My Redmine Gen.2 (ジェネレーション 2)

セキュリティホワイトペーパー

ファーエンドテクノロジー株式会社

目次

1.組織

1-1 企業情報

概要

項目	内容
商号	ファーエンドテクノロジー株式会社（英語表記： Far End Technologies Corporation ）
法人番号	8280001002836
所在地	〒690-0003 島根県松江市朝日町 498 番地 松江センタービル
代表者	前田 剛
設立	2008 年(平成 20 年) 9 月 9 日
資本金	800 万円

届出・認定

項目	内容
総務大臣届出 電気通信事業者	届出番号: F-20-668
ISO/IEC 27001 認証	登録番号: IS 642876 適用範囲: SaaS 提供に関わる企画・開発および運用登録日: 2016 年 3 月 28 日
AWS Partner Network	AWS テクノロジーパートナーセレクト (https://aws.amazon.com/jp/partners/find/partnerdetails/?id=0010L00001jSMEAQA4)

1-2 情報セキュリティへの取り組み

情報セキュリティ方針

項目	内容
情報セキュリティに関する方針	情報セキュリティ基本方針 (https://www.farend.co.jp/profile/security-policy/) にて掲載
情報セキュリティに関する規程	ISO/IEC27001 に適合した社内規程を維持・管理

情報セキュリティ教育

項目	内容
入社時情報セキュリティ教育	全従業員に対して採用時に情報セキュリティ教育を実施

全社員向けの情報セキュリティ教育	年 1 回以上実施
顧客情報保護教育	サポート業務など顧客の情報に触れる社員は年 1 回以上、専用教育訓練を義務付け
システム運用教育	運用中のシステムに触れる社員は年 1 回以上、専用教育訓練を義務付け

改善活動

項目	内容
情報セキュリティ内部監査	年 1 回以上実施
経営陣による見直し	ISO/IEC27001 に準拠したマネジメントレビューを年 1 回以上実施

事業継続活動

項目	内容
事業継続に関する訓練を行っているか	自然災害やその他の事業継続が困難となる状況を想定した訓練を定期的に実施

法令遵守

項目	内容
秘密保持	利用規約第 22 条(秘密保持)において、秘密情報の取り扱いについて定義。また電気通信事業者として登録されており、電気通信事業法により秘密保持を課せられている。
反社会的勢力との関係の断絶	反社会的勢力との関係の断絶に関する表明等をサービス利用規約に明記
個人情報保護に関する方針	個人情報保護方針(https://www.farend.co.jp/profile/privacy/)にて掲載
個人情報保護に関する規程	個人情報保護に関する法律に遵守する社内規程を維持・管理

2.業務環境

社内の業務に関連する規則について抜粋し記載。

2-1 組織・コミュニケーション

項目	内容
従業員の守秘義務に関する誓約	すべての社員より取得済み
インシデント発生時の報告	エスカレーションルール制定済み。全ての報告内容はシステムで記録し必要に応じ再発防止の取り組みを実施

2-2 物理環境

項目	内容
居室入退室管理	セキュリティ要件によりレベルを定めレベルごとの入退室管理を実施
来訪者管理	セキュリティレベルごとに入退室記録を管理
情報漏洩対策	クリアデスク・クリアスクリーン、裏紙使用禁止などのルールを実施

2-3 権限管理

項目	内容
アクセス権限付与方針	役職や担当業務に応じて付与。配属・異動・退職の際に速やかに権限を変更。
情報システムへのアクセス権限付与プロセス	権限変更の申請、権限承認、権限設定の行為者が同一人物にならないように処理し記録を保管。
アクセス権限付与状況の把握	社内ルールに従い権限付与状況のインベントリを実施
共有アカウントを使用した情報システムの使用	原則共有アカウントは禁止。やむを得ず使用する場合は他の情報などで作業行為者が特定可能とする。
特権的アクセス権の付与	上位職者複数名による承認が必要

2-4 端末管理

項目	内容
マルウェア対策	全ての PC に対してセキュリティソフト導入済み
セキュリティソフトパターン更新	提供ベンダーにより随時更新
マルウェアスキャン	ディスク全体への予約検索を 1 回／週実施

最新パッチ適用	随時更新
外部への持ち出し	持ち出し用に指定されたもの以外の PC は社外に持ち出し禁止
暗号化	ノート型 PC は盗難時の情報漏洩の対策のためディスク全体を暗号化
機器廃棄	ディスクの取り出し破壊もしくはサニタイズ処理を実施し廃棄

2-5 媒体管理

項目	内容
社外とのデータの交換	原則ファイル交換システムを使用しファイルを交換
可搬可能な電子媒体の使用	原則媒体を使用したデータ納品の指定がある場合以外は使用不可
紙媒体の取り扱い	裏紙使用禁止。業務で発生した書類はすべて粉砕処理もしくは指定業者による機密文書処理

2-6 ネットワーク管理

項目	内容
業務用ネットワークの制限	IPS を設置し不正な通信からの防御を実施業務上不要な通信ポートを遮断
業務用ネットワークへの接続	認可された機器のみ接続

2-7 開発管理

項目	内容
環境の分離	サービス運用中の環境とその他（開発、検証など）の環境は分離
試験用データ	開発で使用する試験用データは実データ（運用中のデータ）の使用は禁止
変更管理	開発したソフトウェアはすべて指定されたリポジトリにて改変管理を行う

3.サービス仕様

3-1 ファシリティ

使用インフラ

項目	内容
提供者	Amazon Web Services, Inc. （米国）
データセンター	日本国内
所在地	アジアパシフィック (東京) リージョン（住所非公開）

データセンターに関するセキュリティ仕様は Amazon Web Services の web サイトでご確認ください。

link: AWS データセンター
(https://aws.amazon.com/jp/compliance/data-center/)

3-2 サービス

サービス概要

項目	内容
サービス概要	オープンソースのプロジェクト管理ソフトウェア。タスク管理、進捗管理、情報共有等に利用可能。
サービス紹介サイト	https://hosting.redmine.jp
サービス開始時期	2009 年 09 月 07 日
契約数	1200 社以上（2022 年 08 月現在）
契約先	原則非公開（導入事例: https://hosting.redmine.jp/casestudy/ ）
サービス提供先条件	• 日本国内に住所を有すること • 支払いが日本円であること • 口座振替でお支払いの場合は、日本国内の金融機関であること（一部の金融機関を除く） • お問合せや回答、文書でのご案内等弊社との通信（Web サポート、メール、郵便物や電話等）が日本語で対応できること

サービス仕様

項目	内容
URL 形式	サブドメイン形式（ https://[アカウント名].cloud.redmine.jp/ ）
データ容量	スタンダードプラン: 200GB、ミディアムプラン: 400GB
データ所有者	AWS の責任共有モデルをふまえ当社は、OS より上位レイヤーの管理運用について責任を負う。ただし、利用者が Redmine に登録したファイル・データベース情報については、契約者の所有物とする。また Redmine の管理操作（パスワード管理、ユーザ管理等）はご利用の契約者の責任となる。
利用サポート	サポート専用 Web にて対応（24 時間 365 日受付、対応は弊社サポート対応時間内のみ）
サポート対象	利用方法、契約関連、そのほかサービス利用における全般
障害受付	サポート専用 Web にて対応（24 時間 365 日受付、対応はサービス提供全般に関連する内容の際は直ちに調査等開始）
ログの提供	5 ヶ月以内の Redmine のアプリケーション動作ログを提供
契約条件	利用規約を開示 （ https://hosting.redmine.jp/service/terms/ ）
最低利用期間	3 ヶ月
サービス提供に関する契約締結	個別契約の締結は行わない
秘密情報保持に関する個別の契約	同上
サービス提供時間	24 時間 365 日
SLA・SLO	提供無し
計画停止	年間計画等は無し
計画メンテナンスの通知	緊急対応をのぞき 7 日前までに契約担当者様へ電子メールにて通知
サービス提供終了の通知	利用規約に従いサービス停止 30 日以上前に契約担当者様へ電子メールにて通知
サービス稼働率実績・目標	計測および定義無し
障害発生時の通知	サービス稼働状況ページに掲載 https://social.farend.co.jp/@status
過去発生障害	障害ページにて公開 https://hosting.redmine.jp/support/trouble-history/

有料オプション

項目	内容
データの移行	オンプレミスサーバなどで稼働している Redmine の登録データを移行することが可能
データ返却・バックアップ取得	オンプレミスで構築された Redmine などへデータを移行することが可能
削除証明	データ消去報告書によりデータ消去の報告を送付
管理者パスワード再発行	初期管理者 ID のパスワードを仮発行可能
商業登記の登記事項証明書取得	当社の商業登記の登記事項証明書(現在事項証明書・履歴事項証明書)が必要な場合に、お客様に代わって当社で取得し郵送
調査票記入	各種調査票等への記入が必要な場合にご対応

セキュリティ対策等

項目	内容
通信の暗号化	https 通信（TLS1.2 以上を使用）での暗号化通信のみ使用可能
なりすまし使用（不正アクセス）に対する対策	無し
マルウェア対策	アプリケーション動作環境を定期的にリビルドし初期化を実施
接続元 IP アドレスによる接続制限	システム管理者権限を持つユーザーにより任意に設定可能

3-3 アプリケーション

アプリケーション概要

項目	内容
名称	RedMica（レッドマイカ）
概要	プロジェクト管理オープンソースソフトウェアの Redmine の派生アプリケーション。内容は Redmine の最新開発版と同様（参考： RedMica 公式サイト (https://www.redmica.jp/)）
公開サイト	Github (https://github.com/redmica/redmica)
利用フレームワーク	Ruby on Rails
使用 DB	PostgreSQL
アプリケーション脆弱性検査	弊社社内にて定期的に実施

アドオンプラグイン	Redmine Issue Templates, Redmine message customize, My Page Blocks, View Customize, Issues Panel, Redmine IP Filter, UI extension
利用可能テーマ	Redmine 標準, Alternate, Bleuclair, Classic, Farend basic, Farend fancy, こどもれっどまいん緑バージョン

アプリケーション仕様

項目	内容
任意のプラグインの利用	使用不可
カスタマイズ可否	View Customize プラグインにより可能
カスタマイズ依頼	対応不可
API 利用	Redmine 標準の API 利用可能
アプリケーション同時利用可能人数	未計測
アプリケーション管理機能	当社はお客様の Redmine の利用・管理に関与無し。お客様にて管理実施。
システム（OS 等）管理機能	利用者による OS へのログインやミドルウェア類の設定不可
認証強制	管理者にて設定変更可能
二要素認証	時刻同期方式ワンタイムパスワード(TOTP)による二要素認証を設定可能
パスワード最低必要文字数	管理者にて設定変更可能。最大値なし（デフォルト 8 文字）
パスワード必要文字種	大文字・小文字・数字・記号それぞれについて選択可能
パスワード有効期限	管理者にて設定変更可能（デフォルト無制限）
パスワード再設定機能の有効化	管理者にて設定無効化可能
セッション有効期間	管理者にて設定変更可能（デフォルト無制限）

3-4 運用・その他

運用

項目	内容
ベースシステム	Amazon ECS
システム時計	全システム同期（NTP およびクラウドサービス時刻使用）
監視	監視システムによるリソース使用状況およびサーバおよび主要プロセスの死活監視

監視間隔	項目による。最短間隔の項目は 1 分間隔
バックアップ	添付ファイルは変更・削除実施後 31 日保管、データベースはスナップショットを毎日取得 7 世代保管
解約後のデータ削除	サービス解約後約 2 週間後の弊社作業指定日にデータを削除
ログの保管	OS イベント、アクセスログ、アプリケーションログなど 6 ヶ月以上保管
OS・ミドルウェア等パッチ適用	プラットホームはクラウドサービス提供者により管理。一部 Linux システムについてはサービス停止の無い構成としシステムによる自動更新を実施。
アプリケーションバージョンアップ	原則として feature release (3.2.0 → 3.3.0 など真ん中の数字が変わるバージョンアップで新機能追加を伴う)ごとを目標として実施。

セキュリティ対策等

項目	内容
システム構成	提供サービスを構成するシステムのマイクロ化、コアシステムについてクラウドサービス提供マネージドサービス・サーバレスサービスを採用
冗長化	対応
通信制御	クラウドサービス提供のファイアウォール相当機能を設定、クラウドサービス提供の Web Application Firewall を採用
不要プロセスの排除	最小構成の Docker イメージに必要機能のみインストール
通信の暗号化	https（TLS1.2 以上の暗号化に対応）にて利用
データ漏えい・破壊時の補償条件	利用規約第 19 条に、「利用代金月額相当額を限度として責任を負う」 と規定
保存データの暗号化	実施
契約ごとの離隔	インフラを共有。同一プロセスが契約ごとに個別環境変数にて動作。ファイル領域は契約ごとの領域。データベースは契約ごとに個別。
プラットホームの脆弱性調査	クラウドサービスの提供サービスを使用し実施
アプリケーションの脆弱性調査	他社サービスを使用し社内で実施
不正侵入検出などの仕組みの導入	ssh 等のリモートログインの不採用。運用に関するシステムログインはクラウドサービスによる機能を使用しログインを検出・通知。クラウドサービス提供のサービスによりシステムの不正な動作を検出

サービス停止攻撃への対策	クラウドサービス側にて対策を実施
サービス継続に関する仕組み	システムの冗長化、クラウドサービス提供のマネージドサービス・サーバレスサービスの採用、コアシステムについては Rolling Update 方式による更新や提供サービス障害時の自動復旧の実施
ディザスタリカバリ対応	無し

最終更新日

2022 年 8 月 4 日