情報セキュリティガバナンスとマネジメント

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

CSR委員会による情報セキュリティガバナンスの強化

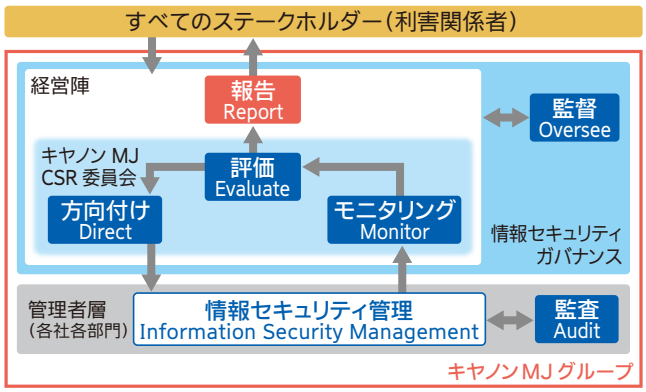
情報セキュリティの取り組みは、コンプライアンスや環境対応、事業継続、品質管理などの社会要請への対応とも密接に関連しています。

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

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

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

● キヤノンMJグループの情報セキュリティガバナンス



効率的なマネジメント体制

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

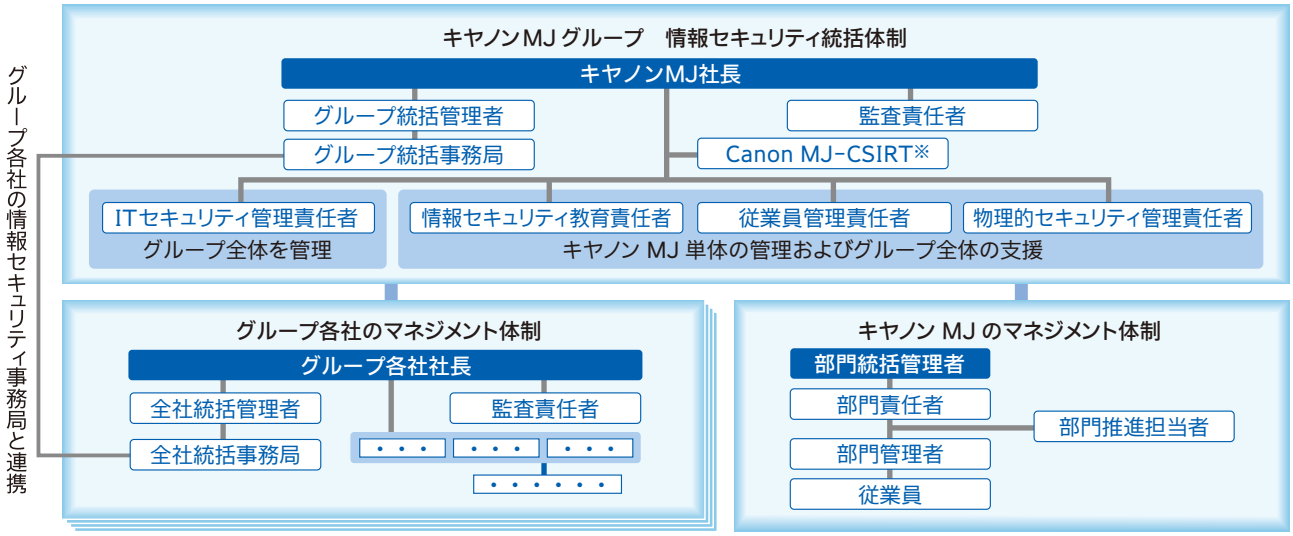
グループ情報セキュリティ統括体制はキヤノンMJの情報セキュリティ主管部門がグループ統括事務局の役割を果たし、グループ全体の情報セキュリティマネジメントを統括しています。

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

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

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

● キヤノンMJグループの情報セキュリティマネジメント体制



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

体系的にルールを整備

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

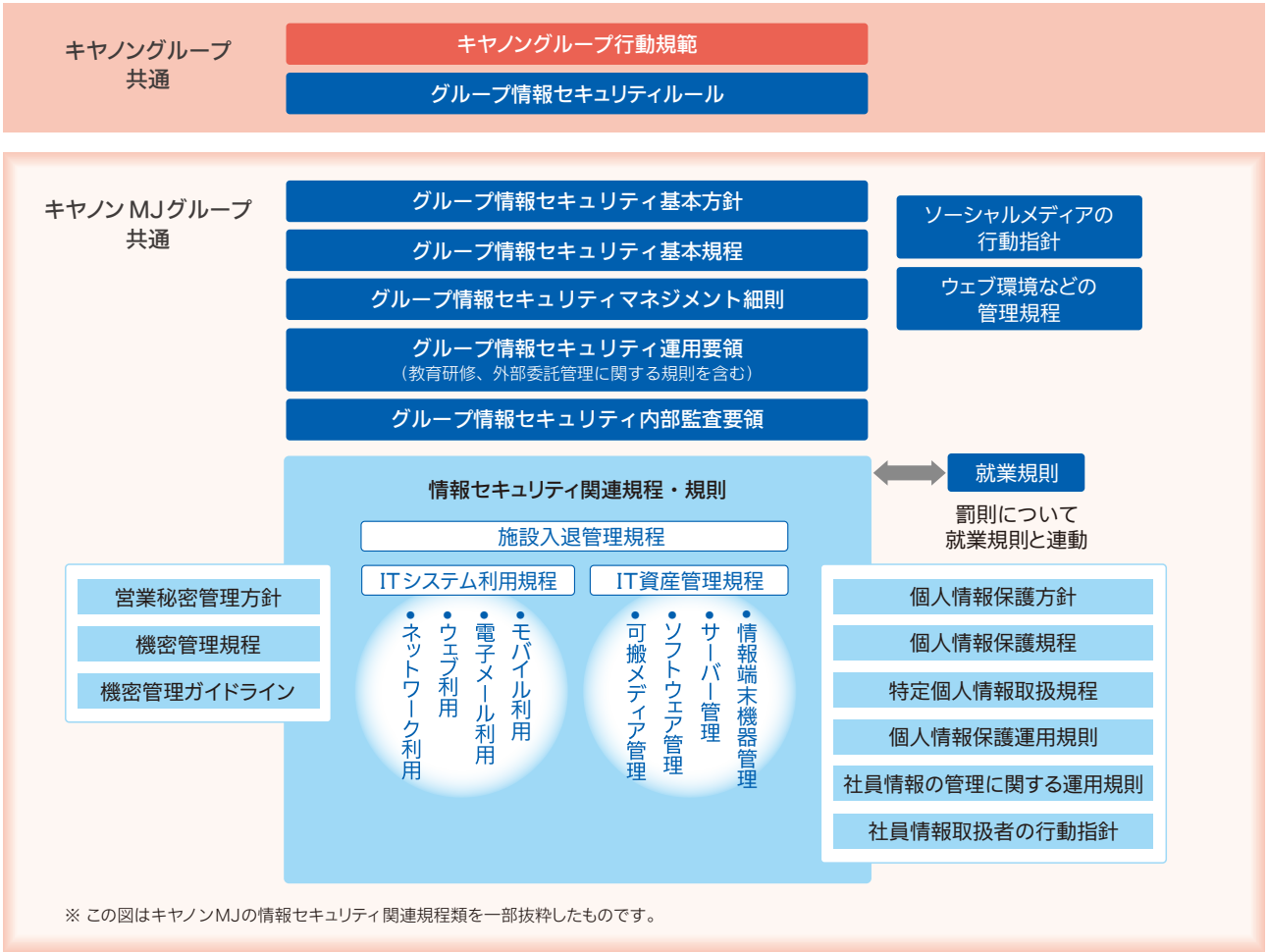
これらの方針や規程を踏まえ、キヤノンMJグループ全体の情報セキュリティ基盤を支える規程類と、重要な情報資産である個人情報保護や機密管理に関する規程類は、それぞれの規程の中で定める要素が重複することがないようにしています。

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

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

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

情報セキュリティに関するルール体系



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

▶個人情報・機密情報を取り扱う業務委託先への管理・監督の取り組み

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

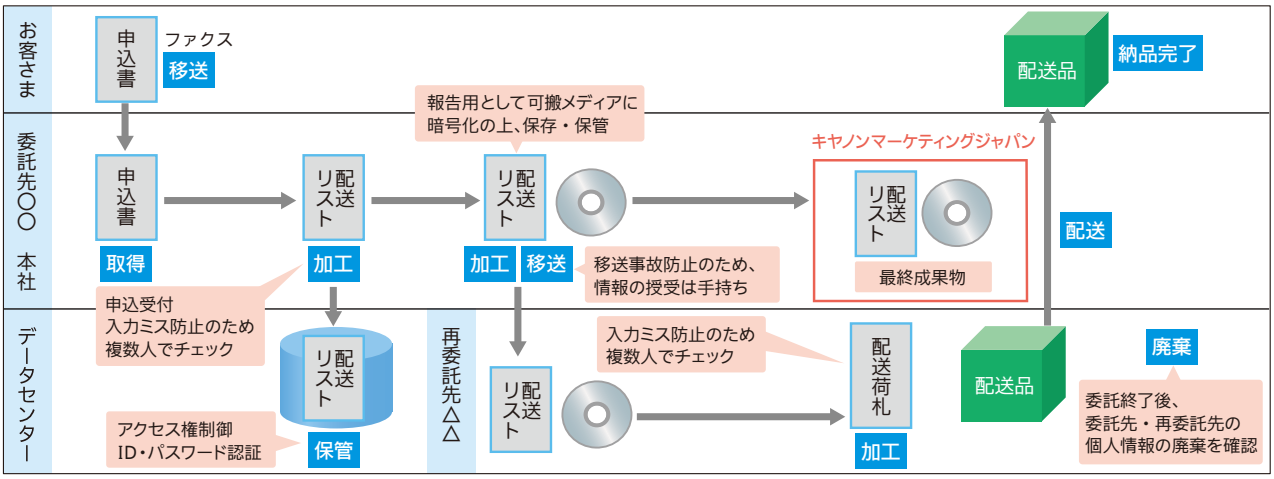
委託先における業務フローや安全管理措置・安全対策の確認

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

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

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

サンプル キャンペーン申込受付・景品発送　業務フロー図



パートナー企業の情報セキュリティ品質の向上

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

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

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

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

▶インシデント管理への取り組み

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

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

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

ウェブ環境の安全管理体制の確立

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

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

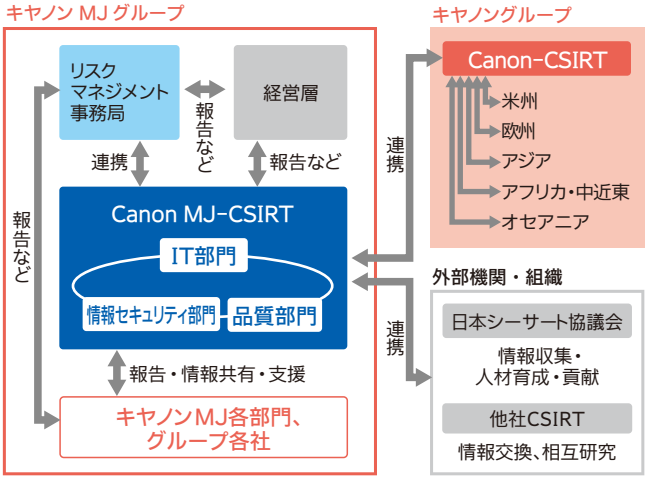
サイバーセキュリティへの取り組み

推進体制と活動

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

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

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



体制図

主な活動内容

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

2 監視
- ログの収集と分析
- 証跡保存

3 対応
- 発生時から収束、再発防止まで一連の支援

標的型攻撃への対応訓練

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