情報セキュリティマネジメント

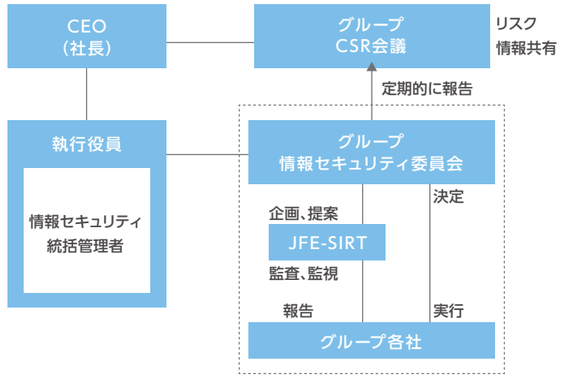
サイバー攻撃やシステム不正利用を防止し事業活動を安全に推進するため、JFEグループでは以下の施策により、情報セキュリティ管理レベルを継続的に向上しています。

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

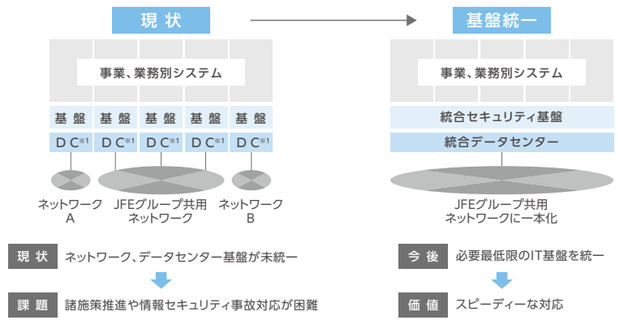


2 主要IT施策のグループ共通化

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



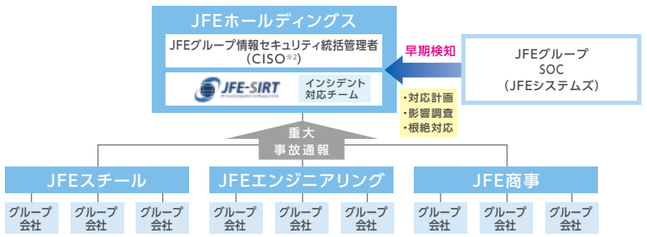
3 情報セキュリティインシデント対応体制の整備

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



サイバー攻撃への対応演習（机上演習）

サイバーインシデント発生時対応の習熟度向上を目的に、JFE-SIRTでは、サイバー攻撃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、過去の事例や公開されているサイバー攻撃をモデルとしたシナリオに沿って、インシデント発生時に当事者となる関係者が参画して演習を進めます。

関係者各自の役割と連携の確認を行い、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策をJFE-SIRTの日々の活動に反映しています。

JFE-SIRT訓練の体系と実施方向性

・参加者、目的に応じて、4つの演習体系で実施
・段階を踏んで、シナリオ、演習規模を拡大することで、対応能力向上と組織対応力強化を図る

訓練対象	CISO・JFE-SIRT関連部門が的確に対応する能力			
手　法	手順の確認・改善のため、主にシナリオを元に会議形式で討議			
種　類	ワークショップ	机上演習	機能別演習	統合演習
目　的	インシデント対応手順の明確化	想定訓練シナリオに基づいたインシデント対応手順の検証	実際の運用環境において、訓練シナリオに基づいた連絡手順の確認	複数の組織が参加し、実想定シナリオに基づいた組織横断的予行演習
参加対象	事故初動対応者 JFE-SIRT	事故初動対応者 JFE-SIRT	CISO JFE-SIRT	CISO JFE-SIRT 事故時関連部門
ねらい	対応レベルの安定・均一化			
ルール・手順	手順整備	手順改善	事故対応課題抽出、ルール改善	
組織・体制		事故対応体制・監視機能改善	事故対応体制・監視機能改善、社内外連携の確認	社内外連携の確認
人		参加メンバー対応力底上げ		経営層への意識醸成

独立行政法人情報処理推進機構（IPA）内に2017年に設立された産業サイバーセキュリティセンターの中核人材育成プログラムに、若手技術者を派遣し、グループの制御系システムのセキュリティ強化を担う人材の育成を進めています。