日本のサイバーセキュリティを「連携」「学び」「創造」

セキュリティ知識分野（SecBoK）人材スキルマップ 2025年版

～新たな時代のセキュリティ人材へ対応～

JNSA教育部会
SecBoK2025改定委員会

Copyright 2025 NPO日本ネットワークセキュリティ協会

SecBoK2025改定委員会

DX with Cybersecurity時代におけるセキュリティ人材の求められる役割の変化への対応

Copyright 2025 NPO日本ネットワークセキュリティ協会

セキュリティ知識分野（SecBoK）とは

JNSA教育部会では、独立行政法人情報処理推進機構（IPA）からの委託事業の実施を契機として、情報セキュリティに関する業務に携わる人材が身につけるべき知識とスキルを体系的に整理した「情報セキュリティスキルマップ」の作成に2003年度から取り組んでいます。2007年からは名称を「セキュリティ知識分野SecBoK（Security Body of Knowledge）」と改め、2016年以降は定期的に改定を行っています。

現行公開版SecBoK2021は、セキュリティ関連業務に従事する人材に求められる1000を超える知識項目の集合になります。多くの方に利用いただけるように、大項目・中項目といった構造化された構成となっており、あわせて下記も提示しています。

・想定している「セキュリティ関連業務」の分類（ロール・役割）を提示
・各ロールとそれに要求される/会得しているべき知識項目との対応を提示

今回SecBoKが参照している米国NISTのNICEフレームワークがv2.0.0へ移行したことに伴う影響と変更、またDX with Cybersecurity時代におけるセキュリティ人材の求められる役割の変化などについて、有識者委員による改定委員会を組織し、そこでの議論をまとめ、「SecBoK2025」として最新の改訂版を公開することとなりました。

Copyright 2025 NPO日本ネットワークセキュリティ協会

SecBoK2025改定委員会　委員

所属・役職	氏名（敬称略）	備考
株式会社トライコーダ	上野　宣	日本セキュリティオペレーション事業者協議会（ISOG-J）
立命館大学	上原　哲太郎	学識有識者
木更津工業高等専門学校	歸山　智治	KOSENサイバーセキュリティ教育推進センター（K-SEC）
順天堂大学	加藤　雅彦	学識有識者
九州大学情報基盤研究開発センター	小出　洋	SECurity CONtest（SECCON） 成長分野を支える情報技術人材の育成拠点の形成（enPiT）
ＮＲＩセキュアテクノロジーズ株式会社	近藤　有馬	セキュリティ業界専門家
グローバルセキュリティエキスパート株式会社	髙﨑　庸一	日本サイバーセキュリティ人材キャリア支援協会（JTAG）
東京電機大学	寺田　真敏	日本シーサート協議会（NCA） 国際化サイバーセキュリティ学特別コース（Cysec）
ＮＲＩセキュアテクノロジーズ株式会社	時田　剛	セキュリティ業界専門家
ＧＯＦＵ株式会社	萩原　健太	ソフトウェア協会（SAJ）
株式会社ラック	長谷川　長一	JNSA教育部会
情報セキュリティ大学院大学	福井　　将樹	学識有識者
株式会社ラック	持田　啓司	情報セキュリティ教育事業者連絡会（ISEPA）
情報経営イノベーション専門職大学	平山　敏弘	JNSA教育部会 部会長
JNSA事務局長	下村　正洋	JNSA事務局長
みずほリサーチ＆テクノロジーズ株式会社	冨田　高樹	事務局

SecBoK2025の特長

「粒度」「役割（ロール）」「使い方（使われ方）」
の視点からの検討

Copyright 2025 NPO日本ネットワークセキュリティ協会

SecBoK 2025の方向性について（粒度）

【現状版は細かすぎる】

- SecBoKやNICEフレームワークは、粒度が細かすぎて使いにくいという意見を色々聞くので、どのくらいの抽象度にするかは検討し直したほうがよい。

【粗くしない方がよい】

- ジョブディスクリプションで使ったり、互いの共通言語として使ったりするとき、ロールを大括りにすると職種との対応がわかりにくく、お互いの誤解を生みやすいなどがあるため。

【細かいものと詳しいものの両方が欲しい】

- 細かいとパッと見たいときに使いにくいが、個々に参照したい場合には詳細が欲しいので、両方あるとよい。
- CSIRTをこれから作りたい顧客からは「SecBoKは細かすぎて諦めた」と言われる。一方既存のCSIRTで一部作業を外部委託から内製に切り替えるためにロールをピンポイントで増やしたいような場面ではSecBoKが役に立つと言われる。

Copyright 2025 NPO日本ネットワークセキュリティ協会

SecBoK 2025の方向性について（役割（ロール））

【役割（ロール）について】

- 一般に使われているロールや名称はまちまちなので、そのあたりをうまく吸収できるとよい。改訂されたNICEフレームワークを見たが、そのまま使ってしまうと日本ではなじみのないロール名が多い印象である。まずは見せ方を工夫しないと使われないのではないか。

- DX推進スキル標準では技術とマネジメントに分かれているが、非技術の役割にはマネジメント以外のもの色々あるのでマネジメントに限らない名称がよい。

- 従来のSecBoKは、人材像（モデル）なのか、ロール（役割）なのかと問われることもあったので、SecBoK2025においては、もう一度ロール（役割）であると明確に位置付けて、定義を行なった。

- 従来のSecBoKにおけるロールは、作成当時は役割が明確であったCSIRTでのロールを意識したものであったが、現在のセキュリティは従来の守りに加えて、DXを推進する役割なども担っているため、ロールの再編成を行なった。

Copyright 2025 NPO日本ネットワークセキュリティ協会

SecBoK 2025の方向性について（使い方（使われ方））

【使い方（使われ方）】

- 海外で使われていることを踏まえると、ドラスティックに変えると影響が大きくなるため、ある程度キープコンセプトで「これはBoKであり辞書である」というところからぶれないほうがよい。学から見たとき、技術の種類がこれだけあるというのがわかりやすいし、あてはめやすい。

- BoKはBoK（Body of Knowledge：知識分野）としてあくまで細かさを維持しつつ、モデルケースのようなものを作り、その際にCSIRT関連をまとめるなどしてDX推進標準のようなことをやりたければ参考にしてくださいというのを作ってはどうか。

- ジョブディスクリプションに基づいた求人募集などの際に、書きやすい内容であると便利で活用されるのではないか。

Copyright 2025 NPO日本ネットワークセキュリティ協会

SecBoK2025の特長

検討結果を受けての方向性

Copyright 2025 NPO日本ネットワークセキュリティ協会

粒度についての方向性
粒度に応じた用途

	知識・スキル項目	ロール・職種
粒度が 粗いもの	●初学者・エントリー向け ●学生に学習目標を示す ●ざっくり把握したい場合	●職種との対応付けを行う
粒度が 細かいもの	●自社にロールを新規作成する ●学生に個別内容を指導する ●細かく参照したい場合	●ジョブディスクリプションを作成する ●共通言語としての利用

Copyright 2025 NPO日本ネットワークセキュリティ協会

粒度についての方向性

- 現状は細かすぎる？粗くしない方がよい？

【細かいので、もう少し大括りに】

- 細かすぎて使いにくいという意見を聞く
- ロールを誰が使うかを考えたとき、細かいものだけがあっても使いにくい
- NICEフレームワークとの対応表を作るのであれば、職種との対応であまり細かくないものが欲しい
- 英語の勉強でいきなり辞書を開くことはない。国語辞典に対する図鑑に相当するような、初学者向け、エントリー向けドキュメントがあるとよい。

【あまり束ねないで】

- ロールを束ねて大きくすると、ジョブディスクリプションを書きにくくなる
- ロールを大括りにするとお互いの誤解を生みやすい。

「細かすぎる」や、逆に「粗くしない方がよい」など双方の意見があるため、スキル項目としては、現状レベルのものでよいが、使い勝手を良くするために下記の点を中心に、SecBoK2025として見直しを行う。

・ロールの再編成（数は現状以上は増やさない）
・スキル項目の数は減らさないが、カテゴリーについては再編成

Copyright 2025 NPO日本ネットワークセキュリティ協会

役割（ロール）について
現状ベースの統合・分割

現行SecBoK2021は、CSIRTのロールを強く意識していた部分もあったため、細かく分かれているロールもあった。一方、大括りにまとめられてしまっているロールもあったため、より分かりやすくするため、分割した方がよいロールも出てきた。

【統合するもの】
- POC、ノーティフィケーション
- コマンダー、トリアージ
- インシデントマネージャー、ハンドラー
- リサーチャー、キューレター
- セルフアセスメント、ソリューションアナリスト

【分割するもの】
- セキュリティ戦略・対策方針
- セキュリティPM
- セキュリティインフラエンジニア
- セキュリティ運用

Copyright 2025 NPO日本ネットワークセキュリティ協会

役割（ロール）について
他のフレームワークや職業分類との連携

下記等のセキュリティ人材フレームワークでの人材モデル・ロールや職種分類などとも意識して、新たなSecBoKの役割（ロール）の作成を行なった。

１．NICEフレームワークの新たなカテゴリーなどとの整合性も意識
セキュリティデザインやアーキテクチャー、およびセキュリティマネジメント領域への対応などを検討。

２．ITSS+セキュリティで定義されている、特にセキュリティ区分の分野との連携を意識
例えば、セキュリティ統括、リスクマネジメント、プロダクト開発などの役割を意識。

３．職業サイトとの連携も意識
職業情報提供サイト（日本版O-NET）収録職業一覧や、本家米国のO*NET（Occupational Information Network）との連携も意識。

４．米国でのサイバーセキュリティ分野の主要な職種も参考に
米国のサイバーセキュリティ分野における人材の需要と供給に関する、詳細なデータを提供するオンラインサイトであるCyberSeekにおいて分類されている主要な職種についても参考に。

Copyright 2025 NPO日本ネットワークセキュリティ協会

SecBoK2025

SecBoK2025の新たな15ロール（役割）

Copyright 2025 NPO日本ネットワークセキュリティ協会

新SecBoK2025ロール（役割）

ロール（役割）		ロール概要
1	セキュリティ経営、 意思決定・戦略策定	社内の情報セキュリティ全体を統括する責任者。組織のサイバーセキュリティ戦略やポリシーなどを策定する。また組織のサイバーセキュリティに係る予算を確保し、組織体制の構築などを行なう。
2	セキュリティ統括	企業の情報セキュリティ対策を組織横断的に統括し、CISOや経営層が意思決定する際の支援を行う。具体的には、セキュリティ戦略の策定、リスク管理、インシデント対応などを担当する。
3	プロジェクト管理	セキュリティ関連の新規システム開発・構築および社内施策プロジェクトにおいて、目標・計画の策定、プロジェクト体制の整備、進捗管理、資産・予算管理などの各種プロジェクト管理業務を実施する。
4	セキュリティ設計	「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。具体的には、セキュリティを確保するためのシステムの要件定義、アーキテクチャ設計、セキュアソフトウェア方式設計、テスト計画などを行なう。
5	開発	「セキュリティ・バイ・デザイン」の考え方に則り、システム開発の段階からセキュリティを実装する。また自組織で発見された脆弱性に対する修正プログラムの作成なども行なう。
6	システム管理・ネットワーク管理	システム設計や構築を担当する。また設計・開発時には、チームメンバーと連携し、システムおよびネットワーク運用・保守に係る作業内容などを記載した運用・保守計画を作成する。
7	監視・運用	各種機器のログの監視、保管、分析などを行ないセキュリティ監視を実施する。セキュリティインシデントを検知した際は、関係各所へ連絡して連携する。また監視ツールの運用、保守を行う。
8	監査	情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、セキュリティリスク評価に基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、もって保証を与えあるいは助言を行う。
9	脆弱性診断・評価	現在の状況とTobe像のFit&Gapからリスク評価を行い、ソリューションマップを作成して導入を推進する。導入されたソリューションの有効性を確認し、改善計画に反映する。また平常時には脆弱性診断・評価などを行う。インシデント対応時には脆弱性の分析、影響の調査などに対応する。
10	教育・訓練	社内のリテラシーの向上、底上げのための教育及び啓発活動を行う
11	法務	システムにおいてコンプライアンス及び法的観点から遵守すべき内容に関する橋渡しを行う。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）に関連する法令などの助言を行う。組織及び従業員のコンプライアンス意識を向上させ、社内ルールなどの管理を行う。

新SecBoK2025ロール（役割）

ロール（役割）		ロール概要
12	対処（インシデントハンドリング）	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。具体的には、セキュリティインシデント発生時、インシデントへの対応を行い、影響の拡大を防止すると共に、インシデントの対応状況を把握する。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。
13	脅威・脆弱性情報収集	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。具体的には、セキュリティインシデント発生時、インシデントへの対応を行い、影響の拡大を防止すると共に、インシデントの対応状況を把握する。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。
14	社内外調整	社外向けではJPCERT/CC、NCO、警察、監督官庁、NCA、他CSIRTなどとの連絡窓口、社内向けではIT部門調整担当社内の法務、渉外、IT部門、広報、各事業部などとの連絡窓口となり、それぞれ情報連携を行う。また組織内を調整し、社内各関連部署への情報発信を行う。社内システムに影響を及ぼす場合にはIT部門と調整を行う。
15	インシデント調査・分析	システム的な鑑識、精密検査、解析、報告を行う。悪意のある者は証拠隠滅を図ることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求される。 また外部からの犯罪、内部犯罪を捜査する。セキュリティインシデントはシステム障害とは異なり、悪意のある者が存在する。通常の犯罪捜査と同様に、動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に捜査対象を絞っていくことが要求される。

Copyright © 2025 Japan Network Security Association

参考資料

参考：プラス・セキュリティ		概要
16	サイバーセキュリティマネージャー	顧客価値を拡大するビジネスの企画立案に際して、デジタル活用に伴うサイバーセキュリティリスクを検討・評価するとともに、その影響を抑制するための対策の管理・統制の主導を通じて、顧客価値の高いビジネスへの信頼感向上に貢献する。
17	サイバーセキュリティエンジニア	事業実施に伴うデジタル活用関連のサイバーセキュリティリスクを抑制するための対策の導入・保守・運用を通じて、顧客価値の高いビジネスの安定的な提供に貢献する。

SecBoK2025のロール（役割）には入らないが、参考資料として、プラス・セキュリティ人材も参考ロールとして掲載します。
プラス・セキュリティ人材については、DX推進人材（デジタルスキル標準にある）「サイバーセキュリティマネージャー」と「サイバーセキュリティエンジニア」の名称をそのまま使用しています。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

1．セキュリティ経営、意思決定・戦略策定

社内の情報セキュリティ全体を統括する責任者。組織のサイバーセキュリティ戦略やポリシーなどを策定する。また組織のサイバーセキュリティに係る予算を確保し、組織体制の構築などを行なう。

セキュリティ確保の観点から、CIO（最高情報セキュリティ責任者）、CFO（最高財務責任者）と必要に応じて対峙する。

人材例）

・CISO（最高情報セキュリティ責任者）

CISOは「Chief Information Security Officer」の略で、企業の情報セキュリティ戦略を立案・実行し、情報資産をサイバー攻撃から守る責任者であり、また経営陣の一員としてリーダーシップを発揮して、組織全体のセキュリティ対策と情報システムの統括を担う。

・経営者

経営者はサイバーセキュリティを経営課題と捉え、リーダーシップを発揮して全体方針を定め、予算や人材を確保し、リスク管理体制を構築する必要がある。経済産業省から公表されている「サイバーセキュリティ経営ガイドライン」などを参考に、サイバーセキュリティ対策を、単なるIT部門の問題ととらえるのではなく、経営層がリーダーシップを発揮し、主体的に取り組むべき姿勢が必要である。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

2．セキュリティ統括

企業の情報セキュリティ対策を組織横断的に統括し、CISOや経営層が意思決定する際の支援を行う。具体的には、セキュリティ戦略の策定、リスク管理、インシデント対応などを担当する。

単に技術的な対策を講じるだけでなく、経営層や現場とのコミュニケーションを取りながら、組織全体のセキュリティ意識を高める役割も担う。

人材例）

・コマンダー（CSIRTチーム全体統括）

CSIRT（コンピュータセキュリティインシデント対応チーム）全体を統括し、サイバーセキュリティインシデント発生時の戦略的かつ組織的な対応を主導する役割を担う。主な役割は、インシデント対応に関する意思決定、経営層との連携、PoC（Point of Contact）や社内関係各所との連携、およびCSIRT全体の統括を行なう。コマンダーは、インシデント発生時におけるCSIRTの司令塔として、迅速かつ的確な対応を指揮し、組織全体のセキュリティインシデント対応を成功に導く責任を持つ。

・CISO補佐官

最高情報セキュリティ責任者（CISO）を支援し、組織の情報セキュリティ戦略の策定・実行を補佐する上級職。CISOがセキュリティ全体の最終責任者であるのに対し、補佐官はその実務を統括し、CISOと現場の橋渡し役を担う。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

３．プロジェクト管理

システム（サービス）開発・構築などのプロジェクトにおいて、セキュリティの視点から、目標や計画の策定、プロジェクト体制の整備、進捗管理、資産・予算管理などの各種プロジェクト管理業務を実施する。

また運用を行うために取り組む、社内セキュリティ施策（ISMS運用、セキュリティポリシー施策など）のプロジェクトにおいて、プロジェクトメンバーのクリアランス、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業務などを行なう。

人材例）

・セキュリティ・プロジェクトマネージャー

セキュリティ・プロジェクトマネージャーとは、情報セキュリティに関連するプロジェクトを計画・実行・完了まで統括し、品質・コスト・納期（QCD）を管理しながらプロジェクトを成功に導く責任者。

プロジェクトメンバーの工程管理や顧客との調整を行い、セキュリティに関する専門知識を活かして技術的な課題解決も担当する。プロジェクトメンバーのクリアランス、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たりも行なう。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

４．セキュリティ設計

「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。具体的には、セキュリティを確保するためのシステムの要件定義、アーキテクチャ設計、セキュアソフトウェア方式設計、テスト計画などを行なう。

人材例）

・デジタルシステムアーキテクト

DXを推進するため、ビジネス課題を理解し、ハードウェアやソフトウェア、アプリケーションなどの技術を統合した高品質なITアーキテクチャを設計・実現する人材。セキュリティ領域における知識と、ビジネス戦略と技術を結びつける洞察力が求められる。ビジネス戦略とITアーキテクチャの橋渡しや、ビジネス課題を分析し、解決策をITシステムとして具現化する要求定義を行ったり、顧客のビジネス目標を達成するための高品質なITアーキテクチャを設計などを行う。

・サイバーセキュリティアーキテクト

企業や組織の情報セキュリティシステム全体を戦略的に設計・構築し、経営戦略と連携してセキュリティ対策を推進する人材。システムの脆弱性を調査・分析し、情報セキュリティ方針の策定や経営への提言を行う役割も担い、データセキュリティやネットワークセキュリティなどの高度な知識に加え、IT戦略立案の能力も必要とされる。セキュアシステム要件定義、セキュアシステムアーキテクチャ設計、セキュアソフトウェア方式設計、テスト計画 などを行う。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

５．開発

組織内外における改善可能性のある業務、サービスの現状を把握し、開発するサービス・製品案を整理する。整理した内容を元に、情報システムなどの要件定義、設計、開発、テスト、評価を行い、サービス・製品などを実用化する。

「セキュリティ・バイ・デザイン」の考え方に則り、システム開発の段階からセキュリティを実装する。また自組織で発見された脆弱性に対する修正プログラムの作成なども行う。

人材例）

・情報システム開発者

企業等の組織が抱える課題を解決したり、業務を効率化したりするために、情報システム（ITインフラ）を設計・開発を行う。「セキュリティ・バイ・デザイン」の考え方に則り、顧客・ユーザーの要望を聞き取って、システム開発の企画段階から要件定義・システムを設計・開発・テスト・保守運用においてセキュリティを実装する役割を担う。

・ソフトウェア開発者

顧客・ユーザーの要望や解決したい課題に対して、「セキュリティ・バイ・デザイン」の考え方に則り、主にプログラミング言語を駆使して、ソフトウェアを設計・開発・テスト・保守する役割を担う。自組織で発見された脆弱性に対する修正プログラムの作成やパッチの適用などを行うこともある。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

５．開発

組織内外における改善可能性のある業務、サービスの現状を把握し、開発するサービス・製品案を整理する。整理した内容を元に、情報システムなどの要件定義、設計、開発、テスト、評価を行い、サービス・製品などを実用化する。

「セキュリティ・バイ・デザイン」の考え方に則り、システム開発の段階からセキュリティを実装する。また自組織で発見された脆弱性に対する修正プログラムの作成なども行う。

人材例）

・サービス開発者

顧客の課題を解決したり、社会のニーズに応えたり、また組織内外における改善可能性のある業務、サービスの現状を把握し、開発するサービス・製品案を整理する専門家。「セキュリティ・バイ・デザイン」の考え方に則り、製品・サービスの開発段階から運用・保守に至るまで、情報漏洩やサイバー攻撃といったリスクを最小限に抑えるための役割を担う。脆弱性の発見、セキュリティ対策の実装、社内外のセキュリティに関する知識の提供など、技術面から組織文化の醸成まで幅広く関わり、システムやサービスを利用する人々を保護し、社会全体の安心に貢献する。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

６．システム管理・ネットワーク管理

システム管理者・ネットワーク管理者の立場で、システム設計や構築を担当する。また設計・開発時には、チームメンバーと連携し、システムおよびネットワーク運用・保守に係る作業内容などを記載した運用・保守計画を作成する。運用・保守計画書に沿って、システム全体の運用・保守のテストを実施し、本番環境への移行を図る。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、技術的な側面から対処にあたる。

人材例）

・システムエンジニア（セキュリティ）

企業や組織の情報資産をサイバー攻撃や不正アクセスなどから守る専門職です。サイバーセキュリティの脅威に対応するために、システム基盤やインフラの設計、実装、および運用を担当します。またID基盤や認証および資源管理なども行う。

ITインフラ、アプリケーション、法律等の幅広い知識が求められ、変化する脅威に対応するため、継続的な学習と最新情報の習得が必要で、倫理とセキュリティ意識が求められる。

・システムエンジニア（ネットワーク）

企業や組織がデータ通信を快適に行えるよう、ネットワークの要件定義、設計、構築、運用、監視、保守までを一貫して担当します。物理的なネットワーク機器を扱うほか、クラウドやソフトウェア、仮想化技術を駆使して、セキュリティを考慮したシステム全体の快適なネットワーク環境を実現・維持する。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

６．システム管理・ネットワーク管理

システム管理者・ネットワーク管理者の立場で、システム設計や構築を担当する。また設計・開発時には、チームメンバーと連携し、システムおよびネットワーク運用・保守に係る作業内容などを記載した運用・保守計画を作成する。運用・保守計画書に沿って、システム全体の運用・保守のテストを実施し、本番環境への移行を図る。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、技術的な側面から対処にあたる。

人材例）

・システムエンジニア（クラウド）

システムエンジニア（クラウド）、またはクラウドエンジニアとは、クラウドサービスを活用して、企業のITインフラの設計、構築、運用、保守などを担当する技術者。従来のサーバーエンジニアが物理的なサーバーやネットワークなど、オンプレミス環境での構築・運用を担当するのに対し、クラウドエンジニアはクラウド上でのネットワーク構築や保守などを行う。

・システム管理者

企業の情報システム全般の運用・保守・管理を行う担当者。設計開発時には担当者と連携し、システム運用・保守に係るシステム運用・保守計画を作成する。またシステムの運用・保守業務を実施するとともに、セキュリティの設定などシステムの安全性を担保し、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、対処にあたる。企業・組織全体のITインフラを安定稼働させ、ユーザーがシステムを円滑に利用できるための基盤を支える存在。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

７．監視・運用

各種機器のログの監視、保管、分析などを行ないセキュリティ監視を実施する。セキュリティインシデントを検知した際は、関係各所へ連絡して連携する。また監視ツールの運用、保守を行う。

人材例）

・セキュリティ運用エンジニア

セキュリティ運用エンジニアは、情報セキュリティの専門家として、システムがサイバー攻撃や障害から安全に運用されるように守る役割を担う。システムを導入した後、システム障害やサイバー攻撃からシステムを守り、安全な状態を維持するための保守業務を行なう。最新情報を常に収集し、セキュリティアップデートを実施したり、実際にサイバー攻撃があった際のインシデント対応も担当する。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

８．監査

情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、セキュリティリスク評価に基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、もって保証を与えあるいは助言を行う。

人材例）

・情報セキュリティ監査人

潜在的な脆弱性の発見と情報資産の保護、サイバー攻撃への対応能力の確認、そして社内・顧客からの信頼性向上を目的として、組織の情報セキュリティ対策が適切に機能しているかを第三者的な視点で検証・評価を行なう。具体的には、監査監査計画の立案、監査の実施、報告書の作成・報告などを行う。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

９．脆弱性診断・評価

現在の状況とTobe像のFit&Gapからリスク評価を行い、ソリューションマップを作成して導入を推進する。導入されたソリューションの有効性を確認し、改善計画に反映する。また平常時にはリスクアセスメントを行う。インシデント対応時には脆弱性の分析、影響の調査などに対応する。

また、ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行い、診断結果の評価を行う。ソフトウェアやシステム、ネットワークなど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。

人材例）

・ペネトレーションテスター

攻撃者の視点でサイバー攻撃をシミュレーションし、システムの脆弱性を特定・評価するサイバーセキュリティの専門家。システムに疑似的な攻撃を仕掛けて侵入を試み、実際のサイバー攻撃で発生するであろう被害を検証します。テスト結果を報告書にまとめ、システムの修正要否やセキュリティ改善策を提案する役割も担う。

・脆弱性診断士

システムやアプリケーションに存在する脆弱性や設定上の不備を発見するためのセキュリティテスト（脆弱性診断）を行なう。脆弱性診断には、プラットフォーム診断、Webアプリケーション診断、モバイル診断などの種類が存在する。

・エクスプロイト開発者

ソフトウェアやシステムの未知の脆弱性（ゼロデイ脆弱性）を攻撃者よりも先に脆弱性を見つけ出し、サイバー攻撃に利用されるエクスプロイト（発見した脆弱性を実際に悪用できるコード）を作成して、その情報をセキュリティ強化のために報告したり、対策を講じたりする。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

１０．教育・訓練

社内のリテラシーの向上、底上げのための教育及び啓発活動を行う。

人材例）

・セキュリティインストラクター（講師）

情報セキュリティに関する知識やスキルを企業・組織内で教育・啓発する専門家。具体的な業務内容は、従業員向けのトレーニングプログラムの提供、情報セキュリティポリシーに関する指導、脆弱性診断やサイバー攻撃への対応策の啓発など多岐にわたる。常に最新のセキュリティ脅威の動向を把握し、知識をアップデートしながら、組織全体のセキュリティレベルを向上させる役割を担う。

・研修企画担当者

従業員に対して情報セキュリティの重要性や対策方法を理解させるための研修を立案を行なう。セキュリティ研修を企画・立案する際には、セキュリティリスクの認識・評価、セキュリティ対策の戦略立案・企画、コミュニケーション能力、教育スキルなどが求められる。

・研修運営担当者

セキュリティ研修の運営担当者は、研修の実施、効果測定などを行なう。常に最新の知識をアップデートする必要がある。主な業務内容は、研修環境や教材の準備、実施の運営、効果測定と報告などを行なう。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

１１．法務

システムにおいてコンプライアンス及び法的観点から遵守すべき内容に関する橋渡しを行う。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。組織及び従業員のコンプライアンス意識を向上させ、社内ルールなどの管理を行う。

人材例）

・セキュリティ法務担当者

情報セキュリティに関する法律業務を担当する専門家。情報資産を守るための契約書チェック、個人情報保護、知的財産権の管理、訴訟対応、関連法規の調査・分析など、多岐にわたる業務を担う。法律知識、ITに関する基礎知識、高いコミュニケーション能力、そして法改正に対応できる最新情報やインシデント事例のアップデートなども求められる。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

１２．対処（インシデントハンドリング）

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。具体的には、セキュリティインシデント発生時、インシデントへの対応を行い、影響の拡大を防止すると共に、インシデントの対応状況を把握する。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。

人材例）

・インシデントマネージャー

インシデントの情報を情報収集担当や情報分析担当から収集し、CSIRT全体統括へ情報共有する。また、インシデント処理担当へ対応指示を行い、状況を管理し、インシデントレポートを記録する、インシデント担当の管理者。

・インシデントハンドラー

発生しているインシデントへの対応を行なう担当者。また、影響しているシステムへの対応支援も行なう。セキュリティベンダーを利用している場合にはベンダーとの連携なども担う。

・トリアージ（インシデント対応優先順位判断）

平常時にはインシデントが発生した時のシステム停止、再開の対応基準を準備しておく。また、インシデント発生時には対応の優先順位をCSIRT全体統括を支援しながら決定する役割を担う。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

１３．脅威・脆弱性情報収集

組織内外の情報セキュリティに関する情報を収集する。収集した情報の分析を実施する。分析した結果を管理及び共有する。

具体的には、セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メディア情報などを収集を行なう。また収集した情報を分析し、その情報を自社に適用すべきかの選定を行う。SOC（セキュリティオペレーションセンター）と対応することが多い。

人材例）

・リサーチャー（収集・調査）

セキュリティ機器から発せられるアラートの調査や予兆を分析し、情報分析担当とともに状況を調査し、インシデント管理担当に報告する。また、脅威情報や自社にかかわる漏えい情報なども収集する。

・キューレター（分析）

情報収集担当が集めたデータを分析し、自社に適応すべきかの判断やトリアージを行う際に必要な情報を整理してインシデント管理担当に報告する。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

１４．社内外調整

社外向けではJPCERT/CC、NCO、警察、監督官庁、NCA、他CSIRT等との連絡窓口、社内向けではIT部門調整担当社内の法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、それぞれ情報連携を行う。また組織内を調整し、社内各関連部署への情報発信を行う。社内システムに影響を及ぼす場合にはIT部門と調整を行う。

人材例）

・POC：Point of Contact（連絡窓口）

社内、社外との連絡窓口の役割を担う。経営者に対してはCSIRT全体統括者とともに連絡を行なう。社外の先としては、NCA、JPCERT/CC、CSIRT、警察、監督官庁等。社内先としては、法務、渉外、広報、各事業部等。

・ノーティフィケーション（情報発信）

脅威情報、脆弱性情報などを自組織内へ情報発信したり、対応調整などを担う。

Copyright © 2025 Japan Network Security Association

新SecBoK2025ロール（役割）

１５．インシデント調査・分析

システム的な鑑識、精密検査、解析、報告を行う。悪意のある者は証拠隠滅を図ることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求される。

また外部からの犯罪、内部犯罪を捜査する。セキュリティインシデントはシステム障害とは異なり、悪意のある者が存在する。通常の犯罪捜査と同様に、動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に捜査対象を絞っていくことが要求される。

人材例）

・フォレンジック

機器類の証拠保全やシステム的な鑑識を行ない、内部で何が起きているのかの足跡を調査する。また、発見されたマルウェアの解析も行う。

・インベスティゲーター（犯罪捜査）

内部犯罪やサイバークライム事案などの調査を必要であれば警察と連携して行なう。

・マルウェアアナリスト

マルウェアアナリストは、悪意のあるプログラムやファイルを分析し、その仕組みや脅威の正体を解明して、特定、除去、そして将来の攻撃を防ぐための対策を立てる専門家。具体的には、マルウェアの検出・解析を行い、その挙動を分析して防御策の立案やインシデント発生時の対応を支援する。

Copyright © 2025 Japan Network Security Association

SecBoK2025

セキュリティ知識分野（SecBoK）人材スキル
マップ2025年版

Copyright 2025 NPO日本ネットワークセキュリティ協会

SecBoK2025ロール（役割）とスキル項目

15の役割（ロール）

セキュリティ知識分野（SecBoK）人材スキルマップ2025年版 全体整理表

※特定非営利活動法人日本ネットワークセキュリティ協会　教育部会 情報セキュリティ知識項目（SecBoK）改訂委員会作成

＜ロール毎の必須知識・スキル＞

1	**前提スキル**（職務遂行の前提として有しておくべき知識・スキル）
2	**必須スキル**（職務遂行の実施に際して必要となる知識・スキル）
0.5	**参考スキル**（職務遂行に際して必須ではないが、あると望ましい知識・スキル）

※「前提スキル」と「必須スキル」の関係
前提スキルを有する人材を確保し、必須スキルに関する教育・トレーニング
を行うと、当該職務を担うことができる人材となる

＜知識・スキルのレベル＞

L	**低**（概ね経験3年未満でも対応可能）
M	**中**（経験3年以上または関連する演習・トレーニング受講者なら対応可能）
H	**高**（経験10年以上または高度な研修受講を前提とする専門実務経験者または「突出した人材」なら対応可能）
P	**ペンディング**（情報収集・インテリジェンスに関するもの。レベル付けの対象外）

新2025ID	旧2021ID	TKS-ID	新旧別	分野	大項目	中項目	レベル	小項目	1 セキュリティ経営、意思決定・戦略策定	2 セキュリティ統括	3 プロジェクト管理	4 セキュリティ設計	5 開発	6 システム管理・ネットワーク管理	7 監視・運用	8 監査	9 脆弱性診断・アセスメント	10 教育・訓練	11 法務	12 対処（インシデントハンドリング）	13 脅威・脆弱性情報収集	14 社内外調整	15 インシデント調査・分析
1	new	K1170	新規	00_基礎	1_数学・物理学・情報学		L	数学モデルに関する知識							0.5								
2	new	K1219	新規	00_基礎	1_数学・物理学・情報学		L	統計処理に関する知識							0.5						0.5		
3	new	K0739	新規	00_基礎	1_数学・物理学・情報学		L	数学の原理と実践に関する知識							0.5								
4	4	K0055	継続	00_基礎	2_計算機・通信工学		L	マイクロプロセッサに関する知識			0.5	0.5	0.5	0.5	0.5		0.5			0.5			0.5
5	new	K0786	新規	00_基礎	2_計算機・通信工学		L	物理的なコンピュータコンポーネントに関する知識		0.5	0.5	1	0.5	0.5	1	0.5	1			1	1		1
6	new	K0787	新規	00_基礎	2_計算機・通信工学		L	コンピュータ周辺機器に関する知識		0.5	1	1	0.5	1	1	0.5	0.5	0.5		1	1		1
7	new	K0674	新規	00_基礎	2_計算機・通信工学		L	ルに関する知識		0.5	0.5	1	1	1	1	0.5	1	0.5		1	1		1
8	new	K1225	新規	00_基礎	2_計算機・通信工学		L	識		1	1	1	1	1	1	1	1			1	1		1
9	new	K1227	新規	00_基礎	2_計算機・通信工学		L	識		1	1	1	1	1	1	1	1			1	1		1
10	new	K1228	新規	00_基礎	3.ソフトウェア		L			0.5	1	1	1	0.5			1			0.5			1
11	new	K1201	新規	00_基礎	3.ソフトウェア		L			0.5	1	1	1	1	1		1			1	1		1
12	19	K0068	継続	00_基礎	3.ソフトウェア		L	に関する知識		0.5	1	1	1	0.5	1		1			1	1		1
13	new	K0694	新規	00_基礎	3.ソフトウェア		L	ム応用に関する知識		0.5	1	1	1	0.5	1		1			1	1		1
14	new	K0750	新規	00_基礎	3.ソフトウェア		L			1	1	1	1	1	1	0.5	1			1	1		1
15	new	K0855	新規	00_基礎	3.ソフトウェア		L	デバッグツールおよび手法に関する知識			1	1	2	0.5	1	0.5	1				1		2
16	new	K0861	新規	00_基礎	3.ソフトウェア		L	ネットワークポートの機能とアプリケーションに関する知識		1	1	1	1	1	1	1	1			1	1	1	1
17	new	S0828	新規	00_基礎	4.データ		L	データをまとめるスキル							1						1		1
18	29	S0011	継続	00_基礎	4.データ		L	情報検索の実施に関するスキル		1					1					1	1		1
19	new	K0707	新規	00_基礎	4.データ		L	データベースシステムやソフトウェアに関する知識		0.5	1	1	1	1	1	1	1				1		1

スキル項目
（約1200弱）

Copyright © 2025 Japan Network Security Association

SecBoK2025年版 知識項目のカテゴリ分類

大項目分類												
	00_基礎	0_総論	1_数学・物理学・情報学	2_計算機・通信工学	3_ソフトウェア	4_データ	5_ICTリテラシー	6_コミュニケーション力	7_思考力	8_AIリテラシー	X_その他の基礎	
	01_IT・セキュリティ基礎	0_総論	1_ICT	2_セキュリティ基礎	X_その他のIT・セキュリティ基礎							
	02_ITヒューマンスキル	0_総論	1_コミュニケーション力	2_思考・判断力	X_その他のITヒューマンスキル							
	03_セキュリティガバナンス	0_総論	1_体制	2_組織アーキテクチャ	3_組織統制	4_リスク戦略	X_その他のセキュリティガバナンス					
	04_セキュリティマネジメント	0_総論	1_ポリシー策定	2_手続等整備	3_資産管理	4_調達・契約	5_評価	6_監査	7_リスク管理	8_要員管理	X_その他のセキュリティマネジメント	
	05_ネットワークセキュリティ	0_総論	1_トラフィック解析	2_侵入検知	3_脆弱性診断	4_フィルタリング	5_アクセス制御	6_VPN	7_深層防御	8_セキュアネットワーク設計	X_その他のネットワークセキュリティ	
	06_システムセキュリティ	0_総論	1_ハードウェア	2_OS	3_アプリケーション	4_データ	5_システムログ	6_セキュリティ機能	7_OTセキュリティ	8_AI利用セキュリティ	9_クラウド利用セキュリティ	X_その他のシステムセキュリティ
	07_セキュア設計構築	0_総論	1_アーキテクチャ	2_セキュリティ要件定義	3_セキュア設計	4_セキュアプログラミング	5_セキュリティ機能実装	6_テスト	7_ツール	8_プロジェクト管理	X_その他のセキュア設計構築	
	08_セキュリティ運用	0_総論	1_定常運用	2_監視	3_保守	4_トラブル対応	5_インシデント対応	6_ツール	7_能動的防御	X_その他のセキュリティ運用		
	09_暗号・認証・署名・ID管理	0_総論	1_暗号	2_認証	3_ID管理	4_電子署名	5_電子透かし	X_その他の暗号・認証・署名・ID管理				
	10_サイバー攻撃手法	0_総論	1_攻撃手法	2_攻撃主体	3_マルウェア	9_その他のサイバー攻撃手法						
	11_インテリジェンス	0_総論	1_情報収集・諜報活動	2_作戦行動	3_分析・レポート作成	4_ツール	X_その他のインテリジェンス					
	12_デジタルフォレンジクス	0_総論	1_収集手法	2_復元手法	3_分析手法	4_ツール	X_その他のデジタルフォレンジクス					
	13_サイバー捜査	0_総論	1_捜査手法	2_内部不正捜査	X_その他のサイバー捜査							
	14_セキュリティ人材育成	0_総論	1_教育企画	2_教材開発	3_教育指導	4_評価	5_キャリア	X_その他のセキュリティ人材育成				
	15_法・制度・標準	0_総論	1_法律	2_制度	3_標準	X_その他の法・制度・標準						
	16_ビジネススキル	0_総論	1_組織経営・戦略	2_ビジネスプロセス	3_マーケティング	4_調達・契約	5_リスクマネジメント	X_その他のビジネススキル				
	17_関連領域	0_総論	1_ICT	2_工学	X_その他の関連領域							

Copyright © 2025 Japan Network Security Association

Copyright 2025 NPO日本ネットワークセキュリティ協会