ノーセキュリティ、ノーテレワーク！

テレワーク用の機器がランサムウエアの標的に！

今年発生したランサムウエアの感染原因の約８割が、VPN機器・リモートデスクトップ等、テレワーク等に利用される機器からの侵入！

ぜい弱性の放置、認証システムの強度不足等、セキュリティ対策の不備を突かれ、サイバー犯罪の被害に！

実施すべき基本対策はこれ！

1　VPN機器やソフトウェアは、最新の状態にアップデート！

2　文字列を長く、複雑なものにする等、パスワードを強化！

3　ワンタイムパスワード等を併用する、多要素認証を採用！

4　セキュリティ対策ソフトを導入！

5　オンライン会議時のURLは秘密に！

これらの対策はセキュリティの基本部分！守れていないと被害に遭う危険性大！

その他の対策については総務省のテレワークセキュリティガイドライン等も参考に！

https://www.soumu.go.jp/main\_sosiki/cybersecurity/telework/

その他サイバー犯罪対策に関する事は、大阪府警ホームページをご確認ください。

企業・組織等に向けたサイバーセキュリティ講演も実施中！