MovableType.net のセキュリティ対策について

2025 年 1 月
シックス・アパート株式会社
カスタマー・リレーション

MovableType.net に関して、以下のセキュリティ対策を行っています。参考情報として、ご参照ください。尚、さらなるセキュリティ向上のため、下記以外の情報は非公開としております。

基本ルールについて

- 所有している PC の台数、状態（使用 OS など）を把握している
- ウィルス対策ソフトを導入し、定期的にウィルス検査を実施している
- OS には可能な限り最新のセキュリティパッチを適用している
- 持ち込み PC の社内ネットワーク利用制限をしている
- 外部記憶媒体を利用する場合は当該業務専用のものを利用し、事前にウィルスチェックを実施している
- 情報セキュリティ対策に関わる管理者が任命されている
- 情報セキュリティに関する教育が継続的に行われている
- 個人情報、機密情報の取り扱いについてルールがある
- 個人情報、機密情報が格納されているコンピュータやサーバー類の管理者、運営者が明確になっており、アクセス制御を実施している
- 個人情報、機密情報を利用者の端末上に残さない設定としている
- システム管理者の行動基準、作業手順が明確になっている
- システム管理者が限定されており、権限も業務遂行上必要最低限のものに限定している
- システム管理者アカウントは個人ごとに発行し、自己の ID/PW は共有しない
- 資格喪失時には速やかにシステム管理者権限を削除している
- 初期 PW は直ちに変更し、その後も定期的に変更している
- 単純なパスワード、推測されやすいパスワードは設定しない
- PW は 8 文字以上とし、英小文字・英大文字・数字・その他記号のうち 3 種類以上を含めること。また、辞書に載っている単語や社名、人名等固有名詞を使用していない
- PW には ID と同一の文字列を使用しない
- 採用や退職の際に守秘義務に関する書面を取り交わすなど、セキュリティに関する就業上の義務を明確にしている
- 障害時の連絡先、復旧対策手順を明確化している

脆弱性について

- バッファオーバーフロー対策を行っている
- SQL インジェクション対策を行っている
- OS コマンド・インジェクション対策を行っている
- パス名パラメータの未チェック／ディレクトリ・トラバーサル対策を行っている
- バックドアとデバッグオプション対策を行っている
- 強制的ブラウズ対策を行っている
- CSRF（クロスサイト・リクエスト・フォージェリ）対策を行っている
- セッションのハイジャック/リプレイ/Fixation 対策を行っている
- クロスサイト・スクリプティング対策を行っている
- HTTP ヘッダ・インジェクション対策を行っている
- 脆弱性診断ツールを導入し、定期的に脆弱性検査を実施している
- 新たな脆弱性が判明した場合、即時に対応を行う体制を整備している

アプリケーションについて

- サービスが停止されないための対策（冗長化など）を行っている
- ID/PW は個人単位で割り当てている
- PW は本人によって変更ができる
- 個人情報を取り扱う場合の通信は暗号化経路を利用している

サーバー管理 PC について

- ウィルス対策ソフトを導入し、定期的にウィルス検査を実施している
- OS およびその他ソフトウェア製品には可能な限り最新のセキュリティパッチを適用している
- 不要なサービスやアカウントを停止または削除している
- サーバー管理用の PC が特定されている
- サーバーへのアクセスは特定の作業者に制限している

サーバーについて

- サーバーの管理者を定めている
- 外部ネットワークと内部ネットワークの分離・独立がされている
- 外部ネットワークに接続する場合、サーバー等を設置しているネットワークとの間にファイアウォールを設置し、アクセスの許可は特定の IP とポートのみに限定している
- DB はインターネットから直接接続できないように設置されている
- インストールされているミドルウェア、ソフトウェアには可能な限り最新のセキュリティパッチを適用している
- OS には可能な限り最新のセキュリティパッチを適用している
- OS やソフトウェアの脆弱性情報の入手と対処を行っている

- 不要なポートの閉塞が行われている
- 不要なサービスの停止が行われている
- サーバーのシステムログ（syslog , su , audit など）は取得できている
- インターネットに接続している Web のアクセスログはすべて取得している
- システムのログを一定期間保存している
- データのバックアップを定期的に行っている
- インターネットに接する Web サーバーに個人情報・機密情報を一時的に格納する場合、暗号化している
- サーバーへのアクセスは暗号化通信を行っている
- サーバーへのアクセスログを一定期間保存している
- サーバーをメンテナンスする経路はサービス用とは異なる回線を使用しアクセス元 IP を制限している
- サーバーをメンテナンスするためのアカウントは適切に保守されている
- 公開鍵認証を使用し、PW 漏洩対策を行っている（PW 認証を使用しない）
- ID は個人単位で割り当てている
- 発行した ID は誰にいつ発行したかを管理しログインログアウトのログを取得、保存している
- ログイン ID が不要になった場合は削除し、定期的に発行ログイン ID のクリーニングを行っている
- ログイン ID ごとに必要な権限のみを付与している
- サーバーの監視は、サービス（アプリケーション）レベルで実施し、異常発見時には、適切な対処を行っている

以上