情報セキュリティおよび個人情報保護

セブン&アイ*HLDGS.*およびグループ各社は、 お客様の情報をはじめグループが保有する情報資産を、不正アクセスやサイバー攻撃などのさまざまな脅威から保護し、グループ全体の情報セキュリティを確保することが、経営上並びに事業上における重要課題であると認識しています。

セブン＆アイグループは、役員・全従業員および委託先を含む業務に携わるすべての関係者が情報資産を適切に取扱い、正しく利用するために方針を定め、情報セキュリティ管理体制や個人情報保護体制を構築し、すべての役員・全従業員に対する教育・訓練を通してその浸透を図ります。また、社会的要請やコンプライアンス、情報セキュリティを取り巻く環境の変化に応じたマネジメントシステムを確立し、個人情報や企業情報の適切な管理・保護に努め、継続的な改善に取り組んでいます。

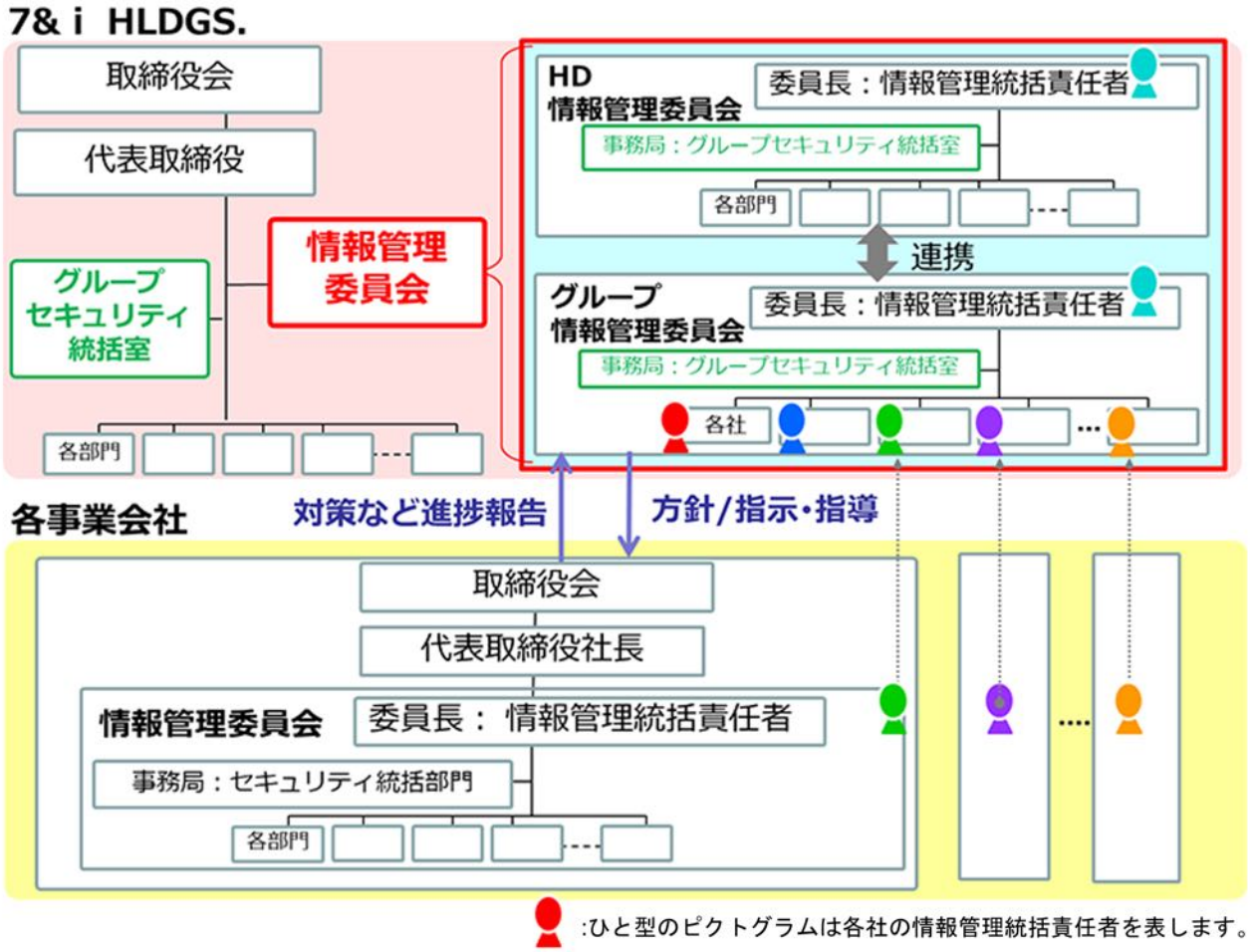
- 「情報セキュリティ基本方針」はこちら
- 「個人情報保護方針」はこちら

情報セキュリティ管理体制の構築

セブン＆アイ*HLDGS.*は、グループ全体の情報セキュリティを統括する組織として、代表取締役社長の直下組織として「グループセキュリティ統括室」を設置し、情報セキュリティや個人情報保護に関する方針や付帯する規程、ガイドラインなどを整備し、グループ各社へ展開しています。また、情報セキュリティマネジメントシステム（ISMS）の構築やセキュリティ人材の育成、モニタリング体制の整備などグループ各社の支援を行い、情報管理全般の強化に努めています。

グループを統括するセブン＆アイ*HLDGS.*の「グループ情報管理委員会」では、各社の情報管理委員会と連携し、情報セキュリティに関する施策の企画、推進、管理など、環境の変化に応じたマネジメントシステムを確立し、継続的な改善に取り組んでいます。また、配下の専門部会を通じた技術的なセキュリティ対策の徹底を図り、さらなる安全性の確保を推進しています。

情報セキュリティに関連するリスクやこれらの活動状況については、定期的に取締役会に報告して助言や指示を受けています。



情報セキュリティ管理体制

国際基準への準拠

セブン＆アイ*HLDGS.*では、情報セキュリティ管理体制の構築にあたり、情報セキュリティ関連の国際認証規格であるISO 27001、NIST（米国国立標準技術研究所）のNIST Cyber Security Framework、Center for Internet SecurityのCIS Controlsなどを参考に情報セキュリティ規程類を作成しています。

セブン＆アイ*HLDGS.*およびグループ各社は、 本規程類に基づいて、情報資産の漏えいや改ざん、サービスの停止など情報セキュリティリスクを管理する仕組み（ISMS）を構築・運用し、継続的に改善することで、情報資産の機密性、完全性、可用性の維持に努めています。なお、お客様の個人情報をお預かりしている事業会社の主要拠点および関連する部門は、ISMSの組織体制を第三者機関の審査によって評価を受け認証を取得し、また認証取得の拡大を進めています。

【ISO27001認証取得主要企業】

- 株式会社セブン＆アイ・ホールディングス
- 株式会社セブン-イレブン・ジャパン
- 株式会社イトーヨーカ堂
- 株式会社セブン・フィナンシャルサービス
- 株式会社赤ちゃん本舗
- 株式会社ロフト
- 株式会社セブン＆アイ・フードシステムズ
- 株式会社セブン＆アイ・ネットメディア
- 株式会社セブンカルチャーネットワーク

情報セキュリティに関わる事故・緊急対応

セブン＆アイ*HLDGS.*は 「重要事実報告ガイドライン」を通じて、グループ間のレポートラインを整備するとともに、情報伝達の確実性を担保し、被害や影響を最小限に抑える体制を構築しています。万が一、情報セキュリティに係るインシデントや疑わしき事象が発生した際は、法令などの報告義務に基づき、被害者ご本人および関係各部署への遅滞のない適切な報告に努めます。

なお、重大な事案については、代表取締役社長並びに情報管理統括責任者へ迅速に報告を行っています。

役員・全従業員のアウェアネス向上

セブン＆アイ*HLDGS.*は、日常業務の中で個人情報や秘密情報を適切に取扱うためには、役員・全従業員一人ひとりが重要性を理解し、情報セキュリティに対する「意識」を高め、そのうえで、正しい判断や行動をするための「知識」を持つことが必要であると考えています。

セブン&アイ*HLDGS.*は、取締役向け、管理職・一般職向けの階層に分けて、情報セキュリティおよび個人情報保護に関する最新動向や管理体制、 一般的な情報セキュリティ対策などの教育を年複数回実施しています。また、これらの教材はグループ各社にも展開し、セブン&アイグループの役員・全従業員が同じ知識レベルを習得し、自らが考え、行動できるよう啓発に努めています。

特に、標的型攻撃メールによるサイバー攻撃の脅威は日増しに拡大しており、実際の対応を想定した訓練が欠かせません。セブン＆アイ*HLDGS.*では、複数パターンの模擬メールをグループの役員・全従業員に送付して、不審メールとはどういうものか、受信した際にどのように対応すべきかなどについて、実体験を通して対応力の強化を図っています。

ITサービスに対するセキュリティの担保に向けた取り組み

適切なセキュリティ対策が行われていないITサービスは、サイバー攻撃を受けるリスクが高くなります。特に個人情報を多く保有する場合、情報漏えいが発生し被害の拡大につながる恐れもあります。

セブン＆アイ*HLDGS.*では、情報システムに対して一定水準のセキュリティの品質を担保するため、システムリリース前までにグループセキュリティ統括室がセキュリティレビューを実施しております。

また、システムリリース前や改修のタイミングなどで外部の知見を活用しながら脆弱性診断を実施しており、サイバー攻撃の起点となる重大な脆弱性が存在しないかのチェックを図り、脆弱性が発見された場合には修正してからリリースする仕組みを運用しています。

サイバーセキュリティ対策の強化について

セブン&アイ*HLDGS.*は、 日々高度化・巧妙化するサイバー攻撃を経営における重大なリスクとして位置付け、ネットワークへの不正侵入防御や適切なアクセス制御などの多層的な防御網の構築、および脅威に対応できる体制の整備、人材の教育や訓練、外部専門機関との連携などを通じて、サイバーセキュリティ対策の強化に努めています。

専門組織の設置と外部との連携

サイバーセキュリティを担う専門組織として7&i CSIRT（7&i Computer Security Incident Response Team）を設置し、セキュリティ事故が発生した際の原因分析、対応の策定などをグループ会社のインシデント対応窓口と協力して行うことで、事故の影響を最小化する体制を整えています。

また、サイバー攻撃などに迅速に対応できるよう、JPCERT/CC、日本CSIRT協議会などの外部組織と連携してサイバーセキュリティに関する攻撃情報や対策動向などの共有を実施しています。

グループ会社のインシデント対応窓口を対象に、サイバーセキュリティ事件・事故を想定した教育・訓練を年に2度以上実施し 、認識された改善点を事故対応マニュアルに反映するなど、グループ各社の事故対応能力の向上に努めています。

また、サイバー攻撃や不正ログイン等を検知する仕組みの内製化を図り、グループにおけるサイバーセキュリティ対策が効率的に行えるよう体制を構築しています。