情報処理学会論文誌 Vol.58 No.12 1935–1942 (Dec. 2017)

インターネットバンキングにおける不正送金被害額の推定

岡林 喬久[1,a)] 猪俣 敦夫[1]

受付日 2017年2月27日, 採録日 2017年9月5日

概要：インターネットバンキングにおける不正送金被害が年々増加している．不正送金の手口は様々であるが，金融機関は日々巧妙化する不正送金手口に対して対策を行っている．不正送金は金融機関の利用者に起因したものがほとんどであるため，不正送金対策としては金融機関側の環境に対する対策だけではなく利用者に対して実施するものが多く存在する．しかし，多くの金融機関ではその対策を利用者の選択式にしていることが多く，セキュリティ対策の効果が発揮できているとはいえない状況である．本論文では，公表されている統計情報より，インターネットバンキング契約口座数規模ごとの不正送金被害件数および被害額の推定を行った．さらに，セキュリティ対策と被害額の関係を表すために，犯罪者の不正送金手口のモデルを提案し，その有用性を評価するためにセキュリティ対策ごとの被害額を利用者の対策導入率も含めて推定した．その結果，利用者におけるセキュリティ対策の導入率を高めることが不正送金額を低減させることを確認した．

キーワード：インターネットバンキング，不正送金

Estimation of Illegal Remittance Amount of Damage in the Internet Banking

Takahisa Okabayashi[1,a)] Atsuo Inomata[1]

Received: February 27, 2017, Accepted: September 5, 2017

Abstract: Illegal remittance damage in Internet banking has been increasing year by year. Modus operandi of illegal remittance may vary, but financial institutions have done measures against illegal remittance modus operandi to sophisticated every day. The cause of the illegal remittance is a user environment of the financial institutions. Therefore, illegal remittance measures are not only measures to financial institutions environment, there are many measures performed on the user's environment. However, many financial institutions, since the measures can't be forced to the user, is not complete effect of the security measures. In this paper, from the statistics that have been published, it was illegal remittance damage number and the estimated amount of damage of Internet banking agreement number of accounts each scale. In addition, in order to represent the relationship between the security measures and the amount of damage, to create a model of the illegal remittance modus operandi of criminals, it was estimated, including measures rate of introduction of user, damage amount of each security measures. As a result, it was confirmed that it is to reduce the illegal remittances to increase the rate of introduction of the user of the security measures.

Keywords: Internett banking, illegal remittance

1. はじめに

現在，インターネットを利用したサービスを提供する事業者が増加しており，利用者に対して利便性の高いサービスが提供されている．それにともない，国内におけるインターネット利用者は 1 億人を超え [1]，生活においてインターネット利用が常識化している．一方，高いインターネットの普及率にともない，サイバー犯罪も増加傾向にあり，サイバー犯罪の傾向も，自己顕示目的から金銭取得目的へと変化しているといわれている [2]．インターネットバンキングにおいても直接金銭を扱うサービスという特徴

[1] 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120–8551, Japan
[a)] okaba815@mocha.ocn.ne.jp

からサイバー犯罪の対象となっており，年々不正送金の被害金額が増加している [3].

被害者である銀行側も不正送金に対応すべく，リスクベース認証等のログイン認証強化や，2 経路認証，2 要素認証等の送金時の認証強化の実施，また，利用者の気づきに期待した，インターネットバンキングの TOP ページへの注意喚起や，送金時に利用者へメール送信する等多くのセキュリティ対策を実施している [4]．しかし，残念ながら不正送金の被害額は年々増加している．銀行側では不正送金被害を軽減させるべくさらなるセキュリティ対策を実施するが，多くのセキュリティ対策を実施すると当然多くの投資コストもしくはシステム維持コストが発生する．銀行では被害額を考慮したセキュリティ投資を行いたいが，自行における不正送金被害額が推定できない以上，セキュリティ対策への投資を続けざるをえないのが実情である．

本論文では，銀行ごとの被害状況を把握するために，公表されている統計情報より，インターネットバンキング契約口座数規模ごとの不正送金被害件数および被害額の推定を行う．また，セキュリティ対策と被害額の関係を表すために，犯罪者の不正送金手口のモデルを提案し，その有用性を評価するためにセキュリティ対策ごとの被害額を利用者の対策導入率も含めて推定した．その結果，利用者におけるセキュリティ対策の導入率を高めることが不正送金額を低減させることを確認した．

2. 不正送金をとりまく状況

2.1 不正送金における関連研究

現在不正送金に関する研究は以下に分類される．

- ✓ 現状の不正送金の現状を分析したもの
- ✓ 個々の不正送金手口に対して分析/防御する方策を提案したもの
- ✓ 金融機関に蓄積される取引ログの特徴から不正取引を検知するもの

「現状の不正送金の現状を分析したもの」では，佐野らが日本における不正送金の状況や海外での状況について昨今金融機関で問題になっている Man in the Browser（以降 MITB）攻撃について現状を報告している [4]．Castell では米国の不正送金の状況を示すとともに，顧客や企業等への教育の重要性について示している [5].「個々の不正送金手口に対して分析/防御する方策を提案したもの」では，土屋らが MITB 攻撃に対する対策として利用者と銀行サーバ間でセキュア通信を実現するチャレンジ&レスポンス方式のプロトコルを提案し，安全性検証を実施している [6]．この提案の方法は銀行サーバから利用者へのチャレンジをブラウザに潜むマルウェアが盗聴できない通信チャネルを通じて送信できるという前提の下でセキュア通信が可能であることを示している．西田らは MITB を引き起こすマルウェアに対して静的解析を行うことで攻撃手法を調査し，検体を一定期間動作させ設定情報の変化を観測することで，金融機関の利用者に対する攻撃が，C&C サーバやマニピュレーションサーバを用いた複雑な枠組みの中で行われていることを示している [7].「金融機関に蓄積される取引ログの特徴から不正取引を検知するもの」では，Carminati が「BankSealer」というオンラインバンキングの取引ログから不正取引の分析と，不正取引を分析する人の判断サポートをするシステム（仕組み）について記載したものである [8].「BankSealer」の特徴は，オンラインバンキングの過去の取引ログから各利用者の特徴を事前に抽出し新たな取引が発生した際にその内容が，事前に抽出した特徴からどれくらい異常なのかどうかをランキングしその結果をログ分析する人に伝えるものである．本論文では，実際の金融機関の取引ログで分析を実施した数少ない文献であるが，金融機関顧客の個人情報を含む取引ログを使用する本テーマへの取り組みは非常に難しい．

不正送金の被害額の推定に関する研究は非常に少ないうえに，公表されている統計情報は日本全体のものであるため，銀行規模ごとで発生件数や被害額は異なるものをどのように自身の銀行で活用するのかについては課題である．本論文では，公表されている統計情報より，インターネットバンキング契約口座数規模ごとの不正送金被害件数および被害額の推定を行った．さらに，セキュリティ対策と被害額の関係を表すために，犯罪者の不正送金手口のモデルを提案し，その有用性を評価するためにセキュリティ対策ごとの被害額を利用者の対策導入率も含めて推定した．

2.2 不正送金の被害状況

不正送金の被害状況について**表 1** に示す．1 件あたりの被害額については，それぞれの期間における被害額と件数より求めている．表 1 より年々被害額が増加していることが分かる．一方不正送金が発生した場合のインターネットバンキング利用者への補償割合は現状 9 割以上であり [4]，事案発生時の被害金額のほとんどを銀行側で補償しているのが現状である．

この現状より，各銀行は不正送金が発生しないようにセキュリティ対策もしくは利用者への注意喚起を実施しているが，多くのセキュリティ対策コストが必要であり，また，日々巧妙化する不正送金手口に追随して新たなセキュ

表 1 不正送金の被害状況 [3]
Table 1 Damage situation of illegal remittance [3].

期間	件数	被害額	1 件当たりの被害額
平成 27 年	1,495	約 30 億 7300 万円	2,055,518 円
平成 26 年	1,876	約 29 億 1000 万円	1,551,173 円
平成 25 年	1,315	約 14 億 600 万円	1,069,202 円

リティ対策を実施するかどうか難しい投資判断を迫られている．そのため，全体的な被害額や被害件数ではなく，それぞれの銀行における被害額や被害件数を推定し，追加するセキュリティ対策の投資コストと比較することで投資判断を行うことは非常に重要と考える．

3. 不正送金被害額の推定

3.1 口座数規模ごとの被害状況

それぞれの銀行を特徴付ける情報として，インターネットバンキングの口座数規模を用いることとした．口座数規模ごとの被害件数や被害額を求めるために，1 年あたりの不正送金確率 p を，インターネットバンキングの契約口座数 N，1 年あたりの被害件数 V を用いて，

$$p = \frac{V}{N}$$

として求める．今回は表 1 の平成 27 年の被害件数を V とし，インターネットバンキングの契約口座数（60,657,628）[9] を N とした．その結果，1 年あたりの不正送金発生確率 p を 0.0025%と求めた．口座数規模ごとの被害件数 v は先ほど求めた不正送金発生確率 p と口座数規模 n を用いて，

$$v = n \times p$$

とする．また，1 件あたりの被害額 c は 1 年あたりの被害件数 V と被害額の全体金額 C を用いて，

$$c = \frac{C}{V}$$

とする．今回は表 1 の平成 27 年の 1 件あたりの被害額を用いた．これらより口座数規模ごとの被害額 d は，

$$\begin{aligned} d &= v \times c \\ &= n \times p \times c \\ &= n \times \frac{V}{N} \times \frac{C}{V} \\ &= n \times \frac{C}{N} \end{aligned}$$

と求めることができる．**表 2** は上記を用いてインターネットバンキングの口座数規模ごとの被害発生件数 v と被害額 d を推定したものである．

この結果は，表 1 のような銀行全体における不正送金被害状況と比べ，インターネットバンキング口座数規模ごとの被害状況の傾向を見るには有用であると考える．しかし，銀行全体の被害状況から求めた結果であるため，銀行ごとの現状のセキュリティ対策実施状況を反映した被害発生件数，被害額になっていない．また，不正送金は犯罪者と銀行間だけでの問題ではなく，インターネットバンキングの利用者も含めた複雑な関係から発生するため，インターネットバンキングに利用者がどのように犯罪者から狙われて不正送金に至るのかを考慮に入れる必要がある．そこで次節では，インターネットバンキングの利用者がどのように不正送金被害にあうのか，不正送金手口のモデル化を実施し，それに対してセキュリティ対策の効果をふまえた被害額を求める．

3.2 手口のモデル化と不正送金金額の推定

3.2.1 不正送金手口のモデル化

不正送金被害額の推定のために，現在想定される不正送金の手口のモデル化を実施する（**図 1**）．攻撃者側から攻撃手口をいくつかの段階に区分化し，モデル化を行うことで全体像を把握するというアプローチとしては，Cyber kill chain モデルが有名である [10]．実際，Society for Worldwide Interbank Financial Telecommunication（以降 SWIFT）の事案に見るように攻撃者は段階的に不正送金に至るといわれている [11]．一般的なサイバー攻撃のモデル化である本モデルを不正送金にそのまま適用することは難しいが，不正送金に至るまでを段階的に遷移させることでモデル化した．モデル化における攻撃の各要素および遷移する確率については関連文献を調査した [3], [4], [12], [13], [14]．図 1 は犯罪者がインターネットバンキングの利用者に対して様々な不正送金手口を利用して不正送金に至る様子をモデル化している．図中の実線は関連文献から得られた統計値が存在するものである．たとえば，「攻撃メール送信」から「マルウェアへ感染させる」と「フィッシング」に実線が伸びており，それぞれの統計値は 0.92 と 0.08 となっている．これは文献 [12] より 2011 年 3 月～2013 年 11 月の不正送金被害が不正プログラムによるものかフィッシングによるものかの割合を計算した結果から得ている．また関連文献で得られなかった情報については破線にしている．破線が複数に分かれる場合は，遷移する確率は等分にしている．ファーミングについては公表されている情報が少ないことから低確率と仮定して 0.01 とした．なお，モデル化に利用した参考文献は調査年月にばらつきがあるが，モデルに影響するほど大きな攻撃傾向の変化はないため影響はない．たとえば，MITB により不正送金の被害に遭う場

表 2 口座数規模ごとの被害発生件数および金額
Table 2 Number of damages and amount of damage per account number.

インターネットバンキング口座数規模	5,000,000	1,000,000	500,000	300,000	100,000
被害発生件数(件/年)	123.23	24.65	12.32	7.39	2.46
被害額(円/年)	253,301,483	50,668,519	25,323,982	15,190,278	5,056,574

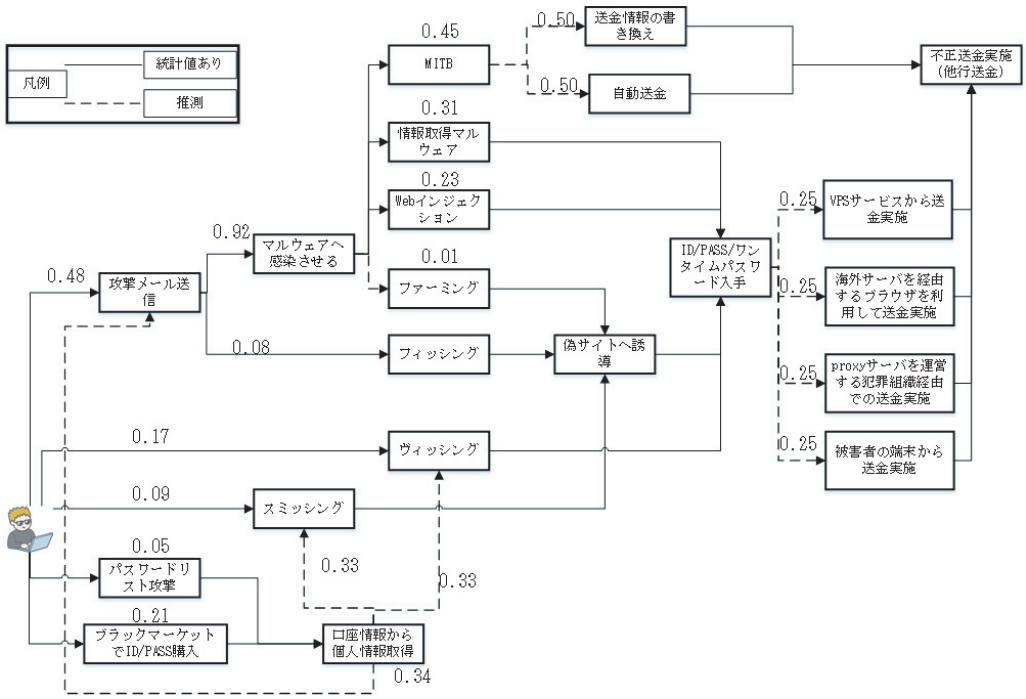

図 1 不正送金手口のモデル化
Fig. 1 Modeling illegal remittance method.

合を考えた場合図 1 では，犯罪者は攻撃メール送信し，被害者はメールに添付されたファイルを開封してしまいマルウェアに感染する．感染したマルウェアが MITB であり，被害者が，インターネットバンキングを利用し送金する際に送金情報を書き換えられて不正送金に至る場合は，「攻撃メール送信」→「マルウェアへ感染させる」→「MITB」→「送金情報の書き換え」→「不正送金実施」と遷移することとなる．今回参照した関連文献は次項以降ではこのモデルを利用し，不正送金被害額を推定する．

3.2.2 不正送金金額の推定

本項では前節で作成した不正送金手口のモデルから不正送金額推定を行う．推定するにあたり，インターネットバンキングの利用者の状況は預金額や保有口座数等様々であるため，本モデルにおけるインターネットバンキングの利用者として以下の仮定をおく．

✓ 1 人（1 世帯）あたりの預金額は，金融資産保有額の中央値である「4,000,000 円」とする [15].
✓ 1 人（1 世帯）あたりの保有口座数は 1 つ．

上記の仮定は被害者の預金をメインバンクにほとんど預けている状態を意味する．不正送金金額 T の推定には図 1 の「不正送金実施」までの経路上の攻撃手口から攻撃手口へ遷移する際の確率 p_i を乗算したものに被害者の預金額 dp を掛けたものをすべての経路で実施したものの和とし，

$$T = \sum \left(\prod p_i \times dp \right)$$

として求める．今回は預金額 dp を「4,000,000 円」とする．1 つの経路で例を示すと，「攻撃メール送信」→「マルウェアへ感染させる」→「MITB」→「自動送金」→「不正送金実施」の場合は，$0.48 \times 0.92 \times 0.45 \times 0.50 \times 4{,}000{,}000$ 円 $= 397{,}440$ 円となる．

3.3 対策実施における不正送金金額の推定

3.3.1 セキュリティ対策の効果

セキュリティ対策を考慮した際の不正送金金額の推定については，ある攻撃手口に対するセキュリティ対策が実施された場合，上記モデルにおいてその攻撃手口を通る経路においては不正送金が発生しないとする．つまり，セキュリティ対策を実施した際の効果として不正送金被害額を減少させることが可能である．本論文ではセキュリティ対策として，全国銀行協会で対策事例として紹介されているものを具体的な対策として読み替え評価を実施する（**表 3** 参照）[16], [17].

それぞれのセキュリティ対策がどの攻撃手口に対して有効なのかについて**表 4** に記載する．2 経路認証やワンタイムパスワードは ID やパスワードが盗まれた際のなりすましに対して強い認証方式であるため「○」となっている [18], [19], [20], [21]．しかし，2 経路認証やワンタイムパスワードは取引そのものを改竄する MITB には脆弱であるため「×」としている．トランザクション認証は，MITB に対して強い攻撃であるため「○」としている．金融機関が利用者に提供しているウイルス対策ソフトについては，製品 HP から効果があると思われるものに対して「○」をつけている．また有効性を確認する中で，ワンタイムパスワードと 2 経路認証については現在の分析軸では同じ効果

であったため，まとめている．この 2 つは，攻撃内容の詳細化や，利用者の使いやすさ，金融機関側導入費用やランニング費用等も分析軸とした場合は別に扱った方がよいと考えるが今回は不正送金手口のモデルからの分析を実施するため対象外とした．分析に際しては，セキュリティ対策は実施すれば攻撃手口に対して効果があると仮定する．たとえば，ワンタイムパスワードの場合，フィッシング等でパスワード情報を取得された直後に不正送金を実施された場合，効果は本来「×」になるはずであるが，複雑になるためそういった場合は考慮しないこととした．

また，これらのセキュリティ対策は利用者の希望，もしくは選択性になっていることが多いため，銀行側がセキュリティ対策として導入していたとしてもその効果を利用者が必ず得られるわけではない．そこでセキュリティ対策導率についても考慮に入れる．セキュリティ対策導入率 t を考慮した被害額の導出式は以下とする．

$$T = \sum \left\{ \prod p_i \times dp \times (1-t) \right\}$$

表 3 全国銀行協会での対策事例
Table 3 Examples of countermeasures in Japanese Bankers Association.

原文	具体的な対策
可変式パスワードや電子証明書などの，固定式の ID・パスワードのみに頼らない認証方式	ワンタイムパスワード（ハードトークン）
取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど，複数経路による取引認証	2 経路認証（携帯電話/スマートフォンへのワンタイムパスワード通知）
ハードウェアトークン等でトランザクション署名を行うトランザクション認証	トランザクション認証
取引時においてウイルス等の検知・駆除が行えるセキュリティ対策ソフトの利用者への提供	ウイルス対策ソフトの提供

先ほど例で示した経路，「攻撃メール送信」→「マルウェアへ感染させる」→「MITB」→「自動送金」→「不正送金実施」の場合において，トランザクション認証を導入しており，導入率が 20%である場合は，$0.48 \times 0.92 \times 0.45 \times 0.50 \times 4{,}000{,}000$ 円 $\times (1-0.2) = 317{,}952$ 円となる．1 件あたりの被害額について対策導入率 20%の場合と 100%の場合について表したものを**表 5** に示す．ここで対策導入率 100%とは利用者全体がそのセキュリティ対策を実施していることを意味している（いい換えると銀行側でそのセキュリティ対策を強制していることを意味する）．本論文では一例として導入率を 20%，100%とするが，試算を行うときは導出式の t を適切に変更する必要がある．なお，1 件あたりの被害額が表 1 の結果と異なり高くなっているのは，導出過程が異なるためである．表 1 は公表されている統計情報をもとに 1 件あたりの被害額を導出しているが，表 5 は 1 人（1 世帯）あたりの預金額である 4,000,000 円全額が不正送金の対象になると仮定しているためである．

3.3.2 セキュリティ対策の効果

上記で求めた，1 件あたりの被害額 T と口座数ごとの被害発生件数 v を用いて，口座数規模ごとの被害額 dn を，

$$dn = T \times v$$

とし，被害額を求めたものを**表 6** に示す．また，表 6 では対策を実施していない場合の被害額 ND を，

表 5 対策導入率ごとの被害額
Table 5 Amount of damage per measure introduction rate.

被害額（1 件当たり）	2 経路認証/ワンタイムパスワード	トランザクション認証	ウイルス対策ソフト配布
対策導入率 20%	3,388,254 円	3,200,000 円	3,585,841 円
対策導入率 100%	941,270 円	0 円	1,929,205 円

表 4 攻撃手口に対するセキュリティ対策の有効性
Table 4 Effectiveness of security measures against attack method.

	2 経路認証/ワンタイムパスワード	トランザクション認証	ウイルス対策ソフトの提供
MITB	×	○	○
情報取得マルウェア	○	○	○
Web インジェクション	○	○	○
ファーミング	○	○	×
フィッシング	○	○	×
ヴィッシング	○	○	×
スミッシング	○	○	×

（○はセキュリティ対策が有効，×は無効）

表 6 口座数規模ごとの被害発生件数と被害額
Table 6 Number of damaged and damage amount per account number.

インターネットバンキング口座数		5,000,000	1,000,000	500,000	300,000	100,000
被害発生件数(件/年)		123.23	24.65	12.32	7.39	2.46
対策していない時の被害額(円/年)		492,920,000	98,600,000	49,280,000	29,560,000	9,840,000
不正送金額(円/年)	(a)	417,534,540	83,520,461	41,743,289	25,039,197	8,335,105
		(75,385,460)	(15,079,539)	(7,536,711)	(4,520,803)	(1,504,895)
(数字)は対策による被害低減額	(b)	115,992,702	23,202,306	11,596,446	6,955,985	2,315,524
		(376,927,298)	(75,397,695)	(37,683,554)	(22,604,015)	(7,524,476)
	(c)	394,336,000	78,880,000	39,424,000	23,648,000	7,872,000
		(98,584,000)	(19,720,000)	(9,856,000)	(5,912,000)	(1,968,000)
	(d)	0	0	0	0	0
		(492,920,000)	(98,600,000)	(49,280,000)	(29,560,000)	(9,840,000)
	(e)	441,883,186	88,390,981	44,177,561	26,499,365	8,821,169
		(51,036,814)	(10,209,019)	(5,102,439)	(3,060,635)	(1,018,831)
	(f)	237,735,932	47,554,903	23,767,806	14,256,825	4,745,844
		(255,184,068)	(51,045,097)	(25,512,194)	(15,303,175)	(5,094,156)

(a) 2経路認証/ワンタイムパスワード:対策導入率 20%
(b) 2経路認証/ワンタイムパスワード:対策導入率 100%
(c) トランザクション認証:対策導入率 20%
(d) トランザクション認証:対策導入率 100%
(e) ウイルス対策ソフト配布:対策導入率 20%
(f) ウイルス対策ソフト配布:対策導入率 100%

$$ND = v \times dp$$

とし，セキュリティ対策を行った際の被害低減額 DD を，

$$DD = ND - dn$$

として，カッコ付きで記載している．表 6 より対策導入率が低い場合（20%）のそれぞれの対策の被害額 S は 7,872,000 円～8,821,169 円（表中の (a)，(c)，(e)）となるのに対し，対策導入率が高い場合（100%）の場合は，0 円～4,745,844 円（表中の (b)，(d)，(f)）となり，セキュリティ対策別の効果よりも，利用者におけるセキュリティ対策の導入率を高める方が不正送金額の被害額を減少させる効果が大きいことが分かる．

4. 結果

本研究では，公表されている統計情報より，インターネットバンキング契約口座数規模ごとの不正送金被害件数および被害額の推定を行った．その結果，口座数規模ごとに不正送金の発生件数やそれにともなう発生金額に大きなばらつきがあることを確認した．さらに，セキュリティ対策と被害額の関係を表すために，犯罪者の不正送金手口のモデルを作成し，セキュリティ対策ごとの被害額を利用者のセキュリティ対策導入率も含めて推定した．その結果セキュリティ対策の利用者の導入率を高めることが不正送金額を低減させることを確認した．

不正送金額の推定に用いたモデルの妥当性検証のために実際に銀行で発生した不正送金事案の実例との比較行う．しかし，不正送金事案における被害額や被害件数の実例については公表されているものは少なく，今回は鹿児島県警察の発表で報告された，鹿児島県の実例を用いることとした [22]．本報告では H27 年の実績で不正送金件数 13 件，不正送金金額は約 20,000,000 円というものであった．鹿児島県ではインターネットバンキングを提供する銀行は 6 行（地銀，第 2 地銀，信金，信組等）あるが，半分の被害が地銀で発生していると仮定すると不正送金件数 6 件，不正送金金額は 10,000,000 円となる．一方地銀の口座数規模は文献 [2] より約 150,000 口座であることから，口座数規模ごとの被害額を求めると被害件数 3.69 件，ウイルス対策ソフトを配布し対策導入率 20%の場合の被害金額は 13,231,754 円となり推定値と近い結果が出ていることが確認できた．実際の被害金額よりも大きい結果がでる理由としては，1 日の送金回数や，1 回あたりの送金金額の上限がある等，今回あげた以外のセキュリティ対策によるものである．

5. 考察

本研究では，攻撃手口のモデル化を実施したうえで，セキュリティ対策を考慮した不正送金被害額を推定した．その結果，現状とりうるセキュリティ対策ごとには大きな差はないものの，そのセキュリティ対策をどれくらい多くの利用者が実施したかでその効果が大きく変わることが確認できた．現状金融機関では，利用者の利便性を損なうとい

う理由や，複雑なセキュリティ対策になると，利用者からの問合せ件数が急激に増加することが考えられ，金融機関のヘルプデスク運用負荷が大きくなることからセキュリティ対策の利用者強制ができていないことが現状であると推察する．しかし，本結果から今後は利用者に対して，セキュリティ対策の導入率を上げるような周知を行う，もしくは利用者に強制することも考慮していく必要があると考える．

比較的インターネットバンキング口座数の少ない金融機関は被害金額も少ないことから実際にセキュリティ対策をする場合には，投資が過剰でないかを本研究の結果もふまえ検討していただきたい．今回あげた対策にかかる投資費用については，各金融機関の規模やシステム構成によって大きく変わるため，投資費用については記載できないが，システムへの初期投資以外にも，たとえばワンタイムパスワードであれば，口座数分のトークン自体のコスト以外に紛失した際の交換にかかる費用等のランニング費用についても考慮する必要がある．特に今回あげたセキュリティ対策を 1 つでも導入しおり，追加の対策を行う場合はインターネットバンキングの利用者に任意にしている既存のセキュリティ対策を実施してもらうように働きかけた方がより大きな効果がでると考える．一方で今回あげたセキュリティ対策を導入しておらずこれからセキュリティ対策を行う場合は，複数の対策を実施することを考える前に，今回の分析よりトランザクション認証を利用者に強制する場合（表 6 の (d)）が最も効果が高いため，トランザクション認証の導入とあわせて利用者に強制することを計画し，銀行の IT 部門やインターネットバンキングのビジネス部門，コールセンタ部門と連携した導入をすることが最も良いと考える．また，今回あげたセキュリティ対策のうち，2 経路認証/ワンタイムパスワード/トランザクション認証は金融機関側で強制が可能であるが，ウイルス対策ソフト配布は利用者が自身の端末にインストールを実施してもらう必要があり，利用者によっては別のウイルス対策ソフトをインストールしていることもあり強制が難しいことも考慮に入れる必要がある．

6. おわりに

本研究で作成したモデルについては，現状得ることのできる公表されている統計情報もしくは参考文献をもとに作成したものである．しかし日々巧妙化，多様化する不正送金手口に対して追随したモデルの改変や分析が必要であると考える．

今後の課題としては，今回の結果は利用した統計情報は法人/個人が混在する形であったが，法人/個人ごとの統計情報が得られれば，それぞれの特色についても検討したい．また，結果で示した実際の被害金額よりも大きい結果がでる理由としてあげた，1 日の送金回数や，1 回あたりの送金金額の上限等，今回あげた以外のセキュリティ対策についても検討したい．

参考文献

[1] 平成 26 年通信利用動向調査の結果，入手先 ⟨http://www.soumu.go.jp/johotsusintokei/statistics/data/150717_1.pdf⟩（参照 2016-09-06）．

[2] インターネットバンキングに係る不正送金事犯被害の実態と防止策，入手先 ⟨https://www.antiphishing.jp/news/pdf/apcseminar2015npa.pdf⟩（参照 2016-09-06）．

[3] 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犯の発生状況等について，入手先 ⟨https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf⟩（参照 2016-09-06）．

[4] 佐野宏明，田中英彦：インターネットバンキングの不正送金対策．第 77 回全国大会講演論文集，No.1, pp.443–444 (2015).

[5] Castell, M.: Mitigating Online Account Takeovers: The Case for Education, *Retail Payments Risk Forum Survey Paper* (2013).

[6] 土屋貴史，藤田真浩，高橋健太，加藤岳久，間形文彦，勅使河原可海，佐々木良一，西垣正勝：Man In The Browser 攻撃対策を実現する人間・サーバ間のセキュア通信プロトコル，研究報告コンピュータセキュリティ（CSEC），No.22, pp.1–9 (2015).

[7] 西田雅太，太刀川剛，岩本一樹，遠藤　基，奥村吉生，星澤裕二：静的解析と挙動観測による金融系マルウェアの攻撃手法の調査，*Computer Security Symposium 2014*, 22–24，pp.859–866 (2014).

[8] Carminati, M., Caron, R., Maggi, F., Epifani, I. and Zanero, S.: BankSealer: An online banking fraud analysis and decision support system, *ICT Systems Security and Privacy Protection*, Vol.428, pp.380–394 (2014).

[9] 公益財団法人金融情報システムセンター（編）：平成 28 版融情報システム白書 (2015).

[10] Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, available from ⟨https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf⟩ (accessed 2016-10-17).

[11] SWIFT の不正送金から得られた教訓—1 億米ドルの不正送金を防ぐ為に，入手先 ⟨https://www.pwc.com/jp/ja/japan-knowledge/archive/assets/pdf/swift-bangladesh-robbery-2016.pdf⟩（参照 2016-10-17）．

[12] 不正送金及び不正アクセス等の被害について，入手先 ⟨https://www.antiphishing.jp/news/pdf/apcseminar2013npa.pdf⟩（参照 2016-09-06）．

[13] 2015 年脅威の統計概要，入手先 ⟨http://media.kaspersky.com/jp/Kaspersky_KSB2015_Statistics-PR-1021.pdf⟩（参照 2016-09-06）．

[14] 平成 27 年における不正アクセス行為の発生状況等の公表について，入手先 ⟨https://www.npa.go.jp/cyber/pdf/h280324_access.pdf⟩（参照 2016-09-06）．

[15] 「家計の金融行動に関する世論調査」［二人以上世帯調査］，入手先 ⟨https://www.shiruporuto.jp/finance/chosa/yoron2015fut/pdf/yoronf15.pdf⟩（参照 2016-09-06）．

[16] フィッシングレポート 2016—世界に広がるフィッシング対策の輪，入手先 ⟨https://www.antiphishing.jp/report/pdf/phishing_report_2016.pdf⟩（参照 2016-09-06）．

[17] セキュリティ対策向上・強化等に関する全国銀行協会の「申し合わせ」（平成 24 年 1 月，25 年 11 月，26 年 5 月，26 年 7 月等）における対策事例，入手先 ⟨https://www.zenginkyo.or.jp/topic/detail/nid/6389/⟩（参照 2016-09-06）．

[18] 本人認証技術の現状に関する調査報告書，入手先 ⟨https://www.ipa.go.jp/security/fy14/reports/authentication/authentication2002.pdf⟩（参照 2016-10-17）．
[19] インターネットバンキングの安全性を巡る現状と課題, 入手先 ⟨https://www.boj.or.jp/research/wps_rev/rev_2006/data/rev06j14.pdf⟩（参照 2016-10-17）．
[20] インターネット・バンキングの安全性を巡る現状と課題—2007 年，入手先 ⟨https://www.boj.or.jp/research/wps_rev/rev_2007/data/rev07j14.pdf⟩（参照 2016-10-17）．
[21] オンライン本人認証方式の実態調査報告書，入手先 ⟨https://www.ipa.go.jp/files/000040778.pdf⟩（参照 2016-10-17）．
[22] インターネットバンキングに係る不正送金事案について，入手先 ⟨https://www.pref.kagoshima.jp/ja12/police/network/netwarkhanzai_119.html⟩（参照 2016-10-17）．

岡林 喬久

1999 年高知大学理学部情報科学学科卒業．2001 年高知大学大学院理学研究科修了．2006 年高知大学大学院医学研究科修了．博士（医学）．2016 年より東京電機大学大学院情報セキュリティ研究室に所属．

猪俣 敦夫 （正会員）

2002 年北陸先端科学技術大学院大学修了．博士（情報科学）．2008 年より奈良先端科学技術大学院大学准教授．2016 年より東京電機大学教授．奈良先端科学技術大学院大学客員教授．一般社団法人公衆無線 LAN 認証管理機構代表理事．一般社団法人 JPCERT コーディネーションセンター理事．暗号とその実装，組み込みシステムセキュリティに関する研究・開発に従事．