

GPT監査テーマ： 年末年始の家庭/職場でのサイバーリスク対策を例示させる

【**プロンプト**（生成AIへの入力内容： Written by Tomonori Tomura）】
「あなたはプロのサイバーリスク対策の指導者です。年末年始に気を付けておきたい家庭や職場のサイバーリスク対策について、特に重要な対策を3つ挙げて、それぞれについて200文字程度の解説をつけて教えて下さい。」

【**アウトプット**（生成AIの出力内容 **Written by ChatGPT-o1 (所要43秒)**）】

1. 端末やアカウントのセキュリティ強化

年末年始は家族や友人と端末を共有する機会が増え、パスワードの使い回しによる不正アクセスのリスクが高まります。各アカウントで異なる複雑なパスワードを設定し、二段階認証を積極的に導入しましょう。また、OSやアプリの更新を怠らず、常に最新状態を維持することで、脆弱性を早期にカバーできます。加えて、万一の流出に備えて、定期的に重要アカウントのパスワードを見直すこともお勧めです。

2. フィッシング詐欺への警戒

年末年始には、贈り物や挨拶メールを装ったフィッシング詐欺が増加しがちです。不審なメールやSNSのメッセージに添付されたリンクは不用意にクリックしないよう注意が必要です。差出人や件名に違和感を覚えた場合は、URLを直接入力する、公式アプリから確認するなど安全策を徹底しましょう。また、添付ファイルの開封や個人情報の入力、必ず正規サイトであることを確認してから行うのが大切です。

3. 安全な通信環境の確保（自宅・外出先ともに）

年末年始は外出先でフリーWi-Fiを利用する機会も増えますが、暗号化の甘いネットワークを経由すると通信内容が盗聴されるリスクが高まります。VPNなどのセキュアな接続手段を導入し、機密情報のやり取りは避けるようにしましょう。自宅やオフィスのWi-Fiルーターも、初期設定のまま使わず、SSIDやパスワードを変更して強力な暗号化方式（WPA2/WPA3）を設定することが肝心です。（※赤字ハイライトとアンダーラインはGPT監査人にて付したもの）

【**所長のGPT監査ノート**（Written by Tomonori Tomura）】

「サイバーリスク対策はそれぞれのIT環境や状況等により、ツッコミを入れ出すとキリがないくらい、様々な留意点や対策があるが、おおよそ、簡単な読み物や家庭・職場での一般的な注意喚起としては、ある程度は使える内容・例示・説明が出力されているように見受けられる。定期的にパスワードを見直すべきかどうかよりも、より強固なパスワード・パスフレーズ・パスコード等を、パスワード管理アプリ等で設定・管理する方が良いように思われるが、テレワーク・在宅ワーク等で見落としがちな自宅のルータについても触れている点は評価したい。3つ例示・各説明の文字数等の制限にて少し時間がかかったようであった。」

