NISTサイバーセキュリティフレームワーク アセスメントシート

統制（GV）

平均スコア	2.55
組織的文脈（GV.OC）	2.40
リスクマネジメント戦略（GV.RM）	3.29
役割／責任／権限（GV.RR）	2.50
ポリシー（GV.PO）	2.00
監督（GV.OV）	3.00
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）	2.10

カテゴリー	日本語	スコア	実装例 EX1	EX2	EX3	EX4	EX5
組織的文脈（GV.OC）							
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。	2	組織のミッションの妨げになり得るリスクを識別する基準を提供するため、当該ミッションを共有する（ビジョンおよびミッションの宣言、マーケティング、サービス戦略などを介して）。				
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、考慮されている。	1	組織内の関連する利害関係者およびそのサイバーセキュリティ関連の期待事項（役員、取締役、顧問からのパフォーマンスおよびリスクに対する期待事項、従業員からの文化的期待事項など）を識別する。	組織外の関連する利害関係者およびそのサイバーセキュリティ関連の期待事項（顧客のプライバシーに対する期待事項、パートナーシップに対する事業上の期待事項、規制当局からのコンプライアンスへの期待事項、社会の倫理的な期待事項など）を識別する。			
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。	4	個人情報の保護に関する法規制（医療保険の移植性と責任に関する法律、カリフォルニア州消費者プライバシー法、一般データ保護規則など）の要求事項を追跡、管理するプロセスを決定する。	サプライヤー、顧客、パートナーの情報に関するサイバーセキュリティマネジメントに対する契約上の要求事項を追跡、管理するプロセスを決定する。	組織のサイバーセキュリティ戦略を法的要求事項、規制上の要求事項、契約上の要求事項に適合させる。		
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。	3	内外の利害関係者から見た能力およびサービスの重要度を判断するための基準を定める。	ミッションの目的達成のために不可欠な情報資産、事業運営、およびそうした事業の損失（または部分的な損失）の潜在的な影響を（ビジネスに対する影響の分析などから）判定する。	さまざまな運用状況（攻撃下、復旧時、通常時など）で重要な能力およびサービスを提供するためのレジリエンスの目標（目標復旧時間など）を定め、周知する。		
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。	2	外部リソース（施設、クラウドベースのホスティングプロバイダなど）との組織の依存関係、組織の情報資産、事業上の機能に対する当該リソースの関係性についての目録を作成する。	組織の重要な能力およびサービスの潜在的な障害点となる外部依存関係を識別、文書化し、その情報を自組織の適切な人員と共有する。			
平均		**2.40**					
リスクマネジメント戦略（GV.RM）							
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。	3	年次戦略計画の一環、または大きな変更が発生した場合の対応として、サイバーセキュリティリスクマネジメントに関する短期的および長期的な目標を更新する。	サイバーセキュリティリスクマネジメントに対する測定可能な目標を定める（ユーザトレーニングの品質の管理、産業用制御システムの適切なリスク防御の確保など）。	上層部はサイバーセキュリティの目的について合意し、リスクおよびパフォーマンスの測定、管理に使用する。		
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。	3	組織にとって適切なリスクレベルに関する期待事項を伝えるリスク選好度ステートメントを決定、周知する。	リスク選好度ステートメントを具体的かつ測定可能で明白に理解可能なリスク許容度に関するステートメントに置き換える。	既知のリスクエクスポージャーおよび残存リスクに基づいて、組織の目的とリスク選好度を定期的に見直す。		
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。	4	サイバーセキュリティリスクを他の企業リスク（コンプライアンス、財務、運用、規制、風評、安全性など）とともに集約、管理する。	サイバーセキュリティリスクマネージャーを企業リスクマネジメント計画に組み込む。	企業リスクマネジメントにおけるサイバーセキュリティリスクのエスカレーション基準を定める。		

NISTサイバーセキュリティフレームワーク アセスメントシート

統制（GV）

	カテゴリー	日本語	スコア	実装例 EX1	EX2	EX3	EX4	EX5
	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。	2	さまざまなデータ分類に対して、サイバーセキュリティリスクを許容、回避する基準を特定する。	サイバーセキュリティ保険に加入するかどうかを決定する。	責任共有モデルが許容される条件を文書化する（特定のサイバーセキュリティ能力を外部委託する、組織に代わって第三者に金融取引を行わせる、パブリッククラウドベースのサービスを使用するなど）。		
	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。	4	合意された期間ごとに上層部、取締役、組織のサイバーセキュリティ態勢の管理者を改定する方法を決定する。	組織全体のすべての部門（経営陣、業務、内部監査、法務、買収、物理的セキュリティ、人事など）がサイバーセキュリティリスクについて相互にコミュニケーションをとる方法を識別する。			
	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。	4	サイバーセキュリティリスク分析に定量的アプローチを使用する基準を定め、確率およびエクスポージャーに関する公式を指定する。	テンプレート（リスク登録簿など）を作成、使用し、サイバーセキュリティリスク情報（リスクの説明、エクスポージャー、処理、所有権など）を文書化する。	企業内において適切なレベルでリスクの優先順位付けを行う基準を定める。	サイバーセキュリティリスクの統合、集約、比較の助けになるよう、整合のとれたリスクカテゴリーのリストを使用する。	
	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。	3	機会を識別し、リスクに関する議論にそれを組み込むためのガイダンスおよび手法を定義、周知する（強み、弱み、機会、脅威＜SWOT＞分析など）。	ストレッチゴールを識別し、それを文書化する。	ネガティブなリスクとともに、ポジティブなリスクを計算、文書化、優先順位付けする。		
	平均		**3.29**					
役割／責任／権限（GV.RR）								
	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。	2	リーダー（取締役など）が組織のサイバーセキュリティ戦略の策定、実施、評価における役割および責任について合意する。	安全で倫理的な文化に関するリーダーの期待事項を共有する（特に、現在のイベントがサイバーセキュリティリスクマネジメントの肯定的または否定的な例を強調する機会を呈する場合）。	リーダーが最高情報セキュリティ責任者に対し、包括的なサイバーセキュリティリスク戦略を維持し、少なくとも年に1度、または重大事象発生後にレビューおよび更新を行うよう指示する。	サイバーセキュリティリスクマネジメントの責任者間で、適切な権限および調整を保証するためのレビューを実施する。	
	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。		リスクマネジメントの役割および責任をポリシーに文書化する。	サイバーセキュリティリスクマネジメント活動の責任者、説明責任を負う人員、それらのチームおよび個人への相談方法と通知方法を文書化する。	サイバーセキュリティの責任および実績要求事項を自組織の人員への説明に盛り込む。	サイバーセキュリティリスクマネジメント責任者の実績目標を文書化し、実績を定期的に測定することで改善すべき範囲を識別する。	業務、リスク機能、内部監査機能におけるサイバーセキュリティの責任を明示する。
	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。	3	サイバーセキュリティリスクマネジメント責任者が必要な権限を持つことを保証するため、マネジメントに関する定期的なレビューを実施する。	リスク許容度、リスクへの対応に応じたリソース配分および投資を見極める。	サイバーセキュリティ戦略をサポートするための適切かつ十分な人員、プロセス、技術リソースを提供する。		
	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。		サイバーセキュリティリスクマネジメントについての検討事項を人的資源プロセス（人員のスクリーニング、オンボーディング、変更通知、オフボーディングなど）に統合する。	サイバーセキュリティの知識を採用、研修、定着に関する意思決定においてプラスの要素であると考える。	デリケートな役割を担う新入社員のオンボーディングに先立ち身元調査を実施し、そうした役割の人員に対する身元調査を定期的に繰り返す。	自組織の人員が自身の役割に関連するセキュリティポリシーを認識、遵守、維持する義務を定義、実施する。	
	平均		**2.50**					
ポリシー（GV.PO）								
	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。	1	経営陣の意図、期待事項、方向性を明記した理解しやすく使いやすいリスクマネジメントポリシーを作成、周知、維持する。	ポリシー、それをサポートするプロセス、手順に対する定期的なレビューを行い、それらがリスクマネジメント戦略の目的、優先事項、高度なサイバーセキュリティポリシーの方向性と一致していることを確認する。	ポリシーに関する上級管理職からの承認を義務付ける。	サイバーセキュリティリスクマネジメントポリシーと、それをサポートするプロセスおよび手順を組織全体に周知する。	雇用時およびポリシーの更新時に加え、年1回はポリシーの受領を確認することを自組織の人員に義務付ける。
	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。	3	サイバーセキュリティリスクマネジメントの結果の定期的なレビューに基づいてポリシーを更新し、ポリシーとそれをサポートするプロセスおよび手順によってリスクが許容可能なレベルに適切に維持される状況を確保する。	組織のリスク環境に対する変更（リスクや組織のミッション目標の変更など）をレビューするためのスケジュールを提供し、推奨されるポリシーの更新を周知する。	法的要求事項や規制上の要求事項の変更が反映されるようポリシーを更新する。	技術の変化（人工知能の採用など）や事業上の変化（新規事業の買収、新規契約の要求事項など）が反映されるようポリシーを更新する。	
	平均		**2.00**					

NISTサイバーセキュリティフレームワーク アセスメントシート

統制（GV）

	カテゴリー	日本語	スコア	実装例 EX1	EX2	EX3	EX4	EX5
監督（GV.OV）								
	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。	2	リスクマネジメント戦略およびリスクの結果がリーダーの意思決定や組織の目標達成にどの程度役立ったかを測定する。	業務またはイノベーションを阻害するサイバーセキュリティリスク戦略を調整する必要がないかを検討する。			
	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。	3	監査結果のレビューを行い、既存のサイバーセキュリティ戦略が内外の要求事項に確実に準拠しているかどうかを確認する。	サイバーセキュリティ関連の役割を担う人員のパフォーマンスの監督状況をレビューし、ポリシーの変更が必要かどうかを判断する。	サイバーセキュリティインシデントを踏まえ、戦略をレビューする。		
	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。	4	主要業績評価指標（KPI）をレビューし、組織全体のポリシーおよび手順がその目的を達成していることを確認する。	主要リスク指標（KRI）をレビューし、起こりやすさや潜在的な影響といった組織が直面するリスクを識別する。	サイバーセキュリティリスクマネジメントに関する指標を収集し、上層部と情報交換を行う。		
	平均		**3.00**					
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）								
	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。	1	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プログラムの目的を示す戦略を定める。	プログラムの実施および改善に係る計画（マイルストーンを含む）、ポリシー、手順などの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プログラムを策定し、当該ポリシーおよび手順を組織の利害関係者と共有する。	組織の利害関係者による合意を受けて実行される戦略、目的、ポリシー、手順に基づくプログラムプロセスを策定、実施する。	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に寄与する機能（サイバーセキュリティ、IT、業務、法務、人事、エンジニアリングなど）間における連携を保証する組織横断的なメカニズムを定める。	
	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。	1	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活動の計画、リソース提供、実行に責任と説明責任を負う1つ以上の特定の役割またはポジションを識別する。	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の役割および責任をポリシーに文書化する。	責任マトリクスを作成し、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活動に責任と説明責任を負う人員、それらのチームや個人への相談方法と通知方法を文書化する。	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の責任および実績要求事項を自組織の人員への説明に盛り込み、明確性を確保し、説明責任を向上させる。	サイバーセキュリティリスクマネジメント固有の責任を負う人員の実績目標を文書化し、定期的な測定により実績を実証、改善する。
	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。	2	サイバーセキュリティや企業リスクマネジメントとの整合および重複範囲を識別する。	サイバーセキュリティリスクマネジメントおよび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統合計画を定める。	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を改善プロセスに統合する。	サプライチェーンにおける重大なサイバーセキュリティリスクを上級管理職に上申し、企業リスクマネジメントレベルで当該リスクに対処する。	
	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。	2	サプライヤーが処理または所有するデータの機密性、組織のシステムへのアクセス頻度、組織のミッションに対する製品またはサービスの重要性などに基づき、サプライヤーの重要度の基準を明示する。	全サプライヤーを記録し、重要度基準に基づいてサプライヤーの優先順位付けを行う。			
	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。	3	サプライヤー、製品、サービスについて、それらの重要度や侵害された場合の潜在的影響に応じてセキュリティ要求事項を定める。	第三者が従うべきすべてのサイバーセキュリティ、サプライチェーン要求事項、当該要求事項の遵守に対する検証方法をデフォルト契約の文言に組み込む。	組織とそのサプライヤーや下層サプライヤー間の情報共有についてのルールおよびプロトコルを契約で定義する。	重要度、あるいは侵害された場合の潜在的影響に基づき、契約にセキュリティ要求事項を盛り込むことによりリスクを管理する。	サービスレベル契約（SLA）においてセキュリティ要求事項を定義し、サプライヤーとの取引過程全体を通じた許容可能なセキュリティパフォーマンスについてサプライヤーをモニタリングする。
	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。	3	調達計画との整合性があり、各サプライヤーとの取引関係におけるリスクレベル、重要度、複雑さに見合った徹底的な適正評価をサプライヤー候補に対して実施する。	技術およびサイバーセキュリティに関する適合性、サプライヤー候補のリスクマネジメントプラクティスについて評価する。	事業上の要求事項、また該当するサイバーセキュリティに対する要求事項について、サプライヤーのリスクアセスメントを実施する。	取得前、または使用前に重要製品の真正性、完全性、セキュリティについて評価する。	
	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。	2	第三者の評判や第三者が提供する製品またはサービスの重要度に基づきアセスメントのフォーマットや頻度を調整する。	契約上のサイバーセキュリティ要求事項遵守に関する第三者の証拠（自己証明、保証、認証、その他の成果物など）を評価する。	さまざまな手法および技法（検査、監査、テスト、その他の形式の評価など）を使用し、取引過程全体を通じてサプライヤーがそのセキュリティ義務を果たしていることを確認するため、重要なサプライヤーをモニタリングする。	重要なサプライヤー、サービス、製品のリスクプロファイルの変化をモニタリングし、それに応じてサプライヤーの重要度およびリスクの影響を再評価する。	事業継続性が確保されるよう、サプライヤーおよびサプライチェーン関連の予期せぬ中断に備えた計画を立てる。
	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。	2	インシデント対応、復旧活動、組織とそのサプライヤー間の状態を報告するためのルールおよびプロトコルを定義、使用する。	インシデント対応における組織とそのサプライヤーの役割および責任を識別、文書化する。	重要なサプライヤーをインシデント対応演習やシミュレーションに参加させる。	組織とその重要なサプライヤー間におけるクライシスコミュニケーションの手法およびプロトコルを定義、調整する。	重要なサプライヤーと共同で教訓セッションを実施する。
	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。	1	ポリシーおよび手順により、取得したすべての技術製品やサービスに関する来歴の記録を義務付ける。	取得したコンポーネントに改ざんがなく、正規品であることを証明する方法について、リーダーに定期的にリスクレポートを提出する。	サイバーセキュリティリスクマネージャーと業務担当者の間で、認証された信頼できるソフトウェアプロバイダからのみソフトウェアパッチ、アップデート、アップグレードを取得する必要性について定期的に情報交換を行う。	承認されたサプライヤーの人員に対しサプライヤー製品の保守の実施を義務付けることが保証されるよう、ポリシーをレビューする。	ポリシーや手順により、重要なハードウェアのアップグレードに不正な変更がないか確認することを義務付ける。
	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終了後に発生する活動に関する規定が含まれている。	4	平時および緊急時の両方について重要な取引関係を終了するプロセスを定める。	コンポーネントの使用期限、保守支援、陳腐化に関する計画を定義、実行する。	組織リソースへのサプライヤーのアクセスが不要になった場合、速やかに無効化されていることを確認する。	組織のデータを含む情報資産がタイムリーかつ安全な方法で返却、適切に廃棄、管理されていることを確認する。	サプライチェーンのセキュリティリスクおよびレジリエンスを考慮したサプライヤーとの取引関係を終了または移行する計画を策定し、実行する。
	平均		**2.10**					

NISTサイバーセキュリティフレームワーク アセスメントシート

特定（ID）

平均スコア	**1.98**
資産管理（ID.AM）	**2.29**
リスクアセスメント（ID.RA）	**2.40**
改善（ID.IM）	**1.25**

カテゴリー	日本語	スコア	実装例 EX1	EX2	EX3	EX4	EX5
資産管理（ID.AM）							
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。	2	IT、IoT、OT、モバイルデバイスなど、あらゆるタイプのハードウェアの目録を維持する。	新しいハードウェアを検出し、目録が自動更新されるようネットワークを常にモニタリングする。			
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。	2	市販品、オープンソース、カスタムアプリケーション、APIサービス、クラウドベースのアプリケーションやサービスなど、あらゆるタイプのソフトウェアおよびサービスの目録を維持する。	ソフトウェアおよびサービスの目録更新のため、コンテナや仮想マシンなどのすべてのプラットフォームを常にモニタリングする。	組織のシステムの目録（インベントリ）を維持する。		
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。	3	組織の有線／無線ネットワーク内の通信およびデータフローのベースラインを維持する。	組織と第三者間の通信およびデータフローのベースラインを維持する。	組織のinfrastructure-as-a-service（IaaS）の使用に関する通信およびデータフローのベースラインを維持する。	認可されたシステム間で通常使用が想定されるネットワークポート、プロトコル、サービスのドキュメントを維持する。	
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。	3	組織が使用するすべての外部サービス（サードパーティのinfrastructure-as-a-service＜IaaS＞、platform-as-a-service＜PaaS＞、software-as-a-service＜SaaS＞オファリング、API、外部にホストされるその他のアプリケーション サービスなど）の目録（インベントリ）を作成する。	新たな外部サービスを利用する際に目録（インベントリ）を更新し、組織によるそのサービスの使用に対するサイバーセキュリティリスクマネジメントによる適切なモニタリングを確保する。			
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。	1	資産の各クラスに優先順位を付けるための基準を定義する。	資産に優先順位の基準を適用する。	資産の優先順位を追跡し、定期的に、または組織に大きな変更が生じたときに更新する。		
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。	1	重要な指定されたデータ型（個人情報、保護対象健康情報、金融口座番号、組織の知的財産、OTデータなど）のリストを維持する。	アドホックデータを継続的に検出、分析し、指定されたデータ型の新しいインスタンスを識別する。	タグまたはラベルを使用して、指定されたデータ型にデータ分類を割り当てる。	指定されたデータ型の各インスタンスの来歴、データ所有者、地理的位置を追跡する。	
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。	4	システム、ハードウェア、ソフトウェア、サービスのライフサイクル全体にわたってサイバーセキュリティに関する検討事項を統合する。	製品のライフサイクルにサイバーセキュリティに関する検討事項を統合する。	ミッションの目的を達成するための技術の非公式な使用（シャドーIT）を識別する。	組織の攻撃対象領域を不必要に拡大する冗長なシステム、ハードウェア、ソフトウェア、サービスを定期的に識別する。	本番環境への導入前に、システム、ハードウェア、ソフトウェア、サービスの環境を適切に設定、保護する。
平均		**2.29**					
リスクアセスメント（ID.RA）							
ID.RA-01	資産における脆弱性が識別、検証、記録されている。	1	パッチが適用されていない、または構成の設定が不良であるソフトウェアを識別するため、脆弱性管理技術を用いる。	サイバーセキュリティに影響を与える設計および実装の弱点を確認するため、ネットワークやシステムのアーキテクチャを評価する。	設計、コーディング、既定の構成設定の脆弱性を特定するため、自組織で開発したソフトウェアのレビュー、分析、テストを行う。	重要なコンピューティング資産を収容する施設の物理的脆弱性およびレジリエンスの問題を評価する。	製品およびサービスの新たな脆弱性に関する情報を得られるよう、サイバー脅威インテリジェンスのソースをモニタリングする。
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。	2	サイバー脅威インテリジェンスフィードが安全に取り込まれるよう、検知または対応機能を備えたサイバーセキュリティツールおよび技術を設定する。	現在の脅威アクターとその戦術、技術、手順（TTP）に関して信頼できる第三者からの助言を受け、レビューする。	新興技術が有し得る脆弱性の種類に関する情報を確認するため、サイバー脅威インテリジェンスの情報源をモニタリングする。		
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。	3	組織を標的にする可能性のある脅威アクターの種類と、当該脅威アクターが使用する可能性のあるTTPについての認識を維持するため、サイバー脅威インテリジェンスを用いる。	脅威ハンティングを実行し、環境内にある脅威アクターの兆候を探す。	内部の脅威アクターを識別するためのプロセスを実装する。		
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。	4	リスクシナリオの発生可能性および影響を推定し、リスク登録簿にそれらを記録するよう業務上のリーダーとサイバーセキュリティリスクマネジメント担当者が協業する。	組織の通信、システム、それらのシステム内またはシステムによって処理されるデータへの不正アクセスによる事業に対する潜在的影響を列挙する。	システム・オブ・システムズの連鎖的な障害の潜在的影響を考慮する。		

NISTサイバーセキュリティフレームワーク アセスメントシート

特定（ID）

カテゴリー	日本語	スコア	実装例				
			EX1	EX2	EX3	EX4	EX5
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。	3	データに対するリスクをより深く理解し、適切なリスクへの対応を見極めるため、脅威モデルを策定する。	推定される発生可能性および影響に基づきサイバーセキュリティリソースの配分、投資の優先順位付けを行う。			
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。	2	リスクの許容、移転、軽減、回避の採否を決定するための脆弱性マネジメント計画の基準を適用する。	リスクを軽減するための補完的管理策を選択するための脆弱性マネジメント計画の基準を適用する。	リスクへの対応の進捗状況を追跡する（行動計画とマイルストーン＜POA&M＞、リスク登録簿、リスク詳細レポートなど）。	リスク対応の決定と措置を通知するため、リスクアセスメントの結果を使用する。	影響を受ける利害関係者に対し優先順位に従って、計画されたリスク対応を周知する。
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。	1	提案された変更および要求された例外の正式な文書化、レビュー、テスト、承認についての手順を実装し、それに従う。	提案された各変更の実施／未実施の場合に想定されるリスクを文書化し、変更のロールバックに関するガイダンスを提供する。	要求された各例外に関連するリスクと、それらのリスクに対応するための計画を文書化する。	計画された将来の措置またはマイルストーンに基づいて許容されたリスクを定期的にレビューする。	
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。	2	契約で定義されたルールとプロトコルに従い、組織とサプライヤーの間で脆弱性情報を共有する。	サプライヤー、顧客、パートナー、政府のサイバーセキュリティ組織によるサイバーセキュリティの脅威、脆弱性、インシデントの開示について処理、分析、対応する責任を割り当て、手順の実行を検証する。			
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。	3	調達と使用の前に主要な技術製品およびサービスの真正性とサイバーセキュリティを評価する。				
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。	3	事業上適用されるサイバーセキュリティ要求事項について、サプライヤーのリスクアセスメントを実施する（サプライチェーンを含む）。				
平均		**2.40**					
改善（ID.IM）							
ID.IM-01	改善が評価を基に識別されている。	1	現在の脅威およびTTPを考慮し、主要サービスの自己アセスメントを実行する。	改善を要する領域を識別するため、組織のサイバーセキュリティプログラムの有効性に関する第三者アセスメントまたは外部監査に投資する。	自動化された手段により、選択したサイバーセキュリティ要求事項の遵守を常に評価する。		
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。	1	インシデント対応アセスメント（机上演習、シミュレーション、テスト、内部レビュー、独立監査など）の結果に基づいて、今後のインシデント対応活動に対する改善点を識別する。	主要なサービスプロバイダおよび製品サプライヤーと連携して実施される演習に基づいて、将来的なビジネス継続性、災害復旧、インシデント対応活動に対する改善点を識別する。	必要に応じて、社内の利害関係者（上層部、法務部、人事部など）をセキュリティテストおよび演習に関与させる。	上層部から承認を受け選択したハイリスクシステムのセキュリティ体制を改善する機会を識別するため、侵入テストを実施する。	製品またはサービスが契約サプライヤーまたはパートナーが製造したものではないことや、受領前に変更されたことが判明した場合の対応と復旧についての緊急時対応計画を実施する。
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。	1	サプライヤーと共同で教訓セッションを実施する。	教訓が考慮されるようサイバーセキュリティの方針、プロセス、手順を年1回レビューする。	運用上のサイバーセキュリティパフォーマンスを経時的に評価する基準を用いる。		
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。	2	業務の妨げ、機密情報の漏洩、組織のミッションおよび存続を脅かす可能性のある有害事象への対応、復旧に対する緊急時対応計画（インシデント対応、事業継続、災害復旧など）を定める。	問合せ窓口および連絡先情報、一般的なシナリオに対処するためのプロセス、優先順位付け、エスカレーション、エレベーションの基準をすべての緊急時対応計画に盛り込む。	あらゆる種類の脆弱性を識別、評価するとともに、リスクへの対応の優先順位付け、テスト、実装を行うために、脆弱性マネジメント計画を作成する。	サイバーセキュリティ計画（更新を含む）を、その実行責任者や影響を受ける当事者に周知する。	年1回、または大幅な改善の必要性が識別されたときにすべてのサイバーセキュリティ計画をレビュー、更新する。
平均		**1.25**					

NISTサイバーセキュリティフレームワーク アセスメントシート

防御（PR）

平均スコア	**2.92**
アイデンティティ管理／認証／アクセス制御（PR.AA）	3.67
意識向上とトレーニング（PR.AT）	4.00
データセキュリティ（PR.DS）	1.75
プラットフォームセキュリティ（PR.PS）	2.67
技術インフラレジリエンス（PR.IR）	2.50

カテゴリー	日本語	スコア	実装例 EX1	EX2	EX3	EX4	EX5
アイデンティティ管理／認証／アクセス制御（PR.AA）							
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。	4	従業員、請負業者などの新規アクセスまたは追加アクセスの要請を開始し、必要に応じてシステムまたはデータ所有者の許可を得て、当該要請を追跡、レビュー、実行する。	暗号化証明書、IDトークン、暗号鍵（鍵管理）、その他の証明書の発行、管理、無効化を行う。	不変のハードウェア特性から各デバイスの一意の識別子を選択する。またはデバイス対してに安全に用意された識別子を選択する。	承認されたハードウェアに、目録作成およびサービス提供を目的とした識別子を物理的にラベル付けする。	
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。	4	政府発行の身分証明書（パスポート、ビザ、運転免許証など）を使用して、登録時に個人が申告した身元識別情報を確認する。	ユーザごとに異なる証明書を発行する（すなわち証明書の共有不可）。			
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。	3	多要素認証を義務付ける。	パスワード、PIN、同様のオーセンティケータの最小強度に関する方針を実施する。	リスクに基づきユーザ、サービス、ハードウェアを定期的に再認証する（ゼロトラストアーキテクチャ）。	緊急事態下での安全保護のために認可された人員が必要不可欠なアカウントにアクセスできる状況を確保する。	
PR.AA-04	IDアサーションが保護、周知、検証されている。	4	シングルサインオンシステムを介して、認証およびユーザ情報を周知するために使用されるIDアサーションを保護する。	フェデレーションシステム間で認証およびユーザ情報を周知するために使用されるIDアサーションを保護する。	すべてのコンテキストにおいてIDアサーションの標準ベースのアプローチを実装し、IDアサーションの生成（データモデル、メタデータなど）、保護（デジタル署名、暗号化など）、検証（署名検証など）に対するすべてのガイダンスに従う。		
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。	4	論理的および物理的アクセス権限を定期的にレビューし、組織の変更または人員の組織からの離脱が発生する都度、不要になった権限を速やかに無効化する。	要求者や要求されたリソースの属性を承認決定の際に考慮する（位置情報、曜日／時間、要求者のエンドポイントのサイバーヘルスなど）。	アクセスおよび権限を必要最小限に制限する（ゼロトラストアーキテクチャなど）。	職務の適切な分離を確認するため、重要なビジネス機能に関連する権限を定期的にレビューする。	
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。	3	施設をモニタリングし、アクセスを制限するため、警備員、防犯カメラ、入り口の施錠、警報システム、その他の物理的制御を用いる。	リスクの高い情報資産を有するエリアに対して追加の物理的セキュリティ管理策を採用する。	事業上重要な資産を有するエリア内ではゲスト、ベンダー、その他の第三者に付き添う。		
平均		**3.67**					
意識向上とトレーニング（PR.AT）							
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。	4	従業員、請負業者、パートナー、サプライヤー、組織の非公開リソースのその他全ユーザに基本的なサイバーセキュリティ意識の向上を促し、必要なトレーニングを提供する。	ソーシャルエンジニアリングの試みやその他の一般的な攻撃の認識、攻撃や不審なアクティビティの報告、アクセプタブルユースポリシーの遵守、基本的なサイバー衛生タスク（ソフトウェアへのパッチ適用、パスワードの選択、証明書の保護など）の実行のため、自組織の人員のトレーニングを行う。	サイバーセキュリティポリシーの違反が個々のユーザおよび組織全体に及ぼす影響について説明する。	基本的なサイバーセキュリティプラクティスの理解度について、ユーザを定期的に評価、テストする。	既存のプラクティスを強化するとともに、新たなプラクティスを導入するために年1回の再教育を義務付ける。
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、意識向上させ、トレーニングを受けている。	4	追加のサイバーセキュリティトレーニングが必要な組織内の専門的役割（物理セキュリティ担当者、サイバーセキュリティ担当者、財務担当者、上層部、事業上重要なデータにアクセスする人員など）を識別する。	請負業者、パートナー、サプライヤー、その他の第三者などといった特殊な役割を担う全人員に役割に基づいたサイバーセキュリティ意識の向上を促し、必要なトレーニングを提供する。	それぞれの特殊な役割に応じたサイバーセキュリティプラクティスの理解度について、ユーザを定期的に評価、テストする。	既存のプラクティスを強化するとともに、新たなプラクティスを導入するために年1回の再教育を義務付ける。	
平均		**4.00**					

NISTサイバーセキュリティフレームワーク アセスメントシート

防御（PR）

カテゴリー	日本語	スコア	実装例 EX1	EX2	EX3	EX4	EX5
データセキュリティ（PR.DS）							
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。	2	ファイル、データベース、仮想マシンのディスクイメージ、コンテナイメージ、その他のリソースに保存されているデータの機密性と完全性を保護するため、暗号化、デジタル署名、暗号化ハッシュを使用する。	ユーザエンドポイントに保存されているデータを保護するため、ディスク全体の暗号化を使用する。	署名の検証によりソフトウェアの完全性を確認する。	データ流出を防止するため、リムーバブルメディアの使用を制限する。	暗号化されていない機微な情報を含むリムーバブルメディアを物理的に保護する（施錠されたオフィスまたはファイルキャビネット内への保管など）。
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。	1	ネットワーク通信の機密性と完全性を保護するため、暗号化、デジタル署名、暗号化ハッシュを使用する。	データ分類に応じて、機密データを含む送信メールおよびその他の通信を自動的に暗号化またはブロックする。	組織のシステムとネットワークから、個人の電子メール、ファイル共有、ファイルストレージサービス、その他の個人用通信アプリケーションやサービスへのアクセスをブロックする。	開発環境、テスト環境、その他の非本番環境において、本番環境から取得した機密データ（顧客記録など）を再利用することを防止する。	
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。	1	機密性の保持が必須のデータ（プロセッサやメモリから取得したデータなど）は、不要になったらすぐに削除する。	使用中のデータを、同じプラットフォームの他のユーザやプロセスによるアクセスから保護する。			
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。	3	重要なデータをほぼリアルタイムで継続的にバックアップし、その他のデータについては合意したスケジュールで頻繁にバックアップする。	あらゆる種類のデータ ソースについて、バックアップと復元を年1回以上テストする。	インシデントまたは災害による損害を被ることのないよう、一部のバックアップをオフラインとオフサイトで安全に保存する。	データバックアップストレージの地理的分離と地理的制限を実施する。	
平均		**1.75**					
プラットフォームセキュリティ（PR.PS）							
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。	1	組織のサイバーセキュリティポリシーを実施し、必須機能のみを提供する強化版ベースラインを策定、テスト、展開、維持する（最小限の機能性の原則）。	ソフトウェアのインストール時またはアップグレード時にサイバーセキュリティに影響を与える可能性のあるデフォルトの構成設定をすべてレビューする。	承認されたベースラインからの逸脱がないか確認するため、実装されたソフトウェアをモニタリングする。		
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。	2	脆弱性マネジメント計画で指定された期間内に定期的または緊急のパッチ適用を実行する。	コンテナイメージを更新し、既存インスタンスの更新ではなく、新たなコンテナインスタンスをデプロイして代替する。	サポートが終了したソフトウェアやサービスのバージョンをサポート対象となる現行バージョンに代替する。	不当なリスクをもたらす未承認のソフトウェアやサービスをアンインストールし、削除する。	攻撃者が悪用する可能性のある不要なソフトウェアコンポーネント（オペレーティングシステムユーティリティなど）をアンインストールし、削除する。
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。	2	必要なセキュリティ能力が不足している場合、または必要なセキュリティ能力を備えたソフトウェアをサポートできない場合はハードウェアを代替する。	ハードウェアの保守サポート終了、陳腐化に対する計画を定義、実行する。	ハードウェアを安全で責任ある監査可能な方法で廃棄する。		
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。	3	ログレコードが生成されるよう、すべてのオペレーティングシステム、アプリケーション、サービス（クラウドベースのサービスを含む）を設定する。	組織のロギング用インフラのシステム、サービス、ログが安全に共有されるようログ生成装置を設定する。	ゼロトラストアーキテクチャに必要なデータを記録するため、ログ生成装置を設定する。		
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。	4	リスクが妥当なものとみなされた場合、ソフトウェアの実行を許可された製品のみに制限する、または禁止対象、未認可のソフトウェアの実行を拒否する。	インストールする前に、新しいソフトウェアのソースおよび当該ソフトウェアの完全性を確認する。	既知の悪意あるドメインへのアクセスをブロックし、承認済みのDNSサービスのみ使用するようプラットフォームを構成する。	組織が承認したソフトウェアのインストールのみ許可されるようプラットフォームを構成する。	
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。	4	自組織が開発したソフトウェアのすべてのコンポーネントを改ざんや不正アクセスから保護する。	組織が作成したすべてのソフトウェアを、リリース時の脆弱性を最小限に抑えて保護する。	本番環境で使用されているソフトウェアを維持し、不要になったソフトウェアを安全に廃棄する。		
平均		**2.67**					
技術インフラレジリエンス（PR.IR）							
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。	2	信頼境界やプラットフォームの種類（IT、IoT、OT、モバイル、ゲストなど）に従って組織のネットワークおよびクラウドベースのプラットフォームを論理的にセグメント化し、セグメント間でのみ必要な通信を許可する。	組織のネットワークを外部ネットワークから論理的にセグメント化し、必要な通信に限り外部ネットワークから組織のネットワークに入ることを許可する。	各リソースへのネットワークアクセスが必要最小限に制限されるよう、ゼロトラストアーキテクチャを実装する。	本番リソースへのアクセスおよび使用を許可する前に、エンドポイントのサイバーヘルスを確認する。	
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。	2	洪水、火災、風、過度の高温多湿など既知の環境的脅威から組織の機器を防御する。	組織に代わってシステムを運用するサービスプロバイダに対する要求事項に、環境的脅威からの防御、適切な運用インフラに係る規定を盛り込む。			
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。	3	システムとインフラの単一障害点を回避する。	容量を増やし、信頼性を向上させるため、負荷分散を用いる。	システムの信頼性を向上させるため、冗長のストレージや電源など、可用性の高いコンポーネントを使用する。		
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。	3	ストレージ、電力、コンピューティング、ネットワーク帯域幅、その他のリソースの使用状況をモニタリングする。	将来的なニーズを予測し、それに応じてリソースを拡張する。			
平均		**2.50**					

NISTサイバーセキュリティフレームワーク アセスメントシート

検知（DE）

平均スコア	**3.13**
有害イベント分析（DE.AE）	**3.67**
継続的モニタリング（DE.CM）	**2.60**

	カテゴリー	日本語	スコア	実装例 EX1	EX2	EX3	EX4	EX5
有害イベント分析（DE.AE）								
	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。	4	セキュリティ情報や、イベント管理（SIEM）またはその他のツールを使用して、既知の悪意ある活動や疑わしい活動についてログイベントを継続的にモニタリングする。	ログ分析ツールで最新のサイバー脅威インテリジェンスを活用して、検知精度を向上させ、脅威アクター、その手法、侵害の指標を特徴付ける。	自動化では十分にモニタリングできない技術について、ログイベントの手動レビューを定期的に実施する。	ログ分析ツールを使用して分析結果に関するレポートを生成する。	
	DE.AE-03	多様な情報源からの情報が相関付けされている。	3	他のソースによって生成されたログデータを、比較的少数のログサーバーに常に転送する。	イベント相関技術（SIEMなど）を使用して、複数のソースで採取された情報を収集する。	サイバー脅威インテリジェンスを活用して、ログソース間でのイベントの相関付けをサポートする。		
	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。	3	影響と範囲を推定し、SIEMまたはその他のツールを使用して、その推定値をレビュー、改善する。	個人単位で独自に影響と範囲を推定する。			
	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。	4	アラートを生成し、セキュリティオペレーションセンター（SOC）、インシデント対応者、インシデント対応ツールにそれが提供されるようサイバーセキュリティソフトウェアを使用する。	インシデント対応者およびその他の権限のある人員はログ分析結果にいつでもアクセスできる。	特定の種類のアラートが発生した際、組織のチケット発行システムでチケットを自動的に作成し、割り当てる。	技術職員が侵害の兆候を検出した場合、組織のチケット発行システムでチケットを手動で作成し、割り当てる。	
	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。	4	サイバー脅威インテリジェンスフィードを、検知技術、プロセス、担当者にセキュアな状態で提供する。	資産目録目録（インベントリ）から取得した情報を、検知技術、プロセス、担当者にセキュアな状態で提供する。	サプライヤー、ベンダー、サードパーティのセキュリティアドバイザリーから、組織の技術に対する脆弱性開示情報を速やかに取得し、分析する。		
	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。	4	活動に関して既知または想定される特性に対してインシデント基準を適用することにより、インシデントを宣言する必要性を判断する。	インシデント基準を適用する際、既知の誤検知を考慮する。			
	平均		**3.67**					
継続的モニタリング（DE.CM）								
	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。	2	有害事象が生じていないか、DNS、BGP、その他のネットワークサービスを監視する。	無許可のエンドポイントからの接続がないか、有線／無線ネットワークをモニタリングする。	設備をモニタリングして、無許可または不正な無線ネットワークがないか確認する。	偏差を検知するため、実際のネットワークフローをベースラインと比較する。	ゼロトラストを目的に、ネットワーク通信をモニタリングして、セキュリティ体制における変化を識別する。
	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。	2	異常なアクセスパターン（標準からの逸脱など）やアクセス試行未遂を検知するため、物理アクセス制御システム（バッジリーダーなど）からのログをモニタリングする。	物理的アクセス記録（訪問者登録、サインインシートなどから取得したもの）をレビューし、モニタリングする。	改ざんの兆候がないか確認するため、物理的アクセス制御（ロック、ラッチ、ヒンジピン、警報など）をモニタリングする。	警報システム、カメラ、警備員を使用して物理的環境をモニタリングする。	
	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。	3	インサイダー脅威が軽減されるよう、行動分析ソフトウェアを使用して異常なユーザアクティビティを検知する。	論理アクセス制御システムからのログをモニタリングして、異常なアクセスパターンやアクセス試行未遂を検出する。	あらゆる使用状況について、ユーザアカウントなどの欺瞞技術を継続的にモニタリングする。		
	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。	4	外部プロバイダが組織のシステム上で実行するリモートおよびオンサイトでの管理、保守管理活動をモニタリングする。	クラウドベースのサービス、インターネットサービスプロバイダ、その他のサービスプロバイダからのアクティビティをモニタリングして、想定される動作からの逸脱がないかを確認する。			
	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。	2	電子メール、ウェブサイト、ファイル共有、コラボレーションサービス、その他の一般的な攻撃ベクトルをモニタリングして、マルウェア、フィッシング、データ漏洩、ハッキングによる情報の窃盗、その他の有害事象を検知する。	認証の試行をモニタリングして、証明書に対する攻撃や証明書の不正な再利用を識別する。	ソフトウェア構成のセキュリティベースラインからの逸脱をモニタリングする。	ハードウェアおよびソフトウェアに改ざんの兆候がないかモニタリングする。	エンドポイントに存在するテクノロジーを使用してサイバーヘルスの問題（パッチの欠落、マルウェア感染、不正なソフトウェアなど）を検知し、アクセス承認前にエンドポイントを修復環境にリダイレクトする。
	平均		**2.60**					

NISTサイバーセキュリティフレームワーク アセスメントシート

対応（RS）

平均スコア	**2.51**
インシデントマネジメント（RS.MA）	3.80
インシデント分析（RS.AN）	1.25
インシデント対応の報告とコミュニケーション（RS.CO）	3.50
インシデント軽減（RS.MI）	1.50

カテゴリー	日本語	スコア	実装例 EX1	EX2	EX3	EX4	EX5
インシデントマネジメント（RS.MA）							
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。	4	検知技術により、確認されたインシデントを自動的に報告する。	組織のインシデント対応の外部委託業者にインシデント対応支援を依頼する。	インシデントごとに担当主任を指定する。	インシデント対応をサポートするため、必要に応じて追加のサイバーセキュリティ計画の実行を開始する（事業継続性や災害復旧など）。	
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。	4	インシデントレポートを事前にレビューして、サイバーセキュリティ関連であり、インシデント対応活動の必要性があることを確認する。	インシデントの重大度を見積もるための基準を適用する。			
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。	4	インシデントの種類（データ侵害、ランサムウェア、DDoS、アカウント侵害など）に基づいてインシデントを詳細にレビューし、分類する。	インシデントの範囲、想定される影響、タイムクリティカルな性質に基づいてインシデント対応の優先順位付けを行う。	インシデントからの迅速な復旧の必要性と、攻撃者の観察またはより徹底的な調査実施の必要性のバランスを取ることで、アクティブなインシデントに対する対応戦略を選択する。		
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。	4	進行中のすべてのインシデントの状態を追跡し、検証する。	インシデントの順位引き上げについて、指定された内外の利害関係者と調整する。			
RS.MA-05	インシデント復旧の開始基準が適用されている。	3	インシデント復旧プロセスを開始する必要性を判断するため、インシデントの既知または想定される特性に対するインシデント復旧基準を適用する。	インシデント復旧活動に対する運用中断の可能性を考慮する。			
平均		**3.80**					
インシデント分析（RS.AN）							
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。	1	インシデント中に発生した事象の順序、各事象に関与した資産およびリソースを判定する。	インシデントに直接的または間接的に関与した脆弱性、脅威、脅威アクターの識別を試みる。	インシデントを分析して、根底にある体系的な原因を見極める。	サイバーデセプション技術により、攻撃者の行動に関する追加情報を確認する。	
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。	1	インシデント対応職務を遂行する各対応者、その他の人員（システム管理者、サイバーセキュリティ エンジニアなど）に対し、各自の措置を記録し、記録を変更しないよう義務付ける。	インシデント担当主任に対し、インシデントを詳細に文書化し、文書の完全性および報告されるすべての情報のソースを保護する責任を負うよう義務付ける。			
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。	2	証拠保全や加工・流通過程の管理手順に基づいて、関連するすべてのインシデントデータおよびメタデータ（データソース、収集日時など）の完全性を収集、保存、保護する。				
RS.AN-08	インシデントの規模が推定、検証されている。	1	侵害の兆候と永続性の証拠を検索するため、インシデントの他の潜在的ターゲットをレビューする。	侵害の兆候と永続性の証拠を検索するため、ターゲットに対してツールを自動的に実行する。			
平均		**1.25**					
インシデント対応の報告とコミュニケーション（RS.CO）							
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。	3	データ侵害インシデントの検知後、影響を受ける顧客への通知など、組織の侵害通知手順を遵守する。	契約上の要求事項に従って、ビジネスパートナーと顧客にインシデントを通知する。	インシデント対応計画の基準および経営陣の承認に基づき、法執行機関と規制機関にインシデントを通知する。		
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。	4	対応計画および情報共有契約に従って情報を安全に共有する。	観測された攻撃者のTTPに関する情報を、すべての機密データを削除した状態で、情報共有分析センター（ISAC）と自発的に共有する。	悪意あるインサイダー活動が発生した際、人事部に通知する。	重大インシデントの状況について上層部に定期的に最新情報を報告する。	組織とそのサプライヤー間におけるインシデント情報共有に関する契約で定義されたルールおよびプロトコルを遵守する。
平均		**3.50**					

NISTサイバーセキュリティフレームワーク アセスメントシート

対応（RS）

	カテゴリー	日本語	スコア	実装例				
				EX1	EX2	EX3	EX4	EX5
インシデント軽減（RS.MI）								
	RS.MI-01	インシデントを封じ込められている。	1	サイバーセキュリティ技術（ウイルス対策ソフトウェアなど）、他の技術（オペレーティングシステム、ネットワークインフラデバイスなど）のサイバーセキュリティ機能により封じ込めアクションを自動的に実行する。	インシデント対応者が封じ込めアクションを手動で選択し、実行できるようにする。	第三者（インターネットサービスプロバイダ、マネージドセキュリティサービスプロバイダなど）が組織に代わって封じ込めアクションを実行できるようにする。	侵害されたエンドポイントを修復用の仮想ローカルエリアネットワーク（VLAN）に自動的に転送する。	
	RS.MI-02	インシデントが根絶されている。	2	サイバーセキュリティ技術、他の技術（オペレーティングシステム、ネットワークインフラストラクチャデバイスなど）のサイバーセキュリティ機能により、根絶活動を自動的に実行する。	インシデント対応者が根絶活動を手動で選択し、実行できるようにする。	第三者（マネージドセキュリティサービスプロバイダなど）が組織に代わって根絶活動を実行できるようにする。		
	平均		**1.50**					

NISTサイバーセキュリティフレームワーク アセスメントシート

復旧（RC）

平均スコア	**3.17**
インシデント復旧計画実行（RC.RP）	**2.33**
インシデント復旧コミュニケーション（RC.CO）	**4.00**

	カテゴリー	日本語	スコア	実装例 EX1	EX2	EX3	EX4	EX5
インシデント復旧計画実行（RC.RP）								
	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。	2	インシデント対応プロセス中または当該プロセス後に復旧手順を開始する。	復旧に責任を負うすべての個人に、復旧計画および当該計画の各側面を実行するために必要な権限を認識させる。			
	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。	3	インシデント対応計画および利用可能なリソースで定義された基準に基づき、復旧活動を選択する。	組織のニーズとリソースの再評価に基づき、計画された復旧活動を変更する。			
	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。	3	復旧した資産の使用前に、侵害の兆候、ファイルの破損、その他の完全性の問題がないか確認する。				
	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。	2	事業上の影響およびシステム分類の記録（サービス提供の目的など）を使用して、重要なサービスが適切な順序で回復していることを検証する。	システム所有者と協力し、システムの正常な回復、通常運用の復旧を確認する。	回復の妥当性を確認するため、回復したシステムのパフォーマンスをモニタリングする。		
	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。	1	回復した資産について、本番環境での使用に先立ち、インシデントの根本原因の是正および侵害の兆候の有無を確認する。	回復したシステムをオンラインにする前に、講じられた回復措置の正確性と妥当性を確認する。			
	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。	3	インシデントそのもの、実行した対応、復旧活動、習得した教訓を文書にまとめ、事後レポートを作成する。	基準が満たされたら、インシデント復旧終了を宣言する。			
	平均		**2.33**					
インシデント復旧コミュニケーション（RC.CO）								
	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。	4	対応計画および情報共有契約に従って復旧の進捗状況などの復旧情報をセキュアな状態で共有する。	重大インシデントに関する復旧状況および復旧の進捗状況について、上層部に定期的に最新情報を報告する。	組織とそのサプライヤー間におけるインシデント情報共有に関して、契約で定義されたルールとプロトコルを遵守する。	組織とその重要なサプライヤー間におけるクライシスコミュニケーションを調整する。	
	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。	4	データ侵害インシデントから復旧するための組織の侵害通知手順を遵守する。	インシデントからの復旧とインシデント再発防止のために講じられる手順について説明する。			
	平均		**4.00**					