管理とポリシー			
ISMS	アイ・エス・エム・エス	組織幹部	ISMS（情報セキュリティマネジメントシステム）は、組織の情報資産を保護するための体系的なアプローチである。情報セキュリティリスクを適切に管理し、組織のビジネス目標と戦略的目標をサポートすることができる。
		社員・職員全般	ISMS（情報セキュリティマネジメントシステム）は、私たちの日常業務における情報の取り扱いを安全に行うためのガイドラインと手順である。これに従うことで、情報の漏洩や不正アクセスから組織を守ることができる。
		情報管理担当者	ISMS（Information Security Management System）は、情報セキュリティのポリシーや手順を策定・実施・監査するためのフレームワークである。これを基に、組織全体の情報セキュリティの水準を向上させる活動を行う。
IoC	アイ・オー・シー	組織幹部	IoC（侵害指標）は、システムがセキュリティ侵害の対象となった兆候を示す情報やデータである。これを早期に検出することで、組織のリスクを低減し、ビジネスの継続性を保護することができる。
		社員・職員全般	IoC（侵害指標）は、私たちの使用するシステムやデバイスに異常が生じている可能性を示すサインである。異常を感じた場合は、速やかに情報管理部門に報告することが求められる。
		情報管理担当者	IoC（Indicator of Compromise）は、セキュリティインシデントの発生を早期に検出するための指標である。これをモニタリングし、適切な対応を行うことで、インシデントの拡大を防ぐことができる。
ISO/IEC27001	アイエスオー/アイエック27001	組織幹部	ISO/IEC 27001は、情報セキュリティマネジメントシステムの国際標準である。この認証を取得することで、組織の情報セキュリティの取り組みが国際的な基準を満たしていることを外部に示すことができる。
		社員・職員全般	ISO/IEC 27001は、私たちが日々の業務で扱う情報の安全性を確保するためのガイドラインとなる国際標準である。この標準に従うことで、情報の漏洩や不正利用を防ぐことができる。
		情報管理担当者	ISO/IEC 27001は、情報セキュリティのリスク管理や方針の策定、実施、維持、継続的な改善を取り組むためのフレームワークを提供する国際標準である。組織内での情報セキュリティの取り組みを体系的に行うための基盤となる。
ICANN	アイキャン	組織幹部	ICANNは、インターネットのドメイン名やIPアドレスの割り当てを管理する国際的な非営利組織である。組織のブランドやオンラインプレゼンスを確保するため、ICANNの方針や動向を理解することは経営上の重要な課題である。
		社員・職員全般	ICANNは、インターネットの安定性やセキュリティを保つための基盤を提供する組織である。日常の業務で使用するウェブサイトやメールのアドレスが正しく機能するためには、ICANNの役割が不可欠である。
		情報管理担当者	ICANN（Internet Corporation for Assigned Names and Numbers）は、ドメイン名の登録やDNSの運用に関するポリシーを策定する組織である。セキュリティ対策の一環として、ドメイン名の取得や更新、DNSの設定変更などの手続きを行う際には、ICANNのガイドライン
ISAC	アイザック	組織幹部	ISACは、特定の産業分野におけるサイバーセキュリティ情報の共有や協力を促進する組織である。組織のサイバーセキュリティ対策を強化するために、ISACとの連携や情報共有は経営上の重要な戦略である。
		社員・職員全般	ISACは、業界内の他の組織とセキュリティ情報を共有するプラットフォームである。新たな脅威や攻撃手法に迅速に対応し、業務の安全性を維持することができる。
		情報管理担当者	ISAC（Information Sharing and Analysis Center）は、セキュリティインシデントや脅威情報の共有を行う組織である。情報管理担当者としては、ISACからの情報を活用し、組織のセキュリティ対策を最新の状況に合わせて更新することが求められる。
エスカレーション	エスカレーション	組織幹部	エスカレーションは、問題や課題が現在の権限や能力を超えた場合に、上位の権限や専門家へと引き継がれるプロセスである。組織の効率的な運営とリスク管理のために、適切なエスカレーションのフローが必要である。
		社員・職員全般	エスカレーションは、自分の業務の範囲や知識を超える問題に直面した場合に、上司や専門部署へと問題を報告・相談することである。迅速な対応と解決のために、エスカレーションの手順を理解し、適切に行動することが求められる。
		情報管理担当者	エスカレーションは、セキュリティインシデントや脅威が検出された際に、適切な対応策を迅速に実施するためのプロセスである。特定のインシデントに対する対応能力や権限を超える場合、上位の組織や専門家へと迅速に情報を伝達することが重要である。
CISO	シー・アイ・エス・オー	組織幹部	CISOは、組織の情報セキュリティ戦略の策定と実施をリードする役職である。組織の情報資産の保護とビジネスの継続性を確保するための重要な役割を担っている。
		社員・職員全般	CISOは、組織の情報セキュリティポリシーやガイドラインを策定し、社員や職員のセキュリティ意識の向上を促進する役職である。日常業務におけるセキュリティの疑問や懸念事項の相談先としても機能する。
		情報管理担当者	CISO（Chief Information Security Officer）は、組織のセキュリティポスチャ（組織やシステムがサイバーセキュリティの脅威や攻撃に対抗するための体制や準備の状態）を維持・向上させるための戦略的な取り組みをリードする役職である。セキュリティインシデントの対応や新しい脅威への対策の策定など、情報管理担当者と密接に連携して活動する。
GDPR	ジー・ディー・ピー・アール	組織幹部	GDPRはEU内の個人データ保護を規定する法規制である。この規則はEU市民のプライバシー強化とデータ保護法統一を目的とする。企業は重大な罰金リスクに直面し、顧客データ保護と透明性が必須である。
		社員・職員全般	GDPRはEU市民の個人データ管理ルールを定める。この規則により、顧客同意の取得、データアクセスの安全保持、情報要求への対応が必要である。
		情報管理担当者	GDPRはデータ保護の技術面に重点を置く。データ収集、保管、処理に厳格な基準があり、セキュリティ対策強化と迅速なデータ侵害対応が求められる。
CSIRT	シーサート	組織幹部	CSIRTは、情報セキュリティインシデントに対応するための専門チームである。組織の情報資産を保護し、ビジネスの継続性を確保するための重要な役割を果たす。
		社員・職員全般	CSIRTは、セキュリティに関する問題やインシデントが発生した際の対応チームである。不審な動きやセキュリティに関する疑問がある場合、このチームに連絡することで適切な対応が行われる。
		情報管理担当者	CSIRT（Computer Security Incident Response Team）は、インシデントの検出、分析、対応、復旧を行う専門のチームである。最新の脅威情報の収集や、対応手順の整備、スキルアップのための研修など、継続的な活動が求められる。
セキュリティ・バイ・デザイン	セキュリティ・バイ・デザイン	組織幹部	セキュリティ・バイ・デザインは、製品やサービスの設計段階からセキュリティを組み込むアプローチである。初期投資は増えるが、長期的にはセキュリティインシデントのリスクを低減し、信頼性の向上に寄与する。
		社員・職員全般	セキュリティ・バイ・デザインは、業務プロセスやシステムの設計時にセキュリティを考慮することである。後からセキュリティ対策を施すよりも効果的なセキュリティが実現される。
		情報管理担当者	セキュリティ・バイ・デザインは、開発の初期段階からセキュリティ要件を明確にし、設計・実装・テストの各フェーズでそれを適用する方法である。
NIC Framework	ナイス・フレームワーク	組織幹部	NICE Frameworkはサイバーセキュリティ職の能力開発と職業訓練のガイドラインである。人材の訓練が不可欠で、職務要件とスキルを定義し、教育とキャリアパス開発に役立つ。
		社員・職員全般	NICE Frameworkはサイバーセキュリティスキルとキャリア開発のガイドラインである。特定の職務に必要な知識、スキル、能力を提供し、自己のキャリア形成に活用できる。
		情報管理担当者	NICE Frameworkはサイバーセキュリティの役割とスキルセットの標準化を目指す。役割ごとの知識とスキルの詳細を提供し、職員の適切な配置と育成に役立つ。

脅威と攻撃手法			
アカウントハイジャック	アカウントハイジャック	組織幹部	アカウントハイジャックは、不正な手段で他者のアカウントにアクセスし、その権限を乗っ取る行為である。組織の情報資産やブランドの信頼性を守るため、このような脅威から組織を守ることは経営上の重要な課題である。
		社員・職員全般	アカウントハイジャックは、個人のアカウントが第三者に不正に利用されるリスクである。日常の業務で使用するアカウントのパスワードを定期的に変更し、二段階認証などのセキュリティ対策を取ることで、このリスクを低減することができる。
		情報管理担当者	アカウントハイジャックは、セキュリティインシデントの一つである。情報管理担当者としては、ユーザー教育やアカウント管理のポリシーを策定し、組織内のアカウントがハイジャックされるリスクを最小限に抑えることが求められる。
エクスプロイトコード	エクスプロイトコード	組織幹部	エクスプロイトコードは、システムの脆弱性を悪用するためのプログラムである。これが悪意のある者に利用されると、組織の情報資産や業務が大きなリスクにさらされる可能性がある。
		社員・職員全般	エクスプロイトコードは、コンピューターシステムの弱点を突くためのツールである。不正アクセスや情報の盗難が行われることがある。安全な業務運用のためには、常に注意が必要である。
		情報管理担当者	エクスプロイトコードは、特定の脆弱性を悪用してシステムに侵入するためのコードである。これを検知し、適切な対策を講じることが情報セキュリティの実務において重要である。
SQLインジェクション	エス・キュー・エル・インジェクション	組織幹部	SQLインジェクションは、不正なSQLコードを注入されることによるセキュリティ脆弱性である。機密情報の漏洩やデータベースの破壊が発生する可能性がある。
		社員・職員全般	SQLインジェクションは、システムの入力欄に不正なコードを入れることで、データベースにアクセスされるリスクがある攻撃方法である。
		情報管理担当者	SQLインジェクションは、入力値の検証やエスケープ処理を適切に行わないと発生する脆弱性である。対策として、プリペアドステートメント（データベースに対するクエリを安全かつ効率的に実行する手法）の使用や入力値の厳格な検証が必要である。
クラッキング	クラッキング	組織幹部	クラッキングは、不正な手段でシステムやデータにアクセスする行為である。組織の情報資産や業績に深刻な影響を及ぼす可能性があるため、適切なセキュリティ対策の実施とリスク管理が求められる。
		社員・職員全般	クラッキングは、外部の攻撃者が私たちのシステムや情報に不正にアクセスする行為である。日常業務において、不審なメールやリンクを開かない、強固なパスワードを設定するなどの基本的な対策が重要である。
		情報管理担当者	クラッキングは、セキュリティの脆弱性を突いて不正アクセスを試みる行為である。定期的なセキュリティ診断やパッチの適用、モニタリングの強化が必要である。
サプライチェーン攻撃	サプライチェーンコウゲキ	組織幹部	サプライチェーン攻撃は、組織の供給チェーンに関連する第三者を通じて、組織の情報システムを狙った攻撃である。この攻撃のリスクは、組織のビジネス継続性や信頼性に影響を及ぼす可能性がある。
		社員・職員全般	サプライチェーン攻撃は、取引先や提携先などの第三者を経由して、我々の組織に侵入する試みである。日常業務での取引先とのコミュニケーションやデータの取り扱いには十分な注意が必要である。
		情報管理担当者	サプライチェーン攻撃は、信頼された第三者のソフトウェアやハードウェアを悪用して組織に侵入する手法である。供給元のセキュリティ対策の確認や、定期的な脆弱性評価が必要である。
C&Cサーバー	シー・アンド・シー・サーバー	組織幹部	C&Cサーバーは、サイバー攻撃者がマルウェアやボットネットを遠隔操作するためのサーバーである。このサーバーを通じて、攻撃者は不正な指示を送信し、情報を盗み取ることができる。組織としては、このような脅威から保護するための対策と監視が不可欠である。
		社員・職員全般	C&Cサーバーは、不正な指示を受け取るための中継地点として機能するサーバーである。自身のデバイスがこのようなサーバーと通信していないか、定期的に確認し、不審な通信を見つけた場合は速やかに報告することが求められる。
		情報管理担当者	C&Cサーバーは、ボットネットの制御やマルウェアの配布に使用される。通信のパターンや振る舞いを分析し、これらのサーバーとの通信を検出・遮断するための対策を講じる必要がある。
ショルダーハッキング	ショルダーハッキング	組織幹部	ショルダーハッキングは、他者が業務中のスクリーンや入力を盗み見る行為である。機密情報が漏洩するリスクがあるため、組織全体としての情報管理の徹底が求められる。
		社員・職員全般	ショルダーハッキングは、他者にパソコンの画面やキーボード入力を盗み見られることである。業務中は、周囲に注意を払い、機密情報を扱う際は特に注意が必要である。
		情報管理担当者	ショルダーハッキングは、物理的なセキュリティの脅威である。モニターの視野角を制限するフィルターや、作業スペースの配置を見直すことで、リスクを軽減することができる。
スニファ攻撃	スニファコウゲキ	組織幹部	スニファ攻撃は、ネットワーク上のデータを不正に傍受する攻撃手法である。情報の漏洩やビジネスの中断のリスクがあるため、経営上のリスクとして認識し、適切な予算とリソースをセキュリティ対策に投資することが求められる。
		社員・職員全般	スニファ攻撃は、第三者が業務でやり取りする情報を盗み見る手法である。公共のWi-Fiなど、安全でないネットワークを使用する際は特に注意が必要である。
		情報管理担当者	スニファ攻撃は、ネットワークトラフィックを傍受し、機密情報を取得する攻撃手法である。ネットワークのセグメンテーション、暗号化技術の導入、およびトラフィックの監視が必要である。
スパイウェア	スパイウェア	組織幹部	スパイウェアは、ユーザーの知らない間に情報を収集するソフトウェアである。企業の機密情報や顧客データの漏洩のリスクがあるため、経営上の重要な課題として取り組む必要がある。
		社員・職員全般	スパイウェアは、私たちのコンピューターやスマートフォンで動作し、行動やデータを盗むソフトウェアである。不審なメールの添付ファイルやリンクを開かないよう注意が必要である。
		情報管理担当者	スパイウェアは、エンドポイントの情報を不正に収集するマルウェアの一種である。エンドポイントセキュリティソリューションの導入や定期的なセキュリティ教育が必要である。
スパムメール	スパムメール	組織幹部	スパムメールは、不要な広告や詐欺を目的とした大量の電子メールである。組織のブランドイメージや信頼性が損なわれる可能性がある。
		社員・職員全般	スパムメールは、不要な情報や誤認を招くリンクが含まれていることが多い。これらのメールを開くと、業務の効率が低下するだけでなく、セキュリティリスクが高まる可能性がある。
		情報管理担当者	スパムメールは、マルウェアの感染源となることがある。適切なフィルタリングや教育を通じて、これらのメールが内部ネットワークに影響を及ぼすことを防ぐ必要がある。
スピアフィッシング	スピアフィッシング	組織幹部	スピアフィッシングは、特定の個人や組織を標的とした詐欺メールである。組織の機密情報が漏洩するリスクがある。
		社員・職員全般	スピアフィッシングは、信頼性のある情報を装って送られてくることが多い。不審なメールやリンクを開く前に、内容の真偽を確認することが重要である。
		情報管理担当者	スピアフィッシングは高度な攻撃手法を使用することが多い。従業員の教育や、メールのセキュリティ対策を強化することで、攻撃を未然に防ぐことが求められる。
セキュリティホール	セキュリティホール	組織幹部	セキュリティホールは、システムやソフトウェアに存在する未知の脆弱性である。これを放置すると、組織の情報資産やブランドイメージに大きな損害をもたらす可能性がある。
		社員・職員全般	セキュリティホールは、使用しているシステムやアプリケーションに潜む予期しない脆弱性である。日常業務中に不審な動きやエラーを発見した場合は、速やかに情報管理部門に報告することが求められる。
		情報管理担当者	セキュリティホールは、未知の脆弱性として存在する。定期的な脆弱性スキャンやパッチの適用、システムのアップデートを行い、早急にこれらのホールを検出し、修正することが必要である。

セッションハイジャック	セッションハイジャック	組織幹部	セッションハイジャックは、ユーザーのセッション（通信の開始から終了までのこと）を不正に乗っ取る攻撃である。機密情報の漏洩や不正な取引が行われるリスクが高まる。
		社員・職員全般	セッションハイジャックは、ログイン中のアカウントを第三者に乗っ取られる攻撃である。公共のWi-Fiなど、安全でないネットワークを使用する際は特に注意が必要である。
		情報管理担当者	セッションハイジャックは、セッションIDを盗むことで実行される。セッション管理の強化や、セキュアな通信の導入、不正なセッションの検出手段を取り入れることで、この攻撃を防ぐことができる。
ゼロデイ攻撃	ゼロデイコウゲキ	組織幹部	ゼロデイ攻撃は、まだ公に知られていない脆弱性を狙った攻撃である。対策がまだ存在しないため、組織に甚大なダメージを与える可能性がある。
		社員・職員全般	ゼロデイ攻撃は、新たに発見された脆弱性を利用した攻撃である。不審なメールやリンクを開く際は十分な注意が必要である。
		情報管理担当者	ゼロデイ攻撃は、未知の脆弱性を利用する攻撃である。情報収集を積極的に行い、可能な限り迅速に対応策を講じることが求められる。
ソーシャルエンジニアリング	ソーシャルエンジニアリング	組織幹部	ソーシャルエンジニアリングは、人間の心理や行動を悪用して情報を不正に取得する手法である。取締役や執行役員としては、組織全体の情報セキュリティリスクを理解し、適切な教育や対策を実施することが求められる。
		社員・職員全般	ソーシャルエンジニアリングは、詐欺メールや偽の電話などを通じて、個人情報や業務情報を騙し取る試みである。日常業務において、怪しいコンタクトや要求には十分な注意を払い、確認することが重要である。
		情報管理担当者	ソーシャルエンジニアリングの対策として、定期的なセキュリティ教育や模擬攻撃の実施、セキュリティポリシーの策定と徹底が必要である。また、インシデント発生時の迅速な対応体制の構築も求められる。
ダークウェブ	ダークウェブ	組織幹部	ダークウェブは、通常の検索エンジンでは検索できないインターネットの隠された部分である。組織の情報がダークウェブ上で取引されるリスクを理解し、情報漏洩の予防策を強化することが必要である。
		社員・職員全般	ダークウェブは、違法な取引や情報の交換が行われる場所である。業務上の情報を安易に外部に共有しないことや、セキュリティの基本的な対策を遵守することが、情報漏洩の予防に繋がる。
		情報管理担当者	ダークウェブの監視ツールを使用して、組織に関連する情報が流出していないか定期的にチェックすることが推奨される。また、情報漏洩の兆候を早期に検知するためのシステムやプロセスの導入も考慮するべきである。
ダウンストリーム攻撃	ダウンストリームコウゲキ	組織幹部	ダウンストリーム攻撃は、取引先やパートナー企業を通じて自社のシステムを狙った攻撃である。取引先とのセキュリティ方針の調整や、連携時のセキュリティ対策の強化が求められる。
		社員・職員全般	ダウンストリーム攻撃は、取引先や外部の業者からの不正なアクセスを介して情報が漏洩するリスクがある。取引先とのやり取りやデータの共有時には、セキュリティの確認を怠らないよう注意が必要である。
		情報管理担当者	ダウンストリーム攻撃への対策として、取引先とのセキュリティ基準の合意や、VPNや暗号化技術を使用した安全なデータ転送方法の導入が考慮されるべきである。また、定期的なセキュリティ監査やリスク評価を行うことも重要である。
チェーンメール	チェーンメール	組織幹部	チェーンメールは、組織の情報セキュリティを脅かす可能性のある電子メールである。これらのメールは、受信者に何らかのアクションを促す内容を含み、従業員がこれに応じることで情報漏洩やマルウェア感染のリスクが高まる。
		社員・職員全般	チェーンメールは、続けて他の人に転送するようにとの指示が含まれたメールである。これに応じることで、組織の情報が第三者に漏れるリスクがあるため、不審なメールを受信した場合は、すぐに情報管理部門に報告することが重要である。
		情報管理担当者	チェーンメールは、フィッシング攻撃やマルウェアの拡散手段として使用されることがある。従業員の教育やメールフィルタリングシステムの導入など、複数の対策を組み合わせて、これらの脅威から組織を守ることが必要である。
中間者攻撃	チュウカシャコウゲキ	組織幹部	中間者攻撃は、組織と顧客やパートナーとの通信を盗聴・改ざんする攻撃手法である。この攻撃により、企業の信頼やブランドイメージが損なわれる可能性がある。
		社員・職員全般	中間者攻撃は、私たちの通信が第三者に傍受され、機密情報が漏洩するリスクがある。常に安全な通信手段を使用し、怪しい活動には注意を払う必要がある。
		情報管理担当者	中間者攻撃を防ぐためには、通信の暗号化や認証手段の強化が必要である。また、ネットワークの監視やログの分析を行い、異常な通信を検出する仕組みを整える必要がある。
DNSキャッシュポイズニング	ディー・エヌ・エスキャッシュポイズニング	組織幹部	DNSキャッシュポイズニングは、攻撃者が偽のIPアドレス情報をDNSキャッシュに注入し、ユーザーを悪意のあるサイトに誘導する攻撃である。この攻撃により、企業のブランドイメージや顧客の信頼が損なわれる可能性がある。
		社員・職員全般	DNSキャッシュポイズニングの影響を受けると、正当なウェブサイトへのアクセスが悪意のあるサイトにリダイレクトされる可能性がある。従業員がこのようなサイトにアクセスすると、機密情報が漏洩するリスクがある。
		情報管理担当者	DNSキャッシュポイズニングを防ぐためには、DNSサーバのセキュリティ設定を適切に行い、最新のセキュリティパッチを適用することが重要である。また、DNSトラフィックの監視を行い、異常な動きを検出するシステムを導入することも効果的である。
DDoS攻撃	ディードスコウゲキ	組織幹部	DDoS攻撃は、大量のトラフィックでサービスを一時的に利用不能にする攻撃である。この攻撃により、ビジネスのオペレーションが停止し、収益損失や企業の評価低下が発生する可能性がある。
		社員・職員全般	DDoS攻撃が発生すると、社内のネットワークや外部との通信が遅延または中断する可能性がある。これにより、日常の業務プロセスに支障が出ることが考えられる。
		情報管理担当者	DDoS攻撃を防ぐためには、トラフィックの監視やフィルタリング、帯域幅の調整などの対策が必要である。また、クラウドベースのDDoS保護サービスを利用することで、攻撃の影響を最小限に抑えることができる。
ドライブバイダウンロード攻撃	ドライブバイダウンロードコウゲキ	組織幹部	ドライブバイダウンロード攻撃は、訪問者がウェブサイトを訪れるだけで悪意のあるソフトウェアが自動的にダウンロードされる攻撃である。この攻撃により、企業の情報資産やブランドの信頼性が損なわれる可能性がある。
		社員・職員全般	ドライブバイダウンロード攻撃は、普段利用するウェブサイトを訪れるだけで感染のリスクがある。不審なウェブサイトやメールのリンクをクリックしないよう注意し、常にセキュリティソフトウェアを最新の状態に保つことが重要である。
		情報管理担当者	ドライブバイダウンロード攻撃は、脆弱性を持つウェブブラウザやプラグインを標的とする。定期的な脆弱性スキャンやパッチの適用、ウェブフィルタリングツールの導入などで、攻撃を未然に防ぐ対策が必要である。
トロイの木馬	トロイノモクバ	組織幹部	トロイの木馬は、正当なソフトウェアに偽装して悪意のあるコードを実行するプログラムである。企業の情報資産を盗むリスクがあり、経営上の大きな損失を招く可能性がある。
		社員・職員全般	トロイの木馬は、正規のソフトウェアやファイルとして偽装されているため、不審なファイルのダウンロードや開封は避ける必要がある。セキュリティソフトウェアを常に最新の状態に保ち、定期的なスキャンを行うことが重要である。
		情報管理担当者	トロイの木馬の対策として、入手したソフトウェアやファイルの信頼性を確認すること、定期的な脆弱性スキャン、セキュリティソフトウェアの導入と更新、従業員への教育が必要である。
なりすまし	ナリスマシ	組織幹部	なりすましは、不正な者が正当なユーザーや組織を装って情報や資産を不正に取得する行為である。このような攻撃は組織の信用やブランドイメージを損なう可能性があり、経営上のリスクとして取り組む必要がある。
		社員・職員全般	なりすましは、日常の業務中にも発生する可能性がある。例えば、偽のメールやウェブサイトを通じて、個人情報や業務情報を騙し取られることがある。常に警戒心を持ち、不審なコンテンツには応じないよう注意が必要である。
		情報管理担当者	なりすまし攻撃の対策として、ユーザー認証の強化やセキュリティ教育の実施が必要である。また、不正なアクセスを検知するための監視体制の構築や、インシデント発生時の迅速な対応が求められる。

ハクティビスト	ハクティビスト	組織幹部	ハクティビストは、政治的・社会的な動機からサイバー攻撃を行う者である。組織の評判や業績に影響を及ぼす可能性があるため、経営戦略の一部としてリスク管理が必要である。
		社員・職員全般	ハクティビストは、自らの信念や主義に基づき、組織に対してサイバー攻撃を仕掛ける者である。業務上の情報の取り扱いに注意し、不審な活動を速やかに報告することが求められる。
		情報管理担当者	ハクティビストは、特定の目的を持って組織のシステムを狙う者である。対策として、外部からの侵入を検知するシステムの導入や、定期的なセキュリティ監査の実施が必要である。
パスワードリスト攻撃	パスワードリストコウゲキ	組織幹部	パスワードリスト攻撃は、既知のパスワードのリストを使用して不正にアクセスを試みる攻撃である。情報漏洩のリスクがあるため、社員への教育やシステムのセキュリティ強化が必要である。
		社員・職員全般	パスワードリスト攻撃は、一般的なパスワードを使って不正ログインを試みる攻撃である。強固なパスワードの設定や定期的な変更が、このような攻撃から身を守るための基本である。
		情報管理担当者	パスワードリスト攻撃は、複数のパスワードを自動的に試行することで不正アクセスを目指す攻撃である。アクセス試行の上限設定や、二段階認証の導入などの対策が効果的である。
ハッキング	ハッキング	組織幹部	ハッキングは、外部の不正アクセス者が組織の情報システムに侵入する行為であり、これにより企業の信用や業績に大きな損害を与える可能性がある。適切なセキュリティ対策と継続的なリスク評価が必要である。
		社員・職員全般	ハッキングは、私たちの業務データや顧客情報が外部に漏れる原因となる。日常業務での情報取り扱いやパスワード管理の徹底が求められる。
		情報管理担当者	ハッキングは技術的・社会的手法を問わず、システムへの不正アクセスを試みる行為である。定期的な脆弱性診断やセキュリティ対策の更新、従業員への教育が必要である。
バックドア	バックドア	組織幹部	バックドアは、システムやソフトウェアに意図的に設けられた隠れたアクセス手段である。通常の認証手続きを経ずにシステムにアクセスすることが可能となる。組織の情報資産や業務の継続性に対するリスクが高まるため、適切な対策が必要である。
		社員・職員全般	バックドアは、不正な方法で情報を取得したり、システムを操作したりするための秘密の入り口である。外部の攻撃者が組織の情報にアクセスすることができる。日常業務において、不審な動きや異常を感じた場合は速やかに情報管理部門に報告することが求められる。
		情報管理担当者	バックドアは、システムの脆弱性を利用して不正にアクセスするための手段である。定期的なシステムの監査や脆弱性のスキャンを行い、不正なアクセスポイントを早期に検出・排除することが重要である。
標的型攻撃	ヒョウテキガタコウゲキ	組織幹部	標的型攻撃は、特定の組織や個人を狙った高度なサイバー攻撃である。組織の評価や信頼性を損なう可能性があり、経営戦略の一部としての対策が必要である。
		社員・職員全般	標的型攻撃は、従業員の個人情報や業務情報を狙った攻撃である。不審なメールやリンクを開く際には十分な注意が必要である。
		情報管理担当者	標的型攻撃は、特定の情報を狙って行われるサイバー攻撃である。侵入検知システムやセキュリティ対策の強化、従業員への教育（意識啓発）が重要である。
フィッシング詐欺	フィッシングサギ	組織幹部	フィッシング詐欺は、正規の組織やサービスを装い、個人情報や機密情報を不正に取得しようとする詐欺行為である。これによる情報漏洩は、組織の信頼やブランドイメージの損失を招く可能性がある。
		社員・職員全般	フィッシング詐欺のメールやウェブサイトには、騙されやすい内容やデザインが用いられることが多い。不審なメールやリンクを受け取った場合は、絶対に開かず、情報部門や上司に報告することが重要である。
		情報管理担当者	フィッシング詐欺への対策として、従業員への教育や情報共有、メールフィルタリングの導入、不正なウェブサイトへのアクセス制限などの技術的な対策を継続的に行うことが必要である。
不正侵入	フセイシンニュウ	組織幹部	不正侵入は、外部の攻撃者が組織の情報システムに無許可でアクセスする行為である。組織の情報資産や業績に大きな損害をもたらす可能性がある。
		社員・職員全般	不正侵入は、外部からの不正なアクセスや攻撃を意味する。自身の業務端末やシステムに異常を感じた場合、速やかに情報管理部門に連絡することが求められる。
		情報管理担当者	不正侵入は、セキュリティの脆弱性を突いた攻撃や、フィッシングなどの手法で発生することが多い。侵入の検出、対応、そして将来の侵入を防ぐための対策の実施が必要である。
マルウェア	マルウェア	組織幹部	マルウェアは、不正な目的で作成されたソフトウェアである。組織の情報資産を守るために、マルウェア対策を強化することが不可欠である。
		社員・職員全般	マルウェアは、デバイスの動作を妨害したり、機密情報を盗む可能性があるソフトウェアである。不審なメールの添付ファイルやリンクを開かないよう注意が必要である。
		情報管理担当者	マルウェアは、組織の情報システムを侵害する主要な脅威である。定期的なセキュリティスキャンやアップデートを行い、最新の脅威情報に基づいた対策を実施することが求められる。
水飲み場攻撃	ミズノミバコウゲキ	組織幹部	水飲み場攻撃は、従業員が頻繁に訪れる信頼されたウェブサイトを悪用してマルウェアを配布する攻撃手法である。この攻撃により、組織の情報資産や業務の継続性が脅かされる可能性がある。
		社員・職員全般	水飲み場攻撃は、日常的に利用するウェブサイトを通じて不正なプログラムが自分のPCに侵入するリスクがある。信頼性のあるサイトであっても、常に警戒心を持ち、不審な動きやリンクをクリックしないよう注意する必要がある。
		情報管理担当者	水飲み場攻撃は、エンドポイントのセキュリティ対策やウェブフィルタリングの強化、従業員への教育を通じて予防することが可能である。また、定期的な脅威情報の収集と分析を行い、最新の攻撃手法に対応する必要がある。
リプレイ攻撃	リプレイコウゲキ	組織幹部	リプレイ攻撃は、正当なユーザーの通信を盗聴し、それを再利用することで不正アクセスを試みる攻撃である。組織の情報資産が危険にさらされる。
		社員・職員全般	リプレイ攻撃は、パスワードやトークンなどの認証情報が再利用されるリスクがある。常にセキュアな通信を心がけ、不審な活動を感じたら速やかに報告することが重要である。
		情報管理担当者	リプレイ攻撃を防ぐためには、通信の暗号化、一度使用したトークンの無効化、時刻情報の組み込みなどの対策が考えられる。
ワーム	ワーム	組織幹部	ワームは、自己複製機能を持つマルウェアの一種である。ワームに感染すると、組織のIT資産が大きなダメージを受ける可能性があるため、適切なセキュリティ対策が必要である。
		社員・職員全般	ワームは、感染すると他のコンピュータにも自動的に広がる危険なプログラムである。不審なメールの添付ファイルを開かない、定期的なセキュリティアップデートを行うなどの注意が求められる。
		情報管理担当者	ワームは、ネットワークを介して迅速に拡散する特性を持つ。感染の兆候を早期に検出し、隔離・除去するための監視体制の構築と対策の更新が不可欠である。
ワンクリック詐欺	ワンクリックサギ	組織幹部	ワンクリック詐欺は、ユーザーが誤って特定のリンクや広告をクリックすることで、不正な請求が発生する詐欺の一形態である。このような詐欺により、組織の財務や評判が大きく損なわれる可能性がある。組織としては、適切な情報セキュリティの教育や対策を実施し、リスクを最小限に抑える必要がある。
		社員・職員全般	ワンクリック詐欺は、見た目は正規の広告やウェブサイトに似ているが、クリックすると高額な請求が発生するリンクを含むものである。業務の過程で不審なリンクやメールに出会った場合、安易にクリックせず、注意深く確認することが求められる。
		情報管理担当者	ワンクリック詐欺は、ユーザーを誘導するための巧妙な手口やマルウェアを使用することが多い。情報管理担当者としては、最新のセキュリティ対策を適用し、組織内のネットワークやシステムを常に監視することで、不正なアクセスや詐欺の試みを早期に検出し、対応する必要がある。

防御とセキュリティ技術			
IDS	アイ・ディー・エス	組織幹部	IDS（不正侵入検知システム）は、組織のネットワークに不正な侵入や異常な通信を検知するシステムである。セキュリティ上のリスクを早期に発見し、経営上のリスクを最小限に抑えることが可能である。
		社員・職員全般	IDS（不正侵入検知システム）は、私たちの業務をサポートするIT環境が安全に運用されるためのツールの一つである。不正なアクセスや怪しい動きを検知し、それを報告することで、私たちのデータや業務が守られる。
		情報管理担当者	IDS（Intrusion Detection System）は、リアルタイムでネットワークのトラフィックを監視し、定義されたルールやヒューリスティックに基づいて異常を検知するシステムである。適切な設定と更新が必要であり、検知されたアラートの分析と対応が求められる。
IPS	アイ・ピー・エス	組織幹部	IPS（不正侵入防止システム）は、不正な通信や攻撃をリアルタイムでブロックするシステムである。組織の資産や情報を守り、ビジネスの継続性を確保することができる。
		社員・職員全般	IPS（不正侵入防止システム）は、私たちの業務に関連する情報やシステムを外部からの攻撃から守るためのツールである。業務の中断や情報の漏洩を防ぐことができる。
		情報管理担当者	IPS（Intrusion Prevention System）は、ネットワークトラフィックを監視し、悪意のある通信や攻撃パターンを検知した際に、その通信をブロックするシステムである。適切なルールの設定と継続的な更新が必要であり、ブロックされた通信の分析と対応が求められる。
アクセスポイント	アクセスポイント	組織幹部	アクセスポイントは、組織のネットワーク接続のゲートウェイである。適切な管理とセキュリティ対策がなされていないと、外部からの不正アクセスのリスクが高まる可能性がある。
		社員・職員全般	アクセスポイントは、無線LANを使用してインターネットや組織の内部ネットワークに接続するためのデバイスである。安全に使用するためには、定期的なパスワードの変更やセキュリティ設定の確認が必要である。
		情報管理担当者	アクセスポイントの設定や管理は、セキュリティの観点から非常に重要である。ファームウェアの更新、WPA3などの最新の暗号化技術の使用、不要なサービスの無効化など、セキュリティ対策を定期的に見直し、実施する必要がある。
アラート	アラート	組織幹部	アラートは、システムやネットワークに異常や脅威が検出された際の警告メッセージである。これに迅速に対応することで、組織の情報資産を守ることができる。
		社員・職員全般	アラートは、使用しているシステムやソフトウェアからの重要な通知である。アラートが表示された場合、指示に従い、必要な場合は情報管理部門に連絡することが求められる。
		情報管理担当者	アラートの設定や管理は、組織のセキュリティを維持するための重要な要素である。アラートの閾値や条件を適切に設定し、異常検出の精度を高めることで、脅威から組織を守ることができる。
EDR	イー・ディー・アール	組織幹部	EDRは、組織のエンドポイントにおけるセキュリティ脅威を検出し、対応するための技術である。組織の資産と情報を保護し、ビジネスの継続性と信頼性を確保することができる。
		社員・職員全般	EDRは、私たちのコンピューターやスマートフォンなどのデバイスに対するセキュリティ脅威をリアルタイムで検出し、迅速に対応するためのツールである。業務の安全性と効率性を向上させることができる。
		情報管理担当者	EDR（Endpoint Detection and Response）は、エンドポイントの動作や通信を監視し、異常な動作や不正なアクセスを検出するためのシステムである。インシデントの早期発見と対応、そして事後分析が可能となる。
エンドポイント	エンドポイント	組織幹部	エンドポイントは、組織のネットワークに接続される全てのデバイスを指す。これらのデバイスの安全性は、組織の情報資産を守るために極めて重要である。
		社員・職員全般	エンドポイントは、業務で使用するPCやスマートフォンなどのデバイスである。これらのデバイスからの情報漏洩を防ぐため、定期的なセキュリティチェックや適切な使用が求められる。
		情報管理担当者	エンドポイントは、攻撃の対象となる可能性があるデバイスである。エンドポイントのセキュリティを確保するために、マルウェア対策やパッチ管理、アクセス制御などのセキュリティ対策を継続的に実施することが必要である。
オートコンプリート	オートコンプリート	組織幹部	オートコンプリートは、ユーザーが入力を開始すると関連する提案を自動的に表示する機能である。この機能はユーザビリティの向上に寄与するが、不適切な情報が表示されるリスクもあるため、適切なガバナンスが必要である。
		社員・職員全般	オートコンプリートは、入力の効率化をサポートする機能である。しかし、機密情報を入力する際には、提案される情報に注意し、不要な情報が表示されないよう注意が必要である。
		情報管理担当者	オートコンプリートの設定や管理は、ユーザーデータの保護と利便性のバランスを取る必要がある。不適切な情報が提案されないようにフィルタリングや設定の最適化が求められる。
仮想パッチ	カソウパッチ	組織幹部	仮想パッチは、ソフトウェアの脆弱性を直接修正することなく、攻撃を防ぐための一時的な対策である。
		社員・職員全般	仮想パッチを利用することで、脆弱性が公開された直後やパッチが提供されるまでの間、システムを保護することができる。
		情報管理担当者	仮想パッチは迅速な対応を可能にするが、長期的な対策としては実際のパッチ適用が必要である。適切な運用と併用が求められる。
仮想LAN	カソウラン	組織幹部	仮想LANは、物理的なネットワーク上で複数の独立したネットワークを構築する技術であり、セキュリティの強化やネットワーク管理の効率化に寄与する。
		社員・職員全般	仮想LANを使用することで、異なる部署やプロジェクトごとに独立したネットワーク環境を提供でき、データのアクセス制御やセキュリティの向上が期待できる。
		情報管理担当者	仮想LANを適切に設定・管理することで、ネットワーク内の通信を隔離し、不正アクセスや情報漏洩のリスクを低減することができる。
キーロガー	キーロガー	組織幹部	キーロガーは、ユーザーがキーボードで入力した情報を秘密裏に記録するソフトウェアまたはハードウェアのことである。不正な目的で使用される場合、企業の機密情報や顧客データの漏洩の原因となる可能性がある。
		社員・職員全般	キーロガーは、入力されたパスワードや業務上の情報を盗むために使用されることがある。不審なメールの添付ファイルやリンクを開かないよう注意し、定期的にセキュリティソフトウェアを更新することが重要である。
		情報管理担当者	キーロガーは、マルウェアの一種であり、感染したシステム上で動作することで情報を収集する。定期的なシステムのスキャン、不正な通信の監視、エンドポイントの保護策の強化が必要である。
境界保護デバイス	キョウカイホゴデバイス	組織幹部	境界保護デバイスは、組織のネットワークを外部の脅威から守るための装置である。不正アクセスやデータ漏洩のリスクを低減し、ビジネスの継続性と情報資産の保護を確保することができる。
		社員・職員全般	境界保護デバイスは、私たちの業務で使用する情報やシステムを外部からの攻撃や不正アクセスから守るための壁の役割を果たす装置である。安全に業務を遂行することができる。
		情報管理担当者	境界保護デバイスは、ファイアウォールやIDS/IPSなどの機能を持ち、組織のネットワークの入出口に配置される。これにより、不正な通信や攻撃を検知・防御し、セキュリティポリシーに基づいた通信の制御を行うことができる。
共通鍵暗号方式	キョウツウカギアンゴウホウシキ	組織幹部	共通鍵暗号方式は、情報の暗号化と復号に同じ鍵を使用する方法である。情報の機密性を保護することができるが、鍵の管理や配布には注意が必要である。
		社員・職員全般	共通鍵暗号方式は、情報を暗号化する際と解読する際に同じ鍵を使用する方式である。この鍵は非常に大切であり、第三者に知られることなく安全に管理する必要がある。
		情報管理担当者	共通鍵暗号方式は、暗号化と復号の速度が速い利点があるが、鍵の配布や管理が課題となる。鍵の取り扱いには極度の注意が必要であり、鍵の漏洩や不正利用を防ぐための対策が求められる。

サンドボックス	サンドボックス	組織幹部	サンドボックスは、不審なファイルやプログラムを安全な環境で実行し、その挙動を観察する技術である。組織の情報資産を保護し、ビジネスの安全性を確保することができる。
		社員・職員全般	サンドボックスは、不明なメール添付ファイルやダウンロードしたファイルを開く前に、その安全性を確認するためのツールである。業務中の誤操作から組織を守ることができる。
		情報管理担当者	サンドボックスは、マルウェアやランサムウェアの挙動を解析し、対策を講じるための環境である。不審なファイルの動作を隔離された環境で確認し、セキュリティ対策の強化に役立てることができる。
SIEM	シーム	組織幹部	SIEMは、組織内のセキュリティ関連の情報を一元的に収集・分析するシステムである。セキュリティインシデントの早期発見や対応が可能となり、組織のリスクを低減することが期待できる。
		社員・職員全般	SIEMは、私たちの業務活動に関連するセキュリティの脅威や異常を検知するためのツールである。日常の業務中に異常な動きやアクセスを感知した場合、SIEMを通じて迅速に情報を共有し、対応を行うことが求められる。
		情報管理担当者	SIEM（Security Information and Event Management）は、ログ情報やイベントデータをリアルタイムで収集・分析することで、セキュリティインシデントの検知や分析を効率的に行うことができるシステムである。適切なルールやフィルターの設定により、高精度な検知が可能となる。
修正プログラム	シュウセイプログラム	組織幹部	修正プログラムは、ソフトウェアの脆弱性やバグを修正するための更新プログラムである。これを適切に適用することで、組織の情報資産を守ることができる。
		社員・職員全般	修正プログラムは、私たちが使用するソフトウェアの問題点を修正するためのものである。定期的に更新を行い、業務の安全性を確保することが重要である。
		情報管理担当者	修正プログラムは、既知の脆弱性やバグを修正するためのものである。これを適切に管理・適用することで、セキュリティインシデントのリスクを低減することができる。
シンクライアント	シンクライアント	組織幹部	シンクライアントは、中央のサーバーでデータやアプリケーションを管理し、端末は表示や入力のみを行うシステムである。情報の一元管理とセキュリティの向上が期待できる。
		社員・職員全般	シンクライアントは、データをローカルに保存しないため、端末の故障や紛失時のリスクが低減する。しかし、ネットワークの接続が切れると作業ができなくなる点に注意が必要である。
		情報管理担当者	シンクライアントは、データの流出リスクを軽減するが、サーバーのセキュリティ対策が不可欠である。サーバーのセキュリティを強化し、定期的なバックアップと監査を行うことが重要である。
ステルス機能	ステルスキノウ	組織幹部	ステルス機能は、マルウェアやウイルスが検出されにくくするための技術である。セキュリティ対策を回避し、組織の情報資産を長期間にわたって危険にさらす可能性がある。経営戦略として、最新のセキュリティ対策の導入と定期的なセキュリティ監査の実施が必要である。
		社員・職員全般	ステルス機能は、不正なプログラムが自身の存在を隠蔽する技術である。日常業務中に不審な動作やメッセージを感じた場合、速やかに情報管理部門に連絡することが重要である。
		情報管理担当者	ステルス機能は、マルウェアの検出を回避するための技術である。定期的なシステムのスキャン、最新のシグネチャの更新、およびセキュリティインシデント対応プロセスの強化が必要である。
生体認証	セイタイニンショウ	組織幹部	生体認証は、個人の生体的特徴を利用して本人確認を行う技術である。不正アクセスのリスクを低減し、組織の情報資産を守るための重要な手段となる。
		社員・職員全般	生体認証は、指紋や顔認証などの個人の特徴を利用して、ログインやデータアクセスの際の本人確認を行う方法である。パスワードのみの認証よりも高いセキュリティを提供する。
		情報管理担当者	生体認証は、特定のハードウェアやソフトウェアのサポートが必要である。適切な実装と継続的な更新が求められる。
多層防御	タソウボウギョ	組織幹部	多層防御は、組織の情報資産を保護するためのセキュリティ戦略である。一つの防御手段だけに依存するのではなく、複数のセキュリティ層を重ねることで、潜在的な脅威からの保護を強化するアプローチである。
		社員・職員全般	多層防御は、さまざまなセキュリティ対策を組み合わせることで、一つの対策が破られたとしても他の対策が侵入を防ぐ役割を果たす考え方である。日常業務においても、この考え方を取り入れることで、情報の安全性を高めることができる。
		情報管理担当者	多層防御は、ファイアウォール、侵入検知システム、アンチウイルスソフトウェアなど、複数のセキュリティツールや手法を組み合わせて実装する戦略である。これにより、一つのセキュリティ対策が欠けた場合でも、他の層が脅威を検知し対応することが可能である。
多要素認証	タヨウソニンショウ	組織幹部	多要素認証は、組織の情報資産へのアクセスをより安全にするための認証手法である。単一のパスワードだけでなく、複数の認証要素を組み合わせることで、不正アクセスのリスクを大幅に低減することができる。
		社員・職員全般	多要素認証は、例えばパスワードとスマートフォンの認証コードの組み合わせなど、2つ以上の認証手段を使用することで、自身のアカウントが第三者によって不正に使用されるリスクを減少させる方法である。
		情報管理担当者	多要素認証は、何かを知っている（パスワード）、何かを持っている（トークンやスマートフォン）、何かである（指紋や顔認証）の3つの要素から2つ以上を組み合わせて認証を行う手法である。これにより、単一の認証手段が漏洩した場合でも、セキュリティを維持することができる。
データダイオード	データダイオード	組織幹部	データダイオードは、情報の一方向の流れを制御する電子部品である。組織の情報セキュリティ戦略の一部として、不正なデータの流入や流出を防ぐための重要な要素である。
		社員・職員全般	データダイオードは、情報が正しい方向にのみ流れることを保証するためのツールである。意図しないデータの漏洩や外部からの攻撃を防ぐことができる。
		情報管理担当者	データダイオードは、物理的または論理的なレベルでのデータの一方通行を実現する技術である。セキュリティポリシーに基づいて情報の流れを厳格に制御することができる。
トポロジ	トポロジ	組織幹部	トポロジは、ネットワークの物理的または論理的な構造を示すものである。効率的な通信と情報セキュリティの確保のために、適切なトポロジの選択と実装が必要である。
		社員・職員全般	トポロジは、デバイス間の接続方法やデータの流れのパターンを示すものである。日常の業務での通信の速度や信頼性を保つために、トポロジの理解が求められる。
		情報管理担当者	トポロジは、ネットワークの設計やトラブルシューティングにおいて基本的な要素である。セキュリティの観点からは、トポロジに基づいて適切なセキュリティ対策を施すことが重要である。
トラッシング	トラッシング	組織幹部	トラッシングは、捨てられたゴミから情報を収集する手法である。企業の機密情報や顧客情報が外部に漏れるリスクがあるため、適切な情報廃棄の方針を策定し、従業員への教育が必要である。
		社員・職員全般	トラッシングは、不要な書類やメモを適切にシュレッダーで処分することで防ぐことができる。業務上の情報を捨てる際は、十分な注意が必要である。
		情報管理担当者	トラッシング対策として、情報廃棄のガイドラインの策定や、定期的なセキュリティ教育、シュレッダーの設置などの物理的な対策が求められる。
二段階認証	ニダンカイニンショウ	組織幹部	二段階認証は、情報セキュリティの強化手段の一つである。パスワードだけでなく、追加の認証手段を導入することで、不正アクセスのリスクを低減することができる。
		社員・職員全般	二段階認証は、業務における情報の安全性を高めるための手段である。例えば、ログイン時にスマートフォンに送られる一時的なコードを入力することで、自身のアカウントの安全性を確保することができる。
		情報管理担当者	二段階認証の導入には、システムの設定や運用の見直しが必要である。また、ユーザーへの教育やサポート体制の整備も重要な要素となる。

ハードニング	ハードニング	組織幹部	ハードニングは、システムやアプリケーションのセキュリティを強化するための手法である。不要なサービスや機能を無効化することで、攻撃対象を減少させ、組織の情報資産を保護することができる。
		社員・職員全般	ハードニングは、使用しているコンピュータやソフトウェアのセキュリティを高めるための作業である。不要な機能をオフにすることで、外部からの不正アクセスのリスクを低減することができる。
		情報管理担当者	ハードニングを行う際は、システムの設定やパラメータを適切に調整し、不要なサービスやポートを閉じることが重要である。また、ハードニング後の動作確認を徹底的に行い、業務に支障が出ないようにする必要がある。
パッチ	パッチ	組織幹部	パッチは、ソフトウェアの不具合やセキュリティ上の脆弱性を修正するための修正プログラムである。適切なタイミングでのパッチ適用は、組織の情報セキュリティを維持し、業務の継続性を確保する上で極めて重要である。
		社員・職員全般	パッチは、コンピュータやソフトウェアの問題点を修正するためのアップデートである。定期的にシステムのアップデートを行うことで、業務の安全性と効率性を保つことができる。
		情報管理担当者	パッチは、特定の脆弱性や不具合を修正するためのコードである。公開されたパッチを速やかに適用することで、セキュリティインシデントのリスクを低減することができる。パッチの適用状況の監視と管理が必要である。
BadUSB	バッドユーエスビー	組織幹部	BadUSBは、USBデバイスのファームウェアレベルでの脆弱性を悪用した攻撃手法である。この攻撃は、組織の情報資産や業務の継続性に深刻なリスクをもたらす可能性がある。
		社員・職員全般	BadUSBは、正規のUSBデバイスに偽装して悪意のあるコードを実行する手法である。不明なUSBデバイスの使用は避け、組織内でのUSBデバイスの取り扱いには十分な注意が必要である。
		情報管理担当者	BadUSBは、USBデバイスのファームウェアを改ざんし、意図しない動作をさせる攻撃手法である。USBデバイスのファームウェアの検証や、USBポートの使用制限などの対策が必要である。
ファームウェア	ファームウェア	組織幹部	ファームウェアは、ハードウェアを制御するための組み込みソフトウェアである。企業の製品やシステムの基本的な動作を担保する要素であり、更新や管理が不適切であると、セキュリティリスクが高まる可能性がある。
		社員・職員全般	ファームウェアは、使用しているデバイスや機器の基本的な動作を制御するソフトウェアである。定期的な更新が必要であり、最新のセキュリティ対策が施されているか確認することが業務の一部として重要である。
		情報管理担当者	ファームウェアは、特定のハードウェア上で動作する低レベルのソフトウェアである。セキュリティの観点からは、ファームウェアの脆弱性が攻撃のターゲットとなることがあるため、定期的なアップデートや検証が不可欠である。
ファイアウォール	ファイアウォール	組織幹部	ファイアウォールは、組織のネットワークを外部の脅威から保護するセキュリティシステムである。適切な設定と管理が求められ、ビジネスの継続性と情報資産の保護に直結する要素である。
		社員・職員全般	ファイアウォールは、不正なアクセスや攻撃を防ぐための壁の役割を果たすシステムである。日常業務でのインターネット利用やデータのやり取りにおいて、安全な環境を提供するための重要なツールである。
		情報管理担当者	ファイアウォールは、ネットワークトラフィックを監視し、定義されたルールに基づいて許可または拒否するシステムである。適切なルールセットの設定やログの監視、定期的な更新が必要である。
ファイルレスマルウェア	ファイルレスマルウェア	組織幹部	ファイルレスマルウェアは、従来のマルウェアとは異なり、ディスクにファイルとして保存されることなくメモリ上で動作する脅威である。検出が難しくなるため、先進的なセキュリティ対策が必要である。
		社員・職員全般	ファイルレスマルウェアは、コンピュータのメモリ内でのみ動作するため、通常のウイルス対策ソフトでは検出が難しいマルウェアである。不審なメールの添付ファイルを開かないなど、日常の注意が求められる。
		情報管理担当者	ファイルレスマルウェアは、ディスク上に足跡を残さずに実行される新しいタイプの脅威である。エンドポイントのセキュリティ対策の強化や、メモリベースの攻撃を検出する高度なツールの導入が必要である。
VPN	ブイ・ピー・エヌ	組織幹部	VPNは、公開されているインターネット上で仮想的な専用ネットワークを構築する技術である。リモートからの安全なアクセスやデータの保護が可能となり、ビジネスの拡大や業務の柔軟性を高めることができる。
		社員・職員全般	VPNを利用することで、外部からも組織内のネットワークリソースに安全にアクセスすることができる。外出先や自宅からも業務を続けることが可能となる。
		情報管理担当者	VPN（Virtual Private Network）は、データの暗号化や認証機能を提供するため、外部の脅威からネットワークを保護することができる。適切な設定と管理を行うことで、情報の漏洩リスクを低減することができる。
フォレンジック	フォレンジック	組織幹部	フォレンジックは、情報セキュリティインシデントが発生した際の原因や影響を詳細に調査・分析する技術である。この技術を活用することで、組織のリスク管理や将来の対策の策定に役立てることができる。
		社員・職員全般	フォレンジックは、不正アクセスやデータ漏洩などのセキュリティインシデントの原因を突き止めるための手法である。日常業務中に異常を感じた場合やインシデントが疑われる場合には、この技術が活用される可能性がある。
		情報管理担当者	フォレンジックは、デジタルデータの取得、保存、分析を行うための専門的な技術と手法である。正確な証拠の収集や、証拠の改ざんを防ぐための手順が求められる。
踏み台	フミダイ	組織幹部	踏み台は、攻撃者が他のターゲットに攻撃を仕掛けるために利用する中継地点となるシステムやサーバーである。組織のシステムが踏み台として利用されると、組織の評価や信頼性に影響を及ぼす可能性がある。
		社員・職員全般	踏み台は、自身の業務端末やシステムが第三者に悪用されることを意味する。不審な通信や動作を発見した場合、迅速な報告が必要である。
		情報管理担当者	踏み台として利用されると、攻撃者の活動を隠蔽するための手段となる。定期的なログの監視や、不正な通信の検出を行い、踏み台としての利用を防ぐ対策が求められる。
ブラウザクラッシャ	ブラウザクラッシャ	組織幹部	ブラウザクラッシャは、特定のコードや内容をブラウザに読み込ませることで、ブラウザの動作を停止させる攻撃手法である。この攻撃は、組織のオンラインサービスへの信頼を損なう可能性がある。
		社員・職員全般	ブラウザクラッシャは、不正なウェブサイトやメールのリンクをクリックすることで発生することが多い。不審なリンクやメールは開かないよう注意が必要である。
		情報管理担当者	ブラウザクラッシャの攻撃を検知・防御するためのツールやシステムを導入し、定期的なセキュリティ教育を実施することが重要である。
ペネトレーションテスト	ペネトレーションテスト	組織幹部	ペネトレーションテストは、組織の情報セキュリティ対策の有効性を確認するための試験である。外部からの攻撃を模倣して、実際の脅威にどれだけの組織が耐えられるかを評価するものである。
		社員・職員全般	ペネトレーションテストは、私たちの業務環境がサイバー攻撃にどれだけ強いかを確かめるためのテストである。このテストを通じて、セキュリティの弱点や改善点を見つけ出すことができる。
		情報管理担当者	ペネトレーションテストは、組織のシステムやネットワークに対する脆弱性を特定し、それを修正するための具体的なアクションを提案するための実践的な手法である。
ボット	ボット	組織幹部	ボットは自動化されたプログラムであり、特定のタスクを自動的に実行するものである。組織のITインフラやデジタル資産を攻撃する悪意のあるボットも存在するため、適切な対策が必要である。
		社員・職員全般	ボットはインターネット上で自動的に動作するプログラムである。煩雑な作業を効率的に行うことができるが、悪意のあるボットには注意が必要である。
		情報管理担当者	ボットはスクリプトやプログラムを使用して自動的にタスクを実行するものである。セキュリティ対策として、ボットの挙動を監視し、不正なアクセスを検出・防止する必要がある。

ホワイトハッカー	ホワイトハッカー	組織幹部	ホワイトハッカーは、組織のセキュリティを強化するために、悪意のない目的でシステムの脆弱性を探る専門家である。彼らの知識と技術を活用することで、組織の情報資産を守ることができる。
		社員・職員全般	ホワイトハッカーは、我々のシステムやネットワークの安全性を確認するための「良いハッカー」である。彼らのフィードバックを受け入れ、セキュリティを向上させることが重要である。
		情報管理担当者	ホワイトハッカーは、エシカルハッキングの手法を使用して、組織のITインフラの脆弱性を特定し、報告する専門家である。彼らと連携し、セキュリティ対策を強化することが求められる。
ホワイトリスト	ホワイトリスト	組織幹部	ホワイトリストは、組織が許可する特定のアクセスや操作のみを明示的にリスト化したものである。不正なアクセスや操作を効果的に防ぐことができる。
		社員・職員全般	ホワイトリストは、業務で使用するアプリケーションやサービスが安全に動作するためのリストである。このリストに載っていないアプリケーションやサービスは使用しないようにすることが求められる。
		情報管理担当者	ホワイトリストは、システムやネットワークにおける許可された操作を明確に定義する手段である。不正なアクセスや攻撃を効果的に検知し、対処することができる。
RAT	ラット	組織幹部	RATは、外部から組織の情報システムに不正アクセスするためのマルウェアである。この攻撃により、機密情報の漏洩や業務の停止などの重大な影響が生じる可能性がある。
		社員・職員全般	RATは、メールの添付ファイルやダウンロードしたファイルを開くことで感染することが多い。不審なメールやファイルは開かず、必要な場合はIT部門に相談することが重要である。
		情報管理担当者	RAT（Remote Administration Tool ）の感染を防ぐためには、エンドポイントのセキュリティ対策の強化や、定期的なネットワークの監視・分析が必要である。また、従業員へのセキュリティ教育を継続的に行い、感染のリスクを低減することが求められる。
ランサムウェア攻撃	ランサムウェアコウゲキ	組織幹部	ランサムウェア攻撃は、組織の重要なデータを暗号化し、その解除のための身代金を要求するサイバー攻撃である。これにより、業務停止やブランドの信頼性低下などのリスクが生じる。
		社員・職員全般	ランサムウェア攻撃は、不正なメールの添付ファイルを開くことなどで感染することが多い。従業員一人ひとりが注意深く行動することで、攻撃のリスクを低減できる。
		情報管理担当者	ランサムウェア攻撃を防ぐためには、定期的なバックアップ、セキュリティソフトの更新、従業員への教育などの対策が必要である。
標準化とプロトコル			
イーサネット	イーサネット	組織幹部	イーサネットは、組織内のデバイスを相互に接続するための技術基準である。情報の迅速な共有とコミュニケーションの効率化が実現される。
		社員・職員全般	イーサネットは、私たちのオフィスや工場内でコンピューターや機器が通信するためのネットワーク技術である。データの送受信や共有がスムーズに行われる。
		情報管理担当者	イーサネットは、ローカルエリアネットワーク (LAN) の構築に使用される通信プロトコルである。セキュリティの観点からは、イーサネットの通信を監視し、不正なアクセスやデータの流出を防ぐための対策が必要である。
HTML	エイチ・ティー・エム・エル	組織幹部	HTMLは、ウェブページの構造や内容を定義するための言語である。組織のウェブサイトやウェブアプリケーションの基盤となる技術であり、ブランドイメージや顧客とのコミュニケーションに直接影響する要素である。
		社員・職員全般	HTMLは、ウェブページを表示するための基本的な言語である。日常業務で使用する社内システムや外部のウェブサイトは、このHTMLを基に作成されている。
		情報管理担当者	HTML（Hyper Text Markup Language）は、ウェブページの表示に使われるが、不適切なコードや外部からの不正なスクリプトの埋め込みがあると、セキュリティリスクとなる可能性がある。常に最新のセキュリティ対策を施し、安全なウェブページの提供を心掛ける必要がある。
HTTP	エイチ・ティー・ティー・ピー	組織幹部	HTTPは、インターネット上で情報をやり取りするためのプロトコルである。組織のウェブサイトやオンラインサービスの利用において、データの送受信の基盤となる技術である。
		社員・職員全般	HTTPは、ウェブブラウザやアプリケーションがウェブサーバーと通信する際の手段である。日常の業務でウェブサイトを閲覧する際やデータを送信する際に使用される。
		情報管理担当者	HTTP（Hyper Text Transfer Protocol）は、平文（暗号化されていないメッセージやデータ）での通信となるため、第三者にデータが傍受されるリスクがある。機密性の高い情報を扱う場合は、暗号化されたHTTPSを使用するなどのセキュリティ対策が必要である。
API	エー・ピー・アイ	組織幹部	APIは、異なるソフトウェアやサービス間でデータをやり取りするためのインターフェースである。組織のデジタル変革や業務効率化を実現するための重要な技術である。
		社員・職員全般	APIは、日常業務で使用する様々なシステムやアプリケーションが連携し、データを共有するための手段である。
		情報管理担当者	APIは外部とのデータのやり取りを行うため、不正なアクセスやデータの漏洩のリスクがある。適切な認証やアクセス制限、監視体制を整えることで、セキュリティを確保する必要がある。
SSL	エス・エス・エル	組織幹部	SSLは、インターネット上での情報の暗号化技術である。お客様や取引先との情報交換が安全に行われることを保証することができる。
		社員・職員全般	SSLは、ウェブサイトやメールなどの通信を暗号化する技術である。個人情報や業務データの漏洩リスクを低減することができる。
		情報管理担当者	SSLは、データの暗号化と認証を行うプロトコルである。適切な証明書の取得と管理、そして期限の監視が必要である。
SPF	エス・ピー・エフ	組織幹部	SPFは、組織のドメイン名を不正に使用した電子メールの送信を防ぐための技術である。ブランドの信頼性の保護やフィッシング攻撃のリスクを低減することができる。
		社員・職員全般	SPFは、受信したメールが正当な送信元からのものであるかを確認する技術である。偽装メールを効果的にフィルタリングすることができる。
		情報管理担当者	SPF（Sender Policy Framework）は、DNSに特定のレコードを設定することで、メールの送信元のIPアドレスを検証する技術である。正確な設定が求められるため、定期的な確認と更新が必要である。
FTP	エフ・ティー・ピー	組織幹部	FTPは、インターネット上でファイルを転送するためのプロトコルである。ビジネスの効率性を高めるためには、FTPの利用が考えられるが、セキュリティの観点からも適切な管理と利用が必要である。
		社員・職員全般	FTPは、業務でのファイルのやり取りに使用されるツールである。簡単に大量のデータを送受信できるが、セキュリティのリスクも伴うため、利用の際は注意が必要である。
		情報管理担当者	FTP（File Transfer Protocol）は、データの転送に使用されるが、暗号化されていない通信が行われるため、セキュリティの脅威となる可能性がある。そのため、FTPの代わりにセキュアなプロトコル（SFTPやFTPSなど）の利用や、適切なアクセス制御が必要である。
WPA2	ダブリュー・ピー・エー・ツー	組織幹部	WPA2は、無線ネットワークのセキュリティ規格である。これはデータ保護とアクセス制御を強化し、企業の情報漏洩リスクを低減する。セキュリティ基準を満たす上で重要な技術である。
		社員・職員全般	WPA2は、会社のWi-Fiの安全を守る技術である。これにより、個人情報や重要な業務データの保護が可能となり、無線ネットワークへの安全な接続が確保される。
		情報管理担当者	WPA2は、無線ネットワークのセキュリティを担うプロトコルである。強力な暗号化と認証機能を提供し、ネットワークのセキュリティを確保し、不正アクセスから保護するために重要である。
TLS	ティ・エル・エス	組織幹部	TLSは、組織の通信を保護するための暗号化プロトコルである。顧客データや業務情報の安全性が確保され、組織の信頼性が向上する。
		社員・職員全般	TLSは、私たちの通信を暗号化し、外部の攻撃者からのデータの盗聴や改ざんを防ぐ技術である。安全なウェブサイトやサービスを使用する際には、TLSが適切に実装されていることを確認する必要がある。
		情報管理担当者	TLS（Transport Layer Security）の実装と設定は、適切な暗号スイートの選択や証明書の管理が必要である。また、定期的なセキュリティ評価やパッチの適用を行い、最新の脅威から組織を守る必要がある。

DHCP	ディー・エイチ・シー・ピー	組織幹部	DHCPは、ネットワーク上のデバイスに自動的にIPアドレスを割り当てるプロトコルである。ネットワークの運用が効率化され、コスト削減に寄与する。
		社員・職員全般	DHCPを使用することで、私たちのデバイスはネットワークに自動的に接続される。しかし、不正なDHCPサーバからの攻撃に注意し、異常な通信には警戒する必要がある。
		情報管理担当者	DHCP（Dynamic Host Configuration Protocol）の適切な設定と管理は、ネットワークの安全性を確保するために重要である。不正なDHCPサーバの検出や、セキュリティポリシーの適用を行うことで、ネットワークを保護する必要がある。
DNS	ディー・エヌ・エス	組織幹部	DNSは、インターネット上のドメイン名をIPアドレスに変換するシステムである。このシステムの存在により、ユーザーは覚えやすいドメイン名でウェブサイトにアクセスできる。経営戦略として、DNSの正確性と迅速性はビジネスのオンラインプレゼンスと信頼性に直接影響する。
		社員・職員全般	DNSは、ウェブブラウザにURLを入力すると、背後でそのドメイン名をIPアドレスに変換してサイトに接続する役割を持つ。業務でのコミュニケーションや情報収集において、DNSの機能は中心的な役割を果たす。
		情報管理担当者	DNSは、インターネットの基盤となるサービスであるため、セキュリティの確保が不可欠である。DNSの設定ミスや脆弱性は、サービスの中断や情報の漏洩につながる可能性がある。
PSK	ピー・エス・ケー	組織幹部	PSKは、暗号化通信を確立する際に事前に共有される鍵である。不適切な管理や漏洩は、組織の情報セキュリティを脅かす要因となる。
		社員・職員全般	PSKは、通信の暗号化に使用される共有鍵である。この鍵の取り扱いには注意が必要であり、無関係な者との共有や記録は避けるべきである。
		情報管理担当者	PSK（Pre-Shared Key）は、VPNやWPA2などの暗号化プロトコルで使用される共有鍵である。鍵の長さや複雑性、定期的な変更などの管理策が求められる。
プロトコル	プロトコル	組織幹部	プロトコルは、コンピュータやネットワーク機器間の通信を行う際のルールや手順である。異なるデバイスやシステム間でも円滑に通信が行われる。
		社員・職員全般	プロトコルは、日常の業務で使用する様々なアプリケーションやサービスが正しく動作するための基盤となるルールである。
		情報管理担当者	使用するプロトコルの種類やバージョンによっては、セキュリティの脆弱性が存在することがある。定期的な更新やパッチの適用が必要である。
POP3	ポップ・スリー	組織幹部	POP3は電子メールの受信プロトコルの一つである。情報のセキュリティを確保するため、最新の暗号化技術や認証手段を使用することが推奨される。
		社員・職員全般	POP3はメールサーバからメールクライアントにメールをダウンロードするためのプロトコルである。安全な通信のため、設定やパスワードの管理に注意が必要である。
		情報管理担当者	POP3（Post Office Protocol version 3）は、メールの受信に使用されるプロトコルである。セキュリティ対策として、SSL/TLSを使用した暗号化通信を実装することが必要である。
MACアドレス	マックアドレス	組織幹部	MACアドレスは、ネットワーク上のデバイスを一意に識別するためのアドレスである。これを管理することで、組織のネットワークセキュリティを強化することができる。
		社員・職員全般	MACアドレスは、各デバイスがネットワーク上で持つ固有のアドレスである。正確なデバイスの識別やトラブルシューティングの際に参照されることがある。
		情報管理担当者	MAC（Media Access Control）アドレスは、ネットワークのアクセス制御やセキュリティポリシーの適用に利用される。不正なデバイスのネットワーク接続を防ぐためのフィルタリングにも使用される。
ネットワークのインフラとコンポーネント			
IoT	アイ・オー・ティー	組織幹部	IoTは、さまざまなデバイスがインターネットに接続され、データを収集・共有する技術である。効率的なビジネス運営や新しいビジネスモデルの創出が期待されるが、セキュリティの観点からも適切な管理が必要である。
		社員・職員全般	IoTは、私たちの業務をサポートするデバイスがインターネットにつながっている状態である。業務の効率化や便益が得られるが、不正アクセスのリスクもあるため、安全な使用が求められる。
		情報管理担当者	IoT（Internet of Things）は、多数のデバイスがネットワークに接続されるため、セキュリティの脅威が増大する可能性がある。各デバイスのセキュリティ設定やネットワークの監視を強化し、不正アクセスや情報漏洩を防ぐ必要がある。
IaaS	イアース	組織幹部	IaaSは、ITインフラをサービスとして提供するクラウドサービスの一つである。組織は物理的なインフラストラクチャの購入や管理の手間を省き、コストを削減することができる。
		社員・職員全般	IaaSは、サーバーやストレージなどのITインフラをオンデマンドで利用することができるサービスである。業務の拡大や変動に柔軟に対応することができる。
		情報管理担当者	IaaS（Infrastructure as a Service）の利用に際しては、セキュリティ設定やアクセス制御の適切な管理が必要である。クラウドプロバイダーが提供するセキュリティツールやサービスを活用し、組織の情報資産を守ることが求められる。
インターフェース	インターフェース	組織幹部	インターフェースは、異なるシステムやデバイス間で情報を交換するための接点や方法である。組織内の情報システムの統合や外部との連携が可能となる。
		社員・職員全般	インターフェースは、私たちが使用するソフトウェアやハードウェアが他のシステムと通信するための「入口・出口」である。異なるシステム間でのデータのやり取りがスムーズに行われる。
		情報管理担当者	インターフェースは、システム間のデータ交換のポイントである。セキュリティの観点からは、インターフェースを通じたデータの流入・流出を監視し、不正なアクセスやデータの改ざんを防ぐための対策が必要である。
SSID	エス・エス・アイ・ディー	組織幹部	SSIDは、無線LANネットワークの識別名である。適切な設定と管理が行われないと、外部からの不正アクセスのリスクが高まる可能性がある。
		社員・職員全般	SSIDは、私たちが接続する無線ネットワークの名前である。正しいSSIDを選択し、安全な接続を確保することが重要である。
		情報管理担当者	SSID（Service Set Identifier）は、無線LANのネットワーク識別子である。公開されるSSIDと非公開のSSIDの管理、および適切なセキュリティ設定が必要である。
オンラインストレージ	オンラインストレージ	組織幹部	オンラインストレージは、データをクラウド上で保存・共有するサービスである。業務の効率化やコスト削減に貢献するが、データ漏洩のリスクも伴うため、セキュリティポリシーの策定と従業員への教育が不可欠である。
		社員・職員全般	オンラインストレージは、どこからでもアクセス可能なデータ保存スペースである。しかし、機密情報のアップロードや共有時には、セキュリティガイドラインに従う必要がある。
		情報管理担当者	オンラインストレージの利用に際しては、エンドポイントのセキュリティ、アクセス制御、暗号化の実施など、多層的なセキュリティ対策が必要である。
外部記憶媒体	ガイブキオクバイタイ	組織幹部	外部記憶媒体は、データの移動やバックアップに使用されるデバイスである。情報の持ち出しや紛失のリスクがあるため、使用に関するポリシーと管理体制の整備が必要である。
		社員・職員全般	外部記憶媒体は、データの持ち運びや共有に便利である。しかし、紛失や盗難の際のリスクもあるため、機密情報の取り扱いには十分な注意が必要である。
		情報管理担当者	外部記憶媒体の使用に関しては、データの暗号化やアクセス制御、持ち出しの承認プロセスなど、セキュリティ対策の徹底が求められる。
仮想化	カソウカ	組織幹部	仮想化は、物理的なリソースを複数の仮想リソースとして利用する技術であり、コスト削減や効率的なリソース管理を実現する手段である。
		社員・職員全般	仮想化を利用することで、一つの物理的なマシン上で複数の作業環境を同時に動作させることができ、業務の柔軟性や迅速性が向上する。
		情報管理担当者	仮想化技術を適切に管理・運用することで、セキュリティの隔離やリカバリの迅速化などの利点を享受できるが、設定ミスや脆弱性の存在によりリスクも伴うである。

基幹システム	キカンシステム	組織幹部	基幹システムは、企業の中核となる業務を支えるITシステムである。これが停止すると、企業の業務に大きな影響が出るため、安定した運用と適切なセキュリティ対策が必要である。
		社員・職員全般	基幹システムは、日常の業務処理に不可欠なシステムである。システムの正しい利用方法を理解し、不正アクセスやデータの漏洩を防ぐための基本的なセキュリティ対策を実践することが求められる。
		情報管理担当者	基幹システムは、攻撃の主要なターゲットとなることが多い。定期的な脆弱性評価、パッチの適用、アクセス制御の強化など、多層的なセキュリティ対策を実施する必要がある。
クラウドサービス	クラウドサービス	組織幹部	クラウドサービスは、インターネットを通じて提供される情報技術のサービスである。初期投資を抑えつつ、柔軟にITリソースを利用することができる。
		社員・職員全般	クラウドサービスは、インターネット経由でアクセスできるサービスやアプリケーションである。場所を選ばずに業務を行うことができる。
		情報管理担当者	クラウドサービスは、外部のプロバイダが提供するサービスであるため、データの保護やアクセス制御などのセキュリティ対策が重要である。プロバイダとの契約時やサービスの利用時に、セキュリティ要件を確認し、適切な対策を講じる必要がある。
クローズドシステム	クローズドシステム	組織幹部	クローズドシステムは、外部との接続が限定された、厳格に管理されたシステムである。情報の漏洩リスクを低減するため、重要な情報を扱う場合などに採用されることが多い。
		社員・職員全般	クローズドシステムは、外部からのアクセスが制限された環境である。業務上、必要な情報のみを取り扱い、不要なデータの持ち出しや外部との共有を避けることが求められる。
		情報管理担当者	クローズドシステムは、外部の脅威から隔離された環境である。システムの設定やアクセス権限の管理、監視体制の構築が重要である。
検疫ネットワーク	ケンエキネットワーク	組織幹部	検疫ネットワークは、不審な通信やマルウェアを検出した際に、その通信を隔離するための特定のネットワーク領域である。組織全体への影響を最小限に抑えることができる。
		社員・職員全般	検疫ネットワークは、セキュリティ上の問題が疑われる通信を一時的に隔離するエリアである。不審な動きや通知があった場合は、速やかに情報管理部門に報告することが求められる。
		情報管理担当者	検疫ネットワークは、不正な通信や感染の疑いがあるデバイスを一時的に隔離するためのネットワークである。隔離後の分析や対応策の実施が必要である。
コネクトバック通信	コネクトバックツウシン	組織幹部	コネクトバック通信は、セキュリティの脅威となる可能性がある通信方法である。不正なアクセスやデータの漏洩を防ぐため、適切な対策が必要である。
		社員・職員全般	コネクトバック通信は、外部のサーバーから組織内のシステムに接続する通信である。不審な通信やアクセスを感知した場合は、速やかに情報管理部門に報告する必要がある。
		情報管理担当者	コネクトバック通信は、マルウェアや攻撃者が組織内のシステムと通信するための手法である。ファイアウォールやIDS/IPSを使用して、このような通信を検出し、ブロックする必要がある。
SaaS	サース	組織幹部	SaaSは、クラウド上で提供されるソフトウェアサービスである。初期投資を抑え、必要に応じてスケールアップやダウンが可能であるため、経営の柔軟性を高めることができる。
		社員・職員全般	SaaSは、インターネット経由でアクセスできるソフトウェアである。専用のインストールやアップデートの手間が不要で、いつでも最新の機能やセキュリティ対策が施されている。
		情報管理担当者	SaaS（Software as a Service）は、外部のサービスプロバイダが管理するため、セキュリティ対策やアップデートの負担が軽減される。しかし、データの保管場所やアクセス制御、サービスのSLA（サービスプロバイダーと顧客の間の契約で、提供されるサービスの品質と基準）を確認し、適切なリスク管理を行う必要がある。
サーバー	サーバー	組織幹部	サーバーは、組織のデータやアプリケーションを中心的に管理するコンピュータである。適切な運用と管理により、業務の効率化と情報資産の保護が実現される。
		社員・職員全般	サーバーは、共有ファイルや業務アプリケーションを提供するコンピュータである。日常業務で使用する多くの情報やツールがサーバー上に保存されている。
		情報管理担当者	サーバーは組織の情報資産を集約するため、セキュリティ対策が不可欠である。定期的なパッチ適用、アクセス制御、監視体制の構築など、多岐にわたる管理が求められる。
サーバー証明書	サーバーショウメイショ	組織幹部	サーバー証明書は、組織のウェブサイトの信頼性と安全性を保証するための電子証明書である。顧客や取引先との信頼関係を強化し、ビジネスの信頼性を向上させることができる。
		社員・職員全般	サーバー証明書は、ウェブサイトを安全に利用するための証明書である。ウェブサイト上での情報のやり取りが暗号化され、第三者による情報の盗み見や改ざんを防ぐことができる。
		情報管理担当者	サーバー証明書は、SSL/TLS通信を実現するための鍵となる証明書である。証明書の取得、更新、適切な管理が必要であり、期限切れや不正な証明書の使用を防ぐための監視が求められる。
CDN	シー・ディー・エヌ	組織幹部	CDNは、ウェブコンテンツを高速に配信するためのネットワークサービスである。ユーザー体験が向上し、ビジネスの成果に寄与する。しかし、セキュリティの観点からも適切な管理と監視が必要である。
		社員・職員全般	CDNは、ウェブサイトやアプリケーションの動作を高速化するためのサービスである。日常業務でのウェブ利用時に、快適なアクセス速度を実現するためのものである。
		情報管理担当者	CDN（Contents Delivery Network）は、コンテンツのキャッシュや配信を最適化するが、誤った設定や脆弱性があると攻撃の対象となる可能性がある。そのため、セキュリティ設定の適切な適用や、定期的な脆弱性評価が必要である。
重要インフラ	ジュウヨウインフラ	組織幹部	重要インフラは、組織の業務遂行や社会の機能を維持するために不可欠なシステムやネットワークである。これを適切に保護・管理することは、組織の存続や社会の安全に直結する重要な課題である。
		社員・職員全般	重要インフラは、私たちの業務活動を支える基盤となるシステムやサービスである。これが停止した場合、業務の遂行が困難となるため、常に注意深く取り扱う必要がある。
		情報管理担当者	重要インフラは、攻撃者の標的となりやすい重要な資産である。これを保護するためのセキュリティ対策や監視体制の強化が求められる。
スイッチ	スイッチ	組織幹部	スイッチは社内ネットワークの中心的な装置で、情報の流れを効率的に管理し、セキュリティを確保する重要な機能を持っている。企業の情報セキュリティを強化するためには、適切なスイッチの選択と管理が不可欠である。
		社員・職員全般	スイッチとは、社内ネットワークにコンピュータやデバイスを接続するための装置である。この装置によって社内の情報共有やインターネットアクセスが可能となる。セキュリティを確保するためには、正しい使用方法の理解が重要である。
		情報管理担当者	スイッチはネットワーク内でのデータ転送を制御し、デバイス間の通信を効率化する装置である。これによりネットワークのパフォーマンスが向上し、セキュリティ対策も強化される。適切な設定と維持管理が必要である。
ドメイン	ドメイン	組織幹部	ドメインは、インターネット上の特定の場所や組織を識別するためのアドレスである。ブランドや組織のオンラインでの信頼性と認知度を確保するために、適切なドメイン名の選択と管理が必要である。
		社員・職員全般	ドメインは、ウェブサイトやメールアドレスの一部として使用されるものである。業務上のコミュニケーションや情報の共有において、ドメインの正確さと信頼性が求められる。
		情報管理担当者	ドメインは、組織のオンラインプレゼンスを識別する要素である。ドメインのセキュリティ対策やドメインの乗っ取りを防ぐための管理が、情報管理担当者にとって重要なタスクである。

ノード	ノード	組織幹部	ノードは、ネットワーク上の端点や接続点を指す用語である。組織のITインフラの構成や拡張性を理解する上で、ノードの役割や配置は重要な要因となる。
		社員・職員全般	ノードは、業務の効率や安定性に影響を与える可能性がある。例えば、サーバーやワークステーションなどのノードが適切に配置されているか、定期的にメンテナンスが行われているかが重要である。
		情報管理担当者	ノードごとのセキュリティ設定やパッチの適用は、情報セキュリティの観点から極めて重要である。また、ノード間の通信を監視し、不正なアクセスや攻撃を検知する体制を構築することが求められる。
PaaS	パース	組織幹部	PaaSは、クラウドサービスの一つであり、アプリケーションを開発・運用するためのプラットフォームを提供するサービスである。組織としては、インフラの設置や運用の手間を省き、迅速にビジネスを展開することが可能である。
		社員・職員全般	PaaSは、アプリケーションの開発や運用に必要なツールやサービスをクラウド上で利用できるサービスである。自分たちでサーバーやミドルウェアを管理する必要がなく、業務に集中することができる。
		情報管理担当者	PaaS（Platform as a Service）を利用する際は、プラットフォームのセキュリティ設定やアクセス制御を適切に行うことが重要である。また、サービス提供者からのセキュリティアップデート情報を常にチェックし、必要な対応を行う必要がある。
パケット	パケット	組織幹部	パケットは、情報を小さな単位に分割してネットワーク上で送受信するデータのことである。業務の効率やセキュリティに影響する要素であるため、適切なネットワーク環境の整備が必要である。
		社員・職員全般	パケットは、コンピュータやスマートフォンがインターネット上で情報をやり取りする際のデータの単位である。業務のスムーズな進行のため、ネットワークの状態を確認することが重要である。
		情報管理担当者	パケットは、ネットワーク上でのデータの移動を表すものである。不正なパケットの検知やフィルタリングを行うことで、外部からの攻撃を防ぐための対策が必要である。
VDI	ブイ・ディー・アイ	組織幹部	VDIは、仮想化技術を活用して中央のサーバー上でデスクトップ環境を提供するシステムである。組織のIT資産管理やセキュリティ対策の集中管理が可能となり、コスト削減や業務効率の向上が期待できる。
		社員・職員全般	VDIを使用することで、どのデバイスからでも統一されたデスクトップ環境にアクセスできる。リモートワークや出張先からも安全に業務を行うことができる。
		情報管理担当者	VDI（Virtual Desktop Infrastructure）は、ユーザーのデータやアプリケーションを中央のサーバー上で一元管理するため、セキュリティアップデートやパッチの適用、不正アクセスの監視などのセキュリティ対策を効率的に行うことができる。
ポート	ポート	組織幹部	ポートは、情報通信を行うための通信チャンネルの入出口である。不要なポートを開放していると、セキュリティリスクが高まる可能性があるため、適切な管理が求められる。
		社員・職員全般	ポートは、コンピュータやネットワークが外部と通信する際の扉のようなものである。この扉を適切に管理しないと、不正なアクセスのリスクが高まる。
		情報管理担当者	ポートは、特定のサービスやアプリケーションがネットワーク通信を行うためのエンドポイントである。開放されているポートの監視や不要なポートの閉鎖は、セキュリティ対策の基本的な要素の一つである。
LAN	ラン	組織幹部	LANは、一定の地域内で複数のデバイスを接続するためのネットワークシステムである。組織の業務効率を向上させるための基盤として不可欠である。
		社員・職員全般	LANは、オフィス内のコンピュータやプリンタなどのデバイスが相互に通信するためのネットワークである。日常の業務で情報を共有する際に使用される。
		情報管理担当者	LANは内部ネットワークであるため、外部からの不正アクセスを防ぐセキュリティ対策が必要である。また、内部からの情報漏洩も考慮し、適切なアクセス制御を施す必要がある。
ルータ	ルータ	組織幹部	ルータは、情報の流れを適切に誘導する装置である。組織の情報通信インフラの安定性や効率を保つため、ルータの適切な管理と投資が必要である。
		社員・職員全般	ルータは、インターネットや内部ネットワークへの接続を中継する装置である。業務での情報のやり取りをスムーズに行うため、ルータの存在と役割を理解することが重要である。
		情報管理担当者	ルータは、ネットワークのトラフィックを制御する中核的な装置である。外部からの不正アクセスを防ぐため、ファイアウォール機能やアクセス制御の設定が必要である。
WAN	ワン	組織幹部	WANは、広範囲にわたる地域をカバーするネットワークである。複数の拠点間の通信を実現するため、組織のビジネス展開や業務効率化に寄与する。
		社員・職員全般	WANは、異なる場所にあるオフィスや拠点間をつなぐネットワークである。これにより、遠隔地の同僚や情報とスムーズに連携することができる。
		情報管理担当者	WAN（Wide Area Network）は、外部との接続点となるため、セキュリティの脅威が高まる。適切なファイアウォールの設定やVPNの利用など、セキュリティ対策を強化する必要がある。
プログラミングと開発			
SQL	エス・キュー・エル	組織幹部	SQLは、データベースから情報を取得、更新、削除するための言語である。組織のビジネスデータを管理する上で、この技術は中心的な役割を果たしている。
		社員・職員全般	SQLは、日常の業務で使用するシステムやアプリケーションの背後にあるデータベースとのコミュニケーションに使われる言語である。
		情報管理担当者	SQL（Structured Query Language）は、データベース操作を行う際の基本的な言語である。適切なセキュリティ対策を施さないと、外部からの攻撃を受けやすくなる可能性がある。
コード	コード	組織幹部	コードは、業務やサービスをサポートするためのプログラムの集合である。適切なコードの管理と更新は、組織の競争力を保つために不可欠である。
		社員・職員全般	コードは、業務を効率的に行うためのツールやアプリケーションを動かす基盤である。正確なコードの使用と理解は、業務の品質を向上させる。
		情報管理担当者	コードは、セキュリティの脆弱性が存在する可能性がある。定期的なコードの監査や脆弱性のスキャンを行い、必要に応じて修正や更新を行う必要がある。
スクリプト	スクリプト	組織幹部	スクリプトは、一連の命令を自動的に実行するプログラムである。業務の効率化や自動化に貢献するが、不正なスクリプトによる攻撃も存在するため、適切な管理が必要である。
		社員・職員全般	スクリプトは、繁 repetitiveな作業を自動化するためのツールである。しかし、不明なスクリプトを実行するとセキュリティリスクがあるため、使用する際は十分な注意が必要である。
		情報管理担当者	スクリプトは、業務の自動化やシステムの管理に使用されるが、スクリプトの脆弱性や不正なスクリプトによる攻撃がある。スクリプトのソースを確認し、定期的なセキュリティチェックを行うことが重要である。

システム管理			
キャッシュ	キャッシュ	組織幹部	キャッシュは、データや情報を一時的に保存して高速にアクセスするための技術である。適切に管理されないと、古いデータや不正確な情報が表示されるリスクがある。
		社員・職員全般	キャッシュは、業務アプリケーションの動作を高速化するために使用される。しかし、キャッシュのデータが古くなると、誤った情報が表示される可能性があるため、定期的な更新や確認が必要である。
		情報管理担当者	キャッシュは、セキュリティの観点からも注意が必要である。キャッシュのデータが漏洩すると、機密情報が外部に露出するリスクがある。キャッシュの保存場所やアクセス制御を適切に設定し、定期的な監査を行うことが重要である。
BIOS	バイオス	組織幹部	BIOSは、コンピュータが起動する際の基本的な動作を制御するプログラムである。正確なBIOSの設定は、組織のIT資産の安全性と効率的な運用を保証するために重要である。
		社員・職員全般	BIOSは、コンピュータを起動するときの初期設定やハードウェアの動作を管理するものである。誤った設定をすると、コンピュータが正常に動作しなくなることがあるため、無闇に変更しないよう注意が必要である。
		情報管理担当者	BIOS（Basic Input/ Output System）の設定は、セキュリティの観点からも重要である。パスワードの設定やブート順序の変更など、適切なセキュリティ設定を行うことで、不正なアクセスやマルウェアの感染リスクを低減することができる。
ベンダー	ベンダー	組織幹部	ベンダーは、組織が利用する製品やサービスを提供する外部の企業や団体である。適切なベンダーの選定と管理は、組織の業績とリスク管理に直接影響を与える。
		社員・職員全般	ベンダーは、私たちの業務をサポートするための製品やサービスを提供する企業である。彼らとの良好な関係を維持することは、スムーズな業務遂行のために重要である。
		情報管理担当者	ベンダーは、多くの場合、組織のIT環境の一部を構成する。そのため、ベンダーのセキュリティ対策や製品の品質は、組織全体のセキュリティリスクを左右する要因となる。
ユーザー権限	ユーザーケンゲン	組織幹部	ユーザー権限は、情報システム上での各ユーザーの役割や業務に応じたアクセス権を定義するものである。適切な権限管理を行わないと、情報の漏洩や不正アクセスのリスクが高まる。
		社員・職員全般	ユーザー権限は、自分の業務に必要な情報や機能のみにアクセスできるように制限されている。不要な情報や機能へのアクセスは避け、権限外の操作を行わないよう注意する必要がある。
		情報管理担当者	ユーザー権限の管理は、最小権限の原則に基づき、定期的な見直しや監査を行うことで、不正アクセスや情報漏洩のリスクを低減することができる。
リンク	リンク	組織幹部	リンクは、情報を伝達するための接続点である。組織の業務効率や情報の流通において、適切なリンクの管理は経営戦略の一部として重要である。
		社員・職員全般	リンクは、コンピュータやデバイス間で情報をやり取りするための接続である。日常の業務で使用するシステムやデータベースへのアクセスには、リンクを通じて行われる。
		情報管理担当者	リンクは、ネットワーク上でのデータの伝送路である。不正なアクセスやデータの漏洩を防ぐため、リンクのセキュリティ対策や監視が必要である。
ログ	ログ	組織幹部	ログは、システムやアプリケーションの動作履歴を記録するものである。業務の透明性を確保し、不正アクセスやシステム障害の原因を追跡するための重要な手がかりとなる。
		社員・職員全般	ログは、私たちが行う業務操作やシステムの動作状況を時系列で記録するものである。問題が発生した際の原因特定や業務の改善点を見つける手助けとなる。
		情報管理担当者	ログは、セキュリティインシデントの検出や分析、対応のための重要な情報源である。定期的なログの監査を行い、異常な動きや脅威を早期に検出することが必要である。
その他			
生成AI	セイセイエイアイ	組織幹部	生成AIは、データを基に新しい情報やコンテンツを生成する技術である。新しいビジネスチャンスや効率化が期待されるが、誤った情報の生成や悪用のリスクもある。
		社員・職員全般	生成AIを利用することで、日常の業務やレポート作成などが効率化される可能性がある。しかし、生成された情報の正確性を確認することが必要である。
		情報管理担当者	生成AIの技術は、セキュリティの脅威としても利用される可能性がある。生成された情報の真偽を確認するツールやプロセスの導入が必要である。