システムリスク管理

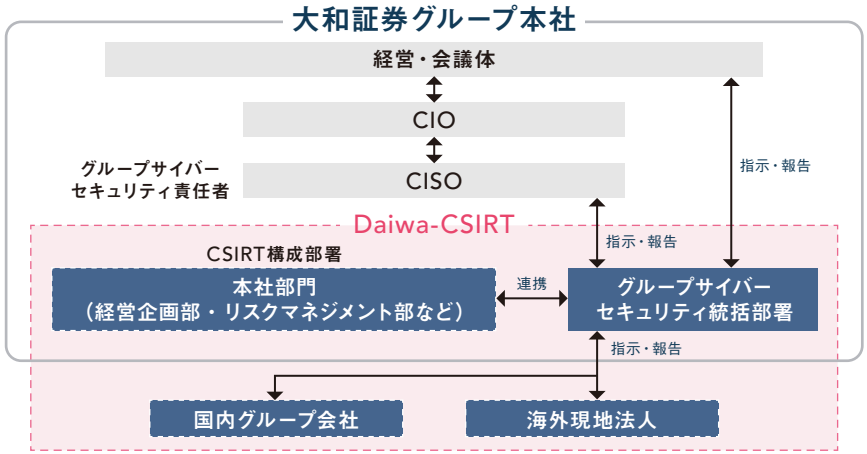
金融機関を取り巻く環境変化によりリスクは複雑化しており、未然防止や特定事象を想定したBCPだけでは重要業務の継続が困難となるおそれがあります。当社グループは、未然防止策を尽くしてもなお業務中断は起こり得るとの前提に立ち、オペレーショナル・レジリエンス(業務の強靭性・復旧力)の確保に取り組んでいます。サイバーセキュリティ、BCP、ガバナンスの3層構造を柱に、お客様に安心してご利用いただけるサービスの提供に努めています。

サイバーセキュリティ

国内外でサイバー攻撃による重大インシデントが相次ぎ、AIを活用した攻撃の高度化・多角化が進んでいます。脆弱性を自律的に発見し短時間で攻撃を完遂し得る先進的なAIの登場により、高度なサイバー攻撃は現実的な脅威です。攻撃に国境はなく、海外からの脅威を含めた包括的な対応が求められています。当社グループは、サイバーセキュリティをグループ経営上の重要課題と位置付け、グループ横断の専門組織であるDaiwa-CSIRTを中心に外部機関とも連携しながら、サイバー攻撃に対する防御力およびレジリエンスの高度化に継続的に取り組んでいます。

2026年7月には、サイバーセキュリティ管理の高度化を目的に専担の統括部署を新設しました。また、グループCISO(Chief Information Security Officer)を設置し、ガバナンス体制を強化しました。これによりサイバーリスクを経営レベルで一元的に把握・管理し、迅速かつ実効性のある意思決定と対策推進を可能としています。

新たな体制のもと、リスクベースの考え方にもとづき重要性・影響度を踏まえた優先順位付けを行い、グループ横断でのサイバーリスクの可視化とグループ会社を含む統一的な管理・モニタリングを強化しています。Daiwa-CSIRTのインシデント対応機能と統括部署のガバナンス機能を一体的に強化し、識別・防御・検知・対応・復旧の各プロセスを通じた一貫したサイバーレジリエンスの高度化を推進しています。



またお客様に安心してお取引いただける環境を提供するため、オンライントレードにパスキー認証を導入しました。パスワードに依存しない生体認証により、フィッシングや不正ログインのリスクを大幅に低減しています。

BCP態勢の強化

BCP面では、首都直下型地震などの大規模災害への備えとして、2025年度までにBCP対応拠点の構築を完了しました。これにより緊急時のシステム継続性の向上に加え、地理的リスクの分散とビジネスレジリエンスの強化を実現しています。2026年度には経営層・従業員向けにBCP訓練を実施し、実効性のさらなる向上を図ります。

3層ガバナンス(AI・データ・IT)の高度化

AIガバナンス、データガバナンスおよびITガバナンスは相互に関係・補完し合うものであるため、当社グループではこれらを「3層ガバナンス」として一体的に捉えて、その態勢強化に取り組んでいます。AIガバナンスでは、「大和証券グループ AIガバナンス指針」を策定・公開し、社会貢献、人間中心のAI、透明性と説明責任、適正利用、法令遵守とプライバシー保護、セキュリティ、態勢・リテラシー向上の7項目を定めています。また「グループAIガバナンス委員会」では、コンプライアンス担当・人事担当・CROなどの役員がAIの提供・活用・リスクコントロールなどを多面的に議論しています。

今後、AIエージェントの普及を安全かつ効率的に実現するため、統合管理基盤の整備、扱うデータの品質管理、権限管理、挙動モニタリングといった施策に取り組んでいきます。

当社グループのAIガバナンスについては、下記のウェブサイトをご参照ください。
https://www.daiwa-grp.jp/about/governance/ai_governance.html