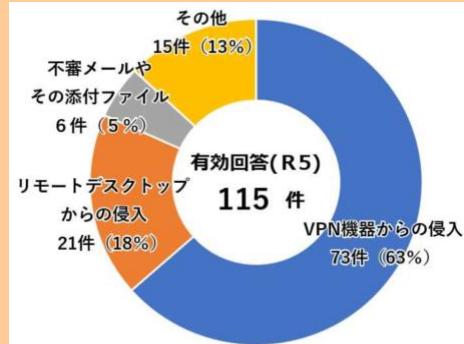
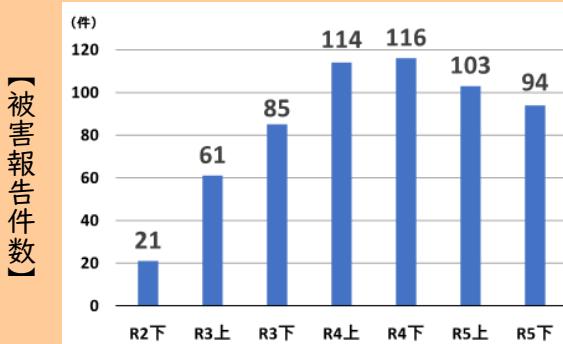


## 令和5年のサイバー攻撃情勢について

警察庁は3月14日、サイバー空間の脅威の情勢を示す指標、事例や警察の主な施策等を取りまとめた「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」を公表しました。

### 令和5年中のサイバー攻撃情勢

- 行政機関、学術研究機関等において情報窃取を企図したとみられる不正アクセス等が多数発生したほか、重要インフラ等の機能に影響を及ぼしたサイバー攻撃が発生
  - ◆ 6月：住宅設備関連機器メーカー（不正アクセスによるクラウドサービスの停止で全国約1,000のLPGガス会社の業務に影響）
  - ◆ 7月：名古屋港（ランサムウェア感染によるシステム障害で、物流に大きな影響）
- ランサムウェア被害の件数が197件と高水準で推移するとともに、データを暗号化する（ランサムウェアを用いる）ことなくデータを窃取し対価を要求する手口（「ノーウェアランサム」）による被害が、新たに30件確認



【感染経路】

- 標的型メール攻撃の傾向・事例として、メールの添付ファイルからフィッシングサイトへ誘導しようとするものや、実在する人物になりすましてメールを送り、複数回メールのやり取りを行い相手を信用させた後、相手の興味・関心を惹くファイル名を付けた不正プログラム（マルウェア）のファイルを送り、実行させるものなどを確認

### 警察における主な取組

- 内閣サイバーセキュリティセンター（NISC）、米国連邦捜査局（FBI）等とともに、中国を背景とするサイバー攻撃グループ「BlackTech」によるサイバー攻撃に関する合同の注意喚起（パブリック・アトリビューション）を実施
- サイバー特別捜査隊等がEUROPOL（ユーロポール）等との国際共同捜査を推進した結果、令和6年2月、関係国捜査機関が、世界各国の企業等に対してランサムウェア被害を与えた攻撃グループ「LockBit（ロックビット）」の一員とみられる被疑者2名を逮捕
- 自治体、電力事業者、金融機関等の幅広い分野の事業者等を対象に、標的型メールを題材とした訓練や警察との連携を確認するための現場臨場訓練等の実践的な共同対処訓練を約700回実施
- 重要インフラ事業者等に対して、ネットワーク機器やソフトウェア等の重大なぜい弱性を悪用したサイバー攻撃の手口に関して全国に注意喚起を実施

異常を検知すれば、警察へ速報をお願いします



京都府警察本部モノづくりプリザーブ事務局 075-451-9111（内線5821）

