2026 年 6 月 19 日
BBSS 株式会社

4 月度ネット詐欺リポート
QR 決済利用の金銭詐取増加、地方銀行やネット銀行を装う詐欺に注意

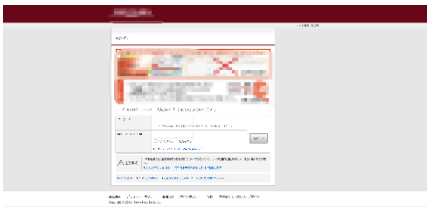
ネット詐欺リポートは毎月調査・収集した詐欺サイトを分析し、傾向をまとめたリポートです。

目次：

■大手銀行以外を狙った手口が増加

４月は、au じぶん銀行や大和ネクスト銀行を装ったフィッシングサイトが増加しています。これは、メールや SMS などで偽サイトへ誘導し、インターネットバンキングの ID やパスワードを盗み取る手口です。近年は、メガバンクだけでなく地方銀行・ネット銀行・信用金庫などにも被害の対象が広がっています。被害を防ぐためには「メールや SMS 内のリンクを安易に開かない」「銀行のサイトは公式アプリやブックマークからアクセスする」「ID・パスワード・確認コードを入力する前に URL を確認する」「不審なメールや SMS はすぐに削除する 」のほか、不審に感じた場合は、金融機関の公式窓口へ確認することが重要です。


au じぶん銀行のフィッシングサイト


大和ネクスト銀行のフィッシングサイト

【重要】au じぶん銀行を名乗る不審な SMS・メールにご注意ください
https://www.jibunbank.co.jp/announcement/2023/0426_01.html
【更新】大和ネクスト銀行を騙る偽のメールや偽サイトにご注意ください

https://www.bank-daiwa.co.jp/info/2026/0415_01.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。

■コード決済で直接金銭詐取する偽サイトが急増

４月から５月にかけて、コード決済を悪用してお金をだまし取る手口が急増しています。これは、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、PayPay などの QR コード※決済の支払い画面へ利用者を誘導し、自ら送金・支払いをさせる手口です。支払い画面で誤ってボタンを押してしまうと、そのまま決済が完了してしまう場合があります。

支払いは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が、受付確定後は QR コードを作成した側しか取り消しできず、返金されない可能性が高くなります。

現在確認されている手口としては、「国税庁を装い、『未納の税金がある』と偽って支払いを求める」「生命保険料や各種料金の支払いを装って送金させる」といったケースがあります。

詐欺被害を防ぐため、内容を十分に確認せずに QR コードを読み取ったり、支払いボタンを押したりしないよう注意が必要です。

※「QR コード」は、株式会社デンソーウェーブの登録商標です。

【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。

■フィッシングサイトブランドランキング

４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。また冒頭で取り上げた au じぶん銀行のフィッシングサイトも３位にランクインしました。Viewcard などクレジット系のフィッシングサイトは前月と変わらず報告されており、注意が必要です。

	2026年3月	割合	2026年4月	割合
1	マネックス証券	12.18%	Apple	13.83%
2	Amazon	8.90%	Viewcard	7.47%
3	三井住友カード	8.47%	auじぶん銀行	6.90%
4	Apple	7.15%	Amazon	6.26%
5	SAISON CARD	6.56%	マネックス証券	6.13%
6	VISA	3.52%	楽天カード	5.92%
7	楽天カード	3.25%	SAISON CARD	5.34%
8	名古屋銀行	3.18%	TEPCO	5.29%
9	ANA	2.61%	SBI証券	3.58%
10	Viewcard	2.54%	三井住友カード	3.02%

■フィッシングサイトカテゴリ別構成比

４月度は、Apple のフィッシングサイトの増加に伴い、ウェブサービスカテゴリのフィッシングサイトの構成比が増加しています。また銀行カテゴリも構成比が増加しています。

	2026年3月	2026年4月	
銀行	7.37%	10.85%	↗
携帯キャリア	2.51%	1.52%	↘
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	33.68%	30.51%	↘
ECサイト	10.62%	9.13%	↘
ポータルサイト	0.07%	0.03%	↘
プロバイダー	3.47%	1.42%	↘

	2026年3月	2026年4月	
官公庁	4.16%	4.50%	↗
株 / 証券	14.88%	12.69%	↘
SNS	1.84%	0.74%	↘
仮想通貨	0.12%	0.15%	↗
Webメール	0.05%	0.00%	↘
Webメールユーザー	0.00%	0.00%	→
Webサービス	20.02%	27.48%	↗
その他	1.19%	0.98%	↘

※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無料サービスを利用し、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

今月のリポートで特に注目すべきは、QR コード決済を悪用して、利用者から直接金銭を詐取する手口が急増した点です。従来のフィッシング詐欺は偽サイトで ID やパスワードを入力させる手口が主流でしたが、今回の手口の特徴は PayPay 等の QR コード決済の支払い画面へ利用者を誘導し、自ら送金や支払いの操作をさせるものです。この手口が深刻なのは、被害者自らが送金を行うため、FIDO 2 をはじめとする多要素認証の強化策が結果として無効化されている点にあります。証券系フィッシングは業界全体の認証強化によって大幅に減少しましたが（２月度本リポート参照）、攻撃者はその対策を回避するために、利用者自身の操作による送金という手口を新たに開拓していると考えられます。

とりわけ警戒が必要なのは、国税庁を装い「未納の税金がある」として QR コード決済での支払いを求めるケースです。国税庁を名乗るフィッシングは 1 月度に前月比 6 倍増でランキング 1 位となり、確定申告シーズンを経た後も高い水準が続いてきました。ここにきて手口が進化し、ID やパスワードの窃取を目的とする従来の攻撃アプローチから、税務当局の権威性を傘に不安をあおることで、利用者にその場で支払い操作を完了させる攻撃アプローチに変化しました。生命保険料や各種料金の支払いを装うケースも確認されており、正規の手続きに見せかける巧妙さが増していることがわかります。

５月から７月にかけては自動車税や固定資産税の納付期限が集中するため、税や行政を装った詐欺が QR コード決済型も含めてさらに活発化することが予想されます。夏に向けては電力会社や航空会社、ETC を装った旅行シーズン便乗型の攻撃にも引き続き注意が必要です。QR コード決済型の詐欺に対しては、「支払い」や「送金」を促すメッセージが届いた際に、内容を十分に確認せずに QR コードを読み取ったり支払いボタンを押したりしないことが基本的な防御策となります。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とともに、本リポートの内容をご家族や周囲の方々と共有し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/