

# 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（抜粋）

## ◆ 令和5年におけるサイバー攻撃の情勢等

### ① 情報窃取を企図した不正アクセス等の事例



- 8月以降、行政機関等は、電子メール関連システム機器の**ぜい弱性を悪用**したとみられる不正アクセスを受け、メールアドレスの一部が外部に漏えいした可能性があると発表した。
- 10月、国内の学術研究機関は、**標的型メール攻撃**により端末がマルウェアに感染した結果、不正アクセスを受け、個人情報等が漏えいした可能性があると発表した。
- 11月、国内の宇宙航空分野の研究開発機関は、同年夏頃に組織内の**イントラネットの管理用サーバに不正アクセス**が行われた可能性があると発表した。

### ② 重要インフラ等の機能に影響を及ぼしたサイバー攻撃の事例

- 6月、住宅設備関連機器メーカーは、同社が運営するクラウドシステムのサーバが不正アクセスを受け、クラウドサービスが停止したと発表した。これにより、全国約1,000のLPガス会社において、**検針業務が行えなくなるなどの影響**が生じた。
- 7月、名古屋港運協会は、コンテナの船積み・船卸や搬出入の作業等を一元的に管理するシステムがランサムウェアに感染し、システム障害が発生したと発表した。これにより、同ターミナルにおけるコンテナの**搬出入等が約3日間停止**し、物流に大きな影響が生じた。



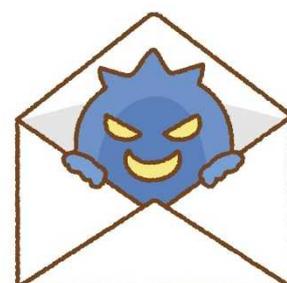
### ③ DDoS攻撃による被害とみられるウェブサイトの閲覧障害の事例



- 8月、政府機関、自治体等が運営するウェブサイトにおいて**閲覧障害が発生**した。同じ頃、SNS上に、ハクティビストのものとされる複数のアカウントから、それらの犯行をほのめかす投稿が確認された。
- 10月以降、事業者等のウェブサイトで**閲覧障害が発生**したほか、小規模サービス事業者が運営する**ウェブサイトが書き換えられる事案**が発生した。それらの発生と同じ頃、SNS上に、反イスラエルを掲げるハクティビストのものとされるアカウントから、それらの犯行をほのめかす投稿が確認された。

### ④ 標的型メール攻撃の傾向

令和5年、警察で把握した標的型メール攻撃の事例は、メールの添付ファイルからフィッシングサイトへ誘導するものや、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）のファイルを送信**し、実行させるものなどが確認されている。

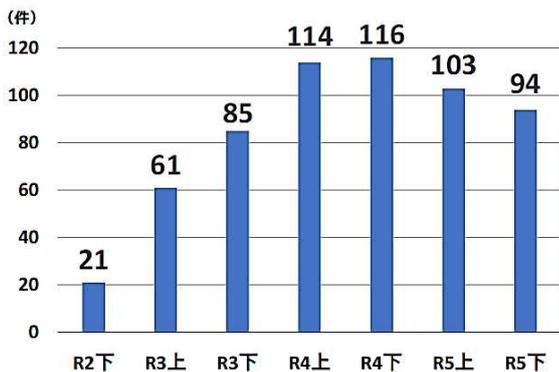


# ◆ 令和5年におけるランサムウェア被害の情勢等

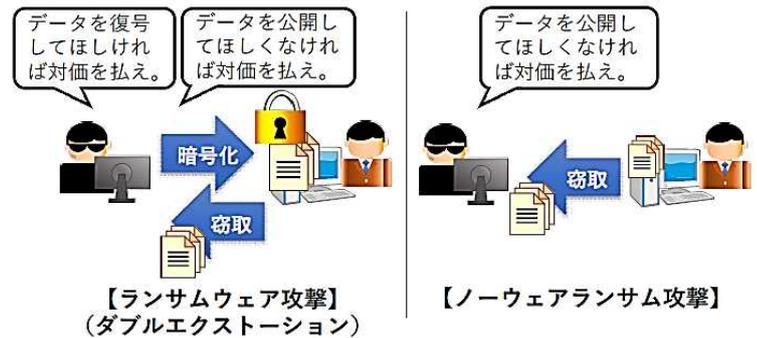
## ● 被害件数

- 令和5年に都道府県警察から警察庁に報告のあったランサムウェアによる被害の件数は**197件**であり、令和4年上半期以降、高い水準で推移している。
- ランサムウェアによる被害のほか、最近の事例では、企業・団体等のネットワークに侵入し、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た上で、企業・団体等に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**確認された。

企業・団体等におけるランサムウェア被害の報告件数の推移



攻撃の流れ (左：ランサムウェア攻撃、右：ノーウェアランサム攻撃)



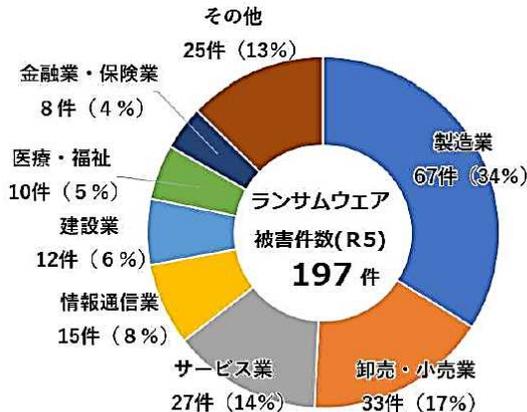
## ● 特徴

- ランサムウェアによる被害 (197件) のうち、手口を確認できたものは175件あり、このうち、**二重恐喝の手口によるものは130件**で74%を占めた。
- 直接的な対価の要求を確認できたものは31件あり、このうち、**暗号資産による支払の要求があったものは27件**で87%を占めた。

## ● 被害企業・団体等の規模

- 企業・団体等の規模別に見ると、大企業は71件、**中小企業は102件**であり、**その規模を問わず**、被害が発生した。
- 業種別に見ると、製造業は67件、卸売・小売業は33件、サービス業は27件であり、**その業種を問わず**、被害が発生した。

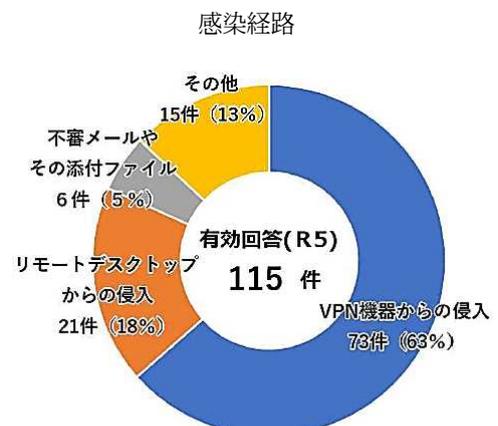
ランサムウェア被害の企業・団体等の業種別報告件数



注：図中の割合は小数第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。

## ● 被害の実態

- **VPN機器からの侵入が73件**で63%、**リモートデスクトップからの侵入が21件**で18%を占め、テレワーク等に利用される機器等のぜい弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが約82%と大半を占めた。



注：図中の割合は小数第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。