情報セキュリティ対策 チェックシート

対策１：ソフトウェアとシステムの更新

1. OS（Windows、macOS、Linux 等）は、最新のアップデートが適用されていますか？
   □ はい　□ いいえ

2. ブラウザ（Chrome、Firefox、MS Edge 等）は、最新バージョンに更新されていますか？
   □ はい　□ いいえ

3. コミュニケーションツール（Teams、Slack、Zoom 等）は、最新バージョンに保たれていますか？
   □ はい　□ いいえ

4. メール管理アプリケーション（Outlook、Thunderbird 等）は、最新バージョンに更新されていますか？
   □ はい　□ いいえ

5. Microsoft Office（Word, Excel 等）や Adobe 系ソフトは、最新版にアップデートされていますか？
   □ はい　□ いいえ

6. その他更新が必要なソフトウェアをリスト化し、定期的に確認していますか？
   □ はい　□ いいえ

7. 重要なセキュリティパッチは、速やかに適用されていますか？
   □ はい　□ いいえ

8. サポートが終了したソフトウェア（旧バージョン）の使用は、避けていますか？
   □ はい　□ いいえ

9. ソフトウェアとシステムの更新状況を定期的に監視・確認していますか？
   □ はい　□ いいえ

10. システムの更新管理ポリシーは文書化され、全従業員に周知されていますか？
    □ はい　□ いいえ

対策２：アンチウイルスソフトの導入

1. 全デバイス（PC、サーバー、モバイル等）に、アンチウイルスソフトがインストールされていますか？
   □ はい　□ いいえ

2. 全てのデバイスにアンチマルウェアソフトがインストールされていますか？
   □ はい　□ いいえ

3. アンチウイルスおよびアンチマルウェアソフトは、最新のバージョンに更新されていますか？
   □ はい　□ いいえ

4. ウイルス定義ファイル（シグネチャ）は、自動的に更新されていますか？
   □ はい　□ いいえ

5. 定期的なスキャン（例：毎日、毎週）がスケジュールされ、実行されていますか？
   □ はい　□ いいえ

6. リアルタイム保護機能が有効になっていますか？
   □ はい　□ いいえ

7. アンチウイルスおよびアンチマルウェアソフトのログが記録され、定期的にレビューされていますか？
   □ はい　□ いいえ

8. 検出された脅威に対する対応手順が文書化され、従業員に周知されていますか？
   □ はい　□ いいえ

9. 従業員は怪しいファイルやリンクを開かないように教育されていますか？
   □ はい　□ いいえ

10. アンチウイルスおよびアンチマルウェアソフトウェアの設定やポリシーが文書化され、従業員に周知されていますか？
    □ はい　□ いいえ

対策３：パスワードの管理と強化

1. パスワードの長さは最低８文字以上になっていますか？
   □ はい　□ いいえ

2. パスワードには英大文字、英小文字、数字、特殊文字（例：@、#、$、%）が含まれていますか？
   □ はい　□ いいえ

3. パスワードは個人情報（名前、誕生日、住所など）を避けていますか？
   □ はい　□ いいえ

4. パスワードは辞書に載っている単語や一般的なフレーズ（例：password、123456、abcdef）を避けていますか？
   □ はい　□ いいえ

5. パスワードは定期的に（例：３ヶ月に１回）変更されていますか？
   □ はい　□ いいえ

6. 以前使用したパスワードの再利用は、避けていますか？
   □ はい　□ いいえ

7. 同じパスワードを複数のシステムやアカウントで使い回すことを、避けていますか？
   □ はい　□ いいえ

8. パスワード管理ツールを使用して、複雑でユニークなパスワードを生成・管理していますか？
   □ はい　□ いいえ

9. 多要素認証（MFA）を設定し、パスワードの他に追加の認証方法を導入していますか？
   □ はい　□ いいえ

10. パスワードは社内のセキュリティポリシーに従って保護されていますか？
    □ はい　□ いいえ

対策４：ネットワークのセキュリティ強化

1. ネットワークにはファイアウォールが設置され、適切に設定されていますか？
   □ はい　□ いいえ

2. ネットワークは複数のセグメントに分割され、アクセス制御が行われていますか？
   □ はい　□ いいえ

3. 仮想プライベートネットワーク（VPN）が、リモートアクセスに使用されていますか？
   □ はい　□ いいえ

4. ネットワークトラフィックは定期的に監視され、不正な活動が検出された場合にアラートが発生するよう設定されていますか？
   □ はい　□ いいえ

5. 無線 LAN には強力な暗号化（例：WPA3）が使用されていますか？
   □ はい　□ いいえ

6. ネットワーク機器（ルーター、スイッチ、アクセスポイントなど）のファームウェアは定期的に更新されていますか？
   □ はい　□ いいえ

7. ネットワーク上の重要なデータは暗号化されていますか？
   □ はい　□ いいえ

8. ネットワークへの物理的なアクセスは制限され、監視されていますか？
   □ はい　□ いいえ

9. 外部からのアクセスには厳格な認証手段（例：多要素認証）が導入されていますか？
   □ はい　□ いいえ

10. ネットワークセキュリティポリシーが策定され、全従業員に周知されていますか？
    □ はい　□ いいえ

対策５：データのバックアップと復元計画

1. 重要なデータは定期的にバックアップされていますか？
   □ はい　□ いいえ

2. バックアップのスケジュールが設定され、確実に実行されていますか？（例：毎日、毎週、毎月）
   □ はい　□ いいえ

3. バックアップデータはオフサイトやクラウドストレージに保存されていますか？
   □ はい　□ いいえ

4. バックアップの内容は暗号化されていますか？
   □ はい　□ いいえ

5. バックアップデータの復元手順が文書化され、定期的にテストされていますか？
   □ はい　□ いいえ

6. バックアップの結果は定期的に監視・確認されていますか？
   □ はい　□ いいえ

7. バックアップ対象のデータは全ての重要なシステムやファイルを網羅していますか？
   □ はい　□ いいえ

8. バックアップの設定やポリシーが文書化され、従業員に周知されていますか？
   □ はい　□ いいえ

9. バックアップストレージの容量や利用状況が定期的に確認されていますか？
   □ はい　□ いいえ

10. バックアップデータの保管期間が設定され、古いデータの適切な管理が行われていますか？
    □ はい　□ いいえ

対策６：物理的なセキュリティ対策

1. 従業員や訪問者には識別バッジが発行され、常に表示するように義務付けていますか？
   □ はい　□ いいえ

2. オフィスや施設への入退室管理システムが導入され、記録が保存されていますか？
   □ はい　□ いいえ

3. デバイスや PC の持ち出しが必要な場合、事前に上司の承認が必要とされていますか？
   □ はい　□ いいえ

4. 持ち出しデバイスや PC のログインには、多要素認証（MFA）が導入されていますか？
   □ はい　□ いいえ

5. 社外で使用されるデバイスや PC には、リモートワイプ機能が有効になっていますか？
   □ はい　□ いいえ

6. 持ち出しデバイスや PC の使用に関する定期的な監査が実施されていますか？
   □ はい　□ いいえ

7. デバイスや PC の持ち出しに関する明確なポリシーが策定され、全従業員に周知されていますか？
   □ はい　□ いいえ

8. USB メモリや外付けハードドライブなどの物理メディアの使用に関して、厳格な制限が設けられていますか？
   □ はい　□ いいえ

9. 紙の書類や物理メディア（USB メモリ、外付けハードドライブ等）は適切に保管され、不要になった際には安全に廃棄されていますか？
   □ はい　□ いいえ

10. 従業員が退職する際に、すべての持ち出しデバイスや PC が回収され、データが消去されていますか？
    □ はい　□ いいえ

対策７：従業員教育と意識向上

1. 従業員全員に対して、定期的な情報セキュリティトレーニングが実施されていますか？
   □ はい　□ いいえ

2. 新入社員向けに、情報セキュリティの初期トレーニングが行われていますか？
   □ はい　□ いいえ

3. フィッシング詐欺やソーシャルエンジニアリング対策に関する、教育が行われていますか？
   □ はい　□ いいえ

4. セキュリティポリシーや手順に関する文書が、従業員に提供されていますか？
   □ はい　□ いいえ

5. 従業員がセキュリティインシデントを報告する時、明確な手順が確立されていますか？
   □ はい　□ いいえ

6. セキュリティ意識の向上キャンペーン（例：セミナー、ワークショップ、啓発ポスター等）が、定期的に実施されていますか？
   □ はい　□ いいえ

7. 従業員が情報セキュリティに関する最新の脅威やトレンドについて、情報を得られる仕組みが整っていますか？
   □ はい　□ いいえ

8. 従業員のセキュリティ知識や意識の向上を測定するため、テストやアンケートが実施されていますか？
   □ はい　□ いいえ

9. 特定の役職や業務に応じたセキュリティトレーニング（例：管理職向け、高度な技術職向け）が、提供されていますか？
   □ はい　□ いいえ

10. 従業員のセキュリティ意識向上の取り組みが、経営層に報告され共有されていますか？
    □ はい　□ いいえ

以上