サイバーセキュリティ人材フレームワーク活用の手引き2026

―― 小規模組織向け ――

国家サイバー統括室
National Cybersecurity Office

令和8年4月3日

本書の位置づけ・利用上の留意点等について

位置づけ

- 本書は、「サイバーセキュリティ人材フレームワーク」の策定背景・目的、整理概念に加え、小規模組織における活用シーン・方法などを解説した「サイバーセキュリティ人材フレームワーク」の手引き書です。
- サイバーセキュリティ人材フレームワークの理解及び活用を支援することを目的に作成したものであり、各組織における人材育成、配置等を一律に義務づけるものではありません（各組織においては、本手引き書の内容を参考としつつ、自らの規模・特性に応じて適切に活用してください）。

想定利用者

- 本手引き書は、官民においてサイバーセキュリティ対策等に関わる者を主な利用者として想定します。
- 特に、専任のサイバーセキュリティ担当者を十分に確保することが困難な官民の小規模組織において活用されることを想定しています。

その他利用上の留意点

効力について

- 本手引き書は、法令、契約又は行政処分等の法的根拠となるものではなく、法的拘束力を有するものではありません。
- 本手引き書の内容と法令又は契約等の間に相違がある場合には、法令又は契約等が優先されます。

用語及び定義について

- 本手引き書にて記載する用語の定義は、基本的にサイバーセキュリティ人材フレームワークにおける定義に基づくものです。

情報の正確性及び更新について

- 本手引き書の内容は、作成時点における情報及び知見に基づくものであり、技術動向等により内容が変更される場合があります。
- 最新の情報については、関係機関が公表する資料等を参照してください。

出典の明示について

- 本手引き書を利用する際は下記の例に倣い、出典を記載してください。

記載例）
出典：国家サイバー統括室「サイバーセキュリティ人材フレームワーク活用の手引き2026（小規模組織向け）」（〇年〇月〇日に利用）

- 本手引き書を編集・加工等して利用する場合は、編集・加工等を行ったことを記載してください。
  なお、編集・加工した資料を、あたかも国（国家サイバー統括室）が作成したかのような態様で公表・利用してはいけません。

準拠法と合意管轄について

- 本手引き書の解釈等については、日本法を準拠法とします。
- 本手引き書に関連して生じた紛争については、東京地方裁判所を第一審の専属的合意管轄裁判所とします。

免責について

- 国（国家サイバー統括室）は、利用者が本手引き書を用いて行う一切の行為（編集・加工等した情報を利用することを含む。）について何ら責任を負うものではありません。

その他

- 本利用ルールは、著作権法上認められている引用などの利用について、制限するものではありません。
- 本利用ルールは今後変更される可能性があります。

目　次

共通事項

小規模組織向け事項

共　通　事　項

1．はじめに（サイバーセキュリティ人材フレームワークとは）

概要

サイバーセキュリティを担う人材について、職種別の役割と、それぞれに求められるタスク・知識・スキルを体系的に整理するとともに、能力等に応じたレベルを設定し、官民共通のフレームワークとして設定するものです。

策定背景

現　状

- 職種ごとの役割やスキルセットが**不十分**
  求められる知識・スキル等が曖昧
- 実務ニーズとサイバーセキュリティ人材の
  要件との対応関係が不明確

人材の育成・確保を効果的・効率的に進めるための
共通基盤が不十分**な状態**

一括りに「サイバー人材」と語られる傾向

策定後目指す効果

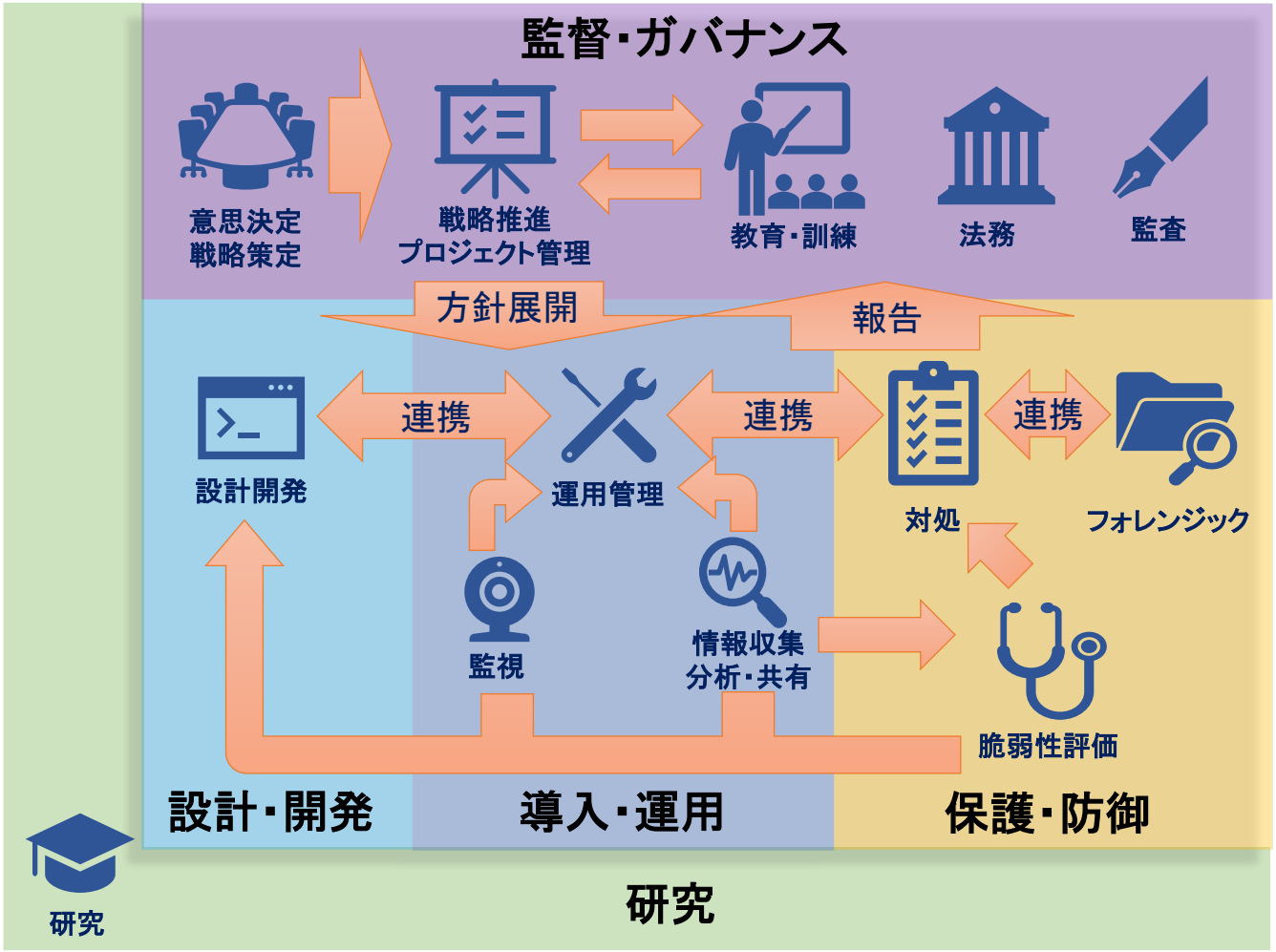
企業等　組織に必要な人材像を明確化し、採用・配置・育成等を計画的に進められる

個人　役割に応じて求められる知識・スキル等が可視化され、学習やキャリア形成の指針となる

教育機関等　ニーズに即したサイバーセキュリティ人材の要件を踏まえ、教育内容やカリキュラムを体系的に企画・設定できる

可視化により、効果的・効率的な人材育成を実現する環境を整備

サイバーセキュリティ人材が担うべき「役割」の全体像（イメージ）



通報・報告・連絡・相談

外部公的機関等

- 警察
- 個人情報保護委員会
- サイバーセキュリティ関連組織（NCO・IPA・JPCERT/CC等）

2．サイバーセキュリティ人材フレームワークの概要

- サイバーセキュリティ人材フレームワーク（Excel）は下表の各要素から構成されます。
- 各役割及び個別のタスク・知識・スキルとNICEフレームワークとの対応関係も明示しています。

各役割の定義シート（①～⑬）	● 13の役割を具体的に説明するため、以下の要素で構成 ➢ 主な業務（例）：その役割で実施する業務内容を示す。タスクの内容をまとめたものに相当 ➢ NICEフレームワークにおける対応ロール ➢ 想定される役職名等：組織において当該役割を担っている人材の主な役職名 ➢ 補足説明：国内の既存のフレームワークとの対応関係等を示す ➢ レベル：ITSSを参照した4段階のレベルを定義 ➢ 各役割で求められる汎用的なTKS:当該役割を担う人材が行うタスク(T)、及びそのタスクを実施するために必要な知識(K)及びスキル(S)

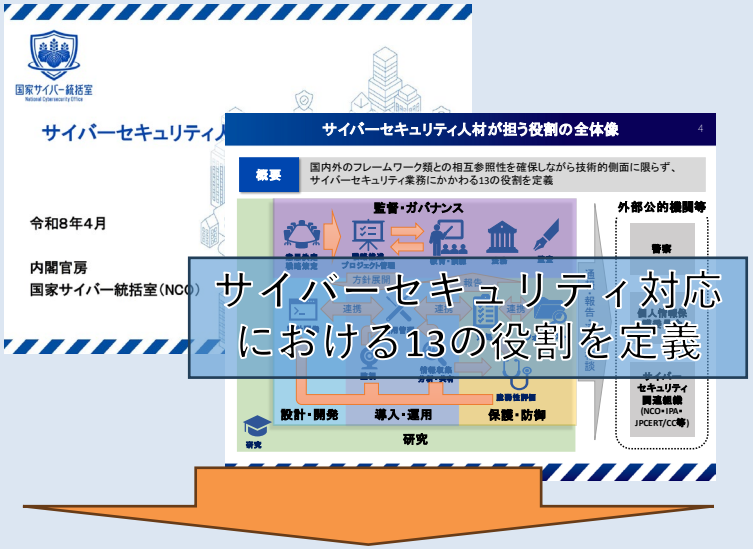
■TKSの考え方

タスク(T)	● 本フレームワークで役割毎に定義しているタスク(T)とNICEフレームワークv2.1.0におけるタスクとの対応表を示す。 ● 原則として、本フレームワークで定義している1つのタスクについてNICEフレームワークのタスクが1つ以上対応するが、一部本フレームワーク独自のタスクが存在する。
知識(K)	● 本フレームワークで役割毎に定義している知識(K)とNICEフレームワークv2.1.0における知識との対応表を示す。 ● 原則として、本フレームワークで定義している1つの知識についてNICEフレームワークの知識が1つ以上対応するが、一部本フレームワーク独自の知識が存在する。
スキル(S)	● 本フレームワークで役割毎に定義しているスキル(S)とNICEフレームワークv2.1.0におけるスキルとの対応表を示す。 ● 原則として、本フレームワークで定義している1つのスキルについてNICEフレームワークのスキルが1つ以上対応するが、一部本フレームワーク独自のスキルが存在する。

3．手引き書とは（人材フレームワークとの対応関係等）

本書では、各組織において求められる「役割」を、各組織の規模・特性を踏まえ、タスク・知識・スキルをベースに「人材像」として具体化して説明します。

■人材フレームワーク



■手引き書(本書)

①：小規模組織

②：大規模組織

13の役割をもとに、組織の個別事情に応じた「人材像」として具体化（例を用いて説明）

③教育機関

人材育成に資する教育コンテンツ等の設計方針などを整理

④-1：個人(専門人材)

④-2：個人(プラス・セキュリティ)

専門人材/プラス・セキュリティ別のスキル向上に役立つ情報を整理

【参考】各手引き書の想定読者一覧

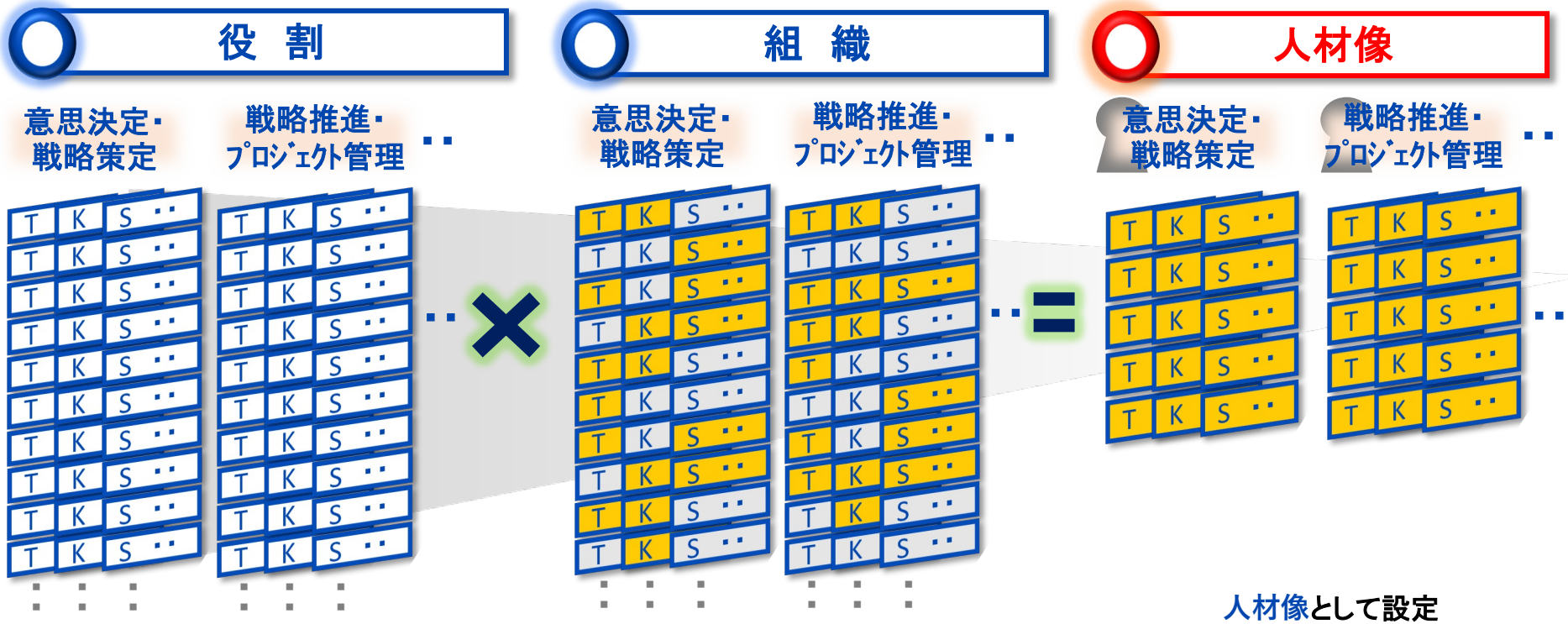
- 手引き書は各対象ごとに「主たる読者の属性」を想定し作成をしているものですが、主たる読者ではない属性の方も参考にしていただけるよう作成しておりますので、以下の対応表を参考にご利用ください。

凡例
◎：主たる想定読者
○：自身の業務等に密接にかかわる情報を含むもの
△：業務等において参考となる情報を含むもの

読者の所属・属性 / 手引き書	小規模組織		大規模組織		セキュリティ事業者	教育機関	
	マネジメント層	担当者	マネジメント層	担当者	―	教員	学生
小規模組織向け	◎	○	△	△	△	△	△
大規模組織向け	―	―	◎ (人事担当者含む)	○	△	△	△
教育機関向け	△	―	△	―	―	◎ (教育事業者含む)	○
個人 (専門人材)	△	△	△	◎ (セキュリティ担当者)	○	―	○ (セキュリティ分野志望者)
個人 (プラス・セキュリティ)	△	◎	△	◎ (バックオフィス、品質管理者等)	○	―	○ (学部の専門性によらず全学生に有益)

【参考】サイバーセキュリティにおける人材像の概念整理

- フレームワーク本体では、13の「役割」と各役割毎に汎用的なTKSを定義します。
- その上で、各組織において求められる役割を実施する人材の定義をフレームワークをもとに具体化したものを「（各役割の各組織における）人材像」とし、その具体化手順について手引き書にて提示します。



各役割毎にTKSを網羅的かつ汎用的に定義

組織特性に応じて、タスク（T）を絞り込み
（イメージ）橙：自組織で対応／灰：外部委託

手引き書では、モデルケースをもとに、人材像の設定方法を提示

フレームワーク本体

手　引　き　書

4．他の人材フレームワークとの参照関係

本フレームワークと国内の他のフレームワークとの関係は以下の通りです。
必要に応じて他のフレームワークも併せてご参照いただけます。

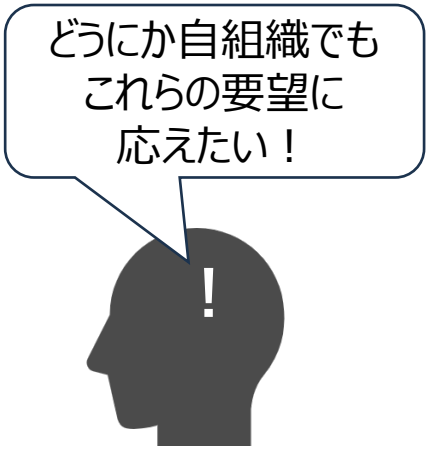
	本フレームワーク	ITSS+（セキュリティ領域）	SecBoK 2025	産業横断サイバーセキュリティ研究会 人材定義リファレンス	CSIJサイバーセキュリティ プロフェッショナル人材ロール
①	意思決定・戦略策定	セキュリティ経営（CISO） デジタル経営（CIO/CDO） 企業経営（取締役） 事業ドメイン（戦略・企画・調達）	セキュリティ経営、意思決定・戦略策定 セキュリティ統括	CISO、CRO、CIO等 システム部門責任者	
②	戦略推進・プロジェクト管理	セキュリティ統括 デジタルシステムストラテジー 経営リスクマネジメント 事業ドメイン（生産現場・事業所管理）	セキュリティ統括 プロジェクト管理 社内外調整	サイバーセキュリティ統括 ISMS担当 個人情報取扱責任者/担当 特定個人情報取扱責任者/担当	
③	監視	セキュリティ監視・運用	監視・運用	SOC担当	
④	対処	セキュリティ監視・運用	対処（インシデントハンドリング）	CSIRT責任者/担当 サイバーセキュリティ事件・事故担当	インシデントハンドラー
⑤	情報収集・分析・共有	セキュリティ調査分析・研究開発	脅威・脆弱性情報収集	SOC担当	
⑥	脆弱性評価	脆弱性診断・ペネトレーションテスト	脆弱性診断・評価	運用系サイバーセキュリティ担当	Web/NW脆弱性診断士 情報システムペンテスター IoTデバイス脆弱性診断士 IoTシステムペンテスター IoT脆弱性分析士
⑦	フォレンジック	セキュリティ調査分析・研究開発	インシデント調査・分析	サイバーセキュリティ事件・事故担当	
⑧	運用管理	セキュリティ監視・運用 デジタルプロダクト運用	システム管理・ネットワーク管理 監視・運用	システム管理者、ネットワーク管理者 運用系サイバーセキュリティ担当、他	クラウドセキュリティプロフェッショナル
⑨	教育・訓練	セキュリティ統括	教育・訓練	サポート教育担当	
⑩	法務	法務	法務		
⑪	監査	セキュリティ監査、システム監査	監査	監査責任者、監査担当	
⑫	設計開発	デジタルシステムアーキテクチャ デジタルプロダクト開発	セキュリティ設計 開発	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、他	サービス企画におけるリスク分析士 クラウドセキュリティプロフェッショナル
⑬	研究	セキュリティ調査分析・研究開発			

小規模組織向け事項

1．背景：最近の情勢を踏まえたサイバーセキュリティ対策のあるべき姿

- 昨今のサイバー攻撃の高度化・巧妙化からサプライチェーンリスク含め、事業者の組織規模にかかわらず、様々なサイバーセキュリティ対策の実施が求められるようになっています。
- IPA「中小企業の情報セキュリティ対策ガイドライン」では、企業が自らやるべきこと（「重要7項目」及び「組織としての対策」）を記載しています。
- なお本書では、必要なセキュリティ対策を、組織の規模・特性を踏まえ画一的・機械的に求めるものではありません。

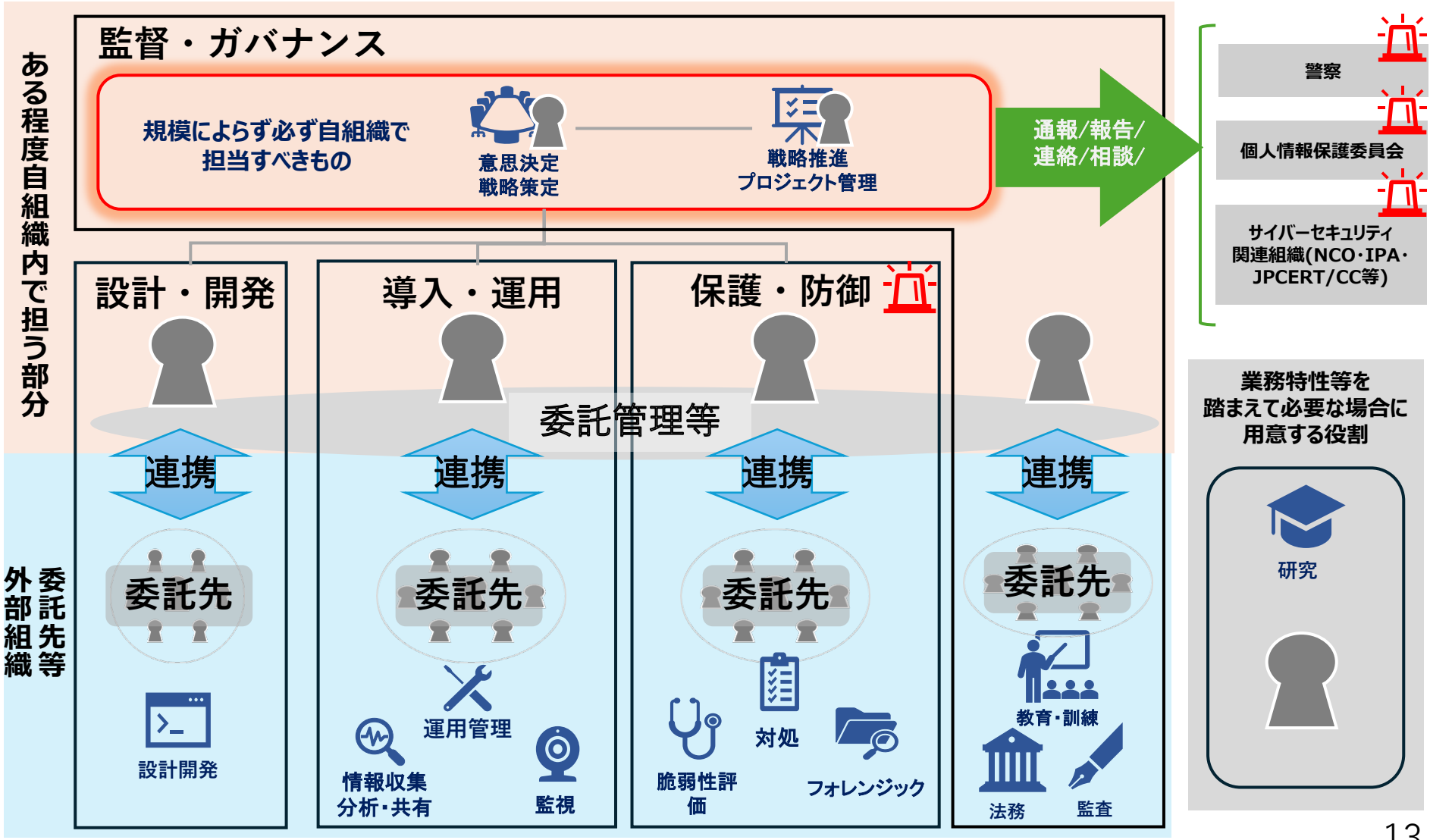
企業が自らやるべきこと	
重要7項目	情報セキュリティに関する組織全体の対応方針を定める
	情報セキュリティ対策のための予算や人材などを確保する
	必要と考えられる対策を検討させて実行を指示する
	情報セキュリティ対策に関する適宜の見直しを指示する
	緊急時の対応や復旧のための体制を整備する
	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
	情報セキュリティに関する最新動向を収集する
組織としての対策	不正アクセス対策機能の設定や、情報公開に関するルールを定めるなどのセキュリティ関連ルールを適切に策定、遵守させる
	従業員向けのセキュリティ教育や注意喚起を実施する
	個人所有機器の業務利用時の対策を明確化する
	重要情報を扱う契約にて秘密保持条項を規定する
	安全・信頼性を考慮してクラウドサービスや外部サービスを選定する
	事故発生に備え緊急体制を整備し対応手順を作成する
	情報セキュリティ対策をルール化し、従業員に明示する
	：



出典：独立行政法人情報処理推進機構（IPA）：『中小企業の情報セキュリティ対策ガイドライン 第4.0版』（表紙、P16～17、P23より引用）を基に作成
https://www.ipa.go.jp/security/guide/sme/about.html

2．小規模組織におけるセキュリティ対策の基本的な考え方

人材フレームワークにて定義された13の役割について、すべての人材を自組織で確保・育成することは現実的ではありません。
そのため自組織で最低限責任をもって実施すべき役割と、外部の委託先等と連携し果たす役割を組み合わせながらセキュリティ対策にあたる必要があります。



「やるべきこと」と「役割」の関係

	「やるべきこと」	「役割」	
重要7項目	情報セキュリティに関する組織全体の対応方針を定める	意思決定・戦略策定	
	情報セキュリティ対策のための予算や人材などを確保する	意思決定・戦略策定	
	必要と考えられる対策を検討させて実行を指示する	監視	脆弱性評価
	情報セキュリティ対策に関する適宜の見直しを指示する	戦略推進・プロジェクト管理	監査
	緊急時の対応や復旧のための体制を整備する	対処	フォレンジック
	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする	戦略推進・プロジェクト管理	
	情報セキュリティに関する最新動向を収集する	情報収集・分析・共有	
組織としての対策	不正アクセス対策機能の設定や、情報公開に関するルールを定めるなどのセキュリティ関連ルールを適切に策定、遵守させる	戦略推進・プロジェクト管理	
	従業員向けのセキュリティ教育や注意喚起を実施する	教育・訓練	
	個人所有機器の業務利用時の対策を明確化する	戦略推進・プロジェクト管理	
	重要情報を扱う契約にて秘密保持条項を規定する	法務	
	安全・信頼性を考慮してクラウドサービスや外部サービスを選定する	運用管理	
	事故発生に備え緊急体制を整備し対応手順を作成する	対処	フォレンジック
	情報セキュリティ対策をルール化し、従業員に明示する	戦略推進・プロジェクト管理	

IPAガイドライン　　本フレームワーク

- IPAのガイドラインが定義する「やるべきこと」について、13種類の役割の中から対応するものを割り当てると左のようになります。
（設計開発と研究は業務特性を選択せず）
- この中には高度な専門性を要するものも含まれているので、各役割を次の3つに分けてそれぞれの対応を検討する必要があります。

ア：原則として自組織で担うもの

イ：自社での対応と外部委託を併用するもの

ウ：原則として外部委託で対応するもの

3. モデルケースに基づく活用例

組織規模や業種の異なる3つのケースを用いて活用例を解説します。

	【ケース１】	【ケース２】	【ケース３】
サイバーセキュリティ対策における悩み	 サイバーセキュリティ対策はこれまで外部業者に任せており、「自組織でやるべきこと」をあまり意識できていなかった。	 取引先から経済産業省の「サプライチェーン強化に向けたセキュリティ対策評価制度」への対応を要求されているが、対応できる人材の育成が必要。	 サイバーセキュリティ対策は代表者が実質一人ですべて対応しているが、やるべきこと（タスク）が何かを把握したい。
想定する企業属性	● 従業員8名 ● 小売業（ネット販売） ● PCは使いこなせるが、セキュリティはよくわからないという従業員が大半。	● 従業員20名 ● 製造業（部品製造） ● 「工場の設備なら慣れているが、PCは苦手」という従業員が多い。 ● 工場はネットに接続していない。	● 従業員2名（代表＋アシスタント） ● サービス業（デザイナー）

ケース１
A社（インターネット小売業）の場合

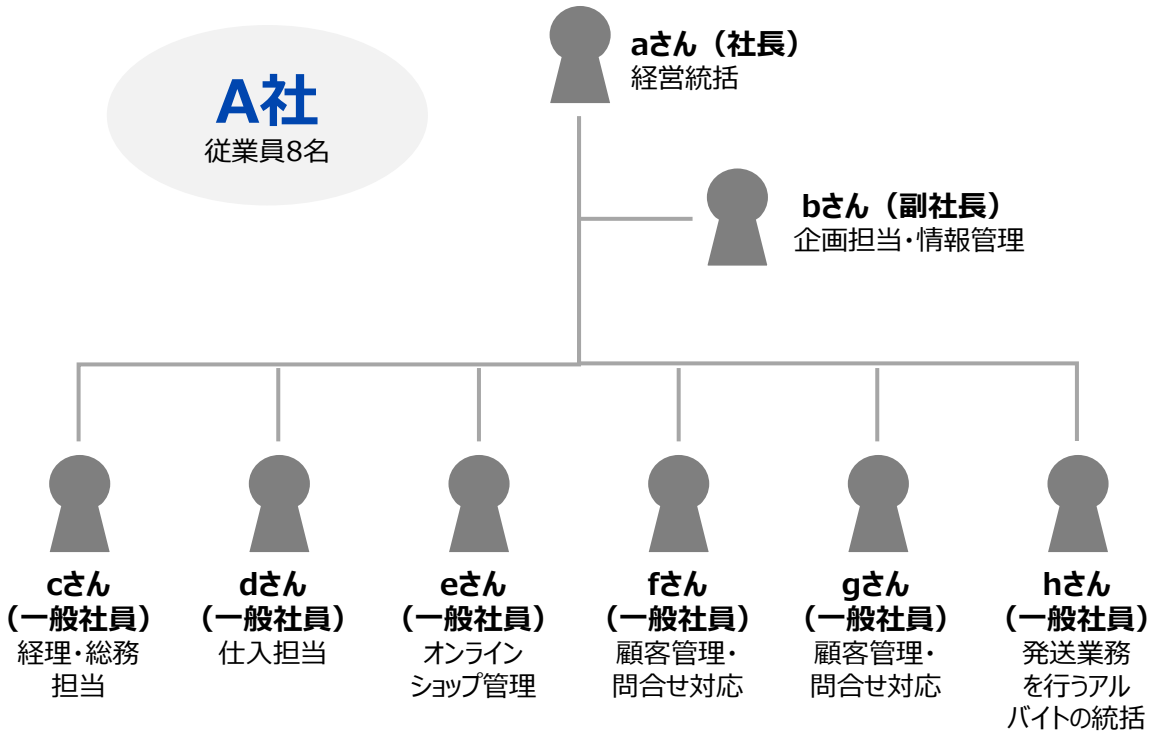
	【ケース１】	【ケース２】	【ケース３】
サイバーセキュリティ対策における悩み	 サイバーセキュリティ対策はこれまで外部業者に任せており、「自組織でやるべきこと」をあまり意識できていなかった。	 取引先から経済産業省の「セキュリティ対策評価制度」への対応を要求されているが、どうすればよいかわからない。	 サイバーセキュリティ対策は代表者が実質一人ですべて対応しているが、やるべきこと（タスク）が何かを把握したい。
想定する企業属性	● 従業員8名 ● 小売業（ネット販売） ● PCは使いこなせるが、セキュリティはよくわからないという従業員が大半。	● 従業員20名 ● 製造業（部品製造） ● 「工場の設備なら慣れているが、PCは苦手」という従業員が多い。 ● 工場はネットに接続していない。	● 従業員2名（代表＋アシスタント） ● サービス業（デザイナー）

ケース 1

A社（インターネット小売業）の場合

モデル組織のA社はこんな会社です

- 地場産品を直売するオンラインショップを運営しています。最近はふるさと納税の返礼品としての発送もあり全員が何かと忙しく働いています。
- オンライン販売はECモール事業者が用意する環境を使っており、セキュリティ対策もECモールに委ねています。それ以外に自社の経営情報をクラウドで管理していますが、対策が十分とはいえません。
- BtoC形態であるため、一般消費者との取引・やりとりも発生する。



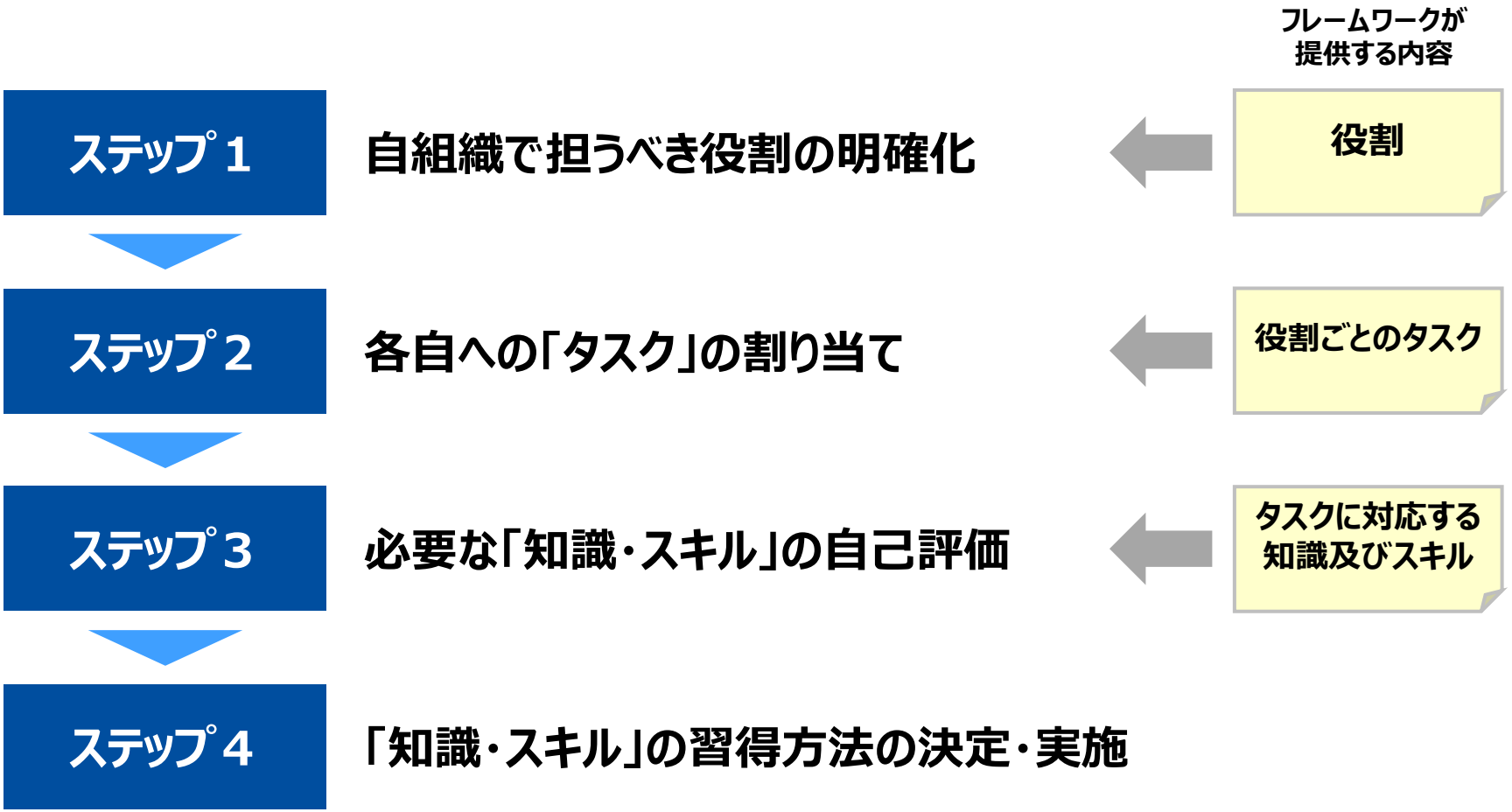
従業員の特徴

aさん	IPAの中小企業セキュリティガイドラインを読んで勉強中。
bさん	情報管理の役割上、ランサムウェアの被害を防ぐ方法は知っている。
cさん	セキュリティ関連の法律は把握しているがデジタルスキルは表計算程度。
dさん	AIに企業秘密を入力してはいけないことを理解している程度。
eさん	クラウドのセキュリティ対策は必要に迫られて覚えたが、やや自己流。
fさん gさん	不審なメールを無視すべきことは理解しているが、最近のフィッシングメールは巧妙なので不安。
hさん	自分よりもセキュリティに詳しいアルバイトがいるので焦っている。

ケース 1

フレームワークを用いたA社での対策のステップ

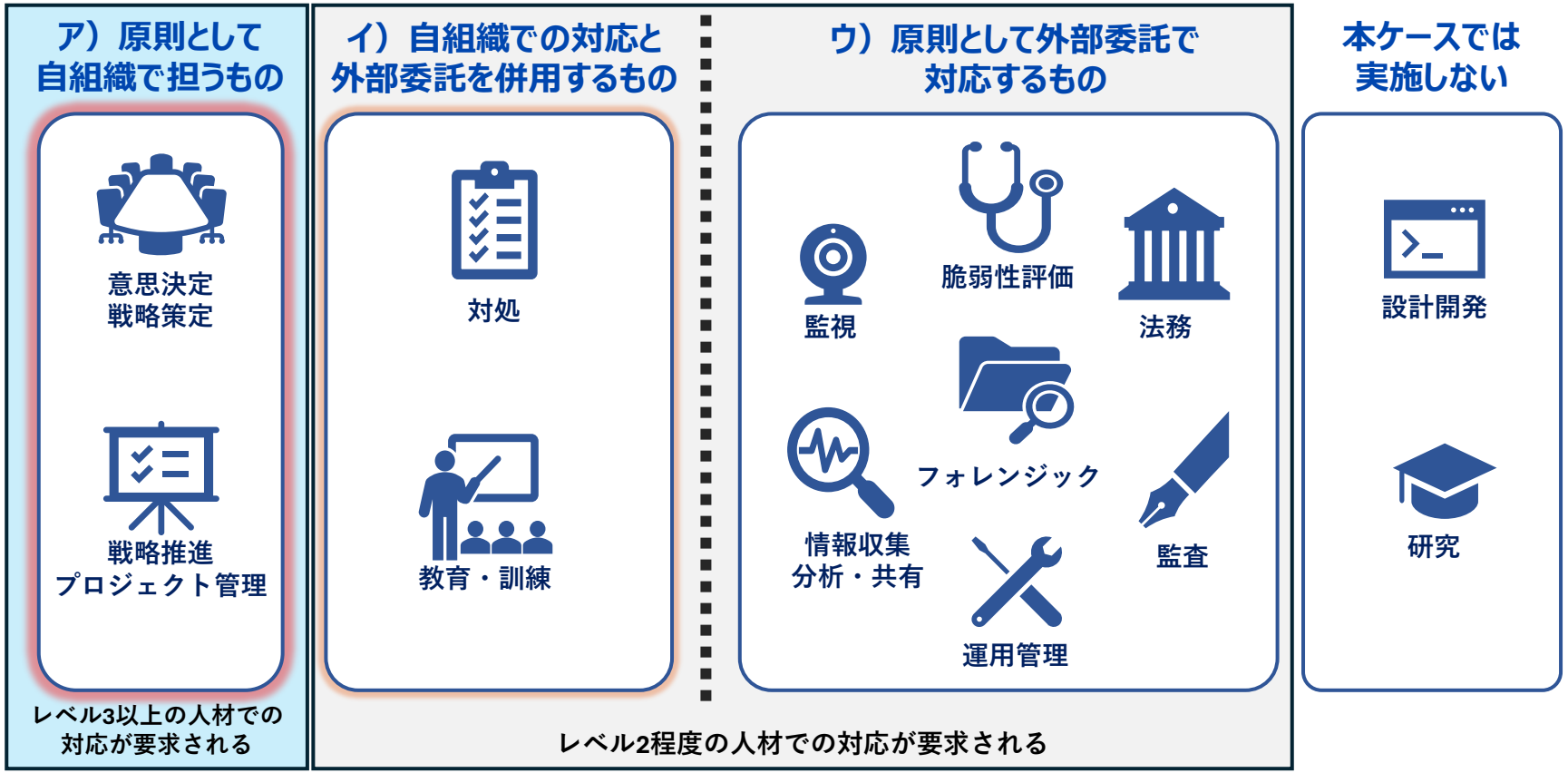
A社ではフレームワークが求めるサイバーセキュリティ人材が果たすべき役割の実現を、以下の４つのステップで実施することとしました。ステップ1～3では右に示すフレームワークの中身を活用します。



ケース 1

ステップ１：自組織で担うべき役割の明確化

- A社の従業員は**８名**であり、求められるサイバーセキュリティ対策をすべて講じるには十分な人的リソースがあるとはいえません。
- このため、**外部委託**に適する役割は委託することとしました。
- **「対処」**と**「教育・訓練」**は**自組織と委託を併用**することとし、「対処」のうち初動対応は自組織で担い、「教育・訓練」のうち初心者向け教育については、教材を購入して実施することとしました（高度な研修が必要な場合のみ外部の研修サービスを利用）。
- なお、A社は小売業であるため、事業にはSaaSの既存サービスを利用し、「設計開発」を行いません。

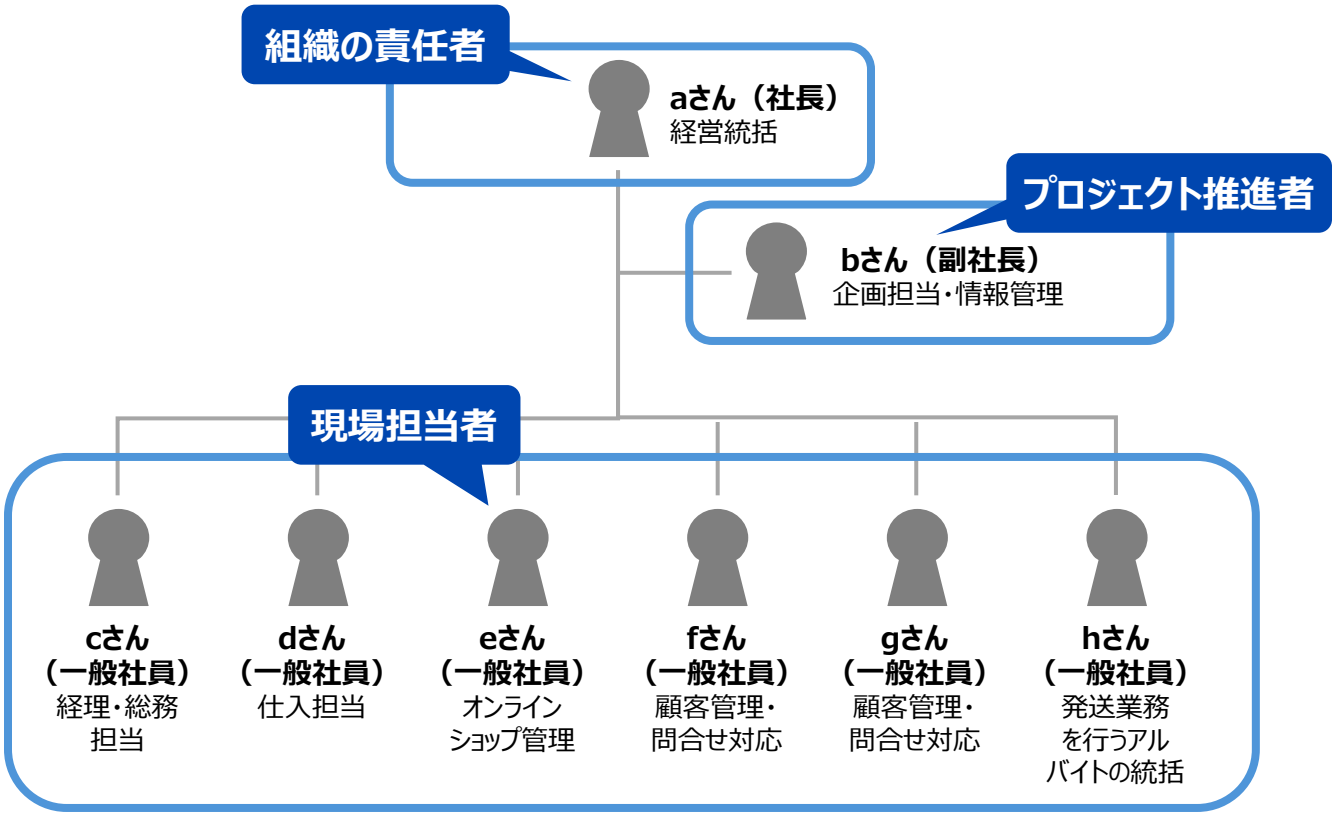


ケース 1

ステップ2：各自への「タスク」の割り当て

要員の類型化について

- 以降の説明では、A社の８名の役職員がフレームワークで定義されているタスクをどのように担当するのがよいかについて、下図のように３種類に類型化して説明します。
- 現場担当者については本来６人が対象となりますが、ステップ３以降では最もタスクが多いeさんを例に説明します。



ケース1

ステップ2：各自への「タスク」の割り当て

ア）原則として自組織で担う役割の検討例

ポイント

組織特性に応じたタスクの抽出と役割分担を行います

フレームワークでは、この役割に相当するタスクとして、下表に示すようなタスクを定義しています。A社では、「実際に無理なく回せるか」という観点から、表のように各タスクの役割分担・連携方法を考えました。

該当する役割	A社におけるタスクの分担イメージ		
	組織の責任者（aさん）	プロジェクト推進者（bさん）	現場担当者（eさんほか）
意思決定・戦略策定	● プロジェクト推進者が作成した案を検討・承認 ● 対策に必要な予算、リソースの確保 ● 通常時・緊急時・復旧時に備えた体制の構築 ● コンプライアンス確保に関する指示 ● 関係者とのコミュニケーションの実施	● 戦略、方針、規定等の案を策定 ● コンプライアンス確保のための社内ルール案等の策定 ● 委託先におけるセキュリティ対策の統括 ● 自己点検チェックリストの作成 ● 関係者とのコミュニケーションの実施	● 意思決定に必要な情報を収集 ● 予算検討に必要な情報を提供 ● コンプライアンス確保のための社内ルールの遵守 ● 自己点検チェックリストによる確認の実施 ● 関係者とのコミュニケーションの実施
戦略推進・プロジェクト管理	● 予算・人員等の調達・執行管理 ● 人事管理	● 運用ルールの立案 ● プロジェクトの立案、工程管理 ● 調達管理、委託先・サプライチェーン管理 ● 情報管理 ● 管理策の適用 ● サービスの品質管理	● 委託先とのコミュニケーション ● 情報管理

（注）表内のタスク名称は簡潔化のためサイバーセキュリティに関する内容であることが明確な場合は、「サイバーセキュリティに関する」等の記載を省略しています。（以降同様）

ケース 1

ステップ2：各自への「タスク」の割り当て

イ）自社での対応と外部委託を併用する役割の検討例

ポイント 外部委託と併用する役割についても、自組織が担うべきタスクを抽出します（タスクの範囲を特定）

A社では、「対処」と「教育・訓練」については自社での対応と外部委託を併用することを考えています。このときの委託先を含めた役割分担・連携方法を下表に示します。なお、「対処」については通常時と緊急時（インシデント発生時）とでタスクが異なることから、分けて記載します。

該当する役割	A社におけるタスクの分担イメージ			
	組織の責任者（aさん）	プロジェクト推進者（bさん）	現場担当者（eさんほか）	委託先
対処（通常時）	● インシデント対処計画承認 ● 委託先の選定案、委託内容案の承認、契約締結	● インシデント対処計画検討 ● 委託内容の選定 ● 委託先の選定 ● 委託先とのコミュニケーション	● 委託先候補の検討 ● 対処対象システムの選定 ● 委託先とのコミュニケーション	● 提案・見積作成 ● 契約締結
対処（緊急時）	● インシデント初期評価案の承認 ● トリアージ案の承認 ● インシデント対応措置の指示	● インシデント速報の受領 ● インシデント速報を受けた初期評価案の検討 ● トリアージ案検討 ● インシデント対応措置の実践	● インシデントの可能性検知 ● インシデント速報報告 ● 委託先への依頼等によるトリアージの実施 ● インシデント対応措置の実践	● インシデントの可能性検知 ● 初動対応 ● インシデント速報報告 ● インシデント初期調査 ● トリアージ案作成 ● インシデント対応措置の実践
教育・訓練	● 教材の発注の承認	–	● 教育・訓練内容の計画 ● 教材の選定・発注	● 教育サービスの提供 ● 教材の提供

ケース 1

ステップ2：各自への「タスク」の割り当て

ポイント 外部委託を基本とする役割についても、自組織が担うべきタスクを抽出します（委託先管理のためのタスク等）

ウ）原則として外部委託で対応する役割の検討例

この役割はA社では原則として外部委託にて実施することから、A社では、それぞれの役割については、主に委託管理に係るタスクが中心となります。そのため、下表では共通性の高い役割をまとめて扱っています。委託先が行う業務は役割によって異なりますが、内容が細かくなるため「委託された業務の実施」として同様にまとめて記載しています。

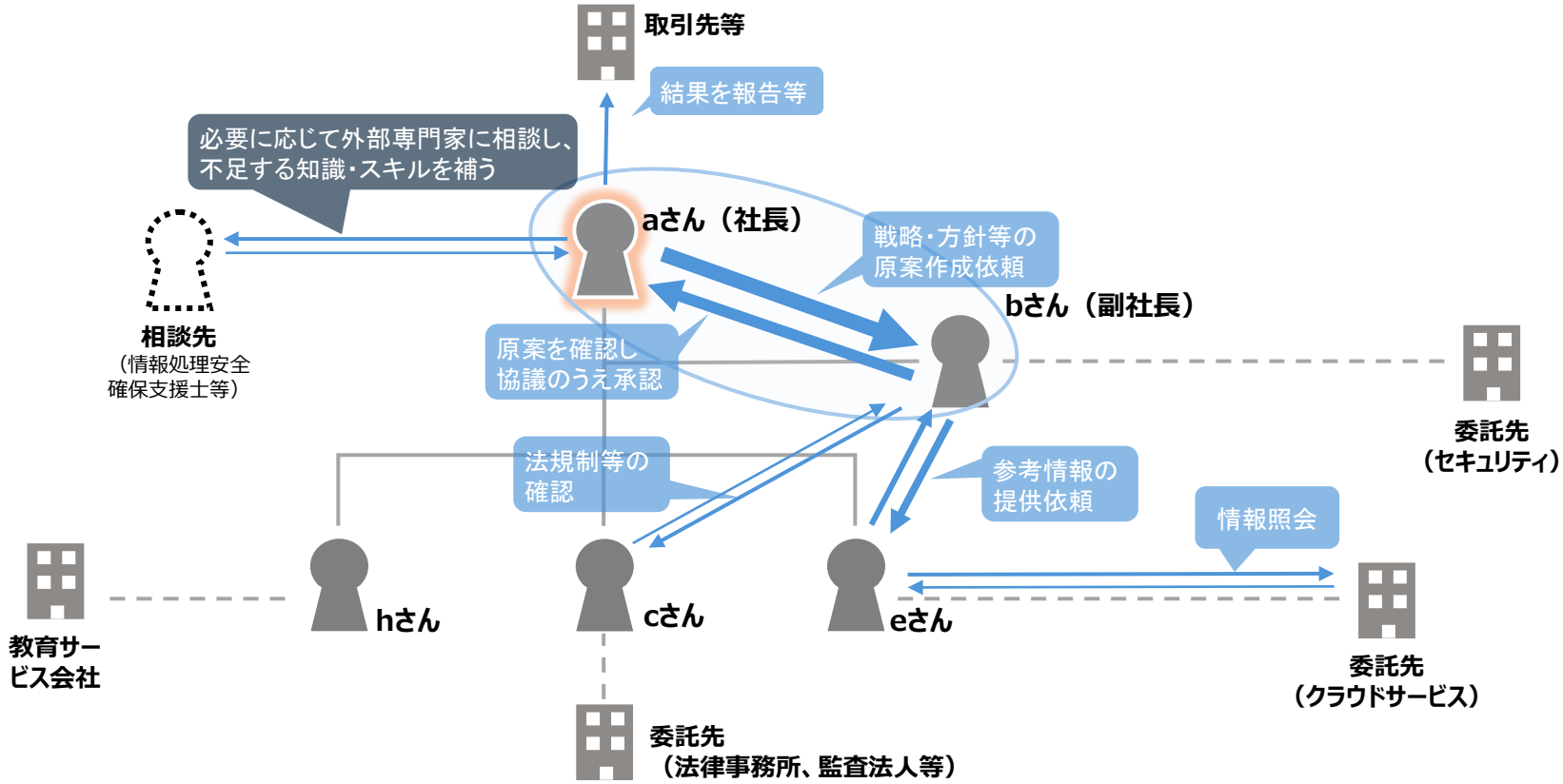
該当する役割	A社におけるタスクの分担イメージ			
	組織の責任者（aさん）	プロジェクト推進者（bさん）	現場担当者（eさんほか）	委託先
監視 **情報収集・分析・共有** **脆弱性診断** **フォレンジック** **運用管理**	● 委託先の選定案、委託内容案の承認、契約締結 ● 定期報告の参照	● 委託内容の選定 ● 委託先の選定 ● 委託先管理 ● 定期報告の参照 ● 委託先とのコミュニケーション	● 委託先候補の検討 ● 対象システムの選定 ● 定期報告の参照 ● 委託先とのコミュニケーション	● 提案・見積作成 ● 契約締結 ● 委託された業務の実施（内容は役割毎に異なる） ● 定期報告の実施
法務	● 委託先の選定案、委託内容案の承認、契約締結 ● 助言内容の活用	● 委託内容の選定 ● 委託先の選定 ● 委託先管理 ● 助言内容の活用	● 委託先候補の検討 ● 専門家の知見が必要な内容についての相談 ● 助言内容の活用	● 提案・見積作成 ● 契約締結 ● 法的リスク分析 ● 分析結果に基づく法的助言 ● 訴訟対応等
監査	● 委託先の選定案、委託内容案の承認、契約締結 ● 監査報告書の確認・承認	● 委託内容の選定 ● 委託先の選定 ● 委託先管理	● 委託先候補の検討 ● 監査対象範囲の選定	● 提案・見積作成 ● 契約締結 ● 監査（リスクアセスメントを含む）の実施 ● 監査報告書の作成

ケース 1

ステップ2：各自への「タスク」の割り当て

組織の責任者に関わる役割の実施フロー（通常時）

前ページまでに示したA社で行うべきタスクのうち、「戦略、方針、規定等の策定」について、組織の責任者をとりまく役割分担・連携のイメージを以下に示します。

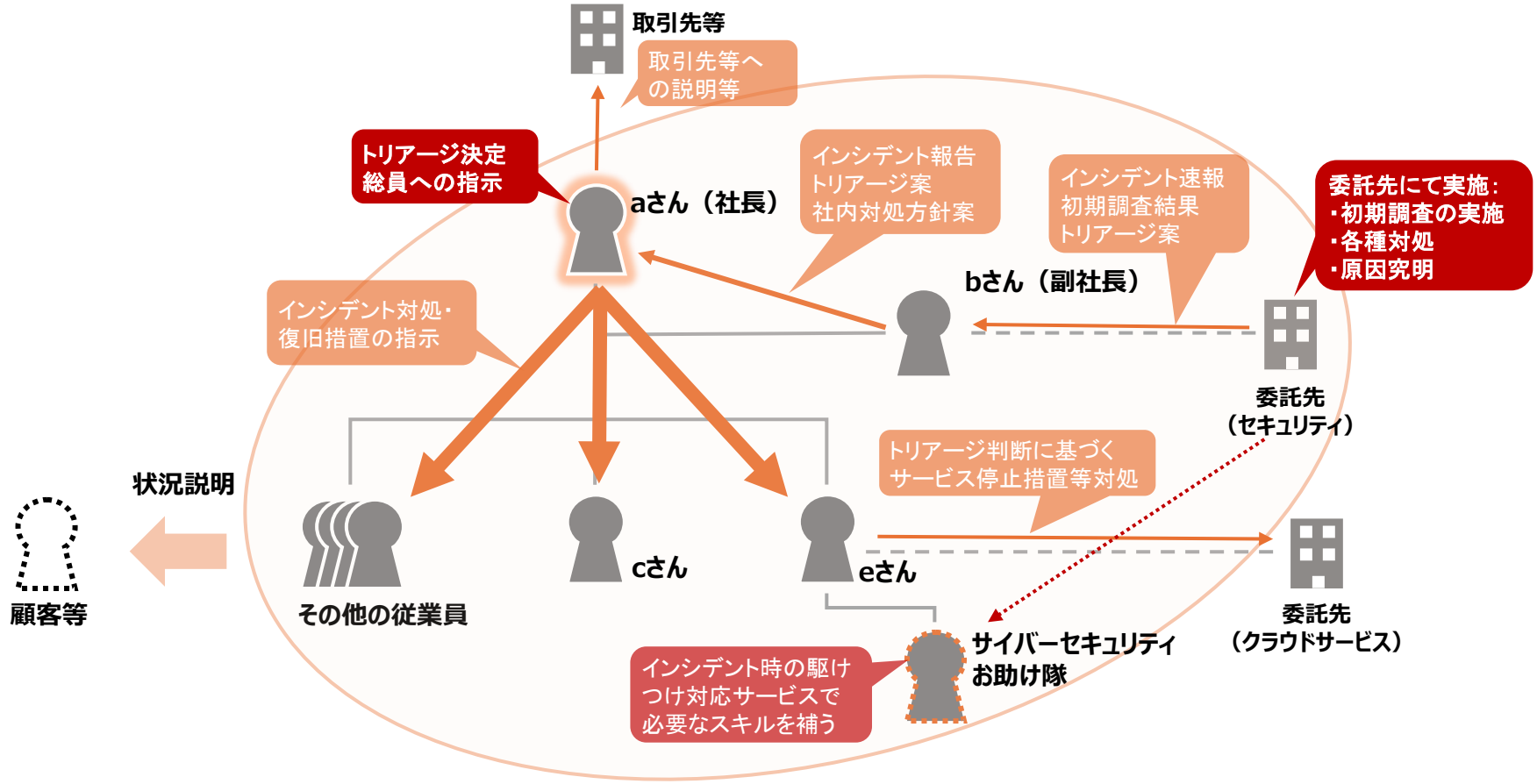


ケース 1

ステップ2：各自への「タスク」の割り当て

組織の責任者に関わる役割の実施フロー（緊急時）

インシデント発生時は、全従業員が一致団結しながら、次のような役割分担の下、連携しながら対処にあたります。
このときのaさんを中心とする役割分担・連携イメージを以下に示します。

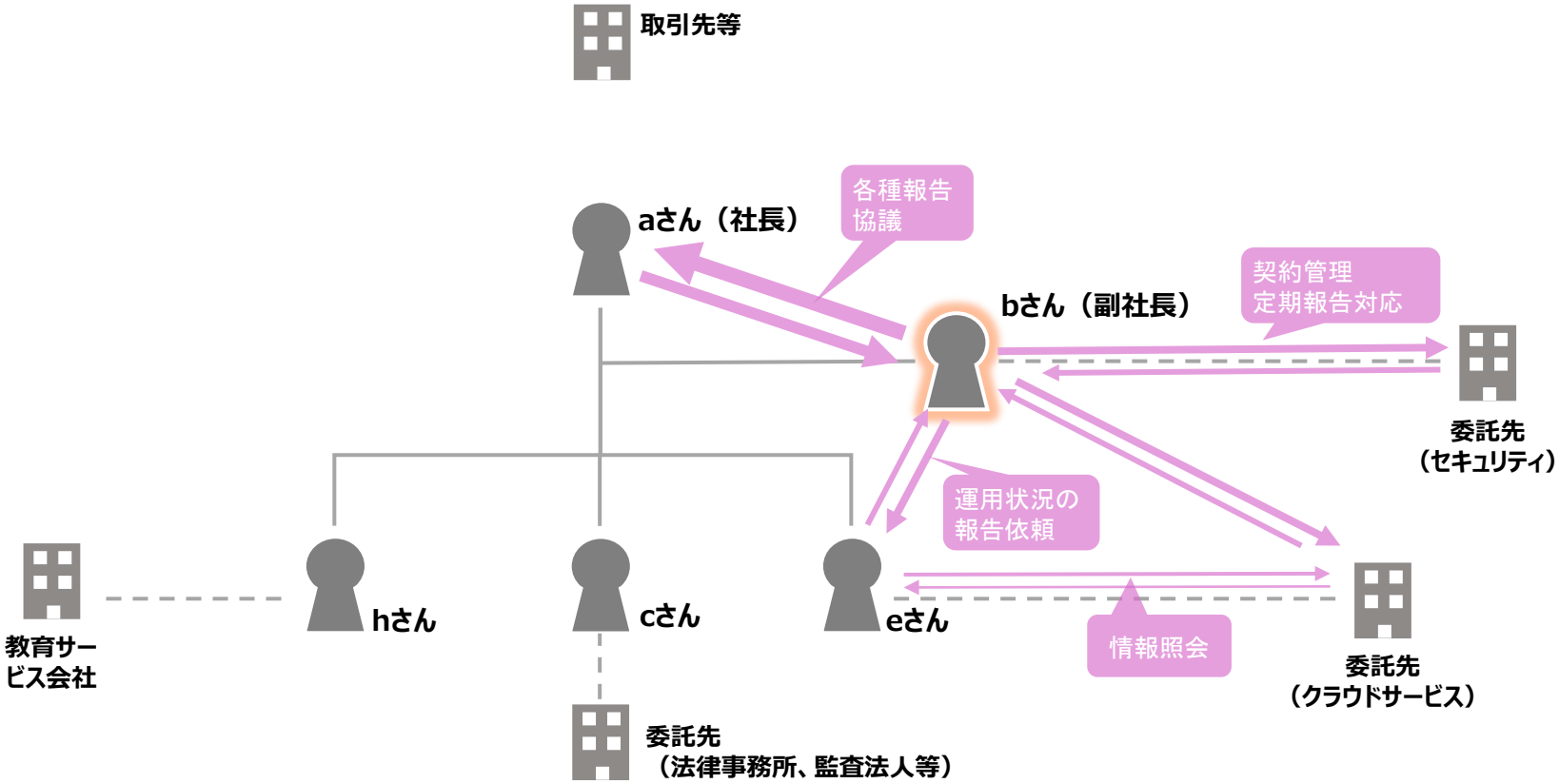


ケース 1

ステップ2：各自への「タスク」の割り当て

プロジェクト推進者に関わる役割の実施フロー

A社で行うべきタスクのうち、プロジェクト推進者であるBさんを中心に行われる「委託先管理」についての役割分担・連携のイメージを以下に示します。

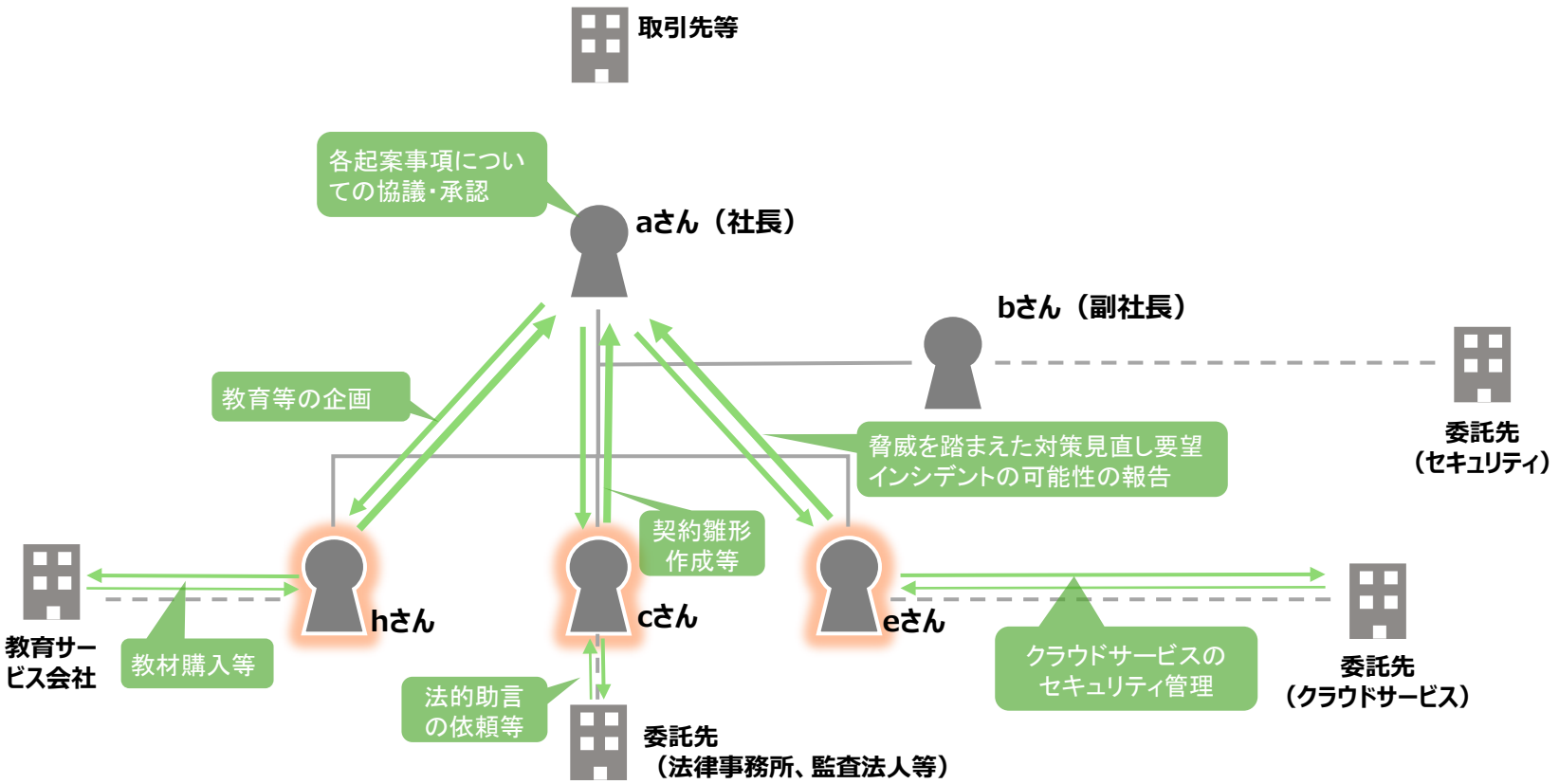


ケース 1

ステップ2：各自への「タスク」の割り当て

現場担当者に関わる役割の実施フロー

A社で行うべきタスクのうち、現場担当者が中心となって実施されるタスクについての役割分担・連携のイメージを以下に示します。

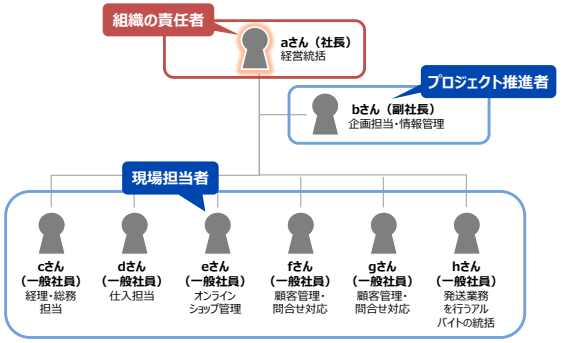


ケース 1

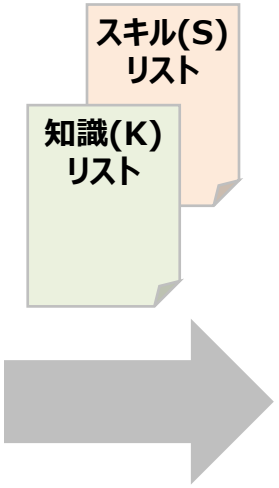
ステップ3：必要な「知識・スキル」の可視化

組織の責任者における人材像の明確化

aさんが担当するタスクを実施するために必要な知識及びスキルは、フレームワークに記載の知識及びスキルのリストをもとに下表のように抽出されます。



フレームワークで定義されているタスクのうち、aさんが担当するタスク	
通常時	各種起案事項の検討・承認
	対策に必要な予算、リソースの確保
	通常時・緊急時・復旧時に備えた体制の構築
	コンプライアンス確保に関する指示
	関係者とのコミュニケーションの実施
	予算・人員等の調達・執行管理
	人事管理
	委託先の選定案、委託内容案の承認、契約締結
	インシデント対処計画承認
	定期報告の参照
緊急時	インシデント初期評価案の承認
	トリアージ案の承認
	インシデント対応措置の指示



フレームワークの知識及びスキルのリストから選定

aさんの人材像に対応する知識・スキル	
セキュリティ関連	サイバーセキュリティ対策に関する基本的知識
	サイバーセキュリティ対策の最新動向に関する知識★
	サイバーセキュリティ関連の法規制や手続等に関する知識
	サイバーセキュリティ分野のインシデント対応に関する知識★
	組織に必要なセキュリティ人材の規模や要件に関する知識●
	組織全体のセキュリティに係る予算の配分手法に関する知識●
	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル★
	組織のサイバーセキュリティに係る方針や目標を策定し、組織設計を行うスキル●
	組織に必要なセキュリティ人材の要件を評価するスキル●
	インシデント対応計画を策定するスキル★
それ以外	経営・組織運営、自組織の戦略に関する知識●
	リスクマネジメントに関する知識
	組織のシステムやネットワークの基本原則や構造に関する知識●
	AI利用時に留意すべき内容についての知識
	組織目標と体制を評価するスキル●
	法令や規制等を評価し、組織への影響を特定するスキル●
	必要な関係者に自組織の戦略等を適切な手段で周知するスキル●
	コミュニケーションスキル

●は自組織の業務ドメインに関する知識の習得が必須であるため、自身で必要な水準の習得が必要な知識・スキル

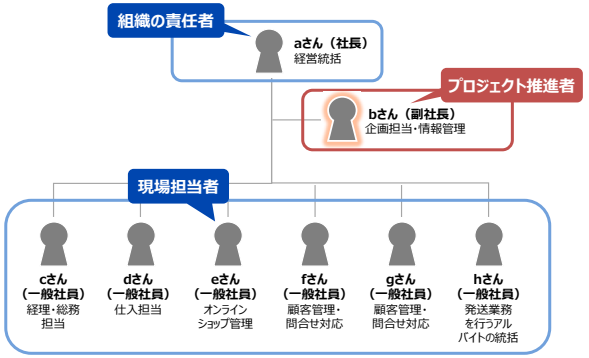
★は情報処理安全確保支援士等の専門的支援を受けることで充足させることが可能な知識・スキル

ケース 1

ステップ3：必要な「知識・スキル」の可視化

プロジェクト推進者における人材像の明確化

bさんが担当するタスクを実施するために必要な知識及びスキルは、
フレームワークに記載の知識及びスキルのリストをもとに
下表のように抽出されます。



フレームワークで定義されているタスクのうち、bさんが担当するタスク	
通常時	戦略、方針、規定等の起案
	プロジェクトの立案、工程管理
	コンプライアンス確保のための社内ルール案等の策定
	委託内容の選定
	委託先の選定
	調達・委託先管理、コミュニケーション
	委託先のセキュリティ対策の統括
	運用ルールの立案
	情報管理
	管理策の適用
	自己点検チェックリストの作成
	インシデント対処計画検討
	定期報告の参照
緊急時	インシデント速報を受けた初期評価案の検討
	トリアージ案検討
	インシデント対応措置の実践

スキル(S)リスト
知識(K)リスト

フレームワークの知識及びスキルのリストから選定

bさんの人材像に対応する知識・スキル	
セキュリティ関連	サイバーセキュリティ対策に関する基本的知識
	サイバーセキュリティ対策の最新動向に関する知識★
	サイバーセキュリティ関連の法規制や手続等に関する知識
	サイバーセキュリティ対策としての監視に関する知識★
	サイバーセキュリティ分野のインシデント対応に関する知識★
	商用サイバーセキュリティサービスに関する知識
	自組織におけるサイバーセキュリティ対策に関する戦略、計画、対象機器等に関する知識●
	サイバーセキュリティ対策において今後考慮すべき内容を把握するスキル★
	サイバーセキュリティ対策に関する方針や計画等を策定するスキル●
	サイバーセキュリティ関連の法規制対応を行うスキル
	サイバーセキュリティ対策の評価及び見直しに関するスキル★
	インシデントにおける一連の対応を実施するスキル★
それ以外	リスクマネジメントに関する知識
	AI利用時に留意すべき内容についての知識
	コミュニケーションスキル

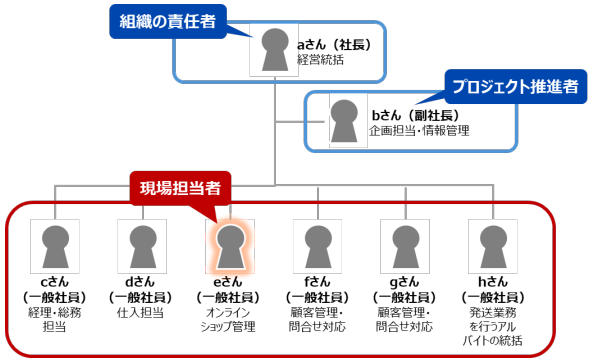
●は自組織の業務ドメインに関する知識の習得が必須であるため、自身で必要な水準の習得が必要な知識・スキル
★はベンダーの専門的支援を受けることを前提に、ベンダーとのセキュリティ対策に関する会話が可能な水準の習得を目標とする知識・スキル

ケース 1

ステップ3：必要な「知識・スキル」の可視化

現場担当者における人材像の明確化

eさんが担当するタスクを実施するために必要な知識及びスキルは、
フレームワークに記載の知識及びスキルのリストをもとに
下表のように抽出されます。



フレームワークで定義されているタスクのうち、eさんが担当するタスク	
通常時	意思決定や予算検討に必要な情報を提供
	コンプライアンス確保のための社内ルールの遵守
	委託や管理の対象システムの選定
	委託先候補の検討
	関係者とのコミュニケーションの実施
	自己点検チェックリストによる確認の実施
	情報管理
	定期報告の参照
緊急時	インシデントの可能性検知
	インシデント速報報告
	委託先への依頼等によるトリアージの実施
	インシデント対応措置の実践

スキル(S)リスト

知識(K)リスト

フレームワークの知識及びスキルのリストから選定

eさんの人材像に対応する知識・スキル	
セキュリティ関連	サイバーセキュリティ対策に関する基本的知識
	サイバーセキュリティ対策の最新動向に関する知識★
	アクセス制御に関する知識
	データセキュリティの管理に関する知識
	検知ツールに関する知識★
	監視ツールに関する知識★
	適切なセキュリティ対策の設定方法に関する知識
	自組織におけるサイバーセキュリティ対策に関する戦略、計画、対象機器等に関する知識●
	システム管理活動の一連の流れを評価し、課題点を改善するスキル★
	組織のポリシーに適したアクセス制御を実施し、正しく制御されていることを確認するスキル●
	インシデントにおける一連の対応を実施するスキル★
	セキュリティ運用においてAIを適切に活用するスキル★
それ以外	リスクマネジメントに関する知識
	AI利用時に留意すべき内容についての知識
	コミュニケーションスキル

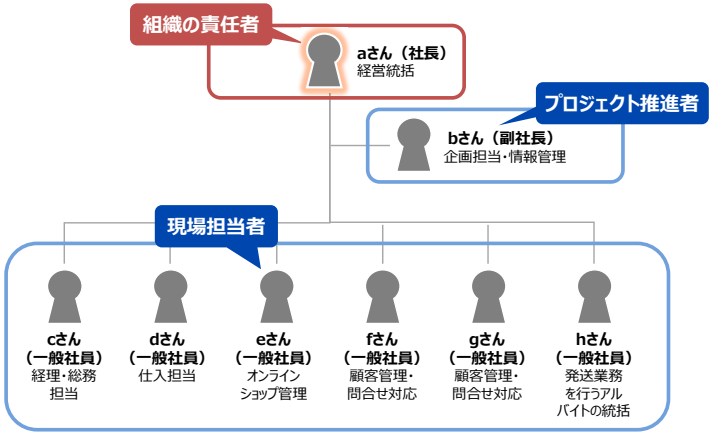
●は自組織の業務ドメインに関する知識の習得が必須であるため、自身で必要な水準の習得が必要な知識・スキル
★はベンダーの専門的支援を受けることを前提に、ベンダーとのセキュリティ対策に関する会話が可能な水準の習得を目標とする知識・スキル

ケース1

ステップ4：「知識・スキル」の習得方法の決定・実施

組織の責任者における習得方針

ステップ3のリストをもとにaさんは現在不足しているセキュリティ関連の知識及びスキルを習得するため、今後次のような取組を進めていくことにしました。



aさんの人材像に対応するセキュリティ関連の知識・スキル
サイバーセキュリティ対策に関する基本的知識
サイバーセキュリティ対策の最新動向に関する知識
サイバーセキュリティ関連の法規制や手続等に関する知識
サイバーセキュリティ分野のインシデント対応に関する知識
組織に必要なセキュリティ人材の規模や要件に関する知識
組織全体のセキュリティに係る予算の配分手法に関する知識
今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル
組織のサイバーセキュリティに係る方針や目標を策定し、組織設計を行うスキル
組織に必要なセキュリティ人材の要件を評価するスキル
インシデント対応計画を策定するスキル

- 情報セキュリティマネジメント試験の受験（レベル2相当）
- CYDER Aコース等、インシデント対応を含む演習への参加（レベル2相当）
- サイバーセキュリティに関する最新トピックスを扱うオンライン研修への参加（レベル2相当）
- フレームワーク手引き書（大規模組織向け）（レベル対象外）

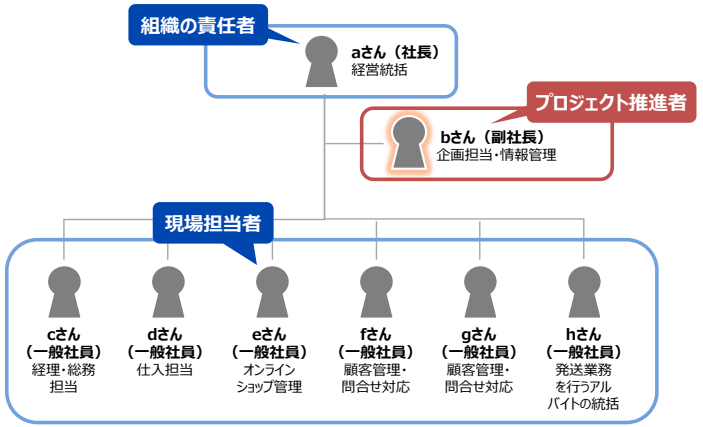
習得のステップ

ケース 1

ステップ4：「知識・スキル」の習得方法の決定・実施

プロジェクト推進者における習得方針

ステップ3のリストをもとにbさんは現在不足しているセキュリティ関連の知識及びスキルを習得するため、今後次のような取組を進めていくことにしました。



bさんの人材像に対応するセキュリティ関連の知識・スキル
サイバーセキュリティ対策に関する基本的知識
サイバーセキュリティ対策の最新動向に関する知識
サイバーセキュリティ関連の法規制や手続等に関する知識
サイバーセキュリティ対策としての監視に関する知識
サイバーセキュリティ分野のインシデント対応に関する知識
商用サイバーセキュリティサービスに関する知識
自組織におけるサイバーセキュリティ対策に関する戦略、計画、対象機器等に関する知識
サイバーセキュリティ対策において今後考慮すべき内容を把握するスキル
サイバーセキュリティ対策に関する方針や計画等を策定するスキル
サイバーセキュリティ関連の法規制対応を行うスキル
サイバーセキュリティ対策の評価及び見直しに関するスキル
インシデントにおける一連の対応を実施するスキル

- 情報セキュリティマネジメント試験の受験（レベル2相当）
- CYDER Aコース等、インシデント対応を含む演習への参加（レベル2相当）
- サイバーセキュリティに関する最新トピックスを扱うオンライン研修への参加（レベル2相当）

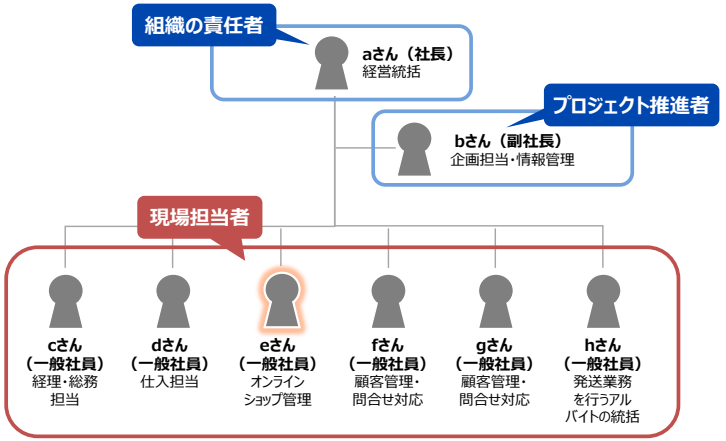
習得のステップ

ケース 1

ステップ4：「知識・スキル」の習得方法の決定・実施

現場担当者における習得方針

ステップ3のリストをもとにeさんは現在不足しているセキュリティ関連の知識及びスキルを習得するため、今後次のような取組を進めていくことにしました。



eさんの人材像に対応するセキュリティ関連の知識・スキル
サイバーセキュリティ対策に関する基本的知識
サイバーセキュリティ対策の最新動向に関する知識
アクセス制御に関する知識
データセキュリティの管理に関する知識
検知ツールに関する知識
監視ツールに関する知識
適切なセキュリティ対策の設定方法に関する知識
自組織におけるサイバーセキュリティ対策に関する戦略、計画、対象機器等に関する知識
システム管理活動の一連の流れを評価し、課題点を改善するスキル
組織のポリシーに適したアクセス制御を実施し、正しく制御されていることを確認するスキル
インシデントにおける一連の対応を実施するスキル

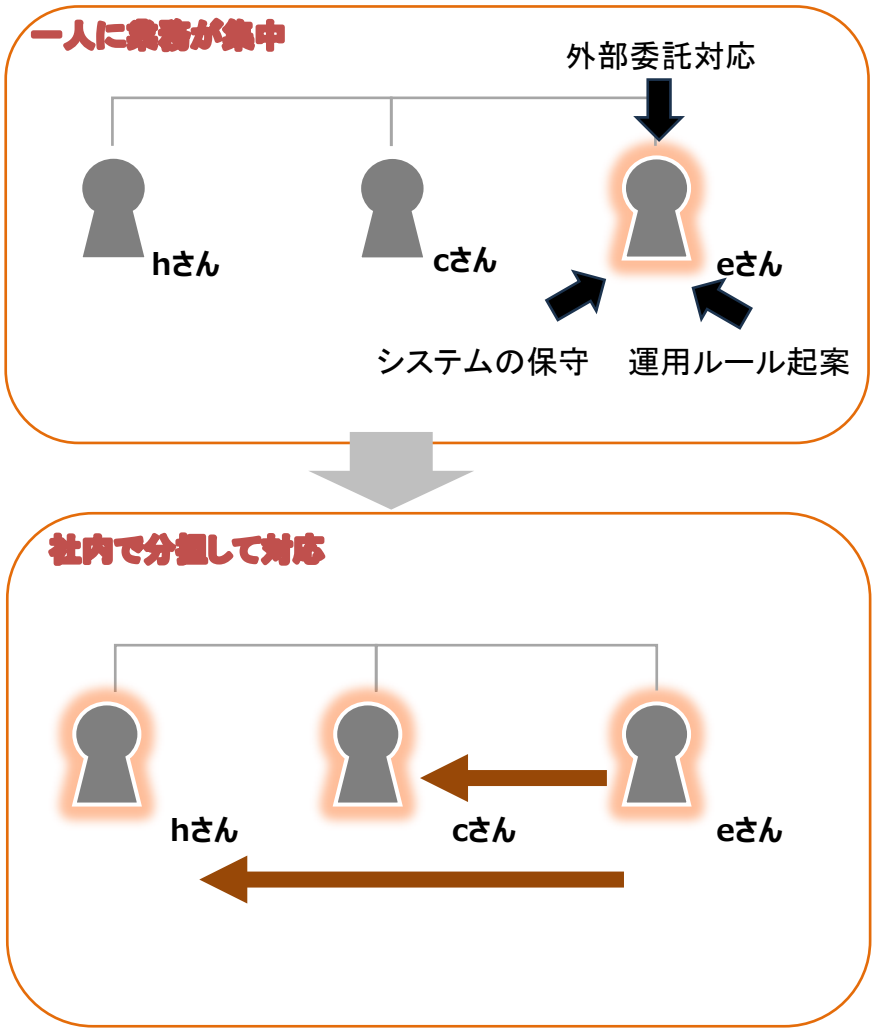
- 情報セキュリティマネジメント試験の受験（レベル2相当）
- CYDER Aコース等、インシデント対応を含む演習への参加（レベル2相当）
- SOCやCSIRTの業務内容を扱うオンライン研修への参加（レベル2相当）
- サイバーセキュリティに関する最新トピックスを扱うオンライン研修への参加（レベル2相当）

習得のステップ

ケース 1

現場担当者への業務の分散

- 小規模組織においても、複数の担当者でセキュリティ関連の業務を担うことは、特定の担当者の負荷を低減し、組織のリスクを下げる上でも重要です。



問題点

- サイバー攻撃や情報漏えいが発生した際に、eさん一人で「被害の初期調査」「ネットワークの遮断」「経営陣への報告」「外部機関・顧客への対応」などを同時に行うことは不可能です。
- eさんが何らかの理由で作業できない場合は、誰もシステムや対応手順がわからないというリスクがあります。

対応

- インシデント対応を分散・移行することで、eさんに業務が集中する事態を回避し、リスクの分散も可能となります。
- 一方で、eさん以外のメンバーが業務を担うことは一朝一夕ではできません。本手引き書で設定したA社の各メンバー（cさんやeさん等）の個人の視点に立ち、既存業務に付加してセキュリティ業務を担うために必要なタスクや学習方法を解説した「サイバーセキュリティ人材フレームワーク活用の手引き2026（個人（プラス・セキュリティ）向け）」（P.17～P.23等の事例）を参照することが有効です。

ケース２
デジタルスキルが不十分な従業員が多い
B社（製造業：部品製造）の場合

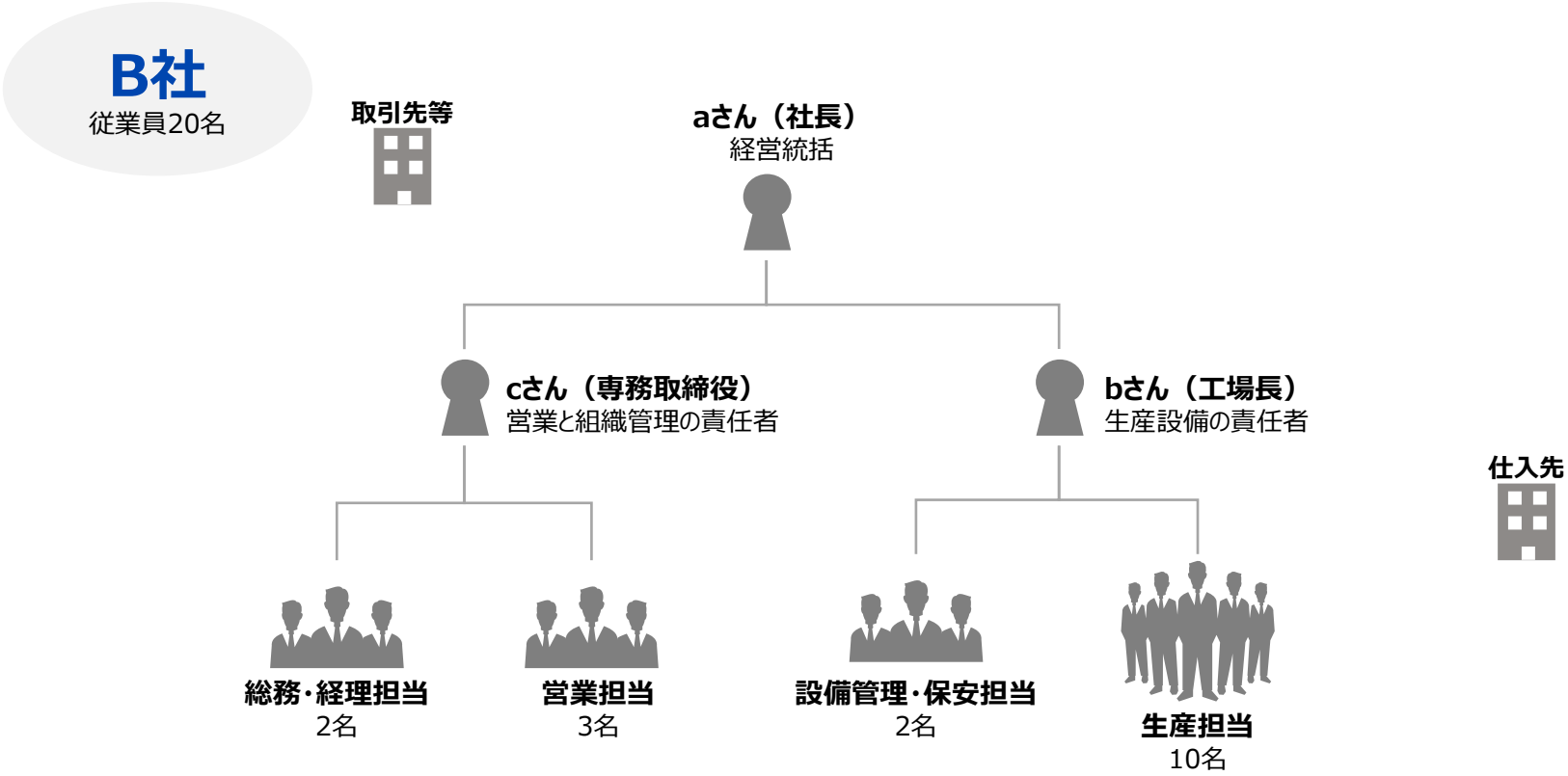
	【ケース１】	【ケース２】	【ケース３】
サイバーセキュリティ対策における悩み	 サイバーセキュリティ対策はこれまで外部業者に任せており、「自組織でやるべきこと」をあまり意識できていなかった。	 取引先から経済産業省の「セキュリティ対策評価制度」への対応を要求されているが、どうすればよいかわからない。	 サイバーセキュリティ対策は代表者が実質一人ですべて対応しているが、やるべきこと（タスク）が何かを把握したい。
想定する企業属性	● 従業員8名 ● 小売業（ネット販売） ● PCは使いこなせるが、セキュリティはよくわからないという従業員が大半。	● 従業員20名 ● 製造業（部品製造） ● 「工場の設備なら慣れているが、PCは苦手」という従業員が多い。 ● 工場はネットに接続していない。	● 従業員2名（代表＋アシスタント） ● サービス業（デザイナー）

ケース 2

デジタルスキルが不十分な従業員が多い B社（製造業：部品製造）の場合

モデル組織のB社はこんな会社です

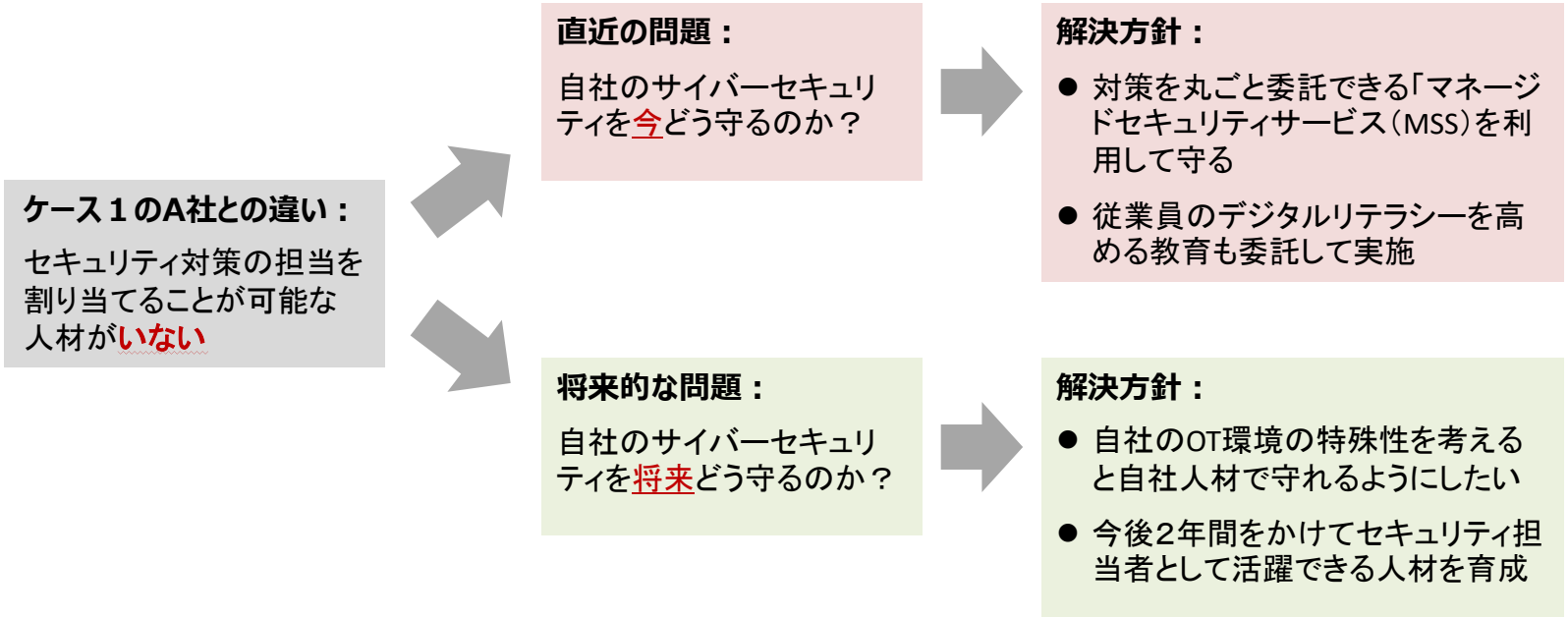
- 機械部品の製造として、複数の取引先に対して製品を供給しているサプライヤーです。部品材料の仕入先も複数あります。
- 取引先より、「経済産業省の『サプライチェーン強化に向けたセキュリティ対策評価制度』に対応する準備をしてほしい」と言われていますが、社長のaさんの目から見て、現状の体制では満足な対応ができるようには思えません。



ケース 2

A社との違い：直ちに担当者を割り当てることが困難

- 現在、あらゆる企業において自社のサイバーセキュリティ対策を自ら説明できることが期待されています。一方で、デジタルスキルが不十分な人材が自組織に必要なサイバーセキュリティ対策を理解し、統制できるようになるには時間を要し、短期での育成などは現実的ではありません。
- そこでケース1で説明したすでにデジタル有スキル者が体制に含まれるA社と同様の方法をとれないB社の場合、まずは下図のように外部委託をフルに活用して従業員に起因するインシデントを発生しにくくすることが考えられます。これで時間を確保した上で、その間に自社の工場を自分で守ることのできる人材を育成することを考えていきます。



ケース 2

自組織で担うべき役割の明確化（現状での対応）

ポイント
- 委託を活用し、インシデントを生じさせない仕組みと教育を徹底
- 並行して今後組織内の管理を担っていく人材を育成

デジタルスキルが不十分な人材が自組織に必要なサイバーセキュリティ対策を理解し、その統制ができるようになるには時間を要することから、B社では当面の間は委託可能なものをすべて委託し、その間にセキュリティを理解した人材を育成することとします。

ア）原則として自組織で担うもの

- 意思決定
- 戦略策定
- 戦略推進
- プロジェクト管理

レベル3以上の人材での対応が要求される

イ）委託可能なものをすべて委託した場合に外部委託される役割

- 対処
  - 対処に限らず幅広くセキュリティ対策をカバーするマネージドセキュリティサービス（MSS）を利用
  - 工場のインシデントは現在の保安要員で対処
- 監視
- 脆弱性評価
- 法務
- フォレンジック
- 監査
- 教育・訓練
  - ケース1で社内実施を想定していたセキュリティ基礎教育ほか、ITリテラシー教育も含めて委託
- 情報収集 分析・共有
- 運用管理

委託先管理という観点で、レベル1～2程度の人材での対応が要求される

本ケースでは実施しない

- 設計開発
- 研究

ケース 2

自組織で担うべき役割の明確化（2年後の目標）

ポイント

- 将来的に、自社のサイバーセキュリティリスクの管理や対処を可能な範囲で自社人材で担う目標を設定

選抜した担当者へのセキュリティの専門教育、及びその他要員へのリテラシー教育を実施した後のB社の役割構成は次のようになり、ケース1のA社と同様にサイバーセキュリティ対策を可能な範囲で自社人材で担うこととします。

ア）原則として自組織で担うもの

- 意思決定
- 戦略策定
- 戦略推進
- プロジェクト管理

レベル3以上の人材での対応が要求される

イ）自組織での対応と外部委託を併用するもの

- 対処
- 教育・訓練

レベル3を目指して自組織の要員を育成

- インシデント発生時には、設備の稼働状況や製造工程への影響を即座に判断し、生産ラインの停止・継続の判断を自社で行う必要
- 工場特有のリスクや業務手順に即した実践を自社で教育が必要。

ウ）原則として外部委託で対応するもの

- 監視
- 脆弱性評価
- 法務
- フォレンジック
- 情報収集 分析・共有
- 監査
- 運用管理

レベル2程度の人材での対応が要求される

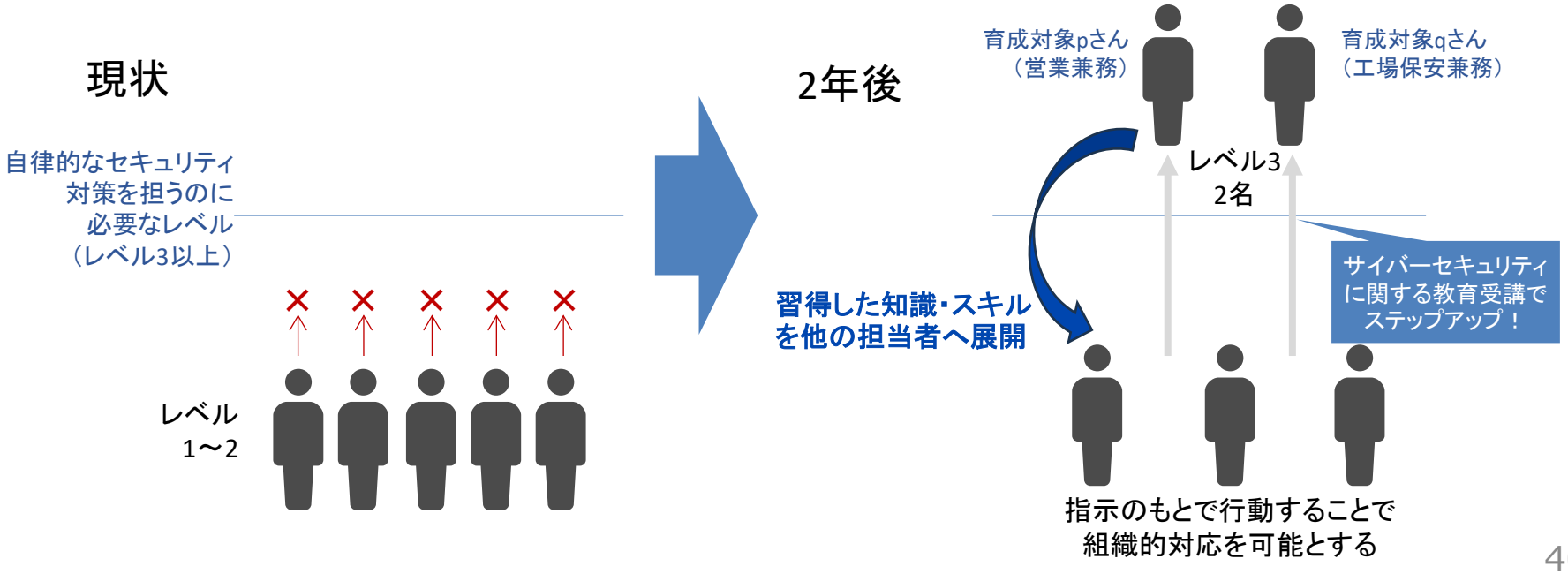
本ケースでは実施しない

- 設計開発
- 研究

ケース 2

必要な役割を満たしていくための方法の検討

- 前ページに示したように、B社も最終的にはA社と同様、インシデント発生時の対処等、自社の事業の存続に関わるような対策は自社の人材で対処できるようにすることを考えています。その実現を2年後に設定し、現状とのギャップを把握した上で、そのギャップを埋めることができる人材の育成を主たる対策として進めることとします。
- B社では上記を踏まえ、セキュリティ担当者(2名程度)を育成することとしました。
- 人選にあたっては、工場の生産設備(OTシステム)に関するインシデント対処には設備固有の専門知識が不可欠であることから、工場の設備や業務プロセスに精通した人材を優先的に選定しました。具体的には、設備管理・保安業務の経験を有するqさんをセキュリティ担当者(工場保安兼務)として選定するとともに、営業担当として取引先のセキュリティ要求を理解しているpさんをもう1名のセキュリティ担当者として選定しました。いずれも知識・スキル習得に前向きな姿勢を示してくれたことも選定の後押しとなっています。
- なお、育成の完了後は、pさん・qさんが習得した知識・スキルを各現場の担当者に展開する役割も担うこととし、社内全体のセキュリティリテラシーの底上げにつなげていく計画です。



ケース 2

習得すべき知識・スキルに関する目標の設定

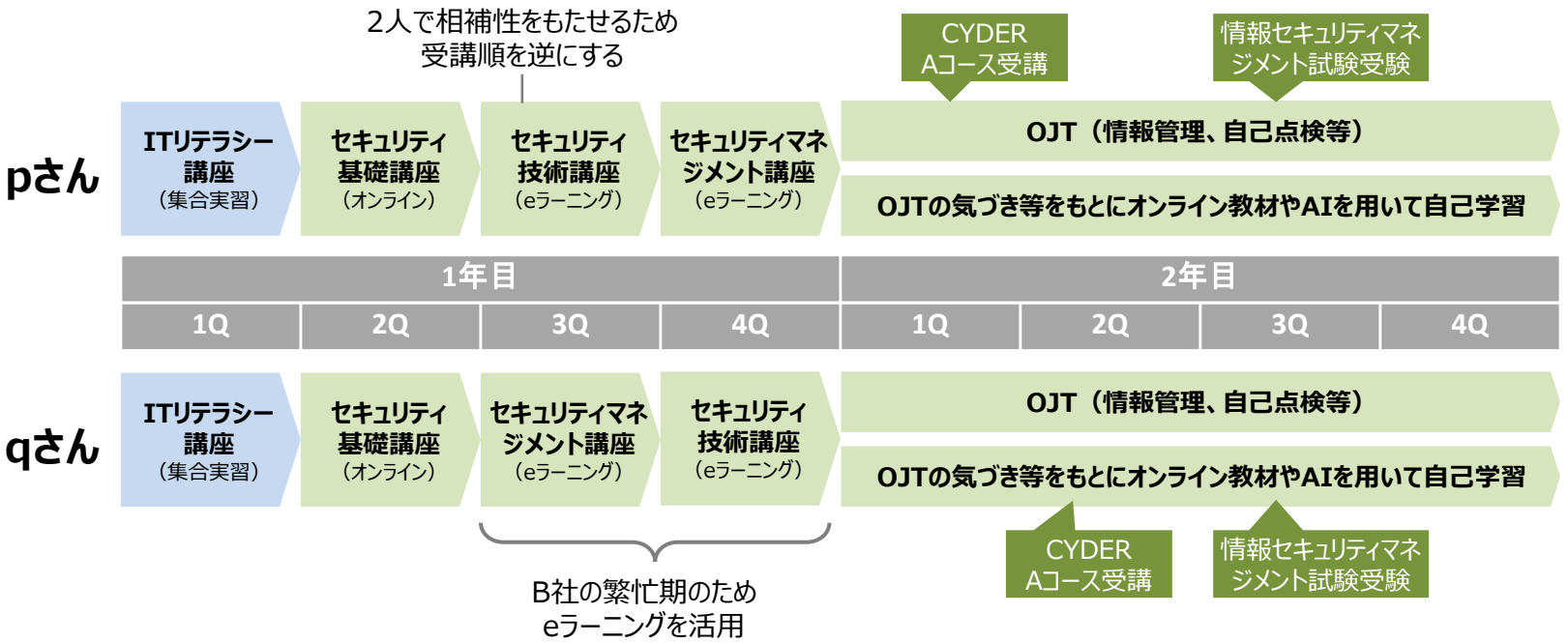
- B社における育成の目標は、外部委託だけでは対応が困難な部分、すなわち工場設備に関する専門的判断や委託先との連携・管理を自社人材で担えるようにすることです。特にOTシステムに関するインシデント対処や、委託先が提供するサービスの内容を適切に評価・管理するためには、社内にセキュリティの知識・スキルを持つ人材が不可欠です。この目標をもとにフレームワークを使ってタスクと知識・スキルを抽出しました。

役割	タスク（社内で担うべきもの）	タスク実施に必要な知識・スキル（抜粋）
 対処	● インシデント対処準備 ● インシデントの可能性検知及び初動対応 ● 初動対応時におけるインシデントの速報の報告 ● 委託先とのコミュニケーションの実施 ● 委託先の選定及び委託内容の調整	● インシデントの可能性がある場合に、適切な報告先へ報告するスキル ● インシデントの初動対応に関する知識 ● インシデントの初動対応を実施するスキル ● インシデント速報の報告手順・対象に関する知識 ● インシデント対応措置及びその実施に関する知識 ● インシデント対処における法律等の規制要件に関する知識 ● インシデント対処を実施するスキル ● インシデント対処活動の手順や手法に関する知識 ● コンプライアンスおよびプライバシーの原則と実践に関する知識 ● OTにおける脅威と対策に関する知識 ● 商用のインシデント対処サービスに関する知識 ● サイバーセキュリティ上のリスク管理の原則と実務に関する知識 ● チームビルディング活動の実施に関する知識 ● リスクマネジメントに関する知識 ● 関係者と適切なコミュニケーションを行うスキル ● 組織内外のステークホルダーと連携・協力するスキル
 教育・訓練	● 教育・訓練内容の計画 ● 教材又は啓発コンテンツの企画・設計・開発 ● 教育・訓練の実施 ● 委託先とのコミュニケーションの実施	● サイバーセキュリティの原則、脅威、脆弱性について教育するスキル ● サイバーセキュリティの新たな技術やリスクに関する知識 ● サイバーセキュリティの新たな技術やリスクについて教育するスキル ● 教材を開発または選定するスキル ● 受講者の学習を指導・ファシリテートするスキル ● 授業目標を設定するスキル ● 教育・訓練を受講する組織のセキュアな組織運営をするための情報収集、管理、対処等に関する知識

ケース 2

人材の育成プラン

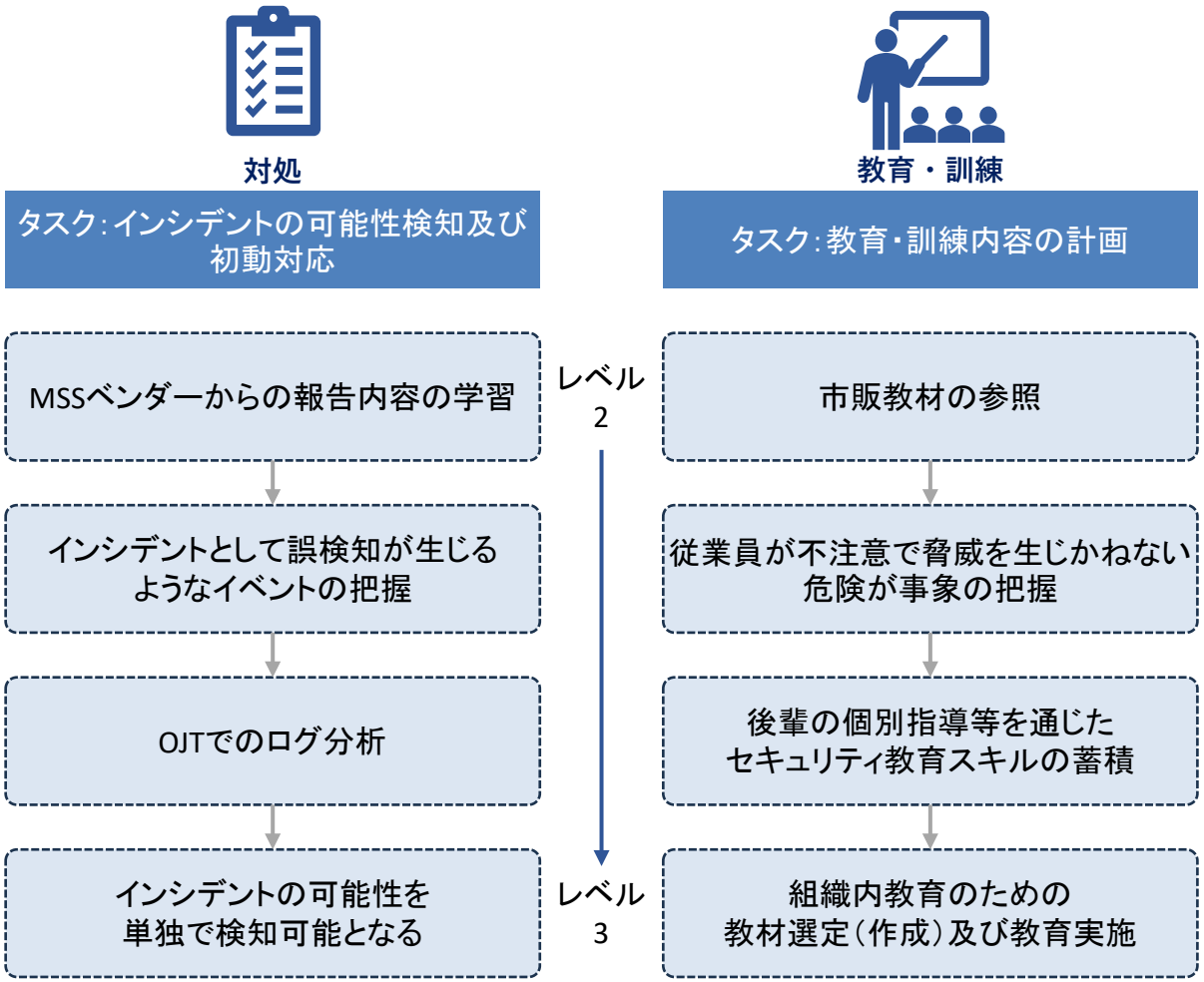
- B社におけるセキュリティ人材の育成プランを示します。B社では2人を選んで業務の負担を減らしつつ、次のようなスケジュールでセキュリティの知識・スキルを習得してもらうこととしました。
- 研修や座学だけでなく、委託先からの定期報告はセキュリティ実務を学ぶ貴重な機会であるので、人材育成に積極的に活用することとします。
- 担当者の育成と合わせて、社長と専務取締役もセミナーを受講することで経営者に求められる知識・スキルの習得に努めます。



ケース 2

知識・習得の経過に応じて担当するタスク

- 前ページの育成計画の経過とともに、自社で行うべきタスクをどのように実施していくかを以下に示します。



ケース３
個人経営に近い企業
C社（サービス業：デザイナー）の場合

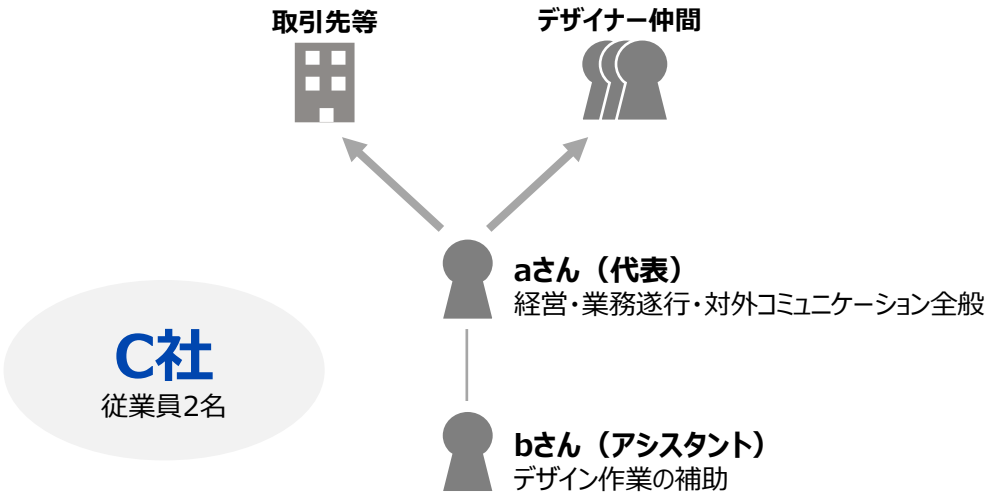
	【ケース１】	【ケース２】	【ケース３】
サイバーセキュリティ対策における悩み	 サイバーセキュリティ対策はこれまで外部業者に任せており、「自組織でやるべきこと」をあまり意識できていなかった。	 取引先から経済産業省の「セキュリティ対策評価制度」への対応を要求されているが、どうすればよいかわからない。	 サイバーセキュリティ対策は代表者が実質一人ですべて対応しているが、やるべきこと（タスク）が何かを把握したい。
想定する企業属性	● 従業員8名 ● 小売業（ネット販売） ● PCは使いこなせるが、セキュリティはよくわからないという従業員が大半。	● 従業員20名 ● 製造業（部品製造） ● 「工場の設備なら慣れているが、PCは苦手」という従業員が多い。 ● 工場はネットに接続していない。	● 従業員2名（代表＋アシスタント） ● サービス業（デザイナー）

ケース 3

個人経営に近い企業C社（サービス業：デザイナー）の場合

モデル組織のC社はこんな会社です

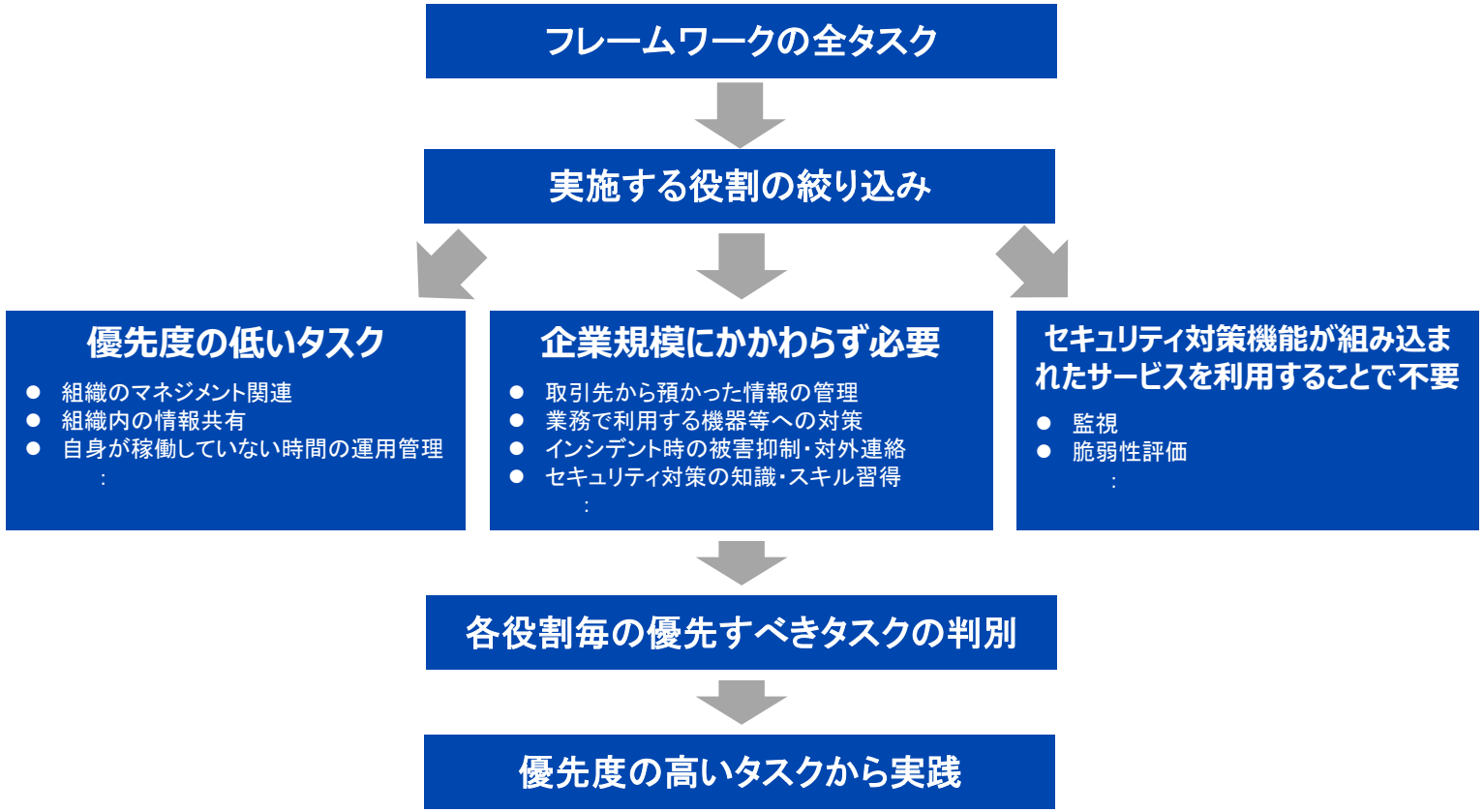
- デザイナーとして独立したaさんが実質１名で運営している法人です。
- 業務は取引先からの受託のほか、デザイナー仲間と共同で受託したデザイン業務を分担することもあります。
- アシスタントはaさんから依頼されたデザインの作業を分担するのみで、取引先等とのやりとりは行いません。
- 肖像権のある写真などを組み合わせてデザインすることもあり、取引先から「適切に情報管理を行ってほしい」と依頼されています。



ケース 3

個人経営に近い企業における役割とタスクの絞り込み

- 実質1名で事業を行っている場合、まず13の役割のうち自組織で実施すべき役割を絞り込みます（役割の絞り込みについては次ページを参照）。その上で、絞り込まれた役割に含まれるタスクについても、要員管理等の組織マネジメントに関するタスクは省くことが可能です。さらに、予めセキュリティ対策機能（監視等）が提供されているクラウドサービスを利用する等で、自分達でそれらの機能を調達することを省くことができます。一方で、顧客から預かった情報を適切に保護することなどは、企業の規模にかかわらず必要です。
- こうして絞り込まれたタスクについて、優先度を付けて実施します。



ケース 3

自組織で担うべき役割の明確化

ポイント
- 企業規模にかかわらず実施すべき役割を絞り込む
- セキュリティ対策が組み込まれたサービスを利用

個人経営的な企業であるC社の場合、予めセキュリティ対策機能（監視等）が提供されているクラウドサービスを利用する等の対策を通じて、個別の外部委託やその管理に関連するタスクを省くことができます。

ア）原則として自組織で担うもの

- 意思決定
- 戦略策定
- 戦略推進
- プロジェクト管理

レベル3以上の人材での対応が要求される

イ）セキュリティサービスの導入で代替するもの

- 対処
- 監視
- 運用管理

監視・対処等の機能を内包するSaaS型のクラウドサービスを利用

これらの役割に対する個別の人材確保は必須ではない

ウ）原則として外部委託で対応するもの

- 情報収集 分析・共有
- 脆弱性評価
- フォレンジック
- 法務
- 監査

必要に応じて外部委託を活用

本ケースでは実施しない

- 教育・訓練
- 設計開発
- 研究

必要な知識とスキルを個人で補うことを前提に、組織としての教育は実施しない

ケース 3

外部サービスで代替する機能の選定

- C社では、監視・対処等の機能を内包するSaaS型のクラウドサービスを利用するため、B社と比較して自社で直接担うべきタスクや必要な知識・スキルはより限定的になります。ただし、クラウドサービスが提供する監視結果やアラートを確認し、自社の業務への影響を判断するタスクは自社側に残ります。この前提のもと、フレームワークを使ってC社で必要となるタスクと知識・スキルを抽出しました。

役割	タスク（社内で担うべきもの）	タスク実施に必要な知識・スキル（抜粋）
 対処	● インシデントの可能性検知及び初動対応 ● 初動対応時におけるインシデントの速報の報告	● インシデントの初動対応に関する知識 ● インシデントの初動対応を実施するスキル ● インシデント速報の報告手順・対象に関する知識 ● インシデント対応措置及びその実施に関する知識 ● インシデント対処における法律等の規制要件に関する知識 ● インシデントの可能性がある場合に、適切な報告先へ報告するスキル ● 関係者と適切なコミュニケーションを行うスキル
 監視	● アラートの監視・調査・分析から不審な兆候を検知し、関係部署へ報告・通報 ● 検知した悪意のある挙動への初動対応	● インシデントの初動対応に関する知識 ● ツール（監視、ログ収集・分析）及びその手法に関する知識 ● 商用監視サービスに関する知識 ● インシデントの初動対応を実施するスキル ● サイバー攻撃や通信障害の可能性があるイベントを検知するスキル ● 収集したログが、機器障害か、不正なアクセスか誤使用によるアクセスであるのかを判別するスキル

※ C社の場合、SaaS型クラウドサービスが監視機能を提供しているため、自らツールを操作して監視を行うのではなく、サービスから提供されるアラートや監視レポートの内容を確認・理解し、不審な兆候を見落とさないようにする水準のスキルを想定しています。

ケース 3

個人経営に近い企業における役割とタスクの絞り込み

- 前ページの方針で絞り込むと、C社で実施するタスクは下表のようになりました。
- C社ではそれを踏まえて、表の右列のような優先順位を付けて実践しています。

役割から抽出されたタスク

戦略、方針、規定等の起案・承認
対策に必要な予算、リソースの確保
~~通常時・緊急時・復旧時に備えた体制の構築~~
コンプライアンス確保に関する指示
関係者とのコミュニケーションの実施
~~予算・人員等の調達・執行管理~~
~~大事管理~~
~~委託や管理の対象システムの選定~~
~~委託先の選定案、委託内容案の承認、契約締結~~
~~定期報告の参照~~
プロジェクトの立案、工程管理
~~委託内容の選定~~
~~委託先の選定~~
~~委託先のセキュリティ対策の統括~~
運用ルールの立案
情報管理
管理策の適用
自己点検チェックリストの作成
インシデント対処計画検討・承認
意思決定や予算検討に必要な情報を提供
自己点検チェックリストによる確認の実施

絞り込み

絞り込まれたタスク	優先順位
意思決定や予算検討に必要な情報を収集	1
戦略、方針、規定等の起案	2
対策に必要な予算、リソースの確保	3
コンプライアンス確保の実践	4
運用ルールの立案	5
情報管理	6
インシデント対処計画検討	7
管理策の適用	8
プロジェクトの立案、工程管理	9
関係者とのコミュニケーションの実施	10
自己点検チェックリストの作成	11
自己点検チェックリストによる確認の実施	12

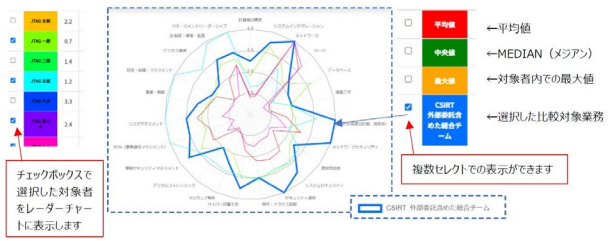
4．育成・確保における活用例

セルフアセスメントにより知識・スキルギャップを可視化することで、より効率的・効果的に人材育成・確保が図られる。

（効率的・効果的な育成モデル）

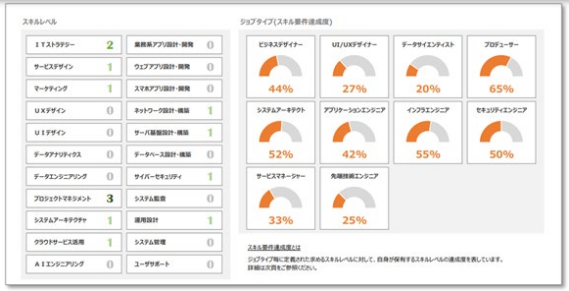
セルフアセスメント → 知識・スキルの可視化 → ギャップ解消に向けた育成

セキュリティ人材のスキル可視化ツール（JTAG財団VisuMe）



（出所）一般財団法人日本サイバーセキュリティ人材キャリア支援協会のプレスリリース「セキュリティ人材のスキル可視化ツール（VisuMe）がさらに進化」

デジタルスキルの可視化（東京都デジタルスキルマップ）



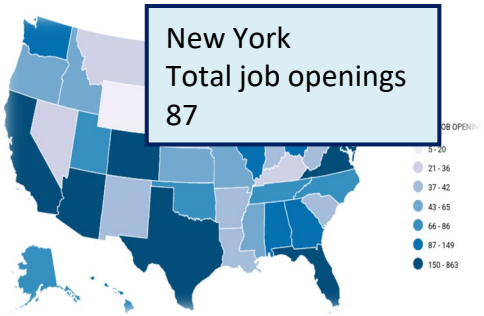
（出所）東京都「デジタルスキルマップによる戦略的人材育成」

海外における先行事例の紹介（米国Cyberseekの例）

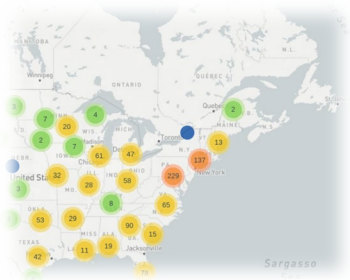
- 米国のCyberseekでは、NICEフレームワークに沿ったサイバーセキュリティ求人情報や教育サービスの検索が可能

（Cyberseek公式サイトにおける表示例）

求人数・採用要件（資格）の可視化　トレーニング情報の可視化



求人数を州単位でマップ表示



プロバイダー（研修事業者・大学等提供者）ごとにトレーニングセンター等の教育機関を地図上に可視化

（米）cyberseek：https://www.cyberseek.org/

おわりに／参考情報

- 本手引き書と併せて活用できる関連資料をご紹介します。
- フレームワーク本体や関連機関のガイドライン等のリンク集として、自組織のセキュリティ対策検討にご活用ください。

- 国家サイバー統括室「サイバーセキュリティ人材フレームワーク活用の手引き（プラス・セキュリティ向け）2026」（P.17～P.23等）
  - 本手引き書のケース1（P.33）では、小規模組織において特定の担当者に業務が集中するリスクを指摘し、各メンバーが既存業務に付加してセキュリティ業務を担うための方法として、本資料の活用を案内しています。セキュリティを主たる業務としない方が、自らの業務に必要なタスクや学習方法を把握する際にご参照ください。

- 独立行政法人情報処理推進機構（IPA）「中小企業の情報セキュリティ対策ガイドライン 第4.0版」（表紙、P16～17、P23より引用）（https://www.ipa.go.jp/security/guide/sme/about.html）
  - 本手引き書では、小規模組織が「やるべきこと」を検討する出発点として本ガイドラインを活用しています。具体的には、同ガイドラインが定める「重要7項目」及び「組織としての対策」をフレームワークの13の役割に対応付けることで、自組織に必要な役割とタスクを明確化する方法をケース1～3で解説しています（P.14等）。