令和６年１０月１０日
情報セキュリティワークショップ
ｉｎ越後湯沢２０２４

サイバー空間における脅威情勢と警察の取組

警察庁サイバー警察局
サイバー企画課長
阿久津　正好

本日の内容

１　サイバー空間をめぐる脅威情勢

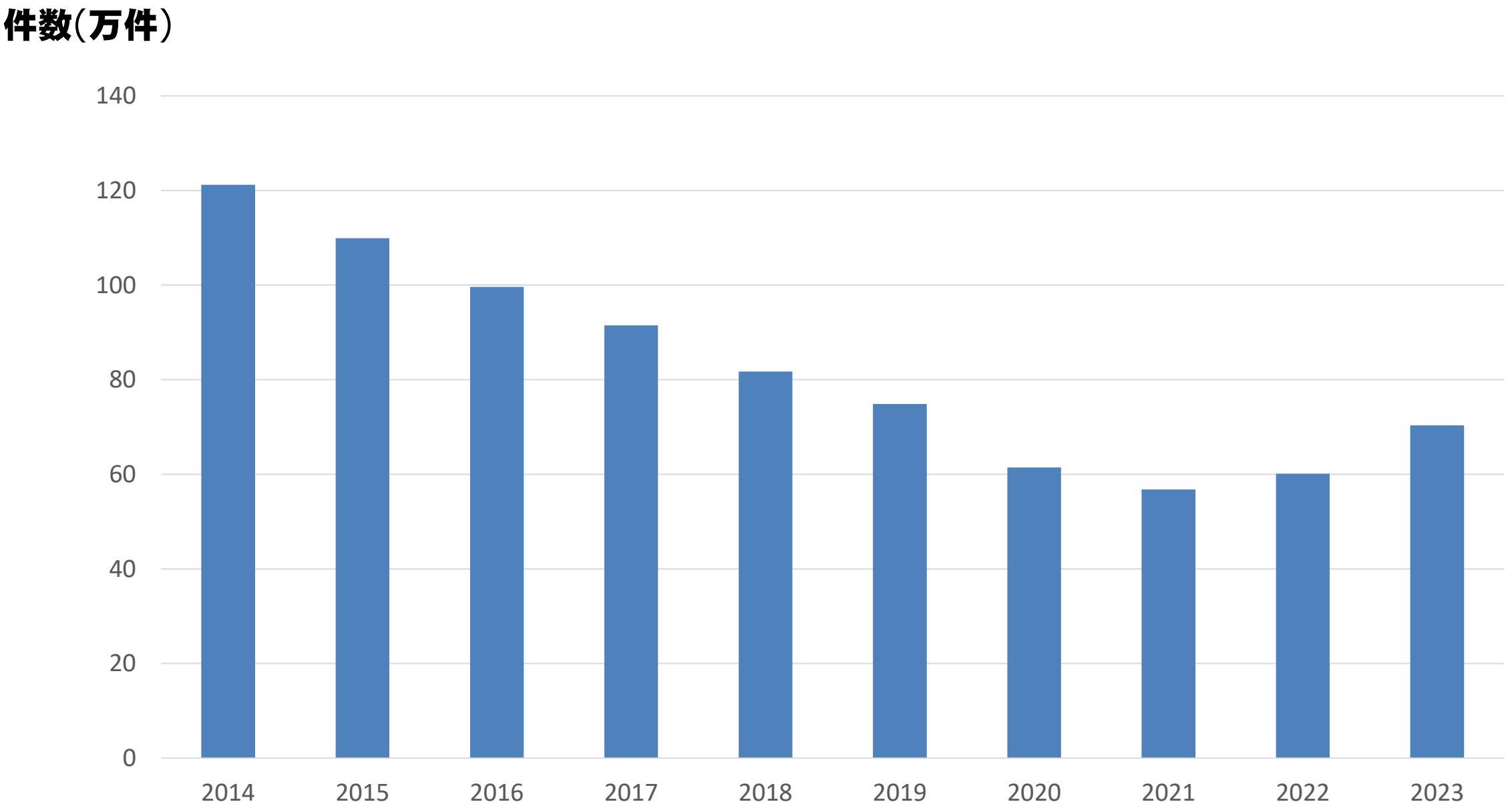
２　被害の未然防止・拡大防止に向けた対策

３　警察における各種取組

サイバー空間をめぐる脅威情勢

治安情勢一般

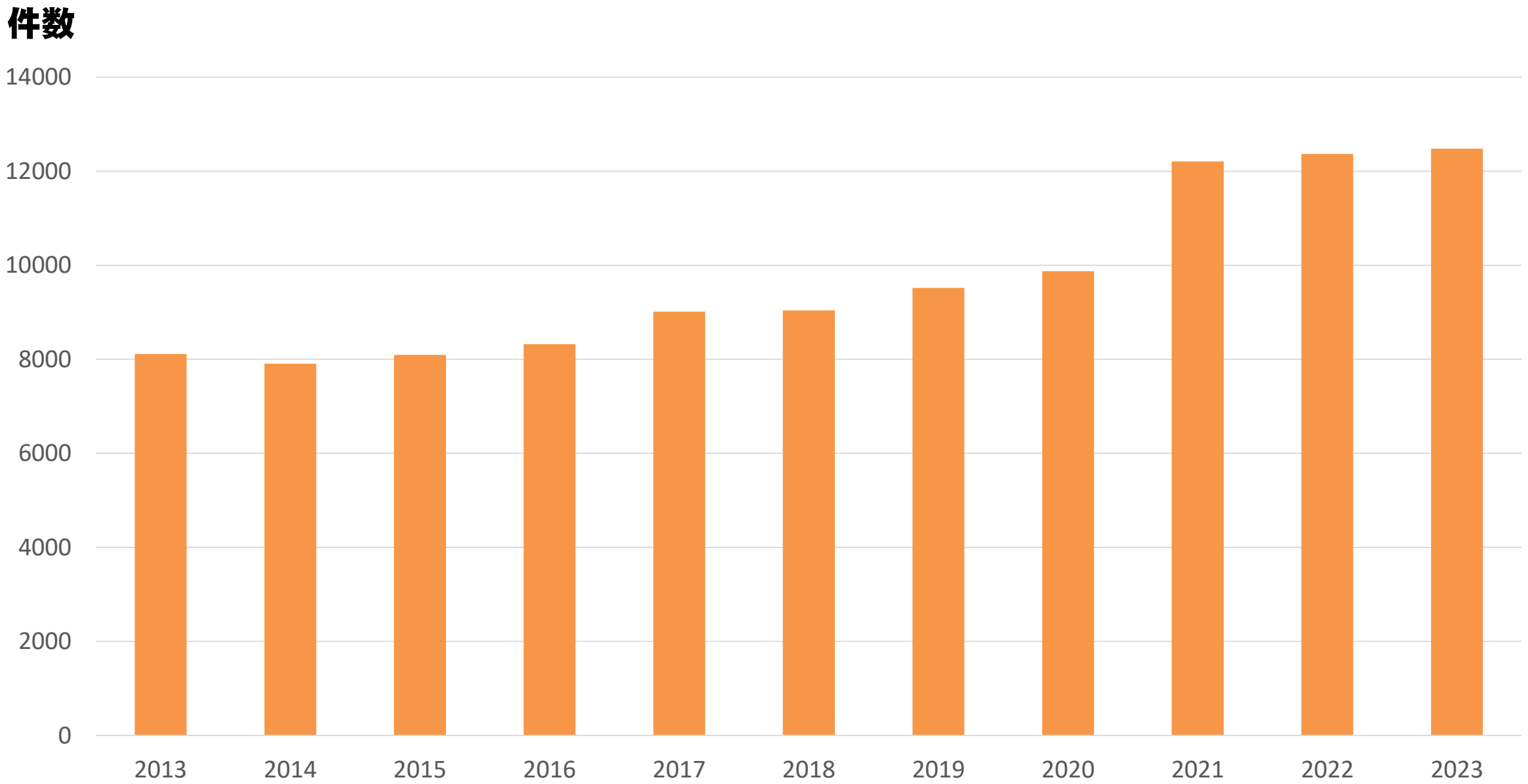
刑法犯認知件数



出典：警察庁「犯罪統計（平成２５年～令和５年）」

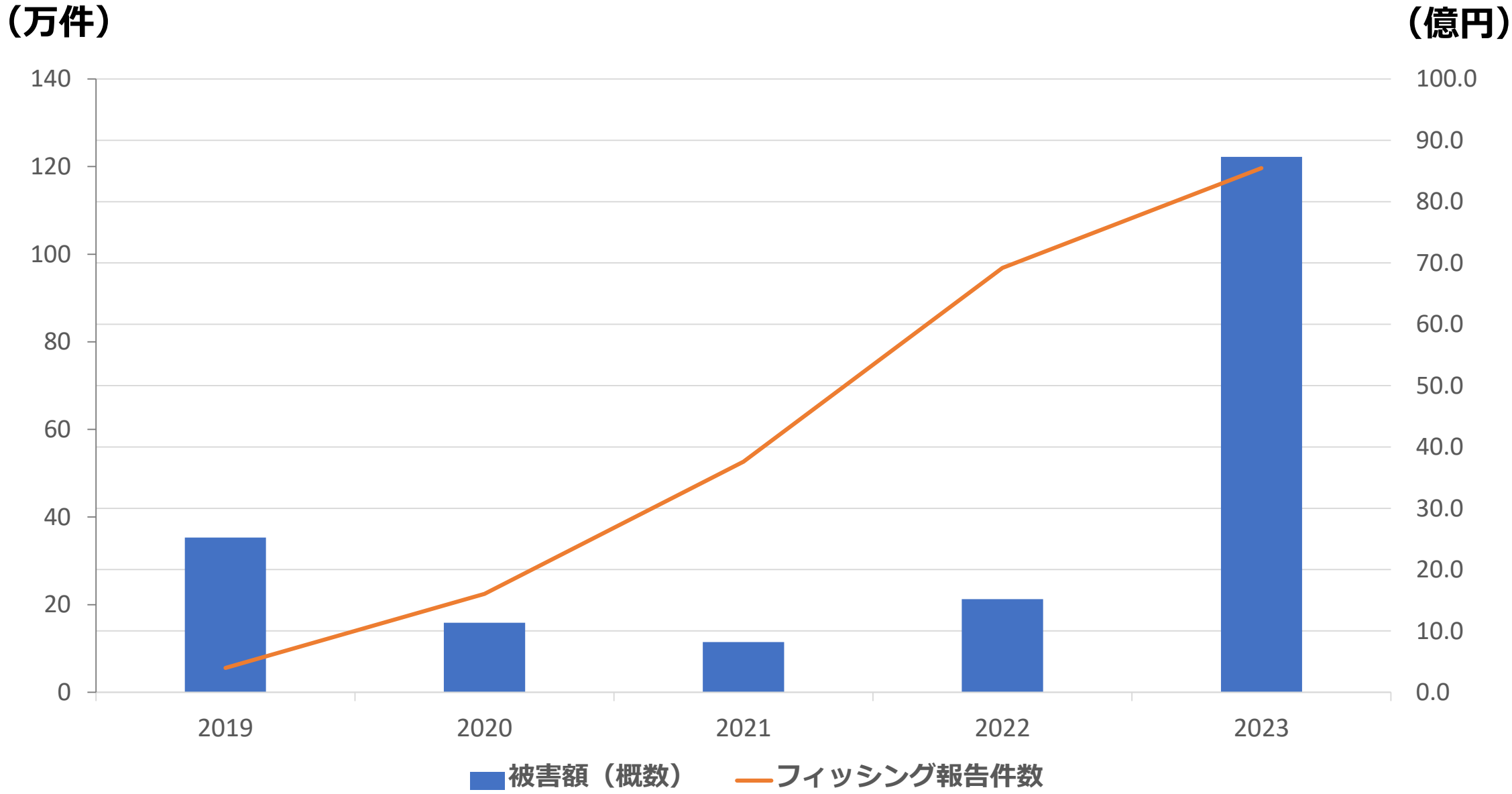
サイバー空間を悪用した犯罪に係る脅威情勢

サイバー犯罪の検挙件数



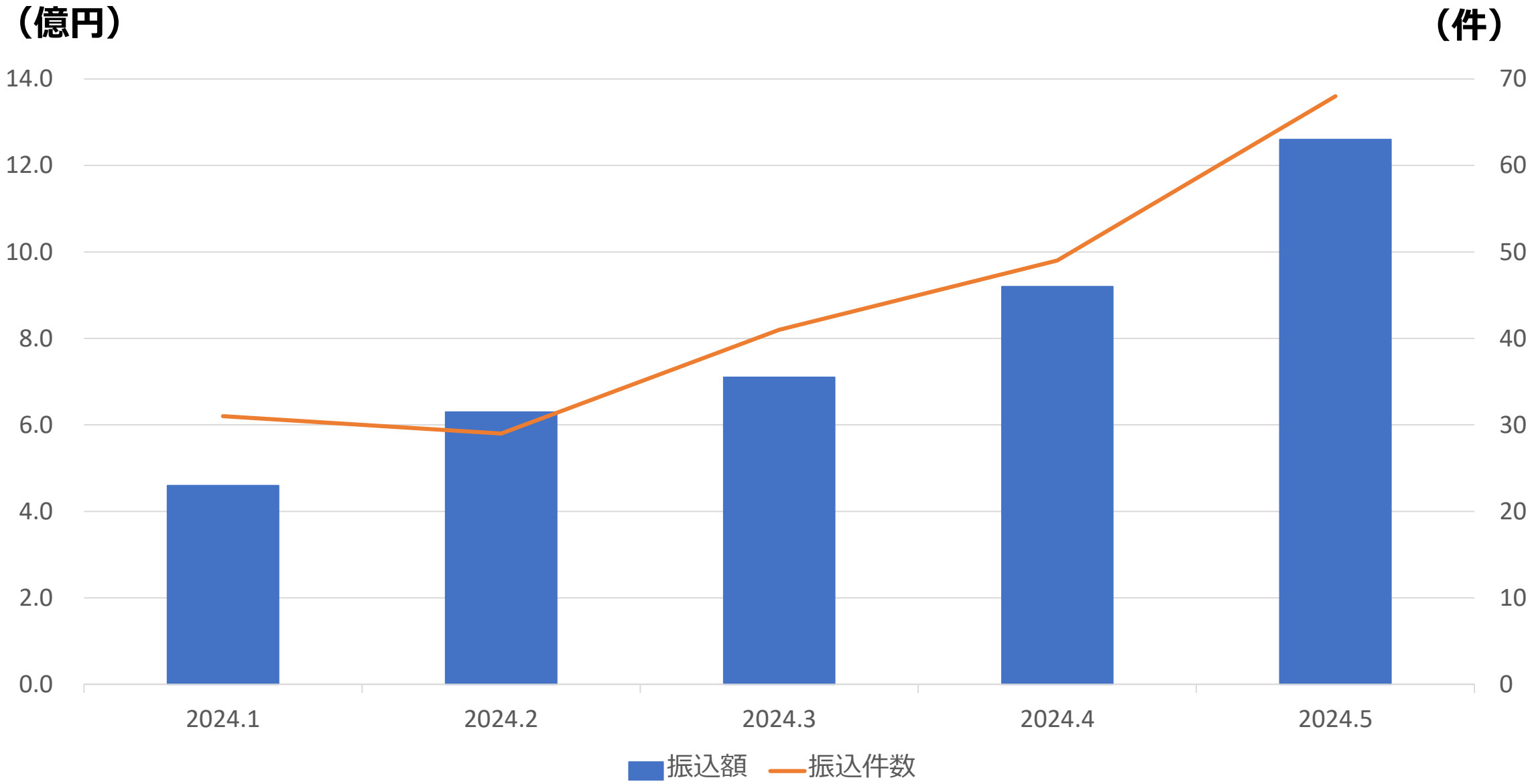
出典：警察庁「犯罪統計（平成２５年～令和５年）」「令和５年におけるサイバー空間をめぐる脅威の情勢等について」

インターネットバンキング不正送金被害額



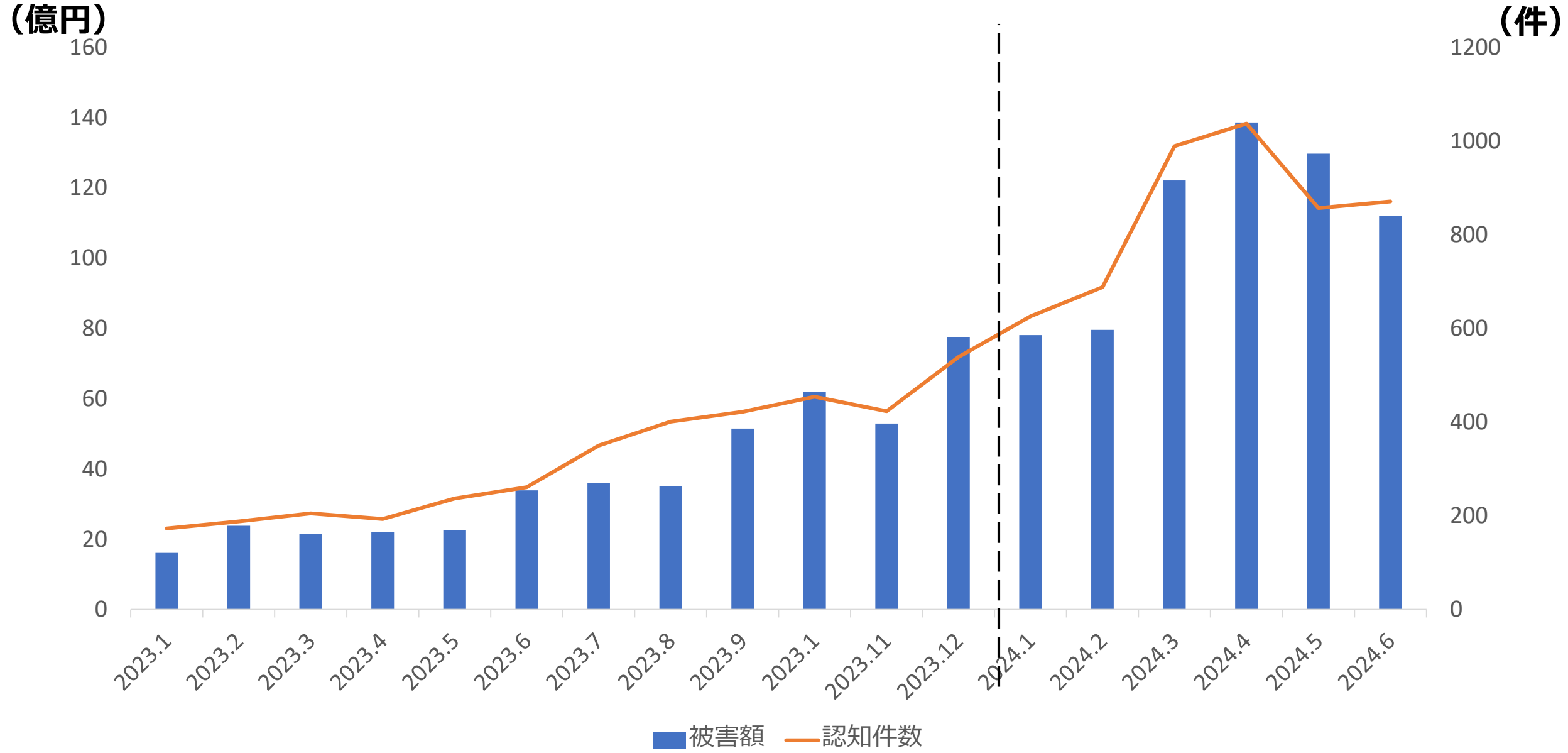
出典：フィッシング対策協議会（https://www.antiphishing.jp/）フィッシングレポート及び月次報告書から作成

特殊詐欺におけるインターネットバンキング振込被害



出典：警察庁「令和６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」から作成

ＳＮＳ型投資・ロマンス詐欺被害

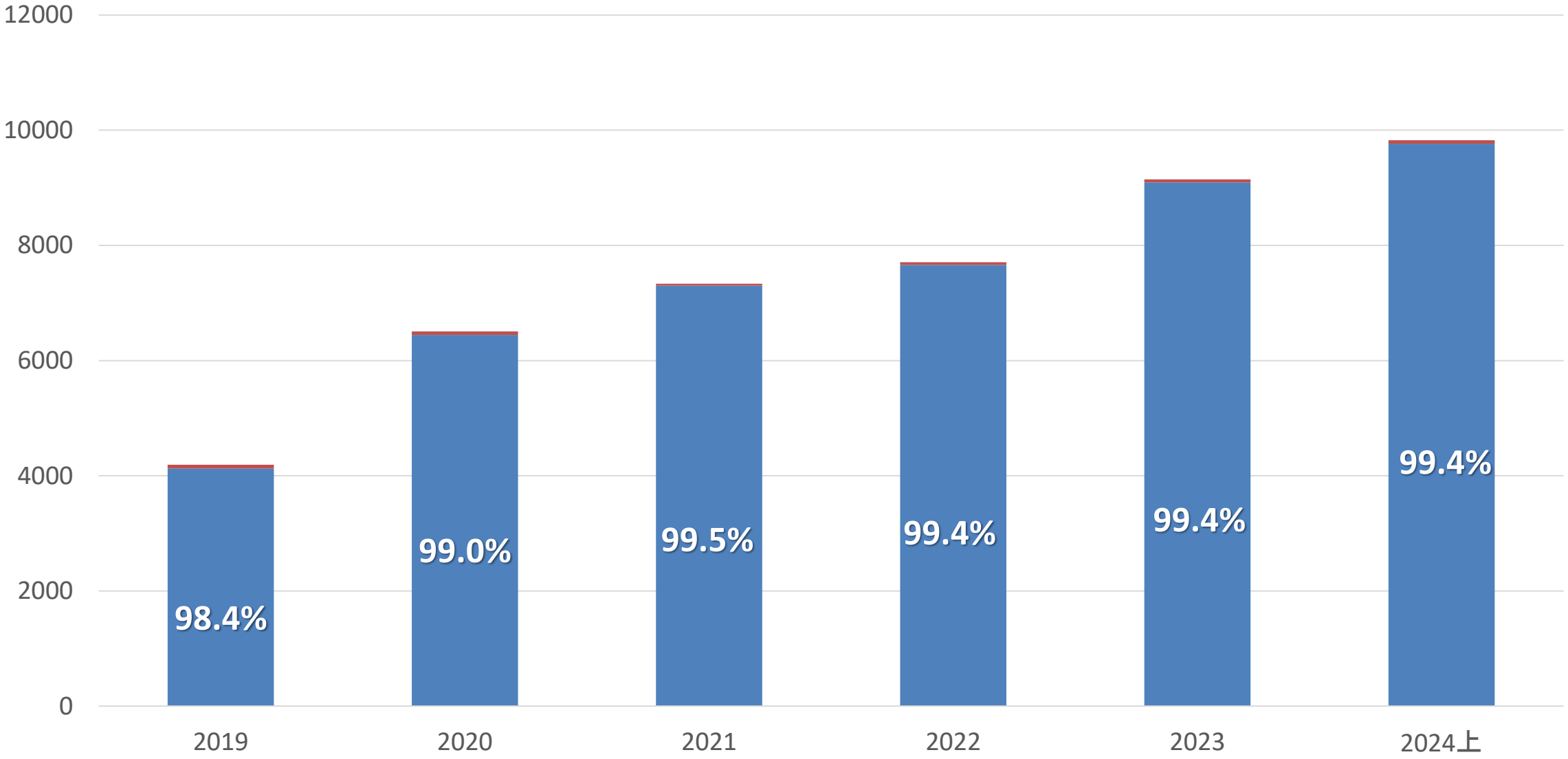


出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」から作成

高度な技術を悪用した脅威情勢

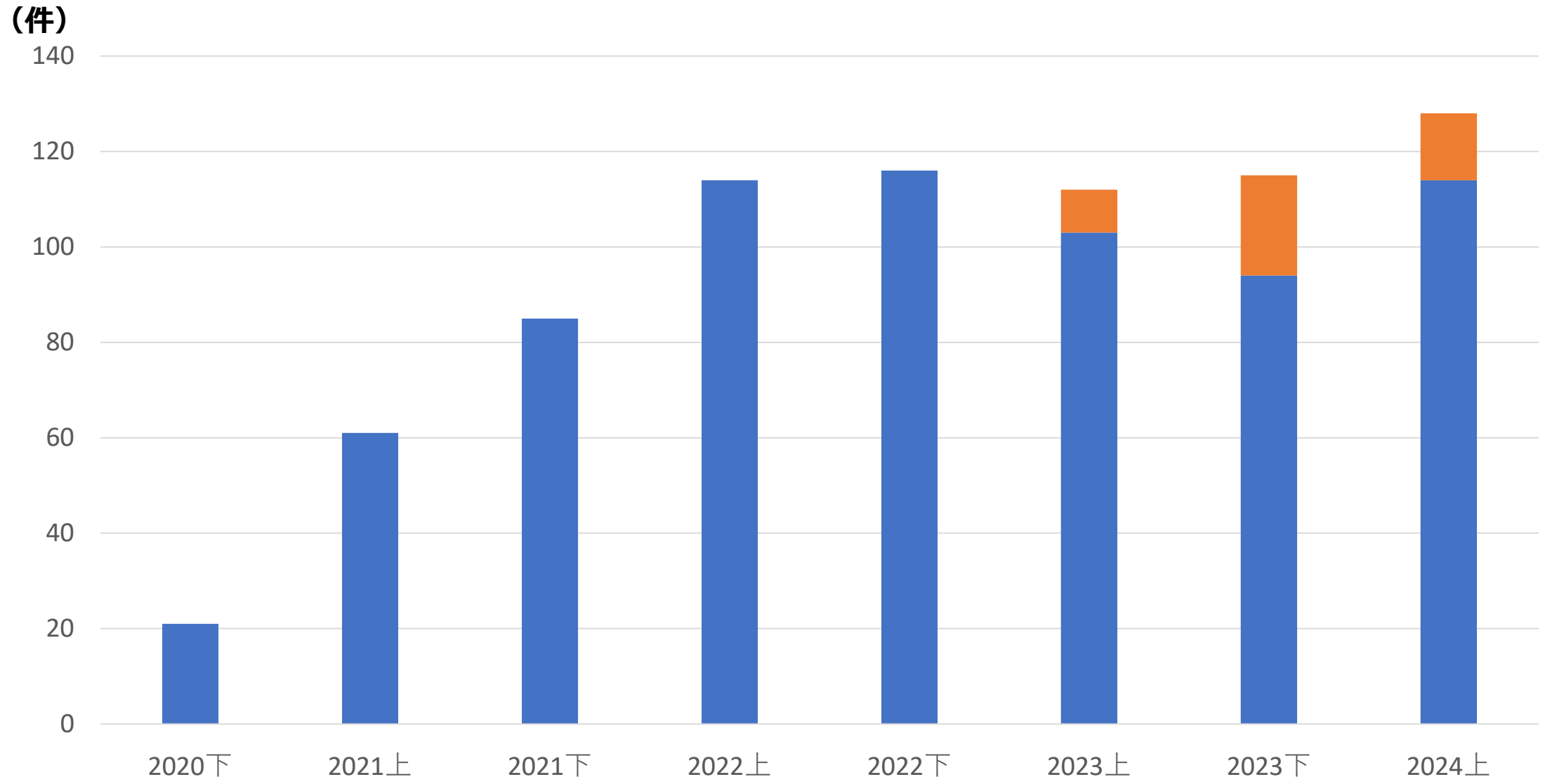
サイバー空間におけるぜい弱性探索行為の観測状況

（件/日・ＩＰアドレス）



出典：警察庁「令和６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」から作成

ランサムウェアによる被害の報告件数

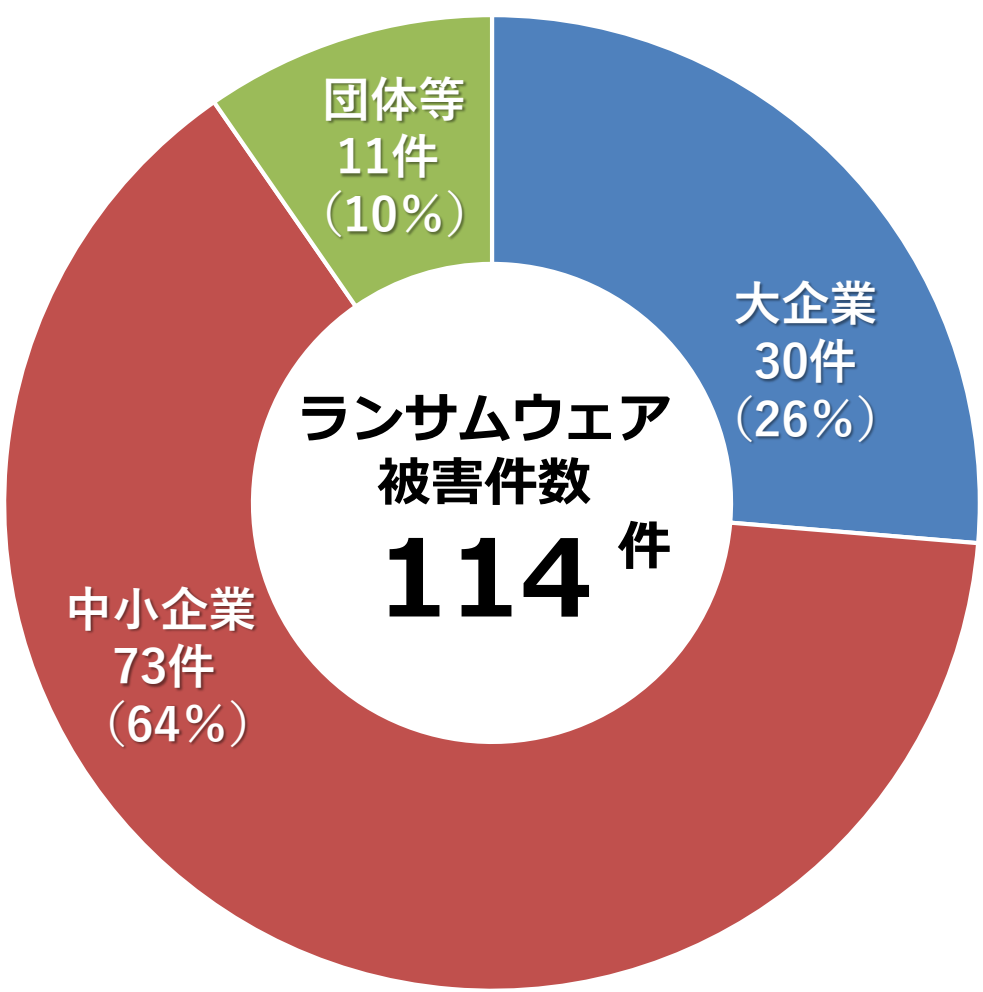


※　2023年以降はノーウェアランサム（オレンジ）を含む。

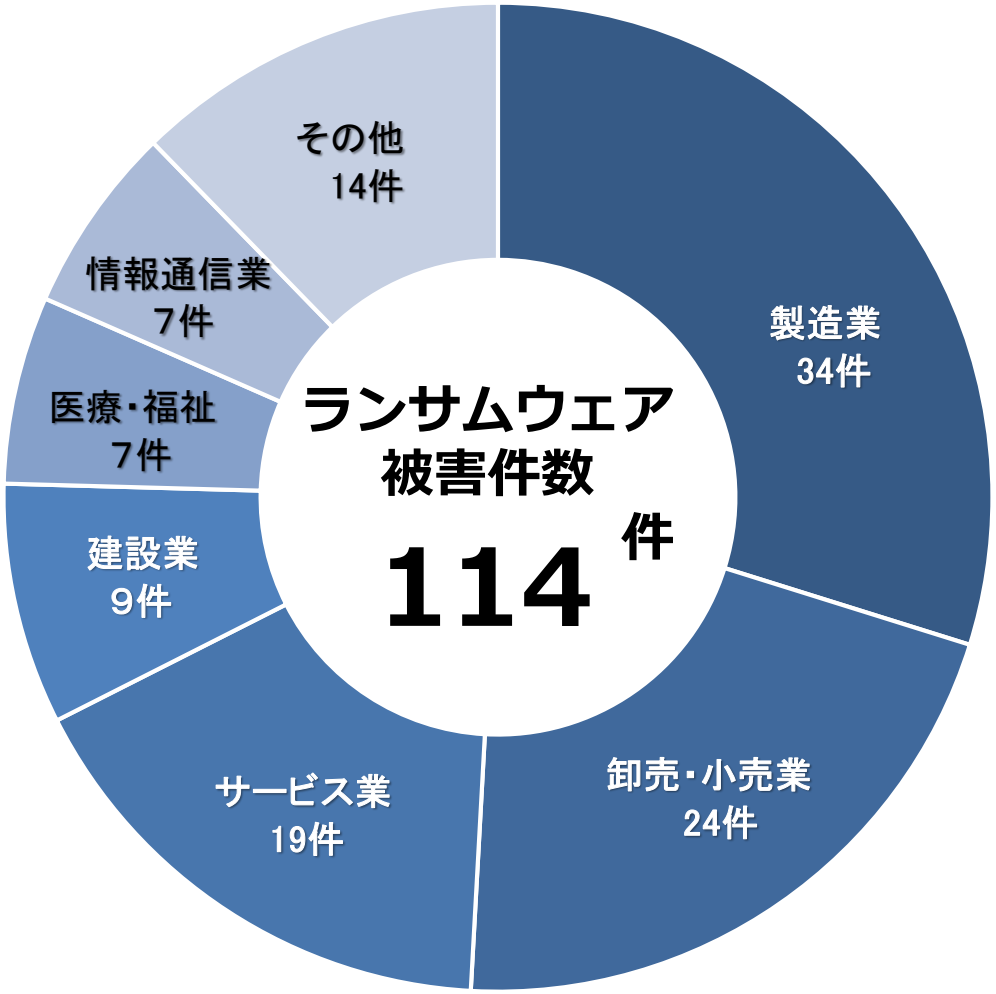
出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」から作成

ランサムウェア被害企業規模・業種別報告件数

規模別



業種別



※　図中の割合は小数点第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。

出典：警察庁「令和６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」から作成

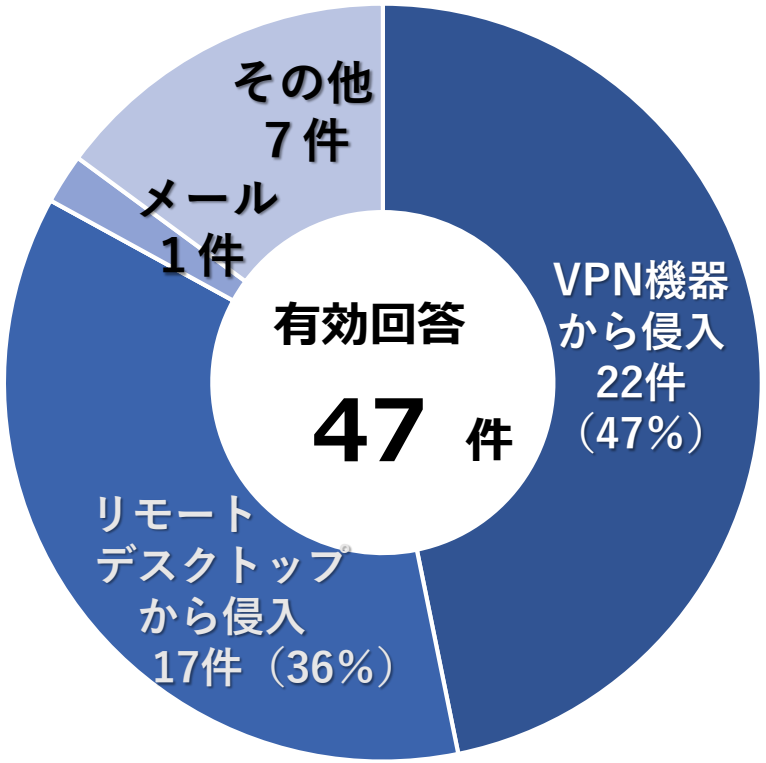
被害の未然防止・拡大防止に向けた対策
～ランサムウェアを例に～

被害の未然防止

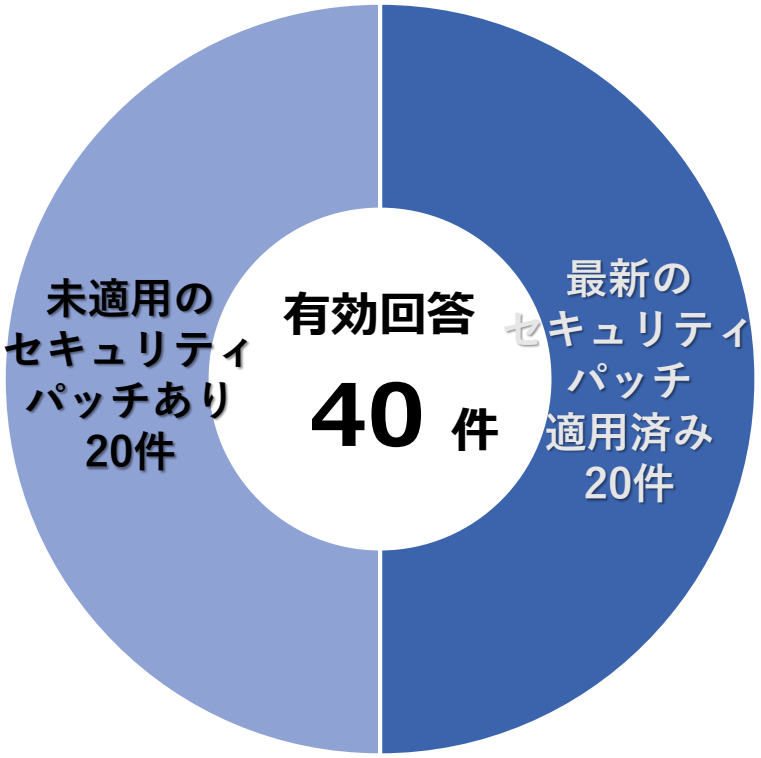
ランサムウェアの感染経路

【調査結果（感染経路）】

感染経路



感染経路のパッチ適用状況

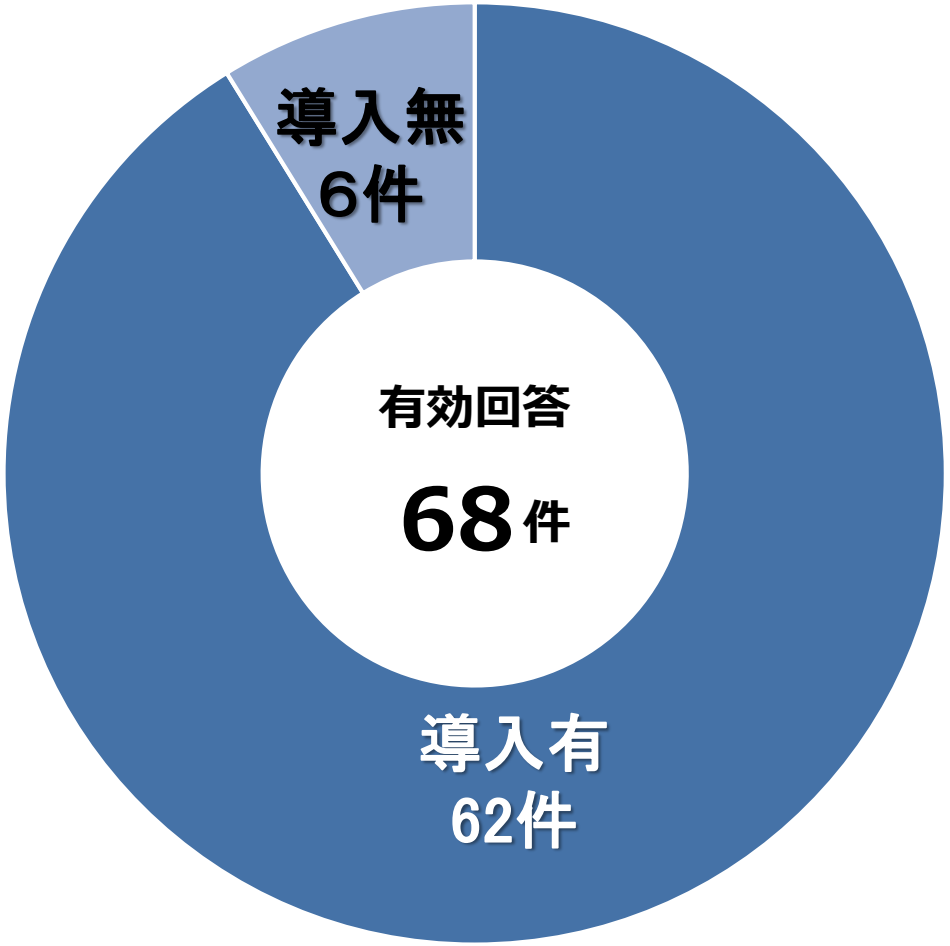


- ○ セキュリティパッチ適用の徹底
- ○ 認証情報の強度向上、厳正な管理
- ○ 機器の設定不備対策

出典：警察庁「令和６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」

ウイルス対策ソフト等の導入状況

【調査結果（導入状況）】



○　ウイルス対策ソフト等は
常に最新の状態に

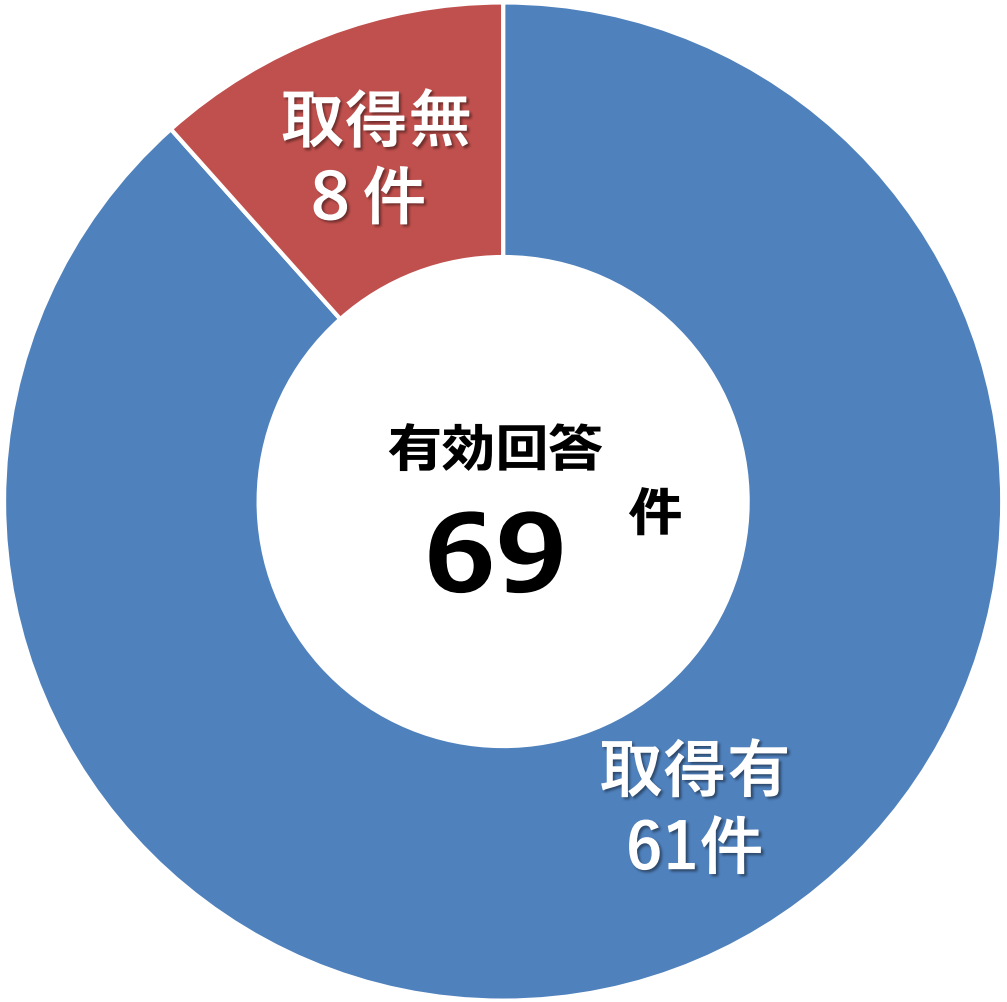
○　**多層防御**
-EDRによる異常検知
-FWによる侵入防止　等

出典：警察庁「令和６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」

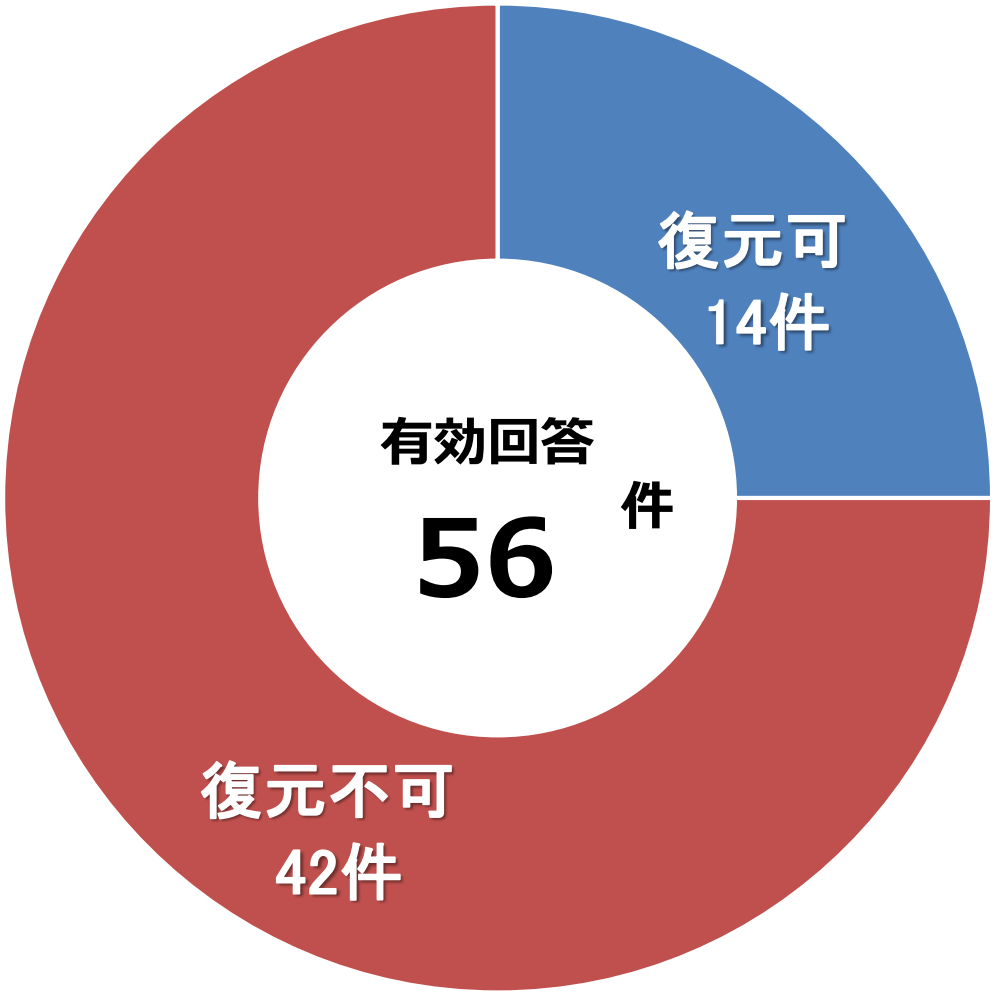
被害の拡大防止

バックアップの取得・復元状況

【調査結果（取得状況）】



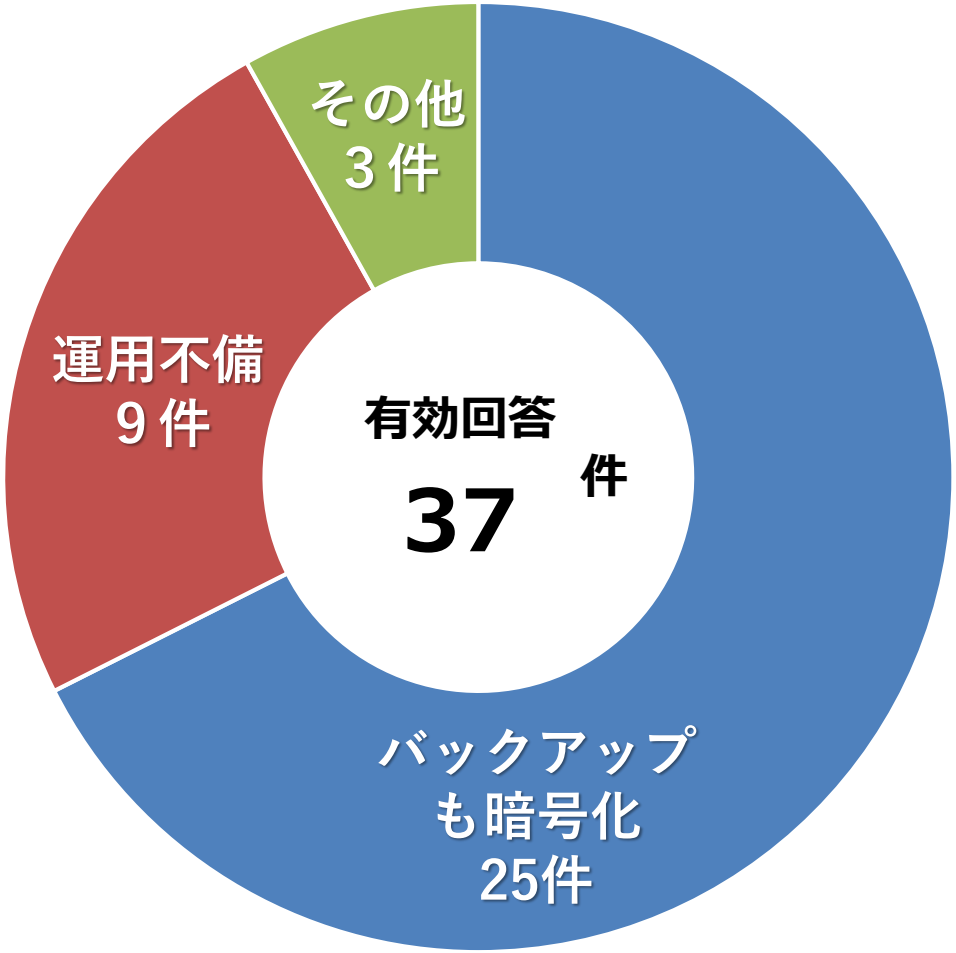
【調査結果（復元結果）】



出典：警察庁「令和６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」から作成

バックアップから復元できなかった理由

【調査結果（不可理由）】



○ **オフラインバックアップ**

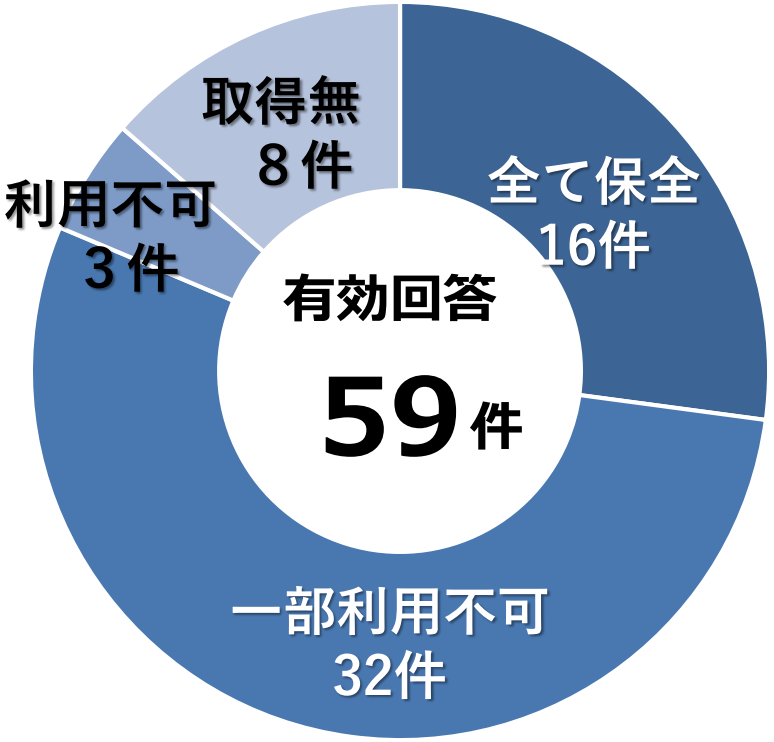
○ **資産の性質を勘案して、
オフライン／オンラインを
組合せた運用を**

出典：警察庁「令和６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」

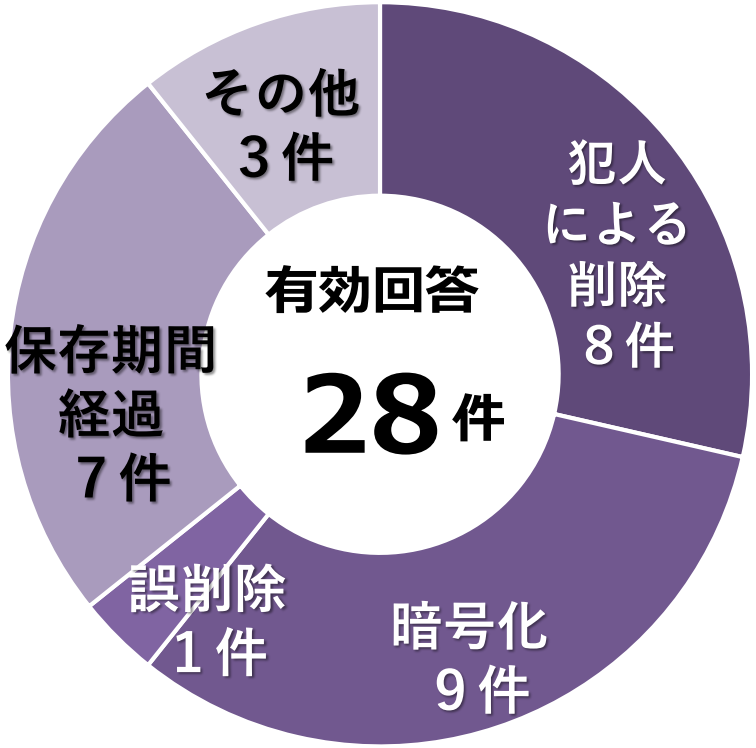
ログの保全状況・使用可否

【調査結果（ログ状況）】

ログ保全状況



ログが利用できなかった原因

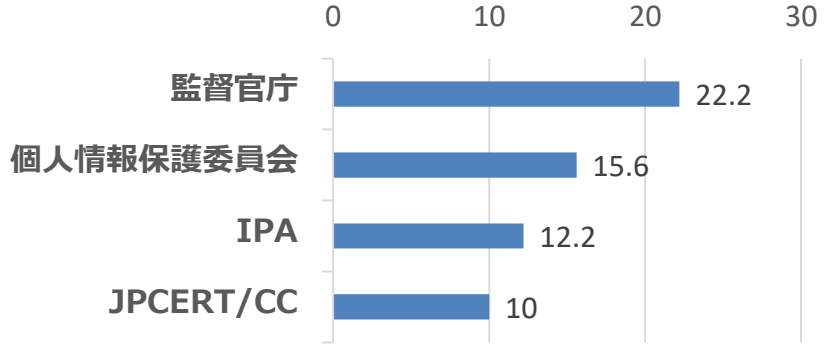


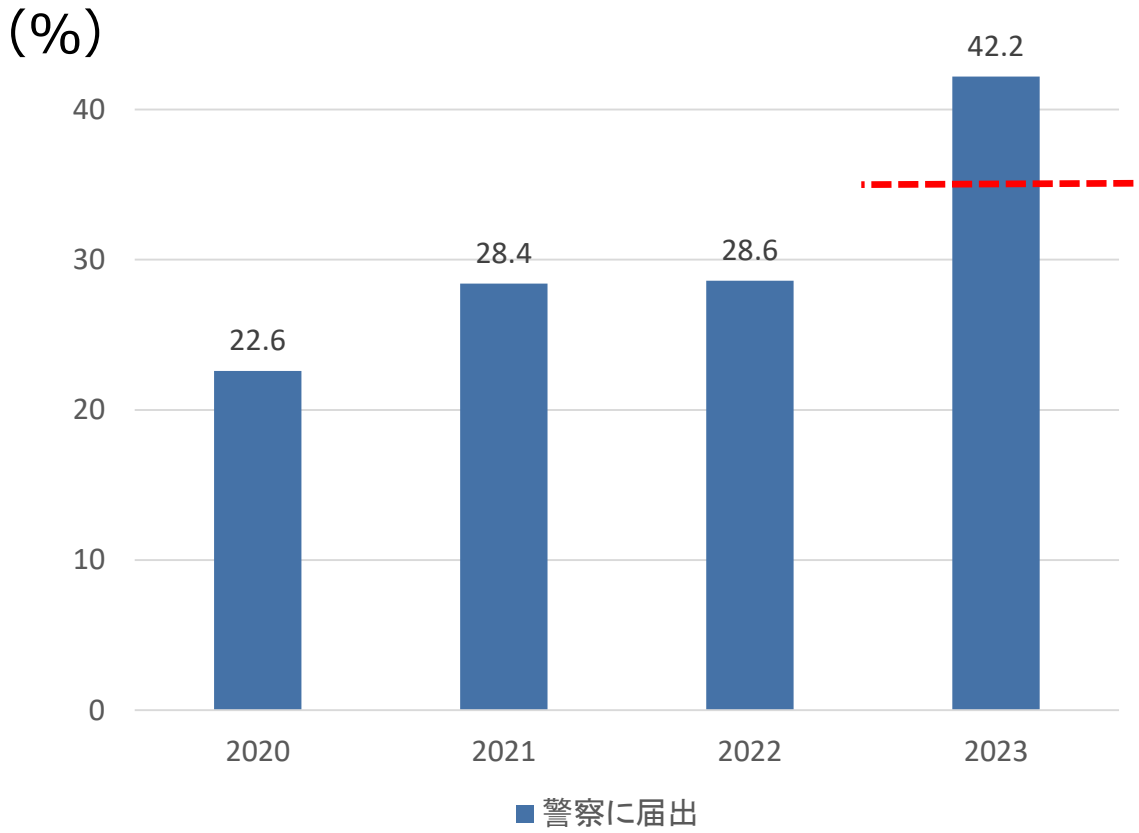
復旧のため、
侵入経路/被害特定に
ログ解析は不可欠

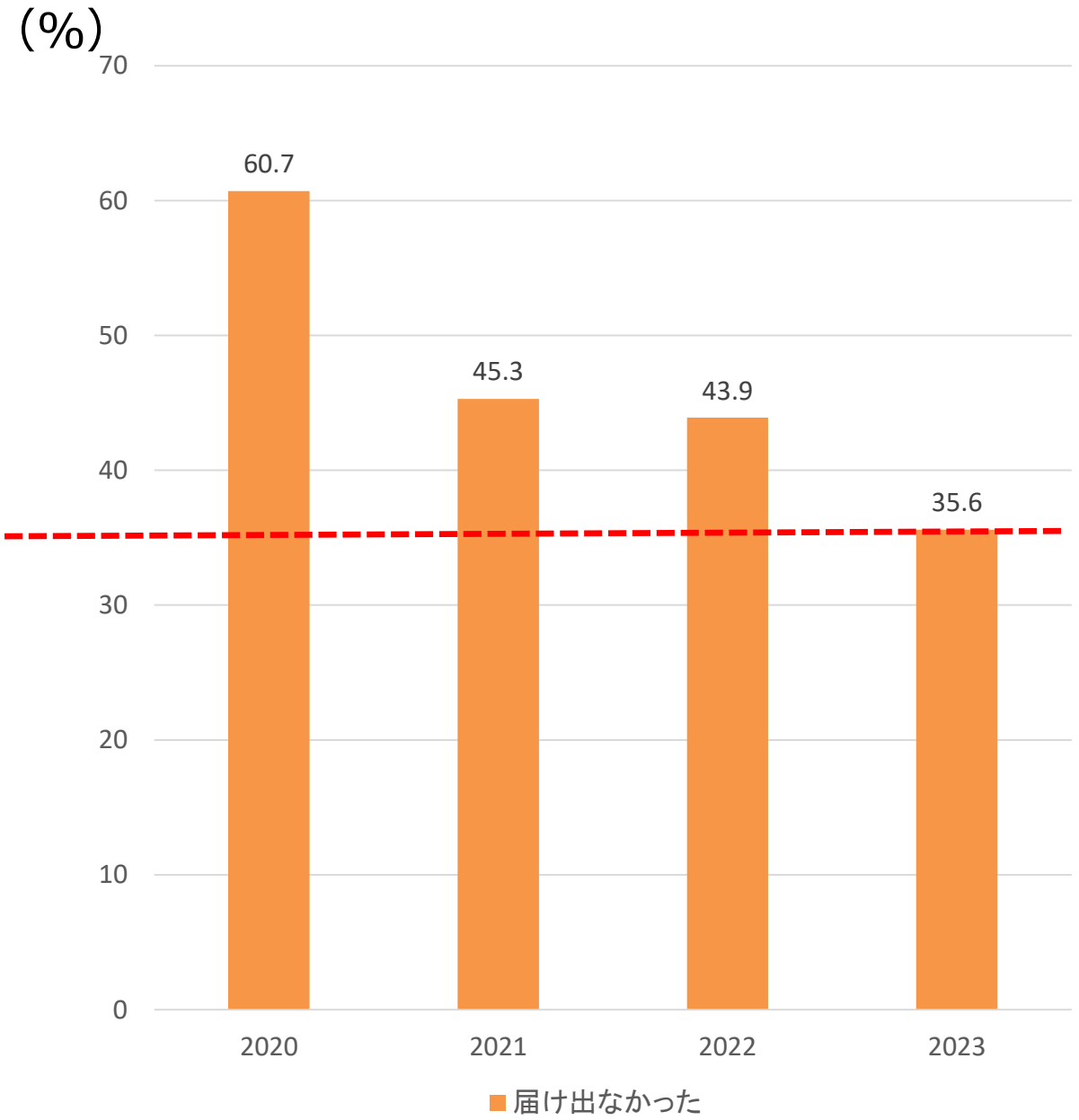
- ○ **サーバ・VPN機器等、多面的なログ取得**
- ○ **オフライン等による保存・管理**

出典：警察庁「令和６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」

警察への通報状況







出典：警察庁「不正アクセス行為対策等の実態調査」

被害に遭うことを想定した対策

■　警察との関係構築

- 事案発生時の相談・対応の円滑化

「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」（名古屋港報告書抜粋）

■　バックアップの取得

- 原因分析のためのログも
- 長期・短期の複数バックアップを

■　業務継続計画（ＩＴ－ＢＣＰ）の策定

- 役割・責任分界点の明確化
- サイバー攻撃によるシステム障害を想定したものを用意
- 訓練を通じた対応手順の確認
- 監査による実効性の点検・是正

警察における各種取組

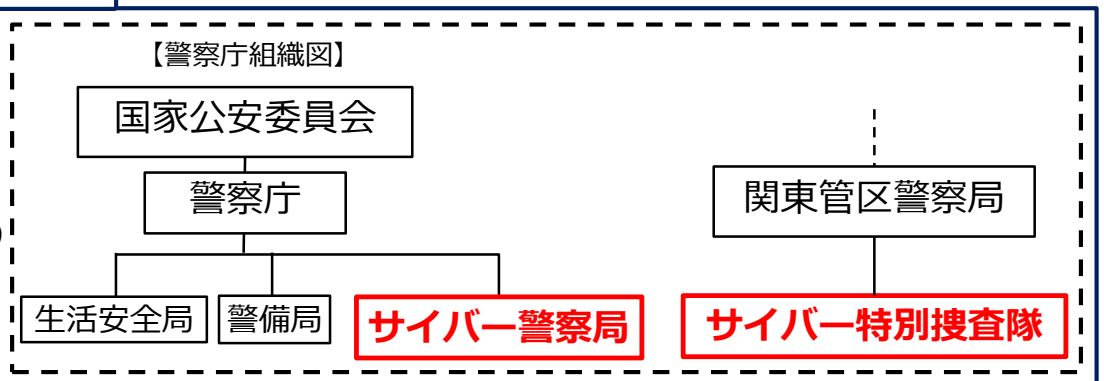
サイバー警察局・サイバー特別捜査部の設置

サイバー警察局・サイバー特別捜査隊の設置

サイバー警察局・サイバー特別捜査隊

Ⅰ　警察庁にサイバー警察局を設置

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



サイバー警察局・サイバー特別捜査隊の取組

海外機関 ⟷ **警 察** ⟷ **産業界**

国際連携を通じた犯人検挙・抑止

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

官民連携を通じた被害防止対策

関東管区警察局サイバー特別捜査部の設置

- 令和６年４月、関東管区警察局サイバー特別捜査隊を発展的に改組。
- 新たに設置したサイバー特別捜査部は企画分析課・特別捜査課で構成。
  捜査のみならず、情報収集・分析機能を更に充実強化。

令和４・５年度

サイバー特別捜査隊

組織改編
増員

令和６年度

サイバー特別捜査部

企画分析課

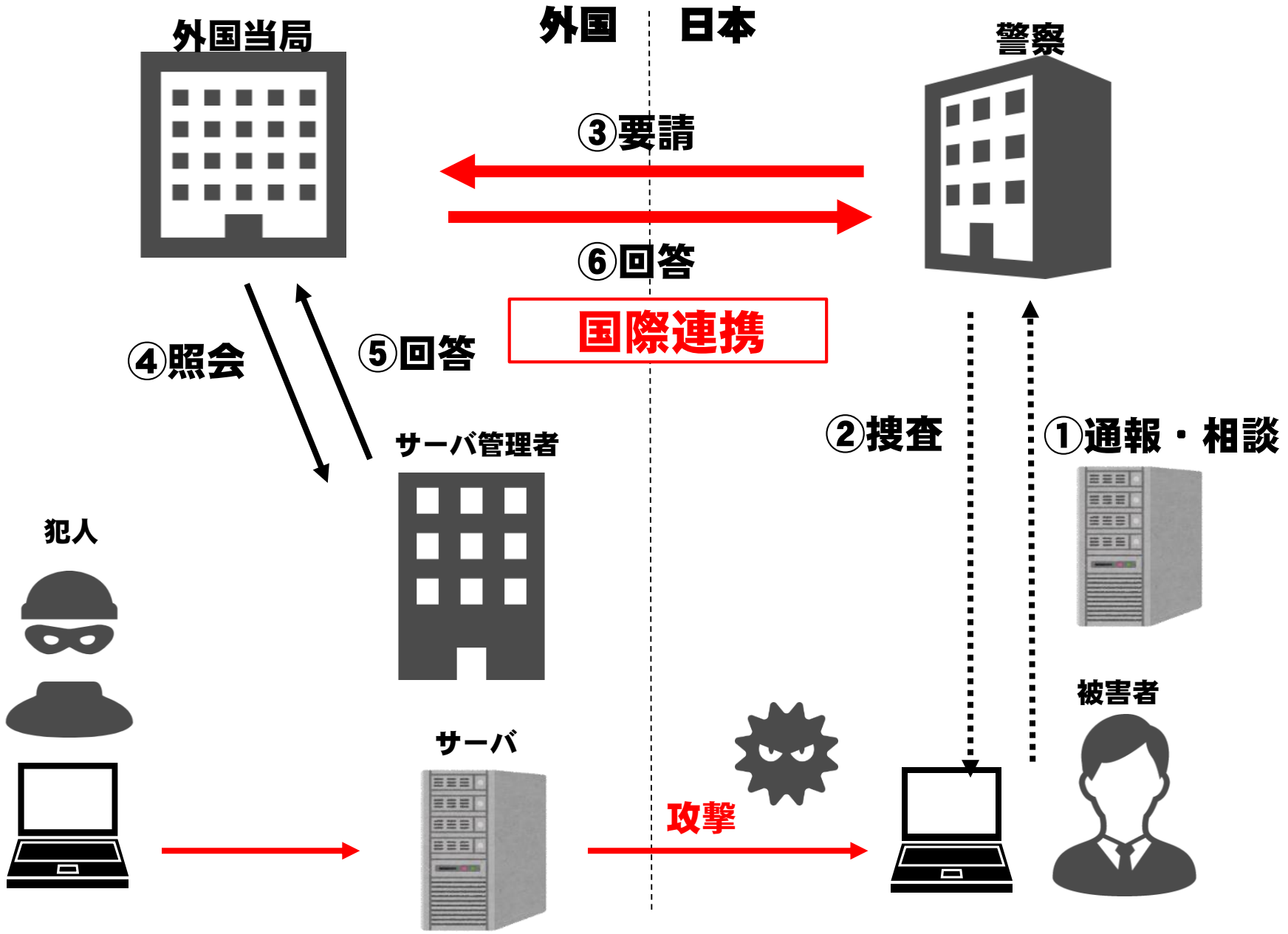
重大サイバー事案に関する情報収集・分析

特別捜査課

重大サイバー事案に係る犯罪の捜査

国際連携による被疑者の検挙等

海外からのサイバー攻撃と捜査の仕組み



国際共同捜査によるランサムウェア被疑者の検挙・被害回復

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

国の捜査機関

サイバー
特別捜査隊(当時)

National Cyber Unit

①逮捕

②テイクダウン
（機能停止措置）

海外所在被疑者

サーバ

捜査

A警察

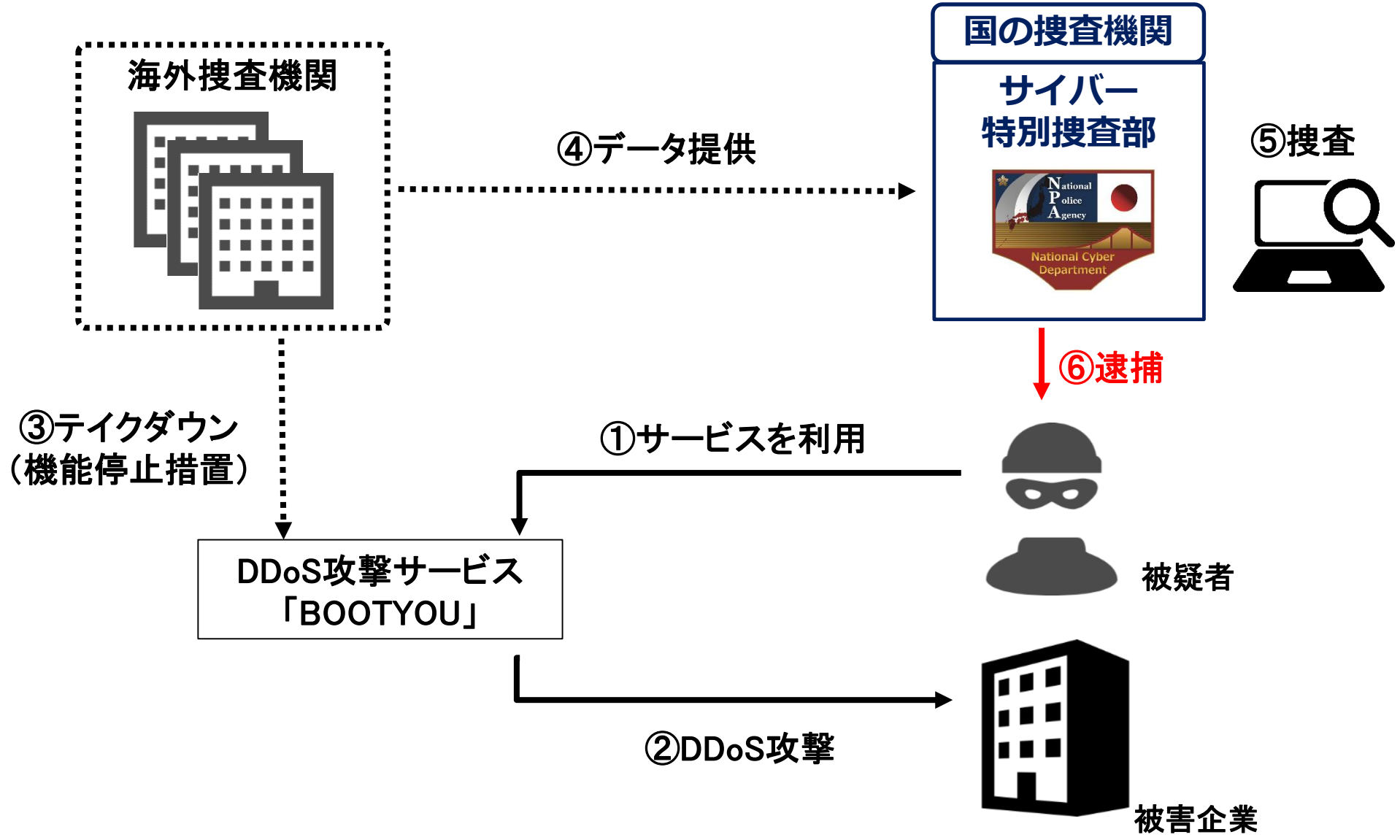
B警察

捜査

被害者

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

国際共同捜査によるDDoS攻撃国内被疑者の逮捕



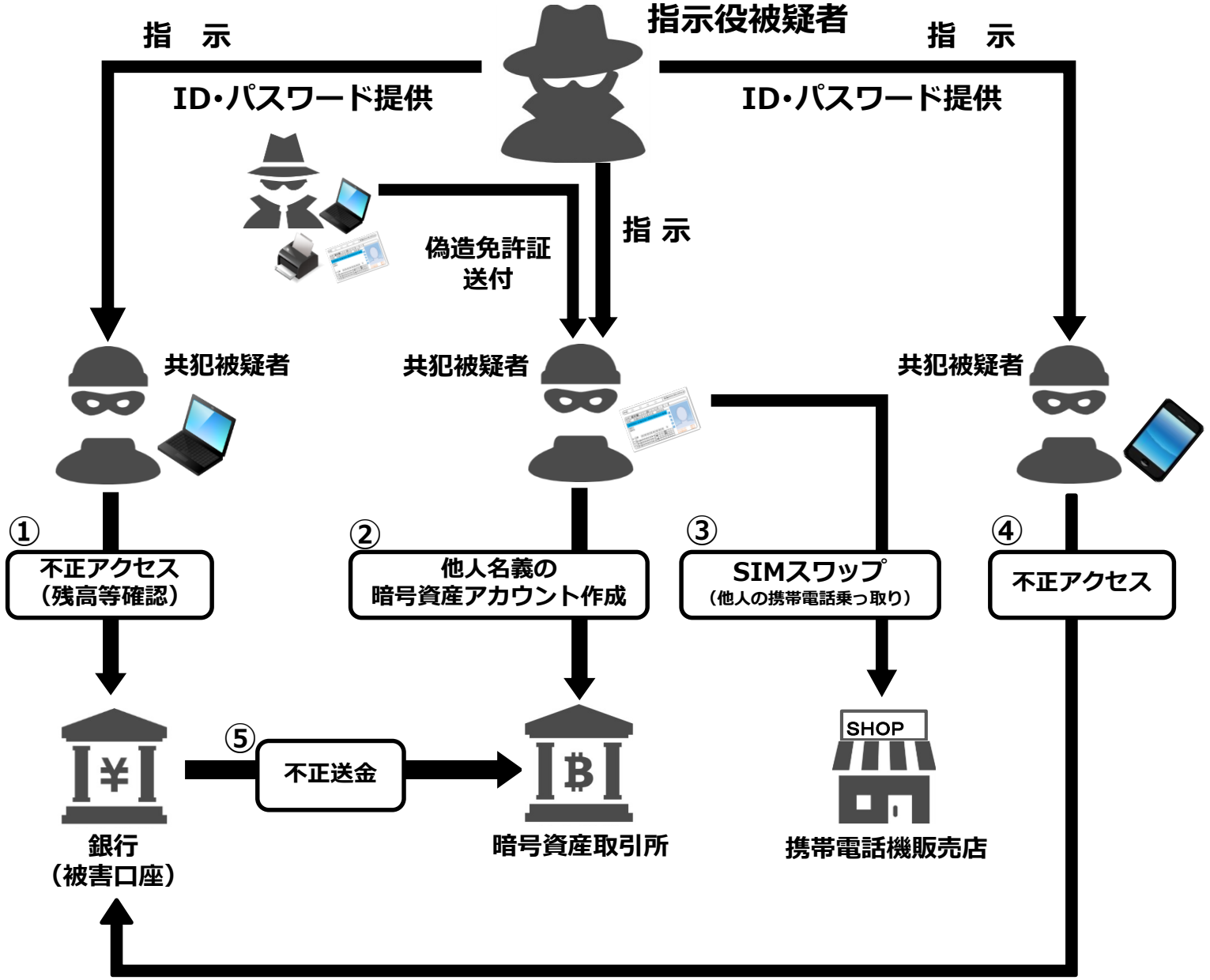
国家背景のサイバー攻撃に対するパブリックアトリビューション

■　**中国を背景とするサイバー攻撃グループ「BlackTech」**が、平成22年頃から、日本を含む東アジアと米国の政府機関や科学技術、電気通信分野等の事業者を標的として、**情報窃取を目的としたサイバー攻撃を行っていることを確認**

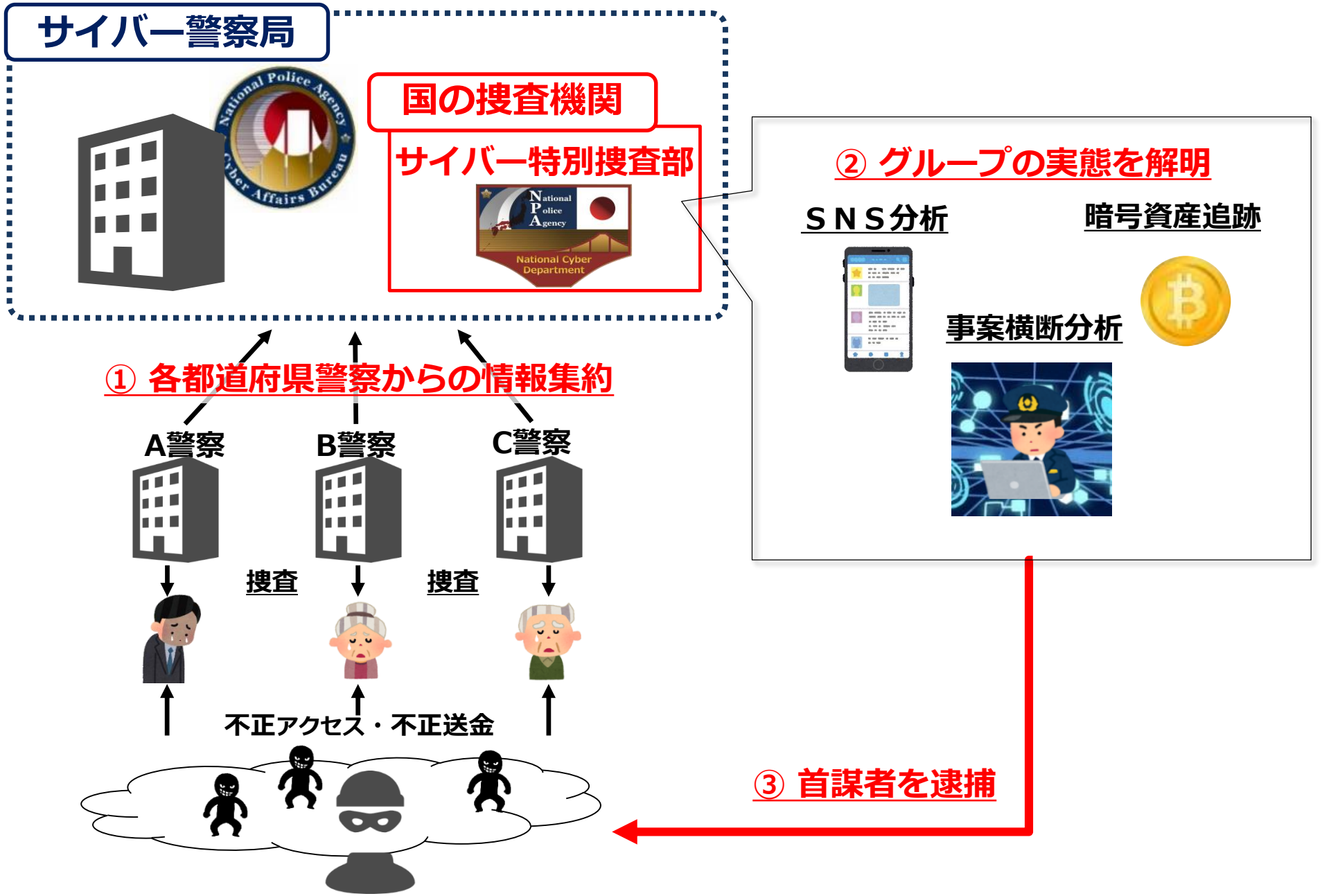
■　これを受け、令和５年９月、**NSA、FBI、CISA及びNISCとともに、合同の注意喚起を実施**

横断的・俯瞰的分析による被疑者の検挙

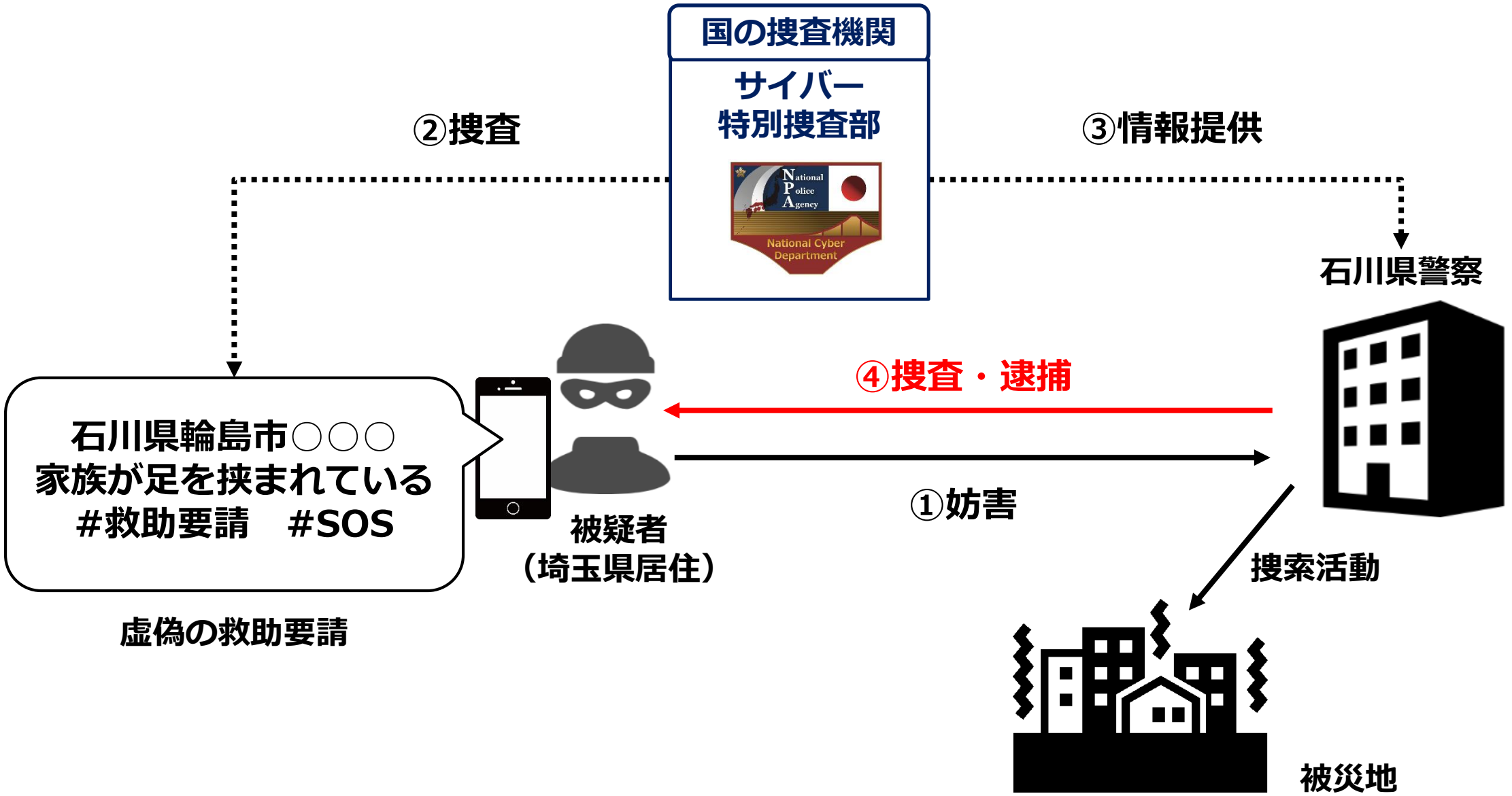
インターネットバンキング不正送金事案の概要



横断的・俯瞰的分析による被疑者の検挙

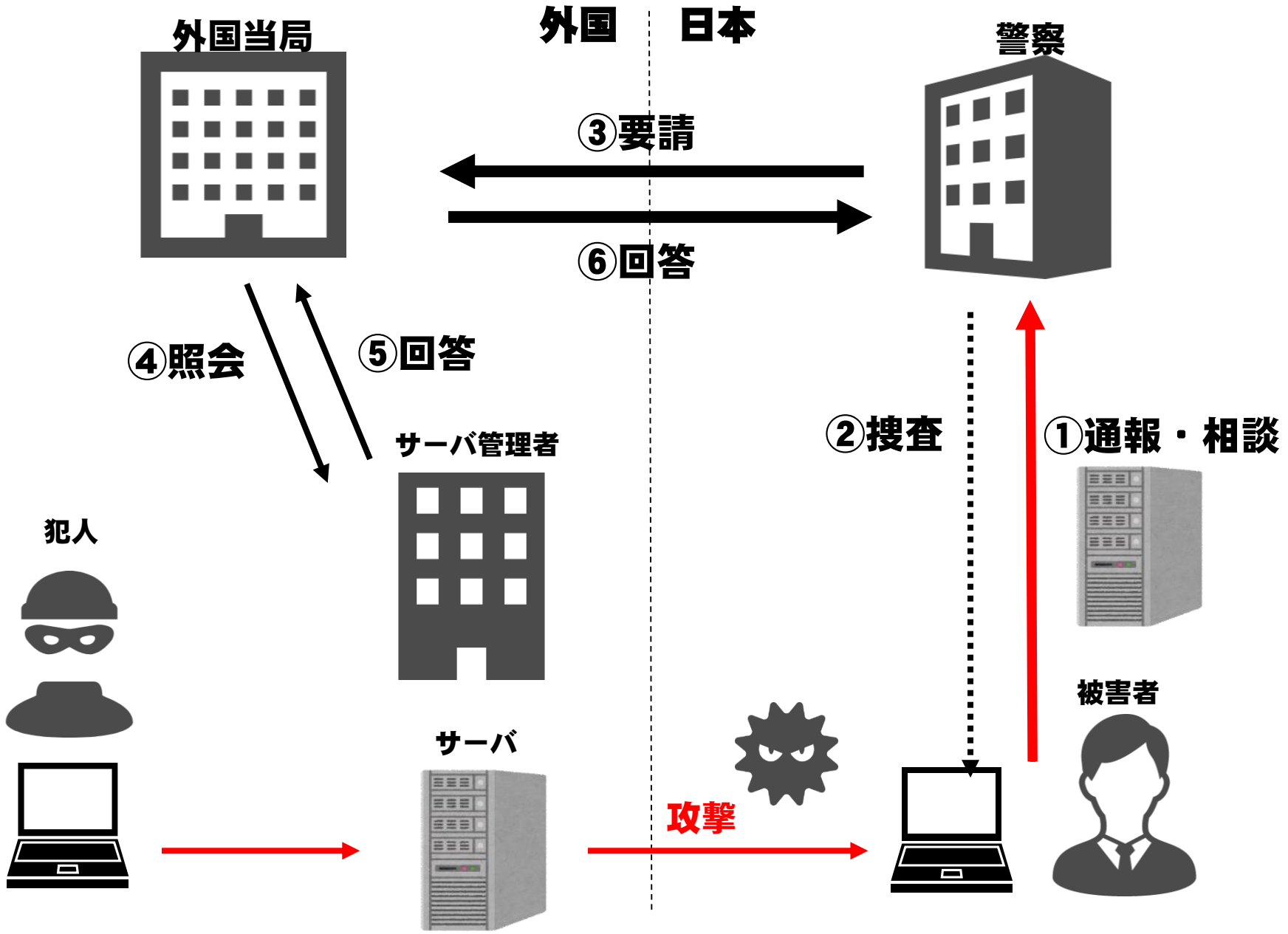


能登地震における偽情報被疑者検挙

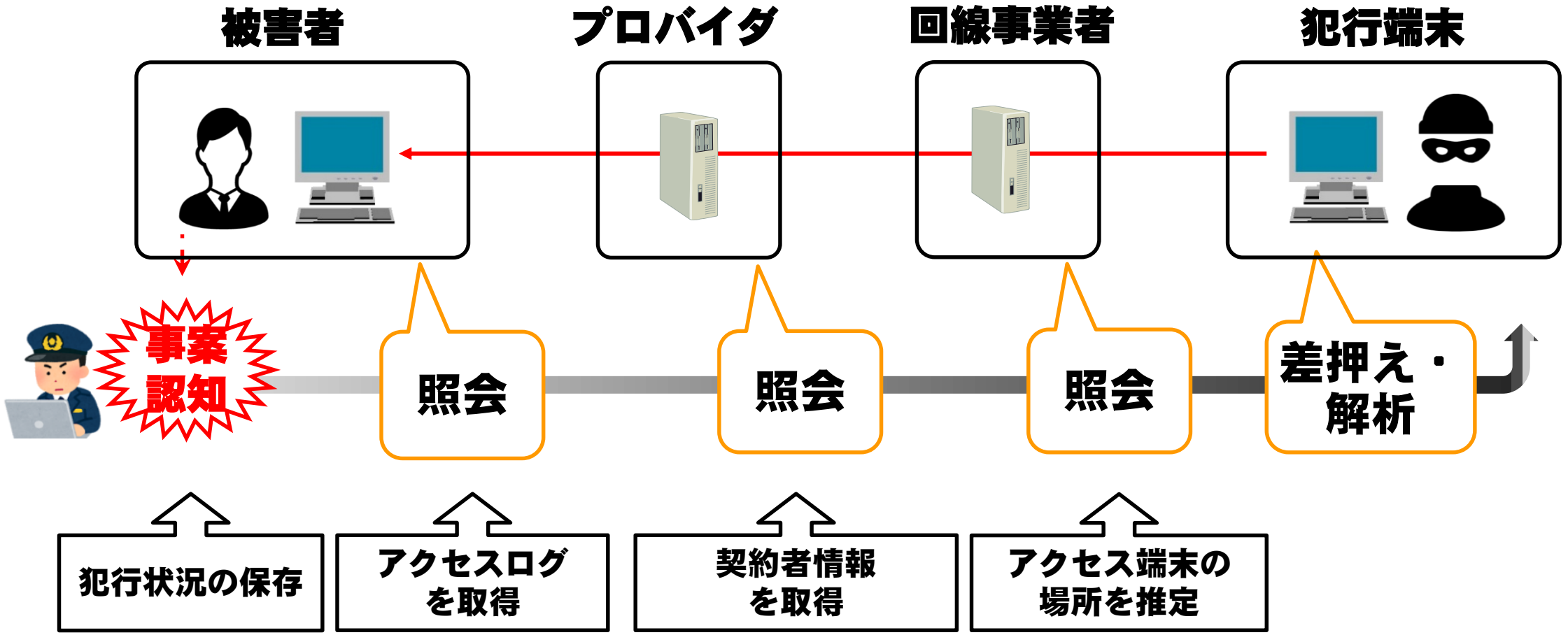


警察捜査の流れと官民連携

海外からのサイバー攻撃と捜査の仕組み



サイバー捜査の流れ（イメージ）



通報・相談とトレーサビリティの確保

■　警察への通報・相談

■　外部からネットワークを切り離し
　〇　外部と接続するケーブルを抜く
　×　再起動する

通報・相談の促進

通報・相談窓口の統一化

サイバー事案に関する通報等のオンライン受付窓口

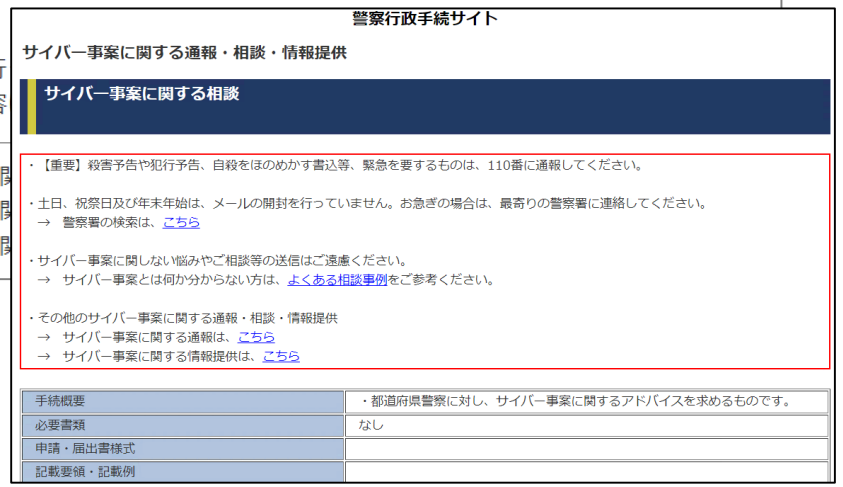
警察庁では、サイバー事案に関する通報、相談及び情報提供（以下「通報等」という。）の全国統一のオンライン受付窓口を設置しています。
この窓口からはサイバー事案に関する

○通報（都道府県警察に対し、サイバー事案に関する通報を行うもの。）
※被害に遭った具体的な事実の通知を伴う場合
○相談（都道府県警察に対し、サイバー事案に関するアドバイスを求めるもの。）
○情報提供（都道府県警察に対し、サイバー事案に関する情報を提供するもの。）

を行うことができます。

この窓口から通報等を行
だきます。通報等の内容

○サイバー事案に関
○サイバー事案に関
○サイバー事案に関



警察行政手続サイト

サイバー事案に関する通報・相談・情報提供

サイバー事案に関する相談

・【重要】殺害予告や犯行予告、自殺をほのめかす書込等、緊急を要するものは、110番に通報してください。

・土日、祝祭日及び年末年始は、メールの開封を行っていません。お急ぎの場合は、最寄りの警察署に連絡してください。
→ 警察署の検索は、こちら

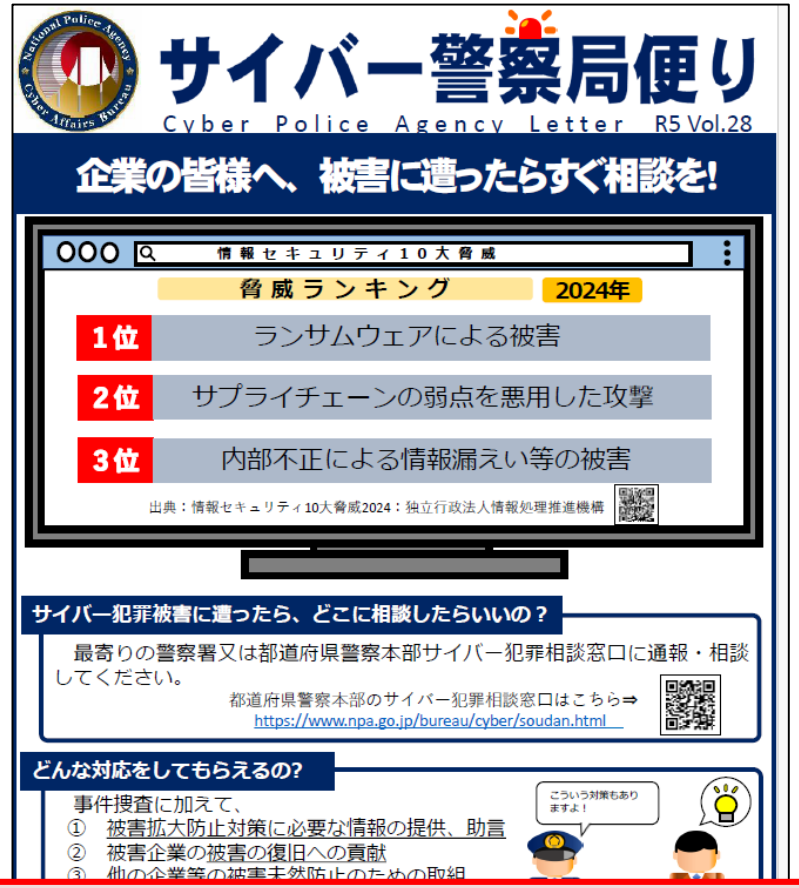
・サイバー事案に関しない悩みやご相談等の送信はご遠慮ください。
→ サイバー事案とは何か分からない方は、よくある相談事例をご参考ください。

・その他のサイバー事案に関する通報・相談・情報提供
→ サイバー事案に関する通報は、こちら
→ サイバー事案に関する情報提供は、こちら

手続概要	・都道府県警察に対し、サイバー事案に関するアドバイスを求めるものです。
必要書類	なし
申請・届出書様式	
記載要領・記載例	

https://www.npa.go.jp/bureau/cyber/soudan.html

広報啓発資料の作成等



サイバー警察局便り

Cyber Police Agency Letter R5 Vol.28

企業の皆様へ、被害に遭ったらすぐ相談を!

情報セキュリティ10大脅威

脅威ランキング 2024年

1位 ランサムウェアによる被害
2位 サプライチェーンの弱点を悪用した攻撃
3位 内部不正による情報漏えい等の被害

出典：情報セキュリティ10大脅威2024：独立行政法人情報処理推進機構

サイバー犯罪被害に遭ったら、どこに相談したらいいの？

最寄りの警察署又は都道府県警察本部サイバー犯罪相談窓口に通報・相談してください。

都道府県警察本部のサイバー犯罪相談窓口はこちら⇒
https://www.npa.go.jp/bureau/cyber/soudan.html

どんな対応をしてもらえるの?

事件捜査に加えて、
① 被害拡大防止対策に必要な情報の提供、助言
② 被害企業の被害の復旧への貢献
③ 他の企業等の被害未然防止のための取組

こういう対策もありますよ！

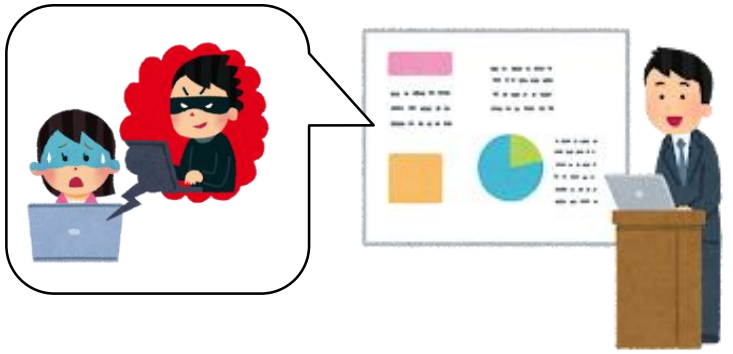
被害に遭ってしまったら
警察へ通報

サイバー警察の取組

海外機関 ⟷ **警 察** ⟷ **産業界・学会**

国際連携を通じた犯人検挙・抑止

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

ご静聴ありがとうございました