別紙２　非機能要件定義書

No.	大項目	中項目	小項目	機能概要
1	ユーザビリティ及びアクセシビリティに関する事項	ユーザビリティ	Webブラウザの利用	Webブラウザから利用可能なこと。
2	ユーザビリティ及びアクセシビリティに関する事項	ユーザビリティ	Webブラウザの汎用性	特定のWebブラウザが保有する機能に依存せず、利用可能なこと。Webブラウザの機能拡張等の操作を必要としないこと。
3	ユーザビリティ及びアクセシビリティに関する事項	ユーザビリティ	可搬性携帯端末等からの利用	・消防・医療機関用インターフェースにおいて、タブレット等の可搬性携帯端末、パソコンでの利用を考慮したインターフェースとなっていること。 ・タブレット等の可搬性携帯端末を用いて簡便かつ迅速な情報入力が可能であること。
4	ユーザビリティ及びアクセシビリティに関する事項	ユーザビリティ	画面の構成	・表示画面上の項目配置や配色等、利用しやすいユニバーサルなデザインとすること。 ・無駄な情報、デザイン及び機能を極力排除し、簡潔で分かりやすい画面とすること。 ・十分な視認性のあるフォント及び文字サイズとすること。 ・画面上でのピンチイン・ピンチアウトやブラウザの表示サイズ変更等による、画面・文字の大きさをユーザー自身で変更可能な設定とすること。
5	ユーザビリティ及びアクセシビリティに関する事項	ユーザビリティ	操作方法やその指示の分かりやすさ	・無駄な手順を極力排除し、最小限の操作でユーザーが使用できること。 ・操作の指示、説明、メニュー等は、ユーザーが正確にその内容を利用できるような用語の使用とすること。 ・各操作の留意点や重要度をユーザーが認識できるような文字やボタンの色・サイズとすること。 ・情報システムに詳しくないユーザーでもマニュアル等を参照せず直感的に操作することで利用可能なインターフェースとすること。 ・医療機関側の画面ではWCAG2.2を考慮した操作性とすること。
6	ユーザビリティ及びアクセシビリティに関する事項	ユーザビリティ	エラー防止と処理	・ユーザーが操作を間違えないようなデザインや案内表示とすること。 ・入力内容の形式に問題がある際に、ユーザーがその都度その対象項目を容易に見つけられるような強調表示とすること。 ・重要な処理を行う前に注意喚起する画面・メッセージの表示とすること。 ・エラーが発生したときは、ユーザーが容易に問題を解決できるようなエラーメッセージの表示とすること。
7	ユーザビリティ及びアクセシビリティに関する事項	ユーザビリティ	ヘルプ・サポート	・ユーザーが操作に迷った際に、操作方法を参照できるような簡易ガイドや詳細な操作説明書・マニュアルを作成すること。 ・実証開始時にユーザーが 本システムをスムーズに利用開始できるような実証開始前の操作研修・説明会を開催すること。
8	ユーザビリティ及びアクセシビリティに関する事項	アクセシビリティ	言語	・画面上に表示する言語は日本語を基本とすること。 ・ユーザーからの質問や回答等については、日本語のテキスト情報に基づき、行うことができること。
9	ユーザビリティ及びアクセシビリティに関する事項	アクセシビリティ	障害等への配慮	ウェブアクセシビリティ導入ガイドブックに準じ、視覚等に障害のあるユーザーに対しても、アクセシビリティが確保されていること。
10	ユーザビリティ及びアクセシビリティに関する事項	アクセシビリティ	文字サイズ	文字サイズをWebブラウザの設定等により拡大・縮小でき、拡大表示した際も問題なく画面表示、操作ができること。
11	機能仕様に関する事項	アーキテクチャ	構築基盤	将来的な全国展開を見据えた機能・画面の迅速な拡張性や柔軟性を確保するために、主にローコードツールで構築すること。
12	機能仕様に関する事項	拡張性	仕様強化・拡張性	・救急業務を取り巻く環境変化に柔軟に対応し、機能増強・拡充が容易に（費用や期間含め）実施できるものとすること。 ・将来における新技術の導入（アプリケーション化等）や新たな機器・端末の追加、事務処理の変更などに柔軟かつ迅速に対応できる拡張性の高いシステムであること。
13	規模に関する事項	利用者数	同時接続	本業務に参加する救急隊及び医療機関からの同時接続が可能であること。
14	規模に関する事項	利用者数	消防救急隊	・本調達仕様書13頁を参照。 ・各救急隊に 1 台の可搬性携帯端末を配布（救急隊が使用する端末同等仕様を指令端末として各消防本部（局）に配布）。
15	規模に関する事項	利用者数	医療機関	・本調達仕様書13頁を参照。 ・各医療機関に 1 台の可搬性携帯端末を配布（三次救急医療機関には、二次・三次用にそれぞれ１台配布）。
16	性能に関する事項	性能目標値	レスポンスタイム	サービスの品質を確保するため、開発時にはサービスの目標応答速度を掲げ、それを達成するための開発を行うこと。
17	性能に関する事項	継続性	目標復旧時間	サービスの停止を検知してからの目標復旧時間を定め、それが実現可能な構成で設計・開発を行うこと。
18	性能に関する事項	可用性	稼働時間	サービスの利用可能時間はデータ更新のタイミングやメンテナンス等による計画的な停止を除き24時間365日を基本とすること。なお、定期又は随時のメンテナンスの日時については、 救急業務に比較的影響を与えたない時間帯とし、発注者と十分に事前に協議の上、システム利用者に対して事前に周知をすること。また、その際、システムの停止時間は１時間程度とすること。
19	情報セキュリティに関する事項	方針	適用範囲	情報セキュリティに関する事項の適用範囲は、原則、本調達範囲の全てとする。なお、本システムの構築において利用するクラウドサービスについては、要件を満たしているサービスを選定すること。
20	情報セキュリティに関する事項	方針	基本的要求事項	本システムの構築においては、クラッカー（悪意を持って情報セキュリティシステムを破壊・改ざんする者）による攻撃や、マルウェア（情報セキュリティシステムに影響を与える不正なソフトウェア）の 影響を受けたクライアント端末やサーバ等を踏み台にした攻撃等のセキュリティリスクに対処し、システム停止や、情報の漏えい・毀損等を防ぐための有効な対策を講じること。
21	情報セキュリティに関する事項	方針	通信の暗号化	・通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、クラウドサービス等庁外のネットワーク上に構築された情報システム間の接続においては、 暗号化を実施した上で、原則として専用回線を利用すること。また、専用回線が利用できない際には、通信事業者が提供する閉域網を利用したVPN（IP-VPN）を利用し閉域接続を行うこと。 ・クライアント端末とサーバ間の通信内容はSSL/TLS等により暗号化すること。なお、証明書発行・更新等に要する手続きは受注者にて実施すること。
22	情報セキュリティに関する事項	方針	外部Webサイト	IPAが公開する最新の「安全なウェブサイトの作り方」（https://www.ipa.go.jp/security/vuln/websecurity.html)に基づき適切な対策を講じること。
23	情報セキュリティに関する事項	不正対策	不正な通信の遮断・検知	本システムで利用しない機能、ポート、ユーザ等を無効化し、不正な通信を遮断・検知すること。
24	情報セキュリティに関する事項	不正対策	ログの取得	本システムに対する不正の検知、発生原因の特定ができるようにするため、本システムに対するアクセス・認証、アカウント管理、例外的事象等に関する証跡を蓄積する機能を有すること。
25	情報セキュリティに関する事項	不正対策	ログの保存期間	ログデータの保存期間については費用対効果等を勘案したうえで、本県と協議を行い決定すること。なお、システム内のデータは発注者等の求めに応じて速やかに提供できるようにすること。
26	情報セキュリティに関する事項	不正対策	不正プログラム対策	・本システムの稼働環境及び開発・テスト環境においては、コンピュータウィルス等不正プログラムの侵入や外部からの不正アクセスが起きないよう対策を講じるとともに、 それらの対策で用いるソフトウェアは常に最新の状態に保つこと。 ・本システムの稼働環境及び開発・テスト環境で用いるOSやソフトウェアは、不正プログラム対策に係るパッチやバージョンアップなど適宜実施できる環境を準備すること。
27	情報セキュリティに関する事項	不正対策	その他セキュリティ対策	個人情報の保護に配慮するなど、利用者が安心して利用できる対策を実施していること。
28	情報セキュリティに関する事項	障害対策	障害対応	・24時間体制でシステム稼働状況の監視による故障の検知、分析、切り分け対応、障害復旧対応等を行うこと。 ・重大障害発生時（業務利用不可等）には、各消防・医療機関に障害発生の連絡を行うこと。また、復旧時には各消防・医療機関に復旧連絡を行うこと。 ・万一のシステム停止や通信不可等、現場での業務が困難になった場合の救急業務の継続運用についても想定すること。
29	情報セキュリティに関する事項	クラウドサービス	暗号化	クラウドサービス上に保存されるデータについては暗号化すること。
30	情報セキュリティに関する事項	クラウドサービス	リージョン	利用するクラウドサービスについては、国内法が適用されることとするため、国内リージョンのものを選定すること。
31	情報セキュリティに関する事項	クラウドサービス	必要な認証	・クラウドサービスを利用する場合は、ISO/IEC 27001（ISMS）適合性評価制度の認証を取得していることに加え、以下のいずれかを満たすこと。 ・ISO/IEC27017を取得していること。 ・ISMAPクラウドサービスリストに登録されているクラウドサービスを利用すること。
32	情報セキュリティに関する事項	クラウドサービス	必要な認証（個人情報含む場合）	・クラウドサービスを利用する場合に加え、クラウドサービス上で個人情報を取り扱う場合には、ISO/IEC 27001（ISMS）適合性評価制度の認証を取得していることに加え、 以下のいずれかを満たすこと。 ・ISO/IEC27017及びISO/IEC27018を取得していること。 ・ISMAPクラウドサービスリストに登録されているクラウドサービスを利用すること。
33	情報セキュリティに関する事項	クラウドサービス	データセンター	・データセンターは、日本データセンター協会が制定するデータセンターファシリティスタンダードのティア３相当の基準を満たした設備とすること。 ・データセンターの物理的所在地を日本国内とし、情報資産について、合意を得ない限り日本国外への持ち出しを行わないこと。
34	情報セキュリティに関する事項	クラウドサービス	個人情報・情報セキュリティの遵守	・個人情報保護法及び本調達仕様書に定める本県情報セキュリティポリシーを遵守すること。 ・ISMS認証またはプライバシーマークを取得していること。
35	情報セキュリティに関する事項	クラウドサービス	データ管理	・デバイス内には情報は保有せず、サービス提供クラウド環境（データセンター内）でデータを保有すること。 ・情報資産は発注者が指示しない限り日本国内に保管されること。 ・データのバックアップを実施すること。
36	情報セキュリティに関する事項	クラウドサービス	データ引継	端末故障時や機種変更時のデータ引継ぎが配慮がされていること。
37	情報セキュリティに関する事項	契約終了時の対応	データ提供	本システム運用開始後に利用者が入力、登録した情報のうち、本県に情報管理権限がある情報については、契約終了後全て抽出し発注者に提供すること。
38	情報セキュリティに関する事項	契約終了時の対応	データ消去	クラウドサービスの利用終了後等に、クラウドサービスで取り扱った情報を消去する場合には、暗号鍵を削除するなどの簡易かつ確実な対応により、保存した情報を復元困難とする管理を行うこと。
39	情報セキュリティに関する事項	契約終了時の対応	オプトアウト	利用者からの申し出により、当該利用者に関する情報を全部または一部削除できる機能を有すること。
40	情報セキュリティに関する事項	関係法規制等への対応	プライバシーポリシー	プライバシーポリシーを表示すること。
41	情報セキュリティに関する事項	関係法規制等への対応	関係法規制の遵守	・本システムについては、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン1.1版」に準拠すること。また、救急医療情報連携プラットフォームについては、 「医療情報システムの安全管理に関するガイドライン第6.0版」に準拠すること。 ・本システムの稼働、運用・提供に関係する関係法規制を遵守するとともに、常に最新動向を把握し、適宜必要な見直し・改善を実施すること。
42	情報セキュリティに関する事項	アカウント管理	アクセス	救急医療情報連携プラットフォームの利用者及び管理者（システム提供事業者）は、多要素認証（知識認証、物理認証、生体認証のうち異なる2つ以上の要素を用いる認証方式）により ログインすることができること。なお、民間救急システムにおいては、可能な限り早期に多要素認証を採用すること。
43	情報セキュリティに関する事項	アカウント管理	利用制限	・本システムを構築する権限設定により、ユーザーの権限ごとにアクセスできるデータが制御できること。 ・管理者（システム提供事業者）が利用者のアカウント情報を確認、修正、削除ができること。 ・各利用者IDの権限を個別に設定し、必要な機能のみを操作・閲覧可能とすることが可能であること。
44	情報セキュリティに関する事項	アカウント管理	利用状況	システムの運用状況や利用状況などの統計情報を定期又は任意の時点で集計し、システム上で消防・医療機関等が確認できること。