

端末を常にクリーンに保とう。

モバイル端末は、常に最新のアップデートを必要とするソフトウェアを搭載したコンピューターです。（ちょうどあなたのノートパソコンやタブレットと同じように）セキュリティ対策機能が組み込まれ定期的に更新されます。ご自宅のすべてのモバイル端末が最新の対策機能を持っていることを、しっかりと時間を割いて確認してください。また、対策機能の更新を行うためにモバイル端末をパソコンへ接続し、同期が必要な場合もあります。更新方法を確認しましょう。

● セキュリティ対策アプリを常に最新の状態に保つ

└ モバイル端末用のセキュリティ対策アプリ、ウェブブラウザ及びOSを最新に保つことが、ウイルスやマルウェア（不正アプリ）などオンライン上の脅威から守る上で最善の策です。

● インターネットに接続する全ての端末を守る

└ コンピューター、スマートフォン、ゲーム機やウェブを閲覧する機能を持つ端末はすべて、ウイルスやマルウェアからの保護が必要です。

個人情報を守ろう。

携帯電話、スマートフォンに入っている個人情報は膨大になることがあります。モバイル端末を紛失したり、盗まれたりした場合、持ち主の個人情報のみならず他の方々の個人情報も収集され、悪用される恐れがあります。携帯電話やモバイル端末もお使いのコンピューターと同様に保護しましょう。

● スマートフォンやタブレットはロックする

└ パスワードの入力や指紋認証などの方法でロックを解除しなければ、他の誰かが勝手につかうことはできません。スマートフォンやタブレットには必ずロックが必要です。

● アプリをダウンロードする前にじっくり考えてみる

└ アプリをダウンロードする前に、まずはプライバシーポリシーをよく読んでみましょう。端末内のどのデータ（位置情報、ご自分のソーシャルネットワークアカウントなど）にアプリがアクセスするのか理解することが必要です。

● 住所や電話番号など個人の情報を聞かれても教えない

└ ネット利用社の中には個人情報を聞き出して悪用したり、相手を誘い出す目的で住所や電話番号、名前を聞き出そうとする人がいます。こうした情報を絶対に教えてはいけません。また許可なくして知人の電話番号を第三者に伝えるべきではありません。ネットの振る舞いだけを見て、だまされないようにすることが必要です。

● 位置情報タグ機能を利用する前にじっくりと考える

└ スマートフォンのカメラ機能や、デジタルカメラの中にはGPSの位置情報を記録できるものがあります。位置情報を記録することで、後からどこで撮影した写真か調べることが可能です。便利な機能ですが、利用には注意が必要です。位置情報付きの写真をうっかり投稿することに不安を感じる方は、あらかじめ位置情報タグの有効/無効を切り替える方法を確認しておくことが必要です。

インターネットへの接続にはご用心。

インターネットへ接続する際も、日常の振る舞いと同様の注意が必要です。安全ではない、または保護管理されていないネットワークから接続する場合、閲覧するウェブサイトやそこで入力する情報に気をつけましょう。

● 公衆無線LAN（Wi-Fi ホットスポット）について正しい知識を身につける

└ 公衆無線LANや暗号化されていないネットワークに接続する場合は、ログイン情報（ID、パスワード）など、個人情報をやりとりするサイトやアプリを利用するのを避けることが必要です。

● 自動接続を無効にする

└ ネットワークに自動的に接続する設定にしておくとはッカーの攻撃に対してぜい弱（弱点）になる可能性があります。使用していない場合はWi-FiやBluetoothの接続を無効にしておくことが必要です。

● お金の移動や個人情報の提供は慎重にする

└ オンラインバンキングやネットショッピングをする際、そのウェブサイトへ暗号化された接続ができるかどうかチェックしましょう。そのサイトのアドレスバーの表記が「https://」で始まっているか確認しましょう。「http://」で始まるURLは暗号化された接続ができないことを知っておくことが必要です。

● 怪しいと思ったら返事をしない

└ サイトに表示される広告、モバイル端末に届くメッセージ、電話を悪用した詐欺行為が激増しています。個人情報を尋ねてきたり、せかすような行動を促すものは詐欺であると疑って接することが必要です。

賢いネット利用者になろう。

ご自身のモバイル端末の最新情報を常に把握するようにしましょう。何かおかしいなと異常に気づいた際にどうすればよいのか理解しておきましょう。

● 安全にインターネットを楽しむための最新情報についてアンテナをはる

└ 信頼のおけるウェブサイトを見て最新情報をチェックするとともに、ご友人、ご家族、同僚の方々と共有し、みんなで賢いネット利用者になりましょう。

● 着信拒否の方法を知る

└ 発信電話番号を使えば、着信全てをブロックすることも、個別の名前や番号のブロックをすることも可能です。

● ネットでしか「知らない」相手に直接会うときは用心する

└ オンラインチャットやSMSでたくさんのやり取りを重ねても、相手が信用できる人物とは限りません。素性のはっきりしない相手と会う約束をしたり、直接会うのはできるだけ避けましょう。



よきオンライン利用者となりましょう。

● 他人へのメッセージは、あなたが受け取りたいと思う内容にする

└ 電話やメール、ソーシャルメディアなどでは、直接会ってでは絶対に言わないようなことでも言いやすいものです。オンラインでも現実世界と同じように相手への敬意をもって接しましょう。

● 許可なくして知人の電話番号を第三者に伝えない

└ 信頼している知人にのみ携帯電話番号を教えましょう。そして知人の番号は同意なしに他人に教えないようにしましょう。

● 携帯電話で他人の写真やビデオを撮影する際には、許可をとるようにする

└ 同様に、ご自分の写真や動画を撮影される前に許可をとってもらう必要があることを他の方々にも伝えましょう。

● 自分にとって安全 = みんなにとって安全

└ オンライン上のご自身の行動によって、ご家族、同僚の方々、世界中の人々を含め、他の方々すべてに影響を及ぼす可能性があります。良いオンライン習慣を実践することは、世界中のデジタル社会に恩恵をもたらすことになるのです。

STOP. 立ち止まる

ボタンやリンクをクリックする前に、安全なものなのか一旦立ち止まって確認しましょう。どのような画面表示にリスクがあるのか知っておきましょう。

THINK. 考える

これから何が起きるのかじっくり考えましょう。警告が出ていないかどうか気を配り、自分の行動によって、ご自分やご家族の安全にどのような影響が出そうなのか考えるようにしましょう。

CONNECT. 楽しむ

自分とコンピューターを守るための適切なステップをとっていることを理解した上で、自信をもってネットを楽しみましょう。

<http://www.stopthinkconnect.org>にさらに詳しい情報があります。