

[illegible]

心当たりのないメールは、
開かない、不用意にURL
をクリックしない等の対策
をお願いします。

などいろいろな被害が想定されます。

檢 索

結論！

全て無視しましょう

そこは社内ではありません！！

そのテレワークセキュリティは大丈夫？



例えば

Webサイトやアプリケーションを介して
コンピュータウィルスに感染し、
情報を盗まれることがあります。



～ 端末や機器、ウィルス対策ソフトは常に最新にアップデート
しましょう。

カフェ等のWi-Fiスポットは、

セキュリティが十分でないものもあり、

通信内容を傍受等されるおそれがあります。



～ Wi-Fiスポット（公衆無線LAN）を利用した通信は、盗聴されるリスクが高まります。
利用時はファイル共有機能をオフにし、通信経路を暗号化（VPN）するとき以外は、
漏洩したとしても支障のない情報だけのやりとりにとどめましょう。

自宅のWi-Fiルータの、管理用IDとパスワード



初期設定のままだとコンピュータ内に侵入されるおそれがあります。

～ そもそも変更した覚えがない・・・そんな方はルータの管理画面
で要確認。「admin」や「password」等のありがちな初期設定に
なっていたら危険です。他人に推測されにくいものに今すぐ変更
しましょう。

その他にも

- 各種パスワードは使い回しはやめましょう。
- 公共の場では覗き見や盗難にも注意しましょう。
- テレワークについての相談を事前に確認しておきましょう。

北海道警察のホームページでは、各種セキュリティ
情報を紹介しております。

北海道警察
サイバーセキュリティ対策本部

サイバーセキュリティひろば

検索