

# 要確認！

## テレワーク時のセキュリティ対策

新型コロナウイルス感染拡大に伴いテレワークが注目されています。

テレワークを実施する場合、オフィスとは異なる環境で仕事を行うため、セキュリティ確保のためのルールが必要となります。

ウイルス感染や機密情報漏洩などのリスクを回避し、安全にテレワークを行うため、使用する端末やアプリケーション利用のルールなど、セキュリティ対策を見直しましょう。



### テレワークに潜むリスクと対策

#### ウイルス感染

パソコンのOSやウイルス対策ソフト、使用するソフトウェアを最新のものに更新し、セキュリティリスクを減らしましょう。

受信したメールやWeb会議の招待についても、不審な点がないかよく確認しましょう。



#### 情報流出

Wi-Fiを利用した通信を盗み見られたり、USBメモリ等の外部記録媒体の紛失による情報流出が考えられます。

Wi-Fiを利用する場合は、ファイル共有機能をOFFにしたり、データの暗号化をしましょう。

USBメモリ等の機器についてもデータを暗号化するなど、機器の適切な管理をしましょう。



#### 不正アクセス

自宅のルータを使う場合は、管理用ID・パスワードを初期設定から変更しましょう。

また、ルータのファームウェアをアップデートして最新の状態にしましょう。

詳細については、下記リンク先についてご確認ください。

総務省 新型コロナウイルス感染症対策としてのテレワークの積極的な活用について

[https://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/telework/02ryutsu02\\_04000341.html](https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/02ryutsu02_04000341.html)

独立行政法人情報処理推進機構（IPA） 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>