White Paper

MedicalCare STATION

2024 年 4 月 1 日
エンブレース株式会社

はじめに

White Paper の目的
MedicalCare STATION は、エンブレース株式会社が提供している全国の医療介護の現場でご利用いただいている地域包括ケア・多職種連携のためのコミュニケーションツールです。

本ドキュメントは、MedicalCare STATION の提供において基盤として利用するクラウドサービスにおけるセキュリティに関する方針、並びにプロセスの概要をご理解いただくとともに、ISMS クラウドセキュリティ認証である ISO/IEC 27017 の要求に従う公表を行うことを目的とします。

White Paper の対象
MedicalCare STATION の導入を検討中の方
MedicalCare STATION を利用中の方

クラウドコンピューティングのための情報セキュリティ方針
当社では、クラウドコンピューティングに関する情報セキュリティの方針を定め、ユーザーに満足いただける機能的でセキュアなサービスの提供を目指しています。

クラウドコンピューティングに関する情報セキュリティ方針
当社は、クラウドコンピューティング環境におけるユーザーの情報資産を情報セキュリティ上の脅威から保護するための措置を講じ、ユーザーが安心してご利用いただけるセキュアなサービスを提供します。

当社の「情報セキュリティ方針」は以下の URL からご確認頂けます。
https://about.medical-care.net/html/informationsecurity/

情報セキュリティ組織
当社では、情報セキュリティに関する統括責任者を任命し、情報セキュリティに関する統括責任と権限を与えています。また、情報セキュリティ委員会を設置し、情報セキュリティのマネジメントシステムの運用と継続的改善に取り組んでいます。

地理的所在地
当社の所在地、並びに当社がユーザーのデータを保存する国は日本国となります。当社が基盤として利用するクラウドサービスにおいて、日本国以外のリージョンにユーザーのデータを保存する必要性が生じた場合、ユーザーに事前に通知したうえで行います。

責任範囲（共有 Model）
仮想レイヤーや施設におけるコンポーネントは、当社が基盤として利用するクラウドサー

ビス事業者によって管理されます。当社は、当社のサプライヤーに対するセキュリティポリシーに従い、調達時のセキュリティ審査、及びパフォーマンスのモニタリングによりクラウドサービス事業者を管理します。
また、当社は、基盤上に構築したアプリケーションに対して責任を負います。
アプリケーション上のデータについては、ユーザーの責任において保護していただく必要があります。

当社の責任
・MedicalCare STATION のセキュリティ対策
・MedicalCare STATION に保管されたユーザー情報の保護

ユーザーの責任
・利用者アカウントの管理（登録、削除、権限設定、管理者設定、アクセス権の設定など）
・パスワード等の利用者の秘密認証情報の管理
・ユーザーが取扱うデータに対してのバックアップ

情報セキュリティの意識向上，教育及び訓練
当社は、全従業員に対する定期的な情報セキュリティ教育を実施し、情報セキュリティに対する意識向上に努めています。また、クラウドコンピューティングに関する契約相手に対しても、同等レベルの教育を求めています。

情報セキュリティのパフォーマンス評価
当社では、定期的（最低でも年に一回）に情報セキュリティに関する内部監査を実施しています。定期的な内部監査以外に、組織、施設、技術、プロセス等の重大な変化にあわせて、独立した内部監査を行っています。

インシデント対応プロセス
当社では、ISO/IEC27001 に準拠した標準化された情報セキュリティインシデント対応プロセスを整備しています。情報セキュリティインシデントに関する報告、エスカレーショ

ンに関する全ての手順が文書化され、情報セキュリティ委員会により一元的に管理されています、報告されたインシデントはインパクトや緊急性に応じてハンドリングされています。

開発/調達

開発プロセス

当社のクラウドサービスの開発は、機能性とユーザビリティの確保はもちろんのこと、情報セキュリティについても配慮することを方針として行われます。開発は非機能要件としてのセキュリティ要件を定義し、厳格な承認プロセスを得たうえで実施されます。セキュリティ機能に関するソースコードはレビューされ、テストプロセスを経たうえでビルドされます。

サプライチェーン

当社のクラウドサービスの提供に関連するサプライヤー、及びサプライチェーンは以下の手段により管理することを方針としています。

・情報セキュリティ水準を当社と同等又はそれ以上に保つことを事前の審査により確実にする
・契約により秘密保持の確保を担保する
・サプライヤーがサプライチェーンを形成しサービス提供している場合、サプライヤーのサプライチェーンメンバーに対するセキュリティ管理の能力について審査する

アプリケーションのセキュリティ機能

情報セキュリティ機能

主にユーザーが検討する情報セキュリティ機能として、本ホワイトペーパーは以下を記述しています。

機能（ISO/IEC27017 の管理策）	本ホワイトペーパーの記述
5.16　識別情報の管理	利用者アクセスの管理
5.17　認証情報	認証情報の管理
5.18　アクセス権	利用者アクセスの管理
8.2　特権的アクセス権	認証情報の管理
8.3　情報へのアクセス制限	利用者アクセスの管理
8.13　情報のバックアップ	バックアップ
8.15　ログ取得	ログ
8.24　暗号の使用	暗号化
CLD.12.4.5 クラウドサービスの監視	クラウドサービスの監視

利用者アクセスの管理

MedicalCare STATION は、ユーザーがストレスなく、安全に利用者アクセスの管理を行うためのユーザインターフェイスと機能を提供します。ユーザーは画面から簡単な操作によりユーザーに対する権限の割り当てを行うことが出来ます。使用方法の詳細は「ユーザーマニュアル」をご参照ください。

認証情報の管理

初期のアカウント登録手順は「ユーザーマニュアル」をご参照ください。アカウントの登録が完了すると、登録したメールアドレスに対し、一定時間のみ有効な本登録用 URL が記載されたメールが届きますので、画面の指示に従い本登録を行っていただきます。

パスワードの設定はユーザーのセキュリティポリシーにもとづいて実施してください。また、MedicalCare STATION のユーザーアカウントはクライアント証明書を使った二要素認証を利用することが可能です。

管理者権限はユーザーのセキュリティポリシーに従い厳重に管理することをお願いします。

ユーティリティプログラム

ユーティリティプログラムは管理者権限に限定して利用可能です。管理者権限を厳重に管理することによりユーティリティプログラムの使用制限につながります。

暗号化

データベースに保管されるユーザーデータは、ASE-256 暗号化アルゴリズムを使用して暗号化しています。
ユーザーのパスワードは、ハッシュ化をしています。
MedicalCare STATION とユーザーとの間での通信は、SSL/TLS で暗号化し、情報の盗聴

等のリスクに対処しています。

運用

変更
ユーザーに影響を与える MedicalCare STATION の変更は、ご登録頂いたメールアドレス宛に事前通知します。
また、各種の変更管理に関する情報は画面より、確認することができます。

管理者用手順
「ユーザーマニュアル」等の各種マニュアルの提供に加え、電話、WEB での QA サポートを提供しています。

バックアップ
システム及びユーザーデータのバックアップは、日次で 8 世代分のデータを保持します。
ただし、ユーザーからのバックアップデータの復元等に関するご要望には対応していません。

ログ
MedicalCare STATION の維持管理に必要となる適切なログ（タイムラインの機能に準ずるメッセージの投稿者、投稿時間、リアクション、通話時間の時刻など）を取得しています。

MedicalCare STATION は、基盤として利用するクラウドサービス事業者が提供する時刻同期サービスを利用し時刻同期を行っています。

ログは、日本標準時（UTC + 9）で提供されます。

クラウドサービスの監視
当社は、MedicalCare STATION が正常に提供され、他社を攻撃する基盤として使用される等に不正に使用されていないこと、データの漏洩が発生していないか等のログの監視を行っています。

技術的脆弱性の管理
アプリケーションを構築する上で使用するソフトウェアに脆弱性が検知された場合、速やかに影響調査と有効な対策を行います。

ネットワーク
MedicalCare STATION 専用の仮想ネットワークを構築し、入口への侵入を IDS/ IPS により監視することによりセキュリティを確保しています。

MedicalCare STATION は、ネットワークの仮想化技術を利用して、他とのネットワークの分離を適切に行っています。

容量・能力の管理
当社は、サーバリソース、及びネットワークリソースを監視しています。またリソースの

増減は GUI から瞬時に実行することができます。サーバリソースはインスタンスの構成を変更せずにスケールアップによることを原則としていますが、将来的なニーズに照らして、必要があればスケールアウトによる対応も行います。

負荷分散/冗長化

MedicalCare STATION は基盤を提供するクラウドサービス事業者のマネジメントサービスを使用し、複数の仮想サーバに処理を振り分ける、ロードバランシングを採用しています。

また、アプリケーションの構成はマシンイメージとして保存し、即時に複製が可能な状態を整えています。

インシデント対応

MedicalCare STATION に関連した情報セキュリティインシデントを検出した場合、以下の内容で速やかに通知します。

項目	内容
報告する範囲	データの消失、長時間のシステム停止等のユーザーに大きな影響を及ぼす可能性のある情報セキィリティインシデント
対応の開示レベル	当社に起因する情報セキュリティインシデントでユーザーに影響があるものは、すべて同等のレベルで対処します。
通知を行う目標時間	検知から 72 時間以内を目標に通知します。
通知手順	ご登録頂いたメールアドレス宛、管理者画面 （必用に応じて電話等の手段を使用する場合もあります。）
問合せ窓口	代表取締役社長　荒木 真哉 TEL：03-6860-4527（代表） メール：info@embrace.co.jp
適用可能な対処	当社に起因する情報セキュリティインシデントでユーザーに影響があるものは、あらゆる手段を講じて対処します。

また、ユーザーにおいて情報セキュリティインシデントを検出された場合、またはその疑いをもたれた場合は、MedicalCare STATION 内のお問い合わせページ、又は本資料末尾の「MedicalCare STATION に関するお問い合わせ」にご連絡ください。

装置のセキュリティを保った処分又は再利用

当社は、情報システム管理者に装置の処分又は再利用に関する役割を集中し、従業員による個別対応を排除することで、セキュア且つ確実な装置の処分又は再利用を実現しています。

その他

証拠の収集
法令また権限のある官公庁からの要求により MedicalCare STATION 上にあるデータ等の情報を、当該官公庁またはその指定先に開示もしくは提出することがあります。合意について別途、「利用規約」をご参照ください。

適用法令及び契約上の要求事項
利用契約に関する準拠法は、日本法とします。別途、「利用規約」をご参照ください。

知的財産権
本サービスを構成する有形または無形の構成物（プログラム、データベース、画像、マニュアル等の関連ドキュメントを含むがこれらに限られない）に関する著作権を含む一切の知的財産権その他の権利は当社に帰属します。別途、「利用規約」をご参照ください。

記録の保護
アプリケーションにおけるデータ操作等のログはユーザーにて保護して頂く必要があります。当社は、仮想ネットワークへのアクセスに関するログ、及びサービスのバージョンアップに関する内部要員による作業ログを一定期間保存します。

暗号化機能に対する規制
MedicalCare STATION において暗号化の規制対象になる地域にはサービスを提供していません。

第3者認証

ISO/IEC27001

当社は、全社を認証範囲として 2020 年 3 月に ISMS（Information Security Management System）の国際規格である ISO/IEC27001 を取得しています。

ISO/IEC27017

当社は、2023 年 4 月に ISMS（Information Security Management System）の国際規格である ISO/IEC27017 を取得しています。

MedicalCare STATION に関するお問い合わせ

代表取締役社長　荒木 真哉
TEL：03-6860-4527（代表）
メール：info@embrace.co.jp

更新履歴

版数	日付	更新内容
第 1.0 版	2023 年 3 月 1 日	初版
第 1.1 版	2023 年 12 月 27 日	「運用」に関する文言改訂
第 1.2 版	2024 年 2 月 15 日	アプリケーションのセキュリティ機能／情報セキュリティ機能　要求事項番号変更
第 1.3 版	2024 年 3 月 14 日	「暗号化」に関する文言改訂
第 1.4 版	2024 年 4 月 1 日	エンブレース株式会社 役員変更に伴い代表者名変更