資料6

「産業横断サイバーセキュリティ人材育成検討会」の取り組み状況

2016.8.2

産業横断サイバーセキュリティ人材育成検討会 事務局

※本検討会の成果物は下記URLよりダウンロードできます。

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

「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）

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、現在計48社

本日のご説明について（要旨）

◆2015年6月9日に発足した当検討会の活動におけるこれまでの成果をご説明します。

◆企業が互いに協力し合い、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）」について、主体的に検討を進めてきました。
【主なテーマ】
① 情報共有、情報交換（産産連携の仕組み醸成を期待）
② 人材定義～人材育成の在り方議論（産業界としての整理）
③ 各種育成施策の共有・連携、産官学連携

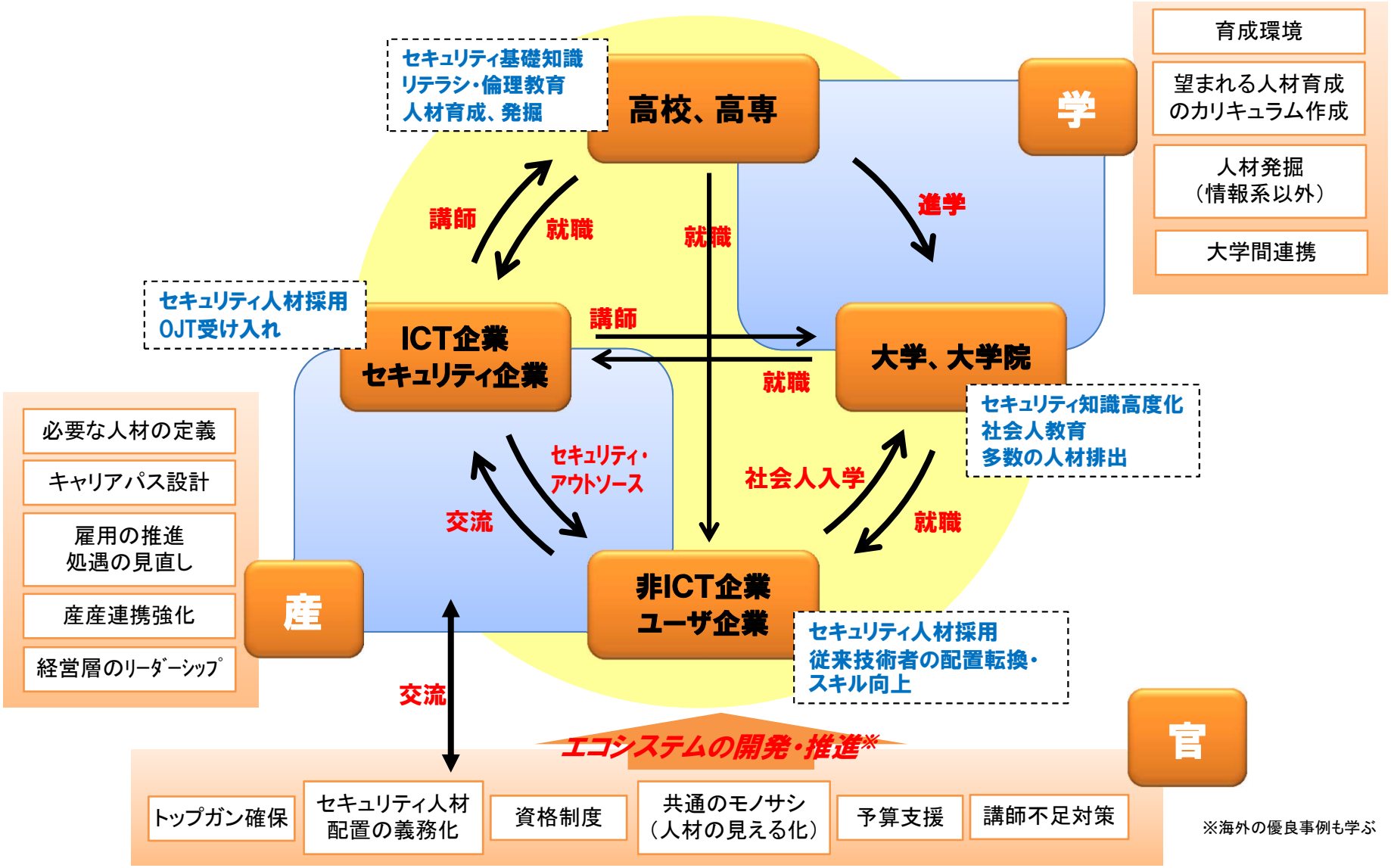
◆経団連の支持の下、国（NISC、文科省、経産省等）との継続的な意見交換、情報交換、各種セキュリティ関連組織との交流により、サイバーセキュリティ人材育成に関する産業界の代表組織として認知して頂くようになりました。

◆発足して一年が経ち、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、一定の整理ができ、本日ご説明させて頂きます。
【主な成果】
“人材定義リファレンス”、“セキュリティ対策カレンダー（AtoZ）”、“セキュリティオペレーションアウトソーシングガイド” など
→日本流のサイバーセキュリティフレームワークとして位置づけられるよう仕上げたいと考えています。

◆今後は、人材の育成と維持のため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みます。

人材育成・維持エコシステム実現のための産学官連携に向けた検討

狙い： 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・維持の具体的施策を立案



※海外の優良事例も学ぶ

サイバーセキュリティ人材定義の検討アプローチ

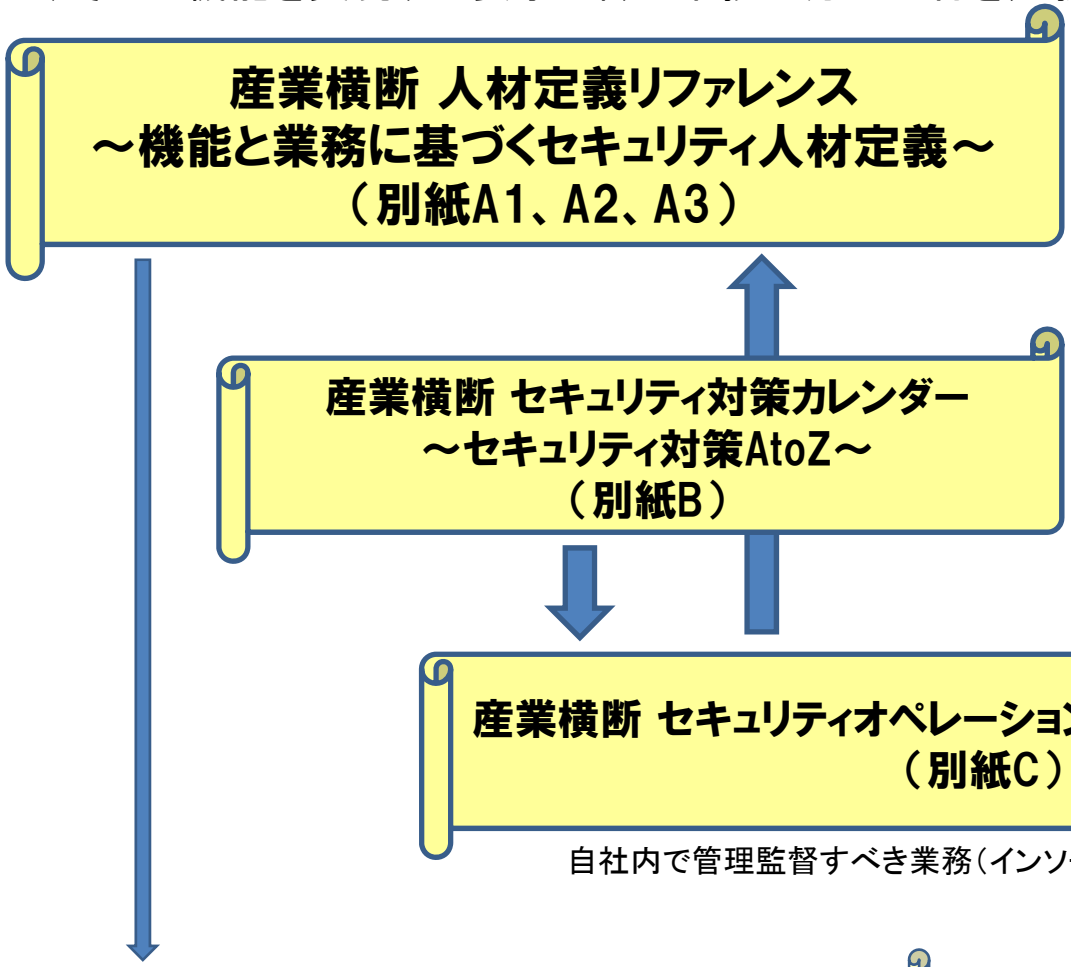
日本企業の特性・実状を深く把握した上で、「実践的」な人材定義を目指すべく、以下のアプローチで検討。

産業横断による検討	日本の多種多様な業界・企業を広くカバーする産業横断の検討体制を構築
日本企業の組織構造	組織の実構造を具体的に紐解くことによって、日本の企業文化、風土に根ざした検討を実施
本来業務とセキュリティ	本来業務の中でのセキュリティ業務の位置づけを考慮して検討

産業横断サイバーセキュリティ機能＆人材定義（当検討会のアウトプット）

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

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する。



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

ユーザー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

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）

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（IPA）によるスキルディクショナリ等にマッピング

産業横断サイバーセキュリティ機能＆人材定義（必要規模試算）

前頁の人材定義を踏まえて、日本国内における人材の必要規模（総人数）を試算してみた。

人材定義を踏まえたセキュリティ人材の必要規模（試算）

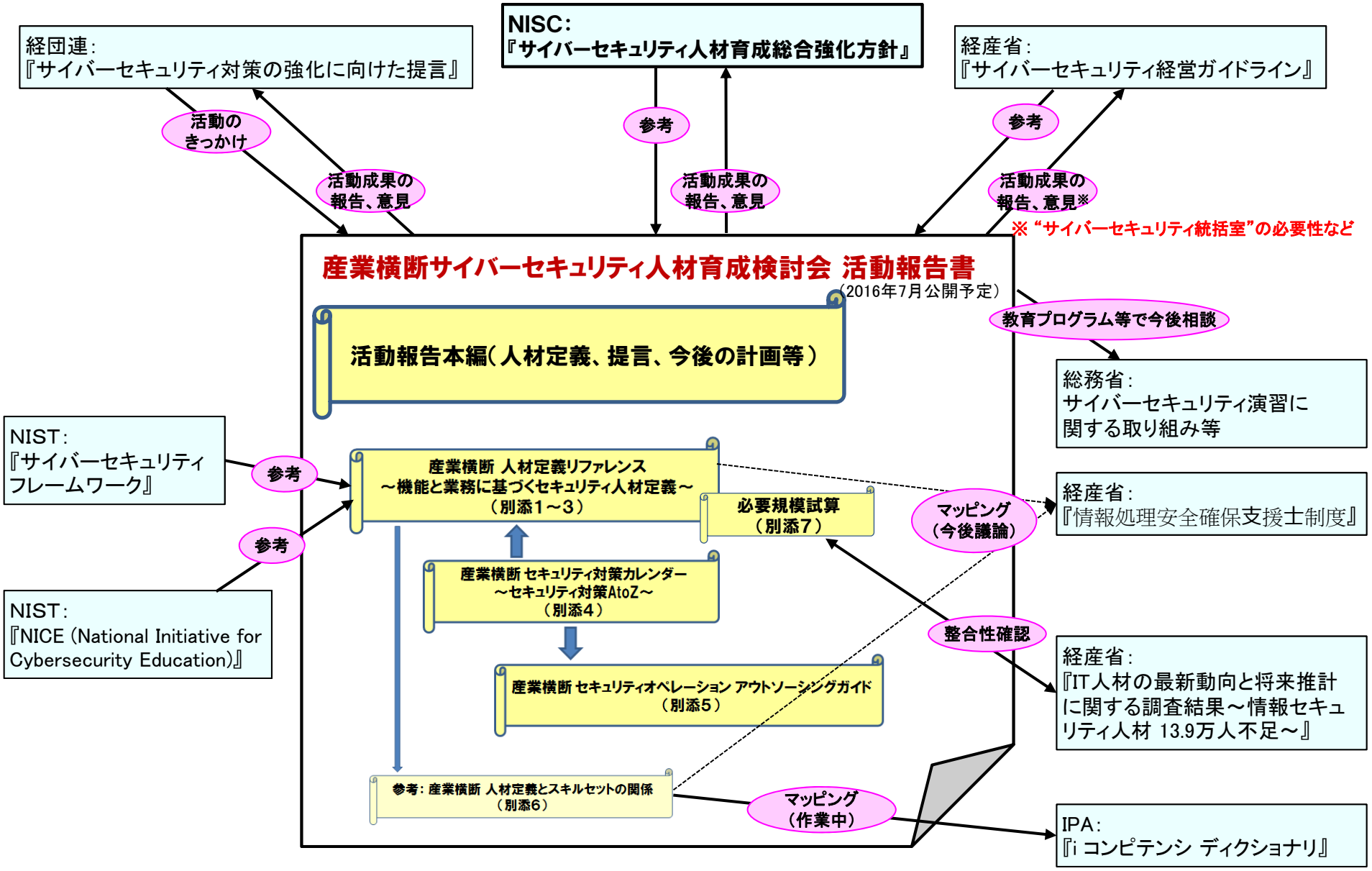
＜試算の流れ＞

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1）において、24種に分類定義されたサイバーセキュリティ人材の役割（担当）をその特質に着目して次の7種に括る。
”CISO等”、”システム部門責任者”、”インシデント対応”、”運用・CSIRT・SOC”、”システム管理者”、”システム運用管理者”、”（システム）各担当”

② 企業規模ごとに、一企業内に上記7種類の人材がそれぞれ何人ほど必要かを、当検討会の知見・見識で推測する。

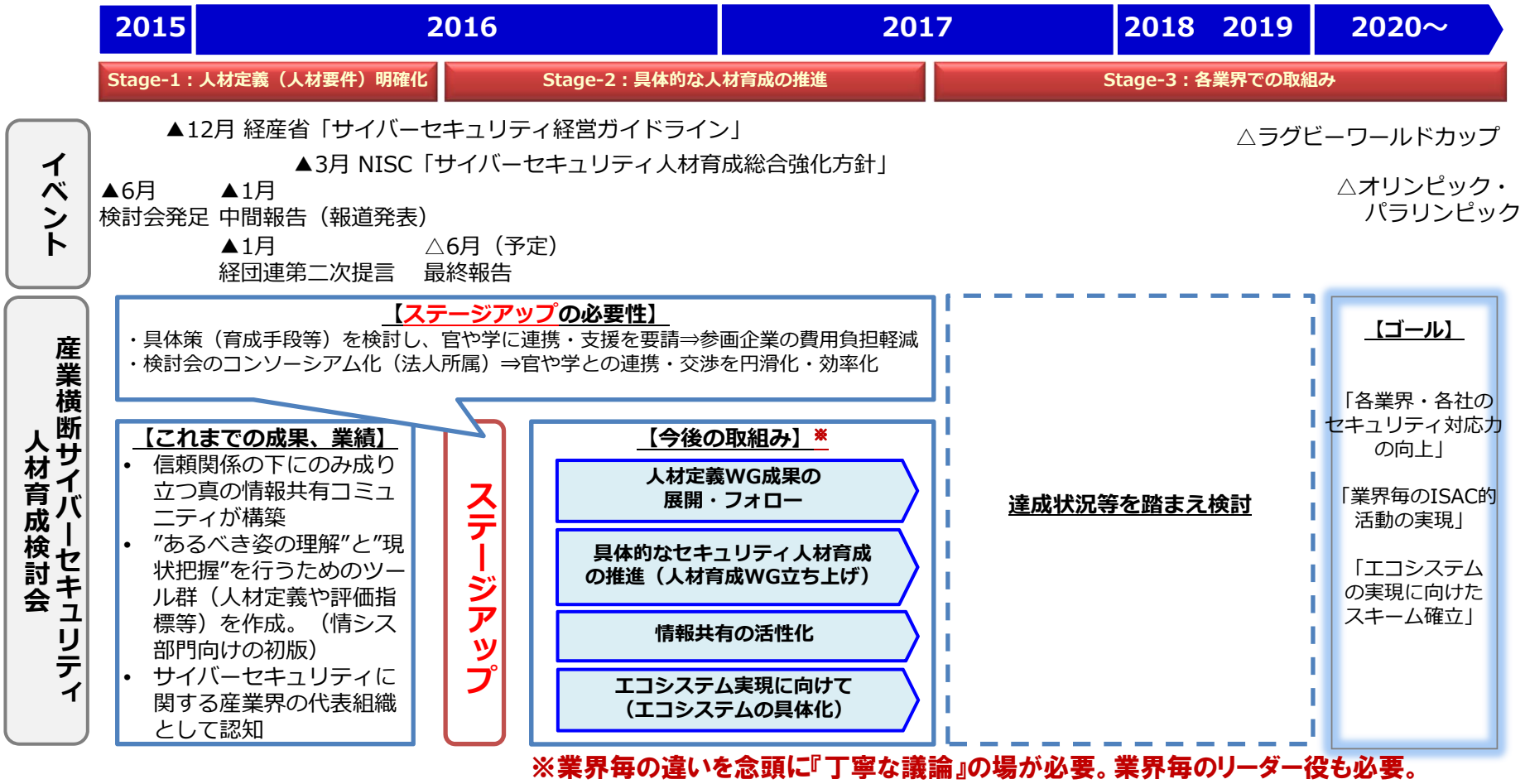
③ 企業規模ごとの上記推測値に、国内の企業数・事業所数※を乗じて、必要なサイバーセキュリティ人材総数を算定する。（※「平成26年経済センサス・基礎調査」より引用。）

本検討会によるアウトプットと国や各界の関連動向との関係



今後の取り組み計画ついて(1/2)

■背景認識
日本の産業界、特にユーザー系企業は、2020年東京五輪も控えてますます激化するサイバー脅威・リスクに対応する人材の確保が急務。産業界に対する攻撃・被害は既に広まりつつある。既存の施策や国の支援には頼れない、間に合わない。
■本検討会の目的
企業が互いに協力し合い、産業界として取り組まなければ実現し得ない（間に合わない）サイバーセキュリティ人材の確保（育成と雇用）について検討、実行推進する。



※業界毎の違いを念頭に『丁寧な議論』の場が必要。業界毎のリーダー役も必要。

今後の取り組み計画ついて(2/2)

情報システム部門 機能分化 → サイバーセキュリティ 機能定義 → サイバーセキュリティ 人材定義 → サイバーセキュリティ 教育体系 → サイバーセキュリティ 資格体系 → サイバーセキュリティ 採用評価モデル

◆『人材育成WG』の活動（案）

1. 定義項目（決め事）

- **教育体系**（ISO22398, DHS:HSEEP を参考）
- **カリキュラム**

2. トレーニング・教育**カタログ**構築

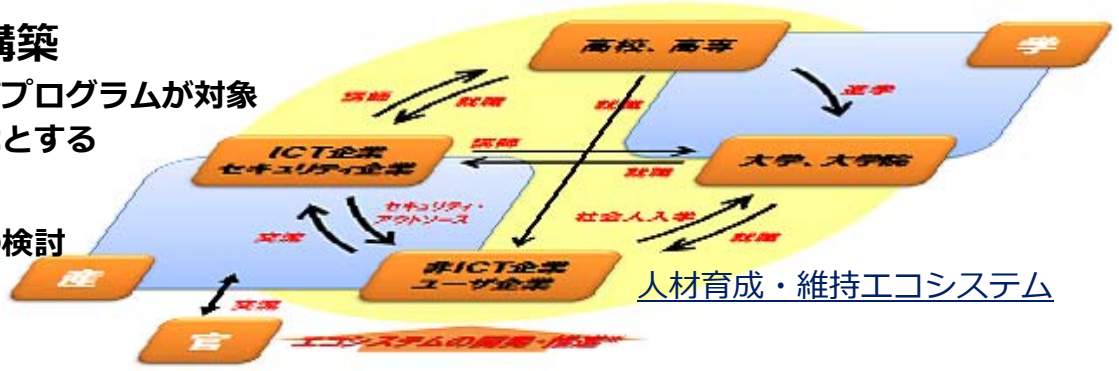
- 日本国内で提供されている様々な教育プログラムが対象
- **ポータル構築**し、登録、検索等を可能とする

3. サイバーレンジ整備

- **演習環境**の要件定義ならびに仕様等の検討

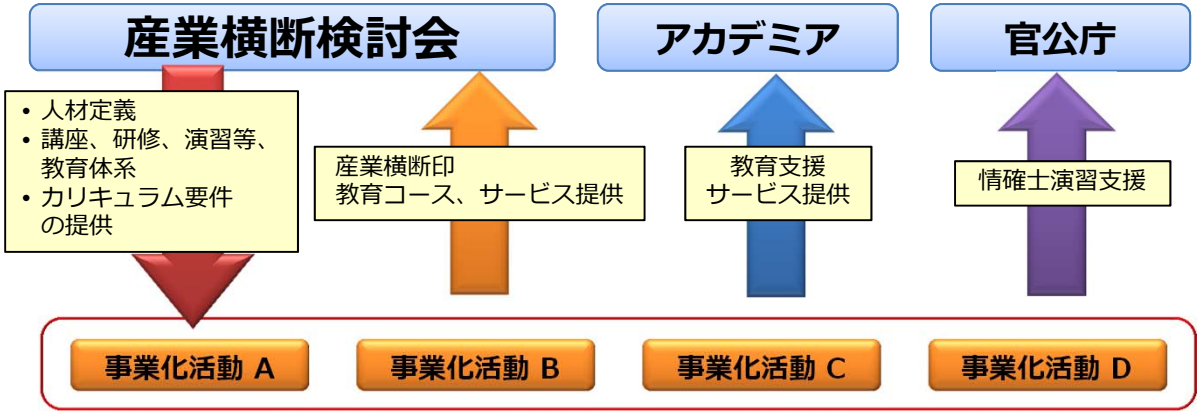
4. 検討会教育環境整備

- メンバーの教育プログラムやツールを**共有し利活用**出来る環境整備



人材育成・維持エコシステム

スケジュール・マイルストーン		
1	8月～9月	定義項目検討
2	10月～1月	ポータル構築
3	随時	カタログ構築 演習環境検討・整備



まとめ（1/3）

●第１期（2015年6月～2016年6月）の到達点：

- **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。**
  ⇒「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）」
  「産業横断人材定義とスキルセットの関係（IPA「iコンピテンシディクショナリ」との対応付）」

- **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、要件定義、教育プログラム等共有環境の構築、人材育成関連ビジネス主体との連携検討などを検討会一丸となって推進。
  ※第1期成果物の知財確保、組織間で利用契約可能な組織形態の見直し含む

まとめ(2/3)

●活動を通して再認識したこと:

・次ステップとして、業界固有の人材定義に関する議論は必須。

- 業界毎の違いについては、『丁寧に議論する』場が必要。
- 業界毎のリーダー役が必要。誰がリーダーとして相応しいかの見定めが必要。
- 業界(事業)毎の違いが議論になりそうな観点:
  ⇒組織的対策面(方針、体制、連携、規約など)、
  人的対策面(育成・教育、雇用など)、
  物理的対策(区画、管理など)、
  技術的対策(適用可能技術など)、
  職務の違い(管理者、運用者、技術者)
- ユーザ企業の業種専門技術者がセキュリティ人材となって活躍し続けることは難しく、セキュリティを得意とするICT企業との協力関係が必要となるケースが多い。

・2020年までにすべきことと2020年以降を見据えてすべきことがある。

- 人材定義も具体的な人材育成施策も両スコープに対して必要。
- 2020年に間に合わせるために、『丁寧な議論(正攻法)』を如何に加速するかが重要。

まとめ（3/3）

●活動を通して再認識したこと：

・本検討会／産業横断の場を活かし、相互支援活動としてできること。

- 必要な人材を見定めることで、必要な育成手段（教育プログラム）が明らかになる。
- 企業毎に必要な人材育成手段（施策）への橋渡し・実行支援が必要。
- 重要インフラ業界は相互依存しているため、全体に跨る検討も必要。
- 2020年に向けた緊急時対応の企業間協力サイバー演習（要件、実行論）の検討。
- 経団連、NISC、各省の施策との協調も必要。産業横断としての責任の明確化も要。

・人材育成・維持のエコシステム実現に向けた推進体制が必要。

- 官、学、それぞれにおける各種施策との効果的な連携を具体化する推進体制。
- セキュリティ関連企業の在り方論、連携論。

・本検討会メンバ企業の実務および経営のトップ層による会合を検討中。

- 目的①：検討会成果を各社内で展開・運用を実行推進する役を担ってもらう。
- 目的②：産業横断のTrusted Networkをトップ層レベルで立ち上げ、
  全ての業界・企業に求められる最低限の意識レベル、人材レベルを共有。

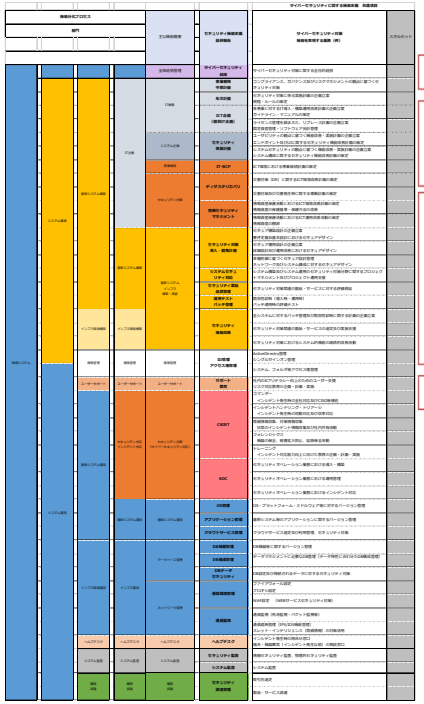
空　白

参考

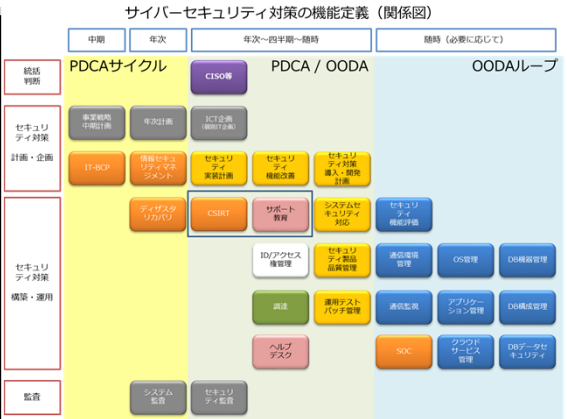
産業横断サイバーセキュリティ機能＆人材定義の解説

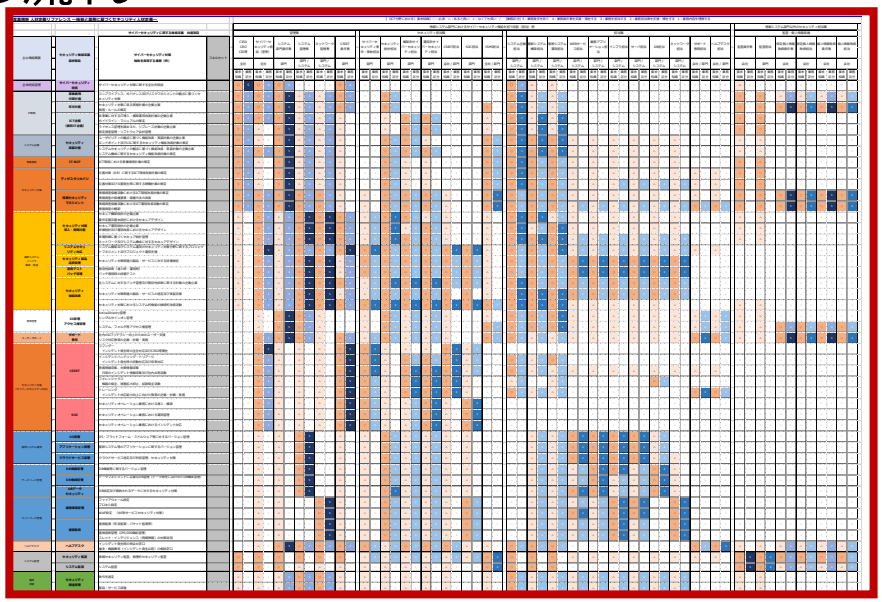
産業横断サイバーセキュリティ人材育成検討会 事務局

“産業横断 人材定義リファレンス” 作成の流れ

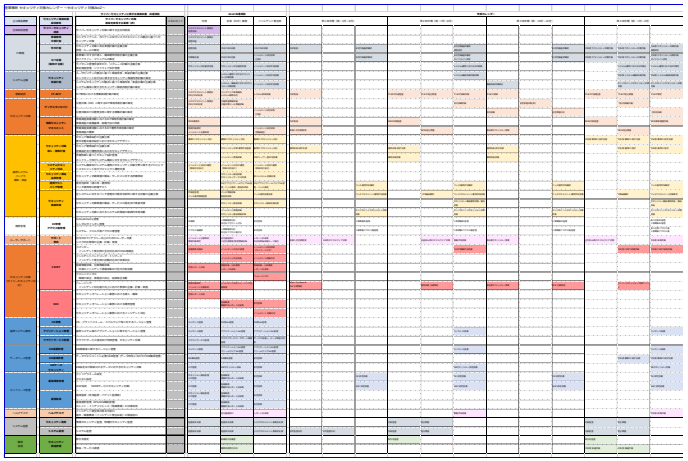


組織分化と機能定義

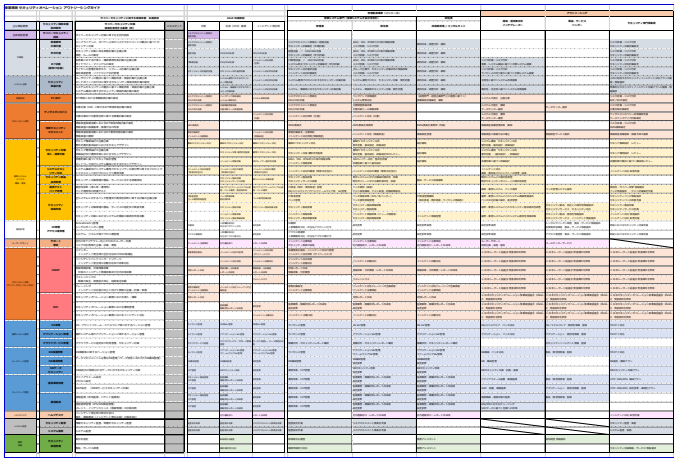




人材定義 リファレンス



セキュリティ対策カレンダー

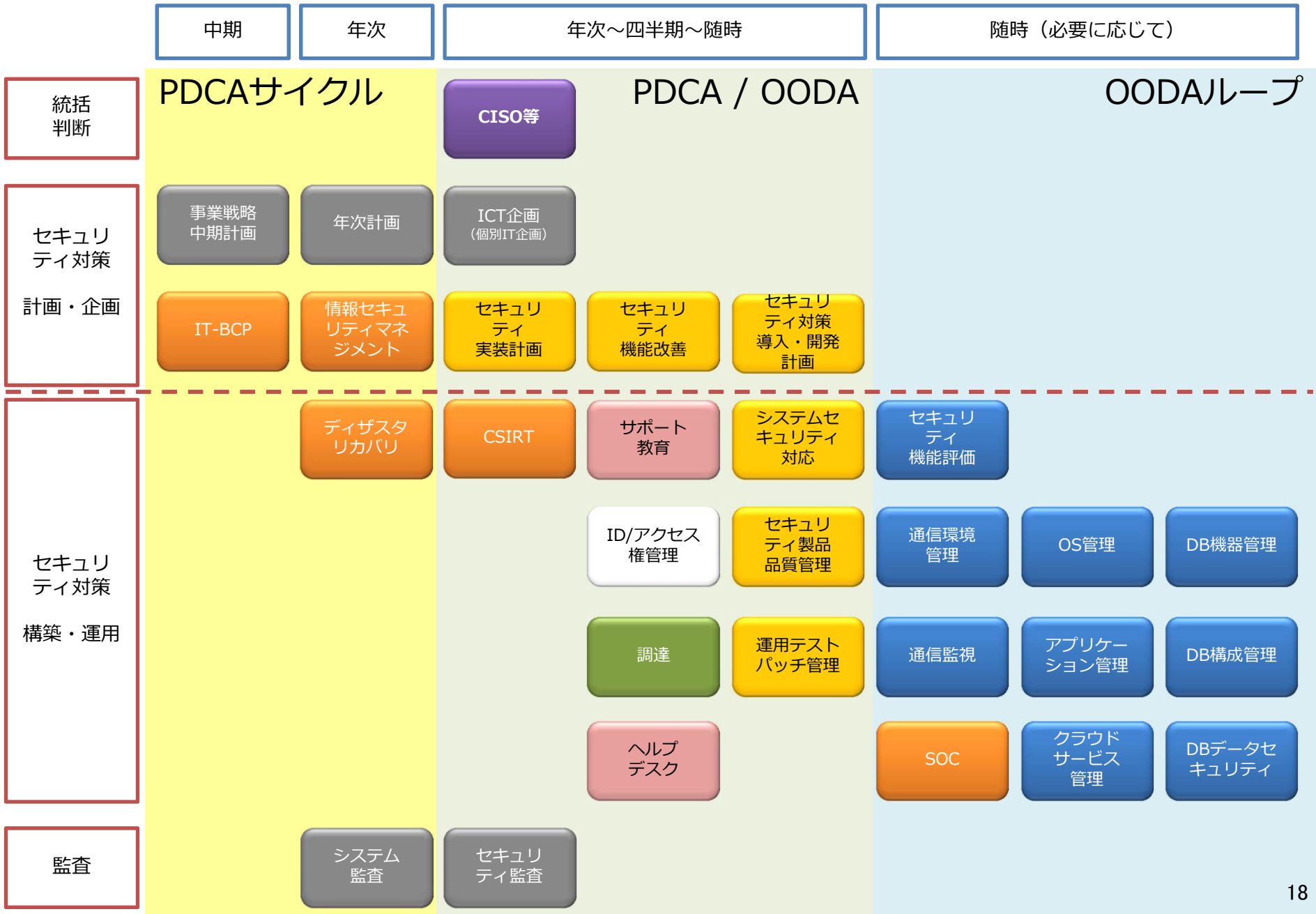


アウトソーシングガイド

アウトプットの一覧

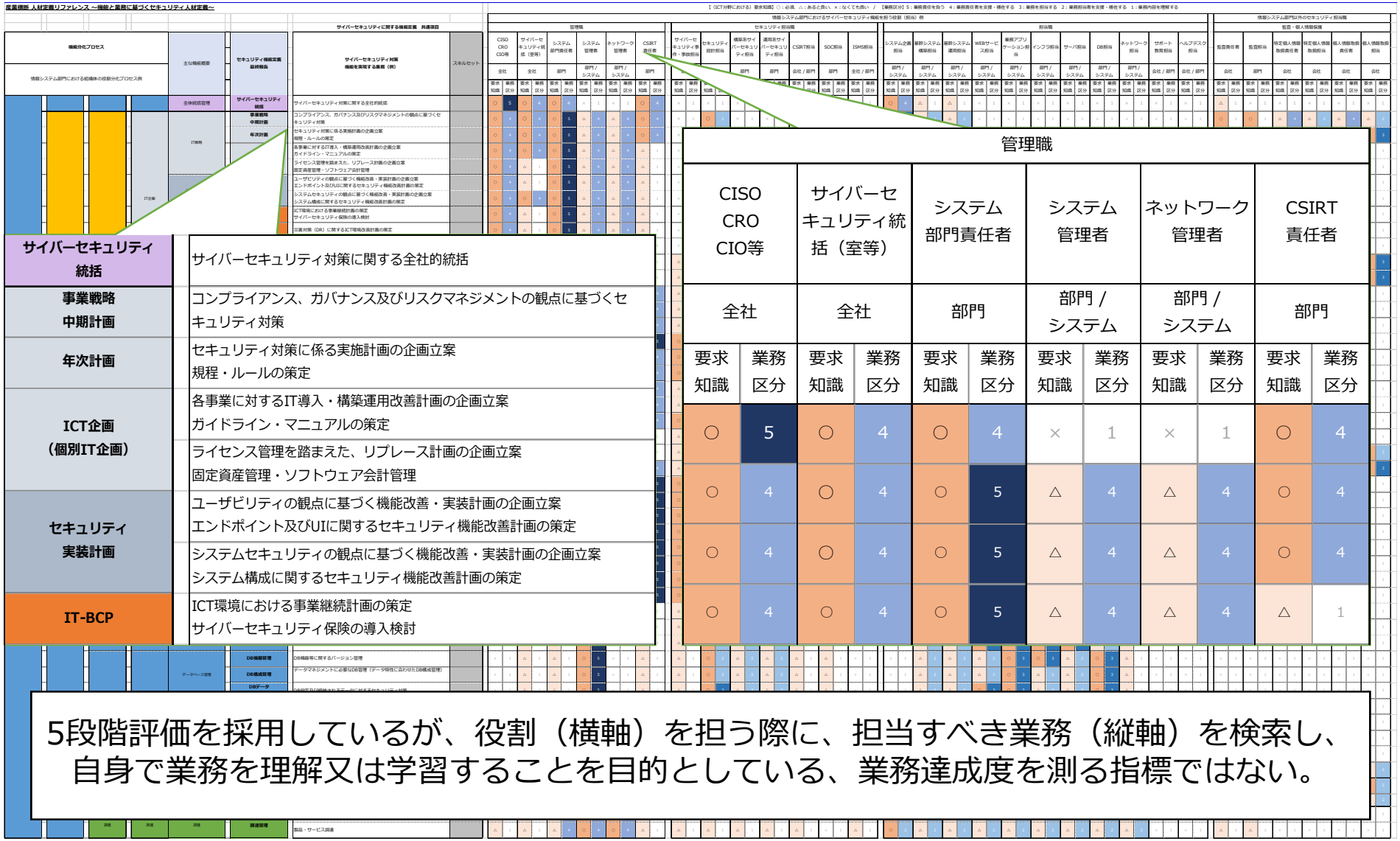
1. **サイバーセキュリティ対策の機能定義**（関係図）：元プロセスマップ
2. **産業横断 人材定義リファレンス** ～機能と業務に基づくセキュリティ人材定義～
   - 産業横断 人材定義リファレンス ：要求知識
   - 産業横断 人材定義リファレンス ：業務区分
3. **産業横断 セキュリティ対策カレンダー** ～セキュリティ対策AtoZ～
4. **産業横断 セキュリティオペレーション アウトソーシングガイド**
5. 産業横断 人材定義リファレンス 別紙 **「情報システム部門におけるサイバーセキュリティ人材イメージ」**

1．サイバーセキュリティ対策の機能定義（関係図）



2. 産業横断 人材定義リファレンス

- 縦軸に19の機能と47の業務例、横軸に30の役割例を表現した一覧。



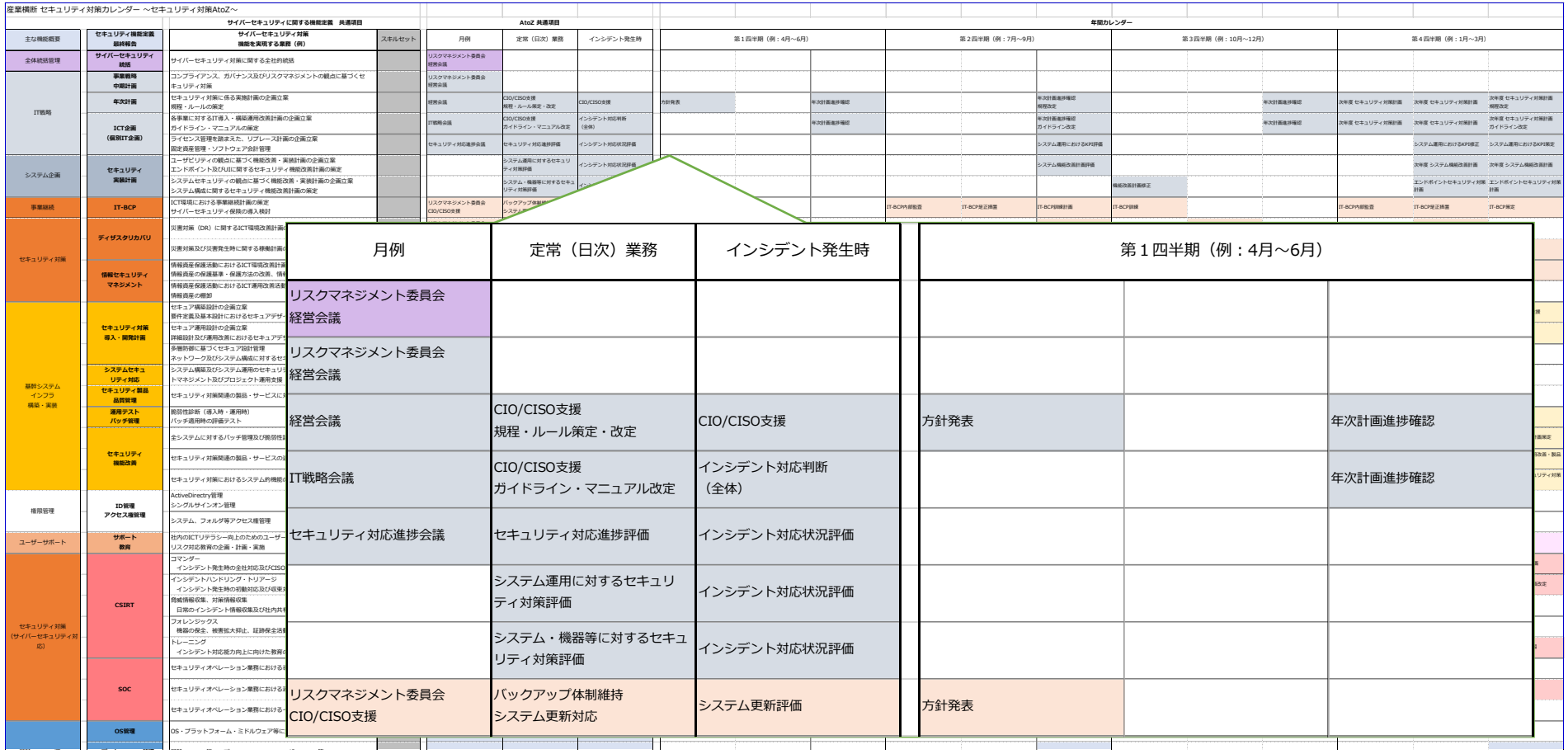
	管理職											
	CISO CRO CIO等		サイバーセキュリティ統括（室等）		システム部門責任者		システム管理者		ネットワーク管理者		CSIRT責任者	
	全社		全社		部門		部門 / システム		部門 / システム		部門	
	要求知識	業務区分	要求知識	業務区分	要求知識	業務区分	要求知識	業務区分	要求知識	業務区分	要求知識	業務区分
サイバーセキュリティ統括	○	5	○	4	○	4	×	1	×	1	○	4
事業戦略 中期計画	○	4	○	4	○	5	△	4	△	4	○	4
年次計画	○	4	○	4	○	5	△	4	△	4	○	4
ICT企画（個別IT企画）	○	4	○	4	○	5	△	4	△	4	△	1

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

5段階評価を採用しているが、役割（横軸）を担う際に、担当すべき業務（縦軸）を検索し、自身で業務を理解又は学習することを目的としている、業務達成度を測る指標ではない。

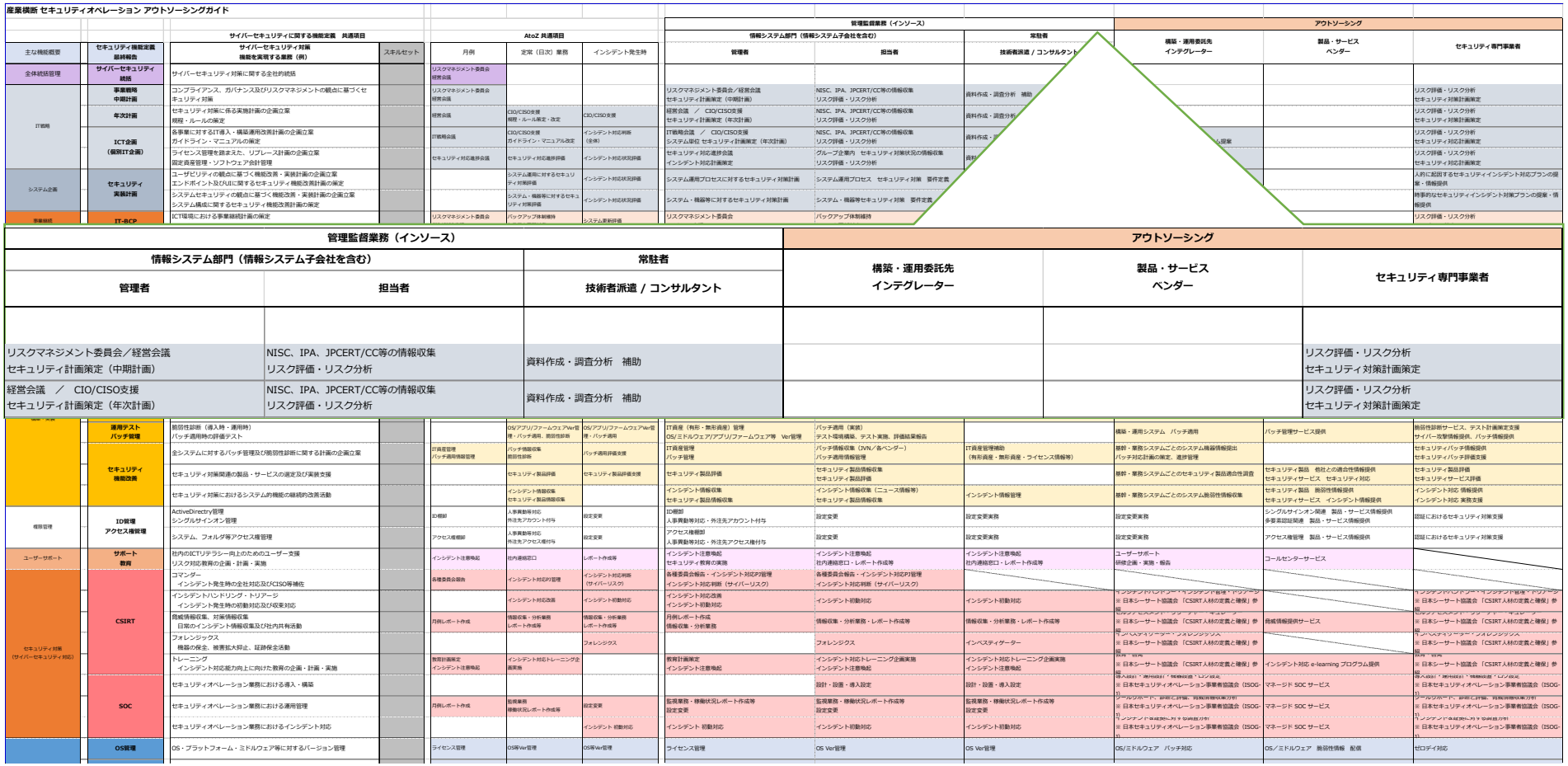
3. 産業横断 セキュリティ対策カレンダー

- 機能定義を行ったそれぞれの機能が、業務としてどのように実施されるのかを俯瞰するために作成。
- 月例・日次、インシデント発生時、更に、四半期ごとの活動スケジュールを想定。
- 各社の決算月や主要イベントにより追記修正が可能。



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

- 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関するアウトソーシングの委託範囲と委託業務内容についてのモデルを示したもの。
- インソース3種、アウトソース3種の計6分類による、業務分担のイメージを整理共有する目的に基づき策定。



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

管理監督業務（インソース）			アウトソーシング		
情報システム部門（情報システム子会社を含む）		常駐者	構築・運用委託先 インテグレーター	製品・サービス ベンダー	セキュリティ専門事業者
管理者	担当者	技術者派遣 / コンサルタント			
リスクマネジメント委員会／経営会議 セキュリティ計画策定（中期計画）	NISC、IPA、JPCERT/CC等の情報収集 リスク評価・リスク分析	資料作成・調査分析　補助			リスク評価・リスク分析 セキュリティ対策計画策定
経営会議　／　CIO/CISO支援 セキュリティ計画策定（年次計画）	NISC、IPA、JPCERT/CC等の情報収集 リスク評価・リスク分析	資料作成・調査分析　補助			リスク評価・リスク分析 セキュリティ対策計画策定

5．「情報システム部門におけるサイバーセキュリティ人材イメージ」

- 氷山モデルに基づき、下記項目について基準・スキルセットを記載
  - 適応力・態度
  - プロフェッショナルスキル
  - （技術以外の）知識
  - 業務経験
  - 倫理観・信条

社内の評価制度等との連携を想定し、
IPA発行「ｉコンピテンシディクショナリ」を活用

役割	機能	スキル																		
		適応力・態度			プロフェッショナルスキル									（技術以外の） 知識	業務経験	倫理観・信条				
		チームワークや作業遂行に必要			対策実務に必要									対策の企画や対応、未知の領域での作業遂行に必要	習熟度に関連し、結果から作業を紐解くために必要	信頼性を担保し、善悪の判断を促す				
		ｉコンピテンシーディクショナリ（ITヒューマンスキル）から参照			ｉコンピテンシーディクショナリ（大分類及び中分類）から参照									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		コンプライアンス等				
					大分類	中分類														
CISO CRO CIO等	サイバーセキュリティ対策の統括責任者	問題発見力	問題分析力	仮説設定力	コンプライアンス	MC06.1	管理方針と体制	MC06.2	実施と評価					会社法/会社法施行規則	経営管理（全般）	アカウンタビリティ（謝罪する立場）				
		論理思考力	概念化力		内部統制状況のモニタリング	MC08.1	実行責任者によるモニタリングと評価	MC08.2	ガバナンスによる評価					COSO内部統制フレームワーク / ERM	英語力（読み書き）	善管注意義務				
		俯瞰力	深耕力		事業戦略策定	ST01.1	事業環境の分析	ST01.2	事業戦略の策定	ST01.3	事業戦略実行体制の確立			刑法 / 刑事訴訟法 / 不正アクセス禁止法 / 不正競争防止法	5,000万円以上の起案又は決裁	忠実義務				
		革新力	継続力		事業戦略把握・策定支援	ST02.1	要求（構想）の確認	ST02.2	新ビジネスモデルへの提言	ST02.3	事業戦略の実現シナリオへの提言			電気通信事業法 / サイバーセキュリティ基本法 / 電子署名及び認証業務に関する法律	サイバーインシデント被害（演習含む）					
		相手の考えを理解する力	自分の考えを伝える力	共感を呼ぶ力	IT戦略策定・実行推進	PL01.1	基本方針の策定	PL01.2	IT化計画の策定	PL01.3	IT戦略実行マネジメント			サイバーセキュリティ経営ガイドライン	BCPの発動					
					IT戦略評価・改善	EV02.1	IT戦略の評価							PMBOK / SP800-53 / SP800-30	コミュニケーション／ネゴシエーション					
					IT運用コントロール	US02.1	IT運用管理	US02.2	情報セキュリティ管理					IPA発行 情報セキュリティ関連ガイドライン						
					情報セキュリティマネジメント	MC03.1	情報セキュリティ戦略と方針の策定	MC03.2	情報セキュリティの運用	MC03.3	情報セキュリティの見直し									
サイバーセキュリティ統括（室等）	社内のサイバーセキュリティインシデント対応を統括する部門・部署・チーム	問題発見力	問題分析力	仮説設定力	新ビジネス・新技術の調査・分析と技術支援	CM05.1	最新技術の研究・検証	CM05.2	技術支援					会社法/会社法施行規則	経営管理（リスク対応）	アカウンタビリティ（謝罪する立場）				
		論理思考力	概念化力		品質マネジメント	MC04.1	品質管理のコントロール	MC04.2	組織全体の品質マネジメント					COSO内部統制フレームワーク / ERM	英語力（交渉力）	コンプライアンス				
		俯瞰力	深耕力		システム評価・改善	EV01.1	ITシステムの評価	EV01.2	ITサービスの評価	EV01.3	Webサイトの評価			刑法 / 刑事訴訟法 / 不正アクセス禁止法 / 不正競争防止法	社外、グループ企業外との情報連携					
		革新力	継続力		データサイエンス	CM06.1	ビジネス目標の決定	CM06.2	状況の評価	CM06.3	目標の決定とプロジェクト計画の策定			電気通信事業法 / サイバーセキュリティ基本法 / 電子署名及び認証業務に関する法律	サイバーインシデント対応（演習含む）					
		相手の考えを理解する力	自分の考えを伝える力	共感を呼ぶ力		CM06.4	データの理解	CM06.5	データマイニングのためのデータの準備	CM06.6	モデリング			サイバーセキュリティ経営ガイドライン	インシデント情報収集					
						CM06.7	評価	CM06.8	結果とモデルの展開	CM06.9	ビジネスでの活用と評価			PMBOK / SP800-53 / SP800-30	コミュニケーション／ネゴシエーション					
					プロジェクトマネジメント	DV14.1	プロジェクト立ち上げ	DV14.2	プロジェクト計画策定	DV14.3	プロジェクト追跡と実行管理			IPA発行 情報セキュリティ関連ガイドライン	ベンダー＆製品情報収集					
						DV14.4	プロジェクト終結	DV14.5	プロジェクト個別の品質マネジメント											
					IT戦略評価・改善	EV02.1	IT戦略の評価													
					IT製品・サービス戦略評価・改善	EV03.1	IT製品・サービス戦略の評価													
					情報セキュリティマネジメント	MC03.1	情報セキュリティ戦略と方針の策定	MC03.2	情報セキュリティの運用	MC03.3	情報セキュリティの見直し									
					事業継続マネジメント	MC02.1	事業継続計画の策定	MC02.2	事業継続計画の運用	MC02.3	事業継続計画の見直し									
						MC02.4	災害復旧計画の策定	MC02.5	災害復旧計画の運用	MC02.6	災害復旧計画の見直し									
					ラインマネジメント	MC01.1	業務計画の策定	MC01.2	業務計画の実行	MC01.3	業務計画に基づく評価									
						MC01.4	リソース計画の策定	MC01.5	リソースの管理	MC01.6	メンバの育成									