



# NetMeister ホワイトペーパー

第2.0版

2021年9月28日

NECプラットフォームズ株式会社

## はじめに

NetMeister（以下、本サービス）では、お客様に安心してご利用いただくために、さまざまなセキュリティ対策を実施しています。

## セキュリティ対策

### アカウントロック

3回ログインに失敗すると、同一アカウントでのログインを30分間ロックします。  
機械的な総当たり攻撃による不正ログインを軽減します。

### 自動ログオフ

ログイン後、30分操作がなかった場合、自動でログオフします。  
離席中に第三者に操作されることを軽減します。

### 多要素認証

通常のパスワード認証と併せて、TOTPの多要素認証設定が可能です。  
ログインアカウントとパスワードが漏洩したときの不正ログインを防止します。

### 権限設定

各機能に対する操作権限を自由に設定し、利用者に付与することが可能です。  
役割や職位にあわせた権限を作成し、無用な情報アクセスを軽減します。

## アクセスログ

各機能に対する操作結果は、操作履歴として 365日分 保存します。  
保存された操作履歴を改変することはできません。  
操作履歴のタイムゾーンは、JST 固定です。

## 未利用者へのメール通知

前回ログインから 180日間 ログインがない場合、お客様へ再ログインを促すメールを送信します。  
その後も継続的にログインがない場合は、90日毎 にメールを送信します。

## マルチテナント

複数の企業（グループ）を管理する場合において、グループID ごとにデータを分離して保存し、グループID間のデータ漏洩を防止します。

## セキュリティ強化の取り組み

### Amazon Web Service の利用

NetMeister は、クラウドサービスプロバイダとして Amazon Web Service（以下、AWS）を利用しています。

AWS は、各種セキュリティ監査において認証されており、責任分界点の範囲において安全にサービス提供することが可能です。

### [AWS コンプライアンスプログラム](#)

### ISO/IEC 27001:2013認証取得

当社は、以下の組織を登録範囲として、情報セキュリティマネジメントの認証基準「ISO/IEC 27001:2013」を取得しています。

- 認証登録番号：IS 500597
- 適用規格：ISO/IEC 27001:2013(JIS Q 27001:2014)
- 登録組織：NECプラットフォームズ株式会社
- 適用範囲：
  - 1) 通信機器のレンタルおよび受託配送事業
  - 2) 情報通信機器の統合管理サービス事業
  - 3) web shop運営業務
- 関連事業所：
  - 掛川事業所 [活動範囲：上記1) ]

- 東京本社 [活動範囲：上記1) 2) 3) ]
- 我孫子事業所 [活動範囲：上記1) 2) ]
- 審査機関：BSIグループジャパン株式会社

## セキュリティに配慮した開発ガイドライン

当社で定めたセキュリティガイドラインを満たしていることを確認する工程を定期的実施しています。問題があれば速やかに対処します。

## 脆弱性対応

当社で定めた脆弱性診断ツールによる監査を定期的実施しています。問題があれば速やかに対処します。

## 環境分離

本サービスの開発環境は、お客様が日々ご利用いただいている商用環境とは分離された資源で構成しています。

## 要塞化

使用している仮想マシンにおいて、不要なプロトコル/ポートを遮断し、サーバ内で起動するサービスを最小限にしています。  
ファイアウォールで不正アクセスを遮断し、適切にログを保存しています。

## 継続的なサービス提供

### サービス提供時間

24時間365日 提供します。  
ただし、定期メンテナンス等の計画停止を除きます。

### 計画停止

2週間前に、本サービスダッシュボードのインフォメーションにて通知します。  
ただし、当社が緊急を要すると判断した場合は、事前の通知なくサービスを停止する場合があります。

### サポート時間

平日：午前8:30～午後5:15  
(年末年始、祝日、当社指定休業日除く)

サポート時間外にお問い合わせをいただいた場合、翌営業日以降の受付とさせていただきます。  
上記時間は、日本時間となります。

## 問い合わせ方法

- Web フォーム  
<https://www.necplatforms.co.jp/product/netmeister/inquiry.html>
- メール  
nm-contact@necpf.jp.nec.com

## システム監視

システム監視を常時実施し、障害が発生した場合、当社の運用規定に沿って対応します。  
セキュリティインシデントにおいては、お客様に実害を与えた可能性があるかどうかを判断基準とし、実害があったケースのみ公開します。

障害通知の目標時間は、原則として運用チームが障害を検知から 1時間 とし、本サービスダッシュボードのインフォメーションにて通知します。

## サービスレベル目標 (SLO)

NetMeister Prime をご利用のお客様には、サービス稼働率 99.5% を目標に定め、運用しています。  
ただし、定期メンテナンス等の計画停止を除きます。

無償でご利用いただける NetMeister においては、上記の限りではありません。

## データ管理

### クロックの同期

本サービスは、Amazon Time Sync Service を利用し、高精度な時刻同期を行っています。

### データ保持国

本サービスにおいて、お客様データを保管する国は日本国となります。

### データの暗号化

本サービスで保存および伝送する全てのお客様情報は、暗号化しています。  
お客様のパスワードはハッシュ化し、平文はシステム内に保存されません。

### データのバックアップ

本サービスで保存する全てのお客様情報は、当社が使用するクラウドサービスプロバイダによって分散管理され可用性を担保しています。

特に、以下のデータにおいては、常に過去35日分のスナップショットを保存しています。

- アカウント情報
- グループ情報
- 拠点情報
- 権限情報

## データの消去

本サービスに登録している「装置」を削除した場合、関連する派生データを以下の条件で削除します。

派生データ	削除条件
装置情報	即時
コンフィグ	即時
デバイス情報	即時
インベントリ情報	即時
パケットキャプチャ	即時
UTM統計情報	即時
UTMセキュリティログ	最大90日で削除
アラーム情報	最大60日で削除 (Prime の場合は 365日)
タスク情報	最大60日で削除 (Prime の場合は 365日)

本サービスに登録している「グループ」を削除した場合、関連する派生データを以下の条件で削除します。

派生データ	削除条件
グループ情報	即時 (システム復旧用のバックアップエリアに保存されている情報は、35日後に削除します)
ゼロタッチプロビジョニング情報	即時
操作履歴	最大365日で削除

本サービスの「アカウント」を解約した場合、関連する派生データを以下の条件で削除します。

派生データ	削除条件
アカウント情報	即時 (システム復旧用のバックアップエリアに保存されている情報は、35日後に削除します)

## データの取り扱い

お客様から預かったデータは、利用規約および個人情報の取り扱いに則し、適切に管理します。

## 資源の処分

本サービスでは、物理資源を保有しないため、当社が使用するクラウドサービスプロバイダにて、適切に廃棄される運用となっていることを確認しています。

以上