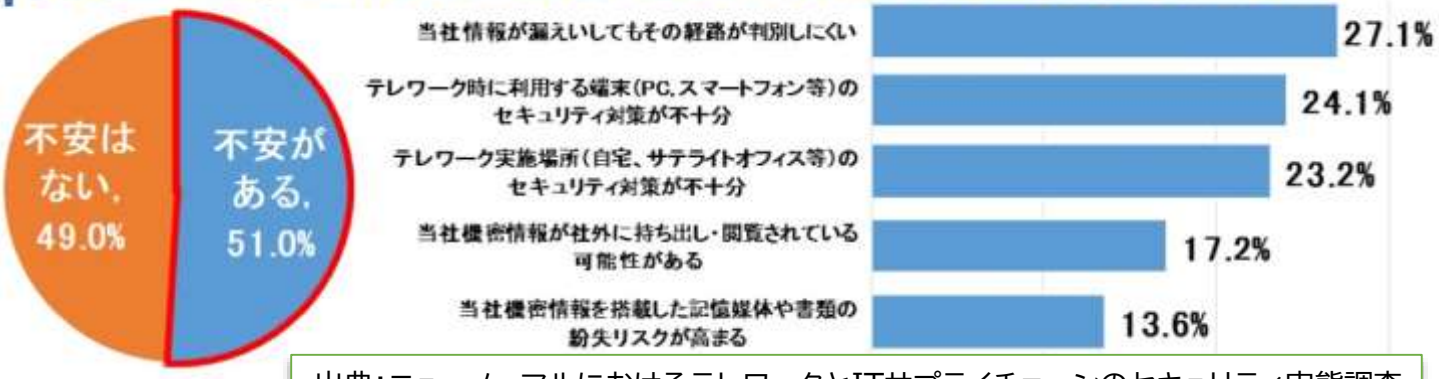
オリパラセキュリティ対策通信

山梨県警察本部
生活安全捜査課
サイバー犯罪対策室

山梨県警察 公式ツイッターアカウント
https://twitter.com/YamanashiPolice

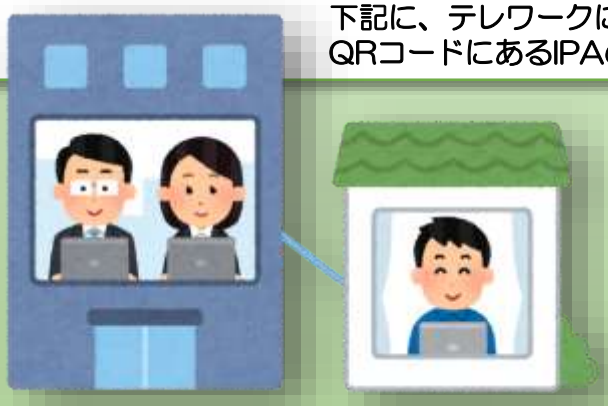
テレワークのセキュリティ、不安はありませんか？

テレワークの導入に伴う取引先のセキュリティ対策に不安を感じている人が5割



出典：ニューノーマルにおけるテレワークとITサプライチェーンのセキュリティ実態調査
https://www.ipa.go.jp/security/fy2020/reports/scrm/index.html

2020年4月に緊急事態宣言がなされてから、テレワークやオンライン会議ツールの活用による働き方が推進され、先行きが見通せない情勢のなか、多くの企業でニューノーマルとして定着しつつあります。
しかし、ほとんどの企業は、緊急事態宣言によって導入せざるを得ない形で始まったICT環境の整備。特にインターネットセキュリティについては、十分に対策ができていないのではないでしょうか。 IPAが行った調査によると、多くの人がセキュリティに不安を抱えていることがわかりました。
下記に、テレワークにおいて留意すべきセキュリティ対策をまとめました。
QRコードにあるIPAの記事をよく読み、インシデントを防ぎましょう！



～日常における情報セキュリティ対策～

- 修正プログラムの適用
- セキュリティソフトの導入と最新化
- パスワードの適切な設定と管理
- 不審なメールに注意
- USBメモリ等の取り扱いの注意
- 社内ネットワークへの機器接続ルールの遵守
- ソフトウェアをインストールする際の注意
- パソコン等の画面ロック機能の設定

～テレワークを始める前に～

- テレワークで使用するパソコン等は、他人と共有しない
- 共有する場合は、ユーザーアカウントを分ける
- ウェブ会議はサービスの設定を確認する

～自宅で行う場合～

- ルーターに最新のファームウェアを適用（ソフトウェアの更新）

～公共の場で行う場合～

- 画面をのぞかれないように注意
- ウェブ会議を行う場合は、話し声が他人に聞こえないように
- 公衆Wi-Fiでは、パソコンのファイル共有機能をオフに
- 公衆Wi-Fiでは、必要に応じて信頼できるVPNサービスを利用
- デジタルデータだけでなく、紙の書類等の管理にも注意

出典：テレワークを行う際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/telework.html