文書番号 04_01

認定特定非営利活動法人育て上げネット

情報セキュリティ・管理規程

目　次

1	総則	改訂日	2022.4.1
適用範囲	全職員（役員、常勤職員、非常勤職員、フェローボランティア等を含む）		

1. 目的

本規程は、認定特定非営利活動法人育て上げネット（以下、「当法人」という。）が保有する情報資産の適切な管理に必要な法人内の機構・体制を定めるとともに、情報セキュリティ領域における、法人構成員の行動規範を示すことで、業務の適正かつ円滑な運営を図ることを目的とする。

2. 適用範囲

本規程は、全ての職員および元職員に適用する。本規程にいう職員とは、理事、役員、職員、フェロー、インターン等名称や雇用条件にかかわらず、当法人の業務及び活動にかかわるすべての者をいう。

3. 規程の改廃

本規程の施行および改廃は、情報セキュリティ責任者が提案し、経営ボード会議で承認するものとする。

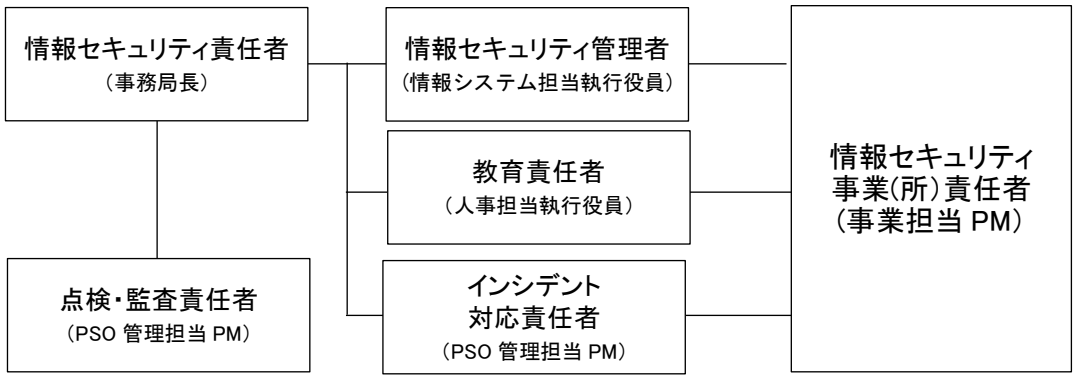
2	組織的対策	改訂日	2022.4.1
適用範囲	全職員（役員、常勤職員、非常勤職員、フェローボランティア等を含む）		

1. 情報セキュリティのための組織内の分掌・体制

法人は、情報セキュリティ管理のため以下の分掌・体制を定め、情報セキュリティ対策の実施と管理（実施状況の把握、法人内外の情報セキュリティに関する情報の収集・共有等）を行う。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者で 1 名配置。事務局長をもって充てる。情報セキュリティ対策などの決定権限を有し、必要に応じて経営ボード会議に諮問を行う。
情報セキュリティ管理者	情報セキュリティ対策のためのシステム管理を行う。情報システム担当の執行役員をもって充てる。
教育責任者	情報セキュリティ対策を推進するために職員への教育を企画・実施する。人事担当執行役員をもって充てる。
インシデント対応責任者	情報セキュリティ事案・事故発生時の対応責任者で、1 名配置 PSO 管理担当プロジェクトマネージャーをもって充てる。
情報セキュリティ事業（所）責任者	各事業・拠点における情報セキュリティの運用管理責任者で、事業（所）ごとに 1 名配置。各事業（所）における情報セキュリティ対策の実施などの責任を負う。事業（所）の長をもって充てる。
点検・監査責任者	情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。PSO 管理担当プロジェクトマネージャーをもって充てる。

＜情報セキュリティ管理体制図＞



1-2.情報セキュリティ取組みの点検

点検責任者は、情報セキュリティ関連規程の実施状況について、年度ごとに１回点検を行い、点検結果を情報セキュリティ責任者に報告する。情報セキュリティ責任者は、報告に基づき、以下の点を考慮し、情報セキュリティ管理体制図のメンバーと共に必要に応じて改善計画を立案する。

●情報セキュリティ関連規程が有効に実施されていない場合は、その原因の特定と改善

●情報セキュリティ関連規程に定められたルールが、新たな脅威に対する対策として有効でない場合は、情報セキュリティ関連規程の改訂

●情報セキュリティ関連規程に定められたルールが、関連法令や取引先の情報セキュリティに対する要求を満たしていない場合は、情報セキュリティ関連規程の改訂

1-3.情報セキュリティに関する情報共有

情報セキュリティ管理者は、新たな脅威及び脆弱性に関する警戒情報等を専門機関等から適時入手し、情報セキュリティ責任者に共有する。

2.情報セキュリティ委員会

情報セキュリティ対策に関する法人の指針及び施策の策定、またその見直しを行うための合議機関として情報セキュリティ委員会を設置する。

- 情報セキュリティ委員会は、情報セキュリティ責任者を議長として、情報セキュリティ管理者、インシデント責任者（PSO 管理担当 PM)、PSO 情報システム担当 PM、PSOPR 担当 PM、DX 推進担当 PM を常任の委員として構成する。
- また情報セキュリティ責任者は委員会での検討内容に応じて、適切な見識を有する者を非常任の委員として任命することができる。
- 情報セキュリティ委員会は、情報セキュリティ責任者が必要と認めたとき、または委員会構成員から招集の要請があったときに適時開催する。
- 本委員会の事務局として DX 推進担当を充てる。

3	人的対策	改訂日	2022.4.1
適用範囲	全職員（役員、常勤職員、非常勤職員、フェローボランティア等を含む）		

1. 雇用条件

職員が当法人の活動に関わる際には秘密保持契約を締結する。

2. 職員の責務

職員は、以下を遵守する。

●職員は、当法人が営業秘密として管理する情報及びその複製物の一切を許可されていない組織、人に提供してはならない。

●職員は、当法人の情報セキュリティ方針及び関連規程を遵守しなければならない。違反時の懲戒については、就業規則に準じる。

※当法人が秘密として管理する情報とは、「情報資産管理台帳」の機密性評価値が 1 以上のものをいう

3. 活動の休止及び終了

●職員は、活動期間中に閲覧・使用を許可された業務に関連する資料、秘密、個人情報、取引先等から当法人が交付を受けた資料又はそれらの複製物の一切を休職及び活動終了時に返還しなければならない。

●職員は、活動期間中に知り得た当法人の秘密等を利用して、競合的あるいは競業的行為を行ってはならない。

4. 情報セキュリティ教育

教育責任者は、以下の点を考慮し、情報セキュリティに関する教育計画を事業年度ごとに立案する。（各事業（所）内で行う研修を含む）。

対象者：全職員

テーマ：以下を必須とする。

- ➢情報セキュリティ関連規程及びマニュアルの説明（入職・活動開始時）
- ➢最新の脅威に対する注意喚起（随時）
- ➢関連法令の理解（随時）

4	情報資産管理	改訂日	2022.4.1
適用範囲	全職員（役員、常勤職員、非常勤職員、フェローボランティア等を含む）		

1. 情報資産の管理

1.1 情報資産の特定と機密性による分類

当法人の事業に必要で管理すべき情報並びに個人情報（以下「情報資産」という）は、情報セキュリティ責任者が「情報資産管理台帳」に記載して管理するものとし、その管理実務は PSO 管理担当が行う。また情報資産の特定と機密取扱いレベルの評価については情報セキュリティ責任者が行う。

情報資産の機密性レベル分類及び対応する法人内の取扱いについては以下のとおり定めるものとし、具体例等の詳細は別表「機密性レベル分類一覧表」において表示、公開する。

機密性４　極秘情報：

法人の全体ないし将来の運営に関わり最高度の保護を行うもの

機密性３　高度機密情報：

法律上の規定に基づく個人情報、また法人と雇用契約ないし取引、寄付の授受関係を有する個人及び法人に関わる機微情報を含み業務取扱上 高度の保護・管理を行うもの

機密性２　限定機密情報：

個別事業及び特定部署・職員の業務遂行上、使用・閲覧者を限定して保護・管理するもの

機密性１　一般機密情報：

法人業務の安全かつ円滑な遂行のため、使用・閲覧の範囲を法人内の役職員に限るもの

機密取扱い分類一覧

レベル	分類	取扱	閲覧範囲
機密性４	極秘情報	経営執行役員外秘	経営担当執行役員のみ
機密性３	高度機密情報	限定職員外秘	限定の業務に従事する役員のみ
機密性２	限定機密情報	限定管理職外秘	経営執行役員・PM
		管理職外秘	ＰＭ限定（横断的に閲覧可）
		部外秘	部署内職員のみ
		横断限定部外秘	限定部署の役・職員
機密性１	一般機密情報	法人外秘	法人内の役職員に限る

1.2 情報資産の分類の表示

情報資産の機密性レベル分類及び取扱い種別は「情報資産管理台帳」において表示する。「情報資産管理台帳」は、職員が情報資産の機密性レベルを随時確認できるよう Microsoft365 上において管理、公開する。

1.3 情報資産の運用管理責任者

情報資産の取り扱いに関する情報セキュリティの運用管理責任者は、当該情報資産を利用する情報セキュリティ事業（所）責任者とする。

1.4 職員の情報資産取扱いの範囲

情報資産の利用・取扱いは、「情報資産管理台帳」に示された範囲の職員に限るものとする。

2.情報資産の外部への開示・法人外持ち出し

2.1 情報資産の外部への開示

業務上の理由等、やむを得ない事情により機密性 1 以上の情報資産を外部に開示するときには、情報セキュリティ管理者の許可を得なければならない。

2.2 情報資産の法人外持ち出し

情報資産の持ち出しには電子媒体等による物理的な持ち出しのほか、クラウド上データの端末へのダウンロードをも含むものとし、これらの行為は原則不可とする。業務上の理由等、やむを得ない事情により情報資産の法人外持ち出しを行う場合には、以下を必須とする。

- ●法人外秘の場合は情報セキュリティ事業（所）責任者の許可を得る。
- ●機密性 2 以上の場合は情報セキュリティ責任者の許可を得る。
- ●法人保有のノートパソコン、スマートフォン、タブレット端末、外付け HDD/SSD、USB メモリなどの小型電子媒体の持ち出しは原則禁止とする。なお、業務上やむを得ず持ち出しが必要な場合は情報セキュリティ事業（所）責任者の許可を得ること。
- ●携行中は常に監視可能な距離を保つ。

2.3 貸与及び私有 IT 機器の業務使用における情報資産の取扱い

許可を得て法人からの貸与、または私有の IT 機器を用いて勤務をする場合、個人情報、機密情報を含むデータを機器上に残してはならない。作業に当たってはダウンロードせずに、クラウド上で開いたファイルを操作することが望ましいが、やむを得ずダウンロードする場合には、1 日の業務が終了するときに、当該データをパソコン上から完全に削除しなければならない。（ゴミ箱にも残っていないことを確認する。）

3.媒体の処分

3.1 媒体の廃棄

法人外秘又は極秘の情報資産を廃棄する場合は以下の処分を行う。

書類・フィルム	細断/溶解によって復元不能な状態とする
USB メモリ・HDD・CD・DVD	破壊

3.2 媒体の再利用

極秘又は法人外秘の情報資産を保存した媒体を再利用する場合は、以下の処分を行う。

書類	裏紙再利用禁止
USB メモリ・HDD・CD-RW ディスク・DVD-RW ディスク・CD-R・DVD-R	再利用不可

4.バックアップ

4.1 バックアップ

情報セキュリティ管理者は、情報資産管理台帳の記載に従い必要なデータのバックアップを定期的に取得する。

4.2 バックアップ媒体の取り扱い

バックアップに利用した機器及び媒体の取り扱いは以下に従う。

＜保管＞

●小型媒体：施錠付きキャビネットに保管

●NAS サーバー：施錠付き室内に設置

＜廃棄・再利用＞

●「3.媒体の処分」に従う

5	アクセス制御及び認証	改訂日	2022.4.1
適用範囲	職員、本部及び事業所		

1. アクセス制御方針

情報資産を扱う情報システム又はサービスに対するアクセス制御は以下の方針に基づいて運用する。対象となるシステム等は別表「アクセス制御対象情報システム及びアクセス制御方法と職員の認証方法一覧」に記載する。

●「情報資産管理台帳」の取扱い可能者の範囲に基づき、職員の業務・職務に応じた必要最低限のアクセス権を付与する。

●特定の情報資産へのアクセス権が、同一人物に集中することで発生し得る不正行為等を考慮し、システム管理等特定業務に係るアクセス権については、当該業務用の個別アカウントを発行して、複数の職員で共用する。なお複数職員共用のアカウントの発行に当たっては、情報セキュリティ委員会またはその指名した者の許可を得るものとする。

2. 職員の認証

情報資産を扱う法人内情報システムは、以下の方針に基づいて職員の認証を行う。認証方法等は別表「アクセス制御対象情報システム及びアクセス制御方法と職員の認証方法」を参照のこと。

●職員の認証に用いるアカウントは、原則職員 1 名につき 1 つを発行する。

●複数の職員が管理に関わる特定業務用のアカウントでも認証を行う場合がある。

3. 職員アカウントの登録

職員の認証に用いるアカウントは、情報セキュリティ管理者の承認に基づき登録する。アカウント名の設定条件は「8. 2 職員アカウント・パスワードの条件」を参照のこと。

4. 職員アカウントの管理

職員の認証に用いるアカウントが不要になった場合、情報セキュリティ管理者は、当該アカウントの削除又は無効化を、当該アカウントが不要になる日の翌日までに実施する。

5. パスワードの設定

職員の認証に用いるパスワードは、以下に注意して設定する。パスワードの設定条件は、「8. 3 職員アカウント・パスワードの条件」を参照のこと。

●十分な強度のあるパスワードを用いる。

●他者に知られないようにする。

6. 職員以外の者に対する職員アカウントの発行

当法人の職員以外の者にアカウントを発行する場合は、情報セキュリティ委員会の承認を得たうえで、秘密保持契約を締結する。

7.端末のログイン/ログアウト機能

情報資産を扱う情報システムの端末もしくは情報機器は、ログイン/ログアウト機能を有するものの利用を必須とし、当該機能を有効にした上で使用しなければならない。 また、職員は「7.ＩＴ機器利用 3.2 クリアスクリーン」を参照し、情報資産への不正アクセスを防ぐ。

8.標準設定等

8.1 アクセス制御対象情報システム及びアクセス制御方法と職員認証方法については、
別に定める別表「アクセス制御対象情報システムへのアクセス制御と職員の認証方法一覧」を参照のこと。

8.2 職員アカウント・パスワードの条件

	一般アカウント
アカウント名	●職員メールアドレスまたは職員番号
パスワード	＜パスワードに使う文字＞ ●10 文字以上 ●当人の名前、電話番号、誕生日等、他者が推測できるものを使わない ●アルファベット大文字･小文字、数字、記号の全てを含む ●英語辞書に含まれる単純な語を使わない（辞書攻撃の防止）

8.3 機器の認証について

職員のアクセス制御、認証にあたってはアカウント ID とパスワード、多要素認証等を多重的に用いることで対応し、個別機器の認証については当面行わないが、将来的にこれを行う可能性がある。

6	物理的対策	改訂日	2022.4.1
適用範囲	全事業（所）		

1. セキュリティ領域の設定

当法人内で扱う情報資産の重要度に応じて法人内の領域を区分する。区分した領域内では以下を実施する。

レベル 1 領域	【本部】：1 階受付・受付前面談スペース、1 階 2 階会議室研修室、中 2 階 JT フロア、半地下（旧経理室、管理担当室を除く）・地下 JT 倉庫（スタジオを除く） 【事業所】：受付・面談ブース・セミナー室等
利用者	職員、法人外関係者、部外者が立ち入り可
施錠	1 階正面自動ドア：18：00 施錠 地下、1 階（受付中扉）・2 階外側会議室研修室鉄扉：常時施錠 中 2 階 JT フロア：最終退室者による施錠
設置可能情報機器	ディスプレイ、プロジェクター、ホワイトボード、利用者用 PC
制限事項	未使用時に法人外秘又は極秘の情報資産の放置禁止
部外者管理	受付スペース以外は職員の許可を受けて入室可能
管理記録	１階正面自動ドア防犯カメラ録画にて画像記録
侵入検知	PSO 管理担当職員による防犯カメラモニター目視 施設全館施錠時　警備会社人感センサー作動
来客検知・確認	1 階受付内線、職員の直接対応により来所目的を確認
火災対策	火災報知器：2 階外側会議室研修室、１階 PC ルーム 地下 JT 倉庫 消火器設置：2 階会議室研修室外側エレベーター前、中 2 階階段脇、１階受付前面談スペース脇、半地下階段脇、地下 JT 倉庫内、地下鉄扉外側エレベーター前 防火シャッター：半地下

レベル 2 領域	【本部】：2 階 JT スタッフスペース、半地下 PSO 管理担当室、地下スタジオ 【事業所】：情報管理スペース
利用者	配属職員以外の入室は配属職員の許可又はエスコートが必要
施錠	半地下 PSO 管理担当室：最終退室者による施錠

	2 階 JT スタッフスペース、地下スタジオ：施錠無
設置可能情報機器	ディスプレイ、プロジェクター、ホワイトボード、 パソコン、複合機、電話機
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止（PM 以上の許可がある場合のみ可能とする）
部外者管理	配属職員の許可を受けて入室可能
管理記録	ー
侵入検知	ー（職員常駐、不在時は備品等施錠管理）
火災対策	煙感知機：半地下 PSO 管理担当室 火災報知器：地下スタジオ 消火器設置

レベル 3 領域	旧経理室
利用者	役員以上・PSO 管理担当職員、役員が入室許可した者
施錠	常時施錠及び警備会社への通報装置作動
設置可能情報機器	パソコン、ルータなどのネットワーク機器
制限事項	情報機器・設備の無段操作禁止・無断持ち出し禁止 スマートホン、USB メモリ、HDD、CD-R、デジタルカメラその他の情報記録媒体の無断持ち込み禁止 秘密書類の無断持出し禁止
部外者管理	役員のエスコート付で入室可能 保守点検時等に入室許可者の立会で入室可能
管理記録	接触型セキュリティカードにより入室管理、警備会社自動記録
侵入検知	ー
来客用名札	ー
火災対策	火災報知器、煙感知器、空調設備

2.関連設備の管理

情報機器に関連する設備は以下を設置する。

●ノート PC は不使用時、施錠可能なラック等収納設備に収納する。

●デスクトップ PC は必要に応じてワイヤーロック等を施す。

3.セキュリティ領域内注意事項

セキュリティ領域では区分にかかわらず以下の点に注意する。

●複合機、プリンタに原稿、印刷物を放置しない。

●FAX 送信時には誤送信防止のため FAX 送信マニュアルにそって行う
●ホワイトボードは利用後に消去する。
●室内での撮影、録音は禁止する。業務上必要な場合は、情報セキュリティ事業（所）責任者の許可を得ること。
●会議室内では会話の盗み聞きを防止するよう配慮する。
●外線受話時の際に相手に不審な点のある場合は、職員の個人情報を伝えてはならない。
●部外者を見かけた場合は用件を確認する。

4.搬入物の受け渡し

郵便物及び宅配便の受取り・受け渡しは、以下を介して行う。

＜本部＞

●郵便物：ポスト/書留便の場合は受付　事業所：受付
●宅配便：本部：1 階受付、事業所：受付

7	Ｉ Ｔ機器利用	改訂日	2022.4.1
適用範囲	業務で利用する情報機器		

1. ソフトウェアの利用

1.1 標準ソフトウェア

業務に利用するパソコンには、法人が指定する標準ソフトウェアを導入する。法人の標準ソフトウェア以外のソフトウェアを導入する場合は、情報セキュリティ管理者の許可を得たうえで導入する。標準ソフトウェアは別表「標準ソフトウェアとアップデート方法一覧」を参照のこと。

1.2 ソフトウェアの利用制限

情報セキュリティ管理者は、法人が貸与するデバイスから職員の業務に不要な機能をあらかじめ取除いて提供する。職員は、業務に不要なシステムユーティリティやインストールされているソフトウェアを追加・利用してはならない。業務に必要なシステムユーティリティやソフトウェアの追加する場合には、情報セキュリティ管理者に申請して別途承認を得ること。また私有 IT 機器の業務利用におけるシステムユーティリティやソフトウェア利用については「私有 IT 機器取扱規程」を参照すること。

＜利用を禁止するソフトウェア＞

●インターネット上で、不特定多数のコンピュータ間でファイルをやりとりできるソフトウェア（ファイル共有ソフト）。

●不審な提供元が提供するソフトウェア。

●正規ライセンスを取得していないソフトウェア。

●提供元のサポートが終了しているソフトウェア。

1.3 ソフトウェアのアップデート

職員は、業務で使用するソフトウェアを最新の状態で利用する。最新の状態で利用する方法は別表「標準ソフトウェアとアップデート方法一覧」を参照のこと。

1.4 ウイルス対策ソフトウェアの利用

1.4.1 ウイルス検知

職員は、以下の方法でウイルス検知を行う。

●ネットワーク経由で入手するファイルは、自動検知機能を有効にしてウイルス検知を実施する。

●電子媒体を用いてファイルの受け渡しを行う場合は、媒体内のファイルにウイルス検知を実施する。方法については PSO 情報システム担当より随時提供される情報（マニュアルを含む）を参照のこと。

1.4.2 ウイルス対策ソフト定義ファイルの更新

職員は、パソコン・スマートフォン・タブレットに導入したウイルス対策ソフトウェアの定義ファイルを随時更新する。持ち出し用ノートパソコンは利用時に定義ファイルの更新を確認する。定義ファイルの更新方法は別表「標準ソフトウェアとアップデート方法一覧」を参照のこと。

1.4.3 法人外機器の LAN 接続

法人の貸与機器および申請に基づいて利用が許可された私有の IT 機器類以外のデバイスを法人のクラウド環境・サーバー及び社内 LAN に接続することを禁止する。

1.5 ウイルス対策の啓発

情報セキュリティ委員会は、適宜ウイルスに関する情報を収集し、重大な被害を与えるウイルスに対しては、対応策及び対応に必要な修正プログラムを社内に公開及び通知する。職員は、感染防止策が通知された場合は、速やかに実施完了すること。

2. ＩＴ機器利用にあたってのセキュリティ管理

2.1.法人貸与機器のアカウント管理

法人が業務のために職員、または利用者に貸与するすべてのデバイス（パソコン・タブレット・スマートフォン）については、貸与時に PSO 情報システム担当が管理者権限を行使できる設定がなされていなければならない。

貸与機器の使用にあたっては、スタッフの使用するアカウントについては管理者権限、利用者の使用するアカウントについてはユーザ権限での設定を行うこと。

2.2.IT 機器利用上のセキュリティ管理

職員は、業務に利用するデバイスには、ログインパスワードを設定する。利用するときには以下を実施する。

●ログインパスワードを他者の目に触れる所に書き記さない。
●外出先等で利用する場合は、他者が画面を盗み見ることが可能な環境で利用しない。
●退勤時又は使用しないときには電源を切り、ノートパソコン・タブレット・スマートフォン・USB メモリ、HDD、CD 等の電子媒体は施錠保管する。

3.クリアデスク・クリアスクリーン

3.1 クリアデスク

職員は、機密性レベル 1 以上の情報を含む書類及び電子データを保存したノートパソコン、USB メモリ、HDD、CD 等の持ち運び可能な機器や媒体について、以下の取扱い（クリアデスク）を徹底する。

●利用時以外には机上に放置しない。
●離席時は書類を保管場所に戻す。
●手書きした資料は作成した当日中に必要事項を電子化し、破棄する。やむを得ず電子化できない資料は施錠保管できる場所で管理する。
●退勤時又は使用しないときには施錠保管あるいはケンジントンロックする。

3.2 クリアスクリーン

職員は、離席時に以下のいずれかによりパソコンの画面をロックし、クリアスクリーンを徹底する。

●スクリーンセーバー起動時間を 5 分以内に設定し、パスワードを設定する。
●スリープ起動時間を 5 分以内に設定し、解除時のパスワード保護を設定する。
●離席時に［Windows］＋［L］キーを押してコンピュータをロックする。
●退勤時又は使用しないときにはパソコンの電源を切る。

4.インターネットの利用

職員は、インターネットを利用する際には以下を遵守する。

4.1 ウェブ閲覧

情報セキュリティ委員会は、ウイルス等悪意のあるソフトウェアに感染するおそれがあると認められる有害ウェブサイトは社内周知して、職員の閲覧を制限する。職員は、業務でウェブ閲覧を行う場合は以下に留意・遵守する。

●公序良俗に反するサイトへのアクセスを禁止する。
●不審なサイトへのアクセス及び社用メールアドレス登録を禁止する。
●私用での Web サービス利用において社用メールアドレスの使用は禁止する。
●パスワードをブラウザに保存しない。
●業務上、個人情報(メールアドレス、氏名、所属等)を入力する場合は、通信の暗号化、接続先の実在性等を十分に確認したうえで行う。(マニュアル参照のこと)

4.2 オンラインサービス

職員は、インターネットで提供されているサービスを業務で利用する場合は、情報セキュリティ管理者に申請して許可を得る。利用する際には以下に留意・遵守する。

＜インターネットバンキング・電子決済＞

●インターネットバンキングを利用する際には、自分で設定したブックマークや銀行が提供する専用アプリケーションソフトを用いる。
●電子決済を利用する際には、SSL/TLS による通信暗号化を採用しているサイトを利用する。
●電子メールに記載されているリンクや、他のウェブサイト等に設置されているリンクは、偽サ

イトへの誘導である可能性があるためアクセスしない。

＜オンラインストレージ＞

●機密レベル 1 以上の情報資産は、アクセス制御対象情報システムに含まれるオンラインストレージに保存する。法人内で共有を行う場合、プロジェクト単位で定められた保管場所に保存する。ただし委託元や協働先の指定などのある場合はこの限りではない。

●情報資産に該当するデータについては、プロジェクトごとに定められたアカウントで保存・共有し、個人で保持しない。

4.3 SNS の個人利用

●法人の業務に関わる情報の書き込みを行ってはならない。ただし、業務上必要な SNS 上での情報拡散については上長であるプロジェクトマネージャーの承認のもと可とする。

●取引先従業者と SNS 上で私的に交流する場合、利益相反のないよう、双方の立場をわきまえ、社会人として良識の範囲内で交流する。

●SNS 用のアプリケーションが提供するセキュリティ設定を行い、アカウントの乗っ取りやなりすましに注意する。

●使用するパソコン、スマートフォン、タブレット上のデータ、写真、位置情報が、予期せず公開される可能性のあることに注意する。

4.4 電子メールの利用

職員は、業務で電子メールを利用する際には以下を実施する。

＜送受信＞

●電子メールの送受信に当たっては別途定める「メール送受信マニュアル」に則って業務を行う。

4.5 ウイルス感染の防止

標的型攻撃メール等によるウイルス感染を防止するため、以下の内容に複数合致する場合は十分に注意し、添付ファイルを開く、又はリンクを参照するなどしない。受信した場合は、上長及び IT ヘルプデスクに報告し、情報セキュリティ委員会は社内に注意を促す。

メールのテーマ	**⑥IDやパスワードなどの入力を要求するメール** ·メールボックスの容量オーバーの警告 銀行からの登録情報確認 ①知らない人からのメールだが、メール本文のURL や添付ファイルを開かざるを得ない内容 ·新聞社や出版社からの取材申込や講演依頼 ·就職活動に関する問い合わせや履歴書送付 ·法人の提供サービス、プログラムに関する問い合わせ、クレーム

	·アンケート調査 ②心当たりのないメールだが、興味をそそられる内容 ·議事録、演説原稿などの内部文書送付 ·VIP 訪問に関する情報 ③これまで届いたことがない公的機関からのお知らせ ·情報セキュリティに関する注意喚起 ·インフルエンザ等の感染症流行情報 ·災害情報 ④組織全体への案内 ·人事情報 ·新年度の事業方針 ·資料の再送、差替え ⑤心当たりのない、決裁や配送通知（英文の場合が多い） ·航空券の予約確認 ·荷物の配達通知
差出人のメール アドレス	①フリーメールアドレスから送信されている ②差出人のメールアドレスとメール本文の署名に記載されたメール アドレスが異なる
メールの本文	①日本語の言い回しが不自然である ②日本語では使用されない漢字（繁体字、簡体字）が使われている ③実在する名称を一部に含むURL が記載されている ④表示されているURL（アンカーテキスト）と実際のリンク先のURL が異なる（HTML メールの場合） ⑤署名の内容が誤っている ·組織名や電話番号が実在しない ·電話番号がFAX 番号として記載されている
添付ファイル	①ファイルが添付されている ②実行形式ファイル(exe/scr/cplなど)が添付されている ③ショートカットファイル(lnkなど)が添付されている ④アイコンが偽装されている ·実行形式ファイルなのに文書ファイルやフォルダーのアイコンと なっている ⑤ファイル拡張子が偽装されている ·二重拡張子となっている ·ファイル拡張子の前に大量の空白文字が挿入されている ·ファイル名にRLO4が使用されている

5.私有ＩＴ機器の利用

職員個人が所有するパソコン、タブレット、スマートフォン、携帯電話等のＩＴ機器を業務で利用する場合は、情報セキュリティ委員会またはその指定する者の許可を得なければならない。

5.1 利用開始時

利用を開始する前に利用する本人が以下を実行する。

●法人が指定するウイルス対策ソフトウェアをインストールし、定義ファイルを更新する。

●ハードディスク、電子媒体に対してウイルスチェックを行う。（マニュアル参照）

●業務に支障が出る可能性があるソフトウェアを削除する。

●法人で契約したサービス以外の Wi-Fi スポットの利用は禁止する。法人からモバイル Wi-Fi ルーターを貸与されている場合はそれを使用する。

5.2 利用期間中

利用期間中は、以下に該当する機能が利用するＩＴ機器や電子媒体にある場合には実行する。

●ウイルス対策ソフトウェアの定義ファイルを常に最新版に更新する。

●OS やアプリケーションソフトのアップデートが通知されたら速やかに実施する。

●社内 LAN へのリモート接続は禁止する。

5.2.1 社内での利用

許可された私有 IT 機器類を社内で利用する場合には以下を実行する。

●社内 LAN への接続を行う場合は情報セキュリティ委員会またはその指定する者の許可を得ること。

●充電を除き、社内のパソコンやクラウド環境・サーバーへの接続は禁止する。

5.3 利用終了時

利用を終了する際には、法人の指定するツールを使用してＩＴ機器業務で利用したデータを完全に消去し、復元できない状態にして情報セキュリティ委員会またはその指定する者の了解を得る。

6.標準ソフトウェアとアップデート方法について

業務に使用する標準のソフトウェアについては、別表「標準ソフトウェアとアップデート方法一覧」に定めるので適宜参照のこと。

8	ＩＴ基盤運用管理	改訂日	2022.4.1
適用範囲	サーバー・ネットワーク及び周辺機器		

1. 管理体制

法人はＩＴ基盤の運用に当たって採用する製品、サービスの情報セキュリティ対策を考慮し選択を行う。ＩＴ基盤の情報セキュリティ対策及び関連仕様は、情報セキュリティ委員会で審議のうえ、情報セキュリティ責任者が承認する。

2. ＩＴ基盤の情報セキュリティ対策

ＩＴ基盤の運用の際には以下の技術的情報セキュリティ対策を考慮すること。

2.1 サーバー機器の情報セキュリティ要件

ＩＴ基盤で利用するサーバー機器に求める情報セキュリティ要件は、情報セキュリティ委員会が決定する。新規にサーバー機器を導入する場合、情報セキュリティ委員会の許可を得て導入する。サーバー機器の情報セキュリティ要件は、「7.1 サーバー機器情報セキュリティ要件」を参照のこと。

2.2 サーバー機器に導入するソフトウェア

ＩＴ基盤で利用するサーバー機器に新規にソフトウェアを導入する場合は、情報セキュリティ委員会の許可を得て導入する。導入するソフトウェアについては、情報セキュリティ委員会が定める標準ソフトウェアの指定に従うこと。

2.3 ネットワーク機器の情報セキュリティ要件

ＩＴ基盤で利用するネットワーク機器に求める情報セキュリティ要件は、情報セキュリティ委員会が決定する。新規にネットワーク機器を導入する場合は、情報セキュリティ要件を満たす製品を選択し、「7.4 標準ネットワーク機器」として定める。情報セキュリティ委員会の許可を得て導入する。ネットワーク機器の情報セキュリティ要件は、「7.3 ネットワーク機器情報セキュリティ要件」を参照のこと。

3. ＩＴ基盤の運用

情報セキュリティ管理者は、ＩＴ基盤の運用を行う際には以下を実施すること。

●情報セキュリティ管理者は、機器の管理画面にログインするためのパスワードは初期状態のまま使わず、推測不可能なパスワードを設定して運用する。

●以下に従い、ゲートウェイにおける通信ログを取得及び保存する。

➢通信ログの保存期間は 3 年間とする。

➢ログファイルの保存状況については、情報セキュリティ管理者が定期的に確認を行う。

●情報セキュリティ管理者は、通信ログについて以下の確認を定期的に行う。

➢管理外のインターネット接続がないか

➢許可なく接続された機器や無線 LAN 機器はないか

➢不審な通信が行われていないか

●情報セキュリティ委員会は、必要に応じて業務に不要なウェブサイト閲覧を社内周知して制限する。

●遠隔診断ポートの利用は、保守サポートなど必要な場合のみに限定し、認証機能やコールバック機能等を備えるなど、適切なセキュリティ対策を施す。

4.クラウドサービスの導入

●ＩＴ基盤の一部としてクラウドサービス等の外部サービスを導入する場合は、情報セキュリティ委員会がサービスプロバイダの情報セキュリティ対策をあらかじめ評価したうえで選定する。新規クラウドサービス等の外部サービスを導入する場合は、情報セキュリティ委員会で審議のうえ、情報セキュリティ責任者の許可を得て導入する。サービスプロバイダの情報セキュリティ対策の評価基準は処理しようとする情報資産の重要度に照らして適切であることとする。

「7.5 クラウドサービス情報セキュリティ対策評価基準」参照のこと。

5.脅威や攻撃に関する情報の収集

情報セキュリティ委員会は、最新の脅威や攻撃に関する情報収集を行い、必要に応じて社内で共有する。

6.廃棄・返却・譲渡

情報セキュリティ管理者は、ＩＴ基盤で利用した機器を返却、廃棄、譲渡を行う場合は、内部記憶媒体の破壊又は専用ツールによりデータを完全に消去し、情報セキュリティ責任者の承認を得たうえ返却、廃棄、譲渡を行う。内部記憶媒体の破壊又はデータの完全消去を、外部に委託する場合は、破壊又はデータの完全消去を実行したことの証明書を取得する。

7.ＩＴ基盤標準

ＩＴ基盤で利用する機器及びソフトウェアの情報セキュリティ要件と、それに基づく法人の標準を以下とする。

7.1 サーバー機器情報セキュリティ要件

対象システム	セキュリティ要件
NAS サーバー	利用者認証機能

	ディスク暗号化機能

7.2ＩＴ基盤標準ソフトウェア

現状、ソフトウェアを搭載して運用する機器類はないため、必要のある場合、情報セキュリティ委員会が適宜指定する。

7.3 ネットワーク機器情報セキュリティ要件

対象システム	セキュリティ要件
ルーター	利用者認証機能
	MAC アドレス認証
	通信ログ取得
監視ツール	ユーザーアクセス監視

7.4 標準ネットワーク機器

種別	名称	開発・販売元	OS バージョン等
ルーター	WiFi	リコージャパン	Ver.11 以降

7.5 クラウドサービス情報セキュリティ対策評価基準

●サービスプロバイダが公表する情報セキュリティ又は個人情報保護への取組方針が、処理しようとする情報資産の重要度に照らして適切であること。

●サービス仕様に含まれる情報セキュリティ対策が、取り扱う情報資産の重要度に照らして適切であること。

●導入を検討するサービスが取扱い情報資産の性質に照らして、適切と思われる第三者による適合性評価制度の認証・認定を取得しているか。

評価時に参考とする適合性評価制度の例

・ISO/IEC 27001/27017/27018
・ISMS 適合性評価制度（ISMS 認証/ISMS クラウドセキュリティ認証）
・クラウド情報セキュリティ監査制度（CS マーク）
・プライバシーマーク制度（P マーク）
・PCI DSS（クレジットカード業界セキュリティ基準）
・ASP・SaaS の安全・信頼性に係る情報開示認定制度
・インターネット接続安全安心マーク
・FISC 安全対策基準（国内基準）
・SOC2/3（国際基準）

9	システム開発及び保守	改訂日	2022.4.1
適用範囲	当法人が独自に開発する情報システム		

1. 新規システム開発・改修

情報システムの開発・改修を行う際には、以下の工程を経て実施する。各工程の実施は、情報セキュリティ委員会で審議のうえ、情報セキュリティ責任者の承認を以て行う。各工程の業務実施担当者は、各工程の完了時に情報セキュリティ責任者に報告を行う。

①対象業務の範囲定義
②ハードウェア・ソフトウェア・ネットワーク機能検討
③必要なパフォーマンスの検討
④情報セキュリティ要件定義
⑤バックアップ/障害復旧要件定義
⑥情報システム運用要件定義
⑦運用体制
⑧移行計画立案

2. 脆弱性への対処

情報システムのソフトウェア開発を行う際には、当該情報システムの利用環境に応じて設計時に技術的な脆弱性を識別し、対策を講じる。脆弱性に対する対策の有効性は情報セキュリティ委員会で審議のうえ、情報セキュリティ責任者が承認する。

（参考）IPA　情報セキュリティ　脆弱性対策
https://www.ipa.go.jp/security/vuln/index.html

3. 情報システムの開発環境

情報システムの開発及び改修は、稼働中の運用環境に支障がないよう行う。新たに情報システムの開発を行った場合や、情報システムの改修を行った場合、当該情報システムの運用にあたっては、事前に必要な情報セキュリティ対策が講じられていることを確認し、情報セキュリティ委員会で審議のうえ、情報セキュリティ責任者がこれを承認する。

4. 情報システムの保守

情報システムの保守を、開発元又は外部の組織に委託することができない場合、以下に挙げる事項に留意し、情報システムに既知の脆弱性が存在しない状態で運用する。

●開発時に用いたソフトウェアに関する脆弱性が公表された場合には、速やかにその影響が

顕在化しないための対策を講じる。

●開発時に用いたソフトウェア及びハードウェアの製造者が提供するサポートが終了した場合、他のソフトウェアやハードウェアを用いた再構築ないしは当該情報システムの利用停止を検討し、情報セキュリティ委員会で審議のうえ、情報セキュリティ責任者がその承認を行う。

5.情報システムの変更

情報システムのハードウェア又はソフトウェアの変更を行う際には、以下の工程を経て実施する。各工程の完了時、情報セキュリティ委員会で審議のうえ、情報セキュリティ責任者はその承認を行う。

①現行システムの問題・課題の把握
②システム変更計画立案
③システム変更計画書に基づくシステム設計
④セキュリティ要求と設計の見直し
⑤移行計画立案（移行時、運用時の障害対応をあらかじめ検討する。）
⑥変更後の仕様書、操作手順書、運用手順書等の関連文書の作成

10	委託管理	改訂日	2022.4.1
適用範囲	情報資産を取り扱う業務の委託		

1. 委託先評価基準

情報セキュリティ部門責任者は、機密性レベル 1 以上の情報資産を取り扱う業務を、外部の組織に委託する場合、委託先の情報セキュリティ管理について、以下に掲げる委託先評価基準を適宜参照し評価を行う。

＜委託先評価基準＞

●情報セキュリティマネジメントシステム（ISMS）適合性評価制度の認証を取得している。
●個人情報保護マネジメントシステム（PMS）に適合し、プライバシーマーク付与を受けている。
●SECURITY ACTION 一つ星／二つ星に取り組んでいる。
●情報セキュリティ監査を定期的に実施している。
●情報セキュリティに関する方針を公開している。
●9-1「委託先情報セキュリティ対策状況確認リスト」に掲げる事項の実施状況

2. 委託先の選定

評価結果に基づき委託先を選定し、情報セキュリティ責任者の承認を得る。

3. 委託契約の締結

委託契約書には、下記に関する事項を明記する。

●当法人の法人外秘又は極秘の情報資産及び個人情報の守秘義務
●再委託についての事項
●事故時の責任分担についての事項
●委託業務終了時の当法人が提供した法人外秘又は極秘の情報資産及び個人情報の返却又は廃棄、消去についての事項
●情報セキュリティ対策の実施状況に関する監査の方法とその権限
●契約内容が遵守されない場合の措置
●事故発生時の報告方法

4. 委託先の評価

委託開始後には、10-1「委託先情報セキュリティ対策状況確認リスト」により、委託先における情報セキュリティ対策の実施状況について定期的に評価する機会を設ける。委託先における情報セキュリティ対策の実施に関して不備又は変更が認められた場合は、双方協議のうえ、対処を検討し、書面で合意する。

5.再委託

原則として再委託は認めない。但しやむを得ない場合であって、情報セキュリティ責任者が認める場合には以下に定める方法により行う。

事前の書面による報告

- 当法人の「1.委託先評価基準」「3.委託契約の締結」「4.委託先の評価」と同等の管理を再委託先に求めて、それを実施していることを確認できる書類
  再委託先が情報セキュリティに関する適合性評価制度の認証・認定を取得している場合にはその証書の写し

10-1　委託先情報セキュリティ対策状況確認リスト

注：このサンプルは、委託先の情報セキュリティ対策の実施状況を確認するためのものです。
必要な項目を加筆修正してご利用ください。

会社名：　　確認者：　　確認日：

区分	No	確認項目	実施状況（○、×）
社内体制	1	情報セキュリティ管理責任者を定めている	
	2	情報セキュリティ対策を定めた規程を整備している	
	3	情報セキュリティへの取り組み方針を職員や取引先に周知している	
	4	情報セキュリティ事故に対する対応手順を整備している	
	5	定期的に情報セキュリティに関する内部点検を実施している	
人的管理	6	情報セキュリティに関する教育を定期的に実施し、受講記録を作成している	
	7	職員と守秘義務契約を交わしている	
物理的管理	8	関係者以外の事務所への立ち入りを制限している	
	9	機密情報の保管について施錠管理をしている	
	10	機密情報を保管している領域に入ることができる人を制限し、入退出記録を取得している	
	11	入退出記録を定期的に確認している	
情報機器・媒体の取り扱い	12	機器・媒体の盗難防止措置を講じている	
	13	媒体の無断複製、不正持出しを防止する措置を講じている	
	14	媒体の移送、受け渡し時の保護措置を講じている	
	15	媒体の安全な消去、廃棄の手順を整備している	
技術的対策	16	業務で使用するサーバー・パソコンのウイルス対策を行っている	
	17	業務で使用するサーバー・パソコンは利用者認証機能を設定している	
	18	業務で使用するサーバー・パソコンに利用制限等を設け管理している	
再委託先管理	19	重要情報の授受を伴う委託先との契約書には、秘密保持条項を規定している	
	20	重要情報の授受を伴う委託先には自社と同等の情報セキュリティ対策を求めている	

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	改訂日	2022.4.1
適用範囲	情報資産及び保有する個人データに関わるインシデント		

1.情報セキュリティインシデントの区分

インシデントについては以下のとおり区分する。

区分	事件・事故の状況
漏えい・流出	法人外秘又は極秘情報資産の盗難、流出、紛失
改ざん・消失・破壊 サービス停止	情報資産の意図しない改ざん、消失、破壊 情報資産が必要なときに利用できない
ウイルス感染	悪意のあるソフトウェアに感染

2.1 漏えい・流出、改ざん・消失・破壊等インシデント発生時の対応

別途定める「危機管理マニュアル」に定める手順に従い、報告・対応を行うこととする。

2.2 ウイルス感染時の初期対応

職員は、業務に利用しているパソコン、サーバー又はスマートフォン、タブレットがウイルスに感染した場合には、ネットワークから切断のうえ、事業担当 PM 及び IT ヘルプデスクに連絡、指示を仰ぐこと。

2.3 届出及び相談

情報セキュリティ責任者は、インシデント対応後に以下の機関への届け出、報告又は相談を検討する。

＜届出・相談・報告先＞

【独立行政法人 情報処理推進機構セキュリティセンター(IPA/ISEC)】

- ウイルスの届出

  https://www.ipa.go.jp/security/outline/todokede-j.html

  TEL: 03-5978-7518

  E-mail : virus@ipa.go.jp

- 不正アクセスに関する届出

  E-mail : crack@ipa.go.jp

  FAX : 03-5978-7518

- 情報セキュリティ安心相談窓口

  https://www.ipa.go.jp/security/anshin/index.html

  TEL:03-5978-7509

  E-mail : anshin@ipa.go.jp

【個人情報保護委員会】

➢ 個人データの漏えい等の事案が発生した場合等の対応

①個人データ（特定個人情報に係るものを除く。）の漏えい、滅失又は毀損

②加工方法等情報（匿名加工情報の加工の方法に関する情報等）の漏えい

③上記①又は②のおそれ

漏えい等事案が発覚した場合は、速やかに下記 UR を参照して個人情報保護委員会等に対し、報告すること

https://www.ppc.go.jp/personalinfo/legal/leakAction/

TEL：03-6457-9685

個人情報保護委員会事務局　個人データ漏えい等報告窓口

➢ 特定個人情報の漏えい事案が発生した場合の対応

①番号法違反又は違反のおそれ

番号法違反又は違反のおそれを把握した場合は、速やかに下記 UR を参照して個人情報保護委員会等に対し、報告すること

https://www.ppc.go.jp/legal/rouei/

②重大事態に該当する事案又はそのおそれ

≪重大事態≫

- 情報提供ネットワークシステム等又は個人番号利用事務を処理するために使用する情報システムで管理される特定個人情報が漏えい等した事態
- 漏えい等した特定個人情報に係る本人の数が 100 人を超える事態
- 特定個人情報を電磁的方法により不特定多数の者が閲覧することができる状態となり、かつ閲覧された事態
- 職員等が不正の目的をもって、特定個人情報を利用し、又は提供した事態

重大事態が発覚した場合は、直ちに下記 UR を参照して個人情報保護委員会等に対し、報告すること

https://www.ppc.go.jp/legal/rouei/

個人情報保護委員会事務局　特定個人情報漏えい等報告窓口

TEL:03-6457-9680