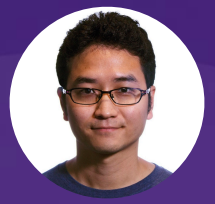
JAMF NATION LIVE

Jamf Proの健康診断

～今こそ見直したい設定とベストプラクティス～



大田 龍志

SALES ENGINEER, JAMF JAPAN

本日の流れ

01 **なぜ今、健康診断か**

OS 27 と 宣言型で前提が変わった

02 **基本検査**

デバイスの様子を見る

03 **精密検査**

構成プロファイルとブループリント

04 **処方箋**

健康診断を続ける仕組み

なぜ今、健康診断か
設定は、入れた日から古くなる

OS 27 ／ 宣言型への移行 ／ 新しいインベントリ項目

基本検査

デバイスの様子を見る

基本検査①

まず、連絡がつくかを確かめる

Last Check-in / Last Contact

一定期間通信のない端末を洗い出す

MDM プロファイルの有効期限

期限切れの前に更新されているか。

自動更新の設定も確認

紛失モードの有効化状態

紛失モード: 有効

基本検査①
「要注意端末」をスマートグループにしておく

グループ名	条件の例
30日以上通信のない端末	インベントリの最終アップデート ／ more than x days ago ／ 30
MDMプロファイルの期限が近い端末	MDM プロファイル有効期限日 ／ less than x days ago ／ 60
紛失モードが有効なデバイス	紛失モード有効済み ／ is ／ Yes

「Jamf Pro Dashboard に表示」をオンにして、件数の変化を見る／ Eメール通知を送信 ／ WebHook 連携

基本検査②

守りの設定が、端末で本当に効いているか



FileVault

判定には「FileVault 2 パーティションの暗号化状態」を使う



ブートストラップトークン

「ブートストラップトークンをエスクロー済」で預け入れを確認



OS バージョン

古いバージョンで止まっている端末はないか

新しいインベントリ項目
端末が自分の状態を報告してくれる

Device System Health - デバイスシステム正常性
カメラ、ディスプレイ、Face ID などの部品の異常や非純正部品に関する情報（iOS / iPadOS 27）

Awaiting Configuration - 構成待ち
初期設定で止まっている端末

Lockdown Mode - ロックダウンモード
ロックダウンモードの有効化状態

Healthy
すべての部品が OK

Unhealthy
Error / Non-genuine が 1 つ以上

MDM コマンドで問い合わせず、DDM の状態報告から自動で更新される

精密検査

構成プロファイルとブループリント

精密検査①

構成プロファイルの3 つの見直しポイント

配布できているか

ダッシュボードで 完了 / 保留 / 失敗を見る

何の設定かわかるか

名前だけで目的がわかるか。例：FileVault個人用回復キーの収集設定

古いやり方のままか

MDM コマンドによるOSアップデート管理は DDM へ移行

精密検査

配布できているか

iOS 構成プロファイル

Jamf Trust / Self Service 通知設定



- 9 完了
- 0 保留
- 0 失敗

ロック画面のメッセージ



- 9 完了
- 0 保留
- 0 失敗

2 / 2 件の iOS 構成プロファイルを表示中

ポリシー

swiftdialog



- 2 完了
- 0 保留
- 0 再試行中
- 0 失敗

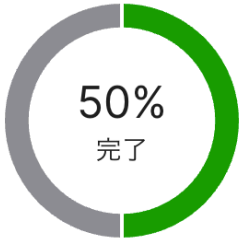
デバイス名をシリアルナンバーにする



- 2 完了
- 0 保留
- 0 再試行中
- 0 失敗

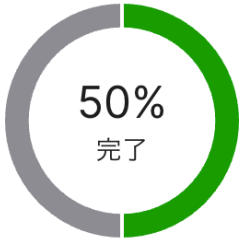
macOS 構成プロファイル

FileVault個人用回復キーの収集設定



- 1 完了
- 1 保留
- 0 失敗

NTPサーバをntp.jst.mfeed.ad.jpに強制する



- 1 完了
- 1 保留
- 0 失敗

2 / 2 件の macOS 構成プロファイルを表示中

精密検査②

同じ設定を、2 か所から配らない

- 構成プロファイルとブループリントで同じ設定を配ると、どちらが勝つかは決まっていない
- Jamf Pro は重複をチェックしない。どの設定をどちらで管理するかを自分で決めて記録する
- 移行は「ブループリントで配布を確認 → 古いプロファイルを外す」の順番で
- 配布状況は全体確認をブループリントで、個別でインベントリ→宣言 から確認可能（Successful / Pending / Error）

精密検査②　分担の決め方

設定の領域ごとに、担当を 1 つに決める

設定の領域の例	担当	考え方
OS アップデートの設定	**ブループリント**	MDM コマンドや構成プロファイルによる設定は廃止。
外部ストレージの制限	**ブループリント**	オンオフの制御が可能。（Jamf Protect でさらに細かく可能）
パスコード設定	**ブループリント**	DDM /プロファイルのどちらでも制御可能。 古いプロファイルと二重になりやすい代表例
Wi-Fi、証明書、PPPC	**構成プロファイル**	現在はブループリントでは設定ができない。

決めた分担は、各設定の説明欄や管理台帳に書き残す

JAMF PRO 自体の健康

サーバー側の「期限」と「権限」も点検する

プッシュ通知証明書とトークン

APNs 証明書、ADE トークン、VPP トークンは毎年更新。担当者と日付を決める

管理者と API の権限

新機能の権限は、カスタム権限のアカウントでは既定でオフ

使われていない設定

使われていないスマートグループやポリシーを棚卸し

処方箋

健康診断を「続ける」仕組みを作る

常時	要注意端末のスマートグループをダッシュボードに並べる
月 1 回	件数の変化を見る
年 1 回	設定の棚卸しと証明書の更新

何を「健康」とみなすかを決めるのは管理者です。Jamf の今後の方向性は、午後の基調講演「Power Up with Jamf」でもぜひ。