サイバー空間の脅威の情勢とJC3の主な活動
～産官学の連携の現場から～

2025年3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の組織概要

10年を超えました！

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主な企業・機関・研究者の方々

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. イオンﾌｨﾅﾝｼｬﾙｻｰﾋﾞｽ株式会社
3. 株式会社イオン銀行※
4. Auﾌｨﾅﾝｼｬﾙﾎｰﾙﾃﾞｨﾝｸﾞｽ株式会社
5. auﾌｨﾅﾝｼｬﾙｻｰﾋﾞｽ株式会社※
6. Auペイメント株式会社 ※
7. SBIﾎｰﾙﾃﾞｨﾝｸﾞｽ株式会社
8. 株式会社SBI証券※
9. SBI EVERSPIN株式会社※
10. NRIｾｷｭｱﾃｸﾉﾛｼﾞｰｽﾞ株式会社
11. 株式会社NTTﾃﾞｰﾀ
12. 株式会社NTTﾃﾞｰﾀﾌｨﾅﾝｼｬﾙﾃｸﾉﾛｼﾞｰ※
13. 株式会社SBI新生銀行
14. 株式会社ｱﾌﾟﾗｽ※
15. 新生ﾌｨﾅﾝｼｬﾙ株式会社※
16. 株式会社ｼﾞｪｰｼｰﾋﾞｰ
17. ｾｺﾑ株式会社
18. 株式会社セブン銀行
19. 株式会社ﾊﾞﾝｸﾋﾞｼﾞﾈｽﾌｧｸﾄﾘｰ※
20. 株式会社ACSiON※
21. 株式会社ｿﾘﾄﾝｼｽﾃﾑｽﾞ
22. ﾃﾞﾛｲﾄ ﾄｰﾏﾂ ｻｲﾊﾞｰ合同会社
23. ﾄﾚﾝﾄﾞﾏｲｸﾛ株式会社
24. 日本電気株式会社
25. 日本ｱｲ･ﾋﾞｰ･ｴﾑ株式会社
26. 野村ホールディングス株式会社
27. 株式会社日立製作所
28. 株式会社bitFlyer
29. 富士通株式会社
30. 株式会社みずほ銀行
31. 株式会社三井住友ﾌｨﾅﾝｼｬﾙｸﾞﾙｰﾌﾟ
32. SMBCｺﾝｼｭｰﾏｰﾌｧｲﾅﾝｽ株式会社※
33. 株式会社日本総合研究所※
34. 株式会社三井住友銀行※
35. 三井住友信託銀行
36. 株式会社三菱UFJ銀行
37. 株式会社ﾒﾙｶﾘ
38. 株式会社ﾒﾙﾍﾟｲ※
39. 株式会社ゆうちょ銀行
40. LINEﾔﾌｰ株式会社
41. LINE Pay株式会社※
42. 株式会社ﾗｯｸ
43. 株式会社ﾘｸﾙｰﾄ
44. 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NTTﾄﾞｺﾓ
3. 株式会社カウリス
4. Gftd Japan株式会社
5. KDDI株式会社
6. KELA株式会社
7. GMOﾌﾞﾗﾝﾄﾞｾｷｭﾘﾃｨ株式会社
8. 株式会社 ｾﾌﾞﾝ&ｱｲ･ﾎｰﾙﾃﾞｨﾝｸﾞｽ
9. SocioFuture株式会社
10. ｿﾌﾄﾊﾞﾝｸ株式会社
11. Chainalysis Japan株式会社
12. トビラシステムズ株式会社
13. 株式会社西日本シティ銀行
14. 日本マイクロソフト株式会社
15. 株式会社ふくおかﾌｨﾅﾝｼｬﾙｸﾞﾙｰﾌﾟ
16. PayPay株式会社
17. PayPay銀行株式会社
18. 株式会社ﾐｽﾐｸﾞﾙｰﾌﾟ本社
19. 株式会社めぶきﾌｨﾅﾝｼｬﾙｸﾞﾙｰﾌﾟ
20. 株式会社横浜銀行

- 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

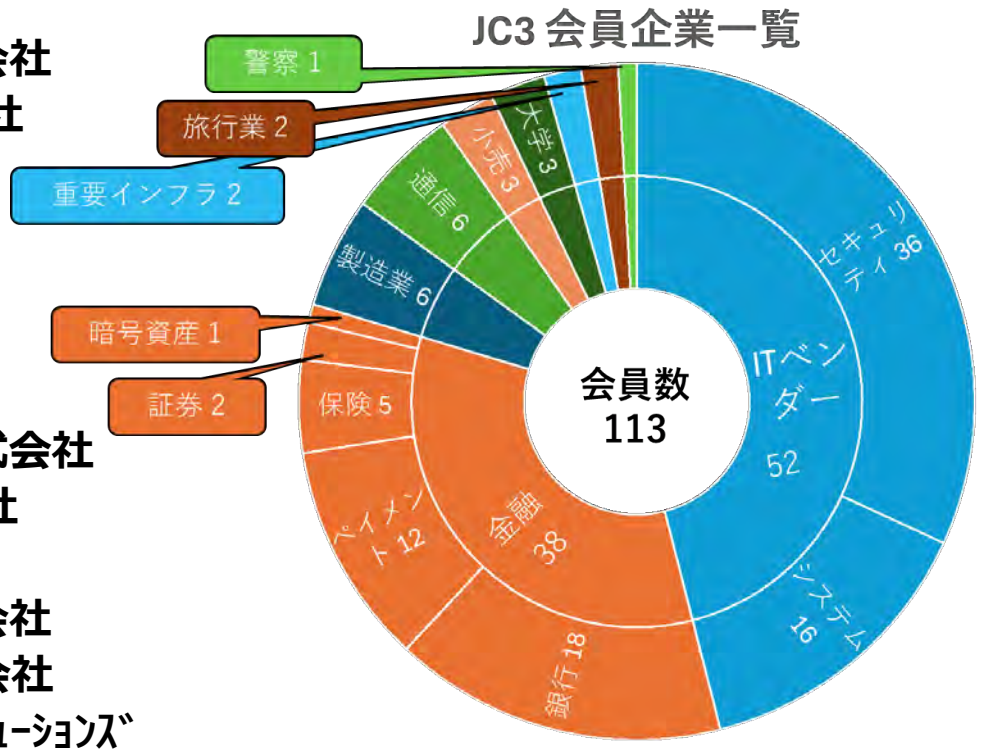
JC3 御賛同いただいている企業・機関・研究者の方々②

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）

◆ トライアル　５社
（賛助会員からトライアルに移行している　KDDIデジタルセキュリティ株式会社を含む。）

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. 株式会社KPMG　FAS
10. 高速道路トールテクノロジー株式会社
11. 株式会社ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所
12. さくらｲﾝﾀｰﾈｯﾄ株式会社
13. ｻﾝ電子株式会社
14. 株式会社JTB
15. ｼｽｺｼｽﾃﾑｽﾞ合同会社
16. Splunk Services Japan合同会社
17. Sky株式会社
18. 住信SBIﾈｯﾄ銀行株式会社
19. 全日本空輸株式会社
20. 綜合警備保障株式会社
21. 株式会社ソフトプレックス
22. 損害保険ジャパン株式会社
23. ﾃﾞｼﾞﾀﾙﾎｰﾙﾃﾞｨﾝｸﾞｽ株式会社
24. 東京海上日動火災保険株式会社
25. TOPPANﾎｰﾙﾃﾞｨﾝｸﾞｽ株式会社
26. 日本信号株式会社
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. BlackBerry Japan株式会社
33. 株式会社マキナレコード
34. 三井住友海上火災保険株式会社
35. 三井物産ｾｷｭｱﾃﾞｨﾚｸｼｮﾝ株式会社
36. 株式会社三越伊勢丹ｼｽﾃﾑ・ｿﾘｭｰｼｮﾝｽﾞ
37. 三菱ＵＦＪﾆｺｽ株式会社
38. Musarubra Japan株式会社
39. 明治安田生命保険相互会社
40. 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

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

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！～

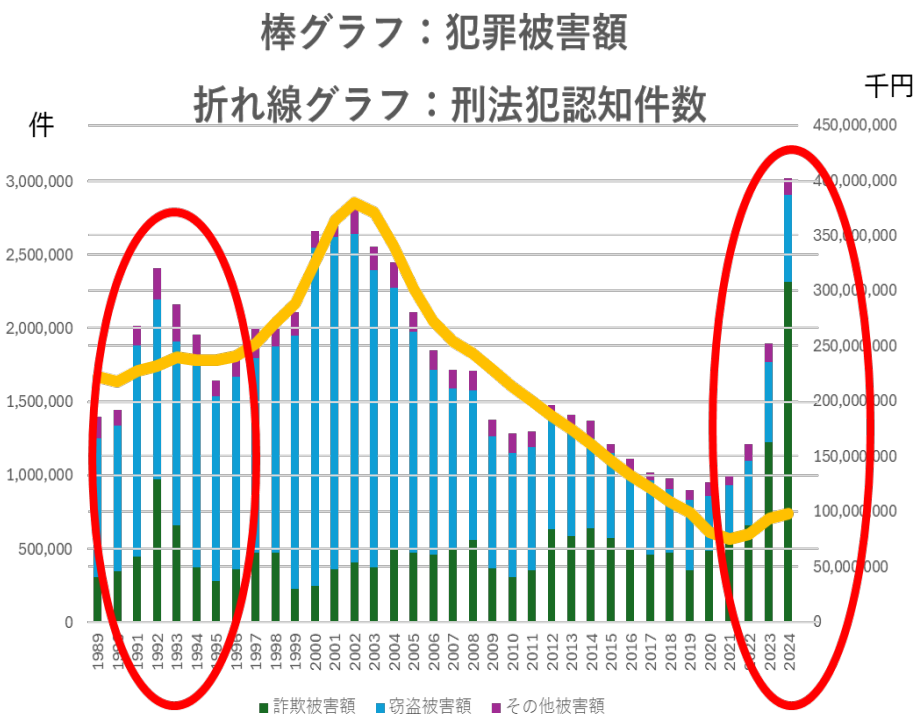
JC3の活動からわかること

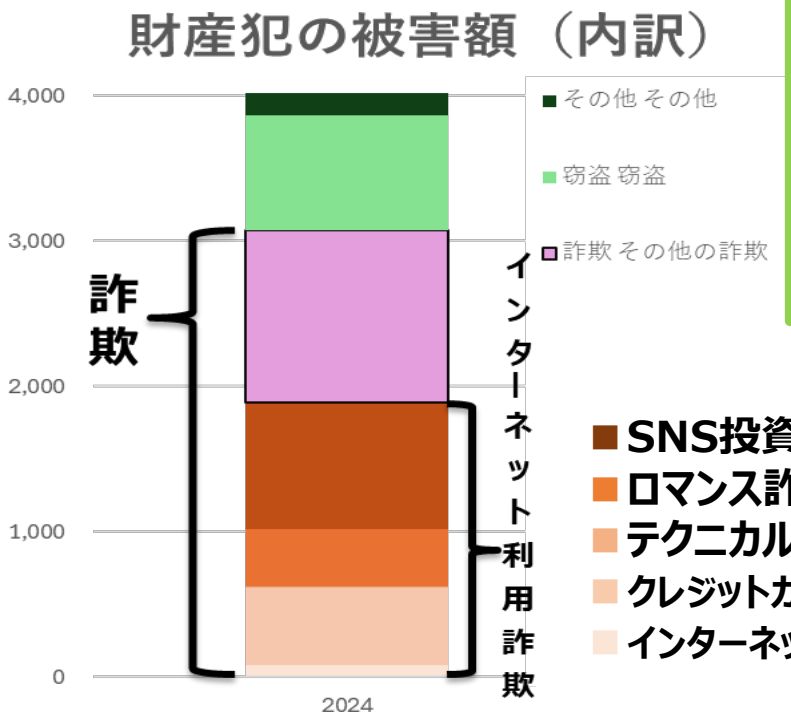
・フィッシングによる情報窃取と詐欺
・ランサムウェア攻撃
・偽ショッピングサイト
・テクニカルサポート詐欺
・標的型APT攻撃　　等

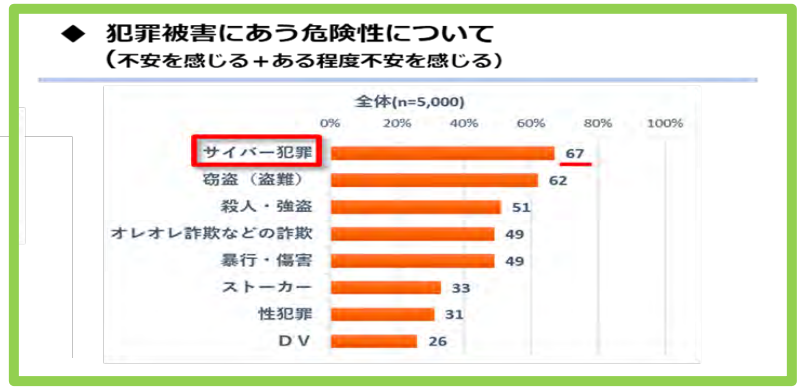
犯罪被害総額の変化から見えるもの　～　詐欺とインターネット犯罪の急増　～

◆ 2024年の　**犯罪被害総額**は、**約4,021億円　と急増し、過去最多**　（前年比　59.6%増加）
　うち　**詐欺による被害額**は**約76%を占める　約3,075億円**で**過去最多**（前年比　89.1%増加）
　　＜財産犯の主流は、窃盗から詐欺に劇的に変化＞

◆インターネット利用した詐欺が、**詐欺被害の約61%、犯罪被害総額の約47%**、を占めている
◆サイバー犯罪・サイバー攻撃等の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（警察庁アンケート結果）







■**SNS投資詐欺**　　**871.0億円**
■**ロマンス詐欺**　　**397.0億円**
■**テクニカルサポート詐欺**　**11.9億円**
■**クレジットカード不正使用**　**約528.0億円**（年間値を推計）
■**インターネットバンクIBによる不正送金**　**82.2億円**
小計　1890.1億円

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）

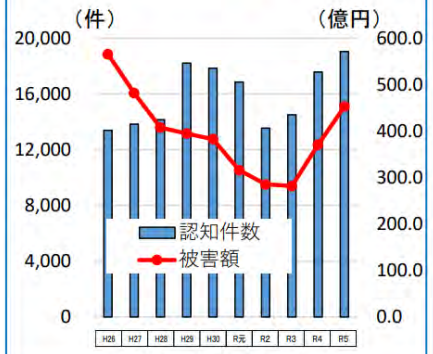
現在の情勢

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。

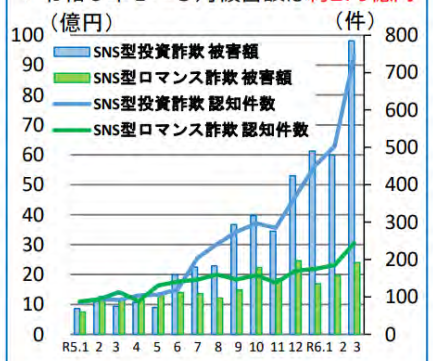
特殊詐欺

✓令和５年被害額は約452億円
✓前年から約80億円増加



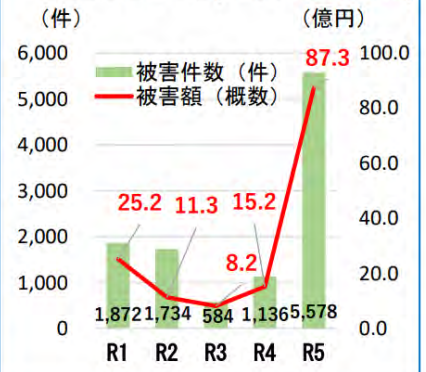
ＳＮＳ型投資・ロマンス詐欺

✓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**

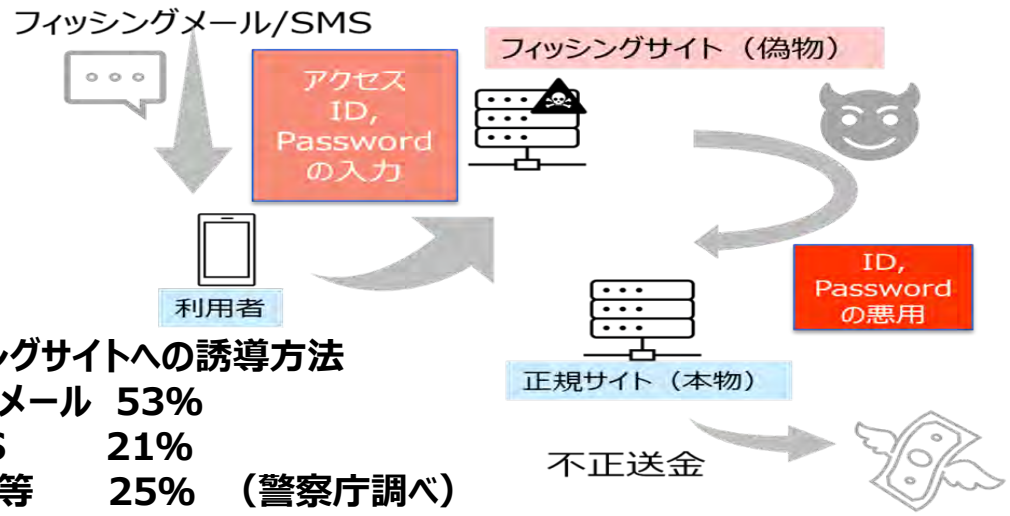
4.「犯罪者を逃さない」ための対策

- **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

情報窃取の裏側にあるフィッシングとその被害（不正送金、クレカ不正使用）

貴方の個人情報が狙われている！

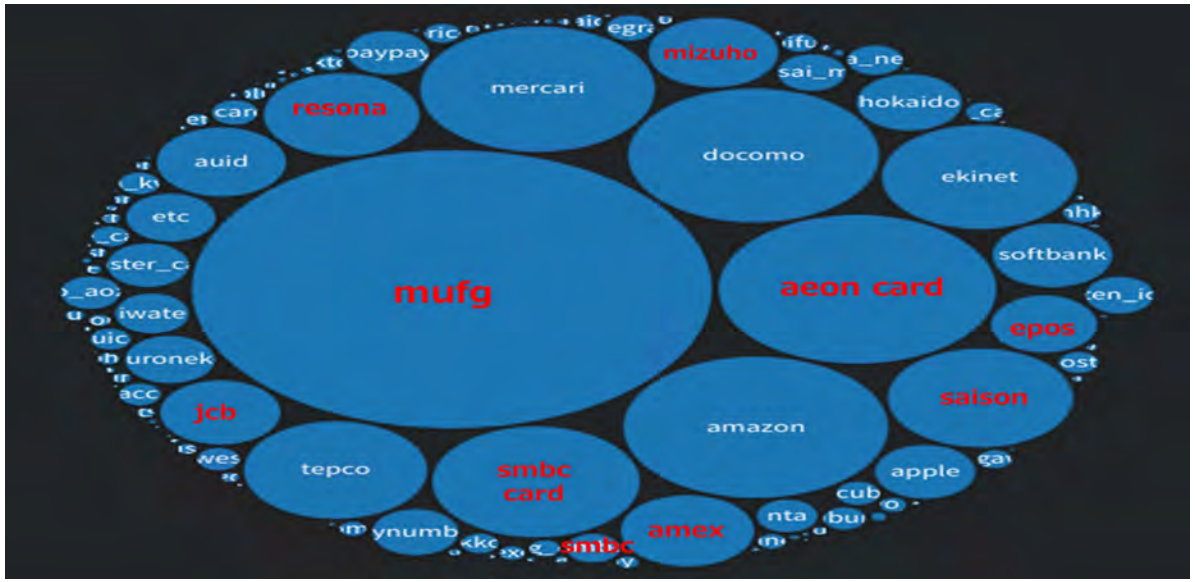
■ フィッシング(Phishing)による情報の窃取



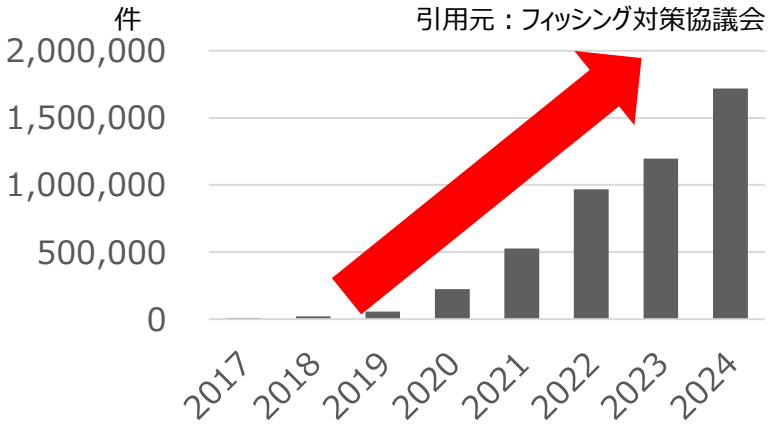
フィッシングサイトへの誘導方法

電子メール　53%
SMS　　21%
不明等　　25%　（警察庁調べ）

フィッシングサイトのターゲット一覧　（2024年　JC3調べ）



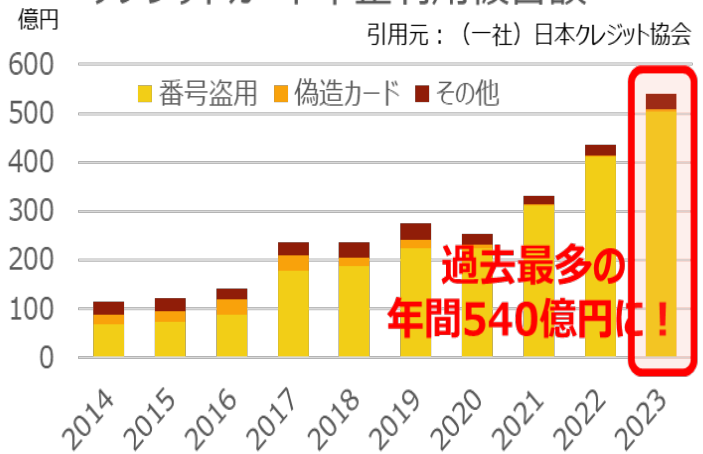
フィッシング報告件数



ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞに係る不正送金

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）

クレジットカード不正利用被害額



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。）

電子メールやSMS等のリンクからアクセスしたWebサイトに、**ID　パスワード**や**個人情報**を入力しないでください。

金融機関の「公式HP」「公式アプリ」 から正しい情報を入力してください。

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）

配送業者等を騙った
メッセージ

【重要なお知らせ】必ずご確認下さい。
https://****.***/
****

①スミッシング

SMS

②リンク先へアクセス

③ iPhoneの場合
フィッシングサイトへ
（架空請求等）

ブラウザ
アップデートを装った
偽サイト

③ Android端末の場合
不正アプリのダウンロード

✓ MoqHao(XLoader)
✓ KeepSpy

配信基盤化

インストールを許可すると
- フィッシングサイトへ誘導され、端末内の情報等が窃取される
- 攻撃のC2サーバと通信して、コマンドを受け付ける
- スミッシングメッセージを他の端末に配信する　etc...

①'スミッシング

SMS

④C2サーバからの指令 C2 Server

トビラシステムズ調べ（2月25日）
Androidマルウェア感染端末台数

3,041

昨年2月初旬には、国内の約2万のスマホが感染し、1日に400万件以上のメッセージが飛び交っていた！

日付	観測件数
2024/1/26	19,873
12/28	5,230
2025/1/7	5,432
1/15	4,363

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

- JC3がSMSを観測し、携帯事業者が行う危険SMS拒否設定によりブロック
- 事業者は端末上で隔離する安心アプリも提供

主要サイトの変化(KeepSpy)（2023年9月～11月）とJC3からの注意喚起

「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

【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

「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

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

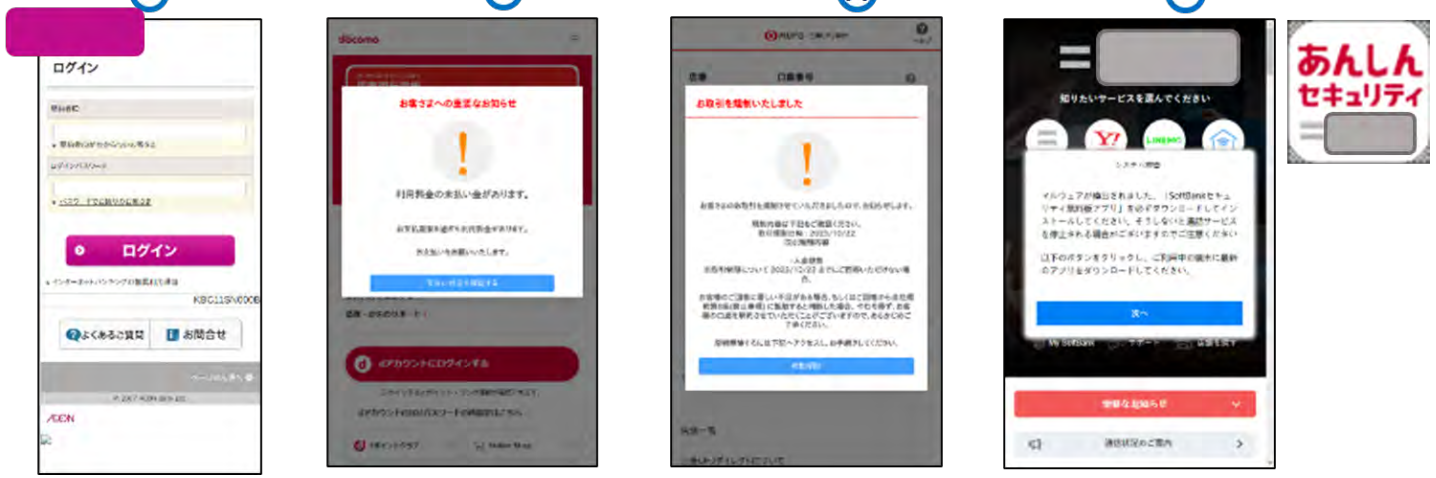
「イオン*銀行」お客様の口座を一時凍結しています。
https://aeonztn[.]github[.]io

【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

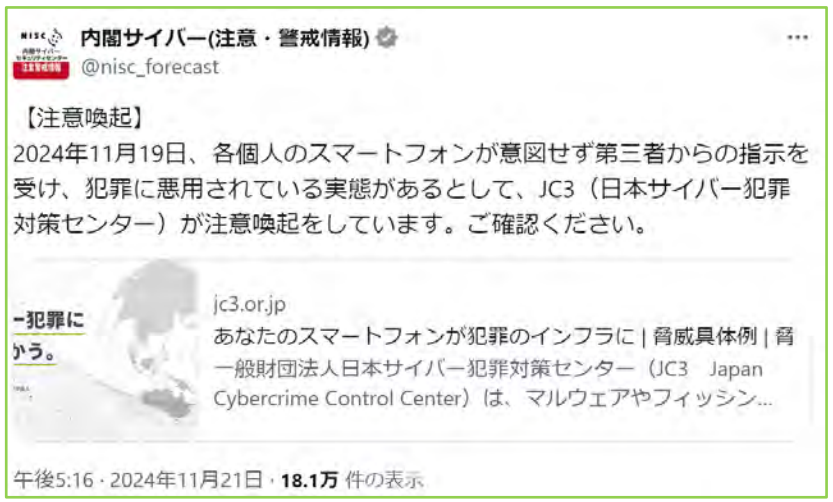
【重要】三菱UFJ銀行お知らせ、お客様の銀行取引を一時的に規制しています、利用再開手続きが必要です。
https://mufgya[.]com

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

9月4日　9月29日　10月22日　11月28



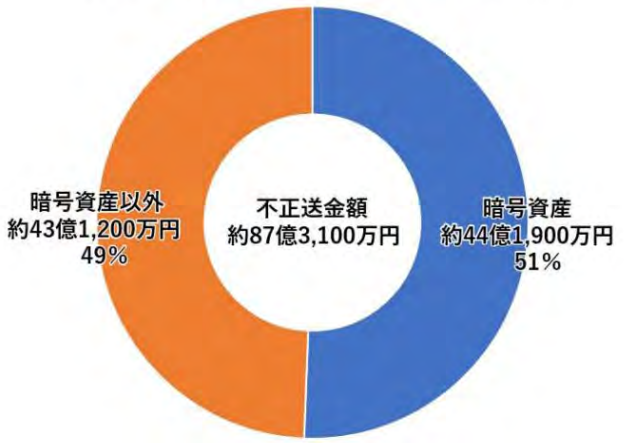
（注意）
KeepSpyのSMSの送付先は、ターゲットやメッセージと符合する地域で発行された携帯電話番号であり、緻密な準備の上で行われていることが類推できる。



不正送金が「暗号資産」に流入している（暗号資産PJにおいて調査継続中）

■ 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

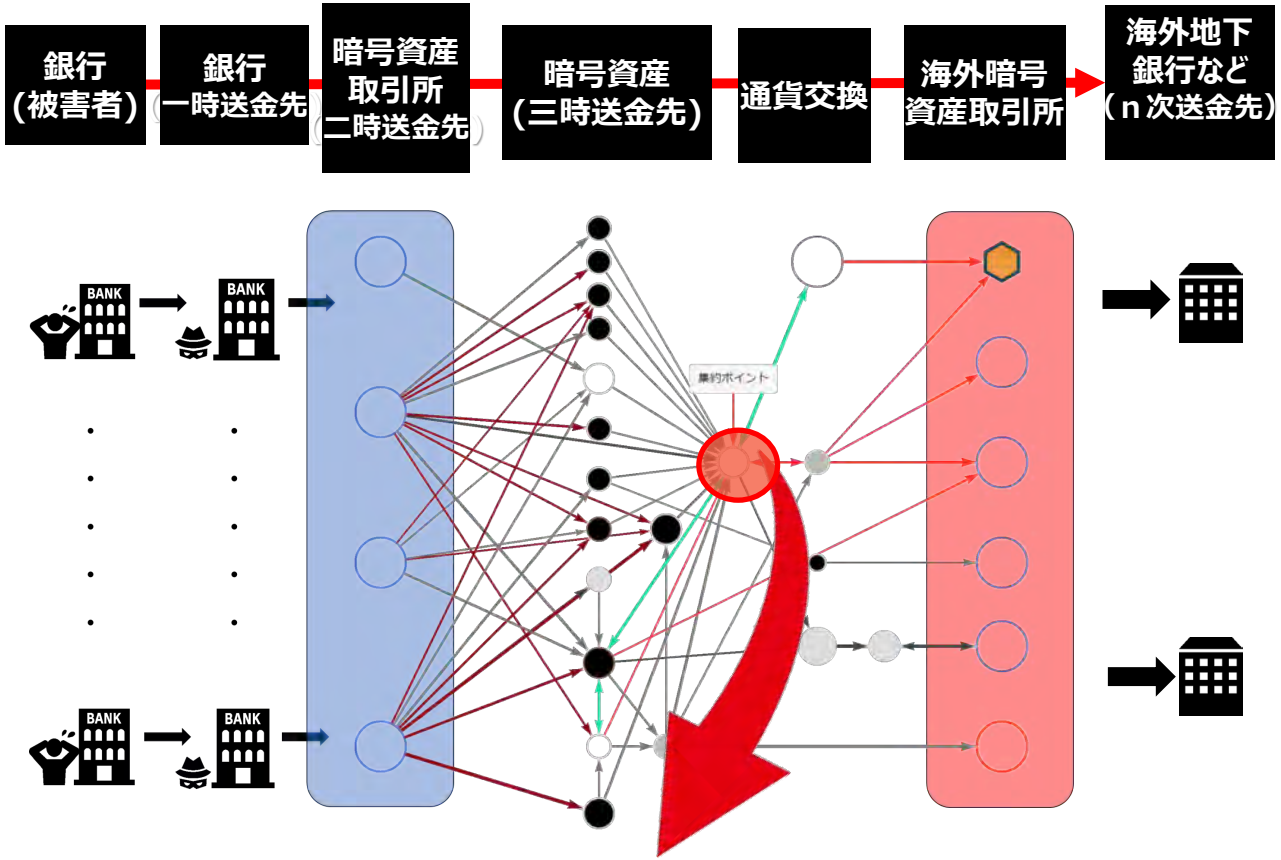
【図表13：暗号資産交換業者の金融機関口座への送金状況】



2024年上半期は、暗号資産交換業者への送金割合が約27%に減少。
金融機関による異名送金への対応の効果か？

■ 暗号資産における不正送金の流れ

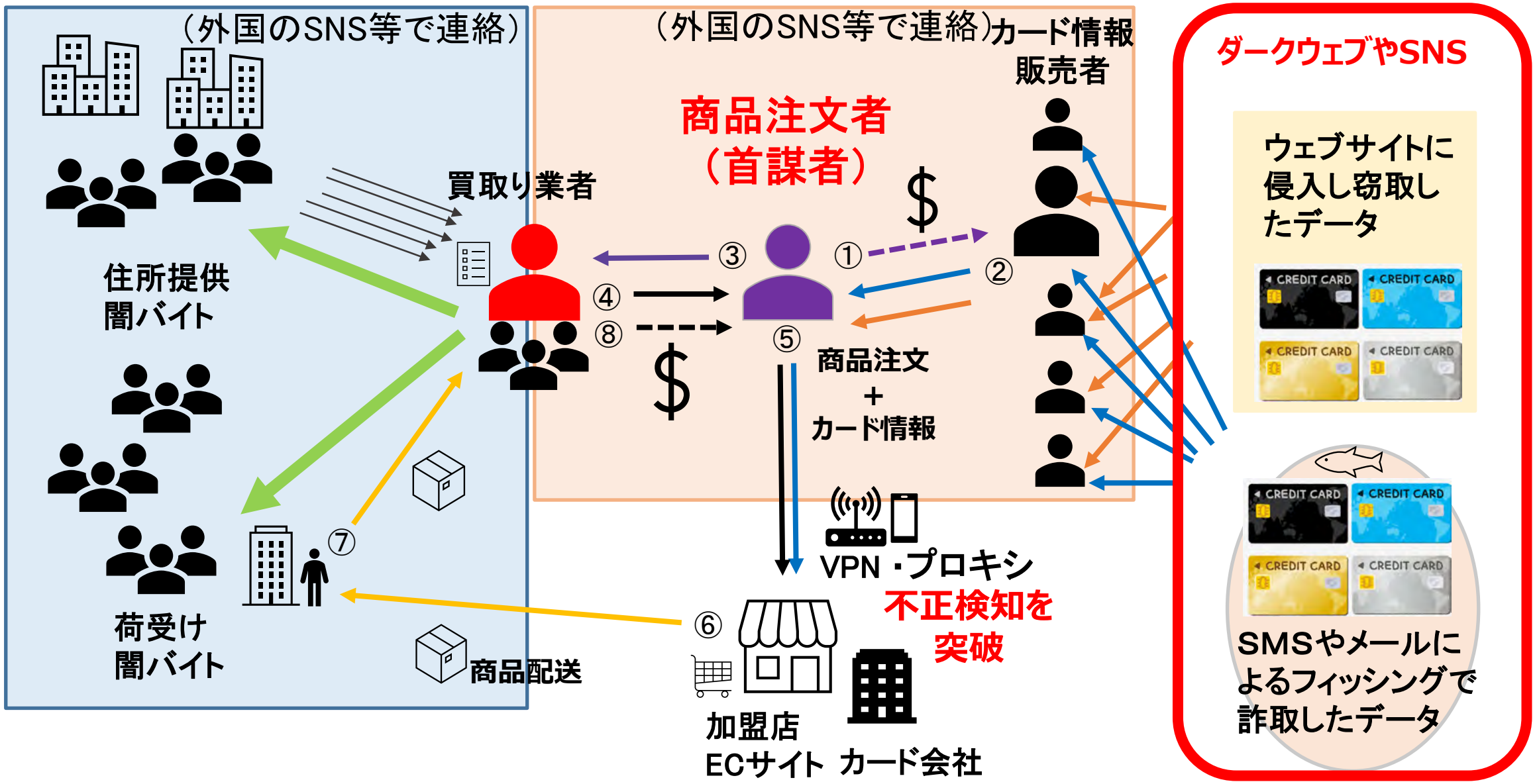
（流れがすべて記録に残っているのが特徴です）



※　提供データを元に研究した結果、集約される場所では、

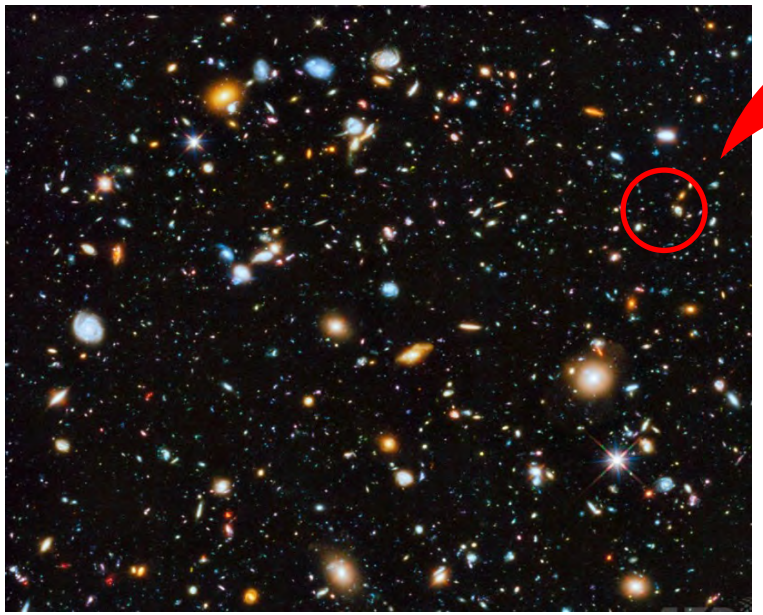
十億円単位の暗号資産が動いていることが多い

クレジットカード情報を悪用した詐欺事案の背景（例）



日本を狙う不正取引コミュニティを知るためにSNSを覗いてみると

テレグラムユーザー約10億アカウント



例えば、中国語で書かれた日本を狙った
犯罪関連サイトは、約50万アカウント存在

不正ツール　不正教材

大量メールアドレス　大量送信メーラー

プロキシ　ドメイン　サーバ構築

パネル　メールの内容　トレンド情報

安全性の低いクレカ会社　ECサイト

３D回避　アカウント代行

商品買取り　配送先リスト

地下銀行業者

クレカや銀行の
個人情報販売アカウント

フィッシングキットの販売アカウント

テレグラムの特徴

- **匿名性が高いメッセンジャーアプリ**
- **スラング多用**
- **チャット機能（チャンネル、グループ、1対1）**
- **グループが多い**
- **1グループの登録者の数（5万人以上のグループもある）**

悪質・組織的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

警察等による徹底した犯罪捜査と摘発 **＋国際的な働きかけ**

ボランティアを巻き込んだテイクダウンの推進に向けて

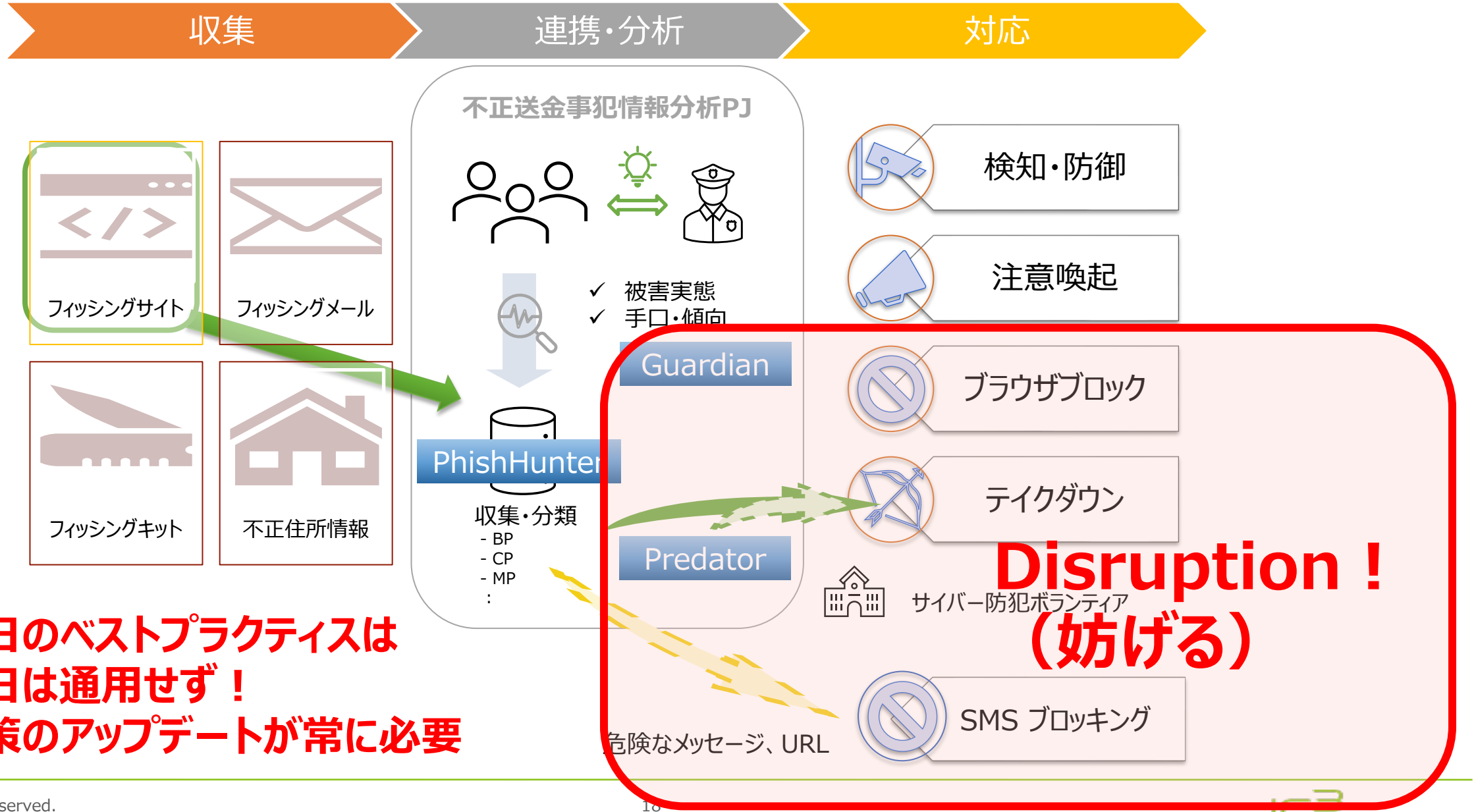
2023/12/21
ボランティアに対する講習

各県警のサイバー防犯ボランティア等がフィッシングサイト撲滅のために
JC3の支援ツール「Predator」を活用して
テイクダウンを競い合う「チャレンジカップ」を開催！

第二回フィッシングサイト撲滅チャレンジカップ

- 大会期間　令和6年7月22日 ～ 29日
- 参加ボランティア団体　359名、46団体（125名、27団体）
  特別参加団体：Gftd Japan株式会社様
- ドメイン事業者　Abuse報告数・・　9,837件(5,464件)
  テイクダウン数・・　2,004件(264件)
- ホスティング事業者　Abuse報告数・・　2,235件(3,855件)
  テイクダウン数・・　197件(4件)
- 合計　Abuse報告数・・ 12,072件(9,319件)
  テイクダウン数・・ 2,201件(268件)　※()は前回

JC3のフィッシング対策への取組み



今日のベストプラクティスは
明日は通用せず！
対策のアップデートが常に必要

ランサムウェア攻撃の特徴　報告件数の推移、規模や業種

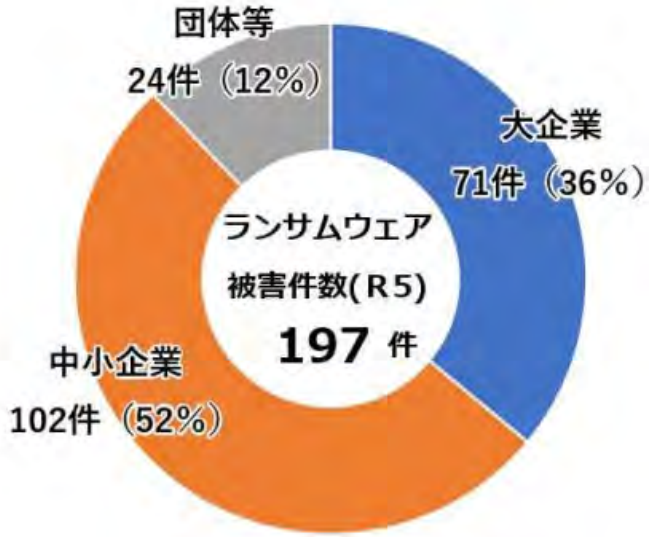
警察庁「令和５年におけるサイバー空間をめぐる脅威の情勢等について」 及び　警察庁実施のアンケート等より

- 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、約半数が被害を公表（JC3調べ）、警察への届け出が少ない
- ＶＰＮ機器やリモートデスクトップを利用した感染が多く、「閉域網だから安心」はあり得ない

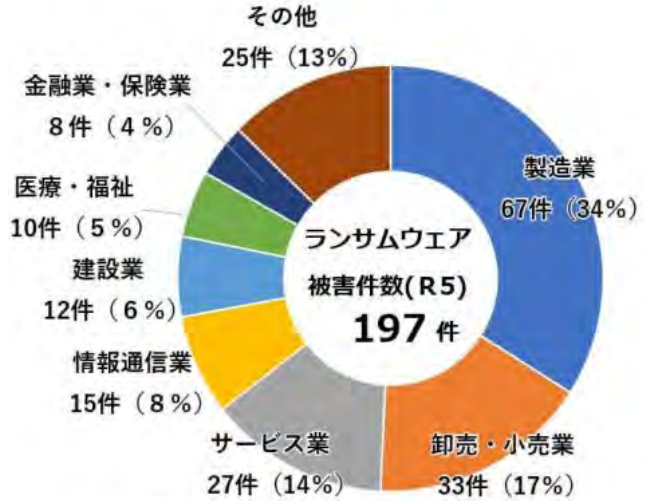
報告件数の推移

※　ノーウェアランサム：暗号化することなくデータを窃取した上で、対価を要求する手口。令和５年上半期から集計。

業種規模別



業種別

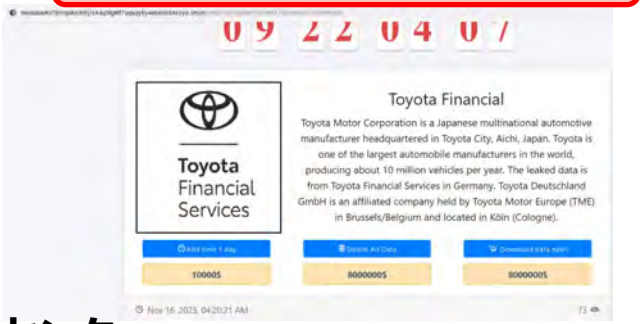


注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

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

ランサムウェア攻撃の手法（イメージ）

閉鎖系（クローズドネットワーク）でも
外部とつながっていないシステムはありません。

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）

⑧ データの収集・持ち出し

被害法人内ネットワーク

⑦ 横展開

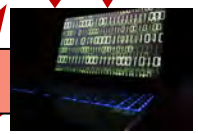
③ 永続化
④ 権限の昇格
⑤ 防御の回避

⑥ 認証情報へのアクセス
⑦ 横展開

Active Directory
サーバ

⑨ ランサムウェアの展開

⑨ ランサムウェアの展開



感染起点
（端末A）

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

凡例
侵入・感染の流れ
データ窃取の流れ

ランサムウェア攻撃に対する国際共同捜査

警察庁は、2024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。この操作においては、日本警察も捜査で得られた情報を提供したほか暗号化された被害データを復号するツールを開発・提供した。

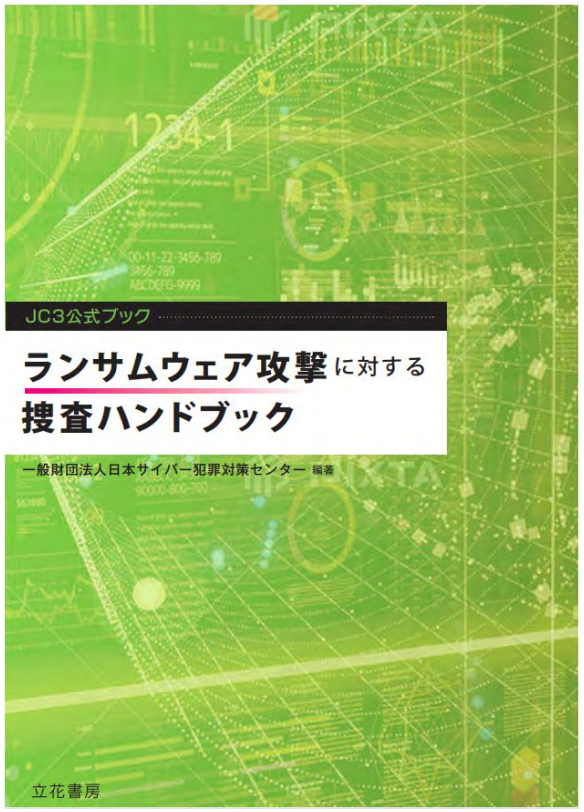
また、2024年11月、米国内の企業や政府機関等に対し被害を与えたランサムウェア攻撃グループ「Phobos」に係る被疑者を検挙した旨を米国司法省がプレスリリースしたが、その中で米国連邦捜査局（FBI）が行った捜査において日本警察を含む各国法執行機関が協力した旨が言及されている。

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。

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

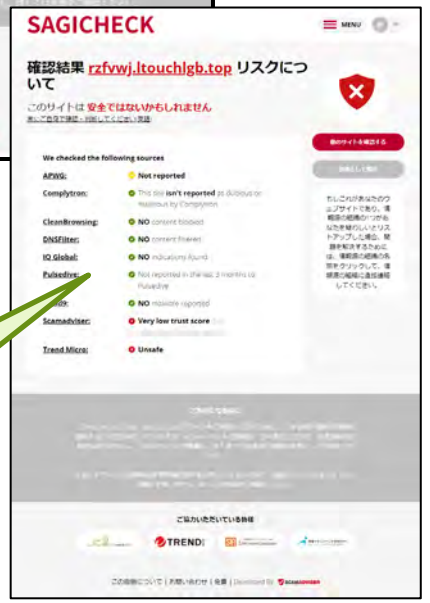
注意喚起

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/

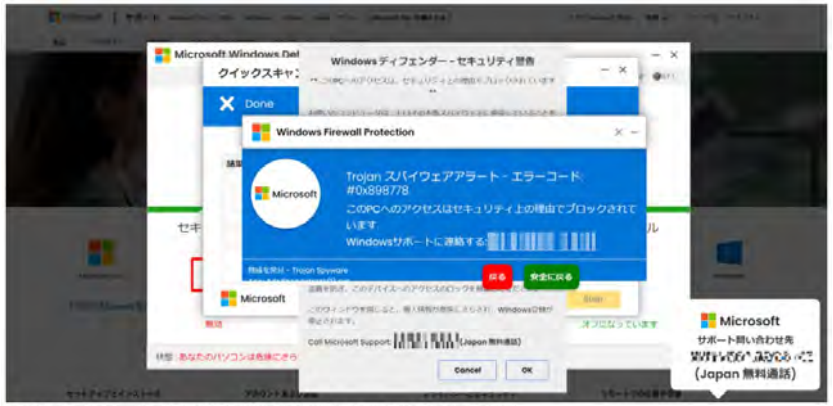


結果が表示される

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　～　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OOOOOOO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！

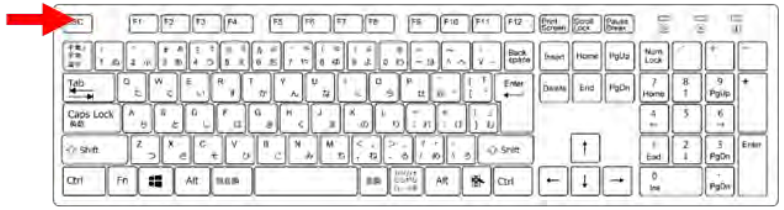
https://www.lac.co.jp/lacwatch/pdf/20230302_cgjournal_vol15.pdf

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。。

電話をかけるとどうなるかを知って、決して「電話をかけない」ことを広げましょう。

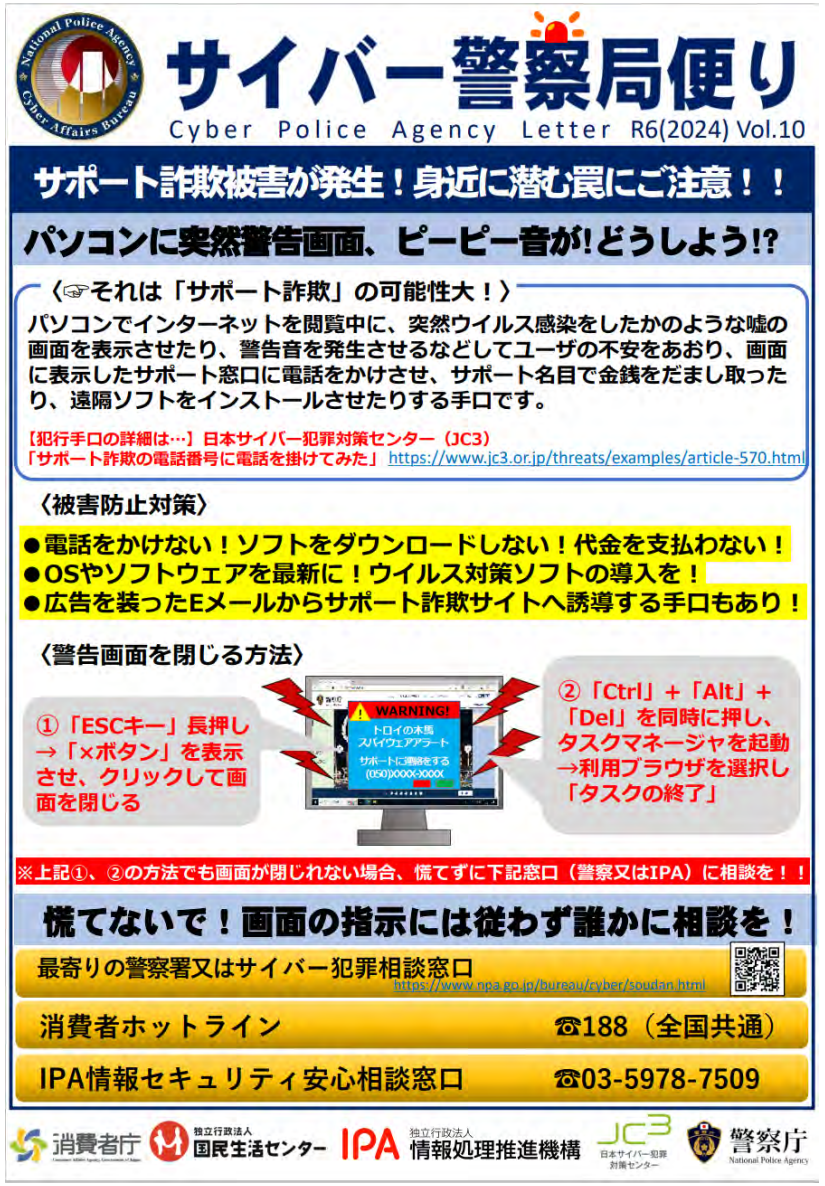
https://www.jc3.or.jp/threats/examples/article-570.html

令和５年

テクニカル サポート詐欺 調査

電話をかけてしまった場合に何が起こるのか

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



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

Digital Crime Consortium 2024@Tokyoで発表

松ヶ谷さん（トレンドマイクロ）、 影山さん（ラック）

『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

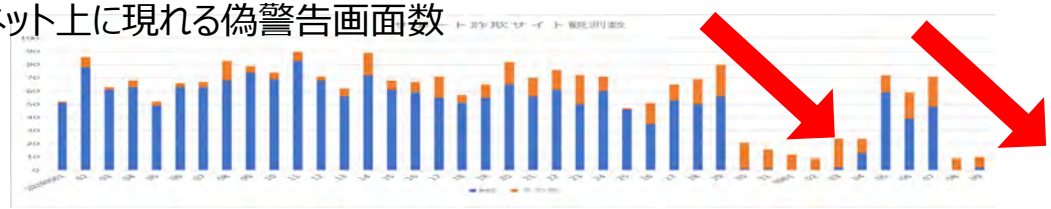
「偽」被害電話によって得られた犯罪プロファイリング』

DCUとの協働テイクダウンへ！

JC３で収集したデータをDCUに提供し、

テイクダウンを継続中

ネット上に現れる偽警告画面数



[Microsoft デジタル防衛レポート 2024](#) から

【仮訳】

マイクロソフトのデジタル犯罪対策ユニットの取組「Microsoft Digital Crimes Unit」は、先駆的な法的戦略、最先端のテクノロジー、そして消費者への脅威に対抗するための連携を活用し、金銭的利益を目的としたサイバー犯罪と闘っています。

また、マイクロソフトは、サイバー犯罪者の活動基盤を積極的に解体し、彼らの金銭的な動機を妨害し、米国のNCFTAや**日本サイバー犯罪対策センター**などの組織と提携して実用的な情報の共有を強化することで、サイバー犯罪者を弱体化させる取り組みも行っています。

世界中でサイバー犯罪の脅威が認識される中、犯罪インフラを破壊し、犯罪者を法的に責任を問う立場に立たせ、サイバー犯罪の被害者を支援するために、官民のパートナーが力を合わせる動きが活発化しています。

※　現在は、AWSにも提供中！

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（Microsoft Copilotで作成した表です）

グループ名	国	主な攻撃対象
APT1（Comment Crew）	中国	商業機密や知的財産
APT2	中国	不明
APT3（Buckeye）	中国	政府機関、軍事機関
APT4（Maverick Panda）	中国	政府機関、軍事機関
APT10（Red Apollo）	中国	政府機関、商業機密
APT12（Numbered Panda）	中国	政府機関、商業機密
APT15（ニッケル）	中国	政府機関、軍事機関
APT17（Tailgator Team）	中国	政府機関、商業機密
APT18（Wekby）	中国	政府機関、商業機密
APT28（Fancy Bear）	ロシア	政府機関、軍事機関、メディア
APT29（Cozy Bear）	ロシア	政府機関、外交機関
Sandworm（APT44）	ロシア	政府機関、エネルギー分野、選挙関連
APT32（OceanLotus）	ベトナム	政治的および経済的情報
APT33（Elfin Team）	イラン	政府機関、エネルギー分野
APT34（OilRig）	イラン	政府機関、エネルギー分野
APT35（Charming Kitten）	イラン	政府機関、学術機関
APT38（Lazarus）	北朝鮮	金融機関
APT40	中国	政府機関、企業、大学（バイオメディカル、ロボティクス、海洋研究など）
APT41	中国	商業スパイ活動、金融詐欺
Turla	ロシア	政府機関、軍事機関
FIN7	不明（ロシア？）	金融詐欺、クレジットカード情報
Cobalt Group	不明（ロシア？）	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。

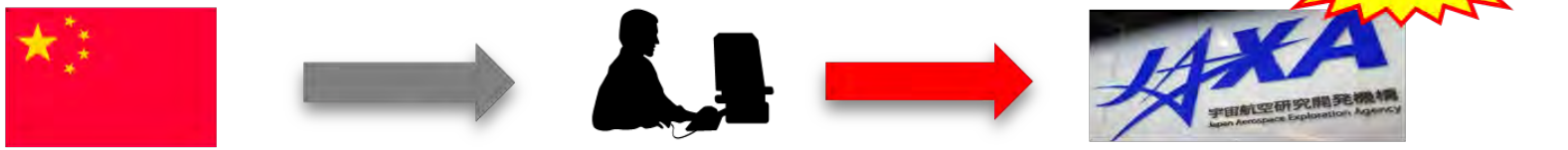
我が国に対するAPTグループによるサイバー攻撃（警察による摘発･公表）

■ **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

欧米等で既に発生しているサイバー犯罪や攻撃

欧米で顕在化しているサイバー犯罪で今後我が国で多発する懸念があるものは、「法人を狙う金融犯罪」。一度に多額の被害を発生させるこの種犯罪では、生成AI等によって偽造された文章、声、ディープフェイク、文書等を使うなど極めて計画的で巧妙な手口が見られ、被害者側の情報を十分に入手した上で攻撃、詐欺等が行われている。　すでに我が国でも、銀行員を騙り「フィッシングサイトに誘導するQRコード記載のFAXやメール後、電話連絡がくる事例」や「電話連絡後、フィッシングメールが送られてくる事例」が発生しており、今後その手口や規模がさらに大きく変わる可能性も高い。（FBIからの警告：　https://www.ic3.gov/PSA/2024/PSA241203）
（参照：トレンドマイクロ　https://www.trendmicro.com/en_us/research/21/d/deepfakes-are-getting-closer-to-reality.html）

ビジネスメール詐欺（Business E-mail Compromise：BEC）

漏えいした情報や乗っ取ったメールを活用するなどの巧妙な騙しの手口を駆使し、偽の電子メールを組織・企業に送り付け、従業員を騙して攻撃者の用意した口座へ送金させる詐欺犯罪。金融機関や法律事務所など多額の資産を取り扱う企業が徹底的に狙われている。（参照：IPA　https://www.ipa.go.jp/security/bec/index.html）

ディープフェイクによるビデオ会議等による詐欺

香港にある多国籍企業に勤務する会計担当者が、ビデオ会議で最高財務責任者CFOを装った相手に騙されて、約３８億円を詐欺グループに送金する事件が発生。出席者全員が公開されていた画像や動画をもとにディープフェイクで作り出された偽画像であったとのこと。香港ではその後も生成AIで作成した架空人物の画像で約70億円もの詐欺を繰り返していたグループが摘発されている。

Pig Butchering Scam（養豚式投資詐欺、豚の屠殺詐欺）

比較的長期間をかけて偽りの信頼関係を築いた上で、高額な見返りの約束を餌とするなどの投資話を持ち掛けて多くの資金を被害者から吸い上げる詐欺の手口。我が国で被害が急増しているマッチングアプリ等におけるロマンス詐欺、SNS投資詐欺もこの一種。

ロシアのランサムウェア組織の裏側で暗躍する英語圏のScattered Spiderグループ

標的企業のITサポート窓口を騙って、CFO等の役員アカウントの多要素認証をリセットし、組織に侵入する手法のほか、ソーシャル・エンジニアリング、フィッシング、SIMスワッピングなど、企業ネットワークに侵入するために様々な手口を使う詐欺グループ。ロシア語圏のランサムウェアグループからの依頼も請け負っており、国境を越えた連携も見られる。

盗まれたクレジットカードで決済を行う検知が困難な新戦術 「Ghost Tap」

欧米では、NFCトラフィックのリレーによりモバイルウォレットに紐づいたクレジットカードから決済する犯罪が多発している。決済は正規のユーザー端末から行われているように見えるため、従来の不正検知メカニズムには引っかからず、購入する商品が安価で疑念を生みにくい上、購入場所は離れた複数箇所で実施されると追跡や特定は困難となる。

＜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ことを認識。

■例えば、、、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を確認」 犯罪に応用！

「ChatGPTは、犯罪の準備プロセスを加速」 犯罪の手口や新しいツールを教える！

「より高度な犯罪者には、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」 手口を高度化・自動化！

「AIによる会話型チャットボットとリアルなディープフェイクなどが、今後の犯罪手法に」 AIが巧妙に人をだます！

■AIが作成したフィッシングメールが非常に高い効果を持つことが明らかに

2025年1月、ベルリン工科大学、ハーバード大学等の研究者らによる研究が発表され、AIが作成したフィッシングメールは人間のエキスパートと同じく54%の人を騙すことが判明し、一方、メール1通を作成するのに、AIは約2分41秒と人間のエキスパートの時間にして13分の1、コスト面でも50分の1に抑えられたとの結果が発表された。

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を持った政府機関と、広範な能力を持った企業等の役割

警察、自衛隊を含めた中央省庁、自治体、セキュリティ事業者、システム提供事業者、通信事業者、学校、そして**金融機関**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 ⇒**サイバー対処能力強化法案等に期待**

【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

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、官民学の違いを超えた「共助」の場で、
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）

他の企業との情報共有に加え、犯罪捜査を行う警察機関との協力を通じ、犯人検挙に協力しつつ、捜査結果からしか得られない、犯罪者側の事情（組織構成、犯行手口・ツール、事後的な収益化等）を知ることで犯罪抑止のヒントが見える可能性が高まる。

→ 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

◆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

【最後に】 今後の課題　企業に何が求められるのか

◆ 敵（犯人）、そして犯罪の具体的な手口を知る努力（自助と共助）。

◆ 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。

◆ セキュリティ担当部門だけでなく、サービス・商品所管部門が業務提供前から犯罪をさせにくい仕組みを作ることで「守る」。

◆ 被害が潜在化しやすいサイバー犯罪や攻撃については、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。 ⇐ 警察への通報・相談が社会を変える！

◆ 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。

◆ 企業本体及びそのビジネスを守るために、積極的なリーダーシップの発揮と必要なサイバー領域における**システム・人材への積極的な投資**を求めたい。

ありがとうございました。

JC3
Japan Cybercrime Control Center