攻撃者視点でのセキュリティ強化

防御側の視点だけでなく、攻撃者視点を取り入れた実践的なセキュリティ強化にも取り組んでいる。2019年には、攻撃者の視点に立って疑似的なサイバー攻撃を行うレッドチームを設立した。サイバーセキュリティの世界では、新しい攻撃手法が次々と生み出され、攻撃者側は一度でも成功すればよいのに対し、防御側はすべての攻撃を防ぐ必要がある。このような状況に対応するため、内部からの疑似攻撃を通じてセキュリティの課題を洗い出している。

レッドチームの活動は単なる模擬攻撃にとどまらず、攻撃後にはシステムの脆弱性や組織としての課題を分析・整理し、改善策を提案する。場合によっては、実際の改善プロセスの実行支援まで行い、グループ全体の防御力向上に貢献している。

さらに、2022年には「バグ・バウンティ・プログラム」の試験運用を開始し、2023年から本格導入した。バグ・バウンティとは、情報システムに潜む脆弱性を発見した人に報奨金を支払う制度であり、外部のセキュリティ研究者やエンジニアが積極的に参加することで、未知の脆弱性を早期に特定する仕組みとなっている。

このプログラムは、セキュリティ向上だけでなく、攻撃者視点でのスキルを磨く機会を提供することで、グループ内の技術者が切磋琢磨できる環境を整えている。試験運用を通じて、バグ・バウンティがNTTのセキュリティ強化と人材育成に貢献することが明らかとなり、継続的にこの制度を洗練させていくことになった。

全社員に向けた取り組み

2015年に開始された認定制度のうち、初級認定については、認定者の増加とセキュリティの重要性の高まりを踏まえ、2020年度より海外社員を含むNTTグループ全社員を対象としたセキュリティ研修プログラムとして再スタートした。これは、「セキュリティは特定の技術者だけのものではなく、全社員が意識すべきものである」という考えを浸透させるための取り組みである。

一般的に、セキュリティ研修は「内容が難しそう」「業務の利便性を損なうのでは」といったイメージから敬遠されがちである。しかし、同研修では、芝居風の機知に富んだ冒頭メッセージやアニメーション動画を活用した親しみやすいコンテンツを導入し、社員の興味を引きつける工夫を施した。

特に、「怪しいと思ったらすぐ報告」という意識付けを強化し、全社員がサイバー脅威に気づいた際に迅速に対応できるよう努めている(**図表5-4-5**)。

日本全体のセキュリティ人材育成への貢献

NTTは、セキュリティ人材の育成をグループ内にとどめず、日本全体の人材強化にも取り組んできた。例えば

図表5-4-5 ▶全社員向けセキュリティ研修の様子

出所：NTT『アニュアルレポート2021』

2015年には、産業界全体でのサイバーセキュリティ人材育成を目的として発足した「産業横断サイバーセキュリティ人材育成検討会」に設立当初から事務局として関与。企業が必要とするセキュリティスキルの明確化や、産業界における協力体制の構築を推進した。2017年にはこの組織が法人化され、特に重要インフラ分野を含む企業間の連携がさらに強化された。

また、産学連携による人材育成にも注力している。2015年には早稲田大学に「NTT寄附講座：サイバー攻撃対策講座」を開設し、実践的なセキュリティ教育を提供。次世代のサイバーセキュリティ専門人材の育成に貢献している。さらに、若手技術者の発掘・育成を目的とする「セキュリティ・キャンプ協議会」に参画し、将来のサイバーセキュリティ分野を担う人材を支援してきた。

加えて、業界横断の情報共有とセキュリティ強化を目的とする一般社団法人「ICT-ISAC Japan」にも参加。国内の通信事業者やソフトウェアベンダーと連携し、サイバー攻撃の分析や情報共有を通じて、日本のICTインフラ全体のセキュリティ向上に貢献している。

さらに、NTTはプライバシー保護技術の研究開発にも取り組んできた。その一環として、2015年に一般社団法人情報処理学会コンピュータセキュリティ研究会が主催する「プライバシーワークショップ(PWS2015)」に参加。同ワークショップ内で開催された「PWS CUP匿名加工再識別コンテスト」では、NTTの参加チーム「Ψ沈黙のジャスティスΨ」が総合優勝を果たし、匿名化技術と再識別技術の分野における高い技術力が評価された。

NTTは、こうした研究開発の成果を活かしながら、専門人材の育成や産業界との連携を継続的に強化している。

(3) グローバル連携の深化

NTTグループ内外との連携

NTTは、One NTTのもと、グローバル事業の競争力強化に向けて、セキュリティ分野においても国際的な連