

テレワークの危険性...

新型コロナウイルスの流行に伴い、テレワークを採用する企業が増加していますが、皆さんの自宅のネットワーク環境に問題はありませんか？対策に不備がある環境でのテレワークを行うことで情報漏えいやウィルス感染など様々なリスクが伴います。

公衆無線LANの利用によるリスク



セキュリティ対策に不備のある公衆無線LAN等を利用することで、会社の重要な情報が第三者に盗み見られるなど、情報漏えいのリスクが高まります。

**【対策】公衆無線LAN等に接続できない設定の推奨
会社貸与のモバイルルータ等、信頼のおけるネットワークのみを利用する**

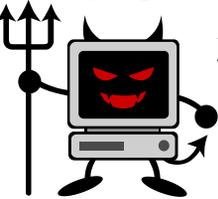
家庭内ネットワークの利用によるリスク

家庭で利用するネットワークにセキュリティ上の不備があると第三者が社内ネットワークに侵入し、踏み台として悪用されてしまいます。



**【対策】ホームルータ等のログインID等を初期設定のままにしない。
第三者に推測されにくいパスワード等を設定する。
更新プログラムが提供される毎に速やかにインストールする。**

私物端末利用におけるリスク



職場が貸与する端末はセキュリティ対策がとられている一方、私物端末のセキュリティ対策は個人の知識やモラルに依存します。私物パソコンのセキュリティ対策があまいと、ウィルス感染や社内システムへの不正アクセス、情報漏えい等のリスクが高くなります。

**【対策】端末には、必ずセキュリティ対策ソフトをインストールする
OSを常に最新の状態に保つ**

万全のセキュリティ対策で大切な情報を守り
安全にテレワークを活用しましょう。

