CaaS クラウドサービス

セキュリティホワイトペーパー

第 1 版

2025 年 4 月 1 日

株式会社中電工
技術本部　情報通信技術部

目次

１．情報セキュリティの役割および責任

株式会社中電工　技術本部情報通信技術部(以下、当社と表記)は、当社と利用者の情報セキュリティの役割および割り当てについて合意した内容に則り、以下を実施します。

・システムの開発
・データセンターにおける運用保守
・利用者へのシステムの提供
・情報漏洩や改ざんなどセキュリティ事故を防止する
・情報セキュリティマネジメント(ISMS)を確立し、運用する

２．利用者の責任

利用者は、以下のセキュリティ対策を実施する必要があります。

・アカウントの適切な管理
・パスワードの適切な管理

３．データ保管場所

お客さまからお預かりしたデータは、AWS(Amazon Web Service)の日本国内リージョンに保管されます。

４．情報のタグ付け

機能を提供していません。

５．アカウントの種類

CaaS クラウドサービスで利用可能なアカウントは一般ユーザです。

６．メンバーアカウントの登録

お客さまでメンバーアカウントの登録はできません。
サービス利用開始時にログイン ID およびパスワードを発行します。
利用者からパスワード変更の要望を受けた際は、パスワードを再発行します。

７．メンバーアカウントの削除

お客さまでメンバーアカウントの削除はできません。

８．アクセス権の管理

一般ユーザアカウントは参照権限です。アクセス権はお客さまでは設定変更できません。

９．パスワードの管理

パスワードの管理はお客さまご自身で行います。
サービス利用開始時にログイン ID およびパスワードを発行します。

１０．データの暗号化

本サービスで管理・保存するデータは暗号化されていません。
ただし、お客さまのパスワードは暗号化して、保存しています。
また、お客さまと本クラウド間の通信は SSL/TLS による暗号化を実施しています。
当社は、日本国内でサービス提供しており、輸出規制の対象となる暗号化の利用はありません。

１１．データの削除

お客さまがサービス契約を解除された場合、クラウドにおいて、当該データおよびファイルを削除します。
・削除除条件：契約期間が満了し、お客さまから契約期間延長の申し出がなく、業務が終了していること
・削除タイミング：契約終了日から 3 営業日以内
・削除対象：VIX クラウド上に登録または蓄積したデータ・ファイル一式(画像、AI 検知結果、ユーザ情報)

１２．変更管理

お客さまに通知する必要が生じるメンテナンスを伴う仕様変更や仕様追加は影響(システム利用停止等)を含め、事前に通知します。
通知方法：メール
通知時期：メンテナンス実施の 2 週間前

１３．情報のバックアップ

バックアップを取得していません。
必要に応じて、お客さま側でダウンロード等を実施してください。

１４．運用管理

お客様が登録するデータに容量の制限は基本的にありません。リアルタイムでサーバ上の容量・能力を監視し、容量・能力の逼迫状況により、必要に応じてスケールアップを実施いたします。

１５．イベントログの取得

仮想マシン上で稼働するオペレーティングシステム、アプリケーションのログ(イベントログ等)および映像の記録をしていますが、お客さまに提供することはありません。

１６．ぜい弱性の管理

技術的なぜい弱性情報を一般公開情報から取得し、対応が必要と判断した場合は、定期または緊急メンテナンスを実施し、セキュリティを確保します。

１７．セキュリティに配慮した開発

VIX クラウドサービス構築にあたって、セキュリティに配慮した開発手順を実施しています。

１８．情報セキュリティインシデント報告

利用者に大きな影響を与えるセキュリティインシデントが発生した場合には、管理者へ電子メールにて通知します。
情報セキュリティインシデントおよび知的財産権に関するお問い合わせは、CaaS ソリューションサイトに掲載のお問い合わせにて、メールにより受付をしています。

１９．クロックの同期

AWS において NTP を使用し、クロックの同期を実施しています。

以上