2021年5月31日
BBソフトサービス株式会社

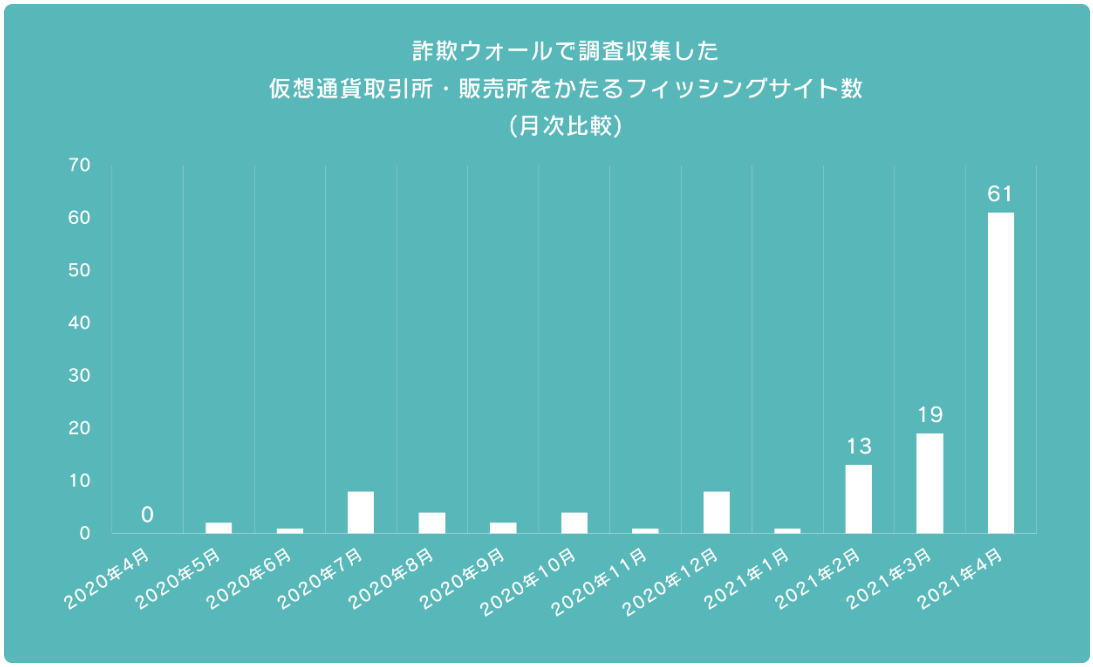
インターネット詐欺リポート（2021年4月度）

仮想通貨取引所をかたるフィッシング詐欺が急増、

フライングセールを切り口にした偽販売サイトが発生

2021年4月度のインターネット詐欺リポートでは仮想通貨取引所をかたるフィッシング詐欺の急増とフライングセールを切り口にした偽販売サイトの発生について取り上げます。

BBSSが調査として収集している仮想通貨取引所をかたるフィッシング詐欺サイト数は、2月の13件から3月は19件、さらに4月は61件と前月比3.2倍に増加しています。2020年5月～2021年1月の期間では10件以下の発生だったものが2021年4月に急増しており、今後も増加する可能性が高いと推測され注意が必要です。



また、2021年4月にBBSSが調査として収集したフィッシングサイトで盗用されていた仮想通貨取引所は以下の5ブランドとなります。

- Coincheck
- bitFlyer
- bitbank
- BITPOINT
- MyEtherWallet

仮想通貨取引所をかたるフィッシングの主な手口は、社名もしくはブランド名を詐称した偽のメールから、偽のログインページにアクセスさせ、ログイン情報（ID・パスワード）や二段階認証コード等を詐取するもので、詐取された認証情報を利用し不正に資産を盗み出される可能性があります。

■偽のログインページ

＜Aサイト＞

＜Bサイト＞

＜Cサイト＞

※画像は偽販売サイトのイメージであり、本文内容とは関係ありません。

参考動画：フィッシング詐欺　手口紹介動画
https://www.youtube.com/watch?v=0Y6dxz4_X30

仮想通貨取引所をかたる偽のメールは、以下の趣旨で送られることが多く、このようなメッセージが含まれたメールが届いた場合は、メールから誘導されているWebページにアクセスしないよう注意してください。なお、アクセスする場合はメール文面が正規のものであるかインターネットで検索し確認した上でアクセスするよう徹底してください。

- アカウント情報の確認をしたい
- パスワード変更の案内
- 異常な操作を検出したため、アカウントが停止されている

■フィッシング詐欺被害防止のためのチェックポイント

1. メールやSMSで案内されたURLが正規URLかを確認する
   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Web検索で正規サイトへアクセスする。
2. SSL通信が提供されているかどうかをチェックする
   個人情報（メールアドレスやクレジットカード番号など）を入力するページのアドレスバーに鍵マークが

表示されない場合には、注意が必要です。

また、2021年4月は通常7月～8月にかけて開催される夏のセール時期に先駆け、特価販売を行う「フライングセール」を切り口にした偽販売サイトが多数発生しました。

「フライングセール」を切り口にした偽販売サイトの共通点として、商品をカートに入れた後に表示されるショッピングカート内の支払方法欄に「銀行振込」と画像で表示される点が挙げられます。取り扱い商品はタイヤやホイール、家具、物置、ファッション関連商品等、サイトによって幅広くさまざまな商品を取り扱っている状況です。欲しい商品をネット上で探し求めた結果、偽販売サイトに行きつく可能性もあるため利用したことのないショッピングサイトを利用する際は注意が必要です。

＜偽販売サイトのトップページ＞

※画像は偽販売サイトのイメージであり、本文内容とは関係ありません。

＜ショッピングカート画面＞

※画像は偽販売サイトのイメージであり、本文内容とは関係ありません。

偽販売サイトで商品を購入すると、粗悪な商品が送られる、または商品が送られずに購入代金を搾取されるなどの被害に遭う可能性があります。また、これらの被害に加えてクレジットカード支払いで商品購入した場合は、犯罪者からカード番号を利用され二次被害に遭う可能性もあります。

参考動画：偽販売サイト　手口紹介動画
https://youtu.be/iXPUtydZEF8

■偽販売サイト被害防止のためのチェックポイント

1. 会社概要をチェックする
   海外の業者は正確な会社概要（運営者氏名・電話番号・住所）や問い合わせ窓口の情報が記載されていないことがあります。詐欺サイトでなくてもこのような業者から購入するのはリスクが高いと考えましょう。
2. 住所を検索して、会社の存在をチェックする
   日本の住所表記や会社名が表記されている場合でも、住所検索で実在する住所かどうか、その住所に会社があるか確認しましょう。
3. 決済方法、口座名義をチェックする
   本物と区別がつかないような、完全なコピーの偽サイトでは、決済方法をチェックしましょう。銀行振り込みしか決済方法がない場合、口座名義が見慣れない名義（無関係な会社名義や個人名など）の場合は、詐欺サイトの危険性が極めて高くなります。
4. SSL通信が提供されているかどうかをチェックする
   個人情報（メールアドレスやクレジットカード番号など）を入力するページのアドレスバーに鍵マークが表示されない場合には、注意が必要です。

■「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ーソフトです。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、セキュリティー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じた情報セキュリティー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：　東京都港区新橋6-19-13　WeWork新橋
社　　長：　代表取締役社長 兼 CEO　瀧　進太郎
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
U　R　L：　https://www.bbss.co.jp/home.html

＜お問い合わせ先＞

BBSS広報事務局（株式会社カーツメディアコミュニケーション内）
担当：堀川、渡邊　TEL：03-6261-7413