

8 月度ネット詐欺レポート

官公庁系の詐欺サイトが増加、USJ の当選詐欺サイトにも 注意

ネット詐欺レポートは毎月調査・収集した詐欺サイトを分析し、傾向をまとめたレポートです。

目次：

- 国税庁、総務省のフィッシングサイトが増加
- USJ 当選詐欺サイトが急増、Android マルウェアにも注意
- フィッシングサイトブランドランキング
- フィッシングサイトカテゴリ別構成比
- フィッシング詐欺被害防止のポイント
- サイトを無料診断「詐欺サイトチェッカー」
- 森 達哉教授のコメント

■国税庁、総務省のフィッシングサイトが増加

8 月は、国税庁や総務省などの官公庁を騙るフィッシングサイトが急増しています。

国税庁を騙るフィッシングでは、e-Tax の認証情報を詐取する手口が増加しています。8 月は個人事業者の消費税・地方消費税の中間申告・納付時期にあたり、e-Tax を利用する機会が増えることから、こうした時期を狙っている可能性があります。

総務省を騙るフィッシングでは「労働力調査」を装った手口が急増しています。これまでは「国勢調査」を装ったフィッシングが中心でしたが、同様の手口が「労働力調査」にも使われている可能性があります。

労働力調査は毎月実施されており、国勢調査と同様に法律上の回答義務があります。また、回答を拒否したり虚偽の回答をしたりした場合には、50 万円以下の罰金が定められています。攻撃者はこうした制度を悪用し、「回答義務」や「罰則」を強調することで利用者の不安を煽り、偽サイトへ誘導していると考えられます。なお、実際の労働力調査は、調査員が対象世帯を訪問して調査書類を配布する仕組みです。突然届いたメールや SMS で回答を求め、リンク先へ誘導するような連絡には十分注意してください。



国税庁のフィッシングサイト



労働力調査の詐欺サイト

※画像は詐欺・危険サイトのイメージであり、本文内容とは関係ありません。

国税庁：不審なメールや電話にご注意ください

<https://www.nta.go.jp/information/attention/attention.htm>

総務省：労働力調査を騙る不審メールについて

https://www.e-survey.go.jp/survey_Infoation/1771

■USJ 当選詐欺サイトが急増、Android マルウェアにも注意

8 月から 9 月にかけて、三井住友カード・VJA 主催の「ユニバーサル・スタジオ・ジャパン貸切ご招待&キャッシュバックキャンペーン」を悪用したフィッシングサイトが確認されています。

「キャンペーンに当選しました」などのメッセージで偽サイトへ誘導し、認証情報などを詐取する手口です。キャンペーンの公式サイトでは、当選通知メール等でクレジットカード番号などの個人情報を確認することはないとしており、キャンペーンの当選をうたう不審なメールへの注意を呼びかけています。

また 9 月に入り、正規のアプリストアを装った偽サイトから、不正な Android アプリをインストールさせる手口も急増しています。

「ポイントを受け取るためにアプリのインストールが必要」などと案内し、利用者の端末に不正なアプリをインストールさせる手口です。楽天や Amazon など、さまざまな有名ブランドを騙った偽サイトが確認されており、ポイント付与やキャンペーンを口実にアプリのインストールを求められた場合は注意が必要です。アプリをインストールする際は、メールや SMS などに記載されたリンクを利用せず、Google Play などの正規のアプリストアから入手することが重要です。



USJ 当選のフィッシングサイト



不正 Android インストールサイト

※画像は詐欺・危険サイトのイメージであり、本文内容とは関係ありません。

■フィッシングサイトブランドランキング

8 月は、国税庁を騙るフィッシングサイトが最も多く確認されました。

また、9 位には Vpass がランクインしています。これは、USJ 当選を装ったフィッシングサイトが増加したことが主な要因と考えられます。そのほか、前月に引き続き ANA やえきねっとなど、夏休みの旅行・帰省需要に便乗したフィッシングも上位にランクインしています。8 月は、税金の納付時期やキャンペーン、夏休みの旅行需要など、季節のイベントや利用者の関心が高まるタイミングに便乗したフィッシングが目立ちました。

	2026年7月	割合	2026年8月	割合
1	三井住友カード	12.69%	国税庁	12.50%
2	JCB	8.35%	Amazon	9.24%
3	LINE	7.09%	総務省	8.82%
4	えきねっと	6.27%	Apple	8.34%
5	Amazon	6.21%	三井住友カード	6.93%
6	イープラス	5.87%	ANA	6.13%
7	Apple	5.35%	えきねっと	4.00%
8	SAISON CARD	4.53%	イープラス	3.52%
9	ETC利用照会サービス	2.94%	Vpass	3.45%
10	国税庁	2.66%	SAISON CARD	3.39%

■フィッシングサイトカテゴリ別構成比

8月度は、官公庁のフィッシングの割合が17ポイント以上増加しています。これは、国税庁や総務省を騙るフィッシングが増加したことによるものです。

	2026年7月	2026年8月	
 銀行	2.91%	4.80%	➡
 携帯キャリア	1.01%	0.33%	➡
 クラウドサービス	0.00%	0.02%	➡
 消費者金融 キャッシング	0.00%	0.14%	➡
 クレジット カード	33.24%	20.57%	➡
 ECサイト	10.12%	10.15%	➡
 ポータルサイト	2.05%	0.57%	➡
 プロバイダー	1.31%	1.15%	➡

	2026年7月	2026年8月	
 官公庁	6.39%	24.28%	
 株 / 証券	0.24%	0.77%	
 SNS	8.81%	1.62%	
 仮想通貨	0.70%	0.23%	
 Webメール	0.12%	0.05%	
 Webメール ユーザー	0.00%	0.00%	
 Webサービス	31.93%	33.73%	
その他	1.17%	1.59%	

※5 ポイント以上上昇したカテゴリは赤色の矢印になります。

※5 ポイント以上減少したカテゴリは黄色の矢印になります。

■フィッシング詐欺被害防止のポイント

1. メールや SMS で案内された URL が正規の URL か確認する

メールや SMS メッセージ上のリンクはクリックせず、事前に登録しておいたブックマークやウェブ検索で正規サイトへアクセスしましょう。怪しいサイトを診断するサービスを利用し、事前に URL をチェックすることも有効です。

2. 個人情報やクレジットカード番号の入力を促すメール・SMS に注意する

クレジットカード会社などでは、個人情報やクレジットカード情報などについてメール・SMS での問い合わせは行っていないため、情報を入力させるページに誘導するメールには細心の注意を払いましょう。

3. ログイン ID・パスワードの使い回しを控える

複数のサービスサイトで同じログイン ID・パスワードを使い回していると、フィッシング詐欺によってログイン ID・パスワードが詐取された場合、他のサービスサイトの不正利用被害に遭う可能性が高まります。被害を最小限に抑えるためにもログイン ID・パスワードの使い回しはせず、サービスごとに登録内容を変更し管理を行うようにしましょう。

4. セキュリティソフトやネット詐欺対策ソフトを導入する

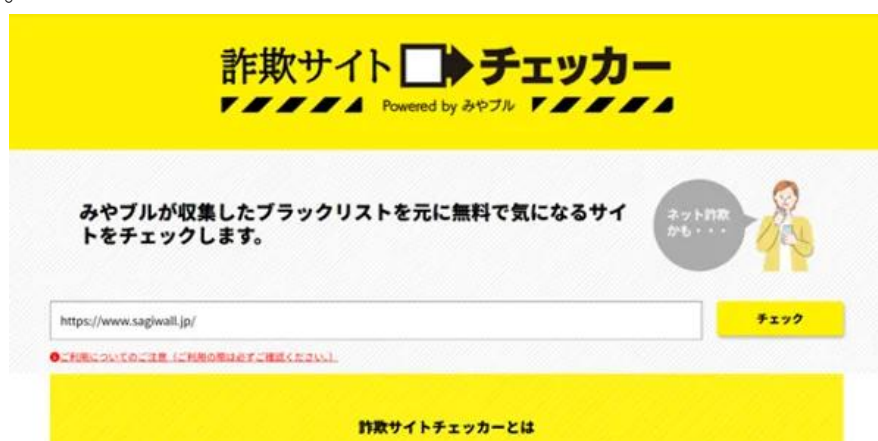
犯罪者の手口は日々巧妙化しており、今まで意識してきた対策が通用しなくなる可能性があります。

す。日々進化するネット犯罪に対抗するには、セキュリティソフトを導入することも必要です。不審なサイトへアクセスした際に警告を表示し、被害の未然防止に役立ちます。

■詐欺サイトを無料で診断「詐欺サイトチェッカー」

不審なサイトの安全性を確認したい場合は、無料で利用できる「詐欺サイトチェッカー」を活用する方法もあります。

ネット詐欺対策ソフトの「みやブル」及び官公庁などから収集したブラックリストの情報をもとに判定を行うもので、気になるサイトの URL がネット詐欺サイトとして報告されているかをチェックすることができます。

詐欺サイトチェッカーのウェブサイトのスクリーンショット。黄色いヘッダーには「詐欺サイトチェッカー」のロゴと「Powered by みやブル」の文字があります。メインコンテンツエリアには、みやブルが収集したブラックリストを元に無料で気になるサイトをチェックする旨のメッセージと、入力欄、チェックボタン、およびネット詐欺のイラストが描かれています。入力欄には「https://www.sagiwall.jp/」が入力されています。チェックボタンは黄色で「チェック」と書かれています。下部には「詐欺サイトチェッカーとは」という見出しがあります。

詐欺サイトチェッカー

Powered by みやブル

みやブルが収集したブラックリストを元に無料で気になるサイトをチェックします。

ネット詐欺かも・・・

https://www.sagiwall.jp/

チェック

●ご利用については、必ず「ご利用の際は必ずご確認ください」。

詐欺サイトチェッカーとは

サイト URL:<https://checker.miyabull.jp/>

■森 達哉教授のコメント

8 月度は国税庁をかたるフィッシングサイトが前月の 10 位から 1 位に上がり、また総務省も 3 位に入ったため、官公庁カテゴリが構成比のほぼ 4 分の 1 を占めました。フィッシング対策協議会の 8 月度報告でも官公庁系の報告は急増しており、統計局が報告数の上位 5 ブランドに入っています[1]。前月の本リポートで、行政系の手口は 9 月から 10 月にかけて再び上昇すると予想しておりましたが、実際には 1 か月前倒しで現れたこととなります。昨年、国税庁をかたる手口が増え始めたのは 10 月度でした（2025 年 10 月度本リポートご参照）。今年は消費税の中間申告の時期にまで狙いが拡大したと見られ、税に関する手口は従来の確定申告期に限らず、年間を通じて警戒すべき段階に入ったと考えるべきでしょう。

総務省をかたる手口では、ターゲットが「国勢調査」から「労働力調査」に変わりました。5 年に一度の国勢調査と違い、労働力調査は毎月実施されるため、攻撃者にとっては時期を選ばずにターゲットにすることができます。回答義務や罰則を強調する攻撃手口は変わらず、今後も長くこのパターンが使われる可能性があります。一方、USJ の当選を装う手口は、不安ではなく「せっかくの当選を逃したくない」という心理に訴える点で、6 月度に取り上げたポイント付与型と同じ系統の手口です。さらに実在のキャンペーンに便乗するため、本物の案内と混同しやすくなった点が巧妙です。また、前月に注目した LINE は上位 10 位から外れ、SNS カテゴリは約 9% から 2% 未満に下がりました。攻撃者がかたるブランドは数日単位で切り替えられているとの指摘もあり[1]、前月の上位だけを警戒するだけでは対策として不十分であることが示唆されます。

今後は年末調整やふるさと納税、年末商戦が重なる時期に入ります。国税庁をかたる手口は確定申告期に向けて続き、当選やポイント還元を装う手口も増えると予想されます。行政機関をかたる連絡は、メールや SMS のリンクを開かず、公式サイトや公式アプリ、ブックマークから確かめることが有効な対策となります。当選の通知も、主催者の公式サイトで通知方法を確認する一手間が有効です。攻撃ターゲットとなるブランドの入れ替わりが速い以上、狙われているブランド名を覚えるよりも、届いたリンクからは入力しない習慣が確実な対策になります。本レポートの内容をご家族や周囲の方々と共有し、攻撃者の手口に先んじて備えていただければと思います。

[1] フィッシング対策協議会「2026/08 フィッシング報告状況」2026 年 9 月 18 日、
<https://www.antiphishing.jp/report/monthly/202608.html>

■監修者プロフィール

森 達哉

早稲田大学 理工学術院 教授

「令和 7 年度科学技術分野の文部科学大臣表彰 科学技術賞（研究部門）」受賞

NICT サイバーセキュリティ研究所 招へい専門員

<会社概要>

社名 : BBSS 株式会社

所在地 : 東京都港区海岸 1 丁目 7 番 1 号 WeWork 東京ポートシティ竹芝

代表者 : 代表取締役社長 兼 CEO 本多 晋弥

設立日 : 2006 年 1 月 17 日

株主 : SB C&S 株式会社 100%

事業内容: コンシューマ向けソフトウェア、および IoT サービスの企画・開発・提供、法人向けライセンス販売

URL : <https://www.bbss.co.jp/>