

サイバーセキュリティ対策に求められる機能と人材定義

「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ついて」

産業横断 サイバーセキュリティ人材育成検討会
日本電気株式会社 武智 洋

自己紹介

武智 洋 (たけち ひろし)

所属: 日本電気株式会社 クラウドシステム研究所

その他活動:

産業横断 サイバーセキュリティ人材育成検討会 事務局
(<http://cyber-risk.or.jp/>)

日本セキュリティオペレーション事業者協議会 (ISOG-J) 代表
(<http://isog-j.org/>)



一般社団法人サイバーリスク情報センター (CRIC) 代表理事
(<http://cric.jp/>)

WASForum Hardening Project 実行委員
(<http://wasforum.jp/hardening-project/>)



国際電気通信連合 電気通信標準化部門 (ITU-T) SG17 Q10
Associate Rapporteur



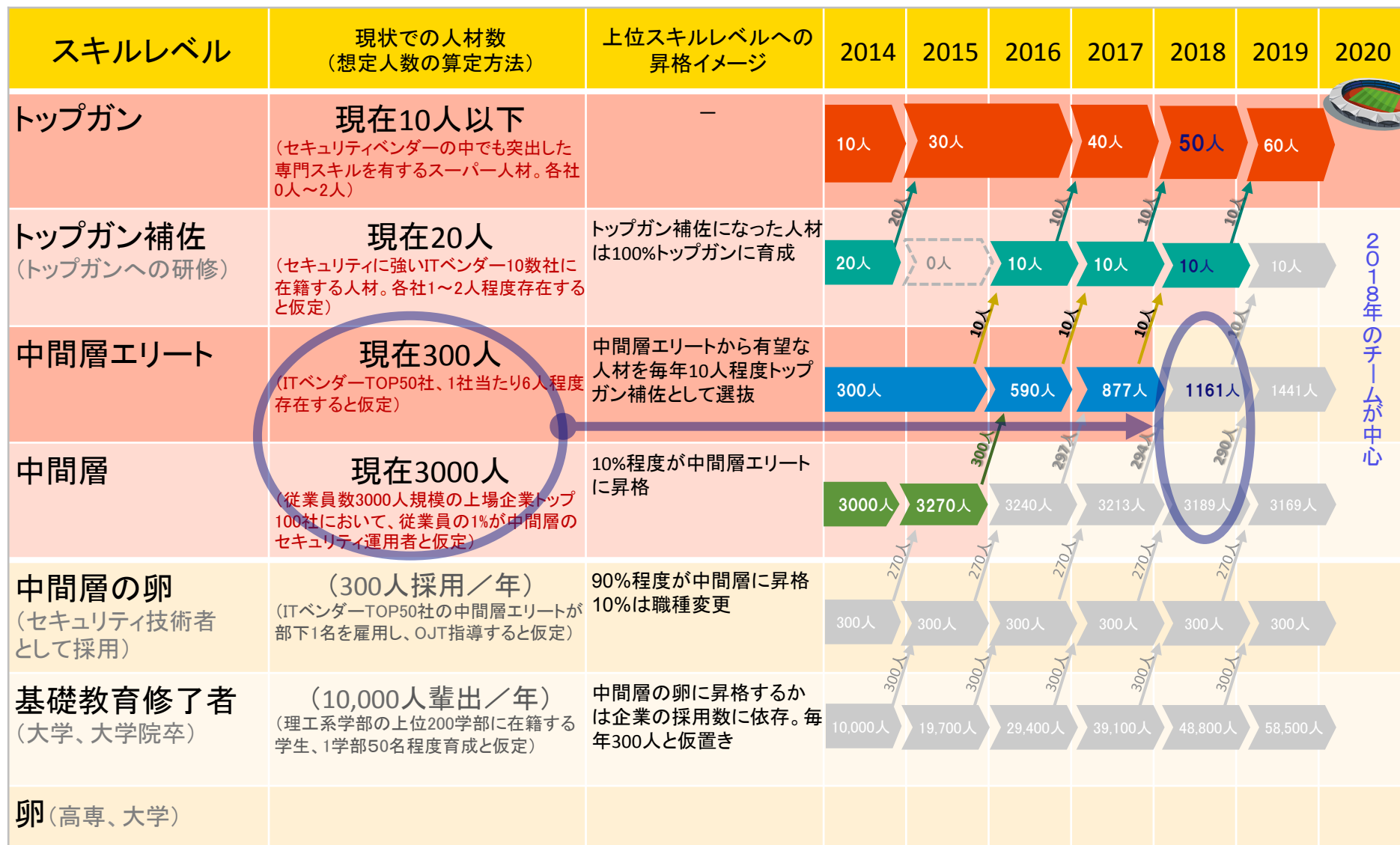
本日の題目

1. セキュリティ人材についての考察(2年前～)
2. 産業横断検討会について
3. 企業にとってのセキュリティ人材
4. 産官学連携とエコシステム
5. 今後の活動について

1. セキュリティ人材についての考察

1. 2年前のシミュレーション

出展：オープンガバメント・コンソーシアム/サイバーセキュリティ分科会 セミナー&報告書



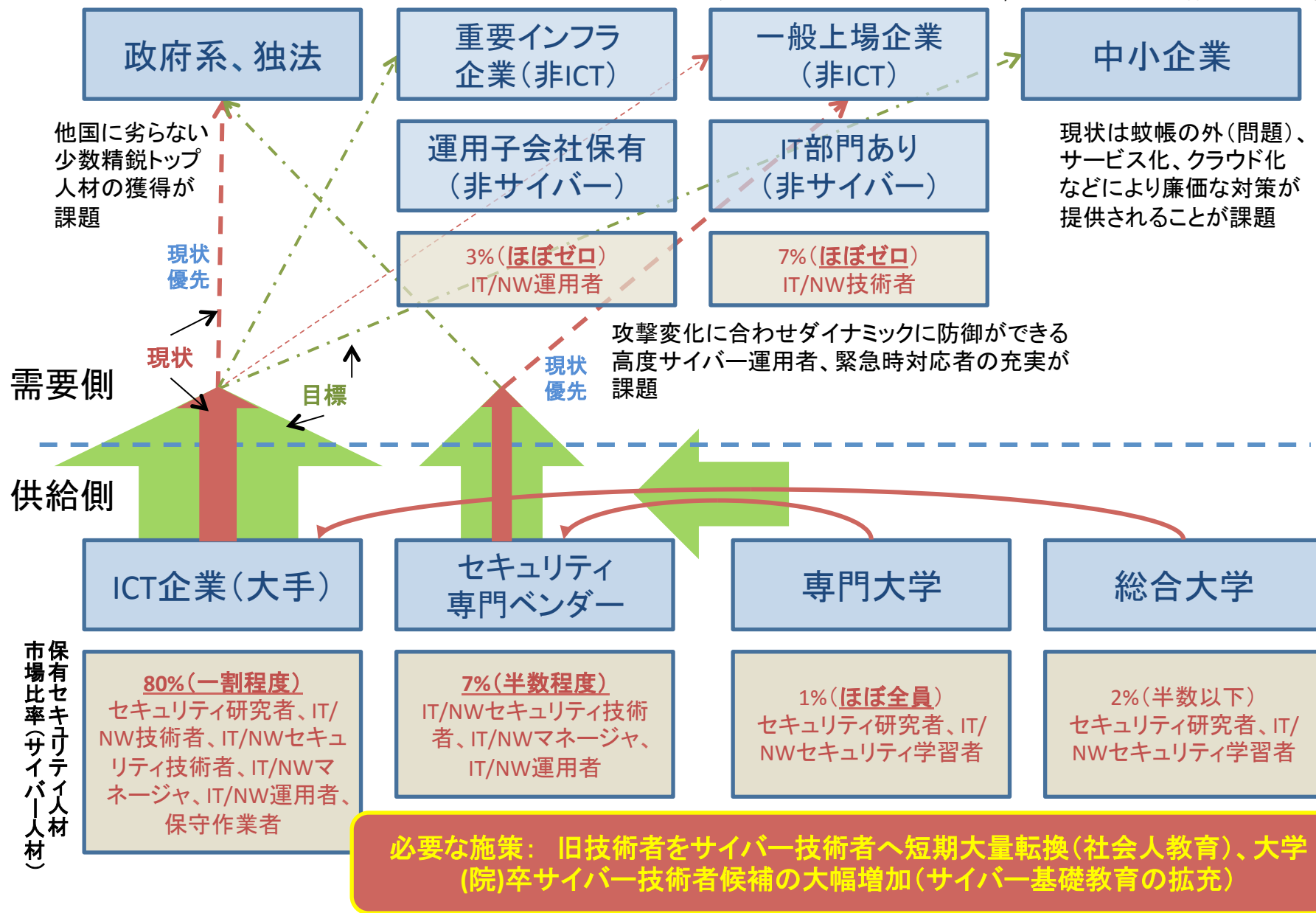
2018年までに実働部隊(中間層エリート・中間層)を如何に増やせるかがカギ

2. その後の検討でわかったこと

- 2020年までの期間を考えると、大学から育成するのでは間に合わない。
- 2020年は企業内の少数現役サイバー技術者(中間層)、多数の潜在サイバー技術者(中間層候補、今は他の仕事をしている)の活用で乗り切るしかない。
- がしかし、2020年以降を支えるサイバー人材として、企業での取り組みに並行して、すぐにでも大学でサイバー人材育成(中間層の卵)に取り組むべき。
- トップガン育成は企業でできない。企業内には場・機会がない。
- 2020年を越えると全国共通の目標を失い、足並みがそろわなくなる。何としても日本人中心で乗り切るべき。

3. 育成対象候補は限られたところにしかない？

出展：オープンガバメント・コンソーシアム/サイバーセキュリティ分科会 セミナー&報告書



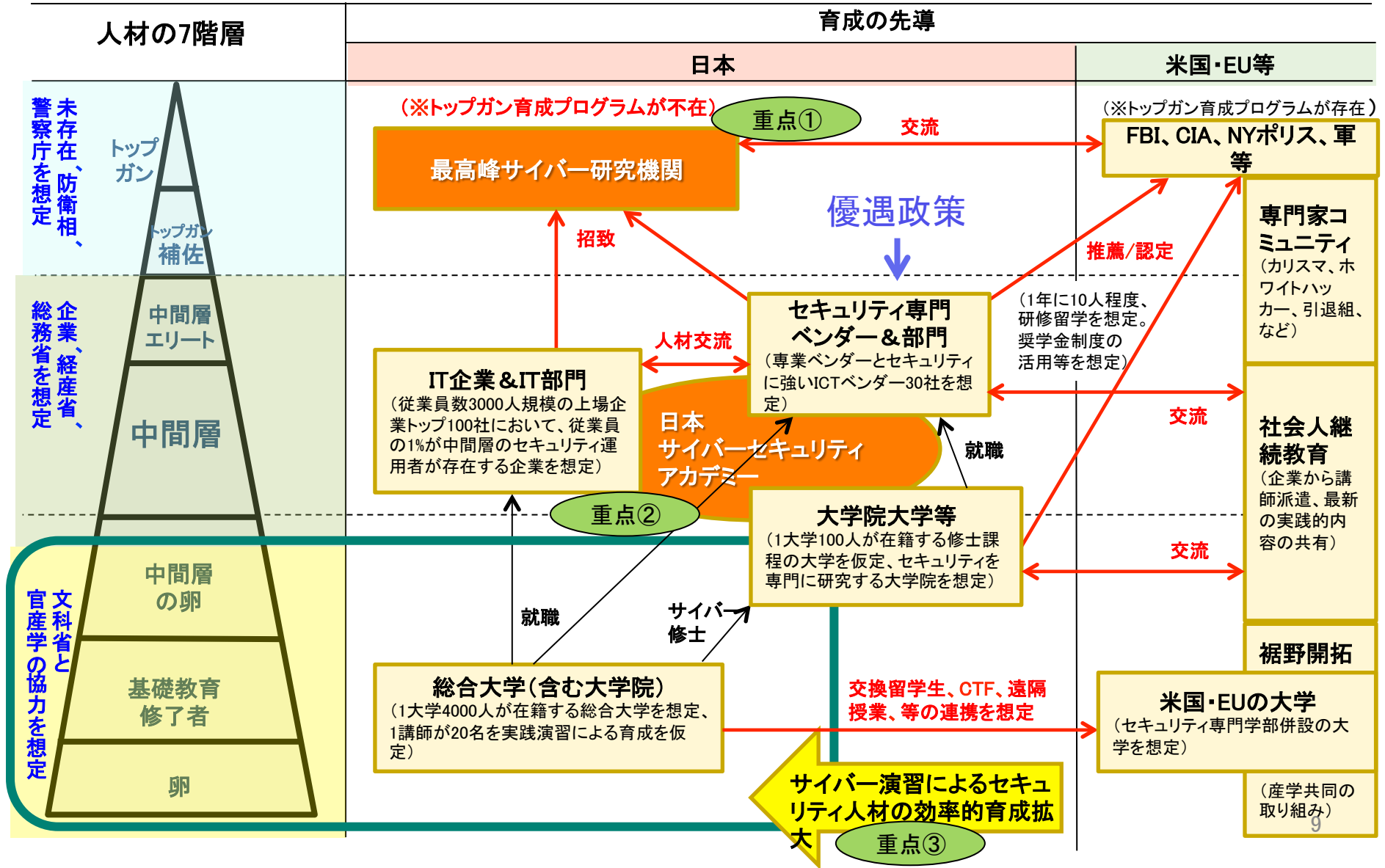
4. サイバー人材育成の候補は

- 育成シミュレーションを行ったとき、大手企業ならどこでもサイバー技術者育成候補がいて考えていた。大きな誤解だと思い知った。
- ほとんどの組織 (非ICT企業、中小、政府、自治体・・・) には候補がない
- 上限はあるものの、大手ICT企業とセキュリティ専業ベンダーには多数いる
- 無限数の可能性があるのは、高校生、高専、大学生
- もっと無限数の可能性があるのは、海外の企業、大学生
- ただし、海外依存は十分な検討と成功の見通しが必要、黒船受け入れ側の器の充実がまず必須

5. サイバーセキュリティ人材育成・維持 エコ・システム

出展：OGC=オープンガバメント・コンソーシアム/サイバーセキュリティ分科会 セミナー&報告書

至急整備: 既存:



2. 産業横断検討会について

1. 「産業横断サイバーセキュリティ人材育成検討会」の活動①

- 経団連配下のサイバーセキュリティ懇談会の参加メンバー、及び重要インフラ企業を中心に、2015.6.9発足。
- 情報通信、金融、航空、鉄道、エネルギー関連等、重要インフラ13業種を中心に43社が参加（2016.1時点）。

産業横断で取り組む意義

- 企業が知りたい／悩んでいる、でもなかなか聞けない／誰に聞けば分からないことについて、互いに共有し合う場が必要
- 業界毎に必要なとなるセキュリティ人材の定義が必要
- 必要な人材を育成するにあたり、育成プログラム、育成ツールを共有することで、セキュリティコスト低減が期待できる
- セキュリティ人材の源である、学生（大学生、高専生等）に対し、産業界が必要とする人材を育成することで、ニーズにマッチした人材育成が可能



情報共有



人材育成



産学連携



2. 「産業横断サイバーセキュリティ人材育成検討会」の活動②

- 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」を推進する。

産業横断サイバーセキュリティ人材育成検討会

情報共有

- 重要インフラ企業を中心とした各業界の現状や課題、セキュリティ対策等の取り組みを共有

サイバーセキュリティ人材定義WG

人材育成

- 守るべき対象の明確化、業界毎の必要スキルの明確化
- 育成プログラム、育成ツールの共有

ユーザ企業向け勉強会

情報共有
人材育成

- 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共有
- セキュリティ対策のアプローチ、方策に関する勉強会開催

次世代に向けた人材育成（産学連携）

産学連携

- 各産業界に必要な人材像の明確化
- 有志企業による学校教育の支援（プログラム作成、資金援助、教育参加など）

3. 活動スケジュール

	2015年度									2016年度		
	2Q			3Q			4Q			1Q		
	7	8	9	10	11	12	1	2	3	4	5	6
対外連携	第二期「サイバーセキュリティに関する懇談会」 ▲7/17 経団連へ活動状況(必要な人材像など)			----->			▲1/19 経団連第二次提言 ▲1/14 報道発表					
メンバ企業各社	各企業内、各業界内での取り組みに展開											
全体会議(月1回) (情報共有& WGエッセンス共有)	フェーズ1: 人材定義(→経団連にインプット)						フェーズ2: 産業界としての取り組み検討					
	○各社プレゼンによる取り組み事例紹介等 例)標的型攻撃に対する社内取り組み、インシデント対応の社内ルール、 金融ISACの取り組み etc.						○人材定義WGを踏まえた人材育成議論 ・自社でできること、外部に頼ること ・育成と雇用 ・学への期待、官への期待 etc.					
ユーザ企業向け 勉強会(月2回) (関心テーマの 知識底上げ)	・制御システムのセキュリティ ・CSIRT活動 ・リスク分析・守るべき 情報資産の整理 etc.						・ICT企業から見たユーザ企業(委託元)に求める人材 ・ユーザ企業が保有すべき人材 ・業界毎の人材育成の現状と課題 etc.					
	○業界毎の守るべき対象整理と必要な人材定義 ・守るべき対象の整理(業界共通、個別) ・必要な人材(職種、役割) ・必要なスキルとレベル						○人材定義に基づくギャップ分析(現状と悩み) ・業界毎の人材育成の現状と課題 ・官や学の取り組みの理解と連携議論 etc.					
人材定義WG(月1回) (アウトプットを意識した各 テーマ討議)	○業界毎の守るべき対象整理と必要な人材定義 ・守るべき対象の整理(業界共通、個別) ・必要な人材(職種、役割) ・必要なスキルとレベル						○人材定義に基づくギャップ分析(現状と悩み) ・業界毎の人材育成の現状と課題 ・官や学の取り組みの理解と連携議論 etc.					

4. 報道発表について(2016年1月14日)

- 本検討会の活動は、経団連第二次提言（1.19公開）にインプット済み。本提言とあわせ、プレス発表を実施することで、本活動を広くアピールすると共に本活動の実効性を高める。
- なお、本検討会の活動内容については、「中間報告書」として取りまとめ、経団連第二次提言とあわせ公開。

<報道発表発表(抜粋)>

2016年1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: 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)

産業横断でのサイバーセキュリティ人材育成に向けた課題を抽出

～人材育成のためのエコシステム実現を目指して～

産業横断で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が連携し2015年6月に発足した「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)では、このたび成果として、日本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い、必要な人材像の定義・見える化に向けた課題を抽出しました。今後、産業界が必要とする人材像の明確化と人材育成のためのエコシステム実現に向けて取り組みます。

<「産業横断サイバーセキュリティ人材育成検討会」立上げの背景>

今後日本で開催される様々な国際イベントを控え、大規模施設やそれを取り巻く様々な環境に対するサイバー攻撃対策が喫緊の課題です。また、あらゆる企業、あらゆる“もの”がネットワークにつながるにつれて、それぞれの業界や企業にとって守るべき対象が拡大しています。セキュリティ対策には、業界や企業の垣根を越えた産業横断によるセキュリティ対応力向上への取り組みが不可欠であり、特に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によるサイバーセキュリティ人材育成がその要です。

2014年10月、一般社団法人日本経済団体連合会(以降、経団連)においてさまざまな業界、企業による議論が進められ、2015年2月17日に経団連から国への提言が公開されました。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」が発足しました。本検討会の参加企業は当初の約30社から、現在(2016年1月現在)は約40社以上まで拡大しています。

<活動内容>

本検討会の目的は、産業界の協力体制構築、産業界に必要な人材像の定義・見える化、産業界の円滑な人材育成であり、将来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)の実現を目指します。

主な活動内容は、以下の3点です。

- ① 情報共有の推進

<報道発表発表の骨子>

- 2020年を見据え、重要インフラ分野を中心とした重要な業界に関わる事業者でのセキュリティ対応力向上に向けた取り組みが必要。
- 2015年2月17日に発表された経団連から国への提言(2015.2.17)を受け、「産業横断サイバーセキュリティ人材育成検討会」を発足(2015.6.9)。
- 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を中心とした議論を実施。
- サイバーセキュリティ人材育成に向けた課題を抽出
- 今後、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。
- 日本の産業界・企業の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エコシステムの具体案を検討・提唱。

5. 記事掲載(日本経済新聞)

1/14 日本経済新聞(朝刊)

サイバー攻撃が企業を脅かす

2011年	三菱重工業の潜水艦などの研究・製造拠点11カ所がウィルス感染
14年	ドイツの鉄鋼メーカーの生産設備の一部がサイバー攻撃を受けて破損
15年	日本年金機構がウィルス感染、125万件の情報が流出 国際的ハッカー集団「アノニマス」が成田空港や厚生労働省、大手新聞社などを断続的に攻撃
16年	米司法省が米化学大手デュポンに不正アクセスして企業秘密を入手したとして中国企業を提訴

「産業横断サイバーセキュリティ人材育成検討会」と呼ぶ組織を立ち上げ、NTTとNEC、同を務めて主導する。各業界の代表的な企業で連携を始め、徐々に加盟企業を広げる考え。14日発表する。

トヨタ自動車やソニー、NTTなど日本の産業界を代表する40社強の企業がサイバー攻撃対策で連携する。最新のサイバーテロに対応できる人材の育成に共同で取り組むほか、攻撃情報も共有する。あらゆるモノがインターネットでつながるIoTが普及すれば、サイバーテロの被害は一企業にとどまらない影響を与えかねない。業界の垣根を越えた取り組みで被害を最小限に食い止める。

人材育成、攻撃情報も共有

トヨタ・ソニーなど40社

サイバー対策、異業種連携

活インフラを支える企業を中心に参加を募った。こうした企業がサイバーテ

6.「産業横断サイバーセキュリティ人材育成検討会」メンバ企業

(五十音順 五十音順)

KDDI株式会社

JX ホールディングス株式会社

住友化学株式会社

全日本空輸株式会社

ソニー株式会社

大日本印刷株式会社

株式会社TBSテレビ

東海旅客鉄道株式会社

東京海上日動火災保険株式会社

東京ガス株式会社

東京地下鉄株式会社

株式会社 東芝

トヨタ自動車株式会社

株式会社 日本経済新聞社

日本生命保険相互会社

日本テレビ放送網株式会社

日本電気株式会社(NEC)

日本電話株式会社

日本放送協会

日本郵船株式会社

株式会社野村総合研究所

株式会社パソナ

東日本旅客鉄道株式会社

株式会社日立製作所

富士通株式会社

株式会社みずほフィナンシャルグループ

三井住友カード株式会社

株式会社三井住友銀行

三菱重工業株式会社

三菱商事株式会社

三菱電機株式会社

株式会社三菱東京UFJ銀行

ヤマトホールディングス株式会社

株式会社リコー

他

7. 経団連「サイバーセキュリティ対策の強化に向けた第二次提言」

URL: <http://www.keidanren.or.jp/policy/2016/006.html>

The screenshot shows the Keidanren website interface. At the top, there is the Keidanren logo and the text 'Policy & Action' and '一般社団法人 日本経済団体連合会'. A search bar with 'Google カスタム検索' and a '検索' button is visible. Below the header, there are navigation tabs: '新着情報', '経団連の概要', 'コメント/スピーチ', '政策提言/調査報告', and '機関誌'. The main content area is titled 'サイバーセキュリティ対策の強化に向けた第二次提言' and includes a date '2016年1月19日' and the organization name '一般社団法人 日本経済団体連合会'. A sidebar on the left lists various policy areas such as '総合政策', '経済政策、財政、金融、社会保障', '税、会計、経済法制、金融制度', etc. The main content area has sections for '【概要】', '【本文】', and a list of sections: '1. はじめに', '2. サイバーセキュリティの意義', '3. サイバーセキュリティ対策', and '4. 産業界の取組み'. A button at the bottom of the main content area says '「科学技術、情報通信、知財政策」はこちら'.

8. 中間報告書の掲載HP

URL: <http://cyber-risk.or.jp/sansanren/>

産業横断サイバーセキュリティ人材育成検討会です。

産業横断サイバーセキュリティ人材育成検討会 お問い合わせは cyber-jinzai-ml@hco.ntt.co.jp

報告書 Report

中間報告

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 (平成28年1月19日公開)

- [「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](#)
- [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](#)
- [別紙2 機能定義とNICE・NIST](#)

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す。

なお、一部図などに著作権表示を提示している部分を除き、本報告書の著作権は、「産業横断サイバーセキュリティ人材育成検討会」に帰属します。

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

▶ [トップページ Top Page](#)

▶ [活動案内 Guide](#)

▶ [報告書 Report](#)

▶ [情報取扱方針 Policy](#)

▶ [お問い合わせ Contact](#)

産業横断サイバーセキュリティ
人材育成検討会

9. 「産業横断 サイバーセキュリティ人材育成検討会」のHPについて

URL:<http://cyber-risk.or.jp>



ようこそ、産業横断サイバーセキュリティ人材育成検討会のホームページへ。

産業横断サイバーセキュリティ
人材育成検討会

Information

お知らせ

- 産業横断サイバーセキュリティ人材育成検討会 中間報告書の公開について
本検討会では、これまで実施してきました活動報告としまして、中間報告書の公開を予定しております。
- 『サイバー攻撃対策、異業種連携 トヨタ・ソニーなど40社』 日本経済新聞電子版
<http://www.nikkei.com/article/DGXLZO96085140U6A110C1TJC000/>
- お問い合わせ
本検討会へのお問い合わせは、右上の[お問い合わせ](#)より、事務局へご連絡ください。

3. 企業にとってのセキュリティ人材

1. 検討会での議論・論点

想定された議論

- 守るべきもの
- 企業活動としてのセキュリティ対策の共通モデル
- **セキュリティ人材定義方法・表現手法**
- 育成の対象となる人材がどこに存在するかについて

産業界としての論点

- ICT企業とユーザ企業
- 企業規模（大手企業と中小企業）
- ICTシステムと制御システム
- 業種による特徴
- 単一ビジネス企業と複合ビジネス企業
- 国内と海外展開
- 情報システム系子会社の有無とグループ会社の関係
- マネージメント層の専門性（CISO/CSO等の特性）
- **セキュリティ人材の要件：スキルセットと役割**

2. 日本企業におけるサイバーセキュリティ人材の定義に向けて

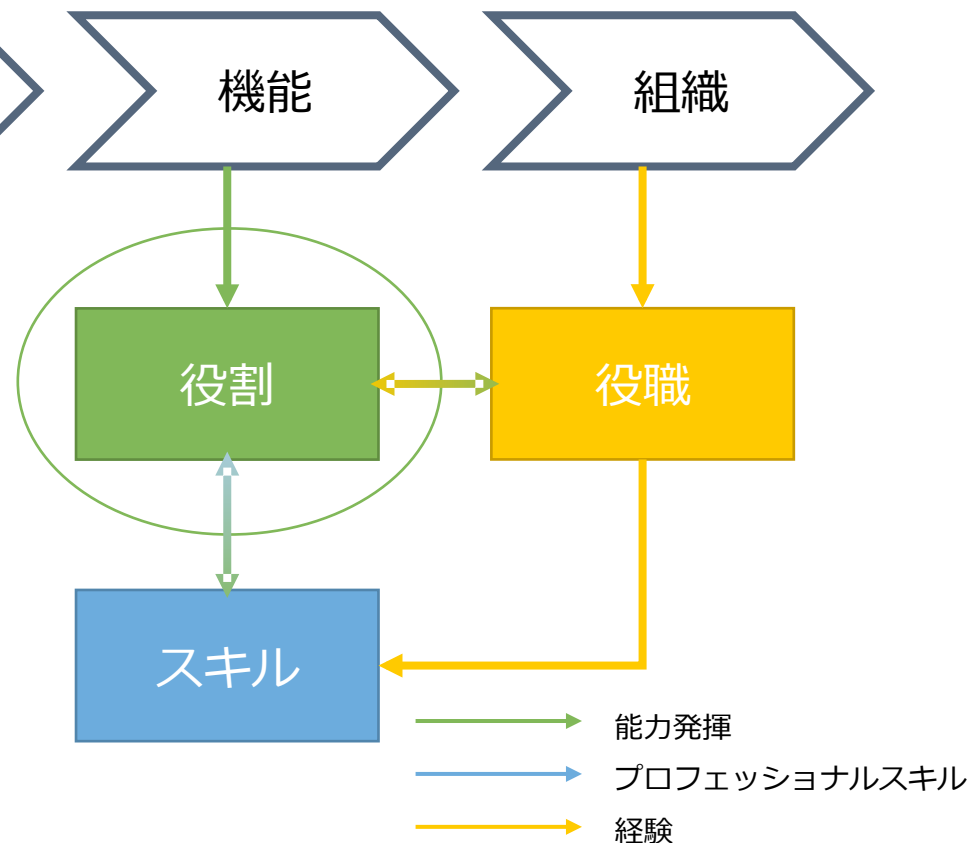
【考慮すべき日本企業の実情】

- セキュリティ機能（ログ分析、マルウェア解析など）で定義しても、機能に該当する職種が必ずしも存在しないため、採用活動の基準にはならない。
- 先行している海外のセキュリティ職種（分析官、フォレンジックなど）をもとに定義しても、日本企業にはその職種が当てはまらず採用が難しい。
- 日本企業の現場においては、セキュリティ業務は本業を持つ管理者、技術者に少しずつ分散して担われている（セキュリティ専任ではない）。

3. 企業におけるセキュリティ人材定義の考え方

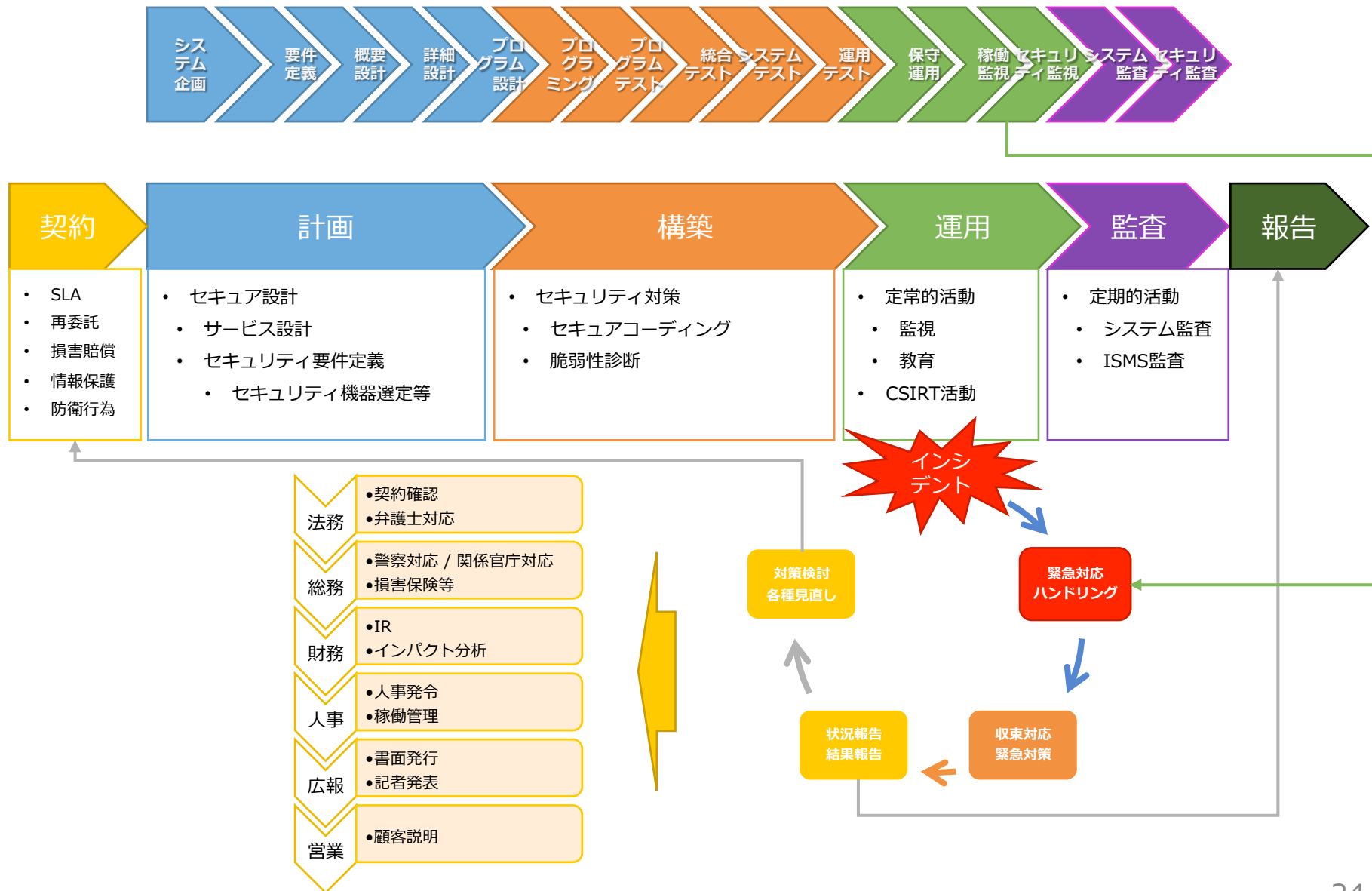
- 組織と人材の関係を考え、**機能**から**役割**と**スキル**を明確にする
- 優秀な人材とは、役割を担うことができる人材であり、それを環境及び個人の観点から実現可能にしていくことが、人事管理の重要なポイントである。
- 組織運営の観点から、**役割**・**役職**・**スキル**の関連を整理すると

- **事業**を遂行するために必要となる**機能**を実現できる**役割**に分解し、それを実現できる**スキル**を持った個人を割り当てる。
- 役割を担う人材を処遇する、又は権限を与えるために**役職**を用意する。
- **役割**を担うために**スキル**を必要とするがさらに**役割**を担う過程で身に付く**スキル**があり、更に**役職**を持つことにより、自身及び組織の管理が強化される



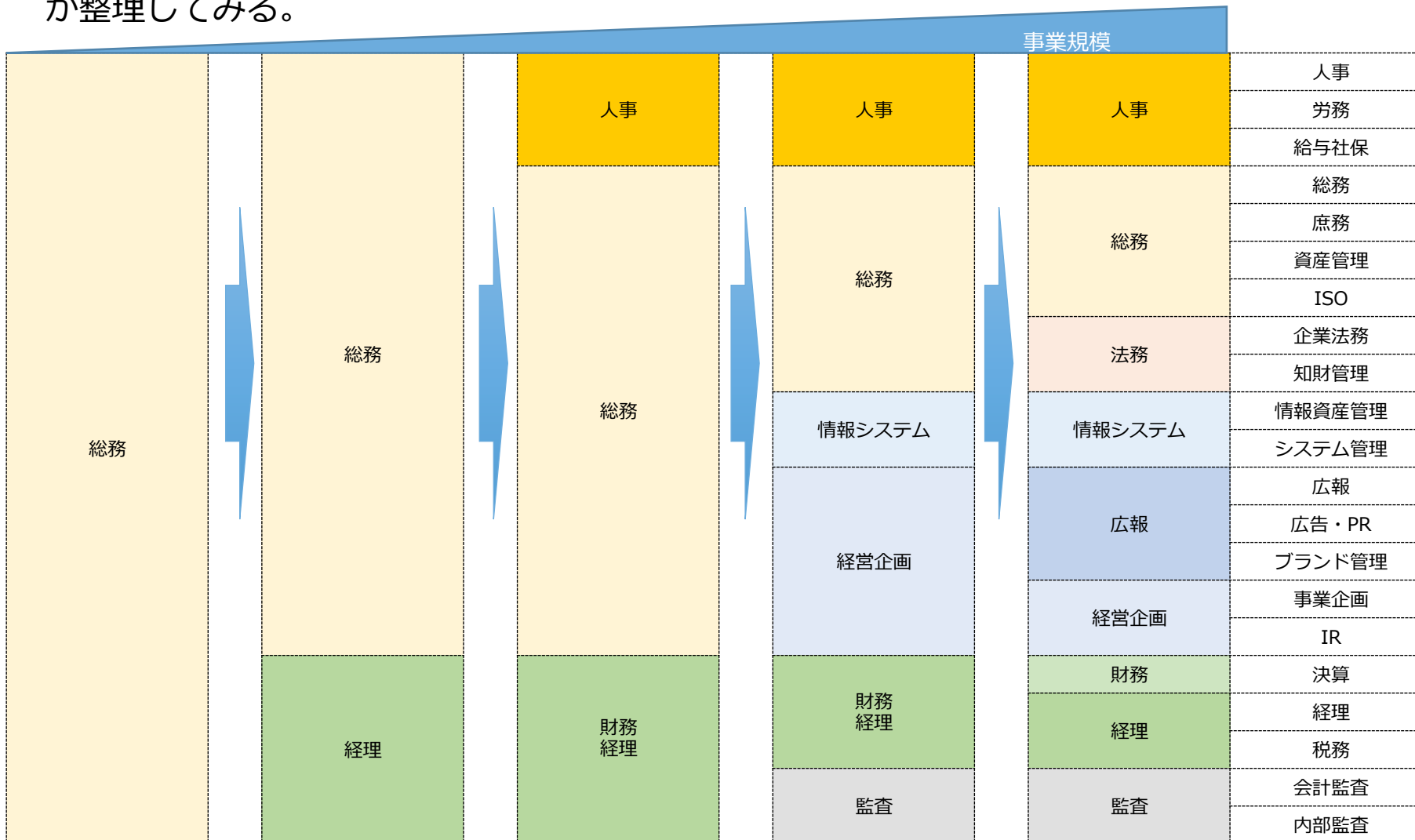
4. サイバーセキュリティ対策のプロセスを整理する（例）

- システム開発・運用プロセスから

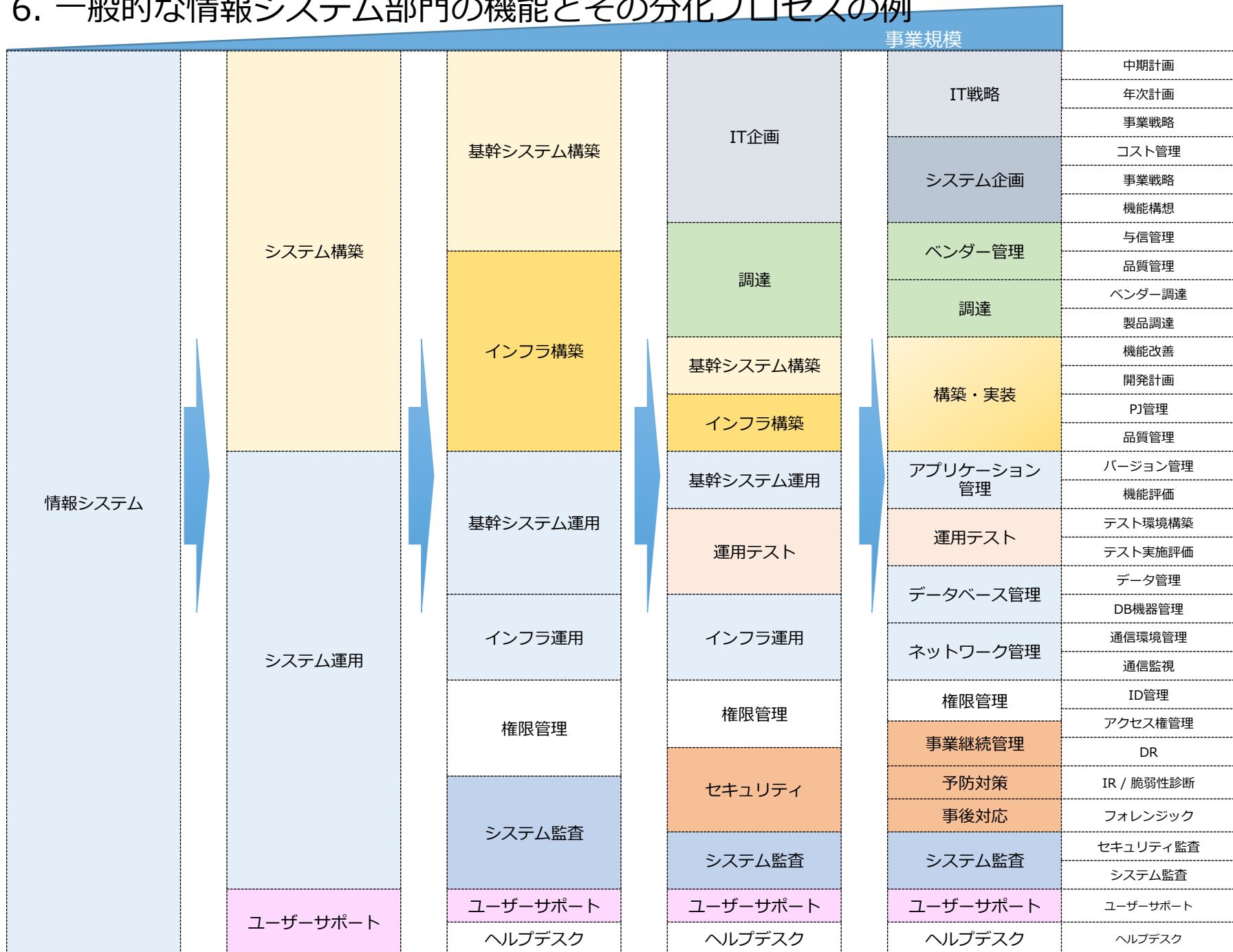


5. 一般的な管理部門の機能とその分化プロセスの例

- リスク発生時には、企業における管理部門がその対応を管理していくことが多い。
- 製造や営業部門との連携を行うために、それぞれの部門がどのような業務を担っているのか整理してみる。

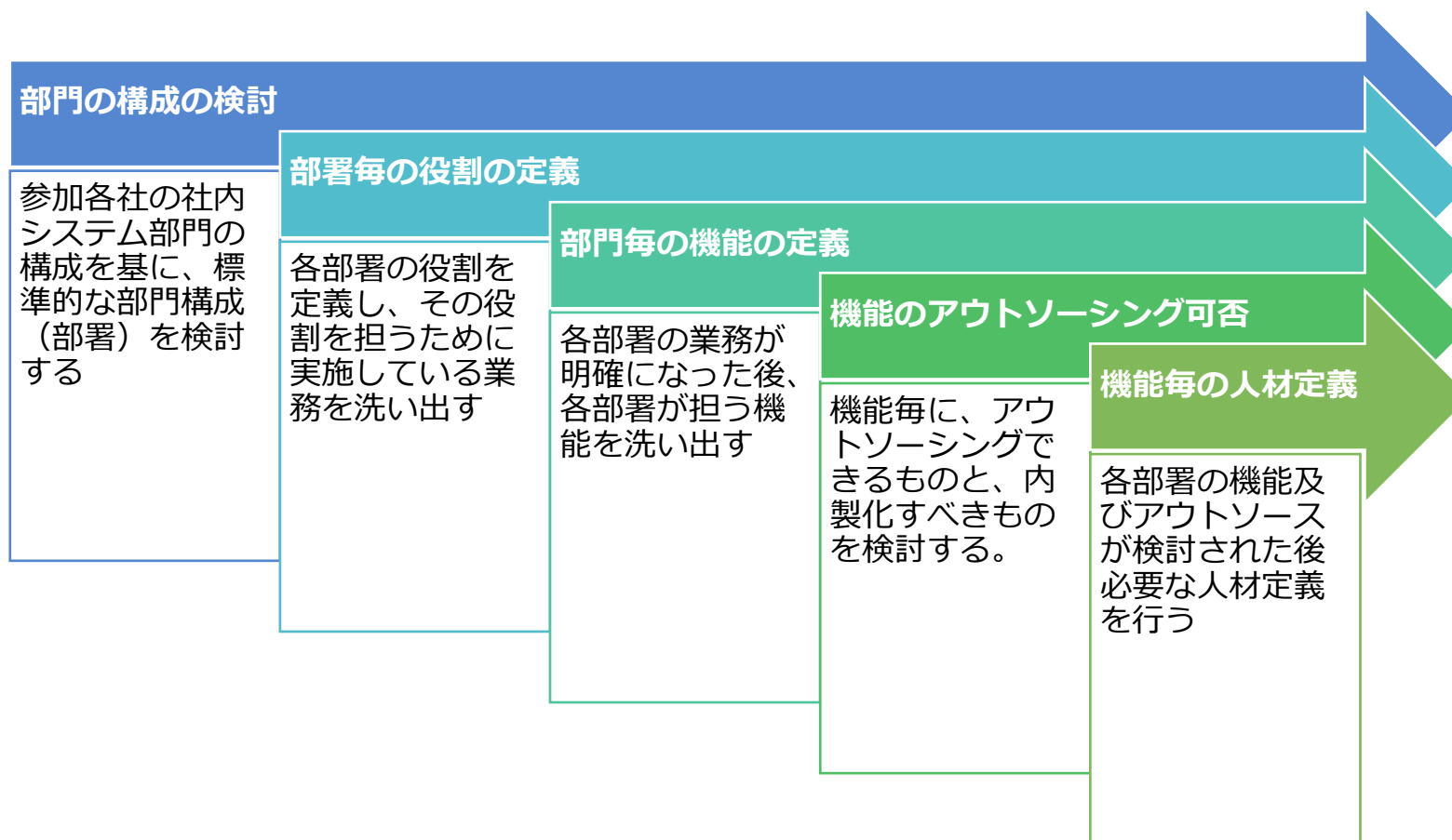


6. 一般的な情報システム部門の機能とその分化プロセスの例



7. 人材定義にむけた検討プロセス

- 現在のシステム部門の役割や機能を分析することにより、必要となる人材を検討する。
- ユーザー企業としてセキュリティ対策すべてを担うのではなく、ユーザー企業に求められる機能を洗い出して、更にアウトソーシング可能な事項を選別した後、社内に必要な人材を定義していく。



8. 各社組織分析(日本企業におけるセキュリティ業務)※本検討会調べ

情報システム部門の機能分化の例

部門	機能	機能詳細	セキュリティ (概念の提供)	運用・保守
IT企業	IT業務	セキュリティ対策 中期計画	1 1 情報保証コンプライアンス	
IT企業	IT業務	セキュリティ対策 年次計画	1 1 情報保証コンプライアンス	
IT企業	IT業務	セキュリティ対策 事業戦略	1 1 情報保証コンプライアンス	
IT企業	IT業務	セキュリティ対策 事業戦略		
IT企業	システム企画	セキュリティ対応 コスト管理	1 4 システム要件計画	
IT企業	システム企画	セキュリティ対応 事業戦略	1 4 システム要件計画	
IT企業	システム企画	セキュリティ対応 機能検証	1 2 ソフトウェア保証とエンジニアリング	
IT企業	システム企画	セキュリティ対応 機能検証	1 6 技術研究開発	
セキュリティ	事業戦略	IT-BCP		
セキュリティ	事業戦略	ディザスタリカバリ		
セキュリティ	予防対策	情報セキュリティ/ISMS	1 1 情報保証コンプライアンス	
高齢システム構築	構築・実装	セキュリティ 機能改善	1 5 システムセキュリティアーキテクチャ	
高齢システム構築	構築・実装	セキュリティ導入 ・開発計画Ⅰ	1 4 システム要件計画	
高齢システム構築	構築・実装	セキュリティ導入 ・開発計画Ⅱ	1 5 システムセキュリティアーキテクチャ	
インフラ構築	構築・実装	セキュリティ対応 PJ管理	1 3 システム開発	
インフラ構築	構築・実装	セキュリティサービス ・製品 品質管理	1 7 試験と評価	
高齢システム運用	アプリケーション管理	アプリケーション バージョン管理	1 2 ソフトウェア保証とエンジニアリング	
高齢システム運用	アプリケーション管理	セキュリティ製品 機能評価Ⅰ		2 5 システムアドミニストレーション
高齢システム運用	アプリケーション管理	セキュリティ製品 機能評価Ⅱ	1 5 システムセキュリティアーキテクチャ	2 6 システムセキュリティ分析
インフラ運用	データベース管理	データ管理Ⅰ		2 2 データアドミニストレー

※セキュリティ機能が
多数の部門に分散

9. 各社組織分析(日本企業におけるセキュリティ業務)※本検討会調べ

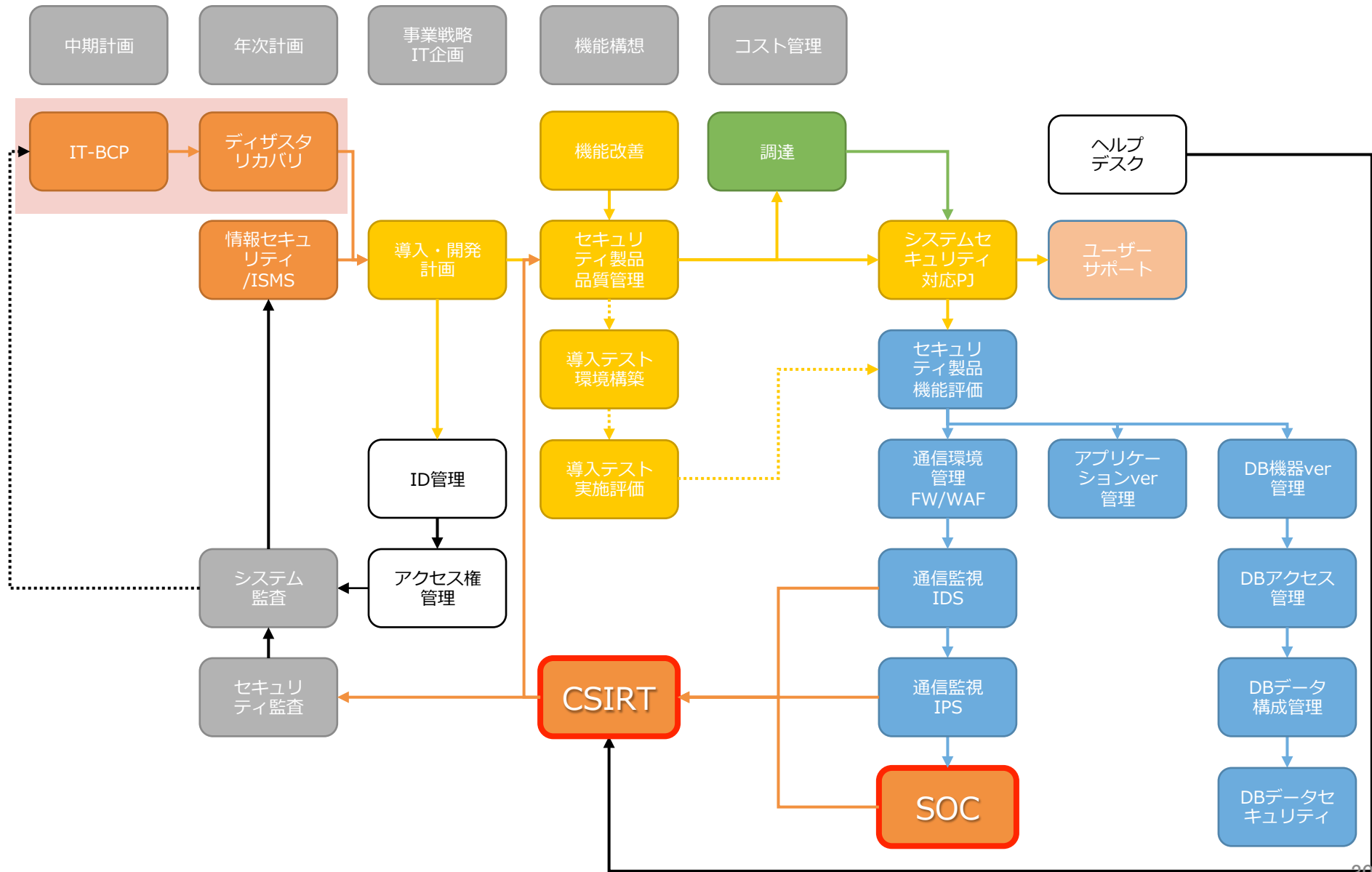
情シス部門のセキュリティ機能

NICE/サイバーセキュリティ教育イニシアティブ

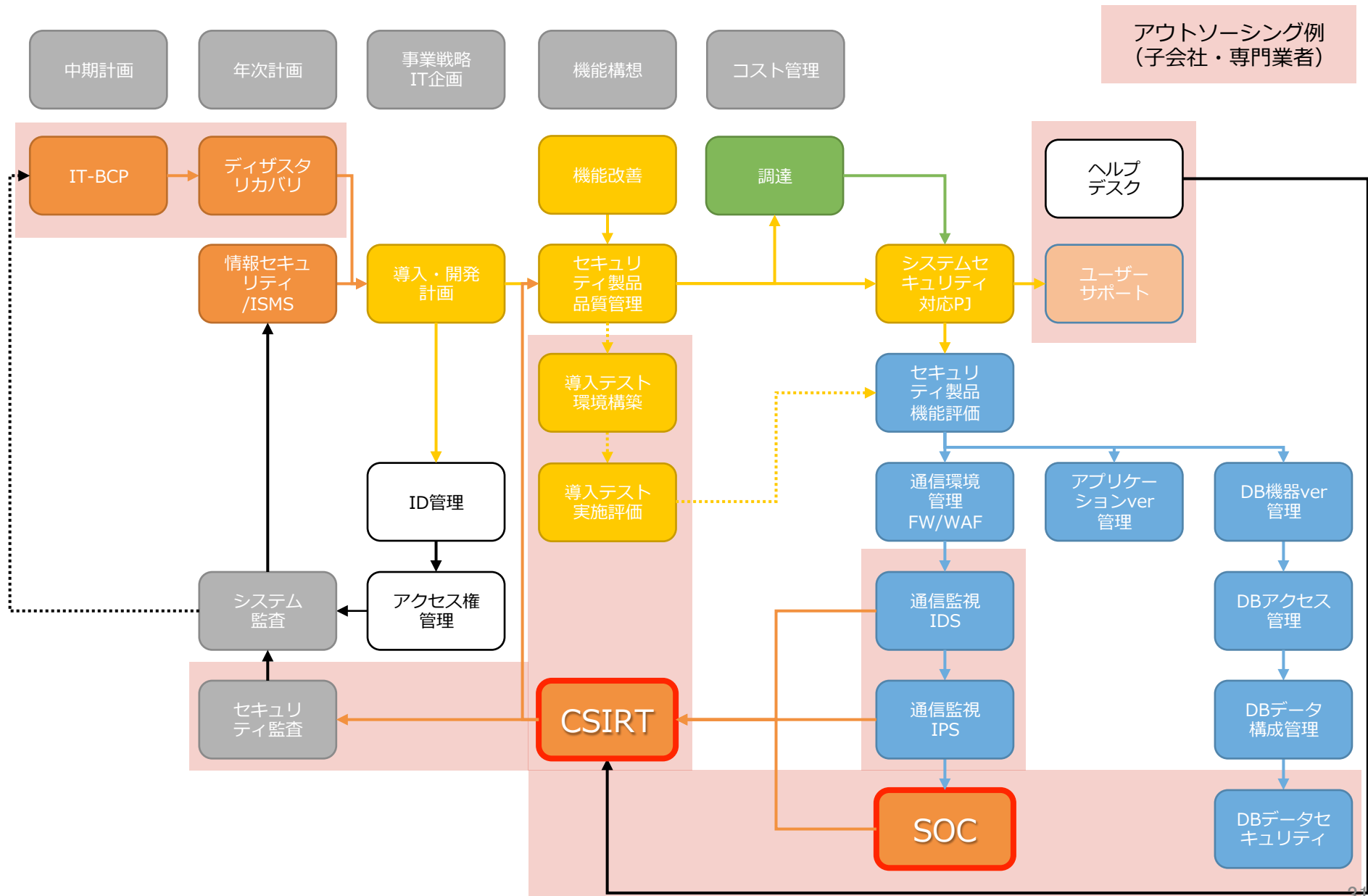
サイバーセキュリティフレームワーク/NIST

情報システム部門の機能分化の例				NICE / サイバーセキュリティ教育イニシアティブ										NIST / サイバーセキュリティフレームワーク									
部門	機能	機能詳細	セキュリティ(種別の提供)	運用・保守	守備・防衛	検知	対応	運用・情報収集	分析	監視と開発	ID	特定	IP	対応	DE	検知	CS	RC	RC	検定			
1	IT企画	IT戦略	セキュリティ対策 の推進	1	1	1	1	1	1	1	BE	ビジネス環境											
1	IT企画	IT戦略	セキュリティ対策 の推進	1	1	1	1	1	1	1	BE	ビジネス環境											
1	IT企画	IT戦略	セキュリティ対策 の推進	1	1	1	1	1	1	1	OV	ガバナンス											
1	IT企画	IT戦略	セキュリティ対策 の推進	1	1	1	1	1	1	1	RM	リスク管理											
1	IT企画	システム企画	セキュリティ対策 の推進	1	4	1	1	1	1	1	BE	ビジネス環境									RP		
1	IT企画	システム企画	セキュリティ対策 の推進	1	4	1	1	1	1	1	RM	リスク管理	IP	情報収集	CH	検知	CS	RC	RC	検定	RP		
9	セキュリティ	事業継続	IT-BCP								RM	リスク管理	IP	情報収集	CH	検知	CS	RC	RC	検定	RP		
9	セキュリティ	事業継続	ディザスタリカバリ								RM	リスク管理	IP	情報収集	CH	検知	CS	RC	RC	検定	RP		
9	セキュリティ	予防対策	情報セキュリティ/目標5								RM	リスク管理	IP	情報収集	CH	検知	CS	RC	RC	検定	RP		
3	基幹システム構築	構築・実施	セキュリティ の推進	1	5						RA	リスクマネジメント	PT	保護技術									
3	基幹システム構築	構築・実施	セキュリティ導入 の推進	1	4						RM	リスク管理											
3	基幹システム構築	構築・実施	セキュリティ導入 の推進	1	5						RA	リスクマネジメント											
4	インフラ構築	構築・実施	セキュリティ対策 の推進	1	3						RM	リスク管理	AT	保護技術									
4	インフラ構築	構築・実施	セキュリティ対策 の推進	1	7						RA	リスクマネジメント											
5	基幹システム運用	アプリケーション の推進	セキュリティ対策 の推進	1	2						AM	資産管理	MA	保守							IM		
5	基幹システム運用	アプリケーション の推進	セキュリティ対策 の推進	1	2						RA	リスクマネジメント											
5	基幹システム運用	アプリケーション の推進	セキュリティ対策 の推進	1	5						RA	リスクマネジメント	PT	保護技術									
7	インフラ運用	データベース の推進	セキュリティ対策 の推進	2	2						RA	リスクマネジメント	DS	データセキュリティ							IM		
7	インフラ運用	データベース の推進	セキュリティ対策 の推進	2	3						IP	情報収集											
7	インフラ運用	データベース の推進	セキュリティ対策 の推進	1	7						MA	保守									IM		
7	インフラ運用	データベース の推進	セキュリティ対策 の推進	1	5						MA	保守									IM		
7	インフラ運用	ネットワーク の推進	セキュリティ対策 の推進	1	5						MA	保守									IM		
7	インフラ運用	ネットワーク の推進	セキュリティ対策 の推進	1	5						MA	保守									IM		
9	セキュリティ	予防対策	SO								RA	リスクマネジメント	IP	情報収集	CH	検知	CS	RC	RC	検定	CO		
6	運用テスト	運用テスト	セキュリティ対策 の推進	1	7						PT	保護技術											
6	運用テスト	運用テスト	セキュリティ対策 の推進	1	7						PT	保護技術											
8	権限管理	権限管理	ID管理								IP	情報収集											
8	権限管理	権限管理	アクセス管理								AC	アクセス制御											
11	ユーザーサポート	ユーザーサポート	ユーザーサポート								AT	保護技術											
11	ユーザーサポート	ヘルプデスク	ヘルプデスク								AT	保護技術											
9	セキュリティ	予防対策	情報収集活動/POC								CH	検知									CO		
9	セキュリティ	事業継続	インシデントハンドラー								RA	リスクマネジメント	AE	異常イベント							IM		
9	セキュリティ	事業継続	インシデントハンドラー								RM	リスク管理	AE	異常イベント	IM	検定					IM		
9	セキュリティ	事業継続	インシデントハンドラー								RM	リスク管理	AE	異常イベント	IM	検定					IM		
9	セキュリティ	事業継続	インシデントハンドラー								PT	保護技術	DP	検知プロセス	AN	分析							
9	セキュリティ	事業継続	インシデントハンドラー								AT	保護技術									AN		
9	セキュリティ	事業継続	インシデントハンドラー																		AN		
2	訓練	ハンダー訓練	セキュリティ対策 の推進																				
2	訓練	ハンダー訓練	セキュリティ対策 の推進																				
2	訓練	ハンダー訓練	セキュリティ対策 の推進								AM	資産管理	AT	保護技術									
2	訓練	ハンダー訓練	セキュリティ対策 の推進								AM	資産管理											
14	システム監査	システム監査	セキュリティ監査																		CO		
14	システム監査	システム監査	システム監査																		CO		

10. 機能分布モデル(日本企業におけるセキュリティ機能の分布) ※本検討会調べ

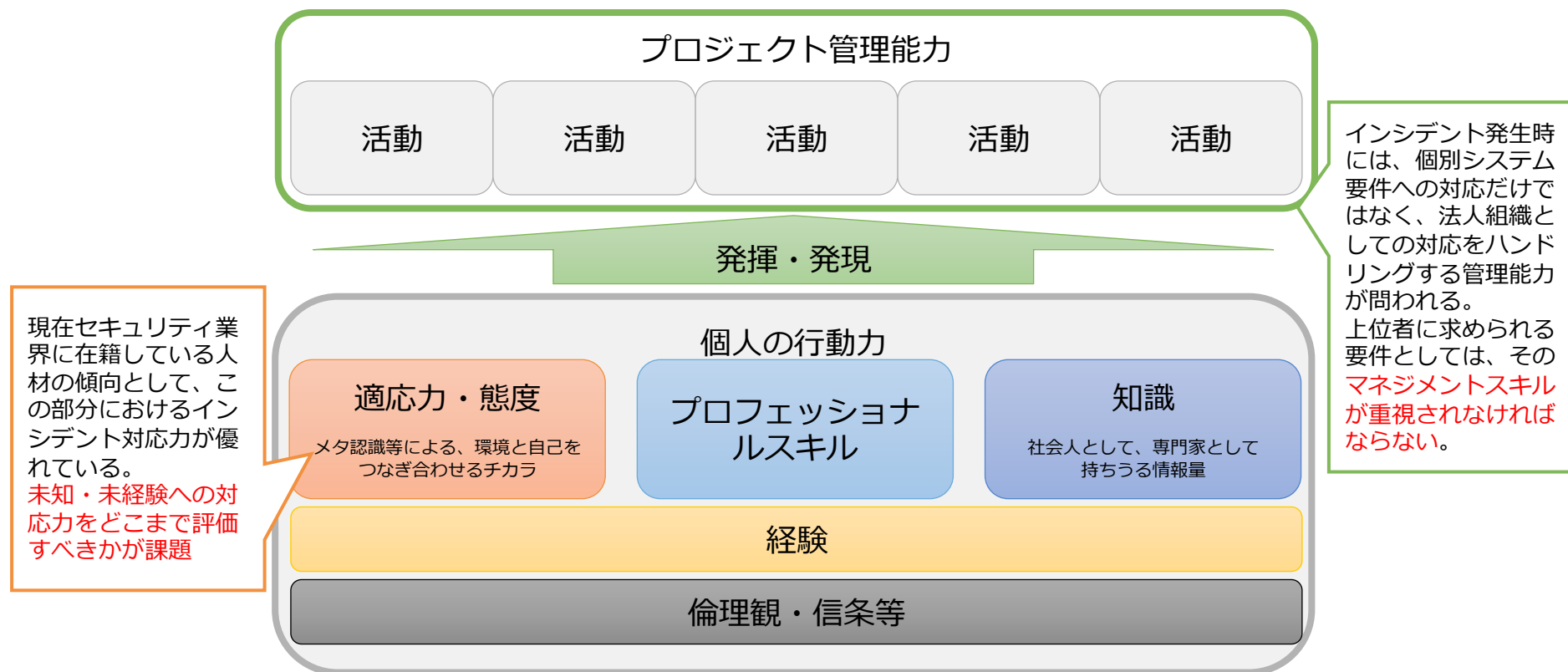


11. 機能分布モデル(日本企業におけるセキュリティ機能の分布) ※本検討会調べ



12. 企業におけるセキュリティ人材定義にむけて評価の考え方

- IT業界での人材評価の取り組みにおける課題は、成果と行動の測定が含まれていない
 - スキルマップに依存した能力評価は「プロフェッショナルスキル（技術力）」偏重となり、外部環境や個別システムへの適応力やプロジェクト稼働率、メンタルヘルス等の影響により想定される成果とのズレが生じている。
 - セキュリティベンダー等の専門環境に従事する企業・人材が策定する「プロフェッショナルスキル（技術力）」の指標では、理想像は描けても、実際の現在就業するエンジニアに展開することが難しい。
 - 「冰山モデル」を参考とした、セキュリティ人材の評価イメージ



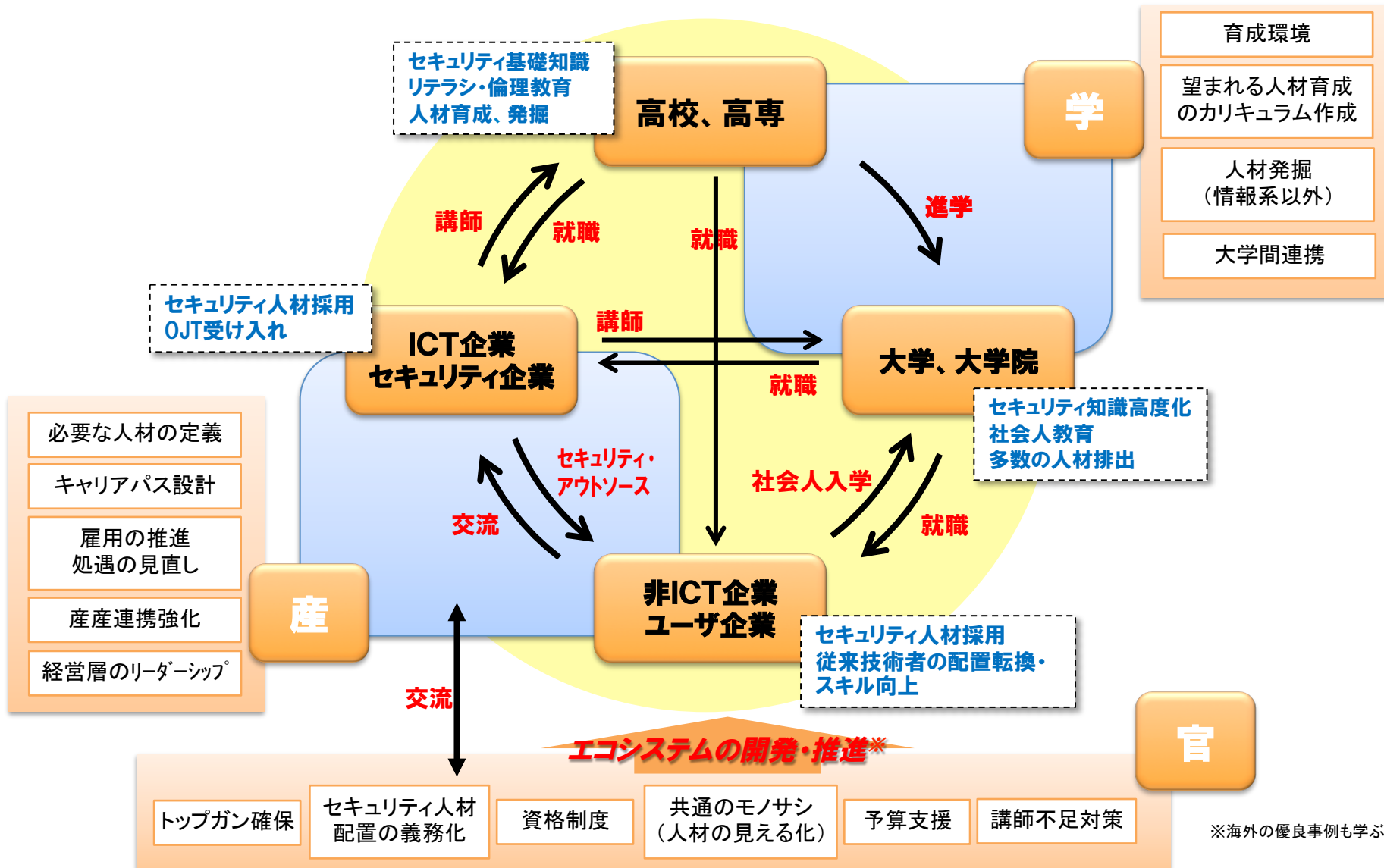
13. これまでの検討から得られた知見

- **産業界(特にユーザ企業)の現場視点が重要**
 - 分散したセキュリティ業務をまとめると新たな職種が導き出せる可能性
⇒ セキュリティ雇用増につながる専任管理者(専門職)の育成
 - まとめられないセキュリティ業務は依然、現場対応が必要
⇒ 本来業務の中でセキュリティも分かる人材の育成
⇒ 各組織の一般管理者に対するセキュリティ知識レベル底上げ
- **日本企業が必要とする人材の多様性**
 - ICT企業と非ICT系ユーザ企業の違い
 - CSO、CISOの在り方を考え直す
 - CISOを支える“橋渡し人材”の必要性
 - アウトソースとインソース
 - 人材育成・維持のためのエコシステム
 - 産学連携の在り方

4. 産官学連携とエコシステム

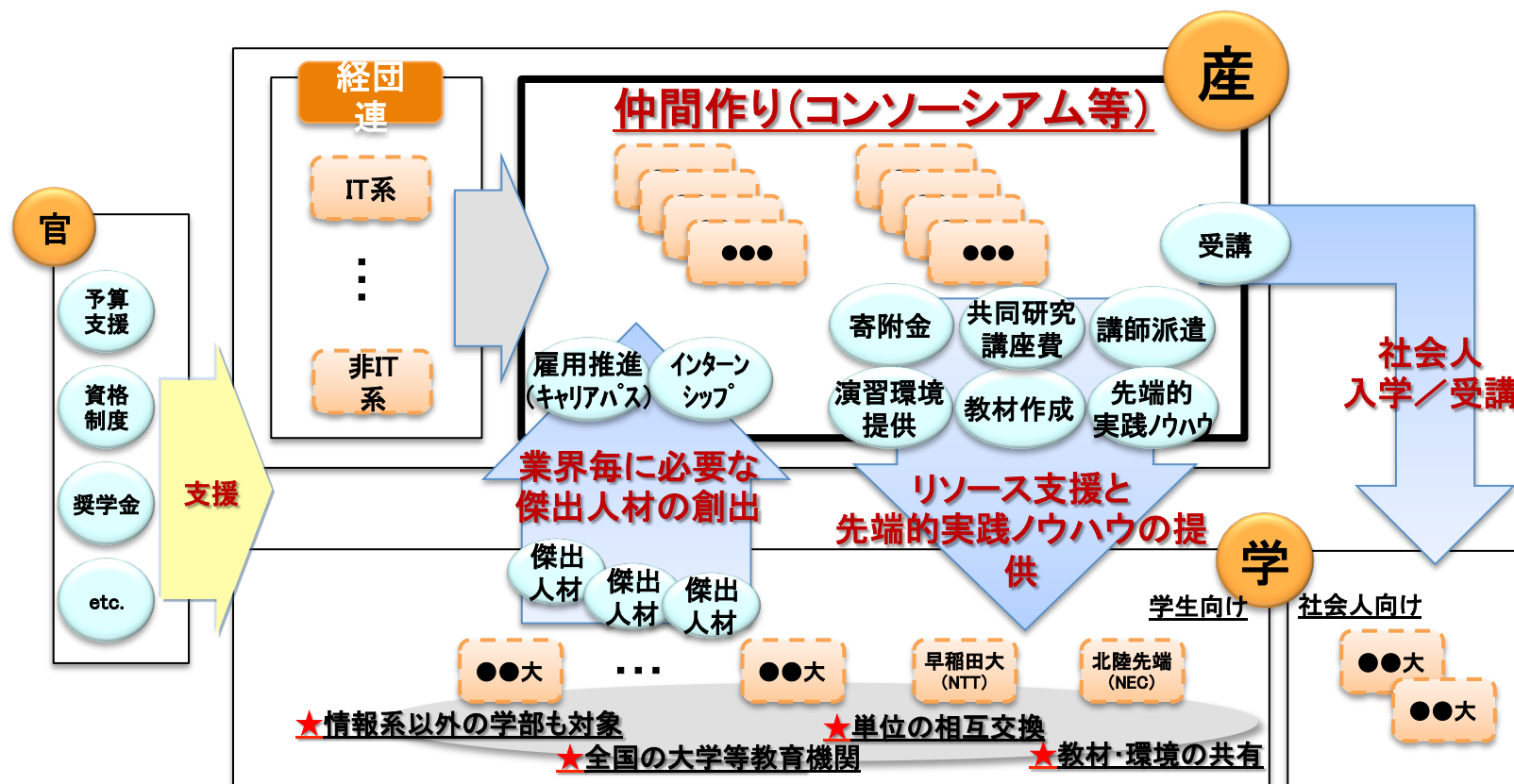
1. サイバーセキュリティ人材育成・維持 エコシステム (検討中イメージ)

ユーザ企業においても雇用・活用に結びつく人材定義と人材育成・維持に向けて



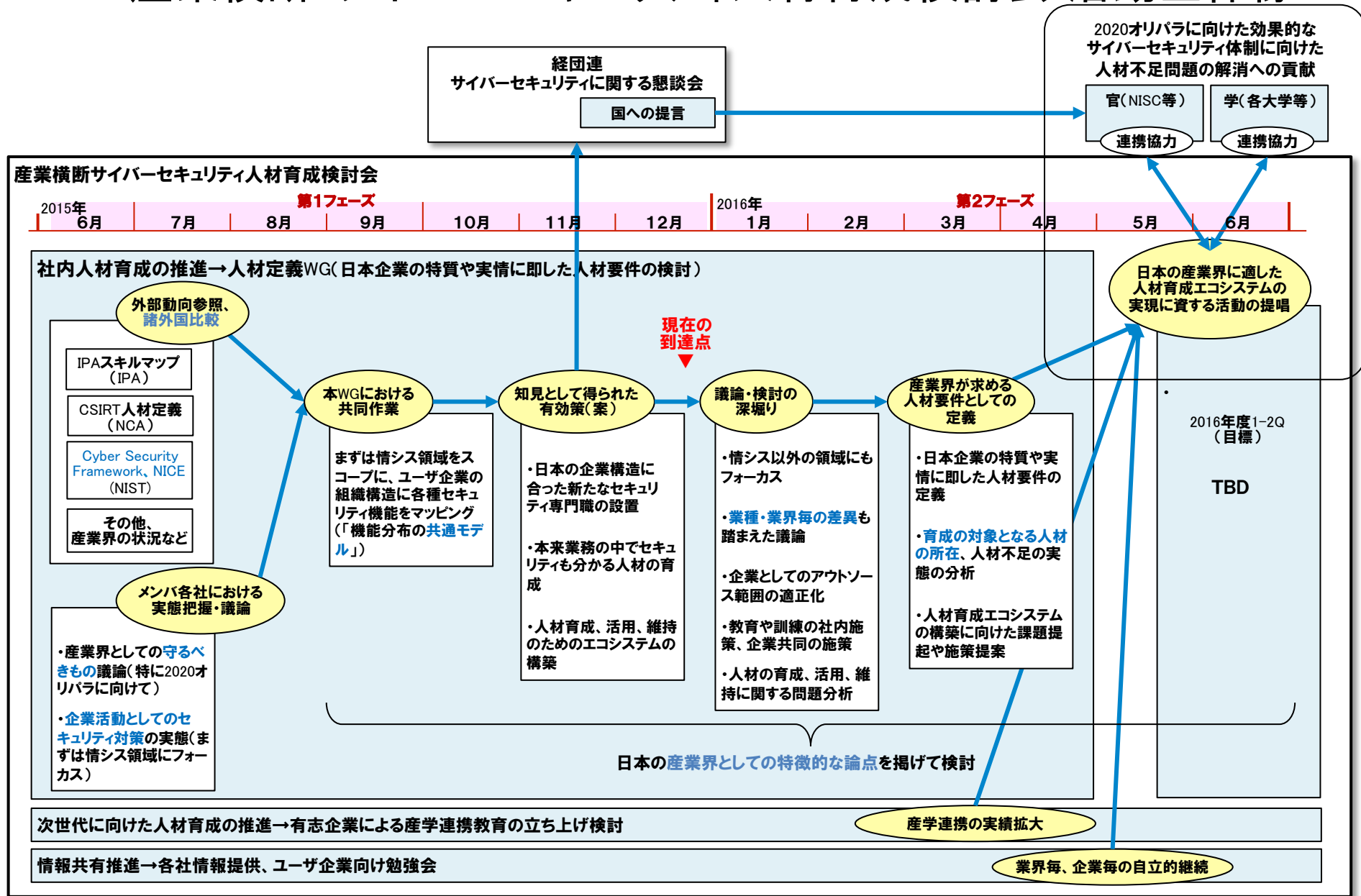
2. 産学連携の在り方(検討中イメージ)

- 2015年度はメンバー企業の寄付講座など、教育機関との連携をとりまとめ、来年度に向けた産業界として一貫性ある取り組み方を検討中。
- 大学に限らず高専との連携も有効と考え検討中。



5. 今後の活動について

1. 産業横断 サイバーセキュリティ人材育成検討会 活動全体像



2. 今後の予定(案): ~2016年度上期

- 業界毎および階層別の具体的人材定義へ拡張。
- 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。
- 日本の産業界・企業の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エコシステムの具体案を検討・提唱。

【以下についても継続】

- 社内人材育成に関する共同取り組みを検討・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。