セキュリティガイドライン

1　利用者との責任分界点

当社の責任

当社は、以下のセキュリティ対策を実施します。

- サービスのセキュリティ対策
- サービス内に保管されたお客様データの保護
- サービス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
- 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　データ保管先

- お客様からお預かりしたデータは、以下のサービスに委託する可能性があります。なお、委託先は、当社の定めた基準を満たした委託先を選定し、適切に当社が管理します。
    - Amazon Web Services
- お客様からお預かりしたデータは、以下の国に保管される可能性があります。

＜日本国内のお客様＞

- 日本

＜海外のお客様＞

- シンガポール

3　装置の安全な処分

- 当社はお客様が利用した装置を廃棄する際には、適切な廃棄専門業者に依頼して確実な廃棄を行います。
- IaaS 等のクラウドサービス環境を利用している場合は、クラウドサービスプロバイダーに装置の適切な処理を確認します。

4　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（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、TLS 通信(SHA256)によって暗号化されます。

5　マニュアルの提供

- お客様が利用できるマニュアルは、Web サイトで閲覧することが可能です。

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、AWS が提供する 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

- 当社は、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、社内で適用時期等の検討を行い、適用する場合は、テスト環境での検証を経た後、速やかに適用されます。

8　開発におけるセキュリティ情報

- 本サービスの開発は、社内の開発メンバーのみがアクセス可能な社内の開発標準に従って実施されます。
- 本サービスの開発は、外部の会社に委託せずに、社内の開発メンバーのみで行います。

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、インシデント発生後、速やかに、障害報告の Web ページで通知します。
- 情報セキュリティインシデントに関する問合せは、サービス毎のカスタマーサポートにより 24 時間 365 日受け付けています。

10 適用法令

- お客様と当社との間の契約は、日本法に基づいて解釈されるものとします。

11 認証

- 当社は、JIPDEC が運営する ISMS 適合性評価制度における、ISMS 認証を取得[1]しています。

[1] https://isms.jp/lst/ind/CR_IS_x0020_586579.html

改訂履歴

版	改訂日	改訂内容
1.0	2017/10/23	初版発行
2.0	2018/1/22	データ保管国を国内・海外に分けて記載