# データとインターネット 接続されたデバイスを 保護するための 12 のヒント

メール、アカウント、デバイス (組織のネットワー クに接続されているものを含む) をサイバー攻撃か らより安全に保護するための12のヒントをご紹介 します。



## リンク付きのメッセージ、特 に個人情報を求めるものには 注意が必要

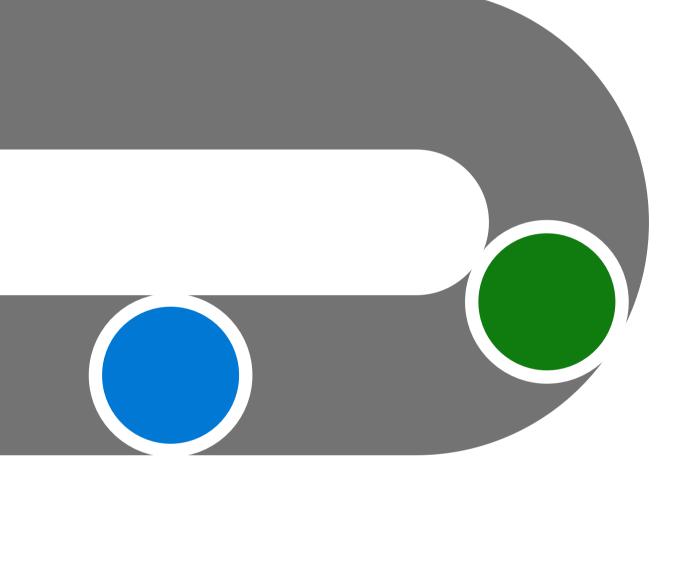
偽のリンクや Web サイトはとても巧妙に作られて いる場合があります。リンクを信頼することな く、差出人の公式 Web サイトで電話番号を探し、 直接電話をかけてメッセージが本物であるかを確 認するようにしましょう。

## 個人情報の共有は リアルタイムでのみ行う

個人情報の共有は、対面または電話で行うのがべ ストです。どうしても個人情報をメールで送らな ければならない場合は、Microsoft Outlook の暗号 化ツールを使用してください。

## パスワードを使用する必要が ある場合は、パスワードマ ネージャーを使用して強力で ユニークなパスワードにする

強力なパスワードには、14以上のランダムな文字 と記号を使用します。Microsoft Edge を使用する と、パスワードの記憶や変更管理を行うことがで きます。



## ソフトウェアの更新プログラ ムをすぐにインストールする

アプリ、ブラウザー、オペレーティング システム

の更新プログラムの多くには、現在進行中の問題 に対するセキュリティ修正プログラムが含まれて いるため、速やかにインストールして最新のセ キュリティ基準を維持してください。

### ん保護をオンにしてセキュリ ティ設定を保護する 常に最新バージョンの Windows を使用しましょ う。改ざん保護機能は、セキュリティ設定に対す

Windows 11 を使用し、改ざ

る不正な変更をブロックしてくれます。

## ファームウェアの スキャン ツールを使用する 作業環境に潜在的な弱点がないかを確認す

することができます。

ることにより、対策を講じてリスクを軽減

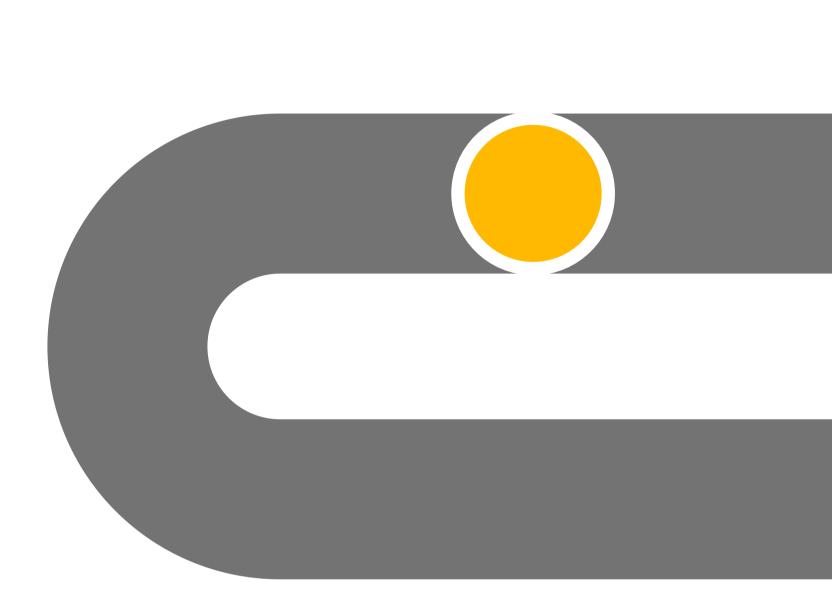


## 添付ファイル付きの メッセージに気を付ける

信頼できる人や組織からのものだと思っても、想 定外の添付ファイルは決して開かないでくださ い。重要なメッセージかもしれないと心配な場合 は、差出人に電話して確認しましょう。

## パスワードレスに移行し、 認証アプリを使用して セキュリティを強化する

パスワードがなければ、パスワードを盗まれる ことはありません。Microsoft アカウントの <u>パスワードレス</u>をオンにして、電話または Windows Hello でサインインしましょう。



## すべてのモバイル デバイス でロック機能を有効にする

デバイスのロック解除には、PIN、指紋、または 顔認証を必須としましょう。

## アプリが正当なもので あることを確認する

デバイス上のすべての

のみ、アプリをインストールしてください。

デバイスに対応した公式のアプリストアから

## 削減する 不要なインターネット接続を消去し、開いている

攻撃対象となる領域を

ポートを制限して、スキャン ツールでデジタル環 境の潜在的な弱点を確認することにより、対策を 講じてリスクを軽減することができます。



# 12

## システム定義を含む ファイルを転送しないこと セキュリティ保護されていない経路や、関係者以

外の人物にシステム定義を送ることは、デジタル 環境への攻撃を可能にし、プロセスの破壊や環境 の脆弱性を招くおそれがあります。

下記のページをご覧ください https://aka.ms/cybersecurity-awareness



参照目的に限り、ドキュメントを複製して使用することができます。