# 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

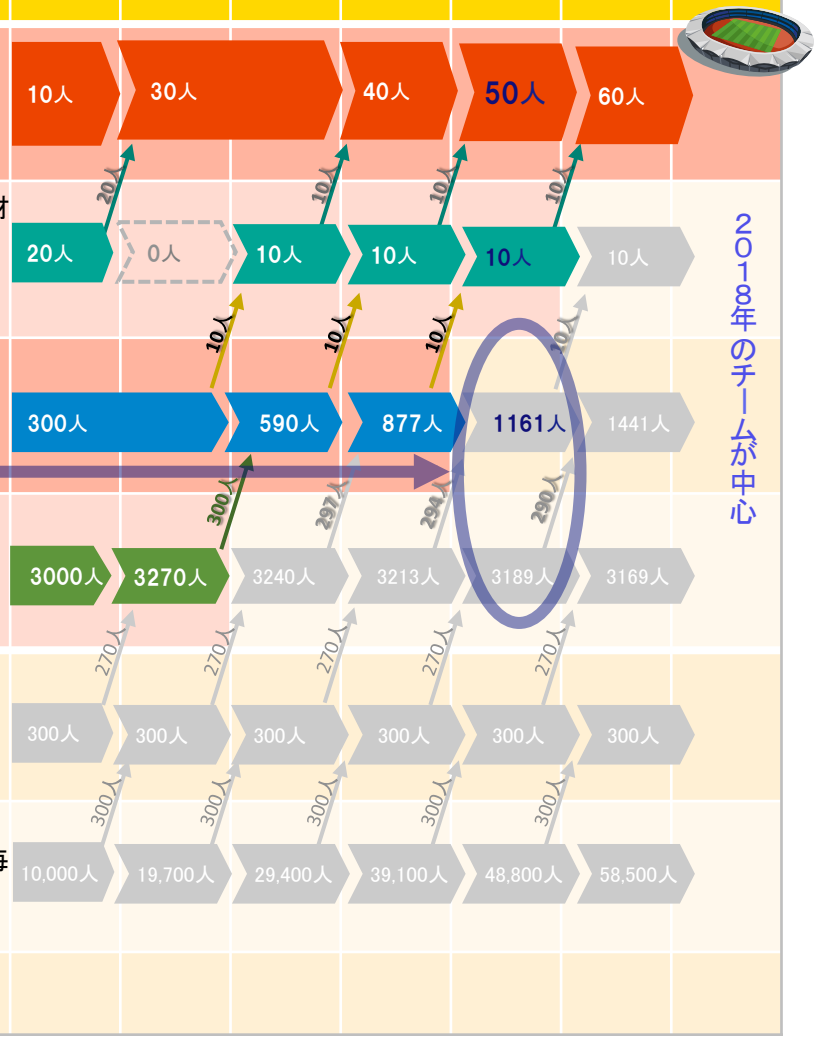
1. セキュリティ人材についての考察（2年前～）
2. 産業横断検討会について
3. 企業にとってのセキュリティ人材
4. 産官学連携とエコシステム
5. 今後の活動について

# 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

| スキルレベル | 現状での人材数<br>（想定人数の算定方法） | 上位スキルレベルへの<br>昇格イメージ |
|---|---|---|
| トップガン | 現在10人以下<br>（セキュリティベンダーの中でも突出した専門スキルを有するスーパー人材。各社0人～2人） | － |
| トップガン補佐<br>（トップガンへの研修） | 現在20人<br>（セキュリティに強いITベンダー10数社に在籍する人材。各社1～2人程度存在すると仮定） | トップガン補佐になった人材は100%トップガンに育成 |
| 中間層エリート | 現在300人<br>（ITベンダーTOP50社、1社当たり6人程度存在すると仮定） | 中間層エリートから有望な人材を毎年10人程度トップガン補佐として選抜 |
| 中間層 | 現在3000人<br>（従業員数3000人規模の上場企業トップ100社において、従業員の1%が中間層のセキュリティ運用者と仮定） | 10%程度が中間層エリートに昇格 |
| 中間層の卵<br>（セキュリティ技術者として採用） | （300人採用／年）<br>（ITベンダーTOP50社の中間層エリートが部下1名を雇用し、OJT指導すると仮定） | 90%程度が中間層に昇格<br>10%は職種変更 |
| 基礎教育修了者<br>（大学、大学院卒） | （10,000人輩出／年）<br>（理工系学部の上位200学部に在籍する学生、1学部50名程度育成と仮定） | 中間層の卵に昇格するかは企業の採用数に依存。毎年300人と仮置き |
| 卵（高専、大学） | | |



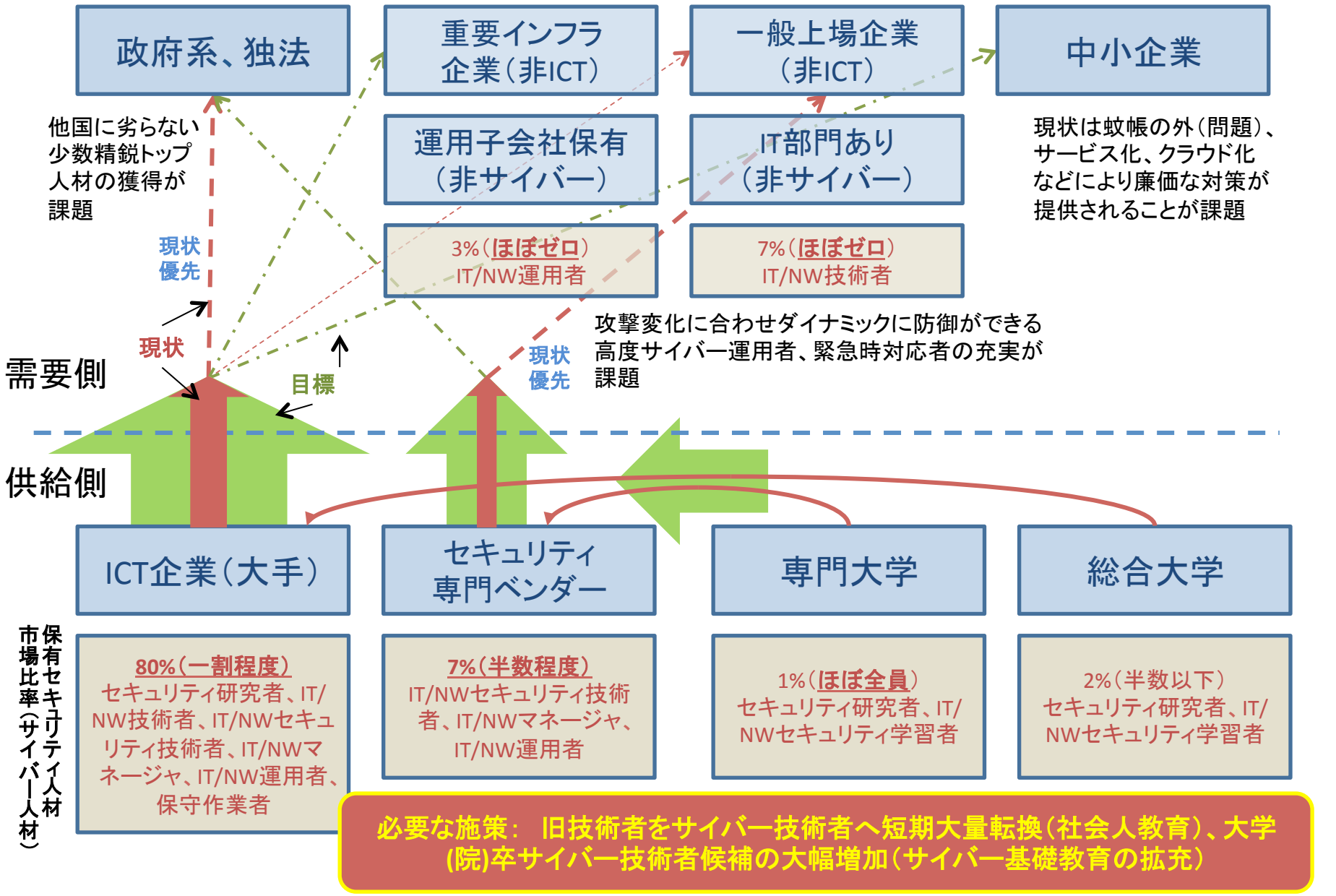

**2018年までに実働部隊（中間層エリート・中間層）を如何に増やせるかがカギ**

# 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いない？

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

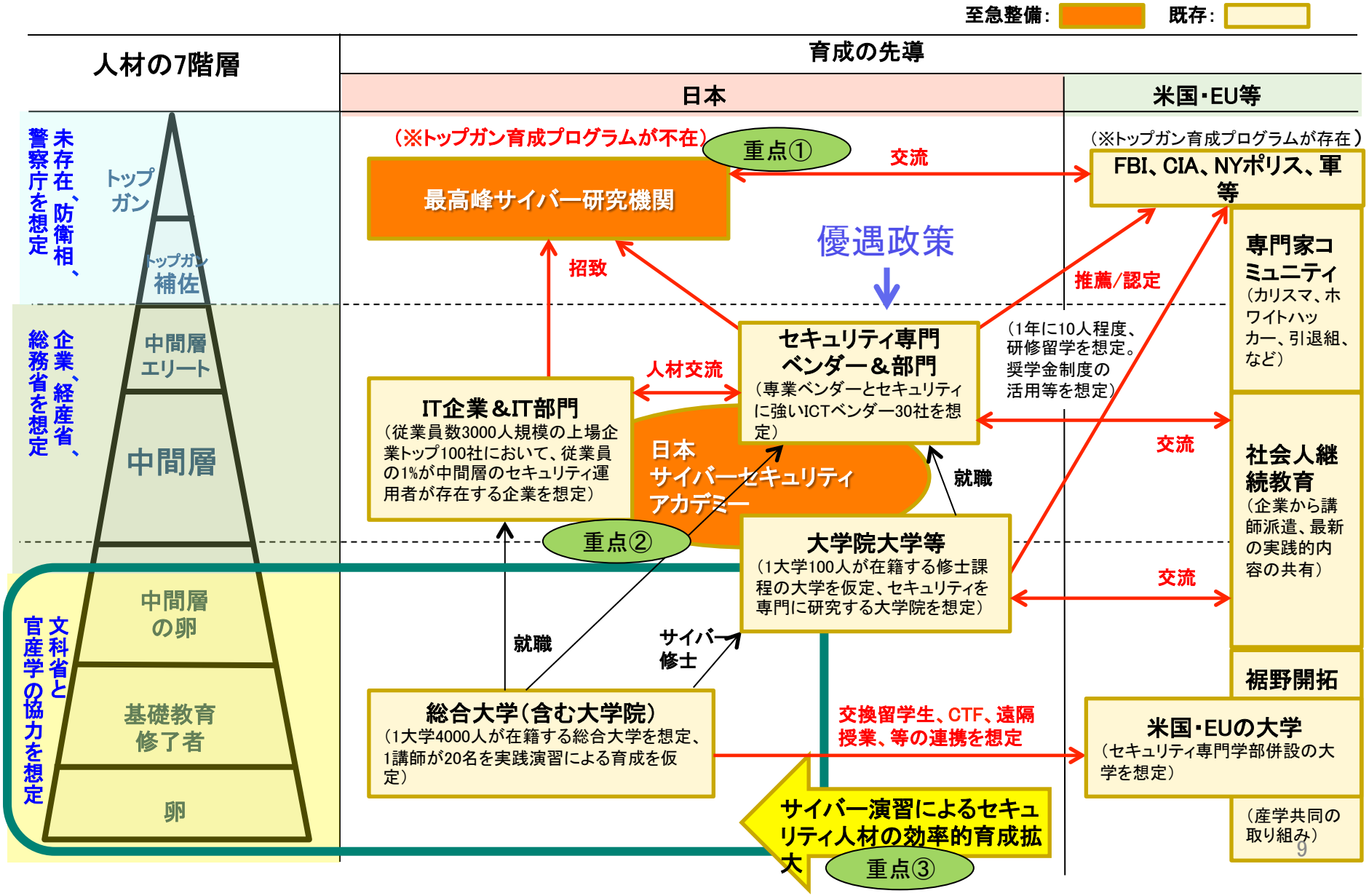
- 育成シミュレーションを行ったとき、大手企業ならどこでもサイバー技術者育成候補がいると考えていた。大きな誤解だと思い知った。

- ほとんどの組織（非ICT企業、中小、政府、自治体・・・）には候補がいない
- 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



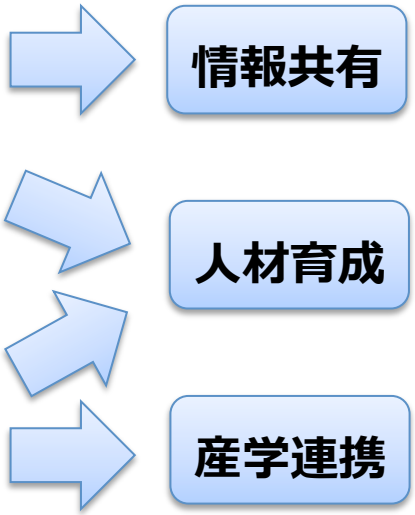
# 2. 産業横断検討会について

# 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



# 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

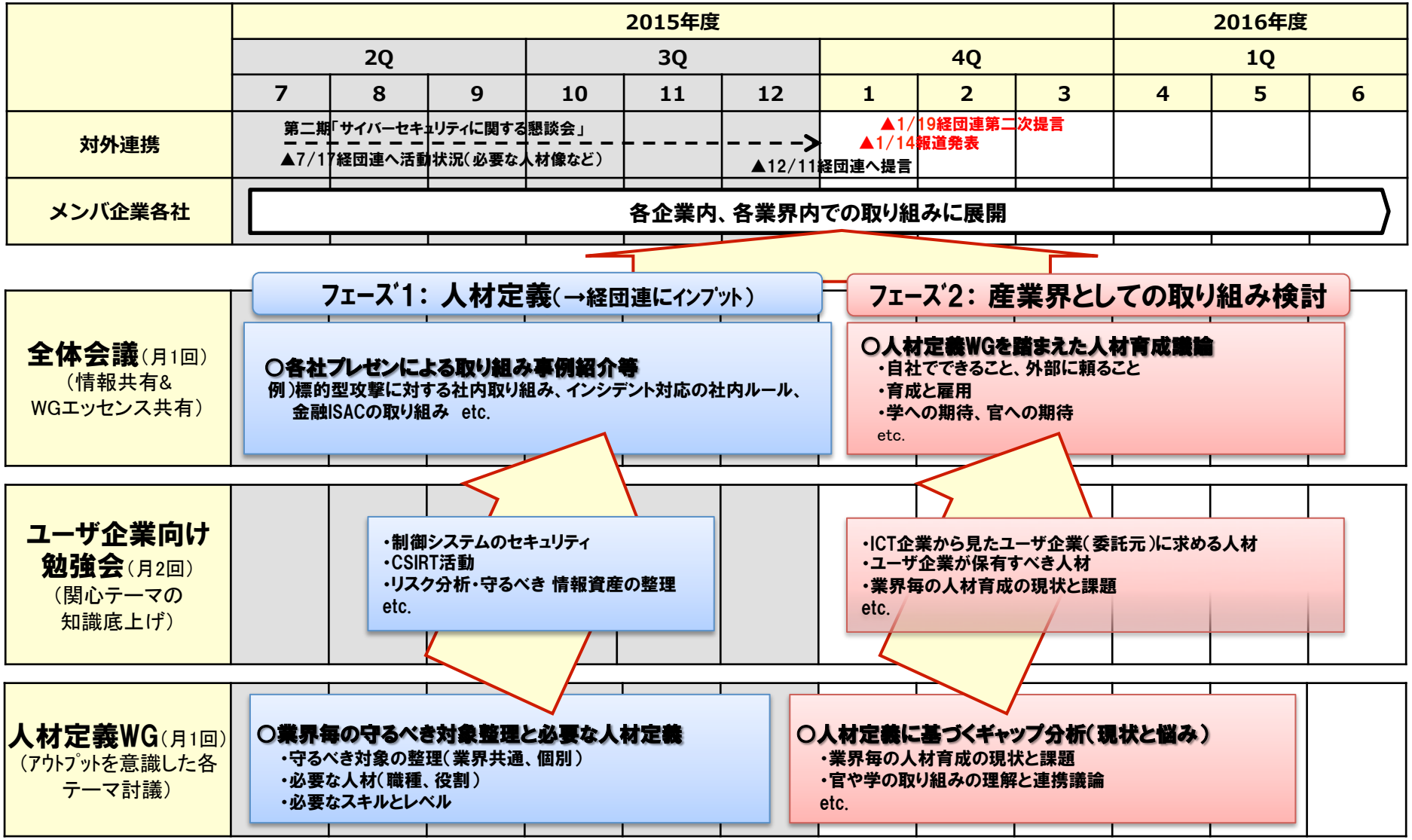
- ユーザ企業間のコミュニティ形成、ユーザ企業ならではの悩みを共有
- セキュリティ対策のアプローチ、方策に関する勉強会開催

### 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



# 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。

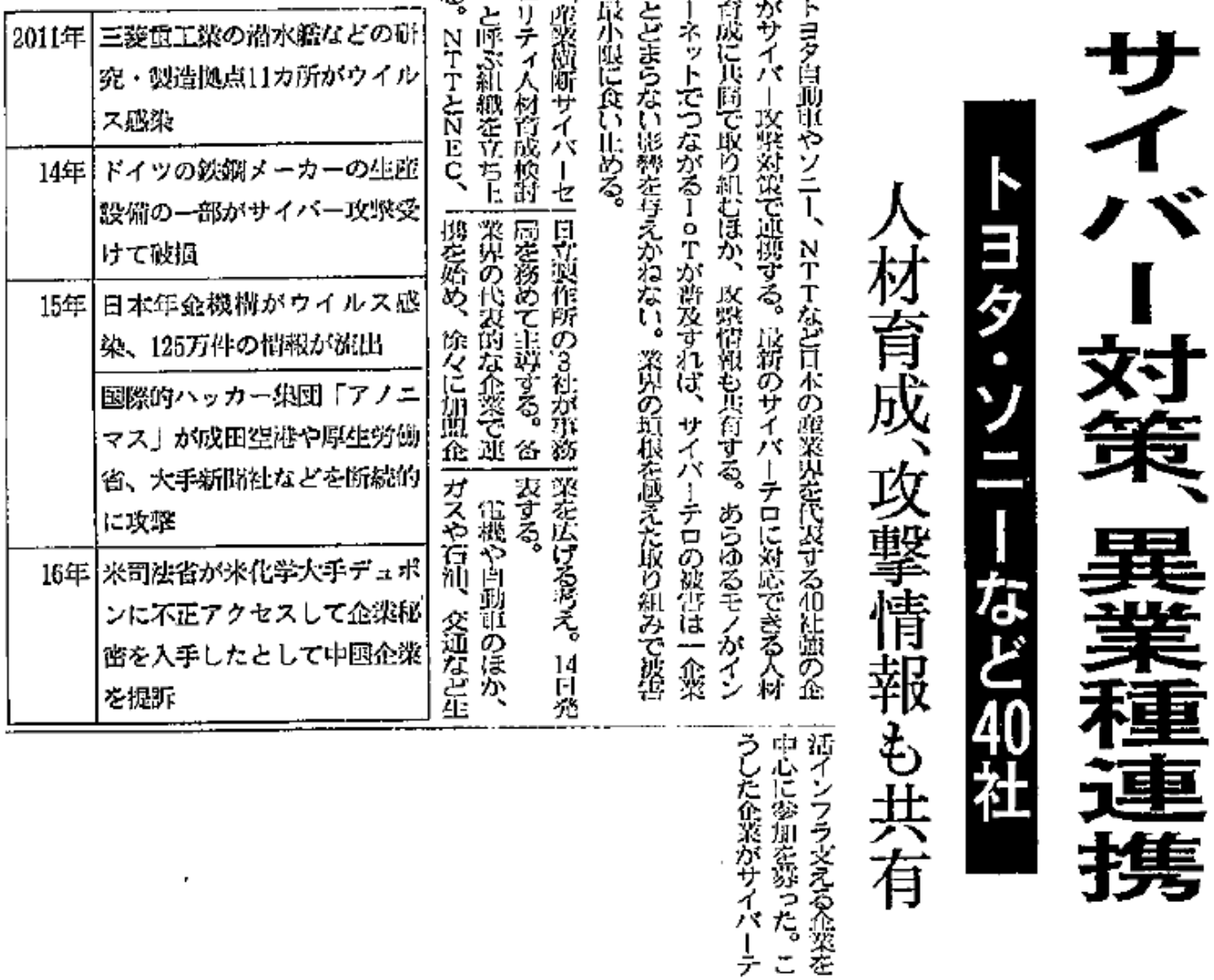
① 情報共有の推進

## ＜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）



# サイバー対策、異業種連携

## トヨタ・ソニーなど40社

## 人材育成、攻撃情報も共有

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。

「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る。NTTとNEC、日立製作所の3社が事務局を務めて主導する。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。

電機や自動車のほか、ガスや石油、交通など生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

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カ所がウイルス感染 |
| 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受けて破損 |
| 15年 | 日本年金機構がウイルス感染、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 |

# 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 ）
日本電信話株式会社
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

# 8. 中間報告書の掲載HP

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

# 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

# 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

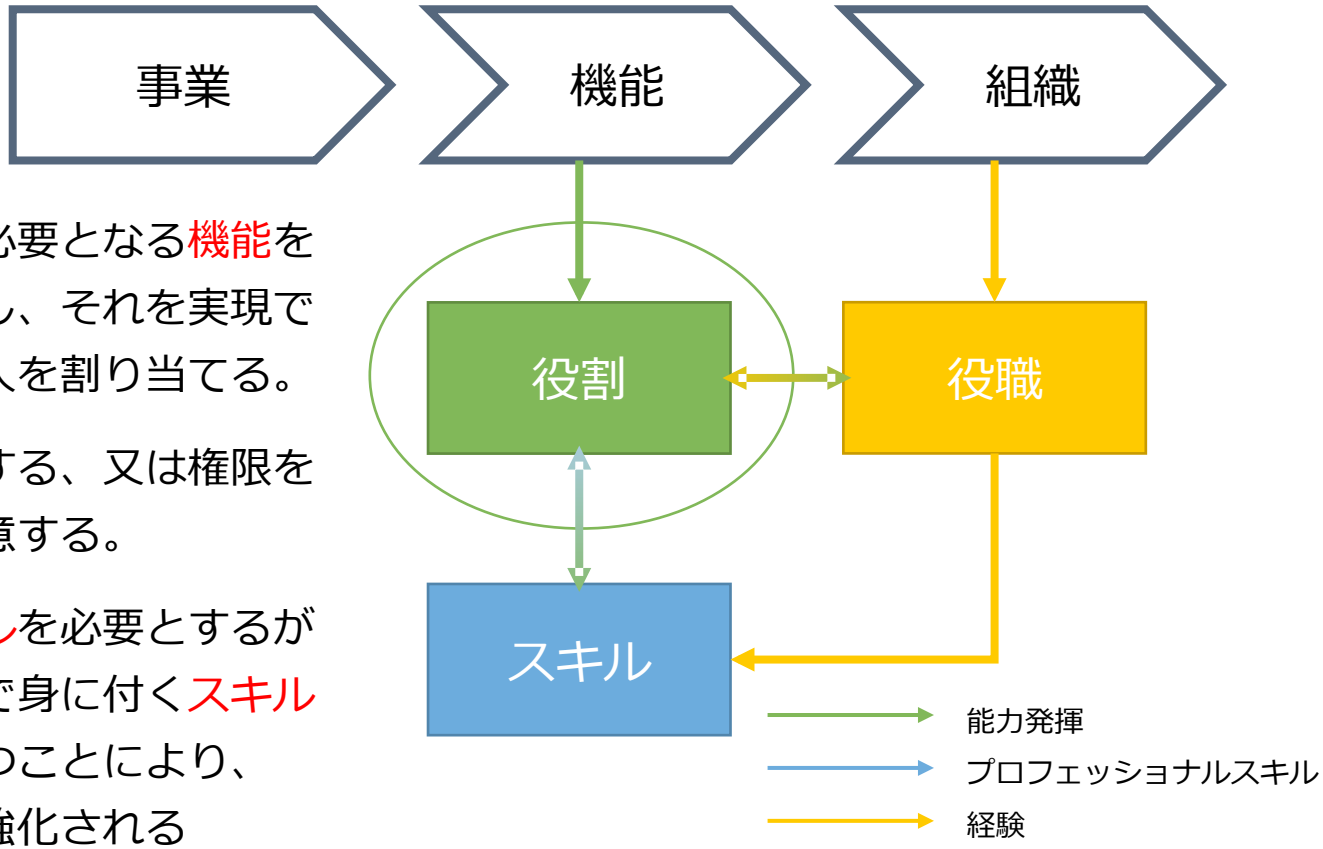
## 2. 日本企業におけるサイバーセキュリティ人材の定義に向けて

### 【考慮すべき日本企業の特性・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

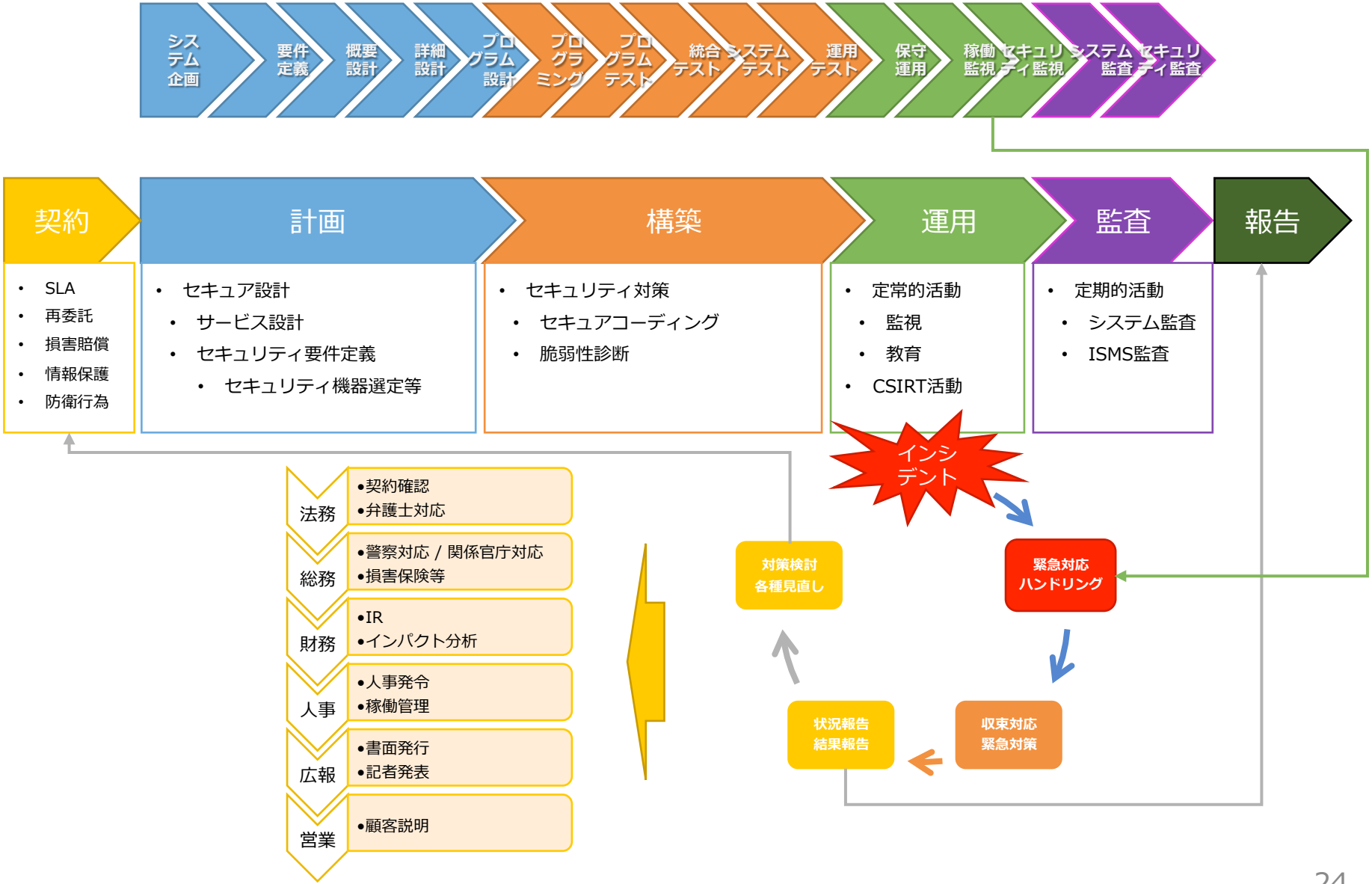
- 組織と人材の関係を考え、機能から役割とスキルを明確にする
- 優秀な人材とは、役割を担うことができる人材であり、それを環境及び個人の観点から実現可能にしていくことが、人事管理の重要なポイントである。
- 組織運営の観点から、役割・役職・スキルの関連を整理すると




- 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

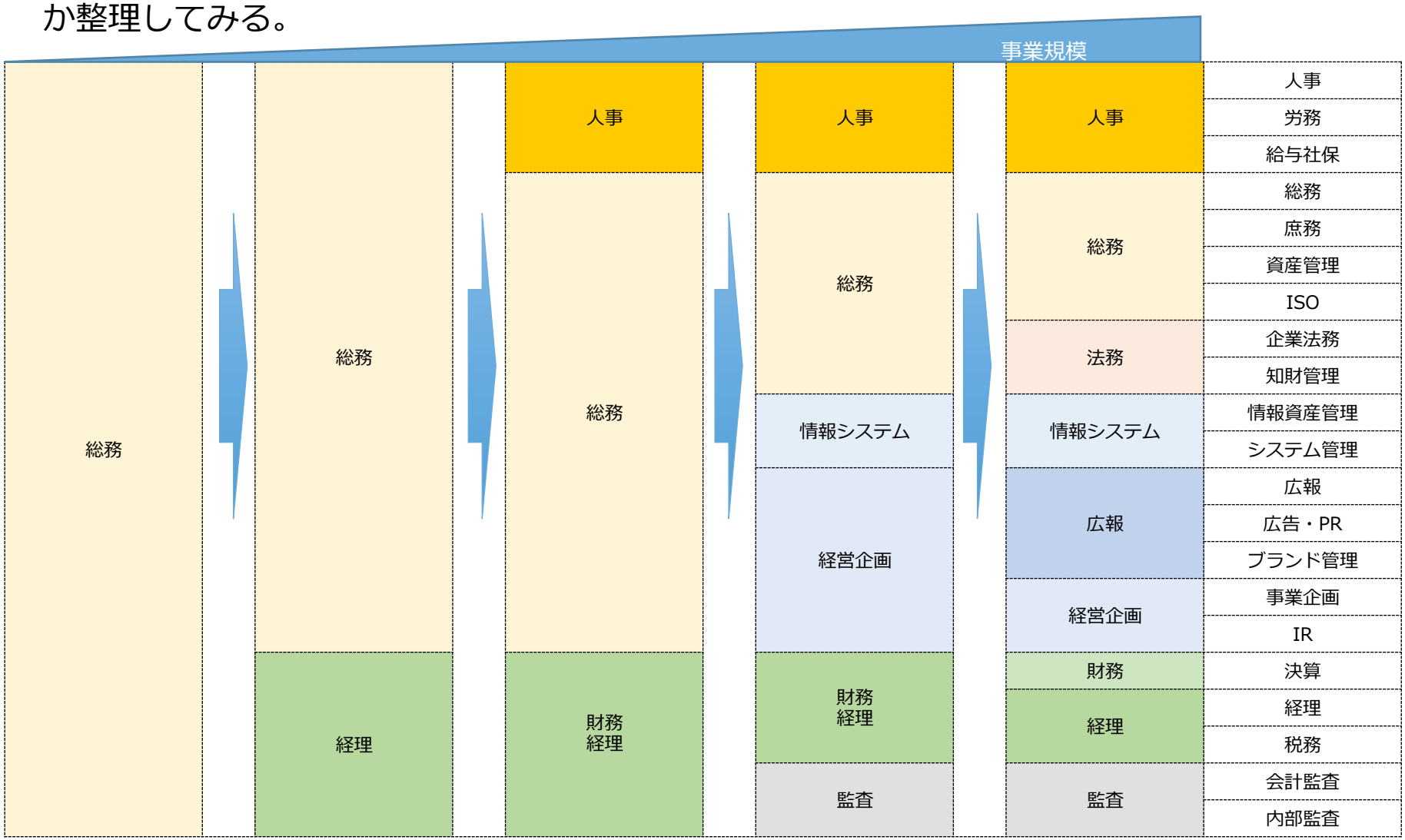
# 4. サイバーセキュリティ対策のプロセスを整理する（例

- システム開発・運用プロセスから

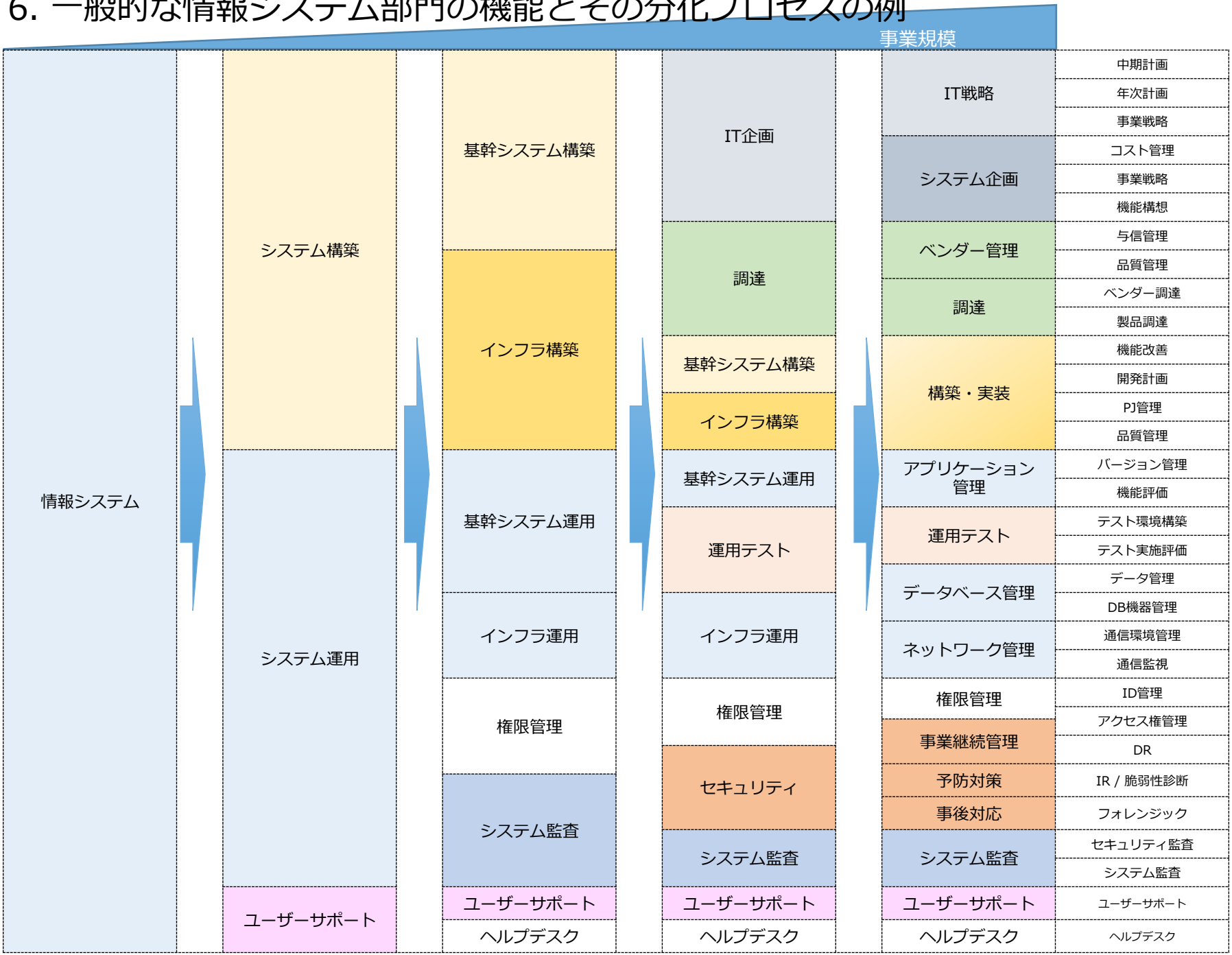


# 5. 一般的な管理部門の機能とその分化プロセスの例

- 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。

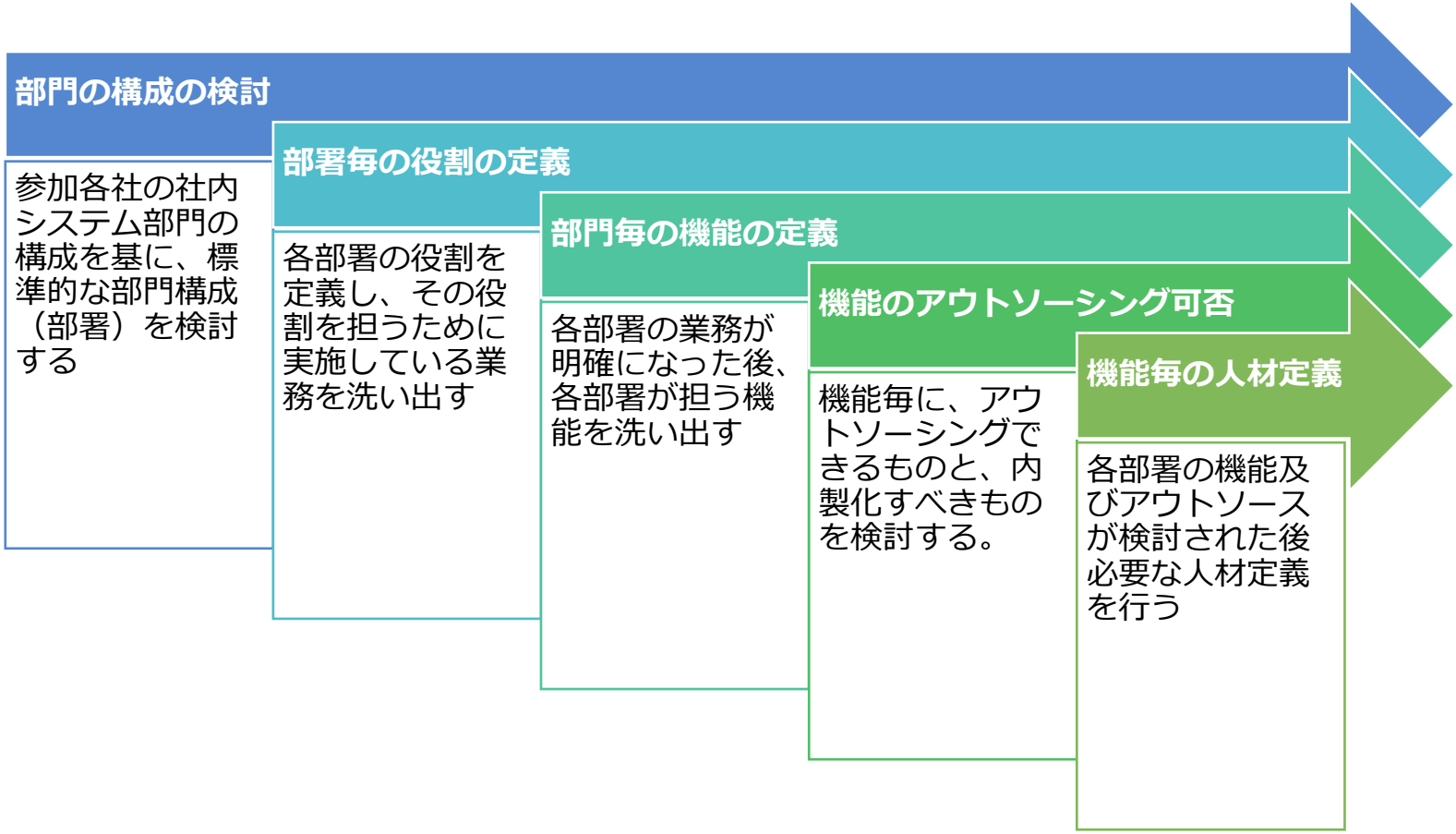


# 6. 一般的な情報システム部門の機能とその分化プロセスの例

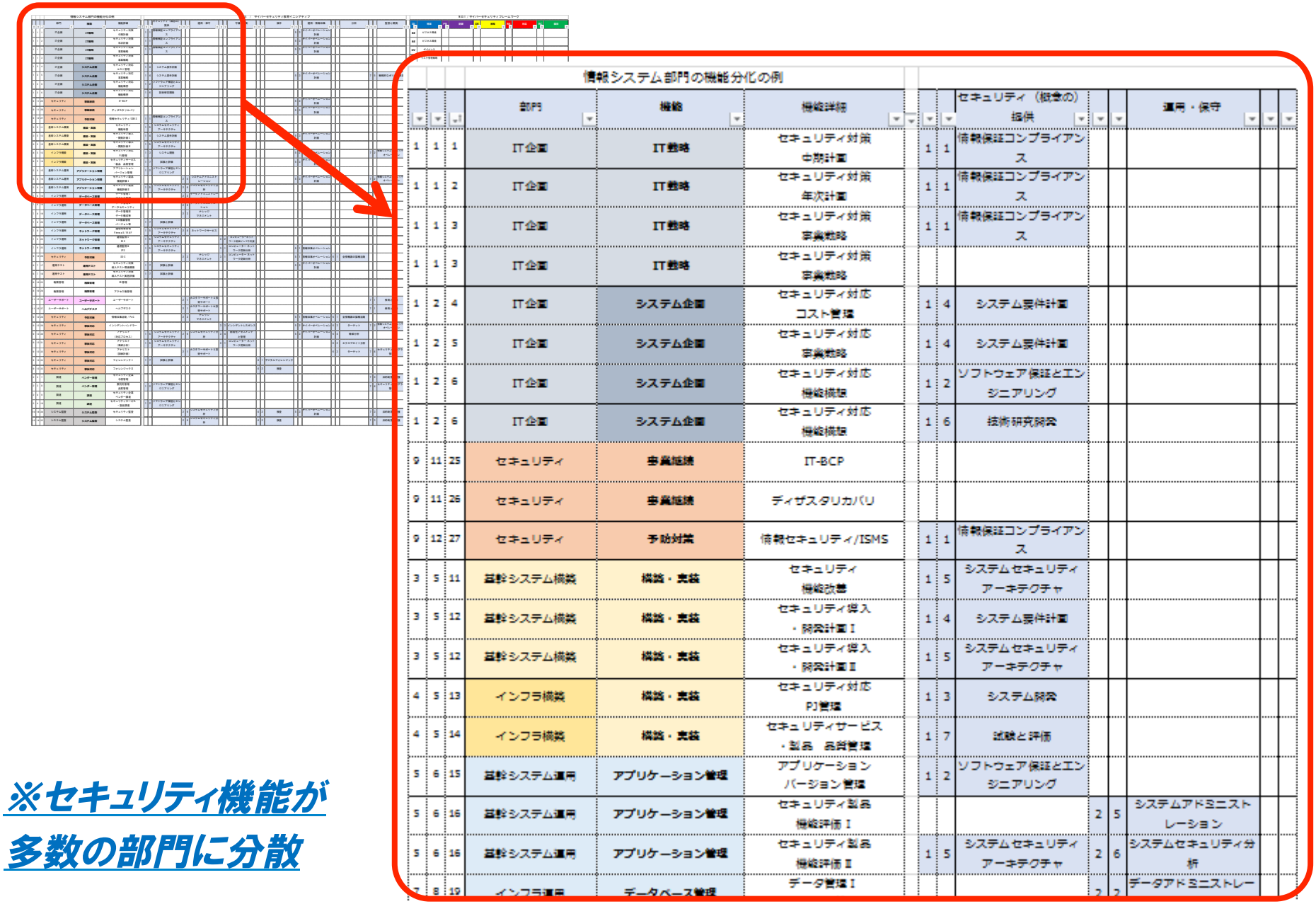


# 7. 人材定義にむけた検討プロセス

- 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



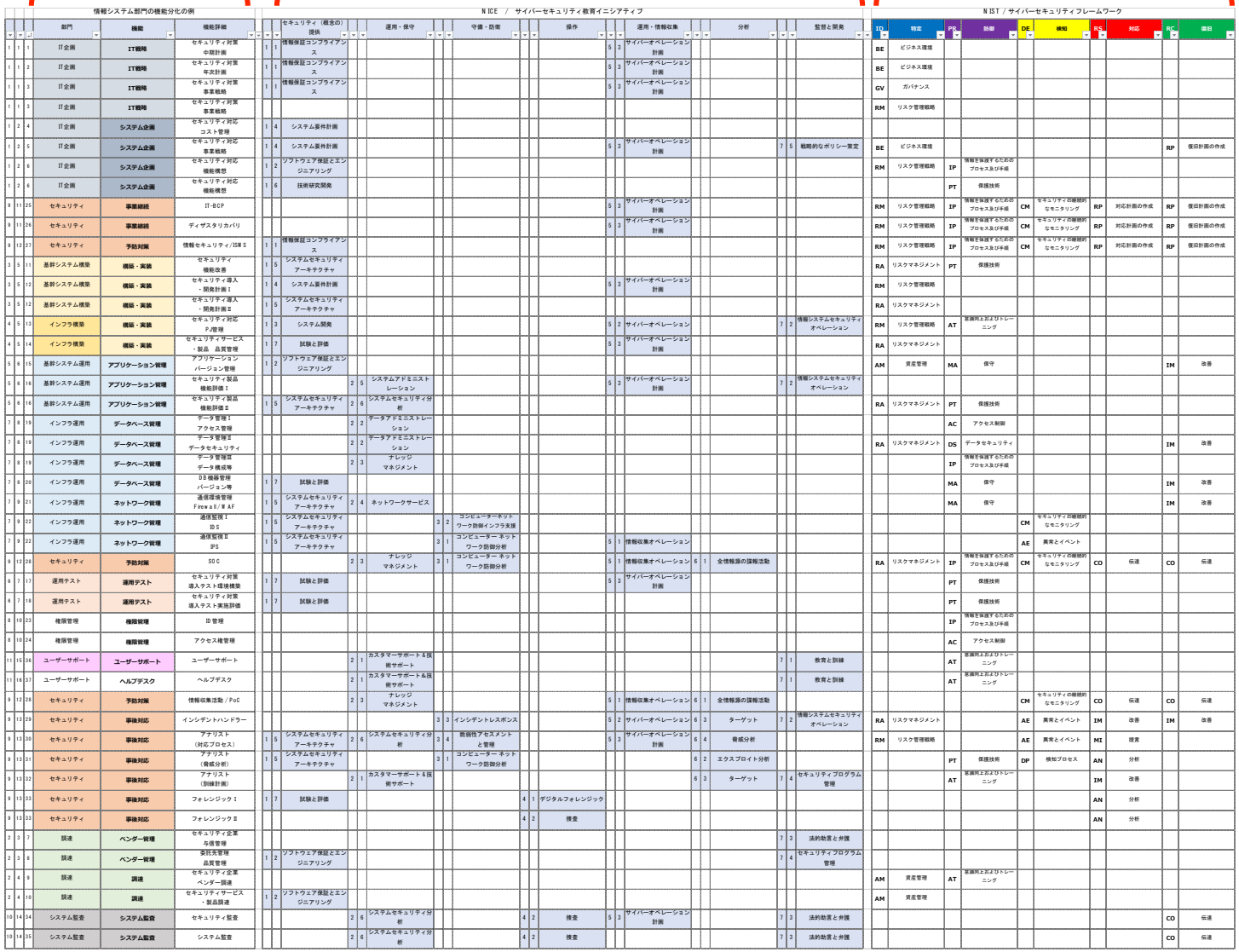
情報システム部門の機能分化の例

| | | | 部門 | 機能 | 機能詳細 | | | セキュリティ（概念の）提供 | | | | 運用・保守 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | IT企画 | IT戦略 | 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 | | | | | | |
| 1 | 1 | 2 | IT企画 | IT戦略 | 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 | | | | | | |
| 1 | 1 | 3 | IT企画 | IT戦略 | 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 | | | | | | |
| 1 | 1 | 3 | IT企画 | IT戦略 | セキュリティ対策事業戦略 | | | | | | | | | |
| 1 | 2 | 4 | IT企画 | 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 | | | | | | |
| 1 | 2 | 5 | IT企画 | 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 | | | | | | |
| 1 | 2 | 6 | IT企画 | システム企画 | セキュリティ対応機能概観 | 1 | 2 | ソフトウェア保証とエンジニアリング | | | | | | |
| 1 | 2 | 6 | IT企画 | システム企画 | セキュリティ対応機能概観 | 1 | 6 | 技術研究開発 | | | | | | |
| 9 | 11 | 25 | セキュリティ | 事業施設 | IT-BCP | | | | | | | | | |
| 9 | 11 | 26 | セキュリティ | 事業施設 | ディザスタリカバリ | | | | | | | | | |
| 9 | 12 | 27 | 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 | | | | | | |
| 3 | 5 | 11 | 基幹システム機能 | 機器・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 | | | | | | |
| 3 | 5 | 12 | 基幹システム機能 | 機器・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 | | | | | | |
| 3 | 5 | 12 | 基幹システム機能 | 機器・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 | | | | | | |
| 4 | 5 | 13 | インフラ機能 | 機器・実装 | セキュリティ対応PJ管理 | 1 | 3 | システム開発 | | | | | | |
| 4 | 5 | 14 | インフラ機能 | 機器・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 | | | | | | |
| 5 | 6 | 15 | 基幹システム運用 | 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 | | | | | | |
| 5 | 6 | 16 | 基幹システム運用 | 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 | | | |
| 5 | 6 | 16 | 基幹システム運用 | 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 | | | |
| 7 | 8 | 19 | 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 | | | |

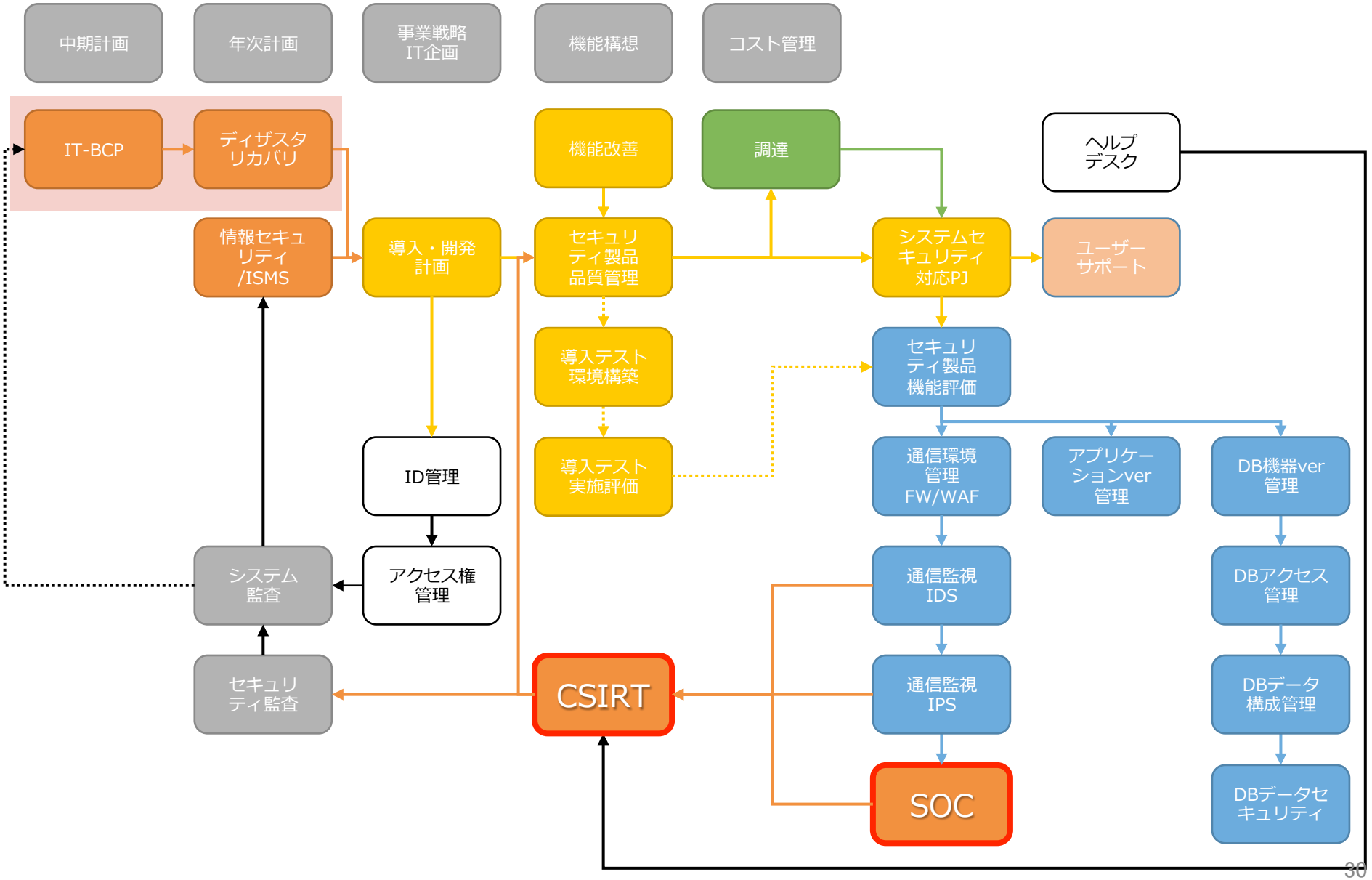
***※セキュリティ機能が多数の部門に分散***

# 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

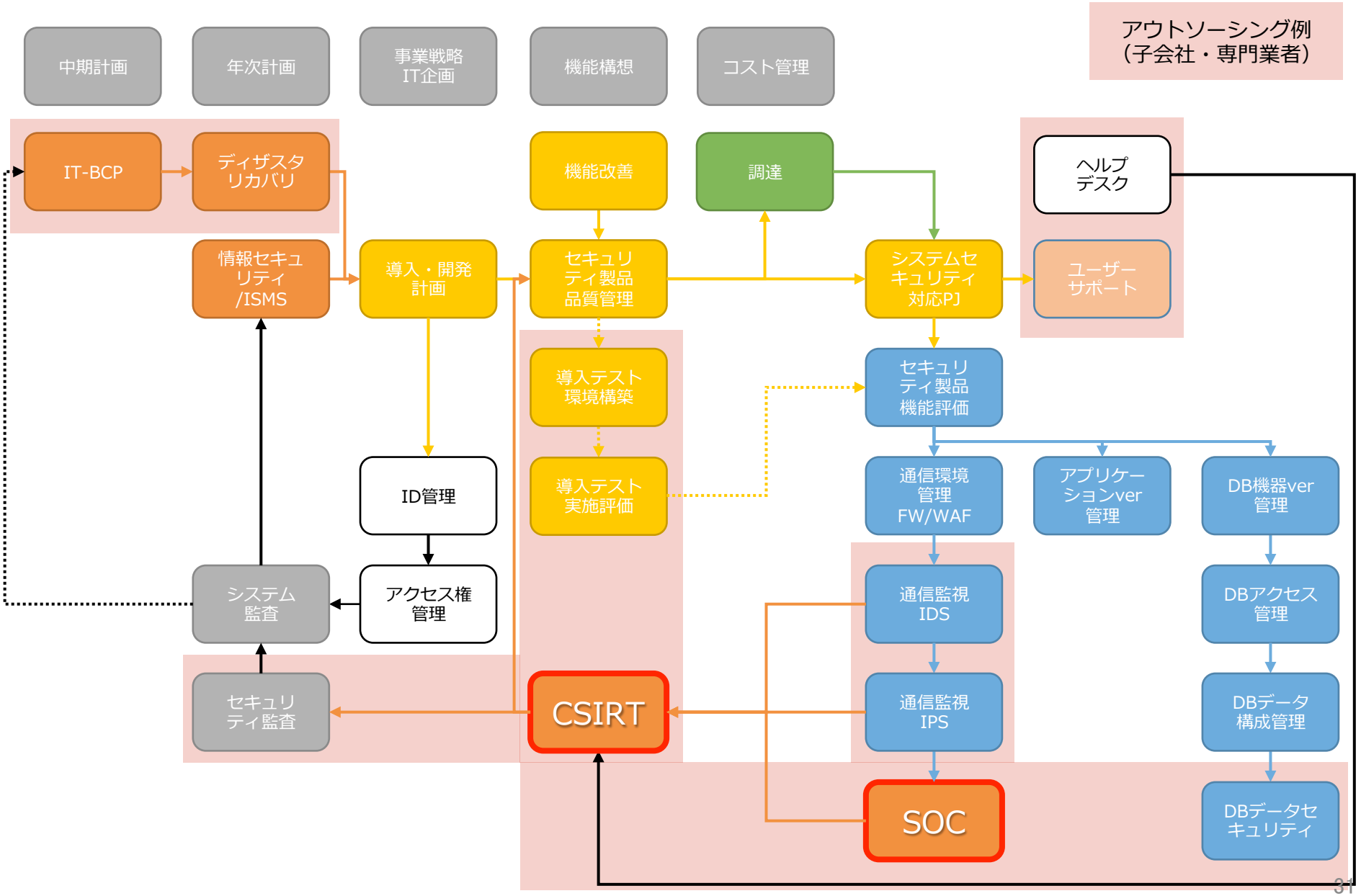
**情シス部門のセキュリティ機能**　　**NICE／サイバーセキュリティ教育イニシアティブ**　　**サイバーセキュリティフレームワーク／NIST**



# 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

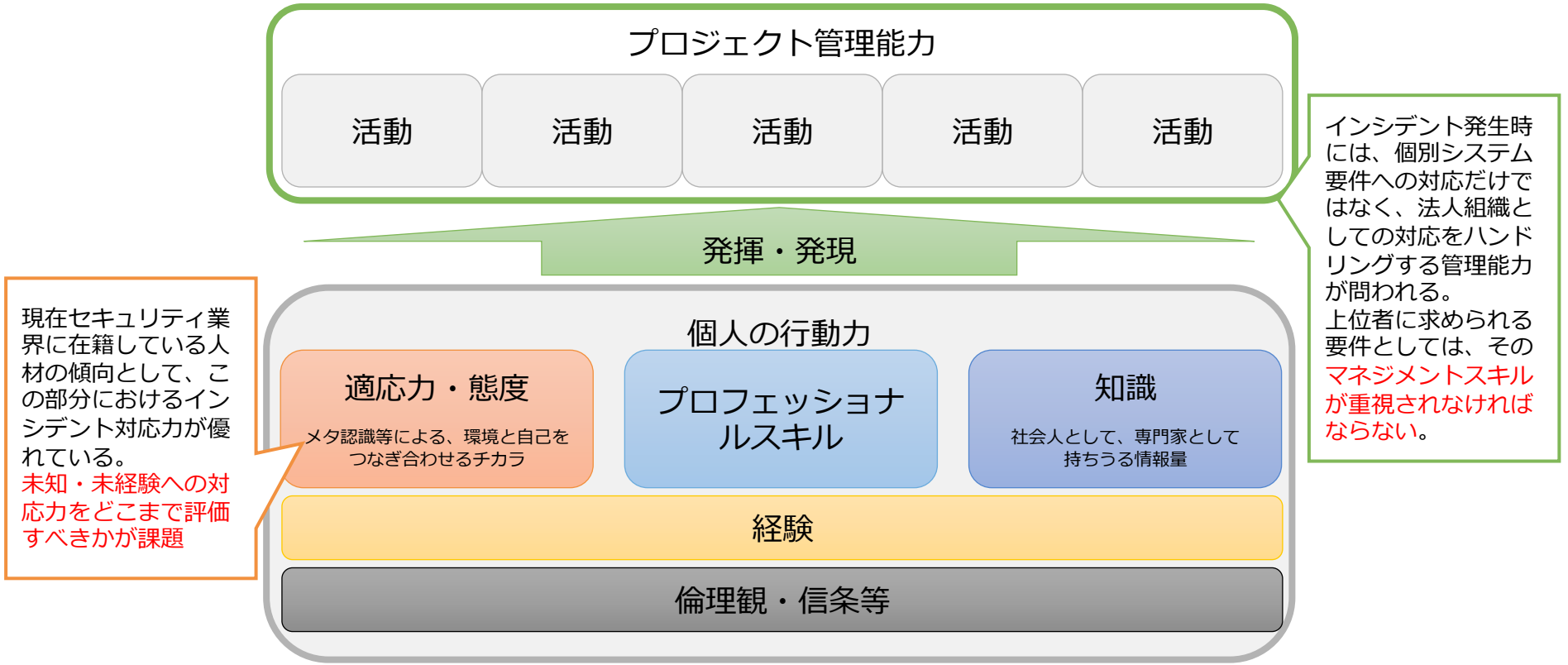


# 11. 機能分布モデル（日本企業におけるセキュリティ機能の分布）※本検討会調べ



# 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業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。
  - 「氷山モデル」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

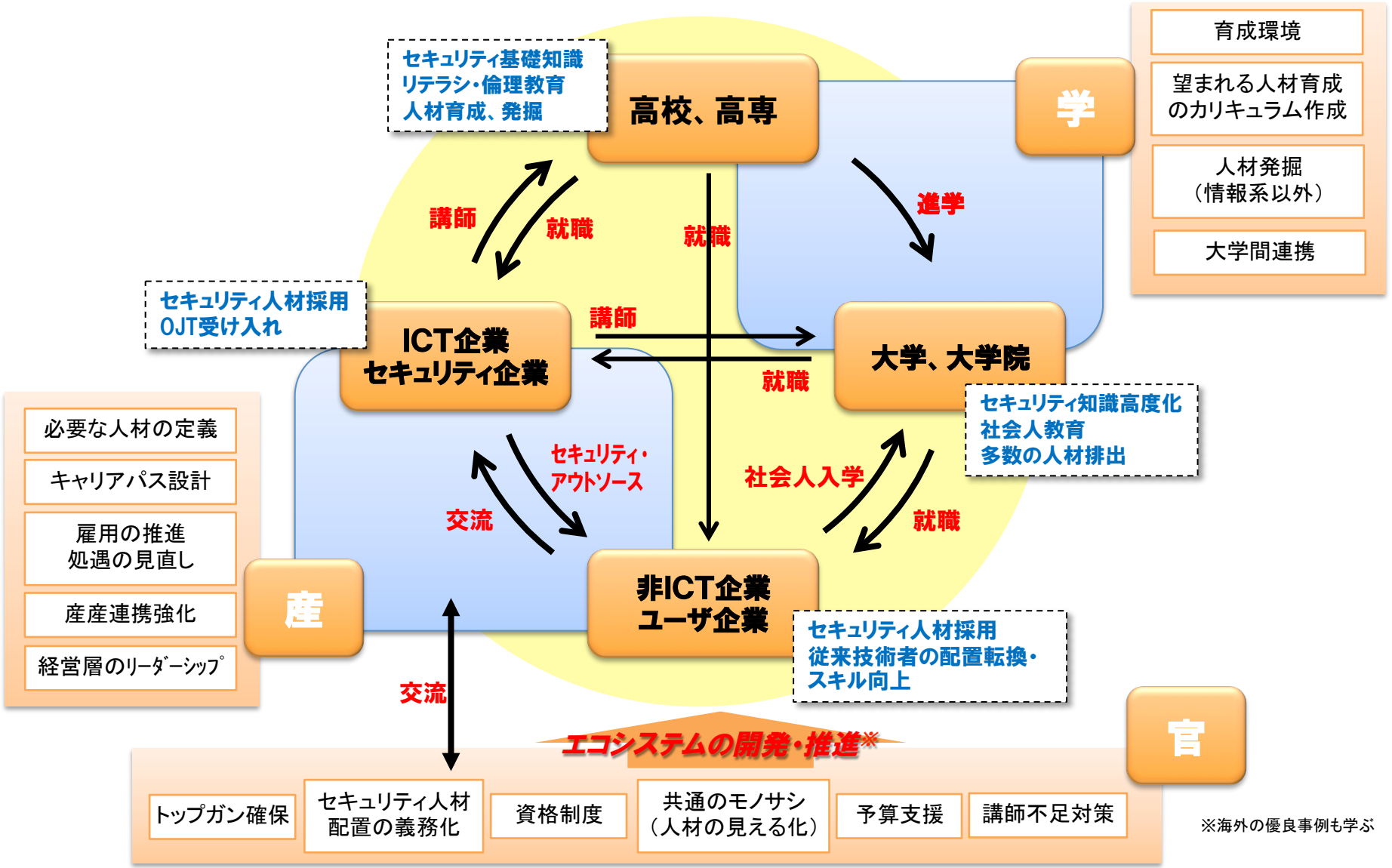
- 産業界（特にユーザ企業）の現場視点が重要
  - 分散したセキュリティ業務をまとめると新たな職種が導き出せる可能性
    ⇒ セキュリティ雇用増につながる専任管理者（専門職）の育成
  - まとめられないセキュリティ業務は依然、現場対応が必要
    ⇒ 本来業務の中でセキュリティも分かる人材の育成
    ⇒ 各組織の一般管理者に対するセキュリティ知識レベル底上げ

- 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）

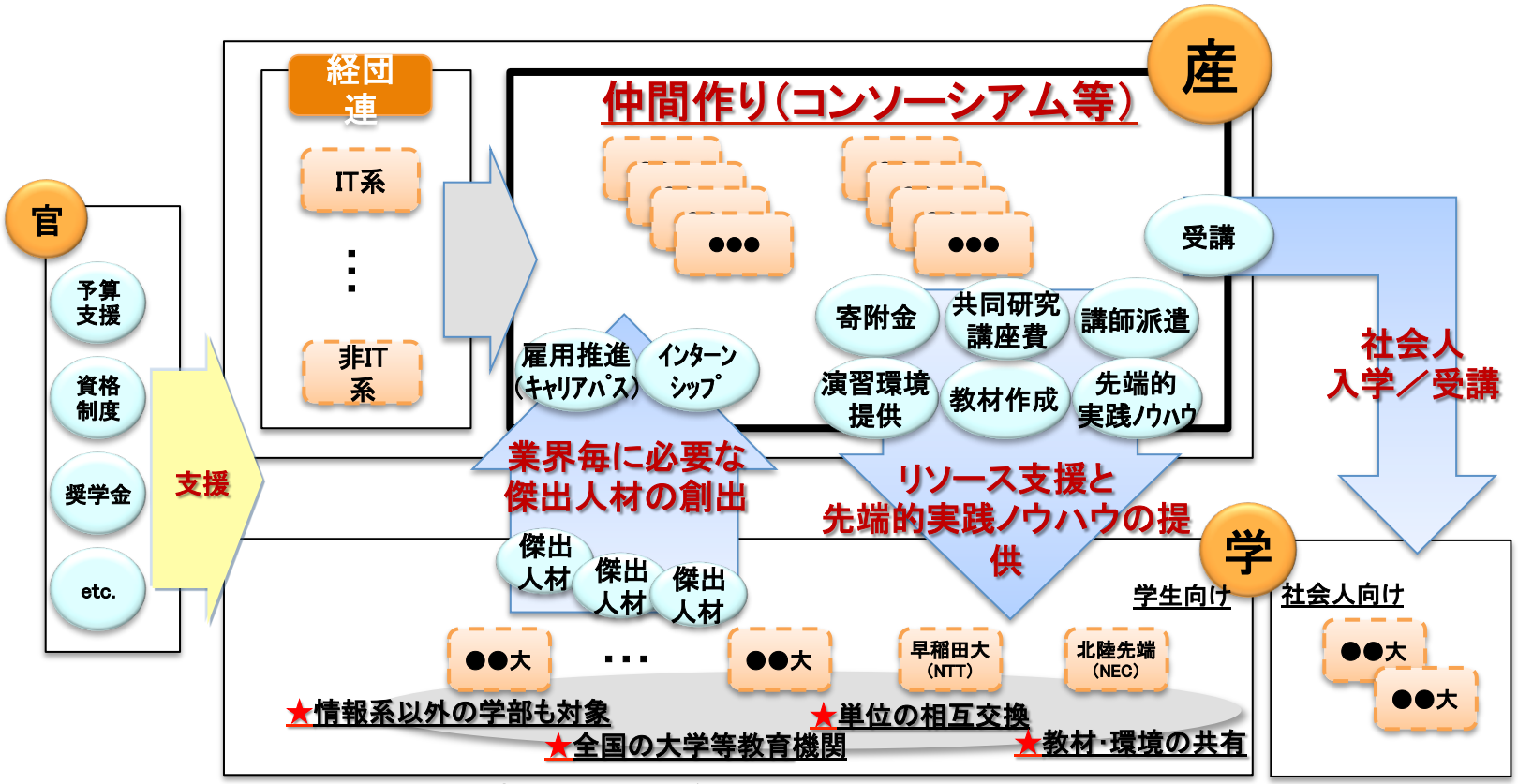
## ユーザ企業においても雇用・活用に結びつく人材定義と人材育成・維持に向けて




※海外の優良事例も学ぶ

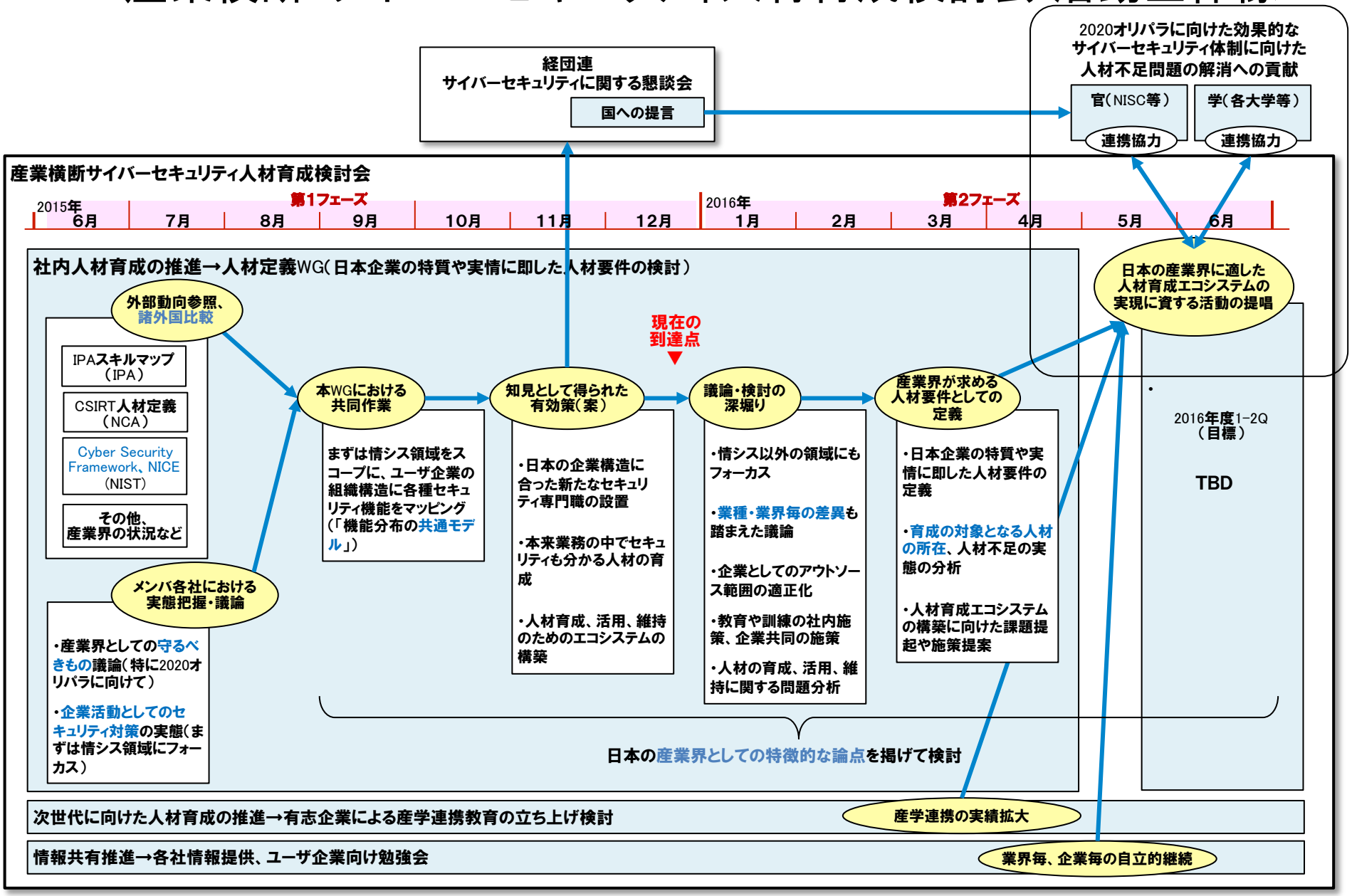
## 2. 産学連携の在り方（検討中イメージ）

- 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。