サイバー攻撃　暗号　プライバシ

安心・安全なデジタル社会に向けたセキュリティR&D

NTTセキュアプラットフォーム研究所では，デジタル社会の実現に向かって大きな環境変化や市場の変遷に伴って生じてくる新たなサイバーセキュリティの脅威への対抗やデータの利活用を取り巻く課題の解決に向け，セキュリティ技術の研究開発（R&D）に取り組んでいます．本稿では，デジタル社会に向けたセキュリティの課題と，それに対応する「守り」「攻め」のセキュリティについて紹介します．

おおくぼ　かずひこ
大久保　一彦

NTTセキュアプラットフォーム研究所　所長

デジタル社会への変貌とセキュリティの課題

ICTをはじめとする近年の革新的な技術の登場によって，今社会は大きな変革を遂げようとしています．いわゆる「デジタルトランスフォーメーション」と呼ばれるような，デジタル技術とデータの活用が進むことによって，サイバー空間とフィジカル空間が高度に融合し，生活環境の変化や産業，社会構造の変革をもたらすデジタル社会の実現へと急速に向かっています．便利で豊かな社会の実現が期待される一方で，これまで起こり得なかったようなサイバー攻撃による被害の拡大や社会的な損失のリスクの肥大化が懸念されています．

サイバー空間においては昨今，自律的な動作能力を高めたマルウェアが出現するなど，サイバー攻撃手法の進化・巧妙化が進みつつあります．脆弱性を悪用することによって感染を拡大するWannaCryによる被害は世界各地におよび，甚大な損害を与えるなど，セキュリティ脅威はますますエスカレートしています．このため，ITの領域では永遠のイタチごっこのように，サイバー攻撃対策技術のさらなる高度化が求められています．サイバー空間とフィジカル空間を融合させるための重要なファクターであるIoT（Internet of Things）を実現した機器は，セキュリティの観点でそもそも脆弱な状態のままインターネットにつながれるものも多く存在し，それらを踏み台とした大規模サイバー攻撃〔DDoS（Distributed Denial of Service）攻撃〕が発生しています．IoT機器がIT機器ほどの計算機リソース（CPUパワー，メモリ・ディスク領域，電源容量等）を持ち得ないことから，従来のIT機器に搭載されていたセキュリティ機能をIoT機器に適用できず，IoT機器向けの新たなセキュリティ技術の確立が急務となっています．また，急速なデジタル化により，これまで直接的にはインターネットにつながっていない工場・プラント等における制御システムといったOT（Operational Technology）の領域や，生活や社会活動に不可欠なサービスを提供している重要インフラに対するサイバー攻撃などのセキュリティ脅威の増大，およびインシデント未然防止やインシデント発生時の対応における稼動不足に対する懸念が深刻なものとなっています．このため，OTや重要インフラのセキュリティ確保にかかわる特殊な技術開発に加え，サイバーとフィジカルの両面からの包括的なリスクマネジメントの強化，およびAI（人工知能）等の導入による各種運用の効率化も喫緊の課題となっています．

デジタル社会の実現のためにはサイバー攻撃への対抗だけでなく，データの活用を活性化させることがポイントになります．デジタル技術により，さまざまなきめ細やかなデータを取得し活用することによって，今まで困難であった精度の高い予測やターゲットを絞ったマーケティングの実現など，データを活用した新たなビジネスチャンスの到来が期待されています．2017年5月の改正個人情報保護法施行，2018年5月のEU一般データ保護規則（GDPR）施行など，デジタルトランスフォーメーションの進展をにらんだ安心・安全なデータ利活用ビジネスに向けた法整備も進んでいます．一方で，個人のプライバシ情報や企業における機密情報等，センシティブなデータを安心・安全に流通させるための技術や環境が不足・未整備であるうえ，心理的および社会的な受容性もいまだに低いことが，データ利活用の障壁となっています．このため，高度な機能を有

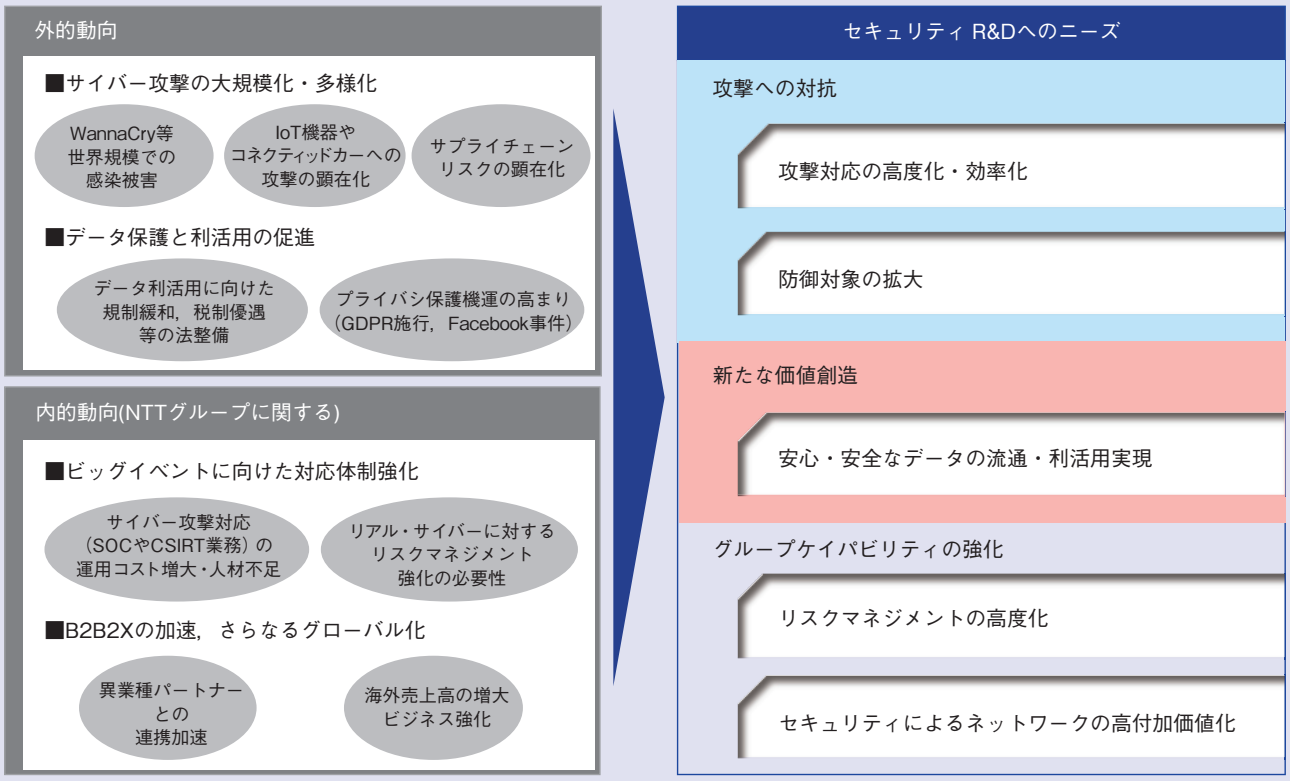


図1　環境変化とセキュリティ R&Dへのニーズ

する暗号等をはじめとするデータセキュリティ技術の活用によるリスク回避と経済活性化に向けた新たな価値創造の取り組みが期待されています．

NTTグループを取り巻く状況においては，通信等のインフラ事業やICTビジネスを支える企業として大きな期待が寄せられている中，ビッグイベント開催の成功に向けた取り組みを強化していくことが求められています．特にセキュリティの面では，巧妙化・高度化するサイバー攻撃に対応する体制〔SOC（Security Operation Center）やCSIRT（Computer Security Incident Response Team）業務〕の運用コストの増加，体制を支えるセキュリティ人材の不足への対応や，ビッグイベントに呼応したリスクマネジメント強化が求められています．

NTTセキュアプラットフォーム研究所における取り組み

前述のように，デジタル社会の実現に向かって大きな環境変化や市場の変遷が起きている中，セキュリティへの課題の解決に向けた研究開発（R&D）に対するニーズとして大きく3つが求められています（**図1**）．

① 巧妙化・大規模化するサイバー攻撃への対抗として，攻撃への対

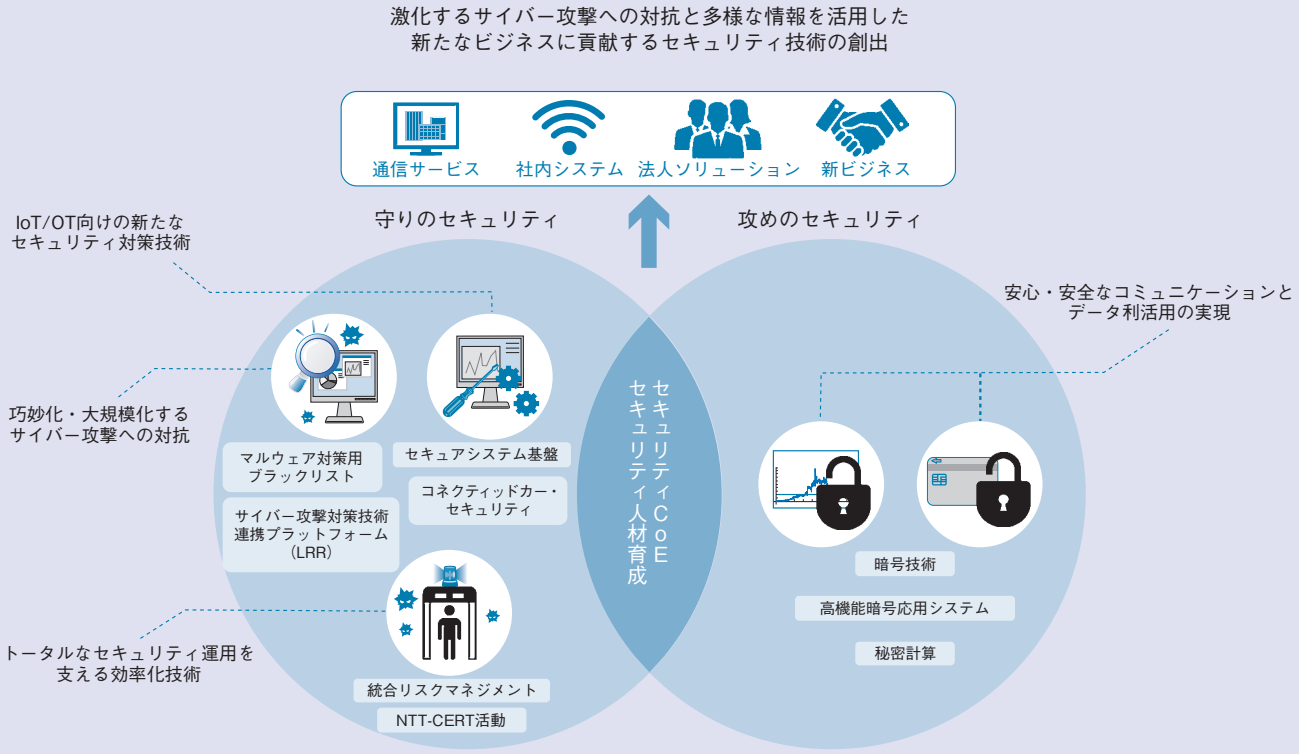


図2　セキュリティR&Dへの取り組み

応をさらに高度化し，効率化・自動化を推進していくこと，またIoTやOTなど新たにセキュリティが求められる領域へ防御対象を拡大していくこと

② 新たな価値創造を実現するために，安心・安全なデータの流通・利活用を実現していくこと

③ NTTグループのケイパビリティを強化するために，リスクマネジメントの高度化やセキュリティによるネットワークの高付加価値化を図ること

NTTセキュアプラットフォーム研究所では，これらのニーズを踏まえて安心・安全なデジタル社会の実現に向けた研究開発に取り組んでいます．具体的には，激化するサイバー攻撃への対抗を中心とした「守りのセキュリティ」，多様な情報を活用した新たなビジネス創出に貢献する「攻めのセキュリティ」，およびこれらを支える技術の源泉ともいうべき基礎研究活動を中心とした「セキュリティCoE (Center of Excellence)」「セキュリティ人材育成」を軸としてさまざまなセキュリティ技術の研究開発を推進しています（**図2**）．

■守りのセキュリティ

「守りのセキュリティ」では，昨今のサイバー環境を取り巻く急激な変化や市場からのニーズをとらえ，従来からの「IT」領域と，これまでと異なり直接インターネットにつながってくることによりサイバー攻撃からの防御が必要になってきた「IoT/OT」「重

要インフラ」のそれぞれの領域について，具現化する脅威やセキュリティの問題を解消すべく，世の中にはないセキュリティ技術の研究開発に取り組んでいます．

⑴　IT

ITの領域では，巧妙化・大規模化するサイバー攻撃に対抗するため，従来の監視対象である法人およびホームネットワークやISP（Internet Service Provider）ネットワークにおいても攻撃に追随すべく，「悪性Webサイト検知」「マルウェア感染検知」「ボットプロファイリング」「ドメインレピュテーション」といった対策技術の高度化に引き続き取り組んでいます．さらにミクロやマクロの観点から，エンドポイントならびにバックボーンネットワークへ監視対象を拡大する必要があることから，エンドポイントにおいては，「メモリフォレンジック」「テイント解析」等の技術を駆使したマルウェア解析に取り組んでおり，これにより高精度なIOC（Indicator Of Compromise）を生成し，MDR（Managed Detection and Response）製品に適用するなど，有効活用に向けた検討を進めています．また，バックボーンネットワークにおいては，大量のフロー情報分析によりボットネットの全体構造を浮き彫りにするとともに，高性能なDDoS検知も可能にし，適材適所の対策につなげています．

⑵　IoT/OT

IoT/OTの領域では，「認証・認可」「構成管理」「検知」「対処」といった一連のセキュリティ技術の確立が必要となってきます．「認証・認可」については，サーバ側でパスワードの管理が不要な次世代認証技術に取り組んでいます．これは，クライアントの初期登録時にデバイス側に秘密情報を払い出し，それとデバイス固有のIDを使って暗号演算を施すことで認証を実現する方式です．この技術によって，IoT機器のパスワード運用をいちいちしなくてよく，また認証に必要な証明書の発行・運用等のコストもかからないで済むといったメリットが生まれます．「構成管理」「検知」「対処」の技術開発においては，ゲートウェイ配下に多種多様なIoT機器がつながる状況下で，一般に利用されているARP（Address Resolution Protocol）フレームの出力特性解析やノイズ除去により，運用条件の厳しいLAN環境においても精度良く機器を特定・推定して構成把握を行うとともに，グラフ理論等を活用して平常時の通信相手（ホワイトリスト）から逸脱したトラフィックをアノマリな状態として検知することで適宜，サイバー攻撃等による異常通信に対する制御（アラートおよび遮断等）を可能にする技術に取り組んでいます．

⑶　重要インフラ

重要インフラの領域では，その「大規模性，複合連動システム化」といった特徴と「汎用化，オープン化，新技術の適用」といった環境変化に伴い増大するリスクを考えることが重要です．前者については，数千台のサーバ機器，数万から数十万台の制御機器といったインフラ設備が珍しくなく，1カ所でもサイバー攻撃が成功すれば影響は広範囲に及ぶおそれがあるため，構成要素がそもそも大丈夫なのかといった観点から，不正な機器の混入や改変を常時確認し，異常動作を阻止する「真贋判定技術」が必要になります．後者については，インターネット技術，Linuxなどのオープンソースソフトウェアの採用が進むことで，脆弱性等の情報が得られやすくなっている点から，サイバー攻撃の成立は大前提となっています．前述の真贋判定技術がビルトインできないようなIoT等の機器やネットワークにおいてもシステムの異常を監視可能なボルトオン型の「動作監視・解析技術」が必要になります．これらの技術については，当該技術の一部を，内閣府が進める戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）にて，2015年度から2019年度にわたり研究開発に取り組んでいます．

■攻めのセキュリティ

「攻めのセキュリティ」では，安心・安全なデータ利活用の実現に貢献する

技術の研究開発に取り組んでいます．改正個人情報保護法の施行により注目を集めている高度な匿名加工技法の代表的なものとしてk-匿名化という手法があります．この手法では情報の粒度を荒くする操作（丸め）により，安全性の指標であるk-匿名性（同じ情報を持つ人が最低k人未満に絞り込まれない）に基づいてデータ加工が施されますが，データの安全性とともに有用性を両立する点に難しさがあることが加工後のデータ活用の観点から懸念されています．そこで情報のランダム化による書き換えを行うことで，k-匿名化と等価な安全性を担保し，かつデータの有用性の確保も可能とする「Pk-匿名化」の技術開発に取り組んでいます．また，医療の発展に欠かせないゲノムデータのような機微なデータについては，匿名化しても外部に出したくないというニーズもあり，このようなケースについては，暗号化したままデータ処理を施せる「秘密計算」が有用です．秘密計算と呼ばれるものには多くの方式がありますが，NTTセキュアプラットフォーム研究所の技術はISO（International Organization for Standardization）標準である「秘密分散」[1]をベースとした秘密計算であり，安全性定義，汎用的計算，常識的性能，国際標準等の観点からもっとも実用的なものであり，今後の技術普及に向けたさらなる研究開発・展開活動に取り組んでいます．

■セキュリティCoE，セキュリティ人材育成

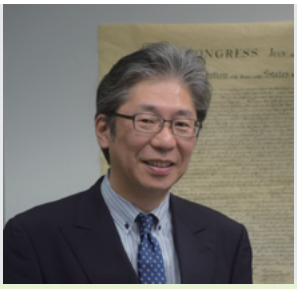
「セキュリティCoE」では，NTTグループ内外を問わず，学術界やハイレベルな専門化コミュニティなど幅広い分野において研究所が有する高度な専門スキルを持つ人材が牽引・貢献を行っています．サイバーセキュリティの分野では，著名なコンテストの運営にかかわるだけでなく，専門家でなくても理解しやすい啓発書・入門書の執筆[2]や大学講義など，「セキュリティ人材育成」の観点からも活動に取り組んでいます．データセキュリティの分野では，暗号理論を代表とする世界最先端の研究を行っており，10年，20年先を見据えた次世代の競争力の源泉となる差異化技術の創出に取り組んでいます．具体的な研究事例としては，次世代の秘密計算といえる完全準同型暗号や，量子コンピュータが実現されても安全性が保たれる耐量子暗号といった技術の研究を進めています．

今後の展開

「守り」のセキュリティでは，サイバー攻撃が起きている現場での分析と，事業に直結できる効果的な対策技術の創出が求められています．「攻め」のセキュリティでは，データを安心・安全に活用できる技術や環境の普及に加え，法制度面からも社会受容性を高める取り組みが重要です．NTTセキュアプラットフォーム研究所は，NTTグループ各社と一丸となってセキュリティ向上に取り組み，外部ステークホルダーと連携しつつ，安心・安全なデジタル社会の実現に努めています．

■参考文献

(1) Focus on the News：“秘密分散技術の初の国際標準にNTTの秘密分散技術が採択，” NTT技術ジャーナル，Vol.30，No.3，pp.58-59，2018.
(2) 中島：“サイバー攻撃 ネットの世界の裏側で起きていること，” 講談社ブルーバックス，2018.



大久保　一彦

セキュリティへの対応は企業における経営の最重要課題の1つとしてとらえられています．私たちは，最高峰のセキュリティR&D成果を持続的に創出し，NTTグループひいては，国，世界レベルでの技術貢献に尽力していきます．

◆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
E-mail　scpflab@hco.ntt.co.jp