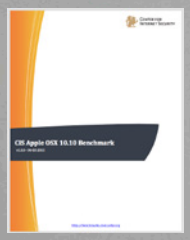


Mac OS X のセキュリティチェックリスト:

OS X 向け Center for Internet Security ベンチマークの導入

Mac OS X の安全性に関する提言

OS X 向け Center for Internet Security (CIS) は、組織がMac デバイスの安全性を確保するうえで確認すべき総合的チェックリストとして広く知られています。そこで Apple デバイス管理のエキスパートである JAMF Software は、本ホワイトペーパーを通じて、このチェックリストの活用方法をご紹介します。

Casper Suite とは?
Casper Suite は Apple の各デバイスを管理するためのツールをセットにしたものです。

JSS とは?
JAMF Software Server (JSS) は Casper Suite の管理サーバーコンポーネント

Policy とは?
クライアント Mac に変更を適用する際に使用するメインツールです。JSS はその Mac のエージェントにコマンドを送信します。

Center for Internet Security

CIS とは?
Center for Internet Security, Inc (CIS) は、公的および民間機関におけるサイバーセキュリティへの対応力を強化することを目的とした非営利組織です。

CIS ベンチマークの作成プロセス

CIS ベンチマークは、専門家によるコンセンサスレビューを経て作成されています。このレビューでは、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、セキュリティ調査、運営、行政、法務など、さまざま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際に実施されます。この段階で、そのテーマの専門家が召集され、ベンチマーク案について議論や立案、テストが行われます。この議論は推奨されるベンチマークについて全員の意見が一致するまで行われます。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ます。ここでは、インターネット上で提示されたすべてのフィードバックを対象に、そのベンチマークに取り入れるべきものについて、レビューが行われます。このコンセンサスプロセスへの参加に関心をお持ちの方は、https://community.cisecurity.orgまでご連絡ください。

- CIS Apple OS X 10.10 ベンチマーク

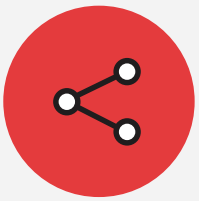
OS X 向けセキュリティのカテゴリー


アップデートとパッチ


システム設定


iCloud


ロギングと監査


ネットワーク構成


ユーザーアカウント


アクセスと認証


その他の考慮点

アップデート、パッチ、セキュリティソフトのインストール

Casper Suite を使用すれば、アップデート内容をパッケージングして遠隔操作にてクライアントの Mac デバイスに適用できるため、OS やアプリケーションを常に最新の状態に保つことができます。また、各デバイスのアップデートの完了/未完了に関する情報もレポートとして取得できます。

CIS の推奨：

- ソフトウェア・アップデート・ツールにて OS およびアプリケーションを最新の状態に保つ
- App Store の自動アップデートを有効にする
- 自動セキュリティアップデートを有効にする

Casper Suite の特徴：

- Casper Suite のパッチ管理機能により、Mac OS X を常に最新の状態で使用可能
- カスタマイズ可能なソフトウェア・アップデート・サーバーにて、Mac に適用可能なアップデート項目をホワイトリスト化できる
- App Store 経由で自動アップデートを有効にするポリシーを実行可能
- クライアント Mac のアップデート状況をチェックするポリシーを実行可能

システム設定

Casper Suite では、お客様のセキュリティニーズに合わせたシステム設定を行うことができます。パスワードやスクリーンセーバーといった共通の設定も遠隔操作で手間なく一斉に実施できるため、Mac のある場所まで出向く必要性を最小限に留めることができます。SSH やファイル共有の無効化といった高度な設定も可能なため、Mac を外部の攻撃から保護できます。

CIS の推奨：

Bluetooth：

- Bluetooth を無効にする
- Bluetooth 発見可能モードを無効にする

日付と時間：

- 日付と時間の自動設定を有効にする

デスクトップとスクリーンセーバー：

- スクリーンセーバーの設定は待ち時間を20分以下にする
- ホットコーナーにスクリーンセーバーの開始を設定する
- スクリーンセーバーより大きな値で「ディスプレイのスリープ」を設定する

共有：

- 共有のリモート Apple イベントを無効にする
- 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（SSH）を無効にする
- DVD や 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
- リモート管理（ARD）を無効にする

エネルギーセーバー：

- Wake for network access を無効にする
- 電源接続時のコンピュータ・スリープを無効にする

セキュリティとプライバシー：

- FileVault 2 を有効にする
- Gatekeeper を有効にする
- ファイアーウォールを有効にする
- ファイアー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・ファイアーウォールのルールを見直す
  (https://support.apple.com/ja-jp/HT201642)

その他：

- iCloud（以下のセクションを参照）
- Terminal.app でのセキュリティ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
- 「確実にゴミ箱を空にする」を利用する

Casper Suite の特徴：

- 上記のシステム設定はすべて JSS Policy または構成プロファイルにて設定可能
- FileVault 2 の利用が可能で、鍵は JSS のインベントリーに供託される
- スクリーンセーバーおよびパスワードの設定が可能
- 共有設定が可能
- セキュリティとプライバシーに関する設定が可能
- Java を無効化できるポリシーの適用が可能

iCloud およびその他のクラウドサービス

Casper Suite は、御社の IT 管理者にクラウドベースのサービスの有効化またはブロックの権限を与えることで、御社の iCloud 戦略の遂行を支援します。

CIS の推奨：

「Apple の iCloud は、複数のプラットフォームにてデータを同期させるために使用される多くのクラウドソリューションの一つに過ぎないため、
自社環境の他のクラウドサービスと合わせて制御することが求められます。事業目標の達成に向けて最良のデータ保護体制を確立できるよう、従業員を巻き込んでアクセス条件を設定しましょう」

Casper Suite の特徴：

- iCloud は構成プロファイルまたは JSS Policy にて無効化が可能
- iCloud が無効であれば、Finder から iCloud Drive の削除が可能

ロギングと監査

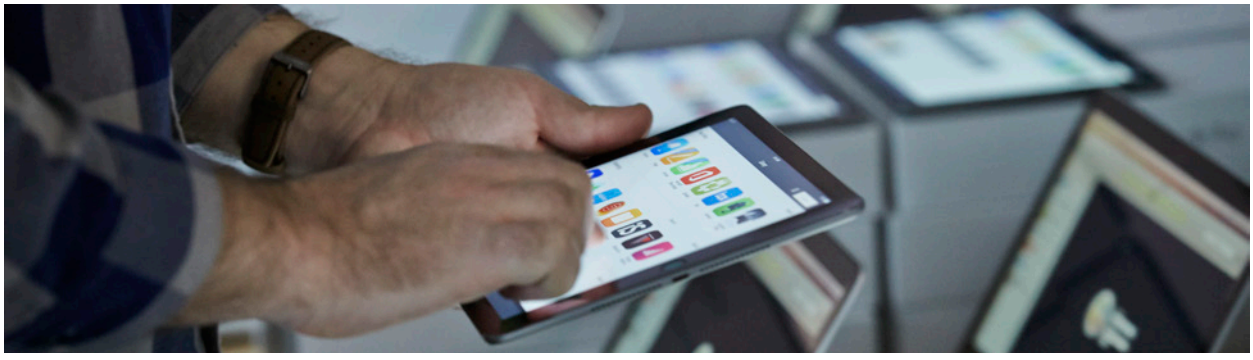
Casper Suite では、IT 管理者は OS X から生成されたログを追跡し、それらを一括管理することができます。また、それらのログに関する詳細なレポートを出力して、セキュリティ上の問題の発見に努めることも可能です。

CIS の推奨：

- asl.conf を設定する
- system.log を90日以上保管する
- appfirewall.log を90日以上保管する
- auth.log を90日以上保管する
- 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設定する
- 安全性が確立されたネットワークでの Mac へのリモートログインを有効にする
- install.log を1年以上保管する

Casper Suite の特徴：

- Config ファイルはスクリプトにて変更が可能
- ログファイルは JSS への送付が可能で、保管期限もなし
- 追加ログは JSS にてキャッシュが可能



ネットワーク構成

Casper Suite は Wi-Fi、VPN、さらには DNS 設定にも対応しているため、ネットワーク構成の展開が容易です。また、OS X の従来のサーバーコンポーネントを一部無効にすることができるため、ユーザー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 の推奨：

- Wi-Fi のステータスをメニューバーに表示する
- ネットワークの具体的なロケーションを作成する
- http サーバーを使用しないようにする（Apache
- FTP サーバーを使用しないようにする
- NFS サーバーを使用しないようにする

Casper Suite の特徴：

- ネットワーク設定は構成プロファイルの中に作成可能
- Apache、FTP、NFS はすべて、JSS Policy のスクリプトにて無効化が可能

ユーザーアカウントと環境

Casper Suite では、Mac にて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ーの作成ができます。また、クライアントマシンにインストールされたJAMF バイナリでは、コマンドの実行権限や新規ユーザーの作成権限を持つ隠れ管理アカウントを作成できます。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 の推奨：

- 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の表示を無効にする
- ゲストアカウントを無効にする
- ゲストアカウントの共有フォルダーへのアクセスを無効にする
- 拡張子を有効にする
- Safari での安全なファイルの自動実行を多目的に行わないようにする

Casper Suite の特徴：

- ログイン画面は構成プロファイルにて設定が可能
- ゲストアカウントは JSS Policy にて無効化が可能
- ユーザーアカウントは、セットアップアシスタントおよび DEP またはイメージングにて作成可能
- 作成されたアカウントは必要に応じて一般アカウントにも管理者アカウントにも設定可能

システムアクセス、認証、許可

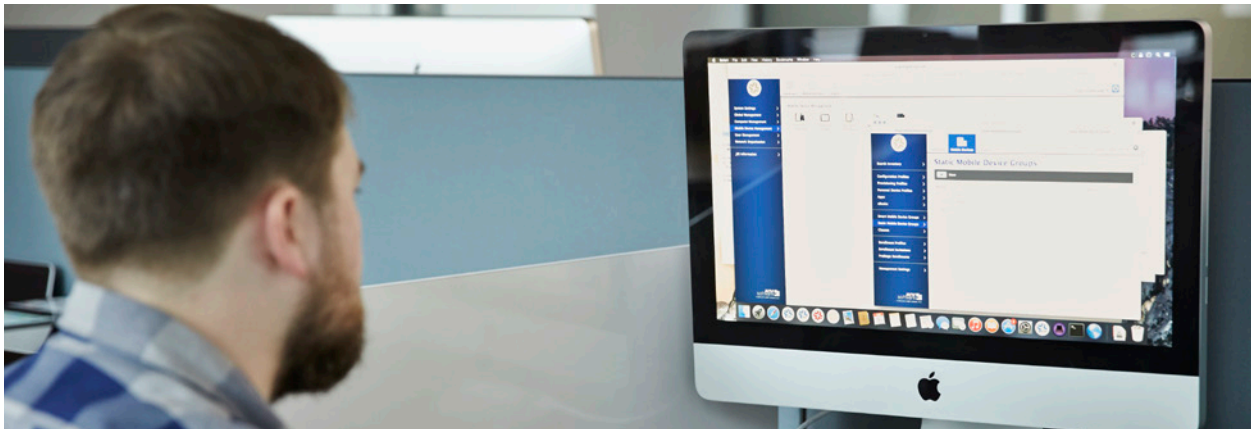
Casper Suite では、ファイル権限の設定、キーチェーンアクセスの管理、ユーザー向けの厳しいパスワードポリシーの設定が可能です。構成プロファイルや JSS Policy を作成すれば、遠隔操作にてシステムアクセス設定を行うことが可能になり、これによって、より安全性の高い Mac を構築できます。

CIS の推奨：

- ホームフォルダーを確保する（他のホームフォルダーへの読み取り許可を無効にする）
- 定期的に権限を見直す
- システム全体のアプリケーションに対して権限に問題がないか調査する
- システムフォルダーに誰でも書き込みできるファイルが存在していないか調査する
- ライブラリフォルダーに誰でも書き込みできるファイルが存在していないか調査する
- sudo のタイムアウト時間を短くする
- ログインキーチェーンを自動的にロックし使用できないようにする
- コンピュータがスリープ状態のときはログインキーチェーンがロックされるようにする
- OCSP および CRL にて証明書の確認を行う
- 「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を解除する際はパスワードの入力を必須にする
- システム全体の設定にアクセスする際は管理者用パスワードの入力を必須にする
- 他のユーザーのセッション（アクティブ/ロックに関わらず）にログインできないようにする
- 複雑なパスワードを要求する（数字、文字、記号の組み合わせ）
- パスワードの最低文字数を設定する
- アカウントのロックアウトしきい値を設定する
- ログイン画面にメッセージを表示する
- ログイン画面のバナーを作成する
- パスワードのヒントを無効にする
- ファーストユーザースイッチを無効にする
- キーチェーン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

Casper Suite の特徴：

- フォルダーのアクセス権限は JSS Policy のスクリプトにて設定可能
- 権限の変更コマンドは Self Service をトリガーとするか、または自動的に実行される
- 権限に問題のあるファイルをシステムやライブラリ内で特定するためのレポートを作成可能
- パスワードのポリシーは構成プロファイルにて設定可能
- ログイン画面とバナーは JSS Policy にて挿入可能



その他の考慮点

Casper Suite では、EFI パスワードの設定やセキュリティが確立された環境での Wi-Fi 利用の無効化など、セキュリティに関する詳細な設定が可能です。また、JSS を使用して Mac の名前を変更することも可能なため、インベントリー管理がさらに容易になります。加えて、組織で所有しているソフトウェアのインベントリーやライセンス状況の管理も可能です。

CIS の推奨：

- Wi-Fi を利用せずイーサネットのみを利用することを検討する
- iSight カメラにカバーをする
- コンピュータに論理的な名前をつける
- ソフトウェアのインベントリー管理を行う
- ソフトウェアのインベントリー管理を行う
- ファイアーウォールを設定する
- 光媒体の自動アクションを設定する
- 他の Mac では App Store の自動ダウンロードができないようにする
- EFI パスワードを設定する
- Apple ID パスワードをリセットする

Casper Suite の特徴：

- Wi-Fi はプロファイルにて無効化が可能
- コンピュータの名前は JSS の設定にて自動的に付与可能
- JSS にてソフトウェアのインベントリーとライセンスの管理が可能
- EFI パスワードはポリシーまたはイメージングにて設定可能

まとめ

Casper Suite を使用することで、独立団体 Center for Internet Security の Apple OS X 向けベンチマークを採用し、これに従うことが容易になります。

Casper Suite を活用した Mac の安全性確保に関する詳細は、
http://www.jamfsoftware.com/ja/securing-apple にてご確認ください。

JAMF software
asia-enquiries@jamfsoftware.com | +852 3008-5865 | www.jamfsoftware.com/ja