情報セキュリティマネジメント

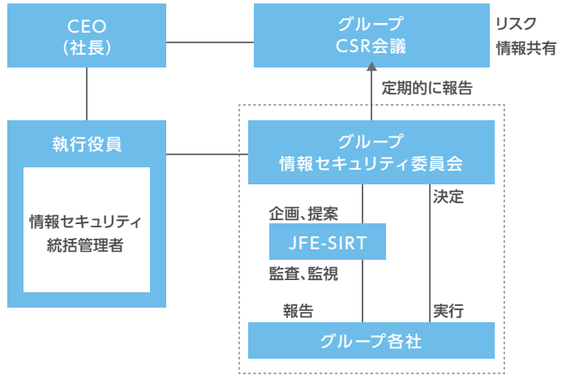
サイバー攻撃やシステム不正利用を防止し事業活動を安全に推進するため、JFEグループでは以下の施策により、情報セキュリティ管理レベルを継続的に向上しています。

1 情報セキュリティガバナンス体制の整備

「グループCSR会議」の下部組織として「グループ情報セキュリティ委員会」を設け、JFEホールディングスの「情報セキュリティ統括管理者」のもとで、各事業会社のIT部門担当役員が参画し情報セキュリティを中心にITの重要課題を審議し、グループとしての方針を決定しています。

同委員会の決定に基づき、各事業会社のIT部門長が参画する「JFE-SIRT」が規程・ルールの制定、IT施策の策定・実施推進、情報セキュリティ監査・教育、情報セキュリティインシデント対応の指導からなる一連の情報セキュリティ向上のPDCAサイクル推進の役割を担っています。

JFEグループ　情報セキュリティガバナンス体制

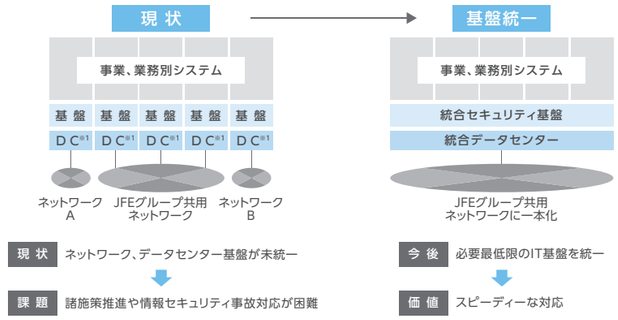


2 主要IT施策のグループ共通化

JFE-SIRTとグループ各社が一体となって、グループ全体の情報セキュリティ対策のレベル合わせと、万一の情報セキュリティインシデント発生時の素早い対応を目的として、ネットワーク、IT機器、セキュリティ関連ソフト等の情報セキュリティ基盤の共通化を促進しています。さらに調達の一元化を実施し廉価化も志向しています。

※1: DC = Data Center

JFEグループ　主要IT基盤のグループ共通化



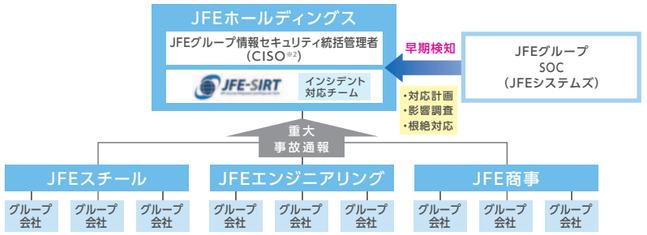
3 情報セキュリティインシデント対応体制の整備

情報セキュリティインシデント発生時の対応要領を策定し、JFEグループ情報セキュリティ統括管理者のもとで、JFE-SIRTにて、報告・処置・復旧の速やかな対応と再発防止策を立案する体制を定めています。

また、情報セキュリティインシデントによる被害を最小限に食い止めるため、統合セキュリティ監視網でグループ全体をカバーし、グループ共通SOC※3がインシデント発生を初期段階で検知する体制整備を進めています。

※2: CISO = Chief Information Security Officer
※3: SOC = Security Operation Center

JFEグループ　情報セキュリティ統合監視網



JFEグループセキュリティ担当者向け机上演習

サイバーインシデント発生時の早期収束を目的に、JFE-SIRTでは、サイバー攻撃への対応演習を事業会社、情報システム子会社と合同で、定期的に実施しています。

インシデント発生を想定した対応要領をもとに、関係者各自の役割と連携の認識を行い、問題点を参加者で議論することで理解を深化させ、演習を通じて抽出された改善案をJFE-SIRTの日々の活動に反映しています。

JFE-SIRTで培った事故対応ノウハウをグループ各社へ展開することを目的に、2019年度よりグループ会社の情報セキュリティ担当者向けに机上演習を実施しました。

昨今の標的型サイバー攻撃の特徴を解説し、ワークショップにて、共通のサイバー攻撃シナリオに沿って設定された質問に対してグループで討議しました。討議では、事故発生から収束まで、自社の状況を振り返りながら対応方法や日頃の準備の必要性を考えていただくことで、運用上の気付きや課題を認識する良い機会となりました。

グループ情報セキュリティ監査

JFE-SIRTでは2017-2018年にJFEグループ国内外約260社を対象に、グローバルで共通の情報セキュリティポリシーのもと、「課題の早期発見とその対応」を目的に情報セキュリティ監査を実施しました。監査結果の通知、是正計画の指導を通じて、情報セキュリティ対策の意義と教育などグループ全体の情報セキュリティレベルの向上につなげています。

また、さらなるセキュリティレベルの向上に向けて、2019年度から2巡目の監査を開始します。2巡目監査では、セキュリティ事故が起こった際に必要なログの整備や共通施策の導入進捗などを確認し、グループ全体のセキュリティ施策を強化していきます。

グループ各社監査方針

自主点検　被監査会社自身および事業会社にて評価し、事業会社を通じてJFE-SIRTに報告、内容をJFE-SIRTで審査し、結果を通知する。