セキュリティ知識分野（SecBoK）人材スキルマップ 2025年版の改定に向けて

～教育部会における取組み～

教育部会 部会長
平山 敏弘

Copyright 2025 NPO日本ネットワークセキュリティ協会

JNSA教育部会の活動ご紹介

Copyright 2025 NPO日本ネットワークセキュリティ協会

JNSA教育部会とは

①従来の「守り」も重要だが、DXを推進できる「攻め」の人材

社会のニーズや時代の変化に適合したセキュリティ人材育成のため、必要とされる知識・技能等の検討を行い、実際に大学や専門学校等で評価実験を行う。また、情報セキュリティ教育のコンテンツとして、講義シラバスや講義資料およびSecBoK2025年更新版の作成・公開を通じて、教育界・産業界への展開・使用を促進することで、情報セキュリティ人材の育成に貢献する。

②スキルの「標準化」「見える化」への対応

③セミナーや講演以外の「教育」の場は意外とない

さらに、継続して講師データベースへの登録講師や講師予備軍の若手による講義・勉強会の開催等、**教える場の提供**を支援することにより、JNSA教育部会メンバーのスキル向上を目指す。

④ASEAN諸国でも活用されているが、シンガポールなどではさらに良いものが出てきており、日本は今やアジアの盟主ではない

【SecBoK関連】

SecBoK2025更新版の作成および使用事例などを盛り込んだ利用ガイド版作成などの活動を実施。

⑤近年は、学術論文だけでなく、実務課題論文のニーズが高まっている

【辻井論文賞関連】

「 辻井重男セキュリティ論文賞」の支援団体の1組織として、教育部会がJNSAを代表して、運営委員会委員および査読委員として参画している。運営委員及び査読委員については、毎年複数名にご協力を頂いている。この活動は、**若手セキュリティ研究者支援及び育成の一環**として実施している。

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

どのように、どこで活用されているのか

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

「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。

SecBoK2019版は、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となり、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改定し、あわせて下記も提示しました。

・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

その後のSecBoK2021版では、SecBoKは、BoK（Body of Knowledge）の原点に返って、「ディクショナリー的な位置付け」として多くの方に利用いただけることが目的であることを再確認し、現在公開されています。

Copyright 2025 NPO日本ネットワークセキュリティ協会

大学シラバスとの連携例（１）
教育界（情報系大学）適用事例
コンピュータサイエンスカリキュラム標準（J17）

「プラス・セキュリティ人材」を育成するためには、情報系の学生全般にベーシックなセキュリティスキルを身に着けさせることも必要です。

分野｜大項目｜中項目	CS	IS	CE	SE	IT	GE	CyS ICT 基礎	CyS セキュリティ基礎	CyS セキュリティ専門
基礎｜ICT 基礎｜情報理論	●			●	●	●	●		
基礎｜ICT 基礎｜計算機ハードウェア	●	●		▲	●		●		
基礎｜ICT 基礎｜ネットワークインフラ	●	●		▲	●	●	●		
基礎｜ICT 基礎｜通信プロトコル・サービス	●	●		▲	●	●	●		
基礎｜ICT 基礎｜データ構造	●	●		▲	▲		●		
基礎｜ICT 基礎｜データベース	●	●		▲	●	●	●		
基礎｜ICT 基礎｜ナレッジマネジメント	●	●		▲	▲	●	●		
基礎｜ICT 基礎｜アルゴリズムとプログラミング	●			●	●	●	●		
基礎｜ICT 基礎｜オペレーティングシステム	●	●		▲	●	●	●		
基礎｜ICT 基礎｜ソフトウェア	●	●		●	●	●	●		
基礎｜ICT 基礎｜システム開発	●			●	●	●	●		
基礎｜ICT 基礎｜システム運用	▲	●		▲	●	●	●		

J17とは、世界標準である米国IEEE/ACMのCC2001-CC2005を土台として、日本の情報専門教育の状況に対応した見直しを行い、まとめたカリキュラム標準。前身の情報専門学科カリキュラム標準（J07）の見直しを行い、コンピュータ科学（CS） 情報システム（IS）コンピュータエンジニアリング（CE）ソフトウェアエンジニアリング（SE） インフォメーションテクノロジ（IT）一般情報処理教育（GE）についてまとめたカリキュラム標準で、2017年に見直しされJ17が公表されている。

人材に必要となるスキルについては、セキュリティ知識分野(SecBoK)人材スキルマップを参考とした。カリキュラムモデルに必要となる教えるべき知識項目の整理するため、サイバーセキュリティのカリキュラム作成の際に参考として、SecBoK人材スキルマップにおける各情報専門教育項目をカバーする範囲の専門レベルを対象としたレベル分けを整理した。

大学シラバスとの連携例（２）
各授業とSecBoK項目とのマッピング

JNSA

大学各授業

<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。今回はレベル付けの対象外）

2021ID	旧2019ID	KSA-ID	新旧別	分野	大項目	中項目	レベル	小項目	情報数学	コンピュータアーキテクチャ	データベース論	コンピュータネットワーク	情報セキュリティ概論	オペレーティングシステム	プログラミング演習基礎	認証とアクセス制御	Web構築	ネットワークセキュリティ	コンピュータフォレンジック	インシデント対応	リスクマネジメン	セキュリティマネジメント	著作権・プライバシー保護	プロジェクトマネジメント
1	1	K0052	旧NICEに類似項あり	00基礎	1数物情報学		L	数学に関する知識（例：対数、三角法、線形代数、微積分、統計、操作解析）	●															
2	2	K0030	旧NICEに類似項あり	00基礎	2計算機・通信工学		L	コンピュータアーキテクチャ（例：回路基板、プロセッサ、チップ及びコンピュータハードウェア）に適用される電気工学に関する知識		●															
3	3	K0036	旧NICEと同一	00基礎	2計算機・通信工学		L	マンマシンインタラクションの原理に関する知識		●				●										
4	4	K0055	旧NICEと同一	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		●														
5	5	K0061	旧NICEとほぼ同一	00基礎	2計算機・通信工学		L	ネットワーク上でトラフィックがどのように流れるか（例： TCP/IP、OSI、ITIL現行版）に関する知識				●												
6	6	K0108	旧NICEに類似項あり	00基礎	2計算機・通信工学		L	通信メディアの基本概念、用語及び幅広い範囲での運用に関する知識（コンピュータと電話のネットワーク、衛星、ファイバ、無線）																
7	7	K0109	旧NICEに類似項あり	00基礎	2計算機・通信工学		L	多様な構成要素と周辺機器の機能を含む、物理的なコンピュータの構成要素とアーキテクチャに関する知識（例：CPU、ネットワークインターフェースカード、データストレージ）の機能を含む、物理的なコンピュータコンポーネントとアーキテクチャに関する知識		●														
8	8	K0113	旧NICEとほぼ同一	00基礎	2計算機・通信工学		L	さまざまな種類のネットワーク通信に関する知識（例：LAN、WAN、MAN、WLAN、WWAN）				●												
9	9	K0114	旧NICEとほぼ同一	00基礎	2計算機・通信工学		L	電子デバイスに関する知識（例：コンピュータシステム/コンポーネント、アクセス制御デバイス、デジタルカメラ、デジタルスキャナ、電子オーガナイザ、ハードドライブ、メモリカード、モデム、ネットワークコンポーネント、ネットワークアプライアンス、ネットワークホームコントロールデバイス、プリンタ、リムーバブルストレージデバイス、電話機、複写機、ファクシミリなど）																
10	10	K0138	旧NICEに類似項あり	00基礎	2計算機・通信工学		L	Wi-Fiに関する知識				●												
11	11	K0395	旧NICEとほぼ同一	00基礎	2計算機・通信工学		L	コンピュータネットワークの基礎に関する知識（ネットワークの基本的なコンピュータコンポーネント、ネットワークの種類など）				●												
12	12	K0491	新規	00基礎	2計算機・通信工学		L	ネットワークとインターネット通信に関する知識（すなわち、デバイス、デバイス構成、ハードウェア、ソフトウェア、アプリケーション、ポート/プロトコル、アドレッシング、ネットワークアーキテクチャとインフラストラクチャ、ルーティング、オペレーティングシステムなど）				●												
13	13	K0516	新規	00基礎	2計算機・通信工学		L	ハブ、スイッチ、ルータ、ファイアウォールなどを含む物理的および論理的なネットワークデバイスおよびインフラストラクチャに関する知識				●												
14	14	K0555	新規	00基礎	2計算機・通信工学		L	TCP/IPネットワーキングプロトコルに関する知識				●												
15	15	K0556	新規	00基礎	2計算機・通信工学		L	通信の基礎に関する知識				●												

この例では、赤枠内は大学の各授業である。その授業内で学べる内容をSecBoKスキル項目とマッピングしている。これによりシラバス作成の際にも、各授業で学べるスキルを明確にすることができる。またSecBoKは、情報系大学のカリキュラム標準である「情報セキュリティ（J17-CyberSecurity）」と連携しているためカリキュラム標準に沿ったシラバス作成が可能となる。

大学シラバスとの連携例（３）
各授業とSecBoK役割（ロール）とのマッピング

SecBoK役割

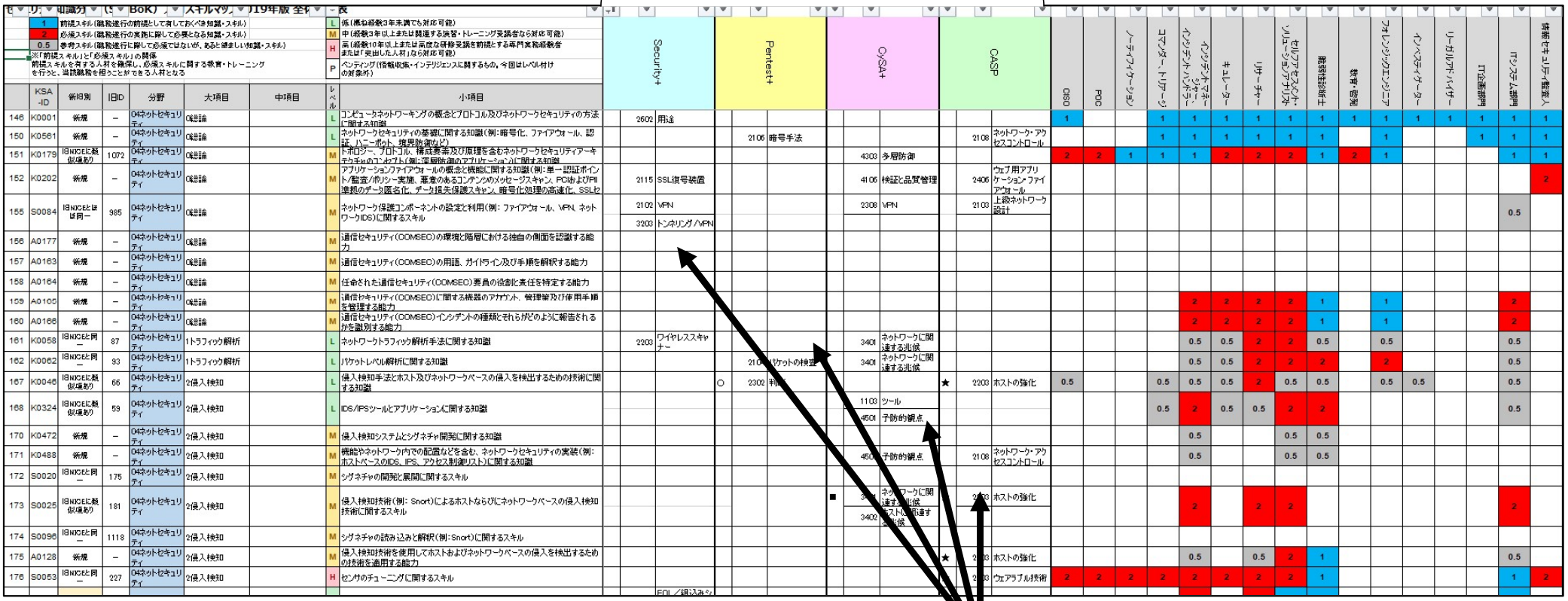
大学各授業

授業	CISO	SOC	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、インシデントハンドラー	キュレーター	リサーチャー	セルフアセスメント・ソリューションアナリスト	脆弱性診断士	教育・啓発	フォレンジックエンジニア	インベスティゲーター	リーガルアドバイザー	IT企画部門	ITシステム部門	情報セキュリティ監査人
情報数学	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
コンピュータアーキテクチャ				●	●	●	●	●	●	●	●	●		●	●	
データベース論					●	●	●	●	●		●	●			●	
コンピュータネットワーク				●	●	●	●	●	●	●	●	●		●	●	
情報セキュリティ概論	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
オペレーティングシステム				●	●	●	●	●	●		●	●		●	●	●
プログラミン演習基礎					●	●	●		●	●	●	●			●	
認証とアクセス制御				●	●	●	●	●	●		●	●		●	●	
Web構築															●	
ネットワークセキュリティ				●	●	●	●	●	●		●	●			●	
コンピュータフォレンジック											●					
インシデント対応	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
リスクマネジメント	●	●	●	●	●									●	●	
セキュリティマネジメント	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
著作権・プライバシー保護													●			●
プロジェクトマネジメント	●			●	●									●	●	

この例では、赤枠内は大学の各授業である。その授業内で学べる内容とSecBoK各役割（ロール）とマッピングしている（青枠）。これにより、授業内容作成の際に、どんな人材育成を目標にしているかを明確にすることができる。また、学生側も自身の目指す人材像を意識して必要なスキルを学べる授業の履修を選択することが可能となる。

資格との連携事例
セキュリティ関連資格とSecBoK

ベンダーニュートラルなIT資格団体であるCompTIAにおいて、各資格で問われているスキル項目とSecBoKスキル項目とのマッピングを実施。これにより資格ホルダーがどのセキュリティロールに適合度が高いかなどか可視化され、個人の育成計画だけでなく部門や組織の体制作りや部門全体の育成などに有用となる。　各資格



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

SecBoK活用事例（海外）

Copyright 2025 NPO日本ネットワークセキュリティ協会

海外利用事例

独立行政法人国際協力機構（JICA）において、SecBoKを利用したセキュリティ人材育成プロジェクトが実施されている。

インドネシア：サイバーセキュリティ人材育成プロジェクト

https://www2.jica.go.jp/ja/evaluation/pdf/2018_1701288_1_s.pdf

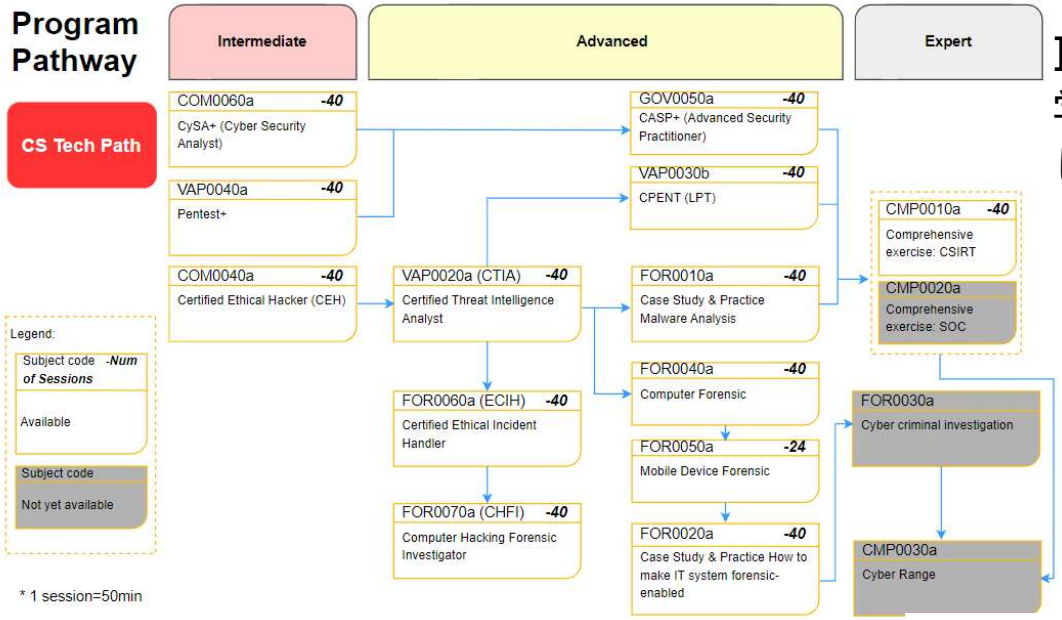
【プロジェクト概要】
インドネシア最高峰の大学の一つであるインドネシア大学におい てプロフェッショナル（実務者）向けサイバーセキュリティ教育システムを立 上げることで、重要情報インフラ分野を中心とする民間機関や政府に対してサイバーセキュリ ティ人材を持続的に供給する。
【事業概要】
本事業は、インドネシア国において、**セキュリティ知識分野（SecBoK）人材スキルマップに準拠**するプロフェッショナル人材育成のためのサイバーセキュリティプログラムをインドネシア大学内に立上げ、諸外国のサイバーセキュリティ人材も巻込みながら、同大学におけるサイバーセキュリティ人材の育成システム強化を図り、民間機関・政府のサイバーセキュリティ対応能力強化に寄与するもの。

ベトナム：サイバーセキュリティに関する能力向上プロジェクト（キャリア開発計画）

https://www2.jica.go.jp/ja/announce/pdf/20190424_190086_4_02.pdf

【プロジェクト概要】
ベトナム情報通信省より「サイバーセキュリティに関する能力向上プロジェクト」実施の要請がなされた。要請された内容は、政府サイバーセキ ュリティ人材の能力向上、政府情報ネットワークをサイバー攻撃から守る機材・技術 の供与、サイバーセキュリティ啓発活動などとなっている。
【活動概要】
SecBoK のフレームワークに定義された役割（ロール）のうち必要とされるものを明らかにし、それぞれの職員のキャリア開発計画を策定する。また**SecBoK のフレームワークに定義された役割（ロール）のうち優先度の高いもの研修コースを計画・実施**する

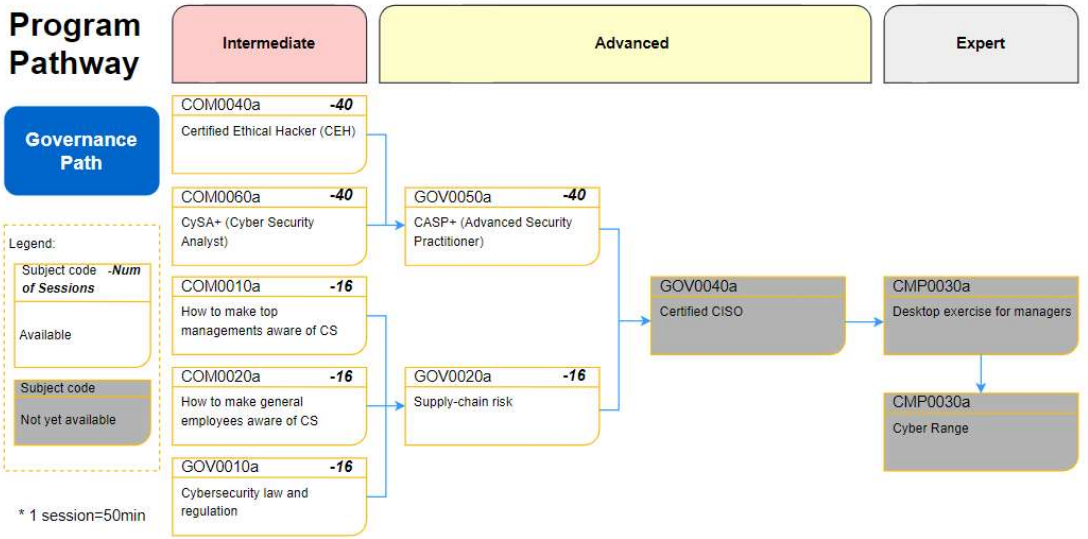
Indonesia Cyber Awareness and Resilience Center (IdCARE.UI)



IdCARE.UIは、2020 年にインドネシア大学工学部 (FTUI) の下に設立され、次の活動を提供しています。

https://idcare.ui.ac.id/

- サイバーセキュリティの大学院プログラム
- サイバーセキュリティ関連の研究
- コラボレーションとパートナーシップ
- 能力開発と認定



インドネシア大学
サイバーセキュリティ人材育成プロジェクト

JICA 独立行政法人 国際協力機構

背景

（1）当該国におけるサイバーセキュリティセクターの開発実績（現状）と課題

情報通信技術（Information and Communication Technology。以下「ICT」という。）の重要性増加に比例し、サイバー攻撃や情報漏えいのリスクも甚大化している。バングラデシュ中央銀行が被害を受けた8100万ドルの不正送金等、重要インフラへのサイバー攻撃が世界各国で確認されており、国家の重要リスクとして認識されている。
インドネシアにおいては、サイバーセキュリティに関する中央政府の担当部門設立やルールの策定は概ね了しているが、民間機関や政府におけるサイバーセキュリティ人材の量・質の不足が行政及び経済団体から指摘されている。研修機会の絶対量が不足していること及びサイバーセキュリティ人材における各役割の定義が曖昧であることがその背景にある。

（2）当該国におけるサイバーセキュリティセクターの開発政策と本事業の位置づけ

情報通信省が2016年に策定したインドネシアサイバーセキュリティ戦略における柱の一つとして、サイバーセキュリティに関する意識改革及び産業界のニーズを踏まえた人材の育成を、高等教育機関を通じて輩出することが計画されている。また、電力、交通、金融をはじめとする8分野を重要情報インフラ（Critical Information Infrastructure。以下「CII」という。）に指定し、サイバーセキュリティ対策の重点としている。
本協力は、インドネシア最高峰の大学の一つであるインドネシア大学においてプロフェッショナル（実務者）向けサイバーセキュリティ教育システムを立上げることで、CII分野を中心とする民間機関や政府に対してサイバーセキュリティ人材を持続的に供給するものである。

プロジェクト概要

プロジェクト名

（和）サイバーセキュリティ人材育成プロジェクト
（英）Project for Human Resources Development for Cyber Security Professionals

対象国名

インドネシア共和国

署名日（実施合意）

2018年11月12日

プロジェクトサイト

プロジェクト目標

インドネシア大学において産業界のニーズを踏まえたプロフェッショナル向けサイバーセキュリティ教育システムが強化される。

成果

1. インドネシア大学において世界水準のプロフェッショナル向けサイバーセキュリティ教育が提供される。
2. 産業界のニーズを踏まえたオープンソースサイバーセキュリティツールが開発される。
3. オープンコースウェアが開発され、公開される
4. 中・長期的なカリキュラムへの参加者・協力者拡大を目的に、諸外国との間でサイバーセキュリティに関するネットワークが強化される。

活動

成果1

1-1. NICE, SecBoK等、他国におけるICTスキル標準に関する事例が研究される。
1-2. 包括的で最新のサイバーセキュリティ関するカリキュラムが設計される。
1-3. 上記カリキュラムに基づきシラバスが設計される。
1-4. 講師への必要なトレーニングが行われる。（民間企業のゲスト講師を含む）
1-5. 長期コースのコンポーネントとなる短期のサイバーセキュリティコースが設立される。
1-6. 必要なタイミングでコースに関係する活動が見直される。

ベトナム
情報セキュリティ協会へのSecBoK説明会

2020年10月13日に情報セキュリティ局（AIS）において、プロジェクトで利用しているSecBoKに関する勉強会を開催しました。SecBoK（Security Body of Knowledge）とは、NPO日本ネットワークセキュリティ協会（JNSA）がセキュリティ業務に携わる人材の役割、タスク、必要とされる技術を体系的に整理し、一覧にしたものです。SecBoKは、アメリカ国立標準技術研究所（NIST）が作成したフレームワークも参照して作成されています。

ベトナム側からはAIS職員の他にベトナム情報セキュリティ協会（VNISA：Viet Nam Information Security Association）から3名の方が出席しました。

現在AISは政府機関におけるセキュリティ業務の役割を定義し、セキュリティ業務に就くための必要な資格を設定することを行っています。ベトナム側は以下のような課題を認識していることから、日本の持つ知見を共有し、そこから学びを得ることを本勉強会の目的としました。
・セキュリティ業務の役割は政府向けであり、民間企業に適用できる形式になっていない。
・ベトナムにはNISTやSecBoKのような役割、タスク、スキル等に関する一覧や関係性を示した資料が存在しない。

なお、日本とは違い、セキュリティ分野で業務する際に資格は持つことが必須条件になります。また、ベトナムでは政府でも民間でも（特に小規模の銀行等）、1人が複数の役割を持つことは普通なので、そのような場合でも新しい職員を体系的に教育する基準を作ることも検討しているとのことでした。

勉強会では、SecBoKを開発したJNSAがWebサイト上で公開している文書・情報をもとにして、JNSAの組織、SecBoKの変遷と概要、利用方法について説明しました。また、日本国内で情報処理推進機構（IPA）が提供しているIT資格やITスキル標準（ITSS）とSecBoKの関係等も説明しました。その後、インドネシアとベトナムにおけるJICAサイバーセキュリティプロジェクトでの適用方法を解説しました。

本勉強会を通して、AIS・VNISAからは以下のようなコメントが得られました。
・日本のSecBoK活用事例から多くの教訓が学べた。
・SecBoKは政府のみならず民間企業にも適用できる、有用なフレームワークである。
・日本は10年以上かけて様々なセキュリティフレームワークを作成し、SecBoKに至っている。しかし、現在でもまだ更新が必要であることから、ベトナムにおいても作成には長い時間がかかるだろう。
・ベトナムの大学でもセキュリティに関するカリキュラムや資格を作りたいと考えており、インドネシアで実施している技術協力プロジェクトには大変興味がある。

Copyright 2025 NPO日本ネットワークセキュリティ協会

カンボジア
CDPインタビューへの活用事例

2023年11月に、カンボジア郵政通信省（Ministry of Post and Telecommunications, MPTC）のICTセキュリティ局の職員9名に対して個別面談を行い、一人一人のキャリア開発計画を作成しました。

キャリア開発計画の作成にあたっては、ベトナムの「サイバーセキュリティに関する能力向上プロジェクト」で確立されたCDP（Career Development Plan）方式を採用しています。CDP方式は、SecBoK（注）をベースとした職務分類と個々人の能力をアセスメントし、それに応じた研修プランを立てて受講させるもので、6ヶ月ごとにレビューを行うことで効果を測定し、プランの見直しを行うことを基本としています。

今後、作成した個人ごとのCDPをもとに年間研修計画を策定し、計画に沿って研修を実施していく予定です。

（注）SecBoK（Security Body of Knowledge）とは、NPO日本ネットワークセキュリティ協会（Japan Network Security Association, JNSA）が作成した、セキュリティ分野における人材スキルマップのことです。セキュリティの業務に必要な役割と、その役割に必要な知識、スキル、技術の対応が示されています。

インタビューの様子（右側がインタビュー対象の職員、左側２名はプロジェクト専門家）

Copyright 2025 NPO日本ネットワークセキュリティ協会

フィリピン
JICA規格競争説明書

2023年4月版

企画競争説明書

業　務　名　称：カンボジア国サイバーセキュリティ能力向上プロジェクト（サイバーセキュリティ）及びフィリピン国サイバーセキュリティ能力開発（サイバーセキュリティ）

調達管理番号：23a00081

【内容構成】

フィリピン国「サイバーセキュリティ能力開発」

（１）成果１に関わる活動

活動 1-1： サイバーセキュリティ局職員に対する研修計画を作成する

1-1-1　セキュリティ業務上の役割と改善すべき知識・技能・能力を明確にする。（National Initiative for Cybersecurity Education（NICE）、Security Body of Knowledge（SecBoK）等のサイバーセキュリティ教育のためのスキル・フレームワーク活用）

1-1-2　研修計画（研修到達目標、研修予定、進捗状況を含む）を作成する。

活動 1-2： セキュリティ研修を実施する

1-2-1　研修計画に基づき、セキュリティ研修を調整・実施する。（一部の研修は現地再委託を想定）

1-2-2　研修の効果を測定し、研修計画をレビューする。

1-2-3　研修計画を更新する。

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

検討経緯について

Copyright 2025 NPO日本ネットワークセキュリティ協会

議論の要旨
SecBoK 2025の方向性について（粒度）

【現状版は細か過ぎる】

- SecBoKやNICEフレームワークは粒度が細かいと感じている。
- 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。

【粗くしないほうがよい】

- 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。職種との対応がわかりにくいという批判には、ロールと実際の人のモデル例を示すのがよい。
- 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お互いの誤解を生みやすい。

【細かいものと詳しいものの両方が欲しい】

- 細かいとパツ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**。
- 学生に見せるためには**粒度が粗いものがよく**、**具体的な内容を扱う際**には「ここに書いてあるだろう」と示せるものがよい。
- 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

議論の要旨
SecBoK 2025の方向性について（役割）

【役割（ロール）について】

- 顧客から「アセッサーとは何か？」という相談をいただくことも多いので、担当者よりも行為でまとめるほうがわかりやすい。

- 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。

Copyright 2025 NPO日本ネットワークセキュリティ協会

議論の要旨
SecBoK 2025の方向性について（使い方）

【使い方】

- 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。

- 「脆弱性診断士の募集」のようなジョブディスクリプションで書きやすいようなエッセンスが加わるとよい。

- 細かすぎると書きにくいと思うので、具体的にこのようなことを書くと良いといったサンプルがあってもよい。

Copyright 2025 NPO日本ネットワークセキュリティ協会

議論の要旨
SecBoK 2025の方向性について（コンピテンシー関連）

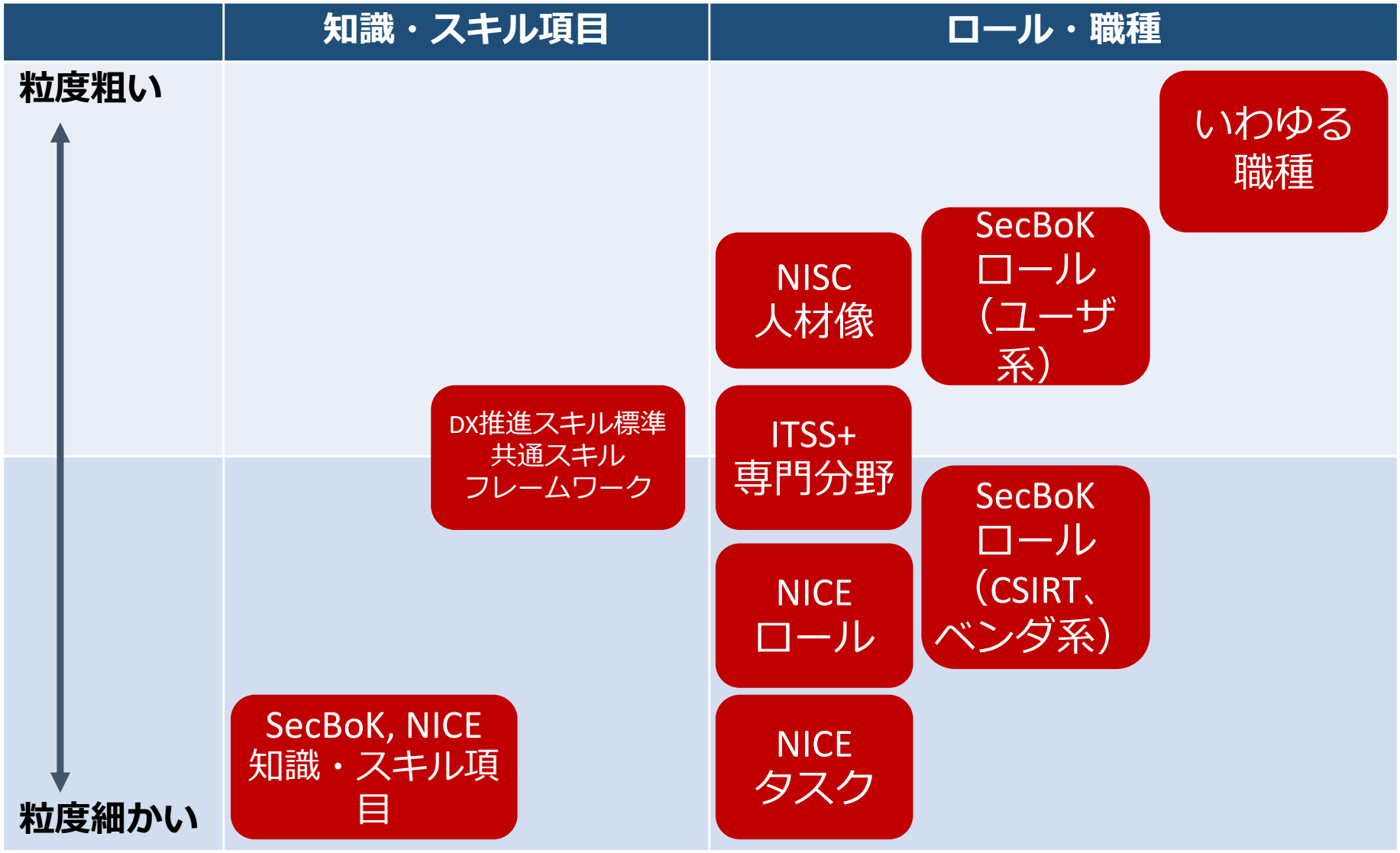
【NICEで扱われるコンピテンシーについて】

- SecBoK2021の検討におけるコンピテンシーやヒューマンスキル的な取組をどうするかの会話において、あくまでセキュリティスキルのディクショナリーであり続けるべきとのまとめにした記憶がある。やるならNICEの定義でやるか、使わないほうがよい。

- コンピテンシーに関して海外のユースケースをみたところで日本と海外で考え方が異なるので、NICEのコンピテンシーを付録的に入れておき、あくまでappendixとして海外で展開するときに参考にしてもらうパターンがよいと思う。

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



Copyright 2025 NPO日本ネットワークセキュリティ協会

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

議論のポイント

- 現状は細かすぎる？粗くしない方がよい？

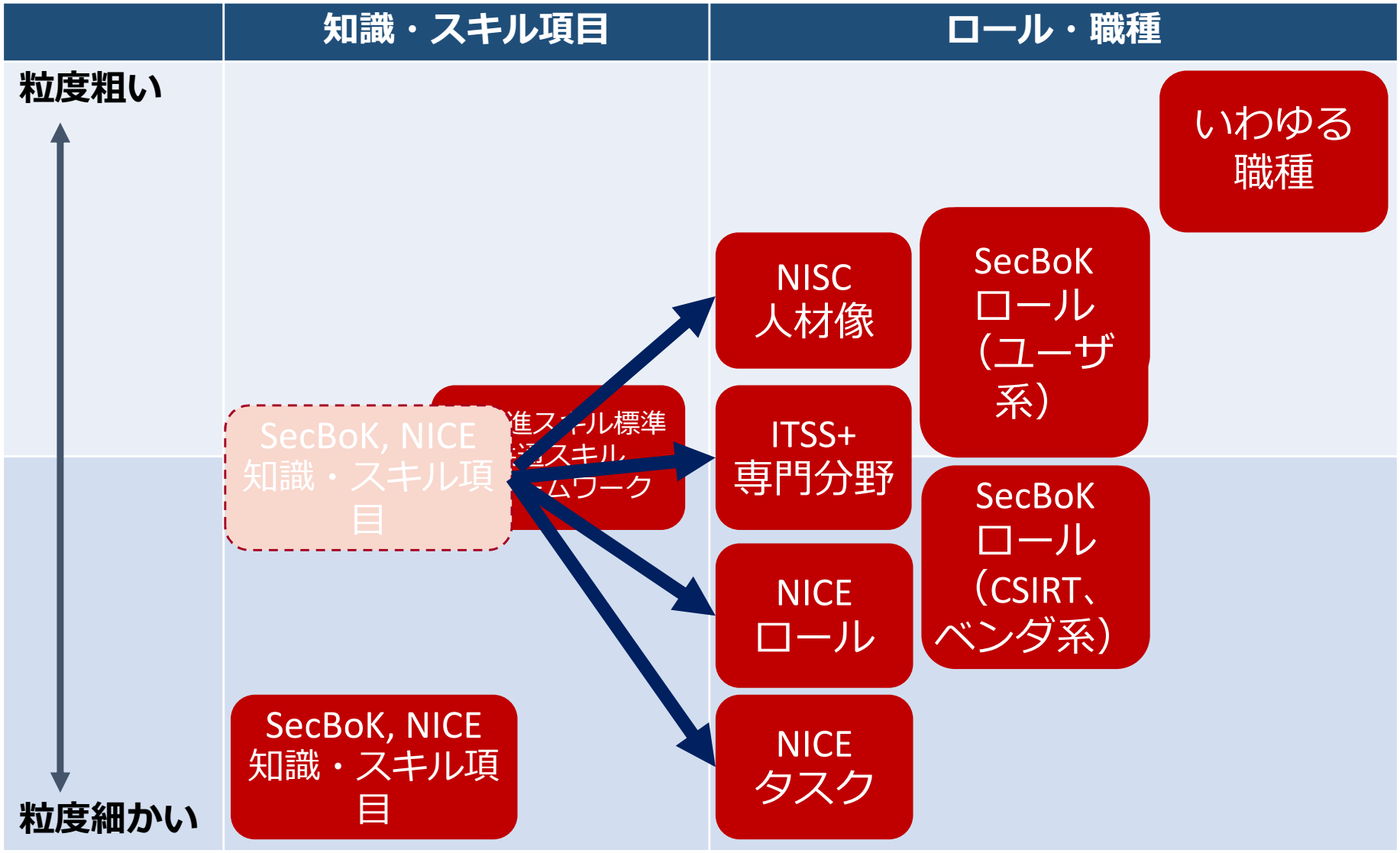
  - 細かすぎて使いにくいという意見を聞く
  - ロールを誰が使うかを考えたとき、細かいものだけがあっても使いにくい
  - NICEフレームワークとの対応表を作るのであれば、職種との対応であまり細かくないものが欲しい
  - 英語の勉強でいきなり辞書を開くことはない。国語辞典に対する図鑑に相当するような、初学者向け、エントリー向けドキュメントがあるとよい。

  - 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。

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の
前段階？メニュー？のようなものが必要か
（大項目、中項目、小項目とは違ったもので）

Copyright 2025 NPO日本ネットワークセキュリティ協会

BoKで、他とのHUBであるならば・・



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

セキュリティ知識分野（SecBoK）人材スキルマップ2021年版 とNICEロールとの対応関係

	SecBoK2021		NICE定義のロール名		NICEにおけるロールの定義
	役割（ロール）	役割定義（ユーザ企業におけるおもな役割）			
1	CISO（最高情報セキュリティ責任者）	社内の情報セキュリティを統括する。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。	1	許可権限者	組織の業務（ミッション、機能、イメージ、評判を含む）、組織資産、個人、その他の組織、国家に許容可能なレベルで情報システムを運用する責任を正式に負う権限を持つ上級管理職または役員。
			27	幹部のサイバーリーダシップ	組織のサイバーおよびサイバー関連の資源及び/又は運用に関する意思決定を行うとともに、ビジョンと方向性を確立する。
			31	IT投資/ポートフォリオ管理者	ミッションと企業の優先度に関する全体的なニーズに合わせたIT投資のポートフォリオを管理する。
2	POC（Point of Contact）	社外向けではJPCERT/CC、NISC、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。		（対応ロールなし）	
3	ノーティフィケーション	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。		（対応ロールなし）	
4	コマンダー	自社で起きているセキュリティインシデントの全体統制を行う。重大なインシデントに関してはCISOや経営層との情報連携を行う。また、CISOや経営者が意思決定する際の支援を行う。	27	幹部のサイバーリーダシップ	組織のサイバーおよびサイバー関連の資源及び/又は運用に関する意思決定を行うとともに、ビジョンと方向性を確立する。
4	トリアージ	事象に対する対応における優先順位を決定する。	27	幹部のサイバーリーダシップ	組織のサイバーおよびサイバー関連の資源及び/又は運用に関する意思決定を行うとともに、ビジョンと方向性を確立する。
5	インシデントマネージャー	インシデントハンドラーに指示を出し、インシデントの対応状況を把握する。対応履歴を管理するとともにコマンダーへ状況を報告する。	35	防衛インシデント対応者	ネットワーク環境またはエンクレーブ内のサイバーインシデントを調査、分析、および対応する。
5	インシデントハンドラー	インシデントの処理を行う。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。状況はインシデントマネージャーに報告する。	35	防衛インシデント対応者	ネットワーク環境またはエンクレーブ内のサイバーインシデントを調査、分析、および対応する。
6	キュレーター	リサーチャーの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。リサーチャーと合わせてSOC（セキュリティオペレーションセンター）とすることが多い。	37	脅威/警告アナリスト	高度にダイナミックなオペレーティング環境の状況を把握するためのサイバー指標を開発する。サイバー脅威/警告評価を収集、処理、分析、および普及させる。
7	リサーチャー	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し、キュレーターに引き渡す。収集のみで分析はしない。	33	サイバー防衛アナリスト	さまざまなサイバー防御ツール（IDSのアラート、ファイアウォール、ネットワークトラフィックログなど）から収集したデータを使用して、脅威を緩和する目的で環境内で発生するイベントを分析する。
8	セルフアセスメント	自社の事業計画に合わせてセキュリティ戦略を策定する。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。	18	システムセキュリティアナリスト	システムセキュリティの統合、テスト、運用、保守の分析と開発を担当する。
8	ソリューションアナリスト	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、影響の調査等に対応する。	18	システムセキュリティアナリスト	システムセキュリティの統合、テスト、運用、保守の分析と開発を担当する。
9	脆弱性診断士	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。	36	脆弱性診断アナリスト	ネットワーク環境内のシステムとネットワークの評価を実施し、それらのシステム/ネットワークが受け入れ可能な構成、特殊又はローカルなポリシーから逸脱している場所を特定する。既知の脆弱性に対する多層防御アーキテクチャの有効性を評価する。
10	教育・啓発	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。	21	サイバー教育カリキュラム開発者	教育上の必要に基づき、サイバーセキュリティを対象とする訓練・教育に関するコース、手法及び技術について開発、立案、調整及び評価する。
			22	サイバーセキュリティインストラクター	サイバーセキュリティ領域における要員の訓練または教育を開発及び主導する。
			25	サイバーセキュリティ要員の育成者・管	サイバー空間の人材、人材、訓練、教育の要件をサポートし、サイバー関連のポリシー、原則、教材、編成、教育訓練の要件に対する変化を扱うためのサイバー空間を対象とする労働力の計画、戦略、指針を開発する。
11	フォレンジックエンジニア	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。	51	法執行フォレンジックアナリスト	サイバー侵入事件に関連するデジタルメディアとログを含めるために、ドキュメンタリーまたは物理的証拠を確立するコンピュータベースの犯罪に関する詳細な調査を実施する。
			52	防衛フォレンジックアナリスト	デジタル証拠を分析し、コンピュータセキュリティインシデントを調査し、システム/ネットワークの脆弱性緩和を支援する有益な情報を導き出す。
12	インベスティゲーター	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。	50	サイバー犯罪捜査員	制御され、文書化された分析および調査技術を使用して、証拠を特定、収集、調査、および保存する。
13	リーガルアドバイザー	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。	19	サイバーリーガルアドバイザー	サイバー法に関するトピックについて、法的な助言や勧告を行う。
14	ＩＴ企画部門	社内のIT利用に関する企画・立案を行う。必要に応じて、ITの利用状況の調査・分析等を行う。	26	サイバーセキュリティ対策方針・戦略の	組織のサイバーセキュリティに関するイニシアチブおよび規制遵守をサポートし、それと整合するようなサイバーセキュリティ計画、戦略、およびポリシーを策定し維持する。
			29	ITプロジェクトマネージャー	情報技術関連プロジェクトを直接管理する。
15	ITシステム部門	社内のITプロジェクトを推進するとともに、アプリケーションシステムの設計、構築、運用、保守等を担当する。	16	ネットワーク運用スペシャリスト	ハードウェアおよび仮想環境を含む、ネットワークサービス/システムの計画、実装、および運用を行う。
			17	システムアドミニストレータ	システムまたはシステムにおける特定のコンポーネントの設定および保守（例：ハードウェアおよびソフトウェアのインストール、構成、更新、ユーザーアカウントの確立および管理、バックアップおよびリカバリタスクの監督または実施、運用上および技術上のセキュリティ管理の実装、組織のセキュリティポリシーと手順への準拠）に関する責任を負う。
			23	情報システムセキュリティ管理者	プログラム、組織、システム等におけるサイバーセキュリティ対策に責任を負う。
			24	通信セキュリティ管理者	組織の通信リソースまたは暗号鍵管理システムの鍵を管理する。
			34	サイバー防衛インフラサポートスペシャ	インフラストラクチャのハードウェアとソフトウェアをテスト、実装、展開、保守、管理する。
16	情報セキュリティ監査人	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、リスクアセスメント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。	32	ITプログラム監査者	標準への準拠状況を判断するため、ITプログラムまたはその個々の構成要素を評価する。

役割（ロール）について
現状ベースの統合・分割

現行SecBoKは、CSIRTのロールを強く意識していた部分もあったが、大枠ではまとめられるロールもある。
一方、より分かりやすくするため、分割した方がよいロールもある。

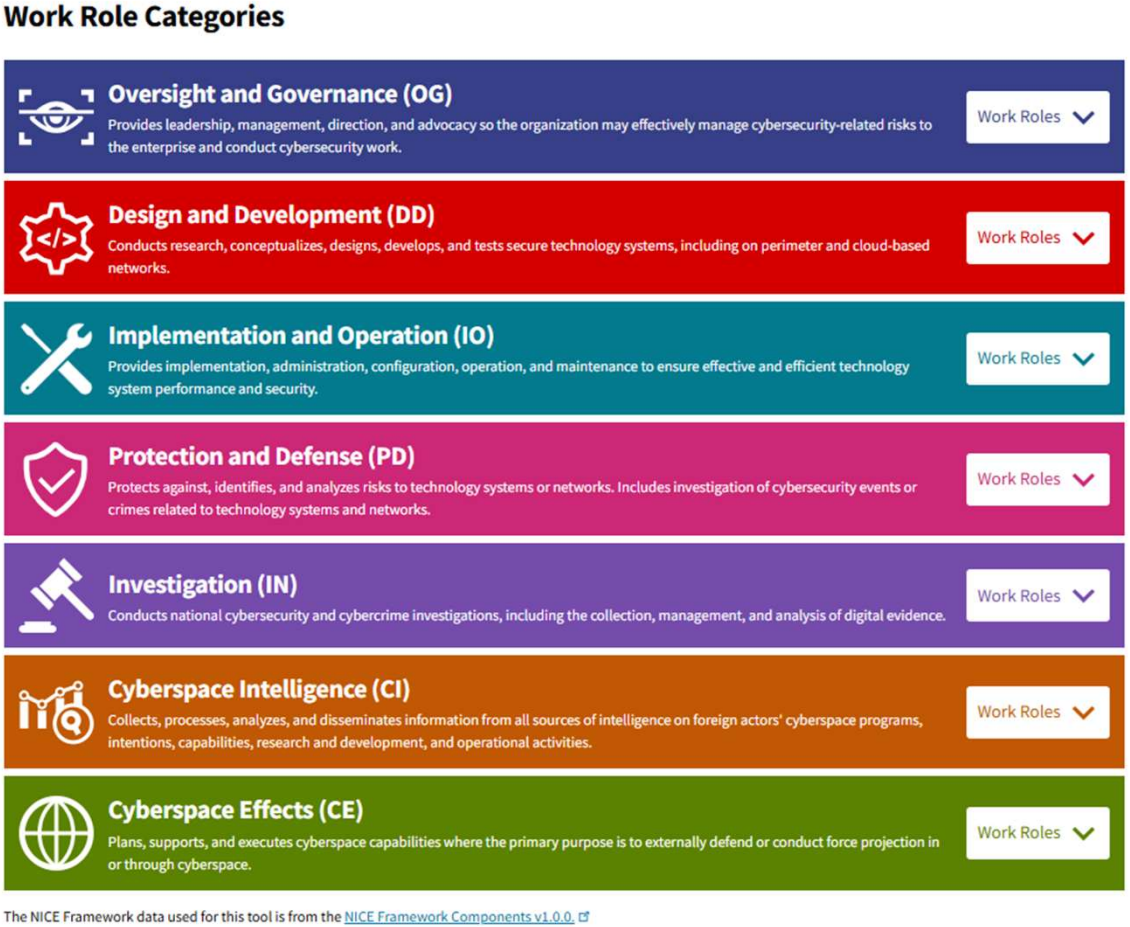
【統合】
- 社内外調整役（POC、ノーティフィケーション）
- インシデント対応PM（コマンダー、トリアージ）
- インシデント対応（マネージャー、ハンドラー）
- 情報収集・分析（リサーチャー、キューレター）
- セキュリティアナリスト（セルフアセスメント、ソリューションアナリスト）

【分割】
- 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
新NICEとのマッピング

NICE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。



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
ITSS+セキュリティとの比較

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。

	区分	分野名	セキュリティ関連タスクの例	担当部署／機能の例（青字は社外ベンダー等）
経営層	デジタル	IT経営（CIO/CDO）	セキュリティ意識啓発、対策方針の指示、セキュリティポリシー・予算・対策実施事項の承認 等	経営者、経営層（CISOを含む）
	セキュリティ	セキュリティ経営（CISO）		
	その他	企業経営（取締役）		
戦略マネジメント層	デジタル	システム監査	システム監査、報告・助言 等	監査部門 ITベンダー・監査法人（システム監査サービス）
		デジタルシステムストラテジー	デジタル事業戦略立案、システム企画、要件定義・仕様書作成、プロジェクトマネジメント 等	経営企画部門、IT企画部門、IT・デジタル部門の企画機能 IT/セキュリティコンサルタント
	セキュリティ	セキュリティ監査	セキュリティ監査、報告・助言 等	監査部門 セキュリティベンダー・監査法人（セキュリティ監査サービス）
		セキュリティ統括	セキュリティ教育・普及啓発、セキュリティ関連の講義・講演、セキュリティリスクアセスメント、セキュリティポリシー・ガイドラインの策定・管理・周知、警察・官公庁等対応、社内相談対応、インシデントハンドリング 等	セキュリティ専門部門、CSIRT セキュリティ委員会 IT・デジタル部門のセキュリティ対策機能
	その他	経営リスクマネジメント	経営リスクマネジメント、BCP／危機管理対応、サイバーセキュリティ保険検討、記者・広報対応、施設管理・物理セキュリティ、内部犯行対策 等	総務部門（リスク管理部門を含む） 経営企画部署、総務部署等のリスクマネジメント機能
		法務	デジタル関連法令対応、コンプライアンス対応、契約管理 等	法務部門、総務部門の法務担当
		事業ドメイン（戦略・企画・調達）	事業特有のリスクの洗い出し、事業特性に応じたセキュリティ対応、サプライチェーン管理 等	事業部門の企画機能 事業戦略コンサルタント
実務者・技術者層	デジタル	デジタルシステムアーキテクチャ	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 等	IT・デジタル部門の設計機能、IT子会社 IT/OTベンダー
		デジタルプロダクト開発	基本設計、詳細設計、セキュアプログラミング、テスト・品質保証、パッチ開発 等	IT・デジタル部門の開発・保守機能、IT子会社 IT/OTベンダー
		デジタルプロダクト運用	構成管理、運用設定、利用者管理、サポート・ヘルプデスク、脆弱性対策・対応、インシデントレスポンス 等	IT・デジタル部門の運用機能、IT子会社 IT/OT/セキュリティベンダー
	セキュリティ	脆弱性診断・ペネトレーションテスト	脆弱性診断、ペネトレーションテスト 等	IT・デジタル部門の運用機能、IT子会社 セキュリティベンダー（脆弱性診断サービス）
		セキュリティ監視・運用	セキュリティ製品・サービスの導入・運用、セキュリティ監視・検知・対応、インシデントレスポンス、連絡受付 等	IT・デジタル部門の運用機能、IT子会社 セキュリティベンダー（セキュリティ監視・運用サービス）
		セキュリティ調査分析・研究開発	サイバー攻撃捜査、原因究明・フォレンジック、マルウェア解析、脅威・脆弱性情報の収集・分析・活用、セキュリティ理論・技術の研究開発、セキュリティ市場動向調査 等	CSIRT/IT・デジタル部門のリサーチ機能、IT子会社 セキュリティベンダー（デジタルフォレンジックサービス）
	その他	事業ドメイン（生産現場・事業所管理）	現場教育・管理、設備管理・保全、QC活動、初動対応 等	運転、保全、計装、品質管理関連部署、PSIRT OT/セキュリティベンダー

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
職業情報提供サイトとの比較

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。

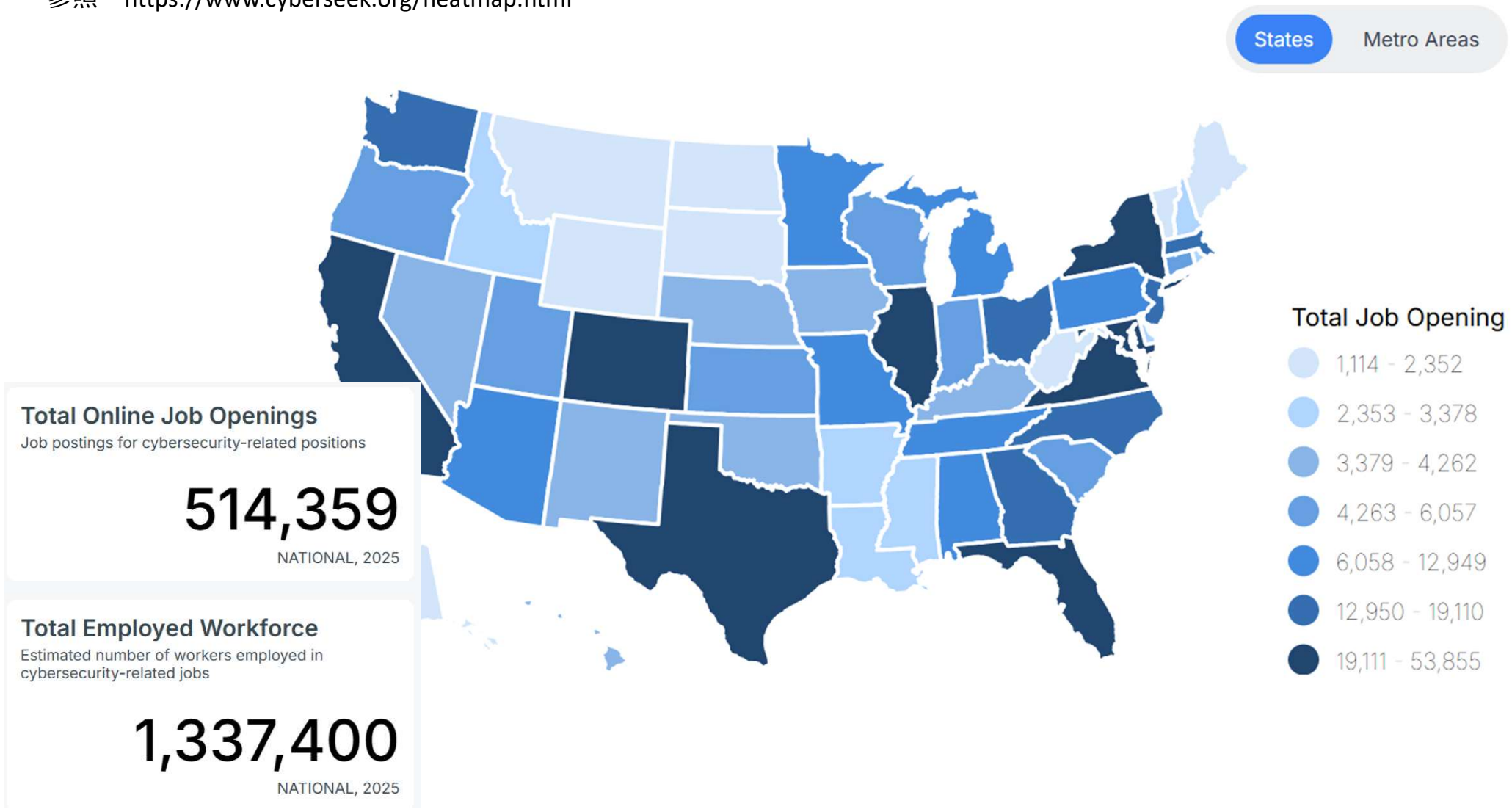
120	プログラマー
121	システムエンジニア（業務用システム）
122	システムエンジニア（基盤システム）
123	システムエンジニア（Webサイト開発）
124	システムエンジニア（組込み、IoT）
125	ソフトウェア開発（パッケージソフト）
126	ソフトウエア開発（スマホアプリ）
127	運用・管理（IT）
128	セキュリティエキスパート（オペレーション）
129	ヘルプデスク（IT）
130	プロジェクトマネージャ（IT）
131	ITコンサルタント
132	営業（IT）
133	データサイエンティスト
134	AIエンジニア
135	デジタルビジネスイノベーター

15-1111.00	Computer and Information Research Scientists
15-1121.00	Computer Systems Analysts
15-1121.01	Informatics Nurse Specialists
15-1122.00	Information Security Analysts
15-1131.00	Computer Programmers
15-1132.00	Software Developers, Applications
15-1133.00	Software Developers, Systems Software
15-1134.00	Web Developers
15-1141.00	Database Administrators
15-1142.00	Network and Computer Systems Administrators
15-1143.00	Computer Network Architects
15-1143.01	Telecommunications Engineering Specialists
15-1151.00	Computer User Support Specialists
15-1152.00	Computer Network Support Specialists
15-1199.01	Software Quality Assurance Engineers and Testers
15-1199.02	Computer Systems Engineers/Architects
15-1199.03	Web Administrators
15-1199.04	Geospatial Information Scientists and Technologists
15-1199.05	Geographic Information Systems Technicians
15-1199.06	Database Architects
15-1199.07	Data Warehousing Specialists
15-1199.08	Business Intelligence Analysts
15-1199.09	Information Technology Project Managers
15-1199.10	Search Marketing Strategists
15-1199.11	Video Game Designers
15-1199.12	Document Management Specialists
15-2011.00	Actuaries
15-2021.00	Mathematicians
15-2031.00	Operations Research Analysts
15-2041.00	Statisticians
15-2041.01	Biostatisticians
15-2041.02	Clinical Data Managers
15-2091.00	Mathematical Technicians

Copyright 2025 NPO日本ネットワークセキュリティ協会

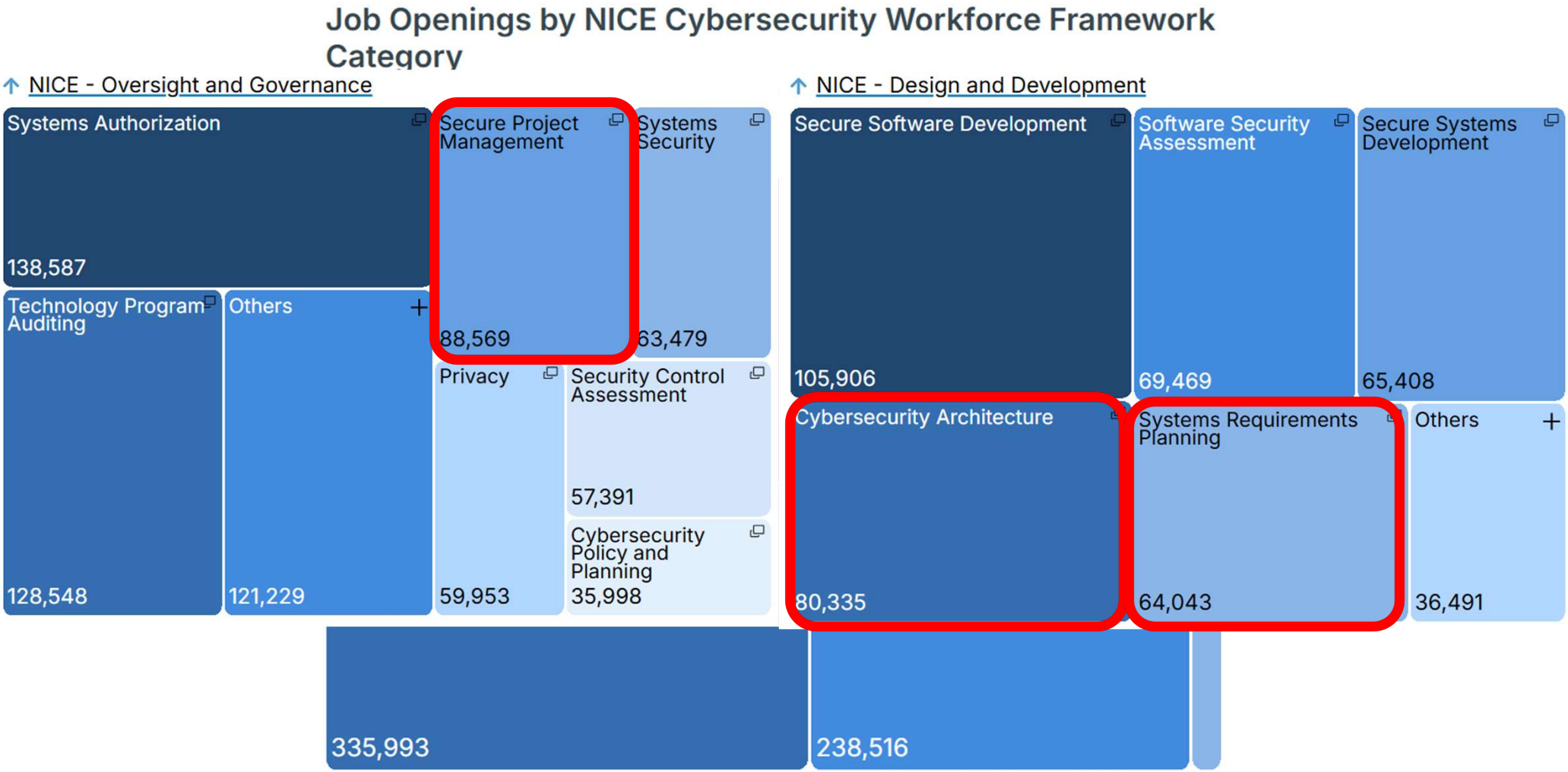
参考：
米国でのセキュリティ業界への就労度

参照　https://www.cyberseek.org/heatmap.html



Copyright 2025　NPO日本ネットワークセキュリティ協会

参考：さらに、詳細を見ていくと



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）案

Copyright 2025 NPO日本ネットワークセキュリティ協会

若手の育成
セキュリティ人材の裾野拡大

Copyright 2025 NPO日本ネットワークセキュリティ協会

教育部会ワーキンググループ

●情報セキュリティ教育実証WG

情報セキュリティを教えることが出来る高度なスキルをもった人材を育成するために、実践での大学などでの講義を通じて、実践力とハイレベルスキルの習得を目的とする。
また作成した成果物（講義コンテンツ）のJNSA会員企業への共有と他の学校関連や団体への展開を計画している。

●ゲーム教育WG

サイバーセキュリティのボードゲームやカードゲーム、ゲーミフィケーション要素のあるイベントや教育などに関わる調査や企画、当WG制作の「セキュリティ専門家人狼」「Malware Containment」の普及プロモーションや講師派遣(主に大学・高専等の教育機関)、ゲーム教育のファシリテーター育成等を行う。

●教育部会産学連携プロジェクト

JNSA教育部会と教育機関（大学、高専、専門学校等）との産学連携活動（主に学生向けの講座やイベント「セキュリティチャレンジスクール」「セキュリティカフェ」）の企画・運営、講師派遣による実施当を行う。

●セキュ女WG

会社の枠を超えた連携を可能にし、女性セキュリティエキスパートの交流場所を提供する。
また、セキュリティに関する専門スキルを持ちたい女性を応援するための活動を行う。

Copyright 2025 NPO日本ネットワークセキュリティ協会

教育部会ワーキンググループ

●情報セキュリティ教育実証WG

情報セキュリティを教えることが出来る高度なスキルをもった人材を育成するために、実践
での大学などでの講義を通じて、実践力とハイレベルスキルの習得を目的とする。
また作成した成果物（講義
他の学校関連や団体への
展開を計画して

●ゲ

サ

●

JNS
の講
座やイ
・運営、
講師派遣によ

教育部会各ワーキンググループへの
参加をお待ちしております！

●セキュ女WG

会社の枠を超えた連携を可能にし、女性セキュリティエキスパートの交流場所を提供する。
また、セキュリティに関する専門スキルを持ちたい女性を応援するための活動を行う。

Copyright 2025 NPO日本ネットワークセキュリティ協会

Copyright 2025 NPO日本ネットワークセキュリティ協会