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

2022 年 6 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 クラウド版のバックアップを作成し、お客様に提供している仮想サーバー内で提供するほか、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、フェイルオーバー機能があり、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を利用してサービス提供を行っています。あるーつのデータセンタ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にて復元し、回復を行う予定です。

アップデート方針

1. Movable Type のアップデート版がリリースされる場合には、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われます。自動アップデートはお客様が適用しないことを選択することが可能です。
2. Movable Type クラウド版で提供する仮想サーバで利用する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、またはサーバの再起動をともなうことがあります。

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い提供します。
6. お客様が仮想サーバ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おり、必要な場合にはご相談ください。

サポート

土曜・日曜・年末年始・休祝日を除くシックス・アパートの営業日となります。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、リストアを行うことができます。

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

管理画面のアクセス制限

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、管理画面を含む、CGI プログラムへのアクセスを制限することができます。

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

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/mt6/users/create.html#stronger-password

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 にサインインするときに、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。

https://www.movabletype.jp/documentation/mt6/users/lockout.html

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/mt7/admin-guide/manage-site/settings/data-api/

Data API を全く使っていない場合、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、BASIC認証や特定の IP アドレスからのみの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が可能です。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、行う必要があります。

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

https://www.movabletype.jp/documentation/mt6/advanced/contents-sync.html

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.cloudflare.com/ja-jp/

https://www.idcf.jp/cloud/cache/

WAFの導入

お客様の必要に応じて、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.cloudflare.com/ja-jp/
https://www.shadan-kun.com/service/

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。お客様のご要望に応じて、有償サービスもご提供できます。

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