

2023 年版 インターネット詐欺レポート ～詐欺サイト検知数が三年連続で上昇、 ブランド別ではイオン銀行のフィッシングサイトが 1 位に～

BB ソフトサービス株式会社（本社：東京都港区、代表取締役社長：本多 晋弥）は、詐欺ウォール®によって調査・収集したデータを分析し、2023 年のネット詐欺の状況をまとめた「2023 年 年間インターネット詐欺レポート」を公開します。

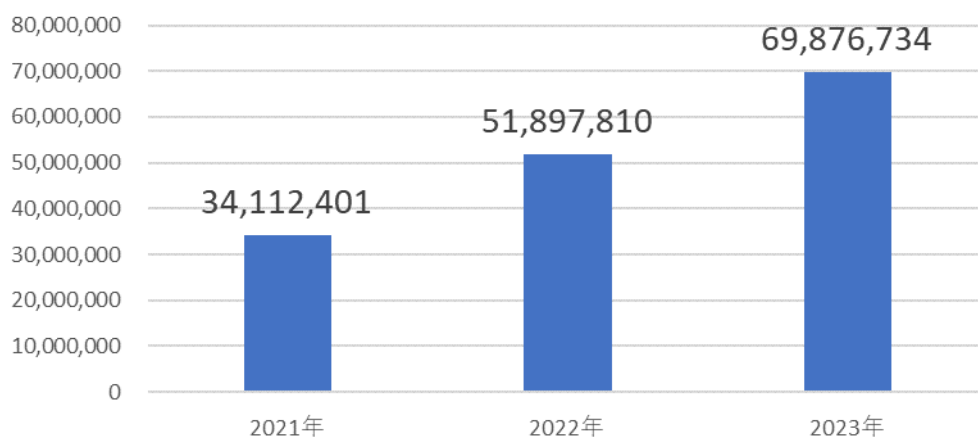
目次：

- 2023 年詐欺サイト検知数レポート
- イオン銀行のフィッシング詐欺サイトが 1 位に
- 2023 年はサポート詐欺が増加
- 2023 年ネット詐欺の手口
- 2023 年フィッシングサイトカテゴリ別構成比
- ネット詐欺 2023 年考察と 2024 年予測
- サイトを無料診断「詐欺サイトチェッカー」

■2023 年詐欺サイト検知数レポート

2023 年の詐欺ウォールによる詐欺サイト検知数は 69,876,734 件でした。前年比で約 1.34 倍、2021 年比では約 2.04 倍に増加しています。＊。

詐欺ウォール年間検知数



※以下記載のアプリバージョン以上の詐欺ウォールを利用しているお客様のアクセス数値を集計
Windows 版：3.3.0 / macOS 版：3.5.0 / Android 版 1.7.0 / iOS 版 3.2.0.4

■イオン銀行のフィッシング詐欺サイトが 1 位に

2023 年に詐欺ウォールで調査・収集したフィッシングサイト*1 で最も多かったのはイオン銀行を騙ったフィッシングサイトでした。近年、同じ内容のフィッシングサイトが短期間で集中的にばらまかれ

る傾向にあり、イオン銀行のフィッシングサイトも 2023 年の 6～7 月に短期集中的に多く確認されました。また、これらのサイトはダイナミック DNS サービス*2 の「Duck DNS」*3 にホストされている傾向があります。「Duck DNS」は無料で使用できるサービスであるため、フィッシングサイトを作成する際に悪用されているものと見られます。

えきねっとや ETC 利用照会サービスといった交通系のフィッシングサイトは短期集中型ではなく、毎月多く報告されており、2023 年全体で見ても上位 10 位内に入っています。増加するブランドには規則性がないため、時期や需要などを考えず、すべてのブランドに注意する必要があります。

*1「フィッシングサイト」は 実在する銀行や EC サイト等を装って個人情報等を詐取する可能性のあるサイトです。

*2「ダイナミック DNS」(正式名称はダイナミックドメインネームシステム)は、IP アドレスが変更されたときに DNS レコードを自動的に更新できるサービスです。

*3「Duck DNS」はダイナミック DNS サービスの 1 つです。

	2022年	割合	2023年	割合
1	三菱UFJニコス	37.7%	イオン銀行	19.2%
2	三井住友銀行	9.3%	SoftBank	11.6%
3	国税庁	8.4%	三井住友カード	7.4%
4	えきねっと	6.7%	Amazon	6.6%
5	三井住友カード	6.3%	国税庁	5.3%
6	au	5.3%	SAISON CARD	5.2%
7	softbank	4.8%	えきねっと	4.5%
8	Amazon	3.3%	日本年金機構	4.1%
9	メルカリ	2.6%	ETC利用照会サービス	3.3%
10	JCB	2.4%	エポスカード	3.3%

イオン銀行のフィッシングサイト

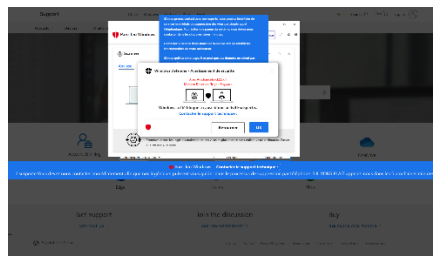
※画像はフィッシング詐欺サイトのイメージであり、本文内容とは関係ありません。

■ 2023 年はサポート詐欺が増加

2023 年の傾向としてサポート詐欺が大きく増加しています。実数で前年比 17 倍以上に増加しています。

サポート詐欺はウイルスに感染したといった内容で警告を出し、表示した電話番号に電話をかけさせて偽の

サポート窓口に誘導する手口です。電話をするとサポート代金として金銭を請求されたり、遠隔操作ソフトをインストールさせられたりするなどの被害に遭う可能性があります。アラート音やアナウンス音声を流すことで閲覧者の不安を煽り、また警告のポップアップが出続ける、全画面表示になるなど警告画面が閉じられないようになる場合もあります。このような警告画面が出た場合は、画面の指示には従わず、パソコンの「ESCボタン」を押してブラウザを閉じるなど、焦らず冷静に対応することが重要です。



サポート詐欺

※画像はサポート詐欺のイメージであり、本文内容とは関係ありません。

■2023 年ネット詐欺の手口

2023 年に詐欺ウォールで収集したネット詐欺の手口で最も多かったのは「偽販売・違法販売」で約 63.53% でした。破格の値段設定などで興味をそそり、偽販売サイトへ誘導する手口です。サイトで購入手続きを行っても、粗悪品が送り付けられる、そもそも何も発送されないなどの被害に遭う可能性があります。実数で前年比 2 倍以上に増加しています。またサポート詐欺が増加した影響で、「ワンクリック詐欺／不当請求」の構成比も高くなっています。

2023 年は NTT docomo、au、SoftBank といった携帯キャリアを騙った「偽ソフトウェア」のサイトが増加しています。WEB ページを閲覧中に「ウイルスが見つかりました」といった警告を表示し、偽ソフトウェアをインストールするよう誘導する手口で、インストールしてもウイルス駆除などの効果はありません。「偽ソフトウェア」は実数で前年比 3 倍以上に増加しています。

	2022年	2023年
フィッシング	49.64%	23.61%
偽販売 違法販売	45.23%	63.53%
ワンクリック詐欺/不当請求	0.07%	0.83%
Web改ざん	0.00%	0.00%
偽ソフトウェア	4.98%	11.96%
公文書違反	0.00%	0.00%
著作権侵害	0.08%	0.05%
違法行為	0.00%	0.00%
不正サイト	0.00%	0.01%

■2023 年フィッシングサイトカテゴリ別構成比

2023 年はイオン銀行のフィッシングサイトが増加した影響で、銀行カテゴリが実数構成比とも増加しています。携帯キャリアは構成比、実数ともに増加しており、NTT docomo、au、SoftBank でフィッシングサ

イトが確認されています。昨年最も多かったクレジットカードの手口は減少しており、また e-Tax・マイナポイントなどのフィッシング詐欺が流行したことで官公庁のフィッシングサイトが実数・構成比ともに増加しています。

	2022年	2023年
銀行	9.7%	21.7%
携帯キャリア	10.4%	14.5%
クラウドサービス	0.0%	1.6%
消費者金融/キャッシング	0.0%	0.0%
クレジットカード/ファイナンス	52.9%	20.3%
出会い系	0.0%	0.0%
ECサイト	7.6%	7.9%
ギャンブル	0.0%	0.0%
オンラインゲーム	0.0%	0.0%
違法広告	0.0%	0.0%
フィッシングリンク	0.0%	0.2%
ポータルサイト	0.2%	0.2%
プロバイダ	0.4%	1.2%
官公庁	8.8%	16.1%
株/証券	0.0%	0.0%
SNS	0.1%	0.3%
仮想通貨	0.1%	0.1%
Webメール	0.1%	0.1%
Webメールユーザ	0.0%	0.0%
Webサービス	9.3%	15.5%
その他	0.5%	0.3%

■ ネット詐欺 2023 年考察と 2024 年予測

2023 年はサポート詐欺が急増しました。情報処理推進機構（IPA）が公開しているデータによると、2023 年に寄せられたサポート詐欺関連の相談件数は 4,145 件で、前年の 1.7 倍以上となっています。^{*4} このサポート詐欺の増加傾向は 2024 年も継続する可能性が高く、被害を防ぐために日頃からサポート詐欺の手法や対処法を理解しておくことが求められます。実際に遭遇した際には警告画面の指示には従わず、冷静にブラウザを閉じるなどの対応を行いましょう。

また、2023 年の 6～7 月に集中的にイオン銀行のフィッシングサイトが確認されました。今後も短期間に特定のブランドを装ったフィッシング詐欺メールが多くばらまかれる可能性があります。このようなメールを受け取った場合は直接 URL をクリック／タップするのではなく、ブックマークや検索から正規サイトにアクセスしてください。

^{*4} 参考：情報処理推進機構（IPA）情報セキュリティ安心相談窓口公開レポート
<https://www.ipa.go.jp/security/anshin/reports/index.html>

■ 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する。または、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

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 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専用ソフトを導入する

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」

日々増加するインターネット詐欺、詐欺サイトかどうかをチェックできるサービス「詐欺サイトチェッカー」を提供開始しました。詐欺ウォールが独自で収集した詐欺サイトのブラックリストと各官公庁から通報のあった詐欺サイトの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。

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

※本記事に記載の「詐欺ウォール」の対象には、「詐欺ウォール」の名称で提供する製品の利用者のみでなく、他の名称で提供している製品の利用者も含まれます。

■「詐欺ウォール® / Internet SagiWall™」について

日本人を標的とするネット詐欺サイトをブロックする、ネット詐欺専用セキュリティソフトです。ウェブブラウザでサイト閲覧中の不用意に悪意のあるサイトにアクセスした場合でも、コンテンツをリアルタイムで検査し自動的にブロックします。ウイルス対策ソフトでは検知が難しい巧妙な詐欺サイトであっても独自の AI 検知技術で高い精度で検出するため、ウイルス対策と併用することでユーザーの安全を高めます。パソコンやスマートフォンの利用に慣れていない方でも、簡単に利用でき、サイバー犯罪被害を未然に防ぐことができます。

※詐欺ウォール®は、iOS、mac OS、Windows®、Android™版を提供しています。

＜詐欺ウォール® / Internet SagiWall™製品サイト URL＞

<https://www.sagiwall.jp/>

■BB ソフトサービス株式会社について

ソフトバンクグループにおいて、セキュリティ製品を主軸とするソフトウェアサービスを、ISP や携帯電話会社などの通信事業者を通じて提供しています。サービス提供のみならず、フィッシング対策協議会やそ

の他の社外団体を通して情報セキュリティに関する啓発活動にも積極的に取り組んでいます。一般消費者のサイバー犯罪被害を減らし、よりよいインターネット利用環境を全てのユーザーに提供することで社会貢献を果たしてまいります。

＜会社概要＞

社名： BB ソフトサービス株式会社
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
社長： 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： ブロードバンドを利用したコンシューマー・SOHO 用アプリケーションサービス、およびオリジナルアプリケーションサービスの企画・開発・販売・運営
URL： <https://www.bbss.co.jp/home.html>

＜本件に関する報道関係者からのお問い合わせ先＞

BB ソフトサービス株式会社 広報事務局（KMCgroup 内）担当:大塚、堀川
TEL: 03-6261-7413（事務局直通：090-9828-9230） FAX: 03-6701-7543 E-MAIL: info@kmcpr.co.jp