Security White Paper (ver1.2)

MakeLeaps セキュリティ対策の方針と取り組み

本誌に関するお問い合わせ
support@makeleaps.com

はじめに

MakeLeaps では、お客様のデータの安全性を重視しています。厳重なデータ・セキュリティーの確保は、弊社の事業や開発業務の重要な一部です。本書では、ユーザーのプライバシー保護、委託されたデータの完全性確保、及びデータの安全性の実現のための弊社の取り組みについて解説します。また、これらを実現するために IT 産業において用いられる手法についてもあわせて記載します。

エンド・ツー・エンドのセキュリティ

本サービスにおいて保管されるデータには、主に下記のアクセス・ポイントからアクセスが可能です。

- 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

ユーザー情報にアクセスするには、適切にログインすることが必要です。弊社は、無権限者がユーザーのデータにアクセスできないように細心の注意を払っています。MakeLeaps の通信は TLS 方式で行われます。弊社がユーザーにデータを送信し、またはユーザーが弊社にデータを送信する際、この暗号化により第三者によるデータ傍受を防止しています。この暗号化により、ユーザー・セッションの乗っ取りを防ぎ、より確実なユーザー識別を実現することも可能になっています。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・サービスを使うことの大きなメリットの一つに、チーム内での協働、協力が簡単かつ円滑になることが挙げられます。同じビジネス・アカウント上で複数人が作業することにより、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可能になります。

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、郵送など作業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を行うことができます。

本誌に関するお問い合わせ
support@makeleaps.com

利用者ごとに異なるユーザー・アカウントを持つことにより、ユーザー名やパスワードを共有する必要がなくなります。ユーザー名やパスワードを共有することは、セキュリティ上の重大なリスクになりますが、各利用者がユーザー・アカウントをもつことにより、このような重大なセキュリティー・リスクを回避することも可能になります。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できることになります。

ユーザー・アカウントを分けることにより、他のユーザー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、すべてのユーザー・データは適切な権限をもったユーザーが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が MakeLeaps のシステム上にそのまま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による変換後に保存されます。

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廃棄されます。
- 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・パッチングを導入し、最新のアップデート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、秘密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。

本誌に関するお問い合わせ
support@makeleaps.com

可用性

ユーザーの重要な業務を行うため、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。

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 冗長化方式で運用され、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・フィルタリングを設定し、セキュリティーの強化を行っています。

暗号化

MakeLeaps のサービスは、全て暗号化された HTTPS 通信を利用しています。また、バックアップ・データは全て暗号化された状態で保管されます。

データの削除およびバックアップ

自社のビジネス・アカウントを削除すると、過去に作成された全てのデータは削除されます。ただし、バックアップ・データは削除されません。

バックアップは継続的に取得され、最低 5 年間保管されます。バックアップ・データは全て暗号化された状態で保存され、実働環境のサーバとは物理的に別のデータ・センターへ保管されます。

バックアップ・ファイルからの復元プロセスは、自動化されたテストにより定期的に確認されます。

障害からの復旧

システム障害が発生した場合、直ちに運用チームに通知され、可能な限り迅速にサービス復旧に努めます。MakeLeaps では、障害発生を想定した復旧プロセスをあらかじめ定義しています。

本誌に関するお問い合わせ
support@makeleaps.com

ロギング

MakeLeaps では、サービスに関するアクセス・ログや負荷状況等をログに記録しています。これらのログは最低 1 年間保存されます。通常、これらのログはエンド・ユーザへ公開していません。

情報漏洩に対する対応

情報漏洩の可能性を発見した場合について、弊社では報告手順および管理プロセスを整備しています。管理プロセスに基づき、直ちに対策チームを結成し、対応に当たります。

データの完全性

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完全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情報は秘密情報として厳重に扱われます。
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。

本誌に関するお問い合わせ
support@makeleaps.com

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作業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作業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。

- 作業を行ったアカウント
- 作業の日時
- 実施された作業についての情報（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、分別が行われております。