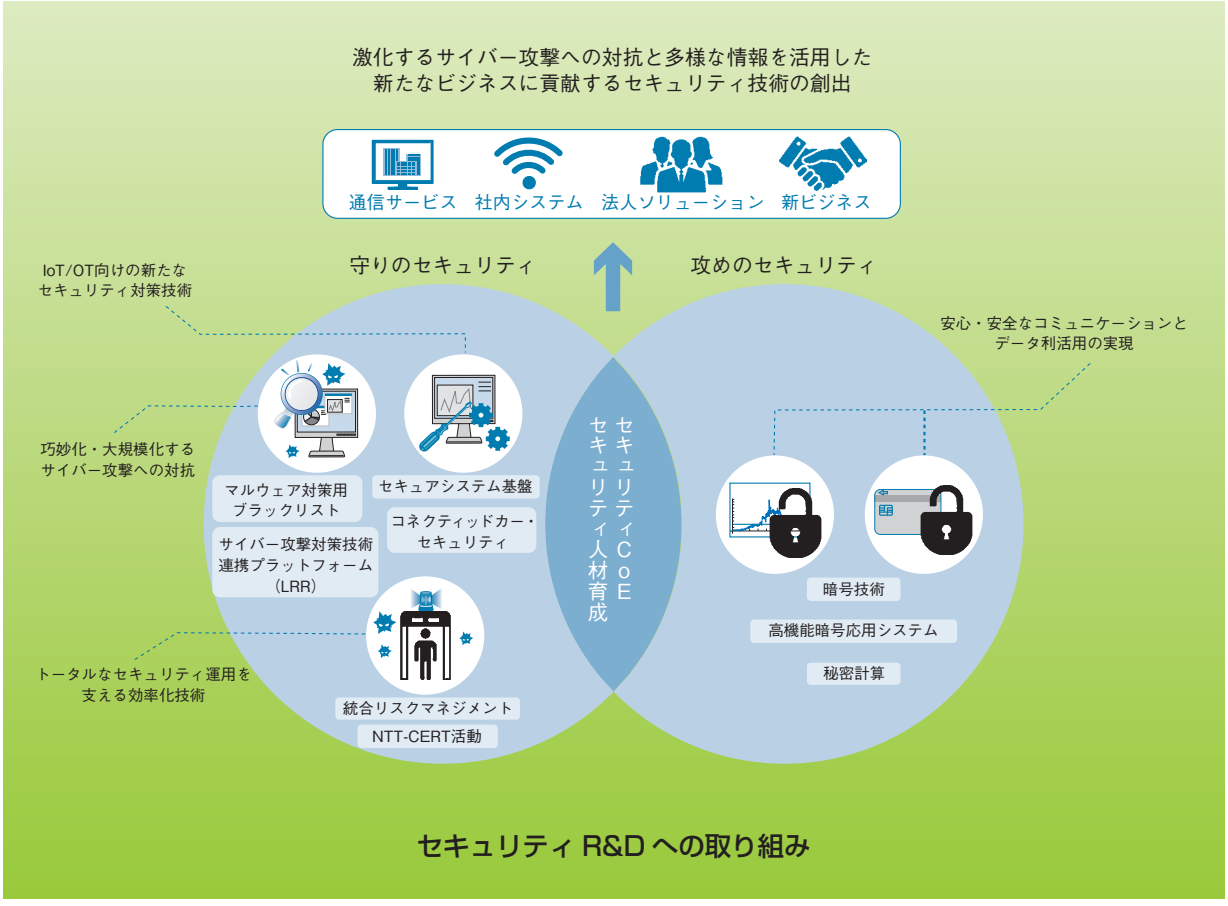
特　集

デジタル社会の実現をの最前線

サイバー攻撃　暗号　Webセキュリティ　秘密計算　耐量子安全性

サイバー空間を取り巻く環境変化により具現化してきた脅威やセキュリティの問題を解消すべく，研究開発が急がれている．本特集では，NTTセキュアプラットフォーム研究所のセキュリティ技術への取り組み，研究所の成果が世界中の有力企業を対策へと動かした実例や近年注目を集める耐量子暗号技術の研究動向を紹介する．



支えるセキュリティ技術

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

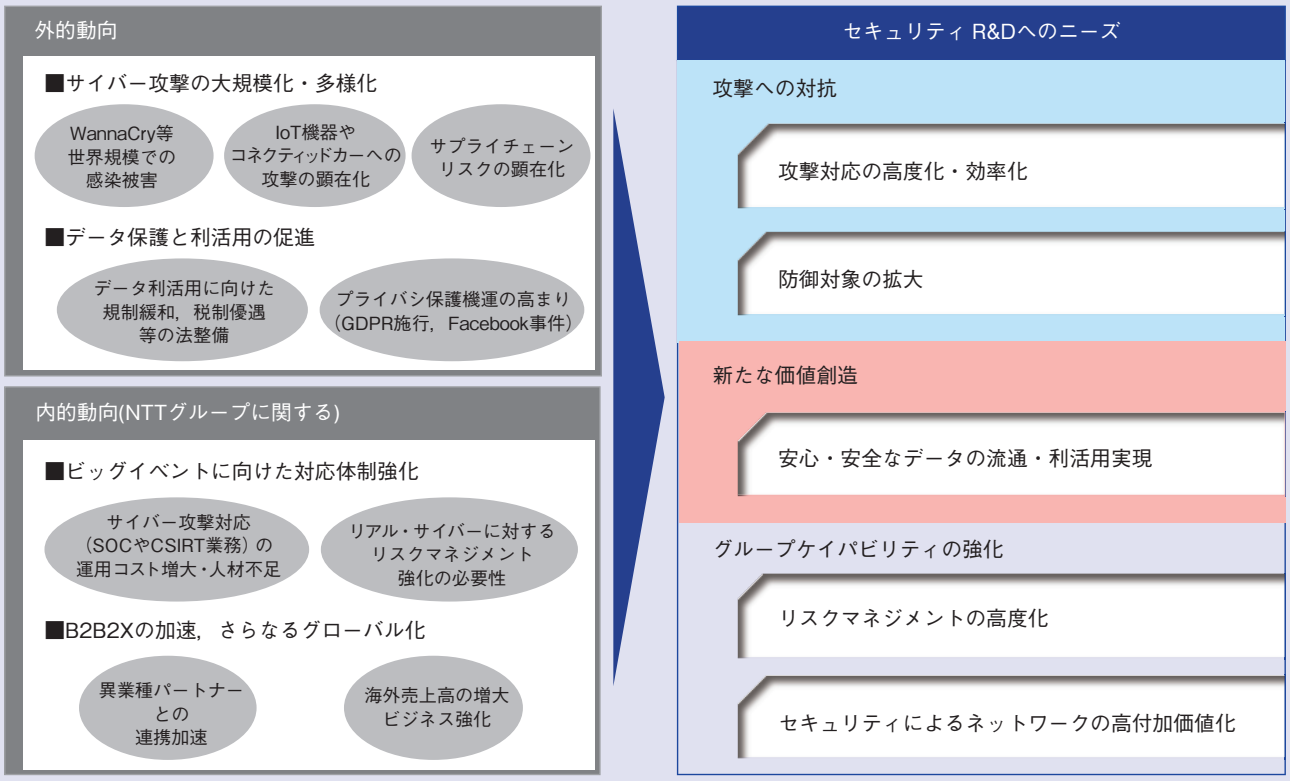


図1　環境変化とセキュリティ R&Dへのニーズ

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

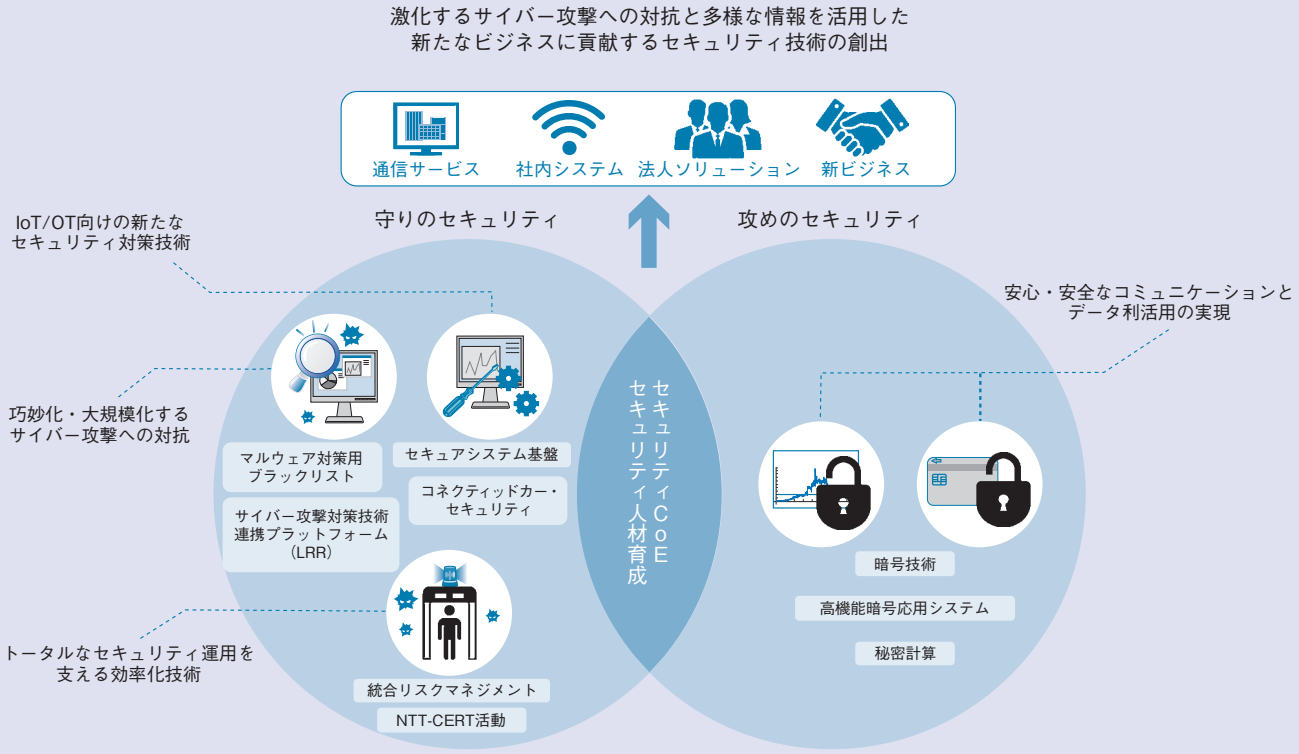


図2　セキュリティR&Dへの取り組み

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

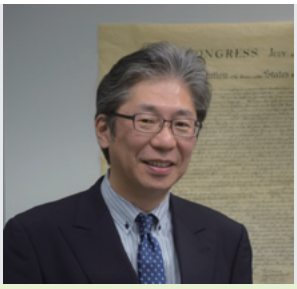
「セキュリティCoE」では，NTTグループ内外を問わず，学術界やハイレベルな専門化コミュニティなど幅広い分野において研究所が有する高度な専門スキルを持つ人材が牽引・貢献を行っています．サイバーセキュリティの分野では，著名なコンテストの運営にかかわるだけでなく，専門家でなくても理解しやすい啓発書・入門書の執筆[2]や大学講義など，「セキュリティ人材育成」の観点からも活動に取り組んでいます．データセキュリティの分野では，暗号理論を代表とする世界最先端の研究を行っており，10年，20年先を見据えた次世代の競争力の源泉となる差異化技術の創出に取り組んでいます．具体的な研究事例としては，次世代の秘密計算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

新たなプライバシ脅威「Silhouette」の発見と対策への取り組み

ユーザおよび事業者にとって，全く未知の脅威による被害を未然に防ぐためには，システムに潜在するセキュリティ上の問題を攻撃者より先に解明し，あらかじめ防御策を講じておくことが重要です．本稿では，こうした脅威実証研究の一環で発見した新たなプライバシ脅威「Silhouette」の仕組みと対策手法，および世界的なサービスやブラウザのセキュリティ機能を強化させるに至った取り組みについて紹介します．

わたなべ　たくや
渡邉　卓弥
NTTセキュアプラットフォーム研究所

Silhouetteがもたらすプライバシ脅威

SNSや動画共有サービスといった，人と人との相互コミュニケーションによってコンテンツが形成されるソーシャルウェブサービス（SWS）は，登場以来めざましい発展を続け，今日では私たちの生活に不可欠な存在となりました．インターネットユーザに対する調査[(1)]によれば，１人当り平均５種類以上のSWSのアカウントを保有していると報告されています．SWS上では，これらのアカウント名を基にユーザのプロフィールや投稿を参照できるため，氏名や顔写真，その人のアクティビティといった個人情報が各アカウントに紐付いているといえます．

NTTセキュアプラットフォーム研究所（SC研）が発見したプライバシ脅威「Silhouette（シルエット）」では，あるユーザが第三者のWebサイトにアクセスした際に，自身の所有するSWSアカウントを第三者から特定されてしまいます．例えば，検索エンジン経由や，一般的なWebサイトに含まれる広告，メールに含まれるリンクによって，本来SWSと全く関係のない悪意のあるWebサイトへアクセスしてしまうと，その悪意あるWebサイトはユーザが利用しているであろうSWSへの通信をユーザには分からないように裏で行い，収集した情報からアカウント名を特定します．

特定が成立してしまう条件は，PCやモバイル端末のWebブラウザにおいて，本脅威に対して脆弱なSWSへのログイン状態を保持しているユーザが，悪意ある第三者の設置したWebサイトを訪問するというものです．一般的なSWSでは，ログアウトを明示的に実施する等の操作によってブラウザのCookie*が削除されるまで，自動的にログイン状態を保持する仕組みになっています．したがって，過去に一度でも脅威の対象となるSWSを利用した経験のあるユーザは，特定の対象となってしまうおそれがあります．

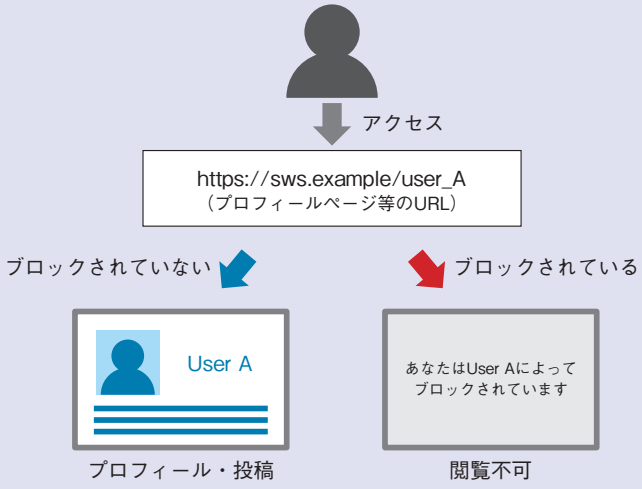


図１　ユーザブロック機能

脅威が成立する仕組み

本脅威を成立させるために，SWSに広く採用されている「ユーザブロック」という機能（**図１**）が悪用されま

＊ Cookie：ユーザ設定，ログイン状態，セッション等を管理するために，Webサービスが訪問ユーザのWebブラウザに情報を保存できる機能です．

す. ユーザブロックは本来, 正当なユーザが悪質なユーザに対して自身のページ閲覧可否をコントロールし，ハラスメントやスパム行為から身を守るための機能です．SC研は，悪質なユーザもまた正当なユーザに対してページの閲覧可否をコントロールできてしまうというユーザブロックの特性に，セキュリティ上の問題が潜在していることを突き止めました．

事前準備として，悪意ある第三者はSWS内に自らアカウント（特定補助アカウント）を作成します．特定補助アカウントを複数用意し，同一サービス上のユーザらを計画的にブロックすることで，さまざまな閲覧可・閲覧不可の組合せパターンを構築することができます．このパターンは，ユーザアカウントを一意に識別するための情報として利用されます（**図2**）．

特定実行時，すなわちアカウント名を特定するためのスクリプトが設置されたWebサイトに訪問したユーザに対しては，それぞれの特定補助アカウントのページへの通信を強制的に送信させます．このときの通信は，異なるサイト間のデータ漏洩を防ぐためにWebブラウザが採用しているSame-Origin Policyによって保護されているため，第三者は応答内容を直接的に取得することはできません（**図3**）．しかしながら，閲覧可能時と閲覧不可能時では通信の応答時間には統計的な差異が発生します．悪意ある第三者はこの差異を用いて，訪問ユーザがそれぞれの特定補助アカウントからブロックされているかどうかを推定することができます．推定結果を，あらかじめ構築したパターンと照合することで，当該ユーザのSWSにおけるアカウント名を特定します．

既存のサイバー攻撃のカテゴリに当てはめると，Silhouetteはクロスサイトリクエストフォージェリ（CSRF）およびサイドチャネル攻撃に分類され

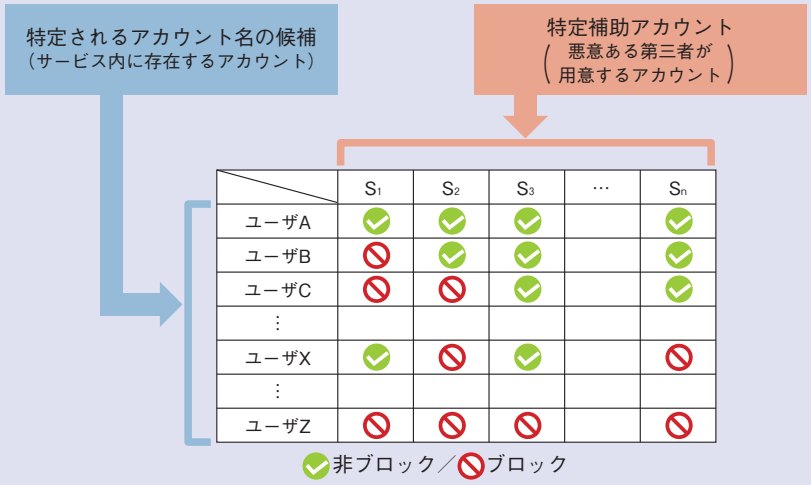


図2　閲覧可・閲覧不可のパターン例

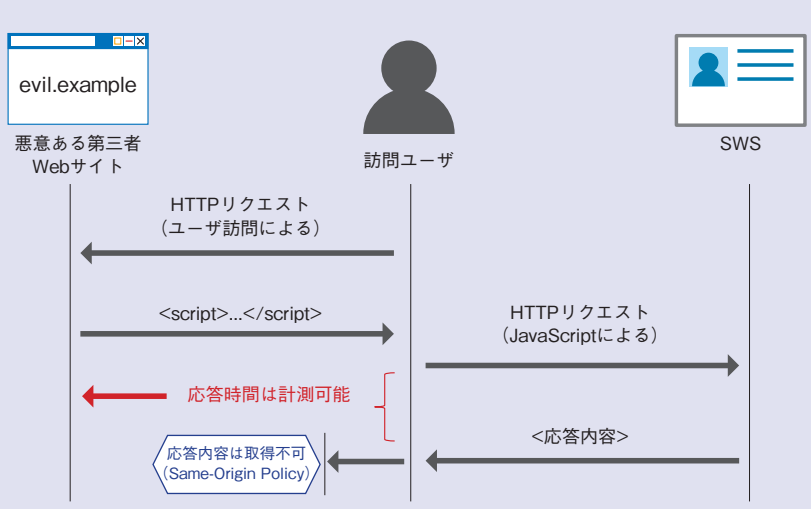


図3　Same-Origin Policyによる応答内容の保護

ます．CSRFとは，ユーザが意図しない異なるサイトへのリクエストを強制的に送信させることで，データの奪取や悪性コードの実行などを行うWeb系の攻撃です．また，サイドチャネル攻撃とは，応答時間や電力消費量といった物理空間の情報を活用し，センシティブな情報の推測を行う攻撃の総称です．本研究は，CSRFとサイドチャネル攻撃を組み合わせることで，SWSに広く採用されているユーザブロック機能を悪用し，正当なユーザのプライバシを脅かすことができてしまうという，サービス設計に潜在していたセキュリティ上の問題を明らかにしました．

対策手法

本脅威に対して，SWS事業者およびユーザが実施可能な対策手法をそれぞれ紹介します．前述したとおり，本脅威はCSRFとサイドチャネル攻撃を組み合わせた攻撃であるため，これらのいずれかを防御することで対策が実現します．サイドチャネル攻撃の対策[(2)]には，タイミング情報の特性を考慮した専門的な見地が必要とされますが，CSRFは，Webサービスのプログラム変更を伴う汎用的な対策が知られています．以下では，CSRFの対策に主眼を置いた対策手法を紹介します．

■前提条件

本脅威の対象となり得るSWSは，アカウント登録機能があり，なおかつユーザブロック機能などによって，あるユーザが他のユーザに対して，ユーザのコンテンツページ（プロフィールなど）の閲覧権限を強制的に変更できる機能を持っているサービスとなります．これらに該当しないサービスは本脅威の対象とはなりません．

■SWSによる対策

SWSが実施できる1番目の対策は，SameSite属性と呼ばれるCookieのオプションを用いたものです．SameSiteが付与されたCookieは，JavaScript等による異なるサイトへのリクエスト時に送信されなくなります．したがって，ログイン状態を管理するCookieにこの属性を指定することで，本脅威を含むCSRFを広く対策することが可能となります．ただし，本機能を利用するためには，ユーザの用いるWebブラウザがSameSiteに対応しているうえで，SWSがHTTPヘッダでSameSiteの利用を宣言する必要があります．後述するとおり，Silhouetteを対策するためのSC研の取り組みによって，世界中の主要なブラウザがSameSiteに対応するようになりました．

2番目の対策は，リクエスト検証と呼ばれるものです．CSRFでは，JavaScriptによってユーザおよびサービスが意図しないHTTPリクエストが発生します．このとき，SWSなどのサービス側で，リクエストの送信元となったWebサイトのURLを示すリファラや，CSRF対策のための特殊な文字列を含んだリクエストパラメータを検証することで，正当なリクエストであるかどうかを判別するという対策手法[(3)]が知られています．リクエスト検証は，Webサービスへの投稿等を行うPOSTメソッドを受け付けるページで採用されることが多いですが，ユーザプロフィールのようなGETメソッドを受け付けるページにおいても採用することができます．ただしこの場合，検索エンジンやブログ記事から直接リンクされた際に検証に失敗し，不正なリクエストとして棄却してしまう可能性があります．そこで，検証に失敗した際には，サービス側が実際のコンテンツを含まない中間ページを返した後，その中間ページのJavaScriptによって実際のコンテンツを取得するという手順を加えることで，ページを表示するまでのリクエスト数は増加するものの，直接リンクからのアクセスを阻害することなく対策できます．

■ユーザによる対策

ユーザが実施できる対策の1つに，ブラウザに搭載されているプライベートブラウジングモードが挙げられます．これはシークレットモード，プライベートウィンドウ，InPrivateなどとも呼ばれており，この機能を有効にしている間は，今までのCookie情報を引き継ぐことなく，また終了時には新たに保持したCookieを削除するようになります．プライベートブラウジングを有効にしてから第三者のWebサイトに訪問することで，本脅威によるアカウント名の特定を防ぐことがで

きます．

ユーザが実施できる2番目の対策は，SWSからログアウトすることです．本脅威では，ユーザがSWSにログインしているという状態に基づいて，アカウント名の特定が実現します．SWSにログインしてサービスを利用した際は，終了時に毎回ログアウト処理を行うなどの手段によって，本脅威によるアカウント名の特定を防ぐことができます．

脅威の成立を未然に防ぐための取り組み

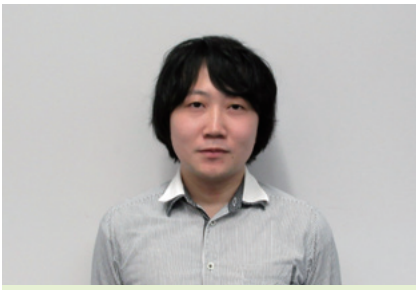
SC研では，Silhouetteに対してSWSが脆弱であるか評価する手法を確立し，NTTグループおよび世界的に著名な外部のSWSの調査を実施しました．その結果，影響力の大きな海外の著名サービスの一部において，実際にアカウント名が特定され得る状態にあることを解明し，事業者に対して脅威の詳細や対策方法の共有と，対策の有効性を検証する実験協力を行いました．この取り組みを受けて，TwitterなどのSWSが仕様変更によってセキュリティ機構を向上させ，アカウント名特定の脅威を未然に防ぐことができました．さらに，Microsoft Edge，Internet Explorer，Mozilla Firefoxといった主要ブラウザにおいて，本研究や類似手法によって発生し得る脅威を回避するため，CookieのSameSite属性が利用できるようになりました．この貢献による影響ユーザは現時点で6億人以上にのぼり，世界中で利用されている多くのSWSの安全性を大きく向上させただけでなく，今後NTTを含むあらゆる事業者がセキュアなWebサービスを設計するための高度な機能を活用できるようになったことを意味します．本研究の成果は，短期的・中長期的いずれの視点においても，世界中のユーザがより安全にインターネットを利用できる環境を実現したといえます．また，脅威の発見および実証と対策手法をまとめた論文[2]は，世界トップレベルの学術会議「IEEE European Symposium on Security and Privacy」に日本から初めて採択されるとともに，サイバーセキュリティ業界に大きな影響力を持つ国際会議「Black Hat Europe」に採択[4]されるなど，世界のWebセキュリティ向上のために極めて大きなインパクトを与えました．

今後の展開

SC研はサイバーセキュリティに関する研究開発の一環として，このたび発見した脅威「Silhouette」を含む新たな脅威を評価する手法の開発を実施するとともに，問題を発見した際には関係機関と協力して対策の実現に向けて取り組んできました．今後も潜在的な脅威の発見と対策の展開を継続することで，NTTが堅牢なサービスを提供できるよう努め，Webサービスや Webブラウザのセキュア化を推進し，インターネットの安心・安全な利用を促進します．

■参考文献

(1) https://www.brandwatch.com/blog/amazing-social-media-statistics-and-facts/
(2) T. Watanabe, E. Shioji, M. Akiyama, K. Sasaoka, T. Yagi, and T. Mori：“User Blocking Considered Harmful? An Attacker-Controllable Side Channel to Identify Social Accounts,” Proc. of EuroS&P 2018, London, U.K., April 2018.
(3) https://www.ipa.go.jp/security/vuln/websecurity.html
(4) https://www.blackhat.com/eu-18/briefings/schedule/index.html#i-block-you-because-i-love-you-social-account-identification-attack-against-a-website-visitor-12912



渡邉　卓弥

どんなに堅牢なシステムを構築しても，攻撃者はときに物理空間の情報まで駆使し，迂回する方法を探します．本当の意味で脅威を未然に防ぐため，攻撃側の視点から彼らより先に脅威を発見し，対策を講じることをめざしています．

◆問い合わせ先
NTTセキュアプラットフォーム研究所
サイバーセキュリティプロジェクト
TEL　0422-59-7466
FAX　0422-59-3844
E-mail　takuya.watanabe.yf@hco.ntt.co.jp

秘密計算システム 算師®の試用提供

北條 裕之（きたじょう ひろゆき）†1 /山口 卓也（やまぐち たくや）†1
西山 小奈未（にしやま さなみ）†1 /高橋 元（たかはし げん）†2
宮島 麻美（みやじま あさみ）†2 /廣田 啓一（ひろた けいいち）†2
西田 祥子（にしだ しょうこ）†2 /橋本 順子（はしもと じゅんこ）†2

NTT研究企画部門†1
NTTセキュアプラットフォーム研究所†2

NTTでは，企業秘密やパーソナルデータなど守るべきさまざまなデータの安心・安全な利活用に向け，データを暗号化したまま，実用的な速度で安全に集計・統計処理できる秘密計算システム 算師®（算師）を開発しました．データ利活用の活性化に向けた取り組みとして，秘密計算の「データを互いに開示することなく，データを暗号化したままで統合分析できる」利点を多くの方に体験いただくべく，期間限定ではありますが，算師を無償で試用提供しています．本稿ではその取り組み内容と秘密計算について紹介します．

背　景

昨今，さまざまな分野のデジタルトランスフォーメーションにより，サービス化，オープン化，ソーシャル化，スマート化への変化が進んでおり，分野横断的なデータの蓄積やデータの利活用がイノベーションを促進し，経済成長などさまざまな分野の発展につながることが期待されています．一方，データの管理に伴うインシデントリスクや社会的責任の大きさ，企業戦略等の保護の観点による，データのセキュリティ対策の必要性などがデータ利活用促進を阻害する要因となっています．

NTTはそのような要因の解消に貢献するため，データを暗号化したままデータ処理可能な秘密計算技術の研究開発に世界に先駆けて取り組んできました．秘密計算の利点は，計算結果以外は誰にも見えないデータ運用ができること（**図1**）と，これにより，今まで他組織に開示することが難しかったデータを持ち寄った新しい統合分析が可能になることにあります．これまで，多施設臨床研究データ[(1)]やゲノムデータの解析[(2)]など，さまざまな分野への適用事例を検証するとともに，演算機能の充実や高速化等の改良を加え，NTTの秘密計算システム 算師®（算師）として開発を進めてきました[(3)]．

算師の試用提供概要

NTTが開発した算師は，秘密計算の持つ「データを互いに開示することなく，データを暗号化したまま統合分析できる」という利点をシステムとして実現したものです．さまざまな分野の多くの方々にこの価値を体感していただくことを目的として，算師を無償で試用提供を開始しました．2018年8月20日より開始し，最長2019年3月まで利用いただけます．現在，ヘルスケア，製造業，SIer等，さまざまな分野のお客さまにご利用いただいています．

利用者には，クラウド上に構築した算師を用いて，データを暗号化したまま集計・統計処理を行う機能を実際に体験いただくことができます．気軽にお試しいただける代表的な分析シナリオと試用データを3種類用意しました（**表1**）．

1番目は，「同業他社との連携強化」で「データ量（行）を増やす」シナリオです．競合他社と相互に情報開示は行いたくないが，業界活性化や業界課題解決につなげることを想定しました．地域商圏を一例とし，算師上に複数事業者による購買データを安全に登

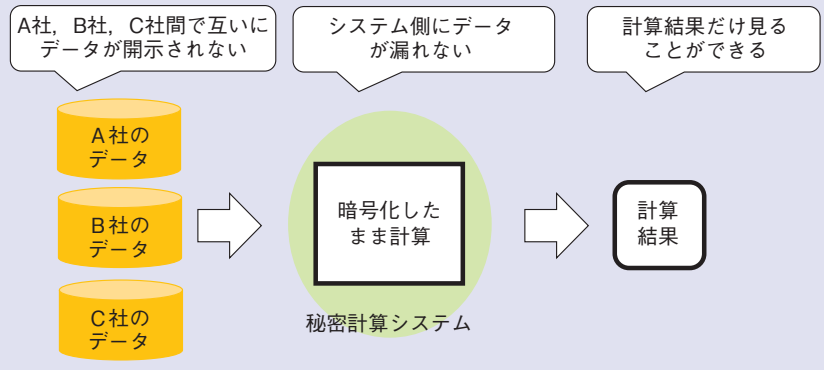


図1　秘密計算の利点

表1　試用提供システムで体験いただける代表的な分析シナリオ

項　目	シナリオ概要
同業他社との連携強化	地域商圏の活性化に向けて，地域にある複数企業の販売データを統合・分析し，地域商圏全体として品ぞろえの充実や販売機会の損失回避を図る
異業種データの連携	ネット販売会社の購買データと，健康支援アプリ提供会社が保有するバイタルデータ（BMI・歩数）を組み合わせて分析し，健康関連商品のマーケティングや商品レコメンド（広告収入拡大）に活用する
演算機能の体験	世帯属性，世帯支出，食費などのデータ群に対して，どのような演算が可能か試用いただく

録し，全事業会社のデータを結合した状態としておき，利用者（データ分析者）は商圏全体の総売上金額や年代ごとの売上上位商材などを確認できます．

2番目は，「異業種データの連携」で「データ項目（列）を増やす」シナリオです．異業種でのデータを組み合わせることで，新たな傾向発見や新たなビジネス価値を生み出すことを想定しました．一例とし，ネット販売会社の購買データと健康支援アプリ提供会社のバイタルを組み合わせ，算師上に安全に登録し，利用者（データ分析者）は健康食品を購入している顧客の年代別の歩数平均などを確認できます．

3番目は，算師がサポートする演算機能を自由に試していただけるシナリオです．公的統計情報（一般用ミクロデータ）を算師上に安全に登録し，利用者（データ分析者）は，消費支出，食費，保険医療費などのデータを用いた演算が可能です．

また，さらなる試用を希望される利用者には，自身が保有するデータに基づき，代表シナリオ以外の個別の分析シナリオ等で算師を試用するサポートもしています．

秘密計算

秘密計算とは，データを暗号化したまま，計算できる技術です．一般的な暗号ではデータの計算時には，復号する必要があるため，データが分析者やシステム運用者に漏洩するリスクがあります．一方，秘密計算は，データを暗号化したまま計算を行うことが可能であるため，分析者やシステム運用者は途中経過を含む一切のデータを見ることができません．このため，企業の秘密情報のようなデータでも，安全に利活用することが可能になります．

秘密計算は，1980年代に計算機科学・暗号理論の分野で“Secure multi-party computation”と呼ばれる理論の大枠が確立されましたが，実用上は計算に時間がかかる（遅い）ことが課題とされてきました．近年高速化・実用化研究が活性化しています．NTTでは秘密計算方式として，秘密分散をベースとした高速な秘密計算方式を開発しました．

■秘密分散による暗号化

NTTの秘密計算の暗号化の仕組みとして，秘密分散を採用しています．秘密分散はデータを複数のシェアと呼ばれる断片に分割し，機密性を高める技術です．個々のシェアから情報は漏れません．さらに，いくつかのシェアが消失してもデータを復元可能です．また，秘密分散方式として，ISO標準準拠（ISO/IEC 19592-2）仕様を用いています．この，ISO化においては，NTTはエディタとして標準化に貢献しました．

■秘密分散をベースにしたマルチパーティ計算

暗号化したまま計算する仕組みとして，秘密分散をベースにしたマルチパーティ計算を採用しています．マルチパーティ計算では，システムは複数のサーバから構成され，サーバ間でデータの交換と演算をあらかじめ決められた手順で行います．各サーバには，秘密分散されたシェアが登録され，データは常に秘密分散のシェアの状態で扱われます．

■秘密計算の安全性

秘密分散された個々のシェアから元データや計算結果を復元することは一切できません．ただし，分割したシェアを複数のサーバに各々登録しますが，一定数のサーバからシェアを不正に取得されるとデータが復元できてしまいます．このため，各サーバを正しく管理することが安全性の条件です．

■秘密計算の原理

秘密計算では，データは複数のシェアに秘密分散されます．ここでは，「2」を3つのシェアに秘密分散する例を紹介します（**図2**）．秘密分散のシェア生成では，乱数を生成し，生成した乱数を元に計算を行います．まず，乱数を2つ生成します．生成される乱数，「0」から「9」のランダムな値とします．乱数として「5」と「3」が生成された場合は，3つのシェアのうち2つのシェアを「5」と「3」とします．次に3番目のシェアをこの2つのシェアから計算して求めます．元のデータ「2」から2つのシェア「5」と「3」を足し合わせた「8」をマイナスします．この際，マイナスして得られた値「−6」は，「4」となり，3番目のシェアは「4」に決まります．

元のデータに復元する際は，3つの

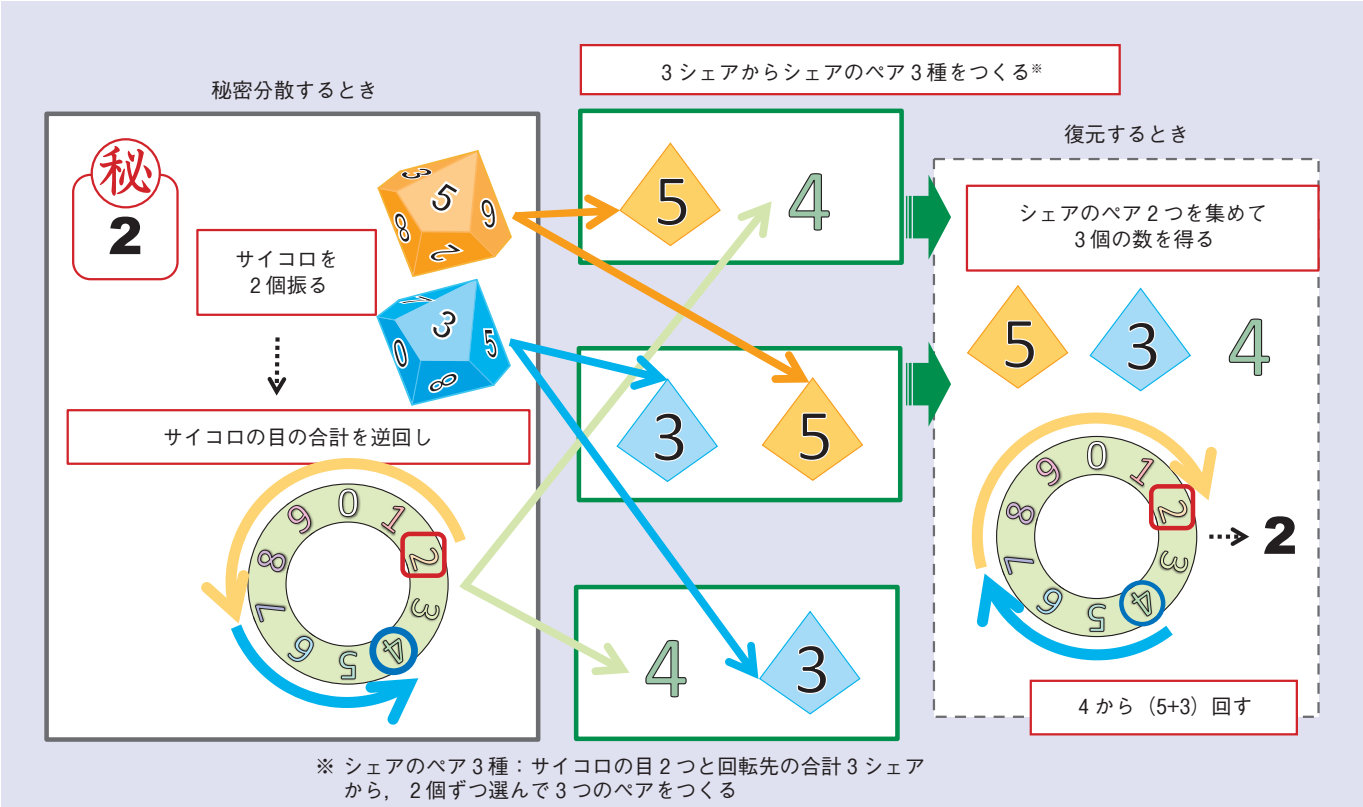


図2　秘密計算の原理

表2　NTTの秘密計算システム算師が具備する主な演算

データ操作	集　計	基本統計		検　定
		総和	最大値	t検定
テーブル結合	度数表（クロス集計）	平均	最小値	
条件によるフィルタ	数量表	分散	中央値	その他
		積和	分位数	Kaplan-Meier法

シェア「5」と「3」と「4」を集めて，それぞれ足し合わせます．この際，「4」に「3」と「5」を足し合わせた値の「12」は，「2」となり，元のデータの「2」が復元できます．

計算は，このように生成されたシェアを各サーバ上でシェアのまま計算を行います．例えば，総和を計算したい場合，各サーバでシェアの状態で総和の計算を行い，最後に，各サーバで計算した値の総和の結果を上記の方法で復元することで，総和の結果を得ることができます．

算師の特長

NTTの算師は，秘密計算の長年の技術課題であった処理速度を劇的に向上し，100属性×1000万件規模のデータの集計や統計演算を実用的な時間内に処理することができる世界最高レベルの秘密計算システムです．豊富な集計・基本統計演算処理を持ち，各演算を高速に実行することができます．

■充実した演算バリエーション

算師では，**表2**に示す演算をWebブラウザ上のGUIや統計解析ソフトウェア「R」のインタフェースでデータを見ることなく実行することができます．さらに，「R」で簡単なプログラムを作成し，回帰分析や主成分分析など，用途に応じた分析を実行することも可能です．試用提供システムでは，これらのインタフェースの一部を利用いただけます．

特に，算師が提供するテーブル結合機能（複数の表を結合キーも漏らすことなく結合できる機能）は，異なる企業間や異業種間で，互いに所有データを見せることなくデータを統合し，横断分析した結果のみを得ることを可能にします．これにより，複数の企業をまたがるサプライチェーンや顧客データの分析など，これまで一企業や一業界では成し得なかったデータ利活用の新たな価値創造に貢献できると考えています．

表 3　代表的な機能の実行時間

機　能	実行時間（ミリ秒）				
データ件数	10^3	10^4	10^5	10^6	10^7
加　算	1	1	1	2	14
乗　算	1	1	5	39	473
ソート	10	23	133	1274	12255
総　和	1	1	1	1	9
積　和	1	1	1	2	15
数量表作成	22	46	255	2252	22676
シャッフル	1	1	8	60	731
テーブル結合	19	65	518	4965	53205
条件によるフィルタ（文字列前方一致）	6	6	14	91	813
条件によるフィルタ（数値一致）	5	5	10	35	413

PC 3 台（CPU: Intel Core i7-6900K, メモリ: 32 GB, SSD: 525 GB, OS: CentOS 7.2）を10 Gbit/sネットワークで接続した環境で測定

■実用に足る高速性

算師では，秘密分散方式の採用[(4)]に加え，独自の高速化アルゴリズムと暗号実装技術により，前述の豊富な演算バリエーションの提供と処理速度の向上を両立させています．

秘密分散に基づく秘密計算では，データ処理の基本となるデータのサイズが小さい，演算を行う際に頻繁に使用される加算と乗算の両方を高速に処理できる，という圧倒的な 2 つの利点があります．そのため，準同型暗号など他の暗号方式に基づく秘密計算と比べ，さまざまな演算を高速に処理することが可能です．

加えてNTTでは，非常に小さい計算コスト・通信コストで動作する秘密計算の基本アルゴリズムを開発し，これを高度な暗号実装技術によって実装することにより，処理速度を劇的に改善し，世界最高レベルの演算速度を達成しています．

代表的な機能の実行時間を**表 3** に示します．1000万レコードの並び替え処理（ソート処理）を12.2秒で実現しています．暗号化されていない1000万レコードのデータを一般的なソートアルゴリズムでソートした場合，1 秒程度の演算時間です．秘密計算と通常のコンピュータ処理の性能比はおよそ「一桁レベル」に迫っています．

■算師のシステムイメージ

秘密計算では複数のサーバが一体となって計算を行うマルチパーティ計算を行います．算師は，秘密計算クライアント，3 台もしくは 4 台の秘密計算サーバから構成されます．データ登録を行う秘密計算クライアントはデータを秘密分散のシェアに分割して各サーバに登録します．また，データ分析を行う秘密計算クライアントは各サーバに計算（データ分析）を要求し，計算結果のみを得ます．データは，リレーショナルデータベースのようにテーブル形式で登録されており，データが格納されているテーブル名や列名を指定して，平均値や分散値等の計算を要求します．計算要求を受けた各サーバは，それぞれ協調して，マルチパーティ計算を行い，計算結果を秘密分散のシェアとしてデータ分析を行う秘密計算クライアントに応答します．秘密計算クライアントは，シェアを復元することで結果を得ます．

今後の展開

NTTは，算師の試用提供を通じて，企業秘密やパーソナルデータの安心・安全な利活用のより一層の促進をめざし，秘密計算をはじめとするデータ利活用技術の開発とグローバルを含めた普及に努めていきます．

■参考文献

(1) http://www.ntt.co.jp/news2012/1202/120214a.html
(2) http://www.ntt.co.jp/news2016/1607/160712a.html
(3) http://www.ntt.co.jp/sc/project/data-security/secure_computation.html
(4) http://www.ntt.co.jp/news2017/1710/171023a.html

（上段左から）西山　小奈未/ 北條　裕之/ 山口　卓也
（下段後列左から）宮島　麻美/ 高橋　元/ 廣田　啓一
（下段前列左から）西田　祥子/ 橋本　順子

秘密計算技術は，流通や金融，医療ヘルスケアなどさまざまな分野のデータ利活用への展開が期待されます．さまざまなパートナーの皆様と連携して，実社会への適用に向けた取り組みを進めていきます．

◆問い合わせ先
NTTセキュアプラットフォーム研究所
データセキュリティプロジェクト
E-mail　seg-product-p-ml＠hco.ntt.co.jp

耐量子暗号技術の研究動向

量子計算機の実現が近いとの観測が広まり耐量子暗号の研究が活発になっています．本稿では，耐量子暗号（ポスト量子暗号：Post-Quantum Cryptography）の研究開発の中心的役割を担っている米国国立標準技術研究所（NIST）の耐量子暗号標準化プロジェクトと，それに対するNTTの取り組みおよび独自研究を紹介します．

草川 恵太（くさがわ けいた）
NTTセキュアプラットフォーム研究所

耐量子暗号技術

現在のインターネット上では，プライバシ情報やクレジットカード番号等の機密性の高い情報が多くやり取りされています．通信内容を秘匿するためには，共通鍵暗号や公開鍵暗号が使われています．相手先や送信内容の真正性を確認するために，電子署名やメッセージ認証符号（MAC）といった認証技術が使われています．公開鍵暗号やデジタル署名の中でも現在広く使われているのが，素因数分解問題の困難性に基づく暗号アルゴリズム（RSA暗号，RSA署名など）や離散対数問題の困難性に基づく暗号アルゴリズム（Diffie-Hellman鍵交換，楕円曲線Diffie-Hellman鍵共有，DSAなど）です．

1994年，Peter Williston Shor氏はこの2つの問題を効率良く解く量子コンピュータ用のアルゴリズムを提案しました．大規模かつ安定して計算が行えるような量子コンピュータが完成すると，現在広く用いられている暗号アルゴリズムは安全でなくなります．そのため，量子コンピュータが完成する前に，量子コンピュータを用いても解読や偽造ができないような暗号技術の研究・開発・標準化が盛んになっています．公開鍵暗号技術の中でも，量子コンピュータが苦手とすると考えられている問題を基に暗号アルゴリズムが設計されているものを，耐量子公開鍵暗号技術と呼びます．

耐量子暗号技術の標準化動向

耐量子暗号技術への移行を検討する必要があるかどうかについては，Michele Mosca氏提案の計算式が参考になります．

- x＝今後生成される情報の安全性を保ちたい年数
- y＝耐量子暗号アルゴリズムへの移行（研究開発，標準化，普及）に必要な年数
- z＝大規模量子コンピュータが完成するまでの年数

x＋y＞zであれば，y年後に「x年間安全性を保ちたい」と思って暗号化した暗号文は，x年未満に量子コンピュータによって破られる可能性があります．したがって，現時点でx＋y＞zだと考えられるのであれば，耐量子暗号技術の標準化や耐量子暗号技術への移行を真剣に検討する必要があります．

昨今の量子コンピュータの開発状況からzが現実的な年数になるのではないかと考えられており，各国のいろいろな組織や標準化団体が移行の検討を進めています．

- 日本のCRYPTREC（Cryptography Research and Evaluation Committees）*は，2014年ごろに「格子問題等の困難性に関する調査」として耐量子暗号技術の調査報告を行っています．
- 米国国立標準技術研究所（NIST）は，2015年春ごろからワークショップを開催し始め，2016年には耐量子公開鍵暗号技術の標準化活動を行うことを宣言しました．
- 米国国家安全保障局（NSA）は，2015年8月，機密情報の保護のために用いる暗号アルゴリズムのリストSuite Bについて，耐量子暗号技術への移行が将来的に行われることを表明しました．
- 欧州電気通信標準化機構（ETSI）は2013年ごろから量子暗号と耐量子暗号技術のワークショップを毎年開催しています．
- 国際標準化機構（ISO）と国際電

＊CRYPTREC：電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクト．

気標準会議（IEC）は2015年ごろから耐量子暗号技術に関する議論の時間を設けています．

・IETFでも，耐量子署名のプロジェクトが進んでおり，RFCとして公開され始めています（RFC8391: XMSS: eXtended Merkle Signature Schemeなど）．

これらの動きの中でも世界の暗号技術標準に強い影響力を持つNISTの耐量子暗号技術標準化プロジェクトを紹介します．

NISTの耐量子暗号技術標準化プロジェクト

NISTの耐量子暗号技術標準化プロジェクトは2016年ごろから本格的に開始しました．デジタル署名，公開鍵暗号，鍵共有の3つのカテゴリの暗号アルゴリズムを選定し標準化するためのプロジェクトです．NISTのスケジュールは以下のとおりです（**図**）．

・2016年2月：耐量子暗号技術標準化開始の宣言
・2016年8月：NISTIR 8105『Report on Post-Quantum Cryptography』の発行
・2016年8月：募集要項および選定基準についてのコメント募集
・2016年12月：受付開始
・2017年11月：受付締切
・2017年12月：書類および形式審査を行い，Round 1の開始
・2018年4月：第1回耐量子暗号技術標準化会議
・2018～2019年：Round 2の開始
・2019年8月：第2回耐量子暗号技術標準化会議の予定
・2020～2021年：Round 3の開始またはアルゴリズム選定
・2022～2024年：ドラフト準備完了

2017年11月締切時点では82の投稿があり，署名の提案が23件，暗号化・鍵共有の提案が59件でした．その後，1カ月ほど書類や形式の審査を行い，2017年12月にRound 1が開始されました．このとき，69件が残りました．のちに5件取り下げがあり，現時点では64件が残っています．署名の提案が19件，暗号化・鍵共有の提案が45件残っています．

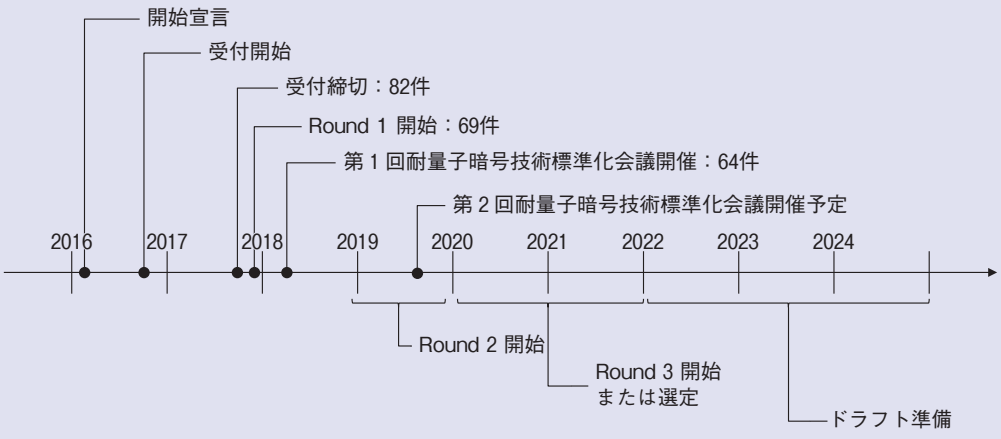


図　タイムライン

すでに書いたとおり，書類および形式を審査した結果がRound 1の候補である69件です．

そのため，Round 1に進んだからといって，安全であるとは限りません．

Round 1の候補が公開された直後から，NISTのpqcメーリングリストにおいて，各方式の安全性について激しい議論が交わされました．

その中でも，以下のように実際に破れることが示された例が多数あります．

・Guess Again（その他・暗号）
・RaCoSS（符号・署名）
・RVB（その他・暗号）→取り下げ
・HK17（その他・暗号）→取り下げ
・CFPKM（多変数多項式・暗号）
・SRTPI（多変数多項式・暗号）→取り下げ
・Edon-K（符号・暗号）→取り下げ
・Comact LWE（格子・暗号）
・WalnutDSA（その他・暗号）
・RankSign（符号・署名）→取り下げ

今後も，Round 2に進むまでに安全性評価手法が改良されることが想定されるため，注視が必要です．

NTTの取り組み

NTTでは，NISTの耐量子暗号標準化活動には独自のアルゴリズムを提出していません．

しかし，安全性強化手法の提案や第三者的立場での安全性評価というかたちで参加し，適切なアルゴリズムが選ばれるよう協力しています．

またNISTの耐量子暗号標準化は耐量子公開鍵暗号技術のみを対象にしていますが，NTTでは独自に耐量子共通鍵暗号技術についても研究を進めています．

■安全性強化手法

実際の通信状況下で安全な暗号通信を行う場合，公開鍵暗号はメッセージを秘匿するだけでなく，メッセージの改ざんを防止する等のより強い安全性が必要です．専門的には，これをCCA安全性と呼びます．現在では，CCA安全性を持つことが現実に使用する公開鍵暗号のための必須の条件とされています．

CCA安全性を持たない公開鍵暗号をCCA安全性を持つ公開鍵暗号へと強化する手法は古くから研究されてきましたが，2010年ごろからこれらの手法が量子コンピュータを利用した攻撃に対しても安全であるかどうかが研究され始めました．

その結果，これらの手法は効率性を落とせば，量子コンピュータに対しても有効であることが証明されました．

しかし，効率性を犠牲にしないで量子コンピュータに対しても有効であるような安全性強化手法は知られていませんでした．

そこでNTTでは，CCA安全性を持たない耐量子公開鍵暗号を，CCA安全性を持つ耐量子公開鍵暗号へ変換し，安全性を強化する新たな手法を開発しました[(1)]．

これにより，世界最高水準の耐量子公開鍵暗号方式を高効率に構成できます．また，今回の手法は汎用性が高く，さまざまな既存の耐量子公開鍵暗号に対しても適用可能です．NIST標準化候補暗号方式でも，少なくとも7件に適用可能であることが分かっています．

この技術に基づく耐量子公開鍵暗号を用いることで，量子コンピュータ実現後の時代においても，既存方法と同程度の負荷で暗号通信が可能になります．

■外部からの安全性評価

69候補の中にGiophantusという暗号アルゴリズムがあります．

これは，もともとはIECという名前で論文発表されていました．IECも安全性証明を持っており，ある問題が難しいということに安全性が依拠しています．また，ある問題が難しいというためには問題のパラメータが大きいことが必要となります．しかし，IECは鍵サイズや暗号文長が短くなるように設計されていたため，基にしている問

題も相当パラメータが小さいことが課題になっていました．

私たちは，さらに小さなパラメータの問題を解いた場合でも安全性が破れるような新しい攻撃手法を考案しました[(2)]．今回の攻撃手法を用いて解読実験を行った結果，デスクトップPCでも30～40秒程度で解読が行えることが分かりました．今回の研究の結果，NISTへの投稿版であるGiophantusではパラメータが大幅に設定し直されています．

■耐量子共通鍵暗号技術

⑴　安全性評価手法

共通鍵暗号に対する汎用的な量子アルゴリズムは今のところ知られていません．そのため，データベース探索に用いるGroverのアルゴリズムを適用した攻撃が，最良のものとして知られています．そこで共通鍵暗号の内部まで詳しく解析することで，Groverアルゴリズムを超えるような量子攻撃手法を考案し，安全性評価を行っています．NTTでは，中間者一致攻撃と量子アルゴリズムを組み合わせることで，世界初の成果や既存の研究よりも優れた成果を得ることに成功しています[(3), (4)]．

また，一部の共通鍵暗号やMACについては，攻撃者が暗号化アルゴリズムやMACアルゴリズムに量子的にアクセスできる場合に安全性が破れてしまうことが知られています．NTTでもそのような攻撃を研究し，一部の共通鍵暗号を量子関連鍵攻撃で破れることを示しています[(5)]．

⑵　安全性証明手法

前述のとおり，共通鍵暗号技術が，量子的にアクセスするような攻撃者を考えても安全かどうかを判定・証明することは非常に重要です．NTTでは，量子クエリができる攻撃者を考えたときであっても，ハッシュ関数の耐量子安全性を証明する技法を開発しています[(6)]．

今後の展開

安全性強化手法や安全性評価手法を取りそろえ，量子コンピュータの完成後も安心・安全な暗号通信技術の開発・実用化に向けた検討を進めていく予定です．

■参考文献

⑴ T. Saito, K. Xagawa, and T. Yamakawa：“Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model,” EUROCRYPT 2018 Part III, LNCS, Vol.10822, pp.520-551, 2018.

⑵ K. Xagawa：“Practical Cryptanalysis of a Public-key Encryption Scheme Based on Non-linear Indeterminate Equations at SAC 2017,” PQCrypto 2018, LNCS, Vol.10786, pp.142-161, 2018.

⑶ A. Hosoyamada and Y. Sasaki：“Cryptanalysis Against Symmetric-Key Schemes with Online Classical Queries and Offline Quantum Computations,” CT-RSA 2018, LNCS, Vol.10808, pp.198-218, 2018.

⑷ A. Hosoyamada and Y. Sasaki：“Quantum Demiric-Selçuk Meet-in-the-Middle Attacks: Applications to 6-Round Generic Feistel Constructions,” SCN 2018, LNCS, Vol.11035, pp.386-403, 2018.

⑸ A. Hosoyamada and K. Aoki：“On Quantum Related-Key Attacks on Iterated Even-Mansour Ciphers,” IWSEC 2017, LNCS, Vol.10418, pp.3-18, 2017.

⑹ A. Hosoyamada and K. Yasuda：“Building Quantum-One-Way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions,” Asiacrypt 2018 Part I, LNCS, Vol.11272, pp.275-304, 2018.

草川 恵太

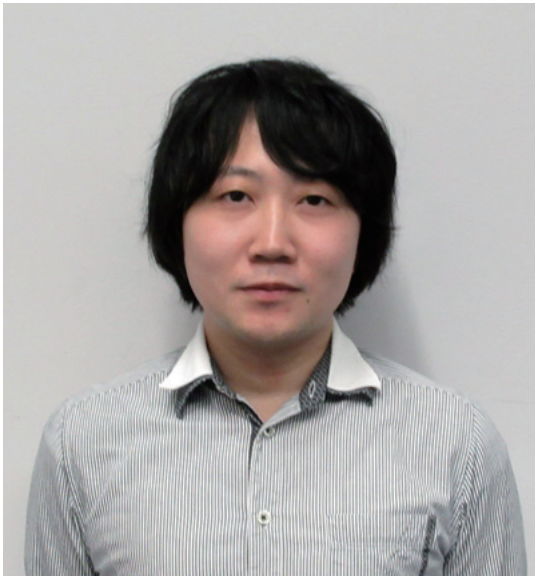
NTTセキュアプラットフォーム研究所では，暗号技術の研究開発を通じて，安心・安全なサービスの実現をめざします．

◆問い合わせ先

NTTセキュアプラットフォーム研究所
データセキュリティプロジェクト
セキュリティ基盤研究グループ
TEL　0422-59-3321
FAX　0422-59-4015
E-mail　keita.xagawa.zv@hco.ntt.co.jp

主役登場

サイバー攻撃の先を行くために



渡邉　卓弥
NTTセキュアプラットフォーム研究所
社員

私の頭の中にある一番古い記憶は，幼稚園のときに大流行していたゲームで家族と対戦する光景です．小さな子どもがゲームで遊ぶことは当時すでに珍しくなく，友人の家にもコントローラーを持ち寄りよく遊んだことを覚えています．私はその中でもとにかく「やりこむ」タイプで，自分より強い相手を探しては，勝つまで執念深く対策を重ねていました．この姿勢は年月を経ても変わらず，解決しがたい問題に直面するたび，寝ても覚めても研究のことを考えてしまいます．「相手を上回るように，行動を予測して戦略を練る」．サイバーセキュリティと対戦ゲームはとてもよく似ています．これは数あるコンピュータサイエンス分野の中でも，打ち負かすべき相手と対峙するサイバーセキュリティだけが持つ特別な性質であり，私がやりがいを持って研究に臨める大きな理由だと考えています．

サイバー攻撃がときに会社業績や人命にまで影響を及ぼす以上，私たちは相手を上回るためのより良い方法論を考え詰め，実行しなくてはなりません．一度発生した攻撃を二度と受けないようにすることも非常に大切です．NTTでは，改ざんサイトを巡回し挙動を記録するハニーポットや，マルウェア感染端末を解析するフォレンジックなどによって攻撃の特徴をとらえることで，防御のためのインテリジェンスを創出しています．しかし，皆様にとって究極の理想は，攻撃が一度も発生せずに通用しなくなることではないでしょうか．このような思いから，私たちは攻撃者の視点に立ち新たな脅威を実証するというアプローチによって，サイバー攻撃に先回りして対策を講じる「脅威実証研究」を立ち上げました．

脅威実証研究の難しさの１つに，プログラムの欠陥を闇雲に探していてはきりがないという点があります．私たちは特定のプログラムのバグだけではなく，一般的な機能に潜在する問題を見つけ出すことで，影響範囲の広い脅威からユーザを保護することをめざしています．もう１つの難しさは，発見した脅威を隠しておけば気付かないうちに攻撃が発生する可能性があり，公開すれば悪意ある人物に模倣されるかもしれないというジレンマです．私たちは，情報を一般公開する前に事業会社や公的機関と連携することであらかじめ対策を施し，適切なタイミングになったらマスメディアなどを介して広く周知し，多くの方が脅威と対策を認識できるよう心掛けています．

脅威実証研究は，世界的なトレンドにもなりつつあります．2018年の初頭に業界を騒がせたSpectreやMeltdown，そして私たちが発見したSilhouette．いずれも研究者が発見した脅威でありながら，製品やサービスに新たなセキュリティ機構を組み込ませ，早期に攻撃の芽を摘み取ることに成功しました．私はこの取り組みに強い手ごたえを感じていますが，脅威の発見が研究者の経験や技量に依存するという課題もあります．今後，私たちは新しい脅威を発見し対策するための属人的でない研究サイクルを模索し，安全なインターネット環境を持続的に提供できるよう努めていきます．