Movable Type クラウド版の「サービスレベル目標」と「お客様で可能な可用性・セキュリティ対策」

シックス・アパート株式会社

2025 年 8 月

Movable Type クラウド版の導入を検討している皆様に向けて、安心して利用を始めていただくにあたり、Movable Type クラウド版の「サービスレベル目標」と「お客様側で可能な可用性・セキュリティ対策」をご案内します。

サービスレベル目標は、別紙「Movable Type (Premium)クラウド版利用許諾契約書」からシックス・アパートの保障と範囲について抜粋及び解説を加えたものです。

お客様側で可能な可用性・セキュリティ対策は、Movable Type クラウド版で行なっている対策と合わせて実施頂くことで、お客様のウェブサイトの安全性・信頼性を全体的に底上げすることを目的としています。

サービスレベル目標

データのバックアップ

1日に1度、Movable Type クラウド版で構築されたお客様環境のバックアップを作成し、お客様が取得できるよう、提供している仮想サーバー内で提供しています。

また、別のクラウドベンダーが提供する国内のストレージサービスにて7世代分のバックアップデータを保管しています。これは、大規模な障害などサービス運営上の問題に備えて行なっているものであり、お客様個別の事由でデータの復元を行えるものではありません。

>> Movable Type (Premium)クラウド版利用許諾契約書 第7条【データの復元】

サービス期間

24 時間 365 日(メンテナンス時間を除きます)

計画メンテナンス

事前にメールで通知します。

>> Movable Type (Premium)クラウド版利用許諾契約書 第5条【サーバーの管理】

サービス品質保証制度(SLA)

定めていません。

>> Movable Type (Premium)クラウド版利用許諾契約書 第15条【保障の限定】

可用性

お客様に提供している仮想サーバーは、サービス基盤となるハードウェアがHA構成（高可用性構成）で構築されており、物理的な障害に対して高い可用性があります。アクティブ-スタンバイ構成のため、物理的な障害時にはサーバーの再起動が発生することがあります。

ディザスタリカバリ

対応していません。

Movable Type クラウド版では、複数のデータセンターを利用してサービス提供を行なっています。ある一つのデータセンターが障害によりサービス提供が困難だと判断した場合には、当社で保持しているバックアップを利用して、稼動している他のデータセンターにて復元し、回復を行なう予定です。

アップデート方針

1. Movable Type のアップデート版のリリース時には、リリース日の早朝までに、自動アップデートが適用されます。自動アップデートの適用時には、プロセスの再起動が行なわれます。
   自動アップデートはお客様が即日適用せず最大30日間延期するよう設定も可能です。
2. Movable Type クラウド版で提供する仮想サーバーで利用するOS、ミドルウェア、ライブラリについては、セキュリティ上の問題にならないよう、随時アップデートを行なっていま

す。アップデートの内容によっては、プロセス、またはサーバーの再起動を伴うことがあります。

3. サーバー環境の大幅な変更(お客様の設定作業が必要となる変更)については、事前にお客様にメールで通知します。
4. シックス・アパートが提供する Movable Type 本体については、クロスサイトスクリプティングやSQLインジェクションなど様々なセキュリティ上の問題に注意して開発を行なっています。
5. 脆弱性が報告された場合、また自ら発見した場合、シックス・アパートは自己の判断でアップデートを行ない提供します。
6. お客様が仮想サーバー内に設置するプラグインやスクリプトについては、お客様がセキュリティ対策を行なってください。

>> Movable Type (Premium)クラウド版利用許諾契約書 第5条【サーバーの管理】

システム監視

運用監視システムで24時間365日サービスの監視を行なっています。運用監視システムがシステム障害を検知した場合、運用監視プロセスに従い、システムの迅速な復旧に努めます。

また、外部から不適切と思われるアクセスを検知したときには、通信を遮断します。

>> Movable Type (Premium)クラウド版利用許諾契約書 第5条【サーバーの管理】

アクセスログ

ウェブサイト、FTPなどのログは、お客様に提供する仮想サーバー上に1カ月間分が保存されており、FTPSを利用して取得することが可能です。シックス・アパートでは過去1年分のログを、当社が管理している国内のストレージサービスに保存しています。必要な場合にはご相談ください。

サポート

サポートは、土曜・日曜・年末年始・休祝日を除くシックス・アパートの営業日に提供しています。マイページ経由でご質問をいただいた後、ご回答までの期間は、3営業日以内を目標にしておりますが、お問合せの内容、混雑具合などによりお時間をいただく場合があります。ま

た、受付時間は平日17:00までとなり、それ以降のお問い合わせは翌営業日受付とさせていただきます。

お客様データの取り扱い

お客様データへのアクセスは、アクセス権限制御管理を行なっています。アクセス権限の所有者は業務執行権限者によって必要最小限の人数が選定されます。

お客様で可能な可用性・セキュリティ対策

バックアップとリストア

1日に1度、同一の仮想サーバー内に、データをバックアップします。意図しない変更を加えてしまったときなどに、Movable Type の管理画面から前日の状態に戻すことが可能です。また、バックアップデータを、自分のパソコンやクラウドストレージサービス等に保管しておくことで、任意の日付のバックアップデータから、リストアを行なうことができます。

https://www.movabletype.jp/documentation/cloud/guide/full-restore.html

管理画面とFTPSのアクセス制限

管理画面のURLを任意のURLに変更することで、悪意のある人間からのサインイン画面URLの推測を難しくします。さらに、管理画面へのアクセスにBasic 認証を掛けることで二重の防御が可能です。また、指定したIPアドレスからのみ管理画面を含む Movable Type のCGIスクリプトやFTPSにアクセスできるよう、制限することができます。

FTPSについては、アクセス可能なIPを127.0.0.1のみに設定する事で、外部からのアクセスを全て制限することも可能です。

https://www.movabletype.jp/documentation/cloud/guide/cfg-security-config.html

ユーザーパスワードの検証ルール

ユーザーがサインインに利用するパスワードの条件を設定できます。

https://www.movabletype.jp/documentation/mt8/admin-guide/manage-system/user-settings/password-validation/

不正サインインに対するアカウントのロック条件の変更

Movable Type にサインインする際、一定の回数以上、ユーザー名とパスワードを間違えると、ユーザーのアカウントがロックされます。これにより、ユーザーアカウントへの辞書攻撃などを防止します。ロックの条件を強化することもできます。

なお、FTPS接続においても不正サインイン対策によるアクセス制限を行なっています。こちらはロック条件の変更はできません。

https://www.movabletype.jp/documentation/mt8/admin-guide/manage-system/system-settings/lockout/

https://www.movabletype.jp/faq/access-restriction-by-mtcloud.html

サインインで多要素認証を利用する

Movable Type の管理画面のサインインで多要素認証を利用することができます。

多要素認証を利用するにはTOTPに対応した認証コードの生成アプリケーション (認証アプリ) が必要です。

https://www.movabletype.jp/documentation/mt8/operations/operation/mfa/

Data APIのアクセス制限

Movable Type には Data API 機能があり、公開状態の記事やウェブページ、コンテンツタイプのデータへのAPIを通じたアクセスを認証なしに可能にします。

Data API を使用しない場合、管理画面のWebサービス設定から「Data API のアクセスを許可する」のチェックを外すことで可能です。サイト毎に設定できます。

https://www.movabletype.jp/documentation/mt8/admin-guide/manage-system/system-settings/data-api/

Data API を一切利用しない場合、環境変数 RestrictedPSGIApp data_api を設定することで、Data API を停止できます。

https://www.movabletype.jp/documentation/appendices/config-directives/restrictedpsgiapp.html

IP アドレス、Basic認証による公開サイトのアクセス制限

任意のディレクトリに対して、Badic認証や特定の IP アドレスからのみ接続を許可する設定が可能です。不正アクセスに対するシンプルな防御となります。また、サイト全体に制限を掛けるとエクストラネットとしての運用も可能になります。なお、管理画面や Data API などへのアクセス制限は、別途行なう必要があります。

nginx プラン

https://www.movabletype.jp/documentation/cloud/guide/cfg-ip-restriction.html
https://www.movabletype.jp/documentation/cloud/guide/cfg-basic-authentication.html

Apache プラン

https://www.movabletype.jp/documentation/cloud/guide/cfg-ip-restriction-apache.html
https://www.movabletype.jp/documentation/cloud/guide/cfg-basic-authentication-apache.html

FTPS パスワードのリセット

Movable Type クラウド版では、国内のウェブ制作業務の実情を考慮し、FTPSアカウントを2つ提供しています。1つを自社で利用するアカウント、もう1つをウェブ制作業務の委託先会社に渡すことで、FTPSアカウントを別に管理することができます。委託先との契約が終了した時点で、委託先に渡したFTPSアカウントのパスワードだけリセットすれば、自社の作業への影響を抑えることができます。

https://www.movabletype.jp/documentation/cloud/guide/cfg-ftps-password.html

異なる公開サーバーを利用する

Movable Type クラウド版では、サーバー上のファイルを、任意の外部サーバーの、任意のディレクトリにFTP(S)で配信することができます。これを「サーバー配信」機能と言います。
サーバー配信機能を用いることで

1. 自社のコンプライアンスルールに適合したウェブサーバーで、ウェブサイトを公開できる。
2. 公開サーバーとステージングサーバーを分けることで、意図しないファイルの公開を防げる。
3. 公開サーバーの一部のコンテンツを Movable Type クラウド版で管理することができる。
4. CMS の利用を隠蔽する。

などが実現できます。併せて、IP アドレス、Basic認証により、Movable Type クラウド版に外部からアクセス・検索エンジンによるクロールができないよう、アクセス制限を設定してください。

https://www.movabletype.jp/documentation/mt8/admin-guide/content-sync/

CDNの導入

急なアクセスの増加に対しては、CDN（コンテンツ配信ネットワーク）を導入することで、サーバー負荷・ネットワーク帯域の逼迫を軽減し、高速で安定したサイト表示が実現できます。当社では、お客様のご要望に応じて Cloudflare CDN、および、Fastly CDN をご提供しています。

https://www.sixapart.jp/movabletype/cloud/#cloud-top-option

https://www.cloudflare.com/ja-jp/
https://www.idcf.jp/cloud/cache/

WAFの導入

お客様のご要望に応じてクラウド型のWAFの併用が可能です。当社では、Cloudflare WAF、および、サイバーセキュリティクラウド社の「攻撃遮断くん」のサーバセキュリティタイプを提供しています。

WAFの導入にあたっては Movable Type クラウド版に特別な設定が必要な場合がありますので、ご相談ください。

https://www.sixapart.jp/movabletype/cloud/#cdn-waf

https://www.cloudflare.com/ja-jp/
https://www.shadan-kun.com/service/

ウイルス検知

Movable Type クラウド版のM8, M16, L8, L16, XL16 プランでは「ウイルス検知オプション」をお客様のご要望に応じて導入可能です。

Movable Type クラウド版のユーザー領域をリアルタイムスキャン、および1日1回の定期スキャンを行ない、万がーマルウェアとしてファイルが検出された場合には、所定のディレクトリへファイルを隔離します。

本オプションを導入していない環境においては、ウイルス対策ソフトは導入しておりません。クライアント側でウイルス対策を行なった上でファイルをアップロードしてください。インターネットからの攻撃については脆弱性対策を行なうことでリスクを低減しています。

https://www.sixapart.jp/movabletype/cloud/#virus-detection

DDoS 対策

Movable Type クラウド版の基盤である、IDCFクラウドのバックボーンネットワーク上にはDDoS対策システムが設置されており、Movable Type クラウド版のすべてのユーザーに適用されています。

https://www.idcf.jp/datacenter/managed/ddos.html

脆弱性検査の実施

お客様提供前の環境については弊社で外部アプリケーションを利用した脆弱性診断を実施しています。

なお、お客様が構築・カスタマイズされた Movable Type クラウド版の環境については、お客様にて脆弱性診断の実施をご検討ください。事前の申請が必要です。

脆弱性検査の結果、FTPプロトコルが有効と判定されることがあります。通常FTPポートとして使用される 21 番ポートは空いていますが、通信内容が暗号化される FTPS プロトコルでのみ利用可能であり、FTPプロトコルは利用できませんので、影響はございません。

https://www.movabletype.jp/faq/perform-security-check-on-cloud.html

メール送信方法の設定と送信ドメイン認証

Movable Type クラウド版からメールを送信する場合、デフォルトではサーバー内の sendmail が使用されます。しかし、昨今のメールセキュリティ対策による影響で、サーバーローカルから送信されるメールに対しても規制や制限の対象になることが増えています。

メールはパスワードの再設定、コメント投稿者の登録、コメントの通知、ユーザーまたはIPアドレスのロックアウト、その他の場合に送信されます。特に、公開サイトにメールフォームなどを設置し、Movable Type クラウド版からメール送信する機会が多い環境では、突然メールが届かなくなる可能性が高くなります。

より確実なメール送信をおこなうため、お客様にて SMTP サーバーを用意し、外部の SMTP サーバーを経由して送信されることをおすすめします。送信ドメイン認証については、SMTP サーバー側で設定・対応をお願いします。

https://www.movabletype.jp/documentation/cloud/guide/cfg-sending-mail.html

プラグインの更新

お客様が構築・カスタマイズされた際に導入した Movable Type プラグインやスクリプトについては、シックス・アパートによるアップデートや脆弱性対策の対象に含まれません。プラグイン提供元より、Movable Typeのアップデートへの対応や脆弱性対応のためのアップデートが行なわれますので、必ず更新情報を定期的に確認しファイルの更新を行なってください。