情報セキュリティの強化

考え方

IHIグループは、お客さまやお取引先の機密情報、会社の経営情報や技術情報などを確実に保護するために「IHIグループ情報セキュリティポリシー」を定め、情報の適正な管理と情報セキュリティの維持・向上に取り組んでいます。

方針

●IHIグループ情報セキュリティポリシー

IHIグループが保有する情報資産の安全性を確保し、お客さまおよびユーザや社会との信頼関係を一層ゆるぎないものにするため、ここにIHIグループ情報セキュリティポリシーを定める。

（活動の基本）

1. IHIグループは、漏洩、盗難、紛失、破壊、不正な侵入、障害および災害等から情報資産を保護し、維持するために、適切な人的・組織的・技術的諸対策を講じる。
   万一情報資産にセキュリティ上の問題が発生した場合は、その原因を迅速に究明し、その被害を最小限に止めるように努める。

（情報資産）

2. 情報資産とは、媒体を問わずIHIグループが事業の活動の中で扱う情報、および情報を扱うために必要な装置・施設・サービスをいう。

（適用範囲）

3. IHIグループ各社の役員、従業員のほか、派遣社員等、IHIグループの情報資産を利用する者に対し本ポリシーを適用する。

（法令等の遵守）

4. IHIグループは、情報資産に関する法令、規範およびお客さまとのセキュリティに関する契約上の要求事項・義務を遵守する。

（教育）

5. IHIグループ各社は、IHIグループの情報資産を利用する者に対し、必要なセキュリティの教育を行ない、セキュリティ意識の向上および維持を図る。

（運用体制等）

6. IHIグループ各社は、情報セキュリティに関する規定を定め、情報管理の責任者を置く等、情報セキュリティの運用管理の仕組みを確立し、維持および改善を含めた活動を継続的に実施する。

（経営幹部の責任）

7. 経営幹部は、率先垂範して本ポリシーを実践するものとする。本ポリシーに反するような事態が発生したときには、自ら解決に当たり、原因究明、再発防止に努め、権限と責任を明確にしたうえで、適正に対処する。

（処分）

8. 情報セキュリティに関する規定に違反する事例が生じた場合には、IHIグループ各社の就業規則等により処分する。

（公表）

9. 本ポリシーは、IHIグループの情報資産を利用する者に対して公表・通知するとともに、一般にも公表する。

情報セキュリティの強化

ガバナンス

IHIグループでは、グループDX担当役員を情報セキュリティ最高責任者とした情報セキュリティ推進体制を構築しています。DX推進委員会に置いた情報セキュリティ部会を取りまとめ機関とし、IHIの本社部門・事業領域・SBUおよび関係会社ごとに統括管理責任者を置いて、情報セキュリティ活動に取り組んでいます。経営上特に重要な事項については、取締役会への付議を行います。

●情報セキュリティ活動推進体制図

●情報セキュリティ部会

部会長	高度情報マネジメント統括本部　本部長
委員	事業領域、SBU、本社部門
事務局	情報セキュリティ部
2023年度の開催回数	3回

リスク管理

情報セキュリティマネジメントシステム

IHIグループは、IHIの本社部門・事業領域・SBUで構成する情報セキュリティ部会を年3回開催し、情報セキュリティ対策の計画・実施・点検を1年サイクルで実施しています。在宅勤務の増加、サイバー攻撃の脅威の増大など、社内外の環境を踏まえ各年度の重点施策を設定し、対策を進めています。

2019年度以降、PDCAにおける「C（Check）」機能の強化として、自組織・事業領域・コーポレート部門による3段階の情報セキュリティ監査体制を構築しています。自組織（IHIの各部門および関係会社）における内部監査、コーポレート部門による文書監査、主管部門である事業領域による監査をそれぞれ実施しています。2021年度以降は、事業領域が、主管する全てのSBU・関係会社を対象として、情報セキュリティ対策状況の監査を実施し、発見された課題に対して改善を進めています。

IHIグループの中でも国の重要な業務に携わる部署およびグループ会社では、社外の専門機関による情報セキュリティの国際規格ISO27001の認証審査を毎年受け、高いセキュリティレベルの維持に努めています。

在宅勤務における情報漏えい対策

新型コロナウイルス感染拡大防止対策としてIHIグループ全体で開始した在宅勤務は、多様な働き方の一つとして定着しています。一方、社外で情報機器を取り扱う機会が増加したことで、情報機器の不適切な利用や紛失・盗難といった情報セキュリティリスクが高まっています。

IHIグループでは、情報機器の不適切な利用を防止するため、社外での業務におけるセキュリティ順守事項について、e-ラーニングや社内報で、従業員への注意喚起を行っています。具体的には、パソコンの私的利用の禁止や本人や家族が共有する情報機器（私有情報機器）への業務情報保存の禁止などが順守事項となっています。

また、社外での業務時は原則として業務データが保存されていないパソコンを持ち出す対策を実施しており、紛失・盗難による情報漏えいリスクを低減しています。

SOCおよびCSIRTの設置

IHIグループは、年々増大するサイバー攻撃の脅威に対応するため、SOC（Security Operation Center）を設置し、PC・サーバやネットワーク機器に対するセキュリティ監視を実施しています。また、CSIRT（Computer Security Incident Response Team）を設置し、セキュリティ監視によりインシデントを検知した場合は迅速に対応する体制を整備しています。サイバーセキュリティインシデントに対して適切に対応できるようにするための対応手順書についても整備しており、侵害範囲の特定や封じ込め処置などの対応手順を記載しています。

情報セキュリティの強化

取り組み

情報セキュリティ対策

IHIグループは、情報セキュリティのリスクに対してルール・ツール・教育の3つの側面から対策を実施しています。ルール面では、「IHIグループ情報セキュリティポリシー」「IHIグループ情報セキュリティ対策基準」「情報システム利用者規程」などの諸規程を定めています。ツール面では、ウイルス対策ソフトウェアなどのセキュリティツールを導入し、適宜最新機種に更新しています。

情報セキュリティ対策レベルの評価

IHIグループでは、IPA（独立行政法人情報処理推進機構）が提供する企業向けの情報セキュリティ対策ベンチマークに基づき、毎年IHIグループ全体の情報セキュリティ対策レベルを定量的に評価しています。
2023年度は、5点満点中3.8点でした。4点を目標スコアとして、2024年度もIHIグループ全体で情報セキュリティレベルの向上に努めます。

●情報セキュリティ対策レベル評価

（単位：点、対象：IHIおよび連結子会社）

項目	2020年度	2021年度	2022年度	2023年度
情報セキュリティ対策レベル評価（5点満点）	3.4	3.7	3.7	3.8

教育・浸透

従業員への教育

IHIグループは、情報セキュリティのルールやツールに対する従業員の理解を深めるためのe-ラーニングを、全従業員を対象に毎年実施し、セキュリティ意識の維持・向上を図っています。

●e-ラーニング受講率

（単位：%、対象：IHI）

項目	2020年度	2021年度	2022年度	2023年度
e-ラーニング受講率	96.0	96.8	96.9	98.9