デバイス1,000台を1人で管理するには:

教育現場で大量のAppleデバイスを一括管理および保護する方法

はじめに:比率の問題

教育機関は、生徒それぞれの学びのパーソナライズ、リソース利用機会の拡大、学習成果の向上という明確な目的の下、テクノロジーに投資しています。デバイス数の増加、1人1台施策の拡大、場所を問わず最適な学びをサポートするデジタルツールへの取り組みの強化がその表れです。

しかし、デバイス数が増えるにつれ、教育現場における運用に負担が生じます。この負担は、導入規模が教育分野におけるデバイス数とITサポート要員数の平均比率である1,000:1を超えると顕著になります。このような状況では、教育の運営が肥大化し、持続が困難になります。

その結果、IT担当者は常に「火消しモード」なってしまいます。つまり、問題から問題へと奔走し、環境整備という本領に集中する余裕がなくなり、ユーザに価値を提供できなくなります。

デバイスライフサイクル管理の中核的なタスクには、次のようなものがあります。

- デバイスの初期設定
- パッチ管理
- セキュリティ監視
- インシデント対応
- 安全なデータ消去

これらのタスクは、限られた人数のIT担当者により数千、数万のエンドポイントに対して手動で行われています。さらには次のように、所要時間はほんの数秒であるものの定期的に発生するタスクもあります。

- パスワードのリセット
- アプリのインストール
- Wi-Fiアクセスの構成

要請の量とそれに対応できる人数に大きな差があるために、解決までに非常に長い時間がかかっています。

この状況を表す一言:アンバランス

アンバランスによって活動中断が発生する

アンバランスの影響は学校全体に連鎖的に広がります。

教室では、接続の不具合が日常的に発生してデジタルリソースにアクセスできなくなります。この問題が発生した場合、現場で対応するのは大抵が教員であり、授業を中断してトラブルシューティングすることになります。

生徒にとって、アンバランスの影響はストレスとなって現れます。教育を充実させるためのテクノロジーだとしても、デバイスが反応しなかったり、アプリがクラッシュしたりすると、生徒はイラ立ち、目の前の課題に集中できなくなります。

時間が経つにつれ、アンバランスの悪影響は深刻化します。生徒と教員の間のずれが広がり、ひいては教員と学校自体のずれが起こります。テクノロジーの機能不全による生徒の学習意欲・機会の喪失から、教育機関そのものが抱える課題に至るまで、そこには一つの共通した因果関係が存在します。それは、教育目標の達成や期待される成果に対して、否定的な影響をもたらすという点です。

一つひとつの悪影響はより大きな問題の一症状にすぎませんが、これらからより広範で、戦略的な問題の存在が見えてきます。学校が無事にデバイスを配布できたとして、包括的なIT戦略にスケーラブルな管理とサポートプロセスを組み込んでいなければ、テクノロジーで実現できるはずの教育成果を得にくくなってしまいます。信頼性、使い勝手、セキュリティが生徒、教員、学校の期待にそぐわず、デジタル格差が解消するどころか、さらなる障壁が生まれてしまいます。

手動プロセスのコスト

デバイス1台の初期設定を手動で行う場合の平均所要時間は2〜4時間です。最小時間で考えると、次のような式が成り立ちます。

1,000 台 X **2** 時間 = **2,000** 時間の初期設定作業

比較として、実際に作業可能な時間数を考えてみましょう。一般的な学校の業務時間は1日あたり8時間、1週間あたり5日です。夏期休暇（年1回の定期更新を行う主要期間）は平均10週間です。

8 時間 X **10** 週間 = **400** 時間の作業（IT担当者1人あたり）

つまり、400時間で2,000時間分の作業量を行わなくてはなりません。ここにデバイスの構成ミス、作業疲れ、防ぎようのない要素も加味すると、初期設定に要する時間は最高値の4時間に近づきます。

現代の初等・中等教育機関では規模に比例して1台あたりのコストを下げるよう求められていますが、手動プロセスにそれは不可能です。求められていることと可能なことに差がある原因は、人ではありません。ほとんどの場合、アーキテクチャが問題です。

本題に入る前に

デバイスライフサイクル管理において、ダウンタイムを最小限に抑え、デバイスを即使用できる状態に初期設定してユーザの手元に効率的に届けるうえで、スケール（規模）は重要な要素です。スケールには、よく似ていますが、微妙に異なるもう1つの意味があります。それは、教育活動への影響を最小限に抑えながら、導入（導入済みデバイスの保守を含む）を効率的に行う能力のことです。

どちらも同じ意味と見なされがちですが、必要な対処方法が同じであること除けば、中心的な部分はまったく異なる概念です。

IT分野におけるスケーリングの基礎認識：
「繰り返し作業の対象となるデバイスを増やす」。

この定義を踏まえると、新規デバイスの導入であるか、デバイスのコンプライアンスの確保であるか、その両方を行うのかにかかわらず、学校でスケーリングを進める場合には以下の3つの重要事項を考慮する必要があります。

不統一：スケーリングにおける標準化の重要性

標準の確立は、スケーラビリティの基礎となり、スケーリング作業の成功を左右するため欠かせません。では、なぜ標準が重要なのでしょうか。それは、変わりうる要素（変数）が存在すると、デバイスに予期せぬ様々な影響が及ぶからです。

こうした変数に対処していない、または考慮していない場合、その影響はちょっとした不便で済むこともあれば、エンドポイントや教育に必要なソフトウェア・構成・システム設定の導入を最初からやり直さなければならないほど深刻になるおそれもあります。

標準化の第一歩は、「ユーザに支給する準備が整った」ことを表すデバイス状態を特定することです。生徒にとっては、これは「学習準備が整った」状態を指し、生徒が学習で能力を最大限発揮できるように学校、学年、登録した授業に必要なすべてが揃っている必要があります。

本書の対象範囲を踏まえると、「学習準備が整った状態」の特定について学校ごと、生徒ごとの違いはないように思えるかもしれませんが、実際は異なります。生徒、教員、学校、地域のニーズなど、大きな違いが多数あるからです。本書の目的は、考えうる標準の膨大な組み合わせを示すことではありません。学校の管理者や教育者に対して学習準備が整った状態を定義する重要性を示し、IT担当者に対して初期設定ワークフローに標準を取り入れ、導入するデバイスがユーザに必要なベースラインを毎回確実に満たすよう促すことにあります。

管理するデバイス数の拡大 = 導入展開の規模拡大、ではない

標準を策定する際に考慮すべき重要なポイントは、柔軟性をどの程度持たせるかです。標準が厳格すぎると、問題が起こったとき（必ず起こります）、標準がニーズに合わず、ダウンタイムが長期化します。その都度固有のニーズに合うように、IT担当者がデバイスを手動で構成しなければならないからです。しかし、標準が緩すぎても、ユーザに必要なツールへのアクセスを提供するという目標を達成できないうえ、環境全体の基本的な管理機能とセキュリティ保護が不足してしまいます。いずれの場合も、多様なユーザのニーズを満たすために手動でデバイスを構成する結果になります。

柔軟性の鍵はバランスです。ハードウェアとソフトウェアの構成を網羅的にするほど、標準の汎用性は高まりますが、セキュリティが低下するので注意が必要です。例えば、生徒向けのiPadに、成績評価に使用する教員向けアプリが含まれている状況を考えてください。あるいは、教員用のノートパソコンと、生徒用の共有ノートパソコンが兼用になっていて、教員が授業計画を保存しようとしたら、生徒が保存したデータでデバイスのストレージ容量が一杯になっておりエラーメッセージが表示された状況を考えてください。

柔軟性に関して伝えたいのは、デバイスを兼用できないということではありません。標準を策定する際は目的の考慮が重要だということです。目的には、学校固有のニーズを正確に盛り込むだけでなく、ユーザに提供するハードウェアとソフトウェアリソースの現実を反映させます。そうすることで、デバイスの導入や再設定が楽になると共に、ユーザがその本分を果たすために必要なツールやリソースに安全にアクセスして、学習や授業を円滑に進めることができる柔軟性が織り込まれます。

スケーリングが失敗する状況の例

ここまでの話をまとめます。「標準」は、デバイスを導入する際に、学習準備が整った状態にデバイスを毎回構成するための基礎的な枠組みを与えるものです。「柔軟性」は、ユーザのニーズの変化に合わせて標準が適応する能力について、教育活動やIT運用の中断を最小限に抑えて出来る限りシームレスに適応するという目的に照らして評価したものです。

この場合、「効率性」は、IT担当者が「標準」を学校内のデバイス全体へ「柔軟に」実装する際にかかる時間の度合いを指します。導入されているデバイスは学校ごとに大きく異なるため、効率性を定量的なデバイス数で測ることはできません。代わりに、デバイスの初期設定・ユーザへの提供・デバイスライフサイクル全体を通じた継続的な保守作業を既存のワークフローでどの程度円滑に行えるかで判断します。デバイスがクラス共用のiPadであるか、地域の方針で複数学年にわたって学校が変わっても個人で継続して使う1人1台のMacBookであるかは問いません。

スケーリングを試みる際、今なお手動ワークフローを使用している学校で起こりやすいのが、効率性でつまずくことです。導入展開（プロビジョニング）の現場において、最も頻発するトラブルが「デバイスの設定ミス」や「必要なソフトウェアの入れ忘れ」であることは言うまでもありません。しかし、どれほど関係者のニーズを把握して「基準（標準化）」を確立し、学校側の変数（個別事情）を考慮した「柔軟性」のある計画を準備していたとしても、根本的な事実は変わりません。それは、デバイス数の増加に伴い、手作業によるプロセスは指数関数的に脆弱（不安定）になるため、最終的には展開プロセス全体が破綻をきたすということです。

効率的でスケーラブルなワークフローの真の評価基準は、1,000台（さらに言えば10,000台）のデバイスの導入を1台、10台、100台のデバイスの導入と同じく容易に、ユーザの活動を妨げることも、運営に悪影響を及ぼすことも、取り組んでいるIT担当者を疲弊させることもなく、安定して行えるかどうかです。

覚えておきたいAppleの設計哲学：

「it just works.」（とにかくちゃんと動く）

要点：疲弊を招くことなく導入を拡大する鍵は再利用性

初等・中等教育機関のデバイス運用の規模を拡大していく上で、最も重要であり、現場の共感を呼ぶキーワードは**再現性（仕組み化）**です。変数に影響されることなく、複数のデバイスに同じ手順を繰り返せれば、運用負荷を最小限に抑えることができます。

しかし、受動型を能動型に、バラバラをキビキビに、手動をオーケストレーションへと変える要因は何でしょうか？

答えは「自動化」です。具体的には、複数のツールを統合して1つのシームレスなアーキテクチャにして、デバイス管理、アイデンティティベースのアクセス管理、エンドポイントセキュリティのワークフローの相乗効果を生み出します。これにより、IT担当者や技術担当者が疲弊することなくスケーリングできる再利用性を実現するうえで重要となる、以下の3つの目標を実現できます。

リソース

一貫したユーザエクスペリエンスで教育目標の達成に寄与するように、ハードウェアとソフトウェアの初期設定を**標準化**します。

有効性

学習ツールへのアクセスを効率化する**柔軟**なワークフローを確立して、教育と学習の中断を最小限に抑えます。

経済性

技術的**効率性**で手作業の負担を取り除き、浮いた教育費用を転用して大きなROIを実現します。

導入戦略を策定する際に考慮すべきことは、すべてを一斉に自動化するのではなく、まず学校や地域固有のニーズを評価して導入とデバイス管理において最も重要な側面に的を絞り、得られるメリットが最も大きいところを自動化することです。

ワンポイント：自動化できるという理由だけでは、自動化するべき（自動化がユーザに有益である）ことにはなりません。

自動化の目的は明確で、包括的かつ再利用可能なワークフローを導入し、手作業を予測可能な作業へと変えることです。力まかせに進める（手作業の必要性に対応するために人員を追加して）のではなく、よく考えて設計されたアーキテクチャ（再利用可能なワークフローによって自動的に統一）の下でこのワークフローを再利用することで、スケーリング要件を満たすことができます。

手作業では、いつまでも困難がなくなりません。IT担当者が手動ワークフローを教育目標に合わせようと試行錯誤しているようでは、以下の作業のために「火消し」モードから抜け出せません。

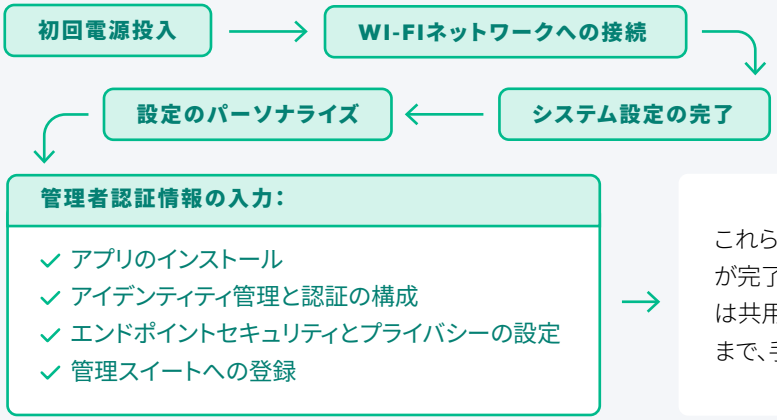
- ハードウェアとソフトウェアのリソースの**正確なインベントリリストを維持する**（デバイスとライセンス割り当てを含む）。
- **積極的にデバイスを監視**し、脆弱なデバイスのリスクが緩和されるようにOS・ソフトウェア・セキュリティのアップデートを適用する。
- 学年や活動場所の異なる生徒・教員用にそれぞれの要件を満たすように**デバイスを構成する**。
- 複数のプラットフォームと様々な種類のデバイスに**ベースラインコンプライアンスを適用**し、統合レポートと監査可能な証拠を用意する。
- 進化を続けるサイバー脅威から**エンドポイントを保護**し、規制要件に従ってユーザのプライバシーを守る。
- **修理の依頼と設備の修繕**に加え、使用寿命を迎えたデバイスの返却・廃棄を行う。

逆に言うと、自動化とは、高度なテクノロジー（本ホワイトペーパーの各章で説明）を組み合わせて1つのソリューションに統合し、「夢のようなワークフローを運用可能な形で円滑に現実化する」ことです。その結果、以下のようなデバイスライフサイクル管理の統合戦略が完成します。

- **デバイスプログラムの成長に合わせて効率的にスケーリング。**
- **学習を始める準備が整ったデバイスすべてで一貫性とコンプライアンスを実現。**
- **学習目標と教育成果をサポート。**
- **業務の力点を手動設定から教育との連携にシフト。**
- **再利用可能な自動導入モデルを採用。**
- **再利用可能なワークフローで、規模によらずIT部門の力を引き出す。**

大規模環境における登録と初期設定

夏期休暇中の大半の時間、IT担当者は新しいデバイスを開梱して作業ラインに並べ、各デバイスを手で操作して以下の作業を行います。



これらのステップを、各デバイスの設定が完了し生徒や教員に支給する（または共用向けに配置する）準備ができるまで、手動で何千回も行います。

しかし、いざ新学期が始まってみると、以下の理由で授業も勉強も行えません。

- デバイスがWi-Fiに接続できない
- ユーザがログインできない
- 必要なアプリがインストールされていない
- セキュリティ設定にミスがある
- 教員用デバイスが生徒用の設定になっている（またはその逆）
- MDMに登録されていないデバイスがある

上に示したのは、初等・中等教育機関にテクノロジーの導入が始まって以来、あらゆる学校が悩まされている問題の実例です。

問題は「IT担当者の努力が足りていない」ことではありません。大量のデバイスを短期間でスムーズに導入するためにはスケールメリットを活用する必要があるのに、相容れない手動の初期設定プロセスを採用していることです。人間には限界がありますし、作業に疲れることもあり、ときにはマーフィーの法則が当てはまってしまうこともあります。デバイスの数が増えるほど、プレッシャーの増大や制御不能な変数が原因で手動プロセスのほつれが目立つようになります。

この問題を解決するためにハリー・ポッターのような魔法使いになる必要はありません。重要なのは魔法ではなく、アーキテクチャだからです。1,000台以上のデバイスをMDMに登録したり、対象ユーザに合わせて自動的に初期設定したりするのは確かに魔法のようですが、何より素晴らしいのはIT担当者がデバイスに触れなくてよいことです。デバイスを開梱して電源を入れるだけで、ワークフローが始まります。ワークフローの進行中でもデバイスを使用できるため、ユーザはすぐに授業/学習を始めることができ、待たされることはありません。

デバイスの手動構成にかかる平均時間は2〜4時間です（構成ニーズにより異なります）。ワークフローを受動型（手動）から能動型（自動）に変えると、構成時間を削減でき、**Macなら約15分、iPadならさらに短く5〜7分**になります。

方針：労力ではなく、工夫を増やす

スケーリングの第一歩は登録です。結局のところ、一括管理、アイデンティティ管理、セキュリティのないデバイスは、しっかりした土台のない家のようなものです。

この点に留意し、Jamfが提案するスケーラビリティのレシピは、3つの不可欠なテクノロジーを緊密に連携させ、登録と初期設定ワークフローを完全に自動化するというものです。これなら、クラス・学年・学校・キャンパスをまたいで、地域全体にさえもシームレスに実施できます。

Apple School Manager（ASM）で登録を自動化

Appleまたは正規販売代理店から直接調達したAppleのハードウェア（Mac・iPad・Apple TVデバイス）は、ASMアカウントにリンクされています。Jamfインスタンスも ASMにリンクすれば、現在だけでなく今後の機器購入も自動的にJamfに表示されるようになり、登録プロセスをできます。さらに、ASMを生徒情報システム（SIS）データと統合すると、生徒と教職員の情報へ簡単にアクセスでき、何時間もかけてデバイスリソースにアクセスするための認証情報を各生徒や職員用に手動で作成しなくて済むようになります。

つまり：MDMへのデバイス登録や管理対象Apple IDの作成があらかじめ行われるので、手動の入力や作業は必要ありません。

ニーズの高まりに応じてJamfで基本的な管理を進化させる

Jamfはそれ単独で、デバイス管理の複雑さを最小限に抑え、唯一の情報源の役割を果たす特化型ソリューションです。同じく重要な特長として、デバイス管理、アイデンティティベースのアクセス管理、エンドポイントセキュリティを設計段階から統合しており、初等・中等教育機関のデバイスライフサイクル管理の負担を大幅に削減します。初等・中等教育機関の環境で使われる一般的なツール（デジタルサイネージ、学習管理システム（LMS）、統合レポートなど）をサポートしているほか、登録の土台を用意し、以降の各段階における中心的な接点の役割を果たします。基本的なセキュリティ体制の実装も、能動的な監視とポリシーベースの修復も、最新状態のインベントリリストの維持と安全な廃棄ワークフローの実施も、Jamfだけで完結します。

ゼロタッチでデバイス初期設定を効率化

ASMとJamfのシームレスな統合により、初等・中等教育機関のインフラ全体でゼロタッチ導入が可能になります。スケーリングを学年、校舎、あるいは学校をまたいで行う場合でも、新規機器導入なのか、問題解決のための再設定なのかにかかわらず、一貫性のある形でデバイスを導入できます。デバイスはユーザのニーズに応じて一貫性を持って瞬時に自動で初期設定されるため、教育活動が中断される事態やヘルプデスクへの問い合わせが減り、ユーザはすぐに生産性を発揮し、IT担当者はエクスペリエンス向上に注力できるようになります。

構成の一貫性の確保

このホワイトペーパーでは、「一貫性」という言葉をばらつきの問題に関して使っています。具体的に言うと、ばらつきはデバイスの設定ミス（構成ドリフトとも呼ばれる）の主な原因であり、導入失敗の一因になります。

一般的に、テクノロジーを長期にわたって使用していると、どうしてもドリフトが発生します。アプリのインストールやOSアップデートなどの必須の作業によって、既存の構成を変更せざるを得ない状況を考えてください。ここで重要なのは、ドリフトが繰り返しのタスクを行う際の注意不足に伴って起きるものでもあると認識することです。1つでも手順の抜けやわずかな設定ミスがあると、手作業での修正に1台あたり30秒かかってしまいます。1,000台すべてを手動で修正する場合、積み重なって8時間の教育時間の損失になります。

1,000
台
X
30秒
1台あたり
＝
8
時間以上の損失

上記は、1つの問題に対応する担当者1人だけを考えた場合です。対応にかかった時間（またはその時間を換算した金銭）があれば教職員、児童・生徒、IT担当者、経営陣、機関が何をできたかと考えてください。

その答えから、一貫性が重要な理由がはっきりします。また、大規模環境では一貫性を軸にしたワークフローが重要であることも浮き彫りになります。

学校が初期設定と導入のワークフローで一貫性と効率性を達成するには、どうすればよいでしょうか。答えは、ワークフローを導入する前に、具体的なタスクに合わせて設計することです。このタスクでは、デバイスの「学習準備が整った」状態がどのようなものかを定義します。この状態は学校ごとに異なるものなので、初等・中等教育機関が一貫性を実現する道はまず、アプリ、設定、構成（つまり、児童・生徒や教職員が学習・授業に必要なものすべて）を特定し、その学校において学習準備が整った状態がどのようなものかを文書化することから始まります。

アプローチ：レジリエンスを考慮して計画を立てる

「1時間を計画に費やせば、作業時間を10時間削減できる」

– Dale Carnegie

「学習準備が整った」状態を定義することが、登録とスケーラビリティの共通部分です。この重要な情報が確定したら、Jamfのツールとテクノロジーによって、各ユーザのペルソナに合わせた一貫性の実現を容易に進められます。つまり、大規模環境において導入を標準化し、ドリフトを最小限に抑えることができます。

Jamfのブループリントで構成をテンプレート化して適用

教育テクノロジー担当者により学習準備の整った状態が定義されたら、教育固有の要件に加えて必須のアプリ、設定、SSO構成をブループリントに保存します。各デバイスは初期設定中に、指定のブループリントに従って自動的に構成され、確実に学習準備が整った状態になります。

生徒・教員・職員など複数のペルソナの管理も、用途ごとに異なるニーズに合わせたブループリントの作成も簡単です。特定のユーザ用のデバイスに、個別のニーズを満たすようにマッピングしたブループリントを毎回確実に適用できます。

最新式の管理でドリフトを自動的に防止

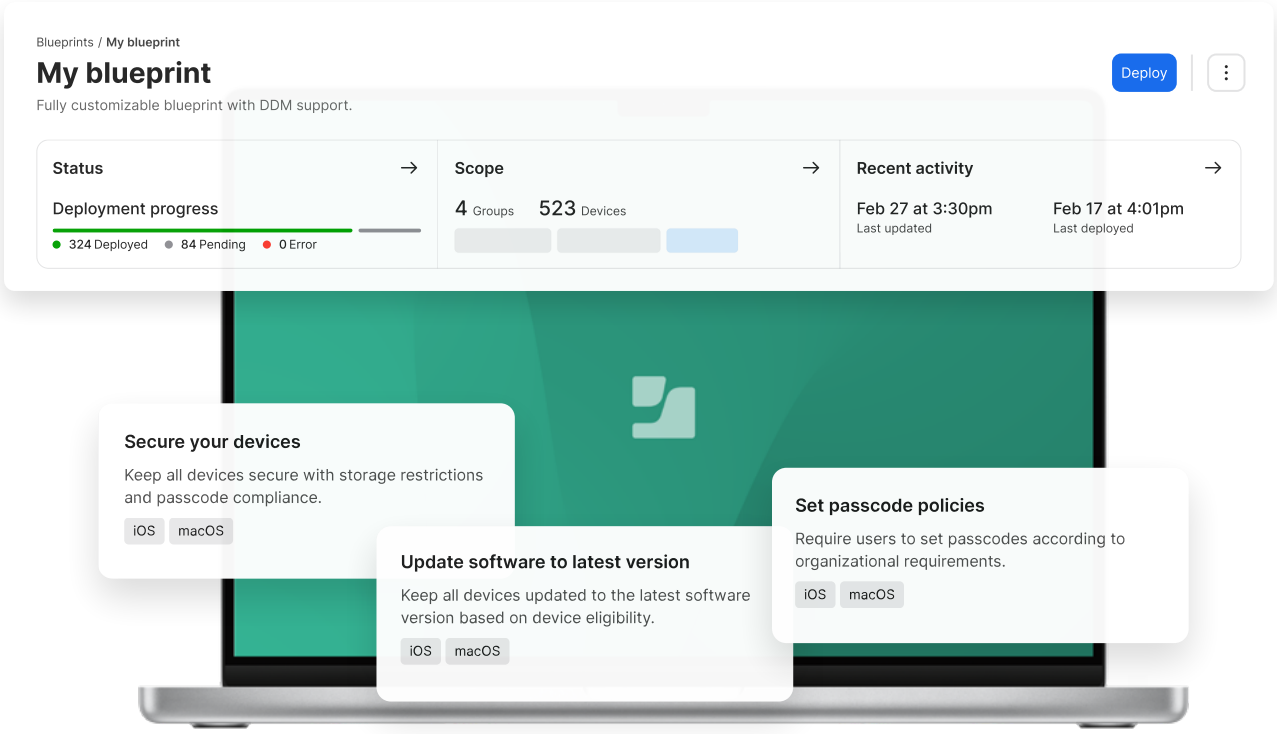
宣言型デバイス管理（DDM）は、Appleが設計したデバイス管理の最新プロトコルです。DDMを使用すると、パフォーマンスとスケーラビリティを考慮した構成をデバイスに確実に適用できます。DDMはブループリントを支えるエンジンです。必要な設定のコピーをデバイス自体に保存し、デバイスの正常性レポートを非同期通信により能動的に行うので、インターネット接続がない環境でもエンドポイントの状態の一貫性を維持できます。

デバイス数が増えるとネットワークトラフィックも増加して、通信に支障が生じてしまいますが、DDMはMDMサーバとデバイスの間のポーリングを最小限に抑えるように開発されているので、接続関連の問題を回避してアップデートを効率的に処理し、学校、自宅、その他どこででも学習を可能にします。

スマートグループで柔軟な管理の組み合わせを実現

Jamfのスコープ機能（大規模環境における自動化の「秘伝のソース」）でデバイスを動的にグループ化し、カスタマイズ、設定、アプリケーション、ブループリントなどを対象ペルソナに応じてデバイスに適用できます。例えば、生徒が進級するときには、デバイスを以前の学年から削除して新しい学年に追加すると、自動的にデバイスが展開・構成され、該当の学年で学習する準備が整った状態になります。

後ほど詳しく取り上げますが、セキュリティ面では、スマートグループをポリシーと組み合わせて、コンプライアンス違反のデバイスを検出したら関連ポリシーを自動的に実行し、バックグラウンドでエンドポイントの修復を行えます。このとき、ユーザが活動を妨げられることも、ヘルプデスクに解決を依頼する必要もありません。



アプリとアップデートの管理

このセクションでは、デバイスでなんらかの機能を実行するために使用されているコード全般を「ソフトウェア」と呼びます。例えば、生徒のクリエイティビティを引き出すアプリ、教員が出席を取るために使うサービス、セキュリティや基盤OSのアップデートが該当します。この区別が必要である理由は、ミクロ視点で言うと、アプリケーション管理ではアプリを最新の状態に保つことだけでなく、初等・中等教育機関でデジタル学習と授業が中断なく行われるようにアプリ利用が正しいデバイスを使い、正しいタイミングで行われているかどうかも重視するからです。

マクロレベルで言えば、アプリライフサイクル管理はソフトウェアエコシステムの重要な要素です。ばらつきは、数量やポリシーのような考慮事項によって増大するものです。その結果、手作業でのソフトウェア管理は、規模が拡大するにつれ著しく難しくなるうえ、デバイス数とばらつきの増大にしたがってパッチ適用されていない脆弱性が格段に増えるため、リスクが著しく高くなります。

簡潔に言えば、ソフトウェア管理が崩壊すると、教育も崩壊します。

初等・中等教育機関における問題の原因

- **必要なソフトウェアツールが学年によって異なる**
- **アクセス許可と構成がユーザの立場によって変化する**
- **アプリの展開先のデバイスを間違える（または展開しない）**
- **ソフトウェアアップデート漏れにより互換性が失われる**
- **アプリの安全性や構成に問題がありリスクが増加する**

上記それぞれの原因は、1デバイスであればほんの数分で解決できるものです。しかし、台数が数百、数千、数万と増えると、IT担当者の対応にかかる作業負荷が数日から数週間にもおよぶうえ、対応中は教育機関では必要なツールにアクセスできず、教育成果を出せなくなります。この規模の問題が起きてもよいタイミングなどそもそもありませんが、特に、ユーザ全員が失敗できないというプレッシャーを感じることになる重大なテスト期間の直前や最中は絶対に防がなければなりません。

大規模環境におけるソフトウェア管理の理想像

- 生徒のデバイスで必要な学習ツールに必要なタイミングでアクセスできる
- 教員がサポートに問い合わせることなく新しいツールを導入できる
- ユーザが操作しなくても、パッチ管理がバックグラウンドで自動的に行われる
- 管理対象アプリのセキュリティとプライバシーがデフォルトで適切に構成されている
- ポリシーベースの管理でデバイスのコンプライアンスが確保されている
- IT担当者が変更を加えたら、アーキテクチャによって変更が配信される
- コンプライアンス体制の監査用に変更が記録され、簡単に取得できる

プロセス：障害を発生前に解決する

障害を防止するプロセスを実装し、教育の阻害要因を潰すことで、IT担当者が受動的ではなく能動的に動けるようになります。こうしてIT担当者は、次々発生する問題に緊急対応したり、もっと悪い場合にはタスクや目標をユーザが完了できない「原因」になったりするのではなく、教育活動に合致した優れたユーザエクスペリエンスの提供に意識とスキルを注げるようになります。

パッチ管理を自動化してセキュリティ体制を維持

嬉しくないことに、教育機関はデータ侵害や設定ミス（アップデートの適用漏れを含む）の観点から価値の高い標的とされており、Verizonの『2025年度データ漏洩/侵害調査報告書』によれば多種多様なエラーによるリスクの30%を占めています。自動パッチ適用では、必要に応じて拡張可能なアーキテクチャを利用し、初等・中等教育機関のスケジュールを考慮しながら（授業に被らないようにアップデートのタイミングを遅らせるなど）デバイスのセキュリティギャップを埋めます。

Jamf Teacherで学習環境を最適化

管理対象アプリをクラスに安全に展開してデジタル指導を強化できる特別なアプリを教員に提供します。このアプリはシンプルかつ使いやすく、Jamfの管理コンソールにアクセスしたりIT知識を習得したりする必要がないので、「必要なツールが見つかった」らすぐに「そのツールを生徒に配布」できます。

App インストーラでアプリ管理の負荷を解消

開発者から安全に調達した多数のアプリケーションをJamfの高度な技術でパッケージ化して、厳選したリストにまとめています。App インストーラを使うと、ベースラインセキュリティ体制を確保するだけでなく、macOSアプリを手動で配布する必要がなくなります。スマートグループと組み合わせれば、学校固有のニーズに合わせてカスタマイズした属性（学年・立場・グループメンバーシップなど）を基準として適切なアプリを適切なデバイスに自動で配信できます。

Self ServiceでIT関連のリクエストを減らし、ユーザの自主性を高める

自分の学校に合わせてカスタマイズされたソフトウェア・設定・共通構成がアプリストアで提供されたら、と想像してください。それを叶えるのがJamfのSelf Serviceです。生徒も教職員も、問い合わせたり待たされたりすることなく、IT担当者承認済みのツールをダウンロードし、インストールして利用できます。ユーザの立場で見ると、これは一定の制約の下で必要なものに必要なタイミングで柔軟にアクセスできるということです。

Jamf Studentで生徒が学習に集中できる環境を確保

インターネットにアクセスできる環境で生徒の学習意欲を保つのは非常に困難です。アプリ関連の問題が発生すると、学習が中断され、簡単に集中が途切れてしまいます。Jamf Studentがあれば、この問題を解決できます。生徒のデバイスで何に（いつ）アクセスできるのかをリアルタイムで制御し、学習の主役として授業時間を守ります。

アイデンティティ管理とログイン摩擦

アイデンティティ管理は認証の同義語です。これら2つの言葉を説明する際に「**ログイン摩擦**」という用語がよく使われますが、この言葉は後者を指す傾向が強く、前者に関してはコンテキストが足りていません。本ホワイトペーパーでは、その目的から、パスワードのリセットや、手動の面倒な作業に伴うログイン疲れ（パスワード入力を求められる回数が多すぎる）などに関する認証の問題を指して「**ログイン摩擦**」、認証情報を提供して初等・中等教育機関のリソースへのアクセスを保護するというセキュリティ寄りの概念を指して「アイデンティティ管理」を使います。

ログイン摩擦の最大の要因は、大規模環境におけるパスワードの管理と言っても過言ではありません。1人1台体制の物理的な負荷に次いで、IT担当者の大きな負荷となっているのがパスワードリセットとアクセスの問題です。これらは、サポート依頼の最大の要因であり、ひいては授業を妨げる原因でもあります。

台数に上限がある物理的なデバイスに対し、アイデンティティの管理には限界がありません。学校に関わるすべての人の個人アカウントはもちろん、システム連携に必要な「サービスアカウント（非人間アイデンティティ）」、そしてそれぞれに付与された無数の「権限」や「特権」が絡み合うため、管理の規模は際限なく膨れ上がっていくのです。これは、ときにIT担当者の悩みになるだけではありません。手作業で管理する場合、問い合わせが絶え間なく行われていると、サポートを求めるユーザの活動を滞らせることになります。一意のログイン情報を必要とするデバイス、ユーザ、アプリ/サービスにより、収拾のつかない順番待ちが発生するからです。

1つのサポート問題が1,000人から10,000人のユーザに影響するので、ログイン摩擦による影響は個々のユーザの生産性を損なうだけにとどまらず、学習、教育、日常業務全体の妨げになるまでの問題になります。最初はちょっとした滞りでも、放っておくと、すべてを停止させるまでに深刻化します。

第4章

フレームワーク：認証と認可の構築

これまでのシナリオで、大規模環境におけるアイデンティティ管理の重要性を示しました。教員の場合、例えばクラウドに保存された授業計画などの教育リソースにアクセスする際に、パスワードを3つも使用する必要がなくなります。生徒の場合、ある授業から別の授業へ移るときにアプリを認証不要でシームレスに切り替えられます。以下で、最新のID統合の導入により、手動の繰り返しタスクを解消して大規模環境で深刻化する摩擦を減らすと同時に、デジタルユーザの安全性、運用セキュリティ、教育継続性の確保を効率化する方法について説明します。

シングルサインオン（SSO）でアプリへのアクセスをシームレス化

SSOを使うと、1回認証するだけで、保護されたアプリ、プラットフォーム、サービスにアクセスできるようになります。ユーザはデバイスまたはポータルで初めの一回だけ認証すれば教育関連のタスクに集中できるので、認証情報を忘れて困る事態が減るほか、弱いパスワードの使用やパスワードの使いまわしといったセキュリティ上の懸念も抑えられます。

IT担当者のパスワードリセット作業負荷を軽減

パスワードは「シンプルな方が効果的」が当てはまり、使う認証情報の数が少なければ、リセットが必要なパスワードも少なくなります。というのも、何十ものアカウントを覚える認知負荷がユーザにかからないからです。これは、IT担当者に2つの恩恵があります。1つはアカウント関連の問題の問い合わせを減らせること、もう1つはその結果生まれた時間で高度なスキルが必要な作業（ユーザエクスペリエンスの向上や、教育目標に沿った価値の創出）に集中できることです。

Jamf + IDプロバイダ（IdP）を連携させてアイデンティティ管理を拡張

既に使っているIdPをJamfと統合して、手動でのアカウント保守から一元的なアイデンティティ管理に移行し、管理・セキュリティワークフローを拡張します。一貫したアクセスポリシーを構成して、特定のデバイスではなくユーザの資格情報に関連付けます。このようにすると、アプリごと、デバイスごと、学年ごとに手動で構成し直さなくても、初等・中等教育機関のユーザに合わせてアクセス許可が適用されます。

アカウントプロビジョニングとアクセス許可を毎回正しく設定

新入生と新規教職員のアカウントプロビジョニングを自動化すると、利用初日からユーザの手元に適切なツールが届きます。ヘルプデスクに問い合わせる必要も、IT担当者によるオンボーディングを待つ必要もなく、必要なアプリ、サイト、サービスに認証するだけで、アクセスが既に構成された状態になります。進級時や異動時の対応は、Jamf、IdP、スマートグループを組み合わせて使うことで、学年や立場の要件に応じて自動的にアクセス許可をアップデートできます。

余分な手間のかからないセキュリティ

ユーザ、デバイス、データを守ると同時に、プライバシーを確保し、コンプライアンス要件を厳密に遵守するのは、それだけでも非常に困難です。ハイブリッド活用をすればなおさらで、1人1台の方針、コンピュータラボ、保管箱に収納された共有デバイスを使い、一部のデバイスはオンプレミスで境界制御により保護されていても、残りのデバイスが自宅から学校、課外活動などで自由に移動する状況ではさらに困難になります。ここで重要なのは、年次更新サイクルを除くと、これらのデバイスが大半の時間、学校外にあることです。

この「対象が移動する」シナリオに加えて、世界各地の初等・中等教育機関は次のような高度な攻撃の脅威に絶えずさらされています。

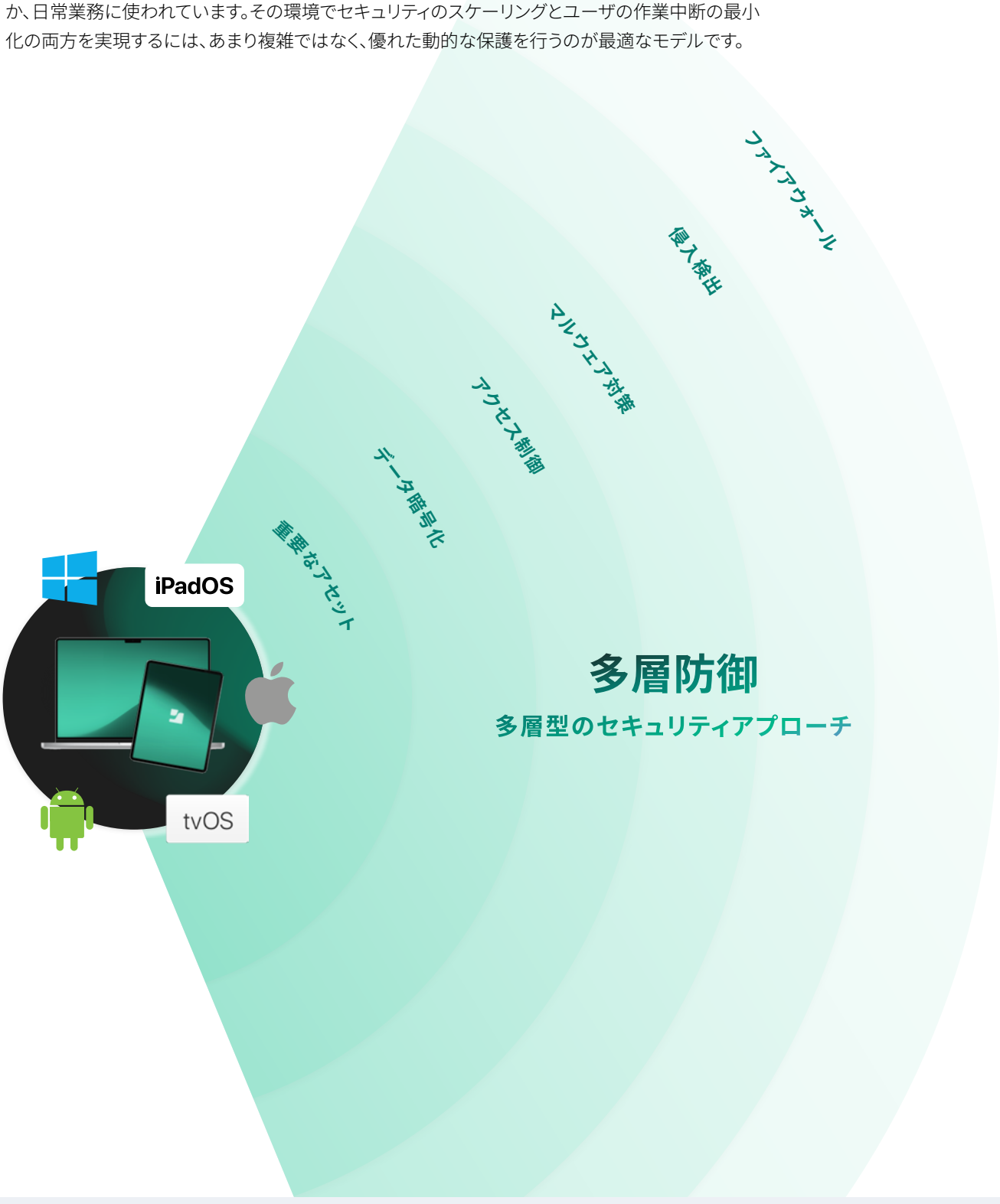
ここにデバイス数の増加による規模の増幅要因が加わることで複雑さが大幅に増し、本ホワイトペーパーで説明してきたスケーリングの課題で対応する範囲をセキュリティ層にも広げる必要性が生じます。

IT担当者には各デバイス、アプリ、接続を直接監視しつつ、脆弱性・攻撃者・ユーザの行動から生じるリスクを減らす責任があります。その結果、大規模環境では毎日何千件ものデータポイントを確認しなければならない事態が起こり得ます。『2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience』によると、2023年7月から2024年12月までの18ヶ月の間に確認されたサイバーセキュリティインシデントは9,300件に上ります。これを別の数字で表すと、548日間にわたり毎日約17件のサイバー攻撃が発生していた計算になります。

言い換えれば、サイバー脅威をもたらす攻撃者は、夜間でも休日でも、学校の都合に関係なくいつでも狙ってきます。だからこそ、初等・中等教育機関のサイバーセキュリティ対策は、デバイスが教室にあるときはもちろん、自宅の食卓でも、あるいは長期休暇中であっても、常に「自動的」かつ「文脈（状況）に応じ」、そして「包括的」に機能するものでなければならないのです。脅威対策が絶対にオフにならず、デバイスの場所と時間帯に合わせてポリシーが調整される場合、それは単なる優れたセキュリティではありません。それこそが唯一の、効率と一貫性を持って初等・中等教育機関のインフラストラクチャ全体で動的かつスケーラブルに機能するモデルです。

モデル：多層防御（DiD）

DiDとは、複数のセキュリティ対策とプロセスを一元化して、多重の防御によりユーザ、デバイス、機関などを高度な攻撃から保護するという概念です。ある攻撃によって1つの階層が突破されても、その前後の階層がセーフティネットとなってリスクを軽減し、事態の悪化を防ぎます。最近の環境では様々な種類のデバイス（コンピュータ、タブレット、メディアコネクタ）が複数のプラットフォーム（macOS、iPadOS、tvOS、Android、Windows）で動作して、教育機関のユーザの学習や授業のほか、日常業務に使われています。その環境でセキュリティのスケーリングとユーザの作業中断の最小化の両方を実現するには、あまり複雑ではなく、優れた動的な保護を行うのが最適なモデルです。



複数プラットフォームにわたってネットワークベースの脅威を防止

現在はフィッシング、通信傍受、クリプトジャッキングといった攻撃が、初等・中等教育機関を標的として記録的な増加を見せています。常時ネットワークに接続しているデスクトップとモバイルデバイスの両方で、Jamfのセキュリティが警備員の役割を果たして、教育目的の通信は許可し、学校のデータをリスクにさらす攻撃経路の通信は防止します。デバイス正常性データの可視化と組み合わせると、標的となっているデバイスとその理由に関する詳細情報を入手して、リスク要因を適宜緩和できます。

Jamf Safe Internet（JSI）で有害コンテンツから生徒を保護

初等・中等教育機関の生徒は年齢・成熟度共に多様です。全生徒に「画一的」アプローチを取るのは有効ではなく、上級生のニーズを満たすと下級生にしわ寄せが及ぶため、常に手動の調整が必要になります。JSIは不適切なコンテンツ（や集中を妨げるコンテンツ）をブロックする機能はもちろん、生徒のオンライン安全性を侵害することなく、学校外（週末など）でのインターネットリソースへのアクセス制御を自動化する年齢に応じたフィルタリングやポリシーなど、詳細な管理機能も備えています。

AIによって進化する脅威への対策

脅威アクターはAIを活用して攻撃を洗練させており、特定や防御が難しくなっています。そこで、Jamfはネットワーク内での対策を補強するため、機械学習（ML）を利用したデバイス上保護機能を実装します。MLによってゼロデイフィッシングなどのAIリスクを評価し、ユーザが誤って悪意のあるリンクをクリックしても被害に遭わないようにします。さらに、この対策は「デバイス上」で行われるため、サードパーティVPNやプロキシ、DNS設定を使用している場合でも有効に機能し、保護回避や保護の抜け穴を排除します。

コンテキストに応じてポリシーを自動で適用

従来は、校内でデバイスを使う場合はユーザが必要とする全リソースへのアクセス権と保護が提供されていましたが、校外で使う際はほとんど提供されていませんでした。今では、初等・中等教育機関のユーザが校内と同じように校外でもテクノロジーを活用する動きが広まっています。しかし、多くの場合、状況の変化に合わせた設定の変更が必要です。そこで、時間帯や学校の年間予定表（週末や祝日）といったコンテキスト情報に従ってポリシーを自動的に切り替える、スケジュールベースのポリシー適合が役立ちます。IT担当者がルールを一度定義したら、Jamfによってコンテキストに合わせた切り替えがすべて処理されます。ユーザの作業が中断されることはなく、手動構成も不要です。

まとめ

本ホワイトペーパー全体を通じて、初等・中等教育機関における管理対象デバイス台数とIT担当者の平均比率である1,000：1を基に話を進めてきました。企業のこの比率は1：70 前後ですが、初等・中等教育機関では予算の制約から、IT担当者を増やして企業の比率に近づけることはほぼ不可能です。**むしろ、地域によっては、この比率が1人あたり10,000台近くまで近づいて（または既に到達して）います。**

初等・中等教育機関の生徒および教職員のサポートだけでも既に非常に重い負荷がかかっています。大規模環境では、以下のような多くの変数があるため、負荷がより厳しいものになります。

- 多様かつ多量のデバイスの初期設定
- 複数の学校/校舎/機関にわたる導入
- クロスプラットフォームサポートとコンプライアンスの徹底
- 校内全体における年齢の考慮
- 複数の学校にわたる学年の要件
- アイデンティティ管理と認証摩擦、オンプレミス/クラウドベース
- 学校内と学校外のセキュリティ体制の同等性

課題：手動プロセスの破綻

1,000台のデバイスに対応している場合、年次更新で全デバイスについて各タスクをすべて終えるには、1日、数日、あるいは数週間でもまったく足りません。

解決策：人手を増やすのではなく、アーキテクチャを改善する

繰り返しになりますが、キーワードはまたも「繰り返し」です（駄洒落を狙っているのではありません）。再利用性が、大規模環境における手作業を撲滅するのです。

「変数に影響されることなく、複数のデバイスに同じ手順を繰り返せれば、運用負荷を最小限に抑えることができます」

デバイスライフサイクルの構成要素には、以下のものがあります。

- **調達**
  計画と登録
- **メンテナンス**
  セキュリティと脆弱性管理
- **導入**
  構成とアプリ管理
- **廃棄**
  インベントリと安全な廃棄
- **監視**
  アイデンティティとアクセスレポート

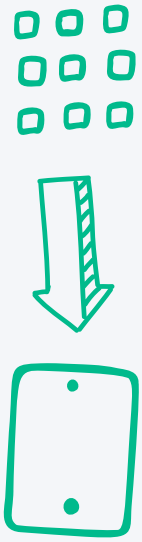
自動化の主題は標準化・柔軟性・効率性です。各章に通底する考えである「タスクとプロセスの自動化」は、「IT担当者を疲弊させずにスケーリングする再利用性の実現」の鍵として合致します。

ビジョン：後手から先手へ

自動化によって、繰り返しの手動タスクが予測可能な操作に変わり、包括的かつ全体的なワークフローが実現します。その結果、新しいデバイスを追加したり、既存のデバイスを再プロビジョニングしたりする際に、ワークフローを何度も再利用して効果的かつ効率的に一貫性のある形でスケーリングできるようになります。

なにより、その際に学習環境が停止することもなければ、その都度IT担当者がタスクの実行に介入する必要もありません。実際、あらゆるスキルレベルのユーザを考慮してアーキテクチャが設計されているため、授業中にアップデートを求めるメッセージが出ても、教員は対応のタイミングを延期してすぐに学習活動に戻ることができます。また、生徒の取り組みの最適化についても、手元にないアプリが必要なとき、生徒がSelf Serviceにアクセスし、事前承認済みソフトウェアをインストールして学習を継続できます。

前述のよくあるシナリオではいずれも、ヘルプデスクにサポートを依頼したり、IT担当者の手を煩わせたりする必要はありません。最も重要なのは、いずれのシナリオでも、管理者権限を持つ誰かが対処するまで、ユーザが作業を止めたり、後回しにしたりしなくてよいということです。



IT担当者と技術担当者に向けたまとめ

デバイス数が増えると、手動プロセスがすぐに持続不能になり、IT担当者が速やかなサポートを提供する能力が低下するだけでなく、教育能力も大幅に損なわれます。

自動化でデバイス数のボトルネックを打破

手動の初期設定作業を自動ワークフローに置き換えて、数時間かかっていた所要時間を数分で完了します。

デバイスを「学習準備が整った状態」に一括で標準化

テンプレート化した構成を使用して、生徒用/教員用デバイスすべてを利用初日から一貫性のある形で設定します。

ゼロタッチ導入でIT担当者の手間を軽減

デバイスを利用開始時に自動で登録および構成されるようにして、新学期初日に向けた準備作業の時間を短縮します。

後手のサポートを先手の運用に移行

火消しではなく学習成果の向上に注力するため、自動化を通じてデバイス、アイデンティティ、セキュリティの各管理を統合します。

リソースをタイミングよく提供し、摩擦を解消

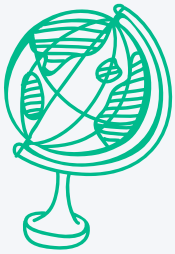
立場や学年に応じてアプリとリソースを動的に割り当て、ユーザが待つことなく即座にアクセスできるようにします。

ログイン摩擦とパスワード疲れを緩和

SSOと自動アイデンティティ管理ワークフローを実装して、パスワードのリセット回数を減らすとともに安全なアクセスを確保します。

学習を妨害せずにセキュリティを拡大

多層防御を展開して、校内外で動的かつシームレスにポリシーを適合させます。



初等・中等教育機関の運用負荷を解消するJamf製品をぜひご体験ください。授業や学習の手を止めることなく、日常的なトラブルを現場でスマートに解決。IT管理のあり方を「日々のトラブルシューティング」から「教育成果への寄与」へと転換し、教育ICTの真の価値を引き出します。

jamf

www.jamf.com/ja/