ユーザ企業のための
セキュリティ統括室
構築・運用キット
（統括室キット）

Part１：概要編

2018/11/21 ver1.0

産業横断サイバーセキュリティ人材育成検討会

人材育成WG

はじめに

- 「統括室キット」
  - 「ユーザ企業のためのセキュリティ統括室 構築・運用キット」（以下、「統括室キット」）は、産業横断サイバーセキュリティ人材育成検討会（CRIC CSF）において、第一期より検討する「セキュリティ統括（室等）」について、組織体としての配置または統括人材としての配置を定め、その業務運用手順を定めるものです。
  - 統括室キットは、CRIC CSFの第二期の人材育成WGの成果物として公開しています。

- 対象者
  - 本「統括室キット」は、下記の方々にお読み頂くことをして作成されています。
    1. 企業経営者
    2. CISO等
    3. セキュリティ部門責任者
    4. システム部門責任者
    5. 事業部門責任者
    6. 経営企画部門責任者
    7. セキュリティ部門担当者
    8. その他、事業のリスクマネジメントを検討されている方々

- 著作権

  統括室キットの著作権は、
  「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」
  に帰属します。

  お問合せ先
  - 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
    事務局（問い合わせメール：office@cric-csf.jp）

統括室キットの構成

- 本「統括室キット」は、以下の構成で策定されています。

1. 統括室キット Part1　概要編
   - CRIC CSFの活動経緯と共有された課題
   - 第一期 成果物「人材定義リファレンス」
   - 第二期 における検討プロセスと活動成果
   - 統括室に求められる機能・役割
   - 統括室を検討する前に確認すべき事項

2. 統括室キット Part2　統括室編
   - 統括室を設置する前に確認すべき事項
   - 統括室を設置する際に確認すべき事項
     - 統括室を組織図に記載するケース
     - 統括室を組織図に記載しないケース
   - 統括室を運用する際に必要となる考え方
   - 全社のセキュリティと部門のセキュリティ

3. 統括室キット Part3　統括人材編
   - 統括室を構成する「統括人材」の定義
   - 「統括人材」に求められる役割・業務の例
   - 「統括人材」に必要とされる育成環境

統括室キット Part1 概要編　目次

0．概要

0-1．産業横断サイバーセキュリティ人材育成検討会の沿革

0-2．セキュリティ統括室及び統括人材に関する解説

0-3．CRIC CSF 人材育成WGの取り組み

0-4．CRIC CSF 人材育成WGの成果物

0-5．CRIC CSF 成果物の紹介・引用例

0-6．本資料における「用語の定義」

1．セキュリティ統括室　検討の背景

1-1．第一期：管理するためのセキュリティと人材育成

1-2．第二期：事業を支えるためのセキュリティと人材育成

1-3．第二期：「セキュリティ統括室」の必要性に関する議論

1-4．第二期：「セキュリティ統括室」の位置づけと対応範囲

1-5．第二期：「セキュリティ統括室」の配置及び運用の形態（例）

2．セキュリティ統括室の設置に向けた準備

2-1．セキュリティ統括室の必要性に関する検討プロセス

2-2．企業経営とサイバーセキュリティ

2-3．危機管理委員会（リスクマネジメント委員会）が想定すべきリスク対応

2-4．情報セキュリティ委員会で取り扱うリスクとサイバーセキュリティ

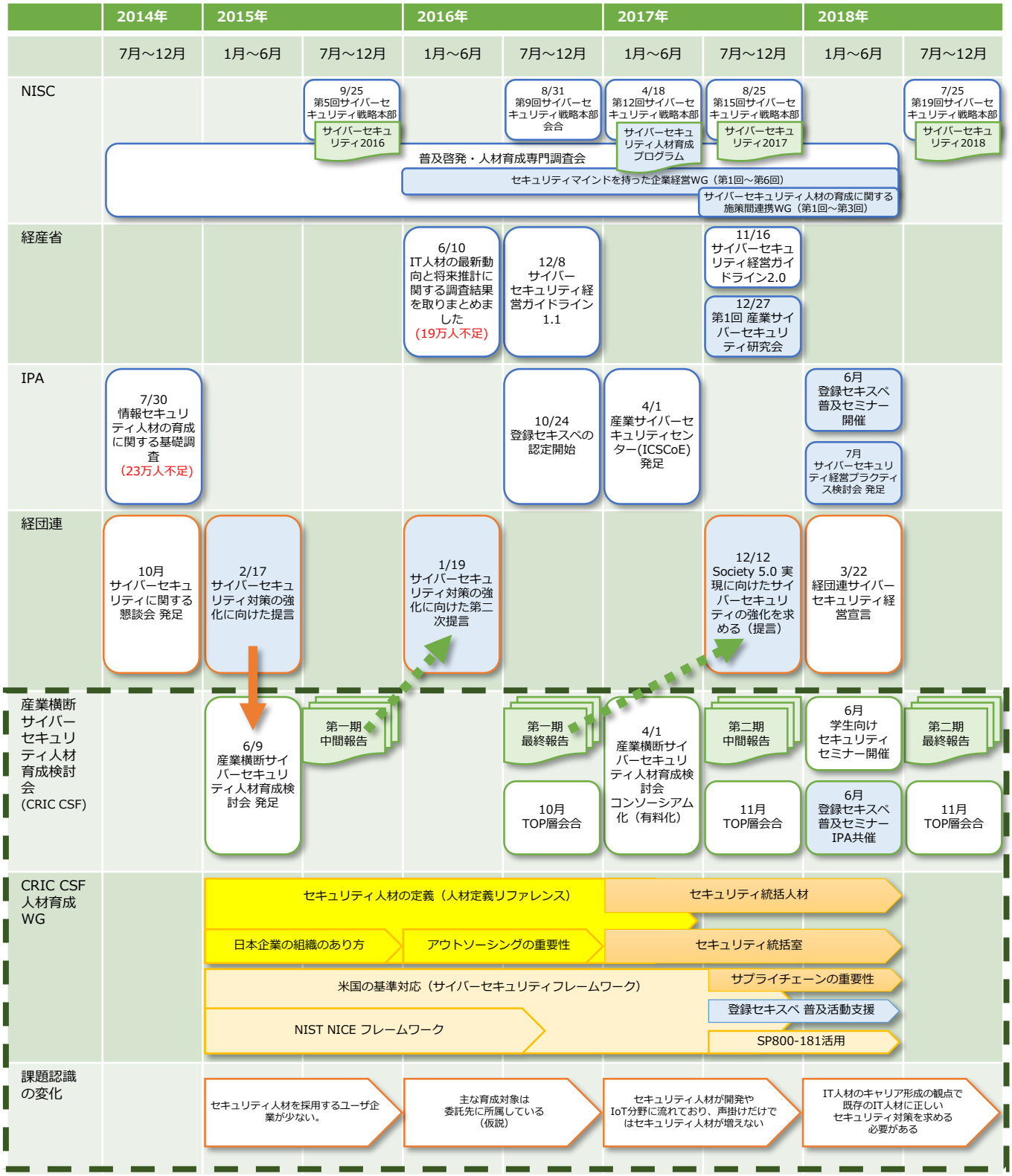
2-5．参照すべき法令、基準・標準、ガイドライン

参考）セキュリティ統括室の役割（例）

０．統括室キットの概要

0-1. 産業横断サイバーセキュリティ人材育成検討会の沿革

- 産業横断サイバーセキュリティ人材育成検討会の成り立ちと活動の経緯



0-2-a 産業横断サイバーセキュリティ人材育成検討会の沿革

：CRIC CSF による活動協力、情報連携、会合参加、並びに資料等の相互参照関係を示す。

0-2. セキュリティ統括室及び統括人材に関する解説

- 統括室キットは、自社のセキュリティ体制に関するアセスメント及び体制構築・運用改善の参考となるべく、以下の3点に配慮し作成されています。

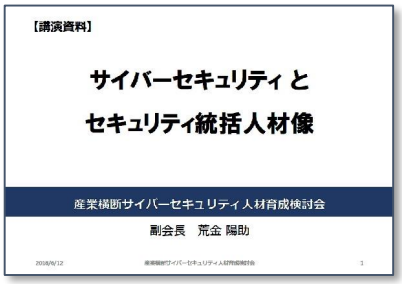
  1. 日本におけるIT構築・運用は、ユーザ企業とベンダー企業の「分業体制」が前提にあるため、サイバーセキュリティに関するそれぞれの責任範囲が適切に管理されていることが望ましい。

  2. 事業におけるIT利用が拡大する中で、不十分なセキュリティ対策は時に事業継続に負の影響を与えることがあり、十分な予算執行を考えるための組織化と権限及び管理者の選任を検討しておくことが望ましい。

  3. 全社リスクマネジメントの観点から、事業部門と管理部門の「連携」を重視し、サイバーセキュリティを司る部署のあり方を例示することにより、今後、セキュリティ体制を検討するための情報源として活用頂きたい。

- 尚、本統括室に関する検討の模様は、以下の資料も合わせてご確認ください。

  - 平成30年6月12日に開催したIPAとCRIC CSFの共催セミナー「今なすべきサイバーセキュリティ対策とそれに必要な人材とは～求められる人材像と情報処理安全確保支援士制度について～」の講演資料はIPAより公開されています。
    - 【講演資料】「サイバーセキュリティとセキュリティ統括人材像」
    - https://www.ipa.go.jp/files/000067124.pdf



  - 上記講演資料の解説は、第二期 CRIC CSF 副会長 荒金氏の講演映像を合わせて確認頂きたい。
    - 【講演映像】「CRIC-CSFが検討を進めているサイバーセキュリティとセキュリティ統括人材像」
    - https://www.youtube.com/watch?v=cJkSQhmS6Ic
      - IPA公式 YouTube サイト

0-3. CRIC CSF 人材育成WGの取り組み

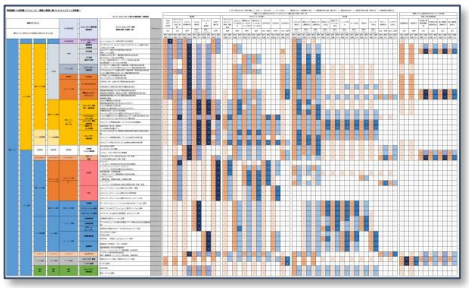
- **CRIC CSF 人材育成WGにおける議論の骨子**
  - CRIC CSFは、サイバーセキュリティ人材の育成に向けた様々な取り組みを討議・検証し、期毎に報告書として発表しています。
  - 人材育成WGにおける第二期のテーマは「セキュリティ統括人材」の配置と育成を中核とし、その所属組織（「セキュリティ統括室」）を、組織論及び権限・分掌、並びに人材育成の観点から整理、検証しています。
  - 日々高度化するサイバー攻撃に対応する人材及び組織を、日本の産業構造及び企業文化に対応し、現実的な解を描き出すことが、CRIC CSF 人材育成WGに課せられたミッションです。

- **CRIC CSFの検討の範囲**
  - CRIC CSFは、重要インフラ事業者を中核とするユーザ企業の集まりとして、事業継続及びサイバーセキュリティ対策の観点から、自社での対応だけではなく、サプライチェーン先との連携及び協業を視野に入れた、ガバナンス、リスクマネジメント、セキュリティ対策を含む幅広い業務に対応する人材育成を議論しています。

- **サイバーセキュリティ人材育成に向けた環境構築**
  - これまで情報セキュリティに対する取り組みは、政府、省庁、各種セキュリティ団体等を通じて広く情報発信がなされてきました。
  - 今後は情報資産の保護という観点だけではなく、IT利活用の拡大及び高度化という時代の変化を踏まえ、事業活動にネガティブなインパクトを与える侵害行為（サイバー攻撃等）に迅速に対応していくための必要な取り組みを整理し「セキュリティ統括人材」および「セキュリティ統括室」の配置、運用、育成等を検討していく必要があるとの議論を進めている。

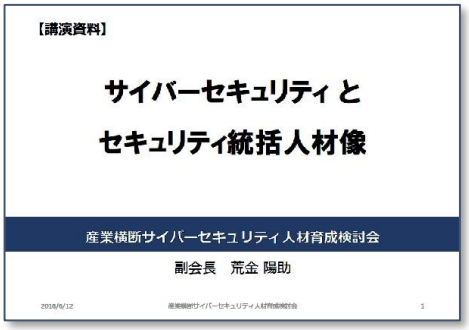
0-4. CRIC CSF 人材育成WGの成果物

- **「人材定義リファレンス」**
  - ユーザ企業における情報システム（IT）領域に関するセキュリティ機能を定義したもの。
  - セキュリティ機能と社内の役割のマトリクスにより構成。
  - 人材の定義だけではなく、セキュリティ対応スケジュールを定めた「カレンダー」と、アウトソーシング業務を確認するための「アウトソーシングガイド」を公開。
  - http://cyber-risk.or.jp/sansanren/index.html



0-4-a 人材定義リファレンス

- **「セキュリティ統括室および統括人材」**
  - Society5.0に対応するセキュリティ人材のあり方とセキュリティ統括室の配置に関する考え方を、IPA共催セミナーにて公開（平成30年6月12日）
  - https://www.ipa.go.jp/siensi/report180612.html



0-4-b セキュリティ統括室および統括人材

- **セキュリティ人材育成 研修データベース**
  - 国内のセキュリティ人材育成に関する研修情報を収集し、様々な切り口により検索できるデータベースサイトを公開し運用中。
  - https://cs-edu.jp/

0-4-c セキュリティ人材育成 研修データベース

0-5. CRIC CSF 成果物の紹介・引用例

- CRIC CSF 報告書及び人材定義リファレンス等の紹介・引用は以下の通りです。

- **日本経済団体連合会**
  - 提言『**Society5.0実現に向けたサイバーセキュリティの強化を求める**』（2017年12月12日）
    - http://www.keidanren.or.jp/policy/2017/103.html
  - 提言『**サイバーセキュリティ対策の強化に向けた第二次提言**』（2016年1月19日）
    - http://www.keidanren.or.jp/policy/2016/006.html

- **内閣サイバーセキュリティセンター（NISC）**
  - 『**サイバーセキュリティ人材育成プログラム**』（2017年4月18日）
    - https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf
  - 『サイバーセキュリティ人材育成総合強化方針』（2016年3月31日）
    - http://www.nisc.go.jp/active/kihon/pdf/jinzai_kyoka_hoshin.pdf

- **金融庁**
  - 『**金融機関のサイバーセキュリティ対策における経営陣・CISO等に期待される役割・責任**』（2017年7月21日）
    - https://www.fsa.go.jp/common/about/research/20170712/20170712.html

- **公益財団法人 金融情報システムセンター**
  - 『**金融機関等におけるIT人材の確保・育成計画の策定のための手引書**』（2018年3月）
    - https://www.fisc.or.jp/publication/disp_target_detail.php?pid=368

0-5. CRIC CSF 成果物の紹介・引用例

- 海外における情報発信を頂いているものは以下の通りです。

- **The National Institute of Standards and Technology (NIST)**
  - **NIST Cybersecurity Risk Management Conference**
    - https://www.nist.gov/news-events/events/2018/11/nist-cybersecurity-risk-management-conference

- **Palo Alto Networks**
  - ***How Japanese Businesses Are Cultivating Cybersecurity Professionals***
    - https://researchcenter.paloaltonetworks.com/2016/10/cso-japanese-businesses-cultivating-cybersecurity-professionals/

  - **サイバーセキュリティ人材育成に関する日本の産業界の取り組みとは**
    - https://www.paloaltonetworks.es/content/pan/ja_JP/company/in-the-news/2016/11-cso-japanese-businesses-cultivating-cybersecurity-professionals.html

0-6. 本資料における「用語の定義」

- **サイバーセキュリティ**
  - サイバーセキュリティとは、電子データの漏えい・改ざん等や、期待されていた IT システムや制御システム等の機能が果たされないといった不具合が生じないようにすること。
    - 参照先）サイバーセキュリティ経営ガイドライン2.0

- **CISO（Chief Information Security Officer）**
  - 経営陣の一員、もしくは経営トップからその役を任命された、セキュリティ対策を実施する上での責任者のこと。
    - 参照先）サイバーセキュリティ経営ガイドライン2.0

- **CISO等**
  - CRIC CSFでは、CISOに求められる役割を担う経営幹部がCISO以外のCRO、CIOや情報セキュリティ委員長等に割り当てられていることを踏まえ、その任にあたる人材を広く「CISO等」と示している。

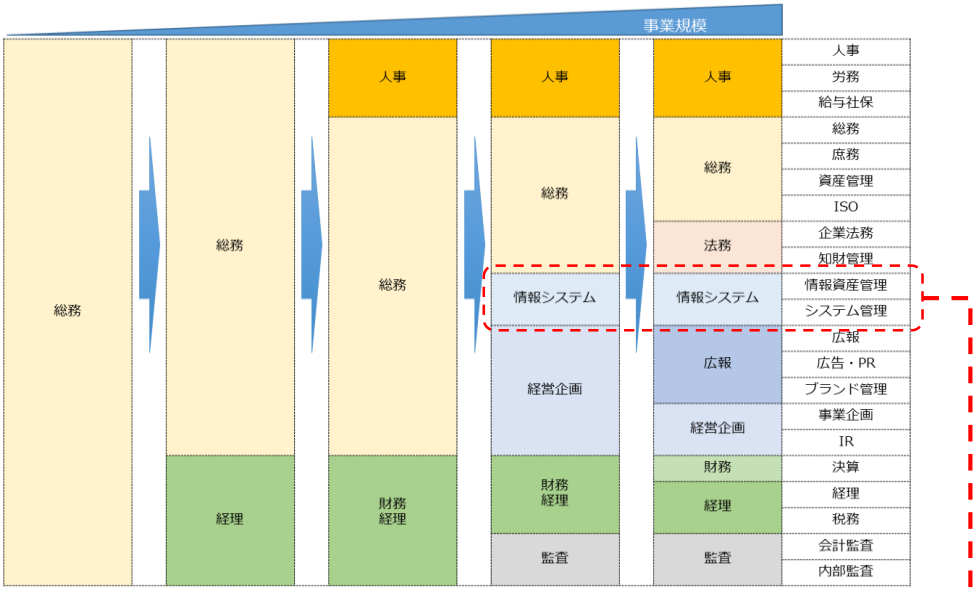
- **セキュリティ統括（室等）**
  - CRIC CSF の第一期「人材定義リファレンス」において定めた役割の1つ。組織図に記載される組織体として配置された場合には「セキュリティ統括室（部、課等も可）」となり、組織図に記載されないチーム体制を敷く場合は「セキュリティ統括」または「CSIRT」等の呼称を用いることになる。

- **セキュリティ統括人材**
  - セキュリティ統括人材は「セキュリティ統括室」または「セキュリティ統括」を構成する人材。
  - セキュリティに詳しい人材という意味ではなく、法人組織のリスクマネジメントの一環として、セキュリティ対策に従事する役割を与えられた人材を指している。
  - 尚、部署横断型のセキュリティ体制を敷いている場合、「セキュリティ統括室」または「セキュリティ統括」に所属していない場合でも、連携して活動するセキュリティ人材については、セキュリティ統括人材と同様の育成が求められると考えている。

1.セキュリティ統括室
検討の背景

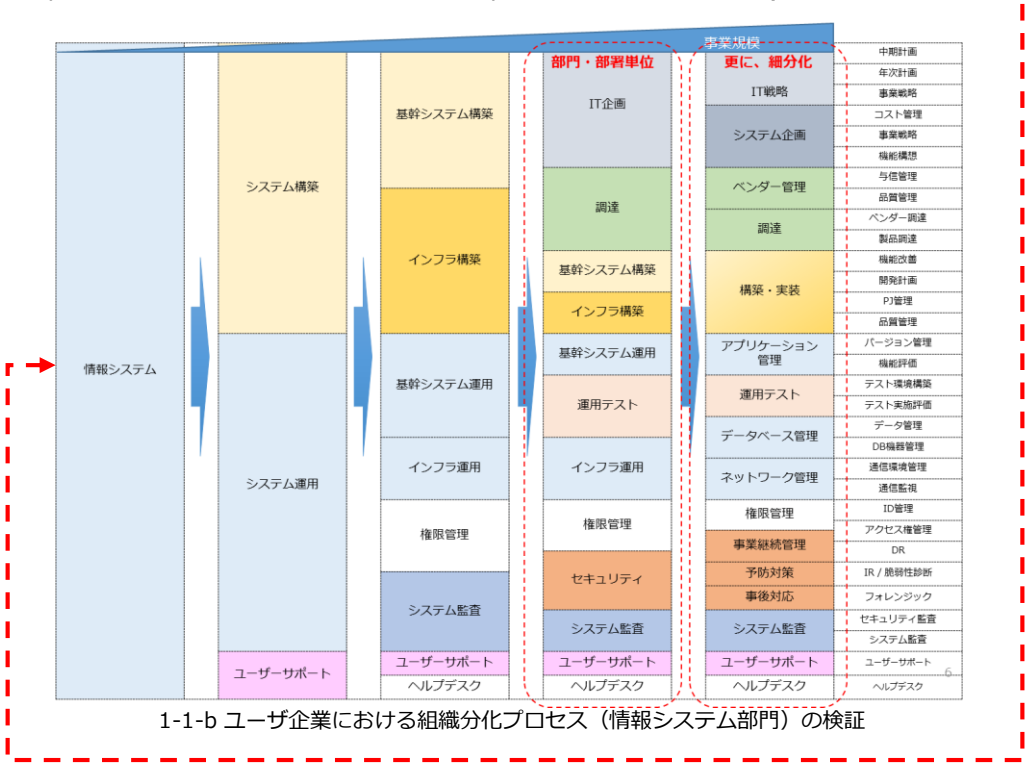
■ **セキュリティ人材とはどのような業務に従事する人材なのかを、企業における事業規模の拡大と組織機能の分化の観点から検証し、セキュリティ人材像を描くこととした。**

- **第一期の検討の流れ**
  - ユーザ企業における組織分化プロセス（総務部門～情報システム部門）の検証



1-1-a ユーザ企業における組織分化プロセス（総務部門～情報システム部門）の検証

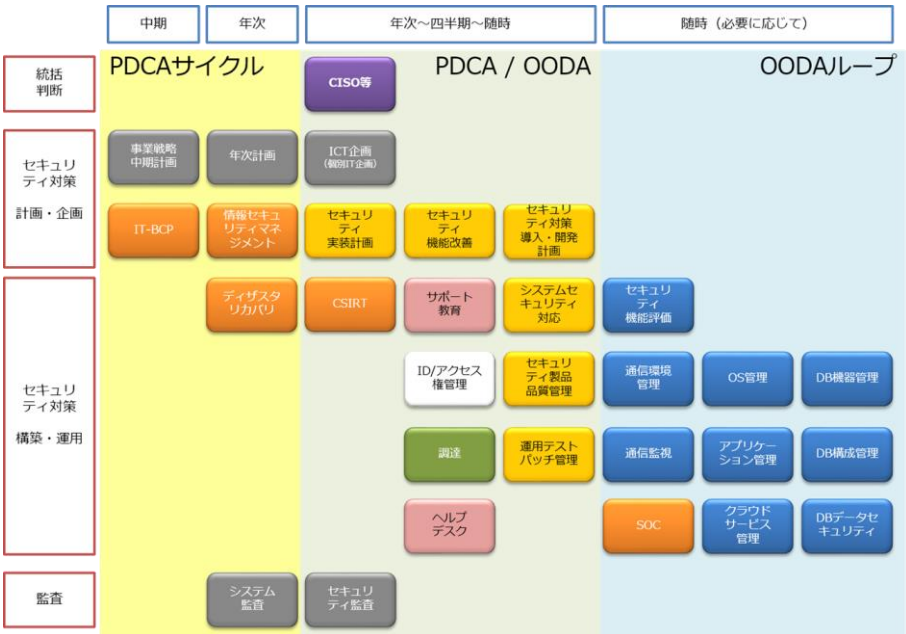
  - ユーザ企業における組織分化プロセス（情報システム部門の機能）の検証



1-1-b ユーザ企業における組織分化プロセス（情報システム部門）の検証

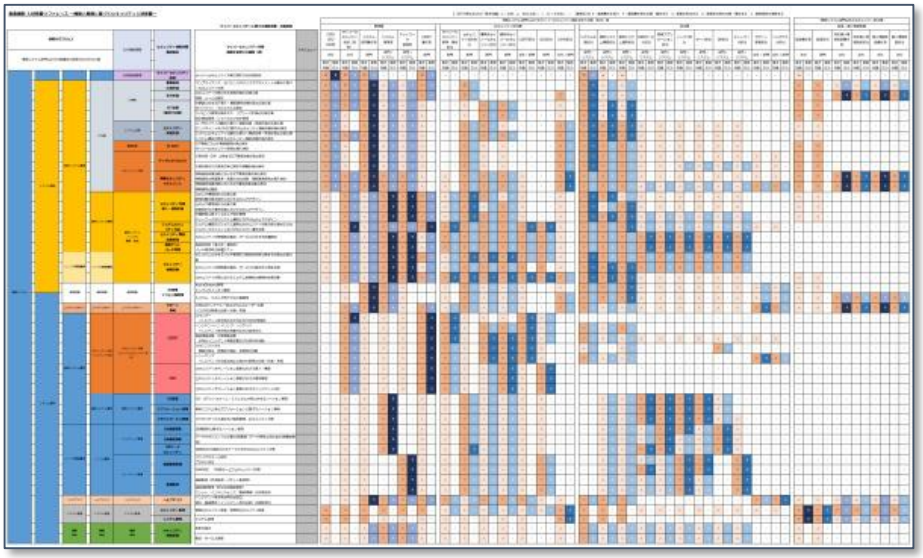
■ **セキュリティ人材を配置し、事業全体のセキュリティ機能を俯瞰するための図を作成し、更に機能と役割を整理し、必要なスキルと知識を整理した。**

- **第一期の検討の流れ**
  - CISO等がセキュリティ対策の全体像を把握するための構成図を作成。



1-1-c サイバーセキュリティ対策の機能定義（関係図）

  - 構成図に基づき、組織体制を検討するための「役割と機能」「スキルと知識」の整理を実施



1-1-d 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～

1-1. 第一期：管理するためのセキュリティと人材育成

・第一期 人材定義リファレンス

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～

機能分化プロセス 情報システム部門における組織体の役割分化プロセス例				主な機能概要	セキュリティ機能定義 最終報告	サイバーセキュリティに関する機能定義　共通項目 サイバーセキュリティ対策 機能を実現する業務（例）	スキルセット	管理職 CISO CRO CIO等 全社 要求知識	業務区分	サイバーセキュリティ統括（室等） 全社 要求知識	業務区分	システム部門責任者 部門 要求知識	業務区分	システム管理者 部門 / システム 要求知識	業務区分	ネットワーク管理者 部門 / システム 要求知識	業務区分	CSIRT責任者 部門 要求知識	業務区分
情報システム				全体統括管理	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		○	5	○	4	○	4	×	1	×	1	○	4
	システム構築	基幹システム構築	IT企画	IT戦略	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		○	4	○	4	○	5	△	4	△	4	○	4
					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		○	4	○	4	○	5	△	4	△	4	○	4
					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		○	4	○	4	○	5	△	4	△	4	△	1
						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		○	4	△	1	○	5	△	4	△	4	△	1
				システム企画	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		○	4	△	1	○	5	△	4	△	4	△	1
						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		○	4	○	4	○	5	△	4	△	4	△	1
				事業継続	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		○	4	△	1	○	5	△	4	△	4	△	1
				セキュリティ対策	ディザスタリカバリ	災害対策（DR）に関するICT環境改善計画の策定		○	4	△	1	○	5	△	4	△	4	△	1
						災害対策及び災害発生時に関する稼働計画の策定		○	4	△	1	○	5	△	4	△	4	△	1
					情報セキュリティ マネジメント	情報資産保護活動におけるICT環境改善計画の策定 情報資産の保護基準・保護方法の改善、情報漏洩保険の導入検討		○	4	○	4	○	5	○	4	○	4	△	1
						情報資産保護活動におけるICT運用改善活動の策定 情報資産の棚卸		○	4	○	4	○	5	○	4	○	4	△	1
			基幹システム構築	基幹システム インフラ 構築・実装	セキュリティ対策 導入・開発計画	セキュア構築設計の企画立案 要件定義及基本設計におけるセキュアデザイン		△	1	○	4	△	4	○	5	○	5	○	4
						セキュア運用設計の企画立案 詳細設計及び運用改善におけるセキュアデザイン		△	1	○	4	△	4	○	5	○	5	○	4
						多層防御に基づくセキュア設計管理 ネットワーク及びシステム構成に対するセキュアデザイン		△	1	○	4	△	4	○	5	○	5	○	4
					システムセキュリティ対応	システム構築及びシステム運用のセキュリティ対策分野に関するプロジェクトマネジメント及びプロジェクト運用支援		△	1	○	5	△	4	○	4	○	4	○	5
					セキュリティ製品 品質管理	セキュリティ対策関連の製品・サービスに対する評価検証		△	1	○	4	△	4	○	5	○	5	△	4
					運用テスト パッチ管理	脆弱性診断（導入時・運用時） パッチ適用時の評価テスト		△	1	○	4	△	4	○	5	○	5	△	4
			インフラ環境構築	インフラ環境構築	セキュリティ 機能改善	全システムに対するパッチ管理及び脆弱性診断に関する計画の企画立案		△	1	○	4	△	4	○	5	○	5	○	4
						セキュリティ対策関連の製品・サービスの選定及び実装支援		△	1	○	4	△	4	○	5	○	5	△	4
						セキュリティ対策におけるシステム的機能の継続的改善活動		△	1	○	4	△	4	○	5	○	5	○	4
		権限管理	権限管理	権限管理	ID管理 アクセス権管理	ActiveDirectry管理 シングルサインオン管理		×	1	△	1	○	5	○	4	△	1	×	1
						システム、フォルダ等アクセス権管理		×	1	△	1	○	5	○	4	△	1	×	1
		ユーザーサポート	ユーザーサポート	ユーザーサポート	サポート 教育	社内のICTリテラシー向上のためのユーザー支援 リスク対応教育の企画・計画・実施		×	1	○	4	○	5	○	4	△	1	○	4
	システム運用	基幹システム運用	セキュリティ対応 インシデント対応	セキュリティ対策 （サイバーセキュリティ対応）	CSIRT	コマンダー インシデント発生時の全社対応及びCISO等補佐		×	1	○	5	△	1	△	1	△	1	○	5
						インシデントハンドリング・トリアージ インシデント発生時の初動対応及び収束対応		×	1	○	4	△	1	△	1	△	1	○	5
						脅威情報収集、対策情報収集 日常のインシデント情報収集及び社内共有活動		×	1	○	4	△	1	△	1	△	1	○	5
						フォレンジックス 機器の保全、被害拡大抑止、証跡保全活動		×	1	○	4	△	1	△	1	△	1	○	5
						トレーニング インシデント対応能力向上に向けた教育の企画・計画・実施		×	1	○	4	△	1	△	1	△	1	○	5
					SOC	セキュリティオペレーション業務における導入・構築		×	1	○	4	△	1	△	1	△	1	○	5
						セキュリティオペレーション業務における運用管理		×	1	○	4	△	1	△	1	△	1	○	5
						セキュリティオペレーション業務におけるインシデント対応		×	1	○	4	△	1	△	1	△	1	○	5
			基幹システム運用	基幹システム運用	OS管理	OS・プラットフォーム・ミドルウェア等に対するバージョン管理		×	1	△	1	△	1	○	5	×	1	△	1
					アプリケーション管理	基幹システム等のアプリケーションに関するバージョン管理		×	1	△	1	△	1	○	5	×	1	△	1
					クラウドサービス管理	クラウドサービス選定及び利用管理、セキュリティ対策		×	1	△	1	△	1	○	5	×	1	△	1
			インフラ環境運用	インフラ運用	DB機器管理	DB機器等に関するバージョン管理		×	1	△	1	△	1	○	5	×	1	△	1
					DB構成管理	データマネジメントに必要なDB管理（データ特性に合わせたDB構成管理）		×	1	△	1	△	1	○	5	×	1	△	1
					DBデータ セキュリティ	DB設定及び格納されるデータに対するセキュリティ対策		×	1	△	1	△	1	○	5	×	1	△	1
					通信環境管理	ファイアウォール設定 プロキシ設定		×	1	△	1	△	1	×	1	○	5	△	1
						WAF設定　（WEBサービスセキュリティ対策）		×	1	△	1	△	1	×	1	○	5	△	1
					通信監視	通信監視（死活監視・パケット監視等）		×	1	△	1	△	1	×	1	○	5	△	1
						通信遮断管理（IPS/IDS機能管理） スレット・インテリジェンス（脅威情報）の対策活用		×	1	△	1	△	1	×	1	○	5	△	1
		ヘルプデスク	ヘルプデスク	ヘルプデスク	ヘルプデスク	インシデント発生時の問合せ窓口 端末・機器異常（インシデント発生以前）の相談窓口		×	1	△	1	○	5	○	4	○	4	○	4
		システム監査	システム監査	システム監査	セキュリティ監査	情報セキュリティ監査、物理的セキュリティ監査		○	1	○	1	○	1	○	1	○	1	○	1
					システム監査	システム監査		○	1	○	1	○	1	△	1	△	1	△	1
		購買 調達	購買 調達	購買 調達	セキュリティ 調達管理	取引先選定		△	1	△	1	△	4	○	4	○	4	△	1
						製品・サービス調達		△	1	△	1	△	4	○	4	○	4	△	1

1-1-e 産業横断 人材定義リファレンス①

1-1．第一期：管理するためのセキュリティと人材育成

【（ICT分野における）要求知識】○：必須、△：あると良い、×：なくても良い　/　【業務区分】5：業務責任を負う　4：業務責任者を支援・補佐する　3：業務を担当する　2：業務担当者を支援・補佐する　1：業務内容を理解する

情報システム部門におけるサイバーセキュリティ機能を担う役割（担当）例																																				情報システム部門以外のセキュリティ担当職											
セキュリティ担当職														担当職																						監査・個人情報保護											
サイバーセキュリティ事件・事故担当		セキュリティ設計担当		構築系サイバーセキュリティ担当		運用系サイバーセキュリティ担当		CSIRT担当		SOC担当		ISMS担当		システム企画担当		基幹システム構築担当		基幹システム運用担当		WEBサービス担当		業務アプリケーション担当		インフラ担当		サーバ担当		DB担当		ネットワーク担当		サポート教育担当		ヘルプデスク担当		監査責任者		監査担当		特定個人情報取扱責任者		特定個人情報取扱担当		個人情報取扱責任者		個人情報取扱担当	
部門		部門		部門		部門		会社 / 部門		部門		全社 / 部門		部門 / システム		部門 / システム		部門 / システム		部門 / システム		部門 / システム		部門 / システム		部門 / システム		部門 / システム		部門 / システム		会社 / 部門		会社 / 部門		会社		部門		会社		会社		会社		会社	
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	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	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	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
×	1	×	1	×	1	×	1	×	1	×	1	×	1	○	4	△	1	△	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	△	1	×	1	×	1	×	1	×	1	×	1
×	1	○	2	×	1	×	1	×	1	×		×	1	○	3	△	2	△	2	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	○	1	○	1	△	4	△	2	△	4	△	2
×	1	○	2	×	1	×	1	×	1	×	1	○	1	○	3	△	2	△	2	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	○	1	○	1	○	5	○	3	○	5	○	3
×	1	△	1	○	2	○	2	×	1	×	1	△	1	○	3	△	3	△	3	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	○	1	○	1	×	1	×	1	×	1	×	1
×	1	△	1	○	2	○	2	×	1	×	1	△	1	○	3	△	3	△	3	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	○	1	○	1	×	1	×	1	×	1	×	1
×	1	○	2	○	2	△	1	×	1	×	1	○	2	○	3	○	3	○	3	△	1	△	1	△	1	△	1	△	1	△	1	×	1	×	1	△	1	△	1	×	1	×	1	×	1	×	1
×	1	○	2	○	2	○	2	×	1	×	1	○	2	○	3	○	3	○	3	△	1	△	1	△	1	△	1	△	1	△	1	×	1	×	1	△	1	△	1	×	1	×	1	×	1	×	1
×	1	○	2	△	1	△	1	×	1	×	1	○	2	○	3	○	2	○	2	△	1	△	1	△	1	△	1	△	1	△	1	×	1	×	1	○	1	○	1	×	1	×	1	×	1	×	1
×	1	○	2	△	1	△	1	×	1	×	1	○	2	○	3	○	2	○	2	△	1	△	1	△	1	△	1	△	1	△	1	△	1	△	1	○	1	○	1	×	1	×	1	×	1	×	1
×	1	○	2	△	1	△	1	×	1	×	1	○	2	○	3	○	2	○	2	△	1	△	1	△	2	△	2	△	2	△	2	△	1	△	1	○	1	○	1	×	1	×	1	×	1	×	1
△	1	○	2	○	2	○	2	△	1	×	1	○	3	○	2	○	2	○	2	△	1	△	1	△	1	△	1	△	1	△	1	△	1	△	1	○	1	○	1	○	5	○	3	○	5	○	3
△	1	○	2	○	2	○	2	△	1	×	1	○	3	○	2	○	2	○	2	△	2	△	2	△	2	△	2	△	2	△	2	○	2	○	2	○	1	○	1	○	5	○	3	○	5	○	3
△	2	○	3	○	2	△	2	△	1	×	1	△	1	○	3	○	3	△	2	△	1	△	1	△	1	△	1	△	1	△	1	×	1	×	1	△	1	△	1	×	1	×	1	×	1	×	1
△	2	○	3	△	2	○	2	△	1	×	1	△	1	○	3	△	2	○	3	△	1	△	1	△	1	△	1	△	1	△	1	×	1	×	1	△	1	△	1	×	1	×	1	×	1	×	1
△	2	○	3	○	2	○	2	△	1	×	1	△	1	○	3	○	3	○	3	△	2	△	2	△	2	△	2	△	2	△	2	×	1	×	1	△	1	△	1	×	1	×	1	×	1	×	1
○	3	○	2	○	2	○	2	○	3	○	3	△	1	○	2	○	2	○	3	△	2	△	2	△	2	△	2	△	2	△	2	△	1	△	1	×	1	×	1	×	1	×	1	×	1	×	1
○	2	○	2	○	2	○	2	○	2	○	2	△	1	○	2	○	2	○	2	○	3	○	3	○	3	○	3	○	3	○	3	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
○	2	○	2	○	2	○	2	○	2	○	2	△	1	○	2	○	2	○	2	○	3	○	3	○	3	○	3	○	3	○	3	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	2	○	3	○	3	○	3	○	2	○	2	△	1	○	3	○	2	○	2	○	2	○	2	○	2	○	2	○	2	○	2	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	2	○	2	○	2	○	2	○	1	○	1	△	1	○	3	○	3	○	3	○	2	○	2	○	2	○	2	○	2	○	2	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
○	3	○	3	○	3	○	3	○	3	○	3	○	2	○	3	○	3	○	3	△	1	△	1	△	1	△	1	△	1	△	1	×	1	×	1	△	1	△	1	×	1	×	1	×	1	×	1
△	1	○	2	△	2	△	2	△	1	×	1	△	1	○	2	○	2	○	3	△	1	△	1	△	1	△	1	△	1	△	1	△	2	△	2	△	1	△	1	×	1	×	1	×	1	×	1
△	1	○	2	△	2	△	2	△	1	×	1	○	2	○	2	○	2	○	3	△	1	△	1	△	1	△	1	△	1	△	1	△	2	△	2	△	1	△	1	○	4	○	2	○	4	○	2
△	2	○	2	△	2	△	2	△	1	×	1	○	2	○	2	△	2	△	2	△	1	△	1	△	1	△	1	△	1	△	1	○	3	○	2	△	1	△	1	○	5	○	3	○	5	○	3
○	3	△	1	△	1	△	1	○	3	△	2	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
○	3	△	1	○	2	○	2	○	3	△	2	×	1	○	2	△	2	○	2	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
○	3	△	1	○	3	○	3	○	3	△	2	×	1	○	2	△	2	△	2	△	1	△	1	△	1	△	1	△	1	△	1	△	1	△	1	×	1	×	1	×	1	×	1	×	1	×	1
○	2	△	1	○	3	○	3	○	3	△	1	×	1	△	2	×	1	△	2	×	1	×	1	×	1	×	1	○	2	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
○	2	△	1	○	3	○	3	○	3	△	1	×	1	○	2	△	2	△	2	×	1	×	1	×	1	×	1	×	1	×	1	○	3	○	2	×	1	×	1	×	1	×	1	×	1	×	1
○	2	△	1	△	2	○	3	△	1	○	3	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
○	2	△	1	△	2	○	3	△	1	○	3	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
○	2	△	1	△	2	○	3	△	1	○	3	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	1	○	2	△	2	△	2	△	1	△	1	×	1	×	1	△	2	△	2	○	3	○	3	○	3	○	3	△	2	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	1	○	2	△	2	△	2	△	1	△	1	×	1	×	1	△	2	△	2	○	3	○	3	○	3	○	3	△	2	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	1	○	2	△	2	△	2	△	1	△	1	×	1	×	1	△	2	△	2	○	3	○	3	○	3	○	3	△	2	△	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	1	○	2	△	2	△	2	△	1	△	1	×	1	×	1	△	2	△	2	△	2	○	3	○	3	△	2	○	3	△	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	1	○	2	△	2	△	2	△	1	△	1	×	1	×	1	△	2	△	2	△	2	○	3	△	2	△	2	○	3	△	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	1	○	3	△	2	△	2	△	1	△	1	×	1	×	1	△	2	△	2	○	3	○	3	△	2	△	2	○	3	△	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	1	○	2	△	2	△	2	△	1	○	2	×	1	×	1	△	2	△	2	△	2	△	2	○	3	○	3	×	1	○	3	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	1	○	2	△	2	△	2	△	1	○	2	×	1	×	1	△	2	△	2	○	3	△	2	○	3	○	3	×	1	○	3	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	1	○	2	△	2	△	2	△	1	○	2	×	1	×	1	△	2	△	2	△	2	△	2	○	3	△	2	×	1	○	3	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
△	1	○	2	△	2	△	2	△	1	○	2	×	1	×	1	△	2	△	2	△	2	△	2	○	3	△	2	×	1	○	3	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1
○	2	△	2	○	2	○	2	○	2	△	1	△	1	○	2	○	2	○	2	×	1	×	1	×	1	×	1	×	1	×	1	○	2	○	3	△	1	△	1	△	4	△	2	△	4	△	2
△	2	△	2	△	2	△	2	△	2	△	2	○	3	○	1	○	1	○	1	△	1	△	1	△	1	△	1	△	1	△	1	△	1	△	1	○	5	○	3	○	4	○	2	○	4	○	2
△	1	△	1	△	1	△	1	△	1	×	1	○	3	○	1	○	1	○	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	×	1	○	5	○	3	△	4	△	2	△	4	△	2
△	1	△	1	△	1	△	1	△	1	×	1	△	1	○	2	△	2	△	2	△	2	△	2	△	2	△	2	△	2	△	2	×	1	×	1	△	1	△	1	×	1	×	1	×	1	×	1
△	1	△	1	△	1	△	1	△	1	×	1	△	1	○	2	△	2	△	2	△	2	△	2	△	2	△	2	△	2	△	2	×	1	×	1	△	1	△	1	×	1	×	1	×	1	×	1

1-1-f 産業横断 人材定義リファレンス②

1-1. 第一期：管理するためのセキュリティと人材育成

• 第一期 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～

- セキュリティ対策カレンダーは、人材定義リファレンスに基づき、CISO等を担う方が、自社のセキュリティの取り組みの全体像を、カレンダー形式で把握するために作成されました。

- セキュリティ対策というと、事後のインシデント対応に意識が向きがちですが、PDCAサイクルを回す情報セキュリティマネジメントの取り組みと、OODAループで回すセキュリティインシデント対応のバランスを取るためのツールとして公開しています。

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～

		サイバーセキュリティに関する機能定義　共通項目		AtoZ 共通項目		
主な機能概要	セキュリティ機能定義 最終報告	サイバーセキュリティ対策 機能を実現する業務（例）	スキルセット	月例	定常（日次）業務	インシデント発生時
全体統括管理	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		リスクマネジメント委員会 経営会議		
IT戦略	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		リスクマネジメント委員会 経営会議		
	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		経営会議	CIO/CISO支援 規程・ルール策定・改定	CIO/CISO支援
	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		IT戦略会議	CIO/CISO支援 ガイドライン・マニュアル改定	インシデント対応判断 （全体）
		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		セキュリティ対応進捗会議	セキュリティ対応進捗評価	インシデント対応状況評価
システム企画	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			システム運用に対するセキュリティ対策評価	インシデント対応状況評価
		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			システム・機器等に対するセキュリティ対策評価	インシデント対応状況評価
事業継続	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		リスクマネジメント委員会 CIO/CISO支援	バックアップ体制維持 システム更新対応	システム更新評価
セキュリティ対策	ディザスタリカバリ	災害対策（DR）に関するICT環境改善計画の策定		リスクマネジメント委員会 CIO/CISO支援	災害関連情報収集 災害対策ツール情報収集	
		災害対策及び災害発生時に関する稼働計画の策定				インシデント対応判断 （災害）
	情報セキュリティ マネジメント	情報資産保護活動におけるICT環境改善計画の策定 情報資産の保護基準・保護方法の改善、情報漏洩保険の導入検討		ISMS委員会		
		情報資産保護活動におけるICT運用改善活動の策定 情報資産の棚卸		教育計画策定 インシデント注意喚起		インシデント対応判断 （情報資産）
基幹システム インフラ 構築・実装	セキュリティ対策 導入・開発計画	セキュア構築設計の企画立案 要件定義及基本設計におけるセキュアデザイン		構築PJ セキュリティ対応	構築PJ セキュリティ対応	構築PJ セキュリティ対応
		セキュア運用設計の企画立案 詳細設計及び運用改善におけるセキュアデザイン			セキュリティ対策 運用状況監視	運用PJ セキュリティ対応
		多層防御に基づくセキュア設計管理 ネットワーク及びシステム構成に対するセキュアデザイン			インシデント情報収集	OSIプレイヤー整合性評価
	システムセキュリティ対応	システム構築及びシステム運用のセキュリティ対策分野に関するプロジェクトマネジメント及びプロジェクト運用支援		インシデント対応PJ運営 （緊急対応含む）	インシデント対応PJ運営 （緊急対応含む）	インシデント対応PJ運営 （緊急対応含む）
	セキュリティ製品品質管理	セキュリティ対策関連の製品・サービスに対する評価検証			セキュリティ製品評価 セキュリティサービス評価	導入システム 評価支援
	運用テスト パッチ管理	脆弱性診断（導入時・運用時） パッチ適用時の評価テスト			OS/アプリ/ファームウェアVer管理・パッチ適用、脆弱性診断	OS/アプリ/ファームウェアVer管理・パッチ適用
	セキュリティ 機能改善	全システムに対するパッチ管理及び脆弱性診断に関する計画の企画立案		IT資産管理 パッチ適用情報管理	パッチ情報収集 脆弱性診断	パッチ適用評価支援
		セキュリティ対策関連の製品・サービスの選定及び実装支援			セキュリティ製品評価	セキュリティ製品評価支援
		セキュリティ対策におけるシステム的機能の継続的改善活動			インシデント情報収集 セキュリティ製品情報収集	
権限管理	ID管理 アクセス権管理	ActiveDirectry管理 シングルサインオン管理		ID棚卸	人事異動等対応 外注先アカウント付与	設定変更
		システム、フォルダ等アクセス権管理		アクセス権棚卸	人事異動等対応 外注先アクセス権付与	設定変更
ユーザーサポート	サポート 教育	社内のICTリテラシー向上のためのユーザー支援 リスク対応教育の企画・計画・実施		インシデント注意喚起 教育計画策定	社内連絡窓口 入社社員教育/教育情報収集	レポート作成等 対応収束後研修テーマ修正
セキュリティ対策 （サイバーセキュリティ対応）	CSIRT	コマンダー インシデント発生時の全社対応及びCISO等補佐		各種委員会報告	インシデント対応PJ管理	インシデント対応判断 （サイバーリスク）
		インシデントハンドリング・トリアージ インシデント発生時の初動対応及び収束対応			インシデント対応手順改善	インシデント初動対応
		脅威情報収集、対策情報収集 日常のインシデント情報収集及び社内共有活動		月例レポート作成	情報収集・分析業務 レポート作成等	情報収集・分析業務 レポート作成等
		フォレンジックス 機器の保全、被害拡大抑止、証跡保全活動				フォレンジクス
		トレーニング インシデント対応能力向上に向けた教育の企画・計画・実施		教育計画策定 インシデント注意喚起	インシデント対応トレーニング企画実施	
	SOC	セキュリティオペレーション業務における導入・構築				
		セキュリティオペレーション業務における運用管理		月例レポート作成	監視業務 稼働状況レポート作成等	設定変更
		セキュリティオペレーション業務におけるインシデント対応				インシデント 初動対応
基幹システム運用	OS管理	OS・プラットフォーム・ミドルウェア等に対するバージョン管理		ライセンス管理	OS等Ver管理	OS等Ver管理
	アプリケーション管理	基幹システム等のアプリケーションに関するバージョン管理		ライセンス管理	アプリケーションVer管理	アプリケーションVer管理
	クラウドサービス管理	クラウドサービス選定及び利用管理、セキュリティ対策		クラウドサービス管理	クラウドサービス・サポート情報管理	サービス見直し、データ移管対応等
データベース管理	DB機器管理	DB機器等に関するバージョン管理		ライセンス管理	アプリケーションVer管理 ファームウェアVer管理	アプリケーションVer管理 ファームウェアVer管理
	DB構成管理	データマネジメントに必要なDB管理（データ特性に合わせたDB構成管理）		DB構成管理	DB構成管理	設定変更
	DBデータ セキュリティ	DB設定及び格納されるデータに対するセキュリティ対策		ログ管理	DBセキュリティ改善	設定変更
ネットワーク管理	通信環境管理	ファイアウォール設定 プロキシ設定		セキュリティ製品管理 ログ管理	監視業務 稼働状況レポート作成等	設定変更
		WAF設定　（WEBサービスセキュリティ対策）		ログ管理	監視業務 稼働状況レポート作成等	設定変更
	通信監視	通信監視（死活監視・パケット監視等）		セキュリティ製品管理 ログ管理	監視業務 稼働状況レポート作成等	設定変更
		通信遮断管理（IPS/IDS機能管理） スレット・インテリジェンス（脅威情報）の対策活用		ログ管理	監視業務 稼働状況レポート作成等	設定変更
ヘルプデスク	ヘルプデスク	インシデント発生時の問合せ窓口 端末・機器異常（インシデント発生以前）の相談窓口			社内通報窓口	レポート作成等
システム監査	セキュリティ監査	情報セキュリティ監査、物理的セキュリティ監査		監査役会支援	監査役会支援	リスクマネジメント委員会支援
	システム監査	システム監査		監査役会支援	監査役会支援	リスクマネジメント委員会支援
購買 調達	セキュリティ 調達管理	取引先選定			新規取引先審査	
		製品・サービス調達			購買申請受付対応	

1-1-g 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～①

1-1. 第一期：管理するためのセキュリティと人材育成

年間スケジュール一覧（例）

年間カレンダー

第１四半期（例：4月～6月）			第２四半期（例：7月～9月）			第３四半期（例：10月～12月）			第４四半期（例：1月～3月）		
方針発表		年次計画進捗確認			年次計画進捗確認 規程改定			年次計画進捗確認	次年度 セキュリティ対策計画	次年度 セキュリティ対策計画	次年度 セキュリティ対策計画 規程改定
		年次計画進捗確認			年次計画進捗確認 ガイドライン改定			年次計画進捗確認	次年度 セキュリティ対策計画	次年度 セキュリティ対策計画	次年度 セキュリティ対策計画 ガイドライン改定
					システム運用におけるKPI評価					システム運用におけるKPI修正	システム運用におけるKPI策定
					システム機能改善計画評価					次年度 システム機能改善計画	次年度 システム機能改善計画
						機能改善計画修正				エンドポイントセキュリティ対策計画	エンドポイントセキュリティ対策計画
方針発表			IT-BCP内部監査	IT-BCP是正措置	IT-BCP訓練計画	IT-BCP訓練			IT-BCP内部監査	IT-BCP是正措置	IT-BCP策定
					防災訓練計画		法定停電対策(例)			（防災訓練計画）	
						防災訓練		法定停電対応			（防災訓練）
方針発表			ISMS内部監査						ISMS内部監査		ISMS更新審査計画
新規入社社員教育				ISMS是正措置		新任者セキュリティ教育				ISMS是正措置	
									次年度 構築PJ 設計支援	次年度 構築PJ 設計支援	次年度 構築PJ 設計支援
運用改善 設計支援			運用改善 設計支援			運用改善 設計支援				次年度 運用PJ 設計	次年度 運用PJ 設計
			運用改善評価			運用改善評価					
		パッチ適用状況確認			パッチ適用状況確認			パッチ適用状況確認			パッチ適用状況確認
		パッチマネジメント運用状況評価		（IT機器棚卸）	パッチマネジメント運用状況評価			パッチマネジメント運用状況評価		IT機器棚卸	パッチマネジメント計画策定
					セキュリティ機能運用評価・製品評価						セキュリティ機能運用改善・製品改善
		エンドポイントセキュリティ対策評価			エンドポイントセキュリティ対策評価			エンドポイントセキュリティ対策評価			エンドポイントセキュリティ対策評価
		人事異動ID管理			人事異動ID管理			人事異動ID管理			新入社員ID管理 人事異動ID管理
		人事異動アクセス権管理			人事異動アクセス権管理			人事異動アクセス権管理			新入社員アクセス権 人事異動アクセス権
新規入社社員教育 ISMS/Pマーク研修	GW明けのマルウェア対策			お盆休み明けのマルウェア対策	稼働状況評価	新任者セキュリティ教育 ISMS/Pマーク研修			正月休み明けのマルウェア対策		次年度 体制計画
					CSIRT稼働状況評価					次年度 CSIRT体制計画	次年度 CSIRT体制計画
					インシデント対応手順改定						インシデント対応手順改定
新規入社社員教育 GW 注意喚起		インシデント対応演習		夏季休業 注意喚起	インシデント対応演習	新任者セキュリティ教育		新年 注意喚起 インシデント対応演習		サイバーセキュリティ月間-イベント	インシデント対応演習
					対象機器の棚卸						対象機器の棚卸
					ライセンス評価						ライセンス評価
					ライセンス評価						ライセンス評価
										次年度 構築PJ 設計支援	次年度 構築PJ 設計支援
					DBセキュリティ設定評価						DBセキュリティ計画
		FW 設定評価			FW 設定評価			FW 設定評価			FW 設定評価
		WAF 設定評価			WAF 設定評価			WAF 設定評価			WAF 設定評価
					稼働状況評価						次年度 体制計画
			内部監査	是正措置					内部監査	是正措置	
会計監査対応	会計監査対応		内部監査	是正措置					内部監査	是正措置	
			取引先監査						取引先監査		
									次年度 調達計画	次年度 調達計画	

1-1-h 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～②

1-1. 第一期：管理するためのセキュリティと人材育成

• 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

- セキュリティオペレーション アウトソーシングガイドは、人材定義リファレンスに基づき、社内の業務と社外へ委託可能な業務を整理するために作成されました。
- 人材定義リファレンスでは、セキュリティ業務は情報システムに関わる全ての業務において分担されるものと定めています。
- しかしながら昨今のサイバー攻撃に代表される様々なインシデントはIT領域という可視化が難しい業務であることから、時に、外部の専門家を招聘する必要もあります。
- そこで、アウトソーシングガイドを通じて、自社で対応する範囲と社外へ委託する範囲を整理する指標として公開しています。

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

		サイバーセキュリティに関する機能定義　共通項目		AtoZ 共通項目		
主な機能概要	セキュリティ機能定義 最終報告	サイバーセキュリティ対策 機能を実現する業務（例）	スキルセット	月例	定常（日次）業務	インシデント発生時
全体統括管理	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		リスクマネジメント委員会 経営会議		
IT戦略	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		リスクマネジメント委員会 経営会議		
	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		経営会議	CIO/CISO支援 規程・ルール策定・改定	CIO/CISO支援
	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		IT戦略会議	CIO/CISO支援 ガイドライン・マニュアル改定	インシデント対応判断（全体）
		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		セキュリティ対応進捗会議	セキュリティ対応進捗評価	インシデント対応状況評価
システム企画	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			システム運用に対するセキュリティ対策評価	インシデント対応状況評価
		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			システム・機器等に対するセキュリティ対策評価	インシデント対応状況評価
事業継続	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		リスクマネジメント委員会 CIO/CISO支援	バックアップ体制維持 システム更新対応	システム更新評価
セキュリティ対策	ディザスタリカバリ	災害対策（DR）に関するICT環境改善計画の策定		リスクマネジメント委員会 CIO/CISO支援	災害関連情報収集 災害対策ツール情報収集	
		災害対策及び災害発生時に関する稼働計画の策定				インシデント対応判断（災害）
	情報セキュリティマネジメント	情報資産保護活動におけるICT環境改善計画の策定 情報資産の保護基準・保護方法の改善、情報漏洩保険の導入検討		ISMS委員会		
		情報資産保護活動におけるICT運用改善活動の策定 情報資産の棚卸		教育計画策定 インシデント注意喚起		インシデント対応判断（情報資産）
基幹システム インフラ 構築・実装	セキュリティ対策導入・開発計画	セキュア構築設計の企画立案 要件定義及基本設計におけるセキュアデザイン		構築PJ セキュリティ対応	構築PJ セキュリティ対応	構築PJ セキュリティ対応
		セキュア運用設計の企画立案 詳細設計及び運用改善におけるセキュアデザイン			セキュリティ対策 運用状況監視	運用PJ セキュリティ対応
		多層防御に基づくセキュア設計管理 ネットワーク及びシステム構成に対するセキュアデザイン			インシデント情報収集	OSI7レイヤー整合性評価
	システムセキュリティ対応	システム構築及びシステム運用のセキュリティ対策分野に関するプロジェクトマネジメント及びプロジェクト運用支援		インシデント対応PJ運営（緊急対応含む）	インシデント対応PJ運営（緊急対応含む）	インシデント対応PJ運営（緊急対応含む）
	セキュリティ製品品質管理	セキュリティ対策関連の製品・サービスに対する評価検証			セキュリティ製品評価 セキュリティサービス評価	導入システム 評価支援
	運用テスト パッチ管理	脆弱性診断（導入時・運用時） パッチ適用時の評価テスト			OS/アプリ/ファームウェアVer管理・パッチ適用、脆弱性診断	OS/アプリ/ファームウェアVer管理・パッチ適用
	セキュリティ機能改善	全システムに対するパッチ管理及び脆弱性診断に関する計画の企画立案		IT資産管理 パッチ適用情報管理	パッチ情報収集 脆弱性診断	パッチ適用評価支援
		セキュリティ対策関連の製品・サービスの選定及び実装支援			セキュリティ製品評価	セキュリティ製品評価支援
		セキュリティ対策におけるシステム的機能の継続的改善活動			インシデント情報収集 セキュリティ製品情報収集	
権限管理	ID管理 アクセス権管理	ActiveDirectry管理 シングルサインオン管理		ID棚卸	人事異動等対応 外注先アカウント付与	設定変更
		システム、フォルダ等アクセス権管理		アクセス権棚卸	人事異動等対応 外注先アクセス権付与	設定変更
ユーザーサポート	サポート 教育	社内のICTリテラシー向上のためのユーザー支援 リスク対応教育の企画・計画・実施		インシデント注意喚起	社内連絡窓口	レポート作成等
セキュリティ対策（サイバーセキュリティ対応）	CSIRT	コマンダー インシデント発生時の全社対応及びCISO等補佐		各種委員会報告	インシデント対応PJ管理	インシデント対応判断（サイバーリスク）
		インシデントハンドリング・トリアージ インシデント発生時の初動対応及び収束対応			インシデント対応改善	インシデント初動対応
		脅威情報収集、対策情報収集 日常のインシデント情報収集及び社内共有活動		月例レポート作成	情報収集・分析業務 レポート作成等	情報収集・分析業務 レポート作成等
		フォレンジックス 機器の保全、被害拡大抑止、証跡保全活動				フォレンジクス
		トレーニング インシデント対応能力向上に向けた教育の企画・計画・実施		教育計画策定 インシデント注意喚起	インシデント対応トレーニング企画実施	
	SOC	セキュリティオペレーション業務における導入・構築				
		セキュリティオペレーション業務における運用管理		月例レポート作成	監視業務 稼働状況レポート作成等	設定変更
		セキュリティオペレーション業務におけるインシデント対応				インシデント 初動対応
基幹システム運用	OS管理	OS・プラットフォーム・ミドルウェア等に対するバージョン管理		ライセンス管理	OS等Ver管理	OS等Ver管理
	アプリケーション管理	基幹システム等のアプリケーションに関するバージョン管理		ライセンス管理	アプリケーションVer管理	アプリケーションVer管理
	クラウドサービス管理	クラウドサービス選定及び利用管理、セキュリティ対策		クラウドサービス管理	クラウドサービス・サポート情報管理	サービス見直し、データ移管対応等
データベース管理	DB機器管理	DB機器等に関するバージョン管理		ライセンス管理	アプリケーションVer管理 ファームウェアVer管理	アプリケーションVer管理 ファームウェアVer管理
	DB構成管理	データマネジメントに必要なDB管理（データ特性に合わせたDB構成管理）		DB構成管理	DB構成管理	設定変更
	DBデータセキュリティ	DB設定及び格納されるデータに対するセキュリティ対策		ログ管理	DBセキュリティ改善	設定変更
ネットワーク管理	通信環境管理	ファイアウォール設定 プロキシ設定		セキュリティ製品管理 ログ管理	監視業務 稼働状況レポート作成等	設定変更
		WAF設定　（WEBサービスセキュリティ対策）		ログ管理	監視業務 稼働状況レポート作成等	設定変更
	通信監視	通信監視（死活監視・パケット監視等）		セキュリティ製品管理 ログ管理	監視業務 稼働状況レポート作成等	設定変更
		通信遮断管理（IPS/IDS機能管理） スレット・インテリジェンス（脅威情報）の対策活用		ログ管理	監視業務 稼働状況レポート作成等	設定変更
ヘルプデスク	ヘルプデスク	インシデント発生時の問合せ窓口 端末・機器異常（インシデント発生以前）の相談窓口			社内通報窓口	レポート作成等
システム監査	セキュリティ監査	情報セキュリティ監査、物理的セキュリティ監査		監査役会支援	監査役会支援	リスクマネジメント委員会支援
	システム監査	システム監査		監査役会支援	監査役会支援	リスクマネジメント委員会支援
購買 調達	セキュリティ調達管理	取引先選定			新規取引先審査	
		製品・サービス調達			購買申請受付対応	

1-1-i 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①

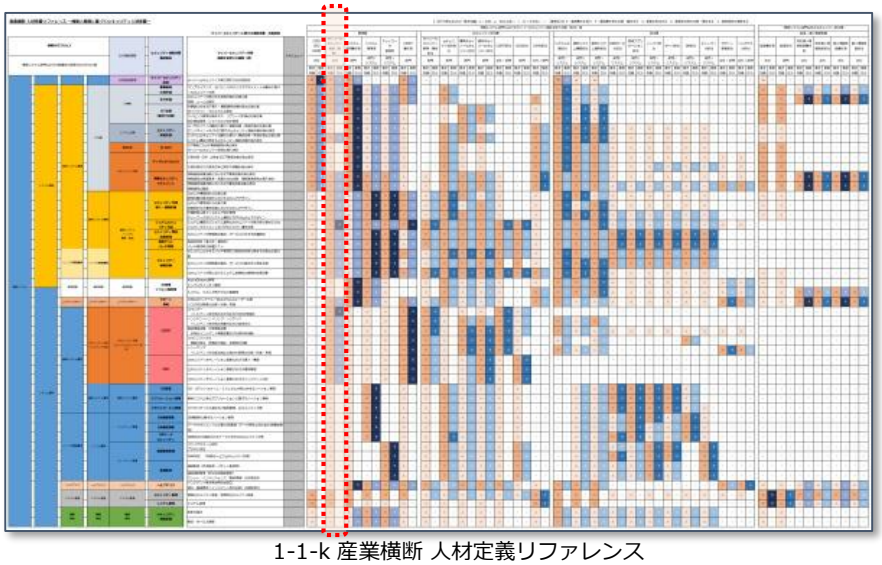
1-1. 第一期：管理するためのセキュリティと人材育成

社内業務（例）			アウトソーシング業務（例）		
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			
管理者	担当者	技術者派遣 / コンサルタント	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
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
IT戦略会議　／　CIO/CISO支援 システム単位 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 事業・システム構成に基づく次期システム提案		リスク評価・リスク分析 セキュリティ対応計画策定
セキュリティ対応進捗会議 インシデント対応計画策定	グループ企業内　セキュリティ対策状況の情報収集 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 ライセンスの切り替えに基づく次期システム提案		リスク評価・リスク分析 セキュリティ対応計画策定
システム運用プロセスに対するセキュリティ対策計画	システム運用プロセス　セキュリティ対策　要件定義	資料作成・調査分析　補助	可用性に基づくシステム改修提案		人的に起因するセキュリティインシデント対応プランの提案・情報提供
システム・機器等に対するセキュリティ対策計画	システム・機器等セキュリティ対策　要件定義	資料作成・調査分析　補助	機密性・完全性に基づくシステム改修提案		時事的なセキュリティインシデント対策プランの提案・情報提供
リスクマネジメント委員会 CIO/CISO支援	バックアップ体制維持 システム更新対応	（総務部門・経営企画部門との連携に基づく） 事業継続計画策定　補助	システム冗長化　企画立案		リスク評価・リスク分析 BCP／BCM 策定
リスクマネジメント委員会 CIO/CISO支援	災害関連情報収集 災害対策ツール情報収集		システム冗長化　構築 データセンター提供	データセンター提供	リスク評価・リスク分析 災害対策計画策定
インシデント対応判断（災害）	インシデント対応（災害）		システム冗長化　運用 データセンター運用		ディザスタリカバリー体制構築支援 データバックアップ計画策定
ISMS委員会	ISMS委員会事務局	ISMS委員会事務局（支援）	情報資産保護管理体制　構築		リスク評価・リスク分析 ISMS構築策定
教育計画策定・注意喚起 インシデント対応判断(情報資産)	インシデント対応（情報資産）	情報資産管理	情報資産の保護方法の確立	情報保管サービス提供	情報資産保護施策・保護手段の提案
構築PJ セキュリティ対応	構築PJ セキュリティ対応 要件定義、基本設計、詳細設計	設計補助	システム構築　セキュリティ対応 要件定義・基本設計・詳細設計		セキュア構築設計　レビュー
セキュリティ対策 運用状況監視	運用PJ セキュリティ対応 要件定義、基本設計、詳細設計及びレビュー	設計補助	システム運用　セキュリティ対応 要件定義・（基本設計）・詳細設計		セキュア運用設計　レビュー
NISC、IPA、JPCERT/CC等の情報収集 インシデント情報収集	OSI7レイヤー対応　整合性評価 多層防御に基づく基本設計	設計補助	多層防御に基づく詳細設計		多層防御の観点に基づく構成図レビュー
インシデント対応P)運営（緊急対応含む）	インシデント対応P)運営（緊急対応含む）		インシデント対応 構築・運用各プロジェクトへの管理・指導		インシデント対応 実務支援
セキュリティ製品評価 セキュリティサービス評価	既存システムに対する機械的適合性　評価 既存ポリシーに対する運用適合性　評価	製品・サービス評価補助	既存システムとの適合性調査 既存セキュリティポリシーとの適合性調査		
IT資産（有形・無形資産）管理 OS/ミドルウェア/アプリ/ファームウェア等　Ver管理	パッチ適用（実装） テスト環境構築、テスト実施、評価結果報告		構築・運用システム　パッチ適用	パッチ管理サービス提供	脆弱性診断サービス、テスト計画策定支援 サイバー攻撃情報提供、パッチ情報提供
IT資産管理 パッチ管理	パッチ情報収集（JVN／各ベンダー） パッチ適用情報管理	IT資産管理補助 （有形資産・無形資産・ライセンス情報等）	基幹・業務システムごとのシステム機器情報提出 パッチ対応計画の策定、進捗管理		セキュリティパッチ情報提供 セキュリティパッチ評価支援
セキュリティ製品評価	セキュリティ製品情報収集 セキュリティ製品評価		基幹・業務システムごとのセキュリティ製品適合性調査	セキュリティ製品　他社との適合性情報提供 セキュリティサービス　セキュリティ対応	セキュリティ製品評価 セキュリティサービス評価
インシデント情報収集 セキュリティ製品情報収集	インシデント情報収集（ニュース情報等） セキュリティ製品情報収集	インシデント情報管理	基幹・業務システムごとのシステム脆弱性情報収集	セキュリティ製品　脆弱性情報提供 セキュリティサービス　インシデント情報提供	インシデント対応 情報提供 インシデント対応 実務支援
ID棚卸 人事異動等対応・外注先アカウント付与	設定変更	設定変更実務	設定変更実務	シングルサインオン関連　製品・サービス情報提供 多要素認証関連　製品・サービス情報提供	認証におけるセキュリティ対策支援
アクセス権棚卸 人事異動等対応・外注先アクセス権付与	設定変更	設定変更実務	設定変更実務	アクセス権管理　製品・サービス情報提供	認証におけるセキュリティ対策支援
インシデント注意喚起 セキュリティ教育の実施	インシデント注意喚起 社内連絡窓口・レポート作成等	インシデント注意喚起 社内連絡窓口・レポート作成等	ユーザーサポート 研修企画・実施・報告	コールセンターサービス	
各種委員会報告・インシデント対応P)管理 インシデント対応判断（サイバーリスク）	各種委員会報告・インシデント対応P)管理 インシデント対応判断（サイバーリスク）				
インシデント対応改善 インシデント初動対応	インシデント初動対応	インシデント初動対応	インシデントハンドラー・インシデント管理・トリアージ ※日本シーサート協議会「CSIRT人材の定義と確保」参照		インシデントハンドラー・インシデント管理・トリアージ ※日本シーサート協議会「CSIRT人材の定義と確保」参照
月例レポート作成 情報収集・分析業務	情報収集・分析業務・レポート作成等	情報収集・分析業務・レポート作成等	セルフアセスメント・リサーチャー・キュレーター ※日本シーサート協議会「CSIRT人材の定義と確保」参照	脅威情報提供サービス	セルフアセスメント・リサーチャー・キュレーター ※日本シーサート協議会「CSIRT人材の定義と確保」参照
	フォレンジクス	インベスティゲーター	インベスティゲーター・フォレンジックス ※日本シーサート協議会「CSIRT人材の定義と確保」参照		インベスティゲーター・フォレンジックス ※日本シーサート協議会「CSIRT人材の定義と確保」参照
教育計画策定 インシデント注意喚起	インシデント対応トレーニング企画実施 インシデント注意喚起	インシデント対応トレーニング企画実施 インシデント注意喚起	教育・啓発 ※日本シーサート協議会「CSIRT人材の定義と確保」参照	インシデント対応 e-learning プログラム提供	教育・啓発 ※日本シーサート協議会「CSIRT人材の定義と確保」参照
	設計・設置・導入設定	設計・設置・導入設定	導入設計・運用設計・機器設置・ログ設定 ※日本セキュリティオペレーション事業者協議会(ISOG-J)	マネージド SOC サービス	導入設計・運用設計・機器設置・ログ設定 ※日本セキュリティオペレーション事業者協議会(ISOG-J)
監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	ツールサポート、診断と評価、脅威情報収集分析 ※日本セキュリティオペレーション事業者協議会(ISOG-J)	マネージド SOC サービス	ツールサポート、診断と評価、脅威情報収集分析 ※日本セキュリティオペレーション事業者協議会(ISOG-J)
インシデント 初動対応	インシデント初動対応	インシデント初動対応	インシデント＆証拠に対する調査分析 ※日本セキュリティオペレーション事業者協議会(ISOG-J)	マネージド SOC サービス	インシデント＆証拠に対する調査分析 ※日本セキュリティオペレーション事業者協議会(ISOG-J)
ライセンス管理	OS Ver管理	OS Ver管理	OS/ミドルウェア　パッチ対応	OS／ミドルウェア　脆弱性情報　配信	ゼロデイ対応
ライセンス管理	アプリケーションVer管理	アプリケーションVer管理	アプリケーション　パッチ対応	アプリケーション　脆弱性情報　配信	ゼロデイ対応
稼働状況・セキュリティレポート確認	稼働状況・セキュリティレポート確認	稼働状況・セキュリティレポート確認		セキュリティインシデント情報　配信	
ライセンス管理	アプリケーションVer管理 ファームウェアVer管理	アプリケーションVer管理 ファームウェアVer管理	DB機器　パッチ対応	製品　脆弱性情報　配信	ゼロデイ対応
DB構成管理	DB構成管理 設定変更	DB構成管理 設定変更	DB　構成管理		DB選定・構築プラン
運用改善・ログ管理	DBセキュリティ改善 設定変更	DBセキュリティ改善 設定変更	DBセキュリティ対策　計画・実施		DBセキュリティ対策プラン
運用改善・ログ管理	監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	ファイアウォール設置　機器監視	製品　脆弱性情報　配信	UTM（IDS/IPS）構成プラン
運用改善・ログ管理	監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	WAF　設置、機器監視	アプリケーション　脆弱性情報　配信	UTM（IDS/IPS）設定変更・最適化プラン
運用改善・ログ管理	監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	通信機器・通信状態の監視	製品　脆弱性情報　配信	
運用改善・ログ管理	監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	IDS/IPSに対するチューニング SOCデータに基づく危機への反映		
	社内通報窓口・レポート作成等	社内通報窓口・レポート作成等			インシデント対応 実務支援
監査役会支援	リスクマネジメント委員会支援				セキュリティ監査　実施
監査役会支援	リスクマネジメント委員会支援				システム監査　実施
新規取引先審査		事務アシスタント		信用調査 情報提供	
購買申請受付対応		事務アシスタント			セキュリティ対策機器・サービス 情報提供

1-1-j 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②

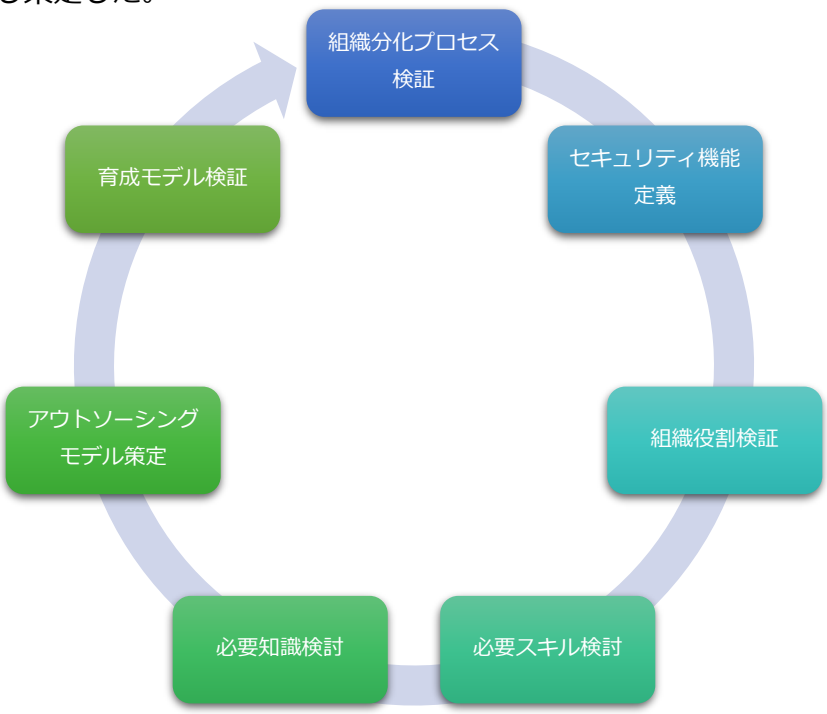
■ **IT領域におけるセキュリティ体制の全体像を「人材定義リファレンス」に定め、CISO等の役割と、その補佐となる「セキュリティ統括（室等）」を配置した。**

- **第一期**
  - IT領域（主にOA環境）に対する、既存組織体制に求められるサイバーセキュリティ対策の機能と役割を定義し「セキュリティ統括（室等）」をCISO等の下に配置した。



1-1-k 産業横断 人材定義リファレンス

  - 人材定義リファレンスの付属書類（カレンダー、アウトソーシングガイド等）は下記プロセスに基づき検証し策定した。



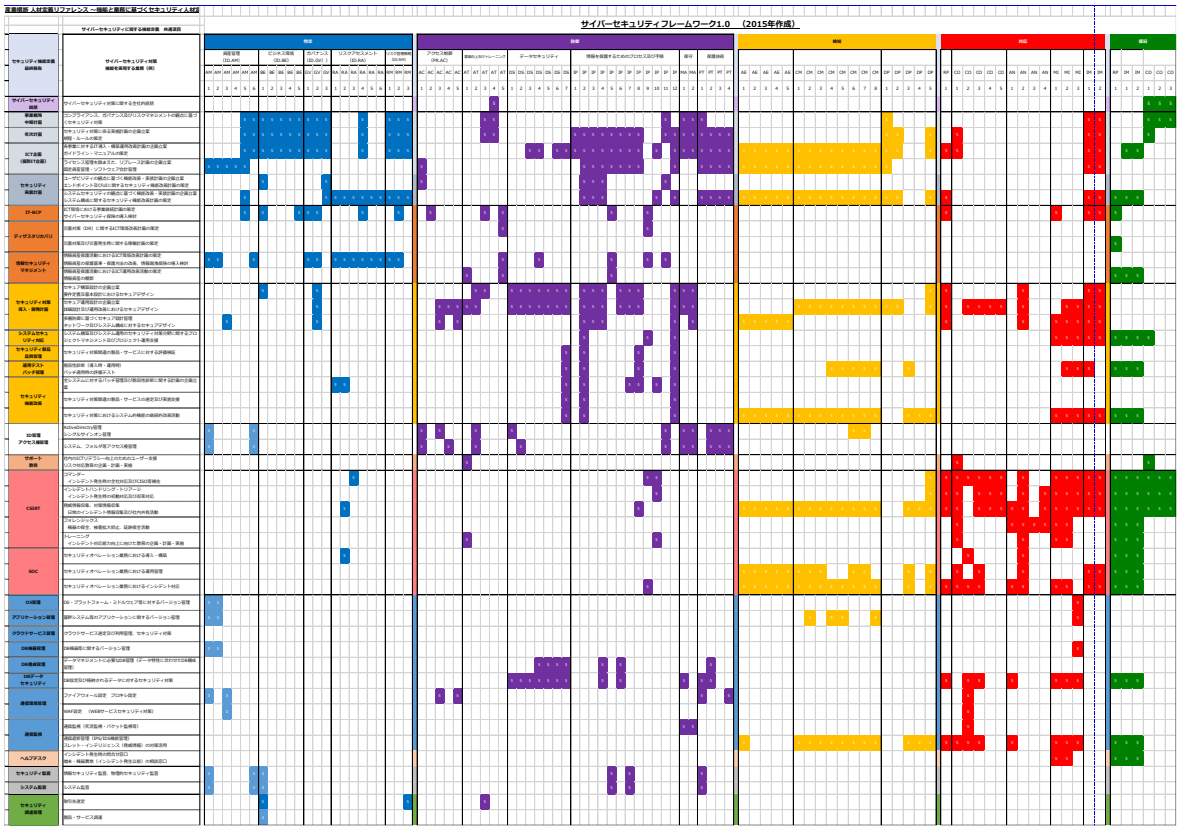
1-1-l 人材定義リファレンスの検証プロセス

1-2. 第二期：事業を支えるためのセキュリティと人材育成

■ **「人材定義リファレンス」に定めた役割を俯瞰し、対策全体を統制する役割として「セキュリティ統括室」を置くことで実装するモデルを策定。**

- **第二期**
  - 第二期では、IT領域だけではなく、OT（制御系）領域や Society5.0 におけるIoT領域に対するサイバーセキュリティの必要性が認識されたことにより、会社全体のサイバーセキュリティを統括できる役割について検証を進めてきました。
  - 特に、企業における経営や様々な事業に対するサイバーセキュリティ対策を検討する際には、事業展開している国ごとのサイバーセキュリティ法制度や各種ガイドラインの実務面での遵守、脅威情報の共有に向けた取り組みなど、これまでのIT関連業務とは異なる役割が求められることを踏まえ、情報収集や方針策定に関する業務をどの部門・部署に求めるのかについて、あるべき姿を議論しています。
  - 更に、第一期に検討を進めた米国NIST発行のサイバーセキュリティフレームワークとの関連性についても、第二期において継続的に検討を進めています。

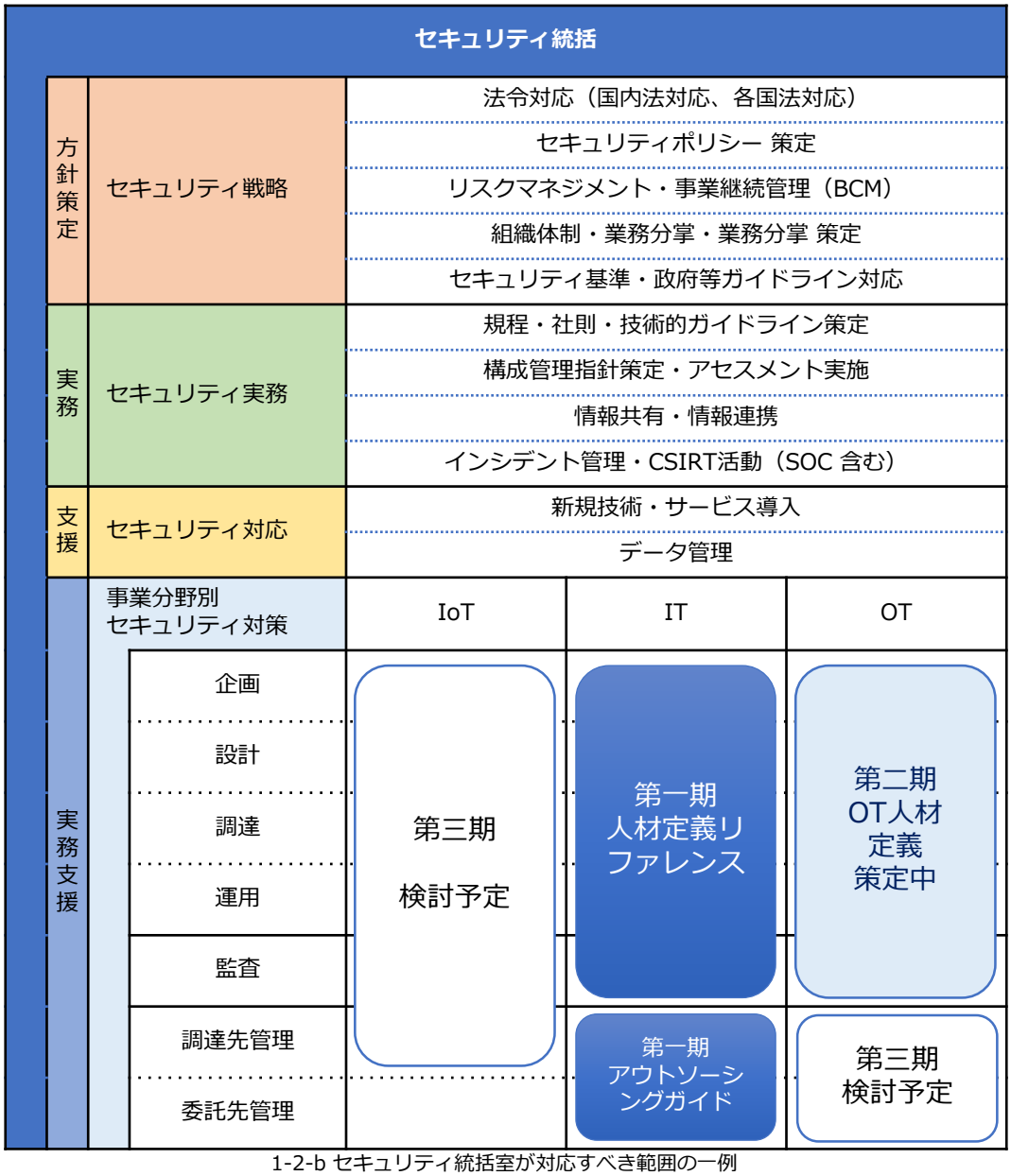
- CRIC CSF セキュリティ機能定義とNISTサイバーセキュリティフレームワーク検討図（初版）



1-2-a 産業横断セキュリティ機能定義とNISTサイバーセキュリティフレームワークとの関連性

■ **セキュリティ統括室が把握する範囲は、経営課題として認識できる全てのセキュリティ領域。**

- **セキュリティ統括室の役割とは**
  - 組織構成や人材の配置を検討する上で、事業上必須と考えられるセキュリティ対策について全体像を整理し、部署として配置した場合の業務モデルを策定しました。
  - 下記モデルに対し、ユーザ企業とベンダー企業でどのように協業・連携していくのかについて検証を進めています。
  - セキュリティ統括室が対応すべき範囲の一例



1-2-b セキュリティ統括室が対応すべき範囲の一例

1-3. 第二期：「セキュリティ統括室」の必要性に関する議論

■ **ユーザ企業の事業活動に必要となる日本を含む世界各国のサイバーセキュリティ法対応及び各国要求事項の整理、対策立案、対策状況の確認等を実行する組織の必要性。**

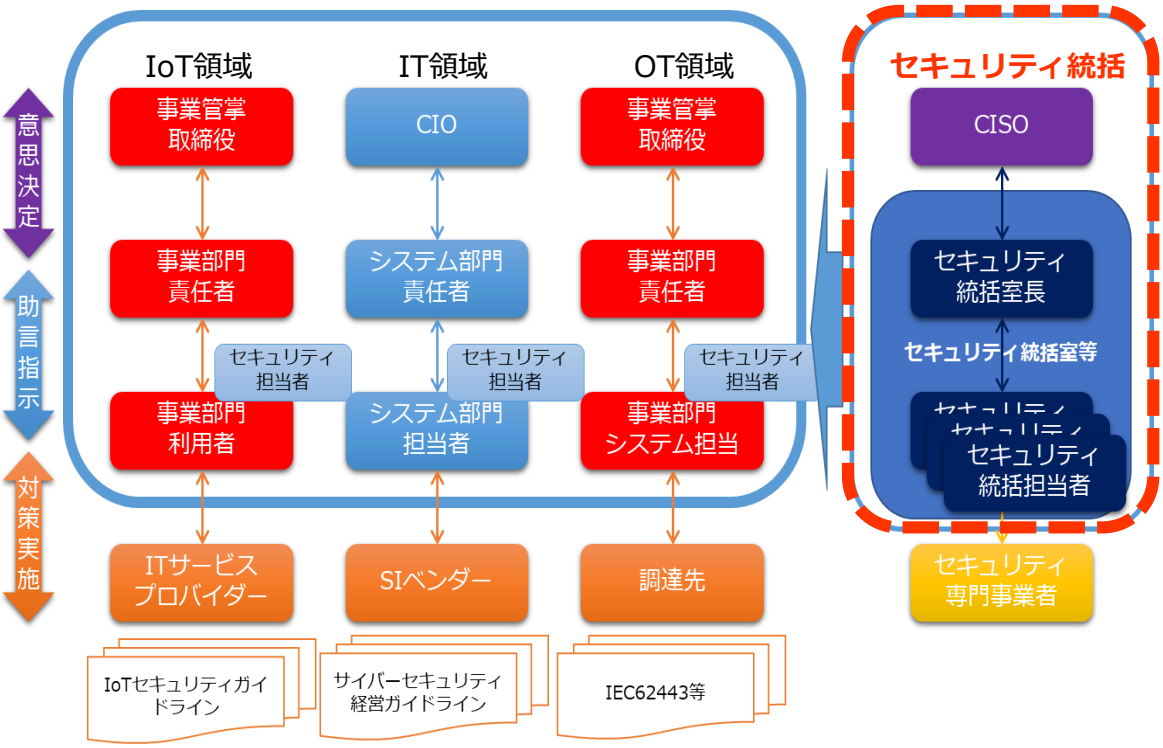
- **CRIC CSFにおける課題認識**
  - 「サイバーセキュリティは経営課題である」と定めたNISCの発表に対し、まずは経営課題となるサイバーインシデントの洗い出しを行いました。
  - 特に、ユーザ企業における経営課題の中でも、サイバーセキュリティの必要性が認識されるべきものを抽出し、どのような対応が必要かまた対応するために必要な機能はどのようなものかを議論し、解決策（モデル）を検討しています。

- **事業展開に必要となる国別対応（日本を含む）**
  - **ガバナンス（経営判断に結び付く情報収集、分析、グループセキュリティ）**
  - コンプライアンス（法令対応）及び、国別、業種別、企業規模別等のセキュリティ対策の追求
  - 事業環境に応じたセキュリティ対策における**費用対効果の追求**
- **セキュリティ対策に必要となるスキル（個人が対応するのではなく、組織化が必要）**
  - **IT領域（インフラ基盤、アプリケーション等）に対する知見**
  - システム構築・運用に対するセキュリティ対策、外注比率に基づく管理策の調整
  - 管理部門間の連携・調整（財務、経理、総務、広報、法務、調達等）
- **サプライチェーンを意識した包括的なセキュリティ対策（社内外との積極的な連携）**
  - **有効性の確保されたセキュリティ対策の実現**（サプライチェーン先への過剰な要求にならない配慮）
  - 対策状況の包括的なモニタリング、改善指導

- **セキュリティ統括室とセキュリティ統括人材に関する議論**
  - 上記課題認識に基づき、第一期に発表した「人材定義リファレンス」において配置した「セキュリティ統括（室等）」の役割を踏まえて、「室等」のあり方について組織体と人材の両面から議論を進めています。

■ **セキュリティ統括室とは、基幹となるIT、製造・運行等のOT、更にデジタルトランスフォーメーションを実現するIoT領域の全てのセキュリティ戦略に対応する組織と規定。**

- **セキュリティ統括室とは**
  - セキュリティ統括室の機能を検討する際、第一期『最終報告書』の記述に従い、IT領域だけではなく、重要インフラ事業者としてのOT領域や、新たな事業創造に向けたIoT領域におけるセキュリティを統括する重要性についても認識し、体制を検討しています。



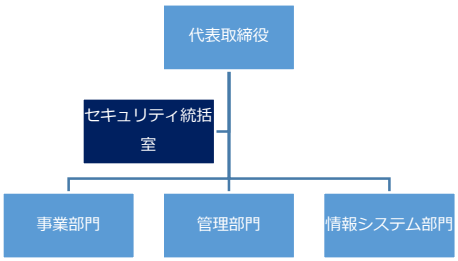
1-4-a 「セキュリティ統括室」の位置づけと対応範囲

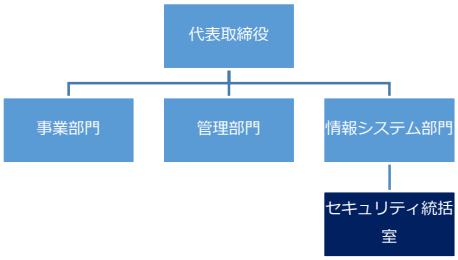
  - 上記体制を検討する中で、セキュリティ統括室は部門横断的な立場でCISO及びCIO等を補佐する部門として配置することが望ましく、更に調達先との連携を重視しサプライチェーンの観点からセキュリティ戦略を遂行することが望まれると定めました。

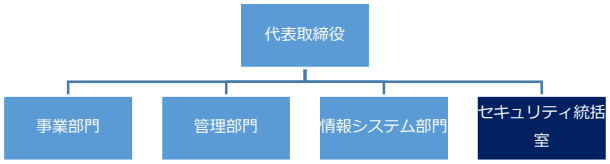
1-5. 第二期：「セキュリティ統括室」の配置及び運用の形態（例）

■ **セキュリティ統括室を配置する場合は、その役割や業務範囲に基づき、適切な配置、権限と責任等を付与していく必要がある。**

- **セキュリティ統括室の配置形態におけるメリットとデメリット**
  - セキュリティ統括室を経営判断に関与する組織体として配置することが重要です。
  - 組織として配置することは、予算執行及び適切な対処が可能となることを意味しています。更に権限と分掌を定義することにより、対応範囲を明確にし、事前準備とインシデント対応、人材育成を含むサイバーセキュリティ全体を業務とすることが可能になるという考え方です。







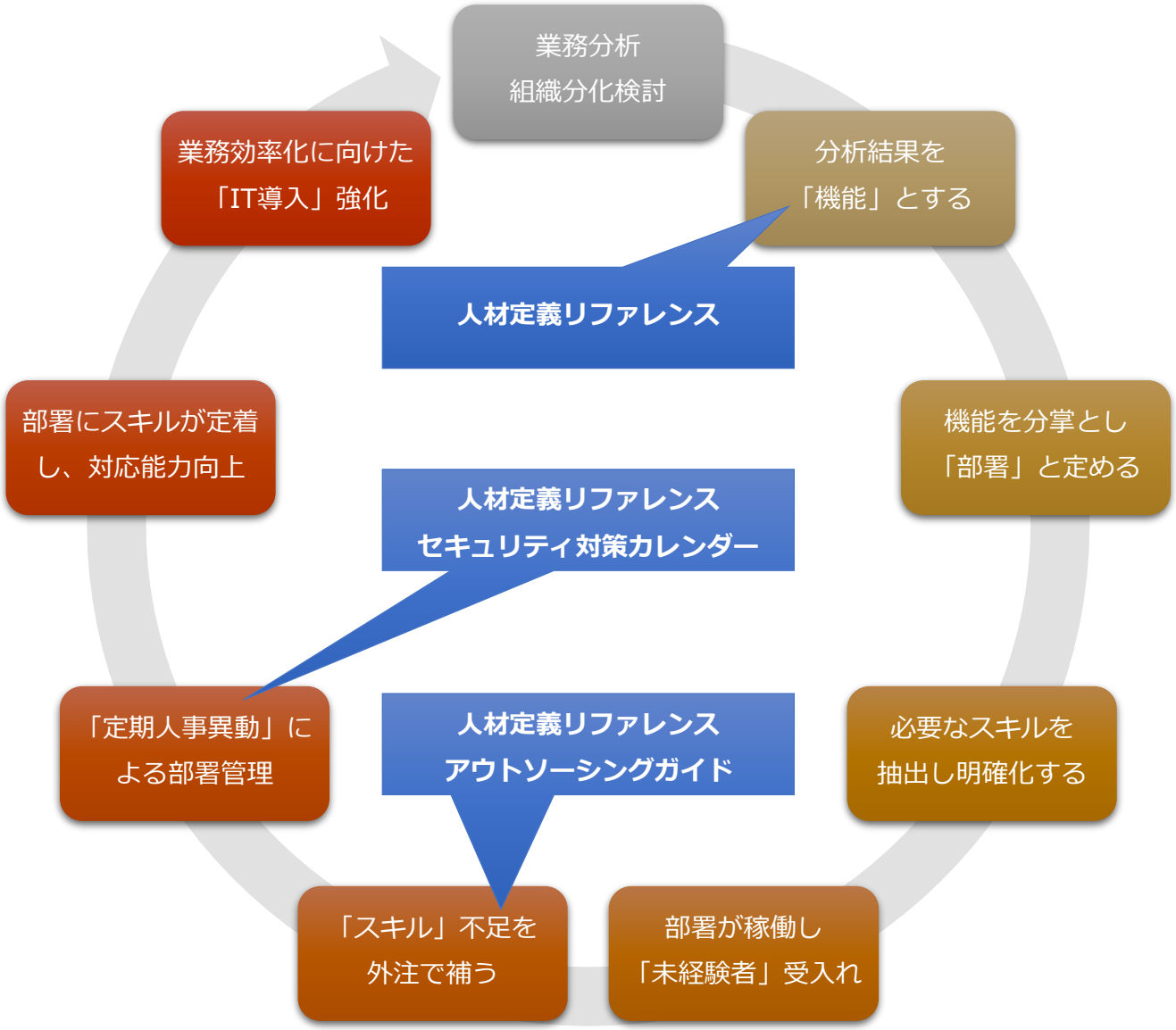
	特徴	メリット	デメリット
社長直轄型特命組織	直轄型組織は、事業活動を実施するのではなく、経営判断をサポートするために配置される。 企画に力点を置き、経営判断として各事業部門に指示を行う際の支援部署として機能する。 活動内容が明確になると組織化され独立する。	経営層の危機感を直接反映し、タイムリーな意思決定が可能である。	ERMの一部として、優先順位付けが難しく、サイバーセキュリティが経営課題となるかどうかは、高度な情報収集と調整力にかかってくる。
情報システム部門の1機能	情報システム部門の中で、セキュリティ機能を担う組織として配置。 主に、OA環境に対するシステムセキュリティについて活動を行う。法令対応や他事業部との連携は、上位者による調整により進む。IT投資枠内で活動する。	IT予算の中で活動するため、システムに関連するセキュリティ対策の強化を迅速に進められる。	外注比率が高く、更にセキュリティを非機能要件として後付けで考えている場合は、予算確保が難しく、対策の実効性に欠ける場合がある。
管理部門等との同列組織	管理部門の1つとして配置され、全社一律の対応を行う組織として配置。 人事や経理と同列にあり、事業部門を問わず、共通の標準化された対策を立案し実行する。IT投資とは別の予算措置がなされる。	管理部門の1つとして、会社として（全社統一）の方針を出すことができ、各部門に対策を指示できる。	全社のセキュリティ対策を実施できる反面、個別事業に対する対策指針を策定するノウハウを集約しにくく、対策状況のモニタリングを中心とした監査的な機能になる。

1-5-a 「セキュリティ統括室」の配置及び運用の形態（例）

2.セキュリティ統括室の設置に向けた準備

2-1. セキュリティ統括室の必要性に関する検討プロセス

- 本編では「セキュリティ統括室」の配置を検討するために必要となる外部環境への理解と既存組織体制についての確認を進めるプロセスを解説します。
- 「サイバーセキュリティは経営課題」や「サイバーセキュリティは費用ではなく投資」といった表現を適切に組織活動・事業活動に落とし込むための考え方を整理し、自社事業にどの程度必要な組織体であるのかを判断する材料を提供します。
- 以下は、第一期において「セキュリティ統括（室等）」の必要性を考えるに至った検討プロセスの例です。

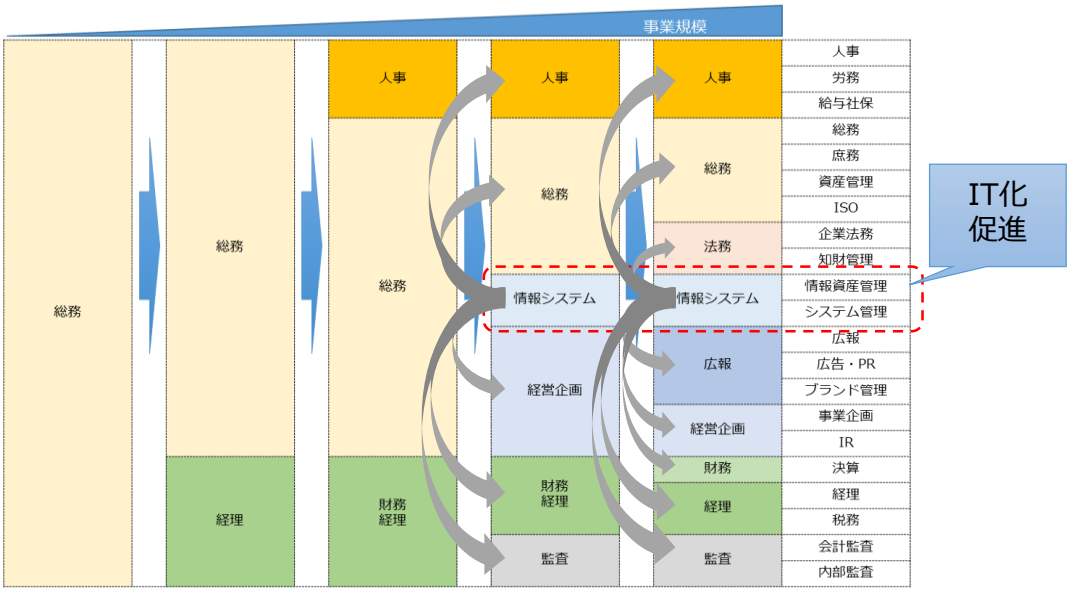


2-1-a 「セキュリティ統括室」の必要性に至る検討プロセス

- **サイバーセキュリティの必要性の議論**
  - サイバーセキュリティ対策は効果測定がはっきりせず、費用対効果が見えにくいと言われます。
  - グローバルIPで繋がるサイバー空間では、そもそも攻撃者の特定が困難であり、仮に特定できたとしても、攻撃者が被害を受けた法人の所在地（国家）と同一の国家において逮捕されなければ（攻撃者と被害者が別々の国に居る場合は）、起訴や賠償請求の実施継続が困難なケースも少なくありません。
  - 更に、サイバー攻撃による事業の損害に対する賠償についても、実際には損害額を事前に特定し相応の保険金額を掛けておく必要があり、一般的なセキュリティ関係の損害保険では、調査費用や弁護士費用、システム復旧に係るコスト等を中心として賠償されています。
  - 情報漏えいでは「お詫びの500円」は補償されるものの、訴訟によって決まる損害賠償金は補償外として扱われています。
  - 結果として、サイバー攻撃を受けた際の対処から復旧に向けたコストは自社で負担をせざるを得ず、費用対効果は、事業遅延や事業停止になった場合のネガティブリスクと、そのような事態を回避または被害軽減のための準備的な対策費用との比較が、容易な整理の仕方となります。
  - 特に、サイバーセキュリティは、情報漏えい対策だけではなく、IT利用に基づく事業活動全般に及ぶため、被害額の算定は事業運営の側面とIT資産や情報資産の側面から、複合的に算定する必要があり、既存の「情報漏えい1件あたりの賠償額」で算定を試みることは、経営判断の材料としては若干不足している可能性があります。

- **サイバーセキュリティを考える際の情報源**
  - 政府関係
    - 内閣サイバーセキュリティセンター　What's New
      - http://www.nisc.go.jp/
    - 経済産業省　情報セキュリティ政策
      - http://www.meti.go.jp/policy/netsecurity/
    - IPA　情報セキュリティ白書2018
      - https://www.ipa.go.jp/security/publications/hakusyo/2018.html
    - 総務省　情報通信白書 平成30年
      - http://www.soumu.go.jp/johotsusintokei/whitepaper/
    - 「金融機関のサイバーセキュリティ対策における経営陣・CISO等に期待される役割・責任に関する調査研究」
      - https://www.fsa.go.jp/common/about/research/20170712/20170712.html
  - 海外レポート
    - 第13回　グローバルリスク報告書（ダボス会議 討議資料）
      - https://www.marsh.com/jp/ja/insights/research/the-global-risks-report-2018.html
      - https://forbesjapan.com/articles/detail/19624
    - Horizon Scan Report 2018：BCIとBSIによるリスクマネジメントレポート
      - https://www.thebci.org/resource/horizon-scan-report-2018.html
  - メディア
    - 日経XTECH　セキュリティ
      - https://tech.nikkeibp.co.jp/theme/security/
  - 書籍
    - 経営とサイバーセキュリティ　横浜信一（日本電信電話株式会社 CISO）著
    - サイバーセキュリティマネジメント入門　鎌田敬介（一般社団法人 金融ISAC 専務理事）著

- **セキュリティの対象領域の変化（業務のIT導入に伴う効率化・高度化）**
  - これまでのIT利用は、社内の組織が細分化する過程において、業務分掌が整理され、業務内容及び業務プロセスが明確化されてきたことで、IT導入に伴う「業務効率化」が促進されてきました。
  - 特に、会計システム（経理システム）の導入により、様々な社内の手続きが電子化され、業務上のデータがITにより処理されるようになってきています。
  - この業務プロセスの変化の間では、情報セキュリティを中心とした、機密情報・重要情報の保護が企業経営において最も重要な取り組みとなっています。

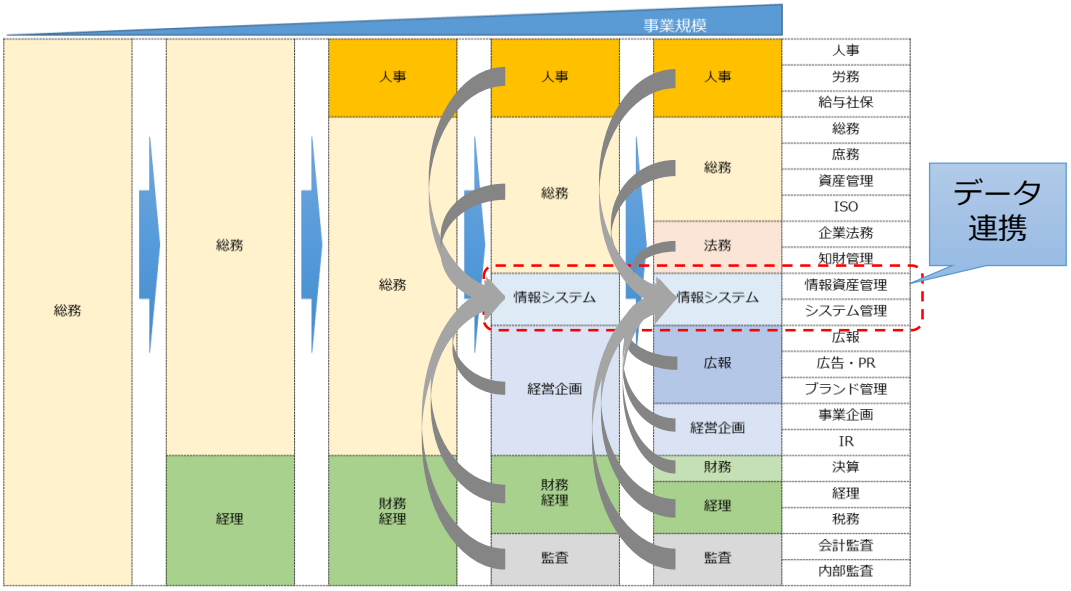


2-2-a ユーザ企業における組織分化プロセス（総務部門～情報システム部門）

  - また、内部統制の観点からも、会計に関するデータは重要視されており、特権ID管理の徹底や会計処理に関する作業履歴（ログ）管理など、情報保護の観点から様々なセキュリティ対策が行われています。
  - 更に、ERPの導入など、社内のあらゆる動きがITによって管理されるようになってきていることから、IT利用の拡大に対するセキュリティリスクが看過できない時期に来ています。

  - 結果として、内閣サイバーセキュリティセンター（NISC）等では「サイバーセキュリティは経営課題」として注意喚起するとともに、セキュリティ戦略の重要性を説いています。

- **セキュリティの対象領域の変化（IT利用に基づく業務の統合、生産性の向上）**
  - CRIC CSFにおいて討議が進む中で、これからのIT利用は、法人組織が細分化する過程において整理されてきた業務上のデータを統合し、さらなる業務改善や情報の統合等による「生産性の向上」を指向しており、これまでのIT利用の発展とは逆の流れで、膨大なデータが社内に集積され、業務に活かすようになってきていることを確認しています。
  - 更に、下図にある管理部門だけではなく、営業・製造・運用/運行等から提供される膨大なデータを収集し、マーケティングや様々な事業予測に役立てていくことが想定されています。



2-2-b ユーザ企業における組織分化プロセス（情報システム部門）

  - IT利用の方向性が、業務プロセスの効率化からデータ利用の効率化へ変化することによって、1つの部門・部署におけるIT利用上の侵害や棄損が発生した場合を想定し、事業全体への影響を考慮した、セキュリティ対策を重視しなければならない時期に入ってきているものと考えています。
  - 上記認識から「サイバーセキュリティは経営課題」という理解を更に進めて「ITによる効率化と合理化を進めている事業基盤の棄損や停止は重大な経営課題」という考え方に基づき、「セキュリティ統括室」の必要性を検討しています。

- **ユーザ企業における危機管理（リスクマネジメント）**
  - 多くの企業では、コーポレートガバナンスの観点から危機管理（リスクマネジメント）に関する取り組みについて、IRや広報を通じて日々ステークホルダーへ説明しています。
  - この取り組みの一環として「危機管理委員会」の設置や「危機管理マニュアル」の策定が実施されており、加えてPDCAサイクルを意識した訓練等が行われています。
  - しかしながら、一般企業においては、重要インフラ事業者においては想定されている「危機の定義」における「サイバー攻撃」が想定されていないことが少なくありません。
  - 今後、サプライチェーンリスクマネジメントの観点から、自社での取り組みだけではなく、事業上繋がりのある法人企業とセキュリティレベルを合わせていくことも、事業継続上の課題として認識されていくものと考えています。

- **「サイバー攻撃」をリスクとして捉えることの重要性**
  - 「サイバー攻撃は事業継続上の重大なリスク」であることは事実ですが、多くの企業では、組織的・人的・物理的なものを含む様々な事件・事故がリスクとして想定されており、IT利用においては「サイバー攻撃」よりも「システム障害」の方が経営リスクとしては大きなものとして捉えられています。
  - 今後、IT利用が「業務効率化に向けたIT導入」から「ITを前提とした事業推進」へ変化することにより「システム障害」だけではなく、様々ITに起因する不具合が及ぼす業務上のリスクマネジメントが重要になっていきます。

- **リスクと想定したものからリスク対応が実施される**
  - 危機管理（リスクマネジメント）体制において、マネジメントできるものとは「想定」されているものになります。想定されていないものは「想定外」として対応が遅れる場合があります。
  - これは全ての事業継続上のリスクに対して事前に準備を行わなければならないという強迫的なものではなく、リスクが経営上のクライシスに転換する可能性のあるものを特定し、ISO31000等を参考に、必要な対策が取れるよう検討を進めておくことが重要という考えによるものです。

- **危機管理委員会（リスクマネジメント委員会）**
  - 危機管理委員会を設置している企業では、その委員会運営を定めた社内文書が存在し、かつ、その文書の中には「リスクの定義」が記載されています。主に、地震、風水害、テロ等です。
  - 社内で定義されている「リスク」に「サイバー攻撃等」の記載が無ければ、リスクアセスメントの対象から外れる可能性があり、経営課題として「サイバーセキュリティ」を議論することが困難になることも考えられます。
  - また、「サイバー攻撃」をリスクとして想定した場合には、リスクマネジメント委員会が重大な懸念事項と決定するまでにはCSIRT活動でいう「トリアージ」が必要となり、国内外の政府・監督官庁、関係機関等への報告義務として定められた期限までに委員会が立ち上がらないことも想定されます。
  - 特に、被害が可視化されてにくいサイバー攻撃等のインシデントに対する危機管理（リスクマネジメント）体制については、事前準備と情報共有が重要です。

- **危機管理委員会（リスクマネジメント委員会）の活動のポイント**
  - 多くの企業では、危機管理委員会の運営規程の中で、危機管理委員会の立ち上げ（活動の起点）が「リスクマネジメント委員会 委員長の宣言」とされているケースが多く見られます。
  - サイバーセキュリティでは一般的となっている「（システム的な）検知」や「通報」によって発動する「サイバーインシデント対応体制」とその活動プロセスにおいては、初動段階では「被害の算定」が進まず、社内の危機管理（リスクマネジメント）体制と直ぐには連携できないケースもあります。
  - 今後、様々なリスクに機動的に対応できる「危機管理体制」とするためには、委員会の発足の基準を自動化し、収束を委員長判断と変更していくことが望ましいと考えられます。

  - 危機管理委員会の活動プロセス（例）

2-3-a 危機管理委員会の活動プロセス（例）

・リスクマネジメントの枠組みに「サイバーセキュリティ」を組み込むための考え方

1. 危機管理委員会の発足要件の定義
   - 重要インフラを担う組織の中には、危機管理体制及び対処活動における発動条件を明示しているところがあります（例えば、地震は震度5強以上、風水害は大雨洪水警報の発令等を指します）。
   - これは自動的に平時から非常時に切り替わり、自己の責任において初動対応を開始し、責任者が収束を宣言することで平時に戻るという体制を採用しています。
   - 上記体制を導入すると、訓練が日常業務に組み込まれることになりますので、日々の業務の中で、非常時にどのように対応するのかが議論され、また必要に応じてトレーニングを実施することが可能となります。

2. サイバーセキュリティの「検知」「通報」を委員会の発足要件にする
   - 先述した通り、サイバーセキュリティは「自衛」が基本です。地震や風水害のような被害の可能性を示すセンサーを自社で所有しているのかが最も重要となります。
   - 検知であればSOCやSIEM、通報であればCSIRTや通報窓口（と連絡体制）ということになります。
   - しかしながら、「サイバー攻撃」は検知や通報の段階では、システム障害と見分けがつきませんので、初動は「セキュリティ統括室」と「情報システム部門」が連携し、協働して対処する必要があります。
   - 更に、クリティカルなシステムを構築・運用保守している企業は、ユーザ企業・ベンダー企業が密に連携し、障害と攻撃の両面から対応する必要があり、その体制を事前に構築しておくことはとても重要です。

3. セキュリティ統括室とCSIRT
   - 本資料は「セキュリティ統括室」という組織体を前提に記述していますが、組織体とすることなく、CSIRTを導入し、サイバーセキュリティにおける対応活動を進めることも平行して検討頂きたいと考えています。
   - セキュリティインシデントへの対応については、CSIRT活動に関する関連文書において体系的に整理されていますので、サイバーセキュリティの会社全体の取り組みを検討する前に、インシデント対応体制を構築することも重要となります。

・リスクマネジメントの枠組みに「サイバーセキュリティ」を組み込むための考え方

3. 社内文書体系から検討する

- 危機管理（リスクマネジメント）関連の文書には様々なものがあります。
- 上位には「危機管理（リスクマネジメント）規程」と「危機管理（リスクマネジメント）委員会運営規程」があり、必要に応じて「危機管理（リスクマネジメント）マニュアル」が策定されていることが多くあります。
- 同時に、日本ではリスクマネジメントの観点から様々な法令があり、それら法令に対応するために、各種規程が制定されています。

	サイバーセキュリティ	情報セキュリティ	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** サイバーセキュリティ管理規程（仮称）		**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	サイバーインシデントに関する対処	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	CISO等	CIO又は情報システム部門責任者	人事管掌役員 又は人事部長	総務管掌役員 又は総務部長	総務管掌役員 又は総務部長	人事管掌役員 又は人事部長
所管部門	セキュリティ統括 又は情報システム部門	情報システム部門	個人情報取扱い部署又は指名された部署	文書取扱い部署又は、指名された部署	総務部門	人事部門 労働安全衛生委員会
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
法令例	不正アクセス禁止法 刑法	個人情報保護法 不正アクセス禁止法 不正競争防止法 刑法	個人情報保護法	不正競争防止法	消防法	労働安全衛生法

2-3-b 社内文書体系から検討したリスクマネジメントの枠組みへの「サイバーセキュリティ」の組込み

- サイバーセキュリティに関する対象範囲、対応部署、対応手順等を定めた社内文書は、内規的に順次整備されていくこともありますが、他のリスクマネジメントに関する規程等を参照し、正式な社内文書として制定することも重要です。
- 尚、サイバーセキュリティに関する規程類の所管部署としては「セキュリティ統括室」または情報システム部門に対してセキュリティ観点で支援・アセスメントができる部署・チームを想定しています。

- **情報セキュリティ**
  - 日本国内では、様々な情報セキュリティに関する取り組みが推進されています。
    - 情報セキュリティガバナンス（経済産業省）
      - http://www.meti.go.jp/policy/netsecurity/secgov-concept.html
    - サイバーセキュリティ経営ガイドライン（経済産業省）
      - http://www.meti.go.jp/policy/netsecurity/mng_guide.html
    - 情報セキュリティ管理基準（経済産業省）
      - http://www.meti.go.jp/press/2015/03/20160301001/20160301001.html
    - 組織幹部のための情報セキュリティ対策（総務省）
      - http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/index.html
    - 情報セキュリティ（情報処理推進機構 / IPA）
      - https://www.ipa.go.jp/security/

  - 多くの企業では上記取り組みに対応し、情報セキュリティに関する体制を整備し、情報セキュリティ関連の規程類を定めています。
  - その中には「社内でやりとりされる情報」と「その情報を電磁的に管理するシステム」を合わせて「情報資産」として定めています。また「社内でやりとりされる情報」については一般的に「文書管理規程」等の中で定義されており、業務に関する情報は全て管理することが定められています。

- **情報セキュリティポリシーの観点**
  - 情報セキュリティ体制を構築している企業は、情報セキュリティポリシーを公開し、その実現のためのセキュリティ環境の構築及び維持運用が行われています。
  - この点においては、サイバーセキュリティも内包されていると考えられ、新たな対策が必要かどうかは、事業領域における監督官庁の指針や業界別のガイドライン等に従って策定されるべきものと考えられます。
  - 更に、事業展開している国によっては、サイバーセキュリティに関する対策が明示されていることもあり、システム的な追加対策を検討する必要があります。

- **情報セキュリティ規程群**
  - 情報セキュリティに関するルールを定めている企業は多くありますが、システムインフラとしてのIT機器が適切に管理されていなければ、追加対策としてセキュリティ製品・サービスを追加導入しても、機動的なインシデント対応は困難は場合があります。
  - セキュリティ対策というフレーズでは「セキュリティ対策」を「追加導入する」ことに関心が向いてしまいますが、実際にはITガバナンスの観点から「構成管理の徹底」（入口・出口対策）がなされていることで、対応できるものも多くあります。
  - セキュリティ統括室は、事業継続上のリスクマネジメントの観点からのセキュリティ対策が主な業務となるため、システム環境を企画・設計段階からセキュアに管理できる状態とし可用性を高めていくための追加対策を行うという方向性が重要となります。

- **情報セキュリティとサイバーセキュリティ**
  - CRIC CSFは、産業横断サイバーセキュリティ人材育成検討会という名称の通り「サイバーセキュリティ」という考え方に基づいて、人材育成やその周辺領域に関する在り方について検討を進めています。
  - 本来「サイバーセキュリティ」は「情報セキュリティ」の一部として考えられるもので「情報セキュリティ」に関する取り組みが、構成管理、脆弱性対応、インシデント対応、脅威情報共有、攻撃分析・対策などリアルタイムに実施されている限りは、明確に分離する必要がないと考えられます。
  - 情報資産の棚卸を中心とした数か月から1年単位でのセキュリティ対策を実施している場合は、サイバーセキュリティの観点でのリアルタイムでのセキュリティ対策が必要になるという考え方に基づき「サイバーセキュリティ」という用語を使用しています。

- **リスクマネジメントの観点**
  - サイバーセキュリティ対策の必要性については、サイバー攻撃等の事例に基づくリスクベースでの検討も重要ではあるが、経営の観点からの整理を先に行う必要がある。

  - 法律で定められたリスクマネジメント
    - 会社法　　第362条4項６号
      - 取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備　＝　内部統制システム
    - 会社法施行規則　　第98条、第100条
      1. 取締役の職務の執行に係る情報の保存及び管理に関する体制
      2. 損失の危険の管理に関する規程その他の体制
      3. 取締役の職務の執行が効率的に行われることを確保するための体制
      4. 使用人の職務の執行が法令及び定款に適合することを確保するための体制
      5. 当該株式会社並びにその親会社及び子会社から成る企業集団における業務の適正を確保するための体制

- **内部統制の観点**
  - ユーザ企業の立場から考える時、そのビジネスの形態を問わず、内部統制体制の構築及び運用が求められていると考えられる。
  - 更に、サプライチェーンの観点から、内部統制体制の重要性は、自社が上場しているか否かだけにとらわれることなく、取引先の内部統制体制の維持と連携しているという認識が重要と考えられる。

  - 法律で定められた内部統制
    - 金融商品取引法　第24条の4の4（内部統制報告制度）
      - 内部統制報告書は「当該会社の属する企業集団及び当該会社に係る財務計算に関する書類その他の情報の適正性を確保するために必要なものとして内閣府令で定める体制について、内閣府令で定めるところにより評価した報告書」と定義されている。

2-5. 参照すべき法令、基準・標準、ガイドライン

- **日本国内**

1. 法令
    1. サイバーセキュリティ基本法
    2. 個人情報の保護に関する法律（個人情報保護法）
    3. 特定電子メールの送信の適正化等に関する法律
    4. 電子署名及び認証業務に関する法律
    5. 不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）
    6. 不正競争防止法
    7. 刑法
        - 情報処理の高度化等に対処するための刑法等の一部を改正する法律
        - 刑事訴訟法
    8. 著作権法
    9. 電気通信事業法
    10. 有線電気通信法
    11. 電波法
    12. 会社法
    - 参考）電子政府の総合窓口 e-Gov
        - http://www.e-gov.go.jp/
    - 参考）国民のための情報セキュリティサイト
        - http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/index.html

2. ガイドライン
    - 2017年発行
        - サイバーセキュリティ経営ガイドラインVer2.0
        - 情報セキュリティ早期警戒パートナーシップガイドライン- 2017年版
        - 組織における内部不正防止ガイドライン（日本語版） 第4版
        - フィッシング対策ガイドライン 2017年度版
        - 証拠保全ガイドライン第６版
        - 制御システムのセキュリティリスク分析ガイド
        - CCDSIoTセキュリティ評価検証ガイドライン Ver.1.0
    - 尚、最新版は、サイバーセキュリティ人材育成 研修データベースにおいて公開
        - https://cs-edu.jp/

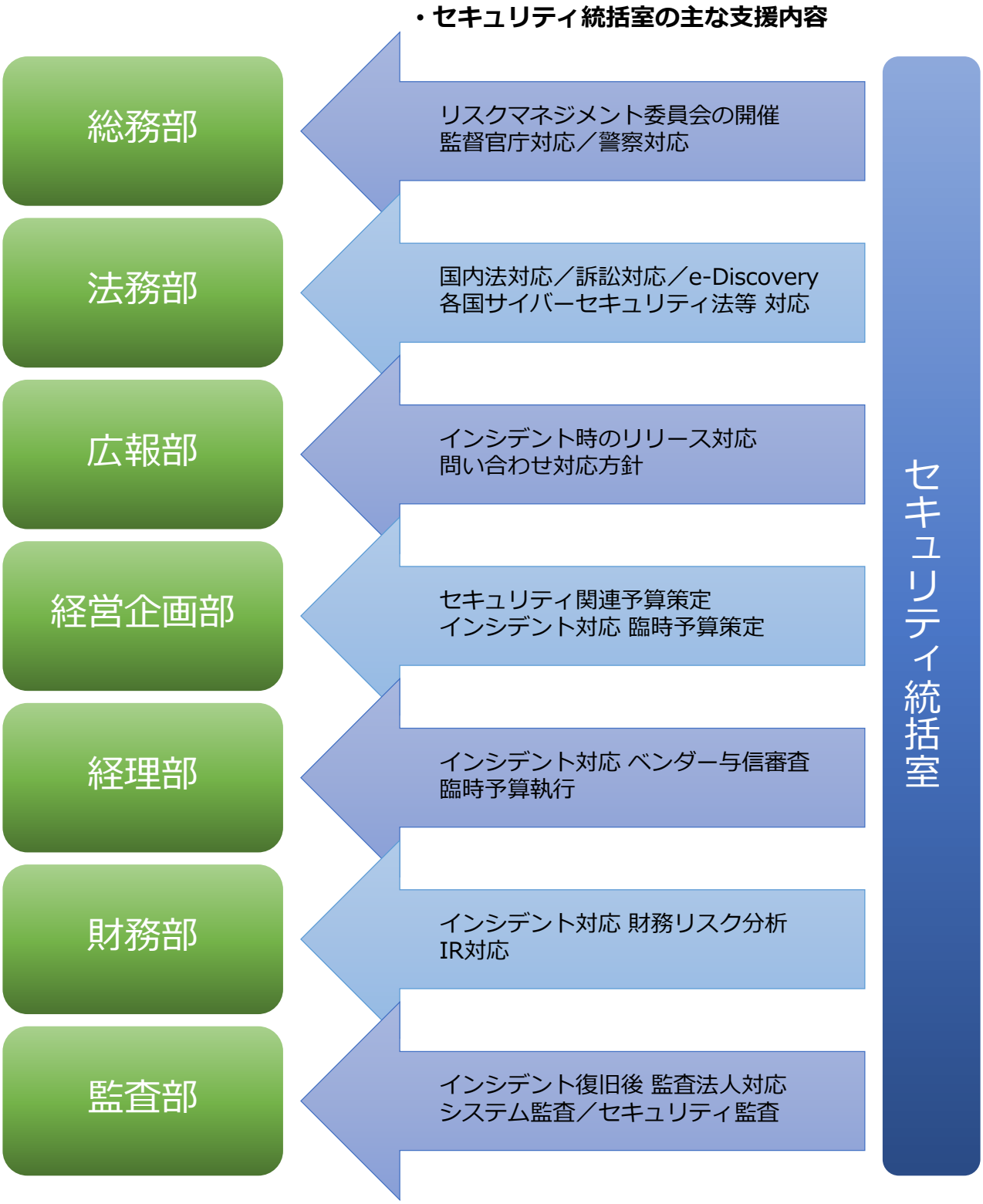
参考）セキュリティ統括室の役割（例）

- セキュリティ統括室の機能（例）
  - セキュリティ統括室は、ITの活用が拡大するユーザ企業のためのセキュリティ対策を網羅的に統括することを目指し、その役割と機能を定義しています。
  - 特に、日本のユーザ企業においては、システム構築や運用を外部委託する傾向が強いことから、適切な「分業体制」を管理することに主眼を置いています。
  - 更に、事業展開する国々の法令やガイドラインへの対応、内部統制やリスクマネジメントの観点から、事業継続上重要となるサイバーセキュリティのあり方を検討・検証する機能を重視しています。

2-6-a セキュリティ統括室の機能（例）

参考）セキュリティ統括室の役割（例）

- 管理部門として位置付けた場合のセキュリティ統括室の役割の例



2-6-b セキュリティ統括室の主な役割（例）