防府市マイナ救急システムに係る安全対策要綱

令和７年５月26日制定

（趣旨）

第１条　本要綱は、総務省消防庁が定めるマイナ救急システムセキュリティガイドライン（以下「マイナ救急システムセキュリティガイドライン」という。）に基づき、防府市消防本部（以下「当消防本部」という。）がマイナ救急システム（以下「本システム」という。）を適切に運用するために必要となる基本的な事項を定めるものとする。

２　本システムからの情報閲覧に当たって使用される機器、端末、ソフトウェア等の適正な取扱いに関して必要な事項を定めるとともに、本システムで取り扱う傷病者の資格に係る情報及び薬剤情報・診療情報・特定健診情報の閲覧のサービス（以下「本サービス」という。）に係る個人情報の適正な管理に関して必要な事項を定めるものとする。

（組織・体制）

第２条　当消防本部に、本システム管理者（以下「システム管理者」という。）を置き、消防長をもって、これに充てる。

２　消防長は、必要な場合、システム管理者を別に指名することができる。

３　当消防本部に、本システムに関する情報管理責任者を置き、警防課長をもって、これに充てる。

４　各救急隊における利用者の中から情報閲覧責任者（以下「閲覧責任者」という。）を置き、救急隊長をもって、これに充てる。

５　本システムの利用者は、救急業務に関する講習で総務省令で定めるものの課程を修了した者、若しくは同等以上の学識経験を有する者として総務省令で定める者とする。

６　システム管理者は、緊急時及び災害時の連絡、復旧体制及び回復手順を定めるとともに、非常時においても当該文書等を参照できる

よう適切に保管する。

（システム管理者の責務）

第３条　システム管理者は、本システムに関する救急時医療情報閲覧用端末の設定変更、更新を行う管理者権限等これらの情報閲覧における最終的な責任を負うものとする。

２　システム管理者は、救急時医療情報閲覧用端末やソフトウェアに変更があった場合にも、利用者が救急業務においてマイナ救急を実施できるよう、環境を整備するものとする。

３　システム管理者は、本システムを正しく利用させ、個人情報及び重要情報の思わぬ漏えいを防ぐために、閲覧方法について、教育・訓練計画等を定めた上で、情報管理責任者、閲覧責任者及び利用者の教育と訓練を行うものとする。

４　システム管理者は、情報管理責任者、閲覧責任者及び利用者に対し、本システムの運用における指揮を行うものとする。

５　システム管理者は、情報管理責任者、閲覧責任者及び利用者の本要綱の順守に責任を負うものとする。

（情報管理責任者の責務）

第４条　情報管理責任者は、本システムで取り扱う傷病者の個人情報の適正な管理に関する責任を負うものとする。

２　情報管理責任者は、本システムで取り扱う情報について、組織内で重要性の度合いを共有するため、各々の情報の機密性を踏まえ、地方公共団体における情報セキュリティポリシーに関するガイドライン（令和６年10月版）や次の重要性分類例を参考とし、当消防本部・管轄市町村におけるセキュリティポリシーに則り重要性分類を定義することとする。

厳秘	機密性が極めて高い情報の種別（例：薬剤情報、診療情報、特定健診情報）
秘密	特定の範囲に限り開示することができる機密性が高い情報の種別（例：実施手順書）

公開	広く一般に公開可能である情報の種別

3　情報管理責任者は、本要綱に定める重要性分類及び当消防本部・管轄市町村におけるセキュリティポリシー等に則りシステムの資産管理を行い、常に最新の資産管理状況に更新するものとする。

4　情報管理責任者は、本システムを正しく利用するための教育と訓練を受けるものとする。

5　情報管理責任者は、特に、本システム導入時、適切に管理されていないメディア使用時、又は外部からの情報受領時においては、コンピュータウイルス等の不正なソフトウェアが混入していないか確認するものとする。

6　情報管理責任者は、本システムの取扱いに当たり、マイナ救急システムセキュリティガイドライン、実施手順書、運用手順書等について利用者に周知の上、常に利用可能な状態にしておくものとする。

7　情報管理責任者は、ネットワークの不正な利用を発見した場合には、直ちにその原因を追求し対策を実施するものとする。

8　情報管理責任者は、関係者以外の者による覗き見を防止するため、端末にスクリーンフィルタを設置する等の対策を施すものとする。

（閲覧責任者の責務）

第５条　閲覧責任者は、本システムの閲覧に当たって使用される機器、端末、ソフトウェア等の適正な取扱い、閲覧者の管理に関する責任を負うものとする。

2　本システムの救急時医療情報閲覧用端末は、マイナ救急やその他救急に係る事務において使用する。したがって、閲覧責任者はマイナ救急やその他救急に係る事務に必要とするソフトウェア以外のソフトウェアがインストールされていないことを確認するものとする。

3　閲覧責任者は、本システムで使用する救急時医療情報閲覧用端末

にコンピュータウイルス対策ソフトウェアがインストールされていることを確認するとともに、ＵＳＢメモリ（使用する場合のみ）と併せて、定期的にコンピュータウイルスのチェックを行い、感染の防止に努めるものとする。

4　閲覧責任者は、ウイルス感染が疑われた場合、直ちにネットワークを遮断し、使用を禁止するものとする。

5　閲覧責任者は、本システムを正しく利用するための教育と訓練を受けるものとする。

6　傷病者の医療情報を閲覧する前に、本システムで閲覧可能な情報、閲覧の目的等について傷病者に説明し、同意取得の上で医療情報を閲覧するものとする。ただし、意識不明時等同意取得が困難である場合はこの限りでない。

7　閲覧責任者は、各救急事案における本システムへのログイン・医療情報の閲覧に関する責任を負うものとする。

8　閲覧責任者は、自身の責任・管理下のもと、閲覧責任者以外の利用者にも本システムへのログインを行わせることができるものとする。また、本システムへログインした者以外の利用者にタブレットに表示された医療情報画面を閲覧させることができるものとする。なお、ログインした者については、台帳や救急活動記録表への記載等の手段を用いて管理できるよう措置を講じること。

9　マイナ救急やその他救急に係る事務に関する目的以外でタブレットの貸出しを行わないこと。

10　閲覧責任者は、利用者でもあるため、第６条　利用者の責務に定める内容も遵守するものとする。

（利用者の責務）

第６条　利用者は、マイナ救急システムセキュリティガイドライン、実施手順書、運用手順書等に定められている事項を遵守するものとする。

2　利用者は、マイナ救急やその他救急に係る事務に関する目的以外

で機器、端末、ソフトウェア等を使用しないものとする。

3　利用者は、本システムを正しく利用するための教育と訓練を受けるものとする。

4　利用者は、職務上知り得た個人情報を漏らさないものとする。その職を辞した後も、同様とする。

5　利用者は、個人情報の漏えい及び改ざんが生じた場合又はそれらが生じる恐れがある場合には、速やかに閲覧責任者に連絡し、その指示に従うものとする。

6　利用者は、救急時医療情報閲覧用端末及び機器の盗難、紛失などが生じた場合はマイナ救急システムセキュリティガイドライン、実施手順書、運用手順書等に定められた手順で対応を行うものとする。

7　利用者は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかに情報管理責任者に相談するものとする。

8　利用者は、本システムで取り扱う情報については、当消防本部内において機密性を踏まえ定義した重要性分類に従って、取扱いを行うものとする。

9　利用者は、関係者以外の者が不正に本システムを利用できないようにユーザＩＤ及びパスワード等を、本人しか知り得ない状態に保つように適切に管理するものとする。

10　利用者は、パスワードについて、類推しやすい文字列、極端に短い文字列、類似の文字列を繰り返し使用しないものとする。

11　利用者は、救急時医療情報閲覧用端末のスクリーンショット機能を用いて救急業務用オンライン資格確認等システム上のデータを撮影・切取りをしないこととする。

（救急時医療情報閲覧用端末機器の遵守事項）

第７条　利用者は、救急時医療情報閲覧用端末及び機器を用いる救急現場に関係者以外が入らないようにすること。

2　利用者は、救急時医療情報閲覧用端末及び機器を無人状態で放置せず、使用しないときでも救急車等施錠可能な環境で施錠の上保管する。その際、安定した場所で落下等の危険がないように保管すること。

3　利用者は、本サービスを利用した救急活動の完了時、救急時医療情報閲覧用端末上の傷病者の医療情報が表示された画面を閉じること。

4　利用者は、端末を利用しない場合には救急時医療情報閲覧用端末にて本システムからのログオフ処理を行い、再び利用する場合は改めてログインすること。

5　情報管理責任者及び閲覧責任者は、救急時医療情報閲覧用端末及び機器の所在を台帳や救急活動記録表への記載等の手段を用いて管理し、定期的に確認し、適切に持ち出し状況が管理されていることを確認すること。

6　利用者は、救急時医療情報閲覧用端末のＢｌｕｅｔｏｏｔｈ機能を業務上必要な場合を除いてオフとすること。Ｂｌｕｅｔｏｏｔｈ機能を用いる場合はデバイス名に機密情報や、救急隊のデバイスであることがわかる情報を含めないこと。

7　利用者は、医療情報閲覧に当たり公衆無線ＬＡＮを利用せず、当消防本部が契約したインターネット回線及びオンライン資格確認ネットワークを利用すること。閲覧責任者は、万が一医療情報閲覧に当たり公衆無線ＬＡＮが利用されたことを覚知した際には、アンチウイルスソフトウェアを用いて救急時医療情報閲覧用端末へのウイルスチェックを行い、安全が確認されるまで当該端末は使用しないこと。

8　閲覧責任者は、救急車外に救急時医療情報閲覧用端末を持ち運ぶ際、火災、大雨等で端末が故障しやすい状況であると判断した場合には、そのリスクに応じた措置を講じた上で使用するか、又は、救急車内での利用とする等適切に判断すること。

９　閲覧責任者は、故障予防のため機器（救急時医療情報閲覧用端末、カードリーダー）に対する外形点検、動作点検、ソフトウェアの最新バージョンへの更新等、故障を予防するための保守点検を定期的に実施すること。

（救急時医療情報閲覧用端末機器の盗難、紛失時の対応）

第８条　救急時医療情報閲覧用端末及び機器の盗難、紛失が発生した場合には、利用者はシステム管理者及び情報管理責任者に対し直ちに報告を行うこと。

２　救急時医療情報閲覧端末の紛失・盗難の報告を受けた情報管理責任者は、当該の救急時医療情報閲覧用端末に対しＭＤＭのリモートデータ削除機能を用いて当該の救急時医療情報閲覧用端末を工場出荷状態にまで初期化を行うこと。

３　ＵＳＢセキュリティキー等の物理媒体の紛失・盗難の報告を受けた情報管理責任者は、当該ＵＳＢセキュリティキー等の物理媒体をログイン時の認証情報として利用している救急時医療情報閲覧用端末の二要素認証情報の削除・利用停止を行うこと。

４　情報管理責任者は、総務省消防庁の問い合わせ窓口に盗難、紛失の発生状況・経過、事由等を報告すること。

５　利用者は、本要綱に定める事項及び当消防本部・管轄市町村におけるセキュリティポリシー等の事項に則り盗難、紛失に適切に対処すること。

（要綱に対する違反への対応）

第９条　システム管理者は、本要綱に定める事項及び当消防本部・管轄市町村におけるセキュリティポリシー等の事項に対する違反があった場合の対処方法について明確にするとともに、それに従って、厳正に対応すること。

（評価・見直し）

第10条　システム管理者は、本要綱に定める事項及び当消防本部・管轄市町村におけるセキュリティポリシー等を評価し、必要に応じ

て、定期的に見直すこと。

（その他）

第11条　適切なセキュリティ対策を図るために、当消防本部は「別表：本システム導入のために特に留意すべきセキュリティ対策」に示す技術的対策等を行うこと。

２　本要綱の実施に関し必要な事項がある場合については、システム管理者がこれを定めること。

附　則

この要綱は、令和７年５月26日から適用する。

別表：（第１１条関係）本システム導入のために特に留意すべきセキュリティ対策

番号	セキュリティ対策
1	本システムへのアクセスについては、利用者の識別と認証を行うこと。
2	本システムを導入する際は、オンライン請求ネットワークを利用し、ネットワーク経路でのメッセージ挿入、コンピュータウイルス混入等の改ざんを防止する対策を行うこと。その際は、ＩＰｖ６接続を推奨する。
3	本システムを導入する際は、コンピュータウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
4	本システムの閲覧に当たって使用される機器、端末等において、接続できる外部記憶媒体（ＵＳＢメモリ等）の制限を実施すること。
5	本システムを導入する際は、外部ネットワークから本シス

	テムへのアクセスを制限する仕組みを導入し、ネットワーク事業者に対して外部ネットワークからのアクセスを制限する仕組みが導入されていることを確認すること。
6	本システムを導入する際は、消防本部内部ネットワークにおいても、セキュリティ要件の異なるシステム間や安全管理上の重要部分との境界にはファイアウォール等を設置し、ネットワークを物理的又は論理的に分割すること。
7	本システムの導入に当たり無線ＬＡＮを利用する場合は、以下の対策を実施すること。 ・パブリック設定かつゲスト向けに設定されたアクセスポイントの使用を推奨すること。 ・ゲスト用Wi-Fi設定の名称は、「ゲストポート」「ゲストＷｉ-Ｆｉ」「ゲストネットワーク」などになっていること。 ・プライバシーセパレータ機能（接続している機器同士のアクセスを遮断する機能）を有効にすること。 ・安全な無線暗号化方法を使用すること（ＷＰＡ３での暗号化を推奨）
8	本システムを導入する際は、ネットワーク事業者に対して、消防本部間との通信を制限する仕組みを導入していることを確認すること。
9	本システムを導入する際は、認証に用いられる手段の強化として、救急時医療情報閲覧用端末へのログインに二要素認証を採用すること。
10	本システムを導入する際は、盗難、置き忘れ等に対応する措置として、救急時医療情報閲覧用端末の起動パスワードを設定する等、容易に内容を読み取られないようにすること。
11	本システムを導入する際は、端末の位置情報・異常を検知

	し、紛失や盗難が発覚した場合、遠隔から端末のデータをリモートで消去する機能（ＭＤＭ等）を搭載すること。
12	本システムを導入する際は、救急時医療情報閲覧用端末上にＰＨＩをダウンロードさせない機能を搭載すること。その際、システムにアクセスするブラウザは常にプライベートモードで起動することで、閲覧キャッシュが残らないように設定すること。具体的には、ブラウザのプロパティからショートカットタブを開き、″リンク先(Ｔ):″項目に既に入力されている内容末尾に″-ｐｒｉｖａｔｅ″を追加すること。
13	本システムを運用する際は、一般に公開された脆弱性に対処するため、業務に影響が出ない範囲でＯＳのセキュリティパッチを適切に適用すること。
14	本システムでは、必要なアプリケーションのみをインストールし、不要なアプリケーションは削除すること。また、ＯＳの標準機能や開いているネットワークポートを精査し、マイナ救急やその他救急に係る事務に不要な機能については削除あるいは停止すること。