jamf

ホワイトペーパー

macOSのセキュリティチェックリスト

Center for Internet Security (CIS) のMac向けベンチマークの導入

macOSのための
セキュリティ推奨事項

macOS向けのCenter for Internet Security（CIS）ベンチマークは、Macのセキュアな運用を行いたいと願う組織のための包括的なチェックリストとして広く知られています。エンタープライズにおけるAppleデバイス管理のスタンダードであるJamfが作成した本ホワイトペーパーでは、CISの推奨事項を組織で実際に導入する方法についてご紹介します。

jamf PRO

JAMF PROとは

Appleデバイスの管理に役立つ複数のツールから構成されるソリューションです。

jamf PROTECT

JAMF PROTECTとは

組織で使用されるMacやApple製品のために特別に設計されたエンドポイントセキュリティソリューションです。

jamf CONNECT

JAMF CONNECTとは

どのデバイスからでも単一のクラウドIDを使って即座に必要なリソースにアクセスすることのできるソリューションです。

CIS Center for Internet Security®

CENTER FOR INTERNET SECURITY（CIS）とは

非営利の501(c)(3)組織であるCenter for Internet Security, Inc.（CIS）は、公営機関や民間企業のサイバーセキュリティに対する準備および対応能力の強化にフォーカスを当てた活動を行っています

CISベンチマーク誕生の経緯

CISベンチマークは、専門家によるコンセンサスレビュープロセスを経て作成されています。このプロセスでは、コンサルティング、ソフトウェア開発、監査、コンプライアンス、セキュリティリサーチ、オペレーション、行政、法務など、多様な分野の専門家がそれぞれの見地から意見を述べます。

各ベンチマークの決定においては、このコンセンサスレビューが2段階で実施されます。最初のコンセンサスレビューは、ベンチマークの策定に取り掛かる段階で行われます。専門家が集まってベンチマークの草案の考察、作成、検証を行い、ベンチマークの推奨事項についてコンセンサスが得られるまで議論が続けられます。2回目のコンセンサスレビューはベンチマークが公開された後に実施され、コミュニティから提供されたフィードバックがコンセンサスチームによって検討され、ベンチマークに反映されます。
コンセンサスプロセスへの参加に興味がある方は、**https://community.cisecurity.org**をご覧ください。

JAMF PROTECTとCIS

Jamf Protectは最近、CISからCISベンチマーク認定を受けました。
これにより、Jamf Protectを使用する組織は、CISベンチマークのベストプラクティスに沿ったmacOSデバイスの構成を行うことができます。

CISは、macOSに関連する複数カテゴリにおいて、データ流出の可能性を減らすための設定に関する推奨事項を提供しています。

Jamf ProにCISの推奨事項に従うための機能やツールが含まれている一方で、Jamf Protectは、CIS関連のセキュリティ設定を日常的かつ自動的に評価する機能を備えており、macOSのベンチマーク全般と組織のセキュリティの優先事項の観点からコンプライアンスステータスや監査の見落としを確認することができます。

macOSセキュリティのカテゴリ


アップデート&パッチ


システム設定


ICLOUD


ログ作成と監査


ネットワーク構成


ユーザアカウント


アクセスと認証


その他の考慮事項

アップデート、パッチ、セキュリティソフトウェアのインストール

Jamf Proでは、アップデートをパッケージ化し、リモートでクライアントMacに導入することで、macOSとアプリケーションを最新の状態に保つことができます。さらに、リアルタイムでOSアップグレードのステータスを監視し、もっとも最新かつセキュアなOSがフリート全体に搭載されていることを確認するためのレポートを作成することもできます。

CISベンチマークの推奨事項

- Appleが提供するすべてのソフトウェアを最新の状態に保つ
- 自動アップデートを有効にする
- アプリのアップデートのインストールを有効にする
- システムデータファイルとセキュリティアップデートのインストールを有効にする
- macOSアップデートのインストールを有効にする

Jamf Proの機能

- macOSアプリやよく使用されるアプリを最新の状態に保つためのパッチ管理機能
- カスタマイズ可能なソフトウェアアップデートサーバで承認済みのアップデートが登録されたホワイトリストを作成
- App Store経由の自動アップデートを有効にするポリシーの実行
- クライアントMacでアップデートをチェックするポリシーの実行

Jamf Connectの機能

- クラウドIDプロバイダのユーザ名とパスワードの要求
- ゲストアカウントの非表示化
- ローカルアカウントでのパスワードヒントの不使用

Jamf Protectの機能

- 上記のすべての設定を評価して、アップデート、パッチ、セキュリティソフトウェアのコンプライアンスを検証

システム設定

Jamf Proは、組織のセキュリティニーズに合わせてシステム設定を構成するための手助けをしてくれます。Macフリート全体に共通の設定や詳細設定を適用することができ、物理的攻撃とリモート攻撃の両方に対してセキュリティを強化することができます。

CISベンチマークの推奨事項

Bluetooth

- Bluetoothを無効にする
- Bluetooth検出可能モードを無効にする

日付と時刻

- 日付と時刻の自動設定を有効にする
- 時間の設定が適切な範囲内で行われていることを確認

デスクトップとスクリーンセーバ

- スクリーンセーバの待ち時間を20分以内に設定する
- スクリーンセーバのコーナーを保護する
- 画面ロックツールやスクリーンセーバを開始するコーナーについてユーザを教育する

共有

- 「共有」でApple Eventsのリモート操作を無効にする
- インターネット共有を無効にする
- 画面共有を無効にする
- プリンタ共有を無効にする
- リモートログインを無効にする
- DVDまたはCDの共有を無効にする
- Bluetooth共有を無効にする
- ファイル共有を無効にする
- リモートマネージメントを無効にする

省エネルギー

- ネットワークアクセスによるスリープ解除を無効にする

プライバシーとセキュリティ

- FileVault を有効にする
- すべてのユーザストレージのAPFSボリュームを暗号化する
- すべてのユーザストレージのCoreStorageボリュームを暗号化する
- Gatekeeperを有効にする
- ファイアウォールを有効にする
- ファイアウォールのステルスモードを有効にする
- アプリケーションのファイアウォールルールを見直す
- 位置情報サービスを有効にする
- 位置情報サービスのアクセスを監視する
- 診断データと使用状況データのAppleへの送信を無効にする

その他

- iCloud (以下のセクションを参照)
- Time Machine自動バックアップ
- Time Machineのボリュームを暗号化する
- リモコンの赤外線レシーバー有効になっている場合はペアリングする
- 「ターミナル」で安全なキーボード入力を有効にする
- Java 6をデフォルトのJavaランタイムにしない
- 必要に応じてファイルを安全に削除する
- EFIのバージョンが有効で定期的にチェックされていることを確認する

Jamf Proの機能

- Jamf Proのサーバポリシーまたは構成プロファイルによる、上記のすべてのシステム項目の設定
- Jamf Proサーバのインベントリで FileVault2を有効化およびキーをエスクロー
- スクリーンセーバーとパスワードの設定
- 共有の設定
- プライバシーとセキュリティの設定
- Javaを無効化するポリシーの導入

Jamf Protectの機能

- 上記のすべての設定を評価してシステム設定のコンプライアンスを検証

iCloudとその他のクラウドサービス

Jamf Proは、クラウドベースのサービスをブロックまたは有効にする能力をIT管理者に与えることにより、組織のiCloud戦略を支援します。

CISベンチマークの推奨事項

AppleのiCloudは、データの保存や、Apple ID（Appleアカウント）に紐づけられたデバイスの検索、制御、バックアップを行うための、消費者向けのサービスです。エンタープライズデバイスでのiCloudの使用は、管理対象デバイスのための利用規約や、ユーザが扱うデータの機密性に関する要件に沿って行う必要があります。iCloudの使用が許可されている場合、Appleサーバにコピーされたデータは、個人デバイスだけでなくエンタープライズデバイスにも複製されます。

iCloud

- iCloudの構成
- iCloudのキーチェーン
- iCloud Drive
- iCloud Driveのドキュメント同期
- iCloud Driveのデスクトップ同期

Jamf Proの機能

- 構成プロファイル経由でiCloudを無効化
- iCloudが許可されていない場合、Finderから削除可能

Jamf Protectの機能

- 上記のすべての設定を評価してiCloudおよびその他のクラウドサービスのコンプライアンスを検証

ログ作成と監査

Jamf Proでは、macOSによって生成されたログを追跡し、それらを一括管理することができます。また、ログに関する詳細なレポートを出力して、セキュリティ上の問題の発見に努めることも可能です。

CISの推薦事項

- セキュリティ監査を有効にする
- セキュリティ監査フラグを構成する
- セキュリティ監査を確実に保管する
- 監査記録へのアクセスを管理する
- install.logを1年以上保管する
- ファイアウォールがログを記録するように構成する

Jamf Proの機能

- スクリプトによる構成プロファイルの変更
- Jamf Proサーバへのログファイルの送信と無期限の保管
- Jamf Proサーバによる追加ログのキャッシュ化

Jamf Protectの機能

- 上記のすべての設定を評価してログ記録と監査のコンプライアンスを検証

ネットワーク構成

Jamf Proでは、Wi-Fi、VPN、さらにはDNS 設定までも配布することができるため、ネットワーク構成の導入が非常に簡単です。また、macOSの旧式のサーバコンポーネントを一部無効にすることができ、ユーザが間違って不要なポートを開ける心配もなくなります。

CISの推薦事項

- Bonjourサービスを無効にする
- Wi-Fi状況アイコンをメニューバーに表示する
- ネットワーク特定のロケーションを作成する
- httpサーバを使用しないようにする
- nfsサーバを使用しないようにする

Jamf Proの機能

- ネットワーク設定を構成プロファイルに組み込み可能
- Jamf Proのサーバポリシー経由でApache, FTP, NFSを無効化

Jamf Protectの機能

- 上記のすべての設定を評価してネットワーク構成のコンプライアンスを検証

ユーザアカウントと環境

Jamf Proでは、Macでローカルアカウントの管理が可能なため、管理者や一般ユーザの作成ができます。また、クライアントマシンにインストールされたJamfバイナリが、管理者権限を持つ隠れ管理アカウントを作成できるため、コマンドを実行したり新規ユーザを作成したりすることもできます。さらに、ログイン画面の安全性を高めたり、ゲストアカウントを無効にしたりするためのポリシーを作成することも可能です。

CISベンチマークの推奨事項

- ログイン画面には名前とパスワードのフィールドのみを表示する
- パスワードのヒント表示を無効にする
- ゲストユーザのログインを無効にする
- ゲストユーザに共有フォルダへのアクセスを許可するオプションを無効にする
- ゲストユーザのホームフォルダを削除する
- 拡張子を有効にする
- Safariで安全なファイルを自動的に実行するオプションを無効にする
- Safariでのインターネットプラグインの汎用を無効にする
- 一元管理されていないシステムにはペアレンタルコントロールを使用する

Jamf Proの機能

- 構成プロファイルでログイン画面を構成
- Jamf Proのサーバポリシー経由でゲストアカウントを無効化
- 設定アシスタントとApple Business Managerへの登録を通じてユーザアカウントを作成
- ニーズに合わせて標準アカウントまたは管理者アカウントを作成

Jamf Protectの機能

- 上記のすべての設定を評価してユーザアカウントと環境のコンプライアンスを検証

システムアクセス、認証、および認可

Jamf Proでは、ファイル権限、厳しいパスワードポリシー、キーチェーンアクセスの管理などの設定が可能です。構成プロファイルやJamf Proのサーバポリシーを作成することで、システムへのアクセス設定をリモートで有効にし、Macをよりセキュアに運用することができます。

CIS 推奨事項：

ファイルシステムの権限とアクセス制御

- ホームフォルダの安全性を確保する
- システム全体のアプリケーションに対して適切な権限が設けられているか確認する
- システムフォルダに誰でも書き込み可能なファイルがないか確認する
- ライブラリフォルダに誰でも書き込み可能なファイルがないか確認する

パスワード管理

- アカウントのロックアウトしきい値を構成する
- パスワードの最小文字数を設定する
- アルファベットを含む複雑なパスワードを要求する
- 数字を含む複雑なパスワードを要求する
- 特殊文字を含む複雑なパスワードを要求する
- 大文字と小文字を含む複雑なパスワードを要求する
- パスワードの有効期限
- パスワード履歴
- sudoのタイムアウト時間を短くする
- ユーザとttyの各コンビネーションに対して個別のタイムスタンプを使用する
- ログインキーチェーンが使用されていない時に自動的にロックする
- コンピュータがスリープ状態の時はログインチェーンがロックされるようにする
- OCSPおよびCRLで証明書をチェックする
- rootアカウントを有効にしない
- 自動ログインを無効にする
- コンピュータのスリープ状態やスクリーンセーバを解除する際はパスワードの入力を必須にする
- セープスリープを有効にする
- システム全体の設定にアクセスする際は管理者パスワードの入力を必須にする
- 他のユーザの（アクティブまたはロックされた）セッションへのログインを無効にする
- ログイン画面のバナーを作成する
- パスワードヒントを無効にする
- ファストユーザスイッチを無効にする
- キーチェーンやアイテムを個々に保護する
- 目的ごとに異なるキーチェーンを作成する
- システム整合性の保護ステータス

Jamf Proの機能

- 権限修復コマンドをSelf Service経由でトリガー、または自動的に実行
- システムおよびライブラリ内の不正な権限をチェックするためのレポートを作成
- 構成プロファイル経由でパスワードポリシーを有効化
- Jamf Proサーバポリシー経由でログイン画面とバナーを追加
- Jamf Proサーバポリシーのスクリプトでフォルダ権限を設定

Jamf Connectの機能

- クラウドIDプロバイダのポリシーに従って複雑なパスワードを要求するログイン画面用のカスタムメッセージを作成

Jamf Protectの機能

- 上記のすべての設定を評価して、システムアクセス、認証、および認可のコンプライアンスを検証

その他の考慮点

Jamf Proでは、EFIパスワードの設定やセキュリティ要件が厳しい環境でのWi-Fiの無効化など、セキュリティ設定の高度なカスタマイズが可能です。また、Jamf Proサーバを使用してMacの名前を変更することも可能なため、インベントリ管理がさらに簡単になります。加えて、組織所有のソフトウェアのインベントリやライセンスの管理も可能です。

CISベンチマークの推奨事項

- macOSのワイヤレステクノロジー
- iSightカメラのプライバシーと機密性への注意
- コンピュータの名前に関する考慮
- ソフトウェアインベントリに関する考慮
- ファイアウォールに関する考慮
- 光学メディア関連の自動アクション
- 他のMacで購入されたApple Storeアプリの自動ダウンロードに関する考慮
- EFIパスワード
- AppleIDを使ったFileVaultとローカルアカウントのパスワードリセット
- アクセス権限の修復はもはや必要なし
- App Storeのパスワード設定
- macOSでのSiriの使用
- macOSで使用できるApple Watchの機能
- リモートコンピュータへのシステム情報のバックアップ
- 統合ログ作成
- AirDropのセキュリティ

Jamf Proの機能

- Wi-Fiを構成プロファイル経由で無効化
- Jamf Proサーバ経由でコンピュータ名の作成を自動化
- Jamf Proサーバ経由でソフトウェアインベントリとライセンスを追跡
- ポリシー経由でEFIパスワードを設定

Jamf Protectの機能

- 上記のすべての設定を評価して、その他の考慮点に関してコンプライアンスを検証

まとめ

Jamfを使用することで、CIS（Center for Internet Security）のmacOS向けベンチマークを簡単に採用することができます。

jamf

www.jamf.com/ja/

セキュリティのベストプラクティスに興味のある方は、ぜひJamfの無料トライアルに **お申し込みください。**