人材定義リファレンス2026 v1.0

権限・責任の分担【凡例】		
	R：Responsible（統括）	実行責任者（複数配置可）
	E：Execute（実行）	実務者（複数配置可）
	A：Accountable（最終責任・承認）	最終責任者（1名）
	C：Consulted（助言・協議）	知見・支援（複数配置可）
	I：Informed（報告）	通知・通達を受ける（複数配置可）

■ セキュリティ統括室等に基づくNICEフレームワーク・マッピング

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。

			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
Work Role	Work Role Description		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。	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。
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）		C（助言）						R（統括）				E（実行）	E（実行）			I（報告）	I（報告）	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）		C（助言）	C（助言）	C（助言）								C（助言）		I（報告）	I（報告）	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）	R（統括） E（実行）		C（助言）	E（実行）	C（助言）	E（実行）			E（実行）				C（助言）	E（実行）	I（報告）	I（報告）	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）	R（統括） E（実行）		C（助言）	E（実行）			C（助言）					C（助言）	E（実行）	I（報告）	I（報告）	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）	R（統括） E（実行）		C（助言）	E（実行）			C（助言）						E（実行）	I（報告）	I（報告）	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）			E（実行）	C（助言）	E（実行）											E（実行）	E（実行）	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）			E（実行）	C（助言）	C（助言）	C（助言）								C（助言）		C（助言）		
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）	C（助言）	C（助言）	E（実行）										E（実行）	E（実行）	
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）	C（助言）		C（助言）	E（実行）	A（承認）	R（統括） A（承認）	R（統括）				E（実行）	E（実行）	C（助言）	E（実行）		
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）	C（助言）		C（助言）	E（実行）	A（承認）	R（統括） A（承認）	R（統括）	E（実行）	E（実行）	E（実行）			E（実行）	C（助言）		E（実行）	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）				C（助言）	E（実行）		C（助言）	R（統括）	E（実行）	E（実行）	E（実行）			C（助言）	C（助言）			
Security Control Assessment	Responsible for conducting independent comprehensive assessments of management, operational, and technical security controls and control enhancements employed within or inherited by a system to determine their overall effectiveness.	システム内で採用または継承された管理上、運用上、技術上のセキュリティ制御および制御強化策について、その総合的な有効性を判断するための独立した包括的評価を実施する責任を負う。	OG-WRL-012	612	A（承認）	R（統括）	E（実行）	C（助言）	E（実行）		E（実行）			C（助言）		C（助言）							I（報告）	I（報告）
Systems Authorization	Responsible for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the nation.	組織の業務、組織資産、個人、他組織、国家に対する許容可能なリスクレベルで情報システムを運用する責任を負う。	OG-WRL-013	611		C（助言）			C（助言）	E（実行）		A（承認）	R（統括）	R（統括）			E（実行）	E（実行）		E（実行）		C（助言）		
Systems Security Management	Responsible for managing the cybersecurity of a program, organization, system, or enclave.	プログラム、組織、システム、または特定領域のサイバーセキュリティを管理する責任を負う。	OG-WRL-014	722	A（承認）	R（統括）	R（統括）	R（統括）	R（統括）		C（助言）			C（助言）	R（統括）	E（実行）	E（実行）	E（実行）	E（実行）	E（実行）	E（実行）	C（助言）			
Technology Portfolio Management	Responsible for managing a portfolio of technology investments that align with the overall needs of mission and enterprise priorities.	ミッション全体と企業の優先事項のニーズに沿った技術投資のポートフォリオを管理する責任を負う。	OG-WRL-015	804		C（助言）				C（助言）	E（実行）	A（承認）	R（統括）	R（統括）	E（実行）		E（実行）			E（実行）	C（助言）	C（助言）		
Technology Program Auditing	Responsible for conducting evaluations of technology programs or their individual components to determine compliance with published standards.	公表された基準への準拠を判断するため、技術プログラムまたはその個別コンポーネントの評価を実施する責任を負う。	OG-WRL-016	805	A（承認）	R（統括）	C（助言）	C（助言）			E（実行）			C（助言）		C（助言）							I（報告）	C（助言）
Cybersecurity Supply Chain Risk Management	Responsible for developing cybersecurity supply chain risk management (C-SCRM) policies, processes, and procedures to identify, assess, protect against, and respond to cybersecurity risks throughout the supply chain, and for advising other stakeholders within an enterprise about supply chain risks.	サプライチェーン全体におけるサイバーセキュリティリスクを特定、評価、防御、および対応するためのサイバーセキュリティ・サプライチェーン・リスク管理（C-SCRM）の方針、プロセス、および手順の策定を担当するとともに、企業内の他のステークホルダーに対してサプライチェーンリスクに関する助言を行う。	OG-WRL-017	TBD	A（承認）	R（統括）	C（助言）	C（助言）	C（助言）	R（統括）	E（実行）	C（助言）		C（助言）	C（助言）	C（助言）	R（統括） E（実行）	E（実行）	E（実行）		C（助言）		I（報告）	I（報告）	C（助言）

人材定義リファレンス2026 v1.0

権限・責任の分担【凡例】		
	R：Responsible（統括）	実行責任者（複数配置可）
	E：Execute（実行）	実務者（複数配置可）
	A：Accountable（最終責任・承認）	最終責任者（1名）
	C：Consulted（助言・協議）	知見・支援（複数配置可）
	I：Informed（報告）	通知・通達を受ける（複数配置可）

■ セキュリティ統括室等に基づくNICEフレームワーク・マッピング

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。

					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
Work Role	Work Role Description		Work Role ID	OPM Code (Fed Use)	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。
DESIGN and DEVELOPMENT (DD) – Conducts research, conceptualizes, designs, develops, and tests secure technology systems, including on perimeter and cloud-based networks.																									
Cybersecurity Architecture	Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems that protect and support organizational mission and business processes.	参照モデル、セグメントおよびソリューションアーキテクチャ、ならびに組織のミッションと業務プロセスを保護・支援する結果として生じるシステムを含む、エンタープライズアーキテクチャのあらゆる側面において、セキュリティ要件が適切に考慮されていることを保証する責任を負う。	DD-WRL-001	652	A（承認）		C（助言）				C（助言）	C（助言）		C（助言）	R（統括）	E（実行）	E（実行）	E（実行）				C（助言）	C（助言）	I（報告）	I（報告）	C（助言）
Enterprise Architecture	Responsible for developing and maintaining business, systems, and information processes to support enterprise mission needs. Develops technology rules and requirements that describe baseline and target architectures.	エンタープライズミッションのニーズを支援するための業務、システム、情報プロセスの開発および維持を担当する。ベースラインおよびターゲットアーキテクチャを記述する技術ルールと要件を開発する。	DD-WRL-002	651		C（助言）	C（助言）	C（助言）			C（助言）	E（実行）	A（承認）	R（統括） A（承認）	R（統括）	E（実行）	E（実行）	E（実行）				E（実行）	C（助言）	I（報告）	I（報告）	C（助言）
Secure Software Development	Responsible for developing, creating, modifying, and maintaining computer applications, software, or specialized utility programs.	コンピューターアプリケーション、ソフトウェア、または専用ユーティリティプログラムの開発、作成、変更、保守を担当する。	DD-WRL-003	621			C（助言）				C（助言）	E（実行）	A（承認）	R（統括）	R（統括）	E（実行）		E（実行）	E（実行）	E（実行）	E（実行）	C（助言）	E（実行）	I（報告）	I（報告）	I（報告）
Secure Systems Development	Responsible for the secure design, development, and testing of systems and the evaluation of system security throughout the systems development life cycle.	システム開発ライフサイクル全体を通じた、システムの安全な設計、開発、テスト、およびシステムセキュリティの評価を担当する。	DD-WRL-004	631 and 632			C（助言）	C（助言）			C（助言）	E（実行）	A（承認）	R（統括）	R（統括）	E（実行）	E（実行）	E（実行）	E（実行）	E（実行）		C（助言）	E（実行）			C（助言）
Software Security Assessment	Responsible for analyzing the security of new or existing computer applications, software, or specialized utility programs and delivering actionable results.	新規または既存のコンピューターアプリケーション、ソフトウェア、または専用ユーティリティプログラムのセキュリティを分析し、実行可能な結果を提供することを担当する。	DD-WRL-005	622	A（承認）		R（統括）	R（統括）			E（実行）			C（助言）	C（助言）	C（助言）										
Systems Requirements Planning	Responsible for consulting with internal and external customers to evaluate and translate functional requirements and integrating security policies into technical solutions.	内部および外部の顧客と協議し、機能要件を評価・翻訳するとともに、セキュリティポリシーを技術的解決策に統合する責任を負う。	DD-WRL-006	641		C（助言）	C（助言）	C（助言）			C（助言）	C（助言）	A（承認）	R（統括） A（承認）	R（統括）	E（実行）	C（助言）	E（実行）	C（助言）			E（実行）	C（助言）			C（助言）
Systems Testing and Evaluation	Responsible for planning, preparing, and executing system tests; evaluating test results against specifications and requirements; and reporting test results and findings.	システムテストの計画、準備、実行、仕様および要件に対するテスト結果の評価、ならびにテスト結果と発見事項の報告を担当する。	DD-WRL-007	671			C（助言）	R（統括）			E（実行）		A（承認）	R（統括） A（承認）	R（統括）	C（助言）		C（助言）		E（実行）	E（実行）		C（助言）			
Technology Research and Development	Responsible for conducting software and systems engineering and software systems research to develop new capabilities with fully integrated cybersecurity. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.	完全に統合されたサイバーセキュリティを備えた新機能の開発に向け、ソフトウェアおよびシステムエンジニアリングならびにソフトウェアシステム研究を実施する責任を負う。サイバースペースシステムにおける潜在的な脆弱性を評価するための包括的な技術研究を実施する。	DD-WRL-008	661	A（承認）			R（統括）			C（助言）	E（実行）		C（助言）	R（統括）	C（助言）		E（実行）				E（実行）	C（助言）			
Operational Technology (OT) Cybersecurity Engineering	Responsible for working within the engineering department to design and create systems, processes, and procedures that maintain the safety, reliability, controllability, and security of industrial systems in the face of intentional and incidental cyber-related events. Interfaces with Chief Information Security Officer, plant managers, and industrial cybersecurity technicians.	エンジニアリング部門内で、意図的・偶発的なサイバー関連事象に直面しても産業システムの安全性、信頼性、制御性、セキュリティを維持するシステム・プロセス・手順の設計・構築を担当。最高情報セキュリティ責任者（CISO）、工場管理者、産業サイバーセキュリティ技術者と連携する。	DD-WRL-009	TBD		C（助言）	R（統括）	C（助言）			C（助言）	C（助言）	A（承認）	R（統括） A（承認）	R（統括）	E（実行）	C（助言）		C（助言）			C（助言）	E（実行）			
IMPLEMENTATION and OPERATION (IO) – Provides implementation, administration, configuration, operation, and maintenance to ensure effective and efficient technology system performance and security.																									
Data Analysis	Responsible for analyzing data from multiple disparate sources to provide cybersecurity and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.	複数の異なるソースからのデータを分析し、サイバーセキュリティとプライバシーに関する洞察を提供する責任を負う。モデリング、データマイニング、研究目的で使用される複雑な企業規模のデータセット向けに、カスタムアルゴリズム、ワークフロープロセス、レイアウトを設計・実装する。	IO-WRL-001	422		C（助言）	R（統括）	C（助言）			C（助言）	E（実行）	A（承認）	R（統括） A（承認）	R（統括）	E（実行）						C（助言）	E（実行）		I（報告）	I（報告）
Database Administration	Responsible for administering databases and data management systems that allow for the secure storage, query, protection, and utilization of data.	データの安全な保存、クエリ、保護、利用を可能にするデータベースおよびデータ管理システムの管理を担当する。	IO-WRL-002	421		C（助言）		C（助言）			C（助言）		A（承認）	R（統括） A（承認）	R（統括）	E（実行）						C（助言）			I（報告）	I（報告）
Knowledge Management	Responsible for managing and administering processes and tools to identify, document, and access an organization's intellectual capital.	組織の知的資本を特定・文書化・アクセスするためのプロセスとツールの管理・運用を担当。	IO-WRL-003	431	A（承認）			R（統括）	C（助言）	I（報告）	C（助言）	E（実行）		R（統括）								E（実行）	E（実行）			I（報告）
Network Operations	Responsible for planning, implementing, and operating network services and systems, including hardware and virtual environments.	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、運用を担当。	IO-WRL-004	441		C（助言）		C（助言）					A（承認）	R（統括） A（承認）	R（統括）					C（助言）	E（実行）	C（助言）			I（報告）	I（報告）
Systems Administration	Responsible for setting up and maintaining a system or specific components of a system in adherence with organizational security policies and procedures. Includes hardware and software installation, configuration, and updates; user account management; backup and recovery management; and security control implementation.	組織のセキュリティポリシーと手順に準拠したシステムまたは特定コンポーネントの構築・保守を担当。ハードウェア・ソフトウェアのインストール、設定、更新、ユーザーアカウント管理、バックアップ・リカバリ管理、セキュリティ制御の実装を含む。	IO-WRL-005	451		C（助言）		C（助言）			C（助言）		A（承認）	R（統括） A（承認）	R（統括）	E（実行）				E（実行）	E（実行）	C（助言）	E（実行）		I（報告）	E（実行）
Systems Security Analysis	Responsible for developing and analyzing the integration, testing, operations, and maintenance of systems security. Prepares, performs, and manages the security aspects of implementing and operating a system.	システムセキュリティの統合、テスト、運用、保守の開発および分析を担当する。システムの実装および運用におけるセキュリティ面の準備、実施、管理を行う。	IO-WRL-006	461	A（承認）	C（助言）	C（助言）	R（統括）			E（実行）	C（助言）		C（助言）	R（統括）	E（実行）				E（実行）		C（助言）	C（助言）	I（報告）	I（報告）	E（実行） C（助言）
Technical Support	Responsible for providing technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational policies and processes.	確立または承認された組織の方針およびプロセスに従い、クライアントレベルのハードウェアおよびソフトウェアの利用支援を必要とする顧客への技術サポートを提供する責任を負う。	IO-WRL-007	411		C（助言）					C（助言）	C（助言）	A（承認）	R（統括） A（承認）	R（統括）	C（助言）					E（実行）		E（実行）		I（報告）	I（報告）

人材定義リファレンス2026 v1.0

権限・責任の分担【凡例】	
R：Responsible（統括）	実行責任者（複数配置可）
E：Execute（実行）	実務者（複数配置可）
A：Accountable（最終責任・承認）	最終責任者（1名）
C：Consulted（助言・協議）	知見・支援（複数配置可）
I：Informed（報告）	通知・通達を受ける（複数配置可）

■ セキュリティ統括室等に基づくNICEフレームワーク・マッピング

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。

					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
Work Role	Work Role Description		Work Role ID	OPM Code (Fed Use)	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。	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つつ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。
PROTECTION and DEFENSE (PD) – Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.																									
Defensive Cybersecurity	Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks.	リスク軽減のため、様々なサイバーセキュリティ防御ツールから収集したデータの分析を担当する。	PD-WRL-001	511	A（承認）		C（助言）	R（統括）			C（助言）	C（助言）												I（報告）	I（報告）
Digital Forensics	Responsible for analyzing digital evidence from computer security incidents to derive useful information in support of system and network vulnerability mitigation.	コンピュータセキュリティインシデントからのデジタル証拠を分析し、システムおよびネットワークの脆弱性軽減を支援する有用な情報を導出する責任を負う。	PD-WRL-002	212	A（承認）			R（統括）			C（助言）												C（助言）	I（報告）	I（報告）
Incident Response	Responsible for investigating, analyzing, and responding to network cybersecurity incidents.	ネットワークサイバーセキュリティインシデントの調査、分析、対応を担当する。	PD-WRL-003	531	A（承認）		C（助言）	R（統括）			E（実行）	C（助言）		C（助言）		C（助言）	C（助言）					C（助言）	C（助言）	I（報告）	C（助言）
Infrastructure Support	Responsible for testing, implementing, deploying, maintaining, and administering infrastructure hardware and software for cybersecurity.	サイバーセキュリティのためのインフラストラクチャハードウェアおよびソフトウェアのテスト、実装、展開、保守、管理を担当する。	PD-WRL-004	521	A（承認）		C（助言）	C（助言）			C（助言）				R（統括）		C（助言）			E（実行）	E（実行）	C（助言）	C（助言）		I（報告）	C（助言）
Insider Threat Analysis	Responsible for identifying and assessing the capabilities and activities of cybersecurity insider threats; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations.	サイバーセキュリティ内部脅威の能力と活動を特定・評価する責任を負う。法執行機関および防諜活動・調査の開始と支援に役立つ調査結果を生産する。	PD-WRL-005	TBD	A（承認）	C（助言）		R（統括）			E（実行）	C（助言）		C（助言）		C（助言）							C（助言）		
Threat Analysis	Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment.	サイバーセキュリティ脅威評価の収集、処理、分析、および普及を担当する。高度に動的な運用環境の状況を把握するためのサイバーセキュリティ指標を開発する。	PD-WRL-006	141	A（承認）	C（助言）	C（助言）	R（統括）			E（実行）	C（助言）										C（助言）		I（報告）	I（報告）
Vulnerability Analysis	Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.	システムおよびネットワークを評価し、許容可能な構成、エンクレーブポリシー、またはローカルポリシーからの逸脱を特定する責任を負う。既知の脆弱性に対する多重防御アーキテクチャの効果を測定する。	PD-WRL-007	541	A（承認）		C（助言）	R（統括）			E（実行）	C（助言）									C（助言）	C（助言）		I（報告）	I（報告）	C（助言）
INVESTIGATION (IN) – Collects, processes, analyzes, and disseminates information from all sources of intelligence on foreign actors' cyberspace programs, intentions, capabilities, research and development, and operational activities																									
Cybercrime Investigation	Responsible for investigating cyberspace intrusion incidents and crimes. Applies tactics, techniques, and procedures for a full range of investigative tools and processes and appropriately balances the benefits of prosecution versus intelligence gathering.	サイバー空間への侵入インシデントや犯罪の調査を担当する。あらゆる調査ツールやプロセスに対する戦術、手法、手順を適用し、起訴による利益と情報収集の利益との適切なバランスを図る。	IN-WRL-001	221	A（承認）	C（助言）		R（統括）			E（実行）	C（助言）		C（助言）		C（助言）						C（助言）	C（助言）	I（報告）	I（報告）
Digital Evidence Analysis	Responsible for identifying, collecting, examining, and preserving digital evidence using controlled and documented analytical and investigative techniques.	管理された文書化された分析・調査技術を用いて、デジタル証拠の特定、収集、検証、保存を担当。	IN-WRL-002	211	A（承認）	C（助言）		R（統括）			E（実行）	C（助言）		C（助言）		C（助言）					C（助言）			C（助言）	I（報告）	C（助言）