情報セキュリティマネジメント

マテリアリティ GRC

ガバナンス

GRI:3-3

不二製油グループは、取締役会の諮問機関であり代表取締役社長 兼 CEOが委員長を務めるサステナビリティ委員会※1にて、ESGマテリアリティ※2「GRC※3」について、マルチステークホルダーの視点で審議・監督し、取締役会へ答申しています。また、最高財務責任者(CFO)管掌のもと、同重点項目「情報セキュリティマネジメント」の取り組みを推進しています。
加えて、管掌役員のもと、情報管理統括責任者およびCSIRT（Computer Security Incident Response Team）を設置しています。CSIRTが各グループ会社に対して情報管理責任者および情報セキュリティ管理者を指名するとともに、外部の専門家の助言を得ながら、計画的に全グループ会社の情報セキュリティ水準向上を図っています。

※1 ガバナンス、戦略および指標と目標、リスク管理＞ガバナンス
https://www.fujioilholdings.com/sustainability/sustainability_management/
※2 ガバナンス、戦略および指標と目標、リスク管理＞戦略および指標と目標
https://www.fujioilholdings.com/sustainability/sustainability_management/
※3 GRC：ガバナンス・リスク・コンプライアンス。

戦略

当社グループは、情報セキュリティリスクを経営に直結するリスクと捉え、そのマネジメント強化に取り組んでいます。
リスクへの対応を怠った場合、サイバー攻撃によるシステム破壊・機密情報の流失など、事業継続の不全や企業価値の毀損につながる恐れがあります。リスクへの対策を進めることで、ステークホルダーからの信頼を醸成し、企業価値向上につながる機会となり得ます。
当社グループは、グループポリシーとして「情報管理規程」および「情報セキュリティ規程」（2022年度改訂）を策定し、規程の周知徹底に向けた従業員教育を継続して行っています。
また、社内外に存在する情報資産の機密性・完全性・可用性を確保・維持するため、情報システムの適切な運用プロセスやルールを定めるとともに、技術的には外部からの不正アクセスを防御する仕組みやコンピュータウイルスを防御する仕組みなど、重層的な対策を講じています。これにより、事業活動に関わる顧客や取引先を含むさまざまなステークホルダーから預かる重要な情報を適切に管理し、信頼性の高い製品・サービスを継続して提供することで企業の社会的責務を果たします。
事業活動においてデジタルとデータ活用が一層重要となる中で、情報セキュリティを確実に保ちながら、当社グループのDXを推進し事業競争力のさらなる強化に努めます。

リスク管理

教育

当社グループの従業員を対象に、2018年度よりeラーニングを中心としたITセキュリティ意識向上のための教育を実施しています。2023年度の受講率は96.3%※で、今後100%を目指して教育内容の充実、受講の促進に努めます。

※ 対象者は、会社貸与のメールアドレスを持ち、通常業務でPCを使用する当社グループの役員、執行役員および従業員。

セキュリティ内部監査

当社グループにおけるセキュリティ要件への遵守状況を明示的な証跡とともに把握し、是正のためのPDCAサイクルを構築するために、2020年度よりセキュリティ内部監査を実施しています。2024年度は監査評価項目を刷新し、OT※におけるセキュリティ対策状況の確認や、業務部門の利用するクラウドサービスに対する確認も含めて、より実効性の高い内部監査・自己点検を実施します。
内部監査の対象会社ごとに監査結果をレビューし、遵守に至らない項目については、各社の情報セキュリティ管理者（主にIT主管者）とともに改善計画を立案し、最終的な結果報告書としてまとめます。その後、各社の情報管理責任者（主に経営責任者）承認のもと、改善施策を確実に実行していきます。

※ OT：工場などの制御機器を制御し運用するシステムやその技術。

指標と目標

GRI:418-1

○：目標に対して90%以上達成、△：目標に対して60%以上達成、×：60%未満

2023年度目標	2023年度実績	自己評価
グループ全体における重篤なセキュリティインシデントの発生防止	事業継続に影響を及ぼす重大インシデントの発生なし	○
セキュリティ内部監査を含むCSIRTによる対策状況評価活動の継続実施（2023年度計画：IT評価6社、OT評価4社）	ITセキュリティ内部監査については計画に基づき計6社、OTセキュリティアセスメントは計画を上回る計6社を対象に実施	○

考察

COBIT※レベル4では、ITセキュリティを担保する活動の実施を証明すること、情報資産保護およびITセキュリティ確保の遵守状況が測定できることの2点に加え、これらの改善が必要な場合に対処できる状態であることが求められています。
これらガバナンス成熟度に関する要件への対応を目的に導入した、セキュリティ内部監査を含むCSIRTによる評価活動において、2023年度はグループ会社計12社の対応状況を確認しました。さらに2023年度は、防御・検知・復旧といったセキュリティ対応の具体的内容も評価対象に加えています。これらの活動により情報セキュリティマネジメントのPDCAサイクルを確実に実行しています。

※ COBIT：ITガバナンスの成熟度を測るフレームワークで、0～5段階で評価。5が最も成熟しているレベル（Optimized）で、当社グループはレベル4（Managed）に位置すると認識。

Next Step

「情報セキュリティ規程」の各社への浸透ならびに確実な遵守を目的として、ITとOT両面においてセキュリティ対策支援を継続します。グループ統一の技術的対策として、2024年度にはさらに、ネットワーク機器の脆弱性管理、PCやサーバーの不審な挙動検出といった対策の導入を進めます。

- セキュリティ内部監査を含むCSIRTによる対策状況評価活動の継続実施（2024年度計画：IT評価12社、OT評価6社）
- 技術的な対策の導入（2024年度計画：ごく小規模拠点や出資比率の低い拠点を除く全社が対象）
- グローバルeラーニングによる従業員へのセキュリティ意識づけ教育を実施