2015.1

企業リスクインフォ ＜2014 No.4＞

インターネットバンキングにおける不正送金被害とその対策

はじめに

インターネットバンキングとは、インターネットを介して主にPCのブラウザで行う銀行取引サービスのことである。専用回線や専用端末が不要であることから、多くの企業・個人で導入が進んでいる。その一方で、2013年頃からウイルスなどにより不正にIDやパスワードを盗まれ自身の口座から犯罪者の口座へと不正送金される事件が急増している。以前は個人の被害がほとんどであったが、最近では法人口座の被害件数が増加している。また法人口座は個人に比べ送金限度額が大きく、一度の不正送金が事業に大きな損失を与える可能性がある。本稿では、法人におけるインターネットバンキングの不正送金被害の概要および手口について説明し、最後に対策についてのポイントを解説する。

（以降、本稿では「インターネットバンキングにおける不正送金」を単に「不正送金」と略）

１．不正送金被害の概要

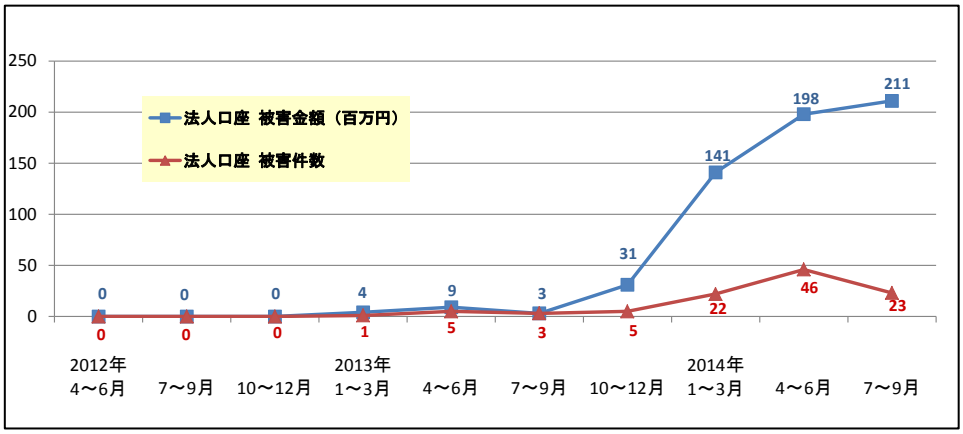
(1)不正送金被害の概要と特徴

不正送金は、主に犯罪者が正規利用者へ成りすまして不正にログインすることで実行される。犯罪者は後述する巧妙な手口（フィッシング詐欺やウイルス）で入手した法人口座のIDとパスワードを使ってログインし、犯行用口座へ送金し、即座に現金預払機（ATM）で出金する。口座残高を確認するまで不正送金の被害に気付きにくいことから発見が遅れ、複数回に渡って不正送金されるなど被害拡大につながりやすい特徴がある。

(2)法人口座の不正送金被害の推移

全国銀行協会が公表した金融機関向けアンケート結果（図表１）によると、本年１月頃から不正送金被害の件数・金額が増加していることがわかる。この理由としては、より巧妙かつ悪質な不正送金目的のウイルス等が出現するも、企業の対策が後手に回ったためと推察される。

【図表１　法人口座の不正送金被害の金額・件数について】

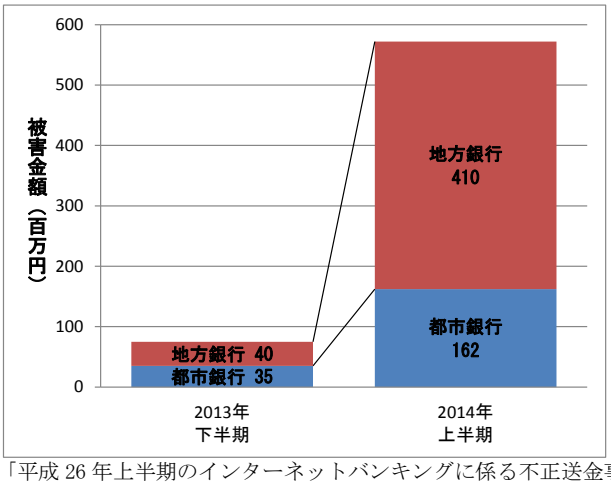


（出典：全国銀行協会「インターネット・バンキングによる預金等の不正払戻し」等に関するアンケート結果」（2014年11月27日））

(3)都市銀行から地方銀行や信用金庫への拡大

警察庁の広報資料（図表２）によると、地方銀行や信用金庫の被害が拡大していることがわかる。これは多発する被害を受け対策を強化した都市銀行から、地方銀行や信用金庫へと標的をシフトさせたためと推察される。

【図表２　金融機関別の被害金額】



（**出典**：警察庁 広報資料「平成 26 年上半期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について」（2014 年 9 月 4 日））

２．不正送金の手口

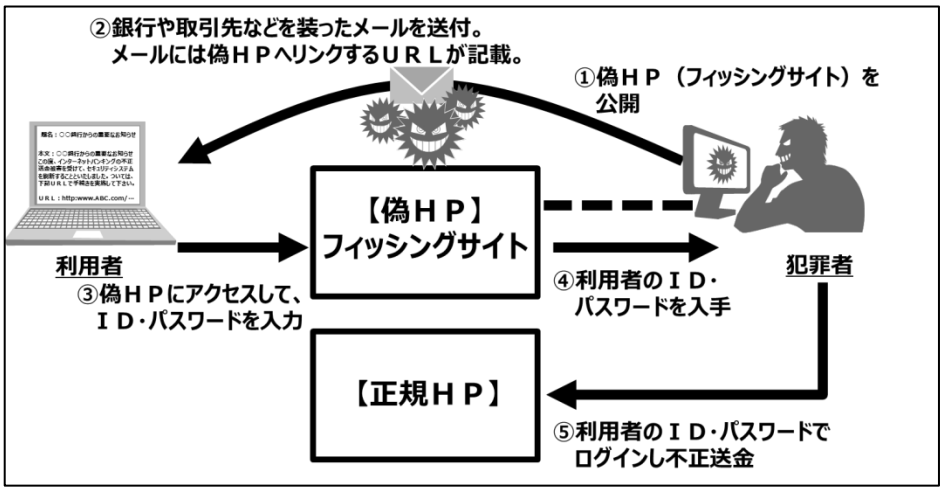
不正送金の多くの手口は前述した通り企業利用者の ID・パスワードを窃取するところが起点となっている。この ID・パスワードを不正に取得する手段として現時点で確認されている主な手口は次の二つである。

（1）フィッシング詐欺

フィッシング詐欺とは、犯罪者が実在する企業を装った電子メールを送付し、それらのウェブサイトに酷似したフィッシングサイト（偽のサイト）に誘導し、ID・パスワードやクレジットカード番号、個人情報等の重要情報を入力させて窃取する詐欺行為である（図表３参考）。

犯罪者は①ID・パスワード窃取用のフィッシングサイトを公開し、②銀行やクレジットカード会社等の実在する金融機関を精巧に模した電子メールを利用者に送り付け、メールに記載された URL からフィッシングサイトへ言葉巧みに誘導し、③利用者に口座番号や ID･パスワードを入力させる。④犯罪者は利用者の ID･パスワードを入手し、⑤その情報で金融機関へログインし不正送金を行う。

【図表３　フィッシング詐欺の概要】



（インターリスク総研にて作成）

フィッシング詐欺自体は 10 年以上前から発生しているが、不正送金の被害にあったケースを見てみると、緊急事態の発生を装うなど非常に巧妙化している点が特徴的である。

例１　貴社の口座が何者かに不正ログインされている可能性があるため、直ちに下記からログインしパスワード変更手続きをしてください。

例２　当行のセキュリティ強度を向上させるためにシステムを緊急アップデートします。全アカウントを停止する必要がありますが、停止を一時回避したい場合は下記にアクセスして停止回避手続きしてください。

また以前はフィッシング詐欺の多くは個人を狙ったものであったため、個人向けにはプロバイダやウェブサイトの運営者により相当の注意喚起や啓発がなされてきた。一方、法人については、2011年ごろから増加した標的型攻撃メールで一定の注意喚起がなされたとはいえ、実際に被害に遭っているのは政府機関や大企業の一部のため、こうした詐欺の手口に不慣れな企業のインターネットバンキング担当者がフィッシング詐欺に遭い、不正送金の被害を被ったものと推察される。

(2) ウイルス（不正送金プログラム）

コンピュータウイルスとは、一般的には、データの破壊や改ざん、窃取などの悪質な行為を行う目的で悪意ある第三者に作られたプログラムのことを指す。感染経路は次の通り多岐にわたる。

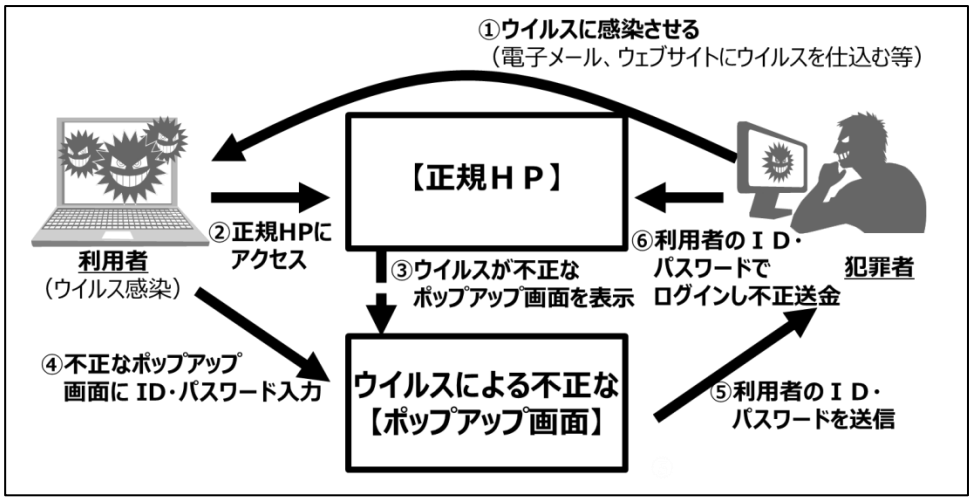
a. 電子メール
　添付ファイルや本文（HTML スクリプト）へのウイルス挿入による感染、メール内記載のリンク先サイトの閲覧による感染（下記 c. 参照）
b. ネットワーク（社内 LAN など）
　感染した PC が原因となりネットワーク経由で感染
c. ウェブサイト
　ウイルスに感染されたサイトの閲覧により感染
d. ソフトウェア
　ウイルスに感染したソフトウェアをインストールすることで感染
e. 電子記憶媒体（USB メモリなど）
　ウイルスが仕込まれた US メモリにより PC に接続した際に感染　など

不正送金で猛威を振るった不正送金ウイルスは次のような流れ（図表４）で被害をもたらしている。

①犯罪者が利用者に電子メールやウェブサイト経由で利用者の PC にウイルスを感染させる。②利用者がウイルスに感染した PC で正規のインターネットバンキングサイトにアクセスすると、③ウイルスがアクセスを検知し、ID・パスワード、第２暗証番号などを入力させる偽のポップアップ画面を表示する。④利用者がこの画面で入力した ID・パスワード情報は、⑤犯罪者に送信され、⑥犯罪者はその情報で金融機関にログインし不正送金を行う。

ウイルス感染に気付いていない利用者にとっては、正規のインターネットバンキングにアクセスした後に発生するため疑うことなく ID・パスワードを入力してしまい、被害に遭っている。

【図表４　不正送金ウイルスの概要】



（インターリスク総研にて作成）

さらに最近は、電子証明書を窃取するウイルスも出現している。電子証明書とは、一般的には正規利用者の PC に格納されており、インターネットバンキングを利用する端末として正当であることを証明するものである。インターネットバンキングへのログインの際に、正しい ID・パスワードを入力しても電子証明書が格納された PC でなければ認証されない。仮に犯罪者に ID・パスワードを盗まれても、正規利用者の端末以外からは送金手続きができないため、不正送金被害を防ぐ効果的な方法とされている。しかしながらこのように高いセキュリティを実現する電子証明書の窃取ウイルスが出現したことで、更なる被害拡大を招いている。

その他ウイルスとしては、PC 内の情報を抜き取るものなどがあり、PC 内に保存していたインターネットバンキングの ID・パスワードを窃取されるということも発生している。

３．不正送金への対策

不正送金対策を講じる上での最大のポイントは、正規利用者に「成りすまし」されないようにすることである。そのためには、成りすましに必要な ID・パスワード窃取の主な手口である上記２．についての対策を講じることが重要である。

対策を講じる上で参照となるものとして、全国銀行協会（以下全銀協）が本年７月に示した「法人向けインターネットバンキングにおける預金等の不正な払戻しに関する補償の考え方」（以下、「全銀協による法人補償の考え方」）が挙げられる。

これは法人の不正送金被害が急増していることを受け、「被害に対する法的責任は金融機関にはないと考えられる場合であっても、継続的なサービスの提供や金融機関の経営戦略等の観点から合理性もありうるとして、法人被害を補償するとの判断がある」との考え方に基づき公表された。

この「全銀協による法人補償の考え方」において、法人被害の補償の考え方に結び付けてセキュリティ対策事例も示されている。補償基準や補償額についてはあくまでも個別行の経営判断※としつつも、補償を受けるために企業が講じるべきセキュリティ対策事例を示している。企業にとって不正送金による被害は金銭的なものであり、被害の回復方法は、銀行による金銭的な補償が現実的である。そこで本稿では全銀協が示した補償要件ともいえるセキュリティ対策事例について、その具体例を示す。

※具体的な補償基準や補償額は金融機関毎に異なるため、各金融機関に確認が必要である

■銀行および法人のお客さまに求められるセキュリティ対策事例と具体例

（「全銀協による法人補償の考え方」別紙１の内容。銀行が講じるセキュリティ対策事例は割愛）

「法人補償の考え方」の別紙１内容		左記の具体例（インターリスク総研作成）
(1)お客さまに実施していただくセキュリティ対策		
①	銀行が導入しているセキュリティ対策の実施 上記 1.に記載のものを含め、銀行が導入しているセキュリティ対策を着実に実施していただくこと※	・取引先の金融機関からの案内は直ぐに確認し、銀行が提示する対策は確実に実施する。
②	インターネット･バンキングに使用するパソコン（以下、単に「パソコン」という。）に関し、基本ソフト(OS)やウェブブラウザ等、インストールされている各種ソフトウェアを最新の状態に更新していただくこと	・ウインドウズアップデートは自動実施にする。 ・OS やブラウザは金融機関が推奨するバージョンを使用する（必ずしも最新版とは限らない）。 ・フリーソフト等、セキュリティが担保できないソフトはインストールしない。
③	パソコンにインストールされている各種ソフトウェアで、メーカーのサポート期限が経過した基本ソフトやウェブブラウザ等の使用を止めていただくこと	・Windows XP、Microsoft Office 2003、Internet Explorer 6 は使用しない。（上記②参照）
④	パソコンにセキュリティ対策ソフトを導入するとともに、最新の状態に更新したうえで、稼動していただくこと	・市販のウイルス対策ソフトや取引先の金融機関が推奨するセキュリティ対策ソフトを導入する。 ・自動スキャン・自動更新設定とする。

		（ウイルス対策ソフト同士の競合によるトラブル発生した場合は金融機関に相談する）
⑤	インターネット･バンキングに係るパスワードを定期的に変更していただくこと	・パスワードは最低でも 3 か月に 1 回変更する。（1 か月に 1 回以上望ましい）
⑥	銀行が指定した正規の手順以外での電子証明書の利用は止めていただくこと	・電子証明書のエクスポートは不可とする。複数 PC で使用したい場合は、都度入手する。
(2)お客さまに推奨するセキュリティ対策		
①	パソコンの利用目的として､インターネット接続時の利用はインターネット･バンキングに限定していただくこと	・業務用 PC とは別にインターネットバンキング専用 PC を用意し使用する。
②	パソコンや無線 LAN のルータ等について、未利用時は可能な限り電源を切断していただくこと	・利用後は都度 PC をシャットダウン（スリープや休止は避ける）する。 ・LAN ケーブル接続の場合は帰宅時に抜いておく ・無線 LAN は使用しない。使用する場合は、アクセスポイント､wifi 機器）も未利用時は電源をシャットダウンしておく。
③	取引の申請者と承認者とで異なるパソコンを利用していただくこと	・左記のとおり（その際の電子証明書の扱いは上記(1)の⑥参照）
④	振込･払戻し等の限度額を必要な範囲内でできるだけ低く設定していただくこと	・初期値は一般に高額のため、万が一の被害を想定し、1 日の利用限度額を業務上支障のない範囲で設定する。
⑤	不審なログイン履歴や身に覚えがない取引履歴、取引通知メールがないかを定期的に確認していただくこと	・取引通知メールは､在社時以外も確認できるよう携帯電話やスマートフォン等のモバイルデバイスのアドレスも指定しておく。 ・PC アドレスの場合､他のメールに埋もれてしまわないようにする（メーラー設定で自動仕分け等を行うなど） ・ログイン履歴は必ず確認する。

※上記１．とあるのは、本稿では割愛した「銀行が講じるセキュリティ対策事例」のこと。

なお､「全銀協による法人補償の考え方」では、減額や補償せずのケースも提示しているため、同様に下記に示す。

■補償減額または補償せずの取扱いとなりうるケースについて

以下のようなケースでは､会員銀行はそれぞれの事情を個別に判断したうえで､補償を減額する、もしくは補償をしない取り扱いとすることが考えられる。

「法人補償の考え方」の別紙 2 内容		左記の具体例（インターリスク総研作成）
１．以下のような対応がお客さまに実施されていないケース		
(1)	（別紙１）２．（１）のセキュリティ対策の導入	・前頁参照
(2)	身に覚えのない残高変動や不正取引が発生した場合の、一定期間内の銀行への通報	・些細な点でもいつもと異なる不自然な点があれば、取引履歴やログイン履歴を確認し、すぐに取引先の金融機関へ連絡する。（通報期限は、10 日～30 日以内が多い。） ・取引行の緊急連絡先をすぐに参照できる場所に登録しておく。 ・可能であれば､すぐにパスワードを変更するなどし、被害の拡大に努める

(3)	不正取引が発生した場合の、一定期間内の警察への通報	・上述の取引先の金融機関への連絡と同時に警察にも連絡する。
(4)	不正取引が発生した場合の、銀行による調査および警察による捜査への協力	・警察等の事情聴取等の捜査に協力する
２.お客さまに過失があると考えられる以下のような事象が認められたケース		
(1)	正当な理由なく、他人に ID・パスワード等を回答してしまった、あるいは、安易に乱数表やトークン等を渡してしまった場合	・担当者や権限者以外には、ログインや取引に必要な情報（ID、パスワード、乱数表、秘密の質問・回答等）やトークン機器を開示しない。
(2)	パソコンや携帯電話等が盗難に遭った場合において、ID・パスワード等をパソコンや携帯電話等に保存していた場合	・上記ログインに必要な情報を紙や電子データで保存しない。 ・乱数表やトークン機器など、紙や物理媒体は、鍵のかかる場所へ保管し、不在時は施錠する。
(3)	銀行が注意喚起しているにも関わらず、注意喚起された方法で、メール型のフィッシングに騙される等、不用意に ID・パスワード等を入力してしまった場合	・電子メールの添付ファイルは信頼できるもの以外は安易に開かない。 ・ID やパスワードを権限のない第三者に絶対に伝えない。 ・取引先の金融機関の関係者を名乗るものであっても、Web 画面や電子メール、電話では絶対に入力や開示をしない。 （金融機関が ID やパスワードを個別に照会してくることは絶対にない）
３.その他、以下のような事例に相当するケース		
(1)	会社関係者の犯行であることが判明した場合	・左記のとおり。
(2)	その他、上記２.の場合と同程度の注意義務違反が認められた場合	・派遣社員やパートでも同様。 ・ログインに必要となる ID やパスワードが容易に推測できるものであったり、その取扱いや管理がずさんな場合が該当。

上記の対策は、インターネットバンキングの利用部門者に対し、なぜこうした対策が必要なのかといった初歩的な内容から教育していくことが重要である。また対策の実施は、利用部門任せにせず、情報セキュリティ担当部門や監査部門による点検や監査を実施し、実効性を確保する必要がある。

４．おわりに

金融機関各社はインターネットバンキング上の技術的なセキュリティ対策を進め、更には不正送金被害時の法人向け補償制度を整備しつつある。また警察や金融機関による啓発活動も盛んであり、企業のセキュリティやリテラシー向上が着実に進めば、不正送金による金銭的被害自体は今後減少していくことが期待される。

しかしながらインターネットに関する犯罪（サイバー犯罪）は、不正送金のように金銭そのものを狙ったものに限らない。営業秘密や個人情報など金銭的価値が高いとされる情報資産も、新たな巧妙かつ悪質な方法によって犯罪者の標的とされうることを想定しなければならない。

こうしたリスクに対処するためには、セキュリティに関する事故事例や他社の取組事例等を収集・分析することや、自社の脆弱性について評価し、対策を講じるなどの予防対策が重要となる。また万一の発生時に備え、迅速に対処できるよう危機管理態勢の整備や、専門家との連携等の対策を講じておくことが重要である。

【参考資料】

一般社団法人 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」（平成 26 年 11 月 27 日）
http://www.zenginkyo.or.jp/news/entryitems/news261127_2.pdf

一般社団法人全国銀行協会「法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方について」（平成 26 年 7 月 17 日）
http://www.zenginkyo.or.jp/news/2014/07/17174000.html

警察庁 広報資料「平成 26 年上半期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について」（平成 26 年 9 月 4 日）
http://www.npa.go.jp/cyber/pdf/H260904_banking.pdf

以上

（文責：事業リスクマネジメント部　統合リスクマネジメントグループ　上席コンサルタント　榎田 貞春　）