包括的なコンサルティングサービスの提供

NTTグループは、企業のセキュリティ対策をより強固なものとするため、包括的なセキュリティ診断やコンサルティングサービスの提供にも注力している。NTT西日本の法人ユーザー向けビジネスを行う子会社のNTTビジネスソリューションズでは「セキュリティ診断サービス」を提供し、ウェブサイトの脆弱性診断を実施するとともに、具体的な対策を提案することで、サイバー攻撃のリスクを低減する取り組みを進めている。

さらに、NTTコムウェアでは、OSやミドルウェアの既知の脆弱性を特定する「プラットフォーム診断」と、ウェブアプリケーションの固有の脆弱性を診断する「Webアプリケーション診断」を組み合わせてシステム全体のリスク評価を実施し、企業がサイバー攻撃を受ける前に脆弱性を特定し、適切な対策を講じられる環境を整えている。

加えて、NTTは大企業向けの高度なセキュリティソリューションだけでなく、中小企業向けのサイバーセキュリティ対策の拡充にも取り組んでいる。NTT東日本と連携し、「おまかせサイバー見守り」や「おまかせアンチウイルス」などのサービスを展開し、企業の規模を問わず、サイバー脅威に対応できる環境を提供している。

産業制御システム向けサービスの展開

NTTグループは、産業制御システム向けのセキュリティ強化にも積極的に取り組んでいる。2018年には、それまでNTTと三菱重工が共同開発を進めてきた重要インフラ(社会基盤)などの制御システム向けサイバーセキュリティ技術「InteRSePT」を、NTT、NTTデータ、NTTコミュニケーションズ、三菱重工業が共同で販売開始し、発電所、化学プラント、交通システムなどの重要インフラのセキュリティ対策を強化した。この技術は、未知のサイバー攻撃に対するリアルタイム異常検知と自動対応を可能にし、システムの運用を中断することなく脅威を検出・対処できる点が特徴である。

従来のシグネチャベースのセキュリティ対策では対応が難しい攻撃にも、AIや機械学習を活用して適応し、より精度の高い防御を実現している。また、汎用ハードウェアとネットワークスイッチを統合した設計を採用することで、導入コストの削減と省スペース化を図り、幅広い産業分野への適用を進めている。

さらに、近年は企業のIT環境がクラウドへと移行し、ネットワークの境界が曖昧になる「ゼロトラスト」の概念に基づいたセキュリティ強化が求められている。これに対応するため、エンドポイントの脅威を検出し、対応するEDR(Endpoint Detection and Response)のマネージドサービスを提供し、SOCと連携してクラウド環境のセキュリティ監視を強化することで、クラウド上のサイバー脅威にも迅速に対応できる体制を構築している。

また、開発と運用を密接に連携し、システム開発の全プロセスにセキュリティ対策を組み込む「DevSecOps(デブセックオプス)」の推進にも注力している。これにより、アプリケーション開発の段階からセキュリティを確保し、脆弱性のリスクを低減する取り組みを進めている。