第 15 回
情報セキュリティ・シンポジウム
「多様化するリテール取引の安全性 II：モバイル化、クラウド化を支える情報セキュリティ技術を中心に」の模様

1. はじめに

日本銀行金融研究所は、2014 年 3 月 5 日、「多様化するリテール取引の安全性 II：モバイル化、クラウド化を支える情報セキュリティ技術を中心に」をテーマとして、第 15 回情報セキュリティ・シンポジウムを開催した（プログラムは次頁のとおり）。

最近のリテール取引を見渡すと、ユーザあるいは加盟店におけるスマートフォン等を使ったモバイル決済サービスが一段と広がりをみせつつある。例えば、安価なカードリーダを接続したスマートフォンを決済端末として利用するサービス等が台頭し、その手軽さゆえに多くの関係者の注目を集めている。また、バンキングや情報管理ツール等のさまざまなアプリケーションは、スマートフォンや PC 等の複数の端末を使い分けるユーザにも対応し、クラウドとの連携を深める傾向にある。こうした新しいサービスについては、従来とは異なる発想のビジネスモデルであることも多く、その安全性がどのように確保されているのかがわかり難い。他方で、学界の研究成果の中には実用性の高いものもあり、こうした成果を取り込むことで、さらに安全性を高めることが可能な場合もあると考えられる。

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

こうした問題意識に基づき、今回のシンポジウムでは、安全な取引処理を支える要素技術や応用技術として、①モバイルでの利便性を兼ね備えた本人認証として注目される「モバイル・バイオメトリクス」技術、②多要素認証の 1 要素として今後も利用されていく可能性があるパスワードの管理技術、③クラウドでの処理を安全に行うために有効な「暗号化状態処理技術」を取り上げ、各技術について専門家や当研究所スタッフによる講演が行われた。また、「モバイル決済技術の現状と課題」と題するパネル・ディスカッションも行った。

本シンポジウムのフロアには、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庁関係者、暗号学者、システムの開発・運用に携わる実務家や技術者等、約 100 名が参加した。

以下では、次頁の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 15 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「多様化するリテール取引の安全性 II：
  モバイル化、クラウド化を支える情報セキュリティ技術を中心に」
  松本　勉（横浜国立大学大学院教授）
- 講演 1「モバイル・バイオメトリクスを巡る動き」
  新崎　卓（ISO/IEC JTC1/SC37/WG3 国内委員会主査、
  富士通研究所主管研究員）
- 講演 2「多要素認証の 1 要素であるパスワードの安全な管理方法：
  パスワードリスト攻撃を踏まえて」
  鈴木雅貴（日本銀行金融研究所主査）
  ※古原和邦（独立行政法人産業技術総合研究所研究グループ長）との
  共同研究に基づく講演。
- 講演 3「『暗号化状態処理技術』を巡る最新動向」
  清藤武暢（日本銀行金融研究所）
  ※四方順司（横浜国立大学准教授）との共同研究に基づく講演。
- パネル・ディスカッション「モバイル決済技術の現状と課題」
  パネル発表 1「PayPal の概要」
  松谷　徹（PayPal Pte. Ltd. ヘッドオブビジネスディベロップメント）
  パネル発表 2「契約関係や法制度の側面から考える」
  杉浦宣彦（中央大学大学院教授）
  パネル発表 3「モバイル環境への進展に伴うリテール取引システムの課題」

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。

廣川勝久（日本銀行金融研究所テクニカル・アドバイザー）

（自由討論）

パネリスト：杉浦宣彦、新崎　卓、廣川勝久

モデレータ：松本　勉

- 総括コメント

今井秀樹（中央大学教授）

2.　キーノート・スピーチ「多様化するリテール取引の安全性 II」

松本 は、環境変化によって登場した新しいリテール取引の形態や、同形態の安全性を考えるうえでのポイント等について、次のとおり発表した。

(1)　リテール取引等を取り巻く環境の変化とその影響

最近の預金の不正払戻しの状況をみると、インターネット・バンキングにおける被害の急増が注目される[2]。その背景には、ログイン時に偽画面を表示することでパスワードだけでなく乱数表等の第 2 認証要素も盗取する攻撃（以下、「MitB：Man-in-the-Browser 攻撃」）等の増加が挙げられる。前回シンポジウムでは、同攻撃への対策として、取引時に振込先や金額等が改ざんされていないことを確認する「取引認証[3]」を取り上げたが、国内でもこうした攻撃の増加を受け、同対策の導入や導入に向けた動きがみられる。

また、リテール取引等を取り巻く環境を見渡すと、①スマートフォン等のモバイル端末の普及、②高速なインターネット通信の低価格化、③アプリケーションのクラウド対応等の動きがみられるほか、攻撃の巧妙化等によって引続き脅威が増大していることが注目される。次に、個々の変化とその変化がリテール取引等に与える影響についてみていく。

2 全国銀行協会［2014］によると、インターネット・バンキングの被害は、1.3 億円、0.6 億円、7.2 億円（2011 年、2012 年、2013 年の順）と 2013 年に急増した。なお、偽造キャッシュカードの被害は、2.8 億円、5.7 億円、0.8 億円（同）と急減した。

3 取引認証（Transaction Authentication）の実現方法は多種多様である。PC と別のデバイス（携帯電話、USB デバイス等）を併用する方法や、1 台の PC 上でウェブブラウザと別の専用ソフトウエアを併用する方法等がある。また、振込先等に紐付いた認証コード（Transaction Authentication Number）を利用する方法や、振込先等にユーザの電子署名を付ける方法（Transaction Signing）等がある。

① スマートフォン等のモバイル端末の普及

従来の携帯電話よりも性能や汎用性が高いスマートフォン等のモバイル端末が普及し、ユーザあるいは加盟店が所有するモバイル端末を活用した新しいリテール取引の形態が登場している。ユーザのモバイル端末を用いる形態には、例えば、オンライン決済等のための本人確認をスマートフォンに搭載された生体認証システムで行う形態（以下、「モバイル・バイオメトリクス」）や、磁気カードに記録されているカード情報等の「決済情報」をスマートフォンに格納しておき、決済時にスマートフォンから同情報を加盟店の決済端末に提示する形態（以下、「ウォレット」）がある。また、加盟店のモバイル端末を用いる形態には、例えば、安価なカードリーダを接続したスマートフォン等をクレジットカード等の決済端末として利用する形態（以下、「スマホ決済」）がある。

② 高速なインターネット通信の低価格化

高速なインターネット通信のサービスは、低価格化しているほか、モバイル端末のデータ通信速度の高速化や街中の無線 LAN 接続ポイントの増加等により、屋外でも利用可能になっている。また、従来から一部の電子商取引では、予め ID に紐付けるかたちで決済情報を登録しておき、取引時には ID に関する本人確認のみで取引を完了させ、バックエンドシステムにおいて同 ID に紐付いた決済情報を用いた決済を行うという形態（以下、「ID 決済」）が利用されている。モバイル端末でも同形態を利用可能になってきており、例えば、ユーザが来店前にモバイル端末から注文しておき、スタッフが店頭で本人確認を行ったうえで商品を渡すというサービスで使われている。

このほか、加盟店の決済端末に関する変化もみられる。従来の決済端末は、決済処理に付随するさまざまな処理[4]も実行しており、多機能かつ高額であった。そうしたなか、カードの読取等の入出力処理以外の処理をクラウドに代行させる形態（「クラウド型決済」と呼ばれる）が登場している。同形態は、決済端末の機能を入出力処理に限定することで価格を抑えられるほか、クラウド側の処理内容を修正することで新しい決済方法等に容易に対応できる点で優れている。

③ アプリケーションのクラウド対応と攻撃の巧妙化

業務遂行のために安価な外部サービスを利用したい、あるいは、複数の端末を保有するユーザが、利用する端末を切り替えてもシームレスにサービスを受けたり自らのデータにアクセスしたりできるようにしたい等のニーズから、クラウドを利用するサービスやアプリケーションが増えている。他方で、クラウド等のサーバか

4 例えば、読み取ったデータの暗号化や、バックエンドシステムから送られてきた暗号文の復号、盗難カード等のネガティブデータとの突合検査等の処理を行う。

ら情報が漏えいする事例も発生している。クラウドを利用したサービスでは、パスワードを用いた本人確認（以下、「パスワード認証」）を行うケースが現在は主流であるが、パスワードを使い回すユーザが多いこともあって、あるサービスから盗取した ID とパスワードを用いて別のサービスへの不正ログインを試行するといった「パスワードリスト攻撃」が新たな脅威として顕現化し始めている。

(2) 今回のシンポジウムの狙い

こうした変化を踏まえ、今回のシンポジウムにおける各講演やパネル・ディスカッションでは、次のような論点を取り上げる。

① 各講演の論点

講演 1 では、モバイル・バイオメトリクスについて取り上げる。金融機関が同技術の利用を検討するためには、技術の実用化レベル、モバイル端末上で生体認証を行うことの利点や留意点等を把握しておくことが望ましい。

講演 2、3 では、クラウドからの情報漏えいリスクの防止に資する技術を取り上げる。具体的には、講演 2 では、ユーザのパスワードをクラウド等に保存し、ユーザからの要求に応じてパスワードを読み出す「パスワード管理技術」に焦点を当て、不正アクセスや不正な管理者等による情報漏えいに耐性を有する具体的な方法について説明する。また、講演 3 では、情報漏えいを防止する対策技術として、クラウド上で暗号化したままデータ処理を行う「暗号化状態処理技術」に焦点を当て、同技術の概要や利用上の留意点等について説明する。

② パネル・ディスカッションの論点

スマホ決済、ウォレット、ID 決済のような決済サービスの定義については関係者のコンセンサスが形成されているとは言い難いが、ここでは「店舗側の決済端末または顧客の端末の少なくとも一方において、モバイル端末を用いた決済サービス」を「モバイル決済」と呼ぶことにする。こうしたサービスは、導入時のハードルの低さや利便性の高さから多くの関心が寄せられているものの、従来とは異なる形態であるため何が安全性の根拠となっているのかがわかり難いという問題がある。そこで、パネル・ディスカッションでは、同問題を取り上げ、将来的なモバイル決済のあり方を模索する。

(3) 金融機関へのメッセージ

スマートフォンやクラウド等の新しい技術が次々と登場しており、今後もそうした技術を活かした安全で利便性の高いサービスが提供されていくことを期待したい。なお、攻撃者の技術も常に高度化するため、何が起きたのかを正しく把握し、対外的に説明できるようにしておくことが一層重要になる。攻撃への対策については、学界の研究成果を活かせるケースもあると考えられることから、研究動向をフォローしたり、金融機関が直面している技術的課題を学界に伝えたりすることも有用であろう。

3. 講演1「モバイル・バイオメトリクスを巡る動き」

新崎は、決済時の本人確認等で利用される「モバイル端末を利用した生体認証(モバイル・バイオメトリクス)」の最新動向について、次のとおり発表した。

(1) モバイル・バイオメトリクスの概要と事例

スマートフォン、タブレット端末、IC カード等のモバイル端末を利用する形態の生体認証(モバイル・バイオメトリクス)が広がりをみせている。モバイル・バイオメトリクスの定義について業界のコンセンサスはまだ形成されていないが、仮に「生体認証に関する3つの処理(生体情報の読取、保存、照合)」のいずれかをモバイル端末で行うもの」と定義すると、次の事例が存在する。

用途例	生体認証に関する処理の概要
オンライン取引時の本人確認	予めスマートフォンに指紋を登録しておき、スマートフォン上で、生体情報を読み取ったうえで照合を行う。
実店舗での ID 決済時の本人確認	予めサーバに顔写真を登録しておき、サーバから店舗レジのタブレット端末に送信された同顔写真を使って、店舗スタッフが支払人を認証する。
実店舗でのカード支払時の本人確認	予め IC クレジットカードに静脈パターンを登録しておき、取引時に店舗レジに設置されたセンサーで読み取った静脈パターンとカード内で照合を行う。

(2) モバイル環境で生体認証を利用する利点

生体認証とパスワード認証を比較すると、①パスワードの強度は個々のユーザに依存するが、生体認証ではそうした個人差が少ない、②パスワードは他人への提供が可能であるが、生体情報は他人への提供が困難、③パスワード認証では本人か否かを一意に識別できるが、生体認証の認証結果には、他人を本人として誤って受け入れるという誤り（「他人受入」と呼ばれる）が一定確率で含まれる等の差異がある。また、日常生活のさまざまな状況や環境（以下、「モバイル環境」）での利用においては、生体認証はパスワード認証よりも次の点で優れる。

- 入力が容易：歩行中や片手での入力、寝室等の暗い部屋での入力等の状況を想定すると、生体認証（指紋、静脈パターン等）では生体情報の提示だけで済むためパスワードよりも入力が容易。
- 覗き見への耐性が高い：電車内やバス内での利用を想定すると、パスワードは覗き見により盗取されるリスクがあるが、生体認証（指紋、静脈パターン等）ではそうしたリスクが想定され難い。
- 紛失し難い：パスワード認証では、パスワードを書いた紙とノート PC を一緒に鞄に入れて持ち歩く不適切な利用者も想定されるが、その際、鞄の紛失によりパスワードとノート PC を同時に盗取されるリスクがある。生体認証では、生体情報を利用するため、こうしたリスクが想定され難い。

(3) モバイル端末で生体認証を利用する際の留意点

モバイル端末での生体認証の利用について 3 つの留意点が挙げられる。1 つ目は、生体情報のデータフォーマット等のデータ互換性についてである。スマートフォン等に搭載されるセンサーは小型かつ安価であることが強く求められる傾向にあることからデータの互換性はあまり考慮されないことが多く、社内システム等のように、一度登録した生体情報をシステム更改後も利用したいというニーズには応えきれない可能性が高いのが実情である。

2 つ目は、スマートフォン等で生体情報を読み取る方法についてである。具体的には、スマートフォン等に標準搭載された「汎用センサー」を用いる方法と別途追加した「専用センサー」を用いる方法がある。汎用センサーは、センサー追加のためのコストが不要であるものの、対応可能なタイプの生体情報（顔等）が限られるほか、スマートフォン等の機種ごとにセンサー性能が異なるため認証精度も機種に依存するという特徴がある。他方、専用センサーは、センサー追加のためのコストが発生するものの、任意のタイプの生体情報（顔、指紋、静脈パターン、虹彩等）

に対応可能であるほか、同じ性能のセンサーをすべてのスマートフォン等に追加することで機種に依存しない認証精度を実現可能という特徴がある。

3つ目は、生体情報のタイプとモバイル環境の相性についてである。例えば、顔認証は満員電車の中や暗い部屋では使い難いほか、音声認証は騒音がある場所での利用は適さない。このため、想定するモバイル環境に応じて生体認証のタイプを選択する必要がある。なお、センサーが低価格化していることを踏まえると、スマートフォン等に複数のタイプのセンサーを搭載し、モバイル環境に応じて使い分けるという考え方も現実的になりつつある。

(4) おわりに

生体認証の利用に関しては、さまざまな国際標準が作成されており、データ互換性や安全性等を確保するための準備が整いつつある。例えば、データフォーマット、認証精度の測定方法、認証結果の信頼性確保（「Authentication Context for Biometrics」と呼ばれる）、登録した生体情報の保護（以下、「テンプレート保護技術」）等に関する国際標準が公表されている。現在は、グミ指等の人工物を用いたなりすましへの耐性評価や、モバイル環境のうちオペレータ等に監視されていない状況での利用等に関する国際標準の審議が行われている。

これまで生体認証は、主として安全性向上を目的として導入されてきたが、近年、利便性向上を目的とした事例もみられるようになった。例えば、ATM取引において、「キャッシュカードと暗証番号」の代わりに「生年月日、生体情報、暗証番号」により本人確認を行うことで、カードの携帯を不要とするサービスが登場している。このように、生体認証を利用することで金融サービス自体の利便性を向上させるような活用方法が今後も登場することを期待したい。

4. 講演2「多要素認証の1要素であるパスワードの安全な管理方法」

鈴木は、使い回しや管理者の管理範囲外からの漏えい等のリスクのあるパスワードをユーザが安全に管理する方法について、次のとおり発表した。

(1) パスワード漏えいへの対策

インターネット・バンキングにおける不正取引（MitB 攻撃等）が急増しており、金融機関は、振込先や金額等が改ざんされていないことを確認する「取引認証」の導入が求められている。他方、多くのユーザが 3 個以下のパスワードをさまざまなサービスで使い回しているとの調査結果があり、それを裏付けるように、インターネット・バンキングや EC サイト等においてパスワードを使い回していたユーザを対象とした不正ログインが多数発生している。そのため、サービス提供者は、自分の管理範囲外（他のサービス等）からのパスワード漏えいへの対策として、パスワード以外の本人認証要素（所持物、生体情報）を併用する「2 要素認証」を導入することが望ましい。

多くの金融機関は、ログインあるいは重要取引の少なくとも一方において 2 要素認証を実行しており、パスワードが漏えいしても不正取引を防止できると考えられる。しかし、①ログイン時に 2 要素認証を実行していない場合には、不正ログインにより口座残高や住所等の個人情報が閲覧されるリスクがあるほか、②取引完了を電子メール等で通知している場合には、漏えいしたパスワードで電子メールサービスに不正ログインされることで、そうした通知が本人に届かず、結果として不正取引の検知が遅れる可能性等も考えられる。このため、2 要素認証を導入している金融機関にとっても、ユーザによる適切なパスワード管理は重要な課題といえる。

本来、パスワード漏えいの影響を局所化するためには、パスワードの使い回しは避けるべきであるが、ユーザにとって利用する多数のサービスごとに異なるパスワードを記憶することは現実には難しい。そうした解決策として、複数サイトでの本人確認を 1 回で済ませる「シングルサインオン」が知られている。しかし、シングルサインオンの利用に当たっては、サービス提供者のシステム改修が必要となるため、直ぐに利用できるとは限らない。そこで、サービス提供者のシステム改修が不要な対策として、複数のサービスのパスワードをマスターパスワードを用いて一元管理する「パスワード管理ツール」が一部のユーザの間で利用されている。同ツールについては、多種多様な製品が存在し、使い勝手や性能面等から比較されているものの、同ツールに求められる安全性要件についての議論はあまりないのが実情である。

(2) 典型的なパスワード管理ツールに対する現実的な脅威と対策

典型的なパスワード管理ツールでは、各サービスの ID とパスワードを「データベース」化したうえでマスターパスワードで暗号化し、サーバまたはユーザ端末に保存している。しかし、最近の研究成果を踏まえると、マスターパスワードが短い

（8 文字程度）場合には、暗号化されたデータベースが漏えいすると、マスターパスワードの全数探索により解読される脅威が現実的になっている。

こうした脅威に耐性を持たせるには、まず、ランダムに生成した暗号鍵でデータベースを暗号化したうえでサーバに預け、同暗号鍵をユーザ端末で管理するという方法等がある。この際、暗号鍵をマスターパスワードで保護することで安全性をさらに高めることも可能である。また、暗号化されたデータベースをサーバから入手する際にサーバとユーザ端末が暗号通信を行うことになるが、現在主流の SSL 暗号通信[5] よりも情報漏えいに対して安全性の高い技術[6] が提案されている。これらの技術の組合せにより、サーバまたはユーザ端末のどちらか一方から情報が漏えいしてもデータベース等が安全であるほか、不正なサーバ管理者からもデータベースを保護できるパスワード管理ツールを実現できる。

(3) パスワード管理技術の活用

パスワード管理ツール以外にも、ユーザの各サービス用パスワード（データベース）を第三者が預かるサービスとして、個人の金融資産管理を支援する「口座情報集約サービス[7]」が金融機関や IT 企業等によって提供されている。一部のサービスでは、インターネット・バンキングへのログインが乱数表によって 2 要素認証化されている場合に、この乱数表の全マスの情報の入力を要求している。仮に、同サービスからこうした情報が漏えいした場合には、不正取引が発生しうることから、こうした運用には留意すべきである。

同サービス提供者が実施可能な対策としては、前述のパスワード管理ツールを参考に、ユーザのパスワードに関するデータベースを平文のまま預からない形態に移行する方法がある。また、インターネット・バンキング提供者が実施可能な対策としては、ログイン時と取引実行時に必要な認証情報を使い分ける方法がある[8]。このほか、同サービス提供者とインターネット・バンキング提供者が協調できるのであれば、「代理アクセス技術[9]」を利用する方法もある。

5 SSL（Secure Socket Layer）暗号通信は、インターネット・バンキング等で利用される標準的な暗号通信技術。

6 具体的には、暗号通信路を確立する際に、マスターパスワードのほかに、ユーザ端末に保存した乱数を併用する「Leakage-Resistant Authenticated Key Exchange」であり、2 要素認証に分類される。

7「アカウント・アグリゲーション・サービス」とも呼ばれる。同サービスにより、銀行口座やクレジットカード利用履歴、電子マネー残高等を一元的に管理することが可能。

8 例えば、ログイン時はパスワード認証を行い、取引時は 2 要素認証を行う方法や、ログイン時に 2 要素認証を行い、取引時は取引認証を行う方法がある。

9 第三者があるサービスに本人としてアクセスするために、第三者にパスワードではなくアクセスする権利（トークン）を提供する技術。OAuth 等が標準化されている。

(4) おわりに

2 要素認証を採用していないサービスや 2 要素認証の 1 要素としてパスワードを利用するサービス等が存在することから、当面はパスワードがなくなることはなく利用され続けると予想される。こうした状況下では、パスワード管理が引き続き重要であるが、適切な管理方法に関するコンセンサスが形成されていないのが実情である。ユーザによる適切な管理を進めるためにも、望ましい管理方法についてオープンに議論し、コンセンサスを醸成したうえで、ユーザに具体的な管理方法について情報提供していくことが求められる。

5. 講演 3「『暗号化状態処理技術』を巡る最新動向」

清藤 は、情報漏えい対策として研究が活発化している「データを暗号化したままデータ処理を行う技術（暗号化状態処理技術）」の最新動向について、次のとおり発表した。

(1) 単なる暗号化では防止困難な脅威の存在

近年、金融機関がクラウド等の外部サーバを利用するケースが増加している。通常、サーバに保存されるデータは、情報漏えい対策として暗号化されており、データ処理が必要な際は一時的に復号される。しかしながら、サーバのマルウエア感染や従業員の不正が少なからず発生していることを踏まえると、一時的に復号されたデータをマルウエアに盗取されたり、サーバ管理者等が復号鍵を不正に利用して暗号化データを復号するといった、単なる暗号化では防止困難な脅威が想定される。こうした脅威への対策として、データを暗号化したまま処理することでマルウエア等にデータを盗取させないというコンセプトの技術「暗号化状態処理技術」が活発に研究されており、既に製品として利用可能なものも登場している。

(2) 暗号化状態処理技術の概要

暗号化状態処理技術は、まだ発展途上にあり、任意の処理を暗号化したまま効率的に実行する方式は知られていない。暗号化したまま実行可能な処理として提案されているものとして、次の 3 つが代表的な技術である。

①秘匿検索

秘匿検索は、暗号化したままキーワード検索を行う技術である。具体的には、まず、ユーザは、検索対象のデータに対して登録用キーワードを設定し、同データと同キーワードをそれぞれ暗号化したうえでサーバに登録する。検索時には、ユーザが検索用キーワードを暗号化したうえでサーバに送信すると、サーバは各キーワードが暗号化された状態のまま検索を行い、その結果をユーザに返すという流れになる。例えば、暗号化された電子メールに対するキーワード検索といった用途や、サーバ上で生体情報を暗号化したまま一致／不一致を判定することで生体認証を行うといった用途（テンプレート保護技術）が実用化されている。学界では、完全一致や部分一致等のさまざまな検索条件を実現する方式が研究されている。

②秘匿暗号化

秘匿暗号化は、変換鍵を用いることで、あるユーザ宛の暗号文を別のユーザ宛の暗号文に変換する技術である[10]。対応する変換鍵があれば第三者（外部サーバ）であってもこうした変換処理が可能であり、その際に元のデータは第三者に漏えいしない。例えば、グループ内のファイル共有システムでの用途が実用化されている。具体的には、まず、グループ管理者は、メンバーと共有したいファイルを自分宛の暗号文として暗号化したうえで外部サーバに登録しておく。グループに新メンバーが加入した場合には、グループ管理者が同メンバー用の変換鍵を生成し、外部サーバに同鍵を預けておく。同メンバーがファイルの閲覧を外部サーバに要求すると、同サーバは変換鍵を用いて同メンバー用の暗号文に変換したうえで同メンバーに送信するという流れになる。学界では、変換処理の効率化や安全性強化等の観点から研究が行われている。

③秘匿計算

秘匿計算は、暗号化したまま数値計算を行う技術であり、計算結果も暗号化された状態で得られる。購買履歴や患者情報等のビッグデータの分析を、データを暗号化したまま外部サーバで行うといった用途が実用化されている。これまでの秘匿計算では、加算した後に乗算を行う（あるいはその逆）といった数値計算を実現できなかったが、近年、こうした計算を実現する方式が提案され、研究が大きく前進している。しかし、同方式は、暗号化しない通常の計算よりも大幅に処理速度が遅くなるため、学界では、処理の高速化の観点から重点的に研究が行われている。

10 学界では、秘匿暗号化を「代理人再暗号化」、変換鍵を「再暗号化鍵」とそれぞれ呼ぶ。

(3) 金融機関へのインプリケーション

前述の 3 つの暗号化状態処理技術を組み合わせて利用することも考えられる。例えば、暗号化された購買履歴のビッグデータに対して、秘匿検索により特定の条件に一致するものに絞り込んだうえで、秘匿計算により統計解析を行うといった応用もありうる。また、各技術は類似しており、「秘匿計算を実現する仕組みがあれば、それを用いて秘匿検索や秘匿暗号化を実現可能」であるという研究成果が示されている。このため、システム開発において、秘匿計算を実現するソフトウエアを用意すれば、残りの 2 つの処理を同ソフトウエアにより実現できるため、開発期間の短縮等につながると期待される。

学界で研究されている暗号化状態処理技術として、上記の代表的な 3 種類の技術に関して解説したが、同一技術に分類される個々の方式が実現する処理内容や安全性等は異なるほか、研究の活発化によりさまざまな方式が次々に提案されるという状況にある。金融機関が同技術を利用するに当たっては、自らのシステム要件を満たす実現方式を探すというアプローチだけでなく、同システム要件を学界に伝えることで自らが必要とする方式の研究開発を促すことも有益であろう。

6. 各講演に対する主な質疑応答

パスワード認証における ID について フロア参加者 から、攻撃者に ID を予測させ難くするために ID をランダム化する対策があるが、ユーザの利便性を損ねずにこうした対策を実現する方法はあるかとの質問が寄せられた。これに対して、鈴木 は、そうした方法は思い付かないと回答したうえで、同対策では ID を 2 つ目のパスワードとみなすことができるが、まずは、攻撃者が ID を入手していたとしてもパスワードを適切に管理することで不正ログインを防止する方法を議論するのが先決ではないかと述べた。そのうえで、パスワード生成について、まず「I am a student」等の英文を作成し、このうち何文字かを別の文字や記号等で置換したもの（例：1am@$tuDent）をパスワードとする生成方法もあると紹介した。また、パスワード認証における不正ログインについて フロア参加者 から、攻撃者はどのような戦略を採りうるのかとの質問が寄せられた。これに対して、鈴木 は、攻撃者がコストパフォーマンスを優先する場合には、漏えいしたパスワードやよく知られた脆弱なパスワード等を用いて、不特定多数の ID に対して機械的に不正ログインを試行するという戦略が考えられると述べた。さらに、攻撃者がコストを掛けてでも特

定ユーザとして不正ログインしたい場合には、いわゆる標的型攻撃のように、さまざまな方法により攻撃を仕掛けるという戦略が考えられると説明した。

秘匿検索や秘匿暗号化を実現する方法について フロア参加者 から、秘匿計算を実現するソフトウエアを利用して他の 2 種類を実現する方法の説明があったが、最初から秘匿検索や秘匿暗号化に特化して実装された各ソフトウエアの方が処理速度等の面で優れているのではないかとの質問が寄せられた。これに対して、清藤 は、ご指摘のとおりであると回答したうえで、効率性が落ちるのを我慢して幅広い方式を汎用的に構成したいのか、あるいは、方式は特定するが効率性を重視したいのか、システム開発時に何を重視するかによって実現方法の方針を選択すればよいと説明した。具体的には、商用システムであればデータサイズや処理速度等へのニーズがあり、各処理に特化した高速なソフトウエアが適しているが、他方、少ない投資でシステムのプロトタイプを短期間で構築したい等のニーズがあれば、秘匿計算を実現するソフトウエアを使い回すという実現方法も考えられると補足した。

7. パネル・ディスカッション「モバイル決済技術の現状と課題」

パネル・ディスカッションに先立つパネル発表では、まず、事業者であるペイパルの 松谷 から自社で展開するサービスの概要や契約関係等の概要について説明があった。続いて、パネル・ディスカッションにあたっての問題提起として、杉浦、廣川 から、モバイル決済に関する法的論点、リスク管理上の留意点についてそれぞれ発表が行われ、既に講演を行っている 新崎 を加え、自由討議が行われた。

(1) パネル発表 1「PayPal の概要」

松谷 は、スマートフォンを利用した決済サービスを提供する事業者としての立場から、同サービスに関する 2 つの事例について次のとおり説明した。

ペイパルは、ユーザ間でのオンライン資金送金サービスの提供を主な業務としており、その規模は、アクティブなユーザが約 1.4 億人、年間の取引金額と取引件数がそれぞれ約 18 兆円と約 30 億件である。近年では、スマートフォンを利用したクレジット決済サービスも提供している。

同サービスには主に 2 つの形態があり、1 つがいわゆる「スマホ決済」である。同形態では、スマホ決済サービスの加盟店はペイパルユーザとして登録したうえで支払人によるクレジットカードの支払いを受ける。その際、イヤホンジャックに

差し込むタイプの磁気カードリーダを普通のスマートフォンに装着してカード決済端末として用いるのが特徴である。加盟店にとっては、カード決済端末の導入コストを抑えられるほか、加盟店審査の基準が従来のクレジットカードよりも緩和されており、これまでクレジットカードを取り扱えなかった場合でも加盟店になりやすい等の利点がある。他方、支払人にとっては、加盟店が増えることからクレジットカードの利用場面が増えるという利点がある。

もう 1 つの形態は、「顔パス支払い」である。同形態では、加盟店に加え支払人もペイパルユーザであることが前提となっている。支払人は、予め自分のスマートフォンに専用ソフトウエアをインストールしたうえで、ペイパルにクレジットカード情報と顔写真を登録しておく。利用時には、支払人が専用ソフトウエアを通じて加盟店への来店を通知（「チェックイン」と呼ばれる）すると、同加盟店には支払人の顔写真が送信される。その後、同加盟店における支払時に、支払人が「顔パス支払い」を選択し、同加盟店のスタッフが顔写真を基に本人確認を行うことで支払が完了する。加盟店にとっては、支払処理に要する時間を短縮できるほか、支払人にとってもクレジットカードを取り出す必要がない等の利点がある。

(2)　パネル発表 2「契約関係や法制度の側面から考える」

杉浦 は、法律の専門家の立場から、情報システムやそこで扱う情報に関する 2 つの法的論点について説明した。

少なからぬ金融機関が情報システムの開発や運用を IT ベンダーに委託している。情報システムに関する専門知識を有する金融機関スタッフの減少とともに、金融サービスにおける IT ベンダーの役割が増大している。例えば、システム開発においては、昨年、IT ベンダーの責任（「プロジェクトマネジメント義務」と呼ばれる）を拡大解釈する方向の判決が示されている。金融機関にとって情報システムがブラックボックス化していくなかで、システム開発の失敗やシステムの欠陥等による損害が生じた場合に金融機関がどこまで責任を負うべきなのか、といった点について議論していく必要がある。

また、企業が収集したユーザの情報に関する論点もある。こうした情報を用いたビジネス等としては、例えば、ユーザの購入履歴に基づきクーポン券等の有益な情報をユーザに提供するもの（例：「Card Linked Offer」）、自社で収集したユーザの行動履歴を個人が特定されないように加工（「匿名化処理」と呼ばれる）したうえでマーケティング用途として別の企業に販売するもの、ユーザの生体情報を用いた本人確認（生体認証）等がある。こうした情報の所有権はユーザ自身と収集した企業のどちらに帰属するのか、保護すべき個人情報に該当するのか、といった点についても議論していく必要がある。

(3) パネル発表 3「モバイル環境への進展に伴うリテール取引システムの課題」

廣川 は、カードビジネスの専門家の立場から、モバイル端末を用いた取引におけるリスク管理上の留意点について説明した。

リテール取引は、窓口、店舗、ATM といった「物理的環境」で行う取引から、PC やモバイル端末等の汎用端末を用いたインターネット環境（「仮想環境」と呼ばれる）で行う取引に拡大してきた。また、その形態は、取引時にユーザから加盟店にカード番号等を提示する形態のほかに、予めカード番号や銀行口座等を ID に紐付けておき、取引時に本人が ID を利用していることを加盟店が確認するという形態も普及しつつある。これらの取引は取引時点におけるカード提示の有無によって「CP：Card-Present 取引」と「CNP：Card-Not-Present 取引」に大別される。

CP 取引については、さまざまな方法による不正取引に直面するなかで対策が高度化してきた。他方、CNP 取引については、利用の多様化に加え関係技術の発展が続いており、CP 取引に比べてリスク管理のノウハウ蓄積が少ないため、対策導入時に想定していた脅威と実際の脅威が乖離する可能性がある。その場合、不正取引のリスクが顕現化することがありうるため、そうした乖離の有無についても定期的に確認する必要がある。

また、CP 取引では、取引の安全性を強化するために、磁気カードから IC カードへの切替えが進められている。IC カードは、安全にデータを格納・処理するための演算処理機能を持った電子媒体（以下、「Secure Element」）の一種であり、その安全性を評価・認定する制度も整備されている。これに対し、CNP 取引で利用される汎用端末については、端末全体の安全性を評価・認定することが現実的には困難である。今後、CNP 取引の安全性をさらに強化するためには、汎用端末において Secure Element を活用してサービス提供者との間で取引に関与する媒体等の真正性確認や取引の正当性確認、幅広いリスク管理を行う必要が生じていくと考えられる。

(4) 自由討議

自由討議では、3 名のパネリストがモバイル決済の課題や生体認証のビジネス利用等について、フロア参加者からの質問も交えつつ議論を行った。なお、松谷 は、パネリストによる自由討論を円滑に進めるため、スマホ決済に関する補足やサービスを展開するに当たってのビジネス上の判断等について、事業者の立場から適宜解説を行った。概要は次のとおりである。

イ．パネリスト等による議論

（イ）スマホ決済について

まず、松谷は、モデレータからの質問に応じ、スマホ決済の利点について、ユーザに身近な汎用端末を利用することで個人や中小店舗が加盟店としてサービスに参加するハードルを下げられる点や、加盟店の業務システムと連携するための汎用端末向けアプリを開発しやすい点を挙げた。また、加盟店になるためのハードルを引き下げることで不正取引のリスクが高まる点について、10 年以上にわたる不正検知のノウハウの蓄積がペイパルのコア技術であり、同技術により適切なリスク管理が可能であると説明した。これを受けて、杉浦は、スマホ決済の加盟店になるための審査基準がスマホ決済の各サービス提供者によって異なることや、スマホ決済を悪用した多額の代金詐取が既に米国で発生していることを紹介した。そのうえで、ユーザにとっては、各サービス提供者の不正取引対策への取組みがわかり難く、優良なスマホ決済サービスを見極めるのが難しいという課題があると指摘した。

次に、ペイパルのスマホ決済において、クレジットカードの磁気ストライプ対応のカードリーダを利用している点について、松谷は、クレジットカードの偽造対策として、グローバルには IC クレジットカードの導入が進められている状況ではあるが、国内では、①IC クレジットカードの利用が必須にはなっていないこと、②磁気ストライプを使ったクレジットカード取引がまだまだ主流であること、③磁気カードリーダは IC カードリーダに比べ圧倒的に安価であること等を踏まえると、IC クレジットカード対応を積極的に進める意義は乏しく、現時点ではスマホ決済を普及させることを優先している結果であると説明した。さらに、IC カードが十分に普及している英国では、IC カードベースのスマホ決済サービスを提供していると補足した。

このほか、杉浦は、スマホ決済の普及のためにはユーザ保護の枠組みを整備することが必要であると述べた。また、そのためには、スマホ決済を支えるさまざまな要素（スマートフォン本体、スマホ決済用アプリ、カードリーダ、通信環境等）の異常により発生したユーザが意図しない取引について、同取引の有効性や同取引により発生した損失の責任の所在等の論点について十分議論する必要があると述べた。

（ロ）生体認証のビジネス利用について

生体認証を利用した決済サービスについて、新崎は、顔パス支払い以外にも指紋等を利用したものが存在すると紹介した。これを受けて、杉浦は、2020 年に開催される東京オリンピックに向けて、生体認証やキャッシュレス決済サービス等を普及させたいという機運が高まっていると補足した。そのうえで、生体認証が普及

するためには、システムに登録した生体情報の漏えいや二次利用等のリスクに関してユーザが感じる気持ち悪さをどうクリアするかが課題であると指摘した。これに対して、新崎は、こうしたリスクへの対策として、生体情報を暗号化したまま登録・照合する「テンプレート保護技術」が研究開発されており、同技術を利用するとともに、その効果についてユーザに啓蒙していくことが有用であると述べた。また、廣川は、生体認証をビジネスで利用する際の課題として、生体認証システムで一定の確率で生じる「他人受入」により、他人が行った不正取引が誤って成立する可能性があることを指摘した。そのうえで、こうした不正取引が発生した時の責任の所在や、生体認証を複数サービス間で相互利用する場合の他人受入の発生確率の設定等について関係者間で議論を重ねていく必要があると説明した。

このほか、生体認証に関する新しいサービスとして、新崎は、限られた範囲で使われるものであるがと前置きしたうえで、第三者機関が生体認証による本人確認を実施し、その結果を提供するという認証サービスも存在すると紹介した。これを受けて、杉浦は、生体認証に限らず、そうした認証サービスは米国政府等においても非常に注目されており、サービスを提供するセンターのセキュリティを担保し、認証結果の信頼性をどのように確保するかが大きな課題となっていると説明した。

また、生体認証を利用する目的について、新崎は、安全性向上のためだけでなく、利便性向上のために導入するサービスも登場していると指摘したうえで、キャッシュカードを用いずに手ぶらで現金を引き出せるようにした事例として、生年月日、暗証番号、生体認証のみで本人確認する ATM を改めて紹介した。さらに、新崎は、例えば、スタッフがユーザの本人確認を行う際に、効率化や確実性の向上のために、顔認証により候補となるユーザを絞り込んでおくといった用途のように、生体認証を利用して人間が判断を下す際に参考となる情報を提供するといった使い方も有望なのではないかと述べた。

ロ．フロアからの質問

フロア参加者から、リテール取引といっても小銭を使った小額取引から 100 万円程度の比較的高額な取引まであり、一律に扱うのは難しいと思うが、リテール決済サービスの対象としてどのように捉えているのか、との質問が寄せられた。これを受けて、松谷は、日常の買い物で利用されるせいぜい 1 万円強程度の金額帯をターゲットとしており、そのため一般の人が使えるよう身近な汎用端末を利用することを考えていると説明した。そのうえで、こうした端末は、専用端末と比較すると安全性で劣る面があるため、汎用端末を含めたシステム全体で取引の安全性を確保することが重要であると強調した。また、廣川は、クレジットカードは高額取引以外にも利用されるが、小額取引において本人確認を省略することで利便性を高め

た利用もあると紹介した。そのうえで、取引金額等に応じて不正取引のリスクが異なることから、リスクに応じたセキュリティ対策を導入し、適切なリスク管理を行うことが重要であると説明した。

8. 総括コメント

今井は、シンポジウムの内容を振り返ったうえで次のとおりコメントを行い、シンポジウムを締め括った。

今回のシンポジウムも前回に引き続き、ますます多様化するリテール取引とその安全性が取り上げられた。モバイルやクラウドを前提とした技術やサービスの進歩は目覚しく、1 回のシンポジウムですべてをカバーすることは難しい中で、クラウドからの情報漏えいへの対策技術、モバイル・バイオメトリクス、スマホ決済等、非常に興味深いトピックが取り上げられており良かったと思う。

この技術を導入すれば大丈夫だといった技術への過信は好ましくないが、他方で、有用な技術が研究開発されているにもかかわらず、ユーザ企業がそうした技術を十分に理解していないために利用していないケースもある。今回のシンポジウムの各講演は、研究者からみれば非常に分りやすく整理されていたが、難しいと感じる参加者もいたかもしれない。情報技術研究センターには、金融業界の課題を学界に伝えるとともに、学界の研究成果が金融業務にどのように活用できるのかといった点を金融業界に平易に伝えることで両業界をつなぐという役割を今後も期待したい。また、前回のシンポジウムでは、インターネット・バンキングに対する MitB 攻撃への対策が取り上げられたが、その後、各金融機関が同攻撃への対策を導入したり、対策に向けた準備を開始しており好ましい傾向だと思う。今後も、情報技術研究センターには、金融機関のニーズを捉えた適切なテーマを設定し、金融業界全体の安全性向上に努めていただきたい。

参考文献

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」、全銀協ニュース、2014 年