

ゼロトラストでグループ全体のレジリエンスを次のステージへ

攻めの戦略を支えるサイバーセキュリティ体制の構築

SBIグループは、サイバー攻撃を経営上のトップリスクの一つに位置付けています。金融サービスのデジタル化や事業領域の拡大に加え、AIをはじめとする新技術の普及に伴い、リスク環境が急速に変化するなか、サイバーセキュリティの確保は、お客さま資産の保護、グループの事業継続、更には金融システム全体のレジリエンスに直結する経営課題となっています。

当社グループでは、新たな事業領域への展開やAI等の革新的技術の活用を成長戦略の重要な柱と位置付けています。こうした取り組みを支える基盤として、サイバーセキュリティを単なる防御策ではなく、持続的成長を実現するための重要な経営基盤と捉え、継続的な投資と高度化を推進しています。

こうした方針のもと、グループ横断的な規範として「グループ情報セキュリティ規程」「SBIグループ セキュリティスタンダード (SGSS)」「SBIグループ 生成AI利用ガイドライン」等を制定し、各社が準拠すべき基準を具体的に定めています。SGSSは米国国立標準技術研究所 (NIST) や CIS Controls といった国際的なフレームワークを基盤としつつ、グループ会社を事業特性とリスク許容度に応じて3つのティアに区分し、各社が遵守すべきルール項目に重みづけを行う構成としています。SGSSは毎年改定を行い、AIの進展に伴う新たなリスクを含め、変化する脅威動向を継続的に反映しています。

また、情報セキュリティ担当役員をグループ情報セキュリティ管理責任者とし、IT統括部が核となってグループ横断的な情報セキュリティ施策を実施しています。IT統括部を事務局としてSBIグループCSIRT (Computer Security Incident Response Team) を設置しており、グループ内の情報セキュリティ管理責任者や有識者が参加する連絡会を四半期ごとに開催し、サイバーセキュリティに関するグループ方針の浸透や最新情報の共有を図っています。

インシデントが発生した場合には、サイバー攻撃への対処などIT分野に特化して対応するIT統括部と、リスク全般を管理するグループリスク管理統括部が共同で対応を行い、多層的かつ総合的なセキュリティ管理の強化を図っています。両部門は隔週で情報を共有するなど、日常的に密接な連携を行っています。なお、取締役会への報告も定期的に行っています。

技術革新を支えるサイバーセキュリティ

近年、AI技術は急速な進化を遂げており、当社グループにおいても、AI活用を経営高度化の重要施策と位置付け、様々な取り組みを推進しています。その一方で、個人情報や機密情報の漏えい、自律型AIの普及に伴う統制上の課題など、AI活用に伴う新たなリスクも顕在化しています。

当社グループでは、役職員教育やグループガイドラインの整備に加え、技術進展に応じた管理体制の高度化を継続的に進めています。また、自律的に動作するAIエージェントの普及も見据え、適切な管理・統制体制の高度化を推進しています。同時に、クラウドサービスの利活用拡大に伴うリスクへの対応も進めています。セキュリティ設定における人的ミスやリスク考慮の漏れは依然として重要なリスクとなっており、当社グループではそれらを一元的に監視し、設定の不備等が発生した場合には強制的に是正するソリューションを導入しています。また、各事業部門におけるシャドーITの極小化に向けては、IT統括部が管理・運用するプラットフォームの利用を促進しています。

加えて、業務委託先を含むサプライチェーン全体でのセキュリティ水準の確保や、国家支援型の脅威アクターによる高度化・巧妙化する攻撃への対応についても、重要な経営課題の一つと捉えています。これらの課題は一企業のみで完結するものではなく、グローバル水準のセキュリティ技術や脅威情報を活用した体制強化が不可欠と認識しています。技術進展や脅威環境の変化を踏まえ、当社グループでは今後も継続的な投資とセキュリティ高度化を躊躇なく実行していく方針です。

ゼロトラストを核とした多層防御戦略

規模や成熟度が様々な会社が存在する当社グループでは、サイバーセキュリティに関する体制や人的リソース、知識の蓄積等の状況が不均衡である場合があり、その平準化を図ることが常に求められています。こうした状況を踏まえ、当社グループは、「インシデントの未然防止」「発生時の迅速な検知・封じ込め」の両軸で取り組みを進めています。予防の中心軸となるのが、「ゼロトラスト」を基盤とするグループ共通のセキュリティプラットフォームです。「いかなるアクセスも無条件に信頼しない」という考え方のもと、継続的な認証・検証を前提としたセキュリティ基盤をグループ全体で展開し

ています。また、グループ内通信の可視化と継続的な監視を通じて、インシデントの予兆を早期に検知・封じ込める体制を構築しています。

その一方で、当社グループでは「侵害は起こり得る」という前提に立ち、被害影響の極小化にも注力しています。当社グループは多数の事業会社で構成されるコングロマリットであることから、一部の事業会社への侵害がグループ全体へ波及するリスクを踏まえ、ネットワークを細分化し、攻撃の拡散を遮断するマイクロセグメンテーションをグループ全体へ展開しています。

このように高度化・複雑化する脅威に対して、「可視化」と「分離」を中核とした防御戦略のもと、グループ全体でゼロトラスト基盤の高度化を推進し、強靱な多層防御体制の実現を目指しています。

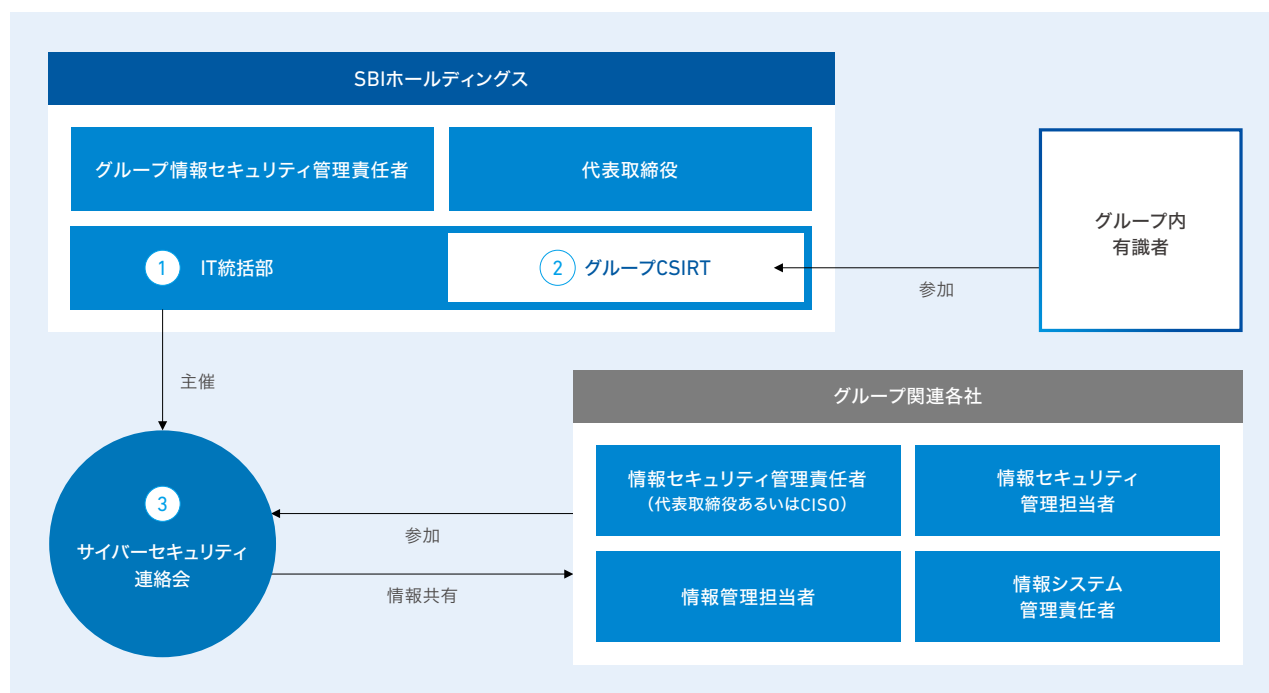
サイバーセキュリティ強化に向けた人材育成

当社グループでは役職員それぞれにセキュリティ対策の教育プログラムを実施しており、経営層に対しては外部有識者を招聘し研修を実施するほか、取締役会においても定期的

に議論を行っています。グループ子会社のシステム運用管理・担当者に対しては、外部講師によるセミナーを定期的で開催するほか、サイバーセキュリティに関する専用の情報共有ポータルを通じて、会社の規模や分野によって偏りがちな知識の平準化を行っています。加えて、昨年度はAIを悪用したボイスフィッシングやビジネスメール詐欺等の脅威拡大を踏まえ、経理・人事・サービスデスク等のバックオフィス部門に対する実践的なセキュリティ教育も強化しています。全従業員に対してはeラーニングを毎年必修とし、倫理観の醸成や知識の共有化を図っています。

こうした活動が評価され、当社は(一社)日本IT団体連盟が2026年1月20日に公表した「サイバーインデックス企業調査2025」において、「優れた取組姿勢および情報開示が確認できた企業」として3年連続で認定されました。当社グループは今後も、セキュリティを確保しつつ技術進化の恩恵を享受するべく、新たな技術動向を踏まえサイバーセキュリティ対策の継続的な高度化を推進するとともに、2～3年単位でのロードマップの実行および機動的な見直しを通じて、持続可能で強靱なセキュリティ体制の構築に取り組めます。

サイバーセキュリティ体制図



主な組織の概要

- ① SBIグループ全体のサイバーセキュリティを管理
- ② 金融業のグループ各社からの参加者も含め、グループ全体でのCSIRTを形成
- ③ グループ全体でのサイバーセキュリティに関する情報共有を図る会