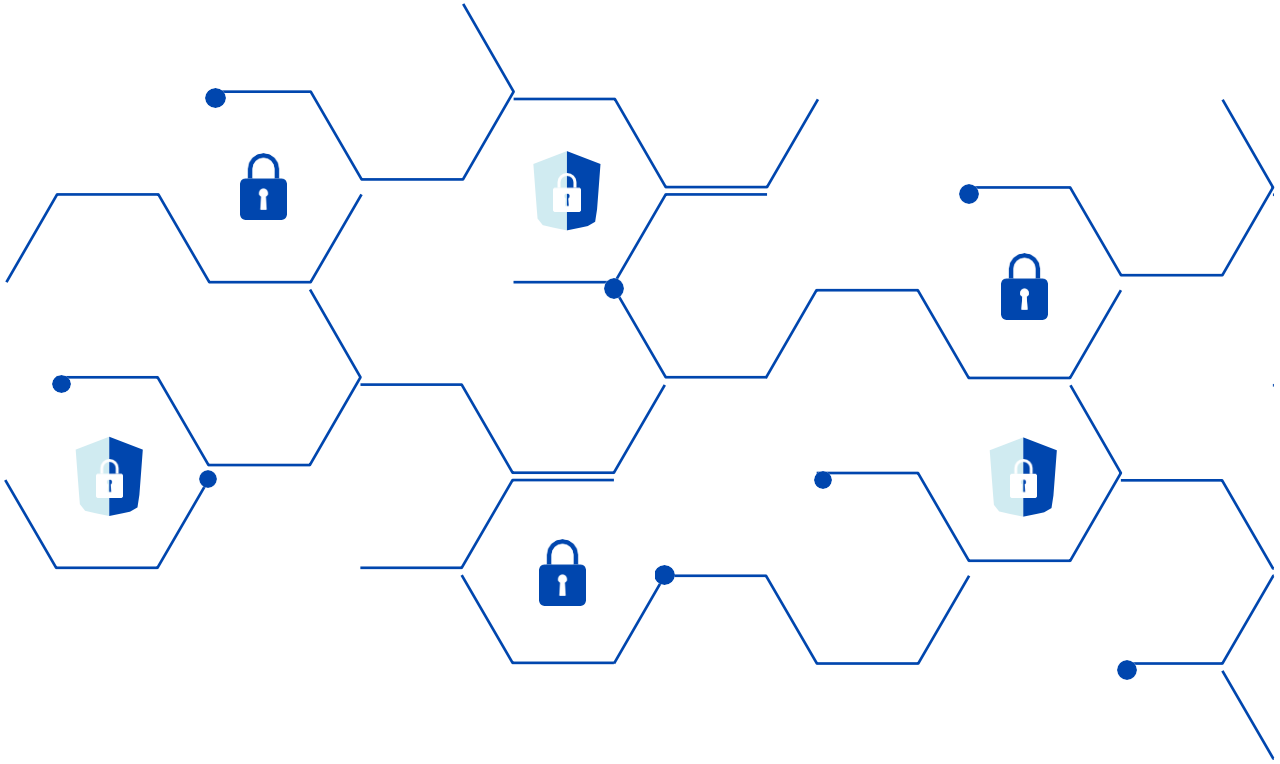
サイバーセキュリティ人材フレームワーク活用の手引き2026

個人（プラス・セキュリティ）向け



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、個人（プラス・セキュリティ）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、各個人における学習やキャリア形成、各組織における人材育成等を一律に義務づけるものではありません（各個人や各組織においては、自身の業務内容や組織の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、バックオフィス（総務・経理・人事等）やIT開発・運用など、サイバーセキュリティの専門業務ではないものの、自身の本来業務に関連してセキュリティの知識・スキル（プラス・セキュリティ）を習得し、活用しようとする個人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（個人（プラス・セキュリティ）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

プラス・セキュリティ向け事項

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

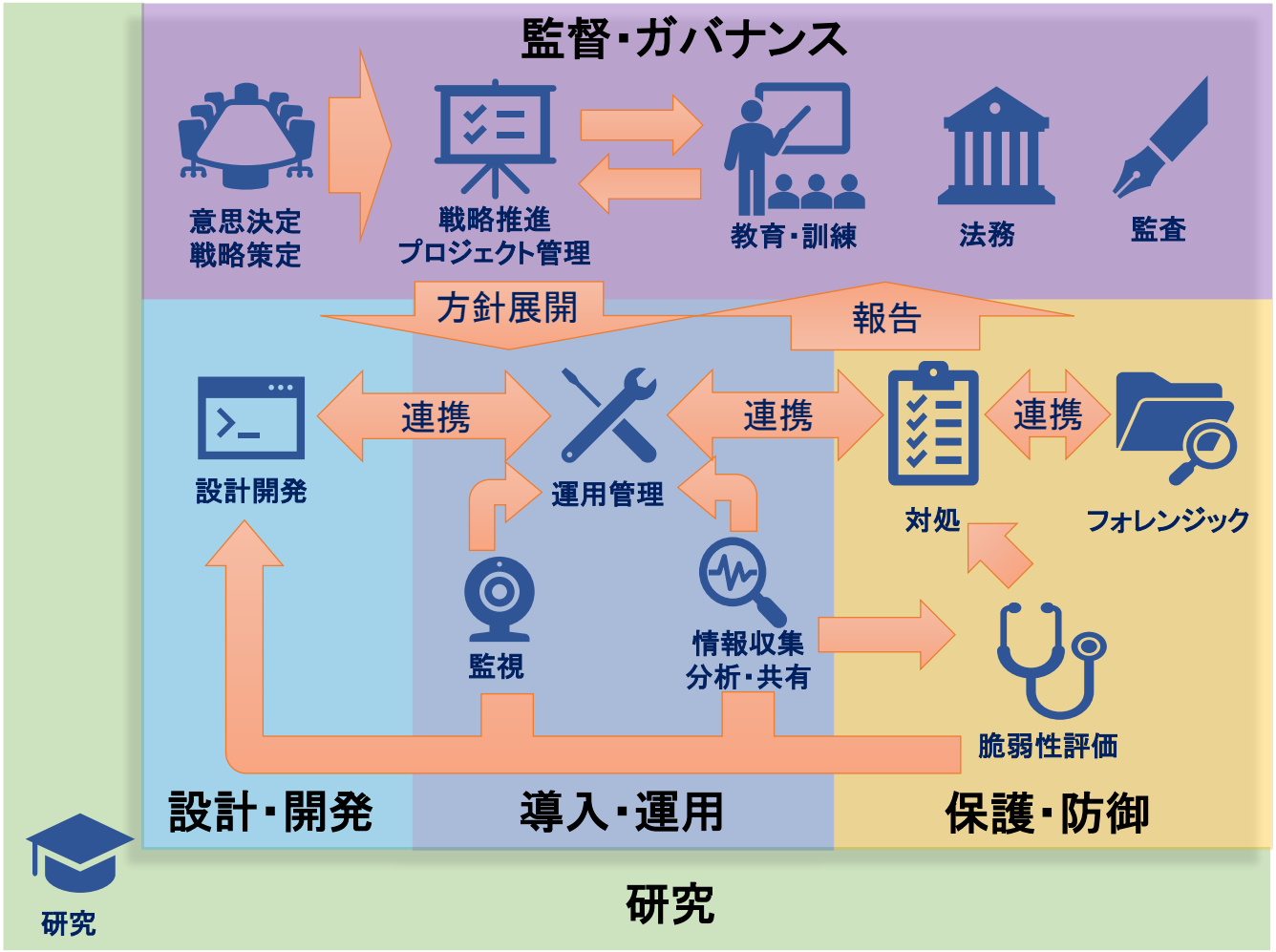
企業等　組織に必要な人材像を明確化し、採用・配置・育成等を計画的に進められる

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)

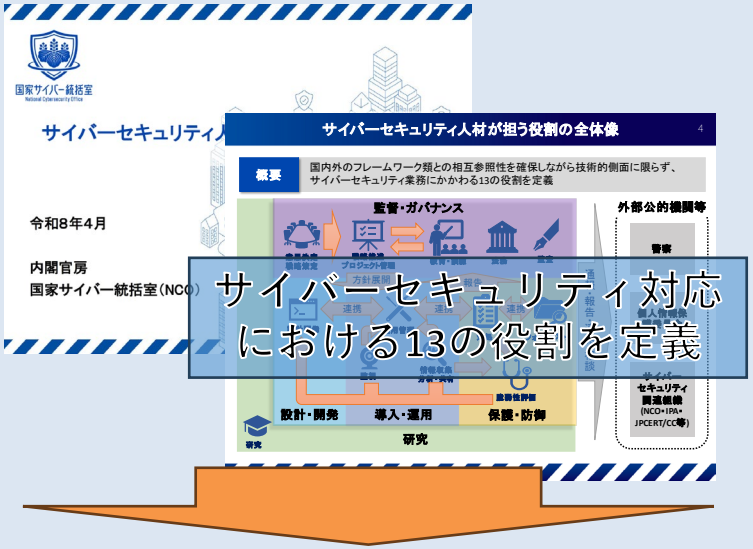
■TKSの考え方

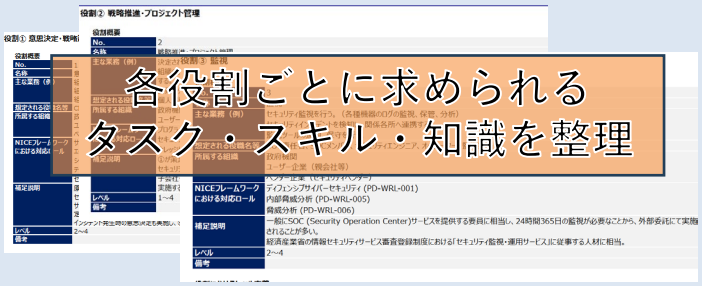
タスク(T)	● 本フレームワークで役割毎に定義しているタスク(T)とNICEフレームワークv2.1.0におけるタスクとの対応表を示す。 ● 原則として、本フレームワークで定義している1つのタスクについてNICEフレームワークのタスクが1つ以上対応するが、一部本フレームワーク独自のタスクが存在する。
知識(K)	● 本フレームワークで役割毎に定義している知識(K)とNICEフレームワークv2.1.0における知識との対応表を示す。 ● 原則として、本フレームワークで定義している1つの知識についてNICEフレームワークの知識が1つ以上対応するが、一部本フレームワーク独自の知識が存在する。
スキル(S)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

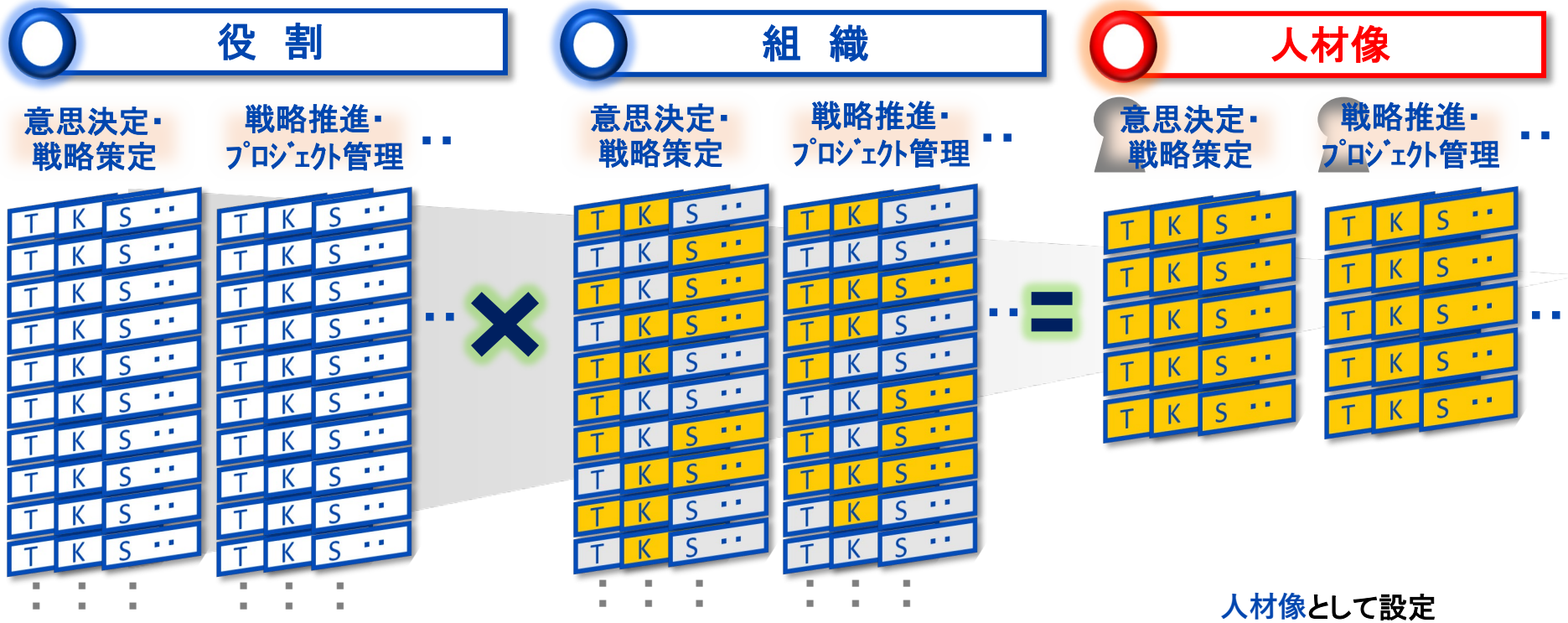
- 手引き書は各対象ごとに「主たる読者の属性」を想定し作成をしているものですが、主たる読者ではない属性の方も参考にしていただけるよう作成しておりますので、以下の対応表を参考にご利用ください。

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。



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			

個人（プラス･セキュリティ）向け
手引き書2026の全体構成

プラス・セキュリティとは？

- プラス・セキュリティとは、「自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと」を、「プラス・セキュリティ」と定義します。組織におけるあらゆる業務において必要となる考え方です。

なぜ今、「プラス・セキュリティ」が必要なのか？

- 組織のサイバーセキュリティ対策は、もはや「セキュリティ担当部署」による対応のみでは対処できません。組織におけるデジタル活用が進展する中で、一般的な事業活動においてもサイバーセキュリティリスクを意識した対応が欠かせなくなっているためです。
- 事業活動において、サイバーセキュリティの観点から不適切な対応を講じることで影響が懸念されるような業務を担っている人材にも、セキュリティに関する意識を養い、対策の実施に求められる知識・スキルを積極的に身につけてもらう必要があります。

サイバーセキュリティのタスクが必要となる例

クラウドを活用した新規事業を立ち上げるプロジェクトの企画担当者	サイバーセキュリティの知識が不十分な場合、目的にそぐわない不適切なクラウドを選定することや、シャドークラウド化（自社のサイバーセキュリティ担当者が把握していないクラウド）により、情報漏洩等のインシデントリスクが高まる恐れがあります。
製品設計において組込ソフトウェアの機能仕様を設計する担当者	サイバーセキュリティの知識が不十分な場合、製品にサイバー攻撃に対する脆弱性を生じさせる恐れがあります
自社の電話、インターネット設備、複合機等の保守契約を扱う総務担当者	サイバーセキュリティの知識が不十分な場合、不適切な設定のまま運用してしまうことで、当該機器を介した情報漏えいの原因となる恐れがあります

デジタルシステムの開発・運用を循環的に実施するDevOpsモデルでは、計画→設計→開発→テスト→デプロイ※→運用といった一連の流れにおいて、「システムアーキテクチャ」「デジタルプロダクト開発」「デジタルプロダクト運用」などの分野を担う担当者が、それぞれの場面でサイバーセキュリティ対策を実施することになります。なお、DevOpsに関しては、サイバーセキュリティ対策を実施することを強調した表現として、"DevSecOps"という表現も用いられています。

※デプロイ：ここではテスト済みのアプリケーション等のソフトウェアを実際の運用環境に導入・設定して利用可能にするプロセスの意味で使用しています。

出典：経済産業省、独立行政法人 情報処理推進機構（IPA）：『サイバーセキュリティ体制構築・人材確保の手引き第2版』（P26より引用）を基に作成
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

「プラス・セキュリティ」を正しく理解するポイント

- 「プラス・セキュリティ」の重要性に対して注目されるようになってから日が浅いこともあり、一部で誤解が生じやすい傾向にあります。
- 誤解しているままでは知識・スキルを習得する必要性が十分に理解できない可能性がありますので、本ページでプラス・セキュリティを正しく理解するための4つのポイントを確認しましょう。

ポイント①

「プラス・セキュリティ」人材という人材を別に確保する必要はない

前頁に例示したような業務に従事する人材が、サイバーセキュリティの知識やスキルを習得することが「プラス・セキュリティ」の取組に相当します。同様に、「プラス・セキュリティ」知識がこれまでのサイバーセキュリティ知識とは別に存在するわけではありません

ポイント②

「プラス・セキュリティ」は、DXに取り組んでいなくても必要

DXへの取り組みの有無に関わりなくITを活用して事業を行うすべての組織で必要です。

ポイント③

「プラス・セキュリティ」の取組は技術系以外でも必要

サイバーセキュリティに関する知識の中には、情報の保護方法と法律との関係、ステークホルダーからの信頼感醸成のための情報提供のあり方等、法務や広報のような技術系以外の業務に従事する人材においてもセキュリティ関連の知識・スキルが必要となる場面も存在します。

ポイント④

「プラス・セキュリティ」で求められる知識・スキルには高度なものもある

「プラス」の語感から付加的な印象を受けるかもしれませんが、「プラス・セキュリティ」の対象となる業務で求められるセキュリティの知識・スキルと、サイバーセキュリティの専門業務で用いられる知識・スキルとの間でレベルに明確な違いがあるわけではありません。どちらの業務においても、平易なものから高度なものまで幅広く活用します。

出典：経済産業省、独立行政法人 情報処理推進機構（IPA）：『サイバーセキュリティ体制構築・人材確保の手引き第2版』（P27より引用）を基に作成
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

個人（プラス・セキュリティ）向け手引き書2026の全体構成

- 本手引書ではバックオフィス(経理・総務・人事等)や営業等、サイバーセキュリティを専門業務としない個人が自身の本来業務に関連して必要となるセキュリティ知識・スキル(プラス・セキュリティ)を特定し、効果的・効率的に習得・実践していくためのステップを解説します。

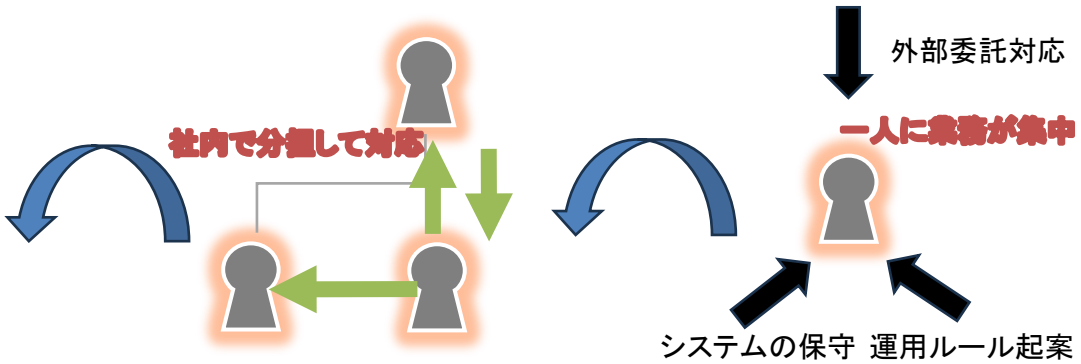
担当者の困りごと

現場担当

- 新しいクラウドサービス(SaaS)を業務で使いたいが、セキュリティリスクがわからない

バックオフィス担当

- 委託先の管理や契約時のセキュリティチェックをどう行えばよいか不安
- インシデント発生時に、専門部署へどう報告・連携すればよいかわからない



自身の業務とセキュリティの接点を明確にし、必要なタスク・知識・スキルを理解することが必要

STEP1

【自身の業務とタスク(T)の紐づけ】

日常業務やインシデント時の関わり方から、フレームワーク上の「タスク」を抽出・特定

STEP2

【知識・スキルの特定】

- 知識の例：個人情報保護法等の法規、リスクマネジメント
- スキルの例：アカウント・IDの適切な管理、専門家とのコミュニケーション

個人の実践(セルフアセスメントと学習)

① 目標と現状のギャップ分析(セルフアセスメント)

抽出した知識・スキルをもとに、「業務で求められる目標レベル」と「現在の自分のレベル」を比較し、優先的に補強すべき要素を客観的に把握。

②ギャップを埋めるための学習計画と実践

対策の例：情報セキュリティマネジメント試験等の資格取得を通じた体系的な学習、CYDER、プレCYDERなどの実践的な研修の受講、社内ルールの再確認など。

個人（プラス・セキュリティ）向け手引き書の内容

ポイント　セキュリティはすべての人の必須素養。本来業務の付加価値を高める第一歩！

- プラス・セキュリティでどのような知識・スキルが必要かは、皆さんが担当している業務（扱う情報や機器など）によって異なります。後半のケーススタディ等をご覧いただき、自身の業務とセキュリティの接点を知った上で、セルフアセスメントを通じて現在の状況を踏まえた学習方針を考えてみてください。
- 本手引き書は次のようなコンテンツで構成されています。

Contents1

業務に付加すべき知識・スキル

- バックオフィス（総務・経理・人事）、IT開発・運用等の具体的な職種ごとに、普段の業務にどのようなセキュリティの業務があるかを解説します。
- フレームワークを用いて、**それぞれの業務で優先して身につけるべき知識・スキル（TKS）を抽出する考え方**を示します。

Contents2

セルフアセスメントと学習方法

- フレームワークや簡易チェックリストを用いて、**自身の現在の知識・スキルの保有状況（強み・不足）を客観的に把握する手順**を説明します。
- 不足している知識を補うための身近な学習ツールや、情報セキュリティマネジメント試験などの目標となる資格を活用した具体的な学習ステップを提示します。

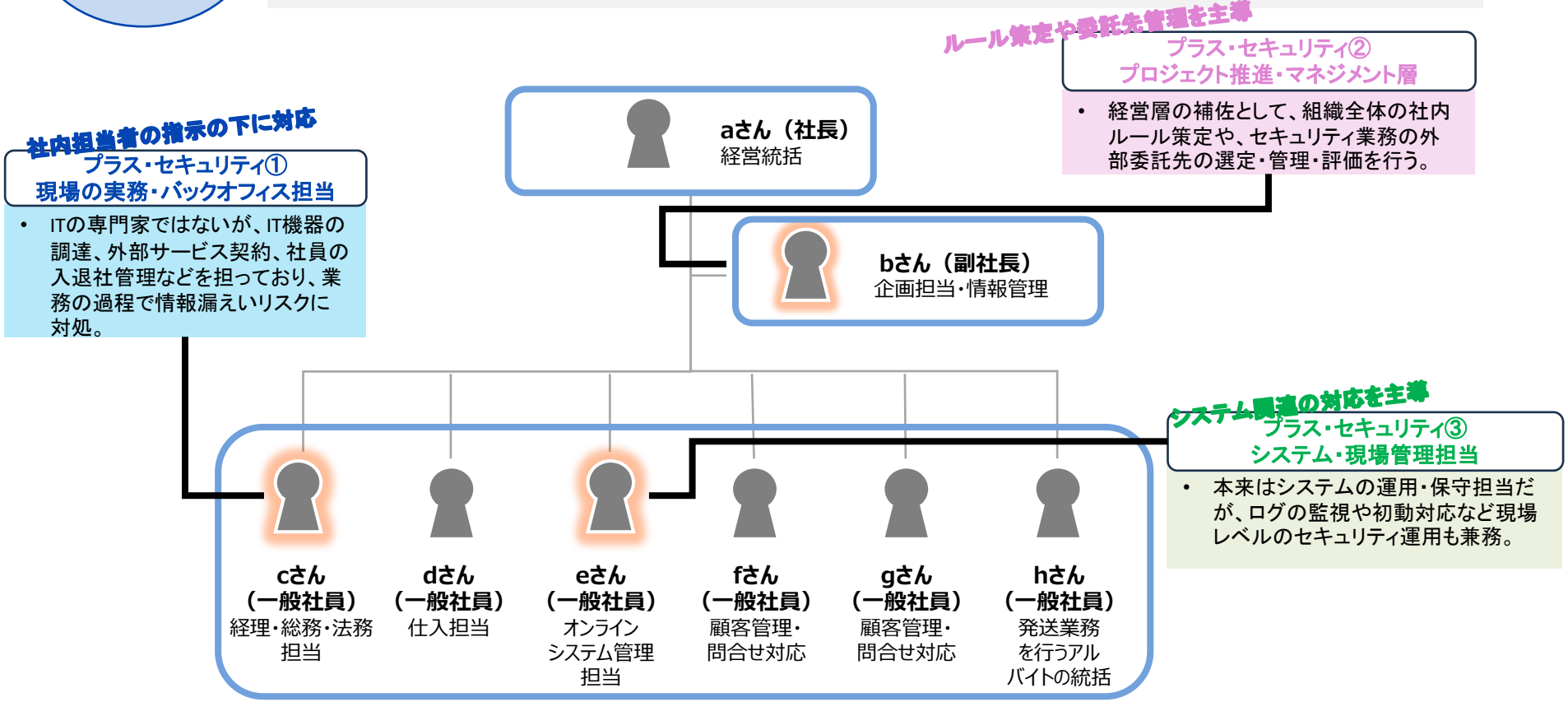
業務に付加すべきセキュリティ知識・スキル

プラス・セキュリティの具体例

- 組織のセキュリティは、一部の専門家だけではなく、さまざまな立場の従業員が連携することで守られます。ここではモデル企業（A社）を例に、社内のどのようなポジションの人が、どのようにセキュリティに関わるのか（あるいは外部専門家と連携するのか）の全体像を示します。

A社
従業員8名

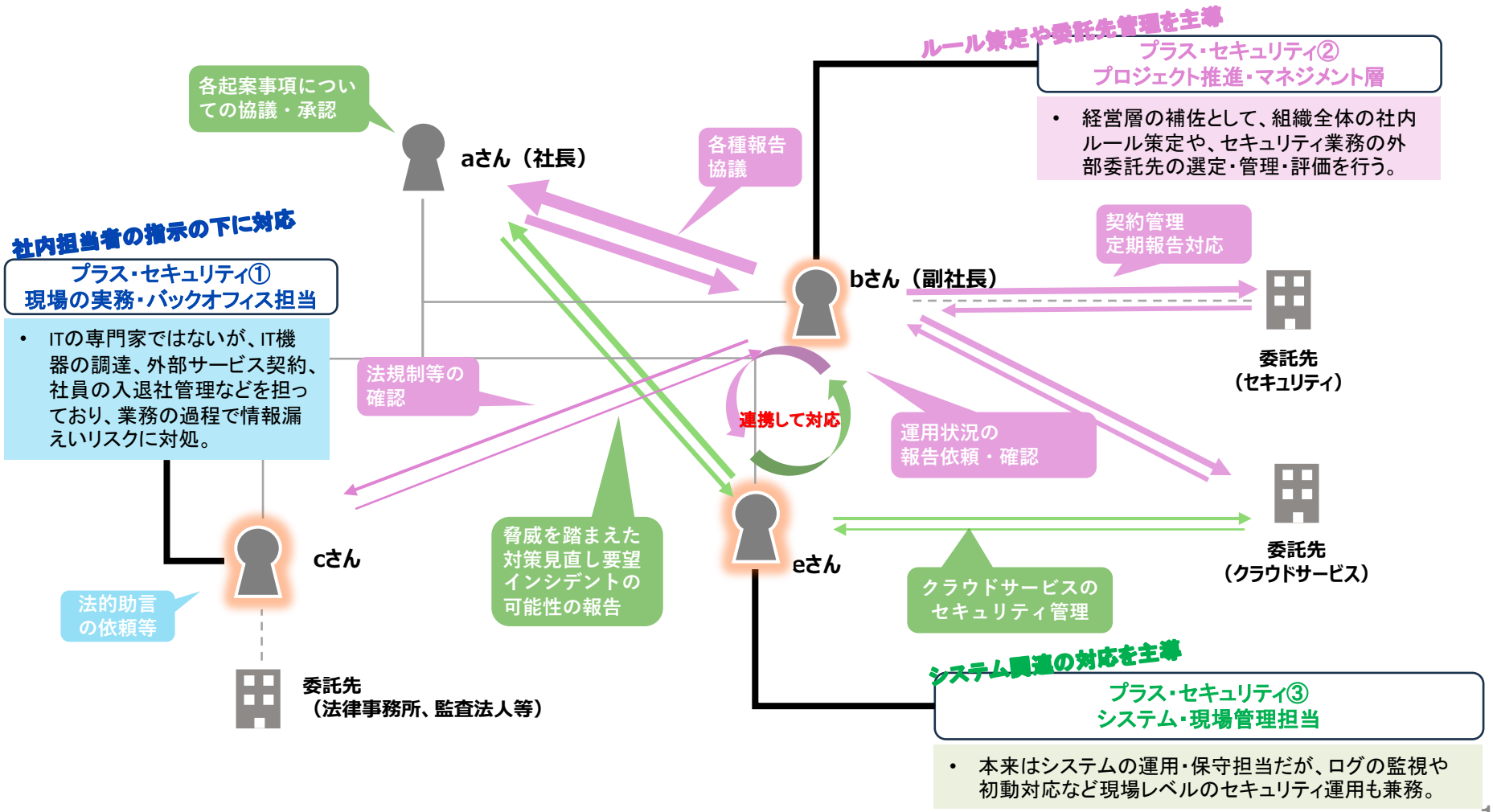
- 地場産品を直売するオンラインショップを運営しています。最近はふるさと納税の返礼品としての発送もあり全員が何かと忙しく働いています。
- オンライン販売はECモール事業者が用意する環境を使っており、セキュリティ対策もECモールに委ねています。それ以外に自社の経営情報をクラウドで管理していますが、対策が十分とはいえません。
- BtoC形態であるため、一般消費者とのやりとりもあります。



※ 本手引き書では「個人の視点」からプラス・セキュリティに関する各従業員の役割やタスクを解説しています。企業における組織全体としてのセキュリティ体制構築に向けたステップや、各役割へのタスク割り当ての考え方については、『**小規模組織向け手引き書**』をご参照ください。

プラス・セキュリティの具体例

- ご自身が「プロジェクト推進・マネジメント層（bさん）」「現場の実務・バックオフィス担当（cさん）」「システム・現場管理担当（eさん）」のどの立場に近いかをイメージしながら、平時やインシデント発生時の関わり方を確認してみましょう。



プラス・セキュリティ①：cさん（一般社員）経理・総務・法務担当

- 総務や経理、法務などのバックオフィス部門の担当者は、IT機器やサービスの調達、社員の入退社管理、外部委託先との契約などを通じて情報漏えいリスクに対処する重要な役割を担います。
- バックオフィス担当者が業務遂行の過程で意識し、実践すべきセキュリティ関連のタスクと、必要になりうる知識・スキルを整理します。高度な実務は外部の専門家に委託しつつ、緊急時の際には自社と外部をつなぐ窓口としての対応も求められます。

業務内容

バックオフィス業務の中でIT資産管理や契約管理等を実践（社内担当者の指示の下に対応）

通常業務ではIT機器やSaaSの調達、外部委託時の秘密保持契約等の締結サポート、社員の入退社に伴うアカウント管理等を担当。インシデント発生時には外部専門家（弁護士等）への連絡や法的助言の社内展開を実施。

運用管理

法務

教育・訓練

分類	内容
タスク	プロジェクトで使用する機器等の調達及びサプライチェーン管理
	ユーザーアカウント・権限管理
	教育・訓練内容の計画
	組織外の関係者対応（訴訟対応等含む）
	法的リスク（平素及びインシデント発生時）の分析と評価
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
	サイバーセキュリティに関する法律についての知識（個人情報保護法など）
	アカウント管理に関する知識
	調達先のリスクの特定、評価に関する知識
	外部関係者対応において必要となる知識
スキル	組織のポリシーや計画に沿ってアカウント・IDを管理するスキル
	調達先のリスクを分析し、判断するスキル
	関係文書や対象サービス等を法的観点から正確に理解するスキル
	関係者（親会社、所管官庁、取引先、外部専門家等）と適切なコミュニケーションを行うスキル
	法的事項や技術的事項を、専門家および非専門家に対して分かりやすく口頭で説明し、理解を促すスキル

自身が実施

社内関係者の指示のもと、自身が実施するタスク・知識・スキル

社内関係者の指示下で支援

社内の関係者をサポートとして実施する業務に関するタスク・知識・スキル

プラス・セキュリティ②：bさん（副社長）企画担当・情報管理

- 経営層の補佐やプロジェクト推進の責任者bさんは、組織全体のセキュリティルールの策定や、セキュリティ業務の外部委託先の選定・管理・評価（委託先管理）といった重要なマネジメント業務を行います。
- **「自組織で実施・保有すべき知識・スキル」と「外部の専門家に委託し、その結果を適切に評価・判断するために必要な知識・スキル」の境界線を把握しておくことが重要**です。

業務内容

戦略・ルールの推進と、委託先管理等のマネジメントを実践（ルール策定や委託先管理を主導）

通常業務では、セキュリティ戦略・方針の起案、自己点検の実施、外部委託先の選定や委託先管理を担当。インシデント発生時には、現場（eさん等）からの速報を受けたトリアージ（初期評価・優先順位付け）の判断、委託先への調査指示、および対外的な窓口（広報対応・関係機関への連絡など）を主導

戦略推進
プロジェクト管理

対処

意思決定
戦略策定

法務

教育・訓練

分類	内容
タスク	通常時・インシデント発生時の運用ルールの起案
	委託先の選定及び委託内容の調整
	プロジェクト運用時における情報管理及びセキュリティ管理策の適用
	インシデントに対する初期評価・トリアージ
	サイバーセキュリティに関する関係者とのコミュニケーション
	ログ分析 / 不審な兆候の検知と通報
	脆弱性評価・ペネトレーションテストの実施
	取得対象データの保全・収集およびデータの解析と評価
知識	リスクマネジメントに関する知識
	商用サイバーセキュリティサービスに関する知識（委託先の選定に必要）
	組織のサイバーセキュリティ体制、機能及び役割に関する知識
	サイバーセキュリティ対策の最新動向に関する知識
	監視ツール、脆弱性診断ツール、フォレンジックツール等に関する専門知識
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
	調達先（委託先）のリスクを分析し、判断するスキル
	自組織内/外から収集した初期調査結果をもとに、事業継続を目的に何の対応を優先すべきかを判断するスキル（トリアージ）
	関係者と適切なコミュニケーションを行うスキル（社内外のステークホルダーとの折衝）
	分析ツールを使用してログ分析を実施するスキル
	機器で行われた操作等を評価し、サイバー攻撃や不正行為を特定・究明するスキル

自身が主導

実務として手を動かし、あるいは判断を下すために直接保有しておくべきTKS

外部に委託

ベンダーからの提案や報告書（レポート）を読み解き、妥当性を判断

プラス・セキュリティ③：eさん（一般社員）オンラインシステム管理担当

- 情報システムの運用保守を担当する人材は、システムの安定稼働だけでなく、日常的なログの監視や権限管理などを通じて、組織のセキュリティを維持する重要な役割を担います。
- ここでは、情報システム運用保守担当者が本来業務に付加して実施すべきセキュリティ関連のタスクと、必要になりうる知識・スキルは、「通常業務との関係」や「インシデント発生時」等の場面に応じて整理されるため、**すぐに使う場面はなくとも「いざという場面では必要なスキル」も存在します。**

業務内容

システム運用・保守を担当し、業務の中でログ確認等を実践（システム関連の対応を主導）

通常業務では社内システムの運用保守を担当。ログ等の監視や、必要な脅威情報の収集等も実施。インシデント発生時には対処を実施。

情報収集
分析・共有

運用管理

監視

対処

分類	内容
タスク	ログの収集・分析
	アラート監視による不審な兆候の検知と関係部署への報告
	社内システムの定期メンテナンスの実施
	システム・ネットワーク機器のアップデートおよびバックアップ管理
	ユーザーアカウントおよび権限の管理
	システムやネットワークにおけるイベントの検知
	セキュリティの脅威に関する情報の収集と分析
知識	各種セキュリティログ（システムログ、アプリケーションログ等）
	システム監視・ログ分析ツールとその手法
	社内システムの運用・保守
	サイバー攻撃や最新の脅威・脆弱性
	脅威情報を収集・分析するためのツールやプロセス
スキル	分析ツールを適切に活用してログ分析を実施
	ログから「機器の障害」か「不正アクセス」かを正確に判別
	監視ツールを用いてシステムの異常や不審なイベントを検知
	イベントやインシデント検知時に、手順通りに迅速に対処・報告
	社内システムのパフォーマンス低下やトラブルに対処し、保守
	収集した脅威情報を分析し、自社システムに影響を与えるリスクを特定

通常業務と並行して実施

普段実施する業務に必要なタスク・知識・スキル

通常時に外部委託で実施

コミュニケーションを取るために必要なタスク・知識・スキル

インシデント時等に自分で実施

緊急時に対応するとともに、緊急時に備えて知識・スキル習得が必須

インシデント発生時等に委託

緊急時にコミュニケーションを取るために必要なタスク・知識・スキル

その他の関連する担当者（人事・広報等）

- 人事や広報部門の担当者は、セキュリティシステムの運用などの技術的な実務を直接行わないことが多いです。しかし、平時における「人材の採用・評価」「社外への取り組みのアピール」、緊急時における「対外的な発表（プレスリリース）」や「社内対応」など、組織のセキュリティ体制を支え、信頼を維持するための重要な周辺業務を担っています。
- ここでは、人事・広報的な役割がサイバーセキュリティとどのように結びつくのか、その視座を整理します。

人事

人材の採用・配置・評価（人事）

- 組織に必要なセキュリティスキルを持った人材の採用計画のサポート。
- セキュリティ教育の受講状況や、ルールの遵守状況を確認。

社内対応（人事）

- 全社的な緊急連絡網の運用サポート。

広報

組織の取組の社外発信（広報）

- 自社が実施しているセキュリティ対策（「SECURITY ACTION」の宣言や各種認証の取得など）をウェブサイトや会社案内等で対外的に発信。

対外的な窓口・発表（広報）

- 経営層（aさん・bさん等）や外部専門家と連携し、インシデントの発生事実や影響範囲、今後の対応等について、顧客、取引先、報道機関に対して正確かつ迅速に発表（プレスリリース・謝罪等）を行う。

社内関係者と連携して対応

対外的に発信する内容の正確性等のヒアリング

現場で求める人材像をヒアリングして採用要件を検討

採用計画や人材育成方針をすり合わせセキュリティ教育の計画を策定

認証取得のプレスや、顧客・報道機関へ発表する内容とタイミングの意思決定を仰ぐ。

社員の入退社時のアカウント管理セキュリティ研修の受講状況を共有・管理

外部有識者へのリーガルチェック等を依頼

cさん（一般社員）
経理・総務・法務担当

プラス・セキュリティ①

- ITの専門家ではないが、IT機器の調達、外部サービス契約、社員の入退社管理などを担っており、業務の過程で情報漏えいリスクに対処。

bさん（副社長）
企画担当・情報管理

プラス・セキュリティ②

- 経営層の補佐として、組織全体の社内ルール策定や、セキュリティ業務の外部委託先の選定・管理・評価を行う。

eさん（一般社員）
オンラインシステム管理担当

プラス・セキュリティ③

- 本来はシステムの運用・保守担当だが、ログの監視や初動対応など現場レベルのセキュリティ運用も兼務。

その他の関連する担当者（開発担当）

- システムやアプリケーションの開発を担当する人材は、設計・実装段階でセキュリティ上の脆弱性を作り込まないようにする重要な役割を担います。システム開発の工程においてもセキュリティを意識した対応が不可欠です。
- ここでは、開発担当者がサイバーセキュリティとどのように結びつくのか、その視座を整理します。

開発担当

セキュリティ要件の確認と実装（開発）

- システムの要件定義・設計段階で、セキュリティ要件（認証・認可、入力検証、暗号化等）が適切に組み込まれているかを確認。
- 開発で使用するライブラリやOSSの脆弱性情報を確認し、安全な部品を選定。

脆弱性対応（開発）

- 自社開発のシステムに脆弱性が発見された場合、影響範囲の調査と修正パッチの開発・適用を実施。
- セキュリティ専門部署やCSIRT等と連携し、脆弱性の技術的な詳細を説明。

社内関係者と連携して対応

使用ライブラリの調達確認

cさん（一般社員）
経理・総務担当

プラス・セキュリティ①

- 使用するOSSやライブラリのライセンス確認、外部開発委託時の契約・調達面での連携

セキュリティ要件の 確認・相談

bさん（副社長）
企画担当・情報管理

プラス・セキュリティ②

- 新規開発案件でのセキュリティ要件の確認、セキュリティ方針に基づく開発ルールの整合性確認

脆弱性発見時の技術的な連携

eさん（一般社員）
オンラインシステム管理担当

プラス・セキュリティ③

- 開発したシステムのリリース前のセキュリティ確認、脆弱性発見時の技術的な連携・情報共有

セルフアセスメントと学習方法

フレームワークで定義する「役割」の確認

- 本フレームワークでは、セキュリティ対策に求められる「13の役割」が定義されています。プラス・セキュリティ人材は、これらの役割を完全に担うわけではありません。
- 以下の質問に回答することで、自身にもっとも近い担当者像を特定し、関連性の深いタスクを確認してみましょう。特定した担当者像をもとに、次ページ以降のセルフアセスメントへ進み、自身の知識・スキルのギャップ分析と学習計画の策定を行います。

Case1：通常業務との関わり方

Q. あなたの主な担当業務は、現場のITシステムの開発・運用・保守ですか？ それとも非IT部門（バックオフィスや事業企画など）ですか？

Q.【ITシステム担当者向け】日常的な業務の中で、以下のような作業を行っていますか？（複数該当あり）

- ネットワークやPC・ソフトウェアの設定、アップデート、バックアップ作業
- システムのログの確認
- 不審なアクセスや異常の確認

Q.【非IT部門向け】あなたの業務において、以下のような関わりはありますか？（複数該当あり）

- IT機器・SaaSの調達手続き
- 外部委託時の秘密保持契約（NDA）締結のサポート
- 社員の入退社に伴うアカウントの登録・削除
- セキュリティルールの周知・教育

- 組織全体の社内ルール作り
- 外部委託先の選定・評価（委託先管理）

Case2：インシデント時の関わり方

Q. 万が一、サイバー攻撃や情報漏えいなどのインシデントが発生した際、あなたは呼び出されてどのような対応を求められますか？

- 取引先や顧客、報道機関に対する対外的な発表（広報対応）
- 社内の緊急連絡網の運用

- 外部の専門家（弁護士や警察等）への連絡や相談の窓口

- 異常を検知した際、一時的なネットワーク遮断などの初動対応

- インシデントの初期評価（トリアージ）や対応の優先順位付けを判断
- 外部委託先への調査指示など対応全体を主導

セルフアセスメントの実施方法

- 前頁で特定したタスクをもとに、人材フレームワークを活用して「現在の自分」と「業務で求められる姿」のギャップを客観的に自己評価し、優先的に学習・補強すべき知識・スキルを特定し、対策します。

STEP1
フレームワークから、**自身の担当業務に合致するタスク・知識・スキルをピックアップ**

Point
タスクに紐づく知識・スキルを抽出

STEP2
抽出したTKSリストに対して、**「現在の保有レベル（自己評価）」と「業務上求められる目標レベル」を判定**

Point
現在地ではなく、
目標となるレベルから逆算

STEP3
目標レベルと現在レベルの差分（ギャップ）を比較し、**今後のステップアップに向けた計画を策定**

Point
手段先行ではなく、
ギャップを埋める手段を選択

	知識・スキル		
一般社員のタスク 日常業務におけるセキュリティルールの遵守、不審なメールや事象の早期発見と報告	【K】組織のセキュリティポリシーに関する知識、インシデントの初動対応（報告手順）に関する知識	【T】目標Lv2（専門家の指示下で確実に行う）⇒ 現在Lv1（サイバー分野のリスクは認識不足） 目の前の業務の実施には？ 【K】知識なし⇒目標Lv1（基礎知識獲得） 【S】スキルなし ⇒目標Lv1（専門家の指示下で対応）	クラウドサービス導入時などに指示を理解するスキルが不足 社内の専門家の指示を正確に理解し支援する「共通言語」を習得すべく、情報セキュリティマネジメント試験の学習を開始
プロジェクト推進担当のタスク 新規事業やシステム導入時のセキュリティ要件の組み込み、部門内のルール徹底、外部委託先の選定	【K】プロジェクト管理におけるリスクマネジメントに関する知識、コンプライアンスの原則 【S】関連部署（IT部門等）との調整・コミュニケーションスキル	【T】現在Lv2（報告を受け入れるのみ）⇒目標Lv3（独力でマネジメント） マネジメントに必要なのは？ 【K】現在Lv1（キーワードは分かる）⇒目標Lv2（委託先と会話可能） 【S】現在Lv1（委託先の選定等は独力で難しい）⇒目標Lv2（委託対応が可能）	委託先ベンダの技術力等を適切に判断する専門知識の不足 ベンダーを適切に管理・評価するための「サイバーセキュリティ概論」や「リスクマネジメント」の知識を補うため、マネジメント層向けのセキュリティ研修を受講
システム運用担当者のタスク 日常業務におけるセキュリティルールの遵守、不審なメールや事象の早期発見と報告	【K】ネットワークやクラウドの基礎知識 【S】アクセス制御・バックアップの運用スキル、委託先とのコミュニケーション・評価スキル	【T】目標Lv3（独力遂行）⇒ 現在Lv2（マニュアルや他者の支援が必要） 独力遂行に必要なKSは？ 【K】現在Lv1（用語を知っている程度）⇒目標Lv2（指示下で理解） 【S】現在Lv1（やり方がわからない・自己流）⇒目標Lv3（独力遂行）	インシデント発生時の対応スキルの目標のギャップが大きい スキルには知識の充足も必要 「初動対応力」と「異常検知スキル」を急務で補強するため、実践的な研修（CYDER、プレCYDER等）を受講

ギャップを埋めるための考え方の例

- セルフアセスメントで特定されたギャップのうち、法規制・リスクマネジメント・アカウント管理・脅威/脆弱性等に関する知識が不足している場合は、資格試験の学習、書籍、eラーニング等が有効です。体系的に知識を整理し、習得度を客観的に確認できます。
- インシデント時の初動対応・ログ分析・対外連絡・トリアージ判断等、実際に手を動かしたり判断を下す場面で必要なスキルが不足している場合は、演習型の研修が有効です。

		ギャップの例	対応策の例
一般社員のタスク 日常業務におけるセキュリティルールの遵守、不審なメールや事象の早期発見と報告	**知識**	サイバー分野のリスク認識不足、法規制の知識不足	ITパスポートでリスク管理やBCP/BCMの基礎を学習
	スキル	インシデント時の社内外連絡・対外発表の対応力不足	セキュリティインシデント対応机上演習教材、ロールプレイング演習
プロジェクト推進担当のタスク 新規事業やシステム導入時のセキュリティ要件の組み込み、部門内のルール徹底、外部委託先の選定	**知識**	委託先管理・評価の判断力不足	ITパスポート試験の調達計画・実施を学習。
	スキル	トリアージ判断・初動対応の実践力不足	CYDER、プレCYDER等、ロールプレイング演習
システム運用担当者のタスク 日常業務におけるセキュリティルールの遵守、不審なメールや事象の早期発見と報告	**知識**	ネットワーク・クラウドの基礎知識不足	ITパスポート試験のネットワーク方式、通信プロトコル、ファイルシステムから学習
	スキル	初動対応力・異常検知スキル不足	CYDER、プレCYDER（実践的演習）

ITパスポート試験の活用

- コンピュータやネットワーク等のITの基礎知識が不足していると感じる場合は、セキュリティの学習に先立って、**ITパスポート試験**等の学習を通じて基礎的なIT知識を習得することが有効です。
- ITパスポート試験のシラバスでは、セキュリティの基礎概念（中分類23：セキュリティ）、ネットワークの基礎（中分類22：ネットワーク）、関連法規（中分類2：法務「5. セキュリティ関連法規」）、リスクマネジメントやBCP（中分類1：企業活動「1.(2) 経営管理」）等が体系的に整理されており、プラス・セキュリティとして求められる知識の土台を効率的に習得できます。
- ITパスポートを通じてオペレーティングシステム等、サイバーセキュリティの学習のみでは身につかないIT関連の知識を補うことにもつながります。

ITパスポート試験と知識の対応例

プラス・セキュリティの知識の例	ITパスポート シラバスの対応分野	内容
サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識	中分類23：セキュリティ「61. 情報セキュリティ」	情報セキュリティの概念、脅威と脆弱性（人的・技術的・物理的脅威）、代表的な攻撃手法
リスクマネジメントに関する知識	中分類23：セキュリティ「62. 情報セキュリティ管理」	リスクアセスメント、ISMS、情報セキュリティポリシー、機密性・完全性・可用性
適切なセキュリティ対策の設定方法に関する知識	中分類23：セキュリティ「63. 情報セキュリティ対策・実装技術」	人的・技術的・物理的対策、暗号技術、認証技術、利用者認証、公開鍵基盤
サイバーセキュリティ関連法規・組織内のポリシー・関連計画に関する知識	中分類2：法務「5. セキュリティ関連法規」	サイバーセキュリティ基本法、不正アクセス禁止法、個人情報保護法、GDPR
ネットワークインフラストラクチャに関する知識	中分類22：ネットワーク「58. ネットワーク方式」「59. 通信プロトコル」	LAN/WAN、TCP/IP、HTTP/HTTPS、ルーター、ファイアウォール
情報システムのバックアップに関する知識	中分類17：ソフトウェア「46. ファイルシステム」	ファイル管理、バックアップ、世代管理
インシデント対応計画の策定に関する知識	中分類1：企業活動「1.(2)経営管理」	BCP、BCM、リスクアセスメント
調達とサプライチェーンに関する知識	中分類7：システム企画「24. 調達計画・実施」、中分類3「12. 経営管理システム」	RFI/RFP、調達の流れ、SCM
監査プロセスに関する知識	中分類12：システム監査「31. システム監査」「32. 内部統制」	システム監査の目的と流れ、内部統制、ITガバナンス

＋ その他一般的なIT関連知識

情報セキュリティマネジメント試験の活用

- 「プラス・セキュリティ」として求められる知識やスキルを体系的に学び、その習得度を客観的に把握・証明するための手段として、公的な資格試験や検定の活用が有効です。
- そのうち、「**情報セキュリティマネジメント試験**」の出題範囲と、本フレームワークで定義する関連知識・スキルとの対応関係を示します。

情報セキュリティマネジメント試験の出題範囲と関連する知識・スキル

出題分野	出題内容の例	区分	知識・スキル	関連する役割
情報セキュリティ全般	機密性・完全性・可用性、脅威、脆弱性、サイバー攻撃手法 など	知識	サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識	③監視 ⑤情報収集・分析・共有
		スキル	様々な情報源から脅威や攻撃の特性に関する知識を収集し、監視対象を決定するスキル	③監視
情報セキュリティ管理	情報資産、リスク、ISMS、インシデント管理などの各種管理策、CSIRT など	知識	インシデント対処の手順に関する知識	⑧運用管理
		スキル	インシデントの初動対応を実施するスキル	③監視
			インシデント対処を実施するスキル	⑧運用管理
情報セキュリティ対策	マルウェア対策、不正アクセス対策、情報漏えい対策、アクセス管理 など	知識	アクセス制御に関する知識	⑧運用管理
			適切なセキュリティ対策の設定方法に関する知識	
		スキル	ハードウェア、ソフトウェア、基幹システム等に適切なセキュリティ対策を設定するスキル	⑧運用管理
情報セキュリティ関連法規	サイバーセキュリティ基本法、個人情報保護法、不正アクセス禁止法 など	知識	サイバーセキュリティ関連法規・組織内のポリシー・関連計画に関する知識	③監視 ⑤情報収集・分析・共有
テクノロジ（関連分野）	ネットワーク、データベース、システム構成要素	知識	ネットワークインフラストラクチャに関する知識	⑧運用管理
			データベース構築・運用に関する知識	
		スキル	組織のポリシーに沿ったネットワークを構成するスキル	⑧運用管理
マネジメント（関連分野）	システム監査、サービスマネジメント、プロジェクトマネジメント	知識	情報システムの変更管理・構成管理に関する知識	⑧運用管理
		スキル	組織のネットワークシステムや情報システムに関する構成管理を実施するスキル	⑧運用管理
ストラテジ（関連分野）	経営管理、システム戦略、システム企画	知識	システムの要件定義・仕様策定に関する知識	⑧運用管理
		スキル	組織の要請を集約し、情報システムの要件定義・仕様を策定するスキル	
科目B（実践力）	業務の現場における具体的な取組み（リスクアセスメント、委託先管理等のケーススタディ）	知識	トラブルが発生した際の対応手順に関する知識	⑧運用管理
		スキル	情報システムのパフォーマンス低下やトラブル発生時に、原因を追究し解決するスキル	⑧運用管理
			通常時及びインシデント発生時の運用ルールを策定するスキル	③監視 ⑤情報収集・分析・共有 ⑧運用管理

研修の活用

- P.26のセルフアセスメント（STEP3）で特定した不足知識・スキルのうち、特に実践的なスキル（演習・体験を通じて習得するもの）については、以下の研修の活用が有効です。ご自身に最も近い担当者（bさん・cさん・eさん）の例を参考に、受講を検討してください。

強化するTKSの例

bさん（副社長）
企画担当・情報管理

分類	内容
タスク	セキュリティ対策に必要な予算等のリソース確保
	インシデントに対する初期評価・トリアージと対応指示
知識	リスクマネジメントに関する知識
	サイバーセキュリティに係る予算管理とコスト評価に関する知識
	インシデント対処手順に関する知識
スキル	費用対効果を踏まえて必要な投資を判断するスキル
	初期調査結果をもとに事業継続を目的に何の対応を優先すべきかを判断するスキル

cさん（一般社員）
経理・総務・法務担当

分類	内容
タスク	組織外の関係者対応（対外発表等）
知識	インシデントレポート共有の手順・対象に関する知識
スキル	関係者（社内外・報道機関等）と適切なコミュニケーションを行うスキル

eさん（一般社員）
オンラインシステム管理担当

分類	内容
タスク	アラートの監視・調査から不審な兆候を検知し関係部署へ報告する
	インシデントに対する初期調査の実施
知識	セキュリティログに関する知識
	監視・ログ分析ツールに関する知識
スキル	ツールを使用して侵入を検出するスキル
	ログが機器障害か不正アクセスかを正確に判別（トリアージ）するスキル

研修の例

- 対策の費用や損失想定をもとに「必要なセキュリティ投資」を検討するロールプレイング演習※1
- インシデント対応について学ぶことのできる実践的な研修（CYDER、プレCYDER等）※2

- インシデント発生時の「社内外連絡」や「模擬記者会見」のロールプレイング演習※1

- セキュリティインシデント対応机上演習教材※3

※1：内閣官房 内閣サイバーセキュリティセンター（NISC）【現国家サイバー統括室（NCO）】「プラス・セキュリティ知識補充講座 カリキュラム例」（https://security-portal.cyber.go.jp/dx/pdf/plussecurity_curriculum.pdf）
※2：国立研究開発法人情報通信研究機構（NICT）「コース案内」（https://cyder.nict.go.jp/course/index.html）
※3：独立行政法人情報処理推進機構「セキュリティインシデント対応机上演習教材」（https://www.ipa.go.jp/security/sec-tools/ttx.html）

役立つリンク集・用語集

- サイバーセキュリティの業務を担うにあたって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。
- サイバーセキュリティ人材フレームワークの本体や、経済産業省やIPAが公表するガイドライン、ツール等のリンク集として学習計画の検討に活用してください。

- 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2026（教育機関向け）」P.22『A. 基礎として学ぶリテラシー領域』、P.26『E.社会に出てからOJT等を通じて学ぶことが有効な実践的な実務領域』
  - 教育機関向け手引き書のP.22『A. 基礎として学ぶリテラシー領域』では、社会人として必要な「セキュリティ・リテラシー」を身につけるための授業設計の例をご紹介しています。また、P.26『E. 社会に出てからOJT等を通じて学ぶことが有効な実践的な実務領域』では、プラス・セキュリティ層（bさん・cさん・eさん相当）が実務で必要とするタスク・知識・スキルと、それに対応する学習区分（「実務とマネジメント」「現場の実践的運用」「プラス・セキュリティ」）が整理されています。セルフアセスメント後の学習計画策定の際にも参考にしてください。

- 内閣官房 内閣サイバーセキュリティセンター（NISC）【現国家サイバー統括室（NCO）】「プラス・セキュリティ知識補充講座カリキュラム例」（https://security-portal.cyber.go.jp/dx/pdf/plussecurity_curriculum.pdf）
  - プラス・セキュリティ知識の知識を補充するカリキュラムの例をご紹介しています。
- 国立研究開発法人情報通信研究機構（NICT）「CYDERコース案内」（https://cyder.nict.go.jp/course/index.html）
  - 実践的サイバー防御演習「CYDER」や、プラス・セキュリティ人材に必要なセキュリティ知識を短時間で学習できる研修「プレCYDER」についてご案内しています。
- 独立行政法人情報処理推進機構「セキュリティインシデント対応机上演習教材」（https://www.ipa.go.jp/security/sec-tools/ttx.html）
  - 一般企業（中小企業）と医療機関の2種類を対象として、実際にセキュリティインシデントが発生した場合を想定した演習教材についてご案内しています。