様式 No.5-2
②厳格な情報保全の必要がある契約用
20250829ver.

個人情報取扱い安全管理措置並びに情報セキュリティ対策

1　個人情報及び特定個人情報の取り扱いに際し講ずべき安全管理措置

本業務を実施するにあたって、次に示す安全管理措置を実施する[1]。なお、個人情報及び特定個人情報は以下総称し「個人情報」と記載する。

大項目	No.	小項目
1. 個人情報の取扱いに係る規律の整備	1	個人情報の取得、利用、保存等を行う場合の基本的な取扱方法を整備する。
2. 物理的安全管理措置	2	個人情報を取り扱う区域を管理し、入退室管理を行う。
	3	個人情報を取り扱うサーバー等の機器を管理している場合は、侵入対策、災害等に備えた予備電源の確保・防水対策等を行う。
	4	記録機能を有する機器・媒体の接続制限を行うとともに、端末を限定する。 （例） ・使用を想定しない USB ポートの無効化、委託事業以外での使用制限等の対策を行う。
	5	個人情報を取り扱う機器及び電子媒体等の盗難等を防止するための措置を講じる。また、持ち出しは責任者の許可制とする。
	6	（電子媒体等を持ち運ぶ場合）持ち運ぶ際に個人情報が漏えいしないための措置を講じる。 （例） ・個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。
	7	本業務の完了後、速やかに個人情報の利用を中止し、個人情報を含む媒体等を発注者に返却、又は、個人情報を復元できないよう消去若しくは適切に媒体等を破壊した上で廃棄する。
3.技術的安全管理措置	8	個人データを取り扱うことのできる機器及び当該機器を取り扱う業務従事者（受託者が個人の場合はその本人（以下同様））を明

[1] 個人情報保護委員会より公開されている「個人情報の保護に関する法律についてのガイドライン（通則編）」10（別添）講ずべき安全管理措置の内容における「中小規模事業者における手法の例示」（https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a10）、及び内閣官房内閣サイバーセキュリティセンターより公開されている「政府機関等の対策基準策定のためのガイドライン」（https://www.nisc.go.jp/pdf/policy/general/guider6.pdf#page=160）p.151-156 を参照のこと。

*情報機器（PCやスマートフォン等）、及び情報システムを使用して個人情報を取り扱う場合（インターネット等を通じて外部と送受信等をする場合を含む）に講じる措置		確化し、個人データへの不要なアクセスを防止する。
	9	個人情報を取り扱う情報システムを使用する業務従事者が正当なアクセス権を有する者であることを、識別したうえで認証する（ユーザーID、パスワード、磁気・IC カード等）。また、管理者権限は最小限の人数に絞る。
	10	外部からの不正アクセス等を防止するための措置（セキュリティ対策）を講じる。 （例） ・個人情報を取り扱う機器等のオペレーティングシステムを最新の状態に保持する。 ・個人情報を取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。
	11	個人情報を取り扱うサーバー等の機器を管理している場合は、アクセスログ等を定期的に確認、またはアクセス状況を監視し、一定量以上の情報が情報システムからダウンロードされた場合に警告表示されるなどの機能の設定、定期確認などを行う。アクセスログについては、その記録の改ざん・不正な消去の防止等を講じる。 （例） ・ログの取得対象は継続的に見直しを実施する。 ・ログの取得プロセスの障害監視を行う。
	12	（該当ある場合）業務上、情報システムで個人情報を取り扱う場合は、入力情報の照合（入力原票や既存の情報等との照合）を行う。
	13	（該当ある場合）業務上、個人情報を取り扱う情報システムの設計・開発・運用保守を伴う場合は、当該情報システムの設計書、構成図等の文書が外部に知られないような対策をする。
	14	取り扱う個人情報のバックアップを作成し、外部からの不正アクセス等を防止するための措置（セキュリティ対策）を講じる。
	15	情報システムの使用に伴う漏えい等を防止するための措置を講じる。 （例） ・メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。

２　情報セキュリティ対策

本業務を実施するにあたって、次に示す情報セキュリティ対策を実施する[2]。

大項目	No.	小項目
Part1.技術的対策	1	業務で使用する機器の OS やソフトウェアは常に最新の状態とする。
	2	業務で使用する機器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（セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル）が自動更新されるよう設定する。
	3	業務で使用する機器、サービス及びシステムにログインする際のパスワードは、強固なパスワードを設定する。 （例） ・10 桁以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」し、複数のサービス間で使いまわさない。 ・可能な場合は多段階認証や多要素認証を利用する。 ・初期パスワードの変更など主体認証情報に関する対策を行う。
	4	情報へのアクセス（データ保管などのウェブサービス及びサービス上での共有設定等）を業務上必要な者のみがアクセスできるよう設定する。 （例） ・主体認証やその属性ごとにアクセス制御を行い、管理者権限を持つ場合には必要最低限の権限と利用に制限した上で、ログを取得する。 ・システム利用者及び使用機器を一意で特定できるようにする。
	5	セキュリティ脅威に対処するための資産管理・リスク評価を実施する。 （例）

[2] 独立行政法人情報処理推進機構（IPA）より公開されている「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/guide/sme/about.html）、及び内閣官房内閣サイバーセキュリティセンターより公開されている「政府機関等の対策基準策定のためのガイドライン」（https://www.nisc.go.jp/pdf/policy/general/guider6.pdf#page=160）p.151-156 を参照のこと。

		・情報システムの変更に係る検知機能やログ解析機能を実装する。 ・外部ネットワークへの接続を伴う非ローカルの運用管理セッションの確立時に多要素主体認証を要求する。 ・定期的及び重大な脆弱性の公表時に脆弱性スキャンを実施し、適時な脆弱性対策を行う。
	6	取り扱う情報及び当該情報を取り扱うシステムの完全性の保護を行う。 （例） ・定期的な検索等によりシステムの欠陥を適時に検出し是正する。 ・ 悪意あるコードに対する保護措置を講じる。 ・ 脆弱性に係る注意喚起の監視と対処を行う。 ・ 安全性の高いアルゴリズム及び鍵長による暗号化及び電子署名機能を実装し、暗号鍵を適切に管理する。
	7	セキュリティ対策の検証・評価・見直しを行う。 （例） ・システムの欠陥の是正及び脆弱性対策について、対策計画を策定し実施する。 ・システムの欠陥の是正及び脆弱性対策等のセキュリティ対策が有効に機能していることの継続的な監視と確認を行う。
	8	脅威や攻撃の手口を知り、対策に活かす。
Part2.業務従事者としての対策	9	不審な電子メールの添付ファイルや URL を安易に開かない。
	10	電子メールの送信先を確認し、送信ミスを防ぐ。
	11	秘密情報[3]を送信する際には、メール本文ではなく添付ファイルに記述しパスワードで保護する。パスワードは予め決めておくか、携帯電話の SMS（ショートメッセージサービス）等の別手

[3] 秘密情報とは、受託者が、本業務を実施する上で、発注者その他本業務の関係者から、文書、口頭、電磁的記録媒体その他開示の方法及び媒体を問わず、また、本契約締結の前後を問わず、開示された一切の情報。ただし、次の各号に定める情報については、この限りでない。
（１）開示を受けた時に既に公知であったもの
（２）開示を受けた時に既に受託者が所有していたもの
（３）開示を受けた後に受託者の責に帰さない事由により公知となったもの
（４）開示を受けた後に第三者から秘密保持義務を負うことなく適法に取得したもの
（５）開示の前後を問わず、受託者が独自に開発したことを証明しうるもの
（６）法令並びに政府機関及び裁判所等の公の機関の命令により開示が義務付けられたもの
（７）第三者への開示につき、発注者又は秘密情報の権限ある保持者から開示について事前の承認があったもの

		段で通知する。
	12	業務で無線 LAN を利用する場合は、安全に利用するために無線 LAN のセキュリティ設定をする。 （例） ・強固な暗号化方式（WPA2、WPA3）を選択する。 ・Wi-Fi ルーター設定のための管理用パスワードを強固で推測されにくいものにする。 ・無線 LAN へのアクセス主体の認証等の対策を行う。
	13	業務でのインターネット利用する際の注意、制限をルール化し遵守する。
	14	秘密情報のバックアップを定期的に行う。
	15	秘密情報は机の上等に放置せず、不要時は鍵付き書庫に保管する。
	16	秘密情報の持ち出し時は、PC、スマートフォンなどはパスワードロックをかける等、盗難や紛失の対策を実施する。 （例） ・テレワークを実施する場合、情報セキュリティ対策[4]を行う。
	17	離席時・退社時に他人が PC を使えない状態にする（スクリーンロックやシャットダウンをする等）。
	18	執務室への関係者以外の立ち入りを禁止する。
	19	機器・備品の盗難防止対策を行う。
	20	作業場所の施錠忘れ対策を行う（最終退出者は、施錠し退出の記録を残す等）。
	21	秘密情報の記録された媒体を破棄する際には、復元できないように消去し、書面で発注者に報告する。
Part3.組織的対策	22	業務従事者（受託者が個人の場合はその本人（以下同様））に守秘義務を徹底する。 （例） ・委託業務に伴う情報を取り扱う従業員等の資格条件を明確化する。 ・従業員等の異動・退職等の際に情報を保護すること等を求める。
	23	業務従事者にセキュリティに関する教育や注意喚起を行う。

[4] 独立行政法人情報処理推進機構（IPA）より公開されている「テレワークを行う際のセキュリティ上の注意事項」参照のこと。（https://www.ipa.go.jp/security/anshin/measures/telework.html）

	24	個人所有の情報機器の業務利用は行わない。やむを得ず利用する場合は、セキュリティ対策を徹底する。
	25	再委託先等との契約において秘密保持や情報セキュリティ対応方針に関する文書を取り交わし、対策状況を確認する。
	26	クラウドサービス等の外部サービスを利用する場合には、安全性・信頼性を把握し選定する。
	27	生成 AI を利用する場合には、安全性・信頼性を把握し選定する。
	28	セキュリティインシデントの発生に備えて緊急時の体制整備や対応手順を作成する。 （例） ・識別・防御・検知・対応・復旧を例とした、準備から事後処理に至る全般的なインシデント対処プロセスを確立する。 ・報告フロー等の概要について、説明ができるようにする。
	29	情報セキュリティ対策に関するルールを明文化し、組織内に周知する[5]。

以上

[5] 受託者が個人の場合は、自らの情報セキュリティに関する行動指針を明確にし、日常的に意識・実践する。