# MAVIS

PNTL

## ハイブリッド マルチクラウド PAM プラットフォーム

## 課題

### 資産運用管理

社内および社外のネットワーク サービスを提供する過程で、企業はサービス要件を満たすために必然的に対応するサーバーを構築する必要があります。企業のポリシー選択により、仮想マシンを備えたクラウド サービスを使用することも、オンプレミス データ センターを構築することも、ハイブリッド マルチクラウド アプローチを採用することもできます。これらの方法のいずれでも、IT スタッフが追加のレコードを維持し、ユーザー権限を管理する必要があります。これにより、作業負荷が増加するだけでなく、クロスプラットフォーム、クロスマシン操作、およびサードパーティ ツールの必要性により、エラーが発生する可能性が高くなります。さらに、これらのレコードが暗号化されていない場合、企業が脆弱性にさらされるリスクが高まります。これにより、ID 制御の欠如やデータ漏洩により、企業に重大な損失が生じる可能性があります。

### アイデンティティと権限

企業が利用する情報システムにとって、アイデンティティと権限の管理は重大なセキュリティリスクとなります。包括的な管理を実現するには、通常、企業の要件とオペレーターに適した運用設定の両方を満たすために、かなりの人員と綿密な計画が必要です。企業や管理者による定期的なメンテナンスがなければ、システムのアイデンティティや権限が業務プロセスの要件を超えてしまうことは容易にあり得ます。このような状況で、これらのアカウントが盗まれたり漏洩したりすると、機密情報を盗むために使用され、企業に回復不能な損害を与える可能性があります。ハッカーの攻撃が成功するには、特権アカウントの悪用や破壊が伴うことが多く、アイデンティティと権限の保護の重要性が浮き彫りになります。これは、企業が注力すべき重要な側面です。

### 操作ログ

現在のオンプレミス データ センターとクラウド サービスの運用では、ツールの制限により、操作ログや操作の使用プロセスを効果的に記録することが困難になっています。その結果、記録やキャプチャを支援するためにさらに多くのツールが必要になり、一部のファイルの漏れや非効率的な管理につながる可能性があります。これには、ファイル ストレージ管理のための追加のストレージ スペースの必要性、および危機が発生した場合に遡及および検索機能を可能にするために記録ファイルを適切に活用するための十分な保持期間が含まれます。ログや操作記録の保存に加えて、監査や管理も時間や運用管理の問題によって妨げられ、担当者が過去に記録された操作ログを効果的に確認することが困難になっています。このような状況では、確認する必要がある実際のファイルまたは記録を見つけるのに通常かなりの時間が必要です。

## 機能説明

- コンプライアンスとセキュリティ標準
  - A.9 制御および A.12 ログ記録を含む ISO 27001 国際認証要件に準拠しています。
  - NIST CSF 標準、具体的には PROTECT (PR.AC) および Data Protection (PR.DS) を参照します。
  - PCI DSS 標準に準拠しており、3 つの主要領域にわたって項目 2、7、8、10 をカバーしています。
  - IEC 62443-2-1 および IEC 62443-3-3 を含む IEC 62443 国際規格に準拠しています。
- 認証とセキュリティのメカニズム
  - 2 要素認証 (TOTP RFC 6238): 時間ベースのワンタイム パスワードを要求することで、システム ログイン セキュリティを強化します。
  - 証明書管理: 安全で暗号化されたデータ転送のためにプラットフォーム証明書を管理および更新します。
  - 暗号化保護: AES-CBC 128 ビット暗号化を使用し、HTTPS/TLS をサポートして、保存時と転送時の両方で機密データを保護します。
- ユーザーとロールの管理
  - ロールベースのアクセス制御 (RBAC): 資産やサービスへのユーザー アクセスを正確に制御し、許可された担当者だけが特定のリソースにアクセスできるようにします。
  - ユーザー管理: ユーザー アカウントのステータスをリアルタイムで監視および管理し、アカウントを即座に設定または非アクティブ化できます。
  - グループ管理: ユーザー グループを管理し、LDAP システムと同期することで、権限の割り当てを効率化します。
- ジャストインタイムアクセス
  - 最適化された承認プロセス: リクエスト処理を高速化し、精度を向上させます。
  - 柔軟なアプリケーション管理: リクエストの事前送信と変更をサポートします。
  - 透明な履歴記録: 履歴操作データを簡単に表示およびエクスポートできます。
  - クイック再申請機能: 以前のデータを再利用することで新しいリクエストを迅速に処理し、時間を節約します。
  - カスタマイズ可能な通知: 特に繰り返しのリクエストに対して、カスタマイズされた通知条件でセキュリティを強化します。
- リソース、資産、接続管理
  - エージェントレス クラウド統合: エージェント ソフトウェアが不要になり、メンテナンス コストが最小限に抑えられるため、サイバーセキュリティのリスクが軽減されます。
  - クラウド資格情報管理: AWS、GCP、Azure、VMware などのプライベート クラウド プラットフォームのクラウド資格情報を迅速にインポートして管理します。
  - プロジェクト管理: オールインワン フレームワークを使用して複数の資産を効率的に管理し、完全な記録を維持しながら簡単に編集および削除できます。
  - アクセス サービス管理: デバイス接続情報を安全に管理し、ユーザーが機密性の高い資格情報に直接アクセスするのを防ぎます。
  - デバイス管理: 手動およびバッチインポート オプションを使用してサーバー管理を簡素化し、Web インターフェイスを介した迅速かつ直接的な接続を可能にします。
  - Web アプリケーション管理: 自動ログイン機能とドメインのホワイトリストを使用して、AWS、GCP、Azure コンソール、GitHub を集中管理します。
  - データベース管理: 一般的なデータベース (PostgreSQL など) を管理および監視して、データのセキュリティと整合性を確保します。
- リアルタイム監視とログ記録
  - リアルタイム監視: ライブセッションのアクティビティとコマンドの使用状況を監視し、危険な接続を即座に終了できるようにします。
  - ログ管理: アクセス ログ、保持ポリシー、特権アクションなど、ユーザー アクションの包括的なログ記録。Syslog 形式と SIEM システムとのシームレスな統合をサポートします。ユーザー セッションのビデオ ログ記録を提供し、完全なアクティビティ追跡を保証します。
  - システム管理とバックアップ
  - システム管理: システム バージョン情報を承認、管理、および表示します。バックアップ メカニズムにより、システム障害やデータ損失が発生した場合でも回復力が確保されます。高可用性 (HA) 設計により、冗長性と自動フェイルオーバー機能が提供され、ダウンタイムが最小限に抑えられ、システムの信頼性が向上します。
  - 接続設定: 多国籍企業のニーズに合わせて地域設定を調整し、安定した安全なシステム接続を確保します。
  - SIEM 統合: システム セキュリティの監視および対応機能を強化します。

# MAVIS
# ハイブリッド マルチクラウド PAM プラットフォーム

## ソリューション

### コアバリュー

MAVIS ハイブリッド マルチクラウド PAM プラットフォーム - 4 つのコア機能を組み合わせることで、企業のセキュリティ レベルを効果的に強化し、管理ユーザーを支援し、管理の負担を軽減します。

### アイデンティティアクセス監視と管理

MAVIS は、リアルタイムのアクセス管理にゼロトラスト アーキテクチャを採用し、特権アクセスのセキュリティとコンプライアンスを確保します。ジャストインタイム アクセスを統合することで、資産管理の効率と保護がさらに強化されます。

### ハイブリッド マルチクラウド リソース統合

MAVIS は、クラウド全体のすべての IT 資産を一元的に統合および管理します。

### 包括的な記録

MAVIS はすべての接続操作を包括的に記録し、コンテンツの検索を容易にします。

### Webアプリケーションの統合

単一のインターフェイスで、よく使用されるアプリケーションに対応し、共有アカウントの責任に関連する問題に対処します。

### 資産アクセス管理

- MAVIS は、ネットワーク管理デバイスや Linux などの SSH 接続を許可するデバイスや、Windows サーバーなどの RDP デバイスへの接続を可能にします。
- クラウド資格情報管理を介してインポートされたサーバーの他に、ユーザーが手動でサーバーを追加することもできます。その場合、プラットフォーム内で統一された管理を行うには、IP アドレスと関連する設定のみが必要です。
- クラウド マシンをインポートまたは手動で追加した後、サービス管理にアクセスするために接続設定を追加する必要があります。これらの設定には、接続デバイスのアカウント パスワードまたはキーが含まれます。構成が完了すると、接続デバイスはターゲット マシンに直接接続することを選択できます。安全なボールト メカニズムにより、資産接続の機密情報は保護されます。
- MAVIS はプロキシ サーバーを介してターゲット マシンに接続し、SSH 対応または RDP 接続に加えて、SFTP 経由で直接ファイルをアップロードまたはダウンロードできます。これにより、サードパーティ ツールの知識やツールの違いに対する要求が軽減されます。
- さらに、ユーザーはシステム内の Web アプリケーションを管理できます。アカウントとパスワードの管理に加えて、ユーザーはシステムを介してログインできるため、関連する Web ページへのアクセス情報を記録する必要がありません。接続は MAVIS によって記録されます。
- MAVIS を介して接続すると、すべての操作記録が完全に記録され、操作を簡単に追跡できます。ユーザーは、ビデオ再生を介して接続の操作を再生したり、ログでコマンドの詳細を表示したりして、迅速なトレースバックと検索を実現できます。
- MAVIS によって管理されるすべてのデバイスでは、追加のエージェント ソフトウェアのインストールは不要であり、重要な資産に馴染みのないソフトウェアをインストールすることなく、企業にとって最も安全な管理を保証します。
- MAVIS は、操作ログの記録に加えて、システム内のすべての人員操作を完全に記録し、プロジェクトまたはシステムの権限に基づいて分類して簡単に検索できるようにします。

## モジュール

### クラウド認証情報管理

- MAVIS は、AWS、Azure、GCP の 3 大パブリッククラウドとプライベートクラウド VMWare の管理を含むマルチクラウド統合機能を提供します。これは、クラウド証明書のインポートまたは API 経由で実現され、企業資産の迅速な管理を可能にします。
- クラウド資格情報の管理に加えて、ユーザーは MAVIS の管理プロセスを使用して必要なサーバーを選択および管理し、管理上の問題の原因となる過剰な未使用のマシン情報が含まれるのを防ぐことができます。
- ユーザーがインポートおよび管理するマシンを選択すると、MAVIS の自動プロセスによって、MAVIS によって管理されるマシンのステータスがクラウドと同期され、担当者は単一のプラットフォームを通じてマルチクラウド管理を実現できるようになります。

### アイデンティティとアクセス管理

- MAVIS はリアルタイムのアカウント制御を可能にし、管理担当者がアカウントを即座に作成および構成できるようにすることで、効率的なログインと操作を促進します。多要素認証メカニズムは、アカウント セキュリティに複数の保護層を提供し、企業の資産とアクセス権限を効果的に保護します。
- MAVIS は特定の権限制御も提供しており、資産にアカウントまたは ID ごとに異なる権限を割り当てることができます。この責任ベースのアプローチにより、ID と資産の権限を細かく制御しながら、構成エラーに関連するリスクを軽減できます。
- プロジェクトベースの資産管理機能では、資産をプロジェクト構造に従って整理し、分類とタグ付けを簡単に行えるため、多数のデバイスの管理が簡素化されます。管理担当者は、現在のログイン アカウントを効率的に監視できます。有害なアクティビティが開始された場合は、危険な操作の継続を防ぐシステム インターフェイスを通じて、これらの問題に迅速に対処できます。
- 最後に、ジャストインタイム アクセス統合機能により、ユーザーは事前に接続リクエストを送信し、必要に応じて変更できるため、接続管理が強化されます。これにより、承認プロセスの透明性が確保され、迅速な再送信が可能になり、全体的なアクセス管理が合理化されます。