資料２－４

サイバーセキュリティ人材育成に向けた産業界としての取り組み
～企業でのセキュリティ人材育成に関する議論について～

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

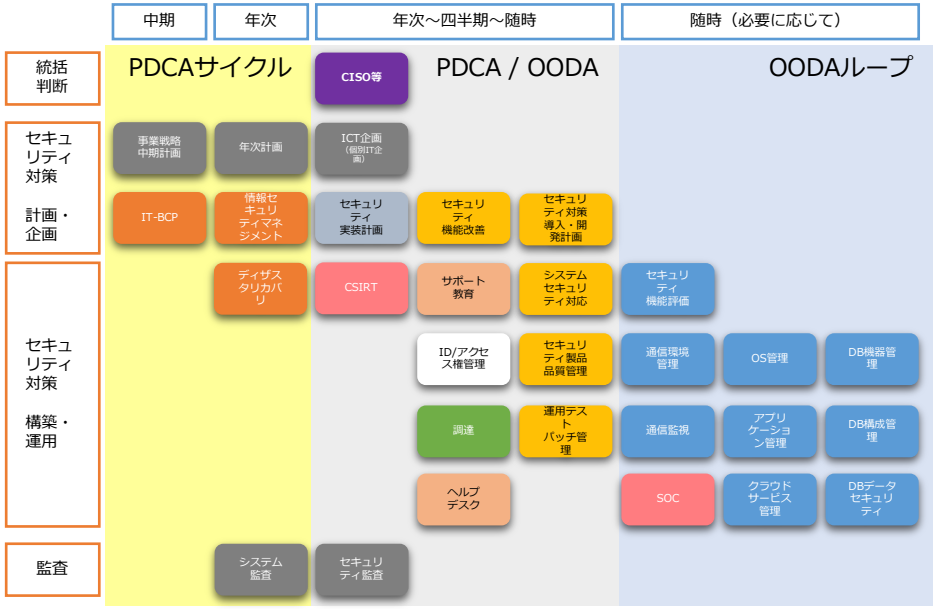
2017年9月14日(木)

はじめに

- 概要
  - 第一期（2015年6月～2016年9月）での検討結果を受けて、第二期（2016年10月～現在）の活動における検証作業及び討議内容についての説明
  - セキュリティ人材のキャリアパスを３つにモデル化し、特に、ユーザ企業のセキュリティ人材の中核として「エキスパート人材（セキュリティ統括人材）」に関する検討プロセスを説明
- 検討の前提：ユーザ企業の分類に関する考え方
  - ユーザ企業の類型として、大きく2つに分類
    - ビジネス自体がインターネット上にある企業、または、ITを駆使してビジネスを行う企業
      - 業界：E-コマース、金融、各種クラウドサービス事業者等
      - 情報を主に取り扱い、情報漏洩や改ざんなど、CIAの順でセキュリティを検討
      - サイバーセキュリティがビジネスに直結していることに自覚的であり、サイバーセキュリティに関して経営層の理解も高い
    - ものづくり的な部分がビジネスの根幹である企業（各種製造メーカ企業等）
      - 業界：電力、ガス、水道、石油、化学、自動車、飛行機、鉄道、その他製造メーカ等（多くの重要インフラ関連企業が含まれる）
      - 情報だけでなく、物理的なプラントや人などの安全も含めた（セーフティ）セキュリティであり、AICの順で優先される場合が多い
      - サイバーセキュリティの重要性を認識しつつも、その優先度は必ずしも高くない

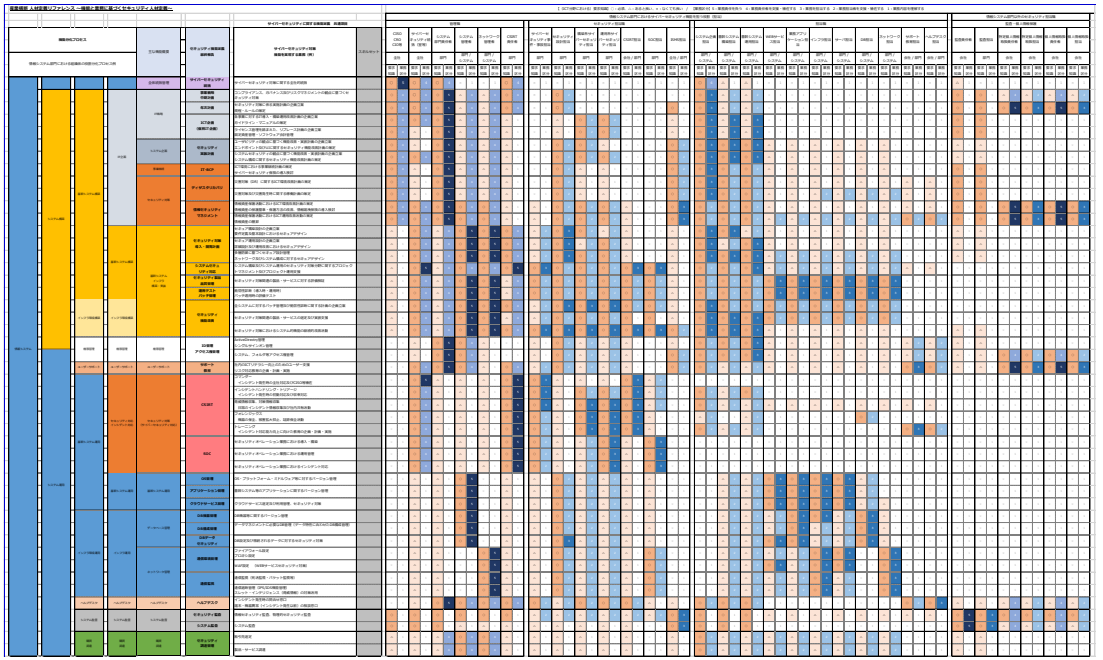
CRIC CSFにおける企業でのセキュリティ人材育成の考え方（１）

- 第一期報告書
  - 企業におけるセキュリティ機能とそれに関わる30の役割
    - 企業の典型的なセキュリティ態勢を切り取ったもの（リファレンスモデル）
    - キャリアパスは考慮されていない （キャリアパスとは、30の役割の担当する人を育成するプロセス）



サイバーセキュリティ対策の機能定義（関係図）

人材定義リファレンス
セキュリティ機能を担う30の役割



第二期 議論に向けた背景 ～日本のユーザ企業にとって最も重要な人材は？～

なぜ「エキスパート人材」を検討してきたのか

1. セキュリティ対策は「エキスパート人材」が決定し、CISOが承認している。

- **「何を、どこまで、どのよう」に実施するかを決める人材**は、検討会メンバーでは**「セキュリティ部署・セキュリティチーム」に所属**している。尚、CISOの役割は、説明責任と予算執行。

2. セキュリティ対策は、セキュリティ製品・サービス導入だけでは不十分。

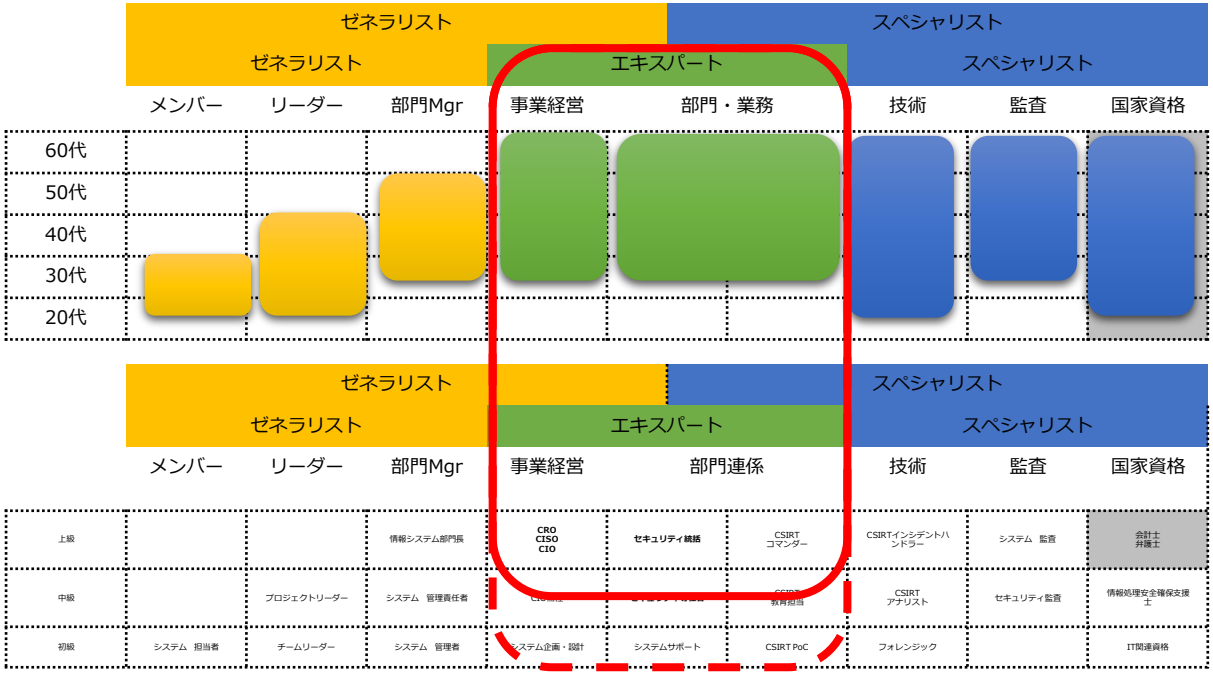
- **サイバーセキュリティが経営課題**として重視されてきている。
- **セキュリティを自社ビジネスのコンテキストで考えられる人材**が重要になってきている。
  - 企業におけるIT活用が、オフィス環境だけではなく、生産現場等にも浸透してきた。
  - クラウドサービス（IaaS,PaaS,SaaS）利用において、選定する段階から自社システム環境を想定した既存システムとの連携や利用法を踏まえたセキュリティ対策の検討・検証が必要になっている。

3. 日本国内におけるIT従事者の75%はベンダーに所属。

- **システム企画と、構築・運用の分離が、セキュリティ対策を不十分なものにしている**可能性がある。
  - ユーザ企業のIT部門は、事業運営に必要となるITシステムを守る立場にあり、システム企画を担当するが、構築及び運用の実務は情シス子会社やベンダーへ委託している。
  - 更に、委託先がセキュリティ人材を確保していない場合、セキュリティ対策の不十分なシステムが提供され運用される恐れがある。

CRIC CSFにおける企業でのセキュリティ人材育成の考え方（２）

- 第二期の議論（人材育成WG)
  - 企業におけるセキュリティ人材の3つのキャリアパス
    - **ゼネラリスト**　：企業における（ライン）マネジメントのキャリアパスとして存在
    - **エキスパート**　：自社事業とセキュリティ活動をよく知り、現場と経営をつなぐ人材（セキュリティ統括人材）、情報処理安全確保支援士 に通じるキャリアパス
    - **スペシャリスト**：専門的技術を持った人材であり、IT/セキュリティベンダー、情報子会社のキャリアパスとして存在



ユーザ企業におけるセキュリティ人材として育成することが必要な人材

エキスパート人材

第二期 議論の仮説 ～人材定義リファレンスからエキスパート人材を検討する～

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	セキュリティ担当職 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	
			部門		部門		部門		部門		会社 / 部門		部門		全社 / 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	要求知識	業務区分
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		×	1	×	1	×	1	×	1	×	1	×	1	×	1
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		×	1	○	2	×	1	×	1	×	1	×		×	1
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		×	1	○	2	×	1	×	1	×	1	×	1	○	1
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		×	1	△	1	○	2	○	2	×	1	×	1	△	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		×	1	△	1	○	2	○	2	×	1	×	1	△	1
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		×	1	○	2	○	2	△	1	×	1	×	1	○	2
	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		×	1	○	2	○	2	○	2	×	1	×	1	○	2
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		×	1	○	2	△	1	△	1	×	1	×	1	○	2
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		×	1	○	2	△	1	△	1	×	1	×	1	○	2
	災害対策及び災害発生時に関する稼働計画の策定		×	1	○	2	△	1	△	1	×	1	×	1	○	2
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		△	1	○	2	○	2	○	2	△	1	×	1	○	3
	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		△	1	○	2	○	2	○	2	△	1	×	1	○	3
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		△	2	○	3	○	2	△	2	△	1	×	1	△	1
	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		△	2	○	3	△	2	○	2	△	1	×	1	△	1
	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		△	2	○	3	○	2	○	2	△	1	×	1	△	1
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		○	3	○	2	○	2	○	2	○	3	○	3	△	1
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		○	2	○	2	○	2	○	2	○	2	○	2	△	1
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		○	2	○	2	○	2	○	2	○	2	○	2	△	1
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		△	2	○	3	○	3	○	3	○	2	○	2	△	1
	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		△	2	○	2	○	2	○	2	○	1	○	1	△	1
	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		○	3	○	3	○	3	○	3	○	3	○	3	○	2

エキスパート人材の定義に適合する「役割」は、人材定義リファレンスにおける**「セキュリティ設計担当」**となる（仮定）。

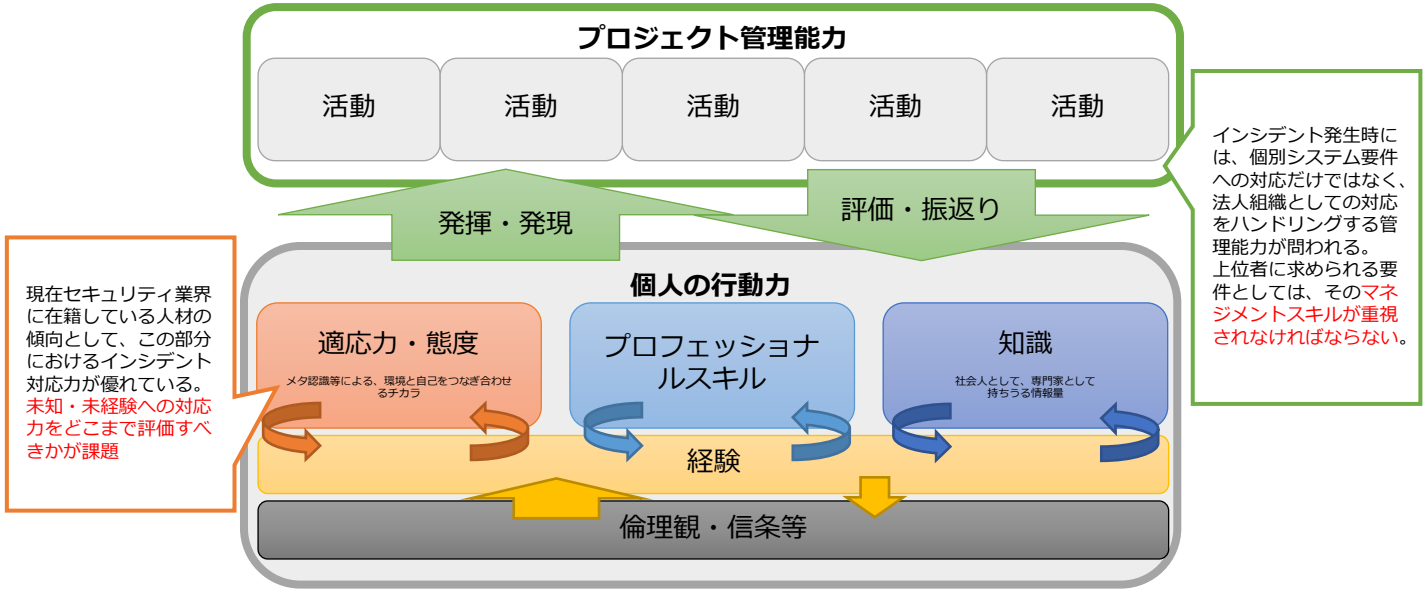
要求知識に加えて、業務区分においても、想定されるエキスパート人材に近似的な分類を行っているため、本役割をエキスパート人材のモデルとして定め、育成の方向性を探っていきたい。

検討のポイント

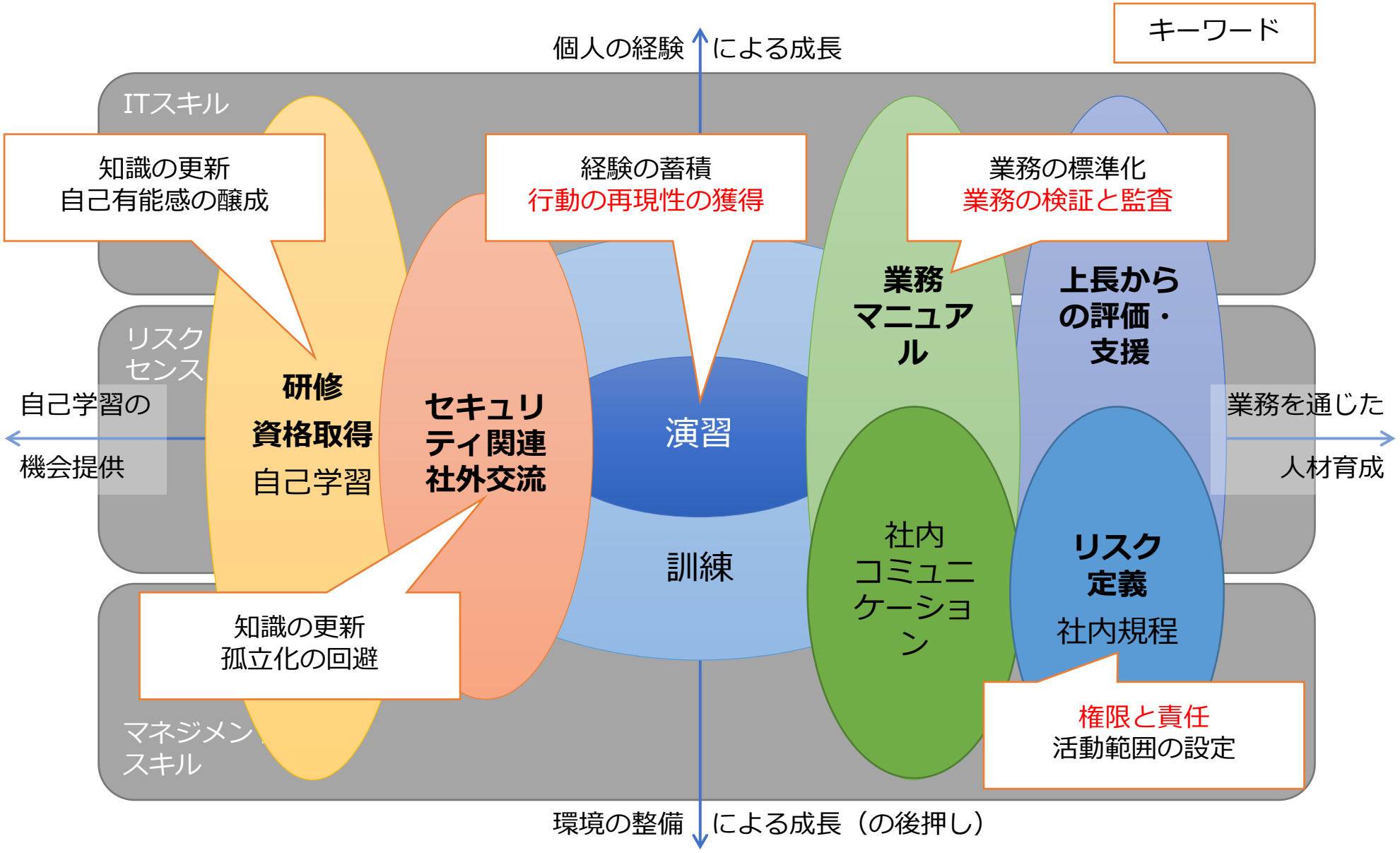
- **何を理解しているべきか**
- **どこまで理解するべきか**
- **能力の発揮を何で測るか**

CRIC CSFにおける企業でのセキュリティ人材育成の考え方（３）

- エキスパート人材の持つべき能力／育成すべき能力を「氷山モデル」で考える
  1. 個人の行動力
     1. 適応力・態度 ⇒ リスクセンスやコミュニケーション → 環境によって醸成されるもの
     2. プロフェッショナルスキル ⇒ 人材定義リファレンス：機能（業務区分）
     3. 知識 ⇒ 人材定義リファレンス：機能（要求知識） → 自主的に学習可能なもの
     4. 経験 ⇒ キャリアパスやこれまでの業務経験（人生経験）
     5. 倫理観・信条等 ⇒ 仕事に対するスタンス → 環境によって醸成されるもの
  2. プロジェクト管理能力
     1. 活動 ⇒ 人材定義リファレンス：機能に対する「実際の業務」
     2. プロジェクト管理 ⇒ 業務の優先順位付けや、達成基準の設定と評価 → 学習と環境の両面から育成されるもの

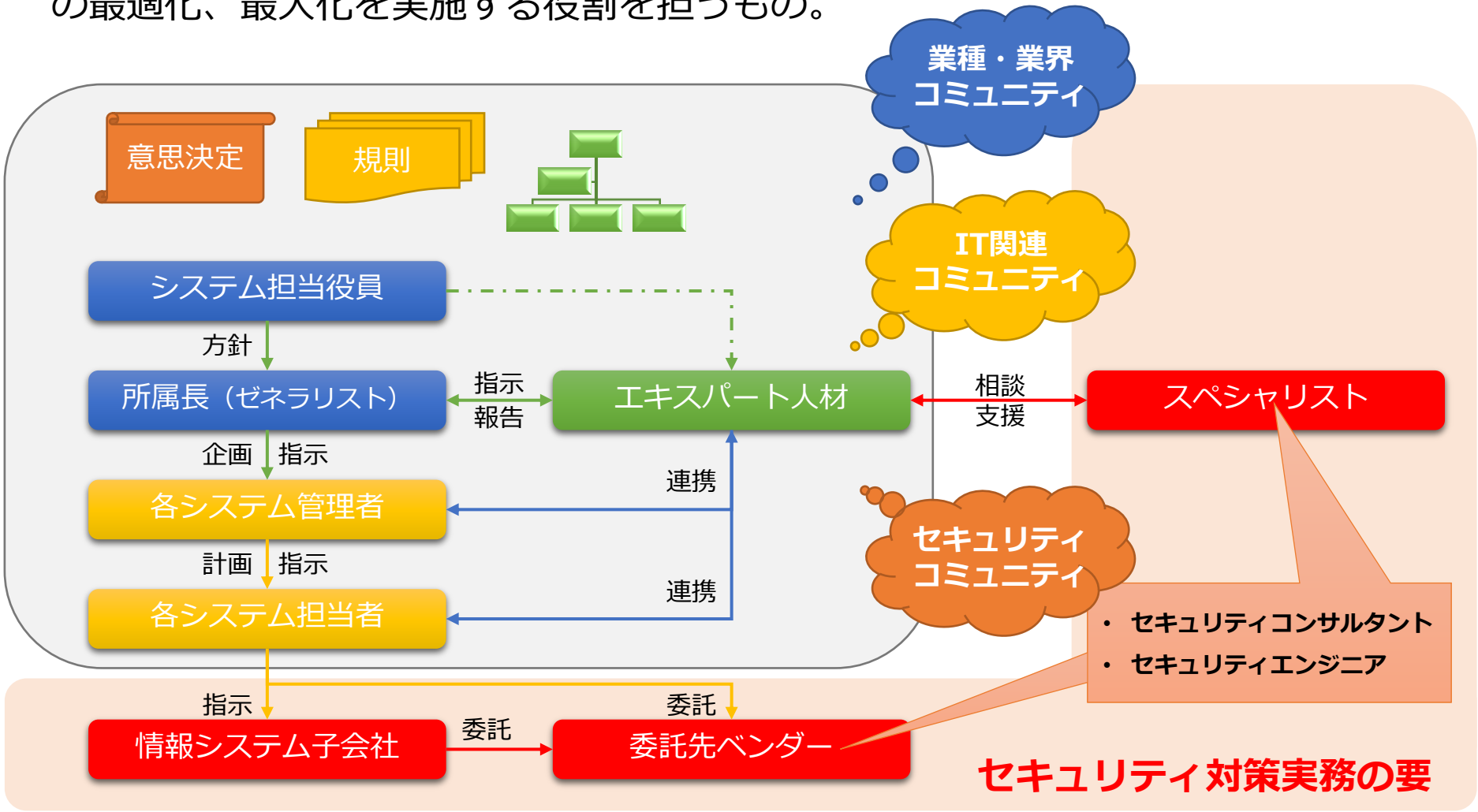


エキスパート人材育成のポイント：横軸＝育成方針、縦軸＝成長要因・手段



エキスパート人材を配置するための環境構築

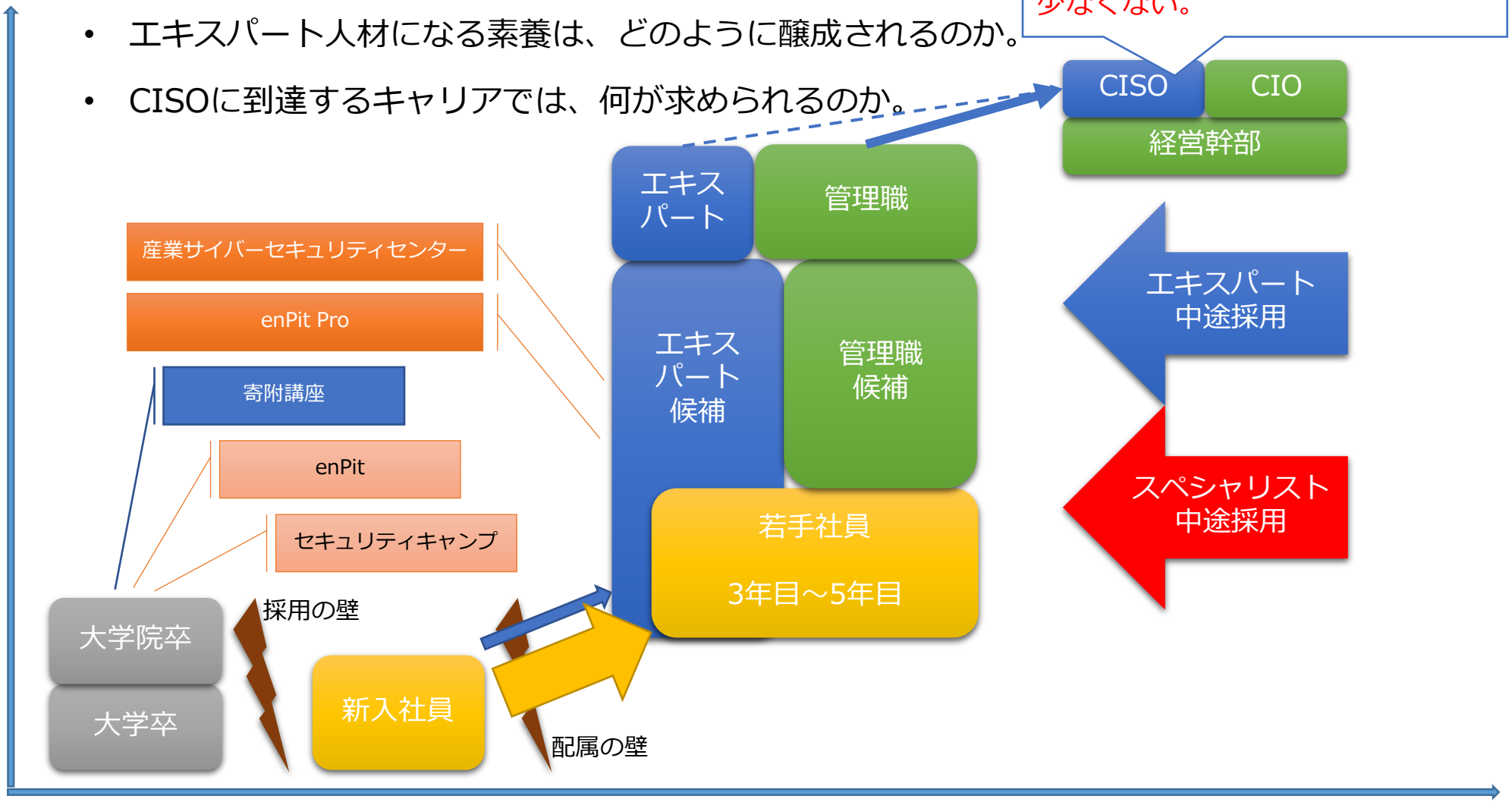
- エキスパート人材は、様々な環境に対応しながら、所属する企業のセキュリティ対策の最適化、最大化を実施する役割を担うもの。



学生からCISOへのキャリアパスイメージ

- エキスパート人材育成を「社外」に広げて俯瞰する
  - エキスパート人材になる素養は、どのように醸成されるのか。
  - CISOに到達するキャリアでは、何が求められるのか。

CISOは業務の専門職が担当する場合もあるが、日本企業では年功序列による定期人事異動により、セキュリティ未経験でも担当となる場合が少なくない。



エキスパート人材に求める全体観と専門性のバランスをどう取るべきか。

- サイバーセキュリティ分野におけるエキスパート人材に求められる要件を考える
  - 社内でセキュリティ業務に従事するために求められる能力とは？

1.	情報収集	：事例収集、セキュリティ対策標準・基準、構成管理と対策手法
2.	情報分析	：事例分析、対策手法の有効性、対応ベンダー候補選定
3.	**セキュリティ分野の知見**	**：自社に適合するセキュリティ対策プランの想定**
4.	**現状把握**	**：リスクアセスメント（対策状況の把握）**
5.	**現状分析**	**：リスクアセスメント（リスク分析）**
6.	**対策立案**	**：多層防御に基づく優先順位付け、予算化**
7.	**対策実施**	**：製品・サービス選定、ベンダー選定・発注**
8.	対策管理	：進捗管理、品質管理
9.	対策確認	：運用管理、改善
10.	監査	：年次評価～月次評価

内製すべきポイント

内製のポイントは
1. ベンダーに騙されない
2. 自社システムに適合できる
3. 過剰なコストをかけない
4. 検証可能な対策を選択する
5. 監査に基づき報告できる

エキスパート人材が習得すべきノウハウ（経験を積むための知識・前提）

1. リスクマネジメント / リスクアセスメント（追加）

- リスクマネジメントの基本的な考え方と、自社事業領域におけるリスクアセスメント
- ISO 31000、ERM等

2. セキュリティマネジメントフレームワーク

- **例）ISO/IEC27001・27002:2013**
- 自社のセキュリティ対策が、世の中の動きと連動し、かつ十分な対応を行なっていることを説明できる取り組み。（ISOのため関連法令への対応を含む）

3. インシデントハンドリング

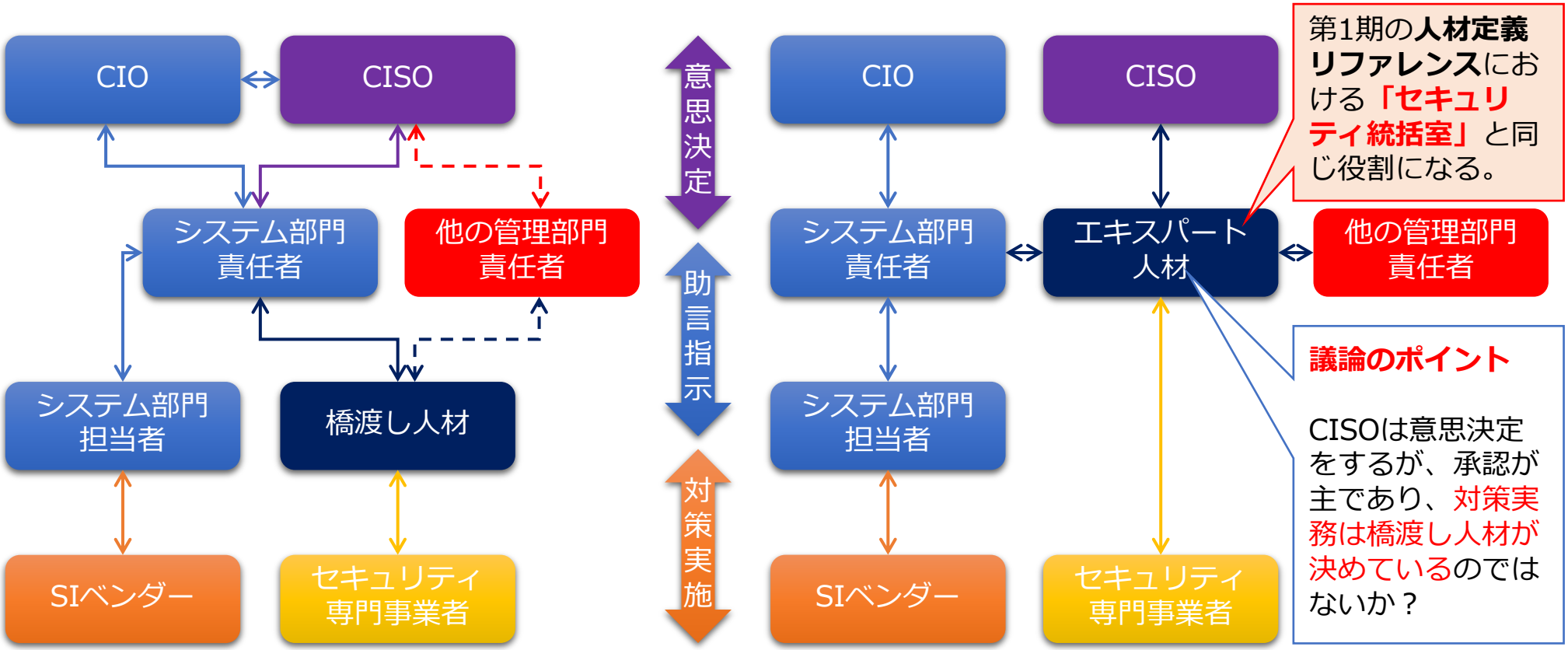
- **例）CSIRT活動**
- インシデント発生前後において着実に対応できるプロセスを明確にし、インシデントマネジメントに基づく対策を選択できる取り組み。（CSIRTにはSOCやフォレンジック等を含む）

4. セキュアバイデザイン

- システムの要件定義の段階から、セキュリティ要件（非機能要件）を明確にし、ベンダーによる対策漏れを指摘できる取り組み。（**セキュリティ設計**には構築だけではなく、運用設計を含む）

CISOとエキスパート人材の役割分担（「セキュリティ統括人材」の根拠）

- これまでの検討会での議論を通じ、説明責任と意思決定について整理する。
  - 普及している意思決定プロセス
  - 議論に基づく意思決定プロセス（検討会案）



- **橋渡し人材が、橋渡しだけではなく、意思決定に関わる**ことを明示していくことも必要。

用語の定義に向けて

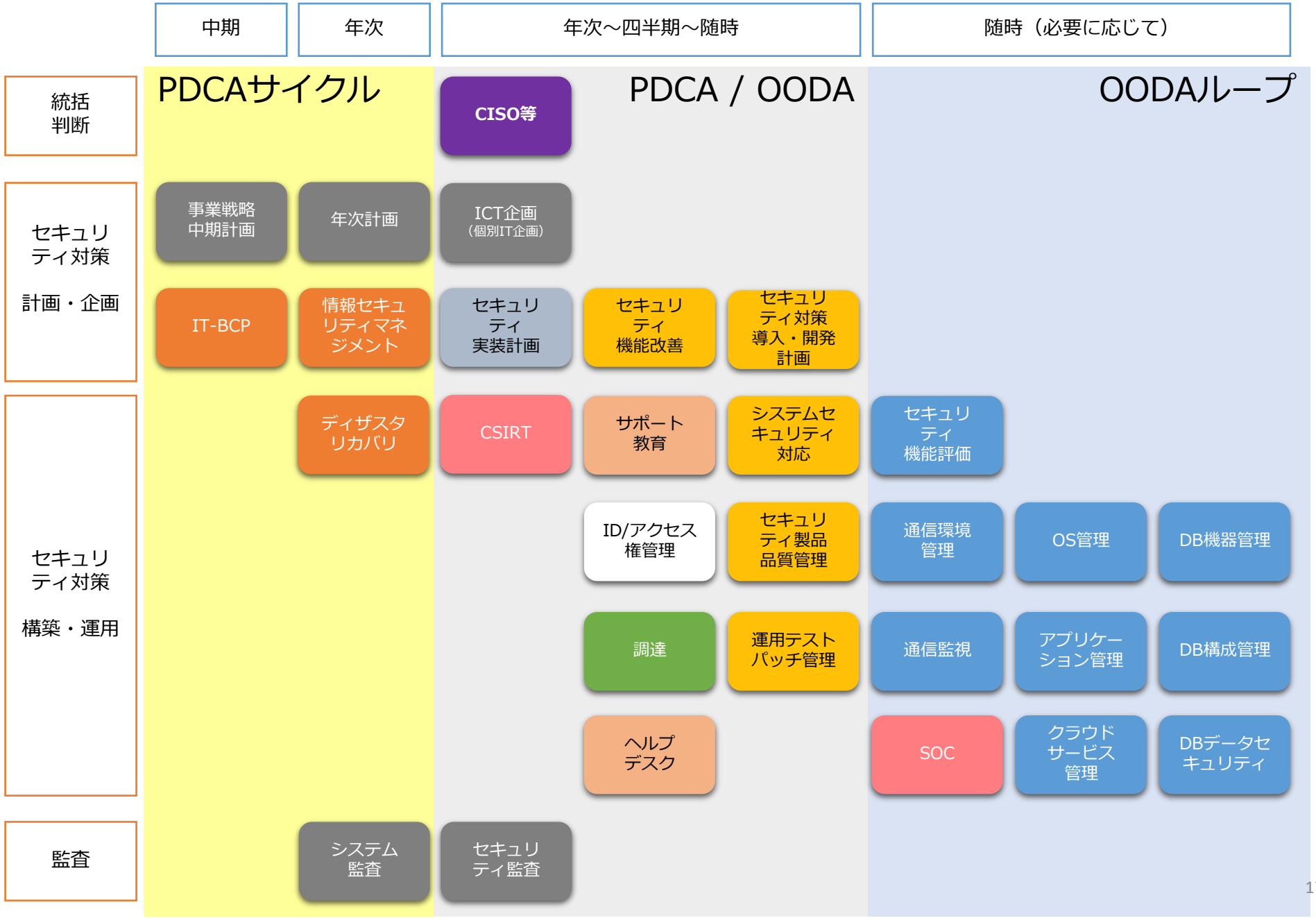
- 「セキュリティ統括人材」を複数の呼び名で認識している。
  - **橋渡し人材**
    - NISC発表資料により「経営陣と技術者を繋ぐ立場」を担う人材として普及している。
    - 検討会での議論を通じて、橋渡し人材のポジションを担う人材は、意思決定に強く関与していることに着目し、今後、検討会として活用する「呼称」について検討を進めている。
  - **エキスパート人材**
    - 経営陣を支えるセキュリティ人材像を定めるため、人材側から定義を進めてきた際に登場した呼称。ゼネラリストとスペシャリストに対比させるために活用中。
    - 日本特有な年功序列型人事制度に基づくゼネラリスト、資格や専門分野に基づくスペシャリストに対応し、ユーザ企業の中で人材を確保し育成するために仮置きしている。
  - **セキュリティ統括人材**
    - 各WGにおける議論の中で、中核となるセキュリティ人材の役割は**「セキュリティ対策を決定し、CISOの承認を受ける（「対策決定」と「承認」を合わせて「意思決定」とする）」**人材であり、現在検討会に参加されている方々がその対象ではないかとの議論に基づき、エキスパート人材の後継として、用語の活用を検討中。

まとめ

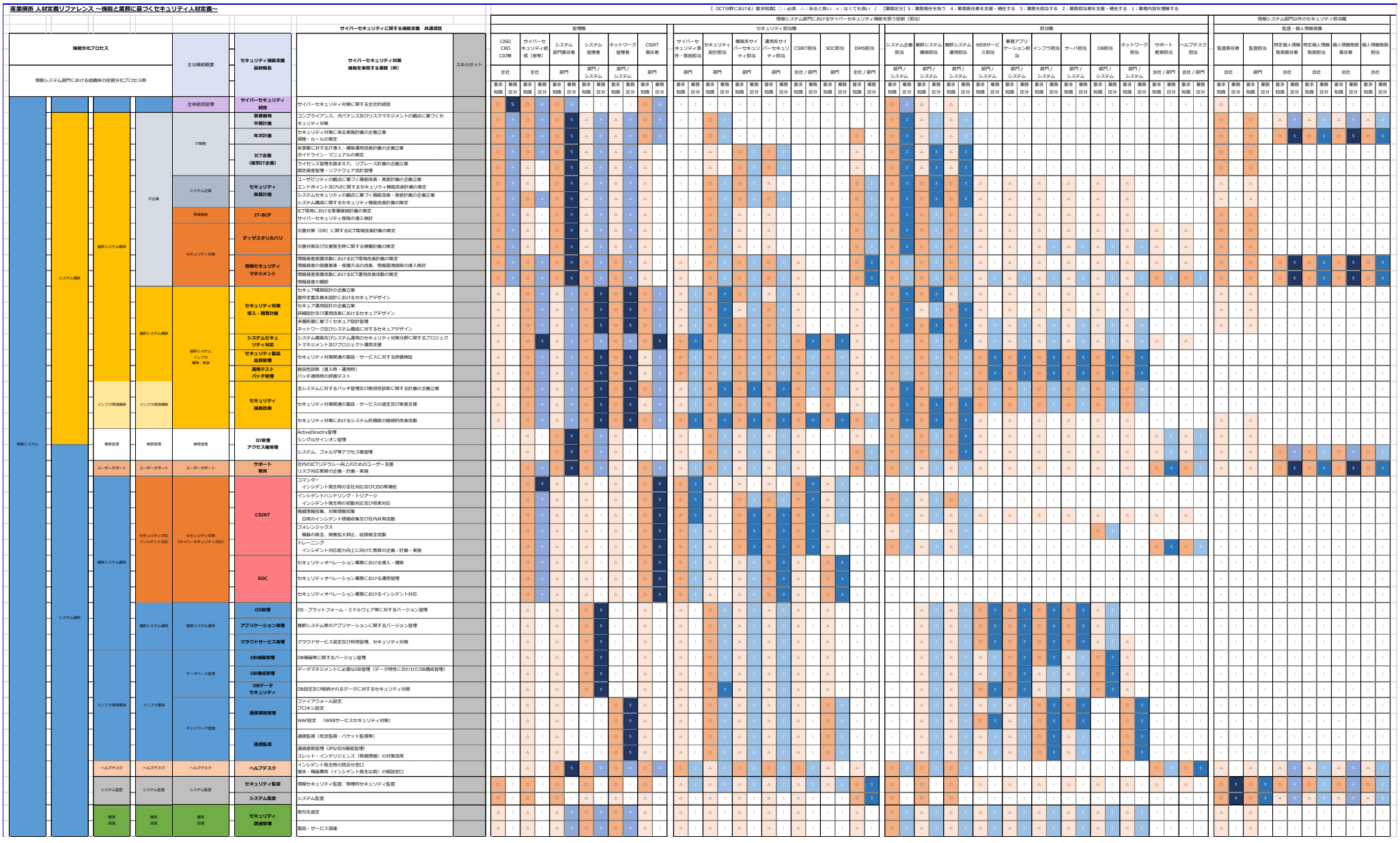
- これまでの検討
  - 第一期報告書では、一般企業におけるセキュリティ機能とそれに関わる30の役割をまとめた
    - リファレンスモデルであり、キャリアパスは考慮されていない
  - 第二期では、企業におけるセキュリティ人材を3つのキャリアパスで検討
    - ゼネラリスト 、エキスパート、スペシャリスト
  - ユーザ企業でのセキュリティ人材として育成することが必要な エキスパート人材育成を検討中
- 今後の検討
  - 引き続き、エキスパート人材育成を検討し、具体的な育成活動を進めるための環境整備を行う。
  - 人材定義WG（OT人材定義）、産学連携人材教育WGなどの検討結果と合わせて、産業界として考えるセキュリティ人材育成を第二期報告書としてまとめる。（11月末目途）
  - スペシャリスト人材については、IT/セキュリティベンダーと連携し、リファレンス的な考え方を提供できないか検討中（12月目途）

参考資料

サイバーセキュリティ対策の機能定義（関係図）



第1期成果物 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 ～

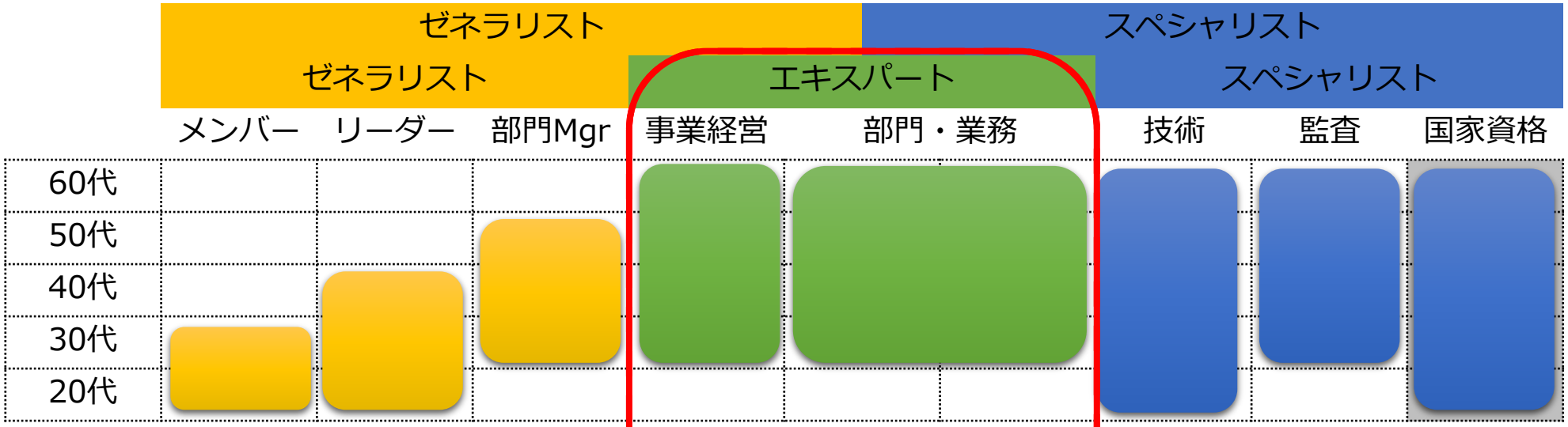


サイバーセキュリティ対策の機能定義（関係図）とエキスパートの例１

サイバーセキュリティ対策の機能定義（関係図）とエキスパートの例２

人材定義リファレンスに対する「エキスパート」の定義について

- 人材定義のマトリックス（セキュリティ人材の観点）



	ゼネラリスト			エキスパート			スペシャリスト		
	メンバー	リーダー	部門Mgr	事業経営	部門連係		技術	監査	国家資格
上級			情報システム部門長	**CRO CISO CIO**	**セキュリティ統括**	CSIRT コマンダー	CSIRTインシデントハンドラー	システム監査	会計士 弁護士
中級		プロジェクトリーダー	システム管理責任者	CIO補佐	**セキュリティ専任者**	CSIRT 教育担当	CSIRT アナリスト	セキュリティ監査	情報処理安全確保支援士
初級	システム担当者	チームリーダー	システム管理者	システム企画・設計	システムサポート	CSIRT PoC	フォレンジック		IT関連資格

内製のポイント（エキスパート人材育成の重要ポイントをどこに置くか）

1. ベンダーに騙されない
   - セキュリティ対策の有効性を何で判断するか
2. 自社システムに適合させる
   - NW構成、システム構成、アプリケーション、エンドポイントの最適化をどう進めるか
3. 過剰なコストをかけない
   - 対策にかかるコストについて、適正価格はどのように判断するか
4. 検証可能な対策を取る
   - 対策の実施状況を何で測るか
5. 監査に基づき報告できる
   - 社内で共有可能なレベルをいかに定めるか

知識やスキルだけではなく
正解が見えない中での対応力＝
「リスクセンス」も重要になる

自社の人材で対応すべき範囲を明確にし、どのレベルで意思決定するかを定めておくことが、セキュリティ対策の有効性を高める重要な基準となる。

会社事業やセキュリティ意識により、人材を採用するか、育成するか、信頼できるベンダーを選定し委託するかが分かれてくる。

エキスパート人材が習得すべきノウハウ（経験を積むための知識・前提）

- 前項の１～４を身に付けた後は、いくつかの方向に分かれていくものと考えられる。
  - **全体を構成するノウハウ**
    - SP800シリーズ（NIST／全般）
    - サイバーセキュリティフレームワーク
    - サイバーセキュリティワークフォース（NIST／SP800-181）
  - **（経営）ガバナンス系（説明責任への対応）**
    - ISO 31000やERM
    - サイバーセキュリティ経営ガイドライン（経済産業省）
  - **ITガバナンス系（事業継続性への対応）**
    - ISO/IEC27001：2013
    - サイバーセキュリティ経営ガイドライン 解説書（IPA）
    - IPA発行ガイドライン各種（セキュリティ設計/標的型攻撃対策）
    - SP800シリーズ（NIST／管理手順、手引き）
  - **システムセキュリティ系（セキュリティ実装）**
    - IPA発行ガイドライン各種（NWセグメント/機器構成の管理等）
    - SP800シリーズ（NIST／チェックリスト、考慮事項、基準等）
    - 各種システムや機器のセキュリティ対策（メーカー発行、脆弱性情報等）

- 橋渡す先を、経営陣とIT技術者とする。
- 経営層にはリスクマネジメントで説明。
- 情報システム部門にはITガバナンスで企画立案
- SIには個別システムセキュリティ対策で対策の指示・確認。

エキスパート人材が習得すべきノウハウ（案）- 既存文書からの考察

- 社内文書とセキュリティ対策（例）

セキュリティポリシー	**サイバーセキュリティ基本法（第六条、第七条） サイバーセキュリティ経営ガイドライン（ver1.1） サイバーセキュリティフレームワーク（2017年5月11日、大統領令に署名） ISO/IEC27001:2013**
文書管理規程	内部統制
個人情報保護方針	**個人情報保護法（改正個人情報保護法）、特定個人情報保護法**
個人情報保護規程	
機密情報保護方針	**不正競争防止法、刑法、刑事訴訟法**
機密文書管理規程	
情報セキュリティガイドライン	**不正アクセス禁止法、ISO/IEC27002**
情報システム管理規程	ISO/IEC27002
システム管理規則・細則	ISO/IEC27002
システム開発マニュアル	開発者向けセキュリティ関連コンテンツ（経済産業省）参照
システム運用規則・細則	ISO/IEC27002
システムユーザマニュアル	
クラウド利用マニュアル	
インシデント対応マニュアル	CSIRT構築・運用関連コンテンツ参照

- システム開発・運用におけるセキュリティ対策がどこまで文書化されているかにより、対策の有効性に影響が出る。