愛知県警察
サイバー犯罪対策課

サイバー犯罪対策通信

第R6-16号
組織向け

中小企業で被害多数 ランサムウェア

サイバー攻撃のリスクを考慮した管理体制の構築を！

出典：警察庁 令和5年・6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 より

中小企業のランサムウェア被害は前年比で約4割の増加

被害未然防止の要は基本的対策の継続

- ＶＰＮ機器等の**ソフトウェア更新**
- **パスワードの強度確保**　等

被害拡大防止のために必要な備え

- サイバー攻撃を想定した**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**

被害発生時は警察へ通報・相談を

※政府広報オンライン「中小企業で被害多数 ランサムウェア」より

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

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

政府広報 **SNSでも関連動画を公開中**

X

Instagram

愛知県警察サイバー犯罪対策課は、X（旧ツイッター）や愛知県警察ホームページでサイバー犯罪被害防止に役立つ情報を発信しています！
サイバー犯罪被害防止対策にぜひご活用ください！

愛知県警察
ホームページ

サイバー犯罪対策課
X（旧ツイッター）

警察庁
National Police Agency

愛知県警察
サイバー犯罪対策課

サイバー犯罪対策通信

第R7-17号
組織向け

組織向け情報セキュリティ対策

長期休暇前にチェックすること

長期休暇中は、平常時に比べ体制が弱くなり、セキュリティインシデントが発生した際に、対応が遅れたり、予期せぬ被害が発生したりするおそれがあります。
有事に備え、しっかりと対策をしておきましょう。

経営者・管理者向け

□ **緊急連絡体制の確認**
不測の事態が発生した場合に備えて、委託先企業を含めた緊急連絡体制や対応手順等が明確になっているか確認してください。

□ **社内ネットワークへの機器接続ルールの確認と遵守**
長期休暇中にメンテナンス作業などで社内ネットワークへ機器を接続する予定がある場合は、社内の機器接続ルールを事前に確認し遵守してください。

□ **使用しない機器の電源OFF**
長期休暇中に使用しないサーバ等の機器は電源をOFFにしてください。

利用者向け

□ **機器やデータの持ち出しルールの確認と遵守**
長期休暇に社外での対応が必要となるパソコン等の機器やデータ等の情報を持ち出す場合は、持ち出しルールを事前に確認し遵守してください。

□ **使用しない機器の電源OFF**
長期休暇中に使用しない機器は電源をOFFにしてください。

□ **持ち出した機器やデータの厳重な管理**
長期休暇中、自宅等に持ち出したパソコン等の機器やデータは、ウイルス感染や紛失、盗難等によって情報漏えい等の被害が発生しないよう、厳重に管理してください。

被害に遭ってしまったら、最寄りの警察に通報・相談してください！

愛知県警察
サイバー犯罪対策課

サイバー犯罪対策通信

第R7-18号
組織向け

組織向け情報セキュリティ対策

長期休暇後にチェックすること

長期休暇明けは、休暇中に異常がなかったかログなどでしっかりと確認しましょう。
また、ソフトウェアの脆弱性情報を確認し、必要に応じてアップデートしてください。
従業員に対しては、再度電子メール対策について注意喚起しましょう。

経営者・管理者向け

□ **修正プログラムの適用**
長期休暇中にOS（オペレーティングシステム）や各種ソフトウェアの修正プログラムが公開されている場合があります。

□ **定義ファイルの更新**
電子メールの送受信やウェブサイトの閲覧等を行う前に定義ファイルを更新し、最新の状態にしてください。

□ **サーバ等における各種ログの確認**
何らかの不審なログが記録されていた場合は、早急に詳細な調査等の対応を行ってください。

利用者向け

□ **修正プログラムの適用**
長期休暇中に公開された各種ソフトウェアの修正プログラムを、システム管理者の指示に従ってインストールしてください。

□ **定義ファイルの更新**
電子メールの送受信やウェブサイトの閲覧等を行う前に、長期休暇中に公開されたセキュリティソフトの定義ファイル(パターンファイル)を更新して、最新の状態にしてください。

□ **持ち出した機器等のウイルスチェック**
組織内で利用する前にセキュリティソフトでウイルススキャンを行ってください。

□ **不審なメールに注意**
不審なメールを受信していた場合、「添付ファイルは開かず」、「本文中のURLにはアクセスせず」、各組織のシステム管理者に報告し、指示に従ってください。

被害に遭ってしまったら、最寄りの警察に通報・相談してください！