

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 2012

Information Security Report 2012



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”にとらえて、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2011年（2011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

お問い合わせ先

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

28 キヤノンマーケティングジャパングループ概要

トップメッセージ

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“暮らし、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、昨年、2011年から2015年までの長期経営構想フェーズⅡをスタートさせました。ミッションとしては「安心安全で豊かな“暮らし、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。

この取り組みを開始した直後に東日本大震災を経験し、改めて、私たちのミッションの持つ意味の重要性を痛感しました。安心・安全をお客さまに提供し続けていく上で、特に「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。

昨今、サイバー攻撃の高度化や電力の安定供給への不安など、情報セキュリティに関わる新たな脅威が出てきています。こうした新たな脅威に適時対応していくためにも、しっかりとしたグループ全体の情報セキュリティガバナンス体制・マネジメントシステムを整備し、継続的に運用のスパイラルアップを図っていくことが重要と考えています。

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の使命を持っていますので、「企業の社会的責任としての情報セキュリティ基盤強化」だけでなく、「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」を加えた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。

具体的には、グループ統合の情報セキュリティマネジメントシステム(ISMS)によって、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。

また、営業・保守サービス・ソフトウェア開発等のプロセスごとに、事業部門が主体となってリスクアセスメントを行い、お客さまへ価値を提供するプロセスの品質を高めていくことで、「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。

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っています。これらを含めて、お客さまの情報セキュリティ課題の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。本報告書をご覧ください。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

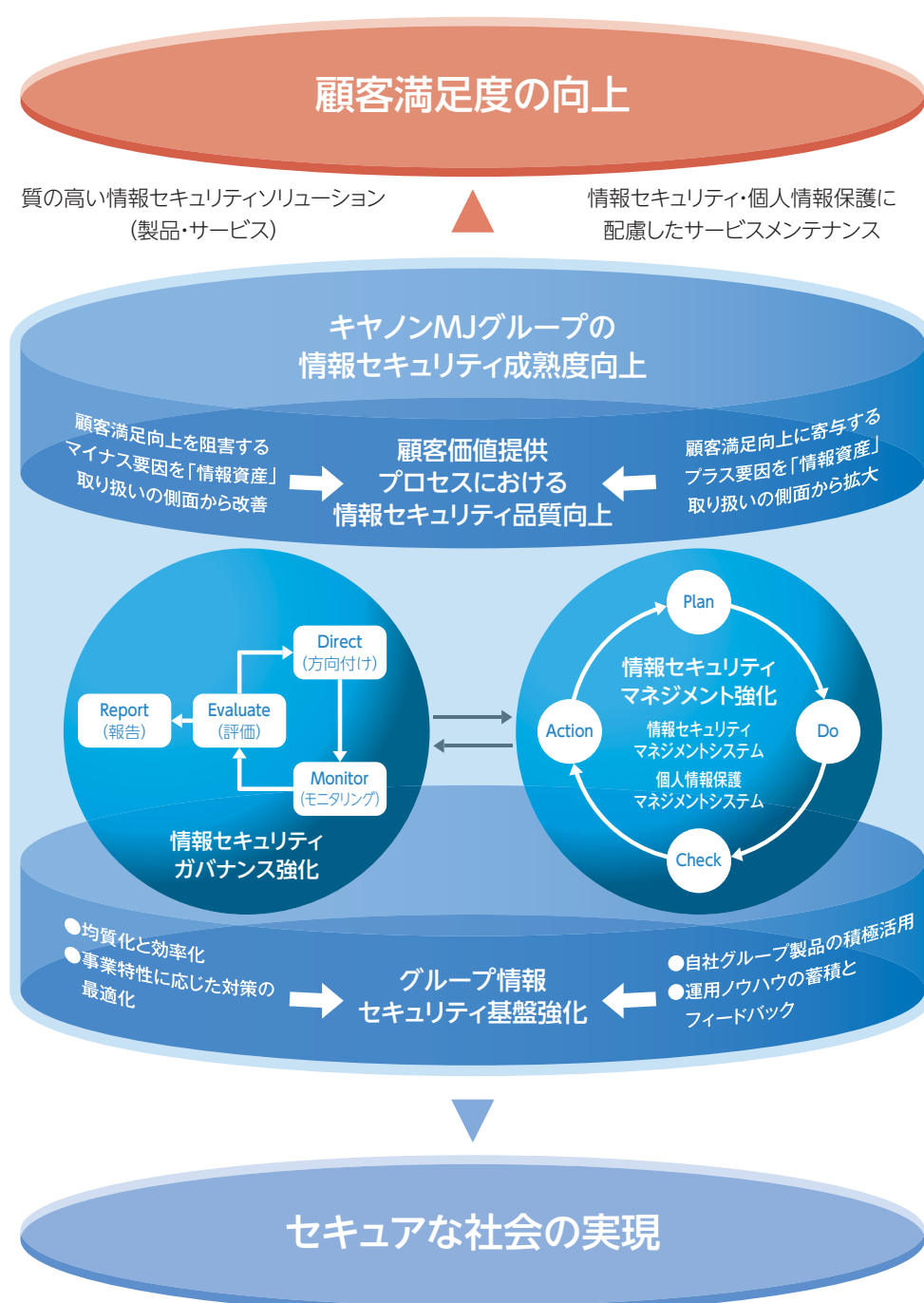
推進フレームワークと主要テーマ

キャノン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改善す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



情報セキュリティマネジメント

体系的にルールを整備

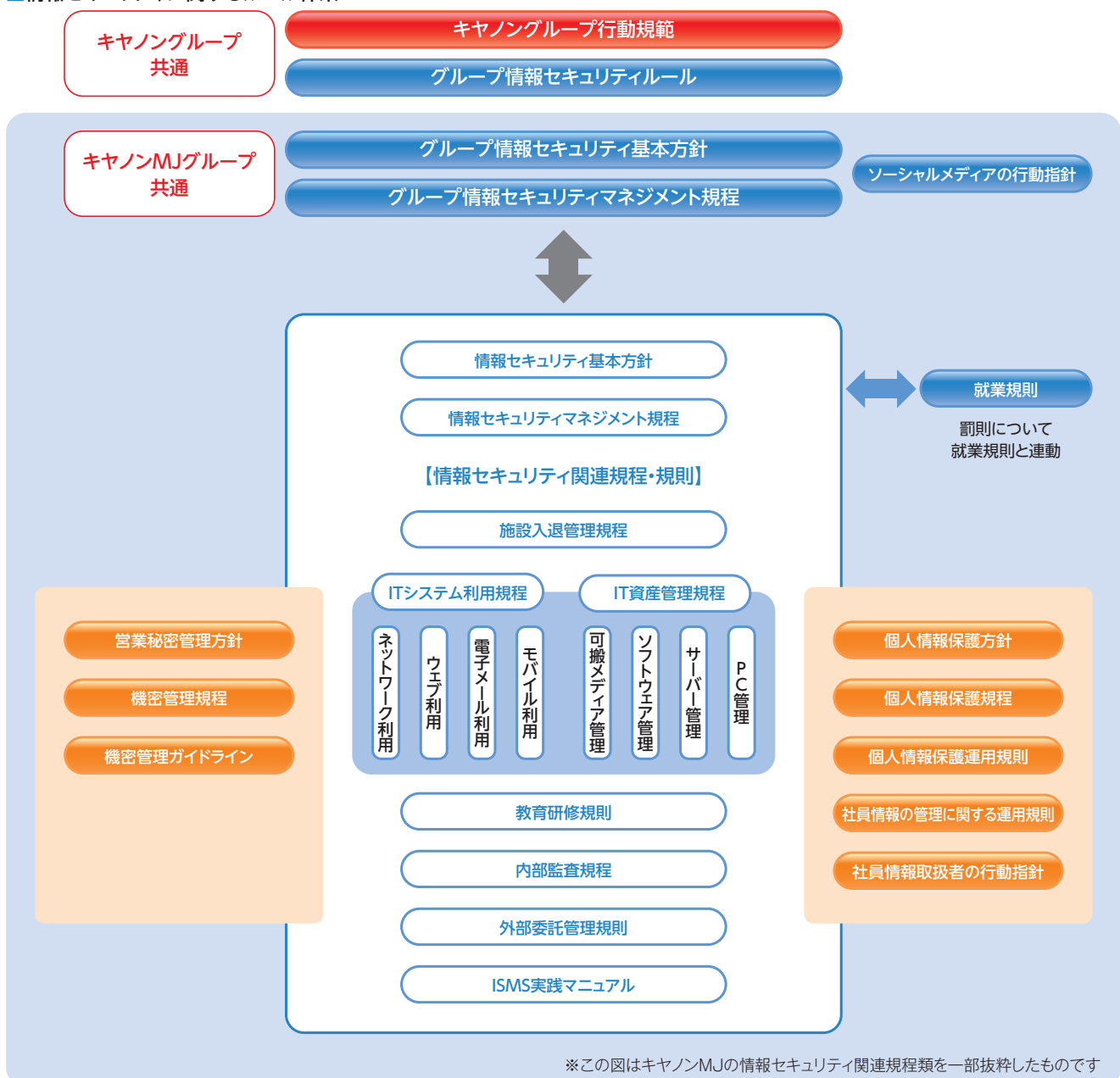
キャノンMJグループでは、キャノン(株)のグローバル基準である「グループ情報セキュリティルール」(ISO/IEC27001:2005に準拠)を基軸としながら、グループ全体の情報セキュリティを推進するための幹となる「グループ情報セキュリティ基本方針」と「グループ情報セキュリティマネジメント規程」を制定しています。

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



※この図はキャノン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

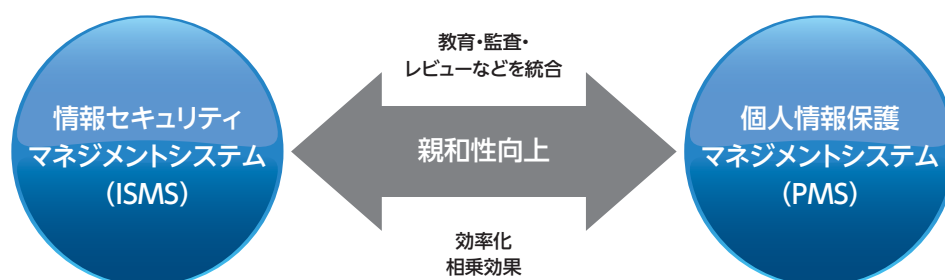
情報セキュリティマネジメント

▶ マネジメントシステムの連携による効果的な運用

キャノン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



▶ 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

キャノン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等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高感度の内容の場合には、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。

グループ会社間で業務委託を行う場合であっても、均質的な情報セキュリティマネジメント体制を構築していることを踏まえて、効率的かつ効果的な管理・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等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。

▶ 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取得
- コンピュータ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。

キャノンMJでは、2010年より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 2011 2011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

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。2011年の主な報告・承認事項は、以下の通りです。

- キヤノンMJグループのウェブサイト不正アクセス対策の報告
- キヤノンMJグループにおけるプライバシーマークの活用方法に関する承認
- 営業秘密管理実態調査の実施に関する報告
- ISMSグループ統合認証審査結果報告

ソーシャルメディアの利用に関する 細則の制定

キヤノンMJグループの各部門がソーシャルメディアを利用した情報公開・配信、および利用者とのコミュニケーションを行うための手順を定め、ソーシャルメディアによる情報公開の安全かつ円滑な運営を図ることを目的に「ソーシャルメディアの利用に関する細則」を制定しました。

パートナー企業の 情報セキュリティ品質の向上

複合機の保守サービス業務を委託しているパートナー企業796社に対し、お客さま先でのサービスマンテナンスプロセスにおける情報セキュリティ対策状況を調査（書面監査）致しました。評価基準を設け、基準に達していない企業には改善をお願いし、サービスマンテナンス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みました。

また、ソフトウェア開発業務を委託しているパートナー企業で当該業務に新たに従事する方を対象に、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600名強の方が受講しました。

委託先ウェブサイトの安全対策の 確認と強化

企業のウェブサイトを対象とした不正アクセス攻撃の増加傾向を踏まえ、ウェブサイトを利用して個人情報を取得する業務の委託先、およびASPサービス事業者、合計15社に対して、IPA（独立行政法人情報処理推進機構）より公表されたチェックシートを参考にして、安全対策の確認を行い、必要に応じて対策の強化を行いました。

「インシデント管理システム」の グループ展開

グループ会社4社へ「インシデント管理システム」を展開しました。

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取り組んでいます。

▶ 第三者認証の活用目的

キャノンMJグループが第三者認証を活用する目的は、「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、事業上の必

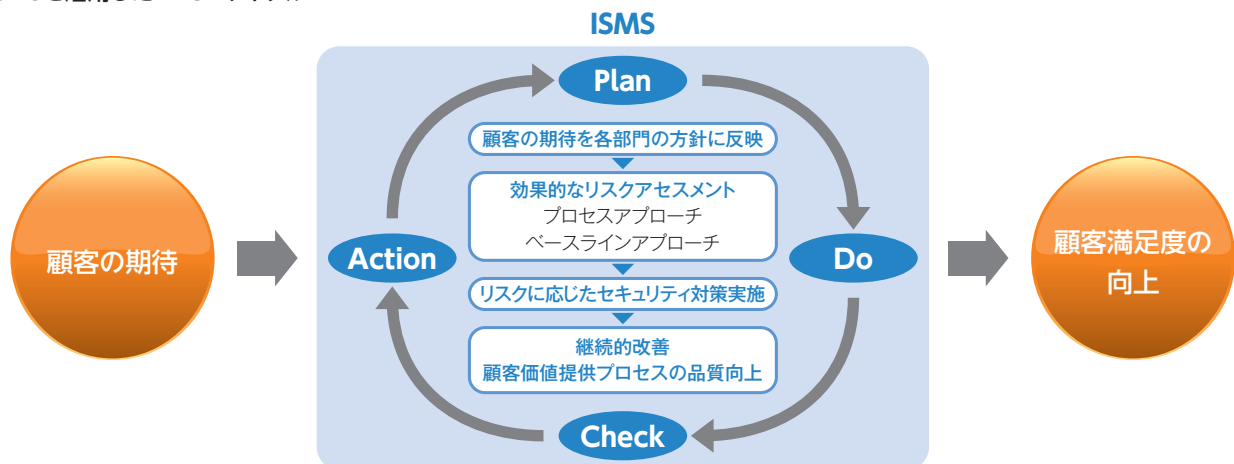
要性に応じて認証を取得することによって、お客さまに客観的判断基準を提供できていると考えています。

▶ ISMSを活用した顧客満足度の向上

キャノンMJグループのISMS（情報セキュリティマネジメントシステム）活動は、情報セキュリティ基盤強化に加えて、お客さまに価値を提供するプロセスの情報セキュリティ品質の向上と、お客さまの情報セキュリティ課題解決への貢献をしていくことで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、グループ共通のセキュリティ対策のほか、お客さまの期待を明確化し、営業やサービスなどの業務プロセスごとにきめの細かいリスクアセスメントを行い、事業特性に応じたセキュリティ対策を実装しています。

■ 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



第三者認証の効果的な活用

▶ プライバシーマークを活用した個人情報保護の強化

JISQ15001に準拠した個人情報保護マネジメントをグループ全社で推進

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、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

ネジメントを推進しています。

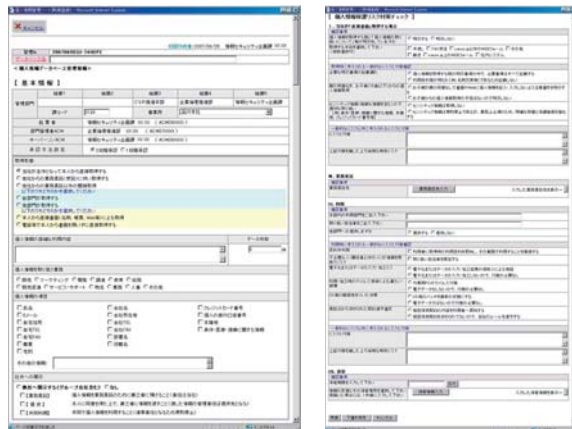
また、事業上の必要性に応じてプライバシーマーク認証を効果的に活用しています。

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、グループ各社の個人情報保護担当者を集めた「グループPMS担当者会議」を定期的で開催しています。この会議ではグループ各社の個人情報保護活動の好事例や、各社の抱える課題とその改善方法を共有し、グループにおける個人情報保護レベルの均質化と運用の効率化を図っています。

また、「個人情報データベース管理システム」を独自に開発し、グループ各社への展開と運用によって、JIS規格に準拠した個人情報の取り扱いを効果的に実現しています。

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、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長

- 法的要求事項やJIS規格に沿った運用のチェック
- 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
- 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。

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。

第三者認証の効果的な活用

■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	○	○
キヤノンシステムアンドサポート	○	○
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		—
佳能信息系统(上海)	○	—
キヤノンソフトウェア	○	○
キヤノンソフト情報システム	○	○
エディフィストラニング	○	
キヤノンビジネスサポート	○	○
オーエーエル	○	○
日本オセ		
キヤノンプリントスクエア	○	○
昭和情報機器		
キヤノンカスタマーサポート	○	○
キヤノンフィールドアシスト	○	○
ウイズフォト		
エルクコーポレーション		○
エルクエスト		
ユニオン・メディカル		
台湾佳能先進科技股份		

2012年5月1日現在

Action 2011 2011年の取り組み

ISMSグループ統合認証の実現

2011年はISMS認証の統合範囲をグループ18社へ拡大し、グループ統合認証を実現しました。

プライバシーマークの認証取得と更新

2011年は、キヤノンマーケティングジャパン、キヤノンITソリューションズ、キヤノンビジネスサポート、キヤノンフィールドアシスト、キヤノンビズアテンダ、エス・エス・ジェイ(2012年5月1日付で「スーパーストリーム」に社名

変更)がプライバシーマークの更新を行いました。

なお、新たにグループ入りしたエルクコーポレーションを含め、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。

「個人情報データベース管理システム」のグループ展開

2011年に新たに展開したグループ会社を含めて合計9社で「個人情報データベース管理システム」を運用しています。(2011年12月までの延べ数)

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あげています。



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

情報セキュリティ対策の実装

▶ 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統制の全体像



情報セキュリティ対策の実装

■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 ガーディアン	取扱会社：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	CompuSec CompuSec コンピュセック	取扱会社：キヤノンITソリューションズ
ウイルス対策ソフト	ESET NOD32アンチウイルス ESET NOD32 Antivirus イーセツ エヌオーディー32 アンチウイルス	取扱会社：キヤノンITソリューションズ

Action 2011 2011年の取り組み

外部サイトの脆弱性対策

キヤノンMJグループでは、世界的に急増しているウェブサイトへの攻撃に対する対応の一環として、第三者機関によるウェブサイトのセキュリティ検査を実施しました。

入退出管理の強化

各事業所の入退出管理について、一部の事業所に対し、「フラッパーゲート」を導入し、共連れを防止するなど、物理的なセキュリティを強化しました。

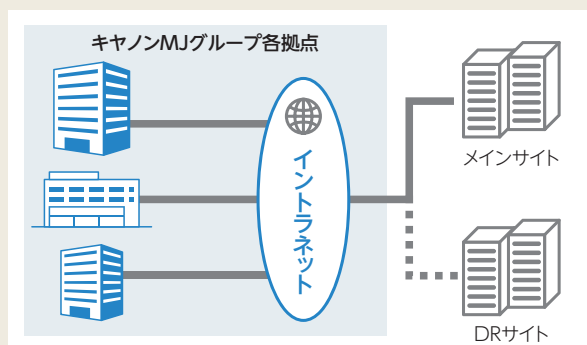


港南事業所のフラッパーゲート

災害対策ディザスター・リカバリーを構築

東日本大震災を機に、キヤノンMJグループでは基幹システムのディザスター・リカバリー(DR) サイト※を2011年7月に構築しました。

※DRサイト (Disaster Recovery Site)：地震などの災害により、メインシステムのサーバーが破壊されたり、障害を受けて機能が停止したり、データが消失することを防ぎ、不断の事業継続を行うために構築するバックアップ機能を有するサイト。



震災発生時の安否確認システムによる従業員の安全確認

震度5強以上の地震やその他の災害・新型インフルエンザなどが発生した際に、対象地域の従業員に対して、携帯電話・メールなどを利用して従業員の安否の確認や、緊急連絡を行うためのシステムをグループ内で導入しています。

2011年は、3月11日に発生した東日本大震災でこのシステムを利用し、安否確認を行いました。また、有事の際に備えた安否確認通報訓練を2回実施しました。

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



▶ 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。

情報セキュリティ人材の育成

▶ 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、「ISMS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 2011 2011年の取り組み

「コンプライアンス・ミーティング」の実施

2011年上期の「コンプライアンス・ミーティング」では、営業秘密・ハラスメント・著作権法・下請法の4つのケース（事例）から一つのテーマを選択する手法で実施しました。

下期には、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、独占禁止法や情報管理等、13のコンプライアンスリスク例を参考にしながら議論しました。

「コンプライアンス・ミーティング」を通じて、情報セキュリティ意識の向上にもつながっています。

「情報セキュリティトレンド」で配信したテーマ

- 情報セキュリティに忍び寄る脅威
～2011年脅威発生予測～
- 大規模な個人情報漏えい事故を教訓にしよう!
- 『情報セキュリティ報告書』でお客さまとのコミュニケーションを!
- 『情報セキュリティ2011』に見る国の政策と我々のビジネス

「今週のコンプライアンス」で配信したテーマ

- 情報を安全に取り扱うためのルールとツール
- ソーシャルメディア・公共の場での情報管理
- メール送信時の確認
- プライベートにおける情報セキュリティへの注意事項
- キヤノンMJグループのISMS活動を再確認しよう
- 不審メールに注意
- 秘密保持契約の締結を求められた際の注意点

スペシャリスト育成の実績

■ 教育実績および累計人材数

対象者	実施人数	累計人材数
個人情報保護キーパーソン	231名	611名
ISMS推進担当者	384名	3,717名
ISMS内部監査員	114名	599名

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。

▶ 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、キャノン 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、キャノン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。

なお、オフィスツアーではオフィスフロアの見学を通じて、私たちの取り組み事例を実際にご覧いただけます。



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

キャノン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 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)

※2012年4月1日現在

Action 2011 2011年の取り組み

..... 教育分野への協力

キャノンITソリューションズは、千葉工業大学からの依頼を受けて、金融・経営リスク科学科の3年生向けに、特別講義「リスクマネジメント演習」の開催に協力しました。

講義では、新たな脅威となっている特定企業を狙ったサイバー攻撃や、ウイルス感染が企業にもたらす被害と影響等についての解説および実習を実施しました。



特別講義「リスクマネジメント演習」の様子

..... NPOへの協力

キャノンMJはNPO情報セキュリティフォーラム*が開催する「情報セキュリティピックアップセミナー」に協力し、キャノンMJグループにおける情報セキュリティの取り組み事例を紹介しました。

※情報セキュリティに関するセミナーや講座のほか、さまざまな事業活動を通じて高度情報通信社会の発展と科学技術の振興を図り、広く公益に寄与しているNPOです。

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グループは、営業やサービス、ソフトウェア開発などの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。

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展開しています。キヤノンS&Sのサービスエンジニアは、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。



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）の紛失・ウイルス感染	- 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。 - 持ち出すパソコンのHDDは暗号化ソフトによりデータ漏えいのリスクにも対応しています。 - 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。
修理受付 (移動中)	- 修理受付用の携帯電話の紛失 - サービス工具（パソコン・USBメモリ）・伝票の紛失	- 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。 - 施錠可能なサービス工具鞆を採用し、伝票類もそれに収納することで紛失のリスクを軽減しています。
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、了承をいただいております。 - 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、了承をいただいております。
帰社後 (社内)	- セキュリティ意識・知識の欠如 - お客さまより預かりしたデータの漏えい	- 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。

お客さまへの安心・安全の提供

安心・安全な修理サービスの実践

キヤノンカスタマーサポートのコンシューマ修理部門は全国12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わせや相談・修理に至るまで、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、安心・安全な修理サービスの提供を日々実践しています。



修理作業風景



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FAX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を行い、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。 ●FAX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。 ●FAX番号二度打ち機能を持つ機器を導入しています。
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	●個人情報に記載された伝票や修理品の誤送付	●配送伝票作成時には、チェックシートを元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。

お客さまへの安心・安全の提供

安心・安全な開発プロセスの実践

キャノンITソリューションズでは、金融、製造、流通・サービス、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など、広範なサービスの提供を通じてお客さまが抱える課題の解決に貢献しています。

開発プロジェクトでは、各開発工程において全社共通のプロジェクト管理基準に準拠した品質管理や情報セキュリティ管理を行い、高品質で信頼性の高い成果物を提供しています。

品質マネジメントに関しては、実務プロセスを基本とした国際的な品質マネジメントシステム「ISO9001:2008」を取得するとともに、ITスキル標準に準拠した社内認定プロジェクトマネージャーが、お客さまとのコミュニケーションを基本としたプロジェクト管理を推進し、高い品質を提供しています。



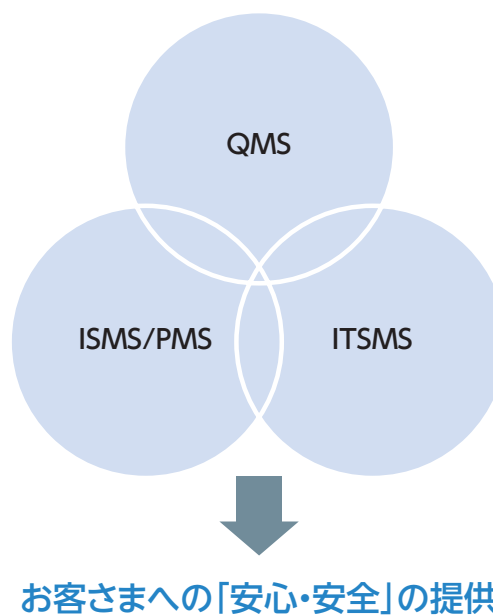
開発環境の様子

情報セキュリティマネジメントに関しては、「ISO/IEC27001:2005 (ISMS適合性評価制度)」および「プライバシーマーク」を取得し、お客さまやビジネスパートナーの情報資産を安全かつ適切に取り扱っています。

また、お客さまのシステムの安定稼働に向けたITサービスのさらなる品質向上を目指し、ITサービスマネジメントの国際規格である「ISO/IEC20000-1:2005 (ITSMS適合性評価制度)」を取得しています。

「品質 (QMS)」「情報セキュリティ (ISMS / PMS)」「ITサービス (ITSMS)」のマネジメントシステムを開発プロセスに組み込み、お客さまに「安心・安全」で質の高い製品・サービスを提供しています。

開発プロセスへのマネジメントシステムの組み込み



お客さまへの安心・安全の提供

▶ 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。

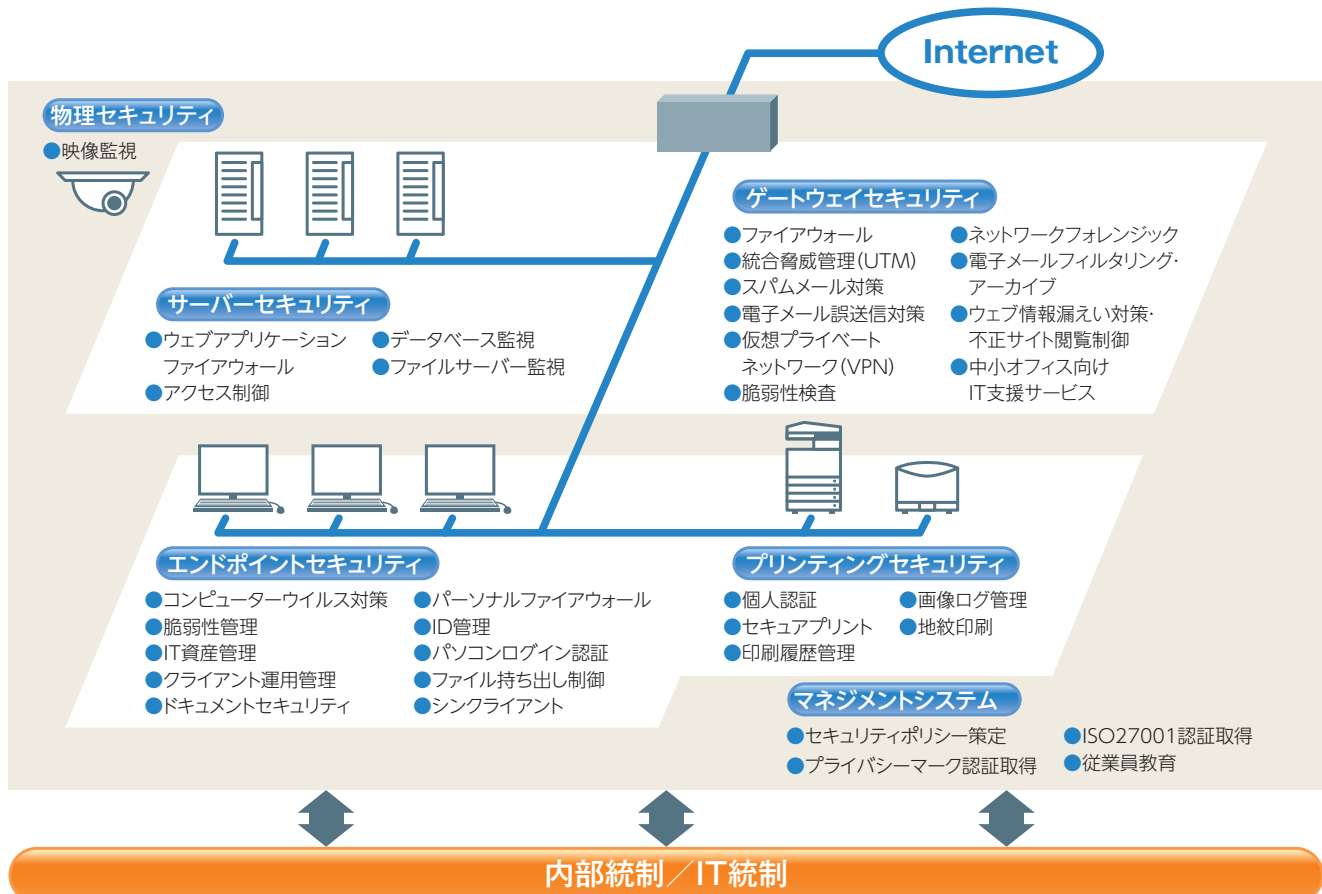
トータルセキュリティソリューションの提供

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。

■ セキュリティソリューションの全体像



お客さまへの安心・安全の提供

製品への情報セキュリティ品質の組み込み

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、コンピューター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。

セキュリティ認証「IEEE2600.1」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。

※imageRUNNER ADVANCE C2020/C2030シリーズでは対応していません。

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。

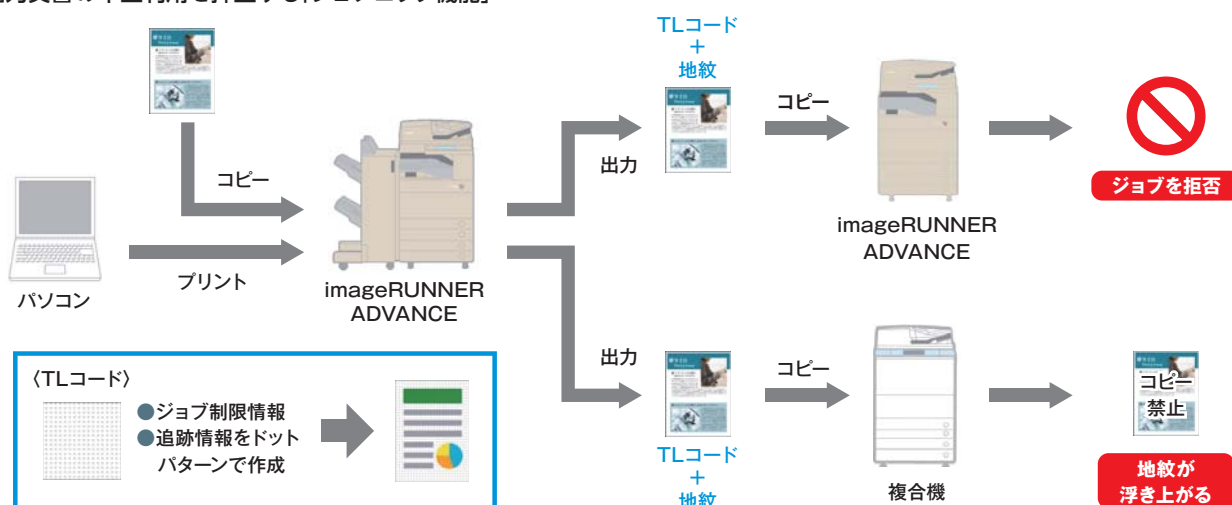
さらに地紋印字と組み合わせれば、ジョブロック未対応機器

を利用した際にも「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・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「ジョブブロック機能」



お客さまへの安心・安全の提供

複合機に保存されている機密情報の漏えい対策

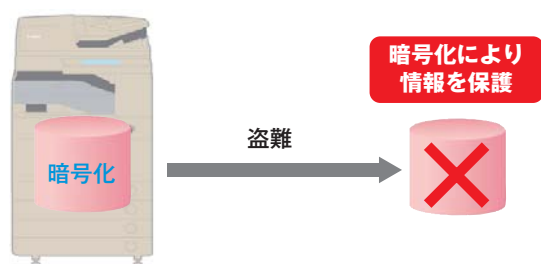
セキュリティ機能の評価適性度を保証するISO15408（コモンクライテリア）認証（EAL3）を取得した「Canon MFP Security Chip 2.00」を搭載し、ハードディスク内データを自動的に暗号化します。

※「HDDデータ暗号化/ミラーリングキット・C1」が必要です。

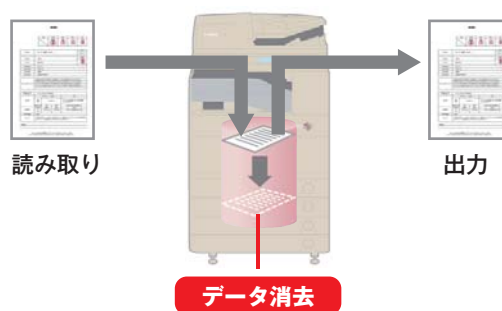
「自動消去」は、コピーやプリントなどの作業を行うたびに、一時的にハードディスク内に生成されるデジタルデータをジョブ終了と同時に自動的に消去する機能です。万一の盗難や本体廃棄後の情報漏えいリスクを低減します。

※「データ消去キット・C1」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」



お客さまへの安心・安全の提供

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。

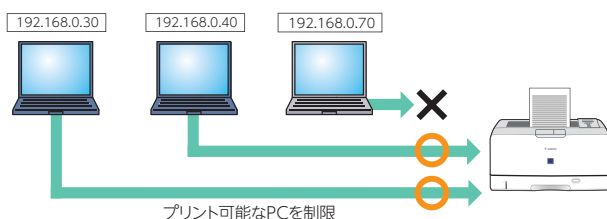
■SSL通信概念図



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。

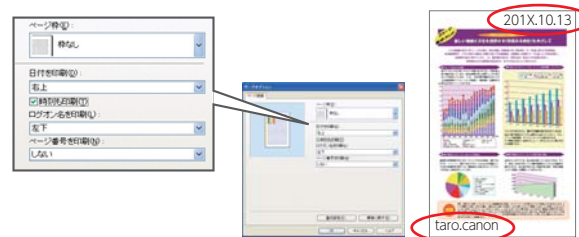
■アドレス制限概念図



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



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



お客さまへの安心・安全の提供

▶ お客さまへの情報セキュリティ課題解決への貢献

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。

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りリモートツールでわかりやすくサポートします。

■「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入侵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／制御	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（「スケジュール」「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、キャノンMJグループが提供するSaaS型アプリケーションです。

「HOME」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わせも増えています。こうしたお問い合わせに対しても、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蛸殻町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

メール誤送信を防ぐための「GUARDIAN CorrectMail」

電子メールの誤送信の原因の多くは、送付先のメールアドレスや内容、添付ファイルをきちんと確かめないままに送信してしまうなどのヒューマンエラーです。電子メール誤送信事故は年々増加傾向にあり、技術的な対策が困難であることから、情報セキュリティ上の大きな課題となっています。

「GUARDIAN CorrectMail」は、送信メールを一定期間システム上で保留するため、送信者や上長、Ccに同報されている第三者のチェックが可能です。間違いに気づいた際は、電子メールを外部に送信する前に取り消すことができるため、誤送信の防止に役立つシステムです。

こうした外部への送信前にメールを取り消すことができる機能のほか、ToやCc宛のアドレスが必要以上に多い場合はメールを削除する等の設定を行うことができ、宛先の間違いによる誤送信事故に加えてメールアドレスが露出することによる個人情報漏えい事故を未然に防ぐことができます。

GUARDIAN CorrectMail

ガーディアン コレクトメール

キヤノンMJグループでの活用事例

メール誤送信への対策：キヤノンITソリューションズ

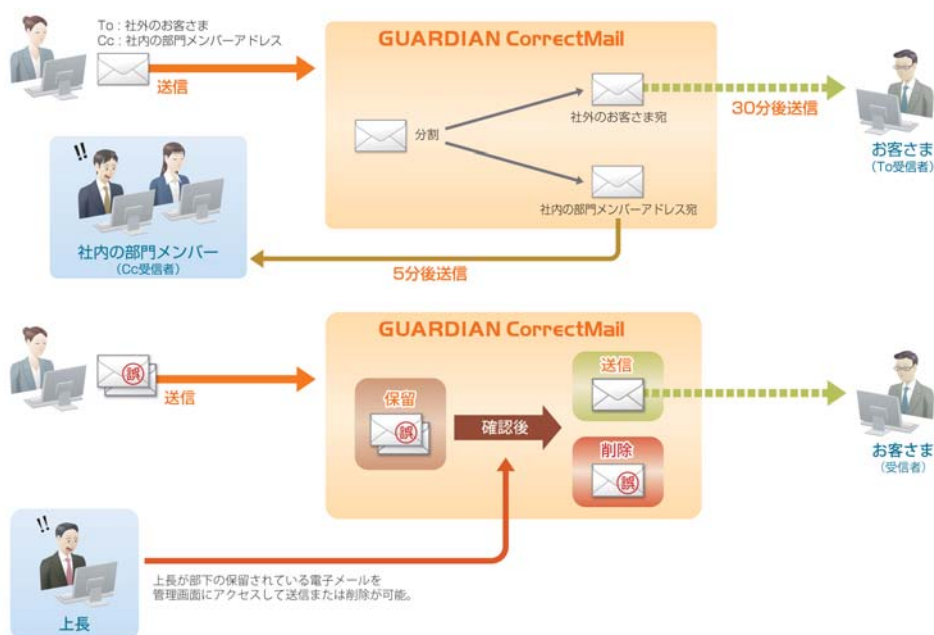
キヤノンITソリューションズのEDIソリューション事業部は、業務上、不特定多数のお客さまに重要情報をメール送信することが多いことから、これまでメール送信時には、複数人によるチェックを行うことでメール誤送信の防止を図っていました。

同事業部では、「GUARDIAN CorrectMail」の一定時間メール送信を保留する機能を有効活用し、誤送信の防止に効果をあげています。実際に、送信者本人がシステムに一定時間保留されたメールを改めて確認することで間違いに気づくなど、ヒヤリハットで済んだケースがありました。また、メール内容を改めて見返すことで、よりわかりやすく丁寧な文章に修正して送信する等、メール品質の向上にもつながっています。

「GUARDIAN CorrectMail」の導入をきっかけに、メール送信担当者だけでなく部門全体の情報セキュリティに対する意識が高まるという効果もありました。

情報セキュリティの事故防止には、ルール作りとその確実な実行が大切です。それを人的な注意だけに頼らずに、システムとして補完することの重要性を痛感しました。

私たちが得られた効果をお客さまにも展開できればと考えています。



お客さまへの安心・安全の提供

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

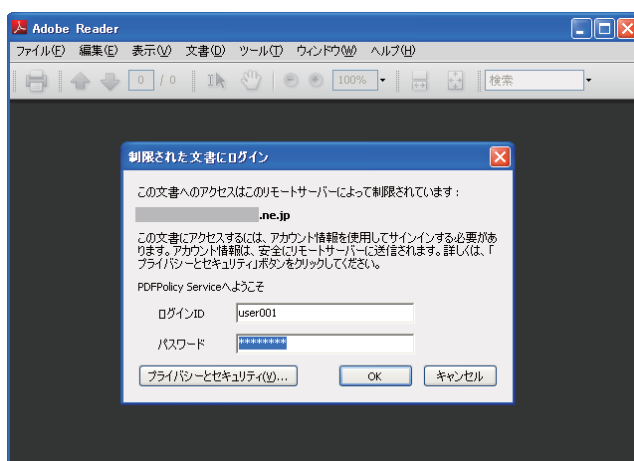
文書の閲覧権限・印刷権限・編集権限などを、ユーザー単位・グループ単位で制御することができます。

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。

ログ管理を社員に通知することは、セキュリティ意識の向上にもなります。

キヤノンMJグループでの活用事例

経営会議資料の配布管理：

キヤノンMJアイティグループホールディングス

経営会議資料には、トップシークレットの情報が含まれています。キヤノンMJアイティグループホールディングスでは、PDFPolicy Serviceを導入し、経営会議資料の閲覧権限を一元的に管理しています。

万が一会議関係者以外に会議資料のファイルが流出しても、ID・パスワードを持たないユーザー、閲覧権限のないユーザーは、そのファイルを閲覧することができません。資料の更新があった場合は、旧版資料を失効させることにより、最新版資料への誘導を図りやすくなりました。また、会議関係者の資料確認状況(閲覧・印刷など)を把握できるようになったため、未確認の参加者に対して、事前確認を促すことも可能になりました。

小規模利用が可能で運用が容易なSaaSを活用し、短期間で機密性と管理性の向上を実現しています。

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

(2011年12月31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

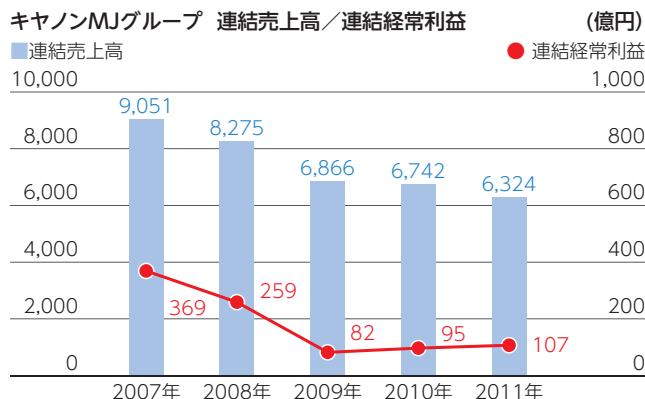
資本金：73,303百万円

従業員：連結：18,861名 単独：5,244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



グループ会社紹介

(2012年5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)
- 日本オセ(株)
- キヤノンプリントスクエア(株)
- 昭和情報機器(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)
 - フォリサイトテクノロジーズ(株)
 - Canon Software America, Inc.
 - 佳能信息系统(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)
 - エディフィストラニング(株)

コンシューマイメージング

- 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)

産業機器

- (株)エルクコーポレーション
 - (株)エルクエスト
 - ユニオン・メディカル(株)
- 台湾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

キヤノン製品を中心に多彩な製品・サービスで、オフィスに生産性の向上をもたらします。

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、競争力と企業価値の向上に貢献します。

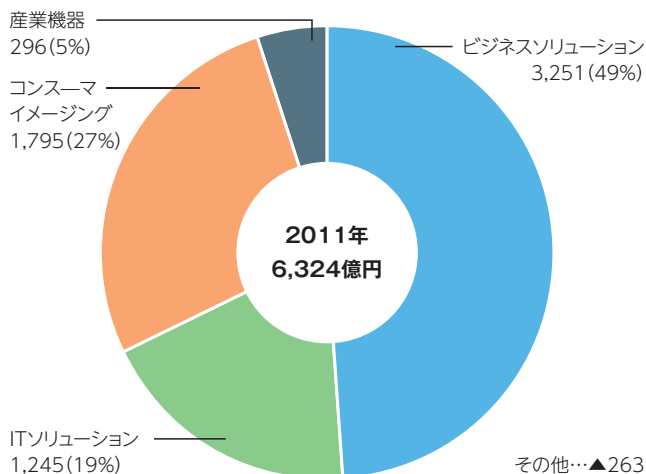
コンシューマイメージング

写真や映像の新しい楽しみ方を伝え、新鮮な喜びと感動のあるフォトライフをお届けします。

産業機器

私たちの暮らしを支える半導体業界と医療業界に、世界の最先端機器と高度なソリューションを提供します。

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、それぞれの単独合計額を基に算出しています

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「暮らし、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

キャ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、キャ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

キャ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

キャ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、キャ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、キャ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員に周知します。
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

キャ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

2012年6月発行