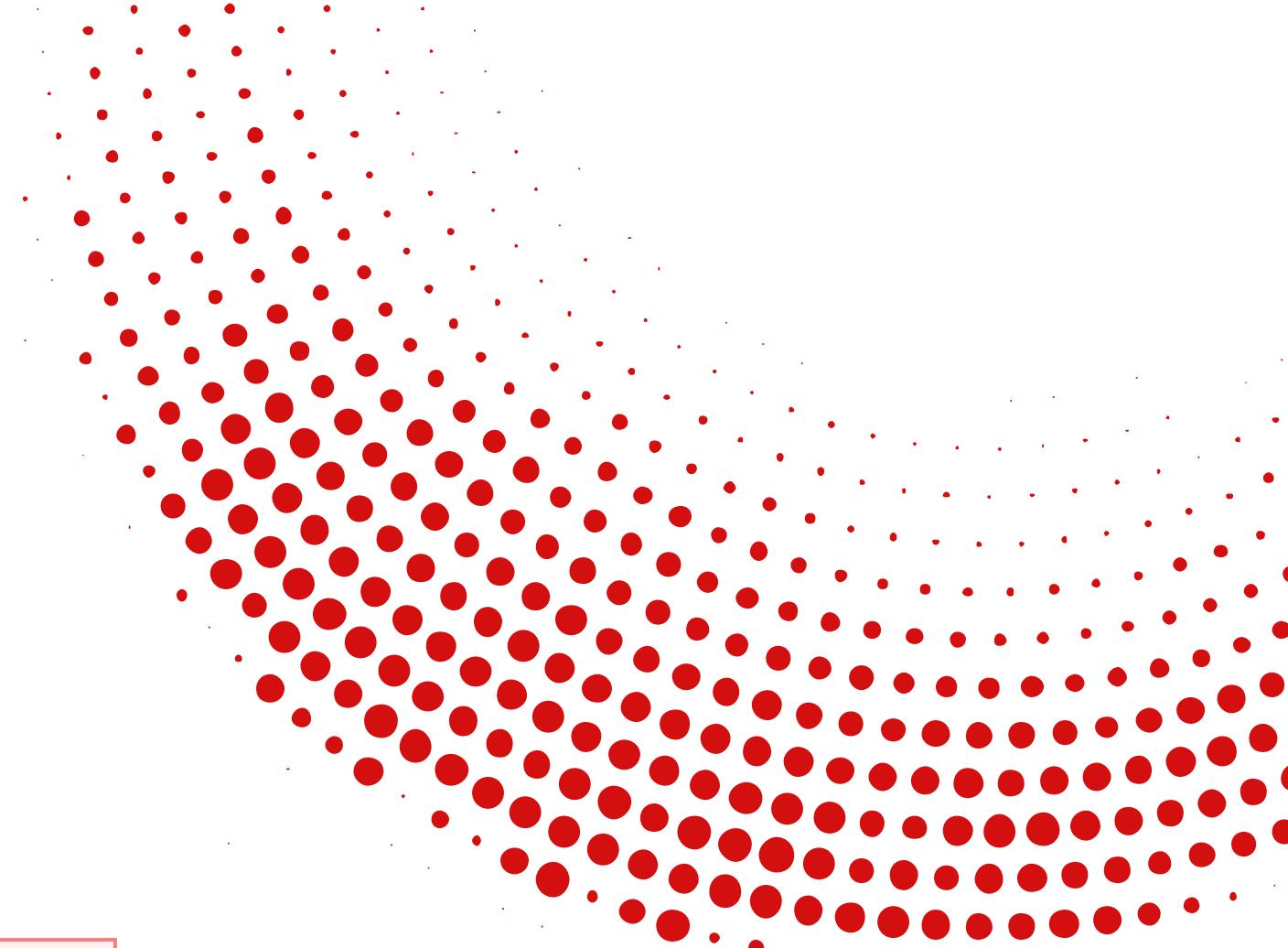




エンドポイントマネージャー クラウド版 ご提案資料

PC・スマホをクラウドで一元管理！IT 資産管理・MDM ツールのご紹介



2024年3月

エムオーテックス株式会社 プロダクトマーケティング部

1. エンドポイントマネージャー クラウド版 の特長
2. 機能一覧・価格体系・サポート体制
3. エンドポイントマネージャー クラウド版 各機能のご紹介

機能紹介① 資産管理（ハードウェア・アプリ管理）

機能紹介② 紛失対策・セキュリティ

機能紹介③ Windows・macOS 操作ログ管理

機能紹介④ Apple Business Manager／Android Enterprise

機能紹介⑤ 関連製品

※資料右上に記載しているアイコンは対応 OS、対応ライセンスを示しています。

i … iOS/iPadOS A … Android W … Windows m … macOS



この場合、**iOS・Android・Windows** に対応している機能であることを示し、利用するためには **ライトA** または**ベーシック**のライセンスが必要です。
尚、**iOS・Android**においてはオプション機能を除き **ライトA** ライセンスで**すべての機能**を利用できるため、**ベーシック**の導入は不要です。

会社概要

会 社 名 エムオーテックス株式会社

代表取締役社長 宮崎 吉郎

設 立 1990年7月

従 業 員 数 466名（2024年4月現在）

株 主 京セラコミュニケーションシステム株式会社
(2012年から資本参加)

事 業 内 容 自社製品の開発・販売、サイバーセキュリティの
コンサルティング・ソリューション導入・運用監
視サービス

拠点

本 社 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

東 京 本 部 東京都港区三田3-5-19
住友不動産東京三田ガーデンタワー22F

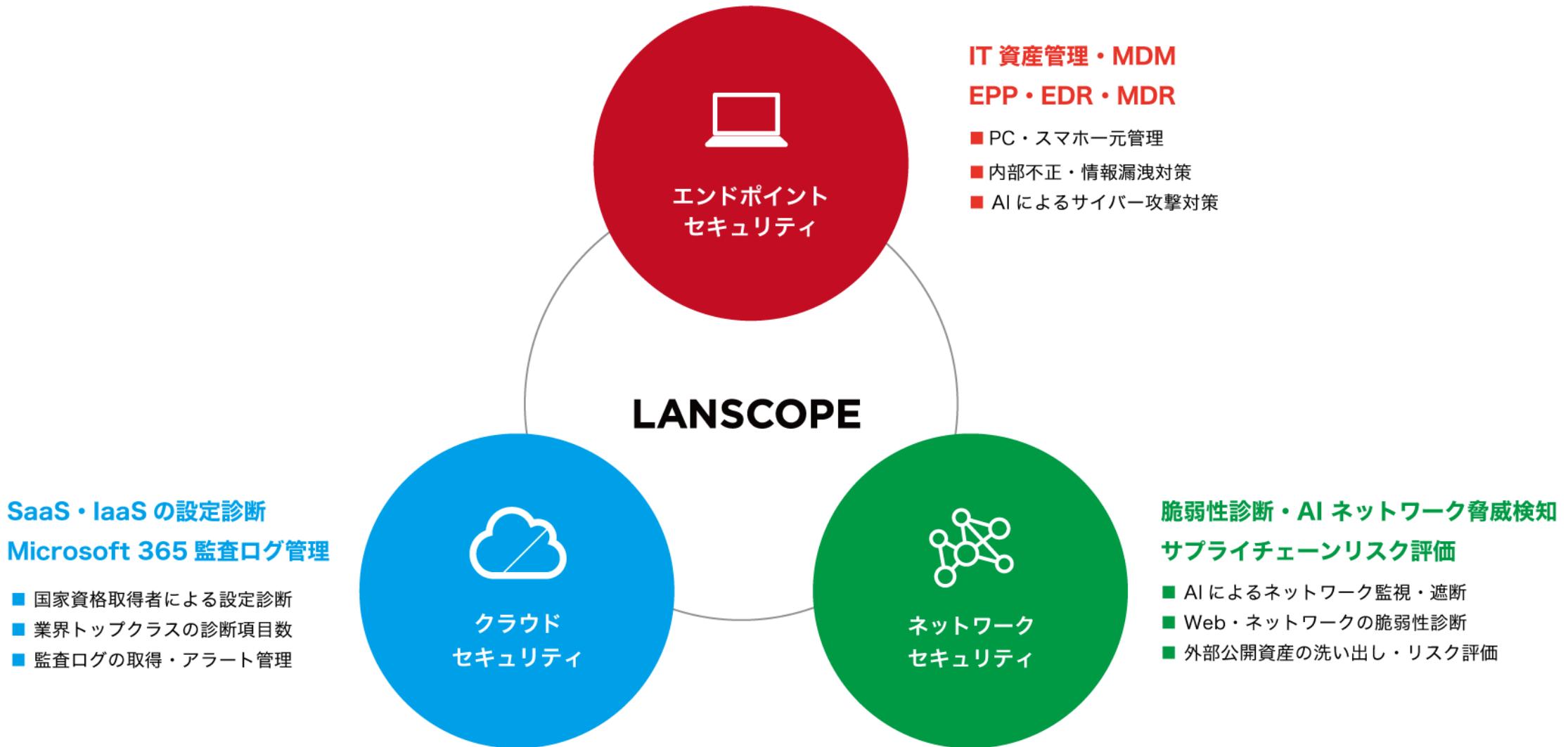
名 古 屋 支 店 名古屋市中区錦1-11-11
名古屋インターナショナル3F

九 州 営 業 所 福岡市博多区博多駅前1-15-20
NMF博多駅前ビル2F

長 崎 Innovation Lab 長崎県長崎市出島町1-41
クレインハーバー長崎ビル3F



エムオーテックス株式会社（MOTEX）は、
大阪・関西万博の運営参加サプライヤー
(LANSCOPE エンドポイントマネージャー クラウド版) です。



「LANSCOPE」を通して、お客様の“Secure Productivity”の実現を支援

エンドポイントセキュリティ

統合エンドポイント 管理



Endpoint Manager

組織の IT 資産管理・内部不正対策・外部脅威対策をオールインワンで対応

IT 資産管理・MDM

内部情報漏洩対策

外部脅威対策

AI アンチウイルス



Cyber Protection

AI を活用したアンチウイルスで未知・亜種の脅威を検知・対処・復旧が可能

EPP

EDR

MDR

リモート コントロール



Remote Desktop

遠隔地のサーバーや PC、スマホへのリモート操作、画面共有などヘルプデスク業務を効率化

リモートアクセス

ヘルプデスク効率化

Microsoft 365 セキュリティ



Security Auditor

Microsoft 365の監査ログを取得。利用状況の見える化やアラート管理が可能

監査ログ管理

アラート管理

セキュリティ 診断



Professional Service

高い技術力を誇るセキュリティエンジニアがWeb・ネットワーク・クラウドの脆弱性を診断

Web 診断

ネットワーク診断

クラウド診断

ネットワークセキュリティ

AI ネットワーク 脅威検知



AI を活用しネットワークを監視、サイバー攻撃や内部不正の兆候を検知・遮断

NDR

ネットワーク遮断

Email 監視

サプライチェーン リスクマネジメント



ドメイン情報やオンライン調査票からサプライチェーンリスクを可視化

セキュリティスコアリング

ASM

お客様のニーズに応じて、クラウド・オンプレミス版のエンドポイントマネージャーをご用意。



クラウド版

こんな方におすすめ

- ✓ サーバーの管理やバージョンアップに運用コストをかけたくない
- ✓ PC だけでなく、スマホ・タブレットもまとめて管理したい
- ✓ 社内 LAN に接続されないテレワークデバイスもリアルタイムに管理したい



オンプレミス版

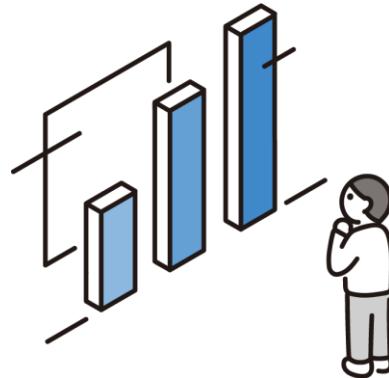
こんな方におすすめ

- ✓ サーバーの管理は自社で行いたい
- ✓ Azure や AWS など保有している IaaS 基盤で利用したい
- ✓ インターネットに接続されないデバイスもまとめて管理したい

1. エンドポイントマネージャー クラウド版の特長

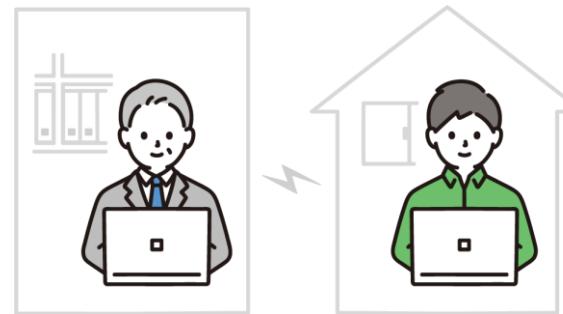
クラウドサービスならではの特長を活かしてデバイス管理の課題解決を支援！

IT 資産管理ツールを クラウド化したい



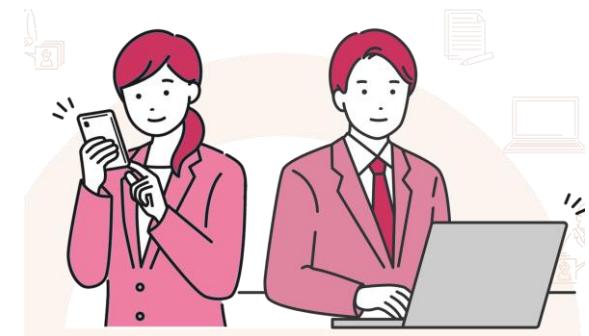
社内のシステムや業務用ソフトのクラウド化を進めており、IT 資産管理ツールもクラウドに移行したい。

所在を問わない デバイス管理を実現したい



出社・在宅・レンタルオフィスなど働く場所の多様化が進んでいる中でも、リアルタイムにデバイスを管理したい。

PC・スマホを クラウドで一元管理したい



管理の効率化のために、PC だけでなく、スマートフォンやタブレットも同じツール・同じ管理コンソールで管理したい。

PC・スマホ・タブレットの一元管理をクラウドで実現

「使いやすい」管理コンソールで、充実の「IT 資産管理機能」と「MDM 機能」を実装

IT review 顧客評価No.1*

使いやすい管理コンソール

充実の PC 管理

操作ログ・セキュリティ

PC 管理に必要な機能を網羅

Apple・Google の認定プログラム対応

充実の「モバイル管理」



* IT 資産管理、ログ管理、MDM・EMM、統合運用管理の4部門でLeaderを獲得

充実の機能を使いやすい管理コンソールで提供
レビュープラットフォーム「ITreview」では既存のお客様から多くの評価

分かりやすく使いやすい

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形も用意されており、社員向けの手順書作成の手間も抑えられた。モバイルだけでなく、Windows PC も管理できることを考えると導入コストが非常に安い。

★★★★★

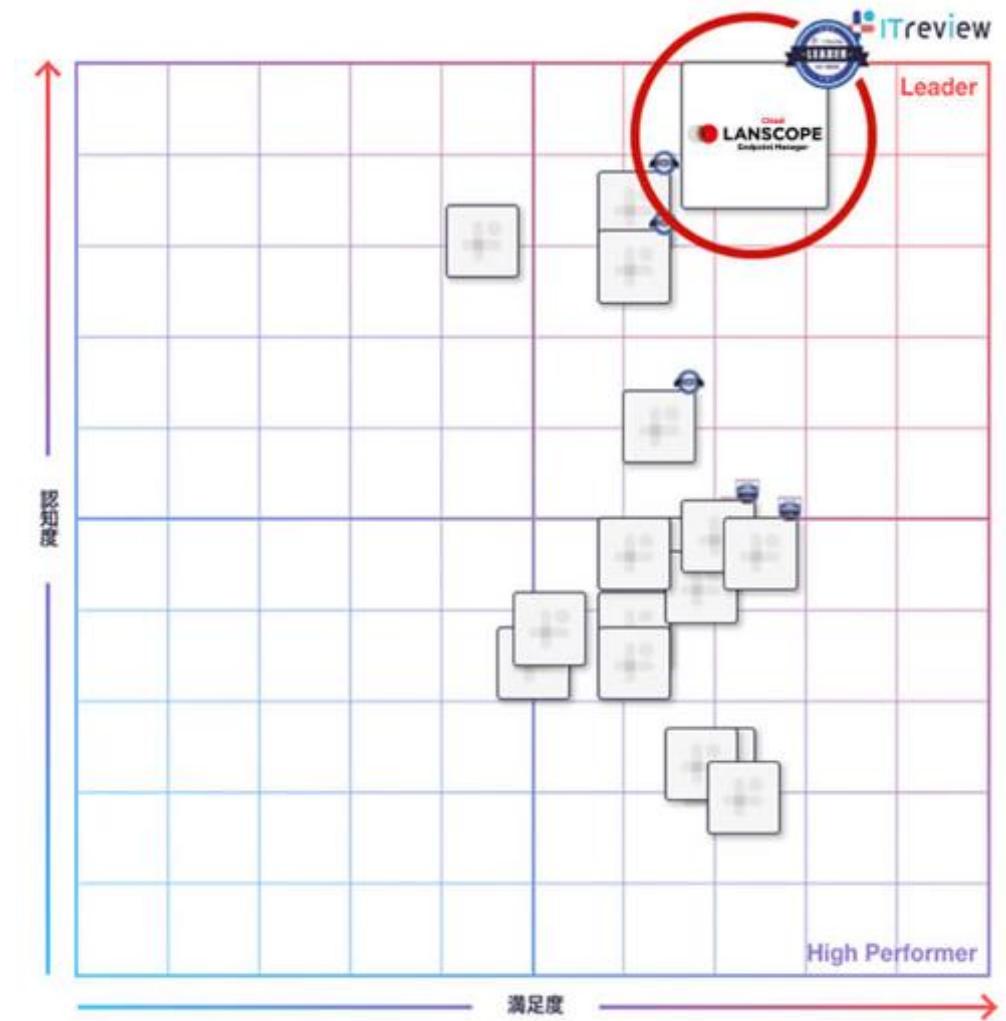
業種 製造業 従業員 300-1,000人未満

MDM の決定版！

スマートフォン用の MDM はこれまで何社か利用してきたが、価格 & 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、変な日本語もなく、管理画面がスッキリとまとまっているのも良い。

★★★★★

業種 総合卸売・商社・貿易 従業員 100-300人未満



3つの特長：操作ログ・セキュリティなど PC 管理に必要な機能を網羅した「充実の PC 管理」

Windows・macOS 管理に必要な機能を網羅

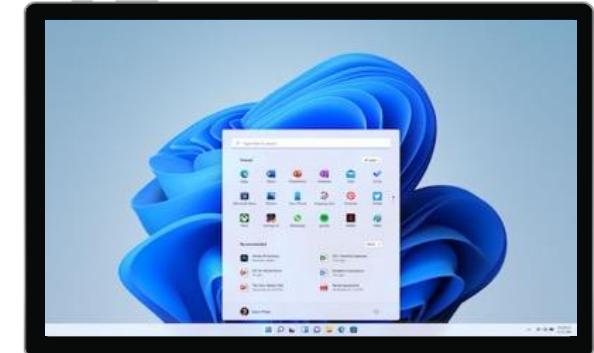
IT 資産管理ツールとしては欠かせない 操作ログ取得機能も実装

01 | 資産管理

Windows

macOS

デバイスのハードウェア情報／設定情報を自動取得し、IT 資産台帳として活用できます。自動取得できない項目は任意項目として管理できるほか、プリンターやルーターなどエージェントがインストールできない機器もまとめて管理できます。



02 | セキュリティ

Windows

macOS

OS によって必要なセキュリティ対策は異なります。Windows のアップデート管理や記録メディア制御、macOS のシステム利用制御、ドライブ・ディスク暗号化の運用に必要な機能をエンドポイントマネージャーで提供します。



03 | 操作ログ

Windows

macOS

内部情報漏洩対策として欠かせない PC の操作ログを自動取得します。取得したログは最大5年分の保存が可能です。また、働き方の見える化を実現するレポートを自動作成し、従業員のマネジメントにも活用できます。

3つの特長：Apple・Google の認定プログラム対応 充実の「モバイル管理」

充実の PC 管理に加えて、スマホ管理に欠かせない Apple Business Manager・Android Enterprise にも対応

01 | MDM としての基本機能

ios

Android

デバイス情報や位置情報の自動取得、リモートロック・ワイプなどスマホ・タブレットを管理するための基本的な機能を網羅しています。

02 | Apple Business Manager

ios

デバイスを効率的に エンドポイントマネージャーの管理下に置き（自動デバイス登録：DEP）、アプリの配信（VPP）やデバイスの利用制御などを実現できる Apple 社が提供するプログラムです。

03 | Android Enterprise

Android

Android Enterprise は、より高度なデバイス管理を実現できる Google 社が提供するプログラムです。Play ストアに表示するアプリを限定したり、アプリをデバイスに強制インストールが可能です。また初期化の禁止やアカウントの追加・変更の禁止など、デバイスの利用制御が可能です。



IT 資産管理ツール・MDM ツールの双方の機能を持つ
エンドポイントマネージャー クラウド版で PC・スマホを一元管理

機能	Cloud LANSCOPE Endpoint Manager	IT 資産管理ツール		MDM ツール	
		製品A（オンプレ）	製品B（クラウド）	製品C（クラウド）	製品D（クラウド）
PC 管理	OS 対応	i A W m	W m	i A W m	i A W m
	デバイス情報の取得	○	○	○	○
	ファイル・アプリ配信	○	○	○	○
	ソフトウェア・アプリの利用禁止	○	○	○	○
	ログオン・ログオフログ	○	○	○	×
	ウィンドウタイトル・ファイル操作・アプリ利用	○	○	○	×
	Web サイト閲覧（タイトル・URL）	○	○	○	×
	記録メディア制御	○	○	○	×
	Windows アップデート管理	○	○	○	×
	リモートロック・ワイプ	○	×	○	○
iOS	位置情報の取得	○	×	○	○
	Apple Business Manager 対応	○	×	×	○
Android	Android Enterprise 対応	○	×	×	○

クラウド版 の提供開始から10年以上、安心の実績でデバイス管理を支援します

サービス提供実績

導入実績 **10,000** 社

サービス提供 **10年** 以上

2012年よりサービス提供開始。
以来 10,000 社以上のお客様に導入。

市場シェアNo.1



クラウドサービスの
IT 資産管理ツール市場でシェア No.1

安心のサービス提供基盤



基盤に採用している AWS の認定、
クラウドサービスに関するガイドライン
規格の ISO27017 を取得。

IT 資産管理ツールのクラウド化や PC・スマホ一元管理により
多くのお客様が管理コストの削減・管理の効率化を実現されています。



オンプレミス型の IT 資産管理ツールから クラウド型の LANSCOPE に移行

サーバーメンテナンスを考えずに長期的・安定的にログが保存できること、機能の充実や使いやすさに加え、PC・スマホの一元管理が可能であることも、エンドポイントマネージャー導入の決め手になった。



管理コンソールの使い勝手や 機能面・コスト面の優位性が決め手に

機能面では、PC の操作ログ取得機能は欠かすことができない要件だった。この点で SaaS 製品で、操作ログまで取得できる製品は少なく、選定の早い段階からエンドポイントマネージャーに絞られていた。



OS のカバー領域の広さと コストパフォーマンスの高さが決め手

業務に応じて、複数の OS の端末を利用しています。エンドポイントマネージャー クラウド版は、Windows だけでなく、macOS や iOS・Android も、単一の管理コンソールで一元管理できることが決め手の一つとなった。

通信の安全性

インターネットサービスの中には、通信の途中で第三者に盗み見られたり、改ざんされる可能性があるものがあります。

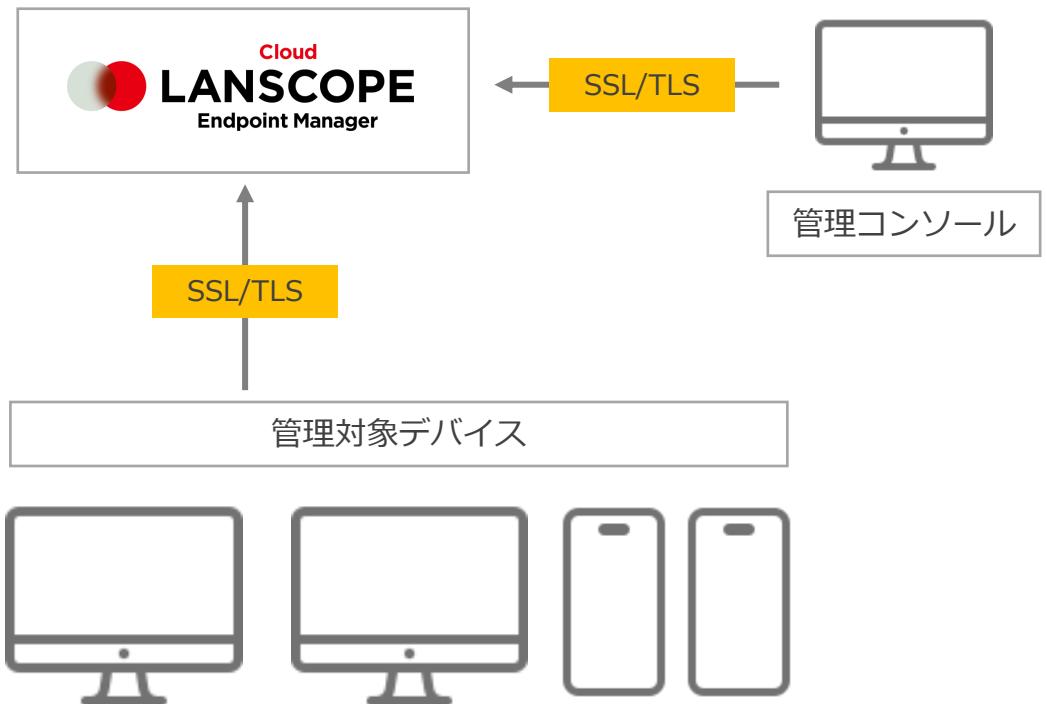
エンドポイントマネージャー クラウド版の通信では SSL/TLS を用いて暗号化しているため、第三者が内容を確認したり改ざんすることができません。

国際的なセキュリティ基準に則った運用体制

国際規格 ISO/IEC 27001 (ISMS) 認証、クラウドサービスの提供や利用に対して適用される国際規格 ISO 27017 認証を取得し、厳格なセキュリティ基準に則って、エンドポイントマネージャー クラウド版の運用を行っています。

高度なセキュリティと信頼性

- AWS サービスレディプログラムは、特定の AWS サービスと連携するパートナーが構築した製品を検証するプログラムで、健全なアーキテクチャと AWS のベストプラクティスへの準拠、市場での採用（お客様の成功を含む）について技術的に評価を受けます。MOTEX は「Amazon RDS サービスレディ」の認定を受けています。
- AWS ファンデーションアルテクニカルレビューでは、AWS Well-Architected Framework で定義されたセキュリティ、信頼性、運用上の優位性に関するベストプラクティスに沿っていることを評価されます。エンドポイントマネージャー クラウド版は、AWS FTR を通過しています。



管理コンソールの不正アクセス・不正操作を防止

安全にクラウドサービスをご利用いただけるよう、エンドポイントマネージャーは管理コンソールのセキュリティ機能を実装。管理コンソールのログイン画面に、許可されていない第三者のアクセスを防止する IP アドレス制限や2要素認証、パスワードポリシーの設定が可能です。また管理コンソール上の操作履歴を1年分保存します。



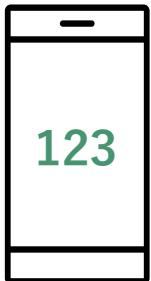
IP アドレス制限

IP アドレスによるアクセス制限を行い、社外 PC などからの不正なアクセスをブロックします。



パスワードポリシー

管理コンソールのパスワード強度・有効期間などポリシーを設定できます。



2要素認証

ログイン時に認証用のモバイルアプリで生成された確認コードの入力を要求できます。



操作履歴

管理コンソールのアカウントの画面閲覧や設定変更などを操作履歴として1年分保存し、閲覧・CSV 出力できます。

2. 機能一覧・価格体系・サポート体制

ライセンス体系

提供機能（ベーシック／ライトA／ライトB いずれか必須購入）	対象 OS				ライセンス体系		
	i	A	W	m	ライトA PC 資産管理・モバイル管理	ベーシック Win・Mac 全機能が利用可能	ライトB Win・Mac 操作ログを取得
デバイス情報の取得（ハード・ソフトウェア情報取得）	●	●	●	●	●	●	▲*1
アプリ / ファイル配信	●	●	●	●	●	●	—
ソフトウェア・アプリの利用禁止	●	●	●	—	●	●	—
メッセージ・アンケート	●	●	●	—	●	●	—
Windows アップデート管理	—	—	●	—	●	●	—
記録メディア制御	—	—	●	●	●	●	—
操作ログ（Windows・macOS）	—	—	●	●	—	●	●
操作ログ（iOS・Android）	●	●	—	—	●	— *3	—
リモートロック・ワイプ	●	●	●	●	●	●	●
位置情報の取得	●	●	●	—	●	●	—
Apple Business Manager・Android Enterprise	●	●	—	●	●*2	— *3	—

+オプションを選択

24/365 紛失サポート	●	●	●	●
VPP	●	—	—	—
外部脅威調査	—	—	●	—
ログ運用			●	●
Web フィルタリング	●	●	●	—
デバイス検査	—	—	●	—

*1 取得した操作ログの管理に必要なデバイス情報の管理（ログオンユーザー名、利用者名など）が可能です。

*2 VPP はオプション機能です。

*3 iOS・Android 向けの機能ため、ライトA ライセンスを購入してください。

機能一覧：ベーシック・ライトBはWindows・macOS管理専用ライセンスです。iOS・Android管理はライトAを契約してください。

必須購入			機能		対象OS			
ライトA	ベーシック	ライトB	機能名	概要	i	A	w	m
●	●	—	ハードウェア情報取得	電話番号やOSなど最大56項目を取得、任意項目も管理できます。	○	○	○	○
●	●	—	デバイス周辺機器管理	プリンター・ルーターなどエージェントをインストールできない機器を登録・管理できます。	○	○	○	○
●	●	—	ソフトウェア（アプリ）情報取得	インストールされているソフトウェア（アプリ）の情報を自動取得、確認できます。	○	○	○	○
●	●	—	アプリ / ファイル配信	ソフトウェアやbatファイル、アプリケーションをデバイスに配信できます。	○	○*1	○	○
●	—*2	—	Managed App Configuration	Managed App Configurationに対応したアプリの設定値を配布できます。	○	—	—	—
●	●	—	ソフトウェア（アプリ）の利用禁止	特定のアプリの利用を禁止できます。	○*3	○	○	×
●	●	—	メッセージ・アンケート機能	管理者からデバイスに対して、メッセージやアンケートを配信できます。	○	○	○	×
●	●	—	省電力設定	ディスプレイやハードディスクの電源を切る、スリープ・スタンバイ状態にする時間を設定できます。	—	—	○	×
●	●	—	Windowsアップデート管理	FU・QU・更新プログラム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。	○*3	○*1	○	×
—	●	●	ログオン・ログオフログ*4	電源ON・OFF・ログオン・ログオフのログを取得できます。	—	—	○	○
—	●	●	操作ログ管理*4	デバイス上での画面閲覧（ウィンドウタイトル）やファイル操作、アプリ利用ログを取得できます。	—	—	○	○
—	●	●	Webサイト閲覧ログ*4	Webサイトの閲覧、Webメールやクラウドストレージへのアップロード／ダウンロードを取得できます。	×	×	○	○*5
—	●	●	プリントログ*4	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*4	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	×	×	○	×
●	●	●	リモートロック・ワイプ	遠隔で画面ロックやデータの初期化することができます。	○	○*6	○*7	○
●	●	—	位置情報管理*8	位置情報を自動で取得し、複数の情報をまとめて表示、またデバイス別に移動履歴も確認できます。	○	○	○	×
●	—*2	—	デバイス利用ログ（モバイル）	デバイスの画面ロック解除時間やアプリの利用ログ、電話の発着信ログを取得できます。	△*9	○	—	—
●	—*2	—	Apple Business Manager	構成プロファイルの配信やDEP・VPP*10・紛失モードなどの機能を利用できます。	○	—	—	○*11
●	—*2	—	Android Enterprise	デバイスの利用制御やアプリ管理（Playストアのカスタマイズ）を利用できます。	—	○	—	—
●	●	●	レポート機能*12	グループ別・デバイス別に取得したデバイス情報・操作ログを自動集計し、レポートで確認できます。	○	○	○	○
●	●	●	管理コンソールのセキュリティ	許可されていない第三者がアクセスできないよう、IPアドレス制限や2要素認証、パスワードポリシーを設定できます。	○	○	○	○

補足 (*1～*12) は次頁を参照してください。

(機能一覧 補足)

*1 Android Enterprise を利用する必要があります。

*2 iOS・Android 向けの機能のため、ライトA ライセンスを購入してください。macOS はライトA・ベーシックいずれの購入でも利用できます。

*3 デバイスを監視モードに設定する必要があります。

*4 ログの保存期間（検索対象・CSV 形式による出力対象）は過去2年分です。ログ運用オプションを導入している場合のログ保存期間は5年です。

*5 macOS は Webサイト閲覧ログの取得のみ対応しています。

*6 Android10 以降のデバイスでは、Android Enterprise を利用する必要があります。

*7 リモートワイプは BitLocker で暗号化されたシステムドライブに対して、遠隔で暗号化キーを削除し、起動できない状態にします。

また Windows Server OS はリモートロック・ワイプは未対応です。

*8 Windows Server OS は未対応です。また取得条件があります。詳細はお問い合わせください。

*9 取得条件があります。またアプリの利用ログは取得できません。詳細はお問い合わせください。

*10 オプション機能です。

*11 VPP・紛失モードは iOS 向けの機能です。macOS には対応していません。

*12 契約プラン、取得する情報に応じて、確認できるレポートは異なります。

機能一覧（オプション）

オプション	購入可能ライセンス			機能		対象OS			
				機能名	概要	i	A	w	m
	ライトA	ベーシック	ライトB						
地図利用料*1	●	●	—	地図利用	取得した位置情報を管理コンソールの地図上で確認できます。	○	○	○	×
24/365 紛失サポート	●	●	●	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、ワイプを管理者の方に代わり実行します。	○	○	○	○
VPP	●	●	—	VPP (Volume Purchase Program)	Apple Business Manager 上で入手したアプリをデバイスに配信できます。	○	—	—	×
外部脅威調査	—	●	●	アプリ稼働ログ	アプリの稼働情報を取得し、未使用アプリを把握できます。	—	—	○	—
				アプリ通信ログ	ファイアウォール等の製品で検知した通信元IPアドレス、通信元ポート情報から、不審な通信を行っているプロセス（アプリ）を特定。アプリ名やハッシュ情報から不審なアプリの解析を行うことができます。	—	—	○	—
ログ運用	—	●	●	長期ログ保存・出力機能	過去5年分の操作ログを保存し、管理コンソールから検索したり、期間・ログ種別を指定した上で CSV ファイルにて出力することができます*2。	—	—	○	○
				Splunk 連携	エンドポイントマネージャーで取得したログを Splunk に自動転送し、Splunk のダッシュボード上でログを確認できます。	—	—	○	○
Web フィルタリング*3	●	●	●	Web フィルタリング機能	Web サイトの利用を監視し、指定したカテゴリに含まれるサイトを自動的に閲覧禁止にできます。	○	○	○	×
デバイス検査	●	●	●	デバイス検査	デバイスの検査を行い、ポリシー違反があった場合は警告ダイアログの表示や利用制限を実行できます。	×	×	○	×

*1 プラン I 専用のオプションです。プラン II・III で購入する場合は、利用料金内に含まれています。

*2 ログ運用オプションを申し込まない場合、ログの保存期間は過去2年分となります。

*3 導入前に体験版による検証をお願いします。

価格表（価格は税抜き表示です）

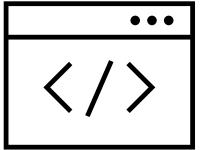
	ライセンス	プランⅢ（自動更新）
必須購入	初期費用	月額利用料 30,000円/契約
	ベーシック	500円/台
	ライトA	300円/台
	ライトB	400円/台
	24/365紛失サポート	150円/台
オプション	VPP ^{*2}	100円/台
	外部脅威調査 ^{*3}	100円/台
	ログ運用 ^{*3}	100円/台
	Web フィルタリング	100円/台
	デバイス検査	150円/台
アップ グレード ^{*1}	ライトA アップグレード	
	ライトB アップグレード	

*1 プランⅢの場合、ライトA またはライトBを解約し、ベーシックを新規で申込みいただきます。その際、初期費用（30,000円/契約）は必要ありません。また環境引き継ぎが可能です。ライトA → ライトB、ライトB → ライト A への移行は不可、ベーシックからライトへのダウングレードはできません。

*2 ライトB のみ購入している場合は、購入できません。ライトA またはベーシックの購入が必要です。

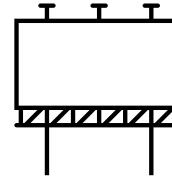
*3 ライトA のみ購入している場合は、購入できません。ライトB またはベーシックの購入が必要です。

ユーザー様専用サイト



エンドポイントマネージャー クラウド版の最新情報、初期設定マニュアルや動画、FAQなど製品を活用していただけるようコンテンツを取り揃えています。

トレーニングセミナー



オンライン形式で製品の基本的な利用方法から運用まで管理コンソールを利用しながらカスタマーサクセス担当が説明します。チャット機能で、その場ですぐに質問し、疑問を解決できます。

ヘルプデスクサポート



エンドポイントマネージャー クラウド版をご利用いただいている中で発生した疑問や質問に対して、電話やメール、チャットによるサポート対応を行っています。

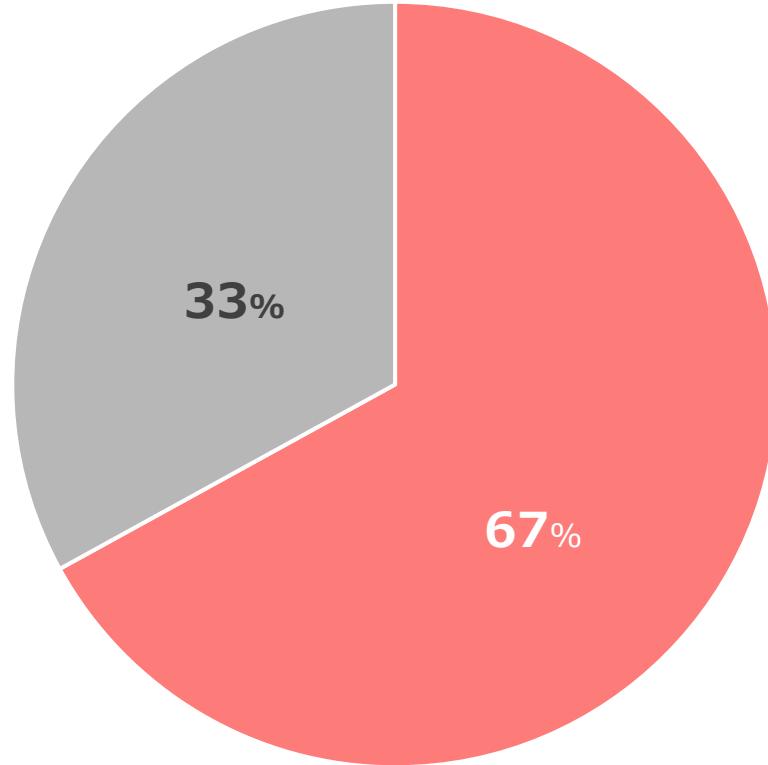


代理ログイン・リモートサポート

お客様に同意をいただいた上で、管理コンソールに代理ログインし、操作案内やトラブル解決を行います。

使いやすさ・管理のしやすさを実感していただくため、60日間の無料体験版をご用意
体験版環境をそのまま製品版へ移行することも可能です。

体験版利用ユーザーの製品版への移行割合



体験版の利用を円滑に進めるためのコンテンツ



オンライン・PDF版のマニュアル



初期設定手順をまとめた動画マニュアル



サポートセンター

体験版ご利用期間中もお電話・メール・チャットでお問い合わせいただけます。

3. エンドポイントマネージャー クラウド版 各機能のご紹介

機能紹介① 資産管理（ハードウェア・アプリ管理）

機能紹介② 紛失対策・セキュリティ

機能紹介③ Windows・macOS 操作ログ管理

機能紹介④ Apple Business Manager／Android Enterprise

機能紹介⑤ 関連製品

管理下のデバイスの最新情報を自動取得し、一覧で表示

デバイスを特定し、1Clickで詳細の資産情報の確認が可能。自動取得できない項目は、任意項目として管理できます。

LANSCOPE リスト レシピ モニター レポート ログ ルール

設定管理者（元中）

デバイス アプリ プロファイル アラート

ネットワーク全体 iOS Android Windows macOS 周辺機器

キーワード検索（例：営業 iPhone）

デバイスの追加 周辺機器の追加 インストール待ちデバイス

□	↑ 管理...	デバイスグループ	デバイスマネジメント名	使用者名	OSタイプ	OSバージョン	電話番号	デバイス
□	9	総務課	iPhone_00000026	森 太郎	iOS	14.4	080xxxxxxxx	iPhone
□	10	営業1課	iPhone_00000029	別所 哲郎	iOS	13.2	080xxxxxxxx	iPhone
□	11	営業1課	Surface Pro 5_0000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134	090xxxxxxxx	Surface
□	12	営業1課	Surface Pro 5_0000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134	090xxxxxxxx	Surface
□	13	営業1課	404KC_0000000023	石井 健二	Android	9	080xxxxxxxx	404KC
□	14	営業1課	404KC_0000000018	平尾 晃作	Android	9	080xxxxxxxx	404KC
□	15	営業2課	404KC_0000000007	KLBR 生込子	Android	10	000xxxxxxxx	404KC
□	16	営業部	iPhone_00000030	佐藤 新	iOS	14.2	080xxxxxxxx	iPhone
□	17	営業2課	iPhone_00000031	鈴木 一	iOS	14.1	080xxxxxxxx	iPhone
□	18	営業2課	iPhone_00000032	佐竹 信弘	iOS	13.5.1	080xxxxxxxx	iPhone
□	19	営業2課	iPhone_00000033	石川 忍	iOS	14.4	080xxxxxxxx	iPhone
□	20	営業2課	Surface 3_0000000054	石川 忍	Windows	Windows 10 Home 10.0.10240		Surface
□	21	営業1課	iPad_00000034	小林 哲司	iOS	14.2	080xxxxxxxx	iPad
□	22		Surface 3_0000000051	荒城 太郎	Windows	Windows 10 Home 10.0.10240		Surface
□	23		Surface 3_0000000047	MO三郎	Windows	Windows 10 Pro 10.0.19041		Surface
□	24		Surface 3_0000000048	MO花子	Windows	Windows 10 Pro 10.0.19041		Surface
□			Surface 3_0000000049	MO二郎	Windows	Windows 10 Pro 10.0.19041		Surface
登録者名			OSタイプ					
所 哲郎			iOS					
吉田 勝平			Windows					
鈴木 信也			Android					
健二			Android					
			Android					

固定列を設定し、ストレスのない横スクロールを実現。表示する項目・順番も並び替え可能。

Windows Surface Pro 5_0000000044 - デバイス詳細

管理No. 11

デバイスグループ
営業1課

使用者名
吉田 勝平

電話番号
090xxxxxxxx

ログオンユーザー名
-

最終稼働
15時間前

取得日時 : -

システム

OSバージョン
Windows 10 Pro 10.0.17134

OSアーキテクチャ
64ビット

Windowsバージョン
1803

CPU名
Intel(R) Core(TM) i7-3770 CPU @ 3.42GHz

CPU周波数
3.40 GHz

メモリ
15.89 GB

ドメイン・ワークグループ名
WORKGROUP

ログオンユーザーID
S-1-5-21-984867327-8815634417-5210944867-5132

ハードウェア

1Clickでデバイスの詳細情報を確認

プリンター・ルーターなどエージェントをインストールできない機器もまとめて管理

最大10,000台まで登録可能、デバイスイメージ（アイコン）の設定で、OS・機器混在環境でも視認性の良い台帳作成が可能

LANSCOPE

- リスト レシピ モニター レポート ログ ルール

デバイス アプリ プロファイル アラート

ネットワーク全体 iOS Android Windows macOS 周辺機器

デバイスの追加 周辺機器の追加 インストール待ちデバイス

□	↑ 管理...	デバイスグループ	デバイス管理名	使用者名	OSタイプ	OSバージョン
□	73	検証用	Surface Pro 3_0000000...	検証用P	Windows	Windows 10 Pro 10.0.1
□	74	検証用	Surface Pro 3_0000000...	検証用Q	Windows	Windows 10 Pro 10.0.1
□	75	検証用	Surface Pro 3_0000000...	検証用R	Windows	Windows 10 Pro 10.0.1
□	76	検証用	Surface Pro 3_0000000...	検証用S	Windows	Windows 10 Pro 10.0.1
□	77	検証用	Surface Pro 3_0000000...	検証用T	Windows	Windows 10 Pro 10.0.1
□	78	検証用	Surface Pro 3_0000000...	検証用U	Windows	Windows 10 Pro 10.0.1
□	79	検証用	Surface Pro 3_0000000...	検証用V	Windows	Windows Server 2012R2
□	80	検証用	Surface Pro 3_0000000...	検証用W	Windows	Windows Server 2016
□	81	検証用	Surface Pro 3_0000000...	検証用X	Windows	Windows Server 2016
□	82	検証用	Surface Pro 3_0000000...	検証用Y	Windows	Windows Server 2019
□	83	検証用	Surface Pro 3_0000000...	検証用Z	Windows	Windows Server 2019
□	84	サポート2課	MacBook_00000084	MO四郎	macOS	11.2.3
□	85	サポート2課	MacBook_00000085	MO五郎	macOS	12.1
□	86	営業1課	本社7階営業部_プリン...	執務室7F	周辺機器	
□	87	営業2課	東京事業所2階ルーター	執務室2Fの真ん中の島	周辺機器	
□	88	システム1課	本社キーボード_00001	本社キーボード1	周辺機器	
□	89	システム1課	廃棄用PC_00005	検証用	周辺機器	
□	90	システム3課	DVDドライブ_00004	本社3F用	周辺機器	

登録済みライセンス: 85 / 100 周辺機器: 5 / 10,000

周辺機器の追加

追加方法を選択してください。

1台ずつ追加 一括インポート追加

基本情報

デバイスグループ* 営業2課

デバイス管理名* 東京事業所2階ルーター

使用者名 執務室2Fの真ん中の島

使用する社員コード

デバイスタイプ ルーター/HUB

Apple ID

使用者の組織名

管理者名

キャンセル 保存

1台ずつ登録 or CSV による一括登録

デバイスイメージ（アイコン）	
	iOS
	Android
	Windows
	macOS
	パソコン
	プリンター
	ルーター / HUB
	入力機器
	スマートデバイス
	その他

インストールアプリ情報一覧

“このアプリ”は“どのデバイス”にインストールされているか？1Clickで把握！

The screenshot displays the LANSCOPE application interface, specifically the 'Apps' tab for iOS devices. The main table lists various applications installed on different devices, including their names, management apps, install counts, developers, categories, and application IDs. A red callout box highlights the search bar at the top, stating "Store カテゴリや アプリ名でも検索可能" (Searchable by category or app name). Another red callout box points to the table, stating "業務と関係ないアプリが 3台 インストールされている！" (3 business-unrelated apps are installed!). A third red callout box points to the right pane, stating "そのデバイスにインストールされているアプリも 1Clickで 確認可能！" (You can also confirm the installed apps on that device with 1 Click!). The right pane shows a detailed view for the iPhone_00000027 device, listing all installed applications along with their names, versions, management apps, developers, categories, and sizes.

アプリ	管理アプリ	インストール台数	開発者	カテゴリ	アプリケーションID
2ちゃんねるまとめサイトビ...	Trysail Inc.	3台	Trysail Inc.	仕事効率化	com.mt2
ATOK	JUSTSYSTEMS CORPORATION	15台	JUSTSYSTEMS CORPORATION	仕事効率化	com.justsystems.atokmobile...
Evernote				仕事効率化	com.evernote.iPhone.Evernote
FastEver XL - 素早く簡単にE...				仕事効率化	com.rakkoentertainment.Fas...
GNewsReader				仕事効率化	jp.co.leadingwin
Lock 'n' Roll Pro	Canned Bananas LLC	3台	Canned Bananas LLC	仕事効率化	com.cannedbananas.locknro...
ガイガーカウンター及び線量...	Image Insight, Inc.	9台	Image Insight, Inc.	仕事効率化	com.dosiapp.RadiationDosi...
チャットワーク - iPhone/iPa...	ChatWork Inc.	8台	ChatWork Inc.	仕事効率化	com.chatwork
メモリーブースター(Memory B...	AIO Toolbox Inc.	7台	AIO Toolbox Inc.	仕事効率化	imoblife.memorybooster.full
Microsoft Outlook	Microsoft Corporation	5台	Microsoft Corporation	仕事効率化	com.microsoft.Office.Outlook
LINE WORKS	Works Mobile Corps.	5台	Works Mobile Corps.	ビジネス	com.nhncorp.worksone
Google マップ - 乗換案内 & ...	Google LLC	1台	Google LLC	ナビゲーション	com.googleMaps
乗換案内	Jorudan Co.,Ltd.	6台	Jorudan Co.,Ltd.	ナビゲーション	jp.co.jorudan.NorikaeAnnai
Pokémon GO	Niantic, Inc.	6台	Niantic, Inc.	ゲーム	com.nianticlabs.pokemongo
100万人のための雀雀	UNBALANCE Corporation	2台	UNBALANCE Corporation	ゲーム	jp.co.unbalance.android.m1...

ハードウェア・インストールアプリ情報取得の API を公開

Microsoft Power Automate などで API をリクエストすると、エンドポイントマネージャーは json 形式でレスポンスします。

■ API の活用例



- API を実行して、自社で利用しているサービスに、デバイスのハードウェア情報を取り込む



- API を実行し、CSV ファイルを生成する bat ファイルを作成することで、ハードウェア・アプリ情報を CSV ファイルで保存する

LANSCOPE クラウド版 API ドキュメント 1.0.0 OAS3

本ドキュメントは、LANSCOPE クラウド版 API を利用する開発者向けのドキュメントです。

API 実行方法

APIリクエストは、APIトークンを使用してhttpsで行う必要があります。
APIトークンは、以下の形でHTTPリクエストヘッダに指定します。

```
Authorization: Bearer {あなたのAPIトークン}
```

APIのベースURLは、<https://api.lanscope.jp> です。
例えば、IT資産情報取得API を実行する場合は、<https://api.lanscope.jp/api/v1/assets> になります。

実行回数制限

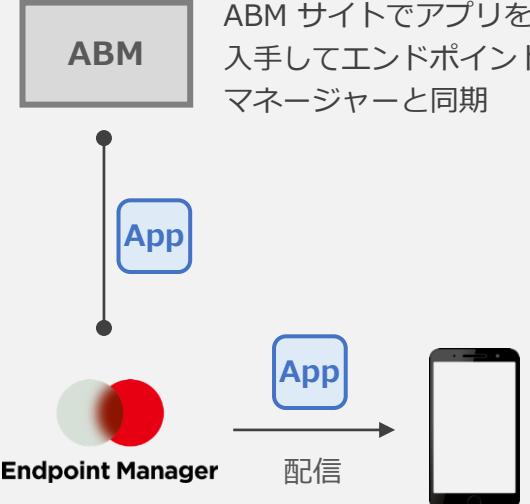
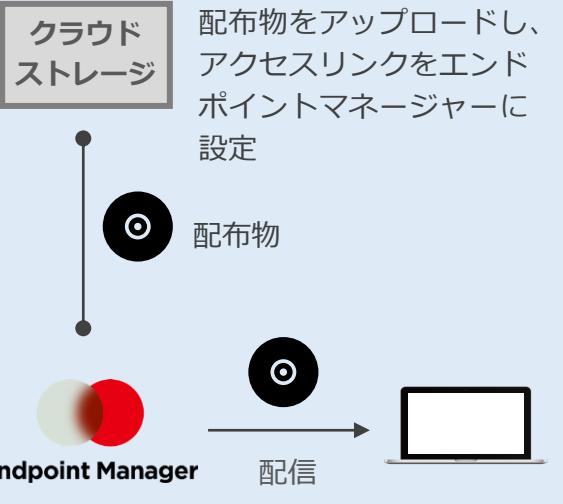
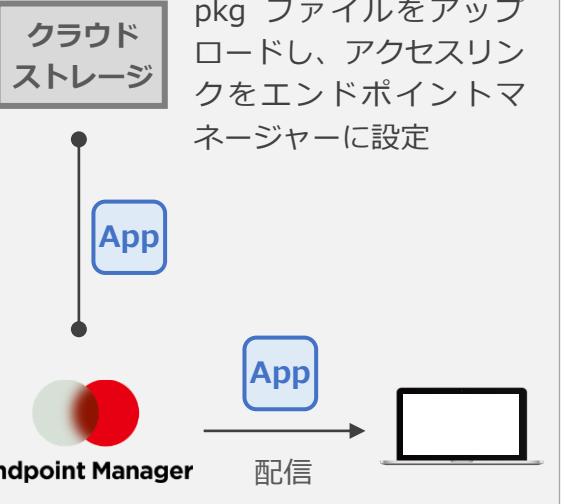
1日あたり10,000リクエスト(※) までとなっています。
実行回数制限を超えて、APIを実行すると、429のレスポンスが返されます。
※ 実行回数制限の仕様は変更する可能性があります。

ページネーション

レスポンスに含まれるデータが大量になる場合、一定件数で打ち切られ、データと合わせて `next_token` を返します。
打ち切りとなる件数はエンドポイントごとに異なります。
レスポンスで `next_token` が返された場合には、その値をリクエストパラメータに指定し、
報を取得できます。
この時、`next_token` 以外のリクエストパラメータは、前回のリクエ

業務に必要なファイル・アプリをデバイスに配信

OS によって仕様が異なります。

iOS	Android	Windows	macOS
<p>Apple Business Managerを利用することで、Apple ID のサインインに依存することなく、アプリの配信・インストールが可能（オプション機能）。</p>  <pre> graph TD ABM[ABM] --> App1[App] App1 --> EM1[Endpoint Manager] EM1 --> Phone1[smartphone] </pre>	<p>Android Enterprise を利用することで、デバイスの Play ストアをカスタマイズして、許可したアプリのみ表示。表示だけでなく強制インストールも可。</p> 	<p>管理者が設定したファイルを、PC 利用者の操作を必要とせず、ダウンロード／実行できます。管理者権限を持たないデバイスにも権限を付与し配信。</p>  <pre> graph TD CS[クラウドストレージ] --> DO[Distribution Object] DO --> EM2[Endpoint Manager] EM2 --> Laptop1[laptop] </pre>	<p>アプリの pkg ファイルをクラウドストレージにアップロードして、対象デバイスにアプリをインストール。</p> 

資産情報ベースとしたアラート一覧

取得した資産情報から、デバイスがルールに従って適切に利用されているかを把握！

レポート Windows アップデート

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。

ネットワーク全体 集計日時: 2022/08/24 18:46:10

危険 (13)
注意 (6)

19台

配下のグループ

部門	台数
ネットワーク全体 (直下)	0台
総務課	1台
人事課	1台
営業部	11台
システム部	3台
サポートセンター	3台
運輸部	0台
検証用	0台

管理No. デバイス管理名 使用者名 セキュリティ警告レベル デバイスグループ OSタイプ

82	MacBook_00000085	MO五郎	危険	サポート2課	macOS
49	HTC_ACE_0000000006	小林 智子	危険	サポート1課	Android
48	volantis_0000000025	武田 郁恵	危険	サポート1課	Android
39	iPad_00000038	森下 信子	危険	システム3課	iOS
32	iPad_00000035	細川 孝信	危険	システム1課	iOS
27	iPhone_00000027	畠山 哲夫	危険	営業2課	iOS
24	Surface 3_0000000048	MO花子	危険	営業2課	Windows
20	Surface 3_0000000054	石川 忍	危険	営業2課	Windows
19	iPhone_00000033	石川 忍	危険	営業2課	iOS
18	iPhone_00000032	佐竹 信弘	危険	営業2課	iOS
14	404KC_0000000018	平尾 晃作	危険	営業2課	Android
9	iPhone_00000026	森 太郎	危険	総務課	iOS
6	L-22D_0000000016	内田 健太	危険	営業部	Android
43	iPad_00000039	山岡 節女	注意	システム3課	iOS
26	Surface 3_0000000050	MO一郎	注意	営業2課	Windows

20 1-19件 / 全19件 | < < 1 > >



危険/注意の警告レベルを設定し、柔軟な設定が可能！

設定したアラートは「危険」「注意」のレベルに振り分けることが可能です。アラート内容を管理者に通知することも可能で、例えば「『危険』のアラートが発生した時のみ、管理者にメールを送る」など柔軟な設定・管理を実現します。

設定できるアラート	i	A	W	m
パスワードポリシーに準拠していない	<input type="radio"/>	<input type="radio"/>	—	—
パスコードロックの設定がオフになっている	<input type="radio"/>	—	—	—
デバイスが管理外になっている	<input type="radio"/>	—	○	○
LANSCOPE Client のバージョンが最新になっていない	<input type="radio"/>	○	○	○
未稼働期間が指定された期間を超過している	<input type="radio"/>	○	○	○
空き容量が不足している	—	○	○	○
位置情報が取得されない設定になっている	—	○	○	—
指定したアプリがインストールされていない	<input type="radio"/>	○	○	○
指定したアプリがインストールされている	<input type="radio"/>	○	○	○
指定したアプリが実行された	—	○	—	—
新しくアプリがインストールされた	—	○	—	—
新規プロファイルがインストールされた	<input type="radio"/>	—	—	○
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	—	○	○	—
デバイスが不正に改造されている (Jailbreak/root化)	<input type="radio"/>	○	—	—
SDカードが抜き差しされた	—	○	—	—
SIMカードが抜き差しされた	<input type="radio"/>	○	○	—
OS バージョンが指定した範囲外になっている	<input type="radio"/>	○	○	—
もうすぐリース切れになる	<input type="radio"/>	○	○	○

3. エンドポイントマネージャー クラウド版 各機能のご紹介

機能紹介① 資産管理（ハードウェア・アプリ管理）

機能紹介② 紛失対策・セキュリティ

機能紹介③ Windows・macOS 操作ログ管理

機能紹介④ Apple Business Manager／Android Enterprise

機能紹介⑤ 関連製品

利用者に依存しがちなパスコードの設定ルールを会社で統一！

パスコードの最小文字数*

9文字

単純値 (aaaa、1234など)
 禁止する

英字と数字
 必須にする

英数字以外の文字の最小文字数
 設定する
最小文字数*
4文字

パスコードの有効期間
 設定する
有効期間 (日) (1 ~ 730 日)*
90

以前使用したパスコードの再使用禁止回数
 禁止する
再使用禁止回数*
2回

パスコード入力連続失敗によるデバイス初期化
 初期化する
連続失敗回数*
5回

この設定を有効にすることで、オフライン時でもワイプが実行されます。
Wi-Fi モデルのデバイスにも有効！

iOS・macOS の設定項目	
パスコードの最少文字数	
単純値 (aaaa、1234など) を禁止	
英字と数字が必要	
英数字以外の文字の最少文字数	
パスコードの有効期間	
以前使用したパスコードの再使用を禁止	
パスコード入力連続失敗によるデバイス初期化* ¹	
デバイスロック開始までの最大許容時間	
画面ロック解除時のパスコード要求までの最大許容時間	
ログイン失敗後の待ち時間* ²	
パスワードリセットの強制* ²	

Androidの設定項目	
パスコードの最少文字数	
使用しなければならない文字の種類	
パスコードの有効期間	
パスコードの有効期限を事前の通知	
以前使用したパスコードの再使用を禁止	
以前使用したパスコードの再使用を禁止	
パスコード入力連続失敗によるデバイス初期化	
スリープ開始までの最大許容時間	

*1 macOS はアカウントのロックが行われます。

*2 macOS のみ対応しています。

👉 パスワードポリシー設定の重要性

パスワードを設定していない場合、画面ロックの解除は容易です。情報漏洩を防ぐためにも、利用者にパスワードの設定条件を委ねるのではなく、会社のポリシーをデバイスに設定することは、紛失対策の基本と言えます。



Android10以降のデバイスの場合、Android Enterprise の利用が必要です。

Windows・Mac デバイス 標準搭載の ドライブ・ディスク暗号化機能の運用管理をエンドポイントマネージャーで！

Windows : BitLocker

BitLocker の回復キーを自動取得できるので、デバイス毎にファイルや印刷で保存する必要がなくなります。



macOS : FileVault

FileVault の設定を強制化したり、復旧キーを自動取得します。



紛失リスクに備える事後対策：位置情報の確認※・リモートロック・ワイプ

位置情報から所在確認！遠隔でリモートロックやワイプを実行し情報漏洩を防止！

Android L-22D_0000000016 - デバイス詳細

管理No. 6

デバイスグループ 営業部	使用者名 内田 健太	電話番号 080xxxxxx	アカウントのメールアドレス kenta.uchida@mot.co.jp	最終稼働 25日前
-----------------	---------------	-------------------	---	--------------

- 管理情報
- デバイスグループ
- デバイス情報
- ネットワーク
- セキュリティ
- インストールアプリ
- 位置情報
- 操作ログ
- △ アラート
- リモート操作
- Android Enterprise
- クライアント

位置情報を自動取得



Android L-22D_0000000016 - デバイス詳細

管理No. 6

デバイスグループ 営業部	使用者名 内田 健太	電話番号 080xxxxxx	アカウントのメールアドレス kenta.uchida@mot.co.jp	最終稼働 25日前
-----------------	---------------	-------------------	---	--------------

- 管理情報
- デバイスグループ
- デバイス情報
- ネットワーク
- セキュリティ
- インストールアプリ
- 位置情報
- 操作ログ
- △ アラート
- リモート操作
- Android Enterprise
- クライアント

リモート操作を実行する

リモートロックを実行

リモートワイプを実行

パスワードを再設定

内容 リモートロック
状態 実行中
実行日時 2019/01/17 16:02:06
詳細 リモート操作を実行中です。

リモート操作を実行する

リモートロックを実行

リモートワイプを実行

パスワードを再設定

内容 リモートロック
状態 実行中
実行日時 2019/01/17 16:02:06
詳細 リモート操作を実行中です。

※ 位置情報の取得のためにはデバイス側で必要な設定があります。詳細はお問い合わせください。また位置情報の取得精度はデバイスに依存します。

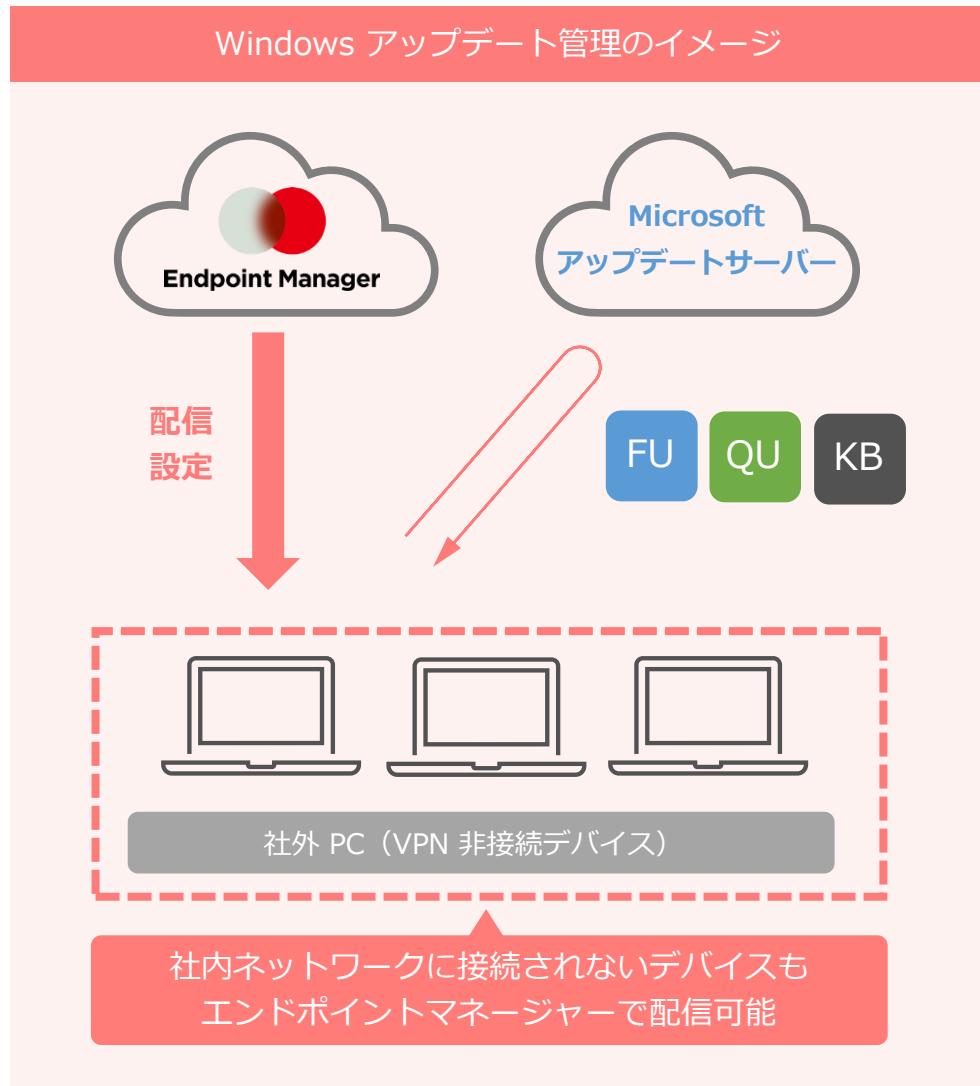
※ OSによってリモートロック・ワイプの仕様は異なります。Windows Server OS はリモートロック・ワイプ機能に対応していません。

※ Windows Server OS・macOS は位置情報取得機能には対応していません。

※ Windows はスリープ状態の場合、位置情報が取得できません。

Windows アップデート管理

Windows アップデートの適用状況を、“視認性の良い” レポート形式で把握



LANSCOPE リスト レシピ モニター レポート ログ ルール 設定管理者 (元中) 設定状況

ログアラート 利用状況 Windows アップデート

集計日時: 2023/06/16 09:08:38

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デバイスを確認して対策できます。

サポート終了 サポート終了間近

Windows 10 8台
Windows Server 2012... 1台
Windows Server 2016 2台
Windows Server 2019 すべてサポート中です

月例パッチ (サーバー) が未適用のデバイス
サーバー用の月例パッチが未適用のデバイスを確認して対策できます。

最新 (2023/06/11)

バッチ未適用

Windows Server 2019 1台
Windows Server 2016 すべて適用済みです
Windows Server 2012... すべて適用済みです

月例パッチ (クライアント) が未適用のデバイス
クライアント用の月例パッチが未適用のデバイスを確認して対策できます。

最新 (2023/06/11)

バッチ未適用

Windows 10 6台

月例パッチの詳細

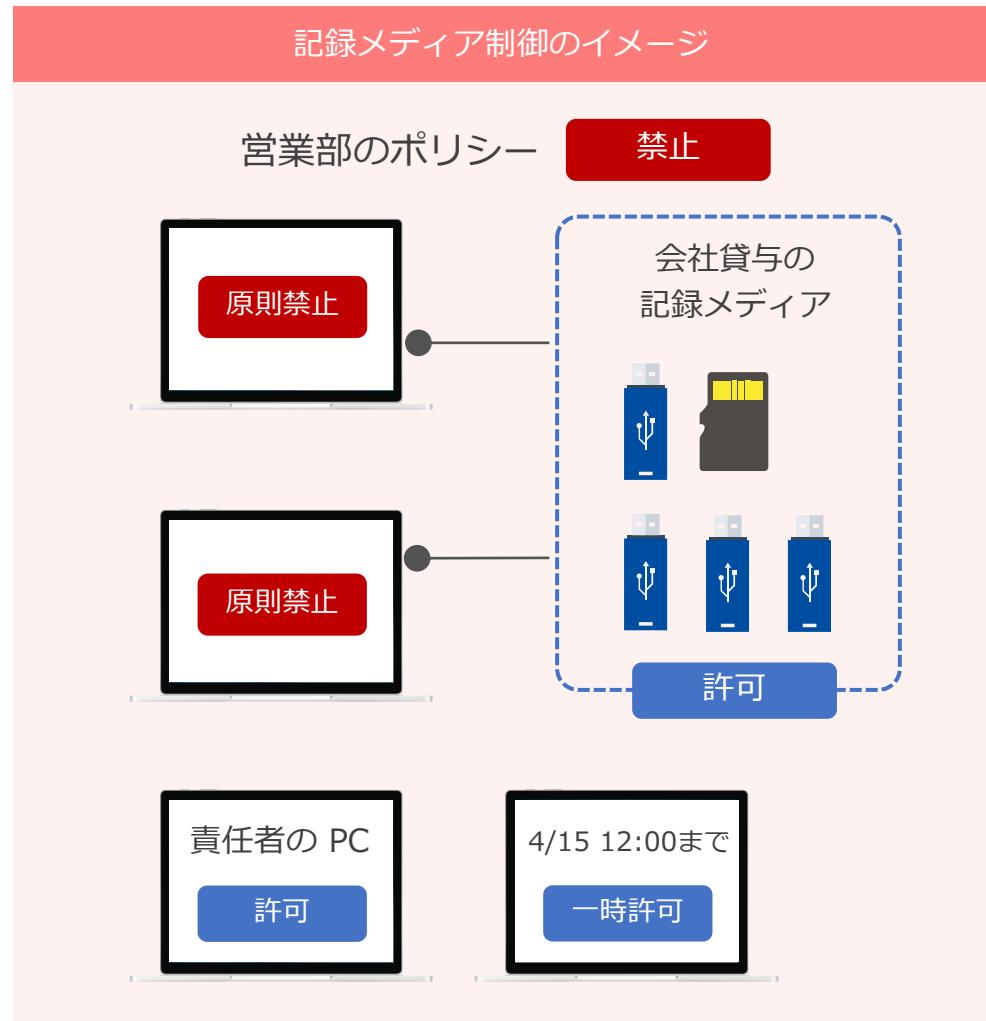
件数を絞り込む インストール履歴

デバイス	適用された月例パッチ	管理ID	デバイスグループ	デバイス管理名	OSバージョン	取得日時
未適用	2023/06/13	29	営業会議	Surface 3_00000000054	Windows 10 Home 10.0.19240	2023/07/29 08:57:29
未適用	2023/06/13	22	営業会議	Surface 3_00000000055	Windows 10 Home 10.0.19240	2023/07/29 08:29:29
未適用	2023/06/13	11	営業会議	Surface Pro 5_00000000044	Windows 10 Pro 10.0.17134	2023/07/29 08:29:27
未適用	2023/06/13	12	営業会議	Surface Pro 5_00000000045	Windows 10 Pro 10.0.17134	2023/07/29 08:29:27

1Clickで未適用デバイスを把握し、
アップデート配信が可能

USB メモリなどの記録メディアの利用を制御し、情報漏洩を防止

グループ単位で禁止・読み取り専用・許可のいずれかから基本ポリシーを設定。特定記録メディアのみ許可/特定 PC のみ許可/特定時間のみ許可など柔軟な設定が可能。



記録メディア制御の全体設定 (Recording Media Control General Settings)

デバイスグループ: ネットワーク全体

選択された部門: 営業部

ネットワーク全体の設定 (Network-wide Settings)

全体設定: 禁止する (書き込み/読み取り可)

除外設定: 設定する (指定した記録メディア毎に許可/読み取り専用にする)

記録メディアの個別設定 (Individual Recording Media Settings)

周辺機器接続ログから追加

シリアル No	ベンダー ID	プロダクト ID	許可	読み取り
35F37B7FB15A03FF91841A...			<input type="radio"/>	-
C2E830DCE0193A38B65964...			<input type="radio"/>	-
f84067126ca57b1	0x0457	0x0151	<input checked="" type="radio"/>	-
f84067126ca57b2	0x0457	0x0151	-	<input checked="" type="radio"/>
f84067126ca57b3	0x0457	0x0151	<input checked="" type="radio"/>	-

特定の記録メディアを許可 (Allow Specific Recording Media)

通知する (Notify): タイトル: 禁止通知 - 記録メディア使用禁止
メッセージ: 記録メディアの使用は、社内ポリシーによって禁止されています。
%MEDIA%
過去に入力された通知設定から引用
※ メッセージに以下のキーワードを入力すると、禁止時の各情報に変換されます。
%TIME% : 抵触時の日時
%MEDIA% : 記録メディアの情報

禁止時には利用者にメッセージを表示 (Display Message to User When Prohibited)

「古い OS を利用していないか」 「セキュリティソフトがインストールされているか」など
検査項目に違反があった場合に、警告・制御・特定アプリの起動を自動実行

▼トリガー・アクション一覧

	トリガー名	概要
検査 (トリガー)	Windows OS バージョン検査	利用している OS バージョンが指定したバージョン外の場合に検査違反と判定します。
	Windows セキュリティパッチ検査	指定したセキュリティパッチがインストールされていない場合に検査違反と判定します。
	アプリインストール検査	指定したアプリがインストールされていない場合に検査違反と判定します。
	アプリバージョン検査	インストールされているアプリが指定したバージョン外の場合に検査違反と判定します。
	プロセス起動検査	指定したアプリが起動していない場合に検査違反と判定します。
	特定宛先への NW 疎通検査	指定したネットワークと疎通が取れていない場合に検査違反と判定します。
警告/制御 (アクション)	不適合警告	警告ダイアログを表示し、警告内容と必要な設定内容などを案内します。
	IP アドレス指定制御	あらかじめ指定した IP アドレス以外への接続を禁止できます。
	ドメイン名指定制御	あらかじめ指定したドメイン名以外への接続を禁止できます。
	特定 URL ブラウザアクセス	ブラウザを起動して、指定した Web サイトが表示されます。
	指定アプリ起動	PC にインストールされているアプリを実行します。

検査（トリガー）



警告・制御（アクション）



カテゴリを指定するだけで関連サイトの閲覧を一括で制御可能

OS によって動作が異なります。事前に体験版環境で動作確認をお願いします。

● 規制内容

許可／書き込み規制／規制／一時解除の4つの規制が可能です。

● カテゴリ別設定

ユーザ設定カテゴリを含めた全26種・148カテゴリで制御が可能です。さらにカテゴリごとにサブカテゴリが設定されており、より詳細な制御が可能です。

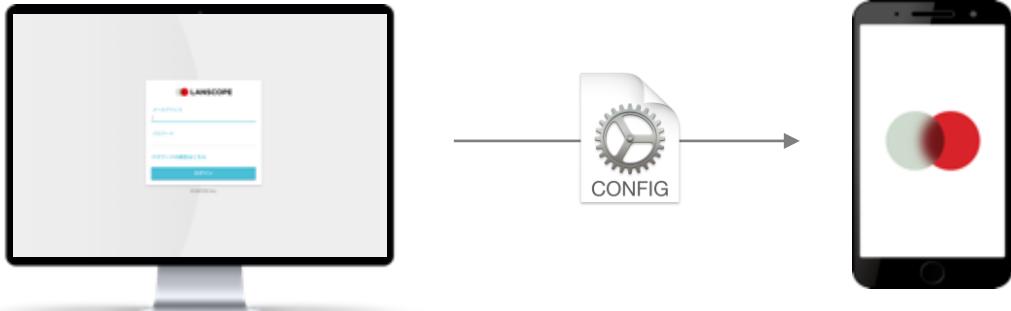
■ カテゴリ別ルール登録

参照ルール名	MOTEX	登録	戻る			
カテゴリ別ルール名						
規制内容	許可 書き込み規制 規制 一時解除					
カテゴリ	サブカテゴリ	設定	全て	全て	全て	全て
ユーザ設定カテゴリ		<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
不法		<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
アダルト・フェティシズム	アダルト・ポルノ	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
	フェティシズム	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
セキュリティ		<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
出会い系		<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
金融		<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
ギャンブル		<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
ショッピング		<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
コミュニケーション		<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>

iOS・macOS は構成プロファイル、Android は Android Enterprise で高度な管理を！

iOS・macOS 構成プロファイル

構成プロファイルを作成し※、デバイスに適用します。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できます。



※ エンドポイントマネージャーと Apple Configurator2 / プロファイルマネージャーで、作成できるプロファイルに違いがあります。

解説 iOS の「監視モード」について

構成プロファイルの中には、デバイスを監視モードに設定しないと適用できないものがあります。監視モードに設定するためには、Apple Configurator 2 がインストールされた Mac デバイスと iOS デバイスを接続し適用するか、自動デバイス登録 (DEP) を利用します。また監視モード適用時、デバイスの初期化が必要です。

Android Enterprise

Android Enterprise を利用※することで、初期化禁止やカメラの利用禁止などデバイスの利用制限を行うことができます。

※ Android Enterprise を利用する場合、デバイスのアクティベーション（初期化）が必要です。そのため、すでに利用しているデバイスで、Android Enterprise を利用したい場合は注意してください。



<ポリシー未適用>

<ポリシー適用>

3. エンドポイントマネージャー クラウド版 各機能のご紹介

機能紹介① 資産管理（ハードウェア・アプリ管理）

機能紹介② 紛失対策・セキュリティ

機能紹介③ Windows・macOS 操作ログ管理

機能紹介④ Apple Business Manager／Android Enterprise

機能紹介⑤ 関連製品

操作ログ取得

「どの部署の」「誰が」「いつ」「何をしたのか」をリアルタイムに取得

取得した操作ログは2年間保存され、検索によるログの抽出と CSV ファイルによる出力が可能。ログ運用オプションの導入で最大5年保存されます。

The screenshot shows the LANSCOPE software interface. On the left, there's a sidebar with sections for 'デバイスグループ' (Device Groups), '検索キーワード' (Search Keywords), and 'ログの種類' (Log Types). The main area displays a table of logs with columns for '日時' (Date & Time), '使用者名' (User Name), 'ログの種類' (Log Type), 'イベント' (Event), 'タイトル' (Title), and 'ファイルパス' (File Path). A specific log entry for 'MO-一郎' on 2022/08/24 at 19:54:00 is highlighted. A modal dialog box is overlaid on the screen, containing two warning messages: 'ファイル操作アラート' (File Operation Alert) and 'アプリケーション禁止' (Application Blocking). Both dialogs have '閉じる' (Close) buttons.

違反操作があった場合は、リアルタイムに警告通知が可能

※1 macOS は Web サイトの閲覧ログのみ対応しています。また対応ブラウザは Microsoft Edge・Google Chrome・FireFox・Safari です。

※2 macOS は周辺機器接続ログのみ対応しています。

※3 外部脅威調査オプションの導入が必要です。尚、macOS は非対応です。

取得できる操作ログ

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※1

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。

周辺機器・通信機器接続ログ※2

USB メモリなどの周辺機器、Wi-Fi・Bluetooth などへの接続／切断などのログを取得できます。

アプリ稼働・アプリ通信ログ※3

バックグラウンドで稼働しているアプリ情報、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。

ChatGPT (<https://chat.openai.com/>) の書き込み内容 = 質問内容の取得に対応、利用実態の見える化に！

対応 OS は Windows、対応ブラウザは Google Chrome・Microsoft Edge・FireFox です。



社内で利用ガイドラインを作ったまでは
良いけど、規定通りの利用ができているか？

そもそも、
どんな使い方をしているんだろう？？

個人情報や機密情報を ChatGPT に
書き込んでいないだろうか・・・

デバイス詳細

日時	ログオンユーザー名	ログの種類	イベント	稼働時間	タイトル	URL
2023/05/23 10:11:13	motex	Webアクセス	閲覧	00:00:11	新しいタブ - Google Chrome	chrome://newtab/
2023/05/23 10:11:25	motex	Webアクセス	閲覧	00:00:03	chatgpt - Google 検索 - Google Chrome	https://www.google.com/search?
2023/05/23 10:11:28	motex	Webアクセス	閲覧	00:00:09	Introducing ChatGPT - Google Chrome	https://openai.com/blog/chatgpt
2023/05/23 10:11:38	motex	Webアクセス	閲覧	00:00:01	無題 - Google Chrome	
2023/05/23 10:11:39	motex	Webアクセス	閲覧	00:00:40	https://chat.openai.com - Google Chrome	https://chat.openai.com/
2023/05/23 10:12:02	motex	Webアクセス	書込み	00:00:00	https://chat.openai.com - Google Chrome	https://chat.openai.com/
2023/05/23 10:12:36	motex	Webアクセス	閲覧	00:00:00	https://chat.openai.com - Google Chrome	https://chat.openai.com/
2023/05/23 14:06:05	motex	Webアクセス	閲覧	00:00:00	https://chat.openai.com - Google Chrome	https://chat.openai.com/
2023/05/23 14:06:35	motex	Webアクセス	閲覧	00:00:00	https://chat.openai.com/?model=text-davinci-002-render-sha	https://chat.openai.com/?model=text-davinci-002-render-sha
2023/05/23 14:09:10	motex	Webアクセス	閲覧	00:00:00	https://chat.openai.com/?model=text-davinci-002-render-sha	https://chat.openai.com/?model=text-davinci-002-render-sha

書込み内容
上司に対して送るメール文面を以下の要素を含む形で作成ください。・納期を超えたことに関するお詫び・原因は、然の相談を受けそちらに集中してしまった・再発防止を含む対策の記載

プログラム名
chrome.exe

※ 書き込みログは、ChatGPT の他、Gmail・Outlook Online・Outlook.com のメール送信内容の取得が可能です。

操作ログ検索

活用シーンに合わせたテンプレートから検索条件をセット。必要な操作ログを簡単に抽出。

検索条件をカスタマイズして、保存も可能。検索から 1Click で前後 30分の操作を抽出。

LANSCOPE リスト レシピ モニター レポート ログ ルール

検索 一括出力

操作ログ (Windows / macOS)

ネットワーク全体

削除済みデバイスのみ検索する

開始日～終了日
2023/06/09 00:00 ~ 2023/06/09 23:59

今日 昨日 今週

検索キーワード
イベント アップロード

ログオンユーザー名
ichiro.mo

+ 追加

ログの種類
すべてチェック すべてはずす
ログオンログオフ ウィンドウタイトル プリント
 Webアクセス ファイル操作 周辺機器接続

条件を保存 検索

2023/06/09 23:40:00
ISO 8601 (2023-06-09T23:40:00+09:00)
対象の前後のログを確認

ログオンユーザー名
ichiro.mo

ログの種類
Webアクセス

イベント
アップロード

タイトル
マイドライブ - Google ドライブ - Google Chrome

URL
https://drive.google.com/drive/u/1/my-drive

稼働時間
00:00:00

管理No.
26

プログラム名
chrome.exe

ファイルパス
C:\Users\ichiro.mo\MOTEX\Desktop\商品案内.xlsx

アラート種別
アップロード

デバイスグループ

クラウドストレージに製品情報をアップロード・・・！

Windows Surface 3_0000000050 - デバイス詳細

デバイスグループ
営業2課

使用者名
MO一郎

電話番号
090xxxxxx

< 2023/06/09 > 23:10 ~ 23:59 11個の項目を選択中

日時	ログオンユーザー名	稼働時間	ログの種類	イベント	タイトル
2023/06/09 23:32:00	ichiro.mo	00:00:00	ファイル操作	ファイルコピー元	
2023/06/09 23:32:00	ichiro.mo	00:00:00	ファイル操作	ファイルコピー先	
2023/06/09 23:35:00	ichiro.mo	00:00:10	ウィンドウタ...	ACTIVE	Desktop
2023/06/09 23:36:00	ichiro.mo	00:00:00	ファイル操作	ファイル名変更前	
2023/06/09 23:36:00	ichiro.mo	00:00:00	ファイル操作	ファイル名変更後	
2023/06/09 23:37:00	ichiro.mo	00:00:00	ファイル操作	ファイル閲覧	
2023/06/09 23:37:00	ichiro.mo	00:00:08	ウィンドウタ...	ACTIVE	マイドライブ - Google
2023/06/09 23:37:00	ichiro.mo	00:00:08	Webアクセス	閲覧	マイドライブ - Google
2023/06/09 23:37:00	ichiro.mo	00:00:09	ウィンドウタ...	ACTIVE	開く
2023/06/09 23:37:00	ichiro.mo	00:00:02	Webアクセス	閲覧	マイドライブ - Google
2023/06/09 23:37:00	ichiro.mo	00:00:03	ウィンドウタ...	ACTIVE	マイドライブ - Google
2023/06/09 23:40:00	ichiro.mo	00:00:00	Webアクセス	アップロード	マイドライブ - Google
2023/06/09 23:41:00	ichiro.mo	00:00:00	ファイル操作	ファイルコピー元	
2023/06/09 23:43:00	ichiro.mo	00:00:00	ファイル操作	ドライブ追加	
2023/06/09 23:43:00	ichiro.mo	00:00:00	ファイル操作	ドライブ追加	
2023/06/09 23:43:00	ichiro.mo	00:00:00	ファイル操作	ファイル名変更前	

→

1Click で前後30分間の操作ログが確認可能。

取得したログの活用：アラートレポート

グループ単位で違反操作の発生状況を見る化し、Click 操作で詳細を確認

レポート形式で確認できるのは過去3ヶ月分です。

The screenshot shows the LANSCOPE software interface. At the top, there are tabs for 'リスト' (List), 'レシピ' (Recipe), 'モニター' (Monitor), 'レポート' (Report) (which is selected), 'ログ' (Log), and 'ルール' (Rule). On the left, a sidebar shows a tree view of network groups: 総務課, 人事課, 営業部, システム部, サポートセンター, 運輸部, and 検証用. The main area displays a bar chart titled 'ログアラート' showing the number of alerts per day from May 1st to 31st. A red box highlights the bar for May 21st, which reaches a value of 40. Below the chart is a table for May 21st (日) showing alert details for two devices:

管理No.	デバイスグループ	デバイス管理名	↓ アラート合計	ウィンドウタイトル	枚数	ドキュメント名	閲覧
26	営業2課	Surface 3_0000000050	20	0	0	0	0
81	サポート2課	MacBook_00000084	20	0	0	0	0

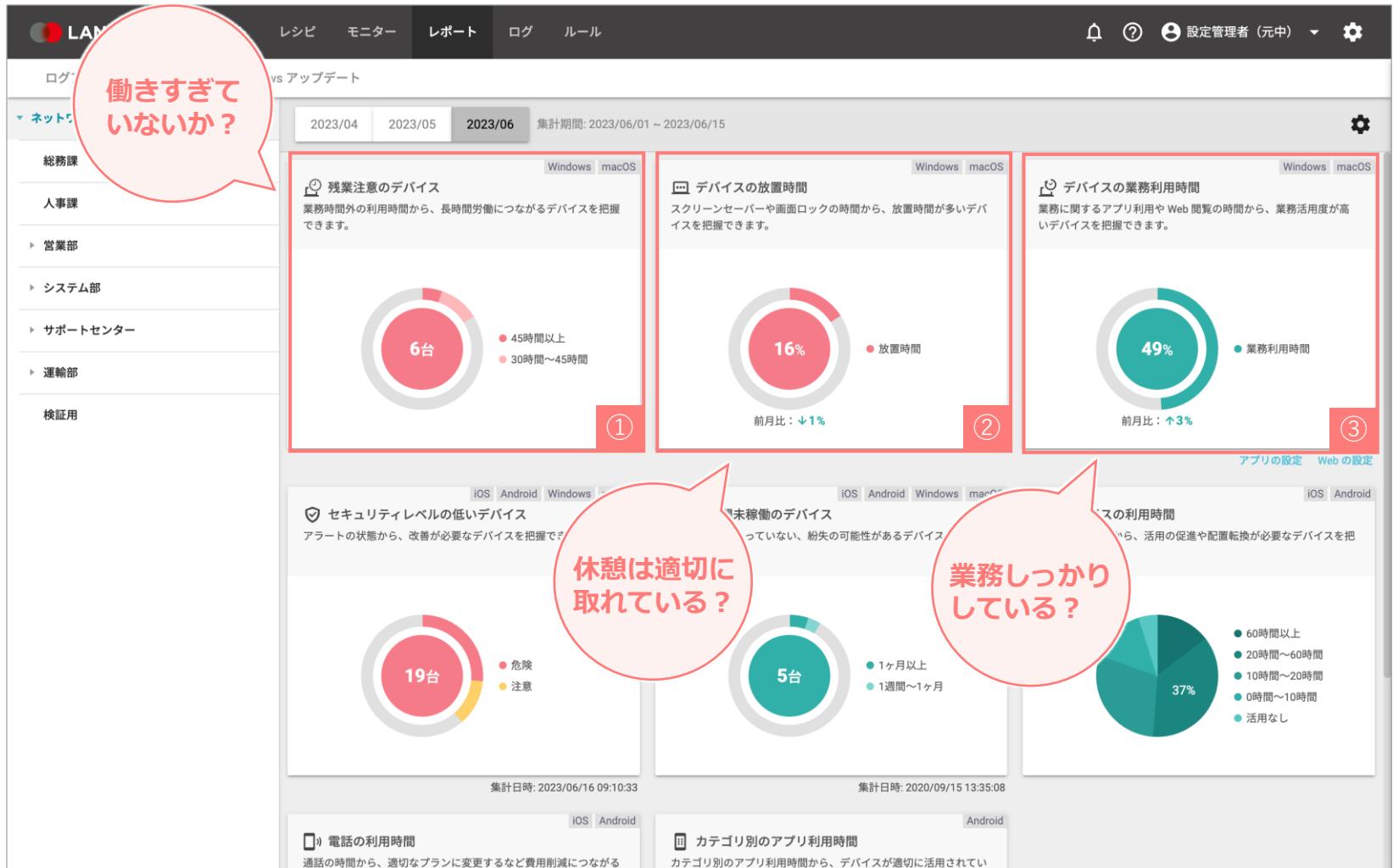
A callout box points to the table with the text: 'その日、どのデバイスで、どのようなアラートが何件発生したのかを確認！' (Check which device and what type of alert occurred on that day!).

設定できる操作ログのアラート	W	m
指定した文字列が含まれるウィンドウタイトル	<input type="radio"/>	<input checked="" type="radio"/>
一定枚数以上の印刷	<input type="radio"/>	<input checked="" type="radio"/>
指定したキーワードがドキュメント名に含まれる印刷	<input type="radio"/>	<input checked="" type="radio"/>
Web サイト閲覧（タイトル / URL）	<input type="radio"/>	<input checked="" type="radio"/>
Web サイトのアップロード/ダウンロード（タイトル / URL）	<input type="radio"/>	—
Web サイトの書き込み（タイトル / URL）	<input type="radio"/>	—
指定したキーワードが含まれるファイル操作	<input type="radio"/>	<input checked="" type="radio"/>
ドライブの追加	<input type="radio"/>	<input checked="" type="radio"/>
ドライブに追加された記録メディアへの書き込み	<input type="radio"/>	<input checked="" type="radio"/>
ローカル共有フォルダーの作成または書き込み	<input type="radio"/>	—
Outlook メールへのファイル添付	<input type="radio"/>	—
機密フォルダー内の操作	<input type="radio"/>	<input checked="" type="radio"/>
CSV ファイルへの出力	<input type="radio"/>	<input checked="" type="radio"/>
ネットワーク上の共有フォルダーへの書き込み	<input type="radio"/>	<input checked="" type="radio"/>
指定した SSID / BSSID への接続	<input type="radio"/>	—
Bluetooth 接続	<input type="radio"/>	—

取得したログの活用：働き方の見える化

「長時間働きすぎていないか？」「休憩は適切に取れているか？」

「業務をしっかりしているか？」の切り口でレポート化



① 残業注意のデバイス

業務時間外の稼働から、申請外の残業や働きすぎにつながるデバイスをみつけます。

<集計単位は1ヶ月間>

- 30時間～45時間
- 45時間以上

② デバイスの放置時間

スクリーンセーバー・画面ロックの時間から利用していない時間が多いデバイスをみつけます。

<集計単位は1ヶ月間>

- 放置時間
- 前月比

③ デバイスの業務利用時間

業務に関するアプリやWebの利用時間から業務での活用度が高いデバイスをみつけます。

<集計単位は1ヶ月>

- 業務利用時間
- その他

取得したログの活用：働き方の見える化

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

The screenshot displays the LANSCOPE application interface, which includes a navigation sidebar, a main dashboard, and a reporting section.

Left Sidebar: Shows departmental navigation (総務課, 人事課, 営業部, システム部, サポートセンター, 運輸部, 検証用) and a summary for "残業注意のデバイス" (Overwork Attention Device) with a count of 6 devices.

Main Dashboard: Features a circular chart showing device usage distribution (45時間以上: 2台, 30時間~45時間: 4台). A red callout bubble with "Click!!" points to this chart.

Reporting Section: Includes tabs for ログアラート, 利用状況 (selected), レシピ, モニター, レポート, ログ, and ルール. The 利用状況 tab shows a list of devices with overwork issues, a chart for "配下のグループ" (Subgroups), and a detailed table of device usage data.

Table Data (Table 3):

管理No.	デバイス管理名	使用者名	業務時間外の利用時間	デバイスグループ	OSタイプ
26	Surface 3_0000000050	MO一郎	76時間15分33秒	営業2課	Windows
25	Surface 3_0000000049	MO二郎	50時間58分56秒	営業2課	Windows
29	ElitePad_0000000052	共有タブレット	37時間33分20秒	システム部	Windows
82	MacBook_000000085	MO五郎	35時間0分0秒	サポート2課	macOS
55	Surface Pro 3_0000000053	検証用A	34時間46分40秒	検証用	Windows
23	Surface 3_0000000047	MO三郎	32時間0分0秒	営業2課	Windows

Callouts:

- ① Points to the "全体の割合" (Overall Ratio) chart in the main dashboard.
- ② Points to the "配下のグループ" (Subgroups) chart in the reporting section.
- ③ Points to the reporting table.
- A red callout bubble with "デバイスをクリックして個人レポートへ" (Click the device to view individual reports) points to the reporting table area.

①全体の割合

選択しているグループ全体の状況を見る化

②グループ別の比較

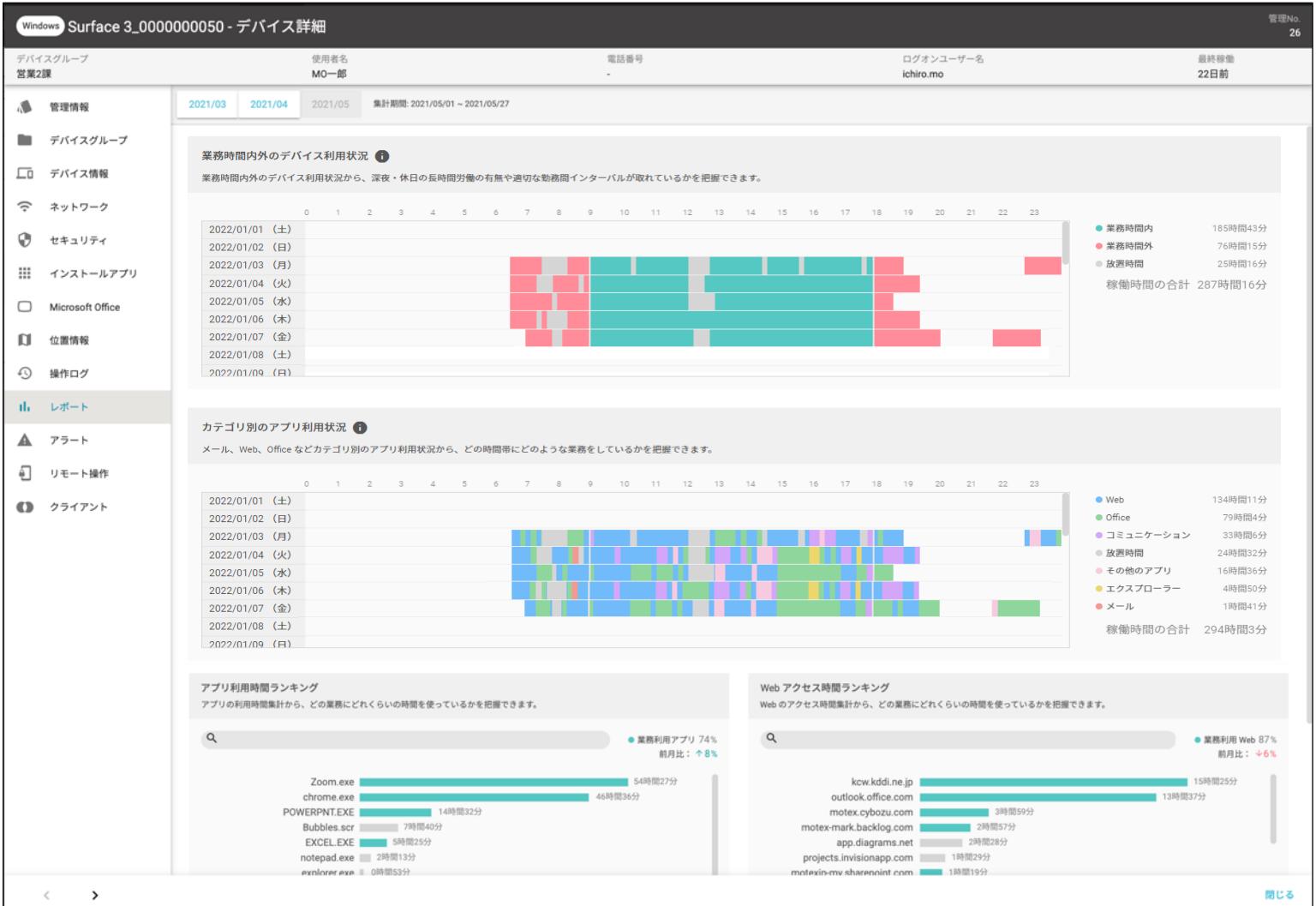
選択している配下のグループをグループ別に
状況を比較

③デバイスの内訳

「グループ別の比較」で選択したグループに所属する
デバイスを一覧で表示

取得したログの活用：働き方の見える化

PC の操作ログからデバイス単位で活用状況をレポート化



○業務時間内・業務時間外の利用時間

個人の1週間のPC稼働時間の割合を表示

- 業務時間内 ○○時間
- 業務時間外 ○○時間
- 放置時間 ○○時間
- 稼働時間合計 ○○時間

○アプリ別の利用時間

アプリ別の稼働情報を解析

10分間の内最もアクティブなアプリを表示

- | | |
|-------------------|-------------|
| • メール | • Web |
| • Office | • その他アプリ |
| • エクスプローラー/Finder | • スクリーンセーバー |

○アプリ利用時間ランキング

アプリ毎のアクティブ稼働時間のランキング

- 業務アプリ
- その他アプリ
- 業務アプリ比率 ○○%アップ／ダウン（前月比）

○Webアクセス時間ランキング

Webのアクティブ稼働ドメインのランキング

- 業務Web
- その他Web
- 業務アプリ比率 ○○%アップ／ダウン（前月比）

取得した操作ログは現状把握・セキュリティ対策に加えて、業務効率化・マネジメントに活用

これまでの「見える化」

管理者・経営者層による“監視”が主な目的



【NEW】「共有」「見せる化」

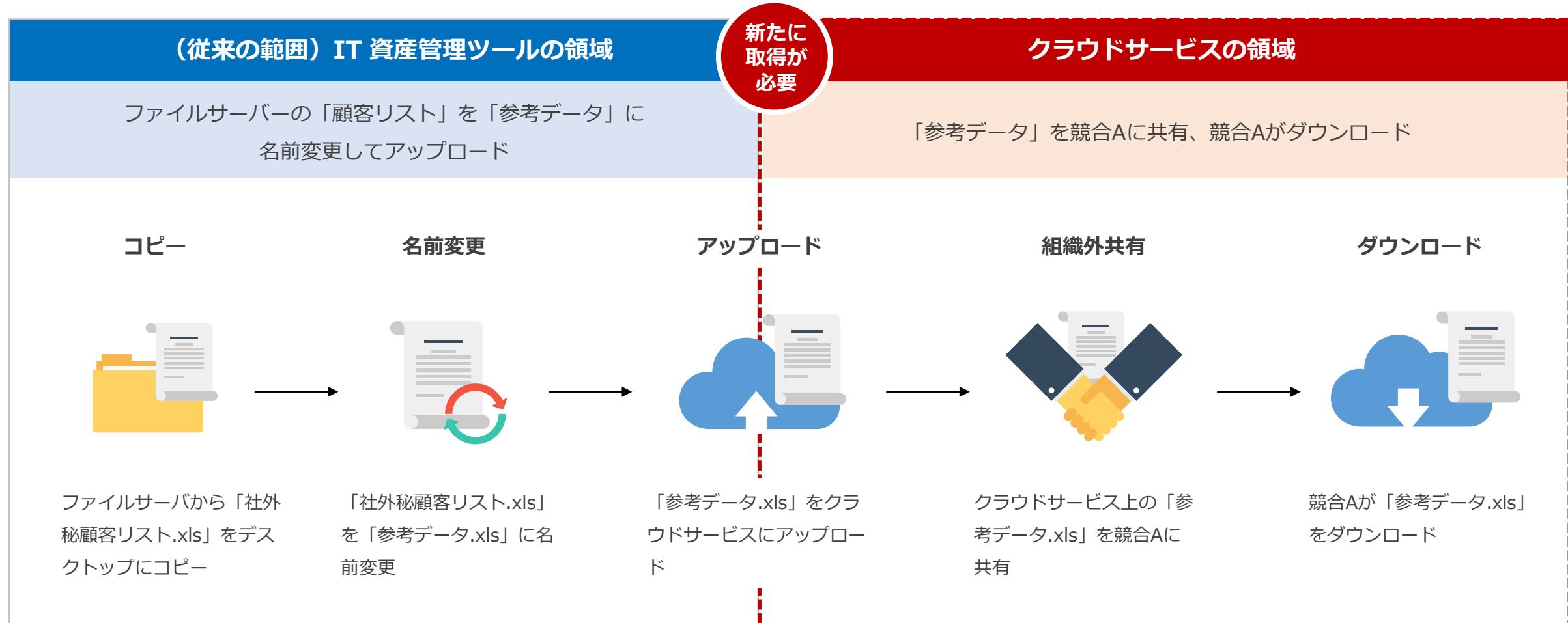
現場のマネージャーによる**業務の効率化や人材育成**に



適切な働き方ができているか？テレワークが進む現代の会社の生産性向上にもログ活用を推進！！

IT 資産管理ツールだけでは、Microsoft 365 経由の情報漏洩経路の特定はできません

Microsoft 365 でのファイル操作や共有状況の把握には、監査ログの取得と解析が必要です。



LANSCOPE セキュリティオーディターなら

Microsoft 365 に社内外からアクセスする全てのユーザーを対象に、情報漏洩対策で必要なログを管理

種類	概要	対象アプリ	
アカウント認証	アカウント認証	各アプリへのサインイン成功・失敗のログを取得できます。	   
Entra ID 設定	ユーザー設定	ユーザーの追加・削除やライセンスの割り当ての変更、パスワードの変更やリセットのログを取得できます。	
	グループ設定	グループ/メンバーの追加や削除、更新のログを取得できます。	
	ポリシー・ロール設定	デバイスアクセスポリシーの変更や管理者ロールの付与・剥奪のログを取得できます。	
メンバー招待	Teams チーム設定	メンバーの追加・削除、チームの作成・削除や設定の変更、チームへのボットの追加・削除のログを取得できます。	
	SharePoint グループ設定	グループの作成・更新・削除、グループメンバーの追加・削除のログを取得できます。	
	SharePoint・OneDrive 共有設定	共有への招待を作成・更新・取り消し・承諾・解除やサイトアクセス許可の変更ログを取得できます。	 
共有リンク操作	共有リンク発行	共有リンク（組織内/すべてのユーザー/特定のユーザー）・アクセス許可レベルの作成や追加・更新・削除のログを取得できます。	  
	共有リンクアクセス	アクセスの要求や更新・承諾のログを取得できます。	  
ファイル操作	ファイル操作	ファイルの閲覧・作成・削除、アップロード・ダウンロード、ファイル名の変更やフォルダー移動のログを取得できます。	  
	ゴミ箱操作	フォルダー/ファイルの復元やゴミ箱からの削除のログを取得できます。	  
	ラベル操作	ファイルに設定できる秘密度ラベルの追加・変更・削除のログを取得できます。	  
	レコード操作	レコードの削除、レコードのロック・ロック解除のログを取得できます。	  
	SharePoint 隠威検出	SharePoint ファイルでのマルウェアの検出ログを取得できます。	
サイト操作	サイト操作	ページの閲覧・作成・変更・削除のログを取得できます。	
	ハブサイト設定	ハブサイトの登録や関連付け・関連付け解除、ハブサイトの登録解除のログを取得できます。	
	地域操作	地域管理者の追加や削除、データの場所の追加・削除のログを取得できます。	
	サイトコレクション操作	管理者の追加・削除・追加の要求のログを取得できます。	

Microsoft 365 の利用状況の見える化と社内ルールの通知までを自動化
 PC 操作はエンドポイントマネージャーで、M365 の操作の見える化はセキュリティオーディターで実現

現状把握

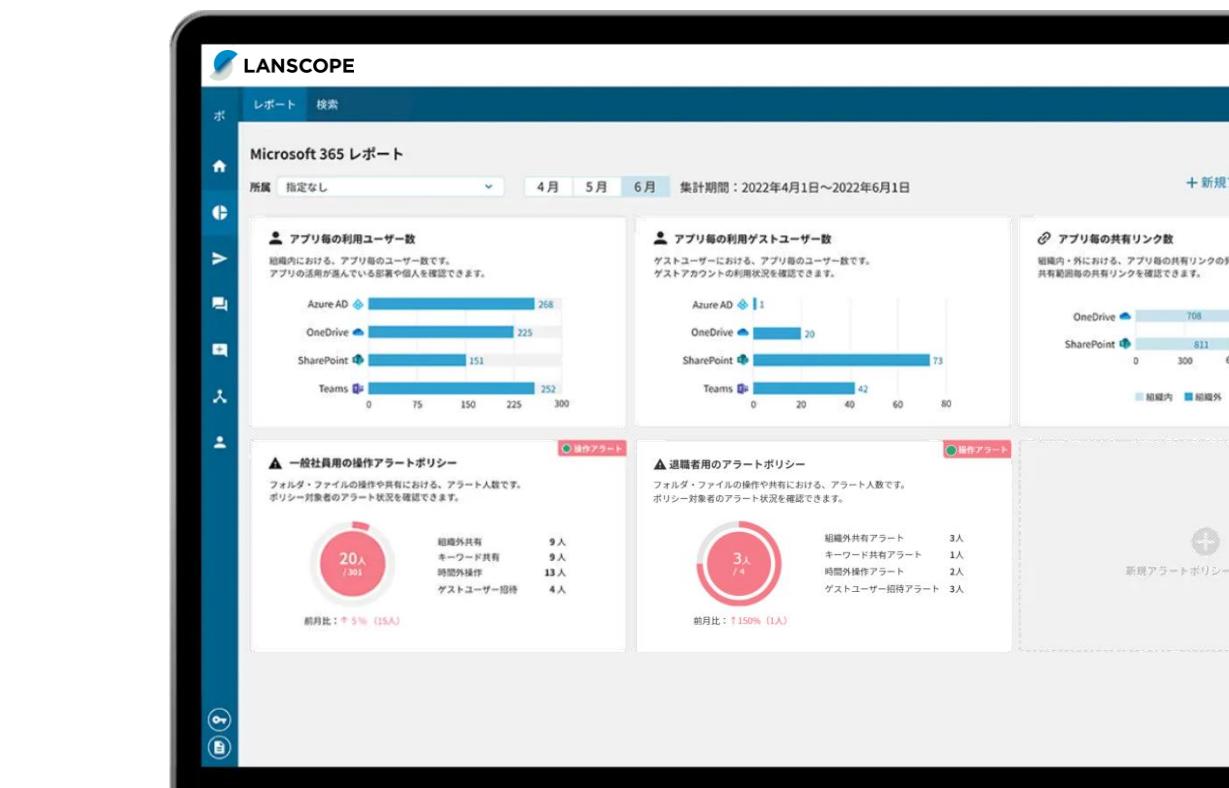
取得したログを分かりやすくレポートに
 利用状況とセキュリティリスクを可視化

アラート通知

通知機能で必要な案内・連絡業務を
 担当者に代わり、ボットが自動通知

監査ログの保存・出力

Microsoft 365 監査ログを2年間保存
 全期間のログを一括出力可能



3. エンドポイントマネージャー クラウド版 各機能のご紹介

機能紹介① 資産管理（ハードウェア・アプリ管理）

機能紹介② 紛失対策・セキュリティ

機能紹介③ Windows・macOS 操作ログ管理

機能紹介④ Apple Business Manager／Android Enterprise

機能紹介⑤ 関連製品



Android 10 以降のデバイスで、インベントリ情報の取得、パスコードポリシー、
リモートワイプなどを利用する場合、Android Enterprise の利用が必須です。

MDM ツール

デバイス情報（ハード・アプリ）の取得

位置情報の取得

リモートロック・ワイプ

セキュリティポリシーの設定

メッセージ・アンケートの通知

+

Apple・Google のプログラム

Apple Business Manager (ABM)

Android Enterprise (AE)

- ✓ MDM と組み合わせて利用する必要がある
- ✓ MDM ツール単体で実現できない、より高度な管理を実現
- ✓ 利用は無償だが、事前準備や利用条件があり、注意が必要

MDM ツール単体でも管理できるものの、ABM・AE を組み合わせて利用するとできる範囲が広がります。

Apple Business Manager とは

Apple Business Manager = 自動デバイス登録 (DEP) + アプリの一括配信 (VPP)

Apple Business Manager とは

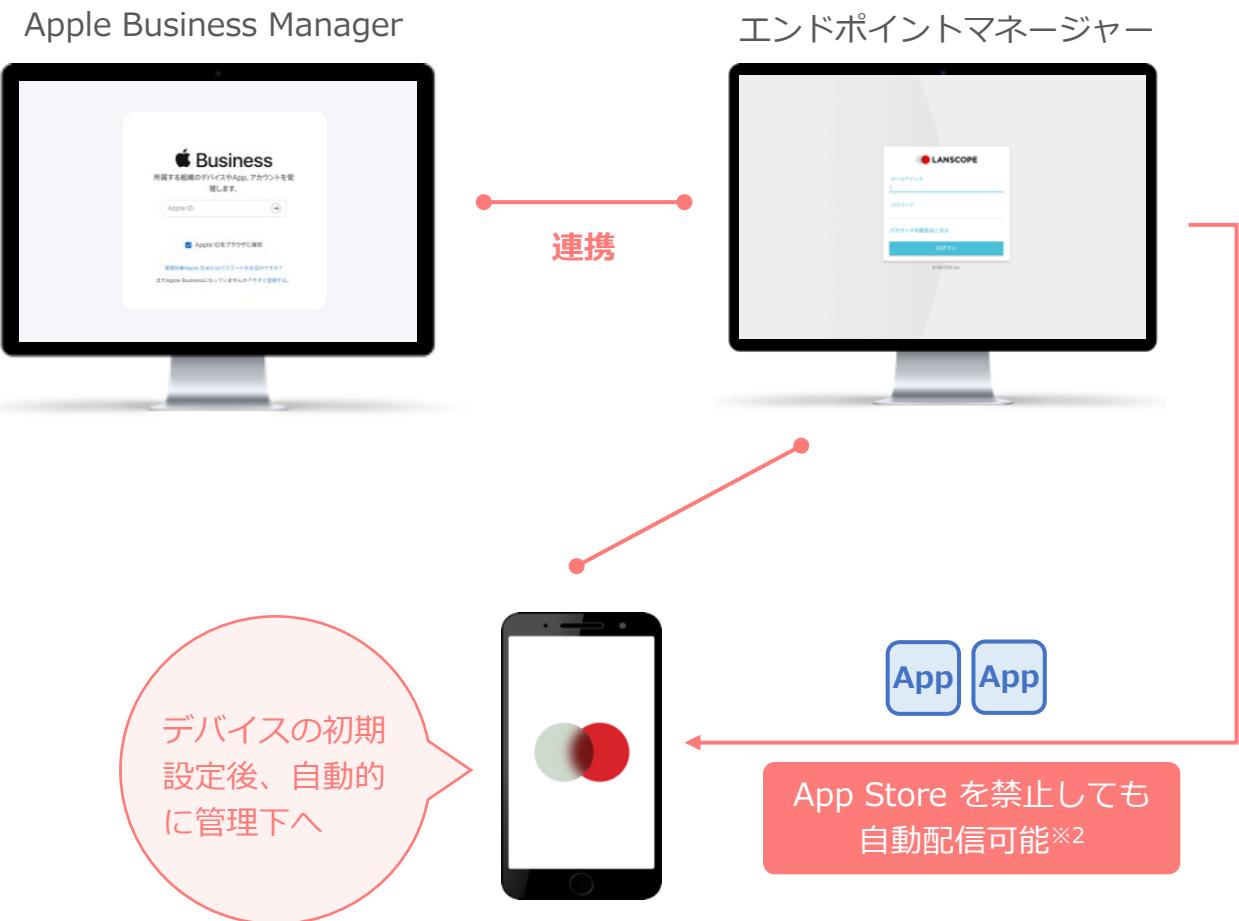
ABM はデバイスを効率的にエンドポイントマネージャーの管理下に置き、アプリの配信やデバイスの利用制御などを実現できる Apple 社が提供するプログラムです。

自動デバイス登録（旧称 DEP）

MDM 構成プロファイルのインストールと監視モードへの適用を自動化します。ABM とエンドポイントマネージャーを連携し、デバイスの初期設定を効率化。

アプリの一括配信（旧称 VPP）※1

Apple ID の設定有無に依存せず、アプリの一括配信が可能。App Store の利用を禁止し、許可したアプリのみ利用を認めるなどの設定が可能です。



※1 オプション機能です。

※2 デバイスを監視モードに設定する必要があります。

Apple Business Manager (DEP・VPP) 機能一覧

主な機能		iOS	macOS	説明
DEP	設定アシスタントのスキップ	○	○	設定アシスタント（初期設定）でスキップする項目を選択できます。
	MDM 構成プロファイルの自動インストール	○	○	デバイスの初期設定の過程で、MDM 構成プロファイルが自動でインストールされます。
	MDM 構成プロファイルの削除禁止	○	○	MDM 構成プロファイルの削除を禁止できます。
	デバイスを監視モードに自動適用	○	—	デバイスを監視モードに自動適用できます。
	監視モード適用時のメリット	紛失モードの利用	○	ロック解除の禁止、位置情報の強制取得など、より強力な紛失対策を実行できます。
		VPP アプリのサイレントインストール	○	VPP アプリとして配信したアプリをデバイスにサイレントインストールできます。
		監視モード専用の構成プロファイル適用	○	監視モードデバイス専用の特定プロファイルを適用できます。
	アカウントの自動作成	—	○	管理者アカウントの自動作成、ユーザーアカウントの設定内容を指定できます。
VPP	アプリの一括配信※	○	—	Apple ID の設定有無に依存しないアプリの配信ができます。



Mac デバイスの監視モードについて

iOS を監視モードに適用する場合、DEP を利用してデバイスをエンドポイントマネージャーの管理下に置く必要があります。一方、macOS 11 (BigSur) 以降の場合は **DEP の利用可否に拘らず、デバイスを管理下に置くことで監視モードが適用**されます（macOS 11未満で監視モードを適用する場合は、DEP の利用が必要です）。

Apple から直接もしくは Apple 正規取扱店と必要な手続きを行った上で購入した iOS・Mac デバイスのみ自動デバイス登録を利用できます。



利用可否はデバイス購入元にお問い合わせください。また、DEP を利用する場合、デバイスの初期設定（アクティベーション）が必要です。そのため、利用中のデバイスの場合は一度初期化し、再アクティベーションが必要です。

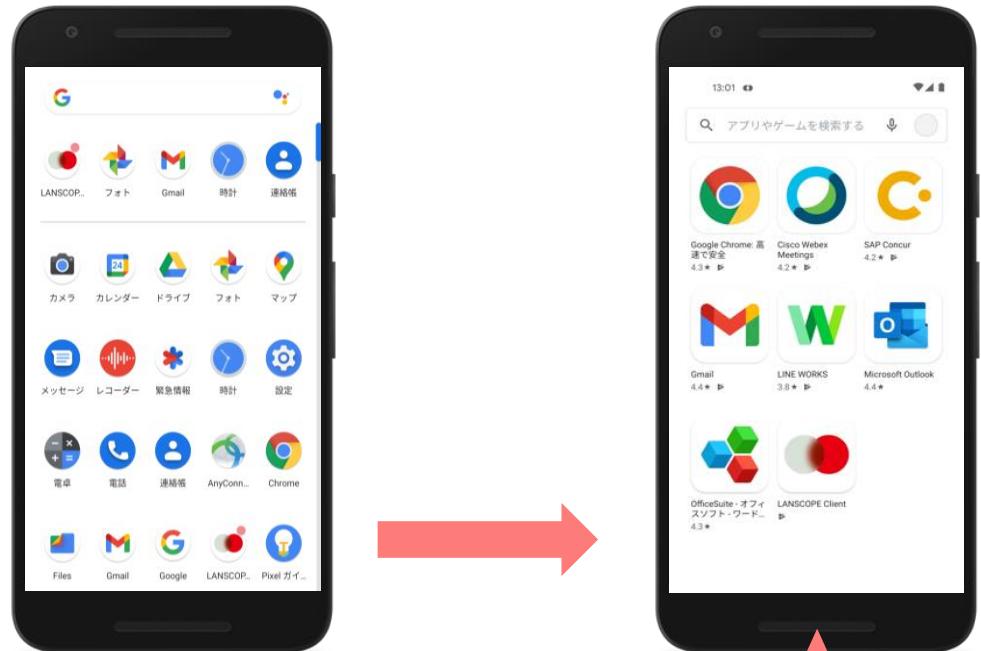
※ オプション機能です。

Android Enterprise とは

Android Enterprise はアプリの配信やデバイスの利用制御など、より高度なデバイス管理を実現できる Google 社が提供するプログラムです。Android Enterprise の利用は無料ですが、事前に利用申請が必要です。

Full Device Management

エンドポイントマネージャーで許可した範囲で、スマホ・タブレット本来の機能を利用してもらいつつ、アプリ管理やセキュリティ対策を実現できます。



キオスクモード

特定のアプリ以外利用できないようにする（Play ストア等、設定アプリ、ホームボタンなども利用不可）など、デバイスの用途を限定できます。



飲食店の注文用タブレットなど
用途がごく限られる場合に利用

Android Enterprise 機能一覧

No	機能	
1	パスワード再設定	デバイスに別のパスワードを上書きで設定できます。
2	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。
3	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。
4	USB接続禁止	ストレージとしての接続やデータ転送を禁止できます。
5	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。
6	Bluetooth機器の接続禁止	Bluetooth機器の接続を禁止できます。
7	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。
8	日付・時刻の変更禁止	日付や時刻の変更を禁止できます。
9	デバッグ機能・セーフブートの利用禁止	デバック機能・セーフブートの利用を禁止できます。
10	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。
11	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。
12	カメラの利用禁止	カメラの利用を禁止できます。
13	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。
14	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。
15	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。
16	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。
17	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。
18	OS アップデートの制御	30日間 OS のアップデートを禁止するなどの設定ができます。

19	アプリ配信	アプリを指定して、デバイスへインストールができます。
20	Play ストア管理	Play ストアに表示するアプリを設定できます。
21	アプリ権限設定	アプリを利用するための権限などを設定できます。
22	アプリの自動更新設定	Play ストアアプリの自動更新を設定できます。
23	提供元不明アプリのインストール禁止	Playストアを経由しないアプリのインストールを禁止できます。
24	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利用を限定できます。



キオスクモードは、Android Enterprise の機能の一つです。キオスクモードの設定を有効にしない場合は、Full Device Management として管理できます。



すでに利用中のデバイスで、Android Enterprise を利用する場合、デバイスを初期化し再度アクティベーションする必要があります。

注意事項：Android Enterprise の利用が必須の機能

Android Enterprise を利用しない場合でも、エンドポイントマネージャー クラウド版にデバイスを登録できますが、**一部機能が利用できません。**そのため、Android デバイスを管理する場合は、**Android Enterprise のご利用を前提に**、管理をご検討ください。

<Android Enterprise の利用が必須の機能>

- シリアルナンバー / IMEI 情報の取得
- リモート操作（パスワードの再設定 / リモートワイプ）の実行
- パスワードポリシーの設定

※ 今後、Google の仕様変更等により、上記機能が増える可能性があります。

3. エンドポイントマネージャー クラウド版 各機能のご紹介

機能紹介① 資産管理（ハードウェア・アプリ管理）

機能紹介② 紛失対策・セキュリティ

機能紹介③ Windows・macOS 操作ログ管理

機能紹介④ Apple Business Manager／Android Enterprise

機能紹介⑤ 関連製品

Microsoft 365 の利用状況を見える化し、ルール違反時には管理者・利用者に通知

Microsoft 365 連携 / エンドポイントマネージャー クラウド版 連携 / FAQ ボット / 定期通知



クラウドサービスと連携し、バックオフィス業務の自動化を支援します。Microsoft 365 連携では、監査ログからルールに従って利用できているかを把握し、ルール違反があった場合は管理者や本人に自動通知します。

また、エンドポイントマネージャー クラウド版と連携し、デバイスを紛失した本人または管理者が連携したビジネスチャット* から位置情報の確認やリモートロック・ワイプを実行できるなど、多彩な機能を実装しています。

Microsoft 365 の利用状況とリスクを見える化

ビジネスチャットと連携して本人と管理者に自動通知

FAQ ボット機能で問い合わせ対応の自動化

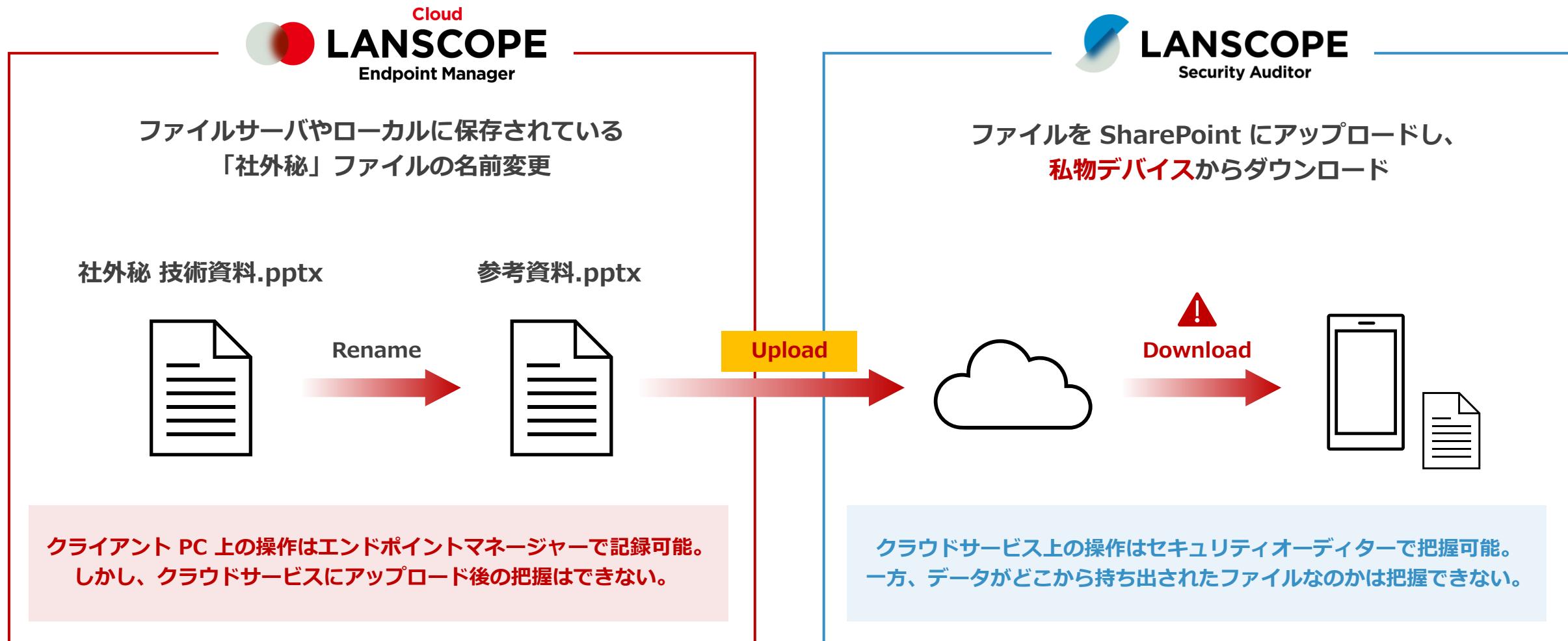
<https://www.syncpit.com/>



Microsoft 365 の監査ログを、誰が見ても分かるよう整形し、管理コンソール上で表示

* 対応しているビジネスチャット … Chatwork / Google Chat / LINE WORKS / Microsoft Teams / Slack

PC の操作は **エンドポイントマネージャー** で、
クラウドサービスの操作は **セキュリティオーディター** で見える化を実現



Appendix

- ・ OS 別 取得可能なデバイス情報
- ・ PC 操作ログ活用シーン
- ・ (Win/macOS) 取得できる操作ログの違い

取得可能なデバイス情報 (iOS)

「デバイス詳細」画面の項目	項目名
管理情報 ※管理コンソール上で編集	デバイス管理名 デバイスタイプ Apple ID 使用者名 使用者の社員コード 使用者の組織名 管理者名 管理者の組織名 管理者の組織コード 使用場所 使用者タイプ 使用状況タイプ 導入日 導入責任者 導入金額 導入タイプ 期限(リース/償却) 月額費用 購入先 補償内容 前回棚卸し実施日 前回棚卸し実施者 前回棚卸し実施結果 任意項目1~20
デバイスグループ	デバイスグループ
デバイス情報	OSバージョン 監視モード 位置情報サービス LANSCOPE Client 位置情報利用許可 正確な位置情報 紛失モード iPhoneを探す おやすみモード アクティベーションロック iCloudバックアップ 最新iCloudバックアップ日時 iTunesアカウント状態 iTunesStoreIdHash デバイス名 モデル名 シリアル番号 UDID ストレージ使用容量 通信方式 IMEI MEID モデムファームウェア ExchangeデバイスID 電池残量
ネットワーク	電話番号 加入キャリア 現在のキャリア キャリア設定バージョン MACアドレス(Wi-Fi) MACアドレス(Bluetooth) ICCID インターネット共有 ローミング データローミング 音声通話ローミング カントリーコード ネットワークコード SIMカントリーコード SIMネットワークコード 現在のカントリーコード 現在のネットワークコード
セキュリティ	Jailbreak パスコードロック パスコードポリシー(プロファイル) パスコード要求までの猶予時間(秒) ハードウェアの暗号化方式
インストールアプリ	アプリ名 バージョン デベロッパー カテゴリー アプリサイズ
プロファイル	プロファイル名 作成者 アプリケーションID 概要
位置情報	移動履歴(地図表示・一覧表示)
操作ログ	時刻 分類 利用時間 内容
アラート	アラート(トリガー)名 アラートレベル
リモート操作	実行履歴(設定日時・実行者・内容・状態・実行日時・メッセージ・電話番号・詳細)
クライアント	MDM構成プロファイルインストール日時 LANSCOPE Clientインストール日時 LANSCOPEクライアント最終稼働日時(MDM構成プロファイル最終通信日時 LANSCOPE Client最終通信日時) LANSCOPE Clientバージョン

取得可能なデバイス情報 (Android)

「デバイス詳細」画面の項目	項目名
管理情報 ※管理コンソール上で編集	デバイス管理名 デバイスタイプ Apple ID 使用者名 使用者の社員コード 使用者の組織名 管理者名 管理者の組織名 管理者の組織コード 使用場所 使用者タイプ 使用状況タイプ 導入日 導入責任者 導入金額 導入タイプ 期限(リース/償却) 月額費用 購入先 補償内容 前回棚卸し実施日 前回棚卸し実施者 前回棚卸し実施結果 任意項目1~20
デバイスグループ	デバイスグループ
デバイス情報	OSバージョン CPU名 CPU周波数 メモリ アカウントのメールアドレス1~3 Android Enterpriseデバイス タイムゾーン 国コード 製品名 製造元 ホスト名 モデル名 シリアル番号 ビルド番号 内部ストレージ使用容量 外部ストレージ使用容量 IMEI 基盤名 ハードウェア名 ブランド名
ネットワーク	電話番号 MACアドレス (Wi-Fi) Wi-Fi状態 IPアドレス デフォルトゲートウェイ サブネットマスク DHCP IPアドレス サーバーアドレス DNSサーバー SSID ネットワーク認証種別 Bluetoothアダプタ名 MACアドレス (Bluetooth) SIMのシリアル番号 SIMの状態 SIMの国コード 加入キャリア 現在のキャリア
セキュリティ	root化 パスワードポリシー USBデバッグ
インストールアプリ	アプリ名 バージョン デベロッパー カテゴリー インストール日
位置情報	移動履歴 (地図表示・一覧表示)
操作ログ	時刻 分類 利用時間 内容 詳細1 詳細2
アラート	アラート(トリガー)名 アラートレベル
リモート操作	実行履歴 (設定日時・実行者・内容・状態・実行日時・詳細)
Android Enterprise	適用されているポリシー 登録日時 ポリシー適用日時 管理モード
クライアント	LANSCOPE クライアントインストール日時 LANSCOPE クライアントバージョン LANSCOPE クライアント最終稼働日時 LANSCOPE クライアントの設定 (デバイス管理者・使用履歴へのアクセス)

取得可能なデバイス情報（Windows）

「デバイス詳細」画面の項目	項目名
管理情報 ※管理コンソール上で編集	デバイス管理名 デバイスタイプ Apple ID 使用者名 使用者の社員コード 使用者の組織名 管理者名 管理者の組織名 管理者の組織コード 使用場所 使用者タイプ 使用状況タイプ 導入日 導入責任者 導入金額 導入タイプ 期限（リース／償却） 月額費用 購入先 補償内容 前回棚卸し実施日 前回棚卸し実施者 前回棚卸し実施結果 任意項目1～20
デバイスグループ	デバイスグループ
デバイス情報	OS バージョン OS アーキテクチャ Windows バージョン CPU 名 CPU 周波数 メモリ ドメイン・ワークグループ名 ログオンユーザー名 ログオンユーザー SID コンピューター名 NetBIOS 名 デバイス名 製品名 製造元 シリアル番号 モデル名 モデムファームウェア IMEI システムドライブ ファイルシステム ポリューム名 国番号 ストレージ容量 プロセッサ数 CPU コア数 Drive数 フルネーム（表示名） Windows プロダクト ID モデム SCSI 機器 BIOS バージョン Windows サービスパック Internet Explorerバージョン IE サービスパック
ネットワーク	Wi-Fi状態 Bluetooth状態 NIC情報（NIC名・NICの種別・MACアドレス・IPアドレス・サブネットマスク・デフォルトゲートウェイ・DNSサーバー） 電話番号 現在のキャリア SIMの状態 ICCID
セキュリティ	ファイアウォール状態 Windowsアップデート アンチウィルス状態 アンチウィルス更新ステータス リモートワイプ実行可否 BitLocker回復キー Defender パターンバージョン Defender エンジンバージョン Defender バージョン CylancePROTECT バージョン CylancePROTECT ポリシー種別 Deep Instinct バージョン Deep Instinct 連携設定
インストールアプリ	アプリ名 バージョン デベロッパー カテゴリー インストール日
Microsoft Office	Microsoft Office 情報一覧
位置情報	移動履歴（地図表示・一覧表示）
アラート	アラート（トリガー）名 アラートレベル
リモート操作	実行履歴（設定日時・実行者・内容・状態・実行日時・詳細）
クライアント	LANSCOPE クライアントインストール日時 LANSCOPE クライアントバージョン LANSCOPE クライアント最終稼働日時

取得可能なデバイス情報 (macOS)

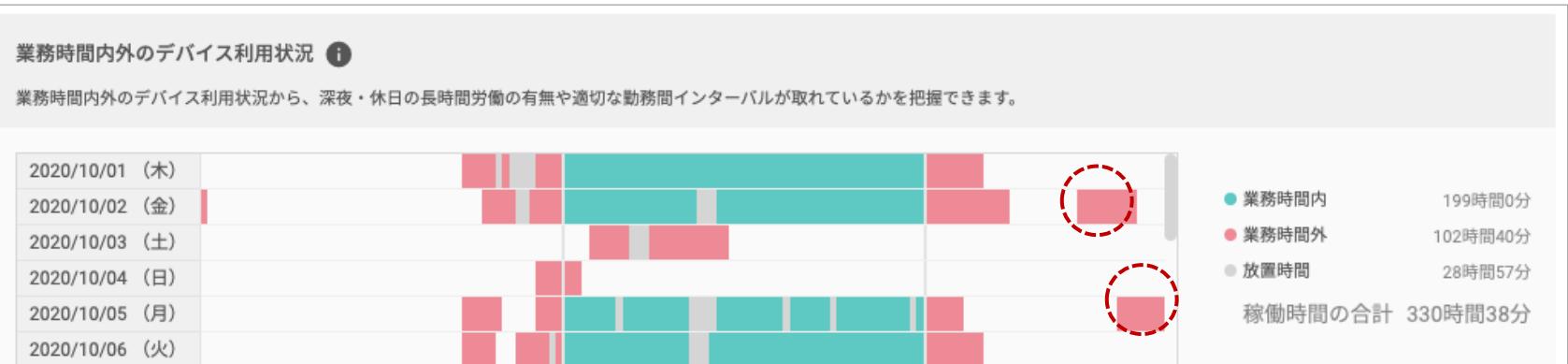
「デバイス詳細」画面の項目	項目名
管理情報 ※管理コンソール上で編集	デバイス管理名 デバイスタイプ Apple ID 使用者名 使用者の社員コード 使用者の組織名 管理者名 管理者の組織名 管理者の組織コード 使用場所 使用者タイプ 使用状況タイプ 導入日 導入責任者 導入金額 導入タイプ 期限(リース/償却) 月額費用 購入先 補償内容 前回棚卸し実施日 前回棚卸し実施者 前回棚卸し実施結果 任意項目1~20
デバイスグループ	デバイスグループ
デバイス情報	OSバージョン CPU名 メモリ ドメイン・ワークグループ名 ログオンユーザー名 iTunesアカウント状態 iTunesStoreIdHash デバイス名 製品名 製造元 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 CPUコア数 BIOSバージョン
ネットワーク	MACアドレス(Wi-Fi) MACアドレス(イーサネット) MACアドレス(Bluetooth) NIC情報
セキュリティ	ファイアウォール状態 System Integrity Protection FileVault パーソナル復旧キー設定 パーソナル復旧キー 所属団体の復旧キー設定
インストールアプリ	アプリ名 バージョン デベロッパー カテゴリー アプリサイズ
プロファイル	プロファイル名 作成者 アプリケーションID 概要
アラート	アラート(トリガー)名 アラートレベル
リモート操作	実行履歴(設定日時・実行者・内容・状態・実行日時・詳細)
クライアント	MDM構成プロファイルインストール日時 LANSCOPE Clientインストール日時 LANSCOPEクライアント最終稼働日時(MDM構成プロファイル最終通信日時 LANSCOPE Client最終通信日時) LANSCOPE Clientバージョン

操作ログ活用シーン① サービス残業防止



申請外の残業を行っていないか？成果を上げるために無理をしていないか？「業務時間内外のデバイス利用状況」で一目で把握

働き方改革関連法の施行で、残業時間の罰則付き上限規制の適用、また従業員の労働時間を把握・記録することが義務化されました。一方で、テレワークの普及により仕事とプライベートの区切りを付けることが難しく、成果を上げるために申請外の残業をしてしまう人もいるかもしれません。上司も同僚もお互いの働く姿が見えづらくなっています。エンドポイントマネージャー クラウド版では「業務時間内外のデバイス利用状況」レポートで、一目で業務時間外の操作ログを把握。申請外の残業を行っている従業員に、事情を聞き、タスクの再分配や働き方の見直しなどのきっかけを作ります。



先週金曜日と今週の月曜日…遅くまでありがとうございました。
でも申請時間外の労働は会社の違法行為になってしまい可能性もあるので行わないようにしよう。

すみません、納期を優先してしまいました。
これからは相談するようにします。

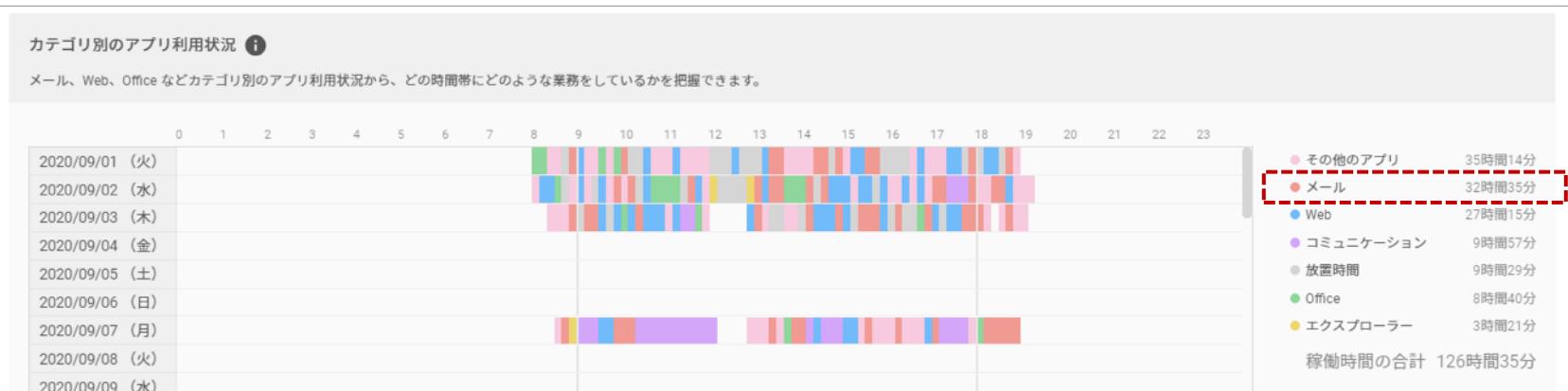


操作ログ活用シーン② シャローワーク対策



「シャローワーク」に要注意！「カテゴリ別のアプリ利用状況」で改善！

人間が集中状態に入るまで、一般的に20分程度かかると言われています。その間に人に話しかけられたり、電話がかかってきたりすると、集中が途切れてしまいます。特に深く考えなくてもできるような補助的な仕事「シャローワーク」の状態が続くと、集中して時間をかけて考える必要のある仕事をやり遂げることができません。個人レポートの「カテゴリ別のアプリ利用状況」では 10分刻みで、その間に最もよく利用されたカテゴリのアプリを色別に表現します。頻繁に色が変わっている場合、集中して一つの仕事に取り組めていないかもしれません。なかなか自覚することが難しい観点を、上司・メンバー間の 1on1 MTG などで気付き・改善活動に活用できます。



先週は頻繁にメール対応しているみたいだけど大丈夫？



言われてみれば…確かに多かったですね。



メール対応をまとめて行う時間など、業務の効率化も行おう！



従業員の健康も気遣い、適切な休憩も大切！

同じ姿勢を長時間続けたり、ディスプレイの文字を長時間見続けることは健康上良くないため、1時間に10分程度は休憩を取るよう厚生労働省がガイドラインで提示しています。レポート画面で従業員が適切な休憩を取得できているか？全体の把握と、デバイス毎にデバイスの放置＝適切な休憩を取得できているか？を把握できます。

※ 1時間に10分程度休憩する＝放置時間は約16%になります。15%前後を目安に見てみましょう。

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。

● 放置時間
16%

前月比: ↓1%

● 長期間未稼働デバイス
Click!!

LANSCOPE リスト レシピ モニター レポート ログ ルール

ログアラート 利用状況 Windows アップデート

く デバイスの放置時間

ネットワーク全体 集計期間: 2023/06/01 ~ 2023/06/15 2023/04 | 2023/05 | 2023/06

● 放置時間
16%

前月比: ↓1%

配下のグループ

エクスポート キーワード検索 (例: 営業 iPhone)

管理No.	デバイス管理名	使用者名	割合	時間	デバイスグループ
24	Surface 3_0000000048	MO花子	38%	72時間0分0秒	営業2課
26	Surface 3_0000000050	MO一郎	9%	25時間16分58秒	営業2課
23	Surface 3_0000000047	MO三郎	2%	23時間24分35秒	営業2課
82	MacBook_00000085	MO五郎	8%	23時間24分35秒	サポート2課
25	Surface 3_0000000049	MO二郎	8%	19時間7分52秒	営業2課
29	ElitePad_0000000052	共有タブレット	9%	19時間7分52秒	システム部
55	Surface Pro 3_0000000053	検証用A	6%	19時間7分52秒	検証用

MO 三郎さん、ちゃんと休憩してるのかな？
次の 1on1 MTG で確認してみよう・・

操作ログ活用シーン④ 生産性向上

👉 アプリ活用・Webアクセスランキングもチームの生産性向上のポイントに？

働き方の傾向だけではなく、具体的にどんなアプリを利用しているか、どんなWebサイトにアクセスしているかをランキング形式で確認できます。例えば最近は、オンラインで商談することも多くなっているので、営業メンバーであれば、オンライン商談用のアプリが上位に来ているか？来ていないメンバーがいれば、お客様との商談数が少ないのではないか？などアプリの利用状況から改善のきっかけを作ることができるかもしれません。

またよく利用・アクセスされているアプリやWebサイトで、業務上活用できるものがあれば、「MO一郎さん、こういうサイトで情報収集しているみたいだよ」というイメージで他のメンバーにも共有するなど、操作ログを活用できます。

Windows Surface 3_0000000050 - デバイス詳細

管理No. 26

デバイスグループ: 営業2課
使用者名: MO一郎
電話番号:
ログオンユーザー名: ichiro.mo
最終稼働: 22日前

2021/03 2021/04 2021/05 集計期間: 2021/05/01 ~ 2021/05/27
2021/05/09 (日)

アプリ利用時間ランキング
アプリの利用時間集計から、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。

アプリ名	時間
Zoom.exe	54時間27分
chrome.exe	46時間36分
POWERPNT.EXE	14時間32分
Bubbles.scr	7時間40分
EXCEL.EXE	5時間25分
notepad.exe	3時間13分
explorer.exe	0時間53分
LogonUI.exe	0時間38分
OUTLOOK.EXE	0時間28分
ShellExperienceHost...	0時間26分
ApplicationFrameHost...	0時間25分
mstsc.exe	0時間14分
mspaint.exe	0時間11分
SearchUI.exe	0時間7分
vpnui.exe	0時間5分
Everything.exe	0時間5分

Webアクセス時間ランキング
Webのアクセス時間集計から、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。

サイト名	時間
kcw.kddi.ne.jp	15時間25分
outlook.office.com	13時間37分
motex.cybozu.com	3時間59分
motex-mark.backlog...	2時間57分
app.diagrams.net	2時間28分
projects.invisionapp.c...	1時間29分
motexjp-my.sharepoint...	1時間19分
doda.jp	1時間12分
www.r-agent.com	1時間10分
mail.google.com	1時間10分
career.leveltech.jp	1時間9分
www.e-fsiken.com	1時間8分
app.innopom.com	1時間8分
techarttarget.itmedia.co.jp	1時間8分
drive.google.com	1時間8分
mynavi-agent.jp	1時間13分



Webサイトのアクセス上位に「●●●.jp」というサイトがあるけれど、どんなサイトなの？



毎朝始業前だったり、休憩がてら情報収集しているサイトです。



そういう取り組みしてるんだね。
他のメンバーにも共有しておいた方が良い内容があれば、ぜひ共有もお願いします！

Windows・macOS 取得できる操作ログの比較

	Windows	macOS	備考
ログオンログオフログ	○	○	
周辺機器接続ログ	○	○	
ウィンドウタイトルログ	○	○	
Webアクセスログ	○	△	macOS は Web サイト閲覧ログのみ取得可能です。
ファイル操作ログ	○	○	
プリントログ	○	○	
アプリ禁止ログ	○	×	
通信機器接続ログ	○	×	
アプリ稼働ログ	○	×	外部脅威調査オプションの導入が必要です。
アプリ通信ログ	○	×	外部脅威調査オプションの導入が必要です。
脅威検知ログ	○	×	CylancePROTECT または Deep Instinct の導入と連携が必要です。



製品に関するお問い合わせ

■ 営業本部

大阪本社 06-6308-8980

東京本部 03-3455-1811

名古屋支店 052-253-7346

九州営業所 092-419-2390

E-mail sales@motex.co.jp

ご導入後の製品利用に関するお問い合わせ

サポートセンター

0120-968995 (携帯・PHSからは06-6308-8981)

お電話受付時間

9:30~12:00/13:00~17:30 (平日、祝祭日除く)

Email お問い合わせ

support@motex.co.jp

- ・記載の会社名および製品名・サービス名は、各社の商標または登録商標です。
- ・製品の仕様・サービスの内容は予告なく変更させていただく場合があります。
- ・MOTEX はエムオーテックス株式会社の略称です。