情報セキュリティ対策基準

目　次

(Ver. 2. 0)

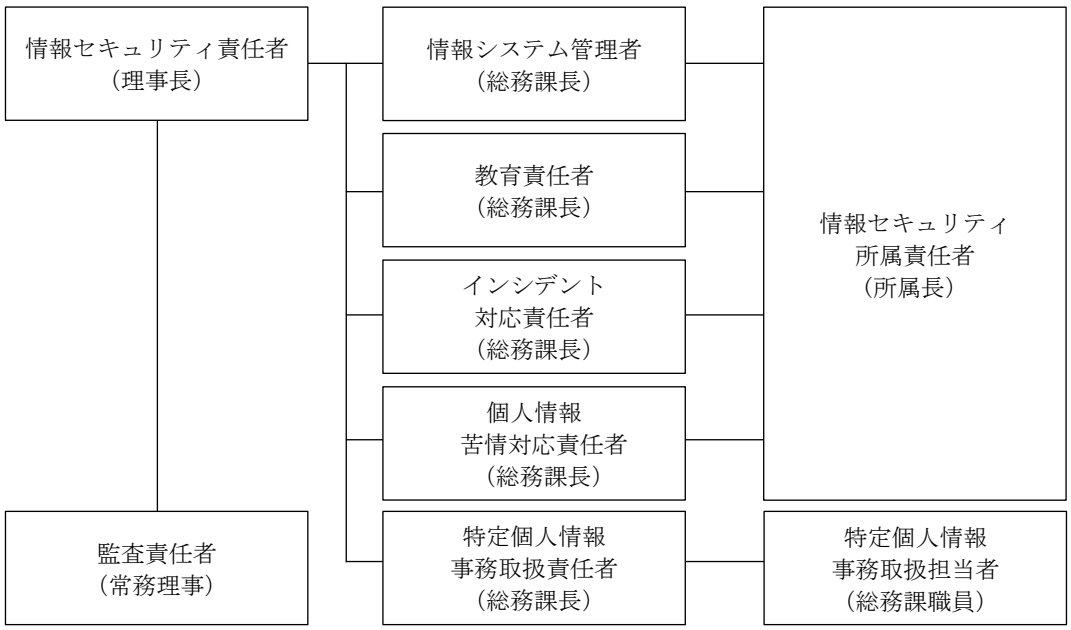
1	組織的対策	改訂日	2021.04.01
適用範囲	協会全体・全職員（役員、職員、短時間勤務、アルバイト、人材派遣社員を含む。以下同じ。）		

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。

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。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報システム管理者	情報セキュリティ対策のためのシステム管理を行う。
情報セキュリティ所属責任者	各所属における情報セキュリティの運用管理責任者。各所属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。
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。
インシデント対応責任者	事故の影響を判断し、対応について意思決定する。
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対策基準をもとに検証又は評価し、助言を行う。
特定個人情報事務取扱責任者	特定個人情報の情報セキュリティに関する責任者。
特定個人情報事務取扱担当者	特定個人情報を取り扱う事務に従事する職員。
個人情報苦情対応責任者	個人情報に関する苦情の対応責任者。

＜情報セキュリティ委員会体制図＞



2. 情報セキュリティ取組みの監査

監査責任者は、情報セキュリティ対策基準の実施状況について、８月に監査を行い、監査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。

・情報セキュリティ対策基準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。
・情報セキュリティ対策基準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、情報セキュリティ対策基準の改訂。
・情報セキュリティ対策基準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、情報セキュリティ対策基準の改訂。

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	2020.06.01
適用範囲	全職員		

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. 職員の責務

職員は、以下を順守する。

・職員は、協会が機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、協会の情報セキュリティポリシーを遵守する。違反時の懲戒については、就業規則及び有期契約職員就業規則に準じる。

※協会が機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２以上のものをいう。

3. 雇用の終了

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、顧客・取引先から協会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。

職員は、在職中に知り得た協会の機密若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

テーマ：以下は必須とする。

- ➢情報セキュリティ対策基準の説明（採用時）
- ➢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）
- ➢個人情報の取り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、受験費用の予算化を含むこととする。

＜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	2020.06.01
適用範囲	協会全体・全職員		

1. 情報資産の管理

1.1 情報資産の特定と機密性等の評価

協会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。

情報資産の機密性は、以下の基準に従って評価する。

機密性 3：極秘	協会の事務で取り扱う情報資産のうち、特に機密性を要するもの（データだけではなく、それらが含まれる電子記憶媒体、パーソナルコンピュータ、システム等も同様） ・特定個人情報及び個人情報 ・法律で安全管理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 ・限定提供データ（一定の条件を満たす特定の外部者に提供することを目的とする情報）として指定されている ・機密（秘密として管理されているもの）として指定されている ・漏えいすると取引先や顧客に大きな影響がある ・部外に漏れた場合に協会の信頼を著しく害する可能性がある ・公開することでセキュリティ侵害が生じる可能性がある
機密性 2：部外秘	・漏えいすると事業に大きな影響がある ・機密性 3 には当てはまらないが、直ちに一般に公表することを前提としていない
機密性 1：公開	漏えいしても事業にほとんど影響はない

情報資産の完全性は、以下の基準に従って評価する。

完全性 2	協会で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、市民の権利が侵害される又は協会の業務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある
完全性 1	完全性 2 以外

情報資産の可用性は、以下の基準に従って評価する。

可用性 2	協会で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、市民の権利が侵害される又は協会の業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある
可用性 1	可用性 2 以外

情報資産の機密性、完全性、可用性のいずれかの重要性分類２以上に分類される情報資産は、この対策基準の対象とする。重要性分類１の情報資産も、必要なものはできる限りこの対策基準に準じた対応を講じるものとする。

1.2 情報資産の分類の表示

情報資産の機密性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表示

・書類：保管先キャビネット、ファイル、バインダーに表示

表示が困難な場合は、「情報資産管理台帳」に機密性評価値を表示する。

1.3 情報資産の管理責任者

情報資産の取り扱い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所属長とする。

1.4 情報資産の利用者

情報資産の利用者の範囲は、「情報資産管理台帳」の利用者範囲欄に示された所属に従事する職員とする。

2. 情報資産の協会外持ち出し

情報資産を協会外に持ち出す場合には、以下を実施する。

・極秘にあたる情報資産は持ち出してはならない。

・部外秘の場合は所属長の許可を得る。

・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、ハードディスク、フォルダー又はデータを暗号化する。

・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、大きなタグを付ける、ストラップで体やカバンに固定する、落としてもすぐに分かるように鈴を付けるなどの対応を行う。

・屋外でネットワークへ接続して部外秘の情報資産を送受信する場合は、暗号化する。

・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

極秘又は部外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、溶解又は焼却
USB メモリ・HDD・CD・DVD	破壊、細断又は完全消去 ※OS による削除・クイックフォーマットは不可

3.2 媒体の再利用

極秘又は部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	完全消去後再利用

スク・DVD-RW ディスク	※OS による削除・クイック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

情報システム管理者は、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
ファイルサーバー	ユーザーファイル	Backup ソフト (SymantecSystemRecovery)	外付け 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
人事管理システム	アプリケーションデータ	同期ツール	外付け HDD
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：施錠付きサーバーラックに収納

＜廃棄・再利用＞

「3.媒体の処分」に従う。

4.3 クラウドサービスを利用したバックアップ

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、協会の情報セキュリティ対策基準に適合している。

・協会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	アクセス制御及び認証	改訂日	2020.06.01
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

部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

部外秘又は極秘の情報資産を扱う協会内情報システムは、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、情報システム管理者は、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

協会の職員以外の者にアカウントを発行する場合は、理事長又は情報セキュリティ責任者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

部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

部外秘又は極秘の情報資産を扱う情報システムの端末若しくは情報機器を、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
ファイルサーバー	Windows Active Directory
給与計算システム	アプリケーションのユーザー認証
人事管理システム	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
ファイルサーバー	Windows ログオン認証：アカウント名・パスワード
給与計算システム	アプリケーションのユーザー認証：ID・パスワード
人事管理システム	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＞ WindowsOS：administrator、admin LinuxOS：root ・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	・パソコン番号
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 ・アルファベット小文字、数字、記号を含む	＜パスワードに使う文字＞ ・8 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 ・アルファベット小文字、数字、記号を含む

	・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	・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

ルータ	ID・パスワード認証
ＨＵＢ	認証なし（インテリ HUB ではない）
サーバ	ドメイン認証(ﾄﾞﾒｲﾝ名・ID・ﾊﾟｽﾜｰﾄﾞ)
パソコン	ドメイン認証(ﾄﾞﾒｲﾝ名・ID・ﾊﾟｽﾜｰﾄﾞ)
複合機	パスワード認証

5	物理的対策	改訂日	2020.06.01
適用範囲	全事業所		

1. セキュリティ領域の設定

協会内で扱う情報資産の重要度に応じて協会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	受付・応接スペース・会議室・倉庫
利用者	役職員、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	未使用時に部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、消火器の設置

レベル 2 領域	執務スペース・理事長室・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及び警備会社への通報装置作動
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、スプリンクラー又は消火器の設置

レベル 3 領域	サーバールーム
利用者	あらかじめ許可された者
施錠	常時施錠及び警備会社への通報装置作動、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・点検時等に総務課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	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。

・サーバーは施錠付き専用ラックに収納する。

・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、情報セキュリティ所属責任者の許可を得ること。

・応接スペース及び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。

＜本部＞

・郵便物：メールボックス、書留便の場合は受付

・宅配便：受付

6	ＩＴ機器利用	改訂日	2021.09.01
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、協会所定の標準ソフトウェアを導入する。協会所定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

情報システム管理者は、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てはならない。

＜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

協会が管理するパソコン及びサーバー以外の機器を協会内 LAN に接続することを禁止する。

業務上必要な場合は、情報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

情報システム管理者は、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協会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、部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。
・退勤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。退勤時又は使用しないときにはパソコンの電源を切る。
・パソコン・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

情報システム管理者は、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協会内周知又は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職員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情報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、情報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＞

・部外秘又は極秘の情報資産を保存する場合は、情報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職員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。

4.3 SNS の個人利用

・協会の業務に関わる情報の書き込みは行わない。
・取引先従業者と 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。

＜傍受による漏えい防止＞

・部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、又は**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、情報システム管理者の許可を得る。

・情報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。

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、情報システム管理者に報告し、情報システム管理者は協会内に注意を促す。

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、情報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。

・情報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。
・協会で契約又は許可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。
・協会内 LAN にリモートで接続する場合は情報システム管理者の許可を得る。
外部から協会内 LAN にリモートで接続する場合は以下を遵守する。
・情報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、直ちに情報システム管理者に連絡し指示に従う。
・職員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。
・協会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。
・部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
・協会が契約又は許可したサービス以外の 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情報システム管理者に問い合わせる。

5.2.1 協会内での利用

利用期間中にＩＴ機器や電子媒体を協会内に持ち込む場合は、情報システム管理者の許可を得る。協会内で利用する場合は以下を実行する。
・協会内 LAN への接続は禁止する。
・充電を除き、協会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、情報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情報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	Windows	Microsoft	10.1 以降
オフィス系ソフト	Office	Microsoft	2013 以降
電子メール	Outlook	Microsoft	2013 以降
パソコン用 ウイルス対策	Kaspersky	Kaspersky	Ver.10 以降
スマートフォン用 ウイルス対策	Kaspersky	Kaspersky	Ver.10 以降
ブラウザ	Microsoft Edge	Microsoft	Ver.92.0.902.84 以降
	Google Chrome	Google	Ver.81.0.4044.122 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	Windows10	Microsoft	更新プログラムの通知が来たら速やかに更新する
業務用ソフト	Office2016	Microsoft	Windows 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。
ブラウザ	Microsoft Edge	Microsoft	Windows アップデータの通知が来たら速やかに更新する。
	Google Chrome	Google	自動アップデートを有効にする。
スマートフォン OS	Android	Google	機種毎の情報を常に調べて必要に応じて対応する
	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	Kaspersky	Kaspersky	定義ファイル更新方法を自動に設定する
スマートフォン用 ウイルス対策	Kaspersky	Kaspersky	定義ファイル更新方法を自動に設定する

7	ＩＴ基盤運用管理	改訂日	2020.12.25
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

情報システム管理者は、ＩＴ基盤の運用に当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。

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、情報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、「**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導入するソフトウェアは、情報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、情報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「**7.2ＩＴ基盤標準ソフトウェア**」を参照のこと。

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、情報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、「**7.4 ネットワーク機器情報セキュリティ要件**」を参照のこと。

3.ＩＴ基盤の運用

情報システム管理者は、ＩＴ基盤の運用を行う際には以下を実施すること。

・情報システム管理者は、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、情報システム管理者が定期的に確認する。

・情報システム管理者は、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

・情報システム管理者は、必要に応じて業務に不要なウェブサイト閲覧を協会内周知又は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。

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、情報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「**7.5 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。

5.脅威や攻撃に関する情報の収集

情報システム管理者は、最新の脅威や攻撃に関する情報収集を行い、必要に応じて協会内で共有する。

6.廃棄・返却・譲渡

情報システム管理者は、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。

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、それに基づく協会標準を以下とする。

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	利用技術・製品
ファイルサーバー	利用者認証機能	Windows Active Directory
	セキュリティログ取得機能	Windows イベントビューワ
	システムログ取得機能	Windows イベントビューワ
	ユーザーアクセスログ取得機能	―
	バックアップ	取得必須（３世代以上）
	ハードディスク冗長化	RAID 構成
NAS サーバー	利用者認証機能	Windows Active Directory
	バックアップ	取得必須（３世代以上）
	ハードディスク冗長化	RAID 構成

7.2ＩＴ基盤標準ソフトウェア

種別	名称	開発・販売元	バージョン
OS	Windows Server	Microsoft	メーカーサポート可能バージョン
ＲＤＢ	SQL Server	Microsoft	同上
ウイルス対策	Kaspersky	Kaspersky	同上
ブラウザ	Internet Explorer	Microsoft	同上

7.3 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	ＲＴＸシリーズ	YAMAHA	メーカーサポート可能バージョン
ファイアウォール	―	―	同上
ＨＵＢ	―	―	同上

7.4 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	認証機能	ＩＤ&パスワード認証
	ＷＡＮ間接続通信暗号化	ＶＰＮ接続（IPsecVPN）
	通信ログ取得	―
無線ＬＡＮ	通信暗号化	WPA2 若しくは WPA2-PSK(AES)、それ以上のセキュリティを有するもの
	ＳＳＩＤステルス機能	SSID ステルス機能有効
	端末認証	―

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、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＞

・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

・プライバシーマーク制度

・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
・SOC2（Service Organization Control）
・FedRAMP（米国政府機関におけるクラウドセキュリティ認証制度）
・SAS70（米国監査基準第 70 号）
・ISMAP（政府情報システムのためのセキュリティ評価制度）

8	システム開発及び保守	改訂日	2020.06.01
適用範囲	協会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。各工程の完了時に情報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

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

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、情報システム管理者の承認を得る。

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又は当該情報システムの利用停止を検討し、情報システム管理者の承認を得る。

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。各工程の完了時に情報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

9	委託管理	改訂日	2020.06.01
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

情報セキュリティ所属責任者は「情報資産管理台帳」の重要度が２以上である情報資産の取り扱う業務を、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、委託先評価基準に基づいて評価する。

＜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 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。
・「**委託先情報セキュリティ対策状況確認リスト**」の各区分で 80%以上の項目について対策を実施している。

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。

・協会の部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
・委託業務終了時の協会が提供した部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、「**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。

＜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「**委託先情報セキュリティ対策状況確認リスト**」を送付し、実施状況について回答してもらう。

5. 再委託

協会が委託する業務を、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、協会の「**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

9-1 業務委託契約に係る機密保持条項

第〇条（機密保持）

1. 甲及び乙は、本契約の履行に当たり、相手方が機密である旨指定して開示する情報及び本契約の履行により生じる情報（以下、「機密情報」という。）を機密として取り扱い、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（※契約ごとに指定し作成する）、乙が甲に機密である旨指定して開示する情報は、別表 2（※契約ごとに指定し作成する）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。

(3)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。

(4)前号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。

(5)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、相手方にその旨を速やかに通知すること。

(6)機密情報は本契約の目的の範囲でのみ使用する。

(7)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。

(8)委託期間満了時又は本契約の解除時、機密情報（(5)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。

(9)前号にかかわらず、相手方から返却また廃棄を求められたときは、機密情報（(5)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。

(10)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

第〇条（権利義務の譲渡）
乙は、本契約によって生じる権利又は義務を第三者に譲渡し、又は承継させてはならない。

第〇条（納入物件の知的財産権）
1. 納入物件に関する著作権（著作権法第 27 条及び第 28 条に定める権利を含む。）、本契約の履行過程で生じた発明（考案及び意匠の創作を含む。）及びノウハウを含む産業財産権（特許その他産業財産権を受ける権利を含む。）（以下、「知的財産権」という。）は、乙又は国内外の第三者が従前から保有していた知的財産権を除き、第〇条の規定による請負業務完了の日をもって、乙から甲に自動的に移転するものとする。

2. 納入物件に、乙又は第三者が従前から保有する知的財産権が含まれている場合は、前項に規定する移転の時に、乙は甲に対して非独占的な実施権、使用権、第三者に対する利用許諾権(再利用許諾権を含む。)、その他一切の利用を許諾したものとみなす。なお、その対価は契約金額に含まれるものとする。

3. 乙は、甲及び甲の許諾を受けた第三者に対し、納入物件に関する著作者人格権、及び納入物件

に対する著作権法第 28 条の権利、その他原作品の著作者又は権利者の地位に基づく権利主張は行わないものとする。

第〇条（知的財産権の紛争解決）
1. 乙は、納入物件に関し、甲及び国内外の第三者が保有する知的財産権（公告、公開中のものを含む。）を侵害しないことを保証するとともに、侵害の恐れがある場合、又は甲からその恐れがある旨の通知を受けた場合には、当該知的財産権に関し、甲の要求する事項及びその他の必要な事項について調査を行い、これを甲に報告しなければならない。

2. 乙は、前項の知的財産権に関して権利侵害の紛争が生じた場合（私的交渉、仲裁を含み、法的訴訟に限らない。）、その費用と責任負担において、その紛争を処理解決するものとし、甲に対し一切の負担及び損害を被らせないものとする。

第〇条（損害賠償）
乙は、乙の責に帰すべき事由によって甲又は第三者に損害を与えたときは、その被った通常かつ直接の損害を賠償するものとする。ただし、乙の負う賠償額は、乙に故意又は重大な過失がある場合を除き、第〇条所定の契約金額を超えないものとする。

第〇条（協議）
本契約に定める事項又は本契約に定めのない事項について生じた疑義については、甲乙協議し、誠意をもって解決する。

第〇条（その他）
本契約に関する紛争については、神戸地方裁判所を唯一の合意管轄裁判所とする。

9-2　委託先情報セキュリティ対策状況確認リスト

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社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	社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	

10	情報セキュリティインシデント対応 並びに事業継続管理	改訂日	2020.06.01
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. 対応体制

情報セキュリティインシデントが発生した場合には、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	発見者又は情報システム管理者

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	責任者
3	・顧客、取引先等に影響が及ぶとき ・個人情報が漏えいしたとき	理事長
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	インシデント対応責任者
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	情報システム管理者

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、対応者又は責任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	部外秘又は極秘の情報資産の盗難、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
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わせ対応を準備する。

	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課に報道発表の準備を指示する。 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兵庫県警察本部のサイバー犯罪相談窓口及び神戸市に届け出る。 ⑦インシデント対応責任者は個人データ※又は特定個人情報漏えいの場合には個人情報保護委員会及び神戸市に報告する。 ⑧理事長は協会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とともに、神戸市に報告する。 ※個人データ：個人情報データベース等（特定の個人を検索できるようにまとめたもの）を構成する個人情報
2	①発見者は発見次第、情報システム管理者に報告する。 ②情報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情報システム管理者は協会内関係者に周知するとともに、神戸市に報告する。
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
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情報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協会内に周知するとともに総務課情報システム担当に連絡する。 ④電子データの場合は情報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機器の場合は情報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所属責任者が可能な範囲で修復する。 ⑦情報システム管理者は原因対策を実施する。 理事長は協会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とともに、神戸市に報告する。
2	①発見者は発見次第、情報システム管理者に報告する。 ②情報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協会内に周知するとともに総務課情報システム担当に連絡する。 ④電子データの場合は情報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機器の場合は情報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所属責任者が可能な範囲で修復する。 ⑦情報システム管理者は原因対策を実施する。
1	①発見者は発見次第、情報システム管理者に報告する。 ②情報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情報システム管理者がバックアップによる復旧若しくは再作成・入手を実行する。 ④機器の場合は情報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所属責任者が可能な範囲で修復する ⑥情報システム管理者は原因対策を実施する
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情報システム管理者に報告する。

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」という。）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情報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情報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情報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。

4.4 届出及び相談

情報システム管理者は、インシデント対応後に以下の機関への届け出、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

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協会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、停電等によるサーバーシステム停止

・想定理由：協会の事業は、業務をサーバーシステムに依存しているため、停止した場合は事業の継続が困難になり多大な損失が発生

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	総務課長	[redacted]
（サーバーシステム） 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 バックアップクラウドサーバー	インシデント対応責任者 情報システム管理者	[redacted]

		[redacted]
市等関係先	所属長	所属関係先リスト参照
職員人的被害	総務課長	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。

11	個人番号及び 特定個人情報の取り扱い	改訂日	2020.06.01
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）		

個人番号及び特定個人情報の適正な取り扱いに関する基本方針

1. 関係法令・ガイドライン等の遵守

協会は、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」という。）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」という。）及び個人情報保護委員会のガイドラインを遵守します。

2. 利用目的

協会は、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) 取引先様の特定個人情報等

・不動産取引に関する支払調書作成事務

・報酬、料金、契約金及び賞金に関する支払調書作成事務

(2) 評議員及び役員の特定個人情報等

・報酬等に関する支払調書作成事務

(3) 協会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

(4) 協会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

協会は、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、個人番号及び特定個人情報取扱規程を定め、これを遵守します。

4. 委託の取り扱い

協会は、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、協会は、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

協会は、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

協会は、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
・協会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、及び質問苦情等は下記までお願いいたします。

総務課　078 - 795－5533

発効日:令和２年６月１日
公益財団法人神戸市公園緑化協会
理事長　桜井秀憲