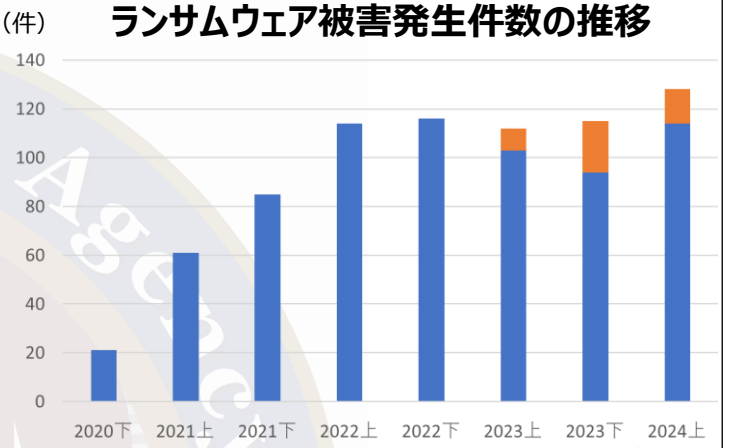
サイバー事案発生に備えた警察への連絡体制の整備等について

○依然として、**サイバー空間をめぐる情勢は極めて深刻**であり、**ランサムウェア攻撃による被害件数は高水準で継続中。**
長期間のサービス停止や大規模情報流出により、**企業経営や市民生活に大きな影響を及ぼす被害が続発。**

○被害企業においては**コンプライアンス遵守の観点からも必要な関係機関への通報が求められる**ところ、レピュテーションリスク等の懸念による**「被害の潜在化」が課題**。

○**警察では、被害拡大防止・早期復旧のための初動対応支援**や**暗号化復号ツールの案内**等を行っている。



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」より

警察庁からのお願い

①　警察への連絡体制の整備について

サイバー事案が発生した際に迅速に対応できるよう、警察への連絡体制の整備をお願いします。

＜対策例＞
・サイバー攻撃対応マニュアル等に警察の連絡先を記載する。
・サイバー攻撃を想定した事業継続計画(BCP)を策定し、初動対応における警察との連携を記載する。

よくある質問①

・関係機関との情報共有（相談）や公表の考え方は何を参考にすればよい？

⇒ **「サイバー攻撃被害に係る情報の共有・公表ガイダンス※」を参考にして下さい。**
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

サイバー事案発生に備えた警察への連絡体制の整備等について

② 被害発生時における対応について

- **速やかな通報・相談**

  最寄りの警察署又は都道府県警察のサイバー犯罪相談窓口に通報・相談して下さい。

  ＜都道府県警察のサイバー犯罪相談窓口＞ https://www.npa.go.jp/bureau/cyber/soudan.html

- **初動対応における警察との連携**

  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。**
  また、必要に応じて以下の内容を伺いますので、情報提供に御協力をお願いします。

  ・被害端末に関する情報(データ暗号化の有無、具体的な症状等)
  ・ネットワークの構成（ネットワーク構成図等）
  ・インターネットに接続可能な機器に関する情報(機器名、利用状況、パッチ適用の有無等)　　等

よくある質問②

・通報したら被害を公表させられるのでは？　レピュテーションリスク（信用の毀損・風評被害）が心配！

⇒ **警察から被害の公表を求めることはありません。警察も保秘を徹底します。**
通報して必要な捜査を行うこと、つまり「社会的責任を果たすこと」が、顧客や取引先等に対する説明責任を負う上で重要な要素となります。

・少しでも早く通常業務に戻したい。通報すると、警察対応で時間をとられて復旧作業が遅れそう。
サーバや端末のデータを全て持って行かれるのでは？

⇒ **警察は、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。**

・攻撃はあったが、被害が発生していない。捜査は望んでいない！

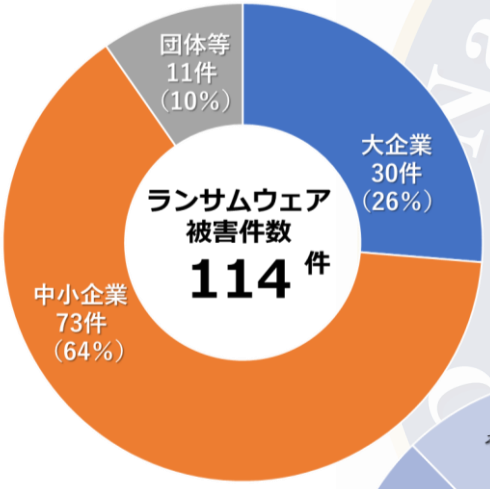
⇒ **「警察への相談 ＝ 捜査」ではありません。予兆や軽微な事案でも、ぜひ情報提供をお願いします。**

【参考１】ランサムウェアによる被害の発生状況

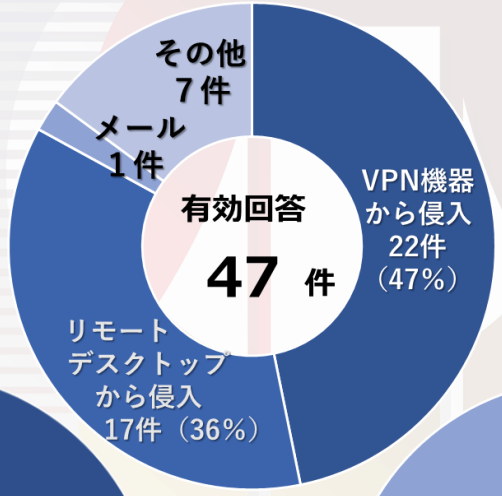
- 侵入経路は、VPN機器／リモートデスクトップからが8割強
- 被害組織の半数は、使用中のVPN機器等において最新のセキュリティパッチが未適用であった
- 約9割がウイルス対策ソフト・EDR等の対策を講じていたが、被害を受けている
  … 窃取した認証情報や機器のぜい弱性を悪用して侵入し、対策ソフト類を無効化する手法等による

VPN機器等のセキュリティパッチの速やかな適用によるぜい弱性対処、認証情報の厳正な管理を

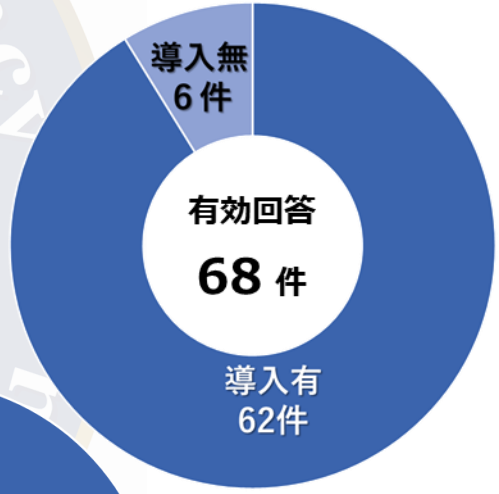
被害件数（規模別）



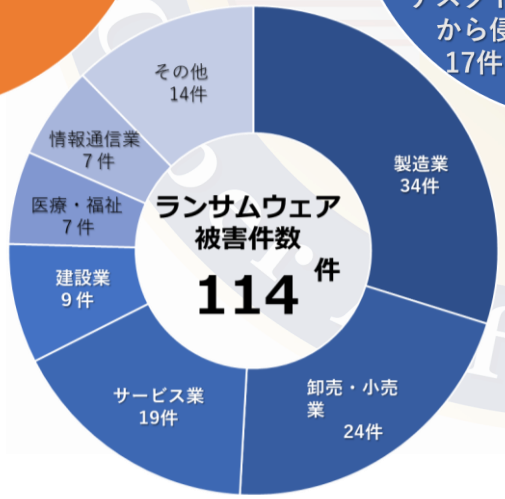
侵入経路



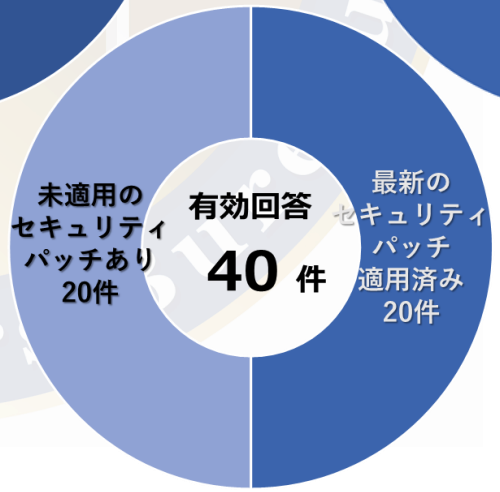
ウイルス対策ソフト等の導入状況



被害件数（業種別）



機器のパッチ適用状況



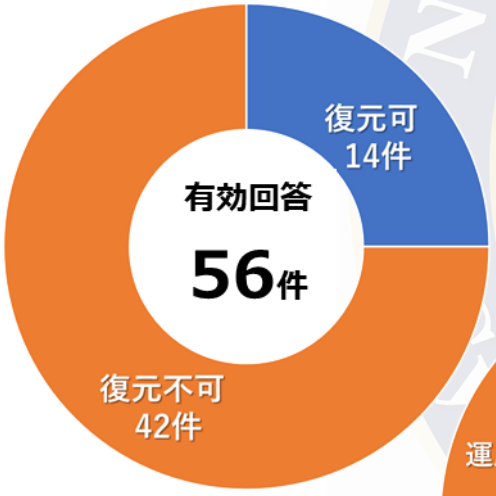
出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」

【参考２】ランサムウェアによる被害の発生状況

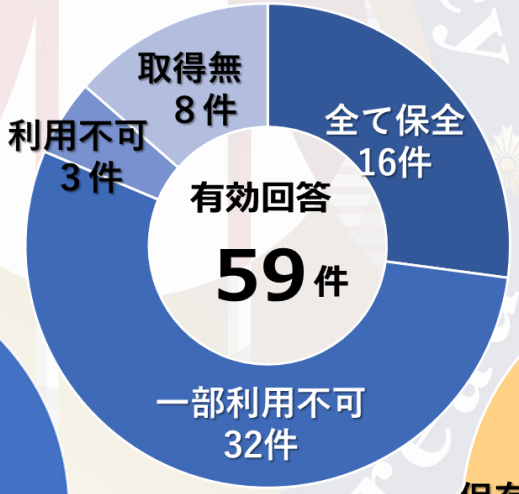
- **7割以上でバックアップからの復元に失敗**
  … オンライン接続されていることによりバックアップデータも暗号化された事例や、運用不備でバックアップを有効利用できない事例が多数。
- **侵入経路や情報窃取範囲の特定に不可欠なログも、ほとんどの場合で閲覧不可**
  … 犯人によって削除や暗号化されている事例が多数。

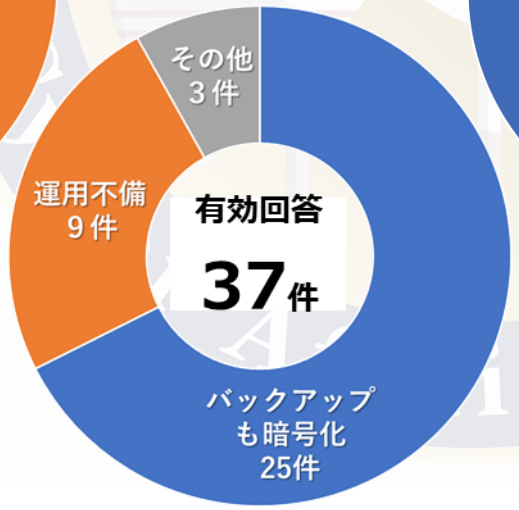
オフライン媒体を含む複数媒体への保存、運用体制の確認や訓練実施の検討を

バックアップからの復元可否

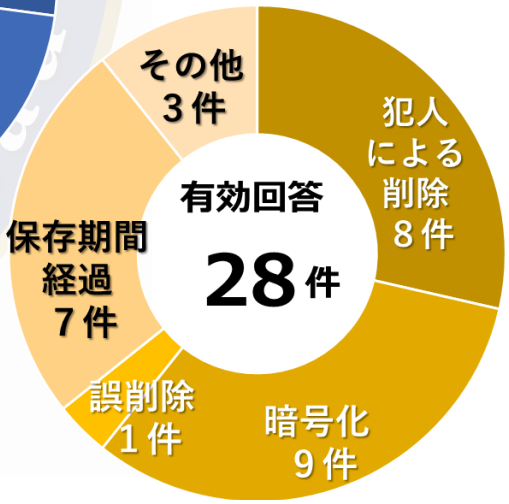


ログ保全状況





復元不可の理由



ログ閲覧不可の理由

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」