ANIPOS Cloud

セキュリティホワイトペーパー

1.5版

株式会社アニポス

1　利用者との責任分界点

株式会社アニポスの責任

株式会社アニポスは、以下のセキュリティ対策を実施します。

- ANIPOS Cloudアプリケーションのセキュリティ対策
- ANIPOS Cloudアプリケーションに保管されたお客様データの保護
- ANIPOS Cloud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

お客様は、以下のセキュリティ対策を実施する必要があります。

- 各利用者に付与された認証情報の適切な管理
- ANIPOS Cloudアカウントの適切な管理（登録、削除、組織管理者権限の付与など）

2　データ保管場所

- お客様からお預かりしたデータは、日本に保管されます。

3　データの削除

- ANIPOS　Cloud利用に関する契約が終了した場合、契約終了時に指示いただいた場合に限り、お客様からお預かりしたデータは完全に消去されます。

4　ラベル付け機能

- お客様の登録する各種情報に対して、任意のラベル付けが可能です。
- ラベル付けを行う時は、「マスタ管理」の「ラベル」より設定ができます。

5　利用者登録および削除

- 管理者権限を保有しているアカウントは「システム管理」の「アカウント」よりアカウントの「登録」、「削除」および「権限の変更」が可能です。
-

6　パスワードの配布方法

- ユーザーを新規登録していただくと、登録したメールアドレス宛に、パスワードの設定を促すURLが記載されたメールを送付いたします。新規登録のユーザーは、そのメールに従ってパスワードを設定してください。
- ユーザーはパスワードを忘れた場合、自らパスワードの再設定をログイン画面から行うことが可能です。対象となるアカウントのメールアドレスを入力することで、パスワードのリセットを行うことが可能です。
- ユーザーは、契約時に送付されたクライアント証明書ファイルをブラウザまたはOSにインストールすることが可能です。

7　暗号化の状況

- データベースに保管される、お客様の各種情報は、適切なアクセス権のもとで保管されます。また、パスワードは、不可逆暗号化(ハッシュ化)された状態で、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。

8　変更管理

- お客様に悪影響を及ぼす可能性のある変更を行う場合は、事前にメールにて通知します。
- また、サービスのバージョンアップが実施された場合、ANIPOS Cloudサポート担当から、サービス登録時に株式会社アニポスにご提供いただいたメールアドレスに対し、メールにてご連絡いたします。

9　バックアップの状況

- データベースに保管される、お客様の各種情報（氏名、メールアドレス、各機能で利用するデータなど）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世代分保管されます。
- 但し、お客様による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。

10　監視機能

利用者と管理者がセキュリティイベントと重要な操作を効果的に追跡できるようにすることを目的として、以下の2つの監視機能が提供されます。

- 利用者の最終ログイン時刻確認機能
- 重要操作のタイムライン機能

保険金処理などの重要な操作を、操作者・操作時刻を含めて、タイムライン形式で表示します。

11 ログのクロックに関する情報

- ANIPOS Cloudサービス内で提供されるログは、タイムゾーンJST(UTC+9)で提供されます。
- ログの時刻は、GCPが提供するNTPサービスと同期しています。

12 脆弱性管理に関する情報

- ANIPOS Cloud開発チームは、システムで利用しているOS、ミドルウェア等に関する脆弱性情報を、定期的に収集しています。
- システムで利用しているコンポーネントに対する脆弱性パッチが公開された場合は、テスト環境での検証を経た後、速やかに適用されます。
- ANIPOS Cloud開発チームが必要と判断した脆弱性情報は、速やかに利用者に通知します。

13 開発におけるセキュリティ情報

- 当社は、お客様のデータとプライバシーの保護に重点を置いています。
- 当社システムにおいては、常に最新の技術と手法を採用して機密情報を保護に努めています。具体的には以下に記載の対策等を実施しています。
  - 外部APIキーや暗号鍵などの機密情報の外部のKMSを通じた暗号化
  - クライアント認証などの多重認証手法
  - 内部・外部ネットワーク上の全通信の暗号化

14 インシデント発生時の対応

- 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、インシデント発生してからお客様の営業時間内であれば3時間以内。営業時間外であれば、翌営業日開始から3時間以内を目標に、ANIPOS Cloud利用契約時にご提供頂いた組織管理者のメールに連絡します。
- 情報セキュリティインシデントに関する問合せは、本セキュリティホワイトペーパー末尾の「ANIPOS Cloudサポート担当」窓口より受け付けています。
- 経過報告については、メールにて行います。

15 お客様データの保護及び第三者提供について

- お客様から預かったデータを適切に保護することは、株式会社アニポスの責任です。ログデータを含むお客様データは、不正なアクセスや改ざんを防ぐため、ANIPOS Cloud開発チームの一部の人間しかアクセスできない、限られたアクセス権のもとで保管されます。
- 但し、裁判所からの証拠提出命令など、法的に認められた形でお客様のデータの提供を要請された場合、株式会社アニポスは、お客様の許可なく、必要最小限の範囲で、お客様情報を外部に提供する可能性があります。

16 適用法令

- お客様と株式会社アニポスとの間の契約は、日本法に基づいて解釈されるものとします。

17 情報セキュリティの独立した監査

- 株式会社アニポスは、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS適合性評価制度における、ISMS認証[1]および、ISMSクラウドセキュリティ認証[2]に準拠した取り組みを行っています。
- 情報セキュリティの自己評価のための内部監査の報告書の開示をご希望の場合は、末尾のお問合せ先までご連絡ください。

18 外部クラウドサービスの利用

- ANIPOS Cloud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	情報
e-SCOTT	クレカ決済	ソニーペイメントサービス	クレカ情報、決済情報 等

[1] https://isms.jp/lst/ind/

[2] https://isms.jp/isms-cls/lst/ind/

Mailgun	メール送信	Mailgun	メールアドレス、メール内容、送信日時 等

改訂履歴

版	改訂日	改訂内容
1.1	2023/05/12	● 初版発行
1.2	2023/06/08	● 表記変更
1.3	2023/09/07	● データベースの暗号化に関する記述を修正 ● 監視機能に関して新たに追記
1.4	2023/09/11	● 脆弱性の利用者への通知について新たに追記
1.5	2023/10/26	● 17項について見出しを変更して詳説

この資料に関するお問い合わせ

株式会社アニポス
ANIPOS Cloudサポート担当
Email：cloud-support@anipos.co.jp