Jamf Nation Live Tokyo 2026

Jamfで始める、見える化からのAIガバナンス

2026年10月30日

株式会社Too Apple事業開発部　米光 慶

株式会社Too コーポレートIT部　大江 聖也

自己紹介



米光 慶（Apple事業開発部）

2013年からセールスエンジニアとして、スタートアップから大企業まで、幅広い規模の組織におけるAppleデバイスの導入・管理・運用を支援。2020年にJamf Integrator認定を取得し、350件以上のオンボーディングを担当。2026年にはJNUCへ初登壇するなど、Jamf製品の技術検証を通じてその知見の発信に取り組んでいる。



大江 聖也（コーポレートIT部）

コーポレートITおよび社内AI活用推進を担当。デバイス管理、ID基盤、セキュリティなどの実務にあわせ、生成AIの業務活用とガバナンス整備に取り組む。「使わせない」ためではなく、「安心して使える」ための仕組みづくりを模索している。

アジェンダ

1. AI利用の実態把握
2. AIガバナンスの判断軸
3. Jamfによる段階的な統制
4. 継続的な運用設計

第1章

AI利用の実態把握

1.1　AIの利用経路はひとつではない
1.2　AI利用の把握が難しかった理由
1.3　Jamf AI GovernanceによるAI利用の可視化
1.4　可視化されたAI利用の広がり
1.5　社内の認識と実態の差

1.1 AIの利用経路はひとつではない

.Too

組織が把握しているAI利用と、従業員の実際の利用は一致しているでしょうか。

ブラウザ

チャットでのやりとりをベースに、質問への回答や文章・ファイルの生成などに利用

デスクトップアプリ

ローカルファイルの参照や他アプリとの連携など、デバイス上の作業と組み合わせて利用

CLI

ターミナルから指示し、リポジトリの調査やファイルの編集、コマンドの実行などに利用

IDE拡張

開発環境内で編集中のコードを参照し、コードの補完や修正、質問への回答などに利用

従業員は、複数の経路を用いて生成AIを業務利用しています。

1.2 AI利用の把握が難しかった理由

利用経路の分散

- 同じAIサービスでも利用経路（ブラウザ、アプリ、CLI、IDE拡張）によって管理方法が異なる
- どの部門、デバイスでなにが使われているかを横断して把握しにくい

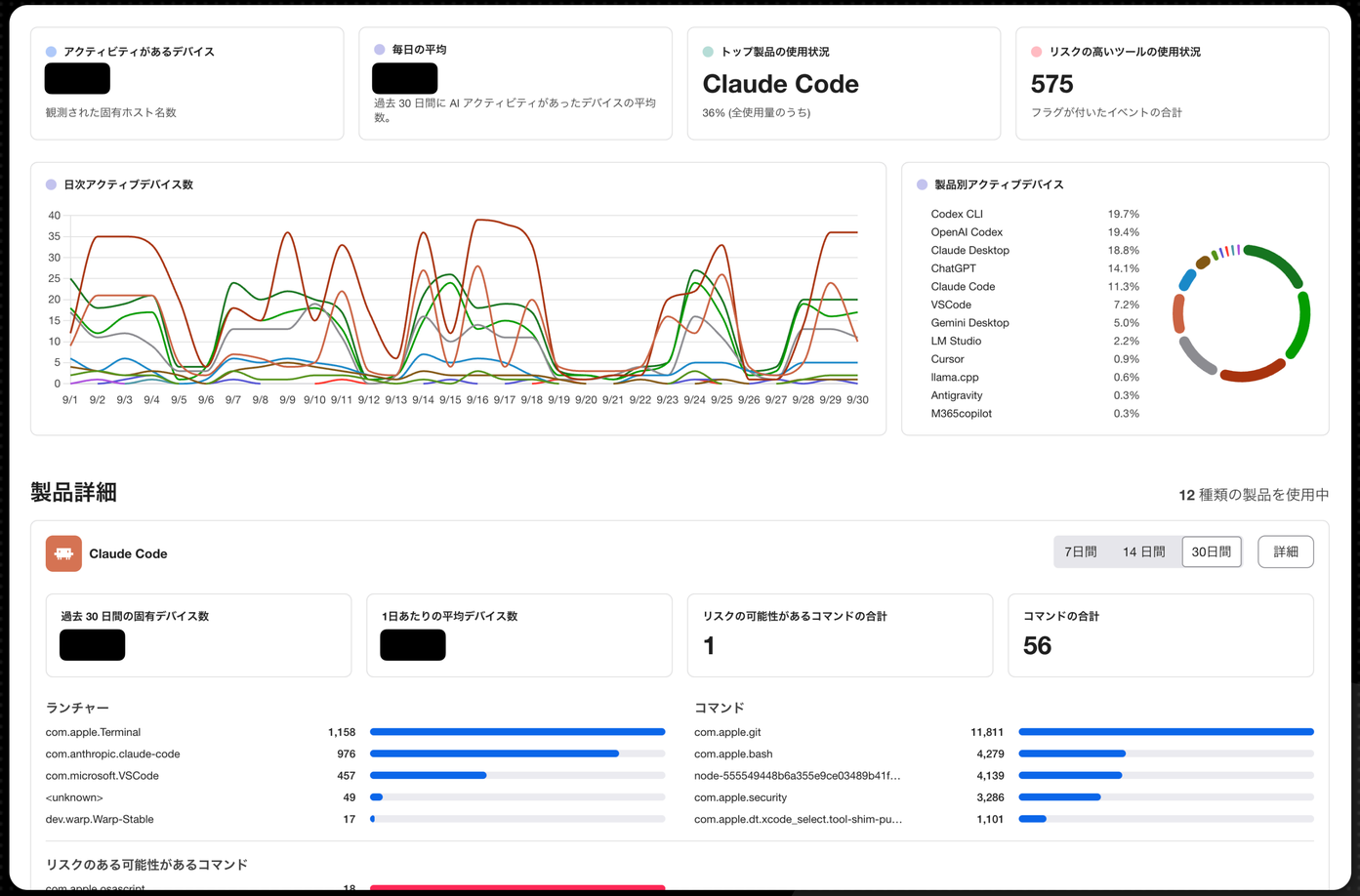
契約・アカウントの混在

- 有償／無償プラン、組織／個人アカウントが混在し、利用条件や管理できる範囲が異なる
- 組織契約があっても、個人契約で利用されている可能性がある

まずは社内のAI利用の実態を把握し、
その結果をもとにルールや管理方法の見直しにつなげます。

1.3 Jamf AI GovernanceによるAI利用の可視化

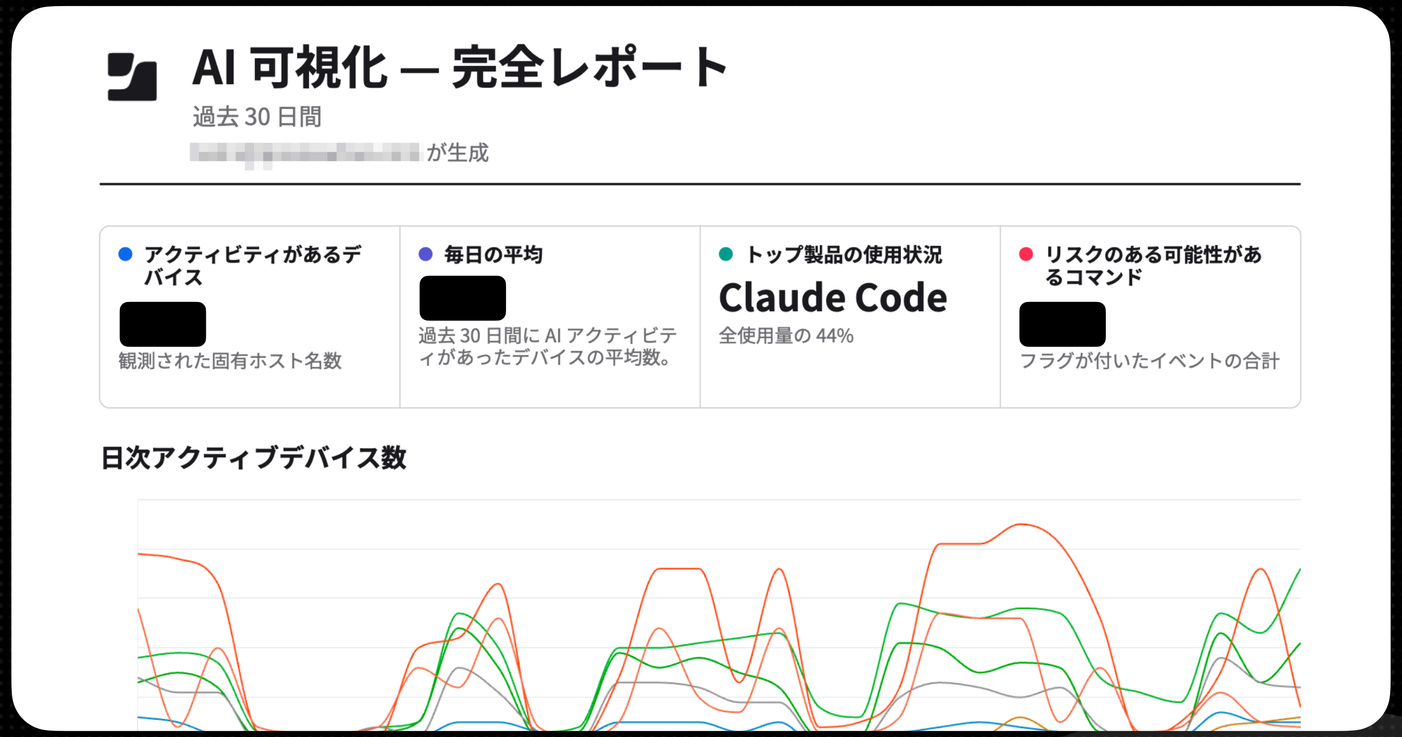
- 2026年8月12日に本番環境でAI Governanceを有効化
- 社内Mac上のAIツール利用状況を確認
- 製品別の利用状況や実行されたコマンドなどのアクティビティを確認
- 運用判断に使える情報と、追加確認が必要な情報を切り分け



1.4 可視化されたAI利用の広がり

約50%

Jamf Proで管理する社内Macのうち、
AI Governance上で直近30日間にAI関連の
アクティビティが確認されたデバイスの割合

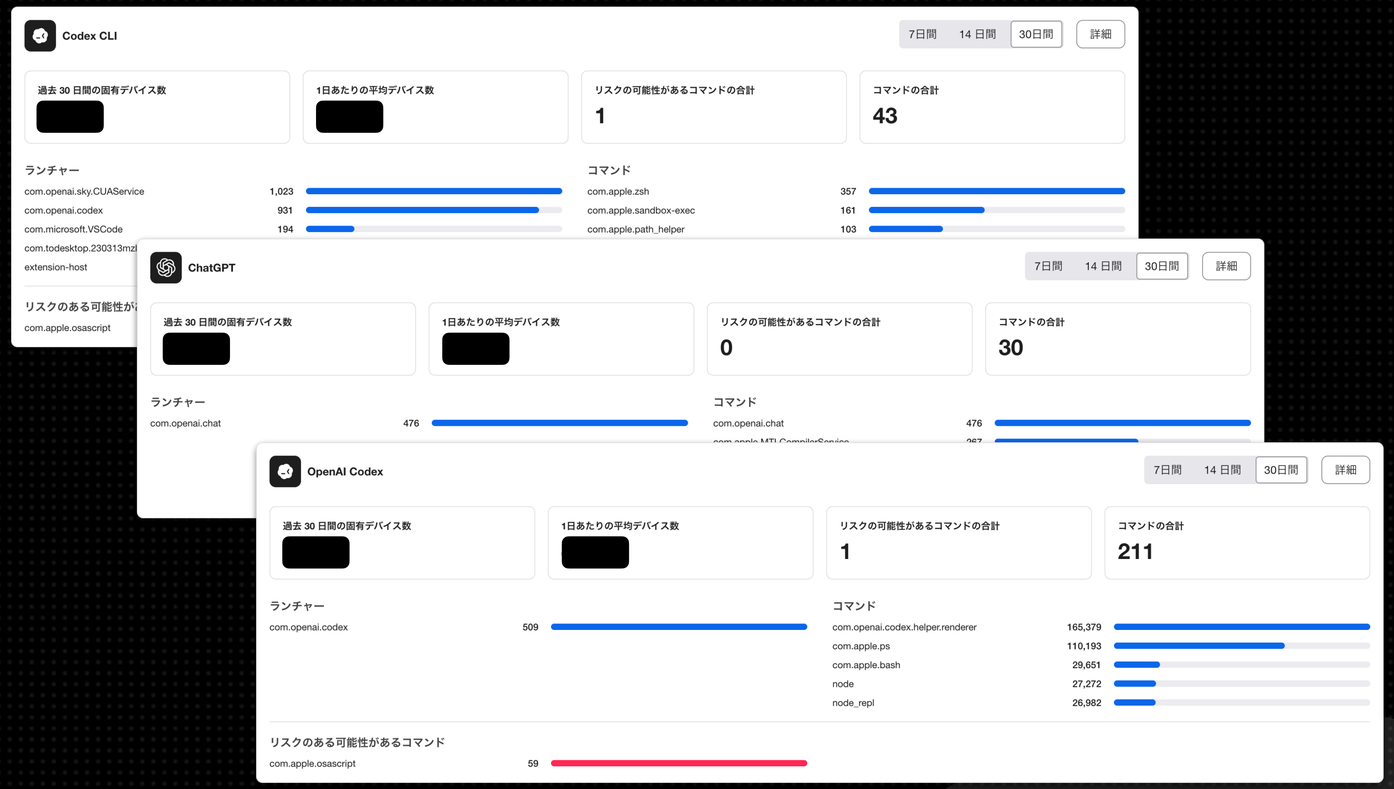


(⚠️注釈) 確認できたデータに基づく割合であり、AIツール利用の深さやすべての業務利用を示すものではありません。

利用実態の可視化は統制だけでなく、
AIの利活用をさらに推進するための判断材料にもなります。

1.5 社内の認識と実態の差

- 利用を許可していたAIツール以外のアクティビティも確認
- 用途をすぐに判断できないアプリやアクティビティも存在
- 同じAIツールでも利用経路によって見え方が異なるケースも確認



把握できていなかった利用を確認できた一方、
可視化した情報だけでは利用目的やその適否までは判断できませんでした。

第2章

AIガバナンスの判断軸

2.1　可視化できる情報と判断に必要な文脈

2.2　統制と推進の課題

2.3　基準となる考え方

2.4　AIガバナンスで考慮する要素

2.1 可視化できる情報と判断に必要な文脈

可視化できる情報

- AIツール名
- アクティビティ
  起動元や実行されたコマンド
- 利用デバイス
  Jamf Proのインベントリと組み合わせて確認

＋

判断に必要な文脈

- 利用目的
- 組織・個人アカウント
- 権限とアクセス先
- 社内での承認状況

機密情報や強い権限にアクセスしていればリスクは高くなるため、
利用回数だけではリスクの高さを判断できません。

2.2 統制と推進の課題

統制の課題

- 未把握の利用について、用途やアカウントを確認する必要がある
- 承認・条件付き利用・制限の判断基準が必要

推進の課題

- 利用実態をもとに、活用を広げる対象や必要な支援を検討
- 安全に使えるアカウントや利用方法を整える必要がある

未把握の利用を減らし、安心して使えるアカウントや利用方法の整備が、統制と利活用の両立につながります。

2.3 基準となる考え方

統制と推進について一貫した判断を行うには、組織として基準となる考え方が必要です。
そこで、AIに関連するリスクを継続的に管理するためのフレームワークである**NIST AI RMF**を参照します。

GOVERN (統治)

- 方針、責任、判断基準を定め、ほかの3指針を通して組織の運用を支える

MAP (マップ)

- 利用目的、利用者、データ、影響範囲など判断に必要な文脈を捉える

MEASURE (測定)

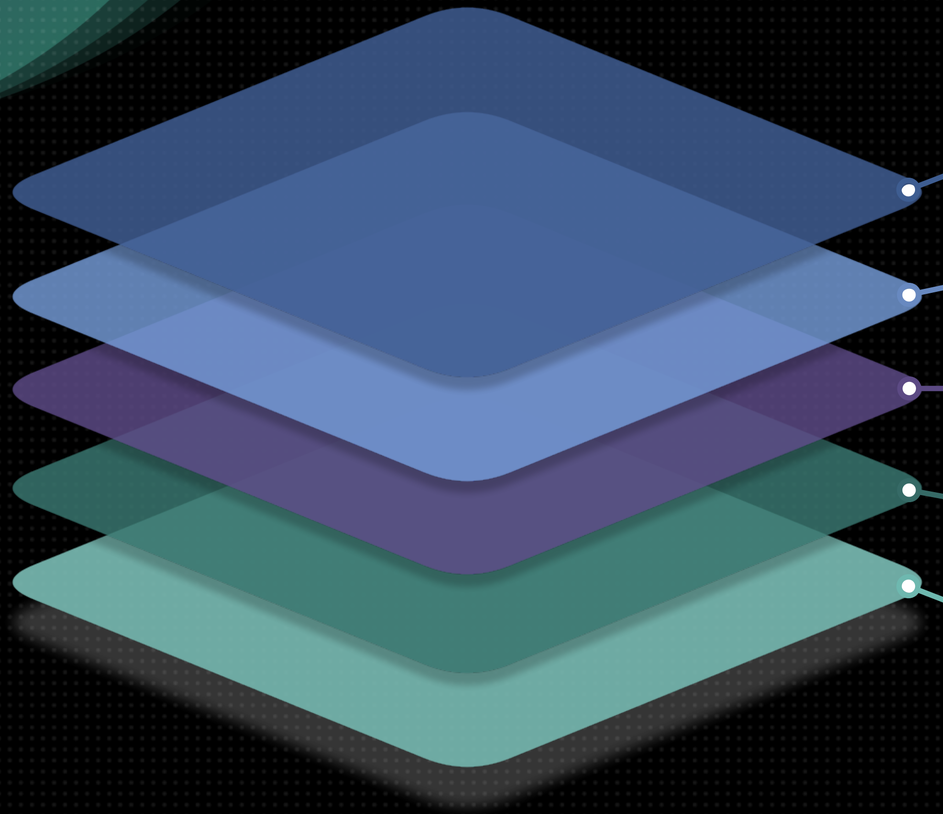
- 特定したリスクや既存の統制が機能しているかを評価・追跡する

MANAGE (管理)

- 優先順位に応じて対応方法を選ぶ
- 実施後も監視し、改善する

次のページではNIST AI RMFが示すリスク管理のプロセスを、5つの実装領域に分けて整理します。

2.4 AIガバナンスで考慮する要素



ルール・契約
利用条件と申請・承認手順

ID・アカウント
組織アカウントとアクセス管理

AIツールの設定
モデル、コマンド、外部連携の制御

デバイス・ネットワーク
アプリ実行とWebアクセスの制御

運用
定期確認、例外対応、方針更新

プロセスと実装領域を分けることで、可視化だけでは足りない部分と、Jamfが担える範囲を整理します。

第3章

Jamfによる段階的な統制

3.1　Jamfが担う領域
3.2　承認する利用条件の適用（Claude Code）
3.3　ポリシーの限定適用と検証
3.4　評価中のツールの一時制限（ChatGPT Atlas）
3.5　アプリ単位から、機能単位の制御へ

3.1 Jamfが担う領域

Jamf AI Governance

- 利用実態の可視化
- AIツール別・期間別の確認
- 統制対象を検討する材料

Jamf Pro

- 承認済みAIツールへの設定適用
- 検証対象を限定した展開
- 段階的な適用範囲の拡大

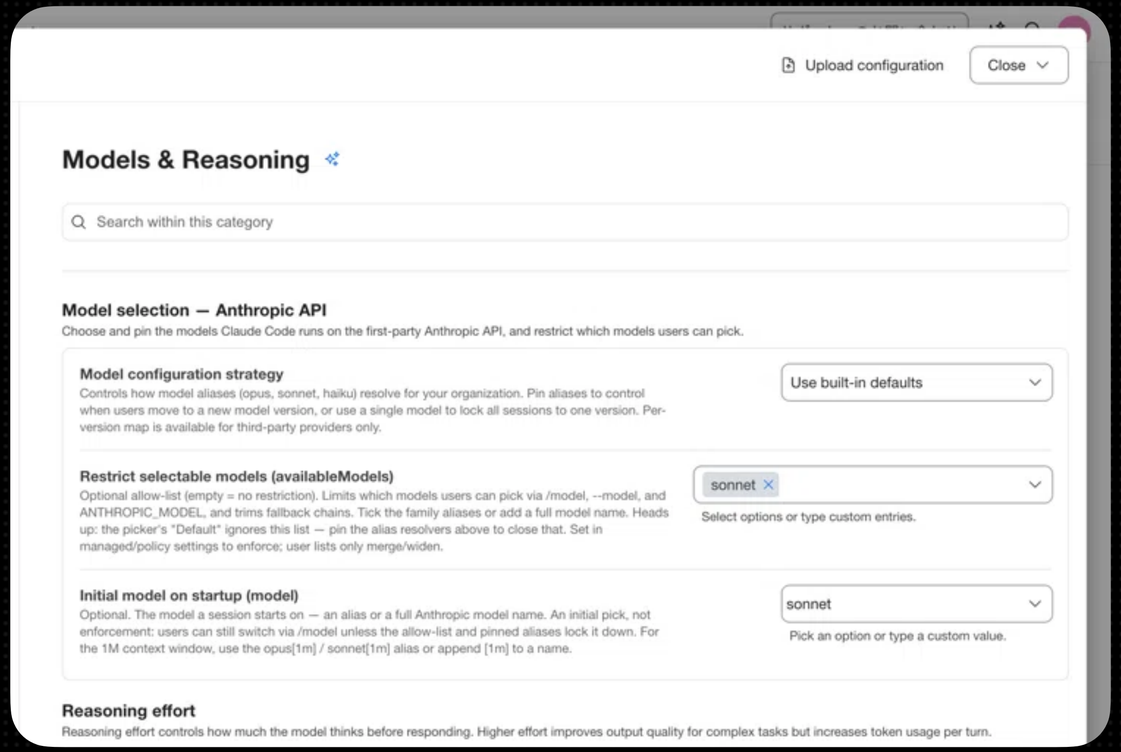
Jamf Protect

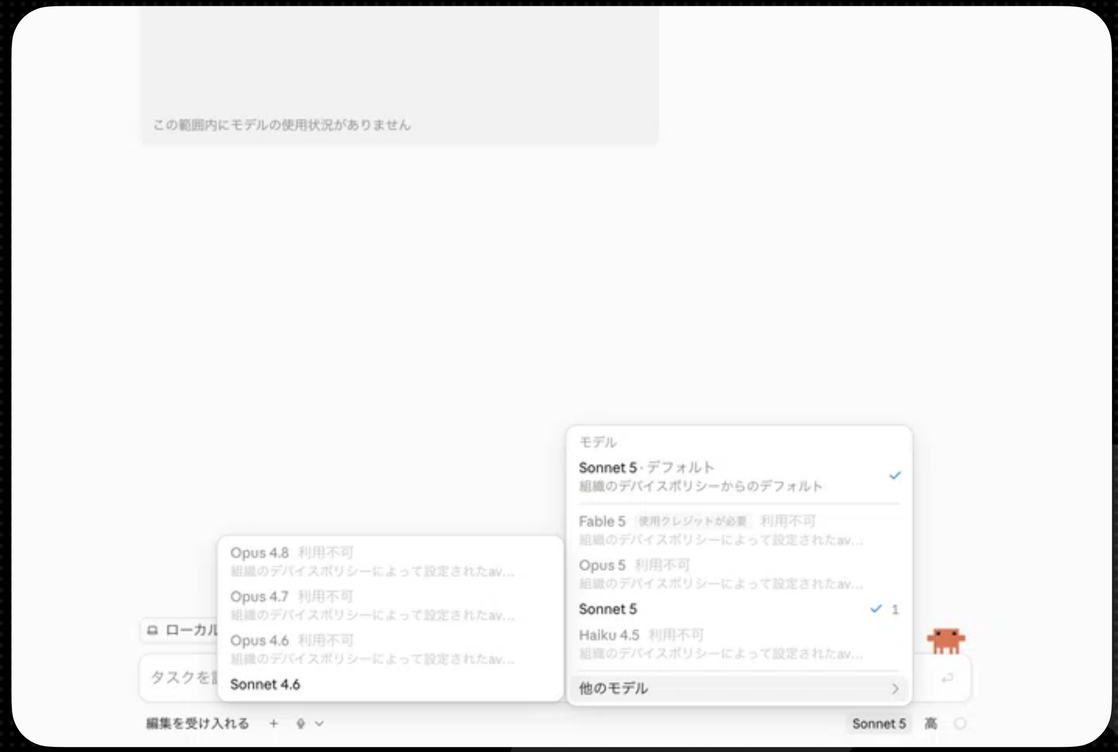
- 未承認アプリの実行制限
- Webアクセスの制御
- デバイス上の脅威への対応

本章では、承認する利用条件の適用と評価中のツールの一時制限を、限定した対象から確認していきます。

3.2 承認する利用条件の適用（Claude Code）

1. **対象**
   Claude Code
2. **設定**
   モデル制限
3. **適用**
   Blueprint配布
4. **確認**
   モデル選択





3.3 ポリシーの限定適用と検証

3.2で作成したポリシーを、限定した対象へ適用して検証します。



検証対象へ適用

Claude Codeのモデル制限を
検証対象へ配布



設定と業務影響を確認

指定したモデルだけを利用可能か
必要な業務を継続できるか



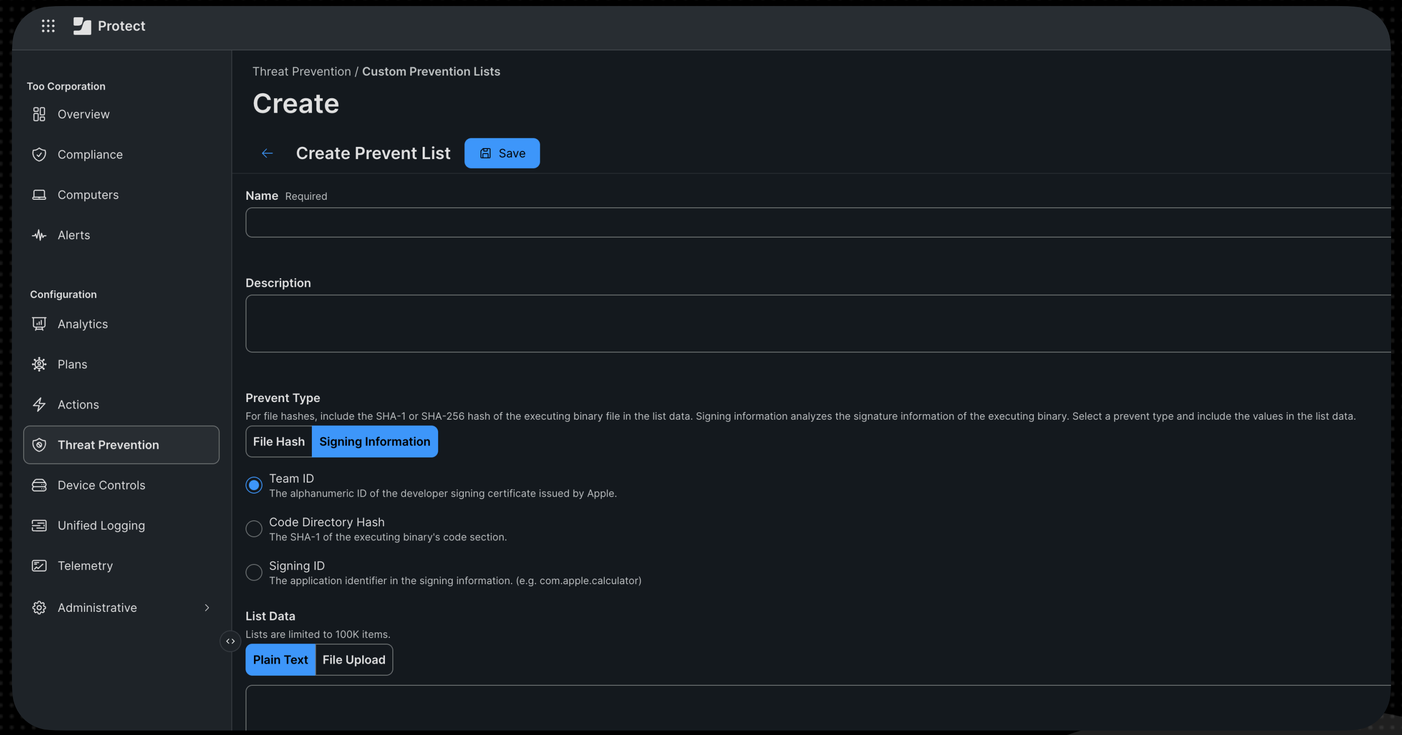
適用条件を整理して拡大

利用者と用途に必要なモデルを整理
適用する対象を段階的に拡大

**限定した対象で設定の挙動と業務への影響を確認し、
問題がない範囲から適用を広げます。**

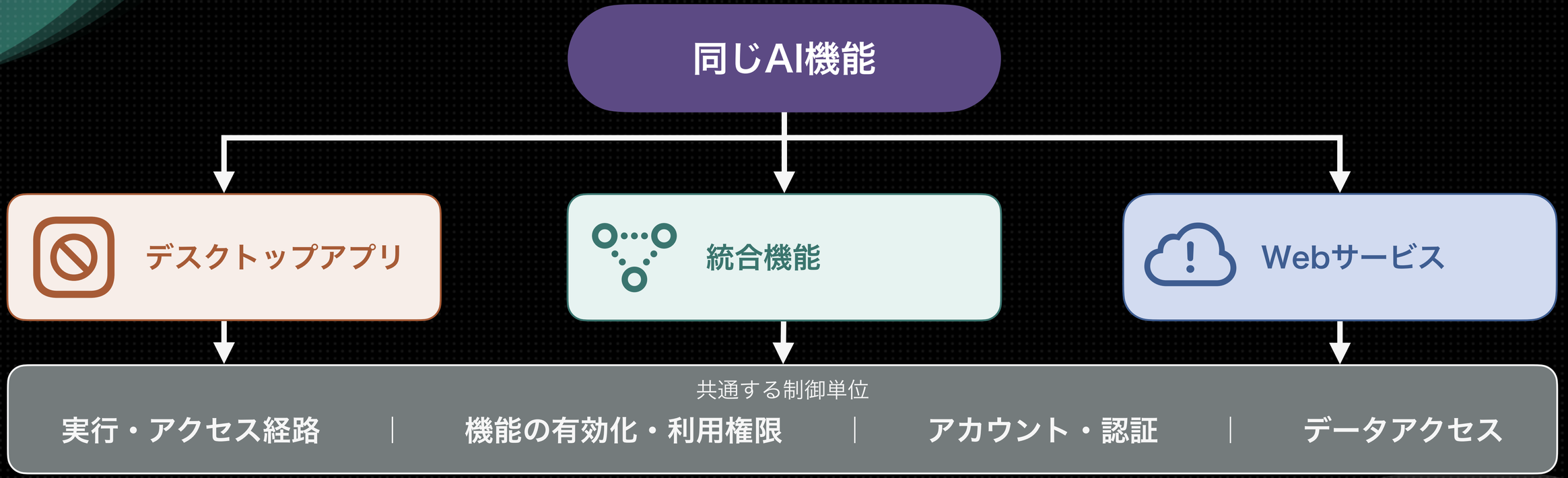
3.4 評価中のツールの一時制限（ChatGPT Atlas）

- 新しい機能・利用形態について、社内利用上のリスクを評価
- Jamf Protectで、評価完了まで対象アプリの実行を一時的に制限
- Custom Prevention Listによるブロック状態を確認



新しい利用形態は経路やデータアクセスを確認するまで一時的に制限し、確認後に扱いを判断します。

3.5 アプリ単位から、機能単位の制御へ



アプリを止めることとサービス全体を使わせないことは別です。
上記を制御単位とし、機能追加や統合に合わせて判断基準を見直します。

第4章

継続的な運用設計

4.1　AI Governanceの新機能

4.2　ブラウザ利用の制御（Browser Insights）

4.3　モデル利用とコスト（Model Insights）

4.4　デバイス単位の調査（AI Activity Insights）

4.5　運用開始前に整えること

4.6　可視化を起点とした運用サイクル

4.7　まとめ

4.1 AI Governanceの新機能

JNUC 2026で発表されたアップデートによって、ブラウザ上の操作やモデル別の利用量、検知された活動の詳細がAI Governanceの判断材料に加わります。

Browser Insights

- ブラウザでのAI利用と個人AIアカウントを可視化
- ポリシーに反する操作 (ファイルのアップロードなど) をブラウザ上でブロック

Model Insights

- 利用者・デバイス・AIツール・モデル・プロバイダ別に利用状況を可視化
- トークン利用量と公開価格から推定コストを表示
- プロンプトと回答は取得しない

AI Activity Insights

- フラグが付いたAIアクティビティを起点に調査
- デバイス・利用者を確認し、コマンドラインまで掘り下げて確認

4.2 ブラウザ利用の制御（Browser Insights）

組織アカウントでの利用を認めながら、個人アカウントへのファイル送信を制御できるか

現在の対応

Jamf Security Cloud

- AIサービス全体のドメインを許可／遮断

AIサービス側の管理

- SSOや組織アカウントの利用を設定

残る差分

- 同じサービス内で、個人・組織アカウントを区別しにくい
- 閲覧を許可しながら、ファイル送信だけを制限しにくい

運用で変わること

- 組織アカウントでの利用は継続しながら、個人アカウントへのファイル送信などをブラウザ上でブロック
- 利用者には通知にて理由を表示

ドメイン単位の制御から、アカウントと操作を踏まえた制御へ広がります。

4.3 モデル利用とコスト（Model Insights）

誰が、どのAIツール・モデルを、どの程度利用しているか

現在の対応

Jamf AI Governance

- AI Visibilityで利用ツールを確認
- Jamf Proのデバイス情報と照合

AIサービス側

- 管理画面やAPIで利用量と費用を確認

残る差分

- サービスごとに取得項目や粒度が異なる
- 利用者、デバイス、ツール／モデルの関係を手作業で照合

運用で変わること

- 利用量と推定コストを、利用者・デバイス・ツール／モデルの同じ軸で比較
- 組織アカウントや利用モデルの整理、契約・推進・統制の検討材料として活用

利用の有無だけでなく、
誰がどのモデルをどの程度使っているかを判断材料にします。

4.4 デバイス単位の調査（AI Activity Insights）

検知されたAIアクティビティを、どのデバイスで、誰が、どのように実行したか

現在の対応

1. **AI Visibility:** 製品と期間を確認
2. **Jamf Pro:** デバイスと設定を確認
3. **Jamf Protect:** 必要に応じて実行イベントを確認
4. **社内確認:** 用途とアカウント情報を補完

残る差分

- 複数の画面やログをまたいで照合
- 検知から利用者・デバイス・コマンドまでがひと続きになっていない

運用で変わること

- 利用量と推定コストを、利用者・デバイス・ツール／モデルの同じ軸で比較
- 組織アカウントや利用モデルの整理、契約・推進・統制の検討材料として活用

技術情報の調査を短縮し、利用目的や承認状況の確認へ繋げます。

4.5 運用開始前に整えること

新機能によって判断材料は増えます。 運用へ組み込む前に、次の4項目を整理します。

アカウントの区分

- 組織・個人・未承認をどう扱うか

利用者・デバイスの紐付け

- 誰が、どのデバイスで利用しているか

許可する操作と判断基準

- アカウント、モデル、ファイル操作の許可範囲

責任者と対応フロー

- 誰が判断するか
- 調査・制限までの流れ
- 見直しのタイミング

機能を有効にするだけでなく、見えた情報を誰がどう判断し、対応するかを先に決めます。

4.6 可視化を起点とした運用サイクル

.Too

1 利用状況を把握	2 利用の文脈を確認	3 利用区分を判断	4 ポリシーを適用	5 変化を確認し見直す
AI Visibility Browser Insights Model Insights	AI Activity Insights 社内確認	ルール・契約	AI Policies Jamf Pro Jamf Protect	定期レビュー
AIツール、ブラウザ、利用量を確認	デバイス、利用者、コマンドと利用目的を確認	承認済み、条件付き、検証中、利用制限に区分	区分に応じて設定や制限を適用	利用状況、コスト、サービスの変化を確認

把握・確認・判断・適用・見直しを一度で終わらせず、
AIサービスと社内の利用状況の変化に合わせて繰り返します。

4.7 まとめ

利用実態を可視化する

- 想定外の利用を把握し、活用を広げる余地を捉えます。

利用の文脈を確認する

- 利用目的、アカウント、権限、データアクセスを確認して判断します。

段階的に適用し、見直す

- 対象と業務影響に応じて制御します。利用状況の変化に合わせて見直します。

AIガバナンスは、見える化を起点に、判断と改善を続けていく運用です。