KARTE

KARTE セキュリティホワイトペーパー

2.0 版

株式会社プレイド

1　利用者との責任分界点

プレイドの責任

プレイドは、以下のセキュリティ対策を実施します。

- KARTE のセキュリティ対策
- KARTE に保管されたお客様データの保護
- KARTE の提供に利用するインスタンスにおける、ミドルウェア、OS 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パスワードの適切な管理
- KARTE アカウントの適切な管理（登録、削除、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、GCP 台湾リージョン・東京リージョンおよび、AWS 東京リージョンに保管されます。

3　データの削除

- KARTE 利用に関する契約が終了した場合、お客様の希望に応じて、プレイドは KARTE によって解析されたお客様側のユーザーID が特定できる全てのユーザーデータを削除します。

4　装置のセキュリティを保った処分又は再利用

- KARTE 提供において使用されるサーバー、ネットワーク機器等の装置は、全て AWS・GCP が管理しています。装置の処分・再利用においては、AWS・GCP のポリシー[1]に従い、セキュリティを保った処分・再利用が行われます。

5　容量・能力の管理

- KARTE を構成するサーバー、ネットワークのリソースは 24 時間常時監視されており、必要に応じて自動的にリソースの追加・削減がなされます。

[1]https://cloud.google.com/security/whitepaper
http://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf

6　実務管理者の運用のセキュリティ

- サポートサイト（https://support.karte.io/）をご用意しております。「はじめての方へ」内の「環境・セキュリティ」を参照してください。

7　クラウドサービスの監視

- KARTE の稼働状況・正常性については、ステータスページ（http://status.karte.io/）にて確認することができます。

8　セグメント機能

- お客様は、KARTE に送信された行動情報およびユーザー情報に含まれるデータから、自由に条件を組み合わせてセグメントを作成することができます。

【操作方法】

1. KARTE 管理画面(https://admin.karte.io/)にアクセス
2. 「セグメント」表示の右側にある歯車マークをクリックし「セグメントの管理」をクリックする
3. 任意のセグメントに対して「編集」もしくは右上の「新規作成」をクリックする

9　利用者登録および削除

- お客様は、契約の範囲内において、いつでも自由にユーザーの追加削除を行うことが可能です。

【操作方法】

1. KARTE 管理画面(https://admin.karte.io/)にアクセス
2. 左端の歯車マークをクリックし「基本設定＆決済設定」をクリック
3. 「アカウント/権限管理」をクリック
4. 「メールアドレスで招待」をクリック
5. 追加するユーザーのメールアドレスを入力し、権限を選択した上で「招待」をクリック
6. 招待されたユーザーにメールが送信されるため、メールの指示に従ってユーザーを有効化

10 アクセス権の管理

- お客様は、登録したユーザーの権限を、自由に切り替えることが出来ます。適切な権限グループを設定することで、閲覧・編集を細かく制御することが可能です。

【操作方法】

1. KARTE 管理画面(https://admin.karte.io/)にアクセス
2. 左端の歯車マークをクリックし「基本設定＆決済設定」をクリック
3. 「アカウント/権限管理」をクリック
4. 変更したいアカウントの「権限グループを変更」をクリック
5. 任意の権限グループを選択し、「保存」をクリック

11 パスワードの配布方法

- 管理者ユーザーが、新規ユーザーを追加したと同時に、新規ユーザーのメールアドレスに、初期パスワードを登録するための、一意の URL を含むメールが送信されます。
  新規ユーザーは、その URL にアクセスし、パスワードを入力・設定することで、サービスの利用を開始できます。

12 暗号化の状況

データ

- 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、暗号化されずに、適切なアクセス権のもとで保管されます。但し、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 通信(SHA256)によって暗号化されます。

ファイル

- 接客サービスで利用するためにアップロードされた画像ファイルは、暗号化されずに、適切なアクセス権のもとで保管されます。

13 手順書の提供

- お客様が利用できる手順書は、サポートサイト（https://support.karte.io/）より閲覧することが可能です。

14 バックアップの状況

データ

- データベースに保管される、イベントデータ、解析データは、日次でバックアップを取得しています。

バックアップは、2 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。

ファイル

- 接客サービスで利用するためにアップロードされた画像ファイルは、AWS・GCP のクラウドストレージ内で冗長的に格納されます。ある箇所でデータが破損しても、復元が可能です。

15 ログのクロックに関する情報

- KARTE 内で提供されるログは、UTC（世界標準時）で提供されます。
- 管理画面内の表示に関しては、全て JST（UTC+9）で提供されます。
- ログの時間は、NICT が提供する NTP サービスと同期しています。

16 脆弱性管理に関する情報

- KARTE 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。

17 開発におけるセキュリティ情報

- KARTE システムの開発には、主に node.js が用いられています。開発は、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。

18 インシデント発生時の対応

- KARTE でのインシデントに関する情報は、下記に記載されていますリンク先からご確認することが可能です。
  - http://status.karte.io/

19 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、プレイドの責任です。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、KARTE 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、プレイドは、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。

20 適用法令

- お客様とプレイドとの間の契約は、日本法に基づいて解釈されるものとします。

21 認証

- プレイドは、JIPDEC が運営する ISMS 適合性評価制度における、ISMS 認証を取得[2]しています。

22 サービスのバージョンアップ報告について

- サービスのバージョンアップに伴う変更に関する情報は、下記に記載されていますリンク先からご確認することが可能です。
  - https://karte_support.releasenotes.io/
- また、管理画面内の「ストア」からもご確認することが可能です。

改訂履歴

版	改訂日	改訂内容
1.0	2018/01/01	初版発行
2.0	2018/03/09	一部項目追加

[2] https://isms.jp/lst/ind/CR_IS_x0020_623929.html

この資料に関するお問い合わせ

株式会社プレイド
KARTE サポート担当
support@plaid.co.jp