令　和　8　年　2　月　2　7　日
サイバーセキュリティシンポジウム道後2026

サイバー空間をめぐる脅威の情勢と対応

警察庁サイバー警察局
サイバー企画課　課長補佐
酒井　千尋

本日の内容

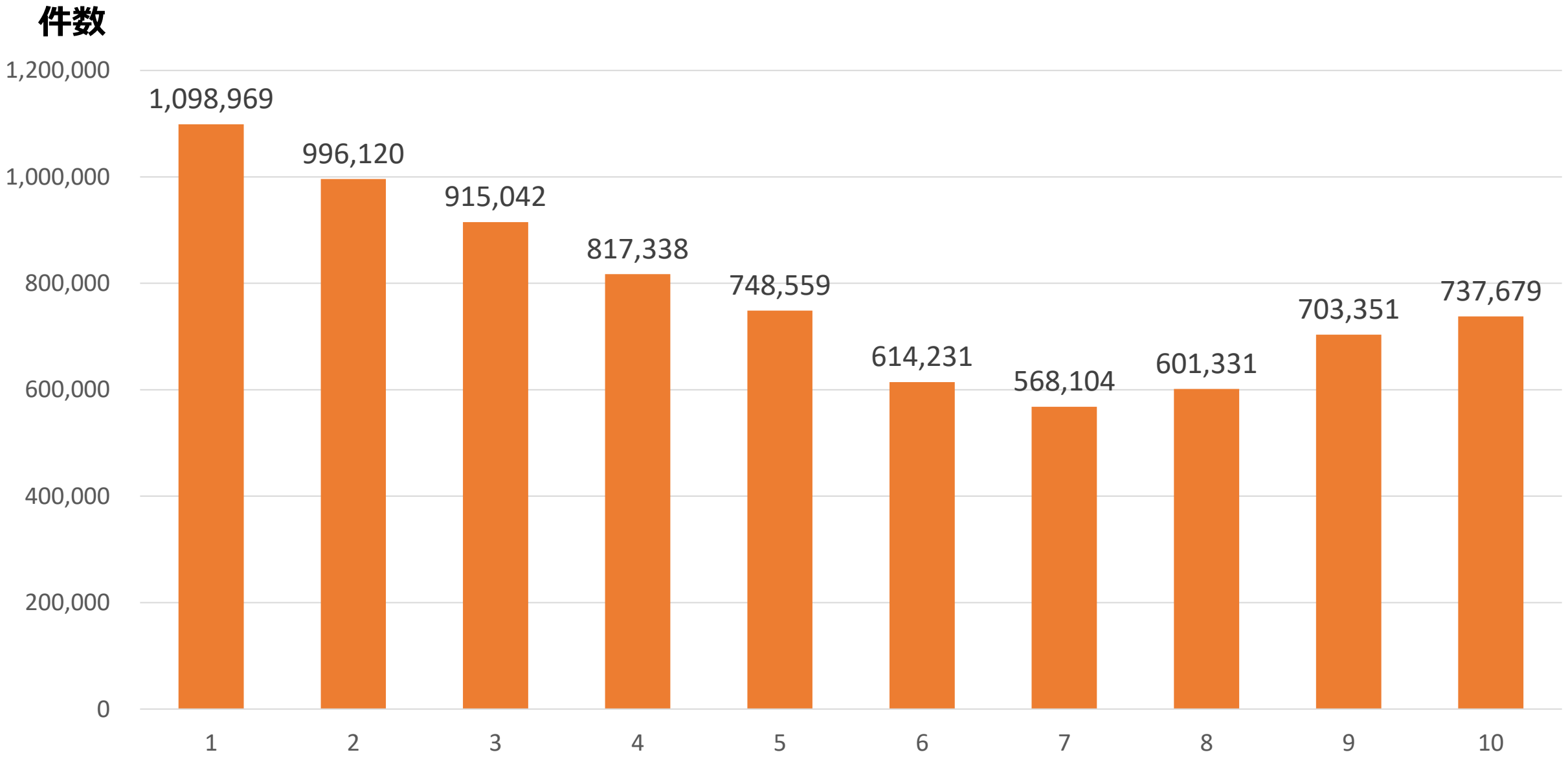
１　サイバー空間をめぐる脅威情勢

２　警察の取組

３　今後の課題

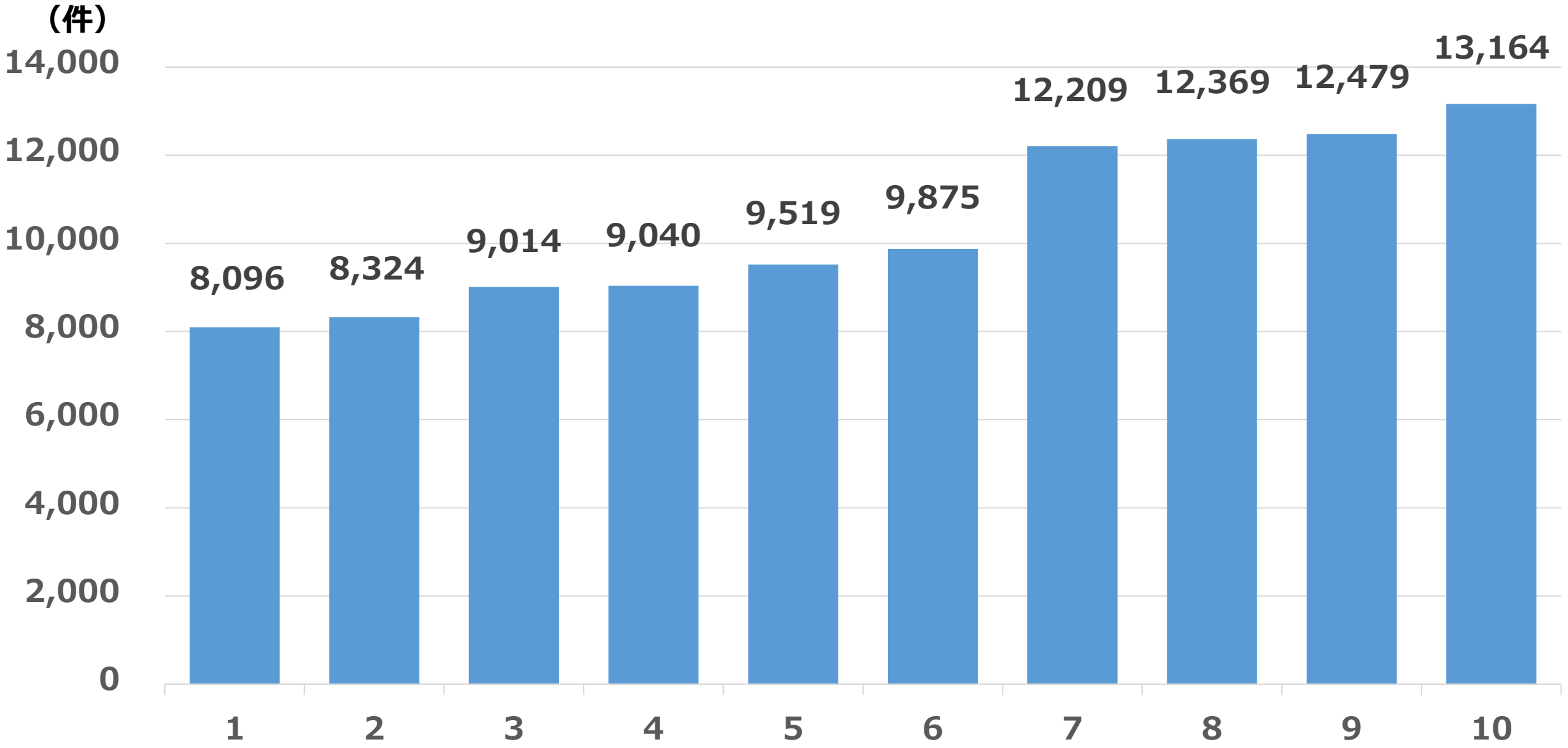
１　サイバー空間をめぐる脅威情勢

刑法犯認知件数



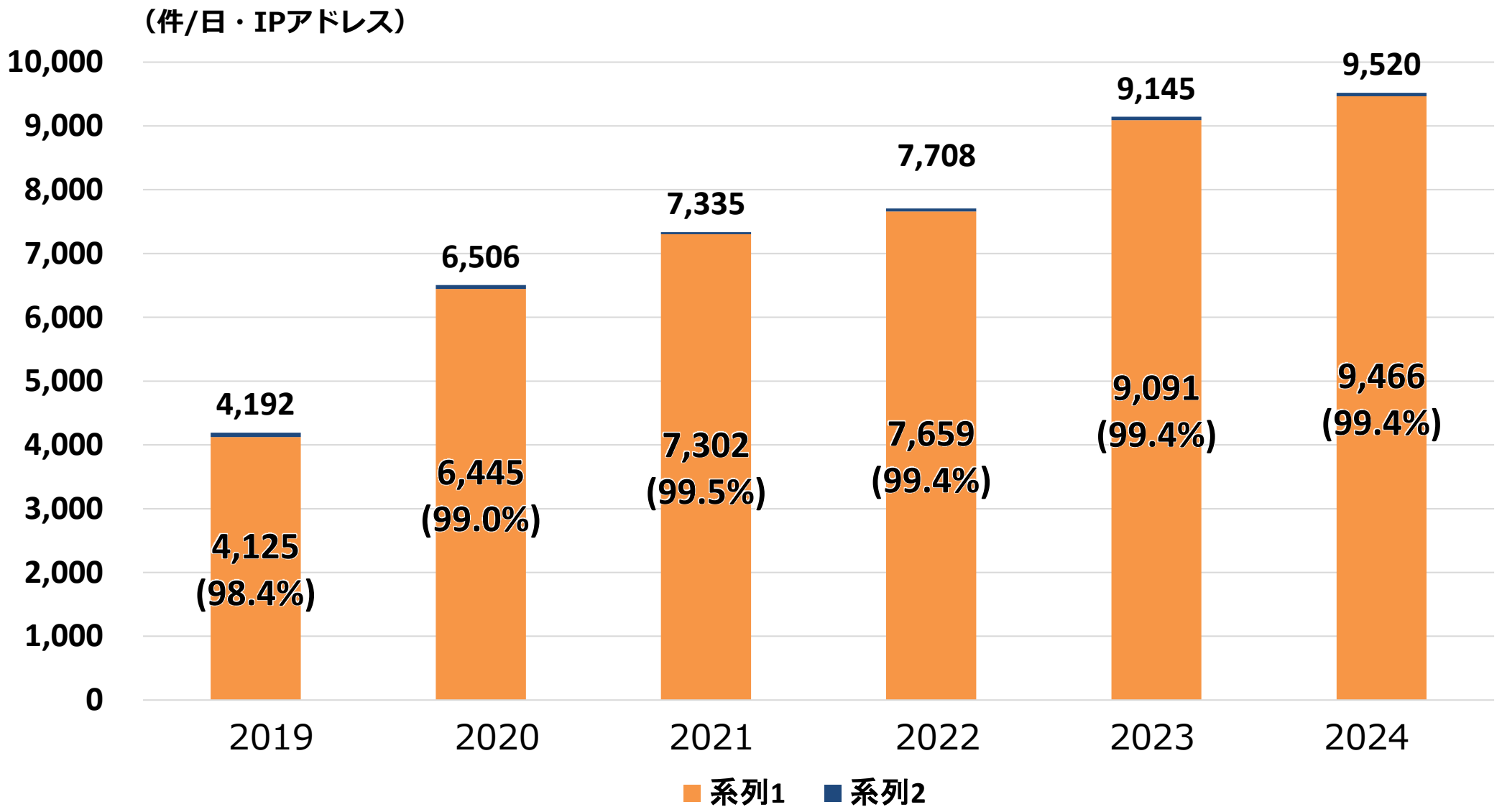
出典：警察庁「刑法犯に関する統計資料」

サイバー犯罪の検挙件数



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

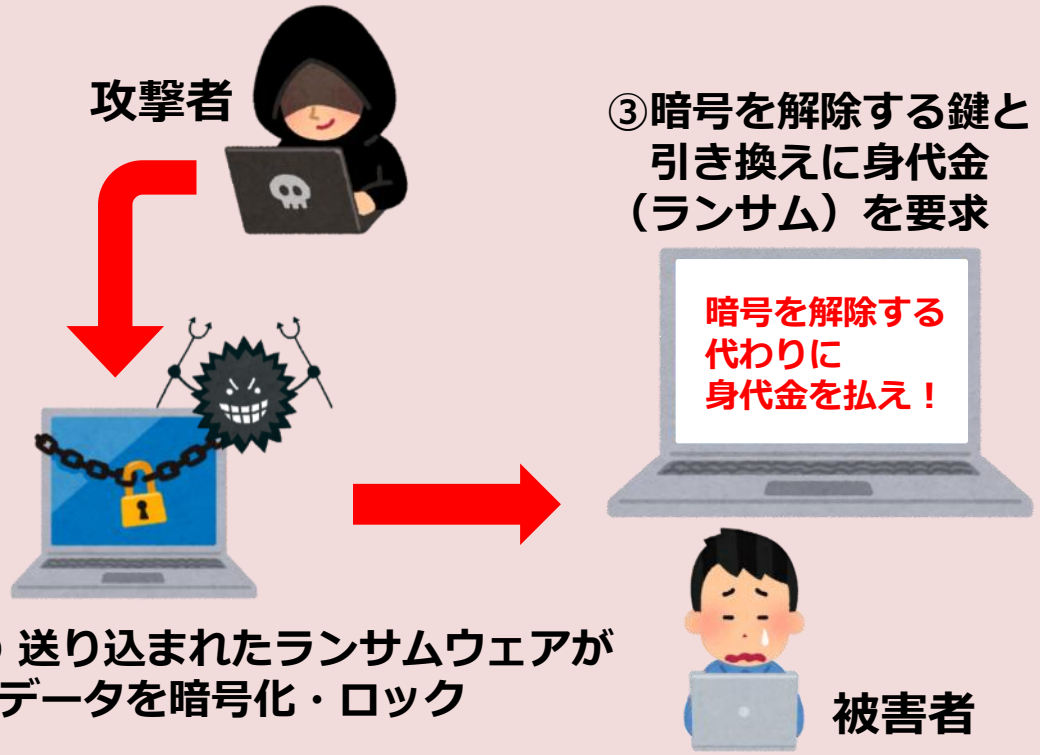
サイバー空間におけるぜい弱性探索行為の観測状況



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

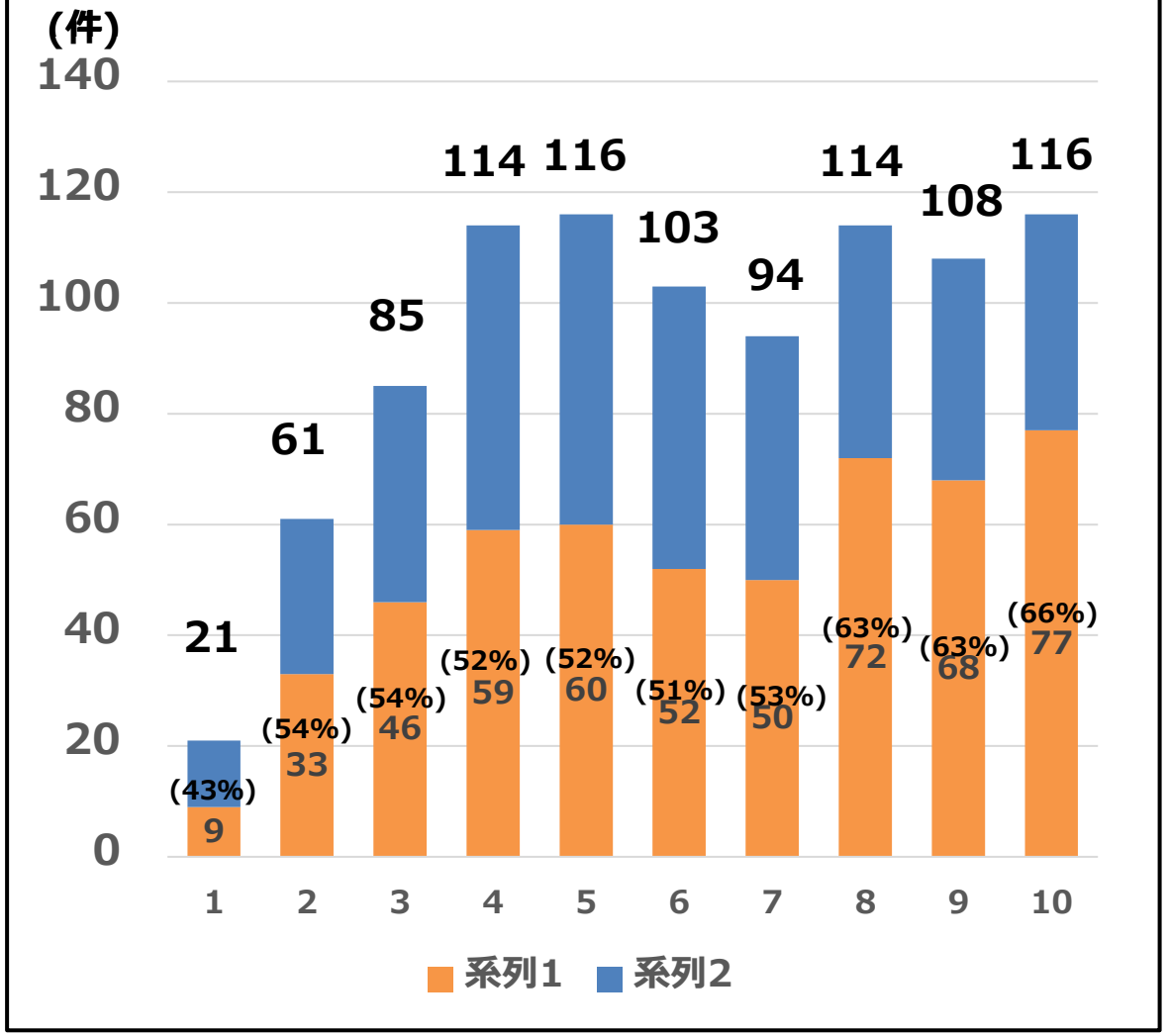
高度なサイバー攻撃　～ランサムウェア～

①「ランサムウェア」が送り込まれる



➡　データを盗み取り「身代金を支払わなければデータを公開するぞ」などと恐喝する「二重恐喝」が行われる場合も。

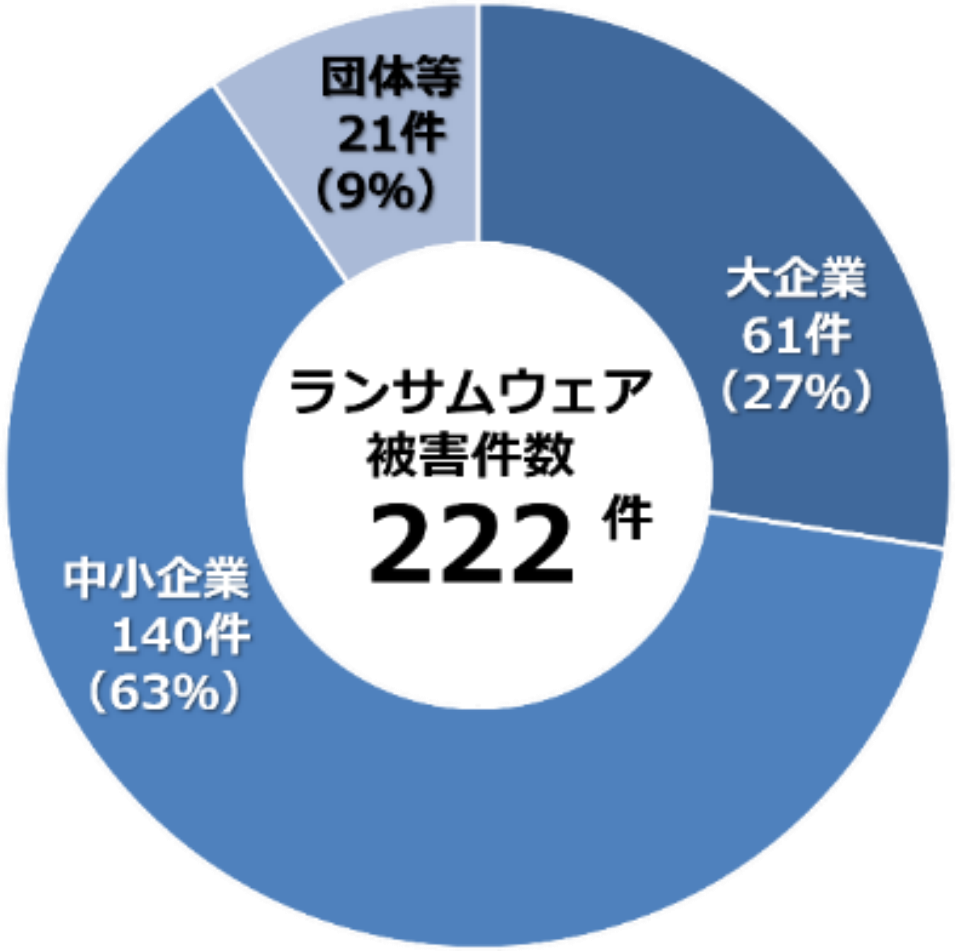
ランサムウェアによる被害の報告件数



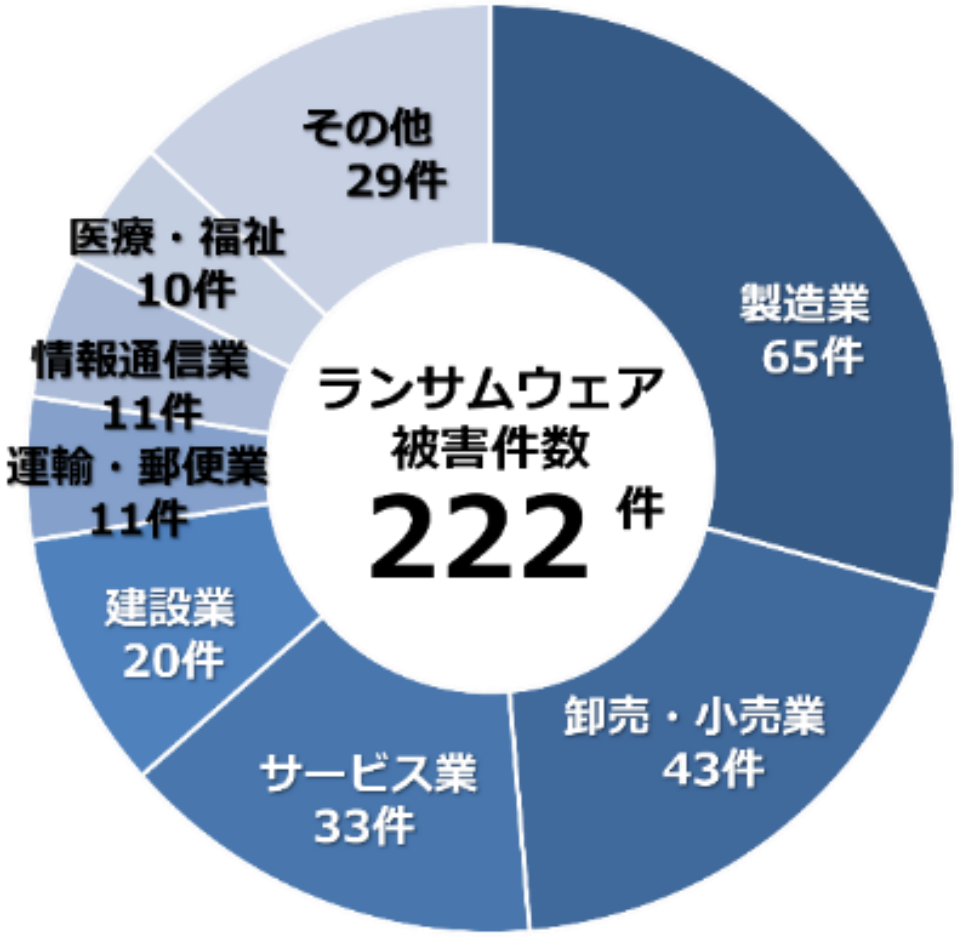
出典：警察庁「サイバー空間をめぐる脅威の情勢等について」を元に作成

ランサムウェアによる被害（規模別・業種別）

規模別



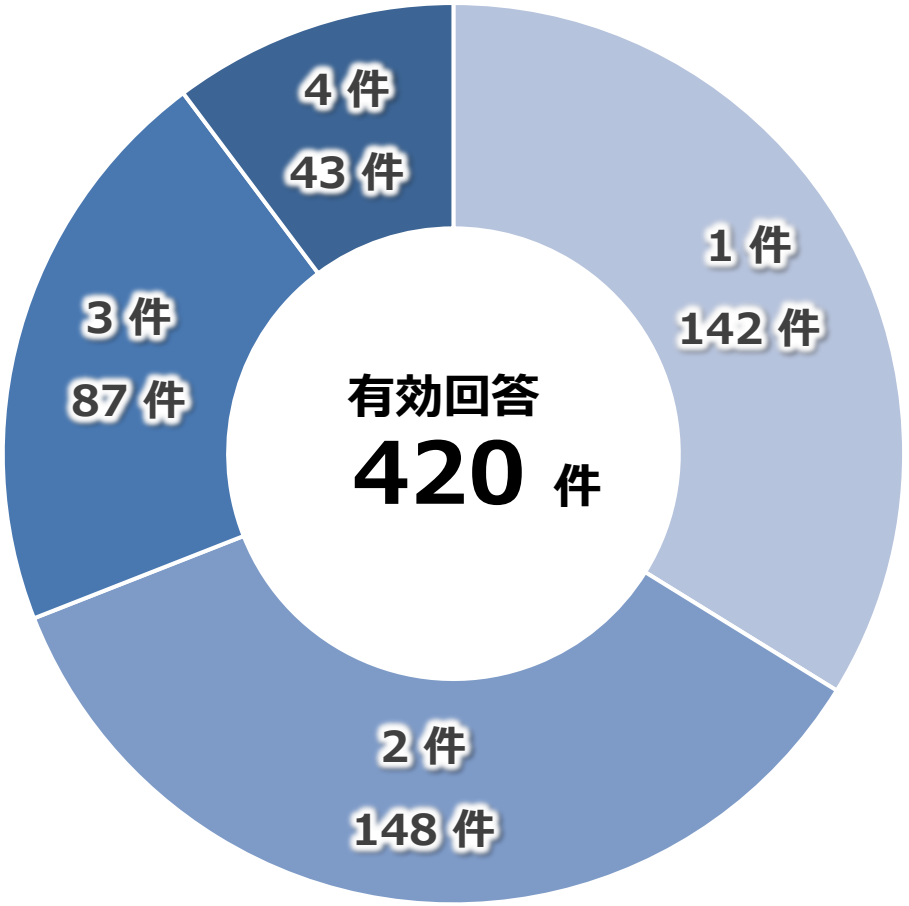
業種別



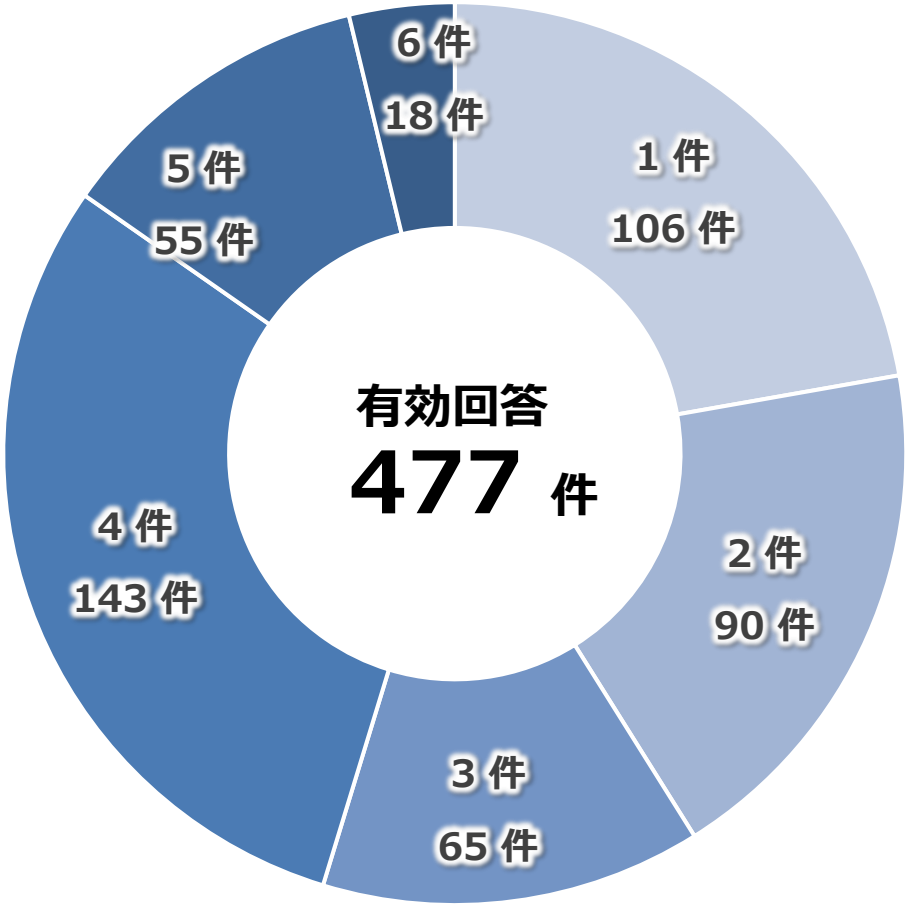
企業規模・業種を問わず、幅広く被害が発生

復旧に要した期間・調査費用

期間



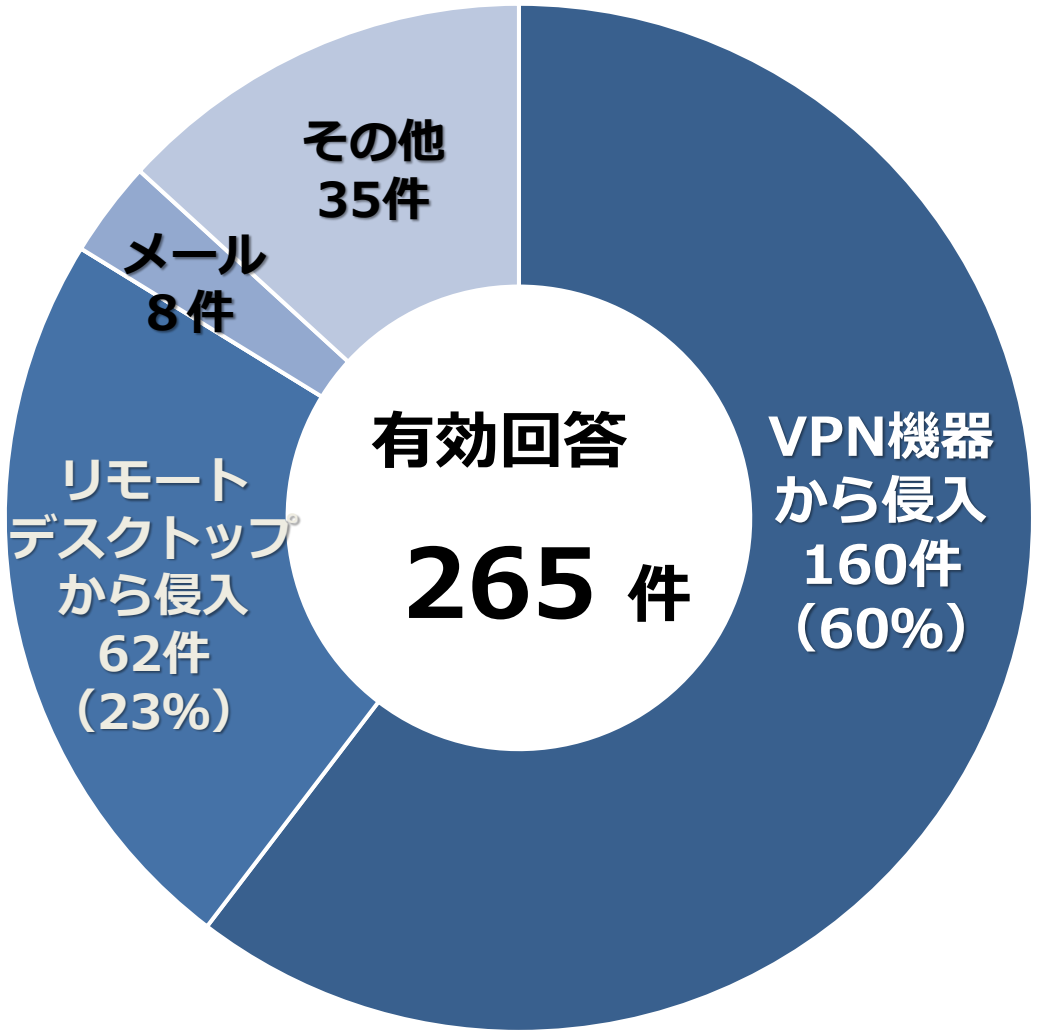
費用



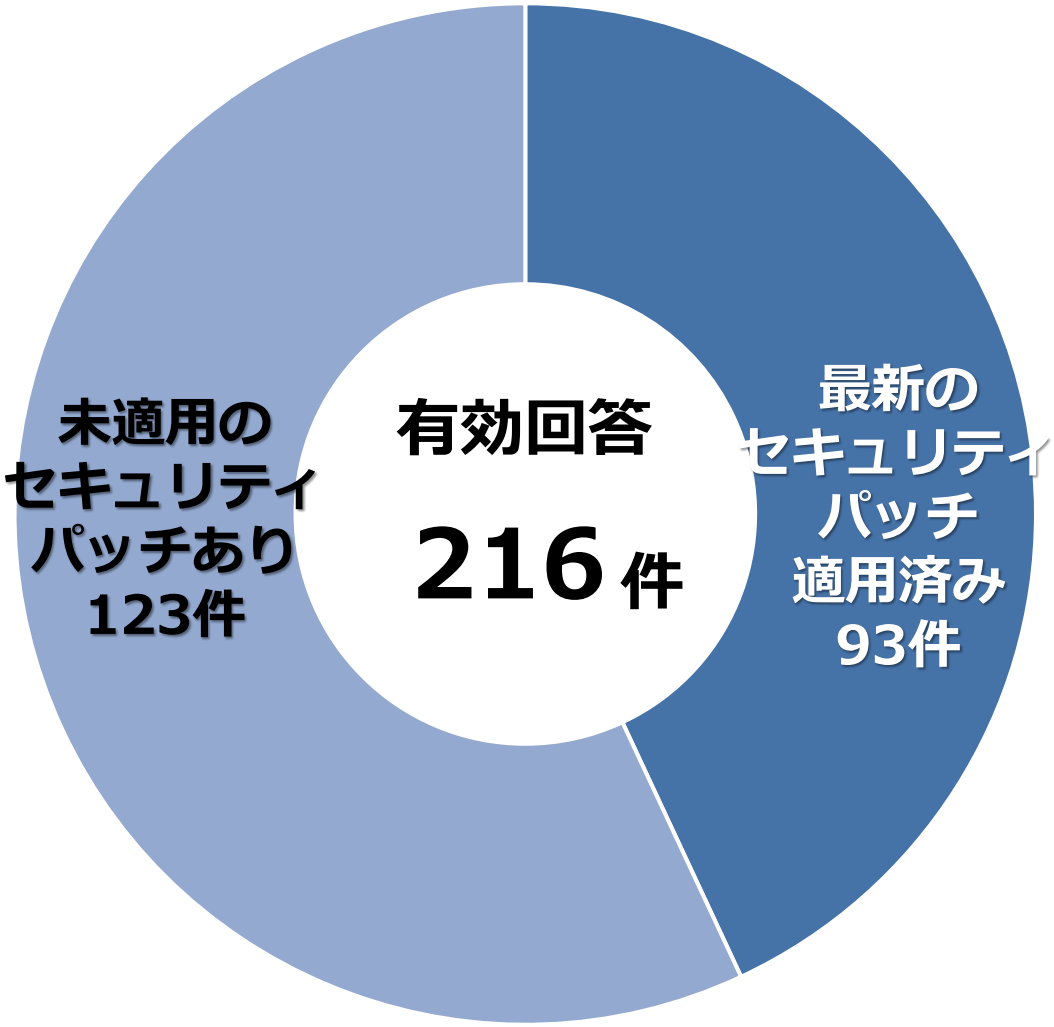
出典：警察庁「ランサムウェア等被害に関する実態調査」（R３～R７上）を元に作成

ランサムウェアの感染経路

感染経路



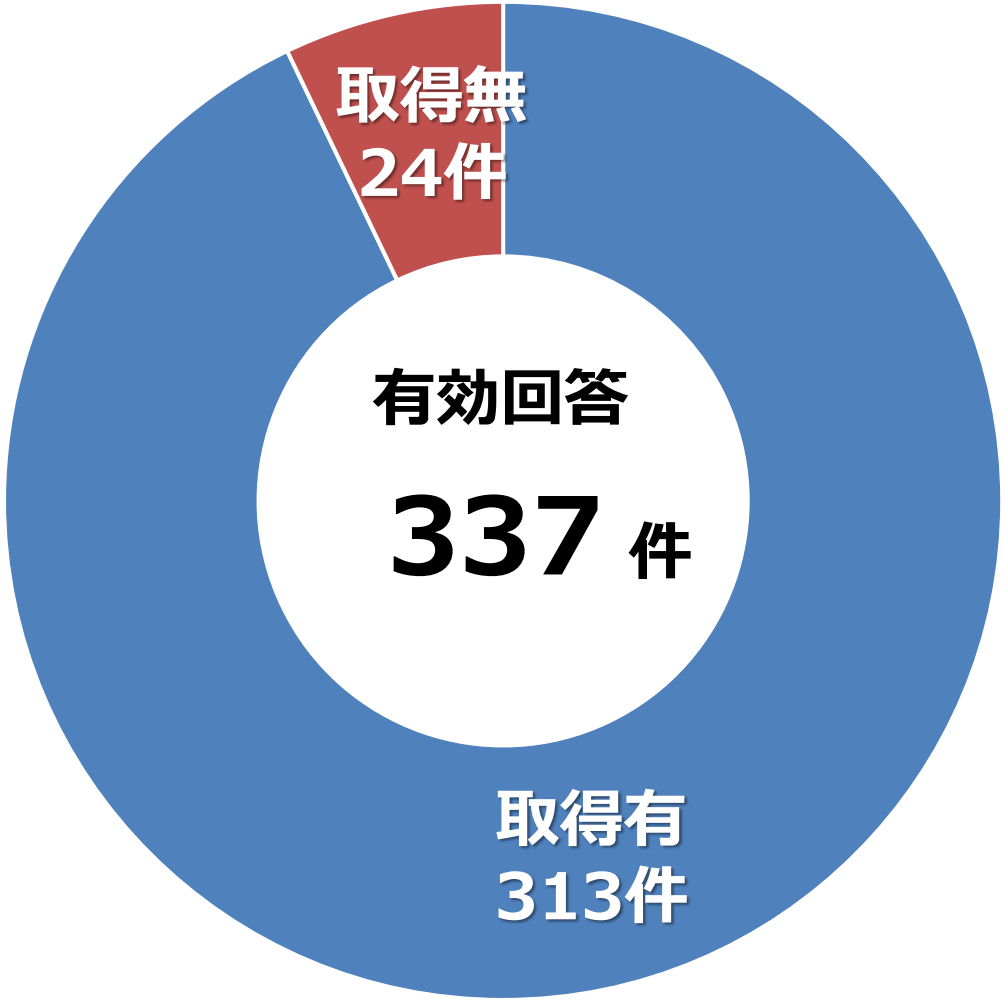
感染経路のパッチ適用状況



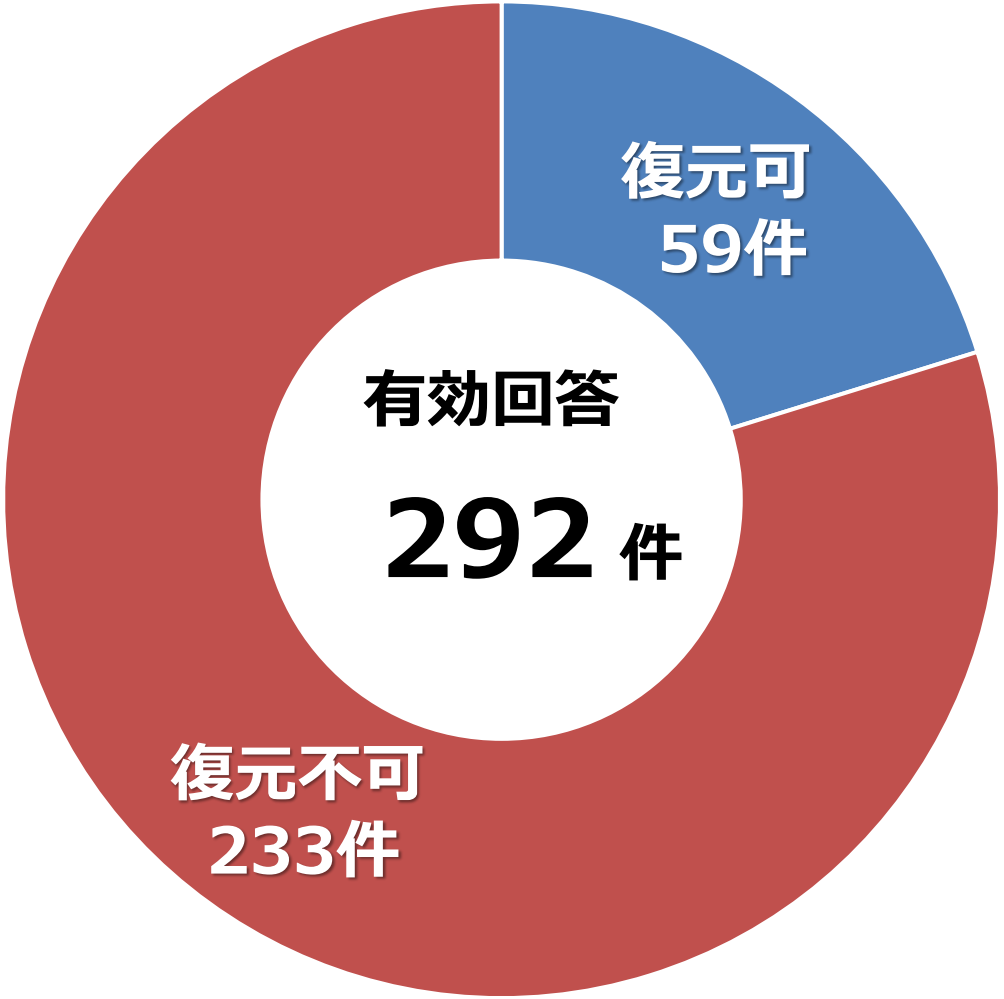
出典：警察庁「サイバー空間をめぐる脅威の情勢等について」(R5～R7上）より作成

バックアップの取得・復元状況

バックアップの取得

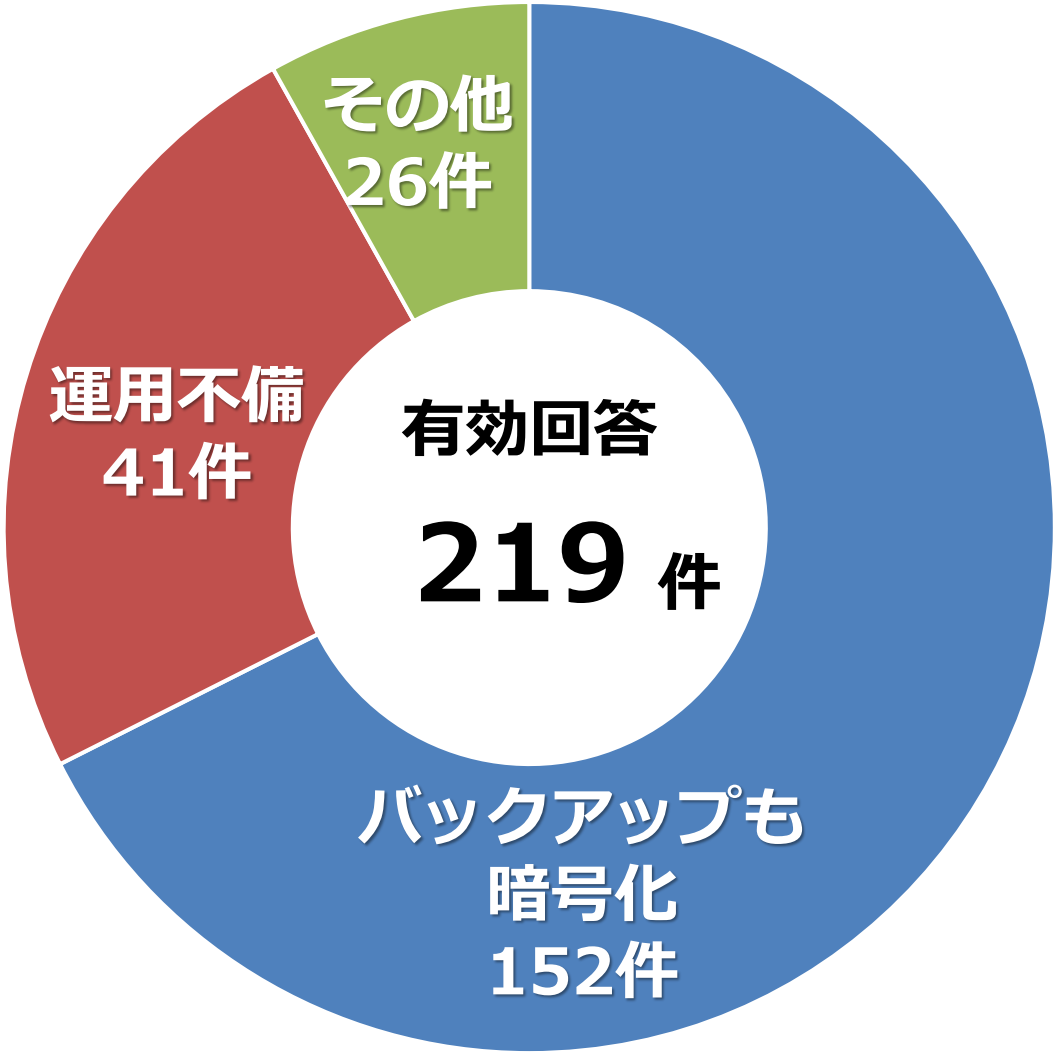


復元の可否



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」(R5～R7上）より作成

バックアップから復元できなかった理由



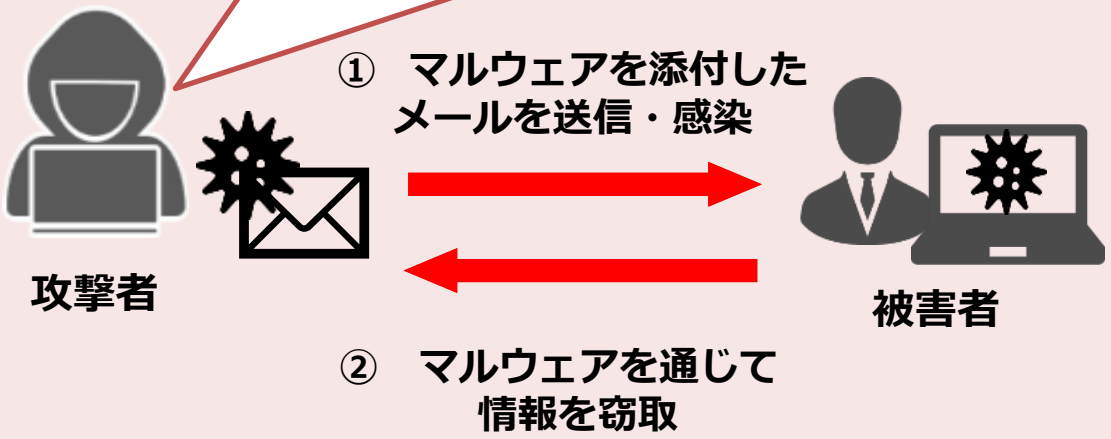
出典：警察庁「サイバー空間をめぐる脅威の情勢等について」(R5～R7上）より作成

懸念国によるサイバー攻撃

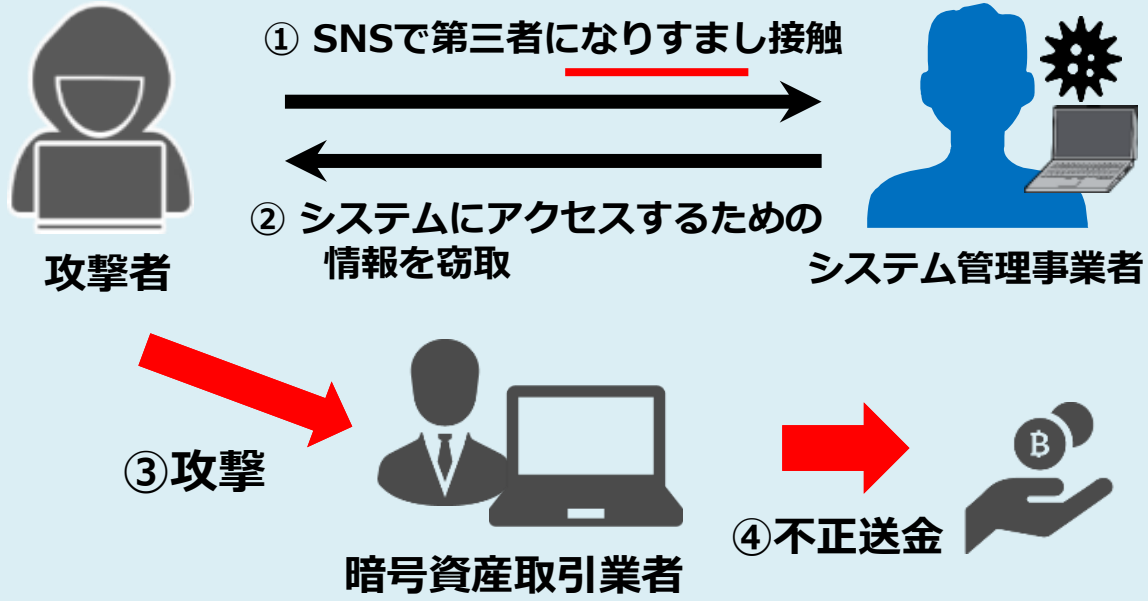
【情報窃取型サイバー攻撃】

○　交流のある人物を詐称

○　関心のある専門分野の有識者を詐称

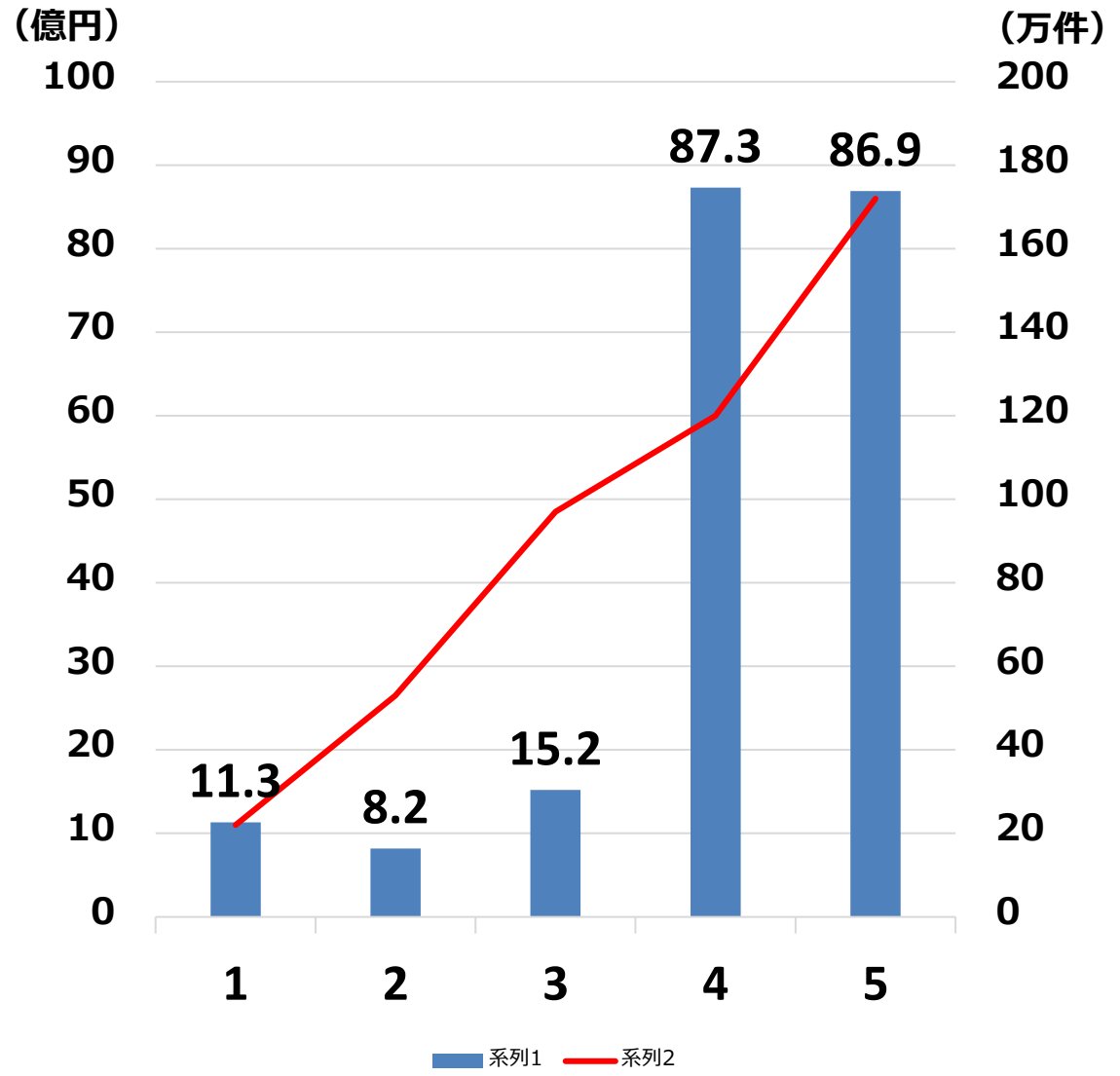


【暗号資産窃取型サイバー攻撃】



システムの脆弱性のみならず人間の脆弱性も悪用

フィッシングを入口としたサイバー犯罪
～インターネットバンキング不正送金～



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

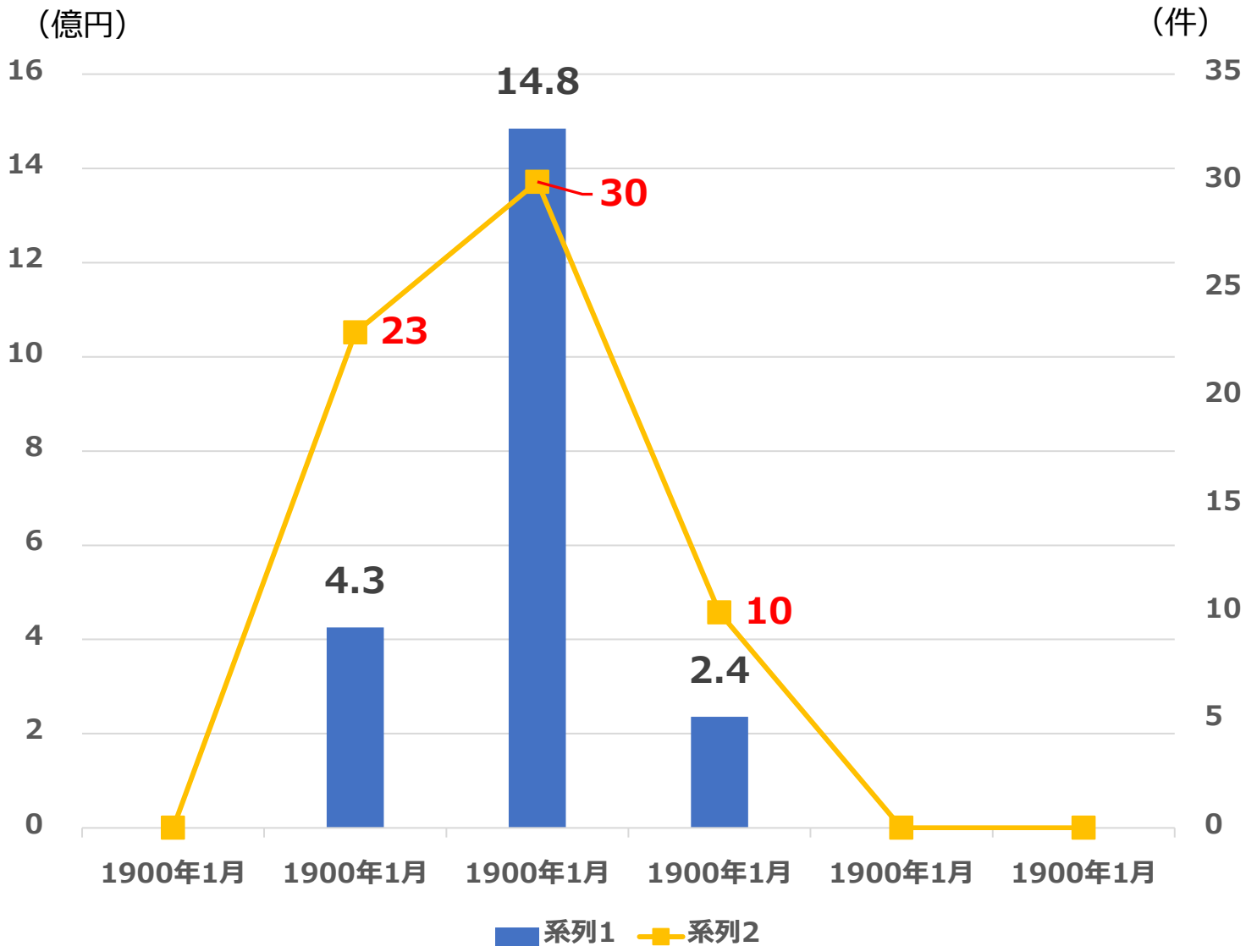
フィッシング（phishing）

メールなどで偽サイトに誘導し、IDやパスワードなどを入力させ窃取

※「洗練された(sophisticated)と「釣り(fishing)」が由来の造語とも言われている

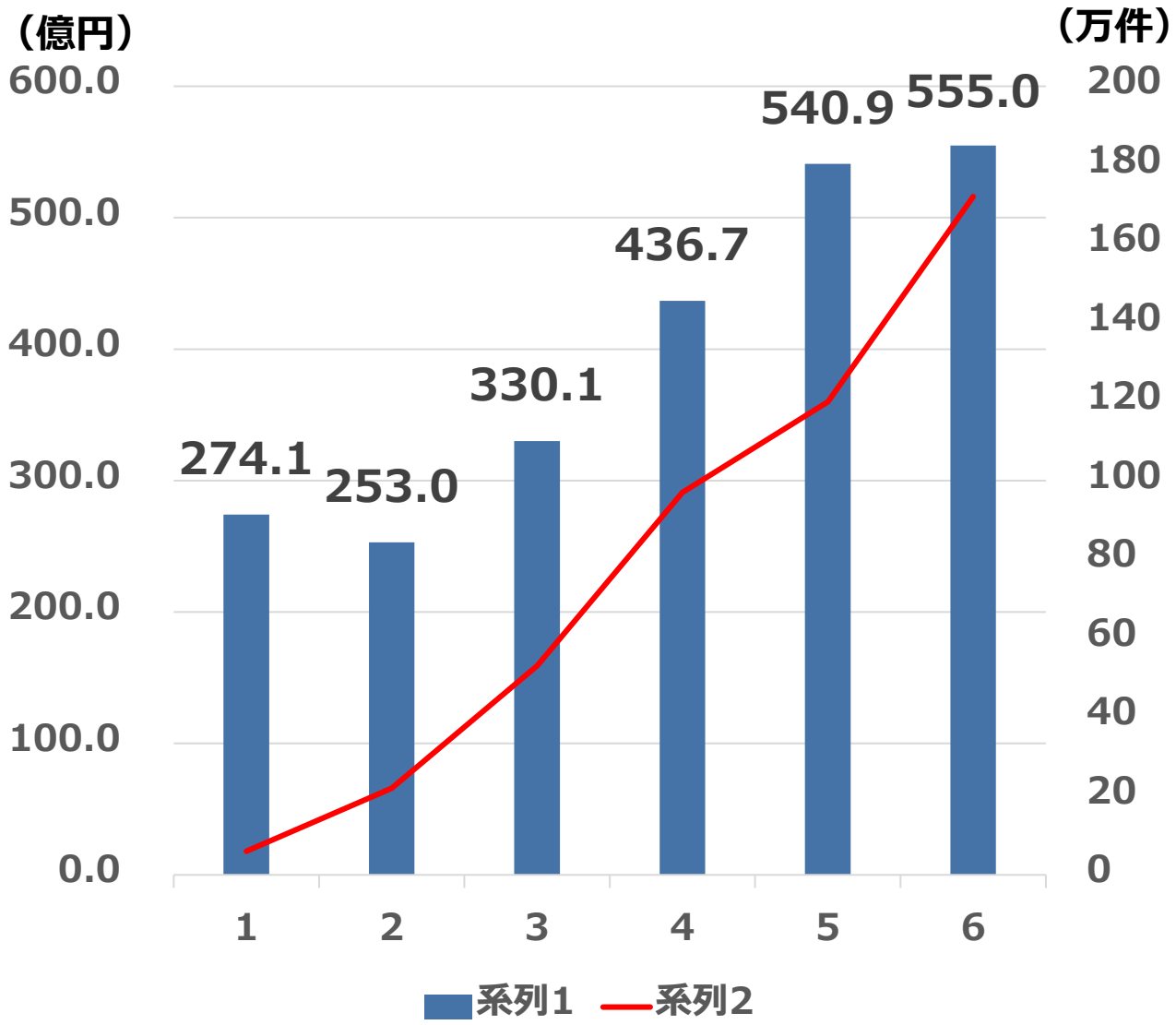
偽サイトに情報を入力し、不正送金被害

ボイスフィッシングによる法人口座の不正送金被害額



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

フィッシングを入口としたサイバー犯罪
～クレジットカード情報不正利用～



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

偽 メール

From: XYZカード
件名:【緊急】不正アクセスを検知しました

第三者からの不正なアクセスを検知しました。
至急ログインして確認してください。

http://xyz-card.com

偽 ショートメッセージ

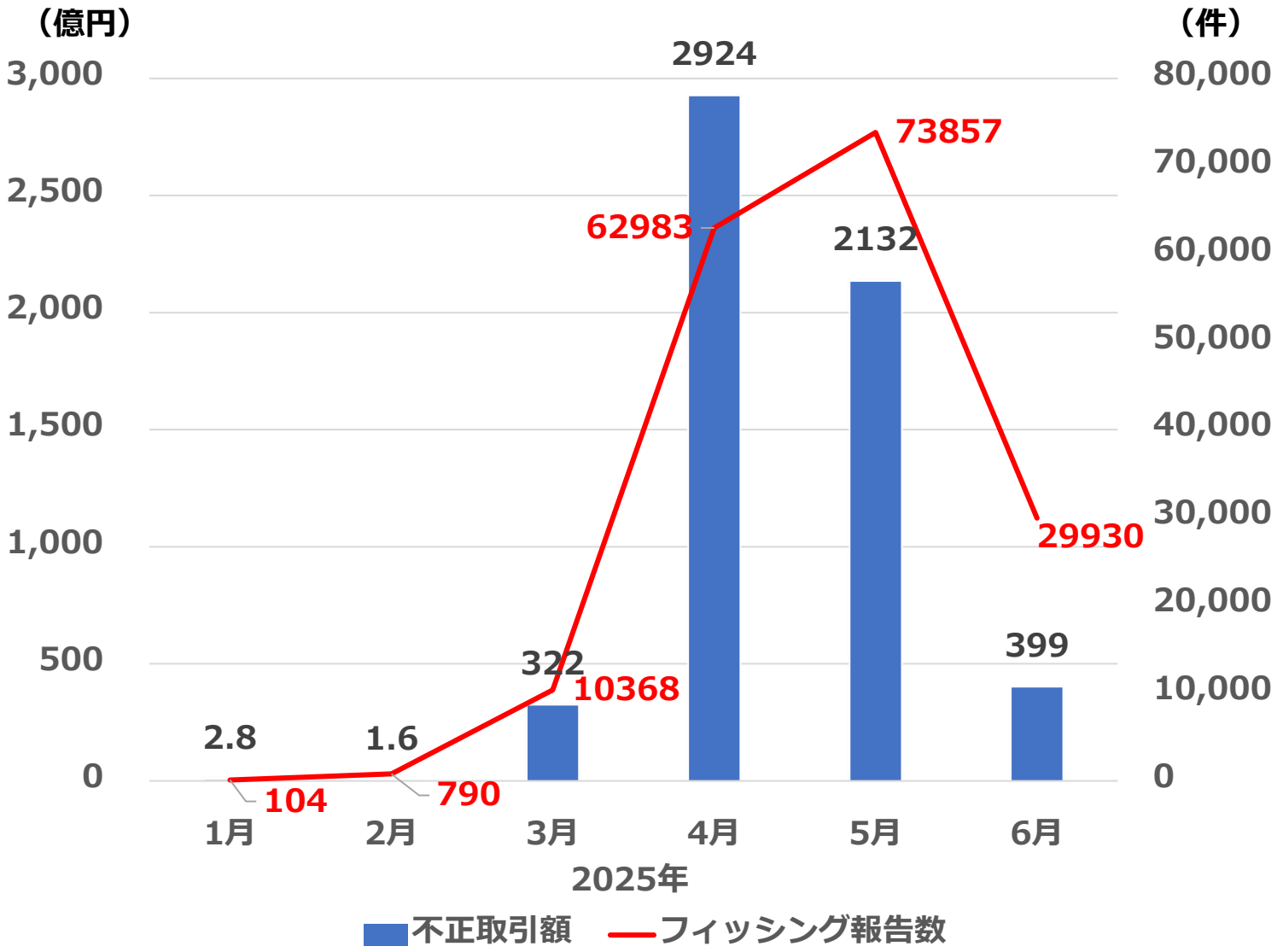
050xxxxxxx

お荷物のお届けがありましたが、不在のため持ち帰りました。
http://example.jp

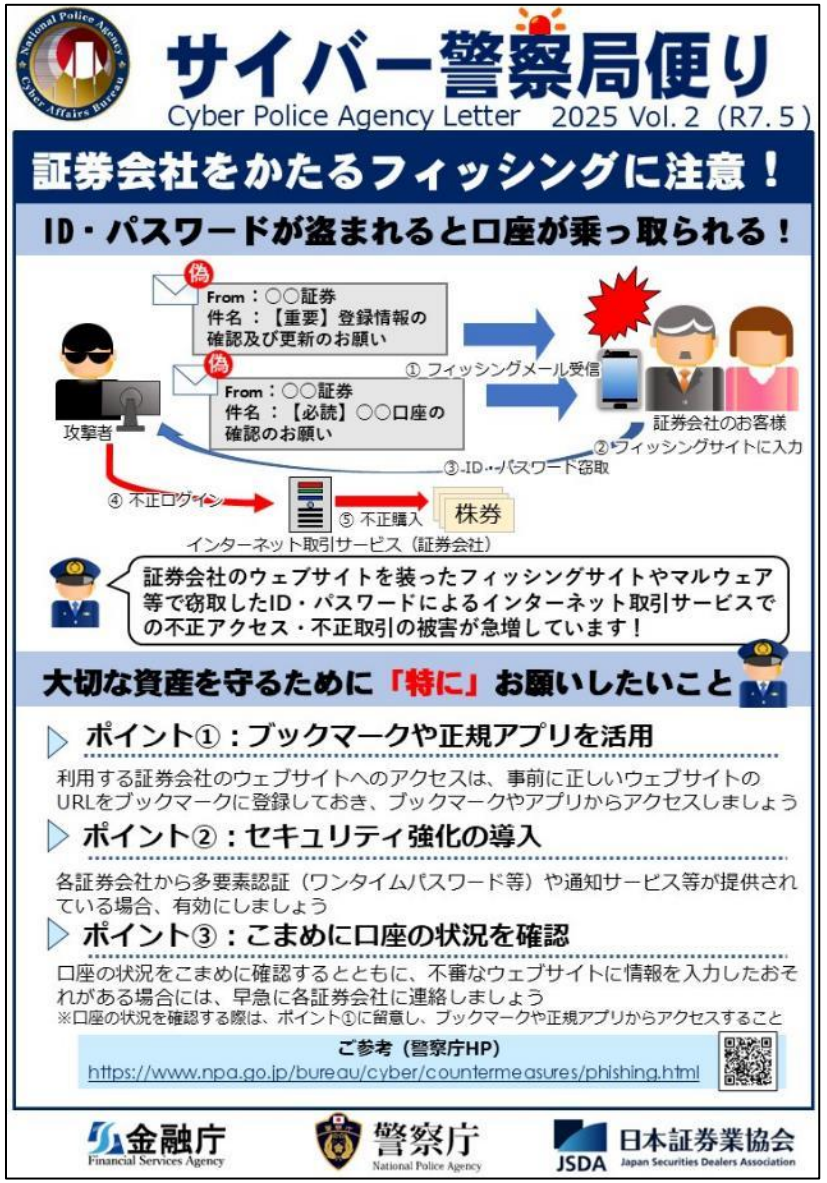
偽サイトにカード情報を入力すると

クレジットカード不正利用の被害

フィッシングを入口としたサイバー犯罪
～証券口座不正取引～



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」



ＡＩの悪用

【ランサムウェア作成】
　生成ＡＩを使用して、ランサムウェアを作成したとして、不正指令電磁的記録作成容疑で男性を令和６年（2024年）５月に検挙。

【不正アクセスの自動化】
　他人のIDとパスワードを使い、生成ＡＩを使用しつつ、電気通信事業者のサイトに不正アクセスし、eSIMを不正取得したとして、不正アクセス禁止法などで中高生の少年３人を令和７年（2025年）１月から２月にかけて検挙。

【フィッシングサイトを作成】
　生成ＡＩを使用して大手ＥＣサイトのフィッシングサイトを構築、公開した男性を不正アクセス禁止法違反で令和７年（2025年）６月に検挙。

出典：警察庁「サイバー空間をめぐる脅威の情勢等について」等

2　警察の取組

警察庁サイバー警察局・サイバー特別捜査部の設置

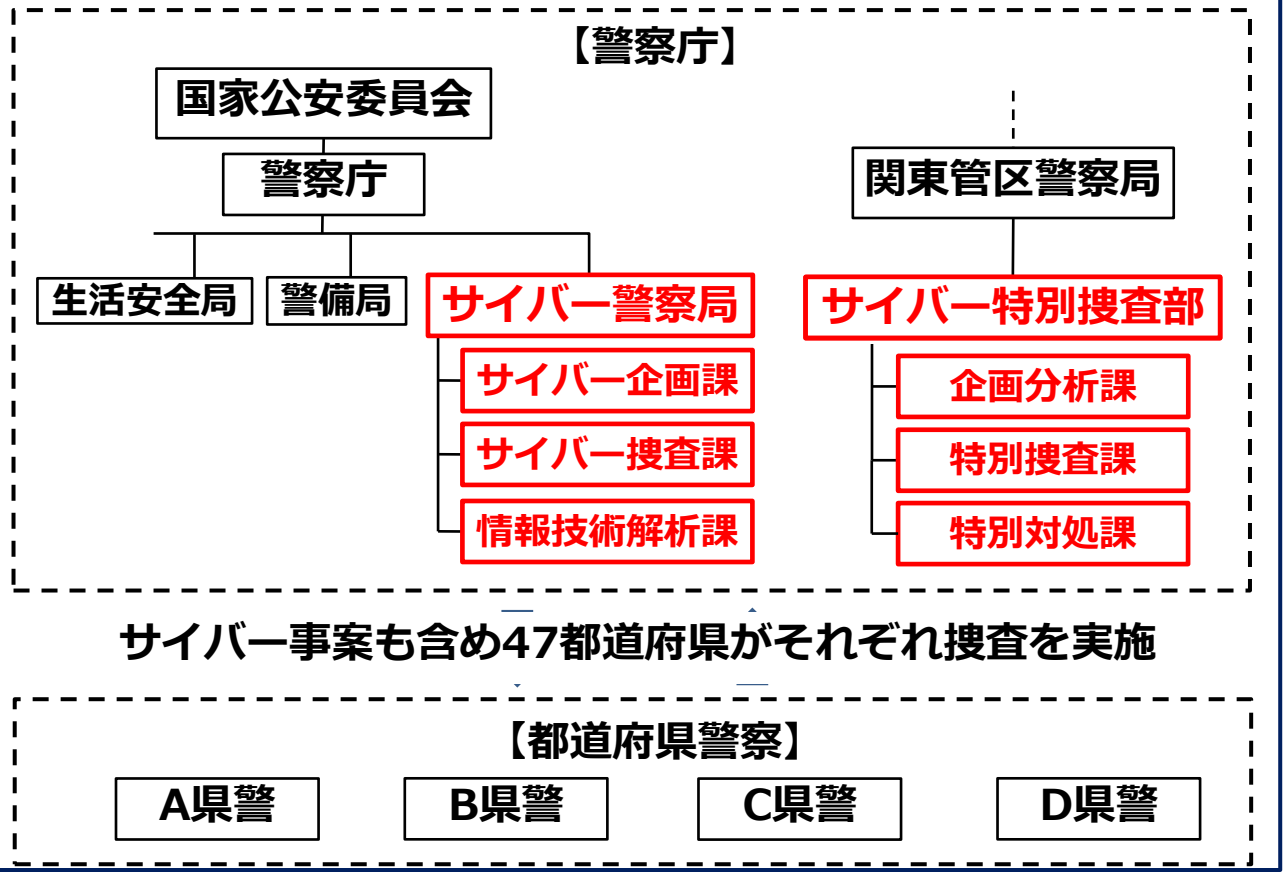
サイバー警察局・サイバー特別捜査部

Ⅰ　警察庁にサイバー警察局を設置(R4.4)

Ⅱ　関東管区警察局に重大サイバー事案の捜査を行うサイバー特別捜査隊を設置(R4.4)

Ⅲ　サイバー特別捜査隊を発展的に改組し、サイバー特別捜査部（企画分析課・特別捜査課）を設置(R6.4)

Ⅳ　サイバー特別捜査部に特別対処課を設置(R7.4)



海外機関 ⟷

国際連携を通じた
犯人検挙・抑止

警 察

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

⟷ 産業界・学会

官民連携を通じた
被害防止対策

国際共同捜査によるランサムウェア被疑者の検挙

国際共同捜査

外国　日本

ユーロポール・外国捜査機関

相互協力

③復号ツールの提供

サイバー警察局

サイバー
特別捜査隊

National Cyber Unit

捜査

①逮捕

②犯罪インフラの閉鎖

A警察

B警察

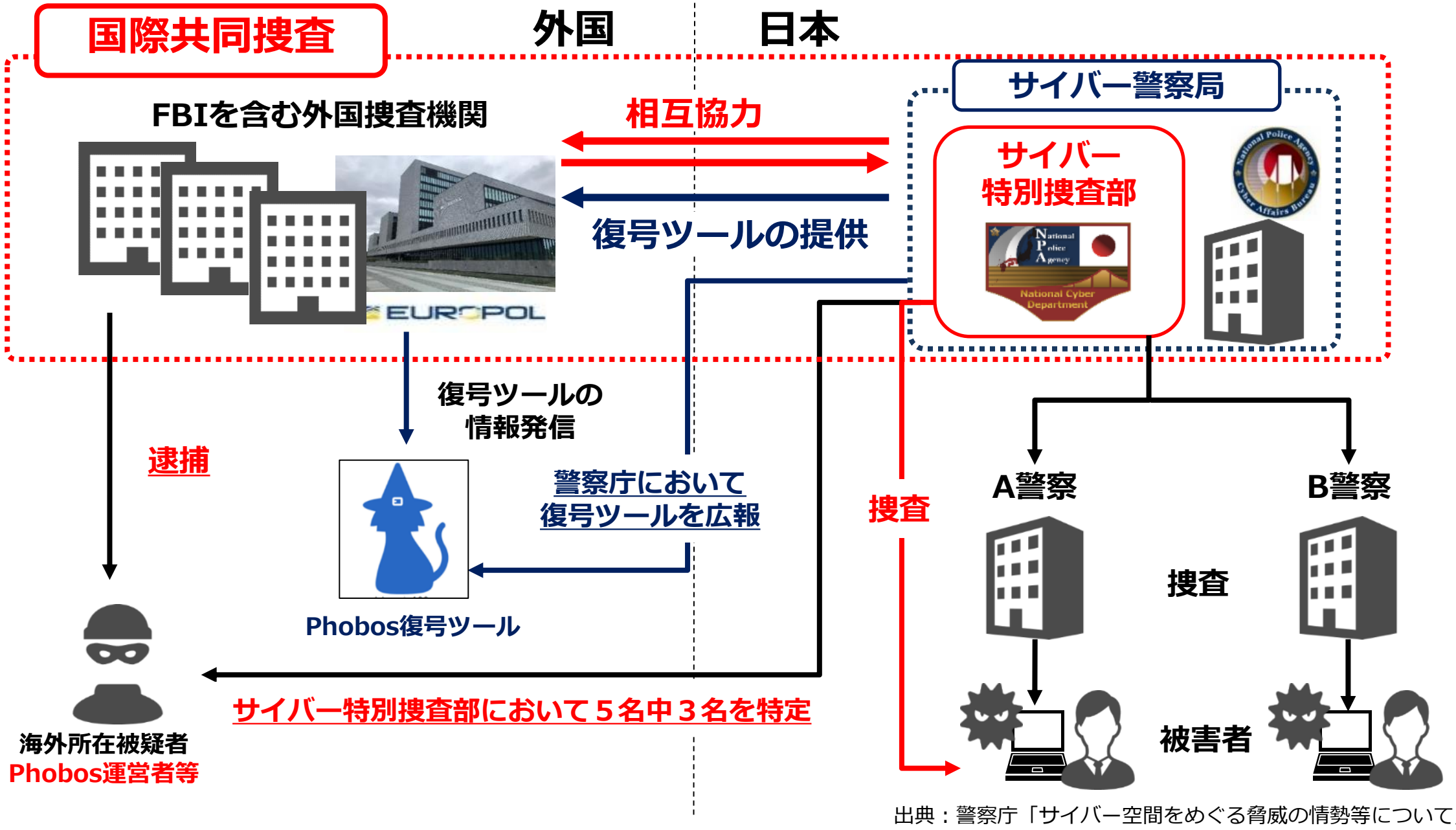
捜査

海外所在被疑者

被害者

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

ランサムウェア（Phobos／8base）被疑者の検挙・被害回復



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

懸念国による情報窃取型サイバー攻撃に対する対処

■　警察庁サイバー特別捜査部等が、 2019年頃から我が国の幅広い層に対して行われてきたサイバー攻撃について、捜査・分析を行った結果、**「MirrorFace」**と呼称されるサイバー攻撃グループによる、**中国の関与が疑われる組織的なサイバー攻撃活動**であると評価。

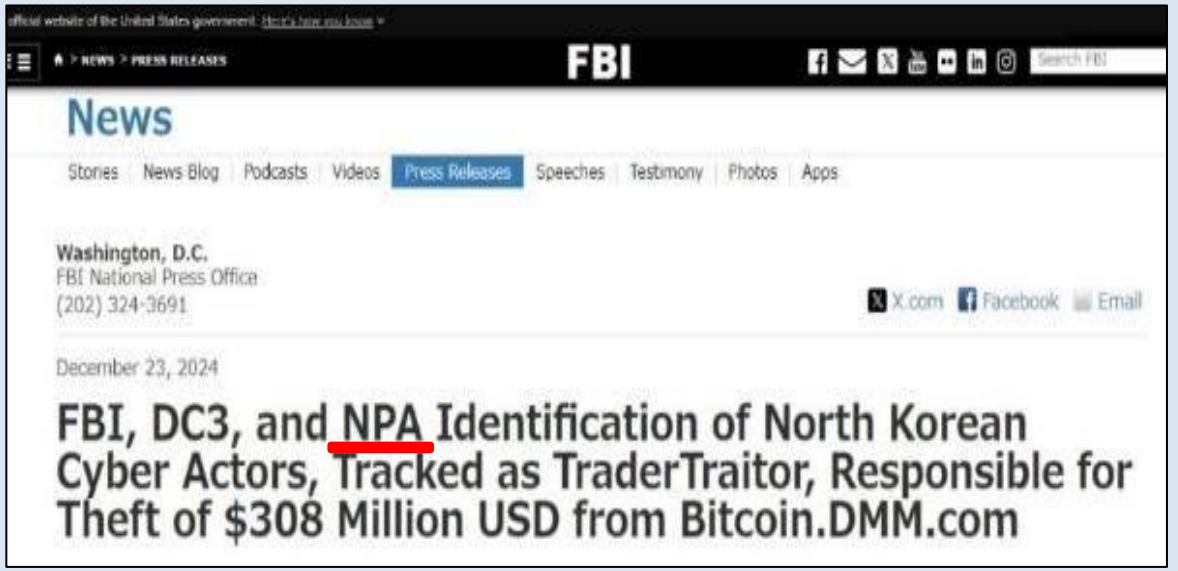
■　2025年１月、ＮＩＳＣと連名で**注意喚起を実施**し、攻撃の手口や未然防止対策案について公表。

出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

懸念国による暗号資産窃取型サイバー攻撃への対処

■　警察庁サイバー特別捜査部・警視庁による捜査・分析の結果、 2024年5月に我が国の暗号資産交換業者から約482億円相当の暗号資産を窃取された事件について、**北朝鮮を背景とする**サイバー攻撃グループ「**TraderTraitor**」が、**SNS上でリクルーターになりすまして、**暗号資産ウォレット管理システムに係る事業者の従業員に接触し、これになりすまして、同システムにアクセスして窃取したものと特定。

■　2024年12月、米国FBI・米国国防省と共同で**パブリック・アトリビューション**を実施するとともに、NISC及び金融庁と連名で注意喚起。



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

国際共同捜査によるフィッシング被疑者の逮捕

国際共同捜査

POLRI
KEPOLISIAN NEGARA REPUBLIK INDONESIA

インドネシア当局

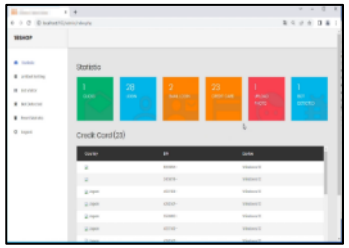
相互協力

サイバー警察局

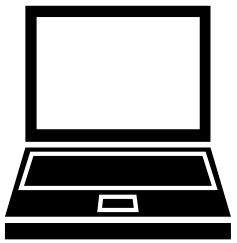
サイバー特別捜査隊

National Cyber Unit

◆インドネシア当局が逮捕（2023年7月）



フィッシングツール
「16SHOP」を悪用



海外在住
フィッシング
被疑者

捜査

大阪府警察

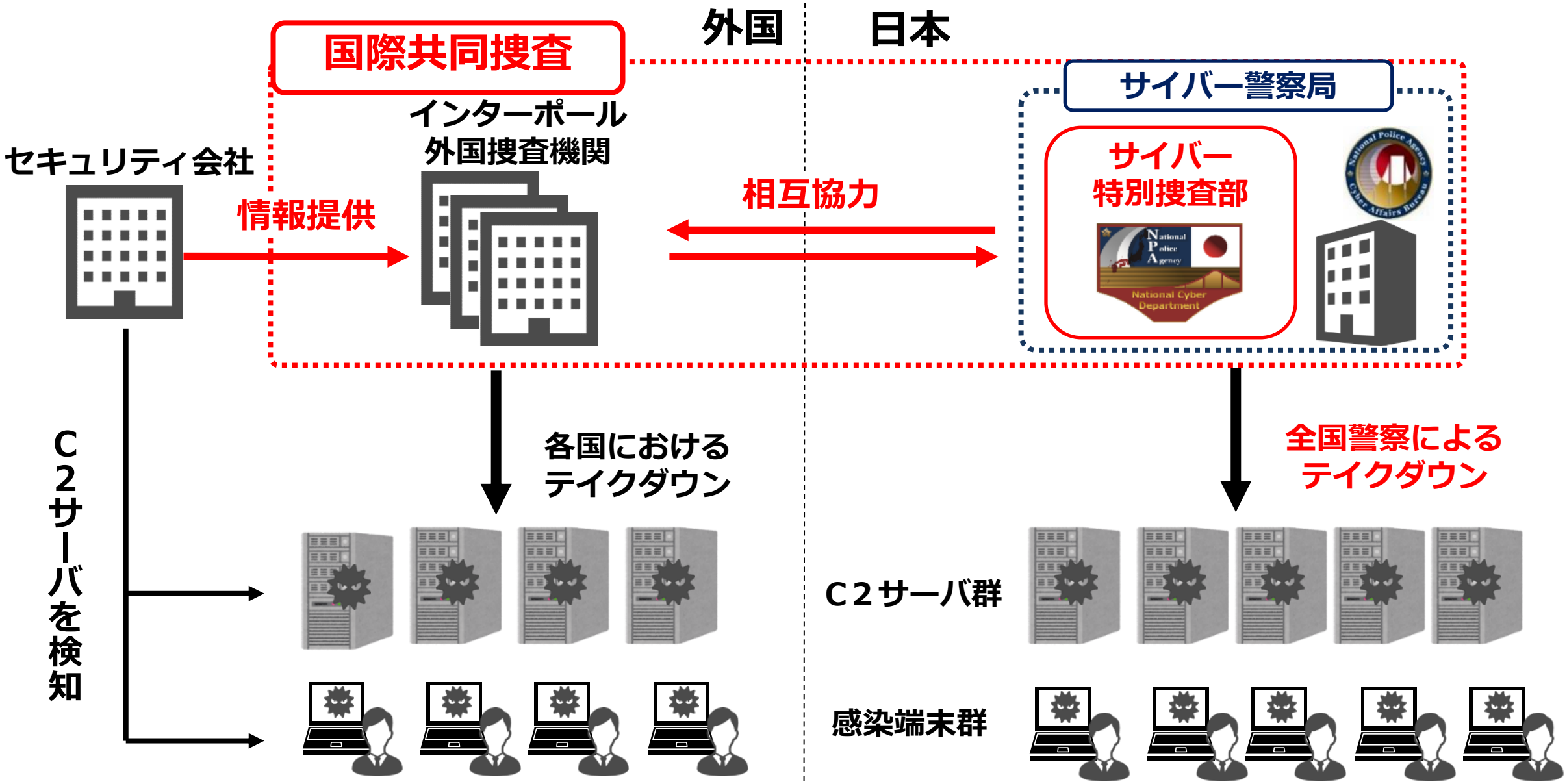
逮捕（2022年8月）

クレカ情報を
悪用した
国内在住被疑者

共謀

出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

国際共同捜査による「インフォスティーラー」のテイクダウン

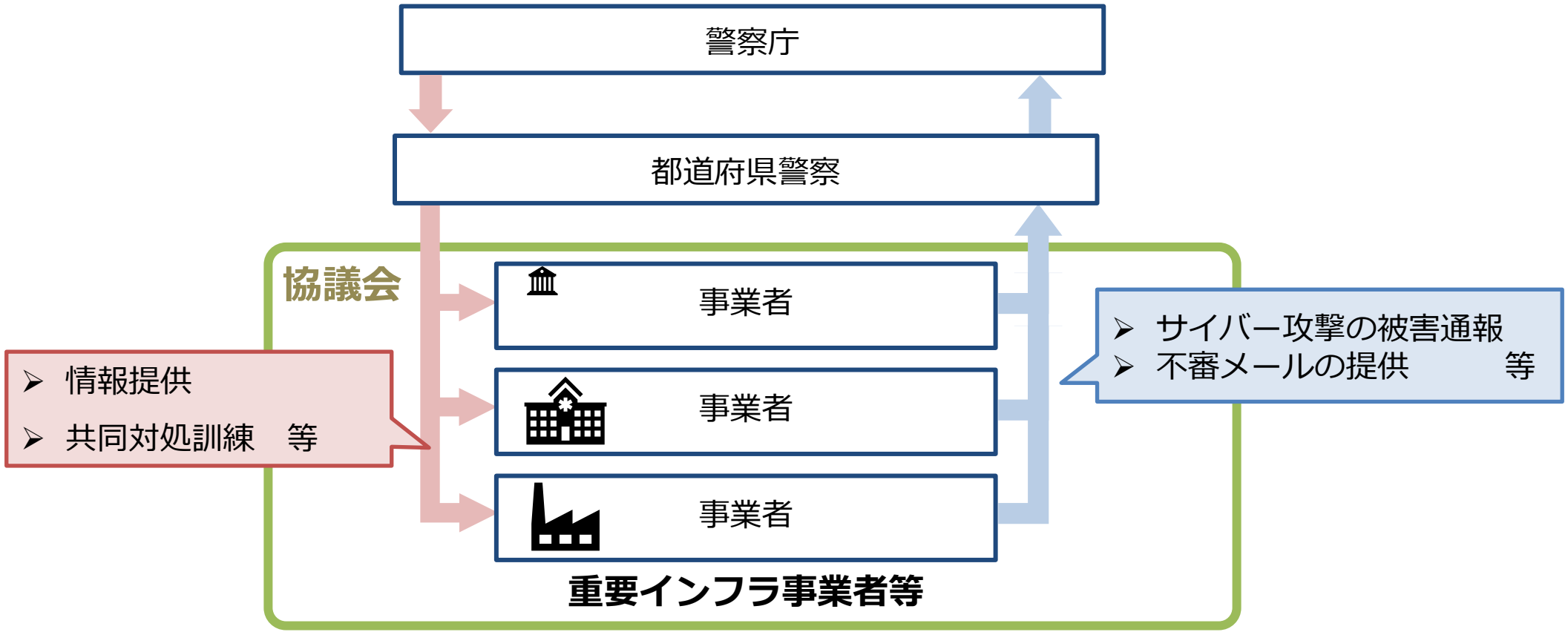


出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

官民連携

官民連携による被害防止

- 都道府県警察ごとに管内の重要インフラ事業者等をメンバーとする**「サイバーテロ対策協議会」を設置。**
- **サイバー攻撃に関する情報共有や共同対処訓練を実施。**



被害に遭うことを想定した対策

○ **サイバー攻撃を想定した「業務継続計画（ＢＣＰ）」の策定**

- データ暗号化からの調査・復旧作業は、物理的損傷からの復旧とは別物
- 災害と異なり自組織だけが被害を受けており、影響度に応じて広報等が必要
- 関係機関（警察、個人情報保護委員会、所管省庁等）への通報・相談が必要

※　通報・相談により、広報時に「警察と連携して対応中」等との記載が可能

○ **オフラインを含む複数のバックアップ取得**

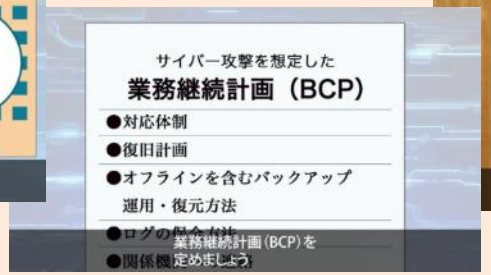
- ランサムウェア攻撃では、オンラインバックアップは暗号化の可能性大

○ **情報流出有無や侵入経路の調査に必要不可欠なログの取得**

○ **訓練（バックアップからの復元、連絡、広報等）の実施**

○ **警察との関係構築**　→次ページ詳細

詳しくは「政府広報」→「中小企業で被害多数　ランサムウェア」をチェック！



あなたへのお願い。
政府広報

政府広報：https://www.gov-online.go.jp/useful/202506/video-298784.html

被害復旧作業における警察との連携

被害企業

被害発生

◎ **「警察と連携して対応中」と広報可能。**ステークホルダーに対して**コンプライアンス重視姿勢**を訴求。

被害拡大防止・復旧に向けた初動対処

- 被害拡大防止に向けたネットワーク隔離
- 復旧調査に向けたデータ・ログの保全

◎ **被害拡大防止・復旧のために必要な初動対処について警察から情報入手。**

◎ **ランサムウェアの種別によっては復号ツールによる復旧の可能性も。**

通 報

連携窓口の設定

捜査協力

情報提供

警　察

認 知

◎ 迅速に初動体制を確立。被害企業の状況を早期把握し、可能な情報提供・助言内容を検討。

証 拠 保 全 ・ 捜 査

- 保全データを入手し**国際捜査**

復 号 事 例

◎ **「Lockbit」等の復号ツールをサイバー特捜部で開発**。被害企業等のデータを復号。

◎ その他のランサムウェアで助言により、復号できた事例も。

「名古屋港ランサムウェア攻撃」（令和５年７月発生）国交省検証報告書

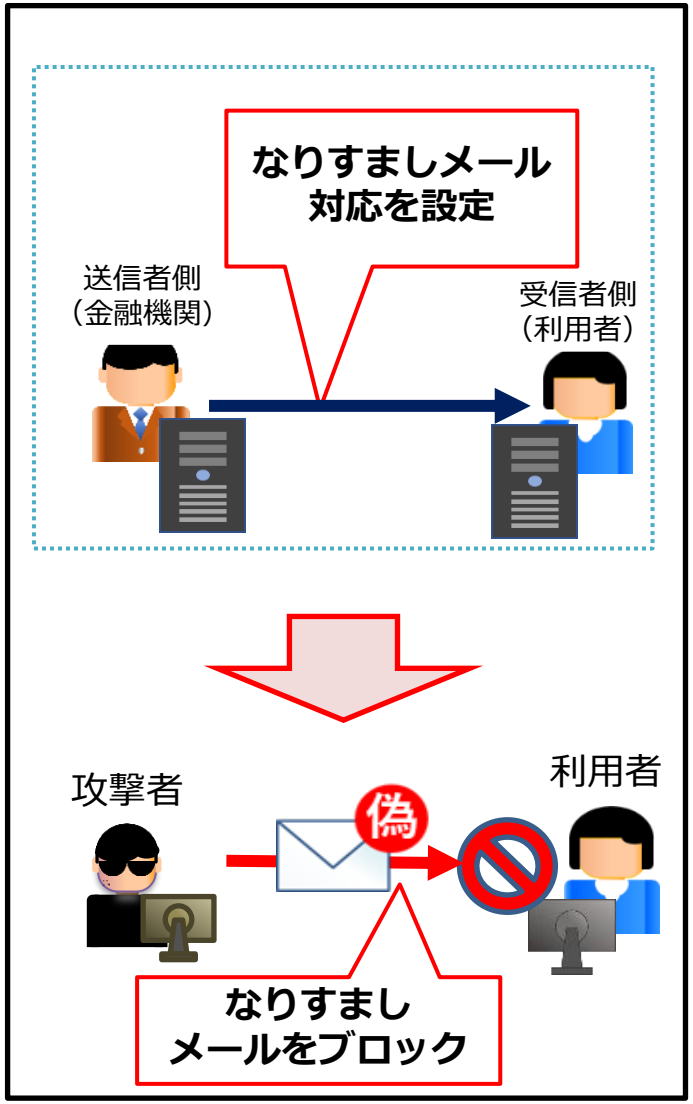
日頃より情報セキュリティ研修等の場を通じて愛知県警と名古屋港運協会との関係が構築できていたこと。

これにより、事案発生時の相談、対応がスムーズになされた。

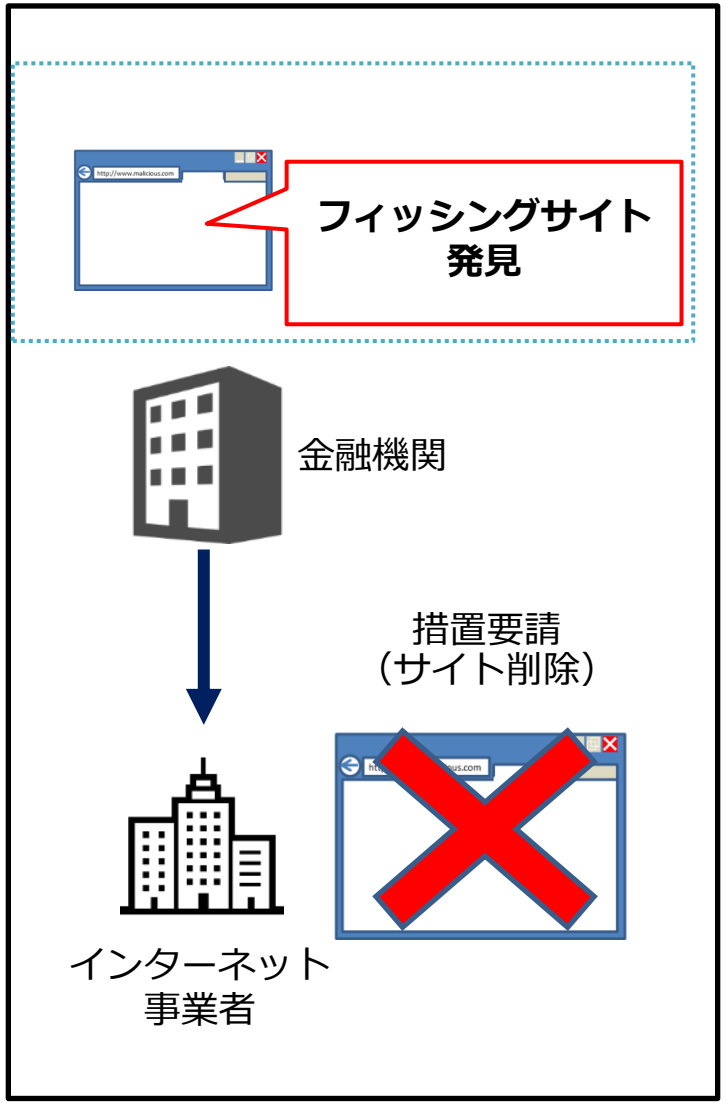
金融機関に対するフィッシング対策の要請（金融庁連名・本年７月）

DMARCの普及促進

※ Domain-based Message Authentication Reporting and Conformance



フィッシングサイトの閉鎖活動促進

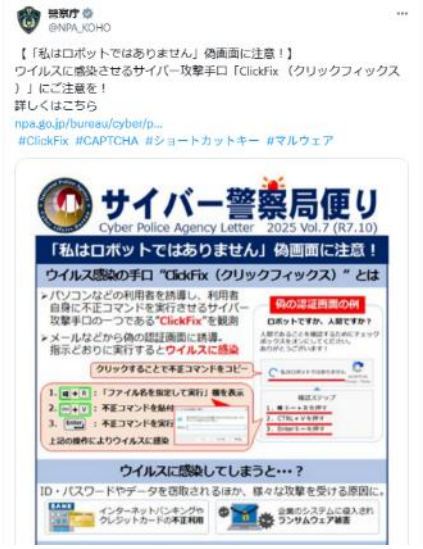


パスキーの導入促進

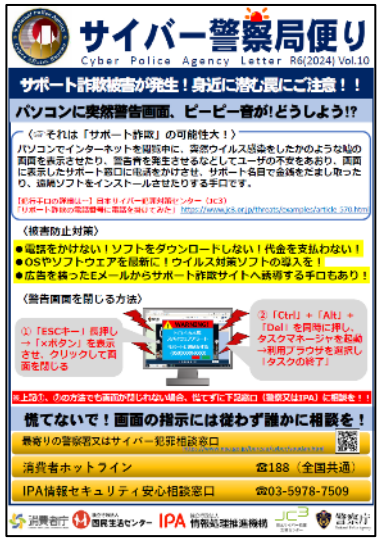
出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

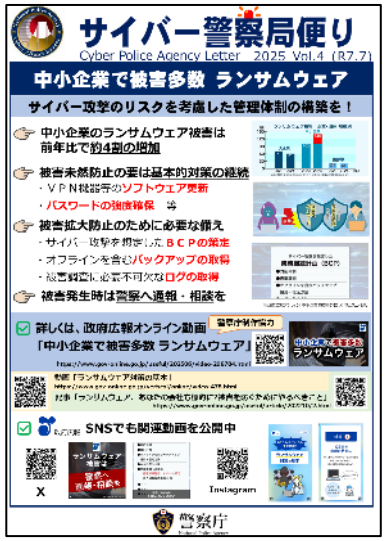
未然防止・拡大防止のために

警察庁 公式X

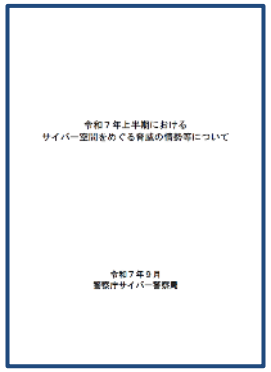


サイバー警察局便り





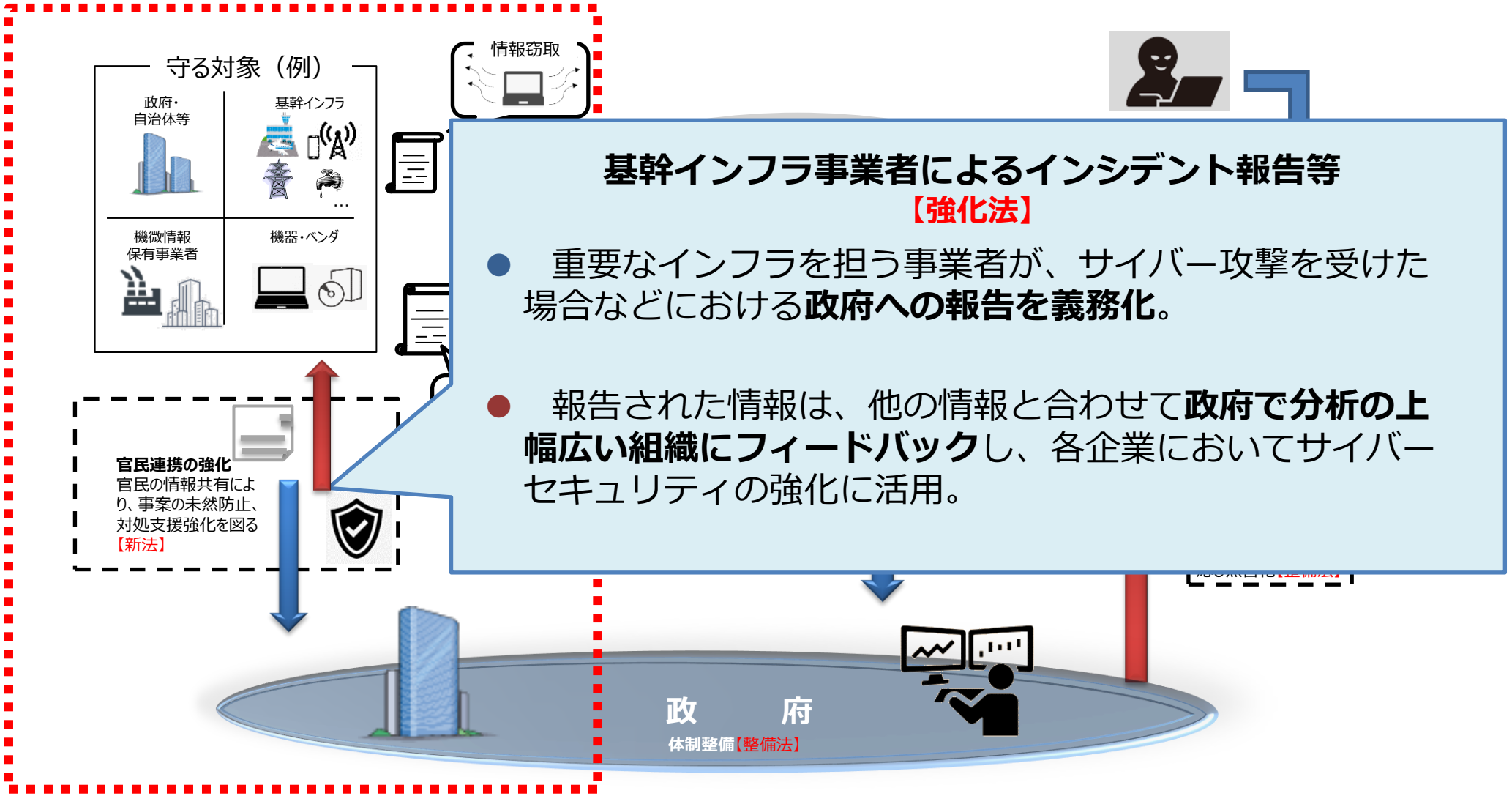
「令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について」



https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

3　今後の課題

サイバー対処能力強化法・同整備法の全体イメージ



出典：内閣官房サイバー安全保障体制整備準備室「サイバー対処能力強化法案及び同整備法案について」を元に作成

人材育成

中途採用・官民人事交流採用のサイバー特捜部の幹部

サイバー特別捜査官として
中途採用（警部補）された幹部警察官

特別捜査課長
丸山　篤　警視正

官民人事交流制度により採用された
幹部警察官

分析官
濵石　佳孝　警視正

出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

「サイバー人材確保・育成方針」の制定（本年３月）

- **現在の人口減少社会において**、極めて深刻なサイバー空間情勢に対処するためのサイバー人材を確保・育成するためには、警察内部の所属・部門間の縦割り等を排し、サイバー部門と警務部門の緊密な連携を中核としつつ、全ての部門が一体となって、その**確保・育成とキャリアパス管理を推進**することが不可欠。
- 以上の基本的考え方を踏まえ、①全ての警察官に対するサイバーに関する教養を推進するなどの**全体の底上げ**と、②警察におけるサイバー人材のキャリアパスを明示しつつ外部にアウトリーチするなどの**高度人材の確保**という双方の観点から、都道府県警察が取り組むべき取組を指示。

サイバー人材の確保

1　試験制度の整備・運用

- ✓ 一般採用試験の前倒し・複数回実施
- ✓ 中途・特別・任期付採用制度の整備運用・リボルビングドアの取組

2　効果的な採用募集活動

- ✓ 高度人材に対するキャリアパス明示（サイバー特捜部出向等）と活躍実例の広報による魅力発信
- ✓ IT関連の広報媒体活用や高等専門学校等への学校訪問の推進
- ✓ 学生対象のサイバーコンテスト開催やサイバー防犯ボランティアの拡大

3　部内のサイバー人材の発掘

- ✓ 部内競技会の開催、経歴・資格の把握を通じた内部人材の発掘

サイバー人材の育成

1　必要な能力の明確化と検定による確認

- ✓ 全警察官に通報・相談受理能力、全捜査員にネットワーク利用犯罪捜査能力、中核サイバー捜査員に高度サイバー事案対処能力を取得させ、検定制度により確認
- ✓ 都道府県警察の昇任試験におけるサイバー関連の出題

2　教養・研修の推進

- ✓ 司令塔となる指導・教養班の設置
- ✓ 専務任用専科等の学校教養におけるサイバー教養の拡充
- ✓ 警視庁等他都道府県警察への派遣・出向、他部門捜査員のサイバー部門受入れによる職場教養の推進
- ✓ 民間研修への積極的派遣及び民間委託研修受講・民間資格取得を支援

サイバー人材のキャリアパス管理

1　サイバー・警務両部門の緊密な連携

- ✓ サイバー・警務両部門を中核に全部門一体となって、中途・特別採用等の高度サイバー人材を含むサイバー人材のキャリアパスを管理

2　キャリアパス管理に基づく職員の配置等

- ✓ 中途・特別採用のサイバー人材は本部への卒業配置に配慮。昇任配置も希望に応じて配置ポストを検討
- ✓ 署配置を行う場合は、能力と適性を活かすことができるポストを検討
- ✓ 高度人材を処遇するためサイバー部門に所要の幹部ポストを整備
- ✓ 高度サイバー人材を、情報通信部や警察庁サイバー特捜部・サイバー警察局に積極的に出向・派遣

出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

サイバー防犯ボランティア

【主な活動】

- 少年、高齢者などを対象とした**教育活動**
- イベントや街頭キャンペーンなどの**広報啓発活動**
- **サイバーパトロール**

サイバー警察の取組

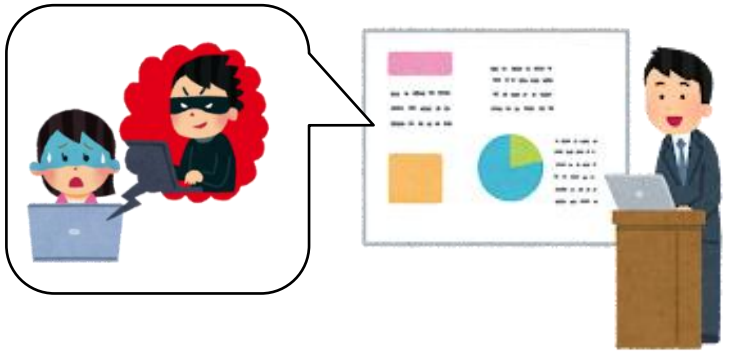
海外機関

国際連携を通じた犯人検挙・抑止

警 察

産業界・学会

官民連携を通じた被害防止対策



実空間と同様「公共空間」である
サイバー空間の安全・安心に寄与

ご清聴ありがとうございました