jamf

IT部門向けMacコンプライアンスチェックリスト

コンプライアンスとは、単に法的要件を満たすだけでなく、セキュリティを高め、リスクを軽減し、信頼を構築します。

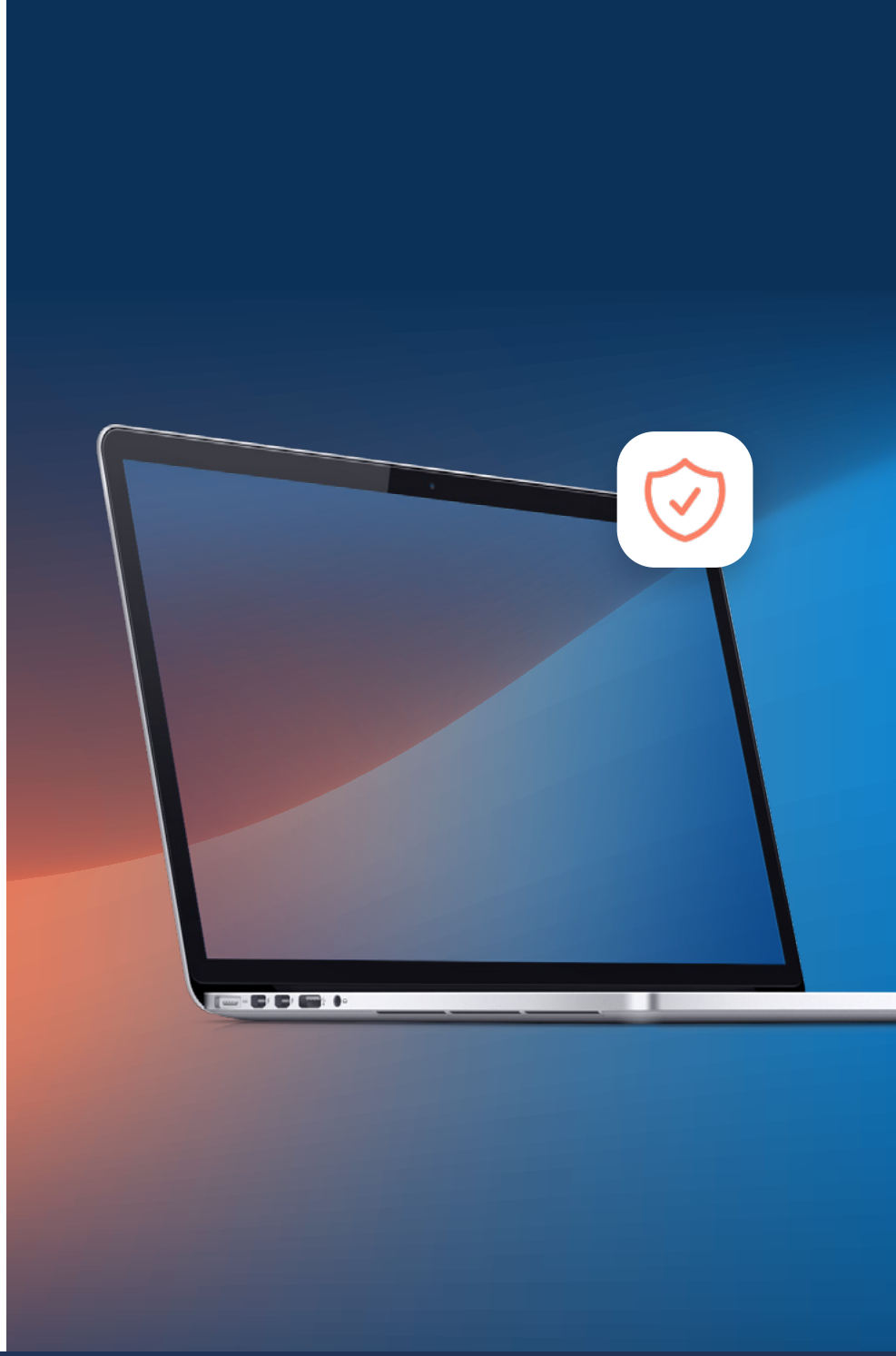
Macのコンプライアンスが重要な理由

規模や業種にかかわらず、特に機密情報を取り扱う場合には、多くの企業が何らかのコンプライアンス規制への対応を求められます。

ITセキュリティにおけるコンプライアンスベンチマークとは、組織が規制や要件を遵守しているかを測定するために使用される基準であり、機密データの保護におけるベストプラクティスを提供します。

例えば、CIS ControlsとCIS ベンチマークは、Center for Internet Security（CIS）が提供する自主ガイドラインであり、GDPRやHIPAAなどの規制要件を満たすために広く採用されています。

組織は、セキュリティリスクを低減し、顧客の信頼を築き、ペナルティを回避するために、これらのベンチマークを遵守しなければなりません。実際、関連規制を遵守できていない場合、多額の罰金や法的措置、イメージの悪化につながる恐れがあります。これらのベンチマークを定期的に追跡し、達成することは、企業がデジタル社会で安全かつ競争力を維持するのを助けます。



IT管理者がMacのセキュリティを維持する方法

IT管理者がAppleを好む理由のひとつは、Macには驚くほど多様なセキュリティ機能が内蔵されているからです。

Macコンピュータはまさにその本質から、他のデバイスよりも安定していて効率的です。そして適切なツールを使うことで、IT部門はAppleの優れた操作性を維持したまま、強力で柔軟なApple特有の管理とセキュアな運用を行うことができ、世界水準のMDMソリューションとAppleの宣言型デバイス管理（DDM）プロトコルを組み合わせることで、企業データ、従業員データ、ネットワークを確実に保護することが可能になります。

Macの規制コンプライアンス：
考慮すべき点

組織内のコンプライアンスにおいて、考慮すべき点は多岐に渡ります。

企業や従業員のデータを安全に保つためにはおそらく複数のコンプライアンス基準を満たす必要があり、業界や政府のベンチマークと同様に、これらを履行する必要があります。

規制の種類

業界や地域にはそれぞれ独自の規制やベストプラクティスがあり、重複する部分もあります。世界各地の規制の例（一部）：

ISO [ISO 27701](#) は、医療分野におけるPII（個人を特定できる情報）の適切な取り扱いを保証する国際規格です。

[DORA](#)は、金融セクター向けのEUの規制です。

CIS. Center for Internet Securityの [CIS ベンチマーク](#) は、システムを安全に構成するために推奨される構成基準を示しています。

NIS2 [NIS2](#) 指令は、EU全域のサイバーセキュリティに関する法令で、確実に遵守されなくてはなりません。

[ドイツのITセキュリティ法1.0および2.0（das IT-Sicherheitsgesetz 1.0 und 2.0）は](#)、独自のコンプライアンス要件でITセキュリティを規制しています。

CYBER ESSENTIALS [Cyber Essentials+](#) は、英国内すべての組織を対象に、最低限のサイバーセキュリティ基準を定めています。

これらの規制を追跡し、遵守するのは確かに大変です。

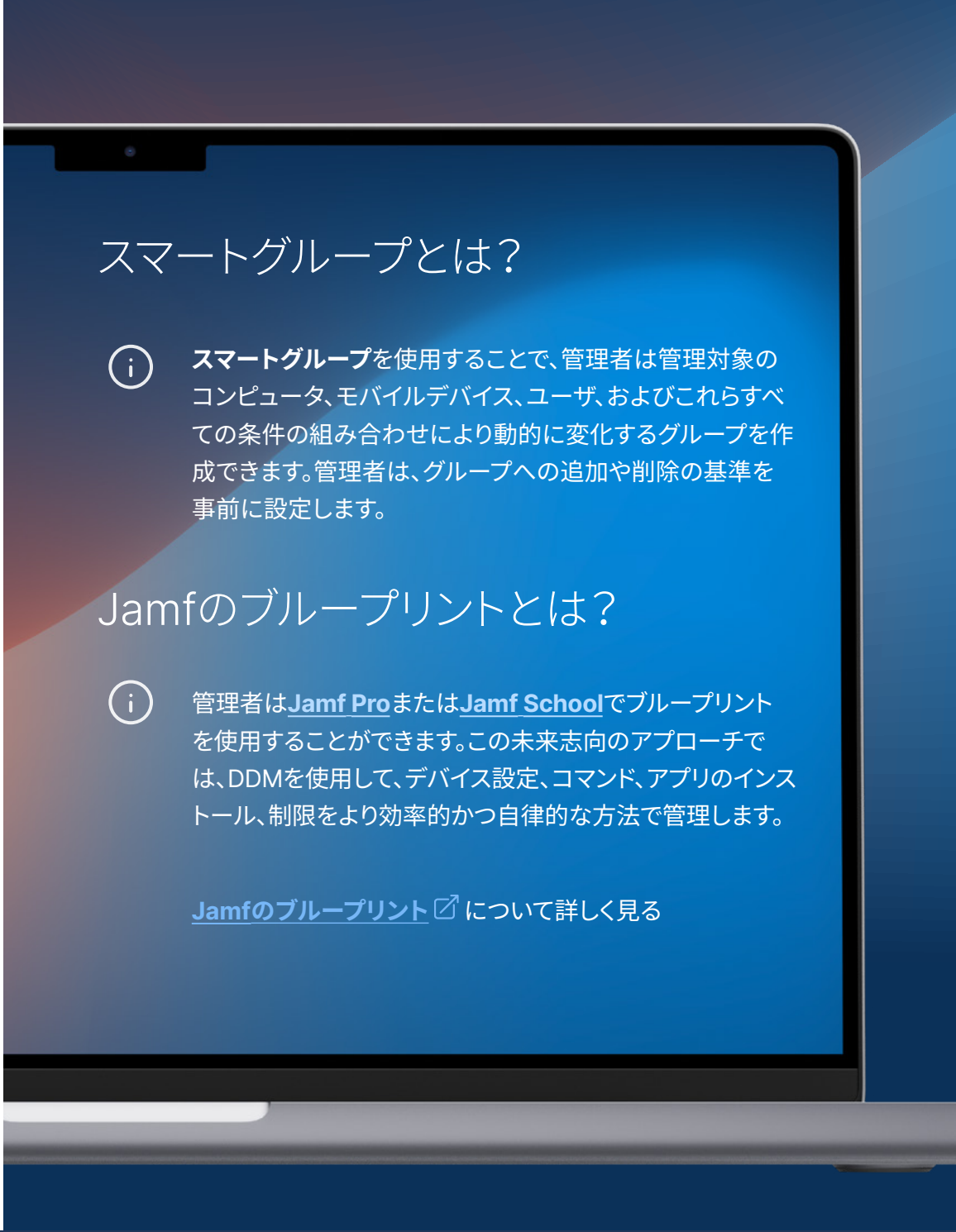
しかし、粘り強く調査し、どの規制があなたの組織とデバイス環境に適用されるかを見極め、その上で、世界水準のMDMと徹底したQAプロセスを組み合わせることで、コンプライアンスを自動で設定し、継続的に検証することが可能になります。

適切なデバイス管理により、以下のようなことが可能になります：

- **適正な構成プロファイル、コンプライアンス宣言、ブループリント**
- **スマートグループ設定によるプロファイルとコマンドのダイナミックな割り当て**
- **即時のコンプライアンス遵守をデバイスレベルで自動化し、管理者の時間を節約**

デバイス管理のおかげで、早々に仕事を切り上げて
久々に昼寝をする余裕も出てくるかもしれません。

補足説明...



...コンプライアンスの内容は絶えず変化しています。

インターネット、IT、商習慣、法律の変化に合わせて、コンプライアンスも変わらなければなりません。コンプライアンスの核心とは、ビジネスの安全と円滑な運営を維持することであり、新たなセキュリティやITの問題に遅れず対応していくことは、そのプロセスの一部です。

そのためには以下が必要です：

- ✓ **定期的なコンプライアンス監査と規制の見直し**
- ✓ **スピーディなOSアップデート**
- ✓ **サイバー脅威のプロアクティブな監視**
- ✓ **変化するコンプライアンス規制への対応**
- ✓ **誰がどのデータにアクセスを持つか規定する従業員ごとのポリシー変更への迅速な対応**

どれも大変そうに見えますが、実際そうなのです。

MacのコンプライアンスチェックリストとJamfでできること

構造化されたチェックリストに従うことで、IT部門はコンプライアンスプロセスを合理化し、進化する規制に先手を打つことができます。遅れを取らないようにするための最善策は、適切なセキュリティ構成、監視、強制を確実に実施するための細かく具体的な手順を含んだチェックリストを用意することです。

そして、これらすべての分野の追跡、監視、強制、アップデートをサポートする一流のソリューションの使用も忘れてはなりません。

準備段階

- ✓ **ユーザアカウントとプロファイルを作成します。**
- ✓ **組織の意思決定者とともに、組織のポリシーと権限を定義します。**
- ✓ **組織が従わなければならない業界または政府の規制に基づいて、外部のコンプライアンス規制を定義します。**
- ✓ **使用するすべてのツールのハードウェアとソフトウェアの互換性を確認します。**

コンプライアンスベンチマーク機能とは?

Jamf Proに内蔵されたコンプライアンスベンチマークにより、IT部門はコンプライアンスを定義、監査、実施することができます。

特徴:

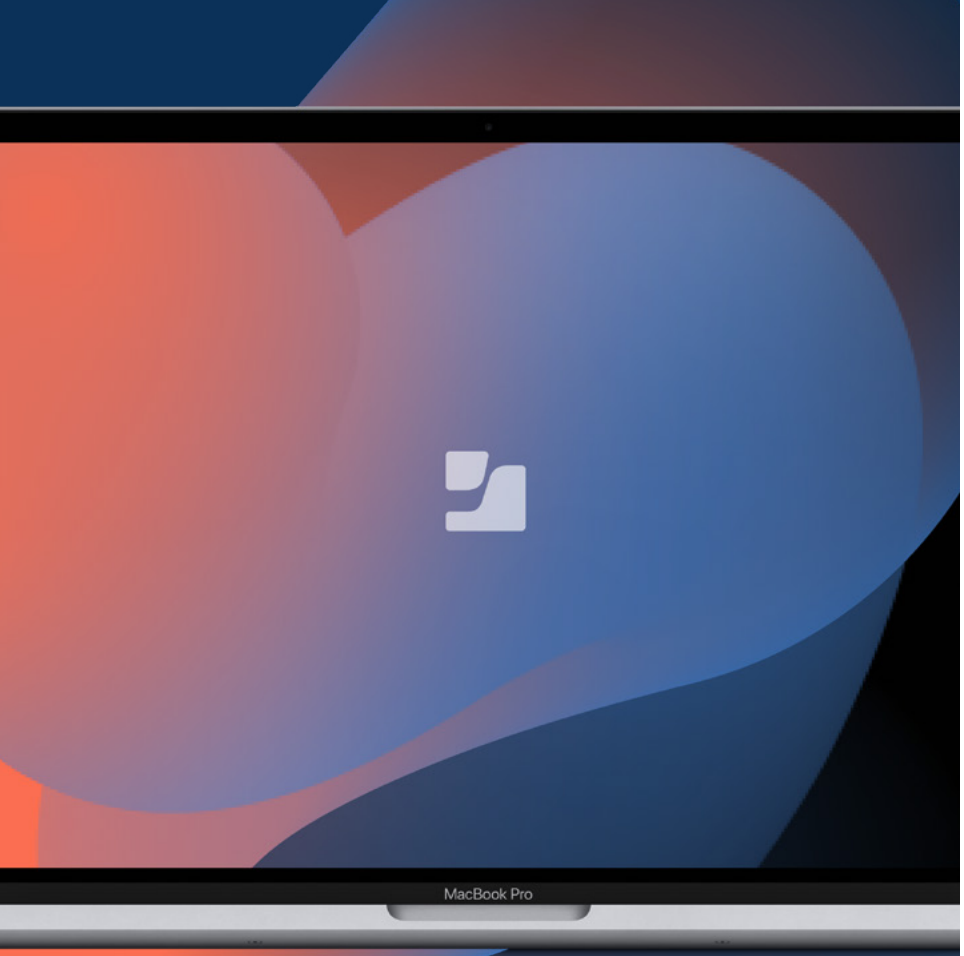
- ✓ **IT管理者がデバイス全体を監査し、コンプライアンスベンチマークを適用遵守させるのにかかる時間を数週間から数分に短縮します。**
- ✓ **シンプルでわかりやすいUIとワークフローで、複雑なコンプライアンス基準、ルール、構成コントロールをスムーズに運用できるようサポートします。**
- ✓ **カスタムデバイスのセキュリティポスチャを強化します。**

コンプライアンスベンチマークは、プロファイル、ポリシー、スクリプト、拡張属性などを含むこれらのすべてを自動的に作成します。Jamf Proの構成機能を活用し、選定されたベンチマークに準拠するようにデバイス設定を変更・維持します。これにより、プロジェクト全体にわたるデータセキュリティを確保するとともに、エンドユーザに対してデバイスの利用準備が整っていることを明確に伝えます。

例:

CISレベル1などのコンプライアンスベンチマークの実施

1. **強制タイプを選択。**
2. **コンピュータの範囲を設定。**
3. **必要に応じてベンチマークをカスタマイズ。**
4. **保存して展開。**



コンプライアンスベンチマークは、macOSセキュリティコンプライアンスプロジェクト（mSCP）に基づいて構築されました。これは、アメリカの国立標準技術研究所（NIST）、アメリア航空宇宙局（NASA）、国防情報システム局（DISA）およびロスアラモス国立研究所（LANL）の連邦運用ITセキュリティスタッフによる共同プロジェクトです。

継続的なメンテナンスとモニタリング

コンプライアンスベンチマークダッシュボードには、作成されたすべてのベンチマークとそのステータスが表示されます。詳細表示では、コンプライアンスルールごとにすべてのデバイスのコンプライアンスが表示され（例えば、パスワードの最小文字数を要求する）、管理者はより詳しく確認することができます。

コンプライアンスベンチマークのデモをご覧ください：

セットアップと構成

MDMとDDMを連携した自動プロビジョニングを使用して、各デバイスが各ユーザに必要なものを正確に備え、アプリとアクセス設定がデバイスレベルでプロアクティブにアップデートされるようにします。

- ✓ **Jamfのコンプライアンスベンチマークは、CISレベル1または2などの一般的なベンチマークに基づいてJamfが作成した要件を使用することにより、ワークフローを簡素化、高速化。さらに管理者はカスタムベンチマークを作成することもできます。**
- ✓ **Jamfのブループリント ウィンドウにある6つのクイックスタートテンプレートのいずれかを使用するか、独自のテンプレートを作成します。パスコードポリシーの設定、サービス構成ファイルの設定、バックグラウンドタスクの管理により、時間の節約とセキュリティ強化が可能になります。**
- ✓ **Self Service+（特定のユーザグループが、それぞれの役割に特化したアプリやリソースにアクセスし、ダウンロードできるようにするサービス）とスマートグループを組み合わせて、必要不可欠なアプリやアップデートをインストールします。**
- ✓ **セキュリティ設定（FileVault、Gatekeeperなど）を構成します。**

検証

- ✓ **アプリやシステム機能を検証します。**
- ✓ **セキュリティ監査の実施：Jamf Protectが保存する監査ログはIT部門の監査作業を助けます。**
- ✓ **このような変更は、実地検証となるように、まずは少人数の従業員に対して展開すると良いでしょう。**

万全の体制で導入を開始

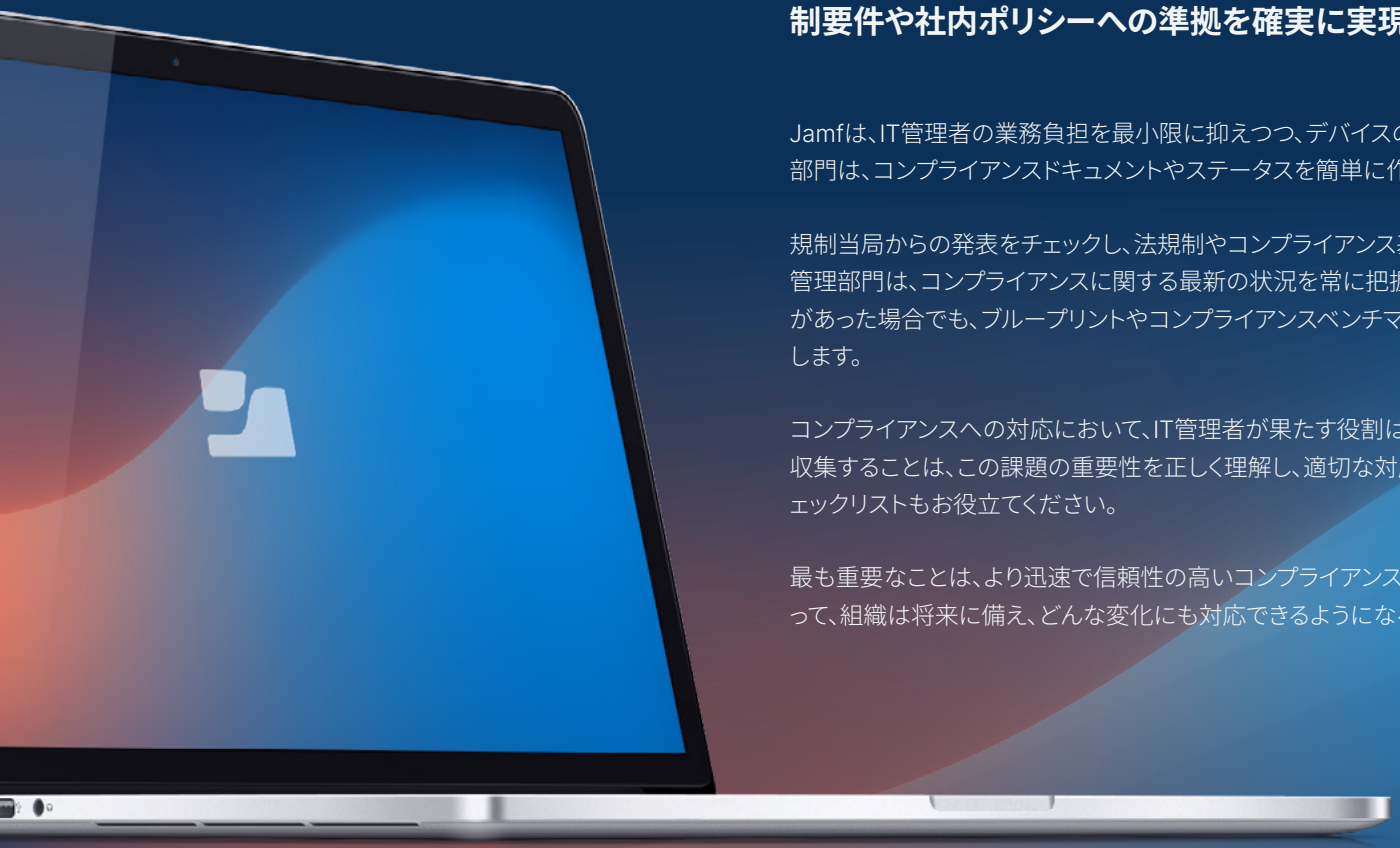
- ✓ **ユーザに明確な指示を出します。**
- ✓ **質問やトラブルシューティングのためのオンボーディングセッションを設定します。**
- ✓ **Jamfでコンプライアンス設定のアップデートを自動化することにより、重要なコンプライアンスプロトコルに関する新たな展開を常に把握する手間が省けます。**

Self Service＋とは？

Self Service+はmacOS向けのエンドユーザポータルであり、ユーザはJamf Proであらかじめ設定されたコンテンツやアップデートにアクセスすることができます。Self Service+でユーザができること：

1. **デバイスのセキュリティステータスの確認。**
2. **App Storeやサードパーティ製のアプリ、構成プロファイル、Bookの閲覧、検索、インストール。**
3. **パスワード変更など、アイデンティティ管理タスクの実行。**

ベストプラクティスと今後の検討事項



Jamfという信頼できるパートナーと連携することで、デバイスを安全に構成し、各種規制要件や社内ポリシーへの準拠を確実に実現できます。

Jamfは、IT管理者の業務負担を最小限に抑えつつ、デバイスのコンプライアンス準拠を実現します。また、セキュリティ部門は、コンプライアンスドキュメントやステータスを簡単に作成し、監査員に提示することができます。

規制当局からの発表をチェックし、法規制やコンプライアンス基準の変更に遅れを取らないようにしましょう。デバイス管理部門は、コンプライアンスに関する最新の状況を常に把握しておく必要があります。Jamfは、基準や要件に変更があった場合でも、ブループリントやコンプライアンスベンチマークを自動でアップデートし、継続的な対応をサポートします。

コンプライアンスへの対応において、IT管理者が果たす役割は極めて大きいと言えるでしょう。このeBookなどで情報収集することは、この課題の重要性を正しく理解し、適切な対応へとつなげるための第一歩となります。併せてこのチェックリストもお役立てください。

最も重要なことは、より迅速で信頼性の高いコンプライアンス戦略と戦術を打ち出すことであり、皆さんの頑張りによって、組織は将来に備え、どんな変化にも対応できるようになるはずです。

jamf

Jamfでコンプライアンス対応をもっとスムーズに

トライアルに申し込む