

サイバーセキュリティのスキルを競う独自のコンテストであるCTF(キャプチャー・ザ・フラッグ)プログラムを通じて、セキュリティ初心者から経験者まで幅広い層が参加できる学習機会を提供している。

このように、NTT-CERTは基本的な活動を着実に遂行しながら、新たな脅威や課題に対応するための取り組みを継続的に発展させている。予防的なセキュリティ対策の強化、脆弱性への包括的な対応、実践的な対応力の向上、そして人材育成の革新的な展開を通じて、NTTグループ全体のサイバーセキュリティ能力の向上を実現している。

(2) セキュリティ体制の強化

セキュリティガバナンスの確立とその歩み

デジタル社会の進展に伴い、企業が取り扱う個人情報は飛躍的に増加している。サイバー攻撃の高度化や国際的な法規制の強化により、その適切な管理は企業の重要な責務となった。特に、情報通信インフラを支えるNTTにとって、ICTサービスの安全性確保と顧客の情報資産保護は、最も基本的な社会的責務である。

セキュリティ対策の不備は、企業としての信頼を損なうだけでなく、知的財産の流出やデジタルインフラへの信頼低下につながり、社会全体のデジタル化を妨げる要因ともなりかねない。一方で、強固なセキュリティ基盤を確立することは、顧客企業のビジネスリスクを低減し、デジタル変革を推進する重要な要素であると同時に、新たな市場機会の創出にもつながる。

こうした考えのもと、NTTは「NTTグループ情報セキュリティポリシー」を策定し、グループ全体で統一的なガバナンス体制の構築を進めてきた。2015年には「グループCISO委員会」を発足し、セキュリティ対策の方針策定から実施、評価までを一貫して管理する体制を整えた。また、グループ横断的なワーキンググループを設置し、日々変化するセキュリティ課題への迅速な対応を整えてきた(図表5-4-2)。

2018年、セキュリティガバナンスの強化を目的に、これまで代表取締役副社長が兼務していたCISO(最高情報セキュリティ責任者)を専任ポストとし、横浜信一氏が就任。NTTグループ各社と連携したガバナンス体制を構築し、グループCISO委員会やセキュリティマネジメント連絡会の定期開催を推進した。さらに、幹部会議を通じてセキュリティに関する社会動向の共有を強化し、インシデント発生時には迅速に社長へ報告する体制を確立した。「セキュリティがあるからNTTグループを選んだ」と評価される存在をめざし、顧客とNTTグループ双方のDXを支える取り組みを加速。この方針は、セキュリティを単なる防御策ではなく、ビジネス成長のための戦略的投資と位置付ける考えに基づいている。

2020年には、グループ全体のセキュリティガバナンスをさらに強化するため、NTTのセキュリティ機能を集約・一元化し、「セキュリティ・アンド・トラスト室」を新設した。グループ横断的なセキュリティ施策の立案と推進、NTT(研究所を含む)のサイバーセキュリティ活動やインシデント対応の強化、グループ全体の代表としての対外的な情報発信や外部機関との連携、ならびにグループ横断での人材育成を主なミッションとし、NTTグループ全体のセキュリティレベル向上をめざした。

また、グループ全体のセキュリティを維持・向上させるため、「三線防御」の考え方を取り入れ、より高度なリスク管理体制を整備した。このモデルでは、第一線(各職場)が現場でのセキュリティ対策を実施し、第二線(セキュリティ推進組織)がグループ全体の方針策定やリスク管理を担い、第三線(監査組織)が独立した視点で監査・検証を行う。こうした三層のアプローチにより、実務・戦略・監査の各レベルでセキュリティを多層的に管理し、グループ全体のセキュリティガバナンスを強化する体制を整えていった(図表5-4-3)。

NTTグループ代表CSIRT「NTT-CERT」設置

2020年代に入ると、国家・経済安全保障環境の激化や中期経営戦略推進に伴う新領域進出を背景に、グループセキュリティガバナンス及び顧客向けサービスセキュリティの一層の強化が求められた。そこで、2025年、世界のセキュリティ組織との連携強化、グループ各社とそのサービスセキュリティ支援強化を目的に、セキュリティ・アンド・トラスト室内にグループ代表CSIRTとして新「NTT-CERT」を設置した。

NTT-CERTは、グループ内外のCSIRTとの連携を担うコーディネーション機能と、脅威分析、デジタルフォレンジック、マルウェア解析、脆弱性分析等の分析機能とを備えており、グループ各社へのセキュリティガバナンス、インシデント対応支援と、最新の知見の共有を両立させている。CSIRTの国際団体「FIRST」(Forum of Incident Response and Security Teams)や日本国内団体「NCA」(一般社団法人日本シーサート協議会)にも加盟し、最新のセキュリティ情報を収集し、活用。グループ内に展開している。

NTT-CERTでは、2004年より2025年3月までにNTT研究所における同名の取り組み(本節1項(1)参照)の活動の下で蓄積された研究開発成果が活用されている。

ゼロトラストへの対応とリスク対応の更なる強化

2020年以降、新型コロナウイルス感染拡大の影響でリモートワークが急速に普及し、従来の「境界型防御」に替わってセキュリティモデルの限界が明らかになった。従来は社内ネットワークに接続する端末を信頼し、外部からのア