4 サイバーセキュリティの強化

4-1. NTTグループを守る

(1) NTT-CERTの設立

設立の背景

1990年代後半、インターネットの普及は社会の在り方を一変させた。電子商取引の拡大、企業内ネットワークの発展、そしてモバイル通信の進化は、世界をリアルタイムでつなぐインフラを構築した。しかし、その利便性の向上とともに、新たなリスクが浮かび上がっていた。サイバー犯罪の増加、不正アクセスやウイルスの流布、個人情報の漏洩といった問題は、企業や政府機関にとって深刻な脅威となった。

NTTも例外ではなく、情報通信インフラを支える企業として、通信ネットワークの安定性を維持し、顧客のデータを保護する責任があった。しかし当時、グループ内には統一的なインシデント対応組織が存在せず、各事業会社が個別にセキュリティ対策を講じる状況が続いていた。サイバー攻撃の高度化に対応するためにも、グループ全体を統括する専門組織の必要性が高まっていた。

このような背景を受け、NTTは2004年1月、NTT情報流通プラットフォーム研究所（当時）内に「先端セキュリティセンター」を発足させ、インシデント対応に関する基礎研究と調査を開始した。そして、同年10月には、グループ全体のセキュリティ対応を統括する正式な組織として「NTT-CERT（NTT Computer Security Incident Response and Readiness Coordination Team）」を設立した（**図表5-4-1**）。

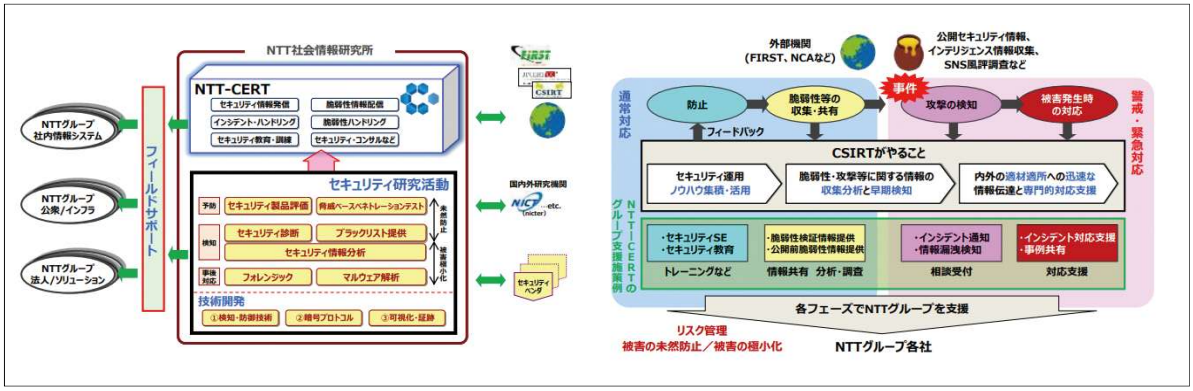
設立当時、欧米では企業や政府機関が競争力維持のため、情報漏洩や不正アクセスなどのサイバーインシデントに迅速に対応する専門チームであるCSIRT（Computer Security Incident Response Team）の設置が急速に進められていた。NTT-CERTの設立はこうした国際的な動向を踏まえたものだった。NTTはセキュリティ対策の強化の観点から、グループ内でのインシデント対応能力の向上と国内外のセキュリティ機関との連携強化に向け、NTT-CERTを設立し、グローバルな視点での脅威対策を推進できる体制を整えた。

グループ内での信頼確立

しかし設立当初は、グループ内での認知度の低さと事業会社との信頼関係の構築が課題となった。当時、各事業会社には既に独自のセキュリティ担当部門が存在し、新設されたNTT-CERTの役割が十分に理解されていなかったためである。このため、NTT-CERTがどのようにインシデント対応を支援し、グループ全体のセキュリティを強化できるのかを明確に伝えることが不可欠であった。

この課題に対応するため、NTT-CERTは2004年から2006年にかけて各事業会社を訪問し、直接説明を行う草の根活動を展開した。セキュリティインシデントのリスクや迅速な対応の重要性、そしてNTT-CERTの具体的な

図表5-4-1 ▶NTT-CERTの概要



出所：NTT社会情報研究所『サイバーセキュリティアニュアルレポート2023』（2023年11月）をもとに作成