2019 年 5 月 30 日

サービス＆セキュリティ株式会社 e-Gate センター

フィッシングの最新情報および対策方法

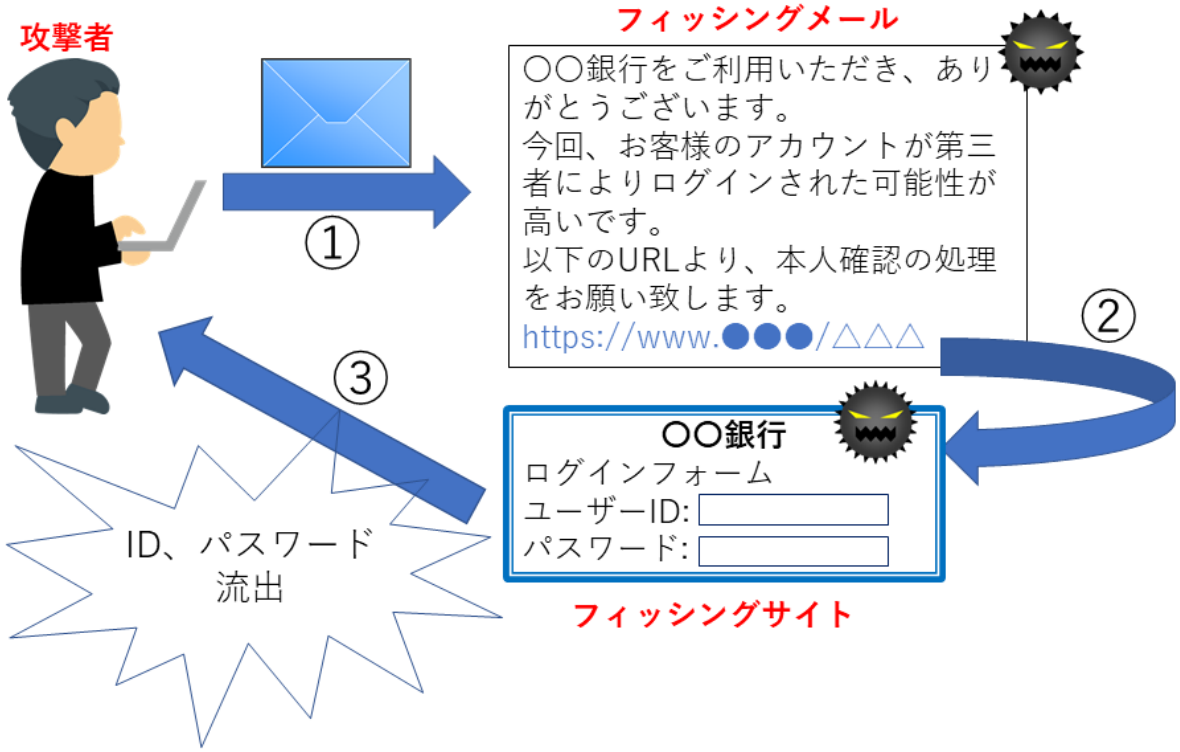
1. はじめに

フィッシングとは、金融機関や有名企業をかたったメール（フィッシングメール）などから、攻撃者が用意した本物そっくりの WEB サイト（フィッシングサイト）へと誘導し、そこでクレジット番号やパスワードを入力させ、個人情報を奪うことを目的とした攻撃です。フィッシングは以前から存在する手口ですが、フィッシング対策協議会に 2019 年 4 月までに寄せられたフィッシング報告件数（海外含む）によると、2019 年に入ってからの報告数は右肩上がりとなっています。これまでにも注意喚起は行われてきましたが、近年はフィッシングメールやフィッシングサイトがオリジナルと見分けが付かないほど巧妙に作られており、見極めるのが難しくなっています。

そこで本記事では、フィッシング攻撃の基本から、最新の手口、フィッシングを回避するために気を付けるべきポイントをご紹介いたします。

2. フィッシングの概要

2.1. 攻撃の流れ



【図 1 フィッシング攻撃の流れ】

① フィッシングサイトにアクセスさせる契機にはメールが主に使われます。「Google」や「Apple」、最近では「LINE」や「メルカリ」など老若男女が利用する有名なサービスをかたり、「アカウント更新のためログインしてください」や「不正ログインが検出されたため確認のためログインしてください」といった文面と共に、フィッシングサイトへの URL やアクセスするボタンを配置しています。メールの文面は、文法的に誤りがあったり、誤字脱字が見受けられたりすることもありますが、本物と見分けが付かないくらい作りこまれているものも中には存在します。

② URL をクリックすると、フィッシングサイトへと誘導されます。メールと同様、本物と見分けがつかないものもあり、注意していないといつも通りログインフォームに ID とパスワードを入力し、ログインボタンを押してしまいます。

③ ログインボタンを押すと、フィッシングサイトを設置した悪意のある者に ID とパスワードが知られてしまいます。いわゆる個人情報の流出です。

2.2. 最新手口の特徴

① フィッシングサイトの HTTPS 対応

一昔前までは、オリジナルサイトは HTTPS に対応しているものの、フィッシングサイトは HTTP のままであるといった場合が多かったため、HTTPS ならばフィッシングサイトではないと判断するケースがありました。しかし、現在では約半数のフィッシングサイトが HTTPS に対応しています。HTTPS だからといって真正なサイトであると判断するのは、非常に危ういことだと言えます。

② フィッシングサイトおよびフィッシングメールの本物度が格段に向上

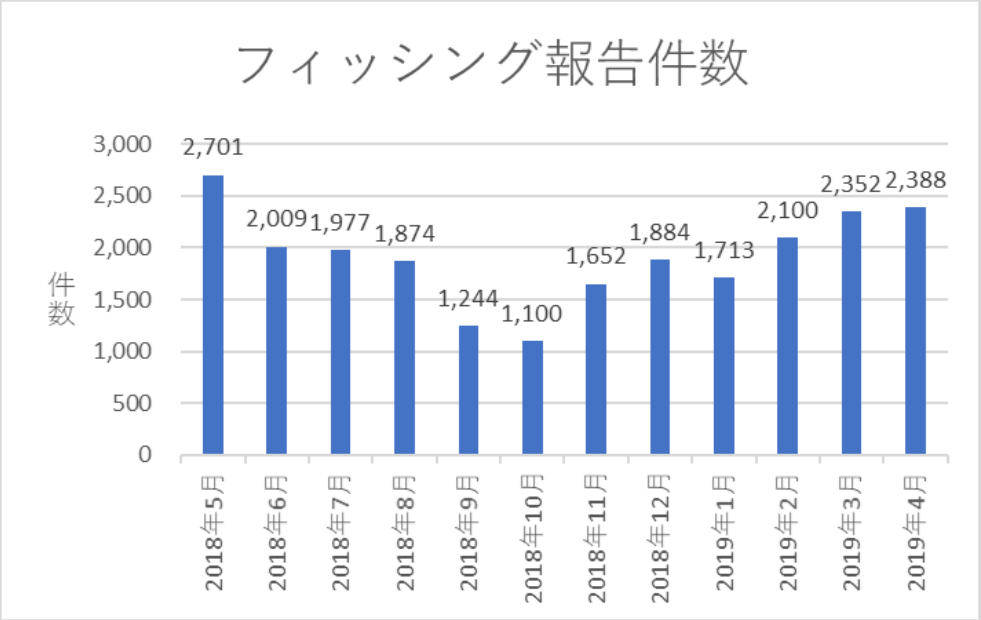
本物と見分けがつかないフィッシングメールやフィッシングサイトが存在します。以前は不自然な日本語の文面や、デザインの違和感などで怪しいと思えることもありましたが、そのような判断はできない場合が多くなってきています。

③ スミッシング

SMS+フィッシングの造語で、スマートフォンなどの携帯端末で用いられる SMS（ショートメッセージサービス）に有名企業をかたったメッセージを送る手法です。PC だけではなくスマートフォンにおいても、フィッシングの被害にあう可能性は十分にあります。また、スマートフォンやタブレットでは、アップデートを促す文面で不正なアプリをインストールさせるといった手口も見られるようになっています。

2.3. フィッシングの件数

フィッシング対策協議会に寄せられたフィッシング報告件数（図 2）を見ていただくと、2018 年 10 月までは下降していましたが、以降ほぼ右肩上がりとなっていることがわかります。よって、今後も増加することが予想されますので、ますますの対策や意識付けが必要です。



【図 2 2019 年 4 月にフィッシング対策協議会に寄せられたフィッシング報告件数 (海外含む)】

3. 対策方法

3.1. メールが来たときに注意すべきこと

- **メールから直接 WEB サイトにアクセスしないようにする**

  メールで重要な情報を伝え WEB サイトへのアクセスを促す場合、その情報はメールだけでなく WEB サイトにも書かれていることがほとんどです。常にフィッシングであるかどうか疑いの目を向け、メールのリンクからではなく、ブックマークや検索サイトから当該 WEB サイトにアクセスすることが重要です。なお、メールに記載されている URL と実際のリンク先の URL を異なるものに偽装することは簡単にできます。そのため、メールの URL を目視で真正な WEB サイトの URL であると判断したとしても、アクセスするのは大変危険です。

- **「重要」「緊急」などの急かす文言に焦らない**

  フィッシングメールは「重要」「緊急」などの、利用者に早急な対応を迫る文言を件名や本文に入れていることが多いです。このような文言のメールを受信したとしても、前述したようにメールから直接 WEB サイトにアクセスしないようにするなど、冷静な対処を心がけましょう。

- **電子署名の確認**

  多くの金融機関などでは、送信元が正規の事業者であることを証明するため、電子メールに電子署名を付与しています。怪しいメールが送られてきた場合、電子署名を確認することも対策になり得ます。

3.2. 普段のセキュリティ対策

- **セキュリティソフトの有効化、最新版への継続的なアップデート**

  セキュリティソフトの中には、怪しい WEB サイトへのアクセスをブロックするものもあります。パターン定義を最新に保ち、新しく登場するフィッシングサイトへのアクセスをブロックできるようにしましょう。

➢ **同じパスワードを別のサービスで使い回さない**

万一パスワードが流出した場合、ほかのサービスでも同じパスワードを使っていると流出したパスワードでログインされ、被害がさらに大きくなります。

3.3. セキュリティ機器の導入、監視

➢ **WEB プロキシアプライアンス、IPS などを導入し、不審なサイトへのアクセスを監視、ブロックする**

プロキシや IPS は通信を監視するネットワーク機器です。怪しい WEB サイト一覧のデータベースを持ち、パケットに含まれるアクセス先の URL を検査し、データベースに一致するとアラートを発報したり、通信を遮断したりする機能を持っています。これらの機器を導入し、適切に運用及び監視することにより、重要な情報の流出や被害の拡大を抑えることができます。

4. e-Gate の監視サービスについて

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うことが重要です。“e-Gate“の 24 時間 365 日有人監視体制のセキュリティ監視サービスをご活用頂きますと、最新の分析システムを活用し精度の高い検知、専任のアナリストによる分析、迅速なセキュリティインシデント対応支援でセキュリティ対策を強化することが可能です。“e-Gate”の MSS の導入をぜひご検討ください。

■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で構築した次世代 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”サービスです。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/

5. 参考情報

■ フィッシング対策協議会

https://www.antiphishing.jp/

«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