そのパソコン
会社のネットワークに接続しても
大丈夫？

新型コロナウィルスのまん延により
テレワークは、ニューノーマルな働き方として定着しつつあります。
しかし、会社の環境と比較し、テレワーク環境(自宅等)は、セキュリティ対策が不十分なことが多く、実際にセキュリティ事故も発生しています。

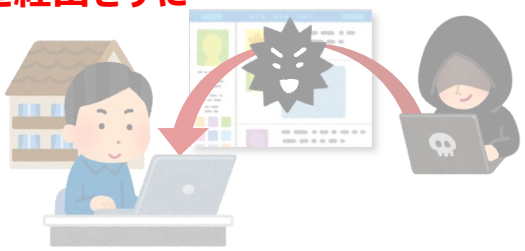
テレワーク環境でセキュリティ事故を起こさないためには、
皆さん一人一人のセキュリティの意識が重要になります。

また、会社のネットワークに接続する前には、
パソコンのOSやアプリケーション、セキュリティソフトが最新の状態であることを確認しましょう。

セキュリティ事故の具体例

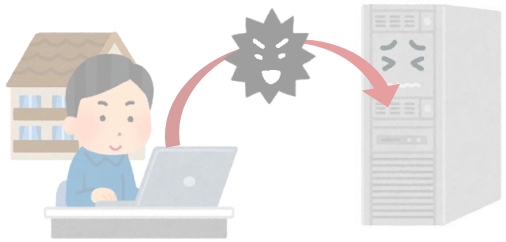
テレワーク時にパソコンがウイルス感染
ウイルス感染したパソコンを社内ネットワークに接続
社内にウイルスが拡散・情報漏洩が発生

- テレワーク時に自宅で**社内ネットワークを経由せずに**
  インターネットへ接続し、SNSを利用。
  その際に、誤ってウイルスを含むファイルを
  ダウンロードしたことにより、
  当該従業員の社用パソコンが感染。



Point 社内のセキュリティルール（業務に関係ないサイトへのアクセスは控える等）を意識して行動しましょう。

- 後日、**ウイルス感染に気付かず**
  社内ネットワークに接続、
  社内ネットワークを通じ感染が拡大。

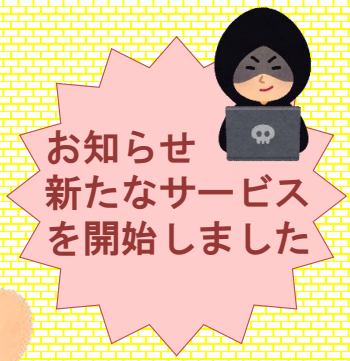


Point 社内のネットワークに接続する前にOS・アプリケーション・セキュリティソフトが最新の状態であることを確認しましょう。

- ウイルス感染により社内ネットワークを利用する
  従業員の氏名およびメールアドレス等の
  情報は漏洩していた。

テレワーク時のパソコンの取り扱いや
セキュリティ対策は、社内のルールを確認し、
ルールに沿った対応をお願いします。
ルールで分からない点があれば、お一人で判断せず
社内の情報システム担当者に相談しましょう。

スマートフォン 偽メッセージに 注意して！



あなたのスマートフォンに、宅配業者や通信事業者を装った偽のメッセージを送る**詐欺事案**があります。

IDやパスワードを盗まれたり、不正なアプリをインストールさせられたりしますのでご注意ください！

偽のメッセージ例

偽メッセージにだまされないための対策

◆ **メッセージをよく確認する**

メッセージをよく見て、不自然な文面はないか、自分宛てのメッセージなのかをしっかり確認しましょう。

◆ **リンクを安易にクリックしない**

メッセージでは実在の企業に似せたURLを表記しているケースもあります。リンクをクリックせず、検索等を行い正規のサイトにアクセスしましょう。

◆ **アプリは信頼できるサイトからダウンロードする**

メッセージから誘導され、アプリのダウンロードを促される場合、不正アプリの可能性もあります。信頼できるサイトなのかしっかり確認しましょう。

被害事例を知り、対策を意識し、
安全・便利にスマホを利用しましょう！