2026 年 9 月 17 日
BBSS 株式会社

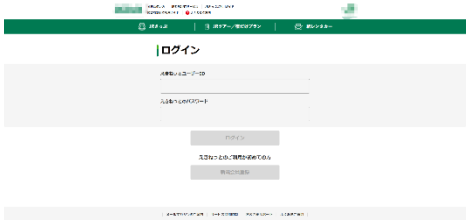
7 月度ネット詐欺リポート
夏季休暇の需要に合わせて交通系詐欺サイト増加

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

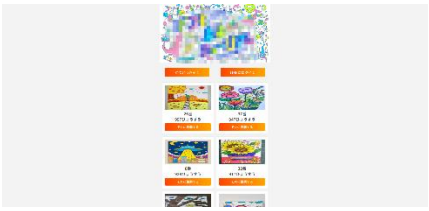
目次：

■夏休みに入り交通系フィッシングが増加、LINE のフィッシングも増加

7 月以降、交通系サービスを装ったフィッシングサイトが増加傾向にあります。昨年度も同じ時期に同様の傾向が見られており、特に「えきねっと」や「ETC 利用照会サービス」を装ったフィッシングが増えています。また、8 月に入ってからは、JAL や ANA を装ったフィッシングサイトも増加しています。これらは SMS やメールなどから偽サイトへ誘導し、ログイン情報を盗み取る手口です。夏休みや帰省などで 7～8 月に利用機会が増えるサービスのため、特に注意が必要です。7 月は、LINE を狙ったフィッシングサイトも増加しています。最近確認されているのが、「ドコモ未来ミュージアム」を装った偽の投票サイトです。「投票してほしい」などと LINE で誘導し、投票時の認証を装って LINE の認証情報を盗み取ります。最近の LINE を悪用した詐欺では、単純に偽のログイン画面へ誘導するだけでなく、「投票をお願いする」という自然なやり取りをきっかけに偽サイトへ誘導する手口が目立っています。SMS やメールだけでなく、知人から LINE で投票を頼まれた場合でも、安易にリンクを開いたり認証情報を入力したりしないことが重要です。



えきねっとを利用したフィッシングサイト


ドコモ未来ミュージアムの詐欺サイト

えきねっとをかたる偽メール(フィッシングメール)偽サイト(フィッシングサイト)にご注意ください！
https://www.eki-net.com/top/oshirase/security/

フィッシングサイト・不審メールにご注意ください　ETC 利用照会サービス

https://www.etc-meisai.jp/caution/caution_phishing.html

※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。

■総務省労働力調査のフィッシングが増加傾向

8 月に入り、総務省の「労働力調査」を装ったフィッシングサイトが急増しています。これまで総務省を装うフィッシングでは、主に「国勢調査」をかたり、偽サイトへ誘導してログイン情報などを盗み取る手口が確認されていました。最近では、その手口が「労働力調査」にも広がっています。労働力調査は国勢調査と同様、対象となった世帯には法律上の回答義務があり、回答を拒んだ場合などには罰則の規定があります。フィッシングではこの制度を悪用し、「回答しないと罰則・罰金がある」などと不安をあおり、偽サイトへ誘導して情報を入力させる手口が使われています。国の機関からの連絡を装い、「回答義務」「罰則」「罰金」などの言葉で焦らせるため、信用してしまう可能性があります。 メールや SMS などで回答を求められた場合は、記載されたリンクをすぐに開かず、公式サイトなどから情報を確認することが重要です。

労働力調査のフィッシングサイト

※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

7 月は、三井住友カードを装ったフィッシングサイトが最も多く確認されました。また取り上げたえきねっとのフィッシングサイト 4 位、ETC 利用照会サービスが 9 位にランクインしています。

	2026年6月	割合	2026年7月	割合
1	Apple	17.95%	三井住友カード	12.69%
2	三井住友カード	11.58%	JCB	8.35%
3	Amazon	8.61%	LINE	7.09%
4	えきねっと	7.85%	えきねっと	6.27%
5	SAISON CARD	4.95%	Amazon	6.21%
6	VISA	3.80%	イープラス	5.87%
7	PayPay	3.36%	Apple	5.35%
8	JRE POINT	2.31%	SAISON CARD	4.53%
9	日本郵便	2.04%	ETC利用照会サービス	2.94%
10	首相官邸HP	1.94%	国税庁	2.66%

■フィッシングサイトカテゴリ別構成比

7 月度は、SNS フィッシングサイトの実数・構成比とも上昇しています。こちらは LINE の投票を促

す詐欺サイトが増加したことが起因しています。

	2026年6月	2026年7月	
銀行	4.10%	2.91%	↘
携帯キャリア	1.42%	1.01%	↘
クラウドサービス	0.00%	0.00%	→
消費者金融キャッシング	0.00%	0.00%	→
クレジットカード	32.45%	33.24%	↗
ECサイト	12.24%	10.12%	↘
ポータルサイト	0.54%	2.05%	↗
プロバイダー	1.72%	1.31%	↘

	2026年6月	2026年7月	
官公庁	3.31%	6.39%	↗
株 / 証券	0.49%	0.24%	↘
SNS	1.08%	8.81%	↗
仮想通貨	0.07%	0.70%	↗
Webメール	0.00%	0.12%	↗
Webメールユーザー	0.00%	0.00%	→
Webサービス	38.70%	31.93%	↘
その他	3.88%	1.17%	↘

※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。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。

サイト URL:https://checker.miyabull.jp/

■森 達哉教授のコメント

7 月度は三井住友カードや JCB などクレジットカード系が上位を固め、カテゴリ別でも前月に続き 3 割を超えました。一方、昨年活発だった証券系のフィッシングサイトは 1%を割り込みました。フィッシング対策協議会の 7 月度報告でも証券系の報告は 1 ブランドのみとなっています[1]。認証強化で証券口座から締め出された攻撃者が、クレジットカード情報の詐取に切り替えた戦略がみてとれます。一方、7 月度は季節に応じた兆候として、交通系フィッシングの増加が見られました。5 月度の本リポートでえきねっとの上昇を夏の予兆として指摘しましたが、7 月には 4 位に定着しました。また、交通系として ETC 利用照会サービスもランク入りしました。昨年も同じ時期に ETC や航空系が急増しており、攻撃者は毎年同じ時期に同じ標的を狙う傾向があることがわかります。6 位に新登場したイープラスも、夏のライブや帰省の予定に紐づく点で同じタイプのフィッシングといえます。前月 1 位の

Apple が 7 位まで下がったように、ターゲットとなるブランドの切り替えは数日単位になっているとの指摘もあり[1]、順位そのものより入れ替わりの速さに注意が必要です。

今月最も注目したいのは、LINE が 3 位に入り、SNS カテゴリの構成比が約 1%から約 9%へ急伸した点です。ドコモ未来ミュージアムの投票を装う手口は、従来型の不正アクセスへの「不安」や、ポイント付与型の「お得感」とも異なり、知人からの頼まれごとに応えたいという「善意」につけこむアプローチです。投票の認証を装って電話番号や認証コードを入力させてアカウントを乗っ取り、そのアカウントから次の知人へ同じ依頼を送る構造となっています。この攻撃では、差出人が本物の知人となるため、差出人や URL を確認するという従来の見分け方が通用しない点に深刻さがあります。日常の連絡手段そのものが乗っ取られると、金銭被害だけでなく人間関係、あるいは社会的生活にも影響が及ぶ点で、ログイン情報の窃取にとどまらない高いリスクが生じます。

今後は 9 月から 10 月にかけて行政系の手口が再び活発化することが予想されます。昨年は国勢調査が増加しましたが、今年は労働力調査が先行しており、装う調査名を変えながら続くと見られます。秋の連休に向けた交通系や航空系、年末に向けたポイント還元やセールに便乗する手口の流行も引き続き予想されます。リンクからログインや決済をせず公式アプリやブックマークから確認する基本に加えて、今月の事例を踏まえ、SMS で届く認証コードは誰に頼まれても他人に教えたり別のサイトに入力したりしないことを強調したいと思います。知人からの依頼であっても、電話など別の経路で本人に確かめる一手間が、自分だけでなく周囲への被害の連鎖を断つことにつながります。本リ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「2026/07 フィッシング報告状況」2026 年 8 月 17 日. https://www.antiphishing.jp/report/monthly/202607.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エア、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/