## 動作環境

### 管理者PC

| | |
|---|---|
| 対応ブラウザ | Mozilla Firefox / Google Chrome / Internet Explorer 11以上 / Microsoft Edge |
| 通信環境 | 以下ポートを解放してください。<br>・HTTPS 通信(port:443) |

### 管理対象デバイス

| | | |
|---|---|---|
| iOS / iPadOS | 対応OS | MDM構成プロファイル：iOS 10.0 ～ / iPadOS 13.1～<br>An Client（アプリ）：iOS 10.0 ～ / iPadOS 13.1～ |
| | 通信環境 | 以下ポートを解放してください。<br>・APNs(Apple Push Notification Service)による通信(port：5223)<br>・HTTPS 通信(port：443) |

| | | |
|---|---|---|
| Android | 対応OS | Android 7.0 ～ |
| | 通信環境 | 以下ポートを解放してください。<br>・FCM(Firebase Cloud Messaging)による通信(port：5228, 5229, 5230)<br>・HTTPS 通信(port：443) |

| | | |
|---|---|---|
| Windows | 対応OS | Windows 8.1, 10 の各エディション(32bit / 64bit)<br>Windows Server 2012, 2012 R2, 2016, 2019のStandard, Essentials, Datacenter |
| | 通信環境 | 以下ポートを解放してください。<br>・HTTPS 通信(port：443) |

| | | |
|---|---|---|
| macOS | 対応OS | macOS Sierra / macOS High Sierra / macOS Mojave / macOS Catalina<br>macOS Big Sur |
| | 通信環境 | 以下ポートを解放してください。<br>・APNs(Apple Push Notification Service)による通信(port：5223)<br>・HTTPS 通信(port：443) |

〈 開発・販売 〉

**エムオーテックス株式会社**

本　　社　〒532-0011 大阪市淀川区西中島 5-12-12 エムオーテックス新大阪ビル TEL：06-6308-8980
東京本部　〒108-0075 東京都港区港南 1-2-70 品川シーズンテラス 5F TEL：03-5460-1371
名古屋支店　〒460-0003 名古屋市中区錦 1-11-11 名古屋インターシティ 3F TEL：052-253-7346
九州営業所　〒812-0011 福岡市博多区博多駅前 1-15-20 NMF 博多駅前ビル 2F TEL：092-419-2390

**TEL：03-5460-1371　受付時間 9：00-18：00**（月～金曜日 祝祭日除く）
**E-mail：sales@motex.co.jp**
**URL：www.motex.co.jp**

● お問い合わせは当社へ

2021.9 発行

● 本カタログは、2021 年 9 月現在の内容となります。最新の情報は弊社Webサイトをご確認ください。
● 本カタログは予告なく変更することがあります。
画面は実際の物とは異なることがありますので、予めご了承ください。
● エムオーテックス／ MOTEX は、エムオーテックス株式会社の登録商標です。
● Google Chat はGoogle LCCの商標です。
● その他、カタログに記載の会社名、ブランド、製品、ロゴなどは、各社の商標または登録商標です。

# LANSCOPE cloud

ウイルス対策も情報漏洩対策も、この１本で。

# Secure Productivity

## 安全と生産性の両立

安全だけを追い求めても、

働く人を縛るシステムなら意味がない。

生産性だけを追い求めても、

高リスクなシステムなら意味がない。

必要なのは、安全と生産性の両立。

矛盾するように見えるこの2つの要素を

独自の技術・発想で成立させる、

それが、私たちMOTEXの使命です。

MOTEX

令和を、
平和に働く。

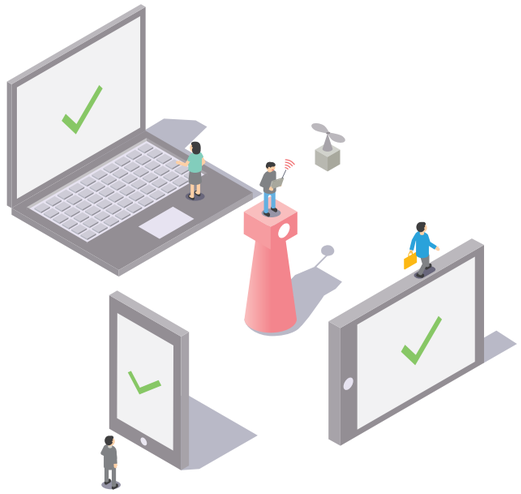
# IT資産管理とMDMを
# クラウドでカンタンに

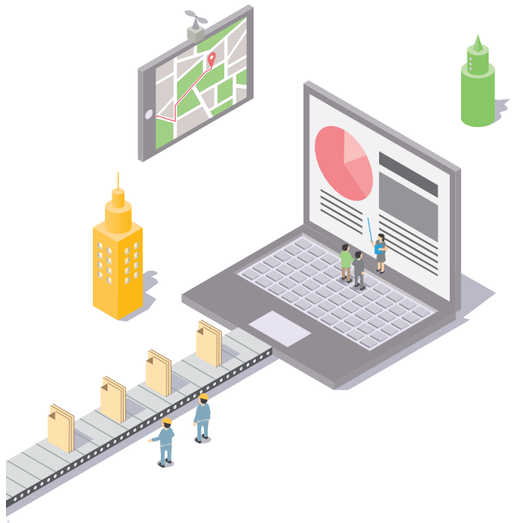
最新のLANSCOPE クラウド版は、Windows管理に必要不可欠な操作ログ取得や記録メディア制御、Windows アップデート管理機能を実装。1996年にリリースのIT資産管理ツール「LANSCOPE オンプレミス版」で培ったノウハウと充実のモバイル管理で、PC・スマホの一元管理を実現します。

# LANSCOPE cloud 3つの特長

## 1. ITreview リーダー獲得 圧倒的に使いやすい管理コンソール

LANSCOPE クラウド版ならではの「使いやすさ」を追求したシンプルなメニュー、分かりやすいレポート。
レビュープラットフォーム「ITreview」では MDM・EMM（モバイルデバイス管理）部門において Leader を獲得。
お客様からも高い評価を頂いています。





## 2. 操作ログ管理まで実現した 充実のWindows管理

アプリの利用、Web サイトの閲覧、Wi-Fi 接続など、「どの PC で」「誰が」「いつ」「どんな操作をしたか」など PC の利用状況を把握できます。またレポート機能は、システム管理者だけでなく、現場のマネージャー・メンバー間で共有し、活動や成果の「見せる化」をすることで、働き方の改善や人の育成をサポートします。

## 3. Apple と Google の プログラムに対応した 充実の iOS・Android 管理

LANSCOPE クラウド版はモバイル管理に不可欠なApple Business Manager、Android Enterprise に対応。紛失対策だけではなく、デバイスの利用制御・アプリ管理など高度なモバイル管理を実現し、組織の PC・スマホ・タブレットの一元管理を可能にします。

# PC・スマホを充実の機能で一元管理
# 多機能でも「使いやすさ」を徹底的に追求します。

アイティクラウド社が運営する法人向けIT製品・SaaSのレビューサイト「ITreview」で「Leader」を獲得。
「ITreview Best Software in Japan 2021」にて
満足度・認知度ともに優れているとして、TOP50に選出されました。

ITreview LEADER 2021 SUMMER

ITreview Best Software in Japan 2021 TOP 50

MDM・EMM
（モバイルデバイス管理）

**社内情報システム マネージャー**
**（従業員 100〜300 名）**

**直感的にわかりやすいUI。**利用者向けのインストールガイドのひな型も用意されており、社員向けの手順書作成の手間も抑えられた。モバイル機器だけでなくWindows PCも含めて管理できる。**Windowsも管理できる事を考えると導入コストが非常に安い。**

**IT管理者**
**（従業員 300〜1,000 名）**

安価で利用できるのに、情シスが管理すべき項目をほぼ網羅できているソフトです。**操作もしやすく、マニュアルを見なくても大体の操作は可能です。**IT初心者でも簡単に管理できるソフトなので、どなたにもお勧めです。

**社内情報システム**
**（従業員 100〜300 名）**

これまで、いくつかの管理ツールを利用してきたが、**機能＆管理画面の使いやすさ等が高水準でまとまっており**、とても使いやすい。国産アプリなので、変な日本語訳もなく、管理画面がスッキリとまとまっているのも良い。



# 機能一覧

| | | | iOS／iPadOS | Android | Windows | macOS |
|---|---|---|---|---|---|---|
| 資産管理 | デバイス情報の取得 | 電話番号やOSバージョンなどのデバイス情報を自動取得、また使用者名やリース期限など自動取得できない項目も任意項目として管理できます。 | ○ | ○ | ○ | ○ |
| | デバイス情報の編集／台帳化 | 取得したデバイス情報を一覧で表示、管理コンソール上での編集や検索ができます。 | ○ | ○ | ○ | ○ |
| | インストールアプリ管理 | 社内で利用されているアプリの情報を自動取得し、アプリごと、デバイスごとに表示できます。 | ○ | ○ | ○ | ○ |
| | アプリインストール禁止 | Google Play や App Store の利用を禁止し、新規アプリのインストールを制限できます。 | ○※1 | ○ | − | × |
| | アプリ利用禁止 | 特定のアプリの利用を禁止できます。 | ○※1 | ○ | ○ | × |
| | アプリ・ファイル配信 | 業務上インストールが必要なアプリやファイルをデバイスに一括で配信できます。 | ○ | ○※2 | ○ | × |
| | アプリカタログ | 管理者が設定したアプリをデバイスに公開し、利用者のタイミングでインストールやアップデートができます。 | ○ | − | − | − |
| | メッセージ／アンケート | 管理者からユーザーに対して、メッセージやアンケートを送信できます。 | ○ | ○ | ○ | × |
| | 省電力管理 | Windowsの省電力設定の一括変更ができます。 | − | − | ○ | − |
| 位置情報管理 | 最新位置情報 | デバイスの位置情報を自動で取得し、複数デバイスの位置情報を地図上でまとめて表示できます。 | ○ | ○ | ○※4 | × |
| | 移動履歴 | デバイスの位置情報を定期的に自動取得し、移動の履歴を地図上で表示できます。 | ○ | ○ | ○※4 | × |
| 紛失・盗難対策 | リモートロック／ワイプ※3 | 遠隔で画面ロックやデータの初期化ができます。 | ○ | ○ | ○ | ○ |
| | パスワードポリシー | パスワードの桁数や英字、数字、複合文字使用など、パスワードの設定ルールを一括で設定・配布できます。 | ○ | ○ | × | × |
| | BitLocker 復元キー取得 | 回復キー48桁の情報を自動収集できます。 | − | − | ○ | − |
| セキュリティ | 資産アラート設定 | 未稼働日数やリース期限、OSバージョンなど、資産情報に関するアラートを設定できます。 | ○ | ○ | ○ | ○ |
| | Windows アップデート管理 | FU や QU の適用状況を把握し、デバイスに最新のプログラムを配信できます。 | − | − | ○ | − |
| | 記録メディア制御 | グループ単位で USB メモリなどの利用を禁止、また会社支給の USB のみ許可などの除外設定ができます。 | − | − | ○ | × |
| | Wi-Fi・Bluetoothの接続制御 | 特定の Wi-Fi への接続のみを許可するなど、Wi-Fi・Bluetooth の接続制御ができます。 | ○※1 | ○※2 | ○ | × |
| | Jailbreak／root 化検知 | Jailbreak/root 化されたデバイスを検知できます。 | ○ | ○ | − | − |
| | SIMカード挿入状態検知 | SIMカードの挿入状態の変化を検知することができます。 | ○ | ○ | ○ | − |
| | Windows Defender 情報取得 | Defender のバージョンやパターンバージョンなどの情報を自動取得できます。 | − | − | ○ | − |
| レシピ | トリガー | 「LANSCOPE クライアントがインストールされたら」など、アクションを実行する条件を設定できます。 | ○ | ○ | ○ | ○ |
| | アクション | 「アラートに設定する」「アンケートを配信する」などデバイスに自動実行する内容を設定できます。 | ○ | ○ | ○ | ○ |
| 操作ログ管理（モバイル） | デバイス活用ログ | デバイスを実際に操作している時間を取得できます。 | ○※5 | ○ | − | − |
| | アプリ利用ログ | アプリの利用情報を取得できます。 | × | ○ | − | − |
| | 電話利用ログ | 電話の発着信情報（日時、通話相手、通話時間）を取得できます。 | ○※5 | ○ | − | − |
| 操作ログ管理（PC） | ログオン・ログオフログ | 電源 ON・OFF・ログオン・ログオフのログを取得できます。 | − | − | ○ | × |
| | ウィンドウタイトルログ | デバイス上での閲覧画面（ウィンドウタイトル・アプリ名）のログを取得できます。 | − | − | ○ | × |
| | ファイル操作ログ | デバイス上でのファイル操作（ファイル・フォルダのコピー／移動／作成／上書き／削除／名前の変更）でのログを取得できます。 | − | − | ○ | × |
| | Web アクセスログ | Web サイトの閲覧、Web メールやクラウドストレージのアップロード／ダウンロードログを取得できます。 | − | − | ○ | × |
| | Web アクセス禁止 | URL やウィンドウタイトルが、設定したキーワードに抵触した場合、閲覧を禁止できます。 | − | − | ○ | × |
| | プリントログ | 印刷状況を記録し、ドキュメントやプリンター、PC ごとに印刷枚数を集計できます。 | − | − | ○ | × |
| | 通信機器接続ログ | Wi-Fi ／ Bluetooth ／有線の接続を把握し、管理外の接続を検知できます。 | − | − | ○ | × |
| | アプリ稼働ログ | アプリの稼働情報を取得できます。 | − | − | ○ | × |
| | アプリ通信ログ | 通信元／先の IP アドレスやポート番号、アプリのハッシュ値を取得できます。 | − | − | ○ | × |
| レポート | 残業注意のデバイス | 業務時間外の利用時間から、長時間労働につながるデバイスを把握できます。 | × | × | ○ | × |
| | デバイスの放置時間 | スクリーンセーバーや画面ロックの時間から、放置時間が多いデバイスを把握できます。 | × | × | ○ | × |
| | デバイスの業務利用時間 | 業務に関するアプリ利用や Web 閲覧の時間から、業務活用度が高いデバイスを把握できます。 | × | × | ○ | × |
| | セキュリティレベルの低いデバイス | アラートの状態から、改善が必要なデバイスを把握できます。 | ○ | ○ | ○ | ○ |
| | 長期間未稼働のデバイス | 長期間電源が入っていない、紛失の可能性があるデバイスを把握できます。 | ○ | ○ | ○ | ○ |
| | デバイスの利用時間 | 実際の利用時間から、活用の促進や配置変換が必要なデバイスを把握できます。 | ○ | ○ | × | × |
| | 電話の利用時間 | 通話の時間から、適切なプランに変更するなど費用削減につながるデバイスを把握できます。 | ○ | ○ | − | − |
| | カテゴリ別のアプリ利用時間 | アプリの利用時間から、よく利用されているアプリのカテゴリを把握できます。 | × | ○ | × | × |
| Apple社提供プログラム対応一覧 | 構成プロファイル情報取得 | デバイスにインストールされている構成プロファイルの情報を自動で取得できます。 | ○ | − | − | ○ |
| | 構成プロファイル配信・削除 | 構成プロファイルを各デバイスに配信、削除ができます。 | ○ | − | − | × |
| | 自動デバイス登録（DEP） | デバイスを自動的に MDM の管理下に置き、デバイス登録に必要な作業の工数を削減できます。 | ○ | − | − | × |
| | アプリの一括配信（VPP） | 一括入手したアプリをデバイスに配信できます。 | ○ | − | − | × |
| | 紛失モード | 回収用メッセージを表示した強制ロックを実行し、位置情報を強制的に取得できます。 | ○ | − | − | × |
| Android Enterprise※6 | デバイス利用制御 | カメラや外部メディアの利用など、デバイスの利用制限を行うことができます。 | − | ○ | − | − |
| | アプリ管理 | 管理者がホワイトリスト／ブラックリスト方式で利用アプリを制御できます。 | − | ○ | − | − |
| | キオスクモード | 特定アプリ以外利用できないようにするなどデバイスの利用を限定できます。 | − | ○ | − | − |
| その他 | 24/365 紛失サポート | 24時間365日、専門スタッフがリモートロックもしくはワイプを管理者に代わり実行します。 | ○ | ○ | ○ | ○ |

○…対応　×…未対応　−…OS仕様により非対応

※1 デバイスを監視モードに設定する必要があります。 ※2 Android Enterprise を利用する必要があります。
※3 OSによって仕様が異なります。Windows Server OS は未対応です。 ※4 Windows7・Windows Server OS は未対応です。
※5 取得条件があります。電話利用ログは通話相手は取得できません。 ※6 Android6.0 以降のデバイスが対象です。

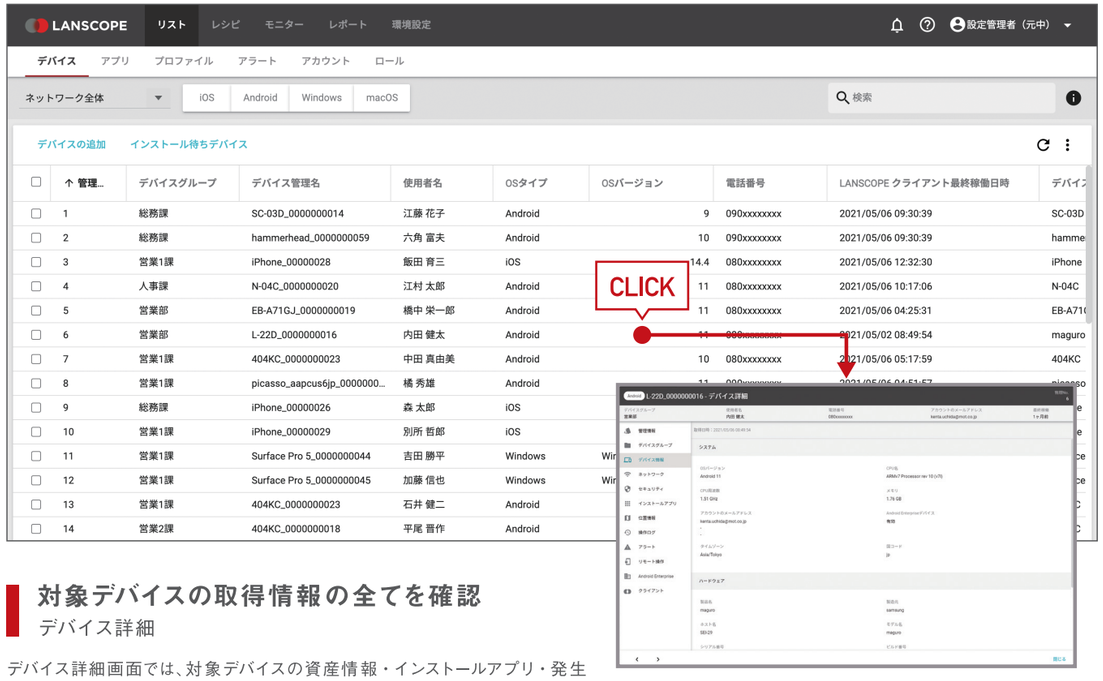
# 資産管理

iOS / iPadOS　Android　Windows　macOS

## ハードウェア・インストールアプリの情報を自動取得
## デバイスの状態を手間なく把握・管理します。

デバイスの資産情報を自動で取得し、iOS・iPadOS・Android・Windows・macOSの混在環境や、複雑なOSバージョン管理の手間を削減。アプリの利用ルールなどに抵触したデバイスは管理者にメールで通知し、迅速に対応できます。

### 必要な情報をわかりやすく表示




### 対象デバイスの取得情報の全てを確認
デバイス詳細

デバイス詳細画面では、対象デバイスの資産情報・インストールアプリ・発生アラート・移動履歴などを確認できます。また、リモート操作の実行も可能です。

### ハードウェア情報・設定情報を自動取得
資産管理

デバイスの資産情報（自動取得項目・編集可能項目）を一覧で管理できます。（以下は抜粋です）

| iOS / iPadOS | |
|---|---|
| OS バージョン | iCloud バックアップ |
| シリアル番号 | 加入キャリア |
| IMEI | Jailbreak |
| 監視モード | モデル名 |
| アクティベーションロック | ストレージ使用容量 |
| 電話番号 | 電池残量 |
| データローミング | iPhoneを探す |
| デバイス名 | 最新 iCloud バックアップ日時 |
| UDID | MAC アドレス（Wi-Fi） |
| MEID | パスコードロック |
| 紛失モード | |

| Android | |
|---|---|
| OS バージョン | IP アドレス |
| モデル名 | SIM のシリアル番号 |
| IMEI | root 化 |
| CPU 名 | 製品名 |
| Wi-Fi 状態 | 内部ストレージ使用容量 |
| サーバーアドレス | ブランド名 |
| モバイルネットワーク設定 | MAC アドレス（Wi-Fi） |
| メールアドレス1～3 | DHCP IP アドレス |
| シリアル番号 | 加入キャリア |
| ハードウェア名 | パスワードポリシー |
| 電話番号 | |

| Windows | |
|---|---|
| OS バージョン | CPU 名 |
| メモリ | ドメイン・ワークグループ名 |
| ログオンユーザー名 | コンピューター名 |
| 製品名 | 製造元 |
| シリアル番号 | IMEI |
| システムドライブ | ボリューム名 |
| ストレージ使用容量 | CPU コア数 |
| プロセッサ数 | Windows プロダクト ID |
| NIC 情報 | 電話番号 |
| 現在のキャリア | Windows アップデート |
| Defender バージョン | CylancePROTECT バージョン |

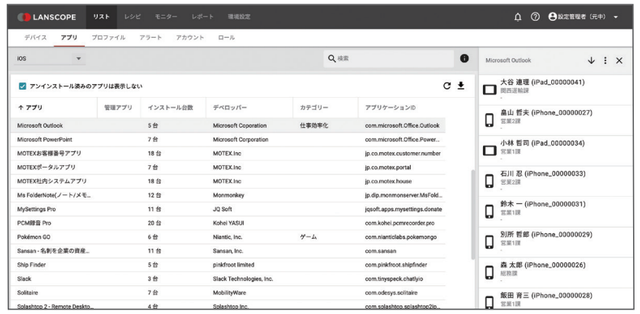
| macOS | | |
|---|---|---|
| OS バージョン | モデル名 | ホスト名 |
| シリアル番号 | UDID（ハードウェア UUID） | ストレージ使用容量 |
| IMEI | iTunesStoreIdHash | MAC アドレス（Bluetooth） |
| iCloud バックアップ | MAC アドレス（イーサネット） | |
| ビルドバージョン | デバイス名 | |

| 編集可能項目 | | | |
|---|---|---|---|
| 送信先メールアドレス | デバイス管理名 | 前回棚卸し実施結果 | 前回棚卸し実施日 |
| 使用者名 | デバイスグループ階層 1～5 | デバイスタイプ | 任意項目 1～20 |
| 導入金額 | 使用者の組織名 | Apple ID | |
| 月額費用 | 導入タイプ | 導入日 | |
| 前回棚卸し実施者 | 購入先 | 期限（リース / 償却） | |



### アプリ情報の管理
インストールアプリ管理

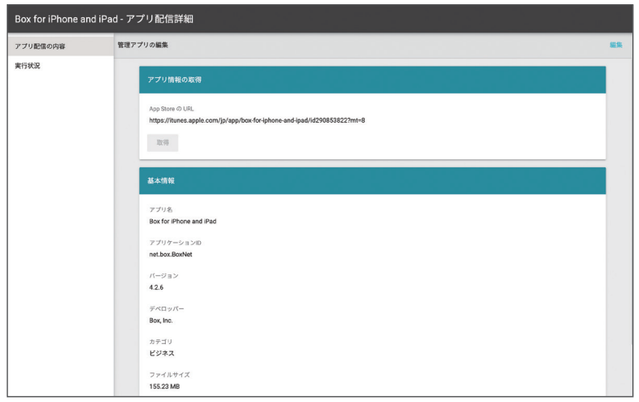
デバイスにインストールされているアプリを【デバイスごと】【アプリごと】に一覧表示し、禁止 / 不許可 / 許可などを設定できます。



### 業務に必要なアプリを配信
アプリ・ファイル配信

業務上インストールが必要なアプリやファイルを管理デバイスに一括で配信、サイレントインストール、アプリカタログへの配信など、OS・利用シーンに応じて配信方式を選択できます。

※ macOS は非対応です。
※ アプリ・ファイル配信の仕様は OS によって異なります。
※ Android のアプリ配信は、Android Enterprise を利用する必要があります。




### 必要な情報を簡単に収集
メッセージ・アンケート機能

管理者からユーザーに対して、アンケートを送信できます。Apple IDや所属部署など自動収集できない情報を、自由記述やプルダウン形式で回答してもらい、回答結果を確認後、管理コンソールに反映できます。

※ macOS は非対応です。

## User's voice

全国に点在する PC・スマホ合計2,000台を
LANSCOPE クラウド版で一元管理。
資産管理の効率化を実感しています。

これまで PC は資産管理ツールで、モバイルは Excel で資産管理を行っていました。しかし、管理対象のデバイスが増え、管理手法が異なることに限界を感じていました。LANSCOPE クラウド版は PC・スマホを同じ画面で管理できるので、半年に 1 回の資産棚卸の効率化にもつながりました。

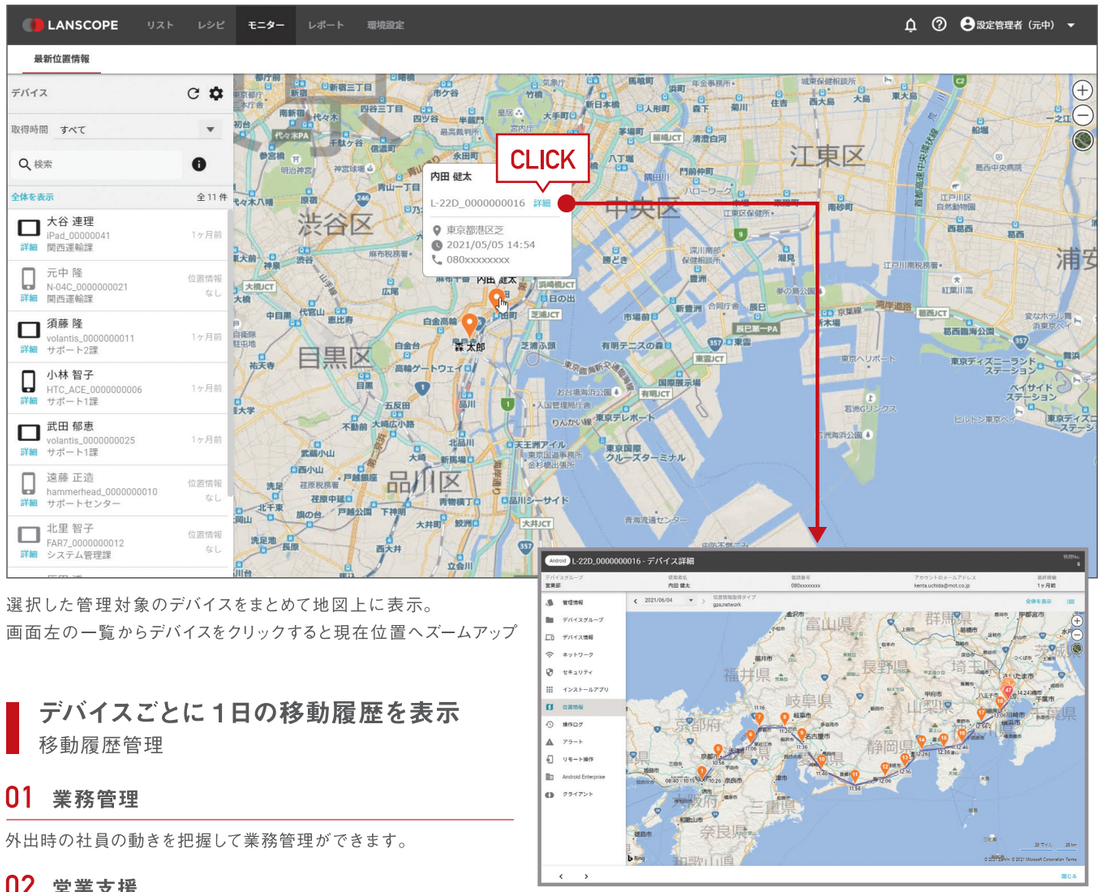
# 位置情報管理

iOS / iPadOS　Android　Windows

## 位置情報を自動取得し、デバイスがどこにあるか一目でわかります。

複数デバイスの所在を地図上に表示し、一目で把握できます。また、移動履歴を記録し、行動管理や紛失・盗難時の発見の手掛かりとしても役立ちます。取得する曜日や時間帯を任意で設定できるので、プライバシーも安心です。

### 複数デバイスの最新位置情報をまとめて表示




選択した管理対象のデバイスをまとめて地図上に表示。
画面左の一覧からデバイスをクリックすると現在位置へズームアップ

※ Windowsの場合、スリープ時は位置情報を取得できません。
　また、Windows 7、Windows Server OS は未対応です。
※ 位置情報の取得精度は、機種及びネットワーク状況によって異なります。

### デバイスごとに１日の移動履歴を表示

移動履歴管理

**01　業務管理**

外出時の社員の動きを把握して業務管理ができます。

**02　営業支援**

複数デバイスの位置を同時に確認。スムーズな営業支援ができます。

**03　紛失対策**

万が一デバイスを紛失しても所在がすぐに確認できます。

### User's voice

**万が一の紛失、
電源がOFFになっていると対策が打てない！
でも、LANSCOPE クラウド版なら…**

営業担当者から紛失の連絡があり、探そうとキャリアに連絡しても既に電源がOFFに…LANSCOPE クラウド版の導入後は電源OFFになる前の位置情報を把握でき、付近の交番に届けられているデバイスを無事に発見。これまでに2台の紛失デバイスの発見につながっています。

# 紛失・盗難対策

iOS / iPadOS　Android　Windows　macOS

## 紛失の事前対策から、万が一の紛失時の対策を実現します。

万が一の際にリモートでデバイスの画面ロックやワイプ（初期化）を実行できます。またパスワード設定の一括適用や利用ルールの違反状況の確認など、リスクを事前に把握してトラブルを未然に防ぐことができます。

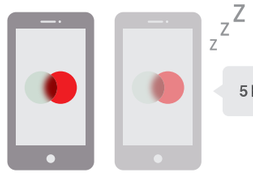
### 紛失に備えた事前の対策

**パスワードポリシーの一括適用**

（iOS / iPadOS、Android対応）

- 数字６桁以上
- 10回連続失敗で初期化
- ６ヶ月毎に変更

**デバイスの稼働状況を確認**




５日間未稼働

管理コンソールから
デバイスの状態を把握！また管理者に
メールでお知らせすることもできます。

### 万が一の紛失時の対策

**STEP 1　位置情報を確認**

（iOS / iPadOS、Android、Windows 8.1 以降対応）

**STEP 2　リモートロック・ワイプを実行**

**紛失モード　iOS / iPadOS**

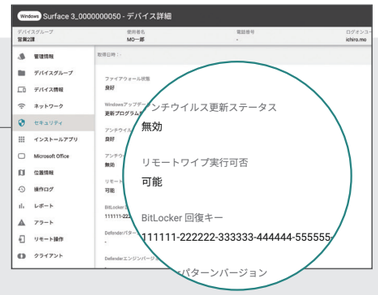
管理コンソールから紛失モードを有効にすることで、強制ロックを実行し、回収用のメッセージと連絡先情報を紛失デバイスの画面に表示します。さらに強制的に位置情報を取得できます。

※ iOS9.3以上、監視モードに設定されているデバイスのみ対象

PICK UP

### BitLockerを利用した紛失対策を実現！

Windows 10ではドライブ暗号化機能であるBitLockerが標準で搭載されました。LANSCOPE クラウド版ではBitLockerによる暗号化の設定有無の状況や回復キーを取得できます。また万が一の紛失時にはリモートワイプ機能で回復キーをデバイスから削除、起動できない状態にできます。




### User's voice

**デバイスの利用ルール違反を
アラートですぐに発見！
セキュリティ状況が把握でき安心です。**

社内で利用ルールなども特に決めないままスマートフォンを導入したため利用者がどのように使っているのか見当がつかず、ずっとセキュリティ面で不安に感じていました。LANSCOPE クラウド版を導入してから、利用者の設定変更や利用ルール違反もアラートですぐに確認できるので、セキュリティ状況の把握に役立っています。

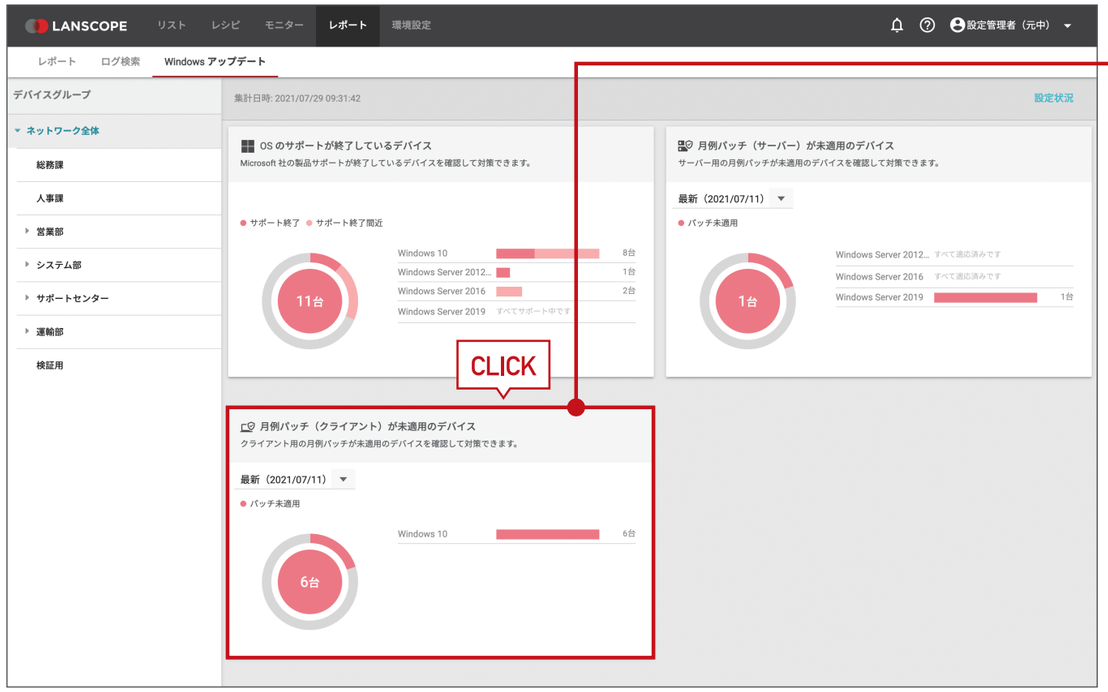
# セキュリティ（Windows アップデート管理）

Windows

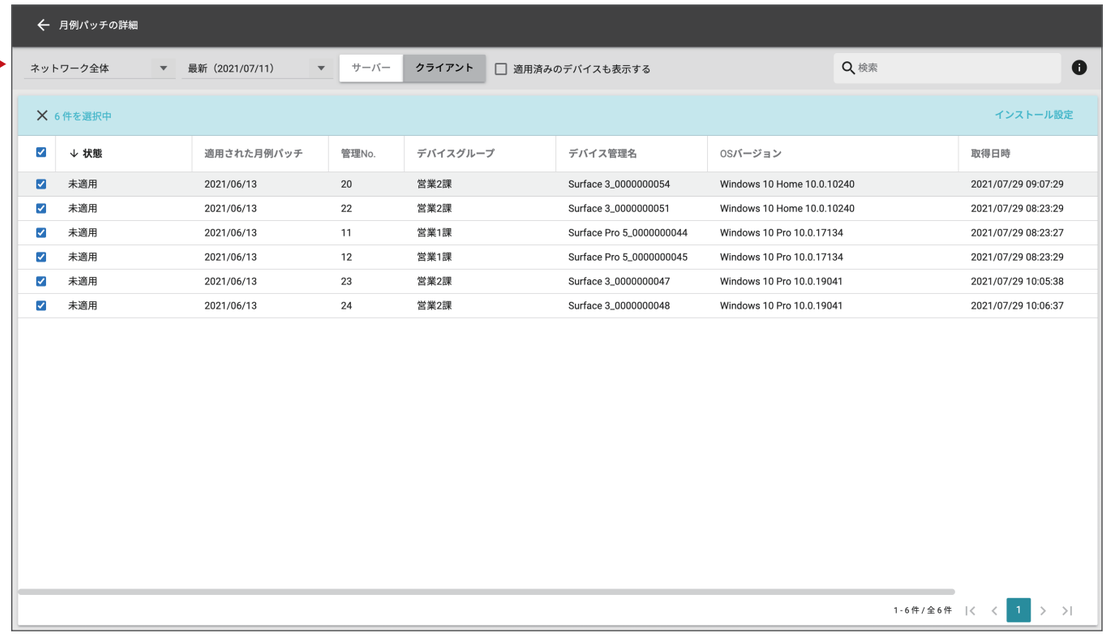
## 最新の FU・QU が未適用デバイスの把握から最新 OS の適用まで。

Windows PC の最も基本的なセキュリティ対策は、Windows OS を最新の状態に保つことです。Windows の機能強化が伴う機能更新プログラム（Feature Updates［FU］）、脆弱性の対応や品質向上などを含む品質更新プログラム（Quality Updates［QU］）の適用状況を把握し、配信まで実現します。

### FU・QU の適用状況をレポート化




### ドリルダウンで未適用のデバイスを特定し、最新の FU や QU を適用




アップデート配信を行うデバイスを選択し、インストール設定を行います。
設定後、デバイスに配信が行われます。

#### ● OS のサポートが終了しているデバイス

Microsoft 社の製品サポートが終了しているOS が残っていないか把握できます。

#### ● 月例パッチ（サーバー）が未適用のデバイス

Microsoft 社の月例パッチ（品質更新プログラム）が未適用のサーバーがないか把握できます。

#### ● 月例パッチ（クライアント）が未適用のデバイス

Microsoft 社の月例パッチ（品質更新プログラム）が未適用のクライアントがないか把握できます。

### User's voice

**テレワーク・社外 PC の アップデート管理の徹底に貢献！**

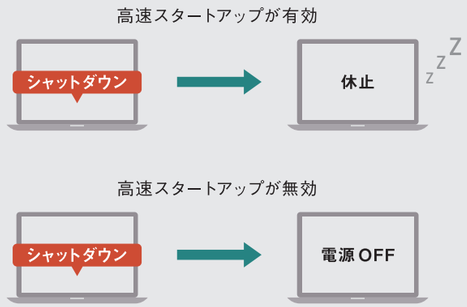
テレワークの実施等で、社内ネットワークにアクセスされないPCのアップデート管理に困っていました。LANSCOPE クラウド版は、最新のOS にアップデートできていないPCをひと目で把握できるだけでなく、クリック操作でアップデート配信までできるため、アップデート管理の課題を解決できました。

PICK UP

### アップデート配信後の「高速スタートアップ」を 一時無効化

最新の QU をデバイスにインストール後、アップデートを適用するためには、デバイスのシャットダウンまたは再起動が必ず必要です。しかし、Windows デバイスで「高速スタートアップ」の機能が有効になっている場合、シャットダウン後は「休止」状態となり、復帰後に正しくアップデートが適用されません。

LANSCOPE クラウド版では、シャットダウン後の次の起動で正しくアップデートが適用されるよう配信完了後に、高速スタートアップを一時的に無効化する機能を実装しています。



# セキュリティ（記録メディア制御）

Windows

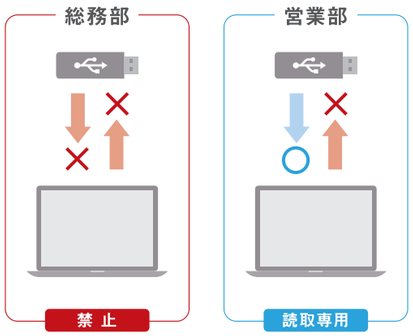
## USBメモリなどの記録メディアの利用を制御し、情報漏えいを防止します。

グループ単位でUSBメモリなどの利用を禁止、また会社支給のUSBのみ許可などの除外設定ができます。禁止だけでなく読取専用の設定（書込み禁止）や、設定した日時のみ利用を許可するなど柔軟な設定が可能です。

### 記録メディア制御

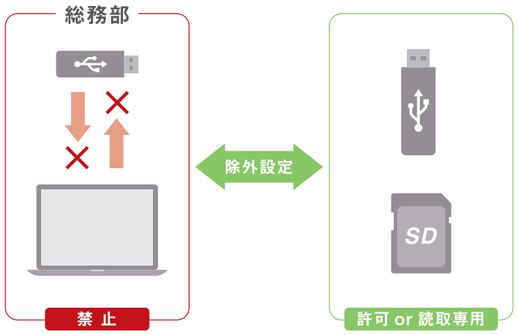
#### STEP 1 グループ単位で利用制御をする

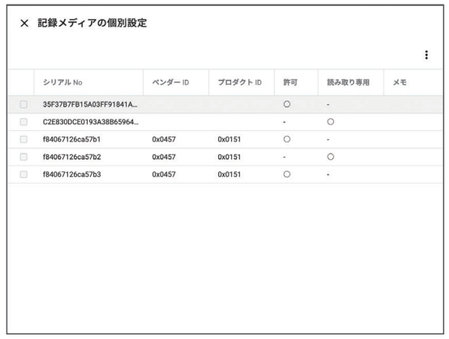
総務部は禁止、営業部は読取専用などグループ単位で記録メディアの「許可」「読取専用」「禁止」の設定を行います。
そのグループに所属する全てのデバイスに対して設定が適用されます。また禁止時にポップアップでデバイスにメッセージを通知できます。



#### STEP 2 除外設定を行う（グループ単位で禁止、読取専用の設定を行っている場合）

グループ単位で「禁止」または「読取専用」の設定を行っている場合に、「シリアル No」「ベンダー ID」「プロダクト ID」のいずれかで許可する記録メディアを設定できます。また特定の PC のみ利用を許可する、指定した日時のみ許可する設定も可能です。




### User's voice

**USBメモリの利用は原則禁止**
**業務に必要な場合は除外設定で運用**

業務上、USB メモリなどの記録メディアはほとんど利用していません。しかし、一部の部署で USB メモリを利用する必要があるため、会社で購入したセキュリティ USB のみを除外設定し、利用してもらっています。記録メディアへの書込みもログとして取得しているので、利便性を落とさずにセキュリティ対策に取り組めています。



# レシピ

iOS / iPadOS　Android　Windows　macOS

## 「自動化」でデバイス管理にかかる工数を削減します。

あらかじめ設定した条件（トリガー）に一致したデバイスに対し、アプリやメッセージの配信など指定したアクションを自動実行します。デバイス管理にかかる工数が減るため、管理者様はより生産性の高いシゴトに集中できます。

**トリガー**
「LANSCOPE クライアントがインストールされたら」
「設定した曜日・時間になったら」など、
アクションを実行する条件を設定します。

**アクション**
「指定アプリを配信する」
「アンケートを配信する」など
デバイスに自動実行する内容を設定します。

### トリガー・アクション一覧
レシピ

● 設定可能なトリガー

| | | iOS / iPadOS | Android | Windows | macOS |
|---|---|---|---|---|---|
| デバイス情報 | リモートロックの実行が成功した | ○ | ○ | ○ | ○ |
| | LANSCOPE クライアントがインストールされた | ○ | ○ | ○ | × |
| | パスワードポリシーに準拠していない | ○ | ○ | × | × |
| | デバイスが管理外になっている | ○ | × | ○ | ○ |
| | LANSCOPE Client のバージョンが最新になっていない | ○ | ○ | ○ | ー |
| | 未稼働期間が指定された期間を超過している | ○ | ○ | ○ | ○ |
| | 指定したアプリがインストールされている | ○ | ○ | ○ | ○ |
| | 指定したアプリがインストールされていない | ○ | ○ | ○ | ○ |
| | パスコードロックの設定がオフになっている | ○ | × | × | × |
| | デバイスが不正に改造されている（Jailbreak / root 化） | ○ | ○ | ー | ー |
| | iOSのバージョンが指定した範囲外になっている | ○ | ー | ー | ー |
| | Androidのバージョンが指定した範囲外になっている | ー | ○ | ー | ー |
| | SIM カードが抜き差しされた | ○ | ○ | ○ | ー |
| | デバイスの設定がリモート操作の実行条件を満たしていない | × | ○ | ○ | × |
| | もうすぐリース切れになる | ○ | ○ | ○ | ○ |
| | ログが取得されない設定になっている | × | ○ | ー | ー |
| | 空き容量が不足している | ○ | ○ | ○ | ○ |
| | 新規プロファイルがインストールされた | ○ | ー | ー | ○ |
| 操作ログ情報 | 新しくアプリがインストールされた | × | ○ | × | × |
| | 指定したアプリが実行された | × | ○ | × | × |
| | SD カードが抜き差しされた | ー | ○ | × | × |
| | タイムゾーンが変更された | × | ○ | × | × |
| 位置情報 | 位置情報が取得されない設定になっている | × | ○ | ○ | × |
| 任意のタイミング | 任意のタイミングで実行する | ○ | ○ | ○ | ○ |
| | 定期的に実行する | ○ | ○ | ○ | ○ |

● 設定可能なアクション

| | iOS / iPadOS | Android | Windows | macOS |
|---|---|---|---|---|
| 管理者にメールでお知らせする | ○ | ○ | ○ | ○ |
| 指定プロファイルを配信する | ○ | ー | ー | × |
| 指定アプリを配信する | ○ | × | × | × |
| 指定VPPアプリを配信する | ○ | ー | ー | × |
| メッセージを配信する | ○ | ○ | ○ | × |
| アンケートを配信する | ○ | ○ | ○ | × |
| アラートに設定する | ○ | ○ | ○ | ○ |
| アラートレポートを送信する | ○ | ○ | ○ | ○ |
| 指定プロファイルを取り除く | ○ | ー | ー | × |
| 指定アプリをアンインストールする | ○ | × | × | × |
| 指定VPPアプリをアンインストールする | ○ | ー | ー | × |
| 操作ログを一括で出力する | ○ | ○ | × | × |
| 位置情報を一括で出力する | ○ | ○ | ○ | × |
| 指定プロビジョニングプロファイルを配信する | ○ | ー | ー | ー |
| 指定プロビジョニングプロファイルを取り除く | ○ | ー | ー | ー |

### User's voice

**インストールは簡単！**
**デバイスのキッティングにも大きく貢献**

管理コンソール上の QR コードを iPhone で読み取るだけで、LANSCOPE をインストールできました。また、インストールされたデバイスには、指定したアプリを自動で配信できるので、基幹業務のアプリを全台に漏れなく整備でき大変助かりました。

# 操作ログ

iOS / iPadOS　Android　Windows

## PC・スマホの操作ログを自動取得し、抑止効果を発揮します。

「どの PC・モバイルで」「いつ」「どんな操作をしたか」など利用状況を把握できます。ログを取得する＝見られているという意識をもたらし、デバイスの利便性を担保し、不正操作を抑止する効果をもたらします。

### Windows の操作ログを取得

● 操作ログの例

ファイルサーバーの「顧客リスト.xls」をデスクトップにコピー ▶ ファイル名を「商品案内.xls」に変更 ▶ ブラウザを立ち上げ Google Drive にアクセス ▶ 「商品案内.xls」を Google Drive にアップロード

23：32　23：36　23：37　23：40

### 取得できる操作ログ

操作ログ（Windows）

| | ログの種類 | 取得内容 |
|---|---|---|
| Windows | ログオン・ログオフログ | 電源 ON・OFF・ログオン・ログオフのログを取得できます。 |
| | ウィンドウタイトルログ | デバイス上での閲覧画面（ウィンドウタイトル・アプリ名）のログを取得できます。 |
| | ファイル操作ログ | デバイス上でのファイル操作（ファイル・フォルダのコピー／移動／作成／上書き／削除／名前の変更）でのログを取得できます。 |
| | Webアクセスログ※ | Web サイトの閲覧、Web メールやクラウドストレージのアップロード／ダウンロードログを取得できます。 |
| | プリントログ | 印刷状況を記録し、ドキュメントやプリンター、PC ごとに印刷枚数を集計できます。 |
| | 通信機器接続ログ | Wi-Fi ／ Bluetooth ／有線の接続を把握し、管理外の接続を検知できます。 |
| | アプリ稼働ログ | アプリの稼働情報を取得できます。 |
| | アプリ通信ログ | 通信元／先の IP アドレスやポート番号、アプリのハッシュ値を取得できます。 |

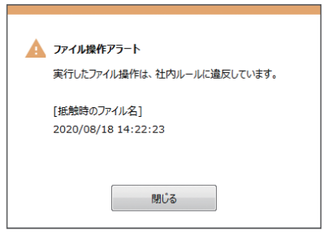
※ 対応ブラウザは、Chrome、Firefox、Internet Explorer、Microsoft Edge です。

### 業務外操作をアラートで検知

操作ログ（Windows）

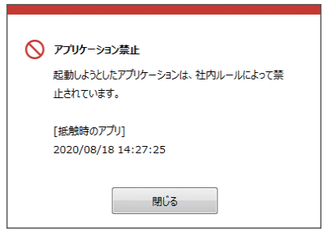
セキュリティリスクのある操作など設定したポリシーに違反した場合、利用者にリアルタイムにポップアップで警告。違反操作をしたことを利用者に警告し、セキュリティモラルの向上を促します。

| 種別 | アラートの内容 |
|---|---|
| ウィンドウタイトル | ウィンドウタイトルに特定のキーワードが含まれる操作 |
| ファイル操作 | ドライブの追加 |
| | USB メモリなど外部メディアへの書き込み |
| | ローカル共有フォルダーの作成または書き込み |
| | Outlook メールへのファイル添付 |
| | 機密フォルダーとして指定したフォルダー内での操作 |
| | CSV ファイルへの出力 |
| | ネットワーク上の共有フォルダーへの書き込み |
| プリント | 印刷枚数の超過 |
| | ドキュメント名に特定のキーワードが含まれる印刷 |
| Web アクセス | 特定のキーワード／ URL が含まれる Web 閲覧 |
| | アップロード／ダウンロード |
| | Web メールの送信 |
| 通信機器接続 | 不許可通信デバイスの接続 |




**操作アラート**

ポップアップで表示できる内容は自社の運用に合うよう編集できます。左の表のアラートに対応しています。



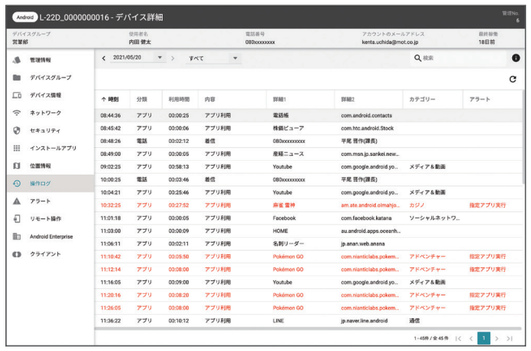

**アプリ禁止**

業務に不要なアプリの利用や Web アクセスを禁止できます。特定の時間帯だけ許可する設定も可能です。

### スマホ・タブレットの活用状況を見える化

操作ログ（iOS・Android）

導入した目的に沿ってスマホ・タブレットが活用されているかの判断や分析のための情報として活用できます。




● 取得可能な操作ログ

| ログの種類 | 取得内容 | iOS / iPadOS | Android |
|---|---|---|---|
| デバイス利用ログ | 日時、利用時間 | ○ | ○ |
| 電話利用ログ | 日時、通話時間、種類（着信・発信・不在着信） | ○ | ○ |
| アプリ利用ログ | 日時、利用時間、アプリ名、パッケージ名 | ― | ○ |
| 新規アプリインストールログ | 日時、アプリ名、パッケージ名 | ― | ○ |
| アプリアンインストールログ | 日時、パッケージ名 | ― | ○ |
| 外部メディア取り外しログ | 日時、メディア名 | ― | ○ |
| 外部メディア認識ログ | 日時、メディア名 | ― | ○ |
| タイムゾーン変更ログ | 日時、変更後のタイムゾーン | ― | ○ |
| デバイス管理者設定 | 日時、デバイス管理者設定成功情報 | ― | ○ |
| 使用履歴へのアクセス設定ログ | 日時、使用履歴へのアクセス設定登録情報 | ― | ○ |

※ iOS/iPadOS の操作ログ取得は条件があります。詳細はお問い合わせください。

## User's voice

テレワークのスムーズな導入に
LANSCOPE クラウド版が活躍！

テレワークを推進していく中で、PC 操作ログの取得・可視化は必須でした。LANSCOPE クラウド版はすぐに導入でき、スムーズなテレワーク体制を築くことができました。従業員にも利用状況を見える化していることを伝え、メリハリを持って仕事をするよう全社で共有しています。

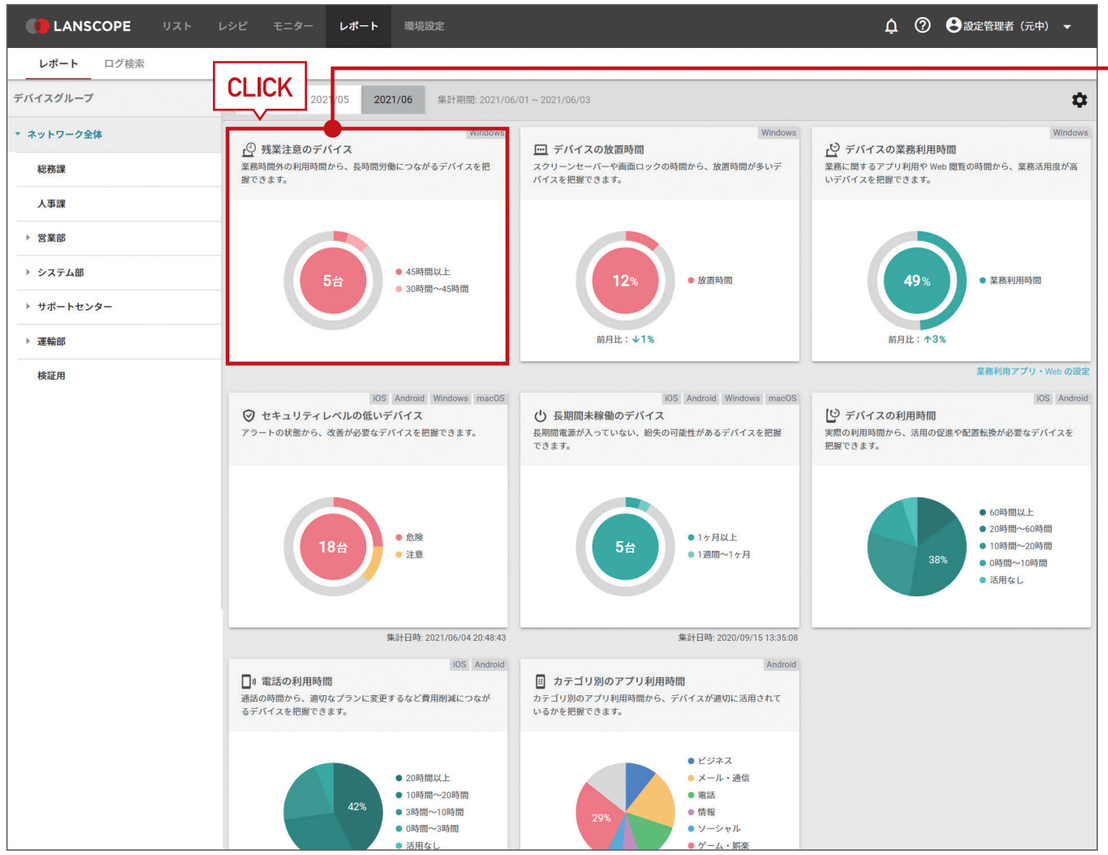
# レポート

iOS / iPadOS　Android　Windows　macOS

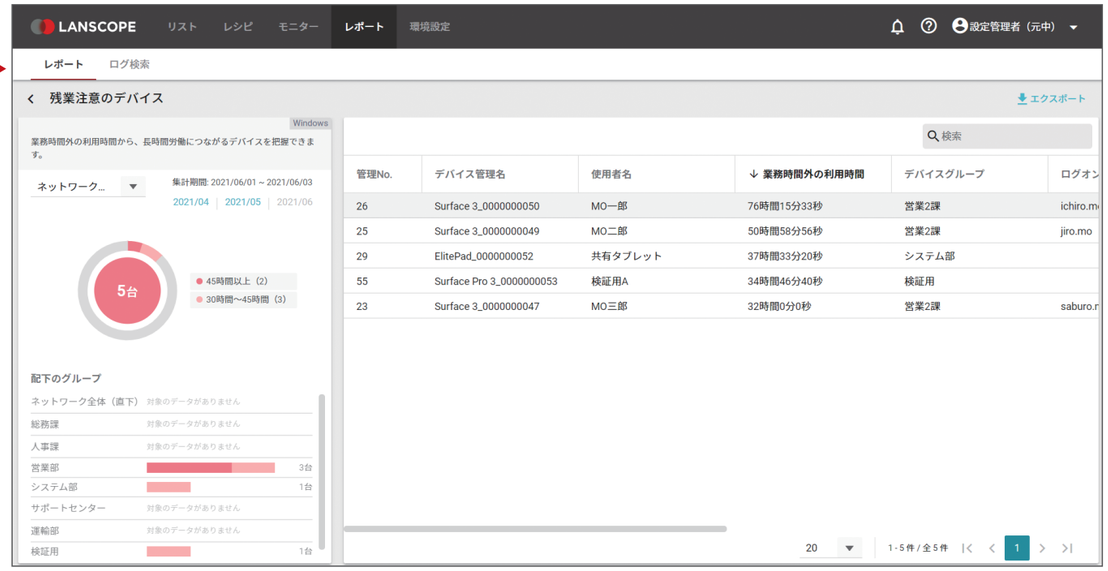
## 豊富なレポートで、デバイスの活用状況を「見える化」します。

取得した操作ログや資産情報のデータからレポートを自動作成し、
デバイスやアプリ、電話が本来の目的に沿って活用できているか、組織全体またはグループ単位で把握できます。

### デバイスの活用状況やルール違反の状況をレポート




### ドリルダウンで、配下の「グループ比較」や「課題のあるデバイス」を特定




トップ画面のレポートをクリックして、グループ別の比較やデバイスのランキングを確認できます。
該当デバイスをクリックすれば、デバイスの詳細や Windows の場合は個人レポートを確認できます。

#### ● 残業注意のデバイス

業務時間外の利用時間から、長時間労働につながるデバイスを把握できます。

#### ● デバイスの放置時間

スクリーンセーバーや画面ロックの時間から、放置時間が多いデバイスを把握できます。

#### ● デバイスの業務利用時間

業務に関するアプリ利用や Web 閲覧の時間から、業務活用度が高いデバイスを把握できます。

#### ● セキュリティレベルの低いデバイス

アラートの状態から、改善が必要なデバイスを把握できます。

#### ● 長期間未稼働のデバイス

長期間電源が入っていないなど、紛失の可能性があるデバイスを把握できます。

#### ● デバイスの利用時間

実際の利用時間から、活用の促進や配置転換が必要なデバイスを把握できます。

#### ● 電話の利用時間

通話の時間から、適切なプランに変更するなど費用削減につながるデバイスを把握できます。

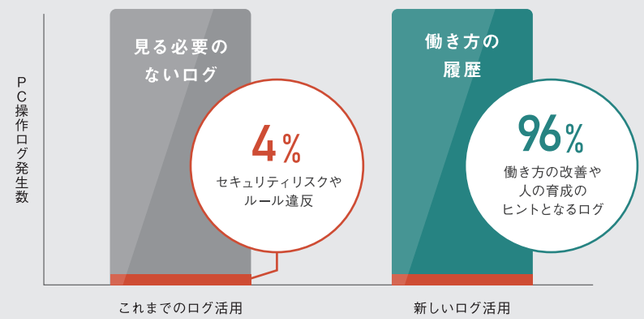
#### ● カテゴリ別のアプリ利用時間

アプリの利用時間から、よく利用されているアプリのカテゴリを把握できます。

PICK UP

### 操作ログをセキュリティだけでなく、業務効率化・マネジメントに活用

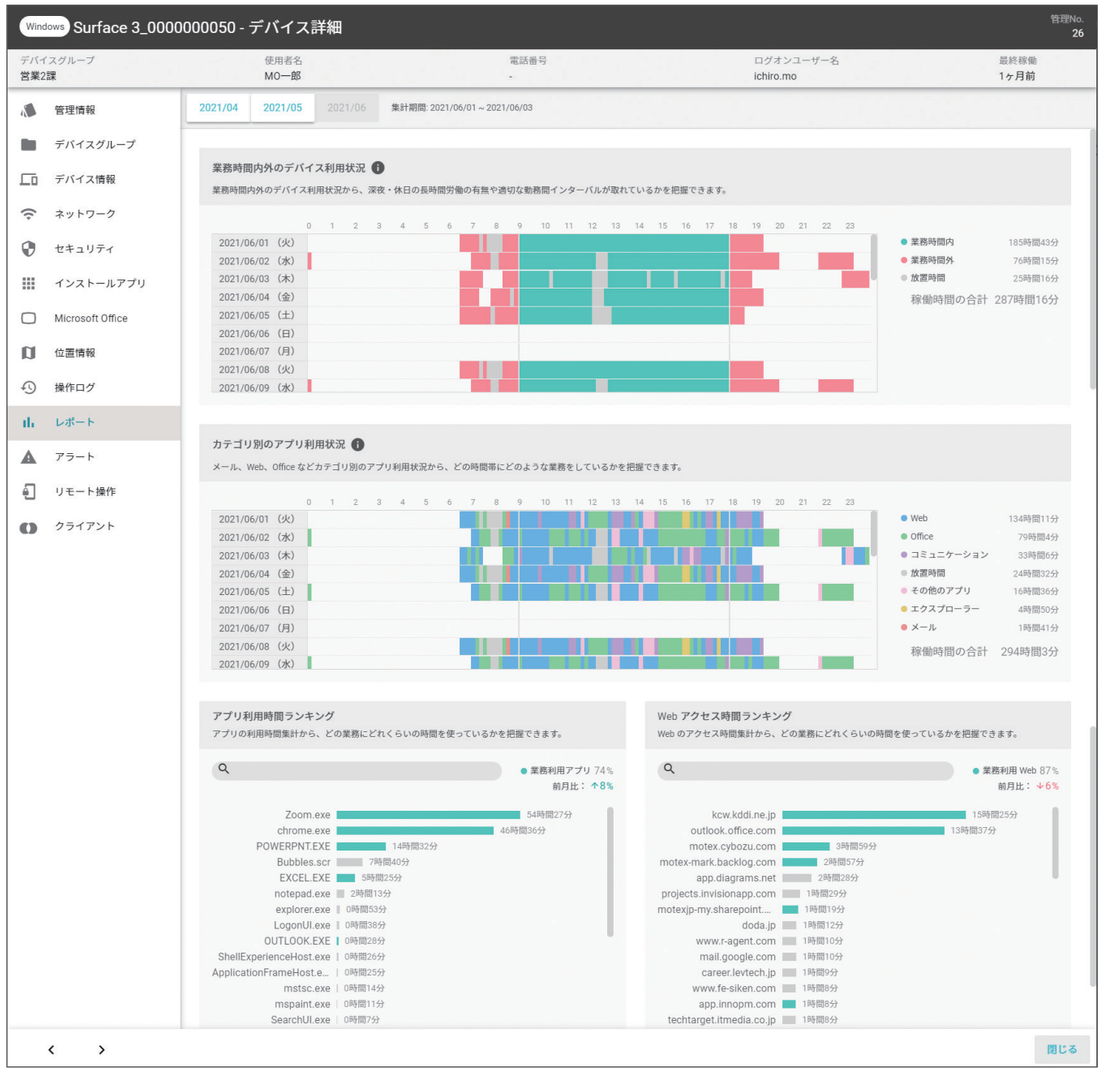
PC 1台あたり1日で1,000件以上の操作ログが発生します。そのうち、セキュリティリスクのある操作やルール違反は全体の4%以下です。一方で今まで見ていなかった 96% のログを「働き方の履歴」として活用する組織が増えています。
これからは、テレワークなど働き方が多様化する中で、PC の操作ログから現状の働き方を正しく把握し、業務効率化やマネジメントに活用できる仕組みが求められています。



# PC の操作ログから、一人ひとりの働き方を「見せる化」します。

現場のマネージャーや従業員に取得した操作ログのレポートを共有し、
働き方についてコミュニケーションを取ることで業務の効率化や人材育成に活用できます。

## 個人ごとに「勤務状況」や「何に時間を使っているか」を分析




## 業務時間内外の利用状況

業務時間内外の利用状況から、適切な勤務間インターバルが取れているかや、休日・深夜の長時間労働が無いかを把握できます。

## アプリ別の利用状況

メール、Web、Office などカテゴリ毎のアプリ利用状況から、どの時間帯にどのような業務をしているかを把握できます。

## アプリ利用時間ランキング

よく利用されているアプリや業務に関するアプリの利用時間ランキングから、どの業務にどれくらいの時間を使っているかを把握できます。

## Web アクセス時間ランキング

よくアクセスされている Web や業務に関する Web の利用時間ランキングから、どの業務にどれくらいの時間を使っているかを把握できます。

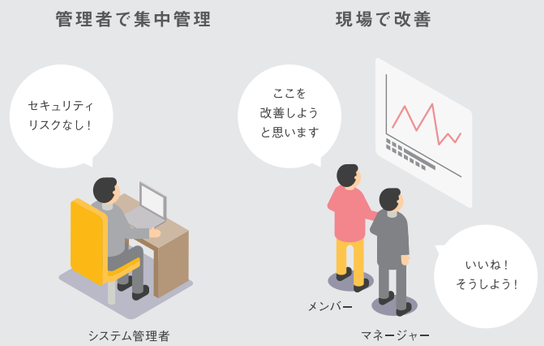
| カテゴリ | 集計対象のアプリ |
|---|---|
| メール | Outlook.exe / thunderbird.exe |
| Web | chrome.exe / firefox.exe / iexplore.exe MicrosoftEdge.exe / Msegde.exe |
| Office | EXCEL.exe / MSACCESS.exe / MSPUB.exe ONENOTEX.exe / POWEPNT.exe / WINWORD.exe |
| コミュニケーション | atmgr.exe / Chatwork.exe / direct.exe / slack.exe / Teams.exe / WMOne.exe / Zoom.exe |
| エクスプローラー | explorer.exe |
| 放置時間 | スクリーンセーバーや画面ロック中に起動されるアプリ |
| その他のアプリ | 上記に該当しないアプリ |

業務で利用しているアプリや Web を設定できます。設定したアプリの利用や Web のアクセスは「業務に関する利用」として表示されます。

PICK UP

## 管理者への「見える化」だけでなく、マネージャー・現場に共有する「見せる化」がポイント

これまでは、取得した操作ログを、管理者・経営者層に「見える化」し、現状把握・セキュリティなど監査を目的としていました。
働き方が多様化するこれからは、現場のマネージャーや従業員に取得した操作ログのレポートを共有して、業務の効率化や人材育成に活用することが求められます。
LANSCOPE クラウド版ではシステムやセキュリティに詳しくない方にも分かりやすいレポートで働き方の「見せる化」を実現。また営業部のマネージャーには営業部のメンバーのレポートだけを確認できるなど管理コンソールの権限分散機能を搭載、現場に即した運用が可能です。

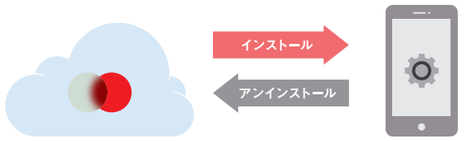


# DEP・VPPの利用で、より幅広いiOS / iPadOSデバイス管理を実現します。

Apple社が提供するDEPやVPPを利用することで、MDM構成プロファイルの削除禁止、アプリのサイレントインストールなど、iOS / iPadOSデバイス管理の課題を解決できます。

## 構成プロファイル管理

構成プロファイルを作成し、デバイスに一括適用できます。App Storeやカメラ、Safariなどの利用制限、Wi-FiやVPNなどの各種設定の効率化を実現します。インストールした構成プロファイルをアンインストールすることもできるため、遠隔で柔軟に設定変更が可能です。




## 構成プロファイルの作成※

iOS / iPadOSのデバイスを制限する「制限」プロファイル、Webサイトのショートカットをデバイスのホーム画面に配置する「Webクリップ」の作成、Wi-Fi・VPNの設定プロファイルを作成できます。

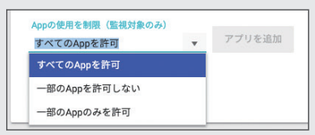
※ LANSCOPE クラウド版とApple Configurator2で作成できるプロファイルに違いがあります。

PICK UP

### アプリの個別制御も可能！より幅広い管理を実現！

例えば、iOS / iPadOS純正のメールアプリの利用を禁止したい、App Storeでインストールできるメールアプリを禁止したいなど、アプリを指定して禁止できます※。
また指定したアプリ以外を利用させないホワイトリスト形式での運用も可能です。

※ デバイスを監視モードに設定する必要があります。




## 自動デバイス登録（DEP）

Apple Business Manager

デバイスを自動的にMDMの管理下に配置でき、デバイス登録に必要な工数を削減できます。また監視モードを自動適用し、MDM構成プロファイルの削除を禁止するなど、より幅広い管理を実現できます。

● 監視モードの主なメリット

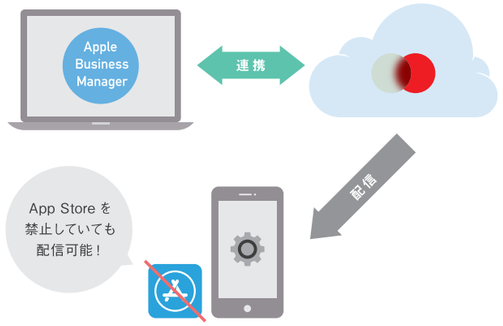
| | |
|---|---|
| 構成プロファイルの配信 | アプリの削除を禁止する、壁紙の変更を禁止するなど、監視モード専用の構成プロファイルをデバイスに配信できます。 |
| アプリのサイレントインストール | 自社開発アプリやVPPアプリのサイレントインストールが可能です。 |
| 紛失モードの利用 | ロック画面の解除不可、メッセージの表示、位置情報の強制取得などを実現する紛失モードを利用できます。 |

## アプリの一括配信（VPP）

Apple Business Manager

Apple Business Manager上で一括入手したアプリを、LANSCOPE クラウド版に連携しデバイスに配信できます。
Apple IDが設定されていない、App Storeの利用を禁止しているデバイスに対してもインストール・アップデート配信が可能なため、効率的なアプリ配信が可能です。

※ App Storeを禁止するためにはデバイスを監視モードに設定する必要があります。




PICK UP

### アプリカタログ機能

デバイス利用者が任意のタイミングで、アプリをインストール

管理者が設定したアプリを、デバイス利用者が選択し、任意のタイミングでインストールできます。もちろん、Apple IDを設定していない・App Storeを禁止しているデバイスでも、インストールが可能です！

## User's voice

**VPPを利用して、業務に必要なアプリのみを一括配信！店舗に備え付けのiPad1,500台を2人で一元管理。**

構成プロファイルを利用して、店舗用デバイスでApp Storeを禁止するなど機能を制限しています。またVPPを利用して、業務に必要なアプリのみを一括配信しています。本部の担当者2人だけで、1,500台のiPadを管理できており、とても助かっています。

# Android Enterprise 対応

Android

## アプリ配信や利用制御など幅広い管理を実現します。

Google社が提供するAndroid Enterpriseを利用することで、管理者が指定したGoogle Playストアアプリのみを利用させたり、デバイスの利用を制御できます。

### デバイスの利用制御

Android Enterprise を利用することで、カメラや外部メディアの利用など、デバイスの利用制御を行うことができます。
また LANSCOPE Client（管理用アプリ）のアンインストールを防止できます。

| | | |
|---|---|---|
| セキュリティ | パスワードポリシー | 桁数や有効期限など設定するパスワードのルールを設定できます。 |
| | 物理的な外部メディアの利用禁止 | SD カードなど物理的な外部メディアの利用を禁止できます。 |
| | USB 経由でのデータ転送禁止 | ストレージとしての接続やデータ転送を禁止できます。 |
| | NFC によるデータ転送禁止 | NFC によるデータの転送を禁止できます。 |
| | Bluetooth 機器の接続禁止 | Bluetooth 機器の接続を禁止できます。 |
| | SMS による通信の禁止 | SMS によるメッセージの作成と受信を禁止できます。 |
| | テザリングの禁止 | テザリングの利用を禁止できます。 |
| デバイス | デバイスの初期化禁止 | デバイスの初期化を禁止できます |
| | 日付・時刻の変更禁止 | 日付や時刻の変更を禁止できます。 |
| | デバッグ機能・セーフブートの利用禁止 | デバッグ機能・セーフブートの利用を禁止できます。 |
| | 位置情報設定の有効化 | ポリシー適用時に位置情報モードを有効にできます。 |
| | 充電中のスリープモードの無効化 | 充電中に画面がスリープ状態にならないように設定できます。 |
| | カメラの利用禁止 | カメラの利用を禁止できます。 |
| | スクリーンショットの取得禁止 | スクリーンショットの取得を禁止できます。 |
| | マルチユーザーの利用禁止 | ユーザーアカウントの複数作成や切り替えを禁止できます。 |
| | アカウント管理の変更禁止 | Google アカウントの追加などアカウントの変更を禁止できます。 |
| ネットワーク | ネットワークの選択禁止 | Wi-Fi ネットワークの選択を禁止できます。 |
| | Wi-Fi 設定 | Wi-Fi の SSID やパスワードなどをデバイスに設定できます。 |
| OS制御 | OS アップデートの制御 | 指定した時間でアップデートしたり、30日間アップデートを禁止するなど、OS アップデートの制御ができます。 |
| キオスクモード | キオスクモードの設定 | 指定したアプリ以外利用できないようにするなどデバイスの利用を制限できます。 |
| | 電源ボタンメニューの表示禁止 | 電源ボタンのメニューの表示を禁止できます。 |
| | システムエラーダイアログの表示禁止 | システムエラーのダイアログの表示を禁止できます。 |
| | ホーム / タスクボタンの表示禁止 | ホームボタン、タスクボタンの表示を禁止できます。 |
| | ステータスバーの表示禁止 | ステータスバーの表示を禁止できます。 |
| | 設定アプリの起動禁止 | 設定アプリが起動できるアプリの場合、起動を禁止できます。 |

### アプリ管理機能

利用できるアプリを指定するホワイトリスト形式、利用を禁止するアプリを指定するブラックリスト形式でアプリを管理できます。指定したアプリのみをGoogle Playストアから利用者が手動でインストールすることはもちろん、管理者がLANSCOPEクラウド版からデバイスに配信することもできます。

管理コンソールから管理したいアプリを検索・選択するだけで、
管理アプリとして設定できます。

### アプリ管理の運用

#### 01 管理者が許可したアプリのみ利用できる（ホワイトリスト）

LANSCOPE クラウド版の管理コンソールで許可設定したアプリのみ Google Play ストアに表示、デバイス利用者が利用するアプリをインストールします。アプリの表示だけではなく、LANSCOPE クラウド版からデバイスにインストールを実行することも可能です。

**手動インストール**

管理者が許可したアプリを、利用者がGoogle Playストアから自由にインストールできます。ストアには許可したアプリのみ表示されます。

**強制インストール**

管理者が指定したアプリが、デバイスにインストールされます。また、アプリのアンインストールを禁止することもできます。

#### 02 Playストアを開放し、アプリを個別に禁止する（ブラックリスト）

デバイス利用者は Google Play ストアから必要なアプリを自由にインストールできます。利用させたくないアプリは、非表示にしインストールを禁止することも可能です。また業務に必要なアプリを LANSCOPE クラウド版から強制インストールできます。

PICK UP

**資産情報・操作ログから活用状況を把握！**

LANSCOPE クラウド版はインストールアプリの情報を確認できるだけでなく、「誰が」「いつ」「どのようなアプリを」利用したか把握できます。
貸与したスマホ・タブレットを充分に活用して欲しい一方で、過度な業務外利用は生産性を落としてしまうので困る… 操作ログは利用状況を見える化し、業務外利用の抑止効果を期待できます。

**User's voice**

Android Enterpriseを利用して
業務に必要なアプリのみを許可。
セキュリティと利便性を両立！

業務に必要なアプリをホワイトリストに登録して、Google Playストアから利用者が必要なアプリのみをインストールできる運用を行っています。アプリの登録は管理コンソールから検索して選択するだけ。分かりやすい 操作で設定の手間もかかりませんでした。

# 製品連携

## 業務効率化からセキュリティまで、組織の課題を解決します。

LANSCOPE クラウド版 は様々なサービスと連携。バックオフィス業務の効率化やセキュリティなど、管理ツール単体では対応が難しい課題を、製品連携によって解決できます。

### SYNCPIT（エムオーテックス）
バックオフィス業務の自動化

ビジネスチャットで利用しているアカウント情報と LANSCOPE の管理下にあるデバイスを連携します。ビジネスチャット上で、操作ログや位置情報を確認した上で、リモートロックやワイプを利用者本人または管理者が実行できます。

### BlackBerry Protect（BlackBerry）
AI アンチウイルス

Cyber Protection Managed Service powered by BlackBerry と連携することで、マルウェアの感染原因となるユーザーの操作を、LANSCOPE で取得した操作ログから簡単に特定できます。

### Garoon（サイボウズ）
グループウェア

LANSCOPE で取得している操作ログを元に、各日の最初と最後の操作実施時刻を Garoon のスケジュールに表示できます。デバイスの利用時間帯とスケジュールの登録内容を比較することで勤務状況の見える化につながります。

### L2Blocker（ソフトクリエイト）
不正 PC 検知・遮断

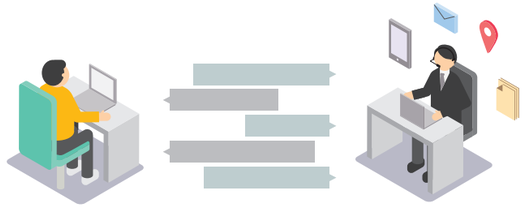
LANSCOPE で管理されていない機器を検知し自動遮断を行います。
管理外の持込機器の利用やシャドー IT を防止することで、セキュリティリスクを排除したネットワークを構築できます。
オンプレミス、クラウドどちらをご選択頂いても連携可能です。
（※実装予定の機能です。）



## 継続利用率90%以上！
## 充実のサポート体制でお客様を支援

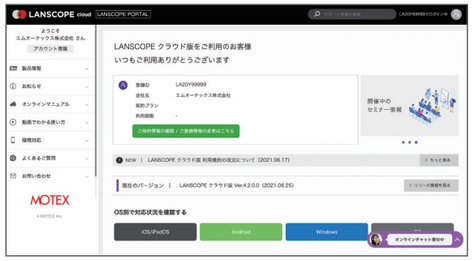
### ヘルプデスクサービス

LANSCOPE クラウド版の操作方法・不明点やトラブル・運用などに関するご質問に専門スタッフがメールや電話で無償対応します。IT資産管理・セキュリティのトップメーカーとして培われた様々なノウハウを活かし、お客様によりご満足いただけるサービスをご提供します。



### ユーザー様専用サイト「LANSCOPE PORTAL」

LANSCOPE PORTALは、LANSCOPE クラウド版をご利用いただいているお客様の専用サイトです。ご契約情報の確認や利用ガイド、よくあるご質問や MOTEXからの最新情報をご確認いただけます。




## ご検討中のお客様向けコンテンツ

## オンライン商談受付中！

**こんな方におススメ!!**
- 実際の画面を見てみたいけど検証まではちょっと…
- デモを見たいけどあまり時間がない…
- なかなかセミナーに参加できない…

**オンライン商談とは …**

お客様に自席で管理コンソールやご提案資料をご覧いただきながら、専任スタッフが製品をご紹介！
搭載機能はもちろん、どのように管理／活用できるのかをご理解いただけます。
「実際に操作しながら教えてもらえるので、わかりやすい！」とご好評いただいています。ぜひご検討ください。

**資料ダウンロード**

導入時にご検討いただく際の各種資料をダウンロードいただけます。

**60日間無料体験**

LANSCOPE クラウド版を今すぐお試しいただける、60日間無料体験をご用意しています。

**簡単お見積**

LANSCOPE クラウド版の価格を簡単にご確認いただけます。

https://www.lanscope.jp/an/ LANSCOPE cloud 検索