「クラウドサービス」

サービス仕様適合開示書

第5版　2024年5月24日

メディカル・データ・ビジョン株式会社

RC-2024023

目次

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日または35日間の保持を行っております。

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　：　データネットワーク企画本部　本部長
- システム管理者　：　開発本部　プロダクト開発部門長
- 運用管理責任者　：　データネットワーク企画本部　販売企画部門長
- 個人情報保護責任者　：　管理本部　リスク・コンプライアンス部門長

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 認証を取得状況

- 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)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。
- 審査登録機関　：　一般財団法人　日本品質保証機構
- 登録証番号　：　JQA-IM1003
- 有効期限　：　2026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

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

- 当社で国外法が適用される事業はございません。

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

次の通り、脆弱性診断を専門の事業者へ委託して定期的に実施しております。

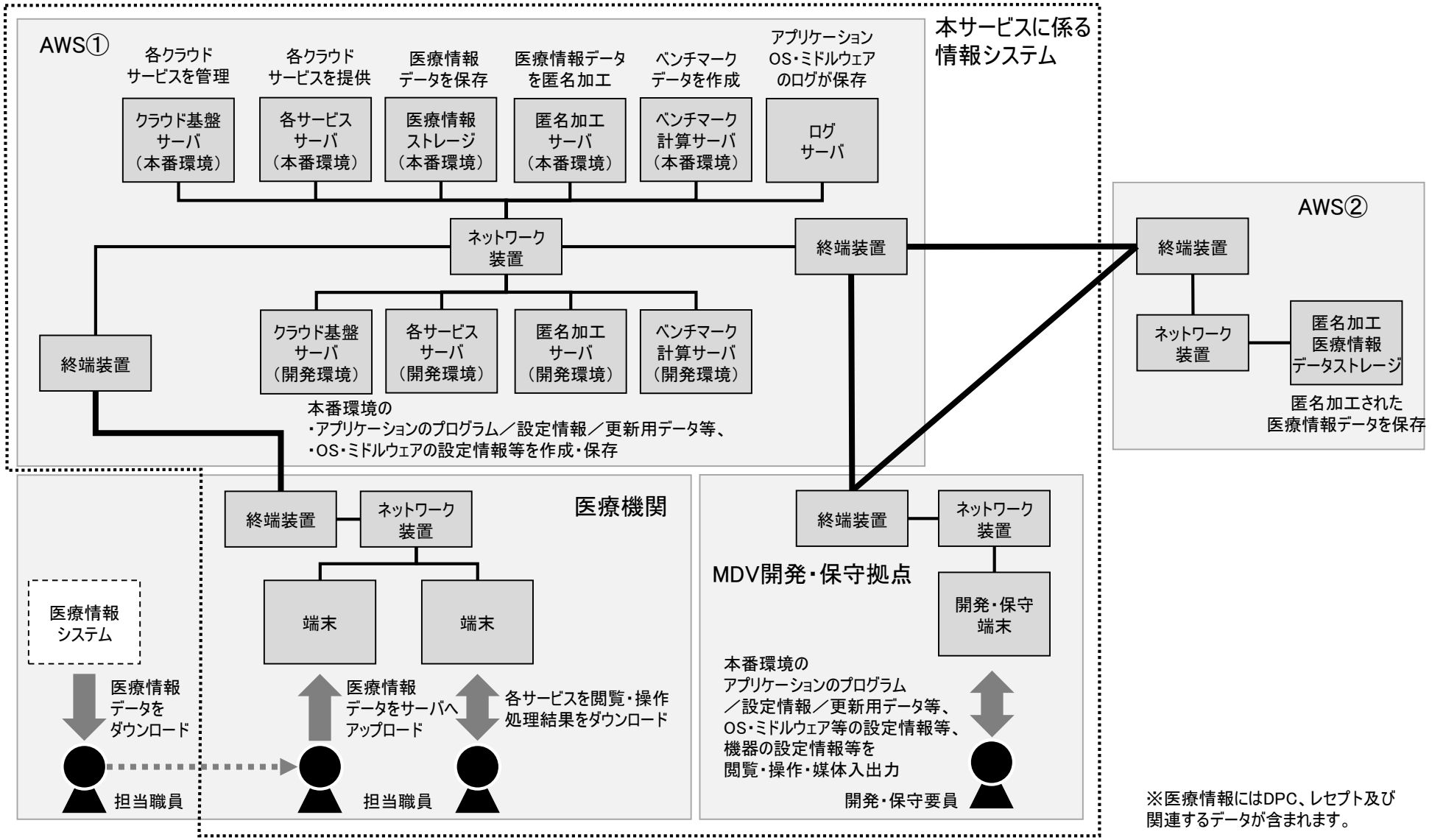
- 診断事業者　：　GMOサイバーセキュリティ byイエラエ株式会社
- 診断実施年月　：　2023年4月
- 診断対象　：　Webアプリケーション
- 診断結果　：　リスクレベル「低」の脆弱性が検出されましたが、一部を除き対応済みです。

【補足】

- リスクレベル「低」の脆弱性について
  ・その脆弱性の単独の悪用では重大事に至らないと考えられる、軽微なシステム情報の出力などで、現実的でない前提条件を要するなど、実際の攻撃が困難な脆弱性攻撃難易度が高く、現実的な時間内で攻撃を成立させることが困難な脆弱性です。
- 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、対応を見送っておりますが、診断対象外の対策により、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。

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



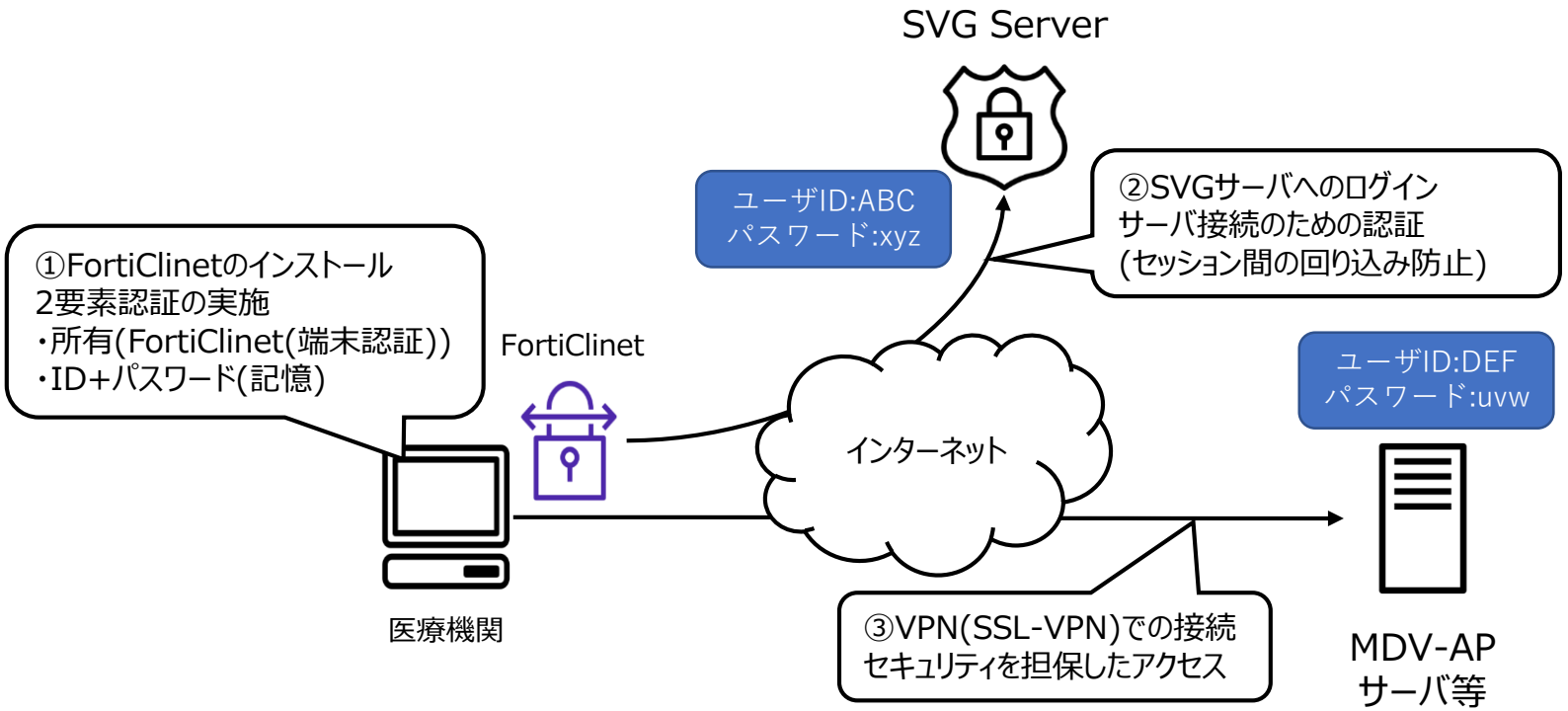
※医療情報にはDPC、レセプト及び関連するデータが含まれます。

4. リスク対応概要

■ 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）なお、SSL-VPN は利用する具体的な方法によっては**偽サーバへの対策が不十分**なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと。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、「偽サーバへの対策」並びに「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

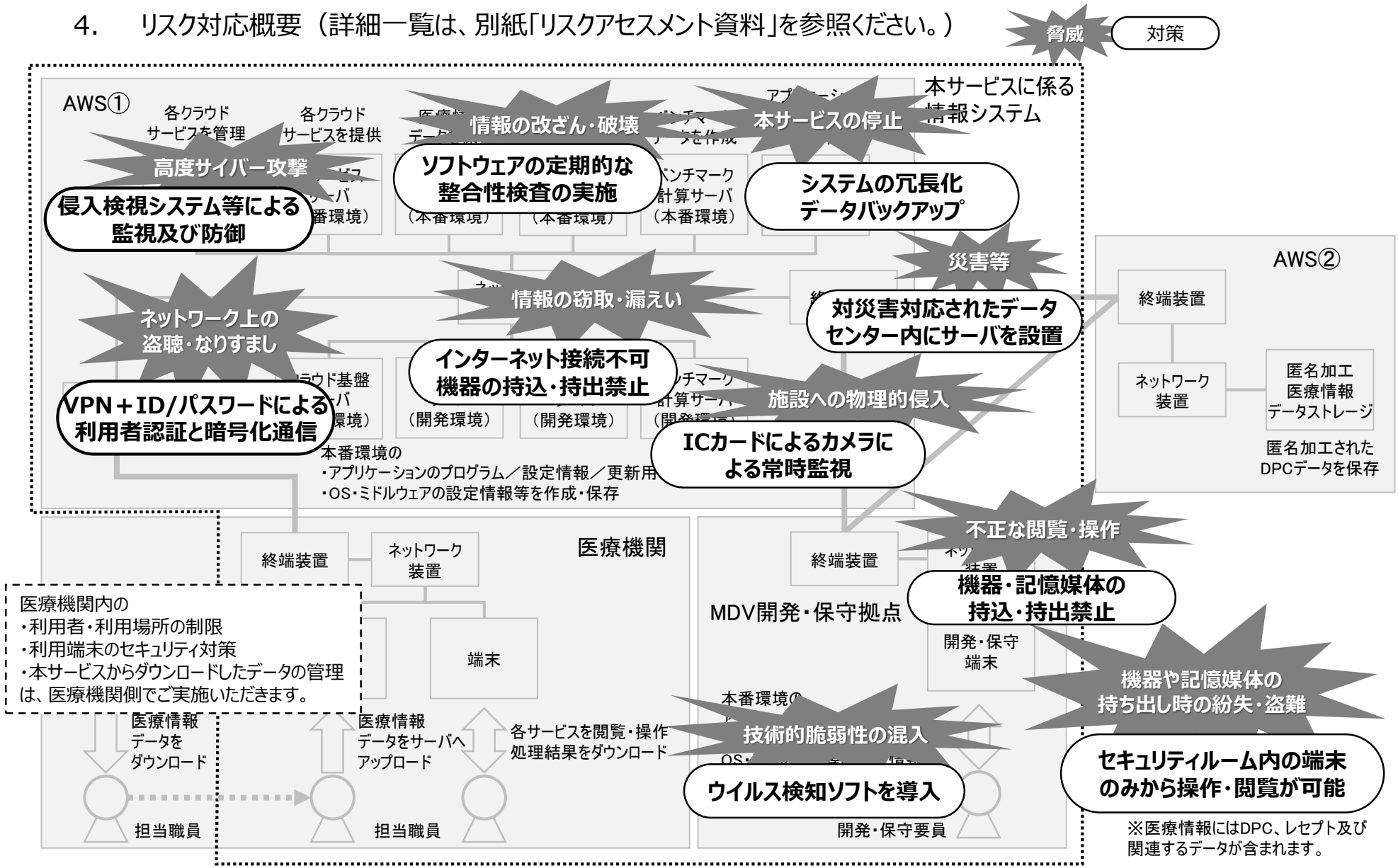
4.　リスク対応概要

◘ 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弊社の責任範囲について

	医療機関 （端末・院内ネットワーク等）	医療機関－AWS① （ネットワーク接続）	AWS① （医療機関専用領域）	AWS② （弊社データ処理領域）
本システムで扱う医療データの管理責任	【医療機関】 医療データ（個人情報）漏えい時の責任 弊社（システム事業者）に対する監督責任			【弊社】 医療データ （匿名加工情報） 漏えい時の責任
本システムの安全管理責任	【医療機関】 **VPN接続に用いるID・パスワード・証明書は医療機関の責任で管理**して頂く必要がございます。 ★ただし、端末用ソフトウェア（FortiClient）のアップデートに関しては、弊社の責任において適切な周知案内を実施いたします。	【弊社】 「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、**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**して頂く必要がございます。		【弊社】 インフラ・アプリケーション・サービス全般

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.　リスク対応概要（詳細一覧は、別紙「リスクアセスメント資料」を参照ください。）



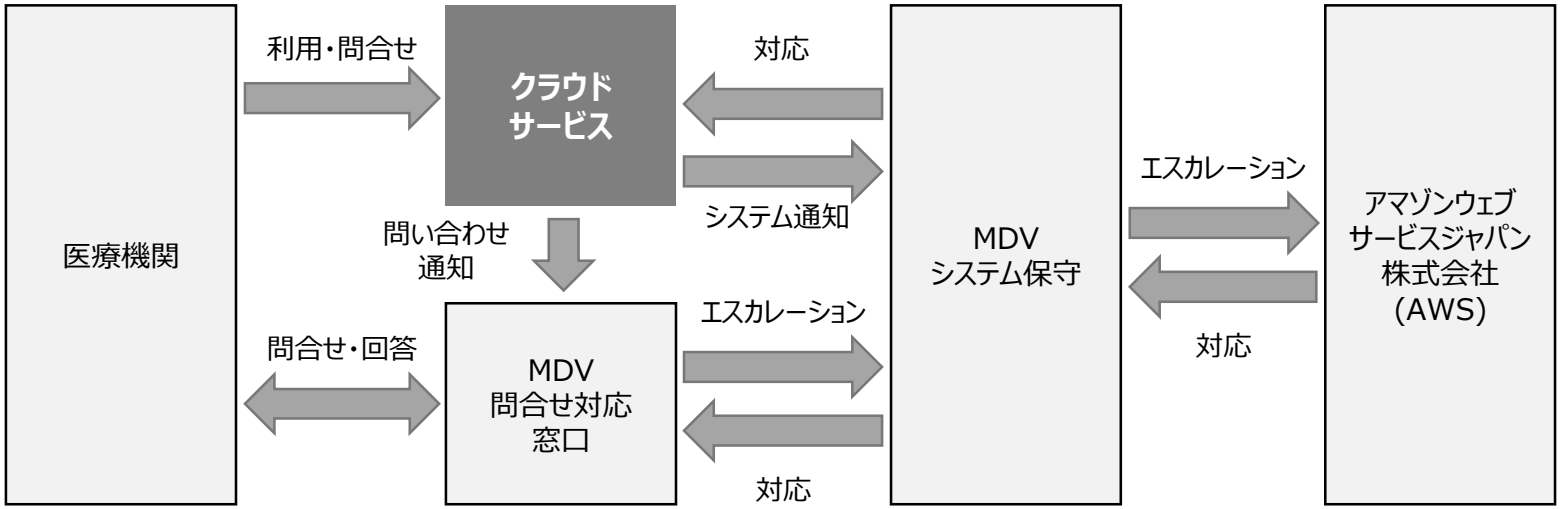
※医療情報にはDPC、レセプト及び関連するデータが含まれます。

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

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

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

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. 事故発生時の対応方法及び医療機関等への報告方法

受託する医療情報が漏洩した場合には、速やかに、お客様管理者へご連絡いたします。

また、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。

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。

また、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。

なお、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/

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 [6/7]

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

本サービスの利用に係る患者等への説明については、第一次的にはお客様において対応して頂くこととし、弊社においては必要な資料等の提供等の範囲で対応いたします。

お客様において受託する情報を分析し、あるいは第三者に提供するために必要な加工を施す際に求められる患者等への説明と同意に関しても同様といたします。

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・コンプライアンス部）

※ 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」をご参照ください。

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 [7/7]

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。

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弊社の責任範囲
第5版	2024年5月24日	社内の組織変更に伴う見直し

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