（注）
本文中又は別紙中「【※検討中】」と表記する箇所は、今回の意見募集段階では検討中のためお示ししないが、発出の際に追記予定である。
なお、当該部分にも別紙を設定する可能性があるため、意見募集段階においては、別紙番号を仮としてアルファベットで表記する。また、追記する場合には、「遵守」類型に相当する内容は含まれない見込みである。

医科診療所向け
電子カルテ及びレセプトコンピュータ
標準仕様書（基本要件）（案）
【第X.X版】

令和８（2026）年XX月XX日

厚生労働省医政局

厚生労働省保険局

デジタル庁国民向けサービスグループ

改訂履歴

版数	改訂年月日	該当箇所	内容
X.X	令和８年 XX 月 XX 日	初版	初版作成

目次

第１章　電子カルテ標準仕様書

1 はじめに

1.1 位置づけ

医科診療所向け電子カルテ標準仕様書（基本要件）（以下本章において「本書」という。）は、第７回「医療 DX 令和ビジョン 2030」厚生労働省推進チーム（令和７年７月１日開催）に提示した「電子カルテ・電子カルテ情報共有サービスの普及」に関する方針に基づき、作成するものである。

1.2 目的

令和４年６月に閣議決定された経済財政運営と改革の基本方針 2022 を踏まえ、国は同年 10 月に医療 DX 推進本部を設置し、国民の更なる健康増進、切れ目なく質の高い医療の効率的な提供等を目的として、関連する仕組みの整備を推進してきた。令和５年６月には、同本部において「医療 DX の推進に関する工程表」を決定し、「全国医療情報プラットフォームの創設」、「電子カルテ情報の標準化等」及び「診療報酬改定 DX」をはじめとする各種取組を進めている。

「医療 DX の推進に関する工程表」では、電子カルテについて、「遅くとも 2030 年には概ねすべての医療機関において必要な患者の医療情報を共有するための電子カルテの導入を目指す」こととしており、令和７年７月に開催した第７回「医療 DX 令和ビジョン 2030」厚生労働省推進チームにおいて、医科診療所向けに、①電子カルテ情報共有サービス及び電子処方箋への対応、②ガバメントクラウド対応が可能となるマルチテナント方式（いわゆる SaaS（Software as a Service）型）のクラウド型サービス、③関係システムへの標準 API の搭載、④データ引き継ぎが可能な互換性の確保等といった要件を参考に、電子カルテの標準仕様（基本要件）を策定する方針を示した。

また、令和７年 12 月 12 日に公布された医療法等の一部を改正する法律（令和７年法律第 87 号）により、同法による改正後の地域における医療及び介護の総合的な確保の促進に関する法律（平成元年法律第 64 号）第 12 条の３第４項において、「政府は、令和 12 年 12 月 31 日までに、電子カルテの普及率（電子診療録等情報その他の心身の状況に関する記録に係る情報に係る電磁的記録を利用する体制を整備している医療機関の全ての医療機関に対する割合をいう。）が約 100 パーセントとなることを達成するよう、クラウド・コンピューティング・サービス関連技術（官民データ活用推進基本法（平成 28 年法律第 103 号）第２条第４項に規定するクラウド・コンピューティング・サービス関連技術をいう。）その他の先端的な技術の活用を含め、医療機関の業務における情報の電子化を実現しなければならない。」旨が規定されたところである。

一方、医科診療所（無床の医科診療所に限る。以下本章において同じ。）における電子カルテに係る現在の状況では、①オンプレミス型である場合、高コストとなりがちなこと（IT 技術者等にとっても、過大な業務負担を伴う仕組みとなっていること）、② 多様な医療 DX サービス群への接続が求められること、③ 検査会社システムとの接続の仕様等が多種多様であるために、円滑な接続が困難となり、追加的なコストがかかっている等の課題がある。

電子カルテの迅速な普及を図るとともに、他の医療機関等との情報連携を円滑に進めていくためには、こうした課題を解決していく必要がある。このため、医科診療所向けの電子カルテについて仕様の標準化を進めることにより、電子カルテ情報共有サービスをはじめとした医療 DX サービス群を含む他のシステムとの円滑な接続や、医療機関間の迅速な情報共有が可能となるシステムの普及を図る等の観点から、本章２に規定する標準仕様（基本要件）（以下本章において「本標準仕様」という。）を策定する。

1.3 本書の見方

1.3.1 対象とする構成要素

本標準仕様が対象とする構成要素に係る考え方は、次表に示すとおりである。

表 1-1 本標準仕様が対象とする構成要素に係る考え方

＜凡例＞○：対象、●：一部対象、△：参考、×：対象外

構成要素		標準対象	考え方
業務フロー		×	本標準仕様は、医療機関における標準的な業務フローを規定するものではない。
機能要件	機能要件	●	電子カルテが医療 DX サービス群と接続して必要な機能を発現するため、関連する機能要件を標準仕様として規定する。
	画面要件	●	電子カルテが医療 DX サービス群と接続して必要な機能を発現するため、関連する画面要件を標準仕様として定める場合がある。
	帳票要件	●	電子カルテが医療 DX サービス群と接続して必要な機能を発現するため、関連する帳票の要件を標準仕様として定める場合がある。
	データ要件	●	電子カルテが医療 DX サービス群と接続して必要な機能を発現するため、関連するデータ要件を標準仕様として定める場合がある。
	連携要件	○	電子カルテと接続する外部システム（各種部門システム、レセプトコンピュータ、医療 DX サービス群、業務効率化ツールを含む。）とのインターフェイスについて、電子カルテ又は各外部システムの導入時又は更改時における流動性を確保する観点から、連携要件として標準仕様を規定する。
非機能要件		○	電子カルテについて、いわゆるクラウド・ネイティブに係る水準を担保するために必要な非機能要件を明確にするため、標準仕様を規定する。
情報提供・公開		○	電子カルテの価格の公開等を求めることにより、電子カルテが医療機関に導入される段階における選択可能性を向上させ、また、導入後の段階におけるサポート等のサービス水準を担保するため、標準仕様を規定する。

1.3.2　類型

本標準仕様に示す各項目は、その対応の必要性に応じ、次表の４類型に分類する。

なお、現に医療機関に設置される電子カルテの仕様のうち、本標準仕様に規定される項目と関連のない機能等の実装については、特に制限を設けない。

表 1-1　類型の分類及び考え方

類型	説明・考え方	ベンダーの対応
遵守	本標準仕様に準拠するため、実装又は対応が必須となるもの。 本標準仕様に準拠するためには、本類型に該当する項目に示された全ての内容に適合している必要がある。	実装又は対応必須
推奨	実装又は対応が推奨されるもの。 本類型に該当する項目に示された機能の実装や対応がなされていない場合であっても、本標準仕様への準拠を標榜することができるが、電子カルテを提供する事業者（以下本章において「ベンダー」という。）が開発する場合には、実装又は対応することが望ましい。 なお、本類型に該当する項目は、今後、本書の改定に際し、規定内容の一部又は全部が「遵守」類型に変更される場合がある。	実装又は対応任意
不可	本類型に該当する各項目に示された機能が実装され、又は示された条件に合致した場合、本標準仕様への準拠を標榜することが不可となるもの。	実装又は条件合致不可
参考	今後「遵守」類型又は「推奨」類型としていくことも含め検討中の事項や、電子カルテに係る具体的な仕様の検討に当たり参考となり得る情報について、参考情報として公表するもの。 なお、本類型に該当する項目は、今後、本書の改定に際し、規定内容の一部又は全部が「推奨」類型又は「遵守」類型に変更される場合があり、その際、規定内容の一部又は全部に変更がなされる場合がある。	実装又は対応任意

1.3.3　本書及び関連文書の一覧

本書及び関連文書の一覧は、次表 1-のとおりである。

表 1-3　本書及び関連文書の一覧

分類	資料名	概要
本書	医科診療所向け電子カルテ標準仕様書（基本要件）	電子カルテの標準仕様（基本要件）を記載した資料。
本書別紙	別紙Ａ　政府情報システムにおける脆弱性診断導入ガイドラインに係る遵守事項一覧	政府情報システムにおける脆弱性診断導入ガイドラインに示された各項目のうち、電子カルテに係る非機能要件として遵守すべき事項を一覧とした資料。
本書別紙	別紙Ｂ　IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧	独立行政法人情報処理推進機構（以下本章において「IPA」という。）が示す「非機能要求グレード」各項目について、電子カルテに係る非機能要件として遵守すべき事項を一覧とした資料。
関連文書	政府情報システムにおける脆弱性診断導入ガイドライン	政府情報システムに対する脆弱性診断を効果的に実施することを目的として、政府情報システムの管理責任や各機関のセキュリティ管理を担う職員に対して、脆弱性診断を実施する際の基準及びガイダンスを提供する文書。 公開先： https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-1d-9c31-0f06fca67afc/b08708cd/20240131_resources_standard_guidelines_guidelines_05.pdf
関連文書	デジタル庁 GCAS ガイド	ガバメントクラウドを利用するにあたって公開されているマニュアル。 公開先： https://guide.gcas.cloud.go.jp/
関連文書	デジタル庁 GCAS ガイド　公共 SaaS の共通要件にかかる技術方針	ガバメントクラウドを利用して公共 SaaS を効率的かつ効果的に整備いただくことを目的に、SaaS の共通要件のうち、技術方針について整理した資料。 公開先： https://guide.gcas.cloud.go.jp/gen

分類	資料名	概要
		eral/saas-technical-policy
関連文書	デジタル庁 GCAS ガイド　公共 SaaS の共通要件にかかる技術方針アーキテクチャ要件を満たすシステム構成例と満たさない例	共用を前提とする環境（マルチテナント）のアーキテクチャ要件を満たすシステム構成例と満たさない例を記載した文書。 公開先： https://guide.gcas.cloud.go.jp/general/saas-technical-policy#310-アーキテクチャ要件を満たすシステム構成例と満たさない例
関連文書	デジタル庁 GCAS ガイド　ガバメントクラウドにおけるモダン化の定義	クラウド環境で構築されるアプリケーションのモダン化の定義を記載。 公開先： https://guide.gcas.cloud.go.jp/modernization-guide/modernization-definition
関連文書	デジタル庁 GCAS ガイド　リファレンスアーキテクチャ	ガバメントクラウド上で構築するアプリケーションのアーキテクチャのリファレンスとして提供されている文書。 公開先： https://guide.gcas.cloud.go.jp/general/quotation-request-procurement
関連文書	オンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局】（令和７年 12 月版）	オンライン資格確認等システムの導入に当たり、オンライン資格確認等システムが提供する機能及び医療機関・薬局のシステムベンダーが提供しているシステムに実装いただきたい内容等について記載した文書。 公開先： https://www.mhlw.go.jp/stf/index_00093.html
関連文書	電子処方箋管理サービスの導入に関するシステムベンダ向け技術解説書【医療機関・薬局】	電子処方箋管理サービスの導入にあたり、電子処方箋管理サービスが提供する機能、及び医療機関・薬局のシステ

分類	資料名	概要
		ムベンダー（電子カルテシステム、薬局システム等のシステムベンダーが対象）が提供しているシステムに実装していただきたい内容等について記載した文書。 公開先： https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/denshishohousen_systemvendor.html
関連文書	電子カルテ情報共有サービス記録条件仕様書 1.04 版 別紙_記録条件仕様_バリデーションチェックルール xlsx 1.06 版 別紙_記録条件仕様_バリデーションチェックルール pdf 1.06 版 別紙_記録条件仕様 XML 定義表 1.03 版	社会保険診療報酬支払基金・公益社団法人国民健康保険中央会により共同で組織される医療保険情報提供等実施機関において維持・運営する医療機関等向け総合ポータルサイトに掲載される、電子カルテ情報共有サービスに係る記録条件の仕様を規定した資料。 提供元： 医療機関等 ONS サイト（ベンダー向けサイト）
関連文書	電子カルテ情報共有サービスの導入に関するシステムベンダ向け技術解説書 電子カルテ情報共有サービスの導入に関するシステムベンダ向け技術解説書（患者サマリー登録・閲覧サービス編）	医療機関等が電子カルテ情報共有サービスを導入するにあたり、医療機関等システムの開発ベンダーに対し、同サービスに係る改修事項等を理解いただくための文書。 公開先： https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/denkarukyouyuu.html
関連文書	オンライン資格確認等システム「外部インターフェイス仕様書」別紙 1-1 外部インターフェイス一覧（オン資格、電子処方箋、電カル情報共有）	社会保険診療報酬支払基金・公益社団法人国民健康保険中央会により共同で組織される医療保険情報提供等実施機関において維持・運営する医療機関等向け総合ポータルサイトに掲載される、オンライン資格確認等システム、電子処方箋管理サービス及び電子カルテ情報共有サービスが提供するインターフェイスを一覧にした資料。 提供元：

分類	資料名	概要
		医療機関等 ONS サイト（ベンダー向けサイト）
関連文書	介護情報基盤「外部インタフェース仕様書」	医療・介護DXサービスの一環である介護情報基盤において、電子カルテシステム等が主治医意見書や請求書を電子的に連携する際に必要となるインターフェイス仕様が記載された仕様書。 公開先： https://www.mhlw.go.jp/stf/newpage_59231.html
関連文書	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（概説編）（令和５年５月） 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（経営管理編）（令和５年５月） 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（企画管理編）（令和５年５月） 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（システム運用編）（令和５年５月）	医療情報システムの安全管理や、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（平成 16 年法律第 149 号）等に適切に対応するため、技術的及び運用管理上の観点から所要の対策を示した資料。 公開先： https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html
関連文書	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第 2.0 版（令和７年３月）	クラウド事業者ガイドラインと情報処理事業者ガイドラインが求める要件について、総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」及び経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」が定める要件を整理・統合した資料。 公開先： https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html
関連文書	ウェブアクセシビリティ導入ガイドブック（令和７年 10 月 16 日版）	ウェブアクセシビリティに初めて取り組む行政官や事業者向けに、ウェブア

分類	資料名	概要
		クセシビリティの考え方、取り組み方のポイントを解説するガイドブック。 公開先： https://www.digital.go.jp/resources/introduction-to-web-accessibility-guidebook
関連文書	医療情報セキュリティ開示書（SDS Ver5.0）	医療機関等が医療情報システムによって保存、伝送される医療情報に関するリスクアセスメントを行うとき、それを支援できる重要な情報を提供するために作られたチェックリスト。 公開先： https://www.jahis.jp/standard/detail/id=1119

2　標準仕様（基本要件）

2.1 電子カルテ

電子カルテの機能要件、非機能要件、アーキテクチャ及びデータ移行に係る仕様について、標準仕様（基本要件）を示す。

※　医科診療所以外の医療機関が、本標準仕様に準拠した電子カルテを設置することを妨げるものではない。

2.1.1 機能要件

（1）考え方

電子カルテの機能のうち、各種医療 DX サービス群との接続機能について、必要な機能要件を定める。

（2）機能要件に係る標準仕様（基本要件）

①「遵守」類型に該当する項目（必須要件）

No	仕様
1	次に掲げる要件の全てに適合すること。 なお、個々の医療機関において、次に掲げる要件に規定する全ての機能を必ず実装することを求めるものではないこと。例えば、訪問診療を実施する機会を有しない医療機関において、訪問診療のみのために必要な機能を実装する必要はない。 （1） 電子カルテについて、「オンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局】」（令和７年12月版又は当該版以後に作成された版）に規定された機能を有すること。 （2） 電子カルテについて、「電子処方箋管理サービスの導入に関するシステムベンダ向け技術解説書【医療機関・薬局】」（令和７年 12 月版又は当該版以後に作成された版）に規定された電子処方箋に係る機能（処方箋取消 UNDO 機能、処方箋変更機能、処方箋変更 UNDO 機能、重複投薬等チェック事前処理機能、処方箋 ID 検索機能、院内処方機能を除く。）を有すること。 （3） 電子カルテについて、医療機関等 ONS サイト上に掲載された「電子カルテ情報共有サービス記録条件仕様書」（第 1.04 版又は当該版以後に作成された版）並びに「別紙_記録条件仕様_バリデーションチェックルール xlsx」（第 1.06 版又は当該版以後に作成された版）、「別紙_記録条件仕様_バリデーションチェックルール pdf」（第 1.06 版又は当該版以後に作成された版）及び「別紙_記録条件仕様 XML 定義表」（第 1.03 版又は当該版以後に作成された版）並びに「電子カルテ情報共有サービスの導入に関するシステムベンダ向け技術解説書」（第 2.0.0 版又は当該版以後に作成された版）に規定された電子カルテ情報共有サービスに係る機能を有すること。 （4） 共通算定モジュールとの接続可能性を踏まえ、クラウド型レセプトコンピュータとの接続機能を有すること。ただし、電子カルテとレセプトコンピュータが一体となったシステムである場合にあっては、この限りでない。

②「推奨」類型に該当する項目（推奨要件）

No	仕様
1	次に掲げる要件に適合することが望ましいこと。 （１） 電子カルテについて、「電子処方箋管理サービスの導入に関するシステムベンダ向け技術解説書【医療機関・薬局】」（令和７年 12 月版又は当該版以後に作成された版）に規定された電子処方箋に係る機能（処方箋取消 UNDO 機能、処方箋変更機能、処方箋変更 UNDO 機能、重複投薬等チェック事前処理機能、処方箋 ID 検索機能、院内処方機能に限る。）を有すること。 （２） 電子カルテについて、医療機関等 ONS サイト上に掲載された「電子カルテ情報共有サービスの導入に関するシステムベンダ向け技術解説書（患者サマリー登録・閲覧サービス編）」（第 1.0.0 版又は当該版以後に作成された版）に規定された電子カルテ情報共有サービスに係る機能を有すること。 （３） 電子カルテについて、「主治医意見書／請求書電送サービスの導入に関するシステムベンダ向け技術解説書」（第 1.02 版又は当該版以後に作成された版）に記載された機能を有すること。 （４） 国が推進する医療 DX に関連した各種サービスについて、当該サービスの利用又は当該サービスとの接続のために必要な電子カルテの機能が公表された場合には、当該機能を有すること。

③「参考」類型に該当する項目

なし

（３）経過措置

（２）①表中１（２）は、電子カルテと電子処方箋サービスとの間でクラウド間の連携が実現した旨の公表の日から起算して３月が経過するまでの間は適用せず、推奨項目として取り扱うものとする。

（２）①表中１（３）は、電子カルテと電子カルテ情報共有サービスとの間でクラウド間の連携が実現した旨の公表の日から起算して３月が経過するまでの間は適用せず、推奨項目として取り扱うものとする。

2.1.2 非機能要件

（1）考え方

電子カルテについて、クラウド技術を活用したモダンシステムへの刷新を図りつつ、医科診療所として必要十分な可用性、セキュリティ、バックアップ環境等を確保するため、必要な非機能要件を定める。

（2）非機能要件に係る標準仕様（基本要件）

①「遵守」類型に該当する項目（必須要件）

No	項目	仕様
1	可用性	次に掲げる要件に適合すること。 ・稼働率の実績が 99.9%以上であること。 なお、稼働率（%）は、以下の計算式により定義する。 【　稼働率＝年間実稼働時間／年間予定稼働時間×100　】 ※　当該計算式において、年間実稼働時間は「利用者がサービスを利用可能であった時間の合計」、年間予定稼働時間は「事前に予定された年間稼働時間（24 時間 365 日であるかどうかは問わない。）から計画停止時間及び大規模災害による停止・縮退時間を除いた時間の合計」と定義する。 このため、年間実稼働時間を算出できない新規製品については、目標稼働率が 99.9%以上であることを要件とする。ただし、既存製品に一部の機能を追加したものを新規製品と称している場合には、既存製品に係る稼働率を算出し、適合性を判断することとして差し支えない。 なお、稼働率は、あらかじめサービス仕様書等において定義された責任分界の範囲内を対象として算出するものとする。
2	セキュリティ	次に掲げる要件の全てに適合すること。ただし、電子カルテがガバメントクラウドを利用している場合にあっては、次に掲げる要件のうち（1）から（3）に適合しているものとみなすこと。 （1） 次に掲げるア又はイの認証（電子カルテを含めた包括的な認証である場合を含む。）を取得したものであること。 ア　政府情報システムのためのセキュリティ評価制度（ISMAP） イ　ISMS 認証及び ISMS クラウドセキュリティ認証 （2） 第三者機関によりペネトレーションテストを実施し、脆弱性を検知した場合は、当該脆弱性について適切な対策を講ずること。 （3） 電子カルテを構成する主要なソフトウェアについて脆弱性診断を実施し、脆弱性を検知した場合は、当該脆弱性について適切な対策を講ずること。 脆弱性診断は、政府情報システムにおける脆弱性診断導入ガイドライン（2024（令和６）年１月 31 日）（「別紙Ａ 政府情報システムにおける脆弱性診断導入ガイドラインに係る遵守事項一覧」に規定する項目に限る。）に適合した態様で実施すること。 （4） システムを構成する各要素に対し、定期的にセキュリティパッチを適用すること。また、緊急のセキュリティパッチが配布

No	項目	仕様
		された場合には直ちに適用できるよう、必要な対策を講ずること。さらに、各医療機関に設置された関係する端末等におけるセキュリティパッチの適用を妨げることのないよう、関係するセキュリティパッチ（最新バージョンの OS や Web ブラウザへの更新を含む。）が公開された場合には、速やかに互換性を検証するとともに、当該検証の結果必要がある場合には、互換性を維持するための手段を速やかに講じること。
3	データ保管	次に掲げる要件に適合すること。 ・データが日本国内で保持され、海外に送信されることのないよう設定すること。
4	バックアップ環境の整備	次に掲げる要件に適合すること。 ・マルウェア感染等により、主たるクラウド上のデータが利用不能となった場合に備え、物理的かつ論理的に隔離された別のクラウドサーバ上又はテープメディア等の外部メディアに定期的なバックアップを行う仕様とし、冗長性、信頼性及び可用性を確保すること。
5	ガイドライン/ 非機能要求グレード	次に掲げる要件の全てに適合すること。 （１） 電子カルテが提供する機能のうち、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（令和５年５月）に関係する部分について、同ガイドラインに適合するものであること。 なお、同ガイドラインは医療機関の運用について規定するものであるところ、電子カルテが提供する機能に関連する部分以外の箇所への適合性については、本標準仕様の対象外とする。 （２） 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第 2.0 版（令和７年３月）に適合するものであること。 （３） 「別紙Ｂ IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧」に規定する各項目に適合すること。

②「推奨」類型に該当する項目（推奨要件）

No	項目	仕様
1	アクセシビリティ	次に掲げる要件に適合することが望ましいこと。ただし、電子カルテがガバメントクラウドを利用している場合にあっては、次に掲げる要件に適合しているものとみなすこと。 ・ウェブアクセシビリティ導入ガイドブック「3.1 達成しないと利用者に重大な悪影響を及ぼすもの」及び「3.2 必ず達成しなければならないもの」に記載の内容を遵守していること。

③「参考」類型に該当する項目

なし

2.1.3 アーキテクチャ

（1）考え方

電子カルテについて、医療機関単位のカスタマイズを廃して標準パッケージとしての機能を充実させるとともに、マルチテナント方式のクラウド・ネイティブ化を図ることによりコストの最適化を図るため、電子カルテのアーキテクチャや処理方式に係る設計の方針について、標準的な仕様を規定する。

（2）アーキテクチャに係る標準仕様（基本要件）

①「遵守」類型に該当する項目（必須要件）

No	項目	仕様
1	クラウドネイティブ・アーキテクチャ指針	次に掲げる要件の全てに適合すること。ただし、電子カルテがガバメントクラウドを利用している場合にあっては、次に掲げる要件の全てに適合しているものとみなすこと。 （1） 電子カルテを構成するアプリケーションは、原則としてパブリッククラウド環境（ガバメントクラウド対象クラウドサービスを利用しているものに限る。）で稼働すること。ただし、次に掲げる機能を有するアプリケーションにあっては、この限りでない。 ① 医療機関内に設置された機器等（例：資格確認端末、プリンター）との通信を中継又は制御するための機能 ② 見読性を担保するためのデータ保管に係る機能 ③ クラウド障害等の非常時における事業継続のための機能 （2） 医療機関に提供される、クラウド上で稼働する全てのアプリケーションは、SaaS 型であること。 （3） 電子カルテの構成は、マルチテナント方式であること。 （4） クラウド上で稼働するアプリケーションのソースコードは、全てのテナントについて共通であることを前提としたサービス設計とし、アプリケーションのテスト、更新等による一時的なものを除き、複数のバージョンが併存しない仕様であること。 なお、特定の診療科に特化した機能を搭載するためにソースコードを区分したものについては、複数のバージョンの併存には当たらないものとする。ただし、ソースコードの管理体系及び各ソースコードが対象とする診療科の整理が明確である場合に限る。 （5） 電子カルテを構成する全てのアプリケーションについて、個々の医療機関におけるカスタマイズに対応不可能な仕様とすること。 ただし、医療機関の要望等により追加した機能を、有償無償にかかわらず、当該電子カルテのオプション機能として、当該電子カルテを使用する全ての医療機関が必要に応じて利用できる場合には、カスタマイズには当たらないものとする。 なお、アプリケーション上の設定やメタデータの変更により、個々の医療機関における環境に対応させることは差し支えない。
2	モダナイゼーション（アプリケーシ	次に掲げる要件に適合すること。ただし、電子カルテがガバメントクラウドを利用している場合にあっては、次に掲げる要件に適合しているものとみなすこと。 ・電子カルテを構成するシステムが、「デジタル庁 GCAS ガイド　ガ

No	項目	仕様
	ョンのモダン化）	バメントクラウドにおけるモダン化の定義」に合致するものであること。

②「推奨」類型に該当する項目（推奨要件）
なし

③「参考」類型に該当する項目
【※検討中】

2.1.4 データ移行

【※検討中】

2.2 システム等間の連携

電子カルテと各種医療 DX サービス群との間及び電子カルテと部門システム、業務効率化ツールその他の外部システム等（医療 DX サービス群は含まない。以下本章において同じ。）との間における連携に係る仕様について、標準仕様（基本要件）を示す。

2.2.1 電子カルテ－医療 DX サービス群間の API 仕様

（1）考え方

電子カルテとの接続が可能となっている各種医療 DX サービス群を可視化するとともに、同サービス群との接続方法を示し、同サービス群の利用を促進することを目的として、電子カルテと同サービス群との間における個別インターフェイスの仕様を標準仕様（基本要件）として規定する。

（2）電子カルテと各種医療 DX サービス群との間における個別インターフェイスに係る標準仕様（基本要件）

①「遵守」類型に該当する項目（必須要件）

No	項目	仕様
1	オンライン資格確認等システム/電子処方箋管理サービス/電子カルテ情報共有サービス	次に掲げる要件に適合すること。 ・医療機関等 ONS サイト上に掲載された「外部インターフェイス仕様書（オン資格、電子処方箋、電カル情報共有）」（第 8.09 版又は当該版以後に作成された版）、「外部インターフェイス仕様書（オン資格、電子処方箋、電カル情報共有_WebAPI 連携編）」（第 8.10 版又は当該版以後に作成された版）、「別紙 1-1 外部インターフェイス一覧（オン資格、電子処方箋、電カル情報共有）」（第 8.07 版又は当該版以後に作成された版）及び「別紙 1-2 外部インターフェイス一覧（薬剤情報等・特定健診情報・臨床情報）」（第 5.03 版又は当該版以後に作成された版）に規定されたインターフェイスとの接続機能を有し、オンライン資格確認等システム、電子処方箋管理サービス及び電子カルテ情報共有サービスとの接続が可能であること。 ただし、電子カルテに接続されたレセプトコンピュータが当該各インターフェイスとの接続機能を有し、レセプトコンピュータから当該各システムに接続がなされている場合は、電子カルテにおいて、当該各インターフェイスとの接続機能を重複して有する必要はないこと。 なお、上記は、個々の医療機関において、「外部インターフェイス仕様書（オン資格、電子処方箋、電カル情報共有）」等に規定する全ての機能を必ず実装することを求めるものではない。例えば、訪問診療を実施する機会を有しない医療機関において、訪問診療のみのために必要なインターフェイスとの接続機能を実装する必要はないこと。

②「推奨」類型に該当する項目（推奨要件）

No	項目	仕様
1	共通算定モジュール	次に掲げる要件に適合することが望ましいこと。 ・「診療報酬改定 DX における共通算定モジュール外部インタフェース利用ガイド」（製品版又はその後に作成された版）に準拠したレセプトコンピュータとの連携機能を有すること。ただし、電子カルテとレセプトコンピュータが一体となったシステムである場合にあっては、この限りでない。
2	その他のサービス	次に掲げる要件に適合することが望ましいこと。 （１）介護情報基盤「外部インタフェース仕様書」に規定されたインターフェイスとの接続機能を有すること。 ただし、電子カルテに接続されたレセプトコンピュータ等が当該インターフェイスとの接続機能を有する場合は、電子カルテにおいて、当該インターフェイスとの接続機能を重複して有する必要はないこと。 （２）国が推進する医療 DX に関連した各種サービスについて、電子カルテとの接続のためのインターフェイスが公表された場合には、公表された仕様に基づくインターフェイスとの接続機能を有すること。

③「参考」類型に該当する項目

なし

（３）経過措置

（２）①表中１のうち電子処方箋に係る部分は、電子カルテと電子処方箋管理サービスとの間で、クラウド間の連携が実現した旨の公表の日から起算して３月が経過するまでの間は適用せず、推奨項目として取り扱うものとする。

（２）①表中１のうち電子カルテ情報共有サービスに係る部分は、電子カルテと電子カルテ情報共有サービスとの間で、クラウド間の連携が実現した旨の公表の日から起算して３月が経過するまでの間は適用せず、推奨項目として取り扱うものとする。

2.2.2 電子カルテ－外部システム等間における連携共通仕様

【※検討中】

2.2.3 API 個別仕様(電子カルテ－部門システム)

【※検討中】

2.2.4 API 個別仕様(電子カルテ－業務効率化ツール)

【※検討中】

2.3 情報提供・公開

（1）考え方

電子カルテが医療機関に導入される段階における選択可能性を向上させ、また、導入後の段階におけるサポート等のサービス水準を担保するため、標準的な電子カルテとして求められる情報提供又は公開に係る考え方について、標準仕様（基本要件）として規定する。

（2）情報の提供又は公開に係る標準仕様（基本要件）

①「遵守」類型に該当する項目（必須要件）

No	項目	仕様
1	情報提供・公開	次に掲げる要件の全てに適合すること。 （1） ベンダーが自ら運営する Web サイト上に、電子カルテの価格（オプション機能に係る価格を含む。）を公開済であること。 （2） 医療機関等（医療機関及び医療機関から委託を受けた者をいう。以下 2.3 において同じ。）の要請があった場合、電子カルテに関して記入済の医療情報セキュリティ開示書（SDS Ver5.0）について開示すること。 （3） 医療機関等の要請があった場合、医療機関におけるサイバーセキュリティ対策チェックリスト（事業者確認用）について開示すること。 （4） 医療機関等の要請があった場合、電子カルテを医療機関に提供する場合のサービス仕様適合開示書及びサービス仕様書について開示すること。 （5） 医療機関等の要請があった場合、電子カルテ間のデータ移行に必要な事項（データ形式を含む。）について開示すること。 （6） 医療機関等又は電子カルテとの接続を求める部門システムに係るベンダーの要請があった場合、電子カルテと部門システムとの間におけるインターフェイスの仕様について開示すること。 （7） 医療機関の要請があった場合、電子カルテについて、医療機関から問い合わせがあった際の一次回答時間の直近３か月の平均値について開示すること。

②「推奨」類型に該当する項目（推奨要件）

No	項目	仕様
1	情報提供・公開	次に掲げる要件に適合することが望ましいこと。 （1） 医療機関等の要請があった場合、契約締結前であっても、システムのデモンストレーション等を実施することにより、電子カルテが有する詳細な機能について開示すること。 （2） 医療機関等の要請に応じ、契約締結前であっても、電子カルテのトライアルが可能であること。また、トライアルの実施期間中又はその前後の期間において、適切な支援が可能であること。 （3） 電子カルテとの接続を求める外部システム等のベン

		ダーが、当該接続について円滑に検討できるよう、適切なテスト環境を整備し、その利用法等について公開すること。

③「参考」類型に該当する項目

なし

2.4 留意事項

（1）第２章（レセプトコンピュータ標準仕様書）との関係性について

本標準仕様は、電子カルテとレセプトコンピュータが別個のシステムである場合には当該電子カルテ部分の、また、電子カルテとレセプトコンピュータが一体となったシステムである場合には当該システムのうち電子カルテ部分の、それぞれ標準的な仕様を規定するものである。

電子カルテとレセプトコンピュータが一体となったシステムでは、一体的な管理運用が想定されるところ、例えば非機能要件の一部等、同一の事項に関して本章の規定と第２章の規定が異なっている場合には、本章の規定内容を優先して適用するものとする。

3 本書の改訂

本書は、一定の頻度による定期的な改定（以下本章において「定期改定」という。）を予定している。

予定される定期改定の内容には、標準化する対象データ範囲の拡大又は一部内容の修正、接続対象となる医療 DX サービスの追加、類型の変更等が含まれる。

また、本書は、定期改定のほか、臨時に改定される場合がある。

(参考)

今後の定期改定の内容としては、以下に掲げるものが対象となり得る。

（１）接続対象となる医療 DX サービスの拡大

医療 DX サービス群に属するシステムは、複数のシステムの開発について国が取組を進めており、順次、技術的な仕様が公開される見込みである。このため、本標準仕様において対象とする医療 DX サービスの範囲についても、定期改定により段階的に拡大することを想定している。

初版においては、以下に掲げるサービスが接続対象となる。

- オンライン資格確認等システム
- 電子カルテ情報共有サービス
- 電子処方箋管理サービス
- 介護保険に係る主治医意見書／請求書電送サービス

今後、以下に掲げる医療 DX に係る取組を通じ、電子カルテからの接続先や対象となるデータの範囲が拡大される見込みであり、次版以降において順次、本標準仕様に規定する予定である。

- 感染症発生届のデジタル化
- 自治体検診 DX（PMH 自治体検診（仮称））
- 死亡診断書の電子的提出化
- 出生証明書の電子的提出化
- 職域がん検診 DX
- その他診断書等の電子的提出化
- 母子保健 DX（PMH 母子保健（仮称））
- 予防接種のデジタル化（予診情報・予防接種記録管理／請求支払システム）

（50 音順。実際の規定の時期については順不同）

（２）標準コード・マスタの策定及び更新の反映

厚生労働省においては、医薬品・検査等の標準コード・マスタ及びこれらの維持管理体制の整備に係る取組を進めているところである。

当該標準コード・マスタの策定は、概ね部門システムの種別毎に検討を進める予定であり、具体的には、①医療現場において使用される臨床情報の整理、②システム間交換規約の策定、③コード体系の策定、④マスタの策定、⑤インターフェイス仕様書の策定を経て、⑥記録条件仕様定義表の策定を目指すこととしている。

これらの検討の結果、当該標準コード・マスタが確立した場合には、主に（３）及び（４）に示す形で、本標準仕様への追加が見込まれる。

また、こうして策定した標準コード・マスタは、状況の変化に適確に対応できるよう継続的に維持管理を行っていくことが想定され、標準コード・マスタの更新があった場合には、当該内容についても、本標準仕様に反映していくことが見込まれる。

（３）電子カルテと外部システム等との間における連携仕様の追加等

（２）に係る検討の結果、部門システムの種別毎に、標準的なコード、マスタ、インターフェイス仕様書及び記録条件仕様定義表が策定されることが見込まれる。電子カルテ－外部システム等間における連携に必要な仕様については、策定された標準的なコード等に基づき、順次、本標準仕様

に規定していく予定である。
　また、標準的なコード等に更新があった場合には、関係部分の仕様について併せて更新することが見込まれる。

（４）データ移行に係る共通仕様及び個別インターフェイスの追加等
　電子カルテ間のデータ移行に係る共通仕様や個別インターフェイスは、（２）の標準的なコード等及び（３）の電子カルテ－外部システム等間における連携に必要な仕様と一定の関連がある。このため、データ移行に係る標準的な仕様については、今後、（２）及び（３）に係る検討も踏まえて策定し、本標準仕様に規定していく予定である。
　また、標準的なコード等に更新があった場合には、関係部分の仕様について併せて更新することが見込まれる。

（５）３省２ガイドラインの改定に伴うセキュリティ要件の追加
　本標準仕様では、３省２ガイドラインへの準拠を原則とした上で、その一部については外部監査により対応できる形で要件を規定している。３省２ガイドラインについては、クラウド型サービスを対象とするために一部改定が検討されており、仮に改定がなされた場合には、本標準仕様におけるセキュリティ要件についても、併せて改定がなされる可能性がある。

4 用語

本書についての解釈に紛れが生じないよう、用いられている用語の解説を以下に示した。ここで示す解説はあくまで本書における考え方であり、用語によっては、本書以外では別の意味で用いられている場合もある。

表 4-1 用語の解説

No	用語	説明
1	アプリケーション	アプリケーションとは、コンピュータ上で使うソフトウェアの一種で、特定の目的や作業を行うためのプログラムのことをいう。本書では、電子カルテの機能の提供を目的にしたソフトウェアのことをいう。
2	インターフェイス	インターフェイスとは、あるシステムが、他のシステムや外部サービスと連携するための接続仕様のことをいう。データの受け渡し方法、通信プロトコル、データ形式（例：JSON、csv）等を定義し、システム間の連携や自動処理を可能にする。
3	オンプレミス	オンプレミスとは、診療所内に IT インフラ（サーバ、ネットワーク機器、データベース、アプリケーション等）を設置し、管理・運用する形態をいう。
4	ガバメントクラウド	「デジタル社会の実現に向けた重点計画」等の政府方針に基づき、安全かつ合理的な利用環境としてデジタル庁が選定した複数のパブリッククラウド（IaaS、PaaS 及び SaaS）のことをいう。 また、情報通信技術を活用した行政の推進等に関する法律（平成 14 年法律第 151 号）第 23 条第２項に規定する共同利用クラウド・コンピューティング・サービスをいい、国と公共情報システム整備運用者が共同して利用することができるものとされたクラウド・コンピューティング・サービスである。
5	共通算定モジュール	日々の外来診療等に伴う診療報酬の算定と患者負担金の計算をオンラインで行う電子計算プログラムをいう。
6	クラウドサービス	クラウド事業者が提供するコンピューティング資源を、ネットワークを通じて利用できるサービス。その提供形態から、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）及び SaaS（Software as a Service）に区分される。また、実現形態から、プライベートクラウド、パブリッククラウド及びハイブリッドクラウドに区分することができる。
7	サービス仕様書	サービス仕様書とは、書面にしたサービス提供者と顧客との合意であって、サービス及びサービス目標を特定した、サービス提供者と顧客との間の合意文書(JIS Q 20000-1:2020)をいう。 作成に当たっては、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別紙１「ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例」を参照すること。
8	サービス仕様適合開示書	サービス仕様適合開示書とは、対象事業者が、自ら提供するサービスの仕様につき、医療情報を取り扱う情報システム・サービスの提

No	用語	説明
		供事業者における安全管理ガイドラインへの適合状況を医療機関等へ開示するために作成するための資料のことをいう。 作成に当たっては、同ガイドライン別紙１「ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例」を参照すること。
9	脆弱性	脆弱性とは、脅威によって悪用される可能性がある欠陥や仕様上の問題をいう。
10	脆弱性診断	脆弱性診断とは、システムやアプリケーション、ネットワークに潜むセキュリティ上の弱点（脆弱性）を事前に検出し、リスクを評価するための技術的な評価手法のことをいう。
11	政府情報システムのためのセキュリティ評価制度（ISMAP）	政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ水準を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度のことをいう。
12	ソフトウェア	ソフトウェアとは、コンピュータやスマートフォン、タブレットなどの電子機器を動かすプログラムやアプリケーションのことをいう。
13	電子カルテ	電子カルテとは、従来、医師が患者の診療記録を記入していた紙のカルテ（診療録）を電子化し、データとして保存したものをいう。紙のカルテを電子化することにより、関連する検査結果や画像等も一元的に管理できるようになり、利便性や検索性が向上するとともに、他のシステムとの連携により、業務効率化にもつながることが期待される。
14	パブリッククラウド	パブリッククラウドとは、クラウドサービス事業者が所有するクラウド基盤を、不特定多数の利用者に広く提供するサービス形態であり、一般的にはインターネット経由で利用される。複数の利用者が共同でインフラを共有する点が特徴である。
15	プライベートクラウド	プライベートクラウドとは、特定の企業や組織専用に構築・提供されるクラウド環境のことをいい、第三者とインフラを共有しない点が特徴である。
16	ペネトレーションテスト	ペネトレーションテストとは、組織が運用するシステムやネットワーク、アプリケーションに対して、攻撃者の視点から脆弱性を検証するセキュリティ評価手法をいう。
17	マルチテナント方式	マルチテナントとは、共同利用を前提とする環境のことをいう。 本書が想定するマルチテナント方式の具体的な態様は、「デジタル庁 GCAS ガイド　公共 SaaS の共通要件にかかる技術方針 3.10　アーキテクチャ要件を満たすシステム構成例と満たさない例」に規定する「アーキテクチャ要件を満たすシステム構成」である。

No	用語	説明
18	モダン化	モダン化とは、最先端の実験的な技術ではなく、ある程度一般化した新しい技術を活用する方針を採用することをいう。 本書が想定するモダン化の具体的な態様は、「デジタル庁 GCAS ガイド　ガバメントクラウドにおけるモダン化の定義」の１～５をいう。 １．API ベースのシステム構成 ２．ステートレスなアーキテクチャ ３．マネージドサービスの活用 ４．運用のコード化、自動化 ５．サービスレベルの定義、計測
19	レセプトコンピュータ（医事会計システム）	レセプトコンピュータとは、医療機関において、診療行為等の情報に基づき診療報酬を算定し、患者負担金を計算するとともに、診療報酬請求のための診療報酬明細書（レセプト）の作成及び請求処理を行う機能を有するコンピュータをいう。 算定から請求までの医事会計業務を一貫して電子的に処理でき、会計・請求業務の正確性・迅速性の向上や事務負担の軽減、業務効率化が図られる。また、他の医療情報システム等との連携により、さらなる効率化が期待される。
20	ライブラリ	ライブラリとは、プログラムの部品や機能をまとめたファイル群のことをいう。
21	API	API（Application Programming Interface：アプリケーション・プログラミング・インターフェース）とは、ソフトウェア同士が機能やデータを相互にやり取りするための接点や規約をいう。
22	BCP	BCP(Business Continuity Plan)とは、事業継続計画のことをいう。
23	IaaS	IaaS(Infrastructure as a Service)とは、CPU、 メモリ、 ストレージ、 ネットワーク等のハードウェア資産をサービスとして提供するクラウドサービスをいう。
24	ISMS 認証	対象となる組織が、国際規格 ISO/IEC 27001 に基づき、情報資産を適切に管理・保護するための仕組みを整備・運用していることについて、認定を受けた第三者機関が審査し認証する制度。
25	ISMS クラウドセキュリティ認証	対象となる組織（クラウドサービス事業者又はクラウドサービスを利用する組織）が、国際規格 ISO/IEC 27017 及び ISO/IEC 27018 に基づき、クラウド特有のリスクに対応した情報セキュリティ管理の仕組みを整備・運用していることについて、認定を受けた第三者機関が審査し認証する制度。
26	SDS	「サービス事業者による医療情報セキュリティ開示書（SDS）」の略称で、（一社）保健医療福祉情報システム工業会（JAHIS）及び（一社）日本画像医療システム工業会（JIRA）が定めた各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する

No	用語	説明
		説明の標準的記載方法（書式）のことをいう。これらの書式は製品/サービスの説明の一部として製造業者/サービス事業者が作成し、セキュリティマネジメントを実施する医療機関等を支援するために用いられることが想定されている。
27	PaaS	PaaS（Platform as a Service)とは、オペレーションシステムや、アプリケーションの実行環境をサービスとして提供するクラウドサービスをいう。
28	SaaS	SaaS（Software as a Service）とは、ソフトウェアがインターネットを通じて提供されるサービス形態をいう。従来のようにユーザーが自社のパソコンやサーバにソフトウェアをインストールして利用するのではなく、SaaS では、クラウド上に構築されたアプリケーションを、Web ブラウザなどを通じて利用する形態となる。
29	３省２ガイドライン	「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」（令和５年５月）及び「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第 2.0 版」（令和７年３月）をいう。

第２章　レセプトコンピュータ標準仕様書

1 はじめに

1.1 位置づけ

医科診療所向けレセプトコンピュータ標準仕様（基本要件）（以下本章において「本書」という。）は、病院情報システムの刷新に関する方針（令和７年１月 22 日付け厚生労働大臣決定。以下「病院情報システム刷新方針」という。）に基づき、作成するものである。

1.2 目的

令和４年６月に閣議決定された経済財政運営と改革の基本方針 2022 を踏まえ、国は同年 10 月に医療 DX 推進本部を設置し、国民の更なる健康増進、切れ目なく質の高い医療の効率的な提供等を目的として、関連する仕組みの整備を推進してきた。令和５年６月には、同本部において「医療 DX の推進に関する工程表」を決定し、「全国医療情報プラットフォームの創設」、「電子カルテ情報の標準化等」及び「診療報酬改定 DX」をはじめとする各種取組を進めている。

こうした中、病院情報システム刷新方針が示され、現在のオンプレミス型のシステムを刷新し、電子カルテ/レセプトコンピュータ（以下本章において「レセコン」という。）/部門システムを一体的に、モダン技術を活用したクラウド型システムに移行することとし、令和 12（2030）年までのできる限り早い時期に、希望する病院が導入できる環境を整備することを目標に取組を進めている。このため、国がシステムの標準仕様を示し、その標準仕様に準拠した病院の情報システムを民間が開発し、小規模病院等から段階的な普及を図るため、今般、電子カルテとともに、本書を作成するものである。

また、レセコンに関しては、現在、診療報酬改定 DX の取組の１つとして、令和８年６月からの共通算定モジュールの本格運用の開始に向けて、先行/協力/準協力レセコンベンダー等において、共通算定モジュールと連携するクラウド型レセコンの開発とモダン化が進められている。本書は、診療報酬改定 DX の推進も図るものである。

これらの方針や政策目的の下、本書において、レセコンを対象にした標準仕様（基本要件）を規定することとしたものである。

本書２に規定する標準仕様（基本要件）（以下本章において「本標準仕様」という。）の各項目は、医療 DX に係る取組の趣旨を踏まえ、主に次に掲げる事項を目的として定める。

① 国が実施する医療 DX に係る各施策について、ベンダーによる迅速な対応を促し、最新のデジタル技術を活用しつつ効率化効果等を医療機関に還元すること。

② 共通算定モジュールと接続し、診療報酬改定の度に発生する間接コストの極小化を図り、適正な診療報酬等の計算や請求事務に係る効率化を図ること。

③ 電子カルテと一体的に運用可能なレセコンの実現とデータの互換性確保を図り、医療機関等が最適なレセコンを低コストで導入及び運用すること並びに当該レセコンへの移行を可能とすること。

④ レセコンの価格公開により医療機関が比較検討しやすい環境を醸成するとともに、現行システムからのデータ引継ぎや連携の規格を標準化することにより、過去に利用していた製品に依存することなく、更改後のレセコンや電子カルテ、部門システムの選定を可能とする環境を実現し、マーケットの透明性及びベンダー間の競争を確保すること。

⑤ 地方自治体による医療費助成の現物給付化される区域の拡大を図るなど、国民の健康・福祉の向上に寄与すること。

本標準仕様に準拠したレセコンが普及することにより、レセコンの導入や移行の際に必要となるデータ移行等の負担低減等を図るとともに市場の健全な競争を促し、標準型電子カルテ（導入版）の普及やオンライン資格確認等の医療 DX サービス群の安定的な運用の定着に寄与すること等が期待される。

1.3 本書の見方

1.3.1 対象とする構成要素

本標準仕様が対象とする構成要素に係る考え方は、次表に示すとおりである。

表 1-1 本標準仕様が対象とする構成要素に係る考え方

＜凡例＞○：対象、●：一部対象、△：参考、×：対象外

構成要素		標準対象	考え方
業務フロー		×	医療機関の標準的な業務フローを規定するものではない。
機能要件	機能要件	●	レセコンが医療 DX サービス群と接続して必要な機能を発現するため、関連する機能要件を標準仕様として規定する。
	画面要件	●	レセコンが医療 DX サービス群と接続して必要な機能を発現するため、関連する画面要件を標準仕様として定める場合がある。
	帳票要件	●	レセコンが医療 DX サービス群と接続して必要な機能を発現するため、関連する帳票の要件を標準仕様として定める場合がある。
	データ要件	●	レセコンが医療 DX サービス群と接続して必要な機能を発現するため、関連するデータ要件を標準仕様として定める場合がある。
	連携要件	○	共通算定モジュールとのインターフェイスについては、共通算定モジュール外部インタフェース利用ガイド等に適合することを標準仕様として規定する。 レセコンと接続する外部システム（各種部門システム、電子カルテ、医療 DX サービス群を含む。）とのインターフェイスについて、レセコン又は各外部システムの導入時又は更改時における流動性を確保する観点から、連携要件として標準仕様を規定する。

構成要素	標準対象	考え方
非機能要件	○	ベンダーが開発するレセコンについて、いわゆるクラウド・ネイティブに係る水準を担保するために必要な非機能要件を明確にさせ、また、共通算定モジュールの協力レセコンベンダー等に求めた非機能要件と整合するものとして標準仕様を規定する。
情報提供・公開	○	レセコンの価格の公開等を求めることにより、レセコンが医療機関に導入される段階における選択可能性を向上させ、また、導入後の段階におけるサポート等のサービス水準を担保するため、標準仕様を規定する。

1.3.2 類型

本標準仕様に示す各項目は、その対応の必要性に応じ、次表の４類型に分類する。

なお、現に医療機関（歯科を除く。以下同じ。）に設置されるレセコンの仕様のうち、本標準仕様に規定される項目と関連のない機能等の実装については、特に制限を設けない。

表１－２　類型の分類及び考え方

類型	説明・考え方	ベンダーの対応
遵守	本標準仕様に準拠するため、実装又は対応が必須となるもの。 本標準仕様に準拠するためには、本類型に該当する項目に示された全ての内容に適合している必要がある。	実装又は対応必須
推奨	実装又は対応が推奨されるもの。 本類型に該当する項目に示された機能の実装や対応がなされていない場合であっても、本標準仕様への準拠を標榜することができるが、レセコンを提供する事業者（以下本章において「ベンダー」という。）が開発する場合には、実装又は対応することが望ましい。 なお、本類型に該当する項目は、今後、本書の改定に際し、規定内容の一部又は全部が「遵守」類型に変更される場合がある。	実装又は対応任意
不可	本類型に該当する各項目に示された機能が実装され、又は示された条件に合致した場合、本標準仕様への準拠を標榜することが不可となるもの。	実装又は条件合致不可

類型	説明・考え方	ベンダーの対応
参考	今後「遵守」類型又は「推奨」類型としていくことも含め検討中の事項や、レセコンに係る具体的な仕様の検討に当たり参考となり得る情報について、参考情報として公表するもの。 なお、本類型に該当する項目は、今後、本書の改定に際し、規定内容の一部又は全部が「推奨」類型又は「遵守」類型に変更される場合があり、その際、規定内容の一部又は全部に変更がなされる場合がある。	実装又は対応任意

1.3.3 本書及び関連文書の一覧

本書及び関連文書の一覧は、次表に示すとおりである。

表 1-3 本書の構成

分類	資料名	概要
本書	医科診療所向けレセコン標準仕様書（基本要件）	レセコンの標準仕様（基本要件）を記載した資料。
本書別紙	別紙Ａ 政府情報システムにおける脆弱性診断導入ガイドラインに係る遵守事項一覧	政府情報システムにおける脆弱性診断導入ガイドラインに示された各項目のうち、レセコンに係る非機能要件として遵守すべき事項を一覧とした資料。
本書別紙	別紙Ｂ IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧	独立行政法人情報処理推進機構が示す「非機能要求グレード」各項目について、レセコンに係る非機能要件として遵守すべき事項を一覧とした資料。
関連文書	診療報酬改定 DX における共通算定モジュール外部イン	クラウド型レセコンを提供するベンダーが、共通算定モジュールを API で利用するに当たり必要となる改修作業や、モジュールのテスト版・製品版の提供スケジュール、運用方針等を整理した、共通算定モジュールの利用に必要なガ

分類	資料名	概要
	タフェース利用ガイド（案）	イダンスを記載した資料。 提供元： 医療機関等 ONS サイト（ベンダー向けサイト）
関連文書	電子レセプトの作成手引き（令和 6 年 9 月版）	社会保険診療報酬支払基金に提出する電子レセプトの記録方法を記載した資料 提供元： https://www.ssk.or.jp/smph/seikyushiharai/iryokikan/iryokikan_02.html
関連文書	アーキテクチャ要件を満たすシステム構成例と満たさない例	共用を前提とする環境（マルチテナント）のアーキテクチャ要件を満たすシステム構成例と満たさない例を記載した文書。 公開先： https://guide.gcas.cloud.go.jp/general/saas-technical-policy
関連文書	政府情報システムにおける脆弱性診断導入ガイドライン	政府情報システムに対する脆弱性診断を効果的に実施することを目的として、政府情報システムの管理責任や各機関のセキュリティ管理を担う職員に対して、脆弱性診断を実施する際の基準及びガイダンスを提供する文書。 公開先： https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/b08708cd/20240131_resources_standard_guidelines_guidelines_05.pdf
関連文書	デジタル庁 GCAS ガイドガバメントクラウドにおけるモダン化の定義	クラウド環境で構築されるアプリケーションのモダン化の定義を記載した文書。 公開先： https://guide.gcas.cloud.go.jp/general/overview/modernization-definition
関連文書	オンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・	オンライン資格確認等システムの導入に当たり、オンライン資格確認等システムが提供する機能及び医療機関・薬局のシステムベンダーが提供しているシステムに実装いただきたい内容等について記載した文書。（電子カルテと機能を重複して実装する必要はない。） 公開先： https://www.mhlw.go.jp/stf/index_00093.html

分類	資料名	概要
	薬局】（令和７年 12 月版）	
関連文書	電子処方箋管理サービスの導入に関するシステムベンダ向け技術解説書【医療機関・薬局】	電子処方箋管理サービスの導入にあたり、電子処方箋管理サービスが提供する機能、及び医療機関・薬局のシステムベンダー（電子カルテシステム、薬局システム等のシステムベンダーが対象）が提供しているシステムに実装していただきたい内容等について記載した文書。 公開先： https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/denshishohousen_systemvendor.html
関連文書	電子カルテ情報共有サービス記録条件仕様書 1.04 版 別紙_記録条件仕様_バリデーションチェックルール xlsx 1.06 版 別紙_記録条件仕様_バリデーションチェックルール pdf 1.06 版 別紙_記録条件仕様 XML 定義表 1.03 版	社会保険診療報酬支払基金・公益社団法人国民健康保険中央会により共同で組織される医療保険情報提供等実施機関において維持・運営する医療機関等向け総合ポータルサイトに掲載される、電子カルテ情報共有サービスに係る記録条件の仕様を規定した資料。 提供元： 医療機関等 ONS サイト（ベンダー向けサイト）
関連文書	電子カルテ情報共有サービスの導入に関するシステムベンダ向け技術解説書 電子カルテ情報共有サービスの導入に関	医療機関等が電子カルテ情報共有サービスを導入するにあたり、医療機関等システムの開発ベンダーに対し、同サービスに係る改修事項等を理解いただくための文書。 公開先： https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/denkarukyouyuu.html

分類	資料名	概要
	するシステムベンダ向け技術解説書（患者サマリー登録・閲覧サービス編）	
関連文書	オンライン資格確認等システム「外部インターフェイス仕様書」別紙 1-1 外部インターフェイス一覧（オン資格、電子処方箋、電カル情報共有）	社会保険診療報酬支払基金・公益社団法人国民健康保険中央会により共同で組織される医療保険情報提供等実施機関において維持・運営する医療機関等向け総合ポータルサイトに掲載される、オンライン資格確認等システム、電子処方箋管理サービス及び電子カルテ情報共有サービスが提供するインターフェイスを一覧にした資料。（電子カルテと機能を重複して実装する必要はない。） 提供元： 医療機関等 ONS サイト（ベンダー向けサイト）
関連文書	介護情報基盤「外部インタフェース仕様書」	医療・介護 DX サービスの一環である介護情報基盤において、電子カルテシステム等が主治医意見書や請求書を電子的に連携する際に必要となる機能要件が記載された仕様書。（電子カルテと機能を重複して実装する必要はない。） 公開先： https://www.mhlw.go.jp/stf/newpage_59231.html
関連文書	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（概説編）（令和５年５月） 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（経営管理編）（令和５年５	医療情報システムの安全管理や、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（平成 16 年法律第 149 号）等に適切に対応するため、技術的及び運用管理上の観点から所要の対策を示した資料。 公開先： https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

分類	資料名	概要
	月） 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（企画管理編）（令和５年５月） 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（システム運用編）（令和５年５月）	
関連文書	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第 2.0 版（令和７年３月）	クラウド事業者ガイドラインと情報処理事業者ガイドラインが求める要件について、総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」及び経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」が定める要件を整理・統合した資料。 公開先： https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html
関連文書	ウェブアクセシビリティ導入ガイドブック（令和７年 10 月 16 日版）	ウェブアクセシビリティに初めて取り組む行政官や事業者向けに、ウェブアクセシビリティの考え方、取り組み方のポイントを解説するガイドブック。 公開先： https://www.digital.go.jp/resources/introduction-to-web-accessibility-guidebook
関連文書	医療情報セキュリティ開示書（SDS Ver5.0）	医療機関等が医療情報システムによって保存、伝送される医療情報に関するリスクアセスメントを行うとき、それを支援できる重要な情報を提供するために作られたチェックリスト。 公開先：

分類	資料名	概要
		https://www.jahis.jp/standard/detail/id=1119

2　標準仕様（基本要件）

2.1 レセコン

レセコンの機能要件、非機能要件、アーキテクチャ及びデータ移行に係る仕様について、標準仕様（基本要件）を示す。

※　医療機関が、本標準仕様書に準拠したレセコンを設置することを妨げるものではない。

2.1.1　機能要件

（1）考え方

レセコンの機能のうち、各種医療 DX サービス群との接続機能について、必要な機能要件を定める。

（2）機能要件に係る標準仕様（基本要件）

①「遵守」類型に該当する項目（必須要件）

No	仕様
1	次に掲げる要件の全てに適合すること。 なお、個々の医療機関においては、業務上必要のない機能を実装する必要はなく、次に掲げる要件に規定する全ての機能を必ず実装することを求めるものではない。 （1）「診療報酬改定 DX における共通算定モジュール外部インタフェース利用ガイド」（製品版又は当該版以後に作成された版）に準拠し、共通算定モジュールと連携すること。 （2）レセコンについて、「オンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局】」（令和７年 12 月版又は当該版以後に作成された版）に規定された機能を有すること。 （3）レセコンについて、「電子処方箋管理サービスの導入に関するシステムベンダ向け技術解説書【医療機関・薬局】」（令和７年 12 月版又は当該版以後に作成された版）に規定された電子処方箋に係る機能（処方箋取消 UNDO 機能、処方箋変更機能、処方箋変更 UNDO 機能、重複投薬等チェック事前処理機能、処方箋 ID 検索機能、院内処方機能を除く。）を有すること。 （4）レセコンについて、医療機関等 ONS サイト上に掲載された「電子カルテ情報共有サービス記録条件仕様書」（第 1.04 版又は当該版以後に作成された版）並びに「別紙_記録条件仕様_バリデーションチェックルール.xlsx」（第 1.06 版又は当該版以後に作成された版）、「別紙_記録条件仕様_バリデーションチェックルール.pdf」（第 1.06 版又は当該版以後に作成された版）及び「別紙_記録条件仕様 XML 定義表」（第 1.03 版又は当該版以後に作成された版）並びに「電子カルテ情報共有サービスの導入に関するシステムベンダ向け技術解説書」（第 2.0.0 版又は当該版以後に作成された版）に規定された電子カルテ情報共有サービスに係る機能を有すること。

②「推奨」類型に該当する項目（推奨要件）

No	仕様
1	次に掲げる要件に適合することが望ましいこと。 （1）レセコンについて、「電子処方箋管理サービスの導入に関するシステムベンダ向け技術解説書【医療機関・薬局】」（令和７年 12 月版又は当該版以後に作成された版）に規定された電子処方箋に係る機能（処方箋取

No	仕様
	消 UNDO 機能、処方箋変更機能、処方箋変更 UNDO 機能、重複投薬等チェック事前処理機能、処方箋 ID 検索機能、院内処方機能に限る。）を有すること。 （２） レセコンについて、医療機関等 ONS サイト上に掲載された「電子カルテ情報共有サービスの導入に関するシステムベンダ向け技術解説書（患者サマリー登録・閲覧サービス編）」（第 1.0.0 版又は当該版以後に作成された版）に規定された電子カルテ情報共有サービスに係る機能を有すること。 （３） 国が推進する医療 DX に関連した各種サービスについて、当該サービスの利用又は当該サービスとの接続のために必要なレセコンの機能が公表された場合には、当該機能を有すること。

③「参考」類型に該当する項目

なし

（３）経過措置

（２）①表中１（２）は、レセコンと電子処方箋サービスとの間でクラウド間の連携が実現した旨の公表の日から起算して３月が経過するまでの間は適用せず、推奨項目として取り扱うものとする。

（２）①表中１（３）は、レセコンと電子カルテ情報共有サービスとの間でクラウド間の連携が実現した旨の公表の日から起算して３月が経過するまでの間は適用せず、推奨項目として取り扱うものとする。

2.1.2 非機能要件

（１）考え方

レセコンについて、クラウド技術を活用したモダンシステムへの刷新を図りつつ、医療機関として必要十分な可用性、セキュリティ、バックアップ環境等を確保するため、必要な非機能要件を定める。

（２）非機能要件に係る標準仕様（基本要件）

①「遵守」類型に該当する項目（必須要件）

No	項目	仕様
1	可用性	次に掲げる要件に適合すること。 ・稼働率の実績が 99.9%以上であること。 なお、稼働率（%）は、以下の計算式により定義する。 【 稼働率＝年間実稼働時間／年間予定稼働時間×100 】 ※ 当該計算式において、年間実稼働時間は「利用者がサービスを利用可能であった時間の合計」、年間予定稼働時間は「事前に予定された年間稼働時間（24 時間 365 日であるかどうかは問わない。）から計画停止時間及び大規模災害による停止・縮退時間を除いた時間の合計」と定義する。 このため、年間実稼働時間を算出できない新規製品については、目標稼働率が 99.9%以上であることを要件とする。ただし、既存製品に一部の機能を追加したものを新規製品と称している場合には、既存製品に係る稼働率を算出し、適合性を

No	項目	仕様
		判断することとして差し支えない。 なお、稼働率は、あらかじめサービス仕様書等において定義された責任分界の範囲内を対象として算出するものとする。
2	セキュリティ	次に掲げる要件の全てに適合すること。 （１） ISMAP に登録されているクラウドサービスを利用すること。特定のクラウドサービスの指定はしない。ISMAP のリストにあるサービスで代替できないサービスを利用する場合は、「政府情報システムのためのセキュリティ評価制度（ISMAP）の暫定措置の見直しについて」（令和３年７月６日サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定）に係る暫定措置の条件を満たすことを確認したうえで、当該クラウドサービスを利用することも可能とする。 （２） 第三者機関によりペネトレーションテストを実施し、脆弱性を検知した場合は、当該脆弱性について適切な対策を講ずること。 （３） レセコンを構成する主要なソフトウェアについて脆弱性診断を実施し、脆弱性を検知した場合は、当該脆弱性について適切な対策を講ずること。 脆弱性診断は、政府情報システムにおける脆弱性診断導入ガイドライン（2024（令和６）年１月 31 日）（「別紙Ａ 政府情報システムにおける脆弱性診断導入ガイドラインに係る遵守事項一覧」に規定する項目に限る。）に適合した態様で実施すること。 （４） システムを構成する各要素に対し、定期的にセキュリティパッチを適用すること。また、緊急のセキュリティパッチが配布された場合には直ちに適用できるよう、必要な対策を講ずること。さらに、各医療機関に設置された関係する端末等におけるセキュリティパッチの適用を妨げることのないよう、関係するセキュリティパッチ（最新バージョンの OS や Web ブラウザへの更新を含む。）が公開された場合には、速やかに互換性を検証するとともに、当該検証の結果必要がある場合には、互換性を維持するための手段を速やかに講じること。
3	データ保管	次に掲げる要件に適合すること。 ・データが日本国内で保持され、海外に送信されることのないよう設定すること。
4	バックアップ環境の整備	次に掲げる要件に適合すること。 ・マルウェア感染等により、主たるクラウド上のデータが利用不能となった場合に備え、物理的かつ論理的に隔離された別のクラウドサーバ上又はテープメディア等の外部メディアに定期的なバックアップを行う仕様とし、冗長性、信頼性及び可用性を確保すること。
5	ガイドライン等/非機能要求グレード	次に掲げる要件の全てに適合すること。 （１） レセコンが提供する機能のうち、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（令和５年５月）に関係する部分について、同ガイドラインに適合するものであること。 なお、同ガイドラインは医療機関の運用について規定するものであるところ、レセコンが提供する機能に関連する部分以外

No	項目	仕様
		の箇所への適合性については、本標準仕様の対象外とする。 （２） 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第 2.0 版（令和７年３月）に適合するものであること。 （３） 「別紙Ｂ IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧」に規定する各項目に適合すること。

②「推奨」類型に該当する項目（推奨要件）

No	項目	仕様
1	アクセシビリティ	次に掲げる要件に適合することが望ましいこと。 ・ウェブアクセシビリティ導入ガイドブック「3.1 達成しないと利用者に重大な悪影響を及ぼすもの」及び「3.2 必ず達成しなければならないもの」に記載の内容を遵守していること。

③「参考」類型に該当する項目

No	項目	仕様
1	セキュリティ	次に掲げる要件に留意すること。 ・ア又はイの認証（レセコンを含めた包括的な認証である場合を含む。）を取得したものであること。ただし、レセコンがガバメントクラウドを利用している場合にあっては、次に掲げる要件に適合しているものとみなすこと。 ア 政府情報システムのためのセキュリティ評価制度（ISMAP） イ ISMS 認証及び ISMS クラウドセキュリティ認証 ただし、レセコンがガバメントクラウドを利用している場合にあっては、全てに適合しているものとみなす。

2.1.3 アーキテクチャ

（1）考え方

レセコンについて、医療機関単位のカスタマイズを廃して標準パッケージとしての機能を充実させるとともに、マルチテナント方式のクラウド・ネイティブ化を図ることによりコストの最適化を図るため、レセコンのアーキテクチャや処理方式に係る設計の方針について、標準的な仕様を規定する。

（2）アーキテクチャに係る標準仕様（基本要件）

①「遵守」類型に該当する項目（必須要件）

No	項目	仕様
1	クラウドネイティブ・アーキテクチャ	次に掲げる要件の全てに適合すること。 ・レセコンを構成するアプリケーションは、原則としてパブリッククラウド環境で稼働すること。ただし、次に掲げる機能を有するアプリケーションにあっては、この限りでない。 ① 医療機関内に設置された機器等（例：資格確認端末、プリンター）との通信を中継又は制御するための機能

No	項目	仕様
	指針	②　見読性を担保するためのデータ保管に係る機能 ③　クラウド障害等の非常時における事業継続のための機能
2	モダナイゼーション（アプリケーションのモダン化）	次に掲げる要件に適合すること。 ・マネージドサービスの利用、疎結合なアーキテクチャの採用、多要素認証の導入等、モダン化がなされた技術を採用すること。

②「推奨」類型に該当する項目（推奨要件）

No	項目	仕様
1	クラウドネイティブ・アーキテクチャ指針	次に掲げる要件の全てに適合することが望ましいこと。 （1） 医療機関に提供される、クラウド上で稼働する全てのアプリケーションは、SaaS 型であること。 （2） レセコンの構成は、マルチテナント方式であること。 （3） クラウド上で稼働するアプリケーションのソースコードは、全てのテナントについて共通であることを前提としたサービス設計とし、アプリケーションのテスト、更新等による一時的なものを除き、複数のバージョンが併存しない仕様であること。なお、特定の診療科に特化した機能を搭載するためにソースコードを区分したものについては、複数のバージョンの併存には当たらないものとする。ただし、ソースコードの管理体系及び各ソースコードが対象とする診療科の整理が明確である場合に限る。 （4） レセコンを構成する全てのアプリケーションについて、個々の医療機関におけるカスタマイズに対応不可能な仕様とすること。 ただし、医療機関の要望等により追加した機能を、有償無償にかかわらず、当該レセコンのオプション機能として、当該レセコンを使用する全ての医療機関が必要に応じて利用できる場合には、カスタマイズには当たらないものとする（機能強化等）。 なお、アプリケーション上の設定やメタデータの変更により、個々の医療機関における環境に対応させることは差し支えない。

③「参考」類型に該当する項目

No	項目	仕様
1	クラウドネイティブ・アーキテクチャ指針	次に掲げる要件に留意すること。 ・レセコンを構成するアプリケーションは、ガバメントクラウドで稼働すること。

2.1.4　データ移行

【※検討中】

2.3 システム等間の連携

レセコンと各種医療 DX サービス群との間及びレセコンと部門システムその他の外部システム等（医療 DX サービス群は含まない。以下本章において同じ。）との間における連携に係る仕様について、標準仕様（基本要件）を示す。

2.2.1 レセコン－医療 DX サービス群間の API 仕様

（1） 考え方

レセコンとの接続が可能となっている各種医療 DX サービス群を可視化するとともに、同サービス群との接続方法を示し、同サービス群の利用を促進することを目的として、レセコンと同サービス群との間における個別インターフェイスの仕様を標準仕様（基本要件）として規定する。

（2） レセコンと各種医療 DX サービス群との間における個別インターフェイスに係る標準仕様（基本要件）

① 「遵守」類型に該当する項目（必須要件）

No	項目	仕様
1	オンライン資格確認等システム／電子処方箋管理サービス／電子カルテ情報共有サービス	次に掲げる要件の全てに適合すること。 ・医療機関等 ONS サイト上に掲載された「外部インターフェイス仕様書（オン資格、電子処方箋、電カル情報共有）」（第 8.09 版又は当該版以後に作成された版）、「外部インターフェイス仕様書（オン資格、電子処方箋、電カル情報共有_WebAPI 連携編）」（第 8.10 版又は当該版以後に作成された版）、「別紙 1-1 外部インターフェイス一覧（オン資格、電子処方箋、電カル情報共有）」（第 8.07 版又は当該版以後に作成された版）及び「別紙 1-2 外部インターフェイス一覧（薬剤情報等・特定健診情報・臨床情報）」（第 5.03 版又は当該版以後に作成された版）に規定されたインターフェイスとの接続機能を有し、オンライン資格確認等システム、電子処方箋管理サービス及び電子カルテ情報共有サービスとの接続が可能であること。 ただし、レセコンに接続された電子カルテが当該各インターフェイスとの接続機能を有し、電子カルテから当該各システムに接続がなされている場合は、レセコンにおいて、当該各インターフェイスとの接続機能を重複して有する必要はないこと。 なお、上記は、個々の医療機関において、「外部インターフェイス仕様書（オン資格、電子処方箋、電カル情報共有）」等に規定する全ての機能を必ず実装することを求めるものではない。例えば、訪問診療を実施する機会を有しない医療機関において、訪問診療のみのために必要なインターフェイスとの接続機能を実装する必要はない。

②「推奨」類型に該当する項目（推奨要件）

No	項目	仕様
1	その他のサービス	次に掲げる要件に適合することが望ましいこと。 （1）介護情報基盤「外部インタフェース仕様書」に規定されたインターフェイスとの接続機能を有すること。 ただし、レセコンに接続された電子カルテ等が当該インターフェイ

No	項目	仕様
		スとの接続機能を有する場合は、レセコンにおいて、当該インターフェイスとの接続機能を重複して有する必要はないこと。 （２）国が推進する医療 DX に関連した各種サービスについて、レセコンとの接続のためのインターフェイスが公表された場合には、公表された仕様に基づくインターフェイスとの接続機能を有すること。

③「参考」類型に該当する項目

なし

（３） 経過措置

（２）①表中１のうち電子処方箋に係る部分は、レセコンと電子処方箋管理サービスとの間で、クラウド間の連携が実現した旨の公表の日から起算して３月が経過するまでの間は適用せず、推奨項目として取り扱うものとする。

（２）①表中１のうち電子カルテ情報共有サービスに係る部分は、レセコンと電子カルテ情報共有サービスとの間で、クラウド間の連携が実現した旨の公表の日から起算して３月が経過するまでの間は適用せず、推奨項目として取り扱うものとする。

2.2.2 レセコン－外部システム等間における連携共通仕様

【※検討中】

2.2.3 API 個別仕様（レセコン－部門システム）

【※検討中】

2.4 情報提供・公開

（１）考え方

レセコン製品のサポートレベル、価格帯等を医療機関が把握しやすくすることを目的として、標準的なレセコンとして求められる情報提供又は公開に係る考え方について、標準仕様（基本要件）として規定する。

（２）情報の提供又は公開に係る標準仕様（基本要件）

①「遵守」類型に該当する項目（必須要件）

No	項目	仕様
1	情報提供・公開	次に掲げる要件の全てに適合すること。 （１）ベンダーが自ら運営する Web サイト上に、電子カルテの価格（オプション機能に係る価格を含む。）を公開済であること。 （２）医療機関等（医療機関及び医療機関から委託を受けた者をいう。以下 2.3 において同じ。）の要請があった場合、レセコンに関して記入済の医療情報セキュリティ開示書（SDS Ver5.0）について開示すること。 （３）医療機関等の要請があった場合、医療機関におけるサイバーセキュリティ対策チェックリスト（事業者確認用）に

No	項目	仕様
		ついて開示すること。 （４）医療機関等の要請があった場合、レセコンを医療機関に提供する場合のサービス仕様適合開示書及びサービス仕様書について開示すること。 （５）医療機関等の要請があった場合、レセコン間のデータ移行に必要な事項（データ形式を含む。）について開示すること。 （６）医療機関等又はレセコンとの接続を求める部門システムに係るベンダーの要請があった場合、レセコンと部門システムとの間におけるインターフェイスの仕様について開示すること。 （７）医療機関の要請があった場合、レセコンについて、医療機関から問い合わせがあった際の一次回答時間の直近３か月の平均値について開示すること。

②「推奨」類型に該当する項目（推奨要件）

No	項目	仕様
1	情報提供・公開	次に掲げる要件に適合することが望ましいこと。 （１） 医療機関等の要請があった場合、契約締結前であっても、システムのデモンストレーション等を実施することにより、レセコンが有する詳細な機能について開示すること。 （２） 医療機関等の要請に応じ、契約締結前であっても、レセコンのトライアルが可能であること。また、トライアルの実施期間中又はその前後の期間において、適切な支援が可能であること。 （３） レセコンとの接続を求める外部システム等のベンダーが、当該接続について円滑に検討できるよう、適切なテスト環境を整備し、その利用法等について公開すること。

③「参考」類型に該当する項目

なし

2.5　留意事項

（1）第１章（電子カルテ標準仕様書）との関係性について

本標準仕様は、レセコンと電子カルテが別個のシステムである場合には当該レセコン部分の、また、レセコンと電子カルテが一体となったシステムである場合には当該システムのうちレセコン部分の、それぞれ標準的な仕様を規定するものである。

レセコンと電子カルテが一体となったシステムでは、一体的な管理運用が想定されるところ、例えば非機能要件の一部等、同一の事項に関して第１章の規定と本章の規定が異なっている場合には、第１章の規定内容を優先して適用するものとする。

3　本書の改訂

本書は、一定の頻度による定期的な改定（以下本章において「定期改定」という。）を予定している。

予定される定期改定の内容には、標準化する対象データ範囲の拡大又は一部内容の修正、接続対象となる医療 DX サービスの追加、類型の変更等が含まれる。

本書は、定期改定のほか、臨時に改定される場合がある。

(参考)

今後の定期改定の内容としては、以下に掲げるものが対象となり得る。

（1）接続対象となる医療 DX サービスの拡大

医療 DX サービス群に属するシステムは、複数のシステムの開発について国が取組を進めており、順次、技術的な仕様が公開される見込みである。このため、本標準仕様において対象とする医療 DX サービスの範囲についても、定期改定により段階的に拡大することを想定している。

初版においては、以下に掲げるサービスが接続対象となる。

- 共通算定モジュール
- オンライン資格確認等システム
- 電子カルテ情報共有サービス
- 電子処方箋管理サービス
- 介護保険に係る主治医意見書／請求書電送サービス

今後、以下に掲げる取組を通じ、レセコンからの接続先や対象となるデータの範囲が拡大される見込みであり、次版以降において順次、本標準仕様に規定する予定である。

- 共通算定モジュールの請求支援機能
- 診療報酬改定に伴う対応
- 医療保険法等の改正に伴う制度改正対応
- 国公費負担医療、地方自治体による医療費助成の現物給付化への対応
- 予防接種のデジタル化（予診情報・予防接種記録管理／請求支払システム）

（順不同。実際の規定の時期についてはそれぞれの改正時期による。）

（2）標準コード・マスタの策定及び更新の反映

厚生労働省においては、医薬品・検査等の標準コード・マスタ及びこれらの維持管理体制の整備に係る取組を進めているところである。

当該標準コード・マスタの策定は、概ね部門システムの種別毎に検討を進める予定であり、具体的には、①医療現場において使用される臨床情報の整理、②システム間交換規約の策定、③コード体系の策定、④マスタの策定、⑤インターフェイス仕様書の策定を経て、⑥記録条件仕様定義表の策定を目指すこととしている。

これらの検討の結果、当該標準コード・マスタが確立した場合には、主に（3）及び（4）に示す形で、本標準仕様への追加が見込まれる。

また、こうして策定した標準コード・マスタは、状況の変化に適確に対応できるよう継続的に維持管理を行っていくことが想定され、標準コード・マスタの更新があった場合には、当該内容についても、本標準仕様に反映していくことが見込まれる。

（３）レセコンと外部システム等との間における連携仕様の追加等

（２）に係る検討の結果、部門システムの種別毎に、標準的なコード、マスタ、インターフェイス仕様書及び記録条件仕様定義表が策定されることが見込まれる。レセコンー外部システム等間における連携に必要な仕様については、策定された標準的なコード等に基づき、順次、本標準仕様に規定していく予定である。

また、標準的なコード等に更新があった場合には、関係部分の仕様について併せて更新することが見込まれる。

（４）データ移行に係る共通仕様及び個別インターフェイスの追加等

レセコン間のデータ移行に係る共通仕様や個別インターフェイスは、（２）の標準的なコード等及び（３）のレセコンー外部システム等間における連携に必要な仕様と一定の関連がある。このため、データ移行に係る標準的な仕様については、今後、（２）及び（３）に係る検討も踏まえて策定し、本標準仕様に規定していく予定である。

また、標準的なコード等に更新があった場合には、関係部分の仕様について併せて更新することが見込まれる。

（５）レセコンの標準的 API において対象とするデータ範囲の拡大

レセコンー外部システム等間における連携については、今後、部門システム等に関する詳細な仕様を順次策定していくことやレセコン機能に係る新たなモジュールの開発に伴い、対象となるデータ範囲の拡大が見込まれる。

（６）３省２ガイドラインの改定に伴うセキュリティ要件の追加

本標準仕様では、３省２ガイドラインへの準拠を原則とした上で、その一部については外部監査により対応できる形で要件を規定している。３省２ガイドラインについては、クラウド型サービスを対象とするために一部改定が検討されており、仮に改定がなされた場合には、本標準仕様におけるセキュリティ要件についても、併せて改定がなされる可能性がある。

4 用語

本書についての解釈に紛れが生じないよう、用いられている用語の解説を以下に示した。ここで示す解説はあくまで本書における考え方であり、用語によっては、本書以外では別の意味で用いられていることもある。

表 4-1 用語の解説

No	用語	説明
1	先行/協力/準協力レセコンベンダー	医科・DPC の共通算定モジュールに係る品質検証等を行うベンダー。共通算定モジュールの開発主体である、社会保険診療報酬支払基金によって、選定されている。
2	アプリケーション	アプリケーションとは、コンピュータ上で使うソフトウェアの一種で、特定の目的や作業を行うためのプログラムのことをいう。本書では、レセコンの機能の提供を目的にしたソフトウェアのことをいう。
3	インターフェイス	インターフェイスとは、他のシステムや外部サービスと連携するための接続仕様を指す。データの受け渡し方法、通信プロトコル、データ形式（例：JSON、CSV）などを定義し、システム間の連携や自動処理を可能にする。
4	オンプレミス	オンプレミスとは、診療所内に IT インフラ（サーバ、ネットワーク機器、データベース、アプリケーションなど）を設置し、管理・運用する形態をいう。
5	ガバメントクラウド	「デジタル社会の実現に向けた重点計画」等の政府方針に基づき、安全かつ合理的な利用環境としてデジタル庁が選定した複数のパブリッククラウド（IaaS、PaaS、SaaS）のこと。情報通信技術を活用した行政の推進等に関する法律（平成 14 年法律第 151 号）第 23 条第２項に規定する共同利用クラウド・コンピューティング・サービスをいい、国と公共情報システム整備運用者が共同して利用することができるものとされたクラウド・コンピューティング・サービスである。
6	クラウドサービス	クラウド事業者が提供するコンピューティング資源を、ネットワークを通じて利用できるサービス。その提供形態から、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）及び SaaS（Software as a Service）に区分される。また、実現形態から、プライベートクラウド、パブリッククラウド及びハイブリッドクラウドに区分することができる。
7	サービス仕様書	サービス仕様書とは、書面にしたサービス提供者と顧客との

No	用語	説明
		合意であって、サービス及びサービス目標を特定した、サービス提供者と顧客との間の合意文書(JIS Q 20000-1:2020)をいう。 作成に当たっては、安全管理ガイドラインの別紙１「ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例」を参照すること。
8	サービス仕様適合開示書	サービス仕様適合開示書とは、対象事業者が、自ら提供するサービスの仕様につき、安全管理ガイドラインへの適合状況を医療機関等へ開示するために作成するための資料のことをいう。 作成に当たっては、安全管理ガイドラインの別紙１「ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例」を参照すること。
9	脆弱性	脆弱性とは、脅威によって悪用される可能性がある欠陥や仕様上の問題をいう。
10	脆弱性診断	脆弱性診断とは、システムやアプリケーション、ネットワークに潜むセキュリティ上の弱点（脆弱性）を事前に検出し、リスクを評価するための技術的な評価手法のことをいう。
11	政府情報システムのためのセキュリティ評価制度（ISMAP）	政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度のことをいう。
12	ソフトウェア	ソフトウェアとは、コンピュータやスマートフォン、タブレットなどの電子機器を動かすプログラムやアプリケーションのことをいう。
13	レセプトコンピュータ（医事会計システム）	レセプトコンピュータとは、医療機関において、診療行為等の情報に基づき診療報酬を算定し、患者負担金を計算するとともに、診療報酬請求のための診療報酬明細書（レセプト）の作成及び請求処理を行う機能を有するコンピュータをいう。 算定から請求までの医事会計業務を一貫して電子的に処理でき、会計・請求業務の正確性・迅速性の向上や事務負担の軽

No	用語	説明
		減、業務効率化が図られる。また、他の医療情報システム等との連携により、さらなる効率化が期待される。
14	電子カルテ	電子カルテとは、従来、医師が患者の診療記録を記入していた紙のカルテ（診療録）を電子化し、データとして保存したものをいう。紙のカルテを電子化することにより、関連する検査結果や画像等も一元的に管理できるようになり、利便性や検索性が向上するとともに、他のシステムとの連携により、業務効率化にもつながることが期待される。
15	パブリッククラウド	パブリッククラウドとは、クラウドサービス事業者が所有するクラウド基盤を、不特定多数の利用者に広く提供するサービス形態であり、一般的にはインターネット経由で利用される。複数の利用者が共同でインフラを共有する点が特徴である。
16	プライベートクラウド	プライベートクラウドとは、特定の企業や組織専用に構築・提供されるクラウド環境のことをいい、第三者とインフラを共有しない点が特徴である。
17	ペネトレーションテスト	ペネトレーションテストとは、組織が運用するシステムやネットワーク、アプリケーションに対して、攻撃者の視点から脆弱性を検証するセキュリティ評価手法をいう。
18	マルチテナント方式	マルチテナントとは、共同利用を前提とする環境のことをいう。 本書が想定するマルチテナント方式の具体的な態様は、「デジタル庁 GCAS ガイド　公共 SaaS の共通要件にかかる技術方針 3.10　アーキテクチャ要件を満たすシステム構成例と満たさない例」に規定する「アーキテクチャ要件を満たすシステム構成」である。
19	モダン化	モダン化とは、最先端の実験的な技術ではなく、ある程度一般化した新しい技術を活用する方針を採用することをいう。 本書が想定するモダン化の具体的な態様は、「デジタル庁 GCAS ガイド　ガバメントクラウドにおけるモダン化の定義」の１～５をいう。 １．API ベースのシステム構成 ２．ステートレスなアーキテクチャ ３．マネージドサービスの活用 ４．運用のコード化、自動化 ５．サービスレベルの定義、計測

No	用語	説明
20	ライブラリ	ライブラリとは、プログラムの部品や機能をまとめたファイル群のことをいう。
21	API	API（Application Programming Interface：アプリケーション・プログラミング・インターフェース）とは、ソフトウェア同士が機能やデータを相互にやり取りするための接点や規約をいう。
22	BCP	BCP(Business Continuity Plan)とは、事業継続計画のことをいう。
23	IaaS	IaaS(Infrastructure as a Service)とは、CPU、メモリ、ストレージ、ネットワーク等のハードウェア資産をサービスとして提供するクラウドサービスをいう。
24	ISMS 認証	対象となる組織が、国際規格 ISO/IEC 27001 に基づき、情報資産を適切に管理・保護するための仕組みを整備・運用していることについて、認定を受けた第三者機関が審査し認証する制度。
25	ISMS クラウドセキュリティ認証	対象となる組織（クラウドサービス事業者又はクラウドサービスを利用する組織）が、国際規格 ISO/IEC 27017 及び ISO/IEC 27018 に基づき、クラウド特有のリスクに対応した情報セキュリティ管理の仕組みを整備・運用していることについて、認定を受けた第三者機関が審査し認証する制度。
26	SDS	「サービス事業者による医療情報セキュリティ開示書（SDS）」の略称で、（一社）保健医療福祉情報システム工業会（JAHIS）及び（一社）日本画像医療システム工業会（JIRA）が定めた各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する説明の標準的記載方法（書式）のことをいう。これらの書式は製品/サービスの説明の一部として製造業者/サービス事業者が作成し、セキュリティマネジメントを実施する医療機関等を支援するために用いられることが想定されている。
27	PaaS	PaaS（Platform as a Service)とは、オペレーションシステムや、アプリケーションの実行環境をサービスとして提供するクラウドサービスをいう。
28	SaaS	SaaS（Software as a Service）とは、ソフトウェアがインターネットを通じて提供されるサービス形態をいう。従来のよ

No	用語	説明
		うにユーザーが自社のパソコンやサーバにソフトウェアをインストールして利用するのではなく、SaaS では、クラウド上に構築されたアプリケーションを、Web ブラウザなどを通じて利用する形態となる。
29	３省２ガイドライン	「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」（令和５年５月）及び「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第 2.0 版」（令和７年３月）をいう。

第１章 別紙Ａ
政府情報システムにおける
脆弱性診断導入ガイドラインに係る
遵守事項一覧

令和８（2026）年 XX 月 XX 日

厚生労働省医政局

厚生労働省保険局

デジタル庁国民向けサービスグループ

改訂履歴

版数	改訂年月日	該当箇所	内容
X.X	令和８年 XX 月 XX 日	初版	初版作成

医科診療所向け電子カルテにおいて脆弱性診断を実施する場合の「政府情報システムにおける脆弱性診断導入ガイドライン」に係る遵守事項は、中小病院向け電子カルテ及びレセプトコンピュータ標準仕様書（基本要件）第X.X版第１章別紙Ａ「政府情報システムにおける脆弱性診断導入ガイドラインに係る遵守事項一覧」に規定するものとする。

第１章 別紙Ｂ
IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧

令和８（2026）年 XX 月 XX 日

厚生労働省医政局

厚生労働省保険局

デジタル庁国民向けサービスグループ

改訂履歴

版数	改訂年月日	該当箇所	内容
X.X	令和８年 XX 月 XX 日	初版	初版作成

IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧

（１）考え方

非機能要件における標準として独立行政法人情報処理推進機構（IPA）が示している「非機能要求グレード」を基に、（２）に掲げる表のとおり、電子カルテが遵守すべき非機能要件を策定した。
なお、策定に当たっては、以下に該当する項目を除外した。
・本標準仕様の他の記載や、本標準仕様において引用している他のガイドライン等と内容が重複する項目
・オンプレミス型のシステムであることが前提となっている項目
・クラウドサービス事業者の責任範囲となる項目
・ベンダーに対し、一律に一定の水準を求めることが必ずしも適切でない項目

（２）遵守事項一覧

遵守事項（必須要件）								要求レベルに対する具体的な考え方及び対応の例	（参考）要求レベルを満たした場合、併せて該当部分が準拠となるガイドライン		
項番	大項目	中項目	小項目	小項目説明	メトリクス	要求レベル			医療情報システムの安全管理に関するガイドライン	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	デジタル庁GCASガイド
						選択レベル	詳細				
A.1.2.1	可用性	継続性	業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件。	対象業務範囲	2	内部向け全業務	サービス仕様適合開示書にて規定する責任範囲内において、診療業務の継続を目的に、電子カルテに登録されている全データの閲覧が可能な状態を継続できる。 また、上記が達成できない場合は、継続性を確保する対象を定義した上で、当該対象を定めるに当たっての考え方(対象業務の特徴、必要性等)を示す。 ※なお、インターネットへの接続性については、インターネット接続を提供する事業者及びそのバックアップ回線を提供する事業者の責務となることが考えられる。		○	
A.1.3.1	可用性	継続性	目標復旧水準（業務停止時）	業務停止を伴う障害が発生した際、何をどこまで、どれ位で復旧させるかの目標。	RPO（目標復旧地点）	3	障害発生時点（日次バックアップ+アーカイブからの復	目標復旧地点は、障害発生時点（日次バックアップ＋アーカイブからの復旧などを想定）とする。 なお、障害発生時点とは、障害が発生する直前のトランザクションなどの処理が完了している時点のことをいう。	○		
B.1.3.1	性能・拡張性	業務処理量	保管期間	システムが参照するデータのうち、OSやミドルウェアのログなどのシステム基盤が利用するデータに対する保管が必要な期間。 必要に応じて、データの種別毎に定める。 保管対象のデータを選択する際には、対象範囲についても決めておく。	保管期間	3	5年	医療情報に関するアクセスを記録したログ（操作ログ等※）を対象に、直近５年以上のログを保管する。 ※対象となるログは以下に掲げるとおりとし、これらに該当しないログの保管期間は任意とする。 ・システム利用者がシステム利用時に医療情報へアクセス又は操作(参照・更新等)した際の証跡となるもの ・運用保守担当が運用保守時に医療情報へアクセス又は操作(参照・更新等)した際の証跡となるもの	○	○	
C.1.2.3	運用・保守性	通常運用	バックアップ	システムが利用するデータのバックアップに関する項目。	バックアップ利用範囲	3	データの長期保存（アーカイブ）	データの長期保存及びデータの回復に対応する。具体的には、以下のとおりである。 〇データの長期保存：医師法第24条（診療録の記載及び保存）及び医療法施行規則 第30条の４（診療に関する諸記録の保存期間）に基づき、以下に掲げる文書は、それぞれ定められた期間の長期保存に対応する。 ・診療録：５年 ・診療に関する諸記録（処方せん、手術記録、看護記録など）：２年 〇データの回復：障害時にバックアップデータからの回復が必要となった場合、その手順が明文化又は自動化されている。	○		
C.1.4.1	運用・保守性	通常運用	時刻同期	システムを構成する機器の時刻同期に関する項目。	時刻同期設定の範囲	4	システム全体を外部の標準時間と同期する	システム全体で標準時間との同期を行う。 ※アクセスログ等の調査やセキュリティ監視において支障を来さないため	○		

IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧

（１）考え方

非機能要件における標準として独立行政法人情報処理推進機構（IPA）が示している「非機能要求グレード」を基に、（２）に掲げる表のとおり、電子カルテが遵守すべき非機能要件を策定した。
なお、策定に当たっては、以下に該当する項目を除外した。
・本標準仕様の他の記載や、本標準仕様において引用している他のガイドライン等と内容が重複する項目
・オンプレミス型のシステムであることが前提となっている項目
・クラウドサービス事業者の責任範囲となる項目
・ベンダーに対し、一律に一定の水準を求めることが必ずしも適切でない項目

（２）遵守事項一覧

遵守事項（必須要件）								要求レベルに対する具体的な考え方及び対応の例	（参考）要求レベルを満たした場合、併せて該当部分が準拠となるガイドライン		
項番	大項目	中項目	小項目	小項目説明	メトリクス	要求レベル			医療情報システムの安全管理に関するガイドライン	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	デジタル庁GCASガイド
						選択レベル	詳細				
E.4.3.2	セキュリティ	セキュリティリスク管理	セキュリティパッチ適用	対象システムの脆弱性等に対応するためのセキュリティパッチ適用に関する適用範囲、方針および適用のタイミングを確認するための項目。 これらのセキュリティパッチには、ウィルス定義ファイル等を含む。 また、セキュリティパッチの適用範囲は、OS、ミドルウェア等毎に確認する必要があり、これらセキュリティパッチの適用を検討する際には、システム全体への影響を確認し、パッチ適用の可否を判断する必要がある。 なお、影響の確認等については保守契約の内容として明記されることが望ましい。	セキュリティパッチ適用方針	2	全てのセキュリティパッチを適用	システムを構成する各要素に対するセキュリティパッチの適用については、対策を実施した際の業務への影響並びに対策処理の速度、可用性及び網羅性について十分な検討を行った上で実施する。セキュリティパッチの適用に当たっては、その基準となるルールを設定する。 セキュリティパッチを適用する範囲は、サービス仕様適合開示書等にて定める責任範囲内の全てとする。（サービスを提供するサーバー及びネットワークに関連する機器のほか、サービス提供の範囲によっては端末(PC)も含む。）	○		
E.5.1.1	セキュリティ	アクセス・利用制限	認証機能	資産を利用する主体（利用者や機器等）を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目。 複数回の認証を実施することにより、抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード等を用いた認証等がある。	管理権限を持つ主体の認証	3	複数回、異なる方式による認証	○システム利用者（ユーザ）認証として二要素認証によりユーザーを識別し、システムへのアクセスを制御する。 ・自システムに認証機能を設ける場合、二要素認証機能を具備する。 ・自システムに認証機能を設けず、外部の認証基盤を用いる場合、二要素認証に対応しているサービスを採用する（電子証明書やICカード、生体認証などの複数の認証方式により識別する）。 ○パスワード認証とする場合、以下に掲げる対策を講じる。 ・パスワード入力が不成功であった場合の対策 ・パスワード再入力の失敗が一定回数を超えた場合の対策	○		
E.5.2.1	セキュリティ	アクセス・利用制限	利用制限	認証された主体（利用者や機器など）に対して、資産の利用等を、ソフトウェアやハードウェアにより制限するか確認するための項目。 例）　ドアや保管庫の施錠、USBやCD-RWやキーボードなどの入出力デバイスの制限、コマンド実行制限など。	システム上の対策における操作制限度	1	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可	以下の３つの観点でアクセスが制御できる。 ・クラウド環境のアクセス制御 　最小権限と権限分離を目的に、特権を有する管理者による不正を防止するため、管理者権限を制御すること。 ・医療機関毎のアクセス制御 　ある医療機関の患者データが、他の医療機関から参照できないよう制御すること。 ・利用者のアクセス制御 　認証情報が悪意のある第三者等によって窃取された際の被害を最小化し、内部からの不正操作や誤操作を防止するため、利用者に必要最小限の権限を付与する仕組みを設けること。 <具体的な対応例> クラウド環境のアクセス制御（最小権限と権限分離）：管理者権限を持つアカウント数は必要最小限に絞り、職務に応じてアカウントを分離する(システム設定管理者と監査ログ管理者を分離 等)、管理者権限の利用は申請に応じて一時的に権限が付与される仕組みとする 等 医療機関毎のアクセス制御：同一のデータベースにプールされたデータをスキーマレベルやテーブルレベルで分離させる 等 利用者のアクセス制御：職種、所属、役職といった属性に基づき、業務に必要な最小限の範囲において権限を付与する 等	○		○
E.5.3.1	セキュリティ	アクセス・利用制限	管理方法	認証に必要な情報（例えば、 ID/パスワード、指紋、虹彩、静脈など、主体を一意に特定する情報）の追加、更新、削除等のルール策定を実施するかを確認するための項目。	管理ルールの策定	1	実施する	クラウド環境へアクセスするアカウントについては、定期的にアカウントの棚卸しを行い、不要となったアカウントの削除を行う。 ※医療機関・利用者のアカウントについては、医療機関の責務で定期的にアカウントの棚卸しを行い、不要となったアカウントの削除を行うことを想定。	○		
E.6.1.1	セキュリティ	データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。	伝送データの暗号化の有無	2	重要情報を暗号化	クライアント端末とクラウド上の電子カルテ間の通信はHTTPS通信（TLS1.3）を用いて暗号化する。 ※新規構築を行わないシステムに限ってTLS1.2を利用する場合は、IPA TLS暗号設定ガイドラインの高セキュリティ型チェックリストに合致したプロトコルスイートを利用する。	○		
E.6.1.2	セキュリティ	データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。	蓄積データの暗号化の有無	2	重要情報を暗号化	クラウド上に保管されているデータ（データベース、バックアップ等）の暗号化を実施する。 暗号化の実施においては、電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)及び暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準等を参照し、適切な暗号化手段を講じる。			○
E.6.1.3	セキュリティ	データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。	鍵管理	2	耐タンパデバイスによる鍵管理	暗号鍵に使用する鍵はFIPS140-2 レベル１相当以上を利用する。 ※ガバメントクラウドで利用できるサービス(AWS・GoogleCloud・Azure・OCI)に関してはGCASガイドに記載があるため、必要に応じた参照を推奨する。			○
E.7.1.1	セキュリティ	不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目。 なお、どのようなログを取得する必要があるかは、実現するシステムやサービスに応じて決定する必要がある。 また、ログを取得する場合には、不正監視対象と併せて、取得したログのうち、確認する範囲を定める必要がある。	ログの取得	1	実施する	「医療情報システムの安全管理に関するガイドライン（システム運用編）」17. 証跡のレビュー・システム監査において遵守事項として規定するログ（医療情報に関するアクセスを記録したログ(操作ログ等)）を取得する。 対象とするログは、クラウドベンダー等の提供するベストプラクティスに従って定義し、また当該定義は定期的に見直す。 ※ログ保管期間は性能・拡張性の「保管期間」の項を参照。	○		

IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧

（１）考え方

非機能要件における標準として独立行政法人情報処理推進機構（IPA）が示している「非機能要求グレード」を基に、（２）に掲げる表のとおり、電子カルテが遵守すべき非機能要件を策定した。
なお、策定に当たっては、以下に該当する項目を除外した。
・本標準仕様の他の記載や、本標準仕様において引用している他のガイドライン等と内容が重複する項目
・オンプレミス型のシステムであることが前提となっている項目
・クラウドサービス事業者の責任範囲となる項目
・ベンダーに対し、一律に一定の水準を求めることが必ずしも適切でない項目

（２）遵守事項一覧

遵守事項（必須要件）								要求レベルに対する具体的な考え方及び対応の例	（参考）要求レベルを満たした場合、併せて該当部分が準拠となるガイドライン		
						要求レベル			医療情報システムの安全管理に関するガイドライン	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	デジタル庁GCASガイド
項番	大項目	中項目	小項目	小項目説明	メトリクス	選択レベル	詳細				
E.8.1.1	セキュリティ	ネットワーク対策	ネットワーク制御	不正な通信を遮断するための制御を実施するかを確認するための項目。	通信制御	1	有り	正規な通信以外を遮断するための手段を講じる。 ＜具体的な対応例＞ ・ポート80/443のみオープンとする ・外部からシステム内部への通信は必要なポートのみAllowにする ・ホワイトリスト（アクセスリスト）の利用	○		
E.8.2.1	セキュリティ	ネットワーク対策	不正検知	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知する範囲を確認するための項目。	不正通信の検知範囲	1	重要度が高い資産を扱う範囲、あるいは、外接部分	不正通信の検知範囲は、外接部分と重要度の高い情報を扱う範囲とする。 ＜具体的な対応例＞ ・VPC Flow Logsの取得、確認 ・WAF / ALB / NLB / CloudFront のアクセスログの取得、確認	○		
E.8.3.1	セキュリティ	ネットワーク対策	サービス停止攻撃の回避	ネットワークへの攻撃による輻輳についての対策を実施するかを確認するための項目。	ネットワークの輻輳対策	1	有り	外接部分へのDoS/DDoS攻撃等のサービス停止攻撃に対応する。 ＜具体的な対応例＞ ・WAFの導入			○
E.9.1.1	セキュリティ	マルウェア対策	マルウェア対策	マルウェア（ウィルス、ワーム、ボット等）の感染を防止する、マルウェア対策の実施範囲やチェックタイミングを確認するための項目。 対策を実施する場合には、ウィルス定義ファイルの更新方法やタイミングについても検討し、常に最新の状態となるようにする必要がある。	マルウェア対策実施範囲	2	システム全体	クラウド提供事業者が提供する、マルウェア対策を行うサービスを利用する。（特に、リアルタイムスキャンが実施可能な製品を優先的に採用する。） 上記のサービスの利用が困難である場合は、IaaSのようなOSレイヤーから利用可能なサービス（クラウド利用者がマルウェア対策の実施責任を負うようなサービス）により、ウイルス対策ソリューションの導入及び最新のウイルス定義ファイルを用いたスキャンを定期的に実施する。	○		○
E.10.1.1	セキュリティ	Web対策	Web実装対策	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。	セキュアコーディング、Webサーバの設定等による対策の強化	1	対策の強化	アプリケーション開発時の品質を管理するため、必要な管理手順や措置を講じる。 ＜具体的な対応例＞ 管理手順や措置の例: ・アプリケーションのセキュリティを確保するため、セキュアコーディングを実施するためのコーディング規約を策定し、担当者による品質のばらつきを抑制する ・コーディングチェックについてはツールや自動化機能を利用し、品質を担保する	○		
E.10.1.2	セキュリティ	Web対策	Web実装対策	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。	WAFの導入の有無	1	有り	アプリケーションレイヤーにおける不正な通信の検知や遮断、監視を実現するため、WAFもしくは同等の防御手段を導入する。 また、導入にあたっては、上記手段が正常に動作するような運用作業を定め、実行する。 ＜具体的な対応例＞ WAFを利用する場合の運用作業例：シグネチャの更新、ルールの管理、監視体制の確立 等	○		○
E.11.1.1	セキュリティ	セキュリティインシデント対応/	セキュリティインシデント対応/復旧	セキュリティインシデントが発生した時に、早期発見し、被害の最小化、復旧の支援等をするための体制について確認する項目。	セキュリティインシデントの対応体制	1	有り	インシデントの早期発見、発生時の被害の拡大防止などを目的とした、いわゆるPSIRTに相当する組織・チームを組成する。		○	

第２章　別紙Ａ
政府情報システムにおける
脆弱性診断導入ガイドラインに係る
遵守事項一覧

令和８（2026）年 XX 月 XX 日

厚生労働省医政局

厚生労働省保険局

デジタル庁国民向けサービスグループ

改訂履歴

版数	改訂年月日	該当箇所	内容
X.X	令和８年 XX 月 XX 日	初版	初版作成

（別紙Ａ）政府情報システムにおける脆弱性診断導入ガイドラインに係る遵守事項一覧

項番	大分類	中分類	小分類	メトリクス	政府情報システムにおける脆弱性診断導入ガイドライン（「遵守」類型に該当する項目（必須要件））		具体的な対応例
					章	文言	
1	セキュリティ	セキュリティ診断	セキュリティ診断	ネットワーク診断実施の有無	3.2 1) ア 3.3 2)	(1)追加や構成の変更が生じた全ての外部公開 IP アドレス（グローバル IP アドレス）を診断の対象とする（必須） (2)診断対象は本番環境とする。システム構成が本番環境と同等である場合に限り、検証環境等での診断を可能とする（必須） プラットフォーム診断に固有の要件を以下に示す。 (1)表 2 - 1 に示す全ての脆弱性種別（以下、(1-1)～(1-4)）を診断対象とすること（必須） (1-1) 不要ポートの開放 (1-2) 脆弱なソフトウェアの利用 (1-3) 設定の不備 (1-4) プロトコル固有の脆弱性 (2)上記(1-1)では、TCP、UDP に対してオープンポートの確認と稼働しているサービスの推定を行うこと。TCP の確認は1～65535 番ポートの全てを対象とすること。UDP の確認には多くの時間を要することから、利用するツールが確認を推奨するポート（一般的に利用頻度の高いポート）の上位 100位相当を確認対象に含めること（必須） (3)上記(1-2)(1-3)(1-4)に関する診断は、表 4 - 1 に示す脆弱性種別を全て網羅すること（必須） (4)ツールによる診断には、最新の攻撃手法を反映した実績ある商用ツールを活用すること。フリーツールや自社製ツールのみによる診断は行わないこと（必須）	サービス仕様適合開示書にて定めている責任範囲内について、「政府情報システムにおける脆弱性診断導入ガイドライン」を参考に、次に掲げる要件を満たす脆弱性診断を実施する。 （１）全ての外部公開IPアドレス（グローバルIPアドレス）を診断の対象とする。 （２）診断対象は本番環境とする（システム構成が本番環境と同等である場合に限り、検証環境等での診断を可能とする）。 （３）次に掲げる全ての脆弱性種別を診断対象に含める。 ①不要ポートの開放 ②脆弱なソフトウェアの利用 ③設定の不備 ④プロトコル固有の脆弱性 （４）（３）①について、TCP/UDPにおけるオープンポートの確認と稼働しているサービスの推定を行い、以下に掲げるものを診断対象に含める。 ・TCP：1～65535番ポートの全て ・UDP：利用するツールが確認を推奨するポート（一般的に利用頻度の高いポート）の上位 100位相当 （５）（３）①～④に関する診断は、以下に掲げる脆弱性種別の全てを網羅する。 ・脆弱なソフトウェアの利用 ・不要なポート、サービス、アカウントの存在 ・公開ディレクトリ、ストレージへの非公開情報の保存 ・DNSの設定不備 ・暗号化されていない、または脆弱な暗号による通信 ・サーバ証明書の不備 ・サーバソフトウェアの設定不備 （６）（ツールによる診断の場合）最新の攻撃手法を反映した実績ある商用ツールを用いる（フリーツールや自社製ツールのみによる診断は行わない）。
2	セキュリティ	セキュリティ診断	セキュリティ診断	Web診断実施の有無	3.2 1) イ 3.3 3)	(1)新規追加や変更の生じた全ての外部公開インタフェース（動的画面や API等）を診断の対象とする。外部公開とは、ネットワーク層での送信元 IP アドレス制限やクライアント証明書等によるアクセス制限等が施されておらず、インターネットから HTTP（WebSocket を含む）による何らかの通信が可能であるものを示す（必須） … (5)診断対象は本番環境を前提とする。検証環境等での診断を行う場合は、全ての外部公開インタフェースが本番と同等に診断できるように、診断用のアカウント設定やデータの投入、外部システム連携等の準備を行うものとする（必須） (1)表 2 - 2 に示す全ての脆弱性種別（以下、(1-1)～(1-5)）を診断対象とすること（必須） (1-1) 固有のビジネスロジックに依存するもの (1-2) 一般的な仕様上の不具合 (1-3) 実装のメカニズムに対する高度な理解が要求されるもの (1-4) 一般的な実装の不備 (1-5) 利用する Web アプリミドルウェア固有の脆弱性 (2)上記(1-1)～(1-3)の診断は全て人手で行うこと。ツールの誤検出の除去ではなく、診断そのものを人手で行うものとする（必須） (3)上記(1-2)(1-4)の診断は以下の基準に準ずること。具体的には、表 4 - 2 に示す脆弱性種別を診断対象として網羅すること。他の基準を用いる場合は、表 4 - 2 に対する充足性を説明すること（必須） (3-1) NISC「政府機関等の対策基準策定のためのガイドライン（令和 5 年度版）」 (3-2) IPA「安全なウェブサイトの作り方 改訂第 7 版」 (3-3) 脆弱性診断士スキルマッププロジェクト「Web アプリケーション脆弱性診断ガイドライン 第 1.2 版」 (4)上記(1-1)～(1-4)の診断は、(3)の基準に加え、熟練者の経験に基づく手動の診断を行うこと（推奨） (5)上記(1-4)(1-5)においてツールを用いる場合は、サイトを手動巡回すること（必須） (6)機能の確認に十分な権限を有するアカウントを用いて診断を行うこと（必須）	「政府情報システムにおける脆弱性診断導入ガイドライン」を参考に、Webアプリの仕様に起因する脆弱性について脆弱性診断を実施し、次に掲げる脆弱性を突く擬似的な攻撃のリクエストを行うことにより脆弱性への対策の有無を確認する。当該診断は、全て手動により実施する。 （１）固有のビジネスロジックに依存するもの ・ID 連携の不備により他のユーザになりすましができる。 （２）一般的な仕様上の不具合 ・他人のデータを読み書きできる。 ・管理者権限の機能を誰でも利用できる。 ・パスワードリセット機能の悪用 ・認証の回避
3	セキュリティ	セキュリティ診断	セキュリティ診断	DB診断実施の有無	2.2 1) 表2-1 3.3 2)	ポートスキャンにより通信可能なポートを確認する。結果として、外部からの接続を意図していないオープンポートや、第三者に仕掛けられたバックドア等の不審なサービスが検出される。 TCP の確認は 1～65535 番ポートの全てを対象とすること。UDP の確認には多くの時間を要することから、利用するツールが確認を推奨するポート（一般的に利用頻度の高いポート）の上位 100位相当を確認対象に含めること	「政府情報システムにおける脆弱性診断導入ガイドライン」を参考に、不要ポートの開放について脆弱性診断を実施する。 具体的には、ポートスキャンにより、外部からの接続を意図していないオープンポートや、第三者に仕掛けられたバックドア等の不審なサービスの有無を確認する。 ※TCP の確認は 1～65535 番ポートの全てを対象とする。UDP の確認には多くの時間を要することから、利用するツールが確認を推奨するポート（一般的に利用頻度の高いポート）の上位 100位相当を確認対象に含める。

第２章別紙Ｂ
IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧

令和８（2026）年 XX 月 XX 日

厚生労働省医政局

厚生労働省保険局

デジタル庁国民向けサービスグループ

改訂履歴

版数	改訂年月日	該当箇所	内容
X.X	令和８年 XX 月 XX 日	初版	初版作成

IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧

（１）考え方

非機能要件における標準として独立行政法人情報処理推進機構（IPA）が示している「非機能要求グレード」を基に、（２）に掲げる表のとおり、レセコンが遵守すべき非機能要件を策定した。
なお、策定に当たっては、以下に該当する項目を除外した。
・本標準仕様の他の記載や、本標準仕様において引用している他のガイドライン等と内容が重複する項目
・オンプレミス型のシステムであることが前提となっている項目
・クラウドサービス事業者の責任範囲となる項目
・ベンダーに対し、一律に一定の水準を求めることが必ずしも適切でない項目

（２）遵守事項一覧

遵守事項（必須要件）								要求レベルに対する具体的な考え方及び対応の例	（参考）要求レベルを満たした場合、併せて該当部分が準拠となるガイドライン		
						要求レベル					
項番	大項目	中項目	小項目	小項目説明	メトリクス	選択レベル	詳細		医療情報システムの安全管理に関するガイドライン	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	デジタル庁GCASガイド
A.1.1.1	可用性	継続性	運用スケジュール	システムの稼働時間や停止運用に関する情報。	運用時間（通常）	5	24時間無停止	24時間 365日の運用とする。 ただし、次に例示するような、自責によらない事象により停止する時間を除く。 ・接続回線の計画停止時間 ・大規模災害等の天災地変に起因する停止時間 ・連携するサービス、クラウドサービス又はスマートフォン端末に係る通信キャリアの障害・計画停止・緊急メンテナンス等に起因する停止時間 ・自システムのメンテナンスによる計画停止時間(リリースによる停止も含む。) ・医療機関自体の停電 ・医療機関内にある機器の故障 上記を満たせない場合は、設定する運用時間を示した上で、運用時間を定めるに当たっての考え方(対象業務の特徴・必要性等)を示す。			
A.1.2.1	可用性	継続性	業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件。	対象業務範囲	2	内部向け全業務	サービス仕様適合開示書にて規定する責任範囲内において、診療業務の継続を目的に、レセコンに登録されている全データの閲覧が可能な状態を継続できる。 また、上記が達成できない場合は、継続性を確保する対象を定義した上で、当該対象を定めるに当たっての考え方(対象業務の特徴、必要性等)を示す。 ※なお、インターネットへの接続性については、インターネット接続を提供する事業者及びそのバックアップ回線を提供する事業者の責務となることが考えられる。		○	
A.1.3.1	可用性	継続性	目標復旧水準（業務停止時）	業務停止を伴う障害が発生した際、何をどこまで、どれ位で復旧させるかの目標。	RPO（目標復旧地点）	3	障害発生時点（日次バックアップ+アーカイブからの復旧）	目標復旧地点は、障害発生時点（日次バックアップ＋アーカイブからの復旧などを想定）とする。 なお、障害発生時点とは、障害が発生する直前のトランザクションなどの処理が完了している時点のことをいう。	○		
B.1.3.1	性能・拡張性	業務処理量	保管期間	システムが参照するデータのうち、OSやミドルウェアのログなどのシステム基盤が利用するデータに対する保管が必要な期間。 必要に応じて、データの種別毎に定める。 保管対象のデータを選択する際には、対象範囲についても決めておく。	保管期間	3	3年	医療情報に関するアクセスを記録したログ（操作ログ等）を対象に直近３年以上保管する。 ※該当ログ以外の保管期間に関しては、任意とする。 ※対象となるログは以下とする。 ・システム利用者がシステム利用時に医療情報へアクセス又は操作(参照・更新 等)した際の証跡となるもの ・運用保守担当が運用保守時に医療情報へアクセス又は操作(参照・更新 等)した際の証跡となるもの	○	○	
C.1.2.3	運用・保守性	通常運用	バックアップ	システムが利用するデータのバックアップに関する項目。	バックアップ利用範囲	3	データの長期保存（アーカイブ）	データ回復、データの長期保存に対応する。（以下詳細） ・データ回復：障害時にバックアップからのデータ回復が必要となった場合、その手順が明文化されていること。もしくは、自動化されていること。 ・データの長期保存：保険医療機関及び保険医療養担当規則に従い、以下の医療関係文書は定められた期間の長期保存に対応すること。 ・療養の給付の担当に関する帳簿及び書類その他の記録：その完結の日から3年	○		
C.1.4.1	運用・保守性	通常運用	時刻同期	システムを構成する機器の時刻同期に関する項目。	時刻同期設定の範囲	4	システム全体を外部の標準時間と同期する	システム全体で標準時間との同期を行う。 ※アクセスログ等の調査やセキュリティ監視において支障を来さないため	○		

IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧

（1）考え方

非機能要件における標準として独立行政法人情報処理推進機構（IPA）が示している「非機能要求グレード」を基に、（2）に掲げる表のとおり、レセコンが遵守すべき非機能要件を策定した。
なお、策定に当たっては、以下に該当する項目を除外した。
・本標準仕様の他の記載や、本標準仕様において引用している他のガイドライン等と内容が重複する項目
・オンプレミス型のシステムであることが前提となっている項目
・クラウドサービス事業者の責任範囲となる項目
・ベンダーに対し、一律に一定の水準を求めることが必ずしも適切でない項目

（2）遵守事項一覧

遵守事項（必須要件）								要求レベルに対する具体的な考え方及び対応の例	（参考）要求レベルを満たした場合、併せて該当部分が準拠となるガイドライン		
						要求レベル			医療情報システムの安全管理に関するガイドライン	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	デジタル庁GCASガイド
項番	大項目	中項目	小項目	小項目説明	メトリクス	選択レベル	詳細				
E.4.3.2	セキュリティ	セキュリティリスク管理	セキュリティパッチ適用	対象システムの脆弱性等に対応するためのセキュリティパッチ適用に関する適用範囲、方針および適用のタイミングを確認するための項目。 これらのセキュリティパッチには、ウィルス定義ファイル等を含む。 また、セキュリティパッチの適用範囲は、OS、ミドルウェア等毎に確認する必要があり、これらセキュリティパッチの適用を検討する際には、システム全体への影響を確認し、パッチ適用の可否を判断する必要がある。 なお、影響の確認等については保守契約の内容として明記されることが望ましい。	セキュリティパッチ適用方針	2	全てのセキュリティパッチを適用	システムを構成する各要素に対するセキュリティパッチの適用については、対策を実施した際の業務への影響並びに対策処理の速度、可用性及び網羅性について十分な検討を行った上で実施する。セキュリティパッチの適用に当たっては、その基準となるルールを設定する。 セキュリティパッチを適用する範囲は、サービス仕様適合開示書等にて定める責任範囲内の全てとする。（サービスを提供するサーバー及びネットワークに関連する機器のほか、サービス提供の範囲によっては端末(PC)も含む。）	○		
E.5.1.1	セキュリティ	アクセス・利用制限	認証機能	資産を利用する主体（利用者や機器等）を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目。 複数回の認証を実施することにより、抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード等を用いた認証等がある。	管理権限を持つ主体の認証	3	複数回、異なる方式による認証	○システム利用者（ユーザ）認証として二要素認証によりユーザーを識別し、システムへのアクセスを制御する。 ・自システムに認証機能を設ける場合、二要素認証機能を具備する。 ・自システムに認証機能を設けず、外部の認証基盤を用いる場合、二要素認証に対応しているサービスを採用する（電子証明書やICカード、生体認証などの複数の認証方式により識別する）。 ○パスワード認証とする場合、以下に掲げる対策を講じる。 ・パスワード入力が不成功であった場合の対策 ・パスワード再入力の失敗が一定回数を超えた場合の対策	○		
E.5.2.1	セキュリティ	アクセス・利用制限	利用制限	認証された主体（利用者や機器など）に対して、資産の利用等を、ソフトウェアやハードウェアにより制限するか確認するための項目。 例） ドアや保管庫の施錠、USBやCD-RWやキーボードなどの入出力デバイスの制限、コマンド実行制限など。	システム上の対策における操作制限度	1	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可	以下の３つの観点でアクセスが制御できる。 ・クラウド環境のアクセス制御 最小権限と権限分離を目的に、特権を有する管理者による不正を防止するため、管理者権限を制御すること。 ・医療機関毎のアクセス制御 ある医療機関の患者データが、他の医療機関から参照できないよう制御すること。 ・利用者のアクセス制御 認証情報が悪意のある第三者等によって窃取された際の被害を最小化し、内部からの不正操作や誤操作を防止するため、利用者に必要最小限の権限を付与する仕組みを設けること。 ＜具体的な対応例＞ クラウド環境のアクセス制御（最小権限と権限分離）：管理者権限を持つアカウント数は必要最小限に絞り、職務に応じてアカウントを分離する(システム設定管理者と監査ログ管理者を分離等)、管理者権限の利用は申請に応じて一時的に権限が付与される仕組みとする 等 医療機関毎のアクセス制御：同一のデータベースにプールされたデータをスキーマレベルやテーブルレベルで分離させる 等 利用者のアクセス制御：職種、所属、役職といった属性に基づき、業務に必要な最小限の範囲において権限を付与する 等	○		○
E.5.3.1	セキュリティ	アクセス・利用制限	管理方法	認証に必要な情報（例えば、 ID/パスワード、指紋、虹彩、静脈など、主体を一意に特定する情報）の追加、更新、削除等のルール策定を実施するかを確認するための項目。	管理ルールの策定	1	実施する	クラウド環境へアクセスするアカウントについては、定期的にアカウントの棚卸しを行い、不要となったアカウントの削除を行う。 ※医療機関・利用者のアカウントについては、医療機関の責務で定期的にアカウントの棚卸しを行い、不要となったアカウントの削除を行うことを想定。	○		
E.6.1.1	セキュリティ	データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。	伝送データの暗号化の有無	2	重要情報を暗号化	クライアント端末とクラウド上のレセコン間の通信はHTTPS通信（TLS1.3）を用いて暗号化する。 ※新規構築を行わないシステムに限ってTLS1.2を利用する場合は、IPA TLS暗号設定ガイドラインの高セキュリティ型チェックリストに合致したプロトコルスイートを利用する。	○		
E.6.1.2	セキュリティ	データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。	蓄積データの暗号化の有無	2	重要情報を暗号化	クラウド上に保管されているデータ（データベース、バックアップ等）の暗号化を実施する。 暗号化の実施においては、電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)及び暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準等を参照し、適切な暗号化手段を講じる。			○
E.6.1.3	セキュリティ	データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。	鍵管理	2	耐タンパデバイスによる鍵管理	暗号鍵に使用する鍵はFIPS140-2 レベル１相当以上を利用する。 ※ガバメントクラウドで利用できるサービス(AWS・GoogleCloud・Azure・OCI)に関してはGCASガイドに記載があるため、必要に応じた参照を推奨する。			○
E.7.1.1	セキュリティ	不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目。 なお、どのようなログを取得する必要があるかは、実現するシステムやサービスに応じて決定する必要がある。 また、ログを取得する場合には、不正監視対象と併せて、取得したログのうち、確認する範囲を定める必要がある。	ログの取得	1	実施する	「医療情報システムの安全管理に関するガイドライン（システム運用編）」17. 証跡のレビュー・システム監査において遵守事項として規定するログ（医療情報に関するアクセスを記録したログ(操作ログ等)）を取得する。 対象とするログは、クラウドベンダー等の提供するベストプラクティスに従って定義し、また当該定義は定期的に見直す。 ※ログ保管期間は性能・拡張性の「保管期間」の項を参照。	○		

IPA「非機能要求グレード」に基づく非機能要件に係る遵守事項一覧

（1）考え方

非機能要件における標準として独立行政法人情報処理推進機構（IPA）が示している「非機能要求グレード」を基に、（2）に掲げる表のとおり、レセコンが遵守すべき非機能要件を策定した。
なお、策定に当たっては、以下に該当する項目を除外した。
・本標準仕様の他の記載や、本標準仕様において引用している他のガイドライン等と内容が重複する項目
・オンプレミス型のシステムであることが前提となっている項目
・クラウドサービス事業者の責任範囲となる項目
・ベンダーに対し、一律に一定の水準を求めることが必ずしも適切でない項目

（2）遵守事項一覧

遵守事項（必須要件）								要求レベルに対する具体的な考え方及び対応の例	（参考）要求レベルを満たした場合、併せて該当部分が準拠となるガイドライン		
						要求レベル					
項番	大項目	中項目	小項目	小項目説明	メトリクス	選択レベル	詳細		医療情報システムの安全管理に関するガイドライン	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	デジタル庁GCASガイド
E.8.1.1	セキュリティ	ネットワーク対策	ネットワーク制御	不正な通信を遮断するための制御を実施するかを確認するための項目。	通信制御	1	有り	正規な通信以外を遮断するための手段を講じる。 ＜具体的な対応例＞ ・ポート80/443のみオープンとする ・外部からシステム内部への通信は必要なポートのみAllowにする ・ホワイトリスト（アクセスリスト）の利用	○		
E.8.2.1	セキュリティ	ネットワーク対策	不正検知	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知する範囲を確認するための項目。	不正通信の検知範囲	1	重要度が高い資産を扱う範囲、あるいは、外接部分	不正通信の検知範囲は、外接部分と重要度の高い情報を扱う範囲とする。 ＜具体的な対応例＞ ・VPC Flow Logsの取得、確認 ・WAF / ALB / NLB / CloudFront のアクセスログの取得、確認	○		
E.8.3.1	セキュリティ	ネットワーク対策	サービス停止攻撃の回避	ネットワークへの攻撃による輻輳についての対策を実施するかを確認するための項目。	ネットワークの輻輳対策	1	有り	外接部分へのDoS/DDoS攻撃等のサービス停止攻撃に対応する。 ＜具体的な対応例＞ ・WAFの導入			○
E.9.1.1	セキュリティ	マルウェア対策	マルウェア対策	マルウェア（ウィルス、ワーム、ボット等）の感染を防止する、マルウェア対策の実施範囲やチェックタイミングを確認するための項目。 対策を実施する場合には、ウィルス定義ファイルの更新方法やタイミングについても検討し、常に最新の状態となるようにする必要がある。	マルウェア対策実施範囲	2	システム全体	クラウド提供事業者が提供する、マルウェア対策を行うサービスを利用する。（特に、リアルタイムスキャンが実施可能な製品を優先的に採用する。） 上記のサービスの利用が困難である場合は、IaaSのようなOSレイヤーから利用可能なサービス（クラウド利用者がマルウェア対策の実施責任を負うようなサービス）により、ウイルス対策ソリューションの導入及び最新のウイルス定義ファイルを用いたスキャンを定期的に実施する。	○		○
E.10.1.1	セキュリティ	Web対策	Web実装対策	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。	セキュアコーディング、Webサーバの設定等による対策の強化	1	対策の強化	アプリケーション開発時の品質を管理するため、必要な管理手順や措置を講じる。 ＜具体的な対応例＞ 管理手順や措置の例: ・アプリケーションのセキュリティを確保するため、セキュアコーディングを実施するためのコーディング規約を策定し、担当者による品質のばらつきを抑制する ・コーディングチェックについてはツールや自動化機能を利用し、品質を担保する	○		
E.10.1.2	セキュリティ	Web対策	Web実装対策	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。	WAFの導入の有無	1	有り	アプリケーションレイヤーにおける不正な通信の検知や遮断、監視を実現するため、WAFもしくは同等の防御手段を導入する。 また、導入にあたっては、上記手段が正常に動作するような運用作業を定め、実行する。 ＜具体的な対応例＞ WAFを利用する場合の運用作業例：シグネチャの更新、ルールの管理、監視体制の確立 等	○		○
E.11.1.1	セキュリティ	セキュリティインシデント対応/復旧	セキュリティインシデント対応/復旧	セキュリティインシデントが発生した時に、早期発見し、被害の最小化、復旧の支援等をするための体制について確認する項目。	セキュリティインシデントの対応体制	1	有り	インシデントの早期発見、発生時の被害の拡大防止などを目的とした、いわゆるPSIRTに相当する組織・チームを組成する。		○	