令　和　7　年　3　月　10　日
中小企業向けサイバーセキュリティセミナー

ランサムウェア被害の情勢と被害発生時の対応について

警察庁サイバー警察局
サイバー企画課
サイバー事案防止対策室

本日の内容

１　サイバー空間をめぐる脅威の情勢

２　ランサムウェア被害の情勢

３　被害発生時における対応

サイバー空間をめぐる脅威の情勢

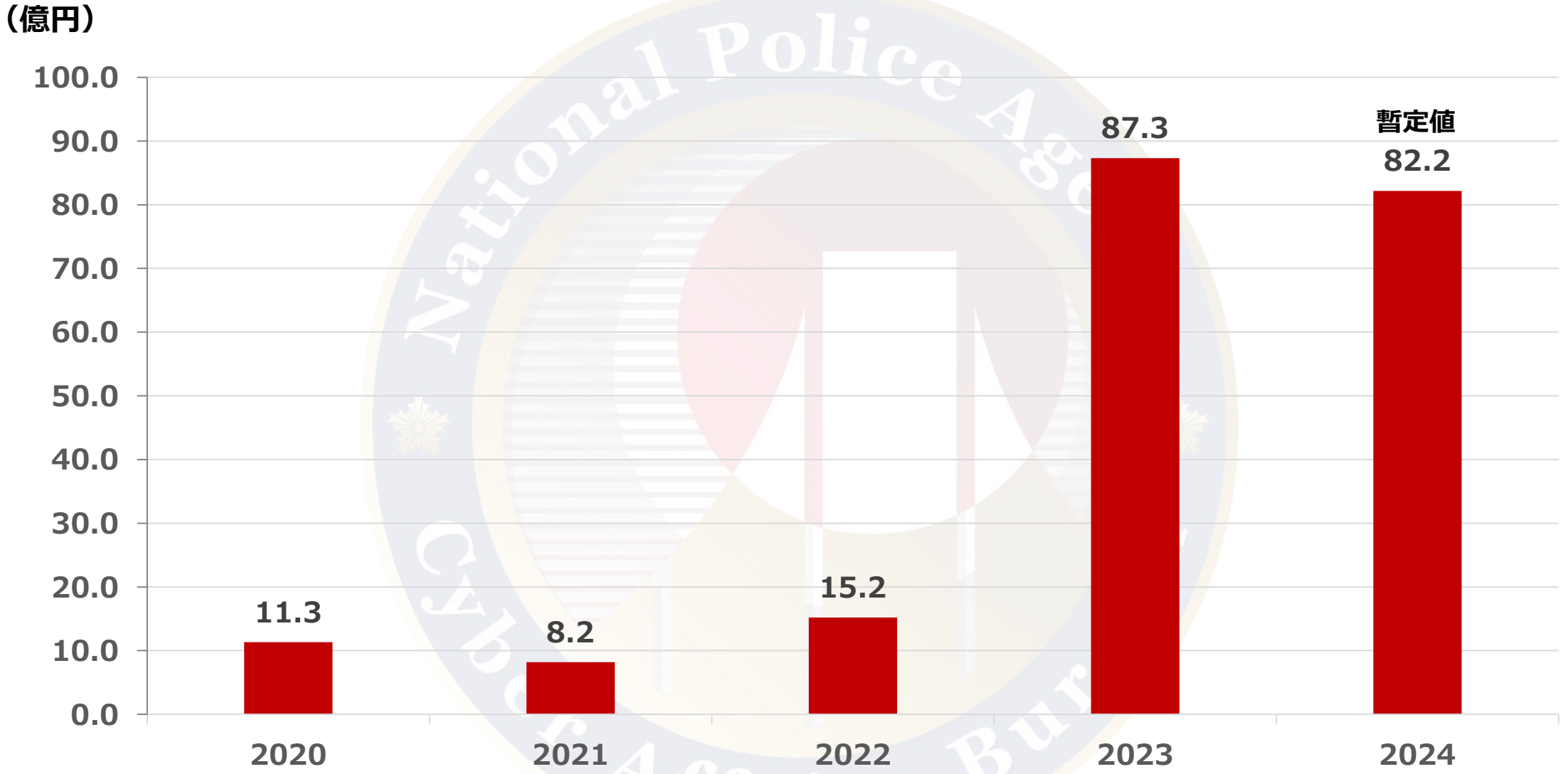
フィッシング報告件数

出典：フィッシング対策協議会の公開情報から作成

クレジットカード不正利用被害額

出典：一般社団法人日本クレジット協会（https://www.j-credit.or.jp）クレジットカード不正利用被害の発生状況から作成

インターネットバンキング不正送金被害額



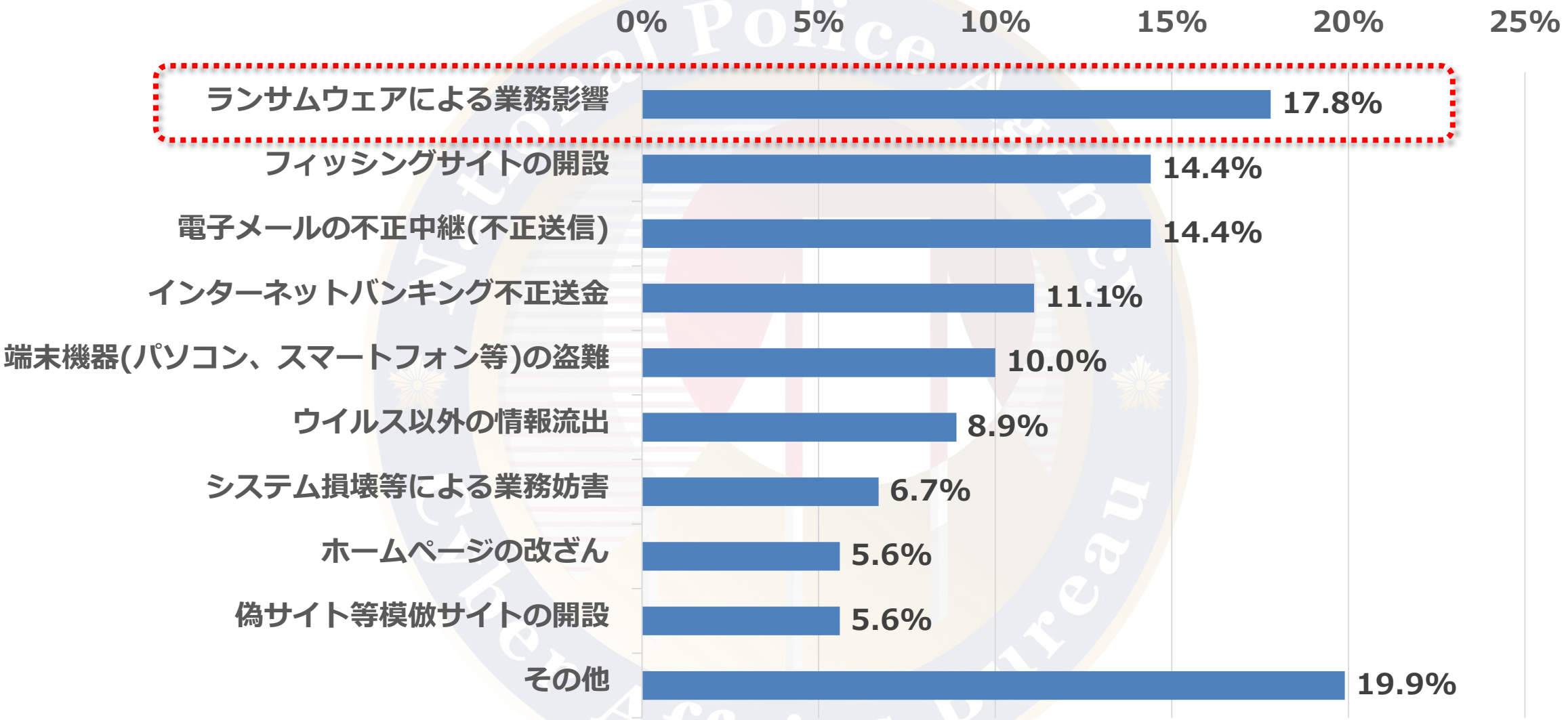
出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」「令和６年の犯罪情勢」から作成

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「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

過去１年間に受けた不正アクセス等被害の種別

（複数回答、n=90）



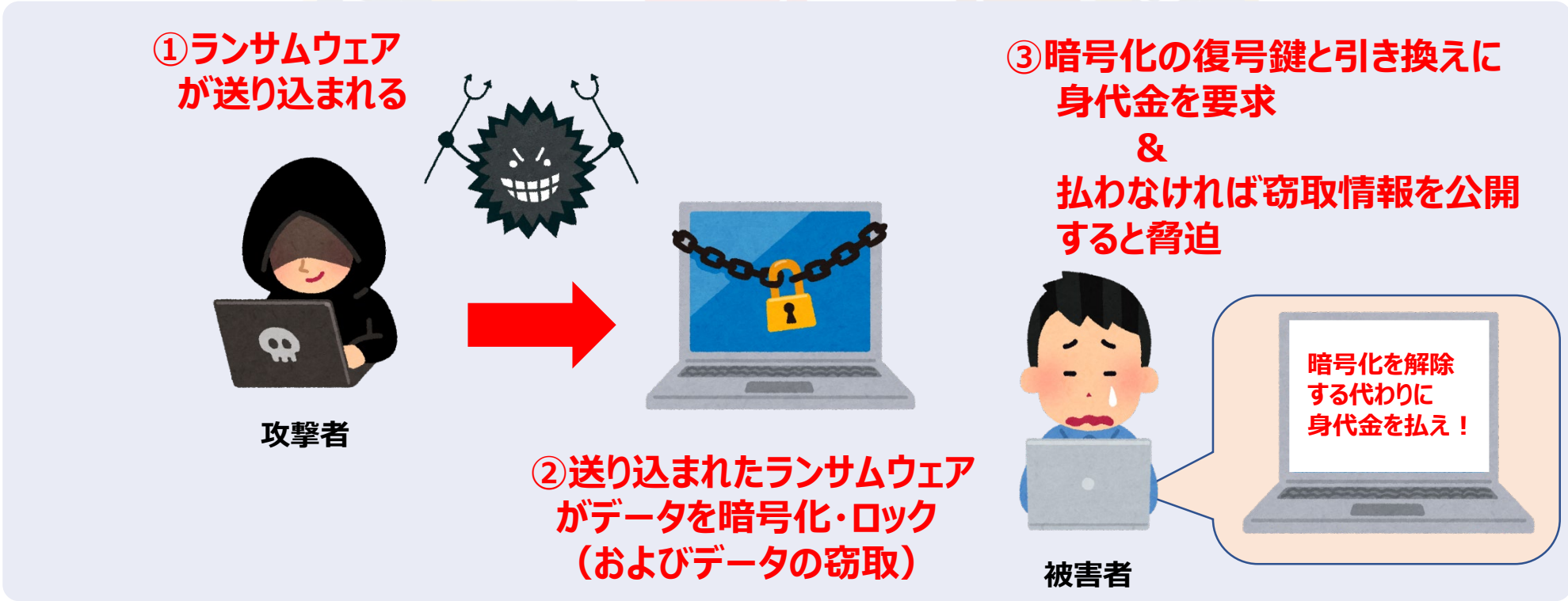
出典：警察庁「不正アクセス行為対策等の実態調査アクセス制御機能に関する技術の研究開発の状況等に関する調査（令和５年）」

ランサムウェア被害の情勢

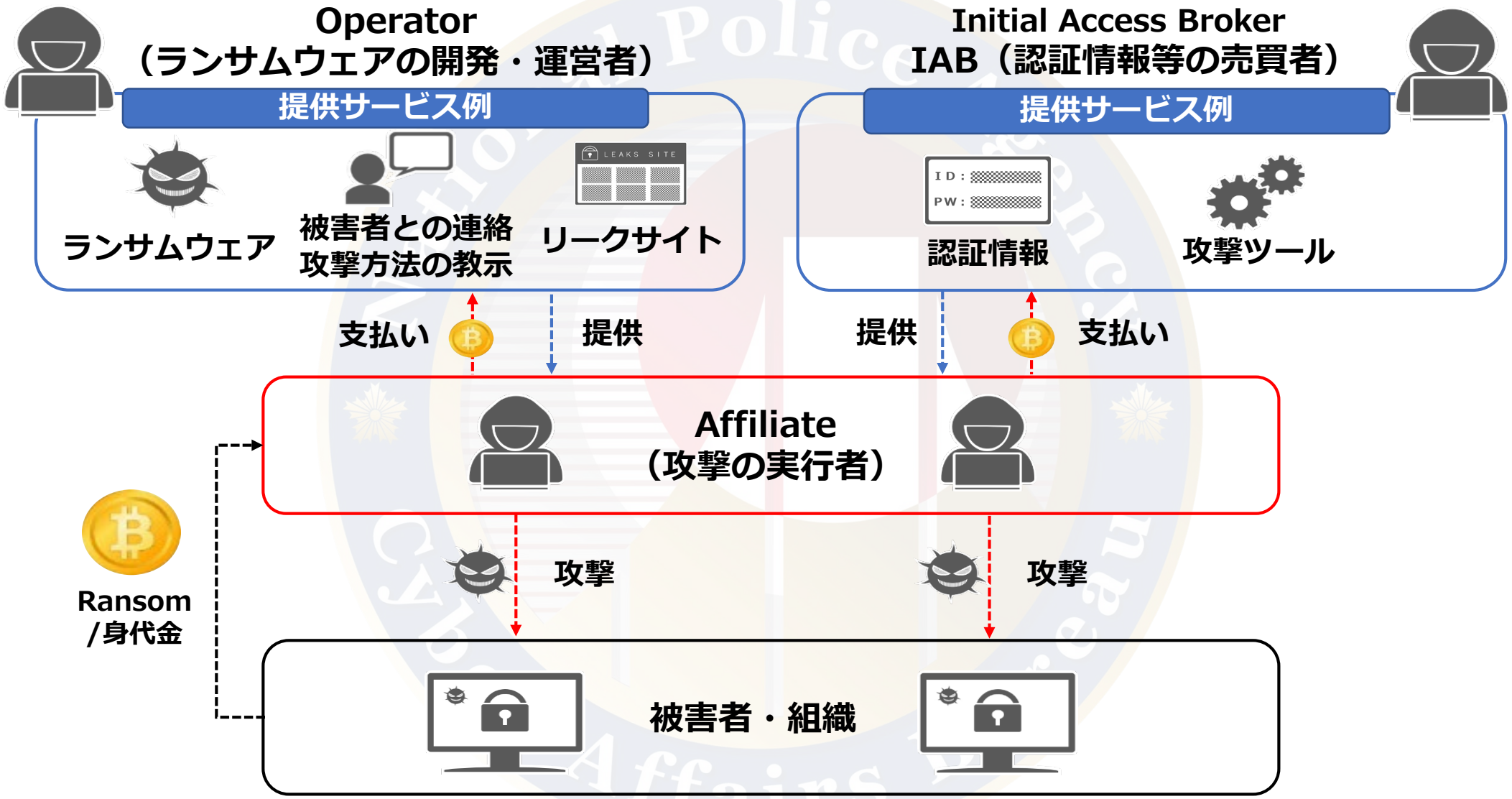
ランサムウェアとは・・・

感染すると端末等に保存されているデータを暗号化して使用できない状態とした上で、そのデータを復号する対価として、いわゆる「身代金」（ランサム）を要求する不正プログラムをいう。

近年は、「対価を支払わなければ窃取したデータを公開する」と脅す、二重恐喝型が多くを占めている。

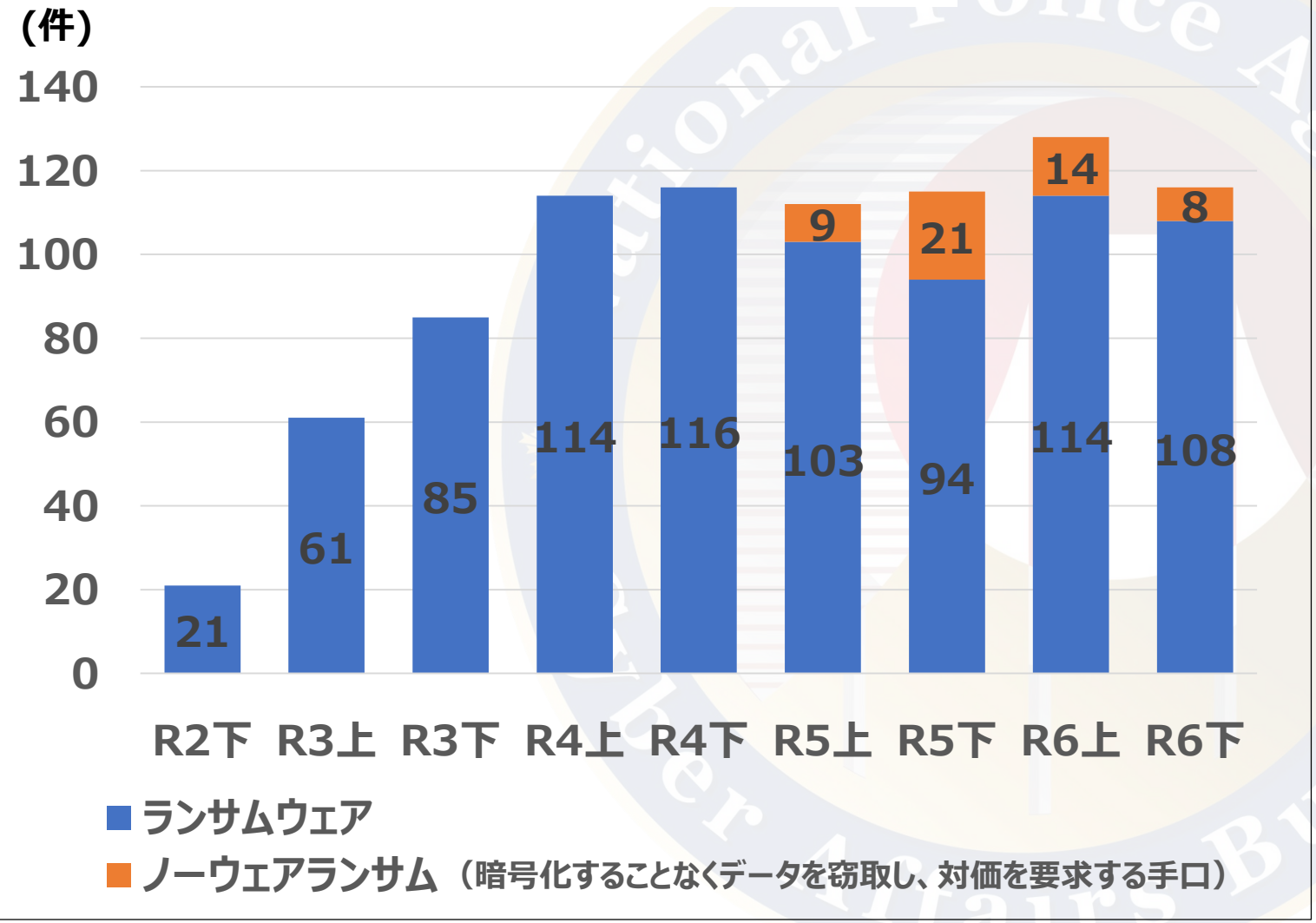


Ransomware as a Service (RaaS)



ランサムウェア被害の情勢

【被害件数の推移】



○被害件数は高止まり

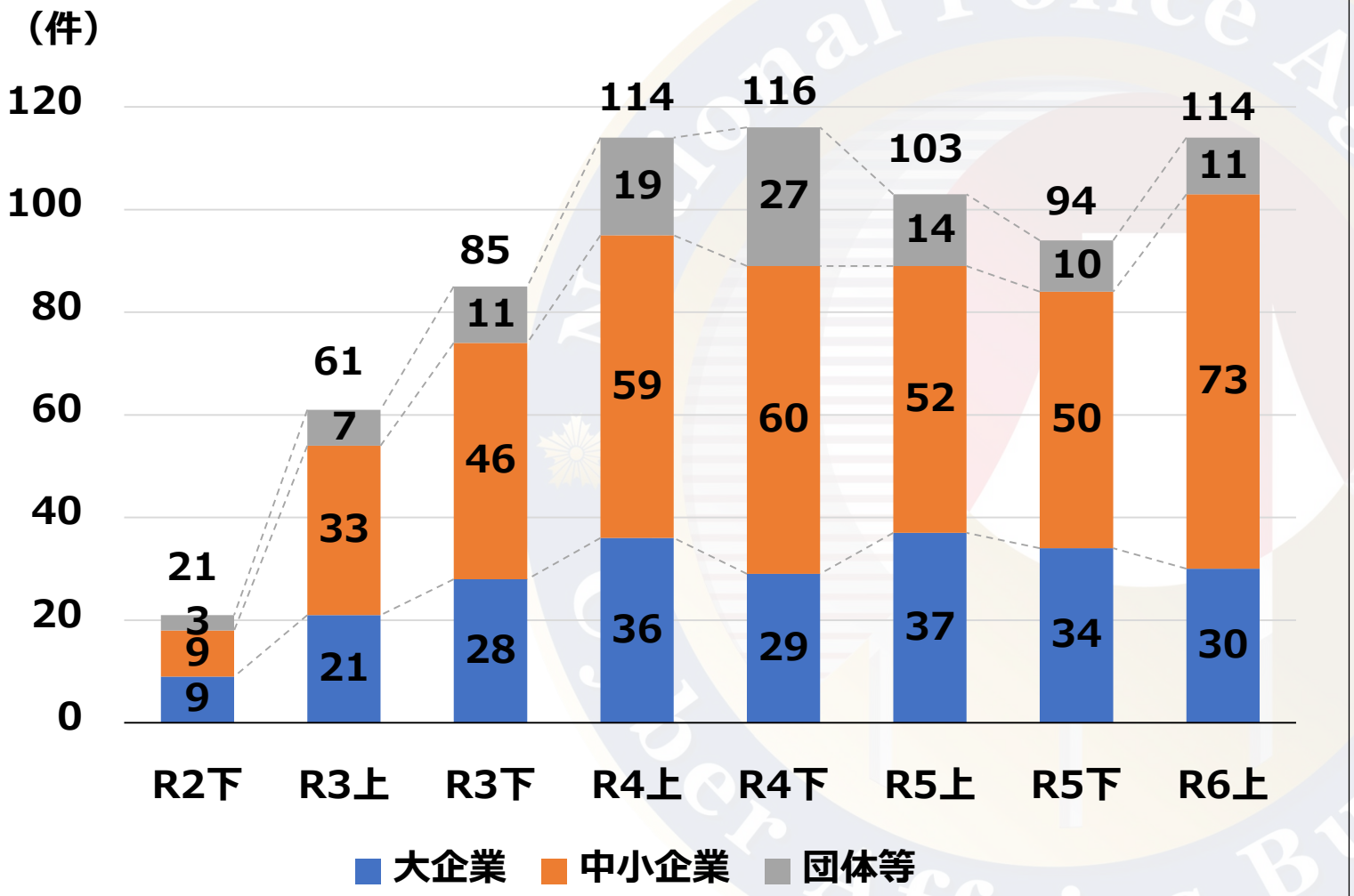
○ランサムウェア被害は大部分が「二重恐喝型」

○暗号化を行わない手口（ノーウェアランサム）も発生

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」「令和６年の犯罪情勢」から作成

ランサムウェア被害の情勢

【被害件数の推移（組織規模）】



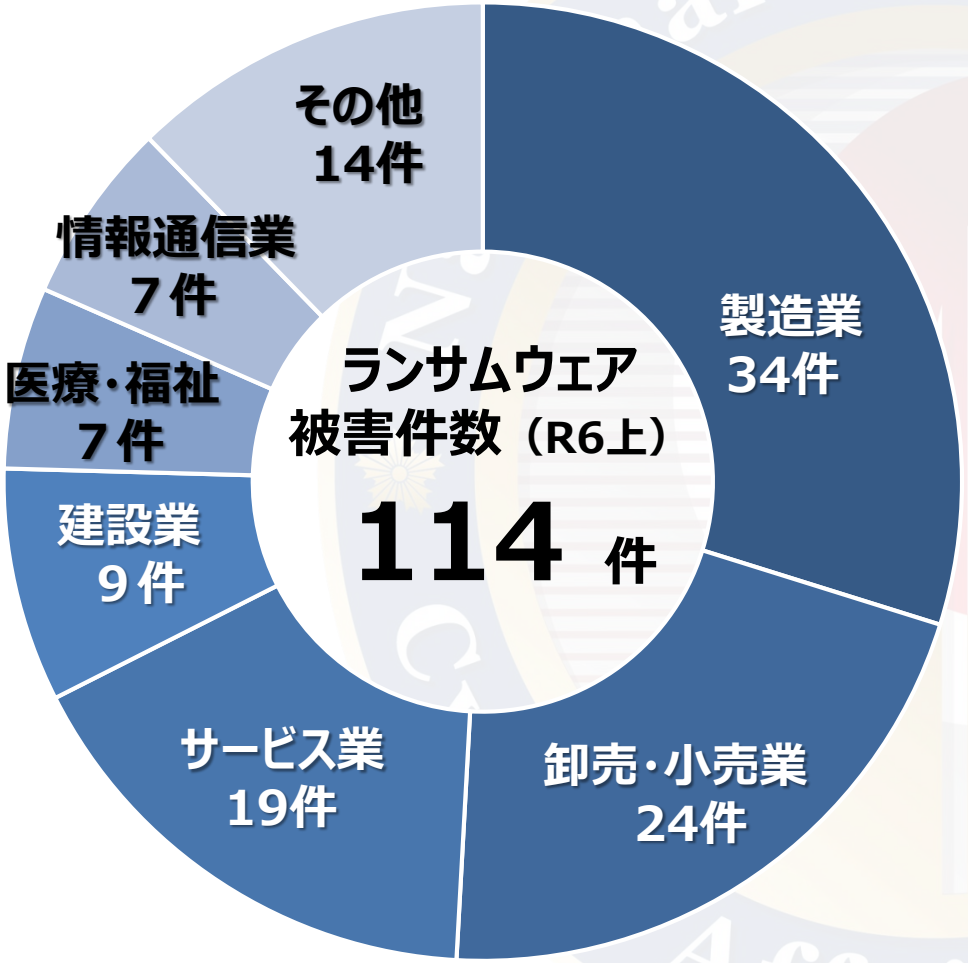
出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」から作成

○中小企業の被害は、前年から約4割増加

○報道される大企業事案以外にも多くの被害

ランサムウェア被害の情勢

【被害件数（業種別）】



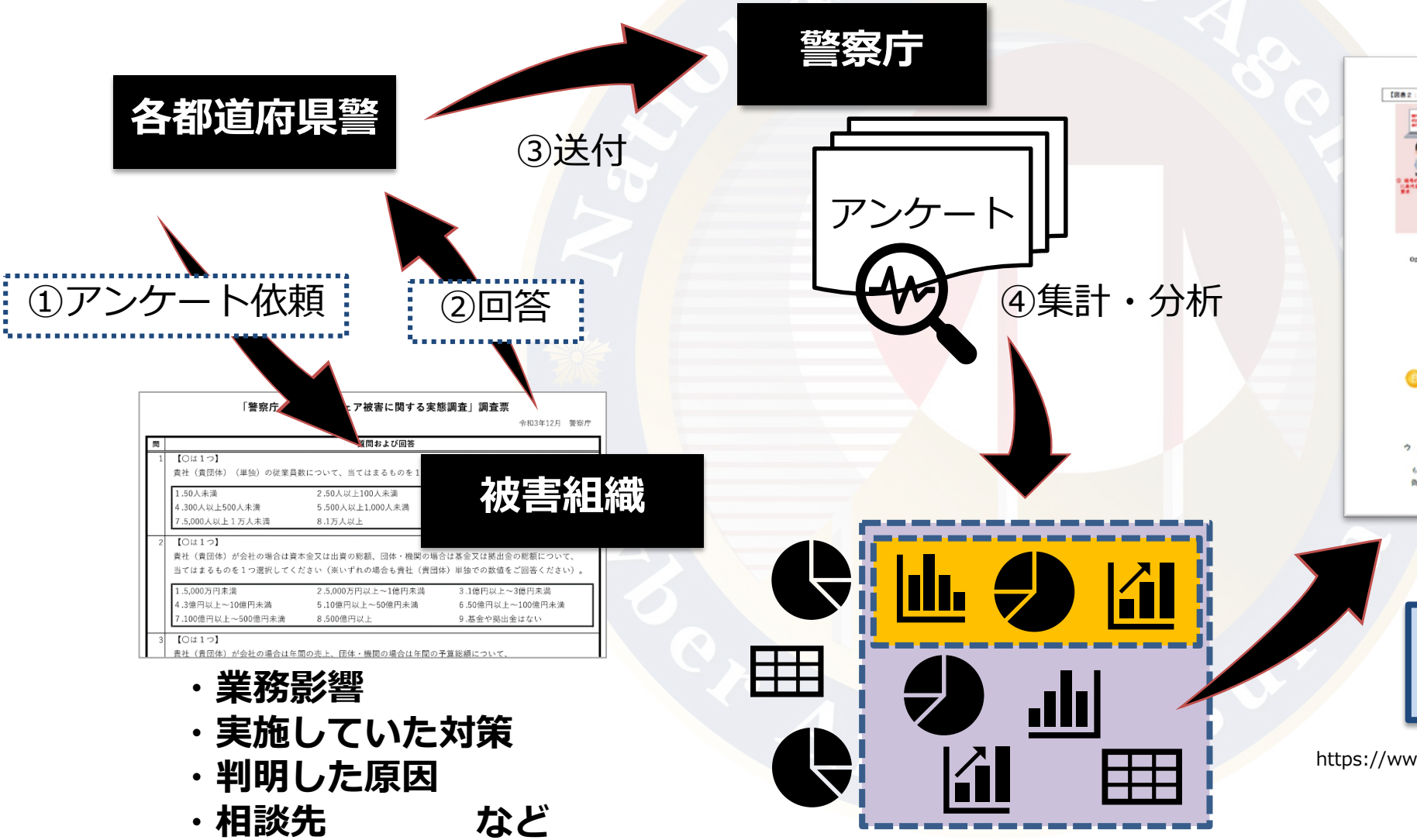
○様々な業種に被害

○多くの攻撃者は、特定の企業・業種狙いではない
- 侵入する隙のある組織を狙っている

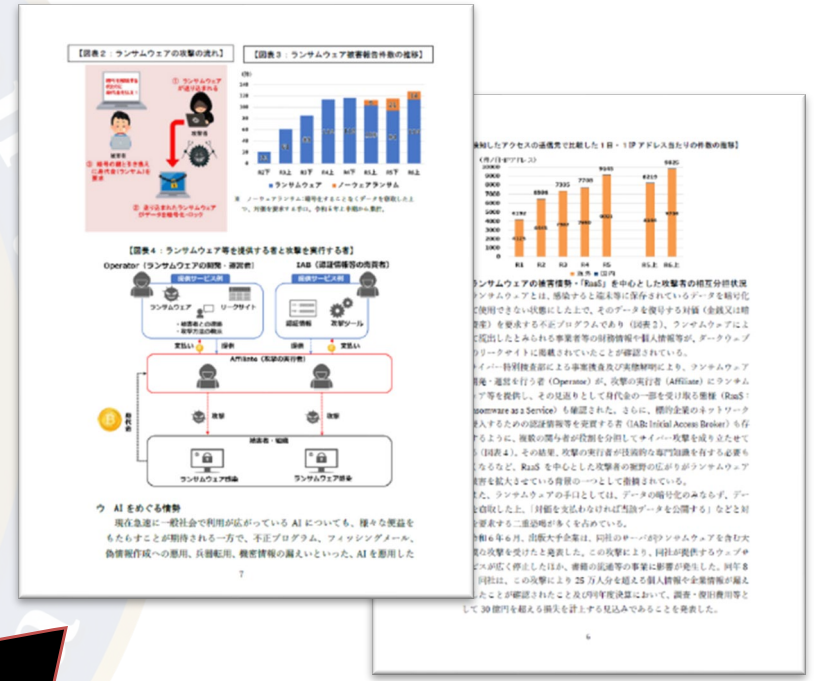
出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」から作成

ランサムウェア被害組織アンケート

ランサムウェアの被害通報を行った組織に対してアンケートへの回答を依頼し、分析結果の一部を半期に１回公表



- 業務影響
- 実施していた対策
- 判明した原因
- 相談先　　など



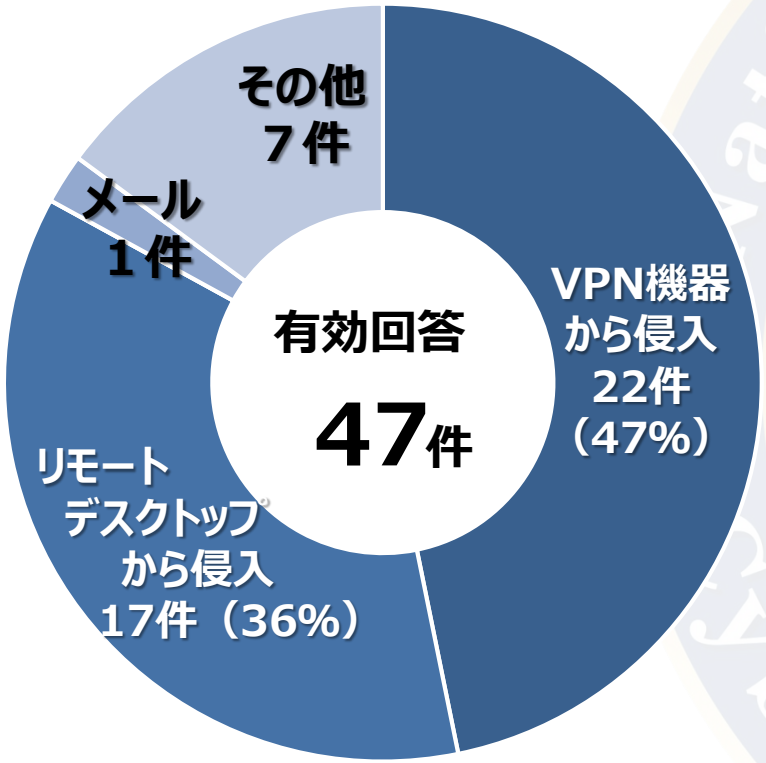
サイバー空間をめぐる脅威の情勢等

https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

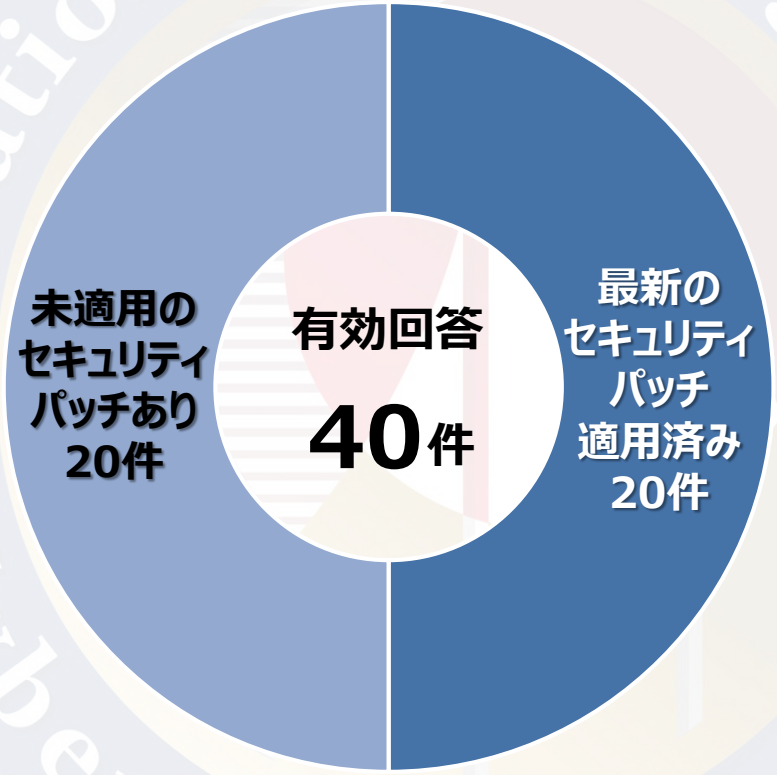
ランサムウェアの感染経路

【調査結果（感染経路）】

感染経路



感染経路のパッチ適用状況



○VPN機器やRDP機能からの侵入が多数

→ セキュリティパッチ適用によるぜい弱性対処

○窃取した認証情報や総当たり攻撃による不正ログインも

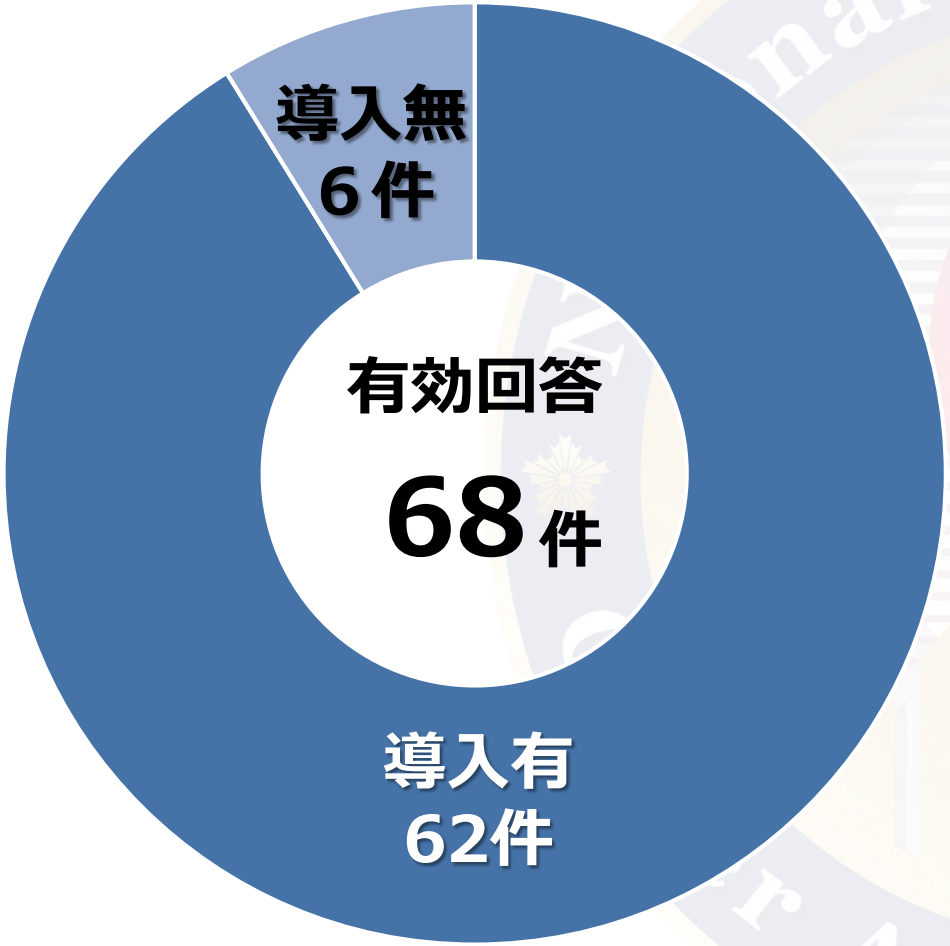
→ 認証強度の向上、認証情報の厳正な管理

→ 接続端末の制限、アクセス権限の適切な設定

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

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では８割、EDRでも半数が検知なし
- 攻撃者による無効化や製品未対応・未更新が原因

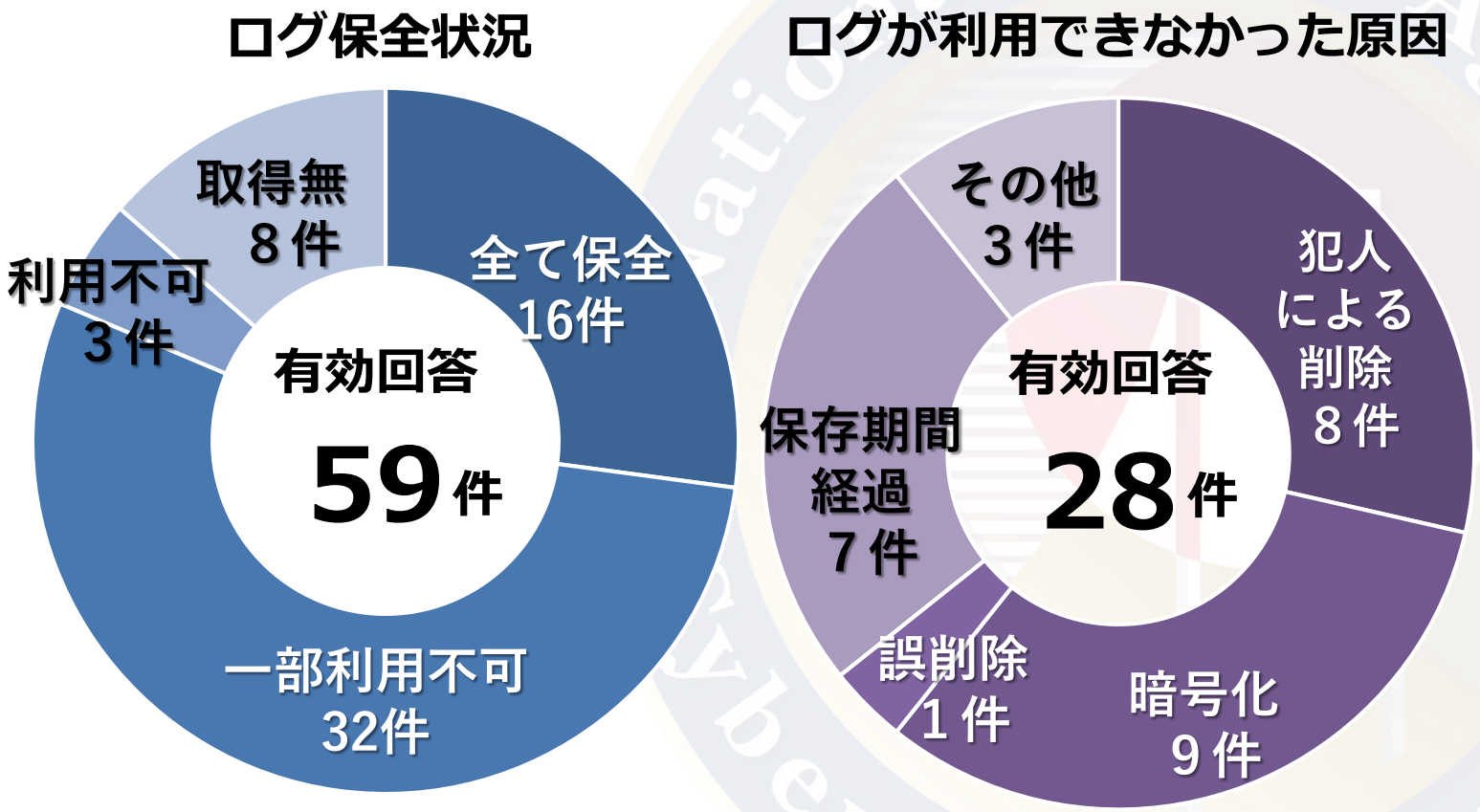
→ ウイルス対策ソフト等は**常に最新の状態に更新**

○**多層防御**による対策を
- 「対策ソフトがあるから安心」はNG

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

ログの保全状況・使用可否

【調査結果（ログ状況）】



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

○侵入経路・侵害範囲特定にログ解析は不可欠

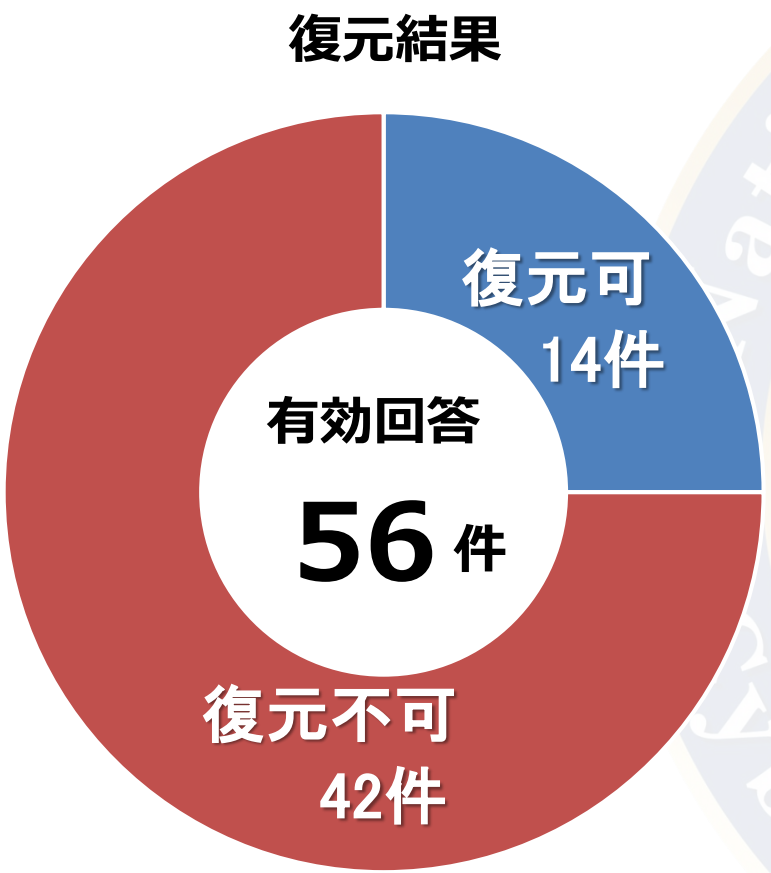
○攻撃者によるログの削除や暗号化が多数

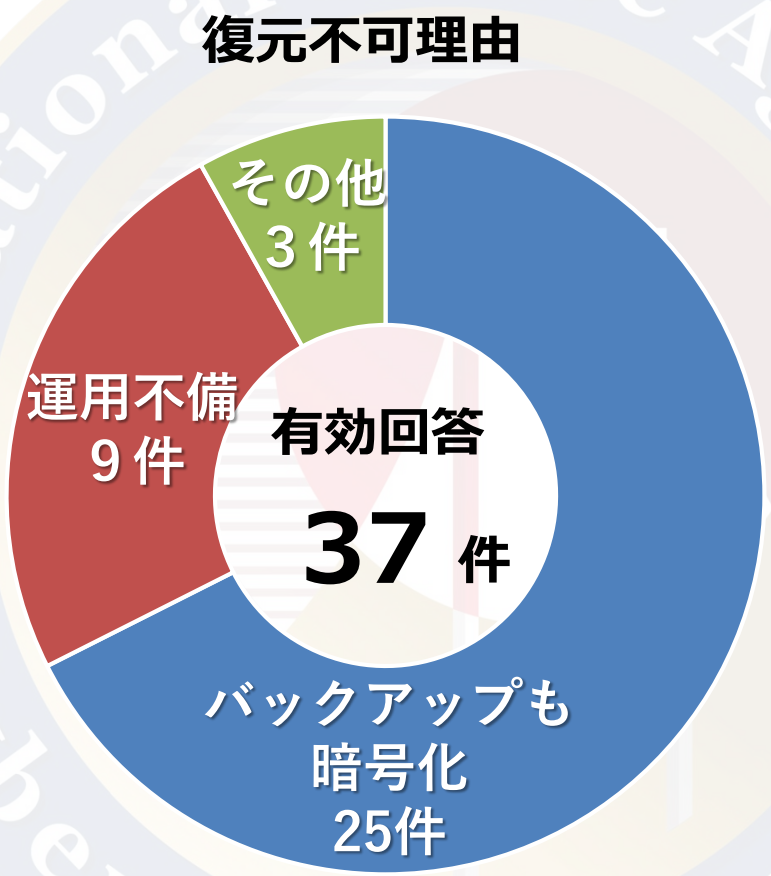
→サーバ・VPN機器等での、多面的なログ取得

→オフライン媒体等によるログの保存・管理

バックアップの復元状況

【調査結果（復元状況）】





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

○バックアップも暗号化される事案が多数

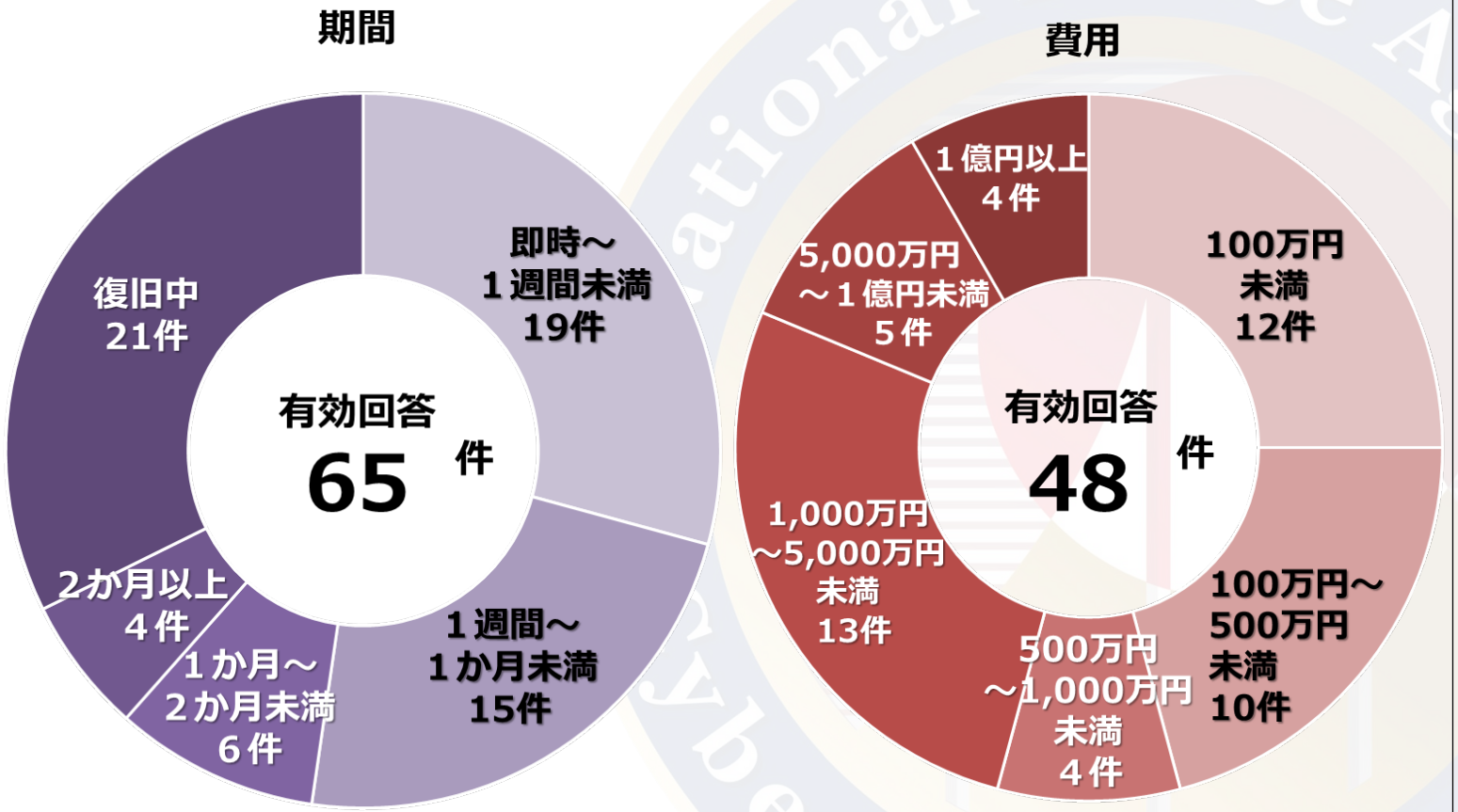
→資産の性質を勘案し、**オフライン／オンラインを組み合せたバックアップ**の運用を

○運用不備による復元不可も約1/4を占める

→運用体制の確認やバックアップからの復旧訓練を

調査復旧に要した期間・費用の総額

【調査結果（調査復旧期間・費用）】



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

○復旧対応は長期に及び、多額の費用が必要

- 約半数は1000万円以上の調査復旧費用
- ここに表れないコストも

○セキュリティ対策の計画的な実施・更新

→ 経営層は関連予算の確保に理解を

被害発生時における対応

被害に遭った際の初期対応

■ ネットワークからの隔離

○ ＬＡＮケーブルを抜き、無線をオフ

× **再起動**

- 端末上に残った攻撃の痕跡を示す
  データが消えてしまう可能性

■ 警察等関係機関への通報・相談

■ ログの保全

- 侵入経路や侵害範囲の特定のため、外部接続機器を
  中心としたログの保全に努めてください

被害に遭うことを想定した備え

■ バックアップ、ログの取得

- **オフラインを含む長期・短期の複数バックアップ**を
- ログは多面的に取得し、消去されない対策も

■ 事業継続計画（ＢＣＰ）等の策定

- 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
- **「警察等関係機関への通報・相談」を対応項目として明記**

  ※連絡方法や窓口も事前に確認

■ セキュリティリスクを考慮した経営

- リスク管理体制の整備
- システムの運用・保守体制の整備（充分な投資）

警察への通報について

■ 警察への速やかな通報・相談

最寄りの警察署や都道府県警察のサイバー犯罪相談窓口等に通報・相談して下さい。

≪サイバー事案に関する通報・相談のオンライン受付窓口≫
https://www.npa.go.jp/bureau/cyber/soudan.html

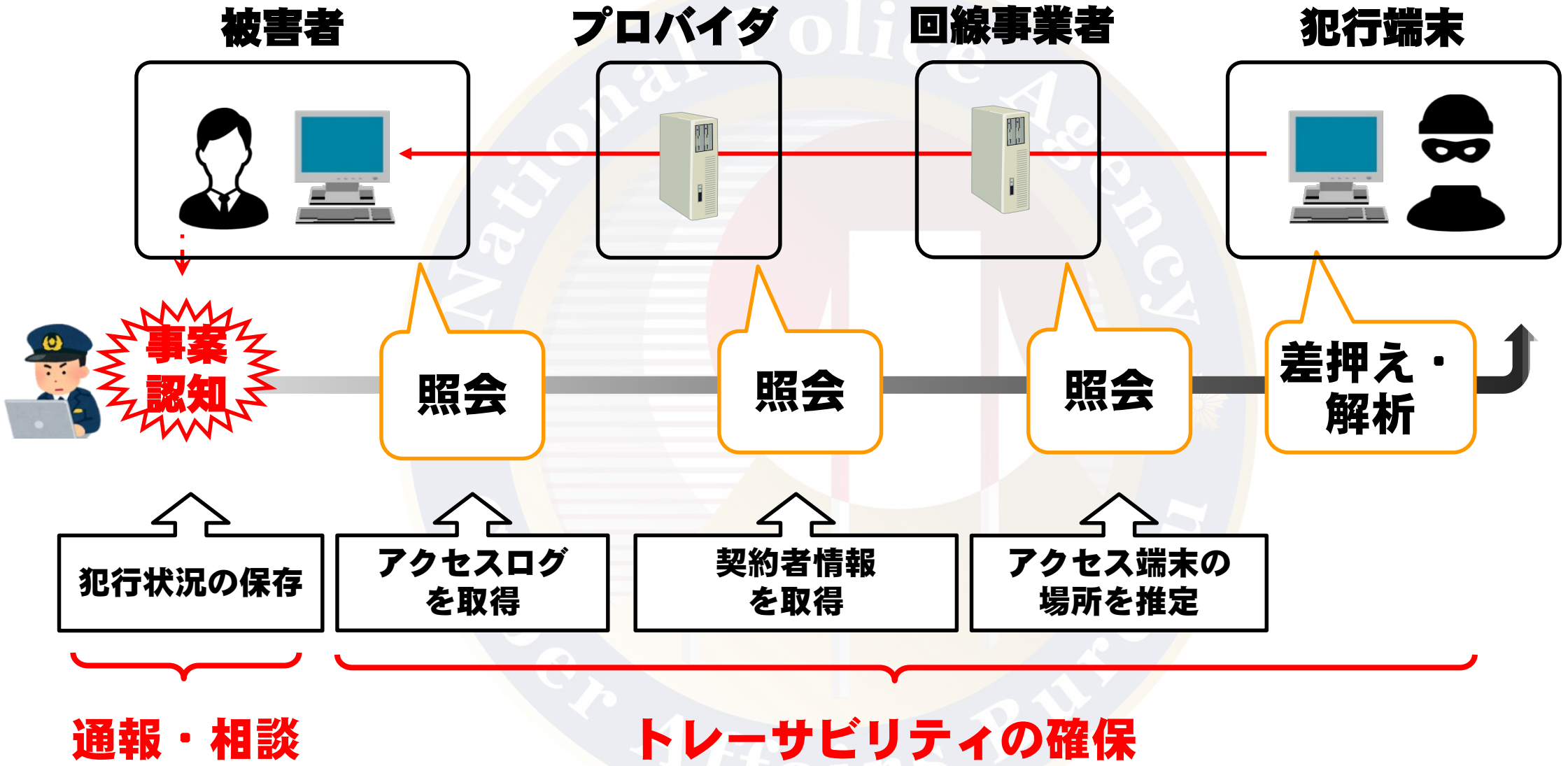
警察では、**被害拡大防止・早期復旧のための初期対応支援や暗号化復号ツールの案内**等を行っています。

【参考】「サイバー攻撃被害に係る情報の共有・公表ガイダンス」

関係機関との情報共有、被害公表、外部組織との連携、機微な情報への配慮等の内容がまとめられています。

本文 https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf
概要 https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_gaiyou.pdf

サイバー捜査の流れ（イメージ）

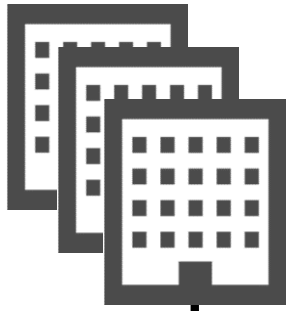


ランサムウェアに係る国際共同捜査（LockBit・Phobos）

国際共同捜査

外国　日本

ユーロポール・外国捜査機関



EUROPOL

相互協力

サイバー警察局

国の捜査機関

サイバー
特別捜査部

National Cyber Unit

逮捕

犯罪インフラの閉鎖

捜査

A警察

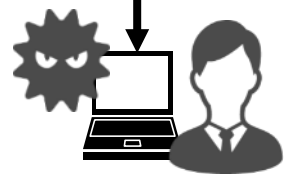
B警察

捜査

海外所在被疑者

サーバ

被害者



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

警察への通報について

■ よくある疑問

- **通報したら被害公表が必要？**
  レピュテーションリスク（信用の毀損・風評被害）が心配…

  ⇒ 警察から公表を求めることはありません。被害情報の保秘は徹底します。

- **警察に通報すると、サーバや端末を全て持って行かれるのでは？**
  復旧作業が遅れそう…

  ⇒ 被害組織の復旧作業や業務継続に最大限配慮しながら捜査を進めます。
  多くの場合、ディスクイメージやログデータを提供いただいています。

- **大した被害が発生していないけど、通報するべき？**

  ⇒ 軽微な事案でも、犯人につながる手掛かりがあるかもしれません。
  「警察への通報＝捜査開始」ではありませんので、情報提供をお願いします。

ご静聴ありがとうございました