DX推進を支える情報セキュリティガバナンス

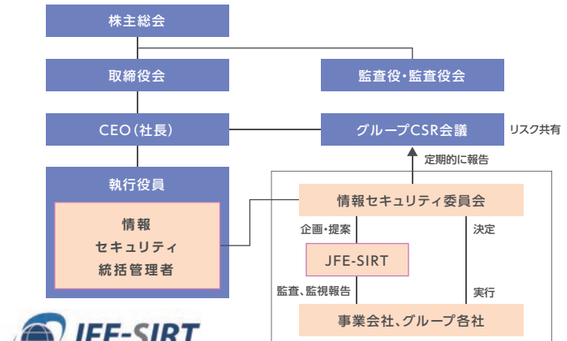
情報セキュリティマネジメント

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。

JFEグループ情報セキュリティ管理体制

2015年の経済産業省の「サイバーセキュリティ経営ガイドライン」の発行を受け、2016年4月にグループ全体のITリスク管理機能を継続的に維持・強化することを目的として、「グループ情報セキュリティ委員会」を設置しました。JFEホールディングスの情報セキュリティ統括管理者※1のもとで、各事業会社のIT部門担当役員が、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。さらに、各事業会社のIT部門長が参画する「JFE-SIRT」を設置し、同委員会の決定に基づき、事業会社ならびにそのグループ会社への、セキュリティ対策とガバナンス強化を推進しています。

JFEグループ情報セキュリティ管理体制



JFE-SIRT（JFE Security Integration and Response Teamの略）は、CSIRT※2として、情報セキュリティの事故の対応だけでなく、グループ共通施策の企画・提案・推進、グループ会社監査、セキュリティポリシーの見直しなどを担っています。

※1 情報セキュリティ統括管理者（CISO）：Chief Information Security Officerの略。最高情報セキュリティ責任者。企業・組織内において情報管理およびその運用を担当し、情報セキュリティを統括する担当役員。

※2 CSIRT（シーサート）：Computer Security Incident Response Teamの略。組織内部で発生する、コンピュータセキュリティに係るインシデントに対処するための組織の一般名称。

JFE-SIRTチームメッセージ

DX（デジタルトランスフォーメーション）の取り組みが活発化しています。JFEグループにおいてもグループ一体となったDX推進を重要な戦略として位置付けています。DXを通じて生産性向上、ビジネス変革、および新たな価値創造を実現するために新しい技術を積極的に取り入れ情報資産を活用することになりますが、そこでは新たなサイバーセキュリティリスクも生じます。お客様へ提供する財、サービスの品質、安全性を担保し、サプライチェーンにおける責任を果たすためにはこうしたリスクから情報資産を適切に保護する必要があります。

JFEグループでは2016年に情報セキュリティ委員会・JFE-SIRTの枠組みを発足させ、国内・海外、およびIT・OT領域も含めたグループ全体のサイバーセキュリティ対策レベルの向上に努めてまいりました。この活動基盤を着実に持続し、発展させることによりDX戦略の推進にも貢献してまいります。

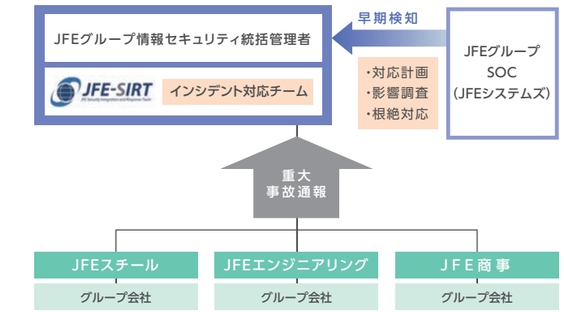
JFE-SIRT　チーム長
酒田　健

セキュリティ統合監視網

企業を狙った標的型サイバー攻撃は日々巧妙化しており、攻撃されていることに長期間気づくことができず、気づいた時には既に情報資産を盗まれた後だったという事態が多発しています。このような脅威を早期に検知して被害拡大を防止するためには、パソコンからネットワークまで多層的に監視するセキュリティ統合監視の仕組みが必要です。グループ共通のSOC※3の体制を整備することで、JFEグループ全体を常時監視できるようにしています。また、各社で起こったセキュリティインシデントは、JFEグループ情報セキュリティ統括管理者のもと、「JFE-SIRT」にて速やかに報告・処置・復旧し、再発防止策を立案する体制を構築しています。

※3 SOC=Security Operation Centerの略。ネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対応策のアドバイスを行う組織。

セキュリティ統合監視網

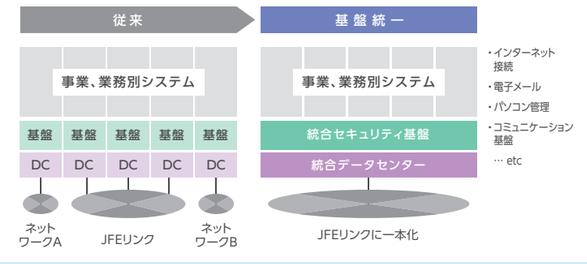


グループセキュリティ基盤の統一

グループ全体の情報セキュリティレベルを底上げし、高度化するサイバー攻撃からグループ内の情報資産を守るため、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推進しています。万が一情報セキュリティ事故が発生した場合でも、共通基盤にすることで、脅威の正確な把握と迅速な対応が可能となります。

昨今のクラウド活用においても、情報コミュニケーション基盤を共通化し、グループ内の安全な情報共有を促進することで、DX分野におけるグループ間のビジネス創造にも寄与しています。

グループセキュリティ基盤の統一



サイバーセキュリティ情報公開

JFEホールディングスでは、株主・顧客・取引先などのステークホルダーの皆様へ、情報セキュリティへの取り組みを情報公開しています。また、JFEグループ各社のDX（デジタルトランスフォーメーション）促進を後押しするために、さまざまなグループ内のコミュニケーション機会を通じ、各社のセキュリティ意識向上とセキュリティレベルアップを推進しています。

対象	情報公開の目的
顧客	製品やサービスをご利用頂く上での安心感の提供
取引先	サプライチェーンにおいて、またビジネスパートナーとしての信頼関係の構築
株主・機関投資家	適切なリスクマネジメントが機能している企業グループであることの表明
	非財務情報を通じた企業価値への理解
社員	当社グループの一員としての誇りと責任の自覚
メディア	社会に対する当社ブランドの浸透

情報公開メディア

- 有価証券報告書
- CSR報告書
- 統合報告書（JFEグループ レポート）
- DXレポート（当レポート）
- 自社ウェブサイトなど

発行時期：2021年2月

JFEグループ サイバーセキュリティ経営宣言

1 経営課題としての認識

サイバーリスクを経営上の重大なリスクと認識し、経営者自らが最新情勢への理解を深めることを怠らず、サイバーセキュリティを投資と位置づけて積極的な経営に取り組みます。

経営者自らが現実を直視してリスクと向き合い、経営者としてのリーダーシップを発揮し、自らの責任で対策に取り組みます。JFEホールディングスおよび各事業会社に設置されたサイバーセキュリティに関する会議体を経営者が主宰し、実効性のある議論と各種対策の検証を行い、必要な対策には適切なリソースを配分しこれを推進します。

2 経営方針の策定と意思表明

特定・防御だけでなく、検知・対応・復旧も重視した上で、経営方針やインシデントからの早期回復に向けたBCP（事業継続計画）の策定を行います。

年次毎にJFEグループのサイバーセキュリティ活動計画を設定し、リスクの特定や防御の取り組み、情報セキュリティインシデント発生時の対応要領を見直すとともに、定期的な訓練を通じたインシデント対応能力の強化、BCPの整備を実施します。加えて、JFEグループ会社への定期的なサイバーセキュリティ監査を実施し、グループ全体の底上げと着実なレベルアップを図ります。

また、経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じたセキュリティ強化の取り組みを各種報告書に記載するなど、自主的な情報開示に努めます。

3 社内外体制の構築・対策の実施

JFE-SIRTを中心に社内体制を整え、予算・人員等のリソースを確保し、人的・技術的・物理的等の必要な対策を講じます。

社内外の各種人材育成プログラムを活用してサイバーセキュリティに精通した高度なプロフェッショナル人材の育成を図るとともに、外部の専門機関とも連携しながらノウハウの共有を進めます。社内の教育訓練や、業界横断的な演習プログラムへの参加等を通じて、JFEグループ各社・各部署における従業員各層の教育と動機付けに取り組みます。

業務委託先等でのセキュリティ対策状況のモニタリング等を通じ、海外も含めたサプライチェーン対策に努めます。

4 対策を講じた製品・システムやサービスの社会への普及

製品・システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努めます。

5 安心・安全なエコシステムの構築への貢献

関係官庁・組織・団体等との連携のもと、積極的な情報提供による情報共有や国内外における対話、人的ネットワークの構築を図ります。また、各種情報を踏まえた対策に関して注意喚起を行うことによって、グローバルベースでの社会全体のサイバーセキュリティ強化に貢献します。

JFE

JFE Group

JFEホールディングス株式会社

〒100-0011
東京都千代田区内幸町二丁目2番3号
https://www.jfe-holdings.co.jp/

[お問い合わせ先]
JFEホールディングス株式会社 企画部
TEL:03-3597-4321（大代表）