健康管理システム「エールプラス（Ailes+）」サービス仕様書

2024/07/25 版

■データ保管場所

お客様からお預かりしたデータは、AWS の東京リージョンに保管されます。

■お客様の情報セキュリティの役割

アカウント登録・変更・削除等は、提供する機能を用いてお客さまに実施していただきます。

■契約解除によるデータの削除

ご契約解除後、解除日の翌月末までに削除いたします。
ストレスチェックのデータに関してはストレスチェック実施者サービスの契約に則り別途削除致します。ログに関して削除は行われません。

■ラベル付の支援

ユーザーごとにアクセスできる範囲を、お客様にて権限付与を行うことにより決定可能です。
（操作手順はマニュアル本文に記載）

■利用者登録及び登録削除

（マニュアル本文に記載）

■利用者アクセスの提供

（マニュアル本文に記載）

■高権限アカウント

一般利用者よりも強度がある認証を採用しております。厳重な情報管理をお願いいたします。

■利用者との責任分界点

＜株式会社ドクタートラスト の責任＞
株式会社ドクタートラストは、以下のセキュリティ対策を実施します。
- Ailes+アプリケーションのセキュリティ対策
- Ailes+アプリケーションに保管されたお客様データの保護
- Ailes+アプリケーションの提供に利用するミドルウェア、OS、その他インフラのセキュリティ対策

＜お客様の責任＞
・Ailes+は社員番号で従業員を識別しています。社員番号の登録・CSV データ取込みは、お客様の責任で整合性が取れるように正しく行ってください。
・健康診断データの取り込みについて、統一基準にて判定が可能なように、取込みデータの準備・加工をしてください。
・Ailes+は IP フィルタリングの設定が可能な機能を提供しています（従業員権限に対しては対象外）。この機能を利用しないことに起因する漏洩や、利用したことによるトラブルについてはお客様側の責任となります。
・ライフログを手入力した際に発生する、ポイント不正受給などのトラブルについてはお客様側の責任になります
・共有のパソコンやデバイスの利用によって生じた結果ならびにそれに伴う一切の責任については、お客様側に帰属するものとします。

■利用者の秘密認証情報の管理

（マニュアル本文に記載）

■サービスの変更について

当社は、サービスの変更に際し、当社規定に基づき、お客様に重大な影響を及ぼす可能性がある場合においては、お客さま管理者への電子メールもしくは当社ホームページなど適切な方法により速やかに通知いたします。

■情報のバックアップ

データベースに保管される、お客様の各種情報は、日次でバックアップを取得しています。
バックアップは、7 世代分のスナップショットが AWS 上に保管されます。
バックアップは作業開始から 1 時間程度で復元を目指します。
但し、お客様からのバックアップデータの復元等に関する要望は、承っておりません。

復旧目標時間については下記の通りです。
・RPO（データの復旧目標時点）：7 日前まで（毎日 AM1 時にスナップショットを取得）
・RTO（復旧目標時間）：復旧作業開始後 1 時間

■個人情報データのサーバー分離について

データの漏洩やハッキング等の対策の一環として、Ailes+に取り込まれたお客様のデータのうち、氏名は別のサーバーにて暗号化を行った上で保管を行います。

■ログについて

システムを通じた DB とのやりとりや画面のアプリケーションログ、およびアクセスログを 12 か月間記録しております。
お客様からの要望により、提示致します。
ただし、人事担当者など法人からの要請に限ります。

・改竄防止
　認証やアプリケーションログは AWS CloudWatch へ出力し、ファイルに出力しない対応としております。
・監視状況について
　ログ上でエラーを感知した際、自動で通知されるようにしております。

■クロック

記録される時刻は、すべて日本時間(JST)に基づいて記録します。
各サーバは AWS が提供する NTP サーバーを参照して同期しています。

■脆弱性について

当社は、定期的に提供するクラウドサービスについて、脆弱性を発見した場合は、お客さま管理者への電子メールもしくは当社ホームページなど適切な方法により速やかに通知いたします。

■ SLA

インフラは AWS を採用しているため、AWS の SLA に準拠します。
https://aws.amazon.com/jp/rds/sla/
https://aws.amazon.com/jp/ecs/sla/

■ セキュリティについて

Ailes＋システムの開発には、主に Ruby On Rails が用いられています。
開発は Rails セキュリティガイドおよび、社内で定められたコーディング規約に従って実施されます。
（Rails セキュリティガイド：https://railsguides.jp/security.html ）

■ セキュリティの診断について

安全な Web サイトの作り方チェックリストに則り、下記を年に 1 度内部監査にて確認をしております。
・SQL インジェクション
・OS コマンドインジェクション
・パス名パラメータの未チェック／ディレクトリ・トラバーサル
・セッション管理
・クロスサイト・スクリプティング
・CSRF（クロスサイト・リクエスト・フォージェリ）
・HTTP ヘッダ・インジェクション
・メールヘッダ・インジェクション
・クリックジャッキング
・バッファオーバーフロー
・アクセス制御や認可制御の欠落

■ 実務管理者の運用セキュリティ

（マニュアル本文に記載）

■ ネットワークセキュリティについて

オンプレのサーバーを利用してサービス提供は行なっておりません。
AWS ロードバランサー上に WAF を適用し SQL インジェクションや DDoS 攻撃の対策を行なっております。

■ 装置のセキュリティを保った処分又は再利用

AWS にて利用している下記を削除致します。
・7 世代前までのスナップショット
・RDS の該当インスタンス

■ パスワードについて

・パスワード長と複雑性
英大文字・英小文字、数字、記号いずれかの 3 種類の混在による最低 8 桁以上。従業員以外の強い権限をもつユーザーは 12 文字以上を必須としています。
・暗号化について
bcrypt にてハッシュ化を行い、平文を避けて保管しています。（ハッシュは厳密には暗号化ではなく、パスワードが不可逆的に解読不能な保管手法になります。）
・ユーザーによる変更機能
システム内にてユーザー自身で変更することが可能です。
・パスワード誤入力
5 回パスワードを誤入力した際はログインが自動で抑止されます。

■ 暗号化の状況

データベースは Amazon KMS にて暗号化され、適切なアクセス権のもとで AWS のストレージに保管されます。
お客様の個人名と、健康情報や属性情報等は別のデータベースに保存されます。
お客様の個人名は AES_256 形式で暗号化され、適切なアクセス権のもとでデータベースに保管されます。
お客様の端末と、システムとの間のインターネット通信は、SSL/TLS 通信によって暗号化されます。

■ 多要素認証について

ID/パスワードによる認証以外に、ワンタイムパスワードによる多要素認証を備えております。
※ただし、ストレスチェックサービスのみご契約のお客様では、受検者に対しては本人の受検のみのため多要素認証を実装しておりません。他人のデータを参照することが可能な実施者/実施事務従事者権限では多要素認証の設定が可能となっております。

■ IP アドレス制御

お客様に提供する管理者用の画面へのアクセスについて、IP アドレスによる通信経路の制限機能を備えております。
※ただしこの制限は衛生管理者や産業医等の従業員以外の権限に適用されます。

■ アクセス制御について

データベースはマルチテナント利用しております。データはお客様ごとに論理分割して管理しております。
顧客専用テナントの提供は行なっておりません。

■ 要塞化について

AWS ロードバランサーを利用。セキュリティグループで http/https などのプロトコルごとにポートを制限しております。
また REDIS などの特定の AWS の機能にアクセスするのもポートの制限をしております。

■ サービスプロセスの冗長化

AWS ECS/Fargate を採用しており、マルチタスクでサービス提供をしております。リソースが一定数を超えた場合はタスク数が自動で増加します。

■ ドクタートラストの PC 環境について

・業務で利用する PC は、貸与された会社が管理する PC を利用しております。
・BYOD の利用は不可です。
・許可されていないハードウェア（可搬性記憶媒体等）の接続はルール上禁止されております。
・運用端末設置拠点への入館・退館、入室・退出には社員証が必要となっております。またそのログは全て記録されます。
・夜間など社員不在時には警備会社を利用しております。

■ ドクタートラストの社員教育について

従業員に対して実施する情報セキュリティに関する社内勉強会を年に 1 回実施し、テストを行なっております。

■ リスクアセスメントについて

年に 1 度リスク評価の見直しを行なっています。

■ 業務継続計画

年に 1 度情報セキュリティ継続計画書を作成の見直しを行なっています。

■ 暗号化の状況

データベースは Amazon KMS にて暗号化され、適切なアクセス権のもとで AWS のストレージに保管されます。
お客様の個人名と、健康情報や属性情報等は別のデータベースに保存されます。
お客様の個人名は AES_256 形式で暗号化され、適切なアクセス権のもとでデータベースに保管されます。
お客様の端末と、システムとの間のインターネット通信は、SSL/TLS 通信によって暗号化されます。

■ 開発の方針

Ailes+ システムの開発には、主に Ruby On Rails が用いられています。
開発は Rails セキュリティガイドおよび、社内で定められたコーディング規約に従って実施されます。
（Rails セキュリティガイド：https://railsguides.jp/security.html）

■ ICT サプライチェーン

「Ailes+」では、次に示す機能を運用するために、外部のクラウドサービスを利用しています。

クラウドサービス	機能	運営会社	預けている情報
Amazon	インフラ構築・運用	Amazon	個人名やメールアドレスなどの個人情報、健康診断等産業保健に関するデータ
クルメル	メール送信・転送機能	株式会社ラクス	Ailes+より送信されるメール（SMTP リレー）
SendGrid	メール送信・転送機能	Twilio Inc.	Ailes+より送信されるメール（SMTP リレー）

■ インシデント

・お客様に大きな影響を与えるセキュリティインシデント(データの消失、長時間のシステム停止等)が発生した場合は、インシデントが発生してから 72 時間以内を目標に、当社ホームページなど適切な方法により速やかに通知いたします。
・ご連絡の対象はインシデント事象が発生している企業全てに通知致します。
・通知内容は事象をお伝えします。また、判明していれば原因および応急対応についてもお伝えいたします。
・上記連絡の後、応急対応が 24 時間以内に完了しない可能性がある場合は、対応の進捗状況を当社ホームページなど適切な方法により速やかに通知いたします。
・情報セキュリティインシデントに関する問合せは、本サービス仕様書記載の「お客さまサポート窓口」にて受け付けています。

■ 証拠の開示

当社は、裁判所からの開示請求など、法律に基づいた正当な開示請求が行われた場合、お客さまの同意なく、利用者のデータを第三者に開示することがあります。

■ 適合法令

適用される準拠法は日本法です。

■ 知的財産の保護

－（前述）

■ 記録の保護

クラウドサービスカスタマの契約情報の保護や廃棄については、重要な記録の区分をするとともに、管理基準を定め、適切に管理しております。

■ 独立した監査

定期的な内部監査、経営者による審査、リスク評価を実施しております。

また、次の認証の取組みを行い、外部機関による監査を受けるなど、安全なセキュリティを維持しております。

・ISO/IEC 27001　ISMS 認証（2022 年 9 月取得済み）

・ISO/IEC27017　ISMS クラウドセキュリティ認証（2023 年 2 月取得済）

・プライバシーマークの認証

内部監査結果の開示を望まれる場合は、相談窓口へお問い合わせ願います

お客さまサポート窓口

当システムに関するお問合せ窓口は次のとおりです。

- 電子メール　system@doctor-trust.co.jp
- 電話　03-3464-4000（土日祝祭日除き 9:30~17:00）