

## ご契約者様 各位

アンダーデザイン株式会社  
ShareLine サポートセンター

### 共用サーバサービス Movable Type の XMLRPC API における脆弱性の対応のご案内

平素より格別のお引き立てを賜り、厚く御礼申し上げます。

シックス・アパート社より、Movable Type の特定バージョンにおいて影響を受ける脆弱性が公表されております。本脆弱性を悪用された場合、お客さまサーバ内情報の破壊や改ざん、漏えいなどの影響がでる可能性がございます。お手数ではございますが、弊社サービスにおいて下記に該当するお客さまは、開発者が提供する情報をもとに最新版の Movable Type へのアップデートを行って下さいますようお願い致します。

※十分なテストを実施の上、修正済みバージョンを適用頂けますようお願いいたします。

現状コンテンツが表示されていないお客さまは、.htaccess ファイル、php.ini ファイルが上書きされている可能性がございますので、該当ファイルをご確認、置きなおしにてご対応下さい。

また、今後上記の影響により共用サーバに悪影響が確認された場合、共用サーバ保守会社作業にて、以下の措置をとらせて頂く可能性がございます事、あらかじめご理解、ご了承下さい。

- 不正ファイルのパーミッションはく奪/リネーム
- 海外 Web アクセスブロックを有効化する可能性

※mt-xmlrpc.cgi を正規利用していた場合にサイトが動作しなくなる可能性もございます。ご容赦下さい。

#### 記

#### ■対象のお客さま

- Movable Typeの対象バージョンをご利用のお客さま
- Movable Typeをご利用でない場合も、Webサーバに対象バージョンのインストールをされているお客さま

#### ■脆弱性の影響を受けるバージョン

Movable Type 7 r.5002 およびそれ以前 (Movable Type 7系)

Movable Type 6.8.2 およびそれ以前 (Movable Type 6系)

Movable Type Advanced 7 r.5002 およびそれ以前 (Movable Type Advanced 7系)

Movable Type Advanced 6.8.2 およびそれ以前 (Movable Type Advanced 6系)

Movable Type Premium 1.46 およびそれ以前

Movable Type Premium Advanced 1.46 およびそれ以前

## ■対策

Movable Typeを最新バージョンへアップデートして下さい。

### 【対象バージョン】

Movable Type 7 r.5003 / Movable Type 6.8.3 / Movable Type Premium 1.47

ご契約のプランによっては、自動インストールに別途有償オプションのお申し込みが必要な場合や、自動インストール自体が行えない場合もございます。あらかじめご了承ください。

脆弱性の詳細は下記をご覧ください。

## ■関連情報

### 【シックス・アパート社】

[重要] Movable Type 7 r.5003 / Movable Type 6.8.3 / Movable Type Premium 1.47 の提供を開始  
(セキュリティアップデート)

<https://www.sixapart.jp/movabletype/news/2021/10/20-1100.html>

【JVN】 Movable TypeのXMLRPC APIにおけるOSコマンドインジェクションの脆弱性

<https://jvn.jp/jp/JVN41119755/index.html>

以上