情報セキュリティマネジメント

マテリアリティ
情報セキュリティ

ガバナンス　戦略　リスク管理　指標と目標

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を設置しています。サステナビリティ委員会では、ESGマテリアリティ重点項目※2「情報セキュリティマネジメント」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、上席執行役員 最高財務責任者CFO兼財務経理本部長管掌のもと、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、リスク管理、指標と目標＞ガバナンス
https://www.fujioil.co.jp/sustainability/sustainability_management/#governance
※2 ガバナンス、戦略、リスク管理、指標と目標＞指標と目標
https://www.fujioil.co.jp/sustainability/sustainability_management/#index

戦略

不二製油グループは、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」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

不二製油グループでは、ESGマテリアリティ・サステナビリティ課題領域「情報セキュリティ」に関するリスクと機会を、全社重要リスク項目と関連づけながら、体系的に管理しています。

全社重要リスク
リスク分類「情報システム」
https://www.fujioil.co.jp/ir/policies_and_systems/risk/

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。2024年度のeラーニング受講完了率は97.2%※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。内部監査はおよそ3年間でグループ全社をカバーする頻度で実施しており、さらに2024年度より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・自己点検を実施しています。
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(Operational Technology):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

2024年度目標	2024年度実績	自己評価
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)	2024年度実績:IT評価14社、OT評価7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)	2024年度実績:部分的に導入未済の対策はあるが、そのような例外を除き全ての対象会社に導入完了	○
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	2024年度実績:計画に従い完了	○

考察

グループ各社におけるITセキュリティ対策の評価を、従前のCOBIT※1 ベースからNIST CSF 2.0※2 などのフレームワークに基づく当社固有の指標※3 へと2025年度より変更する計画です。
これにより、ITセキュリティ対策の方向性を「ITガバナンス全般の強化」から「より実際的なリスク対応の強度向上」にシフトすることを企図しています。

※1 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)。当社グループはレベル4に位置すると認識。

※2 NIST CSF 2.0:セキュリティ対策強化のために定められた標準的なフレームワークで、対応する内容を「特定・防御・検知・対応・復旧・統治」の6機能において定義する。

※3 対策の強度レベルに応じ、スコアを1～3段階で評価 (3が最も高度)。

2025年度から2027年度の目標として、上記の全6機能におけるグループ各社のスコアリング2を目指します。
さらに事業上重要なBlommerと不二製油株式会社では「検知・復旧」の2機能においてスコア3を目指します。

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。

- 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（2025年度計画：IT評価6社）
- IT、OTの新監査手続書の作成、および監査項目に対する評価基準の定義
- 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（受講完了率100%を目標とする）