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

JC3 Japan Cybercrime Control Center

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 All Rights Reserved.

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 All Rights Reserved.

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 All Rights Reserved.

JC3 Japan Cybercrime Control Center

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

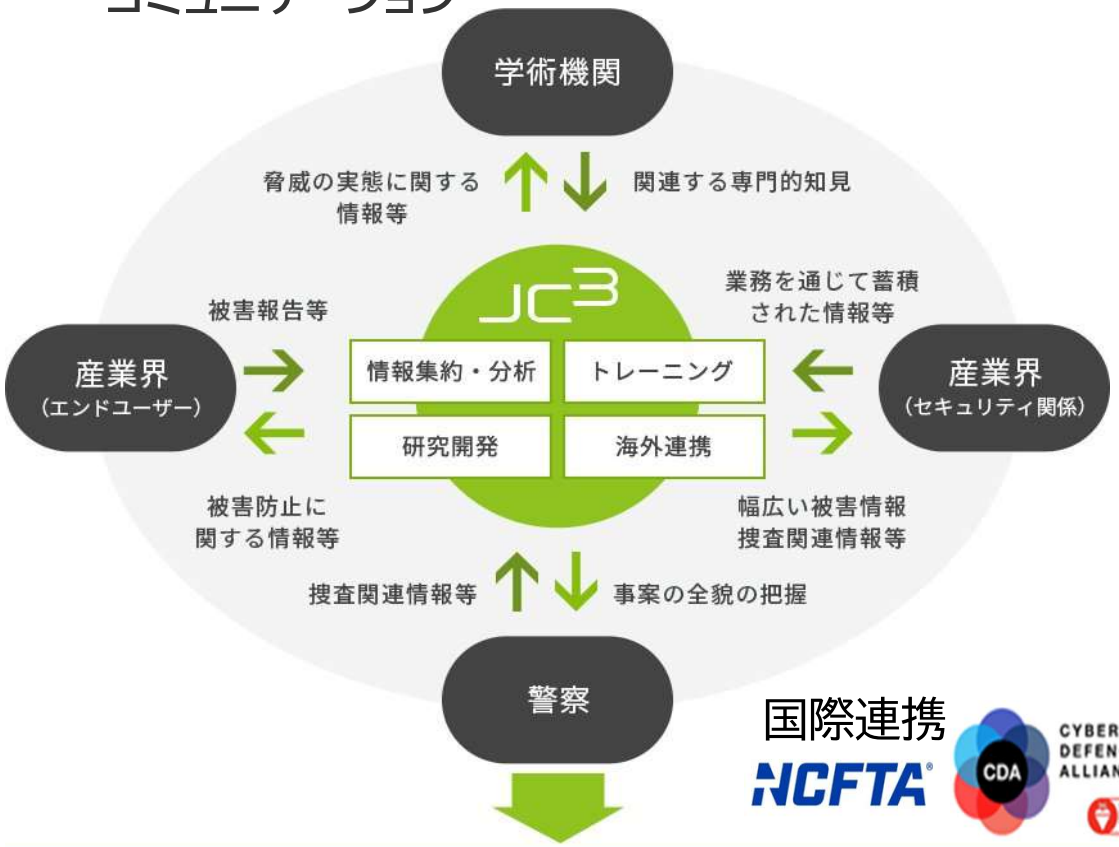
投影限り

© JC3 All Rights Reserved.

JC3 Japan Cybercrime Control Center

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



国際連携

NCFTA　CDA CYBER DEFENCE ALLIANCE

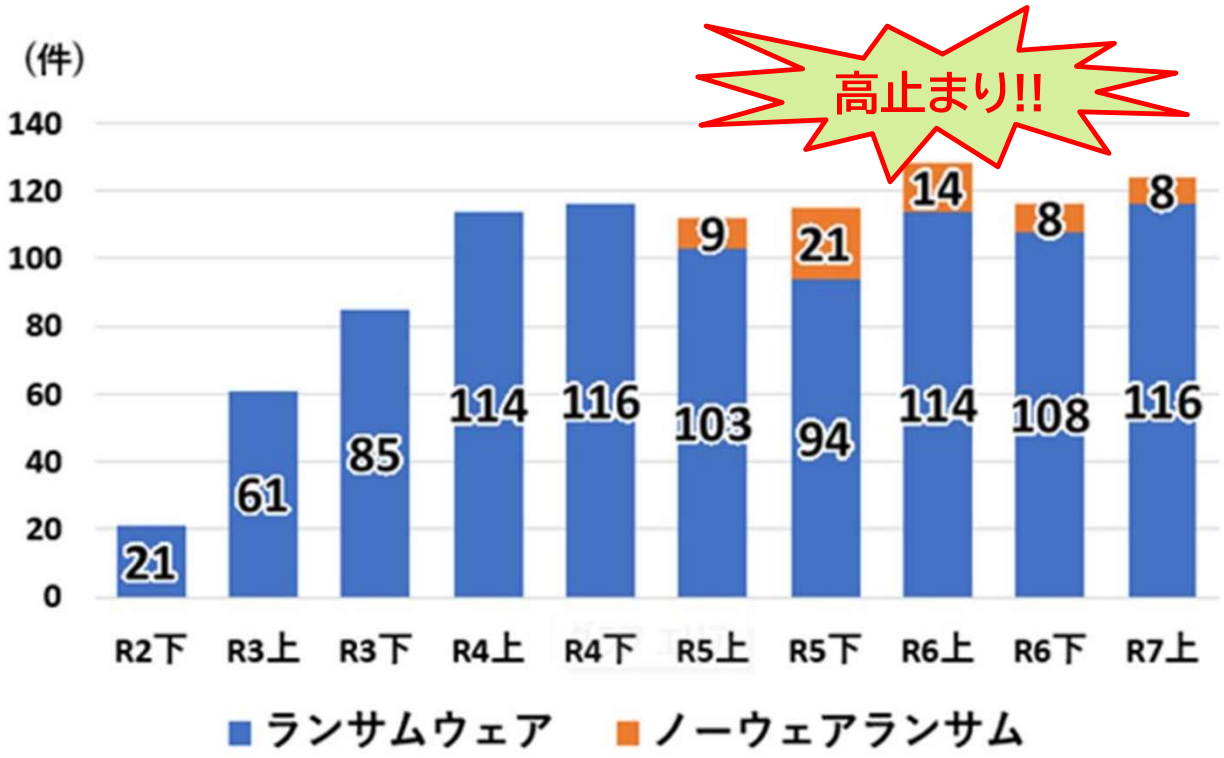
サイバー空間の脅威に関する事象の全貌を把握し、その大本に対処することが可能に

© JC3 All Rights Reserved.

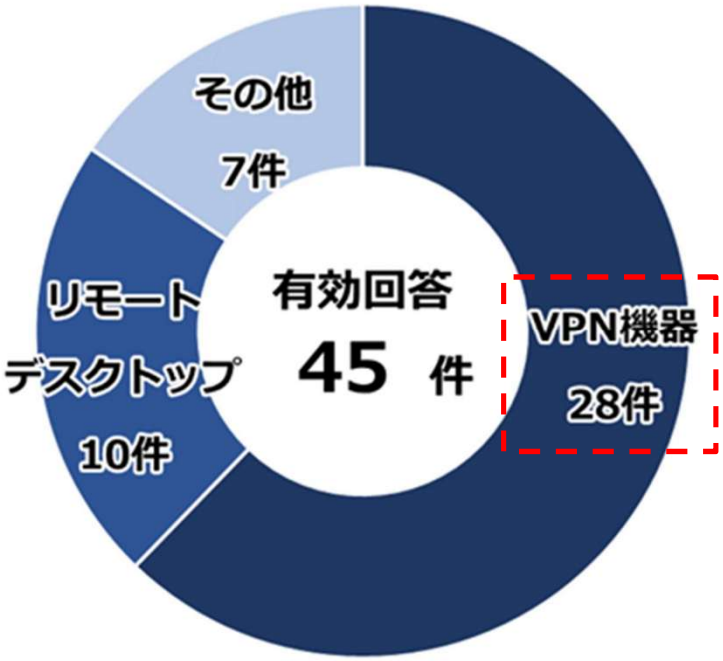
ランサムウェアに関する統計情報

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。



感染経路

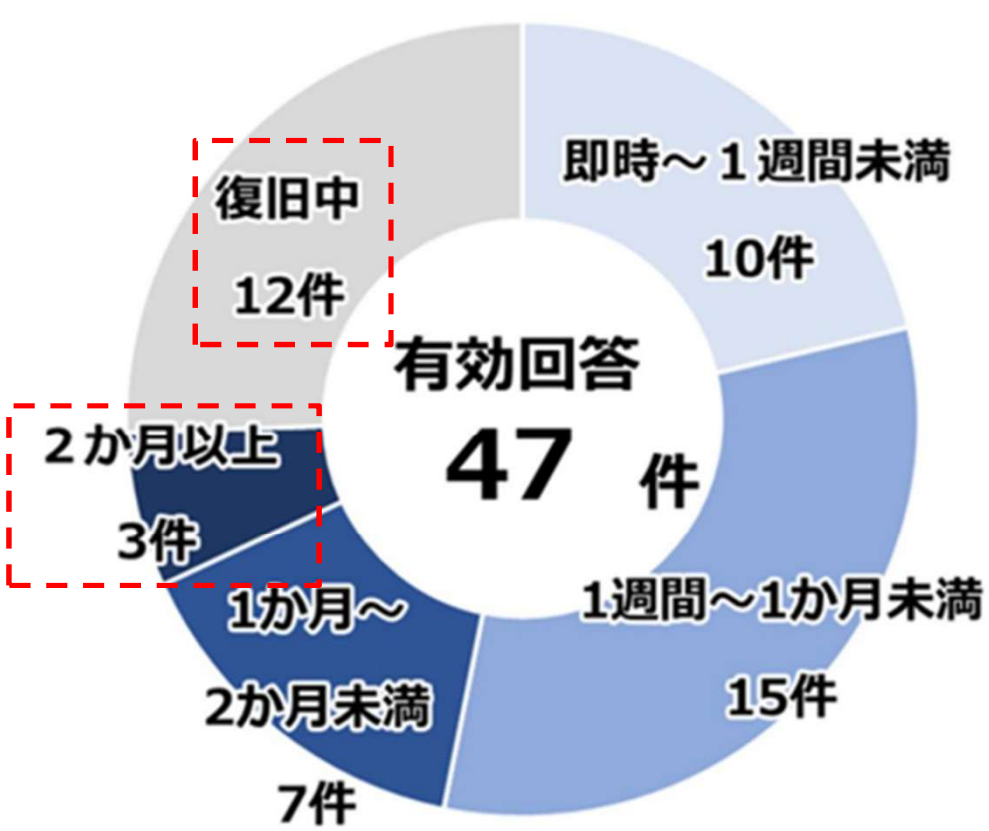


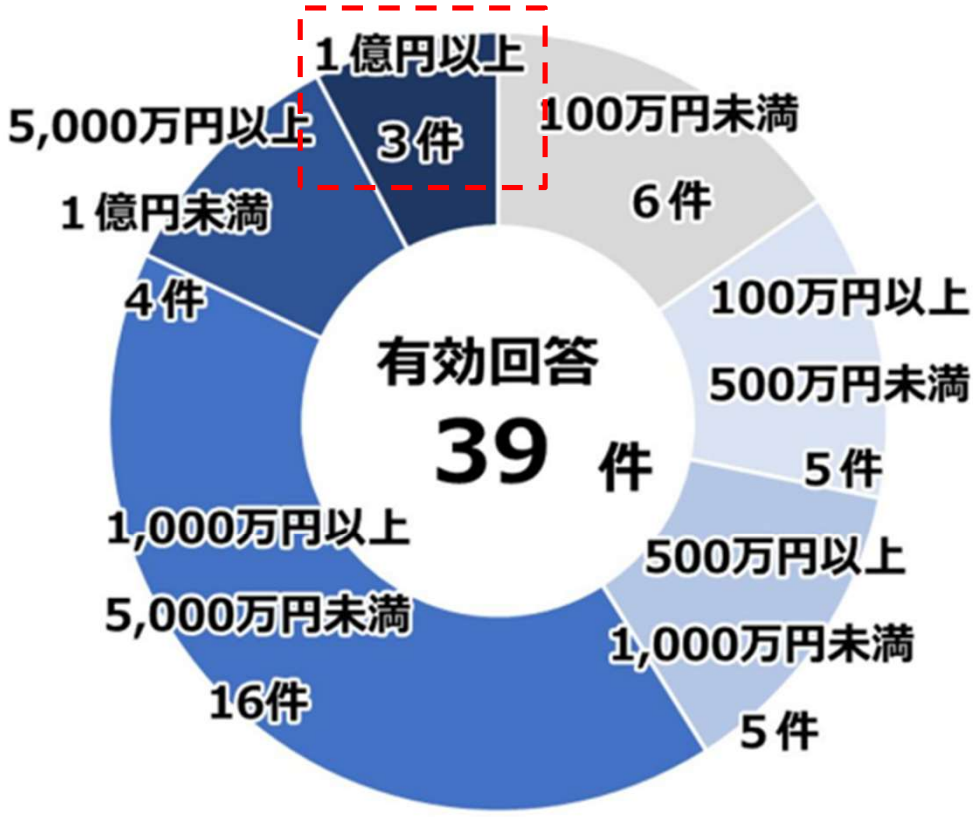
警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

© JC3 All Rights Reserved.

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



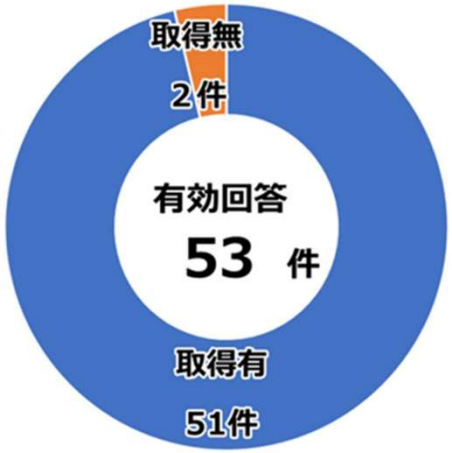


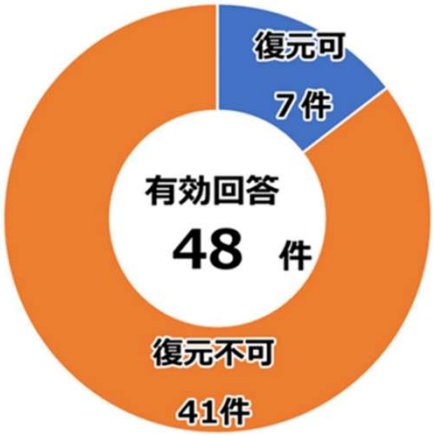
警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

© JC3 All Rights Reserved.

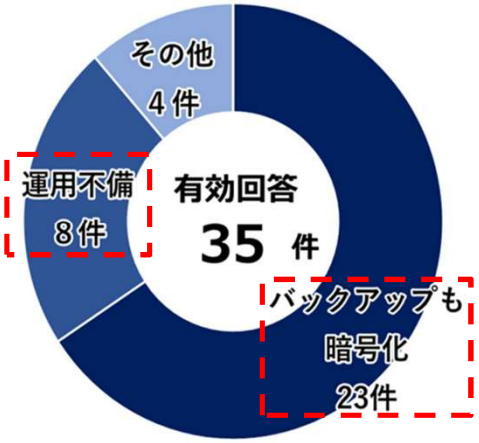
ランサムウェアに関する統計情報

● 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

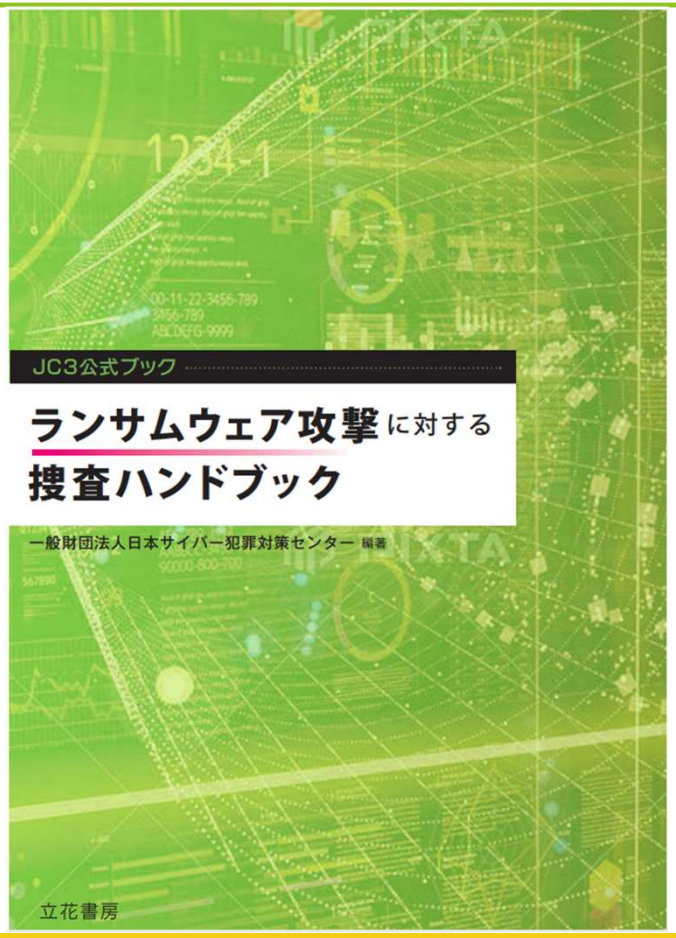
© JC3 All Rights Reserved.

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）



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。

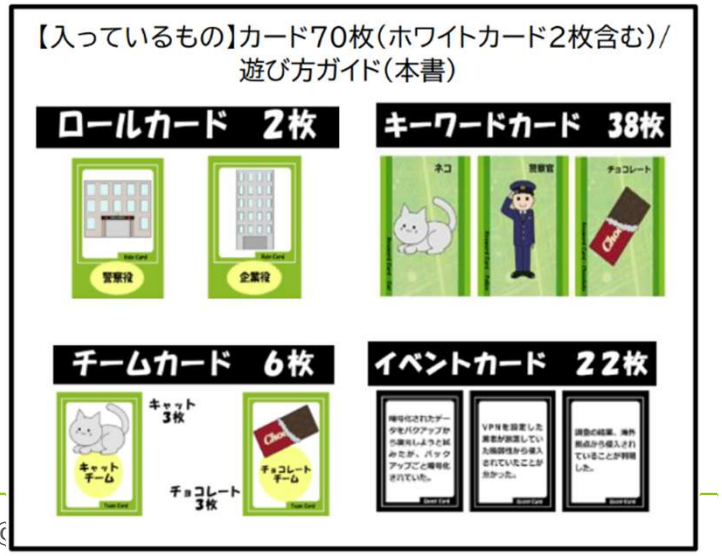
ランサムウェア攻撃への対応を、カードゲームで学ぼう！
～キャット＆チョコレート～

ランサムウェア

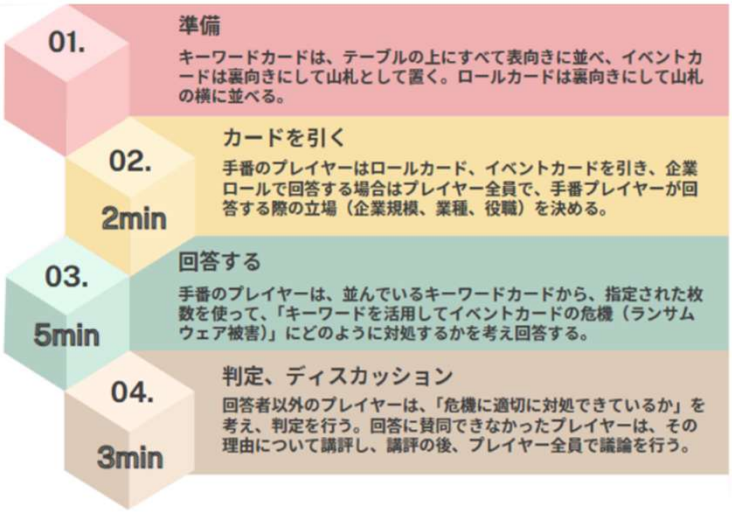
ランサムウェア被害に遭った際の対応についての訓練を、カードゲーム形式で行います。
ゲームを通じて、企業における被害発生時に企業、警察等、それぞれの立場における対応方策を検討し合うことで、

- 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。



●進行フローチャート



JC3Podcast　ランサムウェア・ダイアログのご紹介

ランサムウェア

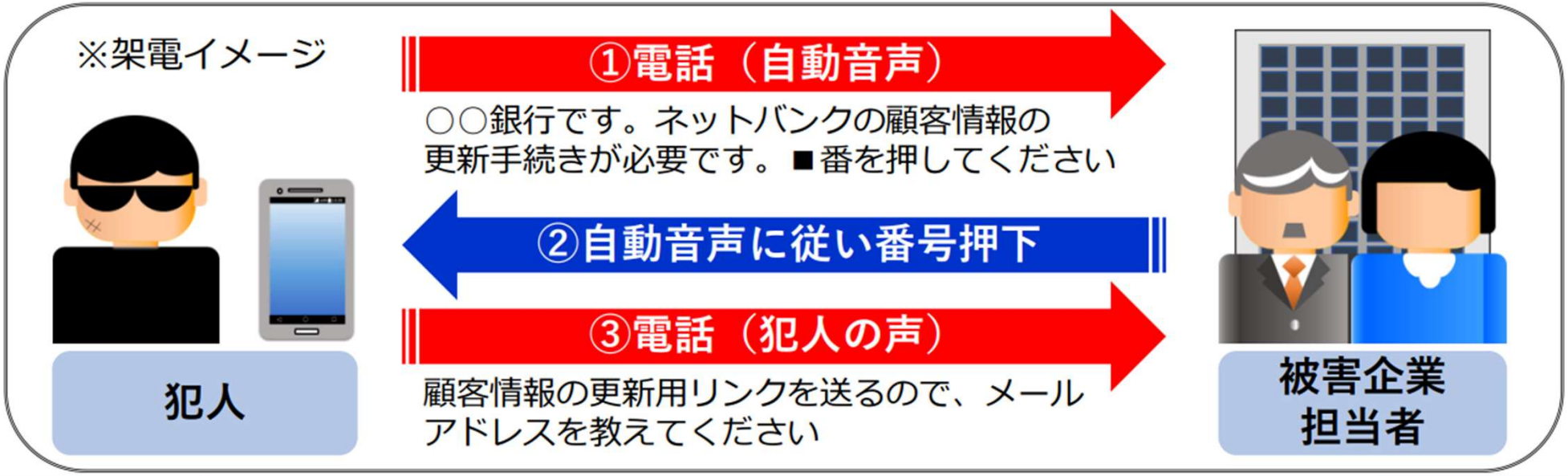
© JC3 All Rights Reserved.

ボイスフィッシングの手口

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



© JC3 All Rights Reserved.

ボイスフィッシングの見分け方と対策

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

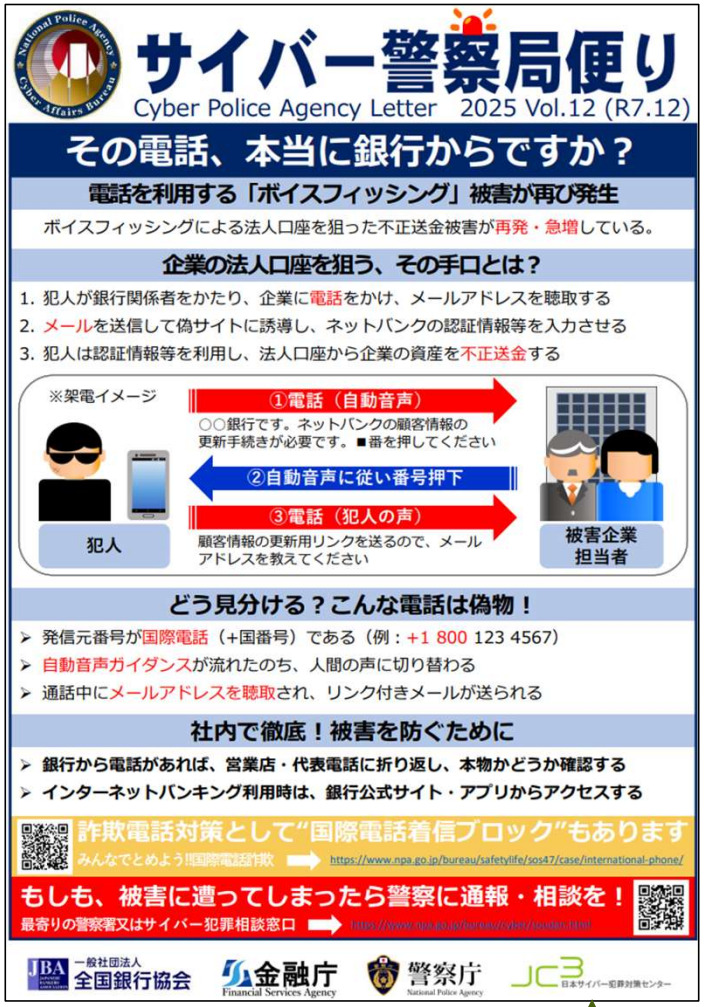
- **銀行から電話があれば、営業店・代表電話に折り返し、本物かどうか確認する**
- **インターネットバンキング利用時は、銀行公式サイト・アプリからアクセスする**

© JC3 All Rights Reserved.

ボイスフィッシングに関する警察庁からの注意喚起

（令和6年12月）

（令和7年4月）



（令和7年12月）

JC3も協力しています!!

© JC3 All Rights Reserved.

Japan Cybercrime Control Center

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

© JC3 All Rights Reserved.

CEO(Chief Executive Officer)詐欺

CEO詐欺

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

© JC3 All Rights Reserved.

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

© JC3 All Rights Reserved.

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

返信 全員に返信 転送

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

© JC3 All Rights Reserved.

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。

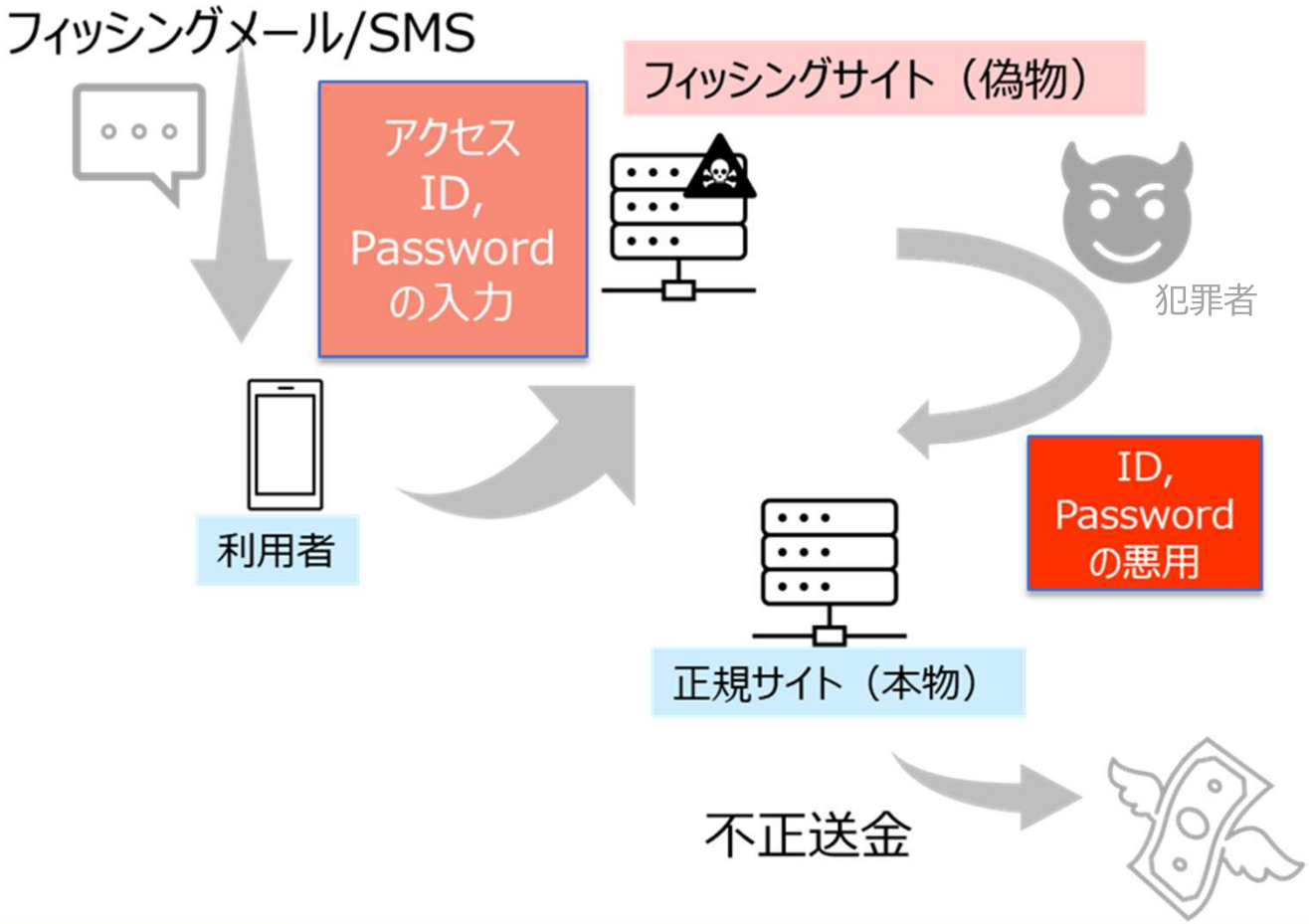
情報を盗まれると、アカウントを乗っ取られてお金を奪われたり、インターネット通信販売サイトで勝手に買物をされたりします。また、マルウェアに感染してしまうと、スマートフォンに登録された電話帳の情報が盗まれたり、自分のスマートフォンがフィッシングＳＭＳの発信源になってしまうこともあります。

フィッシング対策
https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

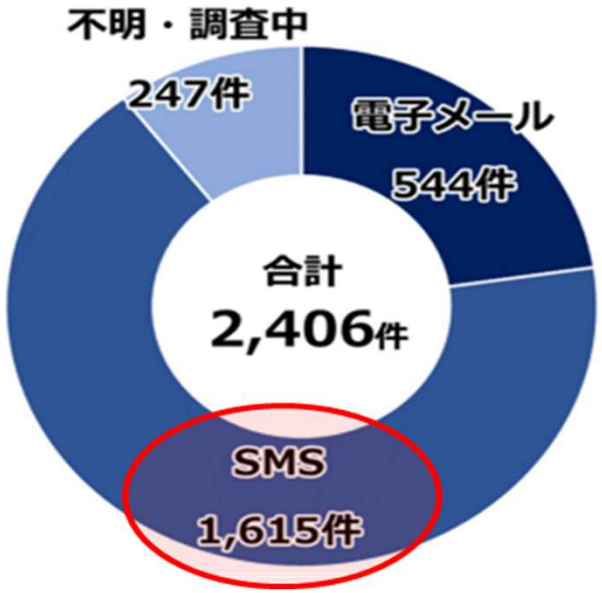
© JC3 All Rights Reserved.

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）



© JC3 All Rights Reserved.

情報を入力させる偽画面

フィッシング

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＞

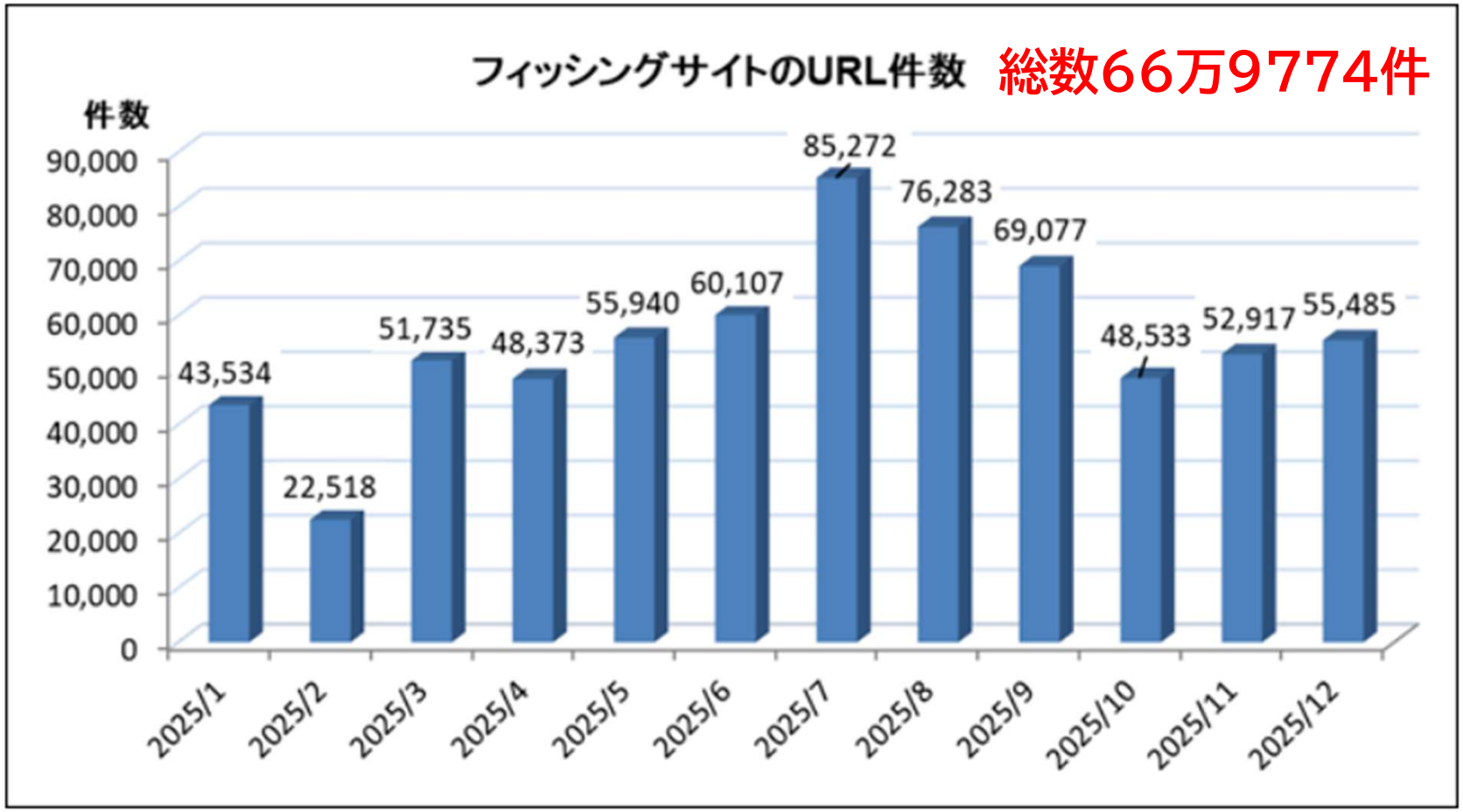
- 金融機関の口座番号、クレジットカード番号、暗証番号（ワンタイムパスワード、乱数表の番号等）
- 住所、氏名、電話番号、生年月日
- 電子メール、インターネットバンキング、ＳＮＳアカウント等のＩＤ、パスワード等
- 運転免許証、マイナンバーカード、乱数表等の画像情報

© JC3 All Rights Reserved.

フィッシング対策
https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

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 All Rights Reserved.

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>

amazon.co.jpからではない

宛先 join@jc3.or.jp

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

「AᴍaᴢᴏN」の字体がおかしい

お客様の AᴍaᴢᴏN 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おりません。

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 <https://click.federicoriva.com/?
qs=eyJkZWtJZCI6Ijk2Yzc5OGE5LWZiNTItNDNlMC05NTA4LTc[illegible]NaelRRYlpXUT09liwiY2l
waGVyVGV4dCI6Im9JU1FGekd5VEJqd1lNSzdQK0lLRlpGQkM4dnB5VTRuNk5tSkh3TUFkV0NUTUlxR2Q4dUpGU0s4Wkoza3RBZFpNSXU1TVp2TGk1clBHcDJUbTR
ZOUMzeDhYbnUycjhLUzFIT3BNS1Z5S2pWcXUyemF5NGtaWjNaelRRYlpXUT09liwiYXV0aFRhZyl6IlBRdDhmRjU3dHEvQ2t0WGpxVENsY2c9PSJ9>

アクセス先がamazon.co.jpではない

（参考）個人情報を狙った犯罪～インフォスティーラー～

「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　　インフォスティーラー

の二つが存在すると考えられています。

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!!

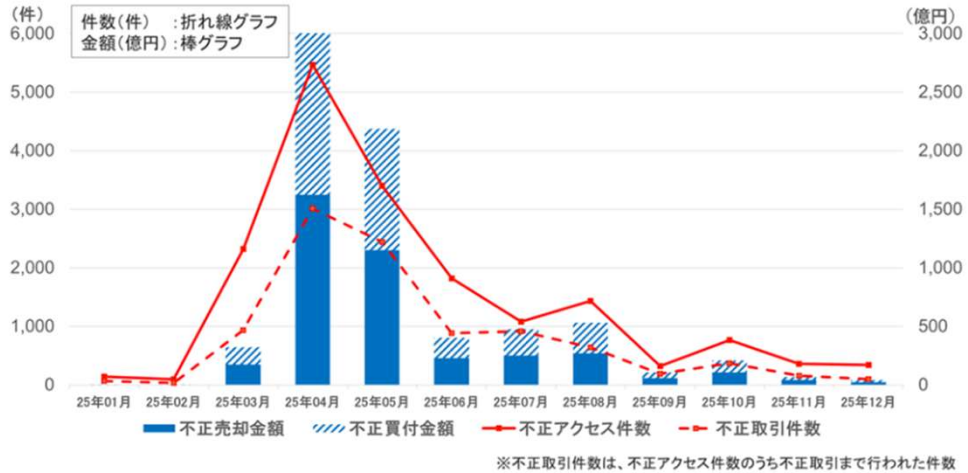
インフォスティーラーとは、「情報窃取専用」のトロイの木馬型不正プログラムです。
感染したPCやスマートフォンからブラウザに保存されたID・パスワードやセッションCookieなどの認証情報を短時間で外部サーバへ送信します。
一般的に画面に目立つ兆候を残さず、利用者は感染に気付きにくいという特徴があります。
感染手法の一つとして、攻撃者は画面に「私はロボットではありません」といった偽CAPTCHAを示し、その操作によって悪意あるPowerShellコマンド実行を誘導することでインフォスティーラーの感染に導きます。

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

金融庁 Financial Services Agency

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装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。



※不正取引件数は、不正アクセス件数のうち不正取引まで行われた件数

不正取引が発生した証券会社数（社）											
25年1月	25年2月	25年3月	25年4月	25年5月	25年6月	25年7月	25年8月	25年9月	25年10月	25年11月	25年12月
2	2	5	10	16	7	6	7	7	8	7	7

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

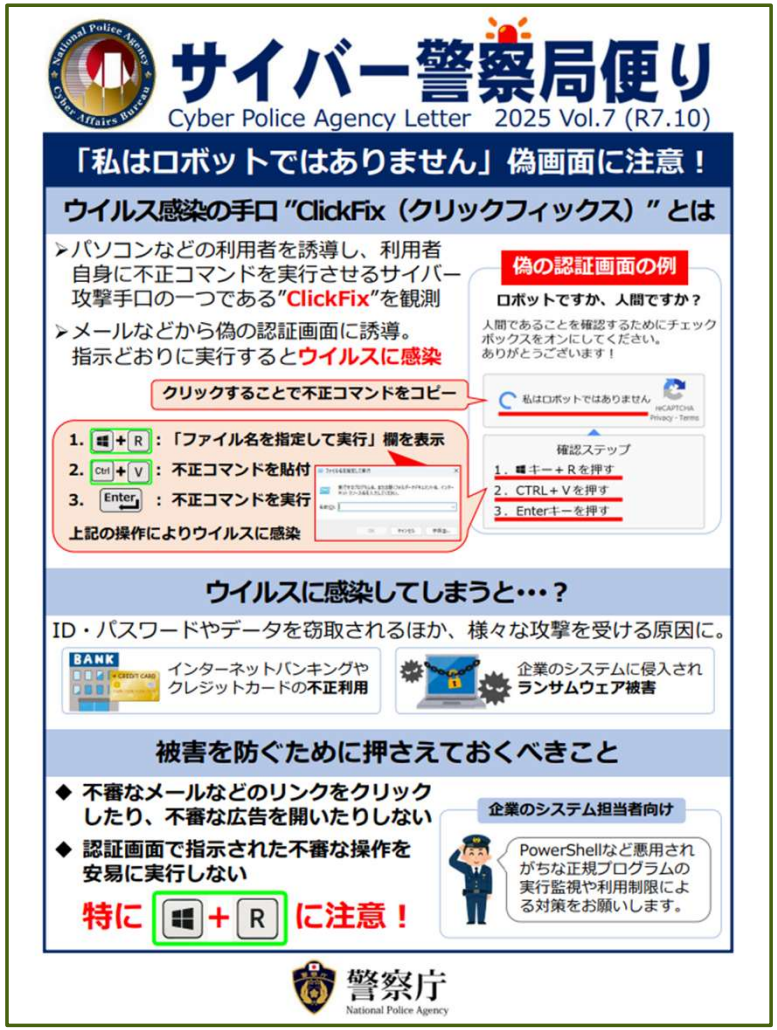
© JC3 All Rights Reserved.

（参考）個人情報を狙った犯罪～インフォスティーラー～

なぜ、**インフォスティーラー** 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

© JC3 All Rights Reserved.

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

© JC3 All Rights Reserved.

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

＜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

© JC3 All Rights Reserved.

（参考）Abuse報告について

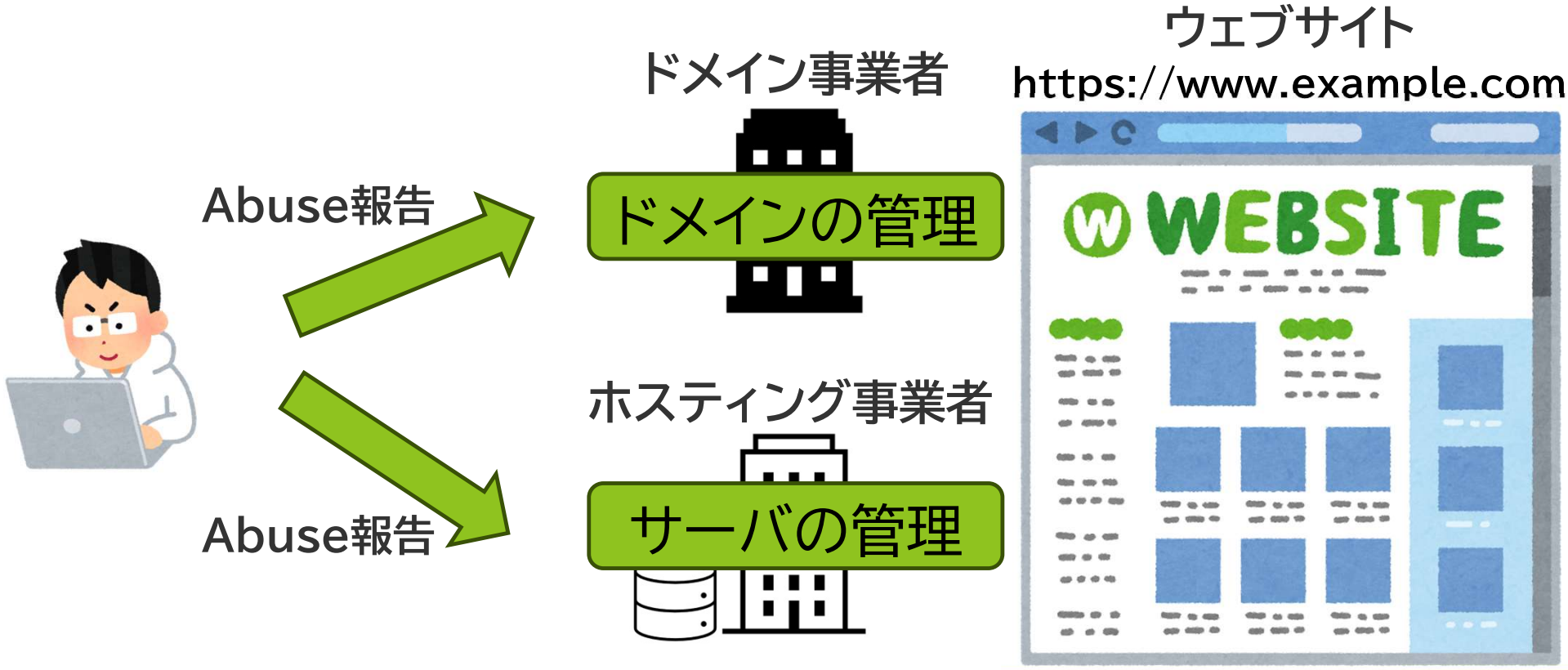
- Abuse報告とは、コンピュータネットワーク上の迷惑行為について、事業者に報告することを言います。
- インターネット上にウェブサイトを構築する際は、
  - ドメイン名の登録・管理を行うドメイン事業者を通じてドメイン（URL）の登録を行う
  - 実際のウェブサイトを設置するホスティング事業者からサーバを借りる

必要があります。

© JC3 All Rights Reserved.

（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。

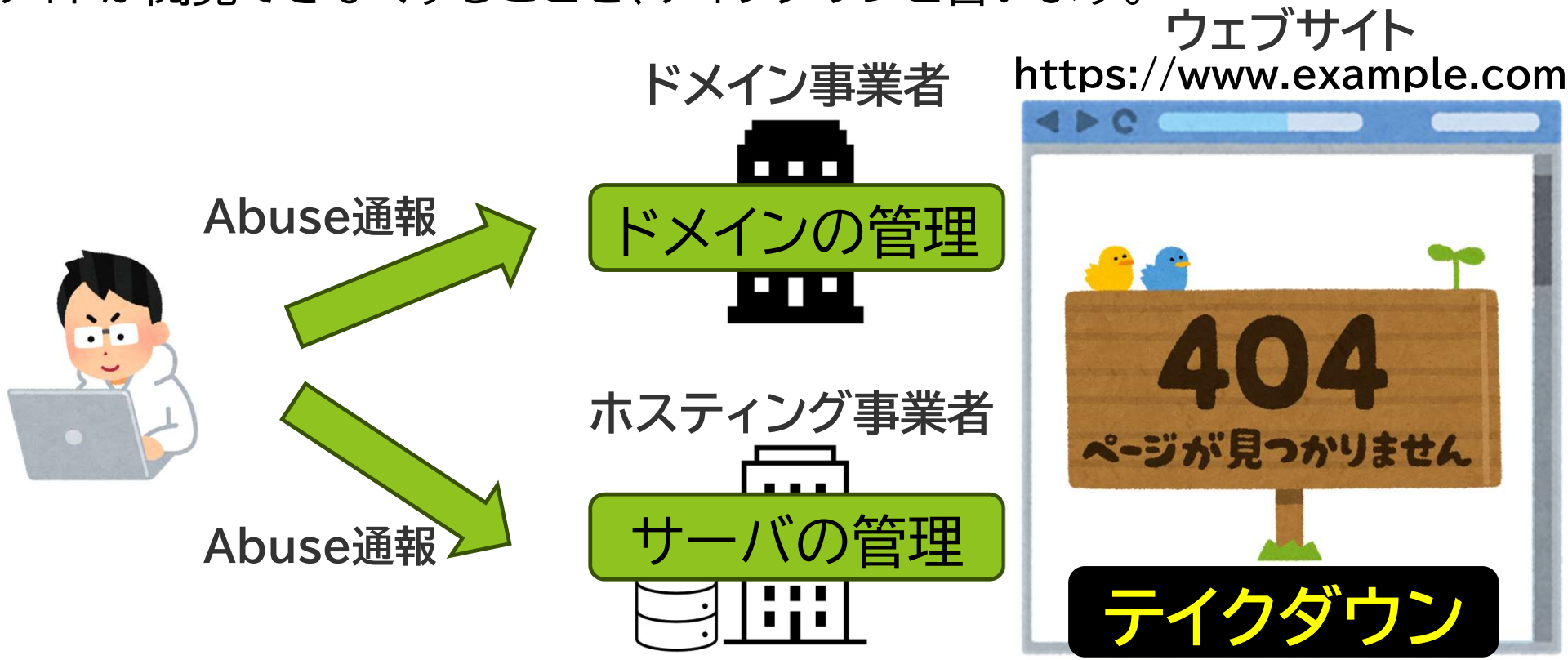


© JC3 All Rights Reserved.

（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。



© JC3 All Rights Reserved.

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

© JC3 All Rights Reserved.

（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

2,242

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

© JC3 All Rights Reserved.

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

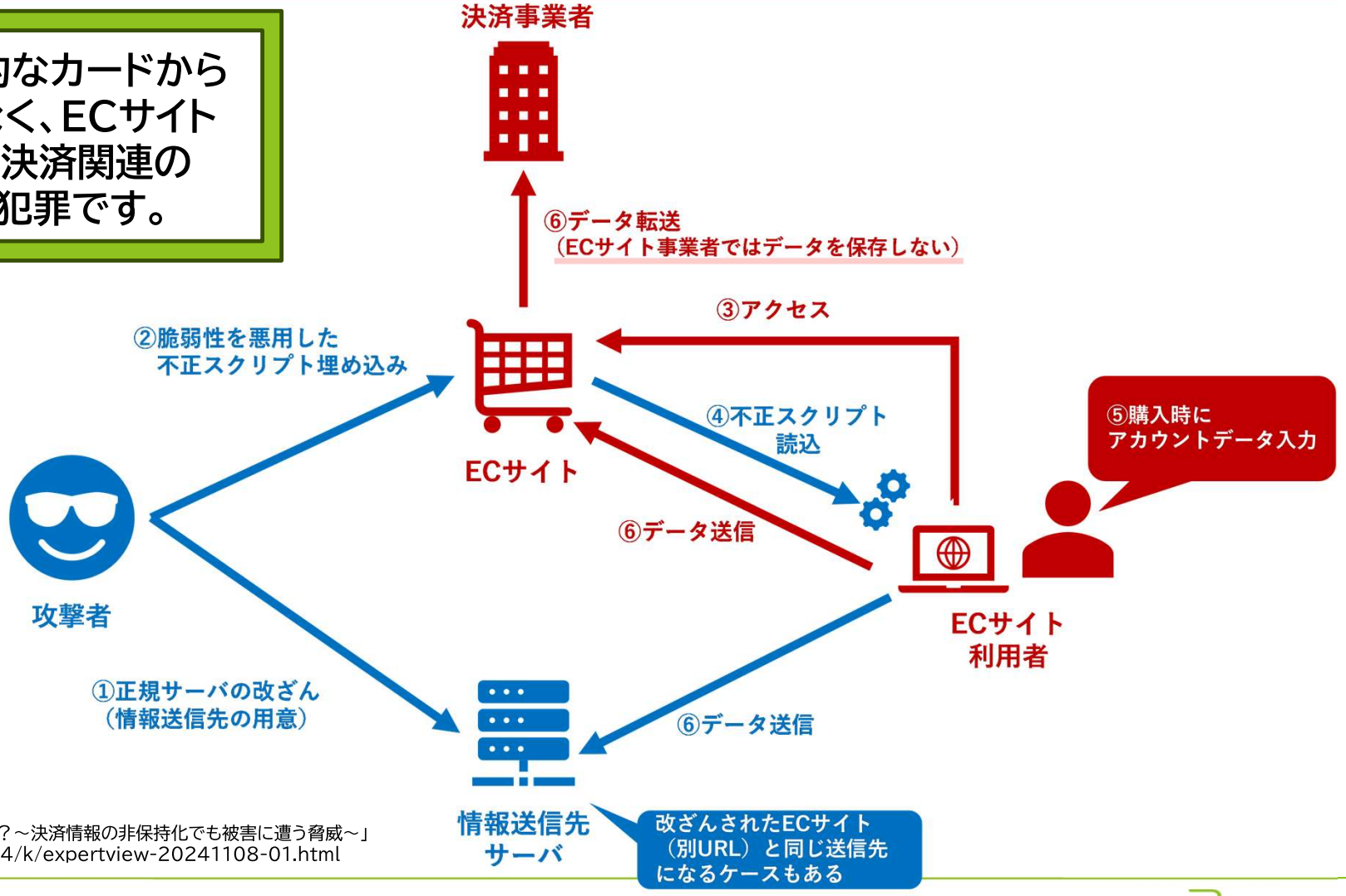
トビラシステムズ「トビラシステムズ「スミッシングトレンドレポート2025」を公開」
https://tobila.com/news/report/p2692/

© JC3 All Rights Reserved.

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

© JC3 All Rights Reserved.

クレジットカードを狙った犯罪～ウェブスキミング～

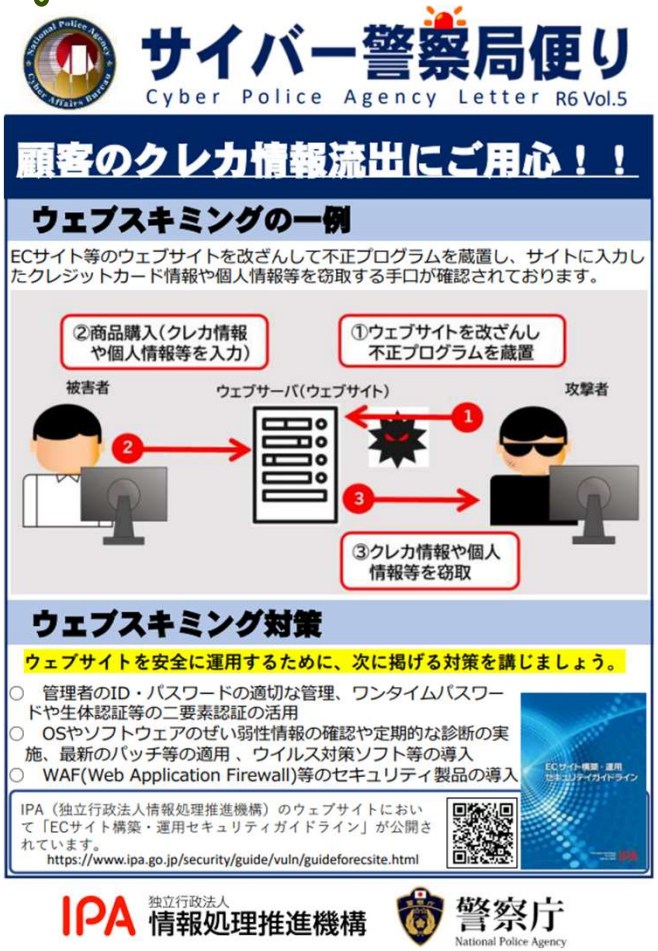
ウェブスキミング

? 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

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

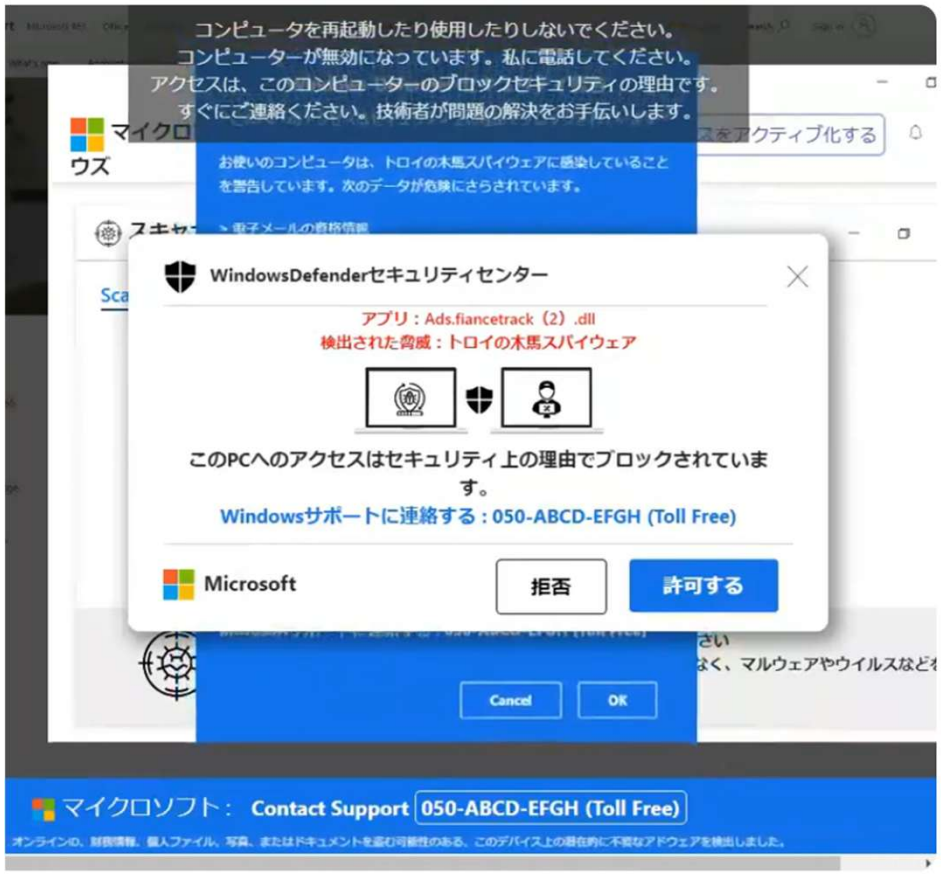
警察庁からの注意喚起



© JC3 All Rights Reserved.

サポート詐欺(テクニカルサポート詐欺)

パソコンを使っている途中に、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、あなたはどうしますか？



- 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に電話をかけさせ、

  - 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。

© JC3 All Rights Reserved.

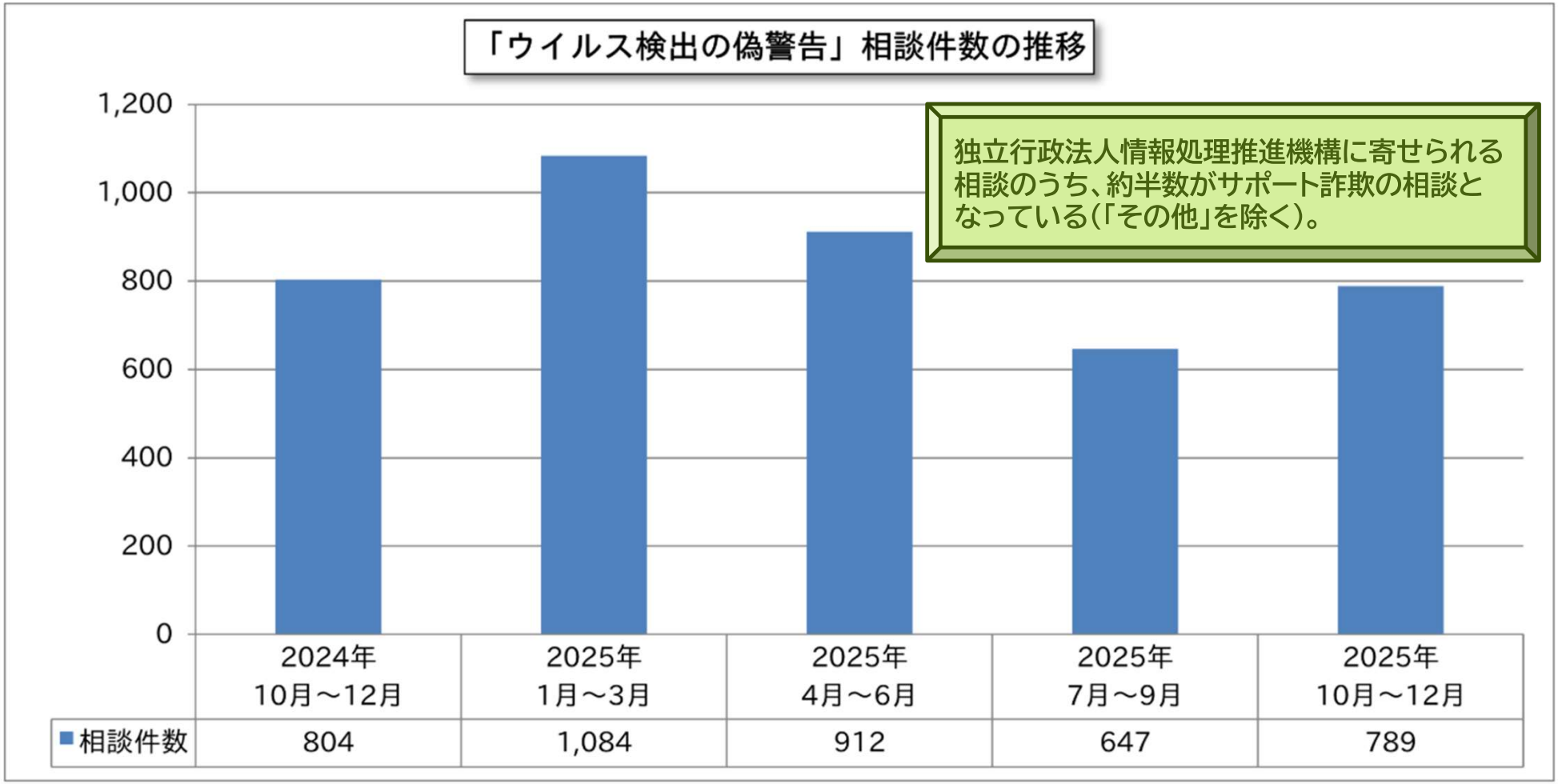
こんな広告、見たことありませんか？

サポート詐欺

投影限り

© JC3 All Rights Reserved.

サポート詐欺(テクニカルサポート詐欺)の相談件数



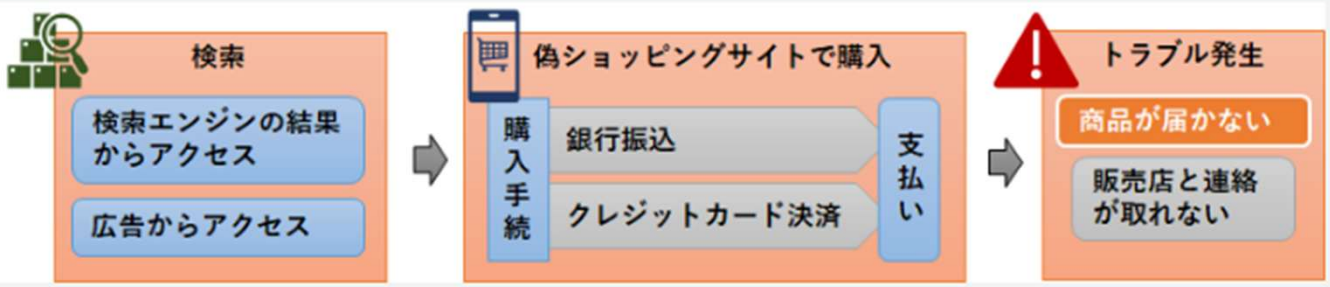
独立行政法人情報処理推進機構「情報セキュリティ安心相談窓口の相談状況[2025年第4四半期(10月～12月)]」
https://www.ipa.go.jp/security/anshin/reports/2025q4outline.html

© JC3 All Rights Reserved.

悪質サイト(偽ショッピングサイト)とは

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。



偽ショッピングサイトによる被害

© JC3 All Rights Reserved.

悪質サイト(偽ショッピングサイト)とは

● 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。

偽ショッピングサイトの一例

● 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。

© JC3 All Rights Reserved.

悪質サイト(偽ショッピングサイト)への誘導方法

(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。

キーワード「激安　送料無料　(商品名)」の検索結果例

© JC3 All Rights Reserved

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。

検索結果に表示される偽ショッピングサイトの広告

© JC3 All Rights Reserved.

悪質サイト(偽ショッピングサイト)の確認方法

(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。

© JC3 All Rights Reserved.

悪質サイト(偽ショッピングサイト)の確認方法

(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 All Rights Reserved.

JC3悪質ECサイトホットライン　通報フォーム

悪質サイト

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

© JC3 All Rights Reserved.

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。

© JC3 All Rights Reserved.

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

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

©
in partnership with CyberPeace Institute GLOBAL CYBER ALLIANCE JC3 Japan Cybercrime Control Center 日本サイバー犯罪対策センター Google.org

JC3 Japan Cybercrime Control Center

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。

◂ 今すぐアクセス

JC3 Japan Cybercrime Control Center

▲ JC3ホームページ お申込みはこちら
https://www.jc3.or.jp/news/2025/20250926-647.html

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）

無料 ¥0　基本用語　20分

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.

企業／組織として申込をする

個人として

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。

☑ 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

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。

ボイスフィッシング

CEO詐欺
(社長騙り詐欺)

★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。

© JC3 All Rights Reserved.

おさらい(注意すべきポイント)その2

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。

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実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。

© JC3 All Rights Reserved.

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。

© JC3 All Rights Reserved.

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

JC3 Japan Cybercrime Control Center