（参考資料）

2023.1.31

日本電信電話株式会社

2 月 1 日～3 月 18 日は「サイバーセキュリティ月間」！
NTT が研究開発を進める、セキュリティ強化に繋がる技術を紹介

NTT は、すべての人が安全で健やかに過ごせ、社会が円滑に活動できる＜スマートな世界＞の実現に向け、セキュアなデータ流通・利活用技術の研究開発を推進しています。今回は、内閣サイバーセキュリティセンターが推進する「サイバーセキュリティ月間」（2023 年 2 月 1 日～3 月 18 日）に際して、セキュリティ強化に繋がる技術を紹介します。

特に昨今、サプライチェーンを狙ったサイバー攻撃や、ディープフェイクのように AI を悪用した攻撃に関して日々報じられる中、セキュリティ強化は喫緊の課題です。また、量子コンピュータの実用化に向けて、迅速かつ柔軟に安全な暗号技術に対応できる「クリプトアジリティ」の確保が重要となってきます。

今回は、今後サイバー攻撃のターゲットとなることが推測され、セキュリティ強化が求められる技術（「サプライチェーン」「暗号化・クリプトアジリティ」「AI 活用」）について、まとめて紹介します。

なお、プレスリリース既発表の技術に関する個別取材も受け付けておりますので、お問い合わせくださいませ。

―――――――― サプライチェーンのセキュリティを強化する技術 ――――――――

（セキュリティトランスペアレンシー確保技術 ／ セキュアマッチング技術）

2022 年 10 月には大阪市の医療機関がサイバー攻撃の被害を受けました。これを受け、厚生労働省は医療機関等におけるサイバーセキュリティ対策の強化について注意喚起を発表しました。

上記の件のみにとどまらず、国内外を問わず、企業や組織のサプライチェーンを狙ったサイバー攻撃およびその被害については日々報道されており、多大なインパクトを残しています。

■セキュリティトランスペアレンシー確保技術　【本件に関する個別取材も受け付けています】

機器の構成や動作仕様といった情報を常時可視化し、セキュリティ検査の結果をリアルタイムに共有することで、関係者全員で不正を監視し、機器の信頼を高め合う技術です。複数事業者がそれぞれ行う検査・監視の結果を集約、横断的に分析し、その差異や傾向に基づいて情報の誤りを発見することが可能です。

また、2023 年度上期には、本技術の活用を通じて、さまざまな企業・組織等が協調してサプライチェーンセキュリティリスク対応に取り組むことを目的とするオープンコンソーシアム設立を予定しています。

本件に関して、本技術が必要とされる背景や、今後の展開等についても個別取材を受け付けています。

詳細はこちらのプレスリリースをご覧ください。

・サプライチェーンセキュリティリスクを低減する技術のフィールド実証を開始
（2022 年 11 月 9 日発表）

・NTT と NEC、情報通信インフラにおけるサプライチェーンセキュリティリスクへの対策技術を開発
（2021 年 10 月 27 日発表）

図 1：セキュリティトランスペアレンシー確保技術の概要

■セキュアマッチング技術

安全なデータの検索・活用が可能となる新時代のデータ基盤「トラステッド・データスペース」の実現に向け、データを暗号化したまま2者間で集計処理が行える技術です。本技術により、異なる組織間のデータの統計処理を安全に行うことが可能になります。

※本件はプレスリリースでは未発表の技術です。実証実験や研究開発に関する具体的な成果は、今後の進捗に応じて発表していきます。本件の概要はこちらのページをご覧ください。

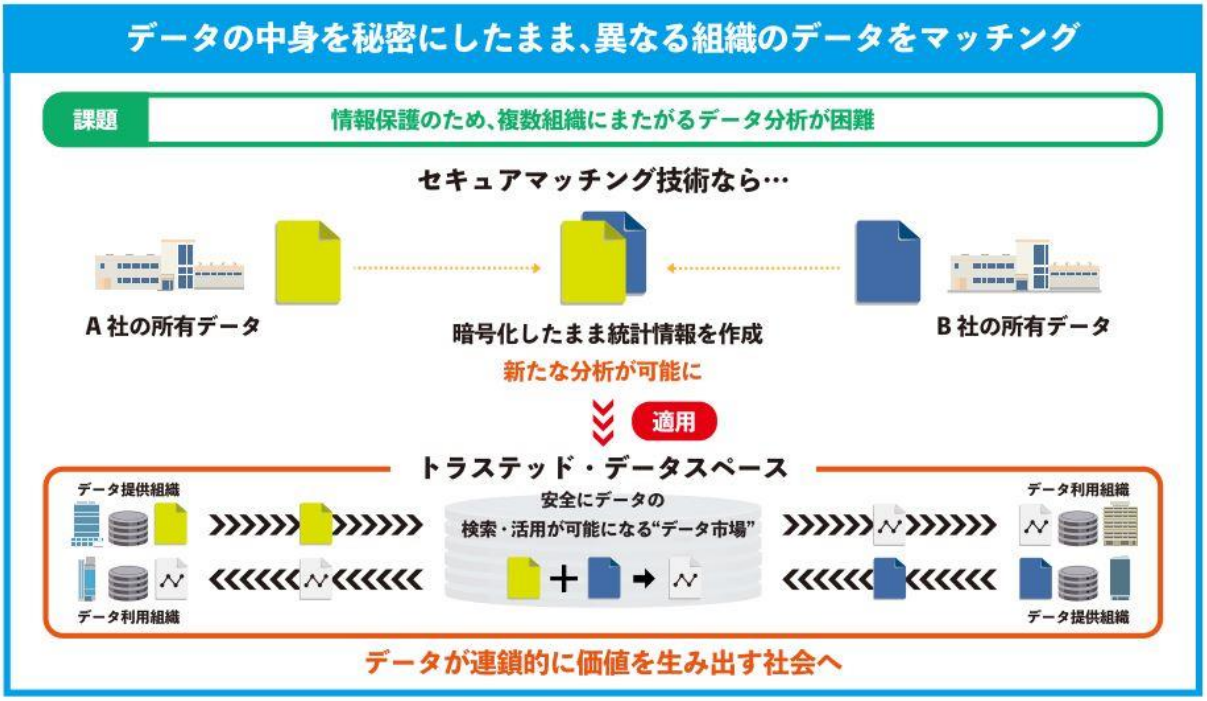

図 2：セキュアマッチング技術の概要

―――――――― 暗号化の安全性、クリプトアジリティを確保する技術 ――――――――

（セキュア光トランスポート技術 ／ 光暗号回路技術）

量子コンピュータが実用化されると、さまざまな分野への応用が期待されている反面、従来の暗号は解読される可能性があり、セキュリティリスクが増大します。2022 年 8 月には、米国土安全保障省サイバーセキュリティー・インフラストラクチャー・セキュリティー庁（CISA）が量子コンピューティングに起因する暗号関連のリスクについて警鐘を鳴らしました。

その脅威に備え、量子コンピュータでも解読できない暗号（耐量子計算機暗号）に移行していくためには、迅速かつ柔軟に安全な暗号技術に対応できる「クリプトアジリティ」を考慮することが重要です。

また、光コンピューティング基盤の安全性を確保するためには暗号演算や認証などのセキュリティ演算を光回路で実現することが必要です。しかし、既存の光演算技術では暗号演算のような複雑なデジタル演算を行う方法が確立されていないことが課題となっていました。

■セキュア光トランスポート技術　【本件に関する個別取材も受け付けています】

ユーザニーズに応じて、安全な暗号アルゴリズムを迅速かつ柔軟に選択・組み合わせることが可能になり、高度なセキュリティを維持したまま、安全な暗号技術へのスムーズな移行に貢献します。

遠隔手術をはじめ、本技術の活用事例についても個別取材を受け付けています。

詳細はこちらをご覧ください。

・遠隔手術を支えるロボット操作・同一環境共有を IOWN APN で実証開始

（2022 年 11 月 15 日発表プレスリリース）

・次世代の高安全な暗号技術を適用した光トランスポートネットワーク技術を開発

（2021 年 11 月 5 日発表プレスリリース）

・特集 IOWN 時代のセキュリティ R&D セキュア光トランスポートネットワーク

（NTT 技術ジャーナル）

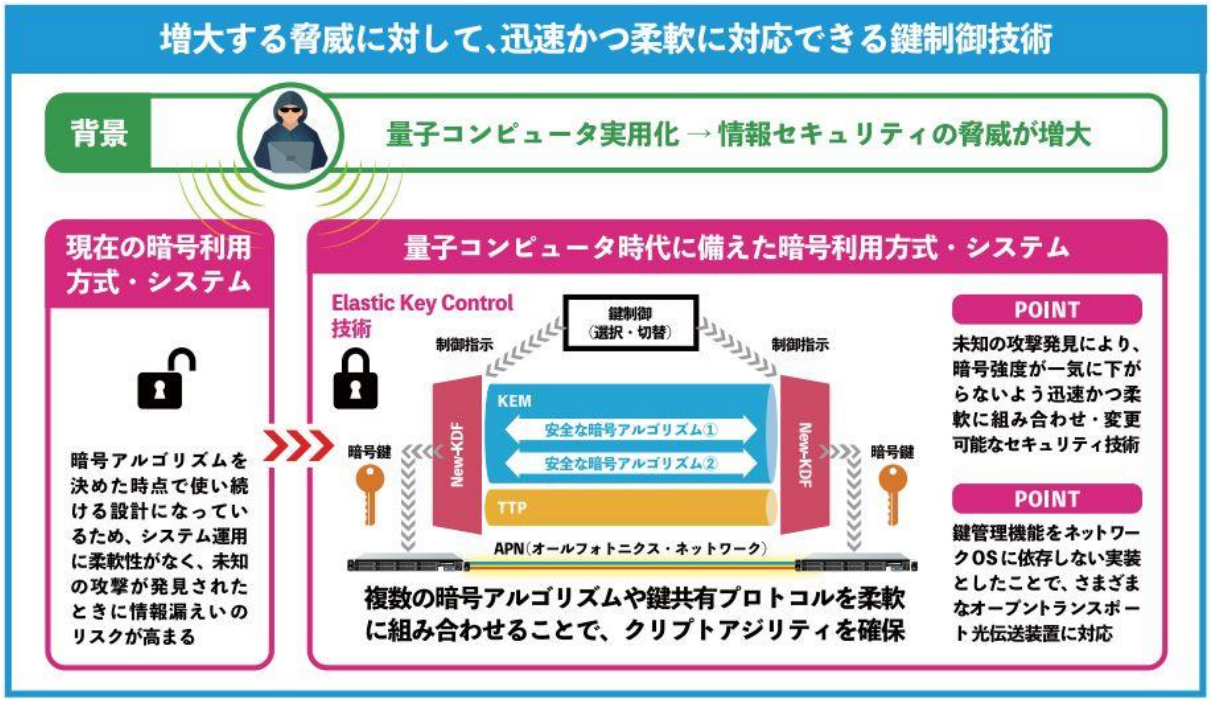

図 3：セキュア光トランスポート技術の概要

■光暗号回路技術

複数のビット値を 1 つの光アドレス値で表現することで、光演算処理を基本とした、複雑なデジタル演算が可能な手法を世界で初めて実現しました。本手法は光配線を用いた演算であるため、将来的に演算全体のボトルネックとならない低遅延・低消費電力の演算が実現可能です。

※本件はプレスリリースでは未発表の技術です。実証実験や研究開発に関する具体的な成果は、今後の進捗に応じて発表していきます。本件の概要はこちらのページをご覧ください。

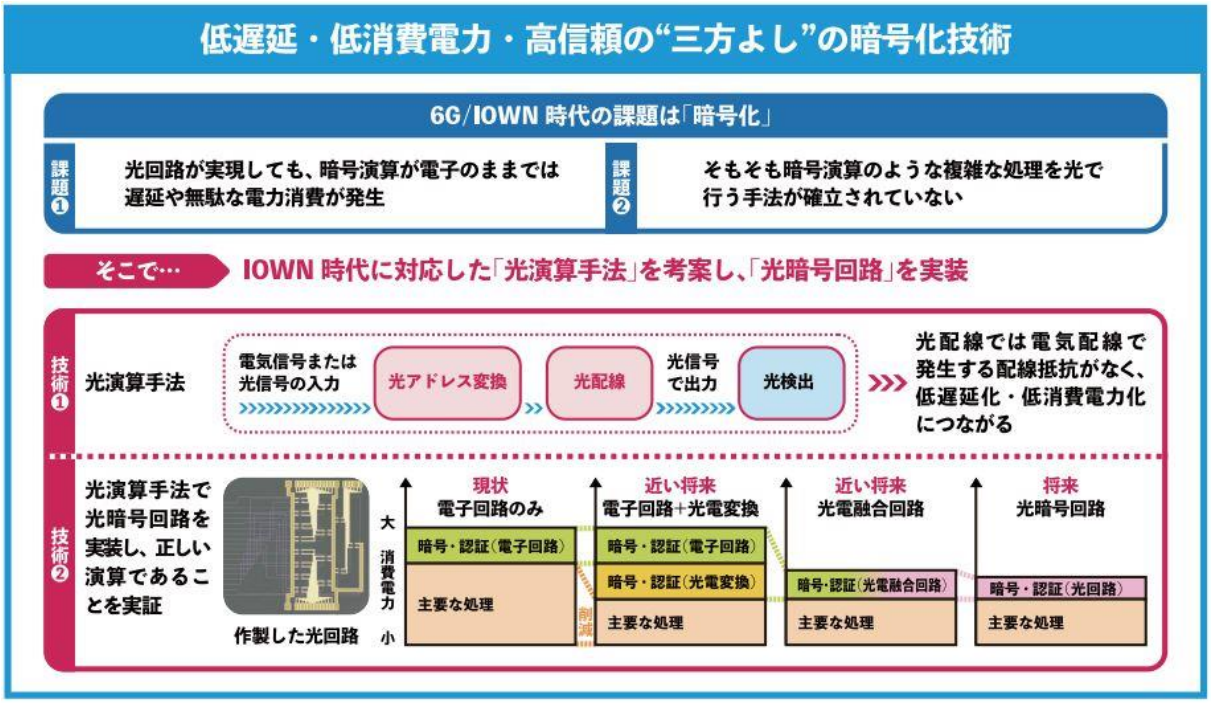

図 4：光暗号回路技術の概要

AI 活用に関する技術

（AI のプロフィールによる同一性検証）

2022 年 6 月に、FBI がディープラーニング技術を悪用して作成された合成メディアである「ディープフェイク」が増えていることについて、注意喚起を発表しました。

今後 AI が普及すると、予期せぬ変化や攻撃者の介入によって意図しない AI に変化してしまう恐れや、AI が不正にコピーされることで、AI のなりすましが発生し、利用者が被害を受ける可能性があります。そのため、利用者自身が AI の同一性を検証できる必要があります。

■AI のプロフィールによる同一性検証

AI が攻撃を受け変化した場合や AI のなりすましが発生した場合には、AI の振る舞いからそれを検知し、AI が日々の学習を通じて変化した場合にはこれまで利用した AI のままかどうかを判別する技術の研究開発を開始しました。本技術により、安心して AI を活用できる未来に貢献します。

※本件はプレスリリースでは未発表の技術です。実証実験や研究開発に関する具体的な成果は、今後の進捗に応じて発表していきます。本件の概要はこちらのページをご覧ください。

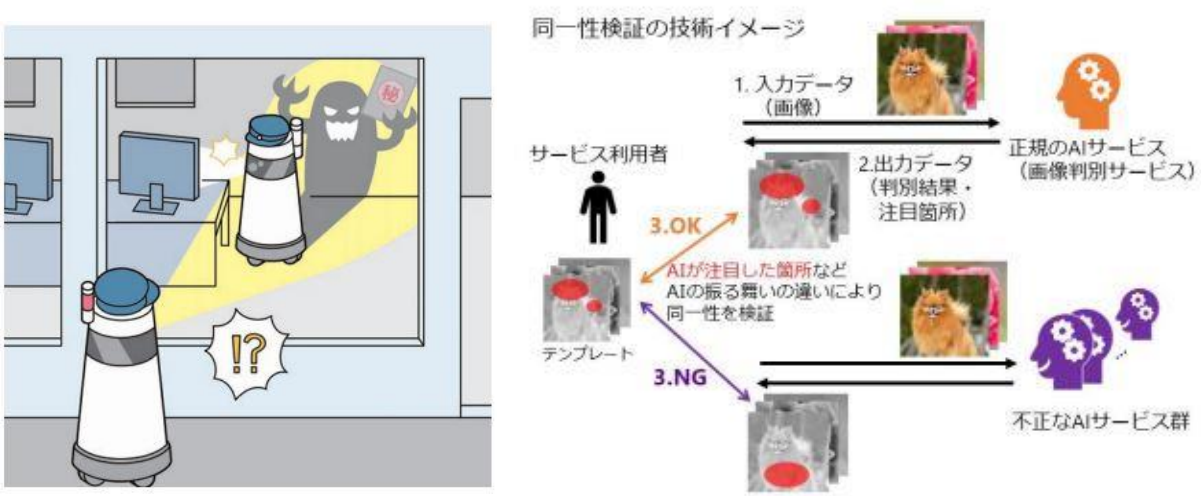

図 5：AI のプロフィールによる同一性検証の概要

今後も、NTT はセキュリティ強化に繋がる技術開発を進め、より安心・安全にテクノロジーを活用することのできる未来および IOWN 構想※実現への貢献をめざしてまいります。

なお、プレスリリース既発表の技術に関する個別取材も受け付けておりますので、ご希望の場合は以下のお問い合わせ先までご連絡くださいませ。

※「IOWN（アイオン）構想」：革新的な技術によりこれまでのインフラの限界を超え、あらゆる情報を基に個と全体との最適化を図り、多様性を受容できる豊かな社会を創るため、光を中心とした革新的技術を活用した高速大容量通信、膨大な計算リソース等を提供可能な、端末を含むネットワーク・情報処理基盤の構想です。

■本件に関する報道機関からのお問い合わせ先
日本電信電話株式会社
NTT 広報室
nttrd-pr@ml.ntt.com