
人材定義リファレンス2026

取組説明資料

2026年9月7日

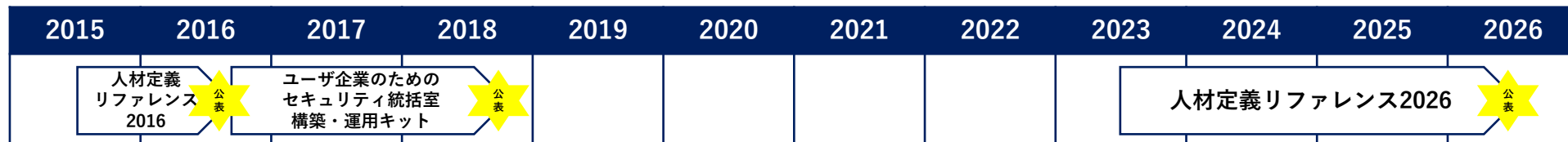
産業横断サイバーセキュリティ検討会

概要説明

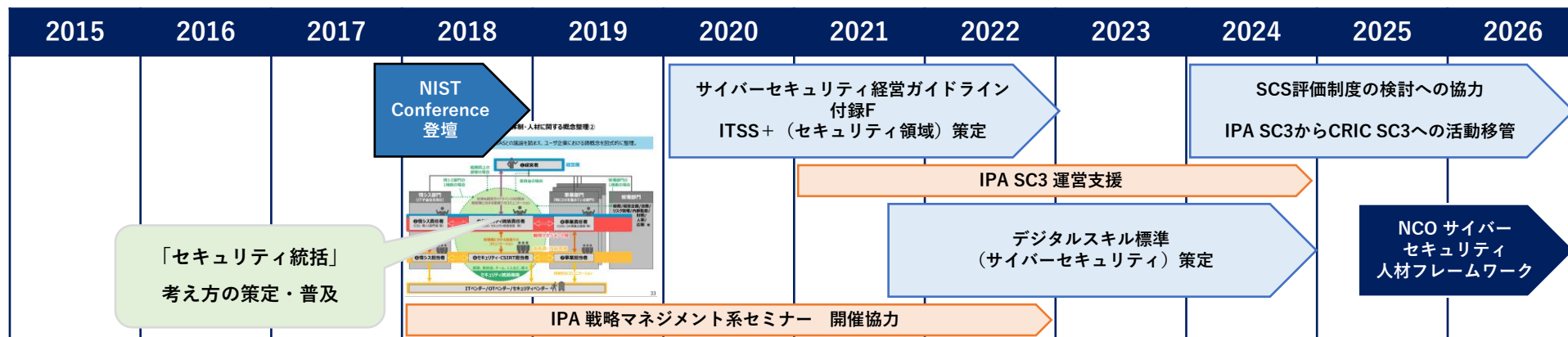
産業横断サイバーセキュリティ検討会

- 産業横断サイバーセキュリティ検討会（CRIC CSF）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発足しました。ユーザ企業が直面するサイバーセキュリティ上の課題を共有し、業種や業界を越えて、組織体制、人材、ガバナンス及び実務上の対応について検討しています。
- 検討成果を独自のリファレンスや実務資料として公開するとともに、政府・関係機関が進める制度、ガイドライン及び人材施策の検討にも、委員参加や知見提供を通じて協力してきました。

◆ CRIC CSFによる主な成果



◆政府・関係機関の取組への協力（委員・WG参加、策定支援、運営支援、知見提供等）



企業における実務的な検討と、国の制度・ガイドライン・人材施策への協力を往復しながら、産業界で活用できる成果を継続的に整理してきました。

産業横断サイバーセキュリティ検討会の会員構成と活動体制

・ 会員一覧（42社）

- ・ 住友化学株式会社
- ・ 全日本空輸株式会社
- ・ トヨタ自動車株式会社
- ・ KDDI株式会社
- ・ JCOM株式会社
- ・ 大日本印刷株式会社
- ・ TOPPANホールディングス株式会社
- ・ 三井不動産株式会社
- ・ 株式会社竹中工務店
- ・ 大成建設株式会社
- ・ 株式会社みずほ銀行
- ・ 日本生命保険相互会社
- ・ ヤマトホールディングス株式会社
- ・ パナソニック ホールディングス株式会社
- ・ 株式会社東芝
- ・ JSR株式会社
- ・ ENEOSホールディングス株式会社
- ・ 中外製薬株式会社
- ・ 東海旅客鉄道株式会社
- ・ 三菱電機株式会社
- ・ 東急不動産ホールディングス株式会社
- ・ 日本電気株式会社
- ・ NTT株式会社
- ・ 株式会社日立製作所
- ・ 富士通株式会社

順不同、その他各社グループ企業

・ 組織構成

WG	名称	活動概要	主な成果物・活動成果
WG1	セキュリティ経営戦略検討WG	ユーザ企業に必要なサイバーセキュリティの組織体制、人材、役割分担及びガバナンスについて検討する。検討成果を実務資料として整理・公開するとともに、国の制度・施策へ知見を提供する。	・ 人材定義リファレンス 2016/2026 ・ セキュリティ統括室構築・運用キット ・ 制度・ガイドライン等への策定協力
WG2	Security Study Meetup	国内外の制度、技術及び実務動向を継続的に収集する。有識者や実務家を招いた勉強会を通じて、会員企業の知識向上と相互交流を図る。	・ 有識者・実務家による勉強会 ・ 国内外の最新動向の共有 ・ 参加者間の情報交換・交流
WG3	情報連携・ナレッジ共有WG	ユーザ企業が直面するインシデントや対策事例について、会員企業間で実務的な情報・知見を共有する。	・ インシデント・対策事例の共有 ・ 各社の取組に関する意見交換 ・ 会員企業限定の非公開活動
WG4	AI WG	AIの利活用、推進体制、リスク及び実務上の課題について情報を収集し、企業における安全かつ適切なAI活用のあり方を検討する。	・ 有識者・企業による勉強会 ・ AI活用事例と課題の共有 ・ 今後の検討テーマ及び成果の整理

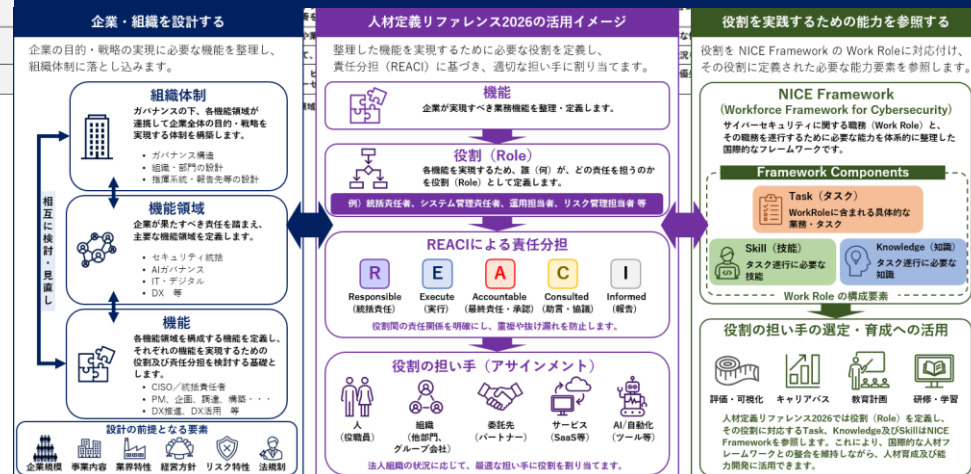
- 人材定義リファレンス2026では、日本企業の組織体制を前提に、サイバーセキュリティに必要な「機能領域」「機能」「役割」「業務」を体系化しました。REACIによる責任分担とNICE Framework Componentsとの対応を示し、組織設計から役割の割当て、人材育成まで一体的に活用できる構成としています。

[illegible]

整理内容 | 企業に必要な機能領域・機能・役割

	機能領域	機能	役割
セキュリティ統括	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。
		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括を推進する。
		テクノ／ロジー	IT・クラウド・OT等の技術動向において、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の支援を担う。
	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、日常運用および発生時における脆弱性の脆弱性を維持する。	
		マネジメント	人材育成、体制整備、監査・評価管理を通じて、セキュリティ活動が継続的に効果的に機能するように支援する。
リスク管理	リスク・評価	リスク・評価	サイバーセキュリティに関する法令・規制、国際・国内の動向の観点から助言を行い、インシデント時の即時リスク評価と対応方針策定を支援する。
		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構築する。AI利用方針、リスク評価、方針・システム基準、監査対応などを実施し、安全かつ適正なAI活用を推進する。
	AI/バリエーション	AI/推進	組織内で「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。ユースケース管理、導入・ロール整備、人材育成を通じて、全社的なAI活用の高度化を担う。
		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。システム等内部統制の観点から、情報システムの修正・更新と継続的改善を推進する。
	情報セキュリティ部門責任者		組織の情報システム全体を統括し、ITガバナンスに基き企画・構築、運用を管理する。資源配分・統制の整備を通じて、ITサービスの安定提供と継続的改善を推進する。
IT・デジタル	システム管理	システム管理責任者	担当システムの利用・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をサービス及び開発・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上で調達及び委任管理を行うため、サプライチェーンリスクを考慮し、委託先の選定、評価、監査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構築・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	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。	

活用方法 | 組織設計から人材育成まで



参考資料①

人材定義リファレンス2026の 策定背景・検討経緯・検討結果

人材定義リファレンス2026策定の背景と経緯（解説書 1. はじめに より）

・ 2015～2018年 産業界共通の人材・組織モデルの整備

- ・ 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を発足しました。
- ・ 2016年：「サイバーセキュリティ人材定義リファレンス」を公表
- ・ 2018年：「セキュリティ統括室構築・運用キット」を公表
- ・ 「セキュリティ統括」の考え方は、ITSS+でも参照され、企業の人材育成・組織体制整備に活用

・ 2020年以降 企業を取り巻く環境の変化

- ・ クラウド、SaaS、ゼロトラスト、サプライチェーン、OT・IoTの普及により、サイバーセキュリティは情報システム部門だけでなく、経営層、事業部門、取引先・委託先を含めて取り組むべき経営課題へと発展しました。さらに、2023年以降の生成AIの急速な普及に伴い、AIガバナンス、AIリスクマネジメント、データ管理、説明責任など、新たな役割と専門性が求められるようになりました。

・ 2023～2026年 人材定義リファレンスの改定

- ・ こうした変化を踏まえ、2023年から改定に着手し、ユーザ企業に求められる組織体制、機能、役割及び責任分担を改めて検討しました。2016年版の基本理念を継承しながら、現在の企業環境と技術動向を反映し、NICE FrameworkのWork Roleとの対応関係を整理した「人材定義リファレンス2026」として取りまとめました。

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て、組織設計、人材育成、
役割・責任の明確化に活用できる実践的なリファレンス

人材定義リファレンス2026が目指したもの（解説書 1. はじめに より）

- ・ 人材定義リファレンス2026 では、特定の職種や人材像を起点とするのではなく、企業の目的・戦略の実現に必要な機能を整理し、その機能を担う役割と責任分担を明確にします。さらに、各役割をNICE FrameworkのWork Roleに対応付けることで、組織体制の整備から担い手の選定・育成までを一貫して検討できる構造としました。

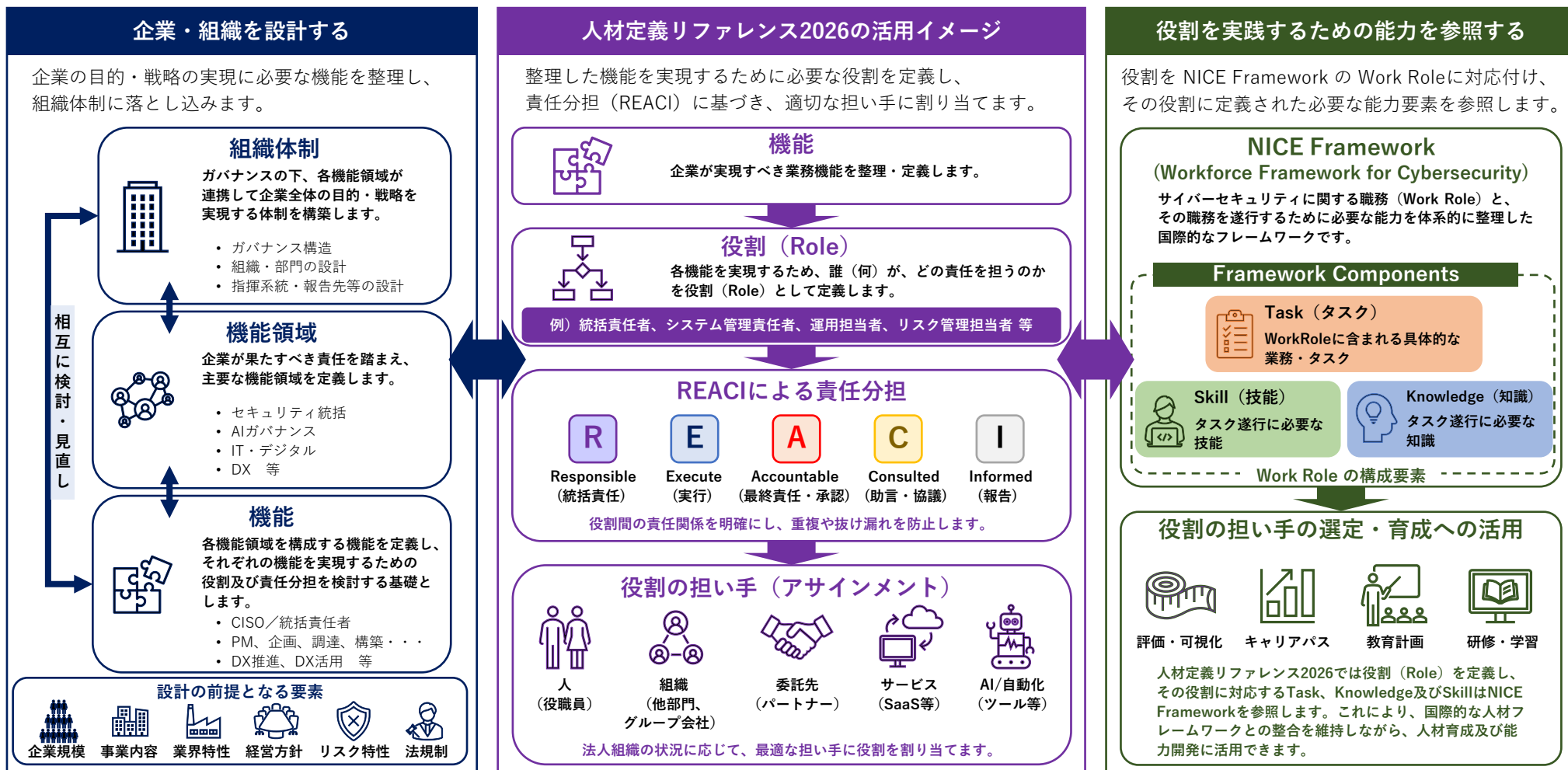


図1 人材定義リファレンス2026が表現する世界

2016年以降に進展した制度・ガイドラインと人材フレームワーク（解説書 8章より）

- 2016年版の公表以降、国内外では、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整備・改定が進みました。また、**NICE Framework Components**や**デジタルスキル標準**など、業務、役割及び能力を体系的に捉える人材フレームワークも発展しています。
- こうした変化を踏まえ、2016年版の基本理念を継承しながら、現在の企業環境と国内外の人材フレームワークに対応した人材定義へと改定する必要がありました。

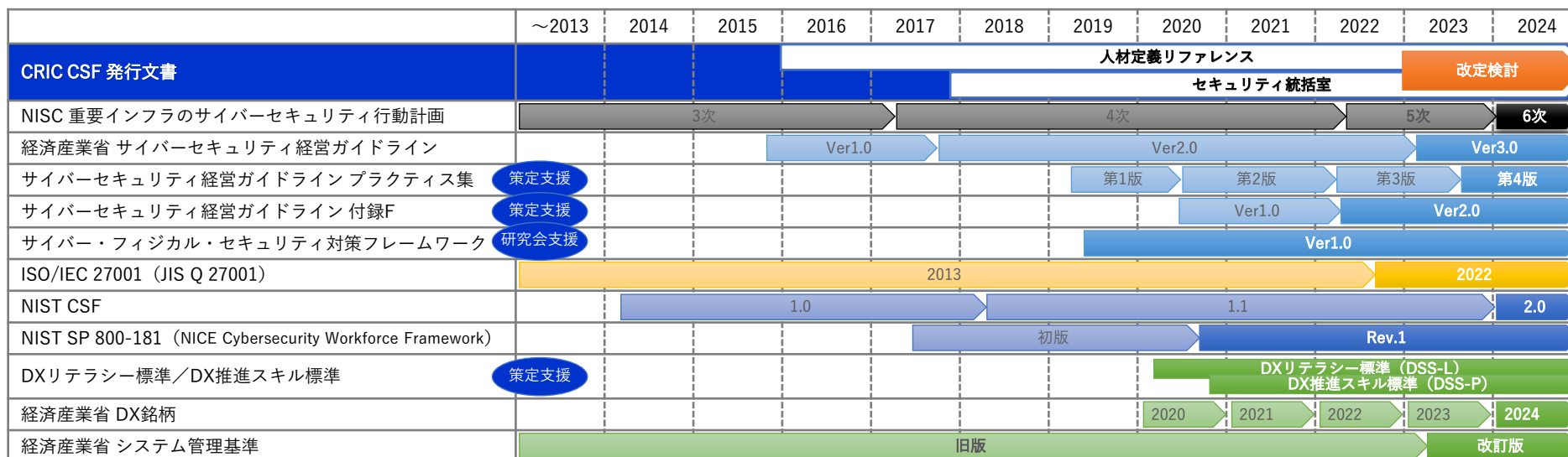


図8-2 関連する制度・ガイドラインの変遷

組織のサイバーセキュリティ管理を示す枠組みだけでなく、
業務・役割・能力を結び付ける人材フレームワークとの接続が必要となった。

課題認識を踏まえて設定した改定の基本方針（解説書 8章より）

- ・ 検討会では、サイバーセキュリティの対象範囲が企業活動全体へ拡大する一方、従来の人材不足を中心とした議論だけでは、企業に必要な業務、役割及び能力を十分に整理できないことを課題として認識しました。
- ・ こうした課題を踏まえ、2016年版の基本理念を継承しながら、**現在の企業環境に適した実践的な人材定義**とするため、5つの基本方針を定めました。

・ 検討会が認識した課題

- ・ サイバーセキュリティの対象範囲が企業活動全体へ拡大
- ・ 人材不足や専門人材の確保に議論が偏っている
- ・ 業務、役割及び能力の関係が整理されていない
- ・ 技術進歩に資格・研修制度が追随しにくい
- ・ 国際的な人材フレームワークとの比較が難しい

・ 改定における5つの基本方針

- ・ 日本企業の組織体制を前提とした人材定義
- ・ 「セキュリティ統括室等」の継承と組織横断的なガバナンスの強化
- ・ クラウド、ゼロトラスト、AI、OT等の新たな技術環境への対応
- ・ NICE Framework Componentsとの対応関係の整理
- ・ 機能、役割及び責任分担の明確化とREACIによる実務への展開



「人材が何人必要か」ではなく、
「企業にどのような機能が必要で、誰がどの役割と責任を担うのか」を起点として人材を捉え直した。

2016年版の基本理念を継承し、現在の企業環境へ発展（解説書 8章より）

- ・人材定義リファレンス2026は、2016年版で示した、日本企業に必要な機能、役割及び業務を整理する基本理念を継承しながら、対象範囲と役割分担の考え方を発展させたものです。
- ・組織横断的なガバナンス、新たな技術環境への対応、REACIによる責任分担及びNICE Frameworkとの対応関係を加え、現在の企業環境に適用できる構成へと拡張しました。

CRIC CSF 人材定義リファレンス2016

This matrix illustrates the roles and responsibilities defined in the 2016 version of the CRIC CSF Human Resource Reference. It is organized into columns representing different functional areas and rows representing specific roles. The matrix uses a color-coded system (blue, orange, green, yellow) to indicate the level of responsibility or involvement for each role in each domain.

図2-1 人材定義リファレンス2016

CRIC CSF 人材定義リファレンス2026

This matrix illustrates the roles and responsibilities defined in the 2026 version of the CRIC CSF Human Resource Reference. It builds upon the 2016 version, adding new roles and responsibilities to address emerging technologies and business environments. The matrix uses a color-coded system (blue, orange, green, yellow) to indicate the level of responsibility or involvement for each role in each domain.

図0 人材定義リファレンス2026

継承
発展

2016年版で確立したもの

ユーザ企業を前提とした人材定義

機能・役割・業務の体系化

セキュリティ統括室等の考え方

NIST CSFを参照

役割分担の整理

ITを中心とした構成

2026年版で発展させたもの

日本企業の組織体制を起点とした全体設計

機能領域・機能・役割・担い手の体系化

組織横断的なガバナンスへの拡張

NICE Frameworkとの対応

REACIによる責任関係の明確化

AI、DX、クラウド、OT等への拡張

検討結果① 組織体制から役割・能力までをつなぐ基本構造（解説書 2章より）

- 人材定義リファレンス2026では、企業の組織体制を起点として、機能領域、機能、役割及び責任分担を段階的に整理しました。さらに、役割をNICE FrameworkのWork Roleに対応付けることで、役割の担い手の選定、人材育成及び能力開発までを一貫して検討できる構造としています。

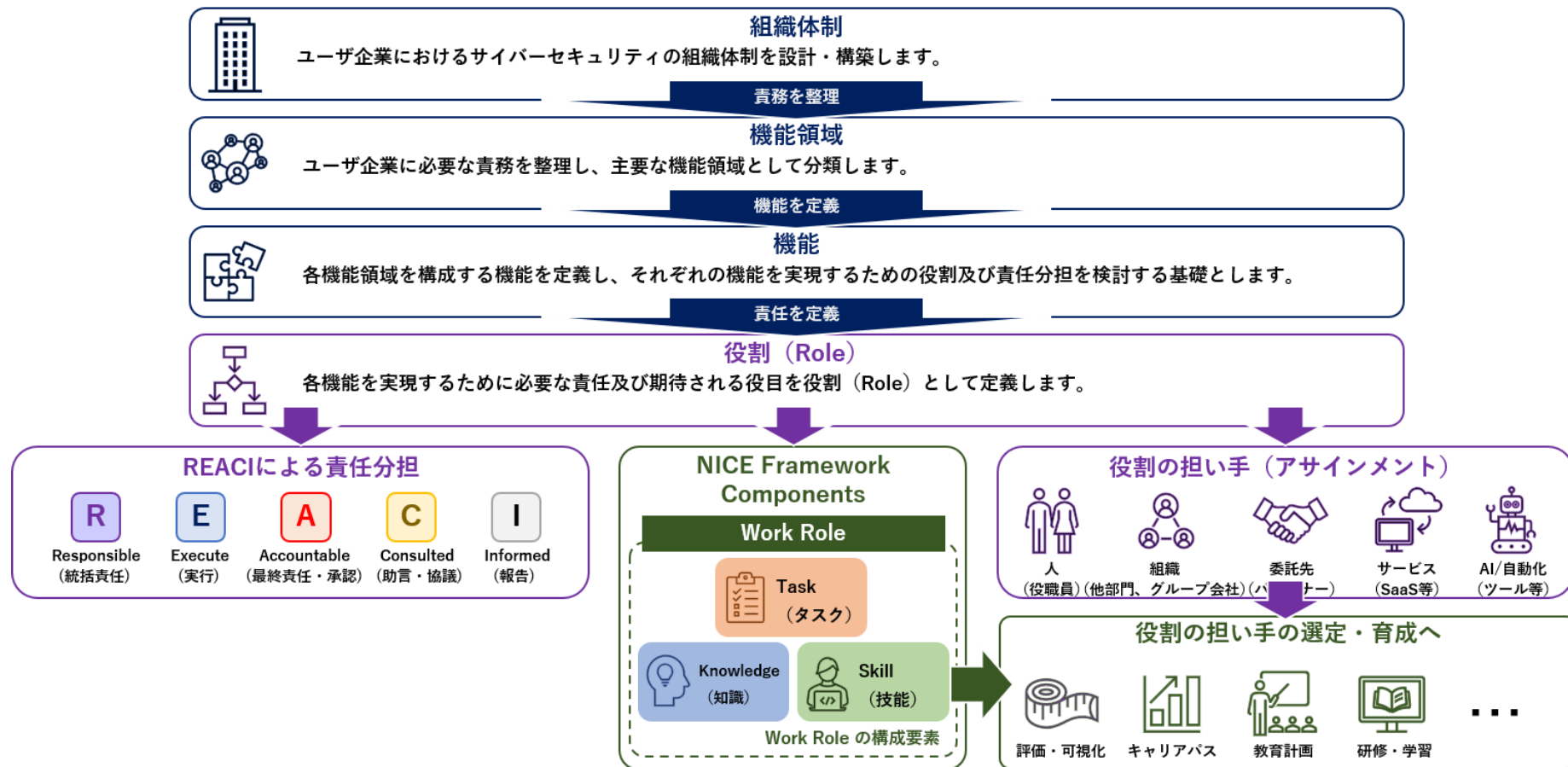


図2-3 人材定義リファレンス2026の基本構造

検討結果② 企業全体を対象とした組織体制モデル（解説書 3章より）

- サイバーセキュリティをセキュリティ専門組織だけの業務として捉えるのではなく、リスク管理、AIガバナンス、IT・デジタル、DX、事業運営及びOTを含む企業活動全体の取組として整理しました。各機能領域が相互に連携し、それぞれの役割を担うことを前提としています。

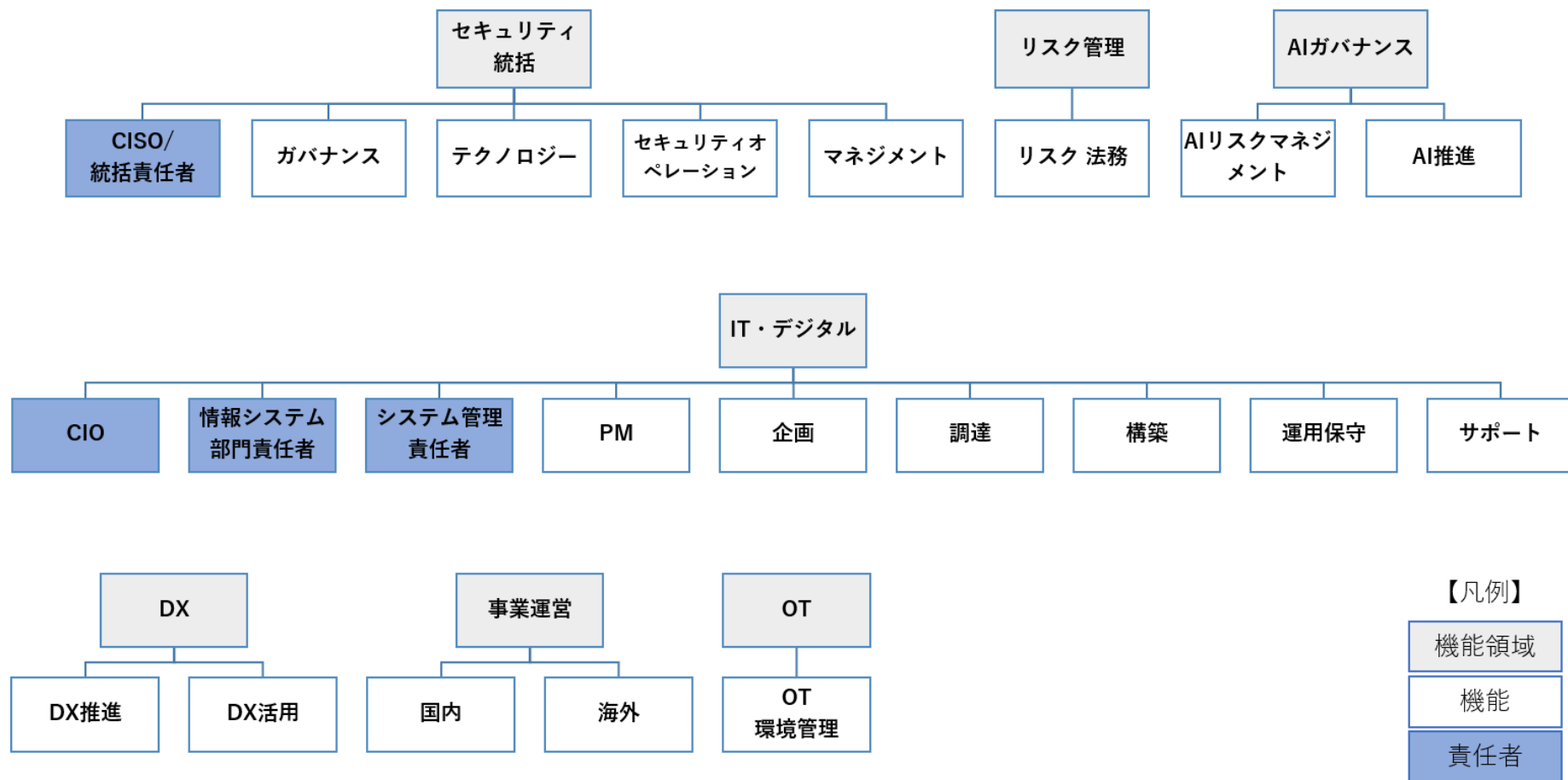


図3-2 人材定義リファレンス2026において想定する組織体制のモデル

検討結果③ 各機能領域に必要な機能と役割を具体化（解説書 3章より）

- 組織体制モデルで示した各機能領域について、その領域を構成する機能と、機能を実現するために求められる役割を具体的に整理しました。これにより、企業は自社の組織や職制と照らし合わせながら、必要な機能の有無と役割の担い手を確認できます。

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括を担う。
		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

検討結果④ 機能・役割とNICE Work Roleを対応付けた全体像（解説書 4章より）

- **人材定義リファレンス2026**では、ユーザ企業に必要な機能と役割を整理するとともに、各役割をNICE Framework ComponentsのWork Roleに対応付けています。
- また、**各機能を担う役割間の責任関係をREACIで示すことで、組織設計、役割分担及び能力開発へ展開できる全体構造としました。**
- 表の構成
 - 縦軸：NICE FrameworkのWork Role
 - 横軸：日本企業における組織・役割
 - 交点：REACIによる責任分担

NICE Work Roleを共通の参照基盤としたことで、国内外の人材フレームワークとの関係を整理できる構造としています。

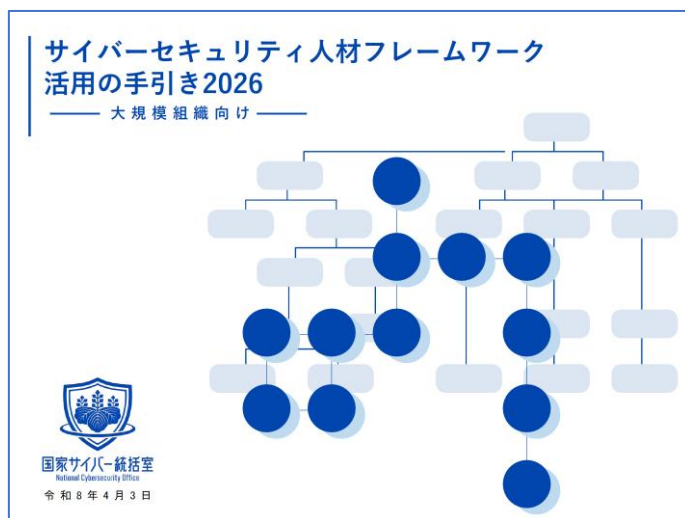
CRIC CSF 人材定義リファレンス2026

[illegible]

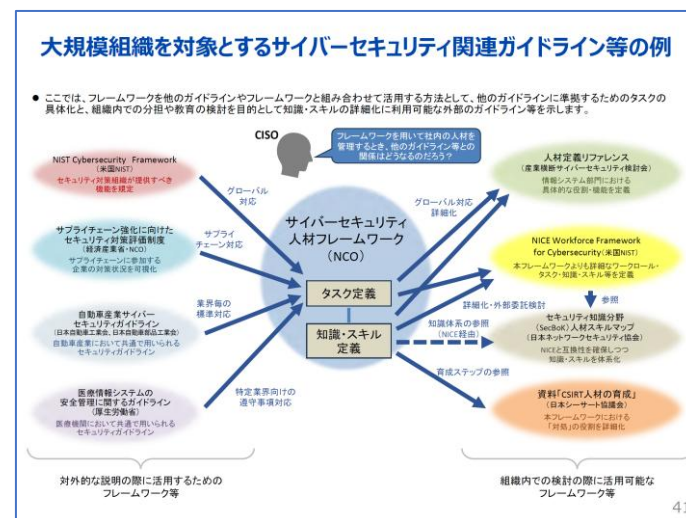
図0 人材定義リファレンス2026

NCO手引きにおける人材定義リファレンスの位置付け（解説書 7.3 より）

- NCOの「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NIST CSF等を参考に、ユーザ企業のサイバーセキュリティ体制と役割を整理しました。その基本理念を継承した**人材定義リファレンス2026**では、新たにNICE Framework ComponentsのWork Roleを参照基盤として採用しています。



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>



2016年版で整理した組織体制と役割の考え方を継承し、2026年版ではNICE Work Roleを介して国内外の人材フレームワークを参照できる構造へ発展させました。

NICE Work Roleを介したNCO人材フレームワークとの関係（解説書 7.2 より）

- 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、それぞれ目的と整理対象が異なりますが、共通してNICE Framework ComponentsのWork Roleを参照しています。NICE Work Roleを介して、企業に必要な役割と、その役割を担うために必要なTask、Knowledge及びSkillを相互に参照できます。

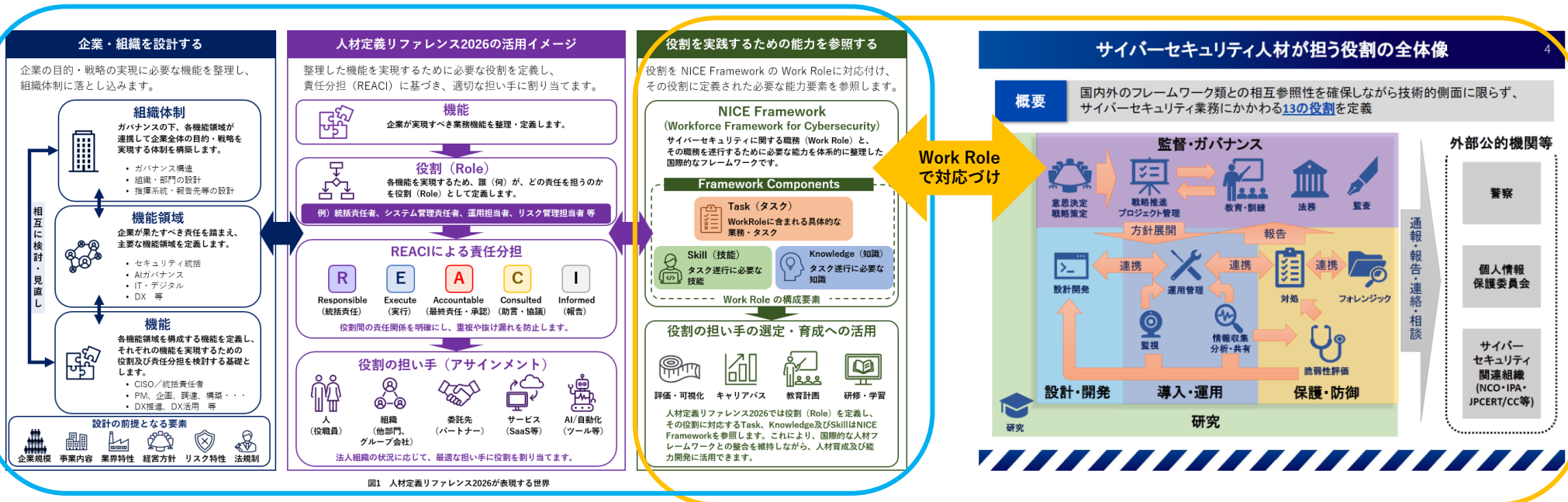


図1 人材定義リファレンス2026が表現する世界

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>

組織に必要な役割の整理と、その役割を担うために必要な能力の参照を、
NICE Work Roleを介してつなぐことができます。

今後の取組

- 今後検討したい事項

- ① 企業における活用事例及び実務上の課題の収集
- ② 組織設計、役割分担及び人材育成への適用方法の具体化
- ③ NICE Framework Componentsの更新内容の継続的な確認
- ④ AI、クラウド、OT・IoT等の環境変化を踏まえた見直し
- ⑤ NCO人材フレームワークとの関係及び活用方法の継続的な整理

人材定義リファレンス2026を完成形として固定するのではなく、
企業における活用と環境変化を踏まえ、継続的に検証・更新していきます。

参考資料②

人材定義リファレンス2026の活用方法

解説書 5. 人材定義リファレンス2026の活用方法

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. 人材定義リファレンス2026の活用方法

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。

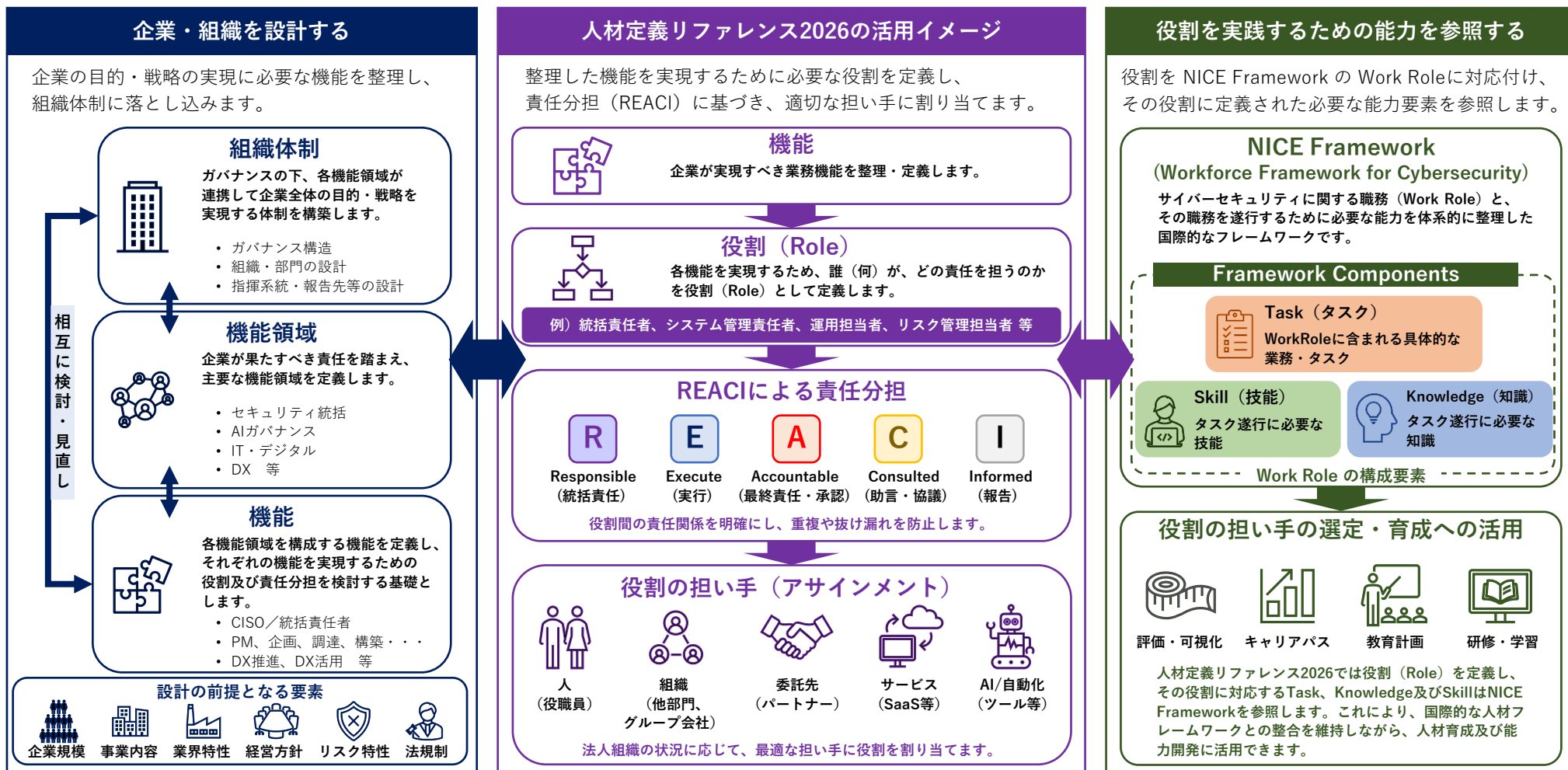


図1 人材定義リファレンス2026が表現する世界

5. 人材定義リファレンス2026の活用方法

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

設計の前提となる要素



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. 人材定義リファレンス2026の活用方法

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



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. 人材定義リファレンス2026の活用方法

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. 人材定義リファレンス2026の活用方法

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