第16回
情報セキュリティ・シンポジウム「金融サービスにおける技術進歩と課題：CITECS設立10周年記念」の模様

要　旨

日本銀行金融研究所は、2015年3月11日、「金融サービスにおける技術進歩と課題：CITECS設立10周年記念」をテーマとして第16回情報セキュリティ・シンポジウムを開催した。本シンポジウムには、情報セキュリティ技術にかかわる金融機関の実務者や官公庁関係者、暗号学者、システム開発・運用に携わる実務家や技術者等、計128名が参加した。

最近の金融サービスにおける技術進歩には目覚ましいものがある一方で、そうした技術を実装し利活用していくことに伴うセキュリティリスクが意識されるようになっている。このような問題意識に基づき、今回のシンポジウムでは、(1) EMVカードに対する新攻撃手法を考察し、インターネット・バンキングにおける「取引認証」の安全な実装に応用する研究や、(2) ICカードに関しサイドチャネル攻撃の観点から安全性評価を行う手法を整理し、実装時の留意点を明らかにする研究、さらに、(3) 最近、耐量子コンピュータ暗号として注目されている格子暗号の最新動向に関する研究についての発表が当研究所スタッフにより行われた。また、金融機関による、インターネット・バンキングにおける不正送金の手口と自行における対策に関する講演に続いて、その中で明らかにされた問題提起を受けるかたちで、「インターネット・バンキングの安全性向上に向けて」と題したパネル・ディスカッションを行った。本稿では、本シンポジウムを構成するキーノート・スピーチ、4件の講演、パネル・ディスカッション、の概要を紹介する。

キーワード： インターネット・バンキング、取引認証、ICカード、格子暗号

本稿に示されている意見はすべて発言者たち個人に属し、その所属する組織の公式見解を示すものではない。

1. はじめに

日本銀行金融研究所・情報技術研究センター（Center for Information Technology Studies: CITECS）は、2015 年 3 月 11 日、「金融サービスにおける技術進歩と課題：CITECS 設立 10 周年記念」をテーマとして、第 16 回情報セキュリティ・シンポジウムを開催した。

最近の金融サービスにおける技術進歩には目覚ましいものがある一方で、そうした技術を実装し利活用していくことに伴うセキュリティリスクが意識されるようになっている。例えば、CITECS 設立以降の 10 年間を振り返ってみてもインターネット・バンキングは、金融機関やその顧客にとって不可欠なサービスになってきている一方、同サービスを利用した不正送金事例は増加しており、社会問題化しているという課題も浮き彫りになっている。このような問題意識に基づき、今回のシンポジウムでは、以下に示したプログラムのもと、講演およびパネル・ディスカッションが行われた。

本シンポジウムには、情報セキュリティ技術にかかわる金融機関の実務者や官公庁関係者、暗号学者、システム開発・運用に携わる実務者や技術者等、計 128 名が参加した。以下では、プログラムに沿って、本シンポジウムの概要を紹介する（以下、敬称略、文責：日本銀行金融研究所）[1]。

【第 16 回情報セキュリティ・シンポジウムのプログラム】

- キーノート・スピーチ「金融サービスにおける技術進歩と課題：CITECS 設立 10 周年記念」
  横浜国立大学大学院　教授　松本勉
- 講演 1「EMV カードシステムへの新攻撃手法を踏まえた、インターネット・バンキングにおける『取引認証』実施時の留意事項」
  日本銀行金融研究所　企画役補佐　井澤秀益
- 講演 2「IC カードの安全性評価手法に関する研究動向と EMV 仕様固有の留意点」
  日本銀行金融研究所　主査　鈴木雅貴
  ※三菱電機株式会社主席研究員　鈴木大輔、同研究員　菅原健と共同で実施した研究に基づく講演。
- 講演 3「量子コンピュータによる解読に耐えうる『格子暗号』を巡る最新動向」
  日本銀行金融研究所　清藤武暢

1 文中における各参加者の所属ならびに肩書きはシンポジウム開催時点のものである。

※独立行政法人情報通信研究機構研究員　青野良範、横浜国立大学准教授　四方順司と共同で実施した研究に基づく講演。

- 講演 4「オンラインバンキング不正送金の手口と対策」
  三菱東京 UFJ 銀行　システム部システム企画室　上席調査役
  大日向隆之
- パネル・ディスカッション「インターネット・バンキングの安全性向上に向けて」
  モデレータ：横浜国立大学大学院　教授　松本勉
  パネリスト：立命館大学情報理工学部　教授　上原哲太郎
  ヤフー株式会社　CSO Board　決済金融カンパニー
  情報セキュリティ責任者　ID 戦略室　室長　楠正憲
  金融 ISAC 理事／ FS-ISAC　Regional Director　鎌田敬介

2. キーノート・スピーチ「金融サービスにおける技術進歩と課題」

松本 は、CITECS 設立から現在に至るまでの CITECS の研究活動実績を振り返ったうえで、本シンポジウムにおけるテーマである「金融サービスにおける技術進歩と課題」の背景について、次のとおり発表した。

(1) CITECS 設立 10 周年を迎えるにあたって

日本銀行金融研究所に設置された情報技術研究センター（CITECS）は、この 4 月で設立から 10 周年を迎える。金融研究所では、CITECS 設立以前より、情報技術や通信技術に関する研究を行っており、例えば 1990 年代には当時の金融研究所の研究第二課（現・制度基盤研究課）において、電子現金と称する電子マネーに関する研究等を行っていた。当該研究成果の一部は論文としてまとめられ、学界等で発表を行っているほか、特許も取得（外部研究機関との共同出願を含む）している。また、1996 年には危殆化が叫ばれるようになってきた DES（Data Encryption Standard）と呼ばれる暗号アルゴリズムの強度評価に関する技術レポートを作成するなど、セキュリティに関する基盤技術の研究および情報発信等も行ってきている。

こうした中、金融業界が情報化社会において直面する新たな課題に適切に対処していくことをサポートするために体制が整備され、2005 年 4 月 1 日付けで、CITECS

図表 1　CITECS 設立以降の主な研究内容

金融機関を巡る状況	CITECS における主な研究
ATM における生体認証技術の導入開始（2004 年頃）	生体認証技術に関する研究 ・「生体認証システムにおける脆弱性について：身体的特徴の偽造に関する脆弱性を中心に」（金融研究 2005.7） ・「生体認証における生体検知機能について」（金融研究 2005.12） ・「生体認証システムの脆弱性の分析と生体検知技術の研究動向」（金融研究 2009.10） ・「生体認証システムにおける情報漏洩対策技術の研究動向」（金融研究 2010.4）
偽造キャッシュカードの社会問題化（2005 年頃）	IC カードに関する研究 ・「金融取引における IC カードを利用した本人認証について」（金融研究 2006.8） ・「リテール・バンキング・システムの IC カード対応に関する現状とその課題」（金融研究 2007.8） ・「IC カードを利用した本人認証システムにおけるセキュリティ対策技術とその検討課題」（金融研究 2007.8） ・「IC カードに利用される暗号アルゴリズムの安全性について：EMV 仕様の実装上の問題点を中心に」（金融研究 2007.8） ・「IC カード利用システムにおいて新たに顕現化した中間者攻撃とその対策」（金融研究 2012.7） 人工物メトリクスに関する研究 ・「人工物メトリック・システムにおける耐クローン性の評価手法の構築に向けて」（金融研究 2009.7） ・「偽造防止技術のなかの人工物メトリクス：セキュリティ研究開発の動向と課題」（金融研究 2009.7） ・「偽造防止技術の新潮流：金融分野における人工物メトリクスの可能性」（金融研究 2009.7）
暗号アルゴリズム 2010 年問題の懸念（2005 年頃）	暗号アルゴリズム 2010 年問題に関する研究 ・「暗号アルゴリズムにおける 2010 年問題について」（金融研究 2006.8）
JCMVP 運用開始（2007 年頃）	安全性評価に関する研究 ・「情報セキュリティ製品・システムの第三者評価・認証制度について：金融分野において利用していくために」（金融研究 2008.8） ・「暗号ユーザーが暗号アルゴリズムの安全性評価結果をどう活用するか」（金融研究 2010.4）
クラウド・コンピューティングの台頭（2009 年頃）	クラウドに関する研究 ・「クラウド・コンピューティングにおける情報セキュリティ管理の課題と対応」（金融研究 2011.1） ・「高機能暗号を活用した情報漏えい対策『暗号化状態処理技術』の最新動向」（金融研究 2014.10）
量子コンピュータの実用化（2011 年頃）	量子コンピュータ・量子暗号に関する研究 ・「量子暗号通信の仕組みと開発動向」（金融研究 2009.10）
国内インターネット・バンキングにおける MitB 攻撃の顕現化（2012 年頃）	インターネット・バンキングに関する研究 ・「インターネット・バンキングに対する Man-in-the-Browser 攻撃への対策『取引認証』の安全性評価」（金融研究 2013.7）
パスワードリスト型攻撃の被害拡大（2013 年頃）	パスワード管理に関する研究 ・「パスワードの使い回しおよび漏えいへの対策の検討：ユーザによる安全なパスワード管理を目指して」（金融研究 2014.10）

備考：括弧内は『金融研究』の発行年月。

が設立された。以降の 10 年間の CITECS の主な研究活動をみてみると図表 1 のようになる。特に、暗号アルゴリズムの 2010 年問題[2] については、CITECS が国内においていち早く警鐘を鳴らし、金融業界の暗号アルゴリズム移行を促すきっかけの 1 つとなったことは、重要な成果であると考えられる。

CITECS の今までの活動を評価すると、金融機関を巡る激しい状況変化に応じたタイムリーな研究を実施してきたほか、学界と金融機関との懸け橋的な役割を果たしてきたといえる。また、CITECS は、金融機関に関係する情報セキュリティ問題を対象に研究を実施している、国内では数少ない組織の 1 つである。これまで、情報セキュリティ・シンポジウムや『金融研究』における論文発表（図表 1）というかたちで、金融機関に適時適切な情報提供を行っているほか、学会等での最新動向を金融機関に分かり易いかたちに噛み砕いて還元するという努力が評価出来よう。

今後、CITECS に期待することは、学界と金融機関との懸け橋的な役割をより強固なものにするということであり、そのためには、金融機関のニーズを適切に把握したうえで、学界に広く提供して欲しいと考えている。学界における研究者は、シーズとなる有用な技術を多数有しているものの、実務の実態に触れる機会が少なく、生かすことが出来ていないという問題がある。学界の研究者は、本当に解決すべきことは何なのか、どのような研究を行えば世の中の役に立つのか（金融機関が何を求めているか）を知りたがっている。金融におけるニーズに関する、より活発な情報提供を期待したい。

(2) 今次シンポジウムの狙いとその背景

今次シンポジウムのテーマは「金融サービスにおける技術進歩と課題」であるが、①技術進歩の例として「インターネット・バンキング」および「IC カード」に関する事項と、②同取引に係る基盤技術である「暗号アルゴリズム」に関する事項に分けて整理すると以下のようになる。

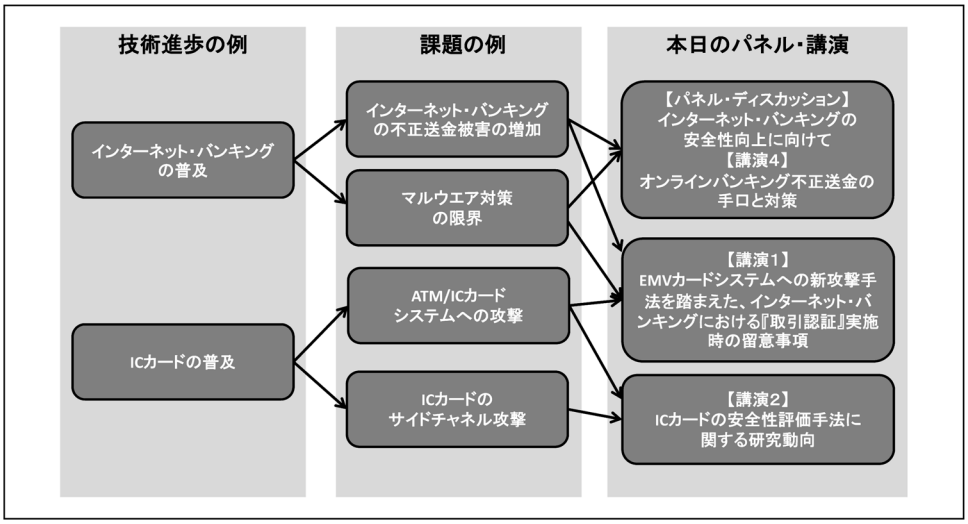
イ. 「インターネット・バンキング」および「IC カード」に関して

金融リテール取引手段の 1 つである「インターネット・バンキング」は、技術進歩が目覚ましく、利用度合いが増えていることは各種統計データ[3] をみても明らか

2 米国立標準技術研究所（National Institute of Standards and Technology : NIST）が、2-key3DES や鍵長 1,024 bit の RSA 暗号や SHA-1 などの当時主流で使われていた暗号アルゴリズムについて、安全性の観点から、2011 年以降、米国連邦政府機関のシステムで使用しない方針を各種ガイドラインにて示した。当時、暗号アルゴリズムの移行をどのように進めるかが重要な問題となり、同問題は「暗号アルゴリズムの 2010 年問題」と呼ばれた。なお、NIST は後に、暗号アルゴリズムの危殆化の速度が思ったほどではなかったとして、移行の期限を 2013 年まで延ばしている。

3 インターネット・バンキング契約口座数は、2005 年は 1,600 万口座程度であったのに対して、2013

図表２ 「インターネット・バンキング」および「IC カード」に関する技術進歩と課題、本シンポジウムの講演の位置付け



である。このような中、インターネット・バンキングの不正送金被害が増加している状況[4]があるほか、日本をターゲットにしたバンキング・マルウエアが出現するなど、課題も浮き彫りになっている。また、もう 1 つのリテール取引手段である ATM 取引においては、磁気ストライプ式のキャッシュカードから IC カードへの切り替えが徐々に進んでいる状況[5]がある。このような中、ATM や IC カードシステムへの攻撃手法が学界で報告（Murdoch *et al.* [2010]）されているほか、暗号モジュール（IC カード等）へのサイドチャネル攻撃も現実的なリスクとして認識されるようになってきている（Oswald and Paar [2011]）。

そこで、昨今の金融リテール取引を巡る技術進歩および課題を踏まえて、本シンポジウムでは、パネル・ディスカッション、講演 1、講演 2 および講演 4 が行われた（図表 2）。

ロ. 「暗号アルゴリズム」に関して

量子力学の性質を情報処理に応用する「量子コンピュータ」に関する研究が学界で盛んに行われている。量子コンピュータには複数の方式があるが、その中でも、「量子デジタル型[6]」と呼ばれる量子コンピュータは、大きな桁数の素因数分解を

年は 6,500 万口座と、年々増加している（金融情報システムセンター［2005、2013］）。

4 インターネット・バンキングによる不正払戻し額は、2012 年度は 1.2 億円程度だったのが、2013 年度は 14.3 億円程度と急増している（全国銀行協会［2015］）。

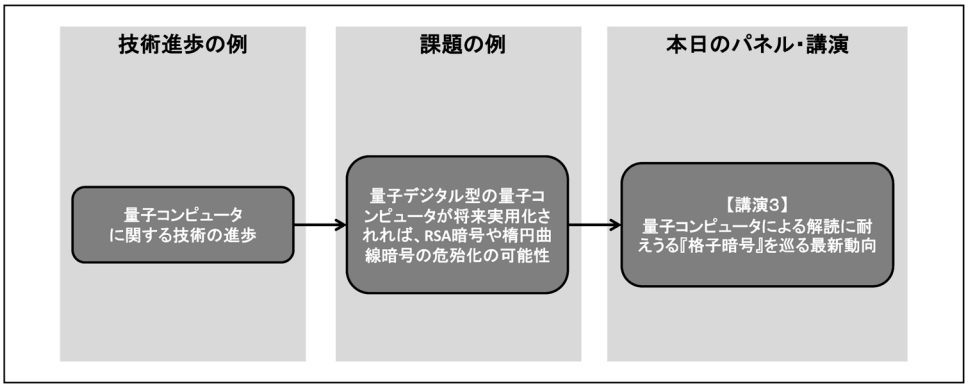
5 キャッシュカードの IC カード化率は、2010 年度は 15％程度であったのに対して、2013 年度は 23％程度と年々増加している（金融庁［2011、2014］）。

6 学界では、量子デジタル型は「量子ゲート方式（量子チューリングマシン）」と呼ばれる。

従来のコンピュータよりも高速に解ける可能性があるため、現在インターネットで広く用いられている RSA 暗号[7] 等の安全性を脅かすものとして注目されている。もっとも、量子デジタル型の量子コンピュータは、同コンピュータにおける計算処理において重要な役割を果たす「量子の重ね合わせの状態」を維持することが外部ノイズの影響等から難しく、現時点では実用化にはほど遠い状況である[8]。したがって、学界でも RSA 暗号等が量子コンピュータにより直ちに危殆化すると考えられているわけではない。

しかしながら、既に利用されている暗号アルゴリズムを切り替えるためには、長期計画に基づく移行が必須であり、将来、RSA 暗号等を脅かす量子コンピュータの実用化を見据えて、事前に量子コンピュータによる解読に耐えうる暗号アルゴリズムの準備を進めていくことが必要である。そこで、本シンポジウムでは、講演 3 において、そのような暗号の有力な候補の 1 つである「格子暗号」を巡る最新動向を紹介した（図表 3）。

図表 3 「暗号」に関する技術進歩と課題、本シンポジウムの講演の位置付け



7 RSA 暗号は「大きな桁数の素因数分解を解くことが難しい」ということを前提に安全性が設計された暗号アルゴリズム。

8 最近、カナダの D-Wave Systems, Inc が販売したとして話題になっている量子コンピュータは、量子アナログ型（学界では、「量子アニーリング方式」と呼ばれる）に分類されるものであり、スケジュールや資源配分の最適化等に応用が利く「組み合わせ最適化問題」を、従来のコンピュータよりも効率良く解けるとされるが、RSA 暗号の安全性の根拠である「素因数分解問題」を同様に効率よく解けるかについては明らかになっていない。

3. 講演1「EMVカードシステムへの新攻撃手法を踏まえた、インターネット・バンキングにおける『取引認証』実施時の留意事項」

井澤は、最近発表されたEMVカードシステムへの新攻撃手法や、それを踏まえたインターネット・バンキングにおける「取引認証」実施時の留意事項について、次のとおり発表した。

(1) EMVカードシステムへの新攻撃手法について

ICカードにおいては、ICカードとそれに利用される端末の仕様を定めた業界標準である「EMV仕様[9]」が日本を含め国際的に利用されている。EMV仕様におけるセキュリティ対策の1つに、メッセージ認証子[10]を用いた、取引の真正性を確保する仕組み（以降、「取引認証」と呼ぶ）がある。ただ近年、英国ケンブリッジ大学の研究グループが、この「取引認証」に対して、ある特定の条件のもとで攻撃が成立し、実質的に正規カードが行う取引と同等の取引が攻撃者作製のカードで可能となることを発表した（Bond *et al.* [2014]）。本攻撃を発表した研究グループは当該攻撃手法を「Pre-play attack」と名付けており、欧州において実際に起こったATMからの不正現金引き出し事件について、本攻撃手法の1つが悪用された可能性が高いことを指摘している。ケンブリッジ大学の研究グループが提案した「Pre-play attack」（2種類）をまとめると図表4のとおりとなる。

(2) インターネット・バンキングにおける「取引認証」の留意事項

インターネット・バンキングの不正送金対策として「取引認証」を導入する動きが国内の金融機関において出てきている。このような中、前述したPre-play attackはEMVカードシステムに限らず、近年導入が進んでいるインターネット・バンキングにおける「取引認証」に対しても適用出来る可能性があると考えられる。

9 EMVは、Europay International、MasterCard International、Visa Internationalの頭文字の略。

10 データの真正性を確認し、認証を行う仕組み。同様の仕組みにデジタル署名があるが、デジタル署名では生成と検証にそれぞれ秘密鍵と公開鍵を用いるのに対し、メッセージ認証子では生成と検証に同一の暗号鍵を用いる点が異なる。

図表 4　Pre-play attack のまとめ

	攻撃手法 1	攻撃手法 2
攻撃が成功すると起こる事象	・攻撃者が用意した IC カードを用いて、被害者の IC カードで行う取引と同等の取引が実施可能となる。	
主な攻撃条件	・攻撃者が用意した端末（ATM や POS）に対して、被害者が自身の IC カードを挿入し、PIN を入力する。	
	・端末のUN[11]生成方法について、EMV仕様上は乱数等の「予測不可能な数」を生成するべきところを、実装の不備等でUNが攻撃者に類推可能である場合。	・端末がマルウエア感染し、攻撃者が端末でやり取りされる情報を自由にコントロールできる場合。
主な原因	・端末の UN 生成方法が脆弱。	・EMV仕様ではチャレンジ[12]（UNを含む取引内容）がすり替えられても、それに対するレスポンスの検証者（金融機関）は、すり替えを知ることが出来ない。 ※EMV 仕様においてはオフライン処理も想定しているため、チャレンジ生成者とレスポンス検証者が異なることを前提としている。
主な対策	・端末の UN に乱数等の「予測不可能な数」を使用する。 ・ホストシステムにて UN が単なるカウンタになっていないか確認する。	・端末のマルウエア感染を防ぐための施策を確認する。 ・AC生成[13]にタイムスタンプ（時刻情報）を利用する。 ・ホストシステムにて UN を生成する。

そこで、本講演では、インターネット・バンキングの「取引認証」への Pre-play attack の適用可能性およびその影響について考察した。もっとも、EMV 仕様とインターネット・バンキングとでは実際にはプロトコルが異なるため、そのままでは Pre-play attack を適用することは難しい。そのため、Pre-play attack を一般化し、その攻撃のもととなる考え方をインターネット・バンキングに当てはめることにより考察を行った。その結果を図表 5 にまとめる。

11 Unpredictable Number の略で、32bit の「予測不可能な数」のこと。EMV 仕様においては、端末がカードに対して送信する取引内容の情報とともに、UN も送信される。

12 チャレンジとは一般に、サーバがクライアントを認証するために提示（質問）する乱数等の値のこと。クライアントは、チャレンジと鍵情報等をもとに、特定のアルゴリズムを用いてレスポンス（回答）を生成したうえでサーバに送信し、その正当性を証明する。EMV 仕様では、端末がサーバに、IC カードがクライアントに、それぞれ該当する。

13 Application Cryptogram の略で、カードが受信した取引内容に対して、（カードとホストシステムとで共有する）鍵を用いて暗号化を施した情報。取引内容の正当性を確認するための「メッセージ認証子」となる。

図表５　インターネット・バンキングの「取引認証」における留意事項まとめ

	攻撃手法 1	攻撃手法 2
攻撃が成功すると起こる事象	・インターネット・バンキングの振込操作について攻撃者の口座に送金を実施してしまう。	
攻撃条件	・取引認証コード（TAN: Transaction Authentication Number）が攻撃者に類推される場合。	・マルウエア感染した PC がユーザに指示を出し、ユーザがそれに従ってしまう場合（ユーザが騙される場合）。
攻撃手法	・振込先確認時に金融機関から送信されてくる TAN が攻撃者に類推され、攻撃者への振込が自動実行されてしまう。	・ユーザが振込先情報を TAN 生成器に入力する際に、PC の画面上に表示された情報（マルウエアによって表示された攻撃者の振込先情報）をユーザが入力してしまえば、攻撃者への振込が実行されてしまう。
原因	・TAN の生成方法が脆弱。 ※Pre-play attack の「攻撃手法１」における原因と同様。	・チャレンジ（取引内容）がすり替えられても、検証者（金融機関）はそれを知ることが出来ない。 ※Pre-play attack の「攻撃手法２」における原因と同様。 ・ユーザが騙される。
主な対策・留意事項	・TAN 生成には、攻撃者による予測が不可能な数字を用いる。	・「TAN 生成機に入力するのは、PC 上に表示された数字ではなく、自分が振り込みたい先の口座情報である」ということを、ユーザに啓蒙する。 ・ブラウザに表示された数字を TAN 生成機に入力させるような作り（ユーザインターフェース）にしない。

4.　講演２「IC カードの安全性評価手法に関する研究動向と EMV 仕様固有の留意点」

鈴木 は、サイドチャネル攻撃の攻撃手法と対策、サイドチャネル攻撃に対する安全性評価手法の研究動向、およびサイドチャネル攻撃に対する EMV カード固有の留意点について、次のとおり発表した。

(1) サイドチャネル攻撃の攻撃手法と対策

IC カードのような暗号モジュールにおいて、暗号処理中の消費電力量の変化や発生する電磁波等の物理現象を計測・解析することで、同モジュールに格納された秘密鍵を効率良く推定する手法に「サイドチャネル攻撃」と呼ばれるものがある。同攻撃により市販の暗号モジュールから、実際に秘密鍵を推定出来たとの報告もあり（Oswald and Paar [2011]）、同攻撃への対策が不可欠といえる。

サイドチャネル攻撃においては、どのような情報が漏洩しうるのかという物理的な側面と、漏洩を使っていかに暗号解読をするかという暗号学的側面からの考察が必要である。両者をつなげるために、何が漏洩するかを「漏洩モデル」として抽象化するのが一般的である。代表的な 2 つの漏洩モデルは、それぞれ次のとおりである。

処理時間モデル：秘密鍵の値に応じて暗号処理にかかる時間（処理時間）が変化するというモデル[14]。処理時間を計測することにより秘密情報を復元出来る。同モデルへの対策としては、ダミー演算を使うことで、秘密鍵によらず処理時間を一定にするという方法が挙げられる。

ハミング距離モデル：計算の途中結果は IC チップのレジスタと呼ばれる一時的な記憶領域に保持される。レジスタの電気的な性質上、保持する値が書き換わったときに大きく電力を消費する。そのため、電力をモニタすれば、計算の途中結果が復元出来、最終的には秘密鍵を推定出来る可能性がある。同モデルへの対策としては、乱数を加えることで平文をマスクし、そのうえで暗号処理を行うことで消費電力の変化からハミング距離[15] を分かり難くする方法が挙げられる。

(2) サイドチャネル攻撃に対する安全性評価手法の研究動向

暗号モジュールの安全性を評価するにあたって、学界では様々な評価手法が提案されているが、ここでは、①波形数を用いる手法、②仮説検定を用いる手法、③通信路容量を用いる手法、の 3 種類を紹介する（図表 6）。

14 例えば、RSA 暗号の復号における剰余演算の高速化にバイナリ法を用いた実装をしている場合、秘密鍵のあるビットが 0 か 1 かで、処理時間が異なる。

15 2 つの値の違いを測る尺度のことで、桁数が同じ 2 つの値を比べたときに、対応する位置にある異なる値の個数。例えば、10<u>1</u><u>1</u>101 と 10<u>0</u>10<u>0</u>1 との間のハミング距離は 2 となる。

図表 6　安全性評価手法の比較

	安全性評価手法		
	評価手法 1 （波形数）	評価手法 2 （仮説検定）	評価手法 3 （通信路容量）
秘密鍵の推定を行うか	行う（攻撃手法を構築するコストが発生）。	行わない（秘密鍵は既知）。	
評価に要するコスト	大きい	小さい	
評価手法の出力	波形数	漏洩の有無	通信路容量
その他の特徴	・N 波形安全という安全性要件の充足を検証可能。	・秘密鍵の推定に繋がらない漏洩を検知する可能性がある。	・秘密鍵の推定に繋がらない漏洩を検知する可能性がある。 ・攻撃に必要な波形数の下限を理論的に算出可能。

波形数を用いる手法：評価対象に対してサイドチャネル攻撃を行い、秘密鍵を推定するまでに、評価対象に何回暗号処理を行わせる必要があるかを確認する手法である。計測する波形数[16]が多いほど安全性が高いとする。

仮説検定を用いる手法：「秘密鍵に関する情報（サイドチャネル情報）を漏洩していない」との帰無仮説を立て、計測した波形を用いて同仮説を棄却することで、対立仮説である「漏洩あり」が成立することを示す手法である。

通信路容量を用いる手法：サイドチャネル攻撃の一連の流れを「サイドチャネル情報を送信する通信」とみなし、1 つの波形（サンプル）で伝送可能なサイドチャネル情報の量（「通信路容量」と呼ばれる）が少ないほど安全性が高いとする手法である。

(3)　サイドチャネル攻撃に対する EMV カード固有の留意点

EMV 仕様に準拠した IC カード（以下、「EMV カード」）を想定すると、同仕様に固有の留意点が存在する。EMV カードを用いた取引の取引認証のプロセスにおいては、AC 生成[17]に用いる「マスタ鍵」が安全性の要になる。マスタ鍵に関して、攻撃者が入手可能な波形数の上限は最大 65,536 波形である。なぜなら、取引毎に更新されるカード内のカウンタ値が上限（65,536 回）に達した場合、同カードを取引に使用出来ない状態にするという規定があるためである。

マスタ鍵への攻撃のハードルを上げるための運用面での対策は 2 種類考えられ

16 暗号処理中の消費電力の推移を記録したデータは「波形」と呼ばれており、攻撃に要した波形の数を「波形数」と呼ぶ。

17 脚注 13 参照。

る。1 つは、カウンタの上限を引き下げるという対策であり、もう 1 つは、マスタ鍵を定期的に更新するという対策である。後者については具体的には、①予め複数のマスタ鍵をカード内に格納しておき、それに切り替えるというオフライン型の方法と、②カードとサーバの通信機能である「Issuer Script」を用いてマスタ鍵を更新するというオンライン型の方法が考えられる。このほか、システム全体で考えれば、サイドチャネル攻撃の影響を受け難い独自の鍵生成方法をシステム設計時に選択しておくことも考えられる。

わが国の IC キャッシュカードについては、EMV カードであるためこれら留意点に気を付けなければならないが、有効期限が設けられていない IC キャッシュカードについては、一度発行した IC カードを長期間利用することが想定されている点にも気を付けなければならない。その場合、新たなサイドチャネル攻撃手法の考案等により IC カードの安全性が経年劣化するリスクがある。

5. 講演 3「量子コンピュータによる解読に耐えうる『格子暗号』を巡る最新動向」

清藤 は、量子コンピュータでも容易に解読出来ないと期待されている「格子暗号」の最新動向について、次のとおり発表した。

(1) 格子暗号の必要性

金融分野をはじめとする様々な分野において、データ保護や通信相手の認証等を行うために、公開鍵暗号等の暗号アルゴリズムが広く利用されている。公開鍵暗号は、公開鍵から秘密鍵を求めることが困難であるという仕組みによりその安全性を保証しており、この仕組みの実現には数学的な問題が利用されている。

しかし、「量子コンピュータ（量子デジタル型）」が実現すると、現在主流の RSA 暗号や楕円曲線暗号が安全性の根拠としている数学的問題[18] を容易に解けることが知られているため、これらの暗号アルゴリズムは安全を保証出来なくなる。現時点では、同コンピュータはまだ広く利用可能な状態ではないが、技術進歩により、今

18 現在主流の公開鍵暗号である RSA 暗号や楕円曲線暗号は、それぞれ「素因数分解問題」、「楕円曲線離散対数問題」と呼ばれる数学的な問題を利用して、安全性を保証している。素因数分解問題は、「2 つの素数の積から元の素数を求める」という問題であり、楕円曲線離散対数問題は「2 つの数 g と t が与えられたとき、g を s 乗した値が t と等しくなるような自然数 s（すなわち、$t=g^s$ を満たす s）を求める問題」を、楕円曲線上のある条件を満たす点のみで扱う数学的問題である。

後利用のハードルは低くなっていくものと推測される。こうした状況を踏まえると、量子コンピュータでも容易に解読出来ないと期待される公開鍵暗号（耐量子コンピュータ暗号）の研究が不可欠であり、この特長を有する公開鍵暗号の 1 つとして「格子暗号」が学界において注目されている。

(2) 格子暗号の特徴

格子暗号は、「格子[19]」と呼ばれる数学的な構造上において定義される数学的な問題（「最近ベクトル問題（Closest Vector Problem）」や「最短ベクトル問題（Shortest Vector Problem）」等[20]）を利用して、安全性を保証している公開鍵暗号の総称である。

格子暗号のメリットの 1 つ目は量子コンピュータでも容易に解読出来ないと期待されている点である。最近ベクトル問題や最短ベクトル問題は、量子コンピュータでも効率よく解けないと期待されているため、同コンピュータが実現された場合でも、格子暗号は安全性を保証出来ると考えられている。

メリットの 2 つ目は、データを暗号化したまま処理を行う技術（暗号化状態処理技術）を実現可能である点である。データを暗号化したままキーワード検索を行う「秘匿検索」や、データを暗号化したまま統計解析等の数値計算を行う「秘匿計算」については、格子暗号を使って実現可能であり、既に製品化も始まっている。

一方、デメリットとしては、鍵サイズが大きい点が挙げられる。格子暗号は RSA 暗号や楕円曲線暗号と比較して、同等の安全性を確保するためには、現時点では数倍から数兆倍の鍵長が必要となることが知られている[21]。

(3) 格子暗号の最新動向および利用する際の留意点

提案されている格子暗号の実現方式の中で、「LWE（Learning with Errors）方式」と呼ばれる方式は、安全性と実用性のバランスの観点から現時点では最も優れているため学界で注目されている。近年、鍵長を数千分の 1 程度まで削減出来る LWE 方式の改良方式が提案され、同方式の安全性評価や実用化に関する研究が活

19 格子とは、空間上に規則正しく並んでいる点の集合。「次元」や「基底ベクトル」と呼ばれるパラメータにより、格子の構造や特徴が一意に定まる。

20 これらの問題は、直感的には「次元や基底ベクトル等のパラメータが与えられたとき、ある条件を満たす格子上の点を探索する」という問題である。

21 例えば、鍵長 2,048 ビットの RSA 暗号と同程度の安全性を確保するためには、格子暗号においては数キロビットから数ペタ（10^{15}）ビットの鍵長が必要と考えられている。

発に行われている。また、他の実現方式である「NTRU 方式」は、国際標準である IEEE1363.1 や ANSI X9.98 において推奨パラメータ等が規定されている[22]。

前述のとおり、格子暗号は現在主流の RSA 暗号や楕円曲線暗号と比較して、同程度の安全性を確保するために必要な鍵長が長いため、例えば IC カードや組込み機器等の計算機性能（計算能力やメモリ等）が制限されている環境での利用には、適さないと考えられる。したがって、同暗号を利用する際には、この特徴を理解したうえで、計算機性能が十分に備わっている PC 等の適切な環境下での利用を検討する必要がある。また、格子暗号の安全性評価に関する研究は発展途上であり、まだ評価が定まっているとは言い難いため、学界における研究動向を定期的にフォローし、最新の研究結果にもとづく適切なパラメータを選定することが重要である。

6. 講演 4「オンラインバンキング不正送金の手口と対策」

大日向 は、オンラインバンキングの不正送金の状況・手口およびその対策について、次のとおり発表した。

(1) オンラインバンキングの不正送金の状況と手口

オンラインバンキングの不正送金の状況（本邦全体）をみると、各金融機関における対策の成果もあり足元の数か月では若干減少傾向にあるものの、年ベースでみると、2012～14 年にかけて、被害件数、被害額ともに年々増加している（警察庁[2014]）。

不正送金の手口は、年々変化しており徐々に巧妙化している。2011 年頃から現在に至るまで断続的に発生している手口として、「フィッシングメールによる情報窃取」がある。これは、攻撃者が顧客に対してフィッシングメールを送付し、顧客をフィッシングサイトに誘導したうえで、偽画面を表示し、顧客の ID、パスワードや乱数表情報を不正に取得する手法である。

2012 年 10 月頃から現在も時々みられる手口として「マルウエアによる情報窃取」がある。これは、攻撃者が顧客の PC をマルウエアに感染させ、顧客がオンラインバンキングに接続したら、マルウエアがブラウザに表示される画面を書き換え乱数表の入力要求を表示し、攻撃者が当該情報等を不正に取得する手法である。

22 ただし、安全性評価の進展にともない、これらの標準に記載されている推奨パラメータの安全性は低下しうることに留意が必要である。

図表 7　不正送金対策のまとめ

	(a) 有効性			(b) 網羅性	(c) 利便性
	フィッシングメール型	情報搾取型	自動送金型		
①異常検知	○	○	×	○	○
②マルウエア検知	×	○	○	○	○
③顧客 PC 強化	×	○	○	×	△
④OTP[23]（メール）	○	△	×	×	×
⑤OTP（トークン）	○	○	×	×	×
⑥トランザクション署名	○	○	○	×	×
⑦スマートフォン認証	○	○	○	×	○

資料：三菱東京 UFJ 銀行

2013 年 9 月頃から現在も続いている手口として「マルウエアによる自動送金」がある。これは、攻撃者が顧客の PC をマルウエアに感染させ、顧客がオンラインバンキングに接続すると、マルウエアが、画面上は「ダウンロード中」という偽画面等を表示しつつも、裏では攻撃者への振込操作を自動実施（その後の乱数表の入力を顧客に求める）するという手法である。

今後発生する恐れがある手口としては、「取引内容の改ざん」がある。この手法は国内ではまだ観測されていないが、欧米では既に報告されている手口である。これは、攻撃者が顧客の PC をマルウエアに感染させ、顧客がオンラインバンキングに接続し、（正規の）振込操作を実施すると、マルウエアがその取引指図の内容を書き換え、攻撃者への振込が行われるという手法である。

(2)　オンラインバンキングの不正送金への対策

不正送金への対策としては、単独でパーフェクトな対策は存在しないため、様々な対策手法を組み合わせ、トータルで安全性を高めることが一般的である。対策としては図表 7 の①～⑦等が存在するが、どの対策をどのように組み合わせるかという点が問題になってくる。それを考えるにあたっては、(a) どのような手口に対し有効に検知や防御が出来るかという有効性、(b) その対策がどの程度の顧客をカ

23 ワンタイムパスワードの略。

バー出来るかという網羅性、(c) 顧客の使いやすさという利便性、(d) コスト、の観点での検討が重要である。

(3) 問題提起

前述対策を金融機関として実施していくにあたり、3 点の問題提起があった。1 点目は、顧客がセキュリティ対策を実施することの難しさである。セキュリティレベルを向上させ「安全性」を高める対策製品があっても、「網羅性」が高くないと効果が限定的であるほか、「利便性」を下げると顧客が利用しづらいというジレンマがある。このように「安全性・利便性・網羅性のバランス」を取らなければならないが、具体的にどのようにすればよいのかは難しい判断である。

2 点目は、個別行単位での対策は利用者にとっては不便であるという点である。認証トークン 1 つをとってみても、複数の金融機関に口座を持つ顧客は、複数の認証トークンを持ち歩かなければならず不便である。このため、各金融機関で共通して使えるトークンのようなソリューションがあれば良いと考えている。例えばシンガポールにおいては「OneKey」と呼ばれるソリューションがあり、複数の組織で 1 つのトークンを利用するフレームワークが存在する。

3 点目は、ほとんどの対策製品が海外製であり、製品選定が難しいという点である。金融機関として、対策製品の比較検討を行いたくても、複数のベンダー製品を網羅的に把握している人物が存在しない点に苦慮している（ベンダーは自社製品には詳しくても、他社製品まで詳しいとは限らない)。

7. パネル・ディスカッション「インターネット・バンキングの安全性向上に向けて」

パネル・ディスカッションでは、3 名のパネリストが、「インターネット・バンキングの安全性向上に向けて」との題目で各々プレゼンテーションを行った後、講演 4 の 大日向 の問題提起を受けるかたちで議論が行われた。複数のフロア参加者からも意見が出るなど、議論はフロアを巻き込むかたちで白熱したが、その概要は次のとおりである。

(1) 安全性・利便性・網羅性のバランスのとり方について

イ. 安全性・利便性・網羅性

鎌田 は、講演 4 の第 1 点目の問題提起（安全性・利便性・網羅性のバランスのとり方）を受けて、多くの金融機関は 1 つのセキュリティ対策であらゆる脅威に対応出来る万能なソリューションを求める傾向にあることを指摘したうえで、現実にはそのような万能な対策は存在せず、実際に「安全性」を高めるためにはいろいろな対策を組み合わせる必要があると指摘した（例えば、不正取引という脅威への対策だけでも、本人認証、取引認証、リスクベース認証等、複数の対策が存在する）。もっとも、複数の対策を組み合わせて使うことに伴い、ユーザの「利便性」の低下が懸念される点が問題であると述べた。それに対して、米国の大手金融機関においては、顧客の利便性を優先する方向で対策が行われる傾向がある点を指摘した。具体的には、取引の際に（ユーザがオペレーションを実施する必要がある）取引認証等は行わない代わりに、金融機関のサーバ側でのセキュリティ対策（例えば、インターネット・バンキングの Web コンテンツに毎日少しずつ変更を加え、バンキング・マルウエアが対応出来なくする対策）を採用する事例があることを紹介した。

上原 は、ある国内金融機関のセキュリティ対策の例をみると、複数のパスワードに加え、ワンタイムパスワード、さらに合言葉による追加認証が求められる場合もある等、「安全性」の面では優れているかもしれないものの、「利便性」を大きく犠牲にし、ユーザに使いたくないと思わせてしまっている例が見受けられると指摘した。そのうえで、人的面での制約が大きい金融機関（規模が小さい金融機関等）においては、ベンダーが提供するセキュリティ対策を、利便性とのバランスについて検討しないまま「全部入り」で導入してしまっている可能性があることを指摘した。このように、金融機関のシステム投資に対する人的制約が「利便性」の低下をもたらしてしまう可能性を述べた。

楠 は、「安全性」の高いセキュリティ対策であっても「利便性」が低いと一般ユーザには利用してもらえないため、負担を強いることなく安全性を向上出来る対策が望ましいと指摘した。そのうえで、スマートフォンアプリにおいては、同要件を満たすと期待される利用方法[24] が存在することから、スマートフォンを使った環境では、インターネット・バンキングにおける「安全性」と「利便性」のバランスを考慮した対策が可能ではないかと述べた。

これに対し、モデレータの 松本 は、全てのユーザがスマートフォンを所持して

24 例えば、Web サイトやスマートフォンにおける ID 認証においては、毎回パスワードを入力することなくサービスを利用出来ることで「利便性」を考慮し、その「安全性」はスマートフォンの画面ロック機能（PIN や顔面認識・指紋認証等）が担保している。

いるとは限らないため、スマートフォンの利用を前提とすることについては、「網羅性」の観点から問題があるのではないかと指摘した。

これを受けて 鎌田 は、全てのユーザの利用環境をスマートフォンに変更するのは難しいため、①スマートフォンを利用しているユーザと②使用していないユーザとで対策を分け、②に対しては、追加的なセキュリティ対策を実施することで、「網羅性」と「安全性」を確保することが出来るのではないかと指摘した。追加的なセキュリティ対策として、金融機関のサーバ側で取引履歴等のログ監視を行う方法もあるという考え方を示したうえで、ログ監視はコストがかかるため、②に限定して実施することでコスト面での効率化も図れるのではないかと指摘した。

ロ. ログ監視と人的リソース問題

ログ監視業務について、鎌田 は、米国の大手金融機関の事例として、100 名程度の人員体制により同業務を行っているところもある一方で、数名程度で同業務を行っている金融機関もあり、体制面では区々であると指摘した。また監視手法については、知識や経験が重要となるため、市販のツールと自社開発したツールを組み合わせた方法を紹介したうえで、各金融機関が試行錯誤しながら行っているのが現状であることについて紹介した。

これに対して、上原 は、米国の金融機関はエンジニアが自組織内に多数おり、システム開発を内製化している例が多い一方で、日本は外注化が進んでいる印象があり、これを踏まえると、日本の金融機関においてログ監視を行うにあたっては、人的リソースの問題があるのではないかと指摘した。

これを受けて、楠 は、自社（ヤフー株式会社）においても、人的リソースの不足は課題であると指摘したうえで、この課題を解決する手法の例として、ログ監視業務のシステム化（自動化）の促進や同業務のアウトソース化等が挙げられると述べた。なお自社においては、ID に関するログ監視のようなコア業務は内製化している一方で、周辺業務に関するログ監視はアウトソースしており、「選択と集中」の工夫をしていると補足した。

ハ. セキュリティ対策の共通化 vs 独自性

ここで、松本 は、講演 4 の第 2 点目の問題提起（個別行単位での対策は利用者にとっては不便）も踏まえつつ、セキュリティ対策全般を共通化することの是非について意見を求めた。

これに対して、鎌田 は、セキュリティ対策の共通化に関連して、国内の金融機関が連携して、最新のサイバーセキュリティに関する脅威およびその対策等について情報共有や分析・議論を行う金融 ISAC（Information Sharing and Analysis Center）について紹介を行った。金融 ISAC においては、知識の共有が目的であり、セキュリティ対策に関連するソリューションやツールの共有等は本来の目的ではないが、同

組織における活動が、将来的には金融業界全体でのセキュリティ対策の共通化につながることもありうると述べた。

これを受けて、フロア参加者Aから、共通的なセキュリティ対策ソリューションを利用していくことは、コスト面・人的面での制約が大きい金融機関（規模が小さい金融機関等）において有用ではないかという指摘があった。

一方、フロア参加者Bから、セキュリティ対策の共通化は、確かにユーザの利便性や業界全体の安全性向上の面で有用と考えられるが、一方で、全ての対策を共通化することには問題があるとの指摘があった。特に、共通化したセキュリティ対策が危殆化した場合、金融業界全体へ与える影響は大きいため、各銀行において異なるセキュリティ対策を行い、安全性の差別化でユーザにアピールするという観点も必要ではないかとの指摘があった。

また、フロア参加者Cからも、セキュリティ対策に関連するソリューションやツールの開発において、関連する技術の向上や性能のチェック機能が働くためにも競争原理が必要ではないかとの指摘があった。

これらの指摘に対して楠は、全てのセキュリティ対策の共通化は確かにリスクが高いとしたうえで、例えば、多要素認証・データ連携方式等のフロントエンド部分は業界全体で共通化し「利便性」に配慮する一方で、ログ監視やリスクベース認証等のバックエンド部分については各金融機関で異なるグループに業務を集約するなどして複数の選択肢を確保することにより、金融サービスの競争原理を維持するとともに、「安全性」の確保にもつながるのではないかとの考えを示した。

松本は、これまでの議論を踏まえたうえで、金融業界におけるセキュリティ対策について、「安全性」、「利便性」、「網羅性」を確保するためには、①スマートフォンユーザとそうでないユーザとでセキュリティ対策を分けるといった「網羅性」にも配慮するということや、②フロントエンドにおける共通化を行い「利便性」に配慮し、③バックエンドでのログ監視等において競争原理を働かせることにより「安全性」も考慮した対策が、今後の金融サービスを考えるうえで1つの解となる可能性がある、とまとめた。

(2) 今後の安全性向上に向けて

松本は、スマートフォンと同様に、今後、一般ユーザにも広く普及すると推測される情報端末（ウェアラブル端末、情報家電、ゲーム機等）の登場に伴い、インターネット・バンキングの利用環境も変化すると考えられるが、この変化に先立ち、予め起こりうる脅威を予測し、先回りして対策を実施することは出来ないか、との問題提起を行った。

これを受けて 上原 は、インターネット・バンキングにかかわる脅威の変化については、金融機関がいち早く気付き対処出来る体制を整備する必要があるとの見解を述べた。例えば、携帯キャリアが提供する、いわゆるキャリアメールについては、従前は（マルウエア感染するリスクが PC に比べて小さい）携帯電話からしか送受信出来ないことから安全性が高いと考えられていたが、最近では Web ブラウザからも利用可能なようにサービス内容が変更になっている携帯キャリアもあり、PC のマルウエア感染により携帯メールの中身を盗み見られたり、勝手に送信されるリスクが出てきている。この例に限らず、情勢変化に伴い、安全性の前提となる条件が変わることにより脅威が変化することは、往々にしてよくあるため、金融機関におかれてはぜひ情勢変化をグリップしてほしいと述べた。

鎌田 は、金融機関はコストの問題等から、顕現化していないリスクへの対策を先回りして行うことは難しいだろうとの見解を示したうえで、万が一リスクが顕現化した場合の行動計画を事前に立てておくことが重要であると述べた。行動計画を立てる際には、情勢変化を見極める力や、そこから発生するリスクを想像する力が必要になるが、金融 ISAC といった枠組みを活用しながら、それらの力を組織として養うことにより、将来の安全性がもたらされうると述べた。

最後に、松本 は、インターネット・バンキング等において、利用端末や環境の変化に伴い、今後起こりうる基本的な脅威の整理および対応策の分析を、金融 ISAC 等を活用したうえで、金融業界全体で予め検討していくことが重要であり、脅威が発生しても適切な対応が可能な体制を構築することが必要ではないかと述べ、まとめとした。

参考文献

金融情報システムセンター、『平成 18 年版金融情報システム白書』、金融情報システムセンター、2005 年

――――、『平成 26 年版金融情報システム白書』、金融情報システムセンター、2013 年

金融庁、「偽造キャッシュカード問題等に対する対応状況（平成 23 年 3 月末）について」、2011 年 7 月 22 日（http://www.fsa.go.jp/news/23/ginkou/20110722-4.html）

――――、「偽造キャッシュカード問題等に対する対応状況（平成 26 年 3 月末）について」、2014 年 8 月 27 日（http://www.fsa.go.jp/news/26/ginkou/20140827-5.html）

警察庁、「平成 26 年上半期のインターネットバンキングに係る不正送金事犯の発生状況について」、2014 年

全国銀行協会、「盗難通帳、インターネット・バンキング、盗難・偽造キャッシュカードによる預金等の不正払戻し件数・金額等に関するアンケート結果および口座不正利用に関するアンケート結果について」、2015 年

Bond, Mike, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, and Ross Anderson, “Chip and Skim: Cloning EMV cards with the pre-play attack,” 2014 IEEE Symposium on Security and Privacy, 2014, pp. 49–64.

Murdoch, Steven J., Saar Drimer, Ross Anderson, and Mike Bond, “Chip and PIN is Broken,” 2010 IEEE Symposium on Security and Privacy, 2010.

Oswald, David, and Christof Paar, “Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World,” *CHES 2011, LNCS*, Vol. 6917, 2011, pp. 207–222.