# 2-3　セキュリティ基盤技術の研究開発概要

盛合志帆

本稿では、第 3 期中長期計画（2011 ～ 2015 年度）で実施されたセキュリティ基盤技術に関する研究開発とその成果概要を紹介する。

## 1　まえがき

情報通信ネットワークを安心・安全に利用・構築するために、暗号技術をはじめ、様々なセキュリティ基盤技術が活用されている。1970 年代に現代暗号の基礎が築かれ、1990 年代に広く普及、2000 年代に標準化が進み、市場における暗号技術は成熟期を迎えている。しかしながら日々新たな解読技術や技術開発が進展していること、また自動車や IoT など暗号技術の導入が遅れていた分野への適用が課題となっていることから、情報通信を担う国の研究機関として、情報通信ネットワークを継続的に安心・安全に利用できるよう、暗号技術の安全性評価を行い、将来に向けたセキュリティ基盤技術の研究開発を推進することは重要な責務である。

セキュリティ基盤技術研究室では、産学と連携して、情報通信ネットワークの安全な利用を支える暗号・情報セキュリティ基盤技術の発展に貢献し、世界を先導する成果を挙げること、そして我が国の電子政府システムで安心して利用できる暗号技術について指針を提示することをビジョンとして掲げ、第 3 期中長期計画（2011 ～ 2015 年度）を進めてきた。

本稿では、第 3 期中長期計画においてセキュリティ基盤技術研究室にて実施した研究開発項目の概要を示す。具体的には、以下の 4 つの研究開発項目である。

- **量子セキュリティ（情報理論的安全性に基づくセキュリティ）技術**
  量子技術と現代暗号技術を融合した、情報理論的安全性をもつセキュリティネットワーク構築のための研究開発
- **長期利用可能暗号技術**
  量子計算機が実現しても長期に渡り強固な安全性を維持できる、長期利用可能な暗号技術の研究開発
- **実用セキュリティ技術**
  多様な利用環境に合わせた安全性を提供する実用的な暗号技術の研究開発
- **暗号安全性評価技術の高度化**
  我が国の電子政府推奨暗号の評価及び電子政府推奨暗号リスト改定、将来の暗号技術の移行に資する暗号安全性評価技術の高度化に関する研究開発及び電子政府推奨暗号の監視・評価を実施する CRYPTREC プロジェクトの事務局運営

## 2　各研究開発課題の概要

### 2.1　量子セキュリティ（情報理論的安全性に基づくセキュリティ）技術

本研究開発課題では、量子技術と現代暗号技術を融合させ、より汎用的で柔軟な量子セキュリティネットワークの構築に向けた研究開発を行った。量子通信を利用すると、情報理論的に安全な秘匿通信路は実現できるが、量子技術だけでは「ユーザ認証」といった基本的な認証機能ですら、情報理論的安全性をもつ方式は実現困難である。そこで、秘密分散法という暗号技術と組み合わせて、1 つのパスワードだけで情報理論的に安全なユーザ認証を提案した。具体的には、クラウド上の複数サーバにデータを分散して保存する際に、パスワードを持たないユーザが複数のサーバ管理者と結託しても、結託者数が決められた閾値以下であれば秘密情報の漏えいがなく、プライバシー保護が実現できることが情報理論的に証明できる認証機能付き秘密分散プロトコルである（東京工業大学との共同研究）（図 1）。さらに、本プロトコルを活用し、量子ネット

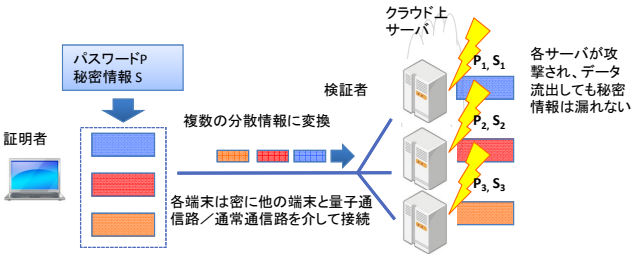


図 1　認証機能付き秘密分散プロトコル

ワーク上で認証機能付き秘密分散機能を備えたセキュアストレージシステムの実装を行った。本システムはNICT の量子 ICT 研究室等との連携プロジェクト「量子鍵配送を利用したセキュアネットワークの研究開発」にて実装したもので、秘匿と認証の両方の観点で情報理論的安全性が保証されたシステムの世界初の実装である。本成果は 2016 年度に Nature Publishing Group の電子ジャーナル Scientific Reports に採録されるなど、学術的にも高い評価を受けた。現在、ISO/IEC JTC 1 /SC 27 において秘密分散法に関する国際規格が作成されており、本認証機能付き秘密分散プロトコルについても国際標準化を進める予定である。

## 2.2　長期利用可能暗号技術

長期に渡り強固な安全性を保証するための長期利用暗号技術については、世界的に最も有望視されている格子理論に基づく方式に重点を置いて、新方式の設計と安全性評価に関する研究開発を行った。格子理論に基づく新方式の設計については、暗号化したままセキュリティレベルを変更でき、かつ暗号化したまま加算と乗算が可能な準同型暗号を世界で初めて実現した。これにより、例えば、100 年以上の長期間の保護が求められる遺伝子データ等を暗号化したまま統計処理を行うなど、プライバシーを保護したデータマイニングが可能になる。具体例としては、暗号化したデータに対する線形回帰計算で従来比 100 倍の高速化を達成したほか、ビッグデータ解析で活用されているロジスティック回帰分析（図 2）を実用的な時間で計算可能とし、暗号化された 1 億件のデータを 30 分以内で複数グループに分類できることをシミュレーションで確認した。本方式の一連の権利化も進めた。

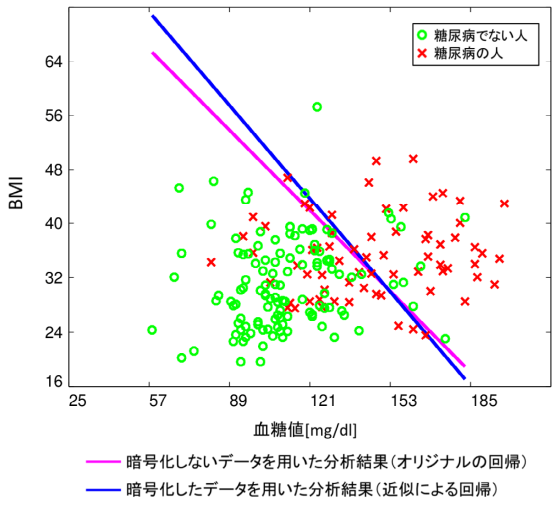


図 2　暗号化したままビッグデータを分類
（ロジスティック回帰分析）

格子理論に基づく方式の安全性評価については、安全性の根拠である格子の最短ベクトル問題の難しさを評価するアルゴリズムの高速化を達成し、暗号のトップカンファレンスの 1 つである Eurocrypt2016 に採録されたほか、ダルムシュタット工科大主催の安全性評価コンテスト “Lattice Challenge”（図 3）において複数の世界記録を更新した。本研究を進めるに当たって、九州大学、フランス INRIA、東京大学、NEC、日本銀行等の外部研究機関と連携を行った。

## 2.3　実用セキュリティ技術

本研究開発課題では、多様な利用環境に合わせた安全性を提供する実用的な暗号技術を目指し、様々な研究開発を行った。

### ● CPS/IoT を支える軽量暗号に関する研究

多様なセンサ群で収集したビッグデータをクラウド等で解析するようなシステムのセキュリティ確保を目的として、軽量暗号の性能評価を行い、既存暗号技術に対する優位性を検証した。また、インターネットに常時接続する「コネクテッドカー（つながる 車 ）」や ITS（Intelligent Transport Systems）、IoT のセキュリティ向上に軽量暗号技術を活用するため、軽量暗号技術を用いたタイヤ空気圧監視システム向けセキュリティプロトコルの試作も行った。また、軽量暗号に関する国際規格 ISO/IEC 29192 -1, 29192 -2, 29192 -5 の標準化にエディタとして貢献した。


図 3　格子暗号の安全性評価（TU Darmstadt Lattice Challenge）
https://www.latticechallenge.org/


図 4　暗号化ファイル共有システム PRINCESS

## ● 暗号化ファイル共有システム PRINCESS と自動車共有システムへの応用

代理復号と代理再暗号化の二機能を実現する ID ベース暗号を用いて、ファイルの機密レベルに応じて安全に共有先を指定できる暗号化ファイル共有システム PRINCESS（Proxy Re-encryption with INd-Cca security in Encrypted file Storage System）を提案、権利化を行ったほか、プロトタイプを開発した（図 4）。

車の各種センサ情報や位置情報に関する（ビッグ）データを活用した新たな高度交通システム・サービスの実用化に向け、自動車ビッグデータのセキュリティ・プライバシー確保が急務となっていることから、この技術を活用してクラウドを介したセキュアな自動車情報共有システムを試作した（図 5）。

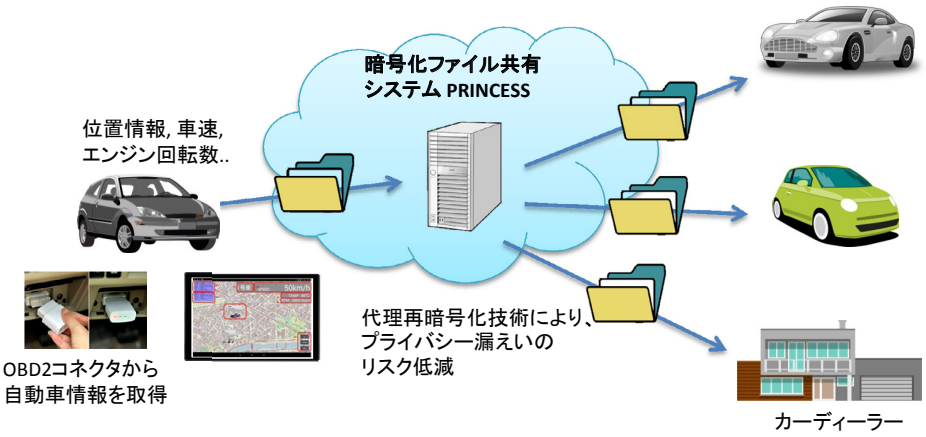


図 5　PRINCESS の自動車情報共有システムへの応用

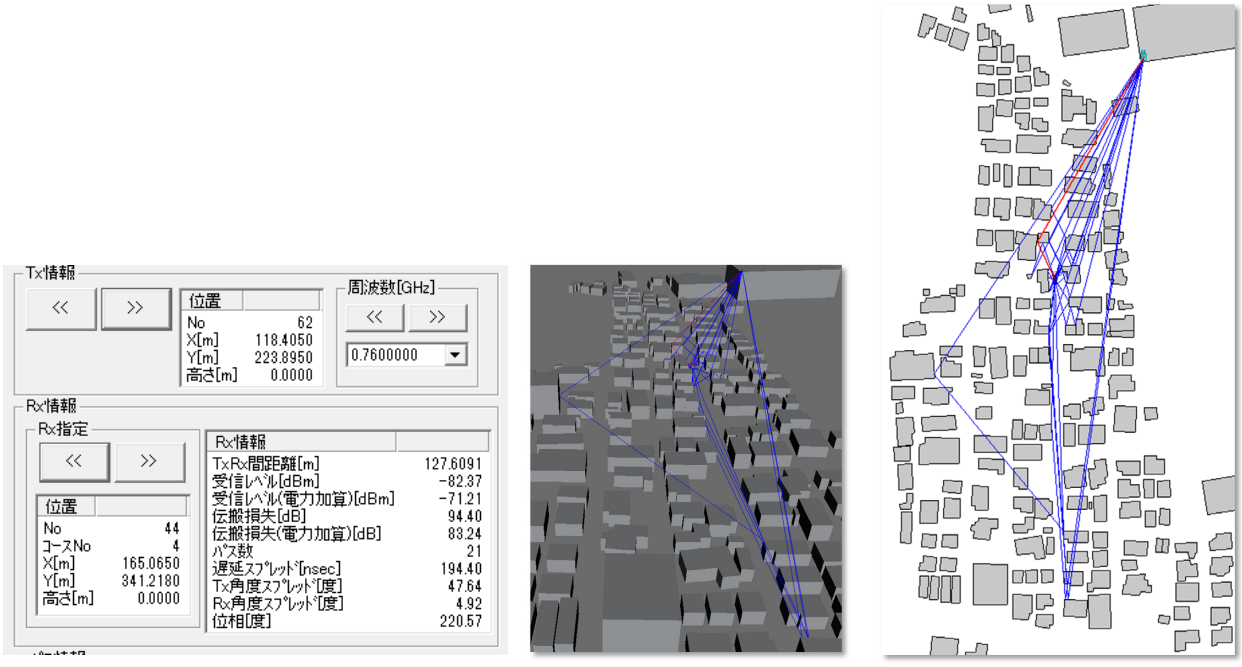


図 6　電波伝搬シミュレーションによるプライバシー漏えい解析

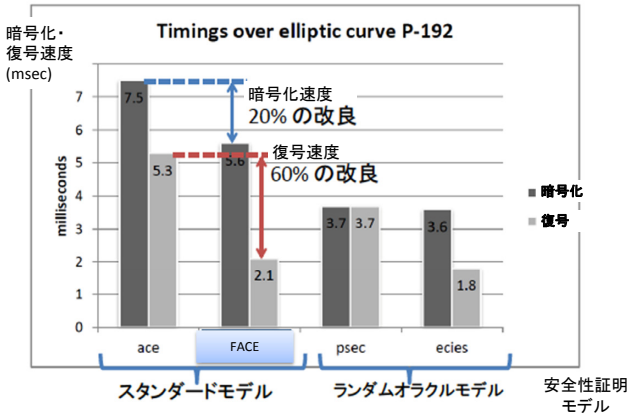


図 7　鍵共有方式 FACE と ISO/IEC 18033-2 他方式の比較

● **車車間／路車間通信におけるプライバシー漏えい解析**

総務省で実証実験を進めている 700 MHz 帯を使った車車間／路車間通信及び 315 MHz 帯を使ったタイヤ空気圧センサーシステムによる車両特定可能情報等のプライバシー漏えいの可能性を検討するため、電波伝播シミュレーションによる解析を行った（図 6）。

● **実用的な鍵共有方式（KEM）FACE の提案と国際標準化**

国際暗号標準 ISO/IEC 18033 -2 に採用されている方式よりも安全性、性能ともに優れた新しい公開鍵共有方式“FACE”を開発（図 7）、ISO/IEC JTC 1 /SC27 にて国際標準化に向けた活動を開始した。2015 年 10 月の会合で、ISO/IEC 18033 -2 への追補に記載する規格化作業を開始することで各国の合意が得られ、現在、規格化作業が進められている。

● **プライバシー検討 WG 立ち上げと PWS CUP 運営への参画**

パーソナルデータ利活用におけるプライバシー問題の解決に関する研究を立ち上げ、ワークショップを開催して様々な分野の有識者から知見を得るとともに、事例収集を行った。これを発展させてプライバシー検討 WG を発足し、第 4 期中長期計画に向けて連携する体制を整えた。また、ユーザのプライバシー意識を調査するアンケートシステムの構築を開始した。また、情報処理学会主催 プライバシーワークショップ（PWS）にて開催された PWS CUP（匿名加工処理や匿名加工データからの再識別処理を競うコンテスト）の運営に貢献した。

## 2.4　暗号安全性評価技術の高度化

● **離散対数問題ベースの公開鍵暗号方式（ペアリング暗号）の安全性評価**

暗号安全性評価の高度化では、クラウドコンピューティング等でのプライバシー保護機能が実現可能な「ペアリング暗号」の安全性評価を行うために、この暗号の安全性の根拠となっている離散対数問題の困難性を評価した。この結果、九州大学、富士通研究所と共同で 923 ビットの離散対数問題を解くことに世界で初めて成功、国際会議 ASIACRYPT2012 で採録されたほか、2012 年 6 月に報道発表を行った（図 8）。この成果は、秘匿データを利活用できる次世代暗号技術の実用化への道を拓く先駆的研究として、2013 年ドコモ・モバイル・サイエンス賞 先端技術部門 優秀賞、2012 年情報処理学会 喜安記念業績賞、2014 年電子情報通信学会業績賞を受賞した。また、この解読を契機に世界的に研究が進展した離散対数問題の解読動向について

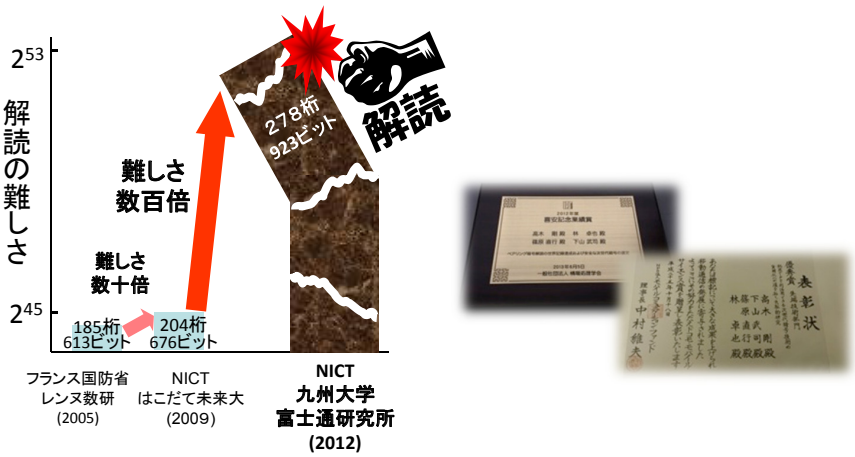


図 8　ペアリング暗号の安全性評価

調査を行い、電子政府推奨暗号への影響を盛り込んで CRYPTREC（Cryptography Research and Evaluation Committees）Report として発行、電子政府システムの安全性・信頼性向上に貢献した。

● **公開鍵検証システム XPIA（エクスピア）の構築と社会貢献**

インターネット上の SSL サーバの公開鍵証明書を収集した SSL Observatory のデータをもとに、RSA 暗号の秘密鍵が複数サーバで共有され、脆弱な状態になっている実態を把握するための安全性検証ツール XPIA（X.509 certificate Public-key Investigation and Analysis system, エクスピア）を開発し（図 9）、2013 年 10 月に報道発表した。この技術を（財）日本情報経済社会推進協会（JIPDEC）に技術移転し、電子署名・認証制度に基づいて運営されている電子入札、電子申請、電子契約等を支える認定認証業務（主務省：総務省・法務省・経済産業省）で使われている「自己署名証明書」について、上記の脆弱性による危険（秘密鍵が推定される可能性）がないことを確認し、2014 年 12 月に報道発表を行った。

● **CRYPTREC における電子政府推奨暗号リスト改定への貢献**

CRYPTREC は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であり、NICT は公的研究機関として世界最先端の暗号安全性評価技術を維持し、15 年以上本プロジェクトの運営を支える活動を行っている。特に、2003 年に発行された我が国の電子政府推奨暗号リストの 10 年ぶりのリスト改定に際し、リスト改定に必須となる評価対象暗号技術の安全性評価を行い、技術的根拠として提示するなど、総務省、経産省、IPA と連携して CRYPTREC 活動に学術面・事務局運営面双方から多大な貢献を行った。

## 3　むすび　今後に向けた展望

本稿では、第 3 期中長期計画においてセキュリティ基盤研究室で実施した主な研究開発項目とその成果概要を紹介した。詳細は 7 章の「セキュリティ基盤技術」の各項目をご覧いただきたい。他にも、本稿で紹介しきれなかった成果が数多くあり、研究室員の努力に敬意を表したい。研究成果のいくつかについては、論文等で発表するのみならず、プロトタイプ開発による検証、技術移転、国際標準化、社会貢献まで進めることができ、公的研究機関としての役割を担えたのではと考えている。今後は、IoT の展開に伴って生じる新たな社会ニーズに対応するための新たな機能を備えた暗号技術の研究開発を行うほか、継続して暗号技術の安全性評価を実施し、新たな暗号技術の普及・標準化に貢献するとともに、安心・安全な ICT システムの維持・構築に貢献していきたいと考えている。また、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い、適切なプライバシー対策を技術面から支援していきたい。

## 謝辞

第 3 期中長期計画の 2 年目より、田中秀磨氏（現在、防衛大学校准教授）から引き継いでセキュリティ基盤

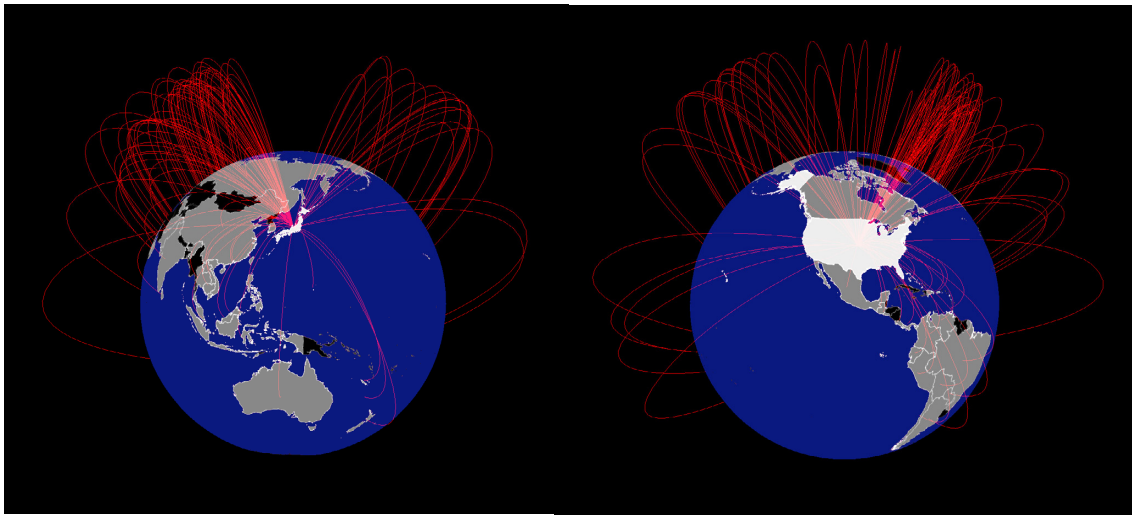

図 9　「XPIA」による脆弱性分布の表示例
（左図は日本側から、右図は米国側から見た図）
共通する素数（秘密鍵）が共有されて危険な状態になっている SSL サーバ間が、赤い線で結ばれている。

研究室の室長を務めさせていただく中、多くの方々に支えていただきました。特に、研究室のマネジメントを行って行く上で多くのご助言を頂きました平和昌所長、今瀬真理事に心より感謝申し上げます。また、室長着任時に円滑に立ち上げられるようご指導いただきました高橋幸雄前所長、企画室の皆様にも感謝申し上げます。また、セキュリティ基盤研究室の運営はグループアシスタントの高橋しおり氏、峯田友子氏の多大な貢献なくしてはありえず、室員全員の活力の源として活動を支えていただきました。ここに感謝の意を表します。

**盛合志帆**　（もりあい　しほ）
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（工学）
暗号技術、セキュリティ評価、
プライバシ保護技術