情報セキュリティ対策チェックシートの解説

当シートは各チェック項目の適切な状態と、最低限必要な対策の例が記載されています。必最低限の対策が実施されている場合は、対策済みとして評価できますので、**対策がまだできていない企業様は、まずは最低限の対策を実施することを検討してください。**

	セキュリティチェック項目	適切な対策	最低限必要な対策例	参考
①	経営者による情報セキュリティ基本方針があるか	情報セキュリティへ取り組みについては、組織全体での対応方針が策定されていないと、組織内での対応が一貫したものとなりません。経営者は情報セキュリティリスクを経営リスクと認識し、方針を組織全体へ宣言します。 また、企業として対応方針を体外的に宣言することにより、ステークホルダー（株主、顧客及び取引先など）の信頼性を高め、ブランド価値向上につながります。	※以下のいずれかの対策を実施する ・企業の経営方針と整合を取ったセキュリティポリシーを策定し、組織全体の対応方針を組織の内外に宣言する。 ・年度方針や社長方針に情報セキュリティに関する取り組みを宣言する。	サイバーセキュリティ経営ガイドライン Ver 3.0 ※指示１ https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf
②	情報セキュリティ管理責任者を置いているか。	情報セキュリティ管理体制を整備していない場合、責任の所在があいまいとなり、適切な対策が講じられず、かつ、インシデント発生時の被害が拡大します。情報セキュリティ管理責任者は、情報セキュリティ管理体制のトップに位置する役割を担います。組織は自社の実態に応じた役割と責任割当に基づく体制を構築し、情報セキュリティリスク管理に取り組みます。	※以下のいずれかの対策を実施する ・経営者が情報セキュリティに関する責任者を任命する。社長など経営者が兼務することも可能です。 ・必要に応じて、管理責任者を補佐する役割(情報セキュリティ管理者)等を任命するなどして、組織全体でリスク対策が取れる体制を構築する。	サイバーセキュリティ経営ガイドライン Ver 3.0 ※指示２ https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf
③	重要な情報資産および個人情報を安全に取扱うためのルールを定めているか。	重要な情報資産や個人情報に関しては、取り扱いルールを定めていないと、情報漏洩事故が発生し、大きな損害が発生します。事故を防ぐために、重要な情報資産や個人情報については、取り扱いルールを定め管理します。	・重要な情報資産や個人情報については、管理や持ち出し方法、バックアップ、破棄などのルールを定める。 例) 資産管理台帳、個人情報管理台帳を作成する 社外に持ち出す際は、所属長の許可を得て持出記録をつける 定期的バックアップを取得する 書類はシュレッターや溶解により処分する　など	
④	セキュリティ事件・事故に対する対応手順があるか。	セキュリティ事件・事故は100%防ぐことはできません。事件・事故が発生した場合は、被害の拡大化を防ぐことが重要です。事業や顧客などに大きな影響があるインシデントが発生した場合に、迅速に対応するための対応手順をあらかじめ決めておきます。	・組織内外の緊急連絡先・伝達ルートを整備し、組織内に周知する。 例) 情報資産紛失時：本人→所属長→情報セキュリティ管理管理者の順に報告 ウイルス感染時：本人→情報システム部門 の順に報告 など	
⑤	当社委託業務を取扱う従業者に情報セキュリティに関する教育を実施しているか。	重要な情報資産や個人情報を取り扱うためのルールを定めただけでは不十分です。教育して理解させないと意味がありません。重要な情報資産や個人情報を取り扱うためのルールなどを教育し理解させます。	・定期的(年1回)に従業者へ情報セキュリティ教育を実施する。	
⑥	当社委託業務を取扱う従業者に情報資産の取扱いルールを理解させているか。		・上記教育後に理解度テストを実施する。なお、理解度が低い場合は、再度教育するなどして理解させる。	
⑦	当社委託業務を取扱う従業者に秘密保持を約束させているか。	従業者に秘密保持を約束させ、責任も持たせることで、情報漏洩や機密情報の不正使用などのリスクを減らすことができます。重要な情報資産や個人情報を取扱う従業者へは秘密保持を誓約させます。	・定期的(年1回)に従業者へ秘密保持に関する誓約書を書かせる。	
⑧	当社委託業務を取扱う従業者を限定しているか。	当社委託業務を取扱う従業者を限定することは情報セキュリティリスクを最小限に抑え、組織の機密情報やリソースを保護するために必要です。従業者を限定することで、機密情報へのアクセスを必要最小限に制限し、セキュリティを向上させることができます。	・当社委託業務を取扱う従業者を可能な限り限定して、当社委託業務に関係ない人には当社に関係する情報へアクセス(情報共有)させない。取扱う従業者が複数名であったとしても問題ありません。 ※業務に関わるかもしれない方は対象から除外して、業務に関わることが分かった時点で情報共有すべきです。	
⑨	重要な情報資産および個人情報を取扱う業務エリアへの入退室を管理しているか。	重要な情報資産および個人情報などの書類を取り扱う(保管する)エリアは、第三者が自由に出入りできないよう施錠された扉や受付などを用意するなどして対策します。	・重要な情報資産を扱う業務エリアにドア(施錠なし)や衝立などを設定して、一般の業務エリアと区別する。(1点) ・重要な情報資産を扱う業務エリアの前に受付を設置して、第三者が自由に出入りできないように監視する。(2点) ・重要な情報資産を扱う業務エリアの前に施錠された扉を用意して、第三者が自由に出入りできないようにする。(2点) ※リモートワークを許可している企業については、重要な情報資産および個人情報などの書類の持ち出し管理を徹底させる必要があります	
⑩	重要な情報資産および個人情報の保管場所の施錠管理を実施しているか。	重要な情報資産および個人情報などの書類は、社内でも取り扱いを慎重に行う必要があります。施錠ができる書棚やキャビネットに書類を施錠保管して許可のない従業者が勝手に閲覧できないようにします。	・重要な情報資産および個人情報などの書類を、書棚やキャビネットなどへ施錠保管する。(1〜2点)	
⑪	情報機器の盗難防止措置を講じているか。	情報機器には重要な情報資産および個人情報が保存されます。物理的なセキュリティ対策（例: 施錠保管、監視カメラ）やデータの暗号化、リモートワイプ（情報機器の遠隔初期化）などで対策して盗難リスクを軽減します。	※以下のいずれかの対策を実施する (1つの対策で1点、2つ以上の対策で2点) ・パソコンをロッカー等で施錠保管して盗まれにくくする。 ・犯罪(盗難など)の抑止として、建物出入口、オフィス出入口等に監視カメラを設置する。 ・パソコン内のデータを暗号化をして、盗まれてもデータを閲覧できない状態にする。 ・パソコンなどにリモートワイプできるシステムを導入する。	

⑫	情報媒体の無断複製、不正持出しの防止等の措置を講じているか。	USBメモリーなどより無断で重要な情報資産および個人情報を持ちだされることを防止するための対策を実施します。	※以下のいずれかの対策を実施する（1つの対策で1点、2つ以上の対策で2点） ・USBメモリーなどの外部デバイスへ書き込みを制限するシステムを導入する。 ・USBメモリーなどの外部デバイスへ書き込み等の操作ログを監視できるシステムを導入し、無断書き込みを抑止する。 ・USBメモリーなどの外部デバイスの利用を禁止するルールを策定する。	
⑬	重要な情報資産および個人情報の搬送、受け渡し時の保護措置を講じているか。	電子データをインターネットで送付する場合、情報漏洩リスクが想定されます。リスクを最小化するには、通信経路を暗号したりデータ自体を暗号化します。また、情報媒体を使って電子データを受け渡しする場合は、データ自体を暗号化します。さらに、持出時に記録等につけることで、情報漏洩やデータの消失時にいつ何を紛失したのかすぐに把握することができ、インシデント対応の際に役に立ちます。	※以下のいずれかの対策を実施する（1つの対策で1点、2つ以上の対策で2点） ・電子化した重要な情報資産をメール送信する場合、当該情報資産へのパスワード設定や暗号化を行う。 ・電子化した重要な情報資産をUSBメモリーなどの各種情報媒体へ保存して受け渡 したり、宅配便等で搬送する場合、当該情報資産へパスワード設定や暗号化を行う。 ・重要な情報資産の持出す場合は、持出記録等により管理する。	
⑭	情報媒体の安全な消去、廃棄の手順を整備しているか。	以下のような情報媒体の安全な消去手順と廃棄手順により、情報漏洩やセキュリティ侵害のリスクを最小限に抑えます。 1. 適切な消去方法を選択し、情報媒体を完全に消去する。 2. 物理的な廃棄が必要な場合は、信頼できる手段（例：破壊、焼却）を使用して情報媒体を処理する。	(紙媒体について、以下のいずれかの対策を実施する) ・シュレッターしてから廃棄する。 ・信用できる廃棄業者で溶解処分する。 (電子媒体について、以下のいずれかの対策を実施する) ・完全消去ツール(※)を使用してから廃棄する。 ・媒体故障などでツールが利用できない状態の場合は、媒体ごと破壊する。 ・信頼できる廃棄業者にデータ消去等を併せて依頼し、消去証明書を取得している。 ※ITトレンド 「おすすめのデータ消去ソフト9選」 https://it-trend.jp/erase_data/article/948-881	
⑮	重要な情報資産および個人情報に対して、関係者以外が閲覧できないようにするなど、適切なアクセス制限するための措置を講じているか。	重要な情報資産および個人情報の機密性を保護するために、以下のような措置を実施します。 ・ユーザーやグループごとにアクセスポリシーを設定し、必要なデータやリソースへのアクセス権を適切に制限します。 ・ユーザーやグループのアクセス権限を定期的に見直し、不要な権限を削除します。	・ファイルサーバー等へ保存する個人情報が含まれるデータ、重要なデータにはアクセス権限を設定する。また、定期的に権限棚卸を実施して、不要な権限を削除する。	
⑯	ウイルス感染、故障や誤操作、自然災害等による情報の消失、破壊に備えて、重要な情報資産および個人情報を保護するための対策を講じているか。	重要な情報資産および個人情報の可用性を保護するために、以下のような措置を実施します。 ・定期的なデータバックアップを実施し、データの消失や破壊に備えます。バックアップデータは、遠隔地やクラウド上に保存することで、自然災害などの場合でもデータの復元が可能となります。 ・データの消失時に正確かつ迅速にデータを復元するため、定期的にリストア訓練を実施します。訓練を通じて、迅速かつ正確な対応が可能となります。迅速なデータ復旧は事業継続性の観点からも重要です。	※以下のいずれかの対策を実施する ・個人情報が含まれるデータ、重要なデータは定期的にバックアップを実施する。 ・個人情報が含まれるデータ、重要なデータはパソコン内に保存せず、定期的にバックアップを実施しているファイルサーバー等に保存するように指導する。	

⑰	当社委託業務で使用する自社パソコンにはウイルス対策を行っているか。	パソコンには、ウイルス対策ソフトウェアを導入し、定期的なアップデートを行います。これにより、新たなウイルスやマルウェアに対して最新の保護を提供します。	※以下のいずれかの対策を実施する ・Windows標準のウイルス対策機能である「Defender」を有効にし、定期的にアップデートを行う。 ・市販のウイルス対策ソフトを導入して、定期的にアップデートを行う。	
⑱	当社委託業務で使用する自社パソコンにはIDとパスワードを設定しているか。	パソコンにログインIDとパスワードを設定することは、パソコンのセキュリティとプライバシーの確保に欠かせない重要な手段です。適切なIDとパスワードを設定し、不正なアクセスや不正利用を防ぎます。	・Windows自動サインインの設定を禁止し、起動時に必ずパスワード入力させる運用を行う。	
⑲	当社委託業務使用する自社パソコンは外部に持ち出さない。または、盗難・紛失時に情報漏洩しないようデータ暗号化等を講じた上で外部に持ち出ししているか。	パソコンを外部に持ち出すと、紛失、盗難のリスクが高まります。これにより、重要な情報資産や個人情報が外部の悪意のある者に漏洩する可能性があります。外部に持ち出さないことが望ましいですが、やむを得ず持ち出す場合は、パソコンのディスク暗号化を実施します。これにより、パソコンが盗難や紛失した場合でも、データの機密性が保たれます。 ※No18の対策が実施されていないとNo19のディスク暗号化対策は無意味になります。	※以下のいずれかの対策を実施する ・Windows標準(Pro限定)の暗号化機能である「BitLocker」を有効にし、ディスク暗号化を実施する。 ・市販の暗号化ソフトを導入して、ディスク暗号化を実施する。 ・パソコン内には重要な情報資産や個人情報を保存せず、重要なデータはクラウドサービス等の外部へ保存する。	