セキュリティソリューションガイド

SECURITY SOLUTION GUIDE

キヤノンマーケティングジャパン株式会社

本ガイドは、組織の情報セキュリティ対策ご担当の方を対象に、サイバーセキュリティ対策に取り組む際の参考として活用されることを想定しています。高度な脅威動向、次世代セキュリティモデル、そして、具体的な課題と対策方法をなるべくわかりやすく説明した内容となっています。お客さまのセキュリティ強化にお役立ていただけますと幸いです。

情報セキュリティにおける脅威の現状

IPA（独立行政法人情報処理推進機構）は、情報セキュリティにおける脅威のうち、2023年に社会的影響が大きかったトピックを「情報セキュリティ10大脅威2024」として発表しました。
「情報セキュリティ10大脅威」を通じて、高度な脅威の特徴や影響範囲など、組織がセキュリティ対策を行う際の参考となる情報を得ることができます。ランキングの下位にあるからといって、影響度が小さいわけではありません。組織における重要度や緊急度を見極めて、必要な対策を順次実施していくことが重要です。

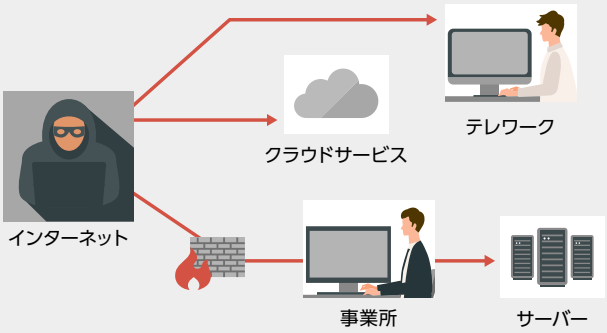
出典：IPA「情報セキュリティ10大脅威 2024」

情報セキュリティ10大脅威 2024

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6	不注意による情報漏えい等の被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	テレワーク等のニューノーマルな働き方を狙った攻撃
10	犯罪のビジネス化（アンダーグラウンドサービス）

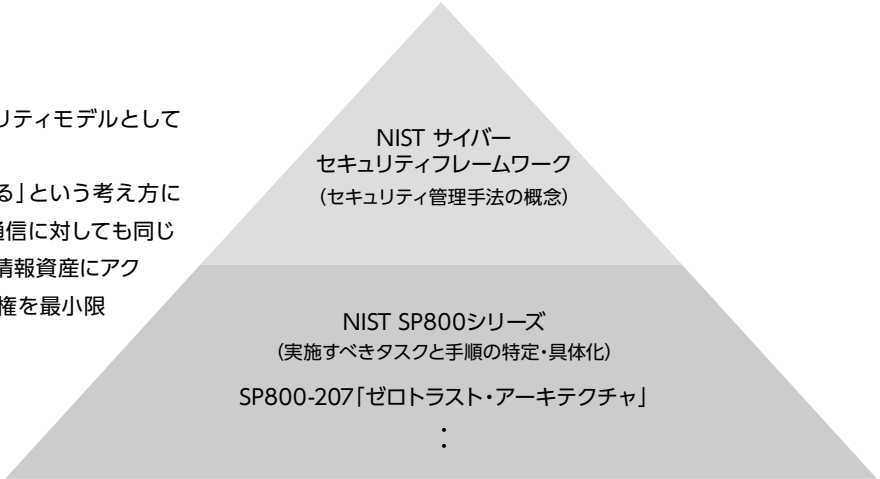
セキュリティ対策の見直しの必要性

既に対策を実施している脅威に対しても定期的な見直しが必要です。脅威を取り巻く環境は対策当時と同一というわけではありません。
現在は、テレワークやクラウドサービスの普及によりサイバー攻撃の標的となる対象（アタックサーフェス）が拡大し、さらに、攻撃の巧妙化により、従来の境界型セキュリティ対策では対応しきれないケースが生じています。また、万が一社内に侵入されると、不正に入手したアカウントを利用して次々に機密情報にアクセスされるなど、被害の拡大を防ぐことが難しいとされています。



新しいセキュリティモデルの登場

従来の境界型セキュリティ対策に代わる次世代のセキュリティモデルとして「ゼロトラスト」という概念が注目されています。
ゼロトラストは、「すべての通信を信頼せず、認証・検証する」という考え方に基づいています。外部からの通信だけでなく、組織内部の通信に対しても同じセキュリティ要件を満たす必要があるというものです。また、情報資産にアクセスするユーザーやデバイスを特定し、ユーザーのアクセス権を最小限にすることもゼロトラストの考え方の一つとなっています。



ゼロトラストの考え方

業種や規模を問わず、多くの組織がサイバーセキュリティ対策のガイドラインとして、NIST（米国国立標準技術研究所）のCSF（サイバーセキュリティフレームワーク）を参考にしています。このCSFの下位概念に位置付けられるドキュメント類の一つに「ゼロトラスト・アーキテクチャ」が存在します。
「ゼロトラスト・アーキテクチャ」にはゼロトラストの7つの基本的な考え方が記されていますが、必要とされる対策はさまざまであり、単一のソリューションでゼロトラストが実現するわけではありません。また、ゼロトラストありきではなく、その考え方を考慮に入れて、具体的な目的や課題に取り組むことが大切です。

ゼロトラスト　7つの原則

		要約	代表的な要素
1	すべてのデータソースとコンピューティングサービスをリソースとみなす	保護すべき情報資産を把握する	IT資産管理
2	ネットワークの場所に関係なく、すべての通信を保護する	社内や自宅、外出先等、場所に関わらず、すべての通信を保護する	SASE
3	企業リソースへのアクセスをセッション単位で許可する	情報資産に対する必要最小限の権限を付与する	
4	リソースへのアクセスは、動的ポリシーにより決定する	情報資産へのアクセスはリクエスト毎に許可する	
5	すべての資産の整合性とセキュリティ動作を監視し、測定する	情報資産のセキュリティ状態を維持・監視する	EDR
6	すべてのリソースの認証と認可を行い、アクセスが許可される前に厳格に実施する	情報資産へのアクセスに伴う認証を強化する	IDaaS
7	資産、インフラ、通信の現状について情報を収集し、セキュリティ態勢の改善に利用する	ログ情報を収集・分析して、セキュリティ対策の改善に利用する	SIEM

高度な脅威に対抗するソリューション

キヤノンマーケティングジャパングループでは、ゼロトラストに関連する要素を備えた、高度な脅威に対抗するソリューションを体系的にご用意しています。グループで長年にわたり蓄積してきたサイバーセキュリティ対策のノウハウや経験を活かして、具体的な課題への対策と、ゼロトラストの段階的な導入を支援します。サイバーセキュリティ対策の継続的改善や高度化に向けて、お客さまの環境に適したセキュリティソリューションをご提供します。

外部脅威	ランサムウェアの被害を防ぎたい	EDR	メールセキュリティ	データ保護	イミュータブルストレージ
	ビジネスメール詐欺の被害を防ぎたい	メールセキュリティ	セキュリティ教育	標的型攻撃メール訓練	
	クラウドサービスを安全に利用したい	IDaaS	SASE	Webフィルタリング	
内部脅威	内部不正による情報漏えいを防ぎたい	メールセキュリティ	IT資産管理	Webフィルタリング	
	不注意による情報漏えい等を防ぎたい	メールセキュリティ	HDD暗号化	物品管理	暗号化消去
運用管理	脆弱性対応を効果的に進めたい	脆弱性情報収集提供	脆弱性・パッチ管理	脆弱性診断	WAF
	セキュリティ対策の運用負荷を軽減したい	SIEM	SOC／MSS	CSIRT	MDR

外部脅威

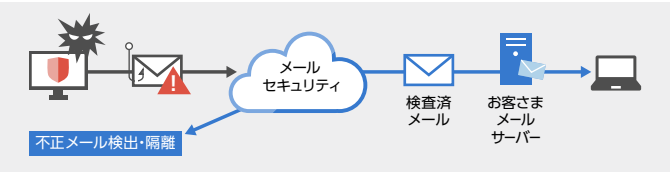
ランサムウェアの被害を防ぎたい

ランサムウェアは、身代金を意味する「Ransom」と「Software」を組み合わせた造語であり、PCに侵入してファイルを不正に暗号化し、ファイルの復号と引き換えに金銭を要求するマルウェアです。当初は、データを暗号化して身代金を要求していましたが、近年は暗号化と同時にデータを外部に盗み出し、身代金を支払わなければ盗み出したデータを公開するという二重の脅迫（ダブルエクストーション）が行われるなど、手口が悪質化しています。

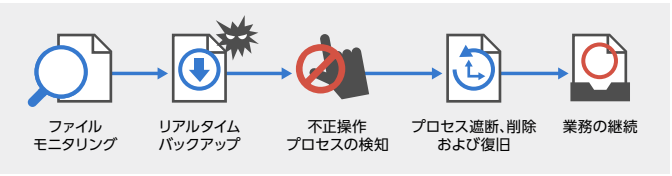
主な対策

EDR（Endpoint Detection and Response）は、PCなどエンドポイントに組み込んだエージェントから情報を収集し、マルウェアやランサムウェアによる不審な動きがないか、常時監視を行います。脅威の侵入を防ぐのではなく、侵入した脅威を検出し、修復を行うのがEDRの目的です。事前対策（EPP：Endpoint Protection Platform）と事後対策を組み合わせることで、より効果的な対策を行うことが可能になります。

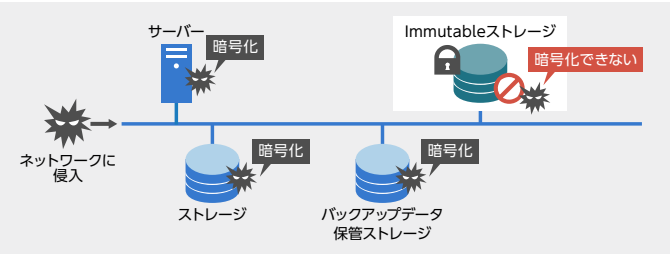
メールセキュリティのさまざまな機能を利用して、マルウェアの侵入を防ぐことができます。不正プログラム検索機能は、添付ファイルの検査を行い、マルウェアが含まれていた場合にそれらを駆除、またはメールやファイルを隔離します。Webレピュテーション機能は、メール本文や添付ファイル内に含まれるURLの検査を行い、不審なURLが含まれていた場合にメールの削除や隔離を行います。



最近では、元データだけでなく、バックアップデータにまでランサムウェアの被害が及ぶケースも報告されており、事業継続の観点からもさらなるデータ保護への取り組みが急務となっています。新たな対策として、シグネチャを使用しない独自の状況認識技術により、未知のランサムウェア被害を防ぐことが可能です。また、リアルタイムバックアップによるファイルの復元も可能です。



イミュータブルストレージは、ランサムウェアなどによるデータの改変や削除を防止するストレージです。イミュータブルは、直訳すると「変更不可能な」となります。バックグラウンドで定期的に変更不可能なスナップショットを取得することで、ランサムウェア攻撃や不正アクセスによるデータの改ざんや削除があっても、スナップショットを使って正常時の状態に復旧することができます。



商品概要

ESETセキュリティ ソリューションシリーズ	ESET社のEDR製品は長年培ってきた脅威検知のテクノロジーが用いられており、EPPと1つのソリューションとして提供されるため、ソリューション間での連携や相関分析といった複雑な開発や設定を必要とせずに短期間で導入することが可能です。（サービス開発・提供元：ESET, spol. s r.o.）
GUARDIANWALL Inbound Security for Mail Gateway	AI技術やサンドボックスによる解析を用いて、ランサムウェアやビジネスメール詐欺などの高度な脅威からさまざまなメール環境を保護するクラウド型メールセキュリティサービスです。（サービス開発・提供元：キヤノンマーケティングジャパン株式会社）
AppCheck	マルウェア対策ソフトウェアとの併用が可能なランサムウェア対策ソフトウェアです。状況認識技術を使用して、ファイルの変更箇所や速度、頻度などを監視し、ランサムウェアによるファイル操作をリアルタイムに検出します。（サービス開発・提供元：株式会社JSecurity）
OneXafe	ランサムウェア対策に有効なバックアップデータ保存用イミュータブルストレージです。SMB／NFS共有経由でバックアップデータを書き込める一方、定期的に変更不可能なスナップショットを取得します。ご利用には別途バックアップソフトとしてARCServe UDPまたはARCServe Backupが必要です。（サービス開発・提供元：Arcserve, LLC）

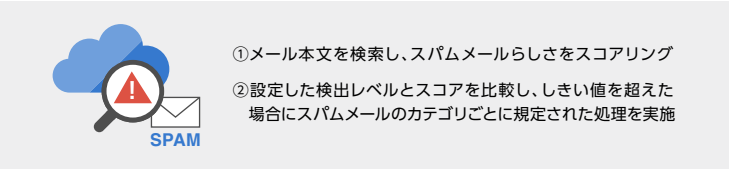
外部脅威

ビジネスメール詐欺の被害を防ぎたい

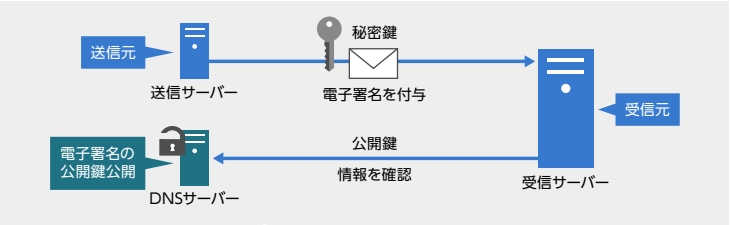
ビジネスメール詐欺（BEC：Business Email Compromise）は取引先や経営者などになりすまし、送金を促すメールを送りつける標的型攻撃の一種です。サーバーに侵入し、送受信の履歴をもとに、メールのやり取りに紛れ込んで振込先の変更などを促し、金銭の詐取を行うといった緻密かつ巧妙な攻撃も確認されています。対策としては、メールセキュリティの機能を実装すると同時に、従業員一人ひとりがビジネスメール詐欺の手口を知り、日常的に注意を払うことが必要です。

主な対策

メールセキュリティの一つであるスパムメール対策機能を利用して、ビジネスメール詐欺の被害にあうリスクを低減することができます。スパムメール対策機能によりメール本文の検査を行い、支払いに関する文言や緊急性を表す記載、行動を促す記載の有無を判断し、ビジネスメール詐欺と思われるメールを検知します。

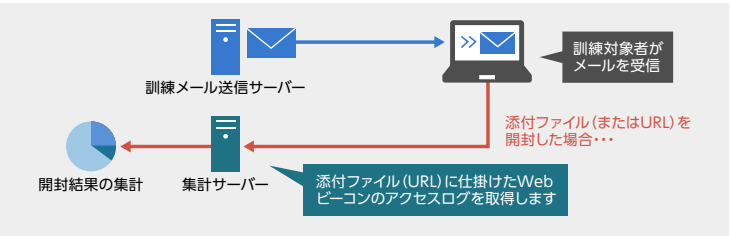


送信ドメイン認証（DKIM：DomainKeys Identified Mail）は、メールの送信時に電子署名を付与し、受信者が署名の検証を行うことで、なりすましや改ざんを検知できるようにする仕組みです。メールの送信者情報を電子署名で照合するため、送信者本人から来たものかどうかを確認し、メールの信頼性を高めることが可能になります。



定期的なセキュリティ教育を行うことで、従業員の情報セキュリティに対する意識やリテラシーを高め、インシデントの発生を抑制する効果が見込まれます。単なる啓蒙活動に留まらず、サイバー攻撃の兆候を見抜き、機密情報を危険にさらさないために必要な知識を身に付けて、従業員の行動を変化させることが目的です。

標的型攻撃メール訓練は、セキュリティ教育の一環として実施される、標的型攻撃を想定した不審メールの対処に関する訓練サービスです。メールを用いた攻撃に対する危機意識とセキュリティ意識が向上し、件名や本文を注意して確認し、不用意に開封しないなどの理解促進が図れます。



商品概要

GUARDIANWALL Inbound Security for Mail Gateway	AI技術やサンドボックスによる解析を用いて、ランサムウェアやビジネスメール詐欺などの高度な脅威からさまざまなメール環境を保護するクラウド型メールセキュリティサービスです。 （サービス開発・提供元：キヤノンマーケティングジャパン株式会社）
GUARDIANWALL Mailセキュリティ・クラウド	「MailFilter on Cloud」、「MailConvert on Cloud」、「MailArchive on Cloud」から構成されているクラウド型メールセキュリティサービスです。いずれもスパムメール対策の一環として、DKIMに対応しています。 （サービス開発・提供元：キヤノンマーケティングジャパン株式会社）
セキュリティ教育サービス	情報セキュリティに関する知識やスキルを養い、悪意ある行為から組織を守る上で取るべき行動や対策を理解、習得することで、組織のリスクを軽減するための研修サービスです。（サービス開発・提供元：株式会社ブロードバンドセキュリティ）
標的型攻撃メール訓練サービス	標的型攻撃メールの疑似メールを送る訓練サービスです。日々送られてくるメールに対し、標的型攻撃のメールであるか否かを判断する力を養い、組織のリスクを軽減させる訓練サービスです。（サービス開発・提供元：株式会社ブロードバンドセキュリティ）

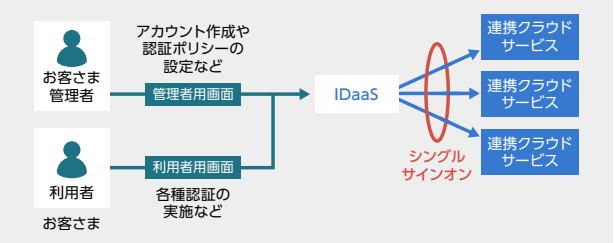
外部脅威

クラウドサービスを安全に利用したい

従来のセキュリティモデルは、社内ネットワークとインターネットに分けて対策を行う「境界型セキュリティ対策」が一般的でしたが、テレワークやクラウドサービスの普及によって外部から社内ネットワークに接続する必要性が生じるなど、多様な通信を前提とした「ゼロトラストセキュリティ対策」が求められるようになりました。このような複雑で多様なIT環境において、煩雑なアクセス管理や不審な通信の検知を行うには単一のソリューションでは難しいとされています。このため、SASEのような包括的なセキュリティ対策が注目されるようになりました。

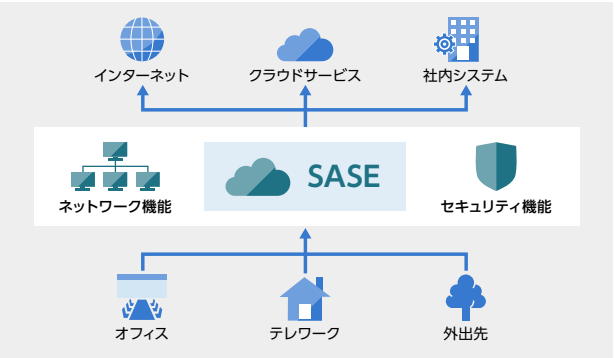
主な対策

IDaaS（Identity as a Service）は、ID管理や多要素認証、シングルサインオンなどを提供するクラウドサービスです。社内システムやクラウドサービスへのログイン時に必要なアカウントを統合して管理することにより、運用負荷を軽減できるだけでなく、多要素認証や証明書を利用した高度な認証によるセキュリティの強化が図れます。ゼロトラストは「すべての通信を信頼しない」という考え方に基づくセキュリティモデルであり、認証の強化はその根幹となるため、IDaaSはゼロトラストの実現に欠かせない要素の一つとなります。

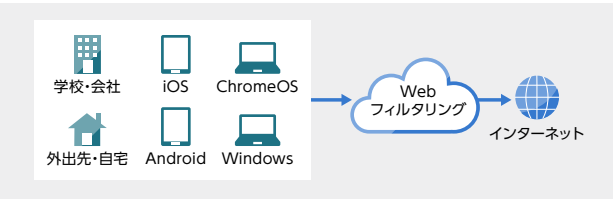


SASE（Secure Access Service Edge）はネットワーク機能とセキュリティ機能を1つにまとめて提供するクラウドサービスです。これにより、複数のセキュリティ製品を一元化し、管理作業やポリシーの徹底が効率的に行えます。主な機能として以下が含まれますが、現状は提供するベンダーによってサービスの内容が異なっています。

- ・CASB　：クラウドサービスの利用状況の監視・可視化（Cloud Access Security Broker）
- ・SWG　：Webアクセスのセキュリティ強化（Secure Web Gateway）
- ・ZTNA　：リモートアクセスのセキュリティ強化（Zero Trust Network Access）
- ・SD-WAN：ソフトウェアによるネットワーク管理（Software Defined Wide Area Network）



Webフィルタリングは、業務に関係のないWebサイトへのアクセスや、マルウェアに感染するリスクのあるWebサイトへのアクセスをフィルタリングする機能です。クラウドサービスとして提供することにより、社内だけでなくテレワークや外出先でのWebアクセスを監視することが可能になるため、デバイスや利用者のロケーションに依存しない安全なWebアクセス環境を実現します。



商品概要

ID Entrance	クラウドサービスを利用する際のIDやパスワードなどの情報を統合管理し、シングルサインオン機能により複数のアプリケーションやサービスを1つのID・パスワードで利用できるクラウド型ID管理サービスです。 （サービス開発・提供元：キヤノンITソリューションズ株式会社）
Cato SASEクラウド	ネットワーク接続／セキュリティ／管理を提供する統合プラットフォームです。これまで個別の製品やサービスで提供されてきた、拠点間やクラウドとの通信を制御するSD-WANと、FWaaS（Firewall as a service）／ZTNA／CASB／SWGなどのセキュリティ機能を一元的に提供するSASEサービスです。（サービス開発・提供元：Cato Networks Ltd.）
フルマネージドSASE　Verona	拠点間や自宅、外出先等から社内に接続するネットワーク機能と、インターネットへの安全なアクセスを実現するセキュリティ機能を一つのクラウドサービスとして提供する、中小規模向けフルマネージドSASEサービスです。 （サービス開発・提供元：株式会社網屋）
InterSafe GatewayConnection	いつ、誰が、どこから、どのデバイスを使っても安心安全なWebアクセスを実現するクラウド型Webフィルタリングサービスです。 （サービス開発・提供元：アルプス システム インテグレーション株式会社）

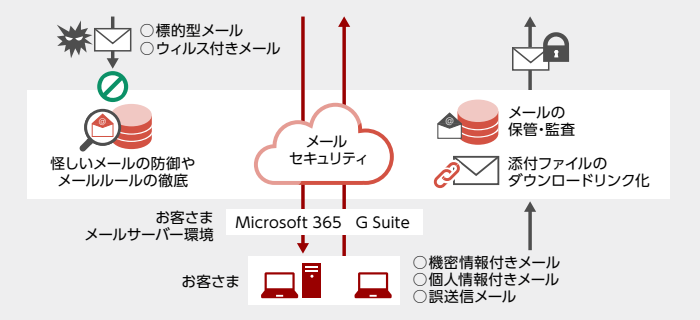
内部脅威

内部不正による情報漏えいを防ぎたい

外部脅威に備えるだけでなく、組織内部によるインシデントの未然防止にも取り組む必要があります。特に、情報漏えいについては外部からの不正アクセスよりも内部不正が原因となっているものが多く、その上、大量の個人情報や重要な営業秘密が持ち出されることから損害が大きくなりやすいことが特徴です。内部不正の多くは正当な権限を持つ従業員が行うため防ぐことが難しいと言われています。

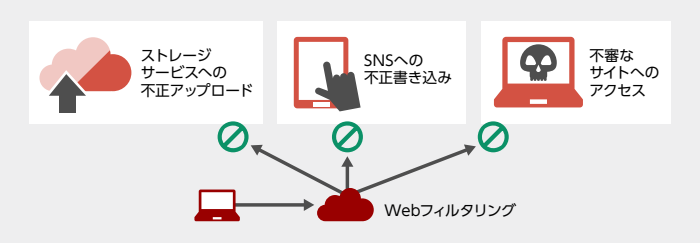
主な対策

メールセキュリティの一つであるフィルタリング機能を利用して、メールによる情報漏えいを防ぐことができます。送受信を監視して、情報漏えいの恐れがあるメールの保留や第三者承認による送信解除といった配送処理を行うことができます。また、アーカイブ機能を利用してメールを保存しておくことにより、インシデントの早期発見と漏えいした情報の特定が可能になるとともに、アーカイブの実態を従業員に告知することで、内部不正に対する抑止効果を得ることができます。



IT資産管理ツールを利用して、USBメモリなどの可搬記憶媒体の使用を制限することができます。組織が保有する可搬記憶媒体を登録し、デバイスごとに、使用可能／読み取り専用などのポリシー設定を行うことが可能です。また、従業員によるPCの利用状況を監視・可視化するため、操作ログを取得することも有効です。許可されていないUSBメモリの使用や大量の印刷出力など、不審な行為を早期に発見したり、禁止操作を行った際にはPCにアラートを表示して不正行為を抑止することが可能になります。

Webフィルタリングは、以前は、業務に不要なWebサイトの閲覧を禁止するなど、業務効率化や内部統制の強化を目的として導入されていましたが、現在は、SNSやオンラインストレージなどへのアクセスを禁止して、投稿やアップロードを制限することにより、故意や過失による情報漏えいを防ぐ対策としても利用されています。また、アクセスログを取得し、従業員によるWebサイトのアクセス状況を可視化することにより、内部不正に対する抑止やインシデント発生時の対処に効果的です。



商品概要

GUARDIANWALL Mailセキュリティ・クラウド	「MailFilter on Cloud」、「MailConvert on Cloud」、「MailArchive on Cloud」から構成されているクラウド型メールセキュリティサービスです。クラウドメールの利用に伴うリスク対策を網羅的に提供します。 （サービス開発・提供元：キヤノンマーケティングジャパン株式会社）
ISM CloudOne	クライアントPCの情報漏えい対策からIT資産管理、脆弱性対策を支援する管理サーバー不要のクラウドサービスです。事業所内のPCはもちろん、テレワーク中のPCやスマートデバイスをインターネットを介して一元管理します。 （サービス開発・提供元：クオリティソフト株式会社）
SKYSEA ClientView	情報漏えい対策やIT運用管理を支援する機能を搭載したソフトウェアです。PCをはじめ、さまざまなIT機器やソフトウェア資産を一元管理することで運用管理を支援、クラウドサービスでも提供しています。（サービス開発・提供元：Ｓｋｙ株式会社）
InterSafe GatewayConnection	いつ、誰が、どこから、どのデバイスを使っても安心安全なWebアクセスを実現するクラウド型Webフィルタリングサービスです。 （サービス開発・提供元：アルプス システム インテグレーション株式会社）

内部脅威

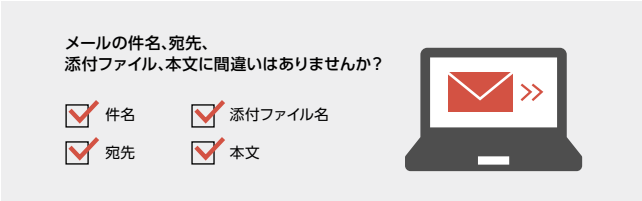
不注意による情報漏えい等を防ぎたい

内部脅威は2つに大別され、悪意のあるものと悪意のないものが挙げられます。悪意のないものは、さらに事故（システム障害や盗難等）と不注意に分けられます。ある調査では、従業員が関与したインシデントの多くは不正によるものではなく、不注意や過失が原因と報告されています。不注意による情報漏えいの例として、以下が挙げられます。

・メールの誤送信　・PCの紛失／置き忘れ　・重要書類の紛失・誤廃棄　・管理ミス（記憶媒体の不適切な廃棄）

主な対策

メールセキュリティの一つである誤送信対策機能を利用して、誤送信リスクを低減することができます。メールの送信ボタンを押すと、内容の確認を促すポップアップが表示されます。件名／宛先／添付ファイル名／本文を確認し、すべてにチェックを入れることでメールを送信することが可能になります。また、個人情報検査などのフィルタリングによって、事前に指定した個人情報が含まれているメールを検知し、情報漏えいを防ぐことができます。



HDD暗号化により、PCの紛失や盗難時の情報漏えいリスクを低減することが可能です。ハードディスク全体を丸ごと暗号化することにより、暗号化を解除するための認証が必要になるため、保存されているデータを第三者が閲覧することが困難になります。また、フォルダ・ファイル単位の暗号化とは異なり、暗号化／復号が自動で行われるため、ユーザーは意識することなくハードディスクを利用できます。

物品管理により、機密書類や契約書原本等の重要書類の管理を強化し、紛失や誤廃棄のリスクを低減することが可能です。重要書類に貼付したICタグやバーコードを読み取ることで、貸出し・返却管理を行うことができます。いつ／誰が／何を持ち出したかが分かるため、紛失防止に役立ちます。また、廃棄期限や契約更新期限をアラートメールで通知することにより、廃棄漏れや契約手続き漏れをなどを防ぐことができます。

システムの利用中止の際に、サーバーやクラウド上に保存されたデータを放置せずに、適正に消去することは情報漏えいを防ぐ上で重要です。暗号化に用いた暗号鍵を抹消すると、データの復元は不可能になります。この仕組みを利用した暗号化消去は、サーバーを廃棄する場合やクラウド上のデータを消去する場合に、高速かつ柔軟にデータを消去する手段として、多くのセキュリティガイドラインで認められています。

商品概要

GUARDIANWALL Mailセキュリティ・クラウド	「MailFilter on Cloud」、「MailConvert on Cloud」、「MailArchive on Cloud」から構成されているクラウド型メールセキュリティサービスです。クラウドメールの利用に伴うリスク対策を網羅的に提供します。（サービス開発・提供元：キヤノンマーケティングジャパン株式会社）
ESETセキュリティ ソリューションシリーズ	ESET社のフルディスク暗号化機能は、ESET PROTECTソリューションに含まれます（一部製品を除く）。PCやUSBメモリの紛失・盗難による情報漏えいから機密情報を守ります。（サービス開発・提供元：ESET, spol. s r.o.）
Convi.BASE	管理ラベル（ICタグやバーコード等）を物品に添付し、スマートフォン（iPhone）やハンディターミナル、RFIDリーダで読み取ることで管理や棚卸を行うことができる物品管理クラウドサービスです。（サービス開発・提供元：株式会社コンビベース）
Cipher Security Service	サーバー暗号化と暗号鍵の保管を同時に提供するクラウドサービスです。不正アクセスやマルウェア感染などにより第三者に重要情報を含むファイルが流出した場合においても情報漏えいの被害を抑えます。（サービス開発・提供元：キヤノンITソリューションズ株式会社）

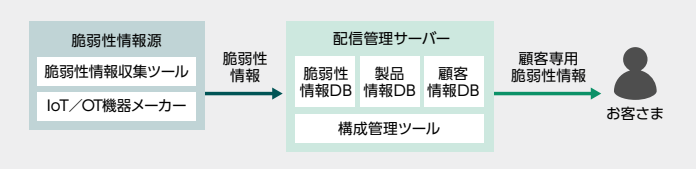
運用管理

脆弱性対応を効果的に進めたい

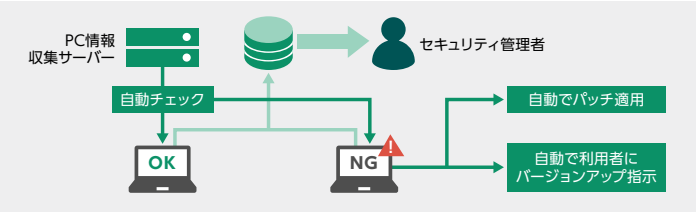
脆弱性はサイバー攻撃に悪用されるため、そのまま放置せず迅速に対処する必要があります。しかし、日々公開される脆弱性への対応を行う人的リソースは限られており、見落としや対応の遅れが発生する可能性があります。このため、脆弱性情報を確認の上、重大度や影響範囲を検討し、実際に対応を行う一連のプロセスを効果的に進めることが重要です。

主な対策

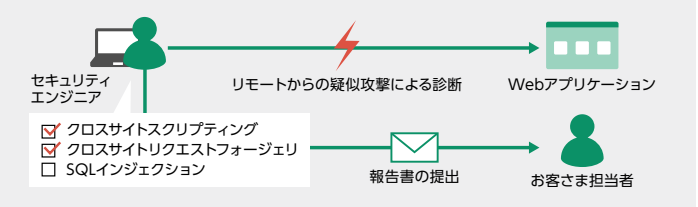
日々公開される膨大な脆弱性情報から、自社システムへの影響度を確認し、対処方法を検討する作業を情報システム担当者だけで行うことは不可能です。**脆弱性情報提供**サービスは、脆弱性情報データベースなどから収集した情報の中から、お客さま環境に合致した必要な脆弱性情報と対策情報のみを提供するサービスです。



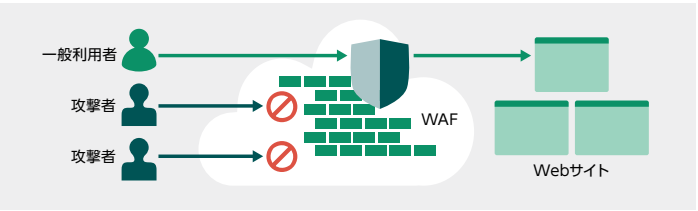
脆弱性・パッチ管理ツールにより、PCにインストールしているアプリケーション脆弱性を影響度に応じて優先順位付けすることで、パッチの適用を効果的に進めることが可能です。脆弱性対応の一連のプロセスを自動化することによって、エンドポイントに対する攻撃を未然に防ぎます。



脆弱性診断は、Webアプリケーションやサーバー／ネットワーク機器、クラウドサービス等に存在する脆弱性を発見する調査サービスです。脆弱性診断にはさまざまな手法があり、ツール診断とサイバー攻撃に精通したエンジニアによる手動診断に大別されます。脆弱性診断を実施し、対策状況を把握することによって、その後に必要な対策や検討すべき課題を洗い出すことができます。



WAF（Web Application Firewall）は、Webアプリケーションの脆弱性を悪用した攻撃を防ぐための専用ツールです。WAFを導入していれば、Webアプリケーションの脆弱性をすぐに修正するのが困難な場合でも、不正アクセスを防ぐ効果があります。マネージドサービスとして提供されるクラウド型WAFであれば、運用管理をサービス提供元に任せることができるため、手軽に導入することができます。



商品概要

脆弱性情報提供サービス	事前にお客さまから提供されたシステム構成情報と、脆弱性情報収集ツールなどから収集した脆弱性情報をマッチングして、お客さまそれぞれが必要とする脆弱性情報のみを提供するサービスです。（サービス開発・提供元：キヤノンITソリューションズ株式会社）
ESETセキュリティソリューションシリーズ	ESET社の脆弱性・パッチ管理機能は、ESET PROTECTソリューションに含まれます（一部製品を除く）。エンドポイントの脆弱性を自動診断し、パッチを適用します。（サービス開発・提供元：ESET, spol. s r.o.）
脆弱性診断サービス	対象となるシステムに、悪用できる脆弱性がないかをチェックしてセキュリティの状態を確認する診断サービスです。適切な対策を施すために、サイバー攻撃のきっかけとなる脆弱性（リスク）を発見することが目的です。 （サービス開発・提供元：GMOサイバーセキュリティ byイエラエ株式会社）
SiteGuard Cloud Edition	SQLインジェクションなど、Webアプリケーションの脆弱性を悪用した攻撃からWebサイトを保護する、マネージドサービスとして提供されるクラウド型WAFです。（サービス開発・提供元：EGセキュアソリューションズ株式会社）

運用管理

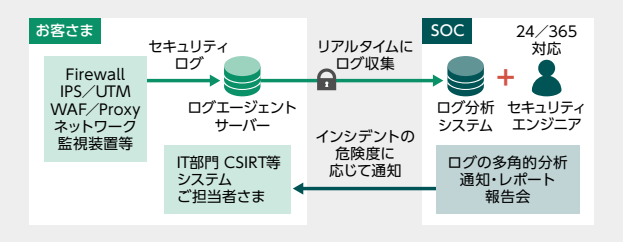
セキュリティ対策の運用負荷を軽減したい

巧妙化するサイバー攻撃に対抗するには、セキュリティ製品の導入だけでなく、専門的な知識やスキルに基づいた適切な運用が不可欠です。このため、こうしたことから、運用を支援するさまざまなサービスが登場しています。

・SOC　：製品の監視やログの分析を行い、サイバー攻撃の兆候を早期に発見します。
・CSIRT：インシデント発生時に主体的な対応を行います。
・MSS　：製品の監視を行い、設定変更や製品のアップデートなど、具体的な措置を行います。

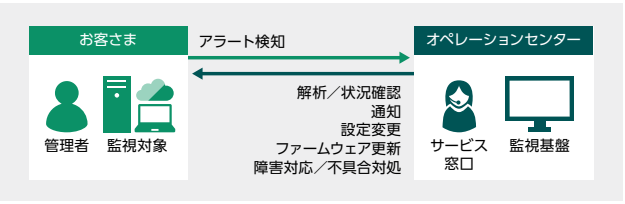
主な対策

SOC（Security Operation Center）は、組織内のネットワーク機器やアプリケーションのログを分析し、インシデント発生の兆候を早期に発見することを目的とする専門チームです。しかし、ログの分析により攻撃の兆候をつかむには高い専門性が要求されるため、アウトソースするケースが増えています。尚、UTMやWAFといったセキュリティ製品のログを一元的に監視し、自動的に分析を行いながらインシデントを検知する製品をSIEM（Security Information and Event Management）と言い、その情報を元にさらに高度な分析、あるいは実際の対応を行うチームがSOCとなります。

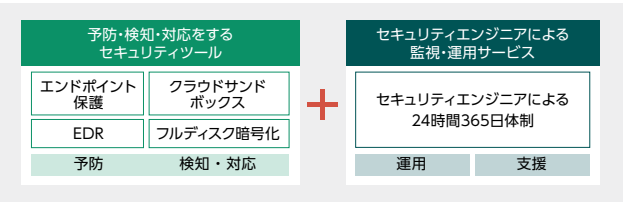


セキュリティ対策の専門チームとして、CSIRT（Computer Security Incident Response Team）を設置する組織も増加しています。SOCがサイバー攻撃の早期発見を主眼に置いているのに対し、CSIRTはサイバー攻撃などのセキュリティインシデントが発生した際に、必要な対策を迅速かつ確実に遂行することを目的としています。

MSS（Managed Security Service）は、セキュリティ対策の管理・運用を請け負うサービスです。MSSでは、お客さま環境に設置されたセキュリティ機器のログを監視し、マルウェア感染や不正アクセスなどが疑われる兆候を検知します。その危険度に応じたアラートがお客さまご担当者に通知され、状況に応じた対策を実施します。アラートの通知だけでなく、その後の対処まで提供するフルマネージドサービスと呼ばれる運用全般を委託するサービスも存在します。



MDR（Managed Detection and Response）は、EDRによる脅威検知をマネージドサービスとして提供するソリューションです。EDRを用いて24時間365日の常時監視を行い、エンドポイントの端末に異常を検知した場合、該当する端末の隔離をはじめ、速やかな復旧のための対策を講じます。

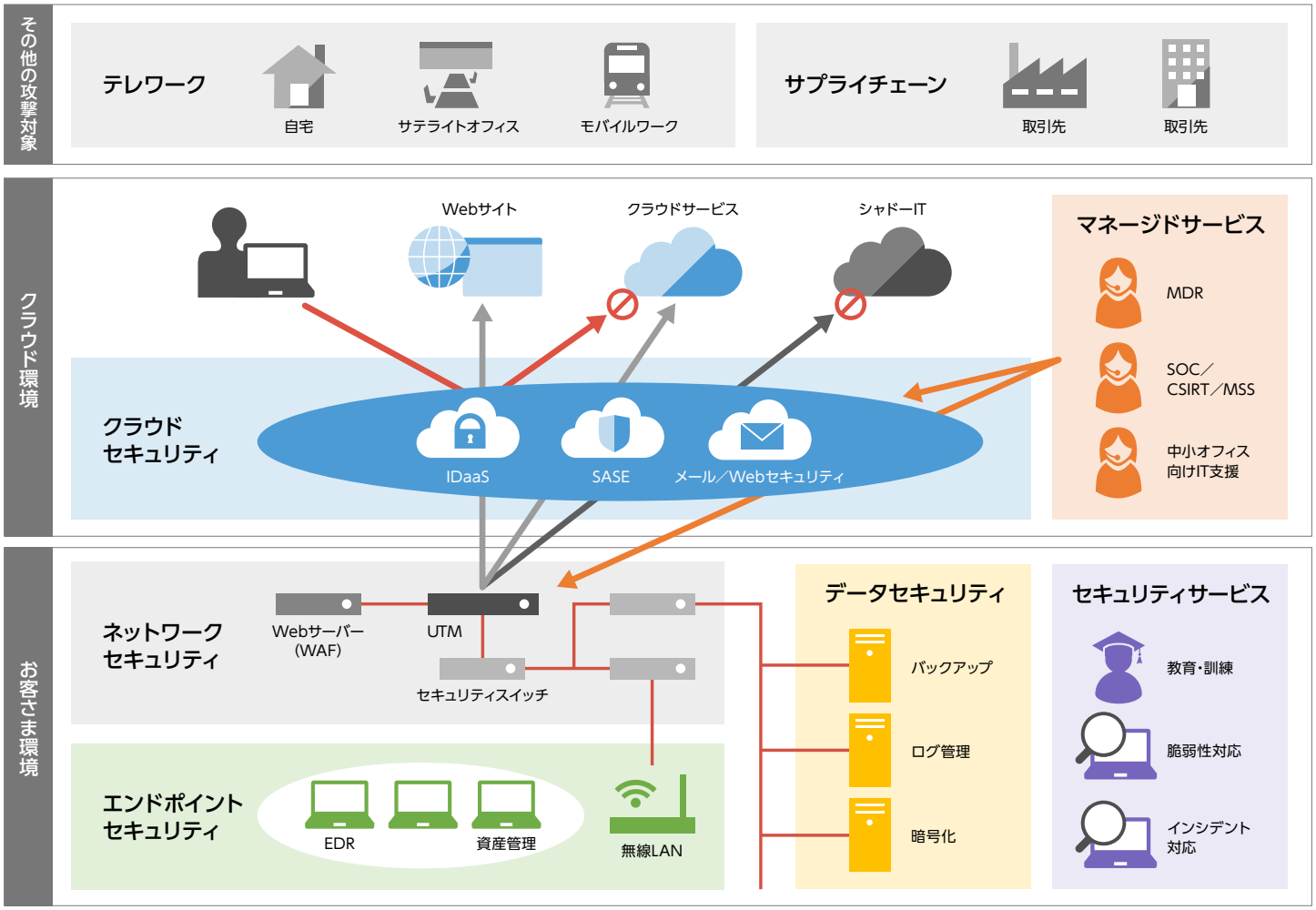


商品概要

UTMセキュリティ運用 支援サービス	FortiGateに対し「ログの収集・保管、脅威分析」など、きめ細やかなセキュリティ運用支援サービスを提供します。年々高度化するサイバーセキュリティインシデントに対して、SOCのセキュリティスペシャリストが遠隔から機器を監視・分析し、安心・安全をお届けします。 （サービス開発・提供元：キヤノンITソリューションズ株式会社）
セキュリティ運用サービス セキュサポ	サイバー攻撃や内部不正の監視、脆弱性診断、インシデント発生時の原因特定や影響範囲の調査、日ごろのセキュリティ相談の窓口など、サイバーセキュリティの専門チームが、セキュリティ対策に求められる包括的な対応を月額固定料金で提供します。 （サービス開発・提供元：株式会社網屋）
マネージド無線LAN Hypersonix	無線LAN環境の設計・構築から導入後の運用や障害対応までを、クラウド上の管理センターに一任できるクラウド型の無線LANソリューションです。複雑なセキュリティ設定はプロが代行するため、設定漏れがなく安心です。（サービス開発・提供元：株式会社網屋）
ESET PROTECT MDR	予防・検知・対応を行う「ESET PROTECT Enterprise」と、専任のセキュリティエンジニアにより運用・支援を行う「セキュリティサービス」で構成され、ワンベンダーによる一気通貫の支援により、セキュリティ対策の強化と、運用負荷の低減を行うことができます。 （サービス開発・提供元：ESET, spol. s r.o.）

商品・サービス

キヤノンマーケティングジャパングループは、複雑化が進むネットワークのさまざまな脅威に対して、情報システムをより安全に運用することを支援する製品やサービスをトータルにご提案します。ツールの導入からアセスメント、運用など、サイバーセキュリティ対策に関するさまざまな課題にお応えします。



エンドポイントセキュリティ

- ESETセキュリティソリューションシリーズ（EDR／HDD暗号化／脆弱性・パッチ管理）
- AppCheck（ランサムウェア対策ソフトウェア）
- ISM CloudOne（IT資産管理）
- SKYSEA ClientView（IT資産管理）
- Convi.BASE（物品管理）

ネットワークセキュリティ

- FortiGate（UTMアプライアンス）
- SonicWALL UTM（UTMアプライアンス）
- SubGate（セキュリティスイッチ）
- SonicWALL SSL-VPN（SSL-VPNアプライアンス）
- SiteGuard Cloud Edition（WAF）

データセキュリティ

- Barracuda Backup（バックアップアプライアンス）
- OneXafe（イミュータブルストレージ）
- ALog（SIEM）
- Logstorage（統合ログ管理システム）
- Cipher Security Service（暗号化支援サービス）

クラウドセキュリティ

- ID Entrance（IDaaS）
- Cato SASEクラウド（SASE）
- マネージドSASEサービス Verona（SASE）
- GUARDIANWALLシリーズ（メールセキュリティ）
- Intersafe GatewayConnection（Webフィルタリング）
- InterSafe WebIsolation Cloud Powered by Ericom（Web分離・無害化）

マネージドサービス

- ESET PROTECT MDR（MDR）
- UTMセキュリティ運用支援サービス（SOC）
- セキュリティ運用サービス セキュサポ（CSIRT）
- マネージド無線LAN Hypersonix（MSS）
- マネージドセキュリティサービス for FG 40F（MSS）
- HOME ネットワークセキュリティサービス（中小オフィス向けIT支援）

セキュリティサービス

- セキュリティ教育サービス
- 標的型攻撃メール訓練サービス
- 脆弱性情報提供サービス
- 脆弱性診断サービス
- サイバーインシデント対応支援サービス
- マルウェア解析サービス

製品に関する情報はこちらでご確認いただけます。

セキュリティソリューション ホームページ
canon.jp/it-sec

●お求めは信用のある当社で

キヤノンマーケティングジャパン株式会社
〒108-8011　東京都港区港南2-16-6 CANON S TOWER

2024年8月現在
SSG2408CMJ-PDF