jamf

教育機関におけるコンプライアンス初心者ガイド

児童・生徒、教職員、そして地域社会を守るために。K-12（初等・中等教育機関）向けコンプライアンス計画の策定ガイド

K-12（初等・中等教育機関）におけるコンプライアンスの最新状況

デバイスとネットワークのセキュリティコンプライアンスは、どの業界においても複雑な課題になる傾向があります。デバイスの機能拡張、法律やベストプラクティスの変化に伴い、業界基準も絶えず変化しています。

初等・中等教育機関の環境では、この複雑さがさらに増幅します。

このガイドの内容：

- **絶えず変化する教育機関のコンプライアンス要件を満たし続ける方法**
- **コンプライアンスインフラへの戦略的なアプローチが重要である理由**
- **持続可能なコンプライアンス体制を構築する方法**

本文書は情報提供のみを目的としており、法的助言を構成するものではありません。コンプライアンス要件は管轄区域や規制当局によって異なります。学校や教育機関が固有のコンプライアンス義務について判断する際は資格を有する弁護士に相談してください。

初等・中等教育機関特有のコンプライアンス課題

一般企業と同様に、教育機関においても、学校ネットワークに接続される多種多様なデバイスとユーザの安全を確保し、サイバー攻撃の脅威から守り抜く必要があります。

一方、企業とは異なり、学校は生徒や教職員だけでなく保護者や地域住民とオープンなコミュニケーションを容易に交わせることも必要であり、これらの人々は教育機関側が管理していないデバイスを使用します。

このことが広範囲にわたる脆弱な攻撃対象領域を生んでいます。多くの学校や教育機関が直面する予算面の制約も考慮に入れると、セキュリティコンプライアンスが常に難しい課題となる理由が容易に理解できるでしょう。

学校のデバイスとネットワークの利用者も特有です。

企業と学校の決定的な違い、それはユーザの圧倒的な多様性にあります。教員や管理者、事務職員だけでなく、IT管理において最も困難な対象である「子供たち」を、安全に守り抜かなければならないからです。

子どもは好奇心旺盛です。児童・生徒には、興味を引きつけるインタラクティブな学習ツールが欠かせません。次世代を担う子供たちに求められるのは、責任あるデジタル市民としての素養を養うこと。そして、得た知識を教員や家庭、コミュニティ全体で分かち合い、共に成長していくサイクルを築くことです。

子どもたちの好奇心は無限大です。.

だからこそ、学校のIT管理においては、子供たちを守るための「適切な境界線」を設けることが不可欠なのです。IT管理者の使命。それは、フィッシング詐欺やマルウェア、不適切なコンテンツから子供たちを守ることです。それも、日々の学習や授業のスピードを一切止めることなく、成し遂げなければなりません。

その上、学校はサイバーセキュリティ対策と児童・生徒のプライバシー保護を両立させることも求められます。さらに、LGBTQIA+をはじめとする特に配慮が必要な児童・生徒にとって、プライバシーの侵害は、メンタルヘルスや身体の安全を脅かす極めて重大なリスクとなります。.

重なり合うコンプライアンス基準と要件

世界のどの国や地域でも、教育現場は多方面からの厳しい監視と大きなプレッシャーにさらされています。

1. **国内外の法規制**

2. **地域の法律と基準**

3. **教育監督機関**

例えば、EUでは一般データ保護規則（GDPR）が児童・生徒のデータを保護しており、英国では英国一般データ保護規則（UK GDPR）と2018年データ保護法がその役割を担っています。米国の児童インターネット保護法のような児童・生徒に特化した法律や規制も関係します。.

さらに、米国障害者法のように、データ、ネットワーク、デバイスのセキュリティに影響を及ぼしうる要件が学校に課せられることも少なくありません。.

学校が満たそうとするセキュリティコンプライアンスのレベルを認証する機関の存在も重要です。例えば米国では、学校が政府組織と連携を希望する場合に、StateRAMPとFedRAMPという2つのセキュリティレベルを求められることがよくあります。

DX（デジタル変革）の課題

コロナ禍と学校の安全意識の急激な高まりによって、世界中の教室で劇的な変化がほぼ一夜にして起こりました。

DXに取り組む学校では、以下のような変化が進んでいます。

紙ベースからデジタルへの学習環境の移行

データの収集と保存に関する要件の増加への対応

リモート学習やハイブリッド学習と、それらがコンプライアンスに与える影響の検討

各フレームワークに共通するコンプライアンスの主眼

学校や教育機関は、企業コンプライアンスにはないさまざまな要素に加えて、以下に関する一般的な要件やベストプラクティスにも準拠する必要があります。

- データ保護とプライバシー
- デバイスとネットワークのセキュリティ
- アクセス制御と認証
- インシデント対応と侵害通知
- 監査証跡とレポート

K-12（初等・中等教育機関）を狙うサイバー攻撃は蔓延しています

残念ながら、学校や教育機関はサイバー犯罪者にとって魅力的な標的です。

学校が保有する個人識別情報などのデータは、サイバー犯罪者にとって極めて価値が高く、格好の標的となっています。教育機関の中には、給食費や諸費用の支払い用として保護者のクレジットカード情報を保管しているところもあり、犯罪者にとって楽に稼げる標的になっています。

これは世界的な広がりを見せている傾向です。英国の「2025年サイバーセキュリティ侵害調査」によると、この年、小学校の44%、中学校の60%が侵害または攻撃を受けたことが確認されています。

コンプライアンス違反がもたらす代償

代償を払ったことのある学校や教育機関は少なくありません。身代金の支払いを余儀なくされた学校、データ漏洩で保護者から訴えられた学校、ネットワーク/データの保護や情報漏洩の報告を怠って大きく報道された学校など、様々なケースがあります。

金銭的制裁と法的帰結

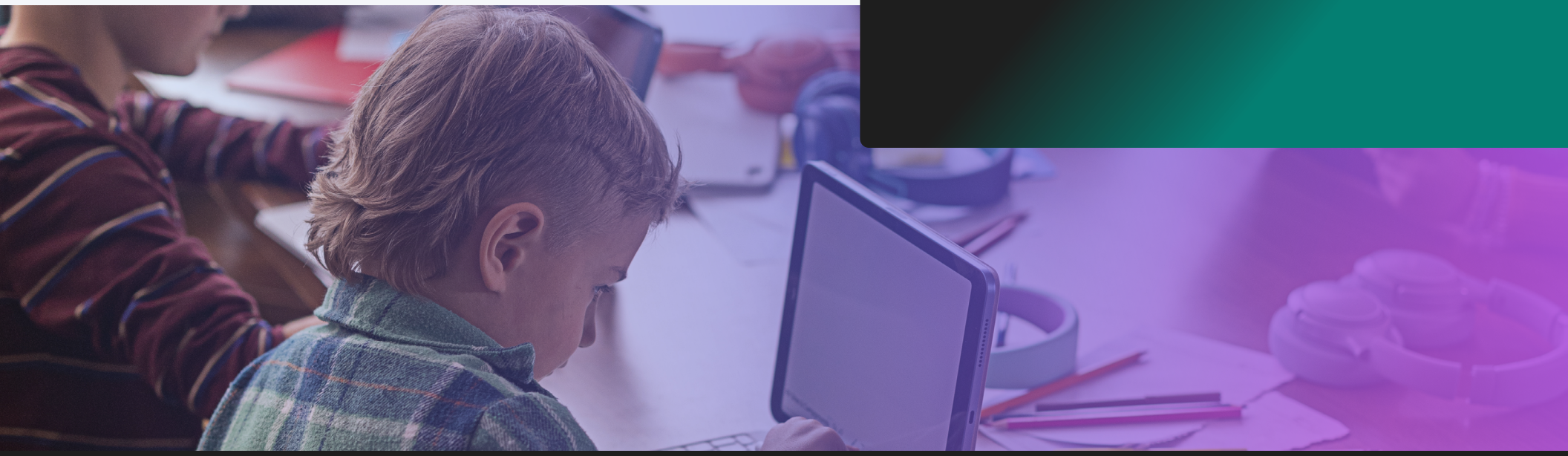
前述のとおり、厳格なセキュリティコンプライアンスやデータ保護のポリシーを順守しなかった学校や教育機関は、さらにはベンダーまでも、金銭的・法的トラブルに陥っています。

法外な身代金を支払わされたり、国内や国際的な児童生徒プライバシー保護法に抵触したり、保護者から訴訟を起こされたりする状況に直面しています。

ベンダーに対する最近の攻撃事例

2024年、広く利用されている生徒情報システム（SIS）と教育テクノロジーのプラットフォームが、身代金を支払わなければ生徒のデータを公開すると脅迫したハッカーに285万ドルを支払う事件が発生しました。

翌年には同じハッカーが同社のソフトウェアを使用している各教育機関にも接触を始め、同様の要求を突きつけました。



評判の低下と地域社会からの信頼失墜

学校は、侵害が生じた場合の公表方法について明確なルールがない場合は特に、資金提供者、保護者、地元企業といった地域社会の信頼を大きく損なう可能性があります。

教育機関に対する最近の攻撃事例

2023年にランサムウェア攻撃を受けた米国の都市部にある教育機関は、ハッカーが身代金を要求していることや、支払わなければ機密性が極めて高いデータを公開すると脅していることを公表しませんでした。教育機関は身代金の支払いに応じなかったため情報は公開されてしまいました。その後になっても、影響を受けた生徒たちへの通知は数ヶ月も放置されました。この件に対する世論の怒りは、この教育機関の評判に大きなダメージを与えました。

児童・生徒のプライバシー保護に対して、人々が敏感になるのは当然のことです。しかし、明確なガイドラインがなければ、学校や学区は周囲からのバラバラで時に矛盾した助言に翻弄され、収拾のつかない混乱状態に陥ってしまいます。対応の不透明さやブレは、人々に最悪のシナリオを予感させます。学校運営において、一貫性の欠如は信頼を失う最大の要因となります。

業務の中断とリソース配分

サイバー攻撃の最終的な目的は利益を得ることかもしれませんが、その手口は学校システムに様々な形で混乱をもたらし、結果として以下のような事態を招く可能性があります。

- **給与支払いの遅延**
- **成績通知の遅延**
- **数日間にわたる学校の完全閉鎖**

最近の学校閉鎖の事例

2026年1月、英国の中等学校がサイバー攻撃を受け、1週間にわたる完全閉鎖を余儀なくされました。この攻撃により、「電話、E メール、Google Classroom、学校管理システム、Microsoft SharePointなどの学校のITシステム全体が機能停止」に陥りました。

これらのリスクを理解したところで、続いては、堅牢なコンプライアンス計画を策定するための基本的な要素を見てみましょう。

K-12（初等・中等教育機関）におけるコンプライアンスの主要な4つの柱

1. 生徒データプライバシー

生徒データの定義

どんなデータが生徒（あるいは教職員や保護者）データに該当するかを理解することは、そのデータを保護するためのポリシーや手順を策定する最初の一歩です。このデータには、以下のようなものが含まれますが、これらに限定されるものではありません。

- 氏名、生年月日、住所、個人のE メールアドレス
- 保護者の氏名、勤務先情報、クレジットカード番号
- テストの点数や成績などの学習データ
- 健康状態、活動、出席の記録

データ最小化の原則

収集するデータの内容と保存期間を最小限に抑えることは、生徒データのプライバシー保護に大きな効果を発揮します。必要な業務の遂行に必要なデータのみを収集し、必要な期間のみ保存するようにしましょう。サイバー犯罪者は保存されていない情報にアクセスすることはできません。

実際に必要な人だけが必要なデータのみにアクセスできるようにする：
アクセスを制限することで、攻撃対象領域を小さくすることができます。

同意と通知に関する要件を設定する：収集するデータの内容と収集する理由、保存場所、保存期間を透明性をもって伝達しましょう。そうすることでコミュニティからの信頼が大いに得やすくなります。

サードパーティベンダーをきめ細かく管理する：試験実施業者や教育ソフトウェア会社などが**安全性とプライバシーに関するルールを順守していることを**確認しましょう。ベンダーにアクセスを許可するデータとその扱い方、使用目的を正確に把握するためのポリシーとワークフローを設定しましょう。これにより、最も一般的な攻撃であるサードパーティ経由の情報漏洩を防ぐことができます。

K-12（初等・中等教育機関）におけるコンプライアンスの主要な4つの柱

2. アクセス管理の要点

役割ベースのアクセスの原則

前述したとおり、ネットワークとデータへのアクセスは、教職員やベンダーに必要最小限の権限のみを付与して管理することが極めて重要です。業務に必要なものだけを与え、それ以上は与えないようにしましょう。「誰が、いつ、何にアクセスすべきか？」を常に自問してください。

役割ベースのアクセス制御（RBAC）の徹底

教職員が必要な時に必要な場所でアクセスできるように権限を制御しつつ、ゲストや訪問者には最小限のアクセス権限のみに制限できる安全な仕組みを確保しましょう。このような権限は、生徒、保護者、教職員のIDに紐づけることで最も効果的に管理できます。

年齢に基づく柔軟性

アクセスと認証の要件は、役割だけでなく年齢によっても異なる場合があることに留意しましょう。低学年の児童は複雑なパスワードを覚えられないかもしれませんが、高学年の生徒なら可能です。当然、生徒の年齢が上がるにつれて、新しいカリキュラムに基づくアクセス権限も変化します。生徒に学年別や年齢別の役割を割り当てることで、長期的には管理の手間を大幅に省くことができます。

K-12（初等・中等教育機関）におけるコンプライアンスの主要な4つの柱

3.

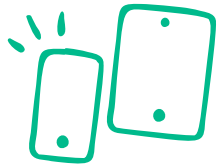
セキュリティインフラの要件

セキュリティインフラの要件を明確に設定し、堅牢なエンドポイント保護戦略を策定することは、侵害を一部で食い止められるか全体に及んでしまうか、デバイスが侵害されるか安全な状態に保たれるかを分ける重要なポイントです。

エンドポイント保護戦略

以下の機能を提供するエンドポイント保護が導入されていることを確認しましょう。

- 自動化された脅威防御と修復
- デバイス上での分析とプロアクティブなレポート
- データポリシー運用の自動化と強制適用



機能そのものと同じくらい重要なのは、ソリューションの導入によってセキュリティ、プライバシー、パフォーマンスが損なわれないようにすることです。

ネットワークのセグメント化に関する考慮事項

一部の被害を全体のシステム停止に繋げないための最善策の一つは、ネットワークの分離です。利用者や組織の部門に基づいてネットワークを分割・管理することが重要です。例えば、管理者・教職員用ネットワーク、生徒用ネットワーク、ゲスト用ネットワークなどが考えられます。

ージへ続く...

K-12（初等・中等教育機関）におけるコンプライアンスの主要な4つの柱

3. セキュリティインフラの要件

暗号化の基準と実装

各規制当局が求める暗号化および実装の戦略と、実装可能なベストプラクティスを詳しく確認しましょう。

- 強力な暗号化アルゴリズム
- セキュアな鍵管理
- 保存中および転送中のデータ暗号化

定期的なセキュリティ評価

生徒数は変化し、教育テクノロジーツールは進化するため、セキュリティ評価を定期的に実施することが必要です。このようなセキュリティ維持はコンプライアンス状態を保つうえで欠かせない取り組みです。

評価を実施することで、以下のことが可能になります。

- 新しいテクノロジーや新興テクノロジーの導入
- 内部/外部のコンプライアンス要件やベストプラクティスの変化に合わせたポリシーの策定
- レポートの手薄な箇所や新たなレポートニーズの確認
- ベンダーの評価や新たなニーズや拡大したニーズへの適合性の確認

K-12（初等・中等教育機関）におけるコンプライアンスの主要な4つの柱

4. 文書化と監査の準備

監査への準備は、ともすれば「面倒な雑務」のように感じられるかもしれません。しかし、監査に対して適切に備えておくことは、いざという時の大幅な時間短縮になるだけでなく、長期的にはネットワークやデータの安全性をより強固に保つことにも繋がります。

準備方法は以下のとおりです。

管理・レポートすべき主なデータカテゴリ

追跡が必要なデータには主に3つのグループがあることを念頭に置いてください。

生徒データ：出席状況、成績、活動記録
運用データ：IT資産レポート、ネットワーク構成、セキュリティログ
法務データ：コンプライアンス文書、ベンダー契約、監査報告書

重要な記録管理の取り組み

データを安全で一元化され、コンプライアンスに準拠した状態に維持しましょう。主な取り組みには次のようなものがあります。

- 生徒情報システム（SIS）の活用
- ハードウェア/ソフトウェアインベントリの管理
- 状況に即した記録のデジタル化

ージへ続く...

K-12（初等・中等教育機関）におけるコンプライアンスの主要な4つの柱

4. 文書化と監査の準備

ログと監視の自動化

セキュリティログデータをリアルタイムで自動的に収集・分析・対応する取り組みが実装済みであれば、監査ははるかに容易になります。常に最新のリストが保持されるだけでなく、セキュリティ上の脅威を先回りして特定し、本格的な攻撃に発展する前に解決することができます。

インシデント文書化の手順

セキュリティインシデントは「もし起こったら」ではなく「いつ起こるか」の問題です。起こったときに備えて、文書化の手順を事前に策定しておくことで、学校内外で不信感を招かないようにできます。以下の内容を記録・提示する手順を整えましょう。

- 時系列に沿ったインシデント発生状況の明確な記述と、インシデント対応に使用したツール
- 安全面・運用面・財務面の影響評価
- コマンド出力、ログファイル、影響を受けたシステムに関するレポート

定期的なコンプライアンスレビュー

定期的なセキュリティ評価と同様、この取り組みも欠かせないものです。コンプライアンスのツールや要件、ベストプラクティスは常に変化します。定期的にコンプライアンスを見直すための時間と人員を確保することで、法的制裁や罰金、長期的な評判低下を防ぐことができます。

コンプライアンス準備態勢の診断と現状分析

準備はできていますか？

セルフチェックのためのリスト

厳格かつ複雑で、絶えず進化するこのプロセスの実装には、なかなか着手しづらいかもしれません。
以下の有用なチェックリストを活用すれば、チームは見落としを出すことなく準備を整えられます。

ITインフラの対応状況

以下の項目が導入・整備されていますか？

- [ ] デバイスのインベントリ・管理システム
- [ ] ID管理とアクセス権限の一元化
- [ ] 生徒用システムと事務用システム間のネットワーク分離
- [ ] すべてのデバイスへのエンドポイント保護の導入
- [ ] 保存中および転送中のデータ暗号化
- [ ] 自動化されたバックアップとリカバリの手順
- [ ] セキュリティ監視とアラートの機能

ポリシーとガバナンスの準備状況

以下の項目を文書化または確立していますか？

- [ ] 包括的な利用規定
- [ ] データの保持と廃棄に関するポリシー
- [ ] インシデント対応手順
- [ ] 職員トレーニングプログラム
- [ ] ベンダー管理・適正評価プロセス
- [ ] 定期的なポリシー見直しと更新のスケジュール

.

運用面の準備状況

以下を実施していますか？

- [ ] コンプライアンス担当者または担当チームの任命
- [ ] 定期的なセキュリティ評価
- [ ] 監査証跡機能の有効化
- [ ] 侵害通知手順の確立
- [ ] 保護者および生徒とのコミュニケーション方法の設定
- [ ] 文書化・記録管理システムの有効化

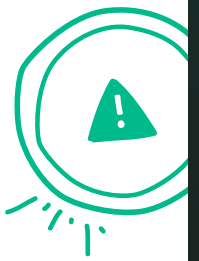
ベンダーおよびサードパーティの準備状況

以下の項目は策定済みですか？

- [ ] すべてのベンダーとのデータ処理合意書（DPA）の締結
- [ ] セキュリティ認証の検証プロセス
- [ ] 定期的なベンダーセキュリティ評価
- [ ] 明確なデータ共有とアクセスの制御
- [ ] ベンダーによるインシデント通知の義務化

Jamf for K-12によるコンプライアンス支援

Jamf for K-12は、それ自体で学校のコンプライアンスを自動化・保証するものではありませんが、以下の機能を通じて包括的なコンプライアンス戦略を支援する強力なインフラを提供します。



デバイスの管理とセキュリティ：

- デバイスの登録と構成の一元化
- セキュリティポリシー適用の自動化
- リモートでのデバイスの管理と保護
- 包括的なデバイスインベントリとレポート

拡張可能な管理：

- すべてのデバイスに対する一貫したポリシー適用
- 大規模なデバイス導入の効率的な管理
- 大規模なデバイス環境に拡張可能なポリシー展開
- 多様な学習環境（1人1台、共有デバイス、BYOD）のサポート

アクセス制御と認証：

- シングルサインオン（SSO）を実現するためのIDプロバイダとの統合
- 役割ベースのアクセス管理
- 役割に基づいたアプリとコンテンツの制限
- デバイスやプラットフォームを横断した安全な認証

統合機能

- 既存の学校情報システムとの連携
- サードパーティ製教育用アプリケーションのサポート
- ネットワークインフラとの統合
- アイデンティティベースのアクセス管理ソリューションとの接続

Jamfのプラットフォームは、コンプライアンスフレームワークに必要な信頼性・安全性・管理性に優れたテクノロジー環境を教育機関が構築するための基盤となります。

Jamfの自動化機能と高度なテクノロジーにより、担当者は日々のデバイス管理に追われることから解放されます。その結果、ポリシーの策定やトレーニング、戦略的なコンプライアンスの推進といった、より本質的な業務に専念することが可能になります。

K-12のコンプライアンス
に終わりはありません。

コンプライアンスとは一度限りの取り組みではありません。導入しているテクノロジー、在籍する生徒、そして法規制を取り巻く環境の変化に合わせ、絶えず進化させていくべき継続的なプロセスなのです。

心配は無用です。その基盤を、学校（あるいは現場）だけで築き上げる必要はありません。

Jamf for K-12導入することで、デバイス管理やポリシー運用の自動化、さらには厳格な監査への備えが、ひとつのプラットフォームで完結します。管理の煩わしさから解放され、教育環境の質を高めるための本質的な業務に集中できるようになります。

まずは無料トライアルから

jamf