Make Leaps

Security White Paper (ver1.0)

MakeLeaps セキュリティ対策基準による方針と取り組み

本紙に関するお問い合せ
support@makeleaps.com
03-4550-1548
(9:00〜18:00, 土日祝休)

はじめに

MakeLeapsではお客様のデータの安全性を大変重視しており、厳重なデータセキュリティーの確保を軸に弊社の事業や開発を行っております。

本白書では弊社においてユーザーのプライバシーを保護し、委託されたデータの完全性を保証し、データの安全性を確保するための取り組みについて解説します。また、これらを実現するにあたり用いたIT産業において奨励される手法も合わせて記載します。

エンド・ツー・エンドのセキュリティ

本サービスに保管されたデータは下記のいずれかの方法で取得することが可能です。

- アプリケーションのウェブサイト（ウェブブラウザを利用）
- APIのアクセスポイント

すべてのユーザー情報の取得には適切なアカウントでのログインが必要です。権限の無いユーザーが他のユーザーのプライベートデータを取得できないよう、細心の注意を払って対応しています。

MakeLeapsの通信はAES暗号を利用したTLS方式で行われます。これにより第三者によるデータ通信の傍受を防止しています。同時にユーザーセッションの乗っ取りも防ぐこともでき、より確実なユーザー識別を実現しています。

APIの認証とアクセスには業界標準のOAuth2認証プロトコルを使用し、データの安全性を確保しています。APIで接続する各サービスにはアクセストークンの取得が求められます。また、必要に応じてアクセストークンを無効化することも可能です。

ユーザーの管理

MakeLeapsのようなクラウドサービスを使う大きなメリットの一つに、チーム内での簡単かつ円滑な協力体制の実現が挙げられます。同じビジネスアカウントを複数人で共有することで、ビジネス上のすべての書類を一箇所で容易に確認することができます。

本サービスでは利用者ごとに個別のユーザーアカウントを作成することができます。これにより書類の作成や編集、郵送などアクションの履歴をどのユーザーが行ったのか正確に記録することが可能です。また、これらの情報を元に自社のビジネスアカウント内で行われた作業の調査が行えます。

利用者ごとに異なるユーザーアカウントを持つことで、ユーザー名やパスワードを共有する必要がなくなり、重大なセキュリティーリスクの回避も可能です。これによりMakeLeapsの利用者はデータセキュリティーのベストプラクティスを実践することができます。

本紙に関するお問い合せ
support@makeleaps.com
03-4550-1548
(9:00〜18:00, 土日祝休)

ユーザーアカウントを分けることで、他の利用者に影響を与えることなく自社のビジネスアカウントから、特定のユーザーのみを退会させることも可能になります。また、すべてのデータは適切な権限をもったユーザーとしてログインしない限り、閲覧や編集を行うことはできません。

ユーザーアカウントのパスワードはMakeLeapsのシステム上に平文で保管されることはありません。パスワードはソルトやストレッチなどを利用する業界標準の鍵導出関数での変換後に保存されます。

シングルサインオン

本システムはエンタープライズユーザー向けに、サードパーティーや既存のログインシステムを用いた認証も提供しております。認証のエンドポイントとしてSAML（Secure Assertion Markup Language）がサポートされます。このような他の認証システムと連携を通じて、エンタープライズユーザーは各企業のユーザーポリシーに合わせてMakeLeapsへのアクセスや退会の管理が行えます。

ホスティングサーバー

MakeLeapsは世界水準の非常に信頼性の高いサーバー管理、データホスティングサービス上で運営されています。ホスティングプロバイダーは厳格なセキュリティー基準であるSSAE 16 Type IIを満たしており、ユーザーデータの安全性を確保しています。

- データの完全性：すべてのサーバーデータはRAID 10で冗長化されたSSDに保存されているため、ハードウェアが故障した場合においてもデータの紛失を最小限に留めることができます。

- 物理的なセキュリティー：ユーザーデータを保管しているハードウェアへの不正アクセスを防止するため、様々なセキュリティー規則が導入されています。これには生体認証を用いたサーバールームへのアクセス管理や、24時間体制でのセキュリティースタッフの配置などが含まれます。ハードウェアがサービスに利用されなくなった場合には、データストーレッジは厳格なセキュリティー基準のもとに破棄されます。

- システムのセキュリティー：すべてのサーバーにシステムパッチングを導入、最新の修正を迅速に適用することで、常に脆弱性への対応を行っております。また分散型サービス妨害（DDOS）に対しては軽減レイヤーを利用することで、サーバーの安全性をさらに高めています。

- 運用面のセキュリティー：サーバー施設に関わるすべてのスタッフには身辺調査が行われています。また、監査証跡用に従業員の行動は常に記録され、極秘情報に対するアクセスは必要最小限に制限されています。

MakeLeaps

本紙に関するお問い合せ
support@makeleaps.com
03-4550-1548
(9:00〜18:00, 土日祝休)

可用性

重要な業務を行うために、MakeLeapsには非常に高い可用性と安定性がユーザーから求められています。ベストプラクティスとホスティングプロバイダの組み合わせにより、99.9%の可用性を達成しています。

- 電力供給や接続システム等の構成上で重要な項目はすべてN+1冗長方式で運用され、ハードウェア障害が発生した場合でも高い可用性の維持を実現しています。

サーバー構成

柔軟にユーザーからのリクエストに対応するため、MakeLeapsは複数のサーバーによって構成、提供されています。さらに下記の独自の構成要素の追加を行うことでセキュリティーの強化を行っています。

- ホストネットワーク外からの攻撃対象領域を減らすため、使用しているすべてのサーバーには個別にファイアーウォールとポートフィルタリングが設定されています。

- ホストネットワーク内でもすべてのサーバーはVPN（バーチャルプライベートネットワーク）で接続されています。これらサーバー間の通信は暗号化され、ホストネットワーク内のセキュリティーも強化されています。

データの整合性

MakeLeapsには非常に重要なユーザーデータが預けられており、ハードウェア障害を含め、いかなる状況においても整合性を確保するために細心の注意が払われています。またオフサイトサーバーへの継続的なユーザーデータのバックアップも行われております。このバックアップデータからデータベースを復元することで、継続的なサービス提供が可能になります。

郵送代行

弊社サービスの一環として、ご依頼いただいた書類の印刷、日本郵送での郵送代行サービスもユーザーに提供しております。これらの書類に記載された個人情報は厳重に扱われます。

これらの書類へのすべてのアクセスを記録、監査証跡とすることでデータのセキュリティーを確保しております。

セキュア送信

MakeLeapsでは、書類をオンライン上でクライアントに送信するサービスも提供しています。これらの書類は、始めは期限付きのリンクとしてクライアントに送信されます。アクセス権の無い部外者に推測されないよう、このリンクは業界基準の乱数アルゴリズムよって生成されます。

また書類を受け取ったクライアントがMakeLeapsに登録していただくと、その後の送受信はすべてMakeLeaps内で完結するようになり、情報漏洩のリスクをさらに低減します。

マルチテナント

チーム管理システムによって、ユーザーは自社のビジネスアカウントに他のユーザーをチームメンバーとしてメールで招待できます。この際、招待された方のアドレスには専用の招待リンクが個別に送信されます。このリンクは短期間のみ有効であり、業界基準の乱数アルゴリズムで生成されます。また、このリンクは招待が承認されると直ちに失効し、第三者がリンクを利用することはできなくなります。

システム上での他のアクションと同様、ユーザーの招待は履歴に記録され、監査証跡に利用できます。

監査

マルチテナントシステムにより、MakeLeapsではシステム上で行われたユーザーのアクションを監査用に記録しています。また、ユーザー自身もこれらのアクションの記録を閲覧することが可能です。下記の情報がシステムによって記録されています。

- アクションを行ったアカウント
- アクションの日時
- 行われたアクションの情報（書類作成、ユーザーの招待など）

ユーザーデータへのアクセス方針

ユーザーサポートや円滑なサービスを提供するため、MakeLeapsの開発チームや営業チームがユーザーデータにアクセスする必要が生じる場合もあります。ユーザーデータへのアクセスは必要最低限に制限されており、またデータは厳密な部類分けによって、分離が行われております。

本紙に関するお問い合せ
support@makeleaps.com
03-4550-1548
(9:00〜18:00, 土日祝休)