

サイバー犯罪被害に係る 企業・団体を対象としたアンケート調査結果及び対策

過去1年以内に受けたことのある被害

ランサムウェア被害が倍増

R2

1位	メール不正中継	12.8%
2位	ランサムウェア	11.9%
3位	情報流出	6.4%

※ 被害を受けた団体における割合

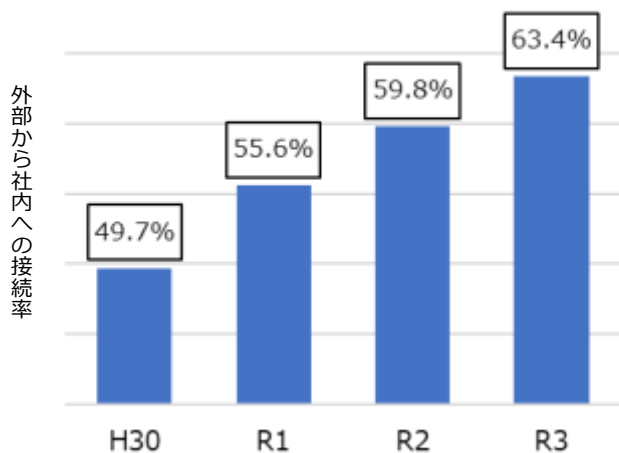
R3

1位	ランサムウェア	22.1%
2位	メール不正中継	15.8%
3位	情報流出	12.6%

※ ランサムウェアとは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価として金銭を要求する不正プログラム

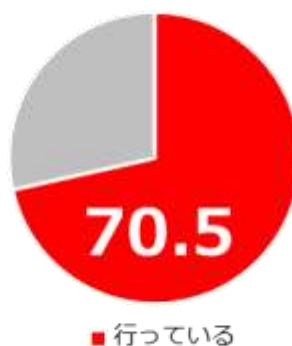
外部から社内への接続・テレワーク

業務上の外部からの接続が急増

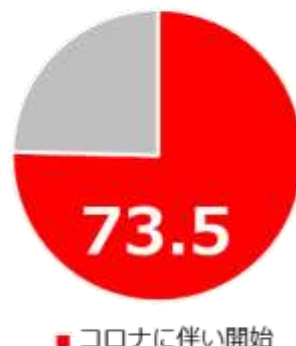


新型コロナ拡大による開始は7割以上

テレワーク実施状況



テレワーク開始時期

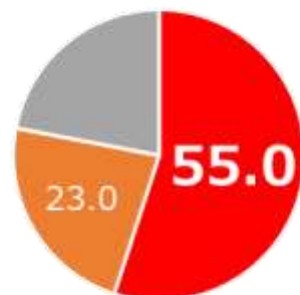


セキュリティ対策

VPNの導入が増加

	H30	R1	R2	R3
1位	ファイヤーウォール	IDパスワード	IDパスワード	IDパスワード
2位	IDパスワード	ファイヤーウォール	ファイヤーウォール	ファイヤーウォール
3位	Proxyサーバ	Proxyサーバ	VPNの利用	VPNの利用

ランサム感染経路は半数以上がVPN

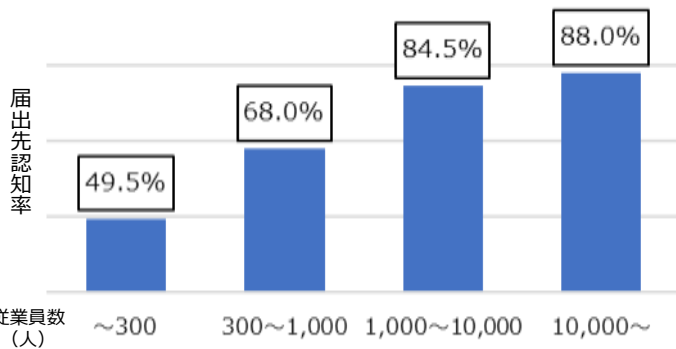


■ VPN機器からの侵入
■ リモートデスクトップからの侵入

被害発生時の届出先の認知状況等

中小企業の認知率が低い

最も多い届出先は「警察」



1位 警察

2位 情報処理推進機構

3位 監督官庁

被害に遭わないために

OSなどの脆弱性対策

OSやアプリケーションソフト、VPN機器などに脆弱性があるとマルウェアに感染したりネットワークに侵入されるおそれがあります。

OS・ソフトウェアの更新

ウイルス対策ソフトの更新

ネットワーク機器ソフトウェアの更新

認証情報の適切な管理

VPN機器やリモート・デスクトップ・サービスなどの認証パスワードが脆弱な場合、ネットワークに侵入されるおそれがあります。

パスワード長は一定以上に

異動で使わなくなったIDは削除

IDを複数ユーザで共有しない

⚠ 被害に遭ってしまったら 警察へ通報

より詳しい被害防止対策は警察庁「ランサムウェア被害防止対策ページ」 → <https://www.npa.go.jp/cyber/ransom/index.html>

