jamf

白書

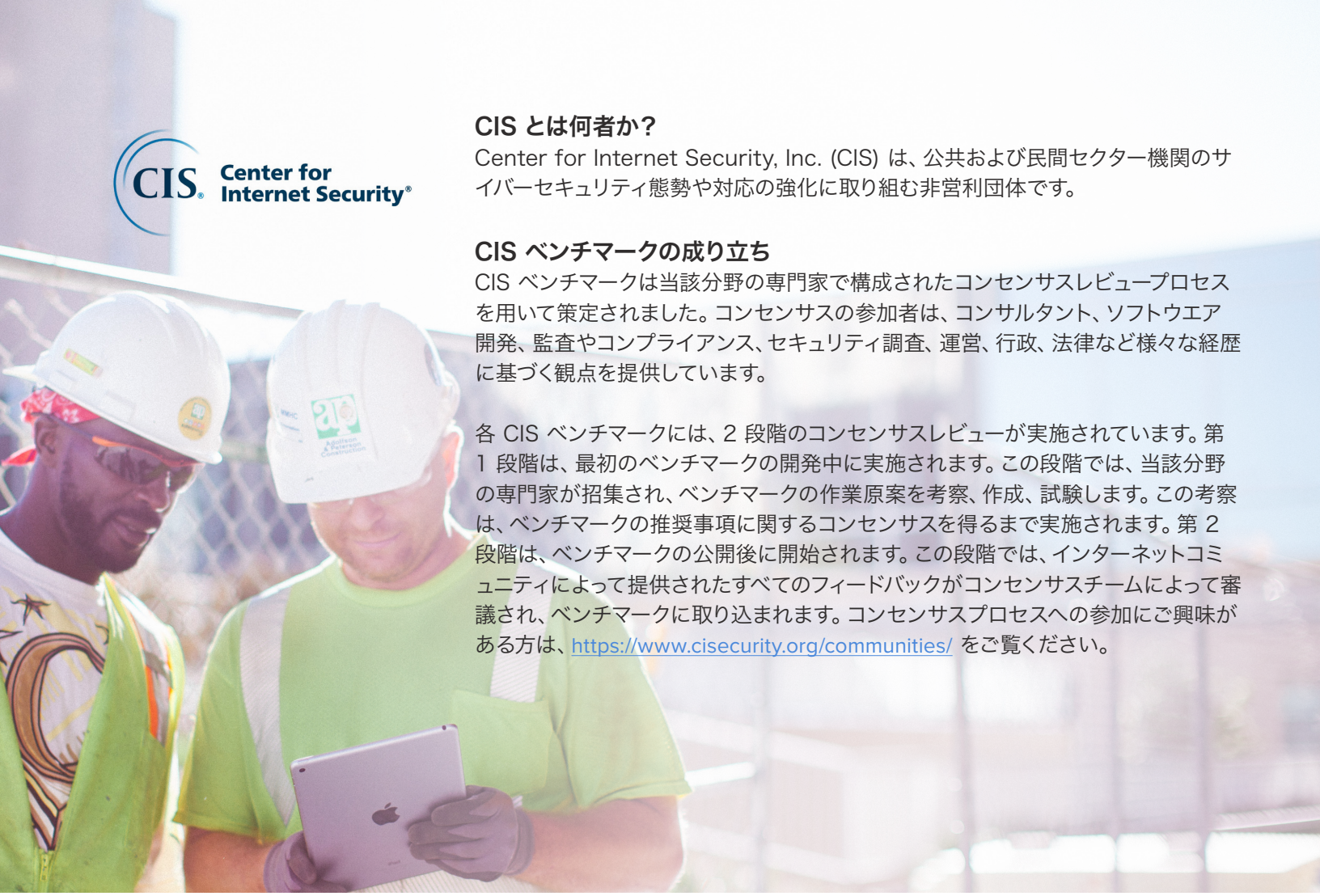
iOS セキュリティのチェックリスト

iOS に対する Center for Internet Security (CIS)ベンチマークを実装する

iOS を保護するための推奨事項

iOS に対する Center for Internet Security (CIS)ベンチマークは、iPad や iPhone デバイスを保護するために従うべき包括的なチェックリストとして企業から広く認知されています。本ホワイトペーパーでは、独立した組織の推奨事項を実装する方法について説明します。

Jamf Pro が iOS デバイスの保護と 理にどのようにお役に立てるかについては、**www.jamf.com/ja**からご覧になれます。



CIS とは何者か？

Center for Internet Security, Inc. (CIS) は、公共および民間セクター機関のサイバーセキュリティ態勢や対応の強化に取り組む非営利団体です。

CIS ベンチマークの成り立ち

CIS ベンチマークは当該分野の専門家で構成されたコンセンサスレビュープロセスを用いて策定されました。コンセンサスの参加者は、コンサルタント、ソフトウエア開発、監査やコンプライアンス、セキュリティ調査、運営、行政、法律など様々な経歴に基づく観点を提供しています。

各 CIS ベンチマークには、2 段階のコンセンサスレビューが実施されています。第 1 段階は、最初のベンチマークの開発中に実施されます。この段階では、当該分野の専門家が招集され、ベンチマークの作業原案を考察、作成、試験します。この考察は、ベンチマークの推奨事項に関するコンセンサスを得るまで実施されます。第 2 段階は、ベンチマークの公開後に開始されます。この段階では、インターネットコミュニティによって提供されたすべてのフィードバックがコンセンサスチームによって審議され、ベンチマークに取り込まれます。コンセンサスプロセスへの参加にご興味がある方は、https://www.cisecurity.org/communities/ をご覧ください。

モバイルデバイス管理の概要

MDM とは？

モバイルデバイス管理 (MDM) は Apple の iOS、macOS、および tvOS 用のビルトイン管理フレームワークです。Jamf Pro は Apple MDM の標準ソリューションです。

構成プロファイルとは？

構成プロファイルは、iOS デバイスの設定を定義するもので、MDM を介してデバイスに配布されます。

スーパービジョンとは？

デバイスが Apple のデプロイメントプログラムや Apple Configurator を介して管理に登録されると、スーパービジョンによってより深いレベルの iOS 管理が実施されます。

デバイスの所有権

セキュリティ要件は、個人所有機器の持ち込み (BYOD) イニシアチブを介しての個人所有、設備所有、ユーザーへの配布など、組織のテクノロジーモデルによって異なります。

セキュリティレベル

レベル 1 (L1) またはレベル 2 (L2) は、個人所有または施設所有のデバイスに適用しなければならないセキュリティ要件と設定を定義します。L2 では、デバイスはより厳しい管理下に置かれ、基本的なセキュリティ要件を超えた要件が求められます。

APN とは？

iOS 管理には Apple Push Notification サービス (APN) が必要です。APN について詳しくは、以下の記事をご覧ください。https://www.jamf.com/blog/what-is-apple-push-notification-service-apns/requirements

施設所有デバイスの保護

最新の調査では、企業従業員の 74% が個人所有のデバイスよりも会社発行のデバイスを好むことが明らかとなりました。Jamf Pro は、組織がその施設所有の iOS デバイスプログラムを安全に実装できるよう支援し、さらに施設所有の iPad や iPhone デバイスを円滑に配布および管理できるようにします。

CIS 推奨事項

セットアップ:

・登録プロファイルの同意メッセージと説明を設定する。
・プロファイルを削除できるようにする。

機能性:

• **L2:** スクリーンショットと画面録画を無効にする。
・デバイスのロック中は音声ダイヤルを無効にする。
・デバイスのロック中は Siri を無効にする。
・iCloud バックアップ」を無効にする。
・iCloud の文書とデータを無効にする。
・iCloud のキーチェーンを無効にする。
・「マネージドアプリが iCloud にデータを保管可能にする」を無効にする。
・「強制的に暗号化バックアップ」を有効にする。
・「すべてのコンテンツと設定を許可する」を無効にする。
• **L2:**「ユーザーが信頼できない TLS 証明書を受け入れることを許可する」を無効にする。
・「構成プロファイルのインストールを許可する」を無効にする。
・「VPN 構成の追加を許可する」を無効にする。
・「セラーデータアプリ設定の変更を許可する」を無効にする。
・ L2: 「非コンフィグレーターホストとのペアリングを許可する」を無効にする。
・ アンマネージド宛先のマネージドソースからの文書を許可する」を無効にする。
・「マネージド宛先のアンマネージドソースからの文書を許可する」を無効にする。
・「AirDrop をアンマネージド宛先として扱う」を有効にする。
・「ハンドオフを許可する」を無効にする。
・「フォースアップルウォッチリスト検出」を有効にする。
・「近くの新しいデバイスのセットアップを許可する」を無効にする。
・「ロック画面にコントロールセンターを表示する」を無効にする。
・「ロック画面に通知センターを表示する」を無効にする。

アプリ:

・不正警告強制」を有効にする。
・Cookie が「アクセスした Web サイトから」または「現在の Web サイトからのみ」に設定されていることを受け入れる。

ドメイン:
・マネージド Safari Web ドメインを構成する。

パスコード:
・「単純な値を許可する」を無効にする。
・ 最小パスコード長を「6」以上に設定する。
・ 最大オートロックを「2 分」以下に設定する。
・デバイスロックの最大猶予期間を「即時」に設定する。
・最大試行回数を「6」に設定する。

VPN:
・VPN が「構成済み」であることを確認する。
・アプリごとの VPN が望ましい。

メール:
・ユーザーの Eメールアカウントを Eメールプロファイル付きでセットアップする。
・「ユーザーがこのアカウントからメッセージを移動することを許可する」を無効にする。

通知:
・すべてのマネージドアプリの通知設定を構成する。

ロック画面メッセージ:
・「紛失したら…に戻る」メッセージを構成する。

Jamf Pro の機能

Jamf Pro では、上記の構成プロファイルを介してすべての L1 および L2 システム設定を設定、有効、および/または無効にすることができます。これらの設定のいくつかでは、登録中に iOS デバイスを監視する必要があります。
iOS スーパービジョンについて詳しくは以下を参照してください。
https://support.apple.com/en-us/HT202837.

また、Jamf Pro により、パーソナライズされたロック画面メッセージを設定し、デバイスが安全に返却され、ロック解除されたり改ざんされたりしないようにすることもできます。

*https://www.jamf.com/ja/resources/e-books/survey-the-impact-of-device-choice-on-the-employee-experience/

BYOD および個人所有デバイスの保護

CIS 推奨事項

セットアップ:
・登録プロファイルの同意メッセージと説明を設定する。
・プロファイルを削除できるようにする。

機能性:
・デバイスのロック中は音声ダイヤルを無効にする。
・デバイスのロック中は Siri を無効にする。
・「マネージドアプリが iCloud にデータを保管可能にする」を無効にする。
・「強制的に暗号化バックアップ」を有効にする。
・L2: 「ユーザーが信頼できない TLS 証明書を受け入れる」を無効にする。
・「アンマネージド宛先のソースからのマネージド文書」を無効にする。
・「マネージド宛先のアンマネージドソースからの文書」を無効にする。
・「AirDrop をアンマネージド宛先として扱う」を有効にする。
・L2: 「ハンドオフを許可する」を無効にする。
・「ロック画面にコントロールセンターを表示する」を無効にする。
・「ロック画面に通知センターを表示する」を無効にする。

アプリ:
・Safari の不正警告強制」を有効にする。
・Cookie が「アクセスした Web サイトから」または「現在の Web サイトからのみ」に設定されていることを受け入れる。

ドメイン:
• マネージド Safari Web ドメインを構成する。

パスコード:
単純な値を許可する」を無効にする。
・最小パスコード長を「6」以上に設定する。
・最大オートロックを「2 分」以下に設定する。
・デバイスロックの最大猶予期間を「即時」に設定する。
・最大試行回数を「6」に設定する。

VPN:
・VPN が「構成済み」であることを確認する。
・アプリごとの VPN が望ましい。

メール:
- ユーザーの Eメールアカウントを Eメールプロファイル付きでセットアップする。
- 「ユーザーがこのアカウントからメッセージを移動することを許可する」を無効にする。

通知:
- VPN が「構成済み」であることを確認する。
- アプリごとの VPN が望ましい。

Jamf Pro の機能

Jamf Pro の BYOD ソリューションでは、登録プロファイル用にカスタムの同意メッセージおよび説明を作成でき、さらに退職者向けに、組織やプログラムを離れる際に BYOD プロファイルを削除する簡単なプロセスを作成できます。

組織において CIS 推奨の L1 および/または L2 のセキュリティ設定をすべて実装する必要がある場合は、iOS デバイスを監視されない設備デバイスとして登録できる Jamf Pro の機能をご利用ください。また、「個人所有デバイス」の iOS 登録についてはユーザー開始の登録設定を無効にすることをお勧めします。Jamf Pro 内に構成ファイルを作成し、配布することで、1 台の iOS デバイスまたは iOS デバイスのグループに対する、L1 および L2 のすべてのセキュリティ設定の構成、無効化、および/または有効化が可能です。

その他の考慮事項

Jamf Pro により、デバイスは常に最新のソフトウェアを実行し、不正攻撃から確実に守られるため、進化したデバイス管理と構成プロファイルを実現できます。

CIS 推奨事項

・iOS デバイスが明らかに非改造であることを確認する。
・ソフトウェアを常に最新版にする。
・アプリアップデートの自動ダウンロードを有効にする。
・エンドユーザーのデバイスに限り、「iPad を探す」および/または「iPhone を探す」を有効にする。
・最新の iOS デバイスアーキテクチャがデバイス上に重要な情報を持つユーザーが使用されていることを確認する。

Jamf Pro の機能

Jamf Pro では、iPad および iPhone のオペレーティング システムにゼロデイサポートを提供するため、最新のソフトウェアが常にサポートされます。さらに、Jamf Pro の Sefl Service では、ユーザーが必要とするリソース、アプリ、構成ユーザーすべてを取り込んだ独自のカスタムアプリカタログを構築できます。IT にヘルプチケットを提出することなくオンデマンドアクセスがユーザーに付与されます。デバイスの紛失や盗難の際は、Jamf Pro が安全にデバイスをロック、ワイプ、リセットし、企業データと個人データの漏洩を確実に防止します。

優れたデバイスセキュリティはここから始まります

Jamf Pro なら独立した組織である Center for Internet Security の Apple iOS ベンチマークを簡単に実装し、準拠することができます。

無償のトライアルをご請求の上、このガイドをお客様の環境で実践してみてください。