内製IdPでも、いつものPCデリバリーを
～約2,200台のMacで実践した Jamf Connect 連携～

Keigo Akiba
株式会社ディー・エヌ・エー

2026年10月30日

© DeNA Co., Ltd.

自己紹介



Keigo Akiba

IT本部IT統括部IT戦略部

- 職歴
  - 1社目：COBOL を書く
  - 2社目：万屋情シス（1,500台）
  - 現在：端末管理情シス（5,000台）

© DeNA Co., Ltd.

DeNA Engineering Blog



2026.03.09 技術記事

DeNAが辿り着いた端末管理の完全自動化 — 稼働率100%と棚卸しからの解放

#windows #mac #pc #endpoint-management #corporate-it



2025.09.18 技術記事

5,000台のPC管理を自動化！稼働率最適化とコスト削減

#windows #mac #pc #endpoint-management #corporate-it



2025.01.30 カルチャー・環境

QCDを基盤とするDeNAの端末管理メソッド

#windows #mac #pc #endpoint-management #corporate-it

© DeNA Co., Ltd.

CONTENTS.0

DeNAについて

BUSINESS PORTFOLIO



© DeNA Co., Ltd.

BUSINESS PORTFOLIO [事業ポートフォリオ]

■ ゲーム



mobage



■ ライブコミュニティ

Pococha

IRIAM

■ ヘルスケア・メディカル

kencom　MySOS

ONSEI　Join

■ スポーツ・スマートシティ




川崎新!


■ 新領域・その他

DeNA × AI

delight ventures

© DeNA Co., Ltd.

IdP を丸ごと入れ替えたら
Jamf Connect を
理解せざるを得なくなった話です

目次

1 **IdP を内製するらしい** — Mac の届け方は、変えたくなかった

2 **Jamf Connect の中身** — プリセットがなく、一つずつ決めた

3 **2,200台を切り替える** — 難しいのは、いま使われている Mac

4 **まとめ** — 仕組みを理解して、IdP の入れ替えを越えた

© DeNA Co., Ltd.

1 IdPを内製するらしい

Mac の届け方は、変えたくなかった

© DeNA Co., Ltd.

1 これまで：Okta × Jamf Connect

2021年からは Okta × Jamf Connect で運用

2012年

Okta を導入。以後10年以上、社内の認証基盤

2021年春

Okta × Jamf Connect での運用開始

© DeNA Co., Ltd.

IdPを内製するらしい

© DeNA Co., Ltd.

1 Okta から 内製IdP へ

2012年から使ってきた Okta をやめ、内製 IdPに移行した

2012年

Okta を導入。以後10年以上、社内の認証基盤

2021年春

Okta × Jamf Connect での運用開始

2025年5月

Jamf Connect 検証開始

2026年1~3月

Mac を切り替え 3月に完了

詳しくは：DeNA Engineering Blog「IdP 移行」第1〜3回／「Jamf Connect × 内製IdP連携の全記録」

© DeNA Co., Ltd.

1 いつもの PC デリバリー：この流れは変えたくない

1

Apple Business で端末と組織を紐づけ

電源を入れてネットワークにつなぐと、Jamf Pro に自動登録

2

IdP の資格情報でローカルアカウントを作成

ここを担うのが Jamf Connect、または PSSO

3

アプリと設定が自動で入る

macOS Onboarding や Setup Manager

© DeNA Co., Ltd.

Jamf Connect は、
既に入って動いていた。
設定の中身は、説明できなかった。

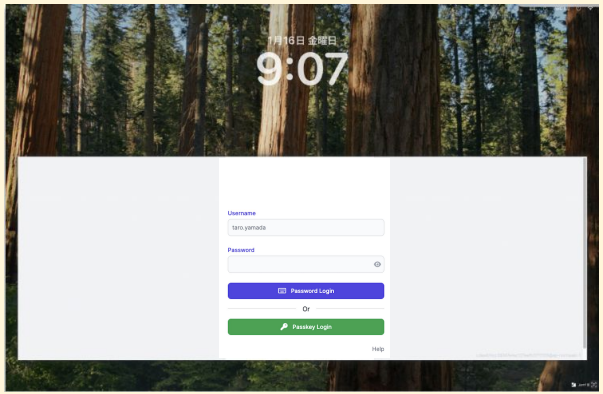
© DeNA Co., Ltd.

1 この後に出てくる2つの仕組み

Jamf Connect も PSSO も、Mac のアカウントを IdP とつなぐ仕組み

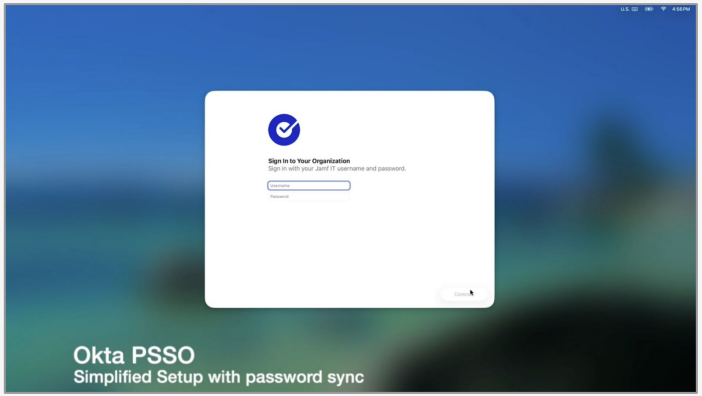
Jamf Connect

Jamf の製品



Platform SSO（PSSO）

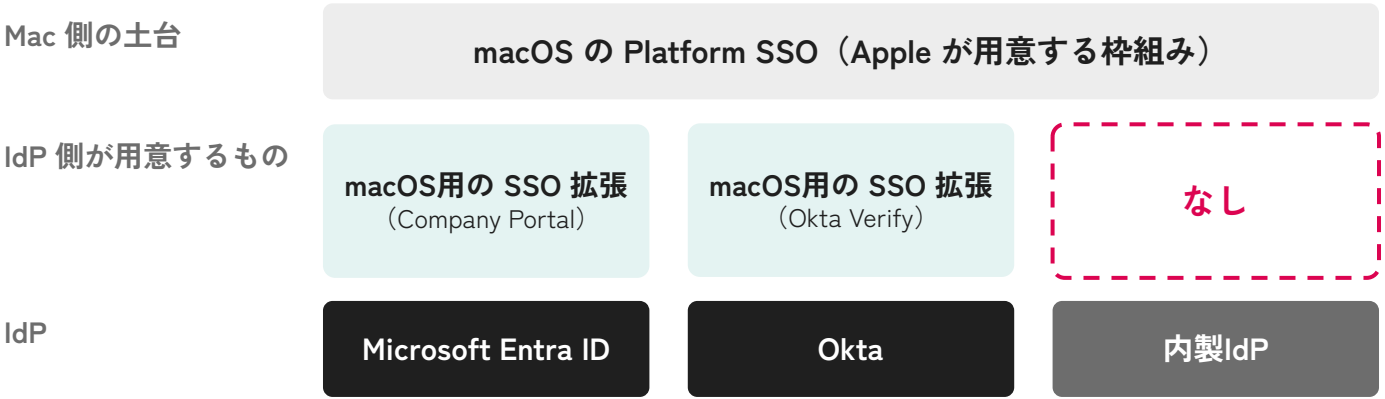
Apple の仕組み（macOS 13 以降）



© DeNA Co., Ltd.

1 PSSO は IdP ベンダーの拡張があって初めて使える

内製IdP には SSO 拡張がない。だから PSSO は選べなかった



出典：Jamf Concepts「Platform SSO for macOS」ほか

© DeNA Co., Ltd.

内製IdP では PSSO は選べない
Jamf Connect を続ける
では、何を設定すればいい？

© DeNA Co., Ltd.

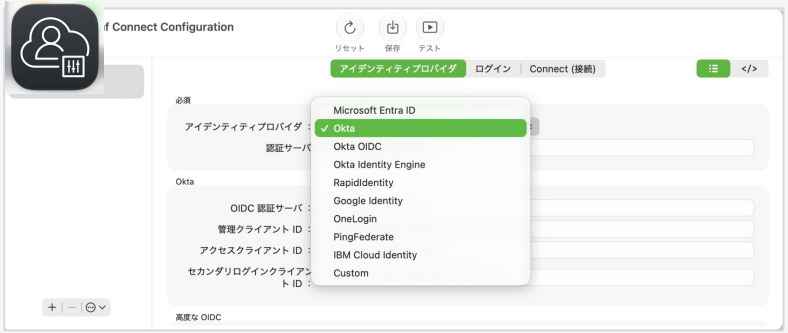
2 Jamf Connect の中身

プリセットがなく、一つずつ決めた

© DeNA Co., Ltd.

2 構成プロファイル（com.jamf.connect.login）の設定値を見直す

Okta（これまで）



プロバイダーに Okta を選べば、ほぼ完了

内製IdP



Discovery URL、クライアント ID、リダイレクト URI、ROPG、スコープ、ユーザー名に使うクレーム…を一つずつ決めた

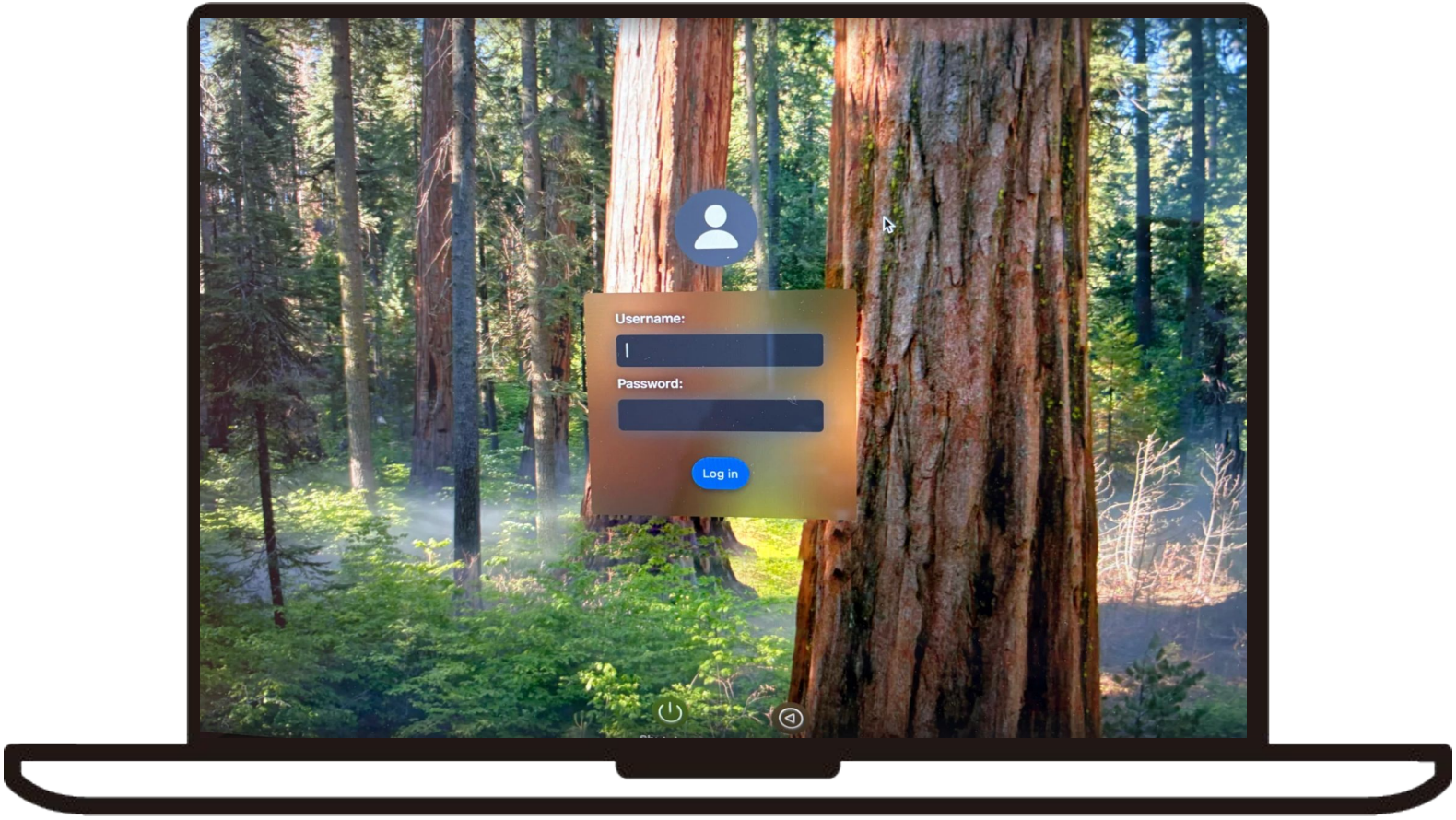
© DeNA Co., Ltd.

①ログイン画面での問題

© DeNA Co., Ltd.

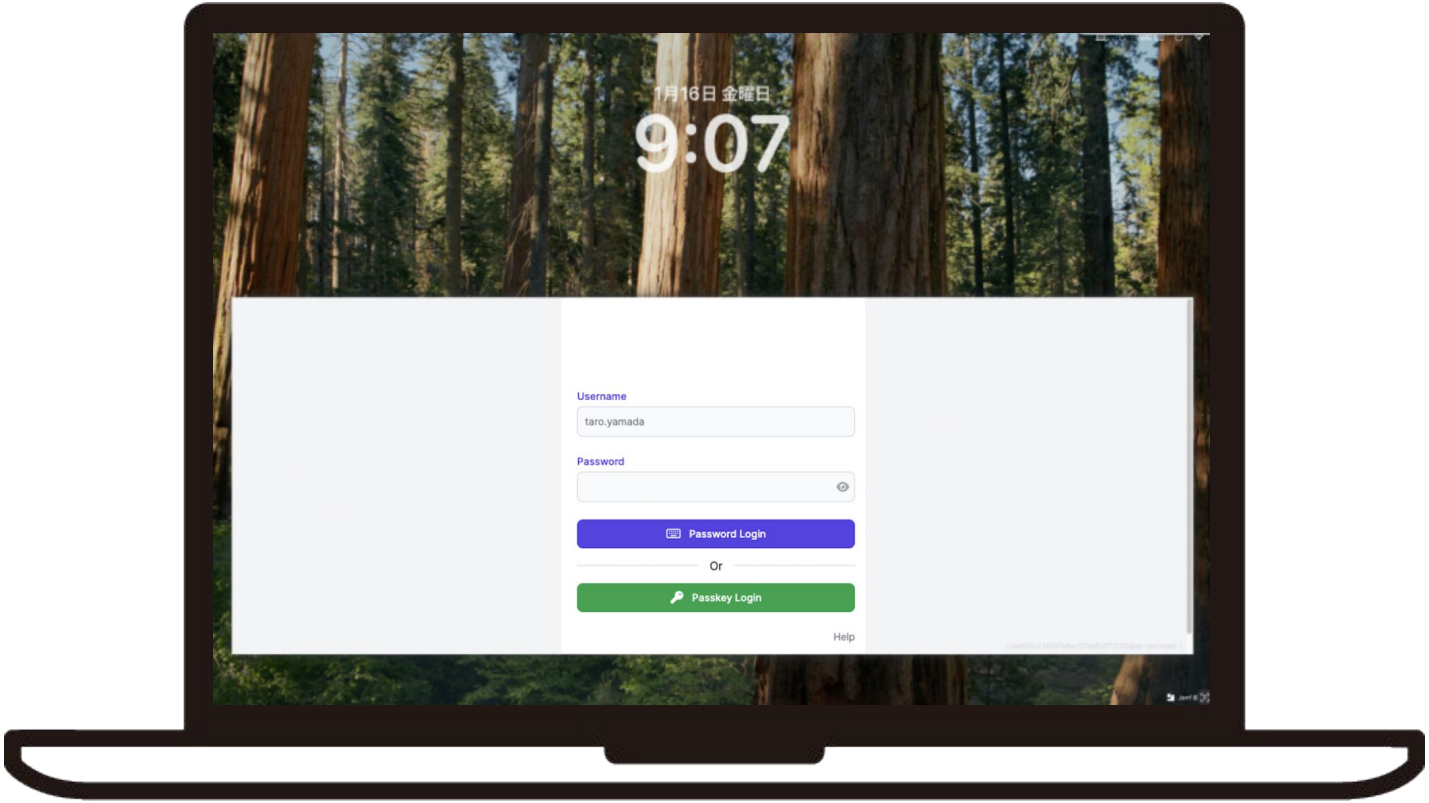


© DeNA Co., Ltd.



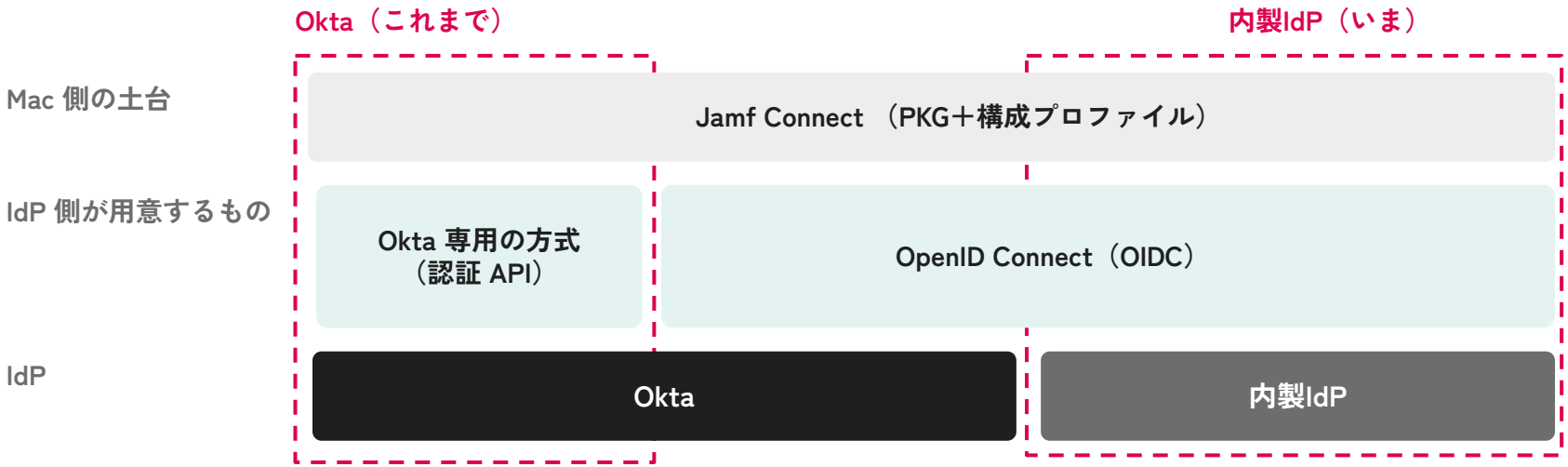
© DeNA Co., Ltd.

2 ログイン画面が Web 画面に変わり、アカウント作成に進まなくなった



© DeNA Co., Ltd.

2 つなぎ方が、Okta 専用の方式から OIDC に変わった



© DeNA Co., Ltd.

2 直した設定は2つ

設定（構成ツールの表記）	どうしたか
パススルー認証を使用 （OIDCUsePassthroughAuth）	true にする
別のローカルパスワードを作成 （OIDCNewPassword）	書かない ※false にすると期待どおりに動かなかった

『書かない』と『false』は、同じではなかった

© DeNA Co., Ltd.

②パスワード同期での問題

© DeNA Co., Ltd.

2 内製IdP につなぐと、パスワード同期が通らなかった



© DeNA Co., Ltd.

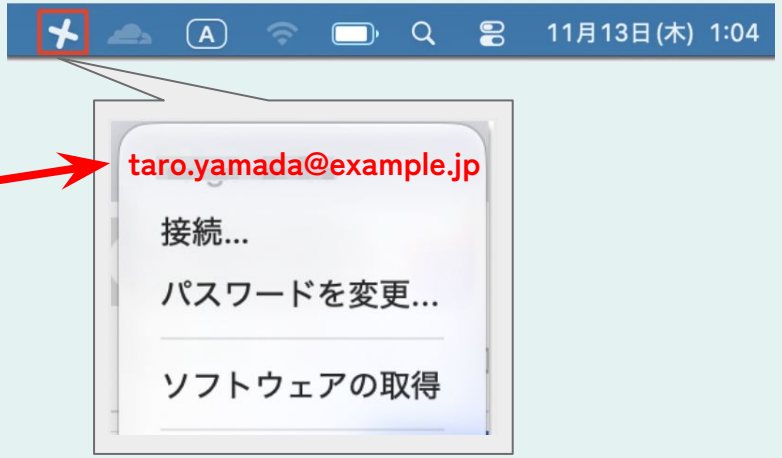
2 Menubar のユーザー名が、メールアドレスになっていた

内製IdP が返す ID トークン

email: taro.yamada@example.jp

name : taro.yamada

Jamf Connect Menubar



© DeNA Co., Ltd.

2 クレームは設定している

内製IdP が返す ID トークン

email: taro.yamada@example.jp

name : taro.yamada

Jamf Connect Configurationの一部



© DeNA Co., Ltd.

2 Jamf Connect は、決まった順番でクレームを探していた

順番	クレーム	OIDC 標準	内製 IdP の ID トークン
1	unique_name	標準外	なし
2	login	標準外	なし
3	username	標準外	なし
4	preferred_username	標準	なし
5	**email**	**標準**	**あり → これが使われた**

name は、探す順番に入っていなかった

出典：Jamf サポートの回答（2025-09）

© DeNA Co., Ltd.

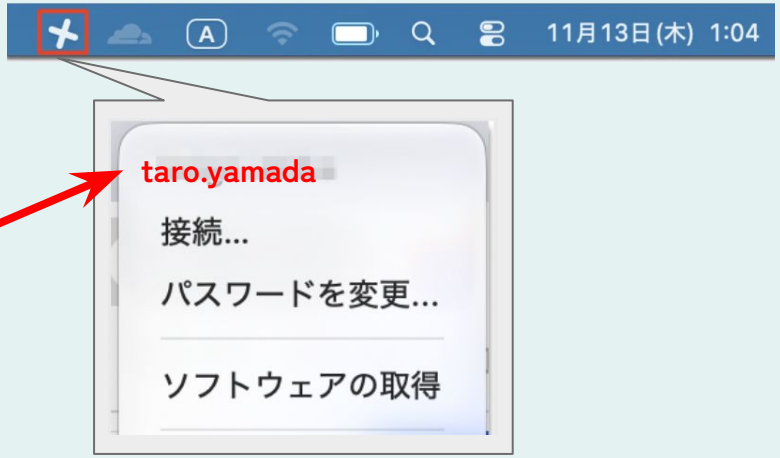
2 内製idpにカスタムクレームを追加するように改修して解決

内製IdP が返す ID トークン

`email`: taro.yamada@example.jp

`unique_name` : taro.yamada

Jamf Connect Menubar



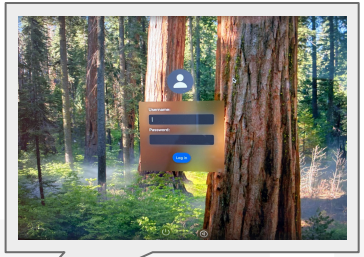
© DeNA Co., Ltd.

3 2,200台を切り替える

難しいのは、いま使われている Mac

© DeNA Co., Ltd.

3 全体の流れ（from Jamf公式ドキュメント）



1

ログイン画面の無効化

macOS 標準のログイン画面に戻す。切り替え中の締め出しを防ぐため

2

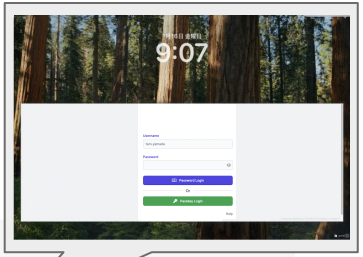
Mac から旧 IdP 属性の削除

旧 IdP の構成プロファイルを外し、IdP 属性を削除するスクリプトを実行

3

新 IdP の構成を配布

新 IdP の構成プロファイルとSelf Service＋ の PKG配布



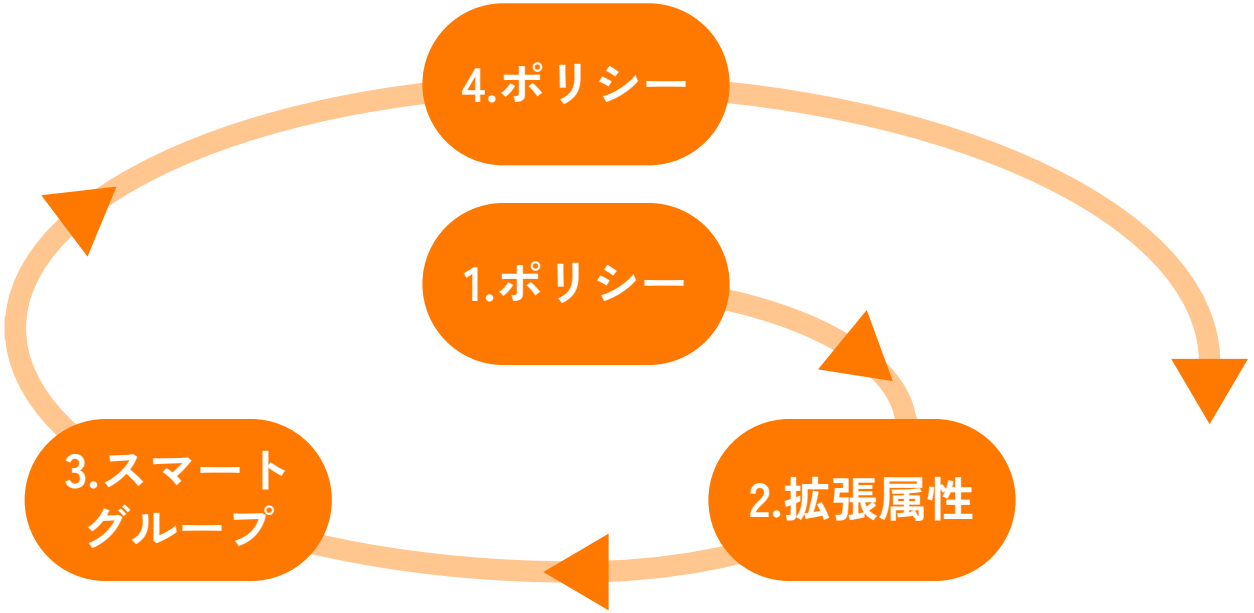
4

ログイン画面の有効化

Jamf Connect のログイン画面に戻し、新 IdP で再ログインしてもらう

© DeNA Co., Ltd.

3 Jamf Pro でどのように構成したのか？



© DeNA Co., Ltd.

3 ポリシーの最後に、完了の印を置く



© DeNA Co., Ltd.

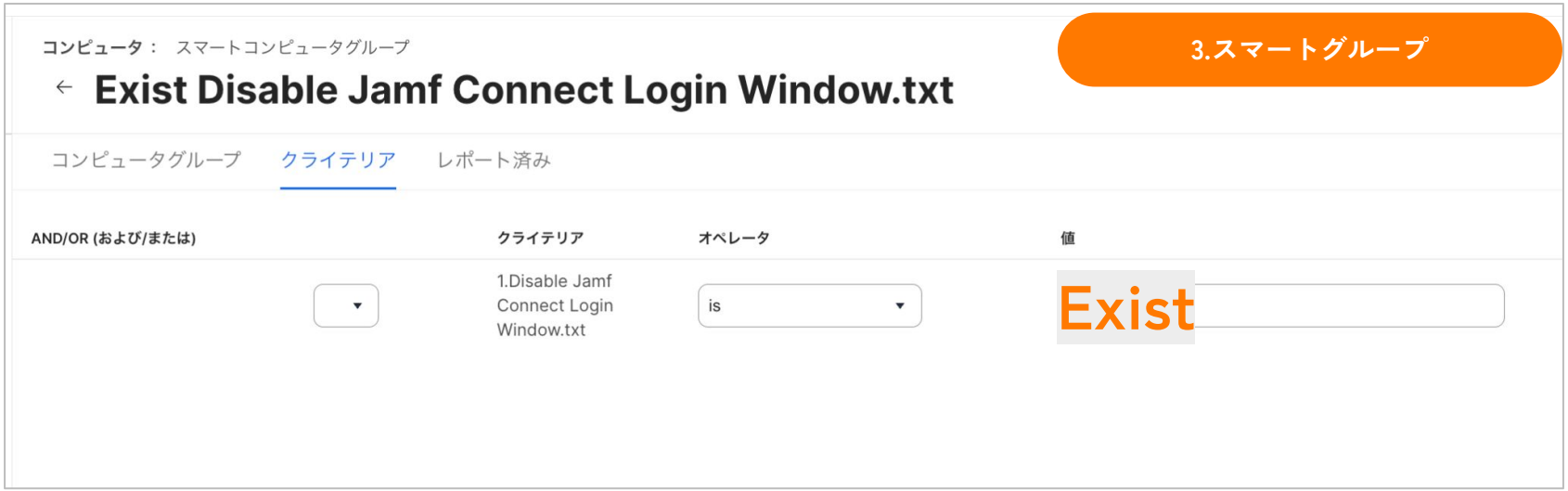
3 印があるかを、拡張属性で見る

2.拡張属性

1.Disable Jamf Connect Login Window.txt:	Exist
2.Remove Okta Configuration File.txt:	**not exist**
3.Re-Enable_Jamf_Connect_Login_Window_v2.txt:	**not exist**
4.idp destination:	**Okta**

© DeNA Co., Ltd.

3 印のある Mac だけが、次のステップに進む



© DeNA Co., Ltd.

入口はスタティックグループ

© DeNA Co., Ltd.

最後の再ログインまでは
ユーザーは気づかない

© DeNA Co., Ltd.

最後の1歩だけは
ユーザーにしかできない

ログアウトして、新しい IdP でログインし直す

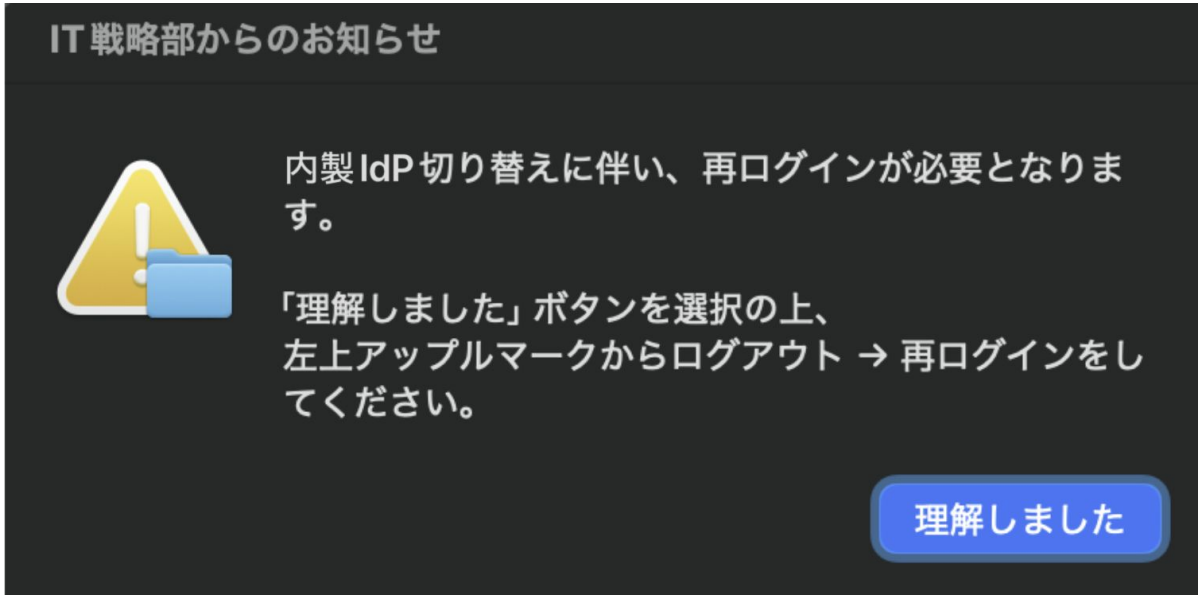
© DeNA Co., Ltd.

1か月で約2,000台

問い合わせは数件

© DeNA Co., Ltd.

3 ログアウトしていない Mac にだけ、ポップアップを出した



© DeNA Co., Ltd.

3 結果

- 1か月で約2,000台、3月に完了
- 問い合わせは数件

© DeNA Co., Ltd.

3 学び

- 内製 IdP でも、できないことはなかった
- 完了の印を、macOS が削除する場所に置いていた

© DeNA Co., Ltd.

4 まとめ

仕組みを理解して、IdP の入れ替えを越えた

© DeNA Co., Ltd.

「こうだったから」で済ませず
自分で確かめる

私は、IdP を変えるまで説明できませんでした

© DeNA Co., Ltd.

一人ひとりに　想像を超えるDelightを

:DeNA



© DeNA Co., Ltd.