情報セキュリティポリシー

目　次

1	組織的対策（基本方針）	2 ページ
	組織的対策	5 ページ
2	人的対策	7 ページ
3	情報資産管理	9 ページ
4	マイナンバー対応	12 ページ
5	アクセス制御及び認証	21 ページ
6	物理的対策	24 ページ
7	ＩＴ機器利用	26 ページ
8	ＩＴ基盤運用管理	34 ページ
9	システム開発及び保守	37 ページ
10	委託管理	39 ページ
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	41 ページ
12	社内体制図	46 ページ
13	委託契約書機密保持条項サンプル	47 ページ

（Ver.1.4）

1	組織的対策（基本方針）	改訂日	2018.10.01
適用範囲	当法人全体		

1. 情報セキュリティ基本方針

情報セキュリティ基本方針を以下のとおり定める。情報セキュリティ基本方針を当法人のホームページで公表する。

＜情報セキュリティ基本方針サンプル＞

昨今の高度情報化社会において情報資産が事故・災害・犯罪などの脅威にさらされる中、社会の信頼に応えるべく、当法人は情報資産を守るため、情報セキュリティ基本方針を定め、当法人の情報セキュリティに対する取り組みの指針といたします。

1. 法人内体制および情報セキュリティポリシーの整備

当法人は、セキュリティの維持及び改善のために必要な管理体制を整備し、必要な情報セキュリティ対策を法人内の正式な規則として定めます。

2. リーダーシップにおける責任および継続的改善

当法人の代表は、本方針の遵守により、当法人及び会員の情報資産が適切に管理されるよう主導します。

3. 法令、契約上の要求事項の遵守

当法人の職員は、事業活動で利用する情報資産に関連する法令、規制、規範及び会員の個人情報のセキュリティ要求事項を遵守します。

4. 職員の取組み

当法人の職員は、情報セキュリティの維持及び改善のために必要とされ知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

5. 違反及び事故への対応

当法人は、情報セキュリティに関わる法令、規制、規範及び会員の個人情報に関わる違反及び情報セキュリティ事故への対応のための体制を整備し、違反及び事故の影響を低減します。

平成 30 年 10 月 1 日

特定非営利活動法人ふまねっと

理事長　北澤　一利

2. 個人番号及び特定個人情報の適正な取扱いに関する基本方針

個人番号及び特定個人情報の適正な取扱いに関する基本方針を以下のとおり定める。個人番号及び特定個人情報の適正な取扱いに関する基本方針を当法人のホームページで公表する。

＜個人番号及び特定個人情報の適正な取扱いに関する基本方針サンプル＞

1.関係法令・ガイドライン等の遵守

当法人は、個人番号及び特定個人情報（以下「特定個人情報等」といいます。）の取り扱いに関し、「行政手続における特定の個人を識別するための番号の利用等に関する法律」（以下「マイナンバー法」といいます。）及び「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」、並びに「個人情報の保護に関する法律」（以下「個人情報保護法」といいます。）及び各省庁のガイドラインを遵守します。

2.利用目的

当法人は、提供を受けた特定個人情報等を、以下の目的で利用します。

(1) 当法人の職員等の特定個人情報等

【税務】

・源泉徴収票作成事務

・扶養控除等（異動）申告書、保険料控除申告書兼給与所得者の配偶者特別控除申告書作成事務

【社会保険】

・健康保険・厚生年金保険届出、申請・請求事務

・雇用保険・労災保険届出、申請・請求、証明書作成事務

(2) 当法人職員等の配偶者及び親族等の特定個人情報等

【税務】

・源泉徴収票作成事務

・扶養控除等（異動）申告書、保険料控除申告書兼給与所得者の配偶者特別控除申告書作成事務

【社会保険】

・健康保険・厚生年金保険届出事務

3.安全管理措置に関する事項

当法人は、特定個人情報等の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために、別途「情報セキュリティポリシー４　マイナンバー対応」を定め、これを遵守します。

4.委託の取り扱い

当法人は、特定個人情報等の取り扱いを第三者に委託することがあります。この場合、当法人は、マイナンバー法及び個人情報保護法に従って、委託先に対する必要かつ適切な監督を行います。

5.継続的改善

当法人は、特定個人情報等の取り扱いを継続的に改善するよう努めます。

6.特定個人情報等の開示

当法人は、本人又はその代理人から、当該特定個人情報等に係る保有個人データの開示の求めがあったときは、次の各号の場合を除き、遅滞なく回答します。

・本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
・当法人の業務の適正な実施に著しい支障を及ぼすおそれがある場合
・法令に違反することとなる場合

特定個人情報等の開示に関するお問合せ、および質問苦情等は下記までお願いいたします。

特定非営利活動法人ふまねっと　事務局
電話番号　011-807-4667
Mail info@1to3.jp

平成30年10月1日
特定非営利活動法人ふまねっと
理事長　北澤　一利

1	組織的対策	改訂日	2018.10.01
適用範囲	当法人全体		

1. 情報セキュリティのための組織

情報セキュリティ対策活動を推進するための組織として、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以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

情報セキュリティ委員会	
情報セキュリティ責任者	理事長
情報セキュリティ　部門責任者	事務局長
インシデント対応責任者	
個人情報　苦情対応責任者	
システム管理者	システム管理主任
教育責任者	
点検　責任者	総務主任
特定個人情報　事務取扱責任者	理事長
特定個人情報　事務取扱担当者	総務主任

2. 情報セキュリティ取組みの点検

点検責任者は、情報セキュリティポリシーの実施状況について、8 月に点検を行い、点検結果を情報セキュリティ委員会に報告する。情報セキュリティ委員会は、報告に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。

- ➢情報セキュリティポリシーが有効に実施されていない場合、その原因の特定と改善
- ➢情報セキュリティポリシー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、情報セキュリティポリシーの改訂
- ➢情報セキュリティポリシーに定められたルールが、関連法令や取関連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、情報セキュリティポリシーの改訂

3. 情報セキュリティに関する情報共有

情報セキュリティ責任者は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し、委員会で共有する。

【専門機関】

- ➢独立行政法人情報処理推進機構（略称：IPA）

［情報セキュリティ］

https://www.ipa.go.jp/security/

[ここからセキュリティ]

https://www.ipa.go.jp/security/kokokara/

➢JVN（Japan Vulnerability Notes）

https://jvn.jp/index.html

➢一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）

https://www.jpcert.or.jp/

➢個人情報保護委員会

http://www.ppc.go.jp/

2	人的対策	改訂日	2018.10.01
適用範囲	全職員（役員、正職員、契約職員、パート･アルバイトを含む）		

1. 雇用条件

職員を雇用する際には秘密保持契約を締結する。

2. 代表及び職員の責務

代表及び職員は、以下を遵守する。

●代表及び職員は、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。

●代表及び職員は、当法人の情報セキュリティ方針及び関連規程を遵守する。違反時には就業規則第 39 条に従い懲戒処分の対象とする。

※当法人が営業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. 雇用の終了

●代表及び職員は、在職中に交付された業務に関連する資料、個人情報、関係機関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退職時に返還する。

●代表及び職員は、在職中に知り得た当法人の営業秘密もしくは業務遂行上知り得た技術的機密を利用して、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年度単位で立案する。

対象者：全職員、パート・アルバイト

テーマ：以下は必須とする。

- ➢情報セキュリティポリシーの説明（入社時、就業時）
- ➢最新の脅威に対する注意喚起（随時）
- ➢関連法令の理解（関連法令の施行時）
- ➢特定個人情報の取扱いに関する留意事項

5. 人材育成

教育責任者は、以下に挙げる推奨資格の取得による職員の情報セキュリティに対する意識向上を年度単位で計画する。計画には関連テキストの配付、公開セミナーへの派遣を含むこととする。

＜情報セキュリティに関わる推奨資格＞

IPA　情報処理技術者試験・情報処理安全確保支援士試験

- 情報セキュリティマネジメント試験
- システム監査技術者試験
- 情報処理安全確保支援士試験

3	情報資産管理	改訂日	2018.10.01
適用範囲	当法人事業に必要で価値がある情報及び個人情報		

1. 情報資産の管理

1.1 情報資産の特定と重要度の評価

当法人事業に必要で価値がある情報及び個人情報（以下「情報資産」という）を特定し、「情報資産管理台帳」に記載する。情報資産の機密性における重要度は、以下の基準に従って評価する。

機密性 2：極秘	●法律で安全管理措置が義務付けられている ●守秘義務の対象として指定されている ●漏えいすると会員や関連機関に大きな影響がある
機密性 1：社外秘	●漏えいすると事業に大きな影響がある
機密性 0：公開	漏えいしても事業に影響はない

1.2 情報資産の分類と表示

情報資産の重要度は以下の方法で表示する。

●電子データ：保存先サーバーのフォルダー名に重要度を明示

●書類：保管先キャビネット、ファイル、バインダーに重要度を明示

表示が困難な場合は、「情報資産管理台帳」に機密性評価値を明記する。

1.3 情報資産の管理責任者

情報資産の管理責任者は、理事長とする。

1.4 情報資産の利用者

情報資産の利用を許可する範囲は、「情報資産管理台帳」の利用者範囲欄に担当者名を記載する。

2. 情報資産の社外持ち出し

情報資産を社外に持ち出す場合には、以下を実施する。

●社外秘の場合は事務局長の許可を得る。

●極秘の場合は理事長の許可を得る。

●ノートパソコンのハードディスクに保存して持ち出す場合は、データ・フォルダーを暗号化する。

●スマートフォン、タブレットに保存して持ち出す場合は、セキュリティロックを設定する。

●USB メモリ、HDD 等の電子媒体に保存して持ち出す場合は、不要データは全て完全消去専用

ツールで消去し、持ち出すデータを暗号化する。

●USB メモリ等の小型電子媒体は、紛失しないよう大きなタグを付ける。

●屋外でネットワークへ接続して社外秘又は極秘の情報資産を送受信する場合は、暗号化通信で行う。

●携行中は常に監視可能な距離を保つ。

3.媒体の処分

3.1 媒体の廃棄

社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・焼却のいずれかの方法
USB メモリ・HDD・CD・DVD	破壊・細断・完全消去のいずれかの方法

3.2 媒体の再利用

社外秘又は極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	完全消去後再利用 ※OS の削除機能による削除・フォーマットは不可
CD-R・DVD-R	再利用不可

4.バックアップ

4.1 バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
Network HDD	共有フォルダ	定期的バックアップ	HDD
会計システム	アプリケーションデータ	アプリケーションバックアップ機能	NAS サーバー
会員管理システム	アプリケーションデータ	同期ツール	NAS サーバー
Web サーバー	ホームページ	同期ツール	レンタルサーバー

4.2 バックアップ媒体の取扱い

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＞

●Network HDD 鍵付きの部屋に設置し、職員が不在の際は施錠する。

●NAS サーバー：鍵付きの部屋に設置し、職員が不在の際は施錠する。

＜廃棄・再利用＞

●「3.媒体の処分」に従う

4.3 レンタルサーバー、クラウドサービスを利用したバックアップ
レンタルサーバー、クラウドサービスを利用し、外部のサーバーにバックアップを保存する場合は、以下のサービス要件を確認し、情報セキュリティ責任者の許可を得て導入する。

＜サービス要件＞
●サービス提供者のサービス利用約款、情報セキュリティ方針が、当法人の情報セキュリティポリシーに適合している。
●当法人事業所がある地域で発生する震災、水害等の影響を受けない地域の施設であること。

4	マイナンバー対応	改訂日	2018.10.01
適用範囲	特定個人情報（マイナンバーを内容に含む個人情報）		

1. 総則

1.1 目的

本規程は、個人番号及び特定個人情報（以下「特定個人情報等」という。）の適正な取扱いの確保に関し必要な事項を定めることにより、当法人の事業の適正かつ円滑な運営を図りつつ、個人の権利利益を保護することを目的とする。

1.2 定義

本項における用語の定義は、次に定めるところによる。

個人情報：

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述又は個人別に付された番号、記号その他の符号により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別できることとなるものを含む。）をいう。

個人番号：

行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「マイナンバー法」という。）第 2 条 5 項が定める住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。

特定個人情報：

個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報をいう。

個人情報データベース等：

個人情報を含む情報の集合物であって、特定の個人情報について電子計算機を用いて検索することができるように体系的に構成したもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして「個人情報の保護に関する法律施行令」（平成 15 年政令第 507 号。以下「個人情報保護法施行令」という。）で定めるものをいう。

個人情報ファイル：

個人情報を含む情報の集合物であって、特定の個人情報について電子計算機を用いて検索することができるように体系的に構成したもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして「個人情報の保護に関する法律施行令」で定めるものをいう。

特定個人情報ファイル：

個人番号をその内容に含む個人情報ファイルをいう。

個人データ：

個人情報データベース等を構成する個人情報をいう。

保有個人データ:
個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして個人情報保護法施行令で定めるものをいう。
個人番号関係事務:
マイナンバー法第 9 条第 3 項の規定により個人番号利用事務（行政機関、地方公共団体、独立行政法人等その他の行政事務を処理する者が同条第 1 項又は第 2 項の規定によりその保有する特定個人情報ファイルにおいて個人情報を効率的に検索し、及び管理するために必要な限度で個人番号を利用して処理する事務）に関して行われる他人の個人番号を必要な限度で利用して行う事務をいう。
個人情報取扱事業者:
個人情報データベース等を事業の用に供している者（国の機関、地方公共団体、独立行政法人等及び地方独立行政法人を除く。）をいう。
本人:
個人番号によって識別され、又は識別され得る特定の個人をいう。
職員:
当法人の組織内にあって直接間接に当法人の指揮監督を受けて当法人の業務に従事している者をいう。具体的には、職員のほか、理事、監事を含む。
1.3 当法人の責務
マイナンバー法その他の個人情報保護に関する法令及びガイドライン等を遵守するとともに、実施するあらゆる事業を通じて特定個人情報等の保護に努めるものとする。

2. 特定個人情報等の取り扱い
2.1 利用目的の特定
●特定個人情報等を利用できる事務の範囲を、社会保障、税及び災害対策に関する特定の事務に限定するものとする。
●利用に当たっては前項で定めた事務の範囲の中から、具体的な利用目的を特定した上で、利用するものとする。
●特定した利用目的を超えて利用する必要が生じた場合には、当初の利用目的と相当の関連性を有すると合理的に認められる範囲内で利用目的を変更して、本人に通知を行い、変更後の利用目的の範囲内で利用するものとする。

2.2 取得に際しての利用目的の通知等
●特定個人情報等を取得した場合は、あらかじめその利用目的を通知又は公表している場合を除き、速やかに、その利用目的を本人に通知し、又は公表するものとする。

●前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式等で作られる記録を含む。）に記載された当該本人の特定個人情報等を取得する場合その他本人から直接書面に記載された当該本人の特定個人情報等を取得する場合は、あらかじめ、本人に対し、その利用目的を明示するものとする。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

●前 2 項の規定は、次に掲げる場合については、適用しない。

⑴利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

⑵利用目的を本人に通知し、又は公表することにより当法人の権利又は正当な利益を害するおそれがある場合

⑶国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき

⑷取得の状況からみて利用目的が明らかであると認められる場合

2.3 取得の制限

●特定個人情報等を取得するときは、適法かつ適正な方法で行うものとする。

●マイナンバー法第 19 条各号のいずれかに該当する場合を除き、他人の特定個人情報等を収集しないものとする。

2.4 個人番号の提供の求めの制限

マイナンバー法第 19 条各号に該当して特定個人情報の提供を受けることができる場合を除くほか、他人に対し、個人番号の提供を求めないものとする。

2.5 本人確認

本人又はその代理人から個人番号の提供を受けるときは、マイナンバー法第 16 条の規定に従い、本人確認を行うものとする。

2.6 利用目的外の利用の制限

●「2.1 利用目的の特定」の規定により特定された利用目的の達成に必要な範囲を超えて、特定個人情報等を取り扱わないものとする。

●合併その他の事由により他の法人等から事業を継承することに伴って特定個人情報等を取得した場合は、継承前における当該特定個人情報等の利用目的の達成に必要な範囲を超えて、当該特定個人情報等を取り扱わないものとする。

●前 2 項の規定にかかわらず、次の各号のいずれかに該当する場合には、「2.1 利用目的の特定」の規定により特定された利用目的の範囲を超えて特定個人情報等を取り扱うことがで

きるものとする。

(1)マイナンバー法第 9 条第 4 項の規定に基づく場合

(2)人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意があり、又は本人の同意を得ることが困難であるとき

2.7 特定個人情報ファイルの作成の制限

マイナンバー法第 19 条 11 号から 14 号までのいずれかに該当して特定個人情報を提供し、又はその提供を受けることができる場合を除き、個人番号関係事務を処理するために必要な範囲を超えて特定個人情報ファイルを作成しないものとする。

2.8 特定個人情報等の保管

マイナンバー法第 19 条各号に該当する場合を除くほか、特定個人情報等を保管しないものとする。

2.9 データ内容の正確性の確保

「2.1 利用目的の特定」により特定された利用目的の達成に必要な範囲内において、特定個人情報等を正確かつ最新の内容に保つよう努めるものとする。

2.10 特定個人情報等の提供

マイナンバー法第 19 条各号に該当する場合を除くほか、特定個人情報等を提供しないものとする。

2.11 特定個人情報等の削除・廃棄

個人番号関係事務を処理する必要がなくなった場合で、かつ、所管法令において定められている保存期間を経過した場合には、個人番号をできるだけ速やかに廃棄又は削除するものとする。ただし、その個人番号部分を復元できない程度にマスキング又は削除した場合には、保管を継続することができるものとする。

2.12 特定個人情報等を誤って収集した場合の措置

●従業者は、誤って特定個人情報等の提供を受けた場合、自ら当該特定個人情報等を削除又は廃棄してはならず、速やかに事務局長、「3.1 事務取扱担当者・責任者」に定める事務取扱責任者に報告しなければならない。

●前項の報告を受けた際、「5.3.4 個人番号の削除、機器及び電子媒体等の廃棄」に従って、当該特定個人情報等をできるだけ速やかに削除又は廃棄したうえで、その記録を保存するものとする。

2.13 安全管理措置

特定個人情報等の取り扱いに関し、「4.委託先の監督」及び「5.安全管理措置」に定める安全管理措置を講じるものとする。

3. 組織及び体制

3.1 事務取扱担当者・責任者

●別途定めるとおり、特定個人情報等を取り扱う事務の範囲を明確化し、明確化した事務において取り扱う特定個人情報等の範囲を明確にしたうえで、当該事務に従事する職員（以下「事務取扱担当者」という。）を明確にするものとする。

●別途定めるとおり、前項により定められた各事務における事務取扱責任者を明確にするものとする。

●事務取扱責任者は、次に掲げる業務を所管する。

(1)特定個人情報等の利用申請の承認及び記録等の管理

(2)特定個人情報等を取り扱う保管媒体の設置場所の指定及び変更の管理

(3)特定個人情報等の管理区分及び権限についての設定及び変更の管理

(4)特定個人情報等の取扱状況の把握

(5)委託先における特定個人情報等の取扱状況等の監督

(6)特定個人情報等の安全管理に関する教育・研修の実施

(7)特定個人情報等管理責任者に対する報告

(8)特定個人情報等の安全管理に関する規程の承認及び周知

(9)事務取扱責任者からの報告徴収及び助言・指導

(10)特定個人情報等の適正な取扱いに関する事務取扱担当者に対する教育・研修の企画

(11)その他特定個人情報等の安全管理に関する事項

3.2 苦情対応

●特定個人情報等の取扱いに関する苦情（以下「苦情」という。）の対応について必要な体制整備を行い、苦情があったときは、適切かつ迅速な処理に努めるものとする。

●苦情対応の責任者は、事務局長とする。

3.3 職員の義務

●当法人の従業者又は職員であった者は、業務上知り得た特定個人情報等の内容をみだりに他人に知らせたり、不当な目的に使用したりしてはならない。

●特定個人情報等の漏えい、滅失もしくは毀損の発生又は兆候を把握した職員は、その旨を事務取扱責任者に報告するものとする。

●本規程に違反している事実又は兆候を把握した従業者は、その旨を事務取扱責任者に報告するものとする。

●事務取扱責任者は、前3項による報告の内容を調査し、本規程に違反する事実が判明した場合には遅滞なく理事長に報告するとともに、関係部門に適切な措置をとるよう指示するものとする。

4.委託の取扱い

4.1 委託

特定個人情報等の取扱いの全部又は一部を当法人以外の者に委託するときは、委託先において、マイナンバー法に基づき当法人が果たすべき安全管理措置と同等の措置が講じられるか否かについてあらかじめ確認したうえで、原則として委託契約において、特定個人情報等の安全管理について委託先が講ずべき措置を明らかにし、委託先における特定個人情報の取扱状況を把握するものとする。

4.2 再委託

委託先が特定個人情報等の取扱いの全部又は一部を再委託する場合には、当法人の許諾を得るものとする。また、再委託が行われた場合、当法人は、委託先が再委託先に対して必要かつ適切な監督を行っているかについて監督するものとする。

5.安全管理措置

特定個人情報等の漏えい、滅失又は毀損の防止その他の特定個人情報等の安全管理のために、以下に定める措置を講ずるものとする。

5.1 組織的安全管理措置

特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じる。

5.1.1 組織体制の整備

安全管理措置を講ずるために、「3. 組織及び体制」に従い、組織体制を整備する。

5.1.2 取扱規程等に基づく運用

「情報資産管理台帳」に、以下を登録する。

情報資産管理台帳の項目	登録内容
情報資産名称	特定個人情報ファイルの種類、名称
備考	対象者及び個人情報の項目 明示・公表等を行った利用目的 削除・廃棄状況
利用者範囲	アクセス権を有する者
媒体・保存先	保管場所・保管方法
保存期限	保存期間

なお、「情報資産管理台帳」には個人番号は記載しない。

5.1.3 取扱状況を確認する手段の整備

本規程に基づく運用状況を確認するため、以下の項目をシステムログ又は利用実績として記録する。

・特定個人情報ファイルの利用・出力状況の記録
・書類・媒体等の持出しの記録
・特定個人情報ファイルの削除・廃棄記録
・削除・廃棄を委託した場合、これを証明する記録等
・特定個人情報ファイルを情報システムで取り扱う場合、事務取扱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）の記録

5.1.4 情報漏えい等事案に対応する体制の整備

情報漏えい等の事案の発生又は兆候を把握した場合には、事務取扱責任者は「情報セキュリティポリシー」に定める安全管理措置に従って対応を行う。

5.1.5 取扱状況の把握及び安全管理措置の見直し

特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組むため、事務取扱責任者が、毎年 8 月、取扱状況を点検し、安全管理措置を見直す。

5.2 人的安全管理措置

特定個人情報等の適正な取扱いのために、「情報セキュリティポリシー２　人的対策」に従い人的安全管理措置を講じる。

5.2.1 従業者の監督・教育

特定個人情報等の安全管理のために、職員に対する必要かつ適切な監督・教育を行うものとする。

5.3 物理的安全管理措置

特定個人情報等の適正な取扱いのために、「情報セキュリティポリシー６　物理的対策」の物理的安全管理措置を講じる。

5.3.1 特定個人情報等を取り扱う領域の管理

特定個人情報ファイルを取り扱う情報システムを管理するセキュリティ領域（以下「レベル〇領域」という。）及び特定個人情報等を取り扱う事務を実施するセキュリティ領域（以下「レベル〇領域」という。）を明確にし、「情報セキュリティポリシー６　物理的対策」に定める安全管理措置を講ずる。

5.3.2 ＩＴ機器及び電子媒体等の盗難等の防止

管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、「情報セキュリティポリシー７　ＩＴ機器利用」に定める安全管理措置を講ずる。

5.3.3 電子媒体等を持ち出す場合の漏えい等の防止

特定個人情報等が記録された電子媒体又は書類等を社外に持ち出す場合、「情報セキュリティポリシー７　ＩＴ機器利用」に定める安全管理措置を講じる。

5.3.4 個人番号の削除、機器及び電子媒体等の廃棄

個人番号を削除又は廃棄する際には、「情報セキュリティポリシー７　ＩＴ機器利用」に定める安全管理措置に従って、復元できない手段で削除又は廃棄する。

5.4 技術的安全管理措置

特定個人情報等の適正な取扱いのために、以下の技術的安全管理措置を講じる。

5.4.1 アクセス制御

事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。

5.4.2 アクセス者の識別と認証

特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証するものとする。

5.4.3 外部の不正アクセス等の防止

情報システムを外部からの不正アクセス又は不正ソフトウェアから保護するため、「情報セキュリティポリシー７.ＩＴ機器利用」「情報セキュリティポリシー８　ＩＴ基盤運用管理」に定める安全管理措置を講じる。

5.4.4 情報漏えい等の防止

特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するため、「情報セキュリティポリシー７　ＩＴ機器利用」に定める安全管理措置を講じる。

6.特定個人情報等の開示、訂正等、利用停止等

6.1 特定個人情報等の開示等

本人から、当該本人が識別される特定個人情報等に係る保有個人データについて、書面又は口頭により、その開示（当該本人が識別される特定個人情報等に係る保有個人データを保有していないときにその旨を知らせることを含む。以下同じ。）の申出があったときは、身分証明書等により本人であることを確認のうえ、開示をするものとする。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。

(1)本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

(2)当法人の事業の適正な実施に著しい支障を及ぼすおそれがある場合

(3)他の法令に違反することとなる場合

開示は、書面により行うものとする。ただし、開示の申出をした者の同意があるときは、書面以外の方法により開示をすることができる。

特定個人情報等に係る保有個人データの開示又は不開示の決定の通知は、本人に対し、遅滞な

く行うものとする。

6.2 特定個人情報等の訂正等

●本人から、当該本人が識別される特定個人情報等に係る保有個人データの内容が事実でないという理由によって当該特定個人情報等に係る保有個人データの内容の訂正、追加又は削除（以下「訂正等」という。）を求められた場合には、その内容の訂正等に関して他の法令の規定により特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該特定個人情報等に係る保有個人データの内容の訂正等を行うものとする。

●前項の規定に基づき求められた特定個人情報等に係る保有個人データの内容の訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨（訂正等を行ったときは、その内容を含む。）を通知するものとする。

●前項の通知を受けた者から、再度申出があったときは、前項と同様の処理を行うものとする。

●前第 2 項の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めるものとする。

6.3 特定個人情報等の利用停止等

●本人から、当該本人が識別される特定個人情報等に係る保有個人データが「2.6 利用目的外の利用の制限」の規定に違反して取り扱われているという理由又は「2.3 取得の制限」の規定に違反して取得されたものであるという理由によって、当該特定個人情報等に係る保有個人データの利用の停止又は消去（以下「利用停止等」という。）を求められた場合、又は「2.10 特定個人情報等の提供」の規定に違反して第三者に提供されているという理由によって、当該特定個人情報等に係る保有個人データの第三者への提供の停止（以下「第三者提供の停止」という。）を求められた場合で、その求めに理由があることが判明したときは、遅滞なく、当該特定個人情報等に係る保有個人データの利用停止等又は第三者提供の停止を行うものとする。ただし、当該特定個人情報等に係る保有個人データの利用停止等又は第三者提供の停止に多額の費用を要する場合その他の利用停止等又は第三者提供の停止を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

●前項の規定に基づき求められた特定個人情報等に係る保有個人データについて、利用停止等を行ったときもしくは利用停止等を行わない旨の決定をしたとき、又は第三者提供の停止を行ったときもしくは第三者提供の停止を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知するものとする。

●前項第 3 項及び第 4 項は本項に準用する。

5	アクセス制御及び認証	改訂日	2018.10.01
適用範囲	情報資産の利用者及び情報処理施設		

1. アクセス制御方針

社外秘又は極秘の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「9.1 アクセス制御対象情報システム及びアクセス制御方法」に記載する。

●「情報資産管理台帳」の利用者範囲に基づき、利用者の業務・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、複数名に分散してアクセス権を付与する。

2. 利用者の認証

社外秘又は極秘の情報資産を扱う社内情報システムは、以下の方針に基づいて利用者の認証を行う。認証方法等は「9.2 利用者認証方法」を参照のこと。

●利用者の認証に用いるアカウントは、利用者 1 名につき 1 つを発行する。

●複数の利用者が共有するアカウントの発行を禁止する。

3. 利用者アカウントの登録

利用者の認証に用いるアカウントは、理事長又は情報セキュリティ責任者の承認に基づき登録する。アカウント名の設定条件は「9.3 利用者アカウント・パスワードの条件」を参照のこと。

4. 利用者アカウントの管理

利用者の認証に用いるアカウントが不要になった場合、システム管理者は、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

利用者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、「9.3 利用者アカウント・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利用者アカウントの発行

当法人の職員以外の者にアカウントを発行する場合は、理事長の承認を得たうえで、秘密保持

契約を締結する。

7.機器の識別による認証

社外秘又は極秘の情報資産を扱う情報システムに、ネットワーク接続によりアクセスする際の認証方式として、機器の識別による認証を用いる。認証方法等は「9.4 機器の認証方法」を参照のこと。

8.端末のタイムアウト機能

社外秘又は極秘の情報資産を扱う情報システムの端末もしくは情報機器を、アカウントを付与していない者が接触可能な場所に設置する場合は、接続時間制限やタイムアウト等機能を利用する。

9.標準設定等

9.1 アクセス制御対象情報システム及びアクセス制御方法

情報システム・サービス	アクセス制御方法
Network HDD	暗号化
会員管理システム	アプリケーションのユーザー認証
メールサーバー（ホスティングサービス）	ホスティングサービスのユーザー認証
Web サーバー（ホスティングサービス）	ホスティングサービスのユーザー認証

9.2 利用者認証方法

情報システム	利用者認証方法
Network HDD	ログオン認証：アカウント名・パスワード
会員管理システム	アプリケーションのユーザー認証：ID・パスワード

9.3 利用者アカウント・パスワードの条件

	特権アカウント	一般アカウント
アカウント名	●推奨：推測困難であるもの ＜禁止アカウント名＞ ●1 つの特権アカウント名を 2 名以上で共用しない ●Guest 用アカウントは無効化する	●職員番号 ●職員コード
パスワード	＜パスワードに使う文字＞ ●12 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	＜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 ●辞書に含まれる単純な語を使わない ＜パスワードの管理＞ ●システムにパスワードポリシー設定機能がある場合は本項の条件を設定する ●過去1年間に使用したパスワードと同一パスワードを使用しない ●ロックアウトのしきい値は3回、時間は6時間に設定する	●アルファベット大文字･小文字、数字、記号の全てを含む ●辞書に含まれる単純な語を使わない ＜パスワードの管理＞ ●システムにパスワードポリシー設定機能がある場合は本項の条件を設定する ●過去1年間に使用したパスワードと同一パスワードを使用しない ●ロックアウトのしきい値は5回、時間は1時間に設定する

9.4 機器の認証方法

MAC アドレス	受信側のルーターで設定
IP アドレス	受信側のルーターもしくはサーバー
ドメイン名	受信側のルーターもしくはサーバー

6	物理的対策	改訂日	2018.10.01
適用範囲	情報処理設備が設置される領域		

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社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	講習会会場
利用者	職員、社外関係者、部外者が立ち入り可
施錠	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
制限事項	未使用時に社外秘又は極秘の情報資産の放置禁止
部外者管理	職員の許可を受けて入室可能
管理記録	ー
侵入検知	ー
来客用名札	着用不要
火災対策	火災検知器、消火器設置

レベル 2 領域	執務室・書庫
利用者	職員以外の入室は職員の許可又はエスコートが必要
施錠	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、 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
部外者管理	職員の許可を受けて入室可能
管理記録	入退室を所定様式に記録
侵入検知	センサーによる警備会社通報
来客用名札	要着用
火災対策	火災検知器、消火器設置

レベル 3 領域	サーバールーム
利用者	予め登録された者
施錠	常時施錠、鍵の管理責任者

設置可能情報機器	サーバー、ルーター等のネットワーク機器
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止 スマートフォン、USB メモリ、HDD、CD-R、デジタルカメラその他の情報記憶媒体の無断持込み禁止
部外者管理	保守・点検時等に登録者のエスコート付で入室可能
管理記録	入退室を所定様式に記録
侵入検知	センサーによる警備会社通報
来客用名札	要着用
火災対策	火災検知器、消火器設置

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。

●サーバーは鍵付きの部屋に設置し、職員が不在の際は施錠する。

●LAN ケーブルは回線盗聴防止のため床下配線とする。

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宛先を複数回確認する。

●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、情報セキュリティ部門責任者の許可を得ること。

●外線受話時の際に相手が不審な場合は、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。

＜本社＞

●郵便物：郵便受（事務所建物内）/書留便の場合は総務主任

●宅配便：事務所 1 階

7	Ｉ Ｔ機器利用	改訂日	2018.10.01
適用範囲	業務で利用する情報処理設備･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、当法人の標準ソフトウェアを導入する。当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、システム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「6.1 標準ソフトウェア」を参照のこと。

1.2 ソフトウェアの利用制限

システム管理者は、利用者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利用しない。

＜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）。

●不審なベンダー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。

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「6.2 ソフトウェアのアップデート方法」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。

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「6.3 ウイルス対策ソフトウェアの定義ファイルの更新方法」を参照のこと。

1.4.3 社外機器の LAN 接続

当法人が管理するパソコン及びサーバー以外の機器を社内 LAN に接続することを禁止する。業務上必要な場合は、システム管理者の許可を得たうえで、当該機器にインストールされているウイルス対策ソフトの定義ファイルを最新版に更新し、当該機器のフルスキャンを実行し、ウイルスが検知されないことを確認してから接続する。

1.5 ウイルス対策の啓発

システム管理者は、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機器の利用

職員は、業務に利用するパソコン・タブレット・スマートフォンには、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行する。

●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。

●屋外で利用する場合は、他者が画面を盗み見可能な環境で利用しない。

●退社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、社外秘又は極秘の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の扱いについて、以下のように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。

●離席時に書類を伏せる、引き出しに入れる等する。

●退社時又は使用しないときには机の引き出しに保管し、施錠する。

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。

●ログオフ状態ではシステム操作画面は非表示に設定する。退社時又は使用しないときにはパソコンの電源を切る。

●スマートフォン・タブレットを外出先で利用する場合は、他者が盗み見できる環境で利用しない。

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

システム管理者は、ウイルス等の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/ウェブフィルタリングソフトを使用して、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注意する。

●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。

●パスワードをブラウザに保存しない。業務で特定のウェブサービスを利用する場合で、パスワードをブラウザに保存する必要があるときはシステム管理者の許可を得る。

●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。

●信頼できるサイトから署名付きのモバイルコードをダウンロードする場合を除き、モバイルコード(クライアントパソコン側で動作するプログラム)を実行しない。

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、システム管理者の許可を得る。利用する際には以下に注意する。

＜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＞

●社外秘又は極秘の情報資産を保存する場合は、システム管理者の許可を得る。

●メールアドレスの登録が必要な場合は社用メールアドレスを登録する。

●セキュリティポリシーを公表していないサービスの利用は禁止する。

●不審なベンダーが提供しているサービスの利用を禁止する。

4.3ＳＮＳの利用

●当法人の業務に関わる情報の書き込みは行わない。

●関連機関従業者とＳＮＳ上で私的に交流する場合、双方の立場をわきまえ、社会人として良識の範囲で交流する。

●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。

＜誤送信防止＞

●電子メールソフトの即時送信機能を停止する。

＜メールアドレス漏えい防止＞

●同報メール（外部の多数相手に同時に送信するとき）を送信する場合は、宛先（TO）に自分自身のアドレスを入力し、BCC で複数相手のアドレスを指定する。

※CC 又は宛先（TO）に複数アドレスを指定すると、送信相手に複数全員のアドレスが通知され、個人情報の漏えいになります。

＜傍受による漏えい防止＞

●社外秘又は極秘の情報資産を送信する場合は、メール本文ではなく添付ファイルに記載し、ファイルを暗号化して送信する。

＜添付ファイル暗号化の方法＞

パスワード保護の設定又はパスワード付きの ZIP ファイルにする。/パスワードは先方とあらかじめ決めておくか電話で知らせるなど、パスワードが傍受されないよう配慮する。

＜クラウド型メールの利用＞

●業務でクラウド型メールを利用する場合は、システム管理者の許可を得る。

●システム管理者から許可されたパソコン以外で、メールサーバーからのメールの取り出し及びエクスポートを禁止する。

＜禁止事項＞

●業務に支障をきたすおそれがある使用。

●私用電子メールサーバーへの接続。

●私用メールアドレスへの転送。

●受信メールの HTML 表示（テキスト形式に変換して表示）。

●HTML 形式メールの中に含まれる不正なコードを実行しないよう以下を設定する。

●プレビューウィンドウを無効化する。

●モバイルコード実行を無効に設定する。

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、3 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、システム管理者に報告し、システム管理者は社内に注意を促す。

メールのテーマ	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 ·製品やサービス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 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
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・電子媒体の利用

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機器及びUSBメモリ、HDD、CD等の電子媒体を業務で利用する場合は、システム管理者の許可を得る。

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。

●システム管理者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。

●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。

●当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。

5.2 利用期間中

利用期間中は、利用するＩＴ機器や電子媒体に以下に該当する機能が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へのリモート接続する場合はシステム管理者の許可を得る。

●社外から社内LANにリモートで接続する場合は以下を遵守する。

●システム管理者の許可を受け指定された方法で接続する。

●画面の盗み見、不正操作等を防ぐよう、適切な環境で行う。

●端末機器から離れる場合は、端末機器を停止するか他者が利用できないようにする。

●リモート接続で利用する端末機器を紛失した場合は、直ちにシステム管理者に連絡し指示に従う。

●社用メールアドレスで受信したメールを職員個人のアドレスに転送することを禁止する。

●社内で利用したデータを職員個人のアドレスに送信することを禁止する。

●社外秘又は極秘の情報資産の保存を禁止する。

●以下のアプリケーションソフトのインストールと利用を禁止する。

･機器ベンダーの公式な公開場所（App Store、Google Playなど）以外から提供されるもの

・不審なベンダーが提供するもの

・正規ライセンスを取得していない違法なもの

●会社で契約したサービス社外の Wi-Fi サービスの利用を禁止する。

●自宅や屋外で利用する場合は以下を遵守する。

●信頼できる通信回線のみを利用する。

●機器は原則として勤務時間のみ稼働させる。

●不審なメールの受信など、情報セキュリティで不安がある場合はシステム管理者に問い合わせる。

5.2.1 社内での利用

利用期間中にＩＴ機器や電子媒体を社内に持ち込む場合は、システム管理者の許可を得る。社内で利用する場合は以下を実行する。

●社内 LAN への接続する場合はシステム管理者の許可を得る。

●充電を除き、社内のパソコンや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、システム管理者が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システム管理者の了解を得る。

6.標準等

6.1 標準ソフトウェア

種別	名称	開発・販売元	バージョン
パソコンＯＳ	mac	Apple	sierra 以降
	Windows	Microsoft	7 以降
オフィス系ソフト	Office	Microsoft	2010 以降
	Office for max	Microsoft	2016 以降
電子メール	Gmail	google	2007 以降
パソコン用 ウイルス対策	Symantec Endpoint protection	Symantec	Ver.13 以降
ブラウザ	Chrome	google	Ver.69 以降
	Internet Explorer	Microsoft	Ver.11 以降

6.2 ソフトウェアのアップデート方法

種別	名称	開発・販売元	アップデート方法
パソコンＯＳ	mac	Apple	更新プログラムを自動的にインストールする を選択する
	Windows	Microsoft	
業務用ソフト	Office	Microsoft	Microsoft Update の自動更新機能を有効にする
	Adobe Reader	Adobe	自動アップデートを有効にする。
スマートフォンＯＳ	iOS	Apple	iOS アップデート

6.3 ウイルス対策ソフトウェアの定義ファイルの更新方法

種別	名称	開発・販売元	アップデート方法
パソコン用ウイルス対策	Symantec Endpoint protection	Symantec	定義ファイル更新方法を自動に設定する

8	ＩＴ基盤運用管理	改訂日	2018.10.01
適用範囲	情報資産を扱うサーバー・ネットワーク等のＩＴインフラ		

1. 管理体制

システム管理者は、ＩＴ基盤の運用にあたり情報セキュリティ対策を考慮し製品又はサービスを選択する。ＩＴ基盤の情報セキュリティ対策及び関連仕様は、情報セキュリティ責任者が承認する。

1.1 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。

1.1.1 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、システム管理者が決定する。新規にサーバー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、システム管理者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、「6.1 サーバー機器情報セキュリティ要件」を参照のこと。

1.1.2 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導入するソフトウェアは、システム管理者が標準ソフトウェアを選定する。新規にソフトウェアを導入する場合は、システム管理者の許可を得て導入する。標準ソフトウェアは「6.2ＩＴ基盤標準ソフトウェア」を参照のこと。

1.1.3 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、システム管理者が決定する。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、システム管理者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、「6.4 ネットワーク機器情報セキュリティ要件」を参照のこと。

2. ＩＴ基盤の運用

システム管理者は、ＩＴ基盤の運用を行う際には以下を実施すること。

- ●システム管理者は、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、システム管理者が定期的に確認する。

●システム管理者は、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
●システム管理者は、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/ウェブフィルタリングソフトを使用して制限する。
●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。

3.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、システム管理者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、システム管理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「6.5 クラウドサービス情報セキュリティ対策評価基準」を参照のこと。

4.脅威や攻撃に関する情報の収集

システム管理者は、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。

5.廃棄・返却・譲渡

システム管理者は、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。

6.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、それに基づく当法人標準を以下とする。

6.1 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	利用技術・製品
Network HDD	利用者認証機能	ID PW
	セキュリティログ取得機能	標準仕様
	システムログ取得機能	標準仕様
	ユーザーアクセスログ取得機能	標準仕様
	ハードディスク：容量〇TB 以上	４TB 以上

	RAID 構成	
ＮＡＳサーバー	利用者認証機能	ID PW
	ディスク暗号化機能	有
	ハードディスク：容量〇GB 以上	４TB

6.2ＩＴ基盤標準ソフトウェア

種別	名称	開発・販売元	バージョン
ＲＤＢ	FileMaker	FileMaker	Ver.13 以降
ウイルス対策	End Point	Symantec 社	Ver.16 以降
ブラウザ	Chrome	Google 社	Ver.70.0 以降

6.3 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	Time Machine	Apple 社	Ver.10 以降

6.4 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	利用技術・製品
ルーター	利用者認証機能	ID　PW
	MAC アドレス認証	有
	通信ログ取得	標準仕様

6.5 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、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。

●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こと。

＜適合性評価制度の種類＞

➢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

9	システム開発及び保守	改訂日	2018.10.01
適用範囲	当法人が独自に開発及び保守を行う情報システム		

1.情報システムの開発

1.1 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。各工程の完了時にシステム管理者の承認を得る。

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

1.2 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システム管理者が判断し、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

1.3 情報システムの開発環境

情報システムの開発及び改修を行う環境は、運用環境とは分離する。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は、当該情報システムの運用を開始する前に、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、システム管理者の承認を得る。

1.4 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又は当該情報システムの利用停止を検討し、システム管理者の承認を得る。

1.5 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。各工程の完了時にシステム管理者の承認を得る。

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	2018.10.01
適用範囲	情報資産を取り扱う業務の委託		

1. 委託先の評価（クラウドサービスの利用を除く）

1.1 委託先評価基準

社外秘又は極秘の情報資産の処理あるいは授受を伴う業務を外部の組織に委託する場合は、委託先の情報セキュリティ管理について、下記の評価基準に基づいて評価する。

（委託先評価基準）

社内管理体制	①経営者による情報セキュリティ基本方針がある
	②情報セキュリティ管理責任者を置いている
	③情報セキュリティ対策を定める規定等を整備している
	④情報セキュリティ事故に対する対応手順がある
職員の監督	⑤全ての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
	⑥従業者から秘密保持に関わる誓約書等を取得している
オフィス内のセキュリティ	⑦会員の情報を扱う領域への入退室を管理している
	⑧会員の情報の保管について施錠管理を実施している
情報機器・媒体の取扱い	⑨機器・媒体の盗難防止措置を講じている
	⑩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
	⑪媒体の移送、受け渡し時の保護措置を講じている
	⑫媒体の安全な消去、廃棄の手順を整備している
サーバー・パソコン等の管理	⑬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
	⑭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
	⑮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

1.2 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。

1.3 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。

①当法人の社外秘又は極秘の情報資産及び個人情報の守秘義務

②再委託についての事項

③事故時の責任分担についての事項

④委託業務終了時の当法人が提供した社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

⑤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
⑥契約内容が遵守されない場合の措置
⑦事故発生時の報告方法

1.4 委託先の評価
委託開始後には、1.1 委託先評価基準の委託先における実施状況について定期的に評価する機会を設ける。委託先における評価基準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。
＜委託先評価の方法＞
- 委託先事業所に訪問して現場を観察する。
- 委託先の管理責任者にインタビューする。
- 委託先に書面で確認事項を通知し、実施状況について報告してもらう。

1.5 再委託
当法人が委託する業務を、委託先が他の組織又は個人に再委託する場合には、事前に書面による報告を委託先に求める。報告には必要に応じて以下の提供を含め、当法人の「1.1 委託先評価基準」「1.3 委託契約の締結」「1.4 委託先の評価」と同等の管理を再委託先に求めていることを確認し、情報セキュリティ責任者の承認を得たうえで再委託を認める。
- 委託先と再委託先との契約書案の写し（情報セキュリティに関連する部分のみ）
- 再委託先の選定基準
- 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

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	2018.10.01
適用範囲	情報セキュリティ事故対応及び事業継続管理		

1. 対応体制

情報セキュリティインシデントが発生した際には以下の体制で対応する。

最高責任者	理事長
対応責任者	インシデント対応責任者
一次対応者	発見者又はシステム管理者

2. 情報セキュリティインシデントの影響範囲と対応者

情報セキュリティインシデントが発生した場合、以下を参考に影響範囲を判断して対応する。

事故レベル	影響範囲	対応者
3	●会員、関連機関等に影響が及ぶとき ●個人情報が漏えいしたとき	理事長 インシデント対応責任者
2	事業に影響が及ぶとき	インシデント対応責任者
1	職員の業務遂行に影響が及ぶとき	システム管理者
0	インシデントにまでは至らないが、将来においてインシデントが発生する可能性がある事象が発見されたとき	システム管理者

3. インシデントの連絡及び報告

レベル 1 以上のインシデントが発生した場合、発見者は対応者に速やかに報告し、指示を仰ぐ。

4. 対応手順

インシデントを以下のとおりに区分し、それぞれの対応手順を示す。

区分	事件・事故の状況
漏えい・流出	社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

4.1 漏えい・流出発生時の対応

事故レベル	対応手順	対応者
3	①発見者は即座にインシデント対応責任者及び理事長に報告する。 ②インシデント対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策を実行する。 ③インシデント対応責任者は被害者/本人対応を準備する。 ④インシデント対応責任者は問い合せ対応を準備する。 ⑤インシデント対応責任者は影響範囲・被害の大きさによっては総務主任に報道発表の準備を申請する。 ⑥インシデント対応責任者はサイバー攻撃等の不正アクセスによる被害の場合は都道府県警察本部のサイバー犯罪相談窓口に届け出る。 ⑦インシデント対応責任者は個人情報の漏えいの場合には監督官庁に届け出る。 理事長は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。	理事長 インシデント対応責任者
2	①発見者は発見次第、システム管理者に報告する。 ②システム管理者は漏えい先を調査し、インシデント対応責任者に報告する。 ③システム管理者は社内関係者に周知する。	インシデント対応責任者
1	※情報漏えい・流出は全て事故レベル 2 以上	

4.2 改ざん・消失・破壊・サービス停止発生時の対応

事故レベル	対応手順	対応者
3	①発見者は即座にインシデント対応責任者及び理事長に報告する。 ②システム管理者は原因を特定し、応急処置を実行する。 ③インシデント対応責任者は全職員に周知する。 ④電子データの場合はシステム管理者がバックアップによる復旧を実行する。 ⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。 ⑦システム管理者は原因対策を実施する。 理事長は法人内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。	理事長 インシデント対応責任者

2	①発見者は発見次第、システム管理者に報告する。 ②システム管理者は原因を特定し、応急処置を実行する。 ③インシデント対応責任者は全職員に周知する。 ④電子データの場合はシステム管理者がバックアップによる復旧を実行する。 ⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。 ⑦システム管理者は原因対策を実施する。	システム管理者 インシデント対応責任者
1	①発見者は発見次第、システム管理者に報告する。 ②システム管理者は原因を特定し、応急処置を実行する。 ③電子データの場合はシステム管理者がバックアップによる復旧もしくは再作成・入手を実行する。 ④機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑤書類・フィルム等の原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する ⑥システム管理者は原因対策を実施する	システム管理者
0	発見者は発見次第、発生可能性のあるインシデントと想定される被害をシステム管理者に報告する。	システム管理者

4.3 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（以下「コンピュータ」といいます。）がウイルスに感染した場合には、以下を実行する。

①ネットワークからコンピュータを切断する。

②システム管理者に連絡する。

③ウイルス対策ソフトの定義ファイルを最新版に更新する。

④ウイルス対策ソフトを実行しウイルス名を確認する。

⑤ウイルス対策ソフトで駆除可能な場合は駆除する。

⑥駆除後再度ウイルス対策ソフトでスキャンし、駆除を確認する。

⑦システム管理者に報告する。

以下の場合など職員自身で対応できないと判断される場合はシステム管理者に問い合わせる。

➢ウイルス対策ソフトで駆除できない。

➢システムファイルが破壊・改ざんされている。

➢ファイルが改ざん・暗号化・削除されている。

4.5 届出及び相談

システム管理者は、インシデント対応後に以下の機関への届け出又は相談を検討する。

＜届出・相談先＞

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

5.情報セキュリティインシデントによる事業中断と事業継続管理

理事長は、情報セキュリティインシデントの影響により当法人事業が中断した場合に備え、以下を定める。

5.1 想定される情報セキュリティインシデント

以下のインシデントによる事業の中断を想定する。

●情報セキュリティインシデント：大型地震の発生に伴う設備の倒壊、回線の途絶、停電等によるシステム停止

●想定理由：当法人の事業は、停電によりシステムが停止しても直ちに被害は生じない。電源復旧に伴い事業を再開する。

5.2 復旧責任者及び関連連絡先

被害対象	復旧責任者	関係者連絡先
電源設備　空調機	総務主任	（株）エスワーク
ハードウェア ソフトウェア ネットワーク機器 回線サービス	理事長	（株）エスワーク
会員	総務主任	営業部関連機関リスト参照

職員人的被害	総務主任	職員名簿参照

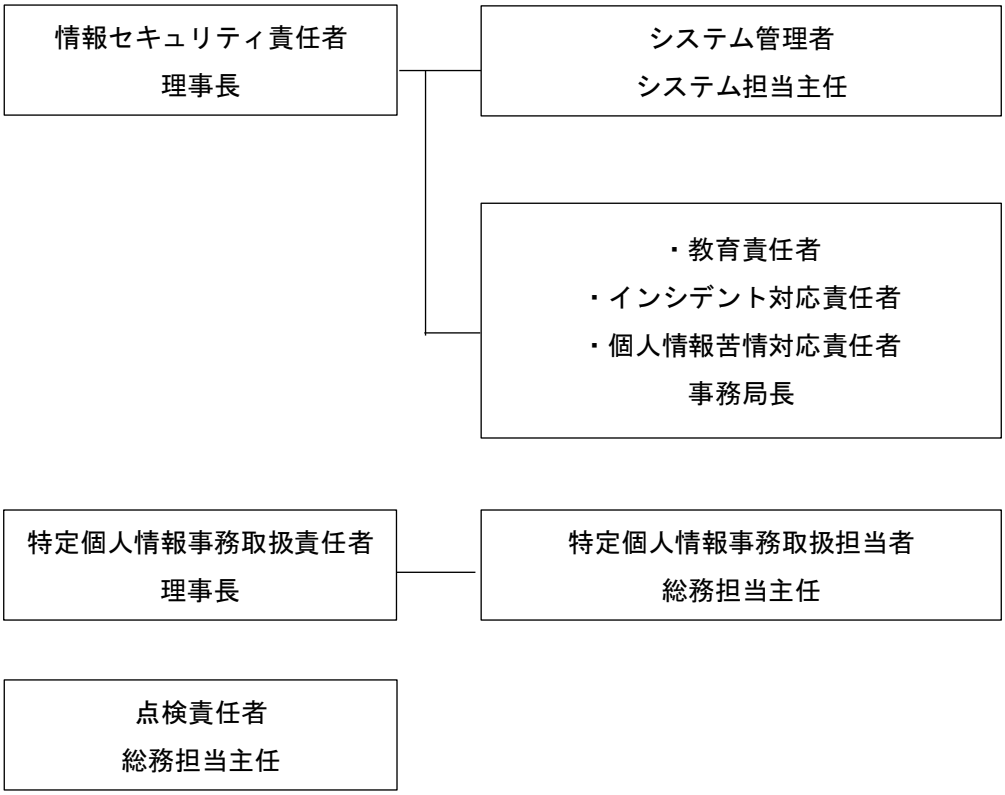
5.3 事業継続計画

インシデント対応責任者は、想定する情報セキュリティインシデントが発生し、事業が中断した際の復旧責任者の役割認識及び関係者連絡先について、有効に機能するか検証する。復旧責任者は、被害対象に応じて復旧から事業再開までの計画を立案する。

12	社内体制図	改訂日	2018.10.01
適用範囲	当法人の情報セキュリティ管理		

1. 情報セキュリティのための組織

「1. 組織的対策」における「2. 情報セキュリティのための組織」を下図に示す。組織の変更があった場合は、情報セキュリティ責任者が本体制図の更新を行う。



13	委託契約書機密保持条項サンプル	改訂日	2018.10.01
適用範囲	外部委託契約の締結時		

1. 委託契約時の機密保持契約条項

機密性評価値が 1 以上の情報の処理あるいは授受を伴う業務を外部の組織に委託する場合は、契約に以下の機密保持条項を規定するか、別途文書により合意する。

＜機密保持条項サンプル＞

（甲：委託元、乙：委託先）

注：このサンプルは、外部委託に関する契約書における機密保持に関する条項を示すものです。甲と乙とが、それぞれ相手から機密として提供される情報の守秘義務を負う双務契約の形式としています。

第〇条（機密保持）

1. 甲及び乙は、本契約の履行にあたり、相手方が機密である旨指定して開示する情報および本契約の履行により生じる情報（以下「機密情報」という）を機密として取扱い、相手方の事前の書面による承諾なく第三者に開示してはならない。ただし、次の各号のいずれかに該当する情報については、この限りではない。

①開示を受けたときに既に公知であったもの

②開示を受けたときに既に自ら所有していたもの

③開示を受けた後に自らの責によら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守秘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自らが独自に開発したことを証明し得るもの

2. 甲が乙に機密である旨指定して開示する情報は、別表 1（本案では、特に例示しない）、乙が甲に機密である旨指定して開示する情報は、別表 2（本案では、特に例示しない）の通りである。なお、別表 1 及び別表 2 は甲乙協力し常に最新の状態を保つべく適切に更新するものとする。

3. 甲及び乙は、相手方より開示された機密情報の管理につき、自ら保有する他の情報、物品等と明確に区別して管理するとともに、以下の事項を遵守する。

(1) 機密情報の管理責任者及び保管場所を定め、善良なる管理責任者の注意をもって保管管理する。

(2) 機密情報を取り扱う職員を必要最小限にとどめ、上記保管場所以外へ持ち出さない。

⑶機密情報の管理責任者名、機密情報を取り扱う職員名及び機密情報に関する情報セキュリティ対策を、〇年〇月〇日までに相手方に報告する。また、報告内容に変更が生じた場合には、速やかに当該変更内容を相手方に報告する。

⑷⑶にて報告した機密情報を取り扱う職員に対して本契約の内容を周知徹底させ、機密情報の漏洩、紛失、破壊、改ざん等を未然に防止するための措置を取る。

⑸甲の書面による承諾を得た場合を除き、機密情報を複写、複製せず、また、機密情報を開示、漏洩しない。但し、政府機関又は裁判所の命令により要求された場合、その範囲で開示することが出来る。なお、その場合には、相手方にその旨をすみやかに通知すること。

⑹機密情報は本契約の目的の範囲でのみ使用する。

⑺事故発生時には直ちに相手方に対して通知し、事故再発防止策の協議には相手方の参加を認める。

⑻委託期間満了時又は本契約の解除時、機密情報（⑸に基づく複写、複製を含む）を相手方に返却、又は自己で廃棄の上廃棄の証拠を相手方に報告する。

⑼⑻にかかわらず、相手方から返却また廃棄を求められたときは、機密情報（⑸に基づく複写、複製を含む）を相手方に返却、又は自己で廃棄の上廃棄の証拠を相手方に報告する。

⑽甲及び乙は、相手方に対して、機密情報の以下の具体的管理状況に関する報告を求めることができる。この報告結果をもとに、甲及び乙が相手方の事務所における機密情報の管理状況を確認するために相手方の事務所への立入検査を希望する場合には、当該検査に協力する。また、甲及び乙は相手方に対して是正措置を求めることができ、相手方はこれを実施するものとする。

①委託契約範囲外の加工、利用の禁止の遵守

②委託契約範囲外の複写、複製の禁止の遵守

③情報セキュリティ対策状況

第〇条（再委託）

1. 乙は、本業務（の全部、又は一部）を第三者へ再委託する場合、甲の事前の書面による同意を得ずに、再委託してはならない。
2. 前項の規定に基づき本業務を再委託する場合、乙は自己が負う義務と同等の義務を再委託先に対して書面にて課すとともに、甲に対して再委託先に当該義務を課した旨を書面により報告し、かつ乙は当該機密情報開示に伴う全責任を負うものとする。また、乙は次項第 3 号の再委託先からの報告を、第〇条（機密保持）第３項の具体的管理状況の報告時にあわせて甲に報告する。
3. 前項に加え、乙は再委託先から次の各号の同意を得なければならない。また、乙は、当該同意を得た旨を甲に書面で報告する。

①事故発生時には直ちに甲に対しても通知すること
②事故再発防止策を協議する際には甲の参加も認めること
③再委託先における機密情報の具体的管理状況の報告は、甲の閲覧も可とすること

【コメント】
以下に示すような「機密保持条項に関連する他の条項」については、業務委託期間終了又は本契約の解除後も、合理的な期間にわたり存続させることが望まれます。

第〇条（権利義務の譲渡）
第〇条（成果の帰属）
第〇条（損害賠償）
第〇条（法令等の遵守義務）
第〇条（協議事項）
第〇条（紛争の解決）

また、第〇条（守秘義務）の規定は、「業務委託期間終了又は本契約の解除後〇年間有効とする」の如く有効期間を示すことが適切です。