「クラウドサービス」

サービス仕様適合開示書

第7.1版　2026年04月20日

MDV
medical.data.vision
メディカル・データ・ビジョン株式会社

目次

本書の目的と位置づけ

- 本サービス仕様適合開示書(以下、本書という)は、本システムが「医療情報システムの安全管理に関するガイドライン」（厚生労働省）が求める安全管理基準に適合していることを示した文書です。
- 本書は、「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」（総務省・経済産業省）で定められた内容のうち、「医療機関等へ情報提供すべき項目」を基に構成しております。

定義

- 本書に定めのない用語の定義は、「クラウドサービス使用許諾基本約款」の定めに従うものとします。
- 本書で使用する主な用語の定義は以下の通りです。
    - 「本システム」とは、当社が本サービスを提供するために使用するプラットフォーム「MDV-AP」、ならびに同プラットフォーム上で動作する個別クラウドサービス、およびこれらを構成するサーバー、ネットワーク、ソフトウェアを含む情報システム全体の総称をいいます。

Ⅰ．医療機関等が医療情報安全管理ガイドラインに基づき、外部保存を受託する事業者の選定にあたり最低限確認する必要がある内容

1. 保存された情報を格納する情報機器等の国内法の適用状況

- 当社で医療情報を保存する情報機器はクラウドサービスも含め日本国法が適用されます。

2. 医療情報等の安全管理に係る基本方針・取扱規程等の整備状況

- 情報セキュリティ基本方針　（https://www.mdv.co.jp/security.html）
- 個人情報保護方針　（https://www.mdv.co.jp/privacy_policy.html）
- 上記方針に基づき、ISO/IEC 27001に適合した情報並びに情報システム管理の規程を整備し、運用しております。

※ 方針以外の規程は社外秘情報のため、公表しておりません。規定内容に関しては、個別にお問合せください。

3. 不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況

- お客様よりご提供頂いたデータは、当社契約のクラウドへシステムで保管および日次でのバックアップを行い、10日間の保持および月次バックアップを行っております。なお、お客様からのバックアップデータによる復元の要望は承っておりません。

4. 医療情報等の安全管理に係る実施体制の整備状況

- 管理責任者　：　企画担当部門　本部長
- システム管理者　：　開発担当部門　部門長
- 運用管理責任者　：　企画担当部門　部門長
- 個人情報保護責任者　：　リスク管理担当部門　部門長

5. 実績等に基づく個人データ安全管理に関する信用度

- 当社では、これまで、個人情報の流出事故は発生しておらず、また、受託情報の目的外利用・不当利用等は行っておりません。

6. 財務諸表等に基づく経営の健全性

- 当社の財務諸表等は、以下のURLで公表しております。

https://www.mdv.co.jp/ir/library/

Ⅰ．医療機関等が医療情報安全管理ガイドラインに基づき、外部保存を受託する事業者の選定にあたり最低限確認する必要がある内容

7. プライバシーマーク認定又はISMS 認証の取得状況

- 当社は、本サービスの開発・運用管理を含む登録範囲について、ISMS(ISO/IEC 27001および、ISO/IEC 27017)認証を受けており、年1回、審査登録機関により評価されております。
- 規格/登録証番号： ISO/IEC 27001　JQA-IM1003
- 規格/登録証番号： ISO/IEC 27017　JQA-IC0161
  （登録範囲）　：病院経営改善アプリケーション「MDV Act」の提供
  　　：および「MDV Act」運用基盤としてのAWSの利用
- 審査登録機関　：一般財団法人　日本品質保証機構
- 有効期限　：2029年1月24日

※ 登録内容は、審査登録機関のWebサイトで公開されております。
https://www.jqa.jp/cgi-bin/06manage/14_touroku/search_j.html

※ ISO/IEC 27017の内部監査記録は以下よりご確認いただけます。
https://portal-ap.mdv.co.jp/wp-content/uploads/2026/02/Internal_Audit_MDV_AP.pdf

8. 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示すいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無

- 当社では情報セキュリティに係る公的な第三者認証としてISMS 認証を取得しており、外部保存に求められる技術及び管理能力を有しております。

9. 医療情報を保存する情報機器が設置されている場所(地域、国)

- 当社で医療情報を取り扱う情報機器はクラウドサービスも含め日本国内に設置されております。

10. 受託事業者に対する国外法の適用可能性

- 本サービスにおいて国外法は適用されません。

Ⅱ．医療機関等との共通理解を形成するために情報提供すべき内容

1．医療機関等の運用管理規程に定める必要がある事項

次の事項に関しては、本サービスを利用する医療機関様にて、管理規程を定めてください。

- 本サービスを利用する場所に関する事項（作業場所の特定、作業場所のアクセス制限など）
- 本サービスを利用する端末のセキュリティ管理に関する事項（アカウントの登録並びにパスワード管理、OS等のセキュリティアップデート並びにコンピュータウイルス対策など）
- 本サービスを利用するアカウントの管理に関する事項（アカウント登録・削除、アカウント管理など）
- 本サービスを利用して得られた情報の管理に関する事項（ダウンロードデータの保管・院外持出制限など）

2．医療情報システムの安全管理に係る点検や評価の結果

- 診断ツール　：　Rapid7 InsightAppSec：動的アプリケーションセキュリティ テスト
- 診断実施年月　：　2026年3月
- 診断対象　：　Webアプリケーション
- 診断結果　：　脆弱性診断ツールより重大な脆弱性が検出されましたが、
  検証の結果、必要な対策は実施済みであり影響がほとんどない低リスクな脆弱性と判断しています。

【補足】

- リスクレベル「低」の脆弱性について

  該当脆弱性単独では重大な問題に繋がる可能性が極めて低く、
  攻撃が成功するためには非現実的な条件がいくつも必要になるような、危険性が限定的な脆弱性を指します。

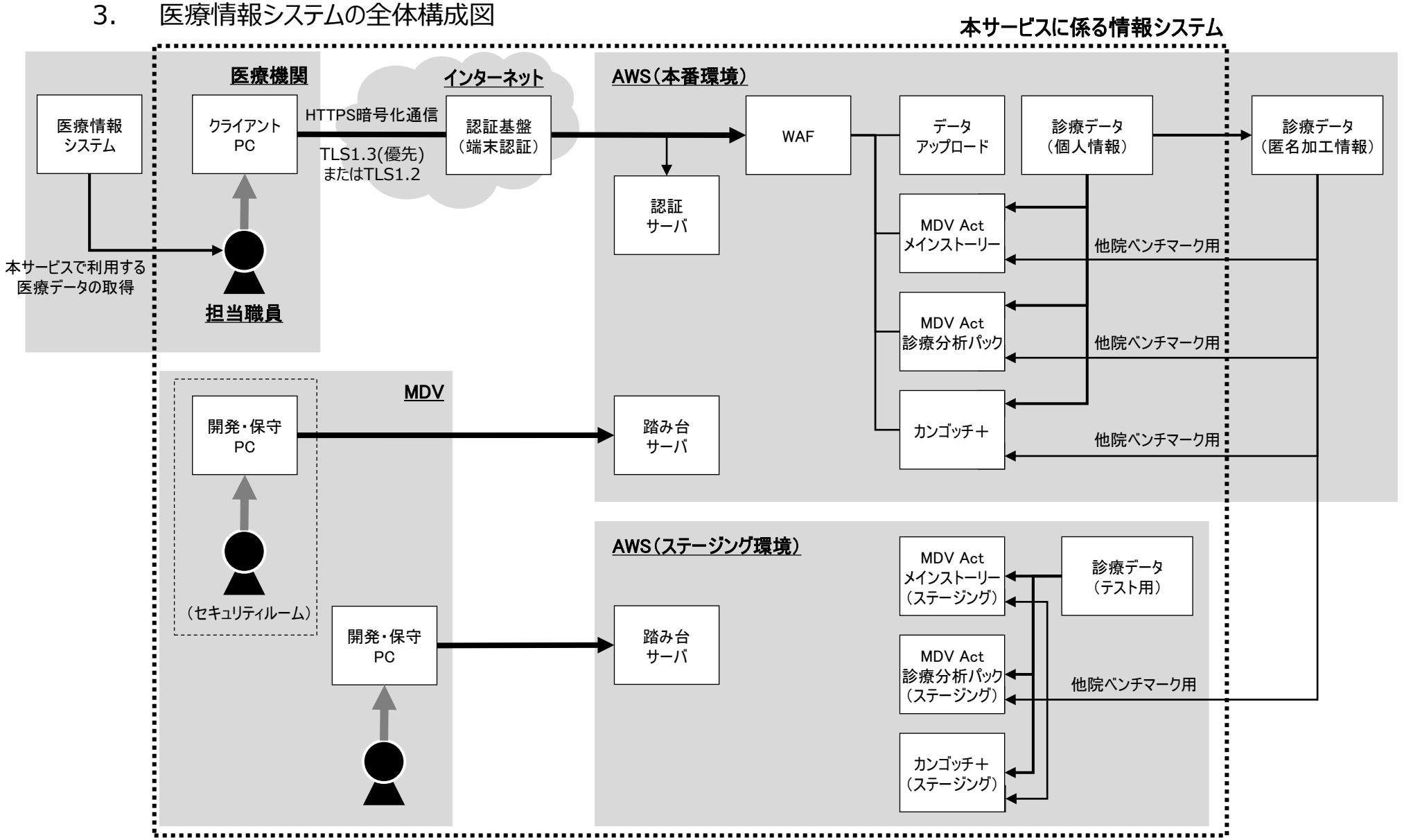
- 未対応の脆弱性によるリスクについて

  検出された脆弱性の一部は、対応することにより通信速度が著しく低下するため、お客様業務への影響を考え対応を見送っております。
  この点は別途セキュリティ対策を実施しているため、リスクが顕在化する（攻撃が成立する）可能性は極めて低いと判断されます。

  なお、本システムは日次で脆弱性情報の収集を行っており、深刻度の高いものは月次で対応を行っています。
  セキュリティパッチの適用は、テスト環境で問題ないことを確認のうえ適用いたします。

Ⅱ． 医療機関等との共通理解を形成するために情報提供すべき内容

3.　医療情報システムの全体構成図



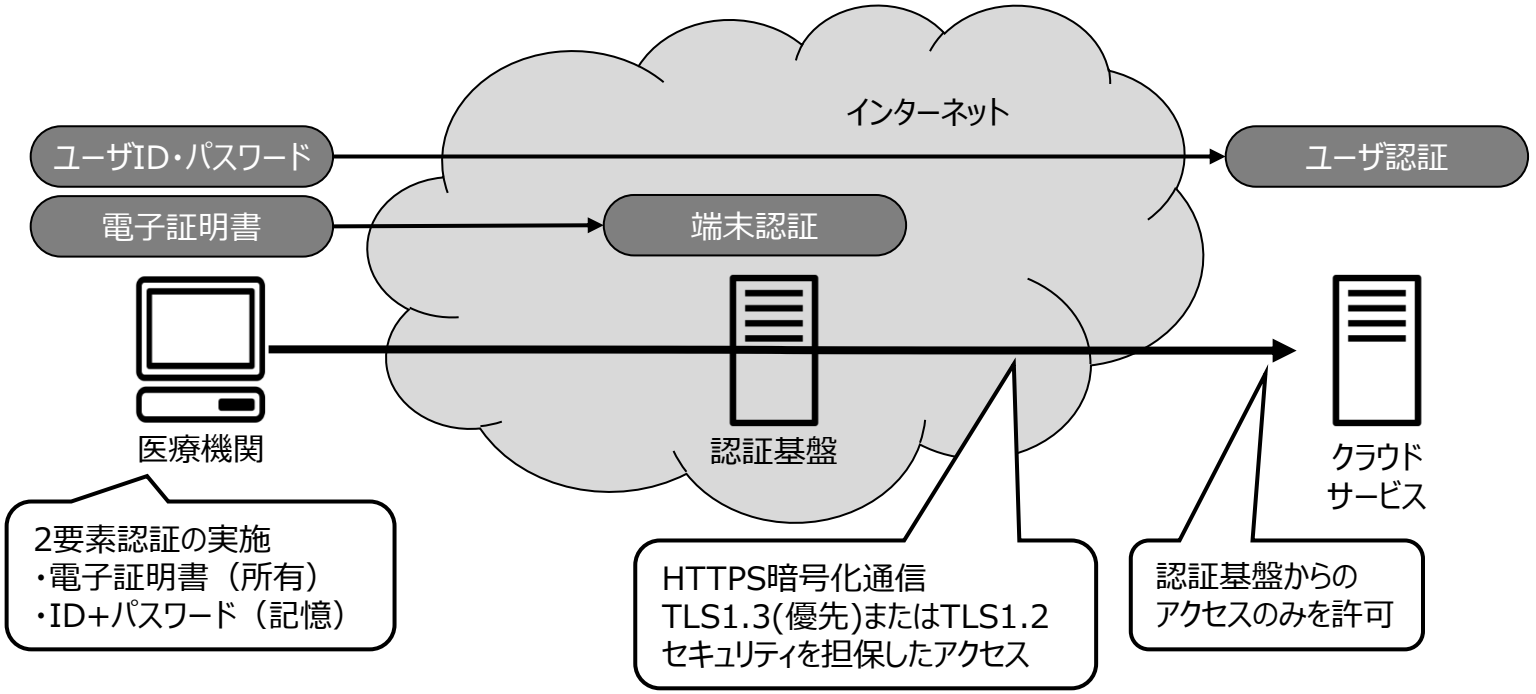
Ⅱ． 医療機関等との共通理解を形成するために情報提供すべき内容

4. リスク対応

◘ 端末（医療機関） – クラウド環境間のネットワーク接続について

【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 13 遵守事項⑥】
（略）HTTPSを利用する場合、TLSのプロトコルバージョンをTLS1.3以上に限定した上で、クライアント証明書を利用したTLSクライアント認証を実施すること。（略）また、ソフトウェア型の IPsec 又は TLS1.2 以上により接続する場合、**セッション間の回り込み**（正規のルートではないクローズドセッションへのアクセス）等による攻撃への適切な対策を実施すること。

本サービスでは、下図の構成とすることで、「セッション間の回り込み」への対策を実施しており、「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」を遵守しております。



Ⅱ．医療機関等との共通理解を形成するために情報提供すべき内容

4.　リスク対応

◘ 本サービスで扱う医療データ、並びに、本サービスの安全管理に関する医療機関と当社の責任範囲について

<table>
<tr><th></th><th>医療機関
（端末・院内ネットワーク等）</th><th>医療機関－AWS①
（ネットワーク接続）</th><th>AWS①
（医療機関専用領域）</th><th>AWS②
（当社データ処理領域）</th></tr>
<tr><td>本システムで扱う
医療データの
管理責任</td><td colspan="3">【医療機関】

医療データ（個人情報）漏えい時の責任
当社（システム事業者）に対する監督責任</td><td>【当社】

医療データ
（匿名加工情報）
漏えい時の責任</td></tr>
<tr><td>本システムの
安全管理責任</td><td>【医療機関】

<u>VPN接続に用いるID・パスワード・電子証明書は医療機関の責任で管理</u>して頂く必要がございます。</td><td colspan="2">【当社】

「医療情報システムの安全管理に関するガイドライン」
を遵守した対策を施すことの責任

具体的な対策内容は、次ページの通り、想定する脅威・リスクに応じて検討・実施しております。

★ただし、<u>本サービスを使用するID・パスワードは医療機関の責任で管理</u>して頂く必要がございます。</td><td>【当社】

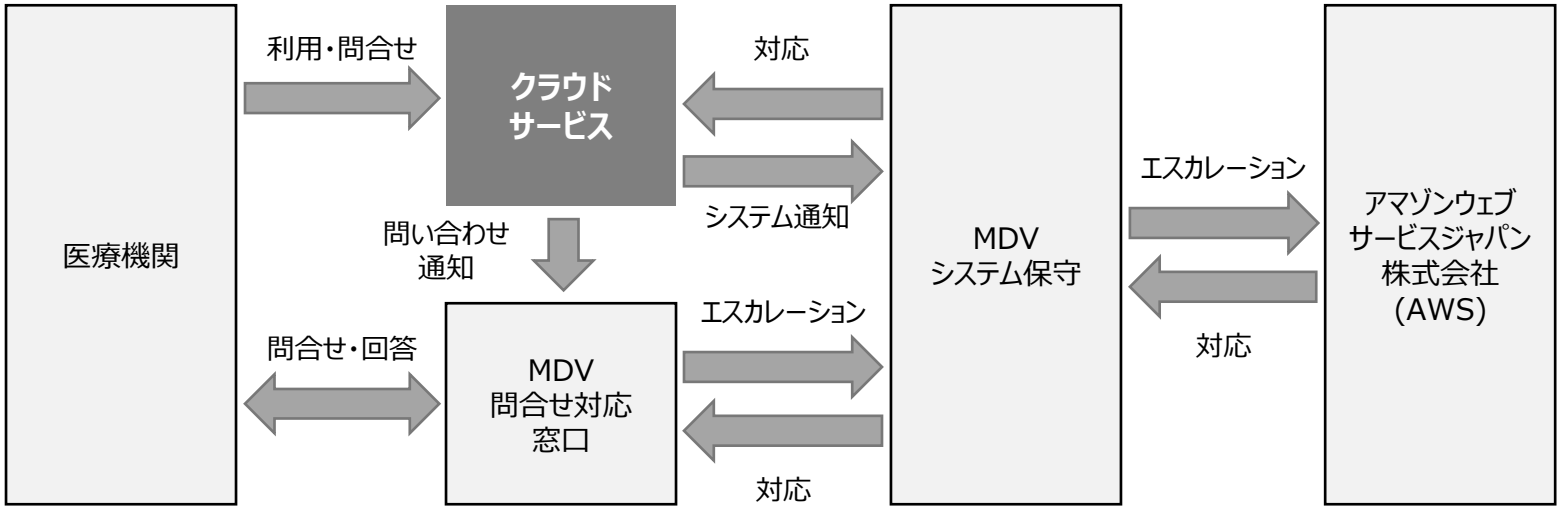
インフラ・アプリケーション・
サービス全般</td></tr>
</table>

Ⅱ．医療機関等との共通理解を形成するために情報提供すべき内容

5.　医療情報システムの安全管理に係る基本方針

※「Ⅰ-1．医療情報等の安全管理に係る基本方針・取扱規程等の整備状況」を参照ください。

6.　医療情報システムの提供に係る体制



※アマゾンウェブサービスジャパン株式会社：クラウド(AWS)のインフラ部分を管理

7.　契約書・マニュアル等の文書の管理方法

- 契約書・マニュアル等は、「文書管理規程」並びに「情報セキュリティ基準」に基づき管理いたします。
  ※ これらの規程は社外秘情報のため、公表しておりません。規定内容に関しては、個別にお問合せください。

8. 機器等を用いる場合の機器等の管理責任の所在・管理方法

- 機器等の管理は、「情報セキュリティ基準」に基づき管理いたします。

※ この規程は社外秘情報のため、公表しておりません。規定内容に関しては、個別にお問合せください。

9. リスク対応策の運用方法

- リスク対応策は、「情報セキュリティ基準」並びに「情報システム・セキュリティ基準」に基づき管理いたします。

※ これらの規程は社外秘情報のため、公表しておりません。規定内容に関しては、個別にお問合せください。

10. 事故発生時の体制および報告窓口

(1)監視

① クライアント認証基盤、ログイン認証サーバ、WAF、並びに、アプリケーションサーバにおいて認証状況並びに処理内容を監視しております。

② 認証状況並びに処理内容に異常を検知した場合は、監視サーバから保守要員に直ちに通知されます。

③ お客様が本システムを利用する際のログデータは、不正なアクセスや改ざんを防ぐため、当社の一部の特別な権限を持つ者しかアクセスできない、限られたアクセス権のもとで保管されます。

(2)事故対応フロー

① 異常を検知した場合、あるいは、医療機関様若しくは第三者からの通報により事故発生を検知した場合は、
当社内の「危機管理フロー」に従い、リスク管理担当部門並びに役員へ報告すると共に、大きな影響を受ける可能性のある医療機関様へは、事故検知後24時間以内に各担当営業を窓口としてご連絡いたします。

② 原因の究明、被害拡大の防止、その他お客様の情報の安全性の確保に必要な対応を行います。
なお、所管官庁その他関係機関への報告については、お客様管理者との協議により対応いたします。

(3)インシデント発生時の報告窓口

- 情報セキュリティインシデントに関する当社へのお問合せは、以下のURLよりサポート窓口へお問い合わせください。
https://support.mdv.co.jp

Ⅱ．医療機関等との共通理解を形成するために情報提供すべき内容

11. 医療情報を格納する記憶媒体等の管理方法

- 医療情報は、「Ⅱ-3.医療情報システムの全体構成図」中のAWS上のサーバに格納し、取外し可能な記憶媒体には保存いたしません。
- サーバのHDD交換時には、AWS内で論理的または磁気的に破壊した後に廃棄いたします。

※ AWSでの医療情報の取り扱いについては下記の「日本の医療情報ガイドライン」をご参照ください。

https://aws.amazon.com/jp/compliance/medical-information-guidelines/

12. 医療機関等の危機管理対応時の受託事業者における体制・対応内容

- 問い合わせ窓口にご連絡を頂き、本システム担当者にて対応を実施いたします。

13. 医療情報の外部保存に係る患者等への説明方法

- ① 本サービスの利用に係る患者様等への説明は、第一次的には各医療機関様において対応して頂くこととし、当社は、医療機関様からの要請に応じて、患者様等への説明に必要な資料等をご提供いたします。
- ② 医療機関様から患者様等へのご説明には、
  - ・医療機関様が本サービスを利用して患者様の医療データを分析すること
  - ・本サービスを利用して得た分析結果を、医療機関様が当該医療機関様以外の第三者にご提供すること

  を含みます。

14. 医療情報システムに対する監査の実施方法

- 本サービスの運用管理部門に対して、年１回、情報セキュリティ管理に関する内部監査を実施し、その結果は、代表取締役社長へ報告しております。（監査担当：内部監査室及びリスク管理担当部門）

※ 監査結果は社外秘情報のため、公表しておりません。結果概要に関しては、個別にお問合せください。

15. 医療機関等の管理者からの問い合わせ窓口

※「Ⅱ-6. 医療情報システムの提供に係る体制」、「Ⅱ-10. 事故発生時の体制および報告窓口」をご参照ください。

16. 制度上の要求事項への対応

① 医療分野の制度が求める安全管理の要求事項

- 個人情報の保護に関する法律、及び、同施行令並びに施行規則
- 個人情報の保護に関する法律についてのガイドライン（通則編、外国にある第三者への提供編、第三者提供時の確認・記録義務編、仮名加工情報・匿名加工情報編）
- 医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス
- 医療情報システムの安全管理に関するガイドライン（厚生労働省）
- 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における安全管理ガイドライン（総務省・経済産業省）

② 電子保存の要求事項

※ 本サービスでは、e-文書法の対象範囲となる医療関係文書は、取り扱っておりません。

③ 法令で定められた記名・押印を電子署名で行うことについて

※ 本サービスでは、法令で定められた記名・押印を電子署名で行う文書は、取り扱っておりません。

④ その他取扱いに注意を要する文書等の取扱い

※ 本サービスでは、②及び③の他、取扱いに注意を要する文書等は、取り扱っておりません。

⑤ 外部保存の要求事項

※ 医療情報の外部保存に関して、①に記載の要求事項に準拠しております。

Ⅲ．クラウドサービス使用許諾基本約款の補足事項

1．　個人情報の第三者提供に関する例外事項（基本約款第12条第2項）

- 当社は、法令に基づき、裁判所、行政機関、またはこれに準ずる権限を有する第三者から開示を求められた場合は、当人の同意なく必要最低限の情報を提供します。

2．　契約終了時のデータの削除（基本約款第19条第2項）

- 当社は、本データを契約終了日の翌日から起算して90日以内に当社のサーバーから削除するものとします。

Ⅲ．クラウドサービス使用許諾基本約款の補足事項

3. 外部クラウドサービスの利用

- 当社クラウドサービスのインフラストラクチャとして AWS（Amazon Web Services） を利用しています。
  サーバなどの装置は、Amazon Web Services, Inc. により適切に管理され、不要になった場合は、安全な方法で廃棄が行われています。

詳細は、以下よりご確認ください。
https://aws.amazon.com/jp/security

AWSはISO/IEC 27001をはじめとした複数の認証を受けています。
https://aws.amazon.com/jp/compliance/iso-certified/
https://aws.amazon.com/jp/compliance/soc-faqs/

4. データの機密保持

- お客様によりアップロードされたデータはクラウド上で暗号化(AES-256)され厳密に保管されます。
  当社はお客様の許可なくお客様がアップロードされた情報へアクセスすることはありません。

5. セキュリティに配慮した開発のための方針

- 当社の開発プロセスは、社内情報セキュリティ基準に準拠しています。
  設計からリリースに至るまで、各段階で情報セキュリティを確保するための管理策を組み込んでいます。

6. クロックの同期

- 本システム内で提供されるログは、タイムゾーン JST (UTC+9) で提供されます。
  ログの時刻は、Amazon Time Sync Service と同期しています。

7. 機能変更

- 本システムでメンテナンスが発生する場合、原則5営業日前までに告知いたします。
  (※ただし、サービス障害・サイバー攻撃等不測の事態にる緊急対応が必要な場合はこの限りではありません。)
  機能変更内容は「お知らせ」画面の「メンテナンス情報」より修正内容をご確認いただけます。

以上

改訂履歴

版数	発行日	改訂履歴
第1版	2021年1月1日	初版発行
第2版	2022年8月1日	社内の組織変更および医療情報システムの安全管理に関するガイドライン改定に伴う内容見直し
第3版	2023年8月1日	社内の組織変更およ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改定に伴う内容見直し
第4版	2024年2月26日	「II-4. リスク対応概要」に次の2項目に関する説明を追記 ・端末（医療機関）－クラウド環境間のネットワーク接続 ・本サービスで扱う医療データ、並びに、本サービスの安全管理に関する医療機関と当社の責任範囲
第5版	2024年5月24日	社内の組織変更に伴う見直し
第6版	2025年1月28日	端末（医療機関）－クラウド環境間の接続方式の変更に伴う内容見直し ・II-3. 医療情報システムの全体構成図 ・II-4. リスク対応
第7版	2025年10月16日	ISO/IEC:27017要求事項に合わせ内容を追記。一部文章を修正 ・本書の目的と位置づけを追加。 ・「Ⅲ. クラウドサービス使用許諾基本約款の補足事項」を追加
第7.1版	2026年4月20日	ISO/IEC 27017認証取得および脆弱性診断実施に合わせ修正 「I-7」にISO/IEC 27017の記述を追記、および有効期限の更新 「II-2」の脆弱性診断実施結果を追記

MDV

medical.data.vision

メディカル・データ・ビジョン株式会社

〒101-0053 東京都千代田区神田美土代町7番地 住友不動産神田ビル10階
TEL.03-5283-6911　FAX.03-5283-6811