

**医科診療所及び中小病院向け
電子カルテの標準仕様に係る認証制度要綱
【第1.0版】**

令和8年10月

厚生労働省政策統括官付医療情報連携担当参事官室

デジタル庁国民向けサービスグループ

改訂履歴

[illegible]

医科診療所及び中小病院向け電子カルテの標準仕様に係る認証制度要綱

第1条(目的)

本要綱は、厚生労働省が実施する医科診療所及び中小病院向け電子カルテの認証制度について、認証手続、審査基準その他の必要な事項を定めることを目的とする。

第2条(用語の定義)

本要綱において用いる用語の定義は、以下のとおりとする。

- (1) 「医科診療所及び中小病院向け電子カルテの標準仕様に係る認証制度」とは、医科診療所又は中小病院向けに開発された電子カルテ製品について、厚生労働省が定めた電子カルテの標準仕様への適合状況を客観的に評価し、当該仕様を満たす製品を認証する制度をいう。
- (2) 「電子カルテの標準仕様」とは、医療 DX の推進、医療情報の標準化及びサイバーセキュリティの強化等を目的として、厚生労働省が別表1に定める機能要件、非機能要件、アーキテクチャその他の基本的な要件をいう。
- (3) 「申請者」とは、本認証制度に基づき、医科診療所及び中小病院向け電子カルテ製品の認証を受けようとする事業者をいう。

第3条(本認証制度の目的等)

本認証制度の目的及び意義は、以下のとおりである。

(1) 本認証制度の目的

本認証制度は、電子カルテの標準仕様への適合状況を客観的に評価・認証することにより、電子カルテの標準仕様への適合を促進することで、医療 DX の推進及びサイバーセキュリティの強化を図り、医療機関において質の高い効率的な医療を提供することを目的とするものである。

(2) 本認証制度の意義

- ① 電子カルテの標準仕様に基づく要件及び評価基準が示されることにより、ベンダー及び医療機関にとってシステム整備の方向性が明確となり、標準化への取組が促進される。
- ② 標準仕様に適合した電子カルテの普及により、医療機関間や関連システムとの円滑なデータ連携が可能となり、切れ目のない医療提供及び医療の質の向上に寄与する。
- ③ クラウド化や標準 API の実装、データ互換性の確保等が進むことにより、システム更新・移行の円滑化、コストの最適化及び医療機関の負担軽減に資する。
- ④ セキュリティ要件を明確化し、その適合状況を継続的に確認することにより、サイバー攻撃による情報漏えいやシステム停止等のリスクの低減を図り、医療機関における安全かつ継続的な医療提供の確保に寄与する。

第4条(本認証制度の設置者、認証の対象及び認証の有効期間)

本認証制度の設置者、認証の対象及び認証の有効期間は、以下のとおりとする。

(1) 設置者

本認証制度は、厚生労働省が設置する。

(2) 認証の対象

本認証制度に基づく認証は、電子カルテ製品ごとに行うものとする。認証を受けた電子カルテ製品について、別表1に定める項目に係る変更がある場合は、当該製品について改めて認証を受けなければならない。

なお、認証は申請された個別の製品に対して付与されるものであり、当該認証をもって他の製品及び後継製品に認証の効力が及ぶものではない。

(3) 認証の有効期間

本認証制度に基づく認証の有効期間は、認証対象年度の4月1日又は認証を受けた日のいずれか遅い日から、当該認証対象年度の末日までとする。なお、認証は第9条に定める手続を行うことで更新することができる。

第5条(認証要件)

電子カルテ製品の認証要件については、以下のとおりとする。

- (1) 別表1に定める評価項目及び評価指標への適合状況を踏まえ、総合的に判断した結果、電子カルテ製品として認証することが適当であると厚生労働省が認めることとする。
- (2) ガバメントクラウドを利用していない電子カルテ製品の認証に際しては、第6条(2)に定める手続に従い、デジタル庁が実施するガバメントクラウド利用に関する事前相談が行われていること、また、その相談結果を踏まえて、①ガバメントクラウドを利用しないまま認証申請を続けることとした理由書及び②ガバメントクラウドを利用しないことに伴う対応計画が提出されていることを確認するものとする。
- (3) 認証後に電子カルテの標準仕様が改正された場合であっても、当該認証は有効期間内において、なおその効力を有するものとする。

第6条(申請の手続)

本認証制度の申請に関する手続は、以下のとおりとする。

(1) 申請書類の提出

申請者は、申請書に所定の内容を記載し、所定の添付書類とともに、設置者に提出する。

(2) ガバメントクラウド利用に関する事前相談の申込

前条(2)に定める事前相談の対象となる申請者は、認証申請に当たり、ガバメントクラウド利用に関する事前相談の申込を行う。事前相談の申込は、申請書への記載をもって行う。設置者が当該申請書を受理したときは、申請者による事前相談の申込があったものとみなす。

(3) 事前相談を踏まえたガバメントクラウド利用の可否の決定

事前相談の結果を踏まえ、申請者は、以下の①～③のいずれかの方針を決定する。

- ① ガバメントクラウドを利用せず、当初の認証申請を継続する
- ② ガバメントクラウド上で構築する新たな電子カルテの認証申請を将来的に行うこととするが、当初の認証申請は継続する

- ③ ガバメントクラウド上で構築する新たな電子カルテの認証申請を将来的に行うこととし、当初の認証申請は取り下げる

なお、上記②により認証申請を継続した場合であっても、その認証の対象は当初申請した電子カルテ製品に限られるものとし、その後にガバメントクラウド上で新たに構築する電子カルテ製品については、第4条(2)の規定に基づき、改めて認証申請を行わなければならないことに留意すること。

(4) 事前相談における技術的指摘の実施

デジタル庁は、事前相談の内容を踏まえて、前項①の申請者に対しては認証申請の対象であるガバメントクラウドを利用しない電子カルテに関する技術的指摘を、また、前項②の申請者に対しては将来的に構築するガバメントクラウドを利用した電子カルテに関する技術的指摘を行う。

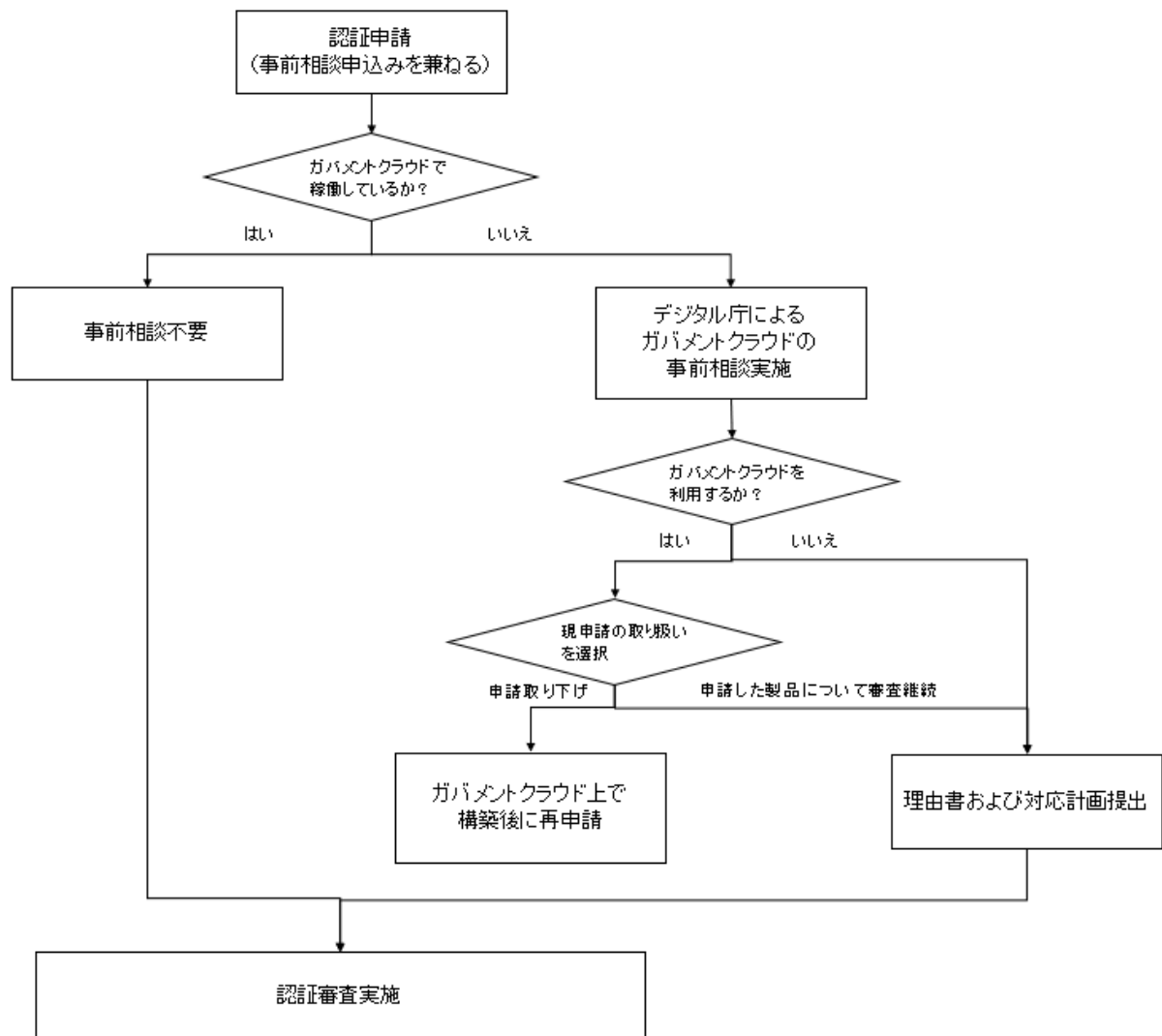
(5) 申請者による対応計画等の作成・提出

(3)①の申請者は技術的指摘への対応内容及びその実施時期を示した対応計画を作成し、また、(3)②の申請者はガバメントクラウドの利用開始時期及び技術的指摘への対応内容を示した対応計画を作成し、ガバメントクラウドを利用しないまま認証申請を続けることとした理由書を添えて、設置者に提出する。

(6) 事前相談の手続の流れの全体像

(2)～(5)を踏まえた認証申請後のガバメントクラウド利用に関する事前相談の手続の流れは、別図1のとおり。

別図1 認証申請及びガバメントクラウド利用事前相談の流れ



第7条(認証の手続)

本認証制度の設置者に関する手続は、以下のとおりとする。

- (1) 設置者は、申請者から認証申請があったときは、正当な理由がある場合を除き、これを受理するものとする。
- (2) 申請者からの認証申請を受理した設置者は、申請書に不足等がある場合には、申請者に申請内容の見直しを要求することができる。
- (3) 設置者は、認証申請に係る書類一式が提出され、必要な書類が全て整っていることを確認した上で当該申請を受理した日から起算して、原則 90 日以内に、審査結果を申請者に通知するものとする。

第8条(認証結果の公開)

認証結果の公開については、以下のとおりとする。

- (1) 設置者は、認証した電子カルテ製品に関する情報を公開するものとする。

- (2) 申請者は、認証を受けた場合、前項の公開後に認証された電子カルテ製品に関する情報を公表することができる。

第9条(認証の更新手続)

認証を受けた事業者が認証の更新を希望する場合は、認証の有効期間が満了する日の 80 日前までに、認証更新に係る書類一式を提出するものとする。

設置者は、更新申請があった場合には、次に掲げる事項について審査を行うものとする。

- (1) 別表1において「更新時に評価項目」として定める事項について、引き続き認証要件を満たしていること
- (2) 第5条(2)に基づき提出された対応計画がある場合は、当該対応計画の進捗状況及び実施結果が確認できること
- (3) 電子カルテの標準仕様が認証後又は更新後に改正されている場合にあっては、当該電子カルテ製品が改正後の標準仕様に適合していること
- (4) 認証後に発生した重大な障害、セキュリティインシデントその他認証要件への適合性に影響を及ぼす事象に対し、適切な対応が講じられていること、又は対応計画が策定され、その実施が確実に見込まれること

設置者は、上記に掲げる事項について審査を行った結果、各事項の要件を満たしていると認めるときは、認証を更新するものとする。なお、審査において、対応計画どおりに進捗していない事項があると認める場合は、当該事項に係る理由及び今後の対応内容を確認の上、事業者に対し、対応計画の見直し及び更新後の対応計画の提出を求めることができる。事業者は、その求めに応じて更新後の対応計画を提出するものとし、設置者は当該計画の妥当性を確認した上で、認証を更新するものとする。

設置者は、認証の有効期間が満了する日までに、認証更新の可否を申請者に通知するものとする。

第10条(報告徴収及び改善指示)

- (1) 設置者は、本認証制度の適正な運営を確保するため必要があると認めるときは、申請者又は認証を受けた事業者に対し、報告又は資料の提出を求めることができる。
- (2) 設置者は、認証要件への適合性の確認その他必要があると認めるときは、申請者又は認証を受けた事業者に対し、改善その他必要な措置を講ずるよう求めることができる。
- (3) 申請者又は認証を受けた事業者は、前項の求めを受けた場合には、速やかに必要な対応を行い、その結果を設置者へ報告しなければならない。

第11条(認証の取消)

設置者は、次のいずれかに該当する場合に、当該電子カルテ製品に係る認証の取消しを行うことができる。

- (1) 申請内容の虚偽、法令違反等が判明した場合

- (2) 本要綱の規定を遵守しない事業者において、第 10 条(2)の求めに従わず、必要な改善が見られない場合
- (3) 申請者から認証取下げの依頼があった場合
- (4) 重大な公序良俗違反その他の本認証制度の信用を失墜させるおそれのある行為が認められた場合

第 12 条(情報の取扱い)

本認証制度に関する情報の取扱いは、以下のとおりとする。

- (1) 厚生労働省及びデジタル庁は、本制度を通じて知り得た申請者の情報を、本制度の実施以外の目的で利用してはならない。
- (2) 厚生労働省及びデジタル庁は、取り扱う申請者の情報の漏えい、滅失、き損の防止等、情報の安全管理のために必要な措置を講じなければならない。
- (3) 厚生労働省及びデジタル庁は、法令に基づく場合を除き、あらかじめ書面により申請者の同意を得ないで、申請者の情報を第三者に提供してはならない。ただし、申請者が当該情報を公表するなど容易に知り得る場合においては、この限りでない。
- (4) 厚生労働省及びデジタル庁は、申請者からの連絡により、申請者の情報が申請者の財産管理上の利益、競争上の地位等を不当に害する恐れのある情報であると判明した場合には、その情報を原則として公表してはならない。

第 13 条(その他)

本認証制度に関するその他の運用に関する取扱いは、以下のとおりとする。

- (1) 本認証制度の運用に当たっては、電子カルテの標準仕様の改正に応じて、評価項目、評価指標等の見直し等を検討するものとする。
- (2) この要綱に定めるもののほか、本認証制度の運用上必要な事項については、設置者が定めるものとする。

第 14 条(免責事項)

本認証は、電子カルテ製品が電子カルテの標準仕様に適合していることを確認するものであり、当該製品の品質、性能、安全性、信頼性、操作性、継続性、サポート体制その他のサービス内容を厚生労働省が保証するものではない。

また、電子カルテ製品の具体的な機能、提供条件、利用料金、保守運用体制、サービスレベル、その他のサービス仕様については各事業者が定めるものであり、厚生労働省はその内容の正確性、完全性又は適切性を保証しない。

厚生労働省は、次に掲げる場合において一切の責任を負わないものとする。

- (1) 医療機関その他の利用者による電子カルテ製品の選定、導入、利用又は契約締結に起因して損害が生じた場合

- (2) 本認証を受けたことをもって、当該電子カルテ製品が特定の用途又は個別の医療機関が求める機能に適合すると誤認したことにより損害が生じた場合
- (3) 電子カルテ製品の瑕疵により、利用者が被害を被った場合
- (4) 利用者の故意又は重過失により、利用者が被害を被った場合
- (5) 電子カルテの標準仕様に係る認証要件、認証結果又は認証製品の公表に関連して、認証を受けた事業者と第三者との間に係争が生じた場合
- (6) 電子カルテの標準仕様又は認証要件の改正又は変更により影響が生じた場合
- (7) その他、本制度に係る認証の範囲を超える事項に起因する問題が発生した場合

附則(施行期日)

この要綱は、令和8年 11 月 1 日から施行する。

以上

別表1

認証制度の評価項目および評価指標

令和8(2026)年10月16日

厚生労働省政策統括官付

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
1.0	令和8年 10 月 16 日	初版	初版作成

別表 1 認証制度の評価項目および評価指標

区分		評価項目		中小病院向け電子カルテ標準仕様書（基本要件）該当箇所	医科診療所向け電子カルテ標準仕様書（基本要件）該当箇所	評価指標	認証更新時に必ず確認する評価項目 ※標準仕様、認証制度要素類その他関連文書の改定に伴い、追加・変更される場合がある。
電子カルテの標準仕様書（基本要件）への準拠	機能要件	－	オンライン資格確認等システムとの接続機能	2.1.1（2）①のNo.1（1）	2.1.1（2）①のNo.1（1）	機能要件に係る標準仕様（基本要件）のうち、オンライン資格確認等システムとの接続機能において「遵守」類型に該当する項目（必須要件）を満たしていること。	－
			電子処方箋サービスとの接続機能	2.1.1（2）①のNo.1（2）	2.1.1（2）①のNo.1（2）	機能要件に係る標準仕様（基本要件）のうち、電子処方箋管理サービスとの接続機能において「遵守」類型に該当する項目（必須要件）を満たしていること。 ただし、電子カルテと電子処方箋サービスとの間でクラウド間連携が実現した旨の公表の日から起算して6か月が経過するまでの間は、本要件は推奨項目として取り扱い、未対応であっても不適合とはしない。 経過措置を適用する場合は、認証審査時に対応予定時期及び対応計画を確認する。	－
			電子カルテ情報共有サービスとの接続機能	2.1.1（2）①のNo.1（3）	2.1.1（2）①のNo.1（3）	機能要件に係る標準仕様（基本要件）のうち、電子カルテ情報共有サービスとの接続機能において「遵守」類型に該当する項目（必須要件）を満たしていること。 ただし、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連携が実現した旨の公表の日から起算して6か月が経過するまでの間は、本要件は推奨項目として取り扱い、未対応であっても不適合とはしない。 経過措置を適用する場合は、認証審査時に対応予定時期及び対応計画を確認する。	－
			クラウド型レセプトコンピュータとの接続機能	2.1.1（2）①のNo.1（4）	2.1.1（2）①のNo.1（4）	クラウド型レセプトコンピュータとの接続機能を保持していること。又はレセコン機能を内包（一体型）していること。	－
	可用性	－	稼働率99.9%	2.1.2（2）①のNo.1	2.1.2（2）①のNo.1	以下のいずれかに該当すること。 ①直近1年間の稼働率の実績が99.9%以上であること。 ②直近1年間の稼働率の実績が99.9%未満の場合は、直近1年間の以下の情報を整理した資料を追加で提出。 「発生した障害日時」、「障害の内容」、「業務影響」、「業務に影響を与えた時間」、「直接的な原因」、「根本原因」、「再発防止策」、「再発防止策の対応状況」 原因分析および再発防止策が整理され、適切に実施されているか総合的に確認。 標準仕様Ver1.0に依る初回の認証審査に限り、稼働実績について直近3ヶ月間を対象とする経過措置との整合を図るため、本項目における「直近1年間」は「直近3ヶ月間」と読み替えるものとする。 尚、稼働開始後3ヶ月未満のため、直近3ヶ月の稼働率の実績を算出できない場合、以下の資料を提出すること。 「目標稼働率」、「稼働開始日」、「稼働開始後の実績稼働率」、「医療機関の業務に影響を与えたインシデントの内容」 <以下、標準仕様から抜粋> 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、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・削除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。このため、例えばクラウドサービスプロバイダーにおける障害によりシステムが停止した時間帯は、算出対象から除外して差し支えない。	○
			外部機関の認証	2.1.2（2）①のNo.2（1）	2.1.2（2）①のNo.2（1）	以下の条件を満たしていること。ただし、電子カルテがガバメントクラウドにおけるSaaS（公共SaaSをいう。）を利用している場合にあつては、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 ※電子カルテの標準仕様Ver1.0に基づく初回認証の申請については、経過措置として、上記ア又はイの認証の取得を認証時の遵守要件（必須要件）としない。 ただし、認証を受けた事業者は、2027年6月30日までに当該認証を取得しなければならない。 また、認証申請時に、認証取得に向けた計画及び認証取得見込み時期を提出しなければならない。	○
			ペネトレーションテスト実施	2.1.2（2）①のNo.2（2）	2.1.2（2）①のNo.2（2）	以下の条件を満たしたペネトレーションテストを実施できていること。ただし、電子カルテがガバメントクラウドにおけるSaaS（公共SaaSをいう。）を利用している場合にあつては、次に掲げる要件に適合しているものとみなすこと。 ・実施頻度：以下の条件を満たすこと 年1回以上の実施を原則とする。やむを得ない場合や、リスク評価の結果、テストの必要性が著しく低いと判断される場合は、その理由が提示できること。その場合でもリリースしてから必ず1度は実施すること。 1),2)の要因が発生した場合は、必ずリスク評価を行うこと 1) 内部環境要因による実施判断を行っていること 次の内容に変更が発生した場合は、再テストを実施すること。 再テストは、原則として変更の影響が及ぶ範囲を対象とする。 ただし、影響範囲の特定が困難な場合は、システム全体を対象とした再診断を検討する。 <更新時に追加テストを求める基準> ■外部公開の追加・変更 外部公開のドメイン／URL の追加・変更 外部公開のAPIエンドポイントの追加・変更 外部公開のグローバルIP の追加・変更 ■重要機能の追加・変更 認証・認可方式の変更 暗号化方式・鍵管理の変更 大きな機能追加・変更 ■セキュリティの変更 WAF/IPS/CDN/API Gateway等の追加・設定変更 2) 外部環境要因による実施判断を行っていること 外部で新たに重大な脆弱性が公表された場合（例：CISA KEV、JVN、クラウドサービス事業者からのセキュリティ通知等） には、当該システムへの影響有無を評価し、必要に応じて追加診断または対策を実施すること ・テスト内容：外部ペネトレーションテストを実施していること ・テスト結果を受けた対策：発見した脆弱性に対する対策状況を提示 CVSSスコアで中（Medium）以上は、原則対策すること	○
			脆弱性診断実施	2.1.2（2）①のNo.2（3）	2.1.2（2）①のNo.2（3）	以下の条件を満たした脆弱性診断を実施できていること。ただし、電子カルテがガバメントクラウドにおけるSaaS（公共SaaSをいう。）を利用している場合にあつては、次に掲げる要件に適合しているものとみなすこと。 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（2024（令和6）年1月31日）に準拠した脆弱性診断の実施、発見した脆弱性に対する対策 ・実施頻度：以下の条件を満たすこと 年1回以上の実施を原則とする。やむを得ない場合や、リスク評価の結果、テストの必要性が著しく低いと判断される場合は、その理由が提示できること。その場合でも直近3年以内の実施を求める。加えて、継続的（定期的または自動）な脆弱性スキャンを実施することを強く推奨する。 1),2)の要因が発生した場合は、必ずリスク評価を行うこと 1) 内部環境要因による実施判断を行っていること ペネトレーションテスト実施の内部環境要因と同等 2) 外部環境要因による実施判断を行っていること ペネトレーションテスト実施の外部環境要因と同等 ・テスト内容：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のプラットフォーム診断、Webアプリケーション診断の実施 ・テスト結果を受けた対策：発見した脆弱性に対する対策状況を提示 CVSSスコアで中（Medium）以上は、原則対策すること	○
			セキュリティパッチの適用	2.1.2（2）①のNo.2（4）	2.1.2（2）①のNo.2（4）	以下の条件を満たした運用が実施されていること。 ・セキュリティパッチの適用に関するルール又は手順が整備されていること ・セキュリティパッチの適用実績が提示できること ・緊急性の高いセキュリティパッチに対し、速やかに適用又はリスク評価を行う運用が定められていること	○
	データの保存／保管	－	電子カルテの三原則（見読性、真正性及び保存性）の担保	2.1.2（2）①のNo.3（1）	2.1.2（2）①のNo.3（1）	以下の観点を確認し、総合的に判断する。 （1）見読性 診療録等の電磁的記録について、必要な時に人が判読可能な状態で閲覧、出力又は表示できること。 （2）真正性 記録の作成者、作成日時及び更新履歴が確認でき、不正な改ざんを防止又は検知できること。 （3）保存性 法令等で定められた保存期間にわたり記録を適切に保存し、障害発生時においても復元可能な状態を維持できること。 上記の確認に当たっては、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）における見読性、真正性及び保存性に関する項目への対応状況を確認する。	－
			国内データ保管	2.1.2（2）①のNo.3（2）	2.1.2（2）①のNo.3（2）	以下のすべての条件を満たしていること。 ・データ※が国内に保管されていること（保存先リージョンが国内であること）。 ・データ※が海外のサーバ等に保存されないこと。 ・通信経路上において一時的に海外を経由する場合であっても、当該データが海外に保存又は継続的に保持されないこと。 ※本要件における「データ」とは、個人情報、機微情報、およびシステムセキュリティに関する情報を指す。	－
		バックアップ環境の整備	データバックアップ	2.1.2（2）①のNo.4	2.1.2（2）①のNo.4	以下の観点を確認し、総合的に判断する。 （1）バックアップ取得 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、定期的なバックアップが取得されていること。 <実装例> ・別クラウドアカウントへのバックアップ ・別リージョンへのバックアップ ・テープメディアへのバックアップ ・オフラインディスクへのバックアップ ・その他同等の対策 （2）バックアップの隔離性 バックアップデータが本番環境から物理的又は論理的に隔離されていることについて、以下の観点から対策状況を確認する。 ・本番管理者による削除制御 ・ネットワーク分離 ・イミュータブル（変更・削除不可）設定 ・その他同等の対策 （3）運用及び復旧体制 バックアップの取得及び復旧に関する運用が整備されていることについて、以下の観点から対策状況を確認する。 ・定期的なバックアップ取得 ・復旧テストの実施 ・復旧手順書の整備 ・運用記録の保管	－

区分		評価項目		中小病院向け電子カルテ標準仕様書（基本要件）該当箇所	医科診療所向け電子カルテ標準仕様書（基本要件）該当箇所	評価指標	認証更新時に必ず確認する評価項目 ※標準仕様、認証制度要綱その他関連文書の改定に伴い、追加・変更される場合がある。	
		大分類	中分類（小分類）					
		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版への準拠	2.1.2（2）①のNo.5（1）	2.1.2（2）①のNo.5（1）	・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版に準拠していること。	－	
			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版への準拠	2.1.2（2）①のNo.5（2）	2.1.2（2）①のNo.5（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版に準拠していること。	－	
		非機能要求グレード	第1章別紙2 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への準拠	2.1.2（2）①のNo.5（3）	2.1.2（2）①のNo.5（3）	・第1章別紙2 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準拠していること。 求める具体的なレベルについては、「要求レベルに対する具体的な考え方及び対応の例」を列を参考にすること。	－	
	アーキテクチャ	クラウドネイティブ・アーキテクチャ	パブリッククラウド環境の利用	2.1.3（2）①のNo.1（1）	2.1.3（2）①のNo.1（1）	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見込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	－	
			SaaS型サービス	2.1.3（2）①のNo.1（2）	2.1.3（2）①のNo.1（2）	以下のすべての条件を満たしていること。 ・利用者（医療機関及び医療従事者）とサービス提供者との責任範囲が明確に区分されていること。 ・利用者の責任範囲は「データ」の管理に限定されるものとし、「アプリケーション」「OS」「インフラ（ハードウェア、ネットワーク、施設等）」に係る管理・運用については、サービス提供者の責任範囲とすること。 ・OS、Webブラウザその他関連ソフトウェアの更新時に、必要に応じて互換性検証を実施する運用が定められていること ・互換性検証の結果、対応が必要な場合は、互換性維持のための措置を講じる運用が定められていること なお、クラウドサービス事業者又はマネージドサービス事業者の責任範囲においてセキュリティパッチが適用される場合は、当該運用内容が確認できる資料をもって適用実績に代えることができる。	－	
			マルチテナント方式	2.1.3（2）①のNo.1（3）	2.1.3（2）①のNo.1（3）	以下のすべての条件を満たしていること。 ・すべての医療機関に対して単一データベース、単一バージョンにより提供されており、個別医療機関の要望に対応するための個別改修を行っていないこと ・すべての医療機関に提供するシステムのバージョンを一斉にアップデート、リリースの自動化ができること（導入医療機関数の増加が起因で、システムのバージョンのアップデート作業が増えないこと） ・すべての医療機関を横断した単一のインフラ運用・監視の仕組みが存在しており、医療機関を横断して一括で運用ができること	－	
			ソースコード共通化	2.1.3（2）①のNo.1（4）	2.1.3（2）①のNo.1（4）	以下の条件を満たしていること。 ・電子カルテを構成するアプリケーションのソースコードが、全てのテナントに対して共通であること。 ・個別医療機関ごとに異なるソースコードを適用する運用を行っていないこと。 ・アプリケーションのテスト又は更新に伴う一時的な場合を除き、本書環境において複数バージョンを恒常的に併存させていないこと。 ・診療科ごと等にソースコードを区分している場合は、管理体系及び対象診療科が明確に整理されていること。	○	
			カスタマイズ禁止	2.1.3（2）①のNo.1（5）	2.1.3（2）①のNo.1（5）	以下の条件を満たしていること。 ・個別医療機関ごとの要望に応じたソースコードの個別改修を前提としないこと。 ・医療機関ごとの差異については、設定変更、パラメータ変更又はメタデータの変更により対応可能な仕組みとなっていること。 ・医療機関の要望により追加した機能については、オプション機能として整理され、必要に応じて全ての医療機関が利用可能な仕組みとなっていること。 ・個別医療機関向けの専用プログラムの生成又は専用機能の提供を恒常的に行っていないこと。	○	
			モダナイゼーション	2.1.3（2）①のNo.2	2.1.3（2）①のNo.2	・ガバメントクラウドにおけるモダン化の定義の「1.APIベースのシステム構成」に記載。 https://guide.gcas.cloud.go.jp/modernization-guide/modernization-definition	－	
		情報提供・公開		ステートレスなアーキテクチャ	2.1.3（2）①のNo.2	2.1.3（2）①のNo.2	・ガバメントクラウドにおけるモダン化の定義の「2.ステートレスなアーキテクチャ」に記載。 https://guide.gcas.cloud.go.jp/modernization-guide/modernization-definition	－
				マネージドサービスの活用	2.1.3（2）①のNo.2	2.1.3（2）①のNo.2	・ガバメントクラウドにおけるモダン化の定義の「3.マネージドサービスの活用」に記載。 （全機能にマネージドサービスの適用が厳しい場合であっても、ガバメントクラウドで定める移行パターンの「Replatform（R1）」※は満たしていること。） https://guide.gcas.cloud.go.jp/modernization-guide/modernization-definition ※ https://guide.gcas.cloud.go.jp/general/basic-concept/basic-concept-concept-for-using-the-gov-cloud	－
				運用のコード化、自動化	2.1.3（2）①のNo.2	2.1.3（2）①のNo.2	・ガバメントクラウドにおけるモダン化の定義の「4.運用のコード化、自動化」に記載。 https://guide.gcas.cloud.go.jp/modernization-guide/modernization-definition	－
				価格公開	2.3（2）①のNo.1（1）	2.3（2）①のNo.1（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。 なお、ここのいう価格とは小売価格のことであり、実販価格ではない。	－
				医療情報セキュリティ開示書（SDS Ver5.0）の開示	2.3（2）①のNo.1（2）	2.3（2）①のNo.1（2）	・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、開示可能であること。	－
				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）の開示	2.3（2）①のNo.1（3）	2.3（2）①のNo.1（3）	・電子カルテに関して記入済の医療機関・薬局におけるサイバーセキュリティ対策チェックリストについて、開示可能であること。	○
				サービス仕様適合開示書及びサービス仕様書の開示	2.3（2）①のNo.1（4）	2.3（2）①のNo.1（4）	・サービス仕様適合開示書及びサービス仕様書について、開示可能であること。	－
				第1章別紙様式1 電子カルテ提示対象機能一覧の開示	2.3（2）①のNo.1（5）	該当なし	・「第1章別紙様式1 電子カルテ提示対象機能一覧」に必要事項を記入の上、開示可能であること。	○
				第1章別紙3 IPA「非機能要求グレード」に基づく非機能要件に係る要開示項目一覧の開示	2.3（2）①のNo.1（6）	該当なし	・「第1章別紙3 IPA「非機能要求グレード」に基づく非機能要件に係る要開示項目一覧」に必要事項を記入の上、開示可能であること。	－
				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	2.3（2）①のNo.1（7）	2.3（2）①のNo.1（5）	・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、開示可能であること。	－
				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の開示	2.3（2）①のNo.1（8）	2.3（2）①のNo.1（6）	・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、開示可能であること。	－
				医療機関から問い合わせがあった際の一次回答時間に係る直近3か月の平均値の開示	2.3（2）①のNo.1（9）	2.3（2）①のNo.1（7）	・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に係る直近3か月の平均値について、開示可能であること。	○
デジタル庁が実施するガバメントクラウド利用に関する事前相談	事前相談	－	－	－	デジタル庁が実施するガバメントクラウド利用に関する事前相談を受けていること。 当該相談の結果、ガバメントクラウドを利用せずにシステムの構築等を行うこととした場合は、①その理由、②事前相談における技術的指摘に対する対応計画等を、厚生労働省による審査の際に提出すること。	－		
直近1年間で一定数以上の医療機関での稼働実績	－	－	－	－	認証の申請時点で、一定数以上の医療機関での稼働実績があること。なお、ガバメントクラウドを利用してシステム構築を行っている場合は、この限りではない。この場合、稼働状況の確認の観点から、性能、障害復旧、業務・運用等に関して実施した検証の結果を示す資料を提出して審査を受けること。 一定数は、以下と定義する。 ▶中小病院向け電子カルテ 認証申請日の前日時点において30施設以上で稼働しており、かつ30施設以上で稼働している状態が直近1年間継続していること。 ▶医科診療所向け電子カルテ 認証申請日の前日時点において200施設以上で稼働しており、かつ200施設以上で稼働している状態が直近1年間継続していること。 認証申請者は、申請時に稼働実績を申告すること。さらに、厚生労働省から求められた場合には、当該稼働実績を確認できる資料を提出できるよう、必要な記録及び証憑を保管しておくこと。 なお、標準仕様Ver.1.0に係る初回の認証審査について、「認証申請日の前日時点において・・・で稼働している状態が直近1年間継続していること」とあるのは、「認証申請日の前日時点において・・・で 稼働している状態が直近3か月間継続していること 」と読み替えるものとする。	○		