人材定義リファレンス2026

解説書

v1.0（初版公開）

2026年7月21日

産業横断サイバーセキュリティ検討会

WG1：セキュリティ経営戦略検討WG

目次

1. はじめに
2. 人材定義リファレンス2026 用語の定義
3. 人材定義リファレンス2026が想定する体制モデル
4. 人材定義リファレンス2026
5. 人材定義リファレンス2026の活用方法
6. 人材定義リファレンス2016と2026 ― 継承と発展
7. NCO人材フレームワークとの関係及び位置付け
8. 参考資料　人材定義リファレンス改定の経緯
9. 参考資料　CRIC CSF 第6期 活動報告書（抜粋）

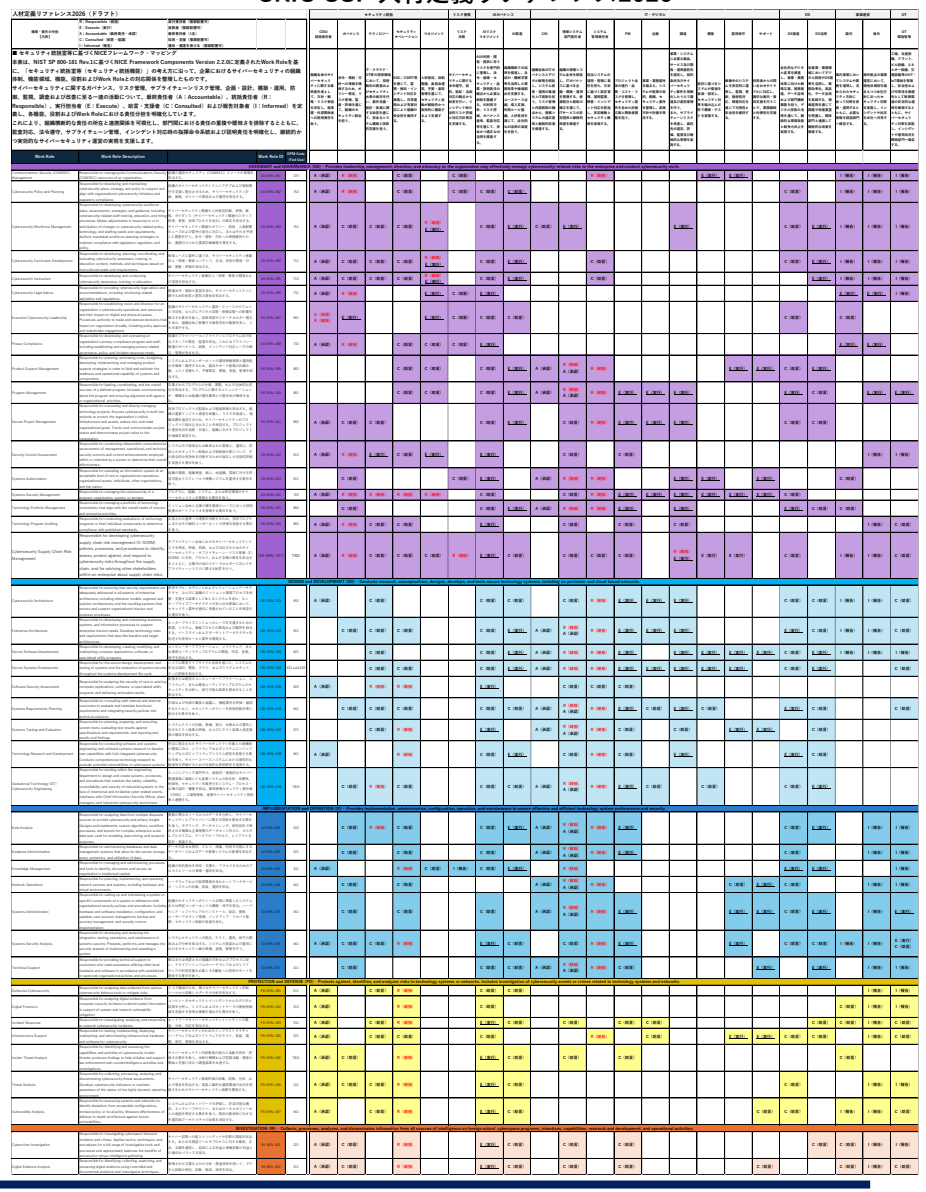


図0　人材定義リファレンス2026

1．はじめに

- 我が国におけるサイバーセキュリティ人材の育成と組織体制の整備については、産業横断サイバーセキュリティ検討会（CRIC CSF）において継続的に検討を進めてきました。
- **本検討会は、2015年6月、重要インフラ分野を中心とする企業の有志により「産業横断サイバーセキュリティ人材育成検討会」として発足しました。**東京2020オリンピック・パラリンピック競技大会を見据え、**産業界が共通して活用できるサイバーセキュリティ人材の考え方と組織体制を整理することを目的として活動を開始しました。**
- その成果として、**2016年に「サイバーセキュリティ人材定義リファレンス」を公表**し、ユーザ企業に必要なサイバーセキュリティ人材の役割、機能及び業務を体系的に定義しました。また、**2018年には、本リファレンスで定義した主要な機能の一つである「セキュリティ統括室等」の具体的な構築・運用方法を示した「セキュリティ統括室構築・運用キット」を公表**し、企業における組織横断的なサイバーセキュリティ推進体制の整備を支援してきました。
- これらの成果は、経済産業省及びIPAが整備を進めたITSS+（プラス）のセキュリティ領域においても参考資料として活用され、**「セキュリティ統括」の考え方は、企業における人材育成及び組織体制整備の参考として広く参照されています。**

出典）情報処理推進機構（IPA）デジタル人材の育成
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/about.html

1．はじめに

- 一方、2020年頃から企業におけるクラウドサービスの利用が本格化し、ゼロトラストアーキテクチャを前提としたシステム構成への移行が進みました。さらに、SaaSの普及、データ利活用の拡大、サプライチェーン全体を対象としたリスクマネジメントの重要性の高まりにより、**サイバーセキュリティは情報システム部門だけの課題ではなく、経営層、事業部門、さらには取引先や委託先を含めたサプライチェーン全体で取り組むべき経営課題へと発展しています**。
- 加えて、**2023年以降は生成AIの急速な普及により、AIガバナンス、AIリスクマネジメント、データ管理及び説明責任など、新たな役割や専門性が求められるようになりました**。また、OT（Operational Technology）やIoTを含むサイバー・フィジカル・システムへの対応も重要性を増しており、従来のIT環境を前提とした人材体系だけでは十分に対応できない状況となっています。
- こうした環境変化を踏まえ、産業横断サイバーセキュリティ検討会では、2023年から人材定義リファレンスの改定に着手し、クラウドサービス、ゼロトラスト、OT・IoT及び生成AIなどの技術動向を踏まえながら、**ユーザ企業に求められる組織体制、人材像及び役割分担について検討を進め、その成果を「人材定義リファレンス2026」として取りまとめました**。

• 人材定義リファレンス2026が表現する世界

- 図1は、本リファレンス全体の考え方を示したものです。本書では、この考え方に沿って、組織体制、機能領域、機能、役割及び責任分担を説明するとともに、NICE Frameworkとの対応関係について解説します。

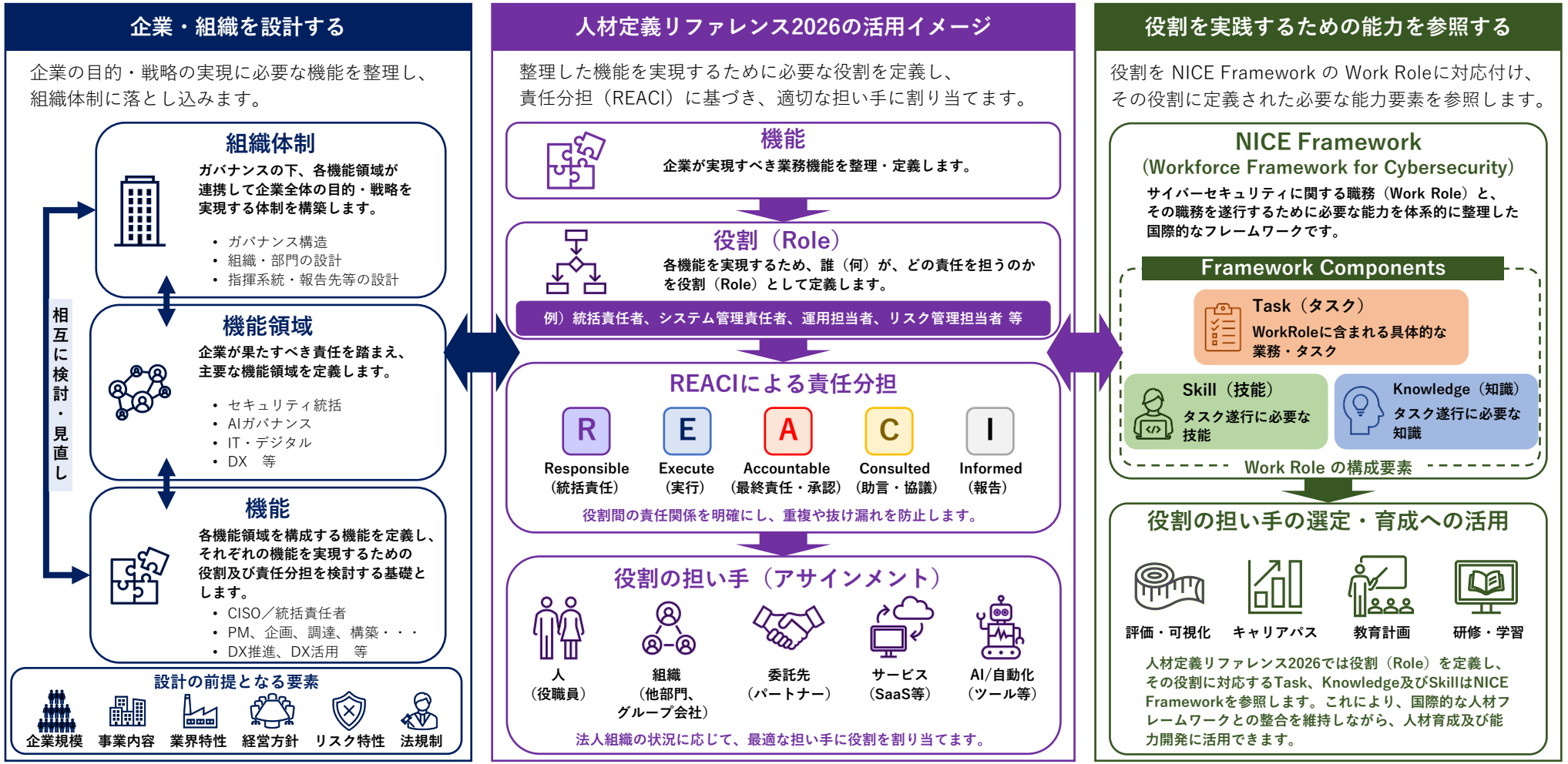


図1　人材定義リファレンス2026が表現する世界

- **本改定では、2016年版の基本理念を継承しつつ、現在の企業環境や技術動向を反映するとともに、NIST SP 800-181（NICE Framework Components）のWork Roleとの対応関係を整理しました。**一方、本リファレンスはNICE Framework Componentsをそのまま採用するものではなく、日本企業の組織体制、役割分担及びガバナンスを前提とした実践的な人材定義として再構成しています。
- 本解説書では、本リファレンスで用いる用語、想定する組織体制モデル、本リファレンスの構成と内容、活用方法、2016年版からの継承と発展、さらに国家サイバー統括室（NCO）が公表する「サイバーセキュリティ人材フレームワーク」との関係について解説します。なお、巻末には、本リファレンスの改定の経緯などを参考資料として掲載しています。
- **本リファレンスは、ユーザ企業及び団体においてサイバーセキュリティ体制の整備・運営に携わる経営層、CISO、セキュリティ統括室等、情報システム部門、人事・教育部門、内部監査部門などを主な対象としています。**
- 人材育成、組織設計、役割・責任の明確化及びガバナンス体制の整備など幅広い実務での活用を想定しており、ユーザ企業の規模、事業特性及びリスクに応じて柔軟に適用できるリファレンスです。**なお、本リファレンスにおいて「ユーザ企業」とは、製品・サービスを提供するベンダ企業に対し、それらを利用して事業活動を行う企業をいいます。**

2026年7月21日
産業横断サイバーセキュリティ検討会

２．人材定義リファレンス2026
用語の定義

2.1　組織体制に対する用語の定義の考え方

- **本リファレンスは、ユーザ企業におけるサイバーセキュリティ体制の整備及び人材育成を支援することを目的として策定しています。**そのため、本リファレンスでは、ユーザ企業に必要な組織体制を起点として、機能領域、機能、役割及び業務を体系的に整理しています。
- 一方、サイバーセキュリティに関する文献やフレームワークでは、「組織」「機能」「役割」「業務」などの用語が統一された意味で用いられているとは限らず、同じ用語でも文書によって指す対象が異なる場合があります。
- **本リファレンスでは、利用者が役割や責任範囲を正しく理解し、ユーザ企業の実情に応じた組織体制を設計できるよう、これらの用語を明確に定義しています。**
- 次節では、本リファレンスで使用する主要な用語について説明します。

	組織体制																					
機能領域	セキュリティ統括					リスク管理	AIガバナンス		IT・デジタル									DX		事業運営		OT
機能	CISO 統括責任者	ガバナンス	テクノロジー	セキュリティ オペレーション	マネジメント	リスク 法務	AIリスク マネジメント	AI推進	CIO	情報システム 部門責任者	システム 管理責任者	PM	企画	調達	構築	運用保守	サポート	DX推進	DX活用	国内	海外	OT 環境管理
役割	組織全体のサイバーセキュリティに関する最終責任者として、方針・戦略・リスク受容を決定し、経営層・外部関係者への説明責任を負う。	法令・規制・方針への準拠を確保するため、ポリシー策定、リスク管理、監査・評価を通じて、組織のセキュリティ統治を担う。	IT・クラウド・OT等の技術領域において、技術動向の調査およびセキュリティ水準の検討を行い、要件定義・設計・実装に関する助言を通じて、安全なシステム構築と技術的支援を担う。	SOC／CSIRT等を通じて、監視・検知・インシデント対応を実施し、日常運用および有事対応により組織の安全性を維持する。	人材育成、体制整備、委員会運営、予算・委託管理を通じて、セキュリティ活動が継続的かつ実効的に機能するよう支援する。	サイバーセキュリティに関する法令遵守、契約、訴訟・当局対応の観点から助言を行い、インシデント時の法的リスク評価と対応方針策定を支援する。	AIの利用・開発・提供に伴うリスクを専門的に管理し、法令・倫理・セキュリティ・品質・説明責任の観点から必要な統制を整備する。AI利用方針、リスク評価、ガバナンス基準、監査対応等を通じて、安全かつ適正なAI活用を推進する。	組織横断でAI活用を推進し、生成AI・機械学習等を活用した業務改革や価値創出を支援する。ユースケース企画、導入支援、利用ルール整備、人材育成を通じて、全社的なAI活用の高度化を担う。	組織全体のITガバナンスとデジタル戦略を統括し、システム投資・運用の最適化とIT統制を担う。リスク管理と内部統制の観点から、情報システムの適正運用と継続的改善を推進する。	組織の情報システム全体を統括し、ITガバナンスに基づき企画・構築・運用を管理する。資源配分と統制の確立を通じて、ITサービスの安定提供と継続的改善を推進する。	担当システムの運用・管理に責任を持ち、方針に基づく設定管理、運用監視、障害・インシデント対応を統括し、安定稼働とセキュリティ確保を実現する。	プロジェクト全体の進行・品質・コスト・リスクを管理し、セキュリティ要件を含めた計画立案と関係者調整を担う。	事業・業務要件を踏まえ、システムや施策の目的、範囲、セキュリティ要件を整理し、実現方針や計画を策定する。	要件に基づき製品・サービス・委託先を選定し、契約条件やセキュリティ要件を明確化したうえで適切な調達を行う。	設計に基づきシステムや環境を実装・設定し、セキュリティ対策を組み込んだ形で構築・テストを実施する。	稼働中のシステムを安定的に運用し、監視、更新、脆弱性対応、障害対応を通じて可用性と安全性を維持する。	利用者からの問い合わせやトラブルに対応し、適切な案内・復旧支援を行うことで、業務継続と利便性を支援する。	全社的なデジタル変革を推進し、事業・業務改革に向けた戦略立案、施策推進、データ活用および部門横断調整を担う。デジタル技術の活用を通じて、継続的な業務改善と競争力向上を実現する。	各事業・業務領域においてデジタル技術やDX施策を活用し、業務効率化、高度化、データ活用を実践する。現場運用を通じて課題や改善要望を把握し、関係部門と連携して継続的な改善を推進する。	国内事業においてシステムや業務を運用し、定められたセキュリティ方針に従って対策を実装・運用するとともに、必要な情報を統括部門へ報告する。	海外拠点の事業運営において、現地法規制を踏まえつつ本社方針に沿ったセキュリティ対策を実施し、インシデントや状況を本社へ共有する。	工場、生産設備、プラント、ビル設備、エネルギー設備、交通設備等のOT・IoT環境を管理し、安全性および可用性を最優先として物理環境の安定的な運用を確保するとともに、サイバーセキュリティ対策を実施し、インシデントや運用状況を関係部門へ報告する。

表2-1　組織体制に対する用語の定義の考え方

2.2　本リファレンスにおける用語の定義

- 本リファレンスでは、サイバーセキュリティに関する組織体制を体系的に整理するため、主要な用語を次のとおり定義します。

用語	定義
組織体制 Organization Structure	**ユーザ企業がサイバーセキュリティを推進するために構築する全体の体制**をいいます。ユーザ企業の規模、事業内容、経営方針及びリスク特性に応じて組織名称や構成は異なりますが、本リファレンスでは、ユーザ企業全体で必要な責務及び役割を実現するための体制全体を対象とします。
機能領域 Functional Domain	**サイバーセキュリティに関する責務を目的又は対象に応じて分類した上位区分**をいいます。本リファレンスでは、「セキュリティ統括」「リスク管理」「AIガバナンス」「IT・デジタル」「DX」「事業運営」「OT」を機能領域として定義します。
機能 Function	**各機能領域においてユーザ企業が継続的に果たすべき責務及び活動を体系的に整理した単位**をいいます。一つの機能には、その機能を実現するための役割及び業務を定義します。例えば、「ガバナンス」「テクノロジー」「セキュリティオペレーション」「マネジメント」は、セキュリティ統括機能領域を構成する機能です。
役割 Role	**機能を実現するために定義する責任及び期待される役目**をいいます。役割は、人だけでなく、組織、委託先、サービス又はAI等の担い手に割り当てることを想定しており、日本企業における組織体制を前提として定義しています。本リファレンスにおける役割は、NICE Framework ComponentsのWork Roleとは異なる概念です。
業務 Task / Activity	**役割を果たすために実施する具体的な活動**をいいます。業務には、方針策定、企画、設計、構築、運用、監視、教育、監査、インシデント対応等、役割を実現するために実施する活動が含まれます。

表2-2　人材定義リファレンス2026　用語の定義

- なお、本リファレンスでは、ユーザ企業に必要な組織体制を起点として、「機能領域」「機能」「役割」及び「業務」を体系的に整理しています。また、各役割についてはNICE Framework ComponentsのWork Roleとの対応関係を示していますが、本リファレンスにおける役割をWork Roleとして定義し、又は置き換えるものではありません。
- Work Roleは、本リファレンスで整理した役割に対応する専門的な職務との関係を示すものです。

2.3　本リファレンスの基本構造

- 本リファレンスでは、組織体制を起点として、機能領域、機能、役割及び業務の階層で整理しています。

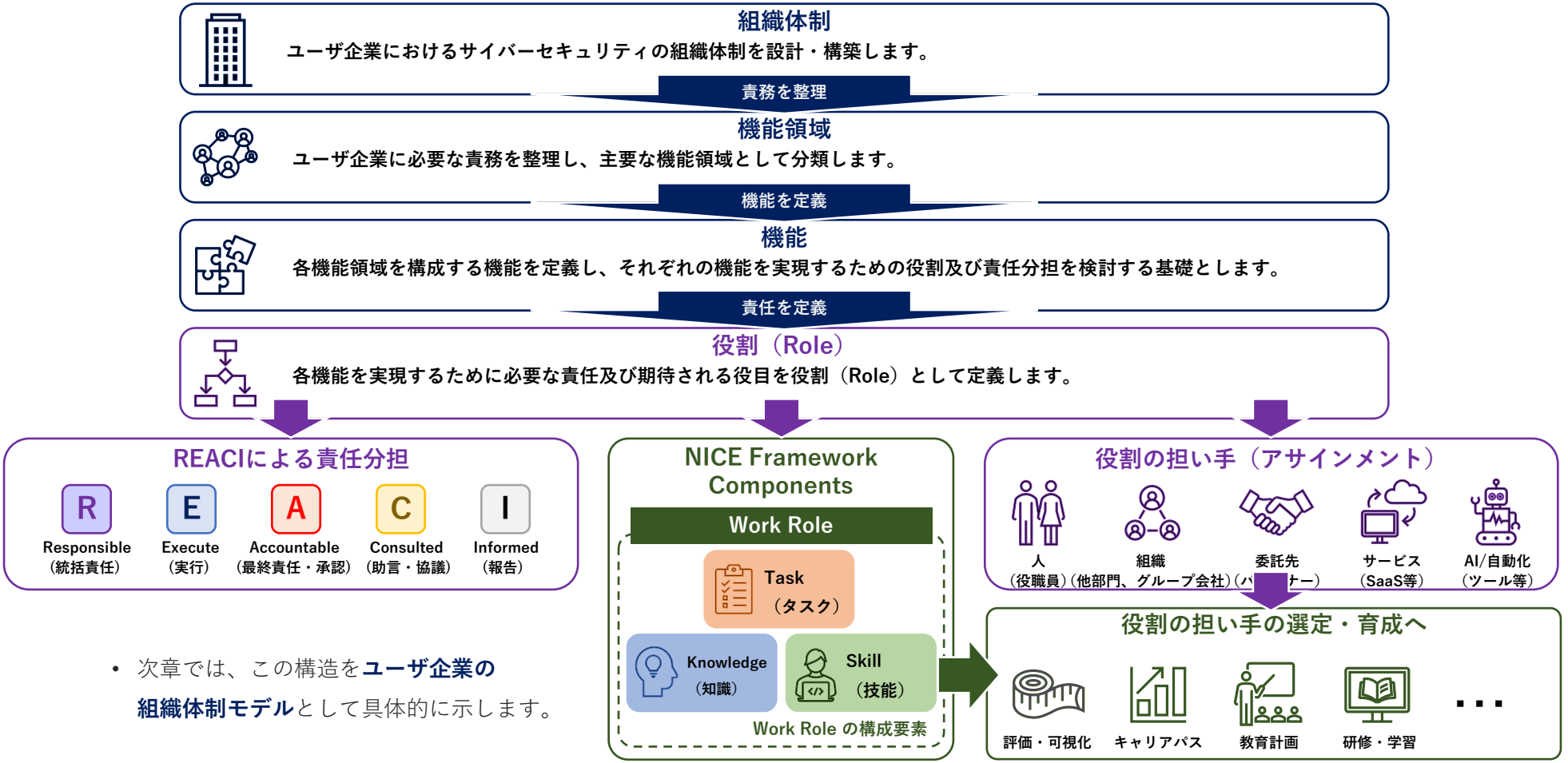


図2-3　人材定義リファレンス2026の基本構造

- 次章では、この構造を**ユーザ企業の組織体制モデル**として具体的に示します。

３．人材定義リファレンス2026が想定する組織体制モデル

3.1　人材定義リファレンス2026において想定する組織体制の基本的な考え方

- 従来、多くの企業では、サイバーセキュリティを情報システム部門や情報セキュリティ部門の責任として位置付け、システムやネットワークを保護するための技術的対策を中心に取り組んできました。しかし、企業を取り巻く事業環境や技術環境の変化に伴い、このような考え方だけでは十分な対応が難しくなっています。
- 近年では、クラウドサービスの利用拡大、DXの推進、生成AIの活用、サプライチェーンの複雑化、さらにOT（Operational Technology）やIoTを含むサイバー・フィジカル・システムの普及により、サイバーセキュリティは企業全体で取り組むべき経営課題となっています。そのため、経営層をはじめ、事業部門、情報システム部門、DX推進部門、OT管理部門、人事部門、法務部門及び内部監査部門など、多様な組織がそれぞれの役割を担いながら連携することが求められます。
- このような環境では、個々の部門が独立して対策を講じるだけでは十分ではありません。経営方針に基づく統一的なガバナンスのもと、各組織が役割と責任を果たしながら連携する組織体制を構築することが重要です。
- **本リファレンスでは、この考え方に基づき、ユーザ企業における一般的な組織体制を想定した「組織体制モデル」を示しています。本モデルは、ユーザ企業に必要な機能領域、機能及び役割を整理した参照モデルであり、特定の組織名称や組織構成を規定するものではありません。ユーザ企業は、自社の規模、事業特性、リスク特性及び経営方針に応じて、本モデルを参考に組織体制を設計することを想定しています。**

3.2　人材定義リファレンス2026において想定する組織体制のモデル

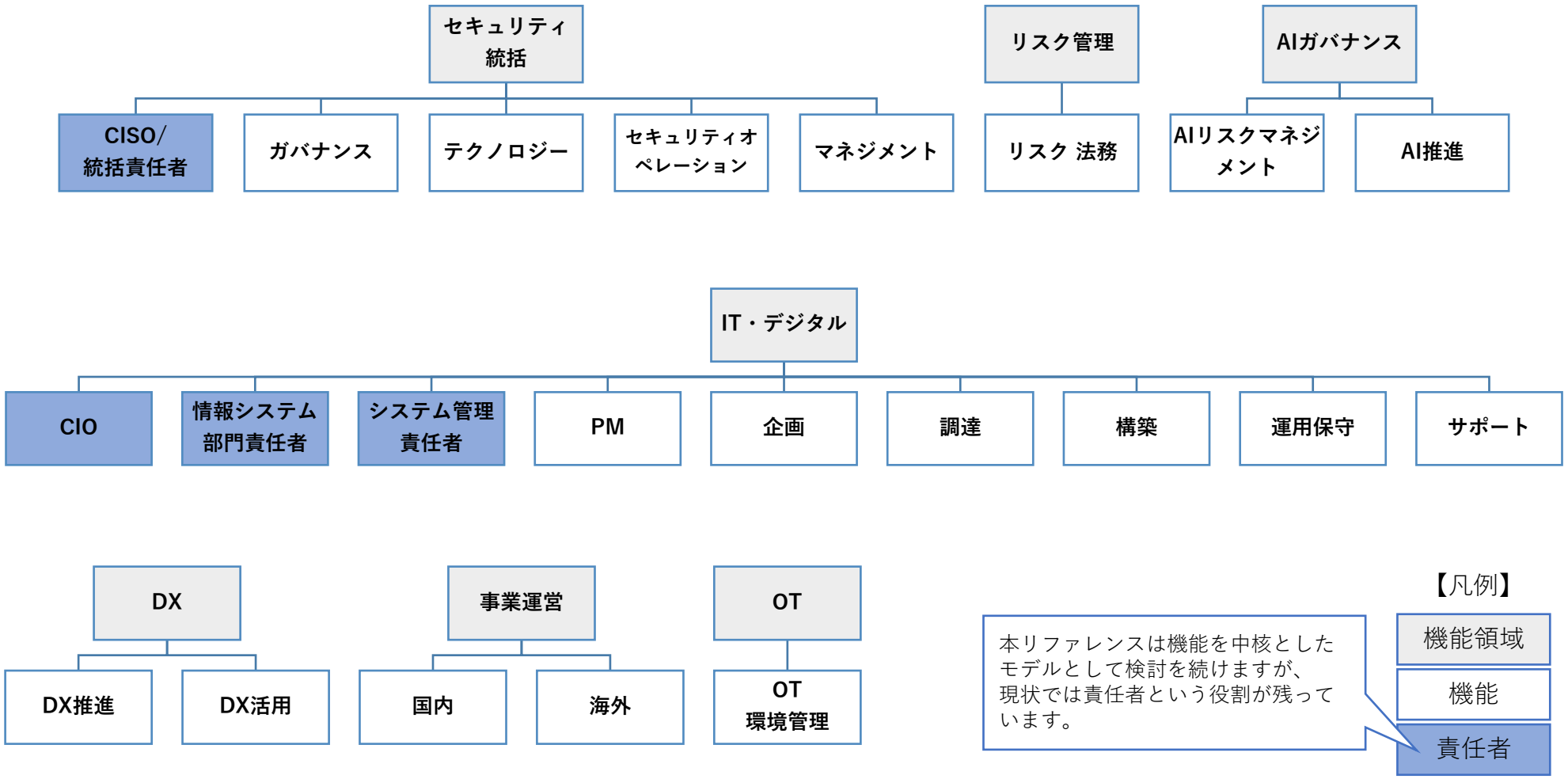


図3-2　人材定義リファレンス2026において想定する組織体制のモデル

3.3　組織体制モデルの考え方

- 前ページは、本リファレンスが想定する組織体制モデルを示したものです。
- 本モデルでは、セキュリティ統括を中心に、リスク管理、AIガバナンス、IT・デジタル、DX、事業運営及びOTを機能領域として整理し、それぞれが必要な機能を担いながら相互に連携することで、組織全体のサイバーセキュリティを実現することを想定しています。
- **本モデルは、ユーザ企業に必要な機能領域、機能及び役割を整理した参照モデルであり、組織名称や部門構成を規定するものではありません。ユーザ企業の規模、事業特性、リスク特性及び経営方針に応じて、一つの組織が複数の機能を担うことや、一人が複数の役割を兼務することも想定しています。**
- また、本リファレンスでは、各機能に対応する役割及び責任を整理するとともに、NICE Framework ComponentsのWork Roleとの対応関係を示しています。
- 重要なのは組織名称ではなく、ユーザ企業として必要な機能を備え、それぞれの役割と責任を明確にすることです。

3.4　各機能領域を構成する機能と役割例：全ての機能領域

	機能領域	機能	役割
組織体制	セキュリティ統括	CISO／統括責任者	組織全体のサイバーセキュリティに関する最終責任者として、方針・戦略・リスク受容を決定し、経営層・外部関係者への説明責任を負う。
		ガバナンス	法令・規制・方針への準拠を確保するため、ポリシー策定、リスク管理、監査・評価を通じて、組織のセキュリティ統治を担う。
		テクノロジー	IT・クラウド・OT等の技術領域において、技術動向の調査およびセキュリティ水準の検討を行い、要件定義・設計・実装に関する助言を通じて、安全なシステム構築と技術的支援を担う。
		セキュリティオペレーション	SOC／CSIRT等を通じて、監視・検知・インシデント対応を実施し、日常運用および有事対応により組織の安全性を維持する。
		マネジメント	人材育成、体制整備、委員会運営、予算・委託管理を通じて、セキュリティ活動が継続的かつ実効的に機能するよう支援する。
	リスク管理	リスク・法務	サイバーセキュリティに関する法令遵守、契約、訴訟・当局対応の観点から助言を行い、インシデント時の法的リスク評価と対応方針策定を支援する。
	AIガバナンス	AIリスクマネジメント	AIの利用・開発・提供に伴うリスクを専門的に管理し、法令・倫理・セキュリティ・品質・説明責任の観点から必要な統制を整備する。AI利用方針、リスク評価、ガバナンス基準、監査対応等を通じて、安全かつ適正なAI活用を推進する。
		AI推進	組織横断でAI活用を推進し、生成AI・機械学習等を活用した業務改革や価値創出を支援する。ユースケース企画、導入支援、利用ルール整備、人材育成を通じて、全社的なAI活用の高度化を担う。
	IT・デジタル	CIO	組織全体のITガバナンスとデジタル戦略を統括し、システム投資・運用の最適化とIT統制を担う。リスク管理と内部統制の観点から、情報システムの適正運用と継続的改善を推進する。
		情報システム部門責任者	組織の情報システム全体を統括し、ITガバナンスに基づき企画・構築・運用を管理する。資源配分と統制の確立を通じて、ITサービスの安定提供と継続的改善を推進する。
		システム管理責任者	担当システムの運用・管理に責任を持ち、方針に基づく設定管理、運用監視、障害・インシデント対応を統括し、安定稼働とセキュリティ確保を実現する。
		PM	プロジェクト全体の進行・品質・コスト・リスクを管理し、セキュリティ要件を含めた計画立案と関係者調整を担う。
		企画	事業・業務要件を踏まえ、システムや施策の目的、範囲、セキュリティ要件を整理し、実現方針や計画を策定する。
		調達	事業・システムに必要な製品、サービス及び開発・運用委託先を選定し、契約条件及びサイバーセキュリティ要件を明確化したうえで調達及び委託管理を行う。また、サプライチェーンリスクを考慮し、委託先の選定、評価、監督及び継続的な管理を実施する。
		構築	設計に基づきシステムや環境を実装・設定し、セキュリティ対策を組み込んだ形で構築・テストを実施する。
		運用保守	稼働中のシステムを安定的に運用し、監視、更新、脆弱性対応、障害対応を通じて可用性と安全性を維持する。
		サポート	利用者からの問い合わせやトラブルに対応し、適切な案内・復旧支援を行うことで、業務継続と利便性を支援する。
	DX	DX推進	全社的なデジタル変革を推進し、事業・業務改革に向けた戦略立案、施策推進、データ活用および部門横断調整を担う。デジタル技術の活用を通じて、継続的な業務改善と競争力向上を実現する。
		DX活用	各事業・業務領域においてデジタル技術やDX施策を活用し、業務効率化、高度化、データ活用を実践する。現場運用を通じて課題や改善要望を把握し、関係部門と連携して継続的な改善を推進する。
	事業運営	国内	国内事業においてシステムや業務を運用し、定められたセキュリティ方針に従って対策を実装・運用するとともに、必要な情報を統括部門へ報告する。
		海外	海外拠点の事業運営において、現地法規制を踏まえつつ本社方針に沿ったセキュリティ対策を実施し、インシデントや状況を本社へ共有する。
	OT	OT環境管理	工場、生産設備、プラント、ビル設備、エネルギー設備、交通設備等のOT・IoT環境を管理し、安全性および可用性を最優先として物理環境の安定的な運用を確保するとともに、サイバーセキュリティ対策を実施し、インシデントや運用状況を関係部門へ報告する。

表3-4-1　各機能領域を構成する機能と役割例：全ての機能領域

3.4　各機能領域を構成する機能と役割例：セキュリティ統括、リスク管理

	機能領域	機能	役割
組織体制	セキュリティ統括	CISO／統括責任者	組織全体のサイバーセキュリティに関する最終責任者として、方針・戦略・リスク受容を決定し、経営層・外部関係者への説明責任を負う。
		ガバナンス	法令・規制・方針への準拠を確保するため、ポリシー策定、リスク管理、監査・評価を通じて、組織のセキュリティ統治を担う。
		テクノロジー	IT・クラウド・OT等の技術領域において、技術動向の調査およびセキュリティ水準の検討を行い、要件定義・設計・実装に関する助言を通じて、安全なシステム構築と技術的支援を担う。
		セキュリティオペレーション	SOC／CSIRT等を通じて、監視・検知・インシデント対応を実施し、日常運用および有事対応により組織の安全性を維持する。
		マネジメント	人材育成、体制整備、委員会運営、予算・委託管理を通じて、セキュリティ活動が継続的かつ実効的に機能するよう支援する。
	リスク管理	リスク・法務	サイバーセキュリティに関する法令遵守、契約、訴訟・当局対応の観点から助言を行い、インシデント時の法的リスク評価と対応方針策定を支援する。

表3-4-2　各機能領域を構成する機能と役割例：セキュリティ統括、リスク管理

3.4　各機能領域を構成する機能と役割例：AIガバナンス

	機能領域	機能	役割
組織体制	AIガバナンス	AIリスクマネジメント	**AIの利用・開発・提供に伴うリスクを専門的に管理し、法令・倫理・セキュリティ・品質・説明責任の観点から必要な統制を整備する。AI利用方針、リスク評価、ガバナンス基準、監査対応等を通じて、安全かつ適正なAI活用を推進する。**
		AI推進	**組織横断でAI活用を推進し、生成AI・機械学習等を活用した業務改革や価値創出を支援する。ユースケース企画、導入支援、利用ルール整備、人材育成を通じて、全社的なAI活用の高度化を担う。**

表3-4-2　各機能領域を構成する機能と役割例：セキュリティ統括、リスク管理、AIガバナンス

- なお、AIに関する二つの機能は議論の途中であり、今後、定義の見直しを実施する予定です。

AIリスクマネジメント	AI推進
主に次の要素を担います。 • AI利用方針、ガバナンス基準及び責任体制の整備 • AIの企画、開発、導入、利用、運用及び廃止におけるリスク評価 • 法令、倫理、人権、公平性、透明性及び説明責任への対応 • AIの精度、信頼性、安全性及び品質に関する評価 • 学習データ、入力データ、出力結果及びログの管理 • AIモデル、基盤モデル、API、OSS、外部サービス等のサプライチェーンリスク管理 • プロンプトインジェクション、データ汚染、モデル窃取等のAI固有のセキュリティリスクへの対応 • AIインシデント、不適切出力、誤判断及び想定外動作への対応 • AI利用状況の監視、監査、是正及び継続的改善 • 高リスクなAI利用に対する承認、制限又は停止の判断支援	**主に次の要素を担います。** • AI活用戦略、ロードマップ及び導入計画の策定 • 業務課題や事業課題に応じたAIユースケースの企画 • 生成AI、機械学習、AIエージェント等の導入及び活用支援 • AIを活用した業務改革、効率化、高度化及び価値創出 • AI製品、サービス、モデル及びツールの選定支援 • PoC、試行導入、本番導入及び全社展開の推進 • AI利用部門、情報システム部門、開発部門及び外部委託先との調整 • AI活用に必要な人材育成、教育及びリテラシー向上 • 利用事例、ノウハウ、プロンプト、テンプレート等の共有 • AI活用の効果測定、利用状況の把握及び改善 • AIリスクマネジメントが定めた基準を、実際の導入・利用プロセスへ反映

表3-4-3　機能領域「AIガバナンス」を構成する機能「AIリスクマネジメント」と「AI推進」の役割分担イメージ

3.4　各機能領域を構成する機能と役割例：IT・デジタル

	機能領域	機能	役割
組織体制	IT・デジタル	CIO	組織全体のITガバナンスとデジタル戦略を統括し、システム投資・運用の最適化とIT統制を担う。リスク管理と内部統制の観点から、情報システムの適正運用と継続的改善を推進する。
		情報システム部門責任者	組織の情報システム全体を統括し、ITガバナンスに基づき企画・構築・運用を管理する。資源配分と統制の確立を通じて、ITサービスの安定提供と継続的改善を推進する。
		システム管理責任者	担当システムの運用・管理に責任を持ち、方針に基づく設定管理、運用監視、障害・インシデント対応を統括し、安定稼働とセキュリティ確保を実現する。
		PM	プロジェクト全体の進行・品質・コスト・リスクを管理し、セキュリティ要件を含めた計画立案と関係者調整を担う。
		企画	事業・業務要件を踏まえ、システムや施策の目的、範囲、セキュリティ要件を整理し、実現方針や計画を策定する。
		調達	事業・システムに必要な製品、サービス及び開発・運用委託先を選定し、契約条件及びサイバーセキュリティ要件を明確化したうえで調達及び委託管理を行う。また、サプライチェーンリスクを考慮し、委託先の選定、評価、監督及び継続的な管理を実施する。
		構築	設計に基づきシステムや環境を実装・設定し、セキュリティ対策を組み込んだ形で構築・テストを実施する。
		運用保守	稼働中のシステムを安定的に運用し、監視、更新、脆弱性対応、障害対応を通じて可用性と安全性を維持する。
		サポート	利用者からの問い合わせやトラブルに対応し、適切な案内・復旧支援を行うことで、業務継続と利便性を支援する。

表3-4-5　各機能領域を構成する機能と役割例：IT・デジタル

3.4　各機能領域を構成する機能と役割例：DX、事業運営、OT

	機能領域	機能	役割
組織体制	DX	DX推進	全社的なデジタル変革を推進し、事業・業務改革に向けた戦略立案、施策推進、データ活用および部門横断調整を担う。デジタル技術の活用を通じて、継続的な業務改善と競争力向上を実現する。
		DX活用	各事業・業務領域においてデジタル技術やDX施策を活用し、業務効率化、高度化、データ活用を実践する。現場運用を通じて課題や改善要望を把握し、関係部門と連携して継続的な改善を推進する。
	事業運営	国内	国内事業においてシステムや業務を運用し、定められたセキュリティ方針に従って対策を実装・運用するとともに、必要な情報を統括部門へ報告する。
		海外	海外拠点の事業運営において、現地法規制を踏まえつつ本社方針に沿ったセキュリティ対策を実施し、インシデントや状況を本社へ共有する。
	OT	OT環境管理	工場、生産設備、プラント、ビル設備、エネルギー設備、交通設備等のOT・IoT環境を管理し、安全性および可用性を最優先として物理環境の安定的な運用を確保するとともに、サイバーセキュリティ対策を実施し、インシデントや運用状況を関係部門へ報告する。

表3-4-6　各機能領域を構成する機能と役割例：DX、事業運営、OT

3.5　組織体制モデルの適用

- **本章で示した組織体制モデルは、ユーザ企業におけるサイバーセキュリティ推進体制を検討するための参照モデルです。すべての組織が同一の組織体制を採用することを前提とするものではなく、企業の規模、事業特性、リスク特性及び経営方針に応じて柔軟に適用することを想定しています。**
- 組織体制を検討する際には、組織名称や部門構成ではなく、ユーザ企業として必要な機能を明確にし、それぞれの役割と責任を適切に定めることが重要です。また、一つの組織が複数の機能を担うことや、一人が複数の役割を兼務することも想定されます。
- 組織体制モデルを適用する際の主な考え方を、次表に示します。

項目	考え方
標準モデル	本モデルは、ユーザ企業に求められる組織体制の標準的なモデルを示すものであり、すべての企業に同一の組織構成を求めるものではありません。
組織名称	「セキュリティ統括室」「情報システム部」などの組織名称は企業ごとに異なります。重要なのは組織名称ではなく、必要な機能領域及び機能を備えることです。
機能の集約・分散	企業の規模や組織構成に応じて、一つの組織が複数の機能を担うことや、一つの機能を複数の組織で分担することができます。
役割の兼務	一人が複数の役割を兼務することを妨げるものではありません。企業の実情に応じて柔軟に役割を配置することができます。
子会社・海外拠点	子会社や海外拠点では、企業規模や事業内容に応じて組織体制を簡素化することができます。ただし、本社との役割分担及び連携体制を明確にすることが重要です。
外部委託	SOC、CSIRT、監視、教育などの機能を外部へ委託することも想定しています。委託する場合であっても、企業として必要な責任及び管理は維持する必要があります。
適用の考え方	企業の規模、事業内容、リスク特性及び経営方針に応じて柔軟に適用し、必要な機能領域、機能及び役割を備えることを重視します。

表3-5　組織体制モデルの適用

４．人材定義リファレンス2026

4.1　人材定義リファレンス2026の基本構造（組織間の連携による実践）

- 第4章では、本リファレンスが想定する組織体制モデルについて説明しました。
- 本章では、その組織体制を構成する各機能について、役割、責任及び業務を整理するとともに、NICE Framework ComponentsのWork Roleとの対応関係を示します。
- **本リファレンスは、企業ごとの組織名称や人員配置を定めるものではなく、ユーザ企業に必要な役割と責任を体系的に整理することを目的としています。**

	組織体制																					
機能領域	セキュリティ統括					リスク管理	AIガバナンス		IT・デジタル									DX		事業運営		OT
機能	CISO 統括責任者	ガバナンス	テクノロジー	セキュリティ オペレーション	マネジメント	リスク 法務	AIリスク マネジメント	AI推進	CIO	情報システム 部門責任者	システム 管理責任者	PM	企画	調達	構築	運用保守	サポート	DX推進	DX活用	国内	海外	OT 環境管理
役割	組織全体のサイバーセキュリティに関する最終責任者として、方針・戦略・リスク受容を決定し、経営層・外部関係者への説明責任を負う。	法令・規制・方針への準拠を確保するため、ポリシー策定、リスク管理、監査・評価を通じて、組織のセキュリティ統治を担う。	IT・クラウド・OT等の技術領域において、技術動向の調査およびセキュリ[illegible]水準の検討を行い、要件定義・設計・実装に関する助言を通じて、安全なシステム構築と技術的支援を担う。	SOC／CS[illegible]を通じて、監[illegible]実施し、日常運用および有事対応により組織の安全性を維持する。	[illegible]整備、委員会運[illegible]セキュリティ活動が継続的かつ実効的に機能するよう支援する。	サイバー[illegible]リティに関する法令遵守[illegible]対応の観点から助言を行い、インシデント時の法的リスク評価と対応方針策定を支援する。	AIの利用・開発・提供に伴うリスクを専門的[illegible]キュリティ・品[illegible]説明責任の[illegible]から必要な統制を整備する。AI利用方針、リスク評価、ガバナンス基準、監査対応等を通じて、安全かつ適正なAI活用を推進する。	組織横断でAI活[illegible]推進し、[illegible]成AI、機械学習等を活用した業[illegible]ユースケース企画、導入支援、利用ルール整備、人材育成を通じて、全社的なAI活用の高度化を担う。	組織全体のITガ[illegible]タル戦略を統括し、システム投[illegible]化とIT統制を担う。リスク管理と内部統制の観点から、情報システムの適正運用と継続的改善を推進する。	組織の情報シス[illegible]を管理する。資源配分と統制の確立を通じて、ITサービスの安定提供と継続的改善を推進する。	担当システムの運用・管理に責任を持ち、[illegible]理、運用監視、障害・インシデント対応を統括し、安定稼働とセキュリティ確保を実現する。	プロジェクト全体の進行・品[illegible]スクを管理し、セキュリティ要件を含めた計画立案と関係者調整を担う。	事業・業務要件を踏まえ、シス[illegible]的、範囲、セキュリティ要件を整理し、実現方針や計画を策定する。	要件に基づき製品・サービス・委託先を選定し、契約条件やセキュリティ要件を明確化したうえで適切な調達を行う。	設計に基づきシ[illegible]セキュリティ対策を組み込んだ形で構築・テストを実施する。	稼働中のシステムを安定的に運[illegible]、脆弱性対応、障害対応を通じて可用性と安全性を維持する。	利用者からの問い合わせやトラブルに対応し、適切な案内・復旧支援を行うことで、業務継続と利便性を支援する。	全社的なデジタル変革を推進し、事業・業務改革に向けた戦略立案・施策[illegible]進、データ活用および部門横断調整を担う。デジタル技術の活用を通じて、継続的な業務改善と競争力向上を実現する。	各事業・業務領域においてデジタル技術やDX施策を活用し、業務効率化、高度化、データ活用を実践する。現場運用を通じて課題や改善要望を把握し、関係部門と連携して継続的な改善を推進する。	国内事業においてシステムや業務を運用し、定められたセキュリティ方針に従って対策を実装・運用するとともに、必要な情報を統括部門へ報告する。	海外拠点の事業運営において、現地法規制を踏まえつつ本社方針に沿ったセキュリティ対策を実施し、インシデントや状況を本社へ共有する。	工場、生産設備、プラント、ビル設備、エネルギー設備、交通設備等のOT・IoT環境を管理し、安全性および可用性を最優先として物理環境の安定的な運用を確保するとともに、サイバーセキュリティ対策を実施し、インシデントや運用状況を関係部門へ報告する。

サイバーセキュリティを情報システム部門だけの活動ではなく、経営層、事業部門、DX推進部門、OT管理部門、法務、調達など、多様な組織が連携して推進する組織横断的な活動として位置付けています。

図4-1　人材定義リファレンス2026の基本構造（組織間の連携による実践）

4.2　人材定義リファレンス2026の全体像

- 本表は、**NIST SP 800-181 Rev.1に基づくNICE Framework Components Version 2.2.0**に定義されたWork Roleを基に、**「セキュリティ統括室等（セキュリティ統括機能）」**の考え方に沿って、**企業におけるサイバーセキュリティの組織体制、機能領域、機能、役割およびWork Roleとの対応関係を整理したものです。**
- サイバーセキュリティに関するガバナンス、リスク管理、サプライチェーンリスク管理、企画・設計、構築・運用、防御、監視、調査および改善に至る一連の活動について、**最終責任者（A：Accountable）、統括責任者（R：Responsible）、実行担当者（E：Execute）、助言・支援者（C：Consulted）および報告対象者（I：Informed）を定義し、各機能、役割　およびWork Roleにおける責任分担を明確化しています。**
- これにより、組織横断的な責任の所在と連携関係を可視化し、部門間における責任の重複や曖昧さを排除するとともに、監査対応、法令遵守、サプライチェーン管理、インシデント対応時の指揮命令系統および説明責任を明確化し、継続的かつ実効的なサイバーセキュリティ運営の実現を支援します。

CRIC CSF 人材定義リファレンス2026

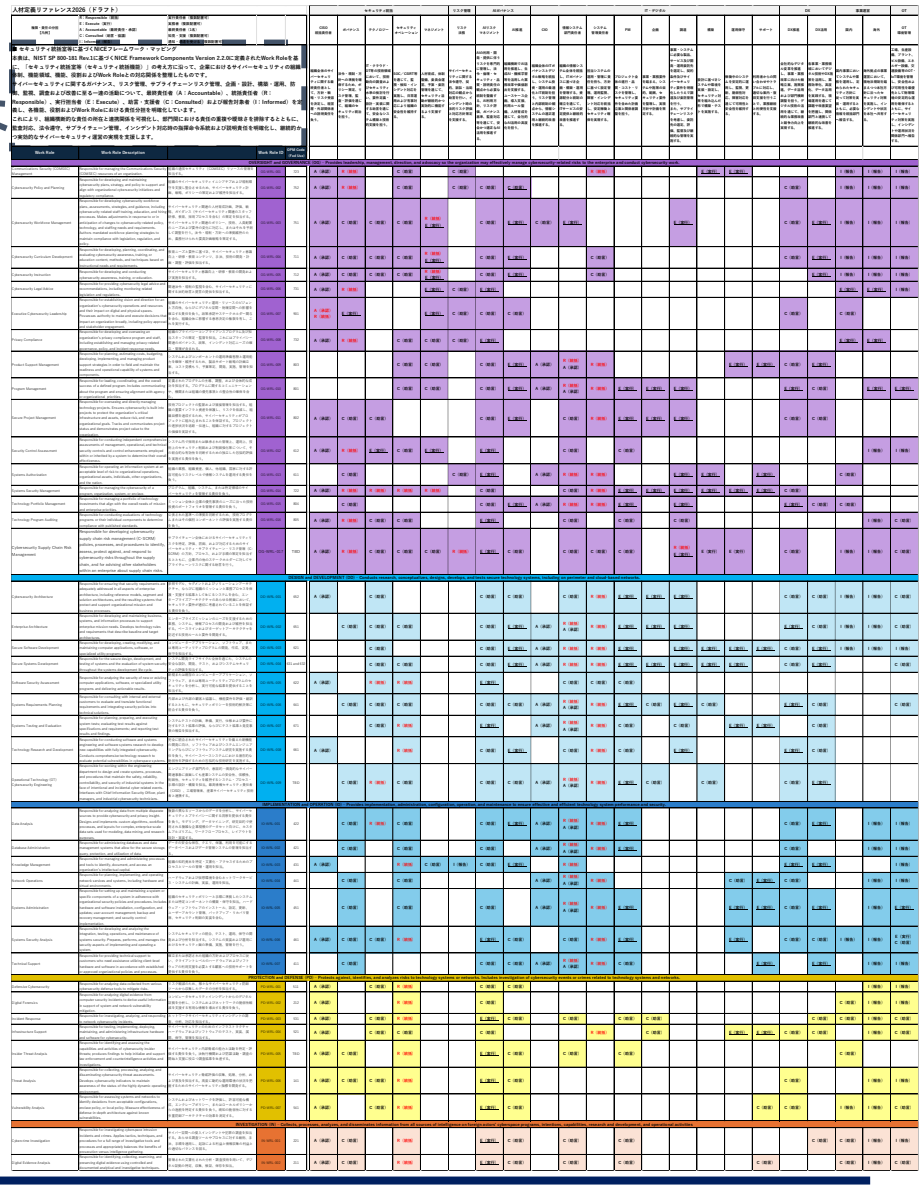


図0　人材定義リファレンス2026

4.3　人材定義リファレンス2026の考え方

- **本リファレンスは、ユーザ企業に必要な組織体制を起点として、機能、役割及び業務を体系的に整理した実務リファレンスです。**
- 各役割は特定の組織や役職に固定されるものではなく、企業の規模や組織構成に応じて、一人が複数の役割を兼務することや、一つの役割を複数の担当者で分担することを想定しています。
- また、本リファレンスでは、企業ごとの組織名称や役職ではなく、ユーザ企業に必要な役割と責任を基準として整理しています。以下に、役割を兼務する場合の例を示します。

セキュリティ統括					リスク管理	AIガバナンス		IT・デジタル								DX		事業運営		OT
CISO 統括責任者	ガバナンス	テクノロジー	セキュリティ オペレーション	マネジメント	リスク 法務	AIリスク マネジメント	AI推進	CIO	情報システム 部門責任者	システム 管理責任者	PM	企画	調達	構築	運用保守	サポート	DX推進	DX活用	国内	海外	OT 環境管理
組織全体のサイバーセキュリティに関する最終責任者として、方針・戦略・リスク受容を決定し、経営層・外部関係者への説明責任を負う。	法令・規制・方針への準拠を確保するため、ポリシー策定、リスク管理、監査・評価を通じて、組織のセキュリティ統治を担う。	IT・クラウド・OT等の技術領域において、技術動向の調査およびセキュリティ水準の検討を行い、要件定義・設計・実装に関する助言を通じて、安全なシステム構築と技術的支援を担う。	SOC／CSIRT等を通じて、監視・検知・インシデント対応を実施し、日常運用および有事対応により組織の安全性を維持する。	人材育成、体制整備、委員会運営、予算・委託管理を通じて、セキュリティ活動が継続的かつ実効的に機能するよう支援する。	サイバーセキュリティに関する法令遵守、契約、訴訟・当局対応の観点から助言を行い、インシデント時の法的リスク評価と対応方針策定を支援する。	AIの利用・開発・提供に伴うリスクを専門的に管理し、法令・倫理・セキュリティ・品質・説明責任の観点から必要な統制を整備する。AI利用方針、リスク評価、ガバナンス基準、監査対応等を通じて、安全かつ適正なAI活用を推進する。	組織横断でAI活用を推進し、生成AI・機械学習等を活用した業務改革や価値創出を支援する。ユースケース企画、導入支援、利用ルール整備、人材育成を通じて、全社的なAI活用の高度化を担う。	組織全体のITガバナンスとデジタル戦略を統括し、システム投資・運用の最適化とIT統制を担う。リスク管理と内部統制の観点から、情報システムの適正運用と継続的改善を推進する。	組織の情報システム全体を統括し、ITガバナンスに基づき企画・構築・運用を管理する。資源配分と統制の確立を通じて、ITサービスの安定提供と継続的改善を推進する。	担当システムの運用・管理に責任を持ち、方針に基づく設定管理、運用監視、障害・インシデント対応を統括し、安定稼働とセキュリティ確保を実現する。	プロジェクト全体の進行・品質・コスト・リスクを管理し、セキュリティ要件を含めた計画立案と関係者調整を担う。	事業・業務要件を踏まえ、システムや施策の目的、範囲、セキュリティ要件を整理し、実現方針や計画を策定する。	要件に基づき製品・サービス・委託先を選定し、契約条件やセキュリティ要件を明確化したうえで適切な調達を行う。	設計に基づきシステムや環境を実装・設定し、セキュリティ対策を組み込んだ形で構築・テストを実施する。	稼働中のシステムを安定的に運用し、監視、更新、脆弱性対応、障害対応を通じて可用性と安全性を維持する。	利用者からの問い合わせやトラブルに対応し、適切な案内・復旧支援を行うことで、業務継続と利便性を支援する。	全社的なデジタル変革を推進し、事業・業務改革に向けた戦略立案、施策推進、データ活用および部門横断調整を担う。デジタル技術の活用を通じて、継続的な業務改善と競争力向上を実現する。	各事業・業務領域においてデジタル技術やDX施策を活用し、業務効率化、高度化、データ活用を実践する。現場運用を通じて課題や改善要望を把握し、関係部門と連携して継続的な改善を推進する。	国内事業においてシステムや業務を運用し、定められたセキュリティ方針に従って対策を実装・運用するとともに、必要な情報を統括部門へ報告する。	海外拠点の事業運営において、現地法規制を踏まえつつ本社方針に沿ったセキュリティ対策を実施し、インシデントや状況を本社へ共有する。	工場、生産設備、プラント、ビル設備、エネルギー設備、交通設備等のOT・IoT環境を管理し、安全性および可用性を最優先として物理環境の安定的な運用を確保するとともに、サイバーセキュリティ対策を実施し、インシデントや運用状況を関係部門へ報告する。

システム企画担当　　**システム運用担当**

図4-3　人材定義リファレンス2026を活用した兼務の例

4.4　人材定義リファレンス2026の構成（NICE Framework ComponentsとREACI）

- **本リファレンスでは、各機能について、役割、業務、REACIによる責任分担及びNICE Framework ComponentsのWork Roleとの対応関係を整理しています。**
- これにより、ユーザ企業に必要な役割と責任を明確にするとともに、組織設計、人材配置、人材育成、規程整備などの実務に活用することができます。
- 本リファレンスの構成を図4-4に示します。

OVERSIGHT and GOVERNANCE (OG) – Provides leadership, management, direction, and advocacy so the organization may effectively manage cybersecurity-related risks to the enterprise and conduct cybersecurity work.										
Communications Security (COMSEC) Management	Responsible for managing the Communications Security (COMSEC) resources of an organization.	組織の通信セキュリティ（COMSEC）リソースの管理を担当する。	OG-WRL-001	723	A（承認）	R（統括）		C（助言）		I（報告）
Cybersecurity Policy and Planning	Responsible for developing and maintaining cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.	組織のサイバーセキュリティイニシアチブおよび規制順守を支援し整合させるため、サイバーセキュリティ計画、戦略、ポリシーの策定および維持を担当する。	OG-WRL-002	752	A（承認）	R（統括）		C（助言）		I（報告）
Cybersecurity Workforce Management	Responsible for developing cybersecurity workforce plans, assessments, strategies, and guidance, including cybersecurity-related staff training, education, and hiring processes. Makes adjustments in response to or in anticipation of changes to cybersecurity-related policy, technology, and staffing needs and requirements. Authors mandated workforce planning strategies to maintain compliance with legislation, regulation, and policy.	サイバーセキュリティ関連の人材育成計画、評価、戦略、ガイダンス（サイバーセキュリティ関連のスタッフ研修、教育、採用プロセスを含む）の策定を担当する。サイバーセキュリティ関連のポリシー、技術、人員配置のニーズおよび要件の変化に対応し、またはそれを予測して調整を行う。法令・規制・方針への準拠維持のため、義務付けられた要員計画戦略を策定する。	OG-WRL-003	751	A（承認）	C（助言）	C（助言）	C（助言）		I（報告）
Cybersecurity Curriculum Development	Responsible for developing, planning, coordinating, and evaluating cybersecurity awareness, training, or education content, methods, and techniques based on instructional needs and requirements.	教育ニーズと要件に基づき、サイバーセキュリティ意識向上・研修・教育コンテンツ、手法、技術の開発・計画・調整・評価を担当する。	OG-WRL-004	711	A（承認）	C（助言）	C（助言）	C（助言）		I（報告）
Cybersecurity Instruction	Responsible for developing and conducting cybersecurity awareness, training, or education.	サイバーセキュリティ意識向上・研修・教育の開発および実施を担当する。	OG-WRL-005	712	A（承認）	C（助言）	C（助言）	C（助言）		I（報告）
Cybersecurity Legal Advice	Responsible for providing cybersecurity legal advice and recommendations, including monitoring related legislation and regulations.	関連法令・規制の監視を含む、サイバーセキュリティに関する法的助言と提言の提供を担当する。	OG-WRL-006	731	A（承認）	R（統括）				I（報告）
Executive Cybersecurity Leadership	Responsible for establishing vision and direction for an organization's cybersecurity operations and resources and their impact on digital and physical spaces. Possesses authority to make and execute decisions that impact an organization broadly, including policy approval and stakeholder engagement.	組織のサイバーセキュリティ運用・リソースのビジョンと方向性、ならびにデジタル空間・物理空間への影響を確立する責任を負う。政策承認やステークホルダー関与を含む、組織全体に影響する意思決定の権限を有し、これを実行する。	OG-WRL-007	901	A（承認） R（統括）	E（実行）				
Privacy Compliance	Responsible for developing and overseeing an organization's privacy compliance program and staff, including establishing and managing privacy-related governance, policy, and incident response needs.	組織のプライバシーコンプライアンスプログラム及び担当スタッフの策定・監督を担当。これにはプライバシー関連のガバナンス、政策、インシデント対応ニーズの確立・管理が含まれる。	OG-WRL-008	732	A（承認）	R（統括）		C（助言）		I（報告）
Product Support Management	Responsible for planning, estimating costs, budgeting, developing, implementing, and managing product support strategies in order to field and maintain the readiness and operational capability of systems and components.	システムおよびコンポーネントの運用準備態勢と運用能力を確保・維持するため、製品サポート戦略の計画立案、コスト見積もり、予算策定、開発、実施、管理を担当する。	OG-WRL-009	803				C（助言）		
Program Management	Responsible for leading, coordinating, and the overall success of a defined program. Includes communicating about the program and ensuring alignment with agency or organizational priorities.	定義されたプログラムの主導、調整、および全体的な成功を担当する。プログラムに関するコミュニケーションや、機関または組織の優先事項との整合性の確保を含む。	OG-WRL-010	801				C（助言）		E（実行）
Secure Project Management	Responsible for overseeing and directly managing technology projects. Ensures cybersecurity is built into projects to protect the organization's critical infrastructure and assets, reduce risk, and meet organizational goals. Tracks and communicates project status and demonstrates project value to the organization.	技術プロジェクトの監督および直接管理を担当する。組織の重要インフラと資産を保護し、リスクを低減し、組織目標を達成するため、サイバーセキュリティがプロジェクトに組み込まれることを保証する。プロジェクトの進捗状況を追跡・伝達し、組織に対するプロジェクトの価値を実証する。	OG-WRL-011	802	A（承認）	C（助言）	C（助言）			

人材定義リファレンス2026		NICE Components
構成要素	**内容**	
組織体制	企業全体のサイバーセキュリティ体制	Organization
機能領域	企業として備えるべき大分類	Capability Area（独自）
機能	各機能領域を構成する個別の機能	Function（独自）
役割	各機能を実現するために責任を担う主体（人、組織、委託先、サービス、AI等）	Role（独自）
業務	各役割が実施する具体的な活動	Task（概念的に対応）
Work Role	NICE Framework Componentsで定義される専門的な職務との対応関係	Work Role
REACI	各役割における責任分担（Responsible、Execute、Accountable、Consulted、Informed）	責任分担（独自）

図4-4　人材定義リファレンス2026の構成（NICEフレームワークとREACI）

4.5　人材定義リファレンス2026におけるREACIを活用した役割分担

- **本リファレンスでは、各役割の責任範囲及び相互の連携関係を明確にするため、REACI（Responsible、Execute、Accountable、Consulted、Informed）を用いて役割分担を整理しています。**
- サイバーセキュリティは、一つの組織だけで実現できるものではなく、経営層、セキュリティ統括、情報システム部門、事業部門、DX推進部門、OT管理部門など、多様な組織がそれぞれの役割を担いながら推進します。そのため、「誰が統括するのか」「誰が実行するのか」「誰が最終責任を負うのか」「誰が助言するのか」「誰へ報告するのか」を明確にすることが重要です。
- 本リファレンスでは、機能及び役割ごとにREACIを用いて責任分担を整理し、ユーザ企業における組織設計、役割分担、規程整備、監査対応及びインシデント対応などに活用できるよう整理しています。
- 本リファレンスで用いるREACIの定義を表4-5に示します。

記号	名称	定義
R	**Responsible（統括責任）**	当該活動を主管し、計画、調整及び実施状況を管理する**役割**（複数配置可）
E	**Execute（実行）**	当該活動を実務として遂行する**役割**（複数配置可）
A	**Accountable（最終責任・承認）**	当該活動に関する最終的な説明責任及び承認権限を有する**役割**（原則1名）
C	**Consulted（助言・協議）**	専門的知見に基づき、助言、協議又は支援を行う**役割**（複数配置可）
I	**Informed（報告）**	活動状況、結果又は意思決定について報告を受ける**役割**（複数配置可）

表4-5　REACIを活用した役割分担

本リファレンスでは、責任分担の整理にあたり、一般的なRACIモデルを拡張したREACIを採用しています。

従来のRACIでは、Responsibleが責任と実行の双方を担うことが一般的でしたが、近年は外部委託、クラウドサービス、マネージドサービス及びAI等の活用により、責任を負う主体と実際に実行する主体が異なることが増えています。このため、本リファレンスでは「Execute（実行）」を追加し、実行主体を明確に区分できるREACIを採用しています。

4.6　人材定義リファレンス2026の適用対象

- **本リファレンスは、ユーザ企業におけるサイバーセキュリティ体制の構築・運営に携わる組織及び担当者が、必要な機能、役割及び業務を整理するための実務リファレンスです。**
- 本リファレンスは、特に次のような場面での活用を想定しています。

活用場面	活用例
組織体制の整備	セキュリティ統括室等の設置、各部門との役割分担、組織体制の見直し
役割・責任の明確化	各機能及び役割の責任範囲を整理し、REACIによる責任分担を明確化
人材育成・教育	必要な役割に応じた育成計画、教育計画及びキャリアパスの検討
人材配置・要員計画	必要な役割を整理し、兼務や外部委託を含めた人員配置を検討
規程・ルールの整備	情報セキュリティ規程、インシデント対応規程等における役割分担の整理
監査・アセスメント	組織体制、機能及び役割を評価し、不足する機能や責任範囲を把握
NICE Frameworkとの比較	Work Roleとの対応関係を確認し、国際的な人材フレームワークとの比較・参照
経営層への説明	サイバーセキュリティ体制、人材配置及び責任分担について経営層へ説明・共有
活用例グループ会社・委託先への展開	グループ会社や委託先にも本リファレンスを適用し、役割及び責任の考え方を統一することで、組織全体として一貫したサイバーセキュリティ体制を構築する。

表4-6　人材定義リファレンス2026の適用対象

4.7　人材定義リファレンス2026の全体像（まとめ）

- 本章では、ユーザ企業に必要な機能、役割、業務、REACIによる責任分担及びNICE Framework Componentsとの対応関係について説明しました。これらの関係を整理すると、本リファレンス全体は次のような構造で構成されています。

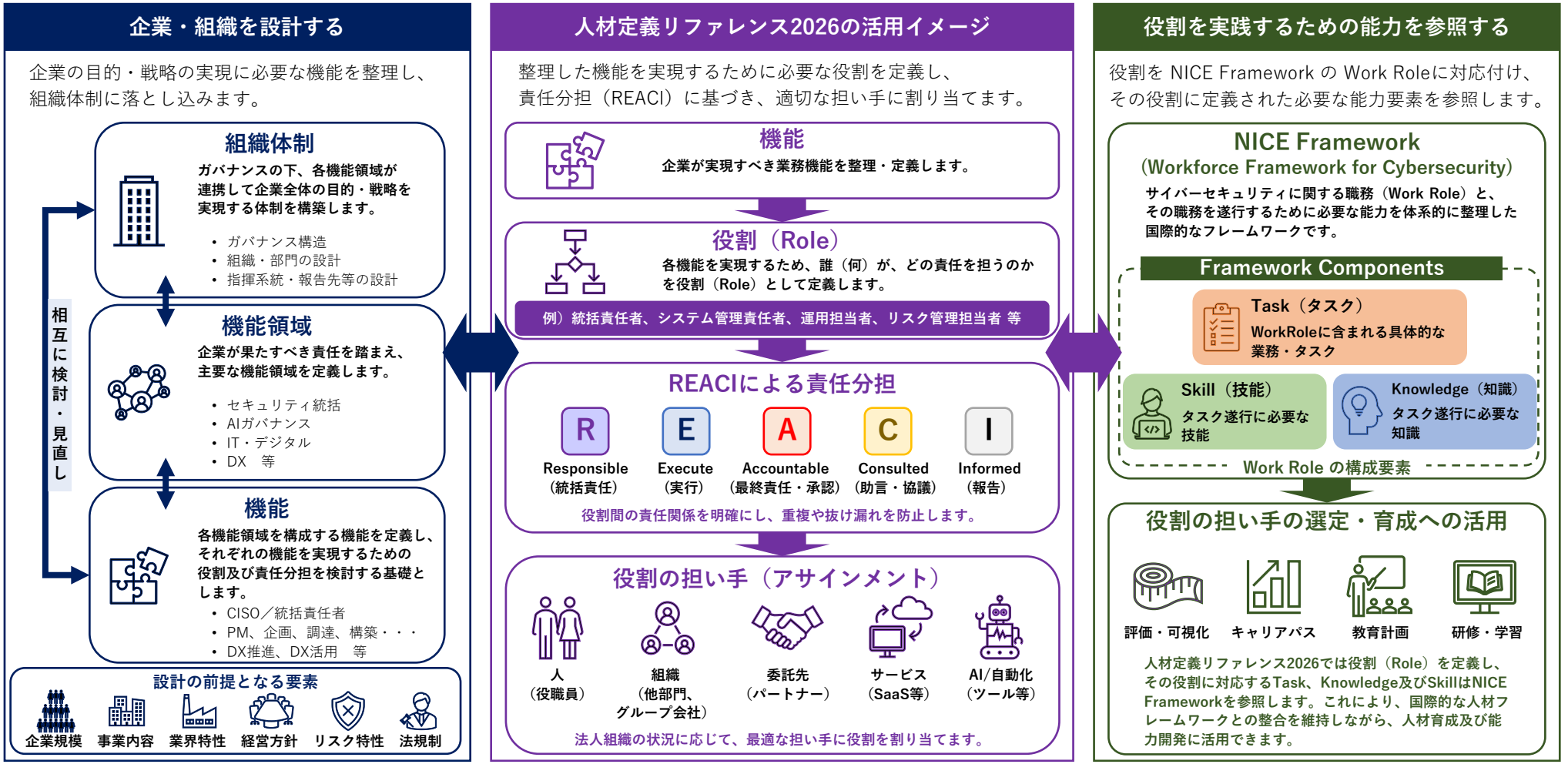


図1　人材定義リファレンス2026が表現する世界

５．人材定義リファレンス2026の活用方法

5.1　人材定義リファレンス2026の活用にあたって

- 本リファレンスは、ユーザ企業におけるサイバーセキュリティに関する役割と責任を整理するための共通的な考え方を示すものです。その活用方法は一つではなく、企業の規模、事業内容、経営方針、リスク特性及び組織体制に応じて柔軟に適用することを想定しています。
- **本章では、本リファレンスを活用する際の代表的な考え方を示します。**これらは活用方法を限定するものではなく、自社の状況に応じて組織体制や人材戦略を検討する際の参考となることを目的としています。
- **本リファレンスを活用する際には、ユーザ企業として必要な機能を整理し、その機能を担う役割と責任を明確にした上で、必要な能力を検討することが重要です。**さらに、その結果を組織設計、人材配置、人材育成、評価及び採用へ展開することで、一貫した人材マネジメントにつなげることができます。
- 以降では、組織設計、人材定義、能力開発など、ユーザ企業における代表的な活用方法について説明します。

この章で考えること	この章で整理すること	この章で活用できること
ユーザ企業として備えるべき機能や、その機能を実現するための役割及び責任をどのように定義するかを考えます。また、その役割を担うために必要な能力や担い手について、多様な観点から検討します。	組織体制、機能、役割、責任及び能力を一貫した考え方で整理します。さらに、それらの関係性を可視化することで、自社の組織や人材マネジメントへの適用を検討します。	組織設計、人材配置、人材育成、評価、採用、外部委託など、ユーザ企業における様々な場面で人材定義リファレンス2026を活用するための考え方を理解できます。

表5-1　人材定義リファレンス活用のポイント

5.2　人材定義リファレンス2026（Excel）の見方と活用方法

- **本リファレンスは、ユーザ企業に必要となる役割、責任及び能力を一覧化したリファレンスです。**
- Excelシートでは、ユーザ企業に必要な役割を列方向に配置するとともに、各役割の責任及びNICE FrameworkのWork Roleとの対応関係を整理しています。

図5-2　人材定義リファレンス2026（Excel）の見方

5.3　組織設計から人材育成までの活用フロー

- 本章では、図1を活用し、**左から順に「企業・組織設計」、「役割の整理」及び「役割に必要な能力」の考え方を説明します。**
- 以降では、それぞれの要素を順に取り上げ、組織設計から人材育成への展開方法を解説します。

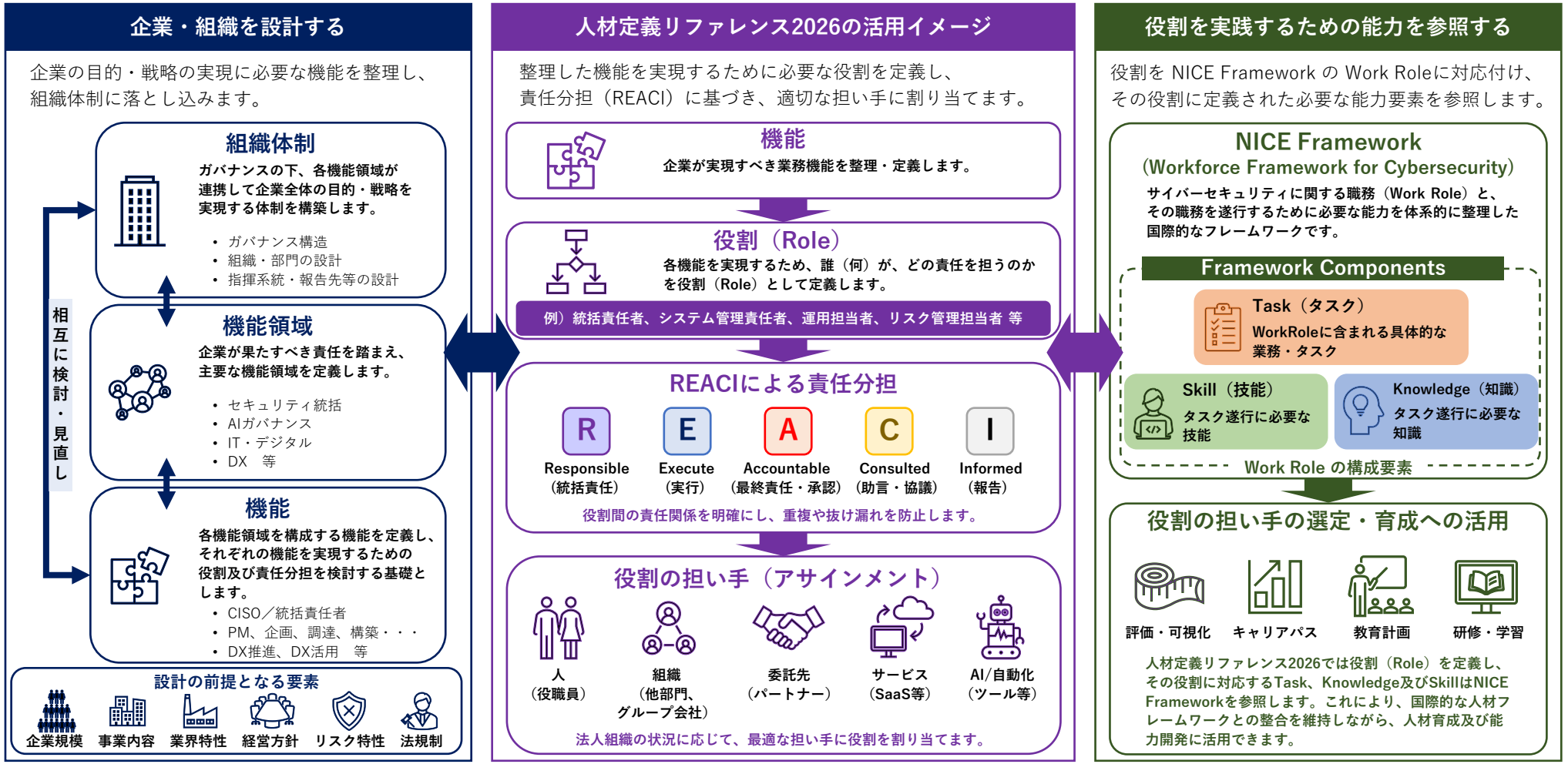


図1　人材定義リファレンス2026が表現する世界

5.4　企業・組織設計の考え方

- **企業・組織の設計では、経営戦略や事業特性に応じて必要な機能を配置し、役割と責任を明確にすることが重要です。**
- 組織体制、機能領域及び機能を体系的に整理し、役割及び責任の明確化並びに組織体制の見直しに活用できます。

企業・組織を設計する

企業の目的・戦略の実現に必要な機能を整理し、組織体制に落とし込みます。

組織体制

ガバナンスの下、各機能領域が連携して企業全体の目的・戦略を実現する体制を構築します。

- ガバナンス構造
- 組織・部門の設計
- 指揮系統・報告先等の設計

機能領域

企業が果たすべき責任を踏まえ、主要な機能領域を定義します。

- セキュリティ統括
- AIガバナンス
- IT・デジタル
- DX　等

機能

各機能領域を構成する機能を定義し、それぞれの機能を実現するための役割及び責任分担を検討する基礎とします。

- CISO／統括責任者
- PM、企画、調達、構築・・・
- DX推進、DX活用　等

相互に検討・見直し

設計の前提となる要素

企業規模　事業内容　業界特性　経営方針　リスク特性　法規制

設計のポイント

人材定義リファレンス2026では、組織名称や既存の部門構成から考えるのではなく、「企業として実現すべき機能」を起点として組織を設計することを基本的な考え方としています。

企業・組織を設計する際の着眼点

■ 組織体制

- 企業の目的及び経営戦略を実現するために必要な組織体制となっているか。
- ガバナンス及び指揮命令系統が明確であり、意思決定が適切に行える体制となっているか。
- 各機能が相互に連携し、継続的な改善及び見直しが行える体制となっているか。

■ 機能領域

- 自社に必要な機能領域を漏れなく整理できているか。
- 企業規模、事業内容及びリスク特性に応じた機能領域となっているか。
- 新たな事業や技術の変化に対応できる拡張性を備えているか。。

■ 機能

- 各機能の目的及び責任範囲が明確に定義されているか。
- 機能の不足、重複又は責任の空白が生じていないか。
- 組織名称ではなく、「実現すべき機能」を基準として整理されているか。

■ 設計の前提

- 企業規模、業種、法令・規制及び経営方針を踏まえているか。
- 将来の組織変更や事業拡大にも対応できる構成となっているか。
- 一つの組織又は担当者が複数の機能を担う場合でも、責任の所在が明確となっているか。

図5-4　企業・組織設計の考え方

5.5　人材定義リファレンス2026の役割の検討

- **役割（Role）は、ユーザ企業に必要な機能を担う主体と責任を明確にするための考え方です。**
- 役職や組織名称ではなく、「誰が、何に責任を持つのか」という観点から役割を整理します。

設計のポイント

本リファレンスでは、役職や所属組織から役割を考えるのではなく、「実現すべき機能」を起点として役割（Role）を定義し、REACIにより責任を明確化した上で、最適な担い手へ割り当てることを基本的な考え方としています。

役割を検討する際の着眼点

■ **役割（Role）**

- 各機能を実現するために必要な役割が整理されているか。
- 一つの役割に求める責任範囲が適切に定義されているか。
- 役職名ではなく、実際に担う責任を基準として定義されているか。
- 複数の役割を一人又は一つの組織が兼務する場合でも責任が明確か。

■ **REACI**

- Responsible、Execute、Accountable、Consulted、Informedが整理されているか。
- 責任の重複又は空白が生じていないか。
- 最終責任者（Accountable）が明確か。
- 関係部門との連携及び報告経路が整理されているか。

人材定義リファレンス2026の活用イメージ

整理した機能を実現するために必要な役割を定義し、
責任分担（REACI）に基づき、適切な担い手に割り当てます。

機能

企業が実現すべき業務機能を整理・定義します。

役割（Role）

各機能を実現するため、誰（何）が、どの責任を担うのかを役割（Role）として定義します。

例）統括責任者、システム管理責任者、運用担当者、リスク管理担当者 等

REACIによる責任分担

R	E	A	C	I
Responsible（統括責任）	Execute（実行）	Accountable（最終責任・承認）	Consulted（助言・協議）	Informed（報告）

役割間の責任関係を明確にし、重複や抜け漏れを防止します。

役割の担い手（アサインメント）

人（役職員）／組織（他部門、グループ会社）／委託先（パートナー）／サービス（SaaS等）／AI/自動化（ツール等）

法人組織の状況に応じて、最適な担い手に役割を割り当てます。

役割を検討する際の着眼点（つづき）

■ **役割の担い手**

- 社員だけでなく委託先やグループ会社も含めて検討しているか。
- SaaS等のサービスが担う役割を考慮しているか。
- AIや自動化によって代替可能な役割を整理しているか。
- 将来の体制変更にも対応できる役割設計となっているか。

■ **検討の前提**

- 組織変更があっても役割が維持できる設計となっているか。
- 役割ごとに必要な責任が一貫して整理されているか。
- 将来的なNICE Frameworkとの対応付けを考慮しているか。

役割は「人」を定義するものではなく、「責任」を定義するものです。

組織変更や人事異動があっても、役割を維持することで責任を継続的に管理できるようになります。

図5-5　人材定義リファレンス2026の役割の検討

5.6　役割を担うために必要な能力の整理

- **役割を定義した後は、その役割を担うために必要な能力要件を整理します。**NICE Framework Componentsを参照し、Task、Knowledge及びSkillを基に能力要件を整理して、人材育成や委託先の評価、サービスやツールとの役割分担へ展開します。

設計のポイント

本リファレンスでは、役割（Role）を定義した後、その役割を遂行するために必要な能力をNICE Framework Componentsと対応付けることを基本的な考え方としています。

能力を整理する際の着眼点

■ **Role**
- 役割を遂行するために必要な業務が明確になっているか。
- 役割の範囲と責任範囲が一致しているか。

■ **Task**
- 役割に必要な具体的な業務が整理されているか。
- 業務内容に漏れや重複はないか。

■ **Knowledge**
- 業務を遂行するために必要な知識が整理されているか。
- 法令、規格及び社内ルールを考慮しているか。

■ **Skill**
- 必要な技術及び実務能力が整理されているか。
- 教育・訓練によって習得可能な能力が明確か。

■ **活用**
- 教育計画へ反映できるか。
- 人材育成及び能力開発へ活用できるか。
- キャリアパス及び評価制度へ展開できるか。
- 採用要件の整理へ活用できるか。

人材定義リファレンス2026は「役割」を定義するものであり、能力そのものを定義するものではありません。

能力要件の整理には、NICE Framework Componentsを参照することで、役割と能力を一貫して設計できます。

役割を実践するための能力を参照する

役割を NICE Framework の Work Roleに対応付け、その役割に定義された必要な能力要素を参照します。

NICE Framework
(Workforce Framework for Cybersecurity)

サイバーセキュリティに関する職務（Work Role）と、その職務を遂行するために必要な能力を体系的に整理した国際的なフレームワークです。

Framework Components

Task（タスク）
WorkRoleに含まれる具体的な業務・タスク

Skill（技能）
タスク遂行に必要な技能

Knowledge（知識）
タスク遂行に必要な知識

Work Role の構成要素

役割の担い手の選定・育成への活用

評価・可視化　**キャリアパス**　**教育計画**　**研修・学習**

人材定義リファレンス2026では役割（Role）を定義し、その役割に対応するTask、Knowledge及びSkillはNICE Frameworkを参照します。これにより、国際的な人材フレームワークとの整合を維持しながら、人材育成及び能力開発に活用できます。

図5-6　役割を担うために必要な能力の整理

5.7　NICE Framework Componentsの概要とTKSの活用

- **役割に必要な能力要件を具体的に整理するため、本リファレンスではNICE Framework Componentsを参照しています。**
- NICE Framework Componentsでは、Work RoleごとにTask、Knowledge及びSkill（TKS）が整理されており、役割に必要な能力要件を客観的に整理・検討できます。

項目	内容	参照先
正式名称	Workforce Framework for Cybersecurity（NICE Framework）。 サイバーセキュリティに関する仕事と、それを遂行するために必要な知識・技能を記述するための人材フレームワーク。	**NIST SP 800-181 Rev.1**
策定主体	米国国立標準技術研究所（NIST）が運営するNational Initiative for Cybersecurity Education（NICE）が策定・維持している。	**NICE公式ページ**
基本文書	NIST SP 800-181 Rev.1。2020年11月公表。NICE Frameworkの目的、構造、基本概念及び活用方法を定める。	**NIST SP 800-181 Rev.1 PDF**
目的	サイバーセキュリティに関する仕事を共通の用語と構造で記述し、人材の特定、採用、育成、配置及び定着に関する関係者間のコミュニケーションを改善すること。	**Getting Started with the NICE Framework**
適用対象	公共部門・民間部門、業種、国・地域を問わず利用できる。利用者として、雇用主、学生、求職者、従業員、教育機関、研修・資格提供者等が想定されている。	**NICE Framework About**
基本構成要素	Task、Knowledge、Skill（TKS）。 Taskは実施する仕事、KnowledgeとSkillは、その仕事を遂行するために知っていること、及び実行できることを表す。	**Getting Started with the NICE Framework**
Task	組織の目的の達成に向けて行われる活動。サイバーセキュリティ業務として「何を行うか」を記述する。	**NICE Framework Components Poster**
Knowledge	Taskを遂行するために理解しておく必要がある概念、原則、事実、情報等を記述する。	**NIST SP 800-181 Rev.1 PDF**
Skill	Taskを遂行するために、学習及び実践を通じて身に付ける能力を記述する。	**NIST SP 800-181 Rev.1 PDF**
Work Role	一人又は複数の者が責任又は説明責任を負う仕事のまとまり。TKSステートメントを組み合わせて定義される。職名や役職名そのものではない。	**Occupations, Jobs, and Work Roles**
Work Role Category	関連するWork Roleをまとめる上位分類。サイバーセキュリティ業務の領域を大きく整理するために用いられる。	**NICE Framework Current Versions**
Competency Area	特定領域のTaskを遂行する能力と関連するKnowledge及びSkillのまとまり。Work Roleと組み合わせて、又は単独で能力開発に利用できる。	**Getting Started with the NICE Framework**
主な活用場面	職務記述、人員計画、採用要件、教育・研修、能力開発、キャリア形成、資格・教材との対応付け、チーム編成等。	**NICE Framework Resource Center**
提供形態	機械可読形式（JSON）でも提供されており、HRシステム、スキル管理システム、教育ツールなどとの連携にも利用できる。	**NICE Framework Current Versions**
性格	認証基準や組織体制を一律に定める規格ではなく、各組織や業界が目的に応じた職務、人材育成及び人材管理の仕組みを構築するための参照基盤である。	**NIST SP 800-181 Rev.1**

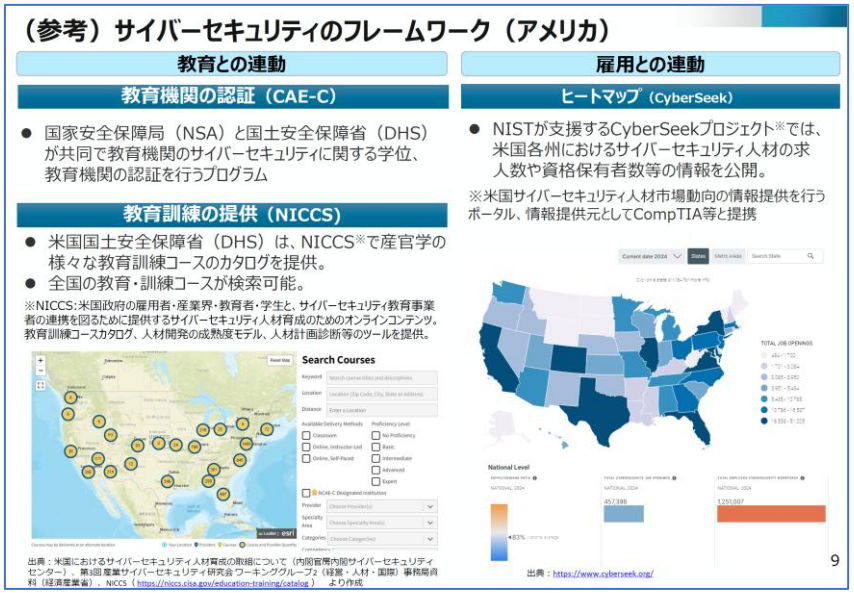
図5-7　NICEフレームワークについて

5.8　米国におけるNICE Frameworkの活用事例

- **NICE Frameworkは、米国政府機関だけでなく、民間企業、教育機関及び資格認証機関など幅広い分野で活用されています。**
- ここでは、人材マネジメントにおける代表的な活用例を紹介します。

活用分野	活用内容	主な利用主体
採用・募集	職務記述書（Job Description）、求人要件の作成	民間企業、政府機関
人材配置	Work Roleに基づく役割設計、適材適所の配置	民間企業、政府機関
教育・研修	TKSに基づく教育カリキュラム・研修設計	教育機関、企業
能力評価	スキル評価、ギャップ分析、能力の可視化	民間企業、政府機関
キャリア形成	キャリアパス設計、リスキリング、能力開発計画	民間企業、教育機関
資格・認証	資格・認証制度との対応付け	教育機関、資格認証団体
教育機関認証（CAE-C）	NICE準拠カリキュラムによる教育機関認証	NSA、DHS、大学等
人材情報共有（CyberSeek）	Work Roleに基づく人材需給・求人情報の提供	NIST、CompTIA、Lightcast

図5-8　米国におけるNICE Frameworkの活用事例



出典）経済産業省 情報技術利用促進課
「**海外のスキル情報収集と活用の事例**」2024年11月26日
https://www.meti.go.jp/shingikai/mono_info_service/society_digital/pdf/002_02_00.pdf

本リファレンスも、こうした考え方を参考に、日本企業に適した人材マネジメントへの活用を目指しています。

米国では、NICE Frameworkは教育・研修のためのフレームワークにとどまらず、組織に必要な人材の計画、採用、人材配置、育成、評価及びキャリア形成までを一貫して支える人材マネジメントの共通基盤として活用されています。政府機関、民間企業、教育機関及び資格認証機関が共通の人材言語として活用することで、人材の可視化、能力開発及び組織横断的な人材活用を実現しています。

5.9 Official NIST Resources for the NICE Framework

- **NICE Frameworkは、サイバーセキュリティの仕事を共通の用語と構造で記述するためのフレームワークです。**
- NISTは、Framework本体に加え、Framework Components、各種ガイド及びオンラインリソースを公開し、教育、人材育成、採用及びワークフォース開発を支援しています。

No.	資料名	内容	主な用途	URL
1	**NIST SP 800-181 Rev.1 – Workforce Framework for Cybersecurity (NICE Framework)**	NICE Frameworkの基本文書。Frameworkの目的、基本概念及び構造を定義する。	**Frameworkの理解**	https://csrc.nist.gov/pubs/sp/800/181/r1/final
2	**Getting Started with the NICE Framework**	NICE Frameworkの概要、基本概念、利用方法及びFramework Componentsを解説する導入ガイド。	**Frameworkの理解**	https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/getting-started
3	**NICE Framework Components – Current Versions**	最新のWork Role Category、Work Role、Competency Area、Task、Knowledge及びSkillをExcel・JSON形式で提供。	**Componentsの参照**	https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions
4	**NICE Framework Components Guide**	各Framework Componentsの定義、相互関係及び利用方法を解説。	**Componentsの理解**	https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/resources/nice-framework-components-guide
5	**Occupations, Jobs, and Work Roles**	Occupation、Job、Position及びWork Roleの違いを説明。Work Roleの位置付けを理解するための参考資料。	**Work Roleの理解**	https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/resources/occupations-jobs-and-work-roles
6	**NIST IR 8355 – NICE Framework Competency Areas**	Competency Areaの考え方、定義及び活用方法を解説。	**Competency Areaの理解**	https://csrc.nist.gov/pubs/ir/8355/final
7	**NICE Framework Resource Center**	NICE Frameworkに関する公式ポータル。関連資料、活用事例、教育資料等を提供。	**総合情報**	https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
8	**Education & Training**	教育・研修、カリキュラム設計及びロールベース教育への活用例。	**教育・育成**	https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/resources/education-and-training
9	**Career Discovery**	Work Roleを活用したキャリア探索及びキャリア形成の支援。	**キャリア形成**	https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/resources/career-discovery
10	**NICE Framework Tools**	NICE Frameworkを利用したマッピング、ワークフォース分析及び実務活用を支援するツール及びテンプレート	**実務活用**	https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/resources/nice-framework-tools

６．人材定義リファレンス2016と2026 ― 継承と発展

6.1　基本理念の継承

- **2026年版は、2016年に公表した「サイバーセキュリティ人材定義リファレンス」の基本理念を継承しながら、企業を取り巻く環境や技術の変化に対応して発展させたものです。**
- 2016年版では、ユーザ企業に必要なサイバーセキュリティ人材の役割、機能及び業務を整理するとともに、サイバーセキュリティを情報システム部門だけの課題ではなく、企業全体で取り組むべき経営課題として位置付けました。また、「セキュリティ統括室等」の考え方を示し、組織横断的な推進体制の構築を支援してきました。
- 2026年版では、これらの基本理念を継承しながら、クラウドサービス、生成AI、OT・IoT及びサプライチェーンなどの新たな環境変化に対応した内容へ発展させています。
- 表6-1に、2016年版から継承している主な基本理念を示します。

2016年版から継承している基本理念	内容
組織体制を起点とした人材定義	個々の人材や職種ではなく、企業として必要な組織体制を起点として役割を整理します。
役割（Role）を重視	組織名称や役職ではなく、組織に求められる役割と責任を定義します。
人材配置モデルではない	一人一役を前提とするものではなく、企業規模や事業特性に応じて兼務や組織統合を想定しています。
柔軟な適用	特定の組織構成や組織名称を求めるものではなく、企業の実情に応じて柔軟に適用することを前提としています。
外部サービスの活用	SOC、CSIRT運営、脆弱性診断、デジタルフォレンジックなど、高度な専門機能は外部サービスの活用も想定しています。
セキュリティ統括室等を中核とした体制	組織横断的なガバナンス機能を担う「セキュリティ統括室等」を中核として位置付けています。
ユーザ企業を対象	ベンダ企業ではなく、ユーザ企業における組織体制、役割及び責任を整理することを目的としています。

表6-1　2016年版から継承している基本理念

6.2　2026年版で発展させた内容

- **2026年版では、2016年版の基本理念を継承しながら、企業を取り巻く環境や技術の変化に対応するため、人材定義リファレンスの内容を拡充しました。**
- 2016年版の公表以降、クラウドサービスの普及、ゼロトラストアーキテクチャへの移行、生成AIの活用、OT・IoT環境の拡大、サプライチェーンリスクへの対応など、企業に求められるサイバーセキュリティの対象領域は大きく変化しました。また、NICE Framework Componentsの整備により、国際的な人材フレームワークとの対応も重要となっています。
- こうした変化を踏まえ、2026年版では、日本企業の組織体制を前提としながら、組織体制、機能領域、機能、役割及び業務を見直すとともに、AIガバナンスなどの新たな領域を追加し、実務への適用性と国際的な整合性を高めました。
- 表6-2に、2026年版で拡充・発展した主な内容を示します。

2026年版で拡充・発展した内容	内容
人材定義の体系化	組織体制、機能領域、機能、役割及び業務の関係を体系的に整理
組織体制モデル	日本企業を前提とした標準的な組織体制モデルを追加
AIガバナンスへの対応	AIリスクマネジメント及びAI推進に関する機能を追加
ゼロトラストへの対応	ゼロトラストアーキテクチャを前提とした機能、役割及び業務を整理
OT・IoTへの対応	OTを独立した機能領域として整理し、サイバー・フィジカル・システムへの対応を拡充
サプライチェーンへの対応	グループ会社、海外拠点及び委託先を含めた組織体制及び役割を整理
NICE Frameworkとの対応	Work Roleとのマッピングを追加し、国際的な人材フレームワークとの対応関係を整理
REACIの導入	各役割の責任分担及び連携関係を明確化

表6-2　2026年版で拡充・発展した内容

6.3　人材定義リファレンス2016と2026の対応関係

- 2016年版では、**ユーザ企業に必要なサイバーセキュリティ人材の役割、機能及び業務を整理していました。**
- 2026年版では、その考え方を継承しつつ、**ユーザ企業に求められる組織体制を起点として、機能領域、機能、役割及び業務へと再構成するとともに、AIガバナンスやDX、OTなどの新たな領域を追加しています。**
- 図6-1は、2016年版と2026年版の対応関係を示したものです。

情報システム部門におけるサイバーセキュリティ機能を担う役割（担当）例																									情報システム部門以外のセキュリティ担当職					
管理職						セキュリティ担当職							担当職													監査・個人情報保護					
①CISO CRO CIO等	②サイバーセキュリティ統括（室等）	③システム部門責任者	④システム管理者	⑤ネットワーク管理者	⑥CSIRT責任者	⑦サイバーセキュリティ事件・事故担当	⑧セキュリティ設計担当	⑨構築系サイバーセキュリティ担当	⑩運用系サイバーセキュリティ担当	⑪CSIRT担当	⑫SOC担当	⑬ISMS担当	⑭システム企画担当	⑮基幹システム構築担当	⑯基幹システム運用担当	⑰WEBサービス担当	⑱業務アプリケーション担当	⑲インフラ担当	⑳サーバ担当	㉑DB担当	㉒ネットワーク担当	㉓サポート教育担当	㉔ヘルプデスク担当	㉕監査責任者	㉖監査担当	㉗特定個人情報取扱責任者	㉘特定個人情報取扱担当	㉙個人情報取扱責任者	㉚個人情報取扱担当

マッピング

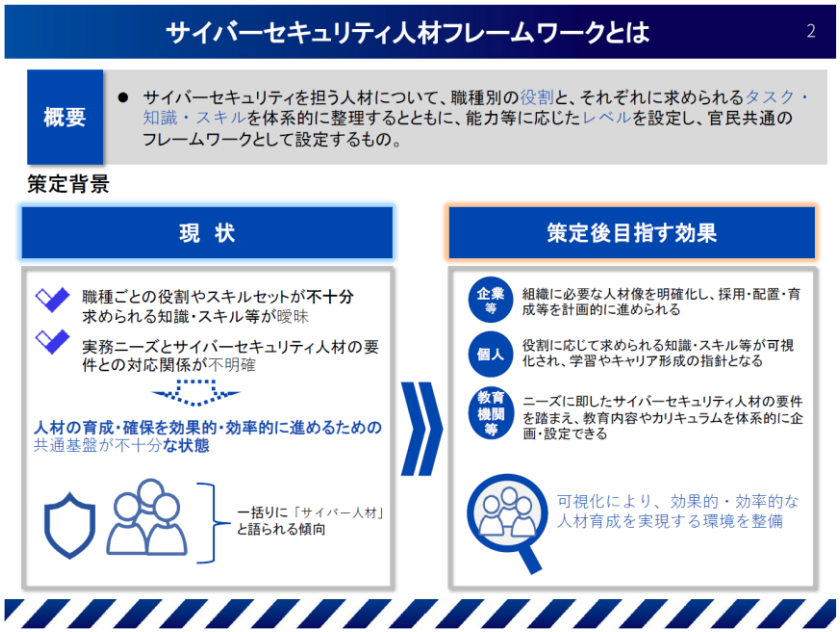
	セキュリティ統括					リスク管理	AIガバナンス		IT・デジタル											DX		事業運営		OT
	CISO 統括責任者	ガバナンス	テクノロジー	セキュリティオペレーション	マネジメント	リスク法務	AIリスクマネジメント	AI推進	CIO	情報システム部門責任者	システム管理責任者	PM	企画	調達	構築	運用保守	サポート	DX推進	DX活用	国内	海外	OT 環境管理
人材定義リファレンス2026（案）	組織全体のサイバーセキュリティに関する最終責任者として、方針・戦略・リスク受容を決定し、経営層・外部関係者への説明責任を負う。	法令・規制・方針への準拠を確保するため、ポリシー策定、リスク管理、監査・評価を通じて、組織のセキュリティ統治を担う。	IT・クラウド・OT等の技術領域において、技術動向の調査およびセキュリティ水準の検討を行い、要件定義・設計・実装に関する助言を通じて、安全なシステム構築と技術的支援を担う。	SOC／CSIRT等を通じて、監視・検知・インシデント対応を実施し、日常運用および有事対応により組織の安全性を維持する。	人材育成、体制整備、委員会運営、予算・委託管理を通じて、セキュリティ活動が継続的かつ実効的に機能するよう支援する。	サイバーセキュリティに関する法令遵守、契約、訴訟・当局対応の観点から助言を行い、インシデント時の法的リスク評価と対応方針策定を支援する。	AIの利用・開発・提供に伴うリスクを専門的に管理し、法令・倫理・セキュリティ・品質・説明責任の観点から必要な統制を整備する。AI利用方針、リスク評価、ガバナンス基準、監査対応等を通じて、安全かつ適正なAI活用を推進する。	組織横断でAI活用を推進し、生成AI・機械学習等を活用した業務改革や価値創出を支援する。ユースケース企画、導入支援、利用ルール整備、人材育成を通じて、全社的なAI活用の高度化を担う。	組織全体のITガバナンスとデジタル戦略を統括し、システム投資・運用の最適化とIT統制を担う。リスク管理と内部統制の観点から、情報システムの適正運用と継続的改善を推進する。	組織の情報システム全体を統括し、ITガバナンスに基づき企画・構築・運用を管理する。資源配分と統制の確立を通じて、ITサービスの安定提供と継続的改善を推進する。	担当システムの運用・管理に責任を持ち、方針に基づく設定管理、運用監視、障害・インシデント対応を統括し、安定稼働とセキュリティ確保を実現する。	プロジェクト全体の進行・品質・コスト・リスクを管理し、セキュリティ要件を含めた計画立案と関係者調整を担う。	事業・業務要件を踏まえ、システムや施策の目的、範囲、セキュリティ要件を整理し、実現方針や計画を策定する。	事業・システムに必要な製品、サービス及び開発・運用委託先を選定し、契約条件及びサイバーセキュリティ要件を明確化したうえで調達及び委託管理を行う。また、サプライチェーンリスクを考慮し、委託先の選定、評価、監督及び継続的な管理を実施する。	設計に基づきシステムや環境を実装・設定し、セキュリティ対策を組み込んだ形で構築・テストを実施する。	稼働中のシステムを安定的に運用し、監視、更新、脆弱性対応、障害対応を通じて可用性と安全性を維持する。	利用者からの問い合わせやトラブルに対応し、適切な案内・復旧支援を行うことで、業務継続と利便性を支援する。	全社的なデジタル変革を推進し、事業・業務改革に向けた戦略立案、施策推進、データ活用およびデジタル技術の活用を通じて、継続的な業務改善と競争力向上を実現する。	各事業・業務領域においてデジタル技術やDX施策を活用し、業務効率化、高度化、データ活用を実践する。現場運用を通じて課題や改善要望を把握し、関係部門と連携して継続的な改善を推進する。	国内事業においてシステムや業務を運用し、定められたセキュリティ方針に従って対策を実装・運用するとともに、必要な情報を統括部門へ報告する。	海外拠点の事業運営において、現地法規制を踏まえつつ本社方針に沿ったセキュリティ対策を実施し、インシデントや状況を本社へ共有する。	工場、生産設備、プラント、ビル設備、エネルギー設備、交通設備等のOT・IoT環境を管理し、安全性および可用性を最優先として物理環境の安定的な運用を確保するとともに、サイバーセキュリティ対策を実施し、インシデントや運用状況を関係部門へ報告する。
人材定義リファレンス2016	①CISO/CRO	②サイバーセキュリティ統括（室等）	②サイバーセキュリティ統括（室等）	②サイバーセキュリティ統括（室等）	②サイバーセキュリティ統括（室等）	㉗特定個人情報取扱責任者			①CIO等	③システム部門責任者	④システム管理者	④システム管理者	⑭システム企画担当	⑭システム企画担当	⑮基幹システム構築担当	⑯基幹システム運用担当	㉓サポート教育担当		⑭システム企画担当	⑭システム企画担当	⑭システム企画担当	⑭システム企画担当
			⑧セキュリティ設計担当	⑥CSIRT責任者	⑬ISMS担当	㉘特定個人情報取扱担当					⑤ネットワーク管理者	⑭システム企画担当	⑧セキュリティ設計担当	⑰WEBサービス担当	⑱業務アプリケーション担当	⑱業務アプリケーション担当	㉔ヘルプデスク担当		⑰WEBサービス担当	⑰WEBサービス担当	⑰WEBサービス担当	⑰WEBサービス担当
			⑨構築系サイバーセキュリティ担当	⑦サイバーセキュリティ事件・事故担当	㉓サポート教育担当	㉙個人情報取扱責任者							⑨構築系サイバーセキュリティ担当		⑲インフラ担当	⑲インフラ担当			㉚個人情報取扱担当	㉚個人情報取扱担当	㉚個人情報取扱担当	
			⑩運用系サイバーセキュリティ担当	⑪CSIRT担当	㉚個人情報取扱担当	㉚個人情報取扱担当							⑩運用系サイバーセキュリティ担当		⑳サーバ担当	⑳サーバ担当						
			㉕監査責任者	⑫SOC担当											㉑DB担当	㉑DB担当						
			㉖監査担当												㉒ネットワーク担当	㉒ネットワーク担当						

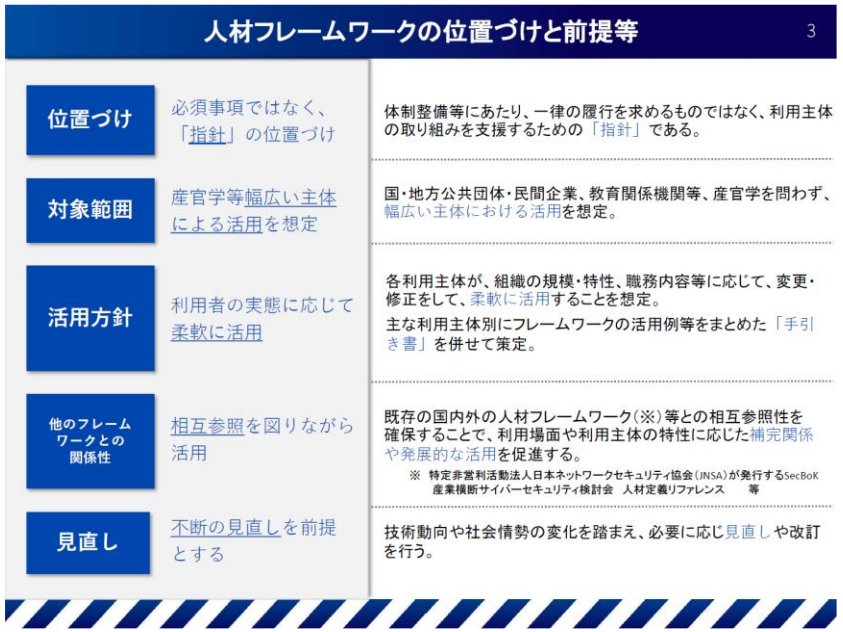
図6-3　人材定義リファレンス2016と2026の対応関係

7．NCO人材フレームワークとの関係及び位置付け

7.1 NCO サイバーセキュリティ人材フレームワークとの関係及び位置付け

- NCOサイバーセキュリティ人材フレームワークは、我が国におけるサイバーセキュリティ人材の育成及び能力開発を支援するため、人材の役割（Work Role）を基盤としてTask、Knowledge及びSkillを体系的に整理した人材フレームワークです。
- 一方、本リファレンスは、ユーザ企業に必要な組織体制、機能、役割及び責任を整理し、組織設計や役割分担を支援することを目的とした実務リファレンスです。
- このように**両者は対象及び目的が異なりますが、いずれもNICE Framework Componentsを共通の参照基盤としていることから、ユーザ企業における組織設計から人材育成までを一貫した考え方で活用することができます。**





出典）国家サイバー統括室（NCO）『サイバーセキュリティ人材フレームワーク2026』
https://www.cyber.go.jp/council/csjinzai/index.html

7.2　NICE Work Roleを活用した対応付け

- **本リファレンスでは、ユーザ企業に必要な役割を整理する際に、NICE Framework ComponentsのWork Roleを共通の参照基盤として採用しています。**
- **NCOサイバーセキュリティ人材フレームワーク**も、同じWork Roleを基盤としてTask、Knowledge及びSkillを整理しています。そのため、**共通のWork Roleを介して、本リファレンスで整理した役割と対応付けることができます。**
- これにより、本リファレンスで整理した役割から、共通のWork Roleを介して必要なTask、Knowledge及びSkillを参照し、**人材育成、教育計画及び能力開発へ展開することが可能となります。**

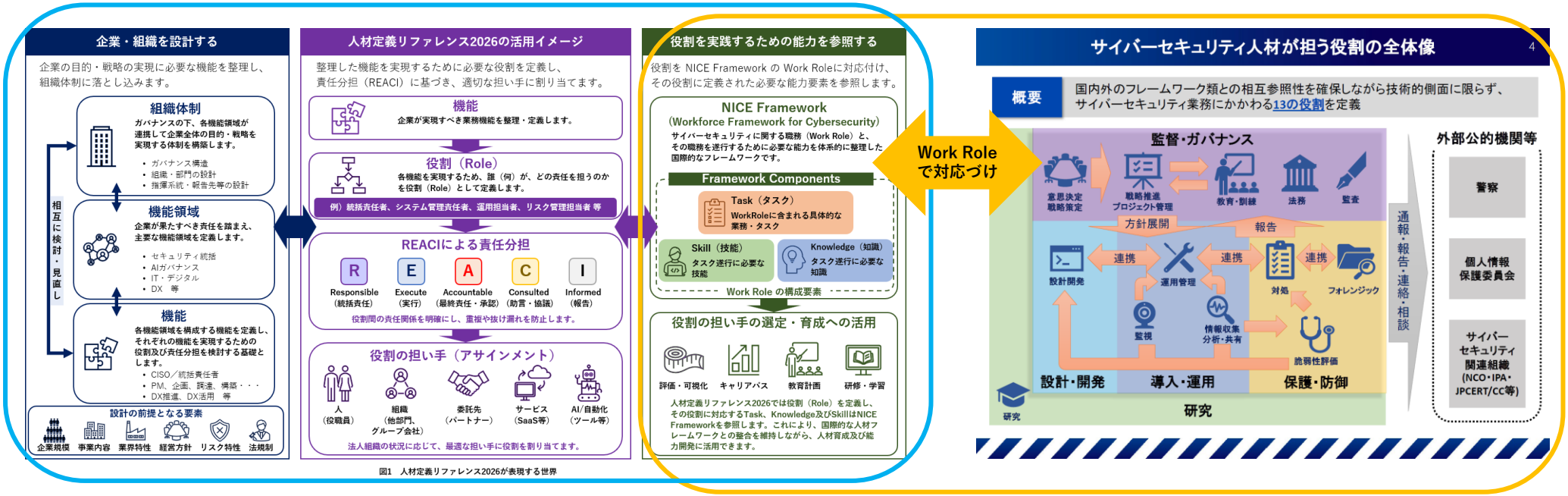


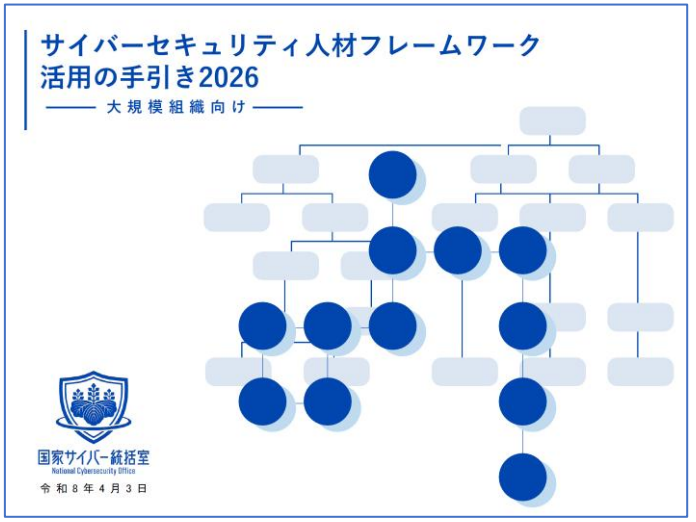
図1　人材定義リファレンス2026が表現する世界

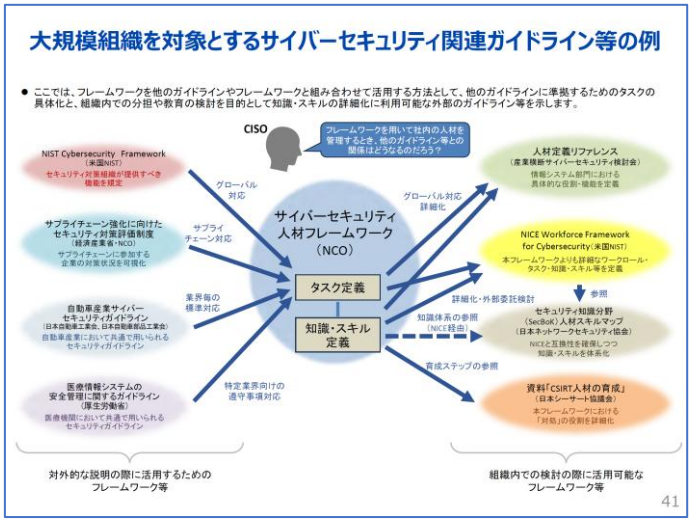
本リファレンスでは、NICE Work Roleを共通言語として採用することで、国内外の人材フレームワークとの対応付けを容易にしています。

出典）国家サイバー統括室（NCO）『サイバーセキュリティ人材フレームワーク2026』
https://www.cyber.go.jp/council/csjinzai/index.html

7.3　他の人材フレームワークとの連携

- NCOが公開する「**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－大規模組織向け－**」では、関連する人材フレームワーク及びガイドラインの例として**人材定義リファレンス2016**が紹介されています。**人材定義リファレンス2016**は、ユーザ企業におけるサイバーセキュリティ体制及び役割を整理するため、**NIST Cybersecurity Framework（NIST CSF）**等を参考として策定されました。
- その後、NISTは**NICE Framework Components**を公開し、人材の役割（Work Role）を中心とした人材フレームワークを整備しました。これを受けて、**人材定義リファレンス2026**では、ユーザ企業に必要な組織体制、機能、役割及び責任を整理するため、また、**NCOサイバーセキュリティ人材フレームワーク**では人材の役割、Task、Knowledge及びSkillを体系的に整理するため、それぞれ**NICE Framework Components**を参照基盤として採用しています。
- このように、**人材定義リファレンス2016から2026への発展の流れ**を踏まえることができるとともに、**人材定義リファレンス2026とNCOサイバーセキュリティ人材フレームワークは、共通のWork Roleを介して相互に対応付けることができます。**これにより、**ユーザ企業における組織体制及び役割の整理と、人材育成、教育計画及び能力開発を相互に参照しながら、一体的に活用することができます。**





出典）国家サイバー統括室（NCO）『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』
「大規模組織を対象とするサイバーセキュリティ関連ガイドライン等の例」
https://www.cyber.go.jp/pdf/council/csjinzai/tebikisyo2026-2.pdf

7.4　人材定義リファレンス2026からNCOサイバーセキュリティ人材フレームワークへの対応関係

- 第6章では、人材定義リファレンス2016から2026への対応関係を整理しました。一方、NCO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では、人材定義リファレンス2016を関連する人材フレームワークの一つとして位置付けています。
- 本リファレンスでは、新たにNICE Framework ComponentsのWork Roleを共通の参照基盤として採用しました。また、NCOサイバーセキュリティ人材フレームワークも共通のWork Roleを基盤としてTask、Knowledge及びSkillを整理しています。
- このため、人材定義リファレンス2016から2026への対応関係を踏まえることで、**本リファレンスで整理した役割を起点として、NCOサイバーセキュリティ人材フレームワークで整理されたTask、Knowledge及びSkillへ展開することができます。**
- 左図は人材定義リファレンス2016と2026の対応関係を、右図はNCO手引き2026における人材定義リファレンス2016の位置付けを示しています。**両図を併せて参照することで、本リファレンスからNCOサイバーセキュリティ人材フレームワークへ展開する流れを理解することができます。**

人材定義リファレンス2016 → 2026 の対応関係（第6章より再掲）

図6-3　人材定義リファレンス2016と2026の対応関係

NCO手引き2026における人材定義リファレンス2016の位置付け

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・[illegible]	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			

出典）国家サイバー統括室（NCO）『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』「4．他の人材フレームワークとの参照関係」
https://www.cyber.go.jp/pdf/council/csjinzai/tebikisyo2026-2.pdf

（参考資料）

８．人材定義リファレンス改定の経緯

8.1 改定の背景

- 2016年に公表した「サイバーセキュリティ人材定義リファレンス」は、ユーザ企業におけるサイバーセキュリティ人材の役割、機能及び業務を体系的に整理したリファレンスとして、多くの企業や関係機関で活用されてきました。また、本リファレンスで示した「セキュリティ統括室等」の考え方は、企業における組織横断的なサイバーセキュリティ推進体制の整備にも活用されています。
- 一方、2016年の公表以降、企業を取り巻く事業環境及び技術環境は大きく変化しました。クラウドサービスの普及、ゼロトラストアーキテクチャへの移行、DXの進展、OT・IoTを含むサイバー・フィジカル・システムの拡大、さらに生成AIの急速な普及などにより、企業に求められるサイバーセキュリティ体制や人材像も大きく変化しています。
- また、この間、国内外ではサイバーセキュリティに関する制度やガイドライン、人材フレームワークの整備が進み、人材に求められる役割や能力を体系的に整理する考え方が発展しました。
- こうした環境変化を踏まえ、産業横断サイバーセキュリティ検討会では2023年より人材定義リファレンスの改定に着手し、現在の企業環境に適した組織体制、人材定義及び役割分担について検討を進めました。
- なお、2016年版「サイバーセキュリティ人材定義リファレンス」の策定に当たっては、当時の国際的なサイバーセキュリティ管理フレームワークであるNIST Cybersecurity Framework（CSF）を参照し、日本企業に適したサイバーセキュリティの機能及び役割を整理しました。この取組は、NISTのSuccess Storiesにおいて「Japanese Cross-Sector Forum」として紹介されています[1]。
- 本改定では、2016年版の基本理念を継承しながら、現在広く活用されている国際的な人材フレームワークであるNICE Framework Componentsを参照し、現在の企業環境に適した実践的な人材定義へと発展させています。

[1] NIST, Success Stories – Japanese Cross-Sector Forum
https://www.nist.gov/cyberframework/success-stories/japanese-cross-sector-forum

参考）2016年に公表した「サイバーセキュリティ人材定義リファレンス」

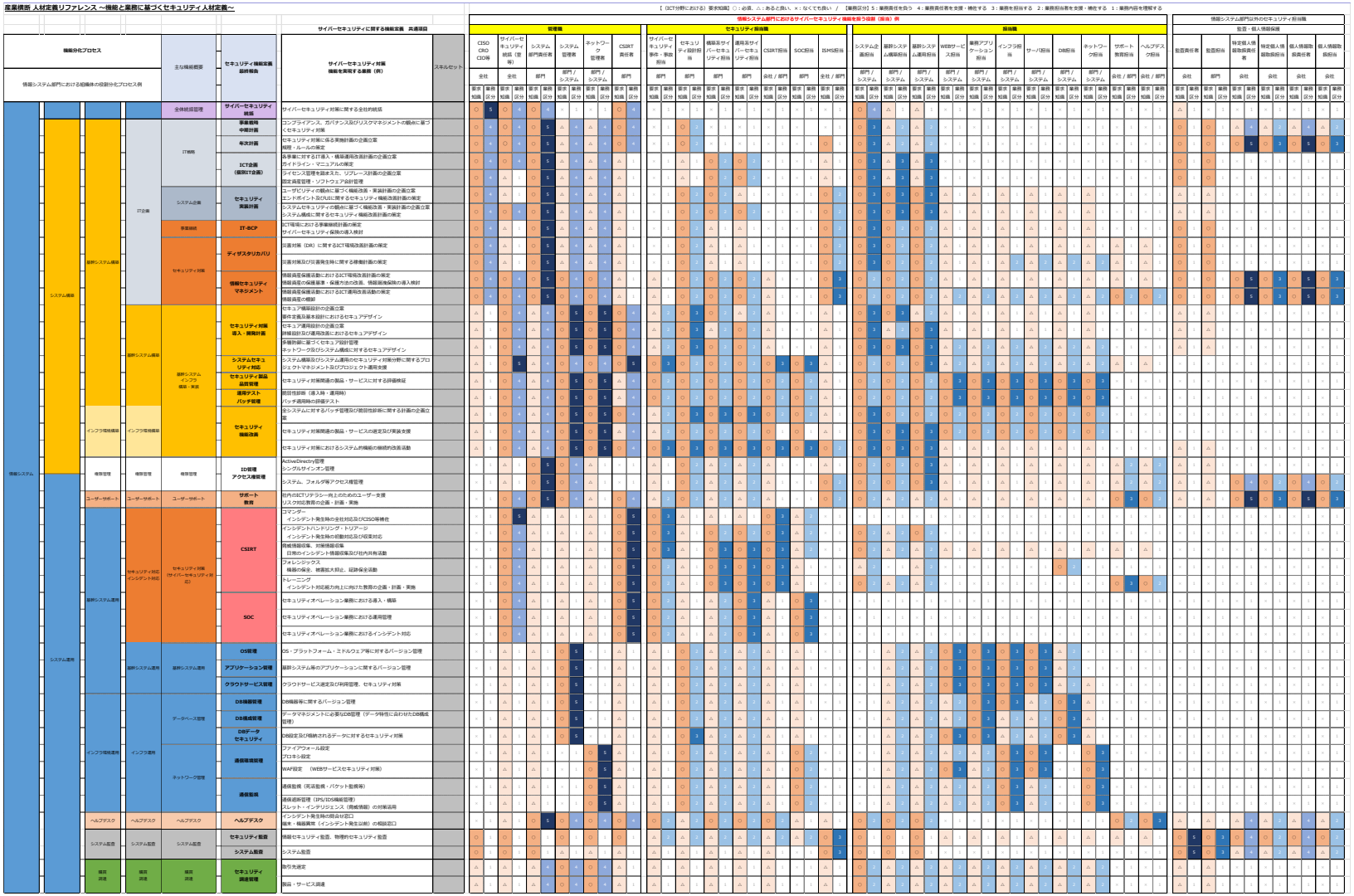


図2-1　人材定義リファレンス2016

8.2　関連する制度・ガイドラインの変遷

- 本リファレンスの改定にあたっては、国内外におけるサイバーセキュリティに関する制度、ガイドライン及び標準の動向を踏まえて検討を進めました。海外では、NIST Cybersecurity Framework（CSF）の改訂に加え、NIST SP 800-181（NICE Framework Components）が整備されました。CSFは組織におけるサイバーセキュリティの管理・改善を目的とした管理フレームワークであり、NICE Framework Componentsは、サイバーセキュリティ人材の役割（Work Role）、Task、Knowledge及びSkillを体系的に整理した人材フレームワークです。国内においても、「サイバーセキュリティ経営ガイドライン」、「サイバー・フィジカル・セキュリティ対策フレームワーク」、ITSS+、デジタルスキル標準（DSS）などの整備が進み、企業に求められる組織体制、人材育成及び能力開発の考え方が発展しています。
- 本リファレンスでは、これらの動向を踏まえ、日本企業の組織体制に適した実践的な人材定義として整理するとともに、NICE Framework Componentsとの対応関係を示すことで、国際的な人材フレームワークとの比較や参照を容易にしています。

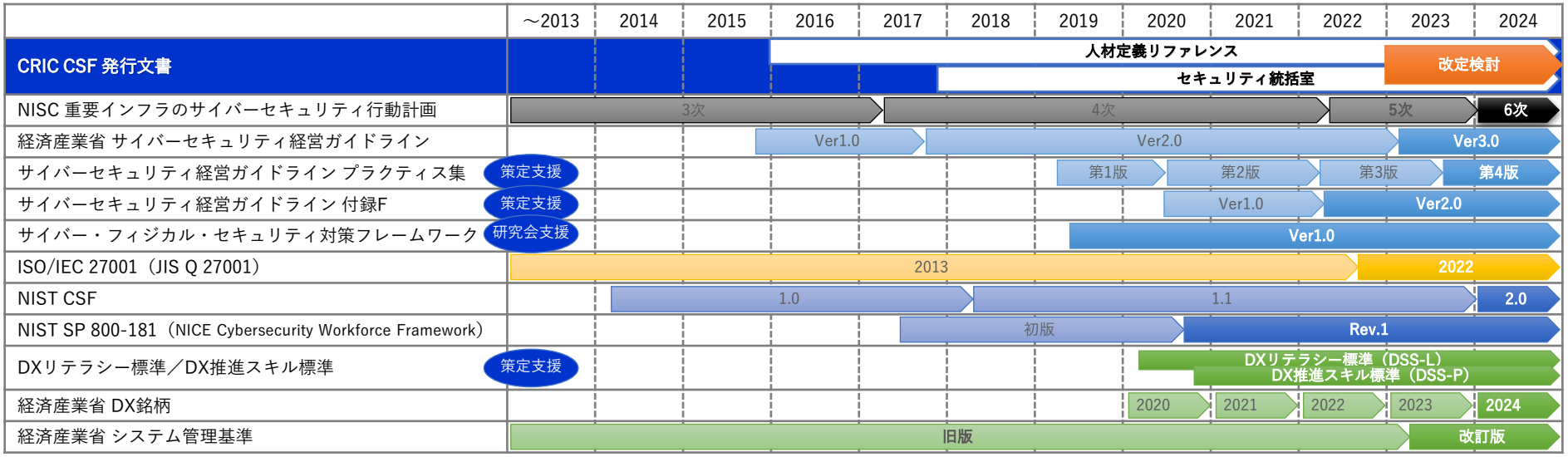


図8-2　関連する制度・ガイドラインの変遷

8.3　人材定義に求められる要件の検討

- 本リファレンスの検討では、ユーザ企業に求められるサイバーセキュリティ人材のあり方について議論を行いました。
- 近年、サイバーセキュリティの対象は、情報システムの保護だけでなく、DX、クラウドサービス、AI、OT・IoT、サプライチェーンなど企業活動全体へと拡大しています。そのため、専門人材だけでなく、各部門と連携しながら事業を安全かつ継続的に支える役割が求められるようになりました。
- 一方、日本では人材不足や専門人材の確保に重点が置かれる一方で、「誰が、どの業務を担い、その役割に何が求められるのか」という観点から人材を整理する考え方は十分に体系化されていませんでした。また、急速な技術の進展に対して、資格や研修制度だけでは企業が求める能力との間に時間差が生じることも課題となっています。
- こうした課題を踏まえ、本リファレンスでは、ユーザ企業に必要な役割と業務を起点として人材を定義し、組織設計、人材配置、人材育成及び能力開発へ展開できる実践的なリファレンスを目指しました。

課題	本リファレンスで目指した方向性
サイバーセキュリティの対象範囲が急速に拡大	企業全体を対象とした人材定義
人材不足中心の議論	人材配置・役割分担・能力開発を重視
業務と能力の関係が整理されていない	業務→役割→能力を体系化
技術進歩に教育が追従しにくい	企業が主体的に能力開発できる仕組み
国際的な比較が難しい	国際的な人材フレームワークとの対応を整理

表8-3　課題意識と本リファレンスにおける対応

8.4　検討の基本方針

- 本リファレンスの改定に当たっては、2016年版の基本理念を継承しながら、企業を取り巻く環境変化や国際的な動向を踏まえ、実務で活用しやすいリファレンスとなることを目指しました。主な基本方針は次のとおりです。

1. 日本企業における組織体制を前提とした人材定義とすること。

- ユーザ企業に必要な組織体制を起点として、機能、役割及び業務を体系的に整理することを基本としました。

2. 「セキュリティ統括室等」の考え方を継承し、組織横断的なガバナンスを強化すること。

- サイバーセキュリティを経営課題として捉え、全社的なガバナンスを担う中核機能として位置付けました。

3. クラウド、ゼロトラスト、AI、OTなど、新たな技術環境へ対応すること。

- 技術環境の変化を踏まえ、企業に求められる機能領域、機能及び役割を拡充しました。

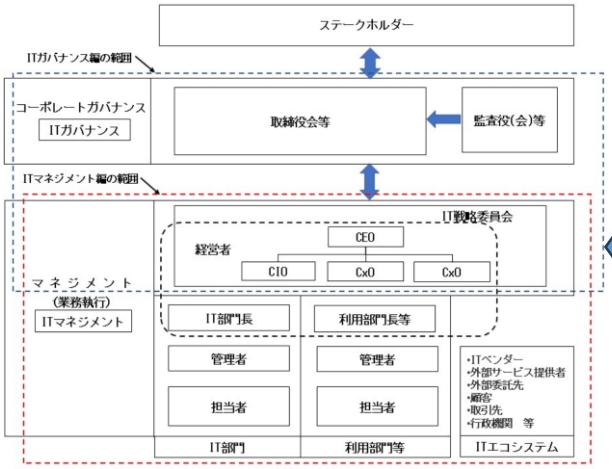
4. NICE Framework Componentsとの対応関係を整理すること。

- 国際的な人材フレームワークとの比較や参照を容易にしました。

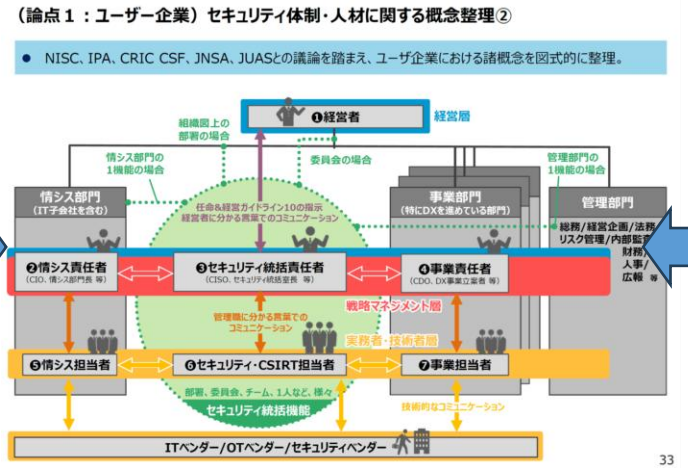
5. 機能を明確化するとともに、各機能を担う役割と責任分担を整理し、REACIモデルを用いて実務への適用を容易にすること。

- REACIを用いて役割間の責任範囲及び連携関係を整理し、組織設計、人材育成、役割分担及び規程整備などへの活用を可能としました。

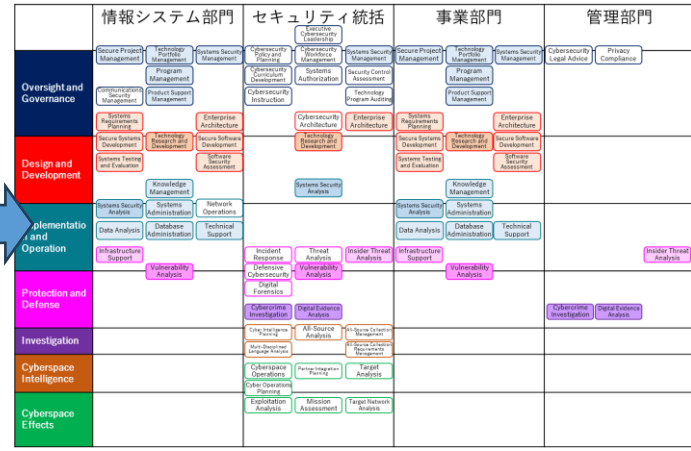
8.5　様々な体制モデルの参照



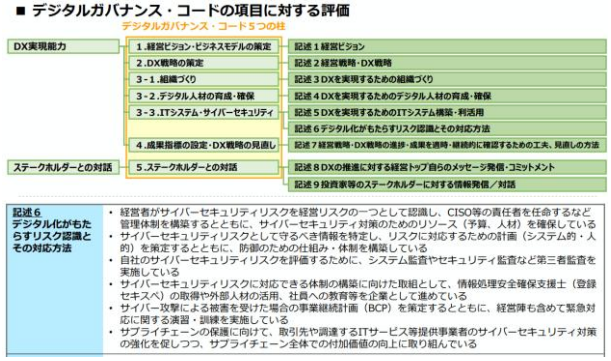
「システム管理基準」が想定する組織体の体制



第4回 産業サイバーセキュリティ研究会 ワーキンググループ2
（経営・人材・国際）資料3　事務局説明資料

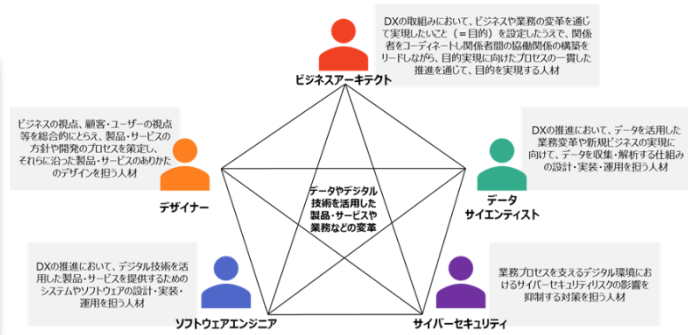


セキュリティ体制・人材に関する概念整理に基づく
NIST SP 800-181マッピング（2023年度版）



デジタルトランスフォーメーション調査（DX調査）2025

人材定義リファレンス
202x



「DX推進スキル標準」の人材類型の定義

図8-5　様々な体制モデルの参照

8.6　NICE Framework Componentsの概要と活用

- 本リファレンスでは、サイバーセキュリティ人材を国際的な人材フレームワークと整合させるため、NISTが策定・公開しているNICE Framework Componentsを参照しています。
- NICE Framework Componentsは、サイバーセキュリティ人材を体系的に整理するための人材フレームワークであり、Work Roleを中心に、Task（タスク）、Knowledge（知識）及びSkill（技能）を関連付けて定義しています。これにより、組織に必要な役割の整理、人材配置、人材育成及び能力開発を一貫した考え方で進めることができます。
- 本リファレンスでは、NICE Framework Componentsをそのまま採用するのではなく、日本企業の組織体制を前提として、「組織体制」「機能領域」「機能」「役割」及び「業務」に対応付けることで、企業における実務へ適用しやすい人材定義として再構成しています。
- なお、本リファレンスは、NICE Framework Components Version 2.0.0を基に検討を開始し、その後公開されたVersion 2.1.0及びVersion 2.2.0の変更内容を反映することで、最新版との整合性を確保しています。
- 表2-6に、NICE Framework Componentsの主なバージョンアップの概要を示します。

バージョン	公開	Update	本リファレンスへの影響
v1.0.0	2024年3月	Major	Componentsの基盤
v1.1.0	2024年8月	Minor	AI・Data Privacyを反映
v2.0.0	2025年3月	Major	本リファレンスの検討開始時の基準
v2.1.0	2025年12月	Minor	AI Security更新を確認・反映
v2.2.0	2026年4月	Minor	サイバーサプライチェーン・リスクマネジメント（C-SCRM）、DevSecOps等を確認・反映

表8-6　NICE Framework Componentsの主なバージョンアップ

Oversight and Governance | Implementation and Operation | Investigation
Design and Development | Protection and Defense | Cyberspace Intelligence | Cyberspace Effects

凡例：NICEフレームワーク（旧版）との関係性

8.7　第6期 検討を進める体制モデルと役割分担（たたき台）

凡例：技術PF（技術ポートフォリオ）
Pg管理（プログラム管理）

図8-7　第6期 検討を進める体制モデルと役割分担（たたき台）

8.8　本改定の位置付け

- 本リファレンスは、2016年版の基本理念を継承しながら、企業を取り巻く環境や技術の変化を踏まえ、その内容を発展・拡充したものです。
- 本リファレンスでは、日本企業の組織体制を前提として、組織体制、機能領域、機能、役割及び業務を体系的に整理するとともに、NICE Framework Componentsとの対応関係を示すことで、国際的な人材フレームワークとの整合を図っています。
- 本解説書を通じて、本リファレンスで用いる「組織体制」「機能領域」「機能」「役割」及び「業務」の考え方を解説しました。

CRIC CSF 人材定義リファレンス2016

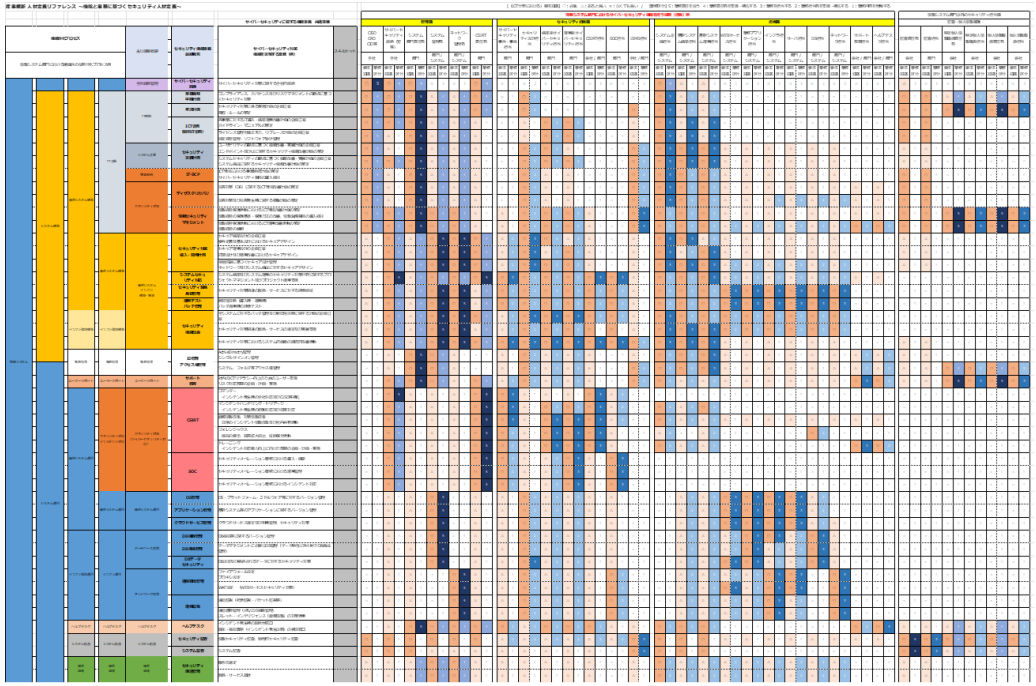


図2-1　人材定義リファレンス2016

継承発展

CRIC CSF 人材定義リファレンス2026

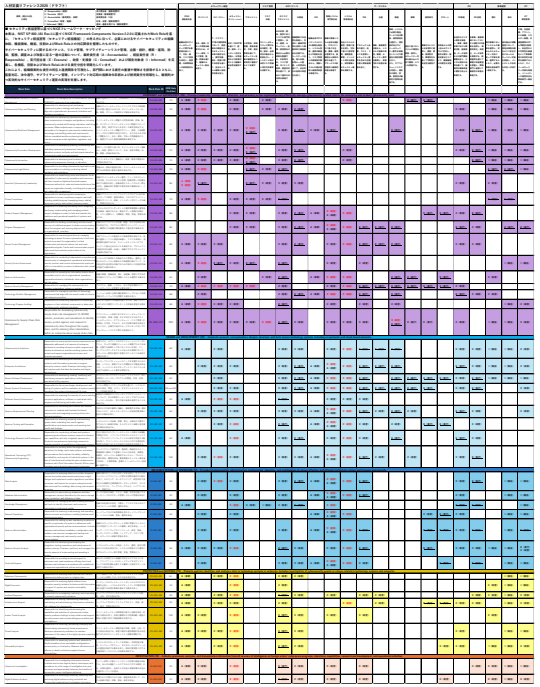


図0　人材定義リファレンス2026

（参考資料）

第6期 活動報告書（抜粋）

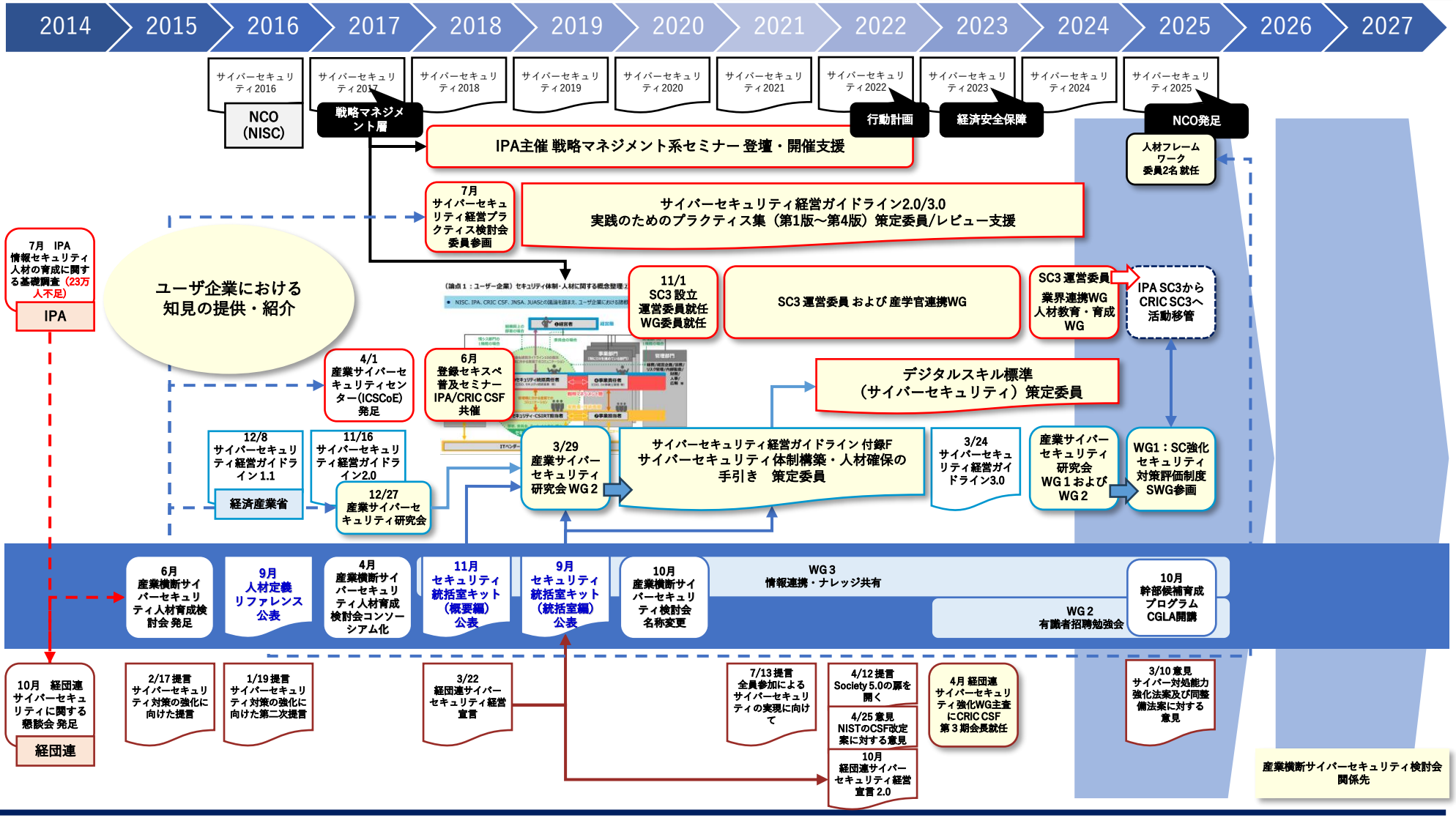
産業横断サイバーセキュリティ検討会について

- 経団連傘下「サイバーセキュリティに関する懇談会」の有志企業により、2015年6月9日「産業横断サイバーセキュリティ人材育成検討会」として発足
- オリパラに向けたセキュリティ対応体制強化を目途に、産官連携による施策展開や、ユーザ企業視点でのセキュリティ人材活用のためのドキュメント等を策定し公開
- 2020年10月より、名称を「産業横断サイバーセキュリティ検討会」に改め、人材育成のみならずユーザ企業が直面するセキュリティ課題について幅広く対応

業界の壁を越えた信頼の輪に基づく情報共有、及び産官学連携の活動を通じて得られたセキュリティ課題の解決を目指し、国内外で活発に活動を行っていく

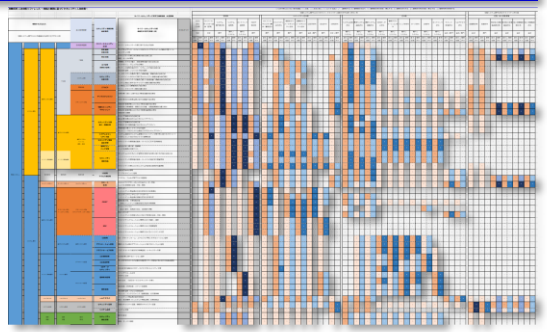
業界横断でのクローズドな情報交換	・平場では話せない事例/ナレッジの共有、議論 ・有識者を交えたWGでのインテリジェンス勉強会
産業界代表として政府／経団連会合等へ参画	・産業サイバーセキュリティ研究会WG ・SC3、サイバーセキュリティに関する懇談会　他
公的機関にも採用・引用される成果物	・人材定義リファレンス ・セキュリティ統括室キット　他
国内外での積極的な活動実績	・米NISTカンファレンスでの講演 ・IPAセミナーへの協力　他

発足から第６期まで活動状況

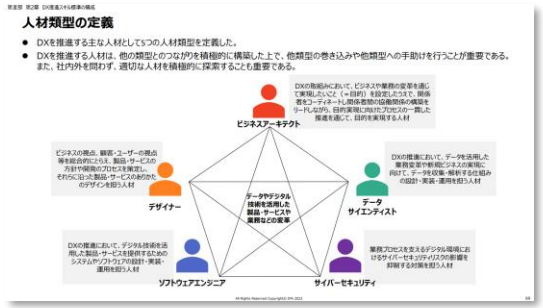


DX推進とサプライチェーンの維持のためのリファレンス改定

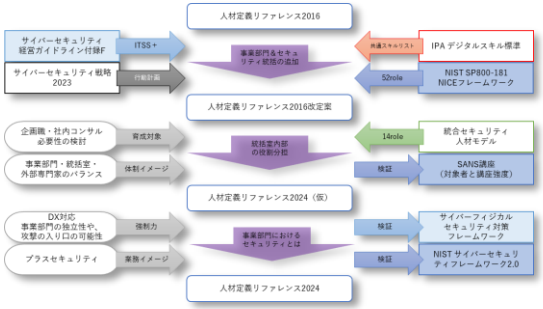
- 2016年、産業横断サイバーセキュリティ検討会（CRIC CSF）ではNIST Cybersecurity Framework1.1を活用し、日本企業の組織体制に適したユーザ企業のためのセキュリティ体制をリファレンスとして公開しました。
- 現在、サイバーセキュリティ経営ガイドライン3.0 が公表され、2024年にはNIST Cybersecurity Framework2.0 が重要インフラ事業者だけではなく全ての事業者を対象として公開されたことにより、**サプライチェーンを意識したサイバーセキュリティに関する情報共有活動**として広がってきています。
- これまでは第５期末を目指し、本紙の活動のスコープで紹介しました様々なセキュリティ課題に取り組むために必要とされる組織体（セキュリティ統括室等）を再定義し、**包括的な全社セキュリティ体制のモデル**として検討を進めて参りましたが、昨今のランサム被害の拡大および急速なAI利用の拡大に伴い、検討の範囲が広がっています。
- 検討にあたっては、様々な要素（サイバー空間におけるサプライチェーンや、ゼロトラストの取り組み等）を加味し、経済産業省の評価制度、IPA デジタルスキル標準など国内で議論が進む枠組みを参考にしながら、ユーザ企業が集まる**産業横断らしいセキュリティ体制及び人材のあり方**を提示していく所存です。
- 更には、NCO人材フレームワークとの連携を想定し実効力のある組織体制のモデルを模索していきます。



CRIC CSF 人材定義リファレンス 2016年度版



IPA/METI　デジタルスキル標準 ver.1.1



人材定義リファレンス 改定プロセス

NIST | Success Story: Japanese Cross-Sector Forum
https://www.nist.gov/cyberframework/success-stories/japanese-cross-sector-forum

セキュリティ機能モデル（体制と人材）｜CRIC CSF 第６期検討資料

- セキュリティ統括室等の体制検討モデル
  - 4つの機能を定め、法人組織や事業等により必要な機能を採用するモデル。
  - セキュリティ統括室等の体制構築に加えてNIST SP800-181（NICEフレームワーク2.0.0）に基づく役割を活用する想定であり、タスクやスキルはNICEを準用し、効果的な体制更新と人材育成を目指すモデルである。