

フィッシングの動向と対策への取組

令和6年11月27日

一般財団法人日本サイバー犯罪対策センター（JC3）

渡邊 泰司

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。

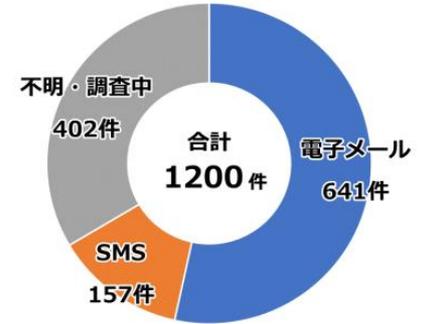
(NCFTA = National Cyber-Forensics & Training Alliance)



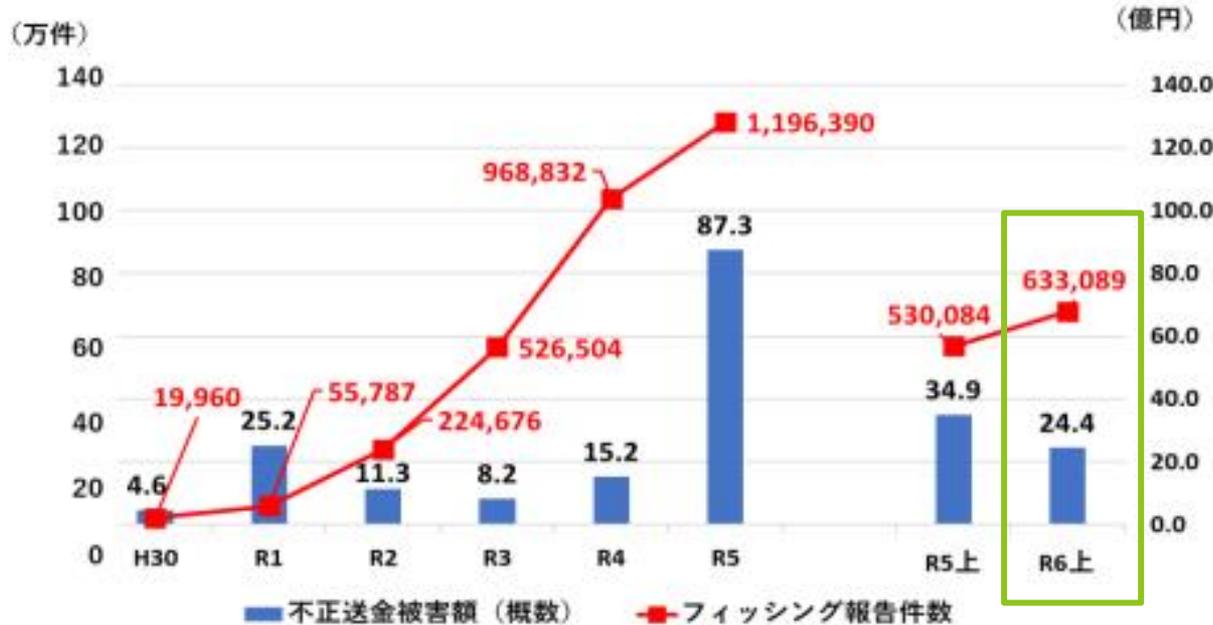
不正送金被害の情勢

- フィッシング報告件数が昨年同期比で約10万件増加
- 不正送金被害も高止まり

14 フィッシングサイトへ誘導する手口別割合



【図表 11：フィッシング報告件数及び不正送金被害額（概数）の推移】



インターネットバンキングに係る不正送金事犯の発生件数及び被害額の推移

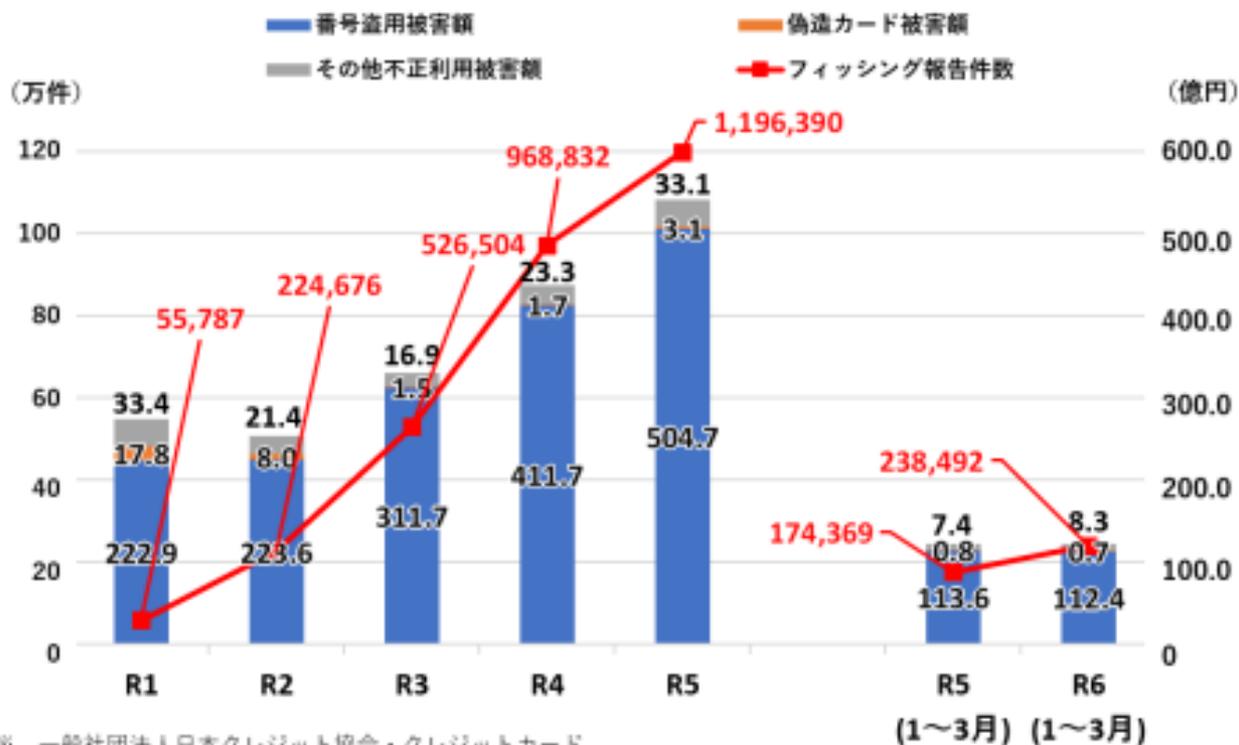


引用元：警察庁「令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について」

クレジットカード不正利用被害の情勢

■ 依然として厳しい

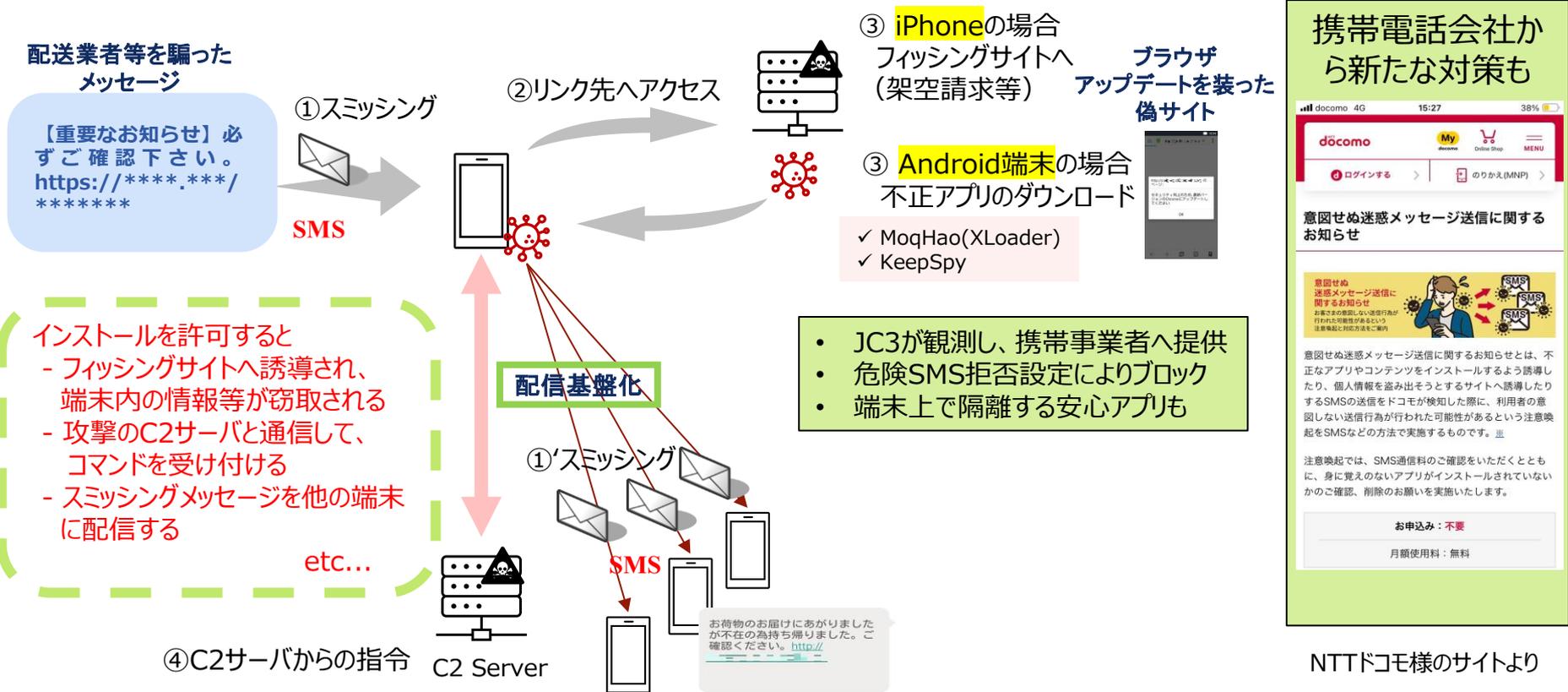
【図表 12：フィッシング報告件数及びクレジットカード不正利用被害額（概数）の推移】



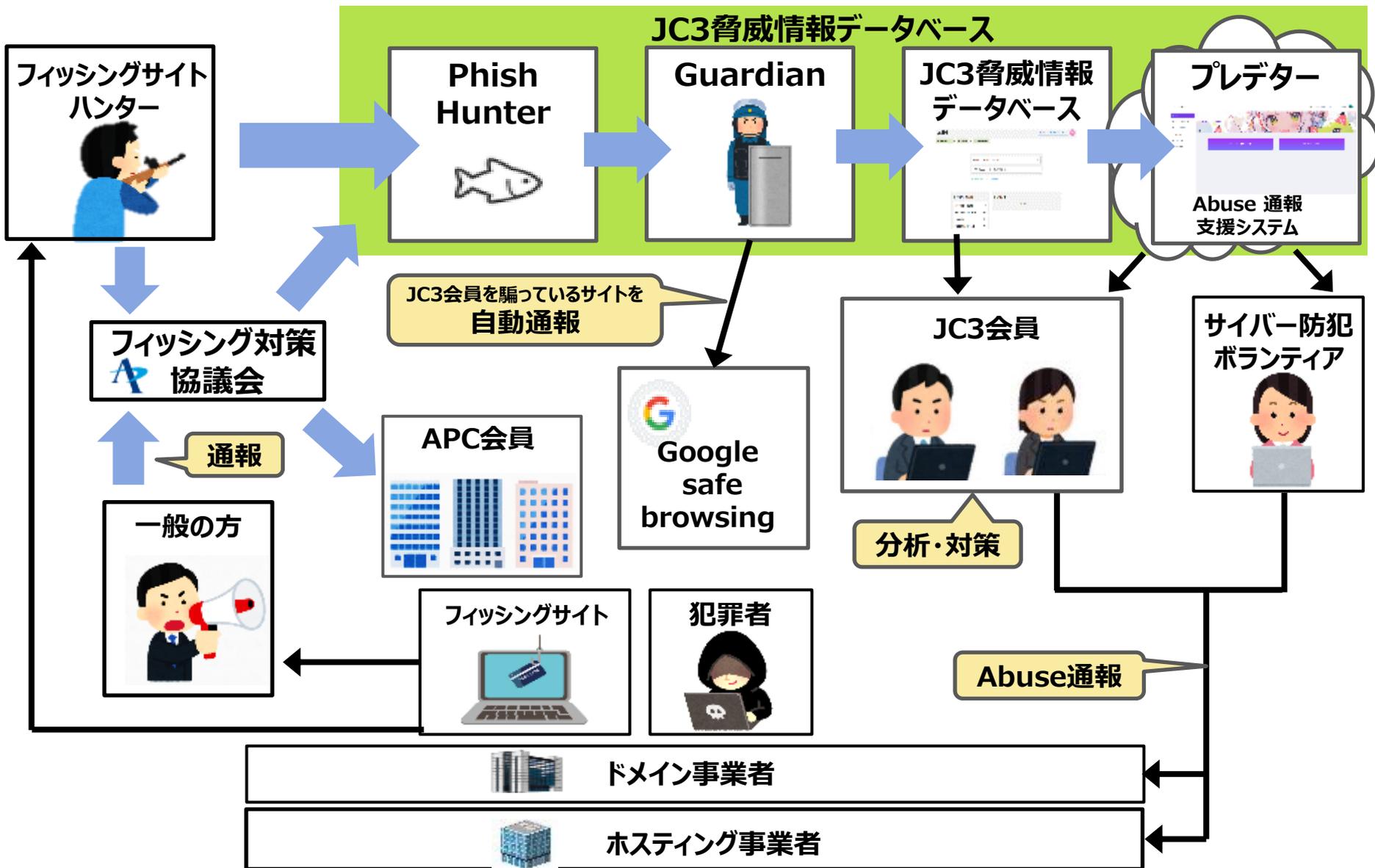
※ 一般社団法人日本クレジット協会・クレジットカード不正利用被害の発生状況から作成

引用元：警察庁「令和6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」

SMSから始まるフィッシング被害（モバイルマルウェア）



JC3におけるフィッシングサイト対策



フィッシング対策への取組

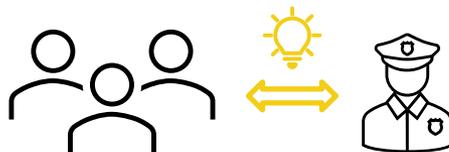
収集

連携・分析

対応



不正送金事犯情報分析PJ



- ✓ 被害実態
- ✓ 手口・傾向

システム

収集・分類

- BP
- CP
- MP
- :

ノウハウの蓄積



検知・防御



注意喚起



ブラウザブロック



テイクダウン

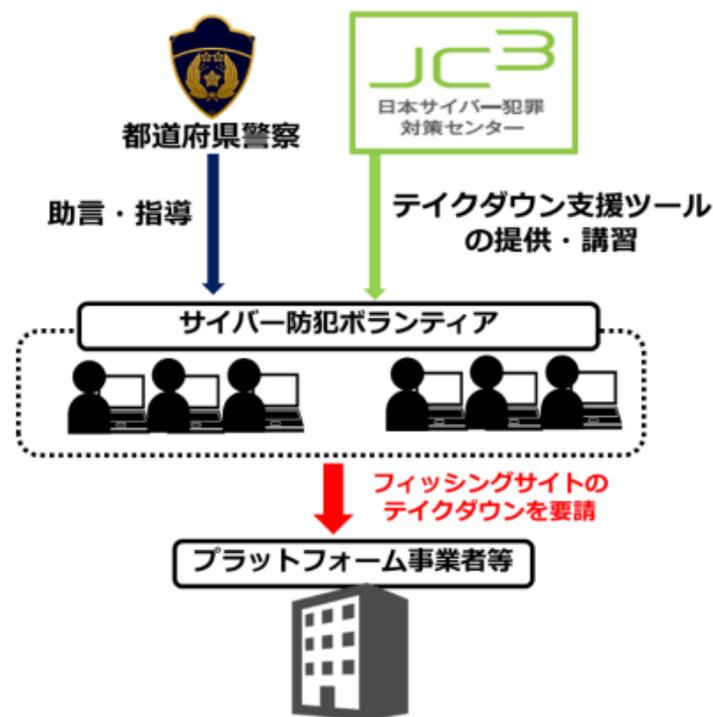


サイバー防犯ボランティア

フィッシング対策への取組（警察庁）

- フィッシングサイトの閲覧防止対策として、各都道府県警察では、サイバー防犯ボランティアの拡大・活性化を図るとともに、フィッシングサイトのテイクダウンがより効果的に行われるよう各団体へ助言・指導している。 加えて、一般財団法人日本サイバー犯罪対策センター（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、令和6年2月から3月にかけて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」を実施しており、警察庁はこれを後援している。

【図表 16：サイバー防犯ボランティアへの支援】



引用元：警察庁「令和6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」

フィッシングサイト撲滅チャレンジカップ

■ 第1回 概要

- 期間：令和6年2月13日～20日
- 参加者：125名
 - 都道府県警察 20都道府県警
 - ボランティア団体 27団体
- 大会結果
 - Abuse報告数：9,319件、テイクダウン数：268件

■ 第2回 概要

- 期間：令和6年7月22日～29日
- 参加者：359名
 - 都道府県警察 31都道府県警察
 - ボランティア団体 48団体
- 大会結果
 - Abuse報告数：12,072件、テイクダウン数：2,201件

結果の詳細等はこの後の「C11」のセッションで

**第2回
フィッシングサイト撲滅
チャレンジカップ**

【開会式】
7/22 (月) 11:00～ (online)

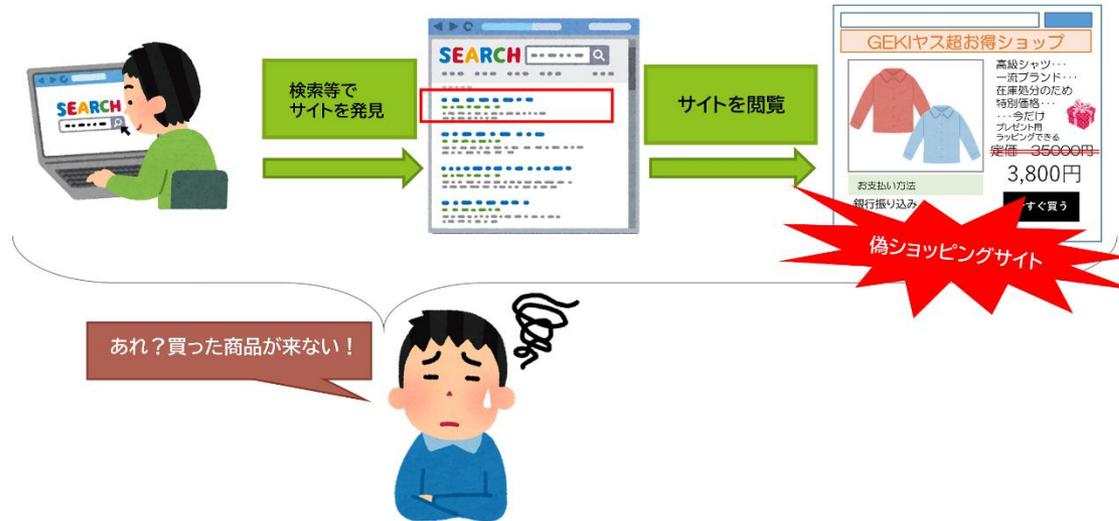
【開催期間】
7/22 (月) 12:00～ 7/29 (月) 18:00

【閉会式・表彰式】
8/8 (木) 13:30～
(さいたま市大宮区 アニメーションセンター)
※ 埼玉県警察による啓発イベントを同時開催

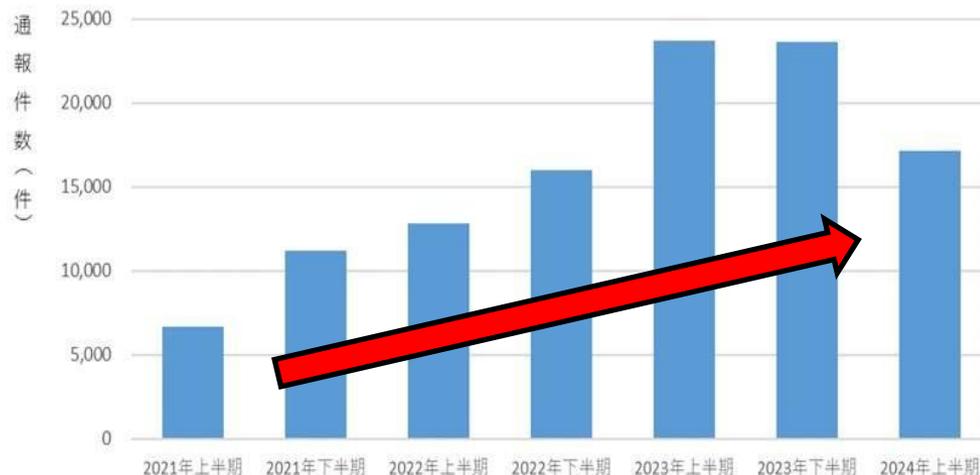
【主催】 一般財団法人日本サイバー犯罪対策センター
【後援】 サイバーセキュリティ戦略本部 経済産業省 警察庁
フィッシング対策協議会
特定非営利活動法人日本ネットワークセキュリティ協会
【協力企業】 トレンドマイクロ株式会社
【協賛企業】 株式会社ラック Gftd Japan株式会社 日本電気株式会社
日本マイクロソフト株式会社 LINEヤフー株式会社

偽ショッピングサイトでクレジットカード情報が盗まれる

■ 検索結果の上位に偽ショッピングサイトが表示される (行為者によるSEOポイズニング)



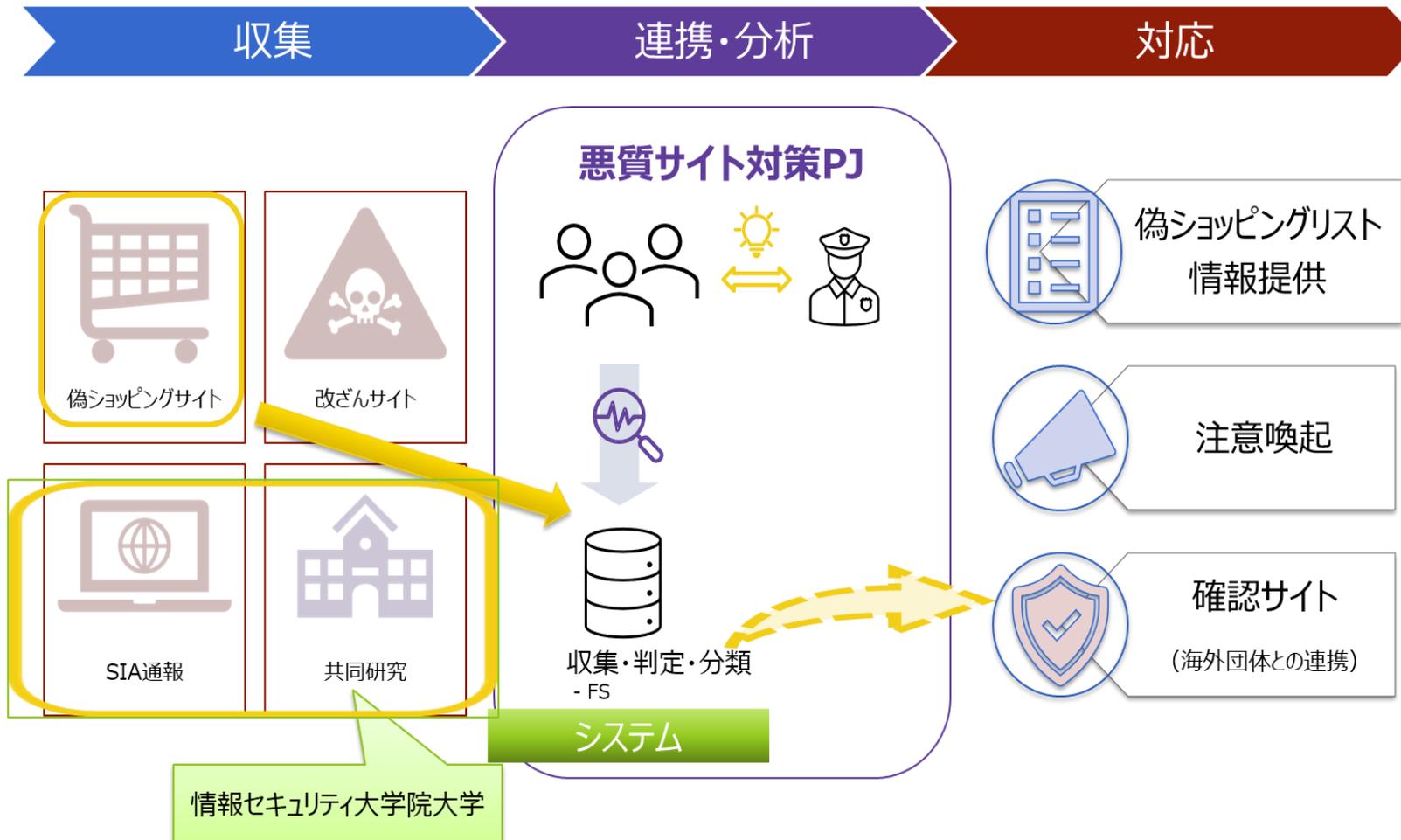
悪質ECサイトホットラインセンターに寄せられた通報



	2020年	2021年	2022年	2023年	2024年 上半期
インターネット検索結果	6,473	12,360	17,777	34,639	11,737
メールに記述されていたURL	1,311	2,614	4,502	4,551	2,604
X (旧Twitter) 等のSNS投稿	676	740	1,267	2,028	638
掲示板などの投稿	162	265	356	325	129
インターネット検索広告	—	—	—	2,518	709
その他	1,342	1,899	4,881	3,003	1,286

	2020年	2021年	2022年	2023年	2024年 上半期
銀行振込	1,505	1,502	2,704	3,795	1,438
クレジットカード決済	512	988	1,160	1,279	484
その他	478	567	979	1,461	940

偽ショッピングサイトに関する取組



毎月約2万件の情報を会員企業、APWG、ScamAdviserに提供

ScamAdviserへの情報提供

SAGICHECK

Check a website:

ウェブサイトへアクセスする前に、信頼できるウェブサイトかどうか、「SAGICHECK」で確認してみま

確認したいウェブサイトのアドレスを入力してください



ここにURLを
入力すると

ご利用になる前に

「SAGICHECK」では、安心してウェブサイトをご利用いただくために、できる限り最新の情報を提供するべく努力を行っていますが、インターネットの情報は、日々変化しており、結果は完璧ではありません。「SAGICHECK」の情報は、あくまでご自身のご判断の参考としてご利用ください。

なお、本サービスの情報は参考情報の提供を目的としたものであり、情報については本サイトは一切責任を負いません。詳しくは免責をご確認ください。

ご協力いただいている皆様



Gogolook



この取組について | お問い合わせ | 免責 | Developed By: SCAMADVISER

SAGICHECK

確認結果 gmmrk.cqhuaer.com リスクについて

このサイトは **安全ではないかもしれません**
常に自身で確認・判断してください(免責)



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、信頼性の組織の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、信頼性の組織の名前をクリックして、信頼性の組織に直接連絡してください。

結果が表示
される

- CERT NZ has no data for this website
- Unknown
- 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す
- 報告があります
- コンテンツはブロックされていません
- コンテンツはフィルタリングされていません
- インディケーションがありません
- 過去3ヶ月間、Pulsediveに報告されていません
- マルウェアは報告されていません
- 非常に低い信頼スコアです (full gmmrk.cqhuaer.com report)

CleanBrowsing:

DNSFilter:

IQ Global:

Pulsedive:

Quadd:

Scamadviser:

詳細情報

サイトの年齢:

2024年8月1日

サーバーの場所:

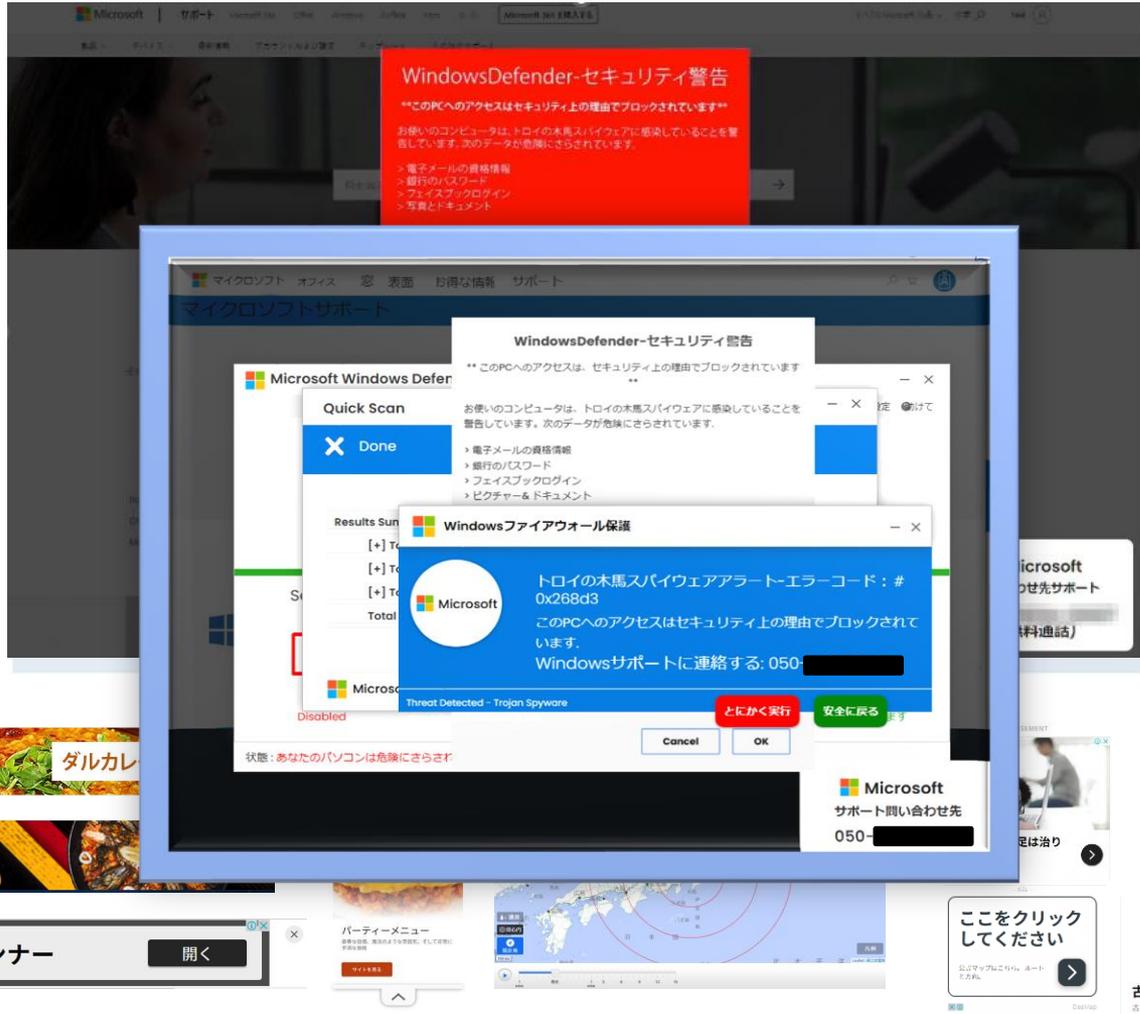
CA



<https://sagicheck.jp/>

テクニカルサポート詐欺 ～誰もが遭遇する恐れのある被害～

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ます。
あなたなら記載のサポートに電話しますか？



電話をかけるとうどうなるかを知っておきましょう

 **テクニカル サポート詐欺 調査**
電話をかけた場合に何が起るのか

詐欺の流れ

- ① 使用しているキーボードの種類を確認
- ② Windowsキー + Rから遠隔操作ツール接続先のURLを入力させる
- ③ 遠隔操作ツールの接続認証コードを入力させて遠隔操作を開始
- ④ 個人情報やカメラ・音声録音など端末情報が窃取される
- ⑤ 支払いの説明
- ⑥ 支払い方法を選ばせる（ギフトカード・銀行振り込み・クレジットカード）
- ⑦ 購入方法の指示
- ⑧ 執拗に支払いを迫られる

**あの、ネット銀行使っていますから
一回ね、ネット銀行開いてください**



<https://www.jc3.or.jp/threats/examples/article-570.html>

- 電話をかける時点で騙されています。**絶対に画面の電話番号に電話しないでください。**
- サポート詐欺に限らずパソコンを使って困ったことが起きたら、親しい身の回りの方や警察に相談してください。

※ 参考文献 サイバーグリッドジャーナルVol.15 特集1 突然の警告!? サポート詐欺の謎に迫る!

https://www.lac.co.jp/lacwatch/pdf/20230302_cgjournal_vol15.pdf

- ✓ 攻撃者、犯罪者は、互いの専門性を共有し、合法、違法様々な手段、方法を講じている。

← **現実の脅威に対抗することは、一企業、一組織単独では困難**

◆ **情報とリソースの共有が重要**

業界を超えて、官民学の違いを超えて

攻撃の主体、動向、対象、手法、犯罪インフラ等のリアルな実態を把握

◆ **<企業>と<法執行機関>等との**連携の「場」**の提供（JC3）**

<定期的+随時>の情報共有等の場の設定

→ 業界を超えた関係者間の相互理解の醸成

脅威へ立ち向かう目的意識を共有する関係者による信頼関係、同志的関係の構築

関係者が活用できるデータ、情報の収集、整理

◆ **攻撃者のエコシステムへの対抗**

社会全体での、攻撃しづらい環境・システムの構築

ご清聴ありがとうございました



Japan Cybercrime Control Center
