Cloud LANSCOPE Endpoint Manager

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

目次

※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 吉朗
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

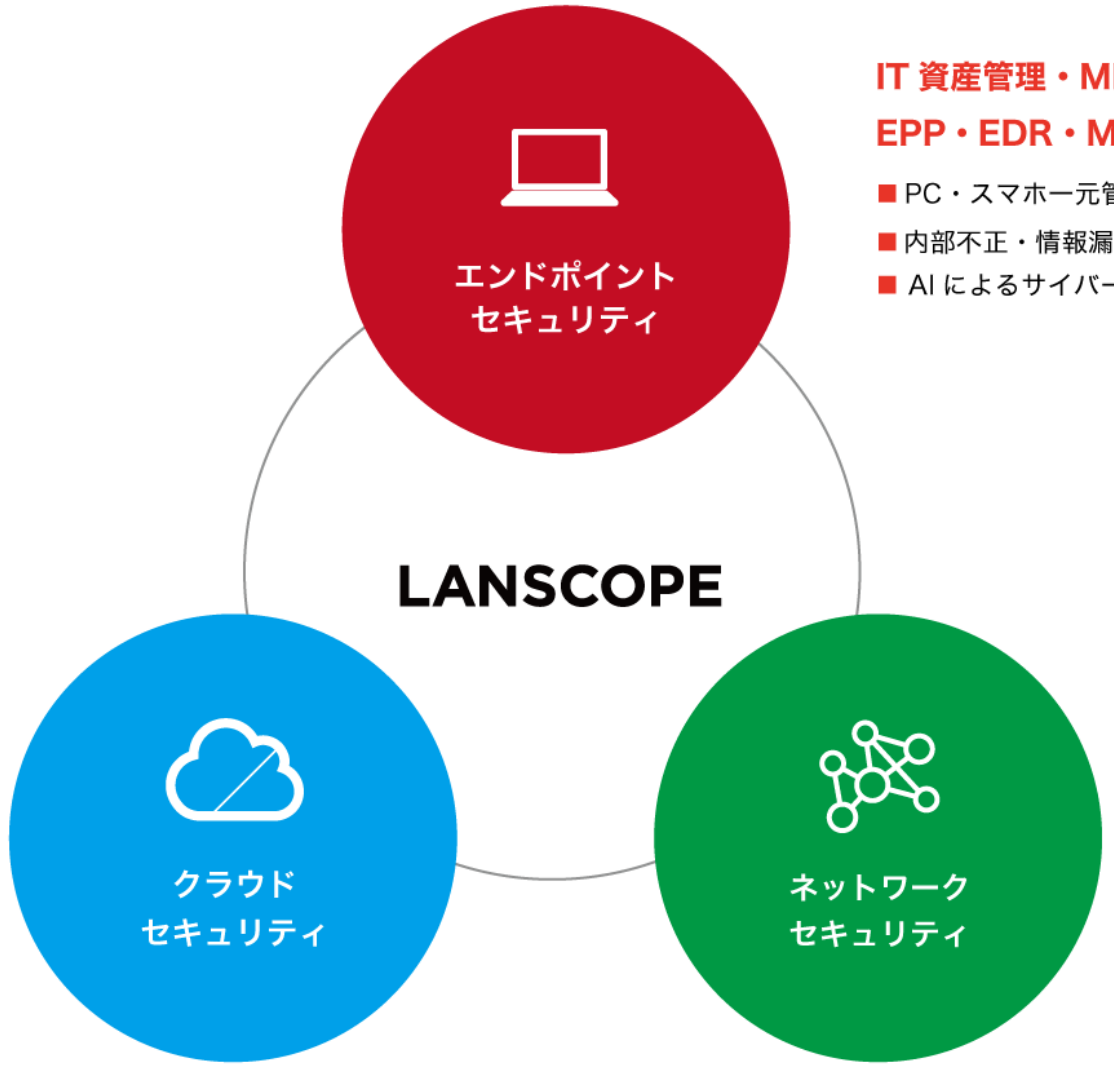
拠点

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 名古屋インターシティ 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

OSAKA, KANSAI, JAPAN EXPO 2025

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。

MOTEX が提供する 3つの セキュリティソリューション



IT 資産管理・MDM
EPP・EDR・MDR

- PC・スマホ一元管理
- 内部不正・情報漏洩対策
- AI によるサイバー攻撃対策

SaaS・IaaS の設定診断
Microsoft 365 監査ログ管理

- 国家資格取得者による設定診断
- 業界トップクラスの診断項目数
- 監査ログの取得・アラート管理

脆弱性診断・AI ネットワーク脅威検知
サプライチェーンリスク評価

- AI によるネットワーク監視・遮断
- Web・ネットワークの脆弱性診断
- 外部公開資産の洗い出し・リスク評価

「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

クラウドセキュリティ

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

DARKTRACE

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

Panorays

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

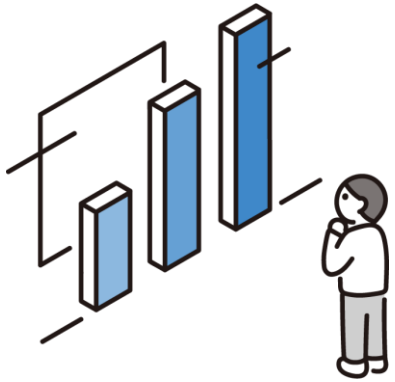
こんな方におすすめ

- 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

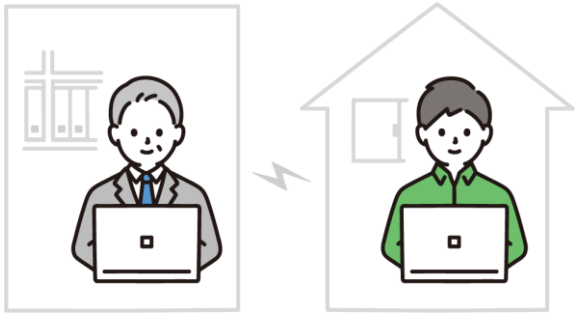
クラウドサービスならではの特長を活かしてデバイス管理の課題解決を支援！

IT 資産管理ツールを クラウド化したい



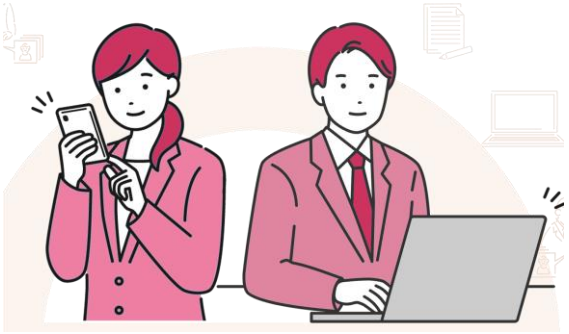
社内のシステムや業務用ソフトのクラウド化を進めており、IT 資産管理ツールもクラウドに移行したい。

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、スマホ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

ITreview

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

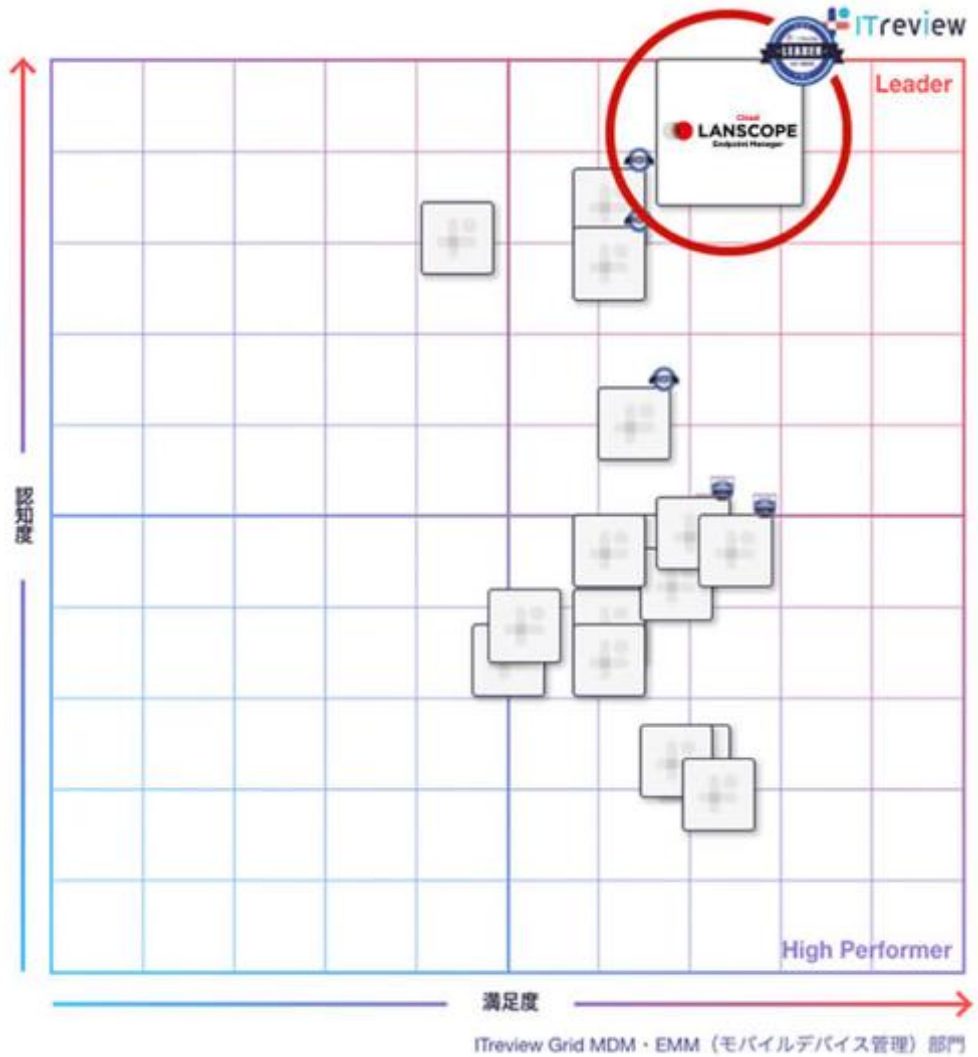
ITreview

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



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

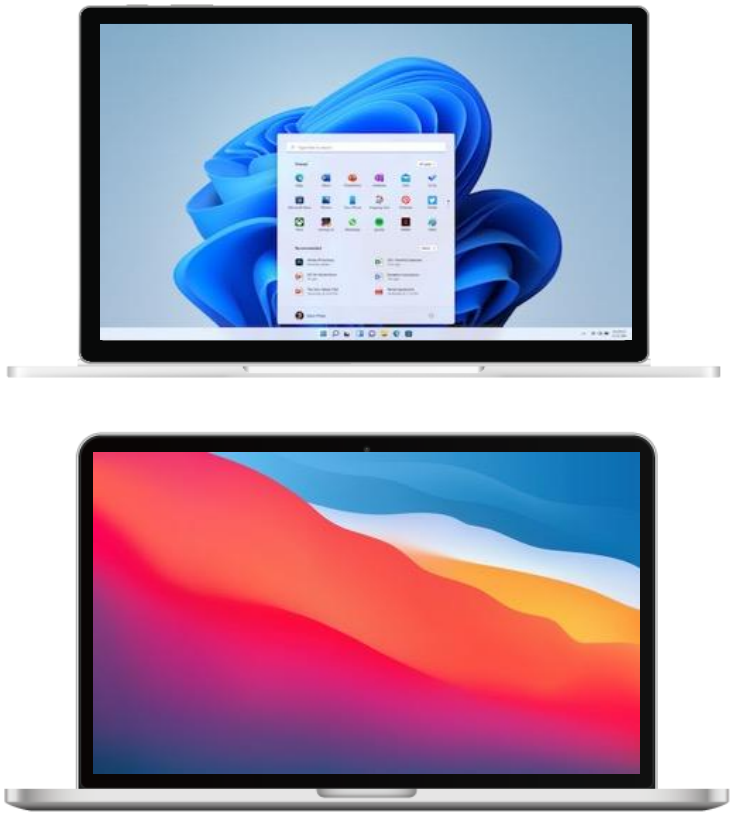
デバイスのハードウェア情報／設定情報を自動取得し、IT 資産台帳として活用できます。自動取得できない項目は任意項目として管理できるほか、プリンターやルーターなどエージェントがインストールできない機器もまとめて管理できます。

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。



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）
共通	OS 対応	i A W m	W m	i A W m	i A W m	i A W m
PC 管理	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	○	×	○	○	○
	位置情報の取得	○	×	○	○	○
iOS	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

aws partner network | service ready

bsi ISO/IEC 27017 Cloud Security Management CERTIFIED

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。

* 株式会社テクノ・システム・リサーチ「PC 資産・PC セキュリティSaaS市場 メーカーシェア 2022年 ブランド別市場シェア」分野

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。

ユーグレナ

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

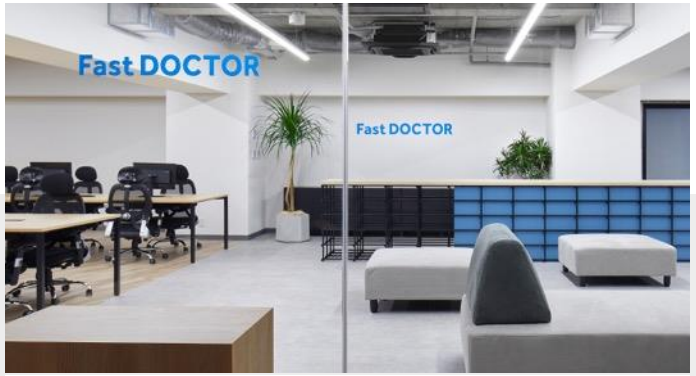
サーバーメンテナンスを考えずに長期的・安定的にログが保存できること、機能の充実や使いやすさに加え、PC・スマホの一元管理が可能であることも、エンドポイントマネージャー導入の決め手になった。

株式会社東京カンテイ

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。

Fast DOCTOR



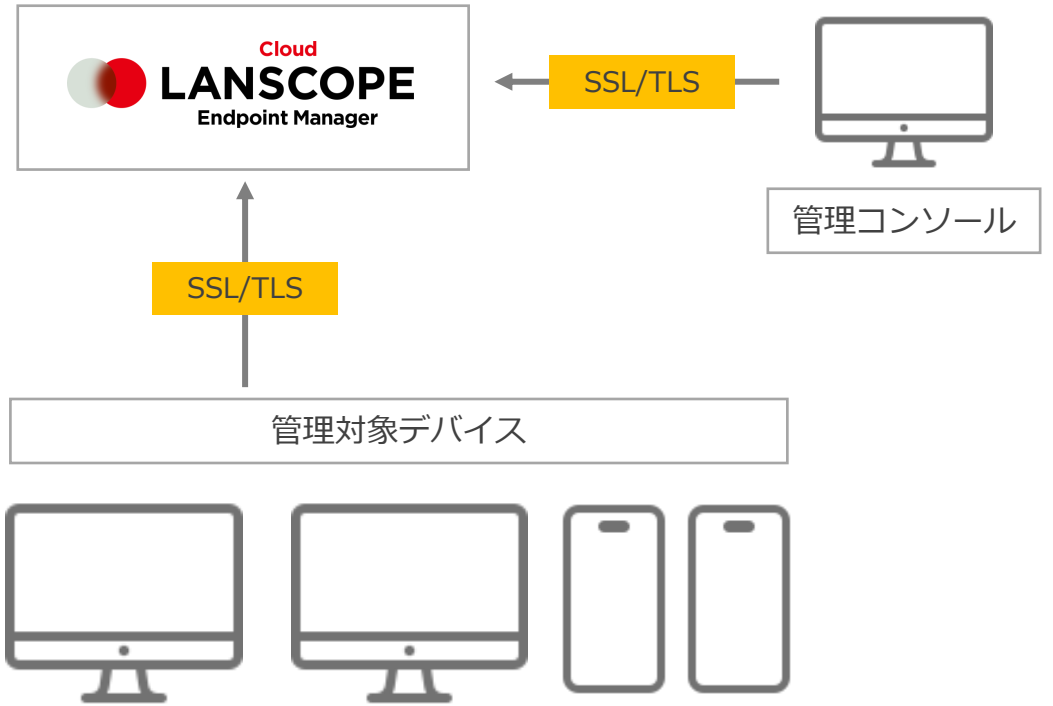
OS のカバー領域の広さと
コストパフォーマンスの高さが決め手

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。

エンドポイントマネージャー クラウド版の運用体制

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

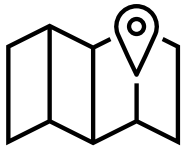
国際規格 ISO/IEC 27001（ISMS）認証、クラウドサービスの提供や利用に対して適用される国際規格 ISO 27017 認証を取得し、厳格なセキュリティ基準に則って、エンドポイントマネージャー クラウド版の運用を行っています。

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 ファンデーショナ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。

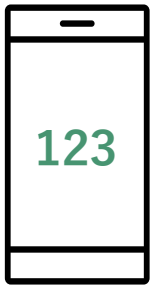


IP アドレス制限

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
●	●	ー	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。	○	○	○	○
●	●	ー	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。	○	○	○	○
●	●	ー	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。	○	○	○	○
●	●	ー	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	○	○
●	ー *2	ー	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。	○	ー	ー	ー
●	●	ー	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	○	○	×
●	●	ー	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。	○	○	○	×
●	●	ー	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。	ー	ー	○	×
●	●	ー	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。	ー	ー	○	ー
●	●	ー	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。	ー	ー	○	○
●	●	ー	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	○	×
ー	●	●	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。	ー	ー	○	○
ー	●	●	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。	ー	ー	○	○
ー	●	●	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
ー	●	●	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。	ー	ー	○	○
ー	●	●	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	○
●	●	ー	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。	○	○	○	×
●	ー *2	ー	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	○	ー	ー
●	ー *2	ー	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。	○	ー	ー	○ *11
●	ー *2	ー	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。	ー	○	ー	ー
●	●	●	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			
	ライトA	ベーシック	ライトB	機能名	概要	i	A	w	m
地図利用料*1	●	●	ー	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	●	●	ー	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。	○	ー	ー	×
外部脅威調査	ー	●	●	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。	ー	ー	○	ー
				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。	ー	ー	○	ー
ログ運用	ー	●	●	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。	ー	ー	○	○
				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。	ー	ー	○	○
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。	×	×	○	×

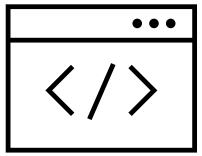
*1 プラン I 専用のオプションです。プラン Ⅱ・Ⅲ で購入する場合は、利用料金内に含まれています。
*2 ログ運用オプションを申し込まない場合、ログの保存期間は過去2年分となります。
*3 導入前に体験版による検証をお願いします。

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） 月額利用料
必須購入	初期費用	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
オプション	24/365紛失サポート	150円/台
	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	

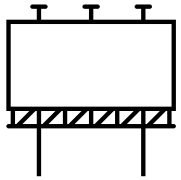
*1 プランⅢの場合、ライトA またはライトBを解約し、ベーシックを新規で申込みいただきます。その際、初期費用（30,000円/契約）は必要ありません。また環境引き継ぎが可能です。ライトA → ライトB、ライトB → ライト A への移行は不可、ベーシックからライトへのダウングレードはできません。
*2 ライトB のみ購入している場合は、購入できません。ライトA またはベーシックの購入が必要です。
*3 ライトA のみ購入している場合は、購入できません。ライトB またはベーシックの購入が必要です。

主なサポート内容（ライセンス利用料の中でご利用いただけます。別途費用は発生しません。）



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

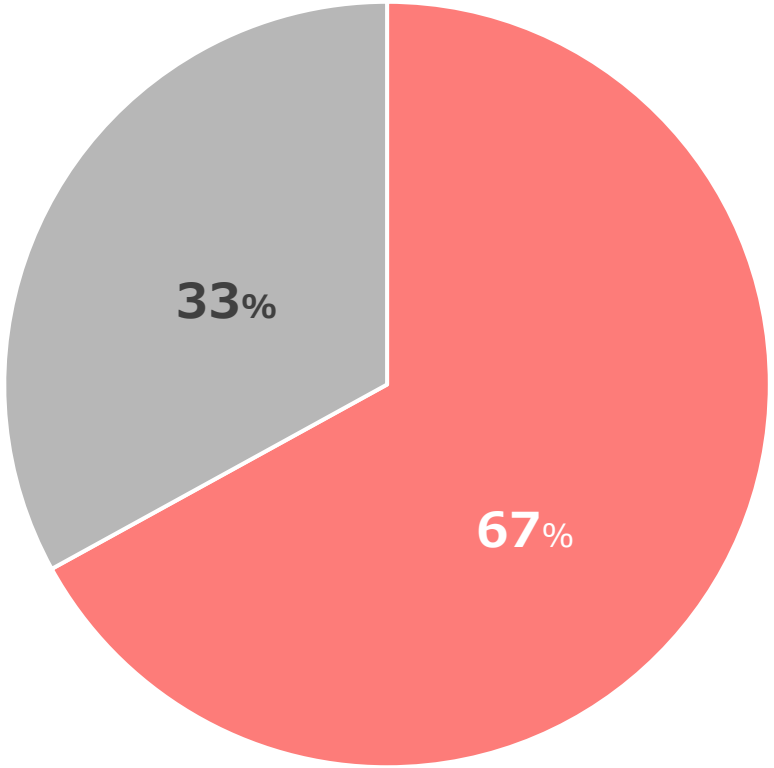
エンドポイントマネージャー クラウド版をご利用いただいている中で発生した疑問や質問に対して、電話やメール、チャットによるサポート対応を行っています。

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

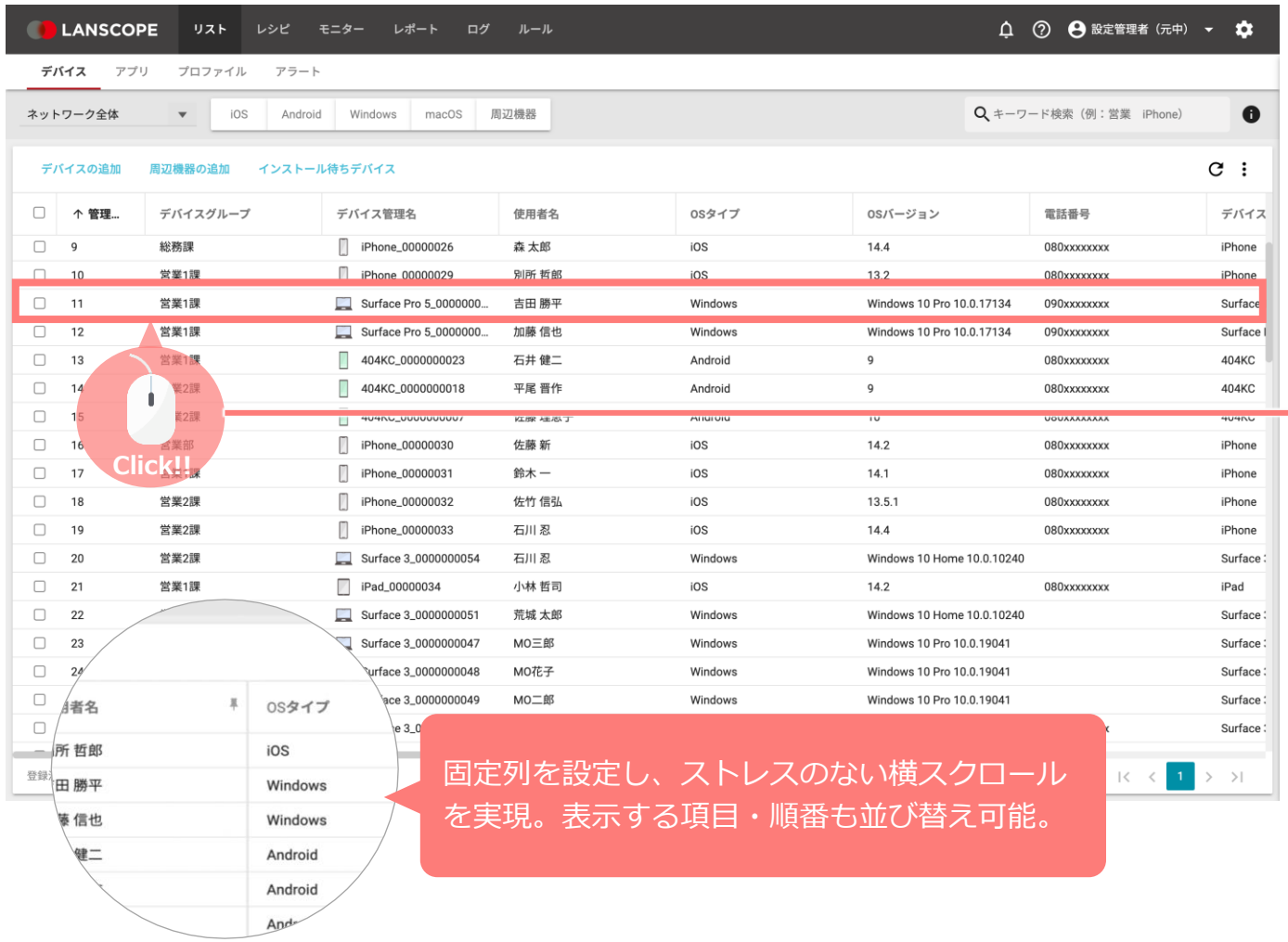
機能紹介③ Windows・macOS 操作ログ管理

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

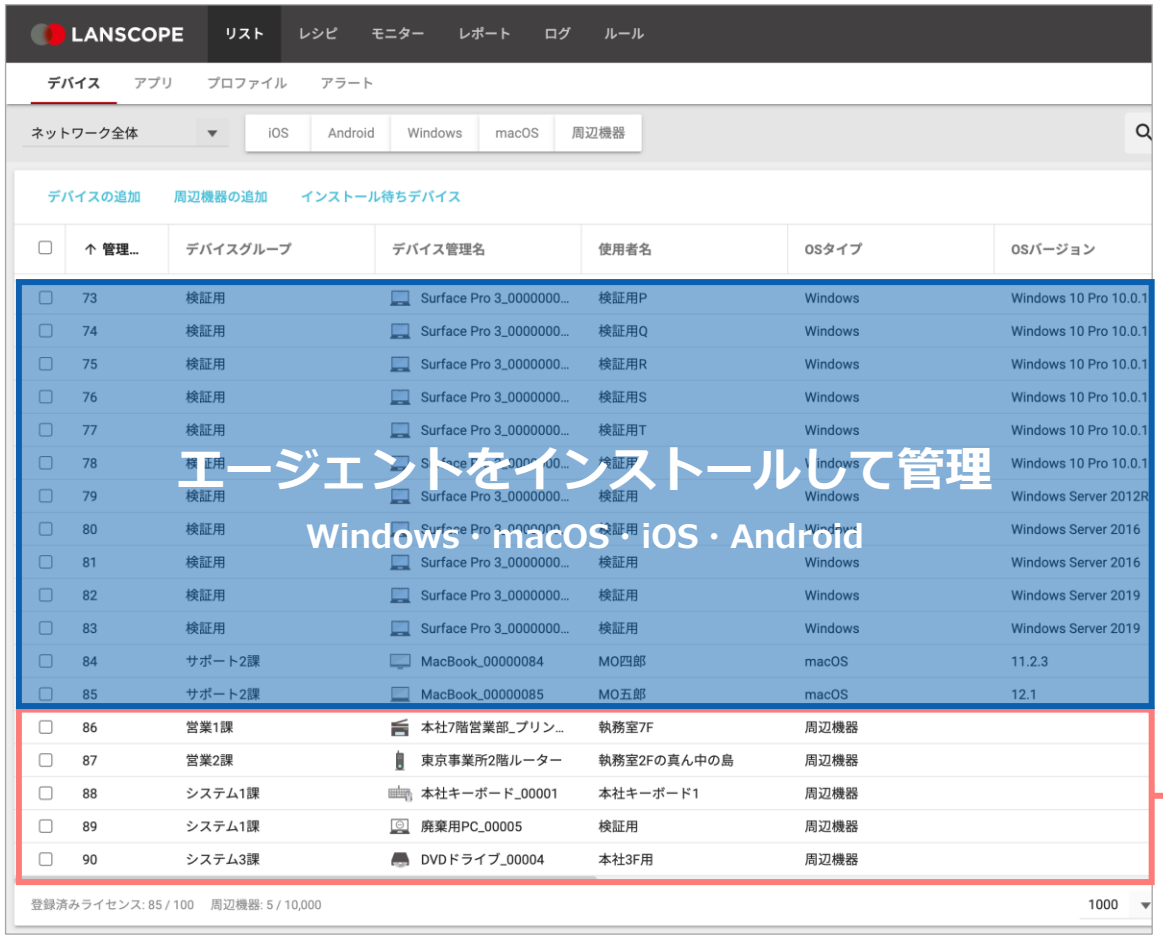
デバイスを特定し、1Click で詳細の資産情報の確認が可能。自動取得できない項目は、任意項目として管理できます。



i A W m
ライトA ライトB
ベーシック

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



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！

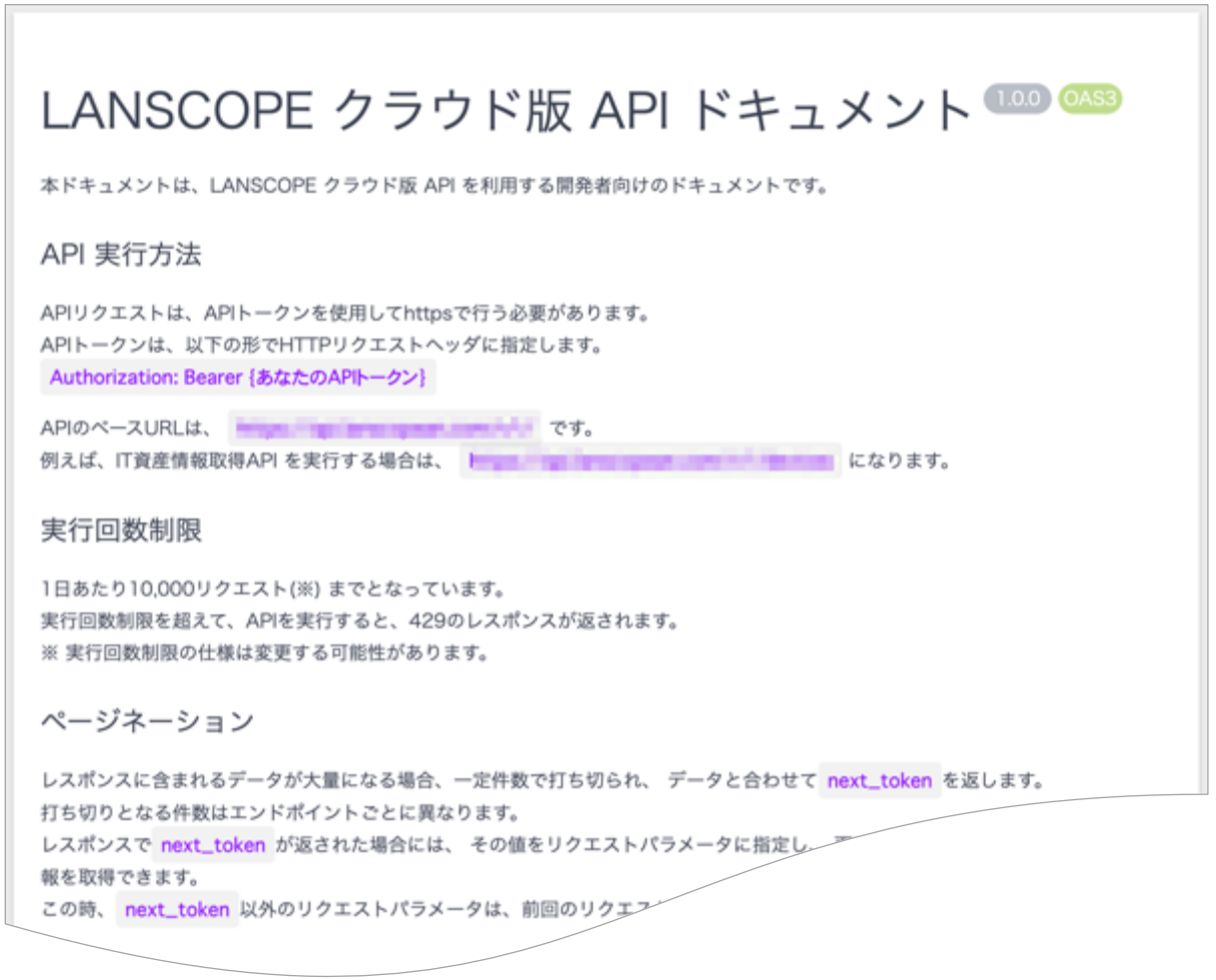
ハードウェア・インストールアプリ情報取得の API を公開

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



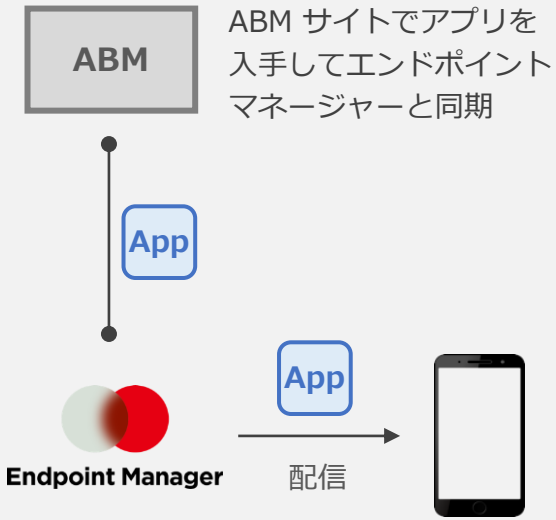
i A W m
ライトA ライトB
ベーシック

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

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）。

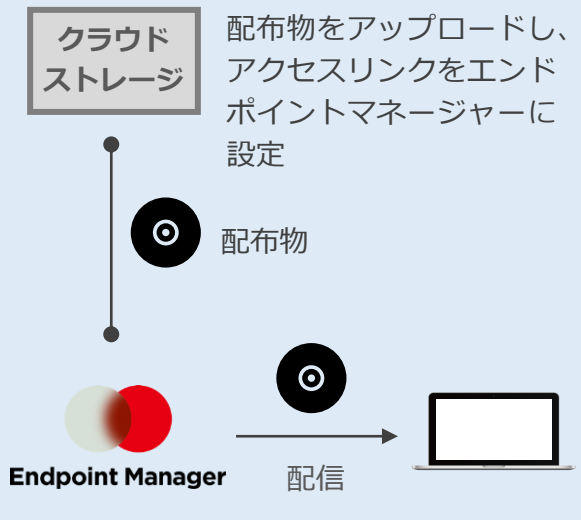


Android

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。

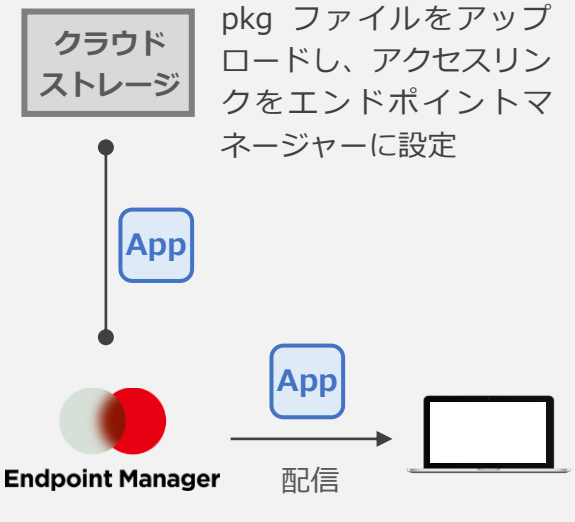
Windows

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。



macOS

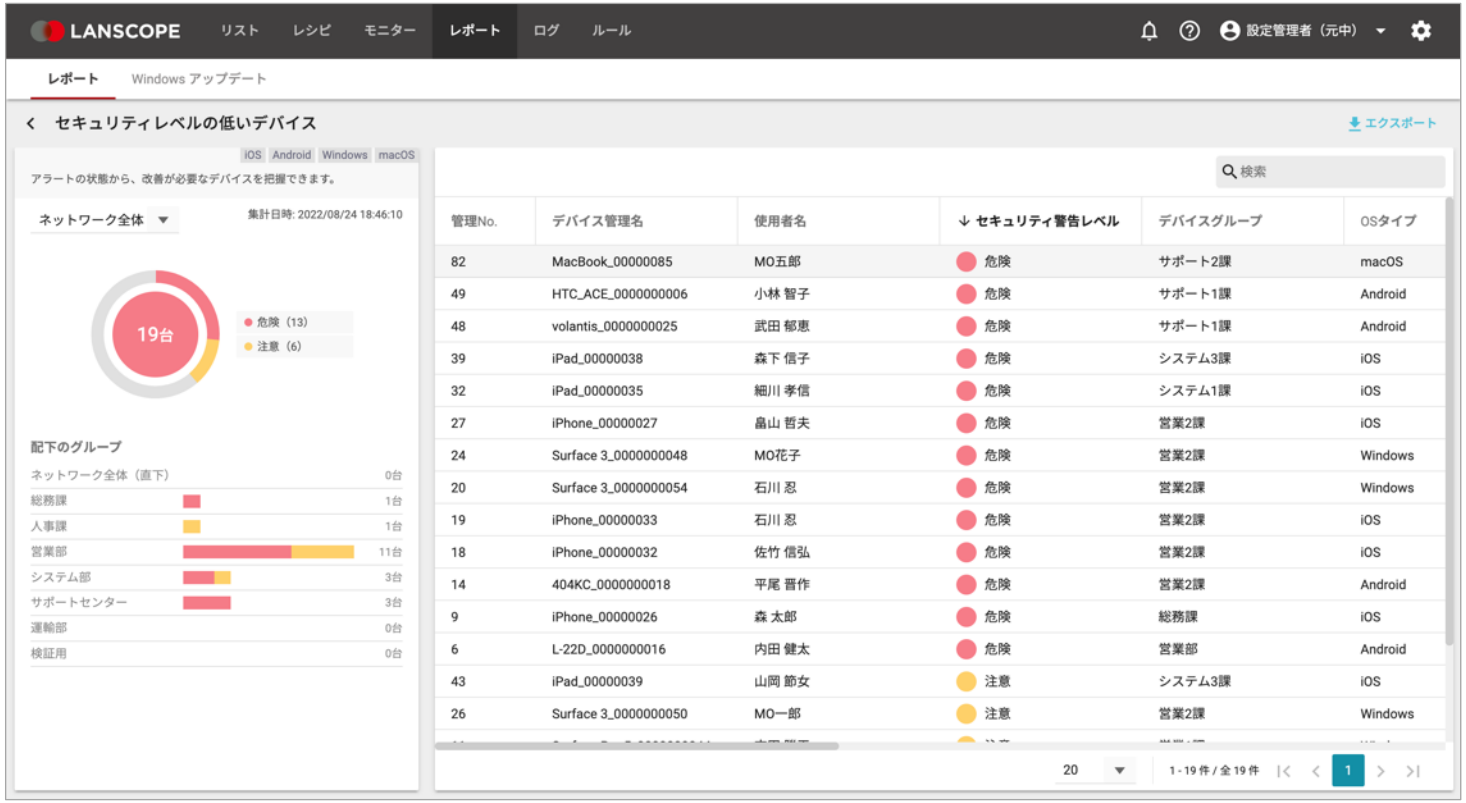
アプリの pkg ファイルをクラウドストレージにアップロードして、対象デバイスにアプリをインストール。



資産情報ベースとしたアラート一覧

i A W m
ライトA ライトB
ベーシック

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！



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

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

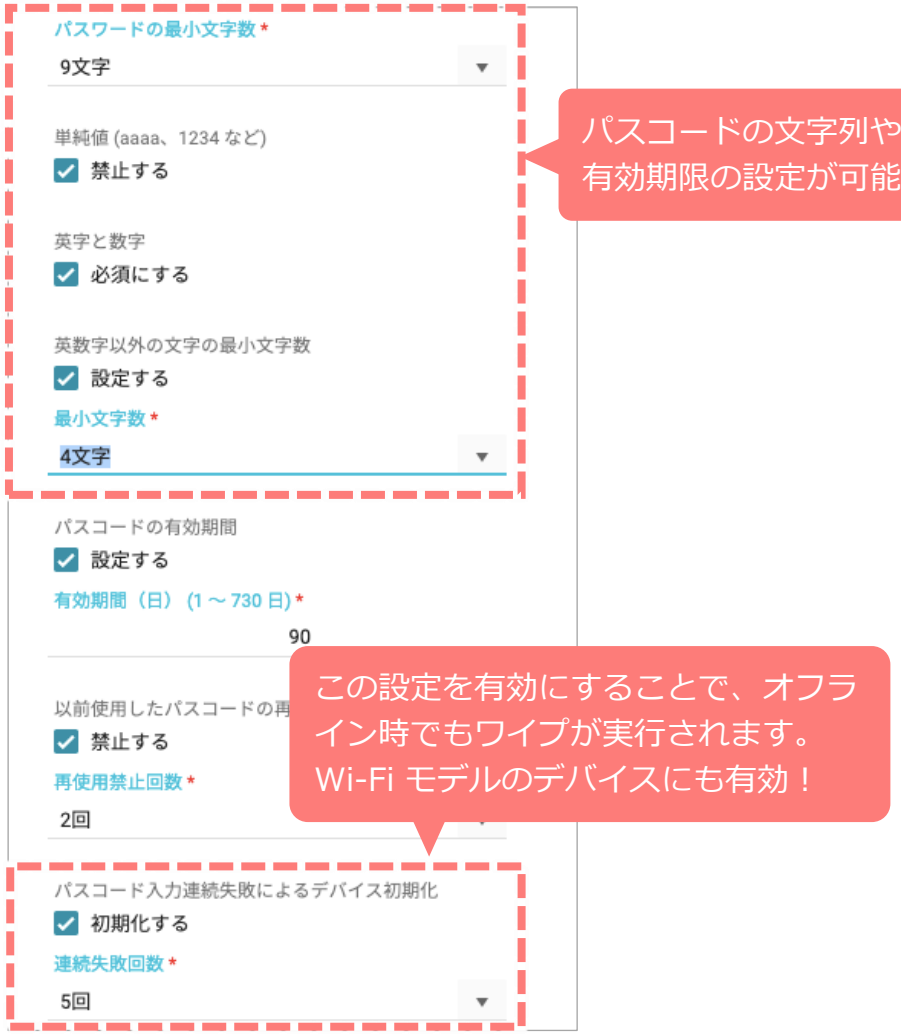
機能紹介③ Windows・macOS 操作ログ管理

機能紹介④ Apple Business Manager／Android Enterprise

機能紹介⑤ 関連製品

紛失リスクに備える事前対策：パスワードポリシー

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！



パスコードの文字列や有効期限の設定が可能

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
パスワードの最少文字数
使用しなければならない文字の種類
パスワードの有効期間
パスワードの有効期限を事前の通知
以前使用したパスワードの再使用を禁止
以前使用したパスワードの再使用を禁止
パスワ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。

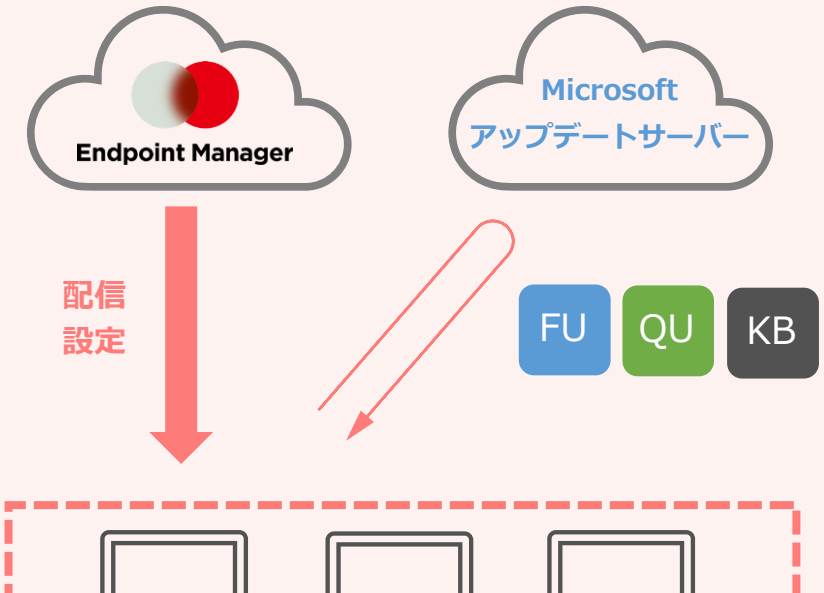
紛失リスクに備える事後対策：位置情報の確認※・リモートロック・ワイプ

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！

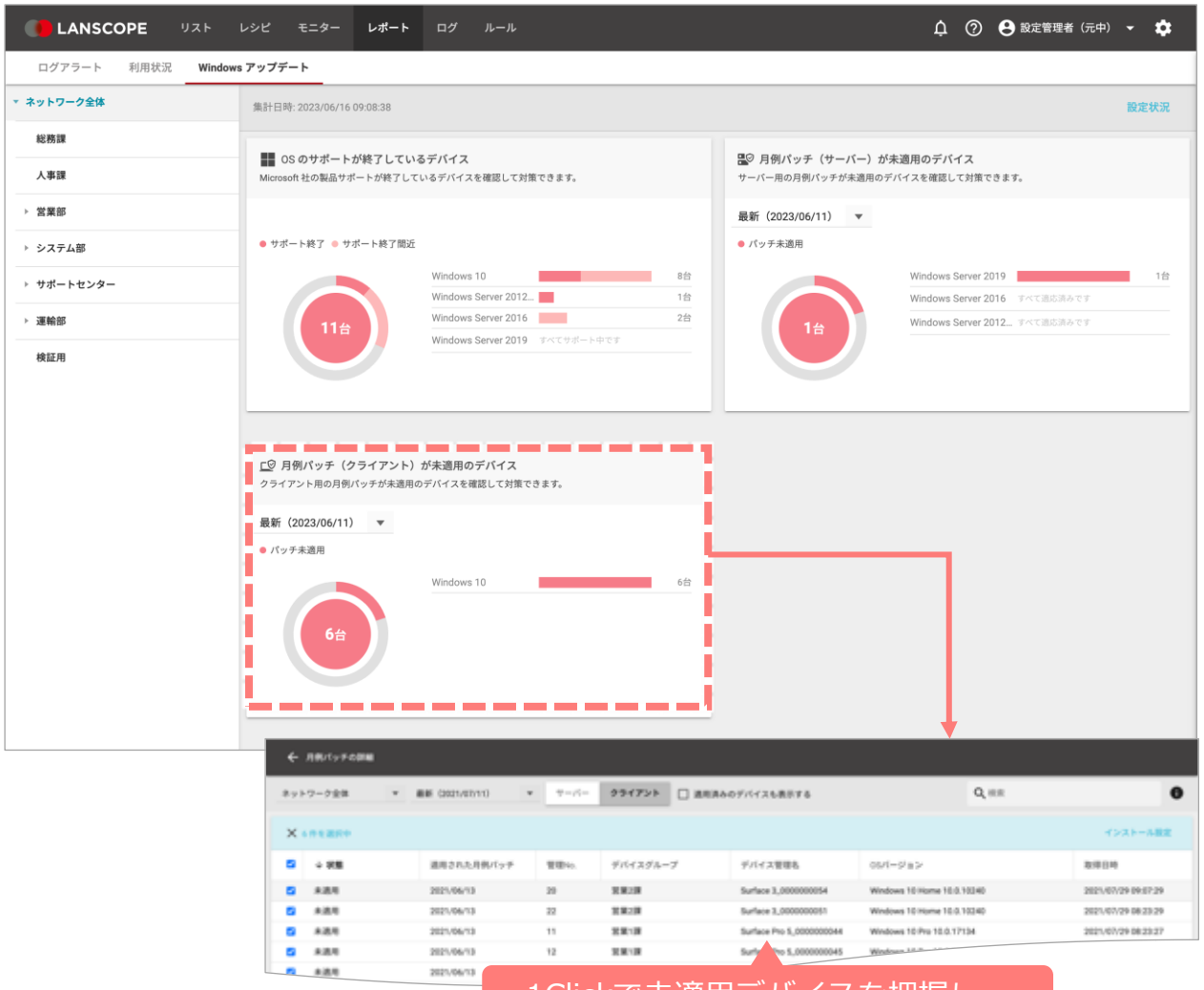
※ 位置情報の取得のためにはデバイス側で必要な設定があります。詳細はお問い合わせください。また位置情報の取得精度はデバイスに依存します。
※ OSによってリモートロック・ワイプの仕様は異なります。Windows Server OS はリモートロック・ワイプ機能に対応していません。
※ Windows Server OS・macOS は位置情報取得機能には対応していません。
※ Windows はスリープ状態の場合、位置情報が取得できません。

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

Windows アップデート管理のイメージ



社内ネットワークに接続されないデバイスも
エンドポイントマネージャーで配信可能

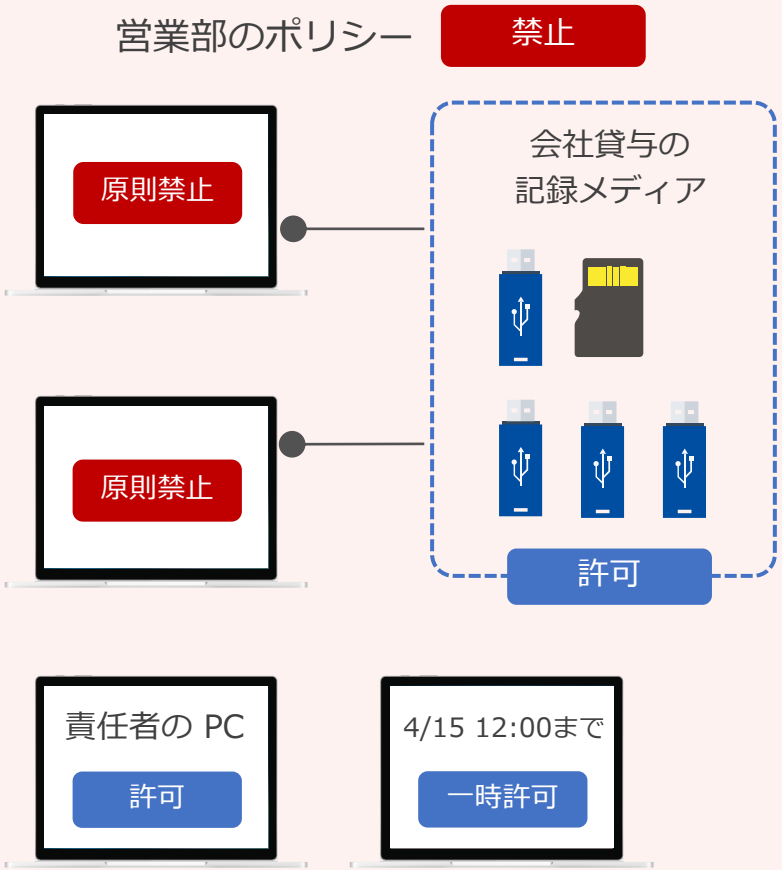


1Clickで未適用デバイスを把握し、
アップデート配信が可能

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・読取専用・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。

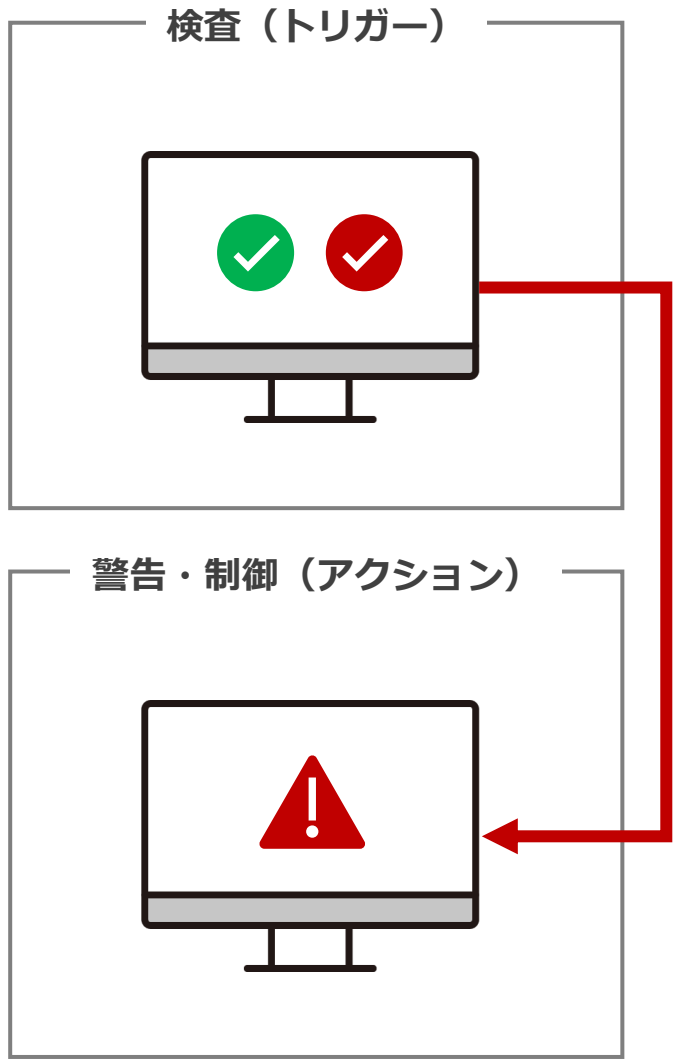
記録メディア制御のイメージ



「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。



i A W m
オプション

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

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。

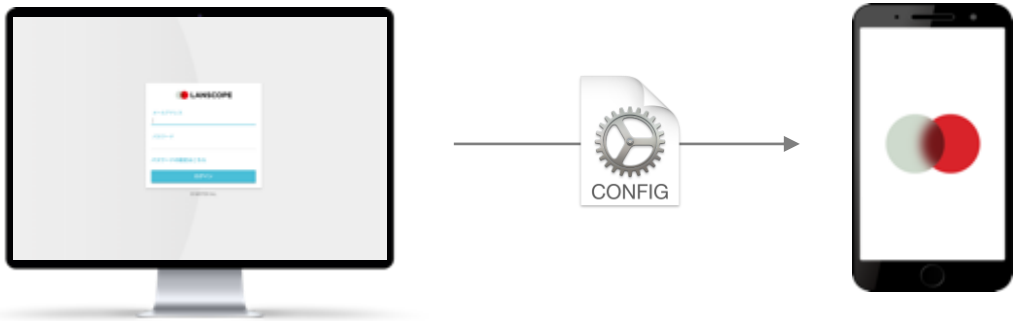
● カテゴリ別設定

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。

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

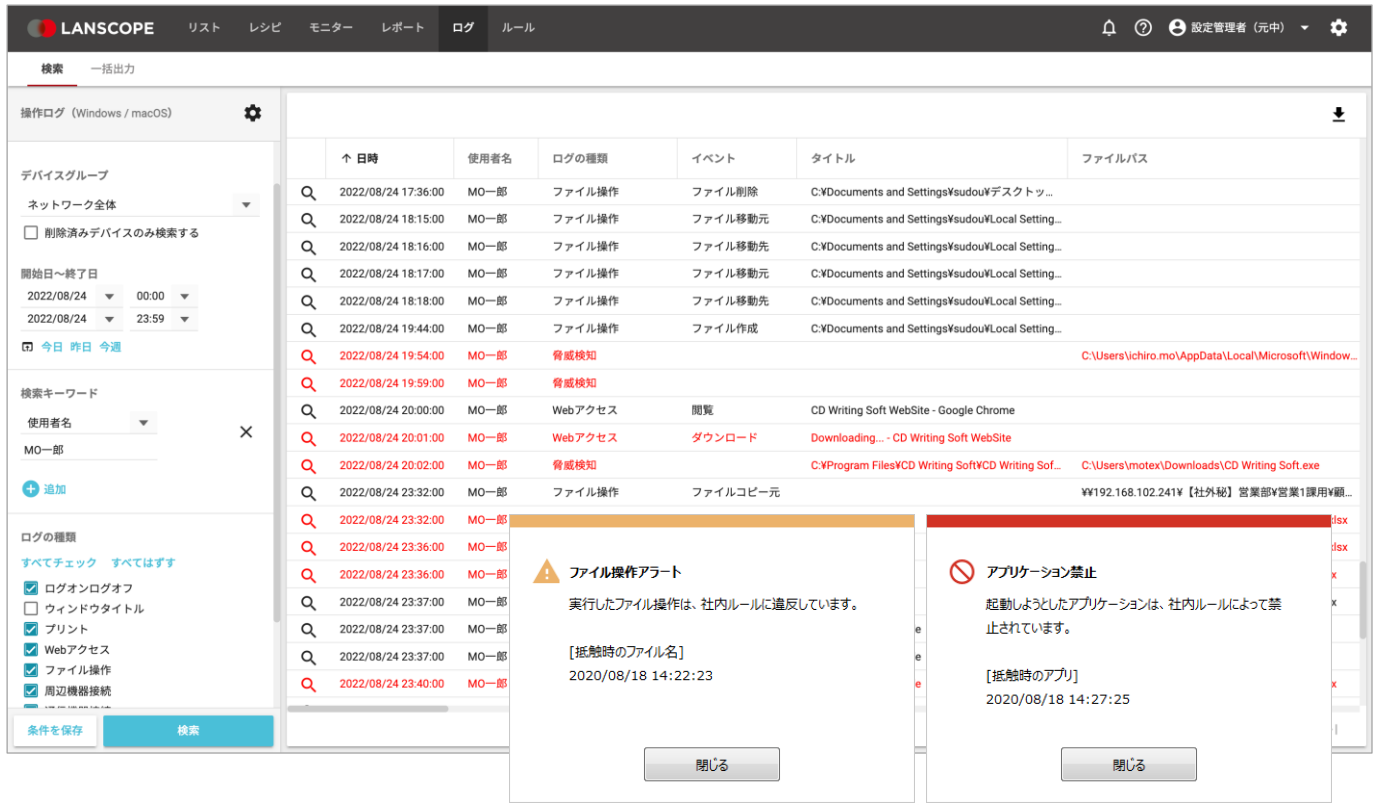
機能紹介④ Apple Business Manager／Android Enterprise

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。



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

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。

※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。

TOPICS ChatGPT の書き込みログ※に対応！

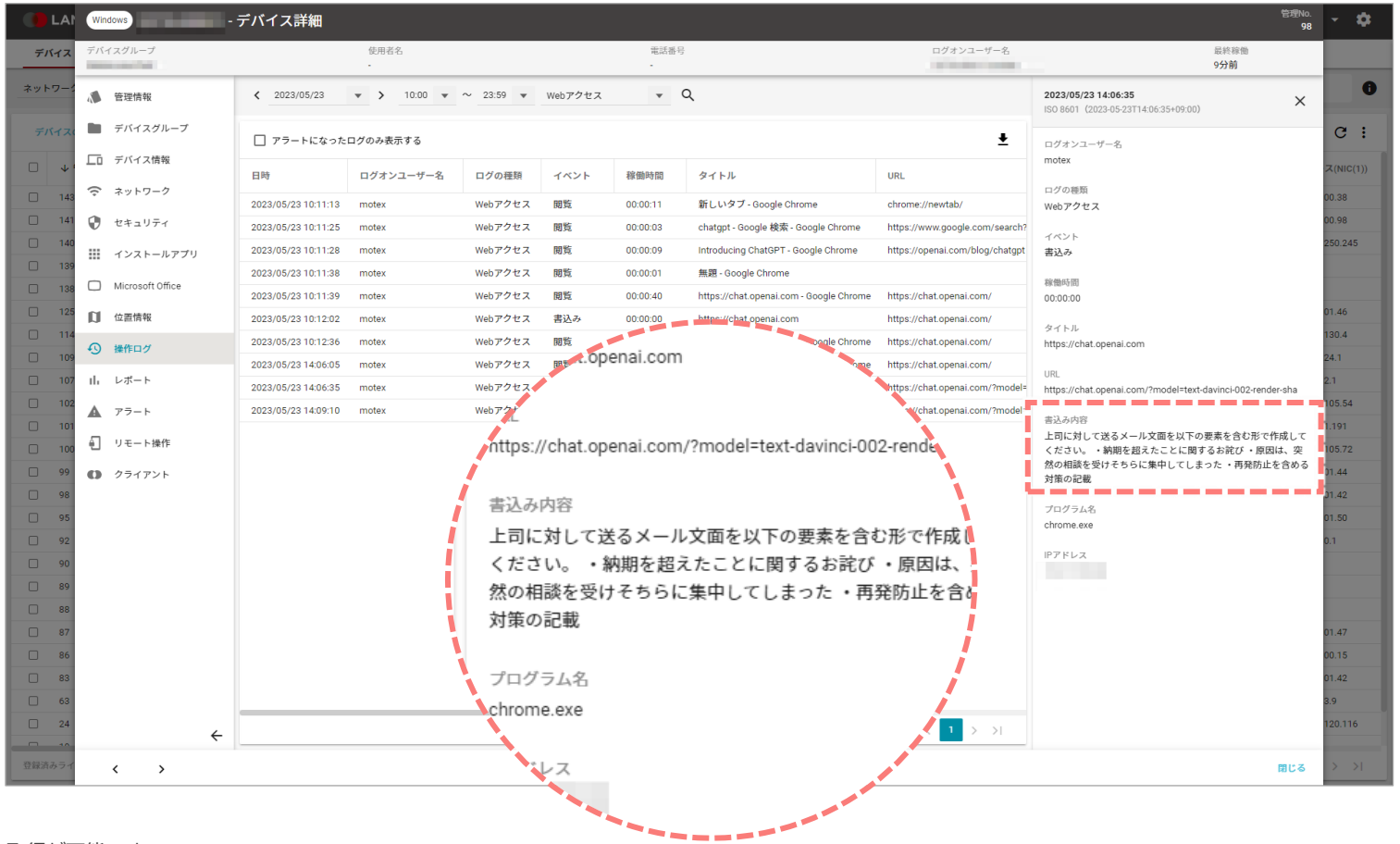
ChatGPT（https://chat.openai.com/）の書き込み内容＝質問内容の取得に対応、利用実態の見える化に！

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・・・

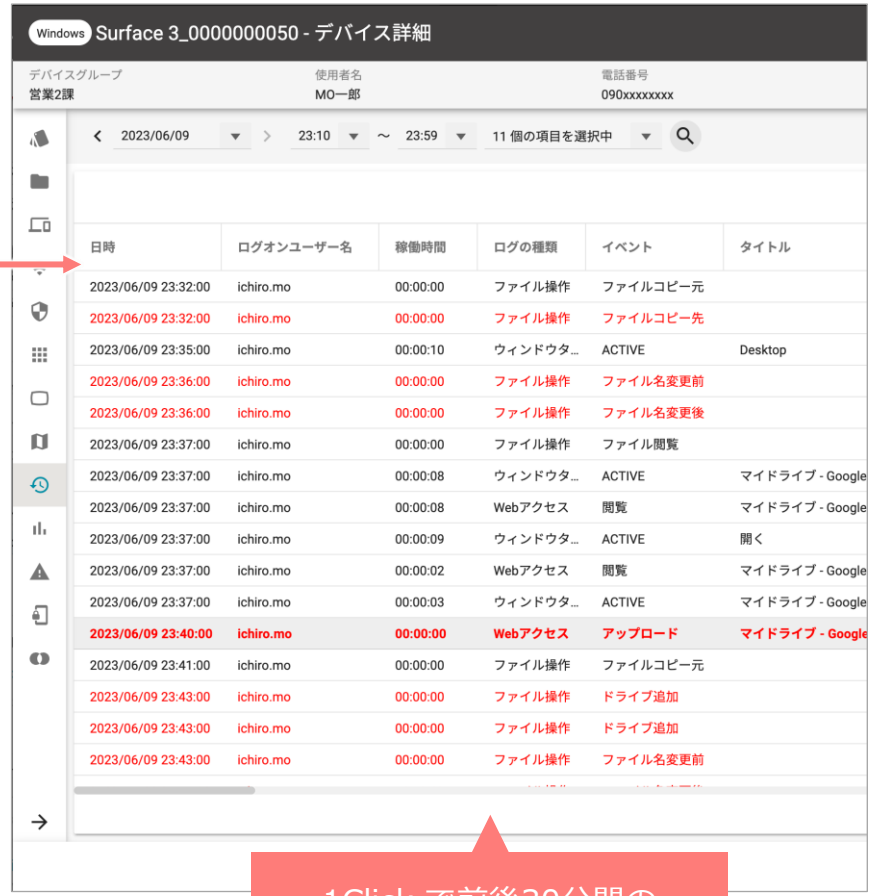


※ 書き込みログは、ChatGPT の他、Gmail・Outlook Online・Outlook.com のメール送信内容の取得が可能です。

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。



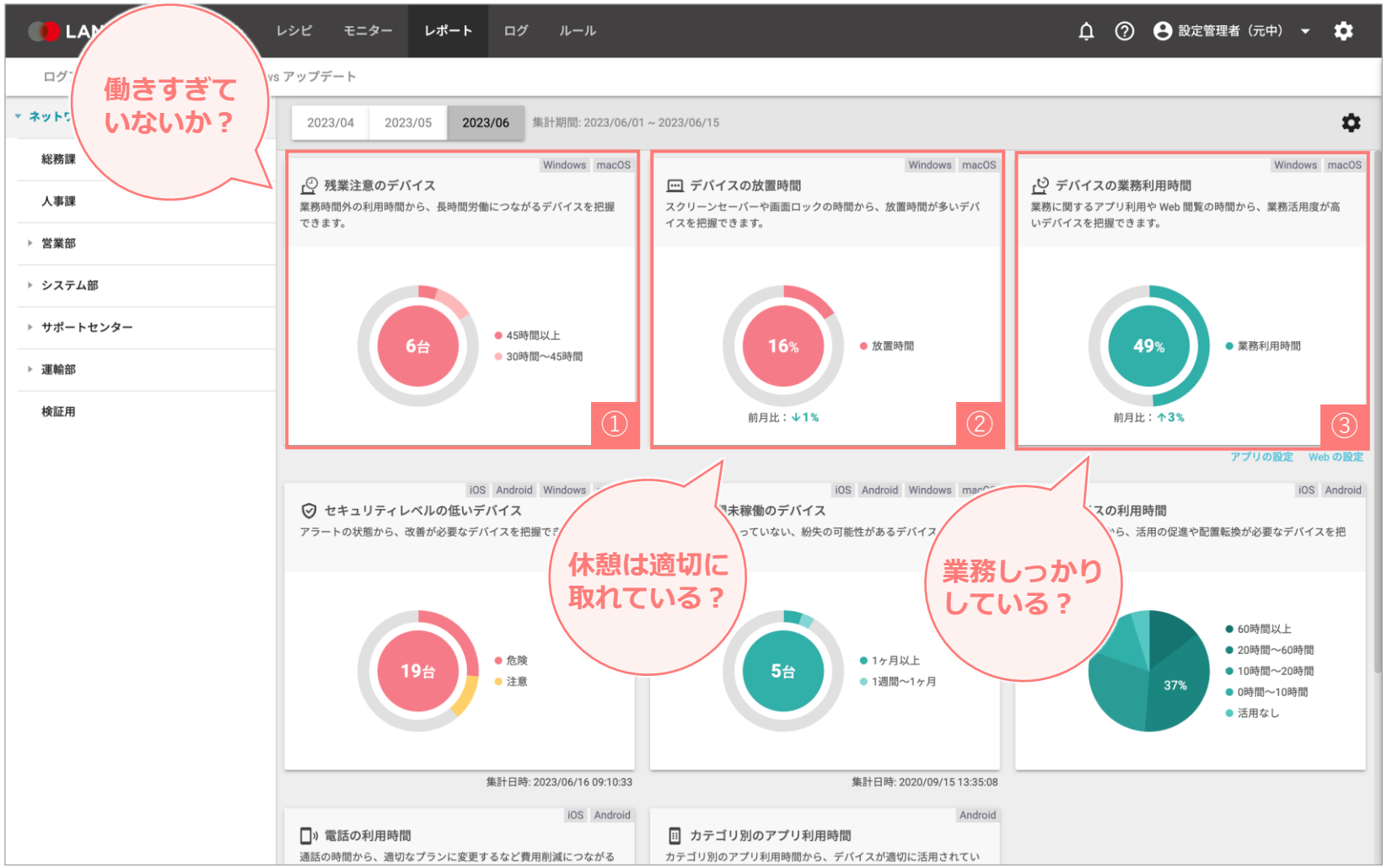
グループ単位で違反操作の発生状況を見える化し、Click 操作で詳細を確認

レポート形式で確認できるのは過去3ヶ月分です。

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	○	○
一定枚数以上の印刷	○	○
指定したキーワードがドキュメント名に含まれる印刷	○	○
Web サイト閲覧（タイトル / URL）	○	○
Web サイトのアップロード/ダウンロード（タイトル / URL）	○	ー
Web サイトの書き込み（タイトル / URL）	○	ー
指定したキーワードが含まれるファイル操作	○	○
ドライブの追加	○	○
ドライブに追加された記録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	○	ー
Outlook メールへのファイル添付	○	ー
機密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	○	○
指定した SSID / BSSID への接続	○	ー
Bluetooth 接続	○	ー

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

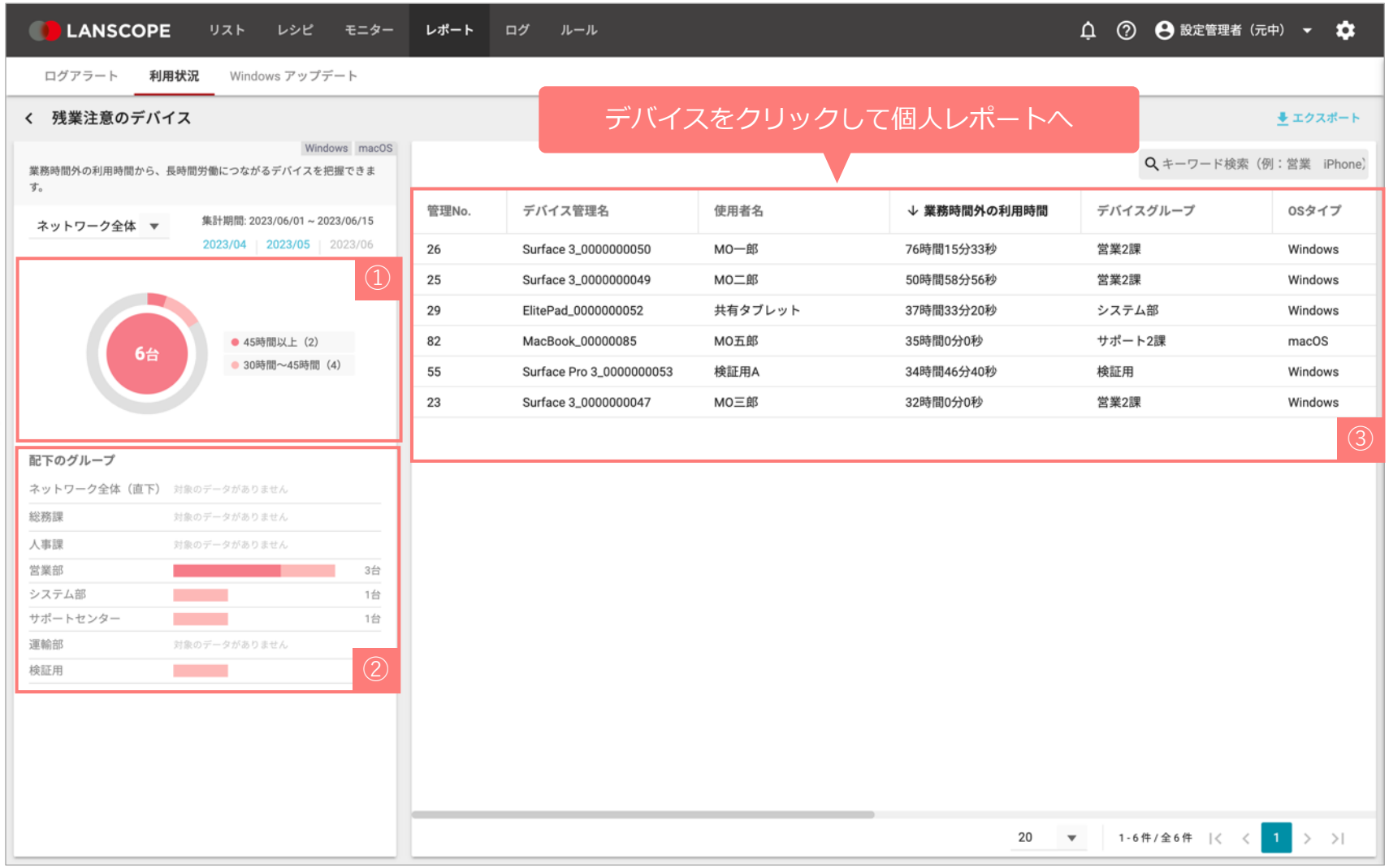
② デバイスの放置時間

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

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



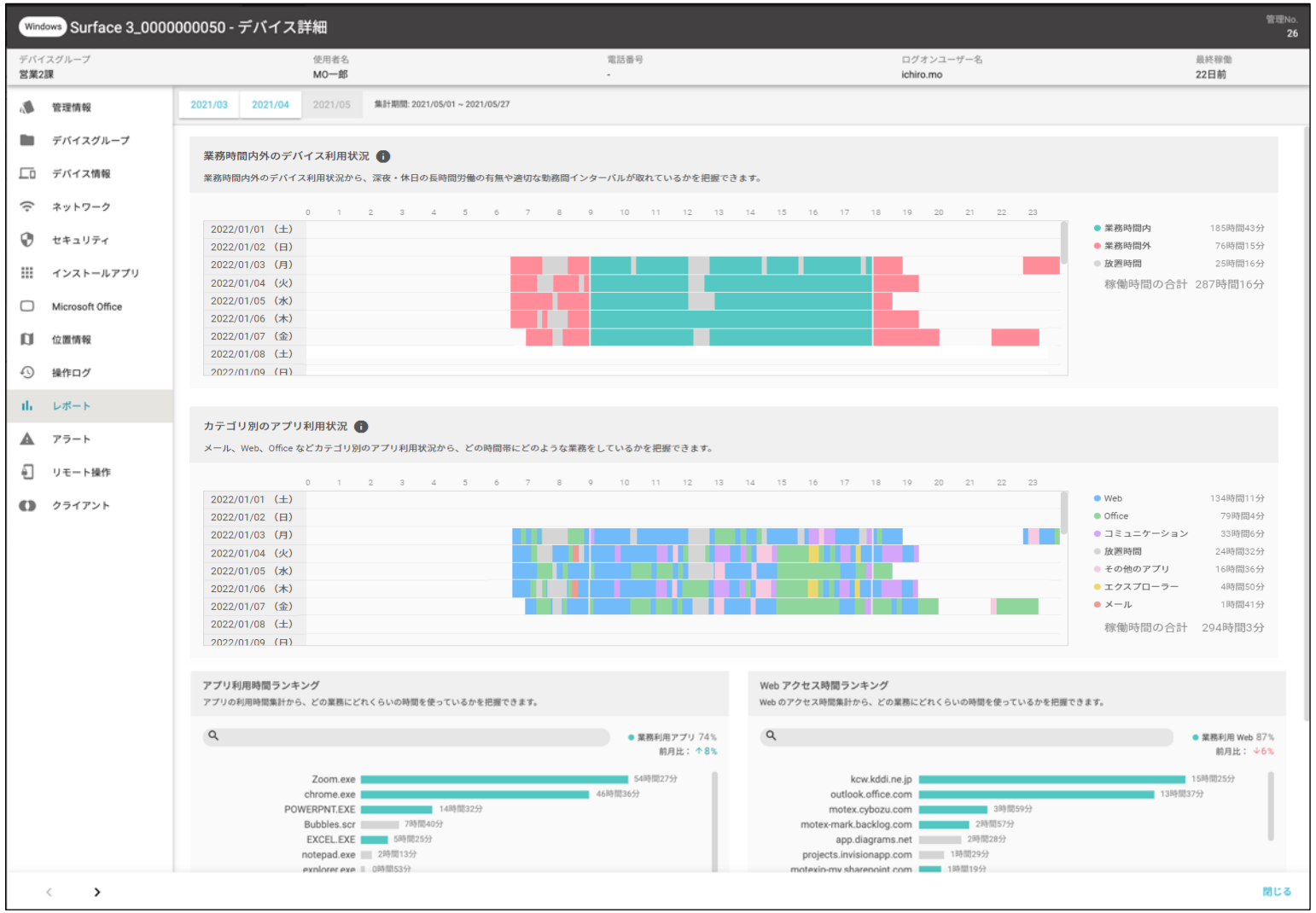
①全体の割合
選択しているグループ全体の状況を見える化

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。

（従来の範囲）IT 資産管理ツールの領域

ファイルサーバーの「顧客リスト」を「参考データ」に名前変更してアップロード

新たに取得が必要

クラウドサービスの領域

「参考データ」を競合Aに共有、競合Aがダウンロード

コピー	名前変更	アップロード	組織外共有	ダウンロード
				
ファイルサーバから「社外秘顧客リスト.xls」をデスクトップにコピー	「社外秘顧客リスト.xls」を「参考データ.xls」に名前変更	「参考データ.xls」をクラウドサービスにアップロード	クラウドサービス上の「参考データ.xls」を競合Aに共有	競合Aが「参考データ.xls」をダウンロード

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 脅威検出	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

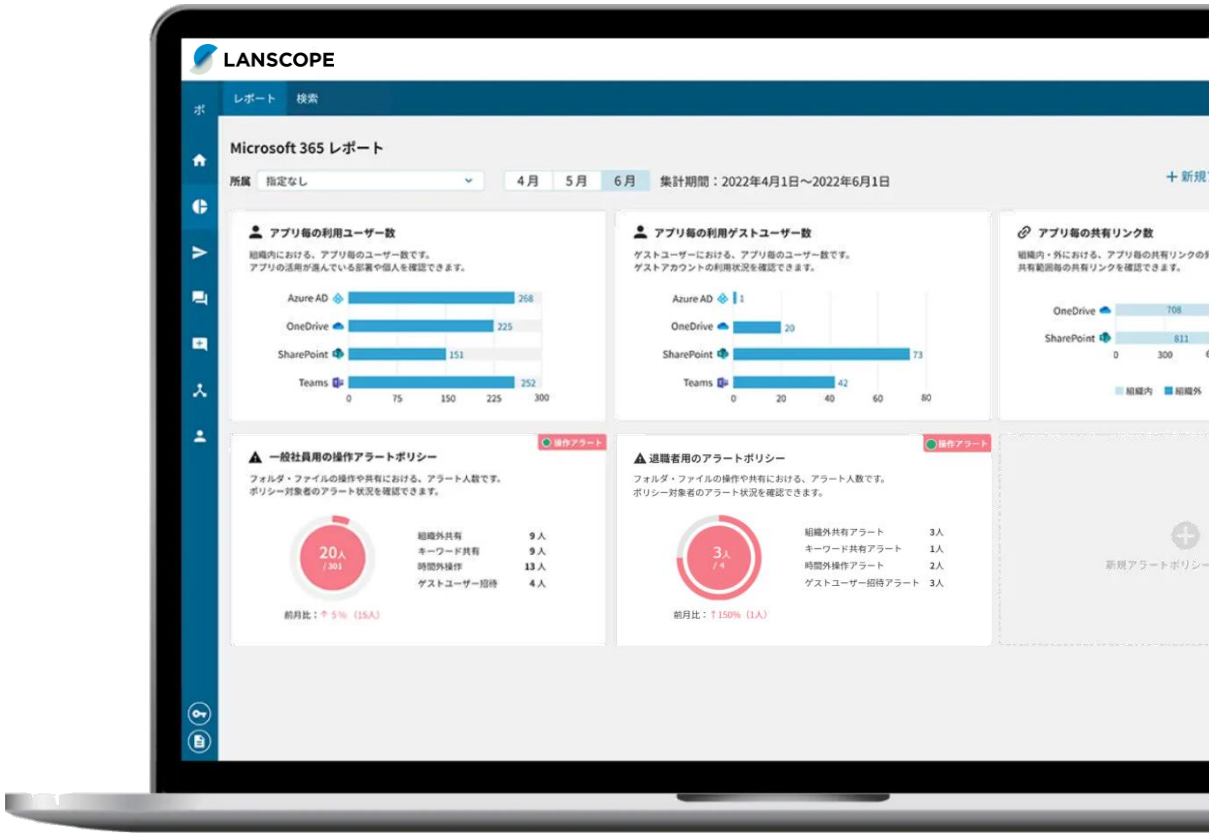
取得したログを分かりやすくレポートに
利用状況とセキュリティリスクを可視化

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。

モバイル管理必携となりつつある「ABM」「AE」

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 = 自動デバイス登録（DEP） + アプリの一括配信（VPP）

Apple Business Manager とは

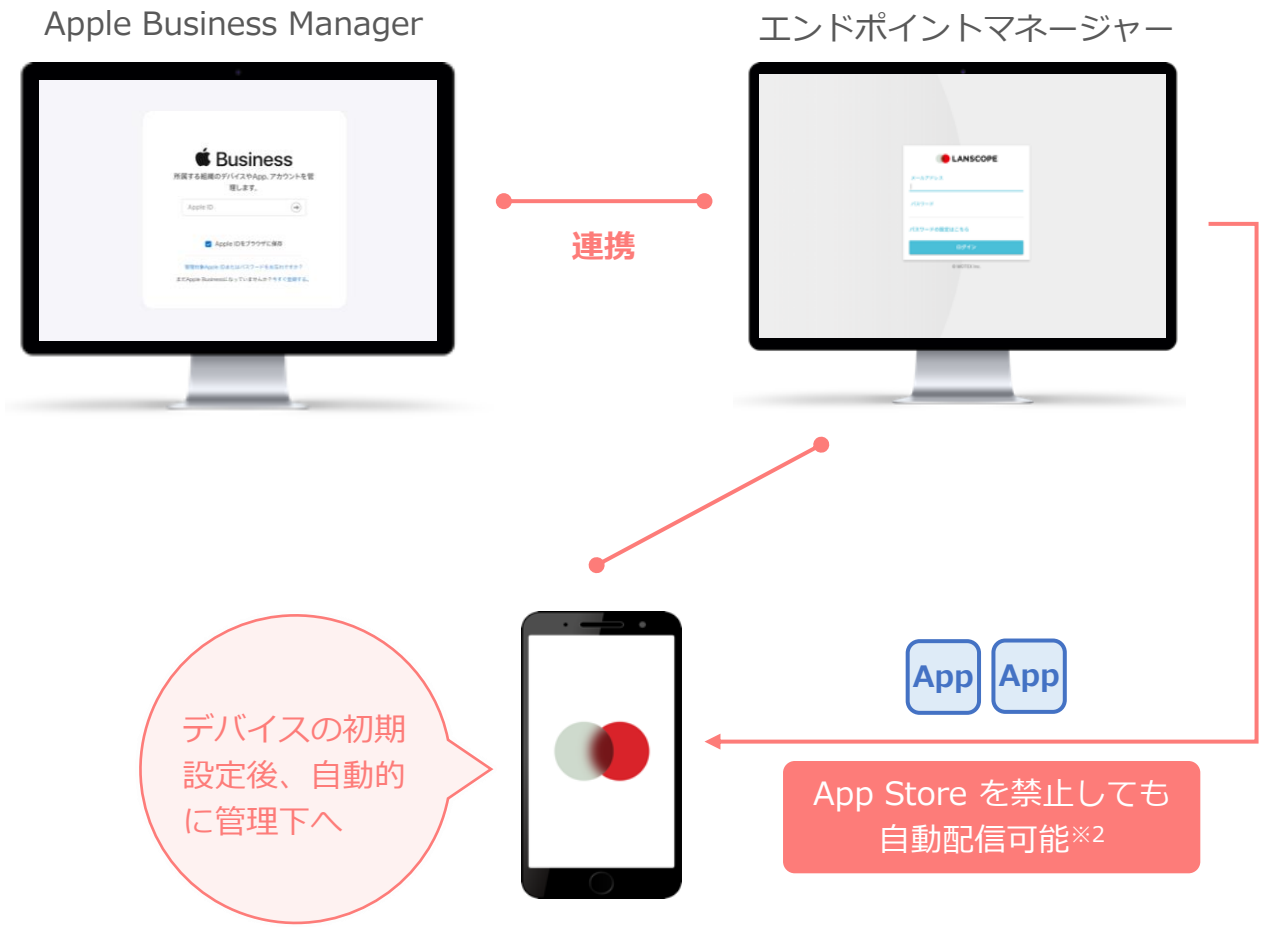
ABM はデバイスを効率的にエンドポイントマネージャーの管理下に置き、アプリの配信やデバイスの利用制御などを実現できる Apple 社が提供するプログラムです。

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		○	ー	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	○	ー	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	○	ー	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	○	ー	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		ー	○	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※		○	ー	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。

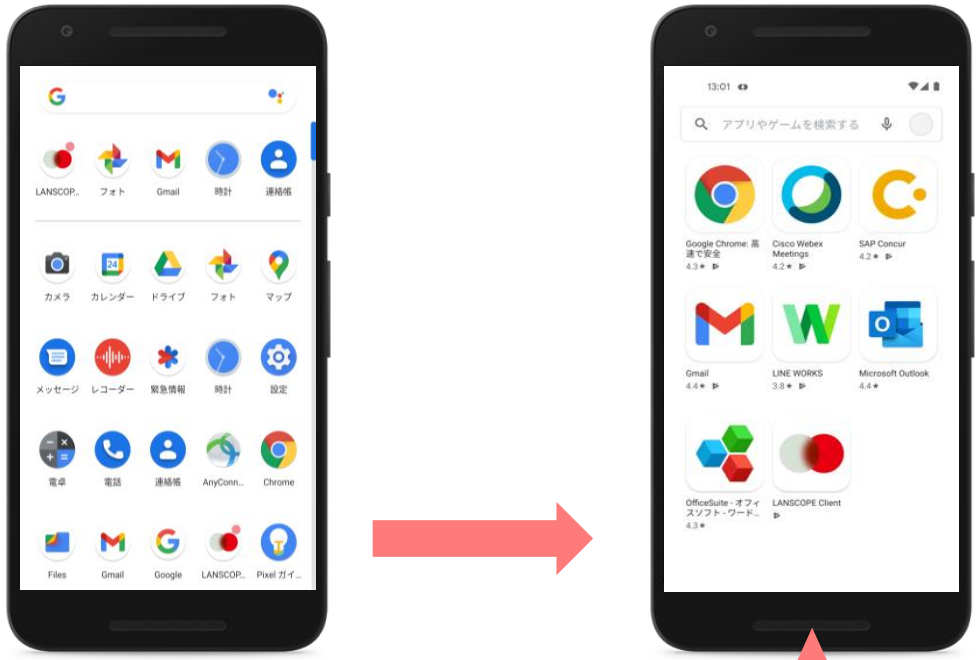
※ オプション機能です。

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。

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

LANSCOPE Security Auditor × Cloud LANSCOPE Endpoint Manager

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

Cloud LANSCOPE Endpoint Manager

ファイルサーバやローカルに保存されている
「社外秘」ファイルの名前変更

社外秘 技術資料.pptx

Rename

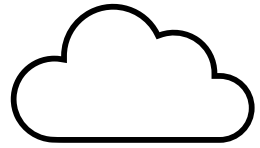
参考資料.pptx

クライアント PC 上の操作はエンドポイントマネージャーで記録可能。
しかし、クラウドサービスにアップロード後の把握はできない。

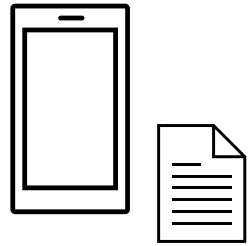
LANSCOPE Security Auditor

ファイルを SharePoint にアップロードし、
私物デバイスからダウンロード

Upload



Download



クラウドサービス上の操作はセキュリティオーディターで把握可能。
一方、データがどこから持ち出されたファイルなのかは把握できない。

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　ボリューム名　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　アンチウイ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）

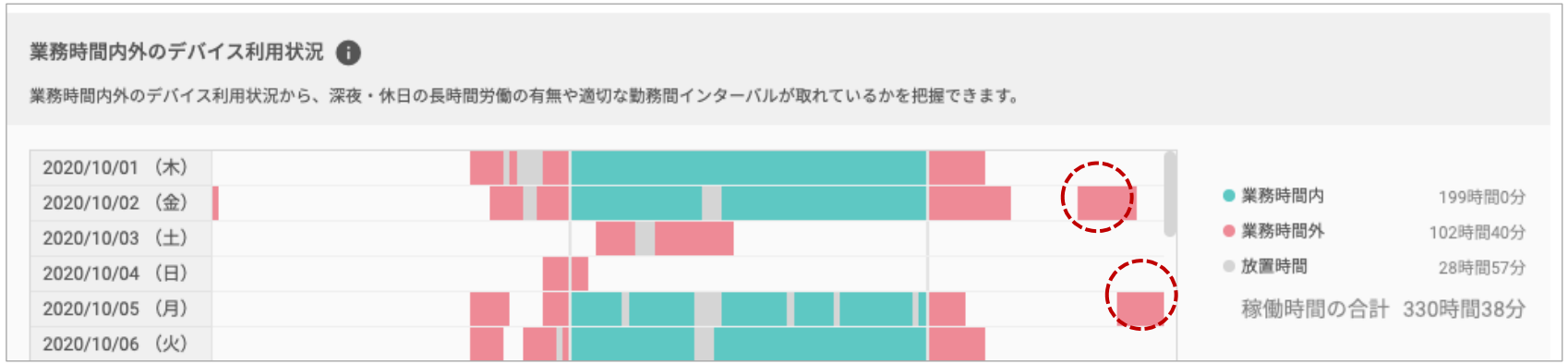
「デバイス詳細」画面の項目	項目名
管理情報 ※管理コンソール上で編集	デバイス管理名　デバイスタイプ　Apple ID　使用者名　使用者の社員コード　使用者の組織名　管理者名　管理者の組織名　管理者の組織コード 使用場所　使用者タイプ　使用状況タイプ　導入日　導入責任者　導入金額　導入タイプ　期限（リース／償却）　月額費用　購入先　補償内容 前回棚卸し実施日　前回棚卸し実施者　前回棚卸し実施結果　任意項目1～20
デバイスグループ	デバイスグループ
デバイス情報	OSバージョン　CPU名　メモリ　ドメイン・ワークグループ名　ログオンユーザー名　iTunesアカウント状態　iTunesStoreIdHash 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

i A W m
ライトA ライトB
ベーシック

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

働き方改革関連法案の施行で、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。



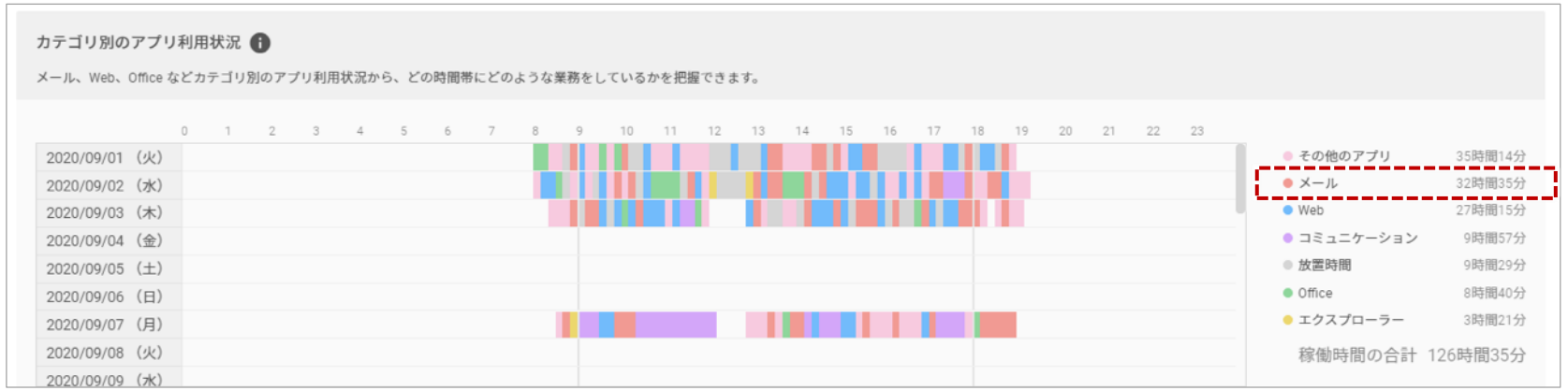
先週金曜日と今週の月曜日・・遅くまでありがとう。
でも申請時間外の労働は会社の違法行為になってしまう可能性もあるので行わないようにしよう。

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。



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


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！

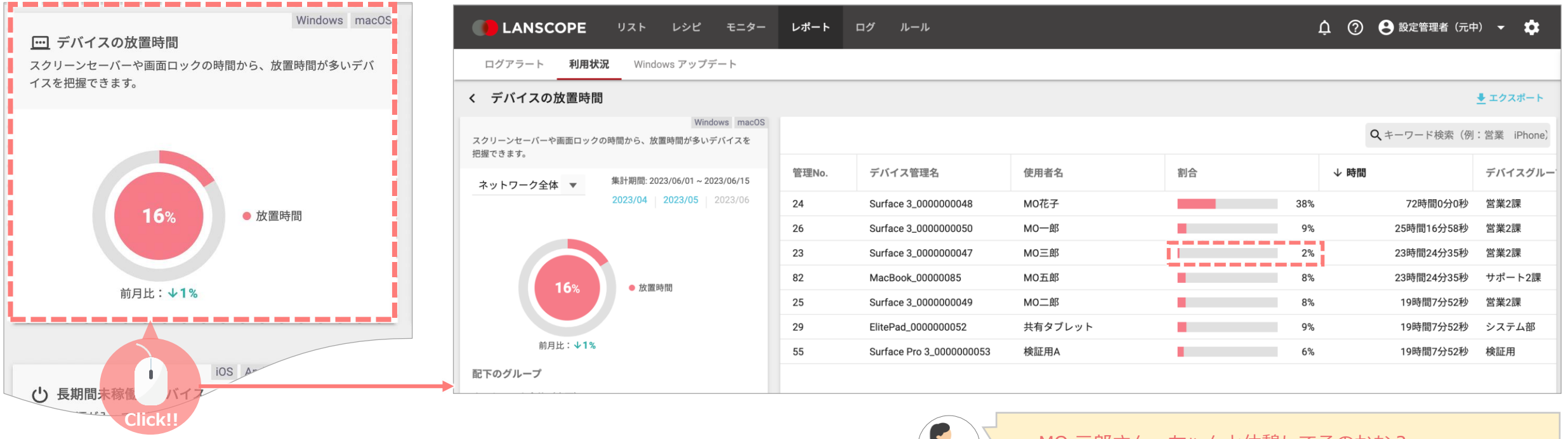
操作ログ活用シーン③ 休憩が適切に取れているか？

Win | macOS
ライトA | ライトB
ベーシック

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。



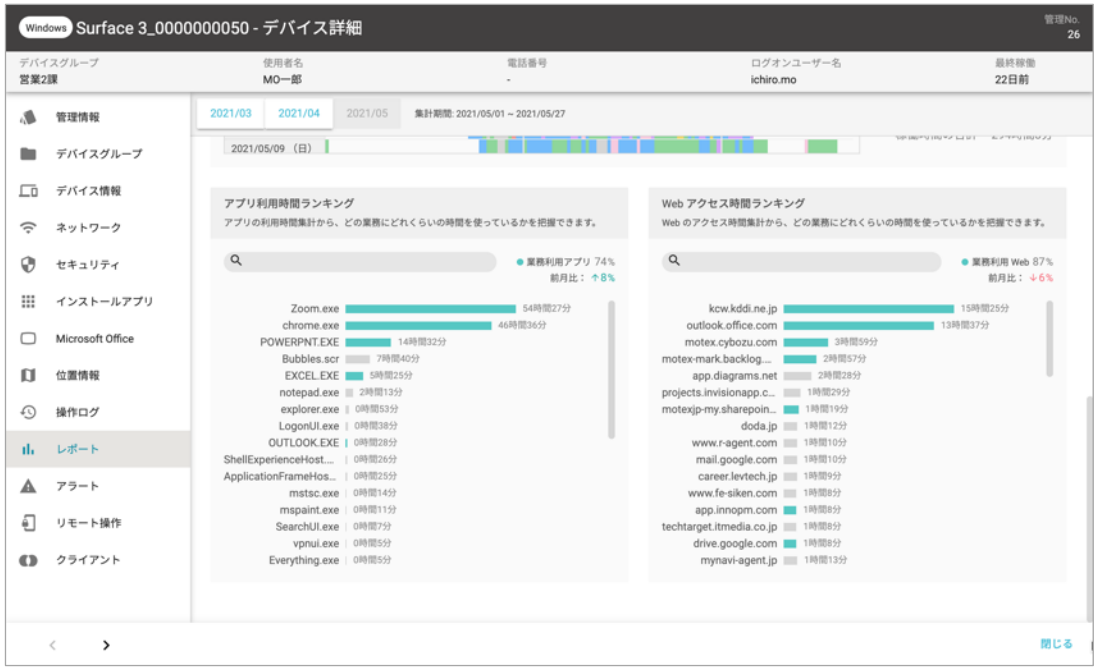
MO 三郎さん、ちゃんと休憩してるのかな？
次の 1on1 MTG で確認してみよう・・

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。



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

i A W m
ライトA ライトB
ベーシック

	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