アプリとプロファイル

このセクションでは、 Apple
デバイス向けの管理対象アプリケーションとアカウントペイロードを構成する方法について説明します。

アプリ管理
アプリ管理 パネルには、アプリ関連の一般的な制限と管理対象アプリの一覧の両方が含まれます。

一般的なアプリの制限

Appクリップを許可
アプリのインストールを許可
アプリの削除を許可
アプリの自動ダウンロードを許可
アプリの非表示を許可
アプリのロックを許可
アプリ内課金を許可
デフォルト ブラウザの変更を許可
エンタープライズ アプリの信頼を許可

管理対象アプリ

アプリケーションを追加
を使用して、ポリシーにアプリを追加します。各管理対象アプリはカードとして表示されます。カードを展
開して設定を編集し、削除アクションでアプリを削除できます。

App Store ID：管理対象アプリの App Store識別子。
バンドル ID：アプリのバンドル識別子。
インストール動作
：アプリをインストールしたままにする必要があるか、ユーザーがインストール／削除できるかを
制御します。
割り当て ：Cerberus
がデバイスごとに選択するライセンスの種類。会社のデバイスではデバイスライセンス、個人の
iPhoneおよび iPad（ユーザー登録）では Managed Apple Account のユーザーライセンス。このフィールドは変更できません。
VPPライセンス ：App Storeを通じたインストールに使用される VPPライセンスの種類。

アプリ選択リストには、各アプリの利用可能なライセンス数と合計ライセンス数が表示されます。無料アプ
リは 無制限 と表示されます。 Appleは無料アプリに無制限のライセンスを付与します。アプリは 1
つのポリシーに 1回だけ追加できます。すでにポリシーにあるアプリと同じ App Store IDまたはバンドル ID を持つアプリは拒否され、同じアプリを 2回リストしたポリシーも保存時に拒否されます。

アプリ選択リストには、 Apple Businessライブラリのアプリが表示されます。アプリを追加するには、
Apple BusinessでApps & Services → Apps & Books → App Storeを開き、アプリを検索して View をクリックします。無料アプリの場合は、 Addをクリックし、 All current and future（または Apps and
Booksトークンの組織単位）を Organizational Unitsで選択し、 Addをクリックしてから Review
をクリックして確認します。有料アプリの場合は、その価格をクリックし、 License Typeとして
Managed Licensesを選択し（引換コードは Cerberus Enterpriseでは使用できません）、 Apps and
Booksトークンの Organizational Unitを選択し、 Licensesの数（注文ごとに最大 1,000
）を入力してから、 Reviewをクリックして購入します。購入前に Settings → Payments & Billing →
Apps & Services → Payment Methods
で支払い方法を設定しておく必要があります。その後、アプリがアプリ選択リストに表示されます。

個人デバイスのアプリ（ユーザー登録）

ユーザー登録で登録された個人の iPhoneおよび iPad
にはシリアル番号がないため、デバイスでサインインしている Managed Apple Accountの
ユーザーライセンス を使用して、ポリシーの App Storeアプリを受け取ります。 Cerberusはアカウントを
Apps and Booksに登録し、無料アプリを含めてライセンスを自動的に割り当てます。 Managed Apple
AccountとApps and Booksトークンは、同じ Apple Business
組織に属している必要があります。有料アプリはアカウントごとに 1
つのライセンスを使用し、そのアカウントのすべての個人デバイスで共有されます。

ユーザーライセンスを待機中 ：アプリは、 Apple
がライセンスを確認した後にのみデバイスに送信されます。通常は数分以内です。デバイスの
アプリケーション パネルに理由が表示されます。
ユーザーライセンスに失敗しました ：Apple
がライセンスを割り当てられませんでした。たとえば、有料アプリに残りのライセンスがない場合
です。 Apple Businessでライセンスを追加してから 再リクエスト を使用してください。 Cerberus も毎日自動的に再試行します。
インストールプロンプト ： iOS
は各アプリをインストールする前にユーザーに確認します。ユーザーがキャンセルすると、アプリ
はユーザーによるインストールの承認待ち と表示されます。 再リクエスト
でプロンプトが再度表示されます。
解放
：ポリシーからアプリを削除するか、アカウントの最後の個人デバイスの登録を解除すると、同じ
アカウントの別の登録済みデバイスがまだ必要としていない限り、アプリが削除され、ライセンス
が解放されます。

詳細については、 Appleアカウント駆動型登録 を参照してください。

管理対象構成

管理対象構成は、アプリのベンダーが文書化した方法で、アプリに設定（サーバーアドレスやアカウント名
など）を提供します。ポリシーでアプリを開き、 管理対象構成を追加 をクリックします。これは iOSまたは
iPadOS 18.4以降 の iPhoneおよび iPad、および macOS 27以降 の Macに送信されます。 Apple Vision Pro
にはまだ送信されません。アプリは管理対象構成をサポートしている必要があります。読み取らないアプリ
は無視します。アプリパネルには、アプリ名の横にキーの数が表示されます。

キー
：各行にはキー、種類、値があります。種類は、テキスト、整数、小数、ブール値、日付、テキス
トリスト、整数リストです。キーは大文字と小文字を区別し、一意である必要があります。
キーを追加 で行を追加し、 構成を削除 ですべてのキーを削除します。
変数 ：テキストおよびテキストリストの値には、 $EMAIL$、$USERNAME$、$FULLNAME$、 $SERIAL$、$UDID$
を含めることができ、各デバイスとそのユーザーの値に置き換えられます。値のない変数（たとえ
ば、ユーザーのいないデバイスの $EMAIL$
）は空のままになり、システムログにその旨が記録されます。ユーザーの詳細が変更されると、デ
バイスは新しい値を取得します。 Google Directory
から同期されたユーザーの場合、値は次回のポリシーまたはデバイスの変更時に更新されます。
構成をインポート ：アプリのベンダーが MDM
向けに公開しているファイルを開くか貼り付けてから、 読み取り をクリックします。 AppConfig
スペックファイル （specfile.xml
）には、アプリがサポートするすべてのキーと、その説明、種類、デフォルト値、許可される値が
一覧表示されます。インポートするキーを選択し（デフォルト値のあるキーはすでに選択されてい
ます）、インポート後に残りを入力します。スペックファイルが別のアプリ用の場合は警告が表示
されます。 プロパティリスト （プロパティリスト全体、または <dict>
のみ）はそのままインポートされます。次に、現在のキーを置き換えるか追加するかを選択します。ネストされた辞書、データ値、混在した種類や不明な種類のリストはサポートされておらず、ス
キップされたものとして一覧表示されます。 Apple
はアプリの構成キーを公開していないため、ベンダーのドキュメントにファイルがない場合はベン
ダーに問い合わせてください。 plistとしてコピー
は、変数が置き換えられる前の、デバイスが受け取る状態の構成をコピーします。
制限 ：アプリごとに最大 200キー、キーは最大 255文字、テキスト値は最大 4,096
文字、リストは最大 200項目で各項目最大 1,024文字、日付は 1970年から 9999
年まで、アプリごとに合計 64 KBまでです。
パスワードには使用しないでください
：構成はそれが構築されたデバイスにのみ送信され、ログにはキー名と種類のみが表示されますが、ダッシュボードの管理者は値を読み取ることができ、デバイスが構成をダウンロードするアドレ
スは値によって変わるため、推測しやすい値（ブール値や小さな数値）はそこから推測される可能
性があります。管理対象構成にはパスワードやその他の機密情報を入れないでください。ステータス
：デバイスがアプリの構成を受け入れなかったことを報告すると、デバイスのアプリケーションパ
ネルのアプリの横に 構成が受け入れられませんでした
が表示されます。これによってデバイスが非準拠になることはありません。デバイスがダウンロー

ドできない構成は、非準拠になります。

アプリのオプション

ポリシーの各アプリ（ App Storeアプリとカスタムアプリ）には、これらのオプションがあります。
デバイスのデフォルト
は、選択をデバイスに任せます。オプションをサポートしていないデバイスには適用されませんが、アプリ
は引き続きインストールされます。

自動更新 ：App Store設定、常にまたはなし。 iOS、iPadOS、macOS、visionOS 26
以降。カスタムアプリでは、 App Store設定は「なし」と同じように動作します。
モバイルデータ通信でのダウンロード ：自動インストールと更新のための App Store
設定、常にまたはなし。 iOSまたは iPadOS 26以降の監視対象の iPhoneおよび iPadのみ。
アプリデータをバックアップ ：アプリデータをデバイスのバックアップに含めるかどうか。 Mac
では利用できません。
ユーザーがアプリを非表示にできる とユーザーがアプリをロックできる ： iOSおよび iPadOS
18.1
以降、監視対象デバイスで適用されます。ロックを許可しない場合は、非表示もできなくなります
。アプリの非表示を許可 とアプリのロックを許可 の制限は、すべてのアプリに適用されます。
お客様の PINが必要な Tap to Pay取引後にデバイスをロック ：iPhoneのみ。
関連ドメイン
：アプリが関連付けられているドメイン（ユニバーサルリンクやパスワードの自動入力など）で、
最大 50個です。 applinks:、ワイルドカード、 ?mode=を付けずに、 www.example.com
のようなプレーンなホスト名を入力してください。 Macでは利用できません。
ドメインを直接検証 ：デバイスは、 Apple
のサーバーを介さずに、ドメインのサイトアソシエーションファイルを直接確認します。インター
ネットから到達できない内部ドメインにのみ有効にしてください。
削除 ：必須 としてインストールされたアプリは、ユーザーが削除できません。

Mac App Storeのアプリ
アプリ選択リストには、各アプリのプラットフォーム（ iPhone/iPad、 Mac、Apple TV、Vision
）が表示されます。 Mac専用のアプリは Macアイコンが表示されます。 Mac専用のアプリは、追加すると Mac
に適用されます。 Mac版のない App Storeアプリは Macに送信されません。ポリシーでは 適用先 の下に "
このアプリには Mac版がないため、 Macには送信されません "と表示されます。 MacはApp Store IDでApp
Storeアプリを取得するため、 Macでバンドル IDが異なるアプリも正しくインストールされます。

Cerberus Enterpriseアプリ
Cerberus は Cerberus Enterpriseアプリを iOS または iPadOS 18.4 以降 のすべての iPhone と
iPad
に、ポリシーの有無にかかわらずインストールします。このアプリはデバイスの位置情報を共有し、通知と

ライブ トラッキング要求を受信します。 必須 としてインストールされ、 Apps and Books のデバイス
ライセンス (個人デバイスではユーザー ライセンス) が使用されるため、ユーザーは削除できません。

初回セットアップ ：無料アプリをライブラリに 1回追加します。 Apple BusinessでApps &
Services → Apps & Books → App Storeを開き、「 Cerberus Enterprise」を検索して View
をクリックし、 Addを選択して All current and futureをOrganizational Unitsで選び、
Addをクリックしてから Reviewをクリックして確認します。アプリに Manage
が表示される場合は、すでにライブラリにあります。アプリを開き、組織単位が All current and future units
であることを確認してください。それまでは、ダッシュボードにバナーが表示され、デバイスでは
アプリが未インストールとして表示されます。 アカウント設定 を参照してください。
ポリシーには追加できません
：このアプリはポリシーに追加できません。アプリ選択リストでは無効になり、カスタムアプリ（
同じバンドル ID
）としても拒否されます。すでにこのアプリを一覧に含むポリシーは、開いたときにエントリが削
除されます。保存してポリシーを確定してください。
インストールされないデバイス : iOS または iPadOS が 18.4 より古いデバイス。 Shared iPad へのインストールはサポートされていますが、アプリの機能はそこで検証されていません。
個人デバイス : User Enrollment で登録された iPhone と iPad にも、インストール プロンプトと
Managed Apple Account のユーザー
ライセンスを使用してアプリがインストールされます。組織からのメッセージを受信し、ポリシー
で 個人デバイスの位置情報とジオフェンス
が有効になっており、ユーザーが許可しない限り位置情報にはアクセスしません。
インストールされたまま保持 ：Apps and Books
トークンが期限切れになるか、アプリがライブラリから削除されると、アプリはデバイスに残り、
デバイスページには Apps and Booksに対応が必要であると表示されます。 24
時間後にまだライブラリにアプリがない場合にのみ削除されます。

カスタムアプリ

カスタムアプリは、 App Storeを介さずに配布する独自の iPhoneおよび iPadアプリ（.ipaファイル）です。
Xcodeで、 Enterprise配布用（ Apple Developer Enterprise Program
：すべてのデバイスにインストールされます）または Ad Hoc
配布用（プロビジョニングプロファイルに登録されたデバイスにのみインストールされます）にアプリを書
き出します。 App Storeビルドはアップロードできません。

カスタムアプリを追加 をクリックして、組織のカスタムアプリを開きます。 アプリをアップロード で.ipa
ファイル（最大 2 GB）を追加します。アプリを選択して ポリシーに追加
をクリックします。一覧には、バージョン、署名の種類、 Ad Hoc
アプリのプロファイル内のデバイス数、プロビジョニングプロファイルの有効期限が表示されます。

新しいバージョン ：同じバンドル ID
のアプリをアップロードします。以前のバージョンが置き換えられ、そのアプリを使用するポリシ
ーのデバイスがアプリを更新します。

要件 ： iOS 17.2以降の iPhoneおよび iPad
。アプリをインストールできないデバイスには配信されません。 iPhone上の iPad 専用アプリ、アプリが必要とするバージョンより古い iOS、Ad Hoc
アプリのプロファイルにないデバイス、有効期限が切れたプロビジョニングプロファイルなどが該
当します。
有効期限
：プロビジョニングプロファイルの有効期限が切れると、アプリは開かなくなります。有効期限日より前に、新しいプロファイルで署名したバージョンをアップロードしてください。
予約済みのバンドル ID：Cerberus Enterpriseアプリのバンドル ID（
com.lsdroid.Cerberus.Enterprise）を持つカスタムアプリは、 Cerberus がそのアプリ自体をインストールするため、ポリシーに追加できません。
削除:
まずアプリをポリシーから削除してください。その後、デバイスからアプリが削除されます。

Mac パッケージ

カスタムアプリでは、 Macインストーラパッケージ (.pkg ファイル)も受け付けます。パッケージは
productbuildでビルドした配布用パッケージ (pkgbuild
のみで作成したコンポーネントパッケージは拒否されます)であり、 Developer ID Installer
証明書で署名されている必要があります。 notarytoolと stapler
による公証とチケットのステープルを推奨します。署名されていないパッケージ、署名後に変更されたパッ
ケージ、他の証明書で署名されたパッケージは拒否されます。

. pkg ファイルを アプリをアップロード でアップロードし、ポリシーに追加します。ポリシーの Mac パッケージ の下に表示されます。 iPhone と iPad では無視されます。

macOS 26 以降 の Mac(監視対象。手動で登録した Macを含みますが、ユーザー登録は含みません)
は、パッケージを 宣言 として受け取ります。 Mac
が自らダウンロード、インストール、再試行、更新を行い、状態を報告します。古い Mac 、および管理対象アプリとしてインストールされたパッケージは、どの macOS バージョンでも MDM
コマンド で受け取ります。 macOS 26 にアップグレードされた Mac
は自動的に宣言へ移行します。各パッケージを一度は再インストールする場合があります。同じパッケージ
を含む別のポリシーへ Macが移動した場合も同様です。

新しいバージョン : 同じパッケージ ID
を持つパッケージをアップロードします。以前のバージョンが置き換えられ、そのパッケージを使
用するポリシーの Macに新しいバージョンがインストールされます。
スキップされた Mac: パッケージが許可するより古い macOS の Mac、および Apple silicon
専用にビルドされたパッケージに対する Intel Mac
です。デバイスページではパッケージが「スキップ」と理由付きで表示されます。以前にインスト
ールされたバージョンは Macに残ります。
インストール : 必須 (既定)は Macにパッケージをインストールします。 任意
はパッケージをインストールせずに Macで利用可能にします。 macOS 26
では、任意のパッケージは「システム設定」や App Store でユーザーに表示されません (macOS

26.3 で確認済み)。そのため、 Mac
上のアプリまたはスクリプトでインストールする必要があります。任意を選ぶのは、そのような手
段がある場合だけにしてください。これは macOS 26 以降の Macに適用されます。古い Mac
は常にパッケージをインストールします。この選択肢は、管理対象アプリとしてインストールされ
たパッケージには使用できません。
パッケージがポリシーから外れたときにパッケージのファイルを削除 (macOS 27 以降):
パッケージがポリシーから削除されると、 macOS 27 以降の Mac
はインストールされたファイルを削除します。既定ではオフです。古い Mac ではファイルは残ります。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使用できませ
ん。
管理対象アプリとしてインストール :
ポリシーのパッケージでこれをオンにすると、そのアプリが管理対象アプリとしてインストールさ
れます (macOS 11 以降、ユーザー登録では不可)。macOS はインストールの失敗を報告し、 MDM がアプリを削除できるようになります。アプリは「アプリケーション」フォルダに直接インストー
ルされ、 Developer ID Application証明書で署名され、公証されている必要があります。
macOS 11 から 13 では、パッケージにはそのアプリのみを含める必要があります (
他のファイルやスクリプトは不可)。カスタムアプリでは、対象となるパッケージがわかります。
Mac
でこのオプションを適用できない場合、パッケージは通常どおりインストールされ、デバイスペー
ジに理由が表示されます。
管理対象アプリの 削除オプション : パッケージがポリシーから削除されたときにアプリを削除
(既定でオン)と、 Macが管理から外れたときにアプリを削除
です。アプリを削除するとそのデータも削除されます。ユーザーが同じアプリをすでにインストー
ルしていた場合、そのコピーが管理対象になり、これも削除されます。
削除: MDM
コマンドではパッケージをアンインストールできません。管理対象アプリとしてインストールされ
たパッケージの場合、ポリシーから削除するとアプリが削除されます (オプションがオンの場合)
。その他のファイルとパッケージのレシートは残ります。 パッケージのファイルを削除
がオンのパッケージは、 macOS 27 以降の Macから削除されます。その他のパッケージ :
ポリシーから削除しても新しいインストールが止まるだけで、ファイルは Mac
に残ります。スキップされた Mac(たとえば、より新しい macOS
を必要とする新しいバージョンの後)
は、パッケージがポリシーにある間はアプリを保持します。その後ポリシーからパッケージを削除
すると、アプリも削除されます。 Mac上の残ったファイルを (
たとえばパッケージ独自のアンインストーラで)削除し、パッケージのレシートを忘れるには sudo
pkgutil --forget <identifier> を実行します。
デバイス上の状態 : Mac
の「アプリケーション」パネルには、ポリシーの各パッケージが、待機中、承認済み (Mac
がコマンドを承認)、ダウンロード済み、インストール済み (アプリを含むパッケージのみ、 Mac
上でアプリが見つかった場合)、または失敗 (エラー付き)として表示されます。 macOS
はコマンドで送信したパッケージのインストールを報告しないため、アプリを含まないパッケージではダウンロード済みが最後の状態です。管理対象アプリとしてインストールされたパッケージは
、 macOS がアプリをインストールできなかった、または Mac
から削除されたと報告した場合にも失敗になります。 再インストール
を実行すると、パッケージが Macに再度送信されます。

宣言ありの状態 : 宣言として配信されるパッケージには、 宣言 チップと、 Mac
が報告する状態が表示されます : 待機中、利用可能 (
ユーザーがインストールしていない任意のパッケージ)
、ユーザーの操作待ち、ダウンロード中、インストール中、インストール済み、または失敗 (理由付き。たとえばダウンロードやインストールの失敗、 Macが宣言を拒否した場合など)。
ポリシーとともに削除されたファイル チップは、ポリシーから外れたときに macOS 27 の Mac がファイルを削除するパッケージを示します。 再インストール は失敗後にのみ表示され、 Mac
に再試行を求めます。 Macが宣言を拒否した場合は表示されません。

アカウント
アカウント
パネルでは、管理対象デバイスに適用するアカウントを設定できます。アカウントの変更に関する制限の切
り替えも含まれます。

制限

アカウントの変更を許可 : 無効にすると、ユーザーは Apple Account やインターネットアカウントなどのアカウントを変更できません。

アカウントを追加

Google アカウントを追加 または メールアカウントを追加を使用して、アカウントのペイロードをポリシーに追加します。各アカウントは、設定フィールドを持つカ
ードとして表示されます。

ユーザーからのアカウント認証情報

Google とメールのアカウントカードには、どちらも ユーザーからのアカウント認証情報の切り替えがあります。有効にすると、システムはユーザーごとにアカウント認証情報を適用します。無効
にすると、ポリシーでアカウントの ID を入力します。

Google アカウントのフィールド
表示名: アカウントについてユーザーに表示される名前。
Google メールアドレス : ユーザーのメールアドレス。
氏名: ユーザーの氏名。

メールアカウントのフィールド

メールアカウントには、 ID フィールドと受信 /送信サーバーの設定が含まれます。ホスト名は必須です。

- 表示名 ：メールアカウントについてユーザーに表示される名前。
- メールアドレス ：ユーザーのメールアドレス。
- 氏名 ：ユーザーの氏名。

受信サーバー

- サーバータイプ ：メールプロトコル (たとえば IMAP または POP)。
- 認証方法 ：サーバーの認証方法。
- **IMAP** パスプレフィックス ：サーバータイプが IMAP の場合にのみ表示されます。
- ホスト名 ：必須。
- ポート ：サーバーポート (1～ 65535)。

送信サーバー

- 認証方法
- ホスト名 ：必須。
- ポート ：サーバーポート (1～ 65535)。

S/MIME オプション

メールアカウントでは、 S/MIME の暗号化と署名の動作も設定できます。

暗号化

- **S/MIME** 暗号化
- **ID** をユーザーが上書き可能
- メッセージごとの切り替えを有効化
- ユーザーが上書き可能

署名

- **S/MIME** 署名
- **ID** をユーザーが上書き可能
- ユーザーが上書き可能

> アカウントと制限のオプションには、ダッシュボードに前提条件と対応 OS バージョンを説明するツールチップがあります。

Revision #6
Created 2026-11-10 15:16:18 UTC by Admin

Updated 2026-11-12 09:55:50 UTC by Admin