研究指導　中澤 真 准教授

インターネットバンキングの認証サービスのあり方 —なりすまし防止と利便性のバランスを考慮して—

遠藤　綾乃

1.　はじめに

フィンテックの浸透により金融サービスの姿が大きく変わりつつある．中でも，オンライン上の決済を可能にするサービスは，インターネット・スマートフォンの普及で多くの場面で目にするようになった[1][2]．しかし，このオンライン決済のメリットである，いつでもどこからでも決済が可能になるという利便性は，いつでもどこからでも不正アクセスによるネット上の様々な脅威にさらされるという諸刃の剣にもなる．こういった脅威から顧客を守るためにセキュリティ強化の取り組みが進められているが，不正取引は増加を続けるばかりである[3][4]．

そこで本研究では，インターネットバンキングの認証に焦点をあて，各銀行が導入している認証技術とその運用方法について調査する．さらに，銀行の業態別および規模別にセキュリティ対策の傾向について比較・検証をして，これからのインターネットバンキングの認証サービスのあり方について考察する．

2.　オンライン決済サービスの現状と課題

2.1　各種オンライン決済サービスにおけるなりすまし防止対策

オンライン決済のなりすまし防止におけるセキュリティ対策の基本は，通信の暗号化，正規サイトであることの電子証明，認証の三種類である[5]．特に認証は利用者に直接かかわる部分であるため，その安全性と利便性のバランスをとるのが最も難しい部分である．このため，サービス内容によって要件も異なり，その特性に応じたセキュリティ対策が求められる．そこで三つのケースに分けて，セキュリティ方針の違いについて説明する．

まず一つは「ネットショッピング」である．老若男女問わず多くの人に利用され，少額決済もかなり多いため，安全性よりも利便性が優先されたセキュリティ対策が行われている．二つ目は「インターネットバンキング」である．これはネットショッピングの決済とは異なり，高額な取引金額の利用場面が多いため，より厳重なセキュリティ対策がとられることが多い．特に認証時のセキュリティが強化されており，ログインIDとパスワードに追加して「第二認証」という形で二段階認証[1]を必要としているサービスも多い．また，ウイルス対策ソフトを無料で提供することで，感染によるパスワード流出などを防ぐための安全対策にも努めている．三つ目は「ネット証券」である．証券会社と株式の売買代金の精算や配当金の受け取りなどの決済が発生する．金銭の移動が利用者と証券会社間に限定されるため，第三者に送金されてしまうような被害が生じにくいことからインターネットバンキングほどの厳重なセキュリティ対策はとられていない．

これらの例を比較すると，オンライン決済の場面においてインターネットバンキングが最も安全性の高いセキュリティ対策を求められていることがわかる．

2.2　インターネットバンキングで考えられるリスク

これだけセキュリティ対策を厳重にしているのにもかかわらず，近年インターネットバンキングによる不正取引は増加傾向にある[3][4]．図1を見ると2011 年から2015 年にかけて被害額が 10 倍に跳ね上がっていることからその深刻さが伺える．発生原因のほとんどはフィッシング(Phishing)によるパスワードの流出である．悪意のある第三者が銀行になりすまして偽のインターネットバンキングサイトに誘導し，ID とパスワードを入力させるように仕向ける．入力された情報は，そのまま悪意のある第三者の手に渡り，他人の銀行口座を自由に操作されてしまうことになる．

このような不正送金被害の増加は利用者の不安を招いている．よりよい銀行づくりのためのアンケートの調査結果[6][7]によると，インターネットバンキングの利用をしている，またはしたいと考えている人の割合は，2012年度が64.7％であったのに対し，2015年度では55.8％と減少している．また，インターネットバンキングを利用しない理由の第二位に「セキュリティ面に不安を感じるから」が挙げられており，不安の増大を裏付ける結果となっている．

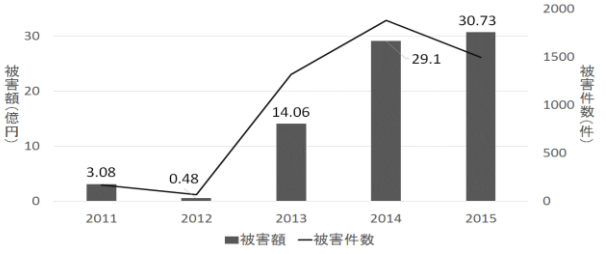

図 1:インターネットバンキングによる不正取引の被害件数と被害額(2011-2015)[3][4]

2.3　不正取引防止のためのセキュリティ対策事例

こういった不正取引の増加や，利用者の不安を払拭するために，インターネットバンキングでは他のサービスよりも積極的にセキュリティ強化の取り組みが進められてきた．

その一つが，一般的に利用されるパスワードに加えて「ワンタイムパスワード」を入力させて本人確認を厳格化する手法である[8]．これは，一度しか使用できない使い捨てのパスワードを都度発行することにより，万が一パスワードが流出しても乗っ取られてしまう可能性を低下させている．ログイン時にワンタイムパスワードを生成

[1] 異なる認証方法で2回本人確認を行うこと．

して銀行のシステム側と利用者側が情報を共有するための手段は，機械生成と紙媒体生成の二つに大きく分けられる．どちらもパスワードに相当する乱数を生成し，この情報を利用者に伝えてシステム画面上に入力させ認証をする．機械生成の場合は三つの方法がある[8]．一つ目はハードウェアトークンと呼ばれる小型で持ち運び可能な装置で生成した乱数を画面に表示させることで利用者に伝える方法である．以前はキーホルダーサイズのものがほとんどだったが，薄型化が進み財布に入るカード型のものが主流になりつつある．二つ目は利用者があらかじめ登録しておいたメールアドレスに乱数を通知する方法である．認証が必要な状態になると，本人宛にパスワードのメールが届くシステムである．三つ目は専用のスマホアプリを用いる方法で，アプリ上に乱数を表示させて利用者に通知する．これらの機械生成に対して紙媒体生成は，あらかじめ利用者に乱数表を配布し，認証時に特定の場所を指定することにより乱数を利用者に伝える方法である．機械生成と比較すると，生成される乱数の組み合わせがかなり限定されるため安全性はやや低くなる．これらすべてを用意して顧客に選ばせる銀行もあれば，指定したものを利用させる銀行もある．

ワンタイムパスワード以外のセキュリティ強化対策としては，「ウイルス対策ソフトの無償配布」と「リスクベース認証[9]」がある．ウイルス対策ソフトは，フィッシングを防止するために真正なウェブサイトであるかどうかの判別をしたり，利用端末への不正アクセスを遮断してパスワードの流出を防いだりする機能が備わっている．リスクベース認証は，利用者のアクセス・ログイン履歴を把握し，普段と異なるIPアドレスや端末からのログインだった場合に追加認証を求めるシステムである．「昔飼っていたペットの名前は？」や「母親の旧姓は？」といった利用者本人しか知りえないようなプライベートな情報を事前に登録し，追加認証時にこれに答えさせることにより，本人確認を厳格化するのである．

そのほかに通信の暗号化を強化することによるセキュリティ対策もある．オンライン上で決済するということは，サーバーと利用者で個人情報のやり取りがネット上で行われることになる．このやりとりを悪意のある第三者に盗聴・改ざんされたりすることを防ぐには暗号化通信が欠かせない．暗号の安全性は一般的に暗号化の際に使用する暗号鍵の長さに比例する．現在は128bitと256bitのいずれかの長さの鍵が，インターネットの暗号化通信に使われている．当然のことながら，256bitの鍵を使用するほうが安全性は高い．

上記で述べたように多種多様なセキュリティ対策が取り入れられているが，不正送金の被害額・被害件数が一向に減少しないのは，銀行のセキュリティ対策の運用に問題があると考えた．そこで本研究では，インターネットバンキングの認証に焦点をあて，各銀行が導入している認証技術とその運用方法について調査する．

3. インターネットバンキングにおけるセキュリティ対策の調査

3.1 調査方法

今回の調査では，全国の都市銀行，地方銀行，第二地方銀行合計109行を対象とする．まず初めに，採用しているセキュリティ対策について表1の項目に基づいて，各銀行のウェブサイトから情報収集を行う．そこで集めた情報から，銀行によって偏りがある項目を抽出・細分化し，導入技術や運用状況について銀行へ電話ヒアリングを行う．

調査項目の一つ「ワンタイムパスワードの強制度」は，インターネットバンキングを利用する際には取引内容にかかわらずワンタイムパスワードが必要というものを「強制」，振込み，個人情報の変更，スマートフォンからの利用時のみなど，特定の条件でのみワンタイムパスワードが必要になる場合を「一部取引で強制」，完全に利用者の判断に任せる場合を「任意」の三つに分類する調査である．強制すれば安全性は高まるが，利用者の手間が増え，利便性が下がる．逆に任意にすれば利用者の手間は増えないが，安全性がどれだけ確保されるかは利用者任せになるということを意味する．この強制度を調査することで，各銀行がインターネットバンキングの安全性と利便性のバランスをどのくらい考慮しているかわかる．

表 1:調査項目

ウイルス対策ソフトの配布	実施		
	未実施		
暗号化方式	256bit		
	128bit		
ワンタイムパスワード	導入している	技術	乱数表
			機械生成
		強制度	強制
			一部取引で強制
			任意
		入力のタイミング	ログイン時
			取引時
	導入していない		
リスクベース認証	実施		
	未実施		

3.2 調査結果の概要

以上の項目を調査した結果を表 2～表 4 に示す．ここで表 2 の項目，表 OPT[2]導入行数は，機械生成，乱数表にかかわらず何らかのワンタイムパスワードを実施している銀行をカウントしたものである．次節では，この調査結果について銀行の業態別，地域別，規模別に分けて詳細に分析する．

表 2:調査結果(各セキュリティ対策の導入・実施行数)

各セキュリティ対策	実施・導入行数	未実施・未導入行数
ウイルス対策ソフトの配布	101	8
ワンタイムパスワード(OTP導入)	102	7
ワンタイムパスワード(機械生成導入)	76	33
リスクベース認証	66	43

表 3:調査結果(暗号化方式)

暗号化方式(鍵長)	128bit	256bit	不明
実施行数	93	4	12

表 4:調査結果(ワンタイムパスワード強制度比率)

強制種別	強制	一部取引で強制	任意	合計
実施行数	6	36	34	76

4. 分析結果と考察

4.1 ウイルス対策ソフト配布実施率

ウイルス対策ソフトの配布について，現在109行中101

[2] One Time Password の略称.

行が実施していることがわかった．また，配布を行っている銀行すべてが無償で配布をしていることもわかった．銀行の業態別に比較すると，都市銀行，地方銀行，第二地方銀行の順に実施率が高いことがわかる(図2)．つぎに銀行の本店が立地している地域別に比較すると，四国・九州地方での実施率が100％となっており，高いことがわかる(図3)．

銀行の業態別に差が出たことから，ウイルス対策ソフトの配布の実施には銀行の資金力や顧客人数が関係してくるのではないかと予想し，実施銀行と未実施の銀行の二群に分けて，平均当期純利益，平均現預金高，平均資本額を比較した．なお，各指標については，2016年3月期のものを使用している．当期純利益，資本額については銀行の規模を表す指標として，現預金高については顧客人数を表す指標として取り扱っている．加えて，これらの値が他行と大きく乖離している都市銀行については，平均値への影響が強すぎるため除外している．図4に示したように，いずれの指標も実施銀行群のほうが大きかったことから，銀行の資金力や顧客人数がウイルス対策ソフトの配布に影響しているといえる．

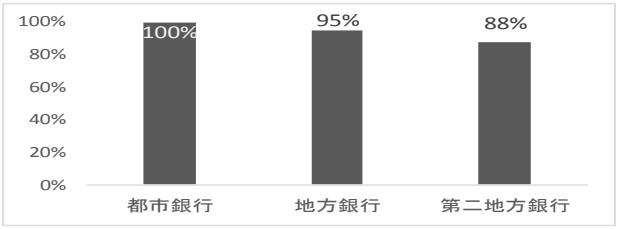

図 2:銀行業態別ウイルス対策ソフト配布実施率

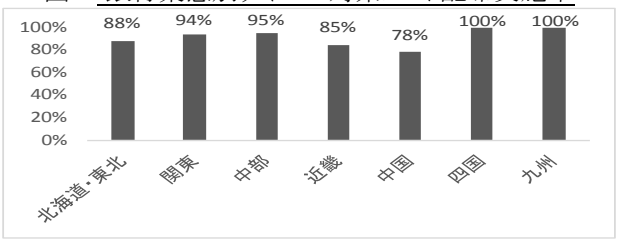

図 3:地域別ウイルス対策ソフト配布実施率

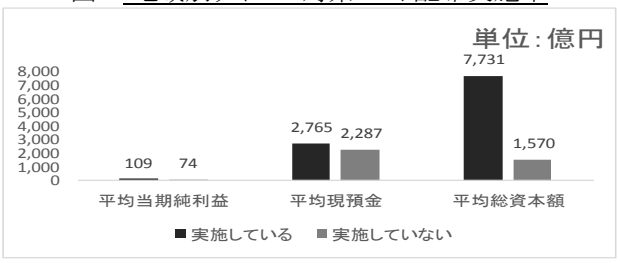

図 4:ウイルス対策ソフト配布の実施・未実施行の銀行規模の比較

4.2　ワンタイムパスワード導入率

前節同様ワンタイムパスワードについても業態別，地域別に差が出るか検証した．表2で示したように，ほとんどの銀行がワンタイムパスワードを導入しているが，機械生成タイプの導入行の場合は76行となり，導入率は7割程度に下がる．これは業態別，地域別に導入率を比較した図5，図6の結果においても，業態や地域にかかわらず同様の傾向が示されている．

一般的に，乱数表によるワンタイムパスワードは，顧客側に紙のカードを郵送するだけの初期費用となるが，機械生成の場合はハードウェアトークンの購入費やスマートフォンアプリの開発費など，銀行側により多くの初期費用の負担が発生する．これが機械生成によるワンタイムパスワードの導入率が低くなっている要因と考えられる．そこで，4.1と同様に，銀行の規模がワンタイムパスワードの導入に与える影響について分析した．

図7に示したように，機械生成によるワンタイムパスワードを導入している銀行は乱数表のみを導入している銀行よりも規模が大きい値となっている．よって，資金力の大きい銀行ほど機械生成タイプのワンタイムパスワードを導入しやすいと結論付けられる．

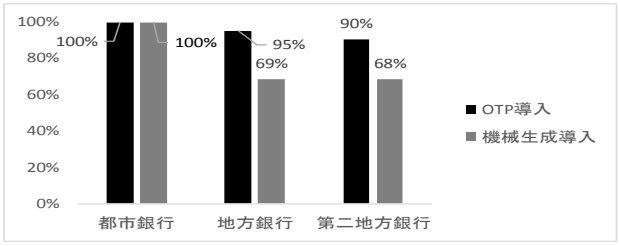

図 5:業態別ワンタイムパスワード導入率

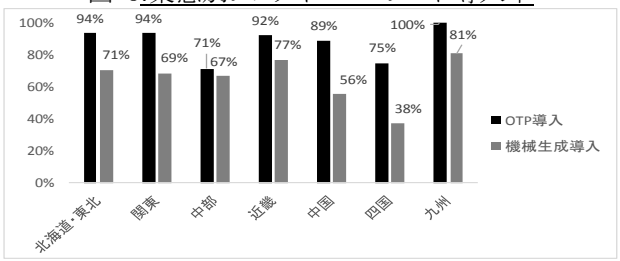

図 6:地域別ワンタイムパスワード導入率

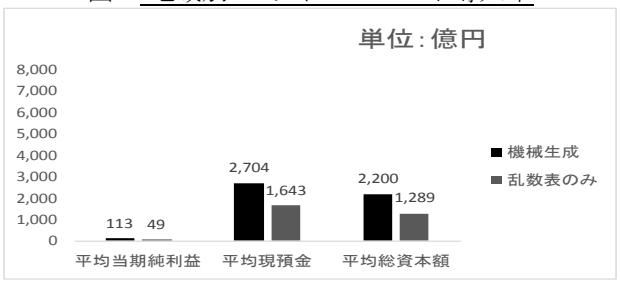

図 7:機械生成導入銀行と未導入銀行の規模の違い

4.3　機械生成のワンタイムパスワードにおける強制度比率

次に機械生成によるワンタイムパスワードを，顧客にどの程度の強制力で使用させているか，強制度を3種類に分けて実施行数の比率を算出した．図 8 に示したように，完全にすべての取引場面で使用するように強制している銀行はわずかであり，一部取引で強制している銀行と任意としている銀行でおおよそ半々という結果になった．

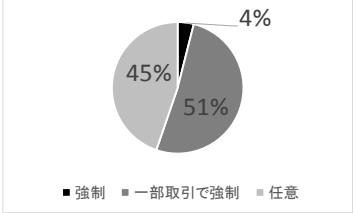

図 8:機械生成のOTPにおける強制度の実施比率

4.4　リスクベース認証の実施率

最後に表 2 の項目において，実施行数と未実施行数のばらつきが最も大きかったリスクベース認証について述べる．これまでの調査項目と同様に，業態別，地域別，規模別に分析した結果を図 9～図 11 に示す．地域別に見ると，北海道・東北，中部，近畿地方での実施率が高いのに対し他の 4 地方は半分以下となり，地域によって実施率の差に大きな差が出る(図 10)．以上のことから，リスクベース認証は他の認証技術に比べてまだまだ浸透していない様子が伺える．

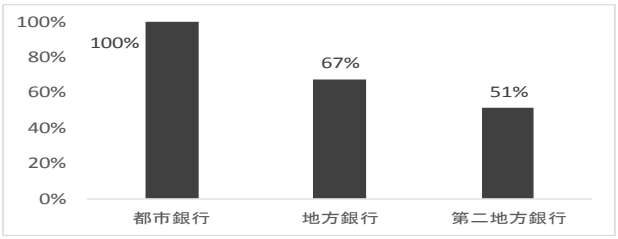

図 9:業態別リスクベース認証実施率

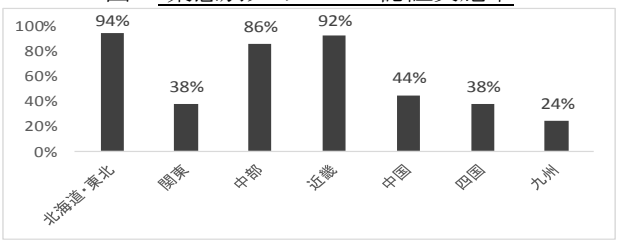

図 10:地域別リスクベース認証実施率

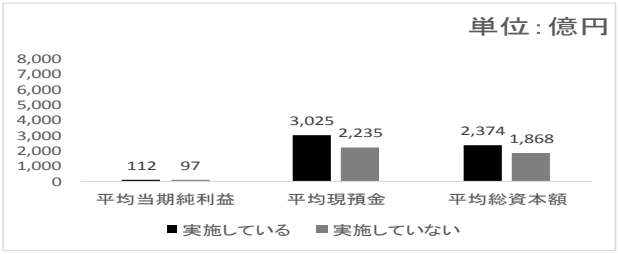

図 11:リスクベース認証実施・未実施の銀行規模比較

4.5　考察

以上より，ウイルス対策ソフトの配布，ワンタイムパスワードの導入についてはほとんどの銀行で実施されていて，機械生成によるワンタイムパスワードの導入，リスクベース認証の実施の有無には銀行によって実施，未実施に大きくばらつきが出ることがわかった．そして，その以上 4 項目を実施銀行，未実施銀行に分けて分析した結果，いずれも資金力のある規模の大きい銀行ほど導入していることが明らかになった．また，ワンタイムパスワードの強制度については，利用の判断を顧客に任せている銀行が半数近くあり，安全性よりも顧客の利便性を優先している姿勢が見て取れた．

以上より，現在のインターネットバンキングのセキュリティ強度は銀行の資金力に左右されがちで，現在利用可能なりすまし防止のためのセキュリティ技術を網羅的に取り入れている銀行は数少ないことがわかった．いくら認証技術が向上しても，銀行が取り入れなければ顧客の安全は守られないうえに，不正取引は増加するばかりである．この問題を解消するためには，顧客へのセキュリティ対策実施の強制度を上げ，不正取引防止につなげていく必要がある．

5.　研究のまとめ

本研究では，インターネットバンキングの認証に焦点をあて，各銀行が導入している認証技術とその運用方法について調査した．さらに，銀行の業態別および規模別にセキュリティ対策の傾向について比較・検証をして，これからのインターネットバンキングの認証サービスのあり方について考察した．

今回は，銀行の業態，地域，規模別にセキュリティ対策強度の調査を行ったが，実際の顧客のセキュリティ対策の実施状況の把握まで至らなかった．また，セキュリティ対策実施に消極的な銀行への聞き込みも行い，現実問題を深堀していくことも今後必要になると考える．

参考文献

[1] 宿輪純一，決済インフラ入門，東洋経済新報社，2015.
[2] 柏木亮二，フィンテック，日本経済新聞社，2016.
[3] 警視庁，平成27年中のインターネットバンキングに係る不正送金事案の発生状況等について，広報資料，2016，https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf.
[4] 警視庁，平成27年中のインターネットバンキングに係る不正送金事案の発生状況等について，広報資料，2015，https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf.
[5] CanonITソリューションズ株式会社，【特集】インターネットバンキングにおける不正送金の手口と対策について，マルウェア情報局，2014.
[6] 全国銀行協会，よりよい銀行づくりのためのアンケート2012年度，2012，http://www.zenginkyo.or.jp/abstract/news/detail/nid/3252/.
[7] 全国銀行協会，よりよい銀行づくりのためのアンケート2015年度，2016，http://www.zenginkyo.or.jp/abstract/news/detail/nid/5798/.
[8] 糸井正幸，多田充，”ワンタイムパスワード認証システムの利便性について”，研究報告コンピュータセキュリティ(CSCE)，2016-CSEC-72巻，21号，pp.1-5，2016.
[9] 平岩啓，満保雅浩，”時系列データの類似度検索を用いたユーザー認証の検討”，コンピュータセキュリティシンポジウム2016論文集，2016巻，2号，pp.1299-1303，2016.
[10] 中村啓佑，宇根正志，”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”，研究報告セキュリティ心理学とトラスト(SPT)，2016-SPT-19巻，15号，pp.1-6，2016.
[11] 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，2015巻，3号，pp.336-339，2015.
[12] 緒方祐介，大森芳彦，山下高生，岩田哲弥，”複数の公開鍵秘密鍵ペアの中継による認証方式のセキュリティに関する考察”，研究報告セキュリティ心理学とトラスト(SPT)，2016-SPT-17巻，16号，pp.1-6，2016.
[13] 平野亮，森井昌克，”パスワード運用管理に関する考察および提案とその開発”，電子情報通信学会技術研究報告.LOIS，ライフインテリジェンスとオフィス情報システム，111巻，286号，pp.129-134，2011.
[14] 大野博堂，サイバーセキュリティとBCPの実務，株式会社きんざい，2016.
[15] アクセンチュア,堅調に推移する2015年における日本でのフィンテック投資,2015，https://www.accenture.com/jp-ja/company-news-releases-20151125.