新しいValueの創出に資するセキュリティR&D

NTTセキュアプラットフォーム研究所では，来たる「スマートな世界」に必要となる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，スマートな世界に求められる「安全なデータ流通の世界」を示すとともに，その世界を支えるNTTセキュアプラットフォーム研究所の取り組みを「スマートな世界を守るセキュリティ」および「スマートな世界を創るセキュリティ」の2つの側面で紹介します．

ひらた　しんいち
平田　真一
NTTセキュアプラットフォーム研究所　所長

スマートな世界

デジタルデータの実世界での活用は,「デジタルトランスフォーメーション」とのキーワードに代表されるように社会活動上のさまざまな場面で人々が直面するようになり，人々の生活，暮らし，働き方が急速に変化しつつあります．

現在，社会活動のさまざまな場面においてフィジカル空間から多量のデジタルデータが取得され，活用されています．この多量のデータをサイバー空間で高度に処理し，フィジカル空間に還元・活用すること，さらにその営みを通じて，すべての人が安全に自分らしくに暮らせること，社会が円滑に活動できるようにすること，を私たちはめざしています．私たちは，こうした世界観を「スマートな世界」と呼んでいます．

「スマートな世界」では，安全で健やかに過ごせる住環境や，自分専用のカスタマイズが可能な生活環境を満たす「個人の最適化」が実現すること，および予測に基づき全体最適が図られる産業システムや，働き手の都合に柔軟に対応可能な労働環境など「社会の最適化」が実現すること，を想定しています．私たちは，この「スマートな世界」に欠かせない，大量のデジタルデータの安心・安全な流通に必要なセキュリティ技術の創出に取り組んでいます．

最近のセキュリティ動向

「スマートな世界」の実現に向けて社会が大きく変革しようとしている昨今ですが,「スマートな世界」が描く便利で豊かな世界を前に，現状のサイバー空間ではどのような脅威がもたらされているのでしょうか．

IT分野では，メール等を使い企業から経営情報を詐取し，脅迫や詐欺を行う「ビジネスメール詐欺」や，情報機器の製品ライフサイクル（設計，製造，使用，破棄）の上で脆弱な関係者（取引先, 受委託先）を標的とする「サプライチェーン攻撃」, そしてソーシャルネットワークを悪用したフェイクニュースの活発化が特筆されます．

ビジネスメール詐欺は，企業の情報システムに侵入し，企業の取引情報や経営情報を詐取した攻撃者が，侵入先企業になりすまして侵入先企業の取引先など関係者に対し偽の情報交換を行うなどして，金銭や企業の機密情報の詐取を試みる攻撃です．

米国FBI インターネット犯罪苦情センタ（IC3）は2019年4月，2018年の米国国内におけるビジネスメール詐欺の被害件数が35万1937件（前年比+17%），被害金額27億ドル（同+46%）にのぼることを示しました[1]．

また，サプライチェーン攻撃は，製品の設計・製造課程や流通過程に侵入し，第三者への攻撃を可能とするハードウェア, ファームウェア, ソフトウェアなどを市中に流通させることで，端末やシステムからの機密情報の詐取，機能停止を試みる攻撃です．市販のPCや，スマートフォンに対し，攻撃者がバックドアを含むファームウェアやソフトウェアの配布に成功した事例が明らかになっています．

OT（制御ネットワーク）分野，IoT（Internet of Things）分野では，重要インフラを対象とした攻撃事例の増加が挙げられます．電気，ガス，水道，通信，放送，交通など人々の生活を支える公共財の内部で稼動する制御ネットワークを標的とした攻撃は，これらの設備そのものを攻撃対象とします．これらの設備の停止や破壊につながる行為は，例えば発電所の発送電の停止，ひいては大規模停電（ブラックアウト）を引き起こすなど，国民生活を

大きく混乱させることが想定されます．

以上のセキュリティ脅威動向に共通していえることは，これまでのサイバー攻撃が企業や団体が対象とされてきたことに対して，近年は，一般市民の安全や，国家そのものの価値の毀損させる，より大規模な標的を対象とした攻撃に進化しつつあることが挙げられます．

スマートな世界を守るセキュリティと，スマートな世界を創るセキュリティ

それでは，来たる「スマートな世界」に向けて，私たちはどのようなセキュリティ技術を提供していかなければならないのでしょうか．

私たちは「スマートな世界を守る」と「スマートな世界を創る」の2つのキーワードに着目しています．「スマートな世界を守るセキュリティ」とは，サイバー攻撃からIT，IoT，ISPなどさまざまなネットワークやITシステム，利用者を防御する技術です．また，「スマートな世界を創るセキュリティ」とは，暗号技術を応用して安全なデータ流通を促進し，企業活動の活性化や安全な日々の暮らしを実現するための積極的なデータ利活用を支え，先に挙げた「スマートな世界」を創り上げる技術です．この2つのキーワードをセキュリティ研究開発の両輪と位置付けて活動しています．

スマートな世界を守るセキュリティ

「最近のセキュリティ動向」の項で述べたように，現在，日々新たなサイバー攻撃手法が登場し，その内容は「攻撃の巧妙化」，および「攻撃の数的拡大」がなお一層高度化すると予想されています．

サイバー攻撃の巧妙化，数的拡大は企業や組織におけるセキュリティリスク増大をもたらします．セキュリティリスクを構成する要素は，「脅威」「脆弱性」「企業や組織が守るべき資産」に大別されます．しかし，個々の企業や組織が負担可能なセキュリティ対策コストはセキュリティを重視する先進的な大企業であってもITシステム予算のおおむね15%程度，中小企業においては5%以下，と限界があり，今後のサイバー攻撃の拡大に対抗するためには，企業や組織のサイバー攻撃に対する防御，対策能力の抜本的な向上が必要です（**図1**）．

私たちは，企業や組織のサイバー攻撃に対する防御，対策能力の向上を図るため，「サイバー攻撃の巧妙化」に対応する「エンドポイント端末のマルウェア検知の高度化技術」「悪性ドメイン判定の高度化技術」「ユーザの心理的な弱みに付け込む攻撃への対抗技術」また「サイバー攻撃の数的拡大」

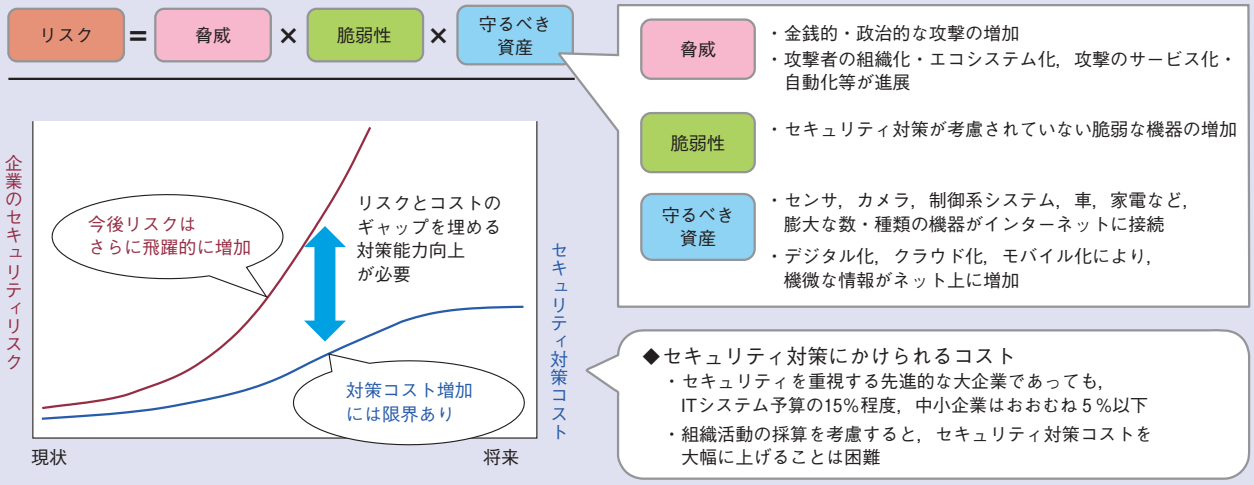

図1　企業のセキュリティリスクと対策コスト

に対応する「運用効率化技術」「分析・判定の省力化技術」に代表される研究開発に取り組んでいます．

一方で，OT/IoT分野におけるサイバー攻撃に対抗するためには，IoT機器や制御機器など多種多様な機器が接続されることを想定したうえで，設計，製造，流通，構築，運用，破棄のサプライチェーンや製品ライフサイクルを通じた安全性の担保や，産業分野間で連携した多層的な対策が行われることが求められています．

例えば，IoT化が進む工場，ビル，農業，監視・保守システム等を適用先と想定し，製造，流通段階，運用段階におけるIoT機器や制御機器の「ソフトウェア改ざん」を検知する「IoT機器向け真贋判定技術」，運用段階における「運用中の不正動作」を検知する「サイバー・フィジカル異常検知技術」などの研究開発に取り組んでいます．また，自動車向けセンサネットワークや自動走行車両など，モビリティ分野の高度化に合わせ，車両による攻撃や車両に対する攻撃を迅速かつ高精度に検知・解析する「車載ネットワーク上でのリアルタイム異常検知技術」「クラウド上での攻撃検知技術」や，虚偽センサデータの混入による交通情報の混乱を防ぐ「虚偽センサデータ検知技術」などの研究開発に取り組んでいます．

OT/IoTシステムにおけるサイバー攻撃への対策は，これらの技術に加えて，ITセキュリティ，セーフティ（機能安全），物理セキュリティの相互依存性を踏まえた統合的な対策技術の創出やルールの策定が求められています．

スマートな世界を創るセキュリティ

「スマートな世界」の実現のためには「安心・安全なデータ流通・利活用」を支える技術，すなわちデータの囲込みやプライバシ侵害，不正利用により生まれる問題を解決し，データの生成・流通・分析・破棄に至るまですべての価値創造プロセスをセキュアに行い，分野横断的にデータを利活用できる柔軟で安全な共有・分析の仕組みが必要不可欠です．

これまでデータは単一の企業体の内部のみで保有，利用されてきましたが，「スマートな世界」の実現には，目的に合わせ安全に必要なデータを組織間で共有するため，組織間でプライバシや企業秘密を保護したままデータを組み合わせて高度な分析（統合分析）を行う仕組みや，分野横断的に統合分析

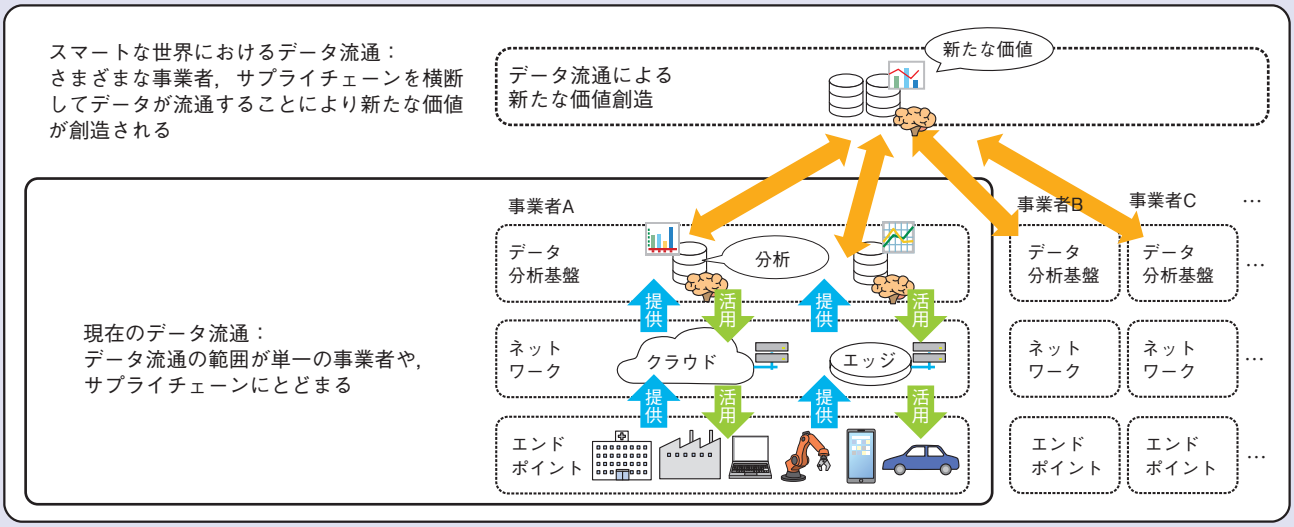

図2　スマートな世界におけるデータ流通

した結果を基に多様な課題を解決・社会へ還元する仕組みが求められます．これらの仕組みにより，業界・分野を超えたセキュアなデータ利活用が可能となり，これまでにない新たな価値の創出が可能となります（**図2**）．

私たちは，こうした価値創造を実現する核となる技術としてデータを暗号化したまま計算する「秘密計算技術」，パーソナルデータの安全な活用を可能とする「匿名化技術」に取り組んでいます．

一般的に，取得したデータを分析・活用する際には，サーバにて暗号化して保存されているデータを復号した実データを処理しなければならず，企業秘密や個人のプライバシにかかわるデータの利活用が進んでいない，との課題がありました．「秘密計算技術」では，個人や企業にかかわる情報の取り扱いに配慮しつつ，目的に応じて必要なデータを組織間で相互利用し，世の中の課題解決を進めやすくする世界を創ることを支えます．私たちは，「秘密計算技術」に関連して，暗号化したままディープラーニングの標準的な学習処理ができる世界初の技術を2019年9月に発表しました．

また，「匿名化技術」では，NTTセキュアプラットフォーム研究所の独自技術を含む，多様な匿名加工情報の作成を可能とします．2017年の改正個人情報保護法の施行により，個人情報を匿名加工情報として加工すれば，本人の同意なく第三者に提供することが可能になりました．私たちの「匿名化技術」は，こうした法制度に対応した技術で，NTTテクノクロスより「匿名加工情報作成ソフトウェア」として製品化されました．

CoE活動

私たちは，NTTグループがスマートな世界を支えるために必要な競争力の源泉となる技術創出として，CoE（Center of Excellence）活動に積極的に取り組んでいます．

CoE活動を通じて，私たちが擁する高度な人材が，学術界や専門家コミュニティを牽引しています．サイバーセキュリティの分野では，専門家コミュニティや世界的なセキュリティコンテストの運営，大学と連携した人材育成に力を入れて取り組んでいます．また，データセキュリティの分野では，10年，20年先を見据え，暗号理論を代表とする世界最先端の研究として，次世代の秘密計算といえる「完全準同型暗号」や，量子コンピューティングが実現されても安全性が保たれる「耐量子暗号」，さらには量子コンピューティングに関する研究も進めています．

私たちは，こうして蓄えられた知見をNTTグループ各社で活用するためのコンサルティング活動にも力を入れており，プライバシ保護や法制度を遵守した安心・安全なシステムやアプリケーションの開発を支援しています．

今後の展開

このように，セキュリティに関するさまざまな研究開発活動に取り組むNTTセキュアプラットフォーム研究所は，NTTグループのセキュリティ技術の高度化，差異化の源泉となるべく活動し，安心・安全な「スマートな世界」の実現に努めていきます．

■参考文献

(1) https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2018-internet-crime-report

平田 真一

私たちは，「スマートな世界」の実現に向けて市民，企業，国家のあらゆるレベルでのセキュリティ対応能力を向上させるために，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