JAMF NATION LIVE

MacのAIガバナンス

～ AIエージェント管理と、あらためて考えるMDMの重要性 ～



佐久間 謙玖

JAMF JAPAN

Agenda

01　なぜ、AIエージェントから考えるのか

チャットとエージェントの違い、既存の統制で見えにくい理由

02　境界が消え、「正解探し」の段階へ

allow / denyの先にある運用設計

03　Jamf - AI ガバナンスでできること

見る・考える・適用する・確かめる

04　あらためて考えるMDMの重要性

AIを統制する設定を確実に届ける

05　これからのAIガバナンス

ブラウザ、コスト、オンデバイスAI

AIは、もうデバイスの中にある

Q1. 今、どれだけのAIが、どのように使われているか。説明できますか？

Q2. 自社に最適なルールを自社で考え、システムと運用に反映できていると言えますか？

WHY AGENTS FIRST

チャットは「答える」、エージェントは「操作する」

チャット型AI

答える

1. 人が質問する
2. AIが答える
3. 人が判断して、操作する

操作するのは「人」

AIエージェント

操作する

人が目的を伝えると、AIが考えて自分で操作する

- シェルコマンドを実行
- ファイルを読み書き
- 認証情報にアクセス
- 社内システムにアクセス

操作するのは「AI」

エージェントは、**本人の権限**で動く

BLIND SPOTS

既存の統制では、見えにくいもの

CASB
見えていない

ドメイン単位の制御では、許可したAIツールが端末の中で何をしているかまでは見えない

EDR
フラグが立たない

「claude」というプロセスは見えても、マネージド設定やMCP接続、エージェント実行時の挙動までは見えにくい

Proxy
中身が見えない

見えるのはAIベンダーへの暗号化された通信。エージェントが何を指示されたかは見えない

MCP：社内システムにつながる、見えない入口

MCPサーバが露出させるもの

- **File systems & databases**
  ファイルシステムとデータベース
- **Internal APIs & services**
  社内APIとサービス
- **Credentials & secrets**
  認証情報とシークレット
- **Code repos & CI/CD**
  コードリポジトリとCI/CD

把握が追いついていないもの

- ⚠ どのMCPサーバが動いているか
- ⚠ それが露出させている社内システムは何か
- ⚠ どのAIクライアントが接続しているか
- ⚠ エージェントがどのような操作をしているか

Shadow IT ≠ Shadow Infra　止めるのではなく、管理する

エンジニアだけの話では、ない

チャットとエージェントの境界が、消えつつある

答える → 操作する

例. Anthropicの場合

Claude（チャット）

質問に答える

チャットとCoworkを一つにする動きが、プランごとに段階的に展開中

Claude Cowork

業務のタスクを実行

中身は、Claude Codeと同じエージェントの仕組みで動く

Claude Code

開発のタスクを実行

エージェントの代表的なツール

WHERE TO START

だから、**リスクの大きいところ**から始める

リスクの大きいところから、段階的に広げる

Step 1

AIエージェント

Claude Code、OpenAI Codex など

提供中

Step 2

デスクトップAIアプリ

Claude Desktop など

提供中

Step 3

ブラウザのAI

Claude、ChatGPT、Gemini など

Q4 2026 GA目標

ALLOW / DENYの先へ

AIガバナンスは「正解探し」の段階

これまで → 今

Step 1

試す

AIで何ができるか、どのくらいコストがかかるかをチャレンジする

Step 2

気づく

ちゃんと管理・制御をしないといけない、という意識が強くなる

Step 3 いまここ

設計する

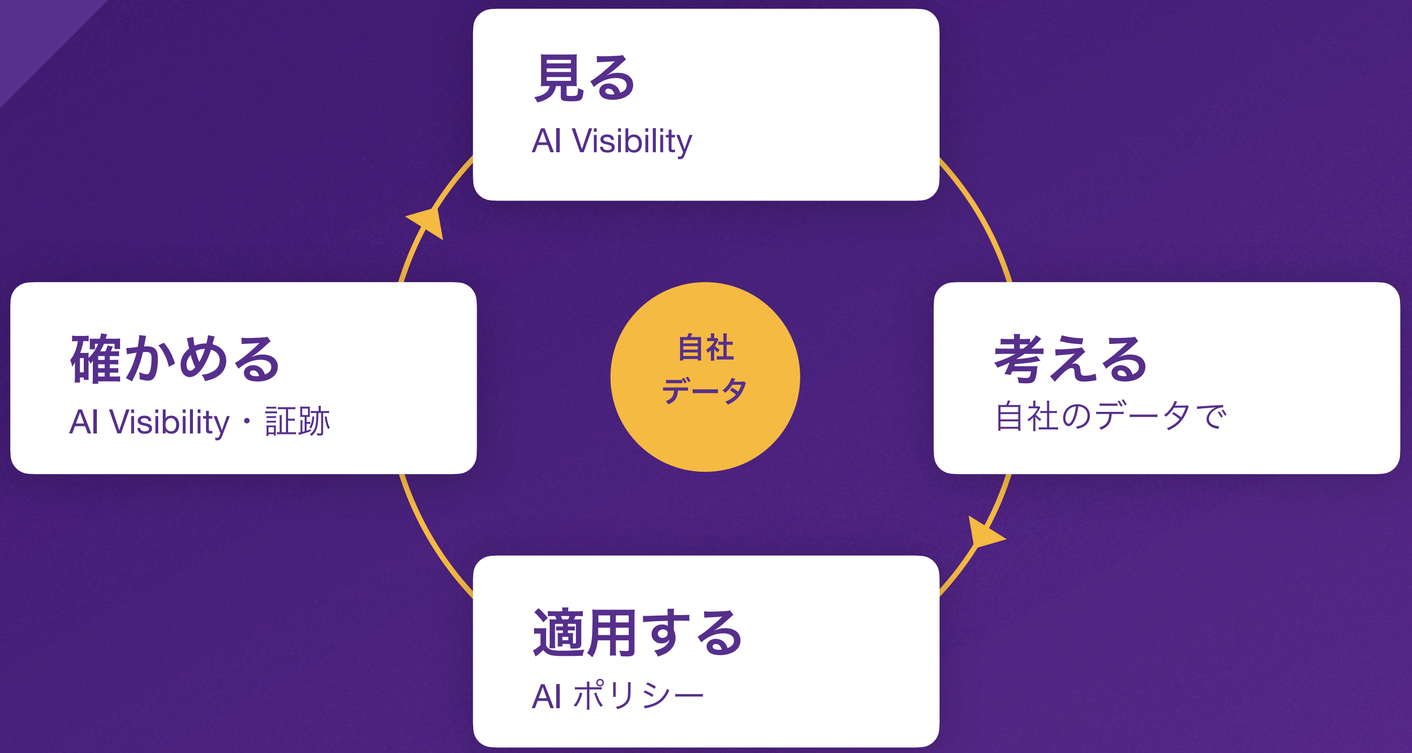
allow / denyの単純な話ではなく、運用ルールとシステムを両面から設計する。ただし、どの企業でも共通とできる明確な正解やベストプラクティスはまだない

Jamf - AI ガバナンス

見える化・制御・証跡で、AIを統制する

JAMF AI ガバナンス

見る → 考える → 適用する → 確かめる



見ずに決めると

締めすぎる

使いたい人が管理外のツールに流れ、かえってシャドーAIが増える

緩すぎる

リスクを抱えたまま、説明もできない

目的は、個人の取り締まりではなく、自社に合ったルールの設計

AI Visibility：何が見えるようになるか

収集データ

収集データ起動元プロセス、実行コマンド、リスクが存在する可能性があるコマンド、MCPサーバの稼働状況

レポート

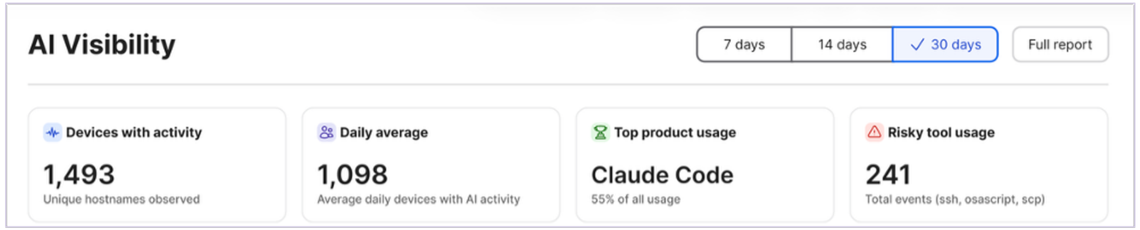
7日／14日／30日の期間でPDFを出力。個別アプリ単位・全AIアプリ包括の両方に対応

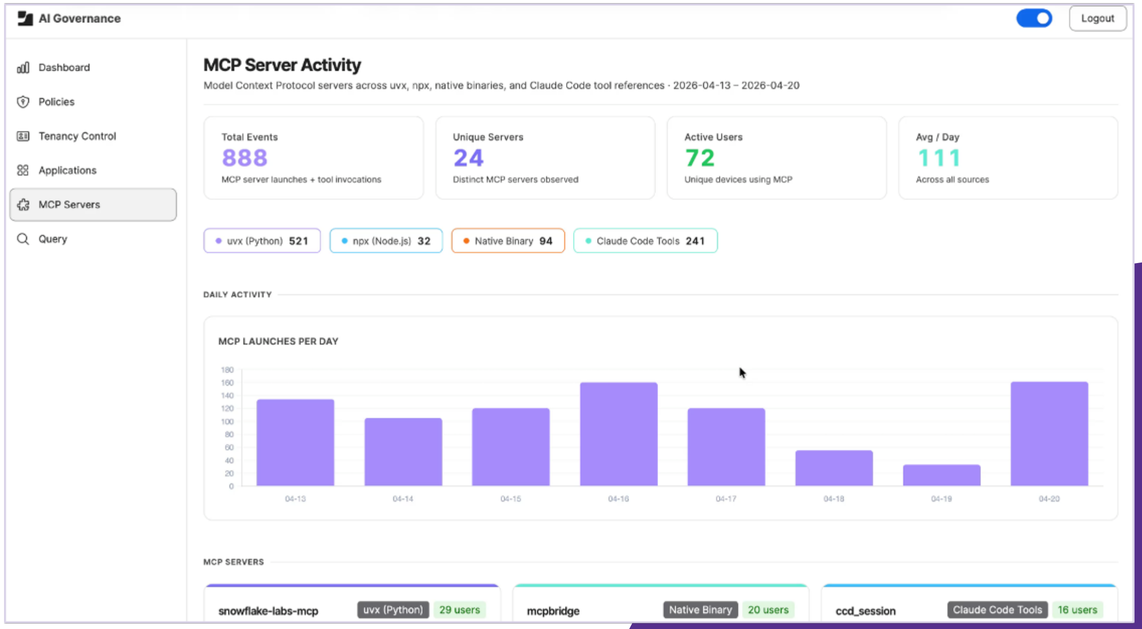
ダッシュボード

デバイス数、日次平均利用デバイス数、プロダクト別の利用状況

対応アプリは順次拡大

- 主な対象：Claude Code、OpenAI Codex などのAIコーディングツールや、デスクトップのAIアプリ
- 2026年8月の追加：Microsoft 365 Copilot、Microsoft Scout など





AI ポリシー：何を制御できるか

配布はJamf Proのブループリント経由。JSONを書かずに、画面のフォームで設定可能

Claude Code

Models & Reasoning
利用モデルの制限

Permissions
コマンド／パス／MCPのallow・deny

Sandbox Isolation
OSレベルの分離

Managed MCP Server Policy

Organization Defaults
上書き不可の基準設定

Claude Desktop

Workspace Restrictions
フォルダ・ネットワーク・高リスクツール

Connectors & Extensions
MCPサーバ・拡張の制限

Login & Organization Binding
組織アカウントでのログイン

Appearance
組織バナー・AI利用ポリシーへのリンク

Telemetry & Updates

OpenAI Codex

Models & Reasoning

Permissions & Sandbox

Command Rules

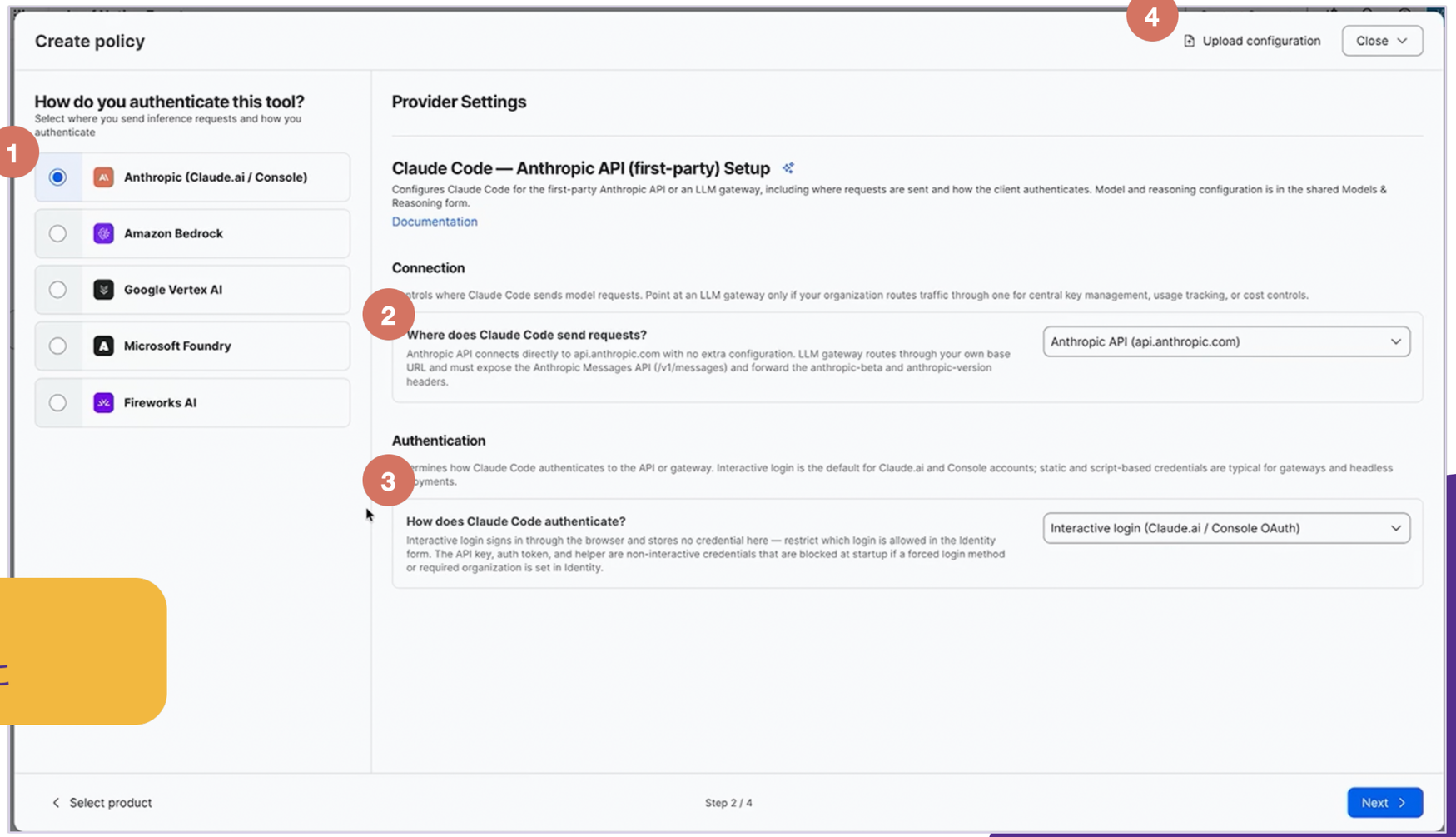
MCP Server Allowlist

Data Residency
データの地理的保管要件

設定は、画面で選択する

1. 対象の選択
2. リクエストの送り先
3. 認証方法
4. 既存の設定を取り込む

JSONを書かずに
誰が設定しても同じ基準に



適用する | AI ポリシー IN ACTION

ポリシーが効く瞬間

```
GVwLW1kwDKmIZ00Dv74ddwnbH3N0uZpDP"}}'
Added http MCP server github to local config
user@Users-Mac-mini code % claude mcp add --transport http atlassian https://mcp.atlassian.com/v1/mcp
Cannot add MCP server "atlassian": server is explicitly blocked by enterprise policy
user@Users-Mac-mini code % claude
```




```
Message from jonmalm@gmail.com's Organization:
Use only approved AI tools and accounts. Never enter confidential or proprietary data into unapproved platforms. All AI-generated output must be
reviewed by a human before use. Violations should be reported to the Security team.  See Jamf's [AI Use in the Workplace
Policy](https://jamf.service-now.com/jamfiverse/en/ai-use-in-the-workplace-policy?id=kb_article&sysparm_article=KB0145279) for more information.
```

01
その場でブロック

許可されていないMCPサーバ（例ではAtlassian）の追加が、拒否される

02
ルールへ案内

画面に、会社のAI利用ポリシーへのリンクが表示される

改めて考えるMDMの重要性

AIを統制する設定を確実に届けるのは**MDM**

配る

会社として決めた設定を、ブループリントで管理下のすべてのMacへ届ける

守らせる

利用者が上書きできない基準として適用する（例：Claude Codeの組織の基準設定）

前提をつくる

管理されたMacでなければ、見える化も制御も届かない

確かめる | AUDIT TRAIL

AIを使えるだけでなく、「証跡が残る」価値

1

AI ポリシーの展開・設定は記録として残る

「何を許可し、どう設定したか」を、後から具体的に示せる

2

レポートはPDFで出力可能

社内報告や監査対応の場面で、資料としてそのまま使いやすい

3

開発も業務も止めずに、説明可能な状態をつくる

ブロックするのではなく、正しく設定し「使って良い」と言えるようにする

COVERAGE

Mac上のAIガバナンスが、**揃っていく**

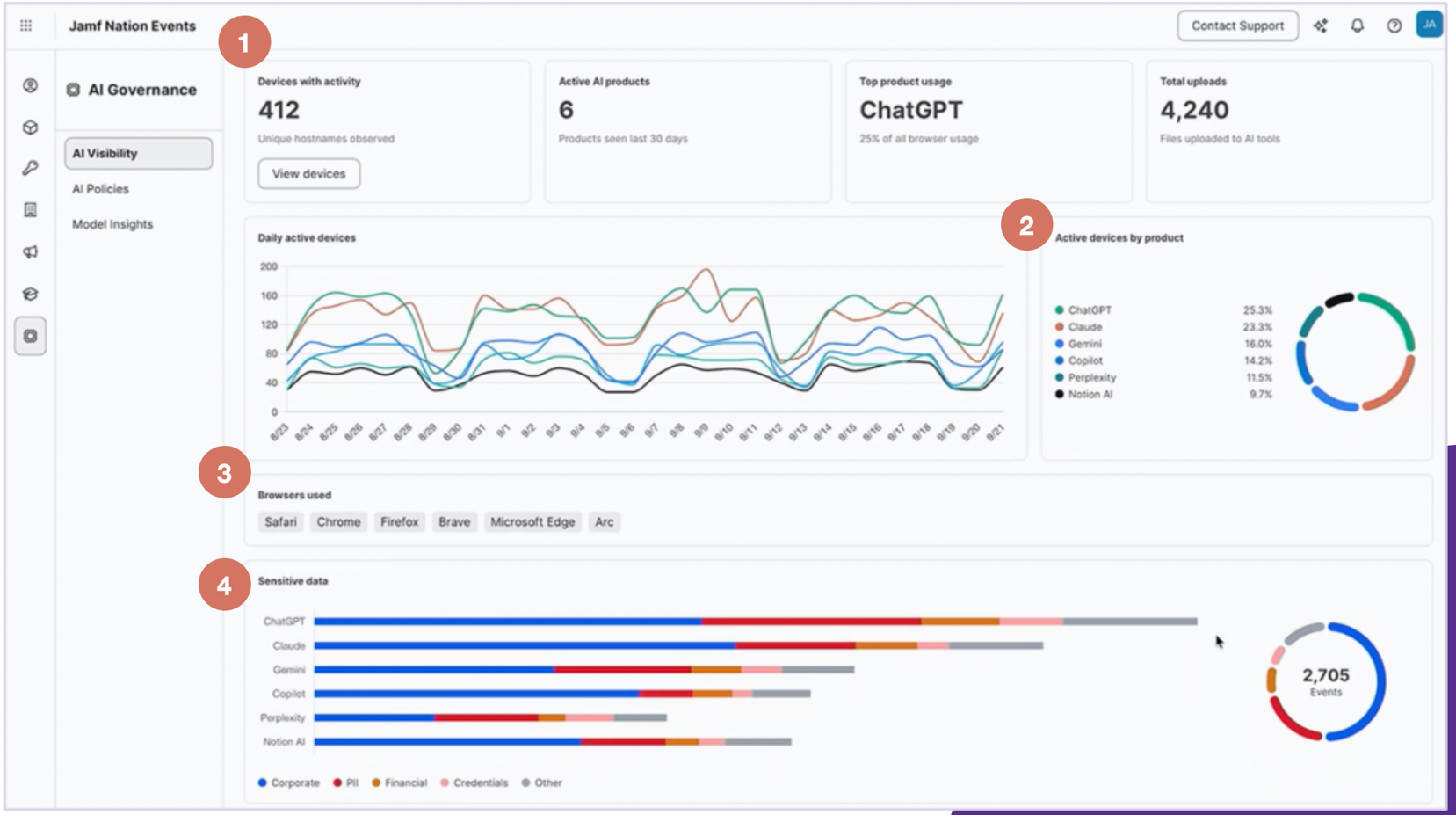
	見える化	制御	証跡
AIエージェント	提供中	提供中	提供中
デスクトップのAIアプリ	提供中（対応アプリ）	提供中	提供中
ブラウザのAI	2026 GA目標	2026 GA目標	—

より深い調査：デバイス・ユーザ・コマンドライン単位まで　2026 GA目標

※GA目標は予告なく変更となる場合があります

ブラウザのAI利用も、見える化へ

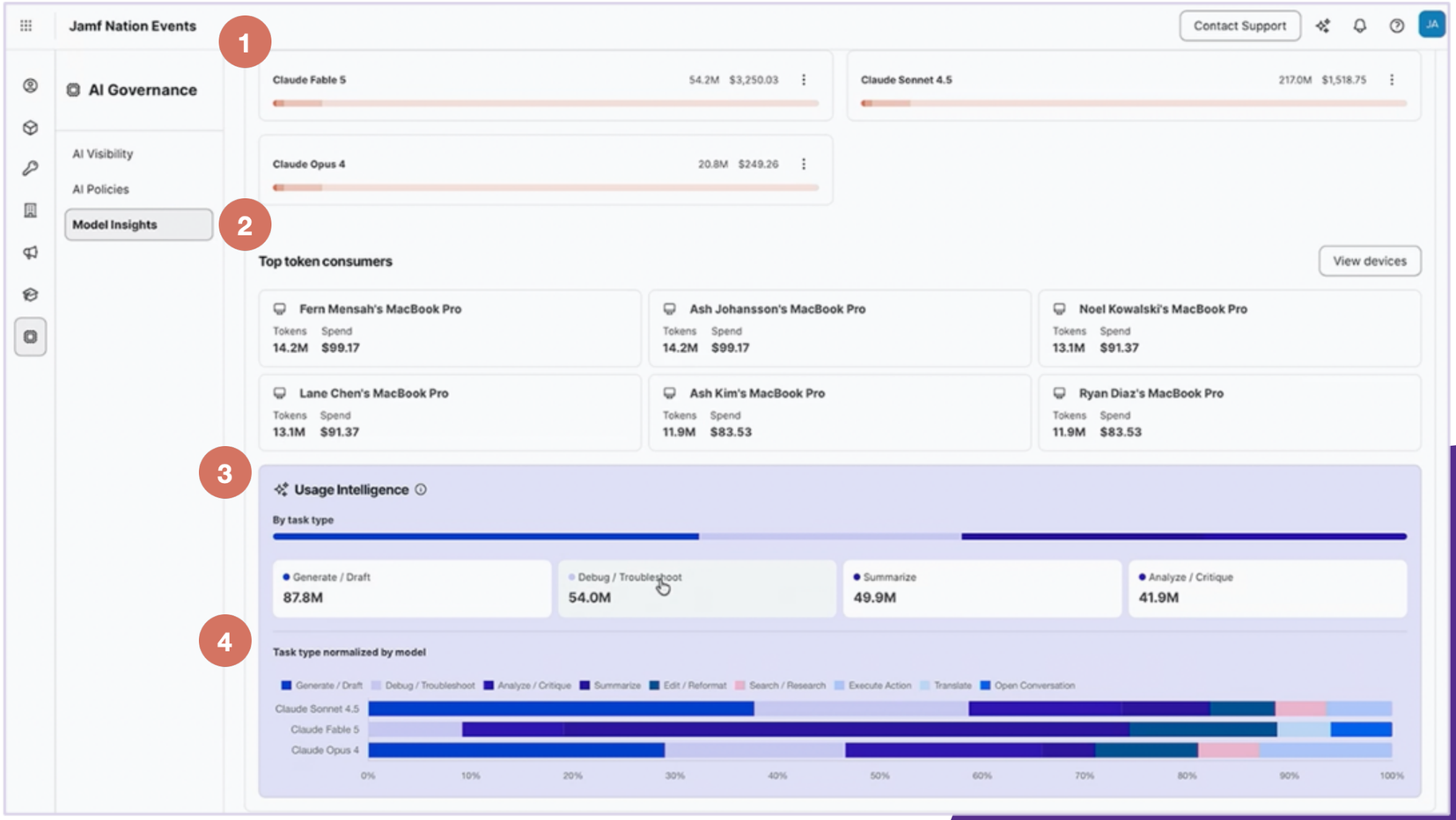
1. 利用状況のサマリ
2. サービスごとの利用
3. 使われているブラウザ
4. 取り扱われたデータの種類



※GA目標は予告なく変更となる場合があります

AIの利用量とコストを見る

1. モデルごとの利用と推定コスト
2. 利用量の多いデバイス
3. 用途別の利用
4. モデルごとの用途の違い



※GA目標は予告なく変更となる場合があります

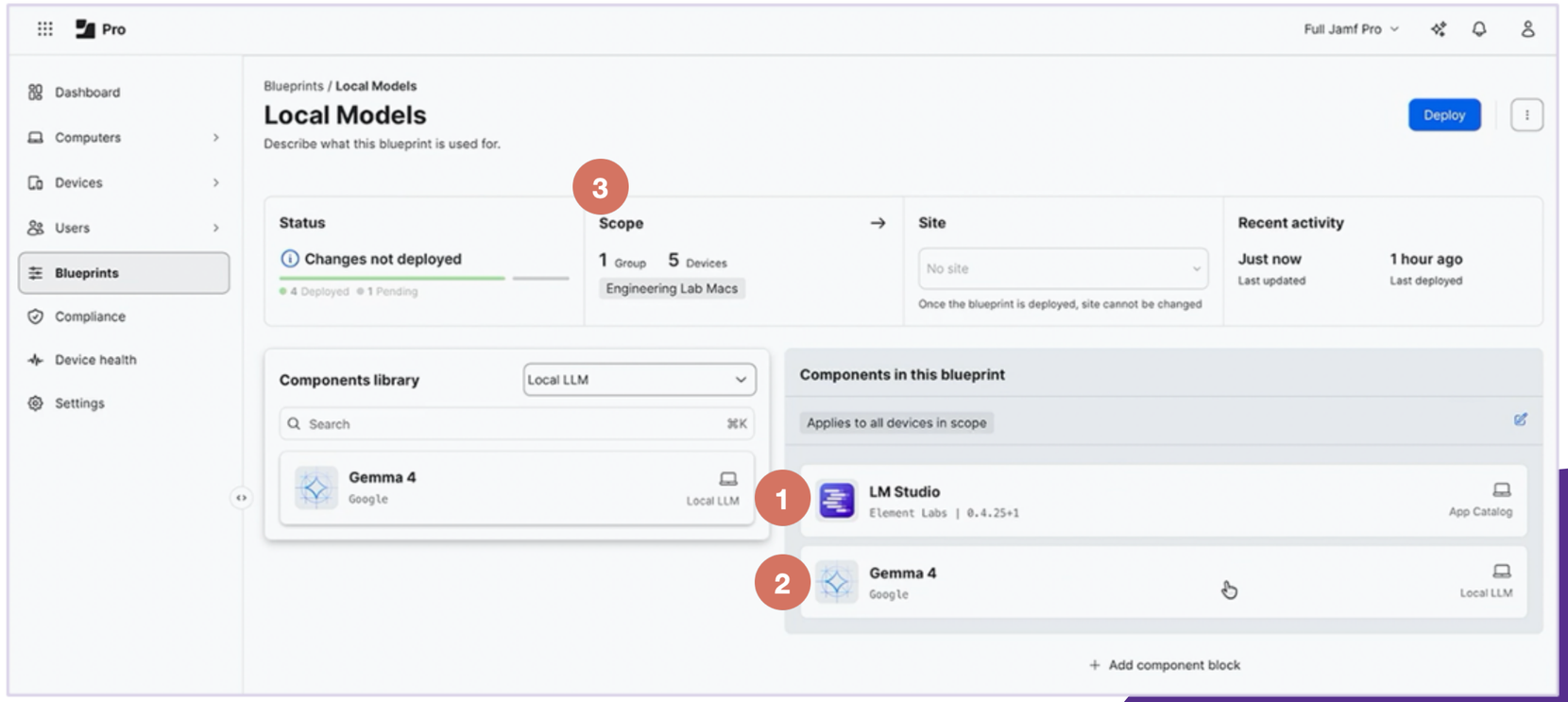
2026 GA目標

Mac上でAIを動かす選択肢も、MDMで

1. ローカルでAIを動かすアプリ配布
2. ローカルLLMを配布
3. 配布先をグループで指定

＋

AI ポリシーで、ツールをつなぐ



※GA目標は予告なく変更となる場合があります

ONE PLATFORM

セキュリティ × コスト × 投資対効果を、一元管理で



AIツールが増えるほど、一元管理の価値が増す

※GA目標は予告なく変更となる場合があります

あらためて考えるMDMの重要性

AIの時代こそ、**MDMが土台**になる

01

見える化・制御の前提

管理されたMacでなければ、見える化も制御も届かない

02

統制の設定を届ける

AI ポリシーを、ブループリントで確実に届け、利用者に変更させない

03

AIそのものを届ける

AIの実行アプリもローカルLLMもブループリントで配る

2026 GA目標

デバイスを管理するというMDMの基本が改めて重要になる

NEXT STEPS

今日からの3ステップ

Step 1

前提を整える

- 管理されたMacを土台に
- Jamf Account経由のSSO
- ブループリント
- Jamf Protect

Step 2

見える化を始める

Jamf Account

▼

AI ガバナンス

▼

AI Visibility

Step 3

次の可視化に備える

Step 1を今から着手していくと、適切なタイミングで、そのままブラウザやコストの可視化につながる

Jamf helps organizations

say **YES** to AI.

Q1 今、どれだけのAIが、どのように使われているか。説明できますか？

Q2 自社に最適なルールを自社で考え、システムと運用に反映できていると言えますか？