FlexCRM セキュリティ対策

FlexCRMでは、顧客情報という重要なデータを取り扱うため、以下のセキュリティ施策を行っています。

- ID／パスワードによる認証、二要素認証、SAML認証
- 全てのデータ通信を暗号化（TLS1.3）
- サーバは、AWS（Amazon Web Service）日本国内リージョンを利用
- 時刻同期はAmazon Time Sync Serviceを利用
- 全ての保存データを暗号化（EC2及びRDSについてはAES-256）し、適切に鍵管理（AWS Key Management Service）
- WAF（Webアプリケーション不正侵入防止装置）を採用し、ハッキングやネットワークへの不正アクセスを防止
- アプリケーションレベルのセキュリティホールチェックおよび脆弱性対策を実施
  クロスサイトスクリプティング、SQLインジェクション、コマンド実行脆弱性、ディレクトリトラバーサル など
- 全てのアクセス履歴の保存（180日間）
- デイリーのフルバックアップを7世代まで保存
- 利用制限機能による利用範囲の制限
- IPアドレスによるアクセス制限
- 操作ログの確認機能
- ISO27001認証を取得

  社内ISMSにもとづいた運用体制
  入退室管理、監視カメラによるオフィス内監視、情報資産管理 など

- 国際的な個人情報保護認証制度 TRUSTeを取得

  TRUSTe https://www.truste.or.jp/
  TRUSTeライセンシー確認ページ（FlexCRM）
  https://www.truste.or.jp/hssl/validate/00150.php
- CSPAクラウドサービス認定を取得
  http://www.smb-cloud.org/index.php/cloudservices/

FlexCRM セキュリティ対策

データセンターの安全性

FlexCRMでは、高い信頼性を持つAmazon Web Servises（AWS）のデータセンターを利用しています。
Amazon社が提供するデータセンターであるAWSは、同社が長年の大規模データセンターを運用した経験をもとに設計・構築・運用されており、非常に高い信頼性を持つ認証と認定を受け、多数の豊富な実績があります。

AWSについて

認証と認定

AWSは、ISO27001認証を取得しているほか、Payment Card Industry（PCI）データセキュリティ基準（DSS）のレベル１サービスプロバイダとしても認定されています。AWSは、毎年SOC１監査を受け、米国連邦政府システムのModerateレベルおよびDoDシステムのDIACAP Level２としての評価を獲得しています。詳細についてはAWSセキュリティセンターをご参照ください。

物理的セキュリティ

- AWSのデータセンターはAmazon社が管理する世界中の地理的リージョンに展開してデータを冗長化しており、正式な業務上の必要性を有しているAmazon社の担当者のみが、これらのデータセンターの実際のロケーションを知っています。
- データセンターの構築される場所は、可用性が高く、物理的に洪水の及ばない地域にあります。
- 専門のセキュリティスタッフがデータセンターを24時間365日、常時監視しており、内部に入るのも2段階認証、センター内に入るには常にセキュリティスタッフが付き添うほか、監視カメラ等も常備しています。
- 正規の手続きができる権限を持った従業員のみが物理的サーバーにアクセスでき、アクセス権限は削除するなど徹底しています。
- 従業員の作業の記録はすべて定期的に監査されています。

準拠法

FlexCRMにおけるAWSのデータセンターは、日本国内のリージョン（主に東京リージョン）を選択しておりますが、AWSに関する準拠法は、アメリカ合衆国ワシントン州法、裁判地はアメリカ合衆国ワシントン州キング郡に所在する州裁判所または連邦裁判所となります。

保存されるデータの安全性

FlexCRMのデータベースは、Amazon社が運用する高い信頼性を持つクラウドサーバーを利用しており、独立した電源、空調、ネットワーク環境を持つ異なる複数のデータセンターにまたがって配備されています。 バックアップデータは、通常の運用サーバーとは異なる系統の専用のストレージサーバーへと、日次でデータ全体のスナップショットをフルバックアップとして保持しています。
当社またはAWSにより取得・保存される記録（例：アクセスログ、操作ログ等）については、不正アクセス防止、改ざん防止、アクセス制御、暗号化等の適切な保護措置が講じられています。AWSにおける記録保護の方針や実装内容の詳細については、AWS公式文書をご参照ください。

FlexCRM セキュリティ対策

通信の安全性

FlexCRMの業務アプリケーションが行うサーバーとの通信はすべてTLS1.3により暗号化されており、重要な情報のやりとりも安全です。
TLS 1.3は現時点で広く推奨されている最新の暗号化プロトコルであり、従来のSSL/TLSに比べて強化されたセキュリティと高速な接続性能を提供します。（暗号化アルゴリズムには、ご使用のブラウザが対応する最も強力な暗号方式が選択されますので、可能な限り最新のブラウザでご利用ください）

高度なセキュリティ対策

XSS（クロスサイトスクリプティング）、CRSF（クロスサイトリクエストフォージェリ）、クリックジャッキング、各種インジェクションをはじめとした脆弱性に対する、業界標準の対策をおこなっております。

プライバシー保護

サーバーに保存されているお客様のデータは厳重に管理・運用され、当社の従業員であったとしても、運用に関わるシステム管理者を除いてアクセスができないよう制限されています。 お客様の同意を得たとき、もしくは警察の捜査など、法令に要求される場合などの、特定の極限られた状況を除いてデータを開示することはありません。

お問い合わせ先

株式会社G.FLEX　情報セキュリティ相談窓口
E-mail：support@flex-crm.com

附則
2023年8月8日 制定・施行
2024年3月29日 改訂
2025年7月1日 改訂