令和３年９月１日制定

国立研究開発法人国立がん研究センター
がんゲノム情報管理センター
「C-CAT 利活用検索ポータル」
サービス仕様適合開示書

国立がん研究センター

がんゲノム情報管理センター

目次

1　サービス仕様適合開示書の目的

1.1　サービス仕様適合開示書の目的

国立研究開発法人国立がん研究センターがんゲノム情報管理センター「C-CAT 利活用検索ポータル」サービス仕様適合開示書（以下、本書といいます）は、情報システム・サービスの提供事業者であるがんゲノム情報管理センター（以下、C-CAT といいます）が、サービスに関する『情報システム・サービスの提供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』(以下、「クラウドサービス医療ガイドライン」といいます)への適合状況や医療ガイドラインに基づいて実施している内容を、サービスご利用者に示すことを目的として作成したものです。

また、サービスご利用者側との責任分界や、役割の範囲、免責事項等を表しており、これにより提供するサービスの品質や内容を示します。

これに加え、個人情報の安全管理を確実にする観点から、本書には、必要に応じてサービスのご利用者に実施を求めることが必要となる事項についても記載しています。

本書には、以下の内容を含んでいます。

① クラウドサービス医療情報ガイドラインにおいて、サービス利用者と、本書を通じて合意すべきとされている事項

② クラウドサービス医療ガイドラインにおける要求事項で、サービス提供に際して実施している事項、あるいは具体的な対応内容

③ 本書に基づくサービス提供に際して、サービスご利用者側に求める対応事項、責任分界等

1.2　個人情報保護指針・プライバシーポリシー

本サービスでは、国立研究開発法人国立がん研究センター（以下、NCC といいます）で定めた下表にある個人情報保護指針（個人情報の保護に関する規程）・プライバシーポリシーを参照すると共に遵守します。

規程等の名称	概要
国立がん研究センター プライバシーポリシー	ホームページによる公開情報 https://www.ncc.go.jp/jp/privacypolicy.html

1.3 本サービスの主体

情報システム・サービスの提供事業者	国立研究開発法人国立がん研究センター(NCC) がんゲノム情報管理センター(C-CAT)
情報システムに関する委託先 ※1	株式会社 日立製作所
保守会社 ※2	株式会社 日立製作所
ヘルプデスク	がんゲノム情報管理センター(C-CAT) ヘルプデスク
インフラストラクチャーの外部委託先	Amazon Web Services, Inc.(以下、AWS といいます)

※1:情報システムに関する委託先

情報システム・サービスの提供事業者(C-CAT)が、医療機関等にサービスを提供するケースにおいて、情報システムに関する委託先と称す。

【内容】

- IT インフラストラクチャーの設計・構築
- アプリケーションの開発
- IT インフラストラクチャー及びアプリケーションの監視・運用

※2:保守会社

アプリケーションの改造と保守を担う会社。

1.4 用語の定義

情報システム・サービスの提供事業者	国立研究開発法人国立がん研究センター(NCC) がんゲノム情報管理センター(C-CAT)
本サービスの利用者	●研究機関等 ・基礎研究 ●医療機関(がんゲノム医療中核拠点病院・拠点病院・連携病院等) ・臨床研究 ●医薬品製造業等 ・創薬・治療方法等開発
契約者	本書に同意の上、本サービスの利用を申請した本サービスの利用者
利用契約	本書に同意し、医療機関等が本サービスの利用申請をし、NCC が定める契約に係る手続き後、契約成立とする
ヘルプデスク	本システム利用者からの参加・変更等の受付及び本システムへの設定業務、本システムを構成する各機器、設備、ソフトウェア等に係る連絡調整業務、本システムに関する相談、苦情の受付と対応等を行う機関

1.5 ガイドライン及び標準規格等参照文書

本システムは、以下のガイドラインに準拠又は参照します。

ガイドラインの対象	行政機関	ガイドラインの対象	ガイドラインの掲載元
医療情報システムの安全管理に関するガイドライン　第5.1 版 【令和 3 年 1 月】	厚生労働省	医療機関等個人情報の利用者 （病院、一般診療所、歯科診療所、助産所、薬局、訪問介護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等）	https://www.mhlw.go.jp/stf/shingi/0000516275.html
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 【令和 2 年 8 月】	総務省・ 経済産業省	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	https://www.soumu.go.jp/main_content/000703894.pdf

1.6 対象とするシステム、設備等

① 本サービスを構成するシステムの機器、ソフトウェア等

② 本システムを設置するデータセンター

③ 本システムの情報のバックアップを行うバックアップセンター(AWS)

④ データセンターから AWS へのアクセス回線
(本システムのご利用者拠点からデータセンターへのアクセスネットワークはご利用者で準備)

1.7 本システムを利用するための環境準備

① 契約者には、本システムを利用するために必要なインターネット環境、PC 等の機器及びソフトウェア等の準備をお願いいたします。

② C-CAT から本サービスで機器、ソフトウェアの提供又は貸与が必要な場合は、別途定めるものといたします。

③ C-CAT からサービス利用者への操作マニュアル等ドキュメントに関しては、別途定めるものといたします。

2 C-CAT における組織的安全管理対策

2.1 組織的取組における基本方針（個人情報保護指針、プライバシーポリシー）

「1.2 個人情報保護指針・プライバシーポリシー」にて定めているとおりです。

規程遵守の対象は、C-CAT のすべての職員及び外部委託業者等で C-CAT の情報資産を利用する者と定めています。

2.2 組織的取組における体制

2.2.1 サービスの提供に関する組織体制

本規程の実施に係る管理運営体制は、次の責任者により構成されています。

下記に掲げた責任者の任命・解任等のルールも策定されています。

運営管理体制責任者	役職
本サービスの提供についての管理責任者	がんゲノム情報管理センター長
本サービスに関する情報システムについての管理責任者	ネットワーク・システム管理室長
本サービスの運用管理責任者	情報利活用戦略室長
本サービスのヘルプデスク責任者	情報利活用戦略室長
本サービスに関する情報システムについてのリモート保守責任者	株式会社 日立製作所

2.2.2 組織体制における役割

各責任者の実施内容は下表の通りです。

サービスの提供についての管理責任者	**【通常運用における責任】** 本サービスの利用者等に対して個人情報の適切な保護のための適切な情報管理の責任を負う。 **■ 説明責任** ・提供するクラウドサービスの仕様、運用、及びセキュリティ対策に関する事項の文書化 ・提供するクラウドサービスの仕様及び品質に関する説明及び必要な情報提供 ・提供するクラウドサービスに関する監査等の情報の提供 **■ 管理責任** ・個人情報保護を含むクラウドサービスの提供体制の明確化 ・クラウドサービスの提供に関する運用状況等の定期的な報告 ・医療機関等の管理者からの問い合わせ等に対して、一元的に対応できる体制の構築 **■ 定期的に見直し必要に応じて改善を行う責任** ・サービス及びセキュリティの向上についての定期的なレビュー結果の報告等 **【事後責任】**

	個人情報について何らかの不都合な事態が生じた場合の責任。「個々の利用者等に対する説明責任」及び「監督機関である行政機関や社会への説明・公表」の責任を果たす。 **■ 事後責任における説明責任** ・緊急時に医療機関等の管理者に対して提供する情報の内容、役割分担等の明確化 ・クラウドサービスの提供状況に関する記録の収集及び緊急時の報告体制の構築 ・媒体及び機器の管理等に関する手順の明確化及び緊急時の報告体制の構築 ・緊急時に備えた、アクセス制御等の手順等の明確化 **■ 事後責任における善後策を講ずる責任** ・情報事故（個人情報漏洩等）等が発生した場合の原因追及に必要な情報提供の範囲、条件等の合意、及び情報提供の実施 ・善後策の提案 ・情報事故が発生した場合の損害填補責任に関する合意
情報システムについての管理責任者	サービスの提供についての管理責任者が選任する者を、情報システムについての管理責任者に充てる。 サービスの提供についての管理責任者の統制下で責務を実施する。 ① 本システムの運用が支障無く行われるよう、実施の責任を持つ ② システム管理者の職務の一部を副システム管理者に委任することは妨げない ③ システムの安全性を確保し、安全性の継続的な確保に努める ④ システムの開発者、保守作業者の登録を管理し、そのアクセス権限を管理し、不正な利用を防止する ⑤ 契約医療機関、利用者及び患者等の登録を管理し、そのアクセス権限を管理し、不正な利用を防止する ⑥ システムの障害、バグ等の発生を運用管理責任者に報告すると共に障害の解決を行う ⑦ 作業手順の整備を行い関係者の教育と訓練を行う ⑧ ヘルプデスク業務、リモート保守業務、相談・苦情受付窓口業務、教育担当業務の管理を行う ⑨ 障害の発生を防止すること及び障害発生時には、運用管理責任者に報告すると共に、問題の解決を行う ⑩ 運用管理責任者に、システムの運用状況を報告する ⑪ 本システムにかかわる保守作業者に対し、個人情報保護に関する教育を実施する
運用管理責任者	サービスの提供についての管理責任者が選任する者を、運用管理責任者に充てる。 サービスの提供についての管理責任者の統制下で責務を実施する。 ① 本システムが円滑に運用される環境を整備し、その実施を管理する責任を持つ ② 運用管理責任者の職務の一部をシステム管理者に委任することは妨げない ③ システム管理者の報告を受け、必要な措置を講じる ④ 契約書類、マニュアル等を整備し、関係者に周知し利用可能な状態に置く ⑤ 必要に応じて、利用者に対して、本システムの運用、個人情報保護に関する教育を実施する ⑥ 次の事項を含む運用状況記録を作成し、保管する ・本システムの障害記録とその是正処置 ・本システムの設定変更内容 ・ログの保存記録 ・バックアップの実施記録

	・保守、セキュリティ対策の実施情報 ・その他　必要なもの ⑦　定期的に運用状況の記録を確認し、不適切な事項、対処を要する事項等が発見された場合、必要な是正をシステム管理者に指示する ⑧　重大な是正を要する事項が発見された場合、サービスの提供についての管理責任者に報告し、是正措置、対処の協議を行う
ヘルプデスク責任者	運用管理責任者が選任する者を、ヘルプデスク責任者に充てる。 運用管理責任者の統制下で責務を実施する。 **【相談、苦情等の受付と対応業務】** ①　本システムの利用に関する問い合わせへの対応 ②　本システムの内容に関する問い合わせへの対応 ③　本システムへの利用者の登録、変更、解消に関する問い合わせへの対応 ④　本システムの障害に関する問い合わせへの対応 ⑤　本システムの操作に関する問い合わせへの対応 ⑥　個人情報の保護に関する問い合わせへの対応 ⑦　個人情報の保護に関する利用者向け教育の支援 **【本システムの運用に係る連絡調整業務】** ①　利用者等からの利用・変更等の受付と本システムへの設定 ②　利用者等の利用・変更情報の関係先との連絡調整 ③　障害等発生時の関係先との連絡調整 ④　本システムの利用登録、利用変更等の履歴管理と利用状況の報告 ⑤　その他　必要な業務
リモート保守責任者	情報システムについての管理責任者が任命する者を、リモート保守責任者に充てる。 リモート保守責任者は、運用管理責任者の統制下で本システムの安全な運用と迅速な対応を行う。 ①　本システムの稼働状況の監視、障害検知 ②　本システムの障害に関する事象の切り分け、復旧対応 ③　本システムの運用に必要なメンテナンス作業の実施

(1) 運用管理内規の開示等の有無、範囲、条件等

文書名	内容の開示の有無
がんゲノム情報管理センター「C-CAT 利活用ポータル」運用管理内規	開示無し (運用管理内規の内容は本書をもって示します)

(2) 個人情報の管理状況に関係する資料の提供

資料提供の可否	開示方法・条件・範囲
可	本サービスの契約者の資料提供要求に応じて行います

2.2.3 受託する個人情報に係るリスク分析の結果と対応措置

リスクを適宜、適切に特定・評価し、リスクに見合った措置（低減・回避・移転・保有）を講じます。

個人情報に係るリスク分析の結果と対応措置に関して、「添付.予見されるリスク」をご参照ください。

2.2.4 セキュリティ対策についてサービスの利用者側に対応いただく措置

本サービスの利用に際し、予見されるリスクシナリオとその対応措置をお願いします。

リスクシナリオと対応措置に関しても、、「添付.予見されるリスク」をご参照ください。

2.3 緊急時の対応について

2.3.1 障害に備えた対応

本サービスの提供に際し、障害対応を速やかに行うための対策として、下記に示す項目を実施します。

① サーバー・ストレージ等の稼働監視、障害監視、パフォーマンス監視を踏まえた定期的なリスク分析・評価と対策。

② アプリケーション、プラットフォーム、サーバー・ストレージ、情報セキュリティ対策機器等の監視。

2.3.2 障害発生時の責任分界

本サービスのシステム等のトラブルにより生じた障害については、C-CAT において調査を行い、その原因及び回復状況等に関する情報を速やかにサービスの契約者へ連絡します。

ただし災害等、不可抗力により生じた障害については、可及的速やかに調査するが、調査結果の公表の時期について、災害等が沈静化以降に実施する場合があります。

本サービスのシステム等のトラブル以外で生じた本サービス提供上の障害については、その調査結果及び対応に関しては免責といたします。

2.3.3 サイバー攻撃等への対応

サイバー攻撃等の非常時における本サービスの安全管理対策については、下記の項目を実施します。

① サイバー攻撃により、本サービスの提供が困難、若しくは大きな支障が生じた場合の原因探査に必要なログ等の記録を保全するための措置を講じている。

② サイバー攻撃によりサービス提供が困難等になっている旨、及び復旧に関する見通し等について、サービスの契約者に速やかに告知を行う。

③ 本サービスの提供に用いるすべてのアプリケーション、プラットフォーム、サーバー・ストレージ等は日本国の法令の執行が及ぶ場所に設置されている。

2.4 セキュリティ上の事故が生じた際の対応

2.4.1 セキュリティ上の事故対応

セキュリティ事故の発生時における対策については、下記に示す項目を実施します。

① 本システムで受託する個人情報が漏えいした場合には、再発防止策を含む適切な対策を速やかに講じると共に、サービスの提供についての管理責任者より、原因の究明、被害拡大の防止、サービスの利用者への情報の安全性の確保に必要な対応、所管官庁への報告及び指示への対応その他を行います。

② 本システムで受託する個人情報が漏えいした場合には、漏洩状況についてホームページで連絡します。

③ 本システムで受託する個人が漏えいした場合には、その原因が明確になるまで、本サービスの一部又は全部の提供を停止することがある旨をサービスの利用者に予め周知します。

2.4.2 C-CAT における個人情報を取り扱う機器・媒体の運用

(1) 機器の管理等の運用

下記の手順にて対応を行います。

① サービス運用のために使用する端末機器について、台帳管理により所在確認を行う。

② サービス運用のために使用する端末機器を C-CAT 施設外に持ち出す際には、事前に運用管理責任者の許可と返却時に確認する。

③ 万一、サービス運用のために使用する端末機器を紛失した場合、センター内の手順に従って届出・対応を行う。これらのプロセスを職員及び外部委託業者等へ徹底する。

④ クラウドサービスで AWS 上に実装するハードウェア、ソフトウェアの構成管理を実施する。

⑤ クラウドサービスで AWS 上に実装するハードウェア、ソフトウェア共に変更された構成情報は構成情報ログにより把握する。構成情報ログは 5 年間保存とし、少なくとも1年間は即時確認できる状態とする。

(2) 個人情報を記録した媒体の運用

下記の手順にて対応を行います。

① 保守作業等にかかわる者は、システム管理者が特に許可した場合を除き、CD、USBメモリ、磁気テープ(以下、可搬型記録媒体といいます)等へ個人情報の複写を禁止することを原則とする。

② システム管理者が許可した場合、保守作業等に関わる者は個人情報を可搬型情報記録媒体に暗号化して記録する。その媒体は、施錠できるキャビネットに保管し、システム管理者は台帳に記録し所在を管理する。

2.5 リスク分析の結果と対応措置

2.5.1 リスクマネジメント

以下のリスクマネジメントを実施します。

- リスクを適宜、適切に特定・評価し、リスクに見合った措置（低減・回避・移転・保有）を講じる。
- 受託する個人情報に係るリスク分析の結果と対応措置に関して、「添付．予見されるリスク」を参照。
- また、セキュリティ対策についてサービスの利用者側でサービスの利用に際し、想定されるリスクシナリオとその対応措置に関しては、添付1を参照のこと。
- 対応措置は、リスクを特定・評価し、リスクに見合った措置（低減・回避・移転・保有）を講じる。

2.5.2 セキュリティ対策についてサービスの利用者側に対応いただく措置

本サービスの利用に際し、サービスの利用者には想定されるリスクシナリオとその対応措置をお願いします。リスクシナリオと対応措置に関して、「添付．予見されるリスク」を参照願います。

2.6 監査の方針

2.6.1 監査の方針

(1) 外部監査

NCC は、独立行政法人 情報処理推進機構（IPA）や、内閣サイバーセキュリティセンター（NISC）といった外部機関から 2 年に1度監査を受けており、その中で C-CAT として監査対象に指定された場合は受査しています。

(2) 内部監査

- 毎年、NCC 監査室が監査対象を決めて監査を実施しています。
- 自己点検、情報セキュリティ監査では、作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成し、管理しています。
- 運用管理責任者及び委託先は、以下の責務に基づいて監査の実務を行います。

  ① 情報システム及びデータの取り扱いに係る監査を実施し、その結果について監査報告書をもってサービスの提供についての管理責任者に報告する。

  ② サービスの提供についての管理責任者は、運用責任者から監査結果の報告を受け、問題点の指摘等がある場合には直ちに必要な処置等を講じなければならない。

  ③ 本規程における法令、ガイドラインへの準拠状況、情報システムの運用状況及び医療情報の取り扱いについて、監査を実施できる状態にしておく。

  ④ 監査は、監査ログを基に実施することとし、監査の実施においては、監査の客観性及び公平性を確保する。

  ⑤ 監査ログは 5 年間保存し、少なくとも1年間はすぐに分析できる状態にしておく。

  ⑥ 当局から、臨時監査を要求された場合には対応する。

  ⑦ 委託先（再委託先も含む）における法令、契約等に基づく医療情報保護に係る措置の遵守状況を確認するため、業務における定常的な確認に加えて情報セキュリティ監査により確認する場合には、実施する情報セキュリティ監査の目的、対象範囲、管理基準、実施主体等について、委託先と協議の上で契約において具体的に定める。

  ⑧ 委託先は、監査へ協力する。

2.7 サービスの利用者からの問い合わせ

質問・苦情の受け付け窓口としてヘルプデスクを設置しています。

(1) 問い合わせ窓口及び時間帯

【ヘルプデスク】

相談窓口	国立がん研究センター　ヘルプデスク
住所	東京都中央区築地 5-1-1
受付対応時間	平日 9時～17時 土・日・祝日は除く

(2) 問い合わせ内容

① 本システムの利用に関する事項

② 本システムの内容に関する事項

③ 本システムの利用者登録、変更、解消に関する事項

④ 本システムの障害に関する事項

⑤ 本システムの操作に関する事項

⑥ 個人情報の保護、取扱いに関する事項

(3) 実施事項

① 本システムの利用者登録、変更、解消

② 利用者向け個人情報の保護、安全管理に関する教育

③ 利用者向けシステム利用に関する教育

2.8 患者等への説明及び同意を得る方法

本サービスの利用に係る患者等への説明及び同意の取得については、医療機関において対応していただきます。

医療機関における患者等への二次利活用への同意に関しては、患者説明文書・同意書・意思変更申出書(モデル文書)に示されています。

3 人的安全管理対策

3.1 サービス提供に従事する要員が遵守する義務

運用管理責任者は、本システムの取り扱いについて運用のマニュアルを整備し、運用に携わる関係者に周知します。

また、本システムの運用に携わる関係者(情報システムに関する委託先を含む)に個人情報の保護に関する教育を行います。

本システムの運用にかかわる関係者は、在職中、退職後にかかわらず、本システムの運用にかかわる業務上に知り得た個人情報に関する守秘義務を負います。

外部に業務委託する場合は、業務委託先と守秘義務契約を締結します。守秘義務契約に定める事項は本書の業務委託における安全管理事項に記載の通りとします。

3.2 従事する要員の遵守規程

3.2.1 遵守規程

本サービスの提供に従事する C-CAT のすべての職員及び外部委託業者等が遵守する義務等について、下記に示している項目を国立研究開発法人国立がん研究センター就業規則・契約等に定めています。

① 情報を分類するための指針を決定し、運用管理責任者が指針に従って適切な分類を行うことができるようにしておくこと。情報の分類指針は「がんゲノム情報管理センターシステム運用管理規程」第5条(情報の格付け)に準ずるものとする。

② 運用管理責任者は情報の分類が正しく行われていることを確認する。

③ 預託される情報に対して分類に基づいたリスク分析を実施する。

④ リスク分析の結果に応じて、リスク低減に必要な管理策を実施する。

⑤ 分類がわかるように情報にラベルをつけること(電磁的記録にラベルをつける方式には実装する方式の詳細及び安全性について、C-CAT 内での確認、承認を得る)

⑥ 各ラベルに応じた処理方式(保存、配送、複製、廃棄等)を定める。

3.2.2 サービス提供に従事する要員に対する教育

運用管理責任者は、本システムの取り扱いについてマニュアルを整備し、運用管理に携わる関係者に周知を行うと共に、本システムの運用に携わる関係者に個人情報の保護に関する教育を行います。

本サービスの提供に従事する要員(C-CAT のすべての職員・派遣従業者・委託先)に行う教育について、以下に示す項目を、就業規程・契約等に定めています。

① C-CAT として、情報セキュリティポリシー遵守を担保する組織体制の構築とその文書化を行う。

② C-CAT として、自施設内の利用者に、個人情報の取り扱い及び本システムの安全な取り扱いと管理に関する教育を実施する。

③ 上記教育は、就業開始時及び就業後に実施する。

④ サービスの提供に従事する要員については、守秘義務に関する内容を、雇用契約又は派遣契約に含め、かつ就業規則に含める。

⑤　サービスの提供に従事する要員が退職した場合の、就業中に取り扱った個人情報に関する守秘義務を遵守させる。

⑥　サービスの提供に従事する要員が業務上管理していた個人情報については、離職時（内部の異動含む）に返却を求め、システム管理者が返却されたことを確認する。

⑦　サービスの提供に従事する要員の退職時又は契約終了時以降の守秘義務について、教育を実施する。

⑧　C-CAT は②にかかわる教育に関し、本サービスの利用者からの協力依頼を受けた場合、これに協力する。

3.3　業務委託における安全管理事項

(1) 外部との業務委託契約

外部との業務委託には、遵守すべき事項を定め、外部委託により行う情報処理関係業務の遂行において必要な情報セキュリティ水準を確保すること、機器等の購入において情報セキュリティの観点から行うべき手続を定め、情報セキュリティの確保に努めています。

その上で、業務を外部に委託する場合は、守秘事項を含む業務委託契約を結びます。業務委託契約には、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します。

①　個人情報の安全管理に関する事項

②　事業所内からの個人情報の持ち出しの禁止

③　個人情報の目的外利用の禁止

④　再委託に関する事項

⑤　個人情報の取扱状況に関する委託元への報告の内容、頻度及び監査への協力事項

⑥　契約内容が遵守されていることを委託元が確認できる事項

⑦　契約内容が遵守されなかった場合の処置

⑧　事件・事故が発生した場合の報告・連絡に関する事項

⑨　漏えい事案等が発生した場合の業務委託先の責任に関する事項

⑩　一連の委託業務終了後に関する事項（終了報告、確実に情報を消去する等）

⑪　確実に削除又は破棄したことを証明書等により確認できる事項

⑫　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）

⑬　従業員に対する監督・教育

(2) 業務委託に基づく業務履歴

・　情報システムの保守等、本システムの操作結果について、操作ログ等により記録し管理する。

・　運用管理責任者は、取得した操作ログ等により、アクセスされた医療情報についての状況をレビューする。

(3) 再委託の安全管理

委託先事業者が再委託を行う場合において、委託先と同等の個人情報保護に関する契約がなされることとする。

また、再委託先が、医療情報ガイドラインに規定する安全管理対策を行っていることを確認する。

4 物理的安全管理対策

4.1 本サービスを提供するデータセンター

(1) 本サービスの提供に供する機器等が格納されている建物種別(建物名)・地域

インフラストラクチャーの外部委託先は AWS とし、AWS の日本のデータセンター(東京リージョン)を使用しています。

建物に関する情報	Amazon Web Services, Inc.の東京リージョン
データセンターの所在	関東広域
建物種別	鉄筋コンクリートによるビルディング内

(2) データセンター設備及びシステムの安全管理対策状況

上記(1) に示す施設における災害対策等安全管理対策の状況は下表の通りです。

災害種別等	対応
地震への対応	・ 洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を選択しています。 ・ 最新式の免震装置の採用を始めとして、日本のデータセンターは日本の震災に関する規格に準拠するように設計されています。
水害への対応	・ 漏水を検出するため、水があることを検出するシステムをデータセンターに備えています。 ・ 水が検出された場合、それ以上の水害を防ぐために水を除去するメカニズムが備わっています。
落雷対策	・ 誘導雷対策を実施しています。
火災対策	・ データセンターには、自動火災検出システム及び鎮火システムが設置されています。 ・ 火災検出システムにおいては、ネットワーキングスペース、機械的スペース、インフラストラクチャースペース内で煙検出センサーが使用されています。また、これらのエリアは鎮火システムによっても保護されています。
停電対策	・ データセンターの電力システムは、完全に冗長化され、運用に影響を与えること無く管理が可能となっています。 ・ 1 日 24 時間体制で、年中無休で稼動しています。 ・ 施設内の重要かつ不可欠な業務に対応するために、電力障害時に運用を維持するための電力供給を可能とするバックアップ電源がデータセンターに備わっていることを保証しています。
熱対策及び結露対策	・ データセンターは、環境を制御すると共に、サーバーやその他のハードウェアの適切な運用温度を保ち、過熱を防ぎ、サーバー停止の可能性を減らすためのメカニズムを使用しています。 ・ 作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。
その他の対策	パンデミックへの対応 ・ 感染症の爆発的な流行の脅威に対して迅速に対応するための準備として、パンデミック対応ポリシーと手順を災害復旧計画に組み込んでいます。

災害種別等	対応
	・ 関連したリスクに関する軽減のための戦略には、重要なプロセスをリージョン外のリソースに移動するために、どのようにスタッフを配置するかという代替モデルと、重要なビジネス業務をサポートするための危機管理の発動計画が含まれます。 ・ パンデミック計画は、国際的な健康関連機関や規制に従っており、国際的な関連機関との連絡窓口等も含まれています。

(3) データセンターの入退管理に関する状況

AWS 従業員によるデータセンターへの入退管理は以下の通りです。

① 場所の秘匿性（重要データが保管される場所は秘匿する方が高いセキュリティというポリシーによる）

② 監視カメラや侵入検知システム、24 時間常駐の専門保安員による物理アクセスの厳密な管理

③ 完全管理された、必要性に基づく物理アクセス

④ 管理者・作業者は、2 要素認証を 2 回以上で入場、入室

⑤ すべての物理アクセスは記録され、監査対象となる

4.2 C-CAT として実施している物理的安全管理対策

4.2.1 個人情報が参照可能な場所の設備と入退室管理

(1) 情報取扱区域の管理責任者

情報を適切に管理するため、C-CAT 内外における情報取扱区域を定め、区域毎に、求める対策の観点から「クラス」の区分を定めています。

特に機微情報を取り扱う区域を「要管理対策区域」と指定しています。

(2) 要管理対策区域の設備と入退室管理等（C-CAT 内における基準）

C-CAT 内の要管理対策区域はクラス2以上であることから、管理目的で本システムにアクセスする場所においては以下を遵守します。

① 要管理対策区域の管理目的で本システムにアクセスする場所は、間仕切り又は独立した室とし、外部の者と隔離されている。

② 要管理対策区域の管理目的で本システムにアクセスする場所のサービスに供する機器や媒体の保存場所（ラック、保管庫含む）においては、取り扱う情報の種類やシステムの機能等が、外部から識別できるような情報が見えないように措置を講じている。

③ 要管理対策区域の管理目的で本システムにアクセスする場所においては、運用業務に供した文書、ノートパソコン等の可搬型情報機器、可搬型情報記録媒体等を保管する、鍵付保管庫を設置する。

④ 鍵付保管庫を要管理対策区域外に設置する場合において、運用業務に供した文書類、データ、機器等の持ち運びに際し紛失、盗難等の防止に十分な注意を払う。

⑤ 鍵付保管庫の鍵は、サービスの提供の管理責任者、運用管理責任者、情報システムの管理責任者及び各管理者が指定した者のみが使用できるものとする。

⑥ 要管理対策区域の管理目的で本システムにアクセスする場所では、ID カード認証と静脈認証により来訪者の記録・識別、入退履歴を取得している。

⑦ 要管理対策区域の管理目的で本システムにアクセスする場所では、不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等を設置している。

⑧ 要管理対策区域の管理目的で本システムにアクセスする場所では、入退状況の管理（入退記録のレビュー含む）は定期的に行う運用としている。

⑨ 防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じている。

⑩ 要管理対策区域では、場所への不明者の入退を発見するために、職員は名札、ゲストは入館許可証を身につけることを義務付けている。

⑪ 要管理対策区域の管理目的で本システムにアクセスする場所では、入室権限者が不在の時は、原則事務室は施錠されている。

⑫ 文書などの情報は、帰宅時には当該情報を鍵付保管庫に戻す。

(3) 解任者からの入室用鍵と保管庫鍵の回収

入館用 ID カード、保管庫用の鍵は、保有している者の解任時に、各責任者によって回収します。

(4) 要管理対策区域への外部者の入室

本システム運用業務の実施中に本システムにアクセスする場所へ入室権限者以外の者が入室する際は、入室権限者の立会いのもとで入室及び退室を行います。

4.2.2 要管理対策区域の端末からの情報漏洩対策

① 要管理対策区域内でパソコンを使用する場合は、パスワードが設定されたパソコンを使用する。また、離席時にはパスワード・ロックを実施し、許可されない者が情報にアクセスすることを防止する。

② 要管理対策区域内でパソコンを使用する場合は、覗き見防止対策を実施する。

5 技術的安全管理対策

5.1 情報区分と保存

取り扱う情報の区分について、機密性、完全性及び可用性の3つの観点での区別を定義しています。

- C-CAT として、保存する情報の中で保護されるべき対象 を洗い出し分類する。分類に応じて重要度のラベル付けを行うが、本サービスでは、要配慮個人情報として機密性が高い情報の区分としている。
- 守るべき情報を明確にし、それを脅かす リスク(脅威) を明らかにする。
- その上で、機密性が高い情報に基づいたリスク分析と、リスク分析の結果に応じてリスク低減に必要な管理策を実施する。

5.2 技術的対策

5.2.1 インフラストラクチャーへのアクセス管理・アクセス制御

① 情報システムのインフラストラクチャー利用者を特定し識別できるように、個人毎にユニークなアカウントの発行を行う。

② それぞれの情報にアクセスする権限を持つ作業者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行う。

③ 本サービス提供に従事する運用・開発担当者(管理責任者含む)における本サービスに関する業務実施に際しては、担当者を一意に特定できる ID だけでなく、パスワード認証及び MFA(二要素認証)によるアクセス制御を実施する。

④ あらゆる操作を可能とする特権 ID は使用しないことにしている。

⑤ インフラストラクチャーへログオンするときのパスワードルールを定め運用している。

⑥ 認可されていない作業者あるいは第三者がログオンを試みた際には、作業者 ID が存在していることを知る手がかりとならないような特段の情報を与えることのないメッセージが表示される。

5.2.2 インフラストラクチャーの運用・保守端末からの情報漏洩対策

① サービスの運用・インフラストラクチャーの操作は、原則として C-CAT 内の指定区域に限定する。

② サービスの運用・保守端末を設置している区域は監視カメラ等により適切に監視を行っている。

③ サービスの運用・保守端末又はセッションの乗っ取りのリスクを低減するため、利用者のログオン後に一定時間の使用中断時間が経過した場合セッションを遮断する。

5.2.3 マルウェア検出/除去

本サービスでマルウェア等対策は、下記に示す項目を実施しています。

① 本サービスの提供に係るシステムに対しては、ウイルスあるいはマルウェア対策ソフトウェアを導入し、最新の攻撃への対策を講じる。

② 本サービスの提供に係るシステムにウイルスあるいはマルウェアが混入しないよう手順を策定し、開発・運用を実施している。

③ ウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新している。

④ 情報システムの構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新のウイルス対策ソフト等の導入を行う。またシステム情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。

⑤ 情報システムの脆弱性に関する情報は、AWS サービスの脆弱性診断情報源から、定期的及び必要なタイミングで取得し、確認する。

5.2.4 不審なアクセス検知の際の対処

不審な通信が検知された場合には、情報システム責任者は当該通信先との通信を遮断します。

5.2.5 データの暗号化

(1) 情報の伝送途中におけるデータの暗号化(チャネルセキュリティ)

・ サービス利用者からは AWS へ IPsec-VPN で HTTPS により接続することとし、高セキュリティ型プロトコルに限定する。SSL/TLS のプロトコルバージョンは TLS1.2 以上を利用する。

・ 電子証明書による TLS クライアント認証を行う。

(2) 保存データの暗号化(オブジェクトセキュリティ)

保管されたデータが意図しない第三者から読みだされるのを防ぐため、保管データの暗号化を必須としています。

5.2.6 外部からの不正な攻撃（DDoS）等への対策

本サービスで外部からの不正な攻撃等への対策は、下記に示す項目を実施しています。

① 不正侵入検知システム(IDS)及び不正侵入防止システム(IPS)等を導入し、不正な攻撃に対するトラフィックの遮断等がとれるような措置を講じている。

② 侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行っている。

③ サーバー等の AWS リソース単位にセキュリティグループを設定することにより、アクセス制御を行っている。

④ サブネット単位にネットワーク ACL を設定することにより、サブネット単位で必要な通信のみに制限を行っている。

5.2.7 冗長構成

ハードウェアの障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施しています。

- サービスで実装するサーバーは、自動復旧機能を有効化し、予備機が準備されていることと同等でである。
- データ保存の冗長構成に関しては、AWS のストレージサービス機能により自動的に 3 つのデータセンター群にまたがり複製される。これにより、高い堅牢制を確保する。

5.2.8 バックアップ

(1) バックアップ

データのバックアップ基準を下表に示します。

データバックアップの頻度	リレーショナルデータベースサービス(Amazon RDS)の機能により、1 日に 1 回スナップショットのバックアップを自動で取得する
データバックアップの時間帯	毎日 0:00～0:30 の間でバックアップを開始
データバックアップの管理世代数	3 世代とする。
バックアップ媒体	AWS のストレージサービスである Amazon S3 とする
データバックアップ監視	データバックアップは監視を行い、バックアップ失敗の際にはリトライを行う バックアップ失敗の原因を調査し対策を講じることとする

(2) 復旧

障害発生の際には、バックアップからリストアを実施し復旧を図ります。

(3) 毀損したデータの取り扱い

本サービスの提供に際して、受託したデータの毀損が生じた場合の対応を下記に示します。

① 本規程に則り、データが毀損した場合でも、速やかに回復できるよう、バックアップ対応及び冗長化対応を講じると共に、その回復手順を定めています。

② 毀損したデータの回復が困難である場合には、毀損したデータに最も近いデータの回復を、回復手順に基づき行います。

③ サービス提供に際して、受託データが毀損した場合において、本項で定める措置を行った上で、なお回復が困難であった場合、C-CAT の故意・重過失があった場合を除き、免責とさせて頂きます。

5.2.9 ソフトウェア開発における開発環境の安全管理

① ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用環境とは直接に接続されていない開発用の環境を用いて行う。

② 開発施設では悪意のあるコードが混入することを避けるため、不特定多数が利用するネットワーク(インターネット等)と接続を持つ場合にはウイルス対策ソフトを入れることを必須とする。

③ 保守で用いるデータに関し、情報システムの動作確認に際しては、原則として受託した個人情報を含むデータを使用せず、テスト用のデータを使用する。

④ アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行う。

⑤ 変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討する。

5.2.10 保守作業時の確認事項

本システムの改造及び保守作業における作業管理・監督、作業報告確認のため、システム管理者は、保守作業に関し、以下の確認を実施します。

① 作業者・作業内容・作業結果の確認

② 保守契約における個人情報保護の徹底

5.2.11 外部の保守会社による保守作業時の確認事項

本システムの改造及び保守作業等において、作業管理・監督、作業報告確認のため、システム管理者は、保守会社における保守作業に関し、以下のような確認を実施します。

① 作業者の所属・氏名、作業内容・作業結果の確認

② 保守契約における個人情報保護の徹底

③ 責任分界点、責任所在等の契約書の確認

5.2.12 サービス品質

(1) 機器・ソフトウェア等の品質管理

機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを規定しています。

機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施しています。

(2) サービスの利用者が使用するインターネット回線、無線 LAN・機器に関する免責

- サービサス利用者の施設、その他の施設において既に設置されているインターネット回線及び無線 LAN を通じて、本サービスを利用する場合、当該 の装置の稼働やセキュリティ対策については、サービスの利用者の責任において対応して頂くものとし、これに起因して本サービスの利用に支障が生じた場合には、本サービスのサポート対象外とします。
- サービスの利用者の施設、その他の施設において既に設置されているネットワーク機器は ISO15408 と同義の CC(EAL 4+)認定(医療情報ガイドライン要求事項)を得ていることを確認済みであること。
- サービスの利用者側で使用されている無線 LAN では以下の対策済みであることを確認していること。
- 利用者以外に無線 LAN の利用を特定されないようにしている。例えば、ステルスモード、ANY 接続拒否等の対策をとっていること。
- 不正アクセスの対策をとっている。少なくとも SSID や MAC アドレスによるアクセス制限を行っていること。
- 不正な情報の取得を防止している。例えば WPA2/AES 等により、通信を暗号化し情報を保護していること。
- 業務上、サービスに使用するモバイル端末を持ち出す場合には、公衆無線 LAN への接続は行わないこと。

ネットワークの責任分担に関しては、本サービスのサポート対象外とし、以下の関連組織の責任分界点、責任の所在を契約書等で明確にしますが、障害発生時には通信事業者と協力の上で早期復旧に努めることとします。

- 診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換にかかわる操作を開始する動作の決定
- 送信元の医療機関等がネットワークに接続できない場合の対処
- 送信先の医療機関等がネットワークに接続できなかった場合の対処
- ネットワークの経路途中が不通又は著しい遅延の場合の対処
- 送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処
- 伝送情報の暗号化に不具合があった場合の対処
- 送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処
- 障害が起こった場合に障害部位を切り分ける責任
- 送信元の医療機関等又は送信先の医療機関等が情報交換を中止する場合の対処
  また、医療機関内における障害発生等事象への責任の明確化

6　情報の廃棄に関する安全管理対策

6.1　情報の破棄に関する安全管理対策

本サービスでは、システム管理者が特に許可した場合を除き、保守作業等にかかわる者がCD、USBメモリ、磁気テープ等可搬型記録媒体への個人情報の複写を禁止しています。

その上で、本サービスの提供に情報機器、紙情報、情報記録媒体等の破棄等における安全管理対策について、下記に示す項目を実施します。

① 運用管理責任者は、個人情報を格納した媒体(紙媒体、CD、USBメモリ等媒体、情報機器を含む)の廃棄が、安全かつ確実に行われるよう管理する。

② 紙媒体の廃棄は、シュレッダーによる粉砕処理とする。外部の廃棄業者に委託する場合は、溶融廃棄証明書を受領する。

③ 電子媒体の廃棄は、原則粉砕処理によるものとする。

④ 情報機器のハードディスク等のデータについては、消去したデータを復元できない方式で消去を行う。ハードディスク等のデータの消去を外部事業者に委託する場合は、消去証明書を受領する。

⑤ 特に重要な情報の廃棄においては、廃棄、消去の結果をサービスの提供についての管理責任者に報告する。

7　クラウドサービスの利用終了

7.1　本システムの変更

・　サービスの提供についての管理責任者は、システムの改良、障害対策等を目的として、本システムを変更することができることとします。

・　運用管理責任者は、重要な変更を行う場合、その旨を利用者に事前に通知します。

7.2　利用の一時停止

①　サービスの提供についての管理責任者は、正常でない利用方法、不正なログオン等が認められ、必要と認めた場合は、当該契約者への事前の通知、承諾を得ること無くサービスの一部又は全部の使用を停止することができることとします。

②　サービスの提供についての管理責任者は、システムの保守、改良等の理由で、一時的にサービスの停止が必要な場合、事前に契約者に通知の上で、サービスの一部又は全部の一時停止を行うことができるものとします。

③　サービスの提供についての管理責任者は、次のいずれかの場合には、契約者に事前に通知すること無く、サービスの一部又は全部の一時的停止を行うことができることとします。

・　システムの保守、障害対策等を緊急に行う必要がある場合

・　天災地変及び事故等により、サービスの提供ができなくなった場合

・　その他の理由で、システムの一時的停止が必要と判断した場合

④　前①②③項により、当該契約者若しくは利用者に損害が発生した場合、サービスの提供についての管理責任者はいかなる責任も負わないこととします。

7.3　本サービスの終了

サービスの提供についての管理責任者は、契約者に少なくとも6か月前に予告をした上で、本システムのサービスの一部又は全部の提供を中止することができる。

7.4　インフラストラクチャーの外部委託先サービスの終了に対する対応

インフラストラクチャーの外部委託先である AWS がクラウドサービスを終了する場合は、可用性、代替可能性等考慮して他のクラウドサービスを選定し移行することとします。

8 サービス利用者に遵守いただく安全管理対策上の対応

8.1 サービスの利用上の安全管理対策

(1) サービス利用者の認証

サービス利用者の認証として以下の対応を実施します。

① 本システムを利用する利用者は、ID・パスワードによる本人認証を行う。

② サービスの利用は 1 年更新であり、1年に 1 回利用者を確認する。

③ ID は C-CAT から利用者 ID を通知する。

④ サービス利用者のパスワードルールは以下の通りとする。

- 使用するパスワードは半角 8 文字以上 16 文字以下。英大文字(1 文字以上)、英小文字(1 文字以上)、数字(1 文字以上)、記号(1 文字以上)とし、利用者 ID を含めることはできない。
- パスワードは 180 日毎の変更を必須とする。
- パスワード入力を 6 回失敗した場合には、本システムへのログインを不能とする。再開にはヘルプデスクに連絡し、ヘルプデスクでは本人確認の上でパスワードをリセットする。

(2) 利用者の ID、パスワードの再発行

利用者が ID、パスワードを失念した等の場合には、予め策定した手順(本人確認を含む)に則り、本人への再発行を行います。

① 本サービスの利用者等が使用するパスワードの再発行を希望する場合は、ヘルプデスクに対して再発行を依頼する。

② ヘルプデスクは、利用者等からパスワードの再発行申請を受け付けた場合、速やかにパスワードを初期化し、初期化後のパスワードを本サービスの利用者に連絡する。

(3) 本システムの情報漏洩対策

本システムでは、無操作状態から 2 時間経過した場合、自動的にログオフする機能を適用します。

(4) サーバーの真正性証明

本システムの実在性を証明し、本システムの Web サーバーと利用者のブラウザ間で通信データの暗号化を行うため、サーバー証明書を使用します。サーバー証明書は閉域網においては独自に設置した認証局において発行された証明書を、インターネットにおいては信頼できる認証局より発行された証明書を用います。

(5) サービスの利用者が使用するインターネット回線、無線 LAN・機器

サービス利用者の施設の内外において使用するネットワーク環境に関しては本書、技術的安全管理対策の「サービスの利用者が使用するインターネット回線、無線 LAN・機器に関する免責」を参照願います。

(6) 利用者の利用範囲

本システムを利用する利用者がそれぞれ登録、閲覧、データ出力等が可能な情報項目については、別途定めるものとします。

8.2 サービスの利用者に求めるセキュリティ対策の実施

サービスの利用者は、本規程に定める事項を周知徹底の上で遵守願います。

サービスの利用者は、本システムを利用した個人情報の取り扱いに関する責任を負い、セキュリティに関して次の各項に定める対策を実施願います。

① サービスの利用者が保有する端末等について、自己の責任により厳重な管理を行うこと。

② サービスの利用者は、自身が管理する施設内における可搬型記録媒体の使用状況を管理すること。特にデータをダウンロードした可搬型記録媒体については、施錠できるキャビネットに保管するなど、厳重なセキュリティ対策を講じること。

③ 端末には、盗難防止用チェーンを取り付けるなどの防犯措置を講じること。若しくは機器が設置されている部屋の施錠や入退室管理を徹底すること。

④ ダウンロードしたデータを印刷する場合は、紛失・盗難が無いよう厳重に注意すること 。

⑤ データ閲覧中の覗き見を予防するために、運用端末に覗き見対策のシートを貼る、無操作から短時間でのパスワード付きスクリーンセーバーを設定する等の対策をすること。又は、運用端末のデータ閲覧中の画面が、利用者以外の者の視野に入らないような対応等を行うこと。

⑥ 本システムと接続する機器等と外部との接続には、厳重なセキュリティ対策を講じること。

⑦ 本システムと接続するパソコン等は、OS 等のセキュリティ対策のアップグレードを行い、マルウェア対策ソフトウェアをインストールし、常に最新の定義ファイルに更新すること。

⑧ 不特定多数へのファイル交換を可能とするソフトウェア等をインストールしないこと。

⑨ パスワードの規則を遵守すること。また、パスワードは 180 日毎の変更を必須とすること。

⑩ パスワードの入力に連続して 6 回失敗した場合にはログイン不能となる。
(その場合はヘルプデスクへ連絡しパスワードリセットを依頼すること。)

8.3 サービスの利用者に求めるセキュリティ事故及び障害時の対応

① 利用者は、本システムの利用に際して、システムの異常、あるいは利用の不可等、正常でない事象を発見した場合、速やかにヘルプデスクに報告を行うものとし、その対応に関し、ヘルプデスクの指示を受け対処すること。

② 契約者は、情報セキュリティに関する事故やシステム上の欠陥を発見した場合には、速やかにヘルプデスクに報告を行うものとし、その対応に関し、ヘルプデスクの指示を受け対処すること。

③ 契約者は、事故及び異常に関し、重要な事象は、ヘルプデスクへ報告を行うこと。

④ サービスの提供についての管理責任者は、前②、③項の報告を受け、重大事項と判断した場合、必要に応じて対策を検討するものとする。

8.4 サービスの利用者に求める禁止行為

契約者若しくは利用者は、本システムの利用に際して次の各号に該当する行為を禁止します。

① 公序良俗に反すること。

② 他の利用者又は個人のプライバシー、財産等を侵害すること

③ 他の利用者又は個人誹謗中傷すること。

④ 虚偽の利用の申請を行うこと。

⑤ 登録された情報の改ざんを行うこと。

⑥ 本規程、本システム個人情報保護方針、本システムセキュリティポリシー等に反して利用を行うこと。

⑦ 電子証明書を不正に使用すること及び不正に使用させること。

⑧ 作為、無作為にかかわらず、パスワードを他者に伝えること。

⑨ 本システムの運営を妨げる行為をすること。

⑩ サービスの提供についての管理責任者が利用者として不適当と判断した行為をすること。

⑪ サービスの提供についての管理責任者が契約者として不適切と判断した行為をすること。

契約者若しくは利用者が前項のいずれかに該当する行為を行った場合、サービスの提供についての管理責任者は、当該契約者に事前に通知することなく、契約者の本システムの利用を中止若しくは解除できることとします。

契約者若しくは利用者が、「サービスの利用者に求めるセキュリティ対策の実施」のいずれかに該当する行為を行ったことで情報システム・サービスの提供事業者が損害を被った場合、若しくは「サービスの利用者に求める禁止行為」の実施において、情報システム・サービスの提供事業者が損害を被った場合、サービスの提供についての管理責任者は契約者に対し被った損害の賠償を請求できることとします。

8.5 サービスの利用期間

本システムの利用者は、本サービスの利用契約期間中に限り、本システムを利用することができます。

期間終了後は、原則利用できないこととします。

9 本書の見直し

9.1 セキュリティポリシー等の変更による見直し

① 本システムに係る個人情報保護方針、セキュリティポリシー等の見直しがあり、本書に影響を与える場合、運用管理内規の見直しを行います。

② 「緊急時、障害時、災害時の対応手順」の見直しがあり、運用管理等に問題がある場合、本書の見直しを行います。

9.2 利用者からの指摘による見直し

サービスの利用者、関係者等からの申し出を受け、運用管理等に問題がある場合、本書を見直すことがあります。

9.3 本書公開、改訂の管理

本書は、サービスの利用者に公開するものとします。

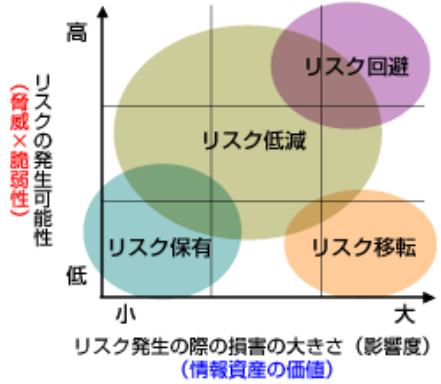
9.4 サービス仕様適合開示書の改訂の管理

サービス仕様適合開示書の改訂管理は、運用管理責任者が行います。

― 以 上 ―

添付．予見されるリスク

- **リスク回避：**脅威発生の要因を停止あるいは全く別の方法に変更することにより、リスクが発生する可能性を取り去ること
- **リスクの低減：**脆弱性に対して情報セキュリティ対策を講じることにより、脅威発生の可能性を下げること
- **リスク移転：**リスクを他社などに移すこと。例えば、リスクが顕在化したときに備えリスク保険などで損失を充当する、情報システムの運用を他社に委託し、契約などにより不正侵入やウイルス感染の被害に対して損害賠償などの形で移転するなどが該当。
- **リスク保有：**そのリスクのもつ影響力が小さいため、特にリスクを低減するためのセキュリティ対策を行わず、許容範囲内として受容すること。「許容できるリスクのレベル」を超えるが、現状において実施すべきセキュリティ対策が見当たらない場合や、コスト（人、物、金等）に見合ったリスク対応の効果が得られない場合等にも、リスクを受容する。



安全管理対策別リスクシナリオ	事業者	利用者	対応	内容
組織的・人的リスクシナリオ				
1.1① 権限のない第三者や内部不正による不正な閲覧や操作が行われる。	✔		低減	・「サービス提供についての管理責任者」、「情報システムについての管理責任者」、「運用管理責任者」、「ヘルプデスク責任者」、「リモート保守責任者」をそれぞれ任命し、不正行為の禁止を徹底する。 ・情報システムについての管理責任者によりシステムの開発者、保守作業者の登録を管理し、不正な利用を防止する。 ・情報システムについての管理責任者により、本システムにかかわる保守作業者に対し個人情報保護の教育を実施する。 ・運用管理責任者により、定期的に運用状況の記録を確認し、不適切な事項、対処を要する事項が発見された場合は必要な是正を情報システムについての管理責任者に指示する。 ・重大な是正を要する事項が発見された場合、サービスの提供についての管理責任者に報告し、是正措置、対処の協議を行う。 ・運用管理責任者により、システムやデータへのアクセスや操作に関する実態を把握し、定期的監査を実施する。監査内容は、サービス提供についての管理責任者に報告し、リスクが発見された場合は速やかに是正措置を講じる。
1.1② 持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	✔	✔	低減	・個人情報を可搬型機器や媒体に保存しないことをルール化する。 ・本システムにアクセス可能な機器の持ち出しを禁じる。

安全管理対策別リスクシナリオ		事業者	利用者	対応	内容
1.1③	情報の廃棄が不十分なまま、再利用が行われることで、情報漏えいが生じる。	✔	✔	低減	・ 個人情報にかかわる事項を紙媒体で扱わない。情報システムについての管理責任者により例外的に紙媒体を使用する場合、シュレッダーを用いた粉砕処理により、紙媒体を廃棄する。 ・ 本サービスでは、システム管理者が特に許可した場合を除き、CD、USBメモリ、磁気テープ等可搬型記録媒体への個人情報の保存・複写を禁止する。 ・ 例外的に情報機器のハードディスクや可搬型記録媒体等に個人情報を格納した場合、そのデータについては、消去したデータを復元できない方式で消去を行う。ハードディスク等のデータの消去を外部事業者に委託する場合は、消去証明書を受領する。消去証明は、データベースからの消去を画面キャプチャーする。 ・ 特に重要な情報の廃棄においては、廃棄、消去の結果をサービスの提供についての管理責任者に報告する。
1.1④	持ち出した機器に格納された情報が漏えいする若しくは、持ち帰った機器から不正なプログラムが感染拡大する。	✔	✔	低減	本システムにアクセス可能な機器の持ち出しを禁じる。
1.1⑤	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏えいする。	✔	✔	低減	本システムにアクセス可能な機器の持ち出しを禁じる。
1.1⑥	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	✔	✔	低減	・ 個人情報が格納・処理される機器はすべてクラウドサービス(AWS)とし、機器の老朽化対策による入れ替えは発生しない。 ・ ソフトウェアの変更に関しては、試験環境を準備し、意図しない情報の虚偽入力、書き換えや消去、混同が生じないことを確認した上で本番環境を変更する。
1.2	動作確認のために利用したテストデータに含まれた個人情報の漏えいが生じる。	✔		低減	試験環境における動作確認等作業に、個人情報を使用しない。
1.3①	医療情報システム提供にかかわる職員(派遣従業員含む)のうち悪意をもった者による情報漏えいが行われる。	✔		低減	・ 情報システムについての管理責任者により、個人情報保護の教育を実施する。 ・ 個人情報へのアクセス権限は必要最小限とし、アクセスのすべては記録され監査対象とする。 ・ 情報システムの改造と保守を担当する者は、個人情報へのアクセス権を付与しない。
1.3②	本システム提供にかかわる事業者(再委託先も含む)による故意又は過失による情報漏えいが行われる。	✔		低減	・ 情報システムについての管理責任者により、個人情報保護の教育を実施する。 ・ 個人情報へのアクセス権限は必要最小限とし、アクセスのすべては記録され監査対象とする。 ・ 情報システムの改造と保守を担当する者は、個人情報へのアクセス権を付与しない。
1.4	医療情報システム提供にかかわる職員(派遣従業員含む)が定められた手順を理解しないことで、過失による事故が発生する。	✔		低減	・ 情報システムについての管理責任者により、作業手順の整備を行い関係者の教育と訓練を行う。
1.5①	医療情報システム提供にかかわる職員(派遣従業員含む)が業務上不必要な医療情報の閲覧や操作を行う。	✔		低減	・ 情報システムについての管理責任者により、個人情報保護の教育を実施する。 ・ 個人情報へのアクセス権限は必要最小限とし、アクセスのすべては記録され監査対象とする
1.5②	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期発見できず、被害が拡大する。	✔	✔	低減	・ 個人情報が格納・処理される機器はすべてクラウドサービス(AWS)とし、機器の紛失や盗難は発生しない。 ・ 機器や媒体の持ち出しを禁じる。 ・ サービス運用のために使用する端末機器について、台帳管理により所在確認を行う。
1.5③	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	✔		低減	・ 計画・承認されたハードウェア、ソフトウェアが実装されているかを構成管理する。また、変更都度、構成情報を管理する。過去の変更履歴も遡及して把握可能としておく。
1.6	搬送中の電子媒体内の情報が抜き取られることで、情報漏えいが生じる。	✔		低減	可搬型の媒体に個人情報を格納することを禁止する。

安全管理対策別リスクシナリオ		事業者	利用者	対応	内容
1.7	患者(サービスの利用者)等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。			—	—
1.8	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏えいが生じる。	✔		回避	保存される個人情報はクラウド(AWS)のストレージに格納されており、情報システム・サービスの提供者がデータを消去した後に、AWS によってワイプ処理を行った後、未フォーマットのローブロックデバイスとして他の AWS 利用者に提供されるため、他にデータが漏えいすることはない。
1.9	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生する。	✔		低減	・ 運用管理責任者により、委託先への本システムの運用、個人情報保護に関する教育を実施する。 ・ 委託先とは、委託契約によって個人情報の適切な管理条項を締結する。 ・ 再委託先においては、委託先の責任において本システムの運用、個人情報保護に関する教育を実施する。また、委託先と再委託先においても、契約によって個人情報の適切な管理条項を締結する。 ・ 運用管理責任者は、委託先と再委託先間で適切な契約が締結されているかを確認する。
1.10①	災害発生時における事業継続のための対策が過少若しくは費用対効果の観点で過剰となる。	✔		低減	・ 取り扱う情報の重要度によって、災害発生における事業継続の対策をとる。 ・ クラウドサービス(AWS)の推奨する冗長構成やマネージドサービスを有効に活用し、事業継続のための対策を講じる。 (ただし、サーバー、Amazon RDS はシングル構成)
1.10②	災害発生時に、医療情報システムを最大許容停止時間内に復旧できない。	✔		低減	・ 取り扱う情報の重要度によって、災害発生における事業継続の対策をとる。 ・ クラウドサービス(AWS)の推奨する冗長構成やマネージドサービスを有効に活用し、事業継続のための対策を講じる。 (ただし、サーバー、Amazon RDS はシングル構成) ・ **AZ 障害時、サーバーは AMI から再構築、Amazon RDS はスナップショットから復旧。**
1.10③	非常時の代替手段で処理した情報が医療情報システム復旧後に正しく処理できない。	✔		低減	非常時における本サービスの提供に際して実施する安全管理対策のうち、以下を定める。 ・ 個人情報を取り扱うサービスにかかわるコンテンジェンシープランの策定。 ディザスタリカバリ(DR)構成によるシステムの実装で、非常時に DR へ切り替えることで業務継続性を確保し、復旧後に切り戻しの手順を策定しておく。これらを適時訓練すること。 ・ サービス回復後のデータ整合性の確保 DR 構成にとるデータ保存の冗長構成により、非常時の代替手段、復旧後も継続的に正しい処理が行える仕組みとする。
1.10④	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	✔		保有	非常時用のアカウントは作成しない。
1.11①	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な対策が講じられない。	✔		低減	サイバー攻撃等の非常時における本サービスの安全管理対策については、下記に示す項目を実施する。 ・ サイバー攻撃により、本サービスの提供が困難、若しくは大きな支障が生じた場合の原因探査に必要なログ等の記録を確保する。 ・ 上記の場合、サービス提供が困難等になっている旨、及び復旧に関する見通し等について、サービスの契約者に速やかに告知を行う。 ・ サービス提供についての管理責任者は、上記方法により状況を速やかに把握し所管官庁への速やかな報告に努める。
1.11②	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	✔		低減	・ サイバー攻撃により、本サービスの提供が困難、若しくは大きな支障が生じた場合の原因探査に必要なログ等の記録を確保する。

安全管理対策別リスクシナリオ		事業者	利用者	対応	内容
					・ ログの保存機能を常に有効とする。
1.12	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	✔		低減	・ システム構成を常に最新化し、責任範囲の明確化を図る。 ・ 本サービスの責任範囲を明文化し、党が医療機関やサービスの利用者に告知しておく。
1.13①	医療情報システムの構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	✔		低減	システム侵入テスト、アプリケーションの脆弱性診断を実施し、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。可能性を低減する。 （ただし、サーバーにおいて Inspector による脆弱性診断は行っていない）
1.13②	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	✔		低減	アプリケーションの脆弱性診断を実施し、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。可能性を低減する。 （ただし、サーバーにおいて Inspector による脆弱性診断は行っていない）
1.13③	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入し、不適切なデータ・プログラムがおかれてしまう。	✔		低減	本番環境と開発環境(試験環境含む)は、クラウドサービス(AWS)内のネットワークレベルで明確に分離し、アプリケーションの改造や保守は本番前に必ず開発環境(試験環境)で評価することを義務化する。
1.14①	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われない。	✔		低減	ハードウェア、ソフトウェアともログから構成管理ができる仕組みを導入し、変更管理によりデグレーションが発生していないことを確認する。
1.14②	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	✔		回避	・ ハードウェアの保守に関しては、AWS 責任共有モデルにおける AWS 責任範囲としてオフロードできる。 ・ ソフトウェアの保守に関しては、本番環境への保守の前に開発環境(試験環境含む)で必ず検証することを義務化し、システム・サービスの停止を最小限に留める。
1.14③	突然の医療情報システムの停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	✔		低減	システムの仕様変更には、医療機関との間で十分な準備が行えるよう、都度合意形成を図る。
物理的リスクシナリオ					
2.1	許可された者以外が機器や媒体に直接アクセスする。	✔		低減	・ AWS インフラストラクチャーやデータへの認証・認可を規定し、それに準じた権限を付与する。 ・ AWS インフラストラクチャーやデータへのアクセスに用いる ID/パスワードは厳重に管理すると共に定期的な変更を必須とする。 ・ AWS インフラストラクチャーやデータへアクセスする場合、なりすまし防止のために二要素認証を用いる。
2.2	サーバーラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	✔		回避	▼AWS インフラストラクチャー AWS 責任共有モデルに則り、AWS が責任をもって実施する事項。
		✔	✔	低減	▼端末、媒体 本運用管理規程で定める機器や媒体の紛失・盗難対策に準ずる。
2.3①	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	✔		回避	▼AWS インフラストラクチャー AWS 責任共有モデルに則り、AWS が責任をもって実施する事項。
2.3②	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	✔		回避	▼AWS インフラストラクチャー AWS 責任共有モデルに則り、AWS が責任をもって実施する事項。
		✔		低減	▼自社設備 ヘルプデスクの管理責任者により、事務室の設備と入退室管理を定めそれを徹底すると共に、定期的監査を実施する。

安全管理対策別リスクシナリオ		事業者	利用者	対応	内容
2.4	物理的安全対策が手薄となったバックアップ施設へ侵入される。	✔		回避	▼AWS インフラストラクチャー AWS 責任共有モデルに則り、AWS が責任をもって実施する事項。
		✔	✔	低減	▼自社設備 ヘルプデスクの管理責任者により、事務室の設備と入退室管理を定めそれを徹底すると共に、定期的監査を実施する。
2.5	医療情報の窃取・破壊・改ざんを目的とした機器や媒体、機具等の持ち込みが生じる。	✔		回避	▼AWS インフラストラクチャー AWS 責任共有モデルに則り、AWS が責任をもって実施する事項。
		✔	✔	低減	▼自設備 個人情報は、本サービスにアクセス可能な PC や可搬媒体及び紙媒体へ格納することを禁止する。
2.6	個人情報が存在する PC 等の重要な機器が盗難される。	✔	✔	低減	▼自設備 個人情報は、本サービスにアクセス可能な PC へ格納することを禁止する。
2.7	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	✔	✔	低減	▼自設備 個人情報を閲覧・表示できる端末には、覗き見防止フィルターを装着することを徹底する。
2.8	地震、水害、落雷、火災等並びにそれに伴う停電等により、医療情報システムが停止若しくは不具合が生じる。	✔		回避	▼AWS インフラストラクチャー AWS 責任共有モデルに則り、AWS が責任をもって実施する事項
技術的リスクシナリオ					
3.1①	正当な利用者以外により、医療情報システム上の情報が閲覧・操作される。	✔		低減	▼脆弱性対策 ・ Amazon GuardDuty により不正な動作(脅威)を検出する。
		✔		低減	▼データ保護 ・ データを格納するストレージは、基本的に AWS KMS を利用して暗号化する。 ・ AWS KMS をサポートしていない AWS サービスはデフォルト暗号化機能を利用する。 ・ データを格納するストレージや DB(Amazon RDS)に対して、アクセスできるユーザやグループをバケットポリシーやセキュリティグループ等を利用して、制限する。
		✔		低減	▼アクセス制御 ・ AWS 内のサーバーへアクセスするルートは、IPsec-VPN 経由とする。
		✔	✔	低減	▼AWS 以外 ・ Web ページへアクセスする際、個人ユーザ毎の ID とパスワードを使う。 （可能であれば、二要素認証を設定することが望ましい。）
		✔		低減	▼調査 ・ 不正や脅威が検出された、もしくは疑われる場合に、Amazon CloudWatch Logs 上のアクセスログなどを参照し、アタック箇所を分析する。
3.1②	利用者の認証に用いる物理的な媒体・身体情報等が欠損した場合、情報システムが利用できない。			—	—
3.1③	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	✔	✔	低減	▼アプリケーション セッションタイムアウトを短めに設定し、離席時に他の人が画面操作できない状態とする。
3.1④	パスワードが窃取若しくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	✔		低減	▼AWS インフラストラクチャー インターネット経由で AWS 内へアクセスする場合には、IAM ユーザの二要素認証を求める設定とする。
			✔	低減	▼アプリケーション Web 画面へのログオン時に、二要素認証を設定する。

安全管理対策別リスクシナリオ		事業者	利用者	対応	内容
					若しくは、フェデレーション認証を行い、Web 画面へアクセスする際、都度パスワードを入力させない。 (※Amazon Cognito を利用することで、外部 ID プロバイダ(Facebook など)とフェデレーション認証可能)
3.1⑤	単一の要素による認証情報が窃取若しくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	✔	✔	低減	単一要素の認証は避ける。
3.2①	一般利用者の権限が高いため、任意のソフトウェアのインストール、持込機器接続、持ち込み Wi-Fi の接続等をされ、不正アクセスを誘発する。	✔		低減	一般利用者の遵守事項・禁止事項を明示し、免責条項とする。
3.2②	情報の区分によらない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	✔		低減	情報の重要度に応じて区分し、アクセス権限を明確に分離する。
3.3①	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	✔		低減	▼AWS インフラストラクチャー ・ AWS CloudTrail により監査ログを取得し、Amazon S3 及び Amazon S3 Glacier へ長期保存する。 (AWS 上で発行された API はすべて監査ログが取得される)
					・ Amazon GuardDuty により不正なアクセスを検知する。
		✔		低減	▼サーバーOS(Amazon EC2) 監査ログ機能を有効化する。
		✔		低減	▼DB Amazon RDS の監査ログを有効化する。
		✔		低減	▼アプリケーション アクセス履歴、操作履歴をログとして保存する。
3.3②	特権 ID が不正利用若しくは乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	✔		低減	▼AWS インフラストラクチャー/アプリケーション ・ 特権 ID は使用しない取り決めとする。
					・ 特権 ID を使用せざるを得ない場合には、二要素認証の設定を行うことを必須とする。
					・ 特権 ID での直接ログオンは禁止とし、個人毎に割り当てられた低権限のユーザでログオン後、作業の内容に応じて、特権 ID 等へスイッチする運用・環境とする。
3.3③	パスワードやパスワードファイルが漏えいした場合に、不正利用される。	✔		低減	▼AWS インフラストラクチャー ・ インターネット経由で AWS 内へアクセスする場合には、IAM ユーザの二要素認証を求める設定とする。
					・ パスワードやパスワードファイル(pem ファイル)を管理する。 (認証パターン:①端末→AWS サーバー間、②AWS 内の AP サーバー→DB サーバーなど)
			✔	低減	▼アプリケーション Web 画面へのログオン時に、二要素認証を設定する。
3.4①	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	✔		低減	▼AWS インフラストラクチャー ・ Amazon GuardDuty により不正なアクセスを検知する。 検知した不正は、Amazon CloudWatch Events→Amazon SNS と連携し、運用者へメール通知する。
					・ ※監査ログの見読性を担保する。
			✔	低減	▼OS 以上(Amazon EC2) ホスト上に 振る舞い検知型のウイルス対策ソフトを導入し、不正行為の検出を行う。

安全管理対策別リスクシナリオ		事業者	利用者	対応	内容
3.4②	内部不正やサイバー攻撃による不正アクセスなどでログが改ざん、消去される。	✔		低減	▼AWS インフラストラクチャー ・ AWS CloudTrail で取得した監査ログについては、AWS CloudTrail が持つ検証機能により不正検知する。 ・ AWS CloudTrail が取得した監査ログへの更新権限は、AWS CloudTrail のみに与える。 （他ユーザは監査ログに対し参照のみ可能とする） ・ 監査ログの取得先である Amazon S3 バケットに関して、AWS KMS により暗号化する。 ・ 監査ログの取得先である Amazon S3 バケットは、Amazon S3 のバージョニング機能により履歴管理する。
		✔		低減	▼OS 以上(Amazon EC2) ・ OS が利用するストレージは、AWS 側で AWS KMS により暗号化する。 ・ 監査ログに対し、ユーザには書き込み権限を与えない。 ・ 監査ログについては、Amazon S3 へも退避する。 ・ 退避先のアクセスログ格納 Amazon S3 バケットに対して、ユーザへの書き込み権限を与えない。
		✔		低減	▼DB ・ DB が利用するストレージは、AWS 側で AWS KMS により暗号化する。 ・ 監査ログについては、Amazon S3 へも退避する。 ・ 退避先のアクセスログ格納 Amazon S3 バケットに対して、ユーザへの書き込み権限を与えない。
3.4③	機器が時刻同期しておらず、診療記録等に不整合が生じ、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	✔		低減	▼AWS インフラストラクチャー ・ Amazon EC2 の時刻同期を行うため、Amazon Time Sync Service を利用する。 ※Amazon EC2 側で本設定を行うことで、OS 以上のレイヤで時刻同期設定は不要となる。 ・ AWS のマネージドサービスについては、AWS 側で時刻同期されている。
3.4④	リモートメンテナンスに用いる ID やパスワード等の認証情報の不適切な管理により医療情報システムへの不正な侵入が生じ、ログから被害が特定できない。	✔		低減	ID やパスワードを不正入手された場合も、不正操作できない方式をとる。 また、万が一、不正アクセスされた場合に、ログから調査できるように監査ログを取得する。
3.4⑤	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	✔		低減	監査ログについては、安価かつ耐久度が高く、長期保存が可能な Amazon S3 及び Amazon S3 Glacier に保存する。 また、下記 2 点の対策をしておくことで、監査ログの消失や書き換えを防止する。 ・ Amazon S3 上の監査ログに対して、書き込み権限を有する AWS サービスを限定する。 （IAM ユーザには書き込み権限は与えない） ・ Amazon S3 のバージョニング機能を用いることで、万が一、監査ログが書き換えられた場合も、変更前の監査ログを保持できるようにしておく。
3.5	不正プログラムの実行により、端末・サーバー内の情報の漏えい・改ざん・破壊のほか、資源の不正使用が行われる。	✔		低減	▼AWS 内のサーバー 不正プログラムを検知する仕組みを導入する。
		✔		低減	▼AWS 外(保守拠点など) ・ホスト上に Trend Micro Deep Security などの対策ソフトを導入し、不正行為の検出を行う。
3.6	端末やサーバーで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	✔		低減	▼AWS 内のサーバー ・ サーバー上で利用しないサービスは、[手動起動]設定としておく。
		✔	✔	低減	▼AWS 外(サービスの利用者・保守拠点など) ・ 仮想 PC を利用し、利用者のポリシーで、仮想 PC へ不正なアプリケーションをインストールさせず、不要なサービスは停止させておく。

安全管理対策別リスクシナリオ		事業者	利用者	対応	内容
3.7①	VPN ルータ等のネットワーク機器の脆弱性から医療情報システムへ不正アクセスが発生し、医療情報システムの停止や情報の窃取・漏えいが生じる。	✔		低減	・ ネットワーク機器のパッチ等を月 1 回確認し、脆弱性がある場合には、パッチ適用する。 ・ 万が一、ネットワーク機器が乗っ取られた場合も、AWS 内のサーバーへアクセスさせないために、サーバーアクセス時に必要となる pem ファイルを端末側に保存せず、サーバー側に保存しておくことでセキュリティを担保する。
3.7②	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システムに不具合が生じる。	✔		低減	・ AWS Trusted Advisor、 AWS Config を確認し、AWS 設定値の改善事項を確認し対策する。 ・ アプリケーションに対するペネトレーションテストを行い、対策する。 ・ 上記 2 点の対策に関しては、本番環境へ適用する前に、検証環境などを用いて検証し、本番システムに不具合が生じないことを確認するのが望ましい。
3.7③	医療情報システムに設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	✔		低減	脆弱性診断及び不正な振る舞いを検知する。 (ただし、Amazon Inspector による Amazon EC2 の脆弱性診断は行っていない)
3.7④	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	✔		低減	▼AWS ・脆弱性への防御として以下を機能実装する。 ・IPS/IDS(UTM など)を実装し、レイヤ 3/4 レベルの攻撃を防御する。シグネチャは定期更新する。
		✔		低減	▼サーバー(Amazon EC2) ・ウイルス対策ソフトウェアを実装し、リアルタイムスキャンを行う。また、パターン定義ファイルは常に最新化する。
		✔	✔	低減	▼端末 ・ウイルス対策ソフトウェアを実装し、リアルタイムスキャンを行う。また、パターン定義ファイルは常に最新化する。
3.7⑤	IoT 機器について製造販売業者が想定していない利用方法により、脆弱性が生じる。			—	—
3.8①	TCP/UDP ポートにより、ネットワークを経由した攻撃を受ける。	✔		低減	・ IPS/IDS(UTM など)を実装し、レイヤ 3/4 レベルの攻撃から防御する。
3.8②	不正なアクセス元若しくはアクセス先における通信の盗聴・なりすましが行われる。	✔		低減	▼AWS マネジメントコンソールへの接続 ・ HTTPS 通信は TLS1.2 以上を用いる。(Web クライアント側で TLS1.2 以上に制限した通信設定が必要)
		✔		低減	・ MFA デバイスを利用した二要素認証を実装し、アクセス元制限を行う。 ▼Web アプリへの接続 ・閉域網については予め許可されたサイトからのみ接続し、すべてのアクセスは有人の監視施設を経由している。 ・インターネットからの接続については、TLS1.2 以上＋電子証明書により通信を行っている。 ・すべてのシステムは統合認証を使用した、二要素認証を行う。
		✔		低減	▼サーバー(Amazon EC2)への接続 ・IPsec-VPN による接続に限定する。
3.8③	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	✔	✔	低減	・ 本システムにアクセス可能な端末は限定し、アクセスの認証・認可を徹底する。 ・ アクセスの認証・認可には、二要素認証を用いることで未許可の端末による物理的ネットワーク接続の際もアクセスが拒否される仕組みとする、
3.8④	無線 LAN 利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。		✔	低減	・ 公共のオープンな環境における無線 LAN の使用を禁止する。 ・ 無線 LAN のセキュリティプロトコルを高いものとする。 ・ 無線 LAN への接続者を限定する
3.9	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	✔		低減	▼AWS 脆弱性対策により DDoS やアプリケーション脆弱性攻撃へ対応する。 (ただし、AWS WAF、AWS Shied による脆弱性診断は行っていない)

安全管理対策別リスクシナリオ		事業者	利用者	対応	内容
		✔		低減	▼サーバーOS(Amazon EC2) ウイルス対策ソフトウェアを実装し、リアルタイムスキャンによるウイルス対策を行う。
		✔	✔	低減	▼端末 ウイルス対策ソフトウェアを実装し、リアルタイムスキャンによるウイルス対策を行う。
3.10①	紛失・盗難した機器が起動され、機器を不正に利用される。	✔	✔	低減	・ 機器には個人情報を保存することを禁止する。 ・ 本システムへのアクセスには二要素認証を必須とし、機器が紛失・盗難した場合でもアクセスできない仕組みとする。
3.10②	紛失・盗難した機器や媒体内に保存された情報の漏えいや改ざんが生じる。	✔	✔	低減	本サービスでは、システム管理者が特に許可した場合を除き、本システムにアクセス可能な端末内やCD、USBメモリ、磁気テープ等可搬型記録媒体への個人情報の保存・複写を禁止する。
3.11①	セキュリティレベルの低い個人所有のモバイル端末(ノートパソコン、スマートフォン、タブレット)に格納した情報の窃取・漏えいが生じる。	✔	✔	低減	サービスの利用者による自己の情報へのアクセスにおいては、ID/パスワードによる認証を必須とする。 サービスの利用者により自己の情報の端末存禁止を求め、違反した場合の情報窃取や漏えいは本サービスの免責事項とする。
3.11②	外部から医療情報システムを利用した際、端末内に保存された情報の窃取・漏えいが生じる。	✔	✔	低減	本サービスでは、システム管理者が特に許可した場合を除き、本システムにアクセス可能な端末内への個人情報の保存を禁止する。
3.12	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	✔	✔	低減	本サービスでは、システム管理者が特に許可した場合を除き、CD、USBメモリ、磁気テープ等可搬型記録媒体への個人情報の保存を禁止する。
3.13①	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読若しくは偽装される。	✔		低減	▼AWS マネジメントコンソールへの接続 ・ HTTPS 通信は TLS1.2 以上を用いる。(Web クライアント側で TLS1.2 以上に制限した通信設定が必要) ・ MFA デバイスを利用した二要素認証を実装し、アクセス元制限を行う。
		✔		低減	▼Web アプリへの接続 ・閉域網については予め許可されたサイトからのみ接続し、すべてのアクセスは有人の監視施設を経由している。 ・インターネットからの接続については、TLS1.2 以上＋電子証明書により通信を行っている。 ・すべてのシステムは統合認証を使用した、二要素認証を行う。
		✔		低減	▼サーバー(Amazon EC2)への接続 ・IPsec-VPN による接続に限定する。
3.13②	暗号アルゴリズムの危殆化や暗号鍵の漏えい時に、暗号化・電子署名について解読若しくは偽装される。	✔		低減	▼AWS ・Amazon EBS、Amazon RDS、Amazon S3、Amazon CloudWatch Logs、は、AWS KMS が発行した暗号鍵により、暗号化する。暗号化強度は AES256 を利用し、1 年に 1 回自動更新させる。 また、KMS ポリシーと IAM ポリシーにより鍵の更新、鍵を用いた暗号化/復号化できる IAM ユーザの権限を必要最低限に制限する。
		✔		低減	▼アプリケーション ・Web アプリケーションによる通信は HTTPS 通信とする。HTTPS 通信に必要となるサーバー証明書は定期更新する。 ・AWS 以外で発行される電子署名を利用する場合には、信頼できる機関により発行されたものを利用する。
3.14	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	✔		低減	▼AWS ・Amazon GuardDuty を実装することで AWS 環境における不正な振る舞いを検知する。
		✔		低減	▼OS(サーバー) ・OS 上のログオン履歴を Amazon CloudWatch Logs へ連携し、Amazon CloudWatch Logs のログフィルターによりログオンを検知する。
		✔		低減	▼DB

安全管理対策別リスクシナリオ		事業者	利用者	対応	内容
					・Amazon RDS の監査ログを Amazon CloudWatch Logs へ連携し、Amazon CloudWatch Logs のログフィルターによりログオンを検知する。
		✔		低減	▼アプリケーション ・アプリケーションへのアクセスログを Amazon CloudWatch Logs へ連携し、Amazon CloudWatch Logs のログフィルターによりログオンを検知する。
3.15①	信頼できる第三者機関と同等の厳格さで本人確認や署名の検証が行われない。	✔		低減	▼アプリケーション ・サーバーに配置するサーバー証明書については作成した証明書を利用する。
3.15②	電子署名を行う機器等の時刻情報が改ざんされることで、電子署名付与時点の時刻及び当該時刻以降の改ざんの有無が証明できない。	✔		低減	▼アプリケーション ・サーバーに配置するサーバー証明書については作成した証明書を利用する。
3.15③	タイムスタンプ付与時点で電子署名を検証することができない。	✔		低減	▼アプリケーション ・サーバーに配置するサーバー証明書については作成した証明書を利用する。
3.16	ソフトウェアの改ざんにより、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	✔		低減	▼AWS ・AWS KMS により、データを暗号化し保存する。 ・AWS へアクセスするための IAM ユーザは二要素認証を設定する。 ・作業者毎に IAM ユーザを作成し、必要最低限の権限を付与する。 ・Amazon S3 バケットポリシーにより、Amazon S3 バケットへのアクセスを制限する。 ・AWS Config により設定変更履歴を取得し、不正な変更を検知できる仕組みを導入する。 ・Amazon GuardDuty により不正な動作(脅威)を検出する。 ・監査ログを取得する。
		✔		低減	▼OS(Amazon EC2) ・ウイルス対策ソフトウェアにより、ソフトウェアの改ざんを防止する。 ・作業者毎に OS ユーザを作成し、必要最低限の権限を付与する。 ・ディレクトリ/ファイルに対するアクセス権限を付与する。 ・監査ログを取得する。
		✔		低減	▼DB ・作業者毎に DB ユーザを作成し、必要最低限の権限を付与する。 ・監査ログを取得する。
		✔		低減	▼アプリケーション ・開発者毎にアプリ開発用ユーザを作成し、必要最低限の権限を付与する。 ・監査ログを取得する。
3.17	各種媒体に分散管理された患者(サービスの利用者)の情報の相互関係がすぐに明らかにできない。	✔	✔	低減	システムにアクセス可能な PC や可搬型媒体に個人情報を格納することを禁止する。
3.18	情報の表示や検索等の応答時間が長いことで医療情報システムの利用目的に支障が生じる。	✔		低減	▼AWS 外 ・既に構築されている監視システムがあれば、Web レスポンス監視を行う。
		✔		低減	▼AWS 内 ・Amazon CloudWatch を利用し、IaaS 系のサービスのパフォーマンス情報を取得しておき、「Web 画面のレスポンス監視で応答劣化を検知」した場合に、問題箇所を特定できるようにする。取得する情報は以下とする。 ・Amazon EC2:CPU 使用率、メモリ使用率、ストレージ容量、ステータス監視(データセンター施設の障害によるもの(物理層:OSI 参照モデルのレイヤ 1)や OS レイヤによる障害(ネットワーク層:OSI 参照モデルのレイヤ 2)を指す) ・Amazon EBS:IOPS(Read/Write)

安全管理対策別リスクシナリオ		事業者	利用者	対応	内容
					・Amazon RDS:メモリ容量、ストレージ容量 上記アラート通知を受け、リソースの増強が必要と判断した場合、Amazon EC2 及び Amazon RDS のインスタンスタイプの変更(スケールアップ)でリソース増強を行い、性能改善する。
3.19①	医療情報システムの単一障害点の障害により、情報システム・サービスが停止する。	✔		保有	単一 AZ の障害時には、システムは停止する。 AWS サービスは AWS 側にて可用性が確保される。システム提供に影響がある主な AWS サービスは以下の通り。 可用性は AWS の SLA 参照 ・ Amazon EC2 ・ Amazon RDS ・ Amazon EBS
3.19②	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じる。	✔		低減	ディスクの劣化や故障への対応は AWS 側で行われる。 AWS で利用するストレージ(Amazon EBS、Amazon S3、Amazon RDS)の可用性は AWS の SLA による。
3.20	医療情報システム障害時に医療情報システム内に保存された医療情報が一切閲覧できない。	✔		低減	システムの可用性は代替機を有すことと同等のサービスを使用し、閲覧できない時間を短くする。
3.21①	情報が毀損や滅失した場合にバックアップされたデータを用いて元の状態に復元できない。	✔		低減	▼AWS ・ Amazon EC2 は、変更時に AMI バックアップを 取得し、Amazon S3 へ保存する。 ・ Amazon RDS は、1 日に 1 回スナップショットを自動で Amazon S3 に取得する。 ・ Amazon S3 上のデータ/ログは、Amazon S3 のバージョニング機能にてバックアップを取得する。
		✔		低減	▼OS(サーバー上) ・ Amazon EC2 の AMI バックアップはオンラインバックアップとなるため、OS レイヤ以上の整合性についてはデータやアプリのバックアップで対応する。
		✔		低減	▼アプリケーション ・ ライブラリ管理ツール(SVN や Git など)上にあるアプリケーションのコードファイルを定期的にバックアップしておく。
		✔		低減	・ 環境構築用の作業ファイルを AWS 外に確保し可用性を担保する。 ▼DB ・ 原本は別システムに存在している。原本データから再構成された利活用システム向けデータ全体が毎週連携される。
3.21②	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	✔		低減	各種バックアップを Amazon S3 へ取得する。 Amazon S3 を実現するハードウェアは、AWS 側で劣化対応が行われる。 また、Amazon S3 は容量の制限なく、オブジェクトを格納できる。
3.22	医療情報システムを更改等により移行する際、移行元で記録された情報が移行後に正しく読みだせない。	✔		低減	・ AWS→他クラウド AWS 上に保存したデータを他クラウドへ移行する場合には、移行後のクラウドで提供されているデータ転送サービス等を利用する。なお、AWS のどのサービスにデータが保管されているかで、移行方法が提供されていないケースもあるため、他クラウドへ移行する場合には、事前にデータ転送の仕様を確認の上、移行先を決定する必要がある。

安全管理対策別リスクシナリオ	事業者	利用者	対応	内容
				・ AWS→オンプレミス Amazon RDS 上のデータは、DB の機能で論理的に Export し、オンプレ環境へデータ移行する。 Amazon S3 上のデータを AWS CLI/SDK にてコピーし、オンプレミス環境へデータ移行する。