NISTサイバーセキュリティのフレームワーク(CSF):IvantiのソリューションのCSF統制へのマッピング

サイバー犯罪者が使用する最も一般的な手法は、過去数年間変わっておらず、フィッシングとランサムウェアが、毎年、上位3つのうちの2つを占め続けています。これらの攻撃は進化し続けており、現在、それには以下の使用が含まれています：

- 機械学習人工知能（AI）
- 自動化
- 既知のゼロデイ脆弱性に対する連鎖的エクスプロイト
- NSOグループによって開発されたゼロクリック・エクスプロイト・キット
- ファイルレスマルウェア
- 「サイバー犯罪対策サービス」ビジネスモデル

これらの進化は、サイバー犯罪者がターゲットの一歩先を行き、企業が立ち上げるほとんどのサイバー防御を打ち負かすのに役立ちます。

世界的なパンデミックによって加速したEverywhere Workplace へのシフトは、サイバーリスクと脅威の状況を変え、特にデータのプライバシーとその保護を取り巻く状況を拡大しました。

Ivanti は、今日の脅威と戦うために、3 つのサイバーセキュリティのフレームワークのうち の1 つ以上を採用した深層防御型サイバーセキュリティ戦略を推奨しています。

- NISTサイバーセキュリティのフレームワーク（CSF）)
- インターネットセキュリティセンター(CIS) クリティカル・セキュリティControls バージョン8
- ゼロトラスト・セキュリティ・アーキテクチャー

解決策は、単純にサイバー犯罪者の前にできるだけ多くの障害物を置くことです。その結果、サイバー犯罪者は諦めて、適切なセキュリティ対策が施されていない他の標的を探す可能性が高くなります。

このホワイトペーパーで、NIST サイバーセキュリティのフレームワークについて詳しく説明し、Ivanti の自社製品がその中の推奨事項にどのように対応しているかを紹介しています。

NISTサイバーセキュリティのフレームワークとは何でしょう？

国立標準技術研究所（NIST）は、1901年に設立され、米国商務省に属しています。NISTの情報技術研究所はサイバーセキュリティのフレームワークをいくつも開発しましたが、弊社は、それらのうちの最も一般的な3つに焦点を当てています。

- NISTサイバーセキュリティフレームワーク（CSF）– サイバーセキュリティの全てのフレームワークの中の最高標準
- NIST特別刊行物800-53
- NIST特別刊行物800-171

2014年2月にリリースされた、NIST サイバーセキュリティフレームワークのバージョン1.0は、「大統領大統領令（EO）13636、重要なインフラのサイバーセキュリティの改善」に対応して策定されました。

このフレームワークは、当初、発電および配電プラント、原子力施設、輸送および通信インフラ、水処理、公衆衛生、食品、農業などの重要なインフラを保護するために使用することを目的としていました。

バージョン1.1は、民間部門の業界からの情報提供と協力によって、2018年4月にリリースされました。このバージョンは、公共部門向けのコンピューターおよび情報技術の標準とガイドラインを提供するだけでなく、民間部門でも広く使用されており、サイバーセキュリティプログラムを開始または改善しようとする全ての企業が、その原則を実行できるものです。

NISTは、最近では2021年9月にNISTIR8374の草稿をリリースしました。これは、企業がより広範なNISTサイバーセキュリティフレームワークの状況の中で、ランサムウェア攻撃から身を守るための基本的な予防ガイドラインを提供するものです。

このフレームワークは、リスクと保護が必要な資産を特定するために、サイバーセキュリティの優良事例を体系的に提示しています。そして、リスクの検出、脅威への対応、サイバーセキュリティインシデント発生時の資産の修復など、企業が守るべきセキュリティ管理を挙げています。各機能の下には1つのカテゴリが含まれており、さらに下の階層に移動すると、守るべきガイドラインとして多くのサブカテゴリがあります。

NISTサイバーセキュリティフレームワークの機能の詳細

Cybersecurity Framework Coreでは、サイバー防衛戦略の一般構造に沿った機能が列挙されています。

特定	防御	検知	対応	復旧
資産管理	身元管理とアクセス制御	異常とイベント	対応計画	復旧計画
ビジネス環境	意識向上と研修	セキュリティの継続的な監視	コミュニケーション	改善
ガバナンス	データセキュリティ	検知プロセス	分析	コミュニケーション
リスクアセスメント	情報を保護するためのプロセスおよび手順		低減	
リスク管理戦略	保守		改善	
サプライチェーンリスク管理	保護技術			

特定

資産とソリューションの包括的なインベントリを特定して維持することは、効果的なサイバーセキュリティプログラムを構築するための最初のステップです。この機能には、企業データにアクセスする企業ソフトウェアとハードウェアシステムの正確なインベントリーが必要です。

エンタープライズソフトウェアのインベントリ	ハードウェアシステムのインベントリ
ソフトウェアコンポーネント	ネットワーク
ライブラリ	サーバー
OSとバージョン	デスクトップ
アプリケーション	モバイルデバイス
ソフトウェア部品表（SBOM）	

次に、企業は、以下のことを行わなければいけません。すなわち、

- すべてのシステム内およびシステム間の脅威、脆弱性、弱点を特定すること
- 収集、使用、保存されるデータ、およびネットワークフローを特定して文書化すること
- サイバーセキュリティポリシー、アクセス制御、全従業員の役割と責任の確立など、包括的なリスク管理戦略を策定して維持すること

防御

防御には、機密データを適切に保護するための社内プロセスの構築と技術的統制の実施が含まれます。これらの統制には、以下が含まれます（但し、必ずしもこれらに限りません）：

- 強力な多要素認証（MFA）の実施
- 保存中、使用中、転送中のデータの暗号化などの保護技術を採用すること
- 定期的なデータバックアップを実行すること。これには、オフラインストレージも含まれる
- 次世代ファイアウォールとクラウドアクセスセキュリティブローカー（CASB）などのポリシー実行ポイントを有効化すること
- インテリジェントなパッチ管理、モバイルデバイスの脅威防御、サーバーやラップトップ、デスクトップのためのウイルス対策など、エンドポイントセキュリティ製品を導入して定期的に更新すること
- 信頼できるユーザーだけでなく、信頼できるデバイス、アプリ、ネットワークソース（場所）、および時間に対しても、堅牢な認証方法と承認方法を採用した堅固なコンテキスト条件付きアクセス制御を活用すること
- 包括的で最新のセキュリティに関する教育研修を従業員に対して実施すること

検出します

データ侵害、ランサムウェア、ビジネスの中断、高度持続的脅威（APT）につながる可能性のあるサイバーセキュリティインシデントを検出することは、どの組織にとっても重要なことです。「検出」機能には、組織がリスクや脅威が発生したときに確実に検知できるよう、定期的にテストされる管理プロセスや手順を導入・開発することが含まれます。

このプロセスには、以下のような自動化と機械知能の活用が含まれます：

- ネットワークインスツルメンテーション
- システムログのモニタリング
- エンドポイント間のデータの流れ
- ストレージ（オンプレミスまたはクラウド）
- データベース
- ネットワーク

包括的な脅威検出戦略の一部には、サイバーセキュリティ・チーム、パートナー、統治機関とのコミュニケーション・チャネルと運用プロトコルの確立が含まれます。

対応

対応機能は、企業が、リスクと脅威のインシデントに迅速かつ効果的に対応できるよう準備することに重点を置いています。これには、内部および外部の利害関係者との調整に加えて、対応プロセスと手順の文書化と定期的なテストの両方が含まれます。

自動応答制御は、以下のような技術的イノベーションによっても実施することができます。

- アウトバウンドトラフィックの検出
- ネットワークのセグメンテーション
- ソフトウェア定義の境界
- 脆弱性とリスクベースのパッチ管理
- 環境、ネットワーク、インターネットの状態やリスクの状況に基づいて、権限やセキュリティポリシーを変更できる動的な属性ベースのアクセス制御ポリシー

復旧

復旧機能には、事業継続の準備と計画、事故前の復旧と復旧力のテスト、事故後の根本原因の分析と教訓の文書化が含まれます。

また、この機能は、社内外のステークホルダーとのコミュニケーションや、広報、風評管理も行います。

復旧の優良事例の重要な技術的要素は、ITIL（情報技術インフラライブラリ（Information Technology Infrastructure Library））のプロセスの適切なレベルに適合した以下のプロセスを上手く統合することです。

- サービス管理
- 構成と変更管理
- リリースの自動化
- テスト
- 検証

Ivantiは、今日の脅威に対抗するために、多層防御のサイバーセキュリティ戦略を常に推奨しています。　企業がサイバー犯罪者の前に置く障害が多ければ多いほど、彼らが諦めて、適切なセキュリティ管理を備えていない他のターゲットを探す可能性は高くなります。

ivanti

機能	カテゴリ	Ivantiの製品マッピング
特定	**資産管理** 企業がビジネス目的を達成するためのデータや人員、デバイス、システム、および設備は、企業の目標およびリスク戦略に対する相対的な重要性に基づいて特定されて管理されます。	**Ivanti Neurons for Discovery** は、すべてのIT資産の正確なリアルタイムの可視性を提供します。これには、ハードウェアシステム、ソフトウェア、データ、サービス、人員目録、および資産を特定し、追跡するためのアクティブスキャンおよびパッシブスキャンを使用したそれらの管理も含まれます。(ID.AM-1、ID.AM-2、およびID.AM-5) **Ivanti Neurons for Spend Intelligence** は、ソフトウェアの使用状況、ソフトウェア構成のドリフト、およびソフトウェアの保守の終了を即座に可視化し、ソフトウェアの環境とアプリ資産のインベントリに関するインサイトを提供します。(ID-AM-2) **Ivanti IT Asset Management (ITAM)** は、ハードウェア、サーバー、クライアント、仮想、クラウド、またはソフトウェアの資産のライフサイクル全体を通して、正確なインベントリ情報と実用的なインサイトを維持します。(ID.AM-1およびID.AM-2) オンプレミスのソリューションに関して、**Ivanti Endpoint Manager (EPM)** は、ハードウェアシステム、ソフトウェア、データ、サービス、人員インベントリ、およびアクティブスキャンとパッシブスキャンを使用した資産の識別と追跡を使用した管理など、IT資産の正確なリアルタイムの可視性も提供します。(ID.AM-1、ID.AM-2、およびID.AM-5) さらに、**Ivanti Neurons for Unified Endpoint Management (UEM)** および **Ivanti Endpoint Manager Mobile (EPMM)**は、登録されているモバイルデバイス、デスクトップクライアント、およびインストールされているすべてのソフトウェアアプリのインベントリを管理します。また、モバイルデバイスとクライアントが常に管理されていることを保証し、会社のセキュリティポリシーおよびプライバシーポリシーへの準拠を強制します。これらの管理されたデバイスとそのコンテンツは、重要性と業務上の価値に基づいて分類されます。(ID.AM-1およびID.AM-2) 追加のIvanti製品: **Neurons for Secure Access (NSA)** (ID.AM-1) **Ivanti Network Access Control (NAC)** (ID.AM-1) **Ivanti Security Controls (ISEC)** (ID.AM-2) **Ivanti Patch for MEM (Microsoft Endpoint Manager)** (ID.AM-2) **Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)** (ID.AM-1 および ID.AM-5) **Ivanti Neurons for App Security Orchestration & Correlation (ASOC)** (ID.AM-2 および ID.AM-5)
	ビジネス環境 企業の使命、目的、利害関係者、および活動は、理解されて優先順位が付けられます。そして、この情報は、サイバーセキュリティの役割、責任、およびリスク管理の決定を知らせるために使用されます。	
	ガバナンス サイバーセキュリティの管理者は、企業の規制、法律、リスク、環境、および運用上の要件を管理および監視するためのポリシー、手順、およびプロセスを理解し、通知を受けます。	

機能	カテゴリ	Ivantiの製品マッピング
特定	**リスクアセスメント** 企業は、ミッション、機能、イメージまたは風評などの企業運営や、企業的資産および個人に対するサイバーセキュリティのリスクを理解しています。	**Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)** は、敵対的なリスクに基づいた修復の優先順位付けを行うことによって、リスクエクスポージャーに対するインサイトを自動的に提供します。このソリューションは、資産の弱点と脆弱性を特定して文書化します。脅威と脆弱性に関する情報は、情報共有フォーラムとソースから受け取ります。潜在的なビジネスへの影響と傾向も特定されます。これによって、脅威、脆弱性、傾向、およびインパクトを使用してリスクを判断し、自動パッチのために適切な対応を特定して優先順位を付けます。(ID.RA-1、ID.RA-2、ID.RA-4、ID-RA-5、およびID-RA-6)。 **Ivanti Neurons for Patch Management** は、すべてのエンドポイントで欠落しているパッチを特定することによって、エンドポイントの弱点と脆弱性をスキャンします。これは、Common Vulnerabilities and Exposures(CVE)データをフィルタリングしてインポートし、インテリジェントなパッチ戦略で使用する機能を備えています。(ID.RA-1) **Ivanti Neurons for GRC (Governance Risk and Compliance)** Ivanti Neurons for GRC (Governance Risk and Compliance)は、内部および外部の脅威を特定して文書化し、潜在的なビジネスへの影響と可能性を明確化します。(ID.RA-3 および ID.RA-4)
	リスク管理戦略 運用リスクに関する意思決定をサポートするために、企業の優先順位、制約、リスク許容度、および仮定を設定し、それらを使用します。	
	サプライチェーンリスク管理 サプライチェーンリスクの管理に関連するリスクの意思決定をサポートするために、企業の優先順位、制約、リスク許容度、および仮定を設定し、それらを使用します。企業は、サプライチェーンのリスクを特定、評価、管理するために、プロセスを確立して実行しました。	**Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)** は、アプリやウェブサービスを含め、ITおよびクラウドインフラにおける実際のエクスプロイトのサイバーリスクを特定します。特許取得済みのVulnerability Risk Rating(VRR)エンジンを使用して、最もリスクが高い脆弱性と弱点に優先順位を付けることもできます。VRRは、ある脆弱性がもたらすリスクを0〜10の数値で表したものです。リスクが高いほど、VRRも高くなります。企業の利害関係者は、サイバーサプライチェーンのリスク管理プロセスに対して、特定し、確立し、評価し、管理し、同意しています。(ID.SC-1) **Ivanti Neurons for IT Asset Management (ITAM)** は、IT資産データを統合し、サイバーサプライチェーンのリスク評価プロセスを使用して、重要な情報システムやコンポーネント、サービスのサプライヤーとパートナーを特定し、優先順位付けし、評価できます。お客様の社内のサプライチェーン資産を、そのライフサイクルを通して追跡、構成、最適化し、戦略的な管理を実現します。(ID.SC-2)

機能	カテゴリ	Ivantiの製品マッピング
防御	**身元管理とアクセス制御** 物理的および論理的な資産と関連施設へのアクセスは、許可されたユーザー、プロセス、およびデバイスに制限されています。また、許可された活動や取引への不正アクセスのリスク評価に基づいて管理されます。	**Ivanti Access を備えた Ivanti Neurons for Unified Endpoint Management (UEM)**は、既存のIDプロバイダーと統合し、信頼できるユーザー、デバイス、アプリケーション、ネットワーク、コンテキストのルールに基づいて条件付きアクセスを実施できますし、また、Ivanti Zero Sign-Onは、承認されたデバイス、ユーザー、およびプロセスの身元情報と資格情報の発行、検証、取り消し、および監査を管理します。(PR.AC-1) **Ivanti Neurons for Zero Trust Access、Ivanti Connect Secure、および Ivanti Tunnel** は、オンプレミス、データセンター、クラウド(SaaSベース)のリソースへの安全なリモートアクセスを管理して提供します。ユーザー、デバイス、アプリ、ネットワーク、時間、および場所の認証は、より強力で適応的な要素を使用した多要素認証(MFA)に基づいて行われます。(PR.AC-3 および PR.AC-7) また、**Ivanti Network Access Control (NAC)** は、南北だけでなく東西のネットワーク・データ・トラフィックに対しても、ネットワークの完全性を確保するためにマイクロ・セグメンテーションを実施できます。(PR.AC-5 および PR.AC-7) **Ivanti Application Control with Privilege Management** は、最小特権と職務分離の原則を取り入れながら、アクセス許可を管理します。RBAC(Role-Based Access Control)を使用して、保護された資産へのアクセスを制御します。(PR.AC-4)
	意識向上と研修 企業の担当者とパートナーには、サイバーセキュリティ意識の教育を実施し、関連するポリシー、手順、および契約に基づいたサイバーセキュリティ関連の義務と責任を実行するための研修を提供します。	
	データセキュリティ 情報と記録(データ)は、情報の機密性、完全性、および可用性を保護するための企業のリスク戦略に基づいて管理されます。	**Ivanti Neurons for Unified Endpoint Management (UEM)** は、iOS、iPadOS、Androidモバイルデバイス上でファイルベースの暗号化を確認、有効化、適用することが可能であり、また、保存データを保護するために、Windows用のBitLockerとmacOSクライアント用のFileVaultを使用したフルディスクの暗号化も行います。また、ワイヤレスネットワーク用のWPA3-個人(同等の安全な認証)および企業を有効にすることもできます。(PR.DS-1、PR.DS-2、PR.DS-4、およびPR-DS-6) オンプレミス展開の場合、**Ivanti Endpoint Manager Mobile(EPMM)** は、iOS、iPadOS、およびAndroidモバイルデバイスでファイルベースの暗号化を確認、有効化、および適用することが可能であり、また、保存データを保護するためにWindows用のBitLockerとmacOSクライアント用のFileVaultを使用したフルディスクの暗号化も行います。また、ワイヤレスネットワーク用のWPA3-個人(同等の安全な認証)および企業を有効にすることもできます。(PR.DS-1、PR.DS-2、PR.DS-4、およびPR-DS-6) **Ivanti Neurons for Zero Trust AccessとIvanti Connect Secure** は、Transport Layer Security version 1.3による強力な暗号化、ならびにユーザー行動、分析、リスクの執行、多要素認証と適応型認証(MFA)および承認、デバイスポスチャー、信頼できるアプリ、アクセスコンテキスト(場所と時間)の制御と共に、転送中のデータを保護します。Lookout Cloud Access Security Broker(CASB)およびSWG(安全なウェブゲートウェイ)ソリューションとの統合、具体的にAPI統制の展開は、インサイダーの脅威とデータ漏洩に対して役立ちます。(PR.DS-2 および PR.DS-5)

機能	カテゴリ	Ivantiの製品マッピング
防御		**Ivanti Neurons for ITAM (IT Asset Management)** および **Ivanti Neurons for ITSM (IT Service Management)** は、削除、転送、廃棄からライフサイクルを通して、デジタル資産を正式に管理し、機密データを使用してシステムを追跡します。(PR.DS-3) **Ivanti Neurons for Unified Endpoint Management (UEM)**, **Ivanti Neurons for Healing, Ivanti Neurons Workspace with Digital Experience Score** (DEX Score) は、管理対象のシステムが、必ず十分な容量を確保・維持できるようにします。(PR.DS-4) **Ivanti RBVM for Applications** は、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用される、完全性チェック構造を実装しています。(PR.DS-6) Also, **Ivanti Neurons for Zero Trust Access** は、ユーザーとアプリに最小限の特権を適用することにより、本番環境とは別に、お客様の開発環境とテスト環境の小区分化を調整します。(PR-DS-7)
	情報保護のプロセスおよび手順 目的、範囲、役割、責任、マネジメントのコミットメント、および企業的エンティティ間の調整に対処するためのプロセスと手順のセキュリティポリシーは、情報システムと資産の保護を管理するために保守され、使用されます。	**Ivanti Endpoint Security (EPS) for Endpoint Manager (EPM), Neurons for Unified Endpoint Management (UEM)** および **Ivanti Neurons for Healing** は、ベースライン構成と構成変更を組み込んで、情報技術と産業用制御システムを作成および保守します。(PR.IP-1) また、**Ivanti Neurons for ITSM (IT Service Management)** は、構成変更管理プロセスの文書化と発券を容易にします。(PR. IP-3) **Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)** は、脆弱性対応計画を管理および実装するためのツールを提供します。(IP-12)
	保守 産業的統制と情報システムコンポーネントの保守および修理は、ポリシーと手順に基づいて実行されます。	**Ivanti IT Service Management (ITSM)** および **Ivanti Neurons for Healing** は、承認および管理されたツールを提供して企業の資産を保全・保守し、タイムリーに実行してログ記録を取ります。(PR. MA-1) さらに、**Ivanti Endpoint Manager (EPM), Ivanti Neurons Workspace** および **Ivanti Neurons for Healing** は、不正アクセスを防止するための承認、ログ記録、およびタイムリーに実行される企業資産の遠隔保守ツールを提供します。(PR.MA-2)
	保護技術 関連するポリシー、手順、合意（契約）に準拠したシステムと資産のセキュリティと復元力を確かなものにするために、技術的なセキュリティソリューションが管理されます。	**Endpoint Security (EPS) for Manager (EPM)** および **Ivanti Application Control and Ivanti Neurons for Unified Endpoint Management (UEM)** は削除可能なメディアを保護し、会社のセキュリティおよびプライバシーポリシーに従ってその使用が制限されていることを確認します。(PR.PT-2) また、**Endpoint Security (EPS) for Endpoint Manager (EPM), Ivanti User Workspace Manager, Ivanti Security Controls, Ivanti Neurons for Zero Trust Access, Ivanti Connect Secure** および特権管理を備えた **Ivanti Application Control** は エンドユーザーに不可欠な機能のみを提供するようにシステムを構成することにより、最小機能の原則を組み込んでいます。(PR.PT-3)

機能	カテゴリ	Ivantiの製品マッピング
防御		**Ivanti Network Access Control (NAC), Ivanti Connect Secure (ICS), Ivanti Virtual Application Delivery Controller (vADC), Endpoint Security (EPS) for Endpoint Manager (EPM)** および **Neurons for Unified Endpoint Management (UEM)** は、通信を保護し、ネットワークを制御できます。(PR.PT-4) また、**Ivanti Virtual Application Delivery Controller (vADC)** は、通常の状況と不利な状況における回復力の要件を実現する目的で、負荷バランシングとホットスワップのための、ネットワークフェイルセーフの仕組みを提供します。(PR. PT-5)
検知	**異常とイベント** 異常な活動が検知され、事象の潜在的な影響が理解されます。	**Ivanti Neurons for Discovery with Service Mapping** は、クラウドまたはデータセンターのネットワークトポロジを可視化し、ITSMプロセスとITOMプロセスの両方に関連するインフラの関係、アプリの依存関係、通信フロー、およびサービスマッピングの表示を可能にします。このソリューションは、ネットワーク操作のベースラインと、ユーザーおよびシステムに期待されるデータフローを確立し、管理します。(DE.AE-1)
	セキュリティの継続的な監視 情報システムと資産は、サイバーセキュリティイベントを特定し、保護対策の有効性を検証するために監視されます。	**Ivanti Neurons for Zero Trust Access** は、ウェブを使用して、ゲートウェイを介してデバイスからアプリへの安全な接続を作成すると同時に、許可されたアクセス事象を検出して記録するための詳細な制約に基づいて、ユーザー、ユーザーのデバイス、アプリ、時間、およびソースの地理的位置を常に確認します。(DE.CM-3) **Ivanti Mobile Threat Defense (MTD)** は、モバイルデバイスを標的とする脅威を防御し、修復します。潜在的なサイバーセキュリティ事象や不正なモバイルコードおよびエクスプロイトキットのエンドユーザー活動を監視し、検出できます。(DE.CM-3、およびDE.CM-5) オンプレミス展開の場合、**Ivanti Endpoint Manager (EPM)** は、許可されていない人員、接続、デバイス、およびソフトウェアを監視するために、SIEMソリューションと連携できます。(DE.CM-7)
	検知プロセス 検知プロセスと手順は、異常事象の認識を確実にするために維持され、テストされます。	
対応	**対応計画** 検出されたサイバーセキュリティ事象に対して遅滞なく対応できるように、対応プロセスと手順が実行され、維持されます。	Ivanti IT Service Management (ITSM) は、Security Operations Contentと共に、事象の間に、または事象の後に実行された対応計画と承認を追跡します。(RS.RP-1)
	コミュニケーション 利害関係者と調整されます(例:法執行機関からの外部サポート)	
	分析 効果的な対応を確実にし、回復活動をサポートするために分析を行います。	

機能	カテゴリ	Ivantiの製品マッピング
対応	**低減** 事象の拡大を防ぎ、その影響を軽減し、インシデントを解決するためのアクティビティを実行します。	**Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)** は、適応的なリスクベースの脆弱性管理ソリューションです。企業は、攻撃領域全体の曝露を無くすための行動を知って管理するのに、僅か数分を要するだけです。管理者は、僅か数秒で実行すべきアクションを知り、攻撃対象領域、インフラ、アプリ、および開発フレームワークにわたって最も重要な脆弱性の曝露ポイントを急いで修復できます。その機能は、セキュリティ・インシデントの封じ込めと軽減、および新しい脆弱性の特定や許容したリスクの文書化を含みます。(RS.MI-1、RS.MI-2、およびRS.MI-3) また、オンプレミス展開の場合、アプリケーション制御を備えた **Ivanti Endpoint Security (EPS) for Endpoint Manager (EPM)** は、感染したデバイスを隔離し、サイバーセキュリティインシデントを封じ込めて軽減することができます。また、新しい脆弱性を特定したり許容されたリスクとして文書化することができます。(RS.MI-1、RS.MI-2、およびRS.MI-3)。 **Ivanti Neurons for Secure Access, Ivanti Neurons for Zero Trust Access (NZTA), Ivanti Connect Secure (ICS)** および **Ivanti Network Access Control (NAC) Profiler** は、**IvantiSentry**および**IvantiAccess**とともに **Ivanti Mobile Threat Defense**と統合されて、サイバーセキュリティインシデントを封じ込める機能を持ちます。(RS.MI-1)
	改善 企業の対応活動は、現在および以前の検出/対応活動から学んだ教訓を組み込むことによって改善されます。	
復旧	**復旧計画** サイバーセキュリティのインシデントから影響を受けたシステムまたは資産の回復を確実なものにするため、回復プロセスと手順を実行して、それらを維持します。	
	改善 回復計画とプロセスは、学んだ教訓を将来の活動に組み込むことによって改善されます。	
	コミュニケーション 復旧活動は、社内外の関係者と連携して行われます(例:調整センター、インターネットサービスプロバイダー、攻撃システムの所有者、被害者、その他のCSIRTおよびベンダー)。	

Ivantiについて

Workplace（場所にとらわれない働き方）」を実現します。場所にとらわれない働き方により、従業員は多種多様なデバイスでさまざまなネットワークからITアプリケーションやデータにアクセスし、高い生産性を保つことができます。Ivanti Neurons自動化プラットフォームは、業界をリードする統合エンドポイント管理、ゼロトラストセキュリティと、エンタープライズサービス管理のソリューションをつなぎ、デバイスの自己修復および自己保護、またエンドユーザーのセルフサービスを可能にする統合ITプラットフォームを提供します。Fortune 100の96社を含む40,000社以上の顧客が、クラウドからエッジまでIT資産の管理、検出、保護、サービスのためにIvantiを選択し、従業員があらゆる場所にいても作業できる優れたユーザー体験を提供しています。詳細については、www.ivanti.co.jp をご参照ください。

Copyright © 2022, Ivanti. All rights reserved. IVI-2694 08/22 MM/FG

ivanti

ivanti.co.jp
03-6432-4180
contact@ivanti.co.jp