jamf

Macのコンプライアンス実務ガイド

増加するAppleデバイスの管理に
課題を感じているIT担当者必読

Macのコンプライアンスの重要性

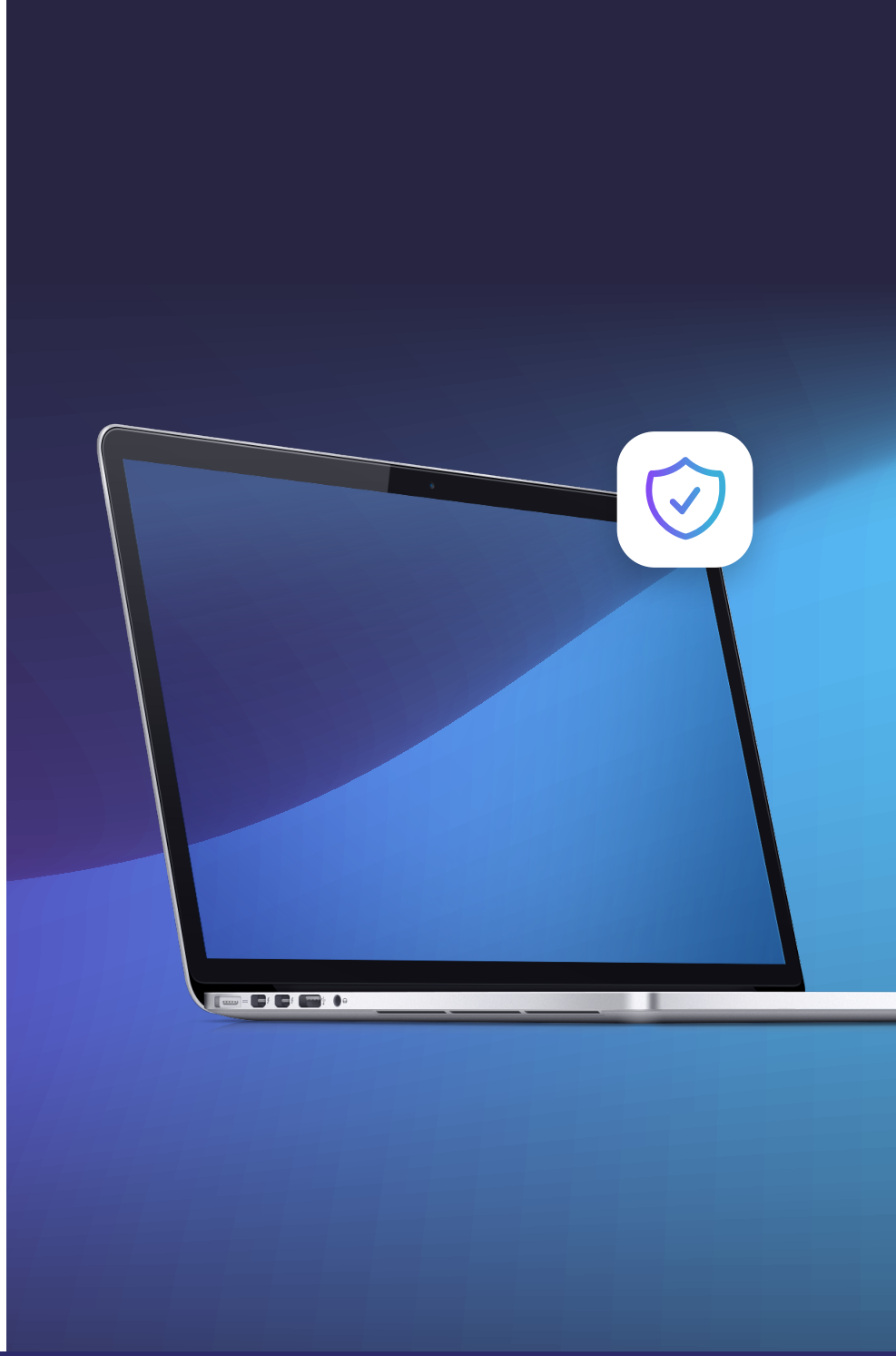
Macやモバイルデバイスを運用する成長企業にとって、コンプライアンス要件の遵守と、IT運用の効率化・簡素化の両立は不可欠です。コンプライアンスは、単に法令を遵守するだけの話ではありません。セキュリティの強化やリスク抑制、ひいては信頼を構築していくうえでも、非常に重要な役割を果たします。もっとも、コンプライアンスを重視するあまり、既に多忙なIT部門の業務を無駄に複雑にすることがないようにするのが大前提です。

Macにおけるコンプライアンスの重要性を理解することは、安全で拡張性に優れたIT環境を構築するための第一歩となります。

コンプライアンスは、根本的にはベンチマークに左右されます。ITセキュリティ分野のコンプライアンスベンチマークは、組織が各種規制や要件を遵守しているかどうかを評価するための基準であると同時に、機密データの保護に関するベストプラクティスを定めたものでもあります。

例えば、CIS コントロールとCIS ベンチマークは、セキュリティのベストプラクティスの土台としてさまざまな業界で広く採用されています。どちらも、特定の規制に紐付けられたものではありませんが、組織が（GDPRやHIPAAで要請されているような）業界または地域に固有のコンプライアンス体制を構築する際のベースとして役立てられています。

組織が拡大するなかで、リスクを抑え、データを保護し、セキュリティの死角をなくす。成長企業は、こうしたベンチマークを指針とすることで、環境の変化に左右されない強固な基盤を維持しています。これは、規制を遵守しなければ、高額の罰金が科せられたり、訴訟に発展したり、自社の評判に傷がついたりすることにもつながるからにほかなりません。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。



Macのセキュリティ管理の手法

AppleがIT管理者に好まれる理由の一つに、Macには優れたセキュリティ機能が内蔵されているという点が挙げられます。

小規模なIT部門がMacやモバイルデバイスの管理を担当している場合には、このセキュリティ機能を一元管理および自動適用すれば、最も効果的に保護を実現できます。

Macコンピュータは、もともと他のデバイスよりも安定性と効率性に優れています。そこに適切なツールを活用すれば、AppleのUIがもたらす高い利便性を損なうことなく、Appleに特化した強力で柔軟な管理やセキュリティ対策が実現します。また、世界レベルのMDMソリューションとAppleの宣言型デバイス管理（DDM）プロトコルを併用すれば、業務データ、従業員データ、ネットワークのいずれも確実に保護できます。

Macの規制コンプライアンス：考慮が必要な事項

組織が満たさなければならないコンプライアンス要件は通常、企業の大小を問わず変わりません。つまり、IT部門の人員やリソースが大企業ほど潤沢でなかったとしても、やるべきことは同じです。

そのため、コンプライアンス業務では、一度にいくつもの基準や要件を取り扱うことになるのが常です。これをお読みの皆様の組織でも、業務でいくつものコンプライアンス基準に対応しているのではないでしょうか。それが、業務データと従業員データの安全を保つことにつながるからです。もっとも、考慮が必要なのはそれだけではありません。業界や政府機関が定めるベンチマークもクリアする必要があります。

さまざまな規制

さまざまな業界や地域が、規制やベストプラクティスを定めています。世界各地の規制の例（一部）：

- **ISO 27701**：医療分野のPII（個人識別情報）の適正な取扱いに関する国際規格
- **DORA**：金融分野を対象としてEUが制定した規制
- **CIS ベンチマーク**：システムを安全に構成するために推奨される構成基準について、Center for Internet Security（CIS）が策定したガイドライン
- **NIS2指令**：EU全域で遵守が求められるサイバーセキュリティに関する規制
- **ドイツITセキュリティ法1.0および2.0（das IT-Sicherheitsgesetz 1.0 und 2.0）**：独自のコンプライアンス要件を定めたITセキュリティに関する規制
- **Cyber Essentials+**：英国内の全組織を対象としてサイバーセキュリティの最小要件を定めた規格

複雑な規制の数々を確実に遵守するには

組織やデバイスに適用される要件を特定したら、今度はその要件に対応するためのプロセスを用意する必要があります。

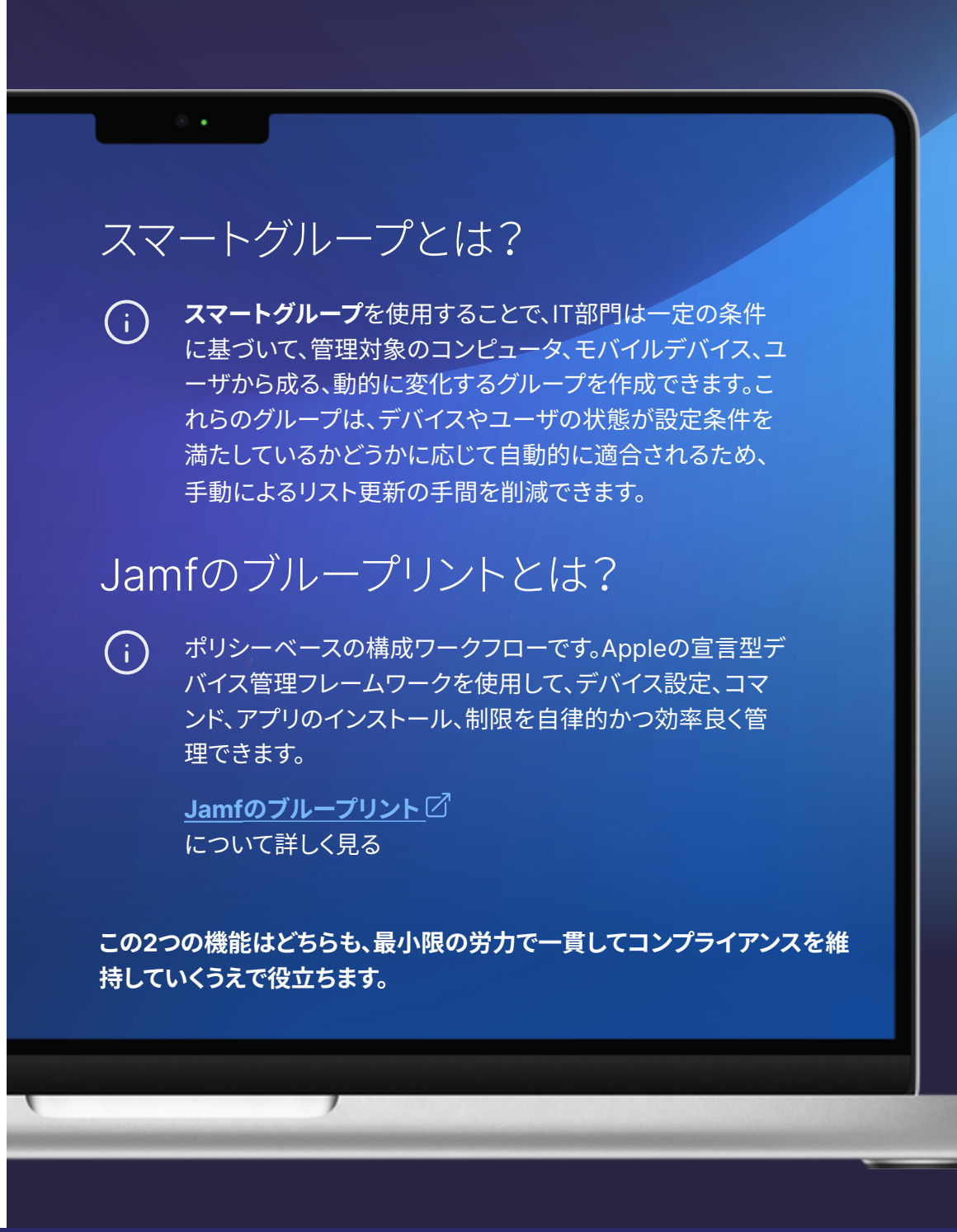
現代のデバイス管理では、この種の作業の大部分を自動化し、組織内のデバイス全体にコンプライアンスを確保していくやり方が主流です。

デバイス管理のメリットは以下のとおりです。

- **一定の構成やコンプライアンスポリシーを常に適用できる**
- **動的グループ化により、設定やアクションを自動で割り当てることができる**
- **自動化により、デバイスレベルのコンプライアンスを保ちつつ手作業を減らすことができる**

ここまでの段階で、すべてがうまく管理できるようになったような気がするかもしれません。少しくらい、その場を離れても大丈夫でしょうか。

そうとは限りません...



コンプライアンスをめぐる状況は常に変化する

テクノロジー、ビジネス、規制が進歩していけば、それに合わせてコンプライアンス要件も変わっていきます。いずれにしても、コンプライアンスの究極目標は、環境が変化しても組織が安全かつ円滑に業務を継続できるようにすることにほかなりません。そのため、次々に発生するセキュリティリスクや規制に対し、随時対応していくことができるプロセスを構築する必要があります。

このプロセスに必要な要素の例は以下のとおりです。

- ✓ **定期的なコンプライアンス監査とレビュー**
- ✓ **オペレーティングシステムとセキュリティのタイムリーなアップデート**
- ✓ **セキュリティ脅威の常時監視**
- ✓ **規制やポリシーの変化への適応**
- ✓ **ユーザの役割やアクセスのニーズの変化に対する迅速な対応**

このようなプロセスを構築することは、大変な作業のように感じられるかもしれません。実際、多くの場合には大変な作業です。

そこで不可欠となるのが、構造化されたコンプライアンス・チェックリストの活用です。

明確で段階的なアプローチを実践することで、IT部門はコンプライアンス対応を効率化し、絶えず変化する要件にも柔軟に適応し続けることが可能になります。

また、優れたチェックリストは、見落としを防いだり、セキュリティ対策、監視、ポリシーや設定を確実に適用したりするうえでも効果を発揮します。

準備段階

- ✓ **ユーザのアカウントとプロファイルを作成する。**
- ✓ **組織内の意思決定者の協力の下で、組織のポリシーと権限を定義する。**
- ✓ **自社が従わなければならない業界規制や公的規制を精査し、外部コンプライアンス規制を定義する。**
- ✓ **採用するツールすべてについて、ハードウェアとソフトウェアの互換性を確認する。**

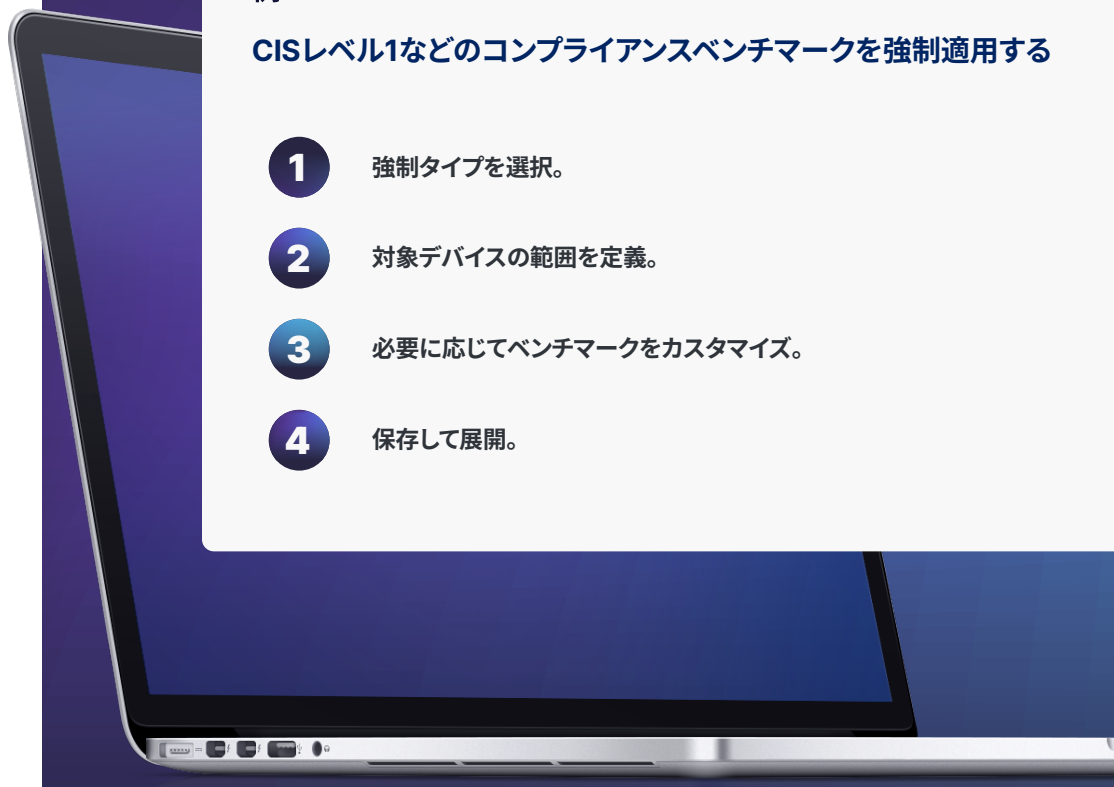
コンプライアンス ベンチマークとは?

コンプライアンスベンチマークを使えば、体系的かつ繰り返し可能な形でコンプライアンスを定義、監査、適用できます。

コンプライアンスベンチマークのメリット

- ✓ **デバイスのコンプライアンスの監査と実施にかかる時間を節約**
- ✓ **複雑なセキュリティ基準と構成要件がシンプルに**
- ✓ **デバイスのセキュリティポスチャー全般の改善に寄与**

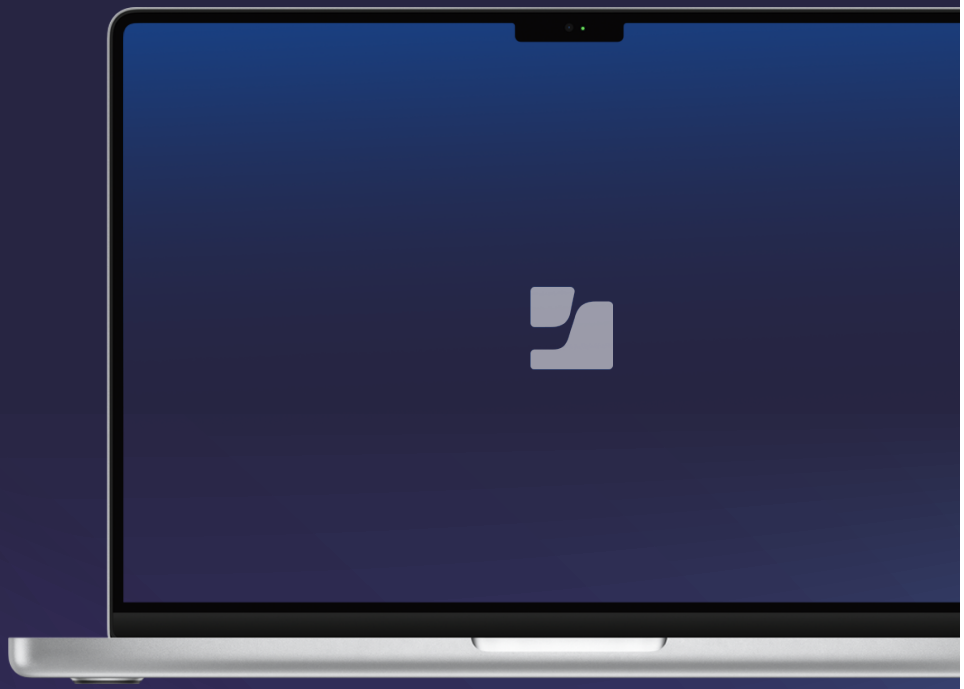
コンプライアンスベンチマークでは、セキュリティ設定の適用とメンテナンスを自動化できるので、デバイスを一定の基準に準拠した状態に維持するうえで役立ちます。



例:

CISレベル1などのコンプライアンスベンチマークを強制適用する

1. **強制タイプを選択。**
2. **対象デバイスの範囲を定義。**
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）に基づくものです。mSCP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ITセキュリティチームによる共同プロジェクトです。

メンテナンスと監視を継続

コンプライアンスベンチマークを使えば、適用しているベンチマークの状況や、デバイスのコンプライアンス状況全般を可視化できます。詳細な情報が表示されるので、（パスワードの要件などの）個別のルールのコンプライアンス状況まで詳しく確認できます。

コンプライアンスベンチマークのデモ

設定と構成

自動プロビジョニングを活用し、ユーザごとに正しいデバイス構成を確保しましょう。また、デバイスレベルでアプリケーションやアクセス設定を最新の状態に保つうえでも、自動プロビジョニングが役立ちます。

- ✓ **CISレベル1、レベル2など、一般によく採用されている基準に基づいた要件を適用するときは、コンプライアンスベンチマークを活用しましょう。構成作業の効率化と時間短縮が期待できます。**
- ✓ **既成の構成テンプレートを使うか、独自のテンプレートを作成しましょう。構成業務の時間節約と一貫性向上に役立つほか、パスコードのセキュリティ設定、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も、時間節約とセキュリティ強化の効果を発揮します。**
- ✓ **業務に不可欠なアプリケーションやアップデートのインストールには、Self Service+とスマートグループを使いましょう。自動割り当てによりIT部門による統制を確保しつつ、ユーザが必要なツールにアクセスできる状態を実現できます。**
- ✓ **ディスク暗号化、システム保護、アプリケーション制御などの重要なセキュリティ設定を構成しましょう。**

検証

- ✓ **アプリやシステム機能を検証しましょう。**
- ✓ **セキュリティ関連のレビューや監査を実施し、コンプライアンスを確認しましょう。**
- ✓ **まずは一部の従業員を「先行テスター」として対象を絞って導入し、実際の業務を通じた検証を行うことから検討してください。**

万全の体制で導入を開始

- ✓ **ユーザにわかりやすい指示を与えましょう。**
- ✓ **オンボーディングセッションを開催し、質問やトラブルシューティングに対応しましょう。**
- ✓ **規制が変わっても大きな労力をかけずにシステムを対応させることができるよう、コンプライアンス関連のアップデートを自動化しておきましょう。**

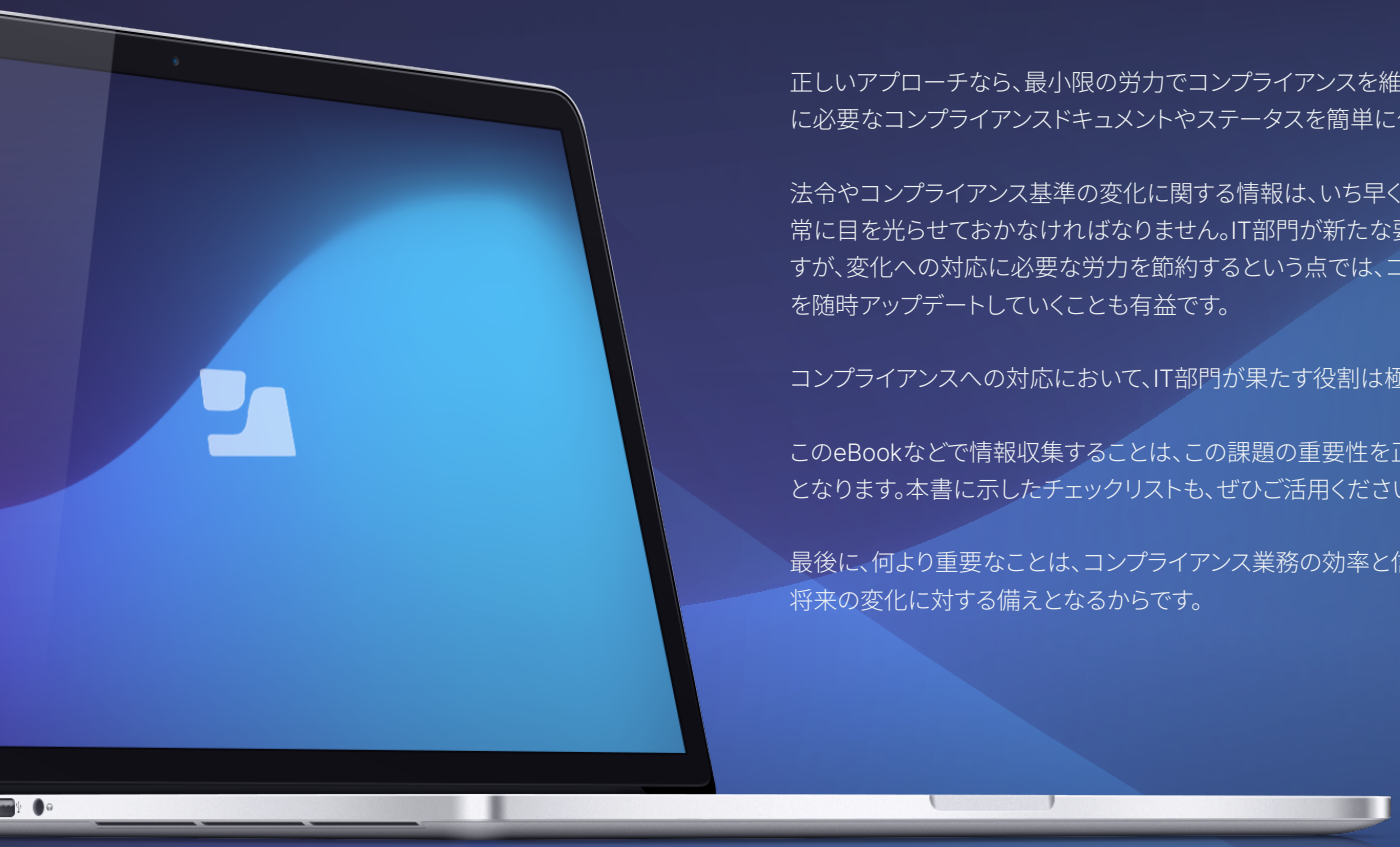
Self Service＋とは？

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+でできることは以下のとおりです。

1. **デバイスのセキュリティ状態を確認する。**
2. **App Storeやサードパーティのストアのアプリ、構成プロファイル、ブックを閲覧、検索、インストールする。**
3. **パスワード変更など、ID関連のタスクを実行する。**

ベストプラクティスと今後の課題

的確なツールとプロセスを駆使すれば、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。



正しいアプローチなら、最小限の労力でコンプライアンスを維持できます。また、セキュリティ部門が監査やレビューに必要な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、提示することも可能になります。

法令やコンプライアンス基準の変化に関する情報は、いち早く入手しましょう。そのためには、規制機関の情報発信に常に目を光らせておかなければなりません。IT部門が新たな要件について理解を深めておくことはもちろん重要ですが、変化への対応に必要な労力を節約するという点では、コンプライアンス関連のフレームワークやベンチマークを随時アップデートしていくことも有益です。

コンプライアンスへの対応において、IT部門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。本書に示したチェックリストも、ぜひご活用ください。

最後に、何より重要なことは、コンプライアンス業務の効率と信頼性を絶えず追求していくことでしょう。それこそが、将来の変化に対する備えとなるからです。

Jamfがコンプライアンス管理の効率化にもたらす効果を、ぜひ一度ご確認ください。

jamf

トライアルに申し込む