拡がる脅威とビジネスチャンスに対応するセキュリティR&Dへの取り組み

セキュリティ面で脆弱な機器を含む多数のデバイスがネットに接続されるIoT（Internet of Things）時代では，これまで安全とされていたインフラ設備などの新たな領域への脅威が急速に拡大しつつあります．その一方，多様な情報を活用した新たなビジネスチャンスも生まれてきています．本稿では，このような環境変化を見据えた新たな脅威への対応とビジネスにおける競争力強化の両面から，NTTセキュリティR&Dの取り組み方針を紹介します．

大久保（おおくぼ）　一彦（かずひこ）
NTTセキュアプラットフォーム研究所　所長

セキュリティを取り巻く環境変化

2020年までに530億個もの多種多様なデバイスがインターネットに接続されるといわれるなど，IoT（Internet of Things）時代が間近に迫っており，一部はすでに実現されています．例えば，IoTシステムやクラウド上で交換・蓄積する多種多様な情報を活用することで，工場の生産性向上，自動車の自動運転，パーソナライズ化されたリコメンデーションサービス，電力需要効率化を図るスマートシティなどの新たなビジネス展開が始まっています．

IoTシステムやクラウド上には膨大な量の多様な情報が蓄積されており，それらを有効に活用できれば新たなビジネスチャンスが生まれると期待されています．そのためには，それらの情報の中の機微データ（パーソナルデータや企業の機密情報など）も含めて安全に利活用できるようにするためのセキュリティ技術の実現がビジネス拡大の重要なカギになっています．

一方，セキュリティ上の問題となるのは，IoTデバイスの処理能力や製造コストなどの点から，PCなどで使われている従来のセキュリティ対策が取り込まれないまま，セキュリティ的に脆弱なIoTデバイスが多数インターネットに接続されることです．このようなIoTデバイスでは，容易に乗っ取られてボット化するおそれがあり，ひいてはDDoS（Distributed Denial of Service）攻撃などのサイバー攻撃が大規模化・巧妙化する要因となることが懸念されています．例えば，ある場所における広域停電という事件が，実はボット化したIoTデバイスからのサイバー攻撃だったというようなことさえ想定されます．実際，監視カメラやネットワークTVの乗っ取りなどの実例が報告されています．2016年10月，米国を中心に多数のWebサイトが接続できなくなる事態が発生しましたが，これもIoT機器を乗っ取るマルウェア「Mirai」によるDDoS攻撃ではないかといわれています(1)．

このようなサイバー攻撃を防御するには，IoTデバイスがボット化などの異常動作をした場合に，正常なIoTデバイスの接続は維持しつつ，異常なデバイスのみをネットワークから切断する等の対策が重要となります．

NTTセキュアプラットフォーム研究所の研究開発

NTTグループが提供するクラウドサービスやコミュニケーションサービスの安心・安全に貢献するための研究開発として，NTTセキュアプラットフォーム研究所（SC研）では，「世界最先端のセキュリティ技術の創出」および「セキュリティ技術を活用した総合的なセキュリティ強化」の方針の下，昨今のセキュリティを取り巻く環境変化に対応して，大きく3つのセキュリティR&Dの方向性を定めています（**図1**）．この方向性を踏まえ，世界最先端の暗号技術やサイバー攻撃対策技術をコアコンピタンスとして，理論からプロダクト・ノウハウの提供，運用支援まで幅広い研究開発を行っています（**図2**）．

3つのセキュリティR&Dの方向性のうち，「激化・巧妙化するサイバー攻撃への対抗」と「IoTの進展等に伴う新たな脅威への対応」は，サイバー攻撃の脅威に対抗するためのいわば「守りの技術」で，NTTグループのネットワーク基盤を含む重要インフラなどの防衛力向上への貢献をめざしています．一方，「データ交換・蓄積・活用

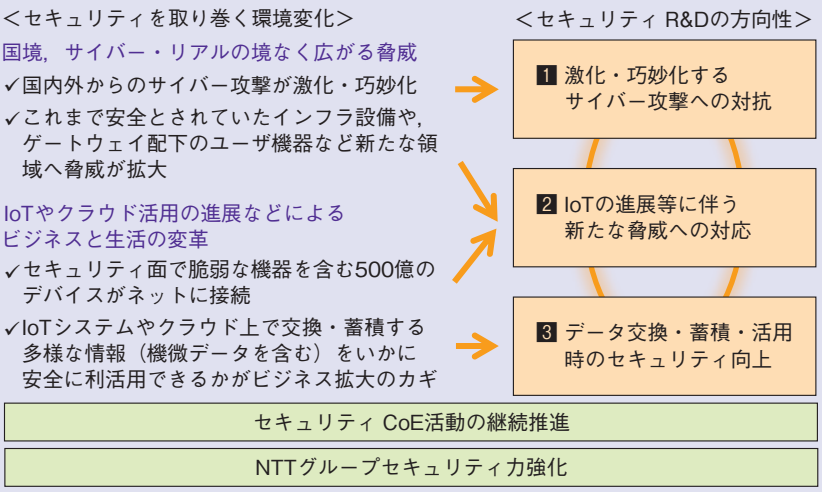

図 1　環境変化とセキュリティ R&Dの方向性

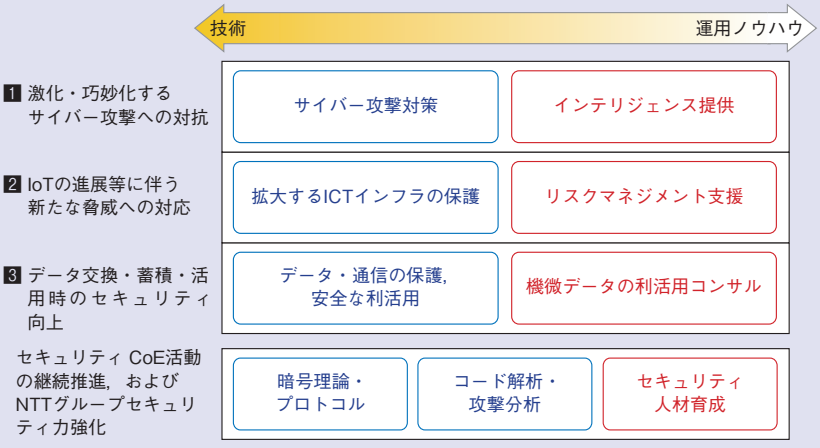

図 2　セキュリティ R&Dの取り組み

時のセキュリティ向上」は，IoTを活用したクラウド・ネットワークサービス，パーソナルデータ活用などの法人向けビジネスにおける事業会社商材の付加価値を高めるためのいわば「攻めの技術」となることをめざした研究開発を進めています．

■激化・巧妙化するサイバー攻撃への対抗

SC研では国内外からのサイバー攻撃の激化・巧妙化に対抗するため，世界最先端のサイバー攻撃検知，収集，解析技術を核とし，事業会社との連携を密にしながら，競争力のある独自技術とセキュリティインテリジェンスの創出に向けた研究開発の取り組みを行っています．

マルウェア感染を引き起こす悪性サイトURLや攻撃に使用されるIPアドレスを収集してブラックリスト化する技術の研究開発では，アクセス元のWebブラウザ環境に応じて挙動を変化させる悪性サイトに対してさまざまなWebブラウザ環境をエミュレートする情報収集技術やWebアプリケーションの脆弱性への攻撃に対応した情報収集技術に取り組んでおり，それらの成果を組み込んだハニーポットを運用しています．さらに，ハニーポットで捕獲したマルウェアの挙動をイン

ターネットに接続して解析するマルウェア動的解析技術のほか，ユーザトラフィックからの悪性なHTTP通信を検知する技術，ドメイン名やIPアドレスの悪性度を評価する技術など，先進的なマルウェア対策技術に基づくセキュリティインテリジェンスのカバレッジ拡大と精度向上に向けた取り組みを行っています．

また，セキュリティログ分析技術の研究開発では，年々巧妙化し事前の防御が困難となってきているサイバー攻撃に対抗するため，通信ログの相関分析や高精度な分析ルール自動抽出による未知マルウェア検知技術，ゼロデイ攻撃を高精度に検知可能なパラメタプロファイリング技術などに取り組んでいます．

これらの技術は，NTTグループ総体でのセキュリティオペレーション強化を目的としたSIEM（Security Information and Event Management）基盤の構築，ならびにNTTグループにおける法人向けセキュリティサービスMSS（Managed Security Service）の展開を支えています．

これらの研究開発に加え，NTTグループの代表CSIRT（Computer Security Incident Response Team）であるNTT-CERTを運営しており，持株および事業会社内で発生したインシデントに対する各種インシデントハンドリングやインシデントの原因究明と影響分析を目的としたフォレンジック調査，サイバー攻撃へのグループ対応力強化に向けたグループ間連携調整なども行っています[(2),(3)]．

■IoTの進展等に伴う新たな脅威への対応

多種・多数のデバイスがネットワークに接続する環境において想定される，デバイスの脆弱性侵害によるボット化などのインシデントに備え，守るべき資産のライフサイクル全般でのリスク予見・管理を徹底すべく，セキュアなシステムのための設計・構築・運用にかかわるセキュリティ技術の確立をミッションとした研究開発を行っています．

具体的には，システムやネットワーク上の機器をセキュリティの観点で統合管理・制御することでサイバー攻撃防御力を向上させるため，①システム導入後のインシデントの抑制に向けた，システムの企画・設計段階でのリスクマネジメントやセキュリティ・バイ・デザインの推進，②暗号技術やセキュリティチップを活用し，接続機器のライフサイクル全体における真正性・完全性確認技術，③新旧設備が混在する環境においてもトラフィックや機器の状態・挙動を監視し，被害の未然防止・極小化に資するネットワーク全体の健全性確認技術，④各種IoTデバイスからのセンサ情報を活用した不正行動検知技術，⑤ネットワークに対する多種の攻撃を自動検知し，セキュリティアプライアンスなどを適切に制御することでセキュリティレベルの維持・早期回復を実現するセキュリティオーケストレーション技術，に取り組んでいます．

また，IoT時代のさまざまなネットワークに接続されるデバイスは，PCやスマートフォン同様にさまざまなセキュリティ脅威にさらされることから，その対策を講じる必要があります．中でも，IoT時代の象徴的な技術として自動車の自動運転技術がスポットを浴びていますが，その実現には自動車の高度制御系システムでのサイバーセキュリティ対策技術が不可欠です．実際，ネットワーク経由で不正に操作されるなどの自動車に対するサイバー攻撃が問題となってきており，SC研でも自動車がネットワークに接続されるときの脅威と対策の検討を進めています．

これらの取り組みの詳細については，本特集記事『安全な重要インフラ

を実現するアーキテクチャ』『クルマのサイバー攻撃対策技術』にて紹介します.

■データ交換・蓄積・活用時のセキュリティ向上

安心・安全な情報流通基盤の実現に向けて，世界最先端の暗号技術を核として，その基礎となる暗号理論研究から，データを安全に保護するための暗号システム化技術や暗号の安全な利用・運用技術に取り組んでいます.

2015年9月の改正個人情報保護法の成立後，パーソナルデータや企業の機密データの利活用への関心が急速に高まっていますが，一方で案件に応じた法的要件の整理や，適法かつ有用なデータの加工処理方法の導出が課題となっており，期待されているほどには機微データの利活用が進んでいません．SC研では，運用的にはセキュリティ・プライバシの法的リスクアセスメントやデータ・用途に応じた機微データ利活用についてのコンサルティング，技術的には匿名化技術・秘密計算などの安全なデータ利活用技術を提供しており，事業会社のセキュリティ商材の付加価値向上に貢献しています.

また，企業からの度重なる情報漏洩や国家権力の介入によりサービス事業者や認証局などへの信頼が揺らいでおり，サーバへのセキュリティや管理者のモラルへの依存度が低いデータ保護・通信保護方式の必要性が顕在化してきています．このような課題に対して，サーバからの情報漏洩があった場合でも通信の秘密を守ることができる安全なビジネスチャットの開発，安全性を保持しつつサーバでのパスワード管理が不要な認証方式の開発[4]などにも取り組んでいます.

これらの取り組みの詳細については，本特集記事『サーバからの漏洩・盗聴を防ぐ暗号ビジネスチャット』『個人情報保護法改正のポイントとパーソナルデータ利活用に向けた匿名加工』にて紹介します.

今後の展開

SC研では，引き続き，世界最先端の暗号技術やサイバー攻撃対策技術をコアコンピタンスとして，理論からプロダクト・ノウハウの提供，運用支援までをカバーする研究開発を推進し，NTTグループが提供するクラウドサービスやコミュニケーションサービスの安心・安全に貢献していきます.

■参考文献

⑴ http://wired.jp/2016/10/24/internet-down-dyn-october-2016/
⑵ 針生・横山・畑田・矢田・八木・秋山・幾世・高田・千葉・田中：“NTTグループのセキュリティビジネスを支えるマルウェア対策用セキュリティインテリジェンス，” NTT技術ジャーナル，Vol.27，No.10，pp.18-22，2015.
⑶ 種茂・林・谷川・安部：“安心・安全ブランド向上に資するセキュリティオペレーション強化の取り組み，” NTT技術ジャーナル，Vol.24，No.8，pp.22-25，2012.
⑷ M. Matsui, H. Ohtsuka, T. Kobayashi, H. Okuyama, A. Nagai, and G. Yamamoto：“Milagro Multi-Factor Authentication，” NTT Technical Review, Vol. 14, No.12, 2016.

大久保　一彦

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研究開発を通じて，新たな脅威への対応とビジネスにおける競争力強化の両面で貢献していきます.

◆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