特集 3

安全安心な社会へ貢献するR&D

安全安心なネットワークのため サイバー攻撃の対処を実現する技術

NTTサービスイノベーション総合研究所

NTTはICTの利用により社会の環境負荷低減に貢献することを宣言しています。このためには、提供するネットワークが安全安心に利用できることが必要です。
IoTの進展等によりネットワークにつながるデバイスは飛躍的に増大し、新たなビジネスチャンスが生まれる一方で、脆弱なセキュリティ環境にあるIoTデバイスなど新たな領域への脅威が急速に拡大しつつあります。
NTTでは安全安心に利用できるよう、セキュリティ技術の開発に注力しています。

激化・巧妙化するサイバー攻撃に対抗するセキュリティ開発

IoTの急速な進展に伴い、IoTデバイスはセキュリティ面で脆弱なため、容易に乗っ取られてボット化したり、DDoS（Distributed Denial of Service）攻撃などのサイバー攻撃が大規模化する要因になることが懸念されています。

NTTグループでは、このようなセキュリティを取り巻く環境変化に対応して、①激化・巧妙化するサイバー攻撃への対抗、②IoTの進展等に伴う新たな脅威への対応、③データ交換・蓄積・活用時のセキュリティ向上――の3つをセキュリティR&Dの方向性として定め、世界最先端の暗号技術やサイバー攻撃対策技術を生かして幅広い研究開発を行っています。

特にNTTグループのネットワーク基盤を含む重要インフラ等の防衛力向上に向けては、悪性化するドメインを予測するドメイン評価技術や悪性URLを高効率で抽出するハニーポット技術、高度なログ分析による未知マルウェア検知技術といった「攻撃検知」、攻撃に関する情報や対策などのセキュリティ・インテリジェンスの収集、インシデント発生時の事後対処やフォレンジック調査といった「運用」、脆弱性や攻撃などの検知後の自動的な機器制御によってシステムのセキュリティレベルの維持・早期回復を図るセキュリティオーケストレーション技術といった「防御」の各機能を組み合わせた多層防御の考えのもとで、各々の技術の高度化をめざした研究開発を進めています。

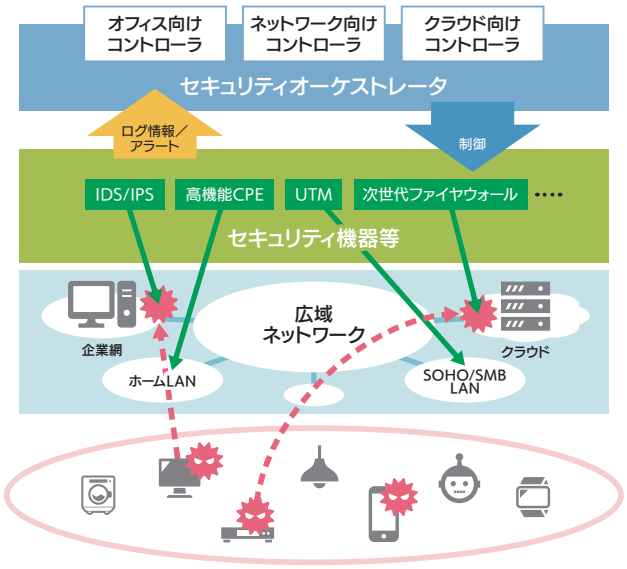
セキュリティオーケストレーション技術

NTTでは、セキュリティ機能を面的かつ多層的に配置し、サイバー攻撃からトータルで守り抜く防御システムとして、サンドボックスや脅威情報基盤と連携し、標的型攻撃への初動対処を実現するセキュリティオーケストレーション技術を、オフィスネットワークやクラウドをターゲットに開発を行ってきました。

急速に導入が進むUTM※を利用するお客さまについても、脅威情報基盤と連携し、従来よりもヒット率の高い脅威情報（ブラックリスト）をUTMに自動配信しオペレータの負担軽減と安全性の向上を実現しています。

今後、IoTの進展で多種・多様なIoT機器がネットワークに接続されるとともに、サイバー攻撃の大規模化・巧妙化が想定され、セキュリティ脅威が、顧客、サービス提供者、キャリアで高まっています。これに対して、IoT時代を見据えたセキュリティオーケストレーション技術の確立をめざします。

※UTM：統合脅威管理。複数の情報セキュリティ対策を統合的に実施できるため、複数の機能からなる高度な情報セキュリティ対策を専門知識を必要とせず導入できる。



セキュリティオーケストレーション技術