# □□□□□□□


- □□□□□□□□
- □□□□□
- SIM □□
- □□□□

# デバイスの概要

ダッシュボード → デバイス
でデバイスの行をクリックして、デバイスを開きます。ページタイトルには、デバイスの モデル
（利用可能な場合）と内部 **ID**が表示されます。

# 履歴データと現在の登録

デバイスに複数の登録がある場合、 Cerberus Enterprise
は読み取り専用の履歴レコードを表示できます。その場合、ページには 履歴データ
バナーと、現在の登録データに戻るためのボタンが表示されます。

# 上部のフィールド

上部のセクションには、デバイスの識別情報、割り当て、管理状態がまとめられています。一部のフィール
ドはプラットフォーム固有で、 Android または Apple デバイスにのみ表示されます。

- **ID**および モデル ：読み取り専用の識別子。
- ユーザー
  ：現在割り当てられているユーザー（存在する場合）を表示します。ユーザーメニューから
  ユーザーを開く または ユーザーを変更
  を実行できます。ユーザーが設定されていない場合は、ユーザーを割り当てることもできます。
- 管理モード および 所有権 ： UI ではツールチップ付きで表示されます。
- 状態 ：現在のデバイス状態 (アイコンとツールチップの詳細付き )。紛失モードのデバイスは、
  Android と Apple の両方で 紛失
  と表示され、ページ上部のバナーに次に行うべきことが表示されます。
- **ADE** プロファイル （ Apple のみ）：割り当てられた Automated Device Enrollment
  プロファイル（存在する場合）を表示し、開いたり変更したりできます。
- ポリシー
  ：割り当てられたポリシーを表示し、開いたり変更したり、ポリシーが設定されていない場合は割
  り当てたりできます。
- ポリシーのコンプライアンスステータス
  （ポリシーが割り当てられている場合）：デバイスがコンプライアンスに準拠しているかどうかを
  示します。
- ポリシーバージョン
  （ポリシーが割り当てられている場合）：デバイスに最新のポリシーバージョンが適用されている
  かどうかを示します。

Cerberus Enterprise アプリ (iPhone と iPad のみ): Cerberus がデバイスにインストールする
Cerberus Enterprise アプリの状態。 利用不可 (iOS または iPadOS が 18.4
より古い、会社デバイスにシリアル番号がない、または個人デバイスに Managed Apple Account
がない); 個人デバイスではまだ利用できません ; デバイス情報を待機中 ; Managed Apple
Account のユーザー ライセンスを待機中 (個人デバイスで、 Apple
がライセンスを確認している間 ); 未インストール (アプリが Apple Business
ライブラリにない、または Apps and Books が設定されていない。 アカウント設定
へのリンク付き ); インストール済み · Apps and Books の対応が必要 (
トークンが期限切れ、またはアプリがライブラリから削除された。アプリはインストールされたま
ま); 構成を利用できません ; インストール中 … (デバイスが 30 分間ステータス
レポートを送信しない場合、ツールチップにデバイスがオンラインであることを確認して再起動す
るよう提案され、通常はインストールが再開されます ); ユーザーの承認を待機中 ;
ユーザーが拒否しました と インストールに失敗しました (どちらも 再試行
付きで、デバイスに再度要求します ); インストール済み · アプリの起動を待機中 (
アプリがまだ開かれていない ); インストール済み · 構成が受け入れられませんでした ;
および、アプリが登録されると、そのバージョン、最後の通信、通知がオンかどうか。
登録日 および 最終ステータスレポート ：登録と最後に報告されたステータスのタイムスタンプ。
登録解除日 ：デバイスの登録が解除されたときに表示されます。

一部のデータとパネルは、デバイスポリシーで対応するカテゴリが有効になっている場合にのみ利用

できます。詳細については、 ステータスレポート と位置情報とジオフェンス
のページを参照してください。

パネル
デバイス
ページは展開可能なセクションで構成されています。プラットフォームと状態に応じて、次のパネルのいず
れかまたは複数が表示されます :

位置情報マップ ：現在のデバイスの 位置情報 履歴と、 Android デバイス、 iPhone および iPad
ではジオフェンス遷移用の ジオフェンス タブを備えたタブ付きパネルです。
SIM 管理 ：デバイス EID とインストール済みの SIM および eSIM。Android ではさらに eSIM
コマンドとその履歴、会社所有の iPhone およびセルラー対応 iPad
ではさらにデータローミング、インターネット共有、 セルラープランを更新

も表示されます。専用の SIM 管理 ページを参照してください。
コマンド ：デバイスにコマンドを送信し、コマンド履歴を表示します（プラットフォーム固有）。
セキュリティ体制 : デバイスのセキュリティ状態とリスク。 Android では Play Integrity
の判定も含まれます。デバイスが報告するまでは 未指定 、セキュリティ
データをまだ送信していない Android デバイスでは まだ報告されていません と表示されます。
デバイスがコンプライアンスに違反している理由 :
デバイスがコンプライアンスに違反している場合にのみ、赤いアラート

アイコンとともに表示されます。開くと理由を確認できます。 Android では違反しているポリシー設定が一覧表示され、 Apple ではコンプライアンス
ルールがデバイスをブロックしたかどうかも表示されます。
デバイスステータス （Apple のみ）： OS
バージョン、ソフトウェアアップデートの進行状況、パスコード、 FileVault 、デバイスから報告されたバッテリーとアカウント、および利用可能な OS アップデート。

コマンド ページを参照してください。
アプリケーション (Android): インストールされているアプリとそのフィードバックおよびエラー
レポート。
アプリケーション （Apple
のみ）：ポリシーによってインストールされたアプリ、コマンドでインストールされたアプリ、ユ ーザーによってインストールされたアプリと、それらのインストール状態、エラー、アクション（
再試行、削除）。 Mac
では、ポリシーによってインストールされたパッケージも一覧表示され、その状態と
再インストール が表示されます。管理対象アプリとしてインストールされたパッケージには
管理対象
チップが付き、パッケージが管理対象外でインストールされた日時と理由、またはダウンロードか
ら 1時間後にアプリが見つからなかった場合に注記が表示されます。 iPhone および iPad では、
Cerberus Enterprise アプリに Cerberus によるインストール チップが付きます。このアプリは
ポリシー
フィルターには表示されません。デバイスが管理対象構成を受け入れなかったアプリには、
構成が受け入れられませんでした チップが付きます。個人所有の iPhone および iPad（User Enrollment）では、 App Store アプリのユーザーライセンスを使用する Managed Apple Account が 1行で表示され、ライセンスの付与を待機しているアプリには
ユーザーライセンスを待機しています または ユーザーライセンスに失敗しました
が表示され、ユーザーがインストールプロンプトをキャンセルしたアプリには
ユーザーによるインストールの承認を待機しています が表示され、 再リクエスト で Apple
にライセンスを再度要求するか、プロンプトを再度表示します。 コマンド
ページを参照してください。
プロファイル、証明書、セキュリティ （Apple
のみ）：デバイスから報告された構成プロファイル、証明書、セキュリティ状態。
インベントリの変更 （Apple
のみ）：デバイスでインストール、削除、更新されたアプリ、プロファイル、証明書のタイムライ

ン。種類と変更内容で検索・フィルタリングできます。 コマンド ページを参照してください。
Shared iPad ユーザー と Mac ユーザー (Apple のみ): Shared iPad のユーザーと Mac のユーザー。 コマンド ページを参照してください。
ステータスレポート
：デバイスから報告された追加データを、カテゴリと値のツリーとして表示します。
登録履歴 ：この同じ物理デバイスの以前の登録を一覧として表示します。

位置情報パネルのタブ

位置情報マップ パネルでは、タブを使用して位置情報履歴とジオフェンスの出入りを分けて表示します。

位置情報
：現在のデバイスの履歴フィルター、日付範囲検索、位置情報マーカー、精度サークル、ライブ追
跡コントロールを表示します。
ジオフェンス （Android、 iPhone、 iPad
）：専用のマップにジオフェンス遷移履歴を表示します。期間フィルター、アーカイブされたジオ
フェンスのオプションの切り替え、遷移のサイドリストがあります。 iPhone および iPad では、デバイスでジオフェンスが機能できない場合にステータス行にも表示されます。

これらのタブの完全な動作については、 位置情報マップ を参照してください。

アクション
ページの下部では、プラットフォーム、デバイスの状態、ライセンスの状態に応じて、データを更新したり
アクションを実行したりできます。

データを更新 ：デバイスレコードを再読み込みします。
デバイスを無効化 / デバイスを有効化 （Android
のみ）：サポートされている状態で使用できます。
デバイスの登録解除
：デバイスから管理を削除します。正確な動作はプラットフォームと所有権によって異なります（
たとえば、 Android
ではワークプロファイルのワイプまたは工場出荷時リセットが行われる場合があります）。
デバイスを削除
：デバイスがすでに登録解除されており、そのレコードを削除できる場合に使用できます。

位置マップ

このページでは、 デバイス概要
で利用できるデバイス固有の位置ツールについて説明します。パネルには、位置履歴用の 位置情報 タブと、 Android デバイス、 iPhone、 iPad ではジオフェンスの遷移用の ジオフェンス タブがあります。

前提条件
Android
では、デバイスの位置情報データは、デバイスポリシーで位置情報の報告が有効になっている場合にのみ表
示されます。有効にするには、ポリシーを開いて 位置情報とジオフェンス → 位置情報の報告

をオンにします。詳細については、 位置情報とジオフェンス を参照してください。

iPhone と iPad では、位置情報はユーザーが許可した後に Cerberus Enterprise アプリから取得されるか、デバイスが紛失モードのときに デバイスを特定 コマンドから取得されます。
Mac やその他の Apple デバイスは位置情報を報告しません。

完全には管理されていないデバイスでは、位置データは、 Cerberus Enterprise アプリに必要な位置情報の権限があるかどうか、およびデバイスで位置情報サービスが有効になって
いるかどうかにも依存する場合があります。

個人デバイス（ User Enrollment）では、 Apple ポリシーで
個人デバイスの位置情報とジオフェンス がオンになっており、ユーザーが Cerberus Enterprise
アプリの位置情報を許可している場合にのみ、位置情報とジオフェンスを利用できます。それ以外の
場合、デバイスページに位置情報アクションやライブ追跡は表示されません。紛失モードは個人デバ
イスでは利用できません。

ダッシュボードから利用できるグローバルな複数デバイスのマップについては、

ダッシュボードの位置マップ を参照してください。

読み込み中とデータなしの状態
位置データの読み込み中は、パネルのマップに読み込み中のオーバーレイが表示されます。

デバイスで利用可能な位置情報データがない場合、パネルには
利用可能な位置情報データがありません というメッセージが表示されます。 Android では、割り当てられたポリシーで位置情報の報告がオフになっている場合、有効にするよう促すメ
ッセージが追加されます。 Apple
では、位置情報の取得元、またはこの種類のデバイスが位置情報を報告しないことが表示されます
。
日付フィルターが有効で一致するサンプルがない場合、パネルには
選択した日付範囲に利用可能なデータがありません と表示されます。

位置情報タブ
位置情報 タブを開いて、 1
つのデバイスの履歴を確認します。利用可能なフィルターには、最後に確認された位置、最近の履歴範囲、
カスタム日付範囲、ライブ追跡があります。

最新 ：最後に確認された位置を表示します。
今日 、過去 7日間 、過去 30日間 ：選択した期間に記録された位置を表示します。
検索 ：カスタムの日付範囲を選択できます。
ライブ ：現在のデバイスのライブ追跡を開始または停止します。

位置情報は 90日間
保持され、それより古いものは毎晩自動的に削除されます。登録済みの各デバイスの最新の位置は常
に保持されるため、長期間報告していない場合でもデバイスはマップに表示され続けます。削除され
たデバイスと過去の登録については、 90日より古い位置情報はすべて削除されます。このため、 検索
の日付範囲を 90日より前から開始することはできません。

マーカーの詳細
位置マーカーをクリックすると、次の情報を含む情報ウィンドウが開きます：

位置情報レコードのタイムスタンプ。
報告された 精度 （メートル単位）。
デバイスが提供する場合に報告される 速度 。
デバイスが提供する場合に報告される 進行方向 または方位。

精度サークル

情報ウィンドウを開いている間、マーカーの周囲に精度サークルが表示されます。円の半径は、報告された
精度（メートル単位）に対応します。情報ウィンドウを閉じると、円は非表示になります。

ライブ追跡
デバイス履歴ビューで ライブ
フィルターを選択すると、その特定のデバイスのリアルタイム追跡リクエストが開始されます。 Cerberus Enterprise は、リクエストを開始する前に確認を求めます。

ライブ追跡は最大 15分間 実行されます。
ライブ追跡が有効な間、 Android デバイスでは通知が表示され、 iPhone および iPad
では位置情報インジケーターが表示されます。
ライブ追跡が有効な間、パネルは最新の位置情報を継続的に更新し、ライブインジケーターは表示
されたままになります。
ライブフィルターをもう一度選択すると、タイムアウトになる前にライブ追跡を停止できます。
iPhone および iPadでは、ライブ追跡は Cerberus Enterprise
アプリを通じて実行され、位置情報へのアクセスは 常に
に設定されています。このリクエストは通常、アプリが開いていない場合でもアプリを起動し、ア
プリはセッション全体にわたって位置情報を送信します。 iOS はこれらのリクエストを保証しません。たとえば低電力モードやネットワーク接続がない場合、リ
クエストが遅延したり、配信されないことがあります。 2 分以内に位置情報が届かない場合、ダッシュボードはリクエストをキャンセルします。ユーザーに
アプリを一度開いてから、もう一度試すよう依頼してください。

ジオフェンスタブ
Android デバイス、 iPhone および iPad では、 2 番目のタブに、割り当てられたポリシーで定義されたジオフェンスから生成されたジオフェンス遷移が表示
されます。

マップには、現在のジオフェンスエリアと記録された遷移ポイントが表示されます。
右側の遷移リストでは、 入場 および 退場 イベントを確認できます。
使用できるフィルターは、 今日 、過去 7日間 、過去 30日間
、およびカスタムの日付範囲検索です。
アーカイブを含める
では、現在のポリシーにもう存在しない古いジオフェンス定義に関連する遷移も表示されます。
ジオフェンスの遷移は 90日間
保持され、それより古いものは毎晩自動的に削除されるため、カスタム日付範囲の検索を 90 日より前から開始することはできません。

iPhone および iPad
では、ポリシーに有効なジオフェンスがある場合、タブ上部のステータス行に、デバイスでジオフェンスが
機能しているかどうかが表示されます。機能しない場合はその理由が示されます。 Cerberus Enterprise アプリがサーバーに接続していないか更新が必要である、位置情報へのアクセスが 常に
に設定されていない、 正確な位置情報 または App のバックグラウンド更新
がオフになっている、アプリが最後に設定を報告したときに 低電力モード
がオンになっていた（その場合、ジオフェンスイベントや変更が数時間遅れることがあります）、またはア
プリが最新のジオフェンスをまだ適用していない、といった場合です。すべてが正常に機能している場合は
、アプリが監視しているジオフェンスの数が表示されます。

ジオフェンス遷移の詳細
遷移を選択すると、マップ上でその詳細が開き、対応するリスト項目が強調表示されます。利用可能な場合
、 Cerberus Enterprise はその遷移のデバイス座標と報告された精度も表示します。

# SIM 管理

デバイス ページには **SIM** 管理 パネルがあります。 Android
デバイスでは、デバイスにインストールされている SIM と eSIM プロファイルを管理し、 eSIM
プロファイルを追加または削除し、デバイスに送信された eSIM コマンドの履歴を表示します。会社所有の
iPhone とセルラー iPad では、デバイスから報告された SIM と eSIM
プランを表示し、デバイスが通信事業者によって準備された eSIM
プランをダウンロードできるようにします。詳細は後述の **iPhone** と **iPad** を参照してください。

> SIM 情報は、デバイスポリシーで ネットワーク情報
> の報告が有効になっている場合、完全管理デバイスによって報告されます（このオプションは
> Cerberus Enterprise によって常に有効になります）。 ステータスレポート
> ページを参照してください。

## デバイス EID

EID（ eUICC Identifier）は、デバイスの eSIM ハードウェアを識別します。通信事業者はこれを使用して
eSIM プロファイルをデバイスに紐付けるため、 EID の取得は通常、 eSIM
プロビジョニングワークフローの最初のステップです。

- 会社所有デバイス （ Android 13 以降）： EID
  はデバイスステータスとともに自動的に報告され、ユーザーの操作は不要です。
- 個人所有デバイス （ Android 13 以降）： **EID** をリクエスト
  ボタンを使用します。ユーザーのデバイスに、 EID
  の共有を求める通知が表示され、リクエストを承認または拒否できます。 EID
  は、ユーザーが承認した場合にのみ表示されます。リクエストが保留中である間、ボタンは無効の
  ままです。

> EID
> リクエストを送信すると、ユーザーのデバイスに通知が表示されるため、最初に確認ダイアログが表
> 示されます。

## インストール済み SIM

インストール済み SIMテーブルには、物理 SIM や eSIM
プロファイルなど、デバイスで現在認識されている SIM
が一覧表示されます。個人所有デバイスでは、デバイスが SIM 情報を報告しない場合でも、 eSIM を追加
コマンドでインストールされた eSIM プロファイルが表示されます。

通信事業者 ： SIM に関連付けられた通信事業者名（報告された場合）。
電話番号 ： SIM に関連付けられた電話番号（報告された場合）。
ICCID：SIM の集積回路カード識別子です。
アクティベーション状態 ： eSIM がアクティブ化されているかどうか。 Android 15 以降の eSIM
についてのみ報告されます。
構成モード ：eSIM が管理者によって構成されたか、ユーザーによって構成されたか。 Android 15
以降の eSIM についてのみ報告されます。
SIM の種類 ：デバイスがそのエントリを eSIM として報告しているかどうかを示します。

削除コマンドが進行中または実行済み（失敗していない）の eSIM には、一時的な 削除中
アクティベーション状態が表示されます。デバイスが更新された SIM
リストを報告すると、エントリはリストから消えます。削除の進行中は、同じコマンドを二重に送信
しないように、削除ボタンは使用できません。

eSIM を削除
インストール済みの eSIM
の横にある削除ボタンを使用して、デバイスからそのプロファイルを削除します。コマンドが送信される前
に、削除する eSIM の ICCID を確認するダイアログが表示されます。 eSIM の削除は Android 15
以降でサポートされています。

eSIM を追加
eSIM を追加 セクションでは、デバイスに新しい eSIM プロファイルをインストールします（ Android 15
以降でサポート）。必要なものは次のとおりです。

有効期間 ：コマンドをすぐに実行できない場合に、そのコマンドが有効な期間。
アクティベーションコード ：通信事業者が提供する eSIM
プロファイルのアクティベーションコード。コード全体を入力することも、 SM-DP+
アドレスのみを入力して、通信事業者がすでに EID
に紐付けたプロファイルをデバイスに検出させることもできます。
アクティベーション状態 ：eSIM
プロファイルをダウンロード後に自動でアクティブ化するか、ユーザーによる手動アクティベーシ
ョンのために未アクティブのままにするか。

コマンド履歴
eSIM を追加セクションの下に、デバイスに送信された eSIM コマンド（ eSIM を追加 、eSIM を削除 、 EID をリクエスト
）の履歴が表示されます。テーブルは並べ替えが可能で、ページネーションに対応しています。一部の行は
展開して、コマンドのパラメーター（アクティベーションコードや ICCID
など）と実行ステータスを表示できます。これには、デバイスで操作が失敗したときの eSIM
エラーの詳細も含まれます。

作成日
コマンド
有効期間
ステータス
エラー ：コマンドの実行で報告された場合に、 eSIM のエラー状態（たとえば ユーザーが拒否 、無効なアクティベーションコード 、ICCID が見つかりません ）を表示します。
実行日

ワイプおよび登録解除時の eSIM ワイプ
コマンドパネルからデバイスをワイプするとき、 eSIM をワイプ フラグで、ワイプ時に eSIM プロファイルを削除するかどうかを制御します。ワークプロファイルを持つ個人所有デバイスでは、このフ
ラグはデフォルトで有効になっています（管理対象の eSIM は削除されますが、個人所有の eSIM は影響を受けません）。同じフラグは デバイスの登録解除 確認ダイアログでも使用できます。

iPhone および iPad
このパネルは、 iPhone と、セルラーデータを報告した iPad（Wi-Fi のみの iPad
にはありません）について、デバイスが会社所有で User Enrollment でない場合にのみ表示されます。デバイスには、デバイス情報とともにセルラー情報が要求されます。要求
のタイミングは、登録時、毎日、 デバイス情報を更新
を実行したとき、所有権が会社所有になったとき、および セルラープランを更新 の数分後です。

デバイス EID：SIM とともに報告された EID
で、通信事業者用にコピーするボタンがあります。デバイスが報告しない場合、ユーザーは設定 >
一般 > 情報で確認できます。
報告済み 、データローミング 、インターネット共有 、モデムファームウェア：デバイスが応答したかどうかと、報告された状態。データローミングとインターネット共有は、

コマンドパネルの デバイス設定 で変更でき、現在の状態も表示されます。
SIM：SIM または eSIM プランごとに 1行（デュアル SIM デバイスでは 2
行）で、デバイスが報告したスロット、そのラベルと種類（デバイスが EID
とともに報告する場合は eSIM、それ以外は SIM カード）、通信事業者（デバイスが別のネットワークでローミングしている場合はツールチップにホーム
通信事業者）、電話番号、 ICCID、 EID、 IMEI、データ通信用および通信用の SIM
、ローミングが表示されます。プランのない eSIM スロットは、 プランなし
としてグレー表示されます。
このデバイスは SIM を報告していません は、デバイスが SIM
なしで応答したことを意味します。 セルラー情報はまだありません
は、デバイスがまだ応答していないことを意味します。 デバイス情報を更新
を使用してください。

電話番号、 ICCID、 IMEI、 EID は個人と回線を識別する情報です。これらは個人所有デバイスや User Enrollment
には要求されません。デバイスが個人所有になると、情報は直ちに削除され、コマンド履歴にある以
前のデバイス情報コマンドの結果では非表示になります。この情報はエクスポートされず、システム
ログにも書き込まれません。

セルラープランを更新

iPhone および iPad は、アクティベーションコードから eSIM をインストールできません。通信事業者は、
eSIM サーバー（ SM-DP+）上で eSIM プランをデバイスの EID
に紐付け（予約）し、そのサーバーのアドレスを提供します。次に セルラープランを更新によって、デバイスは自身を待機しているプランをダウンロードするよう求められます。パネルの
セルラープランを更新 ボタンをクリックすると、コマンドパネルでコマンドが選択され、そこで
通信事業者の eSIM サーバー URLを入力します。

https:// アドレス ：そのまま送信されます。 http://、ユーザー名またはパスワード、あるいは #
部分を含むアドレスは受け付けられません。
ホスト名 （例： smdp.carrier.example）は、 https://smdp.carrier.example
として送信されます。
LPA アクティベーションコード （ LPA:1$server$code、eSIM QR コードのテキスト）：コマンドはコードを伝送できないため、サーバーのみが使用されます。プラ
ンは通信事業者によってデバイスの EID
に紐付けられている必要があり、そうでない場合、デバイスはダウンロードするものを検出できま
せん。

デバイスは、監視対象でない場合でも、ユーザーに確認せずにプランをインストールしてアクティブ化します。コマンド履歴の「成功」は、デバイスがリクエストを承認したことを意味し、プランがインストールさ
れたことを意味するものではありません。インストールには最大 3分かかる場合があり、 Cerberus Enterprise は約 3分後にデバイスに SIM
を再度要求するため、新しいプランがパネルに表示されます。エラー 36001

（デバイスがセルラーシステムに接続できませんでした）、 36002（ eSIM がサポートされていません）、 36003
（セルラーシステムがビジーです。後でもう一度お試しください）については、システムログで説明されています。一度ダウンロードしたプランは再度ダウンロードできません。インストールに失敗した場合は、通信事業者にお問い合わせください。このコマンドは、デバイスページの **Apple** デバイスアクションメニューから複数のデバイスに対して一度に実行することもできます。

# Apple が許可していないこと

- アクティベーションコードからの **eSIM** を追加 ：できません。 EID に紐付けられたプランでセルラープランを更新 を使用してください。
- **eSIM** を削除 ： eSIM をリモートで 1つずつ削除することはできません。 **eSIM** データプランを保持する をオフにしてデバイスを消去すると、すべての eSIM が削除されます。単一のプランを停止するには、通信事業者に非アクティブ化を依頼してください。プランはデバイスに残りますが、接続できなくなります。
- **EID** をリクエスト ：不要です。 EID は会社所有デバイスの SIM とともに取得されます。
- **Mac**にはセルラーまたは eSIM の管理機能はありません。

コマンド
デバイス ページには、管理対象デバイスにリモート コマンドを送信するための コマンドパネルがあります。使用可能なコマンドは、プラットフォーム (Android または Apple) とデバイスの状態によって異なります。

コマンドを送信できるのは、現在登録されているデバイスのみです。登録解除されたデバイス、まだ登録さ
れていない ADE
デバイス、および過去の登録の履歴レコードでは、パネルにはコマンド履歴のみが表示されます。

デバイスが現在オンラインでない場合、コマンドはデバイスがインターネットに接続され次第配信さ
れて実行されます。 Android コマンドでは、 有効期間
パラメーターを設定して、未配信のコマンドが有効な期間を指定できます。

Android (AMAPI) コマンド
Android デバイスの場合、コマンドパネルには 有効期間 フィールド（値＋単位）と コマンドセレクターが含まれます。一部のコマンドには追加のパラメーターが必要で、コマンドを選択すると動的に
表示されます。

共通パラメーター

有効期間 ：コマンドをすぐに実行できない場合に、コマンドが有効な期間。
コマンド ：デバイスに送信するアクションを選択します。

追加フィールドのないコマンド

デバイスをロック : デバイスをロックします。
デバイスを再起動 : デバイスを再起動します。 Android 7.0 以降が必要です。
紛失モードを無効化 : デバイスを紛失モードから解除します。
所有権を放棄 : Android 8.0 以降の会社所有デバイスからワーク
プロファイルとすべてのポリシーを削除し、個人用として残します。個人プロファイルのアプリとデータは保持されます。デバイスがコマンドを確認すると、サーバーからデバイスが削除されます
。この操作は元に戻せません。

# [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

> [redacted]

# [redacted]

[redacted]

## Android [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

# Apple (MDM) [redacted]

Apple [redacted]
[redacted]
Android
[redacted]

# [redacted]

- : **Bundle ID**
- : (  200  )

iPhone  iPad  **Cerberus Enterprise**
(
**Cerberus Enterprise**  )
iOS
2
(
 )

# 

iPhone  iPad
Mac

- : Mac
  6  PIN  PIN
  iPhone
  Lost iPhone
- iPhone  iPad
  
  
  
  
- 
  **iPhone**
  
  iOS
- 
  iPhone  iPad
  
- 
  OS  MDM
- : Mac  Bluetooth  Personal Hotspot  Shared iPad  (  )
  
  Personal Hotspot
  (SIM  Personal Hotspot  )
  Cerberus Enterprise  30

- :
- iPhone iPad eSIM Mac 6 PIN
- iOS 17 iPhone iPad Wi-Fi Ethernet
- iPhone iPad iOS 13 User Enrollment **eSIM** **URL** https:// LPA EID eSIM EID **SIM**
- **eSIM** eSIM **eSIM** iOS 17.2 Apple
- Shared iPad iCloud iPad

# Shared iPad

Shared iPad Managed Apple Account Shared iPad ADE **Apple Automated Device Enrollment** **Shared iPad**

- **Shared iPad** iPad iCloud iPad iPadOS 14

デバイス設定
：各ユーザーのストレージ、想定ユーザー数、ユーザーとゲストセッションがログアウトされる非
アクティブ時間、ゲストセッションのみ、ログイン画面で提案される Managed Apple Account ドメイン、ユーザーがパスワードをオンラインで確認せずにサインインできる日数、新規ユーザー
の言語と地域のセットアップをスキップするかどうか。空のフィールドは現在の値を維持します。
新しい iPadOS が必要な設定は無効になります。

Mac のユーザー

Mac では、 Mac のユーザー パネルに、管理に登録されているユーザー（通常は Mac を登録したユーザー）が一覧表示されます。ポリシーのアカウントは、そのセッションにインストールされ
ます。各ユーザーについて、登録された日時、セッションの最後のレポート、アカウントの状態（ 最新 、ユーザーを待機中 （ユーザーがログインすると Mac がインストールします）、 Mac
から報告された理由付きの 未適用 、ポリシーにアカウントがない場合は アカウントなし ）が表示されます。
再読み込み を使用して一覧を再度読み取ります。

アクティベーションロック

アクティベーションロック
フィールドには、アクティベーションロックがオンかどうかが表示されます。オンの場合、消去されたデバ
イスは、ユーザーの Apple Account
またはデバイスのバイパスコードでのみ再セットアップできます。監視対象デバイスは、 デバイス設定で許可されている場合にのみアクティベーションロックをオンにします。 Cerberus Enterprise は監視対象デバイスにバイパスコードを要求して保存します。フィールドメニューの バイパスコードを表示を使用すると確認できます（管理者のみが可能で、表示はすべてシステムログに記録されます）。その後、
デバイスのアクティベーションロック画面で Apple Account を空のまま、パスワードとして入力します。

リカバリロックとファームウェアパスワード

（ Mac）

Apple silicon を搭載した Mac では リカバリロック フィールドが、 Intel ベースの Mac ではファームウェアパスワード フィールドが表示されます。どちらも起動時に Mac
を保護します。リカバリロックでは recoveryOS
がパスワードを要求し、ファームウェアパスワードでは別のディスクまたはリカバリからの起動時に Mac がパスワードを要求します。フィールドには、 Mac
がパスワードを報告しているかどうかが表示され、ツールチップには Cerberus Enterprise
が保存した日時と最後に検証した日時が表示されます。

パスワードを設定または変更 ：Cerberus Enterprise
は、どのキーボードレイアウトでも同じキー上にある 20
文字のパスワードを生成するか、管理者が入力します（アクセント記号なしの 8〜64

文字。他のロールは保存済みパスワードを表示できないため、生成のみ可能です）。パスワードは送信前に暗号化して保存され、Mac が確認した場合にのみ保存済みのパスワードを置き換えます。Mac に Cerberus Enterprise 以外で設定されたパスワードがすでにある場合は、現在のパスワードとして入力します。これは一度だけ使用され、保存されません。

- パスワードを検証：保存済みのパスワードが正しいかどうかを Mac に問い合わせます。結果はツールチップとシステムログに表示されます。
- パスワードを表示：保存済みのパスワードを表示できるのは管理者のみで、表示はすべてシステムログに記録されます。生成されたパスワードは 4 文字ずつに区切って表示されます。スペースを入れずに入力してください。
- パスワードを消去：Mac からパスワードを削除します。

Intel ベースの Mac は、ファームウェアパスワードの変更を適用するために再起動します。それまでは以前のパスワードが引き続き必要で（「パスワードを表示」に一覧表示されます）、別の変更は送信できません。また、Apple はファームウェアパスワードのコマンドを 30秒に 1 回しか受け付けません。パスワードはコマンド履歴では非表示になります。

Mac が管理から外れると（登録解除、ユーザーによる削除、消去）、macOS はリカバリロックを自動的に削除し、Cerberus Enterprise は保存済みのリカバリロックパスワードを破棄します。Mac がリカバリロックがないと報告した場合（たとえば再登録後）も同様です。Mac を登録解除する（またはそのポリシーを削除する）場合、保存済みのファームウェアパスワードが最初に消去され、Mac が再起動してから管理から外れます。消去に失敗した場合、Mac はそのまま管理から外れ、パスワードは引き続き確認できるように保存されたままになります。ユーザーによって管理から削除された Mac、または消去された Mac はファームウェアパスワードを保持し、Cerberus Enterprise もそれを保持します。デバイスレコードを削除すると保存済みのパスワードが削除されるため、最初に確認が求められます。パスワードを書き留めてください。パスワードがない場合、Apple しか削除できません。

# FileVault（Mac）

**FileVault** フィールドには、Mac のディスクが暗号化されているかどうかと、ツールチップに Cerberus Enterprise が個人用復旧キーを保存しているかどうかが表示されます。Mac は、ポリシーの FileVault 設定を受け取った後に FileVault がオンになると、キーを送信します（Apple ポリシーの **macOS** ページを参照）。

- リカバリキーを表示：キーを表示できるのは管理者のみで、表示はすべてシステムログに記録されます。Mac のログインウィンドウでユーザーのパスワードをリセットする場合、またはリカバリでディスクのロックを解除する場合に使用します。Mac が管理から外れた後も利用できますが、デバイスレコードを削除するとキーも削除されます。

リカバリキーを変更 ： Mac
は個人用リカバリキーを置き換え、新しいキーを暗号化して送信します。古いキーは機能しなくな
ります。これは、保存済みのキーを読み取れる場合にのみ可能です。 Mac はそのキーでロック解除され、ユーザーのパスワードは必要ありません。保存済みのキーはコマン
ド履歴では非表示になり、 Mac が応答すると（または応答なしで 7
日経過すると）サーバーから削除されます。

Bootstrap Token（Mac）
macOS 10.15 以降の Mac は、セキュアトークンを持つユーザーがログインすると、 Bootstrap Token
を管理サーバーに送信します。サーバーはそれを保持し、その Mac にのみ返します。 Mac
はそれを使用して新しいユーザーにセキュアトークンを付与し、 Apple silicon を搭載した Mac
では、管理者パスワードを要求せずにソフトウェアアップデートをインストールしたり、カーネル拡張を承
認したりします。ダッシュボードでもその他の場所でも、誰もトークンを表示できません。 Bootstrap Tokenフィールドにはその状態が表示されます：

エスクロー済み ：サーバーがトークンを保持しています。ツールチップには Mac
が送信した日時が表示されます。
以前にエスクロー済み ：保存されたトークンは、 Mac の最新の登録または MDM 証明書の更新より前に送信されたものです。更新後はこれは想定どおりです。トークンは保持され
、 Mac は再度送信しません。新しい登録後は、有効でなくなっている可能性があります。 Mac
のターミナルで sudo profiles install -type bootstraptoken を実行してください。
エスクローなし ： Mac はまだトークンを送信していません。今すぐ送信するには、 Mac
の管理者がターミナルで sudo profiles install -type bootstraptokenを実行します（ sudo
profiles status -type bootstraptokenでエスクローされているかどうかを確認できます）。

ツールチップには、 Mac が認証にトークンを許可しているかどうかも表示されます。 Automated Device
Enrollment でセットアップされた Mac は自動的に許可します。 Apple silicon を搭載した他の Mac
では、ユーザーが recoveryOS のスタートアップセキュリティユーティリティで許可できます。 Intel Mac
は認証にトークンを使用できません（ サポート対象外
）が、エスクローされたトークンは引き続き新しいユーザーにセキュアトークンを付与します。 Mac
がトークンを送信、削除、または要求するたびに、システムログに記録されます。

デバイスの状態と OS のアップデート

デバイスの状態 パネルには、デバイスが自身について報告する内容が表示されます。 OS
のバージョンとビルド、ソフトウェアアップデートの進行状況（保留中のバージョン、期限、開始理由、失
敗）、パスコードが設定されポリシーに準拠しているかどうか、 Mac の FileVault
、バッテリーの状態、デバイスに設定されているアカウントです。

利用可能なアップデート リストには、デバイスがインストールできる OS
アップデートが表示され、登録時と毎週収集されます。 アップデートを確認 で今すぐ要求し、インストール
でアップデートをすぐにインストールする（確認後にデバイスが再起動します）か、ダウンロードのみを行

ってユーザーにインストールさせることができます。これは監視対象の iPhone と iPad、および Mac で、 iOS、 iPadOS、macOS 26
まで機能します。それ以降のバージョンや多数のデバイスの更新には、ポリシーの必須アップデートを使用

してください（ Apple ポリシーの ソフトウェアアップデート ページを参照）。

Apple silicon を搭載した Mac
が管理者パスワードを要求せずにアップデートをインストールするのは、認証に Bootstrap Token を許可し、トークンがエスクローされている場合のみです（上記の Bootstrap Token を参照）。それ以外の場合、確認では、アップデートのインストール前にユーザーが管理者パスワードを入
力する必要があるかもしれないと表示されます。

アプリケーションとインベントリ

アプリケーション パネルには、デバイスのすべてのアプリが 1 つのテーブルに一覧表示されます。ポリシーまたはコマンドでインストールされたアプリのインストール状態は、デバイスからリアルタイムで報告されます。バージョン、サイズ、ユーザーがインストールしたアプ
リは、登録時と毎週収集される最新のアプリ一覧から取得されます。今すぐ要求するには
デバイスに問い合わせ を使用します。

管理: デバイス ポリシーによってインストールされたアプリは ポリシー 、
アプリをインストール などのコマンドでインストールされたアプリは 管理対象、ユーザーがインストールしたアプリは 未管理 です。 Cerberus Enterprise アプリには Cerberus によってインストール済み チップが付いています。
要対応
：インストールに失敗したアプリ、ユーザーによって拒否または削除されたアプリ、またはユーザ
ーを待機しているアプリ。行を開くとエラーを確認できます。失敗したポリシーのアプリは、再試
行ボタンで再度インストールできます。デバイスが検証されていないと報告した組み込みアプリと
App Store アプリはカウントされません。
アプリを削除
：管理対象アプリは、データとともに削除できます。ポリシーでインストールされたアプリを削除
するには、ポリシーから削除します。ポリシーは、管理対象アプリとしてインストールされた Mac パッケージがポリシーから削除された場合にも、このコマンド自体を送信します。

プロファイル、証明書、セキュリティ
パネルには、デバイスから報告された構成プロファイル、証明書、セキュリティ状態（パスコード、暗号化
、 Mac の FileVault とファイアウォール）が表示されます。

個人所有のデバイスでは、ユーザーがインストールしたアプリは収集されず、 Cerberus Enterprise
が管理するプロファイルと証明書のみが一覧表示されます。

インベントリの変更 パネルには、デバイスから送信された 2 つの一覧の間で変更された内容が表示されます。インストール、削除、更新されたアプリ（新旧バージョン
付き）、インストール、削除、更新されたプロファイル、追加または削除された証明書です。変更は、デバ
イスが新しい一覧を送信したとき（アプリとプロファイルは毎週、証明書は毎日）、または

デバイスに問い合わせ
を使用したときに検出されます。表示される日付は検出された日時で、変更は前の一覧とその一覧の間に発
生しています。デバイスの最初の一覧、および新しい登録または所有権の変更後の最初の一覧は、開始点と
してのみ記録されます。名前または識別子で検索し、種類と変更でフィルターできます。変更は 365
日間保持されます。

OS アップデートによって多数の Apple アプリが一度に置き換えられた場合、それらは展開可能な 1
行（例：「 23個の Apple アプリが更新されました」）として表示されます。 MDM 証明書の更新は
MDM 証明書を更新済み として表示されます。個人所有のデバイスでは、 Cerberus Enterprise
が管理する項目の変更のみが表示されます。

Apple の履歴の列

作成日
コマンド
ステータス : 送信済み (デバイスを待機中、接続されるとすぐに配信 )、成功 、応答済み (
行を開いて結果を表示 )、デバイスを待機中 (デバイスが現在コマンドを実行できない )、失敗 (
行を開いて理由を表示 )、または キャンセル済み (デバイスのコマンド
キューがクリアされた場合。再登録時など )。
実行日

更新
コマンドパネルの更新アクションを使用して、コマンド履歴を再読み込みします。