サイバーセキュリティ

基本的な考え方

〈みずほ〉では、サイバー攻撃を経営上のトップリスクの一つと位置づけ、「サイバーセキュリティ経営宣言」に基づいて、継続的にサイバーセキュリティ対策を推進しています。

サイバーセキュリティ経営宣言　https://www.mizuho-fg.co.jp/company/structure/it/cybersecurity/index.html

社会全体のデジタル化進展に伴うサイバー攻撃の増加

世界の多くの地域ではデジタル化が進展しており、なかでもサイバー空間は個人情報が大量に流通・蓄積される場となっています。また、国家の関与が疑われる攻撃も活発化しており、企業が持つ機密情報を狙ったサイバー攻撃事案も増加しています。

〈みずほ〉におけるサイバーセキュリティの取り組み

Mizuho-CIRT※1を中心に、高度なプロフェッショナル人材を配置し、外部の専門機関とも連携したインテリジェンスや先進技術を駆使しながら、統合SOC※2等による24時間365日の監視体制を整え、ウイルス解析、多層的防御等、レジリエンス態勢強化に取り組むとともに、社内検証だけでなく第三者による客観的評価も実施することで、対策強化を図っています。また有事に備え、TLPT※3や半年に1回以上のフィッシングメール訓練等の実施や人材育成、サプライチェーン対策、お客さまの意識啓発にも注力しています。

※1. Cyber Incident Response Team　※2. Security Operation Center
※3. Threat Led Penetration Test（実際の技術を使用してシステム侵害を試みることで、セキュリティの強度を確認するテスト）

〈みずほ〉におけるサイバーセキュリティ管理体制

〈みずほ〉では、取締役会監督のもと、当社グループ・グローバルのサイバーセキュリティ管理業務全体を統括するグループCISO※4の設置に加え、主要な子会社にもCISOを設置しています。また、グループCISOを2線機能におけるグループCIOに対する牽制機能明確化の観点から、グループCIOのほかグループCROの傘下にも位置づけ、ダブルレポーティングの報告体制をとることで、サイバーセキュリティ態勢強化を図っています。また、各種対策の推進状況については、経営会議・取締役会まで報告を行い、サイバーセキュリティに関する方針や資源配分を見直しています。

※4. Chief Information Security Officer