「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 別紙 WG 活動報告

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（別紙）について

本報告書（別紙）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」）の各 WG（ワーキンググループ）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（別紙）です。

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. 活動経過

本検討会は、第二期の活動を 2016 年 10 月～2018 年 9 月までの 2 年間と定めた。

第二期では、活動開始時期から掲げている「信頼の輪」を醸成していくため、以下の活動等を通じて、日本のサイバーセキュリティ人材育成に向けた様々な活動を進めている。

- ✓ *CISO クラスが集まる「トップ層会合」の開催（2016 年 10 月）*
- ✓ *サイバーセキュリティ戦略本部（座長：内閣官房長官）発表資料による「人材定義リファレンス」の引用*
- ✓ *検討会メンバー間における「情報共有（脅威情報、対策状況、勉強会等）」*
- ✓ *大学・大学院等に「寄付講座」を行っている会員企業による産学連携の推進*

また第二期では、変化の速いサイバーセキュリティ動向に対応すべく活動の自由度を高めていくため、コンソーシアム化として法人格への移行を模索することとなった。

実際には 2017 年 4 月より検討会は一般社団法人サイバーリスク情報センターの一組織となり、国内外の様々な情報に触れる機会が提供されている。

1.1 目標

本検討会は、経団連の提言を受けて発足し、2 年が経過した。2020 年東京オリンピック・パラリンピックの開催も迫り、経済産業省が示すセキュリティ人材不足に対して、実践的な人材育成と雇用の重要性を認識し、共有している。

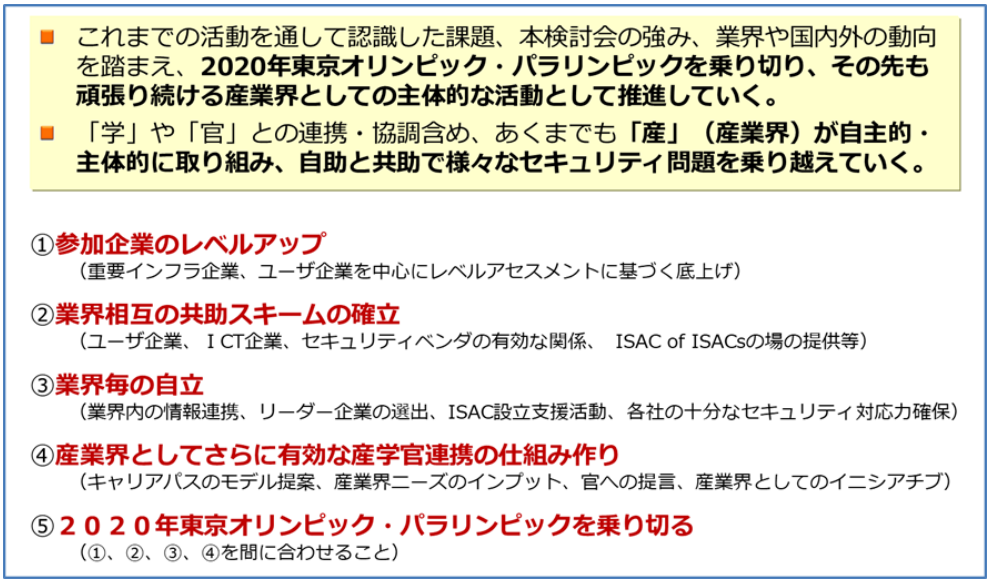

図 1-1 検討会の目標

1.2 会議体

本検討会は、先の目標の実現に向けて、5 つの WG 活動を置き、人材定義及び人材育成のあるべき姿を描き、判断の基準となる情報の共有や、次世代のサイバーセキュリティ人材を育成するための礎となる高等専門学校、大学・大学院への育成支援等を視野に入れて活動している。

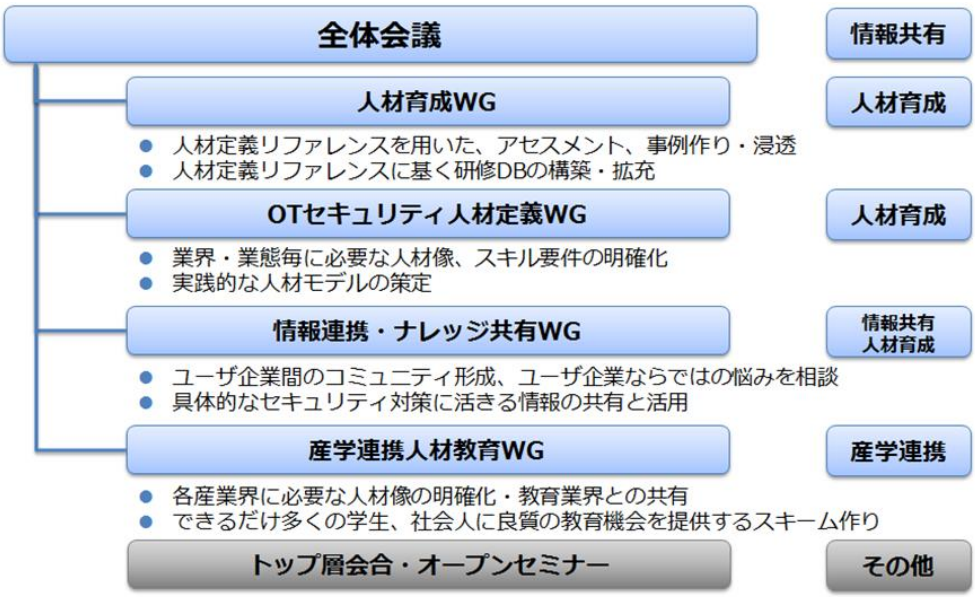

図 1-2 検討会の会議体

また、本検討会の活動では、国内外のセキュリティ関連団体や監督省庁との連携も行っており、様々な会合等において活動の説明や情報提供を実施している。

1.3 スケジュール

スケジュールでは、2016 年 10 月から 2018 年 9 月までを第二期とし、2017 年 4 月からは、本検討会の法人化を進めることとした。（図 1-3）

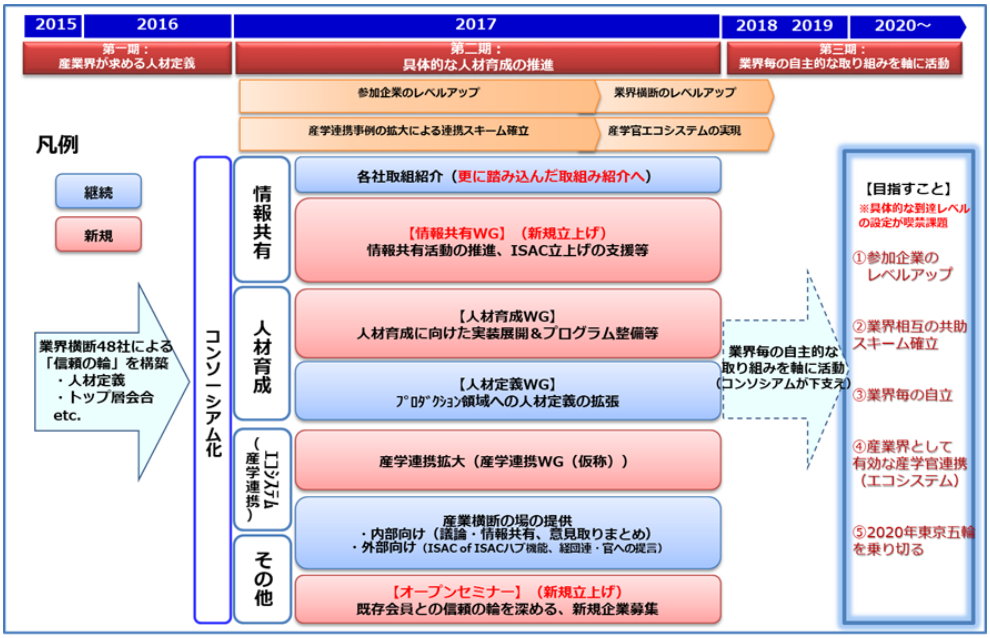

図 1-3 推進スケジュール

また、これまでの会合及びイベントは表 1-3-1，表 1-3-2 の通り開催した。

表 1-3-1 会議体の開催状況

日付	全体会議	人材育成 WG（旧人材定義 WG）	OT セキュリティ人材定義 WG	産学連携人材教育 WG	情報連携・ナレッジ共有 WG
2016 年					
10 月 11 日（火）	○				
11 月 7 日（月）		○			
11 月 16 日（水）	○				
11 月 28 日（月）		○			
12 月 15 日（木）	○				
12 月 22 日(木)		○			

日付	全体会議	人材育成 WG (旧人材定義 WG)	OT セキュリティ 人材定義 WG	産学連携人材教育 WG	情報連携・ ナレッジ共有 WG
2017 年					
1 月 24 日(火)	○				
2 月 23 日(木)	○				
2 月 28 日(火)		○			
3 月 15 日(水)	○	○			
4 月 26 日(水)		○			
4 月 27 日 (木) 28(金)				○	
5 月 25 日(木)	○	○	○		○
6 月 14 日(水)		○	○	○	
6 月 22 日(木)	○				○
7 月 12 日(水)				○	○
7 月 19 日(水)	○				
8 月 3 日(水)				○	
8 月 22 日(火)	○				○
9 月 6 日(水)		○	○		
9 月 14 日(木)				○	
9 月 21 日(木)	○				○
9 月 26 日(火)		○	○		

表 1-3-2　会議体の開催状況

日付	トップ層会合	総会	セミナー		
2016 年					
10 月 17 日(月)	○				
2017 年					
5 月 25 日(木)		○			
7 月 19 日(水)		○	○		

2.人材育成 WG

本 WG は、第一期の人材定義 WG の活動を引き継ぎ、サイバーセキュリティ人材の定義に対する育成モデルの検討という位置づけにより、活動を開始した。

第一期では、最終報告書の別紙に「総括」として以下の通り記載している。

> *これまで17回の議論を通じて、サイバーセキュリティ人材とは情報資産の安全性を確保する人材という広い意味から、日々高度化するICTそのものの技術要件に詳しいだけではなく、会社組織に対する理解、リスクマネジメントを遂行するリスクセンス、更には会社全体で対応していくコミュニケーション能力と幅広いスキルや経験、そしてサイバー空間に流れる様々な情報を扱うための語学力（主に英語力）が求められていることを共有できた。*
>
> *「4.6.16 人材定義WGの活動の総括」より*

また、第一期人材定義 WG におけるアウトプットである『人材定義リファレンス』は、平成 29 年 4 月 18 日に内閣サイバーセキュリティセンター（NISC）が発表した『サイバーセキュリティ人材育成プログラム』において、以下の通り引用されている。

> *例えば、平成 28 年９月に産業横断サイバーセキュリティ人材育成検討会において、情報システム部門を中心としたサイバーセキュリティ人材に必要とされる人材像の定義について報告書が出されている。国や大学・高等専門学校はもちろんのこと、人材育成をビジネスとして行う民間企業においては、教育・訓練などの具体的な取組において、必要とされる人材像の変化にも応じつつ、このような産業界からの発信を踏まえたものとすることが重要である。加えて、人材育成に関する官民の正しい役割分担の検討や、具体的な教育・訓練プログラムの内容の検討において、産学官の連携の強化や、IT の利活用による新しい価値の創造への対応を視野に入れた知の集積を推進することが必要である。*
>
> *『サイバーセキュリティ人材育成プログラム』*
> *平成29年4月18日 サイバーセキュリティ戦略本部*
> *2 現状と課題 (2)IT の利活用による新しい価値の創造への対応*
> *⑦ 人材像に関する共通認識の醸成と産学官の連携強化に向けた仕組みづくり*

上記進捗状況を踏まえて、平成 28 年 9 月からの活動について振り返り、現在議論を進めているサイバーセキュリティ人材の育成に関する議論の経過を整理するものである。

2.1 人材育成 WG の論点

人材育成 WG では、第 11 回までの討議を経て、以下の 3 つ目標を定めることとした。

- ✓ *ユーザ企業には、1 名以上のエキスパート人材（「セキュリティ統括人材」）が必要*
- ✓ *委託先ベンダー企業には、相談ができるセキュリティ人材が必要。*
- ✓ *セキュリティ対策は産業横断での協調領域として認識されるべきもの。*

WG 活動は以下のフェーズに分け、人材育成環境の構築についてモデル策定を進めた。

- ✓ *第 1 回～第 2 回：議論の方向性の共有*
- ✓ *第 3 回～第 4 回：人材定義リファレンス等に基づく人材像の検討*
- ✓ *第 5 回～第 6 回：エキスパート人材の定義と検証*
- ✓ *第 7 回～第 8 回：エキスパート人材の育成環境とキャリアパス*
- ✓ *第 9 回～第 11 回：エキスパート人材の役割と身に着けるべきノウハウ*

また、サイバーセキュリティ人材育成を検討するための環境認識として、以下の 5 項目を意識しながら議論を進めた。これは、第一期の最終報告書において日本特有のビジネス環境として認識されたものである。

- ✓ *日本型雇用システム（終身雇用制度に基づく人事管理）*
- ✓ *ジョブ型のキャリアでは、業務範囲が法令により定められていることが多い。*
- ✓ *日本の IT 従事者の 75％はベンダー側におり、運用保守を担当*
- ✓ *セキュリティ分野は 20 年弱の新しい業界であり人材のすそ野が広くない。*
- ✓ *サイバー攻撃の増加やマイナンバー制度により、社内には一定数のセキュリティ人材が必要となっている。*

2.2 人材育成 WG の 5 つのフェーズ

人材定義 WG から人材育成 WG へ移行する際、これまで NISC や経済産業省と共有してきた課題認識である「人材不足」とその“解消”は、様々な角度からの検証が必要であった。それは「不足しているのであれば充足させるべき」というビジネス上の当然の考え方に立った時、そもそも充足させるのは**「どこの部署に配属される何ができる誰なのか？」**という疑問であった。

既に第一期最終報告書では、セキュリティ機能を担う中核的な役割として「セキュリティ統括（室等）」を定めており、またセキュリティ機能を自社のみで対応できない場合は「アウトソーシング・ガイド」に基づき、委託先ベンダー企業からセキュリティ機能またはセキュリティ人材を提供してもらうことを明確にしている。

しかし、ユーザ企業におけるセキュリティ対策のレベル感を把握できるのは、自社の収益モデルや業務プロセスに明るいユーザ企業に勤務している方々であるという事実と組み合わせると、ユーザ企業の側にも一定数のセキュリティ人材は必要であり、かつその対面にいる委託先ベンダー企業側にもセキュリティのスペシャリストが配置されている形態が望ましいと結論に至った。

以下は、全 11 回を 5 つのフェーズに分けて、それぞれの議論のポイントを解説する。

2.2.1 議論の方向性（第 1 回、第 2 回）

第 1 回では、第 1 期の人材定義 WG を、OT セキュリティ人材定義と IT セキュリティ人材（主に情報システム部門に勤務する人材）育成の 2 つのパートに分ける議論を行った。更に、人材育成そのものを定義するため 4 つの視点を提起し、それぞれの視点について解説し、合意形成を進めた。

また人材育成の方策については、グローバル展開する会員企業においても導入を容易にするため、ISO22398 及び DHS の HSEEP を参考とすることとした。（図 2-2-1）

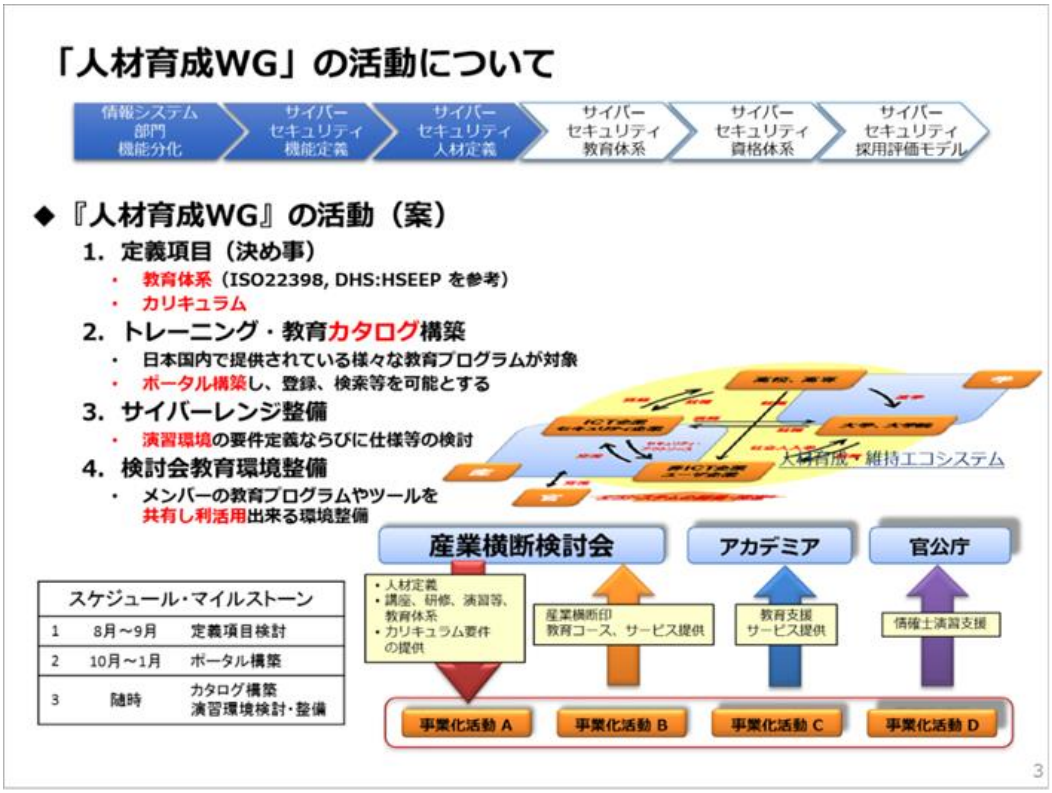

図 2-2-1 人材育成 WG の活動について

第 2 回では、議論の方向性を探るべく、人材育成 WG の作業ステップを提示し、人材育成を取り巻く環境について協議した。特に「セキュリティ人材」の位置付けや範囲、ユーザ企業における人材配置のバランスや人材育成の予算等を踏まえて幅広い議論を行った。

2.2.2 人材定義リファレンス等に基づく人材像の検討（第 3 回、第 4 回）

人材育成 WG としての検討を進めるにあたり、第一期に策定した『人材定義リファレンス』にある 30 役割について、各役割に対する人材育成を進めるかどうかについて協議したが、まずは「ユーザ企業に必要となる人材」について議論を深める必要があったため、サイバーセキュリティ人材育成に求められる要素や「21 世紀型スキル」の解説、更に人材像を明確にするため第一期で議論がなされた「氷山モデル」を再掲し、人材育成のポイントについて議論の振り返りを行った。最後に、検討会会員企業の参加者にキャリアパスに関するアンケートを実施した。

第 4 回では、第 3 回で実施したアンケート結果を報告するとともに、求めるべきセキュリティ人材を、ユーザ企業とベンダー企業の違いを前提とし、整理すべきポイントを明確

にした。また、求められる要素として、以下の 3 つを提起し議論を進めることとした。（図 2-2-2）

図 2-2-2 サイバーセキュリティ人材に求められる要素

更に、想定されるセキュリティ担当者を、専任者と兼務者に分けて、置かれている環境や育成する際に注意すべきポイントを整理した。

2.2.3 エキスパート人材の定義と検証（第 5 回、第 6 回）

第 5 回では、第 1 回～第 4 回の議論を踏まえて、「エキスパート人材」という位置づけを提起し、議論を進めることとなった。議論の発端は、アンケート結果に基づく各社のセキュリティ人材の活動状況に基づき、ユーザ企業の人事制度における「ゼネラリスト」とアウトソーシング先に在籍する「スペシャリスト」の間をつなぐ人材が必要ではないかという提起から、現在各社で活動されているセキュリティ人材をより明確にしていくための仮説検証の議論を進めた。

第 6 回では、人材育成 WG で実施したキャリアパスのアンケート結果に加えて、IPA が発表した資料からセキュリティ人材のキャリアパスの事例を引用し、育成対象及び育成プログラムのあり方についての議論を行った。

2.2.4 エキスパート人材の育成環境とキャリアパス（第 7 回、第 8 回）

第 7 回では、エキスパート人材の位置付けを明確にするため、ユーザ企業における組織構造や人事制度を前提とした議論を進めた。特に、リスクマネジメント体制と年功序列型の人事制度のバランスや、ユーザ企業の立場から企業を守るという役割がどのように設置され醸成されていくかを検証することとした。

この中で、セキュリティ人材に求められる能力を、以下の 3 点を仮説として図 2-2-4 に定めた。

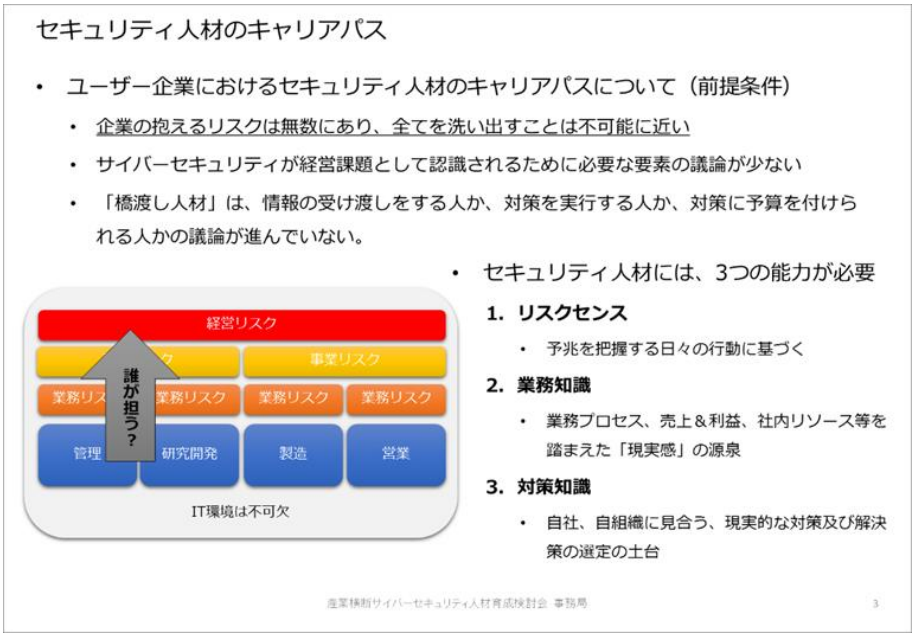

図 2-2-4 セキュリティ人材のキャリアパス

第 8 回は、人材育成 WG 開催の直前に公開されたサイバーセキュリティ戦略本部の発表資料『サイバーセキュリティ人材育成プログラム』に、第一期の人材定義 WG で議論を進めてきた『人材定義リファレンス』等が引用されたことを共有した。

また「エキスパート人材」の定義を進める中で、『人材定義リファレンス』に定めた「セキュリティ設計担当者」が、「エキスパート人材」に相当する人材像として読み替えができることを再度確認し、その人材像に対する育成のあり方について議論を深めた。

2.2.5 エキスパート人材の役割と身に着けるべきノウハウ（第 9 回～第 11 回）

第 9 回～第 11 回では、これまでの「エキスパート人材」の定義を検討するプロセスを踏まえて、能力の定義に移行した。これは、エキスパート人材の働き方に着目し、様々な社内業務を理解し、組織横断での調整力が求められることが認識、共有できたことから、エキスパート人材に求められる様々なスキルのレベル感の理解と共有が重要であると考えられた。

尚、アウトソーシング先のベンダー企業においてセキュリティ人材の採用や育成が進んでいない、あまり興味が持たれていないという課題を共有し、高度化するサイバー攻撃に対しユーザ企業の立場から、外注の多少に拠らず一定の対応力を持つための方法を模索する一環として、議論を進めることとした。

第 9 回は、エキスパート人材に求められるスキルの全体像と専門領域の広さや理解度の深さのバランスを取るところから検討を進めた。特に、エキスパート人材に求められる業務のうち、ユーザ企業の社内に勤務する人材が担当する方が望ましいと考えられるタスクを抽出し、そこに対する育成モデルを検討することとした。ここでは、初出の「エキスパート人材が習得すべきノウハウ（経験をつむための知識・前提）」として、リスクマネジメント、ISMS、CSIRT、セキュリティ設計等を提示し、検証を進めることとした。

第 10 回では、経営陣に対し、サイバーセキュリティの必要性に対する理解得て、エキスパート人材の配置を認めてもらうための要素を討議した。ここでの議論では、「説明責任（Accountability）」に関連するセキュリティ対策を議論の柱とし、「事業継続性」と「ブランド価値の維持・向上」が重要であると定めた。

更に、第 9 回で「議論したエキスパート人材が習得すべきノウハウ」が更新され、以下の 4 点を重視する構成となった。（図 2-2-5）

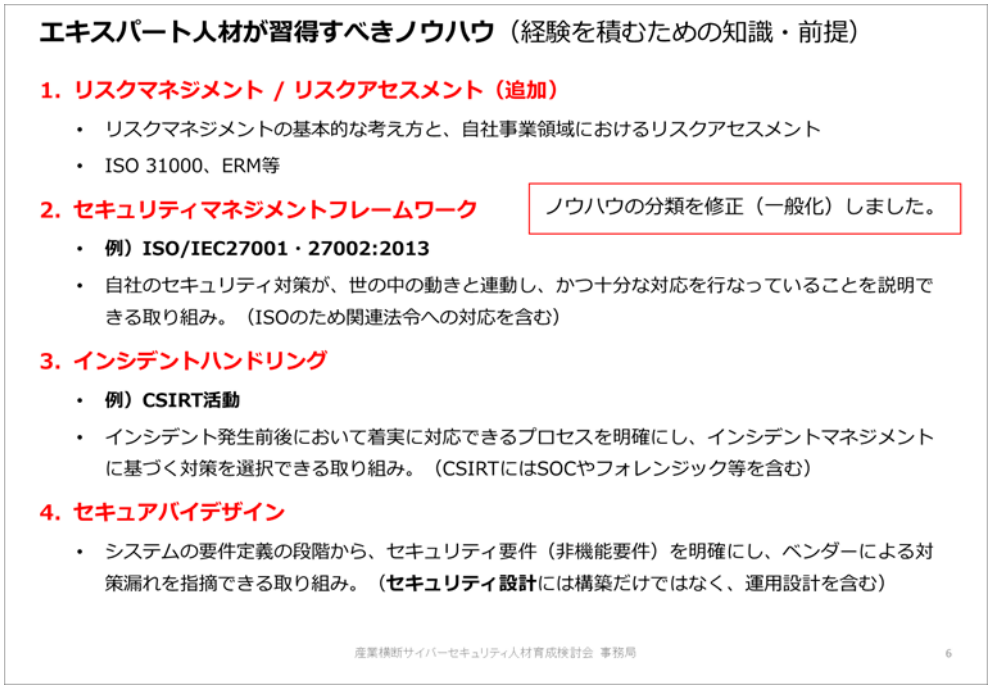

図 2-2-5　エキスパート人材が習得すべきノウハウ

第 11 回では「エキスパート人材」を「サイバーセキュリティ統括人材」と据えて、キャリアパスを含む、育成の方向性や現状の課題を整理する作業を進めた。

以下は、その整理に向けた論点である。

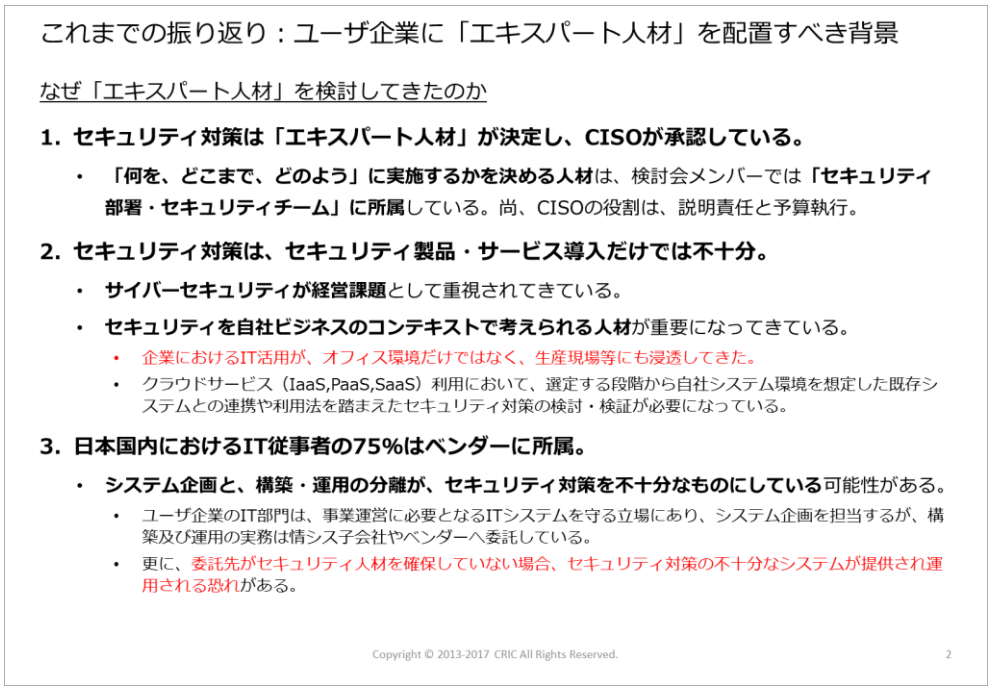

図 2-2-6　ユーザ企業にエキスパート人材を配置すべき

第 11 回での議論では、これまで検討してきた「エキスパート人材」を「セキュリティ統括人材」と定めることにし、第一期の『人材定義リファレンス』の「セキュリティ統括（室等）」との関連付けを行った。

2.3 今後に向けて

人材育成 WG では、人材育成そのものの枠組みを検証するところから活動を始め、まずは法人組織において中核となる「エキスパート人材（セキュリティ統括人材）」をモデルケースとして考証を進めてきた。「エキスパート人材」の定義は、本中間報告をもって仮の決定とし、今後は実際にユーザ企業に配置するために必要なガバナンス、組織論や育成手段、評価手法に議論を移していくこととしている。

これまでの「エキスパート人材」の議論を通じて、経営環境及び事業環境を守るために必要となるセキュリティ人材とは、事前のセキュリティ対策と事後のセキュリティ対応をバランス良く遂行できる人材ではないかとの仮説に基づき、サイバーセキュリティに関する個別事案について対処できる、主に委託先等に所属しているスペシャリスト人材とチームを組み、業務を遂行できる人材像として規定している。

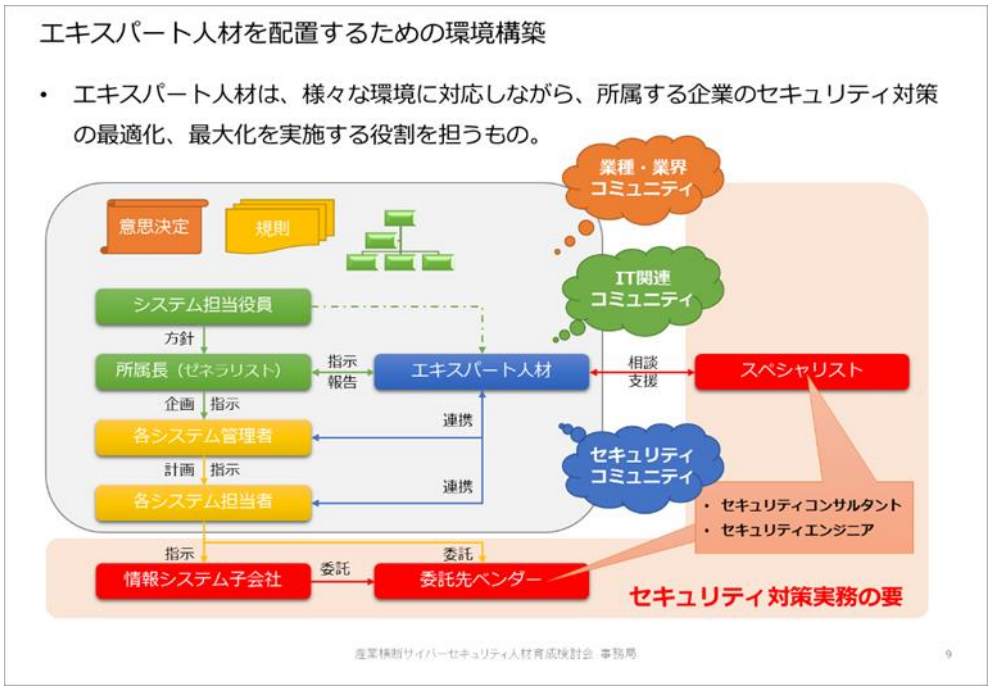

図 2-3　エキスパート人材を配置するための環境構築

今後は、育成環境の整備に関する議論を進める中で、求められる人物像に対応した効率的かつ実践的な育成環境等をより明確に定めていく必要がある。更には、IT スキルに基づくセキュリティ分野と、社内のコミュニケーションを重視する社会人としてのスキルを併せ持つための能力要件の検証を通じて、ユーザ企業に必要となる「セキュリティ統括人材」の役割やキャリアパスについて協議してく予定である。

2017 年にスタートした「情報処理安全確保支援士（登録セキスペ）」や「産業サイバーセキュリティセンター」の取り組みには特に注目しており、これらの資格やプログラムとの関係性を考慮しつつ『人材定義リファレンス』に定めた 30 の役割をより明確にしていくことになる。

そして、法人組織単体でのセキュリティ対策だけではなく、グループ企業間やサプライチェーン先との情報連携を行うことが可能な人材（セキュリティ統括人材）の育成に向けて、人材育成 WG の議論の範囲を拡大していく途上にある。

3.OT セキュリティ人材定義 WG

3.1 「対象となる OT」を確定させる

第一期のサイバーセキュリティ人材定義 WG の成果物を受けて、OT セキュリティ人材定義 WG では、OT（制御システム）セキュリティにまで活動範囲を拡張し、適切な領域に対象を区分していくことを取り決めた。図 3-1 の通り、「共通するコアな OT 領域（赤い枠の領域）」を中心に WG 内でディスカッションを行ない、それを除く「全てを包含する OT 領域（青い枠の領域）」についてはどのように取り扱っていくべきか、各社個別の検討事案として都度整理・確認していくことも必要であると考えた。

また、製造業を中心に、対象を重要インフラ分野にまで拡張して考慮した場合、「共通 OT 領域」をどの分野にまで拡張することが望ましいのかを一緒に議論・確認させていただく進め方を提案し、WG 参加企業からはそれに対する賛同を取り付けることができた。

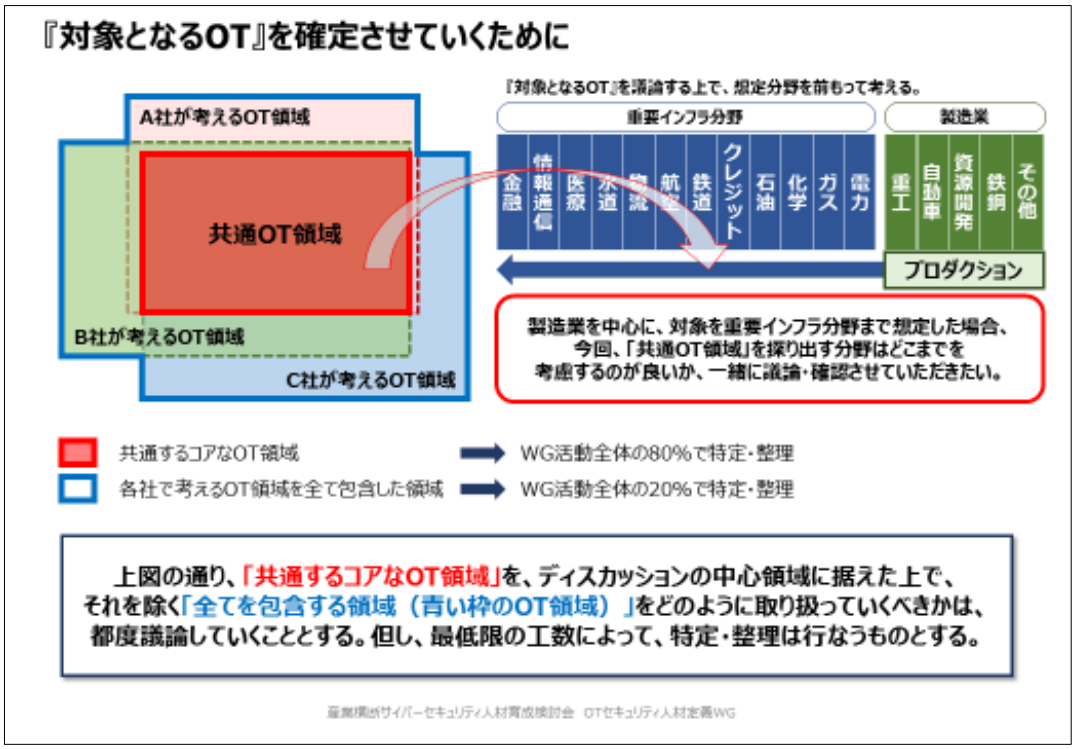

図 3-1　『対象となる OT』を確定させていくために

OT セキュリティ人材定義 WG を開催するにあたって、3 回連続して「制御システム・セキュリティに関する（各社独自の）取り組み」を某ユーザ企業 3 社から発表していただく機会を得た。[1]

そのユーザ企業発表における共通項を以下にまとめていくこととする。

3.2 OT セキュリティを役割・範囲の視点で考える

OT（制御システム）セキュリティを役割・範囲の視点で考えることが求められている。通常、OT セキュリティの役割を検討する上での範囲は、図 3-2 の通り、製造現場における工務（計装）担当と製造現場の IT 担当の双方の役割が重なる赤枠の部分が主に考えられる。この部分の役割を遂行するためには、工場安全・安定操業に関する基礎的な知識を保有していることも大きな前提条件となってくる。

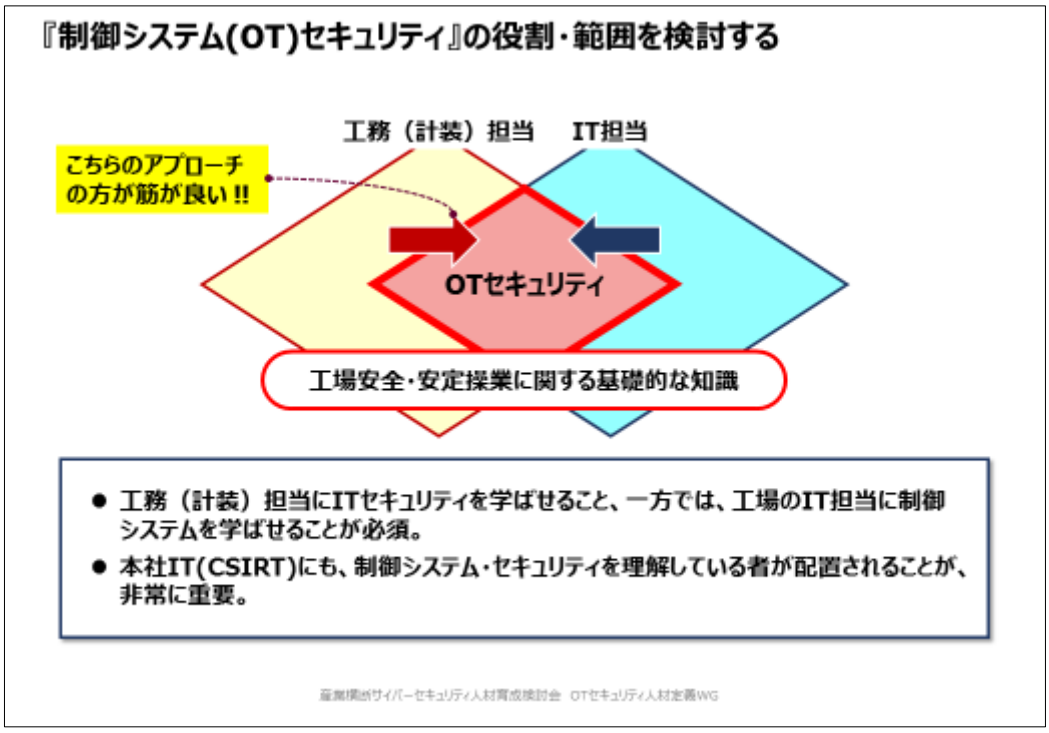

図 3-2『制御システム(OT)セキュリティ』の役割・範囲を検討する

そういった基礎的な知識を学習させる場合には、工務（計装）担当に IT セキュリティを学ばせるのか、あるいは製造現場の IT 担当に制御システムを学ばせるのか、主に 2 通

[1] 2017 年 9 月 6 日, 9 月 26 日, 10 月 4 日に OT セキュリティ人材定義 WG を合計で 3 回開催し、某ユーザ企業 3 社による有志発表の機会を設けたことを、ここでは指す。

りのアプローチが存在している。しかしながら、実際問題としては、製造現場を熟知する工務（計装）担当に IT セキュリティの知識を学ばせる方が筋の良いアプローチと言われている。

その一方で、本社機能の IT 担当（特に、CSIRT チーム等）には、制御システム・セキュリティを理解している者が配置されることも、非常に重要なポイントとなっている。その意図として、本社機能に近く、セキュリティの役割を有する組織・人においては、全社的な展開を想定したプロジェクト運営や活動の推進を求められることが非常に多い。全社的な横断プロジェクトをリードする際には、こういった経験や知識を有するセキュリティ人材を配置し、適切に権限委譲していくことがユーザ企業としては求められているが、そういった人材は不足しており、この観点での人材育成は急務の課題である。

3.3 OT セキュリティを組織・機能面から考える

OT（制御システム）セキュリティを組織・機能の側面から考えることも極めて重要である。ユーザ企業各社によって、取り巻く環境や事情が大きく異なるが、企業各社における「機能」に基づいて、各「役割」が規定されていくことが望ましい姿である。

図 3-3 『制御システム(OT)セキュリティ』の組織・機能面から検討する

一方で、セキュリティの組織構成や運営形態が各社各様である主たる要因は、企業各社の「権限」が「責任分解」点に従って各々規定されているためである。それ故、「権限」と「責任分解」点について特定の関係者間で議論した場合であっても、相違点が必ず生じてくるはずなので、共通の機能や権限に対し『それらの抽象度を如何にして揃えていくべきか』に焦点を合わせることが必要不可欠である。翻って、この観点での議論が OT セキュリティの機能を共通化したり、その機能に連動する必要権限を区分したりすることが可能になる。

今後、この側面における議論を重ねると同時に、ユーザ企業各社の実態を把握させていただくためにも、適切な質問票を慎重に設計した上で、WG 参加企業に対してアンケート等を実施し、現実的な課題を解消していけるような活動に繋げていく所存である。

3.4 OT セキュリティをユーザ視点で考える

OT セキュリティを考慮するにあたって、ユーザ視点（オペレーター視点）で考えることは極めて重要である。オペレーター目線で物事を捉えようとするなら、サイバーセキュリティから先に考えてはいけない。その理由としては、何らかの不具合に遭遇した場合、オペレーターはセキュリティ問題かどうかには通常すぐには気づくことができないからである。日々のプラント異常・故障への対応が主であり、その中でセキュリティ問題を見極められるようになるか否かが、大きな鍵となってくる。

一方、Zero Day [2]遭遇時の製造現場視点で考えることも極めて重要である。実際には、通常のトラブルシューティング能力が成否を分けるのだが、「最小限で動作できる分散制御システム」の役割をオペレーターが熟知していることが前提にある。そのネットワーク制御システムの「素早い切り分け」ができるスキルを保有しているか否かが、Zero Day 遭遇時の適切な対応力・スピードには大きな決め手となってくる。

また、Zero Day に遭遇しないようにすることは極めて困難なことであるため、遭遇することを前提にした事前対策を十分に施すことが大切である。特に、常日頃からの準備として時間を稼げるシステム・仕組みを作ることが必要であり、各種相談・技術派遣等を依頼できる人材バンク・組織との連携を継続していることも緊急時には極めて重要になってくる。

---

[2] Zero Day とは、脆弱性を解消する手段が存在しない状態で脅威に晒される状況をいう。脆弱性が発見されて修正プログラムが提供される日(One Day)より前にその脆弱性を攻撃する攻撃は、Zero Day 攻撃と呼ばれている。

最後に、ユーザ視点の中でも、開発サイドの視点で考慮することは非常に重要である。以下の観点を忘れずに OT セキュリティを構築していければ、堅牢かつしなやかなセキュリティ対策を適切に打ち出すことができるはずである。

- ✓ *現場と共に経験することで得られる、肌感覚の課題認識とシステム構築力*
- ✓ *自ら作成したソフトウェアのミスが現場へ、どのように影響を与えるのか、想像できる当事者意識と能力*
- ✓ *将来のユーザー（次世代オペレーター）が抱く、現場イメージの先取り*

3.5 今後に向けて

OT セキュリティ人材像・人材モデルを策定するためには、その対象となる OT 領域自体を明確に把握し、該当する人材像（タイプ・スキルレベル）を定義していく必要がある。本 WG の目的、目標、及び活動方針については、以下の図 3-5-1 に掲載することとする。

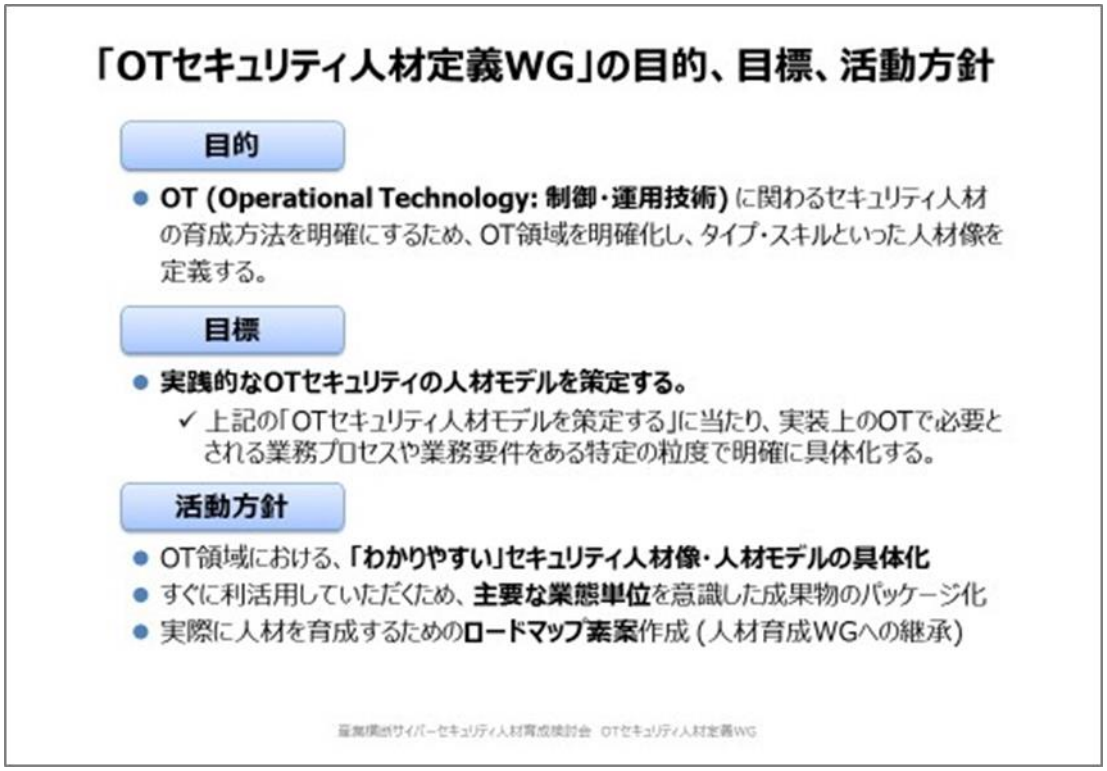

図 3-5-1　本 WG の目的、目標、活動方針

そもそも OT セキュリティの人材を定義するためには、「OT とは何か」を定義することから始める必要があり、ユーザ企業発表、及びその後の集中討議等を通じて、「対象となる OT」をほぼ確定させることができた。[3]

但し、OT 全体を包括して検討する際、OT 領域を「オペレーション視点であるのか、セキュリティ視点であるのか」を意識して整理することは非常に重要なことである。さらに、「要件、アクティビティ、プロセスといった業務的要素が強いものか、あるいは人材スキル、ケイパビリティ等の人的要素の目線で語られるものか」で分類していくと、本 WG 活動の目指す方向性やゴールが見えてくる。

これらの構図は、図 3-5-2 で記している。

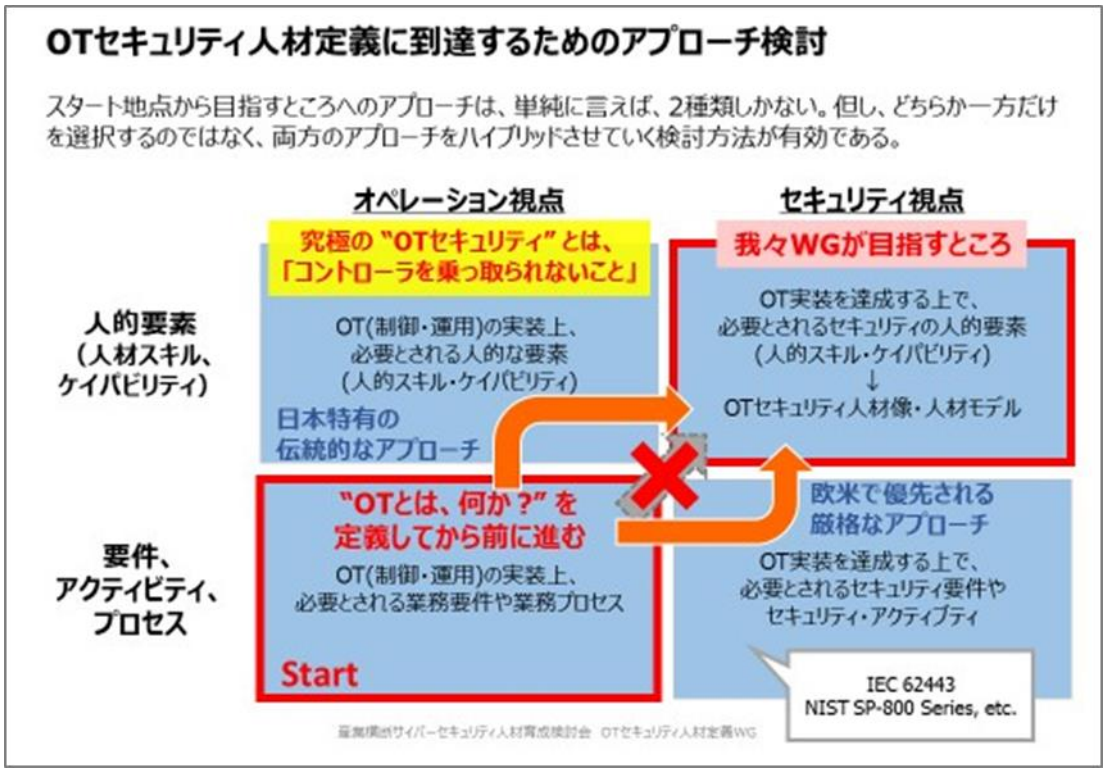

図 3-5-2　OT セキュリティ人材定義に到達するためのアプローチ検討

本 WG 活動のスタート地点から目指すゴールに向かうアプローチは、大きく 2 種類考えられる。一つは、「どのようにすればオペレーションを円滑に運営することができるのか」を重視するアプローチである。実際のオペレーションに重きを置きつつ、業務的要素

[3] “3.1 「対象となる OT」を確定させる”参照

から人的要素に関連させて、進めていくアプローチであるが、製造業を中心とする日本企業では、頻繁に採用される進め方ではないだろうか。

もう一つは、業務的要素を優先するアプローチ、言うなれば、業務プロセスを設計する段階から積極的にセキュリティを考慮するアプローチである。欧米の各業界・業態においては、管轄組織・団体から各企業に対し「セキュアなオペレーションを保証してもらう」ために強制規格化（Regulations）が定期的に行なわれる傾向が強い。したがって、欧米企業では、セキュリティが強く意識されたオペレーションで運営される必要があり、その運営を優先しなければいけない状況にも置かれている。その規格化の好例が、IEC62443 や NIST SP-800 Series である。

双方のアプローチには、オペレーションを行なう上での特徴が存在するが、どちらか一方を選択するのではなく、両方のアプローチをハイブリッドさせていく検討方法が極めて有効であると考えている。

今後、本 WG 活動においては、このハイブリッド・アプローチを模索しながら、最終的な OT セキュリティ人材像・モデル化の策定に向けて、より具体的かつ精緻な検討を繰り返していくこととする。

4.情報連携・ナレッジ共有 WG

4.1 情報連携・ナレッジ共有 WG 発足の経緯

本検討会の 3 本柱の 1 つとして、低コスト、短時間で自社セキュリティ対応力向上につなげるべく、第一期からも「情報共有」活動に取り組んできた。具体的には、1）全体会議における参加企業の取り組み紹介、2）ユーザ企業向け勉強会におけるサイバーセキュリティに関する最新動向等（海外の情報共有の取り組み、サイバー保険等の旬なサービス紹介、サイバーセキュリティ経営ガイドライン等の政府動向紹介等）の知識習得である。

各重要インフラ分野においても民間主導の ISAC と IPA 主導の J-CSIP での活動が代表的なものであり、図 4-1 のとおり、サイバー攻撃に係る情報の収集・分析・共有に関する情報共有の全体像として整理されている。

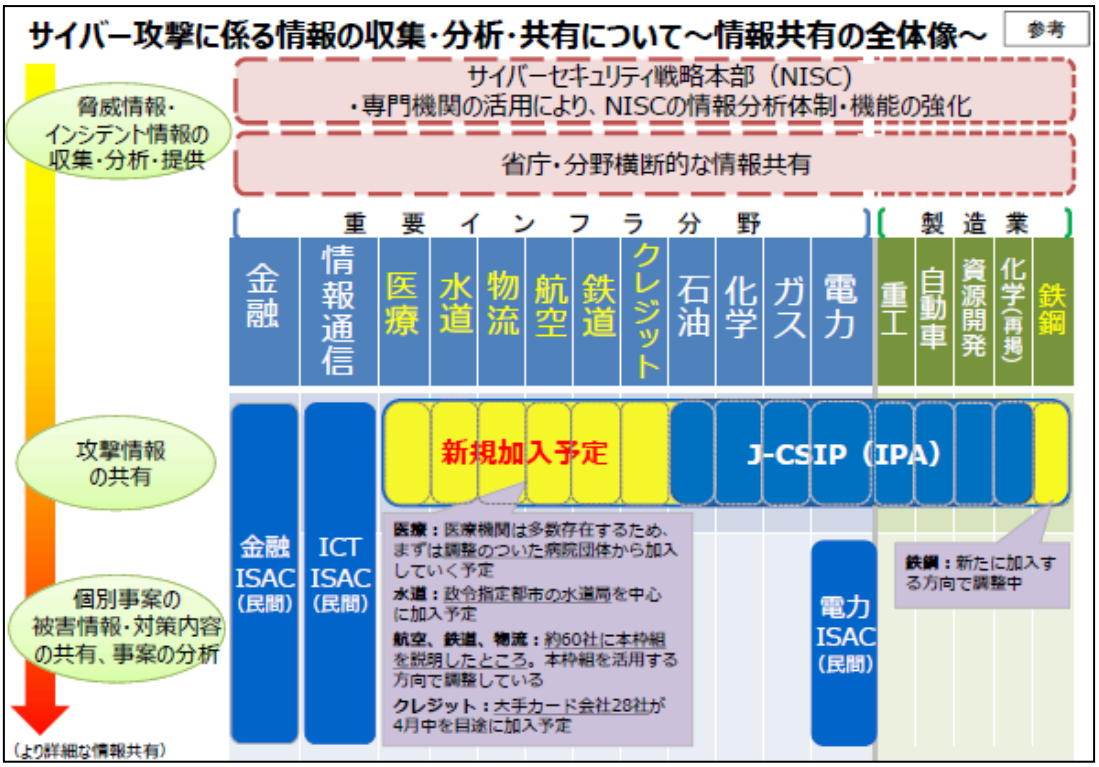

図 4-1 情報共有の全体像

（NISC　サイバーセキュリティ戦略本部　　第 12 回会合（平成 29 年 4 月 18 日）

http://www.nisc.go.jp/conference/cs/index.html）

2015 年 6 月からの 2 年半に亘る活動を通じて、会員企業間の信頼の輪の醸成も進んできたことから、更なる情報共有活性化の土壌も整ってきた。情報共有というキーワードは色んな意味合いがあり、各団体で様々な取り組みもされている。本検討会においては、産業横断活動ならではの活用や、情報共有を通じて各社の課題解決につながる活動とするために、以下のとおり、【WG 名称】、【目的】、【活動内容】、【ゴール】を設定し、2017 年 4 月からの重要インフラ企業中心のユーザ企業が主導する新体制移行に伴い「情報連携・ナレッジ共有 WG」を設置することとした。

【WG 名称】

- ✓ 情報連携・ナレッジ共有 WG

【目的】

- ✓ 会員企業の課題解決に貢献でき、ユーザ企業を中心とした産業横断連携による、情報共有と活用の場を作る。

【活動内容】

- ✓ ユーザ企業間のコミュニティ形成、ユーザ企業ならではの悩みを相談。
- ✓ 効果につながる情報共有・活用のための勉強会の開催。
- ✓ 具体的な情報共有・活用に関する事例集・ベストプラクティスの作成。

【ゴール】

- ✓ 参加各社の課題解決や情報共有活動推進に貢献。
- ✓ 産業界全体のサイバーレジリエンス向上・効率化。

4.2 本検討会ならではの情報共有活動

本検討会ならではの情報共有活動のニーズに関し、概ね以下のニーズ分類となった。

- ✓ *収集のヒントが欲しい*
- ✓ *こんな情報が欲しい*
- ✓ *活用のヒントが欲しい*
- ✓ *情報連携を活性化したい*
- ✓ *他社の取り組みを参考にしたい*

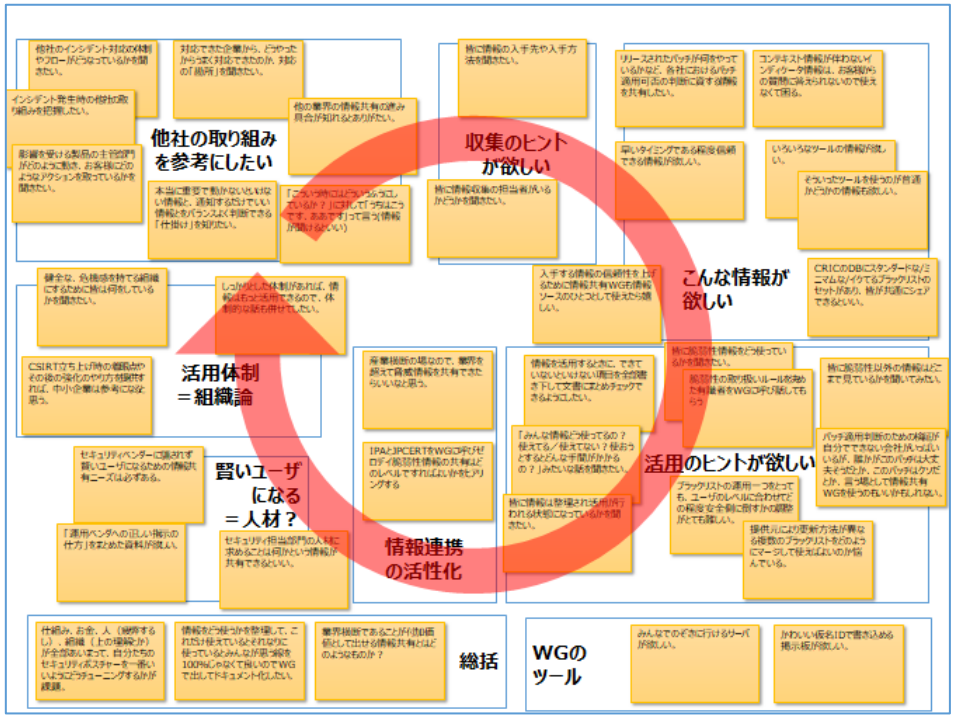

図 4-2-1 ニーズ分類

各分類の詳細をみていくと、情報共有→情報活用→ナレッジ共有のニーズが高いことがわかってきた。産業横断で、社会的責任のある企業で課題解決を図るために、具体的活動として、以下の仮説を立て、会員企業からの声を踏まえ検証していく。

- ✓ ***産業横断で「情報収集・活用のベストプラクティス、もしくは事例集」***

  例）緊急対応マニュアル、調達基準、全体会議での事例紹介

- ✓ ***産業横断で「情報連携の実践（PoC [Point of Contact]の体制整備等）」***

  例）政府機関や関連団体との情報・意見交換する枠組み、ISAC of ISACs

- ✓ ***産業横断で「情報を活用できる人材の育成」***

  例）情報活用人材に求められる機能・役割

- ✓ ***産業横断で「平時/緊急時に集まり相談する場を作成」***

  例）コミュニティ形成

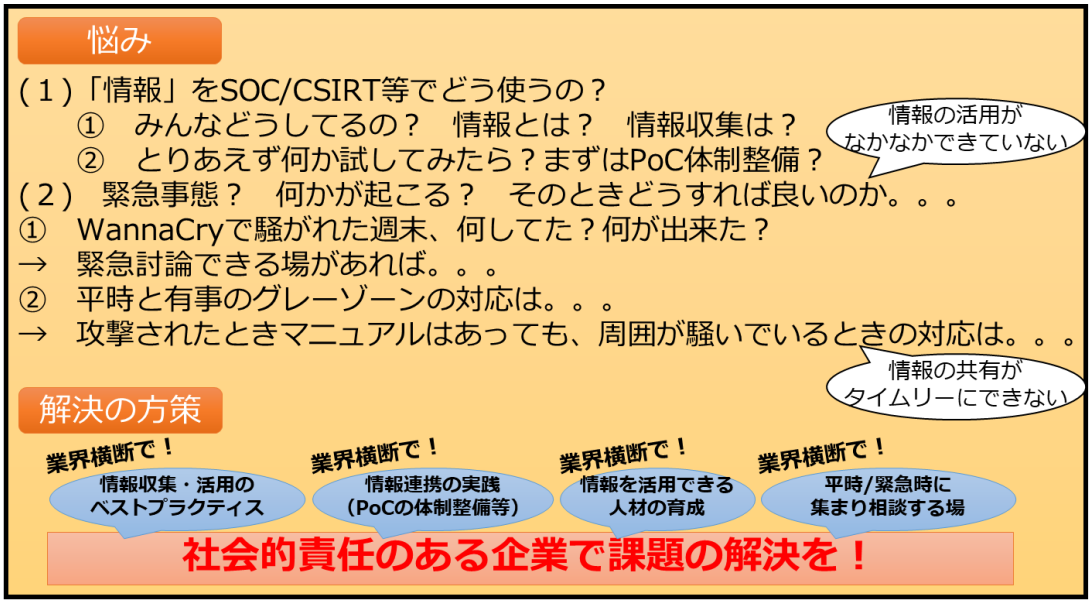

図 4-2-2　活動内容例

4.3 今後の進め方

本検討会ならではの情報共有活動の仮説を検証するためにアンケートを作成し、全会員企業から収集することで、各社の課題（ニーズ）の把握→取組内容決定・優先順位付けに活用、の段取りで進めていく。

合わせて、他団体の情報共有活動を参考にすることで、より内容の濃いものにしていくと共に、他団体とも連携を図ることで、より効果の大きなものにしていく。

また、2020 を契機としたサイバー攻撃に対し、重要インフラ企業を中心とするユーザ企業が自助努力で自社を守るための方策として、情報連携体制の構築、政府との連携も視野に入れ、取り組み内容を具体化していくこととする。

5.産学連携人材教育 WG

5.1 産学連携人材教育 WG 発足の背景

第一期において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り、下記の図 5-1-1 に示す産学連携のイメージを共有していた。

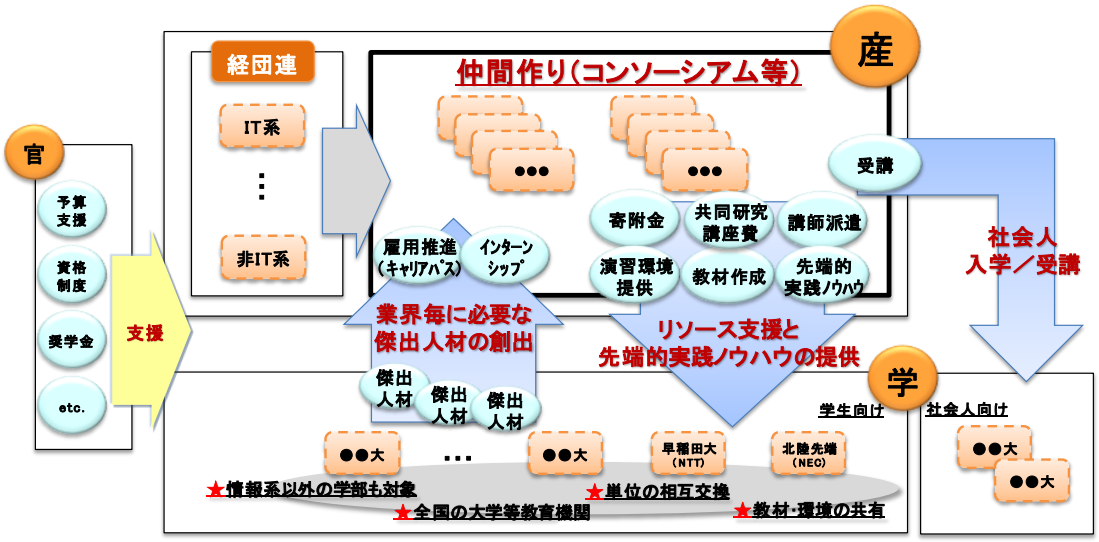

図 5-1-1　産学連携のイメージ

第二期においては、本検討会が CRIC CSF として正式に法人化されたこと、第一期の成果物である人材定義リファレンスが発行されたこと、各社での１社１校の形態での大学連携協定の締結が加速されたこと等の環境変化を受けて、より具体的なアクションを議論すべく有志８社での WG を４月に発足し、WG の正式名称・to-be 像・理念から議論を開始した。

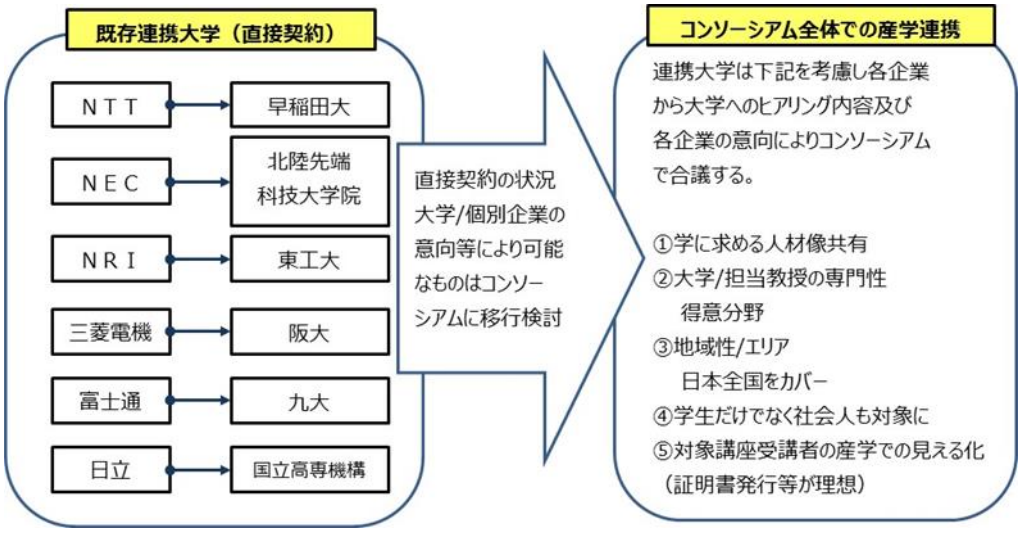

図 5-1-2 産学連携 TO-BE 像

メンバーでの丁寧な議論の結果として、WG の正式名称は文部科学省等との調和を考慮し「産学連携人材教育 WG」とした。また理念は「相互扶助の精神のもと、人材育成に産学連携で対応できる環境づくりの基礎としてわが国において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セキュリティ人材育成エコシステム実現を目指す」とし、産学連携の to-be 像として図 5-1-2 に示す内容を決定した。

5.2 アクションプラン

to-be 像の合意を受けて、具体的なアクションプランの議論への移行を始めるにあたり、WG 参加各社の既存大学連携内容についての情報共有が必須と考え、下記観点を指定したうえで各社の実施内容・検討内容について会合にて紹介して頂いた。

＜既存大学連携紹介の観点＞

- ✓ ***求める人材像***
- ✓ ***連携内容*** ： *講座内容、対象、人数等*
- ✓ ***提供内容（ヒト、モノ、カネ の観点）*** ： *寄附金、講師、教材、他*
- ✓ ***大学・学生からの反響、生の声（良かった点、悪かった点）***
- ✓ ***産業横断メンバーによるその他の既存大学連携と連携できる内容*** ：

  講師派遣、教材提供、コンテンツ提供、ほか
- ✓ ***産業横断メンバーによるその他の既存大学連携から提供して欲しい内容***

- ✓ ***連携先の大学（もしくは先生）の特徴（強み、専門分野）***
- ✓ ***その他　：***

「2020 年までにできるだけ多くの希望者に良質の教育機会を至便な形態で提供する。」ことを目標とした場合、どのようなアプローチができるか

各社からの連携紹介を受けて判ったこと・議論したこととしては

① 寄附講座の形態としては、企業側は大学に出資するのみとし講座実施内容は大学にお任せするやり方（富士通/九大連携）、企業側で教材を作成し講師を派遣する「出張授業」を行うやり方（日立/国立高専連携）、双方を取り入れたやり方があること。また、講義だけではなく演習主体のもの、研究を対象としているもの（NEC/北陸先端大連携）等があること。

② 既存連携内容の中で、アカデミックな分野であれば横展開が可能なものがあること、周辺大学からの学生受入れを検討している連携があること。

③ 各社の直接契約には個別事情があり、それをコンソーシアム全体での契約に移行するには、大学との調整、各社内での稟議等に多大な時間を要すること。新規に講座を開設するには大学との調整に 1 年半程度の期間が必要であること。

④ 産業界として学生に伝えるべきメッセージが重要であること。

⑤ 教育機関の先生が求めるもの、学生が勉強したいこと、産業界が学に求めるものの３つの観点があり、その中で産業界として何が出来るかをヒアリングする必要があること。

⑥ 学に求める人物像ばかりではなく、採用基準・キャリアパス等、産業界から見た人材教育の課題、大学から見た産業界への要望/課題等議論した内容を報告書に纏めて世に問うことが出来るといい。合せてそうした議論を出来る場所を提供することも必要であること。

等があり、それらを考慮した上で議論を進めて行くこととした。

また、第二期のアクションプランとして、図 5-2-2 アクションプランに示す６つのプロセスを検討することとした。

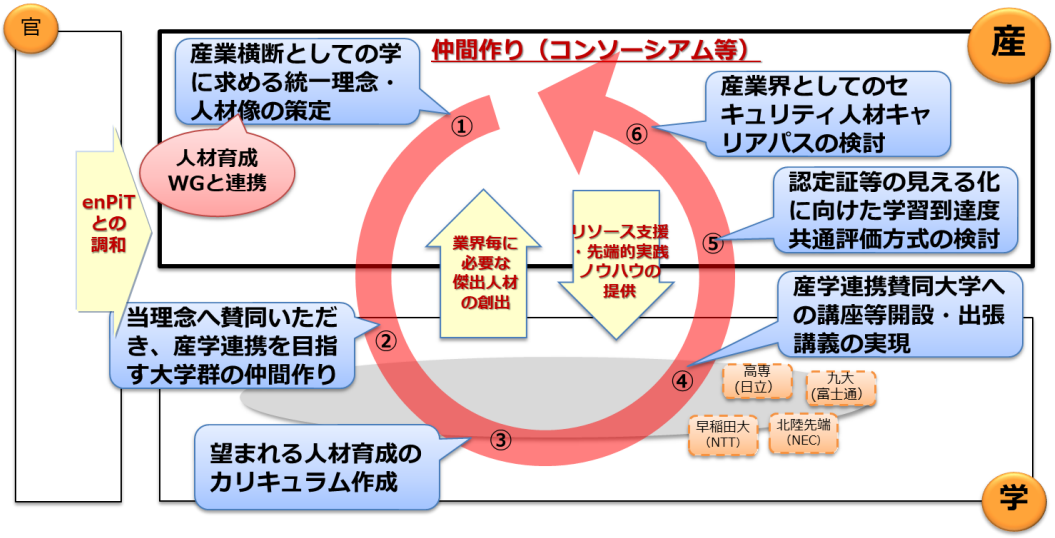

図 5-2-2 アクションプラン

5.3 人材育成 WG との連携

アクションプランの第 1 段階である「産業横断としての学に求める統一理念・人物像の策定」の検討を開始するにあたり、人材育成 WG との連携が必須であると考えた。

人材育成 WG ではスペシャリスト・ゼネラリストに対比したエキスパート人材（セキュリティ統括人材）確保の必要性に言及し、エキスパート人材が習得すべきノウハウ（経験を積むための知識・前提）やキャリアパスについても検討しており、それらの議論を受けてエキスパート人材育成に向けて、大学においてどのようなことを学んだ上で企業に入社して欲しいかが「学」に求める人物像となる。このステップがアクションプランの第 3 段階としての「望まれる人材育成のカリキュラム作成」に該当するものと考えており、その点を考慮した上で本 WG の議論を進めて行くことが必須であると考えている。その中でも、今までのスキームでは輩出できなかった人材を確保すべく、新しい取り組みを含め、議論を進めていくこととした。

5.4 産学連携実施形態

産学連携の講座実施形態として、１）寄附講座、２）CRIC CSF 主催セミナーまたは短期講座の２つがあると考えており、以下に各々の特徴を示している。

5.4.1 寄附講座

① 第一期から続く、学に求める人物像を伝えて、それに見合う講座及び研究を選定し、更に必要な講座提供がある場合には新規に講座開講を目指すもの。

② 既存連携がモデル、学問的要素＋企業での実務要素を加味。 講師・教材は学での準備に加え、企業での教材作成/講師派遣もあり。

③ 大学での新規講座立上げには 1 年半程度の期間を要す。

④ 文部科学省管轄

5.4.2 CRIC CSF 主催セミナーまたは短期講座

① 第二期で検討を開始、大学２年生及び修士１年生を対象とした、専攻選択前に「サイバーセキュリティ」への道を紹介するセミナーまたは短期講座を開講。

② 教材は本検討会会員企業で作成し、会員企業内でアサインした講師が出張授業。

⇒会員企業での既存教材の流用、カスタマイズ・新規作成

正規な講座新設ではないので、寄附講座に比べれば短期間での立上げが可能。

③ 学部等へのアプローチだけではなく学生課や就職課を経由するルートを模索する。

④ 管轄省庁が不明（どの省庁が本取り組みに関心を寄せて頂けるのか不明）であるため、サイバーセキュリティ戦略本部が発表した「サイバーセキュリティ人材育成プログラム」の記載に従い進めるという体裁を採用する。

⑤ 非 IT 企業/重要インフラ企業への入社が理系人材ばかりではなく、文系人材が多数入社している現実を受けて、文理混合学部（コミュニケーション学部等）・法学部・経済学部・商学部・経営学部等の学部生や、彼らが入社後に配属が想定される部署（営業・法務・調達・経理・総務等々）で必要となる IT・セキュリティ知識の提供をスコープとして考慮。

⑥ 参加者は学生だけではなく、先生も招待し、意見交換の場を作る。

そこでの議論を受けた次回内容・新規寄附講座立上げへのフィードバック等を実施する予定。

5.5 今後の進め方

今後の進め方としては、to-be 像で示した通り、検討会会員企業でのファンドを設立しコンソーシアム全体で運営する寄附講座を立上げることがゴールではあるが、これには 1 年半程度の期間を要す他、リソース面での各社での制約も大きい。

まずは、CRIC CSF 主催セミナーまたは短期講座の詳細内容を早急に議論し 2017 年度中に試行的に立上げ、そこでの先生方/事務方のご意見、学生の反応等を見た上で、最終形態であるコンソーシアム全体で運営する寄附講座へと発展させていくことを考えて行きたい。

6.トップ層会合・オープンセミナー

6.1 トップ層会合

6.1.1 トップ層会合開催の背景

経営者がサイバー攻撃への備えを重要な経営課題と捉え、経営者自らが強いリーダーシップを発揮することが求められている。経営者は自社のみならず、系列会社や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が不可欠かつ責務であり、ステークホルダー（顧客や株主等）の信頼感を高めるとともに、平時からのセキュリティ対策に関する情報開示など、関係者との必要なコミュニケーションを必要としている。その一助とすべくトップ層会合を開催することとした。

図 6-1-1 に示すように、通常の本検討会は、経営者への助言や意思決定を支援する中間層の参加者が主体となっている。トップ層会合は、それよりも上位の経営層を対象とし、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るための交流の場である。

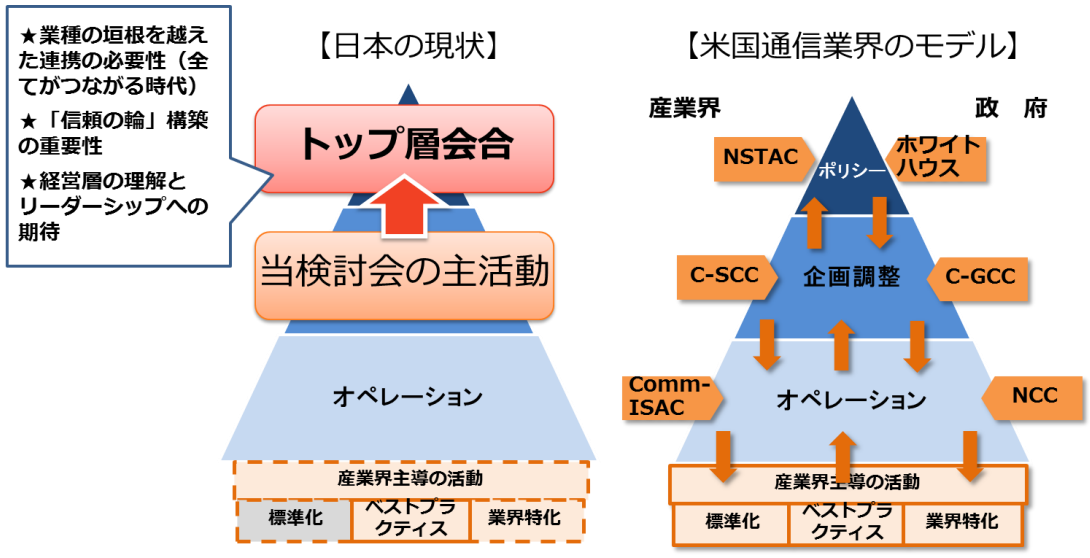

図 6-1-1 トップ層会合の位置づけ

6.1.2 第1回トップ層会合開催模様

第１回トップ層会合の開催にあたり、「経営課題としてのサイバーセキュリティ／2020も見据えて」をテーマに、次の目的を設定した。

- ✓ *検討会の成果と今後の計画を報告し、各社内での展開･実運用の推進をお願いする。*
- ✓ *各社のインシデント情報や対応状況を幹部レイヤで共有し、意識を高めてもらう。*
- ✓ *検討会への継続的参画を支持してもらう。*

また、開催模様は次のとおり。

＜日時＞　日時：平成 28 年 10 月 17 日（月）16:00-19:00

＜場所＞　経団連会館

＜主催＞　本検討会（CRIC CSF）

＜参加人数＞　84 名（38 社）

＜プログラム＞

#	時刻	時間	議題	発表者
第一部：16:00-17:30				
1	16:00-16:05	5分	●開会の挨拶	・日本電信電話株式会社 代表取締役副社長　篠原 弘道
2	16:05-16:15	10分	●活動報告等 ・これまでの活動成果説明 ・成果の活用推進に関するお願い	・事務局
3	16:15-17:35	80分	●講演＆意見交換（テーマ：「経営とサイバーセキュリティ」） ・講演 「ANAのセキュリティ対策と経営の巻き込みについて」 「当社ならびに業界における制御系システム分野のサイバーセキュリティに関する取組み」 （ゲスト講演）「リオ２０１６大会のサイバーセキュリティと東京２０２０大会に向けた考察」 「海外動向のご紹介」 ・質疑応答	・全日本空輸株式会社 ・住友化学株式会社 ・東京オリンピック・パラリンピック競技大会組織委員会 ・日本電信電話株式会社
4	17:35-17:40	5分	●活動計画等 ・検討会の今後の取り組み計画説明 ・事務説明	・事務局
5	17:40-17:45	5分	トイレ休憩・会場移動	
第二部：17:45-19:00				
6	17:45-19:00	75分	●乾杯	・ＪＸアイティソリューション株式会社
			●懇親会	・現場の声、参加者の声をスライド表示
			●中締めの挨拶	・トヨタ自動車株式会社

図 6-1-2 プログラム

開催模様については、本検討会公式 HP（http://cyber-risk.or.jp/）にて公開中。

図 6-1-3 開催レポート

6.1.3 今後の進め方

第１回トップ層会合では、多くの会員企業の経営層に参加いただき、経営層の理解、支持を得、経営層間の交流を図ることができ、有意義な場であった。更には、参加企業から一歩踏み込んだ自社の取り組み紹介をいただけたのも、検討会の活動を通して「信頼の輪」を構築できた成果の１つと考える。

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、「どこまで対策を講じるべきか」を判断することは難しい。このような課題解決に向け、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。

トップ層会合は、「経営層の啓発、継続的なトラストチェーン構築」を実現する重要な場の１つとして、今後も年に１回程度の頻度にて開催し、会員の信頼の輪を醸成・深化すると共に、新規会員候補への拡大、経営層参画への発展、及び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ス集」の策定・活用を推進していく。

6.2 オープンセミナー

6.2.1 オープンセミナー開催の背景

2017 年 4 月からの重要インフラ企業中心のユーザ企業が主導する新体制移行に伴い、本検討会の活動が会員企業以外にも認知され、プレゼンス向上や会員企業の増加につなげるＰＲ機能強化の必要性が高まってきた。第一期において、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していた「ユーザ企業向け勉強会」を発展させ、本検討会に参加してほしい企業や本検討会が連携していきたい団体のセキュリティに従事されているミドル層（経営層への説明者など）の方々に集まってもらい、本検討会の活動内容や活動計画の紹介、並びに本検討会の会員企業の事例紹介や招待講演等も交え、サイバーセキュリティ強化の実践に関する意見交換の場を設定することとした。

6.2.2 第一回オープンセミナー開催模様

第 1 回オープンセミナーの開催にあたり、「2020 年を見据えた企業内セキュリティ強化の実践に向けて」をテーマに、次の目的を設定した。

- ✓ ***参加企業の皆様に本検討会の活動内容、成果、今後の活動計画の認知度を高め、プレゼンス向上につなげる。***
- ✓ ***会員企業間の信頼の輪を高め、今後の活動のスピードアップにつなげる。***
- ✓ ***会員企業以外にも、本検討会に興味、関心を高め、会員増へつなげる。***

また、開催模様は次のとおり。

＜日時＞　日時:平成 29 年 7 月 19 日（水）16:30～19:30

＜場所＞　TKP 東京駅大手町カンファレンスセンター

＜主催＞　本検討会（後援:一般社団法人 日本経済団体連合会）

＜参加人数＞　89 名、43 社・団体（うち招待　19 名、14 社・団体）

6.2.3 今後の進め方

第１回オープンセミナーでは、多くの招待企業・団体に参加頂き、CRIC CSF の理念・活動内容の認知や、業界間の交流を図ることができ、有意義な場であった。今回のセミナーでは、一歩踏み込んだ自社の取り組み紹介を頂けたのも、検討会の活動を通して「信頼の輪」を構築できた成果の１つと考える。

今回のセミナーを産業横断の「信頼の輪」の拡大（新規会員）と深化（既存会員）のきっかけとし、今後も半期に１回程度の頻度にて、交流の場を継続的に設け、参加企業の事例紹介や本検討会の活動内容に関する情報を発信することで、本検討会の認知度向上機能の１つとして活動を推進していく。

以上