3　セキュリティ基盤技術
3　Security Fundamentals Technologies

3-1　セキュリティ基盤研究室における研究開発
3-1　Overview of R&D Activities in Security Fundamentals Laboratory

篠原 直行
SHINOHARA Naoyuki

本稿では、2023 年度までに実施されたセキュリティ基盤研究室における近年の研究開発とその成果の概要を紹介する。

This paper provides an overview of recent R&D activities and achievements in security fundamentals laboratory up to FY2023.

1　まえがき

量子コンピュータや機械学習等の新たな技術の登場及びその性能の向上により、様々な暗号技術及びプライバシー保護技術の必要性が高まっている。セキュリティ基盤研究室では、第 4 期中長期計画（2016 年度～2020 年度）において、新たな機能を備えた機能性暗号技術、認証技術等の暗号技術の研究開発に取り組んだ。さらに、パーソナルデータの利活用に貢献するためのプライバシー保護技術の研究開発を行った。暗号技術の安全性評価については、耐量子計算機暗号等の新たな暗号技術を中心に研究を実施し、その知見を活かして、CRYPTREC の「耐量子計算機暗号研究動向調査報告書（2018 年度）」の執筆に貢献した。

2024 年現在では、第 5 期中長期計画（2021 年度～2025 年度）に基づいて研究開発を進めている。具体的には、検索可能暗号、宇宙機無線通信のための暗号技術、高機能暗号を利用したプライバシー保護連合学習システムである DeepProtect 等の研究開発を実施し、プライバシー保護技術の理解促進及び普及のために、プライバシーポリシーに関する調査を実施した。暗号技術の安全性評価については、耐量子計算機暗号を含む新たな暗号技術及び現在利用されている暗号技術の安全性評価の研究を進めている。特に、量子コンピュータ実機を用いた現代暗号への脅威の評価やエンドツーエンド暗号化に関する安全性評価を実施している。これらの成果により、「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」「CRYPTREC 暗号技術ガイドライン（高機能暗号）」「CRYPTREC 暗号技術ガイドライン（軽量暗号）」の策定及び改定等、CRYPTREC の活動に貢献している。また、エンドツーエンド暗号化に関しては、個々のオンライン会議システムの仕様の変更に貢献し、安全性を高めている。

本稿では、2023 年度までにおいてセキュリティ基盤研究室で実施した代表的な研究開発についてその概要を説明する。具体的には、電子政府推奨暗号等の現在広く利用されている暗号技術及び耐量子計算機暗号等を含む新たな暗号技術やプライバシー保護技術について、それらの研究開発及び安全性評価の成果や取組を中心に紹介する。

2　各研究開発課題の概要

2.1　データを安全に利活用するための技術の研究開発

セキュリティ基盤研究室は、データの提供･収集･保管・解析・展開の各段階におけるセキュリティやプライバシーを確保するために、匿名認証や検索可能暗号等のアクセス制御技術、秘匿計算等のプライバシー保護解析技術等の研究開発を実施している。これらの成果を用いて、組織横断的な連携を含むデータ利活用を促進するとともに、安全なテレワーク等の社会的な課題解決に貢献していく。本節では、「様々な検索可能暗号」「NewSpace における宇宙機との無線通信の暗号技術」「プライバシー保護技術の理解促進・普及に向けた試み」「プライバシー保護連合学習技術 DeepProtect」の成果を簡単に説明する。これらの詳細については、本稿以降の各原稿を参照されたい。

●様々な検索可能暗号

検索可能暗号は、データ及びキーワードを暗号化したまま、それらを復号することなくキーワード検索を実施できる暗号技術である。そのため、データの情報漏洩対策だけではなく、キーワードの情報がデータへのアクセスを許可された以外の第３者に漏れる可能性を低減することが可能な技術である。セキュリティ基盤研究室では、検索可能暗号に関する以下の研究項目等に取り組んでいる。

・動的検索可能暗号
・外部匿名性を満たす放送型検索可能暗号（図 1）
・検索可能暗号の性能評価
・セキュアチャネルフリー検索可能暗号
・検索可能暗号を用いた暗号化ストレージチャットシステムの実装評価

これらの知見を用いて「CRYPTREC 暗号技術ガイドライン（高機能暗号）」策定に貢献している。

●NewSpace における宇宙機との無線通信の暗号技術

公的機関が主導する従来の宇宙開発とは異なり、NewSpace と呼ばれる民間主導の宇宙開発が世界的に活発化している。日本では 2018 年 11 月に宇宙活動法が施行され、ロケットの型式認定に関するガイドラインで、重要なシステム等に関するデータの送受信については、適切な暗号化等の措置を講ずることが求められている。セキュリティ基盤研究室では、宇宙機の乗っ取り防止による飛行の安全確保、宇宙機から伝送される飛行状況や学術的・商業的価値の高いデータの保護を目的とした暗号技術の研究開発を行っている。特に、コストを抑えた民生電子デバイスを使用して、高い安全性を確保できる暗号技術の開発に力を入れている。

●プライバシー保護技術の理解促進・普及に向けた試み

ユーザが自分のデータ提供の際に同意を求められるプライバシーポリシー等の文書は一般的に理解が難しく、読み飛ばされることが多い。結果としてユーザにとって想定外のデータ利用や不利益につながる可能性があると考えられる。セキュリティ基盤研究室では、個人データ収集時のセキュリティ・プライバシー対策をユーザにとって真にわかりやすく、効果的に受け止められるものにするために、プライバシーポリシーの解析や特徴比較を行い、ユーザブルセキュリティの向上に貢献する研究に取り組んでいる。具体的には以下の三つの項目等について実施している。

・プライバシーポリシーで使用される技術用語の理解度とプライバシーポリシーへの同意の調査
・日本人のプライバシーに関わる法制度に対する理解の調査
・差分プライバシー技術を非専門家に説明するにあたり予想される課題の検討

●プライバシー保護連合学習技術 DeepProtect

機械学習は、学習データが多いほど学習の効果が高まる傾向があるため、学習データを所有する複数の組織がデータを共有することは有効であると考えられるが、学習データが機微情報を含む場合はそのような方法を実施することはできない。連合学習では学習データを共有することなく各組織で機械学習を実施し、そこで得られた勾配情報を参加組織で共有して更新するため、上述の問題を解決する一つの手段として挙げられる。しかし、勾配情報から学習データの情報が漏洩する可能性がある。この問題を解決するために、セキュリティ基盤研究室では、データを暗号化したまま加法演算が可能な準同型暗号を利用することで、勾配情報を暗号化したままモデルを更新して共有するプライバシー保護連合学習技術である DeepProtect の研究開発を進めている。さらに DeepProtect と金融の分野の実データを用いた実証実験（図 2）を進めるなど、社会実装に向けた取組も実施している。

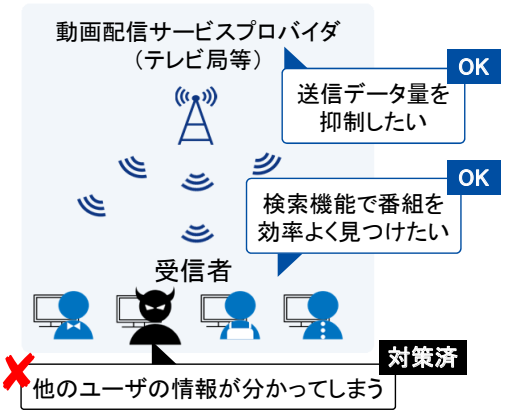

図 1　放送型検索可能暗号

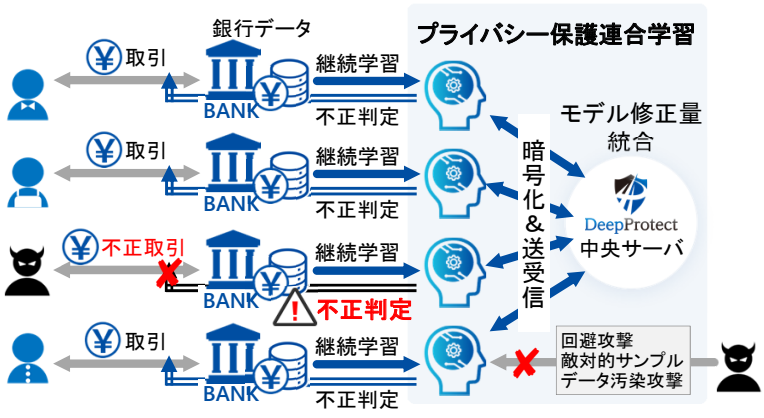

図 2　DeepProtect を用いた実証実験の例

2.2　量子コンピュータ時代に向けた暗号技術の安全性評価

セキュリティ基盤研究室では、現代の暗号技術及び将来的に利用が見込まれる様々な暗号技術の適切な実装と安全な運用に貢献するため、暗号技術の安全性及び実装性能等を評価している。具体的には、量子コンピュータ時代にも安全に利用できる耐量子計算機暗号等の暗号技術や、現在広く使用されている RSA 暗号、楕円曲線暗号等の安全性評価に関する研究開発に取り組んでいる。またその成果を基に、電子政府推奨暗号の安全性を評価及び監視し、暗号技術の適切な実装法や運用法を調査及び検討するプロジェクトである CRYPTREC に貢献している。本節では、「量子コンピュータによる現代暗号の安全性評価」「耐量子計算機暗号の安全性評価」「エンドツーエンド暗号化に対する安全性評価」「CRYPTREC 活動」の成果を簡単に説明する。これらの詳細については、本稿以降の各原稿を参照されたい。

●量子コンピュータによる現代暗号の安全性評価

現在広く利用されている公開鍵暗号は、素因数分解問題や離散対数問題を解く計算の困難性をその安全性の根拠としており、これらの問題が解かれると解読されてしまう。大まかには、解読の計算コストはその問題で扱う数(鍵長)が大きいほど高まる。これらの問題は、量子コンピュータ及びショアのアルゴリズムを用いることで高速に解かれてしまうことが理論的には証明されているため、現在の量子コンピュータ実機による現代暗号への具体的な脅威の評価、すなわち、どの程度の大きさの鍵長に対して解読が成功するかが重要な研究課題となっている。セキュリティ基盤研究室では、離散対数問題が量子コンピュータ実機によって解けたことの定義を世界で初めて提案し、さらに現在の量子コンピュータ実機を用いて、非常に小さい鍵長に対して、世界で初めて離散対数問題を解くことに成功した。本成果は、実際に暗号で使用されている、より大きなサイズの鍵長の離散対数問題を現在の量子コンピュータ実機で解くことはできないこと、すなわち現時点では現代暗号に量子コンピュータの脅威が生じていないことを示している。

●耐量子計算機暗号の安全性評価

耐量子計算機暗号とは、従来の公開鍵暗号が使われている環境でも従来と同様に使用でき、量子コンピュータ及び旧来のコンピュータを用いてもその安全性を保つことができる公開鍵暗号である。簡単には、量子コンピュータ及び旧来のコンピュータを用いても高速に解く方法が発見されていない数学的な問題を安全性の根拠としている公開鍵暗号である。セキュリティ基盤研究室では、耐量子計算機暗号の主要な候補である格子暗号及び多変数公開鍵暗号を中心に安全性評価の研究を進めており、特に多変数公開鍵暗号(図 3)の解読コンテストである Fukuoka MQ Challenge において、解読の世界記録を達成した。これらの研究で得られた知見は、「CRYPTREC 暗号技術ガイドライン(耐量子計算機暗号)」の策定に役立てられている。

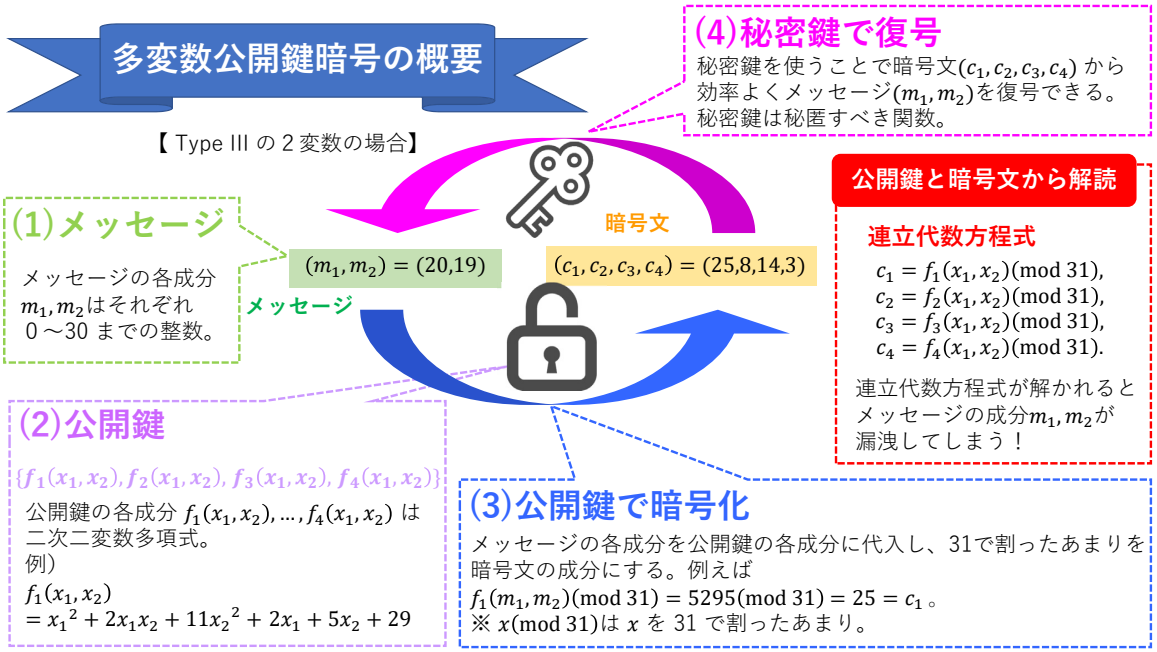

図 3　多変数公開鍵暗号の概要

●エンドツーエンド暗号化に対する安全性評価

エンドツーエンド暗号化は、送受信者の間でのみデータの正常な送受信が可能であり、盗聴者だけではなく、情報通信サービスの提供者であってもデータの情報の取得及び改ざん等が不可能な暗号技術である。エンドツーエンド暗号化は、リモート会議システムで利用されており、テレワークの増加に伴いこの暗号技術の安全性評価は重要な研究課題となっている。セキュリティ基盤研究室では、主要なリモート会議システムで利用されている様々なエンドツーエンド暗号化技術の安全性評価を実施し、それらの脆弱性を発見し、その防衛対策を主要なリモート会議システムの運営者に報告することで安全性の確保に貢献している。

● CRYPTREC 活動

CRYPTREC は、電子政府推奨暗号の安全性を評価及び監視し、暗号技術の適切な実装法や運用法を調査及び検討するプロジェクトである。その事務局は、デジタル庁･総務省･経済産業省･情報通信研究機構･情報処理推進機構が務めている。CRYPTREC の主な活動として、2016 年度に軽量暗号、2018 年度にハッシュ関数 SHA-1、2022 年度に耐量子計算機暗号及び高機能暗号に関するガイドラインをそれぞれ策定した。また、2023 年度には、2016 年度に策定した軽量暗号に関するガイドラインを改定した。2022 年度には CRYPTREC 暗号リストを 10 年ぶりに改定した。

3　むすび

本稿では、2023 年度までにセキュリティ基盤研究室で実施した、暗号技術及びプライバシー保護技術等の研究開発、暗号技術の安全性評価の研究に関する代表的な取組を紹介した。ほかにも紹介したい多くの取組はあるが、それらについては本研究室の web ページ [1] を参照されたい。本研究室は、暗号技術やプライバシー保護技術等に関する基礎研究を担当しているが、CRYPTREC や DeepProtect 等の社会実装も着実に進めている。

今後の展望について幾つか簡単に紹介する。まず、耐量子計算機暗号の研究は重要な課題であると考えている。国内外で研究活動を含め種々の活動が盛んであり、特に米国の NIST が耐量子計算機暗号の標準化を進めており、この動向は日本で利用する耐量子計算機暗号の選定に大きな影響を与える。NIST は 2016 年に耐量子計算機暗号の最初の公募を開始し、2024 年時点で幾つかの方式が標準化されつつある。さらに、2022 年に追加の公募を実施しており、これらの安全性及び実装性能の評価は 2030 年ごろまで続くと考えられる。さらにそこから、実装方法の改良が進み、そのことによって改良された実装方法に対するサイドチャネル攻撃が発見されることなどを考えると、2035 年前後まではセキュリティ基盤研究室及び CRYPTREC において耐量子計算機暗号の研究は重要な課題である。

DeepProtect については、金融の分野の実データを用いた実証実験を実施し、更なる改良をすべき点を発見した。さらに、医療の分野等の新たな分野への応用の見込みとそれによって生じた新たな研究課題がある。DeepProtect の社会実装への取組は進めつつ、並行して研究開発も引き続き実施していく予定である。

謝辞

第 4 期中長期計画から 2024 年度にかけて、盛合志帆氏、野島良氏（現在、立命館大学教授）、私の三名がセキュリティ基盤研究室の室長を務めてまいりました。それぞれが専門とする研究分野は異なっており、本研究室の運営には様々な専門性が求められます。この運営が無事に進められているのは、室員がそれぞれの専門性を活かして協力していることと、長年にわたって多くの方々が本研究室を支えてくださっているためです。特に、本研究室の運営を担当してくださった、阿部妙子氏、高橋しおり氏、田村千代氏、峯田友子氏、矢島美樹子氏の貢献は無くてはならないものでした。ここに感謝の意を表します。

【参考文献】

1　セキュリティ基盤研究室 web ページ, https://sfl.nict.go.jp/

篠原 直行（しのはら なおゆき）
サイバーセキュリティ研究所
セキュリティ基盤研究室
室長
博士（数理学）
暗号に関する数理学

【受賞歴】

2019 年　The 14th International Workshop on Security (IWSEC 2019) Best Paper Award
2013 年　第 12 回（2013 年）ドコモ・モバイル・サイエンス賞先端技術部門優秀賞
2008 年　日本数式処理学会第 17 回大会 2008 年度奨励賞