安心・安全を実現するテクノロジの創出に向けたセキュリティR&Dの取り組み

さまざまな状勢により世の中が大きく変革していく中，NTTが取り組んでいるセキュリティR&Dの将来像を語るには，目の前で起きている問題だけでなく，来る社会のあり方とセキュリティについて考えることが重要です．本稿では，その先の未来を見据えたセキュリティR&Dの取り組みについて紹介します．

平田（ひらた）　真一（しんいち）

NTTセキュアプラットフォーム研究所　所長

はじめに

新型コロナウイルス感染症によって私たちの社会，生活にさまざまな影響が及ぼされました．オリンピック・パラリンピックをはじめとするさまざまなイベントが開催の延期を余儀なくされ，ソーシャルディスタンスの確保を前提とした社会活動，生活様式へ移行せざるを得なくなったことから，オンライン化が急速に進んだことによる働き方の変革や，社会の分断化・非接触化がさまざまな面で生じています．

コロナウイルスによる影響の全世界的な拡大や事態の長期化が予測されていることから，世の中の変革（アフターコロナの新しい生活様式，社会秩序の再構築）が加速され，それに伴ってデジタル化・オンライン化に向けたさまざまな取り組みが急速に進んでいます．また，従来の社会活動を前提としていたサプライチェーンが機能不全となり，個人だけでなく社会の枠組みのレベルでもさまざまな場面で大きな変化が起こっています．

その一方でセキュリティやプライバシに関する懸念や被害も広がっており，在宅勤務などの普及に伴って急増するテレワークをねらったサイバー攻撃や，人の不安に乗じた攻撃による被害はますます深刻になっています．また，感染拡大防止に向けた感染者やその疑いのある人を割り出すための監視や行動追跡などはプライバシへの十分な配慮も求められます．

サプライチェーンにおいても，急速なデジタル化・オンライン化をねらった広域的な攻撃も激化しており，安全なサプライチェーンの再構築が求められています．

NTTでは，安心・安全な社会の実現に貢献するためのセキュリティに関する研究開発を進めています．

世の中が大きく変革していく中，目の前で起きている問題だけでなく，その先の未来を見据えたセキュリティR&Dに取り組んでいくために，来る社会のあり方とセキュリティについて考えていくことが重要です．

将来にわたって安心・安全な社会にしていくために，社会環境の変化やICTを取り巻く技術の発展による未来像（10年後のSmart World）について考えます．

10年後のSmart Worldとは

AI（人工知能），IoT（Internet of Things），ロボットやビッグデータといった革新技術が浸透した社会は，産業革命による工業化社会への発展，コンピュータ技術の発達による情報化社会への発展に続く，社会発展の歴史における5番目の新しい社会（Society 5.0[(1)]）であり，生活をより豊かにしていく未来のあり方（Smart World）として期待されています．

さまざまな革新技術によってサイバー空間（仮想空間）とフィジカル空間（現実空間）が高度に融合されたSmart Worldにおいては，フィジカル空間から集積されるセンサ情報などの膨大なデータが，高知能化されたサイバー空間でのデータ分析・予測に活用され，フィジカル空間へ自律的にフィードバックされます．

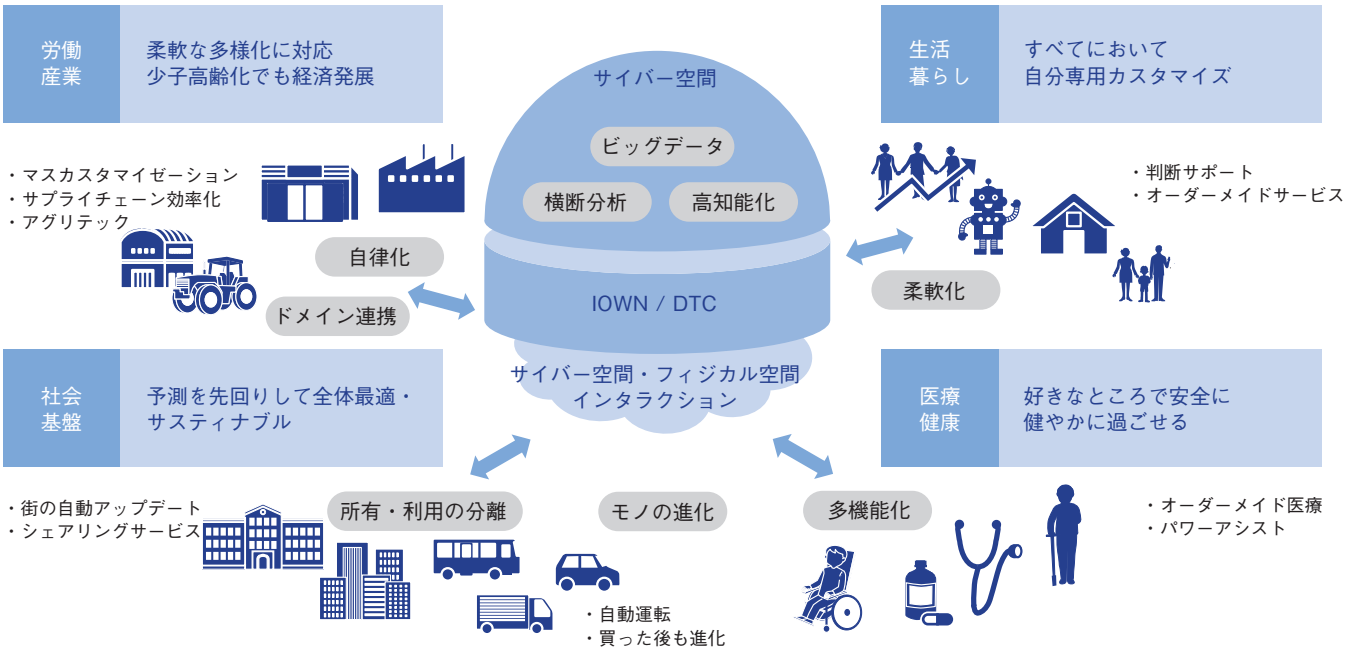

図1　10年後のSmart World

その結果，さまざまなサービスや社会基盤において，利用者個人への最適化と社会全体の最適化の両方が進展し，すべての人が安全に自分らしく暮らせる社会（真のSmart World）が実現されると考えられます．

例えば，個人の暮らしや生活にかかわる面では，個々人の状況に合わせた究極のカスタマイズされたサービスを享受できるようになります．社会インフラにかかわる面では，AI予測によって先回りの対応を行い，社会全体の最適化やサスティナブル（持続可能な）提供が可能になります．経済・産業にかかわる面では，多様化にも柔軟に対応し，少子高齢化が進む社会環境であっても経済を発展させることが可能になります（**図1**）．

一方で，このような理想の世界の実現を支える技術・インフラの高知能化，自律化，柔軟化，ドメイン連携などによって，「脅威にさらされる機会」や「被害の程度・範囲」も一気に拡大してしまうという負の側面も考えられます（**図2**）．

膨大なデータを分析したり利用する際に，プライバシが十分考慮されなかったり，倫理に反するような利用がされるおそれや，意図せぬ情報の漏洩といったことも考えられます．

データ分析アルゴリズムが悪意のある者の手によって改ざんされてしまうという脅威も現実味を帯びてきています．従来はあらかじめ設計されたアルゴリズムに従って作成されたプログラムに直接手を入れたり，プログラムをすげ替えたりしなければ改ざんも難しかったものが，AIが普及した状況では，AIの学習やAIによる判断に対して誤作動を引き起こさせるといった直接的な改ざんを伴わない攻撃が行われるおそれがあります．具体的には，AIに学習させるデータに不正な値を混入させて攻撃者が意図するような判断をさせる，AIに認識させるデータを細工することによって判断を誤らせるといった攻撃や，AIの動作から学習したデータを推測することによってプラ

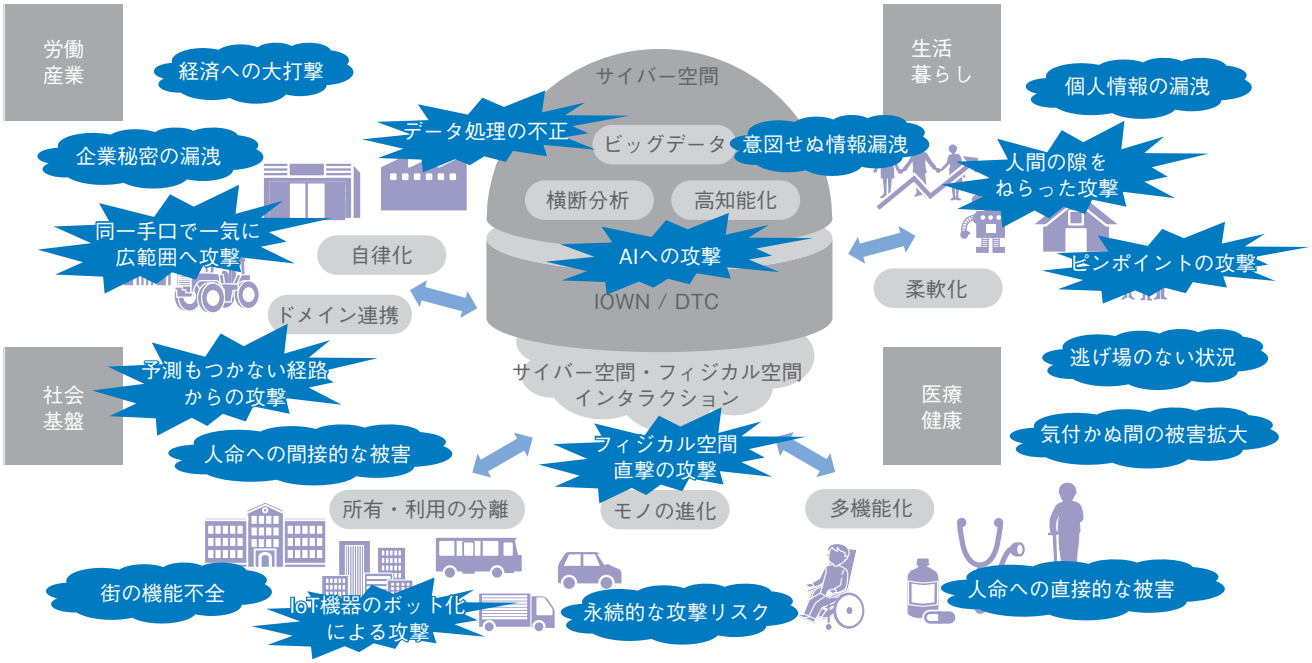

図 2　10年後のSmart Worldに潜むセキュリティ脅威

イバシの侵害に及ぶようなデータを不正に入手されるといった新たな攻撃が考えられます．

アルゴリズムが改ざんされると，データが意図的に漏洩されるだけでなく，分析結果を悪意のあるものに変えられてしまうおそれもあります．悪意のある分析結果がフィジカル空間にフィードバックされてしまうことによって，さまざまなサービスや社会インフラに多大な影響が及んでしまいます．

真のSmart Worldを実現するためには，このようなサイバー空間とフィジカル空間が高度に融合されたことによって新たな脅威となる側面を考慮し，肥大化・巧妙化する攻撃に対抗しつつ，利便性の向上を両立させることのできるセキュリティR&Dをめざしていかなければなりません．

長期的な視点でのセキュリティR&Dの考え方

セキュリティリスクは，攻撃の脅威（人間や社会を含む広い意味での），システムの脆弱性，守らなければならない（情報，金銭面だけでなく人命なども含めた）資産の大きさに依存します．サイバー攻撃が肥大化・巧妙化し，サイバー空間とフィジカル空間の高度な融合によって従来よりもさまざまな脅威にさらされてしまう状況においては，セキュリティリスクは飛躍的に増加してしまいます．

一方でセキュリティ対策を強化することになると相応のコストがかかってしまうため，企業がセキュリティ対策にかけられるコストにも限界があります．今後のサイバー攻撃の拡大に対抗するためには，既存のセキュリティ対策の延長や単なる増強だけではすべての脅威への対策技術を実現することは困難なため，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．

そのため，長期的な視点に立ったセキュリティR&Dとしては，①Smart Worldにおける価値の創造をサポートするために新たな脅威へ対応し，創造

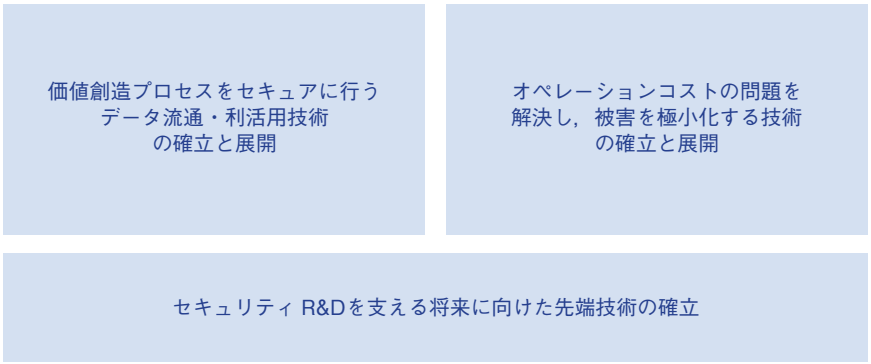

図3　セキュリティR&Dに必要な観点

するための環境を守る技術に注力することと，②脆弱性のリスクをゼロにする技術や，攻撃を予測し事前対処を行う技術など，攻撃者優位の状況を変える技術を創出していくこと，をめざして取り組んでいくことが求められます．

また，NTTグループが今後取り組んでいくビッグイベントへの対応体制の強化，中期経営戦略に基づいた新たな分野（街づくり，エネルギー，ヘルスケア）への展開には安全なデータ利活用の実現，ゲームチェンジをめざすIOWN（Innovative Optical and Wireless Network）構想の実現に必要なセキュリティが求められることから，今後取り組んでいくべきセキュリティの研究開発としては以下の観点が重要なポイントになります（**図3**）．

⑴　価値創造プロセスをセキュアに行うデータ流通・利活用技術の確立と展開

データの囲込みやプライバシ侵害，不正利用の問題を解決し，分野横断的にデータを利活用できる柔軟で安全なデータの共有・分析の仕組みの実現．

⑵　オペレーションコストの問題を解決し，被害を極小化する技術の確立と展開

新たな脅威への対応をしつつ，サイバー攻撃対応のオペレーションを自律化・自動化する技術の確立によって，人は対処の確認および創造性が必要となる新しい脅威の対応に注力できるようにすることにより，総合的な対応力を強化．

⑶　セキュリティR&Dを支える将来に向けた先端技術の確立

セキュリティCoE（Center of Excellence）として，暗号・情報理論，量子情報セキュリティ技術など，将来に向けた基礎技術の確立．

NTTグループに求められる「安全・安心のコミュニケーション」を将来にわたって持続していくために，私たちは将来に向けた先端技術やIOWNの特徴を活かした技術を含め，中長期的なテーマの目的である「データ流通・利活用」と「被害を極小化」の実現に向けた研究開発に取り組んでいきます．

■参考文献

⑴　https://www8.cao.go.jp/cstp/society5_0/

平田　真一

いろいろなことが絡み合いながら変化していく昨今，自らの意識の変革も含めて，既存の枠・価値観にとらわれず進めていけることが大事であると考えています．世の中のこれからの動きを見つつ，私たちの技術により世の中を変えていけるような大きな成果にご期待ください．

◆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