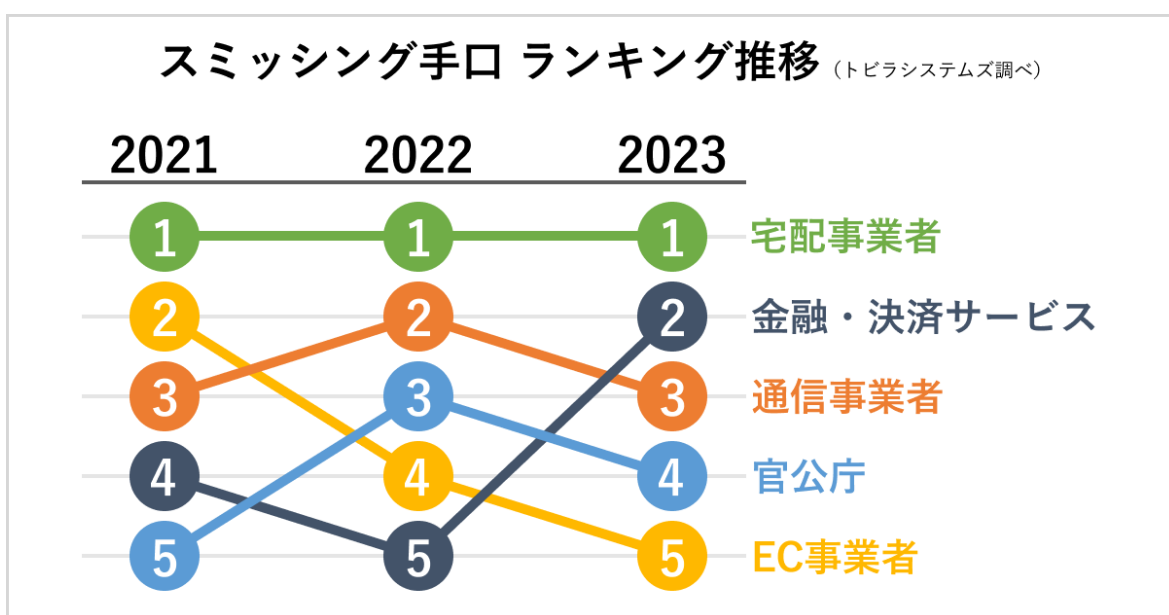
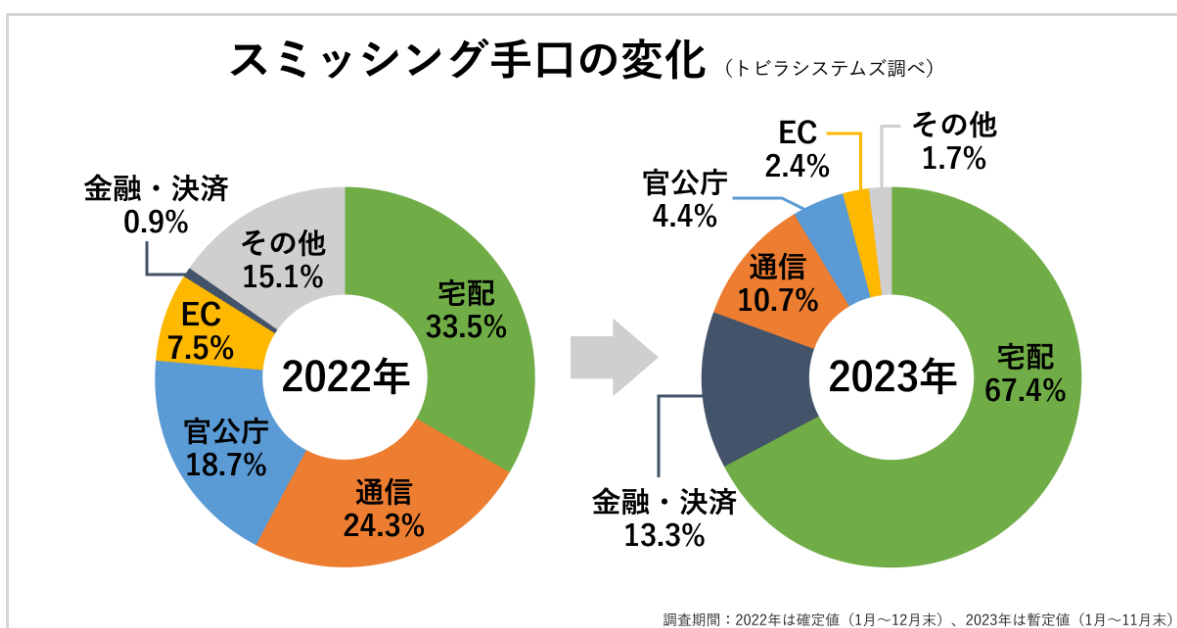


ワードマップに登場する単語は、トビラシステムズの調査において、2023年にスミッシングの文面で頻出した単語です。文面に多く使われた単語ほど、大きく表示されています。

2023年は宅配事業者をかたる手口に関連する単語が大きなトレンドとなりました。また、金融・決済サービスを連想させる単語や企業名・ブランド名なども多く確認されました。ワードマップを参考に、スミッシング対策にお役立てください。

■スミッシング手口1位は宅配事業者。金融・決済サービスは急上昇2位に

トビラシステムズの調査で、2023年に最も多く確認されたスミッシング手口の割合について、1位は宅配事業者、2位は金融・決済サービス、3位は通信事業者をかたる手口となりました。



■2023 年のスミッシング三大手口を解説

トビラシシステムズの調査で確認された、2023 年に発生したスミッシングで特に多かった 3 つの手口について解説します。

1 位：宅配事業者をかたる手口

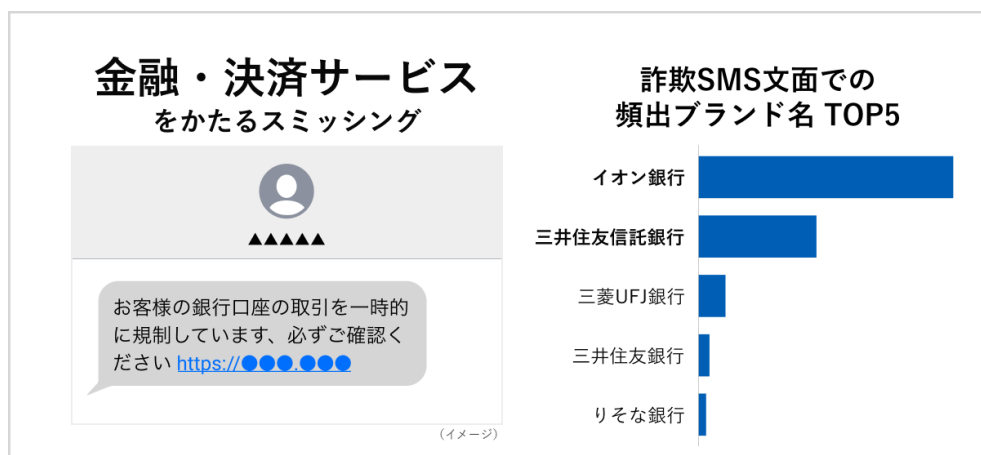
宅配事業者をかたる手口が 3 年連続で 1 位となりました。コロナ禍を契機にネット通販や宅配サービスの利用がより浸透したことから、宅配便の不在通知などを装う詐欺 SMS に引き続き注意が必要です。

詐欺 SMS に添付された URL から偽アプリのインストールに誘導し、被害者の端末をマルウェア（不正なソフトウェア）に感染させ踏み台にすることで、大量の詐欺 SMS を送信するよう仕向ける「ばらまき型」の手口も目立っています。



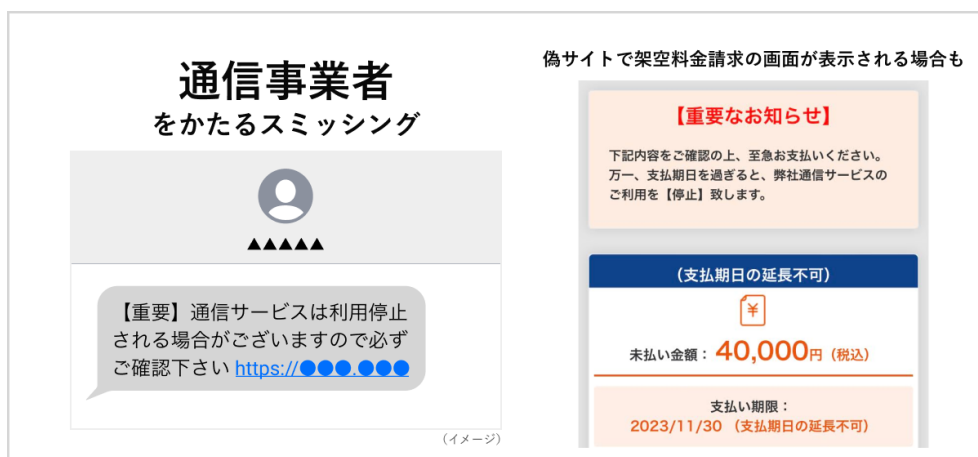
2 位：金融・決済サービスをかたる手口

金融・決済サービスをかたる手口が前年から 3 ランクアップし、2 位となりました。実在する企業やブランドの名前を悪用したスミッシングが多く、**2023 年は新たに 15 種類のブランドが出現**しました。2023 年は「イオン銀行」「三井住友信託銀行」「三菱 UFJ 銀行」「三井住友銀行」「りそな銀行」などの銀行をかたる手口が目立ったほか、「PayPay」など QR コード決済サービスをかたる手口も発生しています。



3位：通信事業者をかたる手口

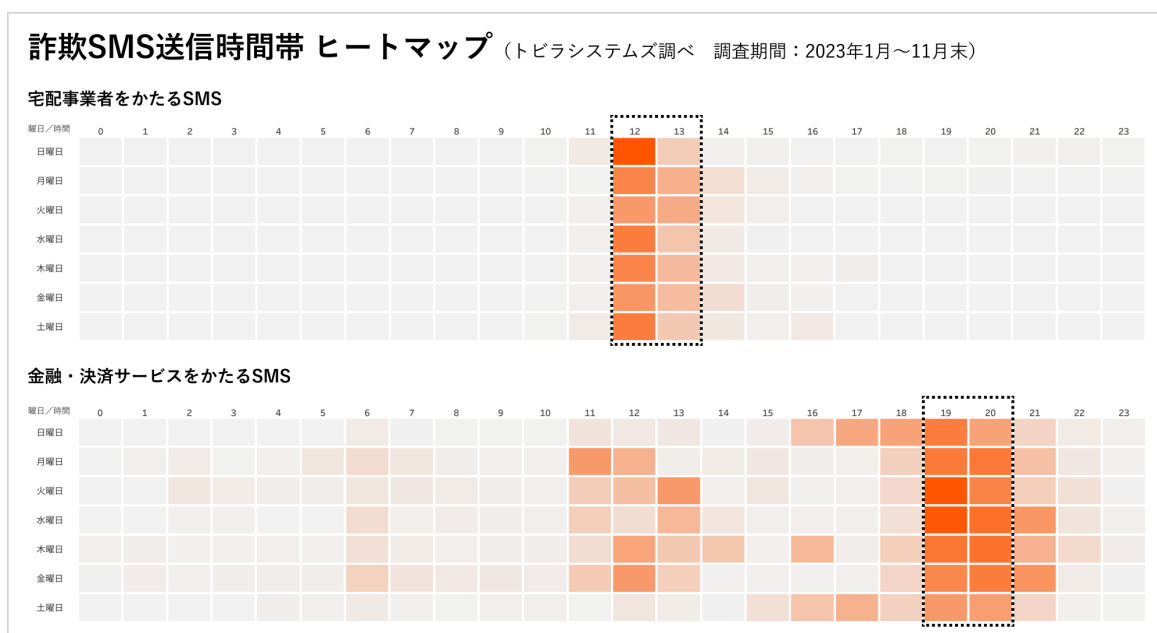
未納料金やアカウント不正利用など緊急を装って文面の URL をクリックさせ、フィッシングサイトに誘導します。偽サイトで個人情報盗み取るほか、通信事業者が提供するセキュリティアプリに似せた偽アプリ（マルウェア）をインストールさせ、感染した端末を踏み台に詐欺 SMS を大量送信させる「ばらまき型」も多発しています。また、未納料金に関する偽サイトに誘導し、プリペイドカード等で支払わせる「**架空料金請求型**」の手口も発生しています。



■詐欺 SMS が増える時間帯はスマホをよく見る「12 時～13 時」「19 時～20 時」

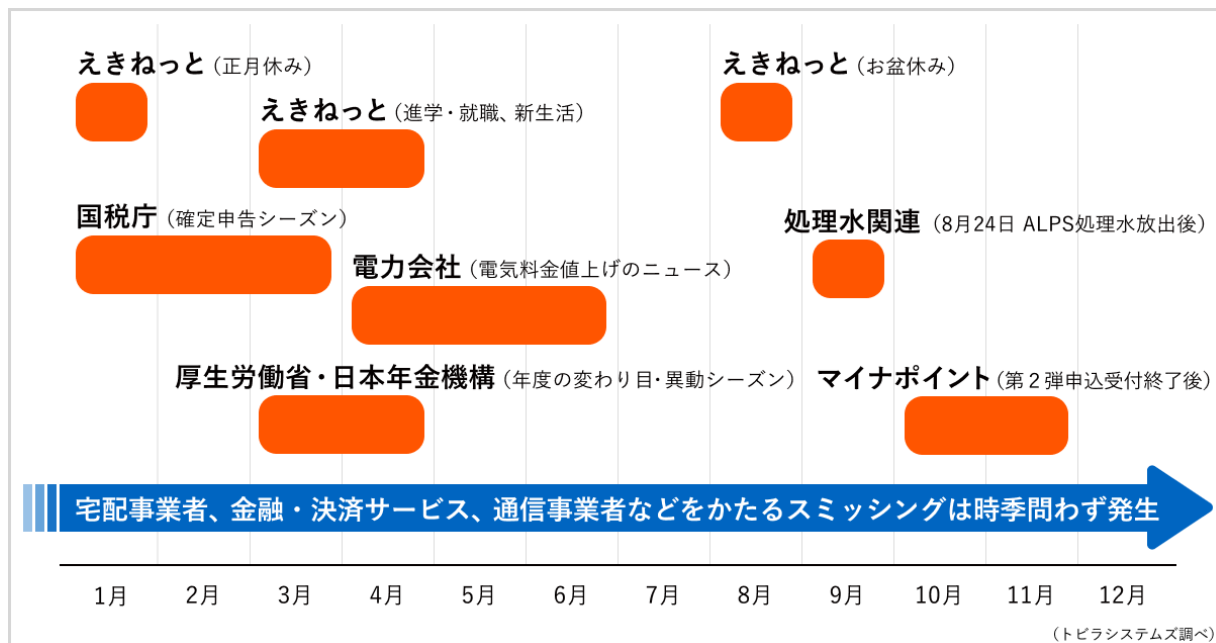
1 位の宅配事業者をかたる SMS と、2 位の金融・決済サービスをかたる SMS が送信される曜日・時間帯をヒートマップにして比較しました。

宅配事業者をかたる SMS は**昼の 12 時～13 時頃**、金融・決済サービスをかたる SMS は**夜の 19～20 時頃**に送信が目立っています。食事時間、仕事や学校の休憩時間、リラックスして過ごすタイミングなど、スマートフォンを見る機会が増えやすい時間帯に、詐欺 SMS が多く送信されていることがわかります。



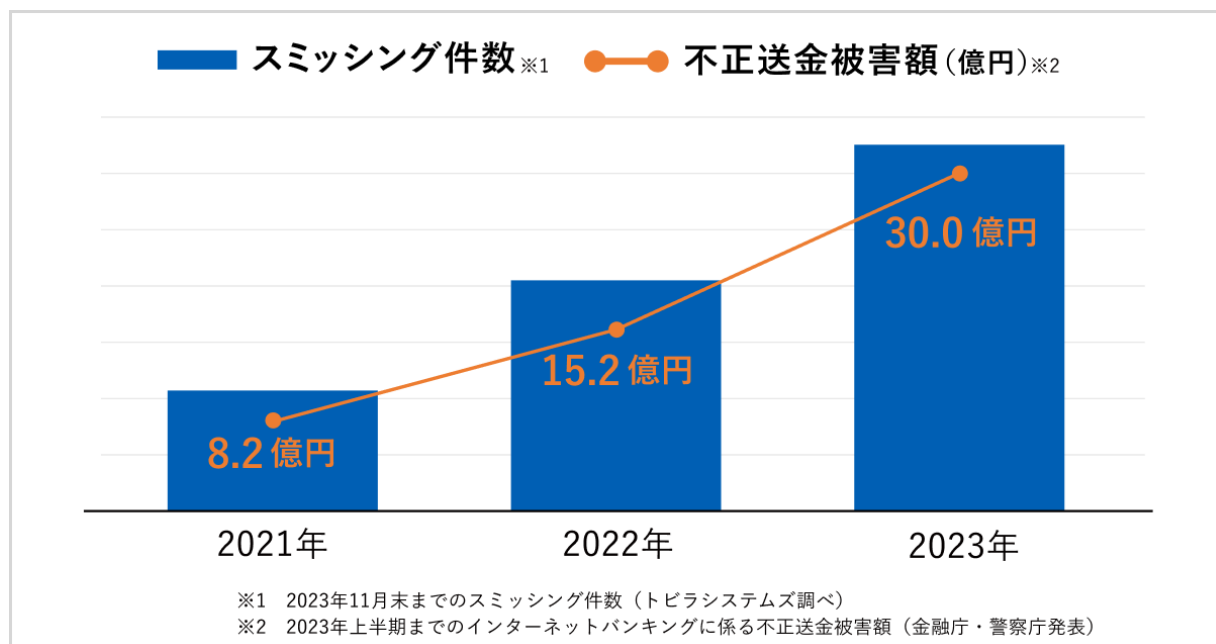
■カレンダーで振り返るスミッシング 2023、帰省ラッシュや「処理水」便乗も

時節的な話題や社会的な出来事・ニュースなどに便乗したスミッシングも発生しています。



■スミッシング件数は前年同期比 1.8 倍に増加、不正送金被害額 30 億円

トビラシステムズの調査で、2023 年 1 月～11 月に確認されたスミッシングの件数は、前年同期比で **1.8 倍に増加**しています。また、警察庁と金融庁が発表した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額は、2023 年上半期において **30 億円**に上っています (※)。



(※) 警察庁・金融庁発表「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 (注意喚起)」 (https://www.fsa.go.jp/ordinary/internet-bank_2.html)

■年末年始のスミッシング対策、家族や友人にも注意喚起を

不審な SMS から偽サイトにアクセスしてしまった場合、個人情報盗み取られたり、不正アプリのインストールにより端末がマルウェアに感染したりする恐れがあります。

よく利用するサービスのブランド名が記載された SMS が届いた場合も、フィッシング詐欺の可能性を疑い、文面上の URL に直接触らず、公式アプリやあらかじめブックマークしたサイトのマイページ等から情報を確認するなど対策を心がけてください。

スミッシング被害を防ぐため、自衛することはもちろん、年末年始に家族や友人など周りの方にも注意喚起をするなどし、対策を行ってください。

<スミッシング被害を防ぐ3つの対策>

- 身に覚えのないメールや SMS が届いた場合、文面に添付された URL に触らない
- 日頃利用するサービスは、公式アプリやブックマークしたサイトから情報を確認
- 迷惑 SMS 対策サービスを活用し、フィッシング詐欺などの不審な SMS を自動で遮断



■トビラシステムズについて



テクノロジーで社会課題の解決を目指し、特殊詐欺やフィッシング詐欺、グレーゾーン犯罪撲滅のためのサービスを提供しています。詐欺電話・詐欺 SMS 等の情報を収集・調査してデータベースを構築し、自動でフィルタリングする「迷惑情報フィルタサービス」は、固定電話、モバイル、ビジネス向けに展開し月間 1,500 万人以上にご利用いただいています。

公式サイト：

<https://tobila.com/>

■本件に関する報道関係のお問い合わせ先

トビラシステムズ株式会社

〒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 7 F

担当：管理部 広報 岩渕

TEL：050-3646-6670（直通）

FAX：052-253-7692

URL：<https://tobila.com/>