



サイバーニュース

令和2年第3号
奈良県警察本部
サイバー犯罪対策課

テレワーク時のセキュリティ対策

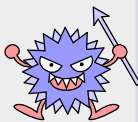
家庭での育児や介護、通勤の問題、働く時間の自由度など多様な働き方が求められる昨今では、多くの企業がテレワークの実施に取り組んでいます。また、新型コロナウイルスの感染拡大防止のため、政府からもテレワークの実施が推奨されています。テレワークを実施する上でセキュリティに気をつける事が重要です。

テレワーク時のセキュリティの7つの落とし穴



✓ ウィルスの入り口対策

インターネットに接続しただけで感染や攻撃の被害に遭うケースの多くが、サーバとの通信に使うポートの設定不備によるものです。**セキュリティソフトを導入**しましょう！



✓ ニセの会議招集メール

急速に普及が進むWeb会議もフィッシングメール、標的型攻撃メールの標的になりつづ有ります。**身に覚えのない会議やネットイベントへの招待は、まず本物かどうか、確認してみた方が良いでしょう。**

✓ パソコンののぞき見による情報漏洩

一瞬ののぞき見でも社名やプロジェクト名などの機密情報が盗まれてしまう可能性があります。**公共の場所でパソコンを使用する場合は、他人から見られないように注意**しましょう！

✓ 公共の場所でのWeb会議

イヤホンマイクを装着してしまうと周りの音が遮断され、思った以上に声が大きくなりがちです。**テレワークによる公共の場でのWeb会議では声による情報漏洩に気をつけましょう！**

✓ 公衆無線LANやクラウドでの共有設定

テレワークにより様々な場所で会社の機密情報を扱うシーンが増えています。設定ミスによる機密ファイルの漏洩などを避けるため、**公共無線LANを使用する際のネットワークプロファイル設定と、クラウドストレージサービスを使用する際の権限設定には特に気をつけましょう！**

✓ ネットワーク機器やパソコンのアップデート

テレワークの実施時はもちろん、**普段からネットワーク機器やパソコンの状態を最新に保つように心掛け、サイバー攻撃を受け付けない状態を保ちましょう。**



✓ ニセの無料無線LAN

公共の場所で提供されている無線LANは、外出先でインターネットに接続する手段として、とても便利で、今では多くの場所で無料の無線LANが提供されています。**無料の無線LANはセキュリティ設定が適切に行われていない場合も多く、ある程度のセキュリティを自分で担保する必要があります。**



これからテレワークを始める方や、最近テレワークを始められた方は、この「テレワーク時のセキュリティ7つの落とし穴」に注意して、テレワークを安全にご活用ください。

【参考】株式会社ラック

「気を付けたい、テレワーク時のセキュリティ7つの落とし穴」

https://www.lac.co.jp/lacwatch/service/20200318_002153.html