Topics サイバーセキュリティ

サイバーセキュリティの基本的な考え方

近年、DXの推進やクラウド、人工知能、IoTなどの新しいテクノロジーの出現により、当社を取り巻くビジネス環境が日々変化しています。IT利活用の機運の高まりと同時に、日々高度化・巧妙化するサイバー攻撃に対するセキュリティ対策は、経営戦略として優先されるべき重要な要素であると認識しており、グループリスク管理責任者(グループCRO：Chief Risk Officer)によるリーダーシップのもと、セキュリティ対策への適切な投資および推進を図っています。

サイバーセキュリティ管理態勢

サイバーセキュリティに関する法令その他の規範を順守し情報資産をサイバー攻撃から保護するため、グループCRO配下に専門組織MY-SIRT*を設置し、“自助・共助・公助”の視点でサイバーセキュリティ管理態勢を敷いています。

自助では、サイバー攻撃への迅速な対処を目的とした24時間365日でのセキュリティ監視や、明治安田グループへのサイバーインシデント対応支援、攻撃者の脅威情報やシステムの脆弱性情報などの収集と当社に対する影響分析を行なっています。

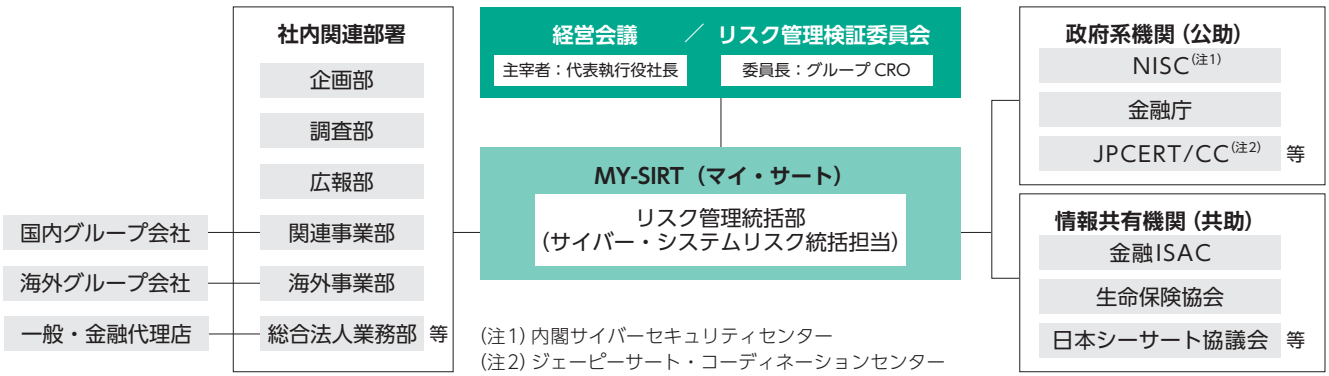
共助では、金融ISACなどの情報共有機関へ加入し、サイバーインシデントなどの情報交換を行なっています。

公助では、NISC・金融庁などの政府系機関と連携して、官民一体でセキュリティ管理態勢を構築しています。

これらMY-SIRTの活動状況や活動から得られた課題などは、定期的にリスク管理検証委員会、経営会議などでグループCROと経営層に報告され、改善を図っています。

*マイ・サートMEIJIYASUDA Computer Security Incident Response Team

● サイバーセキュリティ管理体制図



(注1) 内閣サイバーセキュリティセンター
(注2) ジェーピーサート・コーディネーションセンター

サイバーセキュリティに関する主な取組み

サイバーセキュリティ対策

サイバー攻撃への監視や、攻撃者の脅威情報・システムの脆弱性情報などを収集し活用することで、インシデントの早期発見と迅速な対応を可能にしています。

また、お客さまに安全にサービスをご利用いただくために、個人情報の適正な取り扱いを徹底し、サービス提供前には国際規格に基づくセキュリティ評価を実施しています。

加えて、絶えず変化する最新のセキュリティ対策の情報を常に収集し、“特定・防御・検知・対応・復旧”の観点から積極的に実装・運用しています。実装した対策は定期的に専門のセキュリティベンダーへ診断を依頼し、脆弱性の発見と対処を行なうとともに、その実効性を継続的に検証しています。

サイバーセキュリティ意識向上および人財育成

全社的な意識向上とカルチャー醸成のため、全従業員を対象とした標的型メール訓練、eラーニング基礎研修、経営層向け訓練などを継続的に実施するほか、最新のセキュリティ情報を共有して注意喚起を徹底しています。

キャリア採用も積極的に行ない専門知識を持つプロフェッショナルを継続的に迎え入れながら、業務遂行上のスキルセットを定義し、継続的なトレーニングとスキルアップでセキュリティチームの育成と強化を図っています。

また、サイバー攻撃が発生した場合の対応体制を強化するためにNISC、金融庁、金融ISACなどが主催するサイバー防御演習にも積極的に参加し、組織全体のセキュリティレベル向上に努めています。