令　和　6　年　3　月　8　日
サイバーセキュリティシンポジウム道後

デジタル社会における
サイバー空間の脅威への対応

警　察　庁　サ　イ　バ　ー　警　察　局
サ　イ　バ　ー　企　画　課　　課　長　補　佐
佐　々　木　彩　乃

目次

目次

我が国を取り巻く情勢

- デジタル社会の到来に伴い、サイバー空間の公共空間化が加速
- 絶えず地政学的緊張にさらされるなど、厳しい安全保障環境の中にいる
- 先端技術、知的財産等を有する企業等が国内に多く存在
- 日本国際博覧会等の社会の耳目を集める行事開催を控えている

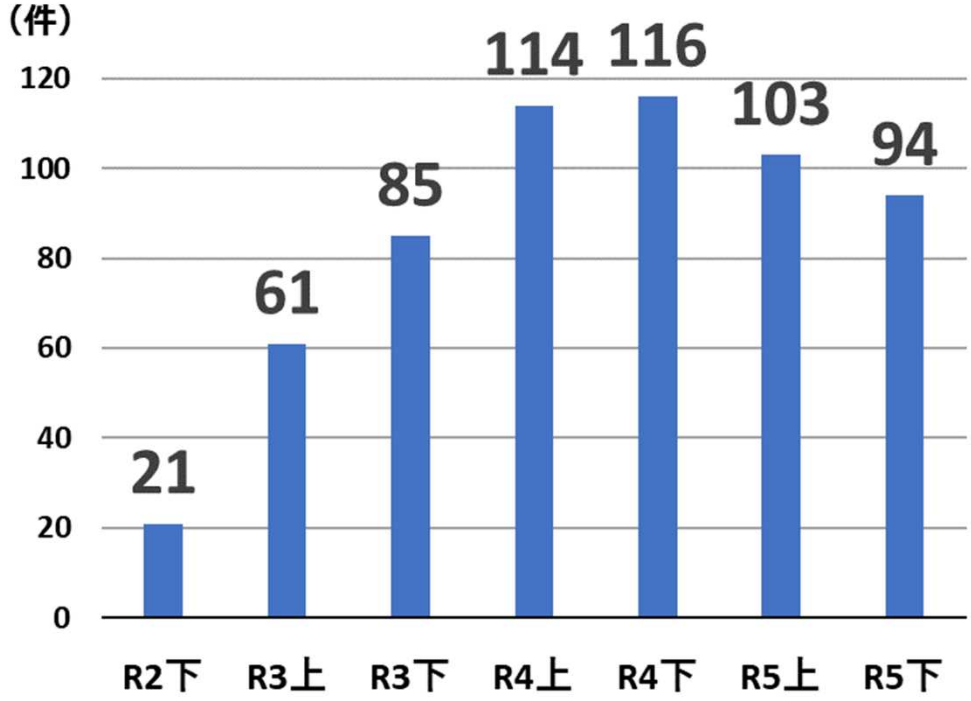
サイバー空間における脅威については
極めて深刻な情勢が継続

ランサムウェア攻撃情勢（１）

- ランサムウェア被害は依然として高い水準で推移
- 企業の規模を問わず被害が発生

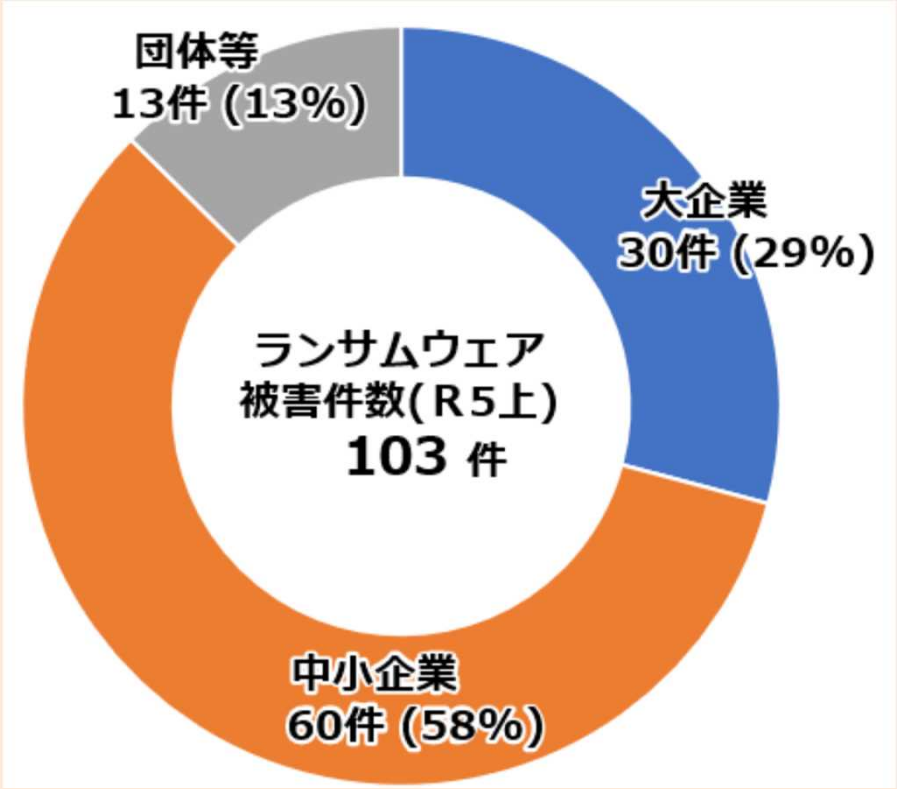
都道府県警察へ被害申告がなされた件数とその内訳

ランサムウェア被害の報告件数の推移



出典　警察庁　「令和５年の犯罪情勢」

被害企業・団体等の規模別報告件数（R5上）

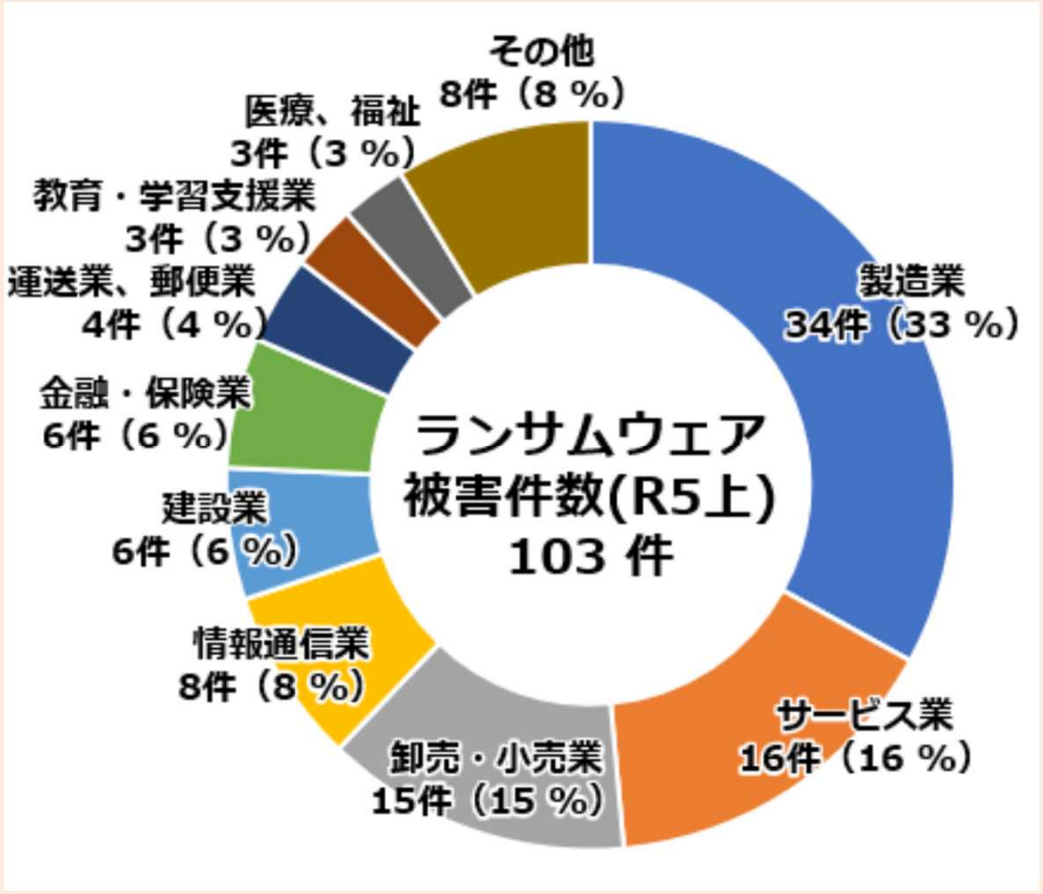


出典　警察庁　「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」

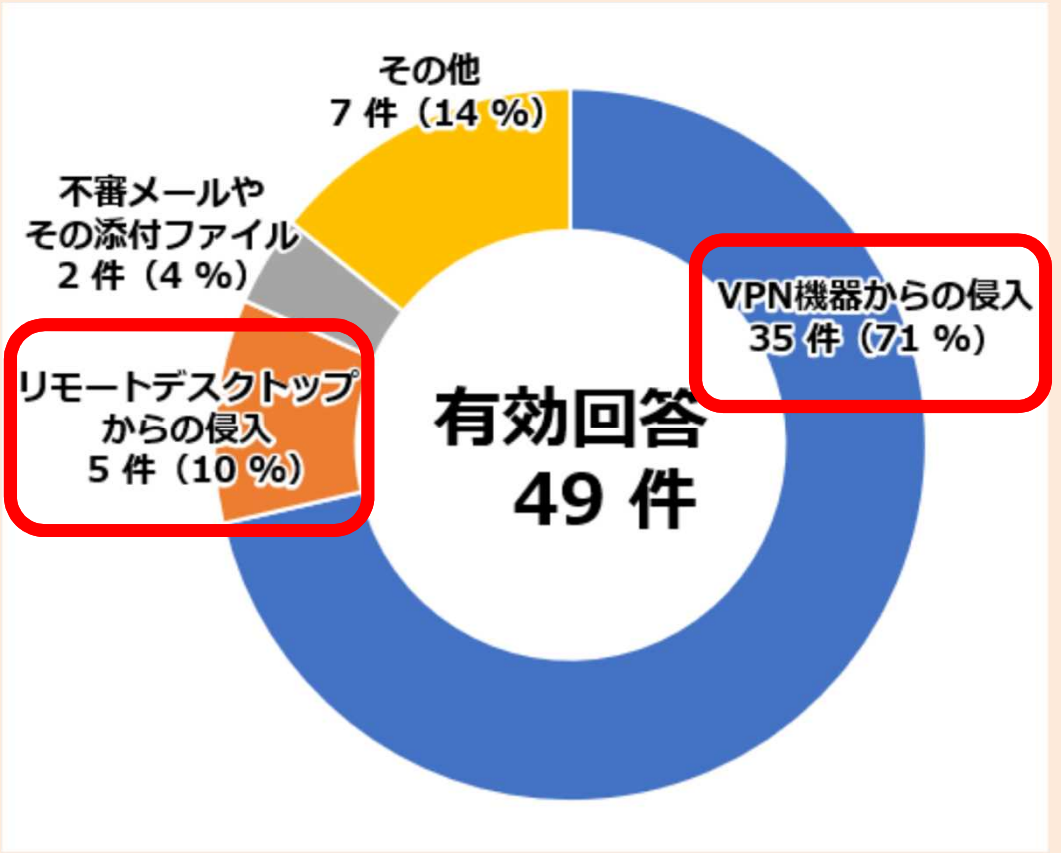
ランサムウェア攻撃情勢（２）

- 業種を問わず被害が発生
- ＶＰＮ機器、リモートデスクトップを利用した感染を多数確認

業種別の報告件数（R5上）



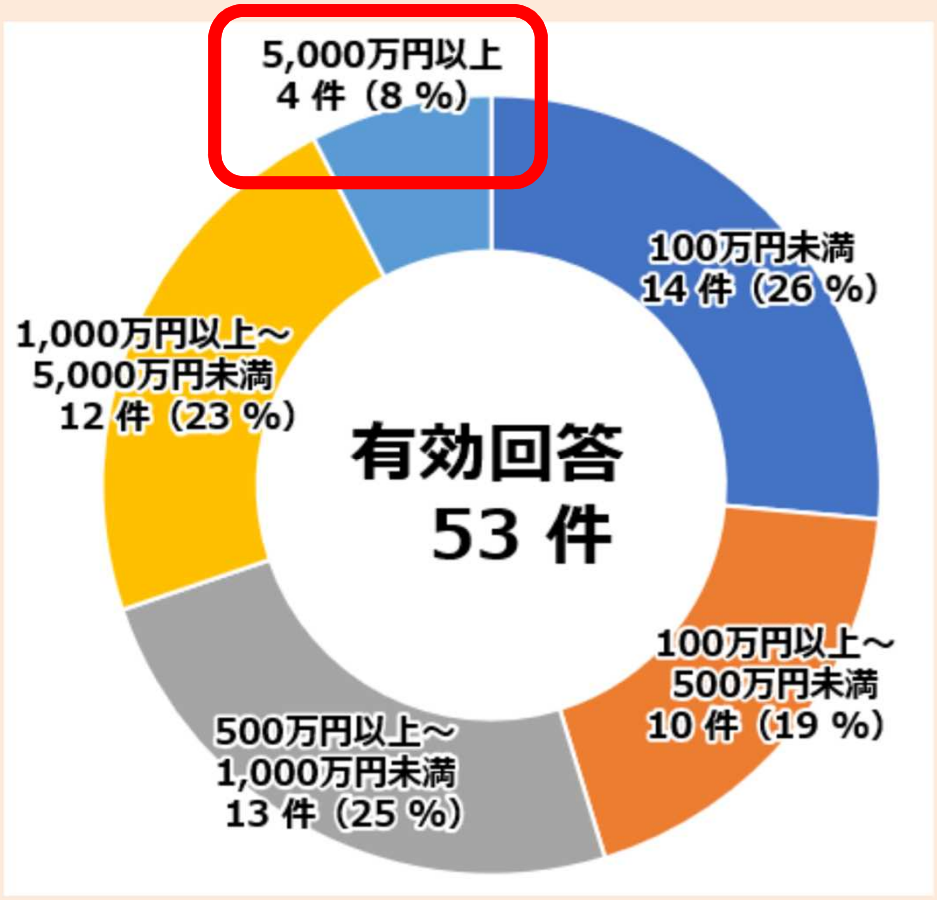
感染経路別の報告件数（R5上）



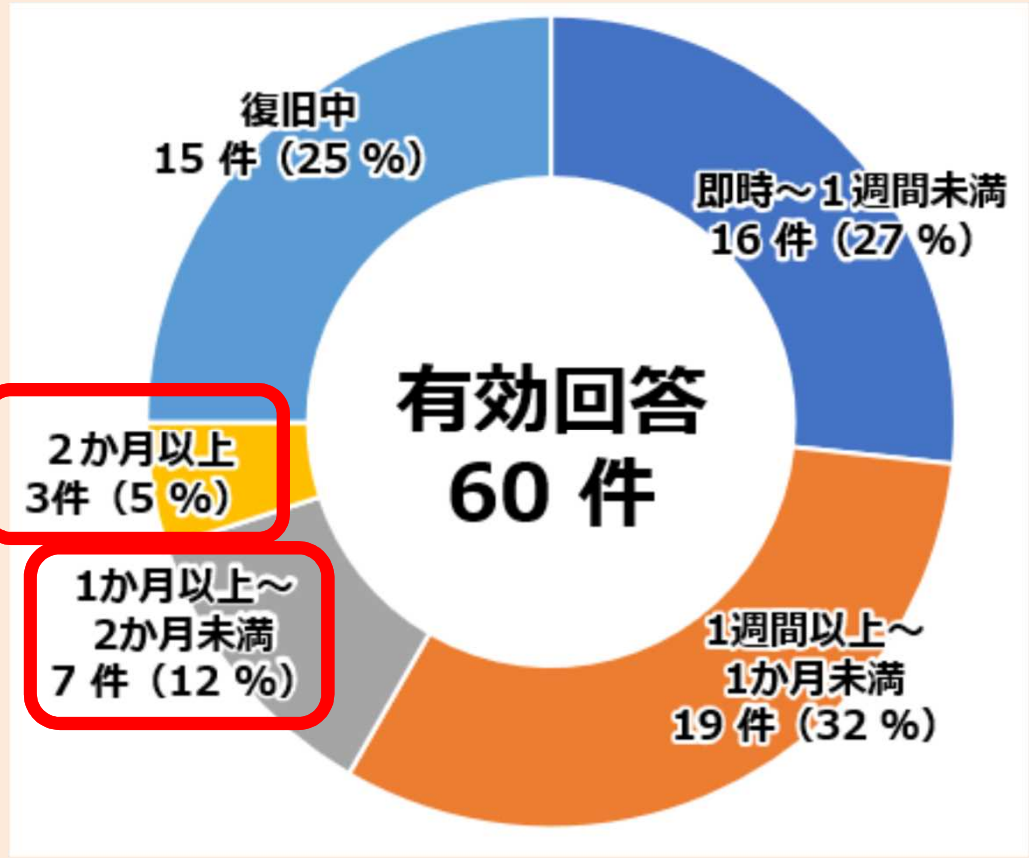
ランサムウェア攻撃情勢（３）

- 調査・復旧に5000万円以上の費用を要した場合が8%
- 復旧までに１か月以上を要したものが17%

調査・復旧費用の総額（R5上）



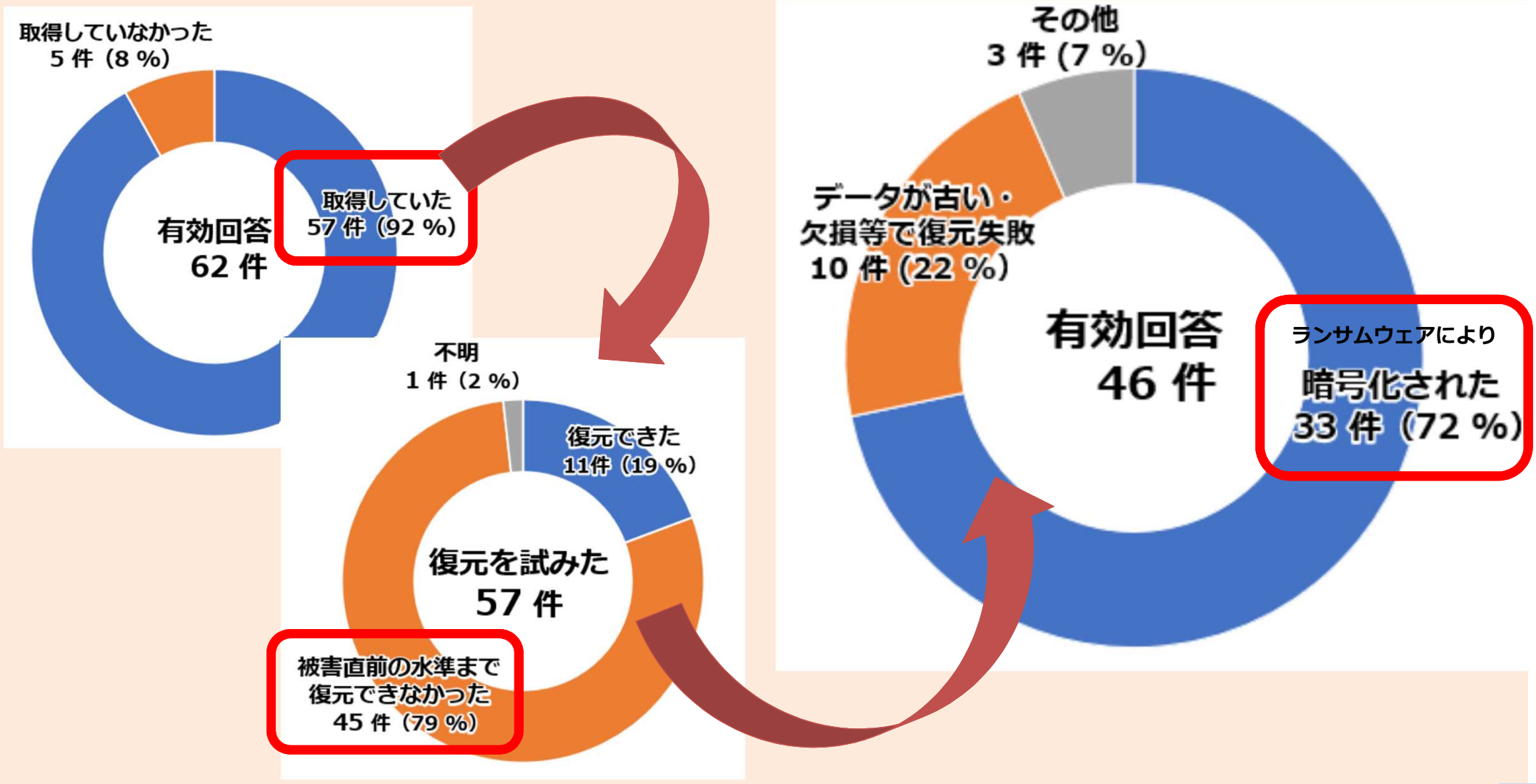
復旧に要した期間（R5上）



ランサムウェア攻撃情勢（４）

■ 多くの組織ではバックアップを取得しているものの、バックアップも影響を受け復元できない場合もある

バックアップの取得・活用状況（R5上）



サイバーインテリジェンスの情勢（１）

- 情報を電子データの形で保有することが一般的となっている中で、先端技術、研究等の機密情報の窃取を目的としたサイバーインテリジェンスの脅威が継続

- 現実空間でのテロの準備行為として、重要インフラ事業者等※の警備体制といった機密情報の窃取のためサイバーインテリジェンスが行われる可能性

※情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット及び石油の14分野

（攻撃手口の例）

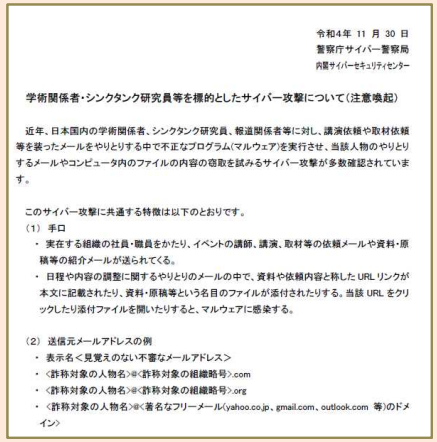
- **標的型メール攻撃**

学術関係者、シンクタンク研究員、報道関係者等に対し、講演依頼や取材依頼等を装った標的型メール攻撃を確認

- **ぜい弱性を悪用した攻撃**

- **海外拠点等からの侵入** ⇒次ページ

注意喚起文の一部



令和4年 11 月 30 日
警察庁サイバー警察局
内閣サイバーセキュリティセンター

学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）

近年、日本国内の学術関係者、シンクタンク研究員、報道関係者等に対し、講演依頼や取材依頼等を装ったメールをやりとりする中で不正なプログラム（マルウェア）を実行させ、当該人物のやりとりするメールやコンピュータ内のファイルの内容の窃取を試みるサイバー攻撃が多数確認されています。

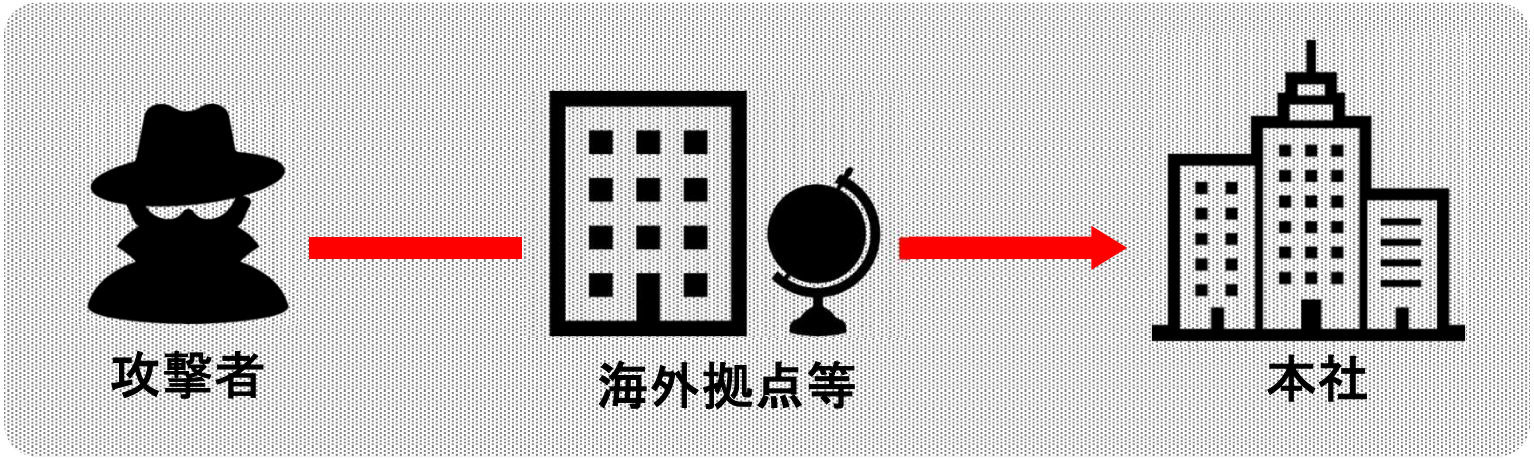
このサイバー攻撃に共通する特徴は以下のとおりです。
（1） 手口
・ 実在する組織の社員・職員をかたり、イベントの講師、講演、取材等の依頼メールや資料・原稿等の紹介メールが送られてくる。
・ 日程や内容の調整に関するやりとりのメールの中で、資料や依頼内容と称したURLリンクが本文に記載されたり、資料・原稿等という名目のファイルが添付されたりする。当該URLをクリックしたり添付ファイルを開いたりすると、マルウェアに感染する。

（2） 送信元メールアドレスの例
・ 表示名＜見覚えのない不審なメールアドレス＞
・ ＜詐称対象の人物名＞@＜詐称対象の組織略号＞.com
・ ＜詐称対象の人物名＞@＜詐称対象の組織略号＞.org
・ ＜詐称対象の人物名＞@＜著名なフリーメール（yahoo.co.jp、gmail.com、outlook.com 等）のドメイン＞

サイバーインテリジェンスの情勢（２）

■ 海外拠点等からの侵入（サプライチェーン攻撃）

- 攻撃者は、海外の拠点や関連子会社などを標的
- セキュリティの弱い拠点から本社のシステムに侵入して攻撃



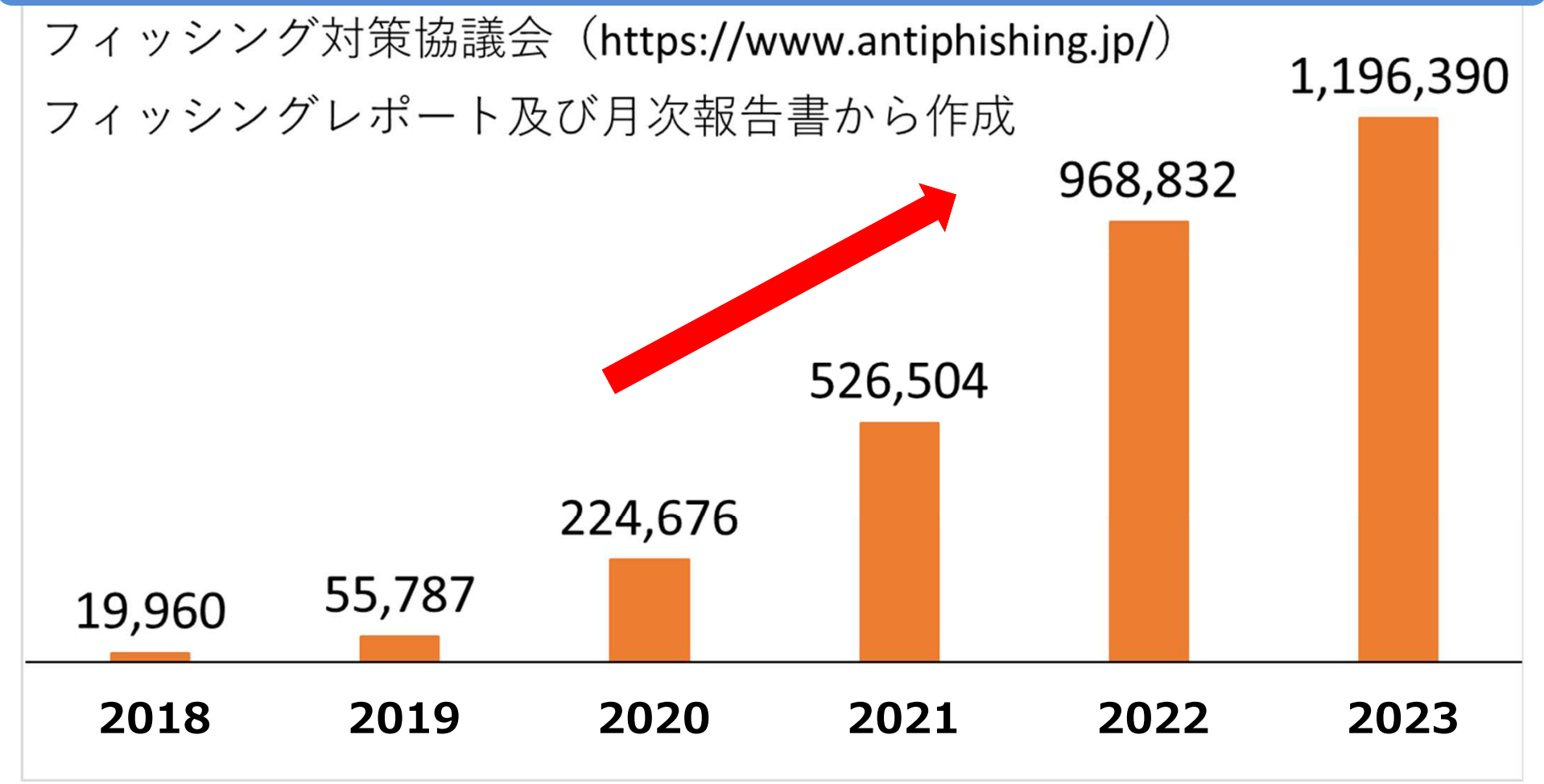
（攻撃パターンの例）

① 脆弱性を悪用し、海外拠点等のシステムに侵入
② 正規のアカウントを不正利用し、本社システムに侵入
③ 横展開・権限昇格等を繰り返し、機密情報を窃取

フィッシングの増加

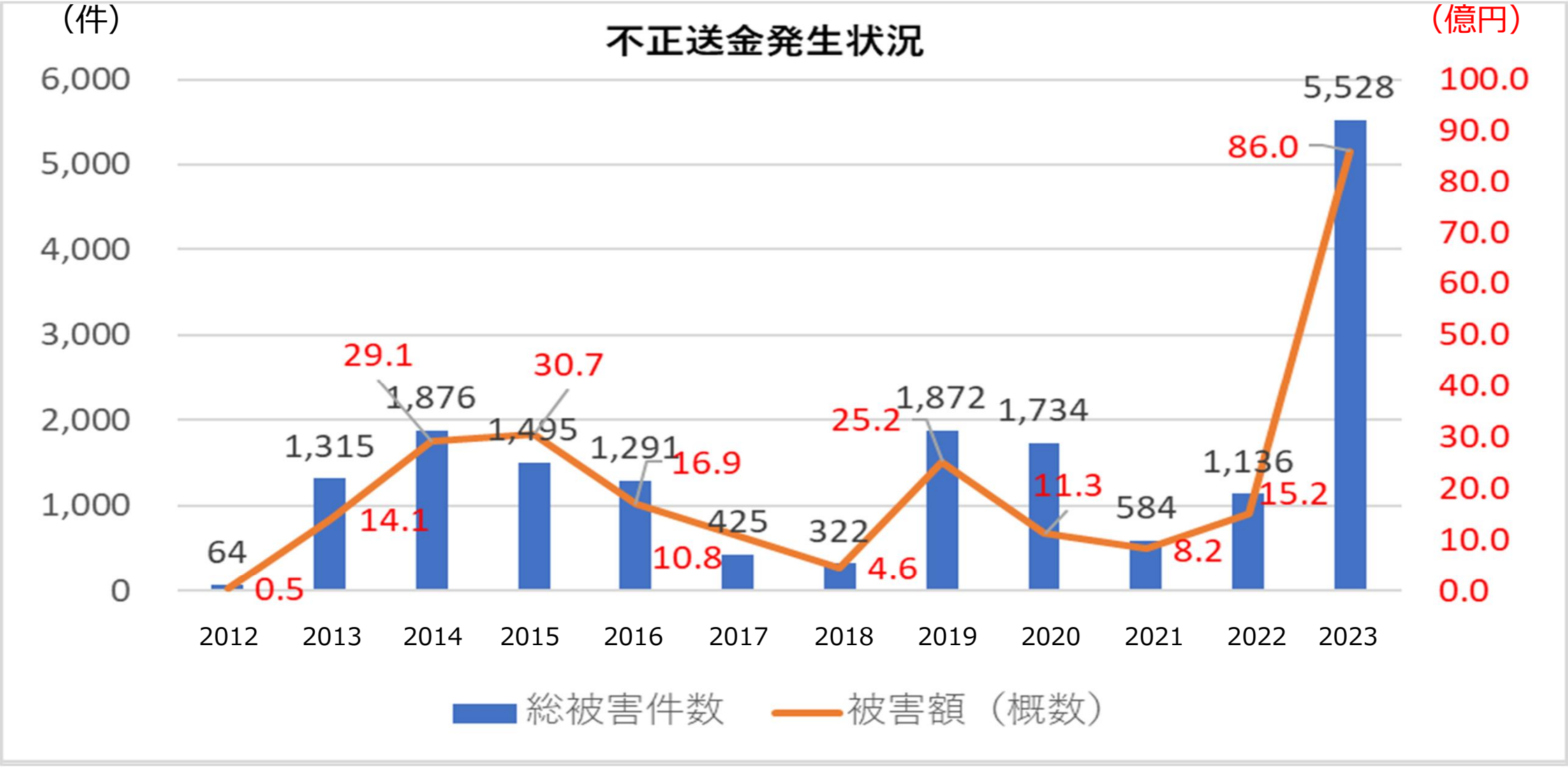
- フィッシング報告件数は右肩上がりで増加
- フィッシングで騙られた企業は、クレジットカード事業者、ＥＣ事業者を装ったものが多い

フィッシング報告件数（件）



インターネットバンキングに係る不正送金発生状況の推移

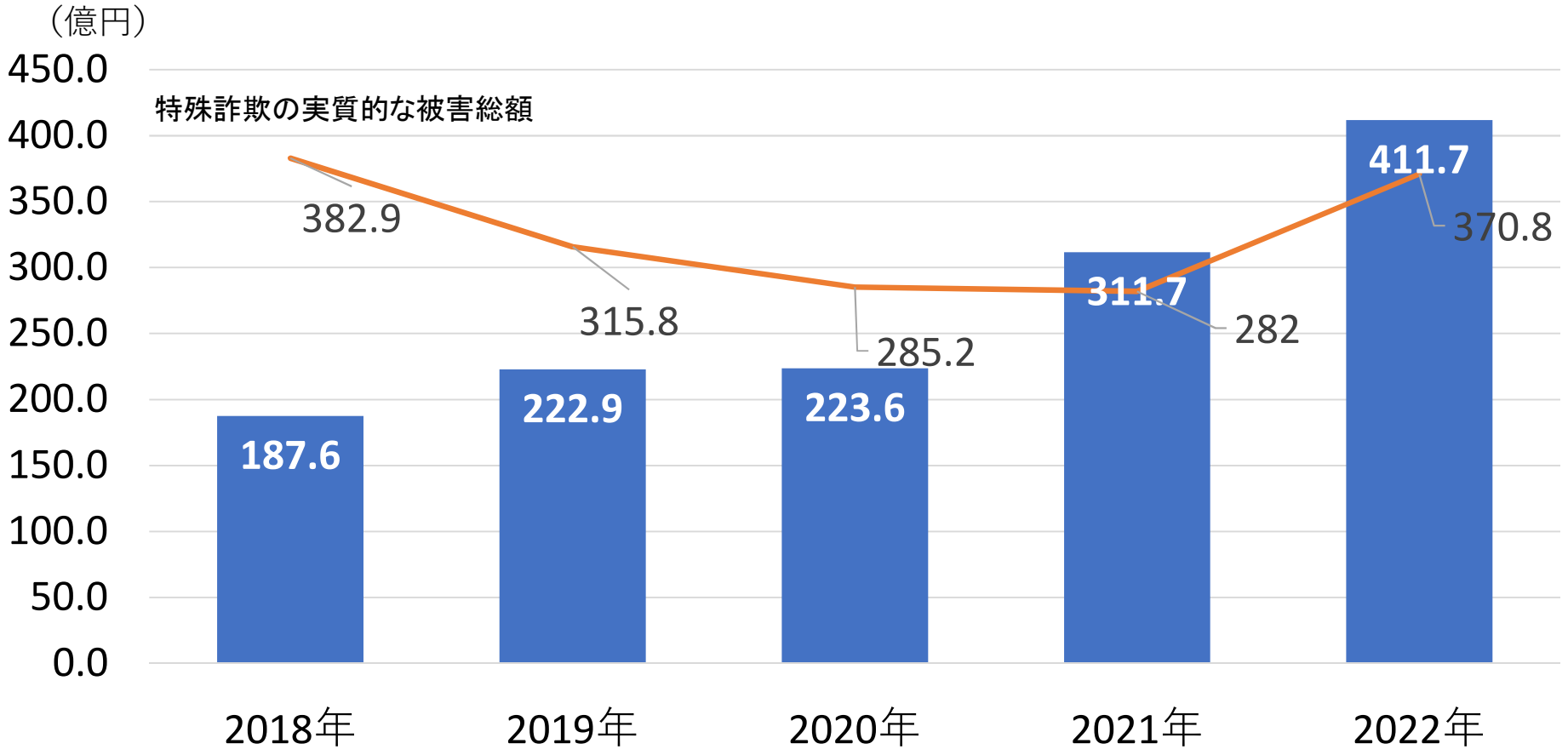
2021年以降、発生件数、被害額ともに増加傾向が続いており、2023年は、被害件数、被害総額ともに過去最多となっている。



クレジットカード不正利用の情勢

クレジットカード情報を窃取するフィッシングサイトの増加等により、クレジットカード不正利用の増加

クレジットカード不正利用（番号盗用）被害額（億円）



「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額の発生状況」
「警察庁　特殊詐欺の認知・検挙状況等について」より作成

目次

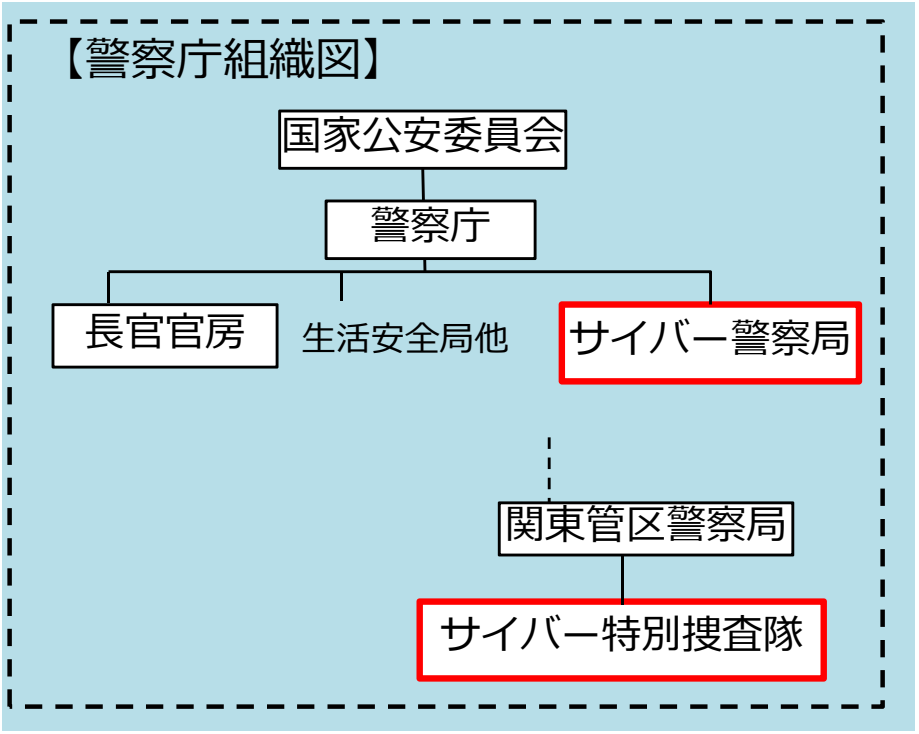
サイバー警察局・サイバー特別捜査隊

背景

- コロナ禍を契機とした社会のデジタル化と、サイバー空間の公共空間化
- 国家を背景としたサイバー攻撃の洗練化、悪質なマルウェアを用いた攻撃手法の拡散など、サイバー空間の脅威の拡大

Ⅰ　警察庁内部部局の一部を発展改組して、**サイバー警察局**を設置

Ⅱ　関東管区警察局に捜査権限の執行を行う**サイバー特別捜査隊**を設置



ランサムウェア被疑者の逮捕

国際共同捜査

ユーロポール・外国捜査機関

EUROPOL

相互協力

復号ツールの提供

サイバー警察局

National Police Agency Cyber Affairs Bureau

国の捜査機関

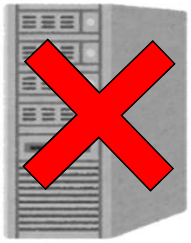
サイバー
特別捜査隊

National Police Agency National Cyber Unit

◆ 関係国捜査機関が逮捕

海外所在被疑者

◆ 関連犯罪インフラの閉鎖



サーバ等

https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-world's-biggest-ransomware-operation

フィッシング事犯被疑者の逮捕

国際共同捜査

インドネシア当局

POLRI
KEPOLISIAN NEGARA REPUBLIK INDONESIA

相互協力

サイバー警察局

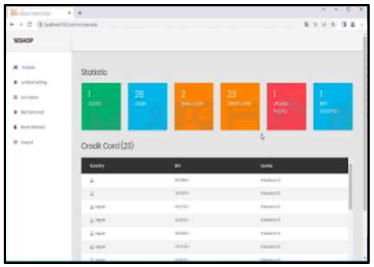
国の捜査機関

サイバー
特別捜査隊

National Police Agency
Cyber Affairs Bureau

National Police Agency
National Cyber Unit

◆ **インドネシア当局が逮捕**



フィッシングツール
「16SHOP」を悪用

捜査

大阪府警察

捜査・逮捕

海外在住被疑者

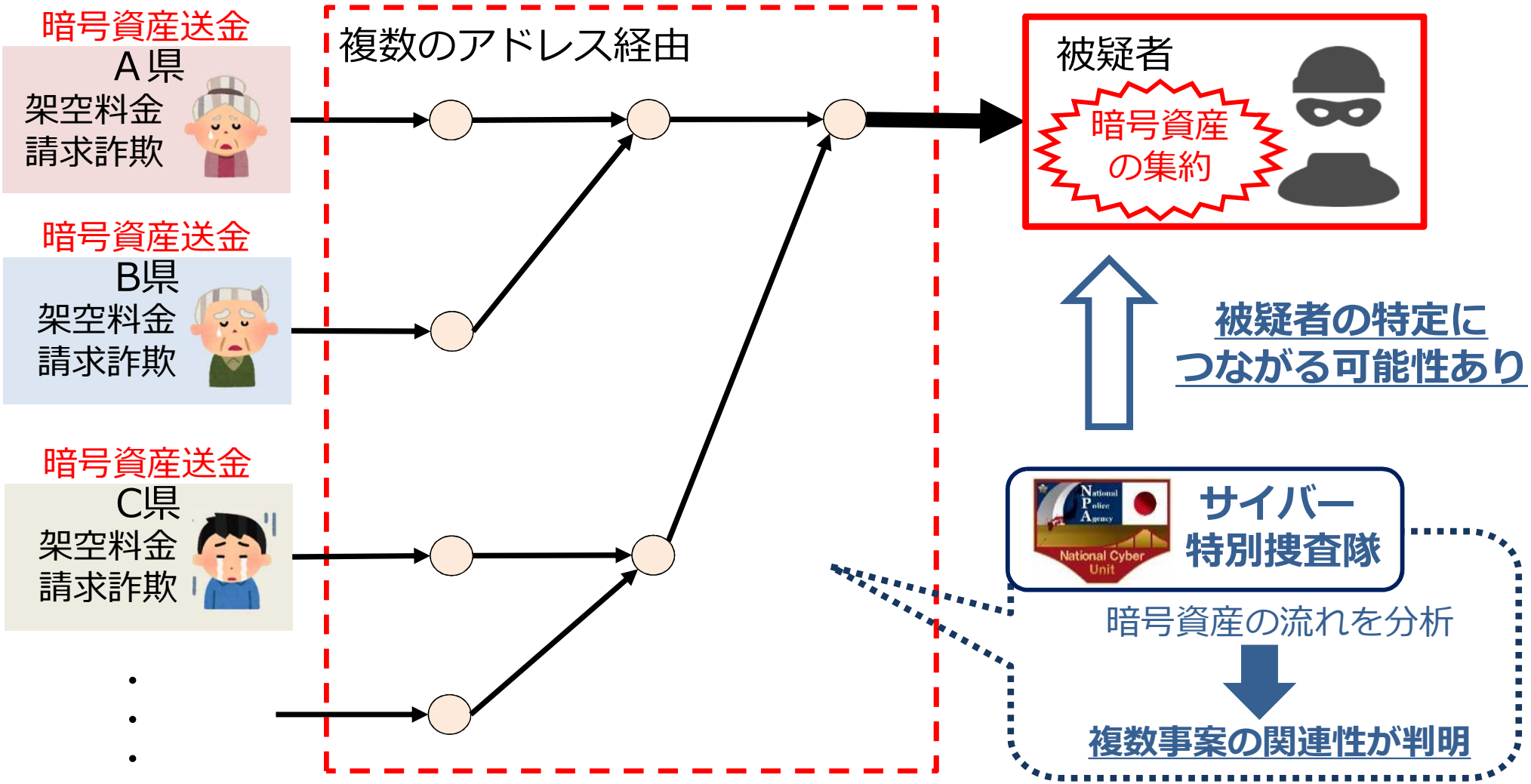
共謀

国内在住被疑者

犯罪に係る暗号資産の追跡捜査

- 暗号資産は、①利用者の匿名性が高い、②移転が瞬時に行われる、③取引所の利用に本人確認等が義務付けられていない国・地域が存在する、などの理由から、犯罪収益の移転に悪用されるケースが存在

  ⇒　犯罪に係る暗号資産の流れを追跡・分析することで複数事案の関連性が判明



パブリック・アトリビューション

捜査の結果、攻撃主体の解明にいたったものについては「パブリック・アトリビューション（※）」を実施し、サイバー攻撃を抑止

※　サイバー攻撃の攻撃者を公表し、非難することでサイバー攻撃を抑止する取組

◆ 中国を背景とするBlackTechによるサイバー攻撃 (2023.9)

BlackTechに関する日米合同注意喚起

BlackTech：
2010年頃から日本を含む東アジアや米国を標的として活動

主な標的：
政府等の公的機関、軍事産業等を含む工業、科学技術、メディア、エレクトロニクス、電気通信分野の民間企業等を標的

主な手口：
海外子会社等のルーターの脆弱性を悪用してバックドアを設置し、そこから標的の企業の本社のネットワーク等に侵入


NISC | Cybersecurity Advisory
TLP:CLEAR

People's Republic of China-Linked Cyber Actors Hide in Router Firmware

Executive summary

The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Japan National Police Agency (NPA), and the Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (hereafter referred to as the "authoring agencies") are releasing this joint cybersecurity advisory (CSA) to detail activity of the People's Republic of China (PRC)-linked cyber actors known as BlackTech. BlackTech has demonstrated capabilities in modifying router firmware without detection and exploiting routers' domain-trust relationships for pivoting from international subsidiaries to headquarters in Japan and the U.S. — the primary targets. The authoring agencies recommend implementing the mitigations described to detect this activity and protect devices from the backdoors the BlackTech actors are leaving behind.

BlackTech (a.k.a. Palmerworm, Temp.Overboard, Circuit Panda, and Radio Panda) actors have targeted government, industrial, technology, media, electronics, and telecommunication sectors, including entities that support the militaries of the U.S. and Japan. BlackTech actors use custom malware, dual-use tools, and living off the land tactics, such as disabling logging on routers, to conceal their operations. This CSA details BlackTech's tactics, techniques, and procedures (TTPs), which highlights the

関係機関と連携した各種対策

◆　フィッシング対策

○　総務省、経済産業省と連携して、送信ドメイン認証技術（DMARC等）の導入等のなりすましメール対策を推進

○　金融庁と連携して、インターネットバンキング不正送金対策に向けて、金融機関に対してフィッシング対策の強化を要請

○　インターネットバンキングに係る不正送金被害額が急増し、過去最多を更新したことを受け、金融庁等と連携して、注意喚起を実施

○　警察庁において、有識者で構成する「キャッシュレス社会の安全・安心の確保に関する検討会」を開催

◆　暗号資産の取引口座対策

○　暗号資産交換業者等と連携して、犯罪に利用された取引口座の凍結スキームを運用開始（2023年４月から対象を拡大）

○　金融庁と連携して、金融機関に対して暗号資産交換業者への不正送金の対策強化（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（2024年２月６日実施）

キャッシュレス社会の安全・安心の確保に関する検討会

検討会概要

○　クレジットカードの不正利用やインターネットバンキングの不正送金の被害が急増するなど、キャッシュレス社会の安全・安心の確保が喫緊の課題

○　フィッシング対策の高度化、官民連携した被害拡大防止策等の推進に関し議論するため、各界の有識者から構成される検討会を開催

有識者

クレジットカードの不正利用対策、インターネットバンキングの不正送金対策の知見等を有する金融業界、EC業界、法曹界、学術界、セキュリティ関係団体（JC３等）の有識者を選定

検討テーマ案

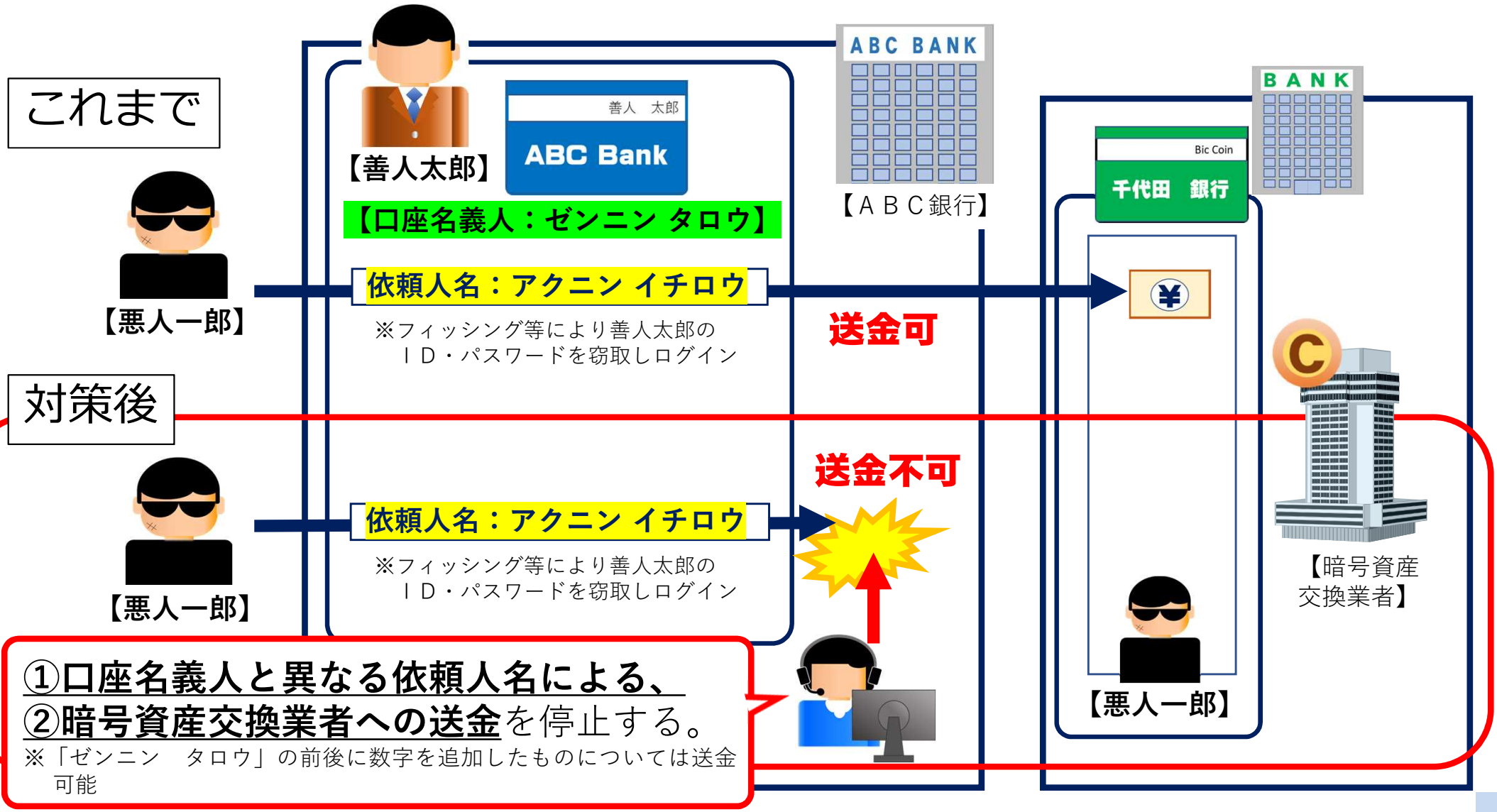
1　先端技術の活用等によるフィッシング対策の高度化・効率化
2　大手EC事業者とのクレジットカード不正利用に関する情報共有による被害拡大防止対策・捜査の推進
3　金融機関における送金先口座対策の推進
4　関係機関等との連携による被害防止対策の推進
5　警察の対処能力の向上

今後の予定

○　11月９日に第１回検討会を開催。年度内に計３回検討会を開催
○　年度内に報告書の取りまとめ及び公表を予定

依頼人名変更時の暗号資産交換業者への送金停止

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。

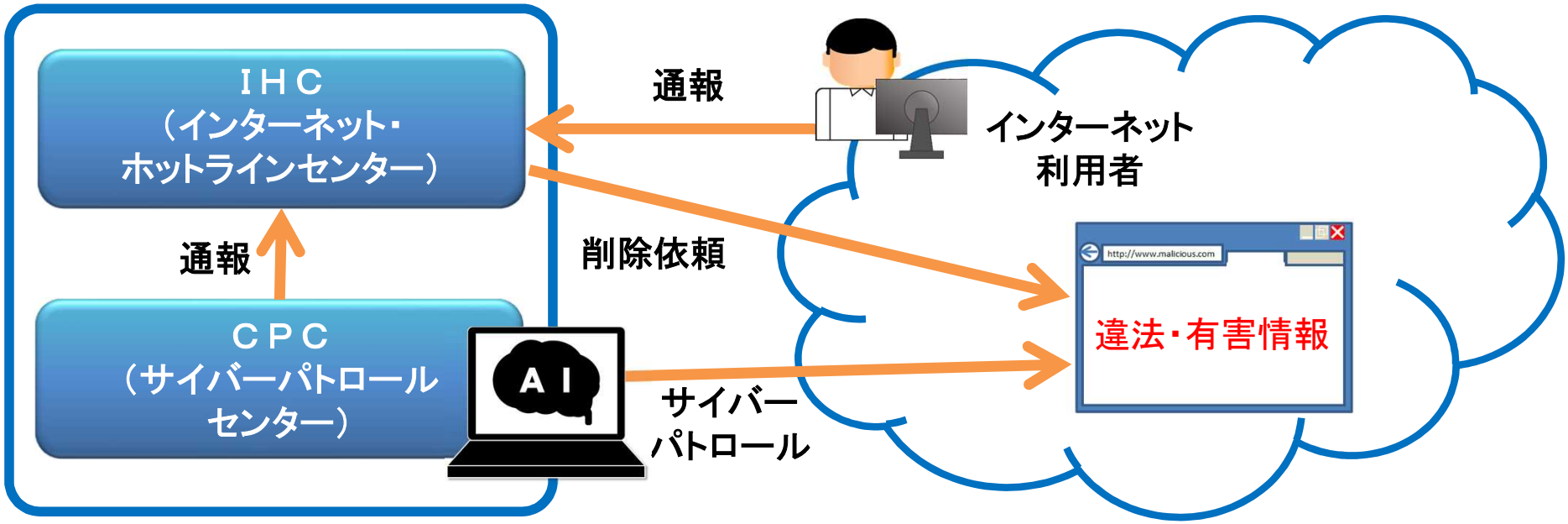


ＡＩの活用（１）

◆　サイバーパトロールの高度化

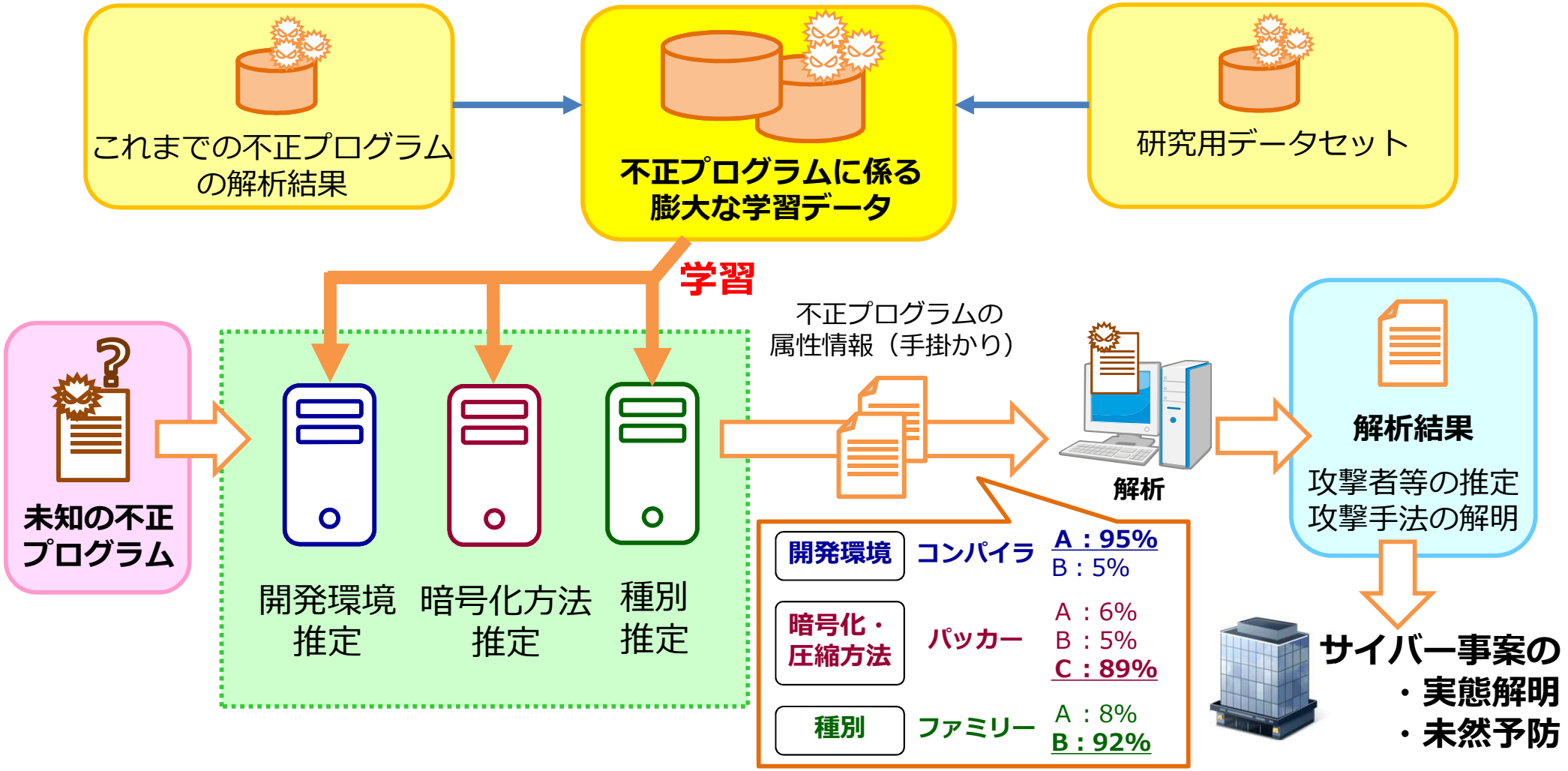
サイバーパトロールセンターに導入したＡＩ検索システムによってインターネット上にある重要犯罪密接関連情報を自動収集し、分析を行い、スコアを付与。

スコアの高いものから優先的にオペレーターが目視確認。
重要犯罪密接関連情報と判断されたものをインターネット・ホットラインセンターに通報。



ＡＩの活用（２）

● 不正プログラム解析の高度化・効率化
　プログラムの特徴を機械学習したＡＩにより、未知のプログラムの開発環境、暗号化方法、種別等を推定し、不正プログラム解析を効率化。



サイバー被害の潜在化の防止

- ○　**被害の拡大防止**
- ○　**再発防止のための注意喚起**
- ○　**実態解明と犯罪インフラ対策**
- ○　**事件検挙に向けた捜査**

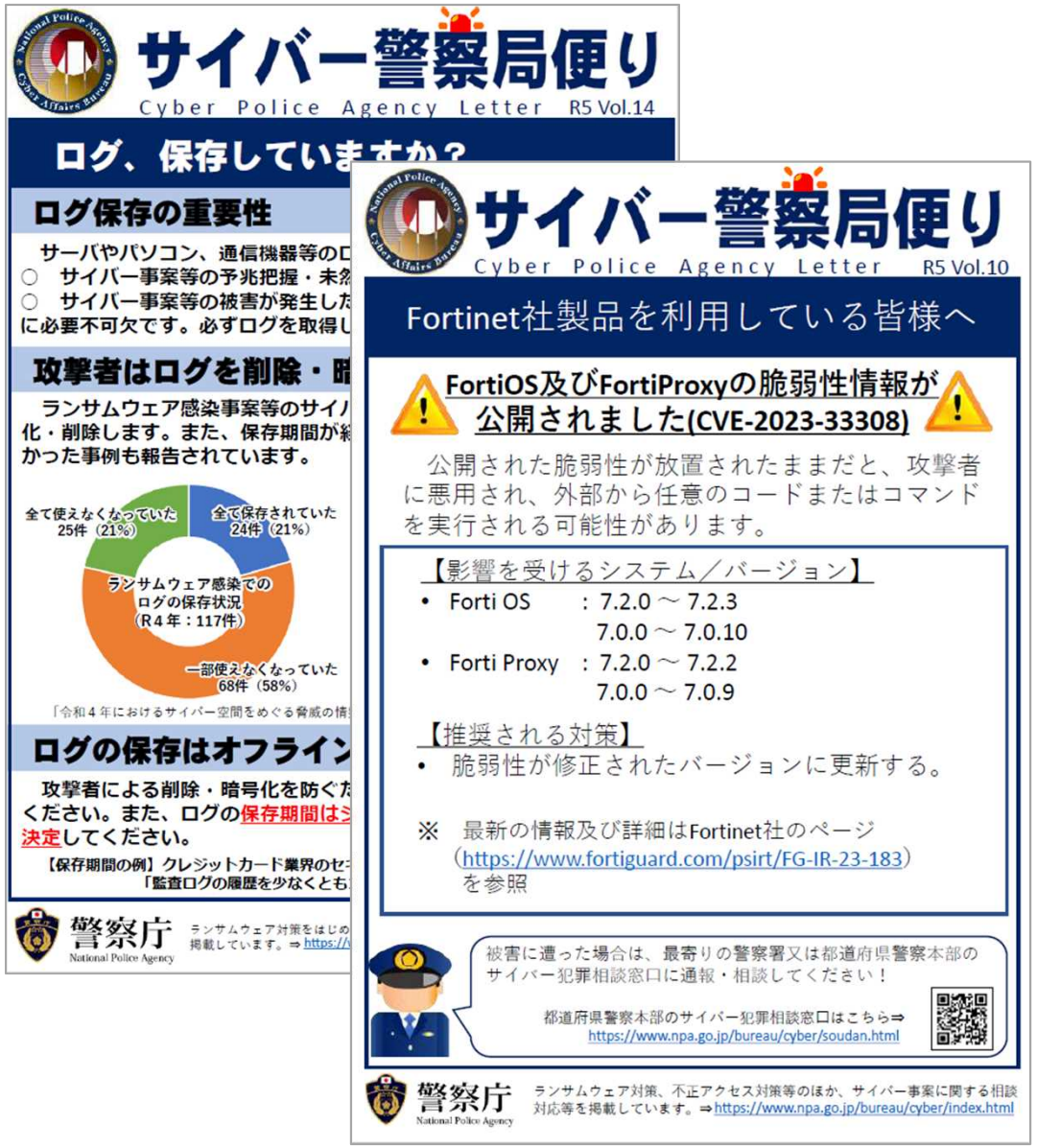
いずれにおいても、警察への通報・相談が不可欠

- ○　都道府県警察の**インターネット上の通報・相談窓口の統一化**
- ○　**関係機関等との覚書の締結**等による通報・相談の促進
- ○　**統一マニュアルの配布や定期的な教養の実施**等による、各都道府県警察における通報・相談への適切な対応の徹底
- ○　**被害の報告に係る様式等の統一**に向けた関係機関等との調整
- ○　ＪＣ３、損害保険会社等を介した**被害実態等の情報共有**

注意喚起等

ECサイト・フリマサイトでの犯罪に加担させる「副業」募集に関する注意喚起(2024.2)

サイバー警察局便り(不定期・月２回程度)



おわりに

- サイバー空間の脅威は深刻な情勢が継続しており、
  一組織の被害が同組織のみならず社会へ大きく影響する可能性
- サプライチェーンを含めた対策が重要
- 産学官の各主体との情報共有といった連携が不可欠

関係省庁、民間事業者・団体、学術・研究機関
といった様々な関係者との連携を積極的に進め、
デジタル社会における安全・安心の実現に貢献