jamf

PCが主流の環境にAppleデバイスを統合するには?

現在、**アイデンティティ（ID）**、**セキュリティ**、**可視性**に関してどのようなシステムをお使いでしょうか?

そのシステムに、新たにAppleデバイスを追加する場面を考えてみてください。**短期間で、多大な労力をかけずに、大きなリスクを冒すことなく**追加できるでしょうか?

現在のシステム環境をそのまま活用し、別個の技術スタックを導入することなくシステムにAppleデバイスを導入できるかどうかを、簡単なセルフチェックで確認してみましょう。

jamf

アクセスと信頼の確認

まずは、現在のアクセスモデルで例外的な設定をしなくてもAppleデバイスをシームレスに使えるかどうかを確認しましょう。

質問:

1. **アクセスポリシー**は、Macユーザと Windowsユーザで共通のものを適用できますか？

2. 組織を再編しなくても、**IDグループ**を使ってポリシーのスコープを調整できますか？

3. **デバイス コンプライアンス**をアクセス可否の判定条件にできますか（ユーザ名とパスワードだけでなく）？

jamf

セキュリティ態勢、検出、対応の確認

次に、現行のセキュリティ運用モデルにAppleデバイスを組み込めるかどうかを確認しましょう。

質問：

1. Appleデバイスのリスクを、Windowsデバイスのリスクと**同じコンソール**で確認できますか？

2. アラートは情報提供にとどまらず、**対応のためのアクションを実行できる**ようになっていますか？

3. Appleデバイスについても、**対応を自動化**できますか（Appleデバイスだけ、手作業による対応が必要になっていませんか）？

jamf

資産と業務フローの確認

さらに、ITの運用や資産のライフサイクルにおいてAppleデバイスの状況全体を（クリーンなデータで）確認できるかどうかも重要です。

質問：

1. **完全なインベントリ**（アプリ、OS、暗号化、所有者）を確認できますか？

2. 余分な作業をしなくても、Apple**エンドポイントを既存のITSMフローに**紐付けられますか？

3. **統合は双方向**（同期とアクションが可能）ですか、それともエクスポートのみの対応ですか？

jamf

統合準備状況のセルフチェック

各カテゴリについて、5段階で評価してみてください。

アイデンティティ（ID）：

- ☐ Appleデバイスに対しても、一貫したアクセス管理とデバイストラストを適用できる
- ☐ グループベースのスコープ設定とライフサイクル自動化が簡単にできる
- ☐ Appleユーザを対象とした例外処理が最小限

セキュリティ：

- ☐ セキュリティの運用フローの中で、Appleデバイスのリスクとセキュリティ態勢を確認できる
- ☐ Appleの宣言型デバイス管理（DDM）により、対応アクションを（単にアラートを出すだけにとどまらず）自動化できる
- ☐ レポートが、社内監査や内部統制の内容に沿っている

可視性：

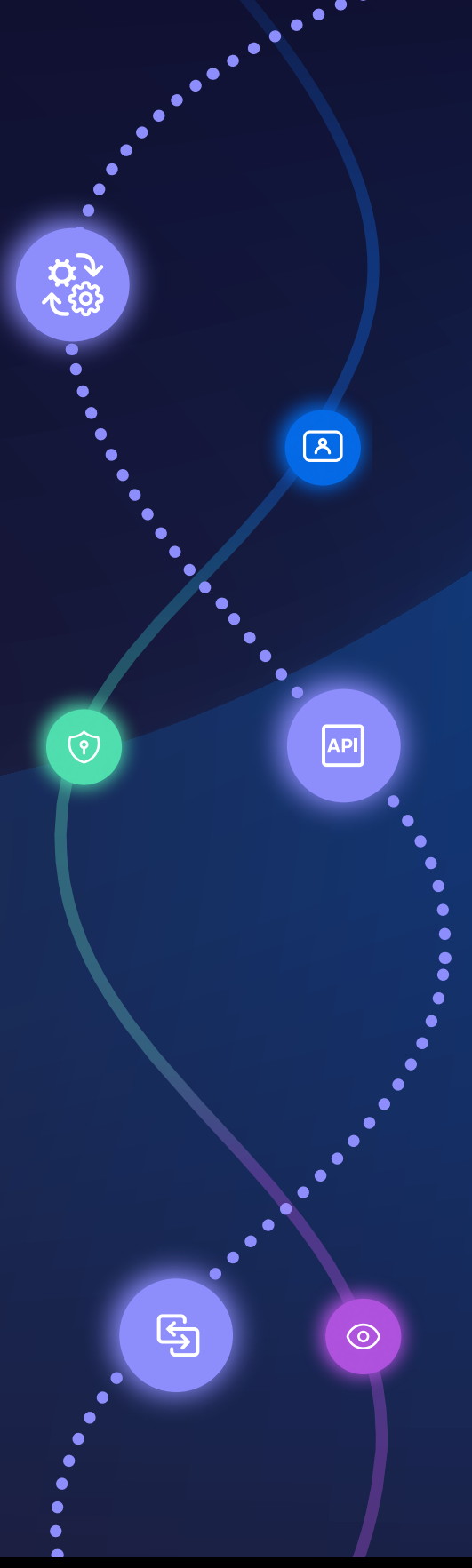
- ☐ Appleのインベントリが完全かつ正確であり、CMDB/ITSMで利用できる
- ☐ （スプレッドシートではなく）デバイスの状態に基づいてリアルタイムでワークフローを実行できる
- ☐ 手作業によるクリーンアップをしなくても、いつでもデータの一貫性が保たれている

いずれかのカテゴリで評価が3を下回っている場合には、手作業による対応が多くなったり、技術的負債が増えたり、大規模展開にスピーディーに対応できなかったりするおそれがあります。

jamf

Jamfで
統合を成功に導く

Jamfなら、**Marketplaceの統合**と**柔軟なAPI**により、アイデンティティ（ID）、セキュリティ、可視性のいずれに関してもAppleデバイスの導入を速やかに進められます。効率的な業務フローを実現しつつ、統合に伴う技術的負債も少ないので、愛用しているツールはそのままに、Appleデバイスを導入・拡張できます。



Jamfは、『IDC MarketScape: Worldwide Unified Endpoint Management Software for Apple Devices 2025–2026 Vendor Assessment』で**リーダー**に選ばれています。