膀胱用超音波画像診断装置「DFree メディカル」

DFree MEDICAL セキュリティガイド

サイバーセキュリティに係る情報提供資料

DFree株式会社

1. 本資料の目的

本資料は、膀胱用超音波画像診断装置「DFree メディカル」（以下「本品」といいます。）のサイバーセキュリティ対策並びに本品が取り扱う情報及びその保存について、本品をご利用いただく医療機関の皆様（医療機器安全管理責任者、医療情報システム安全管理責任者及びシステム運用のご担当者を想定しています。）に説明することを目的としています。

本資料は、厚生労働省の通知「医療機器のサイバーセキュリティ導入に関する手引書の改訂について」（令和5年3月31日付け薬生機審発0331第11号・薬生安発0331第4号）の別添「医療機器のサイバーセキュリティ導入に関する手引書（第2版）」に基づく、顧客向けセキュリティ文書として作成しています。医療機関における本品の導入時のご検討、「医療情報システムの安全管理に関するガイドライン」に基づくリスク分析及び運用管理規程の作成に、本資料をご活用ください。

本資料は、当社ウェブサイトに掲載し、最新版を公開します。SBOM（ソフトウェア部品表）、MDS2（製造業者による医療機器セキュリティ開示書）、詳細なシステム構成図等の詳細な資料は、第13章に定めるとおり、医療機関のお求めに応じて個別に提供します。本資料の記載内容は、製品の改良等に伴い予告なく改訂することがあります。

2. 対象製品

項目	内容
販売名	DFree メディカル
一般的名称	膀胱用超音波画像診断装置（JMDN コード：70013000）
クラス分類	管理医療機器（クラス II）、特定保守管理医療機器
医療機器認証番号	308AHBZX00045000
製造販売業者	DFree 株式会社

本品は、本体（DFree MEDICAL）、スマートフォン端末上の専用アプリ（DFree MEDICAL アプリ。以下「アプリ」といいます。）及び当社クラウドサーバー（別品目（非医療機器））により構成されるシステムとして使用します。測定データの閲覧、記録及び分析には、連携用アプリケーション DFree Viewer 及び WEB サービス DFree Viewer WEB（いずれも非医療機器）を利用できます。

3. システム構成及びネットワーク接続

本品のシステム構成及びネットワーク接続の概要は、図1のとおりです。

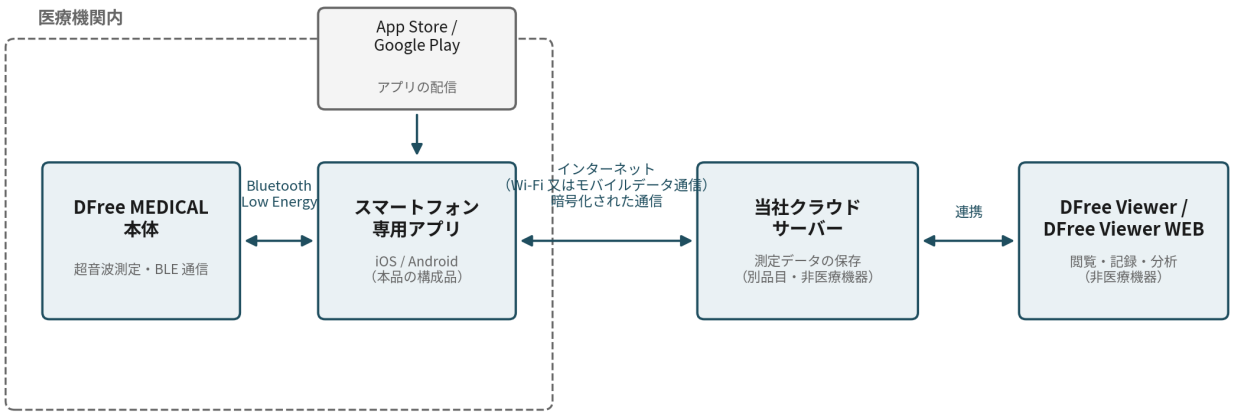

図1　システム構成の概要（概念図。詳細なシステム構成図及び通信仕様は、お求めに応じて提供します。）

- 本体とアプリは、Bluetooth Low Energy（2.4GHz 帯）により通信します。本体は、医療機関の院内ネットワーク（有線 LAN 及び無線 LAN）には直接接続しません。本体とアプリとの間の通信は、暗号化されます。
- アプリと当社クラウドサーバーとの間の通信は、インターネット（Wi-Fi 又はモバイルデータ通信）を経由し、暗号化された通信路により保護されます。
- アプリは、App Store 又は Google Play ストアから配信されます。これら以外の経路ではアプリを配布していません。
- 使用するネットワークポート及び接続先の一覧は、詳細資料（第 13 章）として、お求めに応じて提供します。

4. 取り扱う情報及びその保存先

本品の使用に当たっては、アプリに利用者（患者）の情報を登録し、測定の実施によりアプリ上に尿量等の測定データが生成されます。

本品が取り扱う情報の項目、その保存先（スマートフォン端末内及び当社クラウドサーバー）及び個人情報該当性、当社クラウドサーバーの運用形態及びデータ保護の方法並びに本体内に保存されるデータは、次のとおりです。

4.1 取り扱う情報の項目及びその保存先

本品が取り扱う情報は、アプリが管理するスマートフォン端末内のデータベースに保存されるとともに、その一部が当社クラウドサーバーへ送信され保存されます。測定データ及び本体の状態情報は、アプリが利用者ごとに発行する利用者ID及び本体のシリアル番号に紐づけて記録されます。

区分	情報の項目	保存先	個人情報該当性
利用者（患者）情報	アプリが利用者ごとに発行する利用者 ID、氏名及びふりがな、生年月日、性別、所属する施設、病棟（ユニット）、病室及びベッドの情報、使用する本体の識別情報、ナースコール連携用のコード、ケアプラン等のメモ、利用者ごとの通知等の設定情報（各種通知の有効・無効、しきい値、繰り返し間隔等）、排便及びガスの検知に関する状態及び設定情報並びに外部の記録システムとの連携用の識別情報	スマートフォン端末内及びクラウドサーバー	該当
測定データ	尿量値（補正前の値、補正後の値及び表示用の値）、超音波データ、尿の有無の判定結果、異常検知の判定結果、測定区間の情報並びにスポット測定の結果（超音波データ、加速度、姿勢情報及びメモを含む。）	スマートフォン端末内及びクラウドサーバー	該当（利用者 ID に紐づく）
本体の状態情報	加速度及び姿勢情報、バッテリー情報（残量、温度、充電回数、電圧等）並びに本体とアプリとの Bluetooth 接続ログ	スマートフォン端末内及びクラウドサーバー	該当（利用者 ID に紐づく）
受信生データ	本体から受信した超音波データ、加速度、姿勢情報及びバッテリー情報の生データ	スマートフォン端末内のみ	該当（利用者 ID に紐づく）
監査ログ	アプリの操作履歴（発生日時、イベントの種別、操作者 ID、施設 ID、利用者 ID、本体のシリアル番号、操作の結果等）	スマートフォン端末内のみ	該当（利用者 ID 及び操作者 ID を含む）
記録情報	排尿及び排便の記録（記録日時、トイレ、パッド又はおむつにおける排尿の有無及び量、残尿量、尿意及び尿漏れの有無、排便の量及び便の硬さ、飲水、下剤の使用、姿勢、担当スタッフ名、メモ、外部の記録システムとの連携用の識別情報等）並びに通知の履歴（通知の種別、日時及び通知時の尿量）	クラウドサーバー（アプリから API により登録）	該当（利用者 ID 及び担当スタッフ名を含む）
アカウント情報	アプリの操作者のログイン ID（メールアドレス）、認証情報及び所属する施設の情報	クラウドサーバー（Google Firebase）	該当

本品が取り扱う情報は、利用者情報と紐づけることにより特定の個人を識別できるため、医療機関において個人情報（要配慮個人情報を含みます。）として取り扱ってください。

当社クラウドサーバーに保存された情報は、本品の使用終了後、医療機関からのご依頼に基づき削除します（第11章参照）。スマートフォン端末内の情報は、アプリを端末から削除することにより消去されます。

各情報の詳細な項目については、第15章の窓口にお問い合わせください。

4.2 クラウドサーバーの運用形態及びデータ保護

当社クラウドサーバーは、Amazon Web Services（AWS）及び Google Firebase を利用して運用しています。利用者（患者）情報、測定データ及び記録情報を保存するデータベースは、AWS の東京リージョン（ap-northeast-1）に配置しており、これらのデータは日本国内で保管します。

アプリの操作者のアカウント情報（ログインID及び認証情報）は、Google Firebase Authentication により管理され、同サービスの仕様上、米国のデータセンターで処理及び保存されます。利用者（患者）情報及び測定データが米国のデータセンターに保存されることはありません。

当社クラウドサーバーに保存されるデータは、次の対策により保護しています。

- データベースは、インターネットその他の外部ネットワークから直接接続できない構成としています。データへのアクセスは、当社が提供する API を経由する場合に限られます。
- API によるデータへのアクセスは、アカウントごとに制御しており、認証されたアカウントは、許可された範囲のデータにのみアクセスできます。
- アカウントの認証情報（パスワード等）は、暗号化して保管しています。
- 当社の担当者によるクラウド環境への管理アクセスは、ID 管理サービスによるシングルサインオン及び AWS IAM（Identity and Access Management）により、利用できるサービス及び権限を必要な範囲に制限しています。
- 測定データを保存するデータベース及びストレージは、AWS の標準機能により、保存時に暗号化しています。利用者（患者）情報及び記録情報を保存するデータベースは、上記の接続制限及びアクセス制御により保護しています。

4.3 本体内に保存されるデータ

本体（DFree MEDICAL）には、利用者情報及び測定データは保存されません。本体内には、本体の動作に必要な設定情報及びファームウェアのみが保存されています。

5. 意図する使用環境及び動作必須環境

本品は、医療機関内で医療従事者が使用することを意図しています。アプリは、次の条件を満たすスマートフォン端末及びネットワーク環境でのみ動作を保証します。条件を満たさない環境では、誤作動又は正しい測定ができないリスクがあるため、使用しないでください。

- OS：iOS 18、26 ／ Android 14、15、16
- メモリ（RAM）：4GB 以上
- 電気安全性：IEC 62368-1 に適合していること
- 電磁両立性：CISPR32 に適合していること

スマートフォンメーカーが認めていないシステム改変（改造）を行ったスマートフォン端末では使用しないでください。対応 OS のバージョンは、製品の改良等に伴い変更することがあります。最新の対応状況は、当社ウェブサイトでお知らせします。

6. 当社のサイバーセキュリティ対策

6.1 開発及び品質管理の体制

当社は、医療機器の製造販売業者として、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（薬機法）、QMS 省令その他の法令並びに厚生労働省の通知及び手引書に従い、本品のサイバーセキュリティ対策を実施しています。本品は、JIS T 81001-5-1:2023（ヘルスソフトウェア及びヘルスITシステムの安全、有効性及びセキュリティ―製品ライフサイクルにおけるアクティビティ）に適合したプロセスに基づき設計開発を行い、医療機器の基本要件基準第12条第3項への適合を確認した上で、認証を取得しています。市販後は、品質マネジメントシステム（QMS）及び製造販売後安全管理（GVP）の体制の下で、脆弱性の監視、評価及び対応を継続します。

6.2 製品のセキュリティ機能の概要

本品は、次のセキュリティ機能を備えています。セキュリティ上の理由から、方式等の詳細は本資料には記載しません。詳細な情報が必要な場合は、第13章の詳細資料をご利用ください。

- アプリの利用に当たってのアカウント及びパスワードによるログイン認証
- 本体とアプリの接続における、意図しない端末からのアクセスを防止するための認証
- 通信の暗号化（第 3 章参照）
- ソフトウェア更新の完全性の確認及び不正な旧バージョンへの巻き戻しの防止

6.3 第三者によるセキュリティ評価

本品は、外部の専門機関によるセキュリティ評価を、本体、アプリ及び外部（サーバー）を対象として実施しています。評価結果に基づく対応は、当社のリスクマネジメントプロセスに従って実施しています。

7. 安全にご利用いただくために医療機関にお願いする事項

本品を安全にご利用いただくため、医療機関の皆様に次の事項をお願いします。詳細は取扱説明書をご覧ください。

7.1 アカウント及びパスワードの管理

- 推測されにくい強力なパスワードを設定し、定期的に変更してください。パスワードを第三者に教えたり、共有したり、目につく場所に書き残したりしないでください。
- 複数の方でスマートフォン端末を共用する場合は、使用後にアプリからログアウトしてください。

7.2 スマートフォン端末の管理

- 端末にパスワード又は生体認証等によるロックを設定し、常に有効にしてください。
- 端末の紛失又は盗難が発生した場合は、直ちに貴院の管理者（情報システム部門等）及び当社窓口（第 15 章）にご連絡ください。
- システム改変（改造）を行った端末では使用しないでください。アプリは App Store 又は Google Play ストア以外から入手しないでください。
- OS のセキュリティ更新は速やかに適用することを推奨します。OS のメジャーバージョンアップは、対応状況を当社ウェブサイトでご確認の上、実施してください。

7.3 ネットワーク及び全般的な対策

- スマートフォン端末を貴院のネットワークに接続する場合は、貴院の情報システム管理者の指示（セキュリティ設定等）に従ってください。
- 使用を終了した機器及び端末を、ネットワークに接続したまま放置しないでください。
- 厚生労働省「医療情報システムの安全管理に関するガイドライン」に従った管理をお願いします。本品のリスク分析に必要な情報は、本資料及び第 13 章の詳細資料をご利用ください。

8. ソフトウェアの更新

当社は、脆弱性への対応等のため、アプリ及び本体ソフトウェア（ファームウェア）の更新を提供することがあります。アプリの更新は App Store 又は Google Play ストアを通じて配信しま

す。本体ソフトウェアの更新は、アプリからOTA（Over the Air）を通じて提供します。

セキュリティに関わる重要な更新を提供する場合は、アプリ内の通知、電子メール又は当社ウェブサイトによりお知らせします。更新のご案内を受けた場合は、速やかに適用してください。

9. 脆弱性情報の収集、評価及び提供

当社は、独立行政法人情報処理推進機構（IPA）、JPCERT コーディネーションセンター（JPCERT/CC）、ソフトウェア部品の供給者等から本品に関連する脆弱性情報を継続的に収集し、ソフトウェア部品表（SBOM）に基づき本品への該当性を評価し、深刻度（CVSS）に応じて定めた期限内に修正、緩和策又は補完的対策を実施します。

本品に影響を及ぼす脆弱性又はその対策に関する情報は、セキュリティアドバイザリーとして、当社ウェブサイトへの掲載又は納入先の医療機関へのご連絡によりお知らせします。社会的に影響の大きい脆弱性については、本品が影響を受けない場合にも、その旨をお知らせすることがあります。

当社は、脆弱性を発見された方から報告を受け付けるための協調的脆弱性開示（CVD）ポリシーを当社ウェブサイトで公開しています。本品の脆弱性を発見された場合は、同ポリシーに従いご報告ください。

10. サイバーセキュリティインシデント発生時の対応

10.1 当社における対応

本品に関わるサイバーセキュリティインシデントが発生した場合又はそのおそれを認めた場合、当社は、法令及び社内手順に従い、速やかに影響を評価し、納入先の医療機関への連絡及び情報提供を行います。医療機関がサイバー攻撃を受けた場合には、あらかじめ整理した本品に関する情報に基づき、医療機関と連携して医療提供の復旧に協力します。

10.2 医療機関へのお願い

- 身に覚えのないログイン、利用者情報若しくは記録の改変又はアプリ若しくは本体の異常な動作など、サイバーセキュリティ上の異常が疑われる場合は、本品の使用を中止し、当社窓口（第 15 章）にご連絡ください。
- スマートフォン端末の紛失又は盗難の場合は、当社窓口にご連絡ください。当社は、所定の手順に従い、アカウントの停止等の必要な措置を行います。

11. データのバックアップ及び使用終了時の対応

本品の使用を終了する場合（解約、返却又はスマートフォン端末の入替えの場合）は、アプリからログアウトした上でアプリを端末から削除し、当社窓口にアカウントの停止又は削除をご依頼ください。

12. 製品ライフサイクル（サポート期間）

当社は、本品の製品寿命終了（EOL：End of Life）を、本品の新規の出荷（販売及び貸与）を終了する日とし、サポート終了（EOS：End of Support）を、EOL の日から3年を経過した日とします。EOL の予定時期は現時点では未定です。

EOL までの間は、保守、不具合の修正及びセキュリティ更新を提供します。EOL から EOS までの間は、限定的サポート段階として、セキュリティ更新の提供、脆弱性情報の監視及びセキュリティアドバイザリーの提供並びに保守用部品の供給を継続しますが、患者の安全に重大な影響を与える場合を除き、一般の不具合の修正は行いません。EOS 以降は、すべてのサポートを終了します。

当社は、EOL 及び EOS の予定時期を変更する場合並びに EOS が近づいた場合には、当社ウェブサイト及び納入先の医療機関へのご連絡によりお知らせします。EOS 後も本品を継続して使用される場合は、ネットワークからの分離その他の補完的な対策を実施してください。

なお、対応するスマートフォンの OS のバージョンの範囲並びにクラウドサービスの仕様は、EOL 及び EOS とは別に変更することがあります。この場合も、あらかじめ同様の方法によりお知らせします。

13. 提供可能な資料

当社は、本資料のほか、次の資料を作成しています。これらの資料は医療機器のセキュリティに関する詳細な情報を含むため、医療機関のお求めに応じ、秘密保持に関する取り決め（覚書等）に基づき個別に提供します。ご希望の場合は、第15章の窓口にご連絡ください。

資料	内容
MDS2（製造業者による医療機器セキュリティ開示書）	本品のセキュリティ機能を、国際的に用いられている様式（ANSI/NEMA HN 1-2019）により開示する資料です。
SBOM（ソフトウェア部品表）	本品を構成する主要なソフトウェア部品（名称、バージョン、供給者等）の一覧です。人が読める形式の資料として提供します。
詳細なシステム構成図及び通信仕様	ネットワークポート、接続先等を含む詳細な構成情報及び通信仕様です。

14. 個人情報の取扱いについて

当社の個人情報の取扱いについては、当社プライバシーポリシーをご確認ください。

15. お問い合わせ窓口

窓口	連絡先
サイバーセキュリティに関する問い合わせ・脆弱性の報告窓口	security@dfree.co.jp
医療機器製品に関する一般のお問い合わせ（サポート窓口）	DFree 株式会社 電話：03-5459-1295（受付時間：平日 10:00〜17:00。土日祝日・年末年始を除く。） 電子メール：medical-care@dfree.co.jp

16. 改訂履歴

Rev	発行日	改訂内容
1.0	2026 年 9 月 8 日	初版発行
1.1	2026 年 10 月 21 日	4.2 クラウドサーバーの運用形態及びデータ保護：保存時の暗号化に関する記載について、暗号化の対象を測定データに限定し、利用者（患者）情報及び記録情報を保存するデータベースの保護方法（外部ネットワークからの接続制限及びアクセス制御）を明記するよう修正 4.1 取り扱う情報の項目及びその保存先 並びに 13. 提供可能な資料：取り扱う情報の詳細な項目に関する記載を整理 13. 提供可能な資料：SBOM の提供形式に関する記載を修正