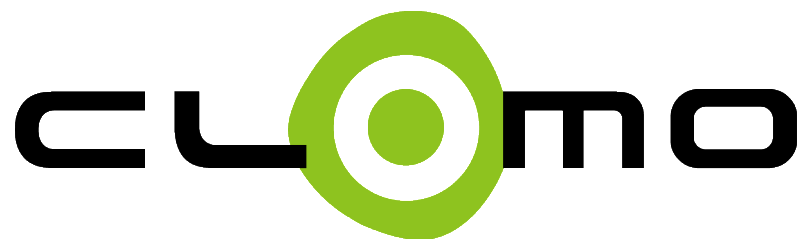


**Mobile
Solution
Market**



CLOMO MDM

スマートデバイスのリモート管理・運用環境のご提案

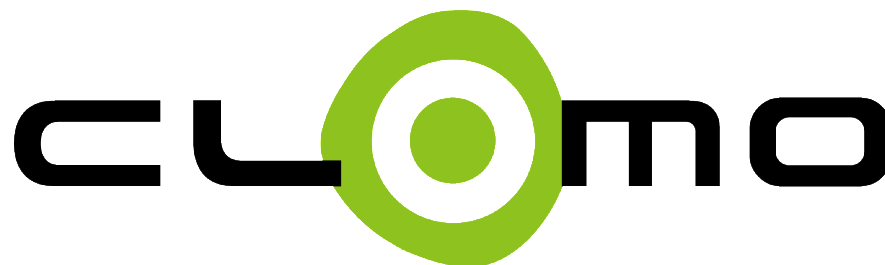
スマートデバイスを ビジネスの武器にしよう

いつでも、どこでも、誰にでも使えるスマートデバイスが、私達の働き方を大きく変えようとしています。メール、メンバーのスケジュールや連絡先、最新の提案資料、社内システム等、ビジネスに必要な全ては、いつでも手の中にあります。もはやデスクに縛られることはありません。時間に縛られることはありません。

私たちはモバイルの力で、ビジネスをもっと自由に、ワクワクする姿へ変えるため CLOMO と モバイル&クラウドソリューションを提供しています。



スマートデバイスをビジネスの武器に



スマートデバイスをビジネスの武器とするためには、セキュリティや管理・運用、緊急対策など、様々な課題解決が必要です。CLOMOでは、導入から活用まで、スマートデバイスのビジネス活用を支援しています。



スマートデバイス、 アプリを管理・運用する

デバイスとアプリ、どう運用・管理する？

- 盗難 / 紛失時の対策手段を持つ
- IT ポリシーに準拠して運用する
- 大量デバイス / アプリを効率的に管理する
- 不正改造防止やウィルス対策を実施する
- 緊急時の体制を持つ
- 有償アプリのライセンスを管理する

CLOMO MDM



アプリを活用する

ビジネスアプリ、必要なことは？

- メーカーやブラウザ、基本から始める
- 社内ファイルを安全に共有する
- 予定を効率的に共有する
- アプリ内のデータを保護する
- IT ポリシーに準拠して運用する

CLOMO SECURED APPs

モバイル管理のスタンダード



※出典:デロイト トーマツ ミック経済研究所「コラボレーション/コンテンツ・モバイル管理パッケージソフトの市場展望」2011～2018年度、「ミックITリポート2020年12月号」2019年度出荷金額実績および2020年度出荷金額予測



CLOMO MDM

スマートデバイスのリモート管理・運用環境



🔍 利用状況の監視

- シリアル番号
 - 電話番号
 - インストールアプリ
 - 位置情報
- など

⚙️ 運用効率化

- カメラ使用禁止
 - パスコードポリシー
 - App Store 利用禁止
- など

🔒 盗難/紛失時の対策

- リモートロック
 - リモートワイプ
 - 紛失モード設定*
- など

CLOMO MDM Agent
CLOMO MDM でのデバイス管理にはエージェントアプリのインストールが必要です



- ・iOS : 任意
- ・Android : 必須
- ・macOS : 不要
- ・Windows : 任意

* : iOS、Android向け機能となります。



※タブレット端末以外にも対応済みです。

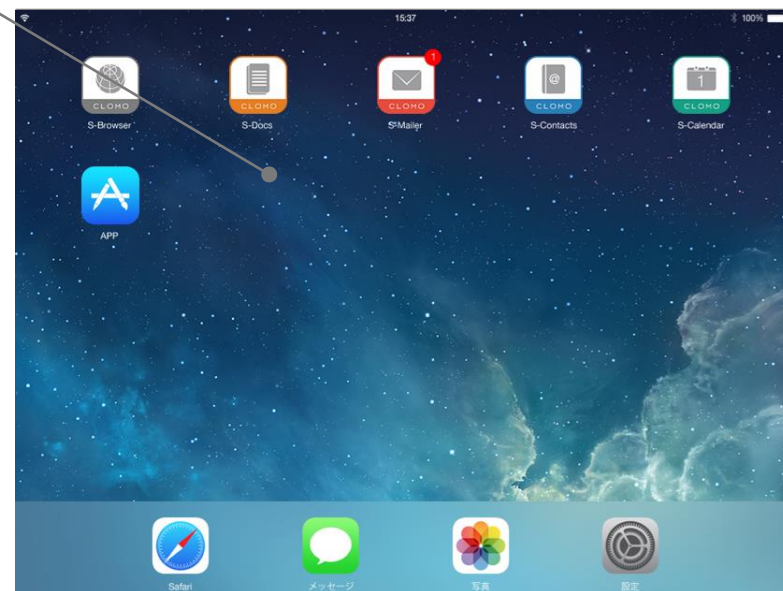
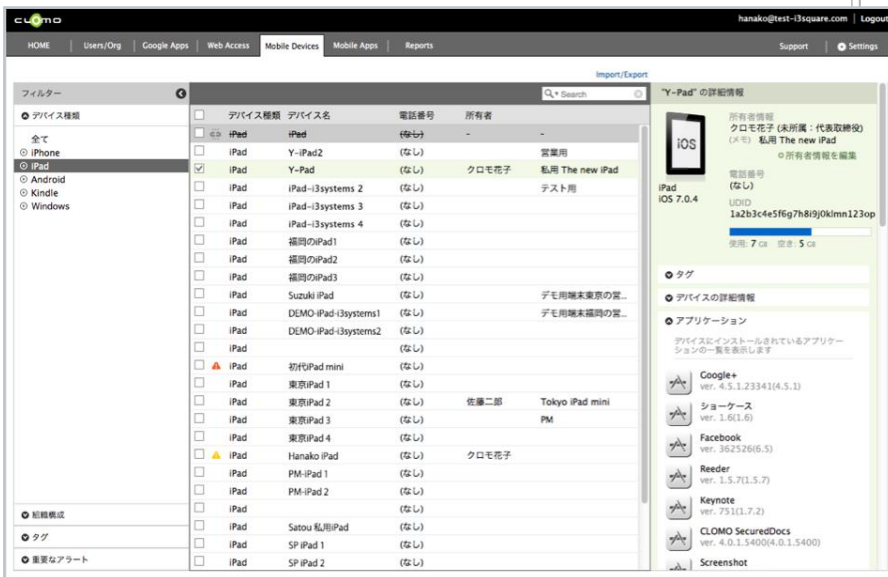
1 いつでも・どこでも・安心して使える

社外に持ち出すスマートデバイスの盗難・紛失リスクに対して、リモートで「デバイスのロック」「デバイス内のデータ削除」を行え、業務データの情報漏えいを防ぎます。

2 手軽に、ビジネスに最適なデバイスを実現する

カメラやメーラー等、標準アプリの利用制限やパスコードの強制設定などをリモートで行えます。

例えば、ある部署では、カメラ撮影を制限するなど、部署のセキュリティレベルに応じたデバイスを手軽に用意できます。



3 リスクの把握・改善で、スマートデバイスをビジネスの武器にする

デバイスやアプリの利用状況（デバイスにインストールされているアプリや OS バージョンなど）をリモートで一元的に把握し、状況に応じてデバイスやアプリの配布を改善できます。また、ウィルス感染や root 化など、重大な危機を検知してアラートするので早急な対策も行えます。



CLOMO MDM 主要機能			CLOMO MDM 管理パネルの特長
スマートデバイス運用効率化 デバイス・アプリの機能制御・自動適用  デバイス・アプリの機能制御や、ネットワークの接続制御などを行います。組織や部門に設定したITポリシーの自動適用も可能です	利用状況の監視 デバイス・アプリ情報の取得  OS、電話番号などのデバイス基本情報や利用中アプリの名称・バージョン等を取得します	盗難・紛失対策 デバイスの起動ロック / 初期化  デバイスの起動ロックや、データ削除を行います ※24 / 365 での代行サービスをオプションとして提供しています	管理者にやさしいUI / UX設計  管理者の管理・運用コスト低減のために、使い勝手にこだわったUI / UX を提供します
アプリの配信・管理  大容量アプリ、有償アプリなど、多種多様なアプリの配信・管理を行います ※各種オプションサービスのお申込みが必要です	ステータスの確認  Root 化の検知や、MDM 管理下にあるかの状況確認と通知をします	盗難・紛失時の簡易対策  メッセージ通知や位置情報の検知など、デバイスのロック / 削除を行う前に利用される機能を提供します	マルチOS・デバイス  iOS / macOS / Android / Windows など、多種多様なOSを問わず一元管理できます。
管理者機能の階層化  全権限を持つ「管理者」の下に管理権限を制限した管理者を設定し、管理権限を委譲できます	デバイス管理と完全統合されたウイルス対策  ウィルス感染の脅威を検知した場合、すぐに通知します ※Android デバイスのみのサービスとなります ※各種オプションサービスのお申込みが必要です	電子証明書連携  電子証明書の強制インストールが可能で、第三者の不正利用を防止します ※各種オプションサービスのお申込みが必要です	マルチキャリア  3G / LTE / Wi-Fiデバイスなど、様々なデバイスを、一元的に管理できます



簡単に管理できます

組織情報に沿ったデバイス選択や、操作を覚えやすい UX 等、管理者にやさしい UI / UX 設計を行っています。さらに、マルチデバイス・マルチキャリアを一元管理できる為、管理デバイスの急な変更にも対応できます。



管理者にやさしい
UI / UX 設計



マルチOS
マルチデバイス



マルチキャリア

スマートデバイスの運用効率を高めます

デバイス・アプリの機能制御や、パスコードの強制設定など、様々なITポリシーの反映や、多種多様なアプリの配信・管理をリモートで行えます。さらに、管理者権限の委譲を行えるため、適切な役割分担のもと、目的に沿った運用を効率的に実現できます。

※ アプリの管理・運用には、CLOMO MOBILE APP PORTAL の申込みが必要です。



デバイス・アプリの
機能制御・自動適用



管理者機能の階層化



アプリの配信・管理

利用状況の監視で、素早く対処できます

管理者の設定にあわせて、デバイス・アプリの基本情報や利用状況を取得する他に、Root 化される、ウィルスに感染する等、重大なトラブルに発展する可能性があるデバイスを検知でき、素早い対処が行えます。

※ ウィルス対策は Android デバイス向けのサービスとなり、ご利用には CLOMO MDM アンチウィルスオプションの申込みが必要です。



デバイス・アプリ
情報の取得



ステータスの確認



デバイス管理と完全統合
されたウィルス対策

盗難・紛失時にも安心です

盗難・紛失が起きても、位置情報の検知やメッセージ通知といった簡易対策から、デバイスの起動ロック・初期化や、電子証明書の失効などの確実な対策まで、業務データの漏えいを防ぐ為に様々な対策を行えます。

※ 電子証明書の利用には、CLOMO MDM 電子証明書連携オプションの申込みが必要です。



デバイス・アプリ
情報の取得



ステータスの確認



デバイス管理と完全統合
されたウィルス対策



デバイス・アプリの準備が簡単です

部署異動や、利用アプリの見直しなど、スマートデバイスの環境を変更する必要が生じた時にも、管理者がリモートで環境を整備できるため、ユーザーによる調整の手間が必要最低限で済み、ストレスを感じさせません。



デバイス・アプリの
機能制御・自動適用



アプリ / アプリ設定の
配布・管理

安心して利用できます

様々な盗難・紛失対策が可能なため、ユーザーは安心してスマートデバイスを業務に活用できます。メールで受け取った最新の資料を外出先の商談で提示する、外出先で商談管理システムにアクセスして商談報告をリアルタイムで行うなどを安心して行えます。



デバイスの
起動ロック / 初期化



盗難・紛失時の
簡易対策



電子証明書連携

CLOMO MDM 管理パネルの利用イメージ

ver. 20210202



ブラウザからアクセスするだけで簡単に使える管理パネル

CLOMO MDM Management Panel Screenshot

Navigation: HOME | Users/Org | Google Apps | Web Access | **Devices** | Applications | Reports

Top Right: hanako@navy-square.com | Logout

Right Side Links: FAQ | Support | Settings

Current View: Devices

Filter: 現在の表示条件を保存 | Import/Export

デバイス種類	デバイス名	モデル名	電話番号	所有者	デバイス管理状態
☐	iPod	HW-0218	iPod	(なし)	管理中
☐	iPad	HW-0125	iPad	(なし)	管理中
☐	iPhone	HW-0497	iPhone	(なし)	管理中
☐	Windows	Windows phone	NEO	(なし)	管理中
☐	macOS	HW-0590	MacBook Pro	(なし)	管理中
☐	Kindle	apollo	KFAPWI	(なし)	管理中
☒	iPhone	HW-0619	iPhone	080	管理中

Device Details for HW-0619:

- OS: iPhone iOS 11.3
- Status: 監視対象
- Alert: アプリ利用ポリシー違反が検知されました
- Owner: クロモ二郎 (営業企画部)
- Type: (メモ) DEPデバイス
- Phone Number: 080
- UDID: 9a2a9a5c50af72769b26ba9ebc90
- Storage: 使用: 10 GB, 空き: 45 GB
- Tags: タグ
- Actions: デバイスの詳細情報, CLOMO アプリケーション, アプリケーション, アプリ管理設定プロファイル, プロビジョニングプロファイル, 位置情報履歴



操作1

対象の区分を選択

「区分情報」から操作したい端末が所属している「組織」や「OS」を選択します



操作2

一覧からデバイスを選択

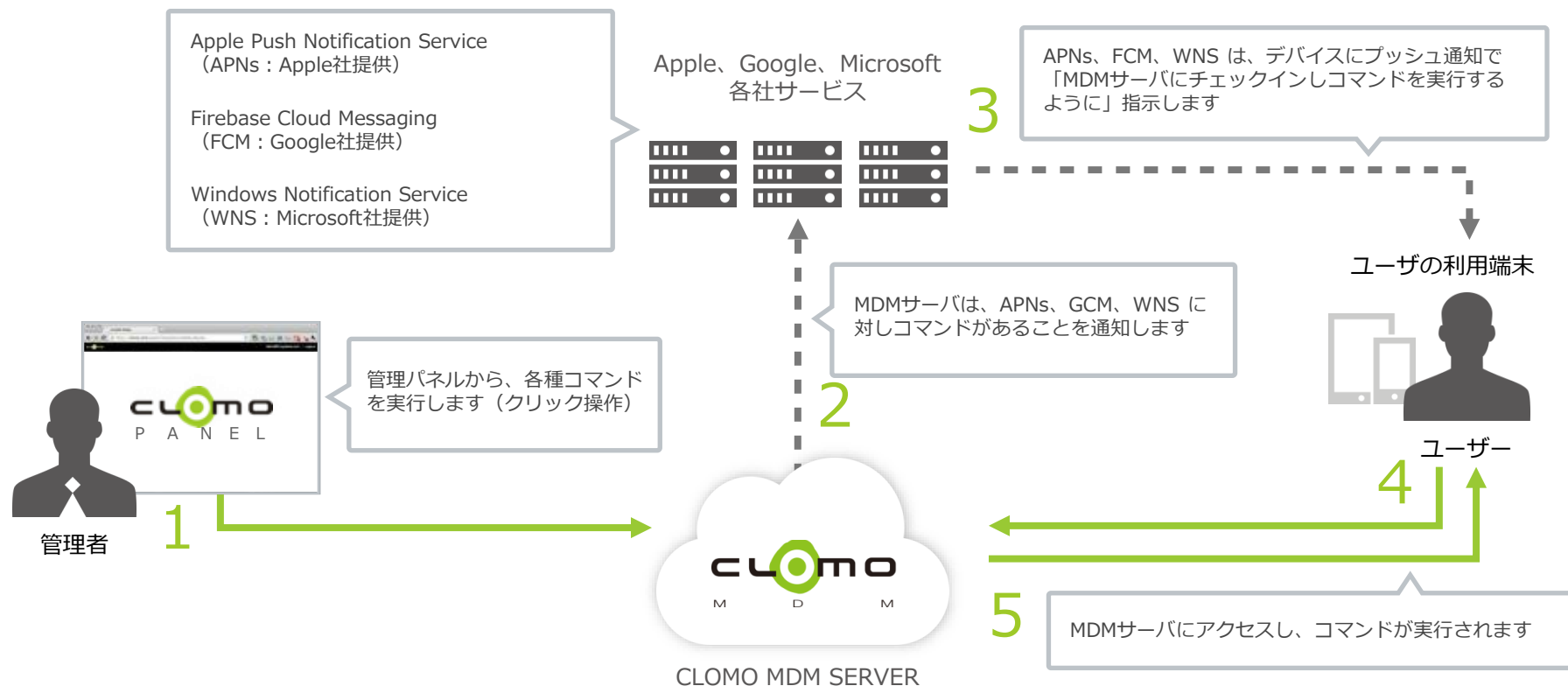
選択部署の「デバイス一覧情報」のリストから、任意のデバイスを選択します



操作3

コマンドを実行

「デバイス詳細情報」画面で情報の閲覧・設定の変更・コマンドの実行を行います



クラウドサービスだから導入・運用もスムーズ & スピーディー



3営業日以内に提供開始

ハードウェアやサーバを購入する必要なく、お申込から数日で提供可能です



柔軟なスケーラビリティ

5台から10,000台をこえる大規模運用まで、クラウドなのでサーバ増強など、お客様の作業は不要です



Windows Update 設定管理に対応

- Windows 10における強制アップデートをコントロール -

オンプレにサーバーを建てず、CLOMO PANELだけで、OSアップデートの管理運用ができます。
アップデートを延長／自動インストールタイミング／再起動のタイミングなどの設定ができます。

Windows 10 Update 設定プロフィール登録

一般設定

プロフィール名 *

90日遅延/ノートPC用

説明

サービス種別

利用するアップデートサービスの種別により制御可能な項目が異なります。

サービス種別

☒ Microsoft Update(MU)

☐ Windows Server Update Services(WSUS)

MU

機能の更新や品質の更新プログラムを PANEL 上で制御する場合に選択します。

WSUS

WSUS の更新制御を利用する場合に選択します。

Windows Update

機能更新プログラムポリシー

☒ 設定しない

☐ 設定する

大型アップデートプログラムの更新を制御できます。

品質更新プログラムポリシー

☒ 設定しない

☐ 設定する

セキュリティ問題や製品の不具合を修正するためのプログラム更新を制御できます。

WSUSポリシー

☒ 設定しない

☐ 設定する

※ WSUSサービスを選択している場合のみ選択可能です。
WSUSで設定した更新プログラムの内容を利用して制御できます。

設定

全般

基本情報

CLOMOアカウント設定

カスタムユーザー情報設定

ジオサイト設定

スケジュール設定

カスタム管理権限スキーム設定

サービス構成設定

サービス設定

Wi-Fi

VPN

プロフィールの作成

✓ プロファイルの種別を選択してください

Windows 10 デスクトップ設定プロフィール

Windows 10 Update 設定プロフィール

デバイス設定プロフィール

パスワードポリシー設定プロフィール

Windows Phone 設定プロフィール

社内アプリケーション等の検証後にOSのアップデートが可能となります。

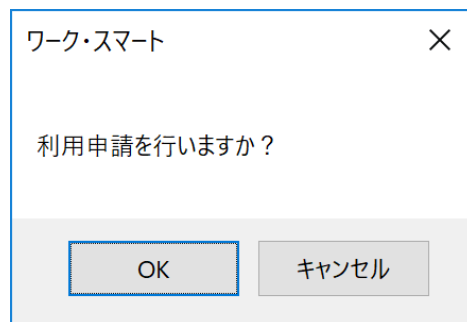
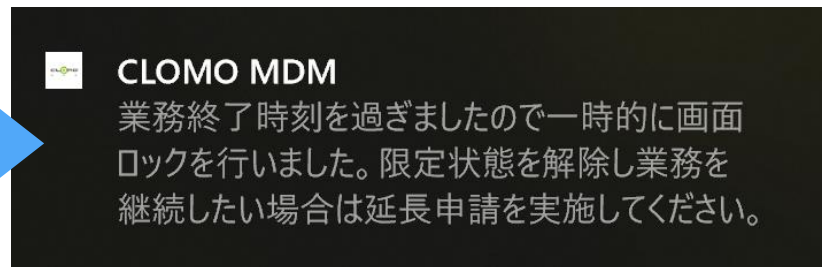


CLOMO MDM for Windowsにも「ワーク・スマート」を搭載

- 企業が把握していない「隠れ残業」を徹底抑止し、「働き方改革」「健康経営」をサポート -

CLOMO MDM Agentから一時制限解除が可能です。

解除実績はサーバー側で保管される為、定期的を確認することにより利用者のデバイス利用実態の把握も可能です。



※ 本機能を利用するには「Winodws : MDM Agent for Windows 3.0.0 以降のインストールが必要となります」



CLOMO MDM Android Enterprise Recommended を取得 グローバルで9社の1社

- Android™ 端末に企業向けの高度なセキュリティ対策を実現 -



仕事専用
DeviceOwnerモード

端末を完全に管理
広範囲なポリシーを適用し、端末を厳格に管理できます。このモードでは、企業所有の端末のアプリやデータを完全に管理することが可能です。



個人利用も可能
COMPモード

1 台の端末でプライベートも仕事も
Android Oreoなら、端末をさらに柔軟に管理することが可能です。企業所有の端末で仕様用プロファイルを使用すると、個人のアプリやデータを分離して管理できます。

特定の用途
Dedicated Device (専用端末) モード

用途に特化した端末を導入
端末を特定の社員用に導入したり、顧客対応業務向けに導入しあります。IT担当者は、セーフモードによる起動を制限したうえで、ロック画面、ステータスバー、キーボード、画面を盛装する他、アプリやアップデートをリモートで適用することも可能です。

本対応の詳細 : <https://www.i3-systems.com/mdm-android-enterprise/>



Android デバイスの持ち出し禁止機能

大型商業施設を運営する企業などで、施設内で使用する目的でAndroidデバイスを配布する際に所定の場所から出た際に、そのデバイスを利用できないようにします。

以下のセキュリティリスクを防止／軽減し管理者様の負担も軽減します。

- ・ 従業員による意図しない持ち出しからの情報漏えい
- ・ 利用を許可しない場所での端末利用

利用可能な施設位置・範囲を設定

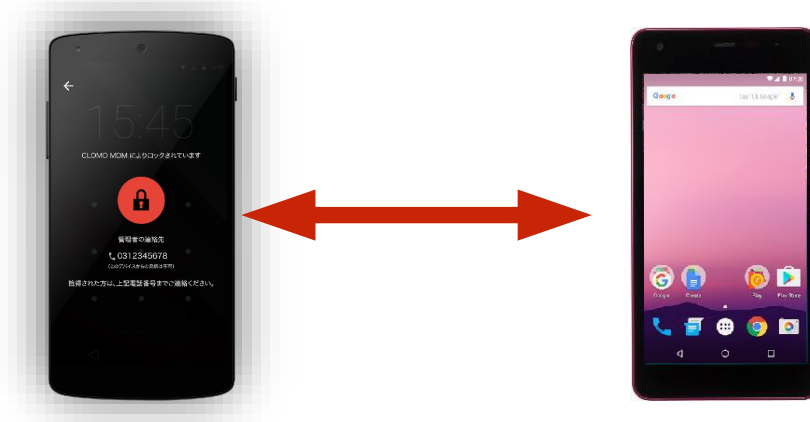
複数施設が存在
一つの企業で複数の施設がある場合、
複数のジオフェンスポイントを設定可能とします。



使用禁止・使用許可を自動化

利用可能範囲外
デバイスの位置を自動感知し、利用可能範囲外へ
出た場合、デバイスを自動ロックを行います。

利用可能範囲内
デバイスを再び利用可能範囲内へ持ち込むことに
より自動的にデバイスの使用を可能とします。





国内初、CLOMO MDM、スマートフォン、 タブレットの紛失対策強化機能を提供

iOS : 設定時の挙動

- ・ 解除不可な強制ロック
- ・ 任意のメッセージを強制表示
- ・ 任意の連絡先情報を強制表示
- ・ 位置情報を強制取得



Android : 設定時の挙動

- ・ 指定パスコードで強制ロック
- ・ 任意のメッセージを強制表示
- ・ 任意の連絡先情報を強制表示
- ・ 位置情報を強制取得



※ 本機能を利用するには「iOS : iOS 9.3.2以上、監視対象設定デバイスであること」「Android : Android OS 2.3 以上」を満たしている必要があります。
 ※ 紛失モード設定時に位置情報を取得する際に、Androidの場合は位置情報サービスをONにしている必要があります。



CLOMO MDM Agent for iOS

iOS デバイスで CLOMO MDM をご利用になる場合、CLOMO MDM Agent for iOS をインストールすることで、より高度な機能をご利用頂けます。エージェントアプリは、App Store からダウンロードできます。(App Store : <http://goo.gl/hmI8to>)

- ※ CLOMO MDM Agent for iOS をインストールせずに CLOMO MDM を運用いただくことも可能ですが、位置情報取得など、エージェントアプリが提供する機能はご利用いただけません。
- ※ Apple Developer Enterprise Program (IDEP) に加入頂くことでご利用頂ける、柔軟な運用が可能なエージェントアプリ CLOMO MDM Agent for iOS Enterprise も提供しています。

▶ CLOMO MDM Agent for iOS の機能

- 位置情報の取得
- メッセージの通知
- ワーク・スマート
- JailBreak 検知
- アップデート時のプッシュ通知



CLOMO MDM Agent for Android

Android デバイスで CLOMO MDM をご利用になる場合、CLOMO MDM Agent for Android のインストールが必須です。エージェントアプリは、Google Play からダウンロードできます。(Google Play : <http://goo.gl/w2eIR>)

Android フィーチャーフォン デバイスで CLOMO MDM をご利用になる場合、CLOMO MDM Agent for Android のインストールが必須です。初期設定マニュアル記載の Web URL からダウンロードできます。

▶ CLOMO MDM Agent for Android の機能

- 位置情報の取得
- メッセージの通知
- Root化 検知
- 禁止アプリ利用のブロック
- VPN 接続 (MPKIご利用の場合)
- コマンド取得間隔の設定(*)



*Android フィーチャーフォン向けの機能となります。



CLOMO MDM Agent for Windows

Windows デバイスで CLOMO MDM をご利用になる場合、CLOMO MDM Agent for Windows をインストールすることで、より高度な機能をご利用頂けます。エージェントアプリは、CLOMO MDM が発行する Web URL からダウンロードできます。

▶ CLOMO MDM Agent for Windows の機能

- 定期位置情報の取得
- リモートロック
- 電子証明書の配布 / 失効
- ワーク・スマート機能
- OneBeプロファイルの配布





iOS向け

🔍 情報取得/閲覧

- ▶ UDID(Unique Device Identifier)
- ▶ デバイスID
- ▶ デバイス名
- ▶ OS バージョン / ビルドバージョン
- ▶ モデル名 / 番号
- ▶ シリアル番号
- ▶ Exchange ActiveSync デバイスID
- ▶ IMEI (International Mobile Equipment Identifier)
- ▶ デバイス容量 / 使用可能な空き領域
- ▶ 監視対象モード
- ▶ 「iPhoneを探す」設定
- ▶ アクティベーションロック設定
- ▶ おやすみモード設定
- ▶ iCloud/バックアップ設定
- ▶ iCloud/バックアップ最終実行日時
- ▶ デバイスの紛失モード情報
- ▶ ネットワーク種別
- ▶ IMEI番号
- ▶ MEID番号
- ▶ ファームウェアバージョン
- ▶ SIMカードのICCID (IC Card Identifier)
- ▶ Bluetooth の MAC アドレス
- ▶ Wi-Fi の MAC アドレス
- ▶ 現在のキャリアのネットワーク
- ▶ SIM キャリアのネットワーク
- ▶ キャリア設定のバージョン
- ▶ 電話番号
- ▶ ボイスローミング設定
- ▶ データローミング設定
- ▶ ローミング状態
- ▶ 契約国コード
- ▶ 契約ネットワークコード
- ▶ 現在の国コード
- ▶ 現在のネットワークコード
- ▶ OSアップデート情報
- ▶ DEPデバイス情報
 - デバイスの説明
 - デバイスの色
 - Appleアセットタグ
 - DEPプロファイル状態
 - DEPプロファイルID
 - DEPプロファイル割り当て日時
 - DEPプロファイル配布日時
 - MDMサーバー割り当て日時
 - 割り当て実行アカウント
- ▶ インストール済みアプリ一覧
- ▶ インストール済みアプリ管理設定プロファイル一覧
- ▶ インストール済みプロビジョニングプロファイル
- ▶ 位置情報履歴
- ▶ インストール済み証明書
- ▶ インストール済み構成プロファイル
- ▶ JailBreak の検知
- ▶ デバイス検索
- ▶ ポリシー違反デバイスの抽出 / 検索
- ▶ ポリシー違反アプリの検知

🖱️ コマンド実行

- ▶ リモートワイプ
- ▶ リモートロック
- ▶ パスコードの消去
- ▶ 紛失モードの設定 (iOS 9.3.2 以降のみ)
 - 表示メッセージの指定 (*iOS 9.3.2 以降のみ)
 - 連絡先番号の指定 (iOS 9.3.2 以降のみ)
 - 下部メッセージ (iOS 9.3.2 以降のみ)
 - 強制位置情報取得 (*1)
- ▶ プロファイルの配布 / 削除
 - DEPプロファイル
 - 構成プロファイル
 - プロビジョニングプロファイル
 - アプリ管理設定プロファイル (*2)
- ▶ ボイスローミングの有効化/無効化 (iOS 5 以降のみ対象)
- ▶ データローミングの有効化/無効化 (iOS 5 以降のみ対象)
- ▶ デバイス情報の取得
- ▶ インストール済みアプリケーション取得
- ▶ インストール済みプロファイル取得
- ▶ 位置情報の取得 (*3)
- ▶ 位置情報のサイレント取得 (iOS 7 以降のみ対象)
- ▶ デバイス証明書の配布 / 失効
- ▶ メッセージの送信
- ▶ OSアップデート情報取得
- ▶ OS の強制アップデート(iOS 9.3.2 以降のみ対象)
- ▶ VPPライセンスの付与 / 剥奪
- ▶ アプリケーションインストールを通知(*4)
- ▶ アプリケーションのアンインストール(*4)

*1 : 本機能を利用するには iOS デバイスを監視モードに設定する必要があります。

*2 : アプリ側が本機能に対応している必要があります。

*3 : 本機能を利用するには CLOMO MDM Agent for iOS をインストールする必要があります。

*4 : CLOMOMOBILE APP PORTAL オプションが別途必要です。



iOS向け

設定 (一部抜粋)

- ▶ プロファイル自動適用
 - 全社・組織別設定
 - 任意のグループ別設定
- ▶ アプリ自動配布 (*4)
 - 全社・組織別設定
 - 任意のグループ別設定
- ▶ Device Enrollment Program (DEP) 設定
 - CLOMO MDMからの離脱防止
 - CLOMO MDMへのデバイス自動登録
 - ワイヤレスで監視対象デバイスに設定
 - デバイス初期設定時の設定画面を省略
- ▶ Apple School Manager(ASM)対応
 - ASMで作成された基本情報の同期
 - Shared iPadの設定、管理
 - Classroomアプリへの設定配布
- ▶ [ASM] 基本情報同期
 - ユーザー情報
 - Managed Apple ID情報
 - 授業情報
 - 場所情報
 - コース情報
- ▶ [ASM] Shared iPadの設定、管理
 - MDM登録時にShared iPad設定を自動付与
 - Shared iPadにログイン可能なユーザー情報の配布
 - Shared iPadにログイン可能なユーザーのクラス情報配布
- ▶ [ASM] Classroomアプリへの設定配布
 - ユーザー情報の配布
 - クラス情報の配布
 - デバイス情報の配布
- ▶ Exchange ActiveSync
- ▶ IMAP / POPメール
- ▶ VPN
- ▶ Bluetoothの制限(*3)
- ▶ Wi-Fi 設定 / 制限(*3)
- ▶ LDAP
- ▶ CalDAV
- ▶ CardDAV
- ▶ 照会カレンダー
- ▶ パスコードの要求
 - 簡単なパスコードの許可
 - 英数字の値の要求
 - パスコード長
 - 複合文字の数
 - パスコードの有効期限
 - 自動ロックまでの時間
 - 再使用までのパスコードの数
 - デバイスロックの猶予期間
 - ローカルワイプまでの失敗再試行回数
- ▶ 定期的に位置情報を取得 (*1)
- ▶ 任意時刻に位置情報を取得 (*1)
- ▶ アプリのインストール
- ▶ アプリケーション内からの購入
- ▶ JailBreak の検知管理者の計画に基づいたエージェントアプリのアップデート適用 (*2)
- ▶ 標準アプリの利用制限(*3)
 - 設定アプリ以外のアプリ
- ▶ カメラの制限
- ▶ スクリーンショットと画面収録の制限
- ▶ AirDrop を制限(*3)
- ▶ iMessage を制限(*3)
- ▶ Siri を制限
- ▶ ローミング中の自動同期を制限
- ▶ "すべてのコンテンツと設定を消去"を制限(*3)
- ▶ VPN 構成の追加を制限(*3)
- ▶ ロック中の音声ダイヤル
- ▶ コンテンツレーティング
- ▶ Safari のセキュリティ設定
 - 自動入力を有効にする
 - 強制的に詐欺警告
 - JavaScript を有効にする
 - ポップアップを開かない
 - Cookie の受け入れ
- ▶ YouTube
- ▶ iTunes Store
- ▶ App Store
- ▶ Safari
- ▶ Facetime
- ▶ iCloud へのバックアップ (iOS 5 以降のみ対象)
 - 書類の同期
 - フォトストリーム
 - 診断データの送信
 - TLS 証明書の受け入れ
 - 強制的に暗号化
- ▶ 証明書と固有名
- ▶ ソフトウェア・アップデートの遅延(*3)
- ▶ WEB クリップ
- ▶ APN 設定
- ▶ ワーク・スマート (*3)(*5)
 - スケジュール設定
 - ワーク・スマート構成

*1 : CLOMO MDM Agent for iOSでは、一部仕様制限があります。
本機能の利用には、CLOMO MDM Agent Enterprise for iOSを推奨します。

*2 : CLOMO MDM Agent Enterprise for iOSのみ対象となります。

*3 : 本機能を利用するにはiOSデバイスを監視モードに設定する必要があります。

*4 : 本機能を利用するにはCLOMO MOBILE APP PORTALの利用が必要です。

*5 : iOS デバイス上で利用できるアプリが「設定」「電話 (iPhone のみ)」「MDM Agent for iOS」に限定されます。



macOS向け

🔍 情報取得/閲覧

- ▶ UDID(Unique Device Identifier)
- ▶ デバイス名
- ▶ OSバージョン / ビルドバージョン
- ▶ モデル名
- ▶ モデル
- ▶ シリアルナンバー
- ▶ デバイス容量
- ▶ 有効な容量
- ▶ Bluetooth の MAC アドレス
- ▶ Wi-Fi の MAC アドレス
- ▶ FireValut
- ▶ インストール済み構成プロファイル
- ▶ インストール済みアプリ一覧
- ▶ アプリ名

⚙️ 設定

- ▶ パスコードの要求
 - 全社・組織別設定
 - 任意のグループ別設定
- ▶ IMAP / POPメール
- ▶ VPN
- ▶ Wi-Fi
- ▶ パスコードの要求
 - 簡単なパスコードの許可
 - 英数字の値の要求
 - パスコード長
 - 複合文字の数
 - パスコードの有効期限
 - 自動ロックまでの時間
 - 再使用までのパスコードの数
 - デバイスロックの猶予期間
 - ローカルワイプまでの失敗再試行の回数

🖱️ コマンド実行

- ▶ リモートワイプ
- ▶ 強制パスコードロック
- ▶ デバイス情報取得
- ▶ インストール済みアプリケーション取得
- ▶ インストール済みプロファイル取得
- ▶ インストール済みプロファイル取得
- ▶ プロファイルの配布 / 削除
 - 構成プロファイル(*1)

*1 : ASM利用時に使用する教育向け構成プロファイルを含みます



Android向け

情報取得/閲覧

- ▶ デバイス名
- ▶ モデル
- ▶ モデル名
- ▶ OS バージョン
- ▶ ビルドバージョン
- ▶ シリアル番号
- ▶ IMEI (International Mobile Equipment Identifier)
- ▶ ICCID (IC Card Identifier)
- ▶ 電話番号
- ▶ Wi-Fi の MAC アドレス
- ▶ 通信キャリア
- ▶ 現在の MNC (Mobile Network Code)
- ▶ 現在の MCC (Mobile Country Code)
- ▶ ローミング設定
- ▶ インストール済みプロファイル
- ▶ インストール済みアプリ一覧
- ▶ アプリ名
- ▶ バージョン
- ▶ 位置情報履歴
- ▶ 電話発信履歴
- ▶ 電話発信履歴のエクスポート
- ▶ デバイス検索
- ▶ ポリシー違反デバイスの抽出 / 検索
- ▶ ポリシー違反アプリの検知
- ▶ CLOMO MDM VirusScanの詳細情報(*11)

設定

- ▶ Android Enterprise 対応 (*2) (*3)
 - Work Managed Device としての設定
 - Work profileの追加設定
- ▶ ストアアプリ (Play for Work) のレイアウト設定 (*4)
 - ページタイトル設定
 - ホームページ設定
 - ページへのリンク設定
 - クラスタ設定
- ▶ Play for Work コンソールで承認したアプリに対する権限設定 (*4) (*5)
- ▶ Play for Work コンソールで承認したアプリに対する制限設定 (*4) (*6)
- ▶ パスコードポリシー
 - 英数字の値の要求
 - デバイス設定優先
 - パスコード長
 - パスコードの有効期限
 - 再使用までのパスコードの数
- ▶ パスコード入力失敗制御ポリシー
 - ローカルワイプまでの失敗再試行の回数
 - ローカルロックまでの失敗再試行の回数
- ▶ 緊急デバイス制御機能 (指定電話番号着信での利用制限)
- ▶ 位置情報を取得
 - 定期的 / 任意時刻
 - 位置情報取得の曜日指定
- ▶ 実行時パーミッションポリシーの制限 (*4)(*7)
- ▶ ストレージ暗号化
- ▶ SDメモリの制限
- ▶ Bluetooth の制限
 - 利用制限(*4)
 - Bluetooth 接続制限 (ヘッドセットのみ許可) (*9)
- ▶ デザリングの制限
- ▶ カメラの制限
- ▶ USB 接続の制限 (*4)
- ▶ 緊急時省電力モードの利用制限(*9)
- ▶ 画面のキャプチャを制限 (*4)
- ▶ Androidビームのデータ送信制限 (*4) (*7)
- ▶ ファクトリリセット操作を制限 (*4)
- ▶ デバッグモードの利用を制限 (*4)
- ▶ セーフブートの利用を制限 (*4)(*7)
- ▶ システムアップデート抑止 (*4)
- ▶ Root 化検知
- ▶ Wi-Fi 制限
 - ホワイトリスト/ブラックリスト
- ▶ 電話発信先制限
 - ホワイトリスト/ブラックリスト
- ▶ SIM カード変更監視
- ▶ データローミング制限(*4)
- ▶ モバイルネットワークの操作を制限(*4)
- ▶ ネットワーク設定のリセット操作を制限 (*4)
- ▶ SMS の送受信を制限 (*4)
- ▶ アプリ利用ポリシー違反検知設定
- ▶ アプリのアンインストール制限 (*4)
- ▶ 提供元不明アプリのインストール制限 (*4)
 - 設定アプリ制限(*9)
- ▶ ユーザー追加の制限 (*4)
- ▶ ユーザー削除の制限 (*4)
- ▶ アカウントの追加 / 削除を制限 (*4)
 - Googleアカウントのみ
 - すべてのアカウント制限
- ▶ 端末管理権限の解除ポリシー
 - エージェントアプリの削除制限
 - CLOMO MDMからの離脱禁止 (*4)
- ▶ 仕事領域制限(*4)
 - 画面のキャプチャを制限 (*4)
 - 提供元不明アプリのインストール制限 (*4)
 - コピー & ペースト制御(*4)
- ▶ ホワイト/ブラックリストによるアプリの利用制限
- ▶ 下記機能を持ったアプリの制限
 - アカウントへアクセスする
 - 利用料金が発生する
 - ハードウェアの機能に直接アクセスする
 - 現在地を追跡する
 - SMS の読み書きを行う
 - SDカードにアクセスする
 - メールの読み書きを行う端末の連絡先に直接アクセス
 - 端末のカレンダーに直接アクセスする
 - 通話の監視、記録、処理をする
 - システムに低レベルのセキュリティ設定でアクセス
- ▶ Android Enterprise初期設定プロファイル対応
 - 標準アプリの利用制限 (*4)
 - 仕事領域/個人領域に分割(*4)
 - 個人領域のアプリケーションを管理する(*4)
- ▶ Wi-Fi 設定
- ▶ VPN 設定
- ▶ ジオフェンス設定
- ▶ 専用端末プロファイル
- ▶ ロックタスクプロファイル

*1: CLOMO MDM Agent 1.16.0 以降の併用が必要となります。

*2: Android OS 5 系 / 6 系 / 7 系 / 8 系デバイスのみ対象

*3: 要工場出荷時設定

*4: Android Enterprise 機能を用いて Work Managed Device として設定されたデバイスのみ対象

*5: 設定できる権限種類はアプリによって異なります。

*6: 設定できる制限種類はアプリによって異なります。

*7: 対応 OS 6.0 以降

*8: 対応 OS 7.0 以降

*9: SONY Xperia™ デバイス向けの固有機能です。

*10: プロファイル内でデバイス管理方式とデバイス種別を選択可能。CLOMO MDM Agent 2.5.0 以降

*11: CLOMO MDM アンチウイルスオプションの契約が必要です。



Android向け

🔍 コマンド実行

- ▶ リモートワイプ
 - 全体削除
 - 仕事領域のみ削除
- ▶ 強制パスコードロック
- ▶ パスコードの消去
- ▶ デバイスを再起動 (*4)(*8)
- ▶ 紛失モードの設定 (*1)
 - 表示メッセージの指定
 - 連絡先番号の指定
 - 強制パスコードロック用
パスコードの設定
- ▶ 設定プロファイルの配布 / 削除
 - 管理プロファイル
 - アプリ制限プロファイル
 - 専用端末プロファイル
 - ロックタスクプロファイル
 - ジオフェンスプロファイル
 - アプリ権限設定設定プロファイル (*4)
 - アプリ管理設定プロファイル(*4)
 - VirusScan 設定プロファイル(*12)
 - デバイス設定プロファイル (*10)
 - DeviceOwner設定プロファイル (*4)
 - VPN 設定プロファイル
 - Wi-Fi設定プロファイル
- ▶ デバイス情報の取得
- ▶ 位置情報の取得
- ▶ デバイス証明書の配布 / 失効
- ▶ 電話発着信履歴情報を取得
- ▶ メッセージの送信
- ▶ アプリケーションのインストールを通知(*4)(*11)
- ▶ アプリケーションをアンインストール(*4)(*11)
- ▶ ウイルススキャンの実行開始(*12)
- ▶ ウイルス定義ファイルの更新(*12)
- ▶ ウイルスソフトの最新情報を取得(*12)

*1 : CLOMO MDM Agent 1.16.0 以降の併用が必要となります。

*2 : Android OS 5 系 / 6 系デバイスのみ対象

*3 : 要工場出荷時設定

*4 : Android Enterprise 機能を用いて Work Managed Device として設定されたデバイスのみ対象

*5 : 設定できる権限種類はアプリによって異なります。

*6 : 設定できる制限種類はアプリによって異なります。

*7 : 対応 OS 6.0 以降

*8 : 対応 OS 7.0 以降

*9 : SONY Xperia™ デバイス向けの固有機能です。

*10 : プロファイル内でデバイス管理方式とデバイス種別を選択可能。CLOMO MDM Agent 2.5.0 以降

*11 : CLOMOMOBILE APP PORTALオプションが別途必要です。

*12 : CLOMO MDM アンチウイルスオプションの契約が必要です。



Android (Google Play 非搭載デバイス向け)

情報取得/閲覧

- ▶ デバイス名
- ▶ モデル
- ▶ モデル名
- ▶ OS バージョン
- ▶ ビルドバージョン
- ▶ シリアル番号
- ▶ IMEI (International Mobile Equipment Identifier)
- ▶ ICCID (IC Card Identifier)
- ▶ 電話番号
- ▶ Wi-Fi の MAC アドレス
- ▶ 通信キャリア
- ▶ 現在の MNC (Mobile Network Code)
- ▶ 現在の MCC (Mobile Country Code)
- ▶ ローミング設定
- ▶ インストール済みプロファイル
- ▶ インストール済みアプリ一覧
- ▶ アプリ名
- ▶ バージョン
- ▶ 位置情報履歴
- ▶ 電話発着信履歴
- ▶ 電話発着信履歴のエクスポート
- ▶ デバイス検索
- ▶ ポリシー違反デバイスの抽出 / 検索
- ▶ ポリシー違反アプリの検知

設定

- ▶ パスコードポリシー
 - 英数字の値の要求
 - デバイス設定優先
 - パスコード長
 - パスコードの有効期限
 - 再使用までのパスコードの数
 - ローカルワイプまでの失敗再試行の回数
- ▶ VPN 設定
- ▶ Bluetooth の制限
- ▶ Wi-Fi の設定 / 制限
- ▶ Wi-Fi デザリングの制限
- ▶ 定期的 / 任意時刻に位置情報を取得
- ▶ 位置情報取得の曜日指定
- ▶ Root 化検知
- ▶ ホワイト / ブラックリストによるアプリの利用制限
- ▶ 下記機能を持ったアプリの制限
 - アカウントへアクセスする
 - 利用料金が発生する
 - ハードウェアの機能に直接アクセスする
 - 現在地を追跡する
 - SMS の読み書きを行う
 - SDカードにアクセスする
 - メールを読み書きを行う端末の連絡先に直接アクセス
 - 端末のカレンダーに直接アクセスする
 - 通話の監視、記録、処理をする
 - システムに低レベルのセキュリティ設定でアクセス
- ▶ エージェントアプリの削除制限
- ▶ カメラの制限
- ▶ SDメモリの制限
- ▶ USB 接続の制限
- ▶ 電話発信先制限
- ▶ ストレージ暗号化
- ▶ 緊急デバイス制御機能 (指定電話番号着信での利用制限)
- ▶ デバイス管理権限の解除検知機能
- ▶ コマンド取得間隔の設定

コマンド実行

- ▶ リモートワイプ
- ▶ 強制パスコードロック
- ▶ パスコードの消去
- ▶ 紛失モードの設定
 - 表示メッセージの指定
 - 連絡先番号の指定
 - 強制パスコードロック用パスコードの設定
- ▶ 設定プロファイルの配布 / 削除
 - アプリ制限プロファイル
 - アプリ管理設定プロファイル
 - デバイス設定プロファイル (*1)
 - VPN 設定プロファイル
- ▶ デバイス情報の取得
- ▶ インストール済みアプリケーション取得
- ▶ インストール済みプロファイル取得
- ▶ 位置情報の取得
- ▶ デバイス証明書の配布 / 失効
- ▶ 電話発着信履歴情報を取得
- ▶ メッセージの送信

*1: プロファイル内でデバイス管理方式とデバイス種別を選択可能。



Windows Desktop 向け

情報取得/閲覧

- ▶ デバイスID
- ▶ デバイス名
- ▶ OS バージョン
- ▶ ビルドバージョン **New!**
- ▶ BIOSバージョン
- ▶ モデル名
- ▶ シリアルナンバー
- ▶ プラットフォーム
- ▶ デバイスの種類
- ▶ システムの種類
- ▶ メーカー
- ▶ 所有者名
- ▶ ログオンユーザ名
- ▶ ホスト名
- ▶ ドメイン名
- ▶ ワークグループ
- ▶ Wi-Fi の IP アドレス
- ▶ タイムゾーン
- ▶ EthernetIPアドレス / IPv6
- ▶ Wi-Fi IP、アドレス / IPv6
- ▶ 電話番号
- ▶ キャリア
- ▶ IMEI
- ▶ ICCID
- ▶ 設定言語
- ▶ WNSステータス
- ▶ パワーオンパスワード設定
- ▶ Intel®AMT機能
- ▶ Intel®AMT向け中継機能
- ▶ ワークスマート情報(*3)
- ▶ インストール済み構成プロファイル
- ▶ インストール済み証明書
- ▶ インストール済みアプリ一覧
- ▶ 位置情報履歴
- ▶ 更新プログラム情報一覧 **New!**

設定

- ▶ パスコードポリシー
 - 英数字の値の要求
 - デバイス設定優先
 - パスコード長
 - パスコードの有効期限
 - 再使用までのパスコードの数
 - 再起動までの失敗再試行の回数
- ▶ VPN 設定
- ▶ Bluetooth の制限
- ▶ Wi-Fi の制限(*3)
- ▶ Wi-Fi の設定
- ▶ Wi-Fiテザリングの制限
- ▶ パスコードの要求
 - 簡単なパスコードの許可
 - 英数字の値の要求
 - パスコード長
 - 複合文字の数
 - パスコードの有効期限
 - 自動ロックまでの時間
 - 再使用までのパスコードの数
 - デバイスロックの猶予期間
 - ローカルワイブまでの失敗再試行の回数
- ▶ 定期的に位置情報を取得(*3)
- ▶ 任意時刻に位置情報を取得(*3)
- ▶ 位置情報取得の曜日指定(*3)
- ▶ 社内アプリのインストール (*3)
- ▶ 管理者の計画に基づいたエージェントアプリのアップ
- ▶ デート適用(*3)
 - CLOMO MDMからの離脱禁止
- ▶ カメラの制限
- ▶ SD メモリの制限
- ▶ USB 接続の制限 (USBマストレージの接続制限)
- ▶ Bitlocker暗号化(*1)
- ▶ 持ち出し監視ポリシー設定 (*2)
 - AC アダプタの接続状況
 - 指定 SSID の検出状況
 - 指定 Bluetooth デバイスとの接続状況
 - インターネット接続の有無
 - インターネット接続時のゲー
 - トウェイ情報
 - GPS (緯度・経度) 情報
 - パスコード認証失敗回数
 - 指定サーバーへの接続状況
- ▶ 違反検知からアクション実行までの猶予期間
- ▶ Windows Update 制御機能 **New!**
- ▶ プロファイル自動適用 (*1)
 - 全社・組織別設定
 - 任意のグループ別設定
- ▶ 持ち出し監視ポリシー違反時のアクション設定 (*2)
 - Windows ロック画面の表示
 - サウンドアラーム付き Windows ロック画面の表示
 - USB 接続による強制アンロック設定
- QR コードによる一時的なアンロック設定
- HID (マウス、キーボード、タッチパネルなど) ロック
- HID ロック時のメッセージ表示
- 指定バスのフォルダ・ファイル削除
- ▶ 持ち出し監視ポリシー準拠時のアクション設定 (*2)
 - Windows ロック画面の解除
- ▶ 即時適用のアクション設定 (*2)
 - HID (マウス、キーボード、タッチパネルなど) ロック
 - 指定バスのフォルダ・ファイル削除

*1 : 後日対応予定です。

*2 : CLOMO MDM secured by OneBe の利用が必要です。

*3 : CLOMO MDM agent for Windowsが必要です。



Windows Desktop 向け

コマンド実行

- ▶ リモートワイプ
- ▶ リモートロック(*3)
- ▶ 設定プロファイルの配布 / 削除
 - デバイス設定プロファイル
- ▶ デバイス情報の取得
- ▶ 位置情報の取得
- ▶ 位置情報のサイレント取得
- ▶ デバイス証明書の配布 / 失効(*3)
- ▶ デバイス証明書のサイレントインストール(*3)
- ▶ デバイスのリモートシャットダウン(*3)
- ▶ OneBe 設定の配布 / 削除 (*2)(*3)

*2 : CLOMO MDM secured by OneBe の利用が必要です。

*3 : CLOMO MDM agent for Windowsが必要です。



iOS / macOS / Android / Windows

- ▶ サポート対象 OS

- ▶ https://support.clomo.com/?page_id=31150

- ▶ 動作確認済みデバイス詳細情報

- ▶ https://support.clomo.com/?page_id=12055

管理パネル動作環境

- ▶ 動作確認済みブラウザ詳細情報

- ▶ https://support.clomo.com/?page_id=12055

※ ご利用予定のデバイスについて、必ず弊社が公開しております動作確認済みデバイス一覧をご確認下さい。
※ 動作確認済みデバイス以外でのご利用につきましては、販売代理店または当社営業までお問い合わせください。



iOS

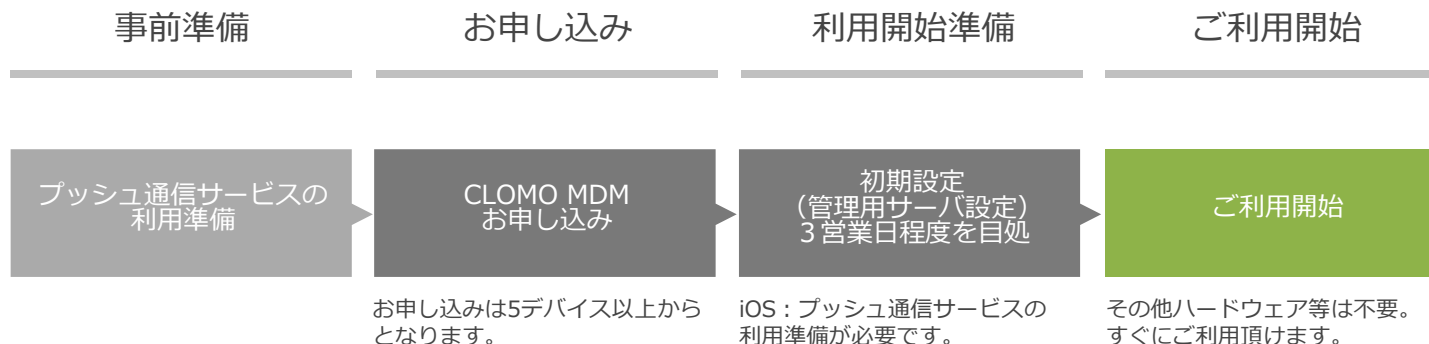
1. Wi-Fiのみの利用環境で、ファイアーウォールを設置している場合は「5223/tcp」「80/tcp」「443/tcp」「53/udp」のポートを開放してください。
2. MDMから削除が可能な構成プロファイルは、MDM経由でインストールされたものに限りです。
3. 構成プロファイルのインストールおよび削除のタイミングは、該当端末がオンライン（LTEまたはWi-Fi）環境にあり、かつ起動ロックが解除されている状態である際に実行されます。
4. iOS、Android、Windows では、制御可能な項目に差異があります。
5. CLOMO MDM Agent Enterprise for iOS・CLOMO SECURED APPs Enterprise for iOS と CLOMO MDM Agent for iOS・CLOMO SECURED APPs for iOS は、同一デバイス上での混在利用を行えません。
6. iOSデバイスの管理機能を全て利用するためには、Apple社が提供する「Apple Configurator」の利用が必要です。「Apple Configurator」を利用するにはMac OSの端末が必要となり、お客様に別途用意頂く必要があります。

Android

1. Wi-Fiのみの利用環境で、ファイアーウォールを設置している場合は「5228/tcp」「5229/tcp」「5230/tcp」「80/tcp」「443/tcp」「53/udp」のポートを開放してください。
※ 5228/TCP、5229/TCP、5230/TCP は、GCMサーバ、CLOMO MDMサーバとのコマンド等の通信に利用しております。
2. Androidは一部機種依存の機能や、OS不具合による制限などがございますので、詳細はお問い合わせ下さい。
3. 位置情報取得においては端末側でGPS機能が有効である必要があります。GPS機能が無効の場合は、位置情報取得は行えません。
4. iOS、Android、Windows では、制御可能な項目に差異があります。

Windows

1. 管理者権限を持たないアカウントを利用している Windows 端末では、CLOMO MDM の機能が一部利用できません。詳細はお問い合わせください。
2. Active Directory など、企業ドメイン配下の Windows 8.1 端末では、CLOMO MDM をご利用頂けません。
3. セキュリティコード認証を行っていない Microsoft アカウントを利用している Windows 端末では、CLOMO MDM をご利用頂けません。
4. Windows 端末から MDMサーバへアクセスが無い状況が30日を超える場合、定期ポーリングが実施されるまでコマンドを実施できない場合があります。
5. Windows 8.1のリモートワイプを実行した場合、対象端末の BitLocker を用いた暗号化済みディスクに対してリモートで暗号化キーを削除し、起動不可能な状態にします。CLOMO MDM secured by OneBe 機能に関わるワイプ機能は BitLocker を用いません。
6. iOS、Android、Windows では、制御可能な項目に差異があります。
7. 本ページに掲載されている画像は、マイクロソフトの許可を得て使用しています。



- ※ iOS 向けで MDM を利用するためには、Apple Push Certificate Portal で事前に MDM 用プッシュ証明書の作成が必要です。
- ※ CLOMO では、JailBreak検知やデバイス位置情報を収集するために iOS 向け CLOMO 用 MDM エージェントアプリのご利用が必要です。
- ※ CLOMO MDM Agent Enterprise for iOS・CLOMO SECURED APPS Enterprise for iOS と CLOMO MDM Agent for iOS・CLOMO SECURED APPS for iOS は、同一デバイス上での混在利用を行えません。
- ※ CLOMO MDM で iOS デバイスを管理するには、Apple 社が提供する「Apple Configurator」の利用が必要です。「Apple Configurator」を利用するには Mac OS の端末が必要となり、お客様に別途用意頂く必要があります。

CLOMO MDM ご利用料金

- ▶ 下記料金案内ページをご覧ください

<https://www.softbank.jp/biz/mobile/solution/partner/clomo/price/>

CLOMO MOBILE APP PORTAL

アプリの高度な管理・運用機能をご提案

CLOMO MOBILE APP PORTAL

アプリの管理・運用機能を備えた「CLOMO MDM シリーズ」オプションのご提案



CLOMO MDM リモートオペレーション サービス(24/365)

万が一のトラブルに
24時間365日の有人サポートをご用意

CLOMO MDM リモートオペレーションサービス(24/365) 利用メリット

ver. 20210202



夜間や休日でも、オペレーターが24時間365日対応

自由に・手軽に持ち運べるスマートデバイスだからこそ、夜間や休日にも紛失・盗難などのトラブルが発生します。本サービスを利用することで、IT管理者が不在の時間帯に、万が一の事態が発生した場合にも、デバイスの利用者が直接オペレーターに連絡し、デバイスのリモートロックや紛失モード設定*、初期化などの緊急対応が可能となります。情報漏洩リスクの一層の低減と、IT管理者の拘束時間の低減が実現されます。



端末ロック、
端末初期化で
情報漏えいを防止



24h 365days

24時間365日
オペレーターが対応



ユーザーから
直接の作業依頼
が可能

オペレーターへの電話で、すぐにリモートロック・紛失モード設定*・初期化ができるから安心。

STEP 1 トラブルの発生



デバイスの盗難、紛失
端末パスコードの失念

STEP 2 専用受付へ緊急電話連絡



端末ロックの依頼
紛失モード設定*の依頼
端末初期化の依頼
端末パスコード解除の依頼

STEP 3 リモート操作の実施



端末ロックの実行
紛失モード設定*の実行
端末初期化の実行
端末パスコード解除の実行

STEP 4 作業完了報告



契約企業様への実施内容
および日時の報告

リモートサービス

リモートサービス詳細

端末ロック

スマートデバイスが不正な操作を受け付けられない様に遠隔でロックします。

紛失モード設定※1

位置情報の強制取得とともに、任意のメッセージや連絡先情報を表示させ強制ロックします。

端末初期化

スマートデバイスに保存されているデータを遠隔で初期化します。

端末パスコード解除※2

端末ロックされたスマートデバイス発見時に、失念したパスコード設定を遠隔から解除します。

※1：本機能を利用するには「iOS：iOS 9.3.2以上、監視対象設定デバイスであること」「Android：Android OS 2.3 以上」を満たしている必要があります。(Windowsは対象外)

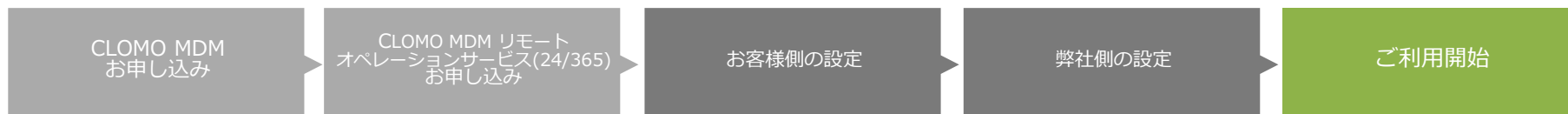
※2：Windowsは対象外



お申し込み

利用開始準備

ご利用開始



お申し込みは5デバイス以上からとなります。

1デバイスからのお申し込みが可能です。

その他ハードウェア等は不要。すぐにご利用頂けます。

CLOMO MDM リモートオペレーションサービス(24/365) ご利用料金

- ▶ 下記料金案内ページをご覧ください

<https://www.softbank.jp/biz/mobile/solution/partner/clomo/price/>



Innovation³

※「CLOMO」「i³ Systems」は、株式会社アイキューブドシステムズの登録商標です。

※ iPhone、iPad、Apple Watch は Apple Inc. の商標です。

※ iPhone 商標は、アイホン株式会社のライセンスに基づき使用されています。

※ Google および Google Apps は Google Inc. の登録商標です。

※ Kindle、Kindle Fire、Amazon および Amazon.co.jp は、Amazon.com, Inc またはその関連会社の商標です。

※ Windows、Windows 8、Windows 10 は、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。

※ 文中の社名、商品名等は各社の商標または登録商標である場合があります。