4　セキュリティ基盤技術
4　Security Fundamentals Technology

4-1　セキュリティ基盤技術の研究活動
4-1　Research Activity on Security Fundamentals Technology

田中秀磨
TANAKA Hidema

要旨

本稿では2006年度から2010年度に行われたセキュリティ基盤技術に関する研究活動を紹介する。

In this paper, we show the activity of research between 2006 and 2010 on security fundamentals technologies.

[キーワード]
セキュリティ基盤技術，暗号，数学，電磁波
Security fundamentals technology, Cryptography, Mathematics, Electromagnetic emanation

1　まえがき

セキュリティ基盤グループは、2005年1月に非常時通信グループを基にした情報通信セキュリティ研究センター発足時に構成グループの1つとして結成されたため、第2期中期計画期間の前から活動を始めている。第2期開始時の2006年4月に情報通信セキュリティ研究センターのグループ構成が改組されているが、セキュリティ基盤グループは名称及び構成員の変更がなされなかった唯一のグループである。2011年度から開始された第3期中期計画期間でもセキュリティ基盤研究室として活動が維持されている。研究テーマは暗号技術に関するものであり、通信インフラの安全性の根幹は暗号技術が担保しているため、その安全性維持のために継続した活動が最も重要である。国の通信の安心・安全を掲げるNICTとしては、セキュリティ基盤グループを維持することは活動の要と言える。

運営の特徴としては少人数である点が挙げられる。プロパー職員が最も多い期間でも3名（2010年度のみ）であり、大部分の期間が2名程度で運営された。短時間の有期研究員を含めても最大で13名であり、予算の半分程度が人件費として使用された。また構成員の特徴として電子政府推奨暗号評価プロジェクト（CRYPTREC）開始時から参画したメンバーを中心としている点もあり、電子政府推奨暗号の評価の継続性を維持してきたこともある。CRYPTRECは文献[1]に譲るが、総務省と経産省の共同プロジェクトであり、事務局がNICTと情報処理推進機構（IPA）に置かれたこともあって、当初から省庁横断的な活動を行ってきた。このため、事前の打ち合わせなどが複雑化し、研究活動以外の会議などにも多くの時間を割くこととなった。さらに暗号の安全性評価は多角的な評価を必要とするが研究員の専門性の違いや人員不足という問題があった。

暗号研究のテーマ設定においては学術的な見地で活動に意義があり、かつ一般にわかりやすく説明をするという難しい問題の解決に何度も直面することとなった。その時々における情勢によって方針や考え方、評価が大きく異なるため、第2期中期計画期間内だけでも同じ活動に対して首尾一貫とした説明にならないこともあったが結果的に

は研究活動は首尾一貫した方針を貫くことができた。一例として、CRYPTREC は、ただの事務局運営だけでなく、前述のように省庁横断の複雑な活動であった。しかしながら、暗号技術の危殆化問題や 2007 年頃からの省庁における暗号技術移行計画あたりから活動が存在感を示すようになり、研究成果の展開と CRYPTREC を結びつけて評価されるようになったので努力が報われた感がある。

研究の性格が数学に基づいたアルゴリズム研究であるため、それをわかりやすく説明するには常に苦渋を極めた。技術的な把握をした上で一般への説明を組み立てるべきであり、一般への説明理解止まりでの研究方針策定に大変な危惧を抱かざるを得ない。これはグループの問題というよりも、独立行政法人の方針決定や活動説明の在り方として今後解決していくべき課題であると言える。NICT 全体の横並び的な方針から研究分野ごとの性質に根差した方針への転換を提案したい。

このようにセキュリティ基盤グループの活動基盤は案外脆弱であり、順風とは言えない運営であった。研究活動の説明が困難であり理解を得るのが難しい一方で、後述するように NICT 内の他の活動と比較して、ほとんど予算を必要としない研究分野であったことが幸いである。また、専門に固執する集団であるとの偏見を多く受けたが、実際は他分野への挑戦や社会展開に意欲的な室員に恵まれ、労をいとわず貢献していただいた。本稿では 2006 年度から 2010 年度の活動の概要を紹介する。**2** では研究テーマごとの概要と成果、**3** では研究テーマごとに費やした予算の状況、**4** では人員構成の変遷を述べる

2　活動の概要

セキュリティ基盤グループの活動テーマは大きく 5 つに分類される。

1）数学的構造とアルゴリズム
2）暗号プロトコル
3）暗号技術安全性評価
4）電磁波セキュリティ
5）CRYPTREC

実際の研究活動は明確な切り分けは困難であり、そのような切り分けはナンセンスであるが、「1) 数学的構造とアルゴリズム」が活動の出発点である。数学的構造とアルゴリズムから、新たなセキュリティ機能の実現を目指した活動を行えば「2) 暗号プロトコル」の研究分野へ関わる。新たな安全性評価の手法の開発へ向かえば「3) 暗号技術安全性評価」となる。さらに電磁波測定技術との組み合わせにより「4) 電磁波セキュリティ」への活動へ進む。「5) CRYPTREC」は活動全体の集約点であり、安全性評価結果の展開だけでなく、新たな技術紹介やその動向調査なども行い、報告書を毎年発行している。一方で CRYPTREC 活動を通じて電子政府サービスにおける問題点の発見や議論から研究テーマを得ることもあった。電子署名法の指針改定や ID ベース暗号、耐量子計算機暗号アルゴリズム（Post Quantum Cryptography）は、そのような活動の一例と言える。主な活動を以下に示す。

1）数学的構造とアルゴリズム

代数、定理自動証明、素因数分解、離散対数問題などに取り組んだ。代数は暗号プリミティブの要素開発や高階差分攻撃など安全性評価への応用を行った。定理自動証明はプロトコルの安全性評価へ展開されている。素因数分解は公開鍵暗号 RSA-1024 の安全性評価の見積もり、離散対数問題は解ける問題の大きさにおける世界最高の結果を出した。

2）暗号プロトコル

研究成果が多用であり代表的なものに、proxy 再暗号化手法、匿名型パスワード式鍵交換スキーム（Anonymous Password based Authenticated Key Exchange： APAKE）、属性暗号及び準同型暗号、鍵情報の一部が漏洩しても安全性が損なわれない署名方式、署名データの構造を一定に保つことができる多重署名方式などが挙げられる。量子 ICT を仮定した量子秘密分散の開発なども行った。

3）暗号技術安全性評価

主に共通鍵暗号に対する安全性評価を行った。素因数分解や離散対数などの公開鍵暗号方式に関する安全性評価は研究の性格から数学的構造とアルゴリズムに分類している。ここでは主に 64 ビットブロック暗号の評価を行った。サイドチャネル攻撃も取り組み、特に故障利用攻撃の実行性検証を行った。また量子 ICT グループと連携し、量子鍵配送、量子雑音秘匿通信の安全性評価にも取り

組んだ。

4）電磁波セキュリティ

EMC グループとの連携活動であり、電磁波を介した情報漏洩とその対策技術開発を行った。特に画面情報漏洩（TEMPEST）に取り組み、開発した対策技術はベンチャー企業から製品化された。また、定量的評価手法や不要電磁波の測定手法はITU-T で国際標準に採用され勧告化された。電磁波セキュリティの総本山と呼ばれるまでに評価を高めたものの、国際標準化に一定の目途がついた2009 年度末を機に活動を終了した。

5）CRYPTREC

詳細は文献 [1] に譲るが、電子政府推奨暗号技術の評価結果の展開及び、電子政府における各種電子サービス仕様の調査を行い、安全性評価や適切な暗号選択のサポートを行う。

図 1 に純粋な研究活動ではない CRYPTREC 以外の論文数の推移を示す。論文数は国内発表から論文誌掲載までを区別することなく 1 件としてカウントしている。第 2 期中期計画初期は活動の基本となる数学的な分野における論文が多くを占め、徐々に暗号技術の応用でありシステム構築に関連のある暗号プロトコルの成果が増えていくことが分かる。暗号技術の安全性評価については定常的に成果を出しているが、2009 年度は安全性評価担当の研究者に対する CRYPTREC 作業の負荷が（体制の変更など）大きく、論文成果が少なかった。電磁波セキュリティの活動は上述のように 2009 年度で終了しているため、2010 年度には成果が無い。

研究テーマと予算用途

セキュリティ基盤グループは、数学的・理論的な研究を中心に実施し、研究成果が実験環境や機材よりも研究者の能力に依存するということから、予算の額に研究成果は依存しない傾向がある。研究活動における予算の主な用途は学会発表のための旅費である。例外的に電磁波セキュリティは実験が主であるため、そのための資材、装置試作、電波暗室の借用などがあった。また、全ての研究テーマで計算機シミュレーションを行うため、共用のサーバを 5 年間かけて構築している。また書籍購入も特徴的な予算用途である。5 年間で 4,000 冊の蔵書となり、そのための移動書架を構築した。ちなみに CRYPTREC 活動のための事務局運営に

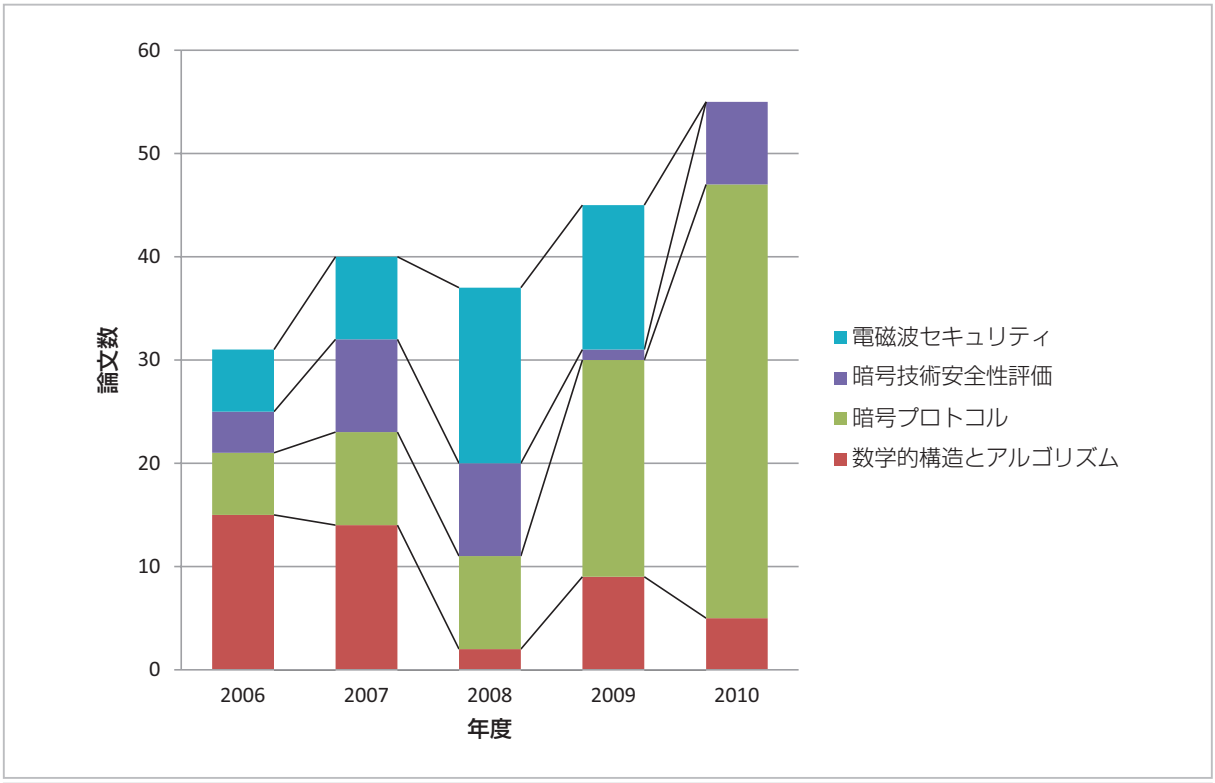

図 1　セキュリティ基盤グループ各プロジェクトの論文数の推移

は年間予算のおおよそ半分が使用されている。

結果的にセキュリティ基盤グループの予算は、電磁波セキュリティにおいて大規模な実験が必要な期間に多くを要したが、それ以外は論文成果数に依存することとなった。つまり、学術的成果が出ればそのための学会出張旅費が増えたからである。2007、2008年度は電磁波セキュリティにおいて実験及びITU-Tでの活動が活発な年であり、電磁波セキュリティで多くの予算を消費した。また、2009、2010年度はISO WG2において暗号プロトコル評価手法に関してエディタとして参画した期間であった。

3 研究テーマと室員の推移

図2にセキュリティ基盤グループのテーマ毎の人員数の推移を示す。前述のように特に数学構造とアルゴリズムは全員が関わっているテーマであるので、ここだけ切り出してカウントするのは適切ではないが、主にこの分野で成果を出す傾向が強かった。セキュリティ基盤グループのメンバーの転入出は頻繁であり、2008年5月に山村グループリーダー（当時）が秋田大学教授に転職するなど年度途中でのプロパー移籍や専攻研究員の着離任も多かった。そのため、人数のカウントは各年度の4月時点で行った。

セキュリティ基盤グループは、パーマネント職員が少ない状況で2008年4月末までは2名であった。2008年5月から2009年4月までは防災減災グループ滝澤グループリーダーの兼任と主任研究員（以下主任研）1名による構成であり、事実上の研究活動を担当したパーマネント職員が1名程度の期間があった。2010年4月から田中がグループリーダーを務めた。パーマネント職員として、2009年4月に松尾主任研、2010年4月に大久保主任研が着任した。両者とも民間企業からの着任であり、即戦力として研究成果だけでなく、グループ運営や多組織との連携活動など多くの貢献をしてきた。

専攻研究員は、年度平均すると7名在籍していた。外国人の在籍もあり、第2期期間で中国人1名、ベトナム人1名が常勤として在籍した。また、研修生として中国人1名を延べ8カ月程度受け入れた。

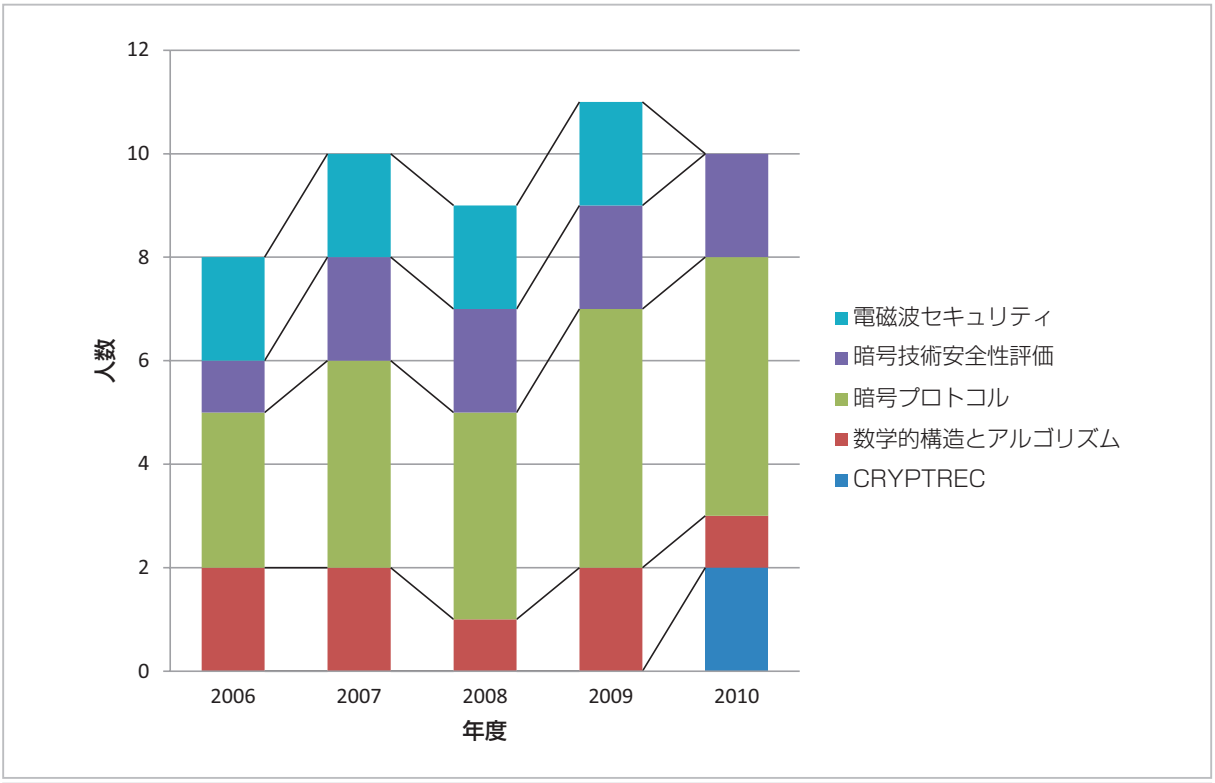

図2 セキュリティ基盤グループ各プロジェクトの人数の推移

テーマ毎に人員の割り当てを見ると、期首に比べると徐々に暗号プロトコルの人員が増強されているのが分かる。これは暗号プロトコルの研究が安全性評価と用途、実装性の組み合わせから様々なサブテーマが発生するため、多種多様な人材を要するからである。その他のテーマも人員を最低1名は割り当て、グループ全体として暗号技術研究分野に対してバランスの良い構成を心掛けた。しかしながら、ソフトウェア／ハードウェア実装技術、情報理論的安全性評価、量子情報理論など重要な分野で人材不足に悩まされた。

4　外部連携

セキュリティ基盤グループは外部の研究機関との活動も活発である。第2期期間では以下の共同研究契約のもとで活動を行った。

A)「ハッシュ関数の安全性評価に関する研究」
国立大学法人電気通信大学（2009年10月1日～2011年3月31日）

B)「安全性が離散対数問題に依存する暗号プロトコルの強度評価に関する研究」
公立はこだて未来大学（2009年2月9日～2011年3月31日）

C)「安全性が離散対数問題に依存する暗号プロトコルの強度評価に関する研究」
国立大学法人九州大学（2010年4月1日～2011年3月31日）

また、以下の大学／企業研究機関などと連携して研究活動を行った。

- 茨城大学　黒澤馨教授
- 筑波大学　岡本栄司教授
- 東京大学　國廣昇准教授
- 東京理科大学　金子敏信教授
- 立教大学　横山和弘教授、望月祐志教授
- 金沢大学　満保雅浩教授
- 富士通研究所　伊豆哲也氏
- 北京郵電大学　王励成講師
- 上海交通大学　曹珍富教授
- コロンビア大学　Moti Yung 教授
- スイス連邦工科大学 Zurich 校　David Basin 教授
- タリン工科大学　Ahto Buldas 教授
- パドヴァ大学　Antonio Assalini 教授

5　むすび

セキュリティ基盤グループの室員は1人当たり年に平均4件程度の学会発表を行っている計算であり、暗号技術の研究分野としては十分な学術成果を挙げていると言える。それだけでなくCRYPTRECを介した社会貢献を実効的なレベルで行い、予算規模から見て極めてコストパフォーマンスの高い活動を挙げていることが分かる。これが可能になったのは室員1人1人が研究者として高いレベルにあるだけでなく、高い意識を持っていたことに他ならない。まさに少数精鋭だったと言える。

また、CRYPTRECでの活動を契機にして、日本銀行金融研究所、日本データ通信協会、タイムスタンプビジネス協議会などとも暗号技術の安全性評価、暗号技術の移行に関する情報提供など幅広い活動する機会に恵まれた。さらにISOでは松尾主任研がエディタ／主査、ITU-Tでは関口専攻研究員が副ラポータを務めるなど国際標準の場でも活躍することができた。

暗号技術の研究分野は基礎研究活動のみに終始しがちであるが、社会貢献を念頭に入れ、公的研究機関としての役割を担ったことは我々の誇りとするところである。

謝辞

初代グループリーダーの秋田大学山村明弘教授にはグループの方針を明確にして頂き活動の基盤を構築してくださいました。大変感謝します。2代目グループリーダーの滝澤修マネージャーには2つのグループの管理という大変な負担の中でお世話になりました。韓太舜R&Dアドバイザー、小林欣吾R&Dアドバイザーにはネットワーク情報理論のセミナー開催など基礎理論の充実でお世話になりました。専攻研究員として在籍された田中三貴氏、関口秀紀氏、中里純二氏、田村仁氏、原山友弘氏、瀬戸信二氏、招聘専門員宮川寧夫氏、グループアシスタントの清水眞紀子氏には多大な貢献を頂きました。ここに感謝の意を表します。

参考文献

1 黒川貴司，金森祥子，“CRYPTREC 活動，” 情報通信研究機構季報，本特集号，4-9, 2011.

（平成 23 年 6 月 15 日 採録）

田中秀磨（たなかひでま）
ネットワーク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）
情報セキュリティ、暗号技術、情報理論