年末年始 情報セキュリティ確認チェックリスト

1. 休暇【前】の最終チェック

長期休暇に入る前に、隙のない状態を作っておきましょう。

- ☐ OS・ソフトの更新: Windows/macOS やブラウザ、ウイルス対策ソフトを最新版にアップデートしたか。
- ☐ 不要な機器の電源 OFF: 使用しない PC、モニター、周辺機器の電源を切り、コンセントを抜いたか（ネットワーク経由の攻撃遮断と節電）。
- ☐ データのバックアップ: 重要なデータは社内の指定サーバーやクラウドストレージへ保存したか。
- ☐ デスク周りの整理: 機密書類を出しっぱなしにしていないか。キャビネットの施錠は確実か。
- ☐ 緊急連絡先の確認: 休暇中にトラブルが発生した際の連絡ルート（上司・情シス担当など）をメモしたか。

2. 休暇【中】の注意点

プライベートでの利用時も、攻撃者は隙を狙っています。

- ☐ 持ち出しデバイスの管理: 社用 PC やスマホを紛失・盗難されないよう、車内放置や飲食店での置き忘れに細心の注意を払う。
- ☐ 不審なメール・SMS への警戒: 「配送業者」や「お年玉キャンペーン」を装った偽メールに注意。URL を安易にクリックしない。
- ☐ 公衆 Wi-Fi の利用制限: 外出先で安全性が確認できないフリーWi-Fi を使って、社内システムやメールにアクセスしない。

3. 休暇【明け】の始業前チェック

休み明けに通常業務を始める前に必ず実施してください。

- ☐ ウイルス定義ファイルの更新: 業務開始前にウイルス対策ソフトを最新の状態に更新する。
- ☐ フルスキャンの実施: 休暇中に社外に持ち出した PC は、ネットワークに接続する前にウイルススキャンを実行する。
- ☐ 不審なログイン・メールの確認: 休暇中に自分のアカウントへ不正なアクセスがなかったか、身に覚えのない重要メールが届いていないかを確認する。