

セキュリティホワイトペーパー

1.1 版

株式会社ハイレゾ

はじめに

- このホワイトペーパー（以下、本書）は、GPUSOROBAN の利用を検討されている方、および、すでに利用いただいている方に向けて、GPUSOROBAN のセキュリティへの取り組みを確認いただくとともに、GPUSOROBAN をセキュアに利用いただくための留意事項を確認いただくことを目的としております。

1 データ保管場所

- お客様からお預かりしたデータは、国内のデータセンターに保管されます。

2 パスワードの配布方法

- ユーザーはパスワードを忘れた場合、ログイン画面から自らパスワードの再設定を行うことが可能です。
- また、パスワードの変更は、会員情報画面から再設定が可能です。

3 暗号化の状況

- 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。
- インスタンスへの接続は SSH を使って暗号化されます。

4 変更管理

- 緊急時を除き、サービスのメンテナンスは原則として 1 ヶ月前にメールにてご連絡いたします。

5 バックアップの状況

- データベースに保管される、お客様の各種情報に対してバックアップは取得しておりません。

6 ログのクロックに関する情報

- 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。

- ログの時間は、パブリックの NTP サービスと同期しています。

7 脆弱性管理に関する情報

- 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、必要に応じて速やかに適用されます。

8 開発におけるセキュリティ情報

- システムの開発は、社内で各プロジェクトごとに合意された開発方針に従って実施されます。

9 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 72 時間以内を目標に、メールにて連絡いたします。
- 情報セキュリティインシデントに関する問合せは、別途お問い合わせフォームより受け付けています。

10 お客様データの保護及び第三者提供について

- 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、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。インスタンスログ及びストレージログは永久保管されます。
- 当社の管理するストレージデバイスなどの装置の処分に関しては、廃棄証明書が入手可能である委託先審査を経た業者に委託して行います。

11 認証

- 株式会社ハイレゾは、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 の国際規格である ISO/IEC 27001(JIS Q 27001)を取得しております。
- 株式会社ハイレゾは、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 クラウドセキュリティ認証である JIP-ISMS517-1.0(ISO/IEC 27017)を取得しております。
- 株式会社ハイレゾは、個人情報保護マネジメントシステムの第三者認証であるプライバシーマーク

の取得準備中です。

12 外部クラウドサービスの利用

- 株式会社ハイレゾでは、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
IDCFクラウド	WEBサーバ	株式会社IDCFフロンティア	・顧客情報 ・インスタンス情報

改訂履歴

版	改訂日	改訂内容
1.0	2022/11/30	初版発行
1.1	2023/5/1	11 認証 (ISMS および ISMS クラウド認証取得の明記)