# サイバーセキュリティの置き薬

2020年
第12号

# テレワーク、もう一度確認！

既にテレワークを取り入れている企業の方々もいらっしゃるかと思いますが、社内での勤務環境とは異なることから、セキュリティ等に関して注意すべき点は多々あります。自社のテレワークについて、もう一度確認しましょう！

## 勤務する場所は大丈夫？

自宅以外、第三者が混在する場所ではソーシャルエンジニアリングに、注意が必要です。

○ショルダーハッキング(覗き見)
○なりすまし電話・メール
○メモ等の廃棄書類あさり

## データ保存は大丈夫？

クラウド上やUSB媒体にデータを保存する場合は、パスワードを設定するなどしてセキュリティを高め、万が一の情報漏えいや紛失に備えましょう。

ランサムウェア感染に備えバックアップすることも大切です。

## ソフトは大丈夫？

利用するソフトウェアやアプリに信頼性はありますか。無料ソフト等にはウイルスが仕込まれている可能性もあり、注意が必要です。

ビデオ会議ソフトを利用する際は第三者乱入を防止するため、パスワードを設定しましょう。

## ネット環境は大丈夫？

ネットバンキング利用やクレジットカード情報を入力する場合は、信頼性のあるインターネット環境を利用することが大切です。

偽 Wi-Fi やぜい弱なセキュリティWi-Fiでは、通信内容が傍受されるおそれがあります。

その他にも･･･

- パソコンやUSB媒体のセキュリティ対策は大丈夫か
- 持ち出す情報は、社内の規約に沿っているか
- パスワードの使い回しはしない
- 公共の場では長時間の離席を避け、壁側に座る等

**万全のセキュリティ対策で、安全にテレワークを活用しましょう！**