あいち地域包括ケアポータルサイト情報セキュリティ実施手順

目次

第１章　総則

（趣旨）

第１　この実施手順は「愛知県情報セキュリティポリシー」（以下「ポリシー」という。）第８条の規定に基づき、あいち地域包括ケアポータルサイトウェブシステム（以下「システム」という。）の情報セキュリティ対策の実施に必要な事項を定めるものとする。

（定義）

第２　この実施手順において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1) 情報機器

サーバ、パソコン、ネットワークハードディスク及びプリンタ（複合機を含む。以下同じ。）等の情報処理を行う機器をいう。

(2) 通信機器

ルータ（ファイアウォールを含む。）、HUB 等のデータ通信を行う機器をいう。

(3) ネットワーク

サーバを使用して事務処理を行うためのハードウェア、ソフトウェア及び通信回線で構成されるものをいう。

(4) 情報システム

情報機器及び通信機器並びにそれらを相互に接続するためのハードウェア及びソフトウェアの総称をいう。

(5) 情報資産

次の資産を情報資産という。

① コンピュータ、情報システム、ネットワーク、電磁的記録媒体（以下「記録媒体」という。）

② コンピュータ、情報システム及びネットワークで取り扱う情報

③ ポリシー、情報セキュリティ実施手順、情報システム仕様書及びネットワーク構成図等の紙媒体によるシステム関連文書（以下「システム関連文書」という。）

(6) コンピュータウイルス

プログラムやデータに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能及び発病機能のいずれかの機能を有するものをい

う。

(7) ユーザＩＤ

コンピュータや情報システムを利用する職員に与えられる利用者識別のための文字列をいう。

(8) パスワード

利用者の情報保護のため、ユーザＩＤごとに設定する認証用文字列をいう。

(9) ネットワーク端末

情報企画課が配備し、又は行政情報通信ネットワークへの接続を承認したパソコン、ネットワークハードディスク及びプリンタをいう。

第２章　人的セキュリティ対策

（セキュリティ管理体制の整備）

第３　システムの情報セキュリティ対策を実施するため、次に掲げる管理体制を整備する。

(1) 情報セキュリティ管理者

情報セキュリティの管理者（以下「情報セキュリティ管理者」という。）は、愛知県福祉局高齢福祉課長とする。

(2) システム管理者

システムの管理者（以下「システム管理者」という。）は、愛知県福祉局高齢福祉課長とする。

（委託事業者に対するセキュリティ対策）

第４　システム管理者は、システムの開発、改修又は運用を外部の事業者に委託する場合、委託業務内容のほか、次の各号に定める事項を契約書、委託仕様書等に記載するものとする。

(1) 業務上知りえた情報を漏えいしないこと。

(2) 情報機器、記録媒体等を持ち込む、又は持ち出す場合は、あらかじめシステム管理者の承認を得ること。

(3) 業務履行場所が愛知県の管理する施設以外の場合には、情報セキュリティに関する遵守事項の確認のために立ち入り検査を行う場合があること。

(4) その他情報セキュリティを確保するために必要な措置をとること。

２　システム管理者は、前項の契約を締結した場合は、当該委託事業者における利用条件の遵守状況を監視する。

（障害に備えた訓練）

第５　システム管理者は、重大なシステム障害に備えた訓練を定期的に実施するものとする。

（事故等発見時、障害発生時の対応）

第６　システムの利用者は、システムに係る事故、障害又は違反行為若しくは違反の疑義の

ある行為（以下「事故等」という。）を発見した場合は、速やかにシステム管理者に報告しなければならない。

２　システム管理者は、災害や事故等に対処するため、異常時連絡体制、応急措置、被害拡大防止策、復旧手順及び記者発表等の対応をあらかじめ別に定めておくものとする。

（重大な事故、障害等の記録）

第７　システム管理者は、システムに事故等が発生した場合は、軽微なものを除きその事故等を分析し、並びに分析結果を記録し、及び保存するとともに、再発防止の措置を講じるものとする。

（ユーザＩＤの種類及び利用者の範囲）

第８　システムにおけるユーザＩＤはシステムの機能を利用するためのＩＤであり、その種類は次のとおりとする。

ユーザーＩＤ　登録団体に対して発行されるＩＤ

管理者用ＩＤ　高齢福祉課地域包括ケア・認知症対策室地域包括ケアＧに発行されるＩＤ

（利用者が遵守すべき事項）

第９　システムの利用者は、次の各号に掲げる行為を行ってはならない。

(1) 情報の改ざん、滅失、き損及び漏えい並びに虚偽の情報を報告すること。

(2) 他の利用者や第三者を誹謗中傷するなどして、その名誉を傷つけること。

(3) 法令又は公序良俗に反して利用すること。

(4) ユーザＩＤ及びパスワードをシステムの利用を認められた者以外に使用させること。

(5) ユーザＩＤ及びパスワードを不適正使用すること。

(6) 業務以外の目的に利用すること。

(7) 営利目的に利用すること。

(8) ネットワーク端末以外の情報機器を行政情報通信ネットワークに接続すること。

(9) 私物の記録媒体で作業すること。ただし、作業をしないことにより職務の遂行に支障をきたすとして、記録に残る形でシステム管理者の許可を得た場合を除く。

(10) その他システムの運営管理に支障を及ぼすおそれのあること。

（情報資産の分類と管理）

第１０　システム管理者は、次の各号によりシステムに関する情報資産の分類及び管理を行うこととする。

(1) ポリシー第１８条第１号ハの規定による重要性Ａの情報資産の管理は、重要性Ａの情報資産管理簿に情報資産の名称、収録情報、保管場所、利用者の範囲を記載して行うものとし、毎月確認することとする。

(2) ポリシー第１８条第２号の規定による情報資産の分類表示は、重要性Ａの情報を記録した記録媒体（システム関連文書を含む。）に、赤色のテープを貼るものとする。

(3) システム管理者は、システムに係るドキュメント及びプログラムを収めた記録媒体

を、施錠可能な場所に保管しなければならない。

(4) 利用者は、情報を記録した記録媒体を庁舎外に持ち出さない。ただし、持ち出さなければ職務の遂行に支障をきたすとして、ポリシー第１８条第６号ただし書の規定により重要性Ｂ以上の情報を記録した記録媒体を持ち出す場合は、情報資産持ち出し管理票により許可を得て行うものとする。

(5) 利用者は、重要性Ａの情報資産を廃棄するときは、重要性Ａの情報資産の廃棄伺いにより許可を得て行うものとする。なお、情報を記録した記録媒体を廃棄するときは、当該情報を消去ソフト等により復元できないように消去し、又はシュレッダー等により粉砕することとする。

(6) 利用者は、重要性Ａの情報資産の廃棄のため業者に引き渡すとき又は賃借期間の終了に伴い情報資産を業者に返却するときは、当該情報を消去ソフト等により復元できないように消去してから引き渡し、又は業者に守秘義務を課して当該情報を復元不可能な状態にさせることとする。

(7) 利用者は、重要性Ａの情報資産を業者に修理させるときは、当該情報を消去ソフト等により復元できないように消去してから引き渡し、又は当該業者に対して守秘義務を課して修理させることとする。

第３章　技術的セキュリティ対策

（管理者権限）

第１１　システムで使用するサーバの管理者権限は、あらかじめシステム管理者が指名する必要最小限の者のみに与えることとする。

２　管理者権限によるサーバのアクセス時間は必要最低限とすることとする。

（パスワード管理）

第１２　発行されたユーザＩＤのパスワードの管理は、次の各号に掲げるとおりとする。

(1) ユーザーＩＤのパスワードは、発行された登録団体が管理するものとする。

(2) 管理者用ＩＤのパスワードは、システム管理者が管理するものとする。

(2) パスワードは、以下の条件によることとする。

ア　８桁以上の半角英数字とすること。

イ　ユーザＩＤと異なること。

ウ　利用者以外の者に知られないようにすること。

エ　必要に応じ変更すること。

(3) 席を外すときはログアウトするなど、セキュリティ対策を実施することとする。

２　サーバの管理者権限のパスワードは、次の各号に掲げる条件により取り扱うこととする。

(1) 半角英数字で８文字以上とし、そのうち半角英数字及び記号を各１文字以上使用すること

(2) 他の者が推測しにくいものとすること。

(3) 管理者権限の使用を認められた者以外の者に知られないようにすること。

(4) 必要に応じ変更すること。
(5) 管理者権限の使用が認められた者が異動、退職等で当該業務を離れる場合は変更すること。

3　システム管理者は、パスワードの不適正使用に関する調査を行い、必要に応じて第１０条による対応を行う。

4　パスワード保管ファイルは、当該ユーザＩＤの利用者以外の者にパスワードが知られないように管理することとする。

（システムの管理）

第１３　システムで使用するサーバの管理を行うにあたり、システム管理者は次の各号に掲げる事項を実施するものとする。
(1) サーバへのアクセス記録を常時取得して、1か月間保管するものとし、必要に応じて分析することにより、異常の有無を調査すること。
(2) 時刻設定をできる限り正確に保つよう措置すること。
(3) 業務に必要のないプロトコルは利用できないよう措置すること。

（ドキュメントの管理）

第１４　システム管理者は、システムに係るドキュメント及びプログラムを収めた記録媒体を、施錠可能な場所に保管しなければならない。

2　職員は、システムに係るドキュメント及びプログラムを収めた記録媒体を外部に持ち出す場合は、ドキュメント等管理記録簿に記録し、システム管理者の承認を得なければならない。

（不正アクセス対策）

第１５　システム管理者は、システムの主要な情報機器等に対し、必要に応じて随時セキュリティ診断を実施し、発見したセキュリティホールは、その緊急度及び影響の重大性に応じて修正プログラムの適応等を行うものとする。

2　システム管理者は、セキュリティホールに関する情報収集に努めるものとする。

（コンピュータウイルス対策）

第１６　システム管理者は、コンピュータウイルスによる被害を防止するため、当該情報機器にコンピュータウイルス対策ソフトを搭載するとともに、当該ソフトを新種のコンピュータウイルスに対応できるように更新していくものとする。

2　システム管理者は、コンピュータウイルスに関する情報収集に努めるものとする。

（私物パソコン等の使用禁止）

第１７　システムの利用者は、私物のパソコン等記録媒体の持ち込み及び使用を行ってはならない。ただし、持ち込み及び使用を行わないことにより職務の遂行に支障をきたすとして、記録に残る形でシステム管理者の許可を得た場合を除く。

第４章　評価及び見直し

（遵守状況の把握、調査・指導等）

第１８　システム管理者は、この要領の遵守状況を把握し、システムの適正な運用を確保するため、必要な調査を実施することができるものとする。

（実施手順の見直し）

第１９　システム管理者は情報セキュリティ監査等の結果、システム運用方法の変更及びポリシー改正に応じて実施手順の見直しを行うこととする。

（委任）

第２０　この実施手順に定めるもののほか、システムの運営管理に関し必要な事項は、システム管理者が定める。

附則

この実施手順は、平成３１年３月２０日から施行する。

附則

この実施手順は、平成３１年４月１日から施行する。

附則

この実施手順は、令和元年１２月１日から施行する。