●JAMF NATION LIVE

# Platform SSOで実現する、Mac ローカルユーザ管理の最適化




グンナレ　ペール

セールスエンジニア

JAMF JAPAN

# 内容

**概要**

Platform SSO とその可能性について

**仕組み**

Microsoft Entra ID 向け SSO の構成方法

**デモ**

ゼロタッチで Mac を新規セットアップ

**参考資料**

ドキュメントのリンク

# macOSアイデンティティの３つの時代

今 PSSO について下す決定が、今後５年間のアーキテクチャを形づくるでしょう。

1

### Directory Binding時代

- Active Directory / Open Directory のバインド
- Kerberos認証・LDAP 同期
- 2000年代〜2010年代の主流アプローチ

2

### Jamf Connect時代

- クラウド IdP との橋渡し
- IdP 連動のローカルアカウント管理
- ヘルパーアプリ・同期エージェントが実行

3

### Platform SSO時代

- 現在地：Apple ネイティブのアイデンティティ機能
- Secure Enclave（SEP）が署名鍵を保護
- SaaS アプリへのシングルサインオン実現

# Platform SSOとその可能性について

- AppleネイティブなmacOS機能
- macOSのローカルユーザアカウントとIdPアカウントの紐付け
- **Simplified Setup for Platform SSOのゼロタッチワークフロー**
  - macOS 26またはmacOS 27・Apple Silicon
  - IdP：Okta、 Entra ID、Ping Federate
- **Secure Enclaveキーモード**
  - フィッシング耐性 ：IdPパスワードが認証経路から消える
  - Mac上のアプリも SaaS アプリも、パスワード入力の手間を減らす




＊PRT: Primary Refresh Token

# Jamf Pro で簡単に導入できる Platform SSO

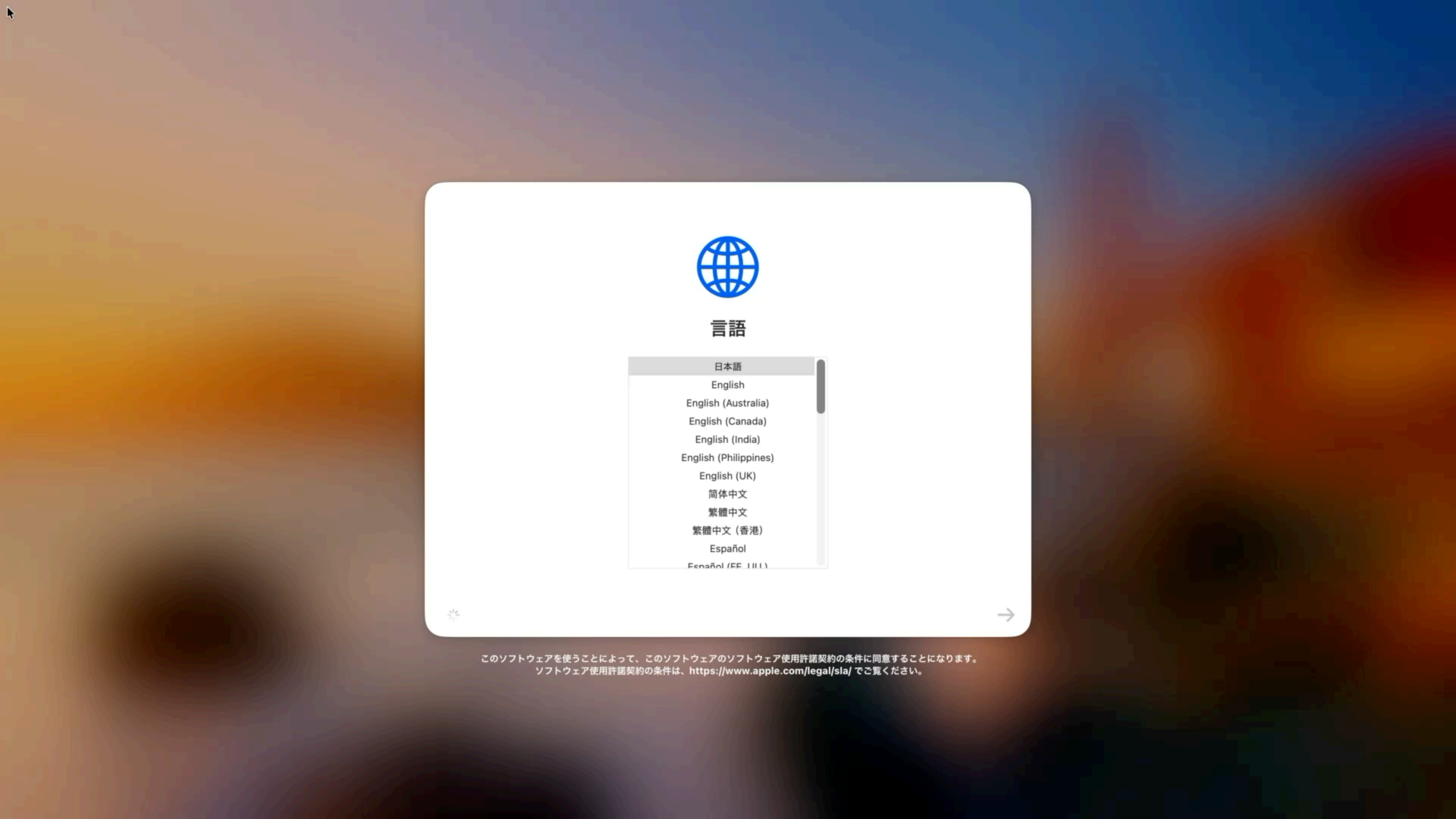
- **構成プロファイル：**
  - シングルサインオン機能拡張
  - FileVaultリカバリーキーのエスクロー
- **事前登録の要素：**
  - プラットフォームシングルサインオンの簡易設定を有効にする
    - 「アイデンティティ優先」モードまたは、「デバイス優先」モード
  - 登録パッケージ：不要
- **認証方式：**ユーザ Secure Enclave キーまたは、パスワード同期
- **ローカルアカウント権限：**管理者、標準




事前登録の要素



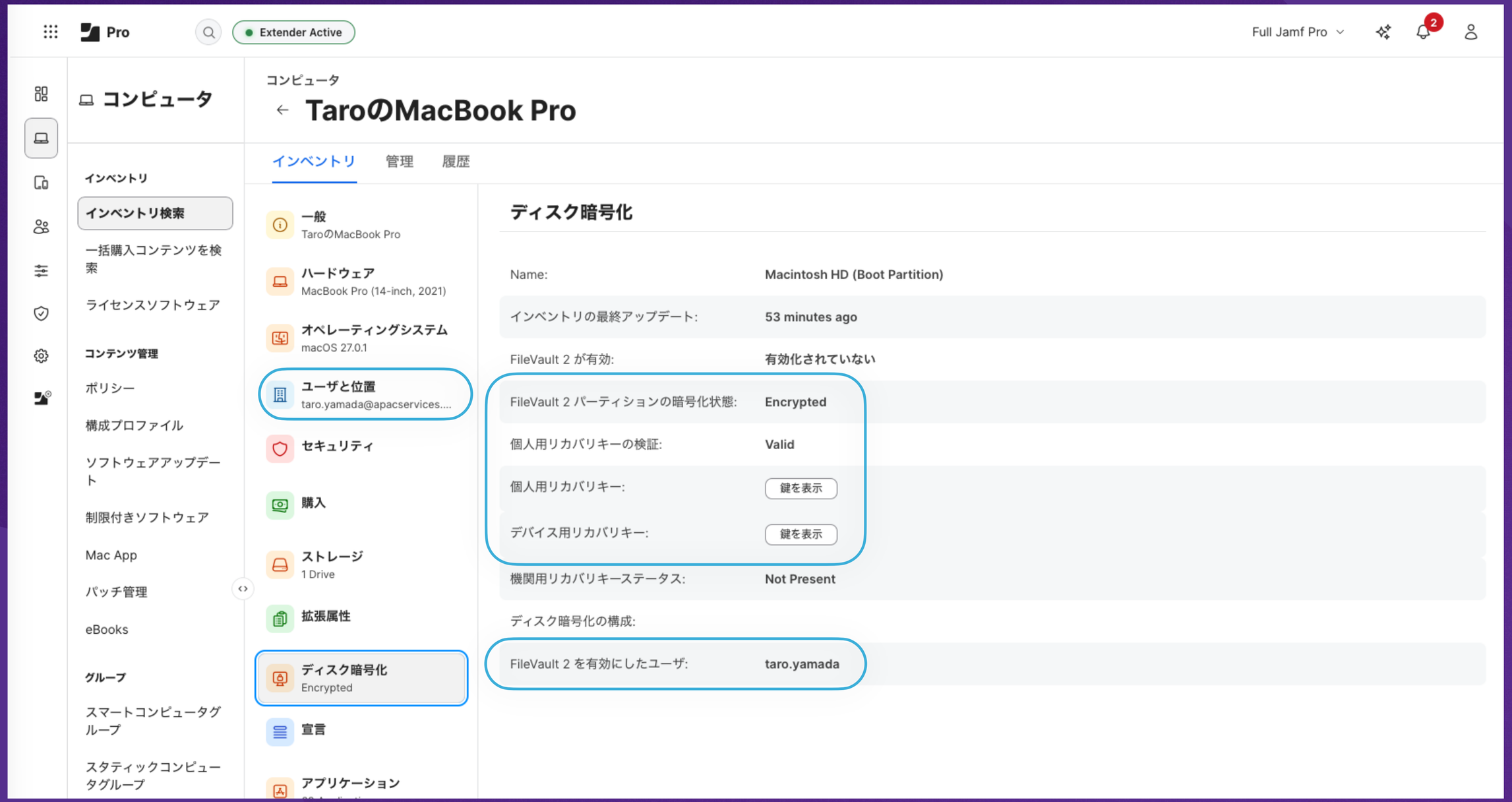

シングルサインオン機能拡張の構成プロファイル




このソフトウェアを使うことによって、このソフトウェアのソフトウェア使用許諾契約の条件に同意することになります。
ソフトウェア使用許諾契約の条件は、https://www.apple.com/legal/sla/ でご覧ください。


Finder
ファイル
編集
表示
移動
ウインドウ
ヘルプ
10月23日(金) 14:58
10月
日 月 火 水 木 金 土
1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 31
付近の天気を表示するには、位置情報へのアクセスが必要です。
処理が完了すると、ここに写真が表示されます。

# Jamf Pro で FileVault の結果確認



アイデンティティ、宣言型 へ

# macOS 27 Golden GateのPlatform SSO関連の新機能

- デバイスが宣言（declaration）を保持し、設定を自ら適用・維持します
- ログイン、Lock Screen、FileVault のロック解除で IdP のサインイン画面が表示可能になります
  - MFA・QR サインインも対応予定
- 機能の最新の情報は Jamf Pro および Microsoft のリリースノートでご確認ください

# まとめ

- Platform SSOはAppleネイティブなmacOS機能
- セットアップ手順は簡単
- Secure Enclaveキーの採用による、フィッシング耐性
- Mac上のアプリも SaaS アプリも、パスワード入力の手間を減らす
- ゼロタッチワークフロー対応（Entra ID、Okta、Ping Federate）
- Microsoft Entra ID を使用する場合の Device Compliance への自動登録

ぜひご自分の環境で Platform SSO をお試しください！

# 参考資料

- Jamf Conceptsポータルサイト: Platform SSO for macOS
  https://jamf.it/psso

- Deploying macOS Platform SSO for Microsoft Entra ID with Jamf Pro：
  https://learn.jamf.com/r/en-US/technical-articles/Platform_SSO_for_Microsoft_Entra_ID

- ユーティリティ：PSSO Utility
  https://github.com/jamf-concepts/psso-utility