Information Security Report 2020

キヤノンマーケティングジャパングループ
情報セキュリティ報告書 2020

私たちの「情報セキュリティ」は顧客満足度の向上を支える業務改善活動です

キヤノンマーケティングジャパングループは、セキュアな社会の実現に向け、企業の社会的責任として「情報セキュリティ」の基盤強化に取り組んでいます。さらに「情報セキュリティ」を、お客さまへの価値提供プロセスの品質を「より安全に」「より確実に」「より効率的に」するための“顧客満足度の向上を支える業務改善活動”ととらえて、成熟度の向上に努めています。

グループ情報セキュリティ基本方針

キヤノンマーケティングジャパングループ（以下「当社グループ」）は、キヤノングループの企業理念である「共生」のもと、「先進的な“イメージング&IT”ソリューションにより社会課題の解決に貢献する」ことをミッションに掲げ事業活動を展開しています。

当社グループは、IoT、クラウドサービス等のデジタル技術と高品質なサービスで真の価値を創造していく情報サービス産業でのリーディング企業グループを目指すため、サイバー攻撃等を含む情報セキュリティリスクを認識し、事業活動で用いる情報資産の適切な取り扱いを重要な経営課題ととらえ、これを実践するために以下の方針に基づき一層の継続的改善に努めます。

方針

1. 法令及び規範並びに契約上の要求事項の遵守

当社グループは、情報セキュリティに関する法令、国が定める指針その他の規範、並びに契約上のセキュリティ義務を遵守します。

2. グループ情報セキュリティマネジメントシステムの確立と実施及び継続的改善

当社グループは、お客さまに価値を提供するための事業活動の円滑な遂行を、情報セキュリティの側面から支えるためのマネジメントシステムを確立し、実施し、継続的に改善します。

3. 教育の実施

当社グループは、全ての役員、従業員および当社業務に従事する者のうち必要と認めた者が、情報資産の正しい取り扱いに関して倫理はもとより、変りゆく環境に常に適合する感覚や知識およびスキルを持ち、行動するための情報セキュリティに関する教育を実施します。

4. 事業継続管理

当社グループは、製品・サービス提供プロセスの中断を引き起こし得る情報セキュリティリスクを、特定、評価し、実効的なセキュリティの対策を講じるとともに、災害や事故等による事業停止に対する復旧手順を確立し、事業継続管理に努めます。

制定日 2010年9月　1日
改定日 2020年6月25日
キヤノンマーケティングジャパン株式会社　代表取締役社長　坂田　正弘

個人情報保護方針

https://cweb.canon.jp/privacy/index.html

※ グループ各社は同様の方針を制定しています。

Contents

編集方針

本書は、キヤノンマーケティングジャパングループの情報セキュリティに関する活動をご報告することによって説明責任を果たすとともに、お客さまの課題解決のための参考情報をご紹介することを目的に発行しました。

編集にあたっては、経済産業省発行の「情報セキュリティ報告書モデル」を参考にしながら、私たちの考え方と実践事例を具体的にご紹介することに努めました。また、定常的に取り組んでいることだけでなく、年次報告として2019年に取り組んだスパイラルアップポイントを、Action2019としてご紹介しています。

※「キヤノンマーケティングジャパン」は、略称として
「キヤノンMJ」と表記する場合があります。

[お問い合せ先]

キヤノンマーケティングジャパン株式会社
CSR本部　CSR推進部　情報セキュリティ推進グループ
〒108-8011 東京都港区港南2-16-6　キヤノンSタワー
TEL：03-6719-9032

■ ウェブサイト
https://cweb.canon.jp/csr/governance/security/

■ 対象期間
主に2019年（2019年1月～12月）の情報セキュリティに関する活動や取り組みを対象としています。
※この期間以降の活動も一部掲載しています。

■ 対象会社
キヤノンマーケティングジャパン株式会社
およびキヤノンマーケティングジャパングループ会社

トップメッセージ

先進的な“イメージング&IT”ソリューションにより お客さまの課題解決とセキュアな社会の実現に貢献します

キヤノンマーケティングジャパングループは、2016年から2020年までの「長期経営構想フェーズⅢ」のミッションとして、「先進的な“イメージング＆IT”ソリューションにより、社会課題の解決に貢献する」を掲げ、ビジョンである「お客さまを深く理解し、お客さまとともに発展するキヤノンマーケティングジャパングループ」の実現に取り組んでいます。

近年、私たちを取り巻く環境はめまぐるしく変化し、自然災害や新たな感染症への対応など、克服しなければならない地球規模の社会・環境課題が山積しています。

人手不足の解消と生産性向上を目指した働き方改革、さらに新型コロナウイルスの感染拡大などを背景に、テレワークの促進やサテライトオフィスの設置などが加速し、それらを支えるITへの需要・期待がさらに高まっています。

当社グループのITソリューション事業は、2019年末時点で、当社グループの売上の1/3を占めるほどのビジネスに成長しました。2020～2022年の中期経営計画でも、「高収益企業グループ」に向けた成長戦略として、社会やお客さまの変化に先んじたソリューションの提供で収益の最大化を目指し、ITソリューション事業に注力することを掲げています。

当社グループにおいては、従来からの情報セキュリティガバナンスのさらなる強化と適切な情報管理・運用を推進するマネジメント体制、およびサイバーセキュリティ専門組織CSIRT※によるサイバー攻撃の予防・検知・発生時対策の実施体制を整備しております。

また、お客さまにご提供している製品・ソリューションにおいては、情報セキュリティを重要な品質要件として、その向上に取り組んでいます。

そして、日々の事業活動の中で培った情報セキュリティ管理・運用ノウハウを付加価値としてお届けすることによって、お客さまの課題解決へ貢献するよう努めています。

私たちはグループ一体となってお客さまの事業活動をトータルでサポートし、お客さまにとって頼りになる真のパートナーとして、お客さまとともに成長していきたいと考えています。

本報告書では、私たちの情報セキュリティに対する考え方や実践事例、お客さまの情報セキュリティ課題解決に貢献できる製品・ソリューションを紹介しています。ご覧いただいた皆さまに少しでもお役に立つことができれば幸いです。

※ CSIRT：Computer Security Incident Response Team

主要注力テーマ

1. サイバーセキュリティリスクに対する対策強化
2. グループ情報セキュリティガバナンスの強化
3. グループ情報セキュリティマネジメントの均質化と効率化
4. 情報セキュリティ人材の育成
5. 情報セキュリティ活動の積極的な情報開示
6. お客さまへの価値提供プロセスにおける情報セキュリティ品質の向上
7. お客さまの情報セキュリティ課題解決への貢献

代表取締役社長 **坂田 正弘**

推進フレームワーク

▶ 推進フレームワーク

キヤノンMJグループでは、情報セキュリティの推進にあたり「企業の社会的責任の遂行」と「顧客満足度の向上」を目的として設定し、大きく2つの取り組みを進めています。

1つ目は「キヤノンマーケティングジャパングループの情報セキュリティ成熟度の向上」です。ここでは「グループ情報セキュリティ基盤の強化」と「お客さまへの価値提供プロセスにおける情報セキュリティ品質の向上」の2つの活動を行っています。

「グループ情報セキュリティ基盤の強化」では、グループ全体の情報セキュリティガバナンスを強化し、情報セキュリティのマネジメントを通じて均質化と効率化を図るとともに、各社・各部門の事業特性に応じたセキュリティ対策の最適化などを推進しています。

「お客さまへの価値提供プロセスにおける情報セキュリティ品質の向上」では、営業・保守サービス・ソフトウェア開発などの業務プロセスごとに、情報資産の安全管理に留まらず、情報の取り扱いと製品・サービスの品質を向上させています。

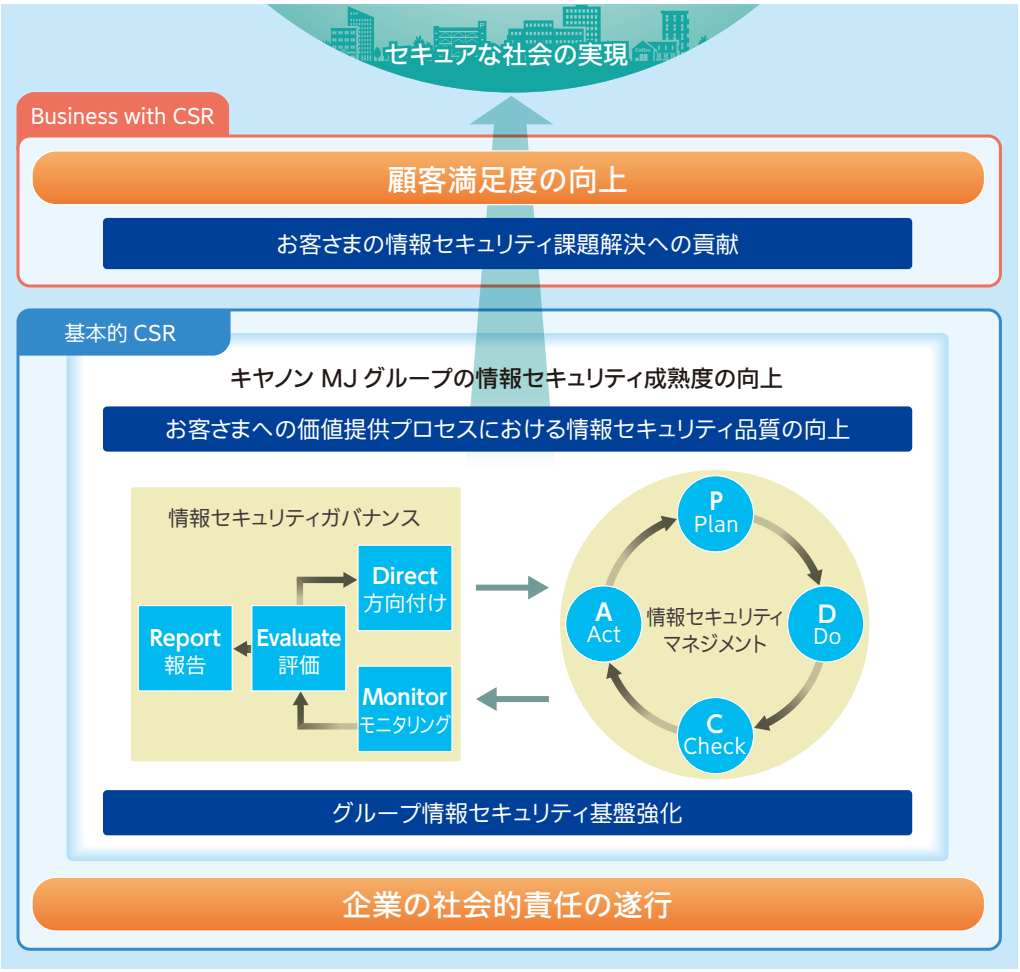
これらの活動の中で、事業活動を営むための前提となるステークホルダーの要請に対応した必要不可欠なCSR活動は「基本的CSR」です。

そして2つ目は、「お客さまの情報セキュリティ課題解決への貢献」です。

ここではキヤノンMJグループが取り扱う各種情報セキュリティ製品・サービス、ソリューションを、グループ内の情報セキュリティ活動を通じて培ったノウハウも含めてお客さまにご提供するよう努めています。

このような事業活動を通じた社会課題の解決や社会価値を提供するCSR活動は「Business with CSR」というスローガンのもとに展開しています。

私たちは、こうした取り組みによって「セキュアな社会の実現」に寄与していきます。



情報セキュリティガバナンスとマネジメント

情報管理リスクは重要な経営課題の一つであるため、経営層による情報セキュリティガバナンスのもとで、情報セキュリティマネジメントを推進しています。

CSR委員会による情報セキュリティガバナンスの強化

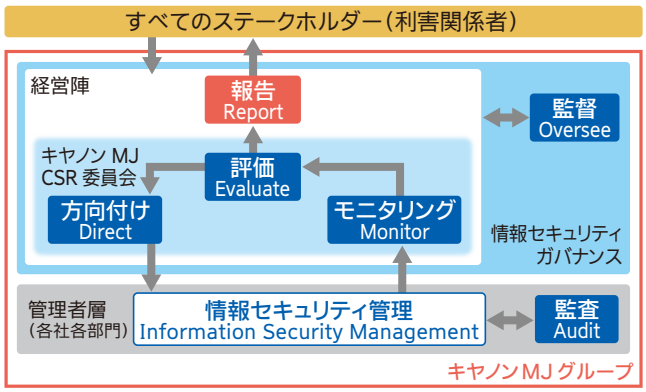
情報セキュリティの取り組みは、コンプライアンスや環境対応、事業継続、品質管理などの社会要請への対応とも密接に関連しています。

そこでこれらの社会的要請事項を所管する「キヤノンMJ CSR委員会」の中で、経営陣がグループの情報セキュリティガバナンスの強化に取り組んでいます。

この委員会の中では、情報セキュリティ方針や戦略などの決定「方向付け(Direct)」を行い、定期的に経営環境やリスクの変化、目標の達成状況などを確認「モニタリング(Monitor)」し、「評価(Evaluate)」し、必要に応じて新たな「方向付け(Direct)」を行うというサイクルを回しています。

これら一連のガバナンスと、そのもとで取り組まれている情報セキュリティマネジメントの状況は、「情報セキュリティ報告書」を通じて社内外のステークホルダー(利害関係者)へ「報告(Report)」しています。

● キヤノンMJグループの情報セキュリティガバナンス



効率的なマネジメント体制

マネジメント体制は、グループ情報セキュリティ統括体制と各社マネジメント体制の2つに分けています。

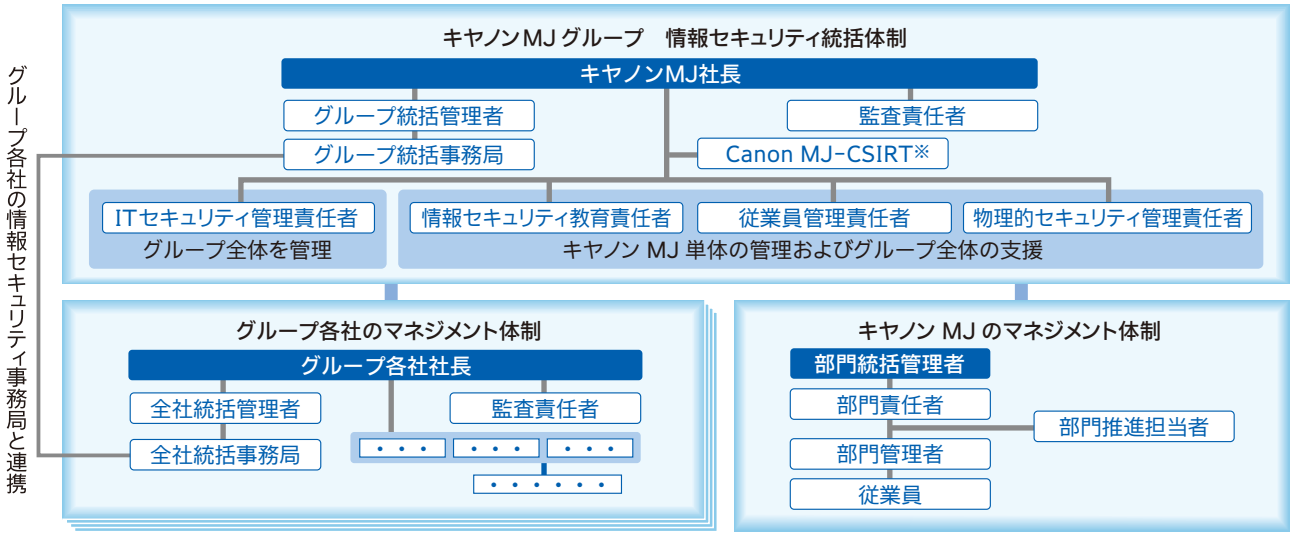
グループ情報セキュリティ統括体制はキヤノンMJの情報セキュリティ主管部門がグループ統括事務局の役割を果たし、グループ全体の情報セキュリティマネジメントを統括しています。

そして、グループ本社機能を持つ組織が、IT・物理・人的セキュリティ施策など、グループ共通のルールや対策の企画立案・推進を行っています。

また、サイバー攻撃に対しては、CSIRT※を配置して予防対策を行っています。

一方、各社マネジメント体制では、それぞれの会社の事業特性に応じて、情報セキュリティ主管部門や部門管理体制を設置し、運用しています。

● キヤノンMJグループの情報セキュリティマネジメント体制



※ CSIRT(シーサート):
CSIRT(Computer Security Incident Response Team)とは、サイバー攻撃などのサイバーインシデントの予防・発生時・収束後の対応支援を専門に行う組織です。
具体的には、予防対策として、サイバー攻撃やソフトウェアの脆弱性などの情報収集、脆弱性対応の推進などを行い、被害の未然防止を図ります。
また、発生時対策として、万が一、攻撃を受けた場合は、被害を最小限に留めるためにインシデントハンドリングなどの支援を迅速に行います。

体系的にルールを整備

キヤノンMJグループでは、キヤノンのグローバル基準である「グループ情報セキュリティルール」を基軸としながら、グループ全体の情報セキュリティを推進するための幹となる「グループ情報セキュリティ基本方針」と「グループ情報セキュリティ基本規程」を制定しています。

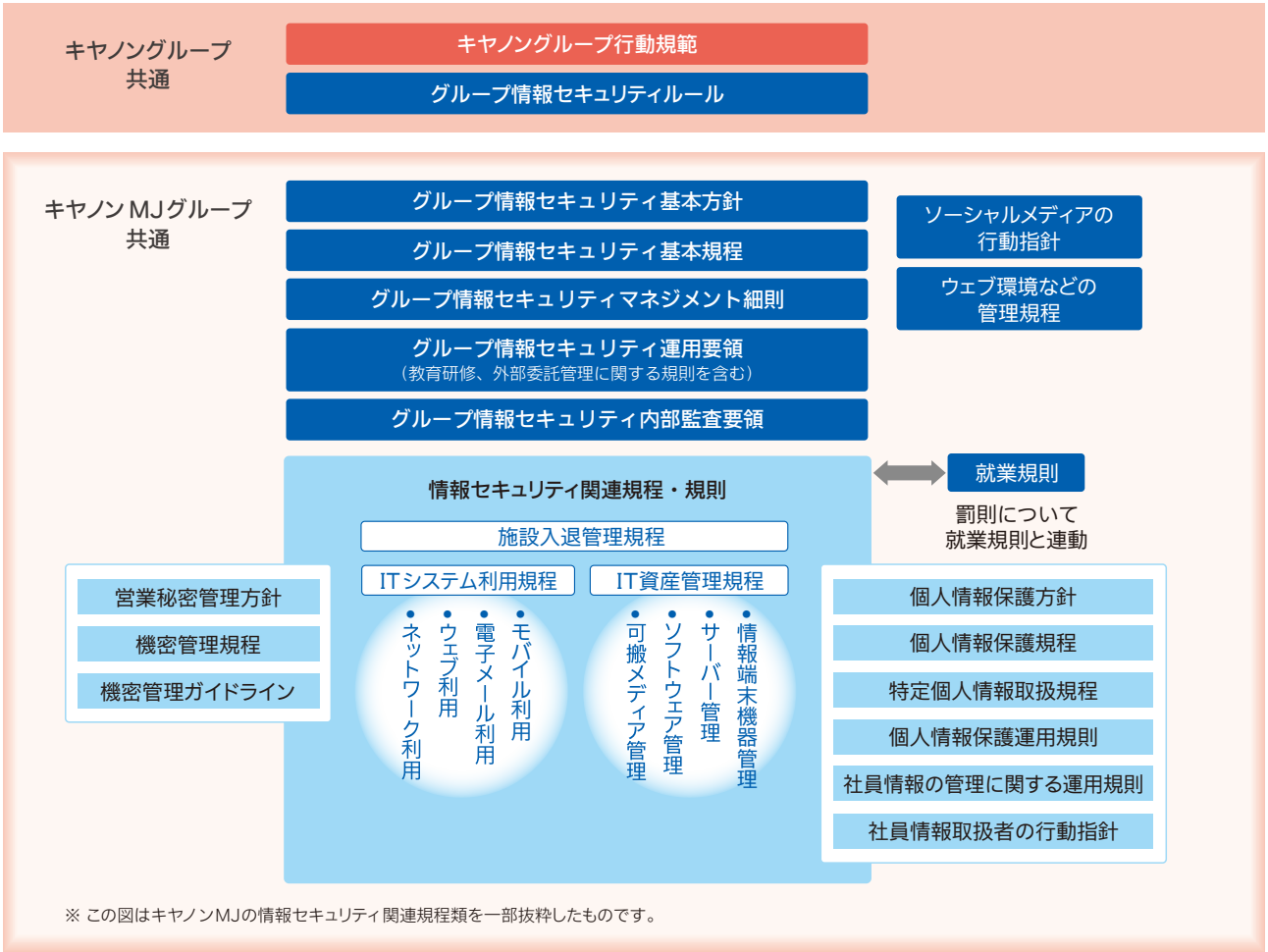
これらの方針や規程を踏まえ、キヤノンMJグループ全体の情報セキュリティ基盤を支える規程類と、重要な情報資産である個人情報保護や機密管理に関する規程類は、それぞれの規程の中で定める要素が重複することがないようにしています。

たとえば、個人情報保護や機密管理に共通する安全管理措置に関する規程については、個別の規程に定めるのではなく、全社情報セキュリティ基盤を支える関連規程などを外部引用しています。これにより、規程類の二重管理の負荷や、各規程間の不整合を防ぐことができます。

また、グループ各社の業種・業態に応じた管理手法を反映させる必要がある規程については、キヤノンMJグループ統一の規程をベースにした上で、個別にカスタマイズすることにより整備しています。

このように、共通する要素の規程間での重複を避け、かつ、各グループ会社の事情に合わせた規程類を整備するような工夫を通じて、体系的なルールの整備に結び付けています。

情報セキュリティに関するルール体系



※ この図はキヤノンMJの情報セキュリティ関連規程類を一部抜粋したものです。

▶個人情報・機密情報を取り扱う業務委託先への管理・監督の取り組み

キヤノンMJグループでは、外部委託先の選定基準や安全管理措置の確認方法などを定めたルールや管理体制を整備し、業務委託先に対して適切な管理・監督を行っています。

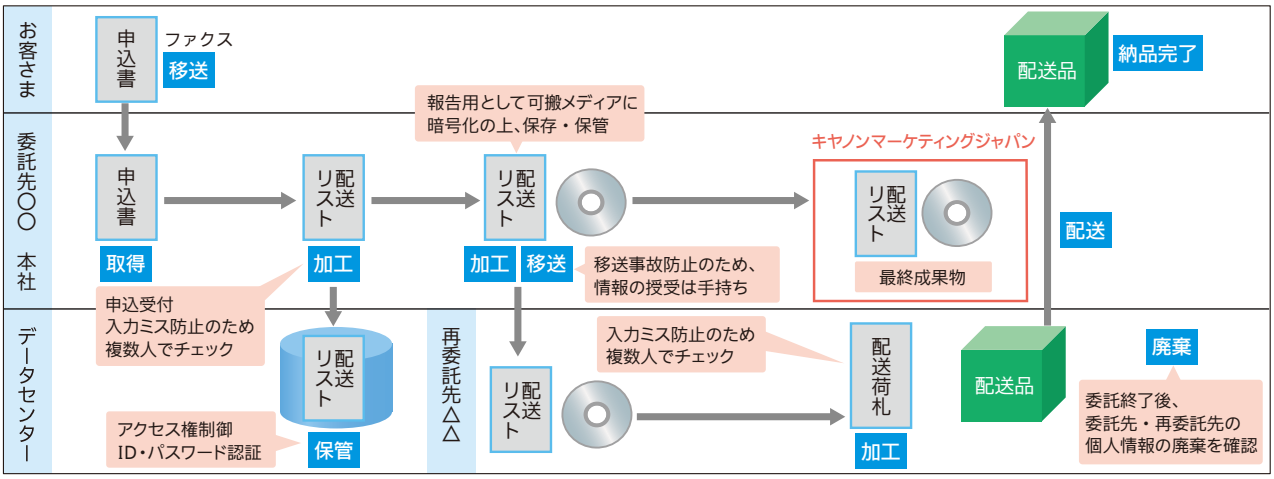
委託先における業務フローや安全管理措置・安全対策の確認

委託先における個人情報の取り扱い業務フローや安全管理措置に関して、書面による確認を定期的に行っています。

さらに、預託する個人情報がセンシティブな内容の場合には、現地視察を含めたより質の高い管理・監督を実施しています。

なお、外部のASPやSaaSなどは、IPA（独立行政法人情報処理推進機構）発行のチェックシートを参考にした独自の書面により、安全対策の確認を定期的に行った上で利用しています。

サンプル キャンペーン申込受付・景品発送　業務フロー図



パートナー企業の情報セキュリティ品質の向上

複合機の保守サービス、ソフトウェア開発、物流の業務委託を行っているパートナー企業に対しては、情報セキュリティの実践教育や、定期的な学習会を実施し、情報セキュリティ品質の向上に努めています。

キヤノンMJグループの複合機の保守サービス業務では、委託先に対する評価基準を設けています。2019年には、438社752拠点に対し、年1回のウェブによるセルフアセスメントを実施し、406社717拠点に対し実地調査を行いました。その上で、基準に満たない場合は、必要に応じて改善指導と結果確認を行いました。

ソフトウェア開発業務では、新たに従事するパートナー社員へウェブによる情報セキュリティ教育を実施しており、2019年は846名が受講しました。またパートナー企業322社を対象に説明会を実施し、情報セキュリティ脅威の動向や当社ルールの周知を行いました。

物流業務においては、キヤノンMJが提供する教育資料を使い、定期的に教育を実施するとともに、パートナー企業を交えた品質会議を月次で開催してインシデント防止をテーマに話し合いを行っています。

▶インシデント管理への取り組み

キヤノンMJグループでは、インシデント発生時には、従業員からの報告を統括事務局が受け、発生原因を究明し、是正処置・再発防止策（予防処置）を部門と連携して速やかに行う体制を構築しています。

万が一、個人情報や機密情報が漏えいした場合には、お客さまへの報告、お詫び、二次被害防止などの救済措置に優先的に取り組みます。あわせて、関係省庁や関係機関への報告も行います。

これら一連のインシデント対応状況を関係者全員でリアルタイムに情報共有し、迅速で適切な対応を実現するため、「インシデント管理システム」を独自に開発し、運用しています。このシステムはグループ会社にも展開しており、グループ全体のインシデント管理レベルの向上を図っています。

ウェブ環境の安全管理体制の確立

キヤノンMJグループでは、事業の必要性からさまざまなウェブ環境（ホームページ、デモ用サイト、開発環境など）を構築し運営しています。インターネットに接続するこのようなウェブ環境は、サイバー攻撃の脅威に備えることが必須となります。そこで、独自に「インターネット接続環境管理システム」というシステムを開発し、サイトの開設にあたって、サイトのシステム構成情報や安全管理措置の確認を行い、承認、管理しています。

なお、このシステムに登録されたウェブ環境については、定期的に脆弱性検査を行うことで、安全性の維持向上を図っています。

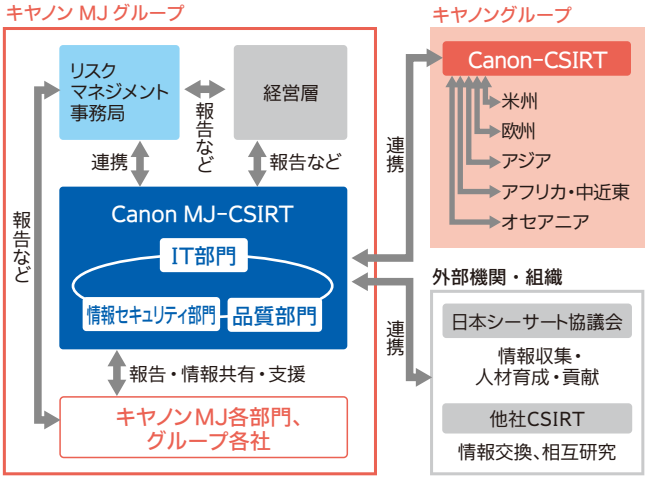
サイバーセキュリティへの取り組み

推進体制と活動

キヤノンMJグループは、昨今のサイバー攻撃が多様化、高度化、巧妙化してきていることから、「『グループ内インフラ』および『お客さまに提供する製品・サービス』に対するサイバーセキュリティのリスク・被害を極小化すること」を目的として、2016年1月に「Canon Marketing Japan Group CSIRT（以下Canon MJ-CSIRT）」を設立し、推進しています。

Canon MJ-CSIRTはキヤノンMJのIT本部内に事務局機能を置き、IT部門、情報セキュリティ部門と、製品・サービスの品質部門の3部門のメンバーから構成された組織です。Canon MJ-CSIRTがグループの中心となって、サイバー攻撃に対する予防・監視活動、発生時の対応を行っています。

また、サイバー攻撃に関する最新の攻撃手法や対応方法などの収集・研究は1社で行うのは難しいことから、キヤノングループをはじめ、「日本シーサート協議会」に加盟するなど、外部の機関や組織と連携しています。



体制図

主な活動内容

1 予防
- 脆弱性情報の収集
- 各種予防対策の実施
- 教育・啓発と訓練の実施
- 危機管理態勢の整備

2 監視
- ログの収集と分析
- 証跡保存

3 対応
- 発生時から収束、再発防止まで一連の支援

標的型攻撃への対応訓練

キヤノンMJグループでは、定期的に標的型攻撃を装ったメールをグループ全従業員へ送信し、実体験を通じた意識啓発を行っています。訓練前には事前教育を行うとともに、実施結果および対処方法については、グループ全従業員が参照可能なイントラネットに開示し、周知徹底しています。

情報セキュリティ人材の育成

さまざまな工夫によって情報セキュリティの意識と知識を持った人材を育成しています。

▶情報セキュリティ人材を育成するしくみ

従業員一人ひとりが日常業務の中で情報資産を適切に取り扱うためには、まず、情報セキュリティに対する「意識」を高め、その上で、正しい判断や行動をするための「知識」を持つことが必要です。このような考えに基づき、さまざまな場面で、全従業員に対する意識啓発や知識教育を実施しています。

また、情報セキュリティを全員参加型の活動として組織ごとに組み込み、維持・改善するために、組織内でマネジメントシステムを支えるキーパーソンを任命しています。

▶すべての従業員を対象とした意識啓発と知識教育

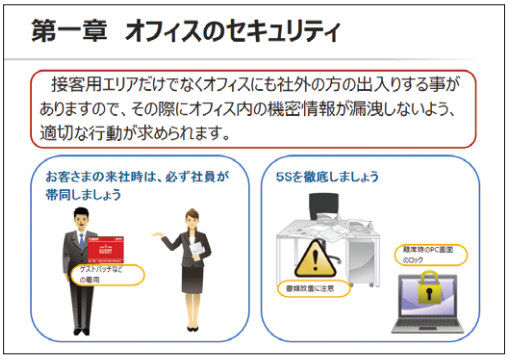
情報セキュリティに対する「意識」や「知識」の定着には、さまざまな機会や方法で繰り返し意識啓発や教育を実施することが必要です。

全従業員の「意識」に働きかけるトップメッセージ

経営者が毎月発信するメッセージの中で、適宜、情報セキュリティの意識啓発を行っています。経営者が自らの言葉で、全従業員に対して直接メッセージを発信することで、情報セキュリティに対する「意識」を高めています。

グループの全役員・従業員を対象としたウェブ教育

キヤノンMJグループでは、グループの全役員・従業員を対象としたウェブ教育を毎年行っています。講座で必要な「知識」を習得し、確認テストでその定着度を測っています。不正解の設問については、その場で解説を確認することで、正しい「知識」を習得します。



教育用コンテンツの例
（スライドとあわせて、そのほかに表示される解説から学習します。）

情報セキュリティに関する情報配信

キヤノンMJグループでは、コンプライアンス活動の一環として、グループの全役員・従業員へメールマガジン「Monthly Compliance News」を毎月配信しています。この活動と連携し、情報セキュリティに関する旬のテーマを配信することで、「知識」の習得や「意識」の啓発につなげています。

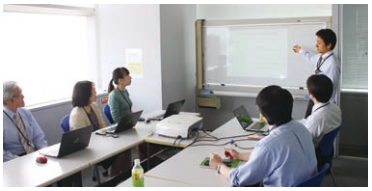
役割に応じた意識啓発を行う対面教育

新入社員や新任管理職には、それぞれの立場に応じたセキュリティ「意識」をしっかりと持ってもらう必要があるため、対面形式にこだわって教育を実施しています。

新入社員に対する対面教育

▶職場におけるリスク管理意識の向上

キヤノンMJグループにて年2回各職場（課）で実施している「コンプライアンス・ミーティング」では、経営上重要なリスクとして位置付けられたテーマの中から、自部門の事業や業務にとって影響の大きいコンプライアンスリスクの洗い出しと、その対策について協議しています。その中で、機密漏えいリスクやサイバー攻撃リスクなど、情報セキュリティに関連するテーマが数多く取り上げられています。各職場の特性に応じたリスク対策を協議することによって、情報セキュリティリスクの低減につなげています。



コンプライアンス・ミーティング

第三者認証の効果的な活用

「ISMS適合性評価制度」と「プライバシーマーク」の認証基準に準拠した運用を
グループ全体で推進しながら、認証取得にも積極的に取り組んでいます。

第三者認証の活用目的

キヤノンMJグループでは、情報セキュリティマネジメントシステム（以下ISMS）や個人情報保護マネジメントシステム（以下PMS）を均質かつ迅速に行うために、第三者認証の基準規格（JIS規格）に基づいて構築しています。

なお、こうした取り組みについて客観的な評価を受けるため、「ISMS適合性評価制度」や「プライバシーマーク」といった第三者認証を活用しています。

ISMSの推進による「顧客満足度の向上を支える業務改善活動」の具現化

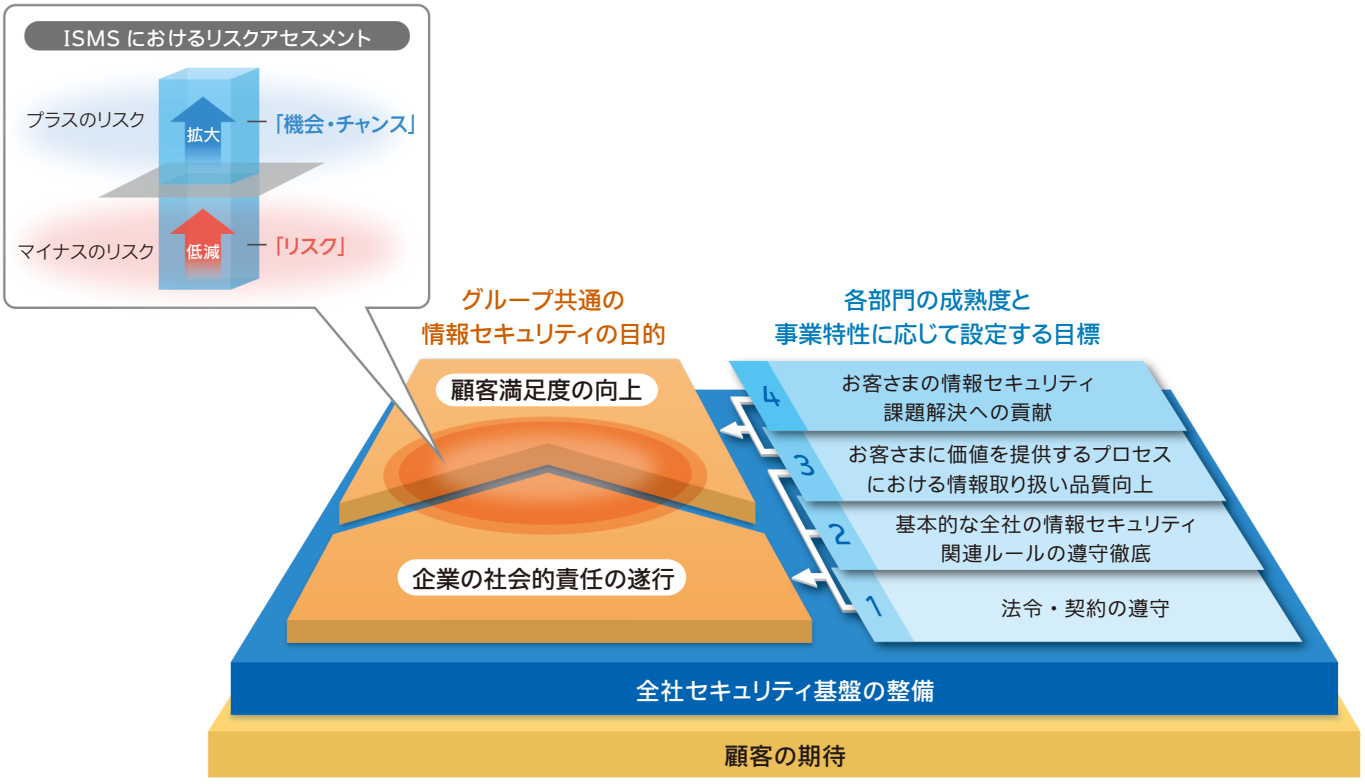
私たちのISMS活動は、大きく2つの目的を掲げています。1つは、情報セキュリティ関連の事故などにより、お客さまにご迷惑をおかけしないという「企業の社会的責任の遂行」という目的です。これに加えて、業務上の情報取り扱い品質を向上させることにより、お客さまにより良いサービスをご提供して、「顧客満足度の向上」を図るという目的も掲げています。

この2つの目的を達成するために、「法令・契約の遵守」「基本的な全社の情報セキュリティ関連ルールの遵守徹底」「お客さまに価値を提供するプロセスにおける情報取り扱い品質向上」「お客さまの情報セキュリティ課題解決への貢献」の4つの目標を、各部門の成熟度と事業特性に応じて設定し、活動を行っています。

設定した目標を達成するために、部門ごとに異なるリスクアセスメントを行っています。全社の情報セキュリティ基盤強化を担う部門では、JIS Q 27001の管理策をもとにして、環境変化を踏まえたベースラインアプローチを行い、情報セキュリティ対策の最適化を行っています。

また、各事業部門では、お客さまの期待を明確にした上で、その期待に応えるべく、それぞれの業務プロセスの改善を目指しています。このときのリスクアセスメントでは、マイナスリスクの低減だけではなく、プラスリスク（機会やチャンス）の拡大も視野に入れた検討を行っています。このような活動を通じて、お客さまにご満足いただけるサービスの提供に結び付けています。

ISMSの推進



プライバシーマークを活用した個人情報保護の強化

キヤノンMJグループでは、個人情報保護マネジメントを法律より一段高い管理レベルで実現するため、プライバシーマークの要求事項であるJIS Q 15001に準拠した個人情報保護マネジメントをグループ全体で推進しています。

なお、プライバシーマーク認証は事業上の必要性に応じて効果的に活用しています。

個人情報保護の高いレベルでの「均質化」と「最適化」に向けた取り組み

キヤノンMJグループは、JIS規格に準拠したマネジメントと、グループ共通の各種対策、独自に構築した「個人情報データベース管理システム」のグループ全体への導入などによって、個人情報管理のPDCAのしくみを「均質化」しています。

一方で、事業内容によってより高い個人情報保護レベルが求められる場合は、それに応じて追加のリスクアセスメントや、ITセキュリティ対策を行うことで「最適化」しています。

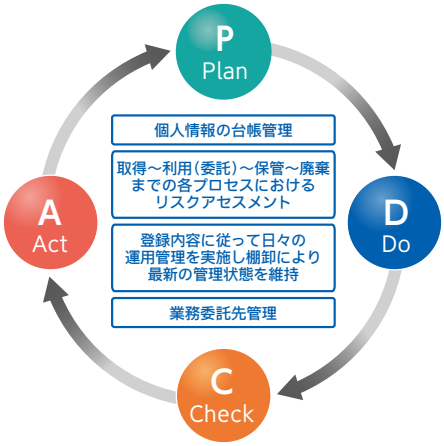
法律より高いレベルでのマネジメントを効果的に実現する管理システム

「個人情報データベース管理システム」では、法律や規格、社内ルールを熟知していなくても、個人情報の取得から廃棄に至るプロセス内のリスクや対策項目の確認と手続きを行うことができます。

たとえば取得プロセスでは、取得方法が書面かウェブフォームかによってリスクが異なるため、それぞれで発生するリスクと対策を自動的に画面に表示します。そのほか、利用方法、保管場所など、取り扱いフローによって異なるリスクに対しても、同様に最適なリスク対策を漏れなく行うことができます。

登録された情報は上長ならびに個人情報保護全社事務局による承認処理が行われ、自動的に全社の個人情報管理台帳が完成します。

また、個人情報の取り扱いを委託している委託先の評価結果や契約内容を一元管理する機能を持っているため、部門間の重複管理を避けることができます。



個人情報データベース管理システムで実現できること

- 全社管理台帳の自動生成と最新状態の維持
- 取得から廃棄までの各プロセスにおけるリスクアセスメント
- 法的要求事項やJIS規格に沿った運用の確認
- 承認ワークフローによるマネジメント
- 業務委託先の評価や契約内容の一元管理

マネジメントシステムの効率的な運用

ISMSやPMSなどのマネジメントシステムでは、それぞれ教育や監査、レビューなど共通する取り組みがあります。そこで、これらの共通事項をまとめて行い、リスクアセスメントなども重複しないよう連携して実施することにより効率化しています。

さらに事業特性に応じて、品質マネジメントシステム（QMS）やITサービスマネジメントシステム（ITSMS）などを導入している部門では、これらとの連携も図っています。

ISO/IEC 27001・プライバシーマーク認証取得状況

（2020年4月1日現在）

会社名	ISMS認証	Pマーク認証
キヤノンマーケティングジャパン株式会社	●	●
キヤノンシステムアンドサポート株式会社	●	●
エーアンドエー株式会社	●	
キヤノンITソリューションズ株式会社	●	●
スーパーストリーム株式会社	●	●
クオリサイトテクノロジーズ株式会社	●	
佳能信息系統（上海）有限公司	●	
キヤノンビズアテンダ株式会社	●	●
エディフィストラーニング株式会社	●	●
キヤノンプロダクションプリンティングシステムズ株式会社	●	●
キヤノンITSメディカル株式会社	●	●
キヤノンカスタマーサポート株式会社	●	●
キヤノンビジネスサポート株式会社	●	

ISO/IEC 15408認証取得製品

製品については、「imageRUNNER ADVANCE」において、国際標準に基づいたセキュリティ対策を実装し、IEEE Std. 2600.1™-2009やIEEE Std. 2600.2™-2009に適合したISO/IEC 15408（コモンクライテリア（CC））認証を取得しています。

認証製品　（2020年4月1日現在。評価・認証中含む）

- imageRUNNER ADVANCE C3500シリーズ（IEEE Std. 2600.2™-2009）
- imageRUNNER ADVANCE C5500シリーズ（IEEE Std. 2600.2™-2009）
- imageRUNNER ADVANCE C7500シリーズ（IEEE Std. 2600.2™-2009）
- imageRUNNER ADVANCE C356F/C356F Ⅲ（IEEE Std. 2600.2™-2009）
- imageRUNNER ADVANCE 4500シリーズ（IEEE Std. 2600.2™-2009）
- imageRUNNER ADVANCE 6500シリーズ（IEEE Std. 2600.2™-2009）
- imageRUNNER ADVANCE 8500シリーズ（IEEE Std. 2600.2™-2009）

情報セキュリティ対策の実装

情報セキュリティ対策の実装にあたり、自社グループの取り扱い製品や技術を活用して、
安全性と効率性を高めています。

▶安全で快適なオフィス環境の実現

IDカードによる入退室管理とプリント制御

キヤノンMJグループでは、各事業所の入退室管理についてIDカードを用いた個人認証を基本とし、フラッパーゲートやセキュリティレベルに応じた生体認証なども導入しています。また、来訪者が立ち入るエリアにはネットワークカメラも導入しています。

入退室管理に使用しているIDカードは、キヤノンの「ICカード認証 Pro for MEAP ADVANCE」と「Anyplace Print for MEAP ADVANCE」を導入し、印刷時の個人認証ならびに印刷ログ管理にも使用しています。印刷時に個人認証を行うことにより、印刷物の取り忘れも減少し、印刷ログ管理とあわせて無駄な印刷の削減や情報漏えいリスクの軽減効果を上げています。


港南事業所のフラッパーゲート


キヤノン S タワーのネットワークカメラ


個人認証プリントシステム

「5S」の徹底によるクリアデスクの実践

安全衛生活動として5S(整理・整頓・清掃・清潔・しつけ)の強化月間を年に3回設け、「居室・会議室の5S」の徹底・定着を図っています。また、クリアデスクの実践では、帰宅する際にパソコンや書類をワゴンやロッカーボックスで施錠保管し、机の上下・周辺には物を置かない状態を継続しています。これにより、情報の紛失や漏えいリスクを軽減させ、適切な情報資産の管理に努めています。


クリアデスクの実践

ゴミステーション方式・機密書類回収ボックス・メディア破砕機による廃棄

大規模な事業拠点を中心に、各デスクサイドに設置されていたゴミ箱をすべて撤去し、廃棄場所を各フロアの決められた場所に集約することで、ゴミの分別廃棄を促す「ゴミステーション方式」を採用しています。また、機密情報や個人情報といった重要書類には専用の機密書類回収ボックスを、CDやDVDなどの廃棄には、メディア破砕機を設置しています。

このような施策によって、機密情報などの重要な情報が不用意に廃棄されることがなくなり、安全な廃棄と適正分別による環境への配慮が両立できています。


ゴミステーション


機密書類回収ボックス


メディア破砕機

グループ全体のITセキュリティ最適化の実現

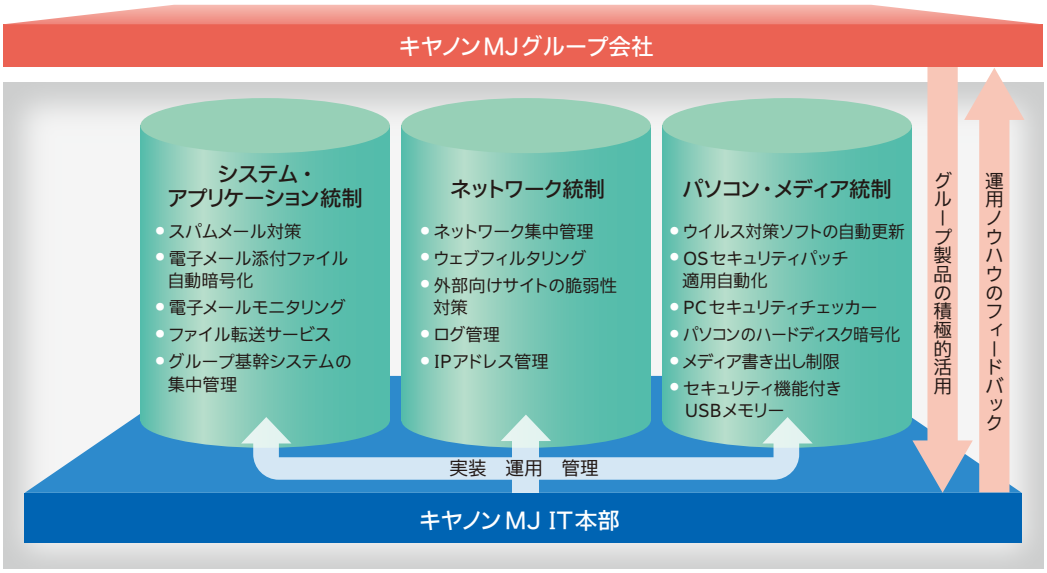
グループ共通対策としてのIT統制

キヤノンMJグループでは、グループ会社を含め、統一されたITセキュリティポリシーに基づき、世の中で日々多発しているサイバー攻撃や不正アクセス、情報漏えいなどの防止に対し、ネットワーク統制、システム・アプリケーション統制、パソコン・メディア統制などのIT統制を行っています。

これにより、グループ内の対策レベルの均一化と運用コストの削減を実現し、安心安全なIT環境を実現しています。

また、ITセキュリティの実装にあたっては、積極的にグループ取り扱い製品を導入することで、運用ノウハウの蓄積や製品改良に活かしています。

● キヤノンMJグループIT統制の全体像



● 積極活用しているグループ製品の例

セキュリティ対策	製品	取扱会社
電子メールセキュリティ強化	総合情報漏えい対策ソリューション「GUARDIANWALL シリーズ」 GUARDIANWALL Mailセキュリティ	キヤノンマーケティングジャパン
ウェブフィルタリング	総合情報漏えい対策ソリューション「GUARDIANWALL シリーズ」 GUARDIANWALL Webセキュリティ	
パソコンの ハードディスク暗号化	ESET セキュリティソフトウェア シリーズ eset ENDPOINT ENCRYPTION イーセット エンドポイント エンクリプション	
ウイルス・スパイウェア 対策ソフト	ESET セキュリティソフトウェア シリーズ eset ENDPOINT PROTECTION ADVANCED イーセット エンドポイント プロテクション アドバンスト	

システム・アプリケーション統制に関する対策の概要

スパムメール対策

スパムフィルター機能を用いたシステム検知を行っており、内部への侵入を防いでいます。

電子メールセキュリティ対策

電子メールにおける情報漏えいリスクを回避するため、不正に情報が社外に送信されていないか随時確認したり、メールに添付されたファイルをシステムが自動的に暗号化したりすることで、メール環境のセキュリティ維持を実現しています。

➡ キヤノンマーケティングジャパン独自開発製品
「GUARDIANWALL Mail セキュリティ」

ファイル転送サービス

電子メールでは送信や受信ができない大容量のファイルを、インターネットを介して外部のサーバーに預けることができるファイル転送サービスを導入しています。通信経路上の情報が暗号化されているため、お客さまとの間での安全な情報の受け渡しが可能です。

グループ基幹システムの集中管理

キヤノンMJグループが利用する基幹システムについては、キヤノンMJのIT本部にて集中管理を行っています。この実施により、ユーザーの認証および一括管理だけでなく、利用状況の監視を行い、適切な資産の管理・統制を実現しています。

ネットワーク統制に関する対策の概要

ネットワーク集中管理

キヤノンMJグループでは、基幹システム同様、ネットワークについても集中管理を行っており、社内外との直接的な通信に制限を行っています。ネットワークへの不正アクセスには常に監視を行い、発見時には直ちに遮断が行えるよう対策を行っています。

ウェブフィルタリング

社外のウェブへのアクセスについては、利用者が無認識のうちにウイルスに感染するなど、年々手口が巧妙化してきています。このため、社外のウェブへのアクセスについては危険なサイトにアクセスできないよう制限するとともに、監視を行っています。

➡ キヤノンマーケティングジャパン独自開発製品
「GUARDIANWALL Web セキュリティ」

外部向けサイトの脆弱性対策

キヤノンMJグループにて用意している外部向けサイトを不正アクセスから適切に保護するために、第三者機関によるウェブサイトのセキュリティ検査を随時行っています。

パソコン・メディア統制に関する対策の概要

ウイルス対策ソフトの自動更新

パソコンのウイルス対策ソフトは、自社グループ取り扱い製品を利用し、ウイルス定義ファイルの自動適用などにより確実に最適化するしくみを実現しています。

➡ キヤノンマーケティングジャパン国内総販売代理店
「ESET Endpoint Protection Advanced」

OSやアプリケーションのセキュリティパッチ適用自動化

利用者の負担を軽減しセキュリティリスクを確実に低減するために、OSのセキュリティパッチ適用や一部アプリケーションのバージョンアップを利用者のパソコンで自動的に行う方式を採用しています。

PCセキュリティチェッカー

個人が適切にパソコンの各種セキュリティ設定や対策を実施しているかを確認できるツールとして、自社開発した「PCセキュリティチェッカー」を公開し、定期的なチェックを促しています。

パソコンのハードディスク暗号化

営業部門の機動力を上げていくためには、パソコンを会社外に持ち出し、社内の情報システムを利用することができるようにする必要がありますが、これにはパソコンの紛失・盗難というリスクもあります。このようなリスクから情報を守るために、外部に持ち出すパソコンについては、自社グループ取り扱い製品であるハードディスク暗号化ソフトを導入することを義務化し、暗号化の実装状況の監視や暗号キーの管理などをIT本部で行っています。

➡ キヤノンマーケティングジャパン国内総販売代理店
「ESET Endpoint Encryption」

メディア書き出し制限

USBメモリーやSDカードなどの可搬媒体を使った情報漏えいリスクを低減するため、パソコンから可搬媒体へのデータの書き出しを原則禁止としています。業務上の理由から書き出しを行う場合も承認制として記録を取得することで、不正な書き出しの抑止を行っています。

セキュリティ機能付きUSBメモリー

USBメモリーにて社外に情報を持ち出す際には、セキュリティ機能付きUSBメモリーを利用することをルール化しています。万一紛失した場合でも、パスワードによる保護と一定回数パスワードを間違えるとデータが自動消去される機能によって、情報が漏えいしないよう対策を行っています。

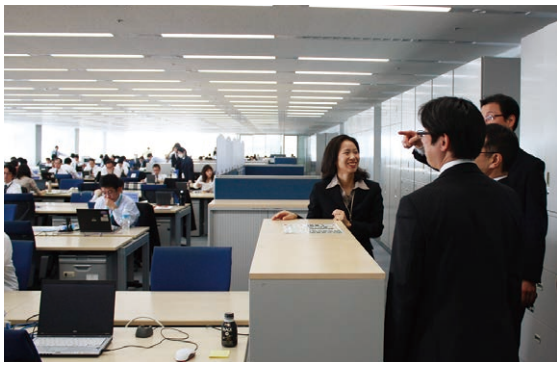
積極的な情報開示と社会への貢献

「情報セキュリティ報告書」の発行のほかにも「オフィスツアー」による活動事例紹介、各種団体への協力、安全なインターネット活用のためのセキュリティ情報サイトの運営などを行っています。

「セミナー」や「オフィスツアー」による情報セキュリティ活動事例紹介

社内外で開催しているセミナーおよびキヤノンS タワーや各支店などで実施している「オフィスツアー」では、お客さまのご要望に応じて、キヤノンMJグループの情報セキュリティの取り組み事例を紹介しています。

この中で、入退室管理やネットワークカメラによる警備など物理的セキュリティ対策の実装事例やドキュメント取り扱いガイドラインの策定、eラーニングによる人材育成、コンプライアンス・ミーティングの定期実施といった人的セキュリティ対策に関して具体的に説明しています。



セミナーおよびオフィスツアーのフロア見学の様子

情報セキュリティ関連団体との連携

キヤノンMJグループは、以下の情報セキュリティ関連団体への参画や賛助を行っています。

- 一般社団法人 コンピュータソフトウェア協会
- 一般社団法人 情報サービス産業協会
- 一般社団法人 情報処理学会
- 一般財団法人 日本科学技術連盟
- 一般社団法人 日本コンピュータセキュリティインシデント対応チーム協議会
- 一般財団法人 日本情報経済社会推進協会
- 一般社団法人 日本情報システム・ユーザー協会
- 特定非営利活動法人 日本ネットワークセキュリティ協会
- フィッシング対策協議会

（五十音順）
※ 2020年4月1日現在

安全なインターネット活用のためのセキュリティ情報の提供

キヤノンマーケティングジャパンは、セキュリティ上の脅威に関する最新情報やその対応方法などをまとめたセキュリティ情報ポータルサイト「マルウェア情報局」を運営しています。お客さまに安心してインターネットを利用していただくために役立つさまざまな情報を本サイトにて発信するほか、Twitterやメールマガジンを活用した情報提供を行っています。

マルウェア情報局の主な掲載内容

- ビジネスやITの最新動向/技術についてのレポート
- マルウェアに関する最新の動向、対処方法
- セキュリティに関するキーワードを解説
- 流行したマルウェアランキング

マルウェア情報局

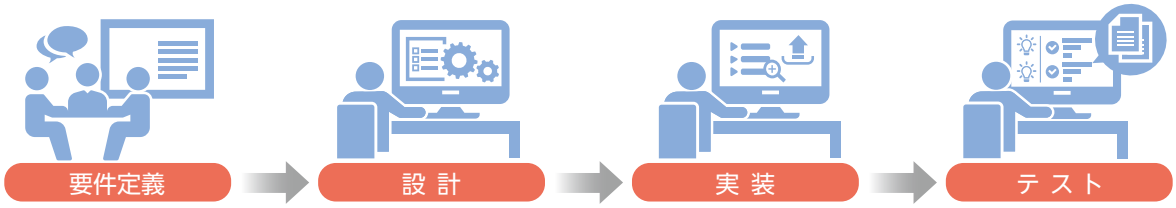
お客さまへの価値提供プロセスにおける情報セキュリティ品質の向上

営業や保守サービス、ソフトウェア開発などの業務プロセスにISMSを中心としたマネジメントシステムを組み込むことによって、情報セキュリティ品質の向上に取り組んでいます。

お客さまに安心安全を提供する開発プロセス

キヤノンITソリューションズでは、金融、製造、流通・サービス、社会公共、公益分野における業種別ソリューションをはじめ、SIサービス、クロスインダストリーソリューション、パッケージ開発など、広範なサービスを通じてお客さまが抱える課題を解決しています。システムの受託開発にあたっては、お客さまからの「信頼」と「安心・安全」にお応えするために、品質管理とともに情報セキュリティへの配慮が不可欠です。

具体的には、「開発環境のセキュリティ」として、体制整備・開発場所の入退室管理・情報資産の適切な取り扱いなどの対策を行うほか、下記のように、「システム開発のセキュリティ」として、各開発プロセスにおけるリスクに応じた情報セキュリティ対策を行っています。



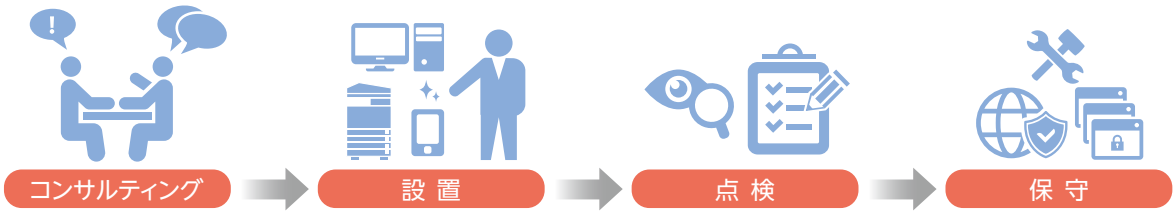
開発プロセスにおけるリスクと情報セキュリティ対策事例

	リスク	対　策
要件定義	●セキュリティ要件の認識誤り ●セキュリティ要件の不足	●開発要件定義にあたっては、十分な知識を持った要員をアサインしてセキュリティ要件を定義し、レビューを行っています。
設計	●セキュリティ要件との齟齬 ●セキュリティ設計のミス	●設計段階においては、セキュリティ要件の定義に基づき、具体的なセキュリティ機能を明確化するためのセキュリティ設計を行っています。セキュリティ設計は、十分なレビューを行い、必要に応じて実現性についての検証も行います。
実装	●コーディングミス ●システムの不十分な構成管理	●実装段階における脆弱性の混入を防ぐため、セキュアプログラミングを行っています。なお、最新のセキュリティ技術については、常に関係者間でノウハウやナレッジを蓄積、共有化しています。 ●また、システムの構成要素の識別と管理を確実に行い、仕様変更や脆弱性が確認された場合の修正を迅速に行えるよう構成管理に万全を期しています。
テスト	●検証と妥当性確認の漏れ	●システムの開発工程でセキュリティの検証と妥当性確認のために、レビューやさまざまなテストを行っています。 ●脆弱性検出ツールなどを用いて十分なテストを実施しています。

お客さまに安心安全を提供する保守サービスの実践

キヤノンシステムアンドサポート（以下、キヤノンS&S）は、全国約170の拠点で、営業・サービス・サポートが一体となってコンサルティングから保守サービスまで一貫してお客さまの支援を展開しています。

キヤノンS&Sは、ISMSおよびプライバシーマークの認証に加えてISO9001を取得しており、それらに準拠した手順を踏まえ、お客さまに安心して複合機やプリンター、ネットワーク機器をご利用いただくための保守サービスを提供しています。



保守サービスプロセスにおけるリスクと情報セキュリティ対策事例

	リスク	対 策
外出前（社内）	●サービス工具（パソコン・USBメモリー）の紛失・ウイルス感染	●サービス工具（パソコン・USBメモリー）は、施錠保管しています。 ●外出前に最新のセキュリティパッチを適用し、ウイルスチェックを実施しています。 ●USBメモリーは日々の持ち出し・返却を記録し、管理しています。
修理受付（移動中）	●修理受付用の携帯電話（スマートフォン）の紛失による情報漏えい	●自動ロック機能、リモートロック機能、リモートワイプ機能、暗号化機能、パスコードロック機能、セキュリティ監視機能を実装しています。 ●携帯電話はネックストラップを使用して、落下・紛失を防止しています。
	●パソコンの紛失による情報漏えい	●社外利用のパソコンはハードディスクパスワード、ログインパスワードに加えてハードディスク暗号化ソフトで保護しています。
点検・保守（お客さま先）	●お客さまデータの漏えい ネットワーク接続時のウイルス流布	●紙詰り処理などで取り除いた用紙には機密情報が含まれる可能性があるため、その処理をお客さまに確認しています。 ●お客さまのデータをお預かりする際は、お客さまに管理方法や作業内容を説明し、了承をいただいています。 ●代替機は、不要なデータが登録されていない状態で貸出し、返却の際にはお客さま情報を消去しています。 ●お客さまのネットワークへ外部のパソコンを接続することを禁止しています。 ●作業上やむを得ず当社パソコンを接続する際には、お客さまにそのセキュリティ対策や作業内容を説明した後、書面にて了承をいただいてから行っています。
帰社後（社内）	●セキュリティ意識・知識の欠如	●サービスメンテナンス時に必要なセキュリティ対策に関する教育を適宜実施しています。
	●お客さまよりお預かりしたデータの目的外利用・誤廃棄・漏えい	●お客さまからデータをお預かりする際は、データの利用目的や返却方法などを「確認書」にてチェックし、その内容に従って取り扱います。 なお、お預かりしたデータは施錠できる環境で保管するなど適切に管理しています。

お客さまに安心安全を提供するIT保守サービス

キヤノンS&S カスタマーサポートセンターは、IT保守をご契約いただいたお客さまの機器に何らかのトラブルがあった際、電話およびリモート操作での復旧支援や必要に応じて現地技術者の訪問手配などを行う、IT機器の障害対応窓口です。

品質推進担当を中心に、リモートツール※の利用におけるリスクの洗い出しと情報セキュリティ対策を実践し、お客さまが安心してパソコンやネットワーク機器をご利用いただけるようサポートします。

リモートツールの利用におけるリスクと情報セキュリティ対策事例

	リスク	対　策
リモート接続	●作業担当者の経験不足によるリスク	●6か月以上の電話対応業務経験および技術研修の受講完了を必須としています。 ●リモートツールによる接続権限の付与条件として、実機を使ってのトラブルシューティングと接続アセスメントを行い、合格者にのみリモート接続の権限を付与しています。
	●お客さまの意図しない接続による情報漏えい	●リモートツールの利用画面上の同意ボタンより、お客さまのご了承をいただき、接続しています。
	●安全性の低いパスワードによる第三者の利用	●リモート接続時には、大文字小文字の英文字および数字を組み合せた複雑なパスワードを使用し、かつ3か月に一回パスワードを変更してセキュリティを高めています。
リモート作業	●盗聴による情報漏えい	●リモートツールは、盗聴・解読が極めて困難な、暗号化技術を採用しています。すべてのデータ通信を暗号化し、高いセキュリティにより情報漏えいの防止を行っています。
	●技術難易度の高い作業による、パソコンの破損やデータを消失するリスク	●リモート作業の内容を5段階のレベルに分け、難易度に応じて上級対応者へのエスカレーション、または現地担当者への訪問対応依頼を行います。
リモート作業後	●接続解除忘れによる情報漏えい	●作業中はお客さまのパソコンの壁紙を黒くして、接続を解除すると通常の壁紙に戻る設定とし、接続中か切断されたかを明確にしています。またお客さまに接続が切れたことを確認いただいた上で、通話を終了しています。

※リモートツールとは、インターネット経由でお客さまのパソコン画面を共有する仕組みです。
この仕組みを利用することで、担当スタッフが遠隔でお客さまのパソコンを操作することが可能となります。

お客さまに安心安全を提供する修理プロセスの追求

キヤノンMJでは、キヤノンホームページにてパーソナル向け製品の引取修理サービスを提供しています。セキュリティ対策を施したサイトから、お客さまご自身で家にいながらいつでも修理をお申し込みいただくことが可能です。

また、銀座・大阪のサービスセンターおよび品川キヤノンプラザS 修理メンテナンス受付コーナーでは、対面にてパーソナル向け製品の修理・メンテナンスのご相談やお申し込みを承っています。

各受付窓口や修理センターでは、お客さまの大切な製品と個人情報をお預かりしている重要性を認識し、情報セキュリティ対策と教育に取り組み、安心して快適に製品をお使いいただけるアフターサポート体制を整えています。

サービスセンターでの
対面受付

ホームページでの
申込受付

修理サービスプロセスにおけるリスクと情報セキュリティ対策事例

	リスク	対　策
受付	●修理受付時のお預かり品（修理品・付属品）の取り違え ●お客さまの個人情報の紛失・漏えい	●窓口で修理受付時にお預かりする機器と付属品、保証書などをお客さまと一緒に確認し、管理用バーコード付きのタグを付けて、専用システムで管理しています。 ●お申し込み時にご提供いただいた個人情報は、強固なセキュリティで保護された当社基幹システム内で管理しています。
	●修理費用のお見積もりをお知らせする際のファクス／eメールの誤送信	●ファクス／eメールはお申し込み時に登録いただいた宛先へシステムから自動送信を行い、誤送信を防止しています。
修理作業	●お預かりした可搬メディアへのコンピューターウイルス感染	●可搬メディアをお預かりした場合は、検疫用パソコンで最新の定義ファイルを用いたウイルスチェックを実施します。 ●修理関連業務用パソコンのすべてにウイルス対策ソフトを導入し、最新の定義ファイルとセキュリティパッチを適用しています。
	●お預かり品の盗難・紛失	●修理センター内の各工程において、管理用バーコードを用い、専用システムに登録されている情報と現品の照合を行っています。 ●修理中に付属品を紛失しないために、作業工程ごとに付属品チェックシートと現品の多重チェックを行っています。 ●盗難・紛失防止として、終業後は施錠環境にて保管しています。
	●修理センターにおける情報セキュリティ事故の発生	●修理センターでは、個人情報の管理・運用手順の指導や教育と、定期的に管理状態の監査を実施しています。
配送	●個人情報が記載された伝票やお預かり品の誤送付	●梱包前に、宅配伝票・修理完成伝票に記載されている機種名と現品が一致していることを確認した上で、修理完成伝票とお預かり品それぞれの管理用バーコードで照合しています。
窓口返却	●お預かり品の誤返却	●お客さまご持参のお預かり書と修理完成伝票に記載されている内容（修理番号、機種・機番、お客さま名、付属品）の声出し確認を行っています。 ●お預かり書・修理完成伝票・お預かり品、それぞれの管理用バーコードを照合し一致していることを確認して返却しています。

NVS導入時におけるセキュリティケア（キヤノンS&S）

NVS（ネットワークビジュアルソリューション）※は、設置した場所の様子をパソコンやスマートフォンなどで、24時間リアルタイムで送信映像を確認することができる監視カメラシステムです。インターネットにつながる製品の性質上、サイバー攻撃を受けるリスクが存在します。そこで、システムそのものへのセキュリティ対策のほか、キヤノンS&SではNVS導入時に次の取り組みを行っています。

管理者パスワードの変更

管理者パスワードは、お客さまにて必ず初期設定から変更していただくことと、安全のために定期的に変更していただくようお伝えしています。

プライベートIPアドレスによる運用を推奨

インターネット接続時は、プライベートIPアドレスでの運用をご提案し、さらにファイアーウォールが設定された環境でのご利用をお勧めしています。

さらにキヤノンS&Sでは、お客さまにNVSの販売とともにUTM（統合脅威管理）ソリューションを同時に提案することで、お客さまにとって容易かつ適正なコストでのセキュリティ対策を実現しています。

※ NVS（ネットワークビジュアルソリューション）＝監視カメラシステム全体のことです。ネットワークカメラとネットワーク録画装置、ネットワーク録画ソフト、アナログカメラ、アナログ録画装置、周辺機器および工事・保守で構成されます。

電子化レポートで、作業報告のペーパーレス化を実現（キヤノンS&S）

キヤノンS&Sでは、タブレットスタイルの2in1パソコンを活用した作業報告書※の電子化を2018年8月より開始し、お客さまに見やすく、わかりやすい作業報告を実施しています。

従来は、作業終了後に手書きの帳票もしくは複合機から出力した帳票にお客さまのご署名をいただいていましたが、現在はタブレット画面上でご説明し電子署名をいただいています。作業報告書の電子化により、見やすく、わかりやすい作業報告とペーパーレス化を実現しています。

また、作業報告書をご入用のお客さまには電子ファイルでお送りすることもできるため、お客さまご自身のパソコン画面上で報告書の内容をご確認いただけます。紙面で保管・管理する必要もなくなり、お客さま満足の向上に貢献しています。

※ 作業報告書とは、複合機、パソコン・サーバーなどの設置・点検・修理などを実施した際に、作業内容を記し、お客さまからご署名をいただく報告書です。

電子化レポートで「見やすい」「わかりやすい」作業報告を実施

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。

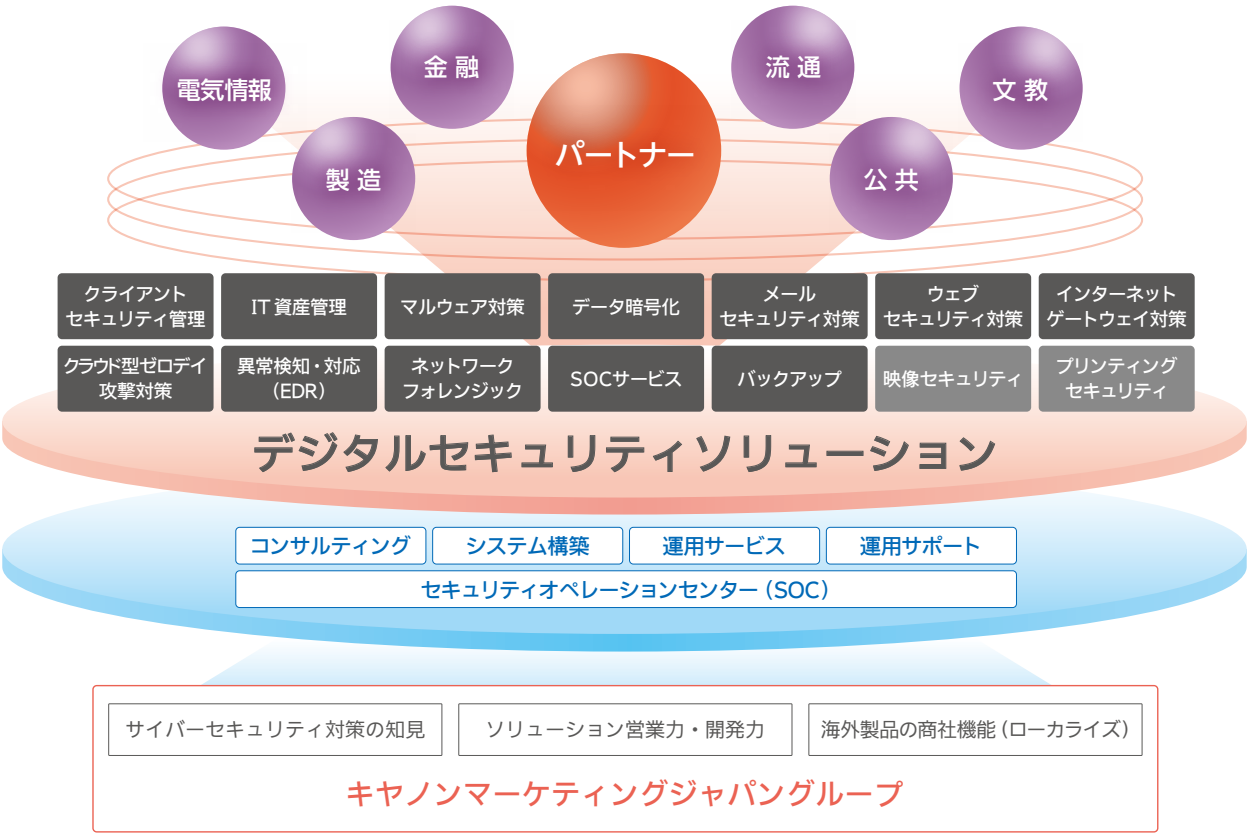
外部環境 サイバー攻撃の増加と新たなセキュリティリスクの表面化

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

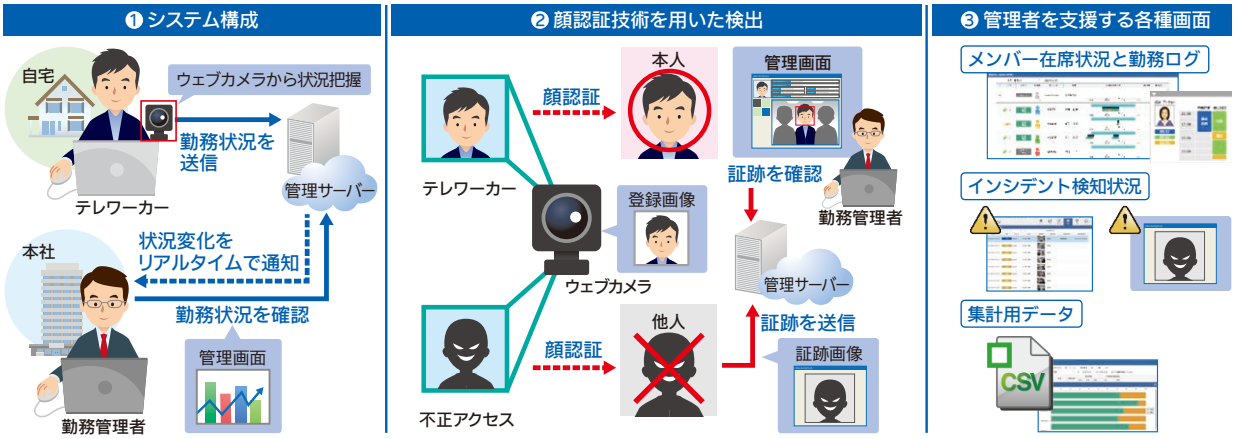
認証資格など	
❶ M&O認証	データセンターのグローバル運営基準※3
❷ ISO 22301	事業継続マネジメントシステム
❸ ISO/IEC 20000	ITサービスマネジメントシステム
❹ ISO/IEC 27001	情報セキュリティマネジメントシステム
❺ SOC2 Type1	保証報告書　グローバル基準の内部統制評価報告書※4

※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

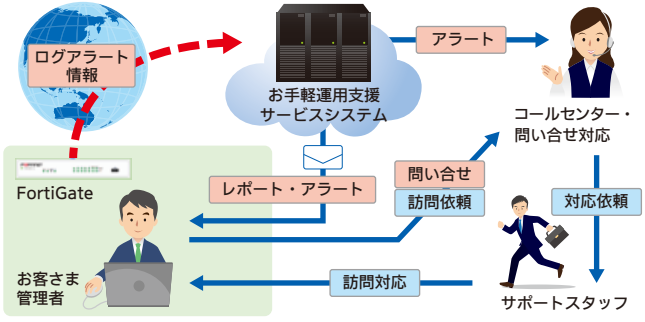
ご導入いただいたFortiGateのログを分析し、脅威カテゴリー単位で状況をレポート化します。

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。

Action2019

2019年の取り組みや実績をご紹介します。

〈第三者認証の効果的な活用〉「クラウドサービスSOLTAGE（ソルテージ）」がISMSクラウドセキュリティ認証（ISO/IEC 27017）を取得（キヤノンITソリューションズ）

「ISMSクラウドセキュリティ認証」（ISO/IEC 27017）は、ISMS認証（JIS Q 27001）に加え、クラウドサービス固有のセキュリティ管理策が適切に導入・実施され、お客さまに安心してご利用いただけるクラウドサービスに対して与えられる第三者認証です。

キヤノンITソリューションズでは、この認証の取得拡大に取り組み、従来から認証取得していた「損害保険会社向けクラウドサービス」に続き、「クラウドサービスSOLTAGE」においても認証を取得しました。

近年、各種クラウドサービスの普及が急速に進んでいます。当社は、クラウドサービスのご提供によりお客さまの業務効率化に貢献するとともに、セキュアなクラウド環境をご提供することで、より安全・確実なお客さまのデータ運用を実現し、顧客満足度を向上していきます。

今後も、クラウドサービス市場の拡大を見据え、「ISMSクラウドセキュリティ認証」の横展開に取り組み、お客さまへ安心・安全をお届けします。

〈お客さまの情報セキュリティ課題解決への貢献〉日経BP社の「日経コンピュータ 顧客満足度調査2019-2020」セキュリティ対策製品部門で7年連続第1位を獲得（キヤノンマーケティングジャパン）

キヤノンマーケティングジャパン※1は、日経BP社が発行する日経コンピュータ誌面にて発表された「顧客満足度調査※2 2019-2020（日経コンピュータ2019年8月22日号）」のセキュリティ対策製品部門で7年連続1位を獲得しました。

あわせて、「自治体ITシステム満足度調査 2019-2020（日経BPガバメントテクノロジー2019年秋号）」のセキュリティ対策製品部門においても3年連続1位を獲得しました。

また、「パートナー満足度調査 2020（日経コンピュータ2020年2月20日号）」のセキュリティ対策製品部門においても1位を獲得しました。

※1 2019年1月より、ITセキュリティ関連商品・サービスの企画・開発機能をキヤノンITソリューションズ株式会社からキヤノンマーケティングジャパン株式会社へ移管しており、本受賞および受賞履歴はキヤノンITソリューションズ株式会社名義です。

※2 顧客満足度調査：コンピューターの利用企業を対象として、セキュリティ対策製品のほかITベンダーが提供するシステム開発・運用サービスやサーバー、ERPパッケージといったハード/ソフト製品などの満足度を調査したものです。

〈積極的な情報開示と社会への貢献〉サイバーセキュリティラボによる調査・研究と啓蒙活動（キヤノンマーケティングジャパン）

キヤノンマーケティングジャパンの「サイバーセキュリティラボ」では、マルウェア解析やサイバーセキュリティ関連技術の研究をもとに、さまざまな活動を行っています。

具体的には、日々発見されるマルウェアの解析結果や話題となっているセキュリティ動向をまとめ、マルウェアレポート（月次および半期で発行）として公開しています。また、知り得た情報を広く認知してもらうため、各種セミナーやカンファレンスで積極的に講演をしています。そのほか、情報セキュリティ関連団体におけるワーキンググループ活動への参画、学術シンポジウムへの論文投稿など、活動の幅を広げています。

高度なセキュリティ人材の育成にも注力しており、ESET社との技術交流やBlack Hat USA／EUROPE※への技術者派遣などを通して、より高度なセキュリティ技術の習得を促進しています。

※1997年から続くサイバーセキュリティの国際カンファレンスで、世界各国からセキュリティ技術者や研究者が参加します。アメリカのほかヨーロッパやアジアで開催されていますが、その中でもBlack Hat USAはセキュリティカンファレンスの中でも最大規模と言われています。

〈お客さまの情報セキュリティ課題解決への貢献〉「情報セキュリティ対策セミナー」を年間61回開催（キヤノンシステムアンドサポート）

2015年頃から中堅・中小企業においても、標的型メール攻撃や身代金要求型のランサムウェア感染など、サイバー攻撃による被害が急増しています。

攻撃手法は巧妙かつ複雑化しているため、ウイルス対策ソフト中心の従来型対策での防御が困難になり、多くの企業で未知の脅威に対する対策の検討、導入が進んでいます。

キヤノンS&Sでは、2019年に外的・内的脅威に対する最新の「情報セキュリティ対策セミナー」を61回（うちオンラインセミナー13回）開催しました。

セミナーでは巧妙化するさまざまなサイバー攻撃について具体的な攻撃手法の解説や多層防御の必要性を説明しており、セミナー受講をきっかけに、自社のセキュリティ課題解決への取り組みを強化されたお客さまも多くいらっしゃいました。

また、各地域で開催している対面型セミナーに加えて、ウェブ視聴型セミナー「オンラインセミナー」を2017年8月より本格始動しました。全国のお客さまが自席からセミナーに参加でき、チャット機能でリアルタイムに質問もできる環境を実現しています。2019年には、「無線LANのセキュリティ課題と解決策」「標的型攻撃メール対策」などのテーマで、オンラインセミナーを実施しました。

お客さまの課題解決につなげるべく、利便性の高いセミナー受講機会をご提供しています。

キヤノンマーケティングジャパングループ

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

2020年6月発行