●JAMF NATION LIVE

学校でのMac活用を支える環境づくりと負担を減らす選択

Mac × Jamf



金崎 崇

教育本部

ACCOUNT EXECUTIVE

世界で選ばれ続ける Jamf、教育機関で2,500万台以上



文科省ガイドライン

図２　いわゆるゼロトラストセキュリティに関する要素技術

①アクセスの真正性に関する要素技術		
①-1	多要素認証	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
①-2	リスクベース認証	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術
①-3	シングルサインオン（SSO）	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術　※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
②通信の安全性に関する要素技術		
②-1	通信経路の暗号化	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
②-2	Webフィルタリング	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
③端末・サーバの安全性に関する要素技術		
③-1	モバイル端末管理（MDM） (Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
③-2	アンチウイルス	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知）　※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
③-3	データ暗号化	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
③-4	EDR (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
③-5	IDS/IPS (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
③-6	WAF (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

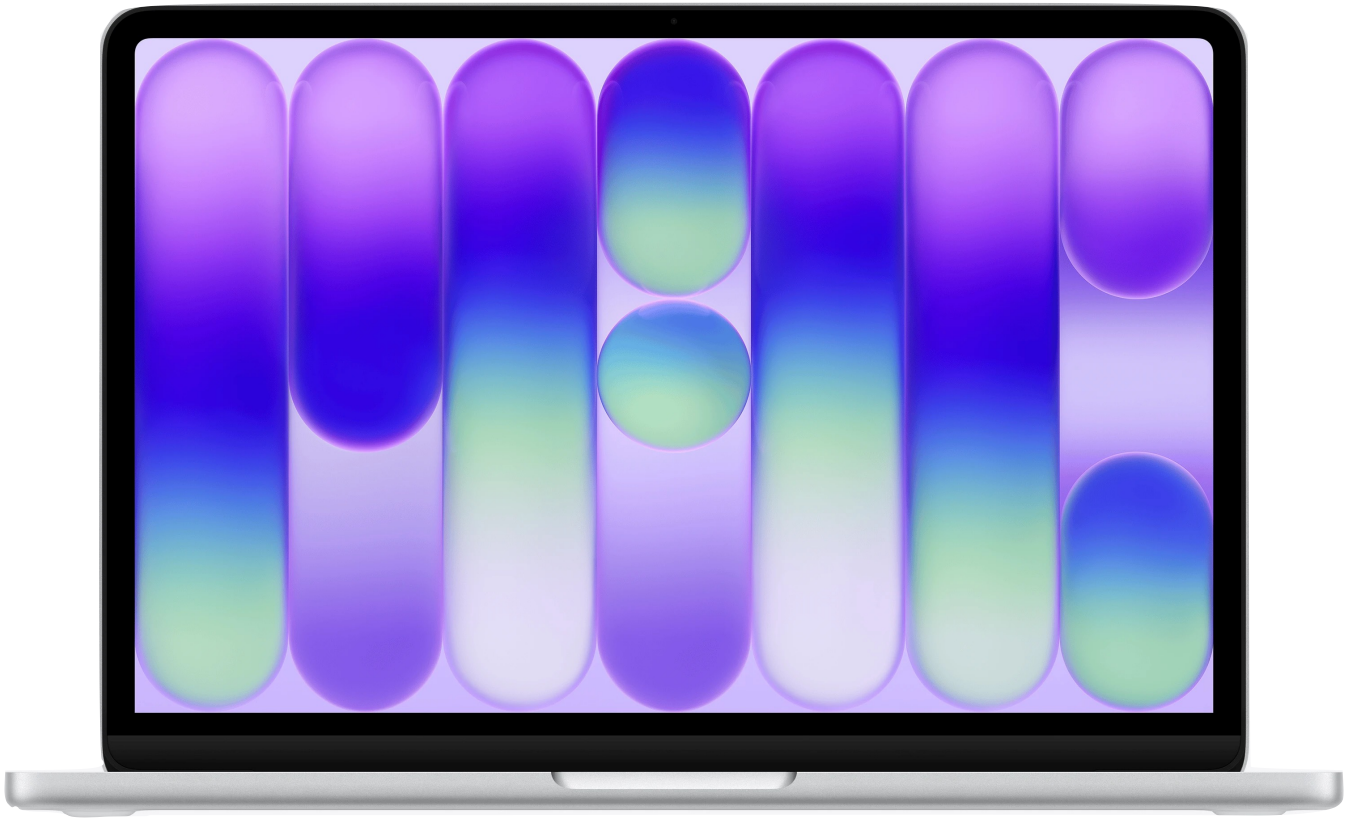
文科省ガイドライン

図２ **いわゆるゼロトラストセキュリティに関する要素技術**

①アクセスの真正性に関する要素技術		
①-1	多要素認証	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
①-2	リスクベース認証	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術
①-3	シングルサインオン（SSO）	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
②通信の安全性に関する要素技術		
②-1	通信経路の暗号化	通信経路を暗号化することで、第三者による通信内容の盗見・改ざんを防止する技術
②-2	Webフィルタリング	マルウェアへの感染につながるセキュリティリスクの高いWebページへのアクセスを防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
③端末・サーバの安全性に関する要素技術		
③-1	モバイル端末管理（MDM） (Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
③-2	アンチウイルス	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
③-3	データ暗号化	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
③-4	EDR (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
③-5	IDS/IPS (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
③-6	WAF (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

Jamfで全て対応可能

jamf

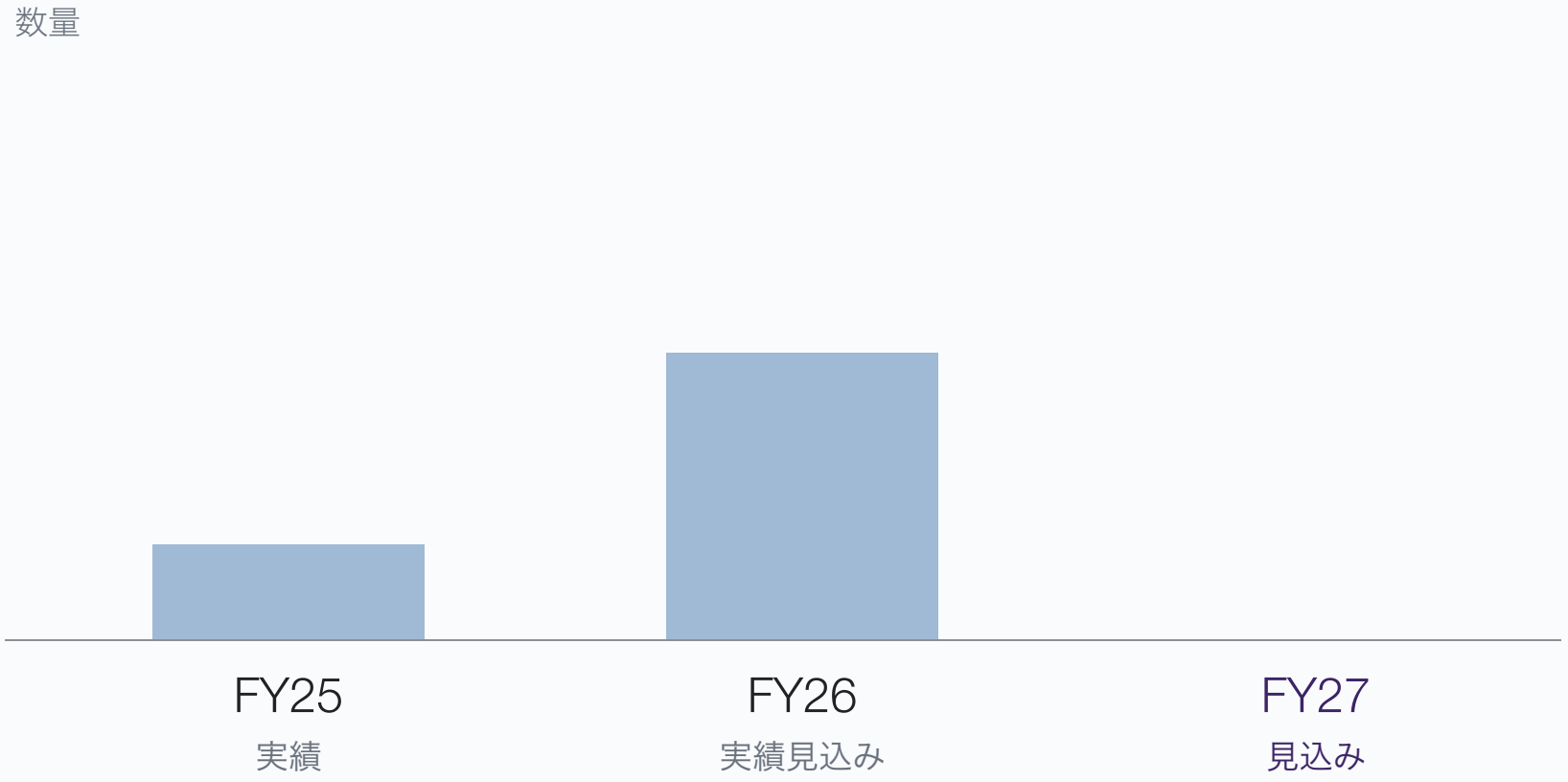


MacBook Neo

JAMF NATION LIVE

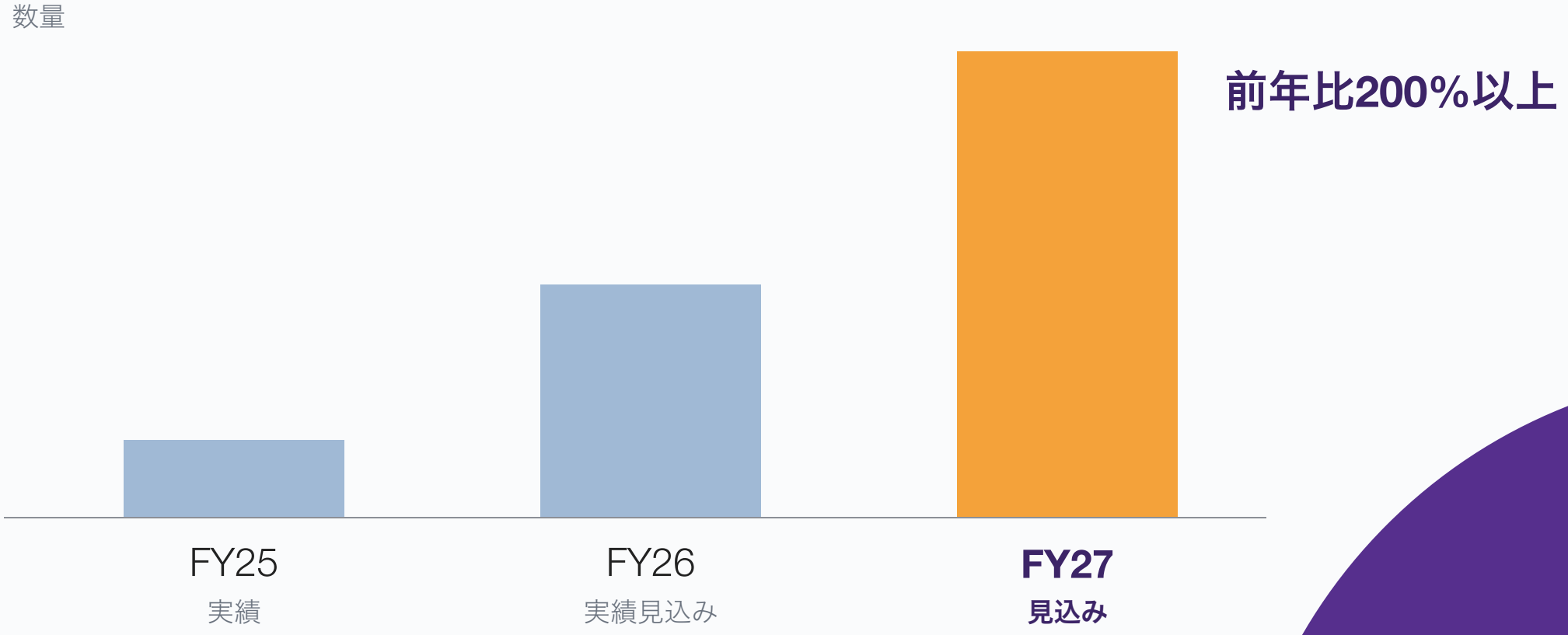
Macの利用は年々拡大、FY27は大幅増を見込む

全国の自治体・教育委員会で導入が進み、FY27には大規模な導入を見込んでいます



Macの利用は年々拡大、FY27は大幅増を見込む

全国の自治体・教育委員会で導入が進み、FY27には大規模な導入を見込んでいます



なぜ、MacはJamfで管理すべきなのか？

Agenda

① Macの導入・キッティングの自動化
〜セットアップマネジャー〜

② Macの管理・運用のポイント
〜アプリ、プリンタドライバー、ブループリント〜

③ OS27 Jamf機能のアップデート
〜PSSO、Jamf Parent for Mac、etc〜

Macの導入・キッティングの自動化

～セットアップマネジャー～

iPadとMacのゼロタッチキッティングの違い

共通の仕組み：電源ON・ネット接続で、ADEによる自動登録と設定配信

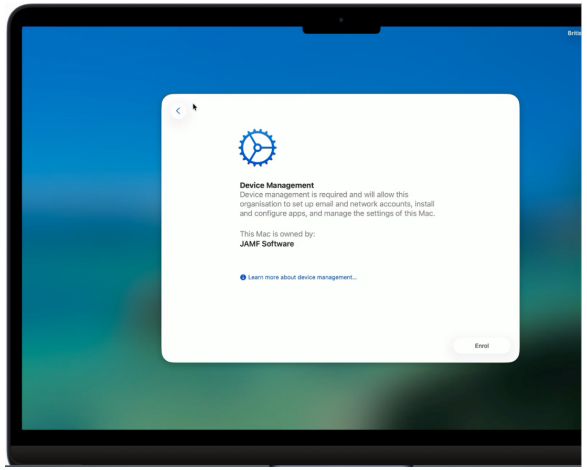
iPad：シンプルに展開

アプリと構成プロファイルの配信が中心。
初期設定の流れを揃えやすく、利用開始が簡単。

Mac：設定の幅が広い

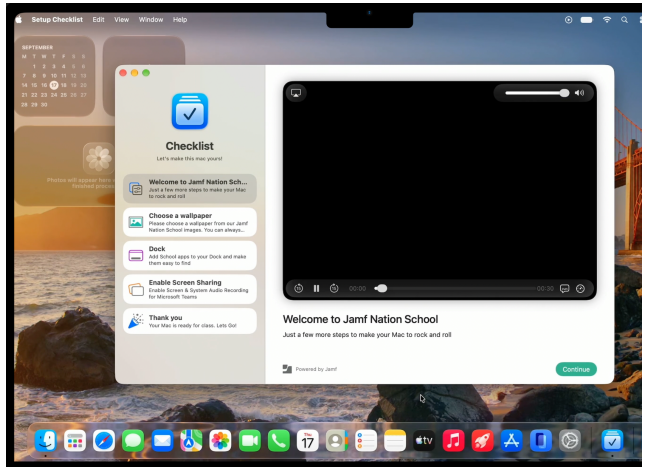
多様なアプリやアカウント設定に加え、
利用者による許可・確認が必要な項目も。

Setup Manager



自動設定の進行状況を可視化

Setup Checklist



利用者が行う設定を
チェックリストで案内

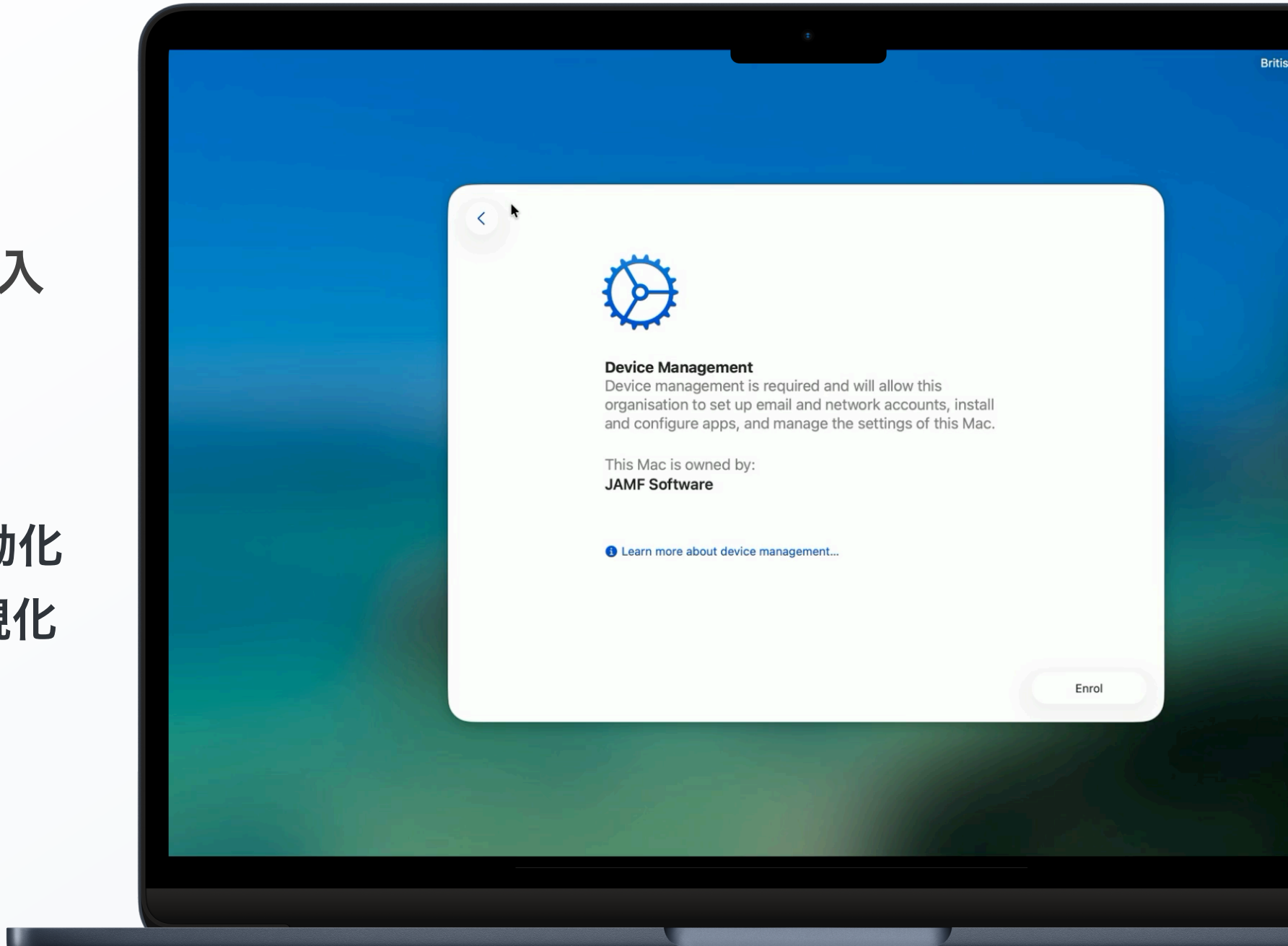
Macも、iPadと同じように「利用者へ直接渡せる」展開へ

●JAMF NATION LIVE

Setup Manager

Macをゼロタッチで導入

- ADEでMac設定を自動化
- 処理の進行状況を可視化



Setup Checklist

導入後の初期設定を
サポート

- 利用前にチェックリストを提供
- 変更が必要な画面を案内



Macの管理・運用のポイント

～アプリ、プリンタドライバー、ブループリント～

Jamf Proならやりたいことを実現

Jamf独自フレームワーク

Jamf Agent

MDMフレームワーク



Macへのアプリ導入方法

Macでは大きく2種類のアプリ導入方法があります。

Mac App Storeのアプリ

AppleのApp Storeから入手

App Storeの仕組みで
インストール・アップデート

例：Pages、Keynote など

App Store外のアプリ

開発元のWebサイトから入手

App Storeでは入手できないアプリ
インストーラなどで導入・更新

例：Google Chrome など

アプリの配布と管理

App Store外のアプリも含めて、Jamfであれば同様に管理制御が可能

「自動パッケージ化」

Google Chrome や Zoomなど
300以上のアプリを Jamf がパッケージ化。
お客様にてインストーラ作成は不要

「アプリのバージョン管理」

配布済みのアプリも継続的にアプリバージョンを追従。常に最新・セキュアな状況を維持。



ポリシー機能

Macに行う管理作業を、対象と実行条件を決めて自動化する機能です。

何ができる？

アプリ配布や日々の管理を効率化

アプリ・ファイルの配布
プリンタの追加、スクリプトの実行
端末情報の更新 など

例：授業で使うアプリをまとめて配布

どう実行する？

対象・タイミング・頻度を指定

対象のMacに条件に応じて自動実行
Self Serviceから
利用者が必要なときに実行することも可能

例：教職員のMacに一度だけ実行

必要な作業を、必要なMacへ、適切なタイミングで。

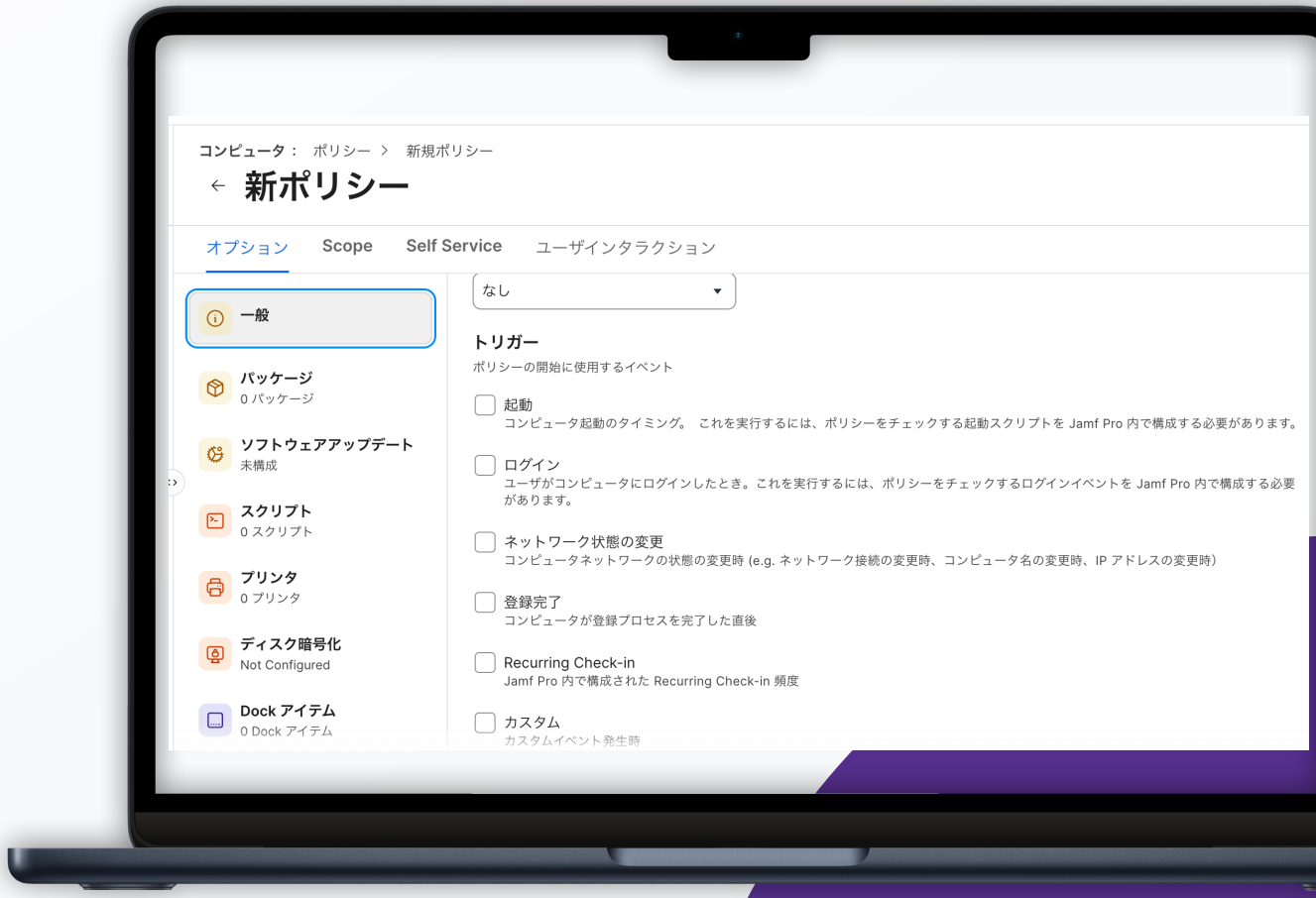
ポリシー機能

「GUIで完結」

頻度やトリガー（ログイン時・ログアウト時 等）
を、チェックボックスだけで設定できる

「柔軟な制御」

細かい条件を管理画面から直接コントロール



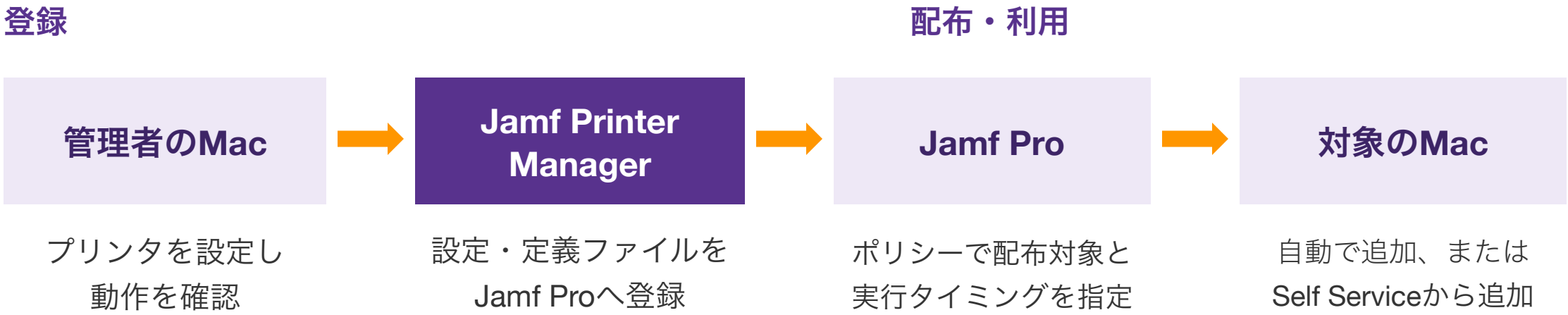
トリガーと実行頻度の組み合わせ

ログイン時・起動時・登録完了時など実行のきっかけを管理画面で指定

ログイン時 × 毎回	**ログインのたびに、必要な処理を実行** トリガー：ログイン　実行頻度：毎回
登録完了時 × 1回	**初期設定やアプリ導入を、デバイスごとに1回実行** トリガー：登録完了　実行頻度：デバイスごとに1回
チェックイン × 1日1回	**定期チェックイン時に、1日1回の処理を実行** トリガー：定期チェックイン　実行頻度：1日1回

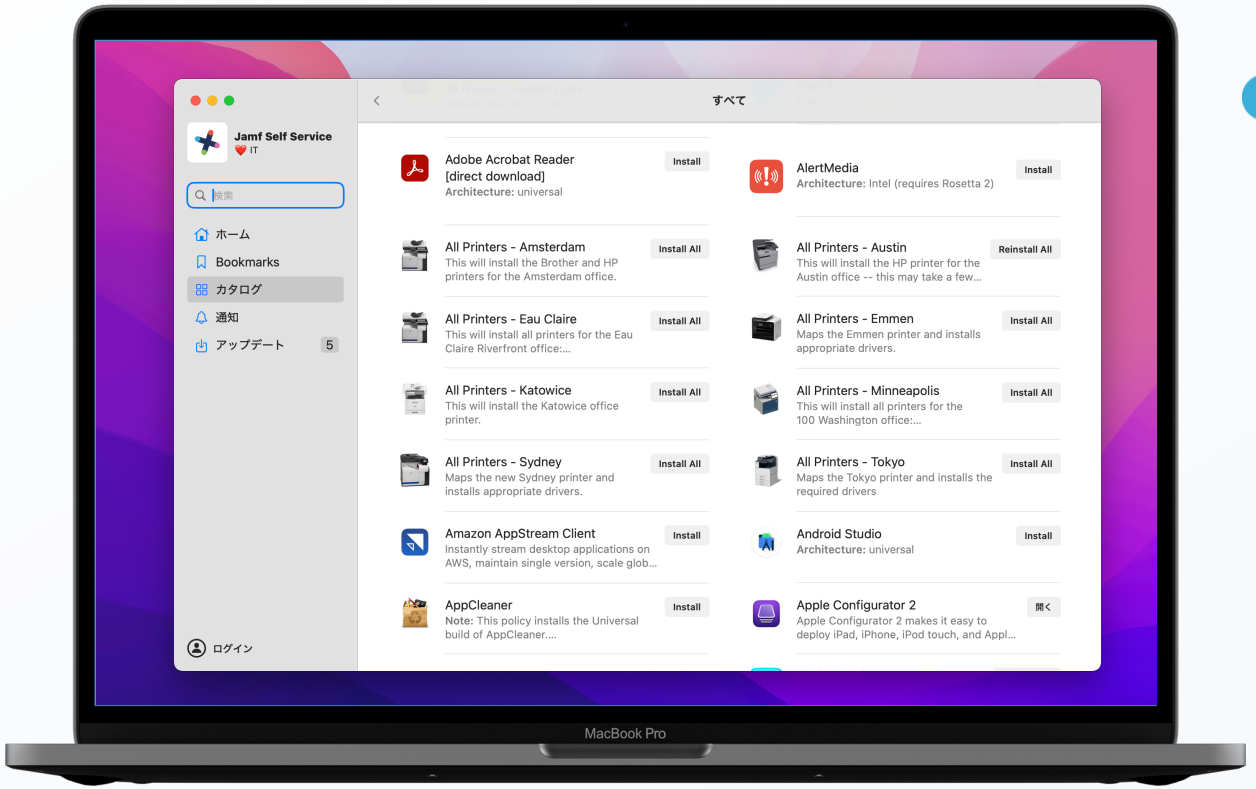
Jamf Printer Manager

設定済みのプリンタ情報を取り込み、Jamf Proから複数のMacへ展開



プリンタ設定の手入力を減らし、Macへの展開を効率化

ユーザが選択形式で簡単にインストールできる環境を提供



Self Service+

- App
- PDFファイル
- プリンタドライバー
- スクリプト etc.

Macログイン (IdP連携)

Microsoft Entra ID

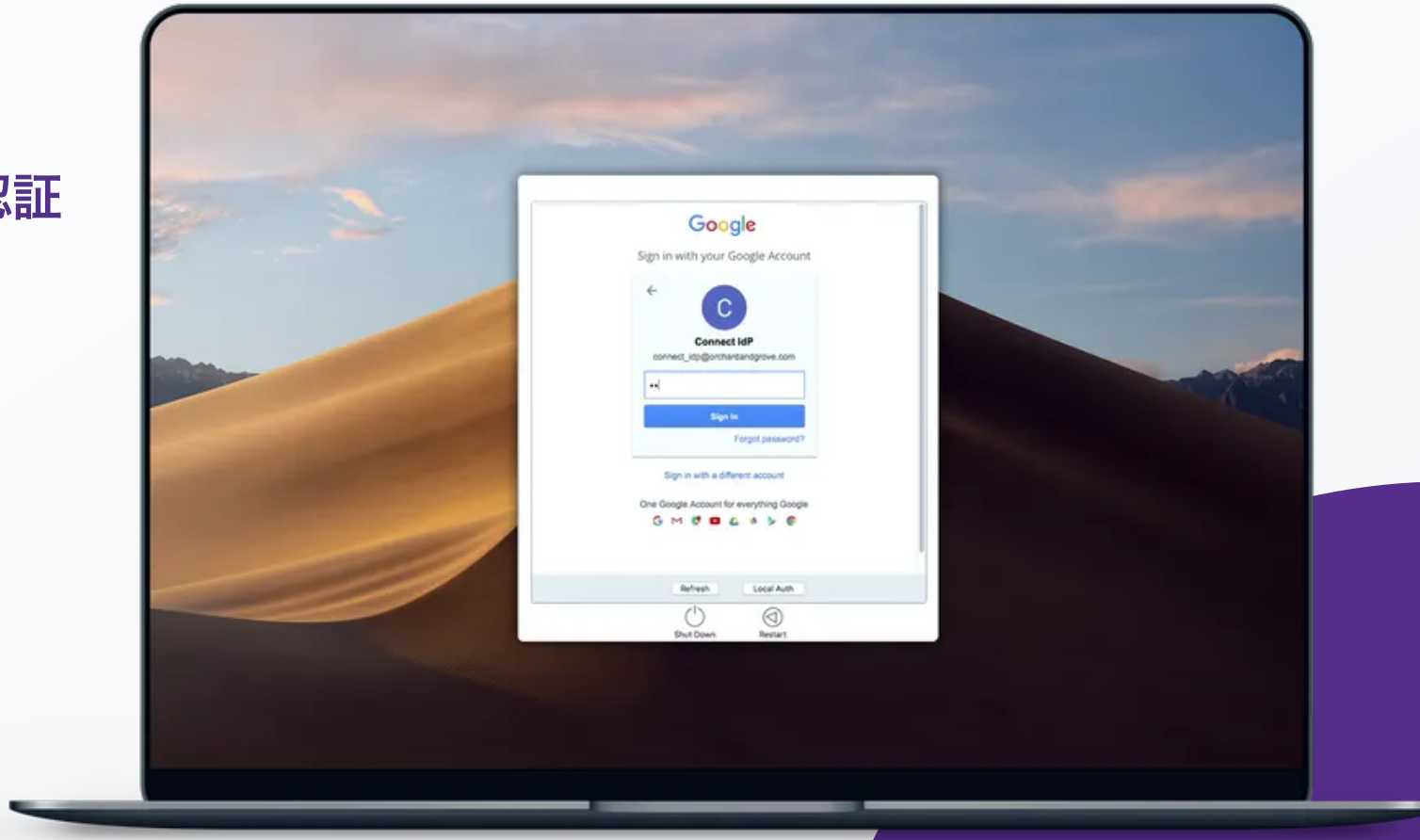
Google

「ログイン画面」

Macのローカルログイン画面を、IdPの認証画面に差し替え

「アカウント自動作成」

認証時にローカルアカウントを自動作成



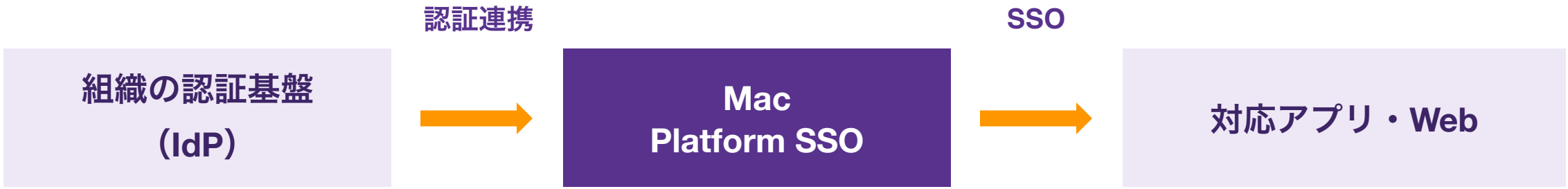
OS27 Jamf機能のアップデート

～PSSO 、Jamf Teacher、Parent～

Platform SSO（PSSO）

Appleが提供する、Macと組織のIDをつなぐ認証連携機能

macOS 13以降に搭載。Macのローカルアカウントと組織の認証基盤を連携します。



組織のアカウントを管理し
利用者を認証

AppleのOS機能と
IdP対応のSSO拡張機能が連携

認証結果を利用し
サインインの手間を軽減

Macの利用と、業務アプリへのサインインをスムーズに

PSSO × Jamf

「新規ユーザ作成」

学校のアカウント(IdP)でログイン
Macアカウントを自動作成

「Macアカウントを連携」

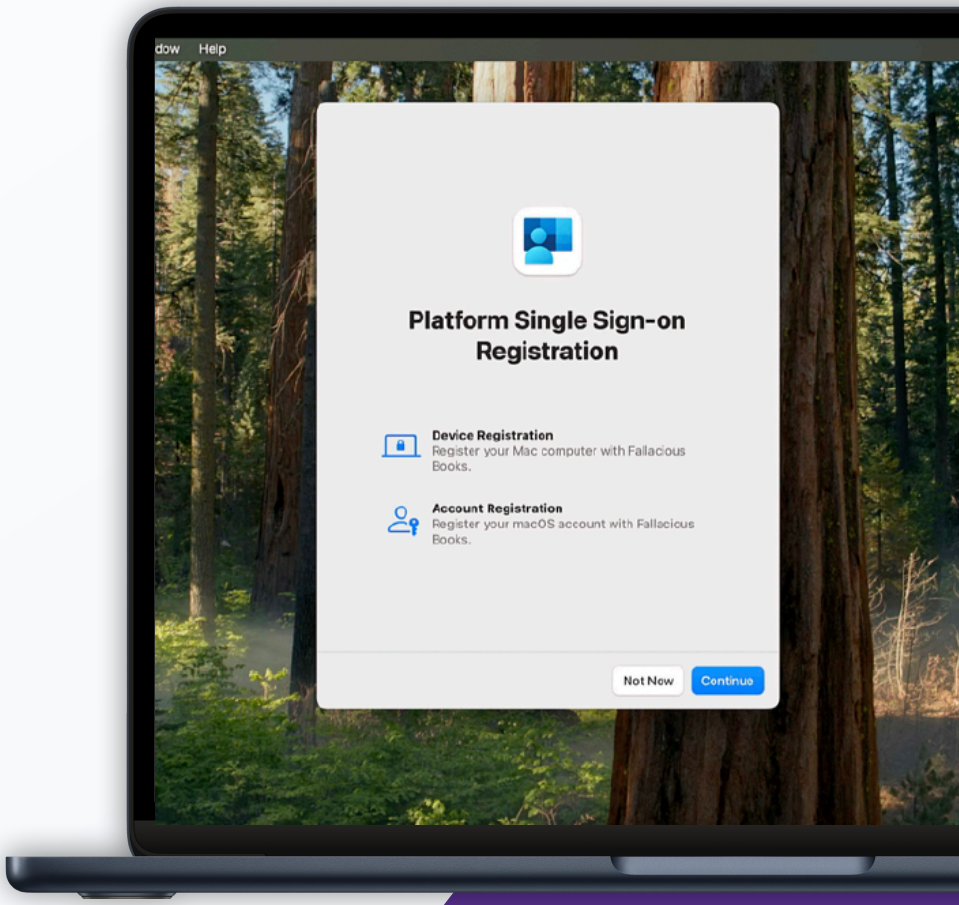
使用中のMacアカウントを
利用中のIDと連携



パソコン教室での利用

PSSOの認証済みゲストモード

ログアウト時に
ユーザデータを自動削除



Jamf Proが担うこと

- 初期設定時のPSSO登録を必須化
- 認証済みゲストモードの設定を配布
- 自動デバイス登録で一括展開

Jamf Parent for Mac

保護者によるMacの利用制限

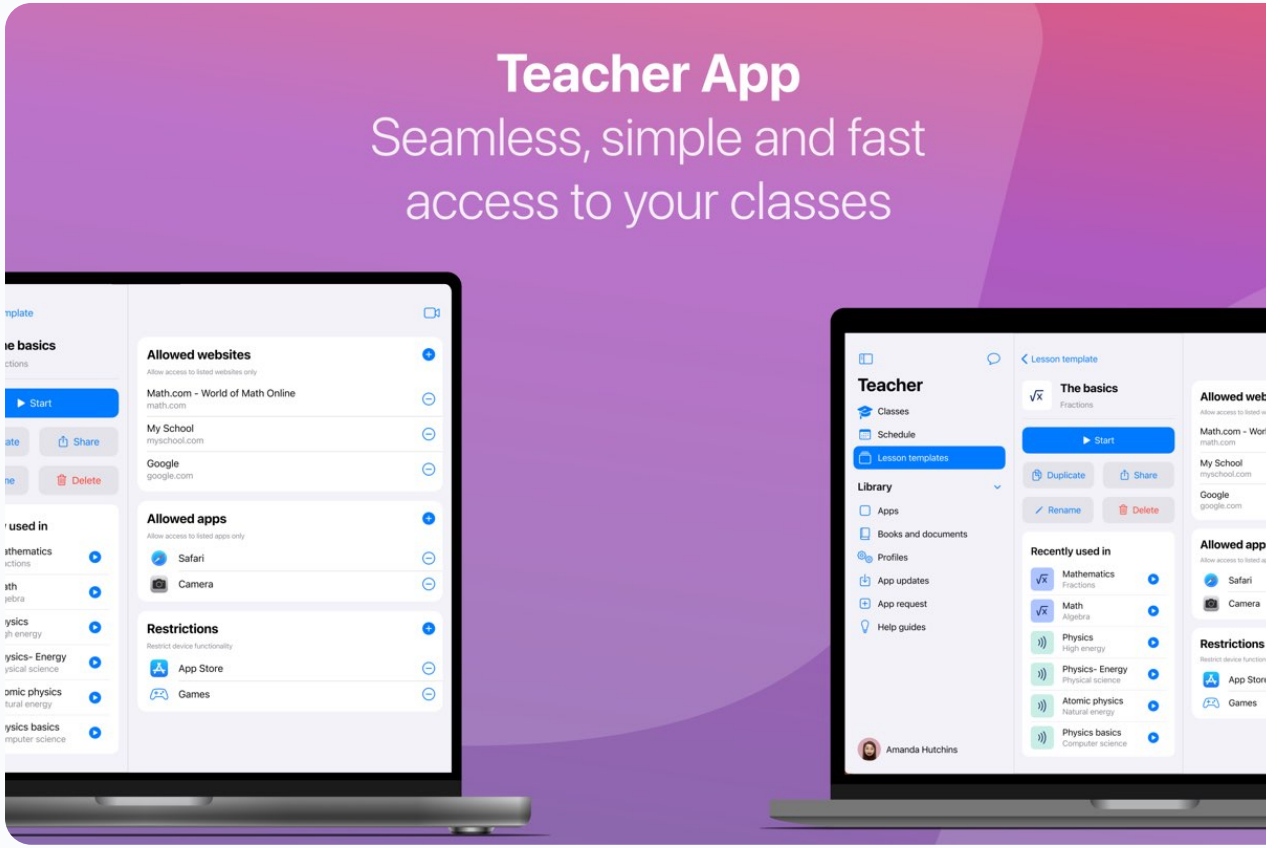
- アプリ利用の制御
- Webサイトの許可・ブロック
- 画面ロック



Jamf Teacher for Mac

先生のMacから授業をサポート

- Webサイトの利用制限
- 生徒とのメッセージ送受信
- 「挙手」による質問の通知



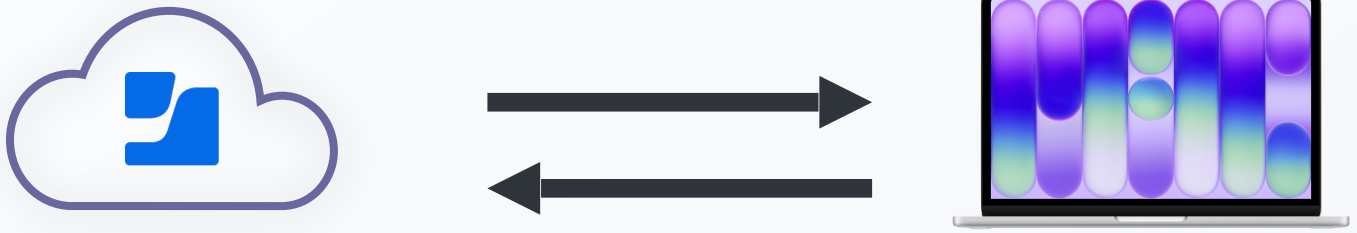
※ Jamf School連携で利用。Mac版はJamf Proでの展開非対応

JAMF NATION LIVE

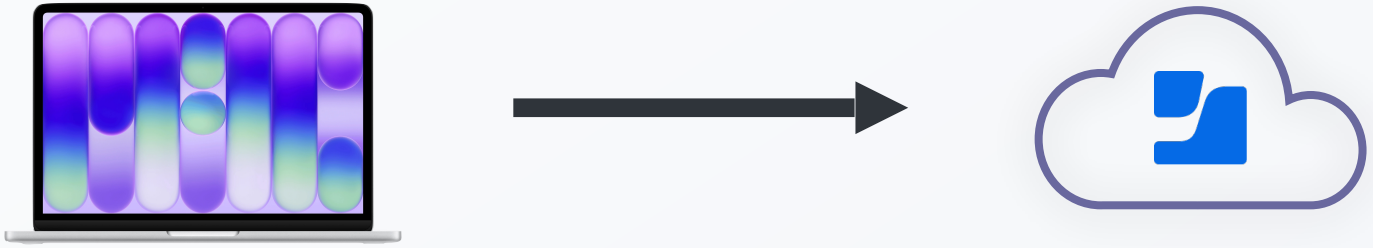
宣言型デバイス管理（DDM）

“あるべき状態” の宣言

従来のデバイス管理



宣言型デバイス管理



Jamf Proのブループリント

宣言型デバイス管理を活用する

新しい設定配信の仕組み。



Jamf製品

Jamf for K-12



Pro

Connect

Protect

School

Jamf Safe Internet

教育機関向け "All-in-One" ソリューション

MDM

IdP Integrate

Endpoint Security

Network Security

まとめ

まとめ

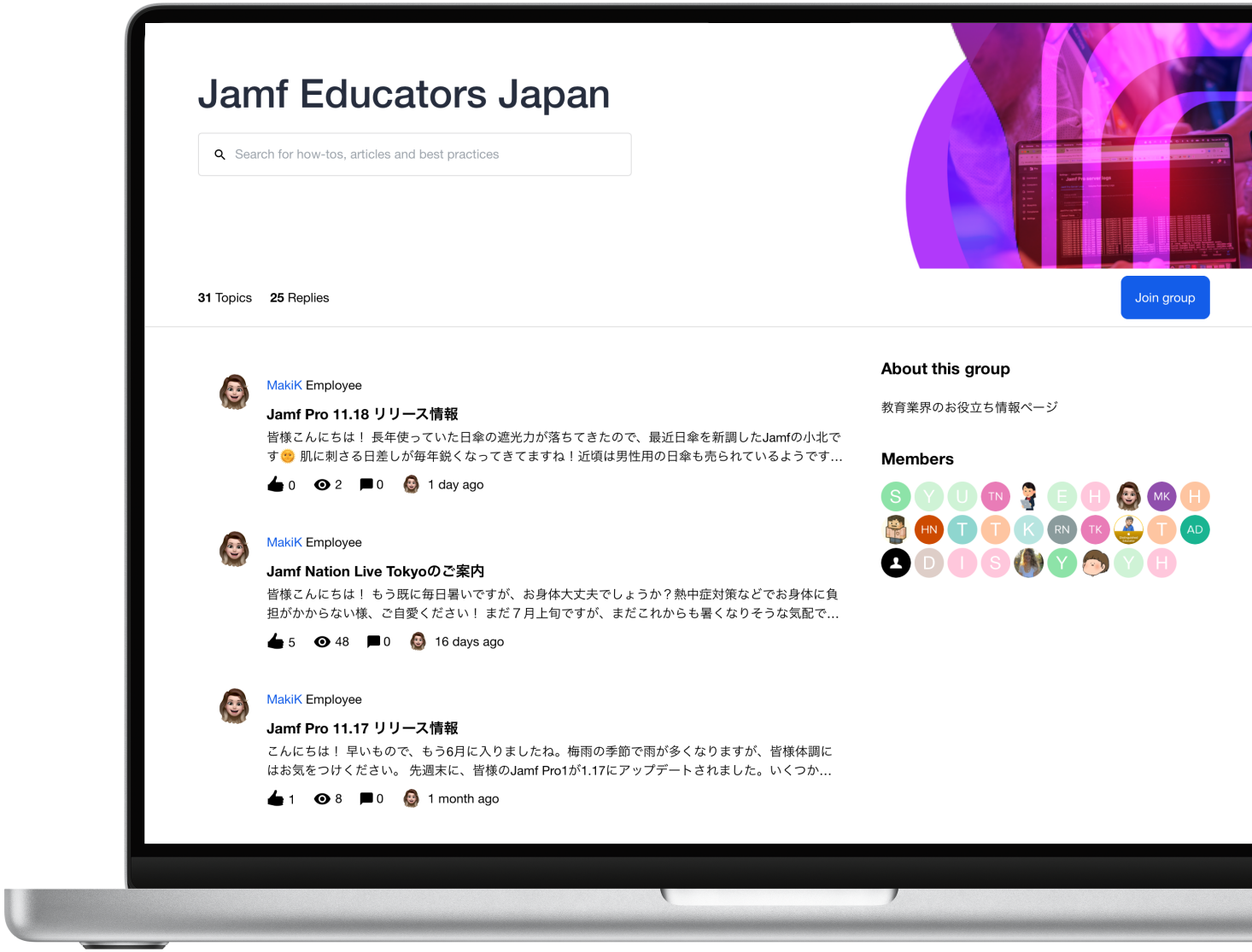
- Macを選択する学校/教育機関が増えています。
- JamfでiPadと同じようにMacを管理することができます。
- Macを管理するのであれば、Jamf for K-12(Pro) 、Jamf for Macが最適です。

最後に

Education
User Community

教育機関のお客さまが集う
Jamf Community

- Jamf の最新情報
- 管理者同士で情報交換
- オフ会など



JAMF NATION LIVE