム
監査
アクセス権
管理
通信監視
IDS
DBアクセス
管理
セキュリ
ティ監査
CSIRT
通信監視
IPS
DBデータ
構成管理
SOC
DBデータセ
キュリティ

3.1.7. 第 9 回 人材定義 WG

本 WG では、前回策定された「機能定義」一覧に基づく業務プロセスモデルに対する機能粒度の調整及びアウトソーシング業務の拡大を念頭に、更に討議を深めることとした。

ここでの議論は、ユーザ企業の情報システム部門が日々意識しているサイバーセキュリティ対策と「機能定義」や業務プロセスモデルとが整合しているかの確認を行い、各機能を社内外のいずれかの人材が担うとなった場合に過剰な人員構成等にならない、無理のない対応体制が構築できることを確認するためのものとした。

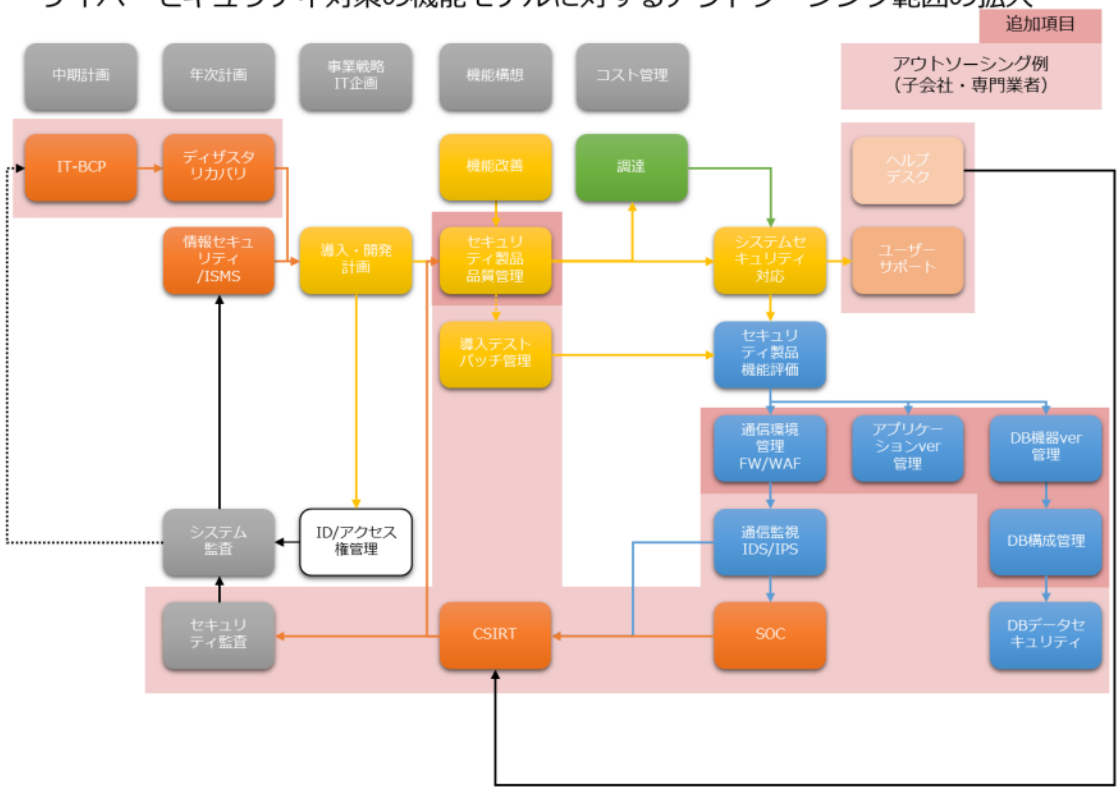


特に、通信監視及びデータベースセキュリティの機能が、サイバーセキュリティフレームワークの分類に影響を受けすぎていることを確認し、機能を統合することとした。

更に、アウトソーシングを委託する範囲を見直し、幅広くセキュリティ専門事業者及び ICT 事業者のスキルを活用できるようにするため、サイバーセキュリティ対策の実施主体と管理監督者の分離が必要との意見を受け、合意した。

最後に、サイバーセキュリティ人材の定義と採用の考え方について事務局より説明し、セキュリティ専門技術者とサイバーセキュリティ人材の間にある壁（差分）の取扱いについて、障害ではなく乗り越えていくべき重点課題として認識するよう意見を受け、修正し合意することとした。

サイバーセキュリティ対策の機能モデルに対するアウトソーシング範囲の拡大



サイバーセキュリティ人材の定義と採用

- サイバーセキュリティ人材へのキャリアパスを整理する
  - 既存のIT技術者やセキュリティ専門技術者を**サイバーセキュリティ人材**とするには、**乗り越える壁**が存在している。

項目	IT技術者	サイバーセキュリティ人材	セキュリティ専門技術者
日常業務	運用業務が優先であり、セキュリティ対策への従事は企業により違いが大きい。	体系的な資格や教材が少なく、国内では希少な技術や、幅広い取組（多層防御等）を追求しているケースが多い。	セキュリティ製品導入経験が主で業務プロセス全体に対する安全・安心を学ぶ機会が少ない。
インシデント対応	セキュリティ対策とトラブル対応の差別化にあまり意味がない。	課題解決には、導入や運用を担当するベンダーや、情報システム部門の協力が不可欠	顧客対応として製品技術に関する対策を中心に業務を遂行する。
評価基準	セキュリティスキルは、IT技術者の業績評価と関係がない。	人材の明確な評価基準がない。	細分化されたセキュリティ対策のスキルセットに依拠している。

  - ※ここでのセキュリティ専門技術者は、これまでの情報セキュリティ対策及びセキュリティ製品導入技術者を指す。
- スキルセットに基づくサイバーセキュリティ人材の選別の課題
  - ユーザー企業が情報システム部門のメンバーとして、サイバーセキュリティ（サイバー攻撃対策等）に関するスキルを持った人材の採用を希望する場合、採用要件はサイバーセキュリティ対策ではあるが、現在転職市場に存在する人材はIT技術者かセキュリティ専門技術者であり、応募段階の書類選考ではサイバーセキュリティに関する業務を担えるのかが未知数に「見える」ことが多い。

3.2. 検証結果

3.2.1. 人事制度からの検証

本 WG の討議を通じて、サイバーセキュリティ人材の採用や育成を考える際には、業務ユーザ企業における人事制度が課題となる可能性があることが想定された。

それは、育成の観点から、定期人事異動による長期的キャリア形成や情報システム部門の中でも多岐に渡る業務を兼務することがあることにより、日々高度化するサイバーセキュリティ対策に対処できる人材を育成していけるのかについて課題が残った。
更に、採用の観点からも、新卒採用はコミュニケーションスキル重視による部門を限定しない採用が行われ、中途採用においても書類選考及び人事面接では非 ICT 技術者による選考が行われていることから、スキルセットに依存した採用の前に、高度スキルを持つ技術者が振り落されている可能性を共有した。

これらの課題を解決する一助として、採用及び育成における課題を解決するために、コミュニケーションスキルだけでも、高度スキルだけでもない人材育成モデル（氷山モデルを参照）を整理、共有することとした。翻って SI 企業においてもシステム構築や運用保守に従事する人員が重視されており、かつ人月契約による常駐型プロジェクトが多いことから、セキュリティ対策のために人材育成を強化、実施することが困難な状況にあると考えられる。

3.2.2. 機能分化プロセスからの検討

人事制度からの検討にある通り、サイバーセキュリティ対策の高度人材を採用育成することが今後のテーマではあるものの、既にサイバーリスクにさらされている現状に対応するためには、サイバーセキュリティ人材の育成や採用だけではなく、アウトソーシングを含む業務の分担による対策の実効性が求められていることを確認した。

特に、ユーザ企業における業種業界の違いによる部分は今後の検討材料として残すこととし、各社共通に求められる機能のモデルを抽出し、底上げを図ることが重要であることを共有し、そのモデルを「機能定義」として定めることとした。またユーザー企業に適合する基準となることを想定し、更には海外拠点でも活用できるモデルとするため、米国で採用されている基準を同時に確認することとした。

これらのプロセスを経て策定した情報システム部門の業務分担とサイバーセキュリティ対策機能の一覧の有効性を担保するため、参加企業へのアンケートを実施し、どの機能がどの部門・部署により対応されているのかを明確し、加えて、情報システム子会社や外注先への委託状況を確認することにより、サイバーセキュリティ対策の標準的な機能分化モデルを策定するに至った。

3.3. 人材定義

本 WG では、人材の定義については今後の検討課題として残すこととした。現状の課題として、人材の定義を行っても、ICT 業界において既存に公開されているスキルセットを満たす人材がそもそも不足している状況を踏まえて、まずユーザ企業としてサイバーセキュリティ対策について何をしなければならないのかを討議することを優先した。

更に、属人的なスキルセットに依拠したサイバーセキュリティ対策を先に考えるよりも、日本企業らしい「共助」の観点から、グループ企業やサプライチェーンでつながる企業とのサイバーセキュリティ体制構築がより重視されていることから、機能を分担したセキュリティレベル向上に向けた指標作り（「機能定義」の策定）を優先させることとした。

結果として、導き出されたサイバーセキュリティ対策に求められる機能定義を実現できる人材像を策定することが重要であると考えられたが、人材に求められるスキルセットは、適宜公開される他団体等の人材定義資料を確認し、今後、採用が可能かを検討することとする。

4. おわりに（今後の課題）

個人が保有するスキルを高度化するという取り組みは、セキュリティ人材が潤沢に存在する場合には有効な手段ではあるが、既に IPA が発表している通りセキュリティ業界の人材不足が大きな課題になっている現状においては、ユーザ企業がそれぞれバラバラに高度セキュリティ人材の採用と育成を目指すことは現実的ではないと考えられる。

これらの課題は日々サイバー攻撃に対処しているセキュリティ専門事業者、高度セキュリティ人材を雇用している SI 企業において議論されるべきものであり、ユーザ企業の情報システム部門においては、そのような高度なスキルを持つセキュリティ専門事業者及びセキュリティ専門技術者をいかに効率的かつ効果的に活用し、企業経営を守っていくのかに

焦点を合わせていくことが望ましい。

さらに、今回は「情報システム」に対するサイバーセキュリティ対策に必要となる機能の定義を行ったが、実際には、これまでの議論を通じて、ICT 利用環境におけるセキュリティ対策の範囲は以下の通りと考えられ、今後議論を深めていく必要があると考えられる。

① 情報システムのセキュリティ
② 生産活動や制御プログラムのセキュリティ
③ 製品、製品開発のセキュリティ
④ インシデントハンドリング（CSIRT）

これらの取り組みに対して、それぞれのセキュリティ機能が存在し、かつ担うべき人材のスキルレベルの高度化及び、対策を実施する組織やチームにおける階層・職位等の検討が想定される。

今後は、機能定義により定められた機能を担える人材を育成する教育プログラムや、それぞれの機能に求められる作業要件について検討していくことと同時に、他の ICT 利用環境におけるセキュリティ対策についても議論を進めたい。

最後に、今後の議論に向け、想定している課題・仮説を以下に述べる。

4.1. 人材育成プログラムの策定と高度化

本 WG における活動を通じて、ユーザ企業におけるサイバーセキュリティ対策に必要となる人材の定義は、今後継続検討すべき課題としたが、同時に、先に述べたサイバーセキュリティ人材育成のエコシステムを踏まえ、産学官が連携した、実効性のある人材育成プログラムを策定していく必要があると考えられる。

それは、サイバーセキュリティ対策を新しい取り組みとして考えるのではなく、既存の情報セキュリティ対策において実践されてきた日本国内の様々な教育プログラムを選定し、「機能定義」により分類された業務に対して能力向上を図るための、複数の教育講座を組合せた、体系的なプログラムの立案が重要になると考えている。

更に、IPA が 2013 年に発表したセキュリティ人材不足に関する資料において、当時はあまり積極的に取り上げられていなかったが、現在活躍する高度セキュリティ人材へのヒアリング結果が重要な事実を示唆していると考えられる。この中では高度セキュリティ人材

が現在のポジションに到達する過程において、他の組織に属する高度セキュリティ人材との直接的な交流や情報交換の場を活用したことが例示されており、日々様々な業務に対応する情報システム部門の社員や、常駐先で 1 つの開発環境や特定の開発言語に縛られ人月稼働のため有給休暇すら取りづらい状況にある IT エンジニアがこのような「刺激を受ける場」をいかに活用できるかが重要なテーマになると考えられる。

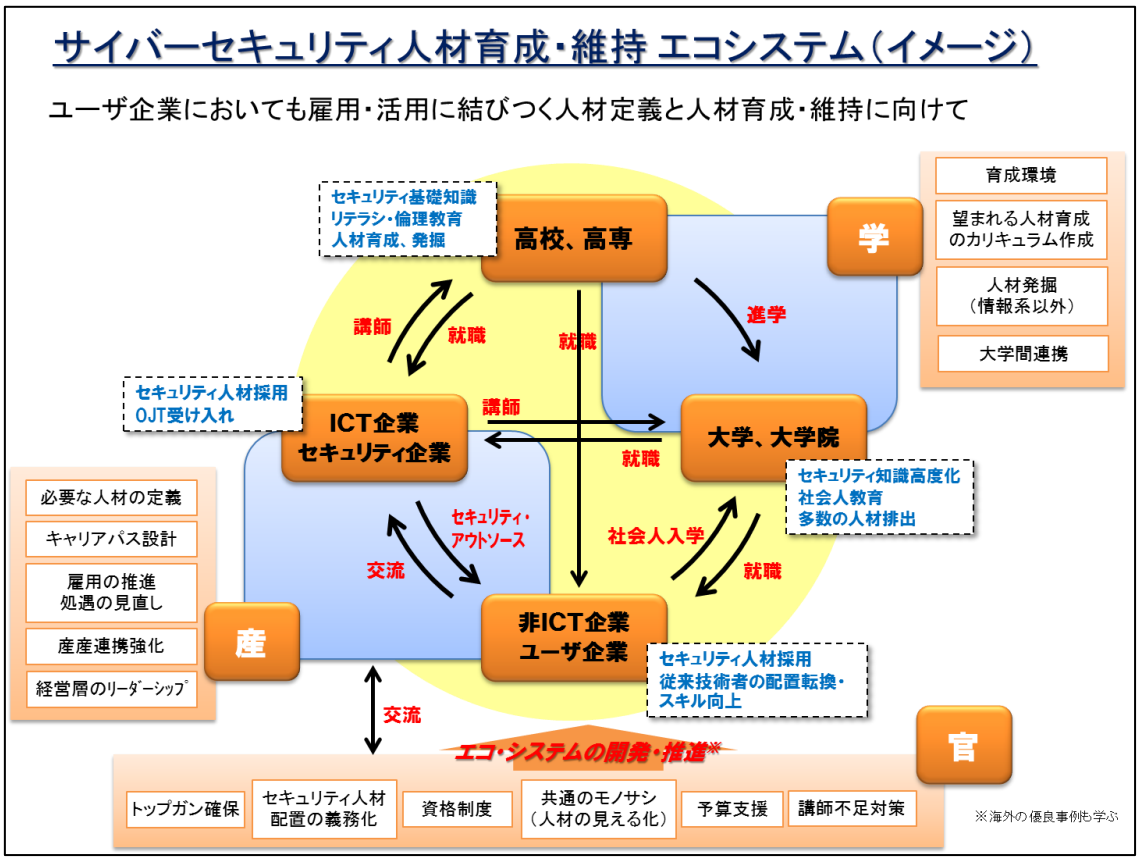
4.2. 作業要件とスケジュール分析

「機能定義」の一覧には、作業要件を例示することとしたが、更に、この作業要件をより効率的に運用するためには、それぞれの作業がいつ発生し、どのように展開し、更に何をもって完了とするものなのかを定義することが望まれる。

これは、ユーザ企業における定期人事異動等に伴う新任者のスキル向上のプロセスの効率化及び、同、企業としてのサイバーセキュリティ対策のレベルを低下させないための歯止めとしての役割を担う指標としての策定を想定しており、人材育成の取り組みを俯瞰するための道具としても活用できるのではないかと考えている。

今回の期間においては詳細を検討するところまでは至らなかったが、企業経営におけるサイバーセキュリティ対策に求められる機能一覧、作業要件と、そのスケジュール感が事前に把握できることにより、企業のサイバーセキュリティ対策の底上げに寄与するものと考えている。

サイバーセキュリティ人材育成のエコシステム（イメージ）



5. Appendix

機能定義と NICE・NIST（別紙 2「機能定義と NICE・NIST」参照）