

成長企業のIT部門のための Mac管理・セキュリティチェックリスト

IT部門が自信を持ってMacデバイスを導入・構成・保護するための実用的なステップガイド

🔌 1. 導入とセットアップ

- ✓ Apple Business Managerを使用してデバイスを自動登録する
- ✓ 必要な構成プロファイルを適用する
- ✓ 可能であればゼロタッチ初期設定を使用する
- ✓ 明確なオンボーディング手順をユーザに提示する

⚙️ 2. 構成とベースライン

- ✓ FileVault暗号化を適用する
- ✓ アクティベーションロックを有効にする
- ✓ セキュアなベースライン構成を適用する
- ✓ システムの権限と制限を設定する
- ✓ 最小OSバージョンを設定する

🔄 3. アプリとOSのアップデート

- ✓ 必要なアプリを自動的に展開する
- ✓ アプリに最新のパッチが適用された状態を常に保つ
- ✓ 業務への影響が最小限になるようにOSアップデートのスケジュールを設定する
- ✓ 全デバイスのアップデートコンプライアンスを検証する

👤 4. アイデンティティとアクセス

- ✓ MacをクラウドIDプロバイダと統合する
- ✓ ユーザに強力な認証を要求する
- ✓ コンテキストベースのアクセス制御を適用する
- ✓ ユーザの役割に合わせてアクセスレベルを調整する

🛡️ 5. エンドポイントセキュリティ

- ✓ AIとMLによる脅威防御を有効にする
- ✓ デバイスでの検出とブロックを使用する
- ✓ エンドポイント上のリスクのあるアクティビティを監視する
- ✓ インシデントに迅速に対応する
- ✓ 機密性の高いリソースへのアクセスを制限する

📊 6. コンプライアンスと監視

- ✓ 社内で採用した基準に照らしてデバイスをベンチマーク評価する
- ✓ 自動ワークフローを使用してポリシーを適用する
- ✓ コンプライアンス状況を定期的に確認する
- ✓ デバイスがコンプライアンスに違反した場合にリアルタイムでアラート通知する

📧 7. ユーザの意識向上とトレーニング

- ✓ フィッシング詐欺を見抜くためのトレーニングをユーザに実施する
- ✓ 安全な行動と対策を推奨する
- ✓ 不審なアクティビティがあればすぐに報告するよう奨励する
- ✓ オンボーディング時のトレーニングを強化する

管理とセキュリティを統合すれば、IT部門は複雑さを軽減し、企業の成長に合わせてMacデバイスを効果的に保護できます。

「企業の成長に合わせたMacデバイスの管理とセキュリティガイド」もご用意していますので、ぜひダウンロードしてご活用ください。

ダウンロード