情報セキュリティ

基本方針

ファイントゥデイグループは、「ファイントゥデイグループ 倫理行動指針」（→P64）の中で機密情報や個人情報の漏えい、紛失などが生じないよう、これらの情報を適正に管理し、不適正な利用はしないことを定めています。この指針のもと、「ファイントゥデイグループ 情報セキュリティポリシー」などの各種規程・ルールを制定するとともに、情報管理の重要性と責任について全事業所の従業員と共有することで、保有する重要な情報資産を守り、適切に管理しています。

－情報セキュリティに関する規程・ルール

- 情報セキュリティポリシー
- 情報システム管理規程
- 情報システム利用規程
- BYOD（業務で使用する従業員個人所有の情報機器）、外部記憶媒体、情報端末、ウイルス対策、ソフトウェアに関するルール
- 機密情報管理規程
- 情報資産取扱規程
- 個人情報保護方針
- プライバシーポリシー
- 個人情報保護規程
- 特定個人情報取扱規程
- ソーシャルメディアポリシー

－ファイントゥデイグループ 情報セキュリティポリシーに定める項目

1. 目的
2. 定義
3. 情報セキュリティの推進体制
4. 外部委託先の評価
5. 教育・点検・監査
6. 具体的な手続き
7. 従業員等の義務

情報セキュリティ体制

ファイントゥデイグループは、グループ全体の情報資産と情報システムの取り扱いに関する包括的な責任者として、統括最高情報セキュリティ責任者（Chief Information Security Officer：CISO）を設置し、強固な情報セキュリティ体制の確立と継続的な強化に取り組んでいます。

グループ各社は、社内に情報資産と情報システムの取り扱いに関する管理責任者を配置し、機密情報管理、個人情報保護、情報システム管理、情報セキュリティ対策に関する諸規程の整備・運用の徹底、安全対策の実施、教育・訓練などを実践しています。また、これらの活動をCISOが監督し、適宜必要な指示などを行っています。

更に、グループ全体の情報セキュリティ体制を継続的に強化していくために、情報セキュリティに関する会議体を定期的に開催しています。

個人情報の取り扱い

ファイントゥデイグループは、個人情報を安全・安心に取り扱うことを企業の責務と認識しており、「ファイントゥデイグループ グローバル個人情報保護方針」を制定し、全グループ会社に適用しています。また、グループ各社においても、各国・地域の法令に基づきプライバシーポリシーを策定し、個人情報保護に関する各種施策を実施しています。

グループ各社・各種キャンペーンなどの施策企画では、これらの方針・ポリシーと関連法規などを踏まえ、個人情報の取り扱いについて個別の方針や利用規約などを定めています。

Webサイト　**ファイントゥデイグループ グローバル個人情報保護方針**
https://www.finetoday.com/jp/privacy-policy/

情報セキュリティ

情報セキュリティインシデントへの対応

ファイントゥデイグループは、先進的なゼロトラスト・セキュリティモデルを適用しており、情報セキュリティインシデントへの対策を強化しています。例えば、業務システムを通じた機密情報への不正アクセスを防止するためにアクセス制限などを設定しているほか、SOC（Security Operation Center）を設置し、外部からの脅威の監視やサイバー攻撃の検出・通知を24時間365日行っています。また、グループ内の各通報窓口において、情報セキュリティ関連の通報も受け付けています。

2023年度には、情報セキュリティインシデントに対応する専任のチームとして、CSIRT（Computer Security Incident Response Team）体制を整えました。CSIRTは、ファイントゥデイのIT部門、総務部門、広報部門から選出されたメンバーで構成されています。有事の際に速やかな行動・対応ができるようにすることが重要と考え、仕組みづくりにとどまらず、平時からメンバーは情報セキュリティインシデント対応に関する専門的な教育や訓練を継続的に受けています。重大なインシデントが発生した際には、グループのサイバーセキュリティ責任者であるファイントゥデイのCIO（Chief Information Officer）の発令のもと、緊急即応体制を敷いて対応します。更なる対応力向上を目的に、今後は事業部門を交えた訓練も実施する予定です。

CSIRTの役割

- 平時の訓練やチームメンバーへの教育による対応力の向上
- 情報セキュリティインシデント発生時の各種対応のリードと被害の最小化（社内外との連携）
- 社内外の一元的な報告窓口

サイバーセキュリティアセスメントの取り組み

ファイントゥデイは、セキュリティガイドラインに基づいたセルフアセスメントを定期的に実施しています。加えて公開ドメインに対する外部評価状況を適宜確認し、早期にリスクを低減できるように取り組んでいます。成熟度を多面的に評価し、その結果をもとに更なる向上のためのアクションを定義し実行することで、日々変化するサイバーセキュリティの脅威への対抗に努めています。

情報セキュリティに関する教育・研修

ファイントゥデイグループは、役員・従業員に対する教育・研修を実施し、情報セキュリティに関するインシデントの未然防止とマネジメント体制の強化に努めています。ファイントゥデイでは、サイバー攻撃の一つである「標的型メール攻撃」への対策訓練を年2回実施しています。