AI アシスタント
セキュリティ技術文書

発行：2026年4月 | 配布方法：一般公開

概要

Jamf AI アシスタントは、AWS Bedrockを通じてClaude（Anthropic社）を活用する、Jamf Pro、Jamf Account、Jamf Protectに統合された会話型インターフェースです。インベントリクエリ、構成分析、コンプライアンスチェック、ナレッジ検索といった実用的なツールを備えています。

本ドキュメントでは、すべてのJamf Cloud地域（米国、EU、アジア太平洋地域）におけるAI アシスタントの運用に適用されるセキュリティアーキテクチャ、データの取り扱い、およびプライバシー制御について説明します。

AI アシスタントは4つのセキュリティ原則に基づいて構築されており、ポリシーやプロンプトレイヤーではなくアーキテクチャレベルで強制的に適用されます。その4つとは、「デフォルトで無効化」、「最小権限アクセス制御」、「APIレイヤーでの読み取り専用の強制」、「透明性が高く根拠が特定可能な回答です。AWS Bedrock Guardrailsにより、すべての環境においてコンテンツ監視とプロンプトインジェクション検出が行われます。

アーキテクチャの概要

インフラストラクチャ

AI アシスタントは、すべてのJamf Cloud地域に展開されています。顧客データはJamf環境がホストされている地域内で処理され、地域の境界を越えて転送されることはありません。

地域	AWS Bedrockリージョン	ステータス
アメリカ合衆国	us-east-1	本番運用中
欧州連合	eu-central-1	本番運用中
アジア太平洋地域	ap-northeast-1	本番運用中

モデル

AI アシスタントは、AWS Bedrockを通じてアクセスするClaude（Anthropic社）を使用しています。Bedrockは、Jamfのインフラストラクチャと Anthropicのモデルとの間で機能する推論レイヤーです。最新のモデルバージョンについては、Jamf Learning Hubをご覧ください。

サブプロセッサとしてのAnthropicとの関係：Anthropicが顧客データを受け取ったりアクセスしたりすることはありません。モデルの推論は、JamfのAWS環境内で稼働するAWS Bedrockのインフラストラクチャで行われます。お客様からのクエリ、ツールの実行結果、会話のコンテキストはBedrock内で処理され、Anthropicに送信されることはありません。AWS Bedrockによるデータプライバシーとセキュリティの取り扱いに関する詳細については、AWS Bedrockのデータ保護に関するドキュメントをご覧ください。

AWS Bedrockのセキュリティ特性：

- 顧客データは、Anthropicのモデルのトレーニングやファインチューニングには使用されない
- データはリージョン内で処理され、顧客の環境がホストされているAWSリージョンから外部に出ることはない
- SOC 2 Type IIに準拠している
- すべての推論リクエストに、AWSの企業向けセキュリティ対策が適用される

モデルの更新：JamfはAWS Bedrockを通じてモデルのバージョンを管理しています。最新のモデルバージョンはJamf Learning Hubで公開されています。変更管理の要件がある場合は、Jamf Learning Hubに随時アクセスしてモデルバージョンの変更を確認してください。

ツールのアーキテクチャ

AI アシスタントはツール呼び出しアーキテクチャを採用しています。ユーザがクエリを送信すると、モデルは呼び出すべきツールを判断し、ユーザの既存の権限を使用して特定のJamf APIに対してツールを実行し、結果を統合して回答を生成します。

ツールが実行する機能はすべて読み取りのみです。AI アシスタントツールは5つのカテゴリに分類されます。その5つとは、ナレッジ検索（Jamfのドキュメントやナレッジベース）、構成へのアクセス（ポリシー、プロファイル、スクリプト、ブループリントなど）、インベントリクエリ

（Macデバイスやモバイルデバイスのデータ）、コンプライアンスチェック（CIS、NIST、DoD STIGなどのベンチマーク評価）、セキュリティインテリジェンス（モバイルアプリのリスク評価）です。Jamf Protectのツール（アラート分析、マルウェア照会）は、限定ベータ版として提供されています。提供状況や製品要件を含む最新のツール一覧については、Jamf Learning Hubをご覧ください。

サードパーティデータのフロー：3つのツールが、Jamfのインフラストラクチャ外にある外部サービスに対してクエリを実行します。透明性を確保するために、これらのツールの連携について公開されています。

- **Apple OS Lookupは**、Appleの公開エンドポイントであるApple Global Device Management Framework（GDMF）API（gdmf.apple.com）に対してクエリを実行します。顧客データが送信されることはありません。このツールは、公開されているApple OSのリリース情報のみを取得します。
- **App Lookupは**、アプリケーションのバージョンとパッチの情報を取得するための代替データソースとしてiTunes Search API（itunes.apple.com）に対してクエリを実行します。顧客データが送信されることはありません。このツールは、公開されているアプリのメタデータのみを取得します。
- **Mobile App Riskは**、NowSecureのMARI（Mobile Application Risk Intelligence）データベースに対してクエリを実行し、セキュリティ評価情報を取得します。送信されるデータは、アプリケーションのストア識別子（iOSのバンドルIDなど）とプラットフォーム（iOSまたはAndroid）のみです。デバイスデータ、ユーザのアイデンティティ、組織情報が送信されることはありません。

セキュリティ設計の原則

デフォルトで無効化：AI アシスタントは、管理者がJamf Accountで明示的に有効化するまで、すべての組織で無効化されています。個々のツールグループは個別に有効化する必要があります。AI アシスタントコアを有効化しても、Jamf Proのツールや将来の製品統合機能が自動的に有効化されることはありません。組織が明示的に有効化を選択しない限り、ユーザはAI機能を利用できません。また、管理者はいつでも任意のツールグループを無効化できます。

最小権限アクセス制御：すべてのツールクエリは認証されたユーザの権限で実行され、既存のJamf ProのRBAC制御をそのまま継承します。AI アシスタントが権限を昇格させたり、ユーザが直接アクセスできないデータにアクセスしたりすることはありません。ポリシーの閲覧権限を持たないユーザは、AI アシスタントを介してもポリシーを取得することはできません。

APIレイヤーでの読み取り専用の強制：AI アシスタントは認証されたユーザのセッショントークンを使用してJamf Pro APIを呼び出します。昇格された認証情報を持つサービスアカウントが別途使用されることはありません。AI アシスタントのツールが発行するAPI呼び出しはすべてGETリクエストです。システム内のどのツールも、Jamf Proに対してPOST、PUT、PATCH、DELETEのリクエストを発行することはありません。これは実装レイヤーで強制的に適用されるアーキテクチャ上の制約であり、巧妙なプロンプト入力によって回避できるような、プロンプトレイヤーの指示やポリシーではありません。クエリがどのように構成されているかにかかわらず、AI アシスタントがデバイス構成の変更、ポリシーの展開、アプリケーションの削除、登録状態の変更を行うことはできません。

透明性が高く根拠が特定可能な回答：すべての回答でソースが明示されるため、管理者は信頼できるドキュメントと照らし合わせて回答を検証できます。ツールからモデルに返される結果は自由形式のテキストではなく構造化データなので、すべての回答でソースを追跡できます。

Bedrock Guardrails：すべてのAI アシスタント環境にAWS Bedrock Guardrailsが導入されています。このガードレールの設定には、暴力、性的コンテンツ、ヘイトスピーチ、侮辱、不正行為といった複数の有害カテゴリに対するコンテンツ監視と高感度のプロンプトインジェクション検出が含まれています。すべてのガードレールイベントは追跡・記録され、フラグが立てられた入出力に関する詳細な監査ログが残ります。

データの取り扱い

データフロー

ユーザがクエリを送信すると、以下の手順で処理が行われます。

1. **クエリの処理：**ユーザからの自然言語によるクエリが、AI アシスタントのバックエンドで受信される
2. **ツールの実行：**関連ツールが、認証されたユーザの権限を使用してJamf APIに対してクエリを実行する
3. **コンテキストの構築：**ユーザのクエリ、関連ツールの実行結果、現在の会話スレッドで推論の準備が整えられる
4. **モデルの推論：**AWS Bedrockによって推論リクエストが処理され、回答が生成される
5. **回答の提示：**生成された回答が、Jamfのインターフェースでユーザに返される

推論中に処理されるデータ

データタイプ	推論レイヤーによる処理の有無	備考
ユーザのクエリ	はい	送信されたままの自然言語による質問
ツールの実行結果	はい	クエリに関連するインベントリデータ、構成の詳細
会話の履歴	はい	永続ストレージから読み込まれた、現在の会話の詳細なスレッド履歴。30日間保持
ユーザの認証情報またはトークン	いいえ	モデルのコンテキストに含まれることはない
データベースの全内容	いいえ	クエリに関連する結果のみが含まれる

データの格納場所

AI アシスタントは、Jamfの地域のデータ境界を遵守します。推論リクエストは、お客様のJamf環境と同じ地域にあるAWS Bedrockのデプロイメントにルーティングされます。

- **米国のお客様：**データはAWS us-east-1で処理されます。
- **EUのお客様：**データはAWS eu-central-1で処理されます。
- **アジア太平洋地域のお客様：**データはAWS ap-northeast-1で処理されます。

デバイスインベントリ、構成データ、その他のお客様固有のデータが地域間で転送されることはありません。

ナレッジ検索に関する注：ナレッジ検索はJamfのドキュメント一式のみを対象としており、デバイスインベントリ、構成の詳細、その他のお客様固有のデータにはアクセスしません。ナレッジ検索を含むAI アシスタントのすべてのクエリは、お客様に割り当てられた地域内で処理されます。

セッションの分離

AI アシスタントの各会話のスコープは、認証されたユーザとその組織に限定されます。会話のコンテキストがユーザ間や顧客組織間で共有されることはありません。ある組織からのクエリに、別の組織のインベントリデータや構成の詳細が表示されることはありません。

会話データは30日間保持された後、自動的かつ完全に削除されます。この保持期間はストレージレイヤーで適用され、遅延やスキップの可能性がある定期クリーンアップタスクではなく、DynamoDBのTTL（Time to Live）機能が使用されます。各会話にアクセスできるのは、その会話を作成したユーザと組織のみです。会話データはJamfのインフラストラクチャ内にのみ保存され、クエリや回答の内容が推論リクエストの範囲を超えてAWS BedrockやAnthropicによって記録・保持されることはありません。

データの保持と監査ログ

会話の内容は30日間保持されます。30日が経過すると、会話データは削除され、復元することはできません。

監査ログは、Jamf Accountの［アクティビティ履歴］→［AI アシスタント］で確認できます。監査ログには、次のような、AI アシスタントの設定に対するすべての管理的変更が記録されます。

- AI アシスタントの有効化または無効化
- ツールグループの追加、削除、更新

- 各変更を行った管理者のアイデンティティ（氏名とE メールアドレス）
- 各変更の日時

監査ログのエントリにアクセスできるのは、Jamf Accountの組織管理者の役割と管理者の役割を持つユーザです。監査ログは構成変更の包括的な記録を提供します。

データタイプ	保持期間	備考
会話の内容	30日間	自動的に削除され、復元はできない
監査ログ（構成の変更）	Jamf Accountの標準保持期間	Jamf Accountの［アクティビティ履歴］で閲覧できる
モデルの推論コンテキスト	セッションの範囲を超えて保持されることはない	セッション終了時に破棄される
モデルのトレーニング	対象外	AnthropicがAWS Bedrockの顧客データを使ってトレーニングすることはない

アクセス制御

認証

AI アシスタントは、認証されたユーザのJamfセッションを継承します。別途のログイン、API キー、認証情報は必要ありません。Jamf環境で認証されていないユーザは、AI アシスタントを利用できません。

AI アシスタントを有効化するには、Jamf Accountの管理者または組織管理者の役割が必要です。標準ユーザや役割が読み取り専用のユーザは、AI アシスタントのツールグループ設定を有効化、無効化、変更することはできません。管理者によるすべての変更は、アクティビティ履歴の監査ログに記録されます。

認可

すべてのツールクエリは、認証されたユーザの権限で実行されます。AI アシスタントが権限を昇格させたり、既存のJamf Proの役割ベースアクセス制御を回避したりすることはありません。

- インベントリクエリは、ユーザに閲覧権限があるデバイスのみを返します。
- 構成に関する説明の結果は、既存のオブジェクトレベルのアクセス制御を遵守します。

- コンプライアンスデータへのアクセスは、標準のJamf Pro RBACに従います。
- ポリシーへのアクセス権がないユーザは、AI アシスタントを介してもそのポリシーの詳細を取得することはできません。

AI アシスタントの有効化と無効化

AI アシスタントは、すべての組織でデフォルトで無効化されています。有効化は、管理者がJamf Accountの［組織］→［AI アシスタント］で明示的に行う必要があります。

AI アシスタントの無効化は即座に反映され、いつでも元に戻せます。管理者がJamf Accountの［Enable AI Assistant］（AI アシスタントを有効化する）チェックボックスをオフにすると、組織内のすべてのユーザに対してAI アシスタントのすべての機能が即座に無効化されます。また、AI アシスタントコアは無効化せずに、個々のツールグループ（Jamf Proの読み取り専用ツール）を無効化することもできます。

慎重に導入を進めたい組織は、環境レベルのスコープ設定を使用して、より細かく制御することができます。Jamf Proの読み取り専用ツールを有効化する際、管理者はすべての環境で一律に有効化するのではなく、特定の環境やテナントへのアクセスのみに制限することができます。これを利用して、本番環境に変更を加えることなく、サンドボックスやステージング環境にAI アシスタントを試験的に導入してから本番環境で有効化することができます。

製品別のツール提供状況

ツールの最新の提供状況、製品要件、ベータ版のステータスは、Jamf Learning Hubで公開されています。

コンプライアンス

AI アシスタントは、Jamfの既存のコンプライアンスプログラムの枠内で運用されます。Jamfの最新の認証一覧については、Jamf Trust Centerをご覧いただくか、アカウントチームまでお問い合わせください。

AWS Bedrockのコンプライアンス（推論レイヤーに適用）：

- SOC 2 Type II
- ISO 27001

FedRAMPおよびStateRAMP：AI アシスタントは、StateRAMPまたはFedRAMPの認証を受けた環境では利用できません。将来のFedRAMPおよびStateRAMPへの対応に関するロードマップの詳細については、Jamfのアカウントチームまでお問い合わせください。

ペネトレーションテスト：AI アシスタントは、Jamfのセキュリティ審査プログラムの一環としてペネトレーションテストを実施済みです。テスト結果は、お客様のご要望に応じて、NDAの締結を条件としてJamfのアカウントチームを通じて開示されます。

セキュリティ制御のまとめ

制御項目	実装方法
転送中データの暗号化	すべての通信にTLS 1.2以上を適用
保存データの暗号化	AWS KMSで暗号化
認証	Jamf Proのセッションを継承 — 別途の認証情報は不要
必要な管理者の役割	Jamf Accountの管理者または組織管理者
認可	すべてのツールクエリにJamf ProのRBACを強制適用 — 権限昇格なし
データの格納場所	地域ごとに処理 — 米国/EU/アジア太平洋、地域間の転送はなし
Anthropicによるデータアクセス	Anthropicは顧客データを受け取らない — 推論はAWS Bedrock内で完結
モデルのトレーニング	顧客データはモデルのトレーニングに使用されない（AWS Bedrock）
サードパーティのプロセッサ	NowSecure（アプリリスクインテリジェンス） — アプリの識別子のみ。Apple GDMF（OSバージョン） — 公開データのみ
監査ログ	構成の変更はJamf Accountの［アクティビティ履歴］に記録 — ユーザ、アクション、タイムスタンプごとに
会話の保持期間	30日間
読み取り専用の動作	実装レイヤーで強制適用 — Jamf Pro API呼び出しはすべてGETリクエストであり、ツールコード内に書き込みメソッドは存在しない

セッションの分離	会話のスコープは認証されたユーザと組織に限定 — 他のユーザや組織からはアクセス不可
デフォルトで無効化	管理者が明示的に有効化するまで、すべての組織で無効
無効化機能	即時に反映 — Jamf Accountで［Enable AI Assistant］（AI アシスタントを有効化する）チェックボックスをオフにする。いつでも元に戻せる
環境レベルのスコープ設定	導入を制御したい場合は、Jamf Proツールのスコープを特定の環境/テナントに限定可能
Webアプリケーションファイアウォール（WAF）	本番環境とステージング環境のAPIゲートウェイレイヤーに適用
Bedrock Guardrails	有害カテゴリに対するコンテンツ監視と高感度のプロンプトインジェクション検出を実施。すべてのイベントを追跡・記録
ペネトレーションテスト	GA前に実施済み。結果はNDAの締結を条件として開示

ドキュメント情報

発行	2026年4月
配布方法	一般公開
場所	jamf.it/aiassistant

詳細情報

- **Jamf Trust Center** — Jamfの最新の認証、コンプライアンスドキュメント、セキュリティ体制： https://www.jamf.com/ja/trust-center/
- **Jamf Learning Hub** — 最新のAI アシスタントツールカタログ、製品要件、モデルバージョン：https://learn.jamf.com/home
- **本ドキュメント** — この文書の最新版はこちらから入手できます：jamf.it/aiassistant
- **ご質問がある場合は**、Jamfのアカウントチームまでお問い合わせください。