Canon

Information Security Report 2018

キヤノンマーケティングジャパングループ

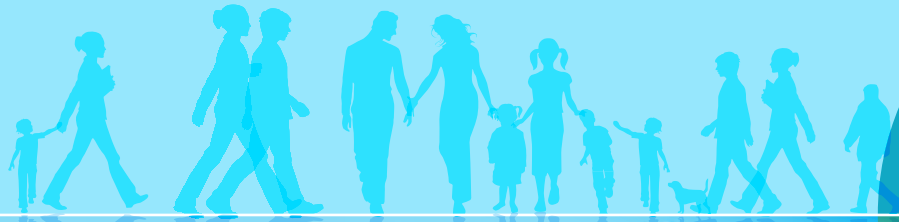
情報セキュリティ報告書 2018

お客さまとともに

50th Anniversary

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。



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2017年に取り組んだスパイラルアップポイントを、Action2017としてわかりやすく掲載することに留意しました。

※「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。

Contents

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って顧客満足度向上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、2018年2月1日に創立50周年を迎えました。これもひとえにお客さまのご支援、ご愛顧のおかげと、深く感謝申し上げます。

50年前、「よりお客さまに近づく」という基本理念のもとでキヤノンの国内販売部門が分離独立して生まれた私たちは、今、新たなミッションとして「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、グループ一丸となってそのミッションを果たすべく取り組んでいます。

現在は、あらゆるものがインターネットにつながるIoT（Internet of Things）が急速に進展し、さまざまな機器やシステムがつながることで得られる膨大なデータは、その活用によって、社会、企業、個人に多大な恩恵をもたらしています。

しかしその一方で、個人情報や金銭などを狙ったサイバー攻撃もさらに高度化・巧妙化が進み、大きな「社会課題」となっています。2017年は、従来型の攻撃のほか、ネットワークを介して感染を拡大するランサムウェア「WannaCry」の登場や、巧妙に細工したメールで企業担当者をだます「ビジネスメール詐欺」によって、被害総額は億単位に及びました。さらには「仮想通貨」を狙う攻撃など、新たな脅威も生まれています。また、爆発的に増大しているIoTデバイスは、サイバー攻撃のターゲットであるのみならず、攻撃のリソースとして活用される動きも見られます。

私たちは、デジタルカメラ、プリンター、複合機、監視カメラなどのハードウェアのほか、各種ソフトウェアやソリューションなど、先進の“イメージング＆IT”ソリューションをお客さまにご提供している事業者として、事業を営む上でこれらの脅威に対するセキュリティの確保は必須の取り組みとなります。

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

現在私たちは、グループ内部においては「サイバーセキュリティ経営」を推進すべく、従来から取り組んでいる情報セキュリティガバナンス・マネジメント体制のもと、個人情報を含む情報資産全体の適切な取り扱いを図るとともに、サイバーセキュリティ専門組織CSIRT※を加え、サイバー攻撃の予防・検知・発生時対策の強化を推進しています。

また、お客さまにお届けしている製品・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、情報セキュリティ品質の向上に取り組んでいます。

さらに、情報セキュリティ関連の製品・ソリューションを取りそろえ、日々の活動の中で培ったノウハウも含めてお客さまにお届けすることによって、お客さまの情報セキュリティ課題解決に貢献するよう努めています。

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・ソリューションをご紹介しています。ご覧いただいた皆さまのお役に立つことができれば幸いです。

※ CSIRT：Computer Security Incident Response Team

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。

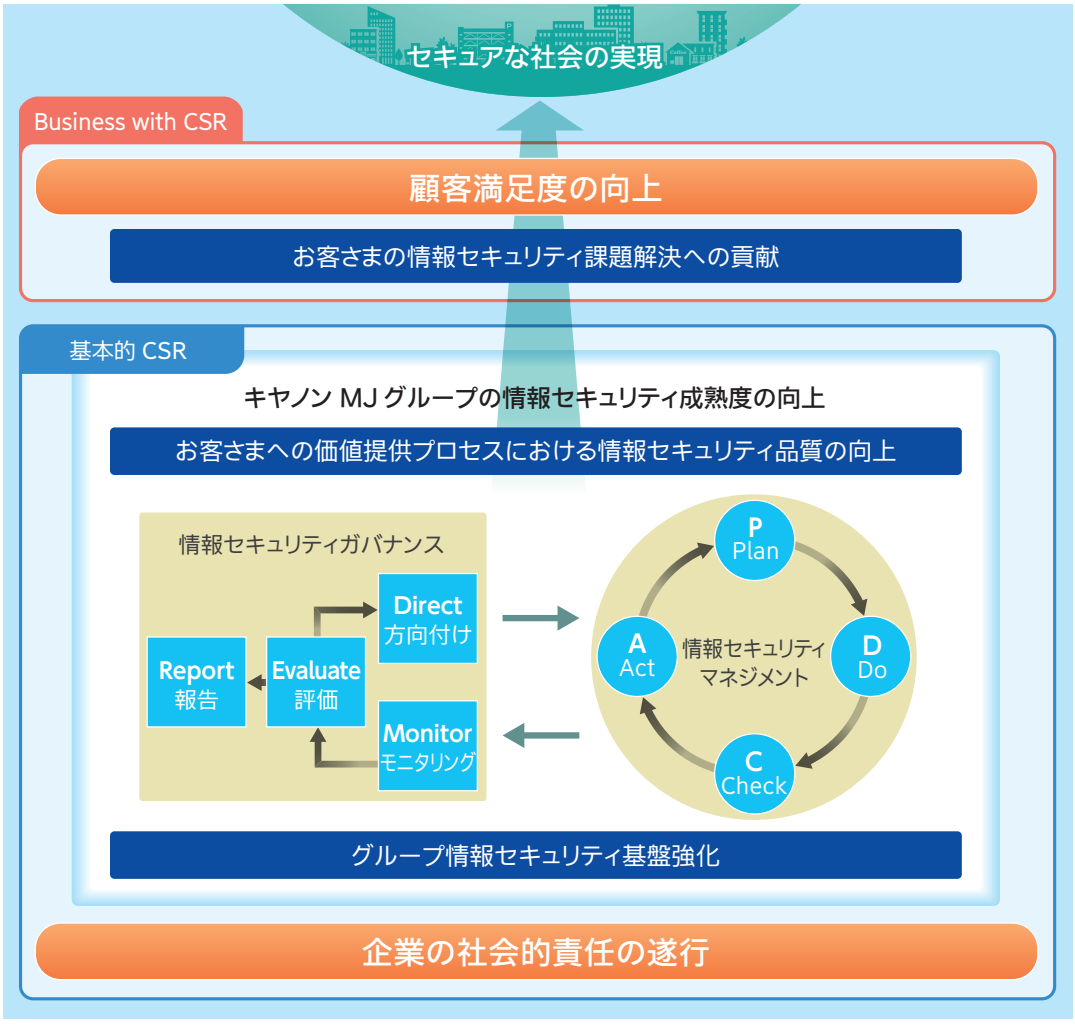
これらの活動の中で、事業活動を営むための前提となるステークホルダーの要請に対応した必要不可欠なCSR活動は「基本的CSR」です。

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

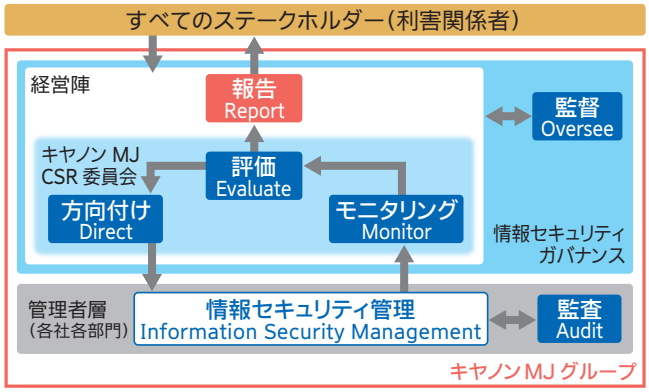
情報セキュリティの取り組みは、コンプライアンスや環境対応、事業継続、品質管理などの社会要請への対応とも密接に関連しています。

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。

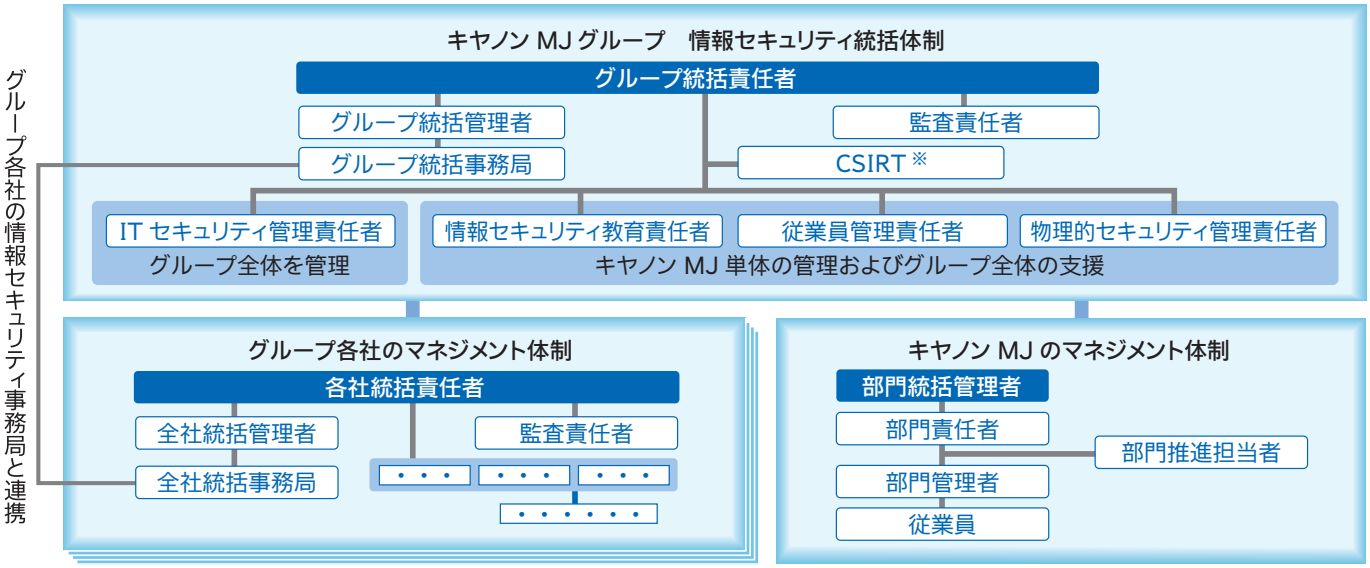
グループ情報セキュリティ統括体制はキヤノンMJの情報セキュリティ主管部門がグループ統括事務局の役割を果たし、グループ全体の情報セキュリティマネジメントを統括しています。

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マネジメント規程」を制定しています。

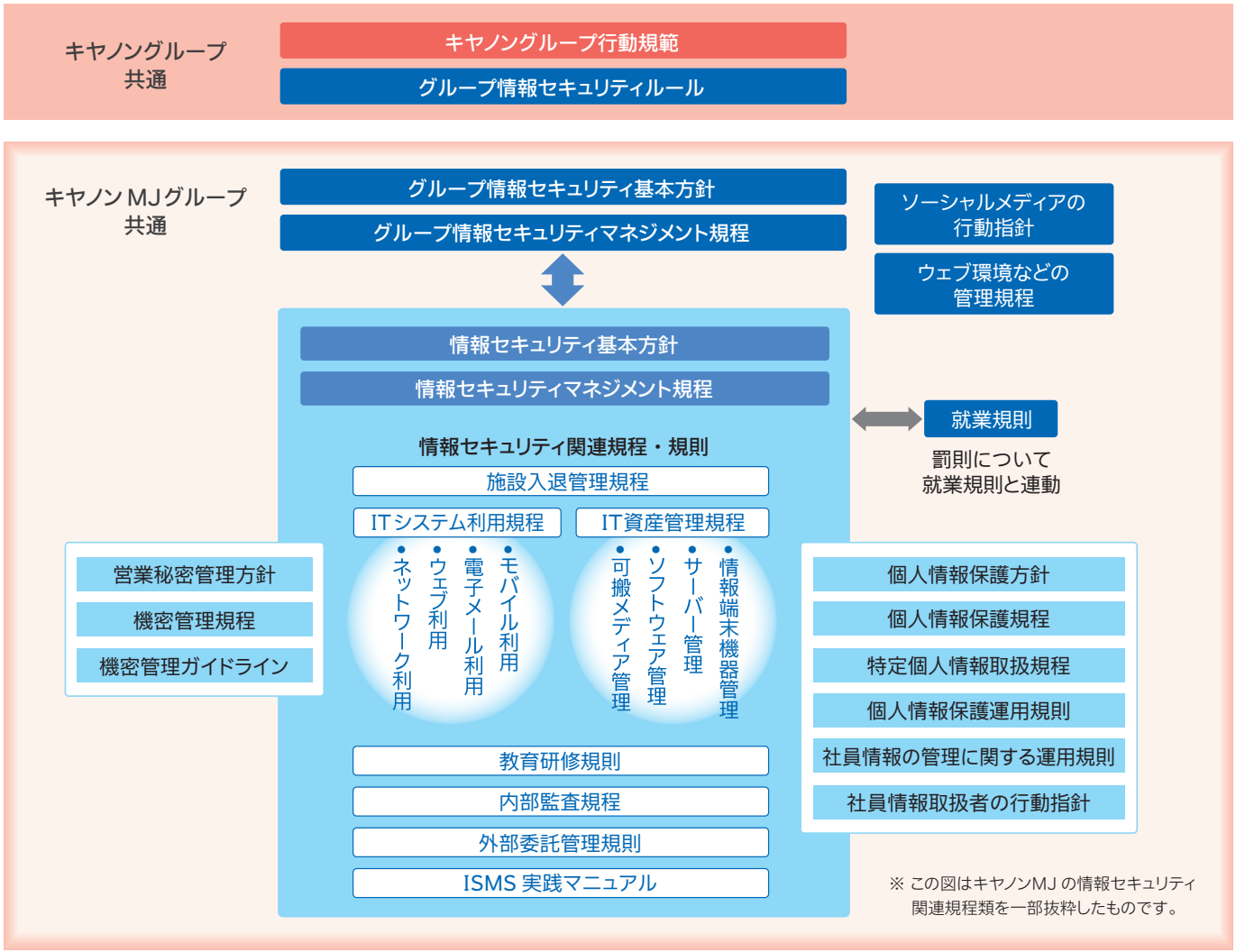
これらの方針や規程を踏まえ、キヤノンMJグループ全体の情報セキュリティ基盤を支える規程類と、重要な情報資産である個人情報保護や機密管理に関する規程類は、それぞれの規程の中で定める要素が重複することがないようにしています。

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、個人情報保護や機密管理に関する規程は、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もあるため、キヤノンMJグループ統一の規程をベースにした上で、必要に応じて、個別にカスタマイズされた規程を整備しています。

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。

具体的には、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、複合機の保守サービス・物流、ソフトウェア開発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。

また、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。

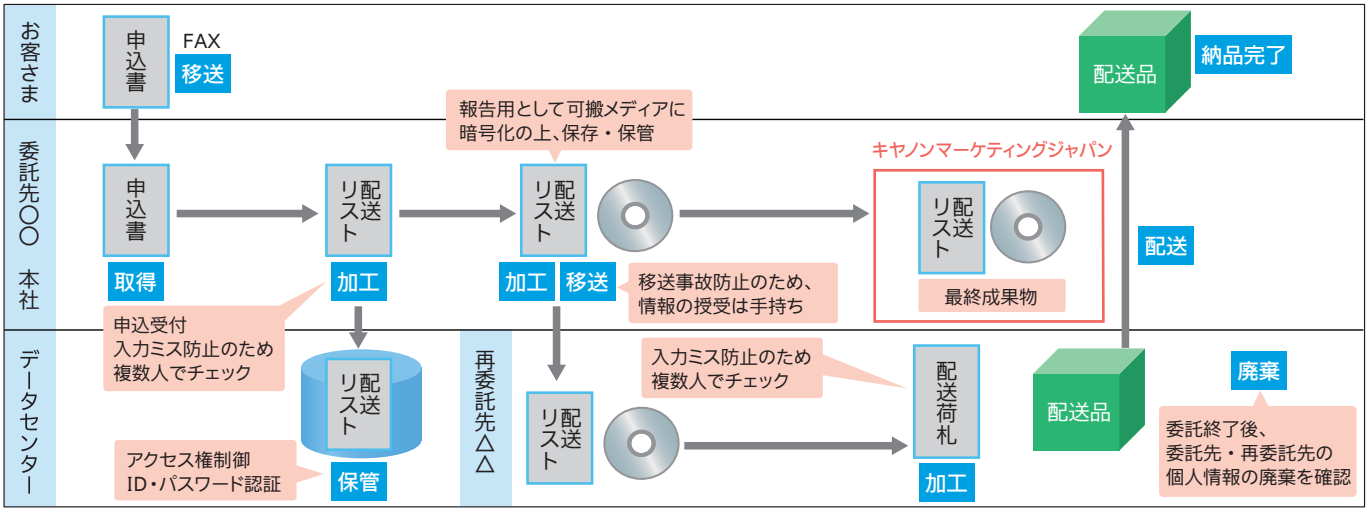
パートナー企業の情報セキュリティ品質の向上

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。2017年には、466社800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、427社749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。

また、物流業務では、キヤノンMJが提供する教育資料を使って120社が自社内で教育を実施しました。

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、2017年は1,223名が受講しました。

サンプル キャンペーン申込受付・景品発送



業務フロー図

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。このシステムは順次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。

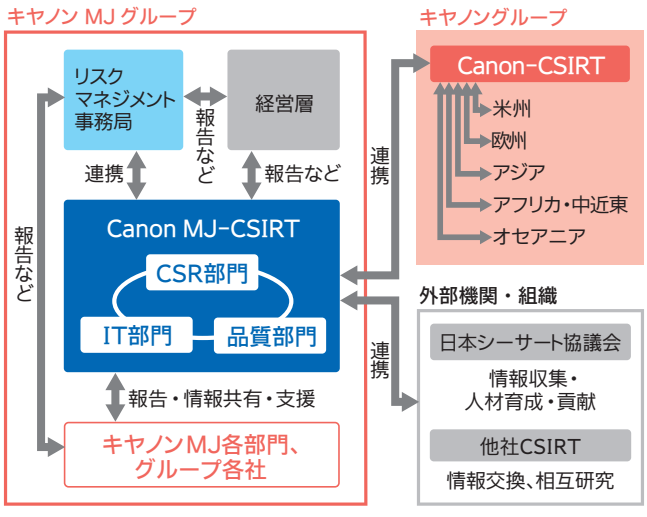
サイバーセキュリティへの取り組み

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CSR部門内に事務局機能を置き、IT部門や製品・サービスの品質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・研究は一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

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。

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

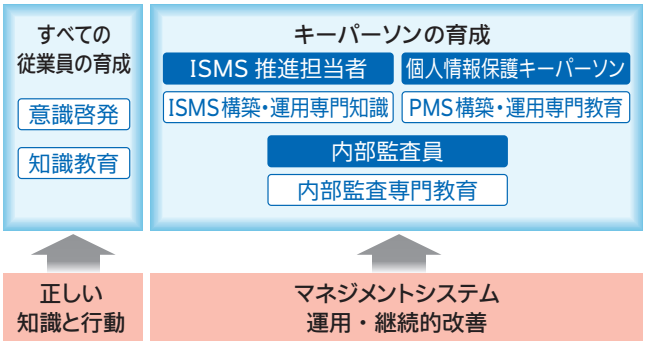
情報セキュリティ人材の育成

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育成しています。



すべての従業員を対象とした意識啓発と知識教育

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。

情報セキュリティに関する情報配信

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。

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「Monthly Compliance News」というメールマガジンを毎月配信するとともに、必要に応じて都度、臨時号も配信しています。この活動と連携し、情報セキュリティ知識の習得や意識啓発につながる内容を適宜配信しています。

従業員が情報セキュリティに関心を払い、社会の共通課題を理解することで、お客さまへの価値提供にも結び付けられると考えています。

「Monthly Compliance News」より一部抜粋

役割に応じた意識啓発を行う対面教育

新しく社会人となる新入社員や職場のマネジメントを新たに担う新任管理職には、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

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、その他に表示される解説から学習します。）

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、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、各職場の特性に応じたリスク対策が協議されることによって、情報セキュリティリスクの低減につながっています。

コンプライアンス・ミーティング

Action2017 2017年の取り組み

「コンプライアンス・ミーティング」の実施

2017年上期のキヤノンMJの「コンプライアンス・ミーティング」では、全組織のうち約7割の組織※が、「機密漏えいリスク」「サイバー攻撃リスク」をテーマとして取り上げ、リスクの洗い出しと、その対策について協議を行いました。グループ会社でも多くの組織が同様にテーマとして取り上げました。

2017年下期には想定される問題事例を使って、登場人物の問題点と予防策を話し合いました。また、自部門において想定される問題事例とその予防策について議論しました。「営業秘密」「個人情報保護」「サイバー攻撃」を、キヤノンMJの全組織の約6割※がテーマとして取り上げました。グループ会社でも、多くの組織が同様のテーマを取り上げました。

※ 複数テーマ選択可

「Monthly Compliance News」で配信した情報セキュリティ関連テーマ

配信月	配信テーマ
2017年2月	最新の脅威動向を知って、リスクを意識し、しっかり対策をしよう！
2017年4月	5月30日から「改正個人情報保護法」が全面施行されます！
2017年8月	あなたの部門の個人情報、保護は大丈夫ですか？
2017年9月	不審メールのURL・添付ファイルを開いてしまったら即連絡を！ ～不審メール受信時に取るべき行動～

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、これらの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

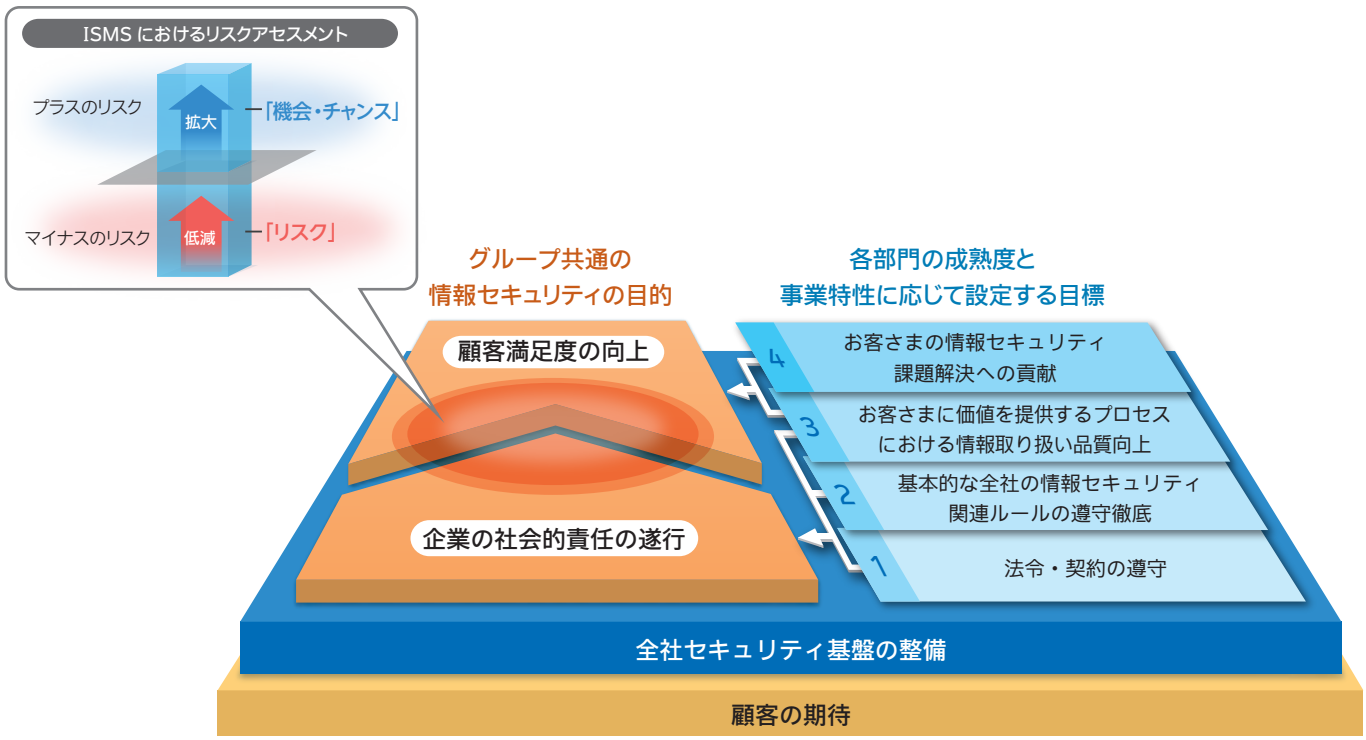
私たちのISMS活動は、大きく2つの目的を掲げて活動しています。1つは、情報セキュリティ関連の事故などにより、お客さまにご迷惑をおかけすることをしないという「企業の社会的責任の遂行」という目的です。これに加えて、業務上の情報取り扱い品質を向上させることにより、お客さまにより良いサービスをご提供して、「顧客満足度の向上」を図るという目的も掲げています。

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。

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

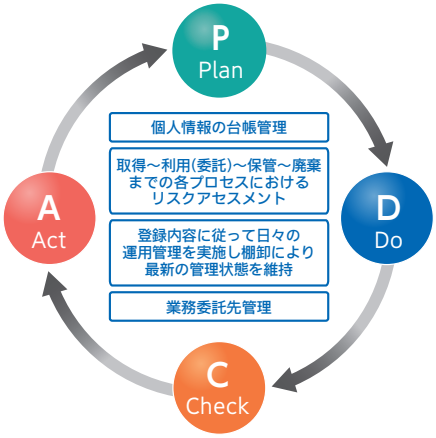
キヤノンMJグループでは、全社台帳管理、リスクアセスメント、委託先管理など、JIS規格に準拠した個人情報の取り扱いを効果的に実現するために「個人情報データベース管理システム」を独自に開発し運用を行っています。

「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、誰でもマニュアルレスで自然に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を実現しています。



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ライフサイクル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

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、個人情報保護を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。

さらに、「均質化」と「最適化」のスパイラルアップを図るため、各社の個人情報保護活動における好事例の共有や課題解決に向けた意見交換などを行う「グループPMS担当者会議」を毎年開催しています。

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。

キヤノンMJグループにおける認証取得状況

（2018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	●	●
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	●	●
コマーシャルプリンティングラボ株式会社	●	
キヤノンライフケアソリューションズ株式会社	●	
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	●	

※ ISMS認証については、一部部門取得の会社があります。

ISO/IEC15408認証取得製品

製品については、imageRUNNER ADVANCEシリーズにおいて、国際標準に基づいたセキュリティ対策を実装し、IEEE Std 2600.1TM-2009やIEEE Std 2600.2TM-2009に適合したISO/IEC15408（コモンクライテリア（CC））認証を取得しています。

● 認証取得製品

（2018年4月1日現在）

- imageRUNNER ADVANCE C3530/C3520
  （IEEE Std 2600.2TM-2009）
- imageRUNNER ADVANCE C5560/C5550/C5540/C5535
  （IEEE Std 2600.2TM-2009）
- imageRUNNER ADVANCE C7580/C7570/C7565
  （IEEE Std 2600.2TM-2009）
- imageRUNNER ADVANCE C356F
  （IEEE Std 2600.2TM-2009）
- imageRUNNER ADVANCE 4545/4535/4525
  （IEEE Std 2600.2TM-2009）
- imageRUNNER ADVANCE 6575/6565/6560
  （IEEE Std 2600.2TM-2009）
- imageRUNNER ADVANCE 8505/8595/8585
  （IEEE Std 2600.2TM-2009）

Action2017 2017年の取り組み

個人情報保護法の法改正に対応

キヤノンMJでは、2017年5月30日から施行された改正個人情報保護法に対応するため、以下の取り組みを実施しました。

1. 個人情報保護関連規程・規則類の改定

個人情報保護に関連する規程・規則類を法改正に適合させるとともに、実運用を考慮して改正しました。また、グループ全体に法改正への対応と遵守を徹底するため、グループ統一の規程・規則類としました。

2. 改正個人情報保護法に対する教育の実施

グループ全社員に周知徹底するため、eラーニング形式の教育を実施しました。

3. 個人情報データベース管理システムの改修と臨時棚卸しの実施

個人情報データベース管理システムの改修を行い、全面施行後の速やかな法改正への対応のため、臨時の棚卸しを実施しました。

4. セルフチェックによる法遵守状況の確認

年1回行う情報セキュリティに関するセルフチェックの際、法改正の確認項目を盛り込み、その理解度の確認および再徹底を図りました。

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

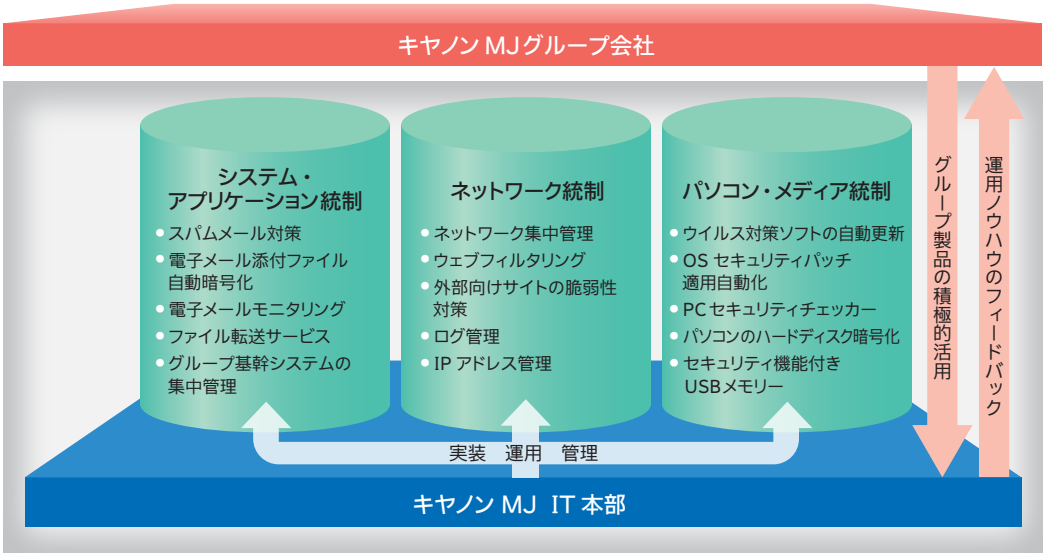
グループ共通対策としてのIT統制

キヤノンMJグループでは、グループ会社を含めた統一された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
電子メールモニタリング	総合情報漏えい対策ソリューション「GUARDIANWALL シリーズ」 GUARDIANWALL Mailファミリー	キヤノンITソリューションズ
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 DESlock+ デスロック	キヤノンITソリューションズ
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	キヤノンITソリューションズ

情報セキュリティ対策の実装

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。

● 電子メール添付ファイル自動暗号化

メール送信時における添付ファイルの情報漏えいリスクを回避するため、システムがメールに添付されたファイルの自動暗号化を行い、お客さまへのセキュアなメール送信環境を実現しています。

● 電子メールモニタリング

電子メールにて不正に情報が社外に送信されていないかを随時モニタリングしています。

【キヤノン ITソリューションズ独自開発製品
「GUARDIANWALL Mailファミリー」】

● 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読み書き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、お客さまとの間で安全に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。

● 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 ITソリューションズ国内総販売代理店
「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 ITソリューションズ国内総販売代理店
「ESET DESlock Plus Pro」】

● 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。

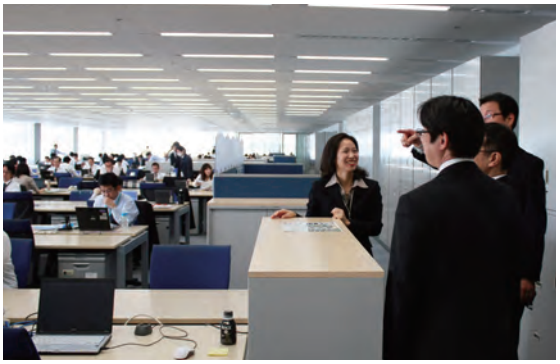
積極的な情報開示と社会への貢献

「情報セキュリティ報告書」の発行の他にも「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、お客さまの目的に応じて、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。

この中では、入退出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
- 一般財団法人 日本科学技術連盟
- 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
- 一般社団法人 日本スマートフォンセキュリティ協会
- 特定非営利活動法人 日本セキュリティ監査協会
- 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
- 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（日本シーサート協議会）

（五十音順）
※ 2018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 IT ソリューションズは、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他、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・開発場所の入退出管理・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。

脆弱性検査の様子

● 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 180 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。

カスタマーエンジニアによる保守の様子

● 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、施錠できる場所に保管しています。 ・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。 ・パソコンの社外持ち出しに関しては社外利用申請システムを使用し、所在管理をしています。 ・USB メモリーは台帳管理を行い、日々の持ち出し・持ち帰り管理を行っています。
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	・持ち出す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暗号化しています。
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	・紙詰まり処理で取り除いた用紙や紙片には機密情報が含まれる可能性があるため、必ず処理方法をお客さまに確認しています。 ・お客さまのデータを預かる際は、お客さまに管理方法や作業内容を説明し、了承をいただいてから行っています。 ・代替機は、不要なデータなどが登録されていない状態で貸し出し、また代替機引き上げの際にはお客さま情報の消去を実施しています。 ・お客さまのネットワークへパソコンを接続することは、禁止しています。 ・作業上やむを得ず接続する際には、お客さまに当社パソコンのセキュリティ対策状態や作業内容を説明した後、お客さまに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」にて確認し、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環境に保管するなど適切に管理しています。

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

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・名古屋・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。

修理受付窓口

● 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弊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	・お預かりした可搬メディアは、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・修理完成伝票と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。

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

NVS 導入時におけるキヤノン S&S のセキュリティケア

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 24 時間リアルタイムでパソコンやスマートフォンで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他、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。

■ネットワークカメラをパスワードで管理する

・管理者パスワードは、お客さまにて初期設定から必ず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 アドレスで運用する

・インターネット接続時の IP アドレスは、プライベート IP アドレス運用をお勧めし、ファイア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、お客さまのご要望に応じた適切な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。

スマートレポートで、『きれい』『見やすい』『わかりやすい』作業報告を実現

キヤノン S&S では、お客さまにわかりやすい作業報告を実現するために、従来の手書きレポートから独自開発の iPhone※専用アプリでレポートを作成し、複合機から出力する「スマートレポート」に切り替えました。複合機本体から収集した正確な品質情報は QR コード化されてシステム登録するため、手入力に比べ情報入力の精度向上、作業効率 UP はもとより、お客さま満足度 UP に大きく貢献しています。

■スマートレポートの特長

・各種カウンター値や消耗品（トナー）在庫数を A4 縦の印字レポートで出力

・お客さまご使用機種シリーズの写真が印刷される

・NETEYE（複合機・プリンターの使用環境遠隔モニタリングシステム）の各種オプションサービスの登録状況がわかる

スマートレポートで「きれい」「見やすい」「わかりやすい」作業報告を実施

※ iPhone は、米国およびその他の国で登録された Apple Inc. の商標です。

『アプリで修理依頼サービス』の推進

従来お客さまからの複合機の修理依頼については、電話での受付としておりましたが、聞き取り項目が多いため、お時間をいただくこととなっていました。

そこで、キヤノン S&S では、お客さまに修理依頼の利便性向上を図るため、「アプリで修理依頼サービス」というアプリケーションの導入を推進しています。

このアプリケーションを導入することにより、複合機の操作部パネルから、簡単な操作で修理依頼を行うことができます。修理センターでは、インターネット経由で暗号化されて送られてくる製品情報および故障情報に基づき、復旧サポートを行い、必要であればサービス担当者を手配します。

これによって、修理依頼の利便性向上とあわせ、メンテナンス対応の迅速化によるダウンタイムの削減を実現し、お客さま満足度の向上につなげています。

お客さまが複合機から
修理を依頼

カスタマーエンジニアが
iPhone で
修理依頼を受付後、
速やかにお客さまと
訪問日時の調整連絡

※ アプリケーションの利用には、複合機「imageRUNNER ADVANCE」シリーズの導入、および遠隔保守サービス『NETEYE』への加入が必要です。

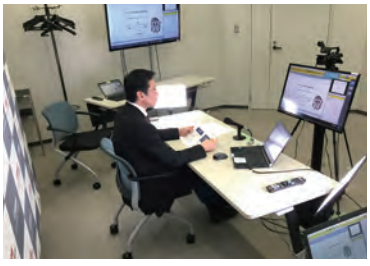
オンラインセミナーの取り組み～集客型ビジネスから非対面ビジネスへ～

キヤノン S&S では、WEB 配信型セミナー「オンラインセミナー」を 2017 年 8 月より本格始動しました。

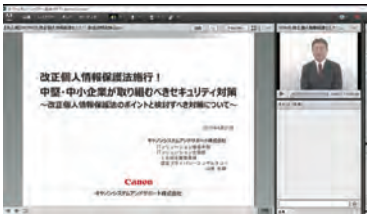
各地域で開催している対面型セミナーに加えて、全国のお客さまが自席からセミナーに参加でき、チャット機能でリアルタイムに質問もできる環境を実現しています。

2017 年 6 月のテストランから計 33 回のセミナーを実施、1,223 名ものお客さまにご参加をいただきました。

働き方改革が推進される中、IT を有効活用した効率的なコミュニケーションツールとして、セミナー運営に取り組んでいきます。



セミナー配信の様子



実際のセミナー映像

お客さまの情報セキュリティ課題解決への貢献

お客さまの情報セキュリティ課題解決に最適な情報セキュリティ製品・ソリューションを、自社グループの運用ノウハウも含めて提供します。

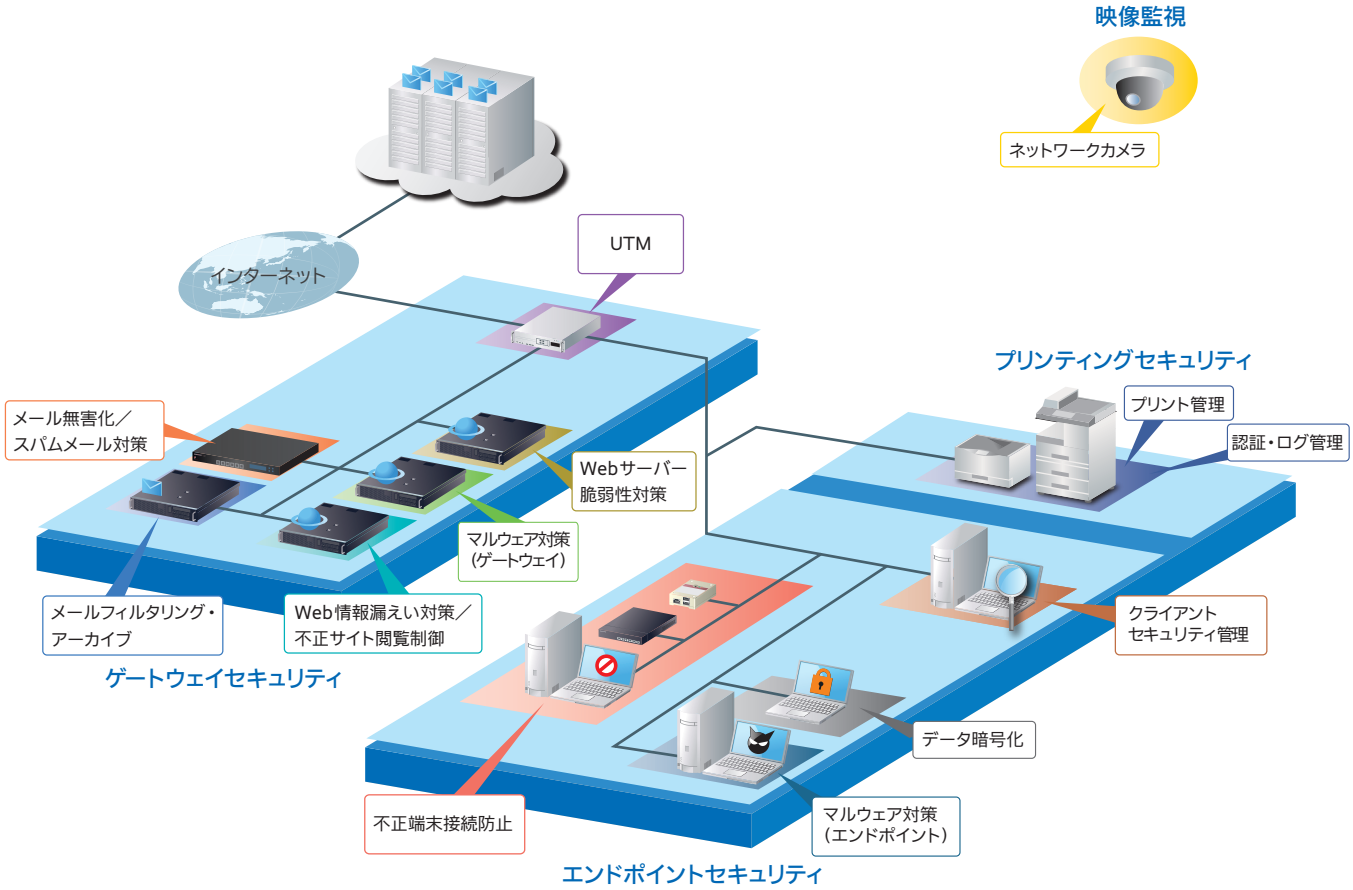
巧妙化するサイバー攻撃と環境変化によるセキュリティリスクの増加

ランサムウェアやビジネスメール詐欺などのサイバー攻撃が巧妙化する一方で、IoTやワークスタイル変革などの環境変化に伴い、新たなセキュリティリスクが発生しています。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となっています。

包括的なセキュリティソリューションの提案

キヤノンMJグループは、自社開発のセキュリティ製品だけでなく、国内および海外ベンダーの実績のある製品を用意するとともに、長年にわたり蓄積してきた経験とノウハウをベースに、情報漏えいや標的型攻撃など組織内外の脅威に対する包括的なセキュリティソリューションを提案します。

● セキュリティソリューションの全体像



セキュリティソリューションのご紹介

映像監視

ネットワークカメラ

高画質な映像とさまざまなニーズにお応えする映像監視を実現

課題 物理セキュリティを強化する手段の1つとして、映像監視は有効な手段です。
しかし、映像監視は、記録映像の画質、撮影範囲、照度、防水・防塵など、使用ニーズに合った機器やシステムそしてサポートを選定しないと、その有効性は担保されません。

対策 キヤノンのネットワークカメラは、高画質な映像、広範囲な撮影、低照度環境での撮影、過酷な環境下での撮影などといったさまざまな使用条件に合ったラインアップをそろえています。また、映像監視をサポートするさまざまなオプションやシステム、保守サービスも取りそろえ、お客さまの映像監視をご支援します。

取扱製品 ネットワークカメラ 「VBシリーズ」(開発元 キヤノン) ／ビデオ管理ソフトウェア「Milestone XProtect」(開発元 milestone)

ゲートウェイセキュリティ

UTM

さまざまな脅威に対するセキュリティ機能を 1 台で実現

課題 外部から特定の組織を対象として情報を盗み取る標的型攻撃が急激に増加しています。また、攻撃を受けた組織内部のPC やサーバーが踏み台となってさらに外部への攻撃に加担する脅威も増えており、外部と内部からの不正アクセスについての対策が必要です。

対策 外部からの攻撃はもちろん、組織内部からの不正アクセスを防ぐことができるUTM (統合脅威管理) 製品。組織の内部と外部、双方向のパケットを監視し、不正な通信を遮断することが可能です。また、高いスループットを誇り、設定・運用も容易であるため導入や運用コストを大幅に抑えることができます。

取扱製品 Clavister (開発元 Clavister AB) ／ SonicWALL (開発元 SonicWall Inc.) ／ FortiGate (開発元 Fortinet, Inc.)

メールフィルタリング・アーカイブ

メールの適切な管理と利用状況を把握して誤送信や情報漏えいを防ぐ

課題 メールは手軽なツールでありながら、一方で誤送信などの思わぬ情報の漏えいを発生させるリスクがあります。利用者への注意喚起だけでは対策として不十分な上、企業の情報管理責任が問われる場合もあります。外部に対して送信する情報の適切な管理方法と、社員のメール利用状況を把握することが求められています。

対策 送信先や添付ファイルが不適切なメールは、社外に送信される前にブロックし、管理者や送信者本人が再確認することにより誤送信や情報漏えいを防ぐフィルタリング機能が有効です。また、アーカイブ機能により、送受信されるメールを保存することで、社員のメール利用状況を把握し、監査することができます。キヤノン ITソリューションズでは、国内のお客さまのニーズをもとに独自開発した製品をご用意しています。

取扱製品 GUARDIANWALL Mailファミリー・GUARDIANWALL Cloudファミリー（開発元 キヤノン ITソリューションズ）

マルウェア対策（ゲートウェイ）

**巧妙化・高度化するマルウェアの脅威を
ゲートウェイで防御**

課題 対策 日々巧妙化・高度化するウイルスやスパイウェアなどの外的脅威により、企業における機密情報漏えいや金銭的被害などが広がっています。ゲートウェイ側でウイルス・スパイウェア対策を行うことでこれらの脅威の侵入を水際で防ぎ、安全なWebやメールの利用ができます。

取扱製品 ESET Mail Security for Linux・ESET Web Security for Linux（開発元 ESET, spol. s r.o.）

メール無害化／スパムメール対策

**メール無害化、誤送信対策、
スパム・ウイルス対策を一台で実現**

課題 対策 スパムメールは受信者側の生産性低下を招くだけでなく、深刻な二次被害をもたらす要因です。スパムメール対策は生産性低下や被害対策から派生するコストを削減するための必須要件となっています。

取扱製品 SPAMSNIPER AG（開発元 Jiransoft）

Web 情報漏えい対策／不正サイト閲覧制御

**Web経由の情報漏えい対策には
Webアクセスの監視が効果的**

課題 対策 Web サイトへの書き込みによる企業情報の漏えいが増加しています。Web 経由の情報漏えい対策にはWebアクセスの監視が重要です。業務に不要なサイトへのアクセスは禁止しつつ、外部への書き込みやアップロードなどをすべて記録し、保存することによってWeb の利用状況を把握できます。

取扱製品 GUADIANWALL Web ファミリー（開発元 キヤノン IT ソリューションズ）

Web サーバー脆弱性対策

Web サイトの脆弱性を狙った情報流出や改ざんを防ぐ

課題 対策 Web サイトの脆弱性を狙った攻撃によって、改ざんや情報流出、Web サービスのダウンなどのリスクが高まっています。こうした攻撃を防ぐには、Web アプリケーションファイアウォールによる対策が有効です。

取扱製品 SiteGuard（開発元 株式会社ジェイピー・セキュア）

エンドポイントセキュリティ

クライアントセキュリティ管理

クライアントPCの一元管理やセキュリティ管理を実現

課題 情報資産ごとに脅威と脆弱性を洗い出して、発生するリスクを特定することが必要です。そして、守るべき情報資産に対するリスクの影響度に応じてセキュリティ対策を実施します。

対策 PCやソフトウェアなどのIT資産情報を一元管理することができます。IT資産台帳をもとに資産状況を可視化し、状況に応じてセキュリティパッチの適用が行えます。ソフトウェアは、PC情報とライセンスの保有情報を照合してライセンス管理が可能となります。

取扱製品 SKYSEA Client View（開発元 Sky株式会社）QND Standard・QND Advance・ISM CloudOne（開発元 クオリティソフト株式会社）

マルウェア対策（エンドポイント）

「検知率」と「軽快な動作」がセキュリティ対策の決め手

課題 企業の機密情報やインターネットバンキングのID、パスワードの取得を狙った攻撃など、日々新種や亜種のウイルスが発生し、攻撃の巧妙化も進んでいます。このような外的脅威からの防御は経営課題の1つとなっています。また一方で、ウイルス対策ソフトによるウイルススキャンは、端末の動作に影響を与え、業務に支障が生じる原因となっています。個々の企業のインフラ環境や運用形態に応じて柔軟に導入できることも、ウイルス対策ソフトを選ぶ上で重要なポイントです。

対策 ウイルス定義データベースによる検出だけでなく、新種や亜種のウイルス検出にも対応したテクノロジーを搭載し、端末の軽快な動作を実現する低負荷設計のウイルス対策ソフトを導入する必要があります。また、レガシーOSを含むさまざまな種類のOSの端末を一元管理できるクライアント管理ツールを利用することで、効率的な管理を実現し、運用負荷を軽減することができます。このような、たくさんの利点を持つ製品を利用することで、コストメリットを活かしたウイルス対策が実現できます。

取扱製品 ESET Endpoint Protection Advanced・ESET Endpoint Protection Standard（開発元 ESET, spol. s r.o.）

不正端末接続防止

社内ネットワークに不正接続した端末を検知・遮断

課題 スマートフォンやタブレットなど、ネットワークに接続されるデバイスの種類や数は年々増加しています。社員や来訪者が持ち込む私物デバイスが社内ネットワークに接続される危険性（いわゆるシャドーIT）も増加しています。その結果、ネットワークへの接続が許可されていないデバイスが発端となる情報漏えいやウイルス感染などのリスクが高まってきています。

対策 社内ネットワークへの不正接続を防ぐには、社内ネットワークに接続されているIT機器の台帳情報を収集する必要があります。その上で、ネットワークへの接続が許可されていない端末の不正接続を防止します。社内ネットワークに不正に持ち込まれた私有PC、タブレット、スマートフォンなどの端末を、アプライアンス装置が検知・遮断します。

取扱製品 NetSkateKoban・NetSkateKoban Nano（開発元 株式会社サイバー・ソリューションズ）

データ暗号化

さまざまなデータを暗号化して、機密情報の漏えいを防止

課題 社外でも業務に利用するモバイルPCでは、盗難や紛失による情報流出のリスクがあります。
また、社外とのデータのやり取りをインターネットなどのネットワークを介した通信で行うことが主流の現在、情報漏えい、搾取、誤送信などのリスクが潜んでいます。サイバー攻撃も高度化かつ巧妙化しており、外的脅威の侵入により、データを外部へ持ち出されてしまう危険性が考えられます。

対策 持ち出しPCの盗難や紛失における情報漏えい対策には、悪意のある第三者による、モバイルPCの不正ログインを防ぐためのOS起動前認証と、ハードディスク全体の暗号化が必要です。また、社外へ送信するデータの漏えいを防ぐためには、ファイルやメールなどの暗号化が有効です。データ暗号化により、万が一、情報が外部に漏れた場合でも、中身を見られる心配がありません。

取扱製品 ESET DESlock Plus Pro（開発元 ESET, spol. s r.o）／Vormetric Data Security Platform（開発元 Thales e-Security, Inc.）

プリンティングセキュリティ

認証・ログ管理

課題 ドキュメントのセキュリティレベルを向上させるために、複合機やプリンターの利用者や利用履歴を記録・管理したい。

対策 社員カードなどのICカードを利用して、オフィス向け複合機「imageRUNNER ADVANCE」や、オフィス向けレーザービームプリンター「Satera」利用時の個人認証を行います。また利用履歴の管理により、いつ・誰が・どんなドキュメントを出力したのか、どこへファクス送信したのかなどを確認することができます。企業内部からの情報漏えいに対する抑止効果を発揮します。

取扱製品 ICカード認証 for MEAP ADVANCE（開発元 キヤノンマーケティングジャパン）／
imageWARE Accounting Manager for MEAP ADVANCE（開発元 キヤノン）

プリント管理

課題 重要な機密文書を、他人に見られることなくプリントしたい。またプリンターに出力されたまま放置されるドキュメントに対し、セキュリティの対策を講じたい。

対策 ICカード認証と連携するサーバーレス Anyplace Print for MEAP ADVANCEを導入することで、重要な機密文書をどの複合機・プリンターからもセキュアに印刷が可能となります。また放置されていた無駄なプリントジョブは、自動的にデータが削除され印刷されません。セキュリティを強化しながら、不要なプリントコストを削減します。

取扱製品 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）

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・防御など、複数のセキュリティ機能を統合的に管理します。

「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）などの通信の特徴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。

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。

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レベルの国内最高水準の建築・設備で、高い堅牢性のビルファシリティ、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、お客さまの次世代IT基盤として活用できます。

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 先進のファシリティ

- 高集積／高密度な機器の設置が可能（床耐荷重 1.5t/m^2）
- １フロア最大800ラック、大規模から小規模まで最適なフロアレイアウトが可能
- 免震ゴム、縦揺れ制震ダンパーなどを備え、お客さまのシステムを保護
- 災害や障害を見越し、電力／通信回線の引き込み２系統化や自家発電用燃料の供給を最優先で受けられる調達体制を確立

西東京データセンターの特長

- 都心から20km圏内、１時間以内でアクセス可能
- 「ティア４レベル」の国内最高水準の建築・設備
- 環境に考慮したPUE=1.4の設備設計
- ７段階の厳密にして堅牢なセキュリティ

評価項目	地震リスクに対する安全性	UPS設備の冗長性	自家発電設備の冗長性	自家発電設備のオイル確保量	熱源機器・空調機器の冗長性	空調用補給水の備蓄量
西東京DC	PML※ 4%	N+1or2	N+1	72時間	熱源機器 2N 空調機器 N+2	72時間

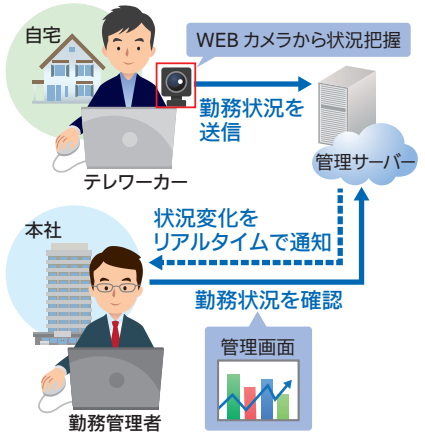
※日本データセンター協会（JDCC）の「データセンターファシリティスタンダード」に準拠

テレワーク支援サービス　「テレワークサポーター」

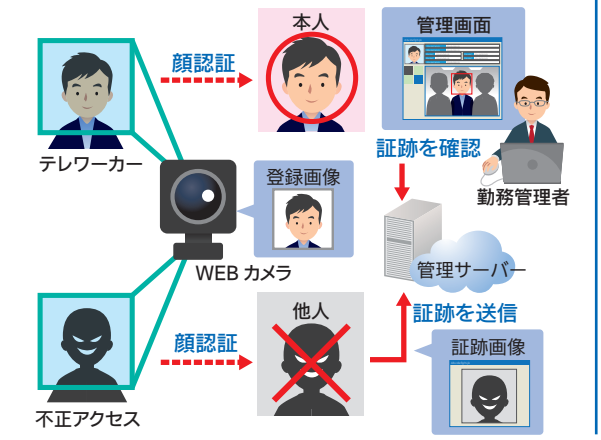
働き方の多様化やワークライフバランスの向上はすべての企業が取り組むべき社会課題です。テレワークサポーターは、情報セキュリティリスクに配慮したテレワーク導入・運用を、キヤノンの顔認証技術を使ったクラウドサービスにより支援します。

勤務の見える化	カメラ映像から社員ごとの在席・離席を自動判断し、勤務状況を集計しますので、 勤務詳細報告書作成の負荷が軽減されます。また、勤務状況の共有やタスク管理にも反映します。
セキュリティ事故防止	「のぞき込み」や「なりすまし」を検知すると画面をオフし、情報流出を防止します。 不正利用はインシデント情報としてその状況画像を記録します。
勤務計画と実績の集計	勤務計画登録の他、集計された勤務実績やインシデント情報を監査・分析することで、 業務改善や問題解決に活用できます。

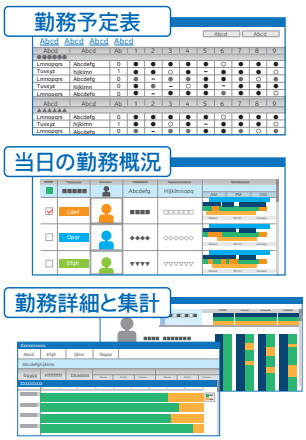
❶ システム構成



❷ 顔認証技術を用いた検出

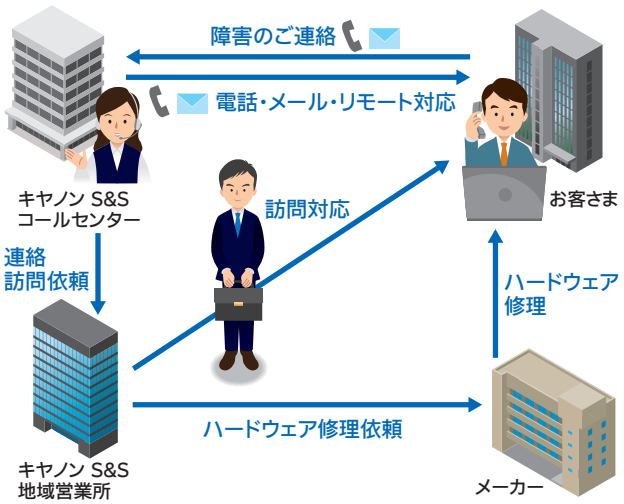


❸ 管理者を支援する各種画面



お客さまの不安を解決するIT保守サービス

キヤノンS&Sではネットワーク/PC/サーバーなどの障害に対して、「IT管理者がいない」「管理者が対応しきれないので、部分的に手伝ってほしい…」などお客さまのお困りごとをスピーディーに解決するために、ネットワークの障害切り分けからシステムリカバリを含むフルサービスまで、お客さまのニーズに合わせたIT保守サービスメニューをご提供しています。



【万全なサポート体制】

- 経験豊かなコールセンター：OSから機器のトラブルまでワンストップで受付・障害復旧支援および訪問手配を行います。
- リモートサポート支援：コールセンターへのお問い合せの際、担当者が必要と判断した場合、インターネット経由でお客さまのPC画面を確認しながら、ご説明いたします。
  また、定期的なサーバーの点検、障害の監視・通知も可能なメニューもご用意しております。
- 全国約180拠点のネットワーク：
  お客さまの最寄の拠点よりオンサイトにて障害復旧を行います。

Action2017 2017年の取り組み

「情報セキュリティ対策セミナー」を227回開催

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2017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227回開催しました。

講師からは巧妙化するサイバー攻撃について具体的な攻撃手法の解説と多層防御の必要性を説明しました。また未知の脅威も含めたサイバー攻撃への対策として、各種ソリューションを組み合せた「次世代セキュリティソリューション」をご紹介しました。

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開始されたお客さまも多くいらっしゃいました。

キヤノンS&Sがフォーティネット社の技術者認定プログラム「NSE4」※の認定者数国内第1位へ

キヤノンS&Sでは、お客さまに安心して導入をお任せいただけるよう、フォーティネット社の技術者認定プログラム「NSE4」の取得を積極的に行い、認定者数が50名を超え、国内第1位のベンダーとなりました。

キヤノンS&Sでは、数多くのお客さまとのかかわりや長年にわたり培ってきた経験やノウハウをもとに、お客さまの抱える潜在的な課題を見える化し、お客さまに最適なセキュリティソリューションを提案しています。

IT専任者が不在の企業における情報セキュリティ対策という社会課題の解決に貢献し、お客さまに安心してネットワーク環境をご利用いただけるよう、導入から運用までトータルなサポートを提供しています。

※NSE(Network Security Expert)は、フォーティネット製品を最大限に活用するためのトレーニングプログラムです。

フォーティネット社製品販売実績および認定状況

■ キヤノンMJグループは、FortiGateの販売・構築台数実績において11年連続国内第1位（2007年～2017年）

キヤノンITソリューションズが日経BP社の「日経コンピュータ 顧客満足度調査 2017-2018」セキュリティ対策製品部門で5年連続第1位を獲得

キヤノンITソリューションズ株式会社は、日経BP社が発行した日経コンピュータ（2017年9月14日号）にて発表された「日経コンピュータ 顧客満足度調査※ 2017-2018」のセキュリティ対策製品部門で5年連続第1位を獲得しました。

あわせて、同社が発行した「日経コンピュータ パートナー満足度調査 2018（2018年2月15日号）」と「日経BP自治体ITシステム満足度調査 2017-2018（日経BPガバメントテクノロジー 2017年秋号）」のセキュリティ対策製品においても満足度 第1位を獲得しました。

※ 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、ITベンダーが提供するシステム開発・運用サービスや、サーバーや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。

Action2017 2017年の取り組み

「お客さま課題解決への貢献」2017年の施策と成果

キヤノンMJグループでは、情報セキュリティの主要注力テーマ「お客さまの情報セキュリティ課題解決への貢献」を掲げ、具体的な施策を計画し、取り組んでいます。

2017年度の施策と成果は、下記の通りとなりました。

2017年		実施会社
施策	実績	
中小企業向けＩＴソリューションの拡大	● 販売実績　（2017年12月末現在） ・キヤノン S&S：FortiGate シリーズ累計販売台数　57,034台 ・IT保守（ファイアウォール製品メンテナンスサービス） 契約件数　19,006契約　19,656台 ● 新たにリリースしたソリューション ・中小オフィス向けIT支援サービス「ＨＯＭＥ　ネットワークセキュリティサービス type-U2 サイバー保険付き 5年パック /type-U2 サイバー保険付き Pro 5年パック」をサイバー攻撃に備える保険を付加したサービスとして新規リリース、リニューアルした「HOME type-AP」、その他各種オプションをリリース	キヤノンMJ/キヤノンS&S
セキュリティを担保する安心安全な社会を実現し、映像ソリューションを活用した新たな価値の提供	● 新たにリリースしたソリューション ・夜間撮影、屋外規格対応の親水コーティングネットワークカメラ3機種 ・最新機能を搭載したネットワークカメラ11機種 ・映像から人物の年齢層・性別を推定するソフトウェア「Profile Analyzer」と、人数をカウントするソフトウェア「People Counter」のラインアップ拡充 ・録画映像確認の効率化を実現する BriefCam 社の映像解析ソフトウェア ・クラウド型新録画サービス「VisualStage Type-S」	キヤノンMJグループ
高度なセキュリティを保ち、環境に配慮したデータセンタービジネスの拡大	● エネルギー（電力）管理状況（PUE=1.4（設計値）のDC設備による省電力化） ● 総量削減義務を果たすため、使用量を把握、分析し、対策を検討 ● セキュリティ事故発生状況 ⇒重大なセキュリティ事故なし	キヤノンITS
ICT活用におけるビジネス脅威対策に貢献するセキュリティソリューションビジネスの拡大	● 販売実績 ・「GUARDIANWALL シリーズ」は、16年連続国内シェア No.1※ ※ 株式会社富士キメラ総研「2017 ネットワークセキュリティビジネス調査総覧」より ・ESET セキュリティ ソフトウェアシリーズ 法人向け販売実績（累計）367,000社（2,284万ライセンス）（2017年12月31日現在） ● 新たにリリースしたソリューション（ニュースリリース順） ・メール無害化・スパムメール対策製品「SPAMSNIPER AG」国内独占販売開始（2月） ・複合機と文書管理システムをシームレスに連携、効率的かつセキュアな文書管理を実現する「GlobalDoc 5 MFP 連携オプション」を提供開始（2月） ・標的型攻撃対策機能を強化した Web フィルタリングソフト「GUARDIANWALL WebFilter」提供開始（5月） ・よりセキュアな暗号化通信方法を採用した端末エミュレーター「TCPLink Enterprise Server」新バージョン販売開始（8月） ・「GUARDIANWALL Mail ファミリー」クラウド型メールとの連携機能を強化した新バージョン提供開始（9月） ・「GUARDIANWALL WebFilter」バージョンアップ、外部攻撃対策機能を強化しより安全な Web 通信を実現（10月） ・西東京データセンターで M&O 認証を取得、グローバル基準を満たす運営品質を実現（11月） ・「ESET セキュリティ ソフトウェア シリーズ」新ラインアップ「まるごと安心パック」提供開始、周辺環境も含めて包括的なサポートを提供（12月）	キヤノンITS

製品への情報セキュリティ品質の組み込み

**製品やサービスに高い情報セキュリティ品質を組み込んで、
お客さまの安心安全への期待や要請に応えます。**

ネットワークに接続される機器のセキュリティについて

複合機をはじめ多くの情報機器がネットワークに接続されており、不正アクセスなどネットワークからの脅威の存在が懸念されています。情報機器全般を安心してお使いいただくためには、適切なネットワーク環境の構築と設定が必要です。キヤノンでは、ホームページで製品別に不正アクセス防止対策をご案内するとともに、設定のサポートなどを行っています。

● 機器を取り巻くセキュリティリスク

オフィス向け複合機「imageRUNNER ADVANCE」および レーザービームプリンター「Satera」における共通のセキュリティ対策

キヤノン製のオフィス向け複合機および、レーザービームプリンターでは、機密情報の不正利用、誤操作、盗難などのリスクに対するお客さまの要請に応えるべく、さまざまなセキュリティ技術を組み込んでいます。

複合機の最新機種「imageRUNNER ADVANCE」および、レーザービームプリンター「Satera」のラインアップに搭載されている機能の一部をご紹介します。

ICカードを使った認証印刷

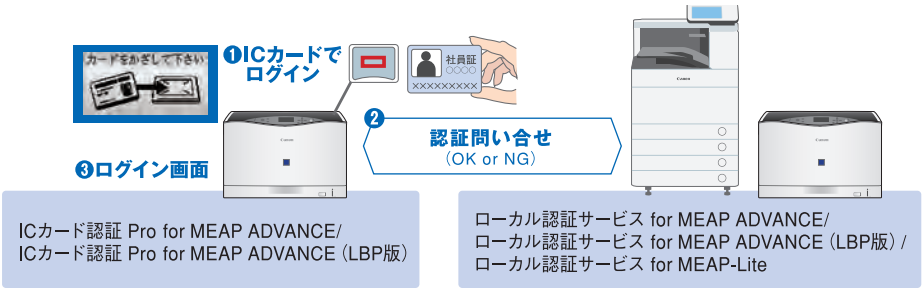
社員証などのＩＣカードを利用し、複合機・プリンターの個人認証が行えるシステムです。また個人認証と連携し、自分の印刷物を、どの複合機・プリンターからもセキュアに印刷できるプリント環境のご提供も可能です。

● ICカードによる認証印刷

Step 1
ICカードリーダーライタに
ICカードをかざす

Step 2
ローカル認証サービスから
OK/NGが返ってくる

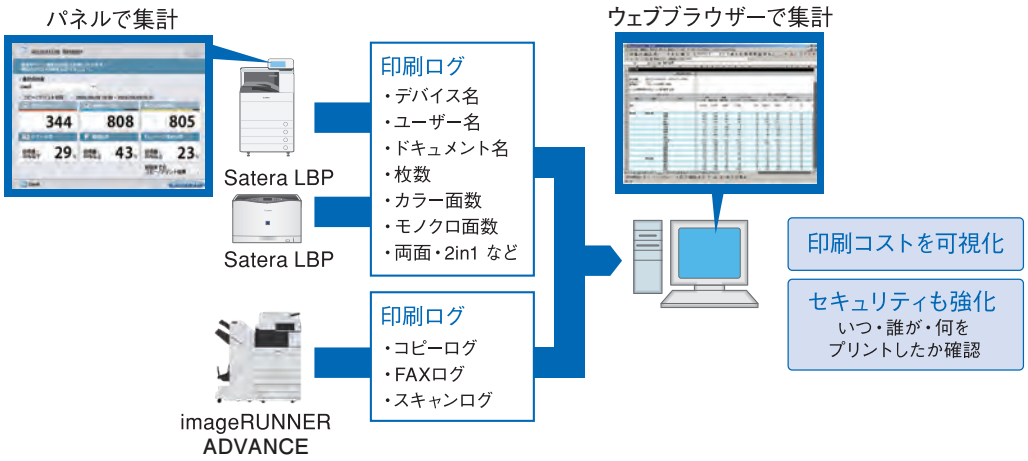
Step 3
ログイン許可（または非許可）



出力ログを収集してプリント情報の集計・管理

ネットワーク接続された複数の複合機・プリンターの出力状況について、集計やログ管理を行います。部門ごとの利用実績の集計や、誰が、いつ、どのファイルを印刷したかなど、利用状況の詳細を正確に確認できます。プリンター管理を効率的にサポートします。

● プリント情報の集計・管理イメージ



「imageRUNNER ADVANCE」におけるセキュリティ対策

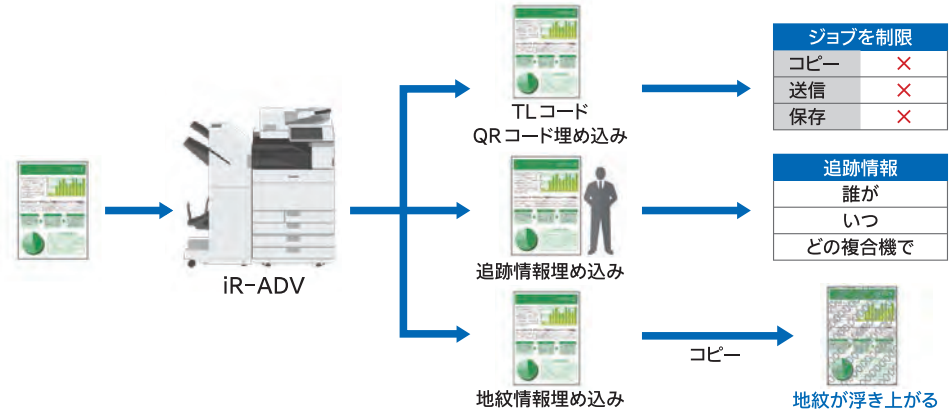
セキュリティ認証「IEEE2600」に準拠

各種オプションの装着による適切な構成や設定を行うことで、複合機・プリンターの情報セキュリティに関する国際的な規格IEEE Std 2600.1TM-2009やIEEE Std 2600.2TM-2009（以下、IEEE 2600）に準拠しており、IEEE 2600で定められたセキュリティを実現することができます。

複合機から紙出力した機密情報の漏えい対策

コピーやプリントをする際、背景に隠れた情報（TLコード）やQRコードを埋め込み、文書の複製を禁止するなどジョブを制限。「誰が・いつ・どの複合機で」複製したのかを追跡するためのユーザー名・日付・デバイス名などの埋め込みや、コピーすると浮き上がる地紋情報の埋め込みも可能です。不正なコピーやファクス、スキャンを抑止することができます。

● 背景に情報を埋め込み不正利用を抑制する。「ジョブロック」※

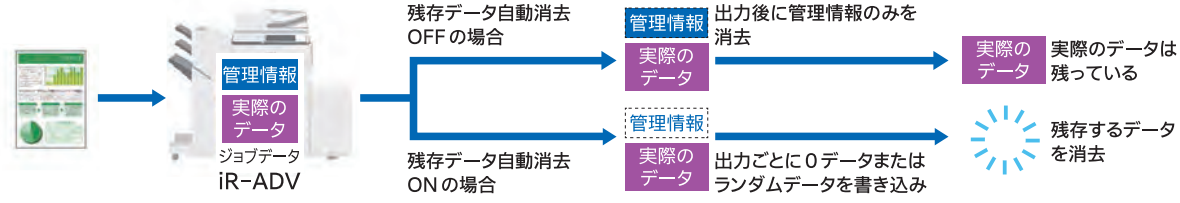


※ オプションが必要です。

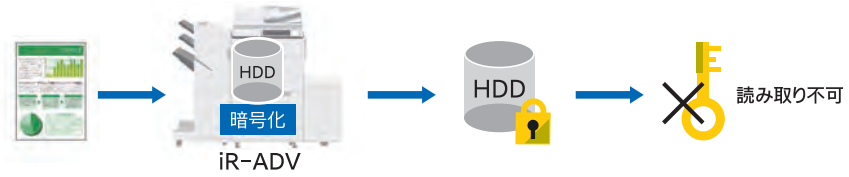
複合機に保存されている機密情報の漏えい対策

コピーやプリントの際にHDD内に生成されるデジタルデータを、ジョブ終了と同時に上書き消去する「残存データ自動消去」。HDD内のデータを暗号化する「HDDデータ暗号化」は、万一の盗難などによる情報漏えいリスクを低減します。マイナンバーなど重要な個人情報を取り扱う業務をサポートします。

● 残存データ自動消去



● HDDデータ暗号化



オフィス向けレーザービームプリンター「Satera」におけるセキュリティ対策

暗号化でセキュアなデータ通信を実現

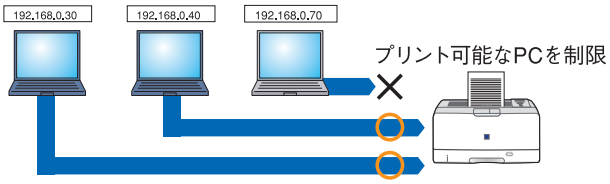
パソコンとプリンター間の通信データを暗号化して、情報漏えいを抑制するSSL通信に対応しており、データの盗み見や改ざんを防ぎます。

● SSL通信概念図

印刷できるパソコンを制限

プリンター接続の許可・拒否について、IPアドレスとMACアドレスで制限することができます。特定のユーザーだけが印刷できるセキュアな環境構築をサポートします。

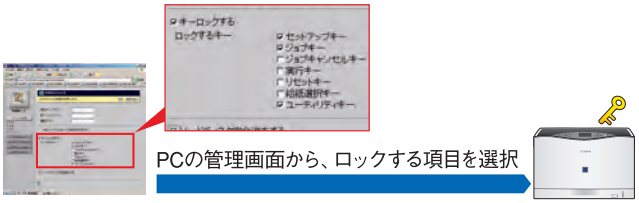
● アドレス制限概念図



プリンターに鍵をかけ、設定変更を防止

本体の操作パネルをロックして、ユーザーによる設定変更を防止できます。ロックするキーは「リモートUI」から容易に選択可能です。

● 「リモートUI」による設定画面イメージ



ネットワークカメラ「VBシリーズ」におけるセキュリティ対策

キヤノン製ネットワークカメラ「VBシリーズ」では、以下の対策により、外部ネットワークからの不正アクセスを防止します。

ネットワークカメラへのアクセスをパスワードで管理

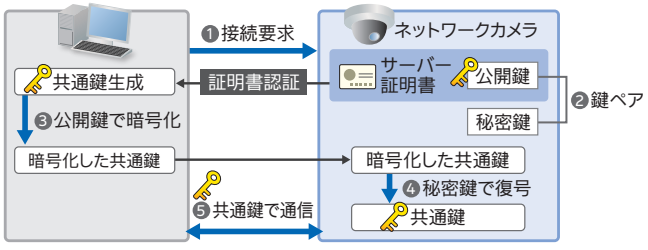
キヤノンのネットワークカメラには、「管理者」「登録ユーザー」「一般ユーザー」の3種類のユーザー権限があり、「管理者」と「登録ユーザー」のアカウントは、パスワードで保護されます。パスワードを必要としない「一般ユーザー」の権限を無効にすることで、それらの一般ユーザーのネットワークカメラへのアクセスを禁止することができます。

● アクセス権限の設定画面イメージ

SSL暗号化通信を設定

ユーザーがブラウザーを通じてキヤノンのネットワークカメラにアクセスする際に、ネットワークカメラにサーバー証明書を導入することで、SSLによる安全な暗号化通信を実現します。

● SSL通信の仕組み



キヤノンマーケティングジャパングループ概要

会社概要 （2018年4月1日現在）

キヤノンマーケティングジャパン株式会社
Canon Marketing Japan Inc.
設立：1968年2月
資本金：73,303百万円
従業員：連結：17,661名 単独：5,461名
本社：東京都港区港南2-16-6
上場取引所：東京証券取引所第一部（証券コード：8060）
事業：キヤノン製品ならびに関連ソリューションの国内マーケティング

グループ会社一覧 （2018年4月1日現在）

エンタープライズビジネスユニット
- 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
  - Canon Software America, Inc.
  - 佳能信息系統（上海）有限公司
  - Canon IT Solutions (Thailand) Co., Ltd.
    - Material Automation (Thailand) Co., Ltd.
      - ASAHI-M.A.T. Co., Ltd.
      - MAT Vietnam Company Limited
- 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

エリアビジネスユニット
- 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

プロフェッショナルビジネスユニット
【プロダクションプリンティング】
- 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
  - コマーシャルプリンティングラボ株式会社

【ヘルスケア】
- キヤノンライフケアソリューションズ株式会社
  - 株式会社エルクエスト
  - キヤノンITSメディカル株式会社

サービス＆サポート
- キヤノンカスタマーサポート株式会社

グループシェアードサービス※
- キヤノンビジネスサポート株式会社

※ グループシェアードサービス：同一グループ内の複数の組織で実施されている共通業務を集中化して、サービスの向上とコスト削減を図る仕組み

事業内容

私たちはイメージングとITの力で
お客さまに最適なソリューションを創造します。

きめ細かなサービスと多彩な製品を自在に組み合せることで、「安心・安全」「映像」「オフィス」「商業印刷」「ものづくり」「金融」「医療」「教育」「流通・サービス」「パーソナル」といったさまざまな現場を支えるソリューションを提供していきます。

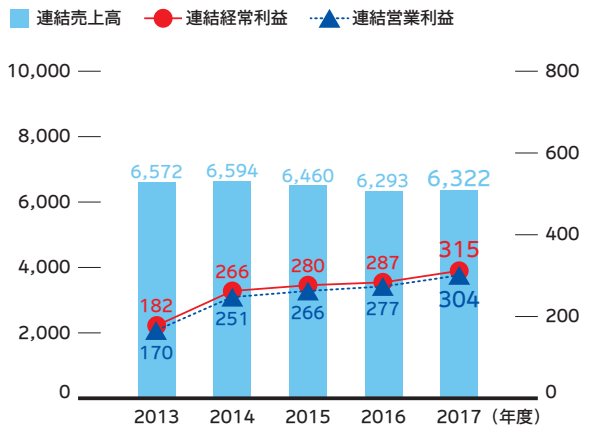
長期経営構想フェーズⅢ （2016～2020）

グループミッション
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

グループビジョン
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

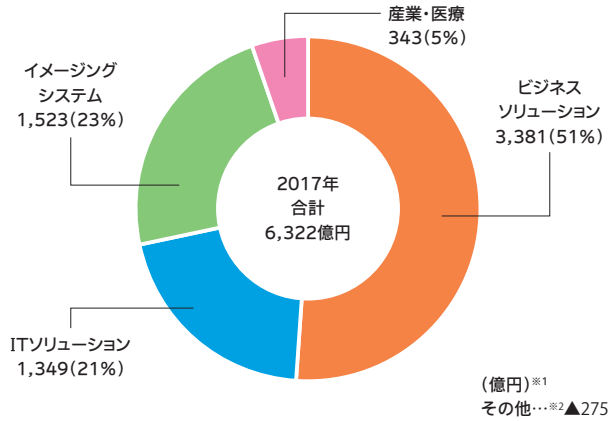
経営データ（連結）

● キヤノンマーケティングジャパングループ
連結売上高／連結営業利益／連結経常利益（億円）



※ 販売費に計上していた費用の一部を、2013年度より、売上高から控除する方法に変更しました。

● キヤノンマーケティングジャパングループ
連結部門別売上高構成（億円）



※1 各事業の連結売上高を合計した数字は、セグメント情報における「その他」の金額が含まれないため、円グラフ中央の合計額と異なります。なお、構成比率は、それぞれの単純合計額を基に算出しています。
※2「その他」には、セグメント間内部売上高や、シェアードサービスなどが含まれています。
※ 2017年度にセグメント間の事業移管を実施致しましたが、上記の実績はセグメント間の組み替え前の数値となっております。

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、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　2016年6月30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

キヤノンマーケティングジャパン株式会社（以下「当社」）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。

当社は、個人情報をこの事業活動に欠かすことの出来ない重要な情報資産として認識し、社会的責務の一つとして以下の方針に基づき、ご本人のプライバシー尊重のために個人情報の保護に一層努めます。

方針

1. 個人情報保護に関する法令およびその他の規範遵守

当社は、日本国の個人情報の保護に関する法律、行政手続における特定の個人を識別するための番号の利用等に関する法律、これらの法律に関する関係官庁の発行するガイドライン、国が定める指針および、個人情報保護マネジメントシステムを確立する為のその他の規範を遵守します。

2. 個人情報保護マネジメントシステムの確立

当社は、キヤノン製品ならびに関連ソリューションの国内マーケティング活動において、利用目的を特定した上で個人情報を取得し、その利用目的の範囲内で利用するとともに、適切な委託、提供、廃棄等の取り扱いを行うために個人情報保護マネジメントシステムを確立します。

3. 個人情報保護マネジメントシステムの実施と継続的改善

当社は、本方針を始めとした個人情報保護マネジメントシステムを全ての従業者に周知します。 当社は、個人情報保護マネジメントシステムを実施し、監査し、継続的に改善します。

4. 個人情報の正確性・安全性の確保

当社は、個人情報の正確性および安全性を確保するため、取扱う個人情報のリスクに応じ、物理的セキュリティ、情報通信技術的セキュリティ、管理的セキュリティ、人的セキュリティの側面から合理的な安全対策を講じて、個人情報への不正アクセス、個人情報の紛失、破壊、改ざん、漏洩等の防止および是正に努めます。

5. 苦情および相談への対応

当社は、個人情報の取り扱いおよび個人情報保護マネジメントシステムに関して、苦情や相談およびご本人からの個人情報の利用目的の通知、開示、訂正、追加または削除、利用または提供の拒否に関する依頼を受け付けて、適切、かつ、迅速な対応を行います。

制定日　2002年4月1日
改定日　2016年6月30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

※ グループ各社は同様の方針を制定しています。

ウェブサイト

http://cweb.canon.jp/csr/security/index.html

■対象期間

本報告書は主に2017年（2017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

■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　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

TEL：03-6719-9032　FAX：03-6719-8360

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

2018年6月発行