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権限を事前に確認しておきましょう。

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

北海道警察