サイバー空間の脅威の現状とJC3の主な取組

～　官民学の情報共有と新たな対策に向けて　～

2024年7月

日本サイバー犯罪対策センター（JC3）　櫻澤健一
info@jc3.or.jp

JC3 Japan Cybercrime Control Center

JC3 日本サイバー犯罪対策センターの概要

JC3の組織概要

今秋が10周年です！

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～ＮＣＦＴＡ＝National Cyber-Forensics & Training Alliance

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た非営利法人としてＮＣＦＴＡを創設。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て活動しており、迅速な情報収集、50人以上のアナリストによる情報分析、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。

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）

1. ｱﾌﾗｯｸ生命保険株式会社
2. Auﾌｨﾅﾝｼｬﾙﾎｰﾙﾃﾞｨﾝｸﾞｽ株式会社
3. SBIﾎｰﾙﾃﾞｨﾝｸﾞｽ株式会社
4. 株式会社SBI証券※
5. SBI EVERSPIN株式会社※
6. NRIｾｷｭｱﾃｸﾉﾛｼﾞｰｽﾞ株式会社
7. 株式会社NTTﾃﾞｰﾀ
8. 株式会社NTTﾃﾞｰﾀﾌｨﾅﾝｼｬﾙﾃｸﾉﾛｼﾞｰ※
9. 株式会社SBI新生銀行
10. 株式会社ｱﾌﾟﾗｽ※
11. 新生ﾌｨﾅﾝｼｬﾙ株式会社※
12. 株式会社ｼﾞｪｰｼｰﾋﾞｰ
13. ｾｺﾑ株式会社
14. 株式会社セブン銀行
15. 株式会社ACSiON※
16. 株式会社ｿﾘﾄﾝｼｽﾃﾑｽﾞ
17. ﾃﾞﾛｲﾄ ﾄｰﾏﾂ ｻｲﾊﾞｰ合同会社
18. ﾄﾚﾝﾄﾞﾏｲｸﾛ株式会社
19. 日本電気株式会社
20. 日本ｱｲ・ﾋﾞｰ・ｴﾑ株式会社
21. 野村ホールディングス株式会社
22. 株式会社日立製作所
23. 株式会社bitFlyer
24. 富士通株式会社
25. 株式会社みずほ銀行
26. 株式会社三井住友ﾌｨﾅﾝｼｬﾙｸﾞﾙｰﾌﾟ
27. SMBCｺﾝｼｭｰﾏｰﾌｧｲﾅﾝｽ株式会社※
28. 株式会社日本総合研究所※
29. 株式会社三井住友銀行※
30. 三井住友信託銀行
31. 株式会社三菱UFJ銀行
32. 株式会社ﾒﾙｶﾘ
33. 株式会社ﾒﾙﾍﾟｲ※
34. 株式会社ゆうちょ銀行
35. LINEﾔﾌｰ株式会社
36. LINE Pay株式会社※
37. 株式会社ﾗｯｸ
38. 株式会社ﾘｸﾙｰﾄ
39. 株式会社りそなﾎｰﾙﾃﾞｨﾝｸﾞｽ
1. 株式会社あおぞら銀行
2. 株式会社ｲｵﾝ銀行
3. 株式会社NTTﾄﾞｺﾓ
4. Gftd Japan株式会社
5. KDDI株式会社
6. KELA株式会社
7. 株式会社 ｾﾌﾞﾝ&ｱｲ・ﾎｰﾙﾃﾞｨﾝｸﾞｽ
8. SocioFuture株式会社
9. ｿﾌﾄﾊﾞﾝｸ株式会社
10. Chainalysis Japan株式会社
11. 日本マイクロソフト株式会社
12. 株式会社ふくおかﾌｨﾅﾝｼｬﾙｸﾞﾙｰﾌﾟ
13. PayPay株式会社
14. PayPay銀行株式会社
15. 株式会社ﾐｽﾐｸﾞﾙｰﾌﾟ本社
16. 株式会社横浜銀行

◆ トライアル　５社

■ 警察庁
■ 情報ｾｷｭﾘﾃｨ大学院大学
■ 東京都立大学
■ 東京電機大学

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

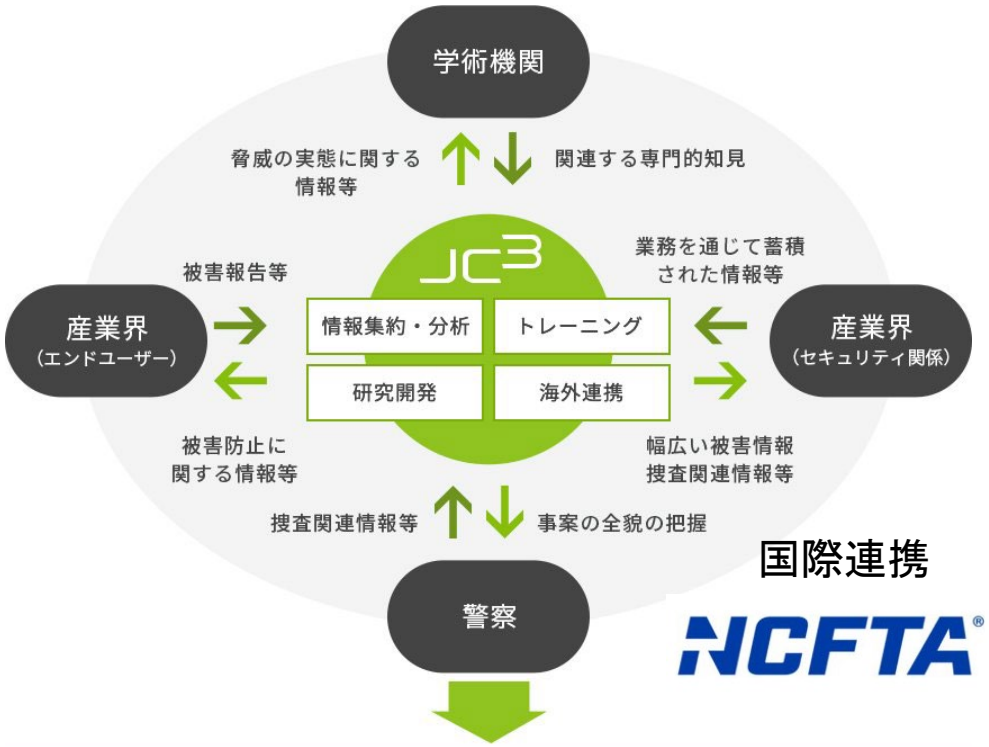
※：親子会社特例制度利用企業

（敬称略）

1.株式会社アーティサン
2.ｱｸｾﾝﾁｭｱ株式会社
3.株式会社一休
4.EY新日本有限責任監査法人
5.S&J株式会社
6.NECセキュリティ株式会社
7.株式会社FFRI
8.グーグル合同会社
9.KDDIデジタルセキュリティ株式会社
10.株式会社KPMG　FAS
11.高速道路トールテクノロジー株式会社
12.株式会社ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所
13.さくらｲﾝﾀｰﾈｯﾄ株式会社
14.ｻﾝ電子株式会社
15.株式会社JTB
16.ｼｽｺｼｽﾃﾑｽﾞ合同会社
17.Splunk Services Japan合同会社
18.Sky株式会社
19.住信SBIﾈｯﾄ銀行株式会社
20.全日本空輸株式会社
21.綜合警備保障株式会社
22.株式会社ソフトプレックス
23.損害保険ジャパン株式会社
24.ﾃﾞｼﾞﾀﾙﾎｰﾙﾃﾞｨﾝｸﾞｽ株式会社
25.東京海上日動火災保険株式会社
26.TOPPANﾎｰﾙﾃﾞｨﾝｸﾞｽ株式会社
27.ﾈｯﾄﾜﾝｼｽﾃﾑｽﾞ株式会社
28.BBｿﾌﾄｻｰﾋﾞｽ株式会社
29.PwCｺﾝｻﾙﾃｨﾝｸﾞ合同会社
30.ﾌｫｰﾃｨﾈｯﾄｼﾞｬﾊﾟﾝ合同会社
31.BLACKPANDA JAPAN株式会社
32.株式会社マキナレコード
33.三井住友海上火災保険株式会社
34.三井物産ｾｷｭｱﾃﾞｨﾚｸｼｮﾝ株式会社
35.株式会社三越伊勢丹ｼｽﾃﾑ・ｿﾘｭｰｼｮﾝｽﾞ
36.三菱ＵＦＪﾆｺｽ株式会社
37.Musarubra Japan株式会社
38.株式会社ﾚｲ・ｲｰｼﾞｽ・ｼﾞｬﾊﾟﾝ

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

分野（産業等）横断的な組織間連携　“Face to Face”の関係の重視　法執行機関（警察）の参画

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、ﾃｸﾆｶﾙｻﾎﾟｰﾄ詐欺PJ、ﾓﾊﾞｲﾙ事犯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

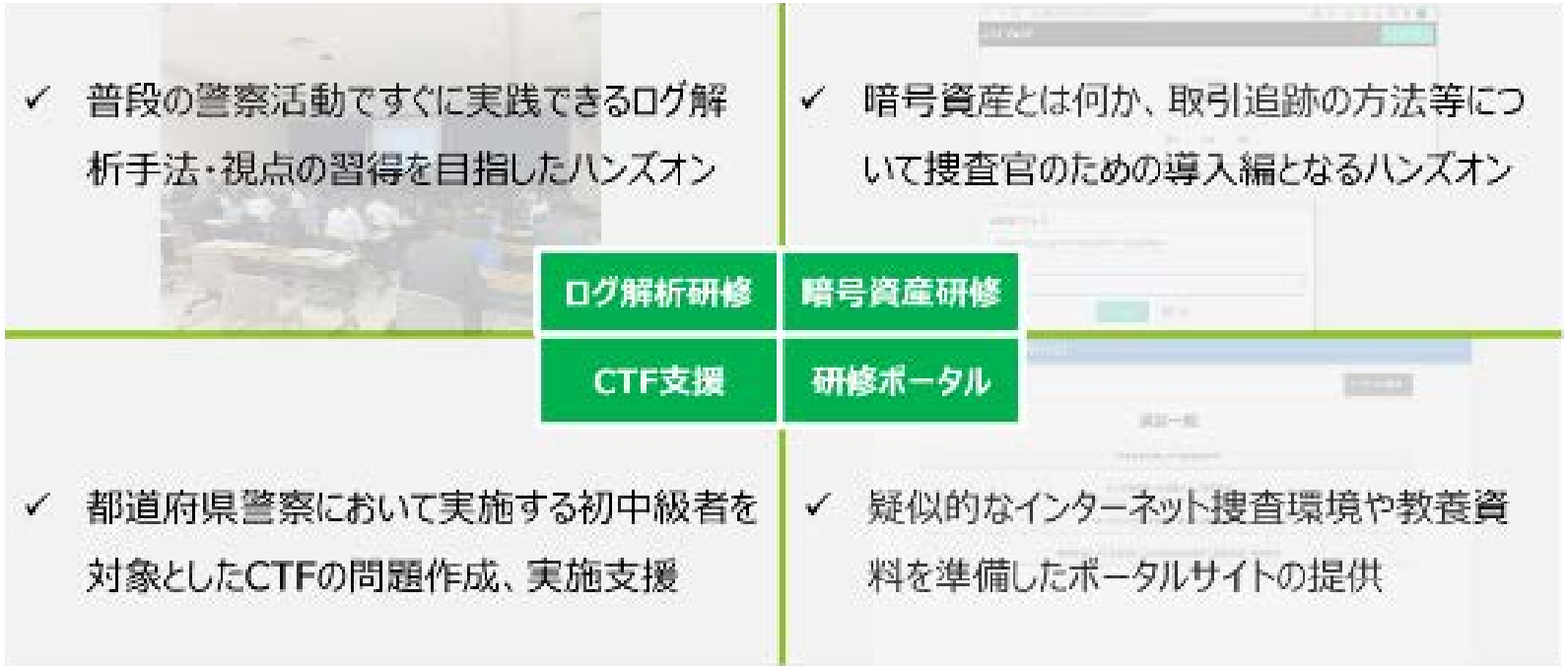
対策の基盤となる活動

- 脅威情報グループ
  DB改善、暗号資産、ｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞ
- 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

法執行機関向け研修事業

- 法執行機関のサイバー脅威への対処能力向上支援を目的に、各種トレーニングプログラムを提供
- **ログ解析研修（基礎編、サイバー攻撃編）、暗号資産研修、CTF支援、クラウドフォレンジック研修**について実施しながら、更なる高度な研修を開発中
- **サイバーパトロール支援システム**の提供

2022年度におけるトレーニングプログラムの概要



国際連携（米国NCFTAのフォーラムに参加）

4月22日（月）から25日（木）、米国ピッツバーグにて開催予定

クローズドの会合に、昨年は９００名以上が参加！

テーマは　　＃DISRUPTION

※　米国サイバーセキュリティ戦略には、「NCFTAと連携し、脅威アクターを混乱（Disrupt）させ、破壊（Dismantle）する」との記述」あり

JC3メンバーは、NCFTA本部訪問やNYオフィスでの米国会員企業の皆様との会合も計画しています

JC3メンバーによるプレゼンテーション

ライトニング　トークにて

G7茨城水戸　内務・安全担当大臣会合への参加

G7 Interior and Security Ministers' Communiqué

December 10, 2023 in Mito, Ibaraki

G7 2023 HIROSHIMA SUMMIT

MITO IBARAKI

the japan times

JAPAN / POLITICS

G7 agrees in Japan to enhance cooperation against organized fraud

Interior and security ministers from the Group of Seven major countries meet in the city of Mito, in Ibaraki Prefecture, on Sunday to step up cooperation in the fight against cross-border organized fraud. | KYODO

https://www.npa.go.jp/bureau/soumu/kokusai/20231210_G7ISMM_communique_principal.pdf

セッション2：サイバー空間の安全確保

・本セッションでは、冒頭、日本サイバー犯罪対策センター（JC3）の堺代表理事から、我が国のサイバー空間をめぐる情勢やJC3の取組について説明がありました。

・これを受けて、ランサムウェアやフィッシング、国家を背景とするサイバー攻撃といったサイバー空間上の脅威への対処について議論しました。

・松村国家公安委員会委員長からは、ランサムウェアやフィッシング等の被害防止に向けた官民連携の取組を紹介したほか、国境を越えるサイバー事案に対処するため、警察庁のサイバー特別捜査隊を中心にG7各国の捜査機関と国際共同捜査を推進している旨の発言があり、国際連携の必要性について確認しました。

・各国からも企業を含めた国際社会の取組や、国際的な捜査協力の推進の必要性に関し活発な発言があり、G7として、捜査能力の向上を図りながら、サイバー事案の厳正な取締りや実態解明、官民連携等を推進していくことを確認しました。

JC3 Japan Cybercrime Control Center

サイバー空間からの攻撃や犯罪

～ありとあらゆる方法で、個人情報・資産と安全が狙われている！～

JC3の活動からわかること

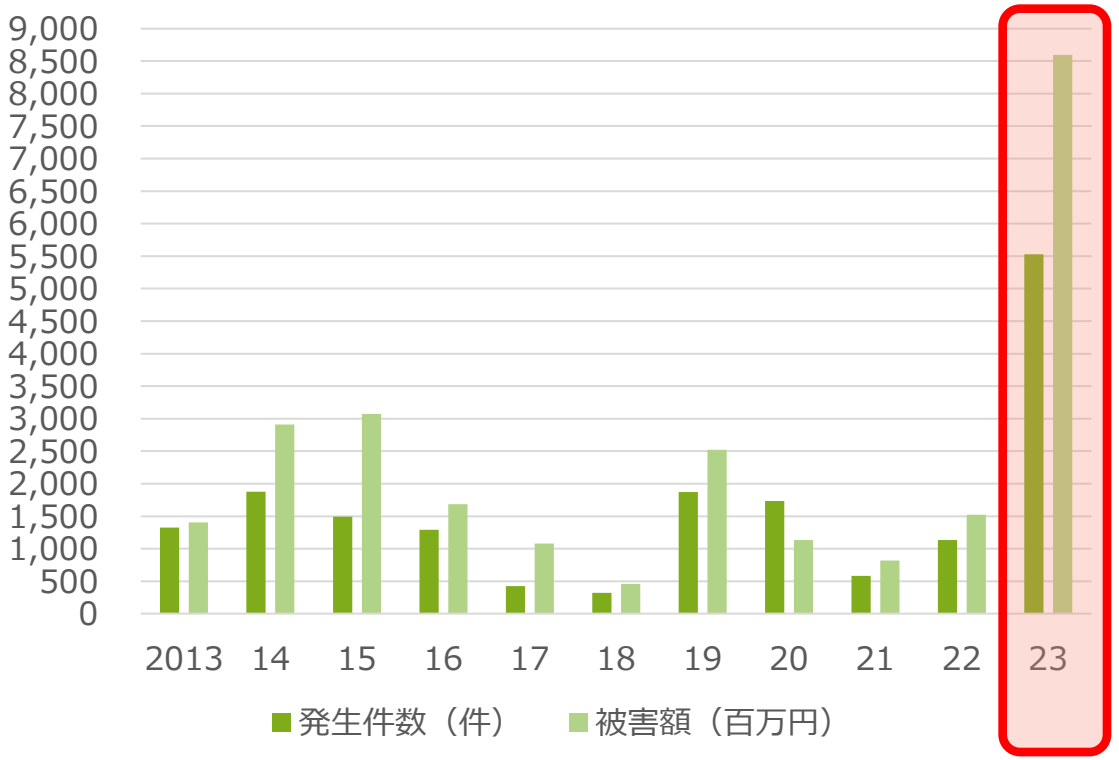
・フィッシングによる情報窃取と詐欺
・ランサムウェア攻撃
・偽ショッピングサイト
・テクニカルサポート詐欺
・標的型APT攻撃　　等

情報窃取の裏側にあるフィッシング　～ インターネットバンキングの不正送金も激増 ～

貴方の個人情報が狙われている！

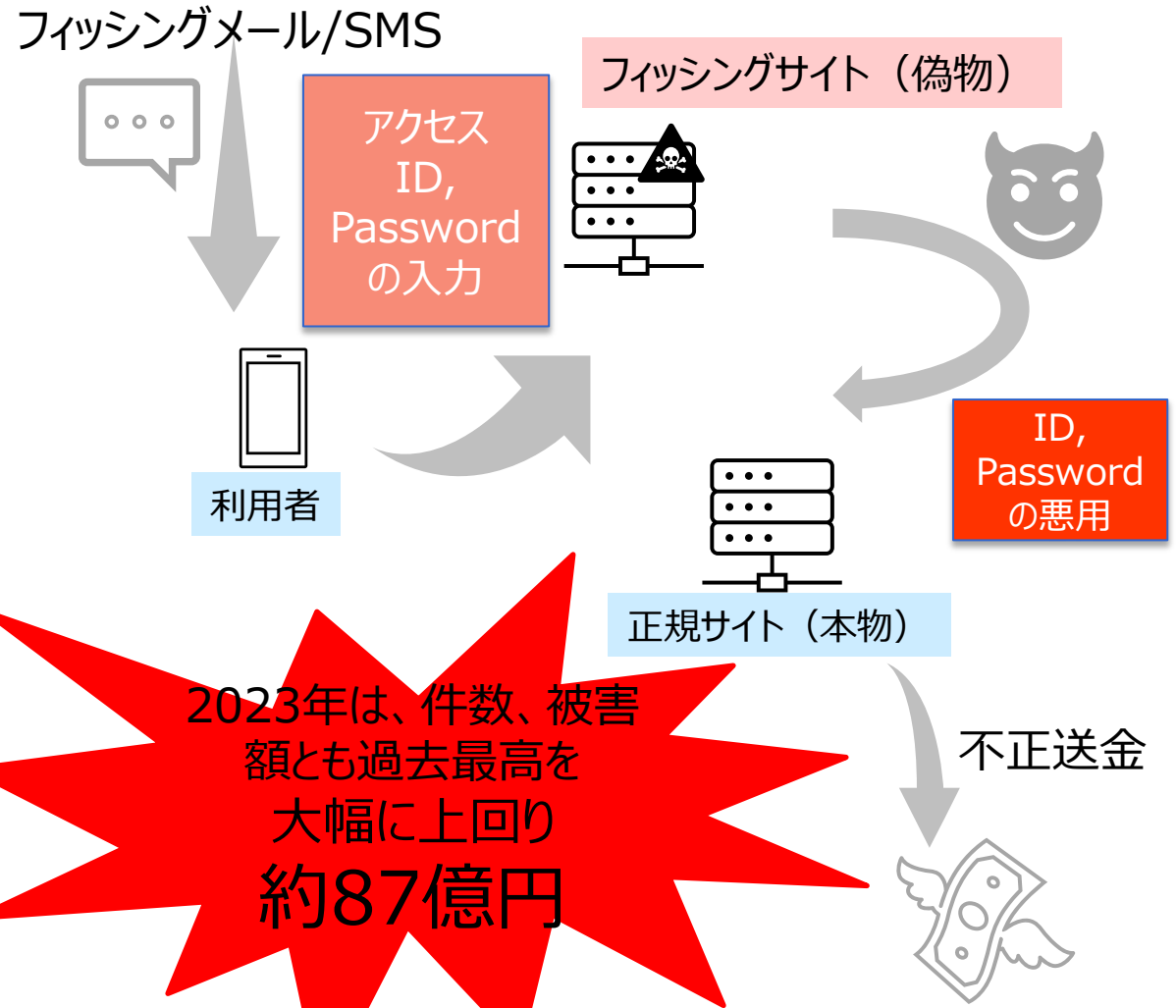
■ 発生件数・被害額

JC３会員企業・警察の連携により減少するも、反転・急増



引用元：令和５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

■ フィッシング(Phishing)による不正送金



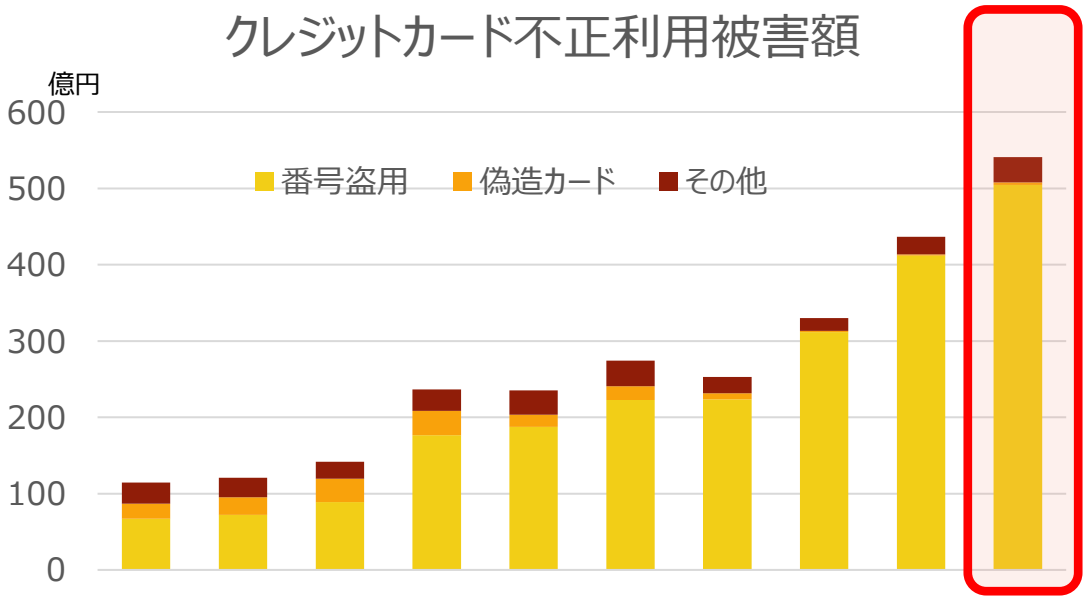
フィッシングターゲットの拡大・変遷により多くの個人情報が漏洩

フィッシングによる被害

- クレジットカード情報を窃取するフィッシングサイトが多数存在
- 不正クレジットカード利用も！
  - 不正購入 →（配送）→ 換金
  - 各種決済サービスに紐づけ

過去最多の
年間540億円に！

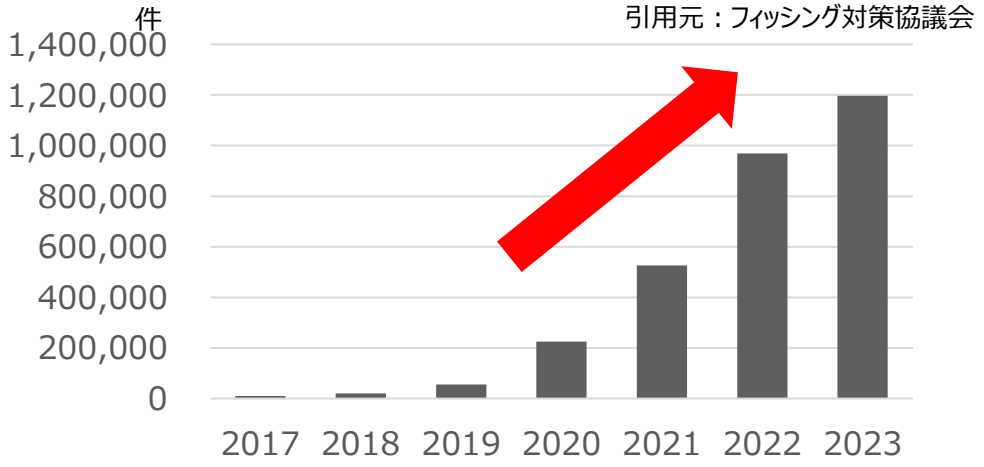
クレジットカード不正利用被害額



引用元：（一社）日本クレジット協会

ターゲット別のフィッシングサイト内訳
（JC３独自調査（PhishHunterの集計結果より）

フィッシング報告件数



引用元：フィッシング対策協議会

見分けられない実際のフィッシングサイト（ホームページやメディアを通じての注意喚起）

偽サイトは本物そっくり

本物の銀行のWebサイトと見分けのつかないそっくりなフィッシングサイトが多数発見されています。（これは一例です。画像は一部加工しています。）

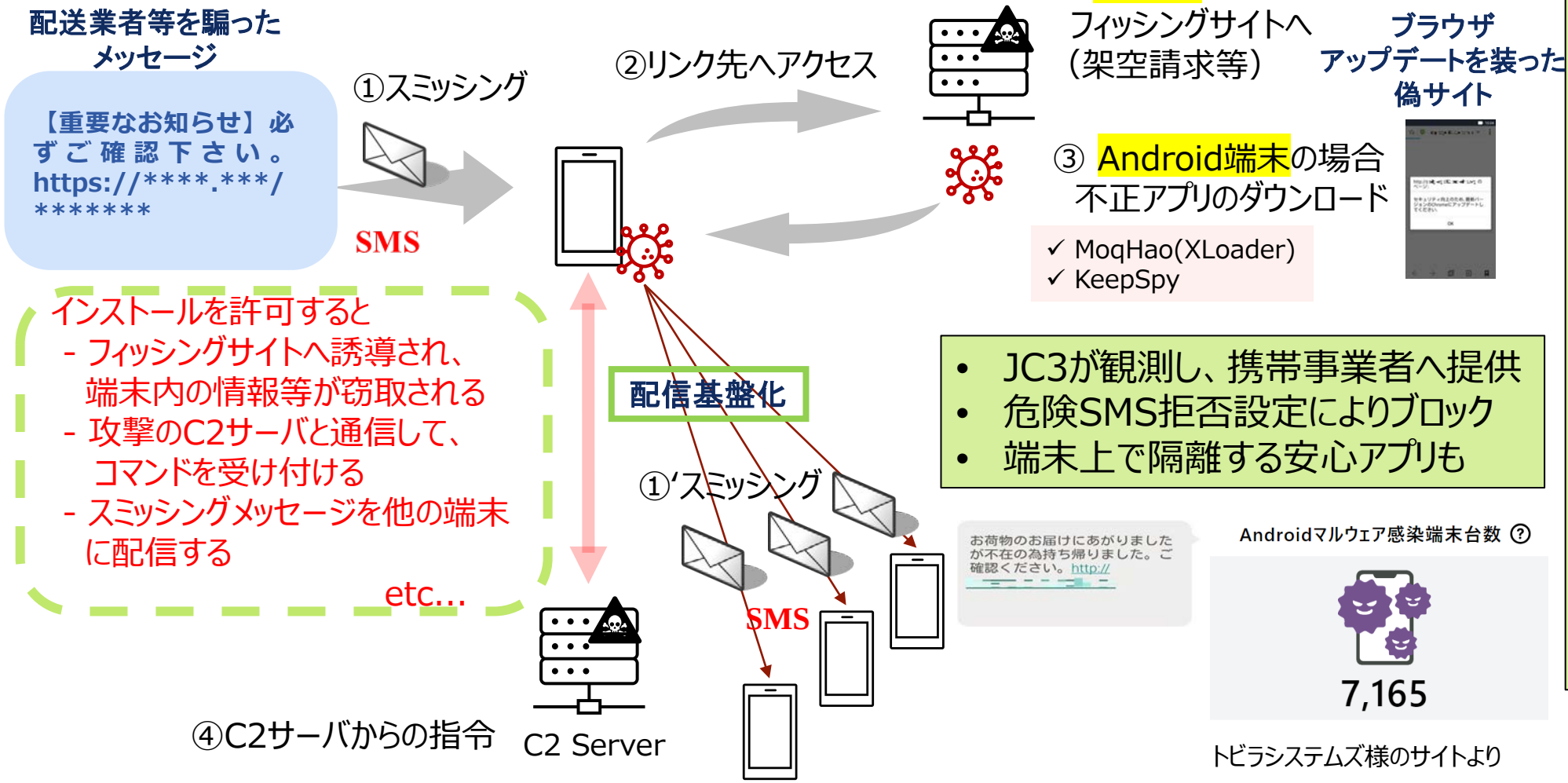
A銀行

B銀行

C銀行

SMSから始まるフィッシング被害（モバイルマルウェア）

スマートフォンを標的としたマルウェアの観測例



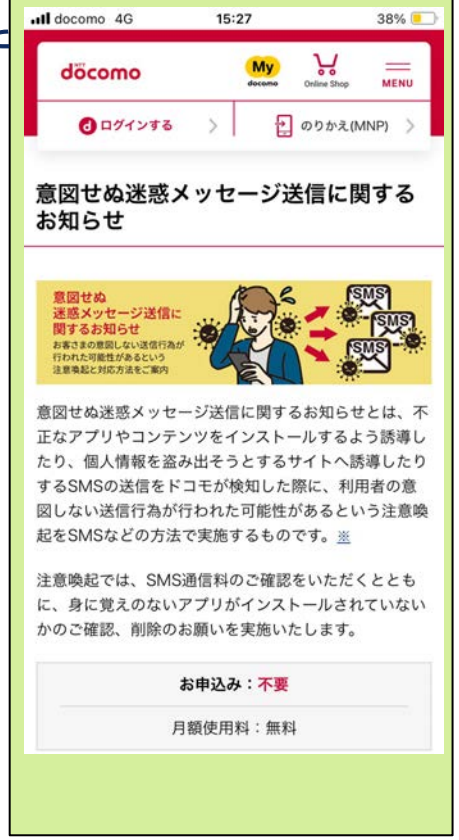
- JC3が観測し、携帯事業者へ提供
- 危険SMS拒否設定によりブロック
- 端末上で隔離する安心アプリも

Androidマルウェア感染端末台数 ?

7,165

トビラシステムズ様のサイトより

携帯電話会社から
新たな対策も



NTTドコモ様のサイトより

主要サイトの変化(KeepSpy) （2023年9月～11月）

「イオン銀行」お客様の口座を一時凍結しています、下記をご確認ください。
https://Cdk2Y[.]aosdwieieh[.]com

「イオン*銀行」お客様の口座を一時凍結しています。
https://aeonztn[.]github[.]io

9月4日

【重要なお知らせ】NTTドコモ未払い料金お支払いのお願い。
https://5wbe90q[.]duckdns[.]org

【イオン銀行】お客様の銀行口座の取引における重要な確認について。下記URLで検証お願いします。
https://aeondxa[.]com

9月29日

「三菱UFJ銀行」お知らせ、お客様の銀行口座の取引における重要な確認について。
https://mufgce[.]com

【重要】三菱UFJ銀行お知らせ、お客様の銀行取引を一時的に規制しています、利用再開手続きが必要です。
https://mufgya[.]com

10月22日

【au】お知らせをご覧いただき、ご確認ください。
https://t[.]co/GXfJDnzOX6

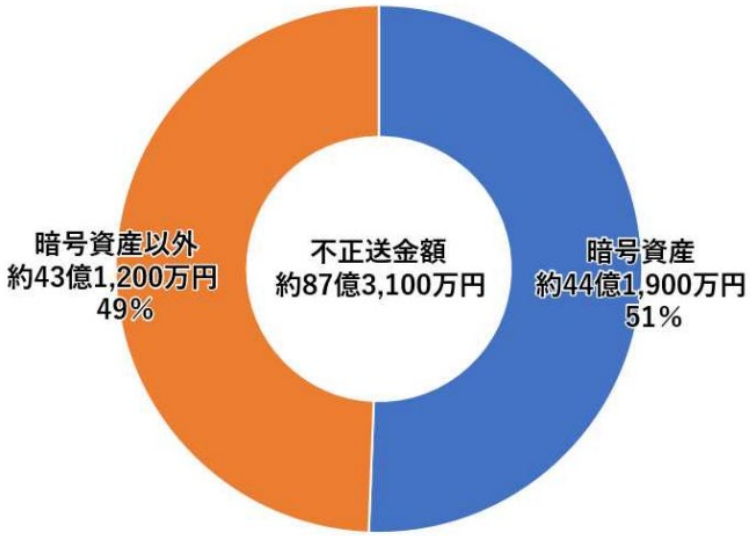
【SoftBank】お知らせをご覧いただき、ご確認ください。
https://t[.]co/YAkQM6zdm5

11月28

不正送金が「暗号資産」に流入している

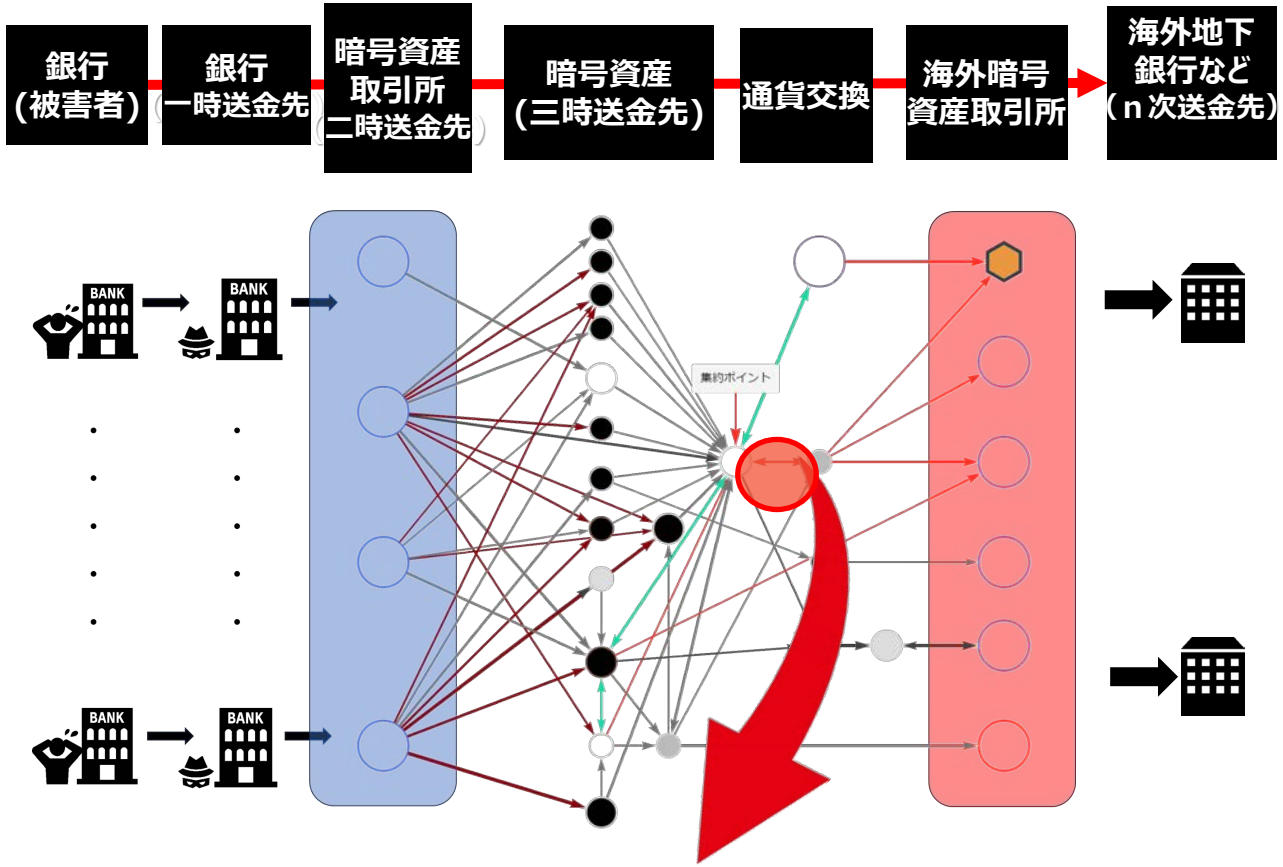
■ 暗号資産交換業者への送信金額が不正送金の半数を占める

【図表13：暗号資産交換業者の金融機関口座への送金状況】



■ 暗号資産における不正送金の流れ

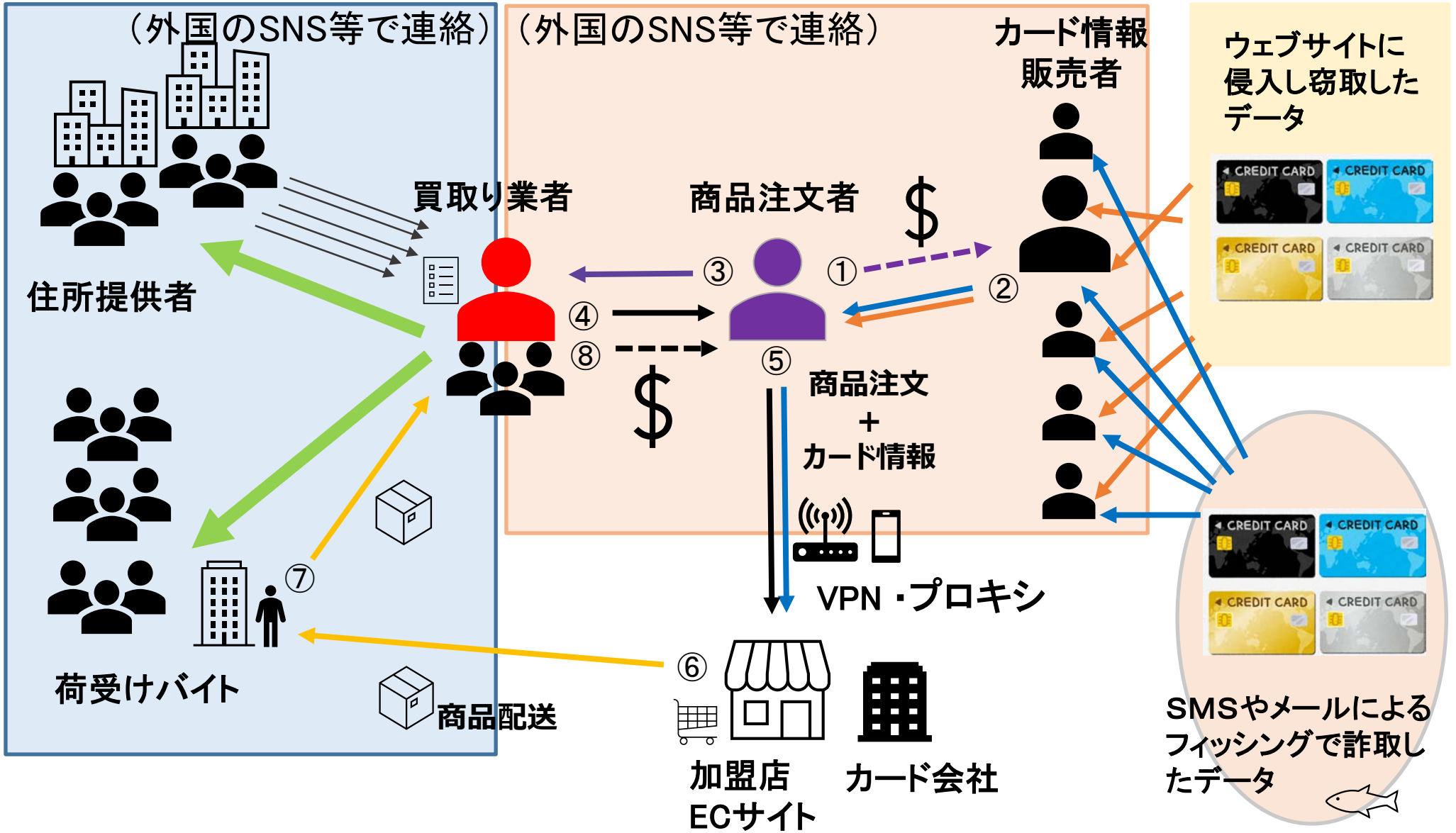
（流れがすべて記録に残っているのが特徴です）



※　提供データを元に研究した結果、集約される場所では、

十億円単位の暗号資産が動いていることが多い

クレジットカード情報を悪用した詐欺事案の背景（例）



悪質なフィッシング攻撃の概要（イメージ）と対策

手元で守るだけでなく、より前に出て抑止する活動を行うことが求められている！と認識

インテリジェンス収集

テイクダウンとブラウザブロック

攪乱へのチャレンジ？

不正の検知と予防
（金融機関、クレジット会社等）

意識啓発・注意喚起

犯罪インフラ対策
犯罪が起きにくい仕組みづくり

DISRUPTION24
By NCFTA

徹底した犯罪捜査と摘発 **＋国際的な働きかけ**
（警察、検察）

JC3 Japan Cybercrime Control Center

フィッシングサイト撲滅チャレンジカップを開催！

各県警のサイバー防犯ボランティアが、JC3の支援ツール「Predator」を活用して
Abuse報告数　と　テイクダウン数　を競い合う！

第2回チャレンジカップは、埼玉県警との共催で7月22日から29日に開催予定
今回から1グループ3人で実施、
申し込みは各都道府県警察を通じて行っています。締め切りは7月19日（金）15:00まで

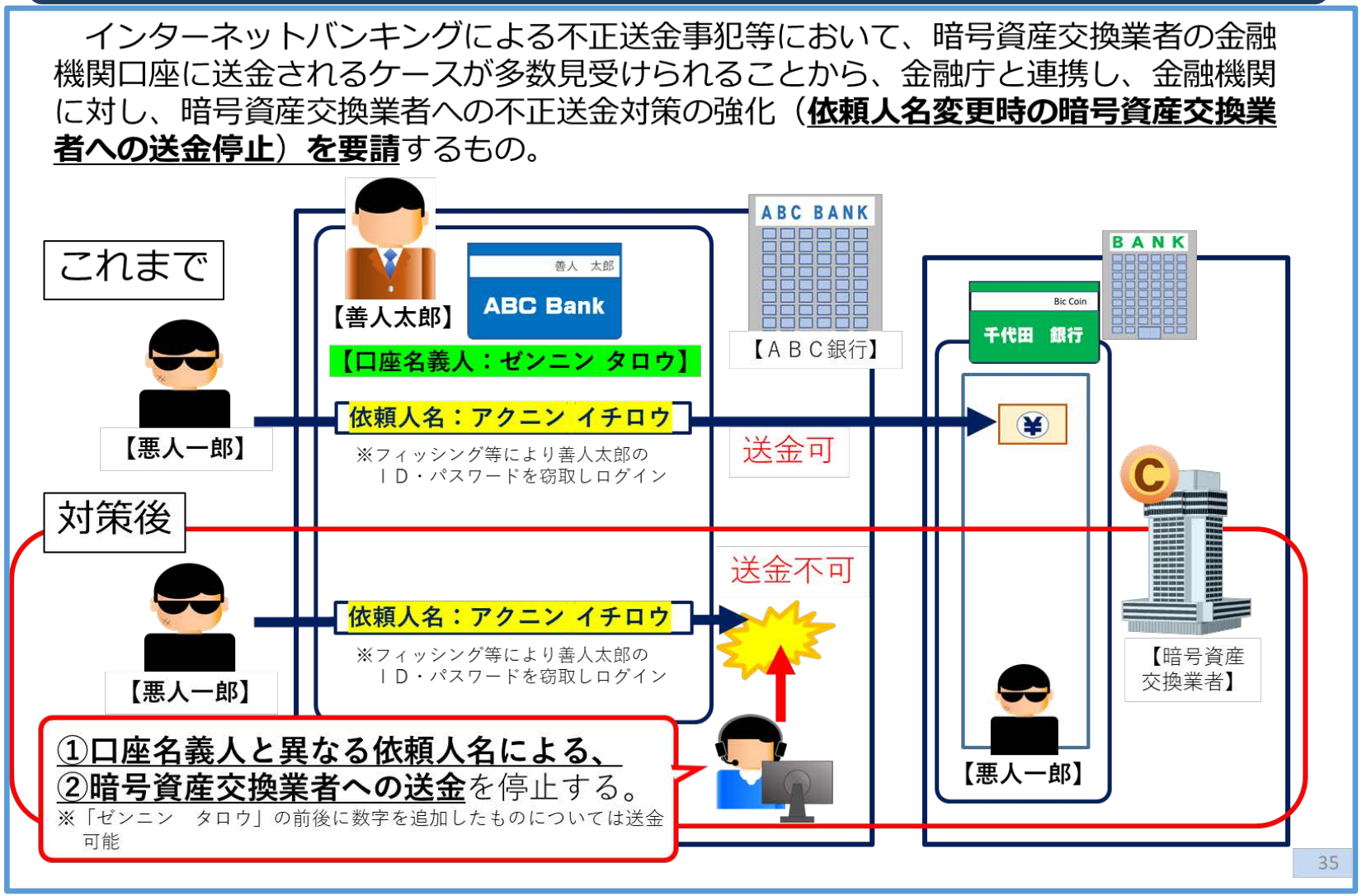
＜第1回　結果概要＞令和4年2月13日18:00～20日18:00

- 参加ボランティア団体　27団体（参加者125名）
  特別参加団体：Gftd Japan株式会社様
- ドメイン事業者　Abuse報告数・・・5,464件
  テイクダウン数・・・ 264件
- ホスティング事業者　Abuse報告数・・・3,855件
  テイクダウン数・・・4件
- 合計　Abuse数・・9,319件
  テイクダウン数 ・・268件
- Google Safe Browsing　報告数　・・・2,870件

暗号資産交換業者への不正送金対策の強化（警察庁）への協力

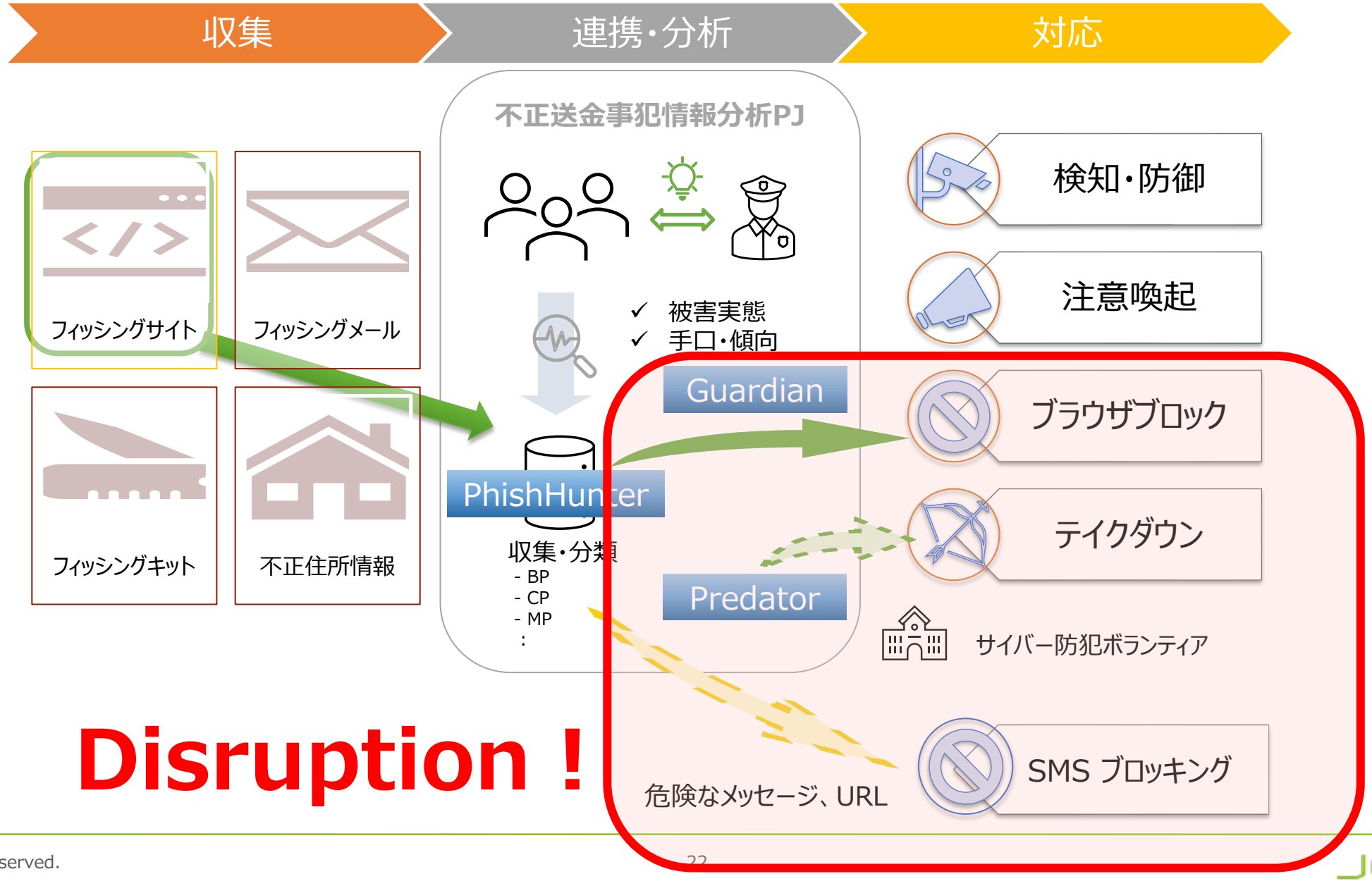
警察庁、金融庁から各金融機関への要請（2024年2月）

インターネットバンキングによる不正送金事犯等において、暗号資産交換業者の金融機関口座に送金されるケースが多数見受けられることから、金融庁と連携し、金融機関に対し、暗号資産交換業者への不正送金対策の強化（**依頼人名変更時の暗号資産交換業者への送金停止）を要請**するもの。



JC3と会員金融機関が協力してその実現を支援

JC3のフィッシング対策への取組み

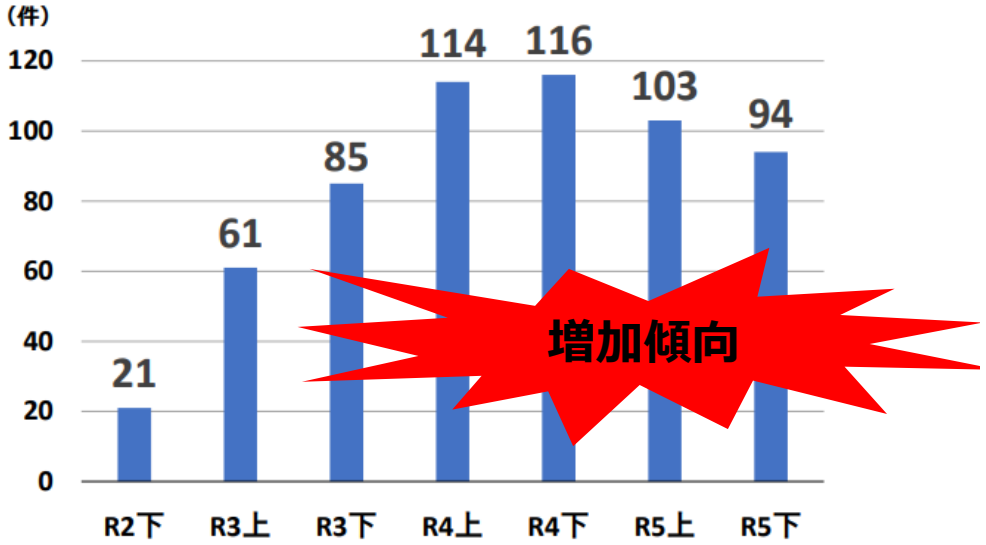


ランサムウェア攻撃の特徴①　報告件数の推移、規模や業種

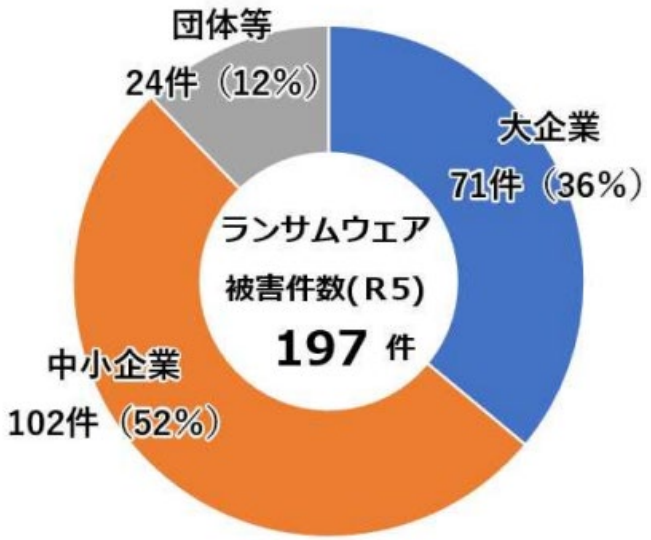
警察庁「令和５年におけるサイバー空間をめぐる脅威の情勢等について」 及び　警察庁実施のアンケート等より

- 情報セキュリティ10大脅威（IPA）では2021年以降連続して1位（組織）
- 企業・団体等におけるランサムウア被害の増加傾向は変わらず
- 二重恐喝（暗号化と流出）が多く、対価は暗号資産を求められる　暗号化をしないノーウェアランサムも
- 企業の規模、業種を問わず被害が発生
- 海外の日本関係企業における被害が約27%（JC3調べ）
- リークサイトに掲載された企業のうち、約50%は被害を公表（JC3調べ）

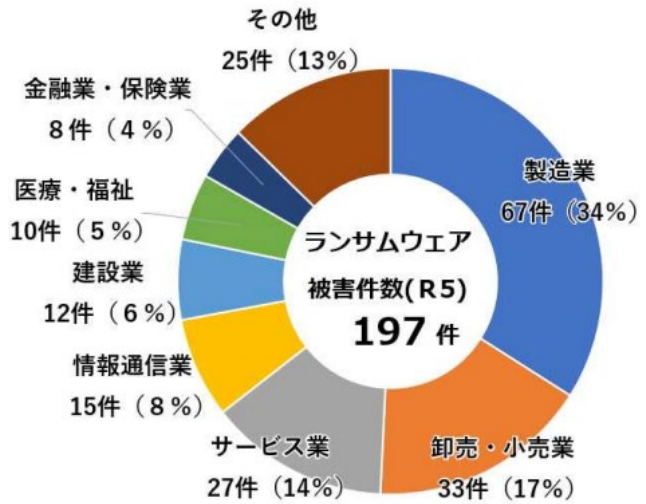
報告件数の推移



業種規模別



業種別

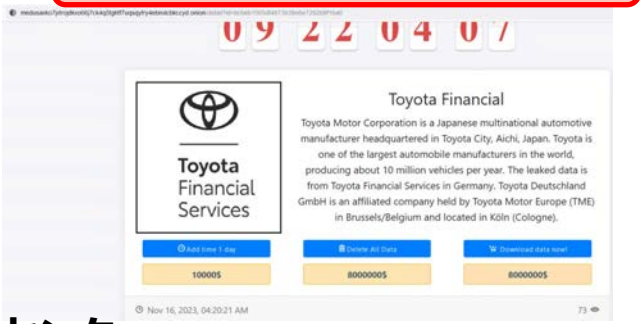


注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

リークサイトや公表情報からみるランサムウェア被害

自社だけではなく、**国民全体**に大きく影響を与える問題

リークサイトより



＜近年の被害報告例＞

- **（2020年）ソフトウエア開発会社、自動車メーカー、医療機関、大手食品メーカー**
- **（2021年）医療機器メーカー、部品製造業、大手ゼネコン、つるぎ町立半田病院**
- **（2022年）車両部品メーカー、食品メーカー、国立大学法人、大阪急性期・総合総合センター**
- **（2023年）名古屋港コンテナターミナル、精密機械メーカー、大手製薬会社**
- **（2024年）大手スーパーチェーン、医療法人、電力機器会社、化学メーカー、情報処理会社、準大手税理士法人、大手出版会社、大手化学品メーカーの海外法人**

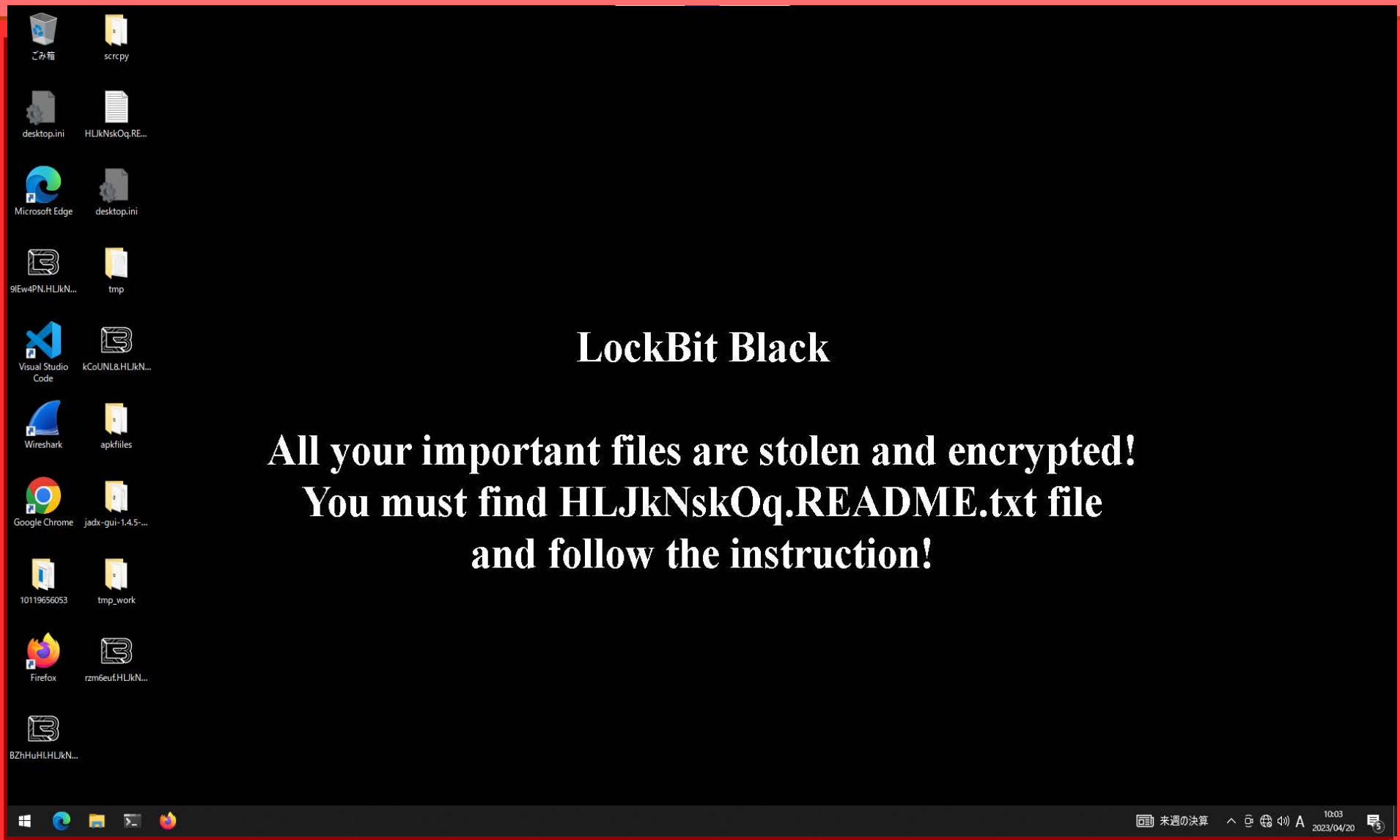
＜つるぎ町立半田病院の例＞

2021年に地方の医療機関が感染。感染経路として、リモートメンテナンス用のVPN機器の脆弱性が悪用された。大規模な感染被害により、電子カルテを始めとした医療データの閲覧が不能となったが、病院スタッフの努力により、医療サービスの提供を継続。 詳細な検証レポートが発表され、海外のメディアによりドキュメンタリも作成される。

調査報告書：https://www.handa-hospital.jp/topics/2022/0616/index.html

ドキュメンタリ： https://www.youtube.com/watch?v=XaVkzX7NjmA

LockBit３.0に感染した場合の画面



Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqyqqxyvjpqkmeyy4l3azl3qv6pyd.onion.ly

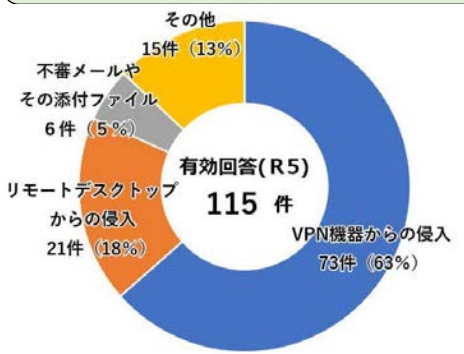
ランサムウェア攻撃に対する国際共同捜査

警察庁は、本年2月、ユーロポールが、ランサムウェア攻撃グループLockBitの一員とみられる被疑者の検挙及び関連犯罪インフラをテイクダウンしたことをプレスリリース。日本警察も捜査で得られた情報を提供するなどの協力を行ったもの。

今後の更なる国際共同捜査や被害回復ツールの開発に期待が高まります！

ランサムウェア攻撃の特徴②　感染経路、検知状況

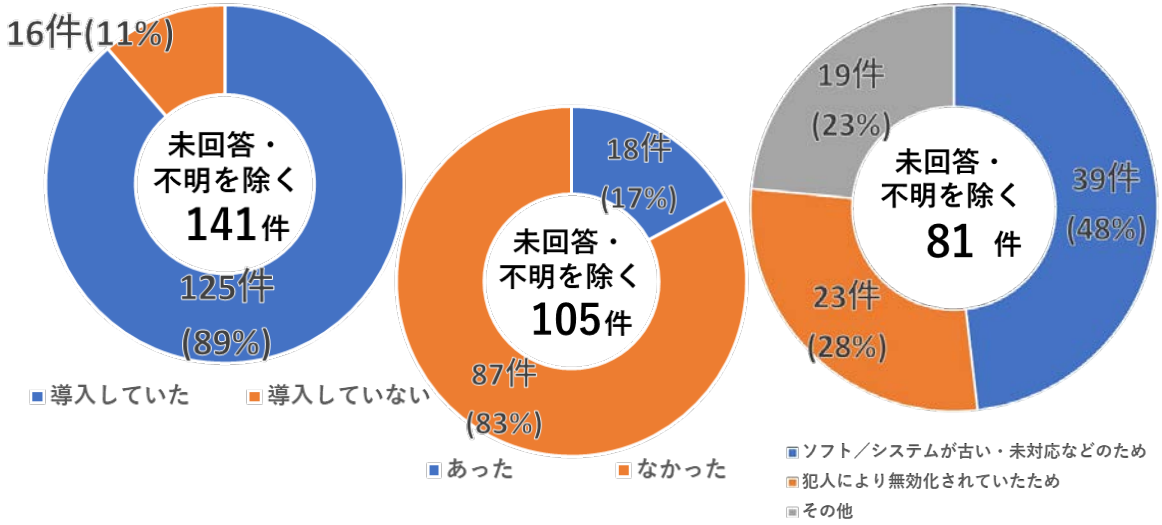
感染経路別の報告件数



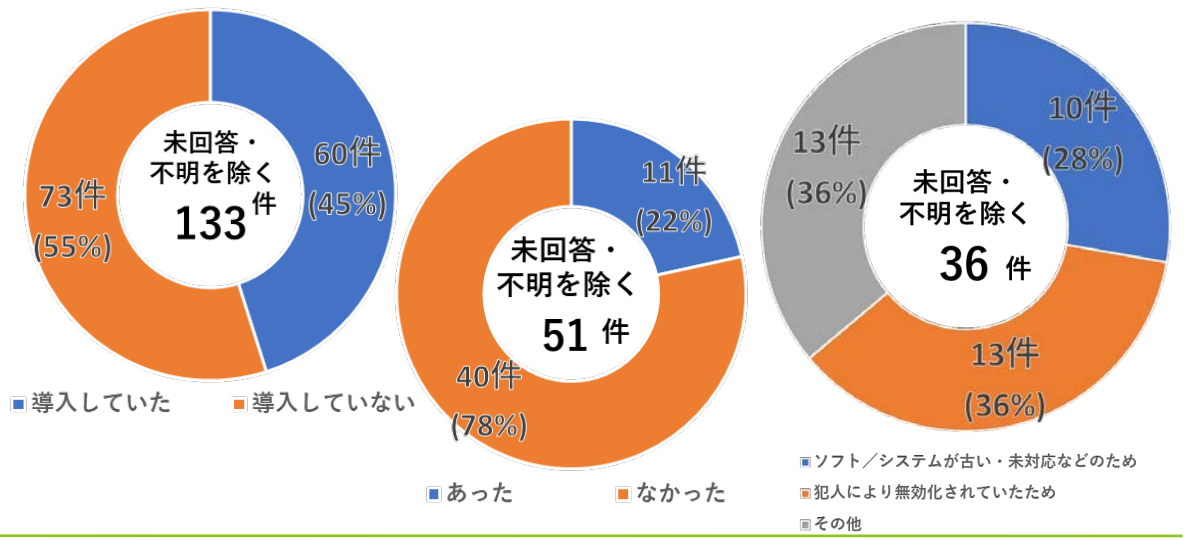
注　図中の割合は小数第1位以下を四捨五入しているため、総計が必ずしも100%にならない。

- ■ ＶＰＮ機器やリモートデスクトップを利用した感染を多数確認
- ■ 殆どの被害企業がウイルス対策ソフトを導入していたが、検出がないケースが多数（半数が原因は運用上の問題と指摘）
- ■ 不正な侵入の兆候を検出する製品（EDR等）については被害企業の約５割が導入していない　（約4割が犯人により無効化されていたことを原因と指摘）

ウイルス対策ソフト導入・検出状況と検出がなかった要因



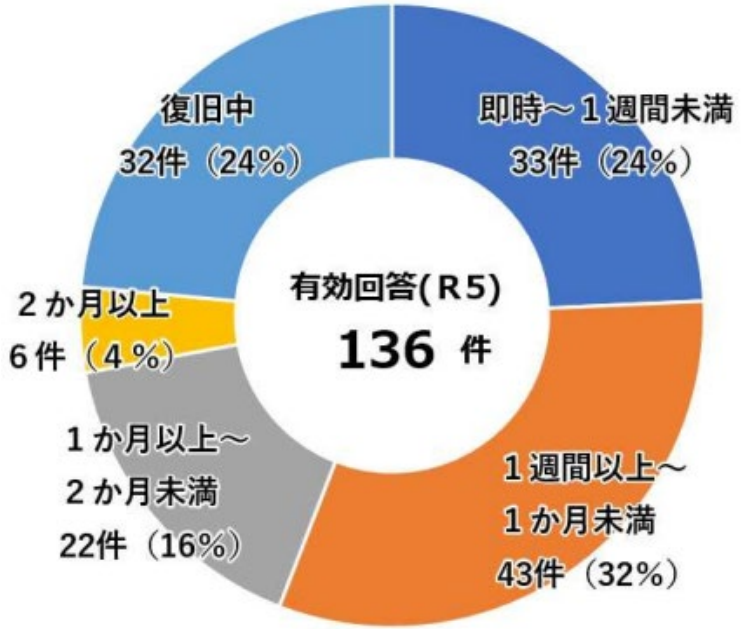
EDR等の導入・検出状況と検出がなかった要因



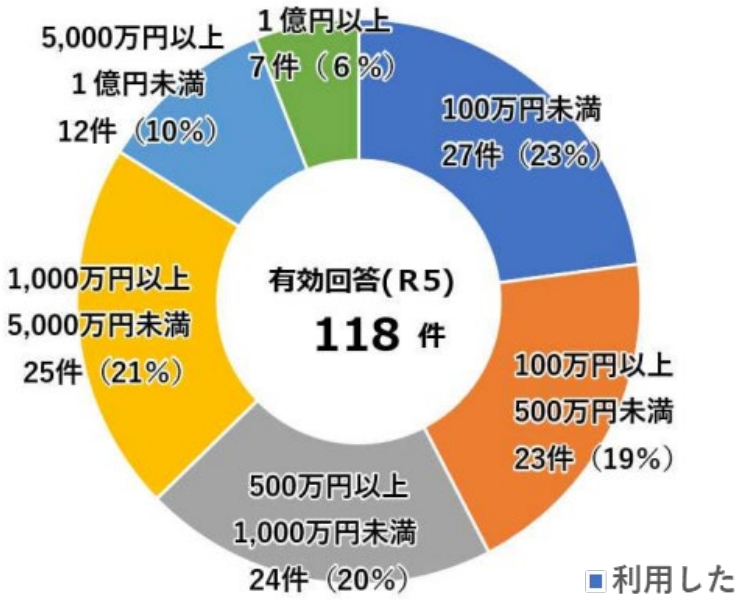
ランサムウェア攻撃の特徴③　復旧に要する期間・費用、サイバー保険

- 復旧中の企業を含め、被害企業の76%が被害復旧に１週間以上を要している
- 調査・復旧費用から見ても被害は甚大
- サイバー保険加入率は全体の30%と外部の調査結果（26.3%）を上回っているものの、加入しながらサイバー保険を利用しなかった企業も存在

復旧に要した期間

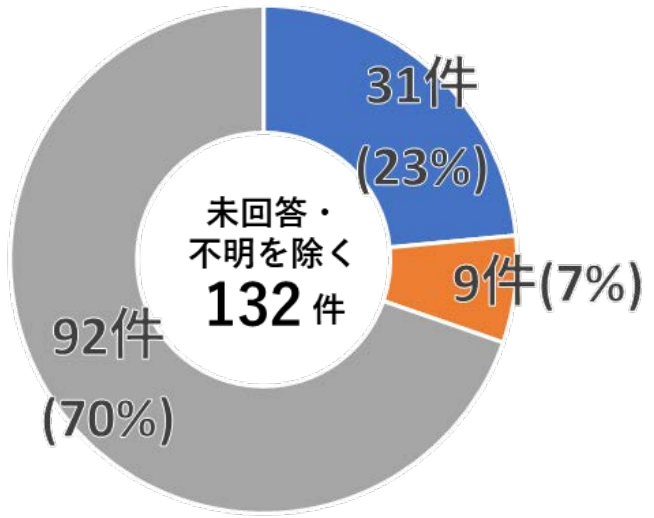


調査・復旧費用



注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

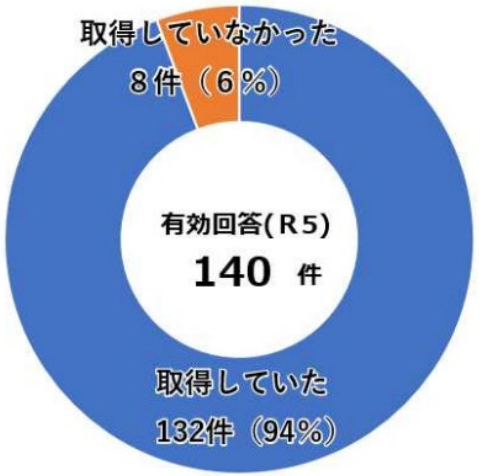
サイバー保険の利用状況



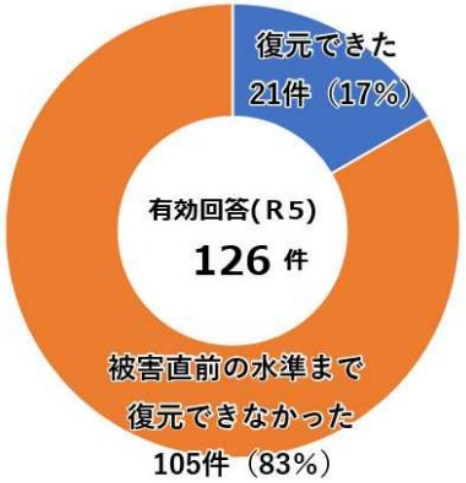
ランサムウェア攻撃の特徴④　バックアップの状況と復元できなかった理由

- バックアップは約９割の企業が取得していたが、完全に復元できたのは２割程度
- バックアップから復元できなかった理由の、69%が「攻撃者に暗号化されたため」、16%が「運用面の課題（データが古い・欠損、保存状態、誤削除）」によるもの
- 暗号化されたバックアップの70%は、社内ネットワークに常時接続されていた

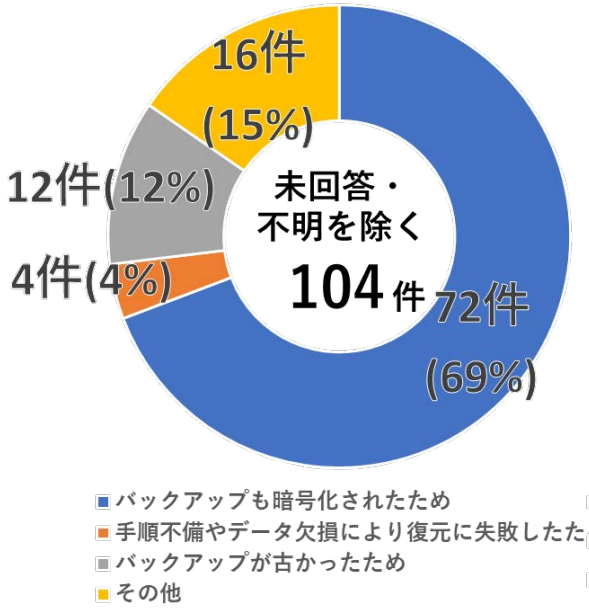
バックアップの取得の有無



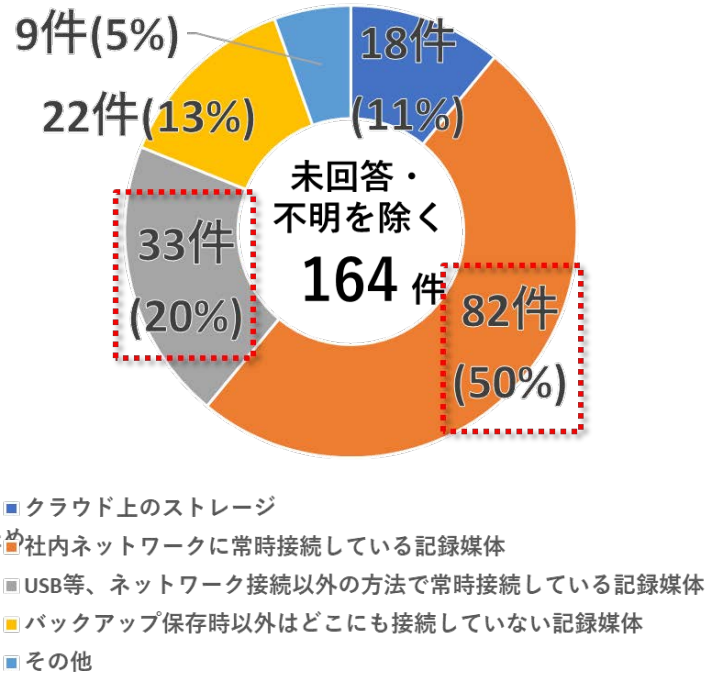
バックアップを取得していた企業の復元状況



バックアップから復元できなかった理由



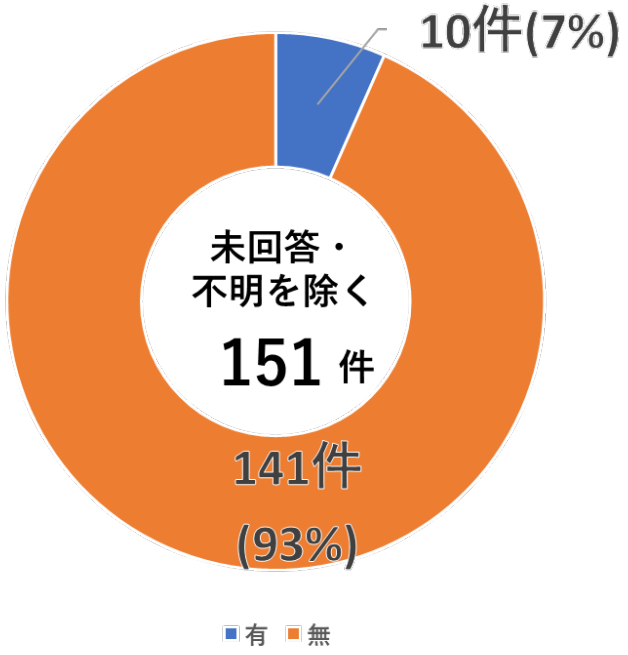
暗号化されたバックアップの保管場所



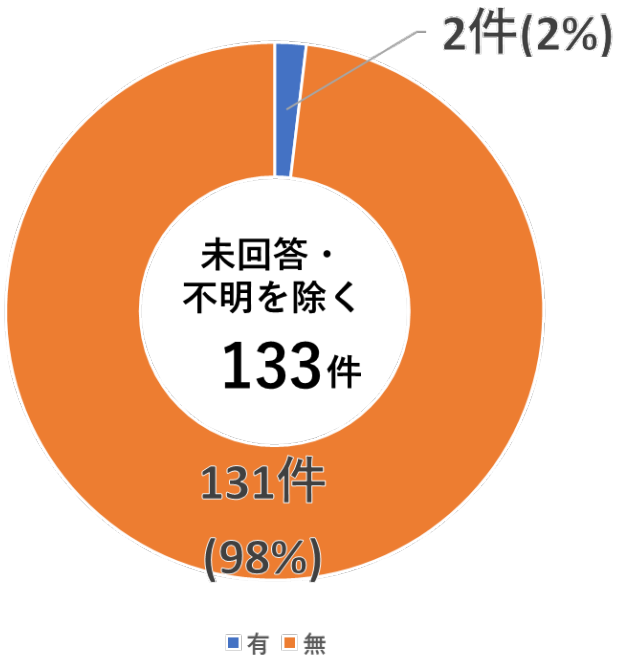
ランサムウェア攻撃の特徴⑤　犯人との交渉状況と金銭支払い状況

- 犯人との交渉を行った事例は10件に留まり、身代金を支払った被害企業は２社
- 1,000万円以上の高額な身代金要求は全体の47%であり、いずれも二重恐喝型のランサムウェアによるもの

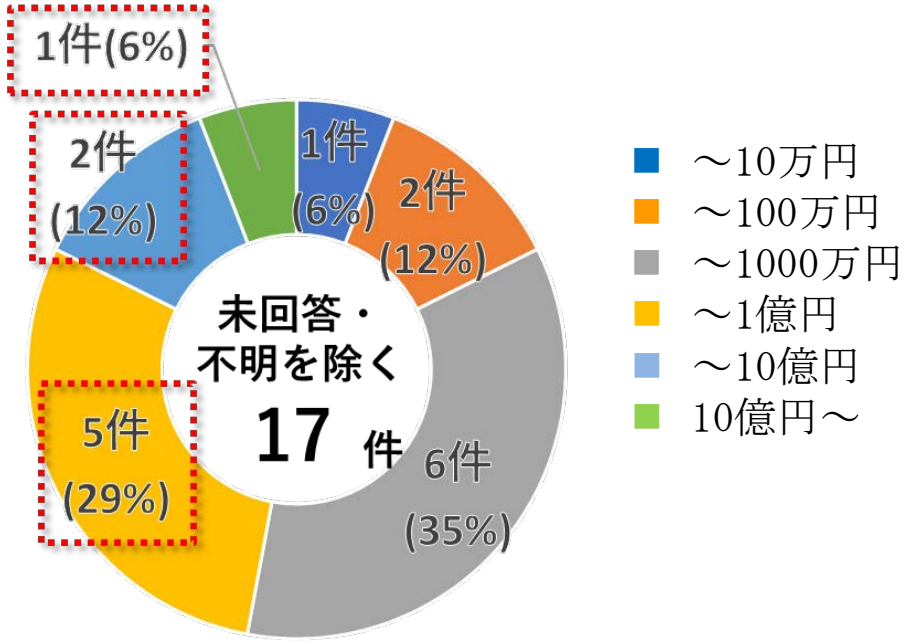
犯人との交渉状況



金銭支払いの有無



身代金要求金額（円換算）

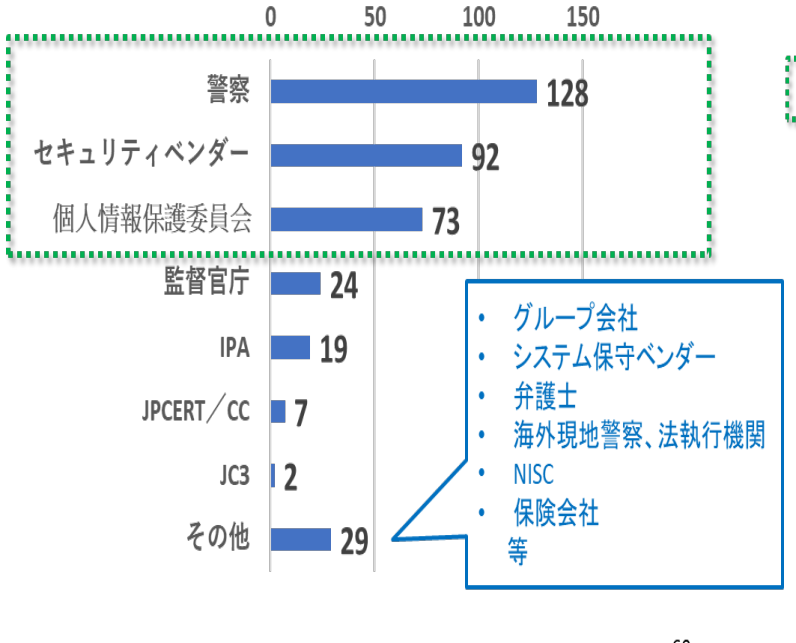


※2024/3/29時点の概算レートで換算（1$=151円，1BTC=1,050万円）

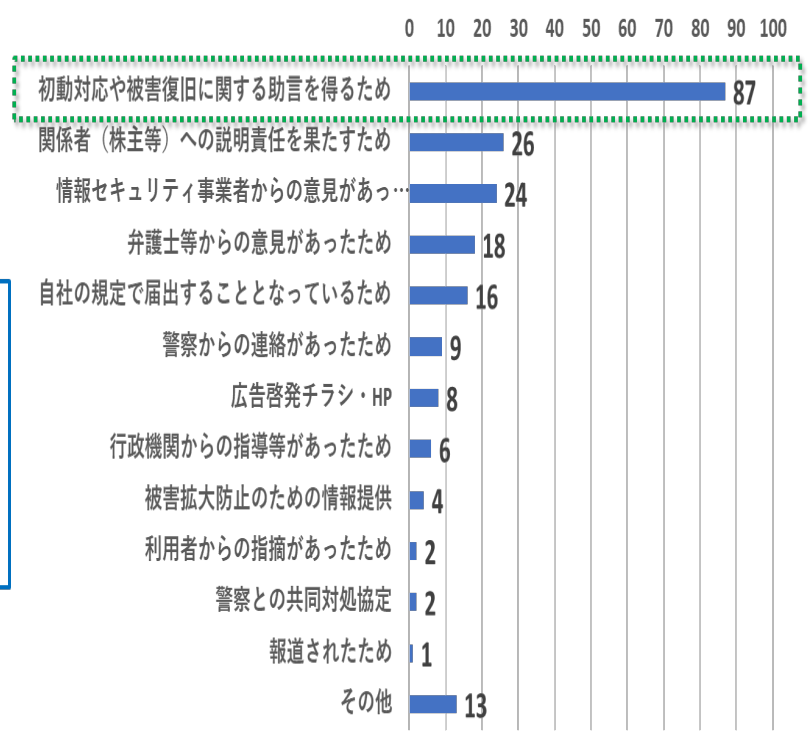
ランサムウェア攻撃の特徴⑥　警察等への通報について

- 警察への通報に加えて行われたのは、セキュリティベンダーや個人情報保護委員会への通報
- 警察に通報する理由は、「初動対応や被害復旧に関する助言を得るため」
- 警察に通報する上で企業が考える課題も多い（通報窓口、通報内容、時間がかかる、解決しない等）

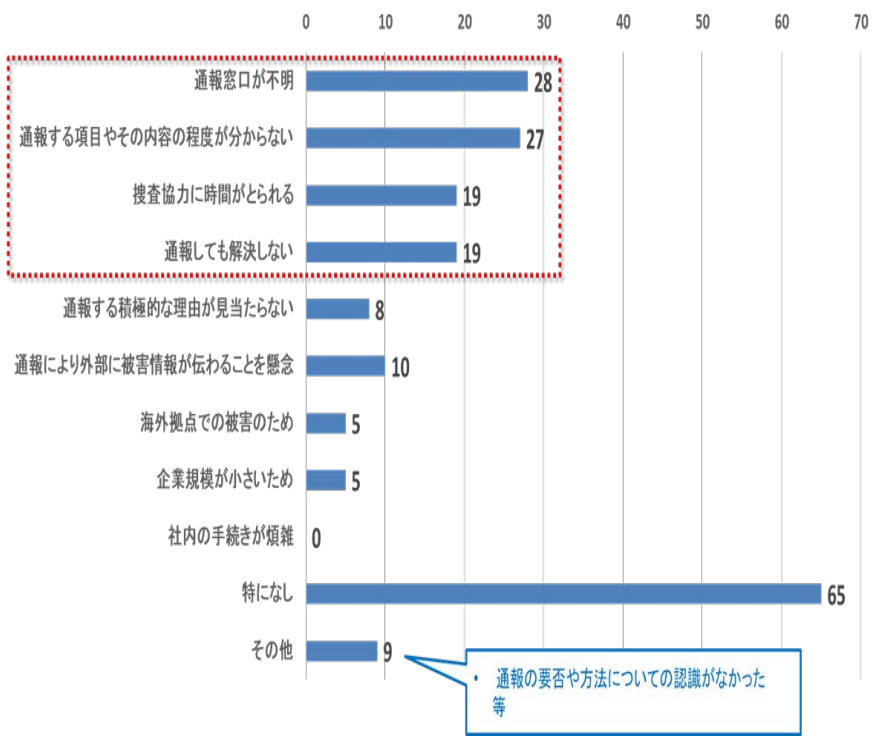
通報先



警察に通報した理由



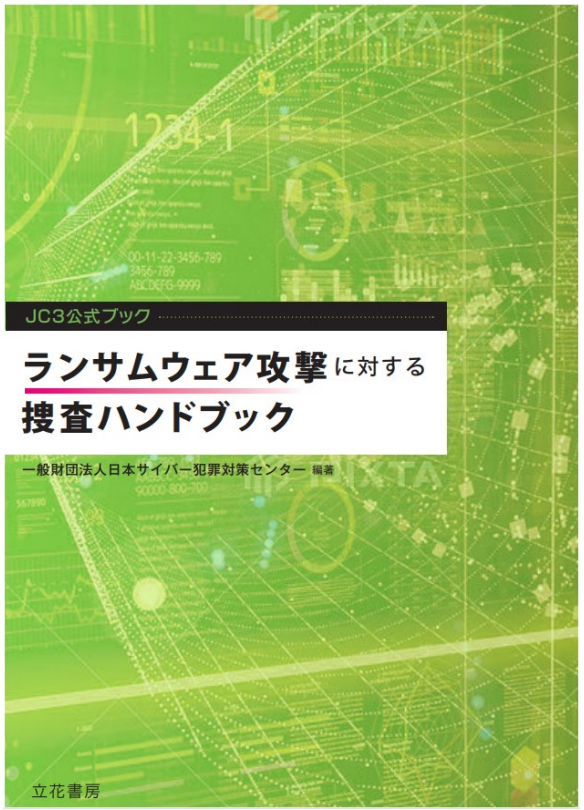
警察への通報を検討する上で企業が考える課題



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

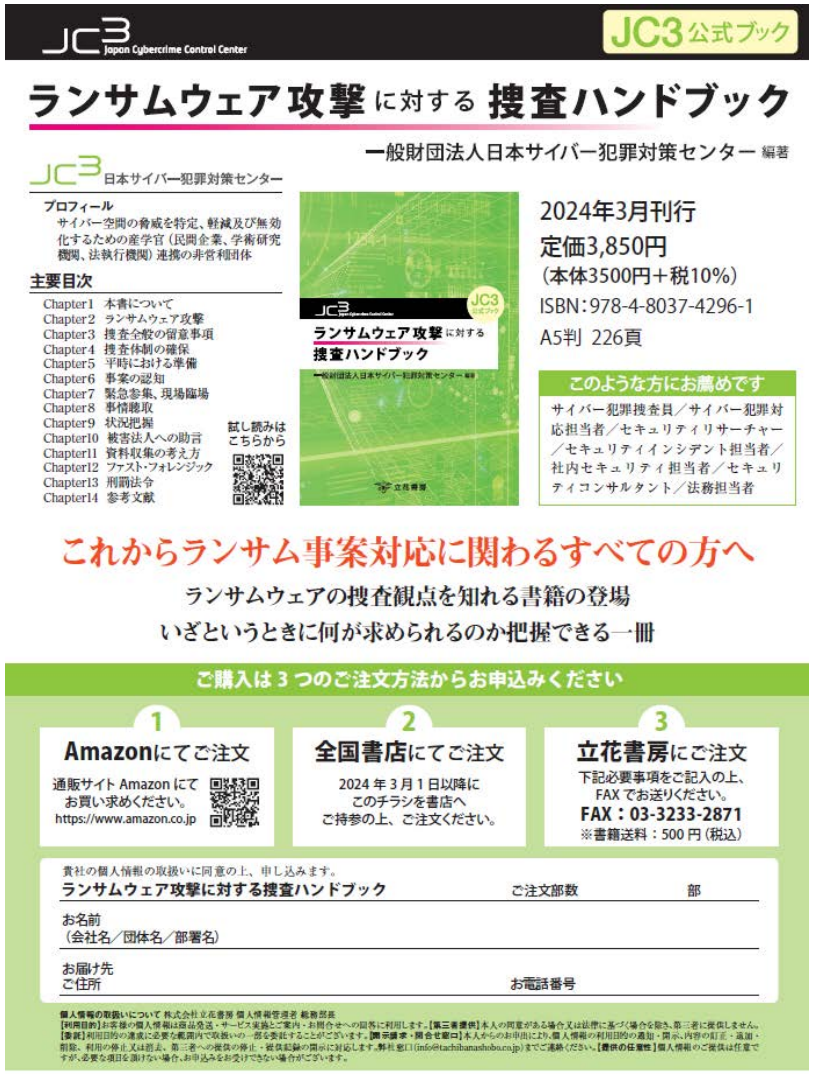
書籍内容（大項目のみ）

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）



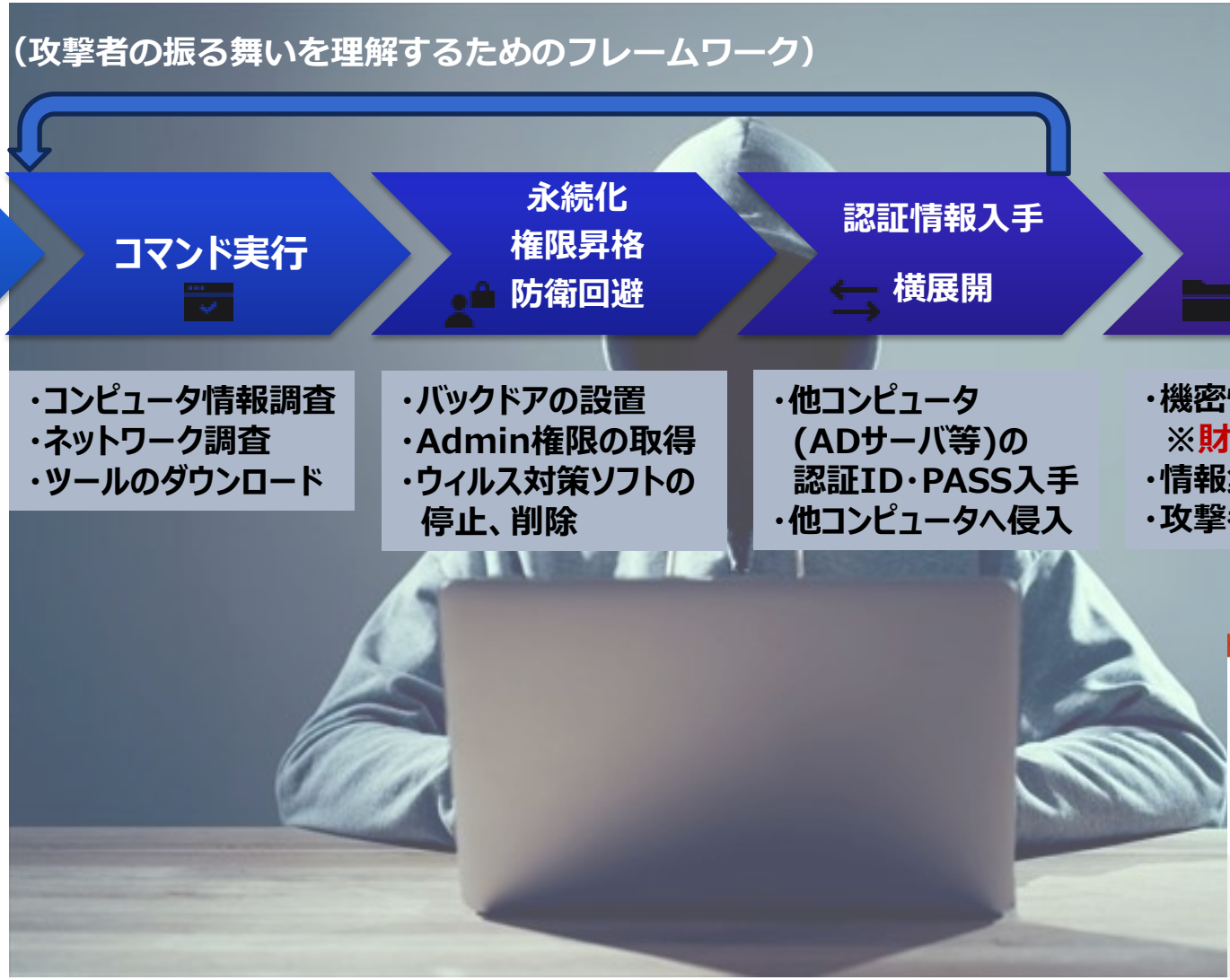
警察による

犯人検挙に向けた **証拠保全**



ランサムウェア攻撃の手法

MITRE ATT&CK（攻撃者の振る舞いを理解するためのフレームワーク）



初期アクセス	コマンド実行	永続化 権限昇格 防衛回避	認証情報入手 横展開	データ収集 データ窃取	暗号化 情報公開 脅迫
・脆弱性攻撃 ・不正入手アカウント ・ブルートフォース攻撃 ・フィッシングメール ・水飲み場攻撃	・コンピュータ情報調査 ・ネットワーク調査 ・ツールのダウンロード	・バックドアの設置 ・Admin権限の取得 ・ウィルス対策ソフトの停止、削除	・他コンピュータ(ADサーバ等)の認証ID・PASS入手 ・他コンピュータへ侵入	・機密情報の探索 ※財務情報等 ・情報集約 ・攻撃者サーバへ送信	・ランサムウェア実行 ・ランサムノート蔵置 ・リークサイトで公開 ・バックアップデータの破壊

出典：MITTER ATT&CK https://attack.mitre.org/

ランサムウェア攻撃の手法（イメージ）

① 初期アクセス

外部サーバ
※被疑者側管理

② 悪意あるコードの実行
※マルウェアやランサム攻撃で悪用されるツールの取得

⑧ データの収集・持ち出し

リークサイト

⑩ 取得情報の公開

⑧ データの収集・持ち出し

外部サーバ
※被疑者側管理

ゲートウェイ
（FW・VPN装置）

被害法人内ネットワーク

⑧ データの収集・持ち出し

⑦ 横展開

⑨ ランサムウェアの展開

本来端末Aに接続権限がないネットワーク

⑥ 認証情報へのアクセス
⑦ 横展開

⑨ ランサムウェアの展開

Active Directory
サーバ

③ 永続化
④ 権限の昇格
⑤ 防御の回避

⑨ ランサムウェアの展開

感染起点
（端末A）

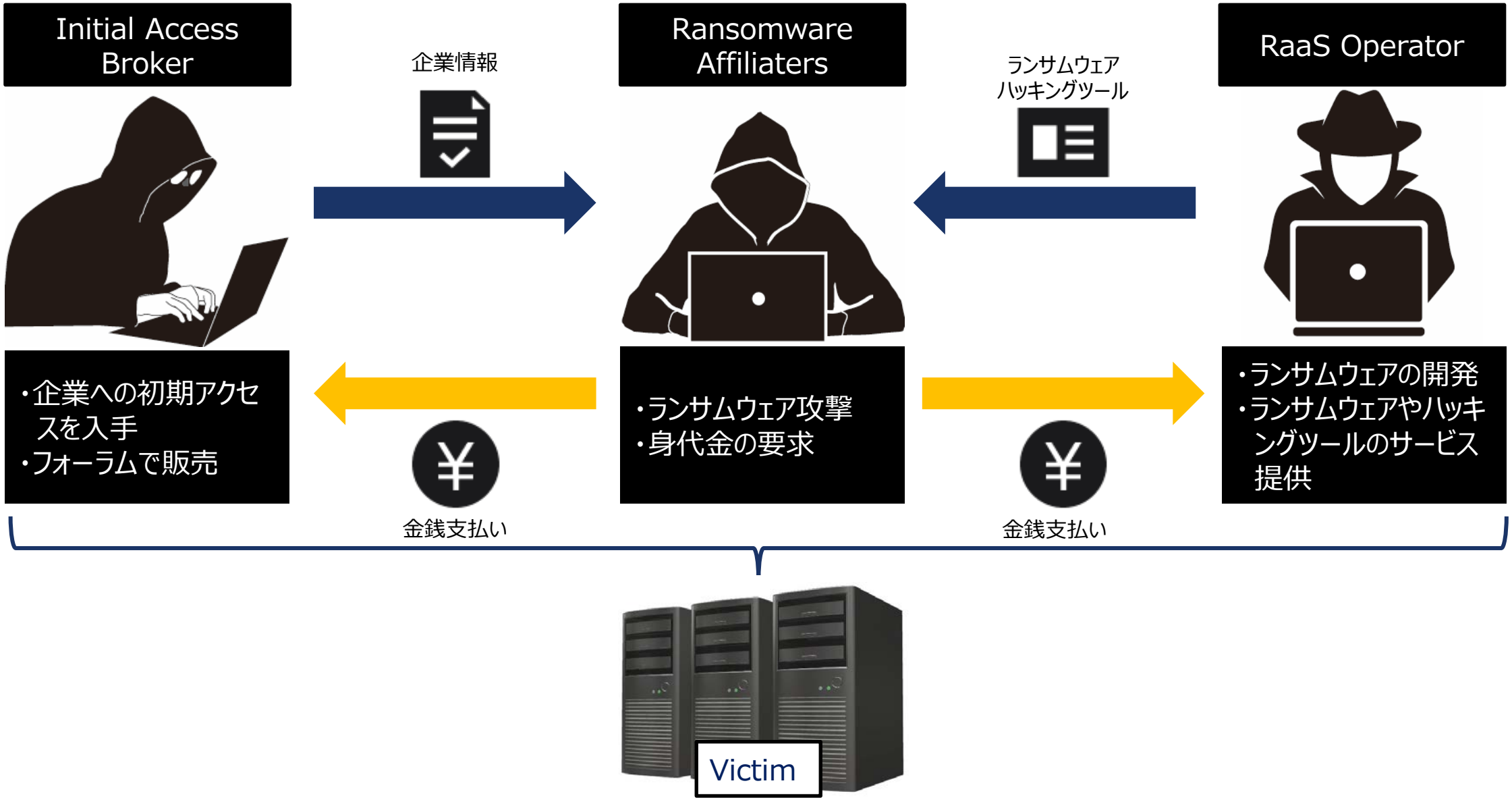
凡例

侵入・感染の流れ

データ窃取の流れ

JC3 Japan Cybercrime Control Center

ランサムウェア攻撃グループ



ランサムウェア攻撃に対する捜査（事情聴取・状況把握）

■ 主な聴取対象及び要請内容

No	関係者	要請内容
1	責任者 ランサムウェア攻撃対応の責任者 警察対応窓口	■ 被害届／被害調書の作成
2	第一発見者	■ 発見時の状況を聴取
3	情報システム担当者 警察対応窓口	■ 参考人調書の作成 ■ **ネットワーク構成図、各種設計書の提供**又は所在場所の聴取
4	業務システム業者 端末システム開発／保守運用業者	■ 業務システムの被害状況の確認
5	端末業者 端末導入／保守運用業者	■ 端末からのメモリダンプ、ディスクイメージ、端末情報等の取得協力
6	ネットワーク業者 ネットワーク機器導入／保守運用業者	■ VPN機器等のネットワーク機器のログを取得協力
7	セキュリティ業者 ランサムウェア攻撃の調査依頼をした業者	■ 収集物・報告書の提供 ※被害企業様経由で依頼

ランサムウェア攻撃に対する捜査（事案の認知）

■ 事案認知時に被害企業様へ要請する主な内容

No	要請内容	目的
1	LANケーブルを抜く、無線LANを無効にする	感染拡大防止
2	端末の再起動や電源オフをしない （端末が起動中の場合）	証拠保全
3	端末の電源をオンにしない （端末が起動していない場合）	証拠保全
4	端末をウイルス対策ソフトによりフルスキャンしない	証拠保全
5	ネットワーク機器の再起動や電源オフをしない （**再起動や電源オフによりログ消失するものが多い**）	証拠保全
6	ファームウェアやOSのアップデートをしない	証拠保全

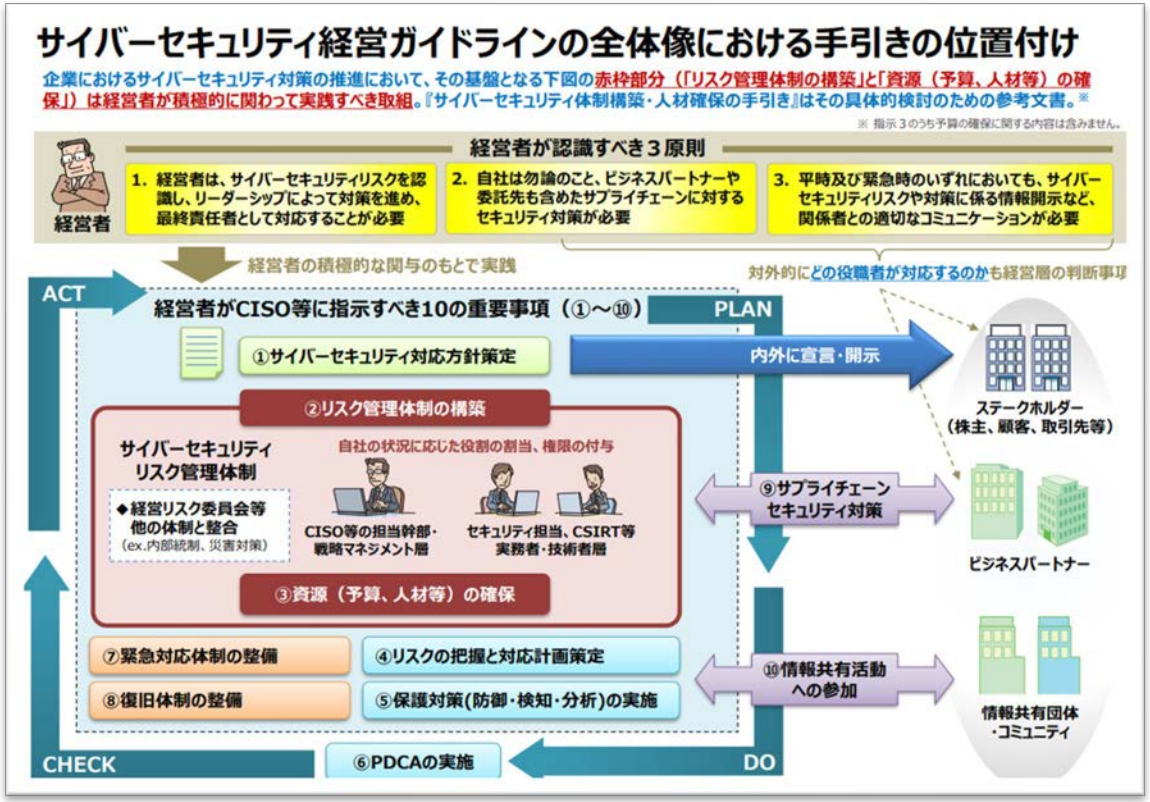
※「２～６」の作業は復旧（事業継続）に向けて、対応する必要がある内容である。
そのため、**事案発生の早期段階**で法執行機関との連携を検討頂きたい

→インシデント対応マニュアル等への反映

企業様へのお願い①

サイバーセキュリティ経営ガイドライン

（2023/03/24 更新）経済産業省
https://www.meti.go.jp/policy/netsecurity/mng_guide.html



被害企業の64%がサプライチェーンからの感染と回答

企業様へのお願い②

身代金支払いに関する注意点

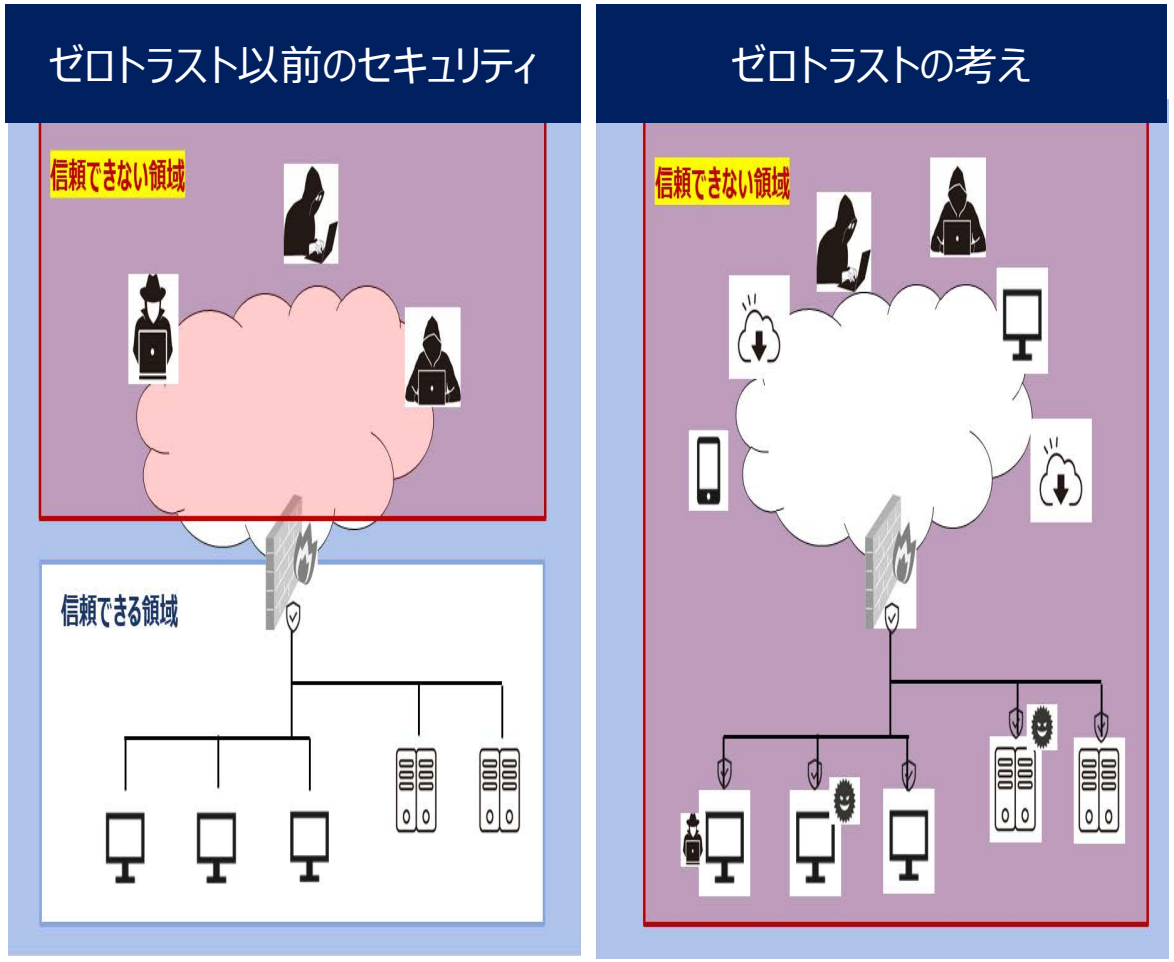
1．身代金を支払っても暗号化ファイルを復号できる保証はないこと
※　ランサムウェアの暗号化処理、復号ツールにバグがあり、ファイルを復号できない場合がある。
そもそも復号ツールが提供されない場合もある。
2．身代金が犯罪組織の資金源となり、犯罪の拡大に手を貸すことになること
3．盗まれた情報がリーク（公開）されない保証はないこと
4．さらなる金銭を要求される可能性が高まること
5．将来、再度のランサムウェア攻撃対象になる可能性が高まること
6．別のランサムウェアグループに狙われる可能性が高まること
7．ランサムウェアが有効であることを攻撃者に証明することになること
8．身代金を支払うことで社会的評判が失墜する可能性があること
9．サイバー保険に入っていても、身代金は補償対象外の場合がほとんどであること

経済産業省のガイドラインでも、「金銭の支払いは厳に慎むべきもの」と注意喚起

https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf

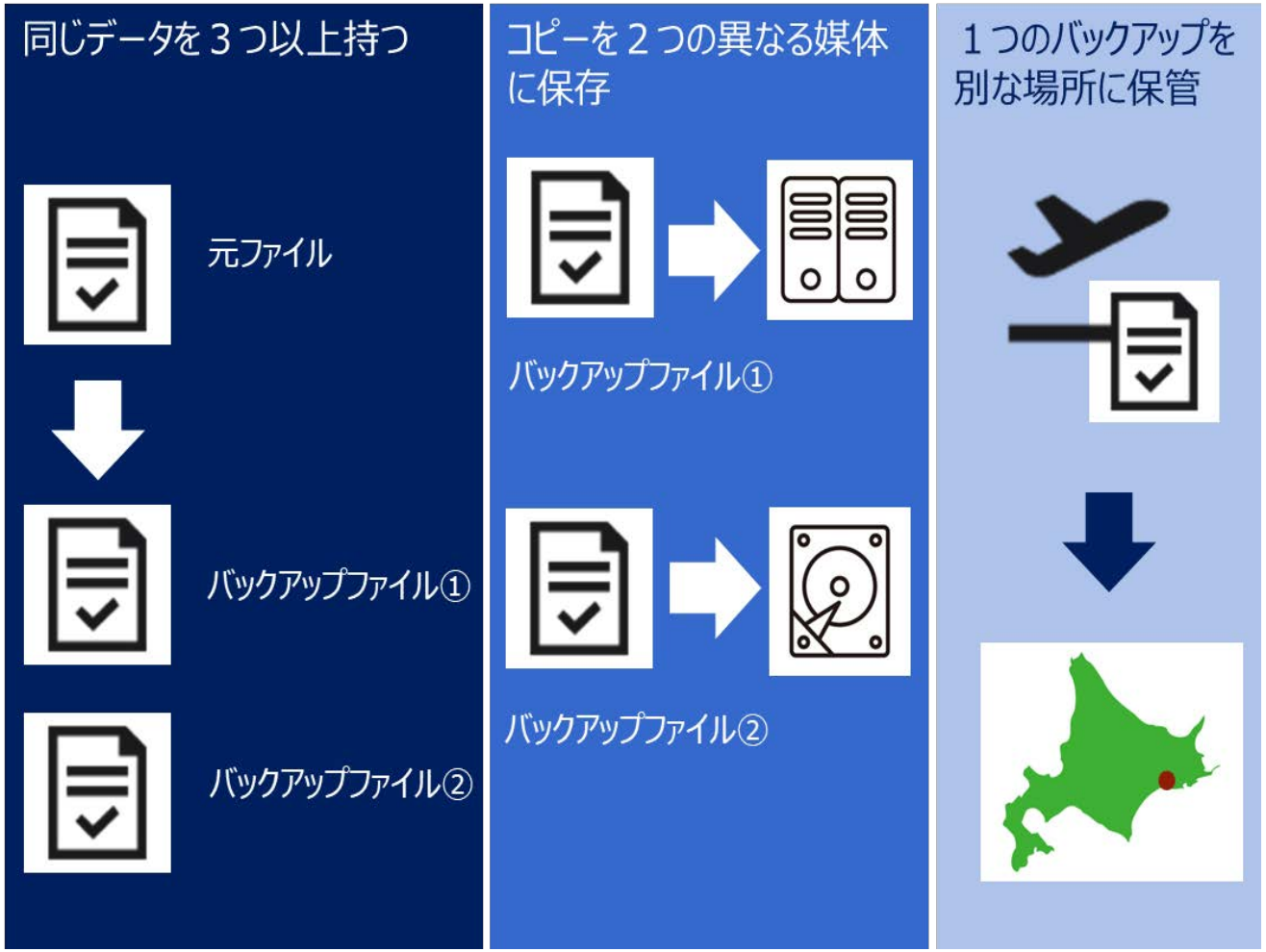
企業様へのお願い③

ゼロトラスト



企業様へのお願い④

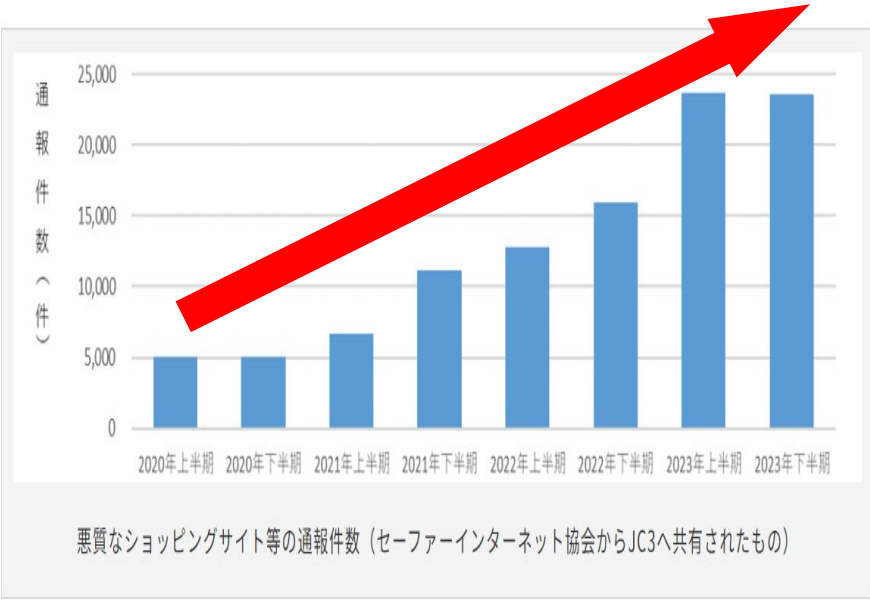
バックアップの重要性（３－２－１ルール）



※３－２－１－１－０ルール：上記に「１つはオフライン保管かクラウド上の保管の場合はデータが不変であること」、「バックアップデータはエラーゼロで完了すること」が加えられたもの

偽ショッピングサイトでもクレジット情報が盗まれている！

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）



悪質なショッピングサイト等の通報件数（セーファーインターネット協会からJC3へ共有されたもの）

偽ショッピングサイトに関する取組み

収集 → 連携・分析 → 対応

偽ショッピングサイト

改ざんサイト

SIA通報

共同研究

情報セキュリティ大学院大学

悪質サイト対策PJ

収集・判定・分類
- FS

システム

偽ショッピングリスト情報提供

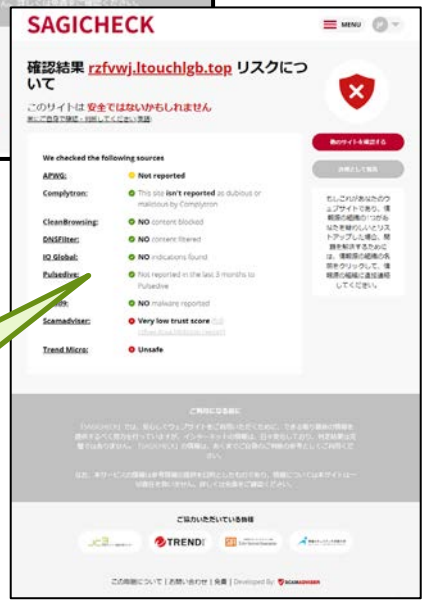
注意喚起

確認サイト
（海外団体との連携）

日本語版 チェックサイトSAGI CHECK（昨年2月から公開中）

ここにURLを入力すると

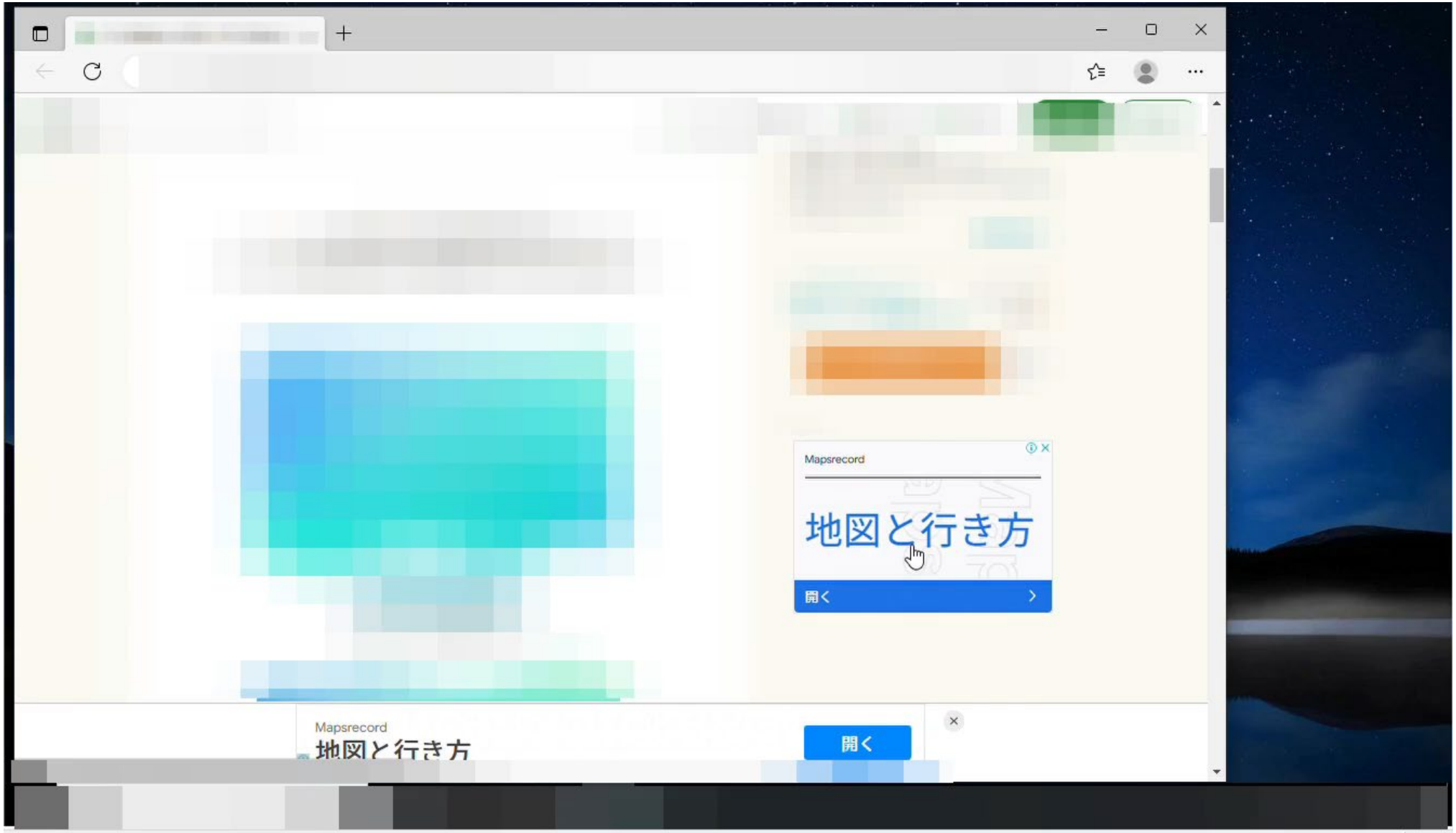
https://sagicheck.jp/



結果が表示される

毎月約2万件の情報を会員企業、APWG、ScamAdovisorに提供

テクニカルサポート詐欺とは（動画）



ブログサイトで
広告をクリック
すると

テクニカルサポート詐欺　～　誰もが巻き込まれる恐れのある犯罪　～

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？　　あわてて○○○○○○○サポートに電話しますか？

※こちらはあくまで一例です。類似した内容や別の電話番号が表示される場合があります。

多くが　IP電話　050-????-????
ですが、
海外の電話番号　0101-?????????　も

引用元：マイクロソフト（https://news.microsoft.com/ja-jp/2021/01/29/210129-information/）

海外でも頻発しており、国際的な協力体制が急務！

- **「サポート詐欺」という犯罪があることを伝えてほしい。**
- **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、絶対に画面の電話番号に電話しないこと　と伝えてほしい。**
- **コンビニなどで高額な電子マネーを買おうとしている人が居たら、声をかけてあげてほしい。話しかけにくければ、店員さんへ。**

※　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！

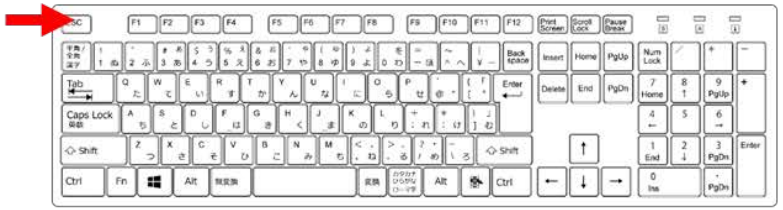
https://www.lac.co.jp/lacwatch/pdf/20230302_cgjournal_vol15.pdf

テクニカルサポート詐欺の遭遇経路（誰でも感染する可能性がある）

- 様々なオンライン広告をクリックすることで遭遇

＜サポート詐欺サイトの消し方＞

- 全画面表示を解除するためにESCキーを押す。**長押しも有効**



- **どうにもならないときは、電源を切る**

- Ctrl＋Del＋Altキーを押し、「タスクマネージャー」を起動させてください。
- サポート詐欺サイトが表示されているブラウザ(Edge, Firefox, Chromeなど)を選び、「タスクの終了」をクリックすればブラウザが落とせます。。

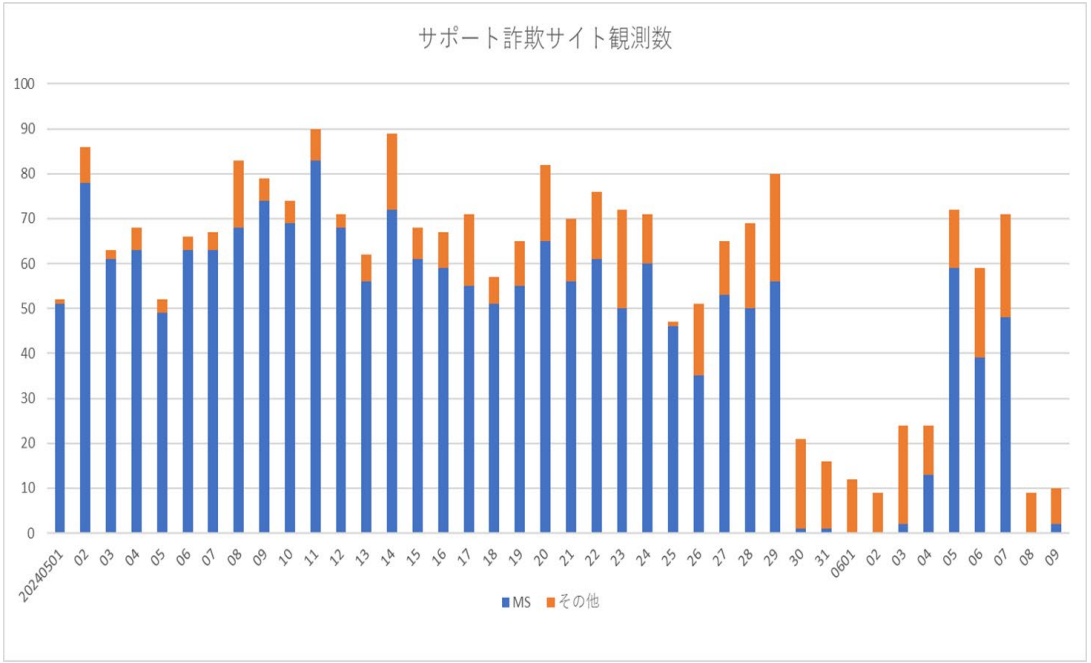
Microsoft社 Digital Crime Unit との協働による対策強化を推進中！

Digital Crime Consortium 2024でプレゼンテーション

松ヶ谷さん（トレンドマイクロ）、 影山さん（ラック）

テーマは、テクニカルサポート詐欺と電話オペレータの追跡の経緯と「偽」被害電話によって得られた犯罪プロファイリング

その結果として・・・



国家を背景とするAPTグループによる標的型攻撃の実態

APTとは、標的型攻撃のうち「発展した／高度な（Advanced）」「持続的な／執拗な（Persistent）」「脅威（Threat）」の略語で、長期間にわたりターゲットを分析して攻撃する緻密なハッキング手法として、2006年ごろに米国空軍のGreg Rattray氏が使用した

標的型サイバー攻撃が、懸念国による諜報活動や情報窃取の最も重要かつ典型的な手段となっている。

ターゲットは、政府機関、重要インフラ、学術・研究機関、シンクタンク、IT・セキュリティ企業等、あらゆる分野の組織や団体となっている。

手口としては、未だ存在を知られていないシステム脆弱性を狙った攻撃（ゼロデイ攻撃）が多く、日本製ソフトウェアの脆弱性も狙われている。

技術情報の窃取には、内通者の存在など、内部脅威も利用されている。

各国のAPT（Advanced Persistent Threat）グループの特徴

主なAPTグループ（ファイア・アイの情報を基に作成）

グループ名	別名	関与が疑われる国家	攻撃対象の業界・業種や企業・組織
APT1	Unit 61398、Comment Crew	中国	情報技術、航空宇宙、行政、衛星／通信、科学研究／科学顧問、エネルギー、運輸など
APT3	UPS Team	中国	航空宇宙／防衛、建設／エンジニアリング、ハイテクなど
APT5	—	未公表	通信事業者の社員やテクノロジー企業、ハイテク製造企業など
APT10	menuPass Team	中国	米国、欧州、日本の建設／エンジニアリング、航空宇宙、通信業界ならびに官公庁
APT12	Calc Team	中国	ジャーナリスト、官公庁、防衛関連組織
APT16	—	中国	日本および台湾のハイテク、行政サービス、メディア、金融業界
APT17	Tailgator Team、Deputy Dog	中国	米国の官公庁、国際的な法律事務所、IT企業
APT18	Wekby	中国	航空宇宙／防衛、建設／エンジニアリング、教育、医療／バイオテクノロジーなど
APT19	Codoso Team	中国	法務、投資業界
APT28	Tsar Team	ロシア	コーカサス地域、東欧諸国の政府および軍隊、欧州の安全保障機関など
APT29	—	ロシア	西欧諸国の政府、外交政策担当グループ、およびその類似組織
APT30	—	中国	東南アジア諸国連合（ASEAN）の加盟各国
APT32	OceanLotus Group	ベトナム	ベトナムの製造、消費者向け製品、コンサルティング、ホスピタリティ分野に投資する外国企業
APT33	—	イラン	航空宇宙、エネルギー業界
APT34	—	イラン	金融、官公庁、エネルギー、化学、通信など。主に中東地域で活動
APT37	—	北朝鮮	韓国、日本、ベトナム、中東諸国の化学、エレクトロニクス、製造、航空宇宙など
APT38	—	北朝鮮	金融機関

＜中国＞
　国家安全部MSSや人民解放軍PLAに関連する組織が多く、政治、外交、行政のほか官民の先進技術情報を狙う。

＜北朝鮮＞
　軍事技術を狙った攻撃のほか、暗号資産等の資金獲得（不正送金等）を目的とした攻撃が多くみられる。

＜ロシア＞
　保安庁FSBや軍参謀本部情報総局GRUに関連する組織が多く、政治、外交、安全保障、機関産業等を狙う。破壊的な攻撃も特徴。

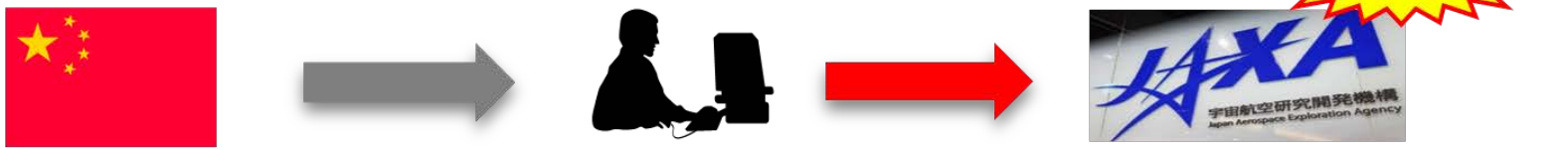
我が国に対するAPTグループによるサイバー攻撃（警察による摘発･公表）

■ **警察の捜査の結果、攻撃主体の解明に至ったものについてはパブリック･アトリビューションや注意喚起が実施され、サイバー攻撃の抑止につながっている**

【ＪＡＸＡ等に対するサイバー攻撃事案の実態解明、公表】（令和３年４月）

- 住所氏名等を偽ってレンタルサーバを契約した中国共産党員の男を検挙
- 所要の捜査の結果、
  - 「Tick」と呼ばれるサイバー攻撃集団によって実行
  - 中国人民解放軍第61419部隊が関与している可能性が高い

と結論づけ、公表



【ラザルスによる暗号資産交換業者に対するサイバー攻撃事案の実態解明、公表】（令和４年10月）

- 国連の報告書等において、北朝鮮当局の下部組織とされるサイバー攻撃集団である「ラザルス」が、暗号資産関連企業等を標的にしている旨の指摘
- サイバー特別捜査隊の捜査等により、
  - 国内の暗号資産交換業者に対しても、暗号資産の不正な窃取を目的としたサイバー攻撃がなされていること
  - 数年来、国内の関係事業者がサイバー攻撃の標的とされていること

が強く推察される状況にあると結論づけ、NISC、金融庁との連名で注意喚起を発出

＜今後の課題＞

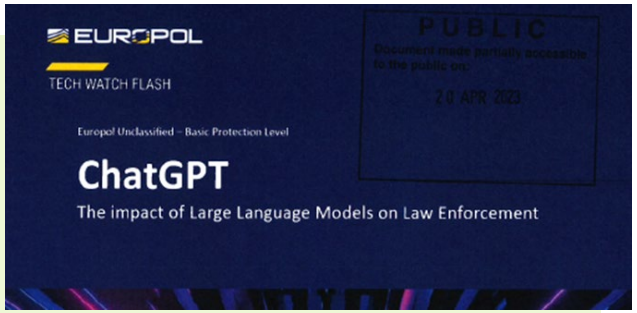
・先進技術の社会実装と安全安心の両立
・身近な公共空間における犯罪の予防のために
・サイバー犯罪対策における官民学連携の意義

① 先進技術の社会実装と安全安心の両立

✓サイバー分野における新たな先進技術の社会実装には、大きな利益とともに一定のリスクが存在している。 ⇐ 予想されるリスクに対して必要十分な規制が実施されるためには、より詳細な実態に関する情報が政府に集約される必要あり

■例えば、、、生成AIによって犯罪も変わる？

ChatGPTが犯罪行為の手助けをしていることをEuropolが警告！



（2023.4.20公表）

「ChatGPTの公開からわずか数週間後には具体的な犯罪行為が確認されています」 犯罪に応用！

「ChatGPTは、犯罪の準備プロセスを加速させ、侵入方法やテロ活動、サイバー犯罪、児童虐待等、広範囲な犯罪について学ぶことができます」 犯罪の手口や新しいツールを教える！

「技術的知識が乏しい潜在的な犯罪者にとっては非常に貴重なリソースで、同時に、より高度な犯罪者は、洗練されたサイバー犯罪の手口をさらに洗練させ、自動化することができます」 手口を高度化！

「会話型チャットボットと非常にリアルなディープフェイクなどの合成メディアを生成できるシステムを組み合わせたAIシステムが、今後の犯罪手法となる可能性があります」 AIが巧妙に人をだます！

② 公共空間におけるサイバー犯罪の予防には何が必要か

✓ 子供からお年寄りまで、知識や技術がある人もない人も、都会の人も田舎の人も、生活もビジネスも、もはやサイバーの世界と関係なしではいられない。

⇐ 今後さらに拡大するサイバーの世界の中で安全安心を確保するには、個人のリテラシーの向上も大切だが、権限・能力があり信頼される組織が対応することが大切

◆ 情報とリソースを持った民間組織の役割

◆ 幅広い情報把握権限・能力と国際連携が可能な行政機関、法執行機関の役割

自衛隊を含めた中央省庁、警察、セキュリティ事業者、システム提供事業者、通信事業者　自治体、勤務先、学校、等が期待に応える能力を備え、積極的に行動することが必要

◆誰にどのような権限を持たせるべきか

【国家安全保障戦略より】

- サイバーセキュリティに関する世界最先端の概念・技術等を常に積極的に活用
- 政府機関等のシステムの導入から廃棄までのライフサイクルを通じた防御の強化、政府内外の人材の育成・活用の促進等
- 能動的サイバー防御の導入に期待

NATIONAL CYBERSECURITY STRATEGY

米国サイバーセキュリティ戦略2023から

サイバー空間における役割・責任・リソースの配分について、根本的な転換が必要

「サイバーセキュリティの負担を、個人・中小企業・地方自治体から切り離し、国民のリスク軽減のための最高の能力・最適な立場を備えた組織に移す」

＜民間セクターとの連携＞

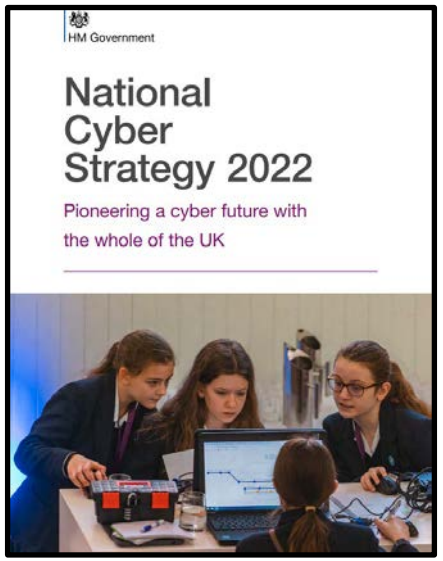
「戦略目標2.2： 敵対勢力を攪乱するための官民作戦オペレーションの強化」

民間部門は、敵対勢力の活動に対する可視性を高めている。その洞察力は、連邦政府よりも広範かつ詳細であることが多い。これは、民間部門とその脅威ハンティング活動の規模が大きいこともあるが、ツールや能力の技術革新のペースが速いことも一因である。悪意あるサイバー活動を効果的に阻止するには、独自の洞察力と能力を持つ民間セクターと、行動する手段と権限を持つ連邦政府機関との間で、より日常的な協力が必要である。（中略）

民間セクターのパートナーは、NCFTAのような、連邦政府との作戦協力のハブとして機能する 1 つ以上の非営利組織を通じて結集し、その努力を組織化することが奨励される。

HM Government

英国サイバー戦略2022　から



＜5つの柱の５＞

- サイバー空間の内部およびサイバー空間を通じた英国の安全保障の強化のために**敵対者を検知し、攪乱し、抑止する**。

＜ 民間セクターとの連携＞

- あらゆる情報源を活用し、**政府、法執行機関、民間セクター全体の専門知識を結集して**、最も深刻な国家的、犯罪的、およびその他の種類の脅威の日常的かつ包括的な調査を実施している。
- 捜査ではあらゆる情報源からの情報を支えとしつつ、**民間セクター全体のスキルと知識も活用し、例えば企業による法執行機関とのデータ共有も円滑化していく**。

National Cyber Security Centre

＜参考＞　英国の　Active Cyber Defense Programme（2016年～）
英国のACDプログラムでは、国民からの通報を受けた政府機関が、１年間にフィッシング関連　6万件を含め、180万件のサイトをテイクダウンするなど、総合的なプログラムで国民の大多数を守るための対策が行われている

③　サイバー犯罪対策における官民学連携の意義

✓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

JC3を通じて警察と連携することの意義、そして今後の課題

■関係被疑者の検挙　→加担していた者の検挙は、犯罪者グループに一定の打撃！

■捜査結果から、犯罪の準備状況、実際の犯行、事後的な収益化まで、
犯行の全体図や犯罪抑止のヒントが見える可能性

犯行の具体的手口や悪用された犯罪のツール（犯罪インフラ）が明らかに

指示役等、上位者とのやり取りや、犯罪収益の流れが見える可能性

犯罪グループの組織構成、組織実態が判明する場合も

→ 企業の皆様からみて、自身のサービスの弱点が分かり、対策を講じるきっかけになるなど、極めて有益な情報が提供されていると評価されている

→ FBI等の海外捜査機関は、「犯罪の拡大や被害防止が捜査機関の役割」と公言し、具体的な働きかけや民間への情報共有を実施。
民間側も、積極的に捜査機関や政府機関に情報を提供

【追加ページ】 今後の課題　企業に何が求められるのか

◆自社（従業員）が標的となる可能性についての意識啓発が、経営層を含め、企業内の各層で十分に行われ、必要な対策が取られることが前提。

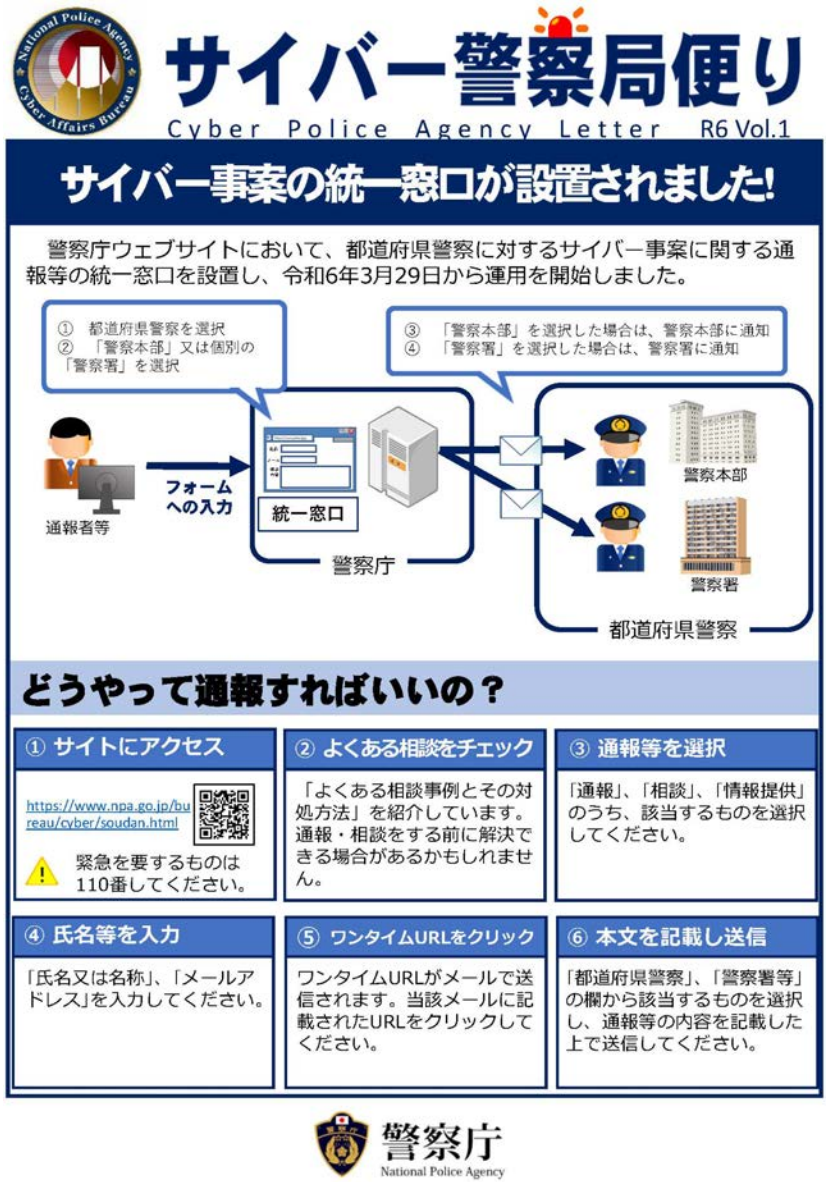
◆被害が潜在化しやすいサイバー犯罪や攻撃（サイバー犯罪や国家支援型のサイバー攻撃への対処）については、より多くの情報に接する民間企業（被害企業を含む。）側からの情報提供・政府への協力が、悪意ある攻撃への対抗手段をとる上で必須。

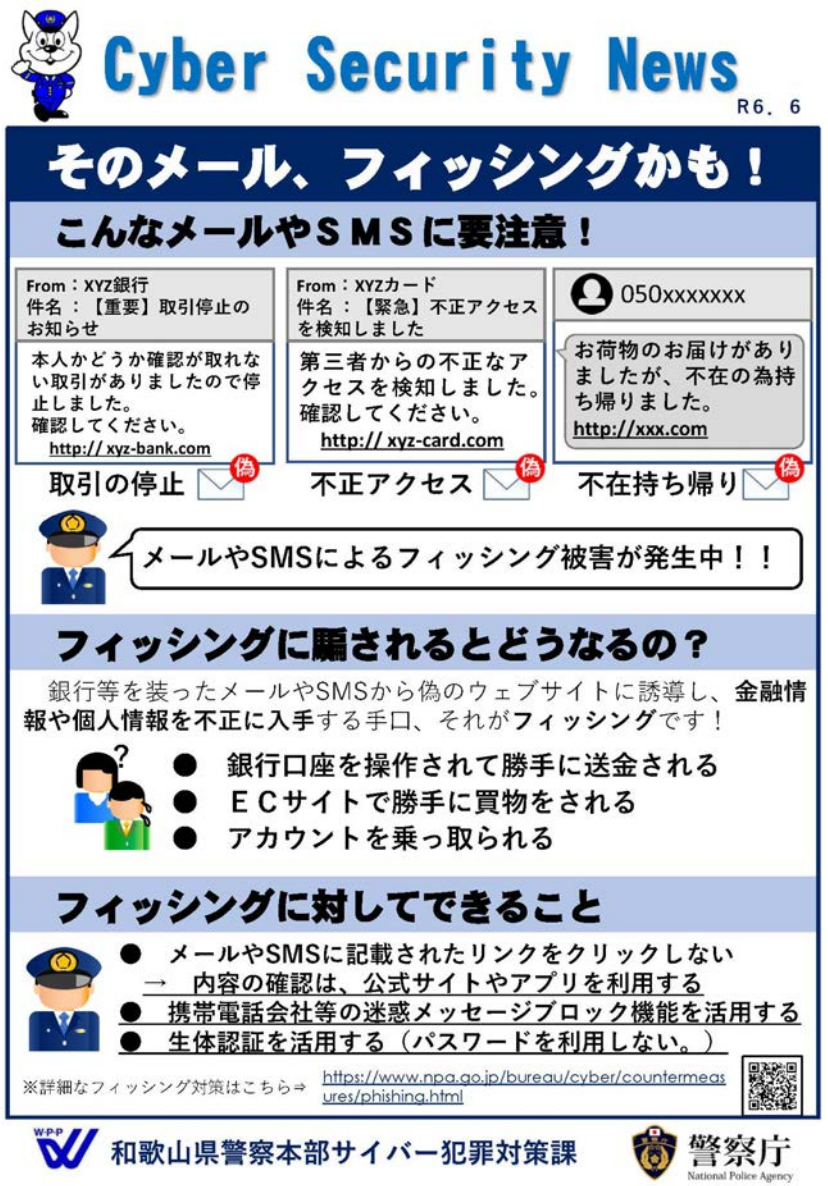
⇐　**警察庁Webサイトに、都道府県警察の通報・相談窓口を統一化**

◆企業側が政府へ情報提供や被害の公表を行う上での、法的リスクやレピュテーションリスクを下げるための産業界全体での取組が必要。

◆　広義のサイバー領域において、企業本体及びそのビジネスを守るために必要な「積極的な投資」を求めたい。

困ったときは、迷わず各都道府県警察・警察庁へ





【追加ページ】　警察に何が求められているのか、期待されているのか

◆　サイバー犯罪・サイバー攻撃やネットワークを利用した犯罪が、国民の治安への不安となっていること（警察庁アンケート結果）

◆　犯罪被害総額の約45%、詐欺被害の約70%を占めていること（JC3推計）

◆　被害が目に見えず、潜在化しやすいサイバー分野の被害について、被害者を含む民間企業側からの積極的な情報提供・協力を求めるためには、警察職員側が十分な知識と経験を積み重ねることが必須
　→　専務員だけでなく全ての職員が、「知らない」「わからない」では済まされないことに留意

◆　企業側が政府へ情報提供を行う上での法的リスクやレピュテーションリスクを下げるためにも、警察における「保全」（秘密の保持）を確実にすること。

時代の変化に遅れない「視野」「知識」「経験」を身に着けよう

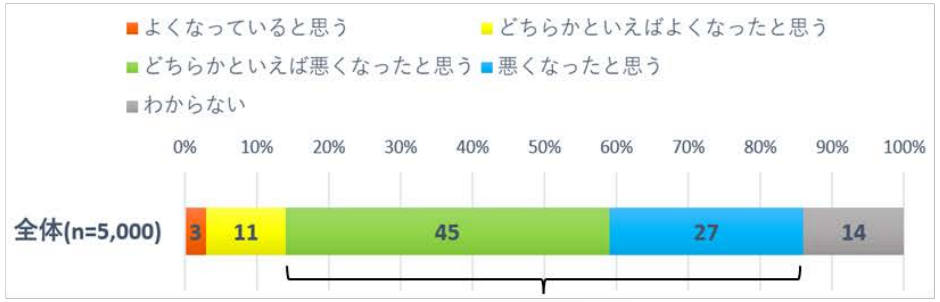
治安に関するアンケート結果（令和5年）

◆ 日本の治安はよいと思うか
（そう思う＋まあそう思う）

65％

注　各数値について小数第１位以下を四捨五入しているため、
総計が必ずしも100にならない。

◆ ここ10年で日本の治安はよくなったと思うか
（悪くなったと思う＋どちらかといえば悪くなったと思う）

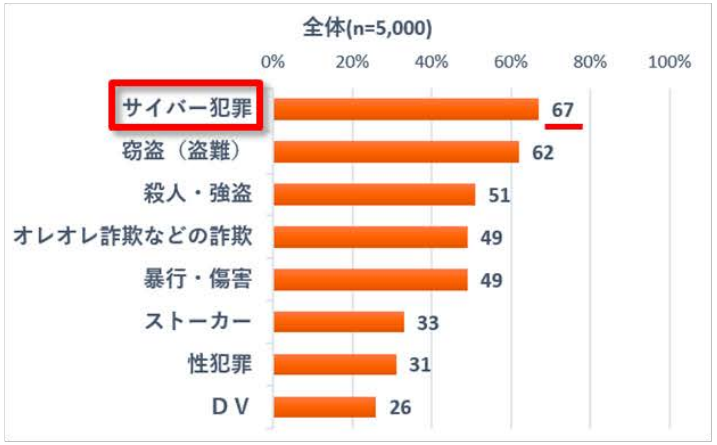


７２％

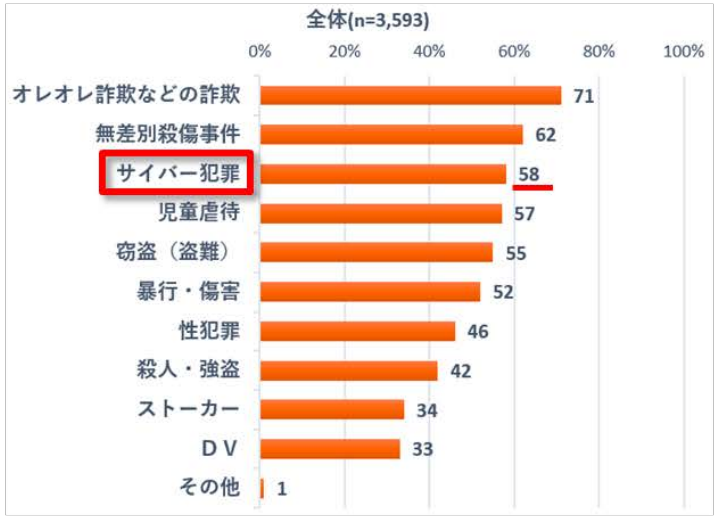
注　各数値について小数第１位以下を四捨五入しているため、
総計が必ずしも100にならない。

※　令和５年10月実施、5,000人対象

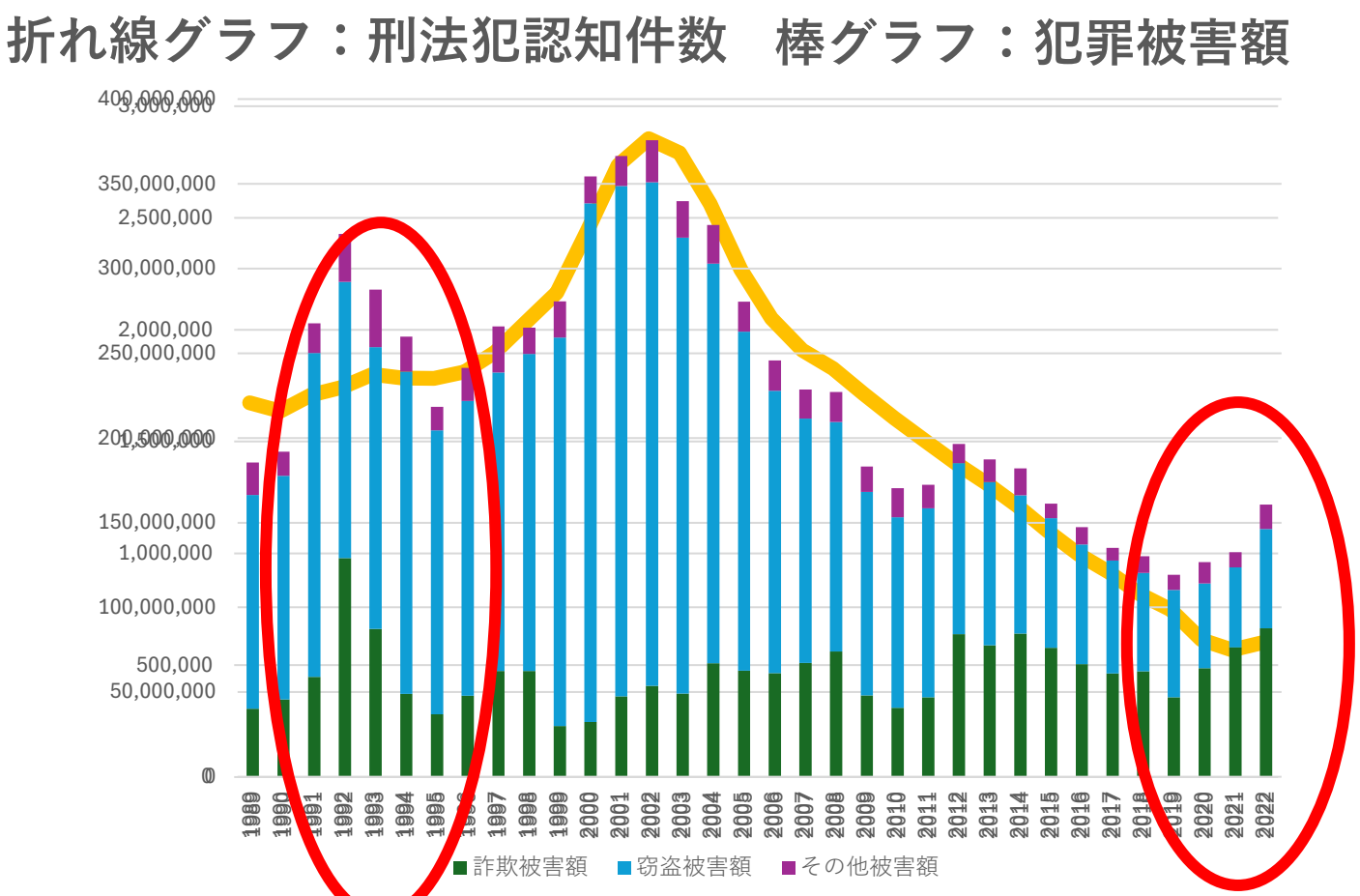
◆ 犯罪被害にあう危険性について
（不安を感じる＋ある程度不安を感じる）



◆ 治安が悪くなったと思う際に想起した犯罪



刑法犯認知件数の減少に対し、犯罪被害総額はどうなっているのか



刑法犯認知件数の推移と異なる被害総額の増加がみられるのは、

バブル期と近年のみ

原因は、詐欺の急増

ではどんな詐欺が今増えている？

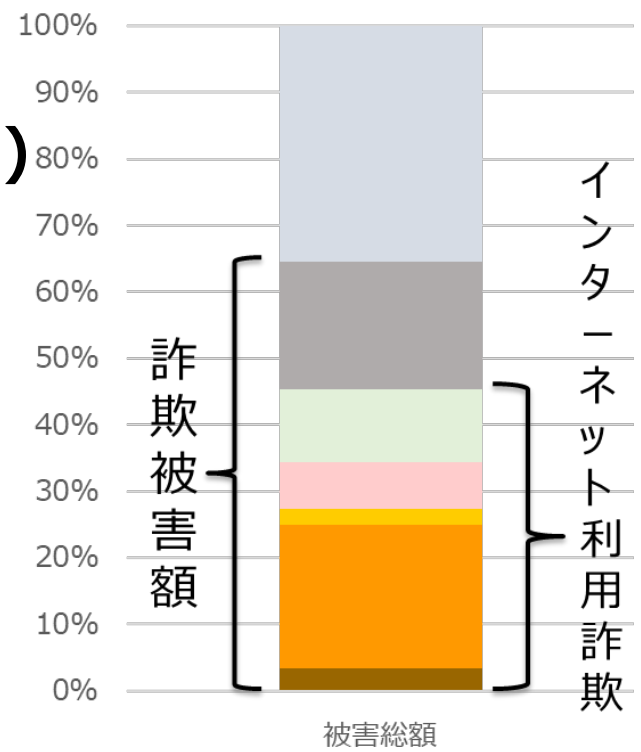
令和5年の**犯罪被害総額は、 約2,519億円** （前年は 約1,608億円 56.7%増加）

うち**詐欺による被害額は約64.5%を占める 約1,626億円**（前年は 約877億円 85.4%増加）

財産犯に占めるサイバー犯罪・インターネット利用犯罪等の割合は？

「インターネットを利用した詐欺の増加等が寄与している」（警察庁）

「被害総額の約45%、詐欺被害の約70%を占めていると推計」（JC3）



- インターネットバンクIBによる不正送金　　87.3億円（前年は　15.2億円）
- クレジットカード不正使用　　540.9億円 (前年は　436.7億円）
- テクニカルサポート詐欺　　約61億円と推計
（架空請求詐欺　約140億の43.7%がポップアップ表示から）
- ロマンス詐欺　177.3億円
- SNS投資詐欺　277.9億円

小計　1144.4億円

「財産犯の被害額の推移については、約 2,519 億円と前年比で 56.7%増加してい る。その内訳を見ると、詐欺による被害額が約 1,626 億円と増加している（前年比 85.4%増加）（図５）。また、詐欺による被害の増加については、インターネットを 利用した詐欺の増加等が寄与している状況が認められた。」（令和5年の犯罪情勢より）

あらゆる犯罪がインターネットやSNS利用型に

警察庁は、「サイバー犯罪」を　①不正アクセス禁止法に規定された不正アクセス、　②刑法に規定された不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪、　③インターネットを主な手段とした各種の犯罪の総称であるインターネット利用犯罪（フィッシング等によるインターネットバンキング不正送金、ECサイト等でのクレジットカード不正使用等）としています。

しかしながら、サイバー犯罪か否かに関わらず、ネットワーク上では様々な犯罪や犯罪に関係する行為が行われています。例えば、

テクニカルサポート詐欺（ネット画面上に突然ポップアップを表示するなどして、修理名目で送金させる）

出会い系サイトやSNSでは

- 未成年者と出会って、わいせつな行為をする・させる
- 出会った人からお金を脅し取ったり（恐喝罪）、だまし取ったり（詐欺罪）する
- 「闇バイト」と称して高額な報酬を払うことを約束して、違法な行為をする人を募集する
- お互いに顔も名前も知らない者同士で、連絡を取り、指示をして犯罪行為を行う

インターネット上で

- 他人の著作物を勝手に利用・販売する（著作権法違反）
- 他人を誹謗中傷する（名誉毀損罪）
- わいせつ画像を掲載する（わいせつ物頒布罪）
- 違法な薬物を売買する（薬物関係法令違反）
- 偽造ブランドの商品を販売

暗号資産取引等を利用して、犯罪行為で得られた報酬をマネーロンダリングする

犯罪対策閣僚会議において　サイバー犯罪も念頭に置いた対応方針を決定

国民を詐欺から守るための総合対策（概要）

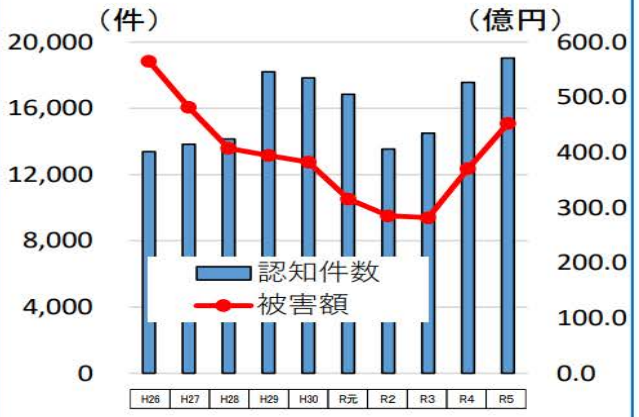
現在の情勢

特殊詐欺等に対しては、「オレオレ詐欺等対策プラン」（令和元年６月25日犯罪対策閣僚会議決定）及び「ＳＮＳで実行犯を募集する手口による強盗や特殊詐欺事案に関する緊急対策プラン」（令和５年３月17日犯罪対策閣僚会議決定）等に基づき官民一体となった対策を講じてきた一方で、令和５年中の詐欺被害は約1,630億円と前年から倍増。

近年、ＳＮＳやキャッシュレス決済の普及等が進む中で、これらを悪用した犯罪の手口が急激に巧妙化・多様化。それによって引き起こされる詐欺等の被害が、加速度的に拡大する状況。

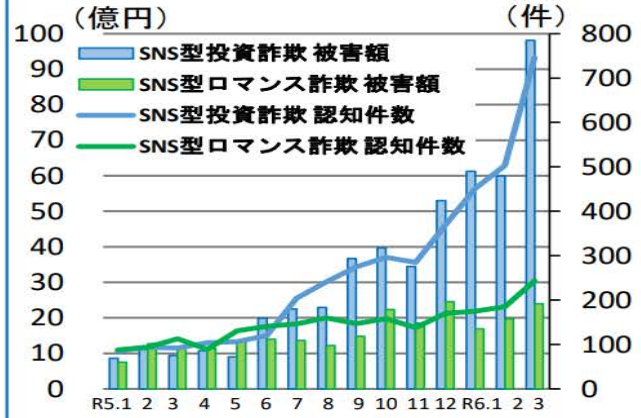
特殊詐欺

✓令和５年被害額は約452億円
✓前年から約80億円増加



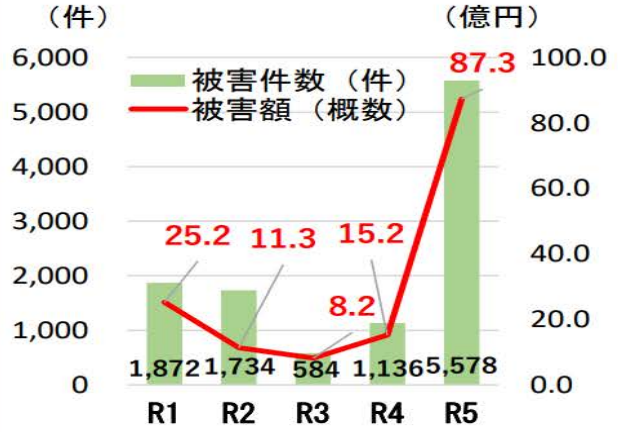
ＳＮＳ型投資・ロマンス詐欺

✓令和５年下半期から急増
✓同年被害額は約455億円
✓令和６年１～３月被害額は約279億円



フィッシングによる被害

✓インターネットバンキングに係る不正送金被害が急増(令和５年約87億円)



総合対策の策定

○　こうした情勢の中、変化のスピードに立ち後れることなく対処し、国民を詐欺の被害から守るためには、官民一体となって、一層強力な対策を迅速かつ的確に講じることが不可欠。

○　従来のプランを発展的に解消させ、特殊詐欺、ＳＮＳ型投資・ロマンス詐欺及びフィッシング等を対象に、総合的な対策を取りまとめ、政府を挙げて対策を推進。

「国民を詐欺から守るための総合対策」における主な施策

1.「被害に遭わせない」ための対策

ＳＮＳ型投資・ロマンス詐欺対策

- **被害発生状況等に応じた効果的な広報・啓発等**
  - ○　不審なアカウントとのやり取りを開始する時など、詐欺の被害に遭う場面を捉えて利用者に個別に注意喚起を行うよう、ＳＮＳ事業者に要請
- **ＳＮＳ事業者等による実効的な広告審査等の推進**
  - ○　プラットフォーム上に掲載される広告の事前審査基準の策定・公表、審査体制の整備（特に、日本語や日本の社会等を理解する者の十分な配置）、広告出稿者の本人確認の強化等をＳＮＳ事業者に要請
  - ○　捜査機関から提供された「詐欺に使用されたアカウント」等の情報に着眼した、広告の迅速な削除等をＳＮＳ事業者に要請
- **なりすまし型偽広告の削除等の適正な対応の推進**
  - ○　なりすまし型の偽広告等に関し、ＳＮＳ事業者に対し、利用規約等に基づき、詐欺広告の削除等の措置を講ずるよう、事業者団体に通知
  - ○　インターネットで拡散する偽・誤情報や、なりすまし型偽広告への対応等について、国際的な動向を踏まえつつ、制度面も含む総合的な対策を推進
- **大規模プラットフォーム事業者に対する削除対応の迅速化や運用状況の透明化に係る措置の義務付け等**
  - ○　インターネット上の違法・有害情報への対応として、削除対応の迅速化や運用状況の透明化を大規模プラットフォーム事業者に義務付ける情報流通プラットフォーム対処法を速やかに施行するとともに、違法情報への該当性に関するガイドラインを迅速に策定
- **知らない者のアカウントの友だち追加時の実効的な警告表示・同意取得の実施等**
- **ＳＮＳの公式アカウント・マッチングアプリアカウント開設時の本人確認強化**
- **新たに開始された金融教育における被害防止に向けた啓発**
  - ○　金融経済教育推進機構（J-FLEC）による関係省庁と連携した金融経済教育の提供等を通じた金融リテラシーの向上

フィッシング対策

- **送信ドメイン認証技術（ＤＭＡＲＣ等）への対応促進**
  - ○　利用者にフィッシングメールが届かない環境を整備するため、インターネットサービスプロバイダー等のメール受信側事業者や、金融機関等のメール送信側事業者等に対して、送信ドメイン認証技術の計画的な導入を要請
- **フィッシングサイトの閉鎖促進**
- **フィッシングサイトの特性を踏まえた先制的な対策**
  - ○　フィッシングサイトが有する、１つのＩＰアドレス上に複数のサイトが構築されるなどの特性を踏まえ、いまだ通報がなされていないフィッシングサイトを把握して、ウイルス対策ソフトの警告表示等に活用するなどを検討

特殊詐欺等対策

- **国際電話の利用休止申請の受付体制の拡充**
  - ○　国際電話番号を利用した詐欺の被害を防止するため、国際電話の利用休止を一括して受け付ける「国際電話不取扱受付センター」を運営する電気通信事業者に対して、申請受付体制の更なる拡充を要請
- **ＳＭＳの不適正利用対策の推進**
  - ○　ＳＭＳの悪用を防止するため、ＳＭＳフィルタリングの活用の拡大等を推進
- **携帯電話を使用しながらＡＴＭを利用する者への注意喚起の推進**

2.「犯行に加担させない」ための対策

- **「闇バイト」等情報に関する情報収集、削除、取締り等の推進**
- **青少年をアルバイト感覚で犯罪に加担させない教育・啓発**

3.「犯罪者のツールを奪う」ための対策

- **本人確認の実効性の確保に向けた取組**
  - ○ 携帯電話等の契約時の本人確認をマイナンバーカード等を活用した電子的な確認方法へ原則一本化
- **金融機関と連携した検挙対策の推進**
  - ○ 金融機関において、詐欺被害と思われる出金・送金等の取引をモニタリング・検知する仕組み等を構築するとともに、不正利用防止の措置を行い、疑わしい取引の届出制度の活用をはじめ、不正な口座情報等について警察へ迅速な情報共有を実施
- **電子マネーの犯行利用防止対策**
  - ○ 詐取された電子マネーの利用を速やかに発見するためのモニタリングの強化、発見した場合の電子マネーの利用の停止、警察への情報提供の体制について検討
- **預貯金口座の不正利用防止対策の強化等**
  - ○ 法人口座を含む預貯金口座等の不正利用を防止するための取引時確認の一層の厳格化等の推進
- **暗号資産の没収・保全の推進**

4.「犯罪者を逃さない」ための対策

- **匿名・流動型犯罪グループに対する取締り及び実態解明体制の強化**
- **ＳＮＳ事業者における照会対応の強化**
  - ○ ＳＮＳ事業者に対し、捜査機関からの照会への対応窓口の日本国内への設置、迅速な照会対応が可能な体制の整備等を要請
- **海外拠点の摘発の推進等**
- **法人がマネー・ローンダリングに悪用されることを防ぐ取組の推進**
  - ○ 実態のない法人がマネー・ローンダリング等の目的で利用されることを防ぐための新たな方策について検討
- **財産的被害の回復の推進**
  - ○ 被害回復給付金支給制度及び振り込め詐欺救済法のきめ細やかな周知など効果的な運用の促進

ありがとうございました

JC3 Japan Cybercrime Control Center