ver. 20181220

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

アクセスを保護する

ネットワーク利用、どう運用する？

- ID / PW 以外の認証条件を持たせる
- 社内ネットワーク接続の認証を強化する
- クラウド / WEB サービス利用の認証を強化する
- 多様なアカウントを効率的に管理する
- 部署毎にアクセスルールを適用する

CLOMO GATE

アプリを活用する

ビジネスアプリ、必要なことは？

- メーラーやブラウザ、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

CLOMO 導入実績 - 市場シェア -

MDM市場*1

7年連続シェアNo.1

※1 出典ミック経済研究所「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」2011~2015年度、「ミックITリポート2017年12月号」2016年度出荷金額実績および2017年度出荷金額予測。

CLOMO MDM

7年連続シェアNo.1*1 スマートデバイスのリモート管理・運用環境のご提案

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*2

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　・macOS：不要
・Android：必須　・Windows：任意

*1 出典ミック経済研究所「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」2011~2015年度、「ミックITリポート2017年12月号」2016年度出荷金額実績および2017年度出荷金額予測。　*2：iOS、Android向け機能となります。　*3：Windows 8.1、Windows 10 以降

CLOMO MDM の主要メリット

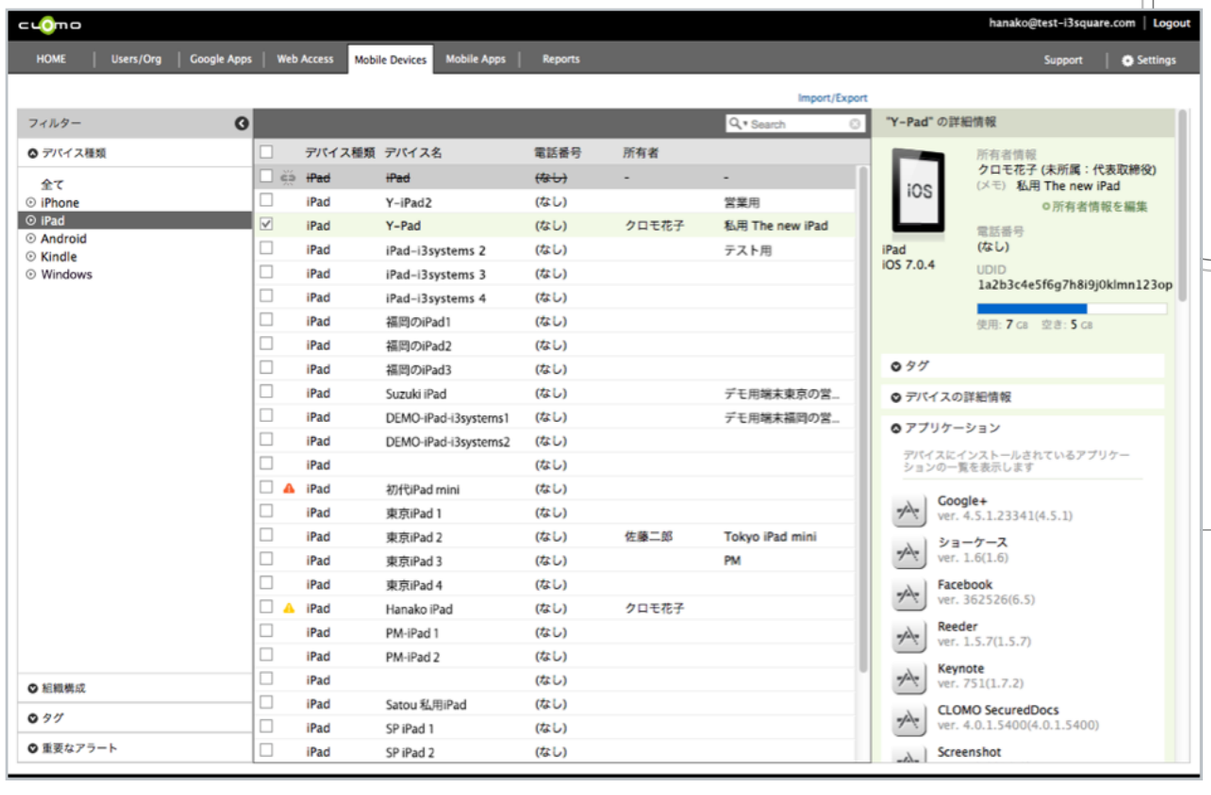
※タブレット端末以外にも対応済みです。

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 の主要機能

CLOMO MDM 主要機能

スマートデバイス運用効率化

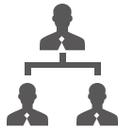
デバイス・アプリの機能制御・自動適用

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

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・管理を行えます
※各種オプションサービスのお申込みが必要です

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

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

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

デバイス管理と完全統合された
ウィルス対策

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

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

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

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

CLOMO MDM
管理パネルの特長

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

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。

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

CLOMO MDM の利用メリット（管理者）

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

CLOMO MDM の利用メリット（ユーザー）

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

ver. 20181220

CLOMO MDM 管理パネルの利用イメージ

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

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

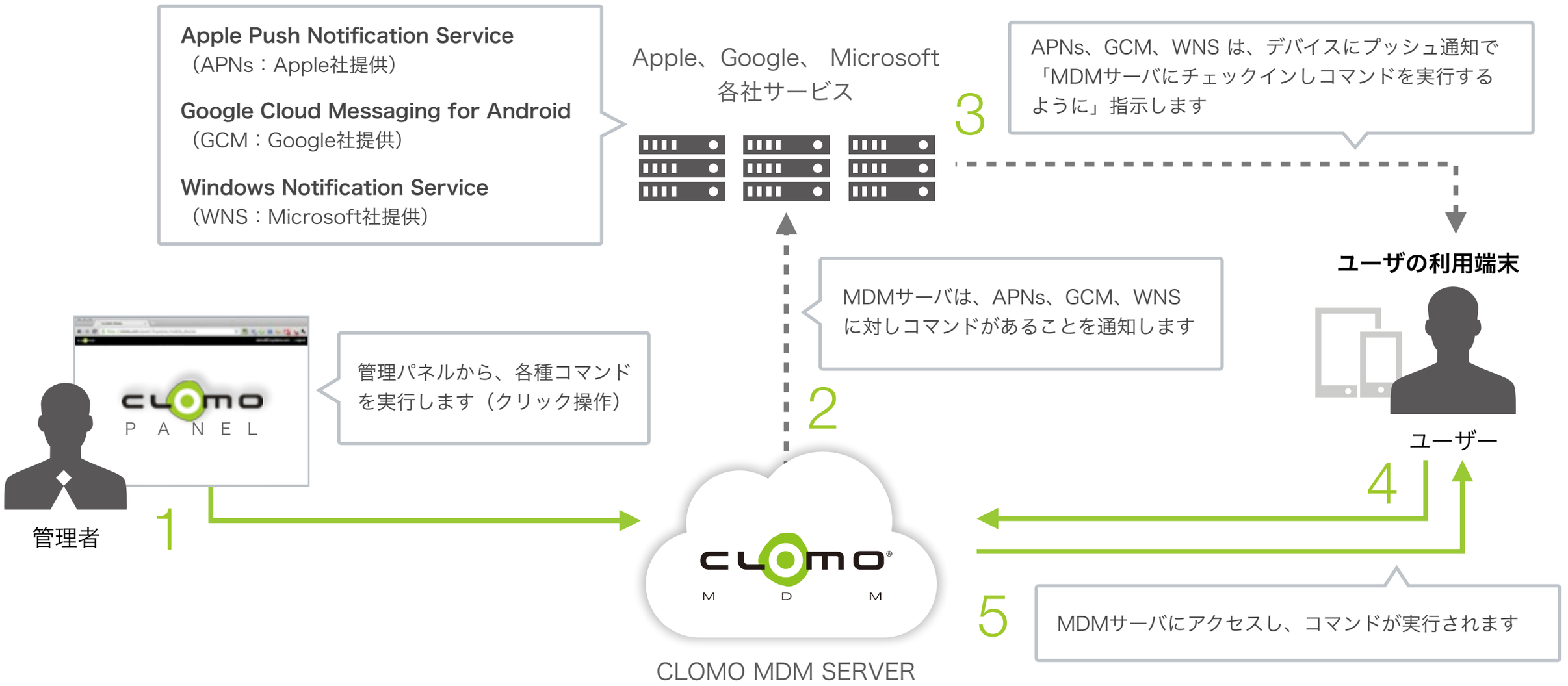
選択部署の「デバイス一覧情報」のリストから、任意のデバイスを選択します

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

CLOMO MDM システム構成イメージ



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

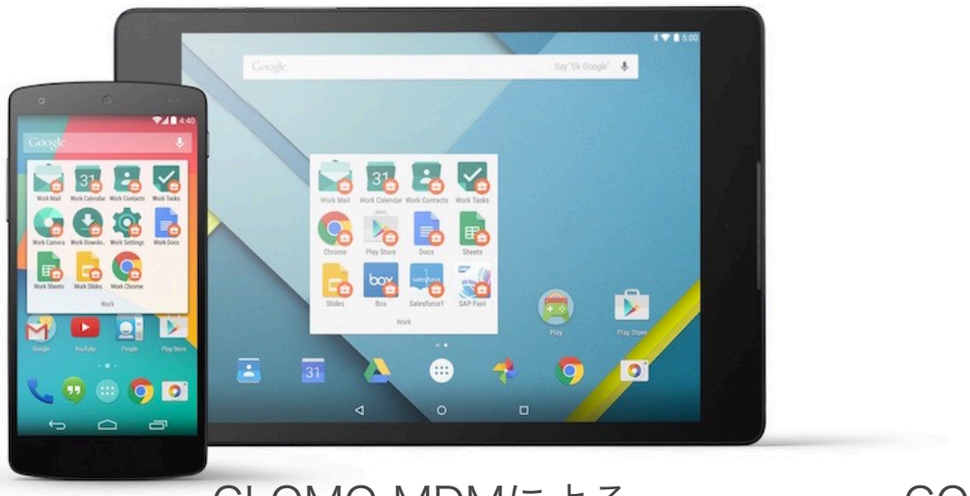
柔軟なスケーラビリティ

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

最新トピックスのご紹介

CLOMO MDM、Android Enterprise DeviceOwnerモード／COMPモードに対応

- Android Enterprise なら企業の多様なニーズに応えるAndroidデバイスを実現 -



豊富な機能制限で セキュリティ対策を高度化

「マルチユーザーの利用制限」「ネットワーク設定の初期化制限」など、MDMベンダー各社が独自の方法で実現していた機能制限をAndroid EnterpriseならOSレベルで確実に実現できます。

CLOMO MDMによる 確実なモバイル管理

MDM管理から外れる原因となる「ユーザーの追加」「Android Enterprise用Googleアカウント削除」「デバイス初期化」などの行為を制限できるため、確実なモバイル管理環境を実現できます。

COMPモードで柔軟なスマホの利用 とセキュリティ強化を実現

個人の携帯やスマートフォンと持ち込めない職場にて、お仕事で利用可能なアプリケーション群と個人利用を許可するアプリケーション群を分割管理しデータの受渡しを制限しセキュリティを高めます。

本対応の詳細：http://www.i3-systems.com/mdm_android_for_work.html

注目トピックスのご紹介

CLOMO MDM
Android フィーチャーフォンの管理に対応

- CLOMO MDM が、Android フィーチャーフォン（※1） を管理できるようになりました。 -

※1 「Android フィーチャーフォン」とは、Android OS を搭載した従来型携帯電話（フィーチャーフォン）です。
Google Play が搭載されていないため CLOMO PANEL 上では、「Google Play 非対応デバイス」として取り扱っており
MDM Agent for Android のインストール方法も通常とは異なるため、初期設定マニュアルをご確認ください。
また、プッシュ通知に非対応であるため、管理プロファイルにて「コマンド取得間隔」を設定することができます。
Android フィーチャーフォン向けの管理プロファイルを作成するには「デバイス種別」として「Google Play 非対応デバイス」を選択して下さい。

※2 管理対象のデバイスには、MDM Agent for Android 2.6.0 以上がインストールされている必要があります。
※3 対象となるデバイスの OS バージョンは、Android 5 系となります。
対応機種については、当社までお問い合わせください。

注目トピックスのご紹介

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」「Andorid：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。

注目トピックスのご紹介

CLOMO MDM、新機能「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 -

管理者が設定した時間になると、端末が電話機能のみに制限される「業務時間外モード」に自動移行されます。本機能を使用することで「隠れ残業」の抑止し、従業員のストレス軽減といった労働環境における課題解決をサポートすることが可能です。詳細な利用条件・方法などは当社までお問い合わせください。

業務時間内モード

業務時間内であれば、管理者が許可している全ての機能・アプリを利用できます。

業務時間外モード

業務時間外は緊急対応に必要な電話機能のみ利用できます。時間外利用が必要な場合には利用申請をすることで「業務時間内モード」に移行できます。

解除申請画面

※ 本機能を利用するには「iOS：iOS 9.3以上、監視対象設定デバイスであること」「Andorid：Android Enterprise を用いて Work Managed Device として設定したデバイスであること」を満たしている必要があります。「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 Agent について(1/2)

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/hml8to)

※ 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(旧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

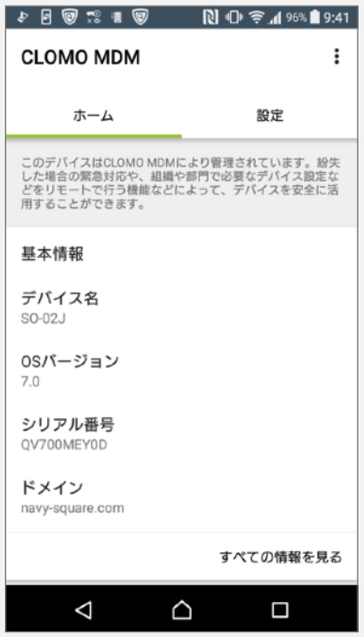
- 位置情報の取得
- メッセージの通知
- ワーク・スマート
- JailBreak 検知
- アップデート時のプッシュ通知

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/w2elR)
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 について(2/2)

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

- 位置情報の取得
- 電子証明書の配布 / 失効
- リモートワイプ

CLOMO MDM機能一覧（1/9）

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
- Exxhange 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
- 芸剤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。

CLOMO MDM機能一覧（2/9）

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
- 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。

CLOMO MDM機能一覧（3/9）

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
- インストール住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

CLOMO MDM機能一覧（4/9）

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
- 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)
- パスワードポリシー
  - 英数字の値の要求
  - デバイス設定優先
  - パスコード長
  - パスワードの有効期限
  - 再使用までのパスコードの数
- パスワ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
  - ローカルワ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)
- テザリングの制限
- 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)
- ファクトリー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

*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。

CLOMO MDM機能一覧（5/9）

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ワードの設定
- 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
  - 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。

CLOMO MDM機能一覧（6/9）

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

- パスワードポリシー
  - 英数字の値の要求
  - デバイス設定優先
  - パスコード長
  - パスワードの有効期限
  - 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 テザリングの制限
- 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
- 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
- SIM カード変更監視
- 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ワードの設定
- 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。

CLOMO MDM機能一覧（7/9）

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
- 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
- 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

設定

- 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
- パワーオンパスワード設定 (*5)
- パスワードポリシー
  - 英数字の値の要求
  - デバイス設定優先
  - パスコード長
  - パスワードの有効期限
  - 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
- 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
  - ローカルワイプまでの失敗再試行の回数
- 定期的に位置情報を取得
- 任意時刻に位置情報を取得
- 位置情報取得の曜日指定
- 社内アプリのインストール（*8）
- 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
- 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マスストレージの接続制限）
- ストレージ暗号化(*7)
- 持ち出し監視ポリシー設定 (*3)
  - 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
  - パスワード認証失敗回数
  - 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
- 持ち出し監視ポリシー違反時のアクション設定 (*3)
  - 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
  - 指定パスのフォルダ・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 (*3)
  - Windows ロック画面の解除
- 即時適用のアクション設定 (*3)
  - HID（マウス、キーボード、タッチパネルなど）ロック
  - 指定パスのフォルダ・ファイル削除

*1：インテル® vPro™ プロセッサーのみ対象。
*2：Windows 8.1 のみ対象。
*3：CLOMO MDM secured by OneBe の利用が必要です。
*4：VAIO Pro 13 | Mk2 (VPJ132) のみ対象
*5：後日対応予定です。
*6：Windows 10では、PINの強制変更で実現します。
*7：BitLockerにて暗号化をします。
*8：MSIファイルのみ登録可能となり、CLOMO MOBILE APP PORTAL からのインストールのみ対応

CLOMO MDM機能一覧（8/9）

Windows Desktop 向け

コマンド実行

- リモートワイプ
- リモートワイプ（SecureWipe：GOST P50739-95 Level 1 方式での論理値 0 書込）(*4)
- リモートロック
- 強制パスコードロック (*6)
- パスコードの消去 (*6)
- 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
- デバイス証明書のサイレントインストール
- デバイスのリモートシャットダウン
- vPro デバイスの電源ON (*1)
- vPro デバイスの AMT 機能 ON / OFF (*1)
- AMT 機能の中継デバイス設定 (*1)
- インテル vPro プロセッサー領域への証明書配布 (*1)(*2)
- リモートデスクトップ接続用 URL の生成 (*1)
- OneBe 設定の配布 / 削除 (*3)

*1：インテル® vPro™ プロセッサーのみ対象。
*2：Windows 8.1 のみ対象。
*3：CLOMO MDM secured by OneBe の利用が必要です。
*4：VAIO Pro 13 | Mk2 (VPJ132) のみ対象
*5：後日対応予定です。
*6：Windows 10では、PINの強制変更で実現します。
*7：BitLockerにて暗号化をします。
*8：MSIファイルのみ登録可能となり、CLOMO MOBILE APP PORTAL からのインストールのみ対応

CLOMO MDM機能一覧（9/9）

Windows Mobile 向け

情報取得/閲覧

- デバイスID
- デバイス名
- OS バージョン
- ファームウエアバージョン
- モデル名
- シリアルナンバー
- プラットフォーム
- メーカー
- Wi-Fi の IP アドレス / IPv6
- Wi-Fi の MAC アドレス
- 電話番号
- キャリア
- IMEI
- ICCID
- 設定言語
- WNSステータス
- PIN
- インストール済み構成プロファイル
- インストール済みプロファイル
- 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

設定

- パワーオンパスワード設定 (*1)
- パスワードポリシー
  - 英数字の値の要求
  - デバイス設定優先
  - パスコード長
  - パスワードの有効期限
  - 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 の制限
- 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
  - パスコード長
  - 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
  - ローカルワイプまでの失敗再試行の回数
- 定期的に位置情報を取得
- 任意時刻に位置情報を取得
- 位置情報取得の曜日指定
- 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マスストレージの接続制限）

コマンド実行

- リモートワイプ
- リモートロック
- 強制パスコードロック (*2)
- 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

*1：後日対応予定です。
*2：Windows 10では、PINの強制変更で実現します。
*3：MSIファイルのみ登録可能となり、CLOMO MOBILE APP PORTAL からのインストールのみ対応

CLOMO MDM動作環境

iOS / macOS / Android / Windows

- サポート対象 OS
  - http://www.i3-systems.com/mdm.html

- 動作確認済みデバイス詳細情報
  - http://www.i3-systems.com/mdm.html

管理パネル動作環境

- 動作確認済みブラウザ詳細情報
  - http://www.i3-systems.com/mdm.html

※ 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。

CLOMO MDM動作環境 ご注意

iOS

1. Wi-Fiのみの利用環境で、ファイヤ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ます。
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（3G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、ファイヤ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. C2DMは現在βリリースのため、Push機構に遅延などが発生する可能性があります。この不具合にそなえ、デバイス側から１時間ごとにコマンド指示の確認を行うよう対応しています。
4. 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。
5. 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 をご利用頂けません。
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サーバー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. CLOMO MDM が持つ標準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。VAIO 端末に対する SecureWipe 機能 と 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、Kindle 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。

CLOMO MDMご利用案内

事前準備	お申し込み	利用開始準備	ご利用開始
プッシュ通信サービスの利用準備	CLOMO MDM お申し込み	初期設定（管理用サーバ設定）３営業日以内	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。	iOS：プッシュ通信サービスの利用準備が必要です。	その他ハードウェア等は不要。すぐにご利用頂けます。

※ 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

  http://www.i3-systems.com/price.html

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
secured by OneBe

Windows 向けの不正持ち出し/利用対策をご提案

CLOMO MDM secured by OneBe利用イメージ

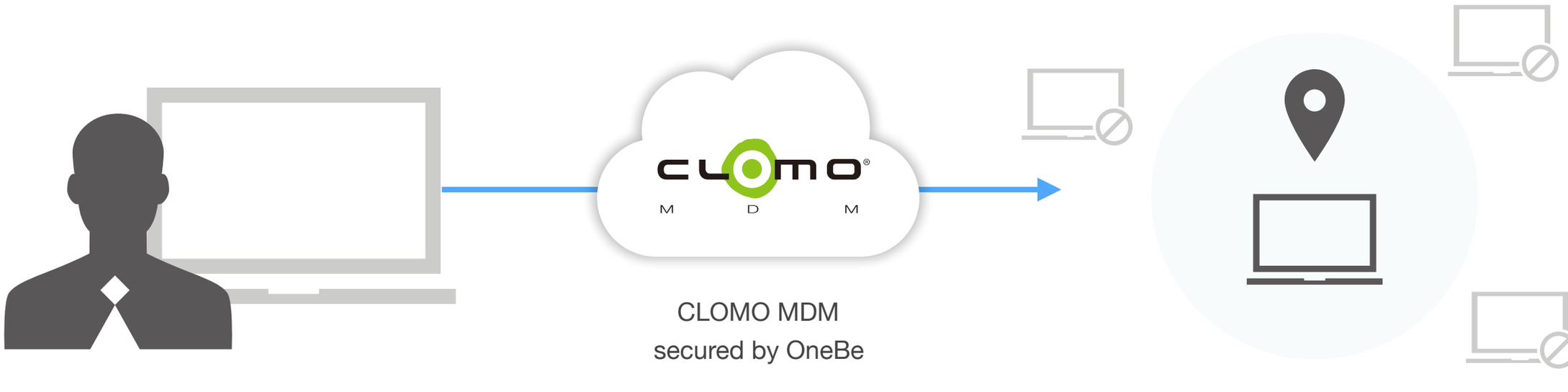
「特定エリアで利用する Windows デバイス」と「利用エリアを限定しない Windows デバイス」を一元管理しながら、利用用途や場所に応じた最適なセキュリティ対策やデバイス設定などをリモートで行えます。

■CLOMO MDM による、Windows デバイス管理のイメージ

	特定エリア			不特定エリア	
Windows デバイス 利用シーン	オフィス	倉庫	店舗	営業先	自宅
	学校	病院	etc…	移動中	etc…
CLOMO MDM 提供機能	不正持出し対策(secured by OneBe機能)			緊急時（盗難・紛失）対策	
	利用状況の監視				
	機能制限／設定の適用・解除				
	アプリのインストール・削除				

CLOMO MDM secured by OneBe利用イメージ

CLOMO MDM 管理パネルの操作で、不正持ち出し対策機能を利用できます。



管理者

デバイス持ち出し
ポリシーを配信

監視を行い、
違反検知時に対策を実施

デバイス持ち出し制限ポリシー設定項目

・ACアダプタ接続
・Wi-Fi検知
・Wi-Fi接続
・GPS(緯度経度)の指定
・パスワード認証の失敗回数　etc…

ポリシー違反検知時のアクション

・Windows ロック
・アラーム付き Windows ロック
・HID(キーボード・マウスなど)の無効化
・指定パスのフォルダやファイルを削除
etc…

CLOMO MDM secured by OneBeご利用案内

お申し込み

CLOMO MDM
お申し込み

お申し込みは5デバイス以上からとなります。

CLOMO MDM
secured by OneBe
お申し込み

5デバイスからのお申し込みが可能です。

利用開始準備

管理用サーバ設定

ご利用開始

ご利用開始

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 secured by OneBe ご利用料金

- 下記料金案内ページをご覧ください

  http://www.i3-systems.com/price.html

CLOMO MDM
Advance for Windows

Windows 向けの高度な管理機能をご提案

CLOMO MDM Advance for Windows主要機能

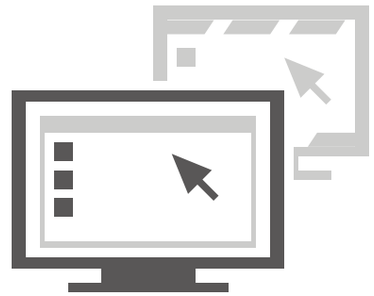
インテル vPro テクノロジー対応 Windows デバイスの高度な管理を実現できます。

インテル vPro プロセッサー領域への特別な証明書格納(※)

「インテル IPT」に対応した電子証明書の強制配信・失効機構を新たに提供します。本機能によって、サイバートラストの電子証明書を PC のインテル vPro プロセッサー内にある安全な領域に格納できるようになりました。インテル vPro プロセッサー内に格納することで、従来の OS領域に格納した電子証明書よりもなりすましや改ざんを確実に防ぐことができます。

インテル vPro プロセッサーによる特別なリモート電源ON / OFF制限

デバイスの電源ON / OFF をリモートで強制的に制御できます。「従業員のいない深夜帯に電源を切り、電源コストを削減する」「授業開始前にデバイスの電源ON を徹底し、円滑な授業進行を実現する」などを実現できます。



インテル vPro プロセッサーによる特別なリモートデスクトップ

遠隔地のデバイスに対して、インテル vPro プロセッサー内に搭載されたリモートデスクトップ機能によって、特別なソフトウェアをインストールすることなく、リモートデスクトップを行えます。ブルースクリーン状態など、OS が応答しない状態でもリモート操作を行えることが特徴です。
本機能を利用すると、「クラッシュ状態のデバイスを復旧」「OS やアプリケーションのバージョンアップ・設定変更」「従業員と同じ画面を閲覧した運用サポート」などを遠隔で行えます。

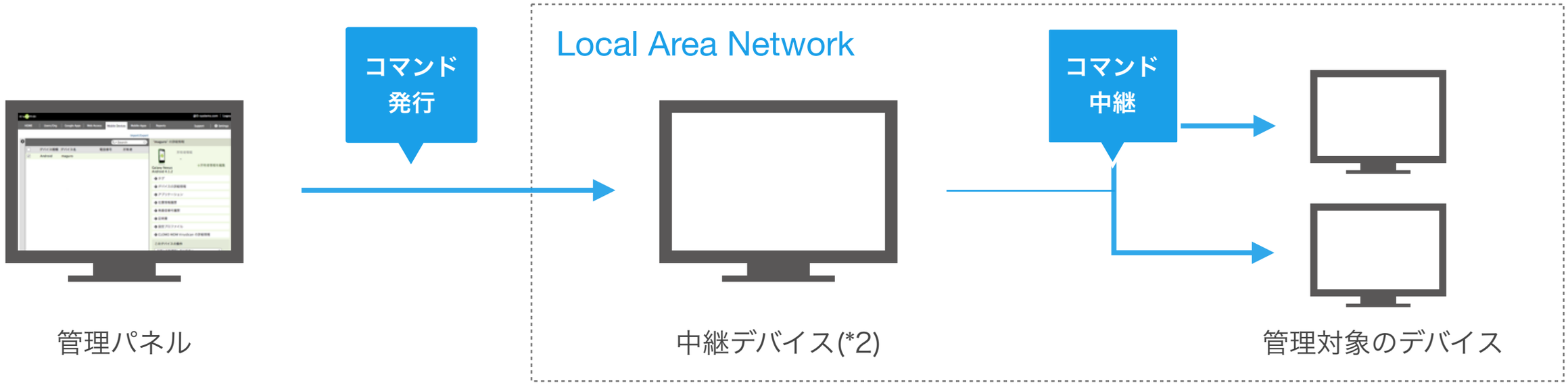
※本機能を利用するには「CLOMO MDM 証明書連携オプション」「CLOMO MPKI secured by Cybertrust」を別途ご利用頂く必要があります。

CLOMO MDM Advance for Windows機能の利用条件

インテル vPro テクノロジーによる特別な管理機能の利用条件を以下に示します。

管理対象デバイス	管理パネルを操作するデバイス	インテル vPro プロセッサーによる特別な機能		
		リモート電源ON / OFF制御	リモートデスクトップ	インテル vPro プロセッサー領域への証明書格納
LAN に接続している	管理対象と同一の LAN に接続している	○	○	○
	管理対象デバイスと異なる LAN に接続している	○ (*1)	×	○ (*1)
	LAN に接続していない	○ (*1)	×	○ (*1)
LAN に接続していない		×	×	×

※ 全てのデバイスはインターネットに接続されている必要があります。
*1：中継デバイスを設置することで、上記の条件においても本機能を利用できます。利用イメージは以下の図をご覧ください。
*2：中継デバイスは常時、電源を「ON」にしておく必要があります。



CLOMO MDM Advance for Windowsご利用案内

お申し込み

CLOMO MDM
お申し込み

お申し込みは5デバイス以上からとなります。

CLOMO MDM
Advance for Windows
お申し込み

5デバイスからのお申し込みが可能です。

利用開始準備

管理用サーバ設定

ご利用開始

ご利用開始

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 Advance for Windows ご利用料金

- 下記料金案内ページをご覧ください

  http://www.i3-systems.com/price.html

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. 20181220

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事で、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。

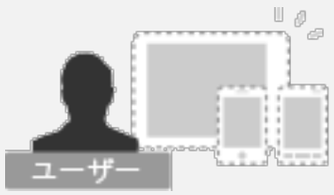
端末ロック、
端末初期化で
情報漏えいを防止

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
端末パスワードの失念

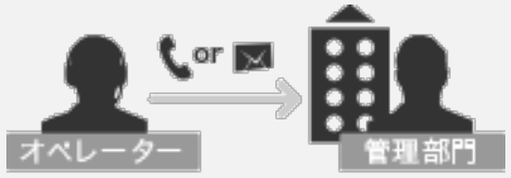
STEP 2 専用受付へ緊急電話連絡

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
端末パスワード解除の依頼

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
端末パスワード解除の実行

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	対応OS	リモートサービス詳細
端末ロック	*1	スマートデバイスが不正な操作を受け付けない様に遠隔でロックします。
紛失モード設定*2		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。
端末パスワード解除		端末ロックされたスマートデバイス発見時に、失念したパスワ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「CLOMO MDM Agent for Windows」をインストールして運用する必要があります。
*2：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」「Andorid：Android OS 2.3 以上」を満たしている必要があります。

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. 20181220

お申し込み

CLOMO MDM
お申し込み

お申し込みは5デバイス以上からとなります。

CLOMO MDM リモート
オペレーションサービス(24/365)
お申し込み

1デバイスからのお申し込みが可能です。

利用開始準備

お客様側の設定

弊社側の設定

ご利用開始

ご利用開始

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

  http://www.i3-systems.com/price.html

CLOMO MDM
証明書連携オプション

サイバートラスト社の電子証明書との連携で
さらに強固な端末認証を実現

CLOMO MDM証明書連携オプション主要メリット

MDMサービスと電子証明書で、強固な端末認証を手軽に実現できます。

	MDM単体で使用した場合	MDM＋電子証明書で使用した場合
01 スマートデバイスの盗難・紛失	何らかの理由でMDMサービスのリモート操作が正しく実行されない場合、ロック・ワイプ等が反映されず、情報漏えいの懸念が残る。	デバイスのネットワーク接続状況に関わらず、デバイスID認証局側で電子証明書の失効を行えるため、紛失したデバイスからのアクセスを確実に無効化できる。
02 ID / パスワード漏えい	Wi-Fi、VPNなど、様々な機器で ID / パスワードの変更を緊急で行う必要がある。	電子証明書が入っていないデバイスからはアクセスできないため、ID / パスワードの漏えいに慎重に対処できる。
03 私物端末からの無許可アクセス	私物パソコン・スマートフォン等から社内システムにアクセスできる為、管理者がデータやファイルの取り扱いを制御できない。	会社が許可したデバイスにのみ証明書をインストールすることで、許可していないデバイスからのアクセスを禁止できる。

CLOMO MDM証明書連携オプション主要メリット

利用用途に応じたデバイス証明書をお選び頂けるため、無駄な導入コストをかける必要がありません。

利用用途	盗難、紛失端末からの不正アクセス対策	私物端末からの不正アクセス対策	ID、パスワード情報の漏えい対策	ユーザー認証（ID、パスワード省略）	ユーザー認証（UPN形式）
CLOMO デバイス証明書 secured by Cybertrust	○	○	○	×	×
CLOMO デバイス証明書 with UPN secured by Cybertrust	○	○	○	○	○ Azure ADのSSOにも対応

CLOMO MDM電子証明書連携オプション利用イメージ

管理パネル

すべての操作を同一の管理パネルに統合

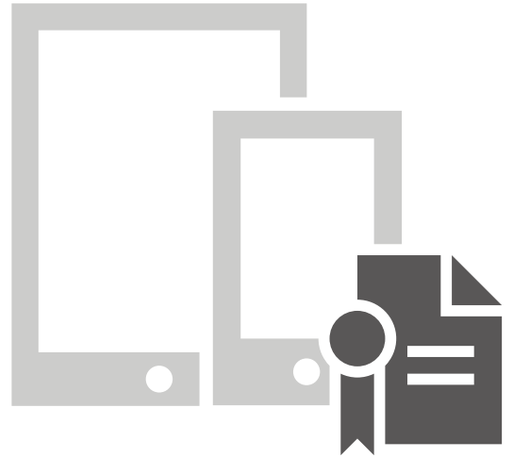
デバイス管理

・デバイスの情報取得
・デバイスの情報制限
・リモートロック/リモートワイプ

電子証明書配布

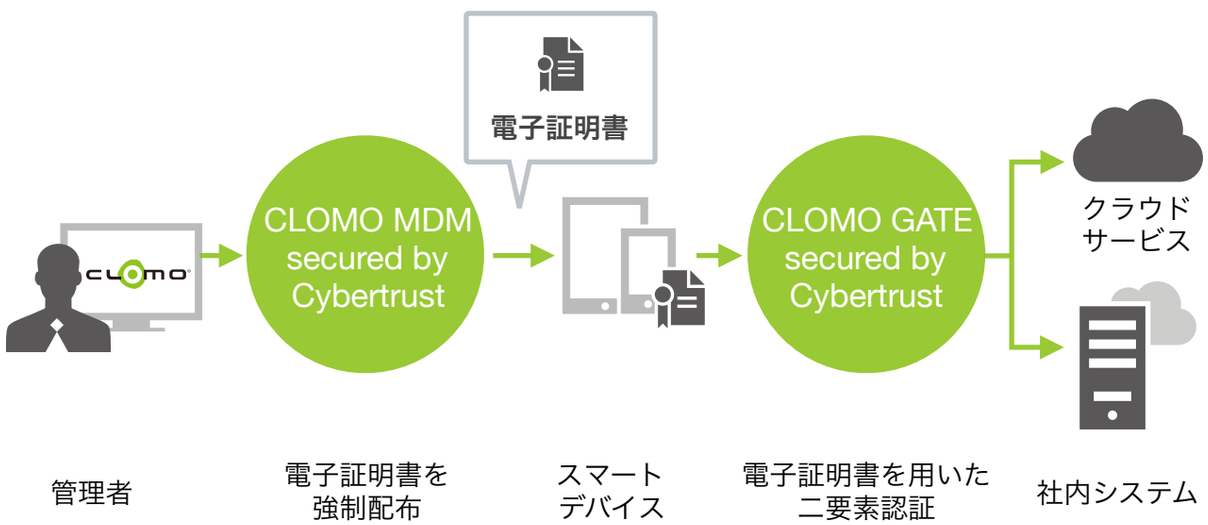
・ 電子証明書の発行・失効
・ 電子証明書のサイレントインストール(iOS / Windows)
・ 電子証明書付きのVPNやExchange
・ 設定プロファイルの配信

電子証明書を強制配布

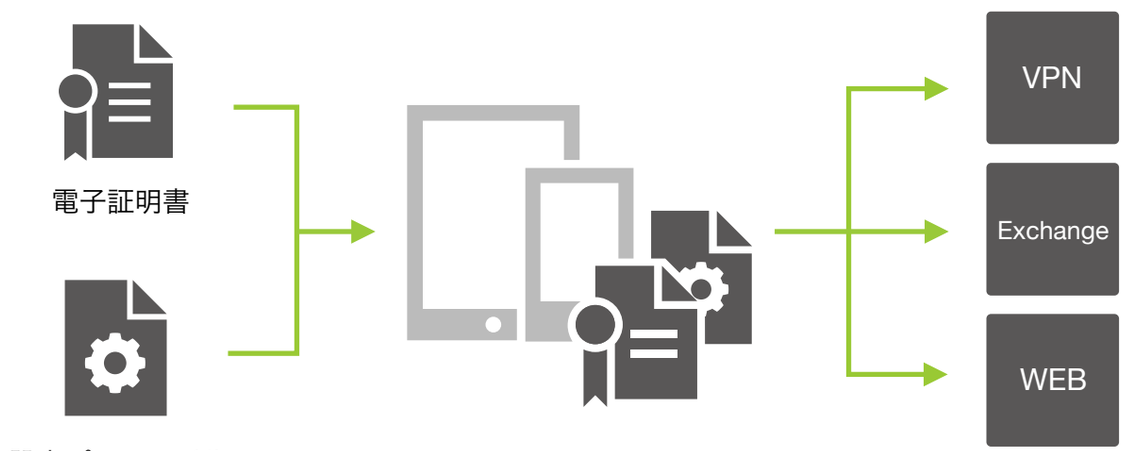


スマートデバイス

CLOMO GATE と組み合わせて、配布から認証まで一貫して実現



VPNやExchangeの設定プロファイルと電子証明書とをセットで配布



CLOMO MDM電子証明書連携オプションご利用料金

お申し込み

CLOMO MDM
お申し込み

お申し込みは5デバイス以上からとなります。

各種オプション
お申し込み

1デバイスからのお申し込みが可能です。

利用開始準備

管理用サーバ設定

ご利用開始

ご利用開始

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 電子証明書連携オプション ご利用料金

- 下記料金案内ページをご覧ください

  http://www.i3-systems.com/price.html

CLOMO MDM
アンチウィルスオプション

McAfeeのアンチウィルスエンジンを採用し
MDMとウィルス対策を完全統合

CLOMO MDMアンチウィルスオプション主要メリット

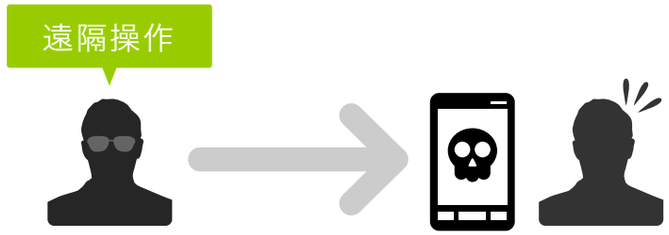
ウイルスに感染したデバイスには以下のようなリスクがあります

情報漏えいの危険性

ウィルスにより、デバイス内の**電話番号や所在地の情報を勝手に送信される**危険性がある

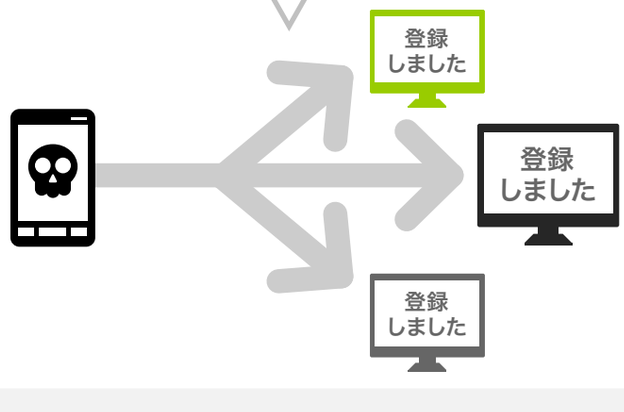
のっとりの危険性

通話の盗聴や遠隔操作など、デバイスを**第三者に乗っ取られてしまう**危険性がある



見知らぬサービスへの自動登録

見知らぬサービスやサイトに**勝手に登録され多額の利用料を請求される**危険性がある



デバイス管理とウィルス対策を完全統合し、ウィルス感染の脅威を徹底排除。

管理画面

デバイス管理

- デバイスの情報取得
- デバイスの情報制限
- リモートでのロック/ワイプ

ウイルス対策

- ウィルススキャン実行
- 定義ファイルの更新
- ウィルス感染デバイスの検知
- アプリの設定変更 など
- ウィルス感染したアプリの削除を通知
- アプリ利用ポリシーのブラックリストに追加
- ウィルス感染したアプリを起動制限 など

- ウィルススキャン（アプリ/ファイル/SDカード）
- 定義ファイルの更新など
- ライセンスアクティベーション

CLOMO MDM with McAfee An Intel Company

ウィルス検知時やデバイスにインストール済のVirus Scanアプリ削除時などの場合、管理パネルやメールにてアラート

利用端末

※ Google Play 非搭載デバイスはご利用いただけません。プロキシサーバー経由でのパターンファイルアップデートはできませんのでご注意ください。

CLOMO MDMアンチウィルスオプション利用イメージ

同一の管理パネルでデバイス管理とウィルス対策を同時に。

デバイス管理

デバイスの情報取得
デバイスの情報制限
リモートロック/リモートワイプ

ウイルス対策

ウイルススキャン実行
定義ファイルの更新
ウイルス感染デバイスの検知

MDMのリモート管理機能を生かして、より安全で効率的な対策を。

スキャン周期など ポリシーを一括設定（*1）

リアルタイムスキャン（*1）やウィルススキャンの周期やタイミングなどを一括設定することができます。

MDM管理下の 端末だけが利用許可

MDMの管理下にあるデバイスにのみアプリ利用を許可し安全な運用が可能です。

ユーザ操作による設定 変更・アプリ削除を防止

ユーザ操作によるウィルススキャンの設定変更や、アプリの削除を防ぐ事ができます。

*1：Android 5.0 以降

CLOMO MDM VirusScan アプリでは、ユーザによる自由な設定変更を防ぐ事ができます。

アプリ起動画面

設定内容は自由に閲覧可能

変更を加えようとすると強制ロック

※ Google Play 非搭載デバイスはご利用いただけません。

CLOMO MDMアンチウィルスオプションご利用案内

お申し込み

利用開始準備

ご利用開始

CLOMO MDM
お申し込み

CLOMO MDM
アンチウィルスオプション
お申し込み

管理用サーバ設定

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 アンチウィルスオプション 動作環境

- Android 4.0.3 ～

動作確認済みデバイス詳細情報
http://www.i3-systems.com/mdm.html

CLOMO MDM アンチウィルスオプション ご利用料金

- 下記料金案内ページをご覧ください

http://www.i3-systems.com/price.html

※ Google Play 非搭載デバイスはご利用いただけません。

会社概要

会社名	株式会社アイキューブドシステムズ
所在地	本社：〒815-0033 福岡県福岡市南区大橋2丁目1-1 花村ビル 東京オフィス：〒105-0013 東京都港区浜松町1丁目27-16浜松町DSビル9F
資本金	1億円
設　立	2001年（平成13年）9月
代　表	佐々木 勉
取締役	畑中 洋亮、大淵 一正、有森 正和、蓑宮 武夫（社外取締役）山形 修功（社外取締役）
監査役	秋好 徳政、永津 洋之（社外監査役）、大野 尚（社外監査役）
パートナー	Apple Japan / Apple Consultants Network Amazon Web Services LLC / AWS Advanced Technology Partner グーグル株式会社 / Android EMM Partner Microsoft / Microsoft Partner Network Silver Cloud Platform & Silver Cloud Productivity

Innovation^3