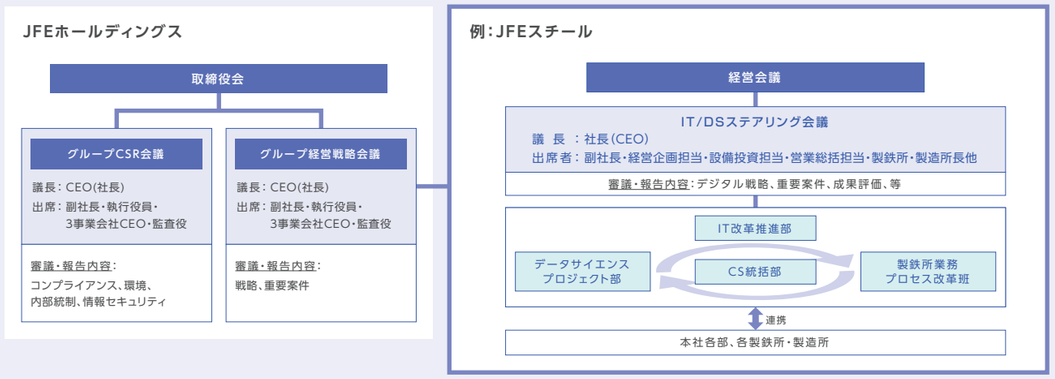
# セキュリティ対応

## デジタル・ガバナンス

### ■ JFEグループにおけるデジタル・ガバナンスの枠組み

コーポレートガバナンスの枠組みにグループのデジタル・ガバナンス機構を組み込んでいます。



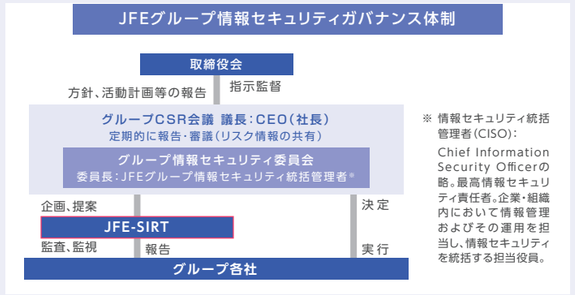

## セキュリティ管理

### ■ JFEグループのセキュリティ管理体制

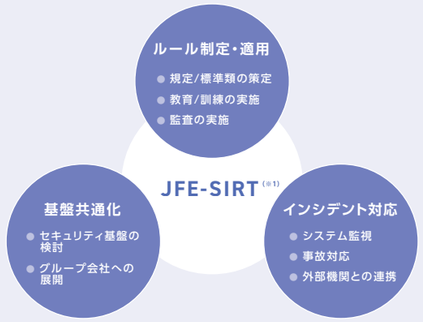
「サイバーセキュリティ経営宣言」のもと、深刻化・巧妙化するサイバー脅威に対し、
JFE-SIRTを中心とした経営主導によるサイバーセキュリティ対策の強化を推進していきます。

**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
2. 経営方針の策定と意思表明
3. 社内外体制の構築・対策の実施
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
5. 安心・安全なエコシステムの構築への貢献

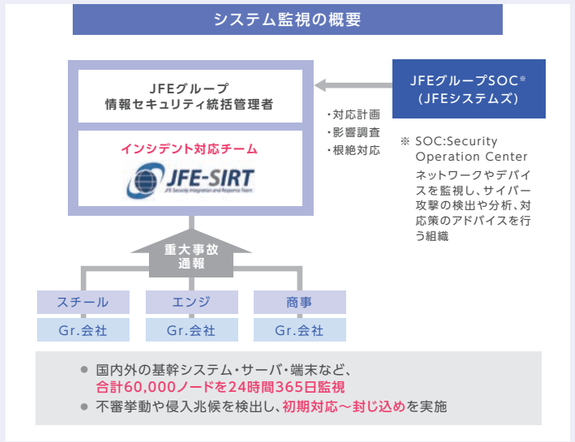



### ■ サイバーセキュリティ監視の取り組み




※1 JFE-SIRT：CSIRT(※2)として、インシデント対応だけでなく、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。

※2 CSIRT：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、DXを進めるうえで必須となる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。

経営者自らがデジタル化に伴うリスクと向き合い、サプライチェーン全体を俯瞰したサイバーセキュリティの強化を経営の重要課題と認識し、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。

サイバーセキュリティ対策のガイドライン・フレームワークの活用や、政府によるサイバーセキュリティ対策支援活動との連携、および、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、サプライチェーン全体、ひいては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。

2023年1月改訂