2020 年 1 月 29 日

サービス＆セキュリティ株式会社 e-Gate センター

急増するフィッシング被害　二要素認証突破の手口と対策

1. 概要

2020 年になり、改めて 2019 年全体を振り返りますと、国内のサイバー犯罪の傾向が変わり、従来の対策の裏をかいたサイバー攻撃が拡大していたことがわかりました。パスワードのみの認証より安全だと思われていた二要素認証が突破され、ログイン情報が盗まれる詐欺手口が確立されたことで、オンラインバンキングの不正送金被害は急増し、過去最悪の水準を記録しています。

金融庁からも不正送金事案が多発していることに関して昨年 12 月に注意喚起がされており、この傾向は今後も継続することが予測されます。身近に発生しているフィッシング詐欺の被害に遭わないためにも、その手口と対策についてご紹介いたしますので、是非ご参照ください。

2. フィッシングによるネットバンキング不正送金被害の増加

ここ最近の国内のフィッシング詐欺では、SMS やメールで通知されるワンタイムパスワードだけでなく、アプリや電話で通知されるもの、暗証カードを用いた二要素認証をも狙った攻撃が確認されています。これらの攻撃の狙いは不正送金と考えられ、ネットバンキングサイトの仕組みを模倣した巧妙な手口が用意されています。昨年は、二要素認証を破る詐欺手口が横行したことにより、図 1 の通りネットバンキングでの不正送金の被害が急増しています。昨年 5 月の弊社セキュリティニュースでも「フィッシングの最新情報および対策方法」として注意喚起を行っておりましたが、9 月以降、フィッシングメールの件数、被害額ともに顕著な増加が見られています。11 月には発生件数が 573 件、被害額は約 7 億 7,600 万円にも拡大し、発生件数、被害額ともに 2012 年以降最多の水準となっています。

【図 1】 不正送金事犯発生状況（2019 年 11 月時点）

(出典：警察庁 HP「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について」)

なかでも、フィッシング SMS を送ることでワンタイムパスワードによる二要素認証を破る手口が横行しています。フィッシング SMS のリンクから金融機関を装ったフィッシングサイトへ誘導し、ログイン情報が盗まれ不正送金される被害が増えています。

3. 二要素認証とは

ネットバンキングやショッピングサイトなどではユーザを認証する信頼性の高い仕組みが必要です。従来は ID とパスワードのみで認証する場合が多くありましたが、パスワード漏洩や不正アクセスの増加を受け、より認証を強化するために、二要素認証や多要素認証が採用されるようになってきました。

そもそも、本人を認証する際には下表の通り 3 種類の方法があります。このうち、2 種類の要素を組み合わせて認証を行うことを二要素認証と言います。例えば、知識情報である「ID・パスワード」を入力後、生体情報である「指紋」認証を行うことでログインが可能になる場合は、二要素認証を行っているということになります。

また、3 種類の要素を組み合わせることもあるため、二要素認証を包括して多要素認証と呼ぶ場合もあります。

【表 1】認証の 3 要素

認証要素	説明	例
知識	本人だけが知っている情報	ID・パスワード、秘密の質問、マトリクス認証
所有物	本人が持っている物	IC カード、トークン、ワンタイムパスワード
生体	本人の身体的特徴	指紋、虹彩、顔、静脈、網膜

このように複数の認証要素を組み合わせることでセキュリティが強化され、一時期フィッシング詐欺は落ち着いていましたが、2019 年に急増しています。これは、ワンタイムパスワードを用いた二要素認証を突破する手口が確立されたことも要因の一つとして考えられます。二要素認証を突破する手法はほかにも次々と確立されており、二要素認証だからといって安心できない状況となっています。

4. 二要素認証を破る手口

従来のフィッシングサイトは、主として ID・パスワードと両方知識情報のみの認証を突破するものでした。しかし、ここ最近の傾向では、中間者攻撃の手法によって所有物や生体情報による認証も合わせて突破しようとする、つまり二要素認証、多要素認証をも破る手口が出現しています。

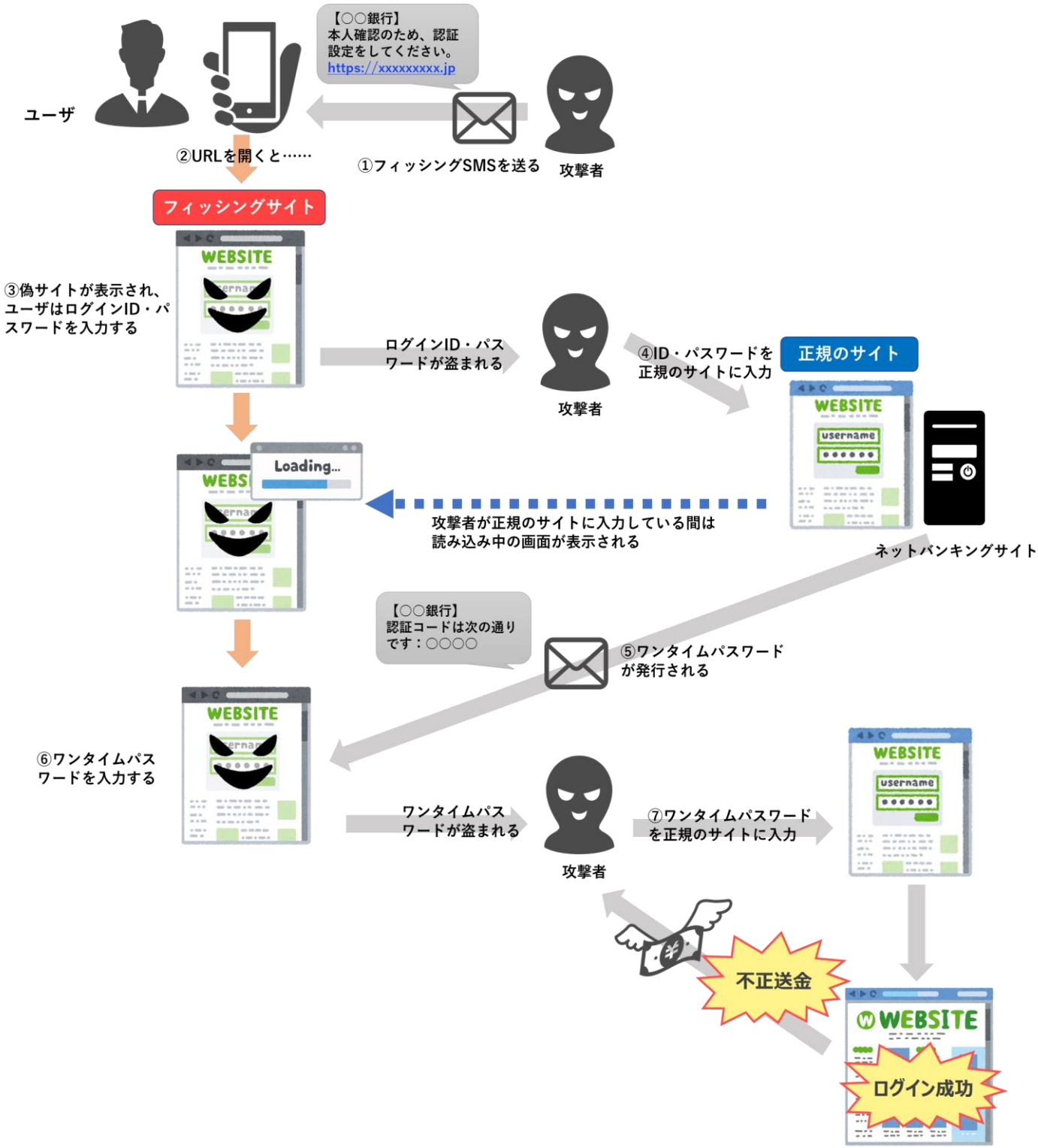
その手口に関して、3 つの例を以下に紹介いたします。

（1）フィッシング SMS を用いた中間者攻撃

模倣サイトでパスワードを詐取するだけの従来の攻撃とは違い、間に入って中間者攻撃が行われることにより、二要素認証の突破が可能となりました。その攻撃手法は下記の通りです。

①攻撃者がユーザにフィッシング SMS を送る。
②ユーザがリンクからフィッシングサイト（ネットバンキングのログイン画面など）にアクセスする。
③フィッシングサイト上で ID とパスワードを入力する。
④攻撃者はその ID とパスワードを用い、正規のサイトにアクセスする。

⑤正規のサイトからユーザにワンタイムパスワードが送られる。
⑥フィッシングサイトにもワンタイムパスワードを入力する画面が表示され、ユーザはワンタイムパスワードを入力する。
⑦攻撃者はこのワンタイムパスワードも入手し、正規のサイトに入力することでログインが可能になる。
⑧ログイン後、攻撃者は不正送金が実行できる。



【図 2】 二要素認証を突破する中間者攻撃の例

【図 3】ワンタイムパスワードの窃取画面例

（出典：一般財団法人 日本サイバー犯罪対策センター HP
「～フィッシングによる不正送金の被害が急増～」2019 年 12 月 19 日 更新）

攻撃者はリアルタイムにフィッシングを行っており、攻撃者が正規のサイトに入力している間はユーザには処理中の画面が表示されています。また、正規の手順でワンタイムパスワードが発行されているため、正規のサービス提供者側が不正に気付きにくいことも被害拡大の一因と考えられます。

一部を自動化している場合もあり、その手法を次項で説明いたします。

（２）ツールを用いた中間者攻撃サイトの自動生成

2019 年より、多要素認証をかいくぐる「Modlishka」（モディスカ）というツールが公開されました。Modlishka ではフィッシングサイトを手軽に作成・運用することができます。ユーザと正規のサイトとの間でリバースプロキシとして動作し、中間者攻撃を行います。

①正規のサイトの情報を基にフィッシングサイトを自動的に生成する。
②ユーザは生成されたフィッシングサイトに二要素認証のコードを入力する。
③そのセッションが詐取され、リアルタイムに乗っ取られる。

さらに、2019 年 6 月には「Muraena」（ムラエナ）と「NecroBrowser」（ネクロブラウザー）というツールが公開されました。Modlishka のリバースプロキシに加え、正規のサイトに合わせた設定ファイルを作成することで、正規のサイトが使用している保護手段を迂回することができます。

（３）URL やドメインの偽装

フィッシングサイトには、正規の発行元による有効な証明書が使用された HTTPS サイトが使われていることも多くなっており、アドレスバーに鍵マークが表示されていても安全とは限りません。さらに、日本のドメイン名「.jp」が使用されているケースも増えてきています。HTTPS に対応し、「.jp」を使用することで、本物のサイトだと信じ込ませるための偽装が一段と巧妙になってきています。

【図 4】巧妙なフィッシングサイトのログイン画面例

（出典：一般財団法人 日本サイバー犯罪対策センター HP
「～フィッシングによる不正送金の被害が急増～」2019 年 12 月 19 日 更新）

5. 対策

詐欺被害に遭わないようにするためには、これまで以上に最新のフィッシング手法の変化を知り、不審なメッセージに注意していく必要があります。また、フィッシングという脅威のリスクを下げるために、セキュリティソフトを必ずインストールし、最新の状態に保つことが基本となります。今回のフィッシング対策として、個人と法人向けに具体的な対策を下記に記載いたしますのでご参照ください。

【個人向け対策】

・不審な SMS やメールは開封しない
・メッセージの内容や送信元をよく確認し、メッセージに記載されている URL に安易にアクセスしない
・正しい Web サイトの URL をブックマーク登録しておき、ブックマークからアクセスするようにする
・表示された Web サイトが正しいかどうか、必ずアドレスバーの URL を確認する
・普段と異なるタイミングで二要素認証や決済情報の入力を求められた場合、その Web サイトの URL を再確認する
・認証アプリや生体認証など、別の認証方法の利用も検討する
・各銀行の Web サイトにおいて「メールでインターネットバンキングのパスワード等を求めることはない」ことなどの情報を確認する

主な注意喚起のページを下記にまとめましたのでご確認ください。また、ご自身が使用されている金融機関の情報もあわせてご確認ください。

【金融庁】

・インターネット・バンキングによる預金の不正送金事案が多発しています（2019 年 12 月 25 日 更新）
https://www.fsa.go.jp/ordinary/internet-bank_2.html

【全国銀行協会】

・ネットバンキング犯罪

https://www.zenginkyo.or.jp/hanzai/7316/

・フィッシング詐欺

https://www.zenginkyo.or.jp/hanzai/15300/

万が一、不審な Web サイトにパスワード等を入力した場合には、速やかに各銀行の問い合わせ窓口等へご相談ください。

【法人向け対策】

・自社サイトで使用しているシステムに脆弱性や設定ミスがないか定期的に確認する

確認には専門家の知識が必要なため、脆弱性診断サービスのご利用を推奨いたします。

脆弱性診断サービスでは、定期的に Web サイトやプラットフォームの脆弱性を調査することで、システムが古いバージョンのままの利用や、サーバの設定ミスなど様々な課題を洗い出すことができます。それらの課題に対処することで、不正アクセスや情報漏洩などセキュリティインシデントの発生リスクを減らすことができます。

・自社サイトに実在証明拡張型（EV）証明書を使用する

EV 証明書は、DV（ドメイン認証型）や OV（実在証明型）よりも厳格な審査を受けて発行されます。アドレスバーに組織情報が表示されるようになり、正規のサイトであることが証明されるため、偽サイトと差別化されます。

・不審なサイトへのアクセスがないか、セキュリティ製品を導入して監視する

セキュリティ製品を導入し Proxy や URL フィルタリング機能の監視を行う、また監視サービスを利用することで不審なサイトへのアクセスをリアルタイムに検知することが可能です。不審なサイトにアクセスしたクライアントを特定することができ、被害拡大を防ぐことができます。

・社内教育や周知の徹底

社内でフィッシング詐欺の手口を周知させ、騙されないよう教育を徹底することで、詐欺被害を未然に防ぐことができます。

近年、「FIDO（ファイド、Fast Identity Online の略）」というパスワードを必要としない新たな認証方式が注目を集めています。FIDO 認証はデバイス側で行う生体情報を用いた本人認証とサーバ側で行うデバイスの認証を分けています。本人認証に関してサーバに伝わるのは「本人である」という情報のみのため、認証情報が詐取されるリスクがなく、よりセキュリティの高い認証方式として注目されています。このような新しく、よりセキュアな認証方式を取り入れることも対策の一つとして考えられます。

6. 参考情報

・ScanNetSecurity

二要素認証の突破や SMS へのメッセージ混入--2019 年サイバー犯罪総括（トレンドマイクロ）

https://scan.netsecurity.ne.jp/article/2020/01/10/43512.html

・ITmedia NEWS

「過去最悪の水準」 ネットバンク不正送金、急増の理由　破られた“多要素認証の壁”

https://www.itmedia.co.jp/news/articles/1912/27/news018.html

・警視庁

フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（全銀協等と連携した注意喚起）

http://www.npa.go.jp/cyber/policy/caution1910.html

・一般財団法人 日本サイバー犯罪対策センター

～フィッシングによる不正送金の被害が急増～

https://www.jc3.or.jp/topics/banking/phishing.html

・TrustLogin

多要素認証の種類と方法

https://trustlogin.com/wp/trustlogin_whitepaper02.pdf

・Trend Micro

国内ネットバンキングの二要素認証を狙うフィッシングが激化

https://blog.trendmicro.co.jp/archives/22696

7. e-Gate のサービスについて

上記のフィッシング詐欺対策を行ったうえで、よりセキュリティ対策を強固にするために、”e-Gate”の MSS や脆弱性診断サービスの導入を是非ご検討ください。

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。“e-Gate“のセキュリティ監視サービスをご活用頂きますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、診断の結果、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター“この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
リンク先のコンテンツは予告なく、変更、削除される場合があります。

※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»

サービス＆セキュリティ株式会社

〒150-0011

東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F

TEL 03-3499-2077

FAX 03-5464-9977

sales@ssk-kan.co.jp