令　和　7　年　3　月　7　日
サイバーセキュリティシンポジウム道後

サイバー空間をめぐる脅威の情勢と取るべき対応

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　被害への備えと対応

National Police Agency Cyber Affairs Bureau

サイバー空間をめぐる脅威の情勢

サイバー犯罪の検挙件数

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」

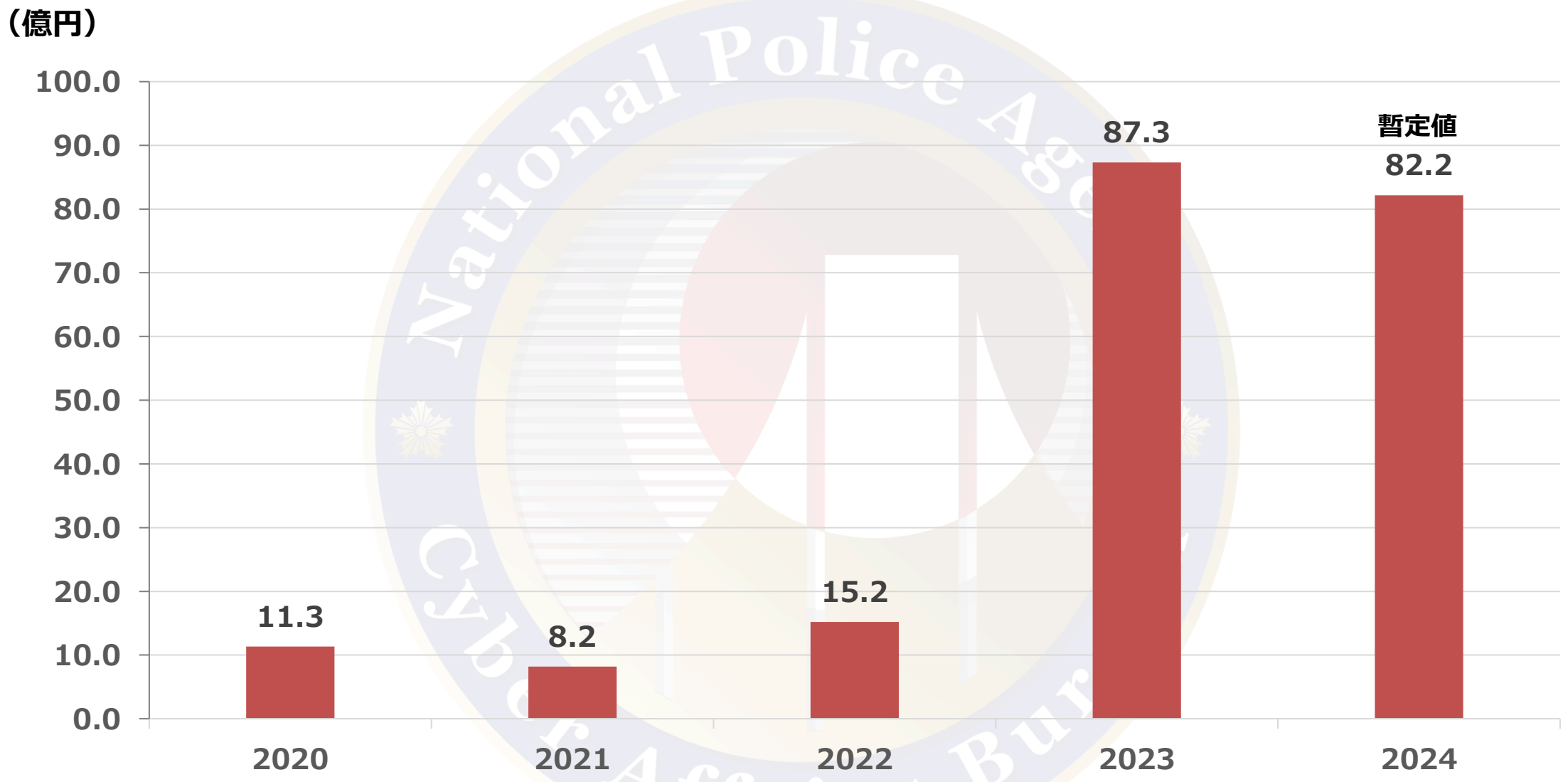
フィッシング報告件数

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



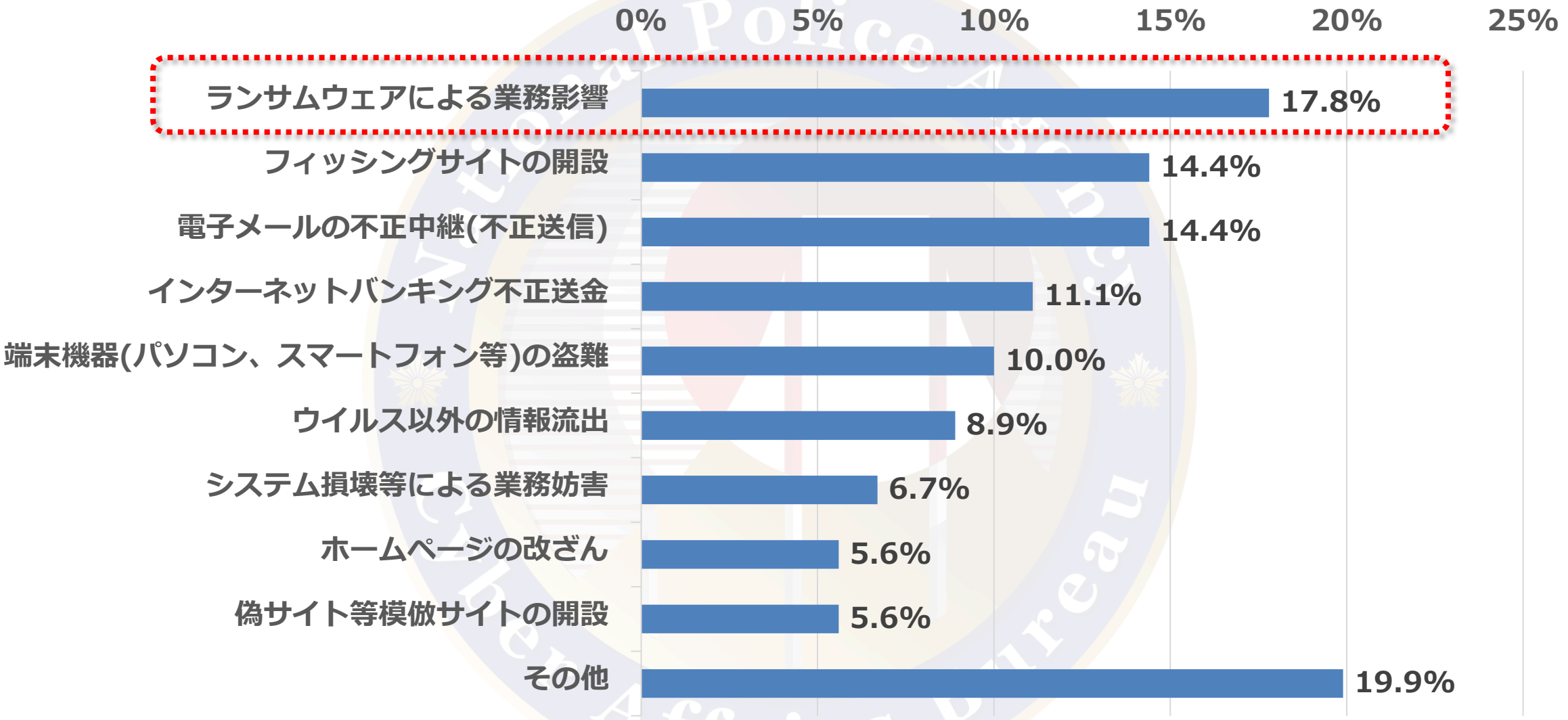
出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」「令和６年の犯罪情勢」から作成

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）

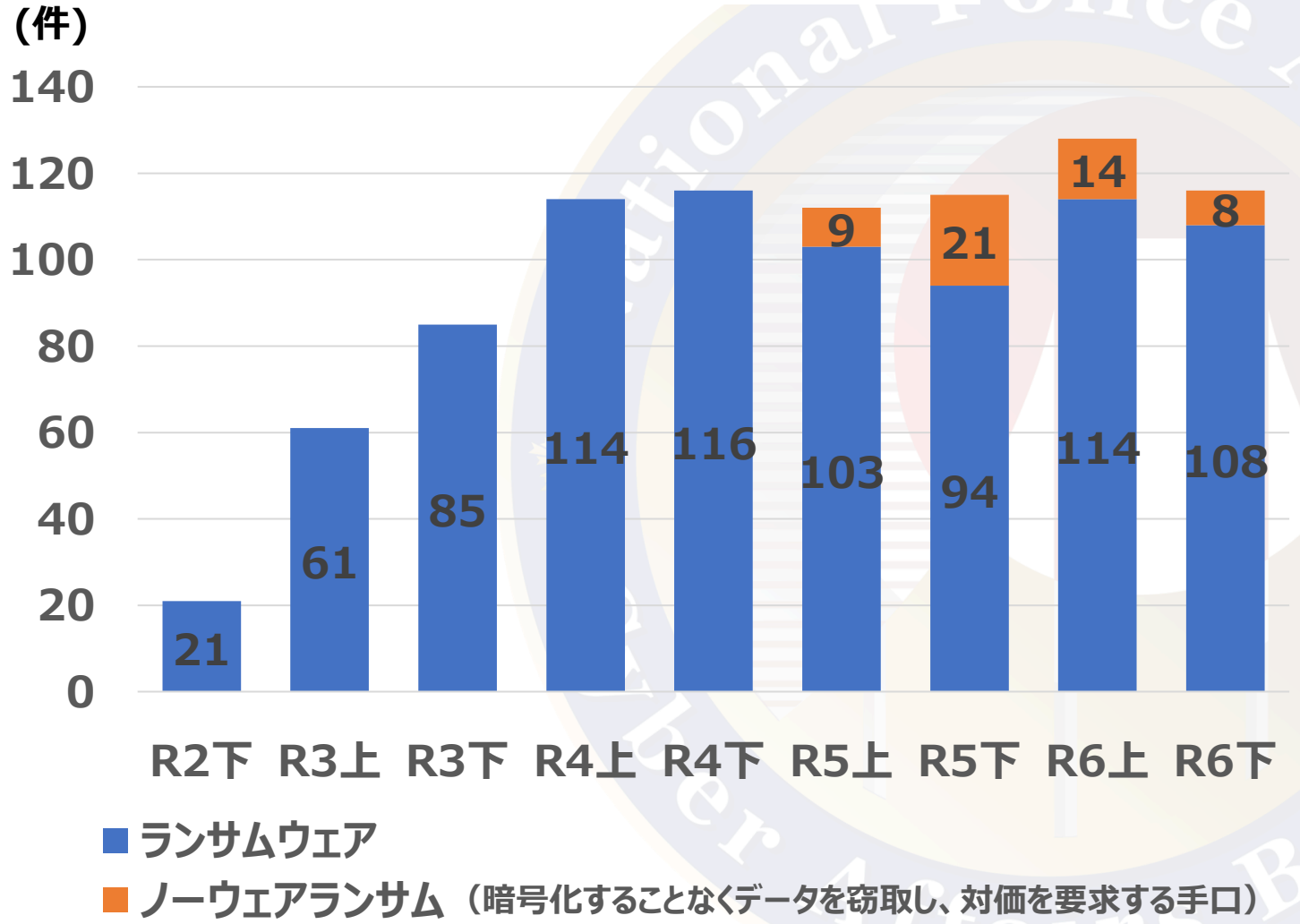


出典：警察庁「不正アクセス行為対策等の実態調査アクセス制御機能に関する技術の研究開発の状況等に関する調査（令和５年）」

ランサムウェア被害の情勢

ランサムウェア被害の情勢

【被害件数の推移】



○被害件数は高止まり

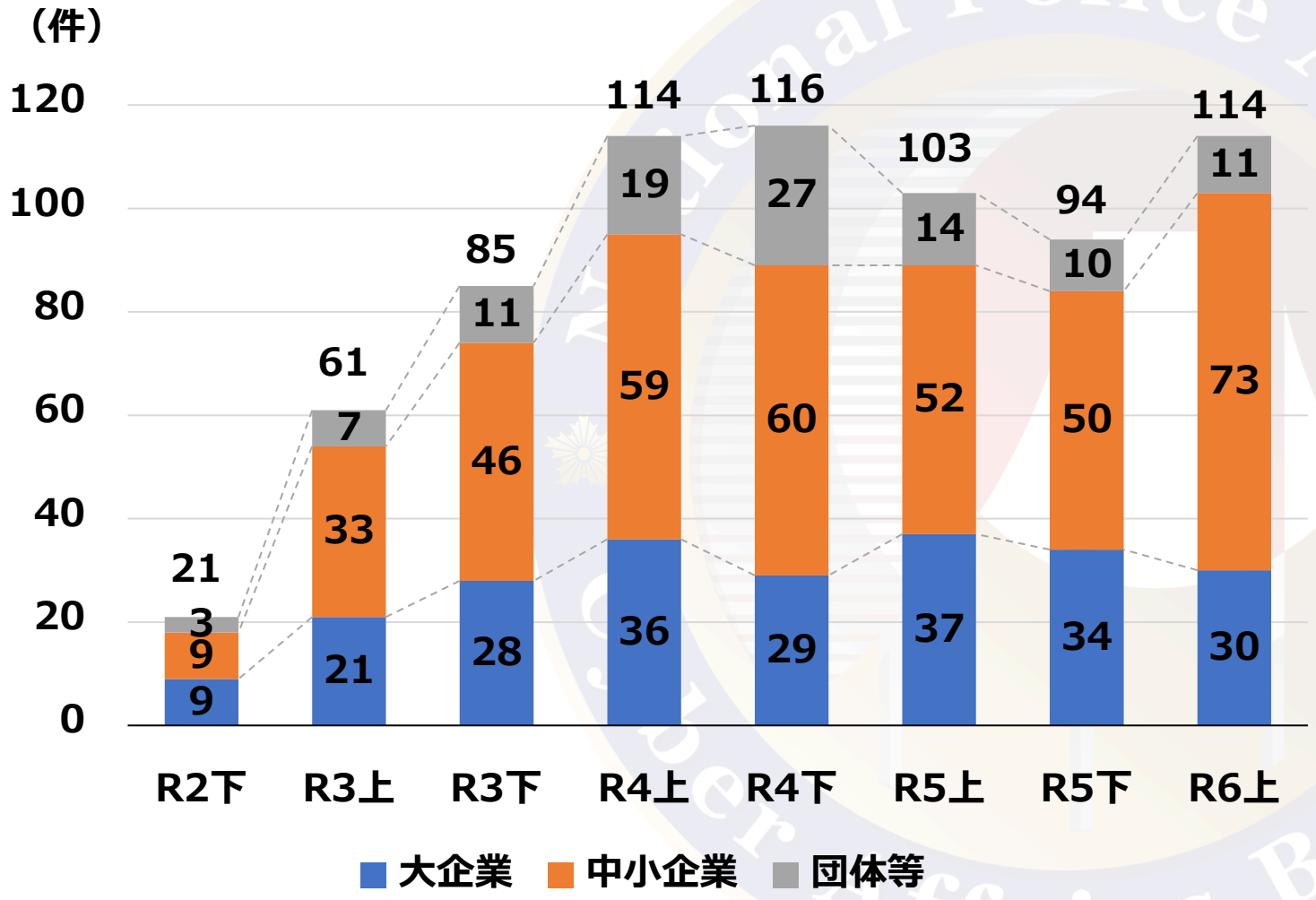
○約8割が「二重恐喝型」

○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）】

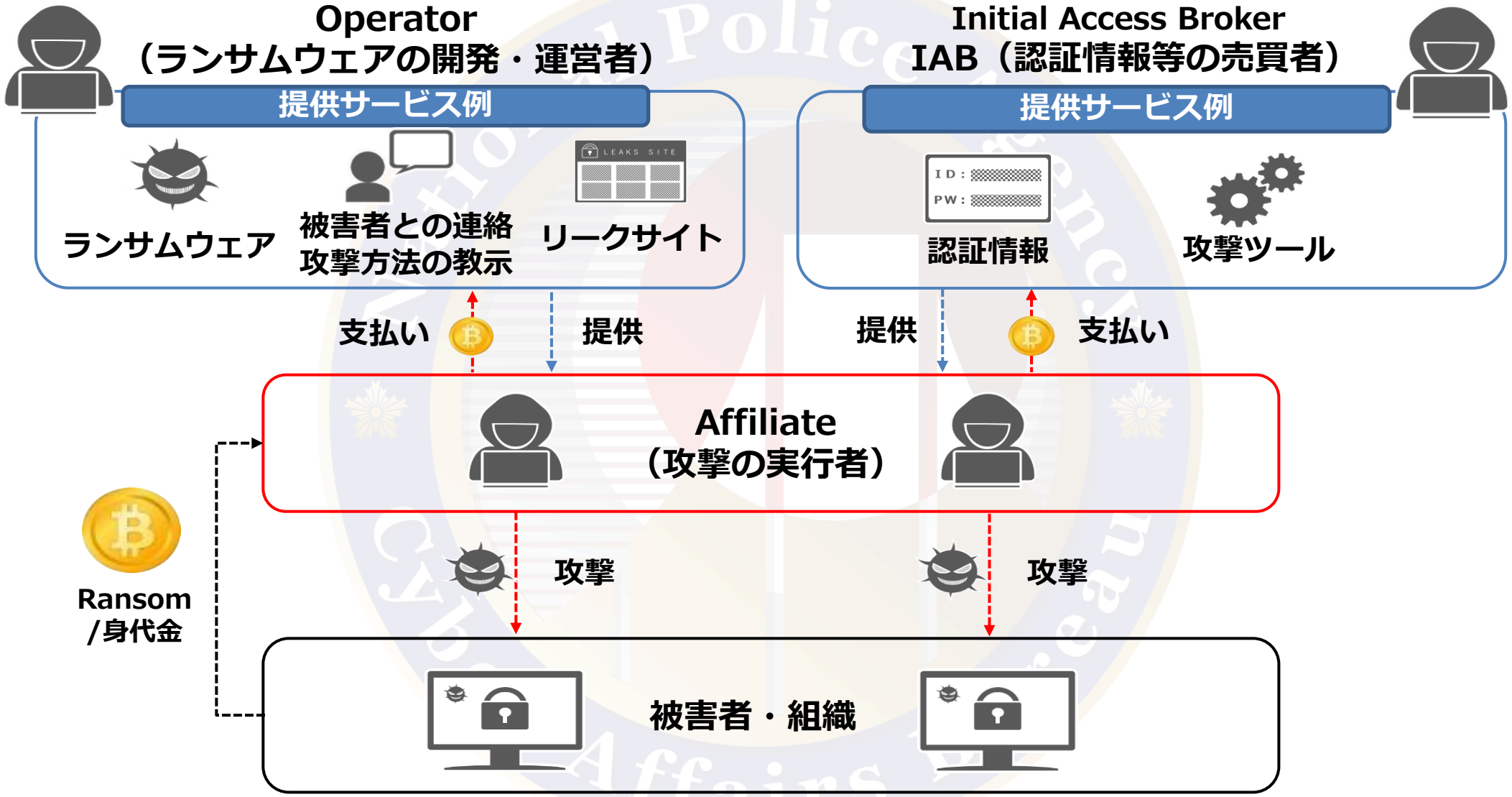


出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」から作成

○中小企業の被害は、前年から約4割増加

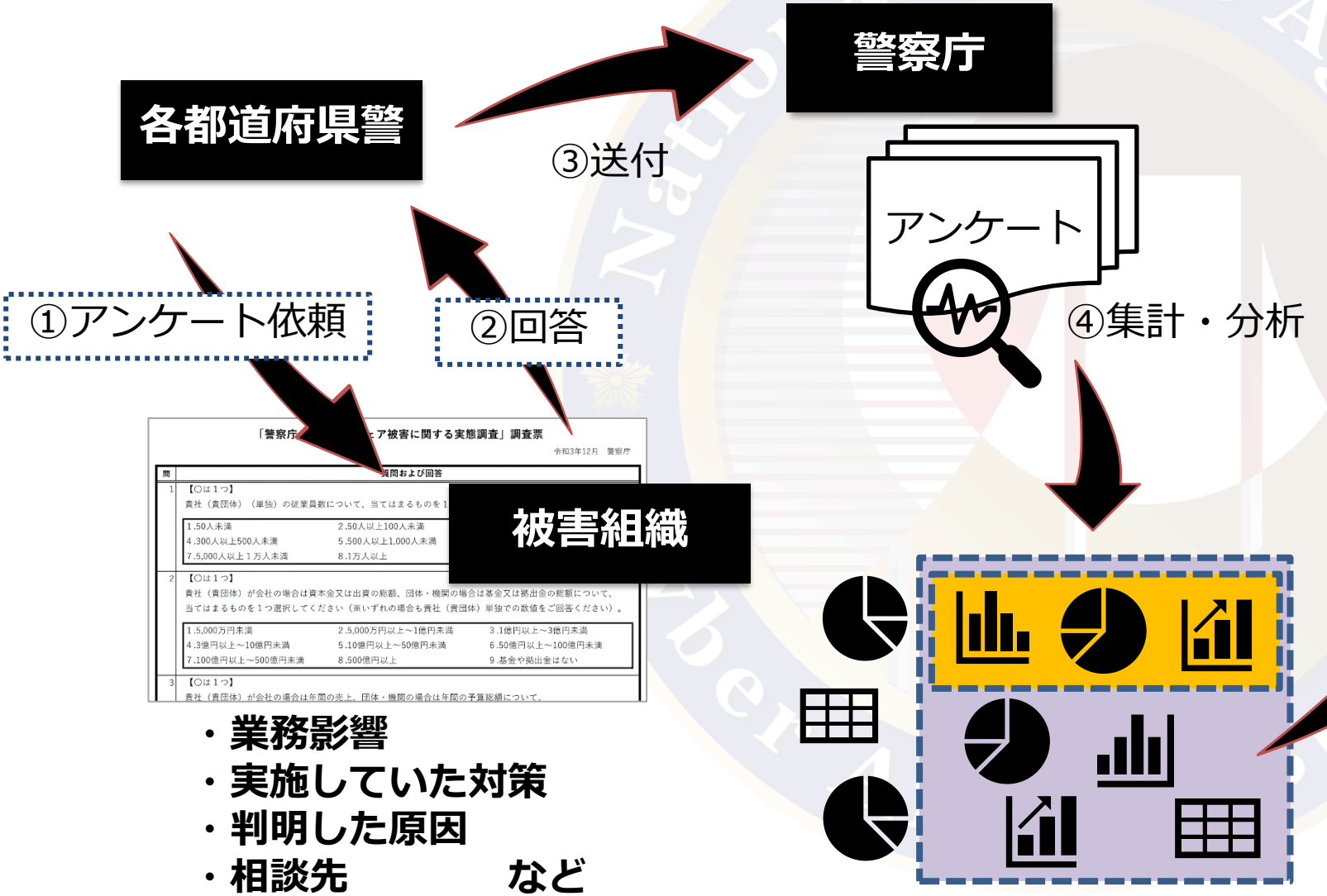
○大企業、団体等は減少
- 対策実施の効果？
- 攻撃側の変化？

Ransomware as a Service（RaaS）



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

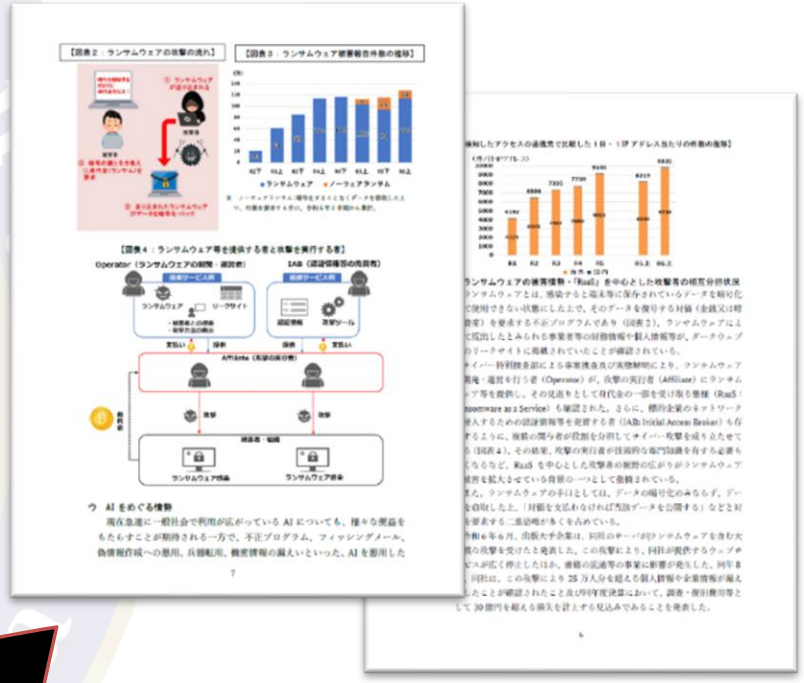


「警察庁　　ェア被害に関する実態調査」調査票

令和3年12月　警察庁

問	質問および回答
1	【○は１つ】 貴社（貴団体）（単独）の従業員数について、当てはまるものを１
	1.50人未満　2.50人以上100人未満 4.300人以上500人未満　5.500人以上1,000人未満 7.5,000人以上１万人未満　8.1万人以上
2	【○は１つ】 貴社（貴団体）が会社の場合は資本金又は出資の総額、団体・機関の場合は基金又は拠出金の総額について、当てはまるものを１つ選択してください（楽いずれの場合も貴社（貴団体）単独での数値をご回答ください）。
	1.5,000万円未満　2.5,000万円以上～1億円未満　3.1億円以上～3億円未満 4.3億円以上～10億円未満　5.10億円以上～50億円未満　6.50億円以上～100億円未満 7.100億円以上～500億円未満　8.500億円以上　9.基金や拠出金はない
3	【○は１つ】 貴社（貴団体）が会社の場合は年間の売上、団体・機関の場合は年間の予算総額について、

- 業務影響
- 実施していた対策
- 判明した原因
- 相談先　　など



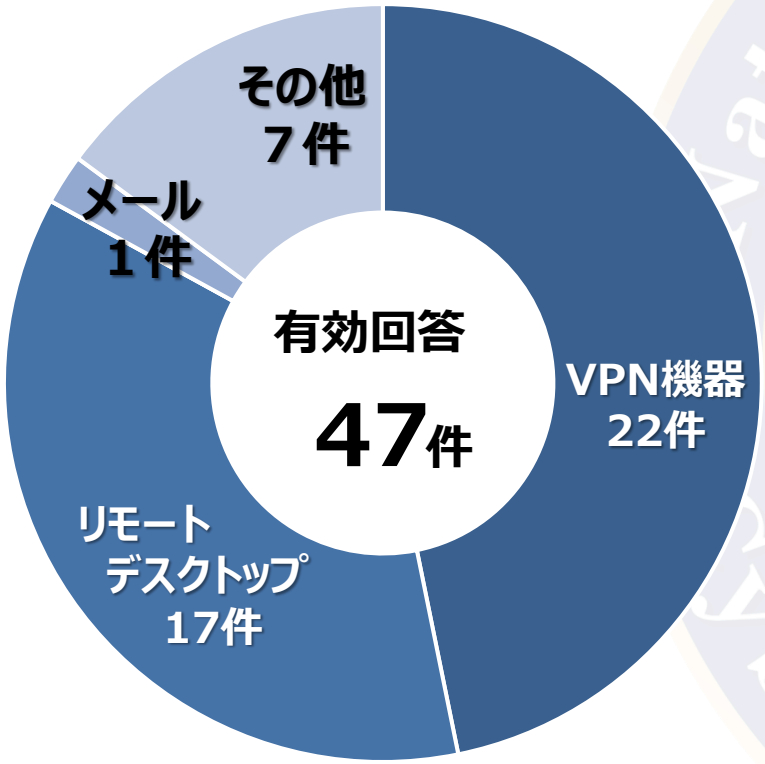
サイバー空間をめぐる脅威の情勢等

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

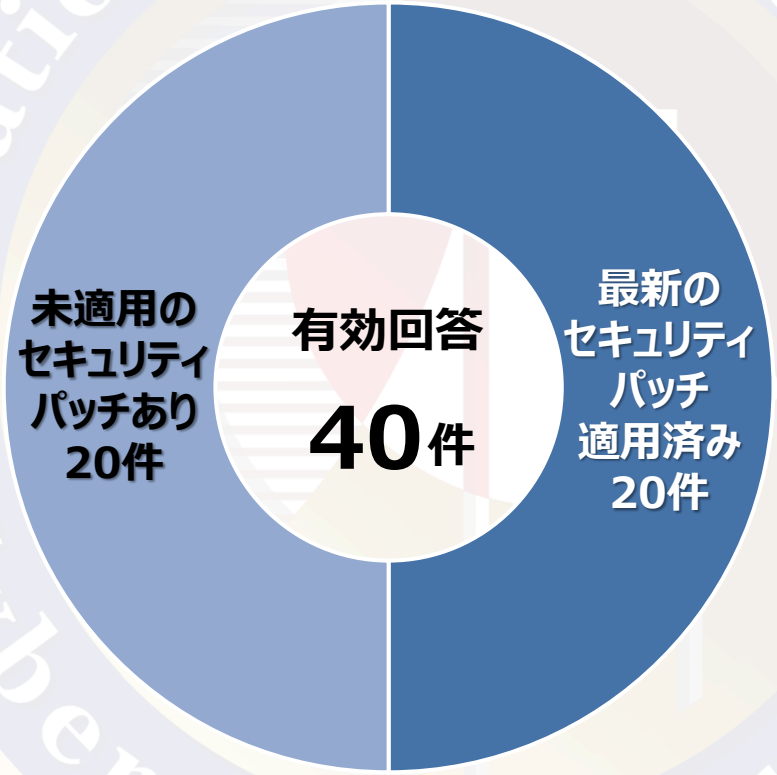
ランサムウェアの感染経路

【調査結果（感染経路）】

感染経路



感染経路のパッチ適用状況



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

○VPNとRDPで８割以上

→ セキュリティパッチ適用によるぜい弱性対処

- 昨年比では、VPN機器の割合減、RDPの割合上昇

○窃取した認証情報や総当たりでの不正ログインも

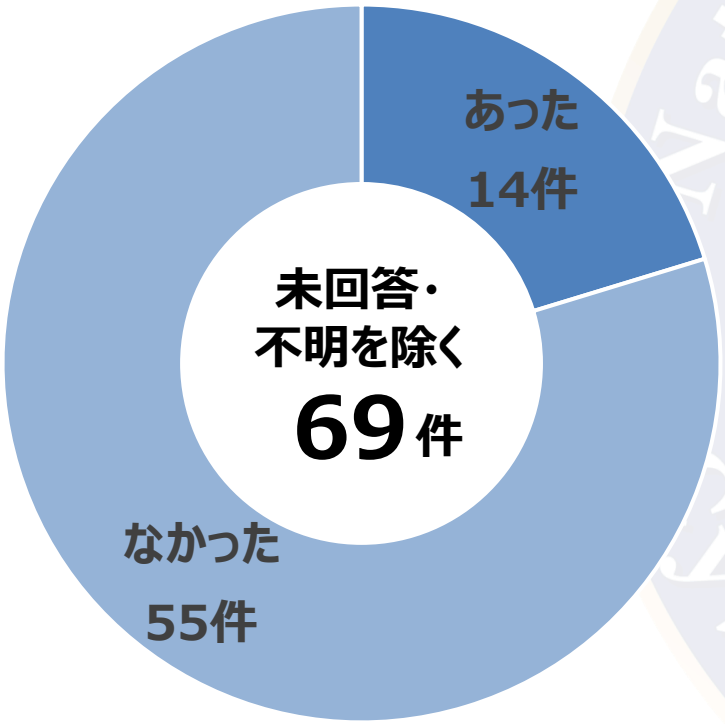
→ 認証強度の向上、認証情報の厳正な管理

→ 接続端末の制限、アクセス権限の適切な設定

セキュリティソフト等による検出状況

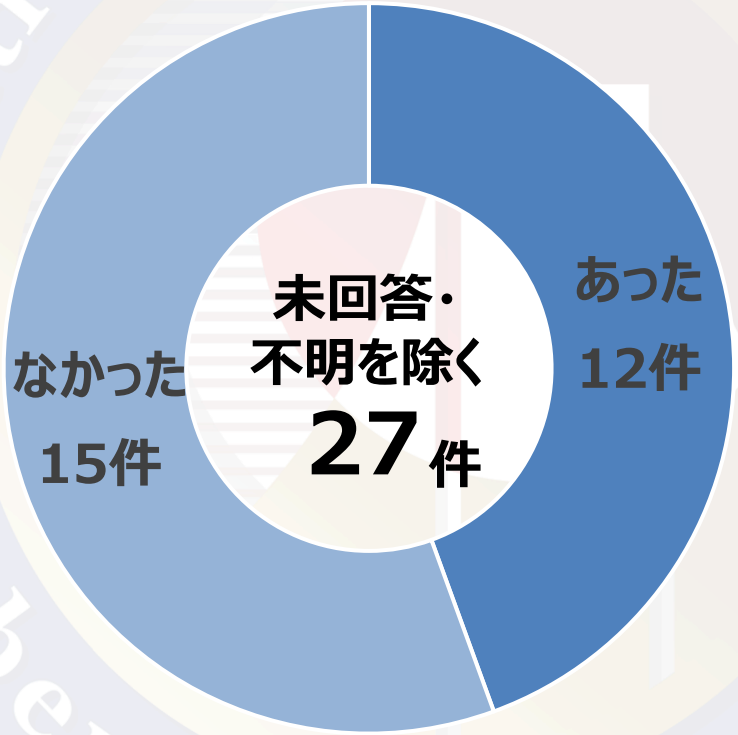
【調査結果（検出状況）】

ウイルス対策ソフト
による検出



※導入率91%

EDRによる検出



※導入率38%

○AVソフトで８割、
EDRでも半数は検知なし

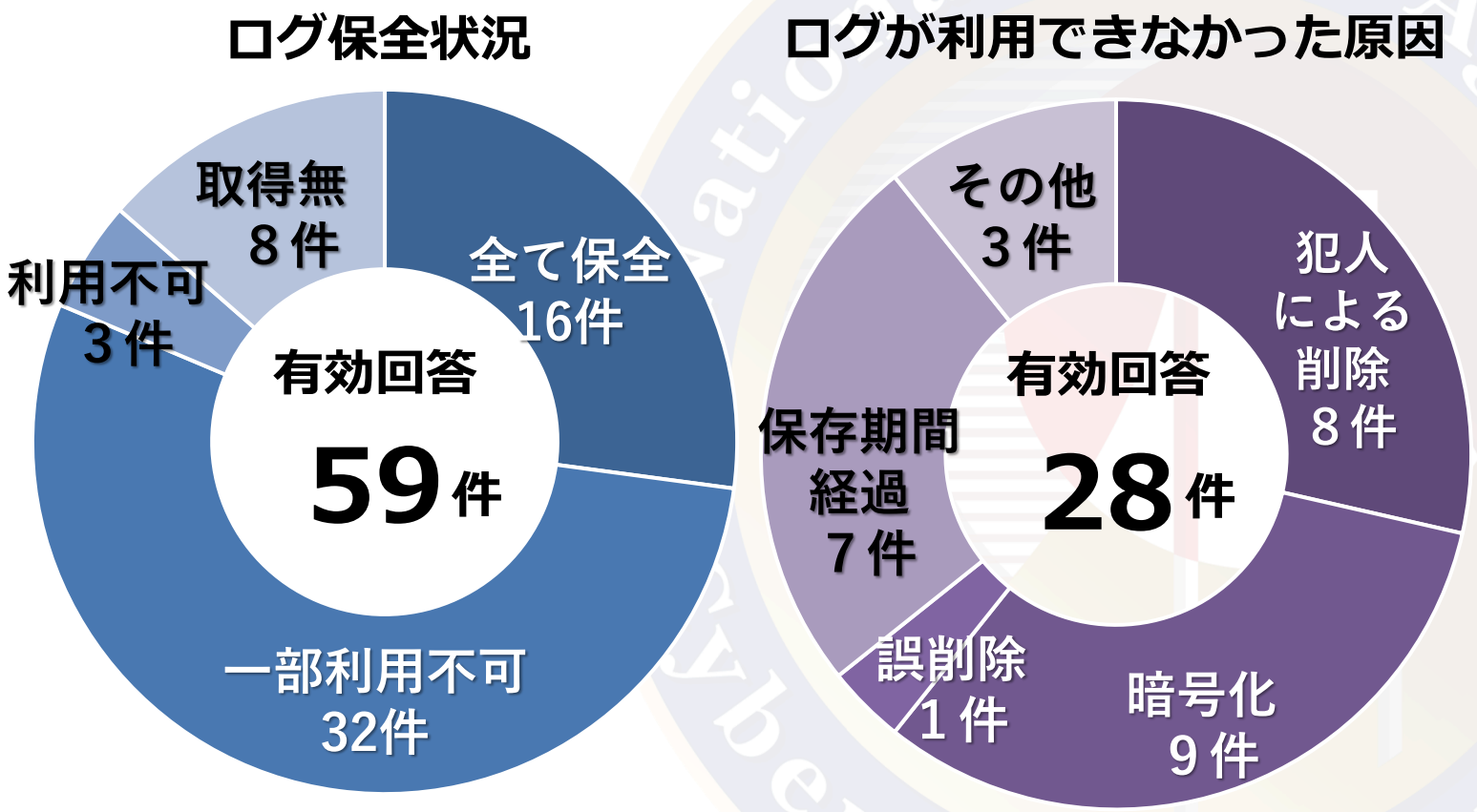
- 攻撃者による無効化や
製品未対応・未更新が原因

○**多層防御**による対策を

→ AV、EDR/xDR、FW…

ログの保全状況・使用可否

【調査結果（ログ状況）】



○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

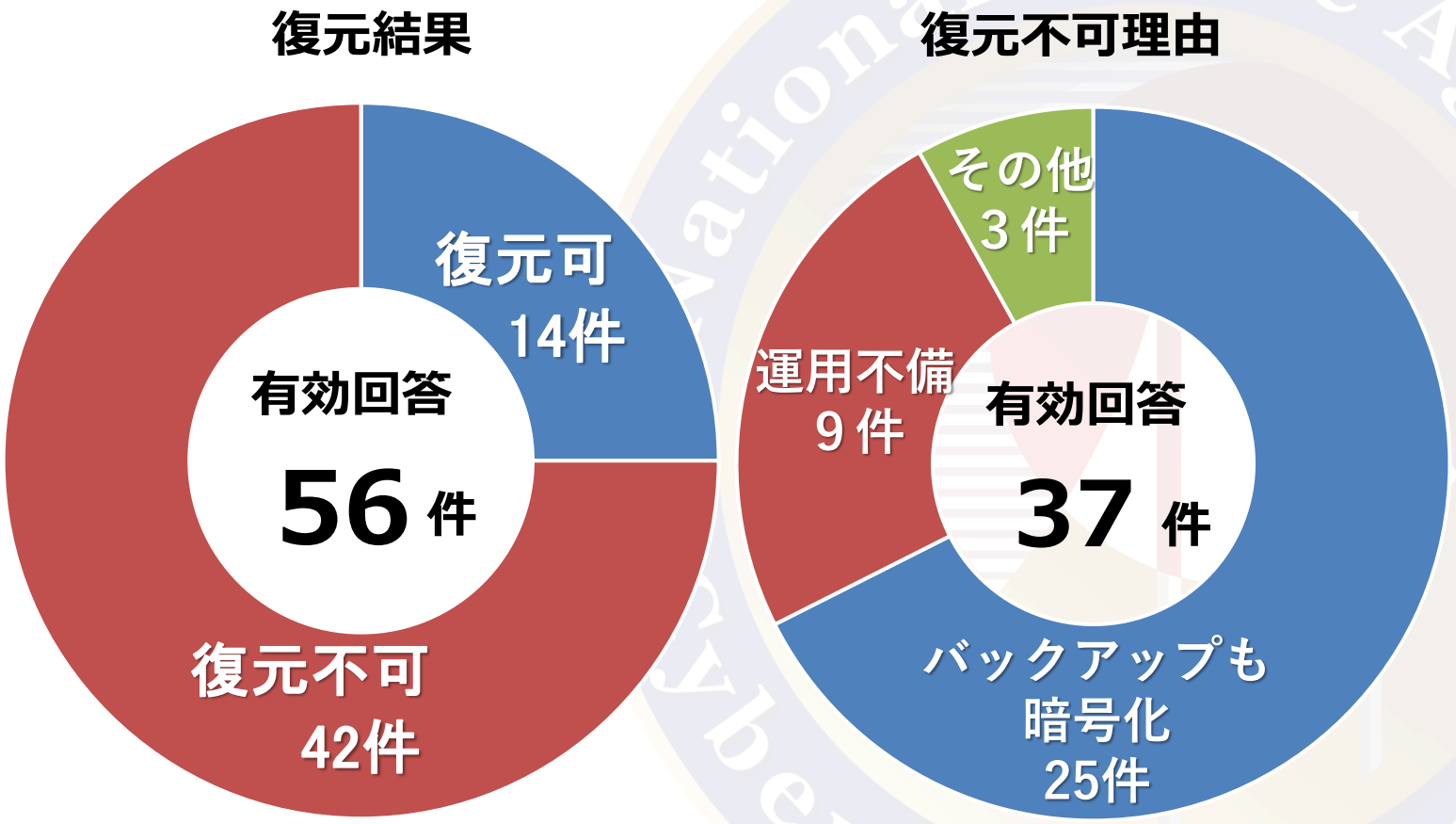
→サーバ・VPN機器等での、多面的なログ取得

→オフライン媒体等によるログの保存・管理

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

バックアップの復元状況

【調査結果（復元状況）】



○バックアップも暗号化される事案が多数

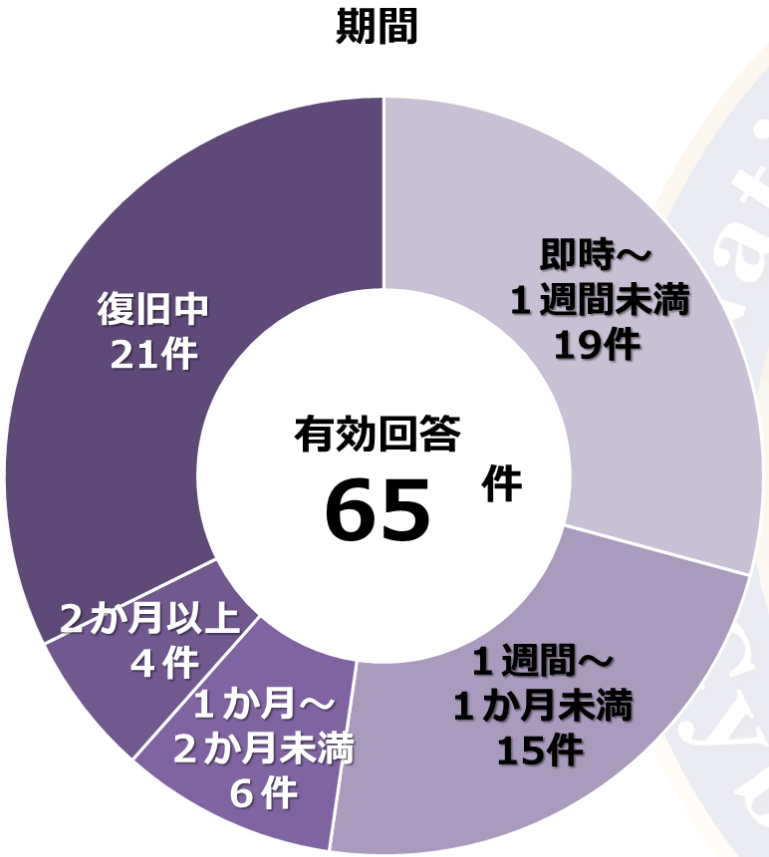
→資産の性質を勘案し、
オフライン／オンラインを組み合せたバックアップを

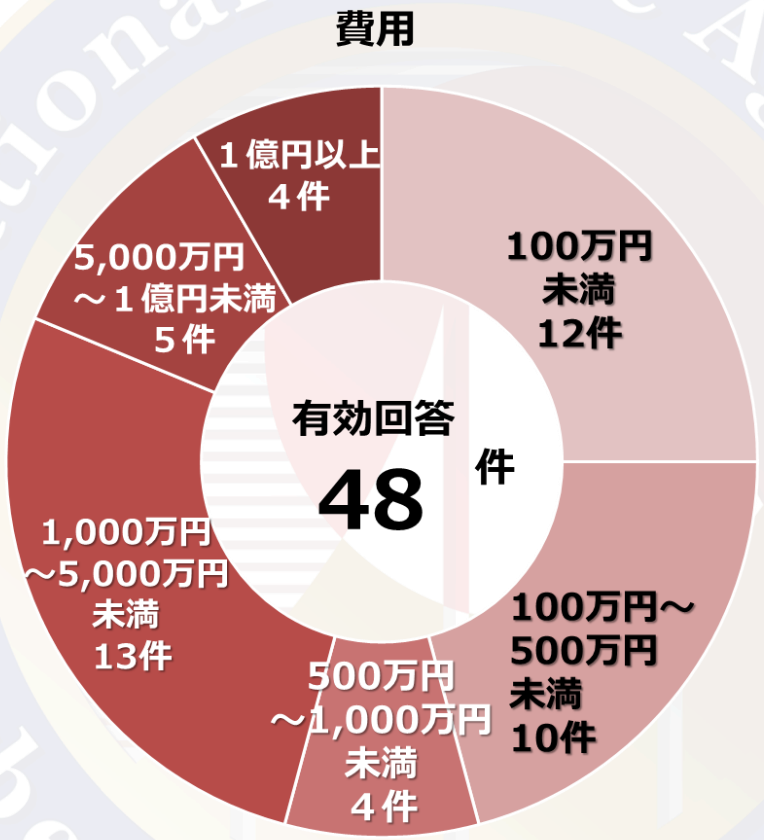
○運用不備による復元不可も約1/4を占める

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

調査復旧に要した期間・費用

【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

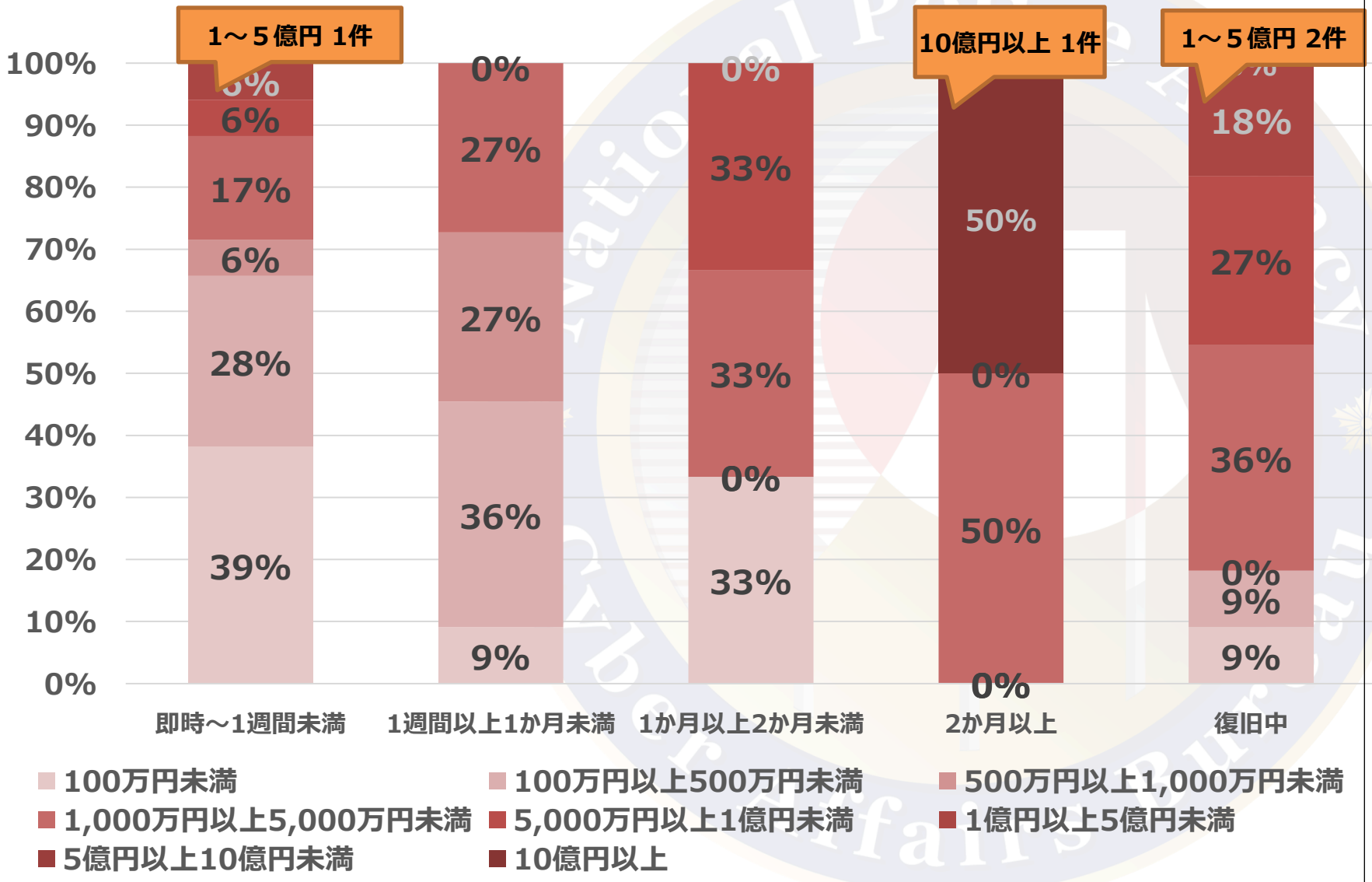
○被害組織の2/3はバックアップからの復元を選択
- 2割はシステム再構築
- 4%は復号ツール

○長期間・多額の復旧対応
- ここに表れないコストも

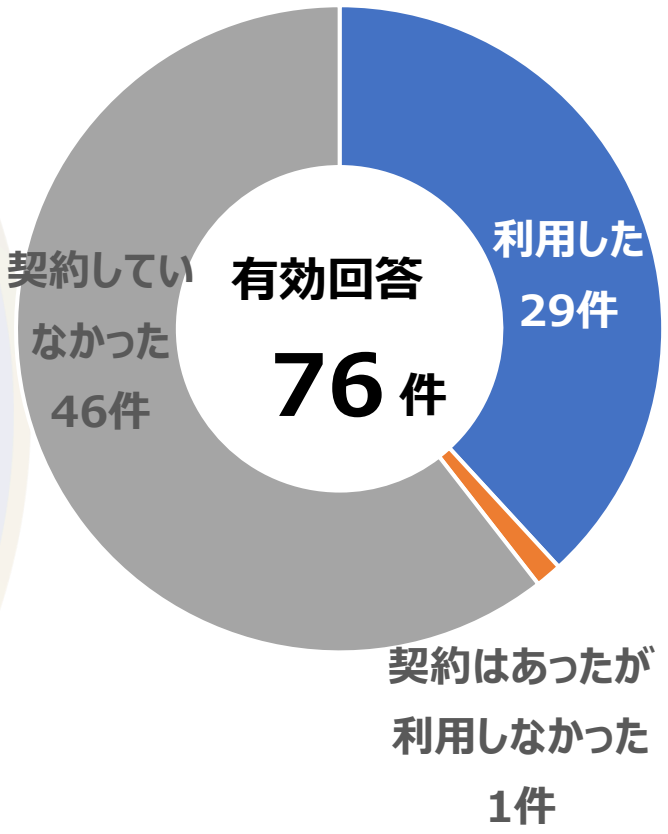
○セキュリティ対策の計画的な実施・更新
→ 関連予算に関する経営層の理解促進

調査復旧に要した期間・費用の相関、保険利用有無

【調査結果（調査復旧期間・費用の相関）】



【調査結果(保険利用有無)】



被害への備えと対応

事業継続のための備え

■ 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）

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

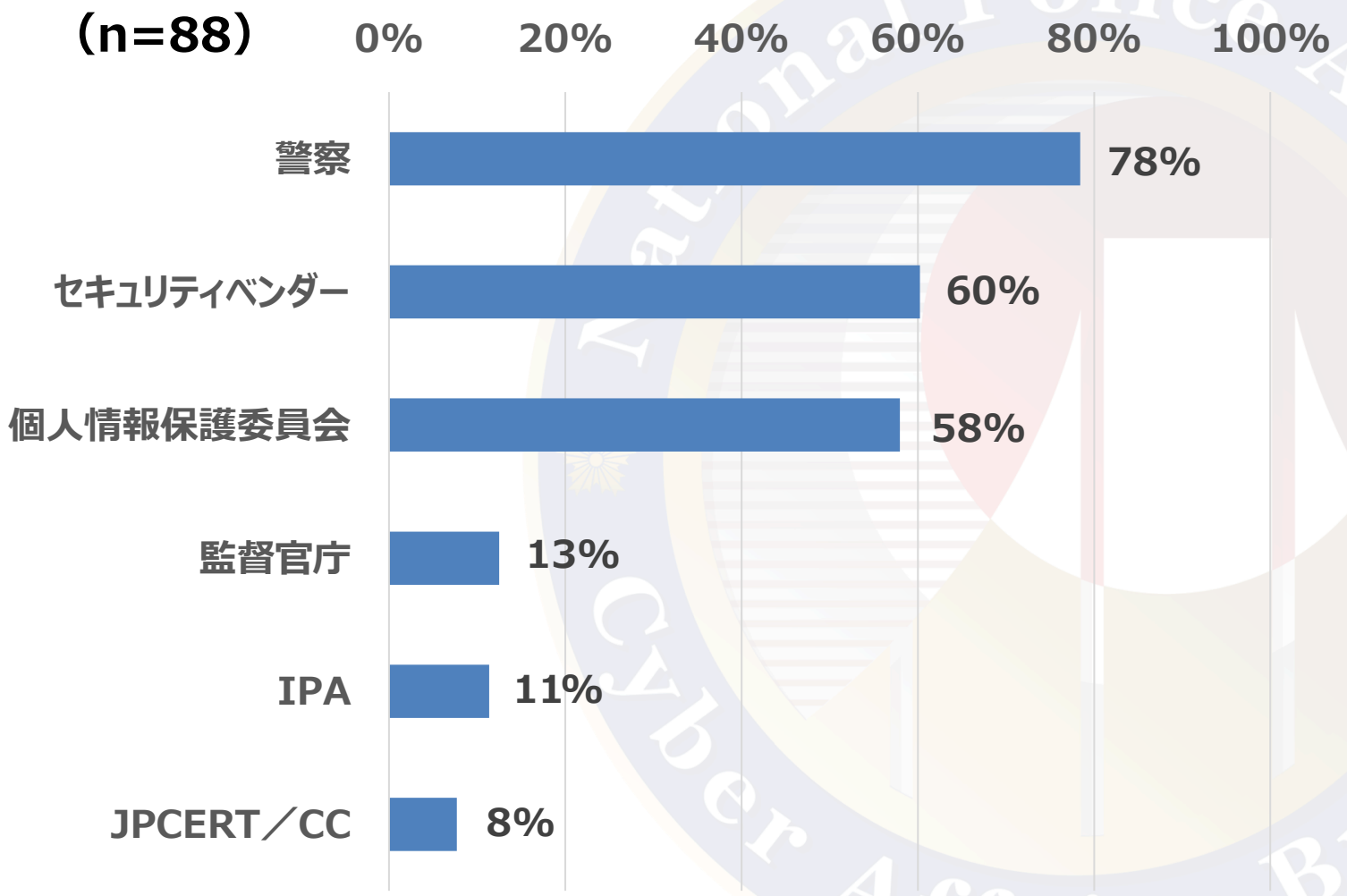
■ 警察等関係機関への通報・相談

■ 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

ランサムウェア被害発生時の通報・相談先

【調査結果（通報・相談状況）】



○セキュリティベンダー
- 大企業で約7割
- 中小企業で約6割

○個人情報保護委員会
- 大企業で８割超
- 中小企業で約半数

※アンケート結果であるものの警察が100%でないのは、未通報だが警察側で認知して連絡した件数があるため

警察への通報について

■ 警察への速やかな通報・相談

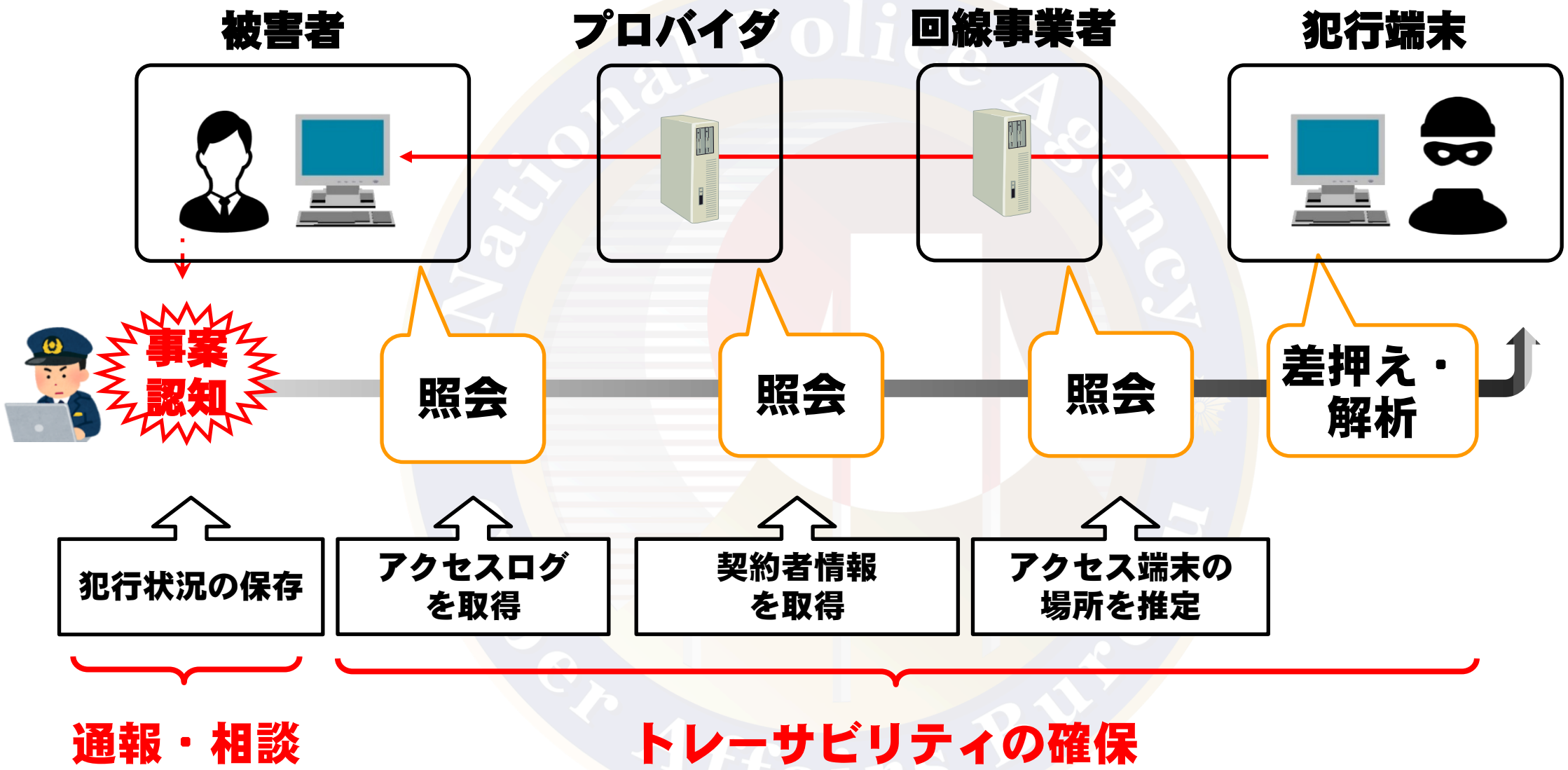
被害発生時は、最寄りの警察署や都道府県警察のサイバー犯罪相談窓口等に通報・相談して下さい。

≪サイバー事案に関する通報・相談のオンライン受付窓口≫

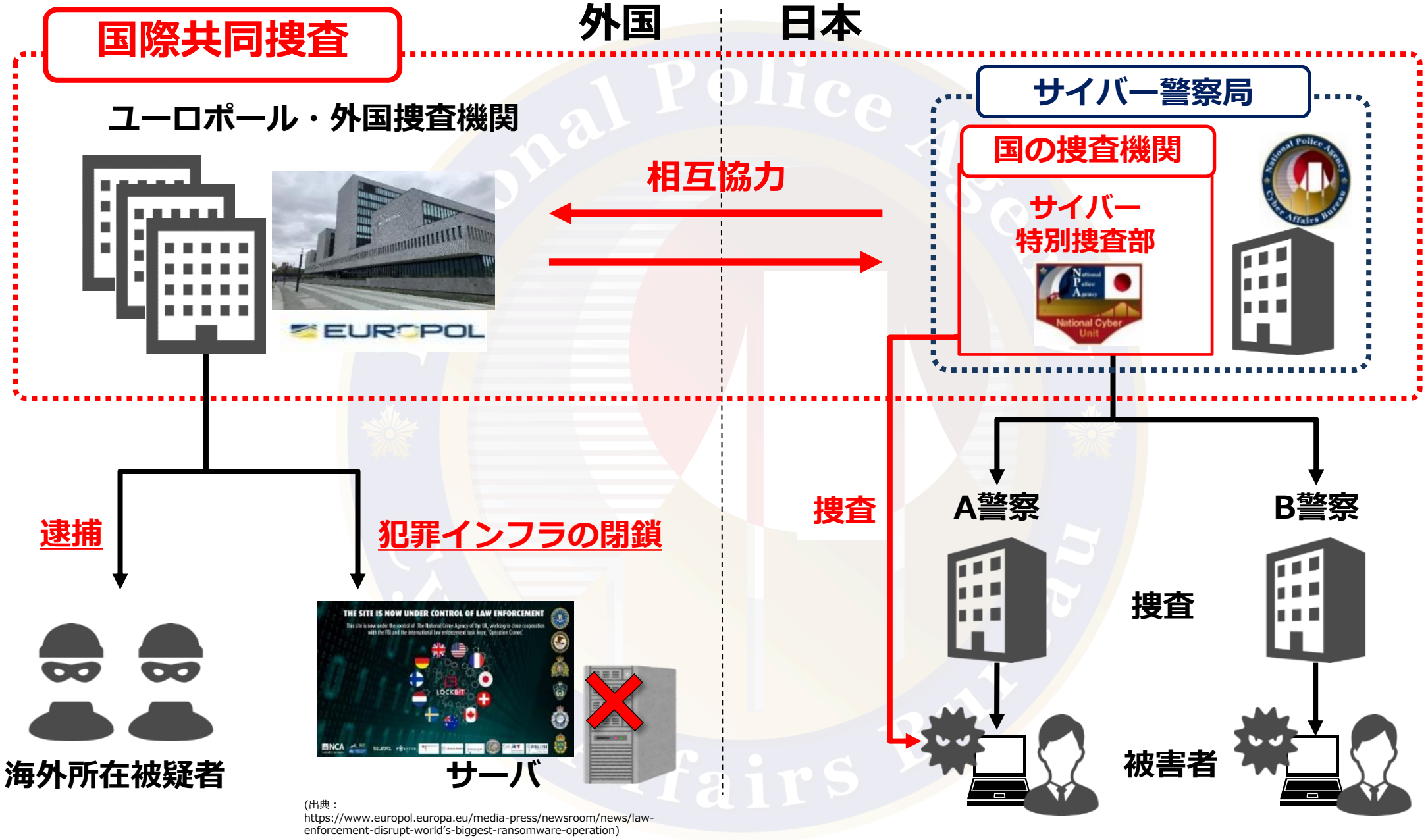
https://www.npa.go.jp/bureau/cyber/soudan.html

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。

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）



（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

海外機関

国際連携を通じた犯人検挙・抑止

産業界・学会

官民連携を通じた被害防止対策