グローバルな脅威に対抗するセキュリティR&D

新たなセキュリティ脅威が世界規模で拡大し続けており，2020年に向けて日本をねらった海外からの攻撃も予想されます．本特集ではグローバルなセキュリティ脅威に対抗するための重要となるポイントを延べ，それらに対応するためのセキュリティR&Dの取り組み方針を紹介します．

中津留 毅（なかつる たけし）/中嶋 良彰（なかじま よしあき）
三好 潤（みよし じゅん）/高橋 克巳（たかはし かつみ）
NTTセキュアプラットフォーム研究所

グローバルなセキュリティ脅威

NTTグループでは，グローバル・クラウドサービスを事業の基軸とすべく積極的にビジネス展開を進めています．そのために，多様なICTサービスをグローバルでビジネスを展開するお客さまのニーズに応じて，全世界に提供できる体制を強化しています．グローバルビジネスにおいても，ICTはさまざまな分野のさまざまな業務において活用される重要な技術となっており，サイバー攻撃を受けてサービスが停止したり，情報が漏洩したりするなど大きな被害を伴う事故が多発しています．近年，これらのサイバー攻撃は，企業の機密情報や金銭の搾取を目的とした，標的を絞って行われるケースも多く報告され，被害額も大きくなっています．グローバルビジネスにおけるこれらの問題に取り組むために，NTTグループではMSSP（Managed Security Service Provider）各社がサービスを展開しています．グローバルビジネスにおけるサイバー攻撃は，産業スパイが企業の機密情報を窃取するために攻撃をしたりするようなものや，電力，ガス，通信などの重要インフラの動作を脅かすものまで懸念されています．

最新のセキュリティ脅威や技術の変化に伴う新たな脅威から，グローバルビジネスを守るためには，大きく3つのポイントが重要であると考えています．

■標的型攻撃に対応するためには技術だけではなく運用が重要

NTTグループのグローバルセキュリティ脅威に関するレポート「GTIR（Global Threat Intelligence Report）」によると，企業などをターゲットとした標的型攻撃は未知攻撃によるものも存在しているが，被害を受けた企業の原因を分析すると，既知の攻撃，場合によっては数年前の脆弱性を利用して攻撃しているものが数多く存在していることが述べられています．これらの事象に対応するためには，攻撃検知などの高度な技術だけではなく，攻撃に対する事前対応として，パッチ管理プロセス，インシデント対応手順の確立をすることや，攻撃を受けた際に対応できる人材のトレーニングなどの運用が重要となります．

■対応コストを削減するために脅威インテリジェンスの活用が重要

サイバー攻撃は組織化されてきており，企業スパイや場合によっては国家が関与しているケースも挙げられています．これらのサイバー攻撃においては，攻撃サイドの利益がはっきりしており，多くのコストをかけることも可能となります．グローバルビジネスを営む際に，セキュリティだけにコストをかけることは難しいため，効率良く対策を実施する必要があります．新たな脆弱性や，攻撃側がどこからどのような手口で攻撃してくるかなどに代表される脅威インテリジェンスを活用して事前に攻撃サイトからのアクセスを遮断したり，問題点の対応を実施したり，運用の効率化を図ることにより，コストバランスのとれた対応ができるようになります．

■IoT時代の対策にはリアル・サイバーの統合が重要

技術の進歩によりあらゆるモノがインターネットに接続される，IoT（Internet of Things）時代が間近に迫っており，一部すでに実現されています．例えば，電力の最適配電，自動車の自動運転などの分野においてIoTを利用する事例が論じられています．このような世界になると，ある場所における広域停電という事件が，実はサイバー攻撃が原因であったなどという事件が発生することが想定されていま

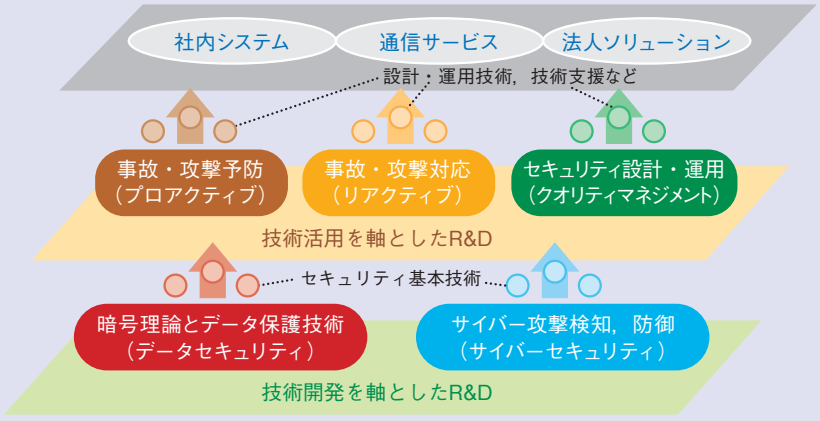


図　セキュリティ対策を実現するための研究開発

す．このような事件を扱う場合，リアルインシデント（物理的な事故）とサイバーインシデントにて発生している事象の関連性を明確にしたうえで取り組むことが必要となります．これらの事象に対応するためには，リアル・サイバーの融合したインシデントレスポンス（事故対応）が重要となります．

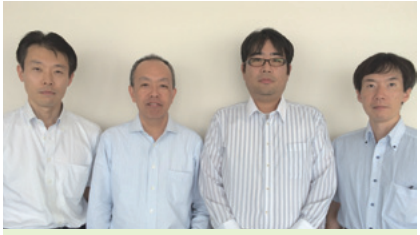
グローバルなセキュリティ脅威に対応する研究開発の取り組み

NTTセキュアプラットフォーム研究所では，最新の脅威や技術の変化に対応したセキュリティ対策を実現するための研究開発に取り組んでいます（**図**）．まず，1番目のポイントに対応するために，世界最先端の技術創出を目指した「技術開発を軸としたR&D」だけではなく，セキュリティ基本技術を活用して，社内システム，通信サービス，法人ソリューションを提供する「技術活用を軸としたR&D」にも取り組んでいます．技術活用を軸としたR&Dでは，事故の事前事後対応だけではなく，簡単に運用できるセキュリティ設計の研究開発にも取り組んでいます．

2番目のポイントに対応するために，2013年に北米の研究開発拠点として立ち上げたNTT I^3や，グローバル事業会社と脅威インテリジェンスの共有等に向けた活動を開始しています．

3番目のポイントに対応するために，NTTセキュアプラットフォーム研究所が従来から取り組んできた，自然災害に対する対応システムのノウハウと，NTT-CERTによるサイバー攻撃に対するインシデントハンドリングのノウハウを融合した，統合リスクマネジメントの研究開発に取り組んでいます．

本特集ではまず，グローバルにおけるセキュリティの脅威に関する事例を紹介したうえで，脅威インテリジェンスに関連する2つの活動および，統合リスクマネジメントに向けた取り組みを紹介します．



（左から）中嶋　良彰／高橋　克巳／
中津留　毅／三好　潤

NTTセキュアプラットフォーム研究所では，最先端のサイバー攻撃にも耐え抜くセキュリティ技術によってお客さまのネット生活を守り，情報の安全性を確保しつつ活用可能とする技術の実現によってグローバルセキュリティ対策強化に寄与します．

◆問い合わせ先
NTTセキュアプラットフォーム研究所
企画担当
TEL　0422-59-3212
FAX　0422-59-2971
E-mail　scpflab@lab.ntt.co.jp