URL　https://journal.ntt.co.jp/article/36090
DOI　https://doi.org/10.60249/25095101

セキュリティR&Dを取り巻く環境変化とNTT社会情報研究所のチャレンジ

私たち，NTT社会情報研究所は，40年以上にわたる世界最先端の暗号研究，20年にわたる先駆的なサイバーセキュリティ研究を礎として，社会の「守り」に貢献しながら，リスクを許容できず従来諦めていた新たな活動やビジネスを具現化することによって，社会の「発展」に貢献するセキュリティR&Dに取り組んでいます．本稿では，その取り組み方針と最新の重点研究テーマを紹介します．

キーワード：#セキュリティ，#IOWN，#AI

中嶋　良彰（なかじま　よしあき）
NTT社会情報研究所　所長

社会の発展に貢献するセキュリティR&D

情報通信技術の発展は，日常のコミュニケーション手段を大きく変えました．インターネット，スマートフォン，クラウドのような情報通信技術によって，私たちは距離や時間の壁を越え，どこにいても誰とでも自由にオンラインでつながり，多様な情報に自由にアクセスでき，人間にしかできないと思われていた複雑な作業もAI（人工知能）に任せることができるようになりました．情報通信技術は，家族や友人等の人間関係，教育や文化，働き方，経済活動，国際関係等，社会のさまざまな場面で変化がもたらされています．NTTが研究開発，普及を進めているIOWN（Innovative Optical and Wireless Network）や大規模言語モデル（LLM：Large Language Models）tsuzumiも，さらなる豊かな社会へと私たちを導く新たな情報通信技術になることでしょう．

情報通信技術はこのように画期的な便益によって社会を変革するとともに，技術の浸透に連れて次第になくてはならない不可欠な存在になります．この時，私たちは，情報通信技術に正の側面がある一方で，負の側面もあることに目を向ける必要があります．前述のように自由にオンラインでつながり多様な情報にアクセスでき，かつAIが高度に支援してくれるという一見良いと思える状況は，プライバシー侵害や偽・誤情報[*1]拡散による混乱，AIを信じた結果による作業誤り，人間関係やメンタルヘルスの悪化などにつながるかもしれません．情報通信技術の誤用，機能不足，悪用，過度な依存などが，実に多様な問題を引き起こす可能性があります．新技術の創造と同時に，その技術が，社会，環境，経済，政治，文化，倫理，健康，セキュリティなど，さまざまな面でどのような変化をもたらすのかを考え対処していくことが重要です．

私たちは，このような考え方のもと，「社会」と「情報通信技術」の関係性について特に「正と負の両側面」に焦点を当て，NTTのIOWNやtsuzumiなどを含め，今後も進化する情報通信技術を人々にとって役立ち，そして不利益をもたらさないものとすべく研究開発に取り組んでいます．私たちの使命は，「人々の視点から社会の発展を支える情報通信技術の研究開発」であり，その目標は「安全かつ公正な情報活用により誰もが自分らしく暮らせる豊かな社会の実現」です（**図1**）．

本稿では，「セキュリティ」の視点から，上記の考え方に基づく取り組みの全体像を紹介します．私たちには，40年以上にわたり暗号研究に取り組んでいる歴史があり，暗号は情報通信や情報管理の安全性を高め「守る」ための根幹となる技術です．また，この20年はサイバーセキュリティ技術の研究開発にも注力しており，不正アクセス，マルウェア感染，DDoS（Distributed Denial of Service）攻撃，フィッシングなどのさまざまな脅威に対処する技術の研究開発に取り組んできました．一方，ここで強調したいことは，セキュリティ技術は「守る」ばかりが目的ではないということです．セキュリティ技術には，従来はリスクが許容できず諦めていたことを可能にできるという効果があります．例えば，直接会うことができない者どうしが本人性や権限を確認可能にする認証・認可技術，他者に開示したくない情報を秘密にしたまま活用可能にする秘密計算技術など，社会の「発展」につながるセキュリティ技術があります．

このように，私たちは情報通信技術がもたらす未来とリスクを見通したうえで，「守る」の視点から必要な技術をそろえていくと同時に，セキュリティによってさまざまな新たな活動を生み出し社会の「発展」に貢献していくという考え方で研究開発に取り組んでいます．

私たちを取り巻く環境

前述のとおり，情報通信技術の革新は利便性や発展に大きく寄与する一方で，さまざまな問題を新たにもたらす可能性があります．そのような問題につながり得る象徴的な現状や社会動向をまとめます．

■脆弱性対応の限界

ソフトウェア開発技術の進化によって，ますます多くのソフトウェアが生産される

＊1　偽・誤情報：個人，社会集団，組織または国に危害を与えるため，意図的・意識的につくられたウソ（虚偽）の情報のこと．

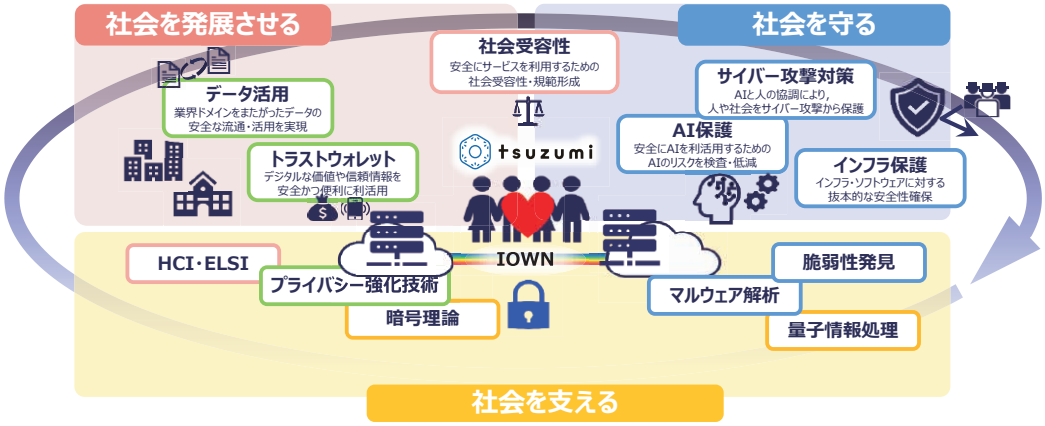

図1　セキュリティR&D　取り組みの全体像

ようになりました．おのずと米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が運営する脆弱性データベース（NVD：National Vulnerability Database）が公開しているソフトウェア脆弱性（セキュリティ上の欠陥）も加速度的に増大しており，もはや対処困難なレベルに達しています[1]．

■AI/LLMの悪用と安全性

AIの発展と普及とともに，攻撃コードの開発にLLMを利用した痕跡が発見されるなど，AIを悪用したサイバー攻撃が顕在化しています[2]．また，多様なシステムの根幹にAIが組み込まれ，AIそのものの安全性に対する危惧も急速に広がっています．

■攻撃に晒される人の認知

便利な検索サービスやSNS等は，攻撃ターゲットとなる人々や組織をオンラインで効率的かつ正確に調査する手段にもなり得ます．その結果，人の認知に影響を与える巧妙な偽・誤情報を効率的に生成・拡散できるようになり，詐欺や社会を混乱させる要因なっています．

■分散型社会への関心と期待

クラウドサービスの発展が社会のオンライン化に寄与する一方で，中央集権的なデータ管理がもたらすリスクが浮き彫りとなっています．特に欧州連合（EU）では，個人のプライバシー権とデータ主権の強化が積極的に図られるなど，個人が情報を主体的に管理・制御することへの関心と期待が国際的に高まっています．

■量子計算機の到来

量子計算機[3]は多様な応用への期待とともに，暗号解読などの新たなリスクももたらします．暗号化機能は社会を支える重要なシステムに広く深く浸透しており，漏れのないリスク対応は容易ではありません．

■国家レベルの脅威・リスク

上記のようなすべての脅威やリスクが，個人や企業のレベルではなく，国の政治・経済・安全保障，国家をまたがるサプライチェーンなどにまで広く波及しつつあります．

■脆弱なセキュリティ人材体制

上記の状況が，セキュリティ人材の責務や重要性をさらに高め，心身の負担感や緊張感がセキュリティ業務の魅力を超えてしまうおそれもあります．結果として，新たな人材が流入しづらくなり，セキュリティ体制の維持を難しくしていく可能性があります．

これらのいずれの動向に対しても，技術面のみならずさまざまな面から総力を結集してリスクに対処していくことが必要です．私たちは，そのようなリスク低減を目的化し，そればかりに躍起になるのではなく，その結果として社会をどのように発展に導くのかという「より良い未来を生み出す視点」でセキュリティ技術の研究開発に取り組むことが肝要と考え，取り組んでいます．

私たちの取り組み

私たちが取り組んでいる主要な研究テーマの全体マップを示します（**図2**）．この図は，NISTが定めるサイバーセキュリティフレームワーク2.0[4]が定めるセキュリティ活動の分類である統治，識別，保護，検知，対応，復旧のそれぞれに私たちの研究テーマを対応付けたものです．このフレームワークに基づき，「守る」の視点から必要な技術をそろえていくと同時に，それらの技術によって向上するセキュリティによってさまざまな新たな活動を生み出すことを可能にし，社会の「発展」に貢献していくという考え方で研究開発に取り組んでいます．

以降では，前述した各動向を踏まえ特に注力して取り組んでいる研究テーマとそのポイントを紹介します．

■社会を守るセキュリティR&D

前述のとおり，社会のデジタル化が進展するとともにサイバー攻撃の機会が増加し，その被害は深刻に進んでおり，私たちはこのような状況は今後も激化していくと予想しています．これまで以上に高度なサイバー攻撃対策を実現すべく，私たちは，人々とAIの協調によってゲームチェンジをもたらす革新的サイバーセキュリティ技術の研究を進めています（**図3**）．

① AIセキュリティ強化技術

AIシステムに対する脅威が日々進化しても対応可能にする技術です．安全性検査を起点に，AIシステム（AIモデル）を調整する方法（アライメント）と，AIシステムの運用時に不適切な入出力を遮断・制御する方法（ガードレール）を効果的に組み合わせて，持続的かつタイムリーな対応を可能にします．

② 脆弱性リスク低減技術

システム開発の上流工程から運用までを含め，脆弱性悪用による被害のゼロ化をめざす技術です．脆弱性はサプライチェーン攻撃の要因にもなっており，サプライチェーン攻撃が重要インフラを停止に追い込む被

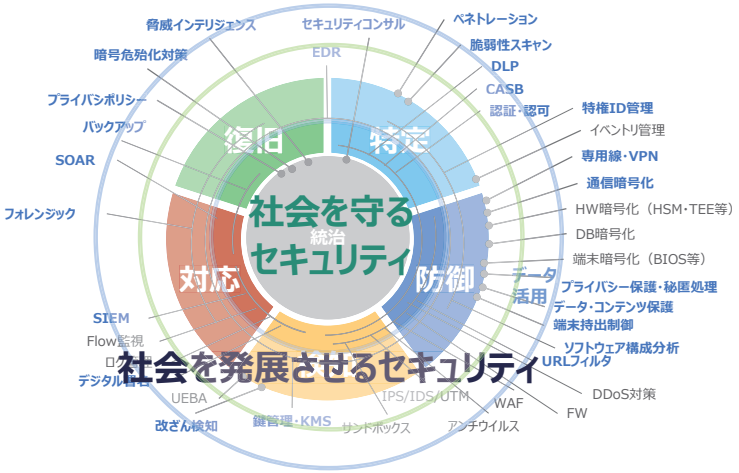

図 2　主要なセキュリティ R&D の全体マップ

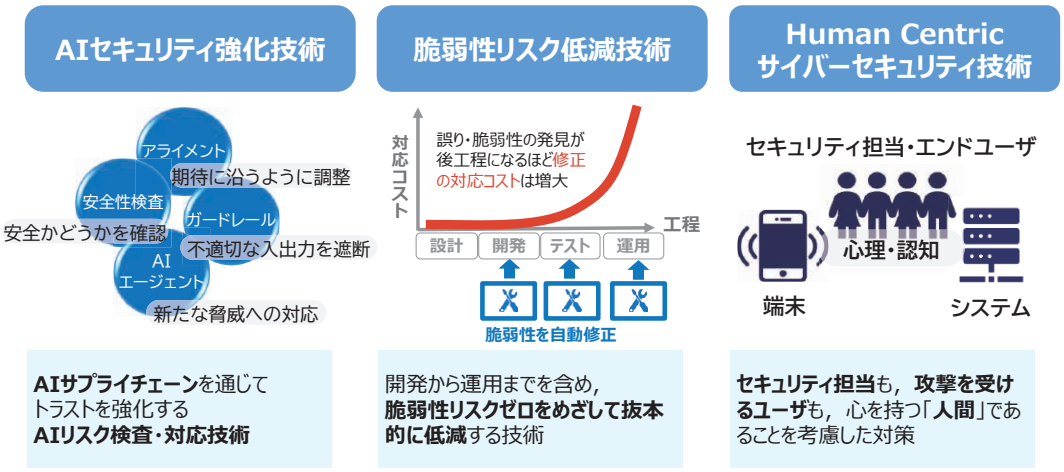

図 3　主要なセキュリティ R&D の全体マップ

害が現実化するなど，脆弱性対策は国家レベルの重要課題にもなっています．

③　Human Centric サイバーセキュリティ技術

人々とAIによる協働型を軸として，活動にかかわる人々の視点から，セキュリティ活動を進化させる技術です．セキュリティ担当も，脅威に晒されるエンドユーザも，心を持つ「人」であることを大前提とした新たな対策技術を創出し，セキュリティの向上のみならずセキュリティ活動の体験をより良いものにします．

サイバーセキュリティ分野における20年に及ぶ知見やデータの蓄積はこれら研究に大いに役立つと考えており，そのアドバンテージを活かしていく考えです．

■社会を発展させるセキュリティR&D

AIの進化によってさらなる加速が期待されるDX（デジタルトランスフォーメーション）では，人々，組織，社会に存在する多様なデジタルデータを，その保有者が相互にトラストを確認しつつ安全に流通させ，効果的に活用可能にすることが重要です．

情報流通システムとAI を人々が真に頼れる存在とする，デジタルトラスト強化技術の研究を進めています．デジタルデータのライフサイクル（生成・流通・蓄積・活用・廃棄等）を通じてデジタルデータの保有者の意思に基づいて流通をコントロールする技術，保有者が異なるデジタルデータをそれぞれ暗号化したまま結合・処理可能としてデータ処理におけるデータ漏洩やプライバシー侵害等のリスクを低減する技術です（**図 4**）．

①　個人起点のデジタル信頼保証技術

Web3，DID（Decentralized Identifier）*2/VC（Verifiable Credential）*3，AIエージェント時代に向け，ビジネスとプライバシーを両立する個人起点のデータ活用・保護技術です．具体的には人・AI，モノ，データに対しクレデンシャルを付与しトラストを保証・流通可能にします．多数のチェーン・レガシーウェブが存在する世界を前提とした次世代のデジタル信頼基盤に資する技術の創出をめざします．

②　プライバシーデータ活用・保護技術

多くのプライバシーデータが多様な経済活動・社会活動を通じて日々生み出されている現状に対して，その生成・利用・消滅までの全体を通じて適切な保護と積極的な活用を支える技術です．プライバシーデータがさまざまな組織・国・主体をまたがる状況に対しても，仮想的に統合したエンド・

＊2 DID：分散型IDのこと．
＊3 VC：検証可能なデジタル証明書のこと．

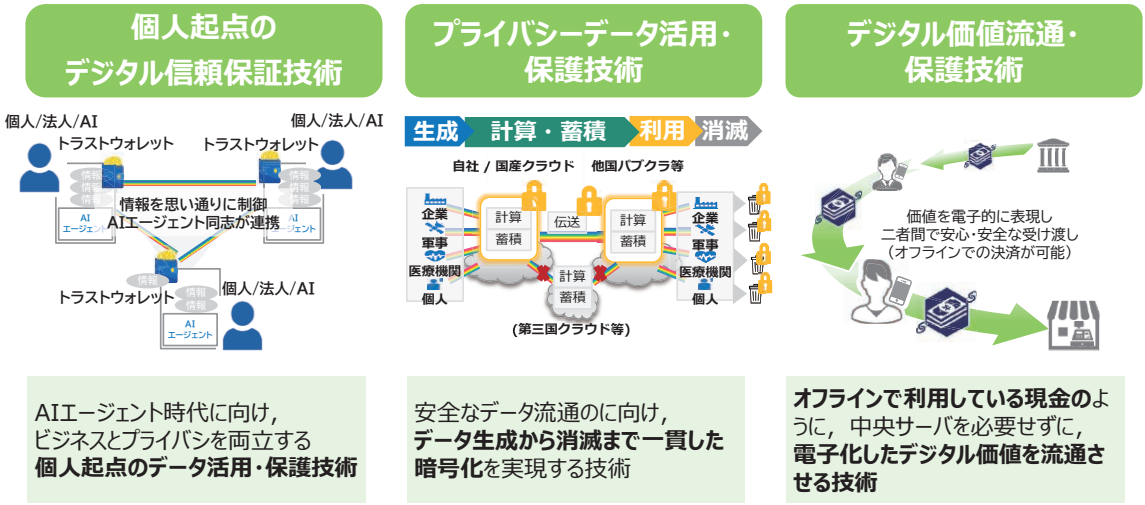

図4　社会を発展させるセキュリティR&D

ツー・エンドの暗号空間をIOWN上に形成することによって，データの強固な保護と柔軟な流通・活用を可能にします．

③　デジタル価値流通・保護技術

電子化した現金や価値情報等のデジタル価値を流通させる技術です．私たちがオフラインで利用している現金のように，中央サーバを必要としない新たな電子価値の流通をめざします．

これら取り組みに加えて私たちは法制度やプライバシー等の人文・社会科学のR&Dも同時に取り組んでおり，技術開発と制度整備の両輪を回しながら社会へ届けていくよう進めています．

■それらを支えるセキュリティR&D

10～20年後の次世代における技術の源泉となる世界トップレベルの情報セキュリティ基礎技術を継続して創出することをめざした理論研究にも取り組んでいます．本取り組みでは難関国際会議・論文誌に数多くの研究成果が継続的に採択されており，世界トップレベルの実績を保有しており，暗号やセキュリティの理論研究におけるCoE（Center of Excellence）として活動しています．

①　耐量子計算機暗号理論

量子計算機でも破れない暗号技術で社会の安心・安全をけん引します．具体的パラメータの安全性や実装安全性の解析に加え，より単純な安全性仮定による構成と効率を両立できる暗号理論の確立をめざします．

②　量子情報処理セキュリティ技術

暗号理論と量子情報処理を融合し，量子環境特有の物理現象を利用した量子情報処理でしか実現できない先駆的なセキュリティ技術の創出を進めます．

③　暗号プリミティブ・プロトコル構成理論

普遍的・効率的な構成を可能にする暗号理論をベースに，社会的に重要・有望な分野のサービスに最適な暗号プリミティブ・プロトコルを提供し，安全・便利・効率的なサービスのタイムリーな提供に貢献していきます．

④　PQCマイグレーション

2030年に直面している量子計算機の実用化に向けて，人々や社会が不利益を生じないように耐量子計算機暗号への移行を適切かつ効率的に実現できるようにするための技術です．創出した技術の標準化活動も取り組んでおり，NTT暗号の利用機会拡大をめざしています．

今後の展開

このように，私たちはセキュリティR&Dを進め，IOWNの普及やAI駆動型社会に向けて，情報通信技術を人々にとって役立ち，そして不利益をもたらさないものとすべく，社会を発展させる技術と守る技術，それらを支える研究開発を推進していきます．研究開発の際には，それぞれの研究を有機的に連携しながら，またNTTグループや外部パートナーとの会話や実証をしながら，社会に歓迎される，人々や社会に真に価値のある技術を創出していきます．

さらに，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，安全かつ公正な情報活用により誰もが自分らしく暮らせる豊かな社会の実現をめざし，さまざまなパートナーと連携しながら邁進していきます．

■参考文献

(1) https://nvd.nist.gov/
(2) https://cdn.openai.com/threat-intelligence-reports/5f73af09-a3a3-4a55-992e-069237681620/disrupting-malicious-uses-of-ai-june-2025.pdf
(3) https://www8.cao.go.jp/cstp/ryoshigijutsu/ryoshi_gaiyo_print.pdf
(4) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

中嶋　良彰

私たちは「守り」の視点と同時に，新たな価値の創造によって社会を「発展」させる視点を持ってセキュリティR&Dに取り組んでいます．セキュリティ技術でより良い未来を切り拓いていきましょう．

◆問い合わせ先

NTT社会情報研究所