White Paper

対面・オンライン診療システム

FOR CLINIC

株式会社 Linc' well

2021 年 10 月 1 日（第1.0 版）

はじめに

White Paper の目的

FOR CLINIC は～を実現する当社のクラウドサービスです。

本ドキュメントは、FOR CLINIC、及び FOR CLINIC がプラットフォームとして利用するクラウドサービスの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

FOR CLINIC の導入を検討中の方
FOR CLINIC 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://reservation.clinicfor.life/policy

当社は「情報セキュリティ方針」を拡充した、「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」を定め、ユーザ様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のための情報セキュリティ方針」は以下の通りです。

「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」

当社は、クラウドコンピューティング環境におけるユーザ様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、ユーザ様に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。

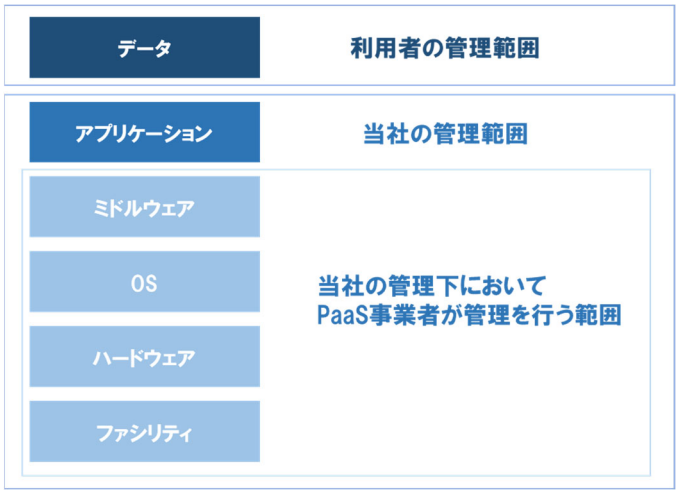
知っていただきたいこと

地理的所在地

当社の所在地、並びに当社がユーザ様のデータ(以下、「カスタマデータ」という)を保存する国は日本国となります。このデータ保存に関するポリシーは、スナップショットやレプリケーションを含むすべてのカスタマデータに適用します。当社が日本国以外のリージョンにカスタマデータを保存する必要性が生じた場合、ユーザ様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カスタマデータについては、ユーザ様の責任において保護していただく必要があります。



当社が、FOR CLINIC のプラットフォームとして利用するクラウドサービスは AWS(Amazon Web Service)になります。ユーザ様には FOR CLINIC におけるシステム機能、及び情報セキュリティ機能が、AWS により提供される機能に依存することについて、理解いただく必要があります。

マネジメントシステム

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。統括責任者は情報セキュリティに関する豊富な知識と業務経験を有することを要件に任命されます。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。

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。

Dev/Ops

開発プロセス

（クラウドサービスを含む）当社における全てのシステム開発は、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して行うこと（Dev/Sec）をポリシーとしています。開発チームには情報セキュリティスペシャリストが参画し、セキュリティ要件はバックログにおける優先項目として扱われます。セキュリティ機能は、開発チームによりレビュー・テストされプロダクトオーナーによりレビューされます。

また、リリース前のみならず、リリース後もマネージドサービス、またはサードパーティを活用して定期的な脆弱性診断を行っています。

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方針により管理しています。

・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

ブルーグリーンデプロイメント

当社の提供するクラウドサービスは、新バージョンのリリース時に、ブルーグリーンデプロイメントを採用しています。現バージョンの仮想環境（グリーン）と新バージョンの仮想環境（ブルー）を同時に用意し、アクセス先を切り替えることで、瞬時に新バージョンへの移行を可能としています。

自動化

CI/CD ツールを用いて、ビルド、デプロイ、及びインフラストラクチャーの構築に関する作業に対する自動化を実現しています。

変更

ユーザ様に影響を与える FOR CLINIC の変更は、ご契約時のメールアドレス宛に事前通知します。
変更に伴うサービスレベルの取扱いについては「利用規約」に従うものとします。

バックアップ

当社のクラウドサービスでは、仮想マシンイメージのスナップショットを取得しています。日次（25 時スタート）で Disk To Disk によるバックアップを取得しており、7 世代以上を保持しています。バックアップはストレージサービス（S3）に保存され、毎日目視で確認しています
また、バックアップ検証用サーバにて年一回バックアップリストア試験を行います。
仮想マシン内のカスタマデータのバックアップはユーザ様の責任において実施してください。

作業ログ

当社はすべてのインスタンスに対し、サードパーティ製のエージェントを導入したうえで、Amazon Cloud Watch Logs によるログ監視、通知を行っています。エージェントが収集したログはストレージ（S3）に保存されます。

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、FOR CLINIC のトップ画面等で通知し、速やかに影響調査を行います。
脆弱性情報の収集は以下の手段により行います。
・JPCERT コーディネーションセンターから公開される脆弱性情報
・当社関係者による検知
・ユーザ様、Amazon 等の外部からの情報提供

検出した脆弱性については、速やかに影響調査を行い、必要な対策を講じます。対策の状況は随時、FOR CLINIC のトップ画面にて公表します。

ネットワーク

FOR CLINIC 専用の仮想ネットワーク（VPC）を構築しています。

FOR CLINIC は、ユーザ様のテナント毎にネットワーク設定を行います。ユーザ様ご指定のネットワーク以外からはアクセス遮断の設定を行う事で、他のユーザ様とのネットワークの分離を行っています。

FOR CLINIC における、ユーザ様に提供するクラウドコンピューティング環境と、当社の運用管理環境は別ロケーションとして分離し、VPN により接続しています。

仮想ネットワーク内のサブネットは、当社のネットワークの設計ポリシーに従い、物理的なネットワークとの整合性を確保したうえで分離、及びルーティングされています。

FOR CLINIC における、インターネットとの境界はインターネット Gateway を設置し、また WAF によりアプリケーションをターゲットとした外部からの攻撃に備えています。

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、スケールアウトも視野にいれています。

負荷分散/冗長化

FOR CLINIC は、アベイラビリティゾーンをまたいで複数のインスタンスに処理を振り分けるロードバランシングを行っています採用しています。ロードバランサー（ELB）は各インスタンスのヘルスチェックを行い、異常の検出されたインスタンスへの転送を停止します。

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

アカウント管理

当社の Amazon アカウント（Root アカウント）は多要素認証（MFA）により厳重に管理し、FOR CLINIC の運用管理において使用しないことを原則とします。

FOR CLINIC の開発、及び運用は IAM アカウント（グループ）にて実施します。権限をミニマムに設定した IAM ポリシーを設け、これに IAM グループをアタッチすることにより権限の割り当てを行います。IAM アカウントは当社のパスワードポリシーに従い設定し、また多要素認証（MFA）を行っています。

インシデント対応

FOR CLINIC 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、当該インシデントによるユーザ様への影響が懸念される場合は、速やかにご契約時のメールアドレス宛に通知します。

また、ユーザ様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、弊社サポートサイトのお問合せページ、又は当社カスタマーセンターへご連絡ください。
　メール:online-support@clinicfor.life

サービス利用停止後のデータの扱い

FOR CLINIC の利用契約終了後のデータの取扱いは。「利用規約」に従います。保持が必要なデータ等が存在する場合、ユーザ様の責任において、利用契約終了前にダウンロード等をお願い致します。

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。

AWS における装置の処分又は再利用については以下を参照ください。
https://d1.awsstatic.com/International/ja_JP/Whitepapers/AWS_Security_Best_Practices.pdf

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

FOR CLINIC がアプリ―ケーションとして実装する情報セキュリティ機能は「ユーザマニュアル」をご参照ください。
ユーザ様は、「責任範囲」に基づき、FOR CLINIC にて取扱うデータに対してバックアップやアクセス権の設定などの対策を行う責任があります。

情報のラベル付け

FOR CLINIC はユーザが任意の名前で作成した「プロセス」と呼ばれるエリアに対してユーザが指定したファイルを取り込みます。「プロセス」に対して、ユーザもしくはユーザグループを指定したアクセス制限設定が可能です。使用方法の詳細は「ユーザマニュアル」をご参照ください。

利用者アクセスの管理

FOR CLINIC は、ユーザ様がストレスなく、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。お客さまは管理者画面から簡単な操作によりアカウント登録・削除を行い、またユーザ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「ユーザマニュアル」をご参照ください。ユーザ様管理者により新規アカウント作成と初期パスワードの設定を行います。新規アカウントユーザは管理者により設定された初期パスワードを使用して初期ログインを行うと、ユーザ様独自のパスワード変更を行うよう指示されますので、パスワードの設定を行っていただきます。

パスワードの設定はユーザ様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、FOR CLINIC のユーザアカウントは 2 段階認証が可能です。

管理者権限はユーザ様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

FOR CLINIC では、ユーザ様との間での通信を SSL/TLS により暗号化し、情報の盗聴等のリスクに対処しています。
データベースに保管されるカスタマデータは、AES-256 暗号化アルゴリズムを使用して暗号化しています。

SSH のキーペアファイル（秘密鍵）は厳重に管理しています。

操作ログ

FOR CLINIC は管理者権限、及びユーザの操作に関連したログを取得します。一定期間のログは管理者画面から確認することができます。サービス提供中における操作ログは内部データベースに全て保持されます。サービス終了後の保存が必要な場合、CSV ファイルとして出力のうえ、ユーザ様の内部環境にて保管してください。

FOR CLINIC 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マネージドサービスを利用し、協定世界時 (UTC)への時刻同期を行っています。

コンプライアンス

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 FOR CLINIC 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様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

FOR CLINIC において暗号化の規制対象になる国は存在しません。

改定履歴

改訂日	版数	内容	承認	作成