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。

Revision #60
Created 2025-12-17 10:39:46 UTC by Admin Updated 2026-11-12 09:56:03 UTC by Admin