NISTサイバーセキュリティフレームワーク V1.1およびV2差分表

統制（GV）

V1.1				V2.0			
カテゴリー	サブカテゴリー	サブカテゴリー詳細	V2でのサブカテゴリー	サブカテゴリー	サブカテゴリー詳細	V1.1からの引継ぎ	新件・見直し項目
組織的文脈（GV.OC）							
	V2新規サブカテゴリー			GV.OC-01	組織のミッションが理解され、サイバーセキュリティリスクマネジメントについて伝えている		✓
	V2新規サブカテゴリー			GV.OC-02	内部と外部の利害関係者が理解され、サイバーセキュリティリスクマネジメントに関するそれら利害関係者のニーズと期待事項が理解及び、考慮されている		✓
	V2新規サブカテゴリー			GV.OC-03	サイバーセキュリティに関する法的要求事項、規制上の要求事項、契約上の要求事項（プライバシーと市民的自由の義務を含む）が理解、管理されている		✓
	V2新規サブカテゴリー			GV.OC-04	外部の利害関係者が組織に依存または期待する重要な目的、能力、サービスが理解、周知されている		✓
	V2新規サブカテゴリー			GV.OC-05	組織が依存する成果、能力、サービスが理解、周知されている		✓
リスクマネジメント戦略（GV.RM）							
	V2新規サブカテゴリー			GV.RM-01	リスクマネジメントの目的が確立され、組織の利害関係者によって合意されている		✓
	V2新規サブカテゴリー			GV.RM-02	リスク選好度とリスク許容度に関する表明が確立、周知、維持されている		✓
	V2新規サブカテゴリー			GV.RM-03	サイバーセキュリティリスクマネジメントの活動と成果が企業リスクマネジメントプロセスに含まれている		✓
	V2新規サブカテゴリー			GV.RM-04	適切なリスク対応オプションを表す戦略的方向性が確立、周知されている		✓
	V2新規サブカテゴリー			GV.RM-05	サプライヤーおよび他の第三者からのリスクを含め、サイバーセキュリティリスクに関するコミュニケーション系統が組織全体にわたり確立されている		✓
	V2新規サブカテゴリー			GV.RM-06	サイバーセキュリティリスクの計算、文書化、分類、優先順位付けのための標準化された方法が確立、周知されている		✓
	V2新規サブカテゴリー			GV.RM-07	戦略的機会（プラスの効果をもたらすリスク）が特徴付けられ、組織のサイバーセキュリティリスクに関する議論に含まれている		✓
サイバーセキュリティサプライチェーンリスクマネジメント（GV.SC）							
	V2新規サブカテゴリー			GV.SC-01	サイバーセキュリティサプライチェーンリスクマネジメントのプログラム、戦略、目的、ポリシー、プロセスが組織の利害関係者によって確立、合意されている		✓
	V2新規サブカテゴリー			GV.SC-02	サプライヤー、顧客、パートナーがサイバーセキュリティに関して負う役割と責任が確立、周知され、内部と外部で調整が図られている		✓
	V2新規サブカテゴリー			GV.SC-03	サイバーセキュリティサプライチェーンリスクマネジメントが、サイバーセキュリティと企業におけるリスクマネジメント、リスクアセスメント、改善のプロセスに統合されている		✓
	V2新規サブカテゴリー			GV.SC-04	サプライヤーが把握され、重要性に応じて優先順位が付けられている		✓
	V2新規サブカテゴリー			GV.SC-05	サプライチェーンにおけるサイバーセキュリティリスクに対処するための要求事項が確立され、優先順位が付けられ、サプライヤーおよびその他の関連する第三者との契約や他の種類の合意に統合されている		✓
	V2新規サブカテゴリー			GV.SC-06	サプライヤーまたは他の第三者との正式な関係を締結する前に、リスクを低減するための計画作成と適正評価が実行されている		✓
	V2新規サブカテゴリー			GV.SC-07	サプライヤー、それらの製品やサービス、他の第三者によってもたらされるリスクが理解、記録、優先順位付け、評価され、それらの当事者との関係の全過程にわたりモニタリングされている		✓
	V2新規サブカテゴリー			GV.SC-08	関連するサプライヤーおよび他の第三者がインシデントの計画作成、対応、復旧活動に含まれている		✓
	V2新規サブカテゴリー			GV.SC-09	サプライチェーンセキュリティプラクティスがサイバーセキュリティと企業のリスクマネジメントプログラムに統合され、それらの実施状況が技術製品やサービスのライフサイクル全体にわたりモニタリングされている		✓
	V2新規サブカテゴリー			GV.SC-10	サイバーセキュリティサプライチェーンリスクマネジメント計画において、パートナーシップまたはサービス合意の締結後に発生する活動に関する規定が含まれている		✓
役割／責任／権限（GV.RR）							
	V2新規サブカテゴリー			GV.RR-01	サイバーセキュリティリスクについて組織の指導者が責任と説明責任を負い、リスクを意識した、倫理的で継続的な改善に取り組む文化の醸成が促進されている		✓
	V2新規サブカテゴリー			GV.RR-02	サイバーセキュリティリスクマネジメントに関連する役割／責任／権限が確立、周知、理解、執行されている		✓
	V2新規サブカテゴリー			GV.RR-03	サイバーセキュリティリスクに関する戦略／役割／責任／ポリシーと一致する適切な資源が配分されている		✓
	V2新規サブカテゴリー			GV.RR-04	サイバーセキュリティが人事プラクティスに含まれている		✓
ポリシー（GV.PO）							
	V2新規サブカテゴリー			GV.PO-01	サイバーセキュリティリスクを管理するためのポリシーが組織的文脈、サイバーセキュリティ戦略、優先事項に基づいて確立、周知、執行されている		✓
	V2新規サブカテゴリー			GV.PO-02	サイバーセキュリティリスクを管理するためのポリシーが要求事項、脅威、技術、組織のミッションの変化を反映する形でレビュー、更新、周知、執行されている		✓

NISTサイバーセキュリティフレームワーク V1.1およびV2差分表

統制（GV）

	V1.1			V2.0			
カテゴリー	サブカテゴリー	サブカテゴリー詳細	V2でのサブカテゴリー	サブカテゴリー	サブカテゴリー詳細	V1.1からの引継ぎ	新件・見直し項目
監督（GV.OV）							
	V2新規サブカテゴリー			GV.OV-01	サイバーセキュリティリスクマネジメント戦略の成果がレビューされ、戦略と方向性を調整するための情報源として利用されている		✓
	V2新規サブカテゴリー			GV.OV-02	サイバーセキュリティリスクマネジメント戦略がレビューされ、組織の要求事項とリスクを確実にカバーするよう調整されている		✓
	V2新規サブカテゴリー			GV.OV-03	組織のサイバーセキュリティリスクマネジメントの実績が、必要な調整のために評価、レビューされている		✓

NISTサイバーセキュリティフレームワーク V1.1およびV2差分表

特定（ID）

	V1.1			V2.0			
カテゴリー	サブカテゴリー	サブカテゴリー詳細	V2でのサブカテゴリー	サブカテゴリー	サブカテゴリー詳細	V1.1からの引継ぎ	新件・見直し項目
資産管理（ID.AM）							
	ID.AM-1	企業内の物理デバイスとシステムの一覧を作成している	ID.AM-01	ID.AM-01	組織が管理するハードウェアの目録（インベントリ）が維持されている	✓	
	ID.AM-2	企業内のソフトウェアプラットフォームとアプリケーションの一覧を作成している	ID.AM-02	ID.AM-02	組織が管理するソフトウェア、サービス、システムの目録（インベントリ）が維持されている	✓	
	ID.AM-3	企業内の通信とデータの流れの図を用意している	ID.AM-03	ID.AM-03	組織が認可したネットワーク通信および内部と外部のネットワークデータフローの表明が維持されている	✓	
	ID.AM-4	外部情報システムの一覧を作成している	ID.AM-04	ID.AM-04	サプライヤーが提供するサービスの目録（インベントリ）が維持されている	✓	
	ID.AM-5	リソース（例：ハードウェア、デバイス、データ、ソフトウェア）を、分類、重要度、ビジネス上の価値に基づいて優先順位付けしている	ID.AM-05	ID.AM-05	資産の優先順位が、分類、重要性、リソース、ミッションに対する影響に基づいて決められている	✓	
	ID.AM-6	すべての従業員と第三者である利害関係者（例：供給業者、顧客、パートナー）に対して、サイバーセキュリティ上の役割と責任を定めている	GV.RR-02, GV.SC-02	ID.AM-06	Not Applicable		
		V2新規サブカテゴリー		ID.AM-07	指定されたデータ型のデータとそれに呼応するメタデータの目録（インベントリ）が維持されている		✓
		V2新規サブカテゴリー		ID.AM-08	システム、ハードウェア、ソフトウェア、サービス、データが、それらのライフサイクル全体にわたり管理されている		✓
ビジネス環境（ID.BE）							
	ID.BE-1	サプライチェーンにおける企業の役割を特定、伝達している	GV.OC-05	ID.BE-01	Not Applicable		
	ID.BE-2	重要インフラとその産業分野における企業の位置付けを特定、伝達している	GV.OC-01	ID.BE-02	Not Applicable		
	ID.BE-3	企業のミッション、目標、活動に関して優先順位を定義、伝達している	GV.OC-01	ID.BE-03	Not Applicable		
	ID.BE-4	重要サービスを提供する上での依存関係と重要な機能を把握している	GV.OC-04, GV.OC-05	ID.BE-04	Not Applicable		
	ID.BE-5	重要サービスの提供を支援する、レジリエンスに関する要求事項を定めている	GV.OC-04	ID.BE-05	Not Applicable		
ガバナンス（ID.GV）							
	ID.GV-1	自組織の情報セキュリティポリシーを定めている	GV.PO-01, GV.PO-02, GV.PO	ID.GV-01	Not Applicable		
	ID.GV-2	情報セキュリティ上の役割と責任について、内部と外部パートナーとで調整、連携している	GV.OC-02, GV.RR-02, GV.RR	ID.GV-02	Not Applicable		
	ID.GV-3	プライバシーや市民の自由に関する義務を含む、サイバーセキュリティに関する法規制上の要求事項を理解、管理している	GV.OC-03	ID.GV-03	Not Applicable		
	ID.GV-4	ガバナンスとリスク管理プロセスがサイバーセキュリティリスクに対応している	GV.RM-03	ID.GV-04	Not Applicable		
リスクアセスメント（ID.RA）							
	ID.RA-1	資産の脆弱性を特定、文書化している	ID.RA-01	ID.RA-01	資産における脆弱性が識別、検証、記録されている	✓	
	ID.RA-2	情報共有フォーラム／ソースより、脅威と脆弱性に関する情報を入手している	ID.RA-02	ID.RA-02	サイバー脅威インテリジェンスが情報共有フォーラムおよび情報源から寄せられている	✓	
	ID.RA-3	内外からの脅威を特定、文書化している	ID.RA-03	ID.RA-03	組織に対する内部と外部からの脅威が識別、記録されている	✓	
	ID.RA-4	ビジネスに対する潜在的な影響と、その可能性を特定している	ID.RA-04	ID.RA-04	脆弱性を利用する脅威の潜在的な影響と発生可能性が識別、記録されている	✓	
	ID.RA-5	リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮している	ID.RA-05	ID.RA-05	脅威、脆弱性、発生可能性、影響が、内在的なリスクの理解とリスク対応の優先順位付けに利用されている	✓	
	ID.RA-6	リスクに対する対応を定義、優先順位付けしている	ID.RA-06	ID.RA-06	リスク対応が選択、優先順位付け、計画、追跡、周知されている	✓	
		V2新規サブカテゴリー		ID.RA-07	変更と例外が管理され、リスクの影響について評価、記録、追跡されている		✓
		V2新規サブカテゴリー		ID.RA-08	脆弱性開示情報の受領、分析、対応のためのプロセスが確立されている		✓
		V2新規サブカテゴリー		ID.RA-09	ハードウェアとソフトウェアの真正性と完全性が調達と使用に先立って評価されている		✓
		V2新規サブカテゴリー		ID.RA-10	調達に先立って重要サプライヤーが評価されている		✓
リスク管理戦略（ID.RM）							
	ID.RM-1	リスク管理プロセスが自組織の利害関係者によって確立、管理、承認されている	GV.RM-01, GV.RM-06, GV.RR-03	ID.RM-01	Not Applicable		
	ID.RM-2	自組織のリスク許容度を決定し、明確にしている	GV.RM-02, GV.RM-04	ID.RM-02	Not Applicable		
	ID.RM-3	企業によるリスク許容度の決定が、重要インフラにおける自組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている	GV.RM-02	ID.RM-03	Not Applicable		

NISTサイバーセキュリティフレームワーク V1.1およびV2差分表

特定（ID）

	V1.1			V2.0			
カテゴリー	サブカテゴリー	サブカテゴリー詳細	V2でのサブカテゴリー	サブカテゴリー	サブカテゴリー詳細	V1.1からの引継ぎ	新件・見直し項目
サプライチェーンリスクマネジメント（ID.SC）							
	ID.SC-1	サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別、定義、評価、管理、承認されている	GV.RM-05, GV.SC-01, GV.SC-06, GV.SC-09, GV.SC-10	ID.SC-01	Not Applicable		
	ID.SC-2	情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが識別、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている	GV.OC-02, GV.SC-03, GV.SC-04, GV.SC-07, ID.RA-10	ID.SC-02	Not Applicable		
	ID.SC-3	サプライヤーおよび第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている	GV.SC-05	ID.SC-03	Not Applicable		
	ID.SC-4	サプライヤーおよび第三者であるパートナーが監査、テストの結果、またはその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている	GV.SC-07, ID.RA-10	ID.SC-04	Not Applicable		
	ID.SC-5	対応・復旧計画の策定とテストが、サプライヤーおよび第三者プロバイダーとともに行なわれている	GV.SC-08, ID.IM-02	ID.SC-05	Not Applicable		
改善（ID.IM）							
		V2新規サブカテゴリー		ID.IM-01	改善が評価を基に識別されている		✓
		V2新規サブカテゴリー		ID.IM-02	サプライヤーや関連する第三者と調整の上で行われるものを含め、セキュリティテストと演習から改善点が識別されている		✓
		V2新規サブカテゴリー		ID.IM-03	運用のプロセス、手順、活動の実行から改善点が識別されている		✓
		V2新規サブカテゴリー		ID.IM-04	運用に影響を及ぼすインシデントへの対応計画および他のサイバーセキュリティ計画が確立、周知、維持、改善されている		✓

NISTサイバーセキュリティフレームワーク V1.1およびV2差分表

防御（PR）

	V1.1			V2.0			
カテゴリー	サブカテゴリー	サブカテゴリー詳細	V2でのサブカテゴリー	サブカテゴリー	サブカテゴリー詳細	V1.1からの引継ぎ	新件・見直し項目
アイデンティティ管理／認証／アクセス制御（PR.AA）							
	V2新規サブカテゴリー			PR.AA-01	認可されたユーザ、サービス、ハードウェアのアイデンティティと証明書が組織によって管理されている		✓
	V2新規サブカテゴリー			PR.AA-02	アイデンティティが証明され、相互作用の文脈に基づく証明書に限定されている		✓
	V2新規サブカテゴリー			PR.AA-03	ユーザ、サービス、ハードウェアの認証が行われている		✓
	V2新規サブカテゴリー			PR.AA-04	IDアサーションが保護、周知、検証されている		✓
	V2新規サブカテゴリー			PR.AA-05	アクセス許可、資格の付与および認証がポリシーにおいて定義、管理、執行、レビューされ、最小権限の原則と職務の分離の原則を組み入れている		✓
	V2新規サブカテゴリー			PR.AA-06	資産への物理的アクセスがリスクと整合的に管理、モニタリング、執行されている		✓
アクセス制御（PR.AC）							
	PR.AC-1	承認されたデバイスとユーザの識別情報および認証情報を管理している	PR.AA-01, PR.AA-05	PR.AC-01	Not Applicable		
	PR.AC-2	資産に対する物理アクセスを管理、保護している	PR.AA-06	PR.AC-02	Not Applicable		
	PR.AC-3	リモートアクセスを管理している	PR.AA-03, PR.AA-05, PR.IR-01	PR.AC-03	Not Applicable		
	PR.AC-4	最小権限および職務の分離の原則を取り入れて、アクセス権限を管理している	PR.AA-05	PR.AC-04	Not Applicable		
	PR.AC-5	適宜、ネットワークの分離を行って、ネットワークの完全性を保護している	PR.IR-01	PR.AC-05	Not Applicable		
	PR.AC-6	IDは、ID利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで使用されている	PR.AA-02	PR.AC-06	Not Applicable		
	PR.AC-7	ユーザ、デバイス、その他の資産は、トランザクションのリスク（例：個人のセキュリティおよびプライバシー上のリスク、その他組織にとってのリスク）の度合いに応じた認証（例：一要素、多要素）が行われている	PR.AA-03	PR.AC-07	Not Applicable		
意識向上およびトレーニング（PR.AT）							
	PR.AT-1	すべてのユーザに情報を周知し、トレーニングを実施している	PR.AT-01	PR.AT-01	人員は、サイバーセキュリティリスクを念頭に置きながら一般的な職務を遂行するための知識とスキルを持てるよう、意識向上とトレーニングを受けている	✓	
	PR.AT-2	権限を持つユーザが役割と責任を理解している	PR.AT-02	PR.AT-02	特殊な役割を担う個人は、サイバーセキュリティリスクを念頭に置きながら関連職務を遂行するための知識とスキルを持てるよう、意識を向上させ、トレーニングを受けている	✓	
	PR.AT-3	第三者である利害関係者（例：供給業者、顧客、パートナー）が役割と責任を理解している	PR.AT-01, PR.AT-02	PR.AT-03	Not Applicable		
	PR.AT-4	上級役員が役割と責任を理解している	PR.AT-02	PR.AT-04	Not Applicable		
	PR.AT-5	物理セキュリティおよび情報セキュリティの担当者が役割と責任を理解している	PR.AT-02	PR.AT-05	Not Applicable		
データセキュリティ（PR.DS）							
	PR.DS-1	保存されているデータを保護している	PR.DS-01	PR.DS-01	保存されているデータの機密性、完全性、可用性が保護されている	✓	
	PR.DS-2	伝送中のデータを保護している	PR.DS-02	PR.DS-02	伝送中のデータの機密性、完全性、可用性が保護されている	✓	
	PR.DS-3	資産について撤去、譲渡、廃棄プロセスを正式に管理している	ID.AM-08, PR.PS-03	PR.DS-03	Not Applicable		
	PR.DS-4	可用性を確保するのに十分な容量を保持している	PR.IR-04	PR.DS-04	Not Applicable		
	PR.DS-5	データ漏えいに対する保護対策を実施している	PR.DS-01, PR-DS-02, PR.DS-10	PR.DS-05	Not Applicable		
	PR.DS-6	ソフトウェア、ファームウェア、情報の完全性の検証に、完全性チェックメカニズムを使用している	PR.DS-01, DE.CM-09	PR.DS-06	Not Applicable		
	PR.DS-7	開発・テスト環境を実稼働環境から分離している	PR.IR-01	PR.DS-07	Not Applicable		
	PR.DS-8	完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている	ID.RA-09, DE.CM-09	PR.DS-08	Not Applicable		
	V2新規サブカテゴリー			PR.DS-10	使用中のデータの機密性、完全性、可用性が保護されている		✓
	V2新規サブカテゴリー			PR.DS-11	データのバックアップが作成、保護、維持、テストされている		✓

NISTサイバーセキュリティフレームワーク V1.1およびV2差分表

防御（PR）

	V1.1			V2.0			
カテゴリー	サブカテゴリー	サブカテゴリー詳細	V2でのサブカテゴリー	サブカテゴリー	サブカテゴリー詳細	V1.1からの引継ぎ	新件・見直し項目
情報を保護するためのプロセスおよび手順（PR.IP）							
	PR.IP-1	情報技術／産業用制御システムのベースラインとなる設定を定め、維持している	PR.PS-01	PR.IP-01	Not Applicable		
	PR.IP-2	システムを管理するためのシステム開発ライフサイクルを導入している	ID.AM-08, PR.PS-06	PR.IP-02	Not Applicable		
	PR.IP-3	設定変更管理プロセスを導入している	PR.PS-01, ID.RA-07	PR.IP-03	Not Applicable		
	PR.IP-4	情報のバックアップを定期的に実施、保持し、テストしている	PR.DS-11	PR.IP-04	Not Applicable		
	PR.IP-5	自組織の資産の物理的な運用環境に関するポリシーと規制を満たしている	PR.IR-02	PR.IP-05	Not Applicable		
	PR.IP-6	ポリシーに従ってデータを破壊している	ID.AM-08	PR.IP-06	Not Applicable		
	PR.IP-7	保護プロセスを継続的に改善している	ID.IM-03, ID.IM	PR.IP-07	Not Applicable		
	PR.IP-8	保護技術の有効性について、適切なパートナーとの間で情報を共有している	ID.IM-03	PR.IP-08	Not Applicable		
	PR.IP-9	対応計画（インシデント対応および事業継続）と復旧計画（インシデントからの復旧および災害復旧）を実施、管理している	ID.IM-04	PR.IP-09	Not Applicable		
	PR.IP-10	対応計画と復旧計画をテストしている	ID.IM-02, ID.IM-04	PR.IP-10	Not Applicable		
	PR.IP-11	人事に関わる対策にサイバーセキュリティ（例：アクセス権限の無効化、従業員に対する審査）を含めている	GV.RR-04	PR.IP-11	Not Applicable		
	PR.IP-12	脆弱性管理計画を作成、実施している	ID.RA-01, PR.PS-02	PR.IP-12	Not Applicable		
保守（PR.MA）							
	PR.MA-1	自組織の資産の保守と修理は、承認・管理されたツールを用いてタイムリーに実施し、ログを記録している	ID.AM-08, PR.PS-03	PR.MA-01	Not Applicable		
	PR.MA-2	自組織の資産に対する遠隔保守は、承認を得てログを記録し、不正アクセスを防げる形で実施している	ID.AM-08, PR.PS-02	PR.MA-02	Not Applicable		
保護技術（PR.PT）							
	PR.PT-1	ポリシーに従って監査記録／ログ記録の対象を決定、文書化、記録、レビューしている	PR.PS-04	PR.PT-01	Not Applicable		
	PR.PT-2	ポリシーに従って取り外し可能な外部記録媒体を保護し、使用を制限している	PR.DS-01, PR.PS-01	PR.PT-02	Not Applicable		
	PR.PT-3	最小機能の原則を取り入れて、システムと資産に対するアクセスを制御している	PR.PS-01	PR.PT-03	Not Applicable		
	PR.PT-4	通信ネットワークと制御ネットワークを保護している	PR.AA-06, PR.IR-01	PR.PT-04	Not Applicable		
	PR.PT-5	メカニズム（例：フェールセーフ、ロードバランシング、ホットスワップ）が、平時および緊急時においてレジリエンスに関する要求事項を達成するために実装されている	PR.IR-03	PR.PT-05	Not Applicable		
プラットフォームセキュリティ（PR.PS）							
		V2新規サブカテゴリー		PR.PS-01	構成設定管理プラクティスが確立、適用されている		✓
		V2新規サブカテゴリー		PR.PS-02	ソフトウェアは、リスクと整合的に維持、代替、削除されている		✓
		V2新規サブカテゴリー		PR.PS-03	ハードウェアは、リスクと整合的に維持、代替、削除されている		✓
		V2新規サブカテゴリー		PR.PS-04	ログ記録が生成され、継続的モニタリング向けに利用可能な状態にされている		✓
		V2新規サブカテゴリー		PR.PS-05	未認可のソフトウェアのインストールや実行が防止されている		✓
		V2新規サブカテゴリー		PR.PS-06	セキュアなソフトウェア開発プラクティスが統合され、ソフトウェア開発のライフサイクル全体にわたりそれらのパフォーマンスがモニタリングされている		✓
技術インフラのレジリエンス（PR.IR）							
		V2新規サブカテゴリー		PR.IR-01	ネットワークと環境が未認可の論理アクセスと使用から保護されている		✓
		V2新規サブカテゴリー		PR.IR-02	組織の技術資産が環境的脅威から保護されている		✓
		V2新規サブカテゴリー		PR.IR-03	通常の状況と緊急時におけるレジリエンス要求事項を達成するためのメカニズムが実装されている		✓
		V2新規サブカテゴリー		PR.IR-04	可用性を確保するための適切なリソース容量が維持されている		✓

NISTサイバーセキュリティフレームワーク V1.1およびV2差分表

検知（DE）

	V1.1			V2.0			
カテゴリー	サブカテゴリー	サブカテゴリー詳細	V2でのサブカテゴリー	サブカテゴリー	サブカテゴリー詳細	V1.1からの引継ぎ	新件・見直し項目
異常とイベント（DE.AE）							
	DE.AE-1	ネットワーク運用のベースラインと、ユーザとシステム間の予測されるデータの流れを特定、管理している	ID.AM-03	DE.AE-01	Not Applicable		
	DE.AE-2	攻撃の標的と手法を理解するために、検知したイベントを分析している	DE.AE-02	DE.AE-02	付随する活動の理解を向上させるため、潜在的な有害イベントが分析されている	✓	
	DE.AE-3	イベントデータを複数の情報源やセンサーから収集し、相互に関連付けている	DE.AE-03, DE.AE-07	DE.AE-03	多様な情報源からの情報が相関付けされている	✓	
	DE.AE-4	イベントがもたらす影響を特定している	DE.AE-04	DE.AE-04	有害イベントの推定上の影響と範囲が理解されている	✓	
	DE.AE-5	インシデント警告の閾値を定めている	DE.AE-08	DE.AE-05	Not Applicable		
		V2新規サブカテゴリー		DE.AE-06	有害イベントに関する情報が、認可された職員とツールに提供されている		✓
		V2新規サブカテゴリー		DE.AE-07	サイバー脅威インテリジェンスおよび他の文脈的情報が分析に統合されている		✓
		V2新規サブカテゴリー		DE.AE-08	定義されたインシデント基準に有害イベントが当てはまる場合、インシデントが宣言されている		✓
セキュリティの継続的なモニタリング（DE.CM）							
	DE.CM-1	発生する可能性のあるサイバーセキュリティイベントを検知できるよう、ネットワークをモニタリングしている	DE.CM-01	DE.CM-01	潜在的な有害イベントを発見するよう、ネットワークとネットワークサービスがモニタリングされている	✓	
	DE.CM-2	発生する可能性のあるサイバーセキュリティイベントを検知できるよう、物理環境をモニタリングしている	DE.CM-02	DE.CM-02	潜在的な有害イベントを発見するよう、物理的環境がモニタリングされている	✓	
	DE.CM-3	発生する可能性のあるサイバーセキュリティイベントを検知できるよう、個人の活動をモニタリングしている	DE.CM-03	DE.CM-03	潜在的な有害イベントを発見するよう、人員の活動や技術の使用状況がモニタリングされている	✓	
	DE.CM-4	悪質なコードを検出できる	DE.CM-01, DE.CM-09	DE.CM-04	Not Applicable		
	DE.CM-5	悪質なモバイルコードを検出できる	DE.CM-01, DE.CM-09	DE.CM-05	Not Applicable		
	DE.CM-6	発生する可能性のあるサイバーセキュリティイベントを検知できるよう、外部サービスプロバイダの活動をモニタリングしている	DE.CM-06	DE.CM-06	潜在的な有害イベントを発見するよう、外部のサービスプロバイダによる活動とサービスがモニタリングされている	✓	
	DE.CM-7	権限のない従業員、接続、デバイス、ソフトウェアのモニタリングを実施している	DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09	DE.CM-07	Not Applicable		
	DE.CM-8	脆弱性スキャンを実施している	ID.RA-01	DE.CM-08	Not Applicable		
		V2新規サブカテゴリー		DE.CM-09	潜在的な有害イベントを発見するよう、コンピューティングハードウェア、ソフトウェア、ランタイム環境、それらのデータがモニタリングされている		✓
検知プロセス（DE.DP）							
	DE.DP-1	説明責任を果たせるよう、検知に関する役割と責任を明確に定義している	GV.RR-02	DE.DP-01	Not Applicable		
	DE.DP-2	検知活動は必要なすべての要求事項を満たしている	DE.AE	DE.DP-02	Not Applicable		
	DE.DP-3	検知プロセスをテストしている	ID.IM-02	DE.DP-03	Not Applicable		
	DE.DP-4	イベント検知情報を適切な関係者に伝達している	DE.AE-06	DE.DP-04	Not Applicable		
	DE.DP-5	検知プロセスを継続的に改善している	ID.IM-03, ID.IM	DE.DP-05	Not Applicable		

NISTサイバーセキュリティフレームワーク V1.1およびV2差分表

対応（RS）

	V1.1			V2.0			
カテゴリー	サブカテゴリー	サブカテゴリー詳細	V2でのサブカテゴリー	サブカテゴリー	サブカテゴリー詳細	V1.1からの引継ぎ	新件・見直し項目
対応計画（RS.RP）							
	RS.RP-1	イベントの発生中または発生後に対応計画を実施している	RS.MA-01	RS.RP-01	Not Applicable		
インシデント管理（RS.MA）							
		V2新規サブカテゴリー		RS.MA-01	インシデントが宣言されたら、関連する第三者と調整を図った上でインシデント対応計画が実行されている		✓
		V2新規サブカテゴリー		RS.MA-02	インシデント報告の対応順位が決定、検証されている		✓
		V2新規サブカテゴリー		RS.MA-03	インシデントが分類され、優先順位が付けられている		✓
		V2新規サブカテゴリー		RS.MA-04	インシデントは必要に応じて順位が引き上げられている		✓
		V2新規サブカテゴリー		RS.MA-05	インシデント復旧の開始基準が適用されている		✓
インシデント対応の報告と周知（RS.CO）							
	RS.CO-1	対応が必要になった時の自身の役割と行動の順番を従業員は認識している	PR.AT-01	RS.CO-01	Not Applicable		
	RS.CO-2	定められた基準に沿ってイベントを報告している	RS.CO-02, RC.CO-04	RS.CO-02	内外の利害関係者にインシデントが通知されている	✓	
	RS.CO-3	対応計画に従って情報を共有している	RS.CO-02, RS.CO-03	RS.CO-03	情報は、指定された内外の利害関係者と共有されている	✓	
	RS.CO-4	対応計画に従って利害関係者との間で調整を行っている	RS.MA-01, RS.MA-04	RS.CO-04	Not Applicable		
	RS.CO-5	サイバーセキュリティに関する状況認識を深めるために、外部利害関係者との間で任意の情報共有を行っている	RS.CO-03	RS.CO-05	Not Applicable		
インシデント分析（RS.AN）							
	RS.AN-1	検知システムからの通知を調査している	RS.MA-02	RS.AN-01	Not Applicable		
	RS.AN-2	インシデントがもたらす影響を把握している	RS.MA-02, RS.MA-03, RS.MA-04	RS.AN-02	Not Applicable		
	RS.AN-3	フォレンジクスを実施している	RS.AN-03, RS.AN-06	RS.AN-03	インシデント発生中に起こった状況およびインシデントの根本原因を立証するための分析が実施されている	✓	
	RS.AN-4	対応計画に従ってインシデントを分類している	RS.MA-03	RS.AN-04	Not Applicable		
	RS.AN-5	プロセスは、内外のソース（例：内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を自組織が受領、分析、対応するために定められている	ID.RA-08	RS.AN-05	Not Applicable		
		V2新規サブカテゴリー		RS.AN-06	調査中に実施された措置が記録され、記録の完全性と出所が保持されている		✓
		V2新規サブカテゴリー		RS.AN-07	インシデントのデータとメタデータが収集され、それらの完全性と出所が保持されている		✓
		V2新規サブカテゴリー		RS.AN-08	インシデントの規模が推定、検証されている		✓
インシデント軽減（RS.MI）							
	RS.MI-1	インシデントを封じ込めている	RS.MI-01	RS.MI-01	インシデントを封じ込められている	✓	
	RS.MI-2	インシデントを低減している	RS.MI-02	RS.MI-02	インシデントが根絶されている	✓	
	RS.MI-3	新たに特定された脆弱性に関して、許容できるリスクである場合にはその旨を文書化し、そうでない場合には低減している	ID.RA-06	RS.MI-03	Not Applicable		
改善（RS.IM）							
	RS.IM-1	学んだ教訓を対応計画に取り入れている	ID.IM-03, ID.IM-04	RS.IM-01	Not Applicable		
	RS.IM-2	対応戦略を更新している	ID.IM-03	RS.IM-02	Not Applicable		

NISTサイバーセキュリティフレームワーク V1.1およびV2差分表

復旧（RC）

	V1.1			V2.0			
カテゴリー	サブカテゴリー	サブカテゴリー詳細	V2でのサブカテゴリー	サブカテゴリー	サブカテゴリー詳細	V1.1からの引継ぎ	新件・見直し項目
インシデント復旧計画実行（RC.RP）							
	RC.RP-1	イベントの発生中または発生後に復旧計画を実施している	RC.RP-01, RC.RP-02	RC.RP-01	インシデント対応プロセスが開始された後、インシデント対応計画における復旧部分が実行されている	✓	
	V2新規サブカテゴリー			RC.RP-02	復旧措置の選択、範囲設定、優先順位付けが行われ、実施されている		✓
	V2新規サブカテゴリー			RC.RP-03	バックアップおよび他の修復資産が復旧のために使用される前に、それらの完全性が検証されている		✓
	V2新規サブカテゴリー			RC.RP-04	インシデント後の運用規範を確立するため、重要なミッション機能とサイバーセキュリティリスクマネジメントが考慮されている		✓
	V2新規サブカテゴリー			RC.RP-05	回復した資産の完全性が検証され、システムとサービスが回復し、正常な運用状態が確認されている		✓
	V2新規サブカテゴリー			RC.RP-06	基準に基づいてインシデント復旧の終結が宣言され、インシデント関連資料の作成が完了している		✓
改善（RC.IM）							
	RC.IM-1	学んだ教訓を復旧計画に取り入れている	ID.IM-03, ID.IM-04	RC.IM-01	Not Applicable		
	RC.IM-2	復旧戦略を更新している	ID.IM-03	RC.IM-02	Not Applicable		
インシデント復旧コミュニケーション（RC.CO）							
	RC.CO-1	広報活動を管理している	RC.CO-04	RC.CO-01	Not Applicable		
	RC.CO-2	イベント発生後に評判を回復している	RC.CO-04	RC.CO-02	Not Applicable		
	RC.CO-3	復旧活動について内部利害関係者、役員、経営陣に伝達している	RC.CO-03	RC.CO-03	復旧活動および運用能力復旧の進捗状況が、指定された内部と外部の利害関係者に周知されている	✓	
	V2新規サブカテゴリー			RC.CO-04	承認された方法とメッセージングを用いて、インシデント復旧に関する公開最新情報が共有されている		✓