

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

- 各種パスワードの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危険性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部

サイバーセキュリティひろば

検索

注意！話題に乗じた犯罪手口

ここ最近、連日報道されていたり、インターネット上で大きな話題となっているニュースや事柄に乗じた犯罪が発生しています！

人々の関心や不安な気持ちなどの心理につけ込む非常に悪質な手口です。

確認されている手口のうち、一例をご紹介しますので、このような場面に出くわしても、被害に遭わないようにしましょう！

● 事例紹介 ～コロナウイルスとサイバー犯罪～

コロナウイルスについては、感染拡大が懸念され、連日報道されています。感染防止対策として、マスクが品薄状態ですが、これに乗じて悪質なフィッシングサイト、通信販売サイトの出現が確認されています。



1 フィッシングに関する手口

マスクを無料送付する旨のフィッシングメールから、宅配業者を騙ったフィッシングサイトへ誘導されて不正アプリがダウンロードされる。

偽ショートメッセージ

新型コロナウイルスによる肺炎が広がっている問題で、マスクを無料送付確認をお願いします <http://.com>

2 悪質なショッピングサイトに関する手口

マスク販売の偽サイトが出現！！

代金を支払っても商品が届かなかったり、会員登録時の個人情報やクレジットカード情報等を盗み取られる可能性があります。

ショートメッセージが届いてもアクセスしない！

怪しいショッピングサイトでは買い物しない！

手口を知って、詐欺被害に遭わないようにしましょう！

利用者の皆様へ

Free 無料Wi-Fiの危険性

暗号化されない通信やセキュリティの強度が低い通信は
内容を盗み見られるおそれがあります！

無料で使うことができる、いわゆる「無料Wi-Fiスポット」は、カフェや公共の施設など多くの場所に設置されています。

とても便利ではありますが、通信方法を確認せずに使用すると、個人情報が盗み見られてしまう可能性があります。

●セキュリティの強度が高い暗号化方式を使いましょう。

暗号化方式

なし

WEP

WPA

WPA2

WPA3

低

高

暗号化方式の確認

Androidの場合

Androidの場合は一般的に、SSIDを選択して表示される「セキュリティ」の項目で確認することができる。（「なし」となっている場合は暗号化される通信ではないので注意が必要）

iPhoneの場合

iPhoneの場合、接続時に、暗号化されない通信は「セキュリティ保護されていないネットワーク」、セキュリティが低い通信（WEP）は「安全性の低いセキュリティ」とメッセージが表示される。



暗号化されない通信、又は、セキュリティの強度が低い通信を使用すると、悪意のある第三者から盗み見られるおそれがあります。

見放題♪

通信内容

閲覧状況、投稿状況、個人情報（ID・パスワード、氏名、住所、電話番号、クレジットカード情報）など



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

大切な情報は自分で守りましょう！

北海道警察