長期休暇における情報セキュリティ対策
～家庭の利用者向け～

長期休暇期間は、インターネットに触れる機会が多くなり、ウイルス感染や不正アクセス等の被害に遭ったり、SNSへの書き込み内容から思わぬ被害にあう恐れがあります。
被害にあわないために、以下の対策を実施してください。

確認してみよう！安全利用のチェックポイント

外出中のSNS投稿に注意

○　SNSで旅行の計画を書き込んだ場合、内容によっては長期休暇中に不在であることが知られてしまう可能性があります。

⚠　撮影した写真をSNSに投稿したことでトラブルに発展することもあるため、**投稿内容**や**投稿範囲**に注意してください。

SNSのやりとりによるトラブルに注意

○　SNSで知り合った人物から言葉巧みに**不正なアプリのインストール**を持ち掛けられ、そのアプリでプライベートな画像を撮影したことが原因で**セクストーション（性的脅迫）**の被害に遭うケースが発生しています。

⚠　**第三者に見られたら困るプライベートな写真**や**動画を撮影**させたり、**データを送信**したりしてはいけません。

偽のセキュリティ警告に注意

○　ウェブサイトの閲覧中に、**「ウイルスに感染している」「パソコンが壊れる」**等の偽の警告に遭遇する場合があります。

○　表示された通り操作したり、電話をかけて遠隔操作を許してしまうと、最終的に有償ソフトウェアの購入や有償サポート契約などに誘導されます。

⚠　偽の警告画面が表示された場合は、**無視**して、**画面を閉じてください。**

⚠　画面が消せない場合は**ブラウザを強制終了**するか、**パソコンを再起動**してください。

不審なファイルやURLに注意

○　メールやショートメッセージ（SMS）、SNSに届く、実在の企業を騙った不審な偽メールによる被害が多発しています。

○　メールの添付ファイルを開いたり、本文中のURLにアクセスするとウイルスに感染したり、フィッシングサイトに誘導されてしまう可能性があります。

⚠　ウイルスに感染した疑いがある場合は、**パソコンの初期化**を検討してください。

⚠　フィッシングサイトで情報を入力してしまった場合は、**パスワードの変更**、**カード会社への連絡等**、入力した情報の悪用を防ぐ対策をしてください。

出典：IPA 独立行政法人 情報処理推進機構

埼玉県警察本部サイバー対策課