

NCO主催 中小企業向けサイバーセキュリティセミナー2026

# サイバー空間の脅威情勢と JC3の取組について

2026年3月12日

一般財団法人 日本サイバー犯罪対策センター(JC3)

酒井 朗



# 本日の目次

## 1 JC3組織概要

## 2 企業を狙った攻撃

ランサムウェア

ボイスフィッシング

CEO詐欺  
(社長騙り詐欺)

## 3 個人を狙った攻撃

フィッシング

モバイルマルウェア  
(スマートフォンを狙ったマルウェア)

ウェブスキミング

サポート詐欺

偽ショッピングサイト  
(悪質サイト)

## 4 サイバー衛生研修のご案内

## 5 まとめ

# JC3の組織概要

## 法人名

- ✓ 一般財団法人日本サイバー犯罪対策センター  
(英語名: Japan Cybercrime Control Center) ※2014年11月13日に業務開始

## 創設の背景

- ✓ サイバー空間の脅威が深刻化する中、個別具体の脅威に対して、事後的に防護措置を講ずる受け身の対応  
→サイバー空間全体を俯瞰し、産学官(警察)それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を組織内外で共有し、サイバー空間の脅威を特定、軽減及び無効化するための活動に貢献する。  
警察庁の有識者会議等を経て、「世界一安全な日本」創造戦略(平成25年12月閣議決定)でも言及

## ～米国のモデル～

米国ではサイバー空間における脅威への対処を目的として1997年、非営利法人NCFTAを創設。FBIをはじめとする法執行機関、大学等の学術機関及び民間企業連携の組織として機能しており、迅速な情報収集、情報の分析、分析した情報に基づく迅速な捜査等を遂行するためのトレーニングを提供している。  
(NCFTA=National Cyber-Forensics & Training Alliance)



# JC3 御賛同いただいている企業・機関・研究者の方々①

正会員等 特定会員 賛同会員 賛助会員  
※：親子会社特例制度利用企業 (敬称略)  
2026年2月

投影限り

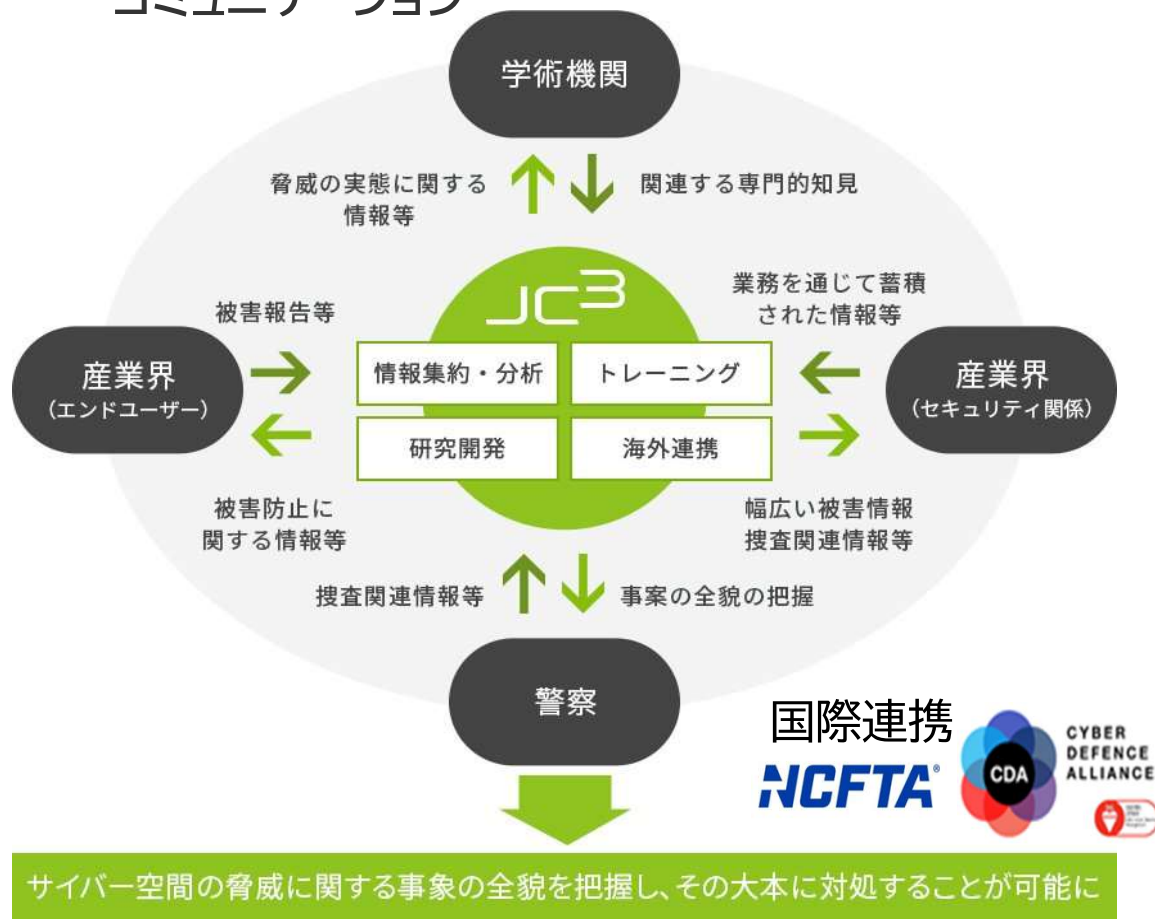
# JC3 御賛同いただいている企業・機関・研究者の方々②

正会員等 特定会員 賛同会員 賛助会員  
※：親子会社特例制度利用企業 (敬称略)  
2026年2月

投影限り

# JC3と官(法執行機関)、民(産業界)、学術機関の連携

産業界と警察との相互理解を深めるための双方向  
コミュニケーション

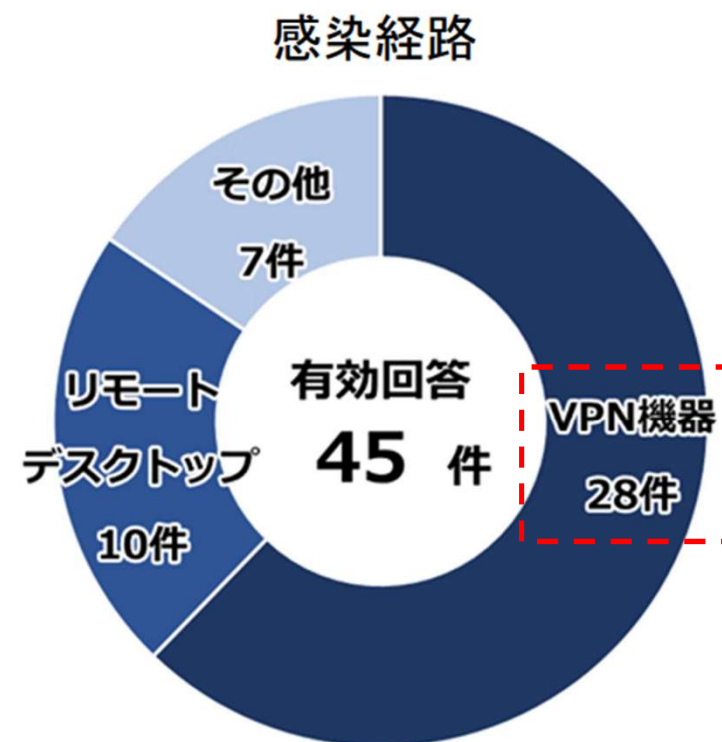
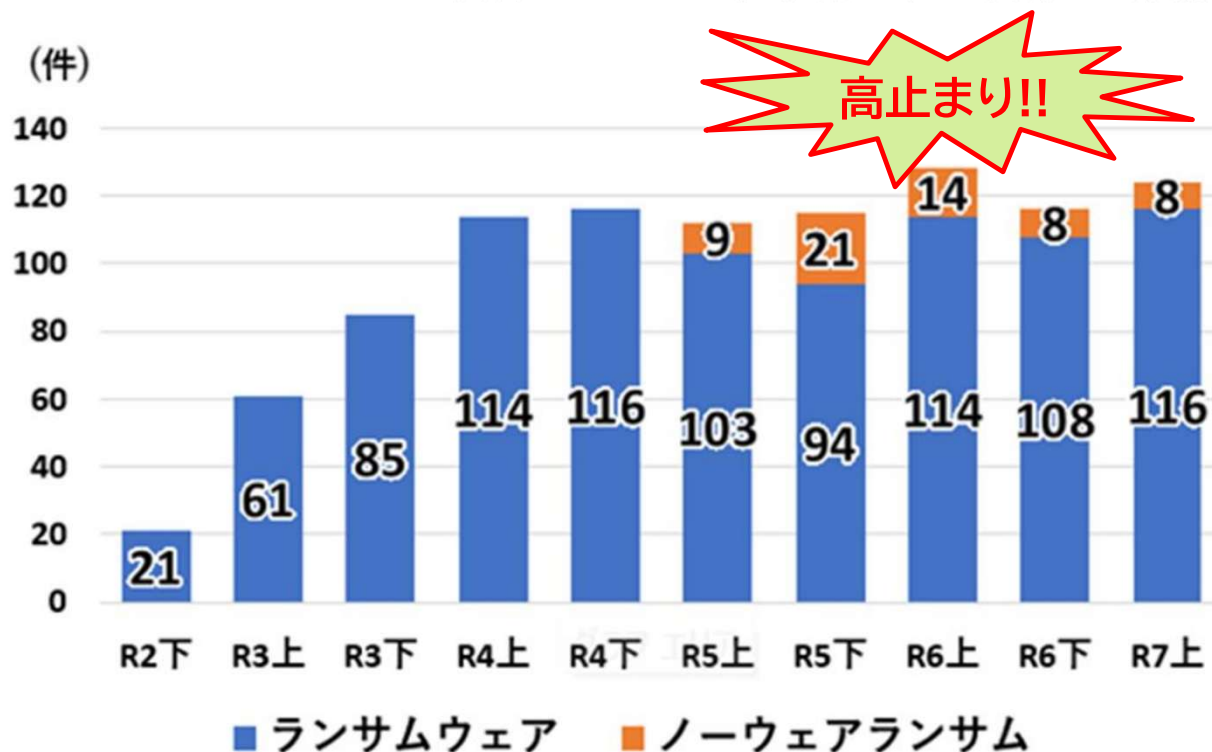


# ランサムウェアに関する統計情報

ランサムウェア

企業・団体等における被害の報告件数の推移

※ノーウェアランサムの被害については、令和5年上半期から集計。

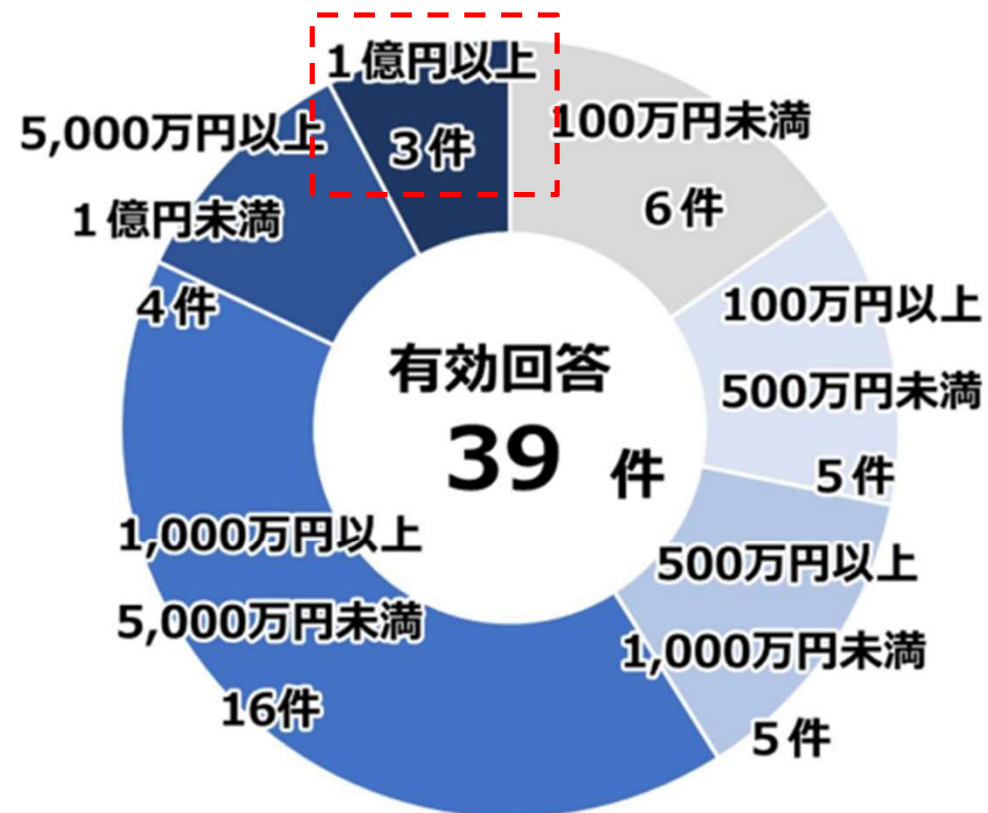
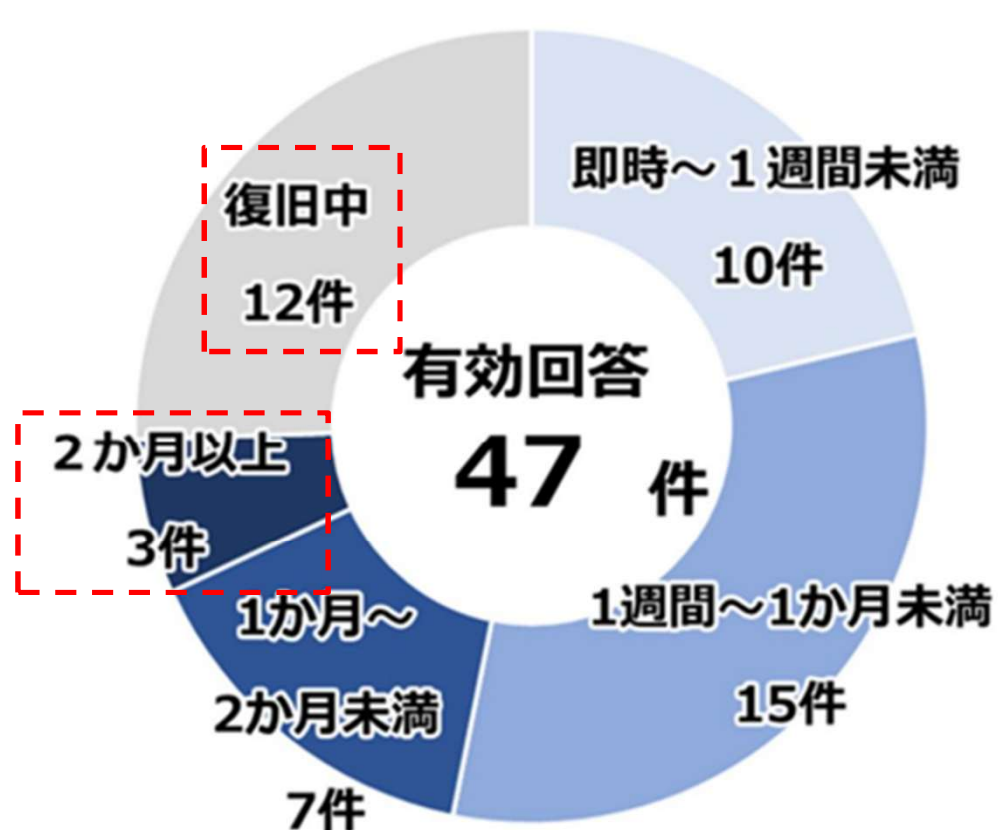


警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」

[https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07\\_kami\\_cyber\\_jyosei.pdf](https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf)

# ランサムウェアに関する統計情報

- 復旧等に要した期間／調査費用の総額／復旧期間と費用の関係性

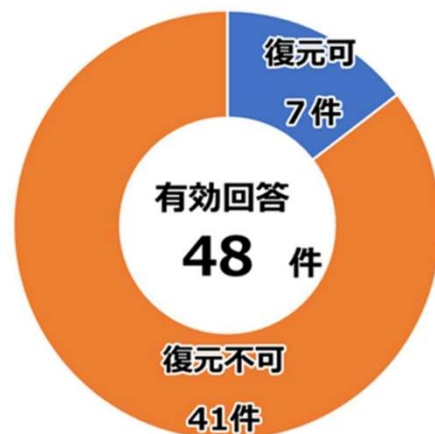
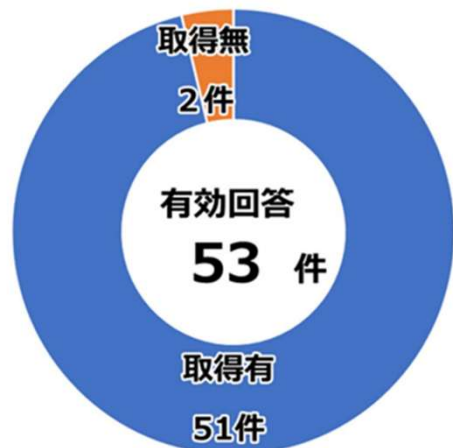


警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」

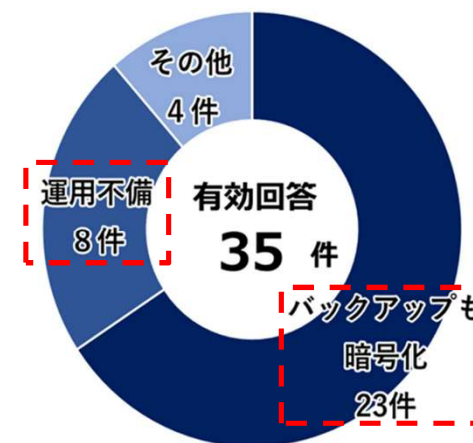
[https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07\\_kami\\_cyber\\_jyosei.pdf](https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf)

# ランサムウェアに関する統計情報

## ● バックアップの取得状況/バックアップからの復元結果



## バックアップから復元できなかった理由



## 推奨するバックアップ方法

### 3-2-1ルール

データをバックアップする際に推奨される運用ルールの一つ。  
「3つの複製を用意」  
「2つの異なる媒体に保存」  
「1つは地理的に離れた場所に保存」

更に推奨

### 3-2-1-1-0ルール

「3-2-1ルール」に加え、さらに  
「1つは変更不能またはコンピュータやネットワークをインターネットなどの外部ネットワークから物理的に完全に隔離する環境で保管」  
「常に復元可能(0個のエラー)であることを保証」

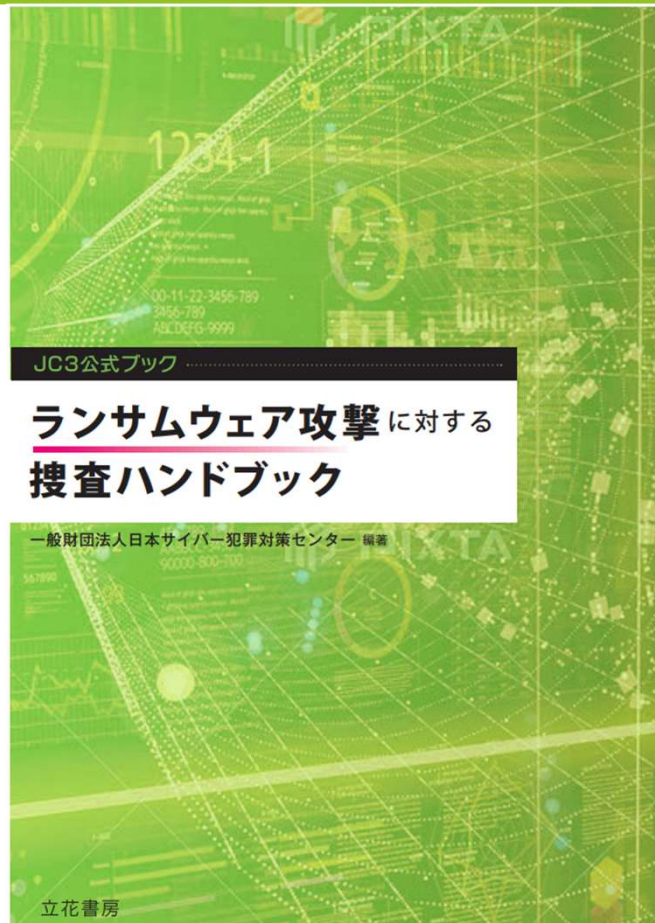
IT用語辞典e-Words「3-2-1ルール」  
<https://e-words.jp/w/3-2-1ルール.html>

# ランサムウェア攻撃に対する捜査能力の向上に向けて書籍を出版

ランサムウェア

## 書籍内容(大項目のみ)

- 1 本書について
  - 2 ランサムウェア攻撃
  - 3 捜査全般の留意事項
  - 4 捜査体制の確保
  - 5 平時における準備
  - 6 事案の認知
  - 7 緊急参集、現場臨場
  - 8 事情聴取
  - 9 状況把握
  - 10 被害法人への助言
  - 11 資料収集の考え方
  - 12 ファスト・フォレンジック
  - 13 刑罰法令
  - 14 参考文献
- (付録)



JC3 公式ブック

### ランサムウェア攻撃に対する 捜査ハンドブック

一般財団法人日本サイバー犯罪対策センター 編著

JC3 日本サイバー犯罪対策センター

プロフィール  
サイバー空間の脅威を特定、軽減及び無効化するための産学官(民間企業、学術研究機関、法執行機関)連携の非営利団体

主要目次  
Chapter1 本書について  
Chapter2 ランサムウェア攻撃  
Chapter3 捜査全般の留意事項  
Chapter4 捜査体制の確保  
Chapter5 平時における準備  
Chapter6 事案の認知  
Chapter7 緊急参集、現場臨場  
Chapter8 事情聴取  
Chapter9 状況把握  
Chapter10 被害法人への助言  
Chapter11 資料収集の考え方  
Chapter12 ファスト・フォレンジック  
Chapter13 刑罰法令  
Chapter14 参考文献

2024年3月刊行  
定価3,850円  
(本体3500円+税10%)  
ISBN:978-4-8037-4296-1  
A5判 226頁

このような方にお薦めです  
サイバー犯罪捜査員/サイバー犯罪対応担当者/セキュリティリサーチャー/セキュリティインシデント担当者/社内セキュリティ担当者/セキュリティコンサルタント/法務担当者

これからランサム事案対応に関わるすべての方へ  
ランサムウェアの捜査視点を知れる書籍の登場  
いざというときに何が求められるのか把握できる一冊

ご購入は3つのご注文方法からお申込みください

- 1 Amazonにてご注文  
通販サイト Amazon にて  
お買い求めください。  
<https://www.amazon.co.jp>
- 2 全国書店にてご注文  
2024年3月1日以降に  
このチラシを書店へ  
ご持参の上、ご注文ください。
- 3 立花書房にてご注文  
下記必要事項をご記入の上、  
FAX でお送りください。  
FAX: 03-3233-2871  
※書籍送料: 500円(税込)

貴社の個人情報取扱いに同意の上、申し込みます。  
ランサムウェア攻撃に対する捜査ハンドブック ご注文部数 部

お名前  
(会社名/団体名/部署名)

お届け先  
ご住所

お電話番号

立花書房  
〒101-0052 東京都千代田区神田小川町3丁目28番地2  
TEL: 03-5259-8856(平日10:00~16:00) FAX: 03-3233-2871  
HP: <https://tachibanashobo.co.jp>

警察による犯人検挙に向けた証拠保全能力の向上が目的ですが、被害発生時に企業側が取るべき対応や、警察からの助言についても言及しています。  
「万が一」に備えるための一冊です。

# ランサムウェア攻撃への対応を、カードゲームで学ぼう！

～キャット&チョコレート～

ランサムウェア

ランサムウェア被害に遭った際の対応についての訓練を、カードゲーム形式で行います。ゲームを通じて、企業における被害発生時に企業、警察等、それぞれの立場における対応方策を検討し合うことで、

- 企業のセキュリティ上の課題への気づき
- 企業、警察間の相互理解
- ランサム被害時の対応力強化

を高めましょう。

カードゲームセットは、**JC3のWebサイトからダウンロードも可能です。**



【入っているもの】カード70枚(ホワイトカード2枚含む)/  
遊び方ガイド(本書)

**ロールカード 2枚**



**キーワードカード 38枚**



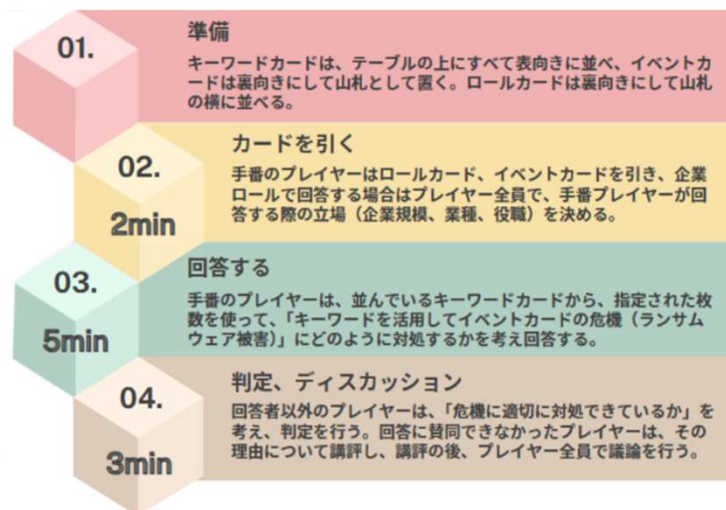
**チームカード 6枚**



**イベントカード 22枚**



## ●進行フローチャート



サイバー犯罪に立ち向かう

## JC3 Podcast

日本サイバー犯罪対策センター

# ランサムウェア・ダイアログ

絶賛配信中!!

ランサムウェアの脅威に  
最前線で立ち向かう  
専門家たちとの対話を通じて  
サイバーセキュリティ対策を考えていく  
ポッドキャストです

### Contents

- Prologue 【JC3について】
- Ep.1 【サイバー犯罪捜査官からみたランサムウェア対策】
- Ep.2 【バックアップと復旧計画】
- Ep.3 【ランサムウェアに関する各種法令と企業  
・組織が考慮すべきこと】
- Ep.4 【医療機関におけるランサムウェア対策】
- Epilogue 【専門家たちの「対話」を振り返る】

JC3 Japan Cybercrime Control Center

JC3 ポッドキャスト

### Listen On

Spotify

Listen on Apple Podcasts

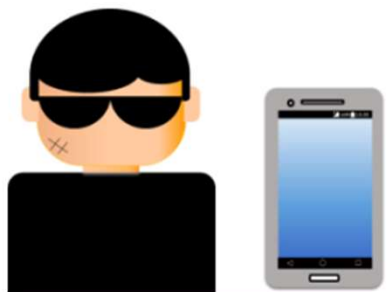
YouTube

令和7年11月に、ボイスフィッシング(ビッシング)による不正送金被害が急増しました。

## 企業の法人口座を狙う、その手口とは？

1. 犯人が銀行関係者をかたり、企業に電話をかけ、メールアドレスを聴取する
2. メールを送信して偽サイトに誘導し、ネットバンクの認証情報等を入力させる
3. 犯人は認証情報等を利用し、法人口座から企業の資産を不正送金する

※架電イメージ



犯人

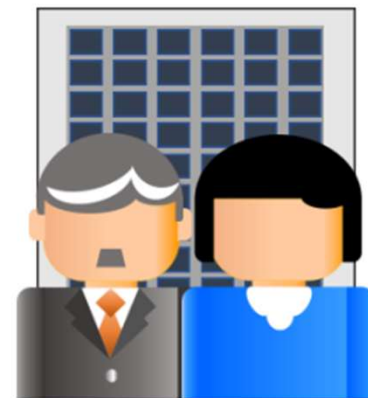
### ①電話（自動音声）

〇〇銀行です。ネットバンクの顧客情報の更新手続きが必要です。■番を押してください

### ②自動音声に従い番号押下

### ③電話（犯人の声）

顧客情報の更新用リンクを送るので、メールアドレスを教えてください



被害企業  
担当者

## どう見分ける？こんな電話は偽物！

- 発信元番号が**国際電話**（+国番号）である（例：**+1 800** 123 4567）
- **自動音声ガイダンス**が流れたのち、人間の声に切り替わる
- 通話中に**メールアドレスを聴取**され、リンク付きメールが送られる

## 社内で徹底！被害を防ぐために

- 銀行から電話があれば、営業店・代表電話に折り返し、本物かどうか確認する
- インターネットバンキング利用時は、銀行公式サイト・アプリからアクセスする

# ボイスフィッシングに関する警察庁からの注意喚起

ボイスフィッシング

**サイバー警察局便り**  
Cyber Police Agency Letter 2024(R6) Vol.15

**今、企業の資産（法人口座）がねらわれている！！**

**電話に注意！「ボイスフィッシング」による不正送金被害が急増**

【手口の概要】

1. 犯人が銀行担当者を騙り、被害者（企業）に電話をかけ（自動音声の場合あり）、メールアドレスを聞き出す。
2. 犯人がフィッシングメールを送信し、電話で指示しながら、被害者をフィッシングサイトに誘導。そして、インターネットバンキングのアカウント情報等を入力させて、盗み取る。
3. フィッシングサイトに入力させたアカウント情報等を使って、犯人が法人口座から資産を不正に送金する。

※架電イメージ

〇〇銀行です。ネットバンクの電子証明書の更新手続きが必要です。更新用のリンクを送りますのでメールアドレスを教えてください。

**ボイスフィッシング被害に遭わないために！3つの対策**

- ◆ 知らない電話番号からの着信は信用しない！
- ◆ 銀行の代表電話番号・問い合わせ窓口で確認する！！  
銀行担当者を騙る者から連絡があった場合には、銀行の代表電話番号へ連絡して確認するなど、慎重に対応してください。
- ◆ メールに記載されているリンクからアクセスしない！！  
インターネットバンキングにログインする場合は、銀行公式サイトや公式アプリからアクセスしてください。

**もしも、被害に遭ってしまったら警察に通報・相談を！**  
最寄りの警察署又はサイバー犯罪相談窓口 → <https://www.npa.go.jp/bureau/cyber/consult.html>

JBA 一般社団法人 全国銀行協会 | 金融庁 Financial Services Agency | 警察庁 National Police Agency | JC3 日本サイバー犯罪対策センター

(令和6年12月)

**サイバー警察局便り**  
Cyber Police Agency Letter 2025 Vol.1 (R7.4)

**銀行から電話…はたして本物？ 企業の資産が危ない！**

**電話を利用する「ボイスフィッシング」被害が引き続き発生中**

- 昨年より、ボイスフィッシング（ピッシング）による法人口座を狙った不正送金被害が継続して発生している
- 全国的に被害拡大しており、1社あたり数億円規模の被害も確認されている

**企業の資産（法人口座）を狙う手口は？**

1. 犯人が銀行関係者をかたり、企業に電話をかけ、自動音声ガイダンスを流す。音声に従い番号を押すと、犯人に切り替わる（始めから犯人が電話することもある）
2. メールアドレスを聴取し、フィッシングメールを送信。メール記載のリンクから偽サイトに誘導し、インターネットバンキングのアカウント情報等を入力させる
3. 犯人はアカウント情報等を利用し、法人口座から資産を不正送金する

※架電イメージ

①電話（自動音声）  
〇〇銀行です。ネットバンクの顧客情報の更新手続きが必要です。■番号を押してください

②自動音声に従い番号押下

③電話（犯人の声）  
顧客情報の更新用リンクを送るので、メールアドレスを教えてください

**どう見分ける？こんな電話は偽物の可能性大！**

- 発信元番号が国際電話（+（国番号））、または非通知となっている
- 自動音声ガイダンスが流れたのち、人間の声に切り替わる
- 通話中にメールアドレスを聴取され、リンク付きメールが送られる

**社内で徹底！被害を防ぐために**

- ◆ 銀行から電話があれば、本物かどうか確認する  
上記に該当する特徴がみられた場合はいちど切電し、営業店・代表電話に確認してください
- ◆ メールに記載されているリンクからアクセスしない  
インターネットバンキング利用時は、銀行公式サイト・アプリからアクセスしてください

**もしも、被害に遭ってしまったら警察に通報・相談を！**  
最寄りの警察署又はサイバー犯罪相談窓口 → <https://www.npa.go.jp/bureau/cyber/consult.html>

JBA 一般社団法人 全国銀行協会 | 金融庁 Financial Services Agency | 警察庁 National Police Agency | JC3 日本サイバー犯罪対策センター

(令和7年4月)

**サイバー警察局便り**  
Cyber Police Agency Letter 2025 Vol.12 (R7.12)

**その電話、本当に銀行からですか？**

**電話を利用する「ボイスフィッシング」被害が再び発生**

ボイスフィッシングによる法人口座を狙った不正送金被害が再発・急増している。

**企業の法人口座を狙う、その手口とは？**

1. 犯人が銀行関係者をかたり、企業に電話をかけ、メールアドレスを聴取する
2. メールを送信して偽サイトに誘導し、ネットバンクの認証情報等を入力させる
3. 犯人は認証情報等を利用し、法人口座から企業の資産を不正送金する

※架電イメージ

①電話（自動音声）  
〇〇銀行です。ネットバンクの顧客情報の更新手続きが必要です。■番号を押してください

②自動音声に従い番号押下

③電話（犯人の声）  
顧客情報の更新用リンクを送るので、メールアドレスを教えてください

**どう見分ける？こんな電話は偽物！**

- 発信元番号が国際電話（+国番号）である（例：+1 800 123 4567）
- 自動音声ガイダンスが流れたのち、人間の声に切り替わる
- 通話中にメールアドレスを聴取され、リンク付きメールが送られる

**社内で徹底！被害を防ぐために**

- 銀行から電話があれば、営業店・代表電話に折り返し、本物かどうか確認する
- インターネットバンキング利用時は、銀行公式サイト・アプリからアクセスする

**詐欺電話対策として「国際電話着信ブロック」もあります**  
みんなでとめよう！国際電話詐欺 → [https://www.npa.go.jp/bureau/safetylife/sos47/case/international\\_phone/](https://www.npa.go.jp/bureau/safetylife/sos47/case/international_phone/)

**もしも、被害に遭ってしまったら警察に通報・相談を！**  
最寄りの警察署又はサイバー犯罪相談窓口 → <https://www.npa.go.jp/bureau/cyber/consult.html>

JBA 一般社団法人 全国銀行協会 | 金融庁 Financial Services Agency | 警察庁 National Police Agency | JC3 日本サイバー犯罪対策センター


(令和7年12月)

# CEO(Chief Executive Officer)詐欺

CEO詐欺

## 【重要】社長・役員を装う「LINEグループ作成依頼」メールによる詐欺にご注意ください

LINE

共有する 

ヘルプセンター

更新日：2026年1月15日

最近、社長や役員などになりすましたメールを従業員へ送り、取引指示を装ってLINEのグループトークへ誘導し、金銭を騙し取る詐欺が確認されています。  
少しでも違和感を覚えたら、すぐにやり取りを中止してください。

### ▲ 重要

- ✓ 送金や緊急対応を求められたら、メール以外（電話や対面など）の手段で必ず本人や上司に確認してください。
- ✓ 不審なメッセージを受け取った場合は、該当メッセージを通報してください。

LINEヤフー株式会社「【重要】社長・役員を装う「LINEグループ作成依頼」メールによる詐欺にご注意ください」  
<https://help.line.me/line/smartphone?contentId=200002034&lang=ja>

## よくある手口

- 「【至急】グループ作成依頼」など緊急性の高い件名でメールが届く
- 「LINEグループを作成し、QRコードを送って」と求められる
- 「他の人は入れないで」と口止めされる
- LINE上で「残高のスクリーンショット」「取引先への支払い」などを理由に、口座情報の提出や振込を求められる

LINEヤフー株式会社「【重要】社長・役員を装う「LINEグループ作成依頼」メールによる詐欺にご注意ください」  
<https://help.line.me/line/smartphone?contentId=200002034&lang=ja>

# CEO(Chief Executive Officer)詐欺

CEO詐欺

⚠ 被害を防ぐために、今すぐできること ⚠

- メールでLINEのグループトーク作成／QRコード送信を依頼された場合、メールへは返信せず別の手段で本人に確認してください。
- 不審なLINEのグループトークを通じて振り込みを指示された場合は、メールやLINEとは別の手段にて本人や上司に報告してください。
- 口座情報・個人情報・残高スクショなどを送らないでください。

LINEヤフー株式会社「【重要】社長・役員を装う「LINEグループ作成依頼」メールによる詐欺にご注意ください」  
<https://help.line.me/line/smartphone?contentId=200002034&lang=ja>

# 代表理事を騙ったメールがJC3にも届きました。

CEO詐欺

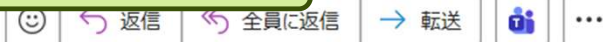
一般財団法人日本サイバー犯罪対策センター

明らかに怪しいメールアドレス



中谷 昇 <styvelastolbnfqa0@outlook.com>

宛先 info



2026/01/08 (木) 10:09

ホームページに公開されているアドレス

お疲れ様です。

本メールを受信されましたら、今後の業務プロジェクト対応のため、新しい LINE のワークグループを作成していただけますでしょうか。

グループ内の他のメンバーの追加につきましては、私が参加した後にこちらで別途手配いたします。

グループ作成が完了しましたら、当該グループの招待用 QR コード（または招待リンク）を発行のうえ、本メールにご返信ください。

私が QR コードからグループに参加し、その後の業務調整を進めさせていただきます。

代表取締役社長

肩書が異なる

中谷 昇

ホームページからのコピーと思われる

一般財団法人日本サイバー犯罪対策センター

# フィッシングとは

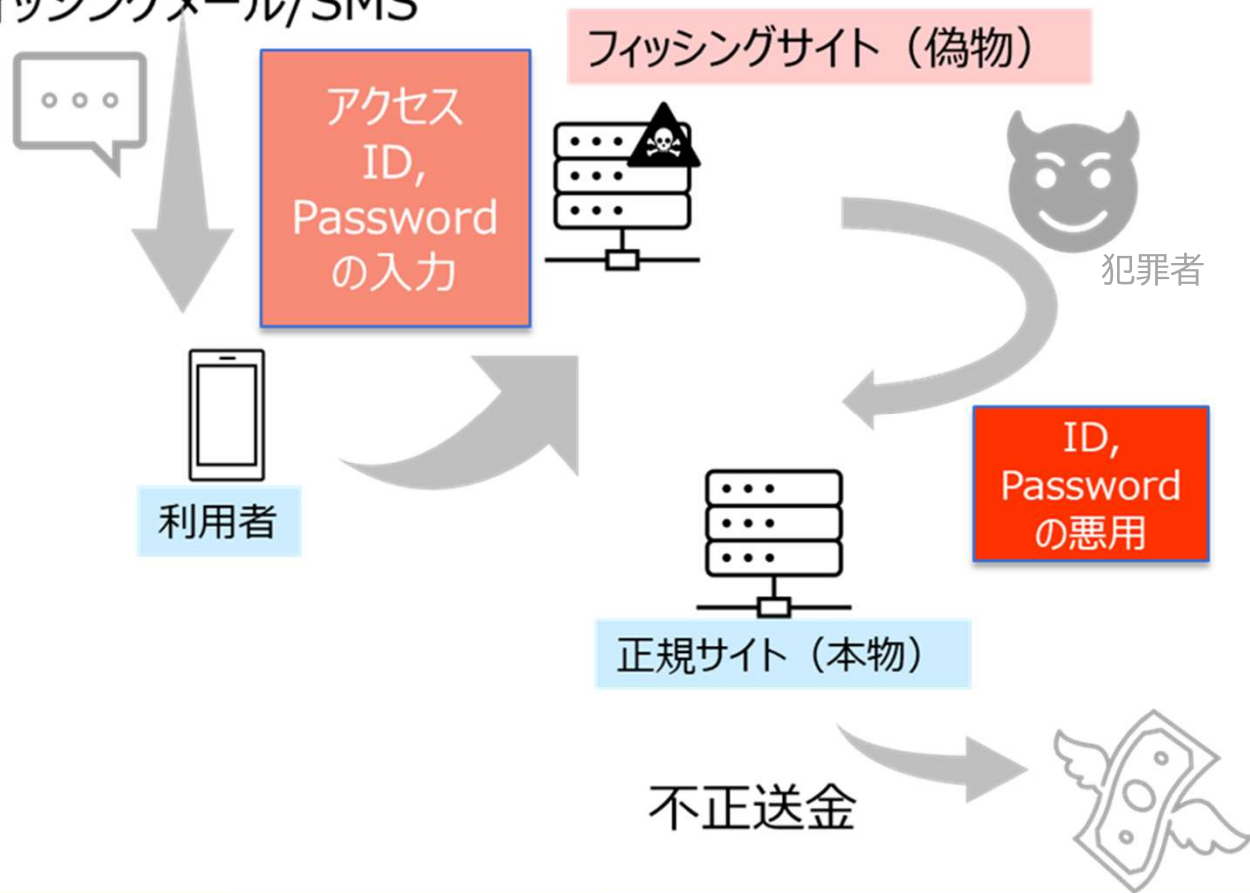
実在のサービスや企業をかたり、偽のメールやSMS（携帯電話のショートメッセージ）で偽サイトに誘導し、IDやパスワードなどの情報を盗んだり、マルウェアに感染させたりする手口です。

情報を盗まれると、アカウントを乗っ取られてお金を奪われたり、インターネット通信販売サイトで勝手に買物をされたりします。また、マルウェアに感染してしまうと、スマートフォンに登録された電話帳の情報が盗まれたり、自分のスマートフォンがフィッシングSMSの発信源になってしまうこともあります。

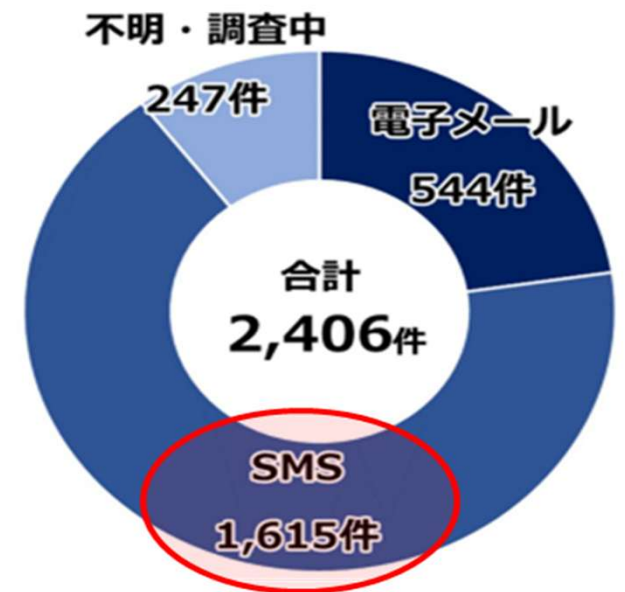
# フィッシングによる不正送金の手口

## ■ フィッシング(Phishing)による情報の窃取

フィッシングメール/SMS



フィッシングサイトへ誘導する  
手口別の不正送金発生件数  
(令和7年上半期)



# 情報を入力させる偽画面

フィッシング

The image shows two examples of phishing pages. The left page is a login page titled 'ログインはこちらから' (Login from here). It contains fields for '会員ID' (Member ID), 'パスワード' (Password), and 'ご利用者の生年月日' (User's date of birth) with dropdown menus for year, month, and day. Below these is an image-based CAPTCHA with the text '3wmm26' and instructions to click on different characters. A green 'ログイン' (Login) button is at the bottom. The right page is titled 'お支払い方法の更新' (Update payment method) and features logos for VISA, Mastercard, American Express, Discover, JCB, and UnionPay. It includes fields for 'クレジットカード名義人' (Credit card name), 'カード番号' (Card number), '有効期限' (Expiration date) with dropdowns for month and year, 'セキュリティコード' (Security code) with a CVV/CW2 field, and '生年月日' (Date of birth) with dropdowns for day, month, and year.

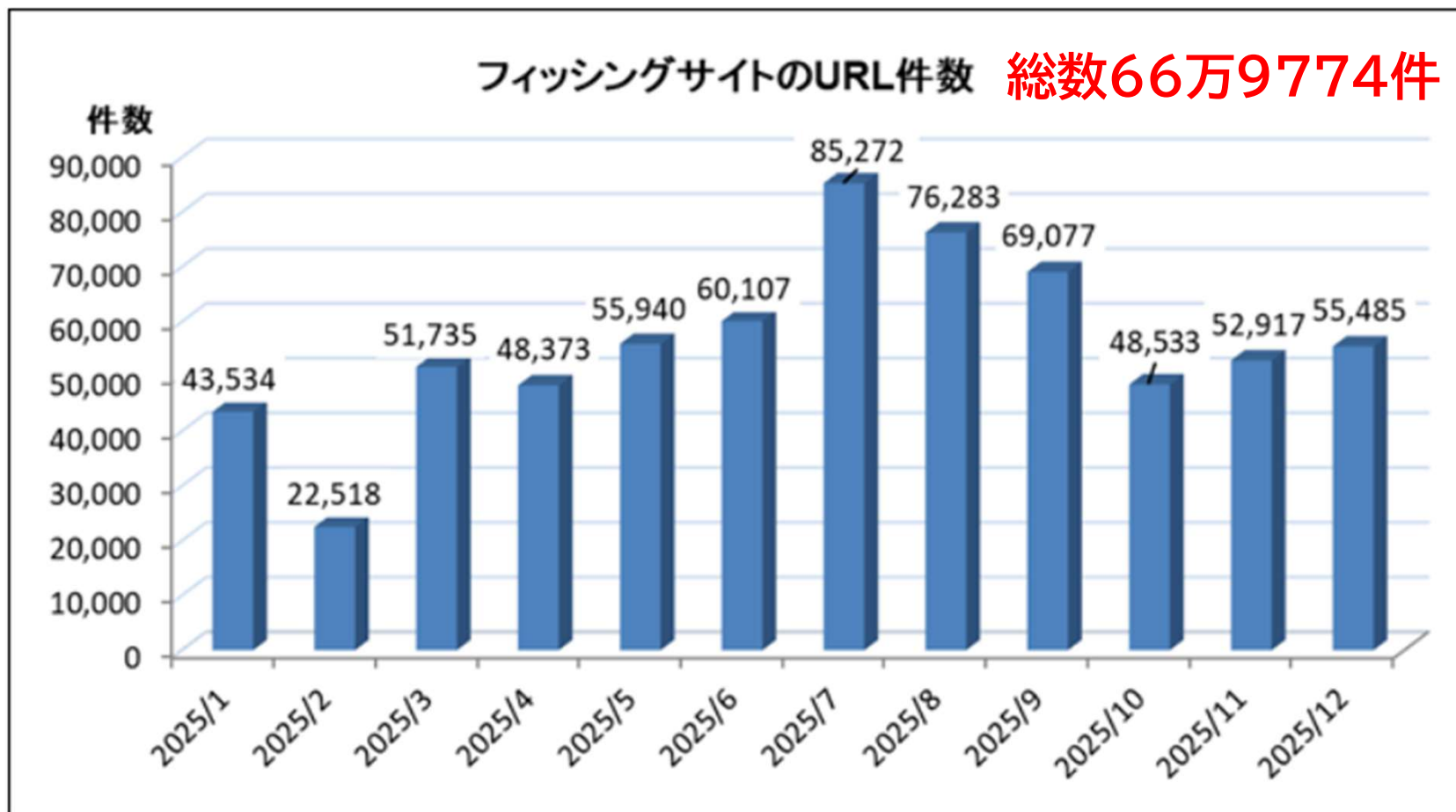
実在する金融機関、通信事業者等のログイン画面や支払いページを模した偽画面の例

## <入力を求められる情報の例>

- 金融機関の口座番号、クレジットカード番号、暗証番号（ワンタイムパスワード、乱数表の番号等）
- 住所、氏名、電話番号、生年月日
- 電子メール、インターネットバンキング、SNSアカウント等のID、パスワード等
- 運転免許証、マイナンバーカード、乱数表等の画像情報

# 令和7年に報告のあったフィッシングサイトのURL件数

フィッシング



フィッシング対策協議会「2025/12 フィッシング報告状況」  
<https://www.antiphishing.jp/report/monthly/202512.html>

# JC3によるフィッシングの注意喚起

フィッシング

## JC3のホームページで「フィッシング」と検索した結果(一部のみ掲載)

### SMSによるフィッシングサイトへの誘導(iPhone)(動画解説) | 脅威情報

一般財団法人日本サイバー犯罪対策センター (JC3) › TOP › 脅威情報 › 脅...  
運送系企業を騙ったSMSによりフィッシングサイトへ誘導され、インターネットバンキングのパスワード等の情報が窃取されることにより、不正送金が行われる手口による被害が ...

### SMSによるフィッシングサイトへの誘導(Android)(動画解説) | 脅威情報

一般財団法人日本サイバー犯罪対策センター (JC3) › TOP › 脅威情報 › 脅...  
運送系企業を装ったSMSからフィッシングサイトへ誘導され、インターネットバンキングのパスワード等の情報が窃取されることにより、不正送金が行われる手口による被害が ...

### フィッシングによる不正送金の被害に注意 | トピックス | 脅威情報

一般財団法人日本サイバー犯罪対策センター (JC3) › TOP › 脅威情報 › ト...  
フィッシングによる不正送金の被害に注意. JC3では、警察、会員企業と連携し、銀行を騙ったフィッシングによる不正送金の被害が急増していることを確認しており、個人情報 ...

### 通信事業者を装ったフィッシングの注意喚起 | トピックス | 脅威情報

一般財団法人日本サイバー犯罪対策センター (JC3) › TOP › 脅威情報 › ト...  
2021/08/10 ... 今後も様々な文面によりフィッシングサイトへ誘導し、個人情報の窃取等が懸念されますので、今回紹介する文面に限らずフィッシングメール/SMSについて注意 ...

### 警察庁を騙るフィッシングに注意 | トピックス | 脅威情報

一般財団法人日本サイバー犯罪対策センター (JC3) › TOP › 脅威情報 › ト...  
警察庁を騙るフィッシングに注意. 6月26日、インターネット上において、警察庁を騙るSMSが確認されました。同SMSは、銀行への認証の設定を促す内容となっており、リンクを ...

### 不正アプリによる銀行を騙ったフィッシングサイトへの誘導 | 脅威情報

一般財団法人日本サイバー犯罪対策センター (JC3) › TOP › 脅威情報 › ト...  
不正アプリによる手口. 現時点においてJC3で確認できた手口として、不正アプリがインストールされたAndroidスマートフォンに銀行のアプリケーションが入っている場合、銀行 ...

### 運送系企業を装ったフィッシングの注意喚起 | トピックス | 脅威情報

一般財団法人日本サイバー犯罪対策センター (JC3) › TOP › 脅威情報 › ト...  
JC3では、佐川急便の偽サイトに関する調査を継続していたところ、この度、新たに、日本郵便を装ったSMSと同社を装った偽サイトを確認しました。また、他の運送系企業を ...

### 様々な金融機関等を狙ったフィッシング | トピックス | 脅威情報

一般財団法人日本サイバー犯罪対策センター (JC3) › TOP › 脅威情報 › ト...  
被害に遭わないために・事前に正しいウェブサイトのURLをブックマークに登録して、ブックマークからアクセスする・各金融機関等のウェブサイトにおいて掲載されている ...

# JC3に送られてきたフィッシングメール

フィッシング

Amazon.co.jp

amazon.co.jpを騙っている



プライム会員資格に関する重要なお知らせ <Amazon-mail@trianglefabrics.com>

宛先 [join@jc3.or.jp](mailto:join@jc3.or.jp)

amazon.co.jpからではない

2026/02/12 (木) 9:34

ホームページに公開されているアドレス

プライム会員資格に関する重要なお知らせ

「AMAZON」の字体がおかしい

お客様の Amazon プライム会員資格は、2026年2月15日に更新予定ですが、現在お支払い情報に問題があるため、更新処理が完了していません。

このままではプライム会員資格が一時停止となる可能性があります。

お支払い失敗の主な原因：

- \* クレジットカードの有効期限切れ
- \* カード残高不足
- \* カード情報の入力ミス
- \* カード会社の承認拒否

3日以内にお支払い方法をご確認・更新いただく必要があります。

⚠ 48時間以内にご対応がない場合、アカウント機能の一部が制限される可能性があります。

お支払い方法を更新する <[アクセス先がamazon.co.jpではない](https://click.federicoriva.com/?qs=eyJkZWtjZCI6IjYzc5OGE5LWZiNTItNDNlMC05NTA4LTczLWZlZjZmNjJmSisimKia1ZicmNpb24iOjE5imZlZjoiS2pwcXQyemF5NGtaWjNaelRRYlpXUT09liwiY2lwaGVyVGV4dCI6Im9JU1FGekd5VEJqd1INSzdQK0lRlpGQkM4dnB5VTRuNk5tSkh3TUFlkV0NUTUlXR2Q4dUpGU0s4Wkoza3RBZFpNSXU1TVp2TGk1clBHcDJUbtRZOUmZeDhYbnUycjhLUzFIT3BNS1Z5S2pWcXUyemF5NGtaWjNaelRRYlpXUT09liwiYXV0aFRhZyl6IIBRdDhmRjU3dHEvQ2t0WGpxVENsY2c9PSJ9></a>></p></div><div data-bbox=)

# (参考)個人情報を狙った犯罪～インフォステイラー～

「証券口座乗っ取り」が発生する主な原因として、

フィッシング

インフォステイラー

の二つが存在すると考えられています。

インフォステイラーとは、「情報窃取専用」のトロイの木馬型不正プログラムです。

感染したPCやスマートフォンからブラウザに保存されたID・パスワードやセッションCookieなどの認証情報を短時間で外部サーバへ送信します。

一般的に画面に目立つ兆候を残さず、利用者は感染に気付きにくいという特徴があります。

感染手法の一つとして、攻撃者は画面に「私はロボットではありません」といった偽CAPTCHAを示し、その操作によって悪意あるPowerShellコマンド実行を誘導することでインフォステイラーの感染に導きます。

トレンドマイクロ「多要素認証でも防げない」証券口座乗っ取りにどう備えるか？  
プロアクティブセキュリティの視点で考える」

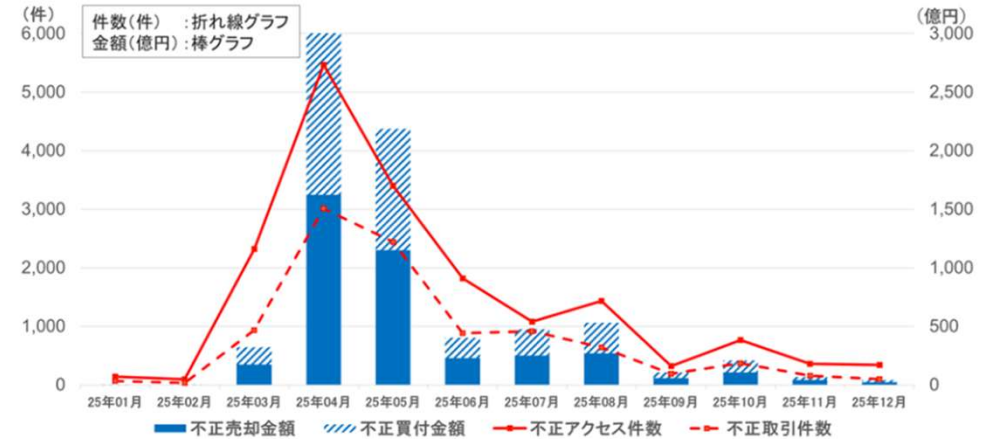
<https://www.trendmicro.com/ja-jp/research/25/g/proactive-security-against-account-takeover.html>

認証情報だけでなく、クレジットカード情報等、様々な個人情報が狙われています!!

インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています



○ 実在する証券会社のウェブサイトを使った偽のウェブサイト（フィッシングサイト）等で窃取した顧客情報（ログインIDやパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。



金融庁「インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています」  
[https://www.fsa.go.jp/ordinary/chuui/chuui\\_phishing.html](https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html)

# (参考)個人情報を狙った犯罪～インフォステイラー～

なぜ、**インフォステイラー** に感染するのか。

**クリックフィックス** によって感染させられてしまう。

クリックフィックスは、ソーシャルエンジニアリングのひとつの手口です。

攻撃者がブラウザ上などで偽のエラー画面や偽CAPTCHA認証画面を表示し、「解決するには(ボットではないことを証明するには)このステップを実行してください」というようにユーザの操作を促す、というものです。

ユーザが疑問を持たずにそのとおりに操作すると、パソコンがマルウェアに感染してしまいます。

トレンドマイクロ「ClickFix(クリックフィックス)とは? 多様な攻撃に悪用されるソーシャルエンジニアリングの手口」  
<https://www.trendmicro.com/ja.jp/jp-security/25/i/securitytrend-20250905-01.html>

**サイバー警察局便り**  
Cyber Police Agency Letter 2025 Vol.7 (R7.10)

**「私はロボットではありません」偽画面に注意!**

**ウイルス感染の手口「ClickFix (クリックフィックス) 」とは**

▶パソコンなどの利用者を誘導し、利用者自身に不正コマンドを実行させるサイバー攻撃手口の一つである「ClickFix」を観測

▶メールなどから偽の認証画面に誘導。指示どおりに実行すると**ウイルスに感染**

**偽の認証画面の例**

ロボットですか、人間ですか?  
人間であることを確認するためにチェックボックスをオンにしてください。  
ありがとうございます!

クリックすることで不正コマンドをコピー

1. **Win+R**: 「ファイル名を指定して実行」欄を表示  
2. **Ctrl+V**: 不正コマンドを貼付  
3. **Enter**: 不正コマンドを実行

上記の操作によりウイルスに感染

確認ステップ  
1. **Win+R**を押す  
2. **Ctrl+V**を押す  
3. **Enter**を押す

**ウイルスに感染してしまうと…?**

ID・パスワードやデータを窃取されるほか、様々な攻撃を受ける原因に。

**BANK** インターネットバンキングやクレジットカードの不正利用

企業のシステムに侵入されランサムウェア被害

**被害を防ぐために押さえておくべきこと**

- ◆ 不審なメールなどのリンクをクリックしたり、不審な広告を開いたりしない
- ◆ 認証画面で指示された不審な操作を安易に実行しない

特に **Win+R** に注意!

企業システム担当者向け  
PowerShellなど悪用されがちな正規プログラムの実行監視や利用制限による対策をお願いします。

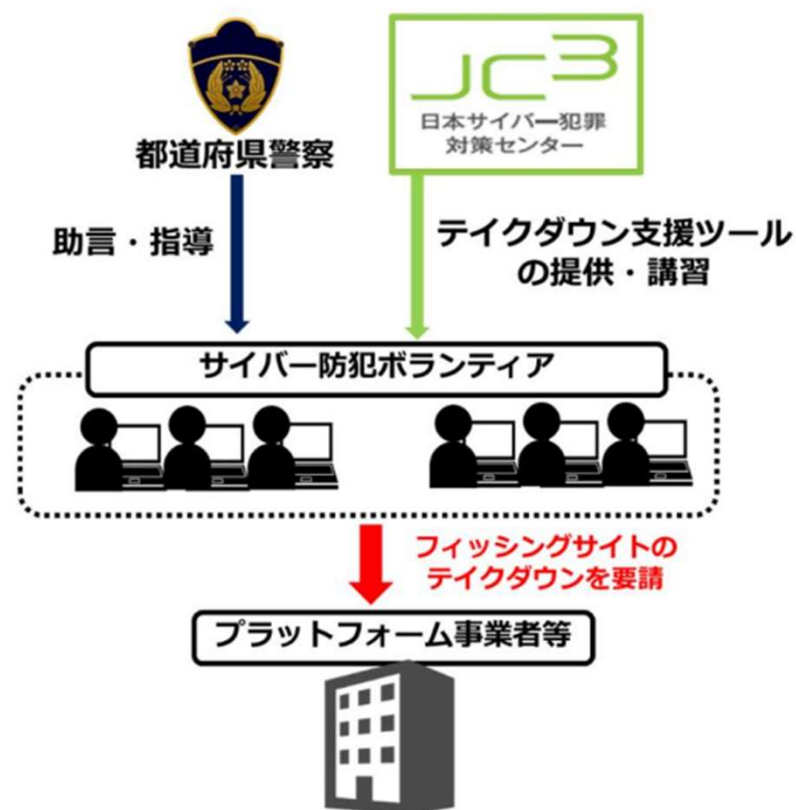
警察庁  
National Police Agency

# フィッシングサイト撲滅チャレンジカップ

フィッシング

フィッシングサイト対策として、  
JC3 では、専門的な知識を持たない人  
であってもプラットフォーム事業者等  
に対してサイトのテイクダウン依頼を  
行うことができるツールを開発し、サイ  
バー防犯ボランティア等に提供する  
とともに、警察庁後援のもと、サイバ  
ー防犯ボランティア向けの「フィッシ  
ングサイト撲滅チャレンジカップ」を  
実施している。

【図表 24: サイバー防犯ボランティア  
への支援】



警察庁ホームページ「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」より引用  
[https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07\\_kami\\_cyber\\_jyosei.pdf](https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf)

## <結果>

### ✓ 第1回(令和6年2月13日から20日)

参加ボランティア団体: **27団体**(参加者 **125名**)

大会結果: Abuse報告数 **9,319件**、テイクダウン数 **268件**

### ✓ 第2回(令和6年7月22日から29日)

参加ボランティア団体: **46団体**(参加者**359名**)

大会結果: Abuse報告数 **12,072件**、テイクダウン数 **2,201件**

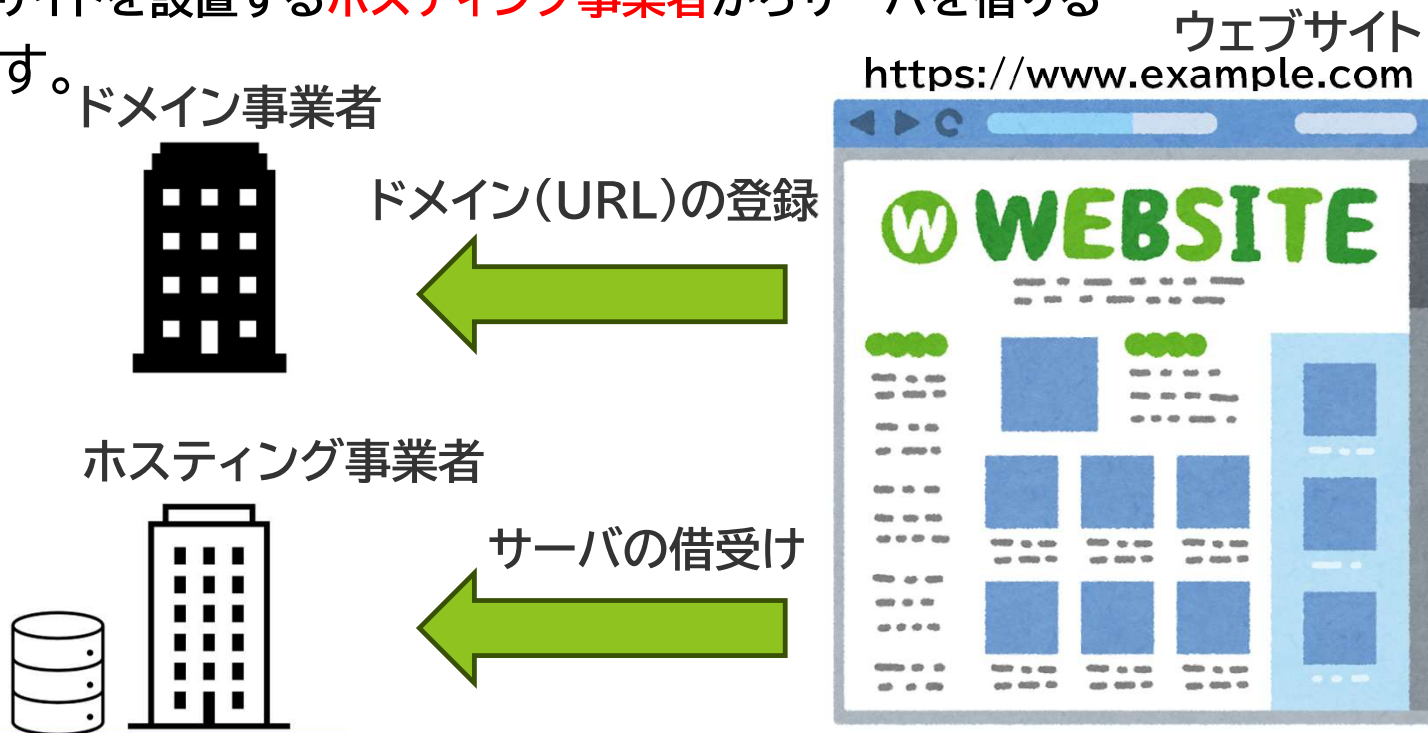
### ✓ 第3回(令和7年12月9日から15日、令和8年1月13日から19日)

参加ボランティア団体: **55団体**(参加者のべ**433名**)

大会結果: Abuse報告数 **16,234件**、テイクダウン数 **2,828件**

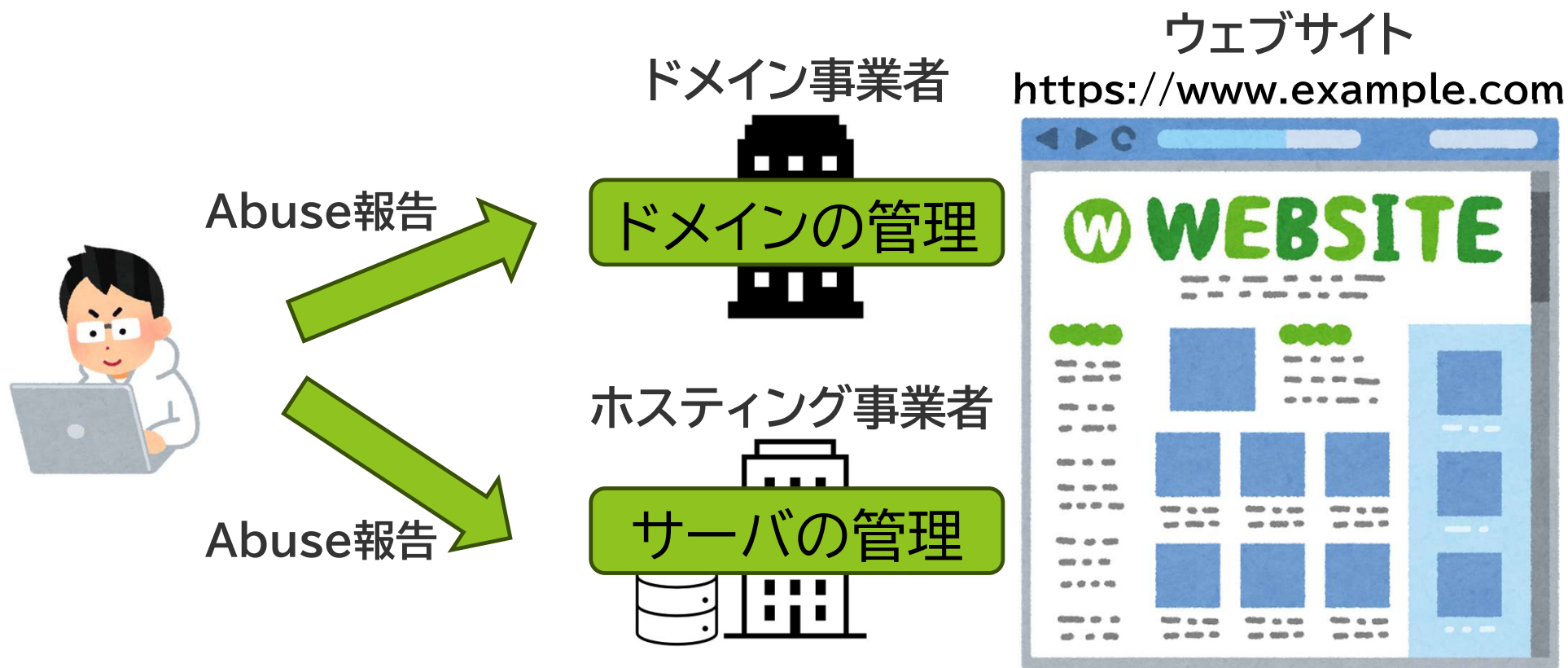
# (参考)Abuse報告について

- Abuse報告とは、コンピュータネットワーク上の迷惑行為について、事業者<sup>に</sup>報告することを言います。
- インターネット上にウェブサイトを構築する際は、
  - ドメイン名の登録・管理を行う**ドメイン事業者**を通じてドメイン(URL)の登録を行う
  - 実際のウェブサイトを設置する**ホスティング事業者**からサーバを借りる必要があります。



# (参考)Abuse報告について

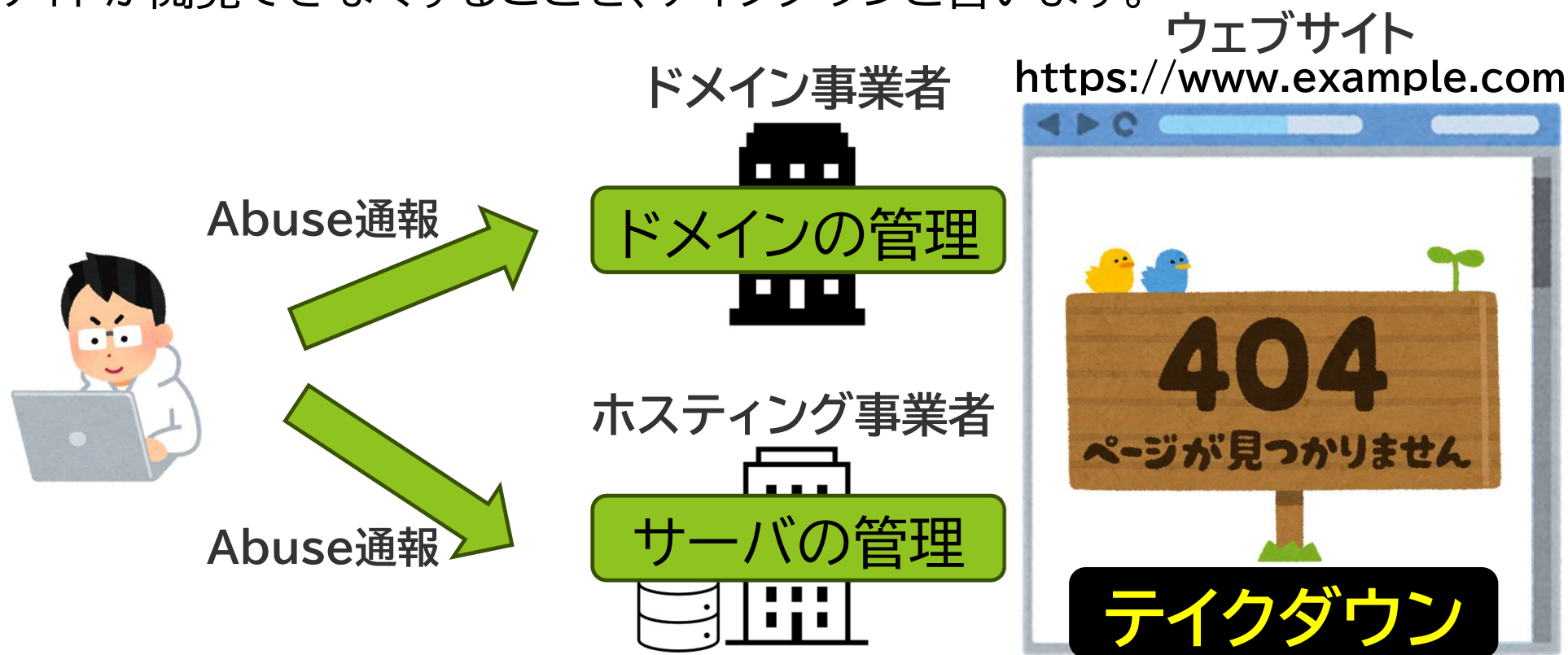
- Abuse報告は、「ドメイン事業者」「ホスティング事業者」のそれぞれに行います。



# (参考)Abuse報告について

- Abuse報告を受けた事業者は、ドメインやサーバの提供を止めて、サイトの閲覧ができないようにします。

サイトが閲覧できなくすることを、テイクダウンと言います。



あなたのスマートフォンが犯罪のインフラに(モバイルマルウェアによるSMS攻撃)

モバイルマルウェア

投影限り

# (参考)リアルタイム詐欺SMSモニター (トビラシステムズ株式会社)

モバイルマルウェア

## https://smon.tobila.com/

Androidマルウェア感染端末台数 (?)



詐欺SMSギャラリー

**国税庁** [注意喚起](#)

**NEW**

【国税庁】ご確認を要する事務連絡がございます。内容をご覧ください。[URL]

✕ [ポストする](#) 掲載日:2026年02月21日

**LINE** [注意喚起](#)

アカウントの利用制限がかかっています。すぐに制限を解除するには、専用リンクをクリックしてください。

[URL]

✕ [ポストする](#) 掲載日:2026年02月20日

**国税庁** [注意喚起](#)

【国税庁】確認を必要とする重要事項についての通知です。内容をご覧ください。[URL]

✕ [ポストする](#) 掲載日:2026年02月19日

**日本郵便** [注意喚起](#)

[郵便局]お荷物の配送に関して住所確認が必要です.再配達の手続きをこちらからお願いいたします:[URL]

✕ [ポストする](#) 掲載日:2026年02月18日

**日本郵便** [注意喚起](#)

[郵便局]お荷物の配送先に不明点があり、配達を見合わせております.再配達の申請はこちら:[URL]

✕ [ポストする](#) 掲載日:2026年02月18日

**国税庁** [注意喚起](#)

【国税庁】重要な事務手続きについてのご案内です。内容をご確認ください。[URL]

✕ [ポストする](#) 掲載日:2026年02月18日

# フィッシング・スミッシング被害を防ぐ3つの対策

モバイルマルウェア

身に覚えのないメールやSMSが届いた場合、  
文面に添付されたURLに触らない

日頃利用するサービスは、公式アプリや  
ブックマークしたサイトから情報を確認

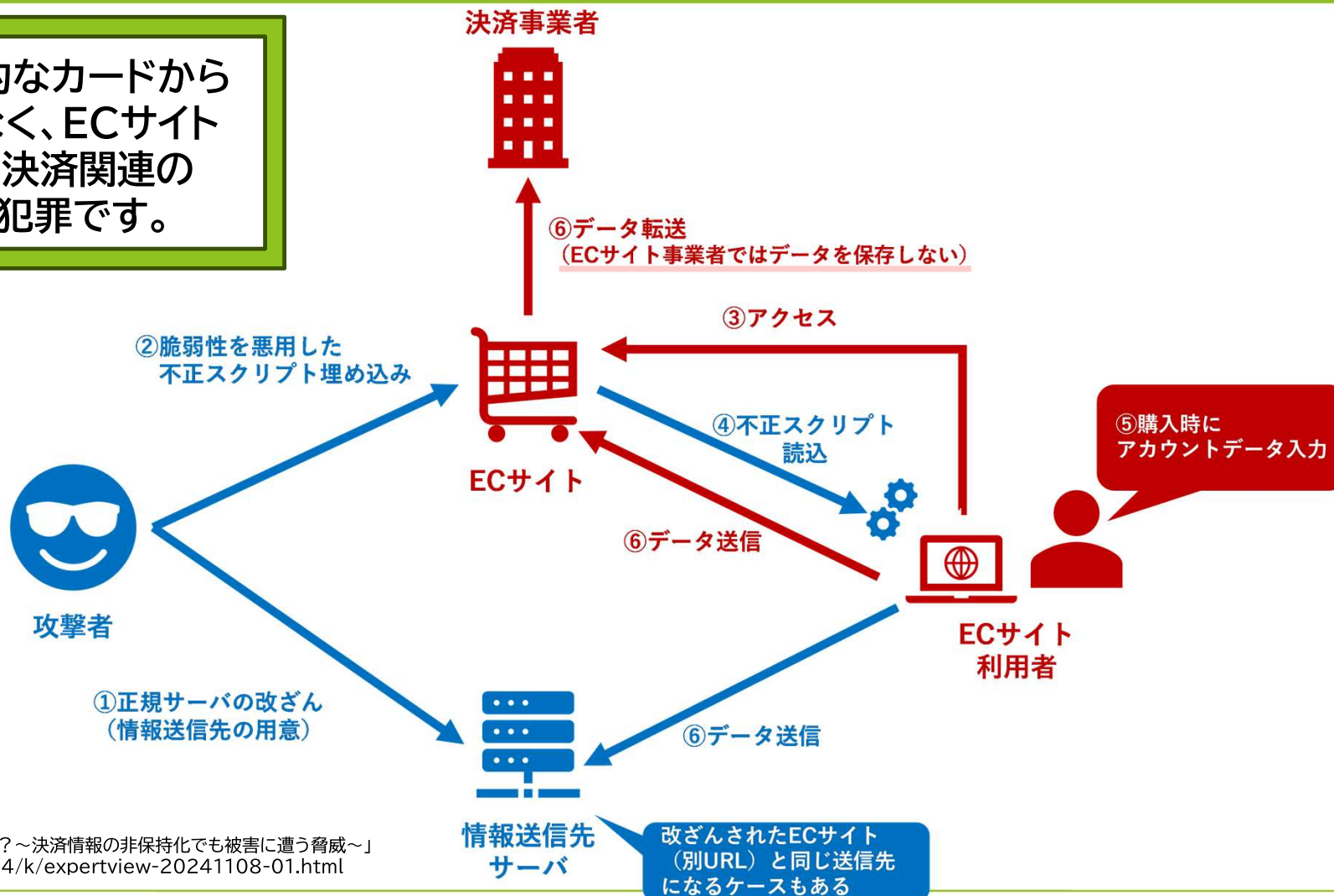
迷惑SMS対策サービスを活用し、フィッシング  
などの不審なSMSを自動で遮断

トビラシステムズ「トビラシステムズ「スミッシングトレンドレポート2025」を公開」  
<https://tobila.com/news/report/p2692/>

# クレジットカードを狙った犯罪～ウェブスキミング～

ウェブスキミング

Webスキミングは物理的なカードから情報を盗み出すのではなく、ECサイトなどで購入者が入力した決済関連の情報を盗み取るサイバー犯罪です。



トレンドマイクロ「Webスキミングとはどのような攻撃なのか？～決済情報の非保持化でも被害に遭う脅威～」  
<https://www.trendmicro.com/ja.jp/jp-security/24/k/expertview-20241108-01.html>

# クレジットカードを狙った犯罪～ウェブスキミング～

ウェブスキミング

? なぜECサイトは改ざんされるのか？

ECサイトの管理者アカウントの漏洩または脆弱なパスワードなどの認証の突破

ECサイトをホストするクラウドサービスなどの設定ミス悪用の悪用

ECサイト構築用プラットフォームの持つソフトウェア脆弱性の悪用

警察庁からの注意喚起

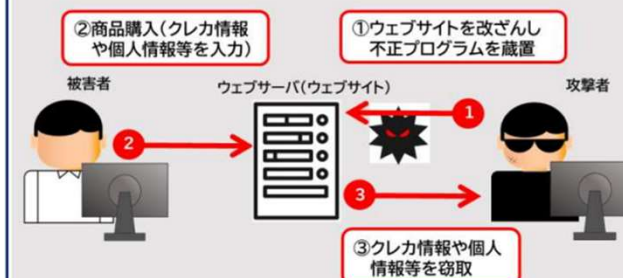


サイバー警察局便り  
Cyber Police Agency Letter R6 Vol.5

顧客のクレカ情報流出にご用心！！

## ウェブスキミングの一例

ECサイト等のウェブサイト改ざんして不正プログラムを蔵置し、サイトに入力したクレジットカード情報や個人情報等を窃取する手口が確認されております。



## ウェブスキミング対策

ウェブサイトを安全に運用するために、次に掲げる対策を講じましょう。

- 管理者のID・パスワードの適切な管理、ワンタイムパスワードや生体認証等の二要素認証の活用
- OSやソフトウェアのぜい弱情報の確認や定期的な診断の実施、最新のパッチ等の適用、ウイルス対策ソフト等の導入
- WAF(Web Application Firewall)等のセキュリティ製品の導入

IPA（独立行政法人情報処理推進機構）のウェブサイトにおいて「ECサイト構築・運用セキュリティガイドライン」が公開されています。  
<https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html>



IPA 独立行政法人  
情報処理推進機構



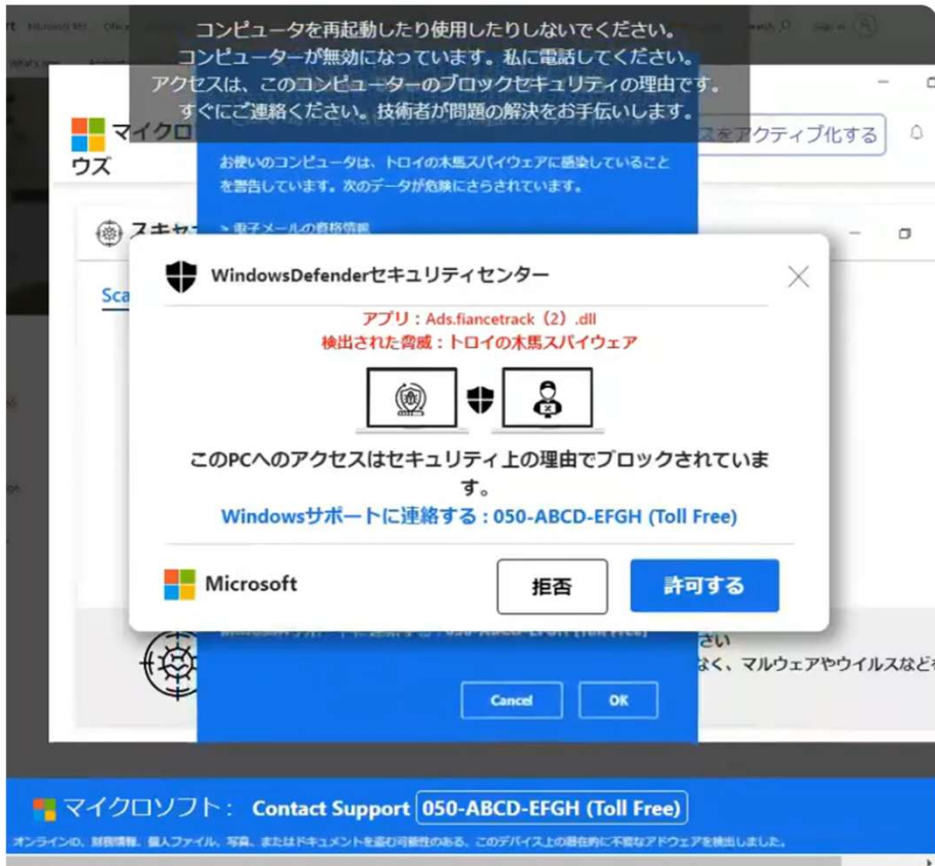
警察庁  
National Police Agency

JC3 Japan Cybercrime Control Center

# サポート詐欺(テクニカルサポート詐欺)

サポート詐欺

■ パソコンを使っている途中で、突然こんな画面とともに警告メッセージが大音量で流れたら、あなたはどのようにしますか？



■ パソコンでインターネットを閲覧中に、

- 突然ウイルスに感染したかのような嘘の画面を表示させる

- 警告音を発生させる

などして、ユーザーの不安を煽り、画面に記載されたサポート窓口で電話をかけさせ、

- サポート名目で金銭をだまし取る

- 遠隔操作ソフトをインストールさせる

詐欺をサポート詐欺(テクニカルサポート詐欺)と言います。

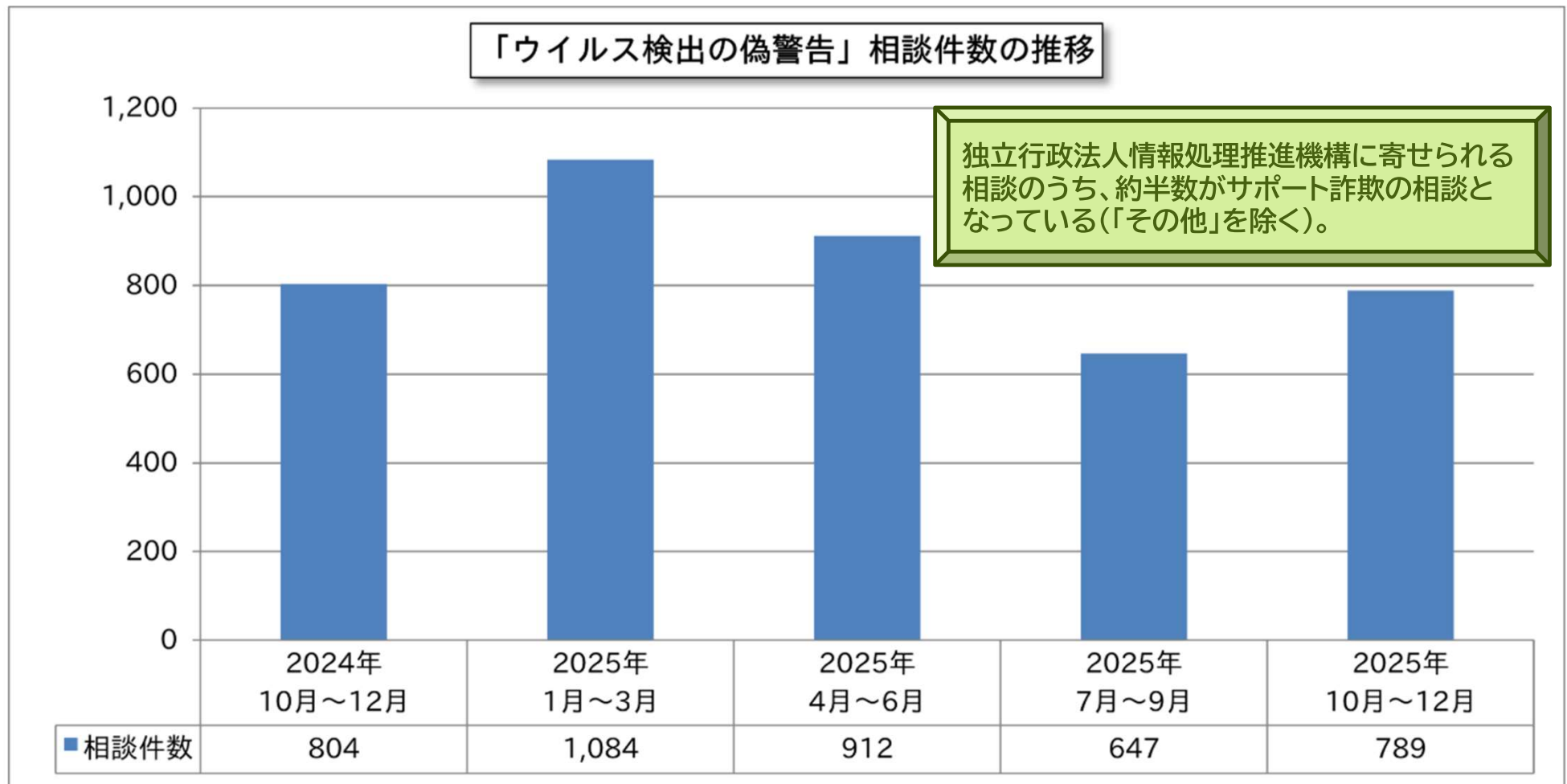
# こんな広告、見たことありませんか？

サポート詐欺

投影限り

# サポート詐欺(テクニカルサポート詐欺)の相談件数

サポート詐欺



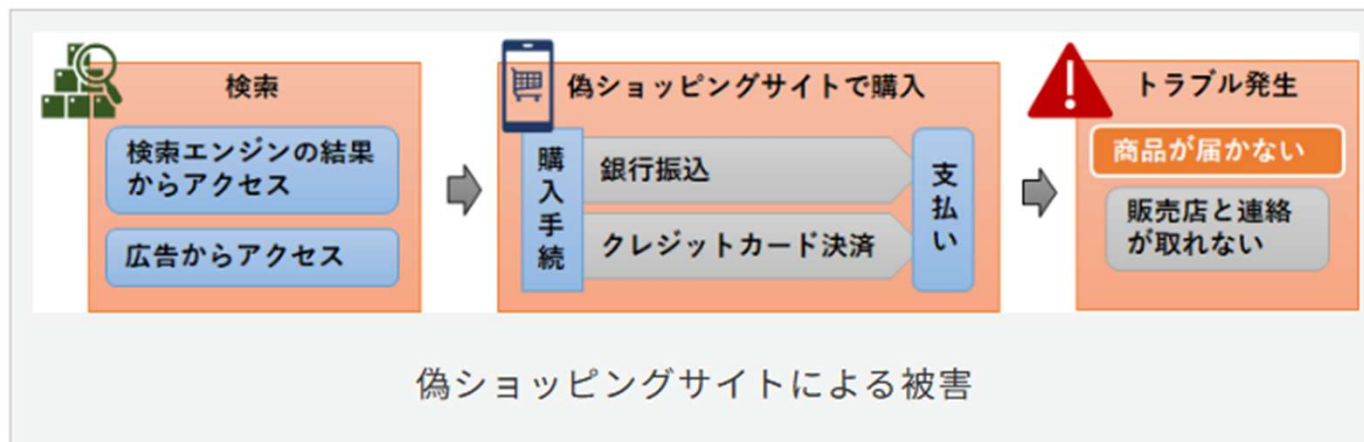
独立行政法人情報処理推進機構「情報セキュリティ安心相談窓口の相談状況[2025年第4四半期(10月～12月)]」  
<https://www.ipa.go.jp/security/anshin/reports/2025q4outline.html>

# 悪質サイト(偽ショッピングサイト)とは

悪質サイト

## 1. 偽ショッピングサイトとは

偽ショッピングサイトとは、正規のショッピングサイトを模倣する等して、利用者から購入代金を騙し取ったり、粗悪品を販売したりするショッピングサイトを指します。これら偽ショッピングサイトで商品を購入してしまった場合、商品が届かないことが多く、届いたとしても、偽物、全く別の物、空箱の場合もあります。



# 悪質サイト(偽ショッピングサイト)とは

悪質サイト

## ● 多種多様な商品を販売するサイト

インターネットの検索エンジンに自分が欲しい商品名などで検索した際、その検索結果の中に、「ショッピングサイトの名称にそぐわない商品を販売している」「取扱商品の種別が混在している」という偽ショッピングサイトが含まれていることがあります。

例えば、子供用品のショッピングサイトでカーナビやタイヤを扱うサイトや、仏壇と発電機を一緒に販売している偽ショッピングサイトも確認されています。



## ● 実在する企業等を騙ったサイト

偽ショッピングサイトの中には、実在している企業のサイトを模倣したものもあります。また、会社名、ロゴや商品画像を無断で転用している場合もあります。

# 悪質サイト(偽ショッピングサイト)への誘導方法

悪質サイト

## (1) 検索結果から誘導される場合

検索エンジンで商品名などのキーワードを入力して検索した際、この検索結果の上位に偽ショッピングサイトへ誘導するサイトが表示される場合があります。これは、偽ショッピングサイトの制作者がSEOポイズニングと呼ばれる攻撃手法を用いて検索結果でのサイトの表示順位を引き上げているためです。

激安 送料無料 テント

https://[redacted].jp> ...  
インターネット通販 かんたん組立テント TA ...  
テントの魅力を最大限に引き出す。組立簡単なワンタッチテントや災害用テントなど丈夫で長持ちするテントを激安・送料無料でご提供。

http://[redacted].jp> ...  
テントタフスクリーン2ルームハウス ...  
他テントともタフスクリーン2 限定カラーテント ブラック系最適な材料限定製作】タフ【即決・送料無料】

https://[redacted].co.jp> ...> テント  
テント オーナーロッジタイプ ...  
人気激安 テント オーナーロッジタイプ 2000-4000 H 4人用 2200 大型天板タイプ (16.9サイズ) (ファインホワイト) (送料無料)

検索結果から偽ショッピングサイトへ転送

キーワード「激安 送料無料 (商品名)」の検索結果例

# 悪質サイト(偽ショッピングサイト)への誘導方法

## (2) 広告から誘導される場合

検索エンジンの検索結果には「広告」も表示されますが、この中に偽ショッピングサイトが表示されることもあります。最近では、SNS上に表示された広告から偽ショッピングサイトへ誘導されるケースも確認されています。

The image shows a comparison of two search results. The top result is a fake advertisement for a furniture store, enclosed in a red rounded rectangle. It features a URL with a misspelled domain and promotional text about a sale. To its right, the vertical text '偽物' (Fake) is written in red. The bottom result is a legitimate advertisement for a furniture store, enclosed in a blue rounded rectangle. It features a correct URL and text indicating it is an official website. To its right, the vertical text '本物' (Real) is written in blue. Below these two results, a caption reads '検索結果に表示される偽ショッピングサイトの広告' (Advertisement for a fake shopping site displayed in search results).

偽物

本物

検索結果に表示される偽ショッピングサイトの広告

## (1) 実在する会社であることを確認する

初めて利用するショッピングサイトでは、会社概要において、事業者の氏名（名称）、住所、電話番号が記載されているか確認願います。会社概要では架空の情報又は実在する会社を騙っていることもあるため、インターネットで名称や連絡先等を検索し、利用するサイトが実在する会社が運営していることを確認してください。

## (2) 正規サイトとは異なる点に注意する

偽ショッピングサイトは次の特徴があるため、いずれも注意が必要です。

### ① 価格が安い

商品価格が他のサイトと比べて極端に安価・割引率が高い。

### ② 支払い方法が銀行振込に限定される

支払い方法としてクレジットカード決済が可能と記載があるものの、決済時に銀行振込のみ可能であると限定されることが多い。また、口座名義人が法人口座ではなく個人口座が案内される場合、その名義が会社概要などに記載された代表者と異なる名義の口座となる場合が多い。

### ③ 不自然な日本語

文章の繋がりや単語などが不自然な日本語表現や、単なる誤記と考えにくい場合がある。

### ④ URLのドメイン名

「.xyz」「.top」等のTLD（トップレベルドメイン）を使用していることが多い。

# JC3悪質ECサイトホットライン 通報フォーム

悪質サイト



The screenshot shows the top navigation bar of the JC3 website, including the logo, language options (JA, EN), and a search bar. Below the navigation is the main heading '悪質ECサイトホットライン 通報フォーム'. A breadcrumb trail reads 'TOP > 悪質ECサイトホットライン 通報フォーム'. The main content area contains a detailed explanation of the reporting form's purpose and a list of examples of malicious sites. A note at the bottom indicates that certain questions are mandatory.

日本サイバー犯罪対策センター  
JC3 : Japan Cybercrime Control Center

脅威情報 活動レポート JC3について 会員向け情報 関連リンク

## 悪質ECサイトホットライン 通報フォーム

[TOP](#) > [悪質ECサイトホットライン](#) [通報フォーム](#)

本通報フォームは、正規サイトを模倣し金銭や個人情報を収集する目的として作成された詐欺サイト等の悪質なサイトの通報を受け付けます。

**【悪質サイト例】**

- ・銀行振込等で支払いしても商品が発送されなかった場合
- ・クレジットカード情報等を盗まれた可能性がある場合
- ・運営するサイトを第三者によって改ざんされた場合
- ・運営するサイトのコンテンツ（会社情報等）を悪用された場合

**【注意事項】**

- ・JC3では独自に分析を行ない、基準に該当するものについては、フィルタリング事業者、セキュリティ事業者等に提供します。
- ・一方で、通報内容についての調査や捜査機関への被害届出の代行等を行うものではありません。
- ・通報に対する処理状況、結果についてのお問い合わせは受け付けておりません。

[Google にログイン](#)すると作業内容を保存できます。[詳細](#)

\* 必須の質問です

URL  
<https://www.jc3.or.jp/akushitsu-ec-form.html>



# 悪質サイト情報の活用事例

悪質サイト

悪質サイトチェックサイト「SAGI CHECK」(日本語版)  
(2023年2月から公開中)  
<https://sagicheck.jp/>



ここにURLを入力すると

結果が表示される。

SAGICHECK MENU JP

## 確認結果 jc3.or.jp リスクについて

このサイトは **正規のものであるように思われます**  
常にご自身で確認・判断してください(英語)

他のサイトを確認する

もしこれがあなたのウェブサイトであり、情報源の組織の1つがあなたを疑わしいとリストアップした場合、問題を解決するためには、情報源の組織の名前をクリックして、情報源の組織に直接連絡してください。

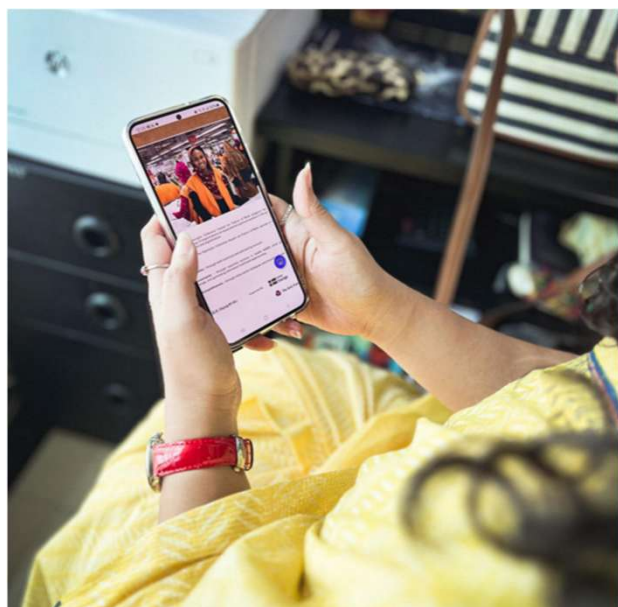
以下の情報源を確認しました

<b>CERT NZ:</b>	● CERT NZ has no data for this website
<b>Maltiverse:</b>	● Unknown
<b>Complytron:</b>	● このサイトはComplytronから危険又は悪意のあるサイトとして報告されていません
<b>APWG:</b>	● 報告されていません
<b>CleanBrowsing:</b>	● コンテンツはブロックされていません
<b>DNSFilter:</b>	● コンテンツはフィルタリングされていません
<b>IQ Global:</b>	● インディケーションがありません
<b>Pulsedive:</b>	● 過去3ヶ月間、Pulsediveに報告されていません
<b>Quad9:</b>	● マルウェアは報告されていません
<b>Scamadviser:</b>	● 高い信頼スコアです (full_jc3_or.jp_report)

# 今すぐできるサイバーセキュリティ対策 ～サイバー衛生研修～

サイバー攻撃は企業を標的とするときも”従業員一人ひとり”を狙ってきます。あなたの注意と行動がサイバー攻撃を防ぎ、会社全体、そして日本社会を守ります。サイバーセキュリティって難しそう、自分には関係ない、と思っているあなたに見ていただきたい動画です。

YouTubeで公開中



APAC Cybersecurity Fund V3.0.0  
The Asia Foundation

今すぐできる  
サイバーセキュリティ対策  
～サイバー衛生研修～

JC3 日本サイバー犯罪対策センター

企業、個人を対象とし、そのサイバーセキュリティの基本的な知識を最も基本的な5項目に絞り込み、**専門用語を使わず、20分の短時間**で学べるように工夫された研修動画です。



◀ 今すぐアクセス

▲ YouTube

<https://youtu.be/qvAhrpiMiQs>

# 今すぐできるサイバーセキュリティ対策 ～サイバー衛生研修～

企業／組織としてもご活用ください。ご担当者はJC3ホームページからお申込みを！  
以下のQRコードから直接アクセスできます。「企業／組織として申込をする」を選んでください。



企業／組織として  
申込をする

個人として  
研修を受講する

こちらのボタンをク  
リックしてください

▲ クリック後、簡単アンケートに  
基本情報を入力いただくと、別メールで  
[組織コード]と[研修用URL]をご連絡いたします。

組織としてお申し込みの企業には、月  
次受講状況をご報告いたします。(希  
望制)



一般財団法人 日本サイバー犯罪対策センター  
研究・研修グループ

CS-hygiene-training@jc3.or.jp

© JC3 All Rights Reserved.

対象

どなたでも可

費用

無料

利用手順

- 研修システムへのアクセス
- アカウント作成・ログイン
- 事前アンケート(10秒)
- 「サイバー衛生研修」視聴(約20分)
- 確認クイズ(全5問)(約3分)
- 事後アンケート(約2分)

※確認クイズ全問正解の方には修了証を発行します

# おさらい(注意すべきポイント)その1

ボイスフィッシング

CEO詐欺  
(社長騙り詐欺)

あくまでも、本講演で触れた内容のみとなります。これだけ注意しておけば大丈夫というわけではないことにご留意ください。

★取引先や加入・契約しているサービスから電話、メール、SMS等で連絡が来た場合、通常使用している手段で折り返し連絡し、真偽を確認する。

フィッシング

モバイルマルウェア  
(スマートフォンを狙ったマルウェア)

★心当たりのないメール、SMSが来た場合、メール、SMSに記載されているURLに安易にアクセスしない。

サポート詐欺

★ウェブページの広告に安易にアクセスしない。

## おさらい(注意すべきポイント)その2

### ランサムウェア

- ★3-2-1-1-0ルールを実施する。

### ウェブスキミング

(自社で運営するサイトに関し、)

- ★頑強なパスワードを使用する。
- ★人為的ミスを検知・修正できる仕組みを構築する。
- ★安全性・信頼性の高いクラウドサービスを利用する。

### 偽ショッピングサイト (悪質サイト)

- ★サイトの運営会社が存在する会社であることを確認する。
- ★正規サイトとは異なる点(価格の安さ、不自然な日本語等)に注意する。

あくまでも、本講演で触れた内容のみとなります。これだけ注意しておけば大丈夫というわけではないことにご留意ください。

## おわりに

攻撃者は、個人/企業に対して、突然攻撃してきます。  
日ごろから、必要十分な対策を実施するとともに、  
その対策を常にブラッシュアップするようにしてください。

攻撃者は、日々、新たな攻撃手法を駆使してきます。  
攻撃手法の把握に努め、その手法に対する、迅速な  
対応を心掛けてください。

攻撃者は、脆弱な「人」を狙ってきます。  
今回、取り上げた内容について、自身だけでなく、周りの方にも  
共有し、組織としてサイバーセキュリティ対策を推進してください。

---

本日は、ありがとうございました。

ご質問があれば、こちらへ

[info@jc3.or.jp](mailto:info@jc3.or.jp)



Japan Cybercrime Control Center

---