資料4

# 人材フレームワーク及び手引き書（案）の進捗状況について


令 和 ８ 年 ２ 月 ９ 日

内　閣　官　房
国家サイバー統括室
人　材　政　策　班

# これまでの議論を踏まえた検討状況について



## 主な御指摘

### フレームワーク（本体）

- 実際の役職名が分かるよう、具体例を示すことが望ましい。
- 技術的な要素だけでなくコミュニケーション・プレゼンテーション力についても考慮すべき。
- 13の人材像は画一的なものではなく、組織規模等に応じた具体例として示されるとよい。

### 手引き書

- フレームワークの利用促進に資する、様々な利用主体を想定したバリエーションに富んだ手引き書とすべき。

## 前回からの進捗状況（概要）

### フレームワーク（本体）

**「人材像」の概念整理**

人材フレームワーク本体では、全体を13の**「役割」**として整理し、各役割に求められる知識・スキル等を体系的に示した上で、各組織がフレームワークに基づき具体化した人材の定義を**「人材像」**として手引き書で提示する。

**役割ごとに想定される役職名等を記載**

現場において各役割を担う人材に対し、一般的に用いられている役職名等を記載。

**役割ごとにタスク・知識・スキル（TKS）を定義**

前回資料を肉付けした上で、13の役割ごとに求められるタスク・知識・スキルを定義。
25年12月に公開されたNICEフレームワーク最新版（v2.1.0）を参考に、AI関係の内容も追加。

**コミュニケーションスキルをレベル設定に内包**

コミュニケーション力や説明力等の業務を遂行する上で各役割に共通する基礎的な能力についても、レベル設定の中に位置づけ整理。

### 手引き書

**利用主体別の活用を想定した記載方針を検討**

利用主体別に多様な活用シーンを想定して骨子案を作成。
小規模事業者向け手引き書(案)では、委託先との連携を含めた体制のあり方などをわかりやすく記載。

国家サイバー統括室

# 人材フレームワーク（案）の進捗状況について

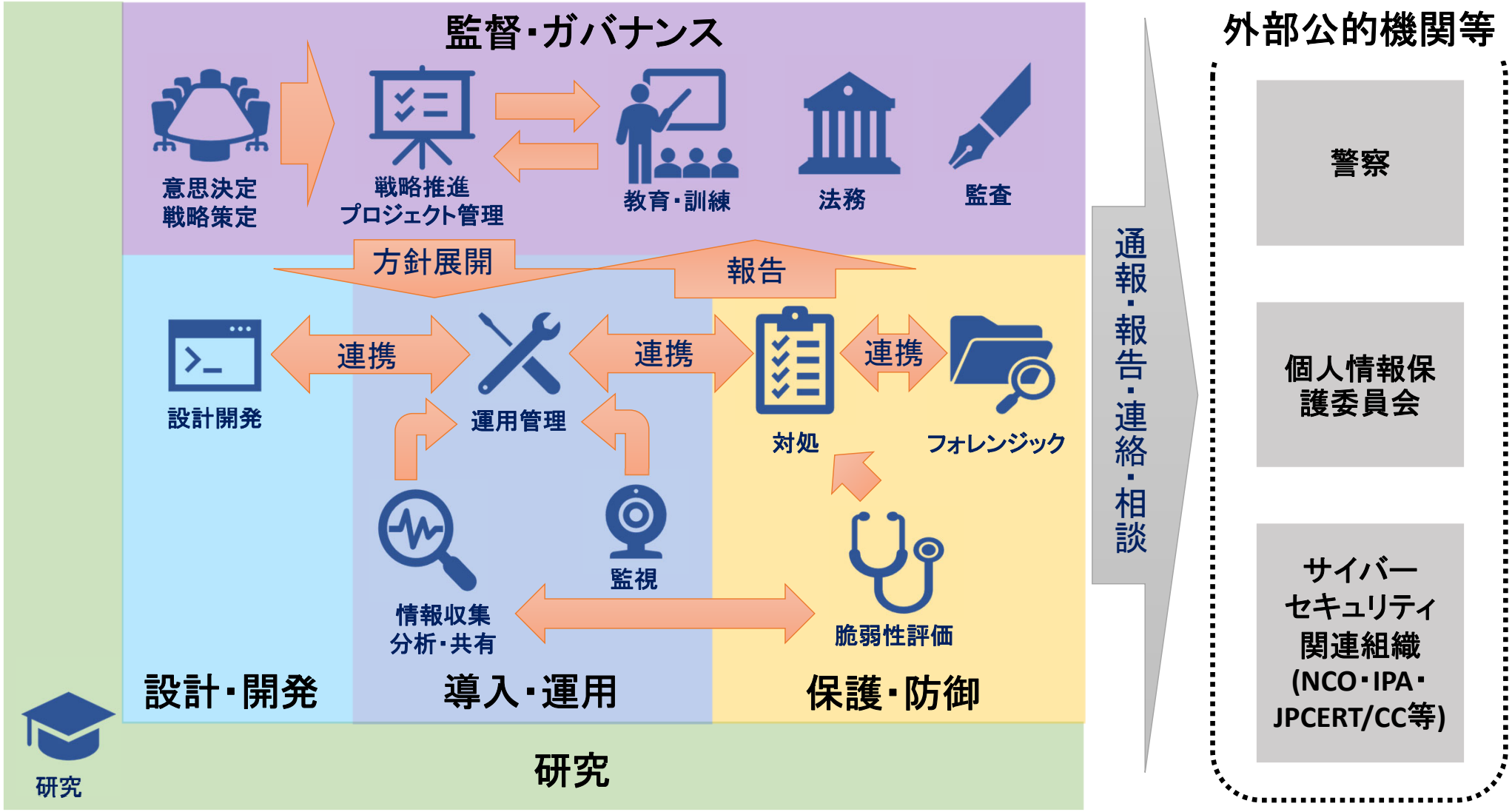
新規追加

# サイバーセキュリティ人材が担う役割の全体像



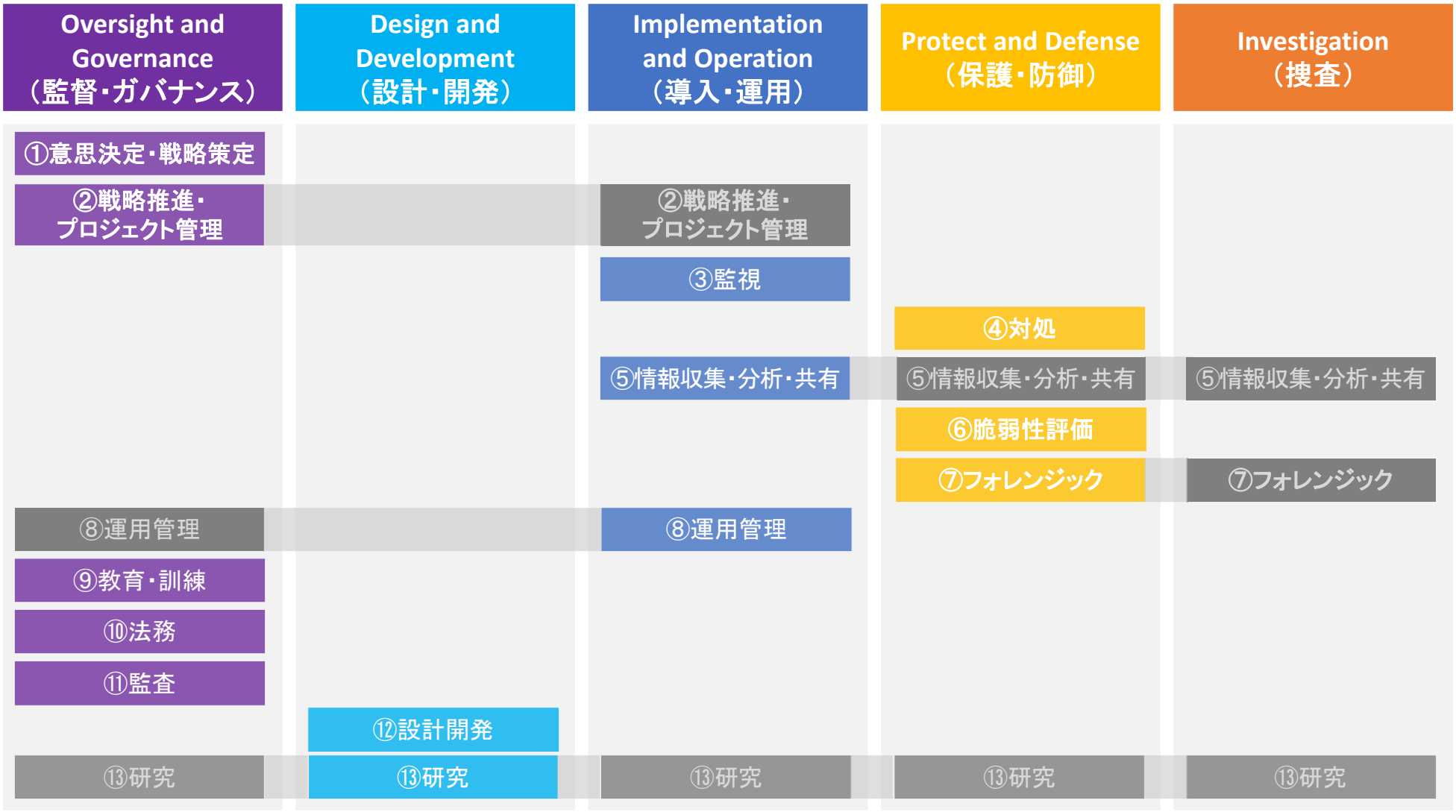
**概要**

国内外のフレームワーク類との相互参照性を図りながら技術的側面に限らず、
各組織でサイバーセキュリティを担う**13の役割**を定義



# （参考）13の役割とNICEフレームワークのカテゴリとの関係





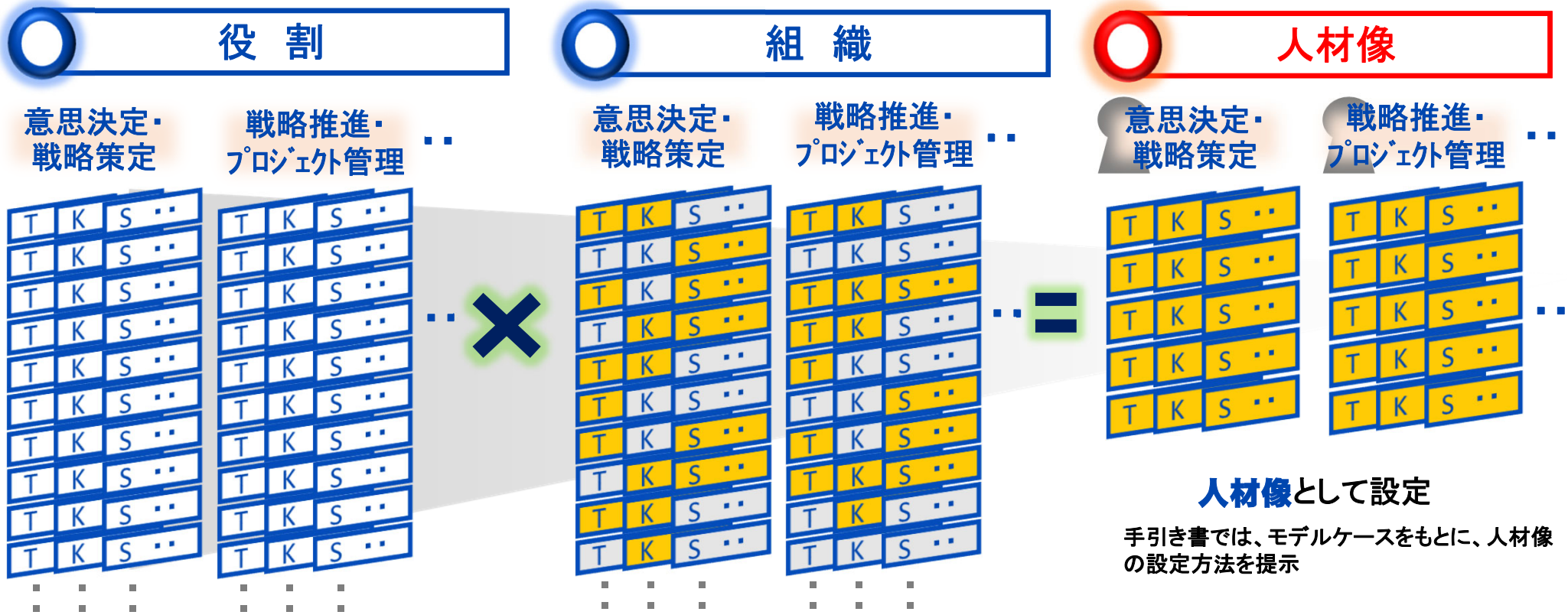
新規追加

# サイバーセキュリティにおける人材像の概念整理



**概要**

- フレームワーク本体において、従前13の「人材像」としていた部分について、**13の「役割」として整理。フレームワークでは、各役割に汎用的なTKSを定義する。**
- 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する。



# 人材フレームワークのレベル設定について



ITSSのレベルと相互参照を図りながら、**4段階のレベル**を設定

※ 前回からの変更箇所は赤字

| レベル | 人材フレームワークのレベルの定義 | 対応するITSSレベル |
|---|---|---|
| 4 | **業務における最終意思決定に対して責任を負う者**<br><br>条件：下記3点のうち2点以上を満たす者<br>① 各役割で定義された知識に加え、業界全体やビジネスに関連する幅広い知識を持っている<br>② 組織全体を俯瞰して、各役割で定義された知識・スキルの向上を企画・立案することができる<br>③ サイバーセキュリティに関する実務経験が10年以上が望ましい | レベル4以上<br>（組織内や業界内等のハイレベルプレーヤ） |
| 3 | **業務を独力で遂行可能であり、かつマネジメントを行う者**<br><br>条件：下記3点のうち2点以上を満たす者<br>① 各役割で定義された知識に基づき、組織内外の連携先と円滑な会話（説明・指導等による管理）ができる<br>② 各役割で定義されたタスクを実行できる<br>③ サイバーセキュリティに関する実務経験が4～10年程度が望ましい | レベル3<br>（独力で遂行可能） |
| 2 | **業務において指示に基づく作業を実行する者**<br><br>条件：下記3点のうち2点以上を満たす者<br>① 各役割で定義された知識の概要に基づき、組織内外の連携先と会話ができる<br>② 他者の指示により、各役割で定義されたタスクを実行することができる<br>③ サイバーセキュリティに関する実務経験が2～4年程度が望ましい | レベル2<br>（指導の下で遂行可能） |
| 1 | **業務に対する最低限必要な知識を有する者**<br><br>条件：下記3点のうち2点以上を満たす者<br>① 各役割で定義された知識のキーワードを理解し、業務に必要な最低限の会話ができる<br>② 他者の指示により、各役割で定義されたタスクを実行することができる<br>③ サイバーセキュリティに関する実務経験が2年未満である | レベル1<br>（最低限必要な知識を有する） |

# 役割の詳細：①意思決定・戦略策定



※ 前回からの変更箇所は赤字

| ①意思決定・戦略策定 | 当該役割を担う人材が所属する組織 | | | | |
|---|---|---|---|---|---|
| | 政府機関 | ユーザー企業（サプライチェーン） | | ベンダー企業（アウトソース先等） | |
| | | 親会社等 | 子会社等 | セキュリティベンダー | 運用保守事業者 |
| | ● | ● | ● | ● | ● |

**主な業務（例）**

- 組織のサイバーセキュリティ戦略やポリシー等を策定する。
- 組織のサイバーセキュリティに係る予算を確保し、組織体制を構築する。
- 組織のシステムのセキュリティ確保に対する責任を持つ。

**NICEフレームワークにおける対応ロール**

| | |
|---|---|
| サイバーセキュリティポリシーと計画 | OG-WRL-002 |
| エグゼクティブサイバーセキュリティリーダーシップ | OG-WRL-007 |
| システム認可 | OG-WRL-013 |
| テクノロジーポートフォリオ管理 | OG-WRL-015 |
| セキュリティ管理策評価 | OG-WRL-012 |

**想定される役職名等**

CISO及びその補佐役

**補足説明**

- 原則として外部委託による対応はできず、自組織にて責任を負うべき人材像である。
- セキュリティポリシー策定等を外部委託にて実施する場合でも、ポリシー策定の責任は自組織で負う必要がある。
- サプライチェーンのセキュリティ確保において、親会社やサプライチェーンを統括する企業が子会社その他の企業のセキュリティ対策に関する戦略決定を包括的に担う場合もある。
- インシデント発生時の意思決定も実施し、④対処を担う人材に指示を行う。
- SecBoKでは「セキュリティ経営、意思決定・戦略策定」、「セキュリティ統括」のロールに対応。
- 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では、「CISO」、「CRO」、「CIO」、「システム部門責任者」等の役割に対応。

新規追加

# 役割の詳細：①意思決定・戦略策定（TKS）



※ AI関連箇所は赤字

| | |
|---|---|
| タスク | サイバーセキュリティに関する意思決定・戦略策定に必要な情報を把握する |
| | サイバーセキュリティに関する戦略、方針、規定等を策定又は承認する |
| | サイバーセキュリティ対策に必要な予算や人員等のリソースを確保する |
| | 通常時のほか、緊急時や復旧時を含むサイバーセキュリティ対応体制を構築する |
| | サイバーセキュリティに関するコンプライアンス確保に対応する |
| | 外部委託やサプライチェーンにおけるサイバーセキュリティ対策を統括する |
| | サイバーセキュリティに関する監査とその結果に基づく見直しを実施する |
| | サイバーセキュリティに関するインシデント発生時の状況把握及び意思決定を行う |
| | サイバーセキュリティに関する啓発又は教育を実施する |
| | 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を行う |
| 知識 | 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 |
| | サイバーセキュリティの基本原則と実践に関する知識 |
| | サイバーセキュリティの最新技術や傾向に関する知識 |
| | 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 |
| | 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 |
| | サイバーセキュリティに係る業界の指標や法律等の規制要件に関する知識 |
| | サイバーセキュリティに関する組織全体の構造と機能に関する知識 |
| | 組織のポリシー等の策定および意思決定に係る手続に関する知識 |
| | 周知対象である関係者や周知手法に関する知識 |
| | セキュリティ業務における手順と実務に関する知識 |
| | 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 |
| | インシデント対応計画の策定に関する知識 |
| | インシデント発生時における組織経営・運営上の意思決定に関する知識 |
| | 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 |
| | インシデント後の分析と改善に関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

| | |
|---|---|
| スキル | 組織目標と体制を評価するスキル |
| | 必要となるサイバーセキュリティ水準を予測するスキル |
| | 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 |
| | 社内外のステークホルダーの意向及び能力を評価するスキル |
| | 業界の自主規制等の要求事項を評価し、組織への影響を特定するスキル |
| | 法令や規制等を評価し、組織への影響を特定するスキル |
| | 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 |
| | 組織のサイバーセキュリティに係る優先順位を設定し、判断するスキル |
| | 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 |
| | 監査結果等から、組織全体のサイバーセキュリティに係る活動を評価するスキル |
| | 組織全体で用いられているシステムやネットワークを評価するスキル |
| | 実施状況を踏まえて組織のサイバーセキュリティに関する運用を調整するスキル |
| | 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 |
| | 自組織内/外からセキュリティ対策に必要な資金を調達するスキル |
| | インシデント対応計画を策定するスキル |
| | 組織の能力や資源を分析し、業務継続または復旧に向けて優先順位を設定するスキル |
| | 法律等の規制要件が定める要求に対応するスキル |
| | インシデントの原因を分析し、方針や戦略に組み込むスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 議論のファシリテ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するスキル |

# 役割の詳細：②戦略推進・プロジェクト管理



※ 前回からの変更箇所は赤字

| ②戦略推進・プロジェクト管理 | 当該役割を担う人材が所属する組織 | | | | |
|---|---|---|---|---|---|
| | 政府機関 | ユーザー企業（サプライチェーン） | | ベンダー企業（アウトソース先等） | |
| | | 親会社等 | 子会社等 | セキュリティベンダー | 運用保守事業者 |
| | ○ | ○ | △ | ● | ● |

| | | |
|---|---|---|
| 主な業務（例） | ● 決定されたサイバーセキュリティ戦略に基づく取組を推進・管理する。<br>● 組織のサイバーセキュリティ対策に関するプログラム又はプロジェクトに関して、目標・計画の策定、プログラム/プロジェクト体制の整備、進捗管理、資産・予算管理、委託先管理、業務改善等の各種管理業務を実施する<br>● 要員のクリアランス、取り扱う個人情報、機密情報の管理・運用、インシデント発生時の運用ルールを定める | |
| NICEフレームワークにおける対応ロール | プログラム管理 | OG-WRL-010 |
| | セキュリティプロジェクト管理 | OG-WRL-011 |
| | ナレッジ管理 | IO-WRL-003 |
| 想定される役職名等 | 個人情報管理責任者、情報管理者、プロジェクトマネージャー、プロジェクトリーダー　等 | |
| 補足説明 | ● ①意思決定・戦略策定が策定したセキュリティ対策に関する施策を実施する役割を担う。明確にプロジェクトとして扱われていない活動も含む。<br>● セキュリティ対策に関する各種プロジェクト（ISMS運営、対策の導入、全社展開等）を推進するプロジェクトマネージャーに相当する。<br>● 子会社・委託先等における“△”は、自組織に限定したプロジェクトの場合は必要であるが、サプライチェーン全体のプロジェクト等を従たる立場で実施する場合は不要であることを意味する。<br>● SecBoKでは、「プロジェクト管理」、「社内外調整」のロールに対応。<br>● 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では、「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」の役割・担当に対応。 | |

新規追加

# 役割の詳細：②戦略推進・プロジェクト管理（TKS）



※ AI関連箇所は赤字

| | |
|---|---|
| タスク | 通常時・インシデント発生時の運用ルールの起案 |
| | サイバーセキュリティ戦略に沿ったプロジェクトの立案 |
| | プロジェクトにおける人員、予算及び資産の調達・執行管理 |
| | 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 |
| | 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 |
| | プロジェクトの工程管理 |
| | サービスの品質管理 |
| | プロジェクトメンバーの人事管理及び安全管理 |
| | プロジェクトの完了と次プロジェクトへの移行 |
| | プロジェクトにおけるインシデント管理 |
| 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 |
| | 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 |
| | リスクマネジメントに関する知識 |
| | 組織のサイバーセキュリティ目標と目的に関する知識 |
| | 組織のサイバーセキュリティに係るポリシーや管理プロセスに関する知識 |
| | 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 |
| | プロジェクト資金の調達方法に関する知識 |
| | 調達先のリスクの特定、評価に関する知識 |
| | サプライチェーンの構造と運用に関する知識 |
| | 調達する機器の選定基準とその評価に関する知識 |
| | 調達時に遵守すべき法令や規制に関する知識 |
| | 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 |
| | 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 |
| | プロジェクト管理ツールの使用に関する知識 |
| | プロジェクトスコープや計画の変更に関する知識 |
| | 組織が提供するサービスのリスクやパフォーマンス管理に関する知識 |
| | プロジェクトに必要な職務要件とスキルセットに関する知識 |
| | チームビルディング活動の実施に関する知識 |
| | メンバーのモチベーションとエンゲージメントを高める方法に関する知識 |
| | 最終成果物や報告書の作成に関する知識 |
| | プロジェクト評価とレビューに関する知識 |
| | プロジェクトに係る文書の整理とアーカイブに関する知識 |
| | 次ステップの計画の立案に関する知識 |
| | インシデント対処に関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

| | |
|---|---|
| スキル | 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 |
| | 組織目標や戦略を分析し、プロジェクト計画を立案するスキル |
| | 遵守すべき組織の規定やプロセスを分析し、プロジェクト計画を立案するスキル |
| | プロジェクト達成に必要な予算の見積もりを立てるスキル |
| | プロジェクト運営時にかかったコストの経時的変化を管理するスキル |
| | 自組織内/外のプロジェクト資金調達先を発見し、交渉するスキル |
| | サプライヤー評価と選定基準を調達プロセスに適用するスキル |
| | プロジェクトにおいて発生した契約事項を管理するスキル |
| | 調達先のリスクを分析し、判断するスキル |
| | 組織のサイバーセキュリティ水準を満たす技術や機器の要件を決定するスキル |
| | 法律や規制の要求事項を調達プロセスに適用するスキル |
| | 遵守すべき法令やプライバシー上の要求事項をプロジェクトに適用させるスキル |
| | プロジェクトで活用している技術の性能を監視、分析するスキル |
| | プロジェクトにおける各業務が組織の求めるセキュリティポリシーに適合しているか監視、分析するスキル |
| | プロジェクトの進行状況を把握し、必要に応じて調整するスキル |
| | 必要な変更を承認し、計画に反映するスキル |
| | 組織が提供するサービスの水準や品質を監視、分析するスキル |
| | 顧客が求めるサービス水準を分析するスキル |
| | フィードバックをもとにサービス改善を行うスキル |
| | プロジェクトに必要な職務要件を基にメンバーを選定、採用するスキル |
| | プロジェクトメンバーに対する情報伝達スキル |
| | プロジェクトメンバーの意見への傾聴スキル |
| | インセンティブや報酬を利用してモチベーションを維持するスキル |
| | プロジェクトの成果、費用等をまとめ、主要なステークホルダーに報告するスキル |
| | プロジェクト全体のパフォーマンスを評価するスキル |
| | 必要な文書を整理・アーカイブし、組織内に教訓や成果を共有するスキル |
| | プロジェクトの成果を分析し、次プロジェクトの計画を立案するスキル |
| | 関係部署と連携し、インシデント対処を行うスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 議論のファシリテ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するスキル |

# 役割の詳細：③監視



※ 前回からの変更箇所は赤字

| ③監視 | 当該役割を担う人材が所属する組織 | | | | |
|---|---|---|---|---|---|
| | 政府機関 | ユーザー企業（サプライチェーン） | | ベンダー企業（アウトソース先等） | |
| | | 親会社等 | 子会社等 | セキュリティベンダー | 運用保守事業者 |
| | ○ | ○ | – | ○ | ● |

| | | |
|---|---|---|
| 主な業務（例） | ● セキュリティ監視を行う。（各種機器のログの監視、保管、分析）<br>● セキュリティインシデントを検知し、関係各所へ連携する。<br>● 監視ツールの運用、保守を行う。 | |
| NICEフレームワークにおける対応ロール | ディフェンシブサイバーセキュリティ | PD-WRL-001 |
| | 内部脅威分析 | PD-WRL-005 |
| | 脅威分析 | PD-WRL-006 |
| 想定される役職名等 | SOC責任者、SOCメンバー、セキュリティエンジニア、オペレーター、監視担当　等 | |
| 補足説明 | ● 一般にSOC（Security Operation Center）サービスを提供する要員に相当し、24時間365日の監視が必要なことから、外部委託にて実施されることが多い。<br>● 経済産業省の情報セキュリティサービス審査登録制度における「セキュリティ監視・運用サービス」に従事する人材に相当。<br>● SecBoKでは「監視・運用」のロールに対応。<br>● 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では、「SOC担当」に対応。 | |

新規追加

# 役割の詳細：③監視（TKS）



※ AI関連箇所は赤字

| | |
|---|---|
| **タスク** | 通常時・インシデント発生時の運用ルールの起案 |
| | 監視対象システム、機器及び範囲の決定 |
| | 委託先の選定及び委託内容の調整 |
| | 委託先とのコミュニケーションの実施 |
| | ツールの選定・設定 |
| | 対象システムや機器等からログを収集 |
| | ログ分析 |
| | ログ分析レポートの作成・共有 |
| | 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 |
| **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 |
| | 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 |
| | リスクマネジメントに関する知識 |
| | 対象システム、機器の脆弱性に関する知識 |
| | 対象システム、機器の構成要素やセキュリティに関する知識 |
| | ツール（監視、ログ収集・分析）及びその手法に関する知識 |
| | 監視対象システム、機器の設定に関する知識 |
| | 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）に関する知識 |
| | 組織内の関連計画、対象システム、機器の構成要素やセキュリティに関する知識 |
| | ログ分析レポートに含めるべき項目に関する知識 |
| | レポート共有の手順・関係者に関する知識 |
| | 監視対象機器の設定に関する知識 |
| | インシデントの初動対応に関する知識 |
| | 商用監視サービスに関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

| | |
|---|---|
| **スキル** | 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 |
| | サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する情報やサイバーセキュリティの脅威やサイバー攻撃の特性・ツールに関する知識を様々な情報源から収集し、監視対象を決定するスキル |
| | 対象システム、機器の脆弱性に関する情報を収集し、監視対象を決定するスキル |
| | 対象機器のセキュリティに関する情報を収集するスキル |
| | ツールの設定値を監視対象や目的に応じた設定にするスキル |
| | ツールを使用してシステムやネットワーク、データベース等を監視し、侵入を検出するスキル |
| | ツールの設定値を見直し、適切な設定値に変更するスキル |
| | 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 |
| | 分析ツールを使用してログ分析を実施するスキル |
| | 組織のサイバーセキュリティ関連計画に応じてログ分析レポートを作成するスキル |
| | 組織のサイバーセキュリティ関連計画に応じて情報共有を実施するスキル |
| | 組織のサイバーセキュリティ体制に応じて、適時適切な対象に情報を共有するスキル |
| | 組織のサイバーセキュリティ関連計画に応じて、アラートを発出するスキル |
| | 機器障害か、不正なアクセスや悪意のある侵入であるかを判別するスキル（トリアージ） |
| | インシデントの初動対応を実施するスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 想定読者に応じて適切な表現や形式のレポートを作成するスキル |

# 役割の詳細：④対処



※ 前回からの変更箇所は赤字

| ④対処 | 当該役割を担う人材が所属する組織 | | | | |
|---|---|---|---|---|---|
| | 政府機関 | ユーザー企業（サプライチェーン） | | ベンダー企業（アウトソース先等） | |
| | | 親会社等 | 子会社等 | セキュリティベンダー | 運用保守事業者 |
| | ○ | ○ | ○ | ○ | ● |

| | | |
|---|---|---|
| 主な業務（例） | ● サイバーセキュリティインシデント発生時、影響の拡大を防止すると共に、発生したインシデントに対する調査、分析、評価、復旧を行う。<br>● インシデント対応に係る関係機関との連絡・調整等を行う。<br>● 組織として実施するインシデントに係る広報等への対応のために必要な情報提供を行う。 | |
| NICEフレームワークにおける対応ロール | インシデントレスポンス | PD-WRL-003 |
| 想定される役職名等 | CSIRT責任者、CSIRTメンバー、インシデントハンドラー、セキュリティエンジニア、オペレーター等（一般にCSIRT以外は通常時の業務における役職名で扱われることが多い） | |
| 補足説明 | ● CSIRTが存在する組織の場合、CSIRTに所属する人材に相当。<br>● インシデント発生時の対処を担う人材として、組織の規模に関わらず全ての組織において必要な人材であるが、専門的な知識・スキルが必要な内容をセキュリティベンダーの専門人材にて対応する等の役割分担が行われることもある。<br>● SecBoKでは「対処（インシデントハンドリング）」のロールに対応。<br>● 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では、「CSIRT責任者/担当」、「サイバーセキュリティ事件・事故担当」の役割・担当に対応。 | |

新規追加

# 役割の詳細：④対処（TKS）



※ AI関連箇所は赤字

| | |
|---|---|
| タスク | インシデント対処準備 |
| | 委託先の選定及び委託内容の調整 |
| | 委託先とのコミュニケーションの実施 |
| | 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 |
| | インシデントに対する初期評価・トリアージ |
| | インシデント対応に係る関係部署への対応措置の指示 |
| | インシデント対応に係る関係部署への復旧措置の指示 |
| | 発生したインシデントの原因究明調査 |
| | 調査結果の評価に基づく再発防止策の策定 |
| | インシデントレポートの作成・共有 |
| 知識 | インシデント対処活動の手順や手法に関する知識 |
| | リスクマネジメントに関する知識 |
| | インシデント速報の報告手順・対象に関する知識 |
| | インシデントの評価、トリアージに関する知識 |
| | リスク／脅威の評価に関する知識 |
| | インシデント対応措置及びその実施に関する知識 |
| | 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 |
| | インシデント復旧措置及びその実施に関する知識 |
| | インシデント後の再発防止策の策定および実施に関する知識 |
| | インシデントレポートに含めるべき項目に関する知識 |
| | インシデントレポート共有の手順・対象に関する知識 |
| | 商用のインシデント対処サービスに関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

| | |
|---|---|
| スキル | 自組織が所有する機器の仕様の理解（アクセス制御リスト、ネットワーク監視ツール等）、必要資材の調達、チーム編成、基本的なツールの準備等を行い、事業活動の継続を第一としたインシデント対処のプロセスを策定するスキル |
| | インシデントを検知した自組織内/外のサイバーセキュリティ関係部署から報告を受け、インシデント対応が必要か否かを判断するスキル |
| | インシデントの概要、自組織内/外への影響、復旧見込を速やかにとりまとめ、組織のCISO、経営層に報告するスキル |
| | 自組織内/外のサイバーセキュリティ関係各所にインシデントの初期調査を指示・依頼し、速やかに情報を収集するスキル |
| | 自組織内/外のサイバーセキュリティ関係各所より収集した初期調査結果をもとに事業の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 |
| | 自組織内/外のサイバーセキュリティ関係各所にインシデントに対する対処作業及び復旧作業を明確化し、指示を与えるスキル |
| | 一連のインシデント対処で生じた新たな情報や外部からの情報を活用し、インシデントの原因を究明するスキル |
| | 原因究明調査の結果を基に、自組織内/外に与えた被害範囲を特定し、損害を評価するスキル |
| | インシデント後の再発防止策策定の助言を行うスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 議論のファシリテ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するスキル |
| | 想定読者に応じて適切な表現や形式のレポートを作成するスキル |

# 役割の詳細：⑤情報収集・分析・共有



※ 前回からの変更箇所は赤字

| ⑤情報収集・分析・共有 | 当該役割を担う人材が所属する組織 | | | | |
|---|---|---|---|---|---|
| | 政府機関 | ユーザー企業（サプライチェーン） | | ベンダー企業（アウトソース先等） | |
| | | 親会社等 | 子会社等 | セキュリティベンダー | 運用保守事業者 |
| | ○ | ○ | － | ○ | ● |

| | | |
|---|---|---|
| 主な業務（例） | ● 組織内外の情報セキュリティに関する情報を収集する（脅威ハンティング等、脅威の能動的な探索の実施を含む）。<br>● 収集した情報の分析を実施する。<br>● 分析した結果を管理及び共有する。 | |
| NICEフレームワークにおける対応ロール | データ分析 | IO-WRL-001 |
| | ディフェンシブサイバーセキュリティ | PD-WRL-001 |
| | 内部脅威分析 | PD-WRL-005 |
| | 脅威分析 | PD-WRL-006 |
| | ナレッジ管理 | IO-WRL-003 |
| 想定される役職名等 | サイバーセキュリティアナリスト、脅威インテリジェンスアナリスト、リサーチャー、セキュリティエンジニア　等 | |
| 補足説明 | ● 脆弱性情報の収集及び脅威インテリジェンスに相当するタスクを含む。<br>● 中小企業では収集した情報から自組織への影響を適切に判断できるスキルを有する人材の確保が困難な場合も多いと想定される。この場合、セキュリティ対策が実施された外部のSaaSサービスを利用すること等により、この役割を担う人材を割り当てない対応も考えられる。<br>● CTEM（Continuous Threat Exposure Management）として、継続的に脅威の検知及びリスクへの対応を行うような取組を含めることも想定される。<br>● SecBoKでは「脅威・脆弱性情報収集」のロールに対応。<br>● 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では、「SOC担当」に対応。 | |

新規追加

# 役割の詳細：⑤情報収集・分析・共有



※ AI関連箇所は赤字

| | |
|---|---|
| タスク | 通常時・インシデント発生時の運用ルールの起案 |
| | 情報収集運用方針の策定 |
| | 情報収集の対象を決定 |
| | 委託先の選定及び委託内容の調整 |
| | 委託先とのコミュニケーションの実施 |
| | 情報の収集 |
| | 情報の分析 |
| | 収集・分析した情報の管理 |
| | レポートの作成・共有 |
| | 情報収集活動の評価分析及び改善 |
| 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 |
| | 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 |
| | リスクマネジメントに関する知識 |
| | 組織の掲げるサイバーセキュリティのあるべき姿に関する知識 |
| | 組織のサイバーセキュリティ関係部署の機能や情報収集能力に関する知識 |
| | 情報収集活動の手順や手法に関する知識 |
| | 情報収集の目的・目標に対する優先順位付けに関する知識 |
| | 情報源に関する知識 |
| | 情報収集のツール、手法及びプロセスに関する知識 |
| | 情報収集先で使用されている外国語や特性(文化的背景、地域的特定)に関する知識 |
| | 情報分析のツール、手法及びプロセスに関する知識 |
| | 情報の分類に関するガイドライン及びその手法に関する知識 |
| | 情報管理に係るポリシーや手順に関する知識 |
| | 情報共有の手順に関する知識 |
| | 情報収集報告書等に含めるべき項目に関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

| | |
|---|---|
| スキル | 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 |
| | 組織のサイバーセキュリティのあるべき姿に適合する情報収集計画を策定するスキル |
| | 収集すべき情報の中から、組織の情報収集能力等を鑑み収集の優先順位を付けるスキル |
| | 組織の目的に適合する情報収集活動の手順や手法を選択するスキル |
| | 情報収集の目的・目標から、組織の能力・リソース等を鑑み収集の優先順位を付けるスキル |
| | 膨大な情報源から実績や発行元等の情報を参考に信頼できる情報源を特定するスキル |
| | 情報収集ツールの特性を理解し、組織の目的・目標・能力に合った最適なツールを選定するスキル |
| | 情報収集先で使用されている外国語を理解し、組織が収集すべき情報を収集するスキル |
| | 「脆弱性情報」等個別で各専門領域における情報を収集する役割と連携し、組織内のリスクに係る情報を収集するスキル |
| | 情報分析ツールの特性を理解し、自組織内/外より収集した情報を元にリスク分析・評価を行い、組織に影響のある脅威/脆弱性を特定するスキル |
| | 情報収集先で使用されている外国語を理解し、収集した情報を分析するスキル |
| | 業界標準に応じて情報を分類するスキル |
| | 収集、分析した情報を分類に応じて適切に管理し、必要なタイミングで活用・共有できるスキル |
| | 計画策定から情報の共有までの情報収集活動の一連の流れを評価し、課題点を改善するスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 想定読者に応じて適切な表現や形式のレポートを作成するスキル |

# 役割の詳細：⑥脆弱性評価



※ 前回からの変更箇所は赤字

| ⑥脆弱性評価 | 当該役割を担う人材が所属する組織 | | | | |
|---|---|---|---|---|---|
| | 政府機関 | ユーザー企業（サプライチェーン） | | ベンダー企業（アウトソース先等） | |
| | | 親会社等 | 子会社等 | セキュリティベンダー | 運用保守事業者 |
| | ○ | ○ | – | ○ | ● |

| | | |
|---|---|---|
| 主な業務（例） | ● ソフトウェアやシステム、ネットワーク等を対象に脆弱性診断・ペネトレーションテストを行い、脆弱性がないか評価する。 | |
| NICEフレームワークにおける対応ロール | 脆弱性分析 | PD-WRL-007 |
| 想定される役職名等 | 脆弱性診断士、脆弱性アナリスト、ペネトレーションテスター、セキュリティエンジニア　等 | |
| 補足説明 | ● 脆弱性の有無に関する判断には専門的なスキルが求められるため、自組織内で関連スキルを有する人材を確保できない場合には外部委託による対応が可能である。<br>● 経済産業省の情報セキュリティサービス審査登録制度における「脆弱性診断サービス」及び「ペネトレーションテストサービス」に従事する人材に相当。<br>● SecBoKでは「脆弱性診断・評価」のロールに対応。<br>● 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では、「運用系サイバーセキュリティ担当」に対応。 | |

新規追加

# 役割の詳細：⑥脆弱性評価



※ AI関連箇所は赤字

| | |
|---|---|
| タスク | 評価対象の選定 |
| | 委託先の選定及び委託内容の調整 |
| | 委託先とのコミュニケーションの実施 |
| | 評価手法の決定 |
| | 脆弱性評価の実施 |
| | ペネトレーションテストの実施 |
| | 発見された脆弱性の分析・評価 |
| | 評価結果レポートの作成・共有 |
| 知識 | 組織内の関連計画、対象システム、機器の構成要素やセキュリティに関する知識 |
| | 脆弱性評価ツール及び手法に関する知識 |
| | ペネトレーションテストツール及び手法に関する知識 |
| | 脆弱性の一般的な評価基準に関する知識 |
| | 脆弱性評価/ペネトレーションテスト結果レポートに含めるべき項目に関する知識 |
| | 評価結果レポート共有の手順・対象に関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

| | |
|---|---|
| スキル | 関係者へのヒアリング及びシステムに係る設計書、構成情報等を収集・整理し、組織の環境・目標を分析し、評価対象を選定するスキル |
| | 組織及び診断対象の性質から最適な評価手法を導き出すスキル |
| | 組織のサイバーセキュリティ環境・目的にあった脅威シナリオを元に脆弱性評価/ペネトレーションテストを行い、脆弱性の有無を明らかにするスキル |
| | 脆弱性評価/ペネトレーションテストツールの特性を理解し、取扱うスキル |
| | 評価/テストで収集した情報を整理し、情報の正確性を分析することで、具体的な脆弱性を特定するスキル |
| | 特定された脆弱性毎に深刻度、影響の大きさ等を元に重大度をスコアリングし、スコアに基づき対応の優先順位を付けるスキル |
| | 評価結果、対応案、対応後の推奨事項等組織の脆弱性対応に繋がる情報を平易な表現でレポートに記載するスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 想定読者に応じて適切な表現や形式のレポートを作成するスキル |

# 役割の詳細：⑦フォレンジック



※ 前回からの変更箇所は赤字

## ⑦フォレンジック

| 当該役割を担う人材が所属する組織 | | | | |
|---|---|---|---|---|
| 政府機関 | ユーザー企業（サプライチェーン） | | ベンダー企業（アウトソース先等） | |
| | 親会社等 | 子会社等 | セキュリティベンダー | 運用保守事業者 |
| ○ | ○ | – | ○ | ● |

**主な業務（例）**

- サイバーセキュリティインシデントが発生した際に、デジタルデータの証拠保全対象を判断し、適切なツールで証拠保全を行う。
- 証拠保全の対象としたデジタルデータを分析し、人材像「対処」と連携し、セキュリティインシデントを調査・報告する。

**NICEフレームワークにおける対応ロール**

| | |
|---|---|
| デジタルフォレンジック | PD-WRL-002 |
| サイバー犯罪捜査 | IN-WRL-001 |
| デジタル証拠解析 | IN-WRL-002 |

**想定される役職名等**

フォレンジックエンジニア、セキュリティエンジニア　等

**補足説明**

- 適切な証拠保全や原因調査等には専門的なスキルが要求されることから、一般の企業等では自社で当該業務を担う人材を有さず、外部委託により対応することが多い。
- 経済産業省の情報セキュリティサービス審査登録制度における「デジタルフォレンジックサービス」に従事する人材に相当。
- SecBoKでは「インシデント調査・分析」のロールに対応。
- 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では、「サイバーセキュリティ事件・事故担当」に対応。

新規追加

# 役割の詳細：⑦フォレンジック



※ AI関連箇所は赤字

| | |
|---|---|
| タスク | フォレンジック調査の対象選定 |
| | 委託先の選定及び委託内容の調整 |
| | 委託先とのコミュニケーションの実施 |
| | フォレンジックツールの整備等対応準備 |
| | 取得対象データの保全・収集 |
| | データの解析と評価 |
| | フォレンジックレポートの作成・共有 |
| | 現場の保全等の初動対応 |
| 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 |
| | フォレンジック対応のプロセス、必要なツール等に関する知識 |
| | データ保全のツール、手法及びプロセスに関する知識 |
| | データ収集のツール、手法及びプロセスに関する知識 |
| | データ分析のツール、手法及びプロセスに関する知識 |
| | レポートに含めるべき項目に関する知識 |
| | レポート共有の手順・関係者に関する知識 |
| | 調査対象の機器の絞り込み、優先順位付けに関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

| | |
|---|---|
| スキル | インシデントの内容から関係者にヒアリングを行うスキル |
| | フォレンジック調査に必要な機器を特定し、調査対象の優先順位を付けるスキル |
| | フォレンジック対応のプロセスから対象機器の仕様・プロトコルの理解、ツール等の必要資材の調達、チーム編成、基本的なツールの準備等を行うスキル |
| | データ保全ツールの特性を理解し、収集したデータを機密性、完全性、可用性を損なわない状態で保全するスキル |
| | データ収集ツールの特性を理解し、調査対象機器から攻撃や不正行為の痕跡に関係のあると考えられるデータを収集するスキル |
| | データ分析ツールの特性を理解し、保全されたデータを分析することで、機器で行われた操作等を特定するスキル |
| | 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するスキル |
| | 被害者等からの通報を受け、事案の特性を踏まえた所管部署へ情報を連携するスキル |
| | 証拠として有用な情報の消滅等を防ぐための初動対応を現場担当者と連携し行うスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 想定読者に応じて適切な表現や形式のレポートを作成するスキル |

# 役割の詳細：⑧運用管理



※ 前回からの変更箇所は赤字

## ⑧運用管理

| 当該役割を担う人材が所属する組織 | | | | |
|---|---|---|---|---|
| 政府機関 | ユーザー企業（サプライチェーン） | | ベンダー企業（アウトソース先等） | |
| | 親会社等 | 子会社等 | セキュリティベンダー | 運用保守事業者 |
| ▲ | ● | ● | ● | ● |

**主な業務（例）**

- 組織の要請に応じ、要件定義・仕様の策定時における開発部署への助言・所要の意見提出を行う。
- 組織で扱うデータを適切に保護するためのアクセス制御、認証及びバックアップ等の管理策を実施する。
- 情報インフラ設備等の運用・保守に係る作業内容等を記載した運用・保守計画書を作成する。
- 運用・保守計画書に沿って、情報インフラ設備等の運用・保守業務を実施する。
- 情報システム及びネットワーク環境におけるセキュリティの設定等ネットワークの安全性を担保し、不審な兆候の検知時やインシデント発生時には関係各所と連携し、対処に当たる。
- 情報システム及びネットワーク環境の運用終了時は、機器の廃棄、データの消去等を適切に行う。

**NICEフレームワークにおける対応ロール**

| | |
|---|---|
| 製品サポート管理 | OG-WRL-009 |
| システムセキュリティ管理 | OG-WRL-014 |
| データベース管理 | IO-WRL-002 |
| システム管理 | IO-WRL-005 |
| システムセキュリティ分析 | IO-WRL-006 |
| 技術的サポート | IO-WRL-007 |
| インフラストラクチャサポート | PD-WRL-004 |
| 通信セキュリティ（COMSEC）管理 | OG-WRL-001 |
| ネットワーク運用 | IO-WRL-004 |

**想定される役職名等**

セキュリティオペレーター、システムオペレーター、セキュリティエンジニア　等

**補足説明**

- 実態としてはセキュリティ対策のみを担う担当者を割り当てるのではなく、情報システム等の運用保守担当者がセキュリティ対策も担う形での実施が想定される。
- 政府機関の“△”は一部機関において組織内で運用管理が実施される場合を想定する。
- SecBoKでは「システム管理・ネットワーク管理」のロールに対応。
- 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では、「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」等の役割・担当に対応。

新規追加

# 役割の詳細：⑧運用管理



※ AI・クラウド関連箇所は赤字

| | |
|---|---|
| タスク | 通常時・インシデント又は通信障害発生時の運用ルールの起案 |
| | 要件定義・仕様の策定時における開発部署への助言・所要の意見提出 |
| | 委託先の選定及び委託内容の調整 |
| | 委託先とのコミュニケーションの実施 |
| | システム及びネットワーク機器に対する初期設定の実施 |
| | ユーザーアカウント・権限管理 |
| | アクセス制御方針の作成及び方針に基づいたアクセス制御の実行 |
| | 構成管理及び変更管理 |
| | システム及びネットワーク機器のアップデート・バックアップの管理 |
| | ユーザーからの問合せに対するサポート |
| | システム及びネットワークの管理業務に対する評価及び改善策の実施 |
| | 自社のシステム及びネットワーク機器又は他社のサービスに対する定期メンテナンスの実施 |
| | システム内又はネットワーク機器内で発見された脆弱性の修正 |
| | システム及びネットワークのセキュリティやパフォーマンス等に関するイベントの検知 |
| | 不審な兆候を関係部署へ報告・通報 |
| | インシデントに対する対処・復旧措置の実施 |
| | インシデントの調査 |
| | 再発防止策の検討と実装 |
| | システム及びネットワークの運用終了時の対応 |
| 知識 | OTにおける脅威と対策に関する知識 |
| | OTを対象とする管理ツールに関する知識 |
| | アカウント管理に関する知識 |
| | アクセス制御に関する知識 |
| | アクセス制御のためのツールに関する知識 |
| | アクセス制御の手法に関する知識 |
| | イベント検知時の対処手順に関する知識 |
| | インシデント対処ツールに関する知識 |
| | インシデント対処に関する知識 |
| | インシデント対処の手順に関する知識 |
| | システムセキュリティに関する知識 |
| | システムの運用終了時における対応に関する知識 |
| | システムの要件定義・仕様策定に関する知識 |
| | システム管理活動全体の評価基準及び手法に関する知識 |
| | データセキュリティの管理に関する知識 |
| | データベース構築・運用に関する知識 |
| | トラブルが発生した際の手順に関する知識 |
| | トラブルシューティングの手法に関する知識 |
| | ネットワークインフラストラクチャに関する知識 |
| | ネットワークセキュリティに関する知識 |
| | ネットワークにおけるインシデントに関する知識 |
| | ネットワークに関連する組織内のポリシー・関連計画に関する知識 |

| | |
|---|---|
| 知識 | ネットワークに対する攻撃に関する知識 |
| | ネットワークの運用終了時における対応に関する知識 |
| | ネットワークの脆弱性に関する知識 |
| | ネットワークの通信障害に関する知識 |
| | ネットワークの要件定義・仕様策定に関する知識 |
| | ネットワーク管理活動全体の評価基準及び手法に関する知識 |
| | ネットワーク機器のアップデートに関する知識 |
| | ネットワーク機器のバックアップに関する知識 |
| | ネットワーク機器のライフサイクルに関する知識 |
| | ネットワーク機器の変更管理の手法に関する知識 |
| | ネットワーク機器の保守に関する知識 |
| | ハードウェア、ソフトウェア、基幹システム等に関する知識 |
| | メンテナンスを実施するツールや手法に関する知識 |
| | 検知ツールに関する知識 |
| | 構成管理に関する知識 |
| | 情報システムに関連する組織内のポリシー・関連計画に関する知識 |
| | 情報システムに対する脅威に関する知識 |
| | 情報システムに対する攻撃に関する知識 |
| | 情報システムのアップデートに関する知識 |
| | 情報システムのバックアップに関する知識 |
| | 情報システムのライフサイクルに関する知識 |
| | 情報システムの障害に関する知識 |
| | 情報システムの脆弱性に関する知識 |
| | 情報システムの脆弱性の修正方法に関する知識 |
| | 情報システムの変更管理の手法に関する知識 |
| | 情報システムの保守に関する知識 |
| | 制御システムにおける脅威と対策に関する知識 |
| | 積極的防御に関する知識 |
| | 組織の情報システムの運用・保守に関する知識 |
| | 調査報告書に含めるべき項目に関する知識 |
| | 通信ネットワーク構成設計に関する知識 |
| | 通信関連システム及び周辺機器に関する知識 |
| | 通信関連システム及び周辺機器の管理手法に関する知識 |
| | 通信障害に関する知識（器材故障、落雷の影響など） |
| | 適切なセキュリティ対策の設定方法に関する知識 |
| | 報告・通報の手順・関係者に関する知識 |
| | クラウドサービスの種類と責任分界に関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

新規追加

# 役割の詳細：⑧運用管理



※ AI関連箇所は赤字

| | |
|---|---|
| スキル | インシデントに対する再発防止策を検討し、実装するスキル |
| | 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 |
| | インシデント対処のためのツールを使用するスキル |
| | インシデント対処を実施するスキル |
| | 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 |
| | システムの運用終了時における対応に関するスキル |
| | 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 |
| | ツールを使用してメンテナンスを実施するスキル |
| | データベースの設計・運用を実施するスキル |
| | データ移行を実施するスキル |
| | ネットワークインシデントに対処するスキル |
| | ネットワークの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 |
| | ネットワークのセキュリティ対策を実装するスキル |
| | ネットワークのトラブルが発生した際に、バックアップシステムへ切り替えるスキル |
| | ネットワークのトラブルが発生した際に、適切な報告先（ユーザ、上位者）へ報告するスキル |
| | ネットワークのトラブルの原因を追究し、ネットワークを再構築するスキル |
| | ネットワークの運用終了時における対応に関するスキル |
| | ネットワークの脆弱性に対処するスキル |
| | ネットワークを保護するために、継続的な監視を実施するスキル |
| | ネットワーク機器に係る情報を適切にバックアップするスキル |
| | ネットワーク機器のアップデートによる変更の情報を整理・管理し、必要に応じて変更情報を検索することができるスキル |
| | ネットワーク機器のライフサイクルに従い、ネットワークの導入・運用・廃棄を実施するスキル |
| | ネットワーク機器を適切にアップデートするスキル |
| | ネットワーク機器を保守するスキル |
| | ネットワーク及び通信関連システム及び周辺機器を操作するスキル |
| | 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 |
| | ハードウェア、ソフトウェア、基幹システム等の性能を把握し、最適な設定を実施するスキル |
| | ハードウェア、ソフトウェア、基幹システム等を管理するスキル |
| | 情報システムのアップデートによる変更の情報を整理・管理し、必要に応じて変更情報を検索することができるスキル |
| | 情報システムのイベントが検知された際に手順通りに対処・報告するスキル |
| | 情報システムのインシデントが発生した際に手順通りに対処・報告するスキル |
| | 情報システムのトラブルが発生した際に手順通りに対処・報告するスキル |
| | 情報システムのパフォーマンスの低下や、トラブルが発生した場合に、原因を追究し解決するスキル |
| | 情報システムのライフサイクルに従い、情報システムの導入・運用・廃棄を実施するスキル |
| | 情報システムの監視において検知ツールを使用して異常を検知するスキル |
| | 情報システムの脆弱性を修正するスキル |
| | 情報システムを修理するスキル |
| | 情報システムを適切にアップデートするスキル |
| | 情報システムを適切にバックアップするスキル |
| | 情報システムを保守するスキル |

| | |
|---|---|
| スキル | 情報提供先のニーズを満たす有用な情報を平易な表現や適切な形式で調査報告書に記載するスキル |
| | 組織のネットワークシステムに関する構成管理を実施するスキル |
| | 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 |
| | 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 |
| | 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 |
| | 組織のポリシーや計画に沿ってアクセス制御を実施するスキル |
| | 組織の情報システムに関する構成管理を実施するスキル |
| | 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 |
| | 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 |
| | 通信関連システム及び周辺機器をインストールし、正しく設定するスキル |
| | 通信関連システム等をインストールし、正しく設定するスキル |
| | 通信障害とインシデントの切り分けの判定に必要な情報を収集し、原因を特定するスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 組織内外のステークホルダーと連携するスキル |
| | 想定読者に応じたレポートを作成するスキル |
| | セキュリティ運用においてAIを適切に活用するスキル |

# 役割の詳細：⑨教育・訓練



※ 前回からの変更箇所は赤字

| ⑨教育・訓練 | 当該役割を担う人材が所属する組織 | | | | |
|---|---|---|---|---|---|
| | 政府機関 | ユーザー企業（サプライチェーン） | | ベンダー企業 | 大学等教育機関 |
| | | 親会社等 | 子会社等 | | |
| | ○ | ○ | ○ | 教育サービス事業者 | ● |

| | | |
|---|---|---|
| 主な業務（例） | ● 組織のサイバーセキュリティ人材に係る育成・確保の方針を策定する。<br>● サイバーセキュリティ人材に対する教育の計画、実施、評価を実施する。<br>● サイバーセキュリティに関する教育や普及啓発を行う際に用いるコンテンツを作成する。 | |
| NICEフレームワークにおける対応ロール | サイバーセキュリティ人材管理 | OG-WRL-003 |
| | サイバーセキュリティカリキュラム開発 | OG-WRL-004 |
| | サイバーセキュリティ指導 | OG-WRL-005 |
| 想定される役職名等 | 講師、インストラクター、教授、研究員、研修担当　等 | |
| 補足説明 | ● 企業規模を問わず、教育・訓練を担当する人材は必要となる。講師や教材作成等を外部委託することは可能。<br>● セキュリティ担当者が担う方法と、人事部門の研修担当者等が担う方法の両方が想定される。<br>● SecBoKでは「教育・訓練」のロールに対応。<br>● 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では、「サポート教育担当」に対応。 | |

新規追加

# 役割の詳細：⑨教育・訓練



※ AI関連箇所は赤字

| | |
|---|---|
| タスク | 企業グループ等組織全体におけるサイバーセキュリティ人材に関する教育・育成計画の立案 |
| | 教育・訓練内容の計画 |
| | 委託先の選定及び委託内容の調整 |
| | 委託先とのコミュニケーションの実施 |
| | 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 |
| | 結果の評価分析と改善 |
| 知識 | 企業グループ等組織全体のサイバーセキュリティポリシーに関する知識 |
| | 企業グループ等組織全体のセキュリティ人材が担当する職務に必要な能力や資格に関する知識 |
| | 企業グループ等組織全体におけるキャリア及び人事に関する知識 |
| | 教育計画、課程およびカリキュラムの立案および管理に関する知識 |
| | 授業形態や教具に関する知識 |
| | 指導技術に関する知識 |
| | セキュリティ業務に携わる者としての倫理や法令順守に関する知識 |
| | 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 |
| | 育成対象が目標とする知識・能力に関する知識 |
| | 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 |
| | 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およびプライバシーの法規制に関する知識 |
| | 受講者の学習に対する評価に関する知識 |
| | 教育、訓練業務のプロセス全体への評価に関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

| | |
|---|---|
| スキル | 企業グループ等組織全体の目標や戦略を分析し、セキュリティ人材の教育計画を立案するスキル |
| | 企業グループ等組織全体のセキュリティ人材のキャリアパスを定義、作成するスキル |
| | 企業グループ等組織全体のセキュリティ人材が担当する職務を特定するスキル |
| | 企業グループ等組織全体の組織のセキュリティ人材が担当する職務に応じたスキルや資格の要件を策定するスキル |
| | 授業目標を設定するスキル |
| | 組織企業グループ等組織全体の組織のセキュリティ人材の技術的スキルの不足を収集、分析するスキル |
| | 教育計画、課程およびカリキュラムを策定するスキル |
| | 教材を開発または選定するスキル |
| | 実践演習に必要な環境を構築するスキル |
| | 授業形式を決定するスキル |
| | 受講者の学習を指導・ファシリテートするスキル |
| | セキュリティ業務に携わる者としての倫理や法令順守について教育するスキル |
| | 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 |
| | ネットワークおよびシステムの設計、運用について教育するスキル |
| | 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ついて教育するスキル |
| | サイバーセキュリティおよびプライバシーの法規制について教育するスキル |
| | 習熟度試験の作成および採点するスキル |
| | 受講者の学ぶ姿勢や習熟度に応じてフィードバックするスキル |
| | 教育・訓練への評価を実施し分析するスキル |
| | 教育効果を評価する基準を策定するスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 議論のファシリテ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するスキル |
| | 想定読者に応じたレポートを作成するスキル |

# 役割の詳細：⑩法務



※ 前回からの変更箇所は赤字

| ⑩法務 | 当該役割を担う人材が所属する組織 | | | |
|---|---|---|---|---|
| | 政府機関 | ユーザー企業（サプライチェーン） | | アウトソース先等 |
| | | 親会社等 | 子会社等 | **法律事務所等** |
| | ▲ | ● | ● | |

| | | |
|---|---|---|
| 主な業務（例） | ● 組織に対して、情報セキュリティに関する事項（個人情報保護等）に関連する法令等の助言を行う。<br>● 組織及び従業員のコンプライアンス意識を向上させ、社内ルール等の管理を行う。 | |
| NICEフレームワークにおける対応ロール | サイバーセキュリティに関する法的助言 | OG-WRL-006 |
| | プライバシーコンプライアンス | OG-WRL-008 |
| 想定される役職名等 | （サイバー）法務担当、リーガルアドバイザー　等 | |
| 補足説明 | ● 一般的には組織内の法務担当者がサイバーセキュリティに関する関連業務を担当する形での実施が想定される。<br>● 政府機関の“△”は政府機関全体の法務機能において当該役割を担う人材が存在することを示す。<br>● SecBoKでは「法務」のロールに対応。<br>● 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に対応する役割（担当）はなし。 | |

新規追加

# 役割の詳細：⑩法務



※ AI関連箇所は赤字

| | |
|---|---|
| タスク | 通常時・インシデント発生時の運用ルールの起案 |
| | 個人情報管理、コンプライアンス等、法的リスク分析の対象とすべき情報、サービスや、その関連法令・社内規定を取得・整理 |
| | 法的リスク（平素及びインシデント発生時）の分析と評価 |
| | リスク低減策を実施するため、法的リスク分析の評価結果を経営層/担当部門へ説明 |
| | 法的リスク分析の評価結果に基づいた組織内の規程・文書の作成、見直しと管理 |
| | 組織外の関係者対応（訴訟対応等含む） |
| | 委託先の選定及び委託内容の調整 |
| | 委託先とのコミュニケーションの実施 |
| 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 |
| | 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 |
| | リスクマネジメントに関する知識 |
| | 自組織におけるサイバーセキュリティに関する規程類（平時及びインシデント発生時に関係するもの）に関する知識 |
| | 法的リスクに対する分析・評価手法及びプロセスに関する知識（例：プライバシー影響評価（PIA）） |
| | サイバーセキュリティに関する法律についての知識<br>※平時及びインシデント発生時に関係するもの。当該業界の業法、ガイドライン等を含む。外国取引がある場合は当該国のサイバーセキュリティ関係法令も含む。 |
| | 自組織における法的助言の社内手続規程（助言ポリシーや手順、法的文書に含めるべき項目や記述ルール等）に関する知識 |
| | 外部関係者対応（行政機関、証券取引所対応、訴訟（※）対応等）において必要となる知識<br>※保有個人データ開示請求対応等を含む |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

| | |
|---|---|
| スキル | 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 |
| | 関係者（※）に法的観点からヒアリングを行うスキル<br>※親会社、子会社、所管官庁、取引先等を含む。 |
| | 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 |
| | 法的リスク分析を行い、組織内の法的リスクを明らかにするスキル |
| | 特定された法的リスクに対し、深刻度や影響の大きさ等を元に重大度をスコアリングし、スコアに基づき対応の優先順位を付けるスキル |
| | 法的リスク分析結果に基づき、サイバーセキュリティ関係法令の非専門家に対して、検討・実施すべき内容を、文書で伝えるスキル |
| | 自組織における法的文書に関し、記載すべき項目やルールに則り作成するスキル |
| | 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 |
| | 対外的に提出する法的文書（訴状、行政機関への報告、保有個人データの開示、顧客・取引先への通知・報告等を含む）に関し、記載すべき項目やルールに則り作成するスキル |
| | 想定読者に応じたレポートを作成するスキル |

# 役割の詳細：⑪監査



※ 前回からの変更箇所は赤字

| ⑪監査 | 当該役割を担う人材が所属する組織 | | | |
|---|---|---|---|---|
| | 政府機関 | ユーザー企業（サプライチェーン） | | アウトソース先等 |
| | | 親会社等 | 子会社等 | 監査法人等 |
| | ▲ | ● | ● | |

| | | |
|---|---|---|
| 主な業務（例） | ● 運用管理から独立した立場から、組織やシステムを対象とするリスク評価を行う。<br>● 情報セキュリティ監査及びシステム監査を行う。<br>● 情報セキュリティ監査及びシステム監査後の改善計画の作成・助言、改善活動の実施・助言を行う。 | |
| NICEフレームワークにおける対応ロール | 技術プログラム監査 | OG-WRL-016 |
| | セキュリティ管理策評価 | OG-WRL-012 |
| 想定される役職名等 | 情報セキュリティ監査人、情報セキュリティ監査技術者、セキュリティアセッサー、セキュリティ監査担当　等 | |
| 補足説明 | ● 監査目的に応じて、内部監査と外部監査の2種類の方法を使い分けることが想定される。<br>● 経済産業省の情報セキュリティサービス審査登録制度における「情報セキュリティ監査サービス」に従事する人材に相当。<br>● 政府機関の“▲”は政府機関全体の監査機能において当該役割を担う人材が存在することを示す。<br>● SecBoKでは「監査」のロールに対応。<br>● 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では、「監査責任者」、「監査担当」の役割・担当に対応。 | |

新規追加

# 役割の詳細：⑪監査



※ AI関連箇所は赤字

| | |
|---|---|
| タスク | 監査計画の作成 |
| | 監査の準備 |
| | リスクアセスメントの実施 |
| | 監査の実施 |
| | 監査結果の評価 |
| | 監査報告書の作成・共有 |
| | 改善計画の作成 |
| | フォローアップ監査の実施 |
| | 委託先の選定及び委託内容の調整 |
| | 委託先とのコミュニケーションの実施 |
| 知識 | 監査プロセスに関する知識 |
| | 監査基準に関する知識 |
| | 監査人倫理規定及び一般道徳に関する知識 |
| | リスクマネジメントに関する知識 |
| | 監査対象組織のサイバーセキュリティポリシーや法規制に関する知識 |
| | プライバシーとデータ保護に関する知識 |
| | ネットワークとインフラストラクチャに関する知識 |
| | 調達とサプライチェーンに関する知識 |
| | システムとアーキテクチャに関する知識 |
| | 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 |
| | 監査ツール及び手法に関する知識 |
| | 監査における国際標準等やベストプラクティスに関する知識 |
| | 評価ツールと評価の手法に関する知識 |
| | 監査報告書に関する知識 |
| | 報告書共有の手順・関係者に関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

| | |
|---|---|
| スキル | 監査計画を作成し、監査対象と調整するスキル |
| | 監査基準に基づき監査項目を作成するスキル |
| | リスクアセスメントを実施するスキル |
| | 監査項目から、事前確認が必要な証跡と現地で確認する証跡を区別するスキル |
| | 独立した立場で高い倫理観を保持して監査業務を実施するスキル |
| | 監査対象組織が定めたセキュリティポリシーの要件や運用状況の適合性を判断するスキル |
| | 管理策の実施状況やプロセスを分析し、セキュリティ要件の適合性を判断するスキル |
| | ネットワークシステムやインフラストラクチャの構成や運用状況が適切であることを判断するスキル |
| | ログを確認し、セキュリティ要件に適合していることを判断するスキル |
| | システムやソフトウェアの構成がセキュリティ要件に適合していることを評価するスキル |
| | 脆弱性評価等の結果から監査対象機器の脆弱性を認識するスキル |
| | 国際標準等やベストプラクティスへの適合性を評価するスキル |
| | 評価ツールを使用して適切な評価を実施するスキル |
| | 監査対象に対する個別の監査結果を踏まえ、セキュリティ要件への適合性を総合的に評価するスキル |
| | 評価から監査結果の結論を導出し、監査報告書にまとめるスキル |
| | 監査結果に対して、改善計画の作成や改善の助言を実施するスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 議論のファシリテーションを行うスキル |
| | 想定読者に応じて適切な表現や形式のレポートを作成するスキル |
| | 目的に応じたインタビューを行うスキル |

# 役割の詳細：⑫設計開発



※ 前回からの変更箇所は赤字

| ⑫設計開発 | 当該役割を担う人材が所属する組織 | | | | |
|---|---|---|---|---|---|
| | 政府機関 | ユーザー企業（サプライチェーン） | | ベンダー企業（アウトソース先等） | |
| | | 親会社等 | 子会社等 | セキュリティベンダー | 運用保守事業者 |
| | ○ | ○ | ● | ○ | ○ |

**主な業務（例）**

- 新規又は更新するサービス・製品案の検討にあたり、望ましいアーキテクチャとその潜在的なリスクを想定した上で、リスクへの対処のために備えるべきセキュリティ機能の設計を行う。
- 整理した内容を元に、情報システム等の要件定義、設計、開発、テスト、評価を行い、サービス・製品等を実用化する。
- 「セキュリティ・バイ・デザイン」の考え方に則り、システム開発の企画段階からセキュリティを実装する。
- 自組織で発見された脆弱性に対する修正プログラムを作成する。

**NICEフレームワークにおける対応ロール**

| | |
|---|---|
| サイバーセキュリティアーキテクチャ | DD-WRL-001 |
| エンタープライズアーキテクチャ | DD-WRL-002 |
| セキュアなソフトウェア開発 | DD-WRL-003 |
| セキュアなシステム開発 | DD-WRL-004 |
| ソフトウェアセキュリティ評価 | DD-WRL-005 |
| システム要件計画 | DD-WRL-006 |
| システムテストと評価 | DD-WRL-007 |

**想定される役職名等**

セキュリティアーキテクト、セキュリティエンジニア、システムエンジニア、テスター　等

**補足説明**

- 情報システム・サービスの設計開発の一連のプロセスのうち、企画段階を担う人材から最終テストを担う人材までを含む。
- SecBoKでは「セキュリティ設計」、「開発」のロールに対応。
- 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では、「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」等に対応。

新規追加

# 役割の詳細：⑫設計開発



※ AI関連箇所は赤字

| | |
|---|---|
| **タスク** | 要件定義 |
| | 予算計画の立案・調達 |
| | 委託先の選定及び委託内容の調整 |
| | 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アーキテクチャの検討 |
| | 設計 |
| | 開発・実装 |
| | テスト |
| | リリース |
| | 運用保守 |
| **知識** | 組織の抱えるシステム上におけるサイバーセキュリティの課題に関する知識 |
| | 要件定義書に記載すべき項目に関する知識 |
| | サイバーセキュリティ機能の実装に掛かる費用に関する知識 |
| | サイバーセキュリティに関するサービス、機器の機能に関する知識 |
| | 基本設計書に記載すべき項目に関する知識 |
| | 詳細設計書に記載すべき項目に関する知識 |
| | コーディング、統合、内部デプロイ等実装に関する知識 |
| | テスト手法及び手順に関する知識 |
| | リリースの手順に関する知識 |
| | 組織の情報システムに関する知識 |
| | 情報システムの変更管理に関する知識 |
| | 情報システムの障害に関する知識 |
| | 情報システムに対する攻撃に関する知識 |
| | 情報システムの復旧方法に関する知識 |
| | OTにおける脅威と対策に関する知識 |
| | 制御システムにおける脅威と対策に関する知識 |
| | OTを対象とする管理ツールに関する知識 |
| | クラウドサービスの種類と責任分界に関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |
| | AI開発において考慮すべきセキュリティに関する知識 |

| | |
|---|---|
| **スキル** | 関係者へヒアリングを行い、システム上のサイバーセキュリティにおける課題を整理するスキル |
| | 設計フェーズに有用な情報を平易な表現や適切な形式で要件定義書に記載するスキル |
| | 要件定義書の作業内容から必要な工数と費用をプロジェクト管理担当者と調整するスキル |
| | 要件定義書で定義された内容を達するためシステムへ実装する機能を具体化、明確化するスキル |
| | OT環境の特徴を踏まえた設計を行うスキル |
| | 実装フェーズで有用な情報を平易な表現や適切な形式で詳細設計書に記載するスキル |
| | 基本、詳細設計書で定められている要求を満たす機能を備えた新たなプログラムを作成、又は既成品を選定し、システムに実装するスキル |
| | 設計書などを元にテスト範囲や評価基準等を決定し、テスト計画書を作成するスキル |
| | テスト計画書やシステムの特性からテスト手法を決定し、テストのための環境設計及び構築を行うスキル |
| | テストを実施、結果を評価し、結果に基づく改善活動を行うスキル |
| | 実装する機能を現場との調整の上段階的に実装するスキル |
| | システムが正常に作動するかどうかを定期的に把握しトラブルを早期に発見するスキル |
| | システムにトラブルや不具合が発生した際に対応及びアップデートなどシステム変更の必要が発生した場合の変更作業を行うスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 組織内外のステークホルダーと連携するスキル |
| | 想定読者に応じたレポートを作成するスキル |
| | 目的に応じたインタビューを行うスキル |
| | セキュア設計構築においてAIを適切に活用するスキル |

# 役割の詳細：⑬研究



※ 前回からの変更箇所は赤字

| ⑬研究 | 当該役割を担う人材が所属する組織 | | | | | |
|---|---|---|---|---|---|---|
| | 政府機関 | 大学等教育機関 | ユーザー企業（サプライチェーン） | | ベンダー企業（アウトソース先等） | |
| | | | 親会社等 | 子会社等 | セキュリティベンダー | 運用保守事業者 |
| | ● | ● | ○ | ● | ○ | ○ |

| | | |
|---|---|---|
| 主な業務（例） | ● サイバーセキュリティに関する先端技術の研究を行う。<br>● 共同研究や技術指導等、研究分野以外の人材と連携し、サイバーセキュリティ分野の課題解決や新たな取組の実現や実用化を支援する。<br>● 技術ロードマップを作成する。<br>● 研究活動を通じてサイバーセキュリティ分野で高度な知見やスキルを有する人材を育成する。<br>● サイバーセキュリティに関する学会やコミュニティ活動に参加する。 | |
| NICEフレームワークにおける対応ロール | 技術研究開発 | DD-WRL-008 |
| 想定される役職名等 | 教授、講師、研究員、R&D担当　等 | |
| 補足説明 | ● SecBoKに対応するロールはなし。<br>● 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に対応する役割（担当）はなし。 | |

新規追加

# 役割の詳細：⑬研究



※ AI関連箇所及び新規追加項目は赤字

| | |
|---|---|
| タスク | 自組織内/外におけるサイバーセキュリティに係る課題の把握 |
| | 研究テーマ及び研究目的・目標の決定 |
| | 先行研究の調査（研究計画作成に資する情報収集） |
| | 研究計画書の作成 |
| | 関連情報の収集（研究実施に必要な情報収集） |
| | 仮説の立案 |
| | 仮説の検証 |
| | 検証結果の評価 |
| | 新方式の提案 |
| | 設計開発担当者等と研究成果の連携 |
| | 学会やコミュニティ活動への参加 |
| 知識 | 組織のサイバーセキュリティ関係部署に関する知識 |
| | 組織の掲げるサイバーセキュリティのあるべき姿に関する知識 |
| | 研究対象の優先順位付けに関する知識 |
| | サイバーセキュリティの研究領域における情報源に関する知識 |
| | サイバーセキュリティ領域の最先端技術に関する知識 |
| | 研究計画書に含めるべき項目に関する知識 |
| | 情報収集のツール、手法及びプロセスに関する知識 |
| | 仮説立案の手法・手順に関する知識 |
| | 仮説検証の手法・手順に関する知識 |
| | 研究結果に対する評価基準及び手法に関する知識 |
| | 研究結果の提案に関する知識 |
| | 研究結果共有の手順に関する知識 |
| | 研究結果報告書等に含めるべき項目に関する知識 |
| | 外部AIサービスを利用する場合の情報保護に関する知識 |
| | AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 |
| | セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識 |

| | |
|---|---|
| スキル | 「情報収集・共有・分析」など関係者へヒアリング等を行い、組織内外におけるサイバーセキュリティに係る課題を把握するスキル |
| | 組織のあるべき姿に適合する研究目的・目標を決定するスキル |
| | 研究対象の中から組織の目的、目標等を鑑み優先順位を付けるスキル |
| | 様々な情報源から研究テーマに対する先行研究を調査し、既存の研究で明らかになっていない事項を導出するスキル |
| | 研究の目的や具体的な研究内容、研究手法、期間等を記載した研究計画書を作成するスキル |
| | 膨大な情報源から実績や発行元等の情報を参考に信頼できる情報源を特定するスキル |
| | 研究テーマの内容に合った最適なツールを使用し、関連する情報を収集するスキル |
| | 研究テーマに対する仮説を先行研究から導出するスキル |
| | 立案した仮説を調査に基づいた実験などを通し、検証するスキル |
| | 研究結果を評価し、研究計画書に記載した研究目的を達することが出来ているかを判断するスキル |
| | (実施した研究が基礎研究であった場合)研究結果が実用化等の発展可能性を判別するスキル |
| | 研究結果を既存の仕組みを改善、刷新する形で提案を行うスキル |
| | 設計開発担当者のニーズを満たす有用な情報を平易な表現や適切な形式でレポートを作成するスキル |
| | 関係者と適切なコミュニケーションを行うスキル |
| | 組織内外のステークホルダーと連携するスキル |
| | 想定読者に応じたレポートを作成するスキル |

# （参考）他の人材フレームワークとの対応関係



※ 前回からの変更箇所は赤字

| | 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）<br>デジタル経営（CIO/CDO）<br>企業経営（取締役）<br>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<br>セキュリティ統括 | CISO、CRO、CIO等<br>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<br>デジタルシステムストラテジー<br>経営リスクマネジメント<br>事業ドメイン（生産現場・事業所管理） | セキュリティ統括<br>プロジェクト管理<br>社内外調整 | サイバーセキュリティ統括<br>ISMS担当<br>個人情報取扱責任者/担当<br>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<br>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<br>情報システムペンテスター<br>IoTデバイス脆弱性診断士<br>IoTシステムペンテスター<br>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<br>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<br>監視・運用 | システム管理者、ネットワーク管理者<br>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<br>デジタルプロダクト開発 | セキュリティ設計<br>開発 | セキュリティ設計担当<br>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<br>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 | | | |

国家サイバー統括室

# 手引き書（案）の
# 進捗状況について

# 手引き書（案）の基本的考え方（概要）



**目的**

サイバーセキュリティ対策を担う人材に関する「採用」、「教育」、「評価」等の場面における人材フレームワークの活用を促進する。

**位置づけ・運用方針**

- ■ 採用、配置、育成、評価等あらゆる場面で、人材フレームワークに基づき円滑な人材育成・確保を図るための補助資料（ガイドライン的な位置づけ）。
- ■ 自組織の実情に応じて、柔軟に活用できるものとする。
- ■ 利用者からのフィードバックや技術トレンド等の情勢の変化を踏まえ、継続的に改善を図る。

**作成方針・スケジュール**

- □ 利用主体ごとに求める使い方が異なるため、**分冊形式で整理**する。
- □ 専門知識を有しない読者も想定し、専門用語等の使用を極力避け、**平易な表現で記述**を行う。
- □ 他機関が公表する資料等も参照し、読者にとって負担の少ない**分量の適正化**を図る。
- □ 年度内に案を作成し、８年度以降速やかな公開の上、具体的活用事例をもとに、より現場に即したものとなるよう改善を図る。

**対象範囲・記載方針**

| | |
|---|---|
| ① 小規模組織 | 必要な体制整備の検討と、それに基づく内部人材育成・確保等に役立つ活用方法等を示す。 |
| ② 大規模組織 | 採用時の職務定義、その後の育成・評価等に役立つ活用方法等を示す。 |
| ③ 教育機関 | 専門教育カリキュラムの検討・立案等に役立つ活用方法等を示す。 |
| ④-1 個人（専門人材） | 目指すキャリアの実現のために習得すべき知識・スキルの把握等に役立つ活用方法等を示す。 |
| ④-2 個人（プラス・セキュリティ人材） | 実務上最低限必要な知識・スキルの習得に役立つ活用方法等を示す。 |

# 手引き書（案）の構成イメージ



※前回からの変更箇所は赤字

手引き書は、利用主体に共通する事項と、主体ごとの固有事項を分けて構成する。

| 共通事項 | |
|---|---|
| ● サイバーセキュリティ人材フレームワークの概要<br>策定背景及び定義する「役割」の全体像等について<br>● サイバーセキュリティ人材フレームワーク本体の構成<br>● 手引き書の概要<br>位置づけや手引き書で具体化する「人材像」の概念について　等 | |
| **利用主体別固有事項** | |
| ① 小規模組織<br>例：中小企業、小規模自治体 等 | ● 小規模組織におけるセキュリティ対策の考え方（役割に基づく体制の一例等）<br>● モデルケースに基づく活用例　等 |
| ② 大規模組織<br>例：中堅・大企業、政府機関 等 | ● 担当者を採用するときの職務記述書の作成方法<br>● レベルを踏まえた人事評価等にあたっての活用方法　等 |
| ③ 教育機関<br>例：大学、教育事業者 等 | ● 輩出したい人材像を定めて、知識・スキルを段階的に習得するためのカリキュラムの作り方（作成にあたっての考え方）　等 |
| ④−1 個人（専門人材）<br>例：専門人材、専門人材を目指す学生等 | ● 専門人材に求められるスキルセットを踏まえたセルフアセスメントの実施方法<br>● スキルギャップを埋めるための学習方法　等 |
| ④−2 個人（プラス・セキュリティ人材） | ● 各役割の概要<br>● プラス・セキュリティ人材に求められるスキルセットを踏まえたセルフアセスメントの実施方法<br>● スキルギャップを埋めるための学習方法　等 |

新規追加

# ① 小規模組織向け手引き書の作成方針案（骨子案）

**方針概要**

- セキュリティの専門人材を十分に確保することが困難である状況を前提に、必要な体制を可視化した上で、役割分担等を検討し、「人材像」として具体化。
- イメージとして分かりやすく示すため、次の3つのモデルケースにおける活用例を記載。
  うち【ケース1】を主として説明しつつ、他のケースで異なる対応が必要な場合を示す。

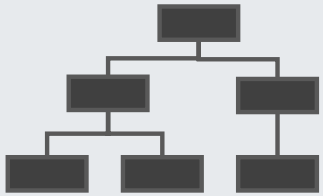
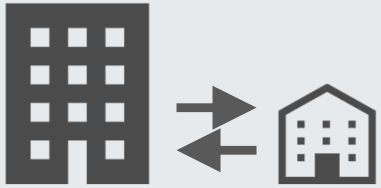
| | 【ケース１】 | 【ケース２】 | 【ケース３】 |
|---|---|---|---|
| **サイバーセキュリティ対策における悩み** |  <br>サイバーセキュリティ対策はこれまで外部業者に任せており、「自組織でやるべきこと」をあまり意識できていなかった。 |  <br>取引先から経済産業省の「セキュリティ対策評価制度」への対応を要求されているが、どうすればよいかわからない。 |  <br>サイバーセキュリティ対策は代表者が実質一人ですべて対応しているが、やるべきこと（タスク）が何かを把握したい。 |
| **想定する企業属性** | ● 従業員8名<br>● 小売業（ネット販売）<br>● 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30名<br>● 製造業（部品製造）<br>● 「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。<br>● 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）<br>● サービス業（デザイナー） |

新規追加

# ② 大規模組織向け手引き書の作成方針案（骨子案）

**方針概要**

- セキュリティ体制がある程度構築されていることを前提に、より効果的・効率的に人材育成・確保（採用）を行うための活用例を示す。
- レベルに応じた評価に関する内容は大規模組織向けのみで詳細を記載するため、必要に応じ、他の利用主体が参照できるよう、汎用性のあるものとして記載。

| 自社に適したガバナンスの検討 | サプライチェーン委託先管理 | 職務記述書の作成 | 人材の評価 |
|---|---|---|---|
|  |  |  |  |
| 自社の特徴に相応しいセキュリティガバナンスの体制の考え方例示ともに示す。 | 委託先において必要最低限のセキュリティ対策を行うために、求められるタスクや教育方法などのノウハウを示す。 | 人材募集において、ミスマッチを防ぐ観点で、応募者が興味をもつような職務記述書の考え方について示す。 | レベルを踏まえた人材の評価にあたって留意すべき内容を示す。 |

新規追加

# ③ 教育機関向け手引き書の作成方針案（骨子案）



**方針概要**

**既存のカリキュラム指標などを基礎としながら、現在実務で活躍しているセキュリティ人材へのアンケートなどを通じて社会ニーズ等を踏まえた教育関係者によるカリキュラム・シラバス等の検討に資する次のような考え方を示す。**

- 人材フレームワークや小規模・大規模組織向け手引き書等を踏まえて、社会においてどういった人材が求められているかを示す。
- 上記の可視化を踏まえて、教育機関等においてはどういった人材を育成していくべきか、またそれらを実現するためにどういった教育カリキュラムの設計が必要となるかという点について、考え方を示す。
- 教育カリキュラム等の設計において、自組織での教育リソースを踏まえて、不足するより専門的な要素を補うための一つの事例として、外部講師の招聘なども含めたより実践的なカリキュラム設計に関する工夫の一例を示す。

| | セキュリティ人材に関する社会のニーズ | カリキュラムを作るための考え方 | 学ぶべき内容を充足するための工夫例 |
|---|---|---|---|
| **項目** |  <br>セキュリティ人材のニーズの種類や傾向 |  <br>サイバーセキュリティに関するカリキュラムを設計する際の考え方や参考情報 |  <br>自組織のリソースを踏まえた、より専門的なカリキュラム構築のための工夫 |
| **具体的内容** | ● それぞれの役割において、フレームワークで定義されたTKSや各種組織向け手引き書等の内容を踏まえた、セキュリティの人材に対する社会からのニーズ | ● 既存のカリキュラム指針等や、左記社会ニーズを踏まえた、カリキュラム設計に関する考え方 | ● 不足している専門領域に対する外部講師の活用や選定の考え方<br>● 他大学や企業、地域コミュニティ等との連携による教育リソースの補完の案 |

# ④-1 個人（専門人材）向け手引き書の作成方針案（骨子案）

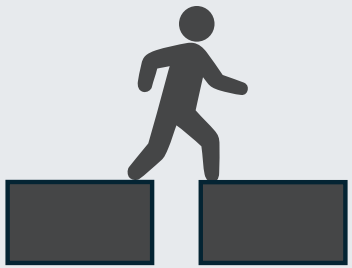


新規追加

**方針概要**

**今後サイバーセキュリティの専門人材として活躍したい人材への参考情報として、次のような内容を示す。**

- セルフアセスメントを踏まえて、明らかとなるスキルギャップについて、現場で実践されている学習方法や経験の積み方（OJT、競技会等）による解消方法の事例を示す。
- 参考として実際の専門人材の経験に基づくキャリアパス事例（マネジメント、技術スペシャリスト等）を示す。

| | セルフアセスメントの方法 | スキルアップとキャリア形成のアプローチ | 専門人材の例（本手引書の対象） |
|---|---|---|---|
| **項目** |  目指す役割に応じて、自身の現状を客観的に評価する観点を整理する |  不足している能力を補うための具体的なアクションプラン |  専門人材のモデルケース |
| **具体的内容** | ● フレームワークを用いて自身の役割を把握する方法<br>● ツールを活用した自己採点の例 | ● モデルとなる専門人材が実践してきた学習方法や経験の積み方の一例（OJT、競技会等） | ● 高度技術者、マネジメント層、研究者等の多様なキャリアの事例 |

# ④-2 個人（プラス・セキュリティ）向け手引き書の作成方針案（骨子案）

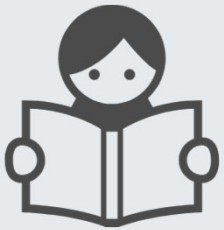


新規追加

**方針概要**

**本来業務にプラスして、習得することが望ましい知識・スキルについて、既存のツール等を活用して確認・習得する方法を提示する。**

- 自身の業務において付加的に求められるタスクとスキルを例示する。

| | 業務に付加すべきセキュリティ知識・スキル | セルフアセスメントと学習方法 |
|---|---|---|
| **項目** |  <br>プラスセキュリティ人材の職務イメージ |  <br>自身の現状評価の方法と学習プランの立て方 |
| **具体的内容** | ● 本来業務（総務、営業、経理等）を遂行する上で、プラスして求められるセキュリティ知識・スキルの例 | ● アセスメントで不足と評価した項目の学習方法<br>● 各種既存資格の活用例 |

国家サイバー統括室

# 小規模組織向け手引き書（案）は資料４（別紙）参照