News Release

報道各位

2020 年 3 月 26 日

トビラシステムズ株式会社

「迷惑 SMS フィルター」がフィッシング詐欺の恐れがある SMS を 99%検知

そのワンタイムパスワードは本物？キャッシュレス社会を狙う詐欺手口が急増

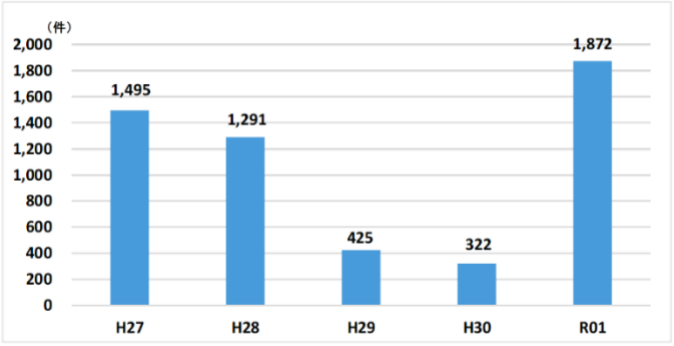
ショートメール（SMS）に添付した URL から詐欺サイトに誘導して個人情報を盗み出し、金を騙し取る「フィッシング詐欺」が後を絶ちません。当社がモバイル向けに提供する迷惑 SMS フィルターサービスは、詐欺の特徴がある本文情報や危険 URL を自動で検知し、被害を未然に防ぎます。2020 年３月現在、**当サービスは検知率 99%の精度で詐欺の恐れがある SMS をフィルタリング可能**です（注１）。

１．SMS を狙った詐欺、二段階認証も突破

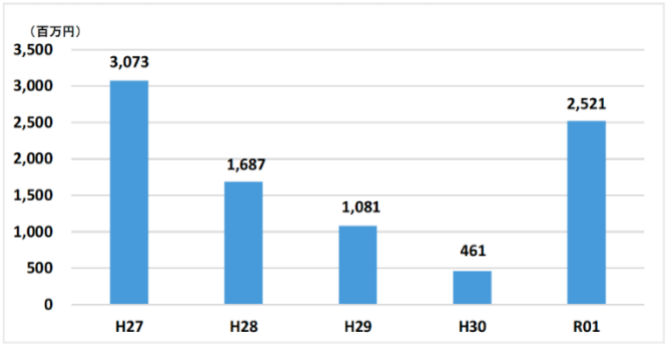
フィンテックやネット通販の進展に伴い、口座振込等の銀行サービス、キャッシュレス決済、宅配便の再配達依頼などがインターネットで行えるようになりました。利便性が高まった一方、これらのネットサービスの普及に乗じて、新たな詐欺手口が増えているのも事実です。

また、フィッシング SMS によって個人情報が盗まれ、知らぬ間にネットバンキングの口座から不正送金される被害が急増しています。警察庁によると、ネットバンキングに係る不正送金事犯は 2019 年９月頃から急増し、2019 年の被害発生件数は過去最多に次ぐ 1,872 件、被害額は約 25 億 2,100 万円と、非常に深刻な状況です（注２）。

【図表11　インターネットバンキングに係る不正送金事犯の発生件数の推移】



【図表12　インターネットバンキングに係る不正送金事犯の被害額の推移】



グラフ出典元：警察庁「令和元年におけるサイバー空間をめぐる脅威の情勢等について（令和2年3月5日発表）」

フィッシング詐欺の中には、SMS に届くワンタイムパスワード、いわゆる二段階認証を悪用した手口も見られます。二段階認証を使用したログインは、固定パスワードのみのログインよりも安全性が高いと認知され導入が進んでいます。しかし昨今、二段階認証のワンタイムパスワードが SMS に届く点を利用して、安全なはずの認証方法を突破する巧妙な詐欺 SMS が横行しています。例えば、「SMS にワンタイムパスワードが届いたので、二段階認証が有効になっている」と思い込ませることで、利用者は気付かないうちに偽サイトにワンタイムパスワードを入力し、犯人側に不正ログインを許してしまうケースが発生しています。情報漏洩を防ぐためには、SMS に添付されたフィッ

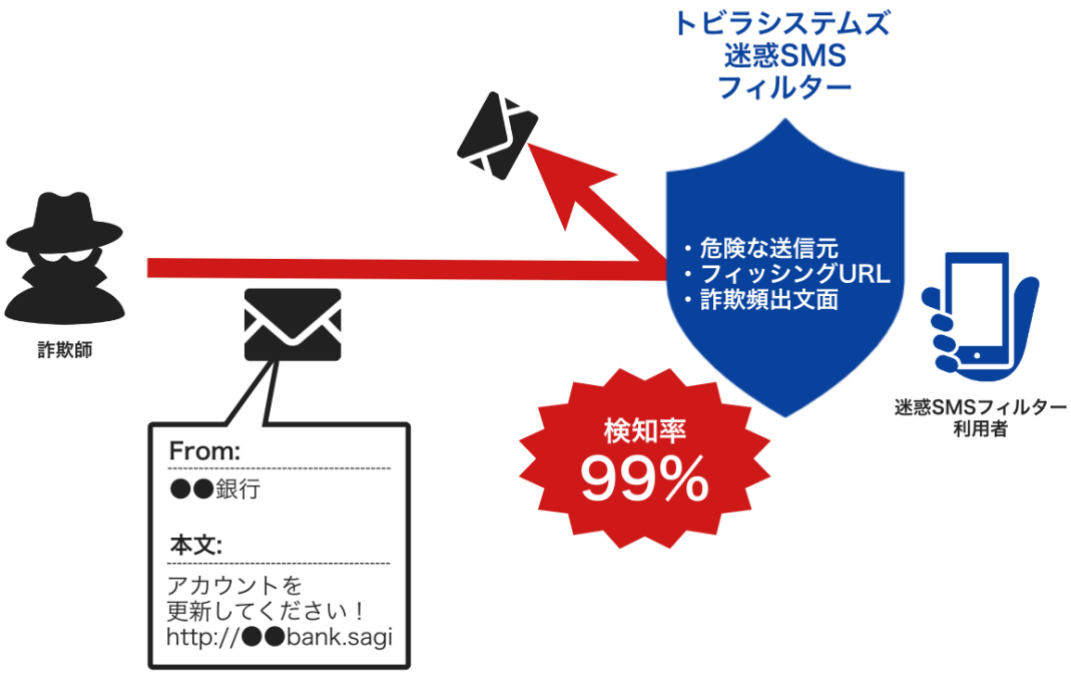
シング URL を誤ってクリックしないことが重要です。

２．検知率 99%の SMS フィルターで、フィッシング詐欺対策を

当社では、詐欺の可能性がある送信元や本文情報、URL などを、独自のアルゴリズムによってパターン抽出し、さらに技術者による社内調査を経てデータベース化し、「迷惑 SMS フィルター」サービスとして提供しております。

当サービス利用者のもとに詐欺の恐れがある SMS が届くと、「迷惑 SMS フィルター」が危険を検知し、自動で警告表示や迷惑メッセージフォルダ振り分けを行います。これにより、利用者が危険な SMS を開封したり、フィッシング URL を誤ってクリックするのを未然に防ぎます。当社の調査によると、**当社モバイルサービス利用者宛てに送信された詐欺の恐れがある SMS のうち 99%を検知**しております（注３）。

詐欺SMSフィルタリングのイメージ



モバイルキャリアにおいても、基本的な迷惑 SMS 対策機能は提供されていますが、フィルタリングの対象は海外送信元や特定の事業者、利用者自らが拒否設定した送信元などに限定されています。また、この場合フィルタリング対象は一括して拒否されてしまうため、正規に利用している海外サービスの二段階認証 SMS や、他社のモバイルキャリアを使用する家族や知人からの SMS など、利用者にとっては必要な SMS までフィルタリングされてしまう可能性があります。モバイルキャリア標準の迷惑 SMS 対策機能のみで、詐欺の恐れがある SMS をフィルタリングするのは困難な状況です。

そこで、当社の「迷惑 SMS フィルター」をご利用いただくことで、詐欺の可能性がある送信元や SMS に含まれる危険度の高い定型文、偽サイトの URL などを検知し、不特定多数に送信される詐欺の恐れがある SMS のフィルタリングが可能となります。当社のサービスをお使いいただくことで、よ

り効果的な詐欺 SMS 対策を行っていただけます。

当社ではこれまでに、以下のようなフィッシング SMS を検知しています。
・宅配業者を装って偽サイトへと誘導する URL を送り、個人情報を盗み出す。
・新型コロナウイルス感染症拡大に乗じて「マスクを配布する」などの文章とともに偽サイトの URL を添付し、個人情報を盗み出す。
・キャッシュレス決済サービスや金融機関を装って「アカウントの更新が必要」などの文章とともに偽サイトの URL を送り、個人情報を盗み出して不正送金などを行う。

＜過去の関連記事＞
https://tobila.com/news/release/p447/

各通信キャリアのオプションパック加入者は、追加料金無しで迷惑 SMS フィルターサービスをご利用いただける可能性があります。大切な個人情報をフィッシング詐欺から守るため、ぜひ防犯対策を実践してください。
当社製品に関しては、下記サイトをご確認ください。
https://tobilaphone.com/

（注１）詐欺の恐れがある SMS とは、犯行に関連可能性がある送信元やフィッシング URL、フィッシング詐欺に頻出する文面情報などを特徴に持つ SMS を指します。

（注２）警察庁「令和元年におけるサイバー空間をめぐる脅威の情勢等について（令和２年３月５日発表）」（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_cyber_jousei.pdf）

（注３）当社の迷惑 SMS データベースは、警察や外部専門機関、パートナー企業、当社サービス利用者などから提供されるフィッシング URL や本文情報、さらに当社の独自調査によって収集した情報をパターン抽出し、構築されております。詐欺の恐れがある SMS の検知率は、当データベースに同一または類似の特徴を持つ SMS の件数（分母）のうち、当社の迷惑 SMS フィルターが自動で検知した件数（分子）の割合を表します。今回発表の検知率は、2020 年２月 22 日～2020 年３月 22 日の集計値となります。

３．本件に関するお問い合わせ先

トビラシステムズ株式会社
管理部広報主任 岩渕
〒460-0003 愛知県名古屋市中区錦２丁目 5-12 パシフィックスクエア名古屋錦７F
IR 代表 TEL：050-3646-3020
代表 FAX：052-253-7692
URL：https://tobila.com/