「情報セキュリティ対策チェックシート(中小事業者向け)」出典：IPA を一部、編集

文責：河東岩夫、作成日：平成 29 年 08 月 04 日

No.	チェック項目	対応済	未対応
1	組織的セキュリティ対策を以下のとおり実施していますか？		
	○経営者の主導で情報セキュリティの方針を示している。 ○情報セキュリティの方針に基づき、具体的な対策の内容を明確にしている。 ○情報セキュリティ対策を実施する体制を整備している。 ○情報セキュリティ対策のリソース(人材、費用)の割当を行っている。		
2	人的セキュリティ対策を以下のとおり実施していますか？		
	○重要情報(個人情報を含む)を扱う全ての者(パートタイマー、アルバイト、派遣社員、顧問、社内に常駐する委託先要員等を含む)に対して就業規則や契約等を通じて秘密保持義務を課している。 ○従業員の退職に際しては退職後の秘密保持義務への合意を求めている。 ○会社の重要情報や個人情報を扱うときの規則や関連法令による罰則に関して全従業員に説明している。		
3	情報資産管理を以下のとおり実施していますか？		
	○管理すべき情報資産は情報資産管理台帳を作成する等、何処にどのようなものがあるか明確にしている。 ○重要情報は業務上必要な範囲でのみ利用を認めている。 ○重要情報の書類に秘マークを付けたり、データの保存先フォルダを指定する等、識別が可能な状態で扱っている。 ○重要情報を社外へ持ち出す時はデータを暗号化したり、パスワード保護をかけたりする等、盗難・紛失対策を定めている。 ○重要情報は施錠保管やアクセス制限をして持ち出しの記録やアクセスログをとる等の取り扱いに関する手順を定めている。 ○重要データのバックアップに関する手順を定め、手順が遵守されていることを確認している。 ○重要情報の入ったパソコンや紙を含む記録媒体を処分する場合、ゴミとして処分する前にデータの完全消去用のツールを用いたり、物理的に破壊したりし、復元不可能にすることを定めている。		
4	マイナンバー対応を以下のとおり実施していますか？		
	○特定個人情報の取扱ルール(管理担当者の割当て、収集・利用・保管・廃棄の方法)を定めている。 ○特定個人情報に関する漏えい等の事故に備えた体制を整備している。 ○特定個人情報の安全管理についてルールや手段を定めている。		
5	アクセス制御と認証を以下のとおり実施していますか？		
	○重要情報(個人情報を含む)を取扱う業務端末をダブルブラウザ(⇒事例はこちら)等でインターネット環境と分離している。 ○業務利用の全てのサーバに対して、アクセス制御の方針を定めている。		

No.	チェック項目	対応済	未対応
	○従業員の退職や異動に応じてサーバのアクセス権限を随時更新し、定期的なレビューを通じてその適切性を検証している。 ○情報を社外のサーバ等に保存したり、グループウェアやファイル受渡サービスなどを用いたりする場合、アクセスを許可された人以外が閲覧できないように、適切なアクセス制御を行うことを定めている。 ○パスワードの文字数や複雑さ等を設定するＯＳの機能等を有効にし、ユーザーが強固なパスワードを使用するようにしている。 ○業務利用の暗号化機能及び暗号化に関するアプリケーションについてその運用方針を明確に定めている。		
6	物理的セキュリティ対策を以下のとおり実施していますか？		
	○業務を行う場所に、第三者が許可無く立ち入りできないようにする対策(物理的に区切る、見知らぬ人には声をかける等)を講じている。 ○最終退出者は事務所を施錠し退出の記録(日時、退出者)を残す等、事務所の施錠を管理している。 ○重要情報やIT機器のあるオフィス、部屋及び施設には許可された者以外は立ち入り不可能に管理している。 ○重要情報を保管および扱う場所への個人所有のパソコン・記録媒体等の持込み・利用を禁止している。		
7	IT 機器利用を以下のとおり実施していますか？		
	○セキュリティ更新を自動的に行う等により、常にソフトウェアを安全な状態にすることを定めている。 ○ウイルス対策ソフトウェアが提供されている製品については用途に応じて導入し、定義ファイルを常に最新の状態にすることを定めている。 ○業務利用のIT機器に設定するパスワードに関するルール(他人に推測されにくいものを選ぶ、機器やサービスごとに使い分ける、他人にわからないように管理する等)を定めている。 ○業務利用の機器や書類が誰かに勝手に見たり使ったりされないようにルール(離席時にパスワード付きのスクリーンセーバーが動作する、施錠できる場所に保管する等)を定めている。 ○業務利用のIT機器の設定について不要な機能は無効にする、セキュリティを高める機能を有効にする等、見直しを行うことを定めている。 ○社外でIT機器を使って業務を行う場合のルールを定めている。 ○個人で所有する機器の業務利用について禁止するか、利用上のルールを定めている。 ○受信した電子メールが不審かどうかを確認することを求めている。 ○電子メールアドレスの漏えい防止のBCC利用ルールを定めている。 ○インターネットバンキングやオンラインショップ等を利用する場合に偽サイトにアクセスしない対策を定めている。		

No.	チェック項目	対応済	未対応
8	IT 基盤運用管理を以下のとおり実施していますか？		
	○IT 機器の棚卸(実機確認)を行う等、社内に許可なく設置された無線 LAN 等の機器がないことを確認している。 ○サーバには十分なディスク容量や処理能力の確保、停電・落雷等からの保護、ハードディスクの冗長化等の障害対策を行っている。 ○業務利用の全てのサーバに対して脆弱性及びマルウェアからの保護対策を講じている。 ○記憶媒体を内蔵したサーバ等の機器を処分または再利用する前に重要情報やライセンス供与されたソフトウェアを完全消去用のツールを用いたり、物理的に破壊したりし、復元不可能にすることを定めている。 ○業務利用の全てのサーバやネットワーク機器に対して必要に応じてイベントログや通信ログの取得及び保存の手順を定めた上でログを定期的にレビューしている。 ○重要な IT システムに脆弱性がないか、専用ツールで技術的な診断を行っている。 ○ファイアウォール等、外部ネットワークからの影響を防ぐ対策を導入している。 ○業務利用のネットワーク機器のパスワードを初期設定のまま使わず、推測できないパスワードに変更して運用している。 ○クラウドサービスを利用する場合は費用だけでなく、情報セキュリティや信頼性に関する仕様を考慮して選定している ○最新の脅威や攻撃についての情報収集を行い、必要に応じて社内で共有している。		
9	システム開発及び保守を以下のとおり実施していますか？		
	○情報システムの開発を行う場合、開発環境と運用環境とを分離している。 ○セキュリティ上の問題がない情報システムを開発する手続きを定めている。 ○情報システムの保守を行う場合、既知の脆弱性が存在する状態で情報システムを運用しないようにする対策を講じている。		
１０	委託管理を以下のとおり実施していますか？		
	○契約書に秘密保持(守秘義務)、漏洩した場合の賠償責任、再委託の制限についての項目を盛り込む等、委託先が遵守すべき事項について具体的に規定している。 ○委託先との重要情報の受渡手順を定めている。 ○委託先に提供した重要情報の廃棄または消去の手順を定めている。		
１１	情報セキュリティインシデント対応ならびに事業継続管理を以下のとおり実施していますか？		
	○重要情報の漏えいや紛失、盗難があった場合の対応手順書を作成する等、事故の発生に備えた準備をしている。 ○インシデントの発生に備えた証拠情報の収集手順を定め、運用している。 ○インシデントの発生で事業が中断してしまったときに再開する計画を定めている。		