第9回情報セキュリティ・シンポジウム「リテール・バンキングのセキュリティ」の模様

１．はじめに

金融研究所は、平成19年3月6日、「リテール・バンキングのセキュリティ」をテーマとして、第9回情報セキュリティ・シンポジウムを開催した。

偽造キャッシュカード犯罪の被害は、主として預金引出限度額の引下げと利用者への注意喚起の効果によって、ようやく沈静化に向かいつつある。しかし、カード犯罪の未然防止策として導入された生体認証やICカードといった新しい情報セキュリティ技術は、現時点ではあまり普及しておらず、その特性が十分に活かされているとはいいがたい状況にある。偽造カード犯罪の根が絶たれたとはいえない現状において、金融業界は、むしろ抜本的なセキュリティ対策を講じるための一時的な猶予が与えられたと受け止めるべきであろう。

今回のシンポジウムは、こうした問題意識から、金融業界がリテール・バンキングのセキュリティを抜本的に改善するためのグランドデザインを描いていくうえで必要とされる検討材料を提示することを目的に開催された。キーノート・スピーチでの問題提起に続き、偽造カード犯罪の未然防止策の「旗印」に掲げられている①生体認証と②ICカードについて、おのおのの技術の安全性を巡る最新の研究結果を報告するとともに、金融業界が今後これらの技術を有効に活用していくための留意点や検討課題についても整理した（プログラムは次頁のとおり）。

フロアには、金融業務における情報セキュリティ対策を担当している金融機関関係者のほか、暗号学者、情報セキュリティ技術に関係の深い官庁関係者、電機メーカーの研究開発部門・標準化部門の実務家や技術者等、約100名の参加を得た。

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）。

●**キーノート・スピーチ**「リテール・バンキングのセキュリティ向上を目指して」
― 岩下直行（日本銀行金融研究所情報技術研究センター長）
●**発表1**「静脈認証システムのテスト物体によるセキュリティ測定・評価」
― 松本 勉（横浜国立大学大学院環境情報研究院教授）
●**発表2**「生体認証システムのセキュリティ：どこまで評価できるか？」
― 宇根正志（独立行政法人産業技術総合研究所情報セキュリティ研究センター）
●**発表3**「ICカード利用システムのセキュリティ：ビジネス環境拡大への対応とその課題」
― 廣川勝久（日本銀行金融研究所情報技術研究センター）
●**発表4**「システム設計から見たICカードの暗号技術の安全性について：EMV仕様を中心に」
― 神田雅透（NTT情報流通プラットフォーム研究所）
●**総括コメント** ― 今井秀樹（中央大学理工学部教授・独立行政法人産業技術総合研究所情報セキュリティ研究センター長）

（備考：所属についてはシンポジウム当日現在のもの）

2．キーノート・スピーチ「リテール・バンキングのセキュリティ向上を目指して」

岩下は、標記論文[1]に基づき、リテール・バンキングの抜本的なセキュリティ向上の必要性について、次のとおり問題提起を行った。

(1) 偽造キャッシュカード被害の推移

2004年から2005年にかけて、偽造キャッシュカードによる不正預金引出が社会問題化し、わが国の金融機関における情報セキュリティ対策に関して世間の関心が高まった。2005年1月には、ゴルフ場の貴重品ロッカーからキャッシュカードを盗み出してスキミングする手口で不正預金引出を行っていたグループが逮捕され、その手口が大きな扱いで報道されると、金融機関の対応を批判する声が相次いだ。このため、銀行業界は、キャッシュカードを偽造されないようにするためにキャッシュカードのICカード化とATMにおける生体認証による本人確認を導入することや、

1 岩下直行、「リテール・バンキングのセキュリティ向上を目指して」、本号所収。

被害の拡大を防ぐためにキャッシュカードの利用限度額を引き下げること等について、各行が積極的に検討していくことを申し合わせた。

偽造キャッシュカードの被害は、2004年度、2005年度と高水準で推移した後、2006年度になって、件数、金額とも、大幅に減少しつつある。特に2006年度（4～12月の9ヵ月間）の被害金額の水準は、社会問題化する以前の2003年度の水準にまで低下してきている。

（2）どの対策が有効だったのか

偽造キャッシュカードの被害を減少させるのに最も有効な対策であったと考えられるのは、キャッシュカードの利用限度額の引下げである。この対策は、ほぼすべての金融機関で実施されており、1件当たりの平均被害額の低下に直接的に寄与したことに加え、犯罪者にとってキャッシュカードの偽造が「割に合わないビジネス」となったことから間接的に被害件数の減少にも寄与し、それらの相乗効果で被害金額が減少したものと考えられる。このほか、金融機関が利用者に積極的に警告を発した効果等により、利用者がカードや暗証番号を慎重に取り扱うことになったことも有効であったと考えられる。

これに対し、セキュリティ対策の「旗印」として掲げられた、ICカードや生体認証等の事前予防対策については、現時点でのICキャッシュカードへの切替えが限定的なものにとどまっていることからも、被害の減少に大きく寄与したとは考えにくい。また、仮に生体認証付きのICカードを利用しているケースであっても、現段階で発行されているICキャッシュカードのほとんどは、磁気ストライプも貼付されているため、磁気データのみを偽造することで不正預金引出が可能である。こうした現在の仕組みを前提とすれば、ICカードや生体認証に、不正預金引出の被害を減少させる強い効果を期待することは難しいといわざるを得ない。

（3）今考えるべき課題

金融機関のセキュリティを巡る状況は、各金融機関が実施したセキュリティ対策により、いわば緊急事態を脱し、平時に復したように窺われる。ただし、現状は、主として利用者の利便性に制限を加え、利用限度額を引き下げることで被害金額をおさえこんでいる状態であり、偽造カード犯罪の根が絶たれたわけではない。こうした視点に立てば、このタイミングでセキュリティ対策の手を緩めるのは適当ではなく、検討を行うための時間的猶予が生じたと受け止めて、従来十分には対応できていなかった、抜本的なセキュリティ対策の検討を進めるべき時期ではないだろうか。

（4）キャッシュカードのICカード化を巡って

ICカードには、金融機関のシステムをクローズド・ネットワークで守るという従来

のセキュリティの設計思想を抜本的に変えていく潜在的な力がある。ICカードとホスト・コンピュータとが直接通信する仕組みを組み込み、トランザクション単位でセキュリティを確保するアプローチに変更していくことにより、信頼性の低いネットワークを利用する業務でも安全に取引を行うことができるようになるからである。

また、ICカードが抱える現実的な問題点として、現在の標準的な技術が既に古いものになりつつあることが挙げられる。現在普及しているICカードに直ちに問題があるわけではないが、これから本格的にICカード化を進めていく場合、実装段階においてこうした点を必要に応じて考慮していくことが、ICカードの安全性を維持するとともに、円滑な普及につながるものと思われる。

(5) 生体認証をどう普及させるべきか

偽造・盗難カード預貯金者保護法は、偽造カードのみならず、盗難カードの被害の補償を定めている。ICカードへの切替えだけでは盗難カードによる被害を防ぐことができないので、生体認証の導入によって本人認証手段のセキュリティを高めていくことは、今後是非必要なことであろう。

生体認証が広く利用されるためには、生体認証に対する理解と信頼を深めることが大切である。生体認証に関する多様な受け止め方が存在することを踏まえて、問題点を十分に検討し、その結果をオープンにしていくことによって、信頼を勝ち得ていくことが必要である。

(6) 短期的な課題と中長期的な課題

リテール・バンキングのセキュリティ上の問題を考えるうえでは、解決すべきものが短期的な課題か、中長期的な課題かを峻別して分析することが有用である。短期的な課題としては、金融機関の実務に利用されているシステムのセキュリティの実態に関するものが多い。既に広く普及してしまっている現行の脆弱な個人認証メカニズムについては、運用面も含めた対策により、その被害を限定することに努めていくしかない。しかし、今後、次世代のシステムに移行したときに、そのシステムのセキュリティのレベルが低いままとなってしまうことを避けるためには、短期的な課題に対処しつつ、次世代のシステムのセキュリティを巡る中長期的な課題についても検討していかなければならない。

情報セキュリティ対策は、ある程度、将来発生する問題を予測しながら対策を講じていくことが必要となる。そのような予測を的確に行うためには、アカデミックな最新の研究成果を意識し、その情報を活用していくことが重要であろう。また、環境の変化に伴い、現場の実務知識だけでは決断を下せないことがある。適切なセキュリティ対策を行うためには、それまで業界内での常識とされてきた慣行に異を唱え、きちんと体系付けられた、アカデミックな情報を収集し、それに基づいて判断することが必要であろう。

３．発表1「静脈認証システムのテスト物体によるセキュリティ測定・評価」

松本は、静脈認証システムの人工物の受入れに対するセキュリティ測定法について、2件の研究論文[2]で報告された実験結果に基づき、次のとおり発表を行った。

(1) 生体認証システムにおける「身体部分でないものの受入れ」

生体認証は、失念のおそれのある記憶ベースの認証や、紛失・盗難のおそれのある所持物ベースの認証と比べ、情報の管理が容易な生体情報を認証に用いていることから、利便性の高い認証方式として注目されている。

生体認証システムは、通常、読取装置を用いて身体部分（指紋、静脈、虹彩等）から生体情報を取得し、必要に応じてパターン抽出を行い、あらかじめ登録された情報との類似度を計算する。そのうえで、この類似度が設定された判定しきい値以上であれば本人であると判断することで認証を行うというものである。

生体認証システムについては、身体部分とは異なる物体を登録できる、あるいは、身体部分とは異なる物体を提示しても登録情報と一致すると判断されうるという潜在的脆弱性（身体部分でないものの受入れ）が存在し、これが顕現化した場合には、当該物体を用いたなりすましが可能となる[3]。したがって、身体部分でないものの受入れに関するセキュリティ評価が必要である。こうしたセキュリティ評価を定量的に行うことができれば、性能条件・運用条件等から導かれるセキュリティ要件を明確に表現できるようになり、求められるセキュリティ要件を満たす生体認証システムの設計や導入も容易になるであろう。さらに、このようなセキュリティ評価手法の確立は、よりセキュリティの高いシステムの開発・研究にもつながると考えられる。

(2)「身体部分でないものの受入れ」に対するセキュリティの測定

「身体部分でないものの受入れ」に対するセキュリティ評価は、生体認証システムが受け入れる物体としてどのようなものが存在するのかをまず特定することが必要である。具体的には、さまざまな種類のテスト物体を用意し、各テスト物体の受入状況を観測することに加え、これを複数の生体認証システムで比較することも含め、より体系的に評価する必要がある。

2 松本 勉・田中瑛一、「指血管パタン認証システムのテスト物体によるセキュリティ測定法」、コンピュータセキュリティシンポジウム2006予稿集、情報処理学会、2006年、639〜644頁。
松本 勉・田中瑛一、「指静脈認証システムのテスト物体によるセキュリティ測定法の研究」、2007年暗号と情報セキュリティシンポジウム予稿集、電子情報通信学会、2007年。

3 指紋、虹彩、指静脈をそれぞれ利用した市販の一部の生体認証システムについて、身体部分とは異なる物体によるなりすましが可能であることが報告されている。

テスト物体については、①認証に利用する身体部分が何か、②どのような方法で生体情報を取得するか、③どのような製法でテスト物体を作製するかにより分類することができる。生体認証システムについても、例えば、身体部分を指静脈とした場合には、①赤外線カメラによる指静脈の撮像、②血管パターン抽出処理（マッチドフィルタ、暗線追跡等）、③類似度計算処理（相互相関値、画素値一致率等）という3つの主な処理により分類することができる。

こうして分類したテスト物体を、実際に評価対象の生体認証システムに提示することにより、当該システムが受け入れやすいテスト物体について評価することができる。逆に、分類した生体認証システムに対して、同一のテスト物体を提示することにより、当該テスト物体に対してセキュリティの高いシステムがどのようなものかを評価することができる。

（3）指静脈認証システムに対するセキュリティ測定法

生体認証システムの内部処理に関する情報が得られる場合には、これらを利用した評価（ホワイトボックス評価）を行うことができる。しかし、製品に適用された技術の漏洩防止やセキュリティの観点から、生体認証システムの処理に関する情報が公開されない場合がある。このような場合においても、セキュリティを評価していくことが重要であるため、評価対象システムの処理に関する情報を利用しない評価（ブラックボックス評価）の手法が必要である。

ホワイトボックス評価では、身体部分を登録したシステムにテスト物体を提示する、あるいは、テスト物体を登録したシステムに身体部分を提示することにより類似度を測定することができる。また、本人であるか否かに利用する判定しきい値をさまざまな値に設定し、類似度と比較することで、各判定しきい値における誤り率（誤判定する確率）についても測定することができる。さらに、提示するテスト物体を固定し、生体認証システムの各処理の組合せを変えて類似度や誤り率を測定することにより、当該テスト物体に対してセキュリティの高いシステムがどれかを体系的に評価することもできる。今回は、独自に構築した8種類の指静脈認証システムについて、指の赤外線撮影画像を印刷したOHPフィルムを重ねて作製したテスト物体群を用いて、①テスト物体の登録成功率、②登録されたテスト物体に対する生体指の認証成功率および相互の類似度、③登録された生体指に対するテスト物体の認証成功率および相互の類似度についての実験結果からホワイトボックス評価を行う手法を示した。

ブラックボックス評価では、複数のテスト物体を提示し、その結果、受け入れられたか否かを観測し、誤り率を測定する。同様に、登録した個々のテスト物体に対し、身体部分を提示した際の誤り率についても測定する。これらの誤り率を用いることで、評価対象システムのセキュリティを評価することができるが、内部処理に関する情報が得られないため、生体認証システムの内部処理のさまざまな組合せに対する体系的な評価を行うことはできない。今回は、市販の1種類の指静脈認証シ

ステムについて、指の赤外線撮影画像を印刷したOHPフィルムを重ねて作製したテスト物体群を用いて、①テスト物体の登録成功率、②登録されたテスト物体に対する生体指の認証成功率、③登録された生体指に対するテスト物体の認証成功率についての実験結果からブラックボックス評価を行う手法を示した。

(4) セキュリティ測定法の今後の展望

生体認証システムの内部処理に関する情報の有無にかかわらず、複数のテスト物体を用いて誤り率を測定することにより、定量的にセキュリティを測定する手段を確立することが重要である。また、生体検知機能が組み込まれているとされる個々の実用システムのセキュリティを明らかにし、想定されるアプリケーションの要求レベルを、そのセキュリティが満たしているかを検討していく必要がある。

4．発表2「生体認証システムのセキュリティ：どこまで評価できるか?」

宇根は、田村との共同論文[4]に基づき、生体認証システムのセキュリティ評価の現状と課題について、次のとおり発表を行った。

(1) 生体認証の脆弱性と攻撃方法

生体認証システムのセキュリティ対策では、想定される脅威と脆弱性を明確化し、考慮すべき攻撃方法を想定したうえで、考えられるセキュリティ対策技術の中から十分なセキュリティ・レベルを確保していると評価されたものを採用することが望ましい。こうした手順は、一般の情報システムのセキュリティ対策の場合と同様であるが、生体認証特有の脆弱性には特に留意すべきである。

生体認証システムにおける代表的な脅威として、なりすましが挙げられる。なりすましにつながりうる脆弱性としては、①生きた本人の生体から直接取得した情報でなくても本人と誤判定してしまう、②運用環境の変化が照合精度に影響を与える、③システム内部が不正に改変されるといった点が知られている。このうち①の脆弱性を利用して実行される攻撃方法としては、センサに誤判定を生じさせる情報を提示することでなりすましを試みる方法がある。具体的には、(a)攻撃者やその協力者が自分の生体情報を提示するゼロ・エフォート（zero-effort）攻撃、(b)なりすましの対象者（以下、攻撃対象者と呼ぶ）の生体情報を人工物によって提示するクローン攻撃、(c)攻撃対象者から切除された身体部分を提示する生体特徴切取攻撃、

4 田村裕子・宇根正志、「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」、本号所収。

(d) 候補となる情報を総当たりで提示するブルート・フォース（brute-force）攻撃、(e) 最近提案されたウルフ攻撃[5]が知られている。

ウルフ攻撃は、生体認証システムの内部構造に関する情報を解析して、最も多くのテンプレート[6]と誤って一致する入力情報（ウルフと呼ばれる）を探し出し、その入力情報を提示するという攻撃である。ある照合・判定アルゴリズムにおいては、判定しきい値によらず、候補となるすべてのテンプレートと100%の確率で一致するウルフが存在することが示されており[7]、留意すべき攻撃の1つであることが既に学会において認識されている。

ウルフ攻撃への対策として生体認証システムの内部構造を秘匿すればよいとの見方もある。しかし、攻撃者がリバース・エンジニアリングによってシステムの内部構造に関する情報を入手する可能性を排除することは困難であり、十分な対策とはいえない。また、こうした可能性を残したままでは、ユーザは安心して生体認証システムを利用することはできない。

(2) 対策技術に関するセキュリティ評価の現状

センサになんらかの情報を提示してなりすましを試みる攻撃については、さまざまな対策技術が提案されている。しかし、その効果を定量的に評価可能な対策技術は非常に限られているのが実情である。すなわち、定量的な評価尺度が存在するのは、ウルフ攻撃およびゼロ・エフォート攻撃への対策技術のみである。ウルフ攻撃については、その成功確率の最大値であるウルフ攻撃確率が提案されているほか、ゼロ・エフォート攻撃については、照合精度尺度の1つである誤受入率や誤合致率といった誤り率が評価尺度となる。

クローン攻撃への対策技術としては、攻撃対象者の生体特徴の推測を困難にする、生体以外を検知するといった手法が知られている。生体特徴の推測を困難にする手法としては、推測に利用する情報を扱うシステムからの漏洩を困難にする耐タンパー化手法や、テンプレートからの生体特徴の復元を困難にするキャンセラブル・バイオメトリクスと呼ばれる手法が知られている。しかし、いずれも定量的な評価尺度や評価手法が確立していない。一方、生体以外を検知する手法としては生体検知手法が知られているものの、現時点では、テスト物体を利用した複数のシステムの比較評価が可能であるというレベルにとどまっており、定量的な評価尺度に基づくセキュリティ・レベルの絶対評価が実現するまでには至っていない。

5 宇根正志・大塚 玲・今井秀樹、「生体認証システムにおける新しいセキュリティ評価尺度：ウルフ攻撃確率」、2007年暗号と情報セキュリティシンポジウム予稿集、電子情報通信学会、2007年。
6 生体認証システムにあらかじめ登録されている個人の生体情報から抽出された固有のデータ。
7 渡邉直彦・繁富利恵・宇根正志・大塚 玲・今井秀樹、「指静脈パターン照合アルゴリズムにおけるユニバーサル・ウルフ」、コンピュータセキュリティシンポジウム2006予稿集、情報処理学会、2006年、621〜626頁。

このように、なりすましへの対策技術においては、セキュリティ評価を実施するための定量的な尺度や手法がほとんど確立しておらず、生体認証システムの定量的なセキュリティ評価は実施困難であるとみられる。ユーザは、「有効なセキュリティ対策技術を採用している」ことを確認することができず、安心して生体認証システムを利用しづらい状況におかれていると考えられる。

(3) 安心して活用できる生体認証システムの実現に向けて

こうした現状を改善し、生体認証システムを安心して利用可能とするためには、各対策技術の定量的なセキュリティ評価手法の開発・確立を最優先課題として行動することが必要である。生体認証システムのベンダは、こうした評価手法が確立されれば、「セキュリティ評価済みの生体認証システム」を提供できるようになるというメリットがある。2006年秋の時点で調査したところ、セキュリティ評価手法の開発を目的とした研究プロジェクトは海外では皆無に近い状況にあるようである。今後、わが国が最初にセキュリティ評価手法を開発・確立し、そうした手法によって評価されたシステムを海外の市場へ投入するというシナリオも、産業振興の観点から十分に検討に値すると考えられる。

ユーザである金融機関は、生体認証システムのセキュリティ評価手法が十分に確立していないという現状を踏まえたうえで、現在利用している、または、今後導入を予定・検討しているシステムのセキュリティ評価結果をベンダやシステム・インテグレータに確認し、その内容を慎重に見極めることをお願いしたい。こうした働きかけは、ベンダやシステム・インテグレータに、セキュリティ評価手法の開発がユーザからの要望であるとの認識をもたらし、現状の改善に向けた活動を少しでも促すことにつながると考えられる。今後、金融機関からのこうした積極的な働きかけを期待したい。

5．発表3「ICカード利用システムのセキュリティ：ビジネス環境拡大への対応とその課題」

廣川は、田村との共同論文[8]に基づき、ICカードを利用したシステムのセキュリティについて、次のとおり発表を行った。

(1) ICカードの機能を活用したリスク管理

偽造キャッシュカード問題への対策として導入が進められているICカードは、リ

8 田村裕子・廣川勝久、「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」、本号所収。

テール・バンキング・システムに介在する端末やネットワークのセキュリティが十分に確保できない場合においても、安全な取引を実現することができるデバイスである。ただし、端末、ホスト・システム、ネットワークのICカード対応状況によっては、ICカードの機能を十分に活用できない場合がある。

「フルICカード対応」[9]のシステムであれば、リテール・バンキングでの取引がカード所持者によって真正なカードを使用して行われていることの確認や、取引内容を示すデータがICカードによって生成されたことの確認（取引データの正当性確認）を、EMV仕様[10]に示されている「取引のオンライン承認」によって実現可能である。取引のオンライン承認では、従来のシステムで送受信されている取引データに加えて、取引データを反映した暗号情報（AC: application cryptogram）がICカードによって生成され、ホスト・システムに伝送される。ACは、取引データ等に対するMACであり、その検証によって、ホスト・システムは取引データがICカードによって生成されたものであり、かつ、改ざんされていないことを確認できるようになる。また、過去に利用されたデータを利用して不正を行うことができないようにするため、MACの対象となるデータには端末が生成した乱数も含まれている。さらに、取引可否を示す電文にもホスト・システムが生成した暗号情報が付与されるため、ICカードはホスト・システムの認証を行うこともできる。

（2）カードを利用した取引を取り巻く環境

オンライン提携の拡大に加え、デビットカード取引の導入等、キャッシュカードの利用環境は大きく変化している。自行の管理下にある端末やホスト・システムのみを利用するシステムでは、システムへの安全対策は比較的講じやすいといえる。一方、自行の管理下にない部分を含む取引システムでは、各関係組織におけるリスク管理の考え方も異なることから、他の組織との間での権限や責任の範囲の明確化が必要になるとともに、それに基づいた安全対策が重要になる。

（3）フルICカード対応の効果

端末がICカード対応であっても、端末とホスト・システム間の電文形式として、磁気ストライプ（MS: magnetic stripe）カードのみに対応している従来のシステムと同じものを使用しつづけた場合、ホスト・システムはICカードとMSカードのいずれが利用されたかを判断することができない。この場合、キャッシュカードをICカードに切り替えても、磁気データをコピーした不正MSカードによる預金引出が

9 リテール・バンキングを構成するすべての端末とホスト・システムがICカードとの処理を実行可能であり、ICカードに関連する新規項目を従来の電文に追加可能である場合を「フルICカード対応」と呼ぶ。

10 ICカードと端末の技術的な要件や通信プロトコルを定めた国際的なデファクト標準であり、MasterCard International、Visa International、JCBの3社が出資するEMVCo. によって策定・維持されている。

可能であるため、ICカード導入の効果は十分に発揮できない。

これに対し、フルICカード対応のシステムでは、AC等を用いた取引データの正当性確認が可能であるため、自行のホスト・システムと自行が発行したICカード間の取引を安全に実行することができる。さらに、ICカードによるホスト・システムの認証機能を利用して、ICカード内のリスク管理面の制御等[11]も可能になる。

(4) フルICカード対応へのシステム移行

わが国の金融機関は、現在、キャッシュカードのICカード化と端末のICカード対応を進めている段階であるが、今後、フルICカード対応への移行を進めるにあたっては、先行して実施されているクレジット業界のシステム・マイグレーションが参考になると考えられる。

例えばVisa Internationalでは、ICカードの発行に際して、加盟店端末とカード発行機関のホスト・システム間のネットワークをICカード対応させることによって、AC等のICカード関連の新規項目が、端末とホスト・システム間で欠損してしまうことがないようにしている。ICカードが生成したACをホスト・システムに送信することができれば、ICカード対応が遅れているカード発行機関が一部に存在したとしても、ICカード対応が進んだカード発行機関ではフルICカード対応の効果を享受できる。

(5) ビジネス環境拡大への対応とその課題

従来のリテール・バンキング・システムは、設備がすべて自行の管理下にあることを前提に、それへの安全対策を施すことで、システム全体の安全性を確保してきた。しかし、今後、自行の管理下にない環境に設置された端末やオープンなネットワークを利用することによりサービスを拡大するのであれば、ICカードが備える機能を活用した安全な取引を実現することが必要であり、そのためにはシステムをフルICカード対応させることが望まれる。わが国の金融業界では、フルICカード対応への移行を特定の期限までに全行一斉に行うことが望ましいとされている。しかし、全行一斉のシステム・マイグレーションには困難が伴うと考えられることから、クレジット業界で実現されたMSカードとICカードの混在を前提としたシステム・マイグレーションを参考にすることが有益であると考えられる。暗号技術等の発展やさらなるサービスの拡大への対応を意識した拡張性を考慮しつつ、早期にフルICカード対応への移行を検討することが望まれる。

11 例えば、PINの誤入力が許容回数を超えた場合、ICカード側で当該カードを利用した取引が実行できないように制御される。このようにホスト・システムの認証が可能であれば、リモートでホスト・システムから取引の実行を可能とするように制御を行うことができる。

6．発表4「システム設計から見たICカードの暗号技術の安全性について：EMV仕様を中心に」

神田は、鈴木との共同論文[12]に基づき、ICカードを用いたシステムで利用する暗号技術の安全性について、次のとおり発表を行った。

(1) EMV仕様から派生するシステム設計・運用上の問題

EMV仕様は、ICカードを用いた取引における技術的なデファクト標準として広く普及しており、わが国においても、このEMV仕様を基に、「全銀協ICキャッシュカード標準仕様」や「ICカード対応端末機能仕様書」等が策定されている。

EMV仕様は、ICカードと端末が備えるべき相互運用のための共通事項を規定する一方で、各カード発行主体が自らのニーズに合わせて詳細な技術要件を独自に設定することができる柔軟性を有している。このため、システムで利用する暗号アルゴリズムの選択によって、セキュリティ・レベルに差異が生じる可能性がある。また、EMV仕様は、継続的な見直しが行われているものの、策定・公開されてから既に10年以上が経過しており、EMV仕様が推奨・例示している暗号アルゴリズムのなかには、現在の暗号技術の水準からみると十分に安全とはいい切れないものも含まれている。

これらは、EMV仕様自体の問題というよりは、EMV仕様のもとで各システムに応じた暗号アルゴリズムを選択する際のシステム設計・運用上の問題といえる。EMV仕様を利用する場合には、各暗号アルゴリズムの特性を踏まえつつ、システムに適したアルゴリズムを選択していく必要がある。

(2) EMV仕様で利用される暗号アルゴリズムの安全性

イ．公開鍵方式に対して想定される攻撃

EMV仕様では、端末やホスト・システムがカードの真正性を確認するために公開鍵証明書等を利用しており、公開鍵証明書を生成するための推奨アルゴリズムとしてRSA署名を挙げている。したがって、RSA署名を偽造することができれば、不正なICカードを用いて、真正であると誤認させることができると考えられる。

現在広く普及しているRSA署名であるPKCS#1 v1.5[13]に対して、署名検証に利用

12 鈴木雅貴・神田雅透、「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」、本号所収。

13 PKCSは、米RSA社が定める公開鍵暗号技術をベースとした規格群のことであり、PKCS#1では、RSAを用いた暗号化方式とデジタル署名方式を定めている。このうち、PKCS#1 v1.5の署名方式は守秘、認証等のセキュリティ機能を持つ電子メール用プロトコルであるS/MIME（Secure Multipurpose Internet Mail Extension）に実装される等、業界標準として広く利用されている。

する公開指数[14]が$e=3$であり、かつ、検証時に署名が付与されているメッセージ形式の検査が不十分である場合には、署名の偽造が可能となる場合があることが指摘されている。この攻撃の前提条件と、EMV仕様で定められている署名検証処理に共通点があるため、この攻撃に類似した攻撃の可能性に注意する必要がある。

ロ．共通鍵方式に対して想定される攻撃

EMV仕様では、取引がカード所持者によって真正なカードを使用して行われることの確認や、取引内容を示すデータがICカードによって生成されたことの確認を行うために、ICカードが生成し取引データを反映した暗号情報としてACを利用している。ACは取引ごとに異なるセッション鍵を用いて生成されているため、ACからセッション鍵を逆に特定できるような場合には、金額等を改ざんした取引データに対するACを偽造することが可能となる。

EMV仕様は、2つのAC生成方式を推奨している。このうち、一方の方式は、セッション鍵を特定する攻撃に対して、攻撃者が取引データとACのペアを大量に入手できる場合には、DESと同程度の安全性しか持たない。

また、EMV仕様における鍵生成は、発行者が管理するシステム鍵からICカードに格納されるマスタ鍵を生成し、マスタ鍵からセッション鍵を生成するという階層構造になっている。このため、鍵生成における階層構造を遡り、セッション鍵からマスタ鍵を解読することができるならば、別のセッション鍵を不正に生成し、改ざんした取引データに対するACを偽造することが可能となる。

また、システム鍵からマスタ鍵を生成する際に利用するアルゴリズムとして例示されている2-keyトリプルDESについては、大量の平文（口座番号等の情報）と暗号文（マスタ鍵）のペアを入手可能なときは、全数探索法よりも効率的にシステム鍵を求めることができる。

（3）システムとしての安全性

上述した各暗号アルゴリズムに対する攻撃は、実環境において攻撃の前提条件を満たすことが困難であるため、直ちに脅威になるとはいえない。しかし、システムとしての安全性を考えた場合には、このような攻撃に対して耐性を備えたより安全な暗号アルゴリズムに移行していくことが理想的な対策であるといえる。

しかし、実際には、システムの相互運用性の確保や技術的な問題等により、安全な暗号アルゴリズムへの移行が困難な場合も考えられる。その場合には、例えば、十分な平文と暗号文のペアを集められないよう定期的に鍵を更新する等、システムの運用に制約を設けることが次善の策として考えられる。ただし、長期に運用するシステムであるならば、アルゴリズムの移行を含めた抜本的な見直しが必要となろう。

14 RSA署名における署名検証では、署名sに対して、公開指数eを利用して$SR = s^e \bmod n$を計算したうえで、メッセージ形式SRの検査を行う。

7．フロア参加者からの主な意見等

キーノート・スピーチに関連して、**フロア参加者**からは、偽造キャッシュカード問題が沈静化したとは必ずしもいいがたく、今後も引き続きセキュリティ対策の向上に努めることが重要であるとの意見が寄せられた。

発表2に関連して、**フロア参加者**は、まず、ベンダもオープンな場で生体認証システムの評価手法に関する検討を行うことが望ましいとの考え方を示したうえで、テスト物体を用いた実際の商用システムの生体検知に関するセキュリティ評価について、各ベンダの内部の取決めにより製品に関する情報を公開できないことが多く、ベンダがそうした検討を行うための体制作りは難しいとコメントした。

別のフロア参加者は、生体認証システムの評価手法を確立することの必要性について同調したうえで、生体認証システムのセキュリティ評価の枠組みとしてどのようなものを策定すべきかと質問した。これに対して**宇根**は、生体認証システムのユーザからのセキュリティ評価手法の必要性に関する要望を受けて、学会・産業界で自主的な検討が進められることが望ましいとしたうえで、セキュリティ評価手法が確立したという状況を前提とすれば、評価の枠組みの候補としてISO等の国際標準や政府調達基準が考えられると述べた。すなわち、現在国際標準案の段階にあるISO/IEC 19792では、コモン・クライテリア[15]をベースとして、生体認証システムのセキュリティ評価を行うための枠組み等を規定する方向で検討が進められており、こうした枠組みを利用することができるのではないかと説明した。また、米国立標準技術研究所（NIST）ではさまざまな政府調達標準（FIPS）を策定しており、わが国においても同様のアプローチによって、生体認証システムに関する政府調達基準を策定し、その基準を活用して評価の枠組みを検討することも考えられると説明した。

また、**別のフロア参加者**からは、データベースに登録されたテンプレートの保護に関する研究動向について質問が寄せられた。これに対して**宇根**は、テンプレートが漏洩した場合でもそのテンプレートから生体情報を推定することを困難にする手法の研究も進められていることを説明したうえで、新しい手法の提案に関する研究成果は多いが、定量的なセキュリティ評価の手法に関しての検討はほとんど知られていないのが実情であると述べた。

さらに、**別のフロア参加者**からは、生体認証システムに生体情報を登録できないという脆弱性についても検討が必要なのではないかとの質問が寄せられた。これに対して**宇根**は、そうした生体認証システムの未対応率の問題は、本人拒否の問題とともにユーザからの改善要望の多くの部分を占めており、利便性向上の一環としてベンダが積極的に検討を行っているのが実情であると説明し、そうしたベンダの努

15 情報システムやそれを構成するハードウエア・ソフトウエアについて、そのセキュリティ機能が適切に設計され、その設計が正しく実装されているかを評価・認証するための基準。ISO/IEC 15408として国際標準化されている。

力によって今後改善が進んでいくことが見込まれるとの見方を示した。

8．総括コメント

今井は、キーノート・スピーチと研究発表の内容を振り返りつつ、次のとおり総括し、シンポジウムを締め括った。

今回のシンポジウムでは、「リテール・バンキングのセキュリティ」をテーマとして、生体認証とICカードの理論と運用に関する研究成果が発表された。これらは、適切に利用すればリテール・バンキングの安全性を大きく高めることのできる技術として期待できる。しかし、アカデミックな検討と実用システムへの適用の間にはギャップがあり、現状では十分に活かしきれているとはいえない状況にある。理論的に可能な攻撃は、いずれは実用システムにも及んでいくものである。こうした攻撃への対策を実用システムでも早めに講じておかないと、やがて情報セキュリティ上の問題に直面することとなる。金融業界のリテール・バンキング・システムの構築に携わる方々が、このような問題意識を共有して、具体的な対応策について活発に議論していくことになれば、今回のシンポジウムは有益だったといえよう。

わが国では、電子マネーが普及し始めており、電子マネーを巡る問題も、技術的な観点だけでなく、社会的・経済的な観点も増え始めている。今後、体系的・総合的な検討が必要である。日本銀行金融研究所情報技術研究センターにおいても、こうした電子マネーに関する研究を今後一段と積極化することを期待したい。独立行政法人産業技術総合研究所情報セキュリティ研究センターとしても、この分野を通じて、さらなる連携を深めていきたいと考えている。