Canon

Information Security Report 2014

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 2014

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2013年に取り組んだスパイラルアップポイントを、Action2013としてわかりやすく掲載することに留意しました。

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2013年（2013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記載しています。

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
総務・CSR本部　情報セキュリティ企画推進グループ
〒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」は、略称として「キヤノンMJ」と表記する場合があります。

CONTENTS

キヤノンマーケティングジャパングループにおける情報セキュリティの位置付け

安心安全で豊かな“くらし、しごと、社会”の実現を支える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

キヤノンマーケティングジャパングループでは、2011年から2015 年までの「長期経営構想フェーズⅡ」のミッションとして「安心安全で豊かな“くらし、しごと、社会”の実現に向けてマーケティング・イノベーションを行い、最高の価値を提供する」を掲げ、従業員一人ひとりが取り組みを進めています。

「安心・安全」をお客さまに提供していく上で、「情報セキュリティ」は欠くことのできないテーマであり、重要な経営課題の一つととらえています。

近年の情報通信技術の飛躍的な進展により、特にクラウドやソーシャルネットワークサービス等は、私たちの利便性を以前とは比べ物にならないほど高めています。また、「ビッグデータ」等の膨大な情報の活用は、マーケティングに大きな活力を生み出しています。しかしその一方で、この利便性や活力を脅かすサイバー攻撃等の脅威もさらに高度化・複雑化しており、これにしっかりと対応していかなければなりません。

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の「情報セキュリティ基盤の強化」と「お客さまへの価値提供における情報セキュリティ品質の向上」という2つの視点で、情報セキュリティ成熟度の向上に取り組んでいます。

「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、ISMS※1やPMS※2等のマネジメントシステムを組み込み、均質化と効率化をはかるとともに、事業特性に応じた各種情報セキュリティ対策の最適化、人材の育成、情報開示などを推進しています。

主要注力テーマ

1.マネジメントシステムのグループ均質化と効率化
2.グループ共通対策と事業特性に応じた対策の最適化
3.情報セキュリティ人材の育成
4.情報セキュリティ活動の積極的な情報開示
5.お客さまへの安心・安全の提供
- ●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
- ●お客さまの情報セキュリティ課題解決への貢献

「お客さまへの価値提供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・ソフトウェア開発等の業務プロセスごとに、事業部門が主体となって、単に情報漏えい対策等のマイナス側面だけでなく、お客さまの視点に立って情報の取り扱い品質を向上させることでお客さまにご満足いただけるようプラス側面への業務改善活動を行っています。

例えば、モバイル機器と関連アプリケーションを活用したワークスタイルの変革では、営業担当者が外出先でも、あたかも社内にいるように、さまざまな部門と安全かつ迅速に情報交換が可能なシステムの運用を開始し、お客さま対応力の向上を図りました。

こうした活動を通じて「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」というキーコンセプトの具現化に取り組んでいます。

また、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や各種情報セキュリティ製品・ソリューションをお客さまにご提供することで、お客さまの情報セキュリティ課題解決に貢献できるよう努めています。

本報告書は、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対する考え方や実践事例を紹介しています。ご覧いただく皆さまに、少しでもお役に立てば幸いです。

代表取締役社長
川崎 正己

※1　ISMS：情報セキュリティマネジメントシステム
※2　PMS：個人情報保護マネジメントシステム

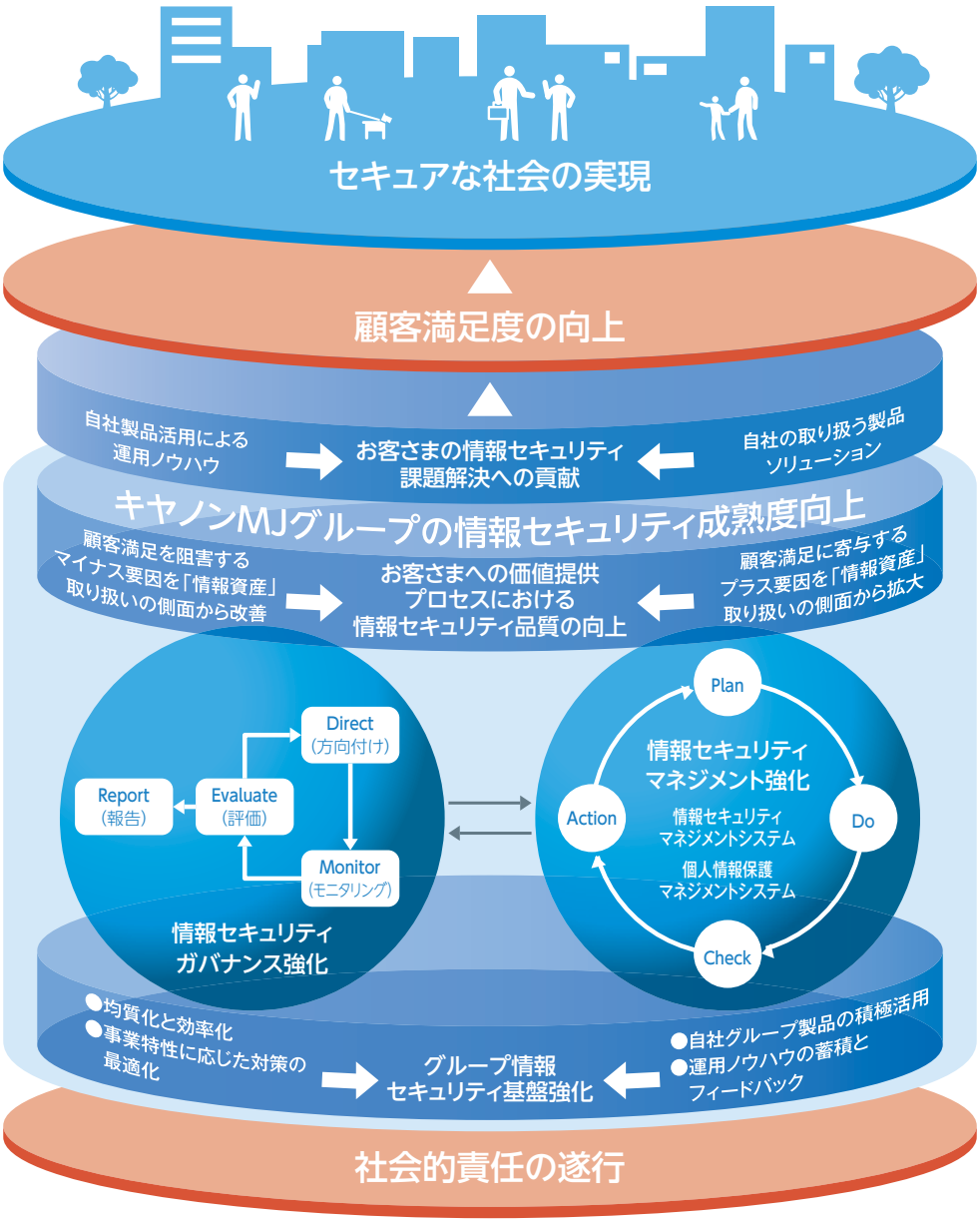
推進フレームワーク

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「社会的責任の遂行」と「顧客満足度の向上」の2つの目的を設定し、その具現化に向け、グループインフラなどをより高いセキュリティレベルにするための「グループ情報セキュリティ基盤強化」と、営業や保守サービス、ソフトウェア開発といった「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」に取り組んでいます。

これらの活動は、経営層による「情報セキュリティガバナンス」に基づき、「情報セキュリティマネジメント」を推進して、その有効性を継続的に改善し、情報セキュリティ成熟度の向上を図っています。

また、この活動では積極的に自社グループが取り扱う製品・ソリューションを活用してその運用ノウハウを蓄積し、それらをお客さまに提供することで「お客さまの情報セキュリティ課題解決への貢献」につなげています。

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

「グループ」「CSR連携」「全員参加」の視点に留意し、グループ情報セキュリティガバナンスと、効果的かつ効率的なマネジメントを継続的に推進しています。

CSR委員会による情報セキュリティガバナンスの推進

キヤノンMJでは、グループの情報セキュリティガバナンス強化をはかるために、キヤノンMJ役員、主要グループ会社社長、社外有識者をメンバーとした「キヤノンMJ CSR委員会」を設置しています。情報セキュリティガバナンスでは、経営戦略やリスク管理の観点から情報セキュリティの「方向付け（Direct）」を行い、活動の状況を「モニタリング（Monitor）」し、「評価（Evaluate）」するサイクルを回しています。また、情報セキュリティ報告書を通じて活動結果を利害関係者などへ「報告（Report）」しています。CSR委員会で情報セキュリティガバナンスを取り扱うことによって、コンプライアンス、環境、労働安全など、CSR関連分野との連携が加速するという効果が上がっています。

効果的かつ効率的なマネジメント体制と運用

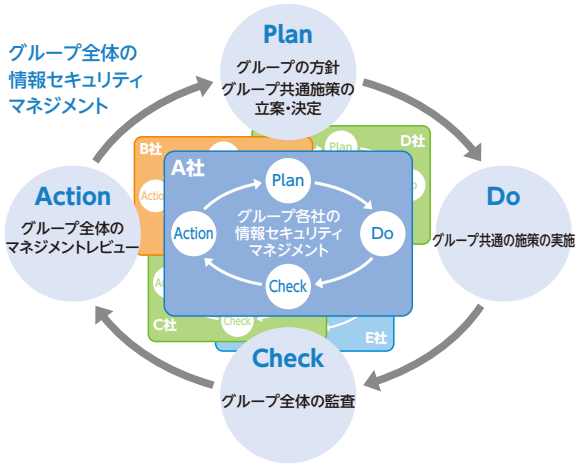
マネジメント体制は、グループ情報セキュリティ統括体制と各社マネジメント体制の2つに分けています。

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。

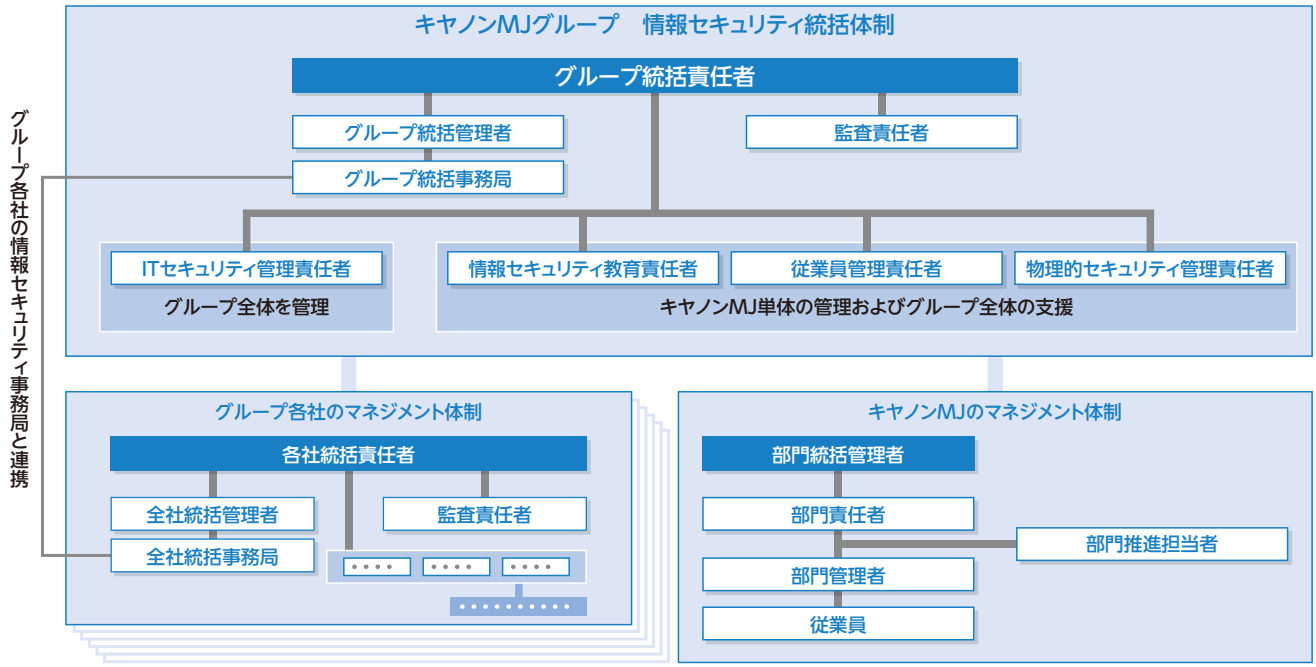
一方、各社マネジメント体制では、それぞれの会社の事業特性に応じて、情報セキュリティ主管部門や部門管理体制を設置し、運用しています。

こういった体制によって、グループ全体のPDCAと各社のPDCAが効果的かつ効率的に回っています。

■キヤノンMJグループ全体のPDCAとグループ各社のPDCA



■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

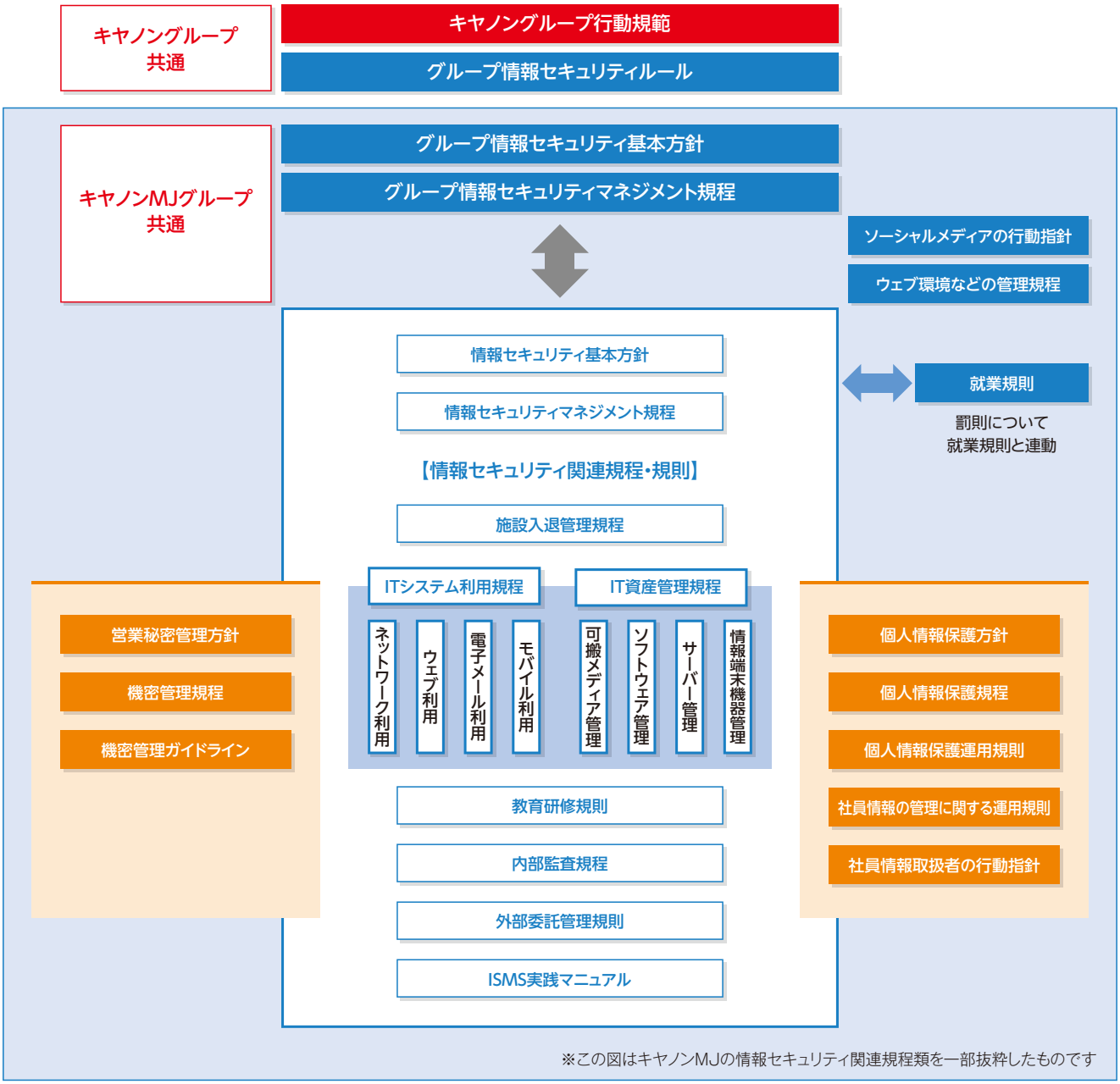


体系的にルールを整備

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。

個人情報と営業秘密については、重要な情報資産であることから、個別の方針・ルールを整備しています。特に個人情報保護については、個人情報保護法よりも一段高いレベルの管理を行うために、JISQ15001：2006に準拠したマネジメントシステムを構築し運用しています。

■情報セキュリティに関するルール体系



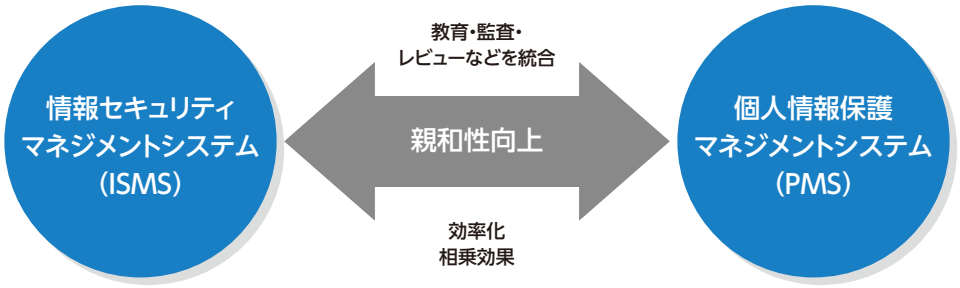
※この図はキヤノンMJの情報セキュリティ関連規程類を一部抜粋したものです

マネジメントシステムの連携による効果的な運用

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（ISMS）と個人情報保護マネジメントシステム（PMS）を両輪として、親和性を向上させ、継続的な運用改善を行っています。具体的には、教育・監査・レビューなどを統合し、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、効率化だけでなく相乗効果も生み出しています。

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）との連携も図っています。

■マネジメントシステムの連携



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、個人情報の委託先における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。また、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。

均質的な情報セキュリティマネジメントを推進しているグループ会社間で業務委託を行う場合であっても、適切な管理・監督を行っています。複合機の保守サービス業務やソフトウェア開発業務などを委託し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。

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。

インシデントの検知と発生時対応

情報セキュリティインシデント（事象・事件・事故）発生時に、適切な対応を迅速に行うため、グループ全体でインシデント管理体制を整備しています。インシデントの検知については、グループITガバナンスの中で、次のような監視を行っています。

- ●電子メールのモニタリング
- ●ウェブ利用状況のモニタリング
- ●ソフトウェアのインベントリー取得
- ●コンピューターウイルスの侵入検知
- ●全社サーバーへの不正アクセス監視
- ●社内ネットワークから外部への不正通信検知
- ●IPアドレスの不正使用監視
- ●モバイル利用状況
- ●パソコンのハードディスク暗号化実施状況

また、従業員にインシデント発生時の報告を義務付けるとともに、報告ルートを整備しています。インシデント発生時には、発生原因を究明し、是正処置・再発防止策（予防処置）を速やかに行います。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っています。

キヤノンMJでは、インシデントの報告と進捗管理をシステム化することで、関係者全員でインシデント対応状況をリアルタイムに情報共有し、迅速で適切なインシデント対応を実現しています。このシステムは順次グループ会社に展開しており、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。

Action 2013 2013年の取り組み

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では、複合機の保守サービス業務を委託しているパートナー企業の情報セキュリティ品質の向上をはかるために、評価基準を設け、基準に達していない企業には改善を指導しています。2013年は約600社1,000拠点に対し、情報セキュリティに関する取り組み状況について、年2回ウェブによるセルフアセスメントおよび実地調査を実施しました。

また、キヤノンITソリューションズ、キヤノンITSメディカル、スーパーストリーム、キヤノンソフトウェアでは、ソフトウェア開発業務を委託している企業の当該業務に新たに従事する方に、情報セキュリティルール徹底のためのウェブ教育を義務付けており、昨年は約1,000名が受講しました。

ウェブ環境の安全性向上に向けたグループガバナンス体制の確立

キヤノンMJグループでは、外部から接続できるウェブ環境(ウェブサイト、デモ用サイト、開発環境等を含む)を取り巻くさまざまなリスクや脅威に備え、「インターネット接続環境管理規程」を制定し、自社開発の管理システムを活用したマネジメントシステムを構築し運用を開始しました。

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。

■情報セキュリティ人材を育成するしくみ

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月次メッセージの中で、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、「設問診断形式」という独自のウェブ教育を毎年行っています。これは、正解・不正解の結果を重視した教育ではなく、設問を読み、複数の選択肢から正答を導き出す過程で、自然と必要な「知識」を習得することができる実践的かつ効果的な教育方法です。

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」をしっかりとも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

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、毎週月曜日に欠かさず全グループの従業員へ「今週のコンプライアンス」というメールマガジンを配信しています。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。

また、イントラネットサイトの「情報セキュリティトレンド」というコンテンツで、情報セキュリティにまつわる世の中の動きを広く従業員に配信しています。

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。

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全従業員へ送信し、実体験を通じた意識啓発を行なっています。実施結果および対処方法については、全従業員が参照可能なイントラネットにて開示し、周知徹底しています。

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、担当業務における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。毎回、情報セキュリティに関連するテーマが数多くの組織で取り上げられています。それにより、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

Action 2013 2013年の取り組み

「コンプライアンス・ミーティング」の実施

2013年上期の「コンプライアンス・ミーティング」では、各職場における実際の業務上のリスクの洗い出しとその対策について、情報管理・情報端末の使い方を含む20のコンプライアンスリスク例を参考にしながら話し合いました。下期では、情報管理（ソーシャルメディア編）・情報紛失・営業秘密・個人情報といった情報関連のテーマを含む13のケース（事例）から1つのケースを選択し、登場人物の問題行動とそれを防止するための対策を話し合いました。

「情報セキュリティトレンド」における情報配信

配信日	配信テーマ
2013年1月	Webメールサービスのアカウントが危ない!
2013年6月	私たちやお客さまに迫りくる脅威! ～2013年版 10大脅威～
2013年7月	「情報セキュリティ報告書2013」の発行

「今週のコンプライアンス」で配信した情報セキュリティ関連テーマ

配信日	配信テーマ
2013年1月	メールソフトの誤操作による情報漏えい事故の防止
2013年2月	セミナー事務局のあなた! ～個人情報の保護は大丈夫ですか?～
2013年3月	PCの社外持ち出し時の情報管理は充分ですか?
2013年5月	機密情報の社外へのメール送信は モニタリングされています! ～機密情報の自宅へのメール送信禁止～
2013年6月	未公表の重要情報の取り扱いに注意してください! ～インサイダー取引を防ぐために～
2013年7月	「機密管理区分」を正しく明示していますか?
2013年10月	「標的型攻撃」の最近の傾向

第三者認証の効果的な活用

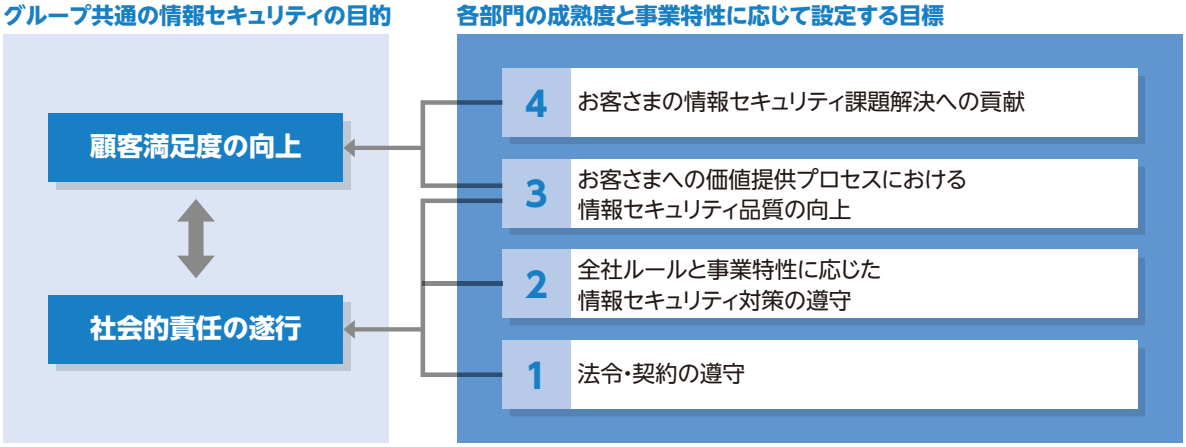
「ISMS適合性評価制度」と「プライバシーマーク」の認証取得、
または認証基準に準拠した運用をグループ全体で行っています

第三者認証の活用目的

キヤノンMJグループでは、ISMSやPMSを、ベストプラクティスであるJIS規格に基づいて構築しています。各部門の目標設定にあたっては、グループ共通の目的である「社会的責任の遂行」と「顧客満足度の向上」を具現化するために、「法令・契約の遵守」「全社ルールと事業特性に応じた情報セキュリティ対策の遵守」「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。そして、事業上の必要性に応じて認証を取得することによって、お客さまに客観的判断基準を提供できると考えています。

■グループ共通の活動目的と部門の目標



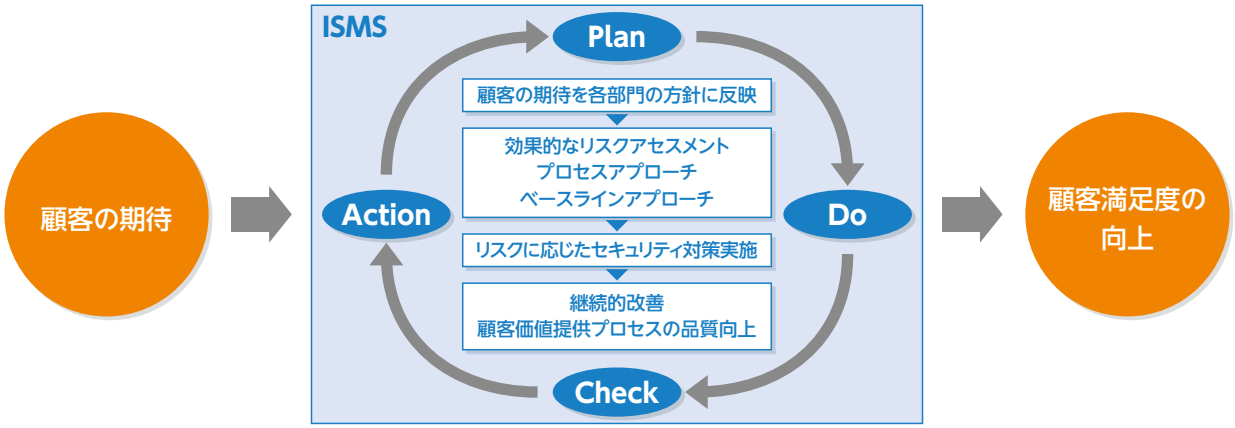
ISMSの推進による「顧客満足度の向上を支える業務改善活動」の具現化

キヤノンMJグループのISMSは、顧客満足度を高めていくための活動として、それぞれの部門が果たす役割に応じた効果的なリスクアセスメント手法を採用して推進しています。

全社の情報セキュリティ基盤強化を担う部門では、JISQ27001の管理策を基とし、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に取り組んでいます。

また、お客さまと直に接するビジネス部門では、お客さまの期待を明確にした上で、それぞれの業務プロセスにおけるリスク対応に留まらず、お客さまによりご満足いただくための業務改善に結び付けています。

■ISMSを活用したPDCAサイクル



■ISMSにおける効果的なリスクアセスメント

プライバシーマークを活用した個人情報保護の強化

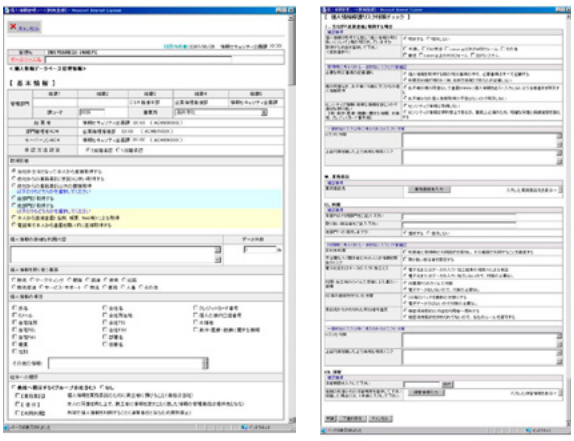
キヤノンMJグループでは、個人情報保護マネジメントを法律より一段高い管理レベルで実現するため、プライバシーマークの要求事項であるJISQ15001に準拠した個人情報保護マネジメントをグループ全体で推進しています。

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。

法律より一段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。



個人情報データベース管理システム

例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。その他、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もっているため、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

■個人情報データベース管理システムによるリスクアセスメント(一部抜粋)

担当者は、システムの画面に沿って個人情報の取り扱い手順を確認します。

取得する手段を選択してください(複数選択可)	□ 手渡し □ FAX受信 ☑ Webフォーム □ 郵送 □ 社内システム □ その他

個人情報取得時の手段にWebフォームを選択すると、それに応じたリスクと確認項目を自動的に表示

お客さまの誤入力	○ メールアドレス等入力ミスを起こす可能性の高い項目は2度入力をお願いし、システムチェックする ○ 受け入れ可能なリスクなため対策しない
本人からインターネット経路上で取得する際の盗聴	□ SSL等の暗号化環境で通信する
Webサイトの脆弱性をついたデータ搾取・盗聴・改ざん	□ Webサイトの脆弱性対策［例：クロスサイトスクリプティング対策等］をする

選択した手順に応じて、動的に法令・規範および社内ルールに応じたリスクと対策項目が生成・表示されますので、担当者はこの内容を確認することで、適切なリスク対策および運用を実施することができます。

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、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等によって、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。

キヤノンMJグループにおける認証取得状況

(2014年4月1日現在)

会社名	ISMS認証※1	Pマーク認証
キヤノンマーケティングジャパン	●	●
キヤノンシステムアンドサポート	●	●
キヤノンプロダクションプリンティングシステムズ※2	●	
キヤノンMJアイティグループホールディングス	●	
キヤノンITソリューションズ	●	●
キヤノンITSメディカル	●	●
キヤノンビズアテンダ	●	●
スーパーストリーム	●	●
ガーデンネットワーク	●	●
クオリサイトテクノロジーズ	●	
Canon Software America		−
佳能信息系統(上海)	●	−
Canon IT Solutions(Thailand)		−
Material Automation(Thailand)		−
ASAHI-M.A.T.		−
MAT Vietnam Company Limited		−
Canon IT Solutions(Philippines)		−
キヤノンソフトウェア	●	●
エディフィストラーニング	●	
キヤノンカスタマーサポート	●	●
キヤノンライフケアソリューションズ	●	●
エルクエスト		
台灣佳能先進科技股份		−
キヤノンビジネスサポート		
オーエーエル	●	

※1 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

imageRUNNER ADVANCEシリーズは、IEEE Std 2600.1TM-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

- imageRUNNER ADVANCE C2230/C2220
- imageRUNNER ADVANCE C5255/C5250/C5240/C5235
- imageRUNNER ADVANCE C7270/C7260
- imageRUNNER ADVANCE C9280 PRO/C9270 PRO
- imageRUNNER ADVANCE 4045/4035/4025
- imageRUNNER ADVANCE 6275/6265/6255
- imageRUNNER ADVANCE 8205 PRO/8295PRO/8285 PRO

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 for MEAP」と「Anyplace Print for MEAP」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」「セキュリティ対策の5S」の徹底・定着を図っています。なかでも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専用の機密書類回収ボックスも設置しています。

このような施策によって、機密情報などの重要書類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

グループ全体のITセキュリティ最適化の実現

販売力およびマーケティング力の強化を実現するIT武装

2011年から2015年までの5カ年計画として策定した新たな成長戦略「長期経営構想フェーズⅡ」のもと、「IT活用による販売力およびマーケティング力の強化」という全社方針を掲げており、この方針に基づき、IT武装による営業部門を中心としたワークスタイル変革を行っています。

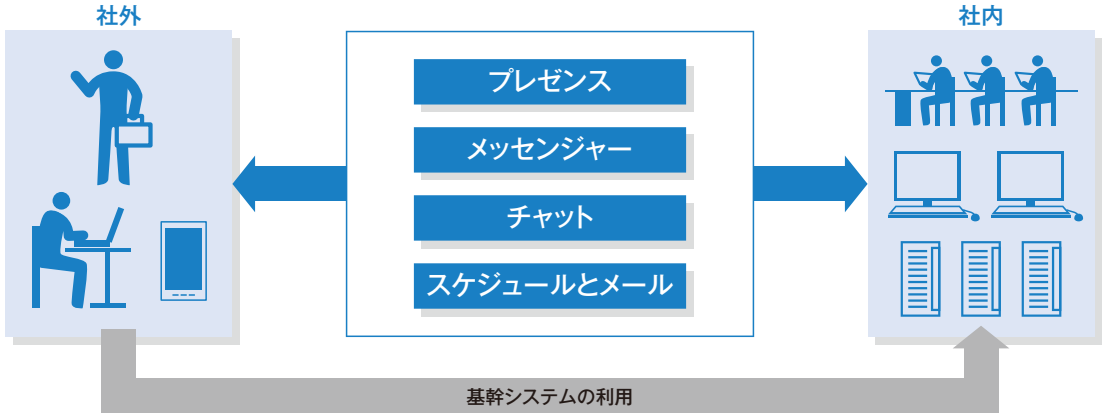
この変革は、営業部門の機動性を上げていくことに重きを置いていますが、機動力を上げても、セキュリティ対策が不十分になってしまっては、競争力を低下させる原因にもなるため、機密性を担保した上で、利便性も十分に考慮したIT武装の実現を行っています。

具体的には、Ultrabookパソコン・iPhone※といったモバイルに適した機器や、データ連携の容易な各種アプリケーションを積極的に導入しました。これによって、会社のパソコンで利用する「基幹システム」「スケジューラー」「電子メール」をiPhone※でも利用可能としました。

また、社内の相手の状態が容易に確認できる「プレゼンス機能」や簡単に声かけができる「メッセンジャー機能」、複数で同時に会話ができる「チャット機能」などにより、営業担当が外出先からでも社内のさまざまなサポート部門の担当者と社内にいるように迅速な情報交換をすることが可能となりました。

このIT武装によって、これまで外出していた際にはできなかったことを実現し、機動力と顧客対応力の向上を図っています。

■ワークスタイル変革の全体像



キヤノンMJグループでの活用事例

キヤノンシステムアンドサポートでの取り組み

キヤノンシステムアンドサポートでは、2009年よりSFA/CRMシステムとしてSalesforceを導入し、営業活動に関するさまざまな情報を社内で共有することでお客さまへの対応力強化に取り組んできました。

それに加えて今回のUltrabookとiPhone※の導入により、従来は社内でしか実施できなかった提案書や見積書の作成等の事務作業を会社に戻らなくても実施できるようになったほか、お客さまの視覚や聴覚に、より直接的に訴求できるプレゼンテーションが可能になりました。また、お客さまからのご要望に対して即座に商品やサービスを検索してご紹介したり、在庫を確認したりすることが可能となっています。このように営業活動のスタイルを変革することで、モバイル導入前と比べてお客さまとのコンタクト件数は約5割アップし、その結果案件増にもつながっています。

また、即答できない質問をお客さまから受けた場合には社内SNSであるSalesforce Chatterに投稿することで、情報をもっている全国の従業員からの回答やアドバイスが得られるため、お客さまへのレスポンス向上にも寄与しています。

※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。

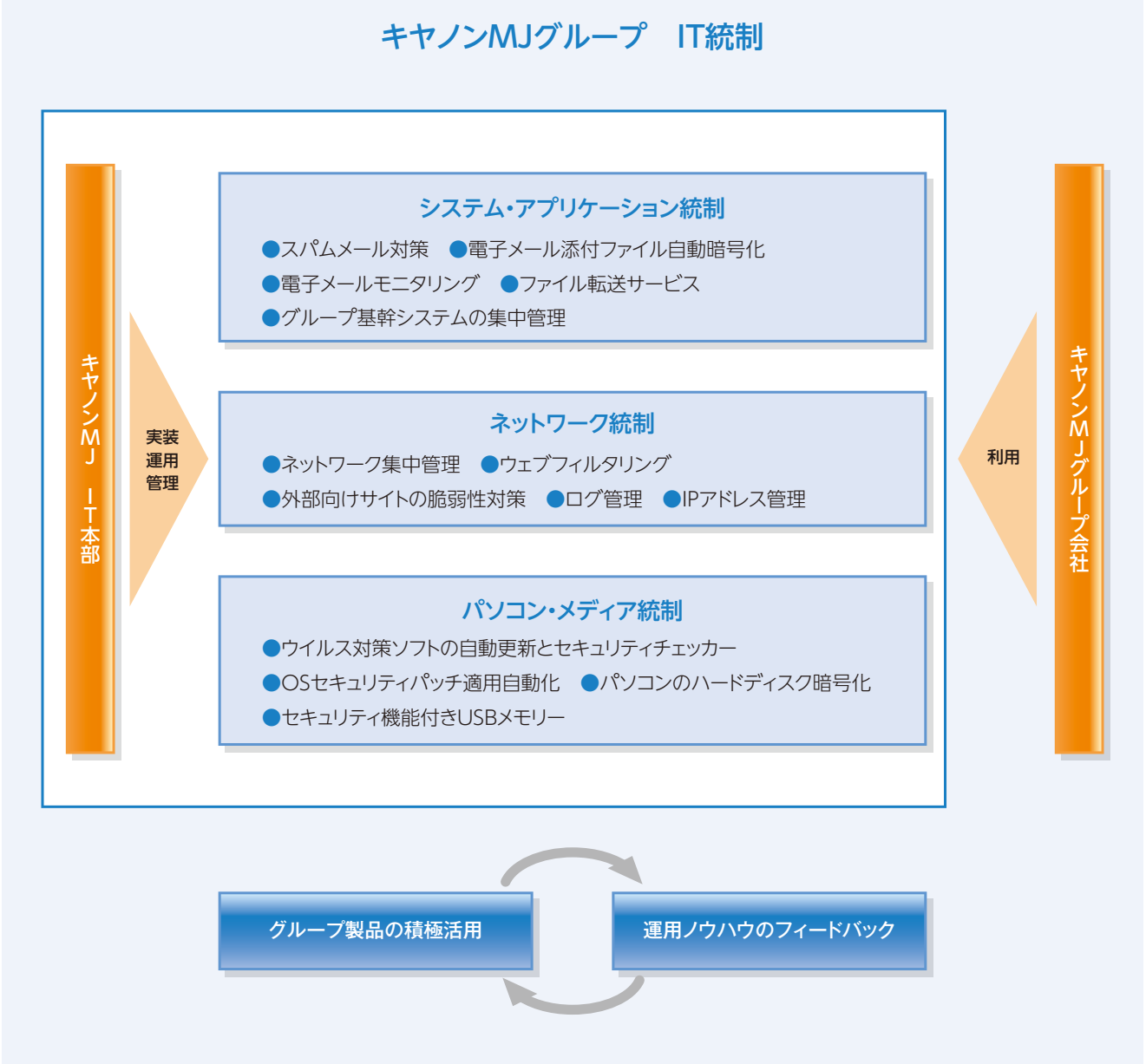
安心・安全を支えるITセキュリティ対策

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、情報漏えい等の防止に対し、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



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。

●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自動更新とセキュリティチェッカー

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。万一ウイルスがグループ内のネットワークに侵入した場合は、キヤノンMJのIT本部にて検知し、適切な対応を行っています。

また、各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。

●OS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はバックグラウンドで各パソコンに自動適用する方式を採用しています。

●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等をIT本部で行っています。

●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義務化しています。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。

■活用しているグループ製品の例

セキュリティ対策	製品と取扱会社
電子メールモニタリング	「GUARDIAN」シリーズ　取扱会社：キヤノンITソリューションズ GUARDIAN シリーズ ガーディアン
パソコンのハードディスク暗号化	CompuSec　取扱会社：キヤノンITソリューションズ CompuSec コンピュセック
ウイルス・スパイウェア対策	ESETセキュリティ ソフトウェア シリーズ　取扱会社：キヤノンITソリューションズ イーセット エンドポイント プロテクション アドバンスド ESET ENDPOINT PROTECTION ADVANCED イーセット エンドポイント プロテクション アドバンスド

Action 2013　2013年の取り組み

部門サーバーの安全性向上

キヤノンMJでは、部門に管理を任せていた部門サーバー環境に対し、データセンターのクラウド基盤ソリューションの一つである、キヤノンITソリューションズが提供している共通基盤「SOLTAGE」への移行推進を図り、安全性をより高めています。

テレワーク（在宅勤務）への取り組み

キヤノンMJでは、柔軟で新しい働き方を提供し労働の質を向上させること、さらにはその取り組みをお客さまとも共有し、自社だけでなくお客さまのワークスタイル変革にも貢献していくことを目指し、2012年より本社管理部門を中心に順次テレワークを導入しています。

テレワーク導入にあたり、在宅勤務における情報セキュリティリスク対策のために、通常のセキュリティ対策に加えて、SSLによる通信の暗号化、ワンタイムパスワード、クライアント証明書などの対策を実施しています。テレワークの取り組みは、2014年2月に一般社団法人日本テレワーク協会による「第14回テレワーク推進賞奨励賞」を受賞しました。


テレワーク推進賞奨励賞の表彰式

事業継続計画・管理（データセンターへの移転）

キヤノンMJグループでは、事業継続の観点から、かねてよりDR※サイトを構築しています。今回、新たにメインサイトをデータセンターへ移設することになりました。

そこで、移転時の万が一のトラブル発生に備え、即座にDRサイトが稼動できるよう万全な体制を整えるとともに、以前から取り組んでいた仮想化によって3日間という最短のスピードで、データセンターへの移転を完了しました。

この実績が貴重なノウハウとなり、移転ビジネスへと結びついた形になっています。

※DR（Disaster Recovery）：災害対策

外部向けサイトの脆弱性検査の実施

サイバー攻撃に対する対応の一環として、キヤノンMJグループでは、外部から接続できるウェブ環境（ウェブサイト、デモ用サイト、開発環境等を含む）についての脆弱性検査をすべて実施し、安全対策が必要なものについては対策の実施を行うスキームの確立を図っています。

2013年度も、ウェブ環境についての脆弱性検査をすべて実施しました。

積極的な情報開示と社会への貢献

説明責任を果たすとともにお客さまの課題解決に向けた参考情報を紹介するために、
自社の取り組み、ノウハウを積極的に開示しています。
また、各種団体への協力や次世代の情報セキュリティ人材育成に向けた教育活動などを行っています。

「CSRナビ」の展開

お客さまのCSR活動を支援するサイト「CSRナビ」をホームページ内に公開しています。このサイトではお客さまがキヤノンMJグループの情報セキュリティの活動事例やノウハウを確認できるだけでなく、「情報セキュリティCSRチェックシート」を通じてお客さま自身の抱える課題を把握することができます。また、その課題解決のためにキヤノンMJグループが提案できる製品やソリューションへナビゲートしています。

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、情報セキュリティガバナンス体制やプライバシーマーク、ISMS認証といったマネジメントシステムの構築・運用方法、セキュリティ対策の実装事例および人材育成などについて具体的に説明しています。

セミナーと「オフィスツアー」の様子

情報セキュリティ関連団体への支援

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

（五十音順）

※2014年4月1日現在

Action 2013 2013年の取り組み

「先端IT活用推進コンソーシアム」への参画

キヤノンソフトウェアは、企業における先端ITの活用および先端ITエキスパート技術者の育成を目指す業界団体「先端IT活用推進コンソーシアム」に参画しています。

その活動の一環として、2013年3月に気象庁と「第1回気象庁XML利活用セミナー」を開催しました。

「第1回気象庁XML利活用セミナー」の様子

「RyukyuFrogsプロジェクト」および「TOMODACHI-Frogs jr.プロジェクト」への参画

「RyukyuFrogsプロジェクト」は、沖縄の将来を担う若者が次世代ビジネスリーダーへと成長する機会を提供する取り組みです。選抜された大学生と高校生に対して、米国シリコンバレーでITビジネスの最先端に触れる派遣研修を中心に、約半年にわたる学びの機会を提供しています。

また、「TOMODACHI-Frogs jr.プロジェクト」は、「RyukyuFrogsプロジェクト」よりさらに若いジュニア層を対象に、シリコンバレーでの派遣研修などで、早期に高いレベルの経験をしてもらう取り組みです。

クオリサイトテクノロジーズはプロジェクト発足からこの趣旨に賛同し、資金援助のみならず講師派遣などの支援も行っています。2013年は、選抜メンバーの自発性とチャレンジ精神を喚起するためのキックオフ研修の講師を派遣しました。

「RyukyuFrogsプロジェクト」の様子

高崎商科大学の特別講座で講義を実施

高崎商科大学では、2013年、情報ネットワーク論（河合博子教授）の特別講座として「ICT活用による福祉支援の現状と近未来への貢献を考える」をテーマに、外部講師を招いた合計15回のリレー講座を開催しました。

学生の皆さんが、情報通信技術の基礎的理解を深めるとともに、自らの社会貢献への可能性を見出すことを目的としたこの講座で、キヤノンMJでは「企業経営を支える今日の情報セキュリティ 」と題し、当社の情報セキュリティの考え方や具体的な取り組みについて講義を実施しました。

講義の様子

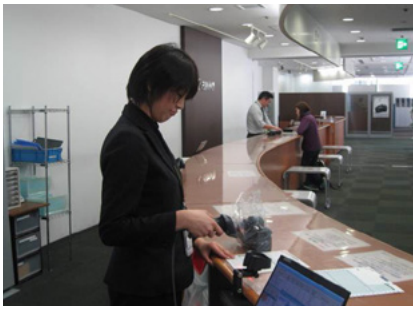
お客さまへの価値提供プロセスにおける情報セキュリティ品質の向上

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・安全を提供する修理プロセスの追求

キヤノンMJグループのコンスーマ修理部門は全国11拠点に展開しており、お客さまの期待を超えるサービスの提供を目指して、カメラ・インクジェットプリンターを中心に、お客さまのお問い合せや相談・修理・情報提供に至るまで、一貫したワンストップ体制を整備しています。

また、お客さまの大事な機器と情報をお預かりしていることの重要性を認識し、さらなる安心・安全な修理サービスの提供に向けて情報取り扱い教育を行い日々実践しています。



修理受付窓口

■修理サービスプロセスごとのリスクと情報セキュリティ対策事例

プロセス	リスク	情報セキュリティ対策事例
受付	●お客さまの個人情報の紛失・漏えい ●修理品・付属品の盗難・紛失 ●修理お見積り額をお知らせする際のファクスの誤送信	●窓口での修理受付時にお預かりする物品の確認をその場で行い、バーコード付きお預かり書をお客さまに発行しています。 ●個人情報を記載した保証書などは、修理受付後、所定の袋に入れた上で修理品と一括管理しています。 ●ファクス番号や送付先の呼称確認とダブルチェックをしています。 ●ファクス番号二度入力機能を持つ機器を導入し送信しています。 ●万が一のファクス誤送信に備え、見積書の個人情報部分の一部を伏せて送信しています。
修理	●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 ●修理品・付属品の盗難・紛失 ●委託先における情報セキュリティ事故の発生	●お客さまよりお預かりした可搬メディアは、修理作業用パソコンに接続する前に、検疫用パソコンにて、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ています。 ●修理業務に用いるパソコンは、すべて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。 ●修理作業中の修理品や付属品は、修理依頼書と突き合わせを行い、現品管理を行っています。 ●終業後は、施錠環境にて保管しています。 ●運用手順の指導や教育を委託先に対して実施しています。 ●定期的に委託先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修理品の誤送付	●配送伝票作成時には、チェックシートをもとに配送伝票と修理品に添付された修理依頼伝票(修理品・付属品送付先)の整合性を確認しています。 ●梱包時には、修理依頼伝票・修理完成伝票・配送伝票の修理番号を出荷台帳へ記録し、間違いのないことを確認しています。
窓口返却	●修理品・付属品の誤返却	●完成伝票に記載されている修理番号、お客さま名、付属品をお客さま持参のお預り書に記載されている内容と声だし確認しています。 ●完成伝票とお預り書のバーコードを照合しお客さまの修理品に間違いないか確認しています。

安心・安全な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、全国に約200の営業所を展開し、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のサービス・サポート部門は、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用いて、お客さまに安心していただける複合機やプリンター、ネットワークなどの保守サービスを提供しています。

サービスエンジニアによる保守の様子

■保守サービスプロセスごとのリスクと情報セキュリティ対策事例

プロセス	リスク	情報セキュリティ対策事例
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、施錠できる場所に管理しています。 ●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 ●パソコンの紛失による情報漏えいリスク	●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。 ●持ち出すパソコンはHDDパスワード、ログインパスワードに加えてHDD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とき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、基本的には禁止しています。 ●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 ●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	●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等を「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。

Action 2013 2013年の取り組み

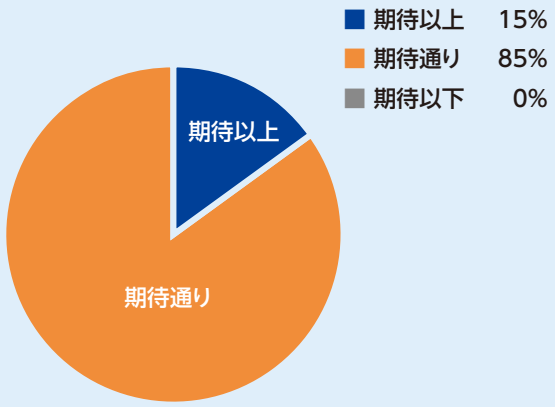
キヤノンMJの情報セキュリティ活動に関する「顧客満足度調査」を実施

キヤノンMJは、お取り引きのあるお客さまから、当社の情報セキュリティに関する取り組み状況について書面調査を受けています。この回答をお返しする際に、当社の取り組み内容に関するお客さまの評価を確認することを目的に、アンケートを実施しました。アンケートの結果、お客さまの満足度が把握できたこととあわせて、さまざまなご意見やご感想をいただきました。

いただいたお客さまの声は、お客さまに安心・安全を提供していくための貴重なご意見として活用していきます。

■アンケート結果(抜粋)

(質問)当社の取り組みは、お客さまのご期待に応えられましたか？



キヤノンMJの取り組みに対する評価結果

お客さまの情報セキュリティ課題解決への貢献

自社グループの製品を活用することによって得られた運用ノウハウも含めて、
最適な情報セキュリティ製品・ソリューションをお客さまへ提供します。

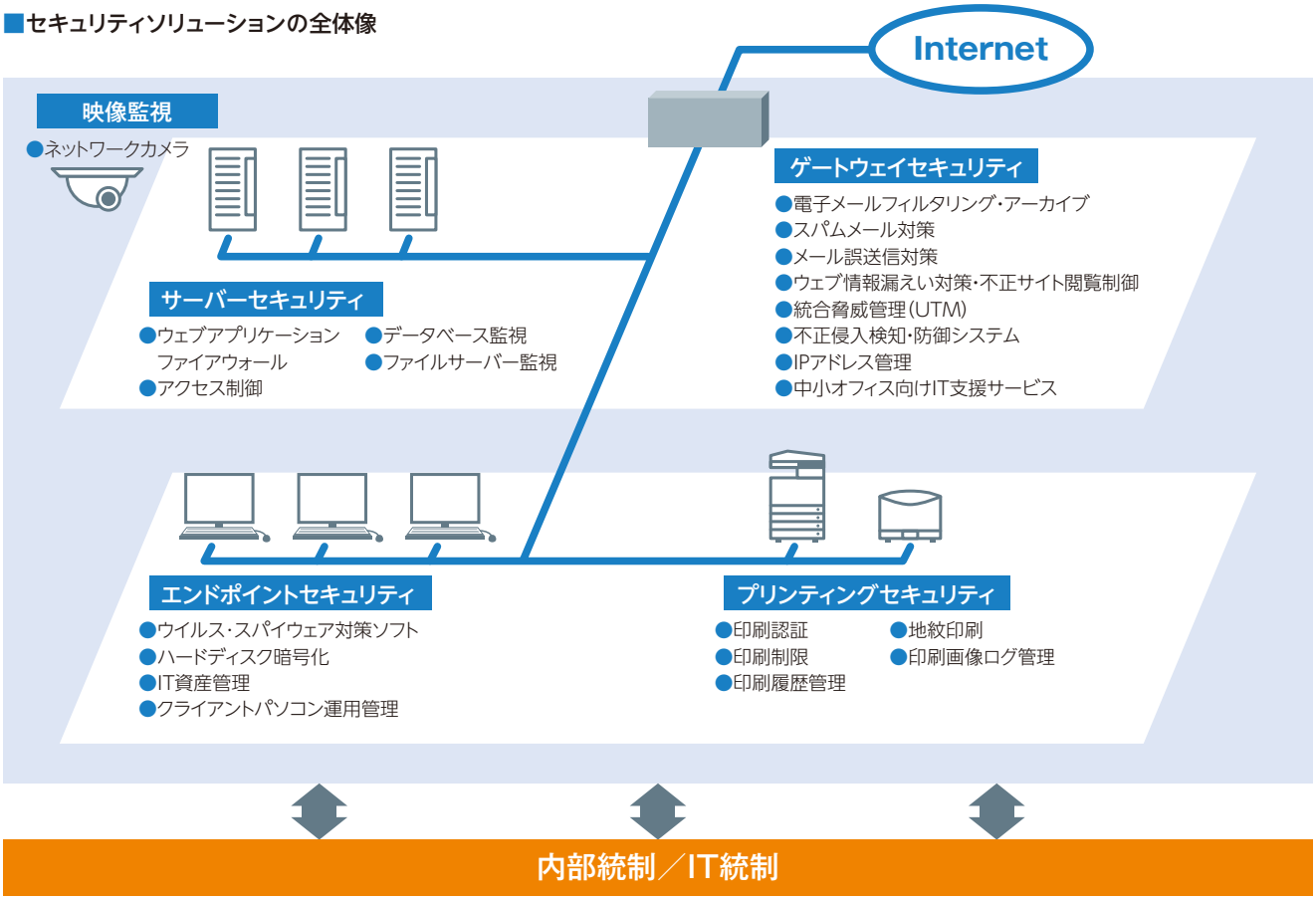
企業の重要課題をセキュリティ対策の視点で支援

リスクマネジメントや内部統制の強化など、企業経営にとって重要な課題を解決するため、企業のIT化はますます加速しています。IT導入の際には、自社ネットワークへの不正侵入や、コンピューターウイルスによる感染被害など、さまざまな脅威への対応が必要不可欠です。キヤノンMJグループは、ITガバナンスの確立や内部統制の強化を実現するIT全般統制の視点から、セキュリティソリューションを提案しています。

最適なセキュリティソリューションの提案

セキュリティ対策に必要な要件を、「映像監視」「サーバー」「ゲートウェイ」「エンドポイント」「プリンティング」の5つのカテゴリーに分けて体系化しています。情報セキュリティの実装はもちろんのこと、高性能ネットワークカメラと監視・録画ソフトによる物理的監視体制の強化に至るまで、お客さまの環境に即した最適なセキュリティソリューションを提案しています。

■セキュリティソリューションの全体像



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	多段階のフィルターで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・制御	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。

情報の有効活用を目的とした玄関口を提供する「HOME-PORTAL」

社内に分散しているさまざまなデータや情報を一括管理して、情報の効率的な利用が可能となる、キヤノンMJグループが提供するSaaS型アプリケーションです。

「スケジューラ」「設備・備品予約」「伝言メモ」「掲示板」に加えて、クラウド上にデータを安全に保管し簡単に活用できるストレージサービスである「HOME-BOX2」機能を備えています。他にもオプションとして、「災害掲示板 安否確認」「リモートバックアップ AOSBOX」「簡易資産管理/モバイルデバイスマネジメント (MDM) HOME-MANAGER」「クラウド型名刺管理 アルテマブルー」「iPad※用文書活用ソリューション Smart Browse Print」などをラインアップしており、災害対策や事業継続計画、ワークスタイルの変革などお客さまのさまざまな課題解決を支援します。

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

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。

「HOME」を導入いただいたお客さまの声

「HOME」を導入することで、グループウェア機能を利用してスケジュールやデータを共有し、各スタッフが最新情報をタイムリーに把握できるようになりました。この結果、納品スピードが早まっただけでなく、コミュニケーションミスによるデザインの修正が減るなど成果物の完成度も上がり、お客さまの満足度を大きく高められました。

また、私自身、情報システムに詳しくないにもかかわらず、「HOME」にはファイアウォールをはじめとするさまざまな対策機能が集約されていて、総合的な情報セキュリティ体制を構築することができました。当社のお客さまは大手企業が多いこともあり、情報セキュリティ対策の実施状況のお問い合せも増えています。こうしたお問い合せに対しても、情報セキュリティ対策の内容を取引先へ明確に説明できるようになり信頼関係を高めることができるようになりました。

代表取締役社長
吉田篤弘様

x code
Commercial Design,Inc.

コマーシャルデザイン株式会社
本　　社：東京都中央区日本橋蛎殻町1-21-7
設　　立：2001年
従業員数：5名
事業内容：広告・デザインの企画・制作

国内最高水準の堅牢性を持つ「西東京データセンター」

キヤノンMJグループの「西東京データセンター」は、「所有するIT」から「利用するIT」へと高度化・複雑化するお客さまのITニーズを見据えた堅牢性や信頼性の高いデータセンターです。また、24時間365日、お客さまのビジネスをストップさせない体制で価値あるサービスを提供していきます。


西東京データセンター

西東京データセンターの堅牢性

西東京データセンターは、その利用価値を最大化するために5つのファクターを強化した次世代型のデータセンターです。

「ロケーション」「セキュリティ」「グリーンデータセンター」「ファシリティ」「運用サービス」の面で国内最高水準の性能を持っており、お客さまに安心・安全を提供しています。

■西東京データセンターの5つの特長

ロケーション　セキュリティ　グリーンデータセンター　ファシリティ　運用サービス

西東京データセンターの5つの特長

●ロケーション

都心から20km圏内、1時間以内でアクセス可能であり、災害時に高波・高潮や液状化の危険性が低いロケーションに立地しており、利便性と耐災害性を兼ね備えています。

●セキュリティ

「金融機関等コンピューターシステムの安全対策基準」(FISC)の厳しいガイドラインに準拠した万全のセキュリティで、お客さまの資産を安全に保護します。

●グリーンデータセンター

自然エネルギーを活用した消費電力削減によって、データセンターの電力使用効率を示す指標であるPUE※を1.4という高い数値で達成することを目指しています。高い冷却効率と環境性能を両立し、高集積・高密度機器の安定した運用を可能にしています。

※PUE：データセンター全体の消費電力÷IT機器による消費電力

●ファシリティ

日本データセンター協会(JDCC)の設計規格「データセンターファシリティ スタンダード」のティア4レベルに準拠。高度な設計技術や、最新設備の導入などで、次世代データセンターとして相応しい設計になっています。

●運用サービス

ITサービス管理・運用規則に関する国際標準であるITILに準拠した運用体制を整備し、設計、運用、継続的なサービス改善などの一連のIT利用をワンストップで提供します。

西東京データセンターが提供するサービス

国内最高水準のファシリティースペックと、既存データセンターの運用で培ったノウハウを活かし、お客さまがデータセンターに求めるサービスを包括的に提供します。

■西東京データセンターが提供するサービス

- ハウジングサービス
- ASP・SaaS
- ホスティングサービス
- ISPサービス

西東京データセンターが提供するサービス

●ハウジングサービス

データセンター内のラックスペースに、お客さまのサーバーなどをお預かりする「ファシリティサービス」と、データセンター内のシステムから高速・大容量のインターネット帯域を提供する「コネクティビティサービス」を提供します。

●ホスティングサービス

データセンターで管理されたネットワーク機器やサーバーのレンタルだけでなく、システム設計から構築・運用・保守までを一括で提供します。

●ASP・SaaS

ハウジングサービスおよびホスティングサービスを利用しホームページなどを公開されているお客さまに、セキュリティ脆弱性・監視を合わせて提供します。また、お客さま拠点のセキュリティを高めるASPサービスでは、システムの脆弱性確認やデータ保全を行います。

●ISPサービス

お客さま拠点でのインターネット回線接続、ホームページなどで利用するドメインの登録およびハウジングサービスやホスティングサービスを利用されているお客さまに対してDNSサービスを提供します。

キヤノンMJグループでの活用事例

より確かな「安心・安全なサービス提供」のために：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IT本部は、2013年5月、基幹システムのメインサイトをオフィスビル内のマシンルームから、国内最高水準の堅牢性を有する新データセンターへ移転しました。移転を実施した結果、従来より一段と高いレベルのセキュリティ、環境対応、サービスレベルが実現されました。2011年に構築したDR※サイトと今回のメインサイト移転により、お客さまへより確かな安心・安全なサービスを提供していきます。

※DR（Disaster Recovery）：災害対策

SaaS型機密情報保護基盤「PDFPolicy Service」

近年、企業は情報セキュリティや営業秘密管理、内部統制などの観点から、機密情報を適切に保護する必要性に迫られています。

その具体的な保護の手法としては、対象ファイルをアクセス制御された文書管理システムに格納する、対象ファイルをパスワードで暗号化するなどが一般的ですが、これらは一度ファイルをダウンロード・配布してしまえばその後の管理が受け取った側に任されてしまうため、将来にわたって機密情報を守り続けることは困難です。

PDFPolicy Serviceはファイル（＝文書）のポリシー管理とユーザー認証により、機密情報の適切な保護を支援します。

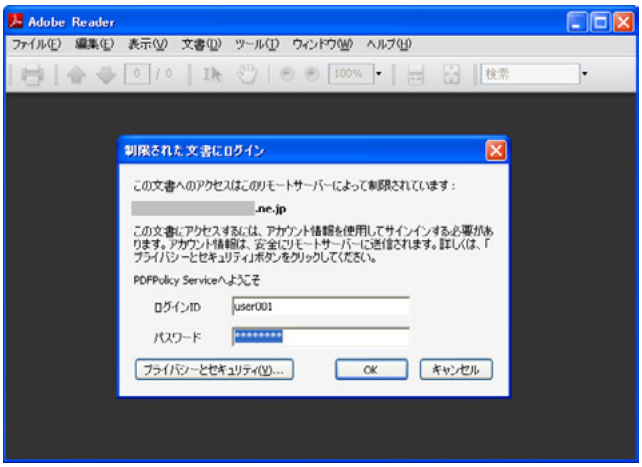
利用権限の制御と失効処理

文書の閲覧権限・印刷権限・編集権限などを、ユーザー単位・グループ単位で制御することができます。

ユーザーはポリシーが付与された文書を利用する際、PDFPolicy Serviceと通信を行い、ID・パスワードによるユーザー認証を行うことで、権限に応じた利用が可能になります。また、適用するポリシーに有効期限を設定しておく、あるいは文書の失効を行うことにより、配布済み文書を任意のタイミングで利用できなくすることも可能です。

	A部	B部	協力社員
閲覧	○	○	○
印刷	○	○	×
編集	○	×	×
期限	4/1～9/30		

ポリシー設定のイメージ



ユーザー認証のイメージ

監査ログの取得

誰が（ユーザー名）、いつ（日付時刻）、どの文書を利用したかといったログ情報を確認できます。この情報は、情報流出時の原因特定や、文書の利用状況確認などに利用することが可能です。

ログ管理を従業員に通知することは、セキュリティ意識の向上にもつながります。

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

ネットワークに接続されるさまざまなオフィス機器は、不正アクセスや情報漏えいリスクにさらされる可能性があります。

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、設定のサポート等を行っています。

■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」におけるセキュリティ対策

キヤノンでは、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複合機に組み込んでいます。

最新機種「imageRUNNER ADVANCE」のラインアップに搭載されている機能の一部を紹介します。

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 2600TM-2008 (以下、IEEE 2600) に準拠しております。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。

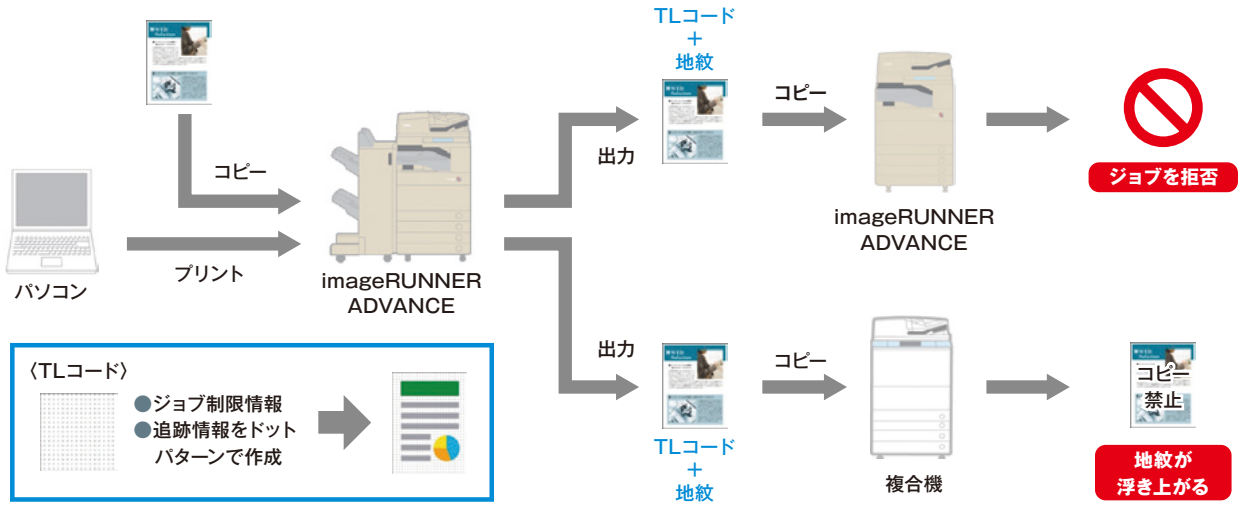
複合機から紙出力した機密情報の漏えい対策

コピーやプリント時に、TLコード（低可視のドットパターン情報）で作成されたジョブ制限情報や追跡情報を埋め込み、ジョブ動作のロックや追跡情報（5W1H）の取得を可能にします。

さらに地紋印字と組み合せれば、ジョブロック未対応機器を利用した際にも「機密」などの地紋が浮き上がります。出力された機密文書の流出を抑止する効果があります。

※ベタや写真などの原稿ではロックしない場合があります。
※「ジョブロック拡張キット」「イメージ解析ボード」が必要です。

■出力文書の不正利用を抑止する「ジョブロック機能」



複合機に保存されている機密情報の漏えい対策

セキュリティ機能の評価適性度を保証するISO15408（コモンクライテリア）認証（EAL3）を取得した「Canon MFP Security Chip 2.00」を搭載し、ハードディスク内データを自動的に暗号化します。

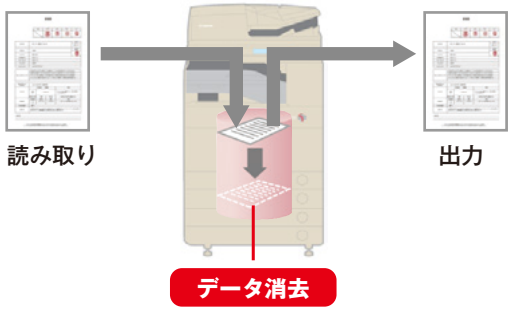
※「HDDデータ暗号化／ミラーリングキット」が必要です

「自動消去」は、コピーやプリントなどの作業を行うたびに一時的にハードディスク内に生成されるデジタルデータを、ジョブ終了と同時に自動的に消去する機能です。万一の盗難や本体廃棄後の情報漏えいリスクを低減します。

※「データ消去キット」が必要です。

■本体データを守る「HDDデータ暗号化」

■ジョブ終了後のデータを残さない「自動消去」



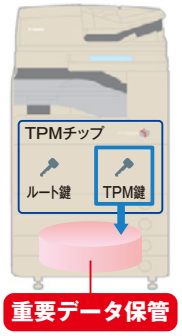
ルート鍵を保護するTPM機能

複合機内にはパスワードや暗号鍵など多くの機密情報が保管されています。TPM (Trusted Platform Module) 機能では以下の方法でセキュリティを維持しています。

●複合機内の重要データとルート鍵を別々に管理
●ルート鍵はセキュリティチップ(TPM)により安全管理

すべての機密情報はTPMチップ内のルート鍵で暗号化してから保存され、ルート鍵はチップ外に流出することはありません。複合機内の物理的解析やネットワークを介した不正アクセスから、安全に保護されます。

■TPM機能概念図



不正操作発生時のログ取得

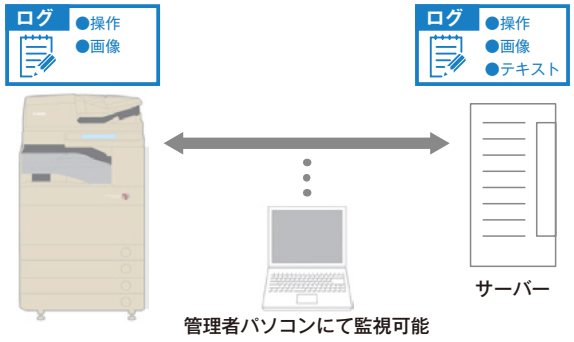
管理者は、本体に保存されるさまざまな「監査ログ」から、不正操作を追跡することができます。

データベースなどの複雑なシステムを使用せずに、誰が、いつ、どの複合機で、どのような操作(印刷・FAX・スキャン等)をしたかという「操作ログ」に加え、どんなドキュメントを取り扱ったかという「画像ログ」まで管理することができます。各ログはExcelを使って検索・閲覧をすることができ、管理、追跡が可能なセキュリティの高いシステムを用意しています。

監査ログの種類

●ユーザー認証ログ
●ジョブログ
●ボックス文章操作ログ
●ボックス認証ログ
●アドバンスドボックス保存ログ／操作ログ
●ネットワーク接続ログ
●本体管理ログ
●一括エクスポート／インポートログ
●監査ログ管理機能のログ

■画像ログの管理



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

オフィス向けレーザービームプリンター「Satera」は、高速・高品質印刷により、業務の効率化や表現力の向上をサポートするだけではなく、優れたセキュリティ機能を搭載し、オフィスでのセキュアなプリント環境を実現しています。

暗号化でセキュアなデータ通信を実現

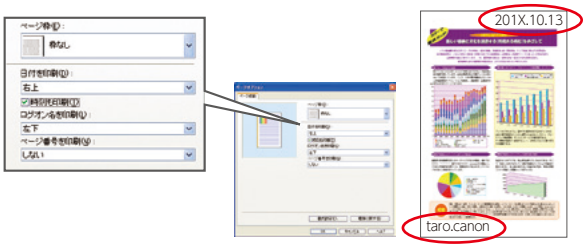
パソコンとプリンター間の伝送経路を暗号化して、情報漏えいを抑制するSSL通信に対応しています。離れた拠点への印刷も安全で、セキュアなプリント環境を構築することができます。

■SSL通信概念図

出力文書に印刷者情報の印字が可能

簡単な操作で、出力文書にユーザー名や日付などの情報を付加することができます。文書管理に役立つだけでなく、印刷物に対するセキュリティ意識を高めます。

■ID印刷機能

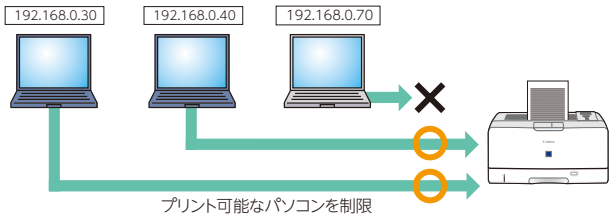


印刷できるパソコンを制限

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



出力の放置をなくし、紛失・漏えいを予防

出力時にプリンタードライバーでパスワードを設定すると、プリントデータをプリンター本体内のハードディスクに一時待機させることができます。本体パネルでパスワードを入力すると、待機させたデータの出力がスタート。第三者に閲覧されることなく出力物を直接手にできるため、情報の漏えいを抑制することが可能です。

パスワード入力画面

Action 2013 2013年の取り組み

キヤノンMJグループでのネットワークに接続する各種機器のセキュリティ対策

2013年、一部の報道におきまして、「複合機の一部でセキュリティ対策が不十分な場合、機器内部の情報がインターネットを通じて外部から見られる状態となる」主旨の記事が掲載されました。

キヤノンMJグループでは以前より、営業・保守サービスの担当を通じてお客さまへ、ファイアウォールの設定やID・パスワードを変更するなど、安心してご使用いただくための具体的な対策についてご案内を行っておりました。昨年のこの報道を受け、改めてこのことをお客さまへご案内しました。

なお、これは複合機だけでなくネットワークに接続される機器全般について言えることです。

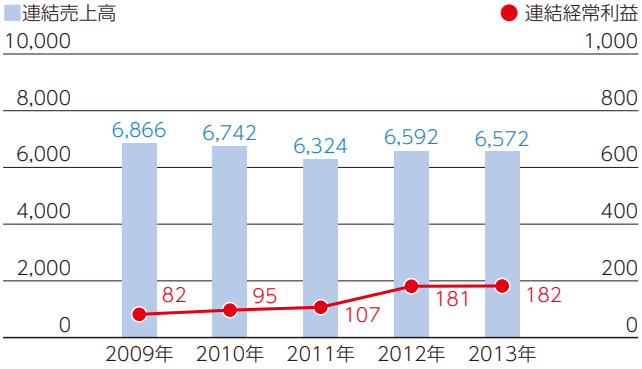
キヤノンシステムアンドサポートでは、報道を受けてお問い合せをいただいたお客さまのご不安をいち早く解決するために、体制を強化し対応しました。あわせて、こうしたリスクはネットワーク環境に脆弱性があることにも起因することから、その課題解決のためのセキュリティソリューションの提供を通じてお客さまの安心安全に貢献しました。

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 (2014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：18,573名　単独：5,383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

キヤノンMJグループ　連結売上高／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。これに伴い、2012年度についても、当該変更を反映した遡及適用後の数値を記しています。

グループ会社紹介 (2014年4月1日現在)

ビジネスソリューション
- キヤノンシステムアンドサポート(株)
- キヤノンプロダクションプリンティングシステムズ(株)

ITソリューション
- キヤノンMJアイティグループホールディングス(株)
  - キヤノンITソリューションズ(株)
    - キヤノンITSメディカル(株)
    - キヤノンビズアテンダ(株)
    - スーパーストリーム(株)
    - ガーデンネットワーク(株)
    - クオリサイトテクノロジーズ(株)
    - 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
    - Canon IT Solutions (Philippines), Inc.
  - キヤノンソフトウェア(株)
  - エディフィストラーニング(株)

イメージングシステム
- キヤノンカスタマーサポート(株)

産業・医療
- キヤノンライフケアソリューションズ(株)
  - (株)エルクエスト
- 台灣佳能先進科技股份有限公司

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)
  - オーエーエル(株)

※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はかるしくみ。

事業領域

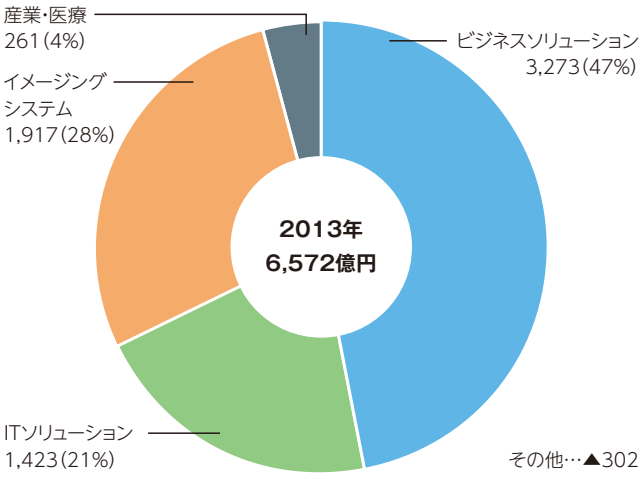
ビジネスソリューション
お客さまの競争力向上のため、多彩なビジネス機器とソフトウエア、運用サービスを連携させたソリューションを提供します。

ITソリューション
グループの総合力で、最先端のIT環境を構築し、お客さまの競争力と企業価値の向上に貢献します。

イメージングシステム
クロスメディアイメージングの楽しさを、より多くの人に。自分のアイデアや工夫が手軽にカタチになる喜びをさらに広げていきます。

産業・医療
●産業機器関連
世界中の半導体業界をはじめとする産業を力強くサポートします。
●医療関連
最先端の医療機器とソリューションで人にやさしい医療の実現を後押しします。

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)※



※「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。
※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。
※2014年より「産業機器」から「産業・医療」にセグメント名を変更しました。

長期経営構想フェーズⅡ(2011～2015)

ミッション
安心安全で豊かな「くらし、しごと、社会」の実現に向けてマーケティング・イノベーションを行い、最高の価値を提供する

ビジョン
『顧客主語』を実践するグローバルな視野をもったサービス創造企業グループ

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」といいます）は、キヤノングループ共通の企業理念「共生」の下、安心安全で豊かな「くらし、しごと、社会」の実現に向けてマーケティング・イノベーションを行い、最高の価値を提供するための事業活動を展開しています。

当社グループは、この事業活動において、情報資産を適切に取り扱うことがお客さまへの価値提供と企業の社会的責任の観点から重要な経営課題と認識し、以下の方針に基づき情報資産の有効活用と保護に努めます。

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
2011年　6月　1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 川崎正己

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」といいます）は、キヤノングループ共通の企業理念「共生」の下、安心安全で豊かな「くらし、しごと、社会」の実現に向けてマーケティング・イノベーションを行い、最高の価値を提供するための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令、国が定める指針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、個人情報の取扱いおよび個人情報保護マネジメントシステムに関する苦情や相談および、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　2005年11月　2日
2007年　1月25日
2011年　6月　1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 川崎正己

※グループ各社は同様の方針を制定しています。

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

2014年6月発行