

★ 端末や機器を最新に アップデートしましょう

OSやソフト、アプリ、機器をアップデートしてセキュリティの穴をふさぎましょう。

サポート期限は大丈夫？

【受けられなくなるサポート】



アップデートしておかなければ
受けられなくなるサポートもあるよ

★ 業務を装うメールや 不審なメールに要注意

添付ファイルは安易に開かないように注意しましょう。メールからのリンク先は偽サイトの可能性が。安易にクリックしたり重要情報を入力したりしないようにしましょう。



そのメール
開く前に
まず、確かメル!!

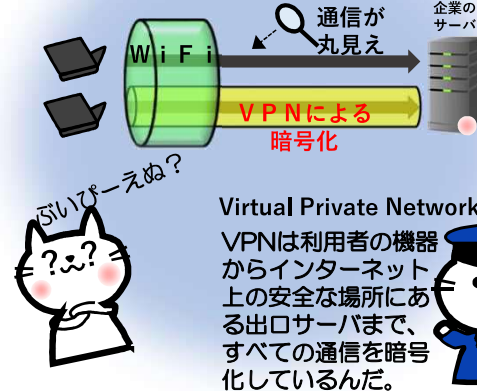


テーマ Telework

オフィスを離れ自宅や公共のスペースなど、場所や通勤等にとらわれず働くことを可能にするテレワーク。
テレワークを実施される方は、注意すべきポイントに気を付けて、仕事上の情報漏えい等や自らの端末・機器等を守る意識を高めましょう。

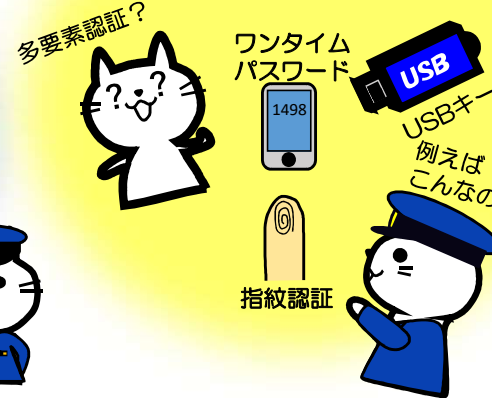
★ 実は丸見え!?通信 は暗号化して安心

公共の場所での通信は、盗聴されるリスクも高まります。VPN接続して通信路を暗号化しましょう。



★ 複雑なパスワードや 多要素認証を使いましょう

お使いになるシステムで用いるパスワードは複雑にし、貴重品のように管理しましょう。



★ 周りは知らない人だらけ

他者からの盗み見（ショルダーハッキング）や大声での電話会議による情報漏えいに注意しましょう。



★ 端末の盗難、紛失 に要注意

持ち運びしやすいノートPCやスマホ、USBメモリ等は盗難、紛失のリスクも。万が一に備えてデータは暗号化しましょう。



テレワーク実施者の方へ インターネットの安全・安心ハンドブック

※このチラシは、内閣府サイバーセキュリティセンター（NISC）ホームページから内容を引用、一部改変して作成しています。NISCのホームページへは右の二次元コードか、<https://www.nisc.go.jp>からアクセスしてください。

他にも、取り組みやすいサイバーセキュリティ対策があります。
詳しくは神奈川県警察のHPで！

