

6 月度ネット詐欺レポート

ポイント付与を装う偽サイトが増加、首相官邸を装う投資詐欺に注意

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：

- ポイント付与のフィッシングサイトが増加傾向
- LINE や総務省などのフィッシングに注意
- 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

■ポイント付与のフィッシングサイトが増加傾向

近年、「ポイントプレゼント」を装い、ログイン情報や個人情報を盗み取るフィッシング詐欺が増加しています。特に 6 月は、JRE POINT をかたるフィッシングサイトが多数確認されました。これまでのフィッシング詐欺は、「不正アクセスが確認されました」「至急ログインしてください」など、不安や焦りをあおってログインを促す手口が主流でした。しかし最近では、「ポイントがもらえる」「キャンペーンでお得」といったメリットを強調し、利用者を誘導する手口が増えています。現在は、QR コード決済やさまざまな Web サービスでポイント還元キャンペーンが頻繁に実施されているため、本物のキャンペーンと思い込み、警戒せずにログインしてしまう可能性があります。ポイント付与をうたうサイトやメールを利用する際は、記載されたリンクを安易に開かず、公式サイトや公式アプリからアクセスしていることを確認しましょう。

また、首相をかたった投資詐欺の報告も増加しています。SNS 広告などを通じて偽の投資サイトへ誘導する手口が確認されており、首相官邸のホームページでも注意喚起が行われています。有名人や著名人を利用した投資広告は安易に信用せず、公式情報を確認することが重要です。

※QR コードは株式会社デンソーウェーブの登録商標です。



JRE POINT を利用したフィッシングサイト



投資詐欺

「JRE POINT」を名乗る不審なメール・サイトにご注意ください

<https://www.jrepoint.jp/information/jrepoint-office/20260512001>

首相官邸ホームページを装った偽サイトにご注意ください

<https://www.kantei.go.jp/jp/headline/kantei-fake-website/index.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。

■LINE や総務省などのフィッシングに注意

最新のデータでは、7 月に入り、LINE や総務省の労働力調査を装ったフィッシングサイトが増加しています。LINE を悪用した手口では、ログイン ID・パスワードを盗み取るだけでなく、投資詐欺サイトへ誘導するために LINE への「友だち追加」を促すケースも多く確認されています。不審なメッセージや広告から LINE へ誘導された場合は、安易に登録しないよう注意が必要です。また、年初に多く確認されていた国勢調査を装うフィッシングに代わり、現在は総務省の労働力調査をかたる手口が増加しています。主にメールなどで送信され、「回答しない場合は法律に基づき罰金が科される」といった内容で利用者の不安をあおり、個人情報を入力させようとするものです。総務省からの案内は、必ず公式サイトなどで確認するようにしましょう。

さらに、イープラスなどのチケット販売サービスを装ったフィッシングも増加傾向にあります。チケットの購入や抽選結果の確認を装ったメールや SMS を受け取った場合は、リンクを直接開かず、公式サイトや公式アプリからアクセスすることを心掛けてください。



LINE のフィッシングサイト



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

6 月は、Apple 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。また本レポートで取り上げた JRE POINT のフィッシングサイトが 8 位、首相官邸の投資詐欺が 10 位にランクインしています。

	2026年5月	割合	2026年6月	割合
1	PayPay	15.66%	Apple	17.95%
2	Apple	11.59%	三井住友カード	11.58%
3	Amazon	7.01%	Amazon	8.61%
4	SAISON CARD	5.04%	えきねっと	7.85%
5	えきねっと	4.87%	SAISON CARD	4.95%
6	LINE	4.39%	VISA	3.80%
7	楽天カード	3.84%	PayPay	3.36%
8	Paidy	3.24%	JRE POINT	2.31%
9	auじぶん銀行	2.92%	日本郵便	2.04%
10	国税庁	2.90%	首相官邸HP	1.94%

■フィッシングサイトカテゴリ別構成比

6月度は、Webサービスのフィッシングサイトの構成比が上昇しています。Apple やえきねっとなどを装ったフィッシングサイトの増加が要因です。また、証券関連のフィッシングサイトは、マネックス証券をかたるサイトの減少に伴い、全体の構成比も低下しています。

	2026年5月	2026年6月	
 官公庁	4.77%	3.31%	↓
 株 / 証券	4.77%	0.49%	↓
 SNS	4.41%	1.08%	↓
 仮想通貨	0.06%	0.07%	↑
 Webメール	0.06%	0.00%	↓
 Webメール ユーザー	0.00%	0.00%	→
 Webサービス	26.81%	38.70%	↑
その他	3.03%	3.88%	↑

	2026年5月	2026年6月	
 銀行	9.41%	4.10%	
 携帯キャリア	1.00%	1.42%	
 クラウドサービス	0.00%	0.00%	
 消費者金融キャッシング	0.02%	0.00%	
 クレジットカード	37.08%	32.45%	
 ECサイト	8.05%	12.24%	
 ポータルサイト	0.00%	0.54%	
 プロバイダー	0.53%	1.72%	

※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。

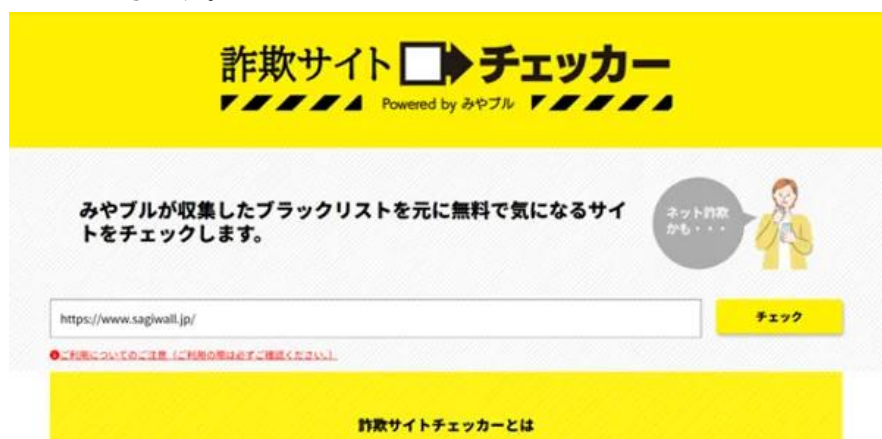
4. セキュリティソフトやネット詐欺対策ソフトを導入する

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「みやぶル」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 みやぶル」の文字があります。メインコンテンツエリアには、みやぶ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、ネット詐欺のイラストがあります。検索欄には「https://www.sagiwall.jp/」が入力されており、右側には「チェック」ボタンがあります。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 みやぶル

みやぶ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、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

6 月度は、ポイント付与を装うフィッシングの増加が特徴的でした。JRE POINT がブランドランキング8位に入るなど、手口の定着化が進んでいます。今回注目すべきポイントは、利用者の心理に対するアプローチの変化です。従来は「不正アクセスが検知された」など不安をあおることでログインを急がせる手口が中心でしたが、ポイント付与型は「もらえるはずのポイントを逃したくない」という消費者の心理を突きます。ポイント還元キャンペーンが日常的に実施されている環境では、本物のキャンペーンと見分けることが困難です。攻撃者がこうした「お得感」の心理について利用者を誘導できる状況は、フィッシング対策の難度を一段階引き上げたと言えるでしょう。

行政機関を装うフィッシングでは、総務省の労働力調査をかたる手口が新たに確認されました。昨年 9 月度の国勢調査、10 月度以降の国税庁、3 月度の eLTAX に続き、装う組織を切り替えながら「行政の権威性」を一貫して利用するフィッシング手口の典型例です。「回答しない場合は罰金」という法的制裁をちらつかせる文言も巧みです。また、LINE を悪用した手口では、ログイン情報の窃取にとどまらず「友だち追加」を経由して投資詐欺サイトへ誘導するケースが増えており、日常的に使っているコミュニケーションツールへの信頼を足がかりに金銭被害へつなげる多段階の手口として警戒が必要です。

今後は秋に向けて、行政手続き関連のフィッシングが再び活発化する時期に入ります。過去の傾向では 9 月から 10 月にかけて国勢調査や NHK を装う手口が増加しており、今年も労働力調査に続いて新たな行政系ブランドの出現が予想されます。さらに、秋から年末にかけてはポイント還元キャンペーンや割引セールが増えるため、ポイント付与型のフィッシングが本物のキャンペーンに紛れて拡大する

リスクも高まります。不審なメールや SMS のリンクは決してクリックせず、公式アプリやブックマークからのアクセスを徹底することがこれまで以上に重要です。本レポートの内容をご家族や周囲の方々と共有し、心当たりのない「ポイント付与」や「支払い請求」には一拍置いて確認する習慣をつけていただければと思います。

■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/>