4-4　暗号プロトコルの研究活動 ―標準化及び外部との共同研究―

4-4 Researches on Cryptographic Protocols —Standardization and Global Collaborations—

松尾真一郎　大久保美也子
MATSUO Shin'ichiro and OHKUBO Miyako

要旨

暗号技術は、情報通信システムにおけるセキュリティを守る基盤技術であるが、一方で情報通信システムにおいては単独で使われることは少なく、通信プロトコルの中で組み合わせられて使われることがほとんどである。このように通信プロトコルの中で使われた場合におけるセキュリティの検証方法やセキュリティレベルの設定においては、研究者が単独で研究するだけでなく、国際的な合意形成を図るために、国際的な連携研究や、その結果としての標準化が重要になる。そこで、本稿では第２期中期計画において、暗号プロトコルの研究において行われた標準化、および連携研究について示す。

Cryptography is fundamental technique to achieve security property in information systems. It is not only used alone, also used as combinations of cryptography and communication in communication protocol. Thus, methods for verification of cryptographic protocols and setting security levels become important research. Then they also requested to be done by global collaboration and used through standardization to achieve international consensus. This article describes standardization activities and international collaborations in researches on cryptographic protocols in the second mid-term plan.

[キーワード]
暗号プロトコル，軽量暗号技術，プロトコル検証，標準化，国際連携
Cryptographic Protocol, Light-weight Cryptography, Verification of Cryptographic Protocol, Standardization, International Cooperation

1　はじめに

暗号技術は、インターネット上で送受信される情報を守る目的をはじめとして、様々な情報の安全性を確保する目的、ネットワークサービスの利用者の認証、さらに応用的な目的として電子マネーや電子投票など、より高度なサービスを行うために多くの研究開発が行われている。

暗号技術は、暗号化や復号のためのアルゴリズムを単独で使う場合よりも、通信プロトコルの一部として、暗号化処理、復号処理、通信などが組み合わさって構成される場合がほとんどである。このような組み合わせを、以下では暗号プロトコルと呼ぶことにする。暗号プロトコルは、NICTのような公的な研究機関だけではなく、大学や民間企業などで広く研究されており、日々新しい暗号プロトコルが提案され、実装される。一方で、そのような様々な暗号プロトコルの安全性を客観的に評価する方法は、技術的にも制度的にも、まだ十分に確立されているとは言えない。技術面では、暗号プロトコルの安全性についての厳密な理論の研究が本格化したのが2002年からであり、その理論については未確立であり、また第三者から客観的に見て合意が取れる方法が確立されていないのが現状である。同様に、暗号プロトコルの安全性について、誰がどのように検証を行い、その安全性の判断を行うのかという制度面の検討も十分には行われていない。上記のような技術的な

客観性や、制度的な公平性を担保するためには、公的な研究機関が中心となった検討が必要であり、一方で暗号プロトコルの主要な提案者である大学や民間の研究者との連携が不可欠である。もちろん、暗号技術は国際標準化機関によって精査され、標準化された技術が、実際に実装されて広く使われることから、国際的な連携や、標準化活動への貢献が重要となる。

そこで、本稿では、日本の公的研究機関であるNICTとして、第2期中期計画期間に、暗号プロトコルの研究おいてどのような外部連携と標準化活動を行い、どのような成果を得たのかという点を示す。

2　暗号技術の国際標準化への貢献

2.1　ISOの標準化に対する貢献

暗号技術の標準化は、主にISO/IEC JTC1 SC27と、IETFにおいて実施されている。ITU-Tでは、暗号技術そのものの標準化は主体的に行っておらず、基本的にはISO/IEC JTC1によって定められた暗号技術を参照している。このうち、IETFに関しては、Webにおける暗号通信の代表的な規格であるSSLなどを始めとして多くの実用的な暗号プロトコルが標準化されているが、その標準化過程では、厳密な意味での安全性に関する議論が十分ではない。一方でISO/IEC JTC1における標準化過程では、安全性評価の学術論文など、理論的な意味での安全性を考慮した標準化の議論を行っている。そのため、NICTでは自らの暗号プロトコルにおける学術的研究成果の展開として、ISO/IEC JTC1を中心に活動を行った。

ISO/IECにおける暗号技術の標準化はJTC1 SC27で行われている。SC27には、5つのワーキンググループ（WG）が存在するが、暗号技術と暗号プロトコルの技術的な議論はWG2で、安全性評価の方法についてはWG3で標準化が行われている。

WG2の活動においては、匿名性を保ちながらエンティティ認証を行う匿名エンティティ認証プロトコルの標準化（ISO/IEC 20009-2）が2010年5月から開始されているが、筆者がこの規格のプロジェクトエディタを務めている。匿名エンティティ認証プロトコルは、電子投票などの匿名性を必要とするアプリケーションへの応用が代表例であるが、今後クラウドコンピューティングが普及するにつれて利用が広がる基本的な技術である。現在、代表的な技術であるグループ署名を用いたエンティティ認証プロトコルを中心に標準化を進めている。また、WG2については、筆者が日本の国内委員会の主査としても活動を行っており、国際標準化会合における日本代表としての職務を行っている。

さらにWG3においては、**3.2.3**で述べるような形式化手法を用いた暗号プロトコルの安全性検証について、Verification of Cryptographic Protocols（ISO/IEC 29128）の標準化を筆者がエディタとして実施している。この規格は、2012年を目途に標準化が完了する予定である。

2.2　米国標準暗号技術の制定に対する貢献

2004年に、暗号プロトコルの中で広く標準的に使われている基本技術であるハッシュ関数の一種であり、米国標準でもあるSHA-1の安全性を脅かす攻撃方法が発表された[1]。この発表を受けて、米国の技術標準を定めるNISTは、2007年からSHA-1の代わりとなる新しいハッシュ関数を世界中から公募することによって選定する作業を始めた。

NICTでは、日本における電子政府推奨暗号に向けた評価作業を行っているが、米国NISTが制定する暗号技術が、事実上国際標準となる暗号技術になる可能性があり、その関係が密接であるだけでなく、日本の電子政府でも将来利用されることが十分に考えられる。しかしこの場合、米国における標準暗号の選定における技術評価基準が、日本の電子政府での利用を考えた場合の技術評価基準と異なる場合、日本における評価をやり直さなければいけないだけでなく、国際的な不整合を起こす可能性が出てくる。そのため、米国における選定作業の中で利用される技術評価基準に対して、筆者が中心となり日本の電子政府における要件を考慮するように提言を行った。

具体的には、日本の電子政府システムにおいては、電子署名の機能を持ったICカードが広く使われており、このような暗号プロトコルにおける使い方を考慮して、ICカードを中心としたハードウェア実装における評価方法の提案を行った。こ

の中では、暗号評価を行う共通プラットフォームとして、独立行政法人産業技術総合研究所のSASEBO-GⅡボードを用いるとともに、このボードの上で公平かつ客観的な評価を行うためのモジュールの実装方法を定めた。また、この共通プラットフォームと実装方法に基づいて、米国のハッシュ関数公募で第2ラウンドに残った14アルゴリズムについて実装結果をとりまとめた[2]。

先述したように、暗号技術、暗号プロトコルの評価は、国際的な観点で客観的かつ公平なものでなくてはいけない。そのために、この評価は日本だけでなく、米国Virginia工科大学、ベルギー・ルーベンカトリック大学といった、暗号技術のハードウェア実装で世界最先端を行く大学と共同検討を行った。筆者はこの共同検討において、評価対象プラットフォームの設定の統括を行うとともに、3か国にまたがる研究プロジェクトのマネジメントを担当した。その結果は、ハードウェア実装に関する国際会議や、国際的なジャーナルで発表するとともに、2010年8月に行われたNIST主催のSHA-3 Candidate Conferenceにおいて発表し、NISTにおけるハッシュ関数評価基準に対して十分な提言を行うことができた。

3　暗号プロトコル研究における外部連携

3.1　より高度な攻撃に対する研究における共同研究

3.1.1　目的

暗号技術、暗号プロトコルの研究においては、従来はサービス利用者などが暗号処理に関する秘密情報（秘密鍵など）を、第三者が知ることができないように安全に管理されていることが前提である。そのため、このような秘密情報はICカードのような耐タンパデバイス（中身をのぞき見ようとすると内容が消えるなどの機能を持ったデバイス）に格納することが通常である。

一方で、このようなデバイスの耐タンパ性自体に対する研究が近年進んでおり、ある程度の時間を掛けることで、上記の秘密情報の一部を攻撃者が入手できることが広く知られ始めている[3]。このような攻撃に対する対処としては、デバイスの耐タンパ性を高度化する方法や、暗号プロトコル自体に秘密情報の一部が漏れても安全性を保つ機能を加える方法がある。この共同研究では、後者のアプローチの研究を実施した。秘密情報の一部が漏れても安全性を保つ暗号プロトコルの研究は2008年から世界的にも本格的に実施されるようになっているが、現実のアプリケーションやデバイスの状況に適合した安全性理論はまだ確立されていない。そこで、特にこのような攻撃を受けやすいRFIDタグや携帯電話などを利用した暗号プロトコルをターゲットとして、安全性モデルの研究を進めるとともに、証明可能な安全性を持つ認証プロトコルの検討を行った。この研究を行うにあたり、当該分野の世界的な権威であるコロンビア大学との共同研究を行った。

3.1.2　共同研究の内容と結果

このテーマにおいては、2つの研究を行った。

1つは、RFIDにおけるIDを認証する暗号プロトコルにおいて、一定割合の秘密情報の漏洩があったとしても安全性を保つ暗号プロトコルの研究を行った。このような暗号プロトコルを設計するにあたって特に考慮する必要があるのは、RFIDタグにおいては実装できる回路規模の制約から非常に制限された暗号処理しか実装することができないという点である。そのため、AESのような疑似ランダム関数として取り扱えるアルゴリズムのみを組み合わせたプロトコルを構成した。さらに、このプロトコルが対象とする新たな安全性モデルを提案した。

この安全性モデルでは、攻撃者が実行可能な攻撃を従来よりも厳密に定義した。すなわち、RFIDにおける認証プロトコルにおけるセキュリティ要件について、以下の2つを対象とした。

- タグの偽造に関する安全性：RFIDタグとRFIDリーダーの間の通信を盗聴し、次回の認証において認証が成功するRFIDタグを偽造する攻撃。RFIDタグの秘密情報に対する攻撃は時間が掛かってしまうとシステムによって発見されてしまうため、時間が許す範囲の一部の情報のみを得られるとする。
- プライバシに関する安全性：RFIDタグからの過去の出力を収集して、RFIDタグ所有者の行動を追跡する攻撃。プライバシに対する攻撃では、攻撃者は無限の時間を使っても良く、システムによる発見をされても攻撃が継続できるた

め、RFIDタグの中の秘密情報はすべて得ることができる。

以上の特徴を持った安全性モデルを提案し、査読付き国際会議RFIDSec2010において発表を行った。

もう1つのテーマは、電子署名に利用する秘密情報（署名鍵）の一部が漏洩しても、漏洩前後の署名の安全性を損なうことのないプロトコルの設計である。電子署名方式においても、秘密鍵の管理は安全性の前提となっており、電子政府システムなどではICカードに格納されているケースが多いが、前述の理由によりこれらの鍵の一部が漏洩することは十分に考えられる。このような攻撃を考慮し、秘密情報を電子署名を作成するデバイスと、別のHelperと呼ばれるデバイス（例えば携帯電話）などに分けて格納し、それぞれの秘密情報が漏洩しても問題がないプロトコルとした。このプロトコルについても、安全性モデル、実現プロトコル、数学的な安全性証明を行い、査読付き国際会議Intrust2010において発表を行った[5]。

3.2 軽量暗号プロトコルに関する連携

3.2.1 軽量認証方式と形式的検証手法

暗号を現実の世界で活用するためには、考慮すべきことが多々ある。利用される環境によっては、暗号アルゴリズムが（その安全性を証明するために）想定している環境が満たされない場合や利用する媒体が想定する計算能力を持たないことも考えられる。

近年は、ネットワークを介したコミュニケーションがデスクトップPCのように物理的に動かない環境で固定されたネットワークによりつながれているものばかりではなく、携帯電話のように通信媒体自体がその物理的に存在する位置が変わり、またそのことにより通信時の環境も変わる、というようなシーンも登場するようになった。また、いわゆる携帯電話のような組み込み機器は、安価にコンパクトに物理的形状が構成されることが求められる場合が多く、そのような場合、従来暗号アルゴリズムを動かす媒体として想定していたデスクトップPCが持ち得るほどの演算能力を物理的に持ちえないケース、というのも存在し得る。このような、近年の通信環境の大きな変化に沿いながら、適切な暗号技術の導入に向けた研究の顕著な動向の1つとして、通信媒体としてRFIDを利用するシーンに関する研究が進められている。

また、これまで暗号の安全性は多くの場合、それぞれの場合について個別に示されてきた。これに対し、形式的検証の知見を活かし、安全性証明などにその手法を活用することにより、個別に示される証明の場合に起こり得る誤りを排除するとともに、安全性証明を（ある程度）自動的に行うことを目指した研究も活発になってきている。

上記動向を踏まえ、組み込み機器へ適用する暗号プロトコルなどを検討していた我々のグループと暗号プロトコルへの形式的検証手法の適用に対する深い知見のある電気通信大学との連携によりこの度の結果を得ることができた。以下ではその概要を紹介する。

3.2.2 軽量認証方式

組み込み機器は多くの場合その通信を無線によるものが多い。想定するプレイヤーとしては、通信媒体となる組み込み機器とそれを受信する側のサーバの2者としてとらえることができる。軽量認証方式は、このような組み込み機器とサーバの2者間で実行されるプロトコルとして示すことができる。

組み込み機器の典型的な一例としてRFIDを想定する。RFIDには大別して自ら電力源を持ちうるアクティブタグと呼ばれるものと、無線通信路により外部から供給される電力により処理を行うパッシブタグと呼ばれるものがあるが、検討では、物理的により厳しい条件となるパッシブタグを想定した。一般的に、（パッシブ）タグは大量に流通されることが考えられ、安価に製造し得ることが望まれる。それに伴い、タグ内に搭載し得るゲート数は制約を受ける。このようなゲート数の制約やシステムが要求する処理時間を加味すると、RFIDタグに搭載し得る暗号回路はかなり小さなゲート数で処理可能な演算のみで構成されるものに限られる。一般的に、公開鍵系の暗号回路は多くのゲート数を必要とし、またその処理時間もある程度の時間を要する。一方、共通鍵系の暗号回路は比較的少ないゲート数で構成することができ、処理も高速であることから組み込み機器の物理的制約条件がある場合などに適しているといえる。

RFID向けの認証プロトコルは、一般的な認証プロトコルの安全性を満たすための条件として挙げられる、なりすまし耐性に加え、プライバシへの配慮がケアされることが望ましい。これは、RFIDのような組み込み機器はその通信が行われる際の物理的なロケーションが一定でないこと、通信が無線を介して行われること等から、これまで固定の場所からのデスクトップPCなどを用いた場合におけるサーバとの通信ではケアする必要がなかった点にも配慮する必要が出てきたからである。

例えば、不用意に行動追跡が可能であったり、RFIDタグとサーバ間の通信から読み取れる情報からRFIDタグもしくはそれを所持しているユーザの何らかの情報を、意図しない盗聴者が盗み取ることが可能であるような状況は防止されることが好ましい。また、安価に製造されるタグは、容易に入手可能であり、またタグを分解するなどして内部に記録されている情報は容易に取り出されることも想定した上で、安全に認証が行えるようなプロトコルが好ましいと考えられる。

3.2.3　形式的検証手法

近年、形式手法を暗号プロトコルの公募に活用する動きがある。CRYPTRECによる電子政府推奨暗号リストの改訂[7]では、(相互)認証プロトコルが公募され、現在、選定作業が行われている。その公募要件の1つとして、形式手法により安全性が検証可能であることが挙げられている。暗号システムの安全性を証明する方法の1つに、ゲーム列による検証がある。ゲーム列による検証では、攻撃の状況を攻撃者と挑戦者間で行われるゲームとして、攻撃者に許す戦略、方式設計者の目標を明確に定義する。B. Blanchetらは、暗号システムの安全性をゲーム列で検証するソフトウェアツールCryptoVerifを開発している。CryptoVerifを用いた検証では、Blanchetのプロセス計算[6]で攻撃モデルと書き換え規則を記述し、攻撃モデルを書き換え規則に従って変換して、安全性が成立するモデルに変換可能か評価する。攻撃モデルは、攻撃者が呼び出し可能なオラクルをプロセスで記述し、それらを組み合わせて表現する。書き換え規則は、観測等価性を満たす2つのプロセスで記述される。大雑把に言うと、プロセスへの入出力など観測可能な値からは、無視できる程度の確率でしか2つのプロセスを識別できない時、観測等価性を満たすという。CryptoVerifでは、プロセスに入力された値や計算された値は、配列として記録され、別のプロセスで記録された値を呼び出し、利用することができる。ただし、値を呼び出す場合、配列のインデックスを直接指定する操作は禁止されており、条件に一致する要素を経由して指定するなど、間接的にしか操作できないよう制約されている。

CryptVerifのような形式検証手法を暗号プロトコルの安全性証明に導入することは従来から行われていた個別に証明を検討する場合に比べ結果の確かさを向上させることが出来、また着実な検討を行うことに有効な手段として期待できる。

3.2.4　提案方法

我々は、**3.2.2**で示したRFIDのような組み込み機器とサーバの2者間で取り交わされる場合に特にケアすべき安全性要件を満たす方式を提案した(図1参照)[8]。

また、提案方式に対し、**3.2.3**で示した形式的検証手法を適用し、その安全性を証明したい。具体的な安全性証明は、形式的検証手法による出力結果と従来から用いられている個別に安全性証明を行う方法とを組み合わせて適用し、最終的に提案プロトコルが安全であることを示している。

3.2.5　今後の展望

ここで示した提案プロトコルは組み込み機器対サーバの2者間の通信にとどまらず、組み込み機器同士の認証への応用なども考えられ得る。しばしば、暗号プロトコルを構成する際に、実際の利用環境とかい離した利用環境を想定して構成されてしまうことがある。このような場合、実際の環境で利用した場合にその安全性を保つことができないというようなことも起こり得てしまう。よってできる限り現実とのかい離が少ない環境を想定した上でプロトコルを構成することが望まれる。特に、組み込み機器などの媒体を用いる場合には物理的制約条件などが直接的にその安全性を脅かしやすい。我々は提案方式を検討する際に、このような点に特に重きを置き方式の構成を検討した。

また、提案方式の安全性を証明するために形式的検証手法を適用したが、このような安全性証明の示し方は、従来のように個別のプロトコルに証明を与える手法に対して大変有効であり、安全性

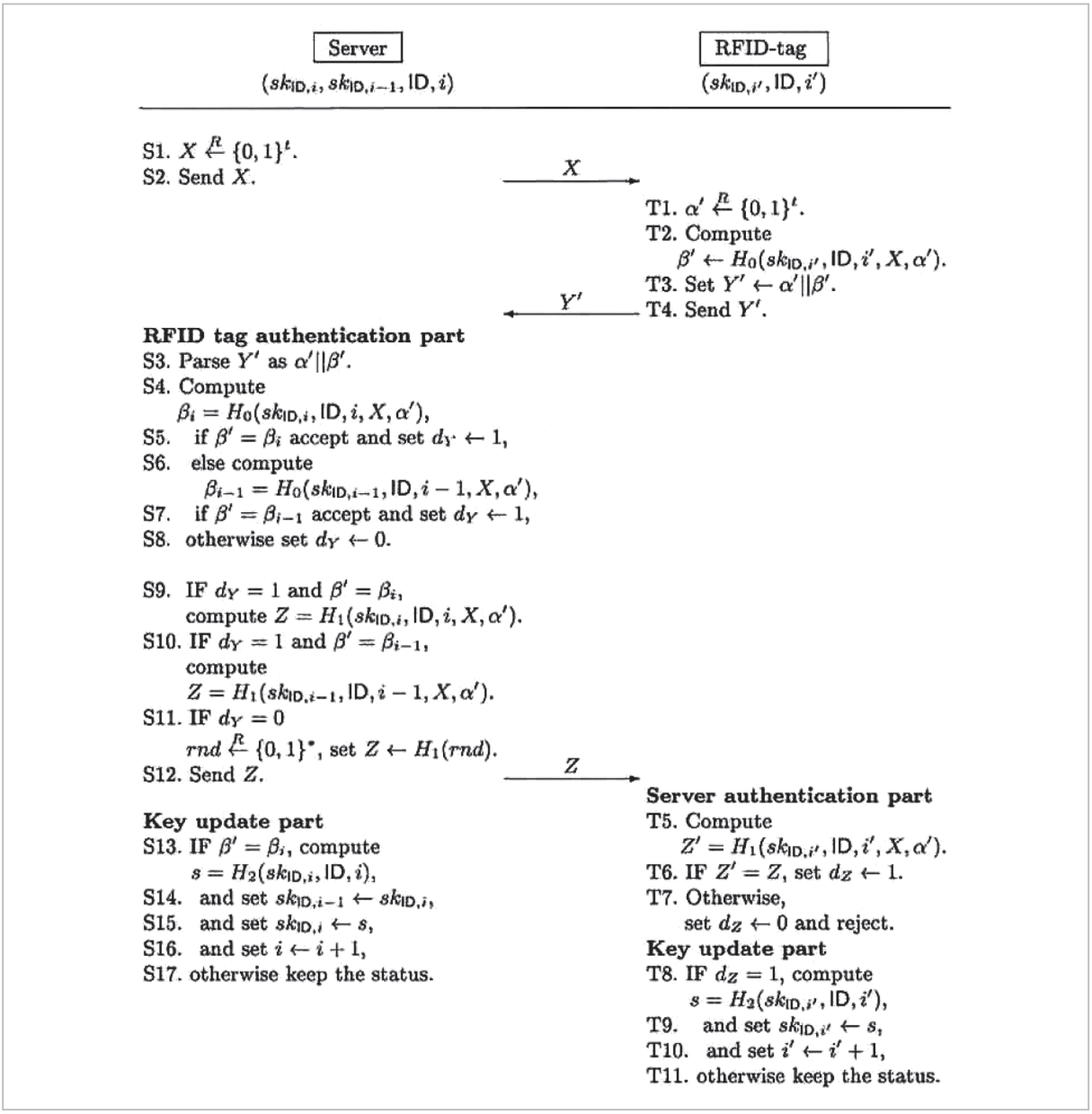


図 1 軽量相互認証プロトコルの構成

証明のプロセスの中での誤りを軽減し、効率的にその安全性を示すことができるようになる。我々が用いたCryptoVerifを用いた形式的検証手法を導入した安全性証明のプロセスは、提案プロトコルに似た状況である暗号プロトコルなどへの応用が期待できる。

3.3 現実的なシステムにおける暗号プロトコルに求められる要件についての連携

3.3.1 連携の目的

インターネットの発展とともに、インターネットを介して利便性の高いサービスを安全に実行するために、様々な暗号プロトコルに関する研究や実装が行われている。例えば、電子マネーや電子投票などはその例である。これらの研究では、現実的なセキュリティ要件を満たすプロトコルから、研究の観点で想定し得る全ての安全性に対する脅威に対応するための（安全性の観点で）究極的なプロトコルに至るまで、様々な角度で研究がなされている。

（学術的に）十分なセキュリティを有する暗号プロトコルの研究が盛んになされている一方で、そ

れらのプロトコルが現実に社会に実装されて利用されるケースは少ない。社会実装される前段階として、想定される脅威について非常に慎重な議論が交わされる一方で、社会的に必要とされる性能要件や、経済的に合理性を持った運用要件などを満たす最適解を導出することができないことが大きな原因であると考えられる。

諸外国において暗号技術や暗号プロトコルを応用したサービスが展開される一方、暗号技術の研究では世界をリードする日本においてその研究成果を社会実装に結びつけられていないとすれば、それは大きな問題である。例えば、日本においてはGPKIや公的個人認証サービスを始めとして、暗号や電子署名といった基本的な暗号処理のための基盤が整備されながら、それらの基盤を活用するアプリケーションの利用は伸び悩んでおり、その鍵となる住民基本台帳カードの発行枚数も伸びていない。また、90年代より、従来の現金に置き換わる電子マネーの研究や、インターネットで選挙が可能になる電子投票プロトコルの研究も盛んに行われている。しかし広く使われている電子マネーのサービスは従来の現金よりも軽いセキュリティ要件に基づく技術であり、電子投票においては投票所タイプの電子投票の実験が過去に行われたが情報システム的における問題で実験が進まず、インターネット投票を実現するにはまだまだ道半ばという状況である。

そこで、暗号プロトコルにおける先端的な研究と、社会実装に適した技術の構築という観点で、「最適解」を導出するための取り組みが必要であり、そのために暗号プロトコルの研究を社会に反映させていく方法を考えることが重要である。そこで、本調査・研究では、社会に実装される暗号プロトコル研究を行うための指針を得ることを目的とした。

3.3.2　連携の内容

本研究では、社会実装に適した暗号プロトコルを研究すると同時に社会実装を促進する「最適解」を求めるための指針を少しでも得るべく、暗号プロトコルの社会実装という観点で世界的にも最先端を進んでいるエストニアにおいて、どのように社会実装される暗号プロトコルが検討され、それがどのように市民に受け入れられ、どのような問題が認識されて、どのように解決したのかについてのベストプラクティスを調査した。

日本において活用が進んでいない（国民的）PKIについては、エストニアにおいてほぼ全国民が利用しており、特にインターネット投票についてもエストニアでは3度の大規模なインターネット投票を実施している。インターネット投票を中心に基盤となるPKIも含め、エストニアでの検討、実施、課題解決の状況を調査し、日本における状況と比較することで、将来の日本における社会実装に対して、暗号プロトコル研究において考慮すべき点を提言した。

本調査は、エストニアにおける電子政府向けの暗号・認証システム研究の中心人物である、タリン工科大学のAhto Buldas教授、および電子政府向け暗号・認証システムの設計を行っているCybernetica社の研究者との議論を通じて実施した。議論は、平成22年12月6～19日まで、研究実施者がエストニアを訪問して、現地において実施した。

3.3.3　連携の成果

まず、エストニアにおけるIDカード国民・PKIシステムの調査、および電子投票システムの調査と、日本におけるPKI、電子投票との比較を行った。

IDカード・国民PKIシステムにおいては、エストニアにおいては罰則規定はないものの、ほぼ全ての国民がIDカードを所有している。これは、IDカードが政府のみならず、銀行からも強くサポートされていること、開発環境が公開されており民間企業がIDカードを活用するためのハードルがきわめて低い。さらに、様々なアプリケーションが存在することによって、IDカード自体の利用のメリットが大きく、それが普及への鍵となっている。アプリケーションにおける連携についても活発に行われており、2011年には運転免許の取得状況とIDカードの情報のリンクが取られるため、IDカードを所持していれば運転免許証の携帯が不要となる予定である。このように、IDカードを様々な利用シーンにおける認証のインフラとして積極的に活用する意思が強いと言える。一方で、プライバシ保護に関する事項についてはエストニアにおいて特別な事情があった。日本において認証に必要な共通IDを広く民間にも開放する場合、行動の把握などプライバシに関わる問題が懸念さ

れた。しかし、エストニア国民自体が、IDカード導入の時点ではプライバシ保護の問題に対して強い関心を持っておらず、そのため高い利便性を提供するIDカードが急速に普及したといえる。ただし、近年IDカードの利用において、プライバシに関する問題を指摘する専門家が現れており、IDカード利用におけるプライバシ問題が政府内でも議論され始めている。現状、プライバシ保護に関するコンセンサスは得られていないとのことであるが、現在のIDカードの体系にどのようにプライバシ保護機能を付加していくのかが議論の対象になると考えられている。

電子投票においては、エストニアで起こったことの大きな特徴は、投票所タイプなどの中間解を経ずに、最初からインターネット投票を実施することを決めたことである。これは、電子投票の目的として、投票集計に関するコスト削減だけでなく、投票率の向上が民主主義の質の向上につながるという点を大きく掲げたことに関係する。さらに、暗号プロトコルの設計という観点においては、既存のシステムとの互換性など、社会実装の観点から「既存の仕組みで行えるセキュリティ対策はその対策をそのまま活用し、新たに暗号技術が必要となる部分にのみ暗号プロトコルを適用する」という考え方を採ったことが特徴的である。インターネット投票に関する安全性要件は、「投票権を持たない人の投票の禁止」、「二重投票の禁止」、「匿名性の確保」、「票の買収の排除」などがある。票の買収の排除に関しては、投票のやり直しを認めることにより買収を企てる攻撃者にとってのメリットを大幅に削減した。また、匿名性の確保においては、Mix-net [9] のような複雑なシステムを採用せずに、運用者の行動の録画を含めて監視できるような運用対処を行っている。その結果、暗号に関わる処理が必要なのは、投票データの暗号化と投票権の確認のための電子署名のみとなっている。電子署名そのものも、IDカードのインフラをそのまま流用できるために、電子投票システム構築に関わるコストを大幅に削減することに成功している。結果として、このような軽い暗号プロトコルにすることにより、集計処理全体は10万人規模の投票でも20分を切っている。さらにエストニア国民が、中央のサーバの信頼に大きく依存する（暗号学者にとっては安全性の根拠としての仮定が強すぎ、安全性の根拠が現実的ではない）システムを受け入れた大きな理由も、プロトコルのシンプルさにある。システム管理者が不正を行わないことを、監査やビデオ撮影によって担保する（不正なシステム管理者の不正行為に対するインセンティブを低下させる）という工夫がある。Mix-netのような複雑な仕組みは一般の国民には理解しづらいという意見も多く存在した。仮に、Mix-net、ブラインド署名、準同形暗号のような特別なプロトコルを導入した場合、既存のIDカードのインフラやPKIのインフラのみでは、そのような処理を賄うことができずに、追加のシステム構築と運用の費用がかかることになる。問題が発生したら紙の投票にいつでも立ち戻ることができるという工夫を含めて、極力既存のインフラとの親和性を保つことが重要であることがわかる。

上記の調査・研究から、社会実装に適した暗号プロトコルの研究開発の遂行に向けた提言を行った。社会実装に適した暗号プロトコルは、(1) 既存のサービスを提供するインフラとの親和性、(2) 利用者に理解しやすいシンプルさ、(3) 追加のシステム構築コストを発生させないようなシンプルさが重要なポイントとなる。それらのポイントを満たすためには、複雑な暗号プロトコルを設計するのではなく、必要なセキュリティ要件のうち既存のインフラや運用を活用することによって暗号技術の利用が不要なものについては、そのようなセキュリティ対策を採用するということが重要になる。例えば、エストニアのインターネット投票の例を見ると、投票内容の変更を認めることにより票の買収を企てる攻撃者のインセンティブを低下させたり、運用のビデオ撮影や監査のこまめな実施により、運用者の内部犯行のインセンティブを低下させるシステム設計となっている。このように、攻撃者のインセンティブを分析して、様々なセキュリティ対策によってそのインセンティブを低下させることが大きなポイントとなる。暗号プロトコル研究の世界では、2002年頃からゲーム理論に基づく安全性モデルの研究が盛んになっている。既存の研究の多くは、暗号プロトコルという狭い領域に閉じた中で厳密な安全性定義を試みている。しかし、社会実装に必要な暗号プロトコルの設計においては、サービスで必要とされるセキュリティ要件と攻撃者のインセンティブを入力

として、ゲーム理論的な観点でリスク分析を実施し、既存の対策によって攻撃者のインセンティブの低下を図れない部分について、暗号技術的解決を行うというアプローチが有効であると考えられる。

エストニアのインターネット投票については、2007年にBuldasらによってゲーム理論的なアプローチで安全性の分析が行われている。エストニアのインターネット投票の基本的なスキームの設計において、前もって学術的な体系をもってゲーム理論的なセキュリティ設計が行われたわけではないようであるが、実際に設計されたシステムは、前述の考え方おいて（結果的に）合理的な設計となっていると考えられる。今後の暗号プロトコルのセキュリティ要件の抽出において、システム設計におけるゲーム理論的リスク分析のような考え方の体系化と実践が重要になってくると考えられる。

4　まとめ

本稿では、情報通信システムにおけるセキュリティを確保するための主要技術である暗号プロトコルの研究において、標準化、および国内外の研究機関との連携の成果について、ISO標準化、米国標準選定への貢献、より強い攻撃者や現実的な攻撃への対応などについての国際連携状況を述べた。暗号プロトコルの安全性基準を定めること、および安全な技術を構成するためには、国際的な合意と連携が不可欠であり、NICTでは今後もこのような活動を継続的に行っていく予定である。

謝辞

本研究について、ご議論頂いた電気通信大学太田和夫教授、崎山一男准教授、花谷嘉一氏に深く感謝します。

参考文献

1 Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu, “Collisions for Has Functions MD4, MD5, HAVAL-128 and RIPEMD”, IACR Eprint archive 2004/199, Aug. 2004.

2 Shin'ichiro Matsuo, Miroslav Kneoevi¢, Patrick Schaumont, Ingrid Verbauwhede, Akashi Satoh, Kazuo Sakiyama, and Kazuo Ota, “How Can We Conduct Fair and Consistent Hardware Evaluation for SHA-3 Candidate? ,” NIST SHA-3 Candidates Conference, 2010.

3 本間尚文，青木孝文，佐藤証，“暗号モジュールへのサイドチャネル攻撃とその安全性評価の動向,” 電子情報通信学会論文誌．A, 基礎・境界　J93-A(2), pp. 42–51, 2010-02-01.

4 Shin’ichiro Matsuo, Le Trieu Phong, Miyako Ohkubo, and Moti Yung, “Leakage-Resilient RFID Authentication With Forward-Privacy,” In Proc of RFID Sec2010, LNCS 6370, pp. 176–188.

5 Le Trieu Phong, Shin Ihiro Matsuo, and Moti Yung, “Leakage Resilient Strong Key-Insulated Signatures in Public Channels,” In Proc of INTRUST 2010.

6 Bruno Blanchet, A computationally sound mech-anized prover for security protocols. IEEE Transactions on Dependable and Secure Computing, 5(4): 193–207, 2008.

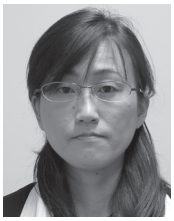
7 CRYPTREC事務局，電子政府推奨暗号リスト改訂のための暗号技術公募要綱（2009年度）.
http://www.cryptrec.go.jp/topics/cryptrec20091001 application guide 2009-2.pdf

8 Yoshikazu Hanatani, Miyako Ohkubo, Shin'ichiro Matsuo, Kazuo Sakiyama, and Kazuo Ohta, "A Study on Computational Formal Verification for Practical Cryptographic Protocol: The Case of Synchronous RFID Authentication," RLCPS2011.

9 M. Abe, “Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers,” In Proc. of Eurocrypt’98, pp. 437–447.

（平成23年6月15日 採録）

まつおしんいちろう
松尾真一郎
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室室長　博士（工学）
暗号プロトコル



おおくぼみやこ
大久保美也子
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室主任研究員　博士（工学）
暗号理論、暗号プロトコル