

レジデンシャルプロキシとサイバー犯罪 ～ Disruptionの必要性 ～

2026年9月

日本サイバー犯罪対策センター（JC3）

業務執行理事 櫻澤 健一

info@jc3.or.jp

【参考】JC3の組織概要

一般財団法人 日本サイバー犯罪対策センター 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、事後的な防護措置を講ずる受け身の対応ではなく、産学官(警察)それぞれが持つ対処経験を集約・分析した情報を共有し、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



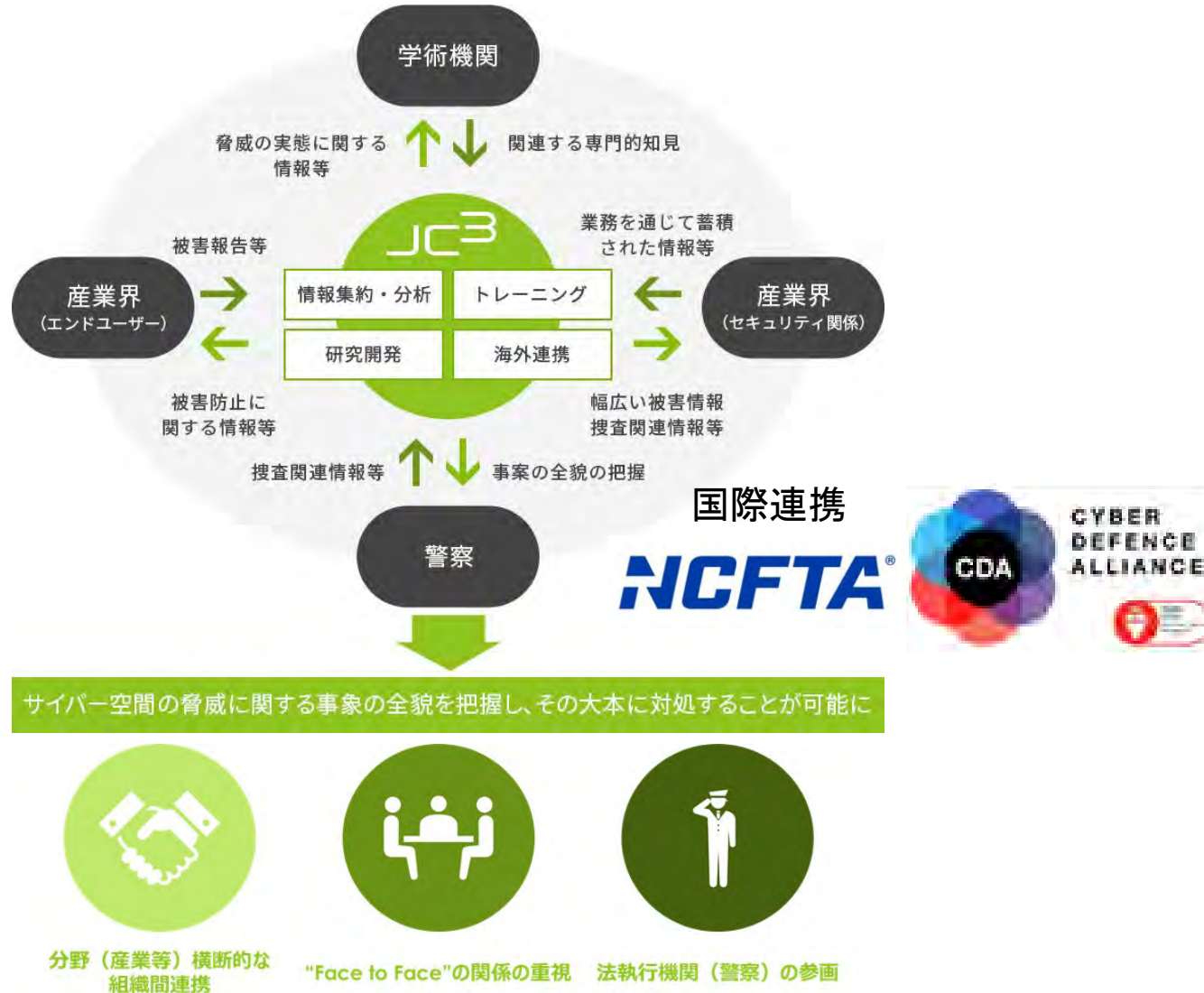
～米国のモデル～ N C F T A = National Cyber-Forensics & Training Alliance

米国の**非営利法人**N C F T Aは2002年以降、FBIをはじめとする法執行機関、大学等の学術機関及び200以上の民間企業との連携組織とし活動しており、迅速かつ具体的な情報収集・共有、50人以上のアナリストによる情報分析や法執行機関向けのトレーニングを提供している。



【参考】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



対策に向けた情報共有・分析

金融犯罪対策グループ
不正送金情報分析PJ、
テクニカルサポート詐欺PJ、モバイル事犯PJ

eコマース対策グループ
悪質サイト対策PJ、不正トラベルPJ

情報流出対策グループ
ランサムウェア攻撃実態解明PJ

対策の基盤となる活動

脅威情報グループ
暗号資産PJ、ソーシャルエンジニアリングPJ
AIセキュリティ研究PJ、DB改善

マルウェア解析グループ

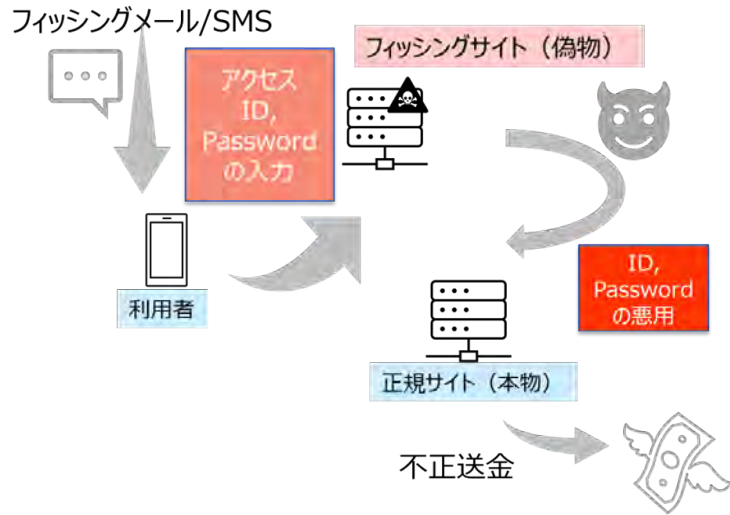
国際連携グループ

研究・研修グループ

フィッシングによるインターネットバンキング不正送金やクレジットカード不正利用の実態

貴方の個人情報狙われている！

■ 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の割合 2025年
(インターネットバンキングに係る不正送金事案数)

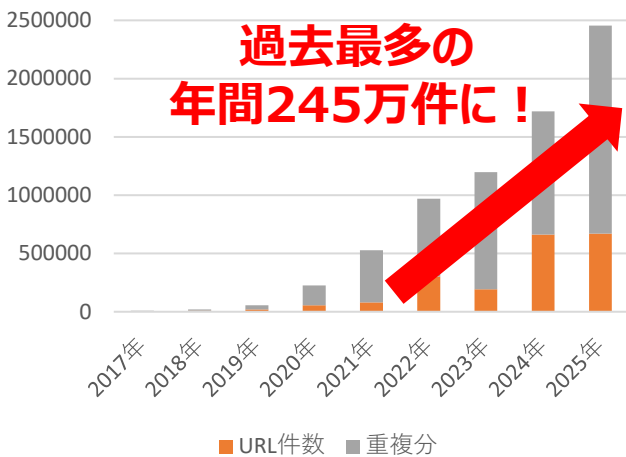


フィッシングサイトのターゲット一覧
(2025年 JC3調べ)



フィッシング通報件数
引用元：フィッシング対策協議会

**過去最多の
年間245万件に！**



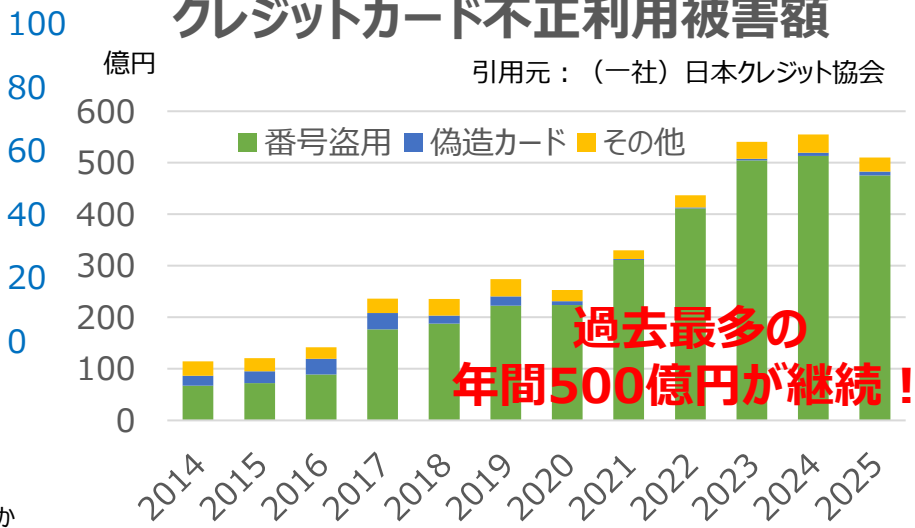
インターネットバンキングに係る不正送金



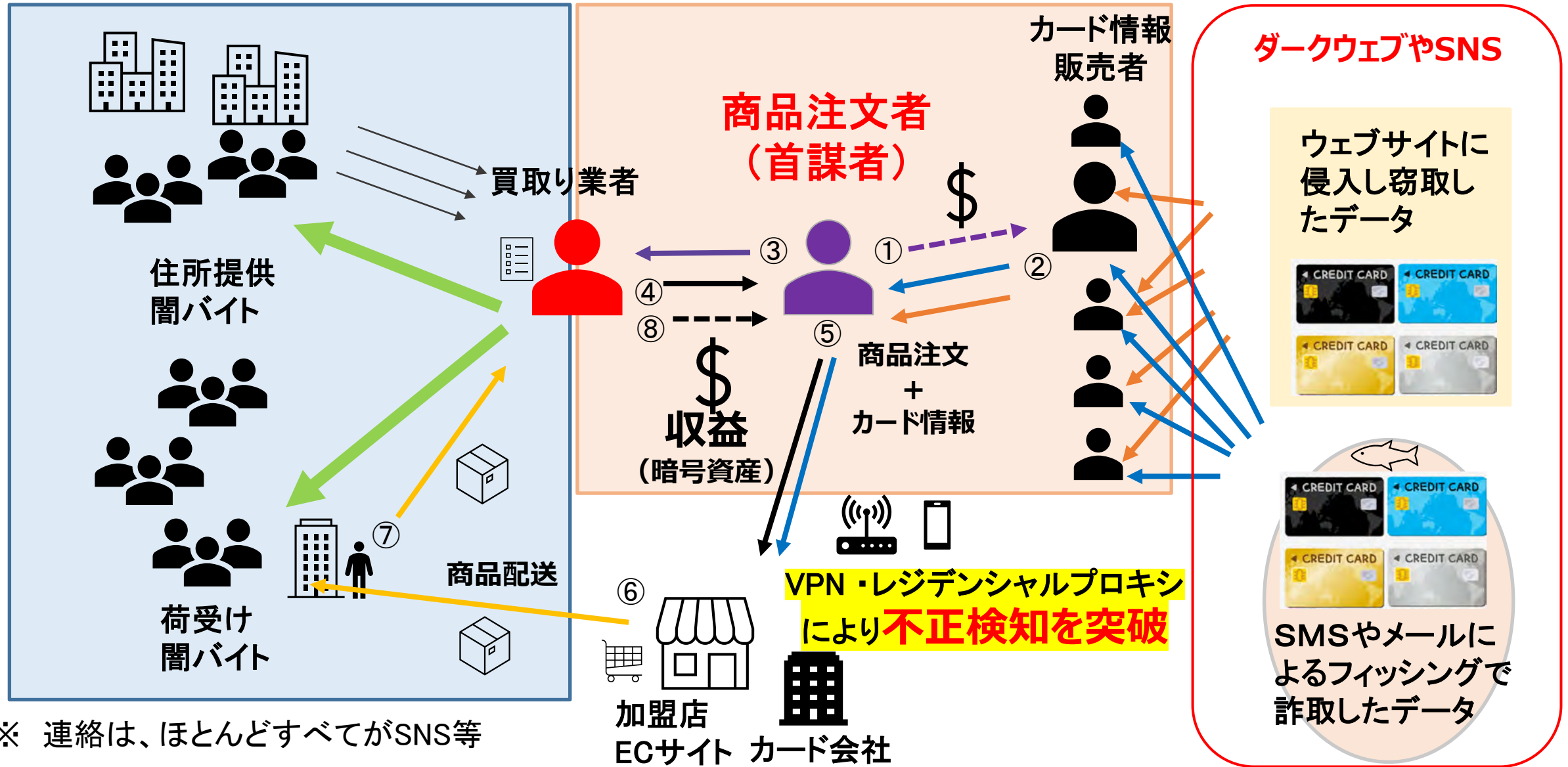
引用元：令和7年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）ほか

クレジットカード不正利用被害額

引用元：（一社）日本クレジット協会

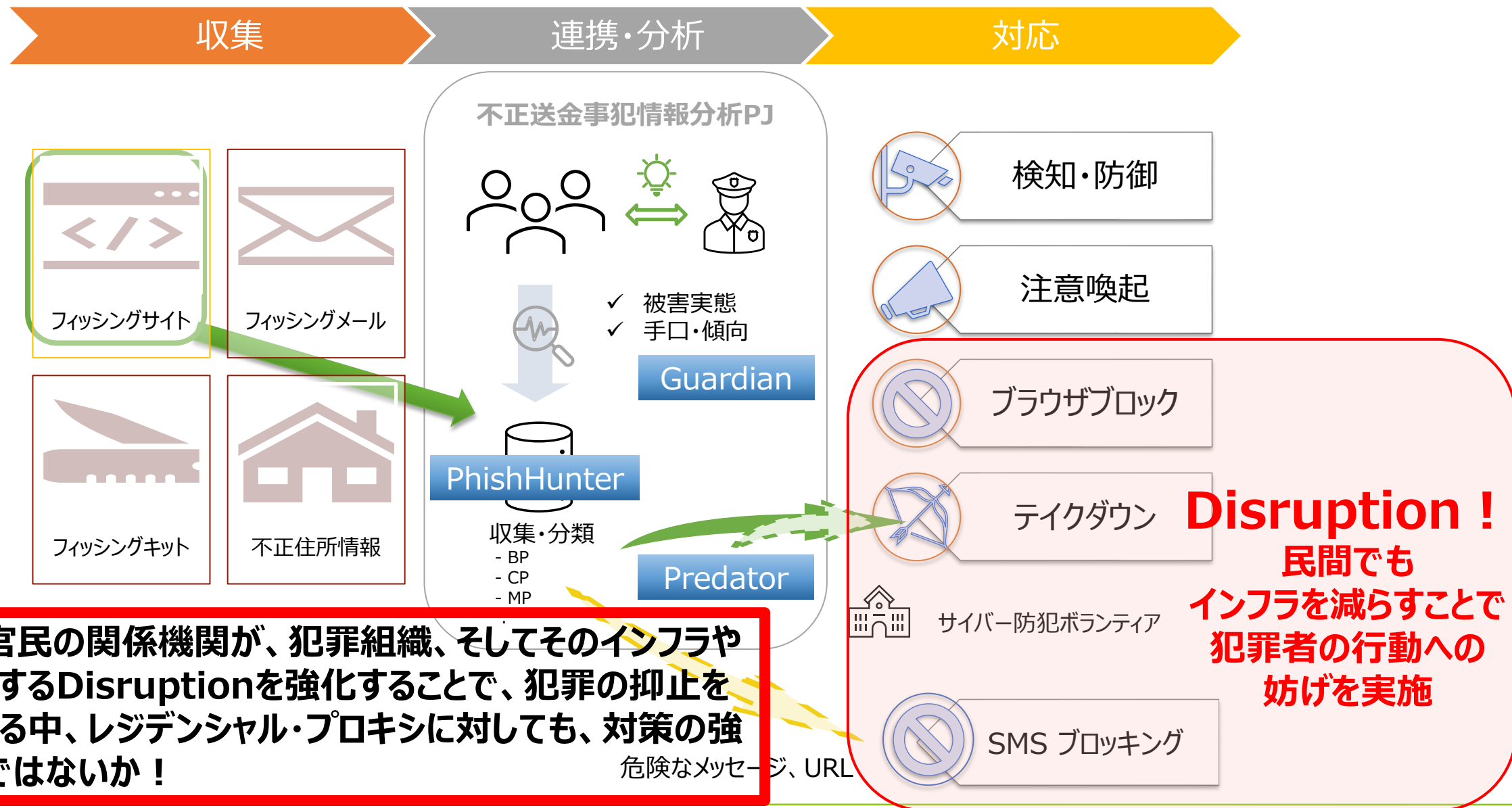


レジデンシャルプロキシを使った検知・アクセス制限の回避 ～クレカ不正利用の背景から～

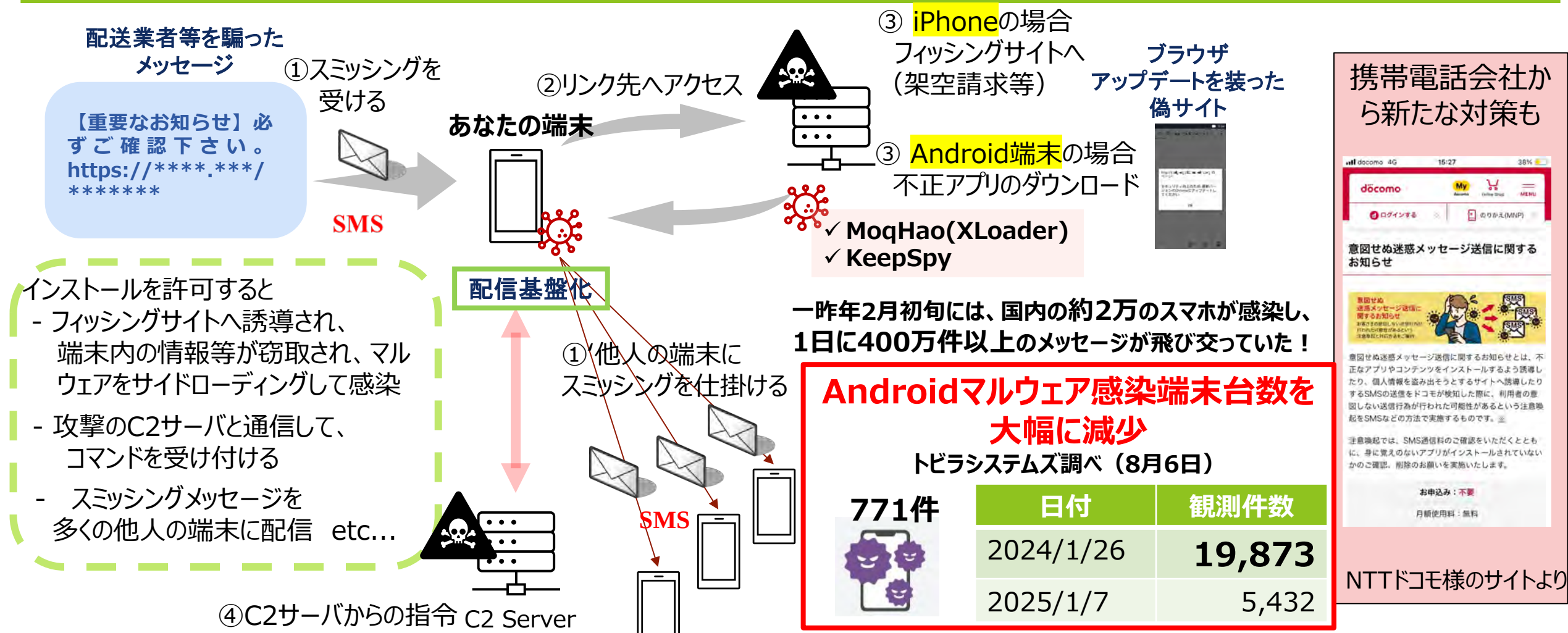


【構成員等限り】

Disruptionの重要性と必要性 ～JC3におけるフィッシング対策を参考に～



【参考】モバイル・ボットネットのDisruption ～モバイルマルウェアによるSMS攻撃を教訓に～



<JC3メンバーの協働による対抗策>

JC3事務局がSMSを観測し、情報を提供した会員企業である携帯事業者が行う危険SMS拒否設定によりブロック
会員企業のIT事業者が端末上で隔離する安心アプリを提供

【参考】テクニカルサポート詐欺対策としてMicrosoft社 DCU等と協働したDisruption！

テクニカルサポート詐欺の全体像

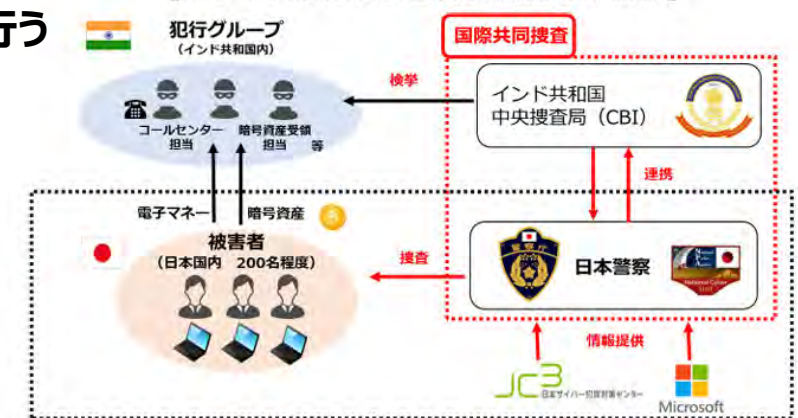


**インドで偽サポートセンターを運営する
被疑者グループを国際共同捜査で検挙！**

インド共和国の法執行機関である中央捜査局(CBI)は日本の警察庁と国際共同捜査を進め、5月28日、インド国内においてテクニカルサポート詐欺の被疑者6人を逮捕するとともに、関係先19カ所の捜索を行ったと発表しました。CBIが捜索した2カ所の違法な偽コールセンターはマイクロソフトのカスタマーサポートになりすましており、約200人の日本人を対象詐欺を行い1億8千万円もの被害を及ぼしました。

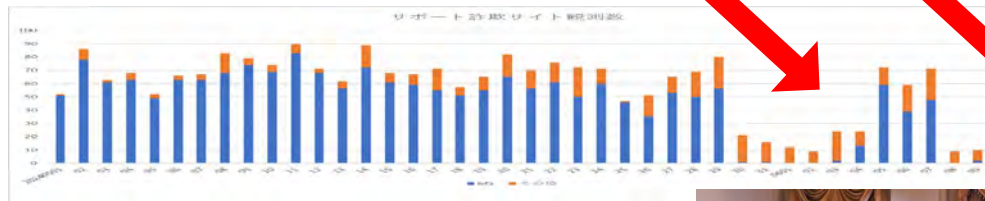
JC3 はマイクロソフトなどとともに日本に関する関係情報の収集・分析・共有を行い、警察庁及び CBI が行う犯罪捜査に全面的に協力しています。

【インド共和国との国際共同捜査の概要】



Microsoft、AWSとの協働でWebサイトをテイクダウン！

JC3で収集したデータを提供し、**テイクダウン**を継続中
ネット上に現れる偽警告画面数



【参考】金融ISAC及び全国の各金融機関等との一斉注意喚起 (2023年)

公開日: 2023.08.31 更新日: 2023.09.04

不正送金被害にあわないために[一斉注意喚起]

✉ Eメール SMS 不正送金 銀行

JC3は、金融ISAC※及び各金融機関等と連携して、本日（8月31日）改めて、フィッシングによるものとみられるインターネットバンキングに係る不正送金による被害を軽減するための一斉注意喚起を行います。

8月8日、警察庁は、令和5年上半期の不正送金被害件数が急増し過去最多を更新したことを発表しました（8月4日時点において、令和5年上半期における被害件数は、過去最多の2,322件。被害額も約30.0億円 https://www.npa.go.jp/bureau/cyber/pdf/20230808_press.pdf）。不正送金の被害にあわないためには、電子メール等のリンクからアクセスしたサイトに、IDパスワード・個人情報を入力しないことが肝要です。金融機関を装って届くメールには、「個人情報の再確認…」、「不正アクセス通知…」、「口座を解約…」といった不安にさせることが書かれています。このようなメールが届いても、慌てずに各金融機関の「公式HP」や「公式アプリ」を使用してアクセスするようにしてください。

※ 一般社団法人 金融ISACは、日本の金融機関によるサイバーセキュリティに関する情報の共有及び分析を行い、金融機関の安全性の向上を推進することにより、利用者の安心/安全を継続的に確保することを目的として、430以上の金融機関を会員とする団体です。

JC3コラム - 悪質な不正送金の実態 <https://www.jc3.or.jp/threats/topics/article-508.html>

不正送金被害急増中!!

電子メール等のリンクから
アクセスしたサイトに
IDパスワード・個人情報
を入力しないで下さい

不安にさせるメールに注意!!

個人情報の再確認…
不正アクセス通知…
口座を解約…

金融機関の「公式HP」「公式アプリ」
から正しい情報を確認してください

金融庁
Financial Services Agency

警察庁
National Police Agency

JBA 一般社団法人
全国銀行協会

JC3 日本サイバー犯罪対策センター

不正送金被害 過去最悪!!

年末年始は特に3メガバンクを
かたるフィッシングに注意!!

「不正アクセス」、「個人情報の確認」
「取引の停止」等のワードに注意!

※ 金融機関が、ID・パスワード等をSMS等
で問い合わせることはありません

※ 金融機関の「公式HP」「公式アプリ」から
正しい情報を確認してください

金融庁
Financial Services Agency

警察庁
National Police Agency

JBA 一般社団法人
全国銀行協会

JC3 日本サイバー犯罪対策センター

参加金融機関等(9月15日現在 40社)

トレンドマイクロ、LAC、SBI新生銀行、セブン銀行、みずほ銀行、三井住友銀行、三菱UFJ銀行、ゆうちょ銀行、三井住友信託銀行、野村證券、あおぞら銀行、住信SBIネット銀行、PayPay銀行、auじぶん銀行、大和ネクスト銀行、

北海道銀行、青森銀行、みちのく銀行、秋田銀行、岩手銀行、東邦銀行、横浜銀行、山梨中央銀行、北陸銀行、北國銀行、十六銀行、京都銀行、南都銀行、山口銀行、百十四銀行、琉球銀行、西日本シティ銀行、北九州銀行、東日本銀行、愛知銀行、もみじ銀行、香川銀行、福岡中央銀行、埼玉縣信用金庫、奈良中央信用金庫

(了)