ポリシー - Apple

Appleポリシー
アプリとプロファイル
キオスクとホーム画面
パスコード
制限
ネットワーク
ソフトウェアアップデート
macOS
位置情報とジオフェンス
アカウント
コンプライアンスルール

Appleポリシー
Appleポリシーは、 Cerberus EnterpriseがMDMを介して Apple
デバイスに適用する管理設定を定義します。これらの設定は、ダッシュボードの Apple
ポリシーエディターで構成します。

開始する前に

Appleデバイス管理では、 Apple Management (APNs)を構成する必要があります。必要に応じて、 Apple

Managementの設定 (APNs)ページをお読みください。

Appleポリシーエディターを開く
ダッシュボードで ポリシー を開き、 新しい Appleポリシーを作成 をクリックします。既存の Apple ポリシーを編集するには、ポリシーテーブルの行をクリックします。

エディターのレイアウト
Apple
ポリシーエディターは、展開可能なセクションのセットとして構成されています。ページの上部では、常に
次の項目を編集できます：

名前 （必須）
ID（読み取り専用）
説明 （任意）

ポリシーセクション
以下のセクションは、 Apple ポリシー エディターで現在利用可能なパネルに対応しています。保存済みのポリシーを開くと、設定が変更されてい
るセクションはすでに開いており、それ以外は閉じたままです :

アプリ管理 ：アプリ関連の制限、管理対象アプリ、 Cerberus Enterprise
アプリの設定を構成します。
キオスクとホーム画面 ：シングル App
モード、許可およびブロックされたアプリ、ホーム画面レイアウト、 Web クリップ、通知設定、ロック画面メッセージ。
セキュリティ ：自動ロック解除や生体認証によるロック解除などの機能を制御します。
パスコード設定 ：パスコードの要件と関連ルールを構成します。
マルチメディア ：カメラと関連機能を許可 /禁止します。
セルラー : セルラー関連の設定 (アプリのセルラー データ設定、 eSIM、プランの変更) とセルラー APN を制御します。
ネットワーク : Wi-Fi ネットワーク (エンタープライズ 802.1X を含む)、VPN
、証明書、グローバル プロキシ、暗号化 DNS と Web コンテンツ フィルター、および AirDrop や
Bluetooth などの接続制限。
システムとユーザー インターフェイス : Handoff、デバイス名、スクリーン
セーバーなどのシステム機能を制限します。
ソフトウェアアップデート ：期限までに OS
バージョンを要求し、アップデートのダウンロードとインストール方法を制御します。
macOS：ファイアウォール、 Gatekeeper
、スクリーンセーバーとロック、外部ストレージとネットワークストレージ、画面共有、プライバ
シー権限、 Macのログイン項目。
Apple のアプリとサービス : iMessage、Game Center、Find My などの Apple
のアプリとサービスを制限します。
Siri と Apple Intelligence: Siri、ディクテーション、 Apple Intelligence
の機能を制限します。
iCloud：特定の iCloud
サービス（バックアップ、キーチェーン同期、プライベートリレーなど）を許可または禁止します
。
位置情報とジオフェンス : Cerberus Enterprise アプリをインストールした iPhone と iPad が出入りしたときに報告するエリア (イベント ルール用)。
アカウント ：アカウントの変更を制限し、メール、 Exchange、Google
、カレンダー、連絡先、ディレクトリアカウントを構成します。
コンプライアンスルール ：デバイスを非準拠にする要件（パスコード、最小 OS
バージョン、監視、 FileVault）と、任意のブロック。

Appleポリシーエディターの多くのオプションには、要件とサポートされている OS バージョンを説明するツールチップがあります。

保存、削除、関連付けられたデバイス
ポリシーを保存
を使用して変更を適用します。保留中の編集がない場合、またはライセンスが期限切れの場合は、ボタンは
無効になります。

既存のポリシーを編集する場合、ページには ポリシーを削除
アクションも表示されます。エディターの下部には 関連付けられたデバイス
リストが表示され、現在ポリシーを使用しているデバイスの数を確認できます。

次のページ
アプリとプロファイル：インストールするアプリと構成プロファイルを構成します。
キオスクとホーム画面：シングル Appモード、許可されたアプリ、ホーム画面レイアウト、 Web
クリップ。
パスコード：パスコードの要件と関連するセキュリティオプションを構成します。
制限：許可する機能と OSレベルの制限を定義します。
ネットワーク : Wi-Fi ネットワーク、 VPN、証明書、接続制限。
ソフトウェアアップデート：必須の OSアップデートとソフトウェアアップデート設定。
macOS：ファイアウォール、 Gatekeeper、画面ロック、ストレージ、プライバシー権限、 Mac のログイン項目。
位置情報とジオフェンス : iPhone と iPad が出入りを報告するエリアと、動作に必要なもの。
アカウント：メール、 Exchange、Google、カレンダー、連絡先、ディレクトリアカウント。
コンプライアンスルール：デバイスの要件と、非準拠デバイスのブロック。

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。

キオスクとホーム画面
Apple ポリシーエディタの キオスクとホーム画面 セクションでは、デバイスを 1 つのアプリに固定し、開けるアプリを選択し、ホーム画面を整理し、 Web サイトのアイコンを追加します。各設定は構成プロファイルとしてデバイスにインストールされます。

Apple は、これらの設定のほとんどを監視対象の iPhone と iPad（Automated Device Enrollment
で登録された、または Apple Configurator
で準備されたデバイス）にのみ適用します。それ以外のデバイスには適用されません。 Web
クリップは監視対象外の iPhone と iPad でも機能します。 Mac
にはこれらの設定は適用されません。

アプリの選択
アプリはバンドル ID で識別されます。アプリ名を入力すると、 Apple
の組み込みアプリとポリシーのアプリから選択できます。任意のバンドル ID(たとえば com.example.app)
を入力することもできます。

シングルアプリモード
デバイスは選択したアプリのみを実行します。ユーザーはホーム画面に戻ったり、他のアプリを開いたりで
きません。先にポリシーでアプリをインストールしてください。設定をオフにするかアプリを削除すると、
デバイスはシングルアプリモードを終了します。

オプション : タッチスクリーン、回転、音量ボタン、着信音 /
サイレントスイッチ、サイドボタン、または自動ロックを無効にし、 VoiceOver
やズームなどのアクセシビリティ機能をオンにします。
ユーザーがオンにできるアクセシビリティ機能 : サイドボタンを 3
回押すことでユーザーがオンにできる機能。

許可およびブロックするアプリ
ブロックするアプリ : デバイスはこれらのアプリを非表示にし、開きません。 com.apple.webapp
はすべての Web クリップをブロックします。設定と、 iPhone
の場合は電話はブロックできません。

一部のアプリのみを許可 :
デバイスはこれらのアプリのみを表示します。すべてのアプリを許可するには、リストを空のまま
にします。 ポリシーのアプリ はポリシーでインストールされたアプリを追加します。
com.apple.webapp はすべての Web クリップを許可します。
シングルアプリモードを開始できるアプリ : 必要に応じて (たとえば試験中に)
デバイスを自身にロックできるアプリ。

一部のアプリのみを許可 を使用すると、リストにないすべてのアプリ (ポリシーのアプリを含む)
がデバイスから消えます。設定と、 iPhone の場合は電話は常に残ります。

ホーム画面のレイアウト
ホーム画面の Dock とページを整理します。アプリ、アプリのフォルダ、ポリシーの Web
クリップを追加し、 追加先 で配置を選びます。アイコンをドラッグして、 Dock
とページの間で移動できます。フォルダをクリックすると、名前とアプリを変更できます。

ユーザーはアイコンを移動したり、ホーム画面からアプリを削除したりできません。レイアウトにないアプ
リは、定義したページの後のページに移動します。 iPhone では Dock に 4 つのアイコンが表示されます。ユーザーは、設定のストレージ画面で必須でないアプリを引き続き削除でき
ます。これを防ぐには、アプリ管理で アプリの削除を許可 をオフにします。

Web クリップ
Web クリップは、 Web サイトを開くホーム画面のアイコンです。ラベルと URL、および必要に応じて画像
(PNG または JPEG、正方形に切り抜き)を設定します。

ユーザーによる削除を許可 : デバイスにアイコンを残すにはオフにします。
全画面: Web サイトが Web アプリとして開き、 Safari のアドレスバーは表示されません。 他の
Web サイトでも全画面を維持 をオンにすると、他の Web サイトへのリンクも Web
アプリで開きます。
このアプリで開く : Safari の代わりに URL を開くアプリ。

通知設定
一部のアプリの通知をデバイスで表示する方法を選択します。通知を許可するかどうか、表示場所 (ロック画面、通知センター、 CarPlay)
、バッジ、サウンド、緊急アラート、バナースタイル、グループ化、プレビューなどです。ユーザーはこれ
らの設定を変更できません。

ロック画面メッセージ
ロック画面の下部に表示されるメッセージ (たとえばデバイスが見つかった場合の連絡先)
と資産タグです。どちらにも変数 $EMAIL$、$USERNAME$、$FULLNAME$、$SERIAL$、$UDID$ を含めることができます。デバイスに対応する値がない変数は空のままになります。

パスコード
パスコード設定
セクションでは、デバイスのパスコード要件と関連するセキュリティルール（最小長や複雑さなど）を制御
します。 Mac（ macOS 13 以降、 User Enrollment
を除く）では、ルールはユーザーのログインパスワードに適用されます。

オプション
Apple
ポリシーエディタでは、パスコードのオプションは切り替えと数値フィールドを組み合わせて構成します。
多くのフィールドには、対応する OS バージョンと監視要件を示すツールチップがあります。

パスコードの切り替え

次回認証時に変更 : 次回ユーザーが認証するときにパスコードのリセットを強制します。
英数字のパスコードを要求 : 少なくとも 1 つの英字と 1 つの数字を要求します。
複雑なパスコードを要求 : 「複雑な」パスコード (
繰り返しや連続したパターンがなく、少なくとも 1 つの英数字以外の文字を含む) を要求します。パスコードを要求 : 追加の長さ /品質要件なしでパスコードを要求します。注 : 他のパスコードキーを設定すると、暗黙的にパスコードが要求されます。

数値フィールド

失敗試行のリセット (分): 失敗試行カウンターがリセットされるまでの分 (
最大失敗試行回数が必要)。
最大失敗回数 ： iPhone または iPad が消去されるまで、または Mac
がロックされるまでに許可される失敗回数（範囲： 2～ 11）。
最大猶予期間 (分): パスコードを要求せずにデバイスのロックを解除できる時間 (0 = なし)。
最大非アクティブ時間 (分): デバイスがロックされるまでのアイドル時間 (範囲: 0～ 15)。
パスコードの最大有効期間 (日): 強制変更までのパスコードの最大有効期間 (範囲: 0～730)。
最小複雑文字数 : 「複雑な」文字の最小数 (範囲: 0～4)。
最小長: パスコードの最小長 (範囲: 0～ 16)。
パスコード再利用制限 : 古いパスコードの再利用を防ぐパスコード履歴の長さ (範囲: 1～50)。

制限
制限セクションでは、管理対象の Apple デバイスで許可する OS 機能を制御します。 Apple ポリシーエディタでは、これらのオプションは複数の切り替えを持つグループ化されたパネルとして表示さ
れます。

アプリ管理 パネルと ネットワーク パネルのトグルは、 Apple ポリシーの アプリとプロファイル ページと

ネットワーク ページで説明されています。

多くの制限は特定の OS
バージョンでのみサポートされ、監視対象デバイスが必要な場合があります。正式な要件は、ダッシ
ュボードのツールチップを参照してください。

ユーザー登録デバイス (仕事用アカウントでサインインして登録した個人デバイス)では、 Apple が許可していない制限は送信されません。ポリシーの制限が 1 つも適用されない場合、これらのデバイスには制限プロファイルが送信されません。ポリシーエディ
タには、ユーザー登録デバイスに適用されない制限の数が表示されます。

セキュリティ
自動ロック解除を許可
ロック解除に指紋を許可
指紋の変更を許可
コンテンツと設定の消去を許可
制限の有効化を許可
ユーザーによるプロファイルのインストールを許可
ホストとのペアリングを許可
診断の送信を許可
診断送信の変更を許可
Apple のパーソナライズ広告を許可
リモート管理の変更を許可

マルチメディア

カメラを許可
ファイル共有の変更を許可
ファイルの USBドライブアクセスを許可
通話の録音を許可
AirPrintを許可
AirPrintの認証情報の保存を許可
AirPrintの iBeacon検出を許可

モバイル通信
アプリのモバイルデータ通信の変更を許可
モバイル通信プランの変更を許可
eSIMの変更を許可
eSIMの送信転送を許可
デバイスを消去しても eSIM を保持
ローミング中のバックグラウンド フェッチを許可

携帯回線の APN

携帯回線の APNは、通信事業者が指定したアクセスポイント名 (APN)を設定します (たとえばプライベートまたはビジネス用のモバイルネットワーク)。アクセスポイント名
と、通信事業者が求める場合は認証 (PAP または CHAP)、ユーザー名 ($EMAIL$ などの変数を使用可)
、パスワード、 IP バージョン (ローミング時も含む)、プロキシサーバーとそのポート、 XLAT464
を設定します。 APN を接続 は、通信事業者がネットワークへの接続用に別の APN
を提供している場合にのみオンにします。

iPhone とセルラー対応 iPad
にのみ適用され、監視対象でなくても適用されます。ユーザー登録で登録されたデバイス (
個人デバイス)には適用されません。
携帯データ通信に使用する SIM にのみ適用されます。別の方法で APN プロファイルがすでにインストールされているデバイスには、インストールされません。
パスワードは他のネットワークパスワードと同様に保護されます。プロファイルは作成対象のデバ
イスにのみ送信され、パスワードはログに記録されません。

APN が誤っていると、デバイスで携帯データ通信が使えなくなります。先に通信事業者の SIM
を入れたテスト用デバイスで設定を試してください。

システムとユーザー インターフェイス

Handoff を許可
自動修正を許可
自動調光を許可
自動スクリーン セーバーを許可
QuickPath キーボードを許可
定義の検索を許可
デバイス名の変更を許可
デバイスのスリープを許可
iPhone ミラーリングを許可
Mac で iPhone ウィジェットを許可
キーボード ショートカットを許可

Apple のアプリとサービス
iMessage を許可
Game Center を許可
Game Center の友だち追加を許可
Find My デバイスを許可
Find My の友だちを許可
Find My の友だちの変更を許可
Book Store を許可
Book Store のアダルト コンテンツを許可
エンタープライズ ブックのバックアップを許可
エンタープライズ ブックのメタデータ同期を許可
iTunes Store を許可
成人向けコンテンツを許可

Siri と Apple Intelligence
Siri を許可
Siri のユーザー生成コンテンツを許可
ロック中も Siri を許可
ディクテーションを許可
外部インテリジェンス統合を許可
外部インテリジェンスへのサインインを許可
Genmoji を許可
Image Playground を許可
Image Wand を許可

iCloud

iCloud アドレスブックを許可
iCloud バックアップを許可
iCloud ブックマークを許可
iCloud カレンダーを許可
iCloud デスクトップと書類を許可
iCloud 書類の同期を許可
iCloud Freeform を許可
iCloud キーチェーンの同期を許可
iCloud メールを許可
iCloudメモを許可
iCloud写真ライブラリを許可
iCloudプライベートリレーを許可
iCloudリマインダーを許可

アカウント（制限）
アカウントパネルには、制限と（任意の）アカウント設定の両方が含まれます。制限のトグルは、ユーザー がシステムアカウントを変更できるかどうかを制御します。

アカウントの変更を許可

ネットワーク

Apple ポリシーエディタの ネットワーク セクションでは、デバイスの Wi-Fi ネットワークと VPN を構成し、証明書をインストールし、 AirDrop や Bluetooth などの接続機能を制限します。各 Wi-Fi ネットワーク、 VPN、証明書はそれぞれ独自の構成プロファイルとしてインストールされ、デバイスの 設定 > 一般 > **VPN** とデバイス管理 （ Mac: システム設定 > 一般 > デバイス管理 、または macOS 13 および 14 では プライバシーとセキュリティ > プロファイル ）と、デバイスページの プロファイル、証明書、セキュリティ パネルで確認できます。

> 証明書は 証明書_____ ページから取得します。先にそこでインポートしてください。ポリシーは証明書を参照するだけなので、証明書がポリシーにコピーされることはありません。

制限

- **AirDrop**を許可
- **AirPlay**の受信リクエストを許可
- **Bluetooth**の変更を許可
- **Bluetooth**共有の変更を許可
- ファイルのネットワークドライブアクセスを許可
- インターネット共有の変更を許可
- コンテンツ キャッシュを許可
- **iTunes** ファイル共有を許可

Wi-Fi ネットワーク

Wi-Fi ネットワークを追加 をクリックし、次を入力します :

- ネットワーク名 **(SSID)**: ネットワークの名前で、最大 32 文字です。
- セキュリティ : なし （オープンネットワーク ）、WEP、WPA または WPA2、WPA2 または WPA3、WPA3 のみ、または任意。
- パスワード : パーソナルネットワークのパスワード。
- 自動的に接続 と 非表示ネットワーク （名前をブロードキャストしないネットワーク用 ）。
- プロキシ : なし、手動 （サーバーとポート ）、または自動 （PAC ファイルの URL。空にすると WPAD でネットワーク上の設定を検索します ）。
- プロファイル名 （任意 ）と 適用先 で、ネットワークを一部のデバイスの種類に限定します。

エンタープライズネットワーク (802.1X)
ユーザーが共有パスワードではなく、自身の認証情報または証明書で認証する場合は、 エンタープライズ (802.1X)をオンにします。

認証: PEAP、TTLS(内部認証あり。たとえば MSCHAPv2)、または TLS(証明書のみ)。
デバイスユーザーの認証情報 : 各デバイスは、ユーザーページで設定されたそのユーザーの EAP
ID、匿名 ID
、パスワードを使用します。ユーザーのないデバイスには、このネットワークは適用されません。
ID、匿名 ID、パスワード : すべてのデバイスで共通です。 ID には変数 $EMAIL$、$USERNAME$
、 $FULLNAME$、$SERIAL$、$UDID$
を含めることができます。パスワードを空にすると、ユーザーがデバイスで入力します。
ID 証明書: デバイスが提示するクライアント証明書です (TLS では必須)
。以下の証明書オプションを参照してください。
信頼された証明書 : RADIUS サーバーの証明書を発行した CA
証明書です。ネットワークとともにインストールされます。
信頼されたサーバー名 : デバイスが受け入れる RADIUS サーバー証明書の名前です (たとえば
radius.example.com や *.example.com)。

VPN

VPN を追加 をクリックして、 iOS、iPadOS、 macOS に組み込まれている IKEv2 または Cisco IPSec VPN
を構成します (VPN アプリは不要です)。

種類 とサーバー 。 IKEv2 の場合はさらに リモート ID(サーバーの ID
。空の場合はサーバーアドレス)とローカル IDも指定します。ローカル ID には変数 $EMAIL$、
$USERNAME$、$FULLNAME$、$SERIAL$、$UDID$ を含めることができます。
デバイスの 認証: 証明書 (証明書ページのもの、デバイスユーザーの証明書、または SCEP
サーバーから要求したもの)、共有シークレット (IPSec の場合は任意のグループ名付き)
、またはユーザー名とパスワードのみを確認する IKEv2 サーバーの場合はなし。
信頼された証明書 : VPN サーバーの CA 証明書で、 VPN とともにインストールされます。 IKEv2 では、期待されるサーバー証明書の発行者と名前も設定できます。
ユーザー名とパスワード : ユーザーはユーザー名 (変数使用可)とパスワード (IKEv2 では EAP、
IPSec では XAuth)
でも認証します。パスワードを空にすると、ユーザーがデバイスで入力します。
VPN 名 (設定に表示されます)と適用先 。

接続

ユーザーが設定で接続 : VPN がインストールされ、ユーザーが必要に応じてオンにします。
オンデマンド : デバイスが自動的に VPN に接続します。 信頼された Wi-Fi を除く
を指定すると、リストした Wi-Fi ネットワーク (たとえばオフィスのネットワーク)では VPN

が使用されません。
常時接続 (IKEv2、監視対象の iPhone と iPad のみ): 携帯回線と Wi-Fi のすべてのトラフィックが
VPN を経由し、ユーザーはオフにできません。他のデバイスにはこの VPN は適用されません。
VPN でユーザー名を使用する場合、パスワードをポリシーで設定する必要があります。
アプリごとの VPN: 一部のアプリのみが VPN を使用します。 アプリ管理
セクションでアプリごとに VPN を選択し (アプリの VPNフィールド、 Mac では使用できません)
、必要に応じて VPN を使用する Safari ドメインをリストします。

常時接続またはオンデマンド VPN
は、先にテスト用デバイスでテストしてください。サーバーに到達できない場合、デバイスが接続で
きなくなる可能性があります。

グローバルプロキシ、暗号化 DNS、 Web コンテンツフィルタ
これらの設定はデバイスのすべてのトラフィックに適用されます。各切り替えでオンにします。

グローバル HTTP プロキシ (監視対象の iPhone と iPad、 Mac): すべての HTTP
トラフィックが、すべてのネットワークでプロキシを経由します。サーバーとポート (
任意のユーザー名とパスワード付き)、または自動構成 (PAC ファイルの URL
。空にするとネットワーク上で検索)を設定します。 Wi-Fi ログインページを許可
をオンにすると、ユーザーはプロキシを使わずに公共 Wi-Fi ネットワークにサインインできます。
暗号化 DNS: デバイスは DNS over HTTPS(サーバー URL)または DNS over TLS(サーバー名)
で、お使いの DNS
サーバーを使用して名前を解決します。必要に応じて一部のドメインのみに限定できます。監視対
象デバイスでは、ユーザーがオフにできないようにできます。
Web コンテンツフィルタ (監視対象の iPhone と iPad): iOS
に組み込まれたフィルタで、常に許可または常にブロックする Web
サイトのリストを使用してアダルトサイトを制限するか、 Web
サイトのリストのみを許可します。許可したサイトは Safari にブックマークとして表示されます。

プロキシまたは DNS
サーバーが誤っていると、デバイスが接続できなくなる可能性があります。先にテスト用デバイスで
設定を試してください。

証明書

証明書を追加 をクリックして証明書を単独でインストールします。 Safari
とアプリが信頼する必要がある認証局、またはアプリが使用する ID です。 Wi-Fi ネットワークや VPN の証明書は、ここで追加する必要はありません。

証明書のオプション

証明書ページの証明書 : すべてのデバイスで同じ証明書です。 証明書を選択
をクリックして選択します。
デバイスユーザーの証明書 :
各デバイスは、そのユーザーにリンクされたクライアント証明書を受け取ります。ユーザーに証明
書がないデバイスには適用されません。ユーザーに別の証明書をリンクすると、デバイスが更新さ
れます。
SCEP サーバーから要求 : 各デバイスが SCEP サーバー (たとえば Microsoft NDES) から独自の証明書を要求するため、秘密鍵がデバイスから出ることはありません。サーバー URL 、サーバーが必要とする場合はチャレンジ、サブジェクト (たとえば CN=$EMAIL$)
、代替名、キーサイズ、キー用途を設定します。

古い RC2 暗号化で保護されたクライアント証明書 (.p12)は、 Apple
デバイスにインストールできません。インポートする前に、 3DES または AES
暗号化で再度書き出してください。

セキュリティ
パスワードや秘密鍵を含むプロファイルは、作成対象のデバイスにのみ送信されます。デバイスは管理証明
書で要求に署名する必要があります。パスワードと証明書はログに記録されません。

ソフトウェアアップデート
Apple Policy Editorのソフトウェアアップデート
セクションは、デバイスを最新の状態に保ちます。期限までに特定の OS バージョンを要求し、デバイスがアップデートをダウンロードしてインストールする方法を制御できます。

必須の OSアップデート
必須アップデートを追加 をクリックして、 OS
バージョンを要求します。デバイスはアップデートをダウンロードし、ユーザーに期限を通知し、ユーザー がそれまでに実行していない場合は期限にインストールします。そのバージョン以降をすでに実行している
デバイスは無視します。 iOSおよび iPadOS 17または macOS 14が必要です。

適用先 （必須）： iPhoneと iPad、または Mac。各 OS
には独自のバージョン番号があるため、それぞれに 1つの必須アップデートを追加してください。 OSバージョン ：インストールするバージョン（例： 18.5、 15.4.1）。
ビルド （任意）：特定のビルド（例：ベータ、バックグラウンドセキュリティ改善）。
インストール期限
：各デバイスの現地時間での期限です。過去の日付を指定すると、デバイスはできるだけ早くアッ
プデートをインストールします。
詳細 URL（任意）：ユーザーに表示される、アップデートに関する Webページ。

デバイスは、アップデートの進行状況（ダウンロード、インストール、失敗）をデバイスページの
デバイスステータス パネルで報告します。

ソフトウェアアップデート設定
iPhoneおよび iPadのソフトウェアアップデート設定 または Macのソフトウェアアップデート設定をオンにすると、それらのデバイスのアップデートを制御できます。トグルがオフの場合、デバイスは独自
の設定を維持します。 iOSおよび iPadOS 18または macOS 15
が必要です。古いデバイスはこれらの設定を無視します。

アップデートを延期 ：新しいアップデートは、指定した日数（ 1〜90
）が経過した後にのみユーザーに表示されます。 Mac では、メジャーアップデート、マイナーアップデート、その他のシステムアップデートに異なる期
間を設定できます。

ユーザーに表示するアップデート （ iPhoneおよび iPad ）：複数のアップデートが利用可能な場合、すべてを表示するか、最も古いマイナーアップデート
のみ、または最新のもののみを表示します。
標準ユーザーがアップデートをインストールできる （ Mac）：管理者権限のないユーザーが macOSアップデートをインストールできます。
必須アップデートについてユーザーに通知
：必須アップデートとその期限に関する通知を表示します。
自動ダウンロード 、自動インストール 、自動セキュリティアップデート
：ユーザーに決定させる（ Appleのデフォルト）、または常にオンまたは常にオフにします。
バックグラウンドセキュリティ改善 ：Apple の迅速なセキュリティ修正をユーザーに提供し、ユーザーがそれらを削除できるかどうかを選択し
ます。
ベータプログラム ：ユーザーが Apple
のベータプログラムに参加できるようにするか、デバイスをプログラムから削除してブロックしま
す（ iPhoneおよび iPadでは、監視対象デバイスのみ）。

デバイスページからアップデートをイ

ンストールする
デバイスの デバイスステータス パネルには、利用可能なアップデートが一覧表示されます。
アップデートを確認 を使用してデバイスに一覧を要求し、 インストールを使用して今すぐインストールするか、ダウンロードしてユーザーにインストールさせます。これは監視対
象の iPhoneとiPad、および Macで機能します。 AppleはiOS、iPadOS、macOS 27 でこれらのコマンドを削除します。これらのバージョンではポリシーの必須アップデートを使用してくださ
い。

macOS

Apple ポリシーエディタの macOSセクションでは、 Mac
のセキュリティ、プライバシー、ログイン設定を管理します。 FileVault、ファイアウォール、 Gatekeeper 、スクリーンセーバーとロック、外部ストレージとネットワークストレージ、画面共有、プライバシー権限
、ログイン項目、および読み込みを許可するシステム拡張機能とカーネル拡張機能です。システムサービス
の構成ファイルとバックグラウンドタスクもインストールします。ポリシーの他のデバイスにはこれらの設
定は適用されません。設定を管理するにはオンにします。オフの間は、ユーザー自身の選択が維持されます
。

ほとんどの設定は構成プロファイルとして Macにインストールされ、「システム設定 > 一般 >
デバイス管理」に表示されます。 FileVault
、プライバシー権限、ログイン項目、拡張機能の設定には、ユーザー承認済み MDM
が必要です。登録 URL または QR コードで登録された Mac
では、ユーザーが「システム設定」で登録プロファイルを承認します。デバイスページの
ユーザー承認済み MDMフィールドに表示されます。ユーザーが後で承認すると、 Mac
はこれらの設定を自動的に受け取ります。

FileVault

FileVault は Macのディスクを暗号化します。この設定をオンにすると、ユーザーはパスワードで FileVault をオンにするよう求められ、 Macは個人用リカバリーキーを、組織だけに属するキーで暗号化して Cerberus Enterprise に送信します。キーはデバイスページの FileVaultフィールドで表示および変更できます (
デバイスコマンドを参照)。この設定には macOS 13 以降とユーザー承認済み MDM
が必要です。ユーザー承認済み MDM がない場合、 Macは FileVault
をオンにするよう求められませんが、ユーザーがオンにするとキーは保存されます。

ログイン時に必須 : 次回のログイン時、一定回数スキップした後 (
ユーザーはログインとログアウトのたびに再度求められます)
、またはユーザーがログアウトしたときのみ。
ログアウト時に確認しない : ユーザーはログイン時にのみ確認されます。 "ログアウト時のみ確認
"とは併用できません。
リカバリーキーをユーザーに表示 :
既定ではオフのため、管理者だけがデバイスページからキーを確認できます。
FileVault のオフを禁止 : 既定でオン。
スタンバイ時にキーをメモリから削除 : Mac
がスタンバイから復帰したときに、ユーザーは再度パスワードを入力します。
キーの保管場所 : ログインウィンドウでユーザーに表示されるテキスト (たとえば Mac
を復元するための連絡先)。既定値は "Cerberus Enterprise"です。

設定を受け取った時点ですでに暗号化されていた Macは、現在のキーを保持し、 Cerberus Enterprise はそのキーを受け取りません。キーは、ユーザーが FileVault
をオフにして再度オンにした後にのみ保存されます ("FileVault のオフを禁止 "がオフの場合)
。設定をオフにした場合や Macを管理から削除した場合でも FileVault
はオフにならず、保存されたキーは引き続き機能します。サーバーがリカバリーキーを保存するよう
に構成されていない場合、この設定は保存できません。

ファイアウォール
ファイアウォールをオン :
オフの場合、ファイアウォールはオフのままで、ユーザーはオンにできません。
すべての着信接続をブロック : 基本的なネットワークサービス (DHCP、 Bonjour、IPSec)
のみが接続を受け付けられます。
ステルスモード : Macは ping 要求や閉じたポートへの接続に応答しません。
内蔵ソフトウェアを許可 とダウンロードした署名済みアプリを許可
により、ユーザーに確認せずに接続を受け付けられます (macOS 12.3 以降)。
特定のアプリのルール : バンドル ID でアプリの着信接続を許可またはブロックします。

Gatekeeper
Gatekeeper はアプリを開く前に確認します。 Macで App Store
のアプリのみを開くか、識別された開発者のアプリも開くかを選択します。 Gatekeeper
がオフの場合、署名されていないアプリや破損したアプリも含め、すべてのアプリを開けます。 macOS 15 以降では、ブロックされたマルウェアを Apple
に送信するかどうかをユーザーに確認するかも選択できます。

スクリーンセーバーとロック
一定時間操作がない後にスクリーンセーバーを開始し、スクリーンセーバーの開始時またはディスプレイの
スリープ時に、すぐにまたは遅延後にパスワードを要求します。 管理対象外
のままにした設定は、ユーザー自身の選択が維持されます。

外部ストレージとネットワークストレ

ージ

Macの外部ストレージ (USB ドライブ、 SD カード、外付けディスク)とネットワークストレージ (ファイル共有)を許可、読み取り専用、またはブロックします。 macOS 15 以降が必要です。

画面共有
画面共有でこれらの Macに接続するユーザーの制限 : Mac
との間のファイルコピー、高パフォーマンス接続、仮想ディスプレイの数です。画面共有をオンにするかは
、ユーザー自身の選択に委ねられます。 macOS 14 以降が必要です。

プライバシー権限
ユーザーが通常「システム設定 >
プライバシーとセキュリティ」で許可するアクセスを、アプリに付与または拒否します。たとえば、バック
アップアプリにフルディスクアクセスを許可したり、アプリにカメラへのアクセスを拒否したりします。権
限ごとに次を選択します :

権限:
フルディスクアクセス、アクセシビリティ、オートメーション、フォルダ、連絡先、カレンダー、
写真、カメラ、マイク、画面収録、その他の「プライバシーとセキュリティ」の項目。
アクセス :
許可または拒否します。カメラ、マイク、画面収録、入力監視はプロファイルで許可できず、拒否
のみ可能です。画面収録と入力監視では、管理者権限なしでもユーザーが許可できるようにできま
す。
アプリ: アプリのバンドル ID、またはプログラム (たとえばコマンドラインツール)のパス。
コード要件 : 署名によってアプリを識別します。ターミナルで codesign -dr - /Applications/Example.app を実行して取得し、 designated => の後のテキストをコピーします。
オートメーション では、制御対象のアプリ (たとえば Finder)とそのコード要件も必要です。

ログイン項目とバックグラウンド項目
ルールに一致するログイン項目とバックグラウンド項目は管理されます。確認なしで実行され、ユーザーは
「システム設定 > 一般 > ログイン項目」でオフにできません。ルールは、アプリの開発者チーム ID
、バンドル ID、または launchd デーモンやエージェントのラベル (先頭部分でも可)に一致します。 macOS 13 以降が必要です。

システム拡張機能

システム拡張機能は、アプリが macOS を拡張するための最新の方法です。ネットワークフィルタや VPN
、エンドポイントセキュリティエージェント、ドライバなどがあります。この設定をオンにすると、リスト
された開発者チームのシステム拡張機能が、ユーザーに確認せずに読み込まれます。 macOS 10.15 以降とユーザー承認済み MDM が必要です。

チーム ID: 開発者の 10 文字のチーム ID です (たとえばアプリの "Signed by"の詳細、または
codesign -dv で確認できます)。各チームは 1 回だけ指定できます。
許可: チームのすべての拡張機能、またはリストされたバンドル ID の拡張機能のみ。
種類:
チームをドライバ、ネットワーク拡張機能、エンドポイントセキュリティ拡張機能に制限します。
何も選択しない場合、すべての種類が許可されます。
削除 (リストされた拡張機能のみ): アプリが管理者なしで拡張機能を削除できる (macOS 12 以降) 、システム整合性保護がオンの間は拡張機能をオフまたは削除できない、または「システム設定」
と Finder で削除できない (macOS 15 以降)のいずれかです。古い macOS の Mac
では、削除オプションなしで拡張機能を引き続き許可します。
ユーザーが他のシステム拡張機能を承認できる :
既定でオン。オフの場合、プロファイルで許可された拡張機能のみが読み込まれます。 Mac
上のいずれかのプロファイルでオフにすると、オフになります。

macOS 11.3 以降では、この設定を削除すると、許可していたシステム拡張機能 (たとえばセキュリティエージェントやネットワークフィルタ)
がオフになります。これは、設定をオフにしたとき、ポリシーを削除したとき、および Mac
がこの設定のないポリシーに移動したときに発生します。エディタは設定をオフにする前に確認を求
めます。

カーネル拡張機能 (レガシー)
カーネル拡張機能は、 macOS
を拡張するための古い非推奨の方法です。ベンダーが提供している場合はシステム拡張機能を優先してくだ
さい。リストされたチームのカーネル拡張機能 (チームのすべての拡張機能、またはリストされたバンドル ID のみ)は、再起動後にユーザーに確認せずに読み込まれます。 macOS 10.13.2 以降とユーザー承認済み MDM が必要です。

ユーザーが他のカーネル拡張機能を承認できる :
既定でオフのため、リストされたチームのみがカーネル拡張機能を読み込めます。
標準ユーザーも承認可能 :
ユーザー承認がオンの場合、管理者権限のないユーザーも承認できます (macOS 11 以降)。

Apple silicon のMacでは、プロファイルだけでは不十分です。誰かが Macを recoveryOS で起動し、「起動セキュリティユーティリティ」で「低いセキュリティ」を選択し、識別された開発
者のカーネル拡張機能のユーザー管理を許可する必要があります。また、承認のために Cerberus

Enterprise に委託された Bootstrap Token が必要な場合があります (デバイスページの Bootstrap
Token フィールドを参照)。

Mac ファイル
サービス構成ファイルとバックグラウンドタスクは、組織の Mac ファイル
にアップロードしたファイルを使用します。 zip アーカイブとプロパティリスト (.plist)で、最大 20 MB
です。 macOS セクションの Mac ファイル ボタン、または設定の ファイルを選択
から、アップロード、使用箇所の確認、削除ができます。ポリシーで使用中のファイルは削除できません。
ファイルを変更するには、新しいバージョンをアップロードしてポリシーで選択します。 Mac はそれを再度ダウンロードします。

サービス構成ファイル
zip アーカイブからシステムサービスの構成ファイルをインストールします。組み込みのサービスは、 SSH サーバー (sshd)、sudo、 PAM、印刷 (CUPS)、Apache Web サーバー、 bash、zsh
、スマートカードログイン、認証です。 com.example.service のような逆 DNS
識別子を持つ独自のサービスも使用できます。 macOS
の管理対象構成ファイルライブラリでファイルを検索します。各サービスには 1 つの設定を指定できます。
macOS 14 以降が必要です。

組み込みサービスはアーカイブ内のファイルのみを使用し、独自のファイル (たとえば sshd の /etc/ssh)
は無視します。構成全体をアーカイブに含め、ディスクのルートから始まるフォルダに配置してくだ
さい (たとえば etc/ssh/sshd_config)。ファイルは Mac
上では読み取り専用で、設定とともに削除されます。最初に 1 台の Mac
でアーカイブをテストしてください。 sudo や PAM
の構成が誤っていると、ユーザーがサインインできなくなったり、管理者権限を使用できなくなった
りします。

バックグラウンドタスク
launchd
によって開始され、バックグラウンドで実行されるプログラムとスクリプトです。ユーザーはオフにできず
、設定とともに削除されます。 macOS 15 以降が必要です。タスクごとに次を選択します :

タスク識別子 : com.example.task のような逆 DNS 識別子で、タスクごとに異なります。

プログラムとスクリプト (任意): Macが /var/db/ManagedConfigurationFiles/BackgroundTaskServices/Services/
の後にタスク識別子を付けた場所に展開する zip
アーカイブです。ファイルの実行権限を保持し、プロパティリストを含めないでください。
launchd プロパティリスト : プログラムを開始するジョブで、デーモン (システム全体、 root として)またはエージェント (各ユーザーセッション内)
として読み込まれます。プログラムは上記のフォルダ内のパスで指定します。

タスクには、プログラムまたは少なくとも 1 つのプロパティリストが必要です。ファイルが変更されると、
Macはタスクを再起動します。

位置情報とジオフェンス
Apple ポリシーエディタの 位置情報とジオフェンス
セクションでは、敷地や倉庫などのエリアを定義します。 Cerberus Enterprise アプリをインストールした iPhone と iPad
は、これらのエリアへの入場または退場を報告し、イベントルールでそれに対応できます。メールを送信す
る、デバイスをロックまたは無効化する、または再び有効化するなどです。 Mac
はジオフェンスを使用しません。

ジオフェンスのフィールド
ジオフェンスを追加 を使用して新しいエントリを作成します。ポリシーには最大 10 個のジオフェンスを含めることができ、名前はポリシー内で一意である必要があります。各ジオフェンスには次のフィールド
があります :

名前: 必須で、一意である必要があります。
緯度 と経度: エリアの中心です。マップをクリックして設定することもできます。
半径 (m): 必須で、 200から 10000メートルの範囲です。
説明: 管理者向けの任意のメモ。
入場を報告 と退場を報告 : 生成するイベントを選択します。少なくとも 1
つはオンのままにする必要があります。
有効: ジオフェンスを削除せずに有効または無効にします。

各ジオフェンスにはマッププレビューがあります。保存済みジオフェンスの中心と半径はロックされていま
す。変更するには、マップのロックボタンを使用します。その他のボタンは、マップをエリアまたは現在地
に中央表示します。

ポリシーを保存すると、 Cerberus Enterprise はポリシーの iPhone と iPad
に新しいジオフェンスを取得するよう要求します。通常は数分かかりますが、 iOS
が遅延させる場合があります (低電力モードやネットワーク接続がない場合など)
。アプリが最新のジオフェンスをまだ適用していない場合、デバイスページに表示されます。

要件
ジオフェンスは、 Cerberus Enterprise アプリをインストールした iPhone と iPad で動作します。 Mac は無視します。デバイス上では次の条件が必要です :

- Cerberus Enterprise [redacted] (Cerberus [redacted])
  [redacted] ;
- [redacted] [redacted] ;
- [redacted] [redacted] ;
- [redacted] **App** [redacted]

[redacted] ([redacted])[redacted]
Cerberus [redacted] ([redacted])
[redacted]
[redacted]
[redacted] Cerberus Enterprise
[redacted] iOS
[redacted]
[redacted] MDM
[redacted] (Apple [redacted])[redacted]

[redacted] [redacted] iOS
[redacted]
[redacted] (
[redacted])[redacted]

[redacted]

iOS [redacted] (
[redacted])
[redacted]
[redacted] iOS [redacted]

[redacted] ([redacted])
[redacted]
[redacted] 1 [redacted]

[redacted] iOS
[redacted] iOS [redacted]

[redacted]

[redacted] [redacted] [redacted] [redacted]
[redacted]
[redacted]
[redacted] [redacted] [redacted] [redacted] [redacted] **App**

更新 がオフ、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だった、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、などです。

ジオフェンスの遷移と位置情報は 90日間
保持され、それより古いデータ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、マップに表示され続けます。

制限事項
ポリシーをコピーしてもジオフェンスはコピーされません。コピー先で再度追加してください。
iPhone と iPad のジオフェンスイベントはベストエフォートです。 iOS
がアプリを実行できるタイミングを決定します。

ジオフェンスイベントに対応するには、 デバイスがジオフェンスに入った または

デバイスがジオフェンスから出た のイベントルールを作成します。詳細は イベントルール
をご覧ください。

アカウント
Appleポリシーエディターの アカウント セクションでは、メール、 Exchange、Google 、カレンダー、連絡先、ディレクトリのアカウントを iPhone、 iPad、 Macに追加します。
アカウントを追加 をクリックし、種類を選択します。このセクションには、 アカウントの変更を許可
制限（監視対象デバイス）も含まれます。

Mac（ macOS 13以降）では、アカウントは管理に登録されたユーザー（通常は Mac を登録したユーザー）のセッションに、そのユーザーがログインしているときにインストールされま
す。デバイスページでは、これらのユーザーが Macユーザー の下に、アカウントの状態とともに一覧表示されます。デバイスユーザーからメールアドレスを取得
するアカウントは、 Cerberus EnterpriseでMacに割り当てられたユーザーを使用します。

共通設定
デバイスユーザーの名前とメール （メール、 Exchange、Google
）：各デバイスは、ユーザーページで設定されたそのユーザーの名前とメールアドレスを使用しま
す（ Googleの場合、ユーザーの Google
アカウント）。ユーザーのいないデバイス、またはユーザーにメールアドレスがないデバイスには
、アカウントは配信されません。それ以外の場合は、固定のメールアドレスと氏名を設定します。
アカウント名 （任意）：設定およびアプリ内でのアカウントの名前。
ユーザー名 とパスワード （任意）：ユーザー名には変数 $EMAIL$、$USERNAME$、 $FULLNAME$、$SERIAL$、$UDID$
を含めることができます。パスワードを空にすると、ユーザーがデバイスで入力できます。両方を
空にすると、ユーザーが両方を入力できます。
適用先 ：アカウントを特定のデバイスの種類に限定します。

アカウントの種類
メールアカウント ： IMAPまたは POP の受信サーバーと送信サーバー、およびそれぞれのポートと認証。送信サーバーは、受信サーバー
と同じユーザー名とパスワードを使用できます。
Exchangeアカウント （Exchange ActiveSync ）：サーバー。空欄にすると、メールアドレスから検索します。サービス（メール、連絡先、カレ
ンダー、リマインダー、メモ）と、ユーザーがそれらを変更できるかどうかを選択します。
最新の認証（ OAuth） では、ユーザーは IDプロバイダー（ Microsoft 365

など）のページでサインインします。 認証証明書 （ iOS 17
以降）は、証明書でデバイスを認証します。
Googleアカウント ：ユーザーは指定されたメールアドレスで Google アカウントにサインインします。
カレンダーアカウント（ CalDAV） と連絡先アカウント（ CardDAV）：サーバー、ポート、パス。
ディレクトリ（ LDAP）
：サーバーとポート、および連絡先の検索に使用する検索（検索ベース、スコープ、説明）。
購読カレンダー ：カレンダーの URL（ https、http、webcal）。

S/MIME

メールおよび Exchangeアカウントは、 S/MIME（iOS 17 以降）でメッセージに署名および暗号化できます。それぞれについて、証明書を選択します：証明書ページのいずれか、デバイスユーザーの証明書、または SCEP サーバーから要求した証明書。ユーザーがオフにできるようにしたり、別の証明書を選択できるようにしたり、暗号化についてメッセージごとに切り替えを表示したりできます。

セキュリティ
パスワードと証明書は、デバイスに送信される設定には含まれません。各デバイスは、管理証明書でリクエストに署名して、 Cerberus Enterprise から独自の認証情報をダウンロードします。これらはログには記録されません。

コンプライアンスルール
Apple ポリシーエディタの コンプライアンスルールセクションでは、ポリシーのデバイスに対する要件を設定します。ルールに違反したデバイスは直ちに非準拠になります。デバイスページの デバイスが非準拠である理由に理由が表示され、デバイスリストでは非準拠として表示されます。ポリシーの設定をデバイスに適用でき
ない場合も、そのデバイスは非準拠になります。

ルール
パスコード : デバイスにパスコードがあり、ポリシーのパスコード設定を満たしていること。
最小 OS バージョン : iPhone と iPad 用、または Mac 用です。デバイスを更新するには、ソフトウェアアップデートで必須のアップデートを追加します
。
監視対象デバイス :
登録プロファイルまたはユーザー登録で登録されたデバイスは監視対象ではありません。
FileVault オン (Mac): Macのディスクが FileVault
で暗号化されていること。他のデバイスには影響しません。

ルールは、デバイスがステータスを送信したとき、ポリシーが保存されたとき、および 1 時間ごとにチェックされます。ステータスが不明なデバイス (たとえば FileVault をまだ報告していない Mac) は、ルールに違反しません。

デバイスのブロック
まだ非準拠の場合にデバイスをブロック をオンにし、何日後にブロックするかを設定します (0
は即時ブロック)。監視対象の iPhone と iPad
は、設定したメッセージとともにロストモードになります。その他のデバイスは一度ロックされます。 Mac は再起動し、 PIN の入力を求められます。 PIN はコマンド履歴のコマンド詳細に表示されます。

ブロック解除 : デバイスが再び準拠すると、ロストモードが自動的にオフになります。
ロストモードを手動でオフにする :
デバイスが再び準拠し、再びルールに違反するまで、デバイスはブロックされません。ユーザーに
デバイスを修正させる場合に使用します。

通知を受け取ったり、別の方法で対応したりするには、 デバイスが非準拠になったのイベントルールを作成します。理由も取得できます。