今すぐ自分で確認できる！
「セキュリティ対策チェックシート」

デバイス（PC・サーバ、スマホなど）

- ☐ OSを最新の状態にしている
- ☐ ブラウザを最新の状態にしている
- ☐ ソフトウェアを最新の状態にしている
- ☐ サポート切れの古いOSや古いブラウザを使用していない
- ☐ ウィルス対策ソフトのウィルス定義ファイル（パターンファイル）を常に最新の状態にしている
- ☐ パスワードロック設定をしている
- ☐ 破られにくい、長く、複雑なパスワードを使用している
- ☐ USBメモリなどの記憶媒体を使用する場合はウィルスチェックをしている
- ☐ ファイルサーバーの適切なアクセス権限設定をしている
- ☐ パソコンやサーバの重要なデータのバックアップを取得している
- ☐ スマホの紛失時に遠隔ロックまたは遠隔削除できるようにしている
- ☐ 提供元不明のアプリをインストールしていない

REMINDER/NOTE

-
-
-

今すぐ自分で確認できる！
「セキュリティ対策チェックシート」

ネットワーク

- ☐ 無線LANの暗号化方式としてWEPを使用していない
- ☐ 無線LANルータやVPN機器などのファームウェアなどを最新の状態にしている
- ☐ 無線LANルータやVPN機器などのID・パスワードを初期設定のまま使用していない
- ☐ ネットワーク接続の機器（複合機、カメラ、ハードディスク（NAS）など）のファームウェアなどを最新の状態にしている
- ☐ ネットワーク接続の機器の適切なアクセス権限の設定をしている
- ☐ 推奨：インターネットとの接続に対してUTM設置などの適切な対策をしている

REMINDER/NOTE

-
-
-

今すぐ自分で確認できる！「セキュリティ対策チェックシート」

電子メール

- ☐ メール送信時に宛先に間違いがないか再確認している
- ☐ メールを複数の宛先に送る場合は、TO/CC/BCCの使い分けをしている
- ☐ メール本文に重要な情報を記載せず、パスワード付きファイルなどで保護している
- ☐ 不審な電子メールに添付されたファイルを安易に開いたり、電子メールの本文に記載されたURLを安易にクリックしたりしていない

クラウドサービス

- ☐ 利用規約などから性能や補償内容を確認して選定している
- ☐ 利用者ごとにアカウントを付与して認証している
- ☐ 機能や共有範囲の適切なアクセス権限の設定をしている
- ☐ 破られにくい、長く、複雑なパスワードを使用している
- ☐ ID・パスワードを使い回していない
- ☐ 推奨：二段階認証を利用している

REMINDER/NOTE

-
-
-

今すぐ自分で確認できる！「セキュリティ対策チェックシート」

テレワーク

- ☐ 持ち出し用の端末のハードディスク（メモリ）は暗号化している
- ☐ 持ち出し用の端末に覗き見防止フィルタを使用している
- ☐ USBメモリなどを持ち出し用の端末で使用できないようにしている
- ☐ 端末での利用履歴を残すためのログを取得している
- ☐ 社内ネットワークにアクセスする際は、VPN方式のようなセキュリティ対策が施された方式を利用している
- ☐ 個人所有の端末や機器を利用する場合は、次のようなセキュリティ対策を実施している
  - ☐ 使用する端末のOSなどの確認及び最新化
  - ☐ 標準ウィルス対策ソフトの導入
  - ☐ 端末内へのデータ保存の制限
  - ☐ WiFiルータなどの通信機器のセキュリティ対策

REMINDER/NOTE

-
-
-

今すぐ自分で確認できる！
「セキュリティ対策チェックシート」

その他

- ☐ インターネット利用やSNS利用に関するルールがある
- ☐ 最新の脅威や攻撃の手口を知り、対策を社内共有する仕組みがある
- ☐ 重要情報の紙媒体は、シュレッダーや溶解などの処理をしている
- ☐ 重要情報は保管場所を決めて、作業に必要な場合のみ持ち出し、作業後は施錠可能な書庫や引き出しなどに保管している
- ☐ PCやサーバを廃棄する時は、データを完全に消去する、または機器を物理的に破壊している
- ☐ PCやサーバの廃棄を業者に依頼する場合は、廃棄証明を取得している
- ☐ 従業員にセキュリティに関する教育を行っている
- ☐ セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成している
- ☐ 情報セキュリティ対策を具体的な手順やルールとして明文化している

REMINDER/NOTE

-
-
-