お客さまの情報セキュリティ課題解決への貢献

キヤノンMJグループが一体となり、セキュリティ・ソリューションラインアップの強化および
事業領域の拡大を進展させ、お客さまに最適なサイバーセキュリティ対策の提案・提供を目指します。

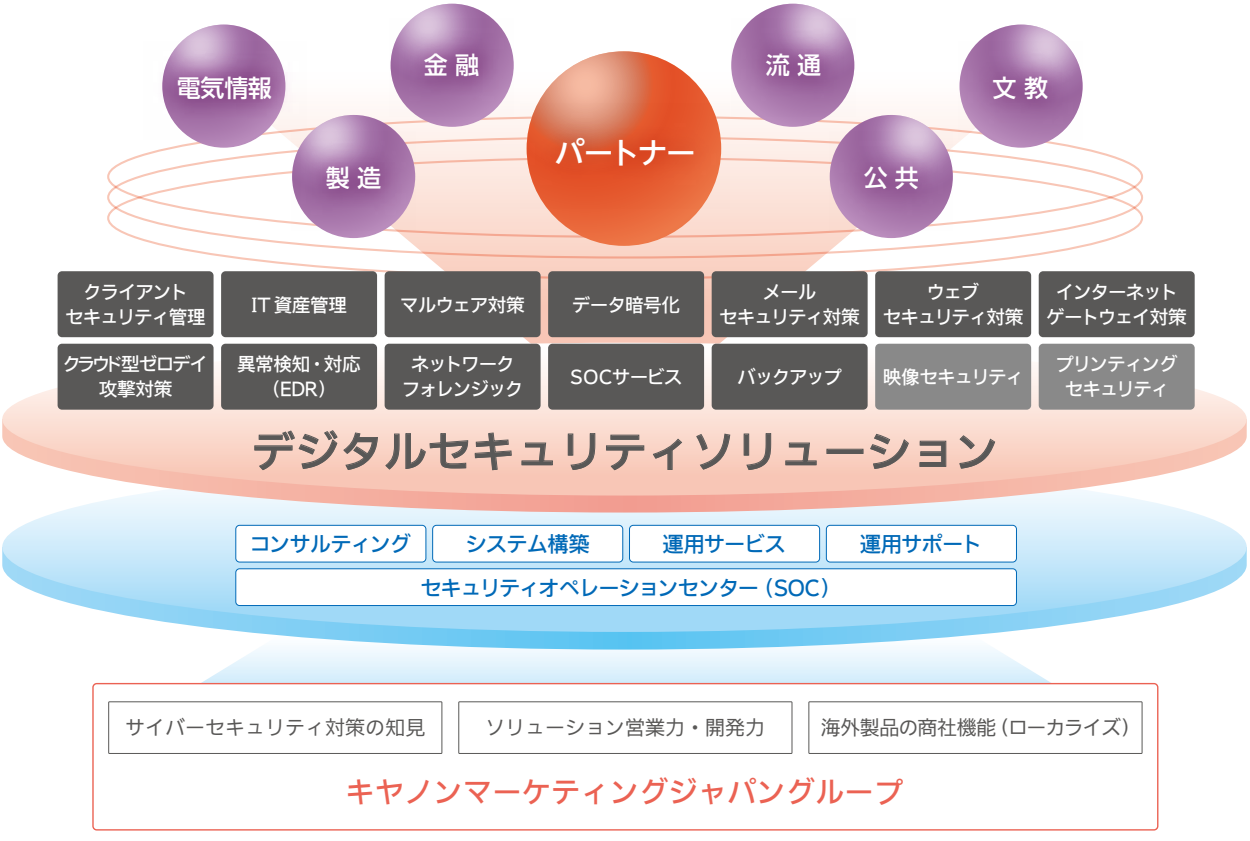
外部環境 サイバー攻撃の増加と新たなセキュリティリスクの表面化

ランサムウェアやビジネスメール詐欺といったサイバー攻撃の脅威、IoTやワークスタイル変革（テレワークや柔軟な働き方の浸透など）の環境変化に伴うセキュリティリスクの発生が前年に続き顕著となっています。また、サプライチェーンの脆弱性を狙った標的への攻撃など、新たな脅威も表面化してきています。インシデントの発生はビジネスの継続や企業の存続にまで影響を及ぼす可能性があり、セキュリティ対策は組織の規模や業種を問わず、重要な経営課題になっているといえます。

お客さまの課題解決を目的とする「デジタルセキュリティソリューション」

長年培ってきたサイバーセキュリティ対策の知見やソリューション営業力・開発力、海外製品の商社機能などを活かすことで、セキュリティ領域におけるお客さまのさまざまな課題解決を「デジタルセキュリティソリューション」として提案します。デジタル時代に求められるセキュリティ対策で社会の「安心・安全」を守り、変革に挑むお客さまを支えます。

● キヤノン MJグループ デジタルセキュリティソリューションのイメージ



フレームワークを用いたソリューションの提案

キヤノンMJグループでは、NIST※が定義する、サイバーセキュリティのリスク管理にともなう一般的な分類法および手法である「Cybersecurity Framework（サイバーセキュリティフレームワーク）」をもとに、お客さまの課題を整理します。また、これをサイバーセキュリティ対策『5つの備え』とし、目的別に最適な製品・サービスを揃えてソリューションを提案します。

※NIST：National Institute of Standards and Technology（米国国立標準技術研究所）科学技術分野における計測と標準に関する研究を行う米国商務省に属する政府機関であり、情報技術に関する6分野の研究を行っているITL（ラボ）にて、コンピューターセキュリティの研究・文書発行を実施

サイバーセキュリティ対策『5つの備え』

識別	防御	検知	対応	復旧
セキュリティリスクを理解する	セキュリティイベントを防御する	セキュリティイベントを検知する	セキュリティインシデントに対処する	セキュリティインシデントから復旧する
情報資産に対するサイバーセキュリティリスクを理解・把握する	サービス提供を確実にするための適切な保護対策を実施する	サイバーセキュリティイベントの発生を検知するための対策を実施する	検知されたサイバーセキュリティインシデントに対処するための対策を実施する	レジリエンス（早期復旧と影響の最小化）を実現するための対策を実施する

セキュリティソリューションのご紹介

クライアントセキュリティ／IT資産管理

識別

セキュリティ対策（内部／外部脅威対策）やIT資産管理、スマートデバイス管理の機能をオールインワンで提供

対策詳細

IT資産状況を管理し、各資産の脅威や脆弱性を洗い出すことで、発生するリスクを特定することができます。また、特定したリスクへの対応策※を実施します。

※ 実施可能な対応策は製品・サービスにより異なります。

取扱製品・サービス

- ISM CloudOne（開発元：クオリティソフト株式会社）
- SKYSEA Client View（開発元：Sky株式会社）
- ESET クライアント管理 クラウド対応オプション（開発元：ESET, spol. s r.o.）

マルウェア対策（エンドポイント）

防御

マルウェアをはじめとする外部からの攻撃や不正侵入、迷惑メールなど、さまざまな脅威からクライアントやサーバーを強力に防御

対策詳細

ウイルス定義データベースによる検出のみでなく、詳細な分析の実行と悪意ある振る舞いの特性を識別することで、新種や亜種のウイルスの脅威にも対処します。なお、キヤノンMJが販売総代理店として取り扱うESETは、ウイルススキャン時の端末動作への影響を軽減した製品で顧客満足度も高いのが特長です。

取扱製品・サービス

- ESET Endpoint Protection Advanced
- ESET Endpoint Protection Standard（開発元：ESET, spol. s r.o.）

データ暗号化

防御

パソコン内のHDDの暗号化のほか、ファイルサーバーやデータベースも暗号化またはトークン化することで、
大切なデータを情報漏えいのリスクから保護

対策詳細

社外利用するパソコンの盗難や紛失による情報漏えいのリスクを防ぎます。また、万が一、外部からの侵入によってファイルサーバーやデータベースから情報を持ち出された場合でも、データが暗号化されていることで内容を見られる心配はありません。

取扱製品・サービス

- ESET Endpoint Encryption（開発元：ESET, spol. s r.o.）
- Vormetric Data Security Platform
（開発元：Thales e-Security, Inc.）

メールセキュリティ対策

防御 検知

標的型メール攻撃の防御やメールの利用状況の管理など、メールに関するセキュリティ対策を提供

対策詳細

外部からの標的型メールを受信する前にフィルタリングで防御するほか、内部からの不適切なメール送信や誤送信の防止、メールアーカイブによる監査などを実施します。自社メールサーバーのほか、Office365などの他社メールサービスと連携した利用もできます。

取扱製品・サービス

- GUARDIANWALL Mailセキュリティ
- GUARDIANWALL Mailセキュリティ・クラウド
（開発元：キヤノンマーケティングジャパン株式会社）

ウェブセキュリティ対策

防御 検知

ウェブサイトのURLフィルタリングやマルウェア感染による外部への不正通信の遮断など、ウェブアクセスに関するセキュリティ対策を提供

対策詳細

業務に不要なウェブサイトへのアクセスを禁止し、業務に集中したウェブ利用を促進します。また、ウェブの利用状況を確認することができるため、万が一の場合にはログデータをもとに監査することもできます。そのほか、マルウェア感染による外部への不正通信の遮断などにも対応します。

取扱製品・サービス

- GUARDIANWALL Webセキュリティ
- GUARDIANWALL Webセキュリティ・クラウド
（開発元：キヤノンマーケティングジャパン株式会社）

インターネットゲートウェイ対策

防御 検知

内外のネットワークの境界で、外部からのさまざまな攻撃の脅威からクライアントやシステムを保護

対策詳細

内外のネットワークの境界は攻撃者が内部ネットワークやシステムへ侵入するときに最も一般的な入口となります。パケットをスキャンして不正な通信を遮断することで、クライアントやシステムに到達する手前で、外部からの脆弱性をついた攻撃やポートスキャン、マルウェアなどの脅威から防御します。

取扱製品・サービス

- FortiGate（開発元：Fortinet, Inc.）
- SonicWall（開発元：SonicWall, Inc.）
- Palo Alto Networks PAシリーズ
（開発元：Palo Alto Networks, inc.）

クラウド型ゼロデイ攻撃対策

防御 検知

未知で高度な攻撃をクラウドテクノロジーで自動解析・自動防御

対策詳細

ゼロデイ攻撃に用いられるような未知で高度なマルウェアを検出し、即座に組織全体の端末を防御するクラウドサービスを提供します。100%の白黒判定ができない不審なサンプルをクラウドに自動送信し、多段階に解析・防御するほか、サンドボックス環境による解析も実施します。

取扱製品・サービス

- ESET Dynamic Threat Defense（開発元：ESET, spol. s r.o.）

異常検知と対応サポート（EDR）

検知 対応

エンドポイントのイベント情報を収集し、不審な挙動や怪しいファイルを検知した場合に、その後の対応策を迅速に実施

対策詳細

エンドポイントへの攻撃に対して、悪意のある異常を発見する「検知」、その攻撃による影響や状況を把握する「可視化」、どの攻撃を防御して排除するかを決定する「対応」の一連の機能を提供します。防御しきれなかった脅威への対応を迅速にとる環境を実現します。

取扱製品・サービス

- ESET Enterprise Inspector（開発元：ESET, spol. s r.o.）
- EDR運用監視サービス
  （開発元：株式会社ブロードバンドセキュリティ）

ネットワークフォレンジック

検知 対応

ネットワークに流れる情報を記録し、監査時の証拠としてとりまとめて追跡できるようにする

対策詳細

ネットワーク上のパケットやログをリアルタイムに取得し、そこで起きた事象と流れたデータを可視化します。そして、可視化した情報をもとに不正な通信を検出して分析をします。また、情報漏えいなどのインシデントが発生した場合には、この情報をもとに証拠としてとりまとめ、対象や原因を追跡できるようにします。

取扱製品・サービス

- RSA Netwitness Network（開発元：RSA Security LLC）

SOCサービス

検知 対応

セキュリティ機器のログ監視やレポート提供を行い、インシデント発生時の対応を迅速にできるようにする

対策詳細

セキュリティの専門家が集まるセキュリティオペレーションセンターで、お客さまのセキュリティ機器のログ収集・分析、インシデントの検知・通知やレポート提供を行います。サイバー攻撃を早期発見し、迅速に対応することで、被害を最小限にできるよう支援します。

取扱製品・サービス

- e-Gate（開発元：株式会社セキュアソフト）

バックアップアプライアンス

復旧

万が一のために大切なデータをバックアップしておき、そのバックアップ環境をセキュアな状態で保持

対策詳細

大切なデータを定期バックアップしておき、データの改変や削除などが発生した場合に復旧できるように備えます。また、バックアップしたデータを保護するため、外部からのアクセスを制限したり、データ自体を暗号化技術で守ることもできます。

取扱製品・サービス

- Barracuda Backup（開発元：Barracuda Networks, Inc.）

映像ソリューション（ネットワークカメラ／映像解析／クラウド）

高画質でさまざまな環境に対応したネットワークカメラと映像解析技術を組み合せることで、映像基盤を構築し物理セキュリティを強化

対策詳細

記録映像の画質や撮影範囲、照度、防水・防塵など、お客さまの利用シーンに合致するラインアップ（機器やシステム、サポート）を揃えています。ネットワークカメラの映像のみでなく、センサーや照明機器を合わせた一元管理のほか、映像解析ソフトウェアと連携したさまざまな把握・検知を実現します。

取扱製品・サービス

- ネットワークカメラ「VBシリーズ」（開発元：キヤノン株式会社）
- ビデオ管理ソフトウェア「Milestone XProtect」（開発元：Milestone Systems）
- 映像解析ソフトウェア「BriefCam」（開発元：BriefCam Ltd.）
- クラウド型録画サービス「VisualStage Type-S」（開発元：セーフィー株式会社）

プリンティングセキュリティ（認証・ログ管理）

複合機・プリンターの利用者と利用履歴を管理

対策詳細

ICカード認証など個人認証機能と連動して、オフィス向け複合機・プリンターの利用履歴を管理できます。いつ／だれが／どのようなドキュメントをコピー／プリントしたのか、またファクス／スキャン送信など、利用履歴を管理することで、企業内部からの情報漏えいを抑止できます。

取扱製品・サービス

- ICカード認証 Pro for MEAP ADVANCE（開発元：キヤノンマーケティングジャパン株式会社）
- imageWARE Accounting Manager for MEAP（開発元：キヤノン株式会社）
- uniFLOW Online Express（開発元：NT-WARE）

プリンティングセキュリティ（プリント管理）

いずれの複合機・プリンターからでも機密文書を他人に見られることなくセキュアに印刷

対策詳細

オフィス内のいずれの複合機・プリンターからでも、重要な機密文書を他人に見られることなくプリントできます。ICカード認証など個人認証してプリントさせることで、出力物の放置や不要な出力コストの発生を抑えることができます。

取扱製品・サービス

- サーバーレス Anyplace Print for MEAP ADVANCE（開発元：キヤノンマーケティングジャパン株式会社）
- uniFLOW Online（開発元：NT-ware）

国内最高水準の堅牢性を持つ「西東京データセンター」

「西東京データセンター」はティア４レベル※1の国内最高水準の建築・設備で、堅牢性の高いビルファシリティ、冗長化された電源設備・空調設備、高度なセキュリティを備えています。運営面においても、複数の第三者認証を取得するなど高く評価されており、お客さまの次世代IT基盤として活用できます。2020年下期には、同規模の新棟が竣工する予定です。

また沖縄にもデータセンターを所有し、BCP対策センターとしても利用できます。コロケーション、ハウジング、クラウドサービスなどで、お客さまのニーズに応えます。

西東京データセンターの特長

- 都心から20km圏、1時間以内でアクセス可能な利便性の高い立地
- 環境に配慮したPUE=1.4の設備設計※2
- 3Dボディスキャナー、生体認証などを採用した7段階の厳密かつ堅牢なセキュリティ
- 床耐荷重1.5t/㎡、高集積／高密度な機器の設置を可能とするフロア仕様
- 1フロア最大800ラック、大規模から小規模まで最適な配置が可能なフロアレイアウト
- 免震ゴム、縦揺れ制震ダンパーなどを備えた基礎免震構造によりお客さまのシステムを保護
- 災害や障害に備え、電力／通信回線の２系統引込みや、自家発電用燃料の供給を優先的に受けられる調達体制を確立

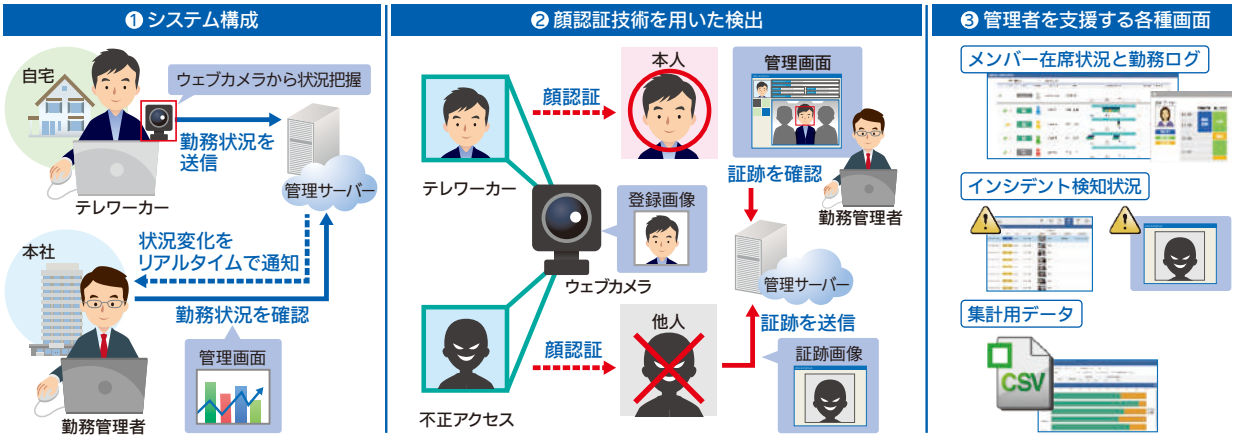
認証資格など	
❶ M&O認証	データセンターのグローバル運営基準※3
❷ ISO 22301	事業継続マネジメントシステム
❸ ISO/IEC 20000	ITサービスマネジメントシステム
❹ ISO/IEC 27001	情報セキュリティマネジメントシステム
❺ SOC2 Type1	保証報告書　グローバル基準の内部統制評価報告書※4

※1 ティア4レベル：特定非営利活動法人日本データセンター協会（JDCC）が策定した「ファシリティスタンダード」における最高レベル
※2 PUE：データセンターの電力使用効率を表す指標で、1.0に近いほど電力効率が良い
※3 M&O認証：米国「Uptime Institute」が定める、データセンターの運営能力を評価する国際的な認証制度
※4 米国公認会計士協会（AICPA）が定めたTrustサービス基準に基づき、監査法人や公認会計士が内部統制の有用性について検証結果を記載した報告書

テレワーク支援サービス「テレワークサポーター」

事業継続や優秀な人材確保のため在宅勤務やテレワークを導入する企業が増えています。テレワークサポーターは、情報セキュリティリスクに配慮したテレワーク導入・運用を、キヤノンの顔認証技術を使ったクラウドサービスにより支援します。

情報漏えい対策	顔認証技術で勤務者以外の第三者の覗き込みやなりすましを検知し、その瞬間のウェブカメラ画像とパソコンのスクリーンショットを取得します。同時に、パソコン画面を自動でブラックアウトにする機能も備え、情報流出を最小限に抑えます。
勤務時間管理	カメラ映像から勤務者の在席・離席を自動判断し、勤務時間を記録します。 1日の勤務時間を可視化し、時間外にパソコンを利用しているサービス残業の把握も可能となります。
業務内容の可視化	勤務者が仕事内容を一覧から選択する簡単な操作を行うことで、仕事内容別の時間が自動集計されます。



中小オフィス向けIT支援サービス「HOME」

企業にとって取引先からの信頼獲得、生産性の向上、あわせてそれを実現するためのITの活用は重要な課題となっています。

「HOME」は、IT管理者不在の中小オフィスのお客さまに、「セキュリティの向上」「コミュニケーションの活性化」「運用管理の支援」を提供し、企業競争力向上を支援します。

複数のセキュリティ機能を統合的に管理する「HOME-UNIT」

外部からの攻撃、内部からの情報漏えいに備え、ファイアウォール機能をベースに、アンチウイルス、アンチスパム、ウェブコンテンツフィルタリング、不正侵入検知・防御、メール誤送信防止など、複数のセキュリティ機能を統合的に管理します。また、サイバー保険を付帯したモデルでは、万が一、被害にあった場合の原因調査やデータ復旧・機器修理などさまざまな対応を保険でカバーします。

「HOME-UNIT」のセキュリティ対策	ファイアウォール	外部からの不正なアクセスや侵入を防止し、内部のネットワークの安全を維持します。
	アンチウイルス	シグニチャやヒューリスティック・エンジンを自動的に更新して、新種のウイルスやスパイウェアが社内に侵入することを防ぎます。
	アンチスパム	メールをチェックし、スパムの可能性があるメールを自動検知します。
	ウェブコンテンツフィルタリング	業務に不適切なウェブサイトへのアクセスを制御し、ネットワークセキュリティへの脅威と帯域の無駄遣いを防ぎます。
	不正侵入検知・防御	ワームやサービス拒否攻撃（DoS）などの通信の特長をとらえて遮断したり、Winnyなどの P2P ソフトの通信を遮断し、社内からの情報漏えいを防ぎます。
	メール誤送信防止	メールで添付ファイルを送る際、自動的にファイルを ZIP 暗号化し、安全性を高めます。また一定時間メールの送信を保留することで、メールの誤送信を防ぎます。

サービスの導入・運用を支援する「HOME-CC」

「HOME」導入後の運用サポートは、「HOME-CC（コンタクトセンター）」の専門スタッフが行います。お客さまからのお問い合せに対し、電話だけでのコミュニケーションでは伝えにくい操作や設定の方法などは、インターネットを利用したリモートツールでわかりやすくサポートします。

IT人材不足によるセキュリティリスクを軽減「お手軽運用支援サービス for FortiGate」

キヤノンS&Sでは、中堅・中小企業のIT人材不足で起こりうるセキュリティリスクを、UTM（統合脅威管理）の運用サポートと保守で軽減する「お手軽運用支援サービス for FortiGate」をご提供しています。

本サービスでは、お客さまに導入いただいたFortiGate※のログを収集・分析し、ウイルス検出や外部への不正な通信などのセキュリティインシデントが発生した際に、お客さまへメールで通知します。また、運用時のお問い合せをコールセンターで対応することに加え、解決できない場合は、サポートスタッフが訪問し、設定変更や運用のアドバイスを行いますので、専任のIT管理者がいなくてもFortiGateを最適に運用いただけます。

サービスの特長

特長1 緊急的な対応をメールで通知

緊急性の高いセキュリティインシデントが発生した際、お客さま管理者へ、その対処方法などを日本語のメールで通知します。

特長2 日次レポートでFortiGateの稼働状況を可視化

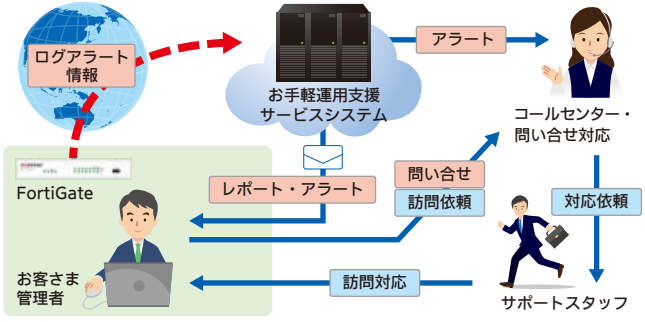
ご導入いただいたFortiGateのログを分析し、脅威カテゴリー単位で状況をレポート化します。

特長3 運用時のお問い合せ窓口開設

受信したアラートやレポートに関する運用時のお問い合せを、当社コールセンターにてメールでお受けします。

特長4 いざというときのオンサイト対応

当社サポートスタッフがお客さま先に訪問し、アラート内容に基づく設定変更およびレポート内容に対するアドバイスをします。



※FortiGateはフォーティネット社の提供するUTM（統合脅威管理）製品で、ファイアウォール、ウイルス／スパイウェア対策、スパム対策、ウェブフィルタリング、アプリケーション制御などのセキュリティ機能とVPN、無線LANコントローラなどネットワーク機能を統合し提供するアプライアンスです。