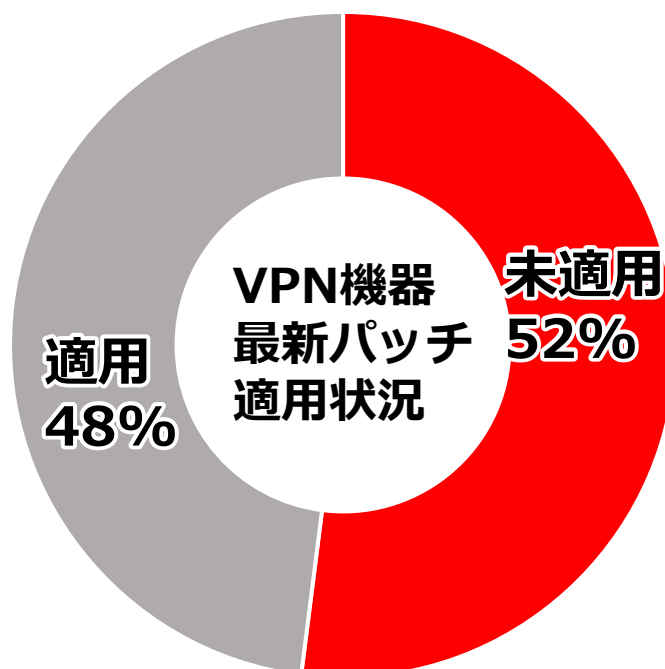


サイバー攻撃の被害に係る 企業・団体を対象としたアンケート調査結果及び対策

アンケートから分かる対策状況

VPN機器を利用している組織の
半分以上が最新のパッチを未適用



全体の約4割が社外からの業務アクセス
時の認証にID・パスワードのみ

認証方法

1位	ID・パスワードのみ	39.8%
2位	電子証明書	27.5%
3位	認証アプリ	23.2%
4位	ワンタイムパスワード	17.8%
5位	SMS認証	6.1%

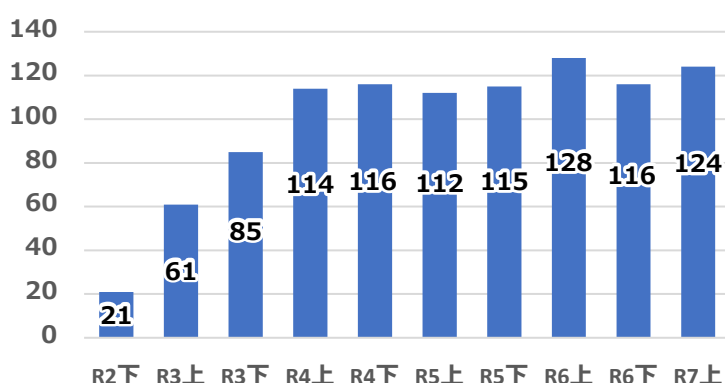
侵入経路の脆弱性放置、弱い認証方式

ランサムウェア被害のおそれ

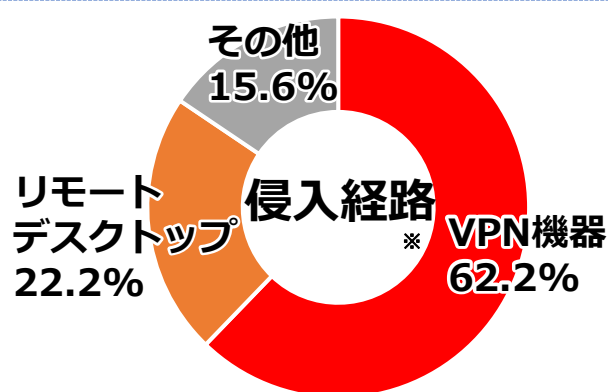
ランサムウェア被害の状況

中小企業を中心として被害は高止まり

被害報告件数の推移※

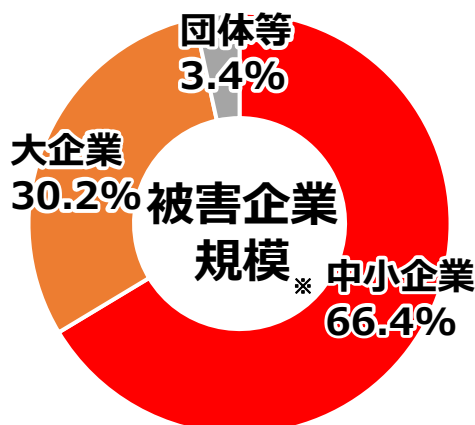
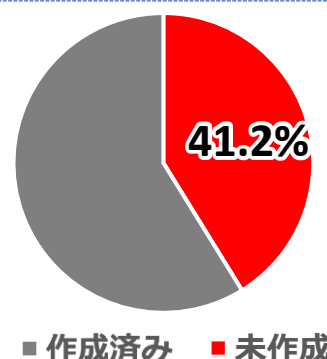


VPN機器の悪用が多数



事故対応マニュアル等の作成

約4割が未作成 被害拡大のおそれ



被害に遭わない、被害を抑えるために

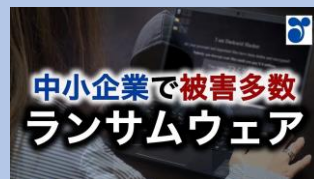


詳しくは、政府広報オンライン動画
「中小企業で被害多数 ランサムウェア」

警察庁制作協力



<https://www.gov-online.go.jp/useful/202506/video-298784.html>



未然防止

■ 認証方式

多要素認証の導入

異動で使わなくなったIDは削除

パスワード長は一定以上に

■ 脆弱性対策

ネットワーク機器のアップデート

OS・ソフトウェアの更新

ウイルス対策ソフトの更新

拡大防止

サイバー攻撃を想定した業務継続計画（BCP）の策定

オフラインを含むバックアップの取得

被害調査に必要不可欠なログの取得



動画「ランサムウェア対策の基本」

<https://www.gov-online.go.jp/vertical/online/video-478.html>

記事「ランサムウェア、あなたの会社も標的に?被害を防ぐためにやるべきこと」

<https://www.gov-online.go.jp/useful/article/202210/2.html>



**⚠ 被害に遭ってしまったら
警察に通報・相談!!**



警察庁

National Police Agency

ご相談は「サイバー事案に関する相談窓口」へ

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

