Canon





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」を参考にしました。

キヤノンMJグループでは、「情報セキュリティ報告書」を2008年から「CSR報告書」との合冊版の冊子として発行し、ステークホルダーの皆さまへの情報開示を進めてきました。

2010年より、環境にも配慮し冊子としての発行は行わず、ウェブサイトへの掲載による報告に切り替えました。ウェブサイトでは情報の更新性の側面を、PDFでは読みやすさの側面を重視して編集しました。

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2010年(2010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 CSR推進本部 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

- 3 トップメッセージ
- 4 推進フレームワークと主要テーマ
- 5 情報セキュリティマネジメント
- 9 第三者認証の効果的な活用
- 12 情報セキュリティ対策の実装
- 15 情報セキュリティ人材の育成
- 17 積極的な情報開示と社会への貢献
- 18 お客さまへの安心・安全の提供
- 23 セキュリティソリューションのご紹介
- **25** キヤノンマーケティングジャパン グループ概要

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づけ

「顧客満足度の向上」と 「セキュアな社会の実現」のために



代表取締役社長 川崎 正己

はじめに、このたびの東日本大震災により被災された皆さまに謹んでお見舞い申し上げますとともに、一日も早い復興を心よりお祈り申し上げます。

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年の長期経営構想フェーズ II をスタートさせました。そ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開始しました。

「安心・安全」の実現にとって、「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であるととらえています。情報通信技術が社会経済の神経系ともいわれるようになった現在、情報を適切に取り扱うことはネットワーク社会の一員としての義務といえます。

キヤノンマーケティングジャパングループは、キヤノン製品を中心に、お客さまの課題に対応した付加価値の高いソリューションをご提供する情報サービス企業として、「企業の社会的責任としての情報セキュリティ基盤強化」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。

「企業の社会的責任としての情報セキュリティ基盤強化」活動では、グループ各社に情報セキュリティ関連のマネジメントシステム (ISMSやPMS) を組み込み、運用の均質化と効率化を図るとともに、各種セキュリティ対策の最適化、人材の育成、積極的な情報開示などを推進しています。

「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」活動では、営業・保守サービス・ソフトウエア開発等の価値提供プロセスごとに、事業部門が主体となってリスクアセスメントを行っています。その際は、情報漏えい事故を防止するという側面だけでなく、お客さまの視点に立って「より安全に」「より確実に」「より効率的に」といった品質向上のための業務改善活動となるように徹底しています。

また、自社グループ内の各種ITセキュリティ対策の実装にあたっては、私たちが取り扱っている製品・サービスを導入し、製品・サービスの改善や運用ノウハウの蓄積を行い、これらを含めて、お客さまご自身の情報セキュリティ活動を支援すべく取り組んでいます。

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、関連するセキュリティソリューションを紹介しています。本報告書をご覧になっていただいた皆さまに、少しでもお役に立てば幸いです。

推進フレームワークと主要テーマ

キヤノンMJグループの情報セキュリティ推進フレームワークは、グループ情報セキュリティ基盤強化によるセキュアな社会の実現と、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による顧客満足度の向上を目指しています。

情報セキュリティ成熟度の向上にあたっては、情報セキュリティガバナンスとマネジメントシステムの有効性を継続的に向上させる取り組みを行っています。

主要注力テーマ

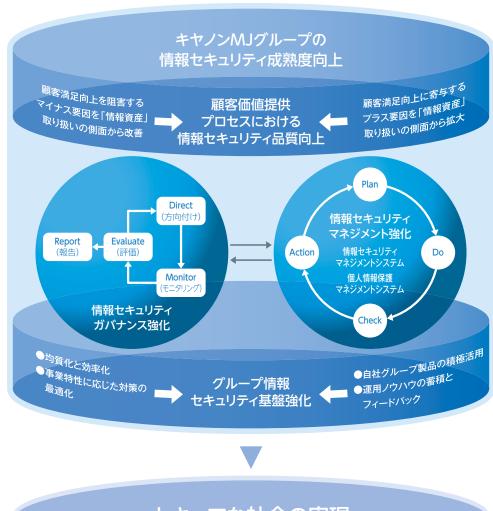
- 1.マネジメントシステムのグループ均質化と効率化
- 2.グループ共通対策と事業特性に応じた対策の最適化
- 3.情報セキュリティ人材の育成
- 4.情報セキュリティ活動の積極的な情報開示
- 5.お客さまへの安心・安全の提供
 - ●お客さまへの価値提供プロセスにおける 情報セキュリティ品質向上
 - ●お客さまの情報セキュリティ課題解決への貢献

顧客満足度の向上

質の高い情報セキュリティソリューション (製品・サービス)



情報セキュリティ・個人情報保護に 配慮したサービスメンテナンス



セキュアな社会の実現

情報セキュリティマネジメント

「グループ」「CSR連携」「全員参加」の視点に留意し、効果的かつ効率的な情報セキュリティマネジメントを推進しています。

CSR委員会による経営レベルの推進体制

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体制の強化を図るために、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活動では、経営戦略やリスク管理の観点から情報セキュリティの「方向づけ (Direct)」を行い、

活動の状況を可視化「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、本報告書を 通じて活動結果を利害関係者等へ「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、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。

グループ全員参加型のマネジメント体制

キヤノンMJグループでは、グループ全体の情報セキュリティマネジメント体制を整備しています。

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、自社およびグループ全体の情報セキュリティマネジメントを推進しています。グループ各社にも情報セキュリティ主管部門を設置し、各社のマネジメントシステムを推進しています。推進にあたっては、グループ各社間の情報セキュリティ事務局業務の重複を解消し効率化を図っています。

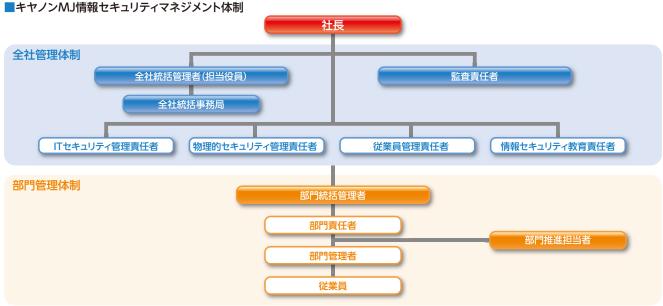
グループ各社の情報セキュリティマネジメント体制は、全社 管理体制と部門管理体制の2つの構造になっています。

全社管理体制では、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。部門管理体制では、各事業部門ごとにPDCAの運用が行えるよう、部門統括管理者や推進担当者を配置しています。

このような体制でマネジメントを推進することで、グループ 全員参加型の活動の定着を図っています。

■キャノンMJグループ全体のPDCAとグループ各社のPDCA





体系的にルールを整備

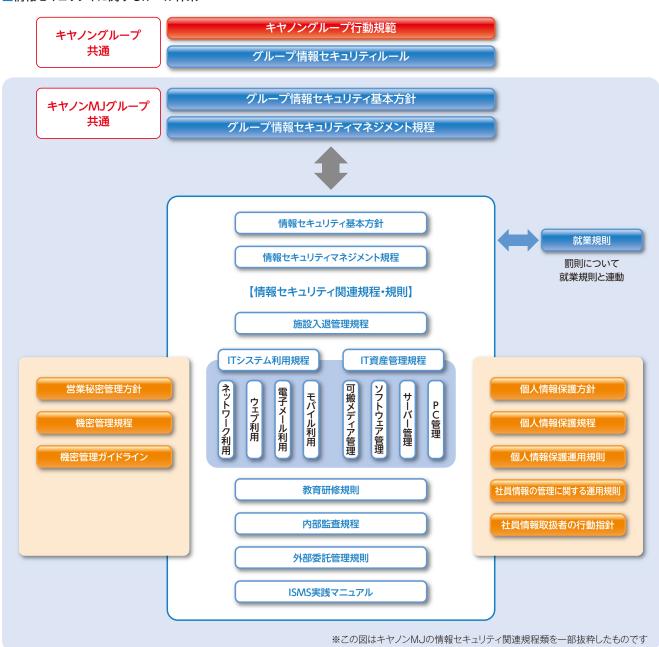
キヤノンMJグループでは、キヤノン (株) のグローバル基準である「グループ情報セキュリティルール」(ISO/IEC27001:2005に準拠) を基軸としながら、グループ全体の情報セキュリティを推進するための幹となる「グループ情報セキュリティ基本方針」と「グループ情報セキュリティマネジメント規程」を制定しています。

その下で、グループ各社で均質化したマネジメントを運用す

るために各社ごとのルール体系を整備し、情報セキュリティマネジメントシステムを構築しています。

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



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、親和性を向上し、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。

■マネジメントシステムの連携



パートナー企業の情報セキュリティ品質向上に向けた取り組み

キヤノンMJグループでは、パートナー企業の情報セキュリティ品質向上のための取り組みを実施しています。

具体的には、複合機の保守サービス業務やソフトウエア開発 業務等を委託しているパートナー企業に対して、委託業務に即 した情報セキュリティへの実践的な留意事項を教育しています。 あわせて、情報セキュリティ状況を確認するために、定期的 に現地調査を実施しています。

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、下記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
- ●ソフトウエ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
- ●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づ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。

Action 2010 2010年の取り組み

CSR委員会での情報セキュリティ 関連テーマの報告・承認

2010年も四半期に一度CSR委員会を開催し、情報セキュリティに関する内外環境変化や活動状況等のレビューを行いました。2010年の主な報告・承認事項は、以下の通りです。

- ●ISMS認証グループ統合化の承認
- ●法規制の動向報告(改正「不正競争防止法」等)
- ●外部脅威への対策状況報告(ガンブラー攻撃への対応状況)
- ●情報セキュリティ報告書の発行報告

グループ方針・規程を制定し、 グループ均質化を推進

キヤノンMJグループは2010年に、「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、グループ全体の情報セキュリティマネジメントの枠組みを確立しました。

情報セキュリティインシデント 管理システムの導入

キヤノンMJでは、2010年より情報セキュリティ・インシデントの管理をシステム化しました。

これにより、必要な関係者全員がインシデントの発生から顧客対応、発生原因の究明、是正・予防処置の実施までの一連の進捗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。

このシステムを順次グループ会社に展開し、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きます。

パートナー企業への学習会の実施

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向けに、安全なサービスメンテナンスをお客さまに提供するための情報セキュリティ学習会を実施しました。2009年7月~2010年8月までに243社、1,691名が受講しました。

また、ソフトウエア開発業務を委託しているパートナー 企業の新規派遣社員向けに、月2回セキュリティルール徹 底のための情報セキュリティ教育を実施し、約500名が参 加しました。



情報セキュリティ学習会の様子



情報セキュリティ学習会資料

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」の認証取得に グループ全体で取り組んでいます。

第三者認証の活用目的

キヤノンMJグループが第三者認証を取得する目的は、「ベストプラクティスを業務プロセスに組み込み、継続的に情報セキュリティ品質を高めていくこと」です。そして、その結果と

して取得した認証によって、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。

ISMSを活用した顧客満足度の向上

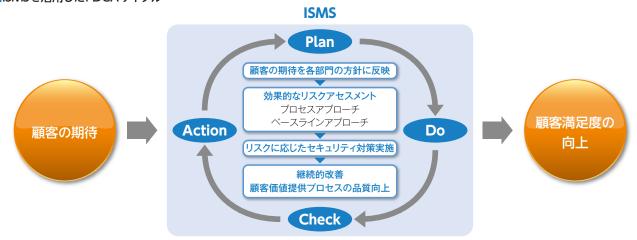
キヤノンMJグループのISMS活動は、情報セキュリティ基盤 強化に加えて、顧客価値提供プロセスの情報セキュリティ品質 を向上し、顧客満足度を高めていくことを目標としています。

この目標を達成するために、営業・サービスや開発などのビジネス部門では「お客さまに価値を提供する主要な業務プロセス」に登場する情報資産の洗い出しとリスクアセスメントを行っています。

一方、全社管理部門では、グループ共通のセキュリティ基盤 を強化するためのリスクアセスメントを行っています。

この2つの組み合わせにより、効果的かつ効率的なリスクアセスメントを実現し、顧客価値提供プロセスの業務改善を図りつつ、グループのセキュリティレベルの均質化と向上につなげています。

■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

●グループ全社へのプライバシーマーク導入を推進

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に、グループ全社へ

の「プライバシーマーク」導入を推進しています。

●個人情報管理レベルの向上と均質化の工夫

キヤノンMJグループでは、従業員一人ひとりの個人情報の管理レベルの向上と均質化を図るために、「個人情報データベース管理システム」を独自に開発し、運用しています。

このシステムは、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適切な対応事項や、個人情報の取得から廃棄に至るプロセス内のリスクと対策項目の確認と手続きを行うことができます。特にリスクアセスメントで

は、取り扱い方法によってリスクと対策が動的に変化するため 必要な対策を漏れなく確認し、実施することができます。手続 きが完了すると全社管理台帳が自動的に完成します。

また、このシステムでは、個人情報の取り扱い業務を委託している委託先の評価や契約内容の一元管理を行うことができます。このしくみによって従業員の個人情報取り扱いレベルの均質化と管理業務の効率化を実現しています。





個人情報データベース管理システム

個人情報データベース管理システムの特徴

- ●法的要求事項やJIS規格に沿った運用のチェック
- ●取得~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
- ●業務委託先の評価や契約内容の一元管理
- ●全社管理台帳の自動生成と最新状態の維持
- 上記の機能を承認ワークフローの中で実現しています。

■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。

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。

■キヤノンMJグループにおける認証取得状況

会社名	ISMS認証	プライバシーマーク認証
キヤノンマーケティングジャパン	0	\circ
キヤノンシステムアンドサポート	0	0
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	0	0
キヤノンITSメディカル		0
キヤノンビズアテンダ	0	0
エス・エス・ジェイ		0
AES		0
ガーデンネットワーク		0
クオリサイトテクノロジーズ	0	
佳能控制系統(上海)		_
キヤノンソフトウェア	0	0
キヤノンソフト情報システム		0
Canon Software America		
エディフィストラーニング		
キヤノンビジネスサポート		0
オーエーエル		0
キヤノンプリントスクエア	0	0
キヤノンカスタマーサポート	0	0
キヤノンフィールドアシスト		0
ウイズフォト		

2011年4月1日現在

Action 2010 2010年の取り組み

ISMSグループ統合認証の推進

新たにキヤノンカスタマーサポート、キヤノンプリント スクエア、キヤノンビズアテンダがISMS認証を取得し、 グループ内のISMS取得企業は8社となりました。なお、 2011年のグループ完全統合認証のステップとして、2010 年はISMS認証の部分統合を行いました。

「個人情報データベース管理システム」 のグループ展開

国内グループ会社のうち、8社で「個人情報データベー ス管理システム」の導入が完了しました(2011年4月まで の延べ数)。

プライバシーマークの認証取得と更新

新たにキヤノンプリントスクエア、オーエーエルがプラ イバシーマークを取得し、グループ内のプライバシーマー ク取得企業は15社となりました。キヤノンシステムアン ドサポート、キヤノンソフトウェアがプライバシーマーク 認証の更新を行いました。

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、さらにセキュリティレベルに応じて、生体認証なども導入しています。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や情報漏えいリスクの軽減効果を上げています。



IDカードを用いた入館チェック



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 書類を施錠付きのワゴンやロッカーボックスへ収納し、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、機密情報の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

グループ全体最適を考えたITセキュリティ

キヤノンMJグループでは、グループ統一のITセキュリティ ポリシーに基づき、ネットワークインフラ統制、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インフラ の統合管理を行っています。

これにより、グループ内の対策レベルの均質化と運用コスト の削減を両立し、安全で使いやすい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セキュリティガバナンスの全体像

キヤノンMJグループITセキュリティポリシー

キヤノンMJグループ統合インフラ統制 システム・アプリケーション統制 パソコン・メディア統制 ●グループ統合基幹システム ●パソコンの標準化・ ●グループ統合ファイルサーバー ライフサイクルマネジメント ●グループポータル ●社内標準ソフトウエア ●スパムメール対策 ●ウイルス対策ソフト ●メール添付ファイル自動暗号化 ●パソコンのハードディスク暗号化 ●ファイル転送サービス ●PCセキュリティチェッカー キャノンMJ グループ会社 キヤノンMJ ●電子メールモニタリング ●OSセキュリティパッチ適用自動化 ●高速通信モバイル ●セキュリティ機能付きUSBメモリ ●社有携帯電話ウェブメール 運用·管理 利用 ネットワークインフラ統制 ●ネットワーク集中管理 ●IPアドレス管理 ●ログ管理 ●ウェブフィルタリング グループ製品の積極活用 運用ノウハウのフィードバック

■積極活用しているグループ製品の例

セキュリティ対策	製品と取扱会社	
電子メールモニタリング	「GUARDIAN」シリーズ	
	GUARDIAN シリーズ	取扱会社:キヤノンITソリューションズ 製品の概要はP23-24をご参照ください。
パソコンのハードディスク暗号化	CompuSec	
	CompuSec	取扱会社:キヤノンITソリューションズ 製品の概要はP23-24をご参照ください。
ウイルス対策ソフト	ESET NOD32アンチウイルス	
	ESET NOD32 Antivirus	取扱会社:キヤノンITソリューションズ 製品の概要はP23-24をご参照ください。

Action 2010 2010年の取り組み

PCセキュリティチェッカーを導入

キヤノンMJグループでは、パソコンのOSや社内標準アプリケーションのセキュリティパッチの適用およびウイルス定義ファイルの更新を自動化していますが、一部のアプリケーションやオフラインのパソコンについては手動での適用が必要です。

そこで、グループ標準のセキュリティ設定やセキュリティパッチの適用状況を利用者本人によって簡単に確認するためのツール「PCセキュリティチェッカー」のオンライン版、オフライン版を開発・導入しました。

メール添付ファイル自動暗号化

添付ファイルのついたメールを送信する際に、誤送信や 通信経路上での盗聴を防止するため、メールサーバー上で すべての添付ファイルを自動的に暗号化して送信するしく みを、グループ内で導入しました。

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ました。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。

情報セキュリティ人材の育成

人的セキュリティが重要であると考え、さまざまな工夫によって情報セキュリティの MATION SECT 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、高い情報セキュリティマインドと情報資 産を適切に取り扱うことができる基礎知識を持ち、正しい行動が できるよう、さまざまな場面で意識啓発や教育を実施しています。

また、情報セキュリティに関するマネジメントシステムを運 用し継続的に改善するために、各職場に専門知識を持ったスペ シャリストも育成しています。

■情報セキュリティ人材を育成するしくみ



スペシャリストの育成 ISMS推進担当者 個人情報保護キーパーソン ISMS構築•運用専門知識 PMS運用専門知識 内部監査員 内部監査専門知識

正しい知識と行動

マネジメントシステム運用・継続的改善

すべての従業員を対象とした意識啓発と教育

●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 キュリティマインドを醸成しています。

●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

●情報セキュリティに関する情報配信

情報セキュリティマインドの定着には、定期的な教育だけで なく、日常的な意識啓発が重要です。

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。

スペシャリストを育成する教育

情報セキュリティを組織ごとに異なる業務プロセスへ適切に 組み込むためには、各組織に情報セキュリティに関するスペシャ リストを配置し、推進することが有効であると考えています。 そこで、キヤノンMJグループでは、個人情報保護に関する 専門的な知識を持つ「個人情報保護キーパーソン」、ならびに ISMS取得部門では、「推進担当者」や「内部監査員」を育成して います。こうして育成された「スペシャリスト」が組織の情報セキュリティを推進しています。

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

Action 2010 2010年の取り組み

コンプライアンス・ミーティングに情報セキュリティのケーススタディを導入

2010年下期の「コンプライアンス・ミーティング」は、 複数のケーススタディを用いて実施しました。この中で、 7割近くの職場が「情報紛失」のケースを選択し、登場人物 の問題行動と組織としての予防策について議論しました。 ケーススタディ形式の採用により、具体的で積極的な意見 交換につながり有効な活動となったことが、ミーティング 開催後のアンケートで確認されました。

「情報セキュリティトレンド」で配信したテーマ

- ●個人情報漏えいインシデントの傾向【2009年上半期】
- ●『国民を守る情報セキュリティ戦略』の策定
- ●「情報セキュリティ2010」の策定

スペシャリスト育成の実績

■教育実施人数および累計人材数

対象者	実施人数	累計人材数	
個人情報保護キーパーソン	31名	380名	
ISMS推進担当者	1,825名	3,333名	
ISMS内部監査員	66名	485名	

「今週のコンプライアンス」で 配信したテーマ

- ●社外に持ち出したPCの管理
- ●ソフトウェア管理
- ●情報持ち帰りの危険性
- ●メール送信時のミスを防ぐための注意事項
- ●個人情報の適正管理と有効活用
- ●不正競争防止法の一部改正施行 営業秘密管理の 強化ポイント
- ●ファイル転送サービスの活用

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」などを通じて、自社の取り組みを積極的に開示しています。また、自社の情報セキュ リティに関するノウハウをお客さまへの価値提供に活かすことで、セキュアな社会の実現に貢献しています。

「情報セキュリティ報告書」の発行

キヤノンMJグループは、2008年から毎年「情報セキュリ ティ報告書」を発行しています。

この報告書は、情報セキュリティ活動について報告し、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 提供することを目的としています。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」を参考にしています。 2010年より、環境にも配慮し冊子としての発行は行わず、 ウェブサイトへの掲載による報告に切り替えました。ウェブサ イトでは情報の更新性の側面を、PDFでは読みやすさの側面を 重視して編集しました。

「オフィスツアー」によるセキュリティ事例紹介

キヤノン S タワーや各支店等で実施している 「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 各種取り組み事例をプレゼンテーションやフロア見学を通じて 紹介しています。

情報セキュリティに関する取り組み事例としては、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

への取り組み方法、セキュリ ティ対策の実践事例および人材 育成などについて具体的に説明 しています。



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への支援

キヤノンMJグループは、下記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 情報サービス産業協会
- ●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

- ●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)

Action 2010 2010年の取り組み

「情報セキュリティ報告書2010」の発行

「キヤノンMJグループ 情報セキュリティ報告書2010」 を発行しました。キヤノンMJグループの情報セキュリティ

の取り組みに関し、定常的に報告 する内容と2009年に取り組んだ活 動や成果をわかりやすく報告して います。



教育分野への協力

キヤノンITソリューションズでは、学生の研究分野につい ての理解をより深めることを目的に、大阪大学大学院情報科 学研究科の「マルチメディア工学特別講義」に講師を派遣し、 情報セキュリティ分野の講義を3回(計6時間)行いました。

講義では、最近の情報 セキュリティに関する潮 流や産業界での技術動向 について、解説しました。

> マルチメディア工学 特別講義の様子



お客さまへの安心・安全の提供

業務プロセスにおける情報セキュリティ品質の向上や、質の高い情報セキュリティ製品・ ソリューションを通じて、お客さまへ"安心""安全"といった価値を提供しています。

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向上

キヤノンMJグループでは、営業やサービス、ソフトウエア 開発などの業務プロセスごとに、お客さまの期待や情報セキュ リティリスクをきめ細かく把握して、「より安全に」「より確実 に] 「より効率的に] といったプラス効果を出すために、業務プロセスの改善や必要な対策を継続的に行っています。

●安全で安心していただけ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、全国に約200の拠点を展開し、営業・サービス・サポートが一体となり、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行っています。キヤノンS&Sのカスタマーエンジニアは、お客さまに安心して複合機やプリンターなどの保守サービスを受けていただくために、そのプロセス上で考えられるリスクへの対応策を十分に検討し、実践しています。



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ごとのリスクと情報セキュリティ対策事例

プロセス

外出前(社内)

修理受付

(移動中)

リスク

- サービス工具(パソコン・USB メモリ)の紛失・ウイルス感染
- 修理受付用の携帯電話の紛失
- サービス工具・伝票の紛失

情報セキュリティ対策事例

- ●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。
- ●パソコンを持ち出す際にはPC社外利用申請システムにて 所属長の承認を得ています。
- ●USBメモリは台帳管理を行い、日々の持ち出し・持ち帰り管理を 行っています。
- 携帯電話にはオートロック機能、遠隔ロック機能、 セキュリティ監視機能を実装しています。
- ●パソコン・伝票類は工具カバンに収納し、常に携行しています。

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やお客さまのネットワークへ 接続する際には上長の許可を得た上で、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。
- ●代替機をお貸し出しする際には、本体内の情報確認と 作業完了時に情報の全消去を実施しています。

帰社後 (社内)

- お客さまよりお預かりした データの漏えい
- ●セキュリティ意識·知識の欠如
- 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。
- ●定期的に、サービスメンテナンス時に必要なセキュリティ対策に 関する教育を実施しています。

お客さまへの安心・安全の提供

INFORMATION SECURITY

お客さまの情報セキュリティ課題解決への貢献

●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化がますます加速しています。IT導入には、自社ネットワークへの不正侵入や、コンピュータ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。

●トータルセキュリティソリューションの提供

■セキュリティソリューションの全体像

セキュリティ対策に必要な要件を、「ゲートウェイ」「サーバー」「エンドポイント」「プリンティング」「物理」「マネジメントシステム」の6つのカテゴリーに分けて体系化しています。

ITによるセキュリティ環境の構築はもちろんのこと、セキュ

リティマネジメント構築、セキュリティ監査、従業員教育、認 証取得に至るまで、企業のセキュリティ強化に必要なソリュー ションをトータルに提供しています。

Internet 物理セキュリティ ●映像監視 ゲートウェイセキュリティ ●ファイアウォール ■ネットワークフォレンジック ●統合脅威管理(UTM) ●電子メールフィルタリング・ ●スパムメール対策 アーカイブ サーバーセキュリティ ●電子メール誤送信対策 ウェブ情報漏えい対策・ ●ウェブアプリケーション ●データベース監視 ●仮想プライベート 不正サイト閲覧制御 ファイアウォール ●ファイルサーバー監視 ネットワーク(VPN) ●中小オフィス向け ●アクセス制御 IT支援サービス ●脆弱性検査 プリンティングセキュリティ エンドポイントセキュリティ ●コンピュータウイルス対策 ●パーソナルファイアウォール ●個人認証 ●画像口グ管理 ●脆弱性管理 ●ID管理 ●セキュアプリント ●地紋印刷 ●IT資産管理 パソコンログイン認証 ●印刷履歴管理 ●クライアント運用管理 ●ファイル持ち出し制御 マネジメントシステム ●ドキュメントセキュリティ ●シンクライアント ●セキュリティポリシー策定 ●ISO27001認証取得 ●プライバシーマーク認証取得 ●従業員教育

内部統制/IT統制

オフィス向け複合機「imageRUNNER ADVANCE」におけるセキュリティ対策

複合機は、コンピュータ機器と同様にお客さまの情報システム環境に接続され、情報ポータル機器としての活用が広がっています。それに伴い、お客さまが守るべき機密情報が紙の出力物、内蔵ハードディスク、データ通信、電子化データ上に残存するケースが生じ、これらを放置すると情報漏えいの原因となるおそれもあります。

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。

●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、ハードディスク内のデータを自動的に暗号化**!します。

「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*2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。

※1 [HDDデータ暗号化/ミラーリングキット・C1]が必要です。 ※2「データ消去キット・C1」が必要です。

■本体データを守る「HDDデータ暗号化」「自動消去」



●複合機から紙出力した機密情報の漏えい対策

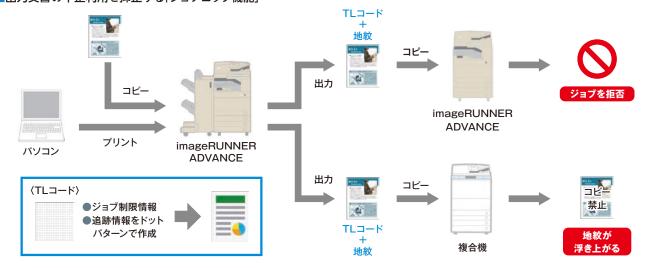
コピーやプリント時に、TLコード (低可視のドットパターン情報) で作成されたジョブ制限情報や追跡情報を埋め込み、ジョブ動作のロックや追跡情報 (5W1H) の取得を可能にします。

さらに地紋印字と組み合わせれば、ジョブロック未対応機器

を利用した際にも「コピー禁止」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・A1」「イメージ解析ボード・A1」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」



中小オフィス向けIT支援サービス「HOME」におけるセキュリティ対策

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。

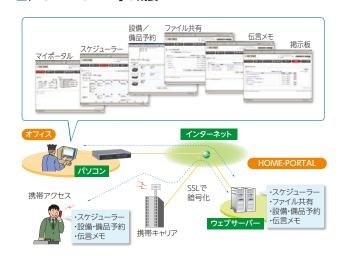
■「HOME-UNIT」のセキュリティ対策

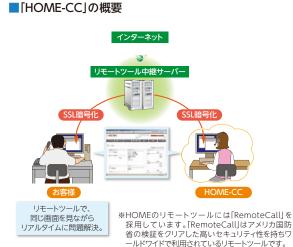
セキュリティ対策	セキュリティ対策の内容
ファイアウォール	外部からの不正なアクセスや侵入を防止し、内部のネットワークの安全を維持します。
アンチウイルス	シグニチャやヒューリスティック・エンジンを自動的に更新して、新種のウイルスやスパイウェアが社内に侵入することを防ぎます。
アンチスパム	多段階のフィルターでメールをチェックし、スパムの可能性があるメールを自動検知します。
ウェブフィルタリング	業務に不適切なウェブサイトへのアクセスを制御し、ネットワークセキュリティへの脅威と帯域の無駄遣いを防ぎます。
不正侵入検知/防御	WinnyなどのP2Pソフトの通信を遮断し、社内からの情報漏えいを防ぎます。

●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(「スケジューラー」「設備/備品予約」「伝言メモ」「ファイル共有」「掲示板」「携帯アクセス」)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。

■「HOME-PORTALIの概要





●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わせに対し、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。

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。

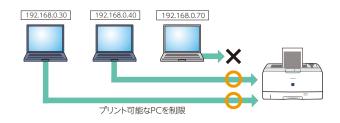
■ID印刷機能



●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



セキュリティソリューションのご紹介

企業が抱えるセキュリティリスクを軽減させるため、リスクに合わせて具体的にご提案します。

エンドポイントセキュリティ

ウイルス・スパイウェア対策ソフトウエア

ESET NOD32 Antivirus

ウイルス定義データベースにない "新種のウイ ルス"を検出することができる「ヒューリス ティック機能」を搭載した強力なウイルス対策ソ フトウエアです。「ThreatSenseテクノロジー」 を搭載し、ウイルスやマルウェアを検出・駆除 します。検査中も他のアプリケーションに影響 することなく、パソコンは軽快に動作します。 開発元: ESET.s.r.o.



総合セキュリティソフトウエア

ESET Smart Security

コンピュータウイルス・スパイウェア対策機 能を備えた [ESET NOD32アンチウイルス] に パーソナルファイアウォールと迷惑メール対策 機能を搭載した総合セキュリティソフトウエア です。



開発元: ESET.s.r.o.

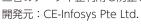
OS起動前認証/ハードディスク全体暗号化

CompuSec

モバイルパソコンやデスクトップパソコンを対象に1台から導入 いただける認証・暗号化セキュリティソフトです。OS起動前に行う

個人認証やハードディスクの全体暗号化をはじ め外部記憶装置や電子メールの暗号化などのさ まざまなセキュリティ機能を備えています。

これにより、パソコンの盗難や紛失時の情報 漏えいを防ぎ、パソコン廃棄時に問題となる第 三者のデータ不正利用も防止します。





IT資産管理

QND Plus

クライアントの現状把握から、台帳作成、自動インストール、脆 弱性検査までをカバー。情報システム管理者の管理工数を削減し、 コンピュータウイルスや情報漏えいなどのITセキュリティリスクか ら企業を守ります。

ESETシリーズとの連携によりパソコンへのウイルス対策ソフトイ ンストールの作業負荷軽減および、パソコンごとのセキュリティ対 策状況の管理負荷軽減を実現します。 ND Plus

開発元: クオリティ株式会社



クライアント運用管理

SKYSEA ClientView

使いやすい操作画面と、情報セキュリティ対策に必要な機能をオー ルインワンでご提供。SKYSEA ClientViewは、情報セキュリティ対 策からIT資産管理・ログ管理、コスト削 減をまとめて解決するソフトウエアです。 開発元: Sky株式会社



ICカードによるパソコンログイン認証

ARCACLAVIS Revo

サーバー/クライアント型の多機能ICカード認証ソリューション です。Windowsへのログオン認証のほか、フォルダ単位、ハードディ スクドライブ単位の自動暗号化/復号や業務システムへのシングル サインオン、さらにはUSBメモリなどの外部デバイス使用制御機能 などを提供します。

開発元:ジャパンシステム株式会社

VARCACLAVIS Revo

ドキュメントセキュリティ

Adobe LiveCycle Rights Management ES PDFファイルの閲覧制限や印刷、編集等の操 作権限などをサーバーでポリシーとして一元管 理することで配信後であっても、動的に制御・ 管理できるPDFドキュメントセキュリティソ リューションです。



開発元: Adobe Systems Incorporated.

ドキュメントセキュリティ

PDFPolicy Service

企業内・企業間でやりとりされるPDF形式・Microsoft Office形 式の機密文書を、ポリシー(利用権限・有効期限等)を付与すること でセキュアに保護する、Adobe LiveCycle Rights Management ES2をベースとしたSaaS型の機密情報保護基盤です。

サービス提供元:キヤノンITソリューションズ株式会社

PDFPolicy Service

PDFポリシーサービス

シンクライアント

Citrix XenApp/XenDesktop

サーバー(中央)でアプリケーションと情報を集中管理し必要に応 じてエンドユーザーにクライアント環境を配信する仮想環境を構築 することで、強固なセキュリティ、管理コスト削減、生産性向上を 実現するWindowsアプリケーション

デリバリー製品です。

開発元: Citrix Systems,Inc.



ゲートウェイセキュリティ



統合脅威管理アプライアンス

SonicWALL

さまざまな規模のネットワークに対応するファイアウォール、IPS (侵入検知・防御)、ゲートウェイアンチウイルス、アンチスパイウェ ア機能などに対応します。

強力なUTM (統合脅威管理) ソリュー ションを優れた操作性と圧倒的なコス トパフォーマンスで提供します。

開発元: SonicWALL, Inc.



統合脅威管理アプライアンス

FortiGate

企業のインターネットゲートウェイに必要な9つのセキュリティ機能(ファイアウォール、IPsec-VPN、SSL-VPN、アンチウイルス、Peer to Peerファイル型交換ソフト対策、インスタントメッセンジャー対策、ウェブコンテンツフィルタリング、IPS、アンチスパム)を1台で実現するUTMアプライアンスです。

開発元: FORTINET INC.



スパムメール対策アプライアンス

SpamHunter

スパムメールの脅威から企業ネットワークを守る、アプライアンス製品です。リーズナブルでありながら高い検出率と低い誤検知率を誇ります。標準でアンチウイルスや誤送信防止などの機能を搭載。 さらに複数のモードを選択可能なため、さまざまなネットワーク環境のお客さまに導入いただくことが可能です。

開発元:株式会社セキュアソフト



電子メールフィルタリング・アーカイブ

GUARDIANWALL

キヤノンITソリューションズが開発・販売する国内シェア57.3%*のメールフィルタリングソフトです。個人情報や知的財産の漏えいを防ぐメールフィルタ機能と、内部統制やEディスカバリー対応に重要な役割を果たすメールの可視化/保全を実現するアーカイブ機能を搭載しています。

上司や監査担当者が、保存されたメールに対し、監査を簡単に実施できる機能を活用することで、メールコンプライアンスの強化が実現できます。

※株式会社富士キメラ総研 [2010ネットワークセキュリティビジネス 調査総覧 | より

GUARDIANWALL

ガーディアンウォール

電子メール誤送信対策

GUARDIAN CorrectMail

電子メールの誤送信は、主にヒューマンエラーが原因であり、技術的な対策が困難なため、各組織で大きな課題となっています。 「GUARDIAN CorrectMail」は、送信者本人や上長による確認、ccに同報されている社内の第三者による気づきによって、誤った電子メールを外部に配送する前に取り消すことで、誤送信の防止に役立ちます。

GUARDIAN CorrectMail

ウェブ情報漏えい対策・不正サイト閲覧制御 WEBGUARDIAN

圧倒的シェアを誇るメールフィルタリングソフト「GUARDIAN WALL」の技術を応用して作られたのが、ウェブフィルタリングソフト「WEBGUARDIAN」です。ウェブの閲覧制限だけではなく、外部に送信するデータのコンテンツチェックや、アーカイブ機能を搭載しています。ウェブメールや掲示板・ブログ・SNSサイト、オンラインストレージサイトなどに送信するすべての内容を保存するため、内部統制の強化が容易に実施できます。

また、標準搭載のレポート機能を活用いただくことで、ウェブの 利用実態や課題の発見ができます。

WEBGUARDIAN

ウェブガーディアン

サーバーセキュリティ

セキュリティアウトソーシングサービス

SiteScan2.0 Enterprise Edition

インターネットに公開しているお客さまのウェブサーバー・ファイアウォールの脆弱性を定期的に検査、いち早くシステムリスクの評価・報告をすることで情報漏えい対策をサポートします。

IT全般統制ソリューション

キヤノンMJでは、自社が米国SOX法に対応したIT全般統制事例を 公開しています。

IT全般統制確立の核となる、ID管理、アクセス制御そしてデータベース監視ソリューションを中心にお客さまの課題に即した提案を行っています。

- ●ID管理(CA Identity Manager 開発元: CA, Inc.)
- ●アクセス制御(CA Access Control 開発元: CA, Inc.)
- ●データベース監視(Chakra 開発元: WareValley Co. Ltd)

物理セキュリティ

■ 映像監視

ネットワークカメラ

「ネットワークカメラVB」シリーズと「ネットワークビデオレコーダーVK-64/VK-16」により、コンピュータルームや文書保管室など、重要な情報が保存されている場所に対しては、人の行動を監視し、記録する、といった物理的対策を行うことが可能です。





キヤノンマーケティングジャパングループ概要

会計概要

(2010年12月31日現在)

会社名: キヤノンマーケティングジャパン株式会社

設立:1968年2月 資本金: 73,303百万円

従業員:連結:18,571名 単独:5,298名

本社: 東京都港区港南2-16-6 CANON S TOWER 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



グループ会社紹介

(2011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)
- ●キヤノンプリントスクエア(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)
 - ●エス・エス・ジェイ(株)
 - ●(株)AES
 - ●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)
 - ●佳能控制系統(上海)有限公司
- ●キヤノンソフトウェア(株)
 - ●キヤノンソフト情報システム(株)
 - Canon Software America, Inc.
- ●エディフィストラーニング(株)

コンスーマイメージング

- ●キヤノンカスタマーサポート(株)
- ●キヤノンフィールドアシスト(株)
- ●ウイズフォト(株)

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

事業紹介

ビジネスソリューション

キヤノン製品を中心に多彩な製品・サービスで、オフィスに新しい価 値を提供します。

ITソリューション

お客さまのビジネスに、ITを最適な形で組み合わせ、業務効率と競争 力の向上に貢献します。

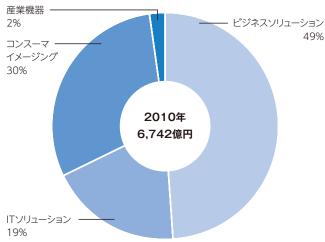
コンスーマイメージング

写真や映像の新しい魅力を伝え、毎日を楽しく豊かにするフォトライ フをお届けします。

産業機器

私たちのくらしを支える半導体製造、医療、放送という業界に、世界 の最先端機器と専門性の高いソリューションを提供します。

キヤノンMJグループ 連結部門別売上高構成



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 改訂日 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

