支援内容を伝えることで、徐々に各事業会社の理解を得ていった。最初は「本当に役に立つのか」といった懐疑的な声もあったが、実際のインシデント対応を通じてその有用性が証明されるにつれ、NTT-CERTの存在意義がグループ内に浸透していった。

また、NTT-CERTが研究所内の組織として設置されたことも、事業会社との信頼関係構築において大きなメリットとなった。本社の管理部門内に設置された場合、事業会社側が「管理・統制のための組織」として警戒する可能性があった。しかし、技術研究機関の一部として発足したことで、現場のエンジニアからは「技術的に信頼できる専門チーム」として受け入れられ、よりスムーズな連携が実現した。

さらに、NTT-CERTは国際的な情報収集力の強化にも注力し、2005年には国際的なCSIRTネットワークである「FIRST（Forum of Incident Response and Security Teams）」に加盟。これにより、世界中のセキュリティチームとの情報共有が可能となり、最新の脅威情報を迅速に入手し、国内外のセキュリティ対策を適用できる体制を確立した。

こうした取り組みを積み重ねることで、NTT-CERTはグループ内での認知度と信頼を確立し、NTTグループ全体のセキュリティ基盤を支える中心的な組織へと成長していった。

活動内容と主な取り組み

2025年現在、NTT-CERTは、NTT社会情報研究所に所属し、NTTグループのセキュリティ対策の中核を担っている。情報セキュリティに関する相談窓口を提供し、グループ内外の組織や専門家と協力しながら、セキュリティインシデントの検知・解決・被害の最小化、さらには発生予防を支援している。その対象者は、NTTグループの情報システム管理者、運用担当者、利用者、セキュリティ管理者などである。

具体的には、以下のような活動を通じてNTTグループのセキュリティ強化に取り組んでいる。

1.情報セキュリティ関連技術の調査・研究・開発
2.セキュリティインシデントや脆弱性の解析
3.有効な施策・対策の普及と啓発
4.セキュリティインシデント対応の支援
5.NTTグループのセキュリティ窓口（Point of Contact）の運営
6.CSIRTの構築支援及び連携強化
7.情報セキュリティに関するトレーニングプログラムの開発・運営

これらの基本的な活動を基盤としながら、NTT-CERTは近年、サイバー攻撃の高度化とDXの進展に伴う新たな脅威に対応するため、より実践的な取り組みを展開している。特に、システム開発段階からのセキュリティ確保と、複雑化する脆弱性への包括的な対応を重点施策として推進している。

例えば、IoT機器の普及やクラウドシステムの活用拡大により、従来型の境界防御だけでは十分な対策とならないケースが増加している。このため、NTT-CERTはシステムやサービスの開発段階から適切なリスクアセスメントを実施する取り組みを強化している。

2022年度には、システム種別や開発形態に応じたリスクアセスメント手法を確立。キャリアネットワーク、インターネット公開システム、IoT関連システムなど、システムの特性に応じた評価方法を整備するとともに、新規開発や機能追加といった開発形態ごとの評価ポイントを明確化した。また、システム構成図のテンプレート作成や、想定される脅威の一覧化など、開発者の負担を軽減する取り組みも進めている。

脆弱性情報の収集・分析においては、複数の情報源を組み合わせた重層的なアプローチを採用している。JPCERT/CC（一般社団法人JPCERTコーディネーションセンター：日本における情報セキュリティ対策活動の向上に取り組む民間の非営利団体）やIPA（独立行政法人情報処理推進機構）からの公開前脆弱性情報、NVD（米国国立標準技術研究所（NIST）が運営する脆弱性データベース）の詳細情報、さらにはダークウェブからの情報収集まで、幅広い情報源からの知見を統合し、NTTグループ全体の対策に活かしている。

2022年度の分析では、年間2.5万件を超える脆弱性が新たに報告され、特にAndroid OSやブラウザ関連の脆弱性が増加傾向にあることが判明。こうした状況を踏まえ、NTT-CERTはCISA（米国サイバーセキュリティ・インフラセキュリティ庁）が提供するKEV（実際に攻撃に悪用されたことが確認された脆弱性リスト）との連携を開始し、実際に攻撃に悪用されている脆弱性を優先的に特定して、グループ内での対策を促進した。

また、重要インフラを標的とする攻撃や国家規模のイベントにおけるサイバーセキュリティ対策にも積極的に関与している。2023年のG7広島サミットでは、NTTグループ内に「サイバー統括班」を設置し、24時間体制での監視強化やDDoS攻撃への対策強化など、包括的な防衛体制を構築した。この経験は、2025年の大阪・関西万博に向けた長期的なセキュリティ計画の策定にも活かされており、地政学的リスクを考慮したモニタリング体制の強化やグループ全体でのガバナンス強化を進めている。

人材育成の面では、技術的な対策と並行して革新的なアプローチを導入している。2023年6月には「西日本横断サイバーセキュリティ・グランプリ」を開催し、500人以上の参加者を得て、実践的なセキュリティスキルの向上を図った。特に、「WEST-SEC CTF」と題したハッキング技術や