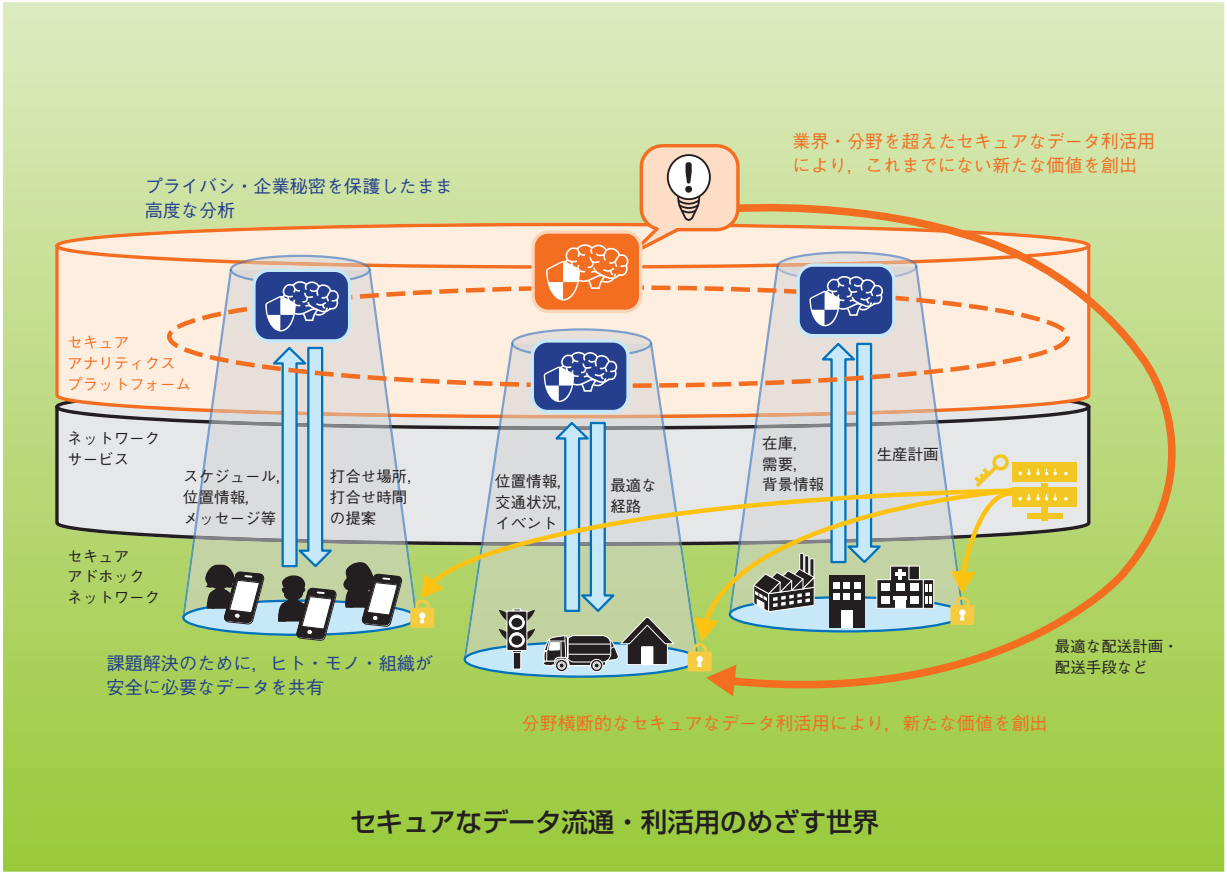
特　集

新しいValueの創出 セキュリティR&D

データ利活用　多者間鍵共有　秘密計算AI　アラートトリアージ　高機能暗号

本特集では，ICTのさらなる普及・発展によってもたらされるさまざまな恩恵によって実現されるスマートな世界をより安心・安全なものにしていくために必要となるセキュリティR&Dについて，NTTセキュアプラットフォーム研究所の取り組みを紹介する．



セキュアなデータ流通・利活用のめざす世界

に資する

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」

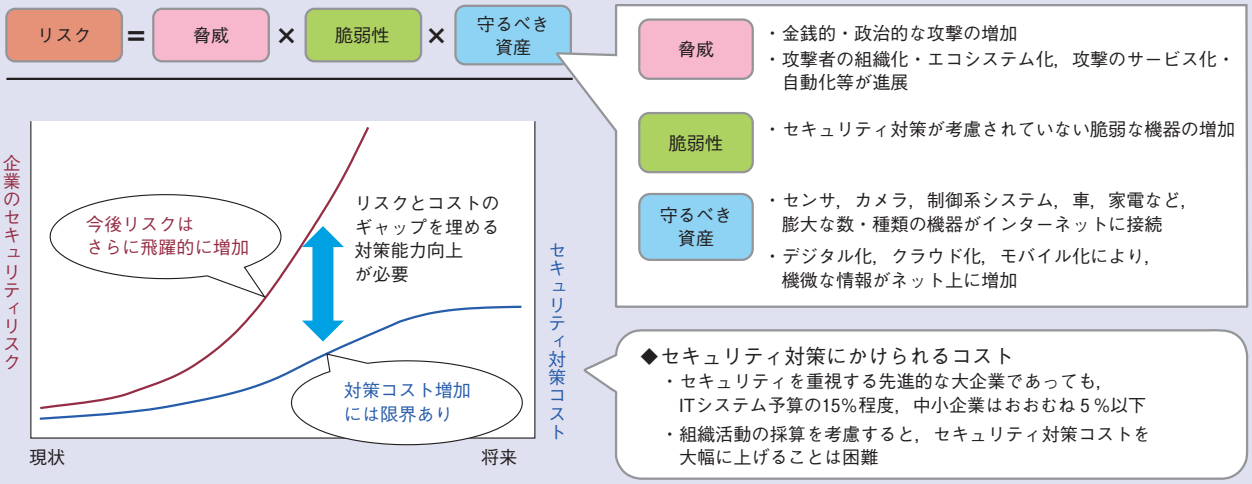


図1　企業のセキュリティリスクと対策コスト

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

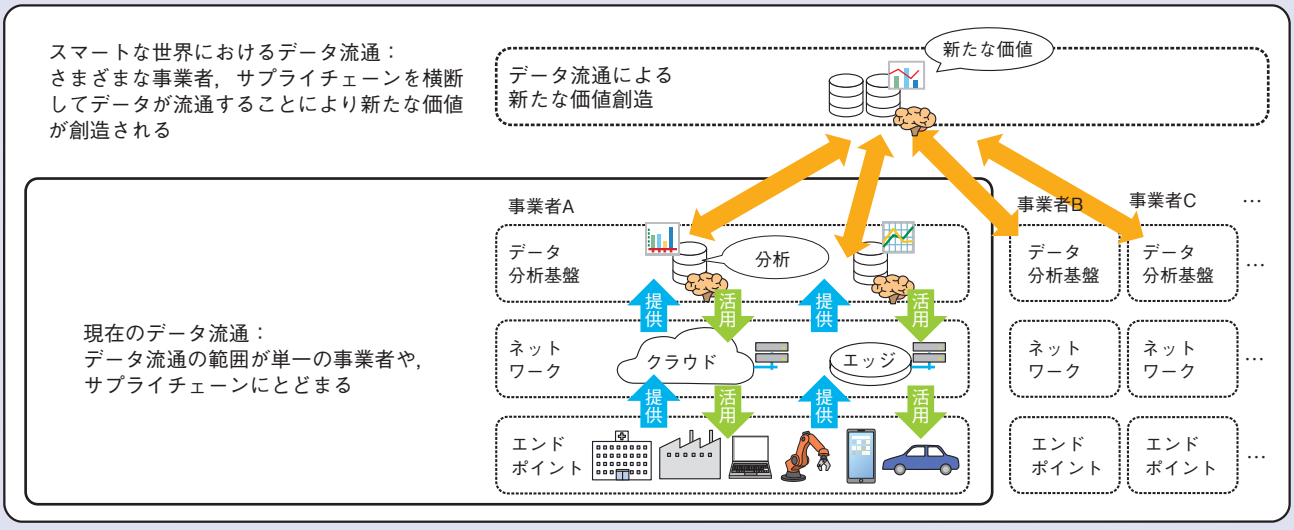


図 2　スマートな世界におけるデータ流通

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

データ流通の将来像とそのセキュリティ技術

デジタルトランスフォーメーション（DX）の加速によりデータの価値は以前にも増して高まるとともに，セキュリティのリスクやプライバシに関する懸念が高まりつつあります．NTTセキュアプラットフォーム研究所では，この課題を暗号技術で解決し，個人・組織が所有するデータを目的に合わせて必要最小限で提供し，課題解決につなげる世界をつくっていきたいと考えています．本稿では，このような世界における安全なデータ流通を支えるNTT研究所の具体的な取り組みを紹介します．

みやざわ としゆき ふくなが としのり
宮澤 俊之 /福永 利徳
たかはし げん きくち りょう
高橋 元 /菊池 亮
たかはし せいじ はせがわ さとし
高橋 誠治 /長谷川 聡
NTTセキュアプラットフォーム研究所

データ流通の将来像

近年，さまざまな分野でデジタルトランスフォーメーション（DX）の加速により，企業や組織のヒト・モノ・プロセスなどのデータ化が進み，高度な分析処理により価値創造や業務効率化などの課題解決につながることが期待されています．これに伴いデータの価値が高まる一方で，セキュリティのリスクやプライバシの懸念も増しています．

企業活動のグローバル化やクラウド・IoT（Internet of Things）の普及によって，多種・多様なエンティティ（人・端末・組織など）が相互接続し，さまざまなデータの授受や共有が進むにつれ，企業や個人にかかわるデータの窃取・漏洩のリスクは高まっています．また，DXにおいて重要な役割を果たすAI（人工知能）や機械学習において個人情報や企業情報の利活用するためには法的な制約やプライバシ等に関する懸念があります．

このようなリスクや懸念を払拭するために，NTTセキュアプラットフォーム研究所では暗号技術を使って，個人・組織のモノ・ヒトに関するデータが目的に合わせて安全に相互流通し，課題解決につなげる世界を実現していきたいと考えています（図1）．本稿では，このような安全なデータ流通を支える技術として，あらゆる通信をエ

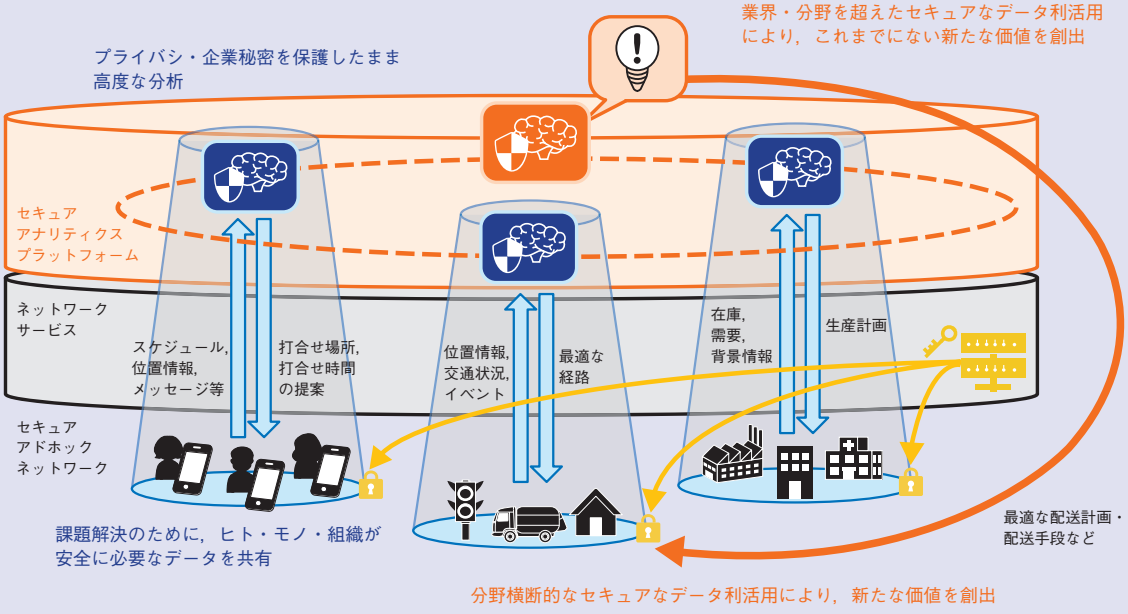


図1　セキュアなデータ流通・利活用のめざす世界

ンド・ツー・エンドで保護する「データの暗号化とその関連技術」，企業秘密やプライバシを保護しながら高度な統合分析を可能とする「秘密計算AI」，個人を特定できないようにパーソナルデータを加工し，これらの情報の利活用を促す「匿名加工技術」について説明します．

データの暗号化とその関連技術

データ流通で行われる重要なデータの授受や共有は，それを行う複数のエンティティの間でのみでき，それ以外には一切情報が漏れないことが重要です．特に最近では，サービス提供者からの情報漏洩リスクも考慮し，データ流通サービスを提供する企業やそのシステム管理者に対してさえもデータを秘匿したいというニーズが高まっています．これを実現するために，信頼するエンティティ間で暗号の秘密鍵を共有し，授受や共有するデータをその秘密鍵で暗号化すること，またそのうえで共有データを検索できることが好ましいですが，大きな技術課題が2つあります．

1番目の課題は，複数エンティティでの効率的な鍵の共有です．データ流通サービスでは，多くエンティティでの鍵の共有が必要ですが，多くのシステムで使われている2者間で鍵を共有するプロトコルを繰り返し実行することは大変非効率で非現実的です．

これに対しNTTでは，サービス提供者が設置する鍵仲介サーバを介して複数のエンティティ間で効率的に鍵の共有ができる技術の研究に取り組んでいます．このとき，鍵仲介サーバでは共有される鍵が復元できないことが原理的に保証されています．現在では，エンティティの数によらずに一定の時間で効率的に鍵の共有ができる方式を発明しています．これにより「その時点で通信にかかわる任意の数のエンティティのみによる，情報流通サービス提供者からも秘匿されたデータの授受・共有」が実現されます．

2番目の課題は，暗号化された共有データのデータ流通サービス提供者の計算機資源を用いた検索です．データ流通サービスはクラウド型で提供されるケースが多く想定されるため，共有データの検索をデータ流通サービス提供者の計算機資源を用いて行うことが望ましいですが，検索のために暗号化データを復号してしまうと，サービス提供者へのデータ秘匿ができません．そこでNTTでは，データとは別に検索インデックスを暗号化し，それを暗号化したまま検索することでこれを実現する方法を研究しています．上述したとおり，共有データはエンティティの追加や削除のたびに頻繁に再暗号化されるため，処理が複雑になるのですが，これを効率的に行う方式を考案しています．

上述した2つの技術の関連技術として，エンティティの追加や削除のたびに，共有する鍵の更新や，それに伴い暗号化された共有データを復号せずに新しい鍵で再暗号化を効率的に行う技術も考案しています．これらの技術を組み合わせ，サービス提供者に対してもデータの内容を漏らさない，電話・チャットなどのコミュニケーションサービスをすでに商用化しています[(1)]．

秘密計算AI

通常，データを利活用するためには，通信時や保管時に暗号化していたとしても，処理を行う際には元データに戻して処理する必要があります．このことは，データ所有者からすると情報漏洩のリスクを感じることから，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に抵抗感を持つユーザや組織が少なくありません．特に所有者から他者，または同一組織内であっても，データを提供して積極的に利活用したい場合には，このことは大きな障害だと考えられます．

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処理ができる秘密計算技術の研究開発を世界に先駆けて取り組んでいます．NTTが取り組む秘密計算技術は，ISO国際標準である秘密分散技術を利用して暗号化されたデータを，一度も元データに戻さずに分析を行うため，企業の秘密情報や個人のプライバシにかかわる情報などの情報を安全に，安心して提供し利活用できる社会の実現に貢献すると期待されています．これまでに，統計分析を行う秘密計算技術は実用段階に達しています．

現在，NTTではさらに高度な分析ができる秘密計算技術の研究開発を進めており，最近では，AIの中でも活用が進み始めているディープラーニングの標準的なアルゴリズムを，暗号化したまま一度も元データに戻さずに処理できる技術を世界で初めて実現しました[(2)]．これは，ディープラーニングでのデータ活用に必要な①データ提

供，②データの保管，③学習処理，④予測処理，のすべてのステップを暗号化した状態で行うことができることを意味します（**図2**）．この技術によって，AIを用いてデータ活用する際に，データ所有者が安心してデータを提供でき，データの量や種類の増加や，これに伴う精度向上・高度分析の実現につながると考えています．例えば個人の位置情報やスケジュールを暗号化したまま，天気や企業のイベント情報などと併せて学習することで，最適な飲食店の仕入れや人員リソースの配備を予測することや，レントゲン写真，MRI，CTスキャン，顕微鏡写真などの医療データを秘匿しつつ学習し，検査結果に悪性腫瘍があるかなどを高速かつ精度良く判定することが可能になると期待されます．

今後はAIの知見を持つパートナーと連携して実証実験等を行うことで，秘密計算を使ったディープラーニングの効果を実証していきたいと考えています．

匿名加工技術

近年，パーソナルデータの利活用に注目が集まり，市場が本格的に活性化しようとしています．NTTでは，パーソナルデータの安全な利活用を促すデータ加工技術の研究を進めています．

2017年施行の改正個人情報保護法によって，個人情報を特定の個人を識別することができないように加工し，当該個人情報を復元できないようにした「匿名加工情報」は，本人の同意なしでも目的外利用，第三者提供が可能となりました．例えば，小売事業者が持つ購買履歴データを匿名加工情報にすることで，製造事業者が消費者属性と購買傾向に基づいた新製品開発を行うことができます．

匿名加工では，匿名性だけを高めようとすると，元のデータの特徴が大幅に損なわれ有用性の低いデータとなってしまいます．そのため，データ保有者の個人識別のリスクを低減したいというニーズと，データ活用者の元データの特徴が保持されたデータを入手したいというニーズの両方を満たす最適な匿名加工が必要となります．NTTは，匿名性と有用性のバランスの取れた匿名加工情報の作成を支援する「匿名加工情報作成ソフトウェア」を開発しました．本ソフトウェアは2018年よりNTTテクノクロスから提供可能となっており，医療・金融分野を中心に市場展開が進められています．

本ソフトウェアは，個人情報保護委員会が規定した匿名加工情報の加工基準1号～5号に対応するための多彩な匿名化技法，評価技法を備えています．特徴的な技法としては，撹乱的な手法によりデータの粒度を変えず高い有用性を確保するNTT独自の匿名化技法であるPk-匿名化を備えています．従来技術であるk-匿名化は「33歳」を「30代」，「東京都千代田区」を「東京都」にするなど，データを抽象化することによってk-匿名性*を担保する手法ですが，情報損失が課題の1つでした．これに対し，データを撹乱させるPk-匿名化を導入することにより情報損失がなく，より正確で幅広い分析が可能となります（**図3**）．

NTTは，データがより活発に利活用される世界の実現をめざし，個人識別のリスクを低減する研究だけでなく，個人の属性の推測リスクを低減する研究にも取り組んでいます．データ利活用において統計情報のような計算結果を用いる場合，例えば2人分のテストの平均点を用いると，1人分の点数を知る人はもう1人分の点数を推測できてしまうという問題があります．このような計算結果に対するプラ

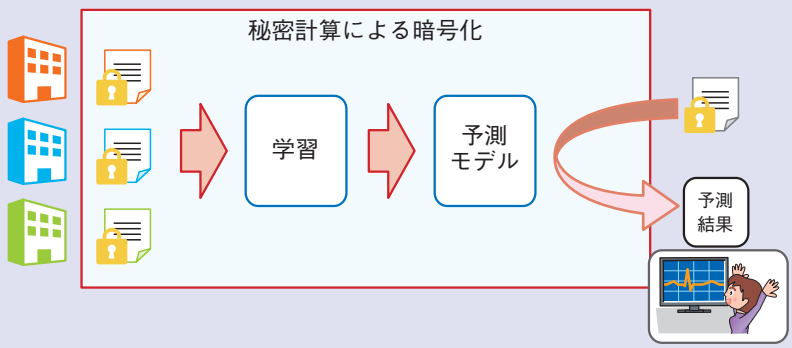


図2　秘密計算AI

＊k-匿名性：加工後のデータから対応する個人を1/k以上の確率で識別できない特性．

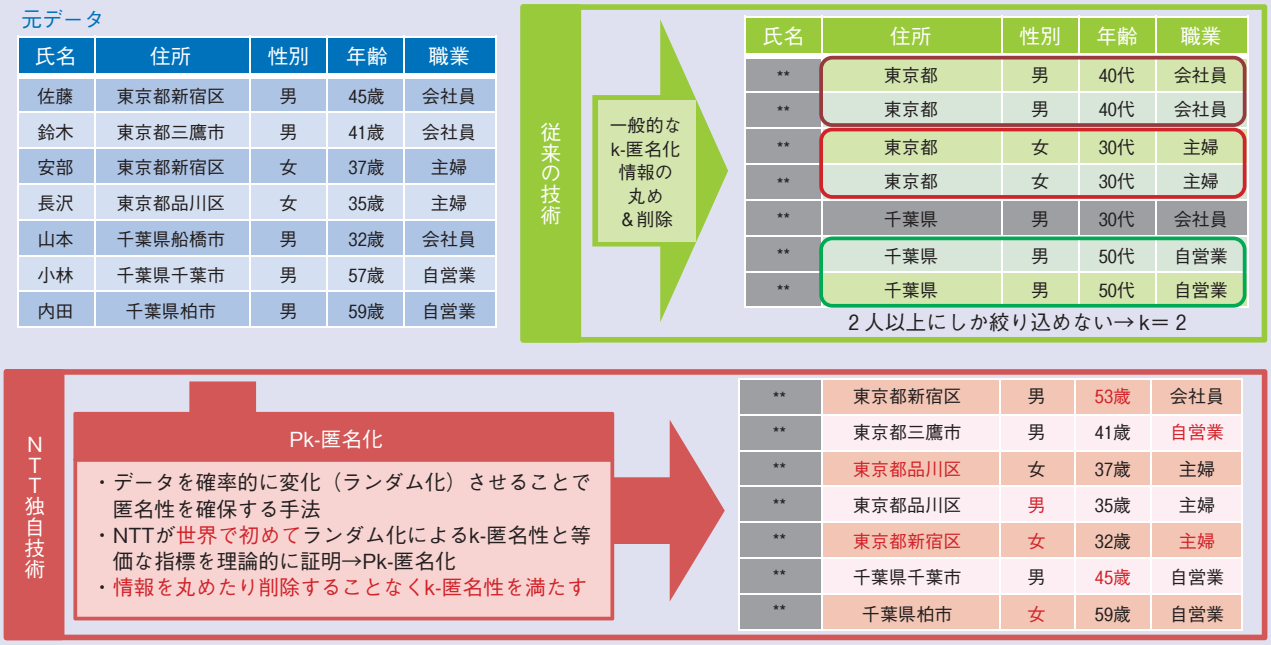


図3　Pk-匿名化の概要

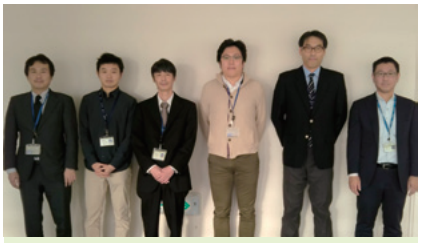
イバシは，出力プライバシと呼ばれ統計分野で広く研究が行われており，NTTでは特に，データ分析技術として有望な機械学習の出力プライバシに注目し，リスク分析技術，保護技術の研究を進めています．

今後に向けて

冒頭で紹介した安全なデータ流通を実現するために，NTTでは本稿で紹介した技術以外にもさまざまな暗号技術の設計・開発に取り組んでいます．例えば，研究開発が加速している量子計算機の実現を見据えた暗号方式の開発やその安全性評価や，プログラムの処理内容を暗号学的に解析不可能にし，安全なプログラムの流通を可能とする暗号学的プログラム難読化などがその一例です[3]．暗号理論・技術の専門性を基に，NTTグループのお客さまや社会的課題の解決に貢献すべく，データセキュリティの研究開発に取り組んでいきます．

■参考文献

⑴ 吉田・岡野・奥山・小林：“サーバからの漏洩・盗聴を防ぐ暗号ビジネスチャット”，NTT技術ジャーナル，Vol.29，No.2，pp.18-22，2017.
⑵ https://www.ntt.co.jp/news2019/1909/190902a.html
⑶ 草川：“耐量子暗号技術の研究動向，”NTT技術ジャーナル，Vol.31，No.2，pp.23-26，2019.



（左から）宮澤　俊之／長谷川　聡／
高橋　誠治／菊池　亮／
福永　利徳／高橋　元

私たちは，最先端の暗号理論研究から次世代の暗号通信・システム方式の研究まで幅広くデータセキュリティの研究に取り組んでいます．増加するデータの安全性を確保しつつ，活用可能とする技術の実現によって新ビジネスの創出と課題解決に貢献していきます．

◆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
E-mail　scpflab@hco.ntt.co.jp

攻撃の痕跡に着目するサイバー攻撃対策の最前線

岩村 誠 /鐘本 楊
黒米 祐馬 /青木 一史
川古谷 裕平 /折原 慎吾
三好 潤
NTTセキュアプラットフォーム研究所

近年のサイバー攻撃は，巧みに標的を騙すことでマルウェアを企業網内に潜り込ませる傾向が強まっており，感染を未然に防ぎ切ることが困難になりつつあります．一方，外部に公開しているWebサーバなどに対しては，攻撃手法がよく知られるにつれ，攻撃頻度が上昇してアラートが多発し，どれから対処すべきか判断に困るようになりつつあります．本稿では，このような状況に打ち勝つための，攻撃時に残される痕跡に着目したサイバー攻撃対策の最前線の取り組みを紹介します．

エンドポイント防御の現状

企業をねらうサイバー攻撃や，そこで用いられるマルウェア（悪性なソフトウェア）は日々高度化しており，未然に攻撃の侵入を防ぐことが難しくなってきています．そうした中，マルウェアによる侵入を許してしまうことは前提とし，侵入後の対処を考慮したEDR（Endpoint Detection and Response）と呼ばれる技術が注目を集めています．

従来のセキュリティ製品は，マルウェアが実行される前にその外見上の特徴（マルウェアの実行ファイルに含まれるパターン等）をルールとして検知することで感染を未然に防いでいました．しかし，昨今のサイバー攻撃では，その外見上の特徴を変化させ，セキュリティ製品による検知を逃れるマルウェアが用いられるようになってきました．マルウェアの外見上の特徴は，比較的簡単に変化させることが可能です．一方で，感染後の振る舞いはマルウェアが行いたいことと密接に関係しており，外見上の特徴と比較して変化させることが難しいと考えられています．現在注目を集めているEDRは，マルウェアが動き出した後の振る舞いや，それらが残す痕跡を検出することで，こうしたサイバー攻撃に対抗しようとしています．

マルウェアに感染した際に残る痕跡を検出するルールはIOC（Indicator Of Compromise）と呼ばれ，EDR製品によっては利用者が独自につくったIOC（カスタムIOC）によって，マルウェア感染を検知することが可能になっています．以下では，マルウェア感染の痕跡とそれを検出するIOCの生成方法について解説します．

マルウェア感染の痕跡とその検出

ここで，ある端末にマルウェアが感染した際に“mal_a.txt”という名前のファイルが痕跡として残ったとしましょう．この痕跡を検出するには，ファイル名が“mal_a.txt”というIOCを用意すれば良さそうです．ただ，同じマルウェアがほかの端末に感染した際にはファイル名が“mal_b.txt”となる場合，元のIOCでは検出できなくなってしまいます．そこで少し工夫をして，ファイル名が“＊.txt”（＊は任意の文字列）というIOCを用意したとします．すると“mal_a.txt”も“mal_b.txt”も，もしかすると今後出てくるかもしれないほかの痕跡についてもカバーできそうです．ただ，EDRで監視している端末ではマルウェアではない通常のアプリケーションも動いています．もし，ある通常のアプリケーションが“leg.txt”というファイルをつくった場合，“＊.txt”というIOCではそのファイルをマルウェアの痕跡として検出してしまいます．従来技術が着目する外見上の特徴よりは変化しにくくなったとはいえ，IOCにも痕跡の変化に追随できるようにカバー率を上げつつ，誤検出を起こさない表現が求められます．

もう1点，IOCに求められることを考えるにあたって考慮しておくべきことがあります．実際にIOCでマルウェアへの感染が発覚したとしましょう．その後の対策の多くはセキュリティ技術者，つまり人間に委ねられることになります．マルウェアはどういった経路で侵入してきたのか，機密情報を外部に送信していないか，ほかに感染している端末はないか，これらを残されたログなどから解明することになります．時には，IOCが検知したものが何であるかを把握し，検知したIOCを改良してほかの端末を検査する必要性も出てくるでしょう．そのときに必要になるのは，人間が見て解釈しやすいIOCです．ある種の機械学習ではその

検知基準が非常に複雑で，改良することはおろか，理解することすら困難なアルゴリズムも存在します．一連の作業フローの中に人間が存在しているセキュリティの現場では，IOCの解釈性も重要になってきます．

IOCの自動生成

NTTセキュアプラットフォーム研究所では，さまざまな解析妨害機能を持ったマルウェアに対しても，その振る舞いを網羅的に抽出するマルウェア解析技術の研究開発に取り組んでいます．ここで紹介するIOCの自動生成技術[1]は，このマルウェア解析技術により抽出された挙動ログを入力として，高い検出精度とカバー率，解釈性を兼ね備えたIOCの生成を実現しています．具体的には以下の手順によりIOCを生成します（**図1**）．

① マルウェアの収集・選定：IOCによる監視を実施する環境に合わせたマルウェアを収集・選定します．

② マルウェア解析技術により挙動ログを抽出：マルウェア解析専用の仮想環境にてマルウェアを解析し挙動ログを抽出します．これまで培ってきたマルウェア解析技術はここで活用されています．

③ マルウェアの挙動ログから複数の抽象度のIOC候補を生成：IOCの候補となり得るさまざまな抽象度の正規表現を，過去のマルウェア解析ノウハウ等から生成します．

④ 検出精度・解釈の容易さを踏まえた最適なIOCセットの算出：前述のIOC候補について，正規ソフトウェアおよびマルウェアの挙動ログを基に，検出精度・解釈の容易さを踏まえ，各マルウェアファミリに対応する最適なIOCを算出します．

こうして生成されたIOCを市中のEDR製品に対して追加投入することで，これまで発見が難しかったマルウェア感染端末を検知することができるようになります（**図2**）．現在は1週間当り約1万検体を収集・選定し，それらのマルウェアの解析結果から生成したIOCのNTTグループ内への配信を始めています．今後はスクリプト形式など，実行ファイル形式以外のマルウェアへの対応を進めていきます．

公開サーバ防御の現状

続いて，ここからは話題が変わり，外部公開サーバに対するサイバー攻撃対策について解説します．

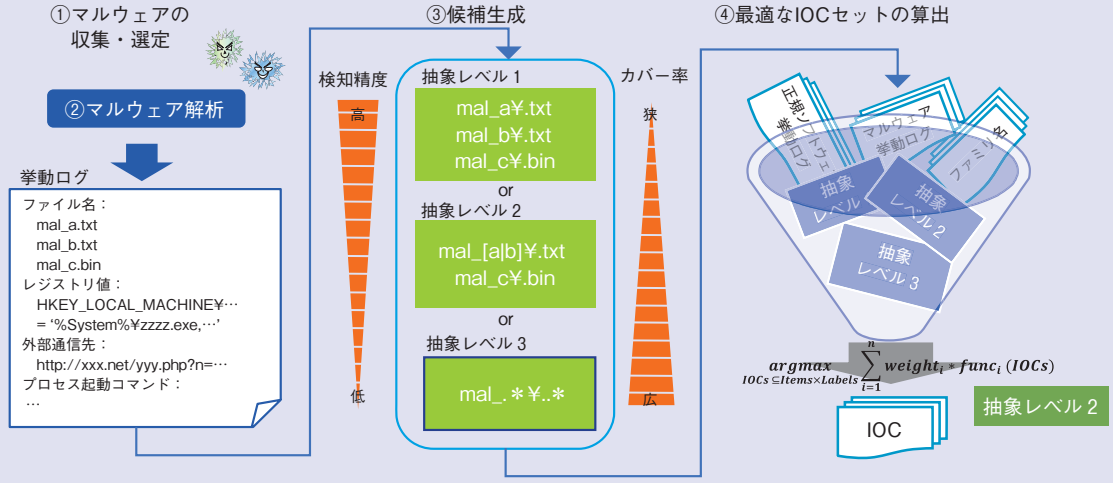


図1　IOC生成手順

図2　カスタムIOCの活用

新たな脆弱性がサーバやアプリケーションで発見されるたび，その脆弱性をねらうサイバー攻撃が発生します．サーバやアプリケーションの脆弱性を悪用するサイバー攻撃は世界で1000万件／日を超える規模となりました．これらの攻撃を検知・遮断するためにIPS（Intrusion Prevention System）*1やWAF（Web Application Firewall）*2といったセキュリティ機器を導入することが一般的となってきています．これらのセキュリティ機器によってすべての攻撃を正しく検知し，遮断できることが理想ですが，現実にはなかなか難しいのです．理由は誤遮断によるサービス品質低下というリスクがあるからです．セキュリティ機器が運用者によって十分にチューニングされていない場合，正常な通信を攻撃として誤って検知して遮断してしまう可能性があります．このリスクゆえに，すべての攻撃を遮断することは運用者によるチューニングがなければ難しいという問題があります．そして，攻撃を遮断するにしても誤検知でないことが確実な一部の限られた攻撃のみであったり，IDS（Intrusion Detection System）*1のように検知のみを行い通知するアラートを人手で対応しているのが実態です．

より効率的なセキュリティオペレーションの必要性

企業や組織でサイバー攻撃の対応にあたるのがCSIRT（Computer Security Incident Response Team）と呼ばれるセキュリティインシデントを専門に対処するチームや，アラートの通知に対応することを専門に行うSOC（Security Operation Center）アナリストです．CSIRTやSOCアナリストは日々，セキュリティ機器から通知されるアラートを基にセキュリティ侵害が発生していないか分析を行います．特にサーバに対する攻撃を検知するWAFやIDSは日々数千・数万のアラートを通知するため，侵害を分析する際はアナリストの知識や経験を基に，より重要なアラートを絞り込んで処理していかなければ発生するアラートの量に到底追いつくことができません．この絞り込みは知識や経験を持った数少ないアナリストのみができることであり，誰しもができることではないため，攻撃が大規模化している現在では完全に人手のみによってすべての攻撃を分析することは現実的ではありません．また，攻撃者もその実状を把握しているため，大量の無意味な攻撃を仕掛けつつ，攻撃の目的を達成する本命となる攻撃はたった一瞬だけ，といった戦術で挑むことも可能です．企業のセキュリティ監視を麻痺させ，CSIRTやSOCアナリストが気付いたときにはすでに時遅しということになってしまいます．そのため，CSIRTやSOCアナリストは常に不利

*1　IPS/IDS：脆弱性を悪用した攻撃からアプリケーションを保護するシステム．IDSは検知のみを行う利用形態を指し，IPSは検知した攻撃を遮断する利用形態を指します．
*2　WAF：IPS/IDSと同様に攻撃からアプリケーションを保護するシステム．Webアプリケーションに特化した検知能力を有します．

な戦いを強いられています．

アラートトリアージ技術

NTTセキュアプラットフォーム研究所では，ネットワーク通信からサーバに対する攻撃の成否を攻撃の痕跡から自動的に判定し，その攻撃に関連付くアラートが優先的に対応すべきものか否かを決めるアラートトリアージ技術[(2),(3)]を開発しました．攻撃の成否に着目してトリアージ（優先度付け）を行う技術は世界初です．この技術により，喫緊の対応が必要な攻撃のみに人手による分析を集中させることができるようになります（**図3**）．

本技術の根幹は次の3つの機能から成ります（**図4**）．

① 攻撃が成功した際に攻撃者がそのサーバに実行したいコードあるいはコマンドを抽出する機能

② 抽出した攻撃コードあるいはコマンドをさまざまなサーバを模擬したエミュレータ内で実行し，IOC と呼ばれる攻撃の痕跡を抽出する機能

③ エミュレータから抽出したIOCが実際の通信に発生しているかを確認し，発生していれば攻撃成功，発生していなければ攻撃失敗と判断する機能

本技術により，アラートが発生した際にそのアラートに対して，攻撃が成功している，攻撃が失敗している，攻撃の成否が不明といった情報を付加することができます（**図5**）．もしア

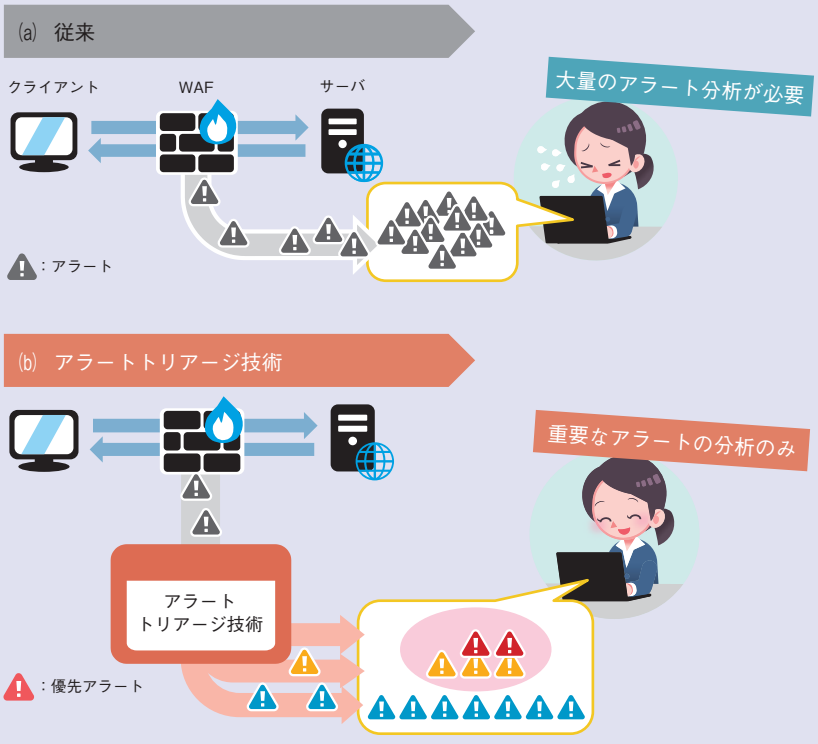


図3　アラートトリアージ技術

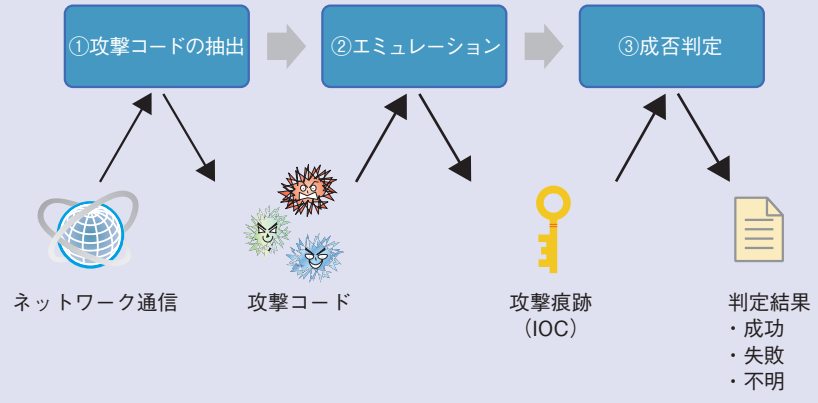


図4　アラートトリアージ技術の仕組み

ラートに攻撃が成功していると情報が付加されている場合，対応優先度は高く，ほかのアラートの確認を後回しにしてでも先にこのアラートを確認すべきです．逆にアラートに攻撃が失敗していると情報が付加されている場合，対応優先度は低く，ほかの攻撃の成否が不明なアラートを先に確認すべきということになります．本技術により優先的に対応すべきアラートが一目瞭然になり，アラート数が大量に増加する大規模なイベントやフォーラム，あるいは攻撃者によるキャンペーンがある場合，アラートトリアージ技術による効果はより顕著に現れると考えています．

実ネットワーク環境を用いた私たちの評価では約52%のアラートを正しく攻撃失敗として判断し，アラートの対応優先度を下げることを実現しました．また，大量のアラートに紛れたわずか0.1%の攻撃成功に関する重要なアラートの優先度を上げることを実現できました．攻撃被害がまだ少ない偵察段階で攻撃が成功していることに気付き，運用者に通知することで攻撃被害が拡大する前に対処を行うことができたという良好な結果を得ることができました．

時刻	アラート内容	送信元	送信先	成否判定※	対応優先度※
2019/12/2 21:38:12	Remote code execution attack detected	x.x.x.x	y.y.y.y	失敗	低
2019/12/2 21:43:03	SQL injection attack detected	x.x.x.x	y.y.y.y	成功	高
2019/12/2 21:43:15	Cross-site scripting attack detected	x.x.x.x	y.y.y.y	不明	中

※本技術により付加される情報

図5　アラートトリアージ技術の効果

今後の展開

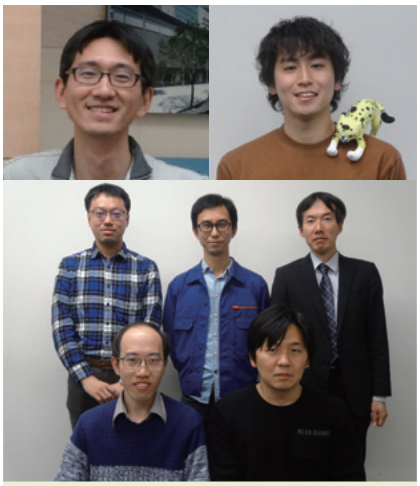
サイバー攻撃を未然に防ぎ切ることは現実的に難しいという現状を踏まえ，本稿では，エンドポイント端末のマルウェア感染や公開サーバへの攻撃の成否を，攻撃時に残される痕跡に着目して判定する技術を紹介しました．今後は，検知後の対応まで自動化する技術の研究に取り組み，ますますの高度化と増加が見込まれるサイバー攻撃に立ち向かっていきます．

■参考文献

⑴ Y. Kurogome, Y. Otsuki, Y. Kawakoya, M. Iwamura, S. Hayashi, T. Mori, and K. Sen: “EIGER: Automated IOC Generation for Accurate and Interpretable Endpoint Malware Detection,” ACSAC 2019, San Juan, U.S.A., Dec. 2019.

⑵ 鐘本・青木・三好・嶋田・高倉：“攻撃コードのエミュレーションに基づくWebアプリケーションに対する攻撃の成否判定手法,” 情処学論, No.60, Vol.3, pp.945-955, 2019.

⑶ Y. Kanemoto, K. Aoki, M. Iwamura, J. Miyoshi, D. Kotani, H. Takakura, and Y. Okabe: “Detecting Successful Attacks from IDS Alerts Based on Emulation of Remote Shellcodes,” Proc. of COMPSAC 2019, Vol.2, pp.471-476, Milwaukee, U.S.A., July 2019.



（上段左から）青木　一史/ 黒米　祐馬
（下段後列左から）折原　慎吾/
川古谷　裕平/
三好　潤
（下段前列左から）鐘本　楊/ 岩村　誠

2020年代を迎え，サイバー攻撃のさらなる激化が予想されます．NTTセキュアプラットフォーム研究所では，攻撃者優位の状況を抜本的に覆すことを目標に最先端の研究開発に取り組んでまいります．

◆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

計算環境の変化に対応する暗号理論研究の最前線

キャッシュカードの偽造事件を契機としてNTTに暗号研究グループが発足してから35年になろうとしています．その流れをくむNTTセキュアプラットフォーム研究所（SC研）では普遍的価値を持つ暗号基礎理論の構築に貢献するとともに，進歩し続ける通信・計算環境の変化に対応した新しい暗号技術の創出に取り組んできました．本稿では発展の著しい量子計算機の出現に備えた暗号技術や情報処理技術に関するSC研の研究活動を紹介します．

阿部 正幸（あべ まさゆき） /徳永 裕己（とくなが ゆうき）
Mehdi Tibouchi /西巻 陵（にしまき りょう）
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

背　景

暗号の安全性は攻撃者がどれくらいの計算資源，すなわちメモリ量や計算速度を持ち得るかによって相対的に評価されます．インターネットが普及し始めた1990年代には RSA暗号の公開鍵は512ビット程度で安全と考えられていました．電子署名法が成立した2001年には1024ビット，2008年から検討されている改定では少なくとも2048ビットが必要とされています．

現在では多くの暗号システムにおいて，より効率的な楕円曲線暗号へ移行しています．さらには，楕円曲線上のペアリング群によってIDベース暗号をはじめとする高機能な公開鍵暗号や，効率的なデジタル署名，非対話ゼロ知識証明が発展しました．暗号は鍵の管理方法によって情報へのアクセスをコントロールする機能を自然に持っています．従来の暗号通信では情報の送り手と受け手が１対１でしたが，クラウドへ暗号化データを保存しておき，送り手が定めた条件を満たす複数の受け手に向けて情報を発信するといった用途に向く高機能な暗号方式が開発されています．

一方，1994年に発表された Shorのアルゴリズムによって，十分な数の量子ビットを十分な精度で扱える汎用のゲート型量子計算機によって現在普及しているRSA暗号やDiffie-Hellman鍵共有などの効率的な公開鍵暗号が破られることが示されました．たとえそのような高度な量子計算機の実現が数十年後になるとしても，その脅威に対して安全な暗号，いわゆる耐量子計算機暗号の開発には量子計算機の実現を待たずに取り組む必要があり，実際に多くの研究開発と標準化が進んでいます．それは暗号システムを提供する者の責任感といった動機だけではなく，次の２つの現実的な理由によります．

まず，新しい暗号方式は開発から普及まで非常に長い時間を要することです．現状動いているようにみえるシステムを互換性のない新たなシステムにアップデートするのは，すべてのユーザが短期間でできることではありません．もう１つの理由は，現在のプライバシが将来の攻撃技術の進展によって毀損されることへの懸念，すなわち長期的な安全性の危殆化です．暗号化された通信であっても，それ自体が傍受・長期保存されて，将来の量子計算機の実現によって内容が暴露される懸念があります．つまり，数十年後に漏洩して困るようなコンテンツにとっては，量子計算機による攻撃は現時点で対応しておかねばならない脅威なのです．また，耐量子計算機暗号は量子計算機上で実行されるのではなく，現在の計算機上で実行されるものです．そのため，現在の計算機環境における実装も含めた安全性が検討される必要があります．

本稿では，まず，量子情報処理技術に関する本研究所での取り組みについて説明します．次に，耐量子計算機暗号に関する最新のトピックを紹介します．最後に，従来の公開鍵暗号の機能拡張の１つである属性ベース暗号について，最新の研究結果を紹介します．

量子情報処理

■SC研における量子情報処理技術

2019年10月，量子コンピュータがついに従来のコンピュータの能力を超える量子超越性を達成したとのニュースが駆けめぐりました．NTTセキュアプラットフォーム研究所（SC研）においても，量子力学の原理で情報処理をする量子コンピュータの研究開発を以前から進めています．

現在までに実現された量子コンピュータはまだ数十量子ビット程度で

あり，規模の拡張性をどのように得ていくかについては，未解決の課題が山積みです．つまり，量子コンピュータをどのようにつくり，どのように拡張性を得ていくかの実装法の研究開発は，現在の暗号の安全性レベルを検証する試金石にもなっています．

また一方で，量子情報処理技術は新たなセキュリティ技術も生み出しています．量子状態は，むやみに観測すると状態を壊してしまう，コピーができないなどの通常のデータとは異なる性質を内在しています．これをうまく活用することにより新たなセキュリティ技術が生み出されます．

■量子コンピュータ開発への道筋

量子コンピュータ実現に向けての一番の障壁はエラーに弱いことです．量子ビットは，現代の主要な情報処理単位であるデジタルデータのようにエラーを小さくすることがそもそも難しいため，少し規模を大きくするとエラーに埋もれて正しい計算が困難になってきます．これを実際に解決する方法は，今までのところ，量子エラー訂正符号しか知られていません．量子エラー訂正符号を用いると，技術的に可能な範囲にある特定の誤り率を下回る制御を達成すれば，符号化された量子状態に載った量子情報の論理的な誤り率を小さくすることが可能となり，エラーに対する規模の拡張性を得られます．

もう１つの課題は量子ビット数自体の規模を拡大することです．個別の量子ビットを精度良く高速に制御しながら規模を大きくしていくことは相反するような技術開発であり，不安定な量子状態に対してこれまであまり行われてきませんでした．精度を保ちつつ，量子ビット数の桁数を上げていく量子物理工学的な技術開発におけるブレークスルーが期待されています．SC研は文部科学省Q-LEAPプロジェクトに参加し，超伝導量子コンピュータの開発に携わっています．量子エラー訂正が可能となるような高度な制御技術と規模の拡大をめざした研究開発に取り組んでいます．

量子セキュアネットワークに向けて

量子情報処理を活用した新たなセキュリティ技術の例が量子暗号（量子鍵配送）です．むやみに観測すると状態を壊すという性質を使うことで盗聴検出が可能となり，原理的に安全な鍵配送が可能になります．しかし，現状の技術の欠点は，損失に弱く通信距離に事実上の制限（100 km程度まで）があること，ネットワーク化する技術がないことです．これを解決する方法が量子中継です．これは高精度に光と物質の量子状態を制御し，損失に耐え得るような量子エラー訂正を行うことに対応します．そのため，実は小～中規模の量子コンピュータをつくるのにほぼ匹敵する技術です．量子中継をめざすためにも，やはり量子コンピュータを実装する研究開発とほぼ同等のことを行っていかなくてはなりません．SC研では，量子中継器に求められる，光と原子の量子状態を精度良く制御し，扱える量子状態の規模を大きくすることをめざした研究に取り組んでいます．

また，科学技術振興機構（JST）のCRESTプロジェクトに参加し，光と原子の相互作用を高精度に行える共振器電気力学を活用した研究開発に取り組んでいます．

耐量子計算機暗号

■安全な実装および標準化への貢献

RSA暗号や楕円曲線暗号といった従来暗号技術のほかに，量子暗号に対する耐久性を持つと思われる耐量子暗号技術は実は数十年も前から研究されています．もっとも基本的な機能である暗号方式と署名方式に関しては，量子計算機に破られにくい問題に基づく理論的な設計方法が昔から知られています．しかし，RSA暗号や楕円曲線暗号に比べて処理速度・通信量などの性能が著しく劣っており，実用性が低いと判断されていたため，耐量子暗号技術の実装はほとんどありませんで

した．

ここ数年，量子計算機の実現が目に見える脅威になってくるにつれ，この脅威がいよいよ真剣に検討され始めました．より高速・高性能の耐量子暗号技術の提案と実装が重要な研究課題となってきました．特に耐量子暗号の有力候補とみなされる「格子暗号」の分野では，強固な安全性根拠を持つ昔からの方式にさまざまな工夫を加え，RSA暗号などに並ぶ性能を達成した新方式が提案・実装されてきました．VPNソフトウェアなどへの実装実験も始まっています[1]．

理論的な安全性根拠が徹底的に検討されている一方，サイドチャネル攻撃やフォールト攻撃などの実装上の脆弱性があまり考慮されていません．また，実装に値する効率的な新方式は「離散ガウス分布の生成」や「棄却サンプリング」など，従来暗号技術に存在しないテクニックに基づいており，実装上の新たな課題になっています．SC研では，これらの実装上の課題に取り組むべく，とりわけ格子署名方式を対象に実装攻撃に対する安全性評価を行い，数多くの脆弱性を発見しました[2]．例えば，格子ベース署名の最速方式として知られているBLISS方式の複数の実装を対象に，署名生成時の電力消費や処理時間を測定することにより，代数学や数論の結果を用いて秘密鍵を完全に復元できることを示しました．このような脆弱性を克服するための対策および新たな実装手法を提案し，その安全性の証明もしています．最高水準の性能を維持したまま，実装攻撃に対する強い安全性を持つ格子ベース署名方式も達成しました[3]．

この一連の研究は，米国標準技術局（NIST）が2016年に立ち上げた現在進行中の耐量子暗号標準化プロセス（NISTコンペ）に大きな影響を及ぼしました．とりわけ，BLISS方式の実装上の脆弱性に関する結果が，提案方式の１つDilithiumなどの設計方針で実装上の脅威として検討されています．その結果により，NISTコンペのほとんどの方式において「離散ガウス分布の生成」が避けられました．なお，NISTコンペ開始後にもDilithiumやFalconの安全な実装に関する成果を得たほか，安全性根拠が薄弱な方式を完全に破り敗退に追い込んだなど，貢献をし続けてきました[4]．

■量子計算機を用いた共通鍵暗号の安全性評価手法

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Groverのアルゴリズムや量子ランダムウォーク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．SC研では，共通鍵暗号の内部まで詳しく解析することで，新たな安全性評価手法を生み出してきました．例えば，NTTコミュニケーション科学基礎研究所と共同で取り組んだハッシュ関数の多重衝突発見問題の改良が挙げられます[5]．

また，将来的に量子計算機を入手できることを見越して，現時点から情報収集・窃取を行っている敵対者も考えられます．このような敵対者の影響を見積もるための安全性評価手法にも取り組んでいます[6]．

■量子計算機を考慮した安全性証明技法

これまでの多くの安全性証明では，敵対者が量子計算機を所持していることを想定していませんでした．そのため，安全性が証明された方式であっても，敵対者が量子計算機を用いて安全性を破ってしまう可能性が残っています．そこで2010年以降，量子計算機を考慮した安全性証明技法が数多く編み出されてきました．SC研でもそのような研究に取り組んでいます．耐量子公開鍵暗号の安全性強化手法[7]や，ハッシュ関数の耐量子安全性[8]，Feistel構造を持つ共通鍵暗号の耐量子安全性[9]，事前計算を許した場合のハッシュ関数への攻撃の一般的な下界評価[10]などがその例です．

属性ベース暗号

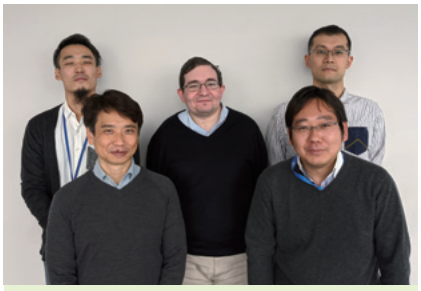
公開鍵暗号の中でも主たるテーマは

いくつかありますが，本稿ではその中の１つである「実用的な効率性を持つ属性ベース暗号の実現」に焦点を絞って紹介します．

公開鍵暗号では情報の送り手は受け手の公開鍵を使って暗号化し，その公開鍵に対応する秘密鍵を持つ受け手のみが情報を復元できる暗号文を生成できています．属性ベース暗号とは，情報の受け手を１人に限定せず，送り手が自由に受け手を指定可能な暗号です．より詳しくいうと，暗号文に受信ポリシーが，秘密鍵に受け手の属性が埋め込まれており，受け手の属性が暗号文の受信ポリシーに合致する場合にのみ受け手は情報を受け取ることができます．このように暗号文と秘密鍵にロジックを埋め込み，きめ細かい情報授受の制限を実現できます．これまでに数多くの属性ベース暗号方式が提案されていますが，実際のシステムに実装することを考えると不十分な点が多くありました．一例としてスケーラビリティが挙げられます．既存の多くの方式は，最初のシステム構築の際に，使用する属性をすべて決める必要があり，以降追加できませんでした．スケーラビリティを考えると，利用できる属性をいつでも追加できるほうが望ましいです．ほかにデータサイズの問題がありました．既存の方式では暗号文のサイズが，埋め込まれるポリシーのサイズや使用する属性の数に比例して大きくなるものがありました．これはストレージを圧迫するので望ましくありませんでした．このように実際に利用するうえでさまざまな性能基準が考えられましたが，そのすべてについて実用上望ましいレベルに達している方式は提案されていませんでした．当グループでは，実用上望ましい性質をすべて兼ね備えた属性ベース暗号を新たに開発しました．

■参考文献

(1) https://github.com/Microsoft/PQCrypto-VPN
(2) T. Espitau, P.-A. Fouque, B. Gerard, and M. Tibouchi：“Side-channel attacks on BLISS lattice-based signatures,” Proc. of ACM CCS 2017, pp.1857-1874, Dallas, U.S.A., May. 2017.
(3) G. Barthe, S. Belaid, T. Espitau, P.-A. Fouque, B. Gregoire, M. Rossi, and M. Tibouchi：“Masking the GLP lattice-based signature scheme at any order,” Proc. of EUROCRYPT 2018, Vol.10821, pp.354-384, 2018.
(4) J. Bootle, M. Tibouchi, and K. Xagawa：“Cryptanalysis of Compact-LWE,” Proc. of CT-RSA 2018, Vol.10808, pp.80-97, 2018.
(5) A. Hosoyamada, Y. Sasaki, S. Tani, and K. Xagawa：“Improved Quantum Multicollision-Finding Algorithm, ” Proc. of PQCrypto 2019, Vol.11505, pp.350-367, 2019.
(6) A. Hosoyamada and Y. Sasaki：“Cryptanalysis Against Symmetric-Key Schemes with Online Classical Queries and Offline Quantum Computations,” Proc. of CT-RSA 2018, Vol.10808, pp.198-218, 2018.
(7) T. Saito, K. Xagawa, and T. Yamakawa：“Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model,” Proc. of EUROCRYPT 2018, Vol.10822, pp.520-551, 2018.
(8) 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.
(9) A. Hosoyamada and T. Iwata：“4-Round Luby-Rackoff Construction is a qPRP,” Asiacrypt 2019, pp.145-174, Kobe, Japan, Dec. 2019.
(10) M. Hhan, K. Xagawa, and T. Yamakawa：“Quantum Random Oracle Model with Auxiliary Input,” Asiacrypt, pp.84-614, Kobe, Japan, Dec. 2014.



（後列左から）草川 恵太/
Mehdi Tibouchi/
西巻 陵
（前列左から）阿部 正幸/ 徳永 裕己

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
企画担当
E-mail scpflab@hco.ntt.co.jp

主役登場

あらゆるIoTサービスへセキュリティが組込まれることをめざして

田村　桜子
NTTセキュアプラットフォーム研究所
研究員

大学時代インターネットとは全く違う分野にいた私は，入社してセキュリティにかかわるまで，電子メールや通販サイトなど日常生活の中で利用していたセキュリティ技術の有難さ・必要性に気が付くことがありませんでした．現在のIoT（Internet of Things）サービスでも同様のことが起きていると思います．現在のIoTでも，元々はインターネットにつながっていなかったモノがインターネットにつながるため，IoT機器の所有者はセキュリティに対する意識が低いことが多く，十分なセキュリティ対策が行われていないことから，IoT機器に対する攻撃が後を絶ちません．そのため私は，日常生活で使っていたサービスのように，IoTサービスでもIoT機器の所有者が意識せずともセキュアにサービスを利用できるようにIoT機器にあらかじめセキュリティ機能を組み込んでおく必要があると考えています．

私の所属するグループでは，IoTセキュリティの中でも，公開鍵ベースのNTT独自の認証認可技術を用いたIoT向けセキュリティ基盤の構築に取り組んでいます．この基盤は，正しい機器であるか保証する認証，正しいアクセス制限を持った機器であるか保証する認可を実現します．一言に認証認可技術をIoT機器に組み込むといっても，IoT機器上でセキュアに鍵を保管・演算処理する技術をはじめ，さまざまな技術が必要となります．実際に検討を進めると，IoT機器特有の技術課題も多く，組込み機器特有の実装ノウハウを持つソフトウェア開発ベンダ，IoT機器に搭載されるチップの製造ベンダ，鍵の管理を行う運用ベンダ等，多くのベンダの協力が必要不可欠となることが分かってきました．展示会等を通じて，それぞれ最適なベンダを探し出し，技術の実用化に向けて共同で検討を進めています．

また，IoT機器では低コストで利用できる狭帯域のネットワーク環境の利用も加速しています．しかし，このようなIoT向けネットワーク環境における，暗号アルゴリズムのフィージビリティや性能面に関しては，まだまだ研究が行われていないため，その必要性があると強く感じました．そこで，実際に狭帯域ネットワークを構築することから始め，そのうえで私たちの技術の動作検証を行い，公開鍵ベースの認証方式が狭帯域のネットワークでも実用的な速度で動作することを，世界で初めて示しました．

現在は，AI（人工知能）により自動で栽培管理を行う農業IoTシステムのセキュリティ強化に取り組んでおります．現在使われているIoTサービスの多くは，センサ等のデータ可視化サービスですが，今後は収集データを活用し，IoT機器へのフィードバックまで行われるようになります．また，サービス間の連携も進み，接続する機器が多様化していきます．結果として，価値の高いデータが至るところに行き交うようになり，よりセキュリティが重要になっていきます．IoT機器の所有者がセキュリティの知識がないことも考慮し，意識せずともセキュアな環境でIoT機器を利用できるよう，安心・安全なサービスに役立つ技術の研究開発を進めていきます．