資料４－２

# 笠間市介護・健診ネットワークシステム
# システム管理規程（未定稿）

# 目次

# 1 総則

## 1.1. 目的

本規程は、「笠間市介護・健診クラウドシステム運用管理規程（以下「運用管理規程」という。）」に準じて、「笠間市介護・健診クラウドシステム（以下「当システム」という。）に関する「システム構成図」に示すシステム及びネットワークの安全な運用及び管理を図るために必要な、運用・保守・事故時の対応等に関する事項を定めることを目的とする。

⇒「笠間市介護・健診クラウドシステム　システム構成図」

## 1.2. 適用範囲

本規程は、笠間市（以下「市」という。）及び当システムに接続する利用者端末及び、当システムで取扱う介護・健診情報に適用する。

## 1.3. 用語および定義

本規程で用いる主な用語及び定義は次の通りとする。

(1) 「事業責任者」とは、当システムに関する最高責任者をいう。
(2) 「参加者」とは、対象者、代諾者、利用機関、利用者をいう。
(3) 「対象者」とは、当システムに自らの介護・健診情報が掲載された市民をいう。
(4) 「代諾者」とは、対象者に十分な同意の能力がない場合に、対象者に代わって同意することが正当なものと認められる対象者の家族、後見人その他これらに準ずる者をいう。
(5) 「利用機関」とは、当システムの利用を市に申請し、利用を許可された介護・健診機関をいう。
(6) 「利用者」とは、当システムを利用することが必要と市が認めた者で、本規程に定める識別番号(以下「ID」という)・パスワードの登録を完了した者をいう。
(7) 「業務利用者」とは、利用者のうち、利用機関に属する者をいう。
(8) 「市民利用者」とは、利用者のうち、対象者及び代諾者その他の業務利用者以外の者をいう。
(9) 「運営管理責任者」とは、当システムの運営・維持等の管理全般についての統括責任者をいう。

# 2 管理体制

## 2.1. 運営事務局・システム管理者

(1) 運営管理責任者は、運営事務局を設置し、当システムの運営実務に当たらせる。
(2) 運営管理責任者は、運営事務局内にシステム管理者を置き、当システムの安全性確保に関して必要な業務を行わせる。

⇒「笠間市介護・健診クラウドシステム運用管理体制図」

### 2.2. 管理する情報の保存期間

当システムが取り扱う情報は、介護・医療機関による最終更新日より○年間、サーバに保管する。

## 3 システム管理者の責務

システム管理者は、関係部署や外部委託先等と協議の上、運営管理責任者の承認を得て、自ら又は外部委託により以下の対策を実施する。

### 3.1. サーバの管理

#### 3.1.1. サーバの導入

(1) 当システムの開発・保守により情報システム機器・ソフトウェア等を導入・取替える場合には、システム要件を明確にするとともに、システムのセキュリティ要件を明確にし、文書化する。

(2) 当システムのリプレース時のデータ移行や関連するデータ交換等、以下の事項の十分な確認を実施する。

① アクセス制御に関する要件の確認
② データ入力権限、入力エラーとする要件、エラー時の対処方法についての必要性の確認
③ データ変更・削除権限、処理順序の制限、障害時の回復処理及び手順等の要件の確認
④ データ出力の方法、装置等に対する要件の確認
⑤ 情報システムの重要度に応じた要件の確認
⑥ 既存システムへの影響（サーバ、ネットワーク等）の有無の確認

#### 3.1.2. サーバの物理的保護

(1) 介護・健診情報を取扱うサーバ等に対する安全管理上の脅威（盗難・破壊・破損等）や、環境上の脅威（地震、漏水、火災、停電等）から以下に従って物理的に保護する。

① サーバ室など隔離されたエリアへの設置
② 隔離されていないエリアに設置する場合は、常時施錠可能なラック等への収容
③ 耐震性、防火性、防水性を考慮した設置
④ 無停電電源装置の設置
⑤ 温度・湿度等の管理

(2) 導入・取替えサーバをサーバ室等のセキュリティが保たれた管理領域に設置する。

#### 3.1.3. サーバ室の入退管理

(1) サーバ室の出入口は常時施錠管理し、その入退室を記録・管理する。

(2) サーバ室等は、スタッフの常駐または施錠できる部屋に設置する。
(3) 承認なしにはサーバ室等に立ち入ってはならない。
(4) 全てのサーバ室等への入退者は、名札を着用し、入退の記録を残す。
(5) 入退の記録は定期的に確認し、問題があれば事業責任者に報告する。

### 3.1.4. サーバの運用

(1) サーバへのアクセス状況・稼動状況を定期的（月１回以上）に確認し、問題がある場合は、速やかに措置を講じる。
(2) 個々のサーバ及び端末機のクロックを定期的（月１回以上）に確認するとともに、誤差が生じている場合は標準時間に設定し直す。

## 3.2. アクセス管理

利用機関別にアクセス範囲を定め、必要に応じてハードウェア・ソフトウェアの確認を行う。また、以下の内容に沿って、アクセス管理を行い、定期的に管理状況を運用責任者に報告をする。

(1) 情報区分とアクセス権限に基づくアクセスできる診療録等の範囲を定め、アクセス管理を行う。
(2) ＩＤ・パスワード等により介護・医療情報へのアクセスにおける識別と認証を行う。
(3) ＩＤには原則として管理者権限は付与しない（ユーザ権限とする）。ただし、サーバ管理のために必要な場合は、システム管理者の承認の上、管理者権限を付与する（原則２名とする）。
(4) Administrator 等の OS のディフォルト ID は使用せず、個別 ID とする。
(5) 当システムの使用状況を監視するため、以下の事項を含むアクセスログを取得する。異常なアクセスがあったときは、ネットワークを切断する等の処置を行う。
・利用者ＩＤ
・端末ＩＤ
・操作の日時
・データへのアクセス結果（誰が、いつ、誰の情報に、どのようなアクセスをしたか）
(6) 取得したアクセスログを定期的に検証し、問題がある場合は、速やかに措置を講じる。
(7) 取得したアクセスログは、情報システムの重要度に合わせ定期的（月１回以上）に検証し、問題のないことを確認する。問題がある場合は、速やかに適切な措置を講じる。
(8) アクセスログは、重要度に合わせ定めた方法・場所・期間に従い保管する。

## 3.3. データのバックアップ

(1) 情報システムの重要度に応じて、システムファイル及びデータのバックアップを定期的に取得する。
(2) バックアップの作業に当たる者は、その作業の記録を残し、運営管理責任者の承認を得る。

(3) バックアップ媒体は、施錠できるキャビネット、耐火金庫等に保管し、その所在を台帳に記録し、管理する。
(4) バックアップ媒体は１年間に１回新品に交換する。媒体に品質の劣化が予想される場合や、劣化原因と思われる障害が発生した場合は、直ちに新品に交換を行う。
(5) 部門管理者は、記録媒体及び機器のログを確認し、記録媒体の劣化や機器の不具合を確認する。エラー・警告のログが発見された場合は、直ちに新品の記録媒体に記録を複写すること。
(6) 情報がき損した時に、バックアップされたデータを用いてき損前の状態に戻せることことを確認し、リストア手順を規定する。

### 3.4. ネットワーク管理

(1) 当システムにアクセスするためのネットワークは、インターネット等の外部ネットワークとはファイアーウォールなどのネットワーク機器によって区分する。
(2) 当システムへ接続を行う場合、利用機関、市民利用者は、市に申請し、承認を得る。
(3) 当システムを利用できる情報システムを制限・管理し、許可されていない情報機器の接続を制御する。

## 4 災害等含めたシステム障害発生時の対策

### 4.1. 適用範囲

この規定は、当システムのシステム障害における、介護・医療サービスへの影響、個人情報の漏洩、滅失、き損等に関する事件・事故及び事件・事故の恐れがある場合（以下「事故」という。）について適用する。

### 4.2. 責任と権限

(1) 事業責任者
当システムにおける事故の全責任を負い、状況調査、原因究明、復旧管理及び関係者への報告等の責任及び権限を持つ。
(2) 運営管理責任者
事故の管理責任を負うものとし、状況調査、原因究明及び復旧管理を行う。
(3) システム管理者
自らの管理するシステムにおける事故の管理責任を負うものとし、状況調査、原因究明及び復旧管理を行う。
(4) 利用機関管理責任者
自らの管理する利用医療機関における事故においては管理責任を負うものとし、状況調査、

原因究明及び事故対応の支援を行う。

### 4.3. 緊急事態のレベル

緊急事態は事故の内容に以下のように分類し、それぞれ適切な対応を図る。

レベル５：個人情報の漏洩、改ざん、破壊等があった場合、その恐れがある場合
レベル４：当システム全端末でアクセスできない場合、その恐れがある場合
レベル３：当システム内の情報が閲覧できない、一部端末からアクセスできない場合
レベル２：利用端末が起動しなくなった、操作不能になった場合
レベル１：事故は発生していないが、将来的に発生する可能性がある事象が発見された場合

### 4.4. 緊急時連絡

利用機関は、当システムが正常に稼働しなかった場合等は、直ちに運営事務局に報告することとする。

### 4.5. 緊急時対応手順

(1) 事故が発生した場合、その状況に応じ、運営管理責任者、運営事務局及びシステム管理者は、障害レベルを判別し、必要な対応を講じる。

(2) システム障害が介護・医療活動に重大な影響を及ぼすものはない場合でも、障害レベル３以上の場合、または、運用に大きな影響が生じる思われる場合は、システム管理者にその旨を報告する。特にレベル４に相当する場合は、緊急に運営管理責任者に報告し、指示に従う。

システム管理者は、障害レベルにより必要な対応を取るとともに、運営管理責任者に報告する。

### 4.6. 事故発生時の対策

(1) 事業責任者は、情報の安全性を侵害する事故が発生した場合は、以下の対策を講じるものとする。

① 事故拡大を防ぐための措置
② ログ情報等の解析及び事故の原因解明
③ 被害状況の調査
④ 対策の検討及び実施
⑤ 復旧確認後の運用再開及び安全宣言の周知
⑥ 再発防止策の検討及び実施
⑦ 必要な情報について関係部署や外部機関への連絡届出

(2) 利用機関管理責任者は、情報の安全性を侵害する事故が発生した場合は、次に掲げる適切な対策を講じるものとする。

① 事業責任者への連絡
② 当システムの利用中止
③ 事故拡大を防ぐための措置
④ 被害状況の調査
⑤ 対策の検討及び実施
⑥ 事故からの復旧が確認できた場合の事業責任者への報告
⑦ 復旧確認後の利用再開及び安全宣言の周知
⑧ 再発防止策の検討及び実施
⑨ 必要な情報について事業責任者への報告及び関係部署への連絡届出

### 4.7. 応急措置及び関係者への連絡

運営事務局は、個人情報の漏洩など、本人への影響が予測される場合は、事故の影響範囲拡大防止のための応急措置を講じ、必要に応じて、関係機関への通知と該当者本人への対応措置を講じる。

### 4.8. 報告、公表

事業責任者は、事故の重大さに応じて、事故の内容、原因、処置結果等を公表するか否か判断し、必要な場合は、外部に公表する。

## 5 業務委託の安全管理措置

### 5.1. 委託契約（保守管理含む）における安全管理

当システム運営・保守業務を外部業者に委託する場合は、以下の措置を実施する。

(1) 守秘事項を含む業務委託契約を結ぶ。
(2) 各担当者は委託作業内容が個人情報保護の観点から適正にかつ安全に行われていることを確認する（委託先が、許可無く個人情報を含むデータを組織外に持ち出すことは禁止する）。
(3) 業務委託の契約書には、次に示す事項を規定し、十分な個人情報の保護水準を担保する。
① 委託者及び受託者の責任の明確化
② 個人情報の安全管理に関する事項
③ 再委託に関する事項（再委託する事業者にも委託先と同等の義務を課すこと）
④ 個人情報の取扱状況に関する委託者への報告の内容及び頻度
⑤ 契約内容が遵守されていることを委託者が確認できる事項
⑥ 契約内容が遵守されなかった場合の措置
⑦ 事件・事故が発生した場合の報告・連絡に関する事項
⑧ 一連の委託業務終了後に関する事項（終了報告、確実にデータを消去する等）
⑨ 保守要員のアカウント情報の管理に関する事項（適切に管理することを求める）

### 5.2. リモートメンテナンス時の安全管理

(1) 外部業者からのリモートメンテナンスを受ける場合、相手の保守会社等、通信事業者、運用委託業者等との間で、責任分界点や責任の所在を契約書等で明確にする。

(2) 適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止する。

### 5.3. 委託先への監査

運営管理責任者は、上記契約状態が適切に維持管理されているか定期的に監査を行って確認することができる。

## 6 事業責任者による見直し

事業責任者は、当システムの運用を維持するために、必要に応じ本規程を見直す。見直しにおいては、次の事項を考慮する。

① 監査及びシステム管理者の運用状況に関する報告
② 苦情を含む外部からの意見
③ 前回までの見直しの結果に対するフォローアップ
④ 安全管理ガイドライン等の標準規格や法令等の規範の改正状況
⑤ 社会の情勢等の変化、国民の認識の変化、技術の進歩などの諸環境の変化
⑥ 情報システムの運用状況の変化
⑦ 内外から寄せられた改善のための提案

## 7 附則

本規程の施行日は、2013 年　　月　　日とする。