機能	カテゴリ	サブカテゴリ	ソリューション・サービス
	資産管理（ID.AM）：組織が事業目的を達成することを可能にするデータ、職員、デバイス、システム、施設を特定し、事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。	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。	■CyberX PLATFORM 収集したデータから自動でネットワーク内のデバイス一覧を作成します。 ■AssetView エージェントを使用し自動でネットワーク内のデバイス一覧を作成します。
		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。	■CyberX PLATFORM ネットワークを利用するアプリケーションに関しては収集したデータからファームウェア、OSやプロトコルのバージョンを含めて検出します。 ■AssetView エージェントを使用し自動でソフトウェアプラットフォームとアプリケーション一覧を作成します。
		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。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）から自動でネットワークのトラフィックフロー図を作成します。 ■Seceon OTM 収集したデータ（Netflow,ログ）からトラフィックフロー統計図を作成します。 ■McAfee MVISION Cloud （CASB） クラウドベースの情報システム、データの可視化をします。
		ID.AM-4: 外部情報システムの一覧を作成している。	
		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。	■CyberX PLATFORM 収集したデータから自動でネットワーク内のデバイスを分類します。 ■McAfee MVISION Cloud （CASB） クラウドベースの情報システム、データのランキング作成を支援します。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） リスクコントロールの専門家がビジネス目標に応じたリソースの分類を支援いたします。
		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。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家が情報セキュリティ委員会を中心としたサイバーセキュリティ対応態勢の構築を支援いたします。
	ビジネス環境（ID.BE）：自組織のミッション、目標、利害関係者、活動を理解し、優先順位付けを行っている; この情報はサイバーセキュリティ上の役割、責任、リスク管理上の意思決定を伝達するために使用される。	ID.BE-1: サプライチェーンにおける企業の役割を特定し、伝達している	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） リスクコントロールの専門家がビジネス目標に応じたセキュリティ環境の整備を支援いたします。 情報セキュリティの専門家がCSIRTや情報セキュリティ委員会を中心としたサイバーセキュリティ対応組織とプロセスの構築を支援いたします。
		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し、伝達している。	
		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め、伝達している。	
		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。	
		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。	
	ガバナンス（ID.GV）：自組織に対する規制、法律、リスクと、自組織の環境、運用上の要求事項を管理しモニタリングするためのポリシー、手順、プロセスを理解しており、サイバーセキュリティリスクの管理者に伝達している。	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。	
		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。	
		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し、管理している。	
		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。	

特定（ID）	リスクアセスメント（ID.RA）：企業は自組織の業務（ミッション、機能、イメージ、評判を含む）、自組織の資産、個人に対するサイバーセキュリティリスクを把握している。	ID.RA-1: 資産の脆弱性を特定し、文書化している。	■CyberX PLATFORM 収集したデータから自動でネットワークとデバイスのリスクと脆弱性を特定し、PDFで出力します。
		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。	■CyberX PLATFORM CyberX PLATFORMはプロプライエタリなOT専用のセキュリティインテリジェンスを使用します。 ■Seceon OTM Secon OTMは様々なITセキュリティインテリジェンスを使用します。
		ID.RA-3: 内外からの脅威を特定し、文書化している。	■CyberX PLATFORM 収集したデータから自動でアタックベクターを特定し、PDFで出力します。
		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。	■CyberX PLATFORM CyberX PLATFORMは収集したデータから攻撃をシミュレーションし、モデル化します。影響の予測と対応の最適化とランク付けをします。
		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。	■Seceon OTM Secon OTMはプリインストールされたダイナミックスレットモデルとAIにより脅威と影響を評価しまし、アラートのランク付けをします。
		ID.RA-6: リスクに対する対応を定め、優先順位付けしている。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） リスクコントロールの専門家がリスクマップを中心としたリスク戦略の策定を支援いたします。
	リスク管理戦略（ID.RM）：自組織の優先順位、制約、リスク許容度、想定を定め、運用リスクの判断に利用している。	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、管理され、承認されている。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） リスクコントロールの専門家がリスクマップを中心としたリスク戦略の策定を支援いたします。
		ID.RM-2: 自組織のリスク許容度を決定し、明確にしている。	
		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。	
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks. サプライチェーンのリスク管理（ID.SC）: 自組織の優先順位、制約、リスク許容値、および仮定が、サプライチェーンリスクの管理に関連するリスク決定を支援するために確立され使用される。 自組織がサプライチェーンのリスクを特定、評価、管理するプロセスを確立し、実施している。	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders サイバーサプライチェーンのリスク管理プロセスは、組織のステークホルダーによって特定され、確立され、評価され、管理され、合意される。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） リスクコントロールの専門家がビジネス目標に応じたサプライチェーンのリスク管理を支援いたします。
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process 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を使用して、情報システム、コンポーネント、およびサービスのサプライヤと第三者パートナーを特定し優先順位付けて評価する。	
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. サプライヤーと第三者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とサイバーサプライチェーンリスクマネジメント計画の目的に合うように設計された適切な措置を実施するために使用される。	
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. サプライヤとサードパーティのパートナーが契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価される。	

		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers 応答と復旧の計画とテストにサプライヤとサードパーティのプロバイダを含まれる。	
	アクセス制御（PR.AC）：資産および関連施設へのアクセスを、承認されたユーザ、プロセス、またはデバイスと、承認された活動およびトランザクションに限定している。	**PR.AC-1: 承認されたデバイスとユーザの識別情報と認証情報を管理している。**	■CyberX PLATFORM CyberX PLATFORMは管理者のインプットを基にしてデバイスの承認・非承認の管理をサポート可能です。 ■Password Manager Pro 厳重な管理が要求される特権IDを安全に管理・運用します。
		PR.AC-2: 資産に対する物理アクセスを管理し、保護している。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がもつベストプラクティスにより、フィジカルセキュリティの向上を支援いたします。
		PR.AC-3: リモートアクセスを管理している。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からリモートアクセスのアクティビティを特定可能です。 ■Seceon OTM 収集したデータ（Netflow,ログ）からリモートアクセスのアクティビティを特定可能です。 ■McAfee MVISION Cloud （CASB） クラウドベースの情報システム、データのリモートアクセスを管理します。 ■Password Manager Pro リモートアクセスに使用する特権IDを安全に管理・運用します。
		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。	■Paloalto NGFW 様々なACLによるネットワークの分離が可能です。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家が最適なアクセスコントロールとネットワークのゾーニング実施を支援いたします。
		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.AC-6: Identities are proofed and bound to credentials and asserted in interactions アイデンティティの証明と資格情報へのバインドが操作に表れる。	■Password Manager Pro 特権IDの利用を監視・監査可能です。エビデンスの取得も可能です。
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) ユーザー、デバイス、およびその他の資産が、取引のリスク（例えば、個人のセキュリティおよびプライバシーのリスクおよびその他の組織的リスク）に見合った認証を受けている。（例えば、単一要因、複数要因）	■Password Manager Pro シチュエーションに合せ特権IDを安全に管理・運用します。異常検出時のアラート発報も可能です。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がコストパフォーマンスを考慮した最適な認証ソリューションの導入を支援いたします。
	意識向上およびトレーニング（PR.AT）：自組織の職員およびパートナーに対して、関連するポリシー、手順、契約に基づいた、情報セキュリティに関連する義務と責任を果たせるようにするために、サイバーセキュリティ意識向上教育と、十分なトレーニングを実施している。	**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。**	■セキュリティサービス（トレーニング） 情報セキュリティの専門家が目的や対象に応じたセキュリティトレーニングのプログラム策定及び、トレーニングマテリアルの作成を支援いたします。
		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-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-4: 上級役員が役割と責任を理解している。	
		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。	

防御（PR）	データセキュリティ（PR.DS）：情報と記録（データ）を情報の機密性、完全性、可用性を保護するために定められた自組織のリスク戦略に従って管理している。	PR.DS-1: 保存されているデータを保護している。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動でデータ保護に影響のあるアクティビティを検出します。 収集したデータ（Netflow,ログ）からAIが自動でデータ保護に影響のあるアクティビティを検出します。 ■McAfee MVISION Cloud （CASB） クラウドベースのシステムに対しデータ保護を支援します。
		PR.DS-2: 伝送中のデータを保護している。	
		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。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がデータのライフサイクルポリシー策定を支援いたします。
		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.DS-5: データ漏えいに対する保護対策を実施している。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動でデータ漏えいを防ぎます。 ■Seceon OTM 収集したデータ（Netflow,ログ）からAIが自動でデータ漏えいを防ぎます。 ■McAfee MVISION Cloud （CASB） クラウドベースのシステムに対しデータ漏えいを防ぎます。
		PR.DS-6: ソフトウェア、ファームウェア、および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。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動でファームウェアの改ざんを検知します。 ■McAfee Application Control ハッシュ情報を使用しリソースの完全性を担保いたします。
		PR.DS-7: 開発・テスト環境を実稼働環境から分離している。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がもつベストプラクティスにより、ステージング環境構築を支援いたします。
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity インテグリティ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る。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がもつベストプラクティスにより、インテグリティチェックプロセスの構成を支援いたします。
		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。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動でシステムのベースラインを作成します。 ■Seceon OTM 収集したデータ（Netflow,ログ）からAIが自動でシステムのベースラインを作成します。 ■McAfee MVISION Cloud （CASB） クラウドシステムの利用にかんするベースライン作成を支援可能です。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がもつベストプラクティスにより、システム設定のベースライン構成を支援いたします。

	情報を保護するためのプロセスおよび手順（PR.IP）：（目的、範囲、役割、責任、経営コミットメント、組織間の調整を扱う）セキュリティポリシー、プロセス、手順を維持し、情報システムと資産の保護の管理に使用している。	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。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がもつベストプラクティスにより、システム開発ライフサイクルの導入を支援いたします。
		PR.IP-3: 設定変更管理プロセスを導入している。	■McAfee EPO （Change Control） McAfeeの統合セキュリティコンソールEPOと連携したChange Controlで未承認のシステム変更を防止。オートメーション規制コンプライアンス制御 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がもつベストプラクティスにより、システムの設定変更管理プロセス導入を支援いたします。
		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。	■運用サービス システム運用の専門家がもつベストプラクティスにより、バックアップ運用を支援いたします。
		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。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動でファームウェアの改ざんを検知します。 ■McAfee MVISION Cloud （CASB） クラウドベースのデータ保護を支援します。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がもつベストプラクティスにより、データライフサイクル管理の導入と運用を支援いたします。
		PR.IP-6: ポリシーに従ってデータを破壊している。	
		PR.IP-7: 保護プロセスを継続的に改善している。	
		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。	
		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）を実施し、管理している。	■セキュリティサービス by DRチーム リスクコントロール専門家と情報セキュリティの専門家がもつベストプラクティスにより、ディザスタリカバリプランの計画を支援し、DRの専門チームが運用を支援いたします。
		PR.IP-10: 対応計画と復旧計画をテストしている。	
		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。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がもつベストプラクティスにより、人事が持つべきセキュリティプロセスを確認・評価いたします。
		PR.IP-12: 脆弱性管理計画を作成し、実施している。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動でシステムの脆弱性を検出します。 ■Rapid7 nexpose アクティブスキャンによりシステムの脆弱性を検出・管理します。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がもつベストプラクティスにより、 脆弱性管理計画を支援いたします。
	保守（PR.MA）：産業用制御システムと情報システムのコンポーネントの保守と修理をポリシーと手順に従って実施している。	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。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）から保守アクティビティを検出・記録可能です。 ■Seceon OTM 収集したデータ（Netflow,ログ）からITの保守アクティビティを検出・記録可です。 ■Password Manager Pro 保守時に使用する特権IDの利用を監視・監査可能です。エビデンスの取得も可能です。
		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。	
		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、文書化し、そうした記録を実施して、レビューしている。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）を記録可能です。 ■Seceon OTM 収集したデータ（Netflow,ログ）を記録可能です。 ■Password Manager Pro 保守時に使用する特権IDの利用を監視・監査可能です。エビデンスの取得も可能です。

	保護技術（PR.PT）：関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティと耐性・復旧力を確保するための、技術的なセキュリティソリューションを管理している。	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、そうした媒体の使用を制限している。	■AssetView エージェントを使用し取り外し可能な外部記録媒体の使用を管理・制限可能です。
		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。	■McAfee Application Control ホワイトリストベースでリソースへのアクセス制御が可能です。 ■AssetView エージェントを使用し取り外し可能な外部記録媒体の使用を管理・制限可能です。
		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。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIがネットワークの異常を検知します。 ■Seceon OTM 収集したデータ（Netflow,ログ）からAIがネットワークの異常を検知します。 ■McAfee MVISION Cloud （CASB） クラウドベースのネットワークデータ移動を保護します。 ■Paloalto NGFW L2～L7の情報を使用しリソースへのアクセス制御が可能です。
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations 正常および異常な状況で回復力要件を達成するためのメカニズム（フェールセーフ、負荷分散、ホットスワップなど）が実装されている。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） セキュリティソリューションの専門家がもつベストプラクティスにより、セキュリティメカニズムの可用性を確認・評価いたします。
	異常とイベント（DE.AE）：異常な活動をタイムリーに検知し、イベントがもたらす可能性のある影響を把握している。	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し、管理している。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動でシステムのベースラインを作成します。 ■Seceon OTM 収集したデータ（Netflow,ログ）からAIが自動でシステムのベースラインを作成します。
		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。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動で検知したイベントを分析します。 ■Seceon OTM 収集したデータ（Netflow,ログ）からAIが自動で検知したイベントを分析します。
		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。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動で検知したイベントを関連付けます。 ■Seceon OTM 収集したデータ（Netflow,ログ）からAIが自動で検知したイベントを関連付けます。
		DE.AE-4: イベントがもたらす影響を特定している。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動で検知したイベントの影響を特定します。 ■Seceon OTM 収集したデータ（Netflow,ログ）からAIが自動で検知したイベントの影響を特定します。
		DE.AE-5: インシデント警告の閾値を定めている。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが検知したアラートを発報します。 ■Seceon OTM 収集したデータ（Netflow,ログ）からAIが検知したアラートを発報します。

検知（DE）	セキュリティの継続的なモニタリング(DE.CM): サイバーセキュリティイベントを検知し、保護対策の有効性を検証するために、能 カテゴリー サブカテゴリー 参考情報情報システムと資産を離散間隔でモニタリングしている。	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。	■CyberX PLATFORM 常にデータ（パケットキャプチャ）をモニタリングしています。 ■Seceon OTM 常にデータNetflow,ログ）をモニタリングしています。
		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。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家がモニタリングすべき物理環境と個人のアクティビティの特定とソリューション導入を支援いたします。 ■Password Manager Pro 個人が使用する特権IDの利用を監視・監査可能です。エビデンスの取得も可能です。
		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-4: 悪質なコードを検出できる。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動で悪質なコードを検出します。 ■Seceon OTM 収集したデータ（Netflow,ログ）からAIがAIが自動で悪質なコードを検出します。 ■McAfee ENS エージェントを使用しエンドポイント上で悪質なコードを検出します。 ■Cisco AMP エージェントを使用しエンドポイント上で悪質なコードを検出します。 ■Carbon Black エージェントを使用しエンドポイント上で悪質なコードを検出します。
		DE.CM-5: 悪質なモバイルコードを検出できる。	
		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。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） リスクコントロール専門家と情報セキュリティの専門家が外部サービスプロバイダの評価計画を支援いたします。
		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。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIがネットワークのモニタリングをします。 ■Seceon OTM 収集したデータ（Netflow,ログ）からAIがネットワークのモニタリングをします。 ■McAfee SIEM 様々なログを使用したアクティビティのモニタリングが可能です。 ■Password Manager Pro 特権IDの利用を監視・監査可能です。エビデンスの取得も可能です。 ■AssetView エージェントを使用しエンドポイント上のソフトウェアの監視をします。
		DE.CM-8: 脆弱性スキャンを実施している。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）からAIが自動でシステムの脆弱性を検出します。 ■Rapid7 nexpose アクティブスキャンによりシステムの脆弱性を検出・管理します。 ■脆弱性診断サービス スポットもしくは定期的なサービスベースでの脆弱性診断を提供します。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） 情報セキュリティの専門家が脆弱性スキャンの実施を支援いたします。

	検知プロセス（DE.DP）：異常なイベントをタイムリーに、かつ正確に検知するための検知プロセスおよび手順を維持し、テストしている。	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。	■CyberX PLATFORM 収集したデータ（パケットキャプチャ）を使用して攻撃検知プロセスの改善が可能です。 ■Seceon OTM 収集したデータ（Netflow,ログ）を使用して攻撃検知プロセスの改善が可能です。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） リスクコントロール専門家と情報セキュリティの専門家が、攻撃検知プロセスの評価計画を支援いたします。
		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.DP-3: 検知プロセスをテストしている。	
		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.DP-5: 検知プロセスを継続的に改善している。	
対応（RS）	対応計画（RS.RP）：検知したサイバーセキュリティイベントにタイムリーに対応できるよう、対応プロセスおよび手順を実施し、維持している。	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。	■CyberX PLATFORM 検出したイベントはレポーティング可能です。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） CISIRT、情報セキュリティ委員会等、最適なインシデント対応組織の立ち上げと運用をサポートいたしします。
	伝達（RS.CO）：法執行機関からの支援を必要に応じて得られるよう、内外の利害関係者との間で対応活動を調整している。	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。	
		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-3: 対応計画に従って情報を共有している。	
		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.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。	
	分析 (RS.AN): 適切な対応を確実にし、復旧活動を支援するために、分析を実施している。	RS.AN-1: 検知システムからの通知を調査している。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） CISIRT、情報セキュリティ委員会等、最適なインシデント対応組織の立ち上げと運用をサポートいたしします。
		RS.AN-2: インシデントがもたらす影響を把握している。	
		RS.AN-3: フォレンジクスを実施している。	■CyberX PLATFORM フォレンジクスに必要なデータ（パケットキャプチャ）を収集・記録します。 ■Seceon OTM フォレンジクスに必要なデータ（Netflow,ログ）を収集・記録します。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） パートナー企業と連携しフォレンジクスサービスと体制構築をサポートいたします。
		RS.AN-4: 対応計画に従ってインシデントを分類している。	■CyberX PLATFORM インシデントは自動で分類されます。 ■Seceon OTM インシデントは自動で分類されます。
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) 組織に開示された脆弱性を社内外のソース（例えば、内部テスト、セキュリティ速報、セキュリティ研究者）から受信し、分析し、対応するためのプロセスが確立されている。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） CISIRT、情報セキュリティ委員会等、最適なインシデント対応組織の立ち上げと運用をサポートいたしします。

	低減（RS.MI）：イベントの拡大を防ぎ、その影響を緩和し、インシデントを根絶するための活動を実施している。	RS.MI-1: インシデントを封じ込めている。	■CyberX PLATFORM 検知したアラートをFWに連携し通信を遮断します。 ■Seceon OTM 検知したアラートをFWに連携し通信を遮断し不正なアカウントは停止します。 ■McAfee ENS エージェントを使用しエンドポイント上でマルウェアを駆除します。 ■Cisco AMP エージェントを使用しエンドポイント上でマルウェアを駆除します。
		RS.MI-2: インシデントを低減している。	■Carbon Black エージェントを使用しエンドポイント上でマルウェアを駆除します。 ■McAfee MVISION Cloud （CASB） クラウドベースのインシデントの封じ込め・低減が可能です。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） CISIRT、情報セキュリティ委員会等、最適なインシデント対応組織の立ち上げと運用をサポートいたしします。
		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。	■CyberX PLATFORM 検出した脆弱性をレポーティングします。 ■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） CISIRT、情報セキュリティ委員会等、最適な脆弱性ハンドリングをサポートいたしします。
	改善（RS.IM）：現在と過去の意思決定／対応活動から学んだ教訓を取り入れることで、自組織の対応活動を改善している。	RS.IM-1: 学んだ教訓を対応計画に取り入れている。	■セキュリティサービス by CSIチーム（オーダメイドコンサルティング） CISIRT、情報セキュリティ委員会等、最適なインシデント対応組織の立ち上げと運用をサポートいたしします。
		RS.IM-2: 対応戦略を更新している。	
復旧（RC）	復旧計画（RC.RP）：サイバーセキュリティイベントによる影響を受けたシステムや資産をタイムリーに復旧できるよう、復旧プロセスおよび手順を実施し、維持している。	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。	
	改善（RC.IM）：学んだ教訓を将来的な活動に取り入れることで、復旧計画およびプロセスを改善している。	RC.IM-1: 学んだ教訓を復旧計画に取り入れている。	
		RC.IM-2: 復旧戦略を更新している。	
	伝達（RC.CO）：コーディネーティングセンター、インターネットサービスプロバイダ、攻撃システムのオーナー、被害者、その他のCSIRT、ベンダなどの、内外の関係者との間で復旧活動を調整している。	RC.CO-1: 広報活動を管理している。	
		RC.CO-2: イベント発生後に評判を回復している。	
		RC.CO-3: 復旧活動について内部利害関係者と役員、そして経営陣に伝達している。	