4段階で学ぶMacのコンプライアンス実務

Macのコンプライアンスが重要な理由

リスク抑制
コンプライアンス違反に起因する罰金、法的トラブル、評判の毀損を回避

信頼獲得
セキュリティを適切に管理し、企業の機密データや従業員データを保護

セキュリティ強化
セキュリティギャップを解消し、脆弱性に発展する事態を予防

規制の状況
CIS ベンチマーク、GDPR、HIPAA、NIS2、DORA、ISO 27701

1. 準備

ユーザのアカウントとプロファイル
ユーザの役割を作成し、初期の時点で必要なアクセス権を定義します。

組織のポリシー
関係者間でルール、権限、オーナーシップを調整します。

コンプライアンスのスコープ特定
業界や地域の要件のなかから、どれが適用されるかを特定します。

互換性の確認
デバイス、アプリ、ツールがコンプライアンスに関する組織のアプローチに対応しているかどうかを確認します。

2. 設定と構成

ベンチマークの適用
組織内のデバイスすべてに、CISレベル1またはレベル2を適用します。

構成プロファイル
標準化されたプロファイルを使用し、一貫した設定を適用します。

コアセキュリティ
暗号化、システム保護、アプリ管理機能を有効にします。

3. テストと導入

機能の検証
組織全体に導入する前に、アプリとシステムの機能をテストします。

セキュリティ監査
運用前に、構成と管理の状況を確認します。

パイロットグループ
比較的小規模なグループで、展開を実際に検証します。

オンボーディング
エンドユーザにわかりやすいガイダンスとサポートを提供します。

4. 継続的なメンテナンス

監査
コンプライアンス状況を定期的に監査します。

アップデート
最新のOSとセキュリティパッチを適用します。

モニタリング
脅威とコンプライアンス状態を継続的に追跡します。

調整
規制やポリシーの変化に応じて、管理策を適宜調整します。

Apple製品の可能性を広げる要素

DDMとブループリント
デバイスを自動で正常な状態に維持できるポリシーベースの構成

スマートグループ
ITターゲット設定やアクションの自動化に役立つ動的グループ

コンプライアンスベンチマーク
セキュリティ基準を監査および適用するための内蔵されたワークフロー

Self Service+
エンドユーザが承認されたアプリ、アップデート、重要なデバイスアクションにアクセス

コンプライアンスベンチマーク、ベンチマークの適用ワークフロー、Macのコンプライアンス管理を効率的に進める方法について、詳しくはガイドをご覧ください。

ガイドをダウンロード

www.jamf.com/ja/