【付録】A.セキュリティ対策チェックリスト

以下の診断事項を確認し、自組織のセキュリティ対策状況を確認しましょう。対策が不十分な項目は、対策例を参考に対策を検討しましょう。

診断項目	No	診断事項	チェック	対策例
Part1 基本的対策	1	パソコンやスマホなどの情報機器のOSやソフトウェアは常に最新の状態にしていますか？		Windows Updateを実施する(WindowsOSの場合）、Adobe製品などの利用中のソフトウェアを最新版にするなど。
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？		ウイルス定義ファイルが自動更新されるように設定する、統合型のセキュリティ対策ソフトの導入を検討するなど。
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？		パスワードは英数字記号含めて10文字以上にする、名前、電話番号、誕生日、簡単な英単語などパスワードに使わない。同じID・パスワードをいろいろなWebサービスで使いまわさないなど。
	4	重要情報に対する適切なアクセス制限を行っていますか？		Webサービスの共有範囲を限定する、ネットワーク接続の複合機やカメラ、ハードディスク（NAS）などの共有範囲を限定する、従業員の異動や退職時に設定の変更（削除）漏れがないように注意するなど。
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？		IPAなどのセキュリティ専門機関のWebサイトやメールマガジンで最新の脅威や攻撃の手口を知る、利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認するなど。
Part2 従業員としての対策	6	電子メールの添付ファイルや本部中のURLリンクを介したウイルス感染に気をつけていますか？		不審な電子メールの添付ファイルを安易に開かない、URLリンクに安易にアクセスしない、不審な電子メールの情報を社内に共有するなど。
	7	電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？		電子メールやFAXを送る前に送信先を再確認する、電子メールはTO・CC・BCCを使い分けて指定するなど。
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？		重要情報は文書ファイルに書いてパスワードで保護する、パスワードはあらかじめ決めておくか、携帯電話のショートメッセージサービス（SNS）などの別手段で知らせるなど。
	9	無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？		強固な暗号化方式（WPA2-PSK）を選択する、パスフレーズ（暗号化キー）は長くて推測されにくいものを使用するなど。
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？		インターネットの利用ルールを作る、SNSの利用ルールを作る、Webフィルタリング機能を導入することでシステム的にインターネットの利用を制限するなど。
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消去に備えてバックアップを取得していますか？		重要情報のバックアップを定期的に行う、バックアップは別の場所に保存するなど。
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？		机の上をきれいにする、重要書類は鍵付き書庫に保管するなど。
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？		重要情報の持ち出しは許可制にする、ノートパソコン・スマートフォン・USBメモリなどはパスワードロックをかける、荷物を放置しないなど。
	14	離籍時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？		離籍時にパソコンをロックする、退社時にパソコンをシャットダウンし、他人がパソコンを使うことを防ぐなど。
	15	関係者以外の事務所への立ち入りを制限していますか？		事務所で見知らぬ人は事務所にいれない、受付を設置するなど。
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？		退社時に机上のノートパソコンやタブレット端末、備品（CD、USBメモリ、外付けハードディスクなど）を引き出しにしまうなど。
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？		鍵の管理を徹底する、最終退社時は事務所を施錠し退出の記録（日時、退出者）を残すなど。
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？		書類は裁断する、電子データは消去ソフトを利用する、物理的に壊してから処分する、専門業者に消去を依頼するなど。
Part3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？		採用の際に守秘義務について説明する、守秘に関する覚書を交わす、秘密としている情報を具体的に示すなど。
	20	従業員にセキュリティに関する教育や注意喚起を行っていますか？		情報管理の大切さや関連する法令などを説明する、定期的な研修の機会を設けるなど。
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？		個人所有パソコン、スマートフォンの業務利用を許可制にする、業務利用する場合のルールを決めるなど。
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？		秘密保持や具体的な対策を明記した契約や覚書を交わす、情報セキュリティ対策方針を公表している取引先を選定する、取引先の情報セキュリティ対策を確認するなど。
	23	クラウドサービスやWebサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？		利用規定や補償内容、セキュリティ対策などを確認して事業者を選ぶなど。
	24	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するなど準備をしていますか？		重要情報の流出や紛失、盗難があった場合の対応手順書を作成し、従業員に周知するなど。
	25	情報セキュリティ対策（上記1~24など）をルール化し、従業員に明示していますか？		情報セキュリティ対策として、診断シート項目のNo.1から24までをルール化して社内で共有する、一度決めたルールでも問題があれば改善するなど。

【出典】IPA：「中小企業の情報セキュリティ対策ガイドライン」https://www.ipa.go.jp/security/keihatsu/sme/guideline/
「情報セキュリティ対策支援サイト」でオンラインでの診断も可能です。https://security-shien.ipa.go.jp/learning/