jamf

コンプライアンス管理

初心者ガイド

コンプライアンスとは？

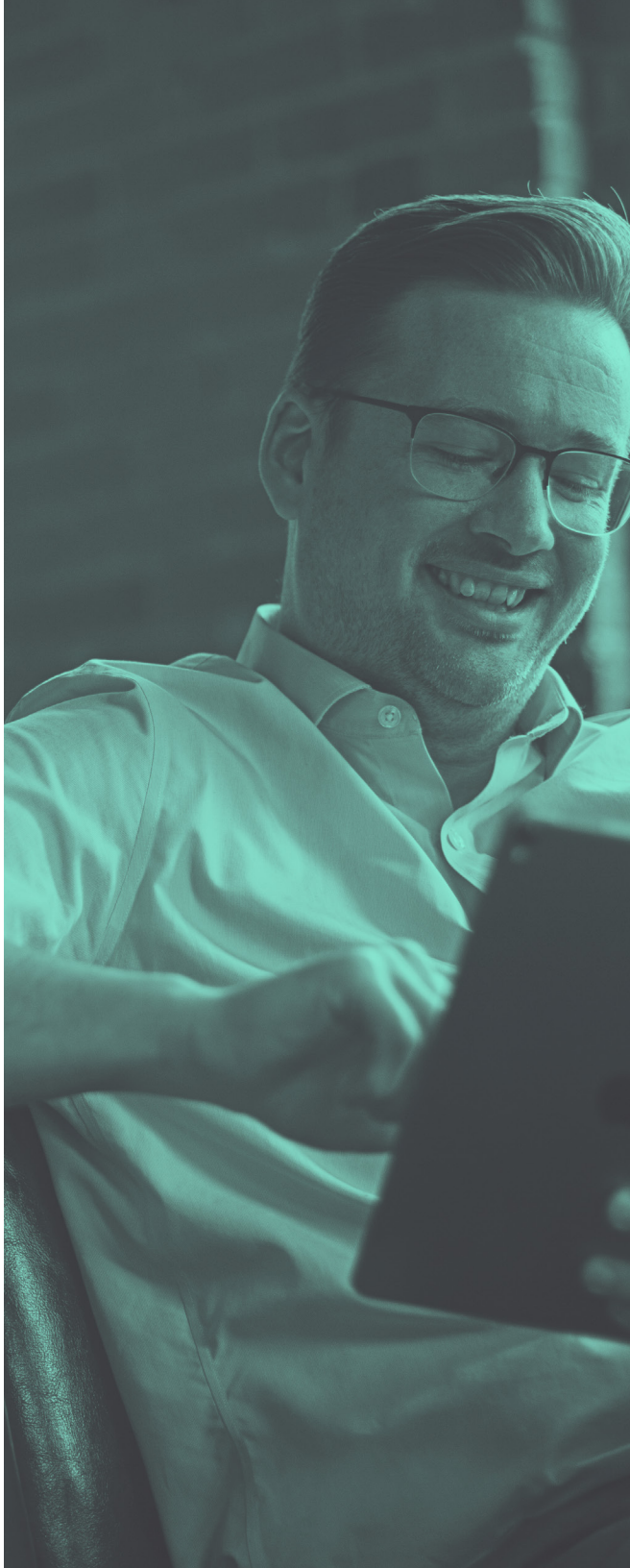
コンプライアンスとは、法律、衛生や安全の基準、データやセキュリティの要件を守ることを意味します。

単純なことのように見えますが、
実はそうでもないのです。

組織の特性によって「コンプライアンス」はまったく異なる意味を持ちます。例えば、近所の学校や町の病院にとってのコンプライアンスは、一般的な会社にとってのそれと大きく異なります。そのため、組織は各自コンプライアンス基準を用意し、従業員たちがそれを遵守できるようなシステムを構築しなければなりません。

コンプライアンスの取り組みを必要とする規制の例

- **法的規制**：差別禁止法、反奴隷法、腐敗防止法など
- **業界基準**：品質基準や個人情報保護基準など
- **セキュリティ基準**：物理的な場所の安全性の確保、デバイスの管理、個人情報の保護など
- **組織が独自に決定する規則や責任**：環境への影響、取引業者に対する要件など



コンプライアンスとは？

こういった各コンプライアンス分野において、それらが及ぼす法的影響や、従業員、生徒、患者、顧客への影響を考慮する必要があります。

また、業界によって次のような法的規制、基準、セキュリティが存在します。

- **医療機関**：HIPAA（医療保険の携行性と責任に関する法律）
- **教育機関**：FERPA（家族教育権とプライバシー法）
- **金融機関**：米国連邦預金保険公社（FDIC）の規約
- **政府機関**：米国連邦情報処理標準（FIPS）と、3つの分類区分の遵守

これらすべてを把握し、守るのは容易いことではありませんが、絶対に欠かせないものと言えます。

コンプライアンスを無視すると何が起こりますか？

以下のような、私たちの周りでよく起きていることが起こります。

- データ侵害
- データ漏洩
- 罰金または賠償金による金銭的損失
- 顧客やアカウント、仕事の喪失
- 評判の損失

国際的にも報道された3つの事例をご紹介します。

1. サードパーティアプリの脆弱性が原因で、グローバルに事業を展開する小売業者の1億1,000万人の顧客のクレジットカード情報が流出。これにより、同社の評判に大きな傷がつき、さらに1,800万ドルの損害賠償を支払うことに

2. 大手のプロフェッショナルネットワーキングサイトが、パスワード流出が原因で125万ドルの賠償金を支払うことに。さらに最近、自社のAPIの脆弱性が原因で7億人のユーザデータが漏洩。同社の信用は大きく損なわれ、経済的ダメージも予想される

3. 中国と米国の大手SNSが、それぞれ5億3,800万人と5億3,300人のユーザに影響するデータ侵害の被害に遭い、10億以上のメールアドレスおよび電話番号が流出

どれも、適切なコンプライアンス手順が踏まれていれば未然に防ぐことができたケースばかりです。

コンプライアンス管理とは？

コンプライアンス管理とは、文字通りコンプライアンスを管理する方法です。

これには、すべてのエリアにおいてコンプライアンスが遵守されていることを確認するために組織が用意するポリシーやプロセス、コンプライアンスを維持するためのデジタルツール、そしてコンプライアンスの完全な遵守に責任を持つ人々が含まれます。

これらすべてが、コンプライアンス違反を検出し、それがもたらす影響や損害から組織を守ってくれます。

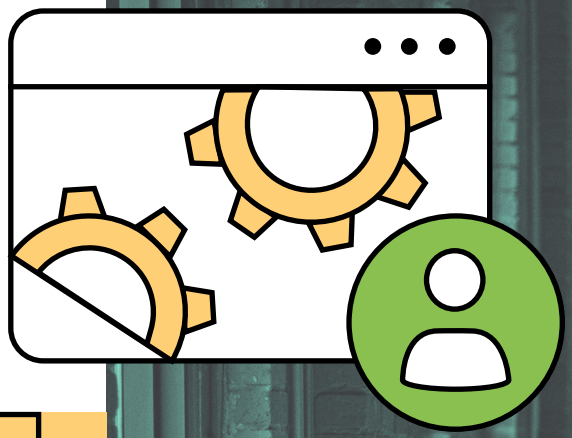
サイバーエッセンシャルとJamf

イギリスの国立サイバーセキュリティセンターが「**サイバーエッセンシャル**」制度を立ち上げた時、新たなセキュリティ要件を満たしたいと望む多くの企業がJamfに助けを求めました。

詳細はこちら（英語のみ）

実際にコンプライアンス管理を開始するには？

何から始めていいか分からないときには、他の大きなタスクを始める時と同じく、まずは扱いやすい小さなパートに分けて、サポートを求めるのが最善の策です。



正しいコンプライアンス管理を始めるためのステップをご紹介します。

1. **組織全体の理解を得る**　コンプライアンスを効率的に管理するには、組織のトップの指示のもと、すべての従業員が一丸となって取り組む必要があります。組織全体に新しいプロセスが行き渡るように、各部門から集められたメンバーで構成されたグループを作ることをお勧めします。

   異なる規制タイプ、業界に特化した規制、そしてそれらがどのような形で組織、従業員、顧客を守るのかなど、必要となるコンプライアンスの概要を把握しておきましょう。

2. **リスクの評価**　リスクを評価することは、正しいコンコンプライアンス管理に繋がります。コンプライアンス管理のそもそも目的は、最終的にリスクを軽減することにあるからです。物理的な設備や建物、倫理的・法的な保護体制、デジタル環境など、組織全体のシステムに問題がないかを確認しましょう。

3. **ポリシーの監査**　既存のポリシーを新しいリスク評価に照らし合わせることで、アップデートが必要な部分を見つけることができます。

実際にコンプライアンス管理を開始するには？

正しいコンプライアンス管理を始めるためのステップをご紹介します。(続き)

4. **トレーニング**　従業員がコンプライアンスの重要性やポリシー構造における自らの位置づけを理解し、組織の安全性を維持するためにどのように貢献できるのか、なぜ貢献しなければならないのかを理解することが大切です。

5. **「一度導入したら終わり」ではないことを理解する**　システム、ソフトウェアおよび監査プロセスを導入し、リスクや規制の遵守ステータスを見直し、システムに足りない部分が生まれる可能性を継続的に評価しましょう。自動レポーティング機能や検証審査システムを味方にすれば、問題が起こる前に把握することができます。

6. **すべての従業員の理解を確認**　必要に応じて継続的にトレーニングを行い、理解度を把握するようにしましょう。コンプライアンスの準拠を妨げる従業員がいる場合は懲戒指針を明確に示し、すべての分野においてコンプライアンスが積極的かつ一貫して確実に守られていることを確認することが大切です。

JamfはデバイスとITのセキュリティ管理の専門家です

コンプライアンス管理ではカバーしなければならない項目がたくさんありますが、同じことがITやデジタルセキュリティにおいても言えます。

コンプライアンスとは複雑なもの

だからこそJamfにお任せください

Jamfがサポートしているコンプライアンス基準

- CISベンチマーク
- DISA-STIG
- NIST 800-171
- CMMC（Cybersecurity Maturity Model Certification）プログラム：サイバー攻撃から防衛産業を保護することを目的として米防衛省によって開発された新しいサイバーセキュリティ基準
- macOSセキュリティ・コンプライアンス・プロジェクト

具体的なサポート内容

- Appleインベントリによるアイデンティティとアプリのライフサイクル管理
- ログ集約、中央記録システム、SIEM
- iOS/macOSと関連アプリのための暗号化、脅威防御およびリスクスコアリング
- 堅牢なデータポリシーと継続的なデータ流出モニタリング

しかし、これ以上に重要なのは、Jamfのワールドクラスのサポートと Appleに関する幅広い知識、そしてAppleを活用するすべての組織の成功を支援したいという信念です。

Jamfが提供するサポートにご興味のある方はお気軽に当社のスペシャリストまでお問い合わせください。無料トライアルも実施しています。

トライアルに申し込む

または、Apple販売代理店までお問い合わせください