Vol.2016-CSEC-74 No.15
Vol.2016-SPT-19 No.15
2016/7/14

# 金融業界において注目されている情報セキュリティ上の研究課題：認証技術に焦点を当てて[†1]

中村啓佑[†2]　　宇根正志[†3]

**概要**：　本稿では，日本銀行主催の「情報セキュリティ・シンポジウム」におけるディスカッションやアンケート結果に基づき，金融機関の実務者が注目している情報セキュリティ上の脅威や，その対策としての認証技術にかかる研究課題について考察する．金融機関の実務者の多くが，インターネット・バンキングにおける不正取引を，最も深刻な問題と認識していることを説明するほか，今後の主な研究課題として，Display Overlay 攻撃等を考慮したスマートフォンによる取引認証の高度化，金融取引にかかるデータマイニングによる異常検知，認証技術のセキュリティにかかる評価手法の研究について説明する．

**キーワード**：インターネット・バンキング，マルウェア，FIDO，FinTech，フィッシング，生体認証，TEE，異常検知，取引認証，スマートフォン

# Research Topics on Information Security from Viewpoints of Financial Institutions: Focusing on Authentication Techniques

Keisuke NAKAMURA　　Masashi UNE

***Abstract***: This paper will discuss information security issues and research topics regarding authentication techniques from viewpoints of financial institutions by referring to discussion and a survey result at the Information Security Symposium held by the Bank of Japan. Namely, the survey result indicates that the majority of participants from financial institutions consider fraudulent transactions in Internet banking services as the most critical issue. As future research topics relating to the authentication techniques, we will also show the following three ones: (1) improvement of transaction authentication schemes secure against display overlay attacks for smartphones; (2) anomaly detection using data mining techniques in financial transactions; (3) development of security evaluation methods for authentication techniques.

***Keywords***: anomaly detection, biometric authentication, FIDO, FinTech, Internet banking, malware, phishing, smartphone, TEE, transaction authentication

## 1. はじめに

金融業界は，金融サービスを提供していくうえで様々なセキュリティ技術を活用し，その時々のセキュリティ情勢に応じた対策を行ってきた．例えば，2004 年頃から，偽造キャッシュカード問題が社会問題化したことを受けて，全国銀行協会は，IC カードや生体認証技術の導入，キャッシュカードの利用限度額の引下げ等の対策を表明し，各金融機関はそれに応じた対応を行ってきた[1].

最近では，インターネット・バンキングの普及に加えて，「FinTech」と呼ばれる新しい金融サービス（図 1 参照）が注目を集めており，スマートフォン等を利用してネットワーク経由で様々なサービスが提供されるようになってきている．一方，足許の情報セキュリティを巡る状況をみると，インターネット・バンキングにおける不正払戻しの金額（図 2 参照）が増加傾向を示している．海外では，マルウエア等による Man-in-the-Browser 攻撃 （以下，MitB 攻撃）に加え，DDoS 攻撃（Distributed Denial-of-Service）と組み合わせて不正送金を実行する事例[4]が報告されるなど，手口

○個人財務管理（PFM）
個人ユーザが、銀行口座、カード履歴等の収入・支出を一元管理するサービス

○オンライン融資
決済データ等を与信作業に活用し、EC事業者へスピーディに運転資金を貸与するサービス

○投資支援
投資ポートフォリオの自動生成・運用を行うサービス

○経営・業務支援
会計や給与計算等の企業活動を支援するサービス

○クラウドファンディング
インターネットを介して不特定多数から資金調達できるサービス

○スマホ・Web決済/送金
スマートフォン装着型（mPOS）等のクレジットカード決済サービスや、SNSアプリを介した送金サービス

○仮想通貨やブロックチェーン
ビットコイン等の仮想通貨や、ブロックチェーンを利用した金融機関同士の電子取引システムサービス

図 1　FinTech の主なサービス

†1 本稿に掲載されている内容や意見は，すべて個人に属し，その所属する組織の公式見解を示すものではない．

†2 日本銀行　金融研究所　情報技術研究センター
keisuke.nakamura@boj.or.jp
†3 日本銀行　金融研究所　情報技術研究センター
masashi.une@boj.or.jp

Vol.2016-CSEC-74 No.15
Vol.2016-SPT-19 No.15
2016/7/14

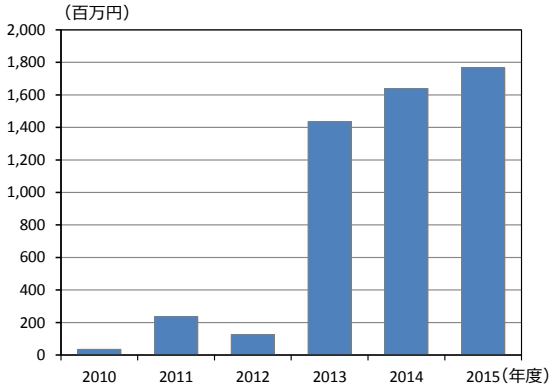


図 2 インターネット・バンキングにおける
不正払戻しの金額[2]（個人＋法人顧客）
（2015 年度の計数のうち 1~3 月分は速報値[3]）

**【第 17 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「金融取引を安心安全に実現するための認証技術：FinTech 時代も意識して」
  横浜国立大学大学院　教授　松本　勉
- 講演 1「次世代認証技術を金融機関等が導入する際の留意点：FIDO を中心に」
  日本銀行金融研究所　企画役補佐　井澤秀益
- 講演 2「生体認証システムのセキュリティ評価：人工物を用いた攻撃に焦点を当てて」
  日本銀行金融研究所　企画役　宇根正志
- 講演 3「暗号ハードウェア等に対するセキュリティ評価および留意点」
  日本銀行金融研究所　清藤武暢
- 講演 4「情報セキュリティのための異常検知技術」
  東京大学大学院　教授　山西健司
- パネル・ディスカッション「インターネット・バンキングのさらなる発展に向けて」
  モデレータ：横浜国立大学大学院　教授　松本　勉
  パネリスト：金融 ISAC 理事／FS-ISAC　Regional Director　鎌田敬介
  セコム株式会社 IS 研究所　マネージャー　松本　泰
  産業技術総合研究所　連携主幹　高木浩光

図 3　シンポジウムのプログラム
（敬称略，各参加者の所属や肩書きはシンポジウム開催時点のもの）

が一段と巧妙化している．また，スマートフォン用のアプリを対象とするマルウェアが報告されるようになってきている．こうした脅威に対応しつつ金融サービスを安全に提供していくうえで，情報セキュリティ技術にかかる最新の研究動向をフォローしながら，中長期的な観点から情報セキュリティ対策の高度化を検討していく必要がある．

こうした問題意識に基づき，日本銀行金融研究所情報技術研究センター（CITECS）では，金融分野において中長期的に重要となる情報セキュリティ上の課題や対応策について研究し，金融機関による課題への対処を支援してきた．また，学界での研究が金融業界のニーズをより反映したものとなることを企図して，情報セキュリティにかかる金融機関の課題やニーズを学会で発表してきた[5].

本稿では，まず，「第 17 回情報セキュリティ・シンポジウム」（開催日：本年 3 月 2 日，場所：日本銀行本店）の参加者を対象としたアンケート結果を基に，金融機関の実務者が注目している情報セキュリティ上の課題について説明する．そのうえで，同シンポジウムの講演やパネル・ディスカッションの内容を紹介しつつ，金融分野における情報セキュリティ技術への研究ニーズについて考察する．

なお，研究ニーズの考察は，具体的な技術研究にかかるニーズの導出を企図して，インターネット・バンキングにおける不正取引対策を前提に行っているが，導出した研究ニーズは，「FinTech」と呼ばれるものも含む，ネットワークを介して実現される金融サービスにおいても重要な研究課題といえる．

## 2. 金融機関の実務者からのアンケート結果

### 2.1 情報セキュリティ・シンポジウムの概要

第 17 回情報セキュリティ・シンポジウム（以下，シンポジウムという）では，「金融取引を安心安全に実現するための認証技術 : FinTech 時代も意識して」をテーマとして，認証技術に焦点を当てた（図 3 参照）．これは，FinTech やインターネット・バンキングなどのサービスにおいて，取引の相手やその内容を確認するために「認証」が不可欠であるためである．4 件の講演では，今後金融分野での活用が考えられる FIDO（Fast IDentity Online），生体認証，TEE（Trusted Execution Environment），データマイニングによる異常検知技術を取り上げた．パネル・ディスカッションでは，「インターネット・バンキングのさらなる発展に向けて」と題して，認証におけるセキュリティ（安全性）・利便性・網羅性のバランスやレガシー対応等に関して議論した[6].

### 2.2 シンポジウムにおけるアンケート

シンポジウム当日は，参加者（160 名）を対象にアンケート（無記名，所属組織の業態のみを選択）を実施し，金融機関の実務者から 28 件の回答を得た（全体では 114 件）．

アンケートの質問は，主に，足許の情報セキュリティ上の課題[7]を問うもの（質問イ）と，金融サービスを提供するシステムにおいて先行き攻撃対象となりうる部分を問うもの（質問ロ）である．各質問は以下のとおり．

- 質問イ： 2015 年に起こった各種ニュースにおいて貴社においても同様の課題があると思われる項目や貴社にも影響が大きいと思われる項目はどれですか？選択肢から選んでください（複数回答可）
- 質問ロ：今後，貴社においても脅威となり得ると考えられる項目にどのようなものがありますか？選択肢から選んでください（複数回答可）

金融機関の実務者の回答を集計したところ（表 1 参照），情報セキュリティ上の課題や脅威に関して，①インターネット・バンキングにおける不正取引や同システムへの攻撃，②サービス利用者の端末への攻撃，③金融機関内部システムからの情報流出の回答率が相対的に高かった．

| イ. 2015年ニュースで同様の課題があると思われるものは？（数字は、各業態内における回答割合） | | 金融機関 N=28 | ベンダー N=46 | 大学・研究機関等N=13 | その他 N=27 | 全体 N=114 |
|---|---|---|---|---|---|---|
| イ-1 | 年金機構の情報流出事件 | 43% | 35% | 38% | 30% | 36% |
| イ-2 | サイバーセキュリティ基本法全面施行 | 14% | 22% | 31% | 22% | 21% |
| イ-3 | 米中サイバーセキュリティ合意によるサイバー戦回避 | 4% | 9% | 0% | 11% | 7% |
| イ-4 | 解消されないセキュリティ人材不足 | 36% | 28% | 38% | 26% | 31% |
| イ-5 | 国がCSIRTの実効ある体制強化を勧告 | 29% | 20% | 31% | 22% | 24% |
| イ-6 | 9.5億台のスマホに影響を与える脆弱性が発覚 | 18% | 13% | 8% | 19% | 15% |
| イ-7 | FlashPlayerに対する脆弱性攻撃の増加 | 0% | 7% | 8% | 4% | 4% |
| イ-8 | 標的型サイバー攻撃相談件数6倍に | 25% | 20% | 23% | 22% | 22% |
| イ-9 | マイナンバー制度施行、通知カードの送付開始 | 39% | 52% | 38% | 30% | 42% |
| イ-10 | インターネット・バンキングの不正送金被害 | 71% | 33% | 31% | 41% | 44% |
| ロ. 今後脅威となり得ると考えられるものは？（数字は、各業態内における回答割合） | | 金融機関 N=28 | ベンダー N=46 | 大学・研究機関等N=13 | その他 N=27 | 全体 N=114 |
| ロ-1 | 顧客端末（PC、スマホ）への攻撃 | 54% | 37% | 23% | 56% | 44% |
| ロ-2 | POS端末やATMへの攻撃 | 14% | 26% | 31% | 26% | 24% |
| ロ-3 | 対外接続系システム（WEBサーバ、インターネット・バンキング）への攻撃 | 61% | 46% | 46% | 19% | 43% |
| ロ-4 | 勘定系システムへの攻撃 | 21% | 9% | 8% | 0% | 10% |
| ロ-5 | 情報系システム（電子メール、ERP）への攻撃 | 29% | 20% | 15% | 22% | 22% |
| ロ-6 | 社員の端末（行員のPCやタブレット）への攻撃 | 29% | 35% | 46% | 52% | 39% |
| ロ-7 | クラウド上のシステムへの攻撃 | 29% | 35% | 15% | 22% | 28% |
| ロ-8 | 設備制御系システム（空調、監視カメラ、IoT等）への攻撃 | 11% | 22% | 23% | 30% | 21% |

表 1　情報セキュリティ・シンポジウムにおけるアンケートの結果

### (1) インターネット・バンキングの不正取引等

質問イの回答では，「インターネット・バンキングの不正送金被害急増（イ-10）」が最も高い回答率（71%）であったほか，質問ロの回答では，「対外接続系システム（WEBサーバ，インターネット・バンキング）への攻撃（ロ-3）」の回答率（61%）が最も高かった．

なお，前回シンポジウムで実施した同様のアンケート[5]においても，情報セキュリティ上の課題や脅威として，「インターネット・バンキングの不正送金被害急増」（回答率50%）と「本邦金融機関に対応したバンキング・マルウェアの高度化」（同 73%）が相対的に高い回答率となっており，これらが引き続き重要な課題として認識されているといえる．

### (2) 金融サービスの利用者の端末への攻撃

質問ロの回答をみると，「顧客端末（PC，スマホ）への攻撃（ロ-1）」が，「対外接続系システム（WEB サーバ，インターネット・バンキング）への攻撃（ロ-3）」に次いで高い回答率（54%）となった．金融機関側のシステムだけでなく，サービス利用者の端末のセキュリティも重視する金融機関の実務者が相対的に多いことを示唆している．

### (3) 金融機関内部システムからの情報流出の脅威

質問イの回答をみると，「年金機構の情報流出事件（イ-1）」の回答率（43%）が「インターネット・バンキング」（イ-10）に次いで高い．前回のシンポジウムでのアンケートにおいても，情報流出事故（ベネッセの個人情報漏えい事件）にかかる回答率（50%）が相対的に高く，組織内部からの情報流出への対策が引き続き重要な課題として認識されているといえる．

## 3. シンポジウムの議論とインプリケーション

### 3.1 金融機関の実務者の問題意識と認証技術

上記 2.のとおり，金融機関の実務者は，インターネット・バンキングの不正取引対策に強い関心を有している．実際に，こうした不正取引を検知・排除する方法として，サービス提供者が金融取引の正当性（取引内容がサービス利用者の意思に基づくものであること）を確認するための「取引認証」を採用する動きが主流となっている．

取引認証として利用されている主な方法は，「取引の申請を行うチャネル（例えば PC）とは別のチャネル（例えばスマートフォン）を通じて，当該申請内容をサービス利用

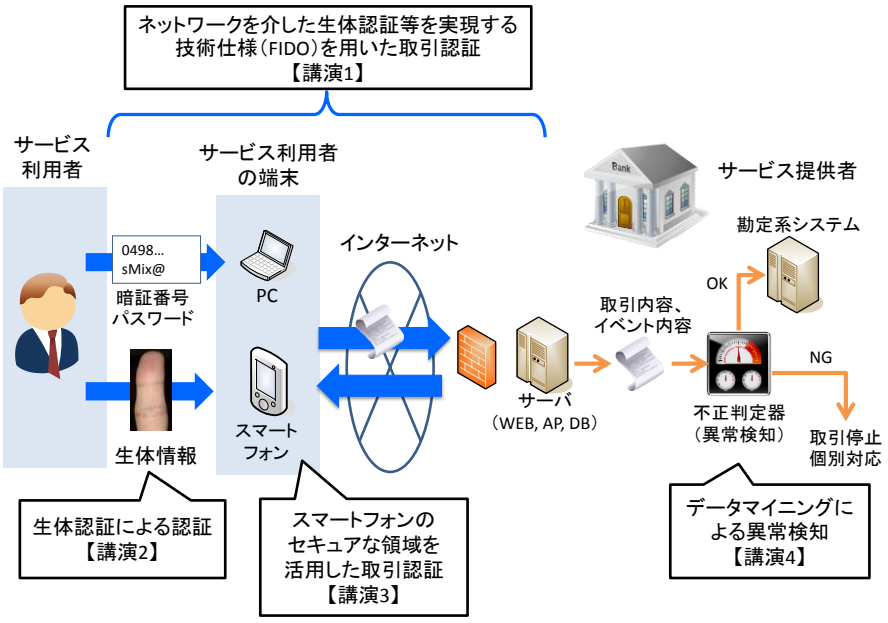


図 4　将来のインターネット・バンキングにおける各種技術の活用と講演の位置づけ（概念図）

者に通知し，サービス利用者がそれを確認してその旨をサービス提供者に返信する」というものである．

もっとも，サービス利用者は複数のチャネルや機器を準備する必要があり，利便性や網羅性が低下する．その結果，こうした対策が期待したほど普及せず，セキュリティが向上しないという状況に至る可能性が懸念される．

こうした点を踏まえ，シンポジウムでは，将来のインターネット・バンキングにおいて，セキュリティ・利便性・網羅性の向上に資する認証技術等について議論した（各講演で取り上げた技術の位置付けは図 4 を参照）．

### 3.2　4 つの講演

#### (1)　FIDO をインターネット・バンキングで活用する際のポイントと留意点

FIDO は，サービスの利用者と提供者の間で，ネットワーク越しの認証に生体認証等を利用するための手順を定めた技術仕様である．既に一部のスマートフォンで FIDO を活用したサービスが利用可能であり，2015 年 9 月，Bank of America が FIDO を利用したインターネット・バンキングのサービス提供を開始している．FIDO では，①生体認証の利用によって ID／パスワードを覚えておく煩わしさや忘失のリスクが低下する，②「Transaction Confirmation」と呼ばれる機能によって 1 つの端末で取引認証を実現可能であるなどのメリットが期待されている．

講演 1 では，インターネット・バンキングに FIDO を適用するモデルを想定し，セキュリティの観点からの留意点が説明された[8]．具体的には，①FIDO の初期設定を行う際に，レガシー認証情報（サービス利用のために当初から使用していた ID／パスワード等）を攻撃者に盗取されないようにする，②取引認証時に不正な取引の内容を表示させるタイプのマルウェアに留意する（Display Overlay 攻撃への対応），③生体認証時のなりすましに留意する，の 3 点である．これらをどう実現していくかが今後の課題といえる．

#### (2)　生体認証システムのセキュリティ評価

講演 1 で留意点として挙げられた「生体認証のなりすましへの対応」に関して，講演 2 において，生体認証システムのセキュリティ評価手法の検討状況が説明された[9]．生体認証システムへのなりすましを企図した攻撃として，「攻撃者が自分の生体特徴を提示するタイプ」と，「なりすまし対象の個人の生体特徴を何らかの手段で入手し，人工物を用いて提示するタイプ（人工物を用いた攻撃）」が知られている．前者については評価手法が確立している一方，後者については標準的な評価手法が確立途上にある．

講演 2 では，人工物を用いた攻撃に対するセキュリティの評価尺度，評価用の試験環境等にかかる研究が活発化しているほか，国際標準化も同時に審議されている旨が説明された．標準的な評価手法が確立すれば，金融機関は，生体認証システムのセキュリティ評価に，そうした手法を活用可能となる．今後は，そうした評価をどう実施するか，また，評価結果をどう活用するかが課題といえる．

#### (3)　TEE の活用とその課題

TEE（Trusted Execution Environment）は，スマートフォン等の内部に安全な実行環境を実現するための技術仕様であり，生体認証のための情報等を内部に安全に格納する機能や，重要な情報を画面に表示する際に当該情報を外部から改ざんされない安全なチャネルを実現する機能（TUI: Trusted User Interface）等を有する．例えば，FIDO において安全な取引認証を実現するうえで今後 TEE を活用して

いくことも考えらえる．

講演 3 では，インターネット・バンキングに TEE を活用し，1 つのスマートフォンで取引認証を行う際のセキュリティ上の留意点が説明された[10]．主な留意点は，①TEE のセキュリティ要件を適切に設定すること，②実際の TEE 製品において同要件が満たされているか否かを確認すること，の 2 点である．また，複数の TEE 製品がコモン・クライテリアに則った評価･認証プロセスの途上にあり,今後，国際標準に基づく評価・認証を取得した製品が利用可能になるとの見通しが示された．評価・認証済みの TEE 製品をどう活用するかが課題といえる．

**(4) 情報セキュリティのための異常検知技術**

講演 4 では，データマイニングによって異常を検知する各種手法，情報セキュリティ対策に資する研究事例や留意点が説明された[11]．金融分野では，システムへの不正侵入の検知，ネットワーク障害と予兆検知，インターネット・バンキングにおける不正取引検知等への応用が想定されるとの説明があった．こうした手法が利用できれば，サービス利用者の対応によらず，サービス提供者が不正取引を検知できるようになることが期待される．

今後の研究にかかる留意点としては，①特定の事象を「異常」と判定するために正常な取引やデータを学習する必要がある，②モデルの精度を高めて誤検知の確率を一定水準以下に抑える必要がある，③生のデータを研究に活用することが求められるなどが説明された．

### 3.3 パネル・ディスカッション

パネル・ディスカッションでは，今後のインターネット・バンキングにおける認証技術の活用について検討するうえで，セキュリティ・利便性・網羅性のバランスをどう考えるべきかといった観点から議論が行われた．今後の研究課題や留意点として，次のような見方が示された．

**(1) リスクの軽重に応じた認証技術の選択**

まず，「提供するサービスのリスクに応じて認証技術を使い分けることが望ましい」との見方が示され，「リスク評価や，利便性等を勘案した適切な認証技術の選択をどう行うか」が課題とされた．例えば，送金と住所変更等の重要な操作を行う際には，セキュリティを重視して取引認証を必須とする一方，残高照会等，上記以外の操作を行う際には，利便性を重視した簡便な手法（サービス利用者の端末内に安全に格納されたトークンをサービス提供者側が確認するなど）を採用するといった方法が紹介された．

また，①認証技術の評価手法の確立・国際標準化，そして，それらの活用という流れを，どのように促進していくか，また，②FIDO や TEE 等の製品を実装する際のリスクの評価をどう実施するかが重要な課題として示された．

**(2) スマートフォンの普及を前提とした認証技術の活用**

スマートフォンの普及が拡大しており，将来的には，インターネット・バンキングの個人の利用者はスマートフォンでのアクセスが主流になるとみられる反面，法人については引き続き PC からのアクセスが大半となるとの見方が示された．そのうえで,「セキュリティや利便性を高めるためにスマートフォンの機能をどう活用すべきか」が課題とされた．また，新しい認証技術等の導入の際に，従来のレガシー技術からどう移行していくかについて金融業界全体として検討すべきとの意見も出された．

**(3) TEE 内部のアプリの正当性の確認・保証**

TEE のセキュリティにかかる論点として，「TEE 内部で稼働するアプリが更新されるケースが想定されるが，その際，不正なものに更新されてしまうリスクを考慮すべき」との意見が出された．また，「TEE 内部で稼働するアプリの正当性を何らかの形で確認し保証するための仕組みを別途準備する必要がる」との発言もあり，TEE 内部のアプリの正当性をどう確認・保証するかが課題とされた．

**(4) 金融サービスの安定した提供**

セキュリティ向上を企図した新技術を導入する際には，「システムの安定稼働をどう確保するかも重要な論点である」との意見が出された．金融機関にとって，サービスを安定的に提供できなくなるリスクは重要な課題であり，新技術の導入を検討するうえで，同技術がシステムの稼働に与える影響をどう見極めるかが課題とされた．

## 4. 今後の研究にかかるニーズ

上記 2，3 を踏まえ，インターネット・バンキングの不正取引対策に資する認証技術の研究ニーズを考察する．研究ニーズは，各要素技術の有効性向上に資するものと，各技術の適切な評価･利用に資するものの 2 種類に分けられる．

### 4.1 各要素技術の有効性向上に資する研究

**(1) スマートフォンでの取引認証の実現方法**

まず，スマートフォンを前提とした取引認証にかかる実現方法（FIDO 等）にかかる研究が挙げられる（上記 3.3(2)(3)に対応）．FIDO を実装する製品・サービスが今後利用可能になると期待されるが，その際,「取引認証時に不正な取引の内容を表示させるタイプの攻撃（Display Overlay 攻撃等）」に対抗する手法の研究開発が望まれる．こうした手法の一つとして TEE の TUI が挙げられることから，TUI の実現方法の検討も重要な研究であるといえる．

このほか，FIDO 以外による取引認証の方法に関しても，セキュリティ・効率性・網羅性の向上に資するものの研究開発の活発化が望まれる（上記 3.3(2)に対応）．例えば，取引認証時に，取引内容のデータを端末から取得し表示する「電子ペーパー」を活用する方法[12]が提案されている．

こうした方法やその評価にかかる研究の進展も期待される．

### (2) データマイニングによる異常検知技術

インターネット・バンキングをはじめとするネットワーク経由での金融取引への適用を前提に，実用上求められる認証精度を評価することに加えて，それを満足する異常検知の方法の開発が望まれる（上記 3.2(4)に対応）．こうした研究を進めるうえで，正常な金融取引にかかるデータを識別・収集し学習する必要があり，金融機関と研究者の間でデータの提供や管理をどのように安全に行うかについて検討する必要がある．

なお，インターネット・バンキング等にかかる脅威が今後も変化していくことを踏まえると，そうした変化に応じて新しいデータを継続して収集し学習する必要がある．研究用のデータの提供・管理をどう継続して行うかも併せて検討することが求められる．

## 4.2 各技術の適切な評価・利用に資する研究

### (1) 認証技術の有効性にかかる評価

上記 3.3(1)で示されたように，提供するサービスのリスクに応じて認証技術をどう使い分けるかが重要な課題といえる．そのためには，各種サービスにかかるリスクの評価を実施することに加え，各種認証技術がセキュリティ上どの程度有効かを評価することが求められる．

こうした点を踏まえると，①現在検討が進められている生体認証システムのセキュリティ評価手法を今後どう活用していくか（上記 3.2(2)に対応），②TEE 内部で稼働させるアプリの正当性をどう保証するか（上記 3.2(3)に対応）にかかる研究の進展が望まれる．また，③スマートフォンを用いて取引認証を実現する各種プロトコル（FIDO を含む）が提案されているなかで，それらを横並びで評価する手法の確立に向けた研究（上記 3.2(1)，3.3(2)に対応）も重要であるといえる．

### (2) 安定稼働への影響にかかる評価

上記 3.3(4)で示したように，新しいセキュリティ対策を導入すると，当該サービスの安定稼働に影響を及ぼす可能性が考えられる．こうした点を踏まえ，新技術を提案する際には，当該技術が既存のサービスの安定稼働にどう影響するかに関しても評価しておくことが望ましい．

## 参考文献

[1] 全国銀行協会，“「偽造キャッシュカード対策に関する申し合わせ」について”，全国銀行協会，2005 年
[2] 全国銀行協会，“「インターネット・バンキングによる預金等の不正払戻し」等に関するアンケート結果”，全国銀行協会，2016 年 2 月
[3] 全国銀行協会，“インターネット・バンキングによる預金等の不正払戻し件数・金額について（平成 28 年 3 月発生分：速報値）”，全国銀行協会，2016 年 4 月
[4] Kuhn, John，“The Dyre Wolf Campaign: Stealing Millions and Hungry for More,”2015
[5] 井澤秀益，“金融業界において注目されている情報セキュリティ上の研究課題について”，コンピュータセキュリティシンポジウム 2015 予稿集，情報処理学会，2015 年 10 月
[6] 日本銀行金融研究所，“情報セキュリティ・シンポジウム（第 17 回）「金融取引を安心安全に実現するための認証技術：FinTech 時代も意識して」の模様”，IMES DISCUSSION PAPER SERIES，2016-J-6，日本銀行金融研究所，2016 年 5 月
[7] 日本ネットワークセキュリティ協会（JNSA），“JNSA 2015 年セキュリティ十大ニュース”，JNSA，2015 年
[8] 井澤秀益・五味秀仁，“次世代認証技術を金融機関が導入する際の留意点―FIDO を中心に―”，IMES DISCUSSION PAPER SERIES， No. 2016-J-3，日本銀行金融研究所，2016 年 2 月
[9] 宇根正志，“生体認証システムにおける人工物を用いた攻撃に対するセキュリティ評価手法の確立に向けて”，IMES DISCUSSION PAPER SERIES，No. 2016-J-2，日本銀行金融研究所，2016 年 2 月
[10] 清藤武暢，“暗号ハードウェア等に対するセキュリティ評価および留意点”，第 17 回情報セキュリティ・シンポジウム発表資料，2016 年 3 月
[11] 山西健司，“情報セキュリティのための異常検知技術”，第 17 回情報セキュリティ・シンポジウム発表資料，2016 年 3 月
[12] 高木浩光・渡辺創，“Man-in-the-Browser の脅威と根本的な解決策”，第 2 回セキュアシステムシンポジウム発表資料，2014 年 3 月