情報セキュリティ管理策一覧

１．組織的安全管理措置

No.	分類	採否	講じる措置	備考(管理策を採用しない場合は、その理由等)
1-01	組織体制の整備	○	①個人データの取扱いに関する責任者を設置し、責任を明確化する。 ②個人データを取り扱う従業者及びその役割を明確化する。 ③個人データを複数の部署で取り扱う場合の各部署の役割分担及び責任を明確化する。	【参照】 個人情報保護体制表
1-02		○	①従業者が取り扱う個人データの範囲を明確化する。	【参照】 個人情報管理台帳
1-03		○	①法や個人情報取扱事業者において整備されている個人データの取扱いに係る規律に違反している事実又は兆候を把握した場合の責任者への報告連絡体制を整備する。 ②個人データの漏えい等事案の発生又は兆候を把握した場合の責任者への報告連絡体制を整備する。	【参照】 緊急連絡網
2-01	個人データの取扱いに係る規律に従った運用	○	システムログその他の個人データの取扱いに係る記録を取得する。 ①個人情報データベース等の利用・出力状況 ②個人データが記載又は記録された書類・媒体等の持ち運び等の状況 ③個人情報データベース等の削除・廃棄の状況（委託した場合の消去・廃棄を証明する記録を含む。） ④個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等）	【参照】 システム機器一覧 外部記憶媒体・スマートデバイス一覧 個人情報印刷・移送・廃棄記録 個人データ廃棄記録 ログ点検記録
2-02		○	①システムログその他の個人データの取扱いに係る記録を定期的に確認・点検する。	【参照】 PMS 定期点検チェックリスト 個別内部監査計画書兼報告書 バックアップ記録
3-01	個人データの取扱状況を確認する手段の整備	○	①個人データの取扱状況を把握する。	【参照】 個人情報管理台帳
4-01	漏えい等事案に対応する体制の整備	○	漏えい等事案の発生時の体制を整備する。 ①事実関係の調査及び原因の究明	【参照】 個人情報保護体制表

			②影響を受ける可能性のある本人への通知 ③個人情報保護委員会等への報告 ④再発防止策の検討及び決定 ⑤事実関係及び再発防止策等の公表等	緊急連絡網
5-01	取扱状況の把握及び安全管理措置の見直し	○	①個人データの取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する。 ②外部の主体による監査活動と合わせて、監査を実施する。	【参照】 PMS 定期点検チェックリスト 個別内部監査計画書兼報告書 PMS 運用状況報告書 是正処置報告書
6-01	テレワーキング	○	①初めてテレワークを実施する場合及びテレワークの実施環境等に変化が発生した場合は、セキュリティ責任者の承認を得る。 ②テレワークに使用する機器等の持ち運び等の状況を記録し、定期的に確認・点検する。	【参照】 テレワーク開始・変更申請書 システム機器一覧
6-02		○	①テレワーク作業場所からのオフィスネットワーク接続（VPN 等）を禁止する。 ②テレワーク作業場所で、無線ネットワークを使用する場合は、暗号化された経路を使用する。 ③テレワーク作業場所で、当社従業者以外の者（自宅の家族を含む）の周囲での挙動に注意を払い、画面等ののぞき見を防止する。 ④テレワーク作業場所で、オンライン会議を実施する場合は音漏れを防止する。	【参照】 PMS 定期点検チェックリスト
6-03		○	①公共の場でテレワークを行う場合、公衆無線ネットワークは接続しない。 ②公共の場でテレワークを行う場合、無線ネットワークのアクセスポイントの自動接続設定をオフにし、かつ、一定時間おきに接続中のアクセスポイントを確認する。	【参照】 PMS 定期点検チェックリスト
6-04		○	①個人所有の情報機器の使用する場合、十分なセキュリティ基準を満たす機器を使用する。 ②テレワーク実施中も、オフィスワーク時と同様に、各種規程に従って、業務を実施する。	【参照】 テレワーク開始・変更申請書 PMS 定期点検チェックリスト

2．人的安全管理措置

No.	分類	採否	講じる措置	備考(管理策を採用しない場合は、その理由等)
1-01	従業者の教育	○	①個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行う。	【参照】 PMS 年間計画書 個別教育計画書兼報告書
1-02		○	①個人データについての秘密保持に関する事項を就業規則等に盛り込む。	【参照】 「就業規則」 「個人情報保護に関する機密保持制約書」 「個人情報保護に関する退職時誓約書」

3．物理的安全管理措置

No.	分類	採否	講じる措置	備考(管理策を採用しない場合は、その理由等)
1-01	個人データを取り扱う区域の管理	○	個人情報データベース等を取り扱うサーバ等の重要な情報システムを管理する区域（管理区域）を適切に管理する。 ①入退室を管理する。 ②その日、最初に入室した者及び最後に退室した者の入退室記録を行う。 ③管理区域に持ち込む機器等を制限する。	【参照】 施錠解錠記録 入退室記録 鍵・入館証管理表
1-02		○	個人データを取り扱う事務を実施する区域（取扱区域）を適切に管理する。 ①権限を有しない者に個人データを閲覧等されないよう、取扱区域を管理する。 ②次の境界について、明確に定義する。 - 従業者が入場可能な入退管理された作業エリア - 社員のみが入場可能な入退管理された作業エリア - 限られた社員のみが入場可能な入退管理された作業エリア - 来訪者が入場可能な共用エリア	【参照】 体制表（オフィスレイアウト）
1-03			従業者が執務を行う区域（執務スペース）を適切に管理する。 ①従業者や来訪者等に、社員証やゲストカード等を着用させ、目に見える何らかの形式で、従業者や来訪者等を識別できるようにする。 ②貸与を受けた鍵や入館証等を、セキュリティ責任者や業務責任者の承認を得ずに、他の者に貸与してはならない。 ③貸与を受けた鍵や入館証等を紛失した場合（そのおそれがある場合を含む。）は、直ちに、セキュリティ責任者に報告する。 ④業務時間内であっても、執務スペース（施錠対象範囲ごと）内が無人となる場合は、退出時に必ず施錠を行う。 ⑤来訪者の対応は、原則として、来訪者が入場可能な共用エリアにて対応する。入退管理された作業エリアに入場する場合は、担当従業者が、常時、付き添うものとする。	【参照】 入退室記録 鍵・入館証管理表 PMS 定期点検チェックリスト
2-01	機器及び電子媒体等の盗難等の防止	○	①個人データを取り扱う機器、個人データが記録された取外し可能な電子媒体やモバイルデバイス又は個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管する。	【参照】 個人情報管理台帳 システム機器一覧 外部記憶媒体・スマートデバイス一覧
2-02		–	①個人データを取り扱う情報システムが機器のみで運用されている場合は、当該機器をセキュリティワイヤー等により固定する。	【採用しない理由】 会議等の際にノート PC やスマートデバイスを各自持参してペーパーレスを実現、作業環境を準フリーアドレス化して

				コミュニケーションを促進しており、当該施策を導入することにより業務効率が下がる。
3-01	取外し可能な電子媒体等の管理	○	①電子媒体の利用及び持ち出しの状況を、記録し、管理する。 ②電子媒体の利用及び持ち出しには、業務責任者の承認を得ることとし、承認を得ずに媒体を利用又は持ち出しすることを禁止する。 ③個人情報を保存する電子媒体（又は媒体に含まれる個人データ）には、暗号化又はパスワード設定を行う。 ④セキュリティ責任者が承認した場合を除き、個人データを格納した電子媒体を、物理的に輸送してはならない（手渡しを原則とする）。	【参照】 外部記憶媒体・スマートデバイス一覧 PMS 定期点検チェックリスト
4-01	モバイル機器の管理	○	①モバイル機器の利用状況（業務用途に使用する個人所有のモバイル端末を含む。）を、記録し、管理する。 ②モバイル機器の利用及び持ち出しには、業務責任者の承認を得ることとし、承認を得ずに媒体を利用又は持ち出しすることを禁止する。 ③モバイル機器の持ち運び時、機器の破損から守るために、可能な範囲で物理的な保護を行う。 ④モバイル機器の持ち運び時、紛失や盗難が発生した際の情報漏えいのリスクを低減させるために、施錠できるケースや鞄に入れて持ち運ぶよう努める。 ⑤遠隔操作による機器の無効化、データの消去又はロックの機能を有するモバイル機器を利用する場合は、当該機能を有効にして利用する。 ⑥起動時及び画面ロック解除時等、モバイル機器が有する認証機能（BIOS パスワード、PIN コード、生体認証等）を有効にして利用する。	【参照】 システム機器一覧 外部記憶媒体・スマートデバイス一覧 PMS 定期点検チェックリスト
4-02		○	個人所有のモバイル機器の使用について、次の通りとする。 ①オフィスネットワーク接続（無線 LAN 等）を禁止する。 ②業務用途に使用する場合、私的な使用と業務上の使用とを区別するようにし、モバイル機器内に保有される業務上の個人情報を必要最小限とする。 ③業務用途に使用可能なソフトウェアやクラウドサービスを、記録し、管理する。	【参照】 ソフトウェア利用状況一覧 PMS 定期点検チェックリスト
5-01	紙媒体の管理	○	①バインダー等に綴じて保管する場合は、個人情報の存在や内容を容易に識別できるよう、バインダー等の表紙や背表紙にラベルを貼付する。 ②個人情報の保管を、倉庫会社等に委託する場合は、信頼できる倉庫会社を用いる。	【参照】 PMS 定期点検チェックリスト 紙媒体印刷・移送・廃棄記録 委託先チェックリスト 委託先一覧 委託業務内容報告書
5-02		○	個人データを格納した紙媒体を、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護するために、紙媒体の輸送方法について、次の通りとする。	【参照】 委託先チェックリスト

			①信頼できる輸送機関又は運送業者を用いる。 ②輸送途中に生じるかもしれない物理的損傷から内容を保護するために、媒体の仕様に合った十分な強度の梱包をし、かつ、輸送業者又は運送業者に適切な指示を行う。 ③物理的媒体の輸送内容を、記録し、管理する。	委託先一覧 委託業務内容報告書 個人データ授受記録
6-01	機器及び媒体等の処分	○	認可されていない者に個人情報が漏えいするリスクを最小化するため、電子媒体及び紙媒体の処分について、次の通りとする。 ①処分内容を記録し、管理する。 ②電子機器を廃棄する場合は、物理的な破壊、専用のデータ削除ソフトウェアの利用等、容易に復元できない手段を採用する。 ③個人データ等の機密情報を含む紙媒体を廃棄する場合は、焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。 ④電子媒体の処分を委託する場合は、適切な管理と処理ができる委託先を選定し、委託先が発行する処分の記録（廃棄証明書等）を取得及び保管する。	【参照】 システム機器一覧 外部記憶媒体・スマートデバイス一覧 紙媒体印刷・移送・廃棄記録 個人データ廃棄記録
7-01	クリアデスク・クリアスクリーン	○	①パソコン端末やスマートデバイスは、離席時には、ログオフ状態にしておくか、又はパスワードが設定されたスクリーン及びキーボードのロック機能によって保護する。 ②パソコン端末を一定時間操作しない場合は、自動的に、前後のログオフ状態及びロック状態となるように設定する。 ③使用しない状態が続くパソコン端末は、原則として、施錠できる場所で保管する。 ④重要な個人情報を印刷する場合は、直ちにプリンタから回収する。	【参照】 システム機器一覧 PMS 定期点検チェックリスト

４．技術的安全管理措置

No.	分類	採否	講じる措置	備考(管理策を採用しない場合は、その理由等)
1-01	利用者及びアクセス権の管理	○	利用者の管理について、次の通りとする。 ①セキュリティ管理責任者は、利用者ごとに一意な利用者 ID を付与する。 ②共有 ID の利用は、業務上又は運用上の理由で必要な場合に限って使用できることとし、使用の際は、セキュリティ責任者の承認を得る。 ③不要となった利用者 ID は、直ちに、無効化又は削除する。 ④セキュリティ管理責任者は、利用者 ID の利用状況を定期的に確認し、新たに不要となった利用者 ID を特定する。 ⑤利用者 ID の再利用（同じ利用者 ID を別の従業者に割り当てること）を行わない。	【参照】 システム管理者作業記録 PMS 定期点検チェックリスト
1-02		○	利用者アクセス権限の管理について、次の通りとする。 ①原則として、情報機器や情報システムへのアクセスに必要な権限単位ごとにアクセス権限グループを作成し、利用者を必要なアクセス権限グループに所属させる方法により、アクセス権限の制御を行う。 ②不要となったアクセス権限グループは、直ちに、無効化又は削除する。 ③セキュリティ管理責任者は、アクセス権限グループの利用状況を定期的に確認し、新たに不要となったアクセス権限グループを特定する。 ④セキュリティ管理責任者は、アクセス権限グループの設定内容を、定期的に確認する。	【参照】 システム管理者作業ログ PMS 定期点検チェックリスト
1-03		○	パスワードの管理について、次の通りとする。 ①セキュリティ責任者は、次の事項を満たすパスワード設定ルールを決定し、従業者に通知する。 - 利用者の関連情報（例えば、利用者 ID、氏名等）から推測できないこと - 大文字、小文字、数字、記号等を混在させること - 適切な長さの文字列であること ②セキュリティ責任者は、パスワード管理システムが、利用者が設定しようとするパスワードの検証機能を有する場合は、当該機能を有効にして利用する。 ③パスワード情報を、例えば、紙、ファイル、モバイル機器等に、記録して保管してはならない。ただし、セキュリティを確保して記録・保管できる場合には、この限りではない。 ④パスワードは秘密にしておき、誰にも漏らしてはならない。 ⑤セキュリティ責任者は、利用者に各自のパスワードを保持することを求める場合は、最初に、仮パスワードを発行し、最初の利用時に利用者に変更させる。 ⑥利用者のパスワード失念によりパスワードを再発行する場合も、前号同様とする。	【参照】 PMS 定期点検チェックリスト
2-01	ネットワーク及びネットワークサービスへのアクセス制御	○	①セキュリティ管理者は、十分な個人情報セキュリティを確保したネットワーク環境を構築し、維持するため、当該情報を文書化する。	【参照】 体制表（ネットワーク構成）

3-01	情報及びアプリケーションのアクセス制御	○	①情報やアプリケーションシステムへのアクセスを、「No.1 利用者及びアクセス権の管理」に準じて、管理する。 ②アプリケーションシステムが次の機能を有する場合は、やむを得ない理由ががある場合を除き、当該機能を活用し、アクセス制御を行う。 - 利用者の利用可能メニューを制御する。 - 利用者がアクセスできるデータを制御する。 - 利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御する。 - 出力に含まれる情報を制限する。	【参照】 システム管理者作業ログ PMS 定期点検チェックリスト
4-01	暗号による管理	○	オフィスネットワークでの無線接続設定及び利用について、次の通りとする。 ①アクセスポイントの SSID を、ステルス設定にする。 ②暗号化方式を、「WPA2-PSK（AES）」以上のセキュリティレベルのものとする。	【参照】 システム機器一覧 PMS 定期点検チェックリスト
			暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」（CRYPTREC 暗号リスト）に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用する。	【参照】 「電子政府推奨暗号リスト」 https://www.cryptrec.go.jp/list.html
5-01	マルウェア対策	○	マルウェア対策について、次の通りとする。 ①インストールするソフトウェアは、販売者又は責任者の連絡先及び更新情報が明確なものを入手する。 ②外部から入手したファイル（電子メールに添付されているファイル、ダウンロードしたファイルを含む。）および電子媒体は、利用する前にウイルスチェックを実施する。 ③マルウェア対策のためのソフトウェア（アンチウイルスソフトウェア）をインストールし、適宜に最新のウイルス定義ファイルに更新し、活用する。 ④アンチウイルスソフトウェアのリアルタイムスキャン機能をオンにし、少なくとも毎月一回、最新のウイルス定義ファイルを使用してフルスキャンを実施する。 ⑤OS やアプリケーションのセキュリティ機能（OS のファイアウォール設定、Microsoft Office 系ソフトウェア使用時のマクロ機能実行設定、ウェブブラウザのセキュリティ設定等）を活用し、被害の未然防止に努める。 ⑥不審な電子メールに添付されたファイル及び電子メール本文中のリンクを開いてはならない。 ⑦信頼できないウェブサイトを訪問しないよう努める。 ⑧判断に迷うことがあれば、セキュリティ管理責任者に連絡・相談し、その指示に従って対応する。	【参照】 ソフトウェア利用状況一覧 PMS 定期点検チェックリスト 緊急連絡網 緊急事態報告書
		○	マルウェアに感染（そのおそれがある場合を含む。）した場合の対応について、次の通りとする。 ①直ちに、感染した情報機器の使用を中止し、ネットワークから当該機器を離脱させ（LAN ケーブルを抜く、無線 LAN 接続を切断・無効化する等）、セキュリティ管理責任者に報告する。 この時、情報機器の電源は切らないようにする。（再起動に発動するウイルスがある、調査のために必要なメモリ上のデータが消失してしまう等の理由による。）	【参照】 システム機器一覧 緊急連絡網 緊急事態報告書

			②セキュリティ責任者は、次の対応を行う。 - 感染した情報機器を調査し、状況を把握する。マルウェアに感染していると判断した場合、その旨を、個人情報保護管理者に報告する。 - 被害の拡大を防止するため、従業者に通知する。 - ウイルスの種類及び感染範囲の解明に努める（必要に応じて、外部委託を検討する）。 - 全ての調査等完了後、感染した情報機器（パソコン、感染時期に接続していた周辺機器等）を初期化し、復旧作業を行う。	
6-01	ネットワークセキュリティ管理	○	ネットワーク構成の決定時には、次の事項を考慮し、決定する。 ①外部からの侵入が困難であること ②外部から侵入されても被害を局所化できること ③外部からの侵入等を、監視・検知できること ④ネットワークの管理・運用が容易であること ⑤ネットワークの調査・復旧が容易であること	【参照】 システム管理者作業ログ 個別内部監査計画書兼報告書
		○	オフィスネットワークの実現については、インターネットとの境界に、次の機能を有するルーターを設置し、次の機能を有効にして利用する。 ①IP アドレス及びポート番号で通信設定可能なファイアウォール機能 ②NAT 機能 ③アクセス元・アクセス先が記録される通信ログ機能 ④個人所有の情報機器や来訪者が接続可能なネットワークを設置する場合は、業務用ネットワークとは分離したネットワークセグメントとする。 ⑤ 外部への公開サーバをオフィス内に設置する場合は、業務用ネットワークとは分離したネットワークセグメント（例えば、DMZ 等）とする。 ⑥リモートの情報システム（ウェブサーバ等）との間で通信する場合は、暗号化された通信経路（SSL、FTPS 等）又は専用線等、安全な通信経路を利用する。	【参照】 体制表（ネットワーク構成） システム機器一覧
		○	公開サーバによる外部へのサービス実現要件を、次の通りとする。 ①ウェブサイトは、HTTPS で公開する。（HTTP でのアクセスを不可とする。）	【参照】 体制表（ネットワーク構成） システム機器一覧
7-01	電子的メッセージ通信の利用	○	電子的メッセージ通信（電子メール、SNS、ファイル共有等）の利用について、次の通りとする。 ①認可されていないアクセス、改ざん、サービス妨害等からメッセージを保護するため、メッセージ送受信の際は、可能な限り認証や暗号化を実施する。 ②正しい送付先及びメッセージ送信が確実となるよう、慎重に操作する。 ③誰でも利用できる外部サービス（例えば、インスタントメッセージ、SNS、ファイル共有）を利用して個人データの転送を行ってはならない。 ④個人データを電子メールの添付ファイルで送信する場合は、添付ファイルにパスワードを付加して送信	【参照】 PMS 定期点検チェックリスト

			する。パスワードは、送信先との間で、あらかじめ決定しておく。	
8-01	FAX の利用	○	①FAX にて個人情報を送る場合は、送信前に相手に連絡し、在席であることを確認する。かつ、送信後に、受領したことを確認する。 ②FAX にて個人情報を受け取ってはならない。意図せず、受信した場合は、直ちに削除する。	【参照】 個人データ授受記録 個人データ廃棄記録
9-01	技術的ぜい弱性管理	○	①セキュリティ任者は、利用中の情報機器や情報システムの技術的ぜい弱性に関する情報を、適宜、獲得し、そのぜい弱性を評価して、適切な措置を講じる。 ②セキュリティ管理責任者は、獲得した技術的ぜい弱性に関する情報が、当社事業に影響を及ぼすものである場合は、被害を防止するため、従業者に通知する。	【参照】 システム管理者作業ログ