

5 月度ネット詐欺レポート

QR コード決済での 不当請求詐欺増加、ポイント付与偽サイトに注意

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：

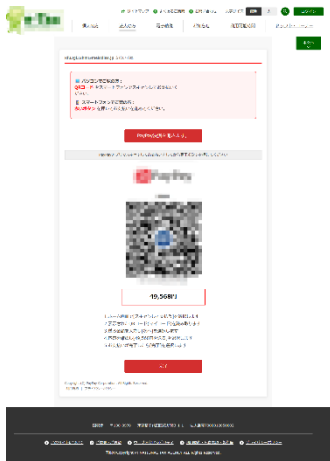
- QR コード決済 を利用した不当請求が増加
- ポイントプレゼントの詐欺サイトに注意
- フィッシングサイトブランドランキング
- フィッシングサイトカテゴリ別構成比
- フィッシング詐欺被害防止のポイント
- サイトを無料診断「詐欺サイトチェッカー」
- 森 達哉教授のコメント

■ QR コード決済 を利用した不当請求が増加

5 月は QR コード決済（※） を悪用した詐欺サイトが増えています。この手口は、ID やパスワードを盗む従来のフィッシング詐欺とは異なり、利用者を QR コード決済の支払い画面へ誘導し、直接送金させるものです。「e-Tax で未納の税金があります」などの偽のメッセージを送り、支払いを促す事例が確認されています。

QR コード決済で支払いをしてしまった場合、受付処理が完了する前であれば取り消せることがあります。しかし、受付が確定した後は、QR コードを発行した側しか取り消しができず、お金を取り戻すことは非常に困難です。不審なメッセージやサイトから支払いを求められた場合は、慌てて手続きをせず、公式サイトや公式アプリで状況を確認するようにしましょう。

※「QR コード」は、株式会社デンソーウェーブの登録商標です。



e-Tax を利用した不当請求サイト



国税庁を利用した不当請求サイト

PayPay をかたる巧妙な詐欺やアカウントの不正利用にご注意ください

<https://paypay.ne.jp/notice/20250715/s-01/>

PayPay 購入をキャンセルしたい・返金したい

<https://paypay.ne.jp/help/c0037/>

※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。

■ポイントプレゼントの詐欺サイトに注意

5月から6月にかけて、「ポイント交換」や「ポイントプレゼント」を装って、ログイン情報や個人情報を盗み取る詐欺が増加しています。この手口は、JRE POINT、楽天ポイント、Vポイント、dポイントなど、さまざまなポイントサービスのブランドを悪用して行われています。

これまでのフィッシング詐欺では、「取引を確認できませんでした」「不正アクセスが検知されました」など、不安をあおるメッセージで利用者を焦らせ、ログインを促す手口が多く見られました。一方、今回の手口は、「ポイントをプレゼントします」「ポイント交換の手続きはこちら」といった、お得感を利用してログインさせるものです。利用者に「ログインしないと損をする」と思わせ、ログイン情報の入力进行を促します。

多くの企業やサービスでは、定期的にポイントプレゼントキャンペーンを実施しています。そのため、不審なメールやSMSであっても警戒心が薄れやすく、だまされるリスクがあります。ポイントの受け取りや交換を案内するメールやSMSを受け取った場合は、記載されたリンクを開かず、公式サイトや公式アプリから直接アクセスして確認しましょう。



楽天ポイントの詐欺サイト



dポイントの詐欺サイト

※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。

■フィッシングサイトブランドランキング

5 月は、PayPay 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。ログイン情報の詐取を目的とした手口のほか、ポイントプレゼントを装った手口も多く確認されています。また、8 位には Paidy を装ったフィッシングサイトも確認されています。QR コード決済 を狙った手口は毎月確認されており、引き続き注意が必要です。

	2026年4月	割合	2026年5月	割合
1	Apple	13.83%	PayPay	15.66%
2	Viewcard	7.47%	Apple	11.59%
3	auじぶん銀行	6.90%	Amazon	7.01%
4	Amazon	6.26%	SAISON CARD	5.04%
5	マネックス証券	6.13%	えきねっと	4.87%
6	楽天カード	5.92%	LINE	4.39%
7	SAISON CARD	5.34%	楽天カード	3.84%
8	TEPCO	5.29%	Paidy	3.24%
9	SBI証券	3.58%	auじぶん銀行	2.92%
10	三井住友カード	3.02%	国税庁	2.90%

■フィッシングサイトカテゴリ別構成比

5 月度は、クレジットカードを装ったフィッシングサイトの構成比が上昇しました。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4月	2026年5月	
 銀行	10.85%	9.41%	
 携帯キャリア	1.52%	1.00%	
 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%	0.02%	
 クレジット カード	30.51%	37.08%	
 ECサイト	9.13%	8.05%	
 ポータルサイト	0.03%	0.00%	
 プロバイダー	1.42%	0.53%	
	2026年4月	2026年5月	
 官公庁	4.50%	4.77%	
 株 / 証券	12.69%	4.77%	
 SNS	0.74%	4.41%	
 仮想通貨	0.15%	0.06%	
 Webメール	0.00%	0.06%	
 Webメール ユーザー	0.00%	0.00%	
 Webサービス	27.48%	26.81%	
その他	0.98%	3.03%	

※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。不審なサイトにアクセスした際に注意喚起を行ってくれます。

■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

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・・・

チェック

●ご利用についてのご注意：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

今月最も注目されるのは、フィッシングサイトブランドランキングで PayPay が首位となったことです。前月の本レポートでも取り上げた QR コード決済を悪用する不当請求の手口は、ID やパスワードを盗む従来のフィッシングと異なり、利用者自身に送金の操作をさせる点が特徴です。トピラスシステムズの調査[1]では、この種の PayPay 送金詐欺は本年 2 月と比べて 22.4 倍に増えたと報告されています。

一般に多要素認証の導入等、認証技術の強化が進んだ結果、攻撃者は認証を突破するのではなく、正規の決済の仕組みをそのまま使わせる方向へ手口を変えています。送金が確定した後の取り消しは難しく、補償の対象外となる場合もあるため、金銭被害に直結しやすい点で従来の手口より深刻です。

利用者の心理をつく変化にも注意が必要です。ポイントプレゼントを装う手口は、「不正アクセスが検知された」と不安をあおる従来型とは反対に、「受け取らないと損」という心理をつくことで、巧みにログインを促します。カテゴリ別では株/証券の割合が大きく低下する一方、クレジットカードが上昇しました。フィッシング対策協議会の2026年5月度報告[2]でも証券会社をかたるフィッシングの報告数は前月から9割以上減っており、金融庁と業界による認証強化の効果が表れた反面、攻撃者が標的を移した様子が見えます。ランキング10位に国税庁が入った点は、自動車税や住民税の納付期限が集中する時期を狙ったものと考えられます。フィッシング対策協議会も5月に住民税や国民年金の納付依頼を装う手口について緊急情報を公開しており、この時期特有の攻撃と考えられます[2]。

今後は夏の旅行シーズンに向けて、鉄道や航空をかたる手口の増加が予想されます。えきねっとがランキング5位に入っている点はその予兆かもしれません。対策の基本は、メールやSMSのリンクから決済やログインの操作をせず、公式アプリやブックマークから直接確認することです。特に送金型の被害は取り戻すことが難しいため、支払いを求められたときこそ一呼吸おいて、請求元へ自分で確認する習慣をつけていただきたいと思います。

参考文献

[1] トビラシシステムズ株式会社「トビラシシステムズ 特殊詐欺・フィッシング詐欺に関するレポート（2026年5月）」2026年6月24日。

<https://prtimes.jp/main/html/rd/p/000000235.000034282.html>

[2] フィッシング対策協議会「2026/05 フィッシング報告状況」2026年6月18日。

<https://www.antiphishing.jp/report/monthly/202605.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/>