



PFISMモデル をスマートに実現

指導へのタブレットやノートパソコンの導入をJamfのソリューションが余すところなくサポート

「PFISM (Parent-Funded, School-Managed)」と呼ばれるモデルを採用する学校が増えています。これは生徒各自の学習用タブレットやノートパソコンを保護者に購入してもらい学校が一元管理するデバイス運用モデルで、生徒用デバイスを学校で調達する必要が一切ありません。所有・保管は各家庭に託しながら、学校のIT管理者が一元的に構成・管理・セキュリティ維持を行えます。

各家庭がすでに所有しているデバイスを持ってきてもらう「BYOD」というモデルもありますが、学校が管理しないため死角ができてしまいます。PFISMモデルであれば、安全かつ公平で統一された学習環境が整えやすくなります。



PFISMとBYODの比較:教育現場での違い



	PFISM	従来型BYOD
デバイスの制御	学校がJamf製品で一元的に行う	学校は関与できない
セキュリティ	一元的に強制適用	各家庭の判断
学習ツールへのアクセス	全生徒で統一	生徒ごとにバラバラ
IT管理者からの可視性	高	低
ポリシーの適用	学校外にある時も全面適用	不可能
学習の公平性	手段と機会が均一	不均一

構想を現実に: JamfがPFSMの成功を強力に後押し

PFSMモデルを円滑に導入するには、IT管理者に適切なツールが不可欠です。Appleデバイスのために開発されたJamfの教育機関専用ソリューションなら、生徒用デバイス全体の管理・可視化・セキュリティ確保を実現できます。

学習の一貫性



Jamf for K-12 + Appleのデバイス監視機能

- 学校のポリシーに準拠する構成をデバイスに設定
- アプリを自動的に導入・アップデート
- 注意散漫を防ぐ制限を適用

教室でのデバイス制御



Jamf Teacher + 「Appleクラスルーム」アプリ

- 特定のアプリやテスト以外に使えないようデバイスをロック
- 授業中の生徒のデバイス操作を監視
- 授業に遅れず集中できるように誘導

セキュリティと安全なインターネット閲覧



Jamf for K-12

- 学校のポリシーに基づいてWebコンテンツをフィルタリング
- 悪意のあるサイトや不適切なサイトをブロック
- パスコードの使用とOSレベルのセキュリティを強制的に適用
- 紛失・盗難デバイスのロックやワイプをリモート実行

家庭でも使用できる柔軟性



Jamf Parent + Jamf for K-12

- 放課後の使い方の管理は家庭に
- 学校と家庭で構成を切り替え
- 柔軟性は保ったまま見守りを維持

PFSMモデルの採用に伴う課題を回避しましょう。 陥りがちな落とし穴にご注意。

PFSMは学校側のコストを抑えながら学習機会を広げられる理想的なモデルですが、導入する意義を正しく理解していないとリスクを招いてしまう可能性があります。ここでは、陥りがちな落とし穴と、Jamfソリューションでそれを避ける方法をご紹介します。

落とし穴1:

生徒用デバイスが監視対象外になっている

- ⊗ 監視対象外のデバイスは一元管理の対象外にもなるため、学校の目の届かない使い方ができてしまいます。
- ✔ JamfソリューションとAppleのデバイス監視機能を組み合わせて使うことで、把握・管理から漏れる生徒用デバイスをゼロにできます。

落とし穴2:

教える側に対する支援がない

- ⊗ 正しく設定されたデバイスであっても、教室で教師が制御できなければ、逆に生徒の集中力を妨げる要因になりかねません。
- ✔ Jamf TeacherとJamf Studentアプリを組み合わせれば、教師はデバイス进行操作するタイミングをリアルタイムで指示できるため、生徒は課題に集中できます。

落とし穴3:

IT管理者の負担が過小評価される

- ⊗ 家庭所有のデバイス全部に対して設定やサポートを手作業で行うのは無理難題です。
- ✔ Jamfソリューションを使用すれば、大量にあるデバイスの設定・アップデート・管理を自動で、しかもスマートターゲティング機能により学年別・グループ別・クラス別に実行できます。

落とし穴4:

学校外にあるデバイスの保護を軽視する

- ⊗ 学びは場所にとらわれませんが、リスクも同じです。
- ✔ Jamf for K-12とJamf Parentを使用すれば、生徒が自宅でデバイスを使う際にも、フィルタリングとポリシーの適用を徹底できます。