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。

Revision #6
Created 2026-11-10 15:16:18 UTC by Admin
Updated 2026-11-12 09:55:47 UTC by Admin