セキュリティホワイトペーパー

JR 鉄道情報システム株式会社
JRシステム

作成日： 2020 年 12 月 1 日

最新改訂日： 2023 年 4 月 1 日

1　利用者との責任分界点

鉄道情報システム株式会社の責任

鉄道情報システム株式会社は、以下のセキュリティ対策を実施します。

- クラウドサービスアプリケーションのセキュリティ対策
- クラウドサービスアプリケーションに保管されたお客様データの保護
- クラウドサービス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パスワードの適切な管理
- クラウドサービス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、外部システム（Microsoft Azure）の東日本リージョンに保管されます。

3　データの削除

- クラウドサービスの契約が終了した場合、及び試行利用の期限切れの場合、契約終了もしくは期限切れから 60 日以内に、お客様からお預かりしたデータは完全に消去されます。
- 契約終了後及び試行利用の期限切れ後も、当社にて取得したバックアップデータおよびログデータは削除せず当社環境にて保管しますが、バックアップデータ 30 日後に、ログデータは 1 年後に完全に消去されます。

4　ラベル付け機能

全般

- お客様は、勤務・休暇種別設定やスタッフ設定など、任意の名称及びカテゴリを設定することが可能です。
  - ○　「ヘルプセンター」（https://www.otasukeman.jp/helpcenter/）をご参照ください。

5　利用者登録および削除

- お客様は、契約の範囲内において、いつでも自由に利用者の登録・削除を行うことが可能です。
- 「利用者・権限設定」「スタッフ」の画面にて、登録・削除を行うことができます。
  - ○　「ヘルプセンター」（https://www.otasukeman.jp/helpcenter/）をご参照ください。

6　アクセス権の管理

- お客様は、登録した利用者の権限を、自由に切り替えることが出来ます。
- システム管理者、シフト作成者、スタッフの各権限を任意に設定することができ、システム管理者権限では、各種機能の管理画面にアクセスすることが可能です。

7　パスワードの配布方法

- システム管理者が「利用者・権限設定」画面にてシフト作成者を追加したと同時に、登録したメールアドレスに、利用者登録するための一意の URL を含むメールが送信されます。シフト作成者は、その URL にアクセスし、ユーザＩＤ,パスワードを設定することで、サービスの利用を開始できます。
- システム管理者またはシフト作成者が「スタッフ」画面にてスタッフを登録すると、アカウント登録用の QR コードが記載された PDF を出力できます。スタッフはこのＱＲコードをスマートフォンで読み込むとアカウント登録用の画面に遷移し、ユーザＩＤ、パスワードを設定できます。このときメールアドレスも設定します。
- パスワードを忘れた際は、ログイン画面のリンク先に登録済みのメールアドレスを入力することで、パスワード再設定用の URL が発行され、再度パスワード設定を行うことが可能です。

8　暗号化の状況

全般

- 「お客様のパスワード」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。それ以外のデータに関しては、データベースのディスク暗号化を用いて暗号化されています。
- 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 通信によって暗号化されます。
  なお、お客様要望による暗号化形式には対応しておりません。

9　変更管理

- サービスのバージョンアップ情報を始めとした、各種の変更に関する情報は、「お知らせ」より閲覧することが可能です。

10 手順書の提供

- お客様が利用できる手順書は、「ヘルプセンター」（https://www.otasukeman.jp/helpcenter/）より閲覧することが可能です。

11 バックアップの状況

全般

- 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。
- 過去 1 年分の勤務表をダウンロードすることができますが、お客様が設定した情報のバックアップからの復元は承っておりません。

12 ログのクロックに関する情報

- クラウドサービスサービス内で提供されるログは、タイムゾーン UTC で提供されます。
- ログの時間は、インフラ提供者が用意しているタイムサーバと同期しています。

13 脆弱性管理に関する情報

- クラウドサービス開発チームは、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。
- 脆弱性検査は、IPA（独立行政法人情報処理推進機構）が公開する「情報セキュリティサービス基準適合サービスリスト」に掲載された事業者*[1]による脆弱性診断を定期的に行っています。脆弱性を含めた脅威が確認された場合は、速やかに対応いたします。

14 開発におけるセキュリティ情報

- クラウドサービスシステムの開発は IPA をはじめとしたガイドラインおよび、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

[1] 経済産業省が策定した「情報セキュリティサービス基準」への適合性を各審査登録機関により審査され、同基準に適合すると認められた事業者

15 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２４時間以内を目標にお客様に通知もしくは直接連絡します。通知方法はお助けマンの通知ページへの表示もしくはサービスのお知らせ表示にて行います。直接連絡はクラウドサービス利用契約時にご提供頂いた組織管理者のメールもしくは電話いたします。ただし、外部システム（Microsoft Azure）にセキュリティインシデントが発生した場合は、インシデントを知得してから２４時間以内を目標にお客様に通知もしくは直接連絡します。通知方法はお助けマンの通知ページへの表示もしくはサービスのお知らせ表示にて行います。
- 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「勤務シフト作成お助けマンサポート担当」窓口より受け付けています。

16 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、鉄道情報システム株式会社の責任です。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、クラウドサービス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、その他の法的な権限のある官公庁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、鉄道情報システム株式会社は、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。

17 適用法令

- お客様と鉄道情報システム株式会社との間の契約は、日本法に基づいて解釈されるものとします。

18 認証

- 鉄道情報システム株式会社は、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[2]を取得しています。

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

19 外部クラウドサービスの利用

- 当社クラウドサービスでは、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
Microsoft Azure	インフラ構築,運用	Microsoft	メールアドレス等
SendGrid	メール送信	SendGrid	システムから送信するメール

改訂履歴

版	改訂日	改訂内容
1.0	2020/12/1	初版発行
1.1	2021/7/2	13.脆弱性管理に対する情報 に項目追加
1.2	2022/2/1	16.お客様データの保護及び第三者提供について 修正
1.3	2023/4/1	3.データの削除　修正

この資料に関するお問い合わせ

鉄道情報システム株式会社　第二営業企画部　営業開発課

勤務シフト作成お助けマン担当

TEL: 0 3 – 6 3 0 0 – 6 0 8 6

Email：kshift_support@jrs.co.jp