Vol.2016-DPS-168 No.15
Vol.2016-SPT-21 No.15
Vol.2016-EIP-74 No.15
2016/11/18

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]　佐々木良一[†1]　猪俣敦夫[†1]

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が起因によるものがほとんどである為、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事が多くセキュリティ対策の効果が発揮できているとは言えない状況である．本稿では、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毎の不正送金被害件数及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為に、犯罪者の不正送金手口のモデルを作成し、セキュリティ対策毎の被害額を利用者の対策導入率も含めて推定した．その結果セキュリティ対策の利用者の導入率を高める事が不正送金額を低減させる事を確認した．

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 amout of damage in the Internet Banking

TAKAHISA OKABAYASHI[†1]　RYOICHI SASAKI[†1]　ATSUO INOMATA[†1]

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．それに伴い、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伴い、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言われている[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、リスクベース認証などのログイン認証強化や、２経路認証、２要素認証などの送金時の認証強化の実施、又、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など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．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が発生するが、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得ないのが実情である．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毎の不正送金被害件数及び被害額の推定を行う．又、セキュリティ対策と被害額の関係を表す為に、犯罪者の不正送金手口のモデルを作成し、セキュリティ対策毎の被害額を推定する．　さらに、セキュリティ対策と被害額の関係を表す為に、犯罪者の不正送金手口のモデルを作成し、セキュリティ対策毎の被害額を利用者の対策導入率も含めて推定した．その結果セキュリティ対策の利用者の導入率を高める事が不正送金額を低減させる事を確認した．

†1 東京電機大学
Tokyo Denki University

Vol.2016-DPS-168 No.15
Vol.2016-SPT-21 No.15
Vol.2016-EIP-74 No.15
2016/11/18

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(2015)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 MITB 攻撃について現状を報告している[4]. Michelle(2013)では米国の不正送金の状況を示すと共に、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(2015)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(2013)では MITB を引き起こすマルウェアに対して静的解析を行う事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事を示している[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、Michele(2014)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)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にて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く、公表されている統計情報で分かる被害額は日本全体という形では示されている. しかし銀行規模毎で発生件数や被害額は異なる為、公表されている統計情報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、銀行の特徴をインターネットバンキング契約口座数規模とし、公表されている統計情報を用いて不正送金被害件数及び被害額の推定を行う.

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 件当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事がわかる. 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.

表 1 不正送金の被害状況[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

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、又、日々巧妙化する不正送金手口に追随して新たなセキュ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. その為、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事は非常に重要と考える.

そこで、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を用いる事とした. 表 1 の平成 27 年の被害件数とインターネットバンキングの契約口座数(60,657,628)[9]より、1 年あたりの不正送金発生確率を求める事ができ、0.0025%と求めた. 表 2. において、求めた不正送金発生確率を用いて、インターネットバンキングの口座数規模毎の被害発生件数と被害額を推定した. 尚被害額については、被害発生件数に平成 27 年の 1 件当た

表 2 口座数規模毎の被害発生件数

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

Vol.2016-DPS-168 No.15
Vol.2016-SPT-21 No.15
Vol.2016-EIP-74 No.15
2016/11/18

りの被害額を掛けたものとした.

この結果は、銀行全体の被害状況から求めた結果である為、銀行毎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. 又、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. そこで次項では、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踏まえた被害額を求める.

3. 不正送金被害額の推定

3.1 不正送金手口のモデル化

不正送金被害額の推定の為に、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). モデル化に際しては攻撃の要素および遷移する確率について関連文献を調査した[3][4][10][11][12]. 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. 又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事から低確率と仮定して 0.01 とした. 例えば、MITB により不正送金の被害に遭う場合を考えた場合図 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」と遷移する事となる. 次節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.

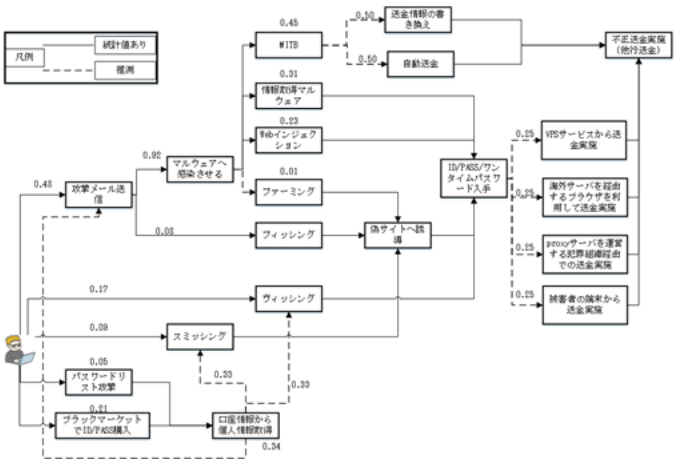

図 1 不正送金手口のモデル化

3.2 不正送金額の推定方法

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など様々であるため、以下の仮定を置く.

- ✓ 一人当たりの預金額は、金融資産保有額の中央値である「4,000,000 円」とする[13]
- ✓ 一人当たりの保有口座数は一つ

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を乗算したものに被害者の預金額「4,000,000 円」を掛けたものを全ての経路で実施したものの和とする. 一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. 48×0. 92×0. 45×0. 50×4,000,000 円 = 397,440 円となる.

3.3 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事が可能である. 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)[14].

表 3 全国銀行協会での対策事例

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

Vol.2016-DPS-168 No.15
Vol.2016-SPT-21 No.15
Vol.2016-EIP-74 No.15
2016/11/18

表 4 攻撃手口に対するセキュリティ対策の有効性

	ワンタイムパスワード	2 経路認証	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)

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. 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. 例えば、ワンタイムパスワードの場合、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事とした.

又、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事が多い為、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. 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、0.48×0.92×0.45×0.50×4,000,000 円×(1 - 0.2) = 317,952 円となる. 1 件当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事を意味している(言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事を意味する).

3.4 口座数規模毎の被害額

上記で求めた、1 件当たりの被害額と口座数毎の被害発生件数から、被害額を求めたものを表 6 に示す. 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事がわかる.

表 5 対策導入率毎の被害額

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

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毎の不正送金被害件数及び被害額の推定を行った. その結果、口座数規模毎に不正送金の発生件数やそれに伴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為に、犯罪者の不正送金手口のモデルを作成し、セキュリティ対策毎の被害額を利用者の対策導入率も含めて推定した. その結果セキュリティ対策の利用者の導入率を高める事が不正送金額を低減させる事を確認した.

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いが、鹿児島県警察の発表では 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 円というものがあった[15]. 鹿児島県にて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[2]より約 150,000 口座であることから、口座数規模毎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事が確認できた. 実際の被害金額よりも大きい結果がでる理由としては、一日の送金回数や、一回当たりの送金金額の上限がある等、今回上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上で、セキ

Vol.2016-DPS-168 No.15
Vol.2016-SPT-21 No.15
Vol.2016-EIP-74 No.15
2016/11/18

表 6 口座数規模毎の被害発生件数と被害額

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
不正送金額(円/年)	(a)	417,534,540	83,520,461	41,743,289	25,039,197	8,335,105
	(b)	115,992,702	23,202,306	11,596,446	6,955,985	2,315,524
	(c)	394,336,000	78,880,000	39,424,000	23,648,000	7,872,000
	(d)	0	0	0	0	0
	(e)	441,883,186	88,390,981	44,177,561	26,499,365	8,821,169
	(f)	237,735,932	47,554,903	23,767,806	14,256,825	4,745,844

(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%

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、現状取りうるセキュリティ対策毎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事が確認できた．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、利用者からの問い合わ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事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事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踏まえ検討して頂きたい．特に今回挙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．

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元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．

7. 今後の課題

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/個人毎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．又、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挙げた、一日の送金回数や、一回当たりの送金金額の上限等、今回上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”．
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”．
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”．
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, 2015 年, no1, p. 443-444
[5] Michelle Castell. 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), 2015 年, no22,p.1-9
[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, 2014 年, 22 – 24, p.859-866.
[8] Michele Carminati, Roberto Caron, Federico Maggi, Ilenia Epifani,

Vol.2016-DPS-168 No.15
Vol.2016-SPT-21 No.15
Vol.2016-EIP-74 No.15
2016/11/18

and Stefano Zanero. BankSealer: An online banking fraud analysis and decision support system, ICT Systems Security and Privacy Protection, 2014, Vol428, p.380-394.

［9］”インターネットと銀行サービスの再考”.
https://www.boj.or.jp/announcements/release_2016/data/rel160314a2.pdf, (参照 2016-09-06).

［10］“不正送金及び不正アクセス等の被害について”.
https://www.antiphishing.jp/news/pdf/apcseminar2013npa.pdf, (参 照 2016-09-06).

［11］”2015 年 脅威の統計概要”.
http://media.kaspersky.com/jp/Kaspersky_KSB2015_Statistics-PR-1021.pdf, (参照 2016-09-06).

［12］“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”.
https://www.npa.go.jp/cyber/pdf/h280324_access.pdf, (参照 2016-09-06).

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

［14］“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 ―”.
https://www.antiphishing.jp/report/pdf/phishing_report_2016.pdf, (参照 2016-09-06).

［15］“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”.
https://www.pref.kagoshima.jp/ja12/police/network/netwarkhanzai_119.html, (参照 2016-10-17).