

動作環境

管理者 PC

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

管理対象デバイス

iOS	対応OS	MDM構成プロファイル：iOS 6.0 ~ An Client (アプリ)：iOS 8.0 ~
	通信環境	以下ポートを解放してください。 ・ APNs (Apple Push Notification Service) による通信 (port:5223) ・ HTTPS 通信 (port:443)
Android	対応OS	Android 4.4 ~
	通信環境	以下ポートを解放してください。 ・ FCM (Firebase Cloud Messaging) による通信 (port:5228, 5229, 5230) ・ HTTPS 通信 (port:443)
Windows	対応OS	Windows 7, 8.1, 10 の各エディション (32bit / 64bit) ※Windows10に関しては、Fall Creators Update まで対応
	通信環境	以下ポートを解放してください。 ・ HTTPS 通信 (port:443)
macOS	対応OS	OS X Yosemite / OS X El Capitan / macOS Sierra / macOS High Sierra
	通信環境	以下ポートを解放してください。 ・ APNs (Apple Push Notification Service) による通信 (port:5223) ・ HTTPS 通信 (port:443)

〈開発・販売〉

エムオーテックス株式会社

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

TEL:03-5460-1371 受付時間 9:00-18:00 (月~金曜日 祝祭日除く)

E-mail:sales@motex.co.jp

URL:www.motex.co.jp

●お問い合わせは当社へ

- 本カタログは、2018年6月現在の内容となります。最新の情報は弊社Webサイトをご確認ください。
- 本カタログは予告なく変更することがあります。画面は実際の物とは異なることがありますので、予めご了承ください。
- エムオーテックス / MOTEX、LanScope、LanScope Cat、LanScope An は、エムオーテックス株式会社の登録商標です。
- その他、カタログに記載の会社名、ブランド、製品、ロゴなどは、各社の商標または登録商標です。

LanScope An

スマホ・タブレット・PCを「カンタン」管理

Version 3.0

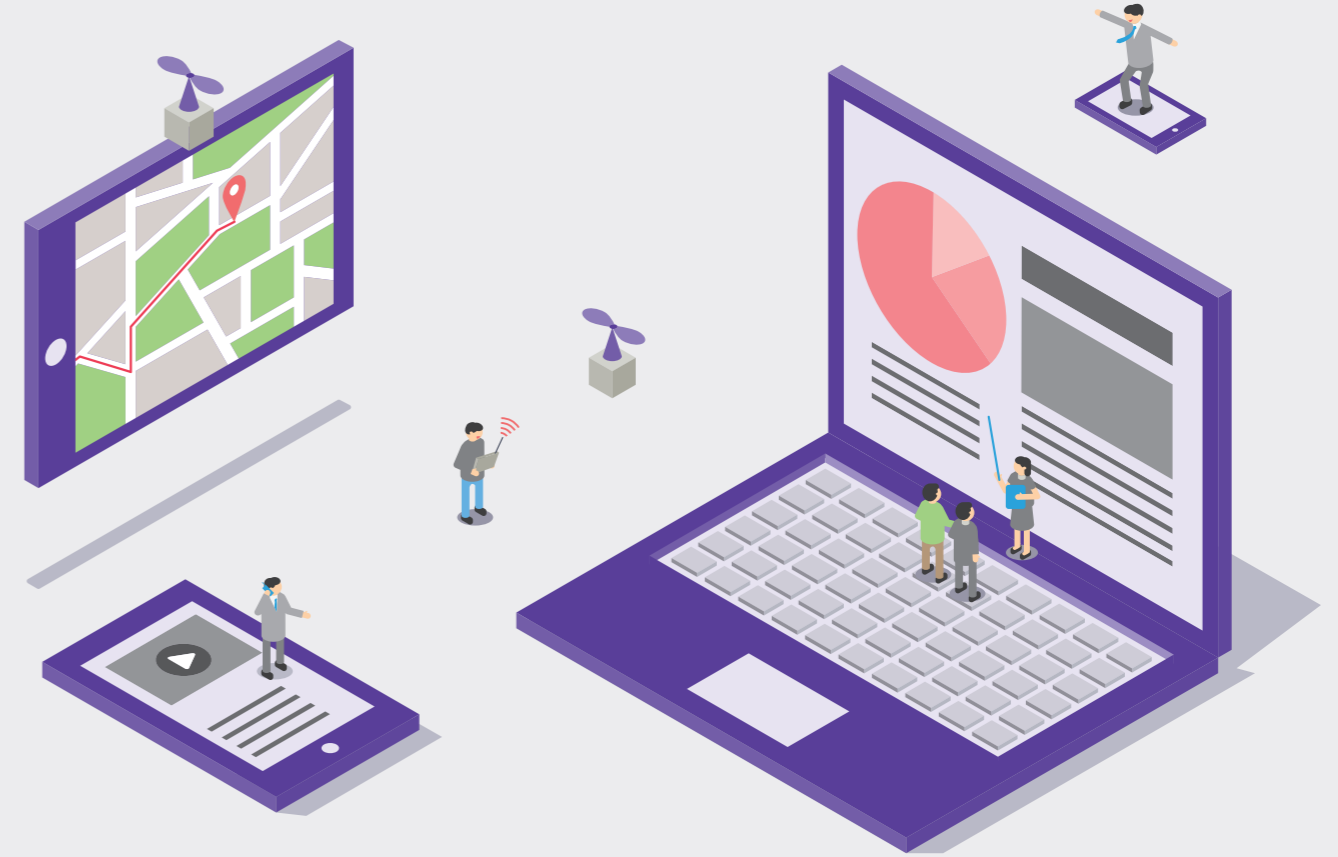


「カンタン」使いやすい・「カンタン」見える化・「カンタン」自動化

カンタンMDM

導入したスマホ・タブレット・PCとそれを活用する人やチームのパフォーマンスを最大限にひきだすため、セキュリティや活用状況の見える化、日々の運用管理を今までにないほどカンタンに実現します。

スマホ・タブレット・PCを一元管理



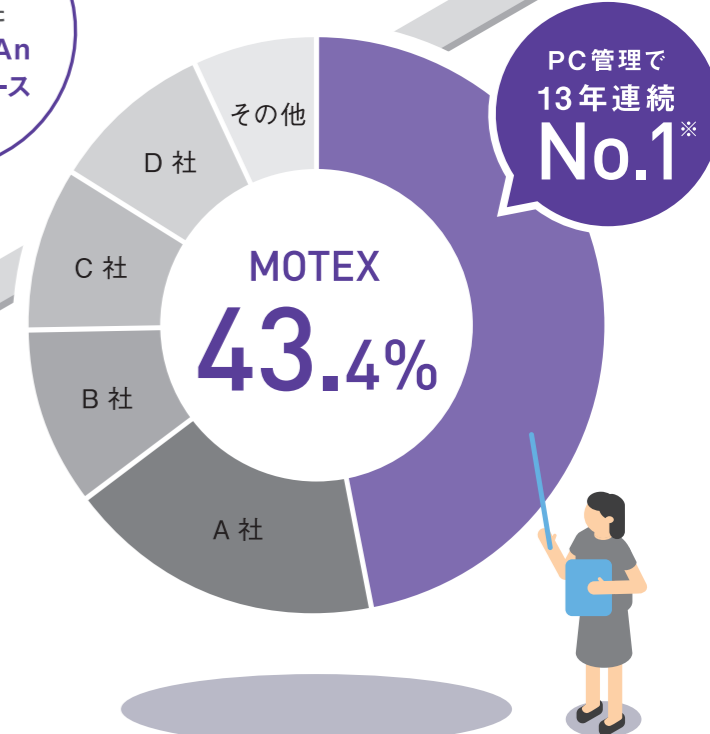
iOS・Android・Windows・macOSに対応

- デバイス情報の自動取得
- デバイス活用状況のレポート
- 遠隔から画面ロックやワイプ
- 位置情報の自動取得
- 管理・運用の自動化
- セキュリティルールを一括適用

MOTEXの歴史・実績



PC 管理のノウハウを、LanScope An へ!

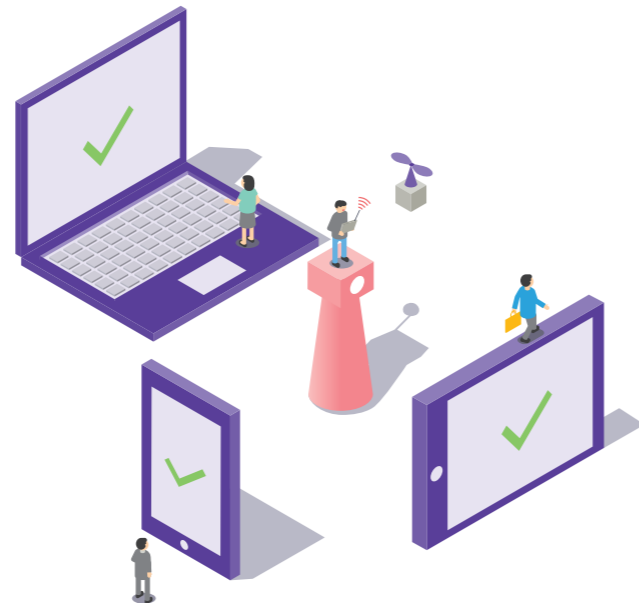


Ver.3.0の3つの特長

機能一覧

1. ストレスのない 使いやすさ

どんな目的でも3STEPの操作で達成できます。
機能がが増えても導線は同じ、
使いやすさを徹底的に追求しています。



2. 活用状況の見える化

導入したデバイスの活用状況を様々なレポートを通して
把握できます。デバイスやアプリの利用時間や回数から、
導入したデバイスの費用対効果の見える化に貢献します。



3. 管理・運用の自動化

スマホやPCの管理・運用を自動化することで、
管理者様の工数を削減、
より生産性の高いシゴトに集中できます。

iOS Android Windows macOS

		iOS	Android	Windows	macOS
資産管理	デバイス情報の取得	○	○	○	○
	デバイス情報の編集 / 台帳化	○	○	○	○
	インストールアプリ管理	○	○	○	○
	アプリインストール禁止	○	○	×	×
	アプリ利用禁止	○ ^{※1}	○	×	×
	不許可アプリ設定	○	○	○	○
	アプリ配信	○	×	×	×
	メッセージ / アンケート	○	○	○	×
	リース期限管理	○	○	○	○
	OSバージョン管理	○	○	×	×
位置情報管理	最新位置情報	○	○	○	×
	移動履歴	○	○	○	×
	リモートロック / ワイプ ^{※2}	○	○	○	○
セキュリティ対策	ローカルワイプ	○	○	×	×
	パスワードポリシー	○	○	×	×
	Jailbreak / root化検知	○	○	-	-
	SDカード抜き差し検知	-	○	×	×
	SIMカード挿入状態検知	○	○	×	×
	マルチユーザー制御	-	○	×	×
	資産アラート設定	○	○	○	○
	BitLocker 回復キー取得	-	-	○	-
	管理者へのメール通知	○	○	○	○
	デバイス利用ログ	○	○	×	×
操作ログ管理	アプリ利用ログ	×	○	×	×
	電話利用ログ	○ ^{※4}	○	-	-
	レポート	○	○	×	×
レポート	デバイス稼働	○	○	○	○
	デバイス活用	○	○	×	×
	アプリ活用	×	○	×	×
	電話活用	○	○	-	-
	セキュリティ警告	○	○	○	○
レシビ	トリガー	○	○	○	○
	アクション	○	○	○	○
その他	管理アカウントの権限分散	○	○	○	○
	24/365 紛失サポート ^{※5}	○	○	○	○
Apple社 提供プログラム 対応一覧	構成プロファイル情報取得	○	-	-	○
	構成プロファイル配信・削除	○	-	-	×
	VPP (Volume Purchase Program) ^{※5}	○	-	-	×
	DEP (Device Enrollment Program)	○	-	-	×
	紛失モード ^{※1}	○	-	-	×

※1 デバイスを監視モードに設定する必要があります。 ※2 OSによって仕様が異なります。 ○…対応 ×…未対応 -…OS仕様により非対応
 ※3 Apple Configuratorで構成プロファイルを作成する必要があります。 ※4 通話相手は取得できません。
 ※5 オプション機能です。

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

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

必要な情報をわかりやすく表示

管理No.	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	電話番号	デバイス名
1	総務課	SC-03D_0000000014	江藤 花子	Android	4.4.2	090xxxxxxx	SC-03D
2	総務課	hammerhead_0000000059	六角 龍夫	Android	6.0	090xxxxxxx	hammerhead
3	人事課	iPhone_000000028	森 育三	iOS	10.0	080xxxxxxx	iPhone5
4	人事課	N-04C_0000000020	江村 太郎	And	8.0	080xxxxxxx	N-04C
5	営業部	angler_0000000019	橋中 栄一郎	Android	8.0	080xxxxxxx	angler
6	営業1課	L-22D_0000000016	内田 健太	Android	6.0	080xxxxxxx	maguro
7	営業1課	404KC_0000000023	中田 真由美	macOS	10.12.6		404KCの MacBook Pro
8	営業1課	picasso_aappcus6jp_00000000...	橋 秀雄	iOS	11.0.2	090xxxxxxx	picasso
9	営業1課	P85SD10_0000000017	石井 健二	Windows	10.0.17134.1	090xxxxxxx	P85SD10
10	営業1課	iPhone_000000029	別所 哲郎	iOS	10.0	080xxxxxxx	iPhone
11	営業1課	Surface Pro 2_0000000044	吉田 勝平	Windows	6.0.9	080xxxxxxx	Surface Pro 2
12	営業1課	Surface Pro_0000000045	加藤 信也	Windows	6.0.9	080xxxxxxx	Surface Pro
13	営業部	iPhone_000000026	飯田 太郎	iOS	10.0	080xxxxxxx	iPhone
14	営業2課	404KC_0000000018	平尾 晋作	Android	6.0	080xxxxxxx	404KC

対象デバイスの取得情報の全てを確認 デバイス詳細

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

ハードウェア情報・設定情報を自動取得 資産管理

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

iOS		Android		Windows	
OSバージョン	iCloud バックアップ	OSバージョン	IPアドレス	OSバージョン	Bluetooth状態
シリアル番号	加入キャリア	モデル名	SIMのシリアル番号	モデル名	Windows アップデート
IMEI	Jailbreak	IMEI	root化	CPU名	リモートワイプ実行可否
監視モード	モデル名	CPU名	製品名	ストレージ使用容量	NetBIOS名
アクティベーションロック	ストレージ使用容量	Wi-Fi状態	内部ストレージ使用容量	Wi-Fi状態	シリアル番号
電話番号	電池残量	サーブアドレス	ブランド名	ファイアウォール状態	メモリ
データローミング	iPhoneを探す	モバイルネットワーク設定	MACアドレス(Wi-Fi)	アンチウイルス更新ステータス	ログオンユーザー名
デバイス名	最新 iCloud バックアップ日時	メールアドレス1~3	DHCP IP アドレス	コンピューター名	NIC情報
UDID	MACアドレス(Wi-Fi)	シリアル番号	加入キャリア	製品名	アンチウイルス状態
MEID	パスワードロック	ハードウェア名	パスワードポリシー	CPU周波数	BitLocker回復キー
紛失モード		電話番号		ドメイン・ワークグループ名	

macOS			編集可能項目		
OSバージョン	ビルドバージョン	デバイス名	送信先メールアドレス	デバイス管理名	前回欄卸し実施結果
シリアル番号	モデル名	ホスト名	使用者名	デバイスグループ階層 1~5	前回欄卸し実施日
IMEI	UDID(ハードウェア UUID)	ストレージ使用容量	購入金額	使用者の組織名	任意項目 1~20
iCloud バックアップ	iTunesStoreIDHash	ログオンユーザー名	月額費用	導入タイプ	Apple ID
加入キャリア	MACアドレス(イーサネット)	MACアドレス(Bluetooth)	前回欄卸し実施者	購入先	導入日
					期限(リース/償却)

アプリ情報の管理 インストールアプリ管理

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

アプリの配信 アプリ配信(iOSのみ)

業務上必要なアプリを複数のデバイスに一斉配信することができます。また、配信したアプリをアンインストールすることができます。

必要な情報を簡単に収集 メッセージ・アンケート機能

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



User's voice

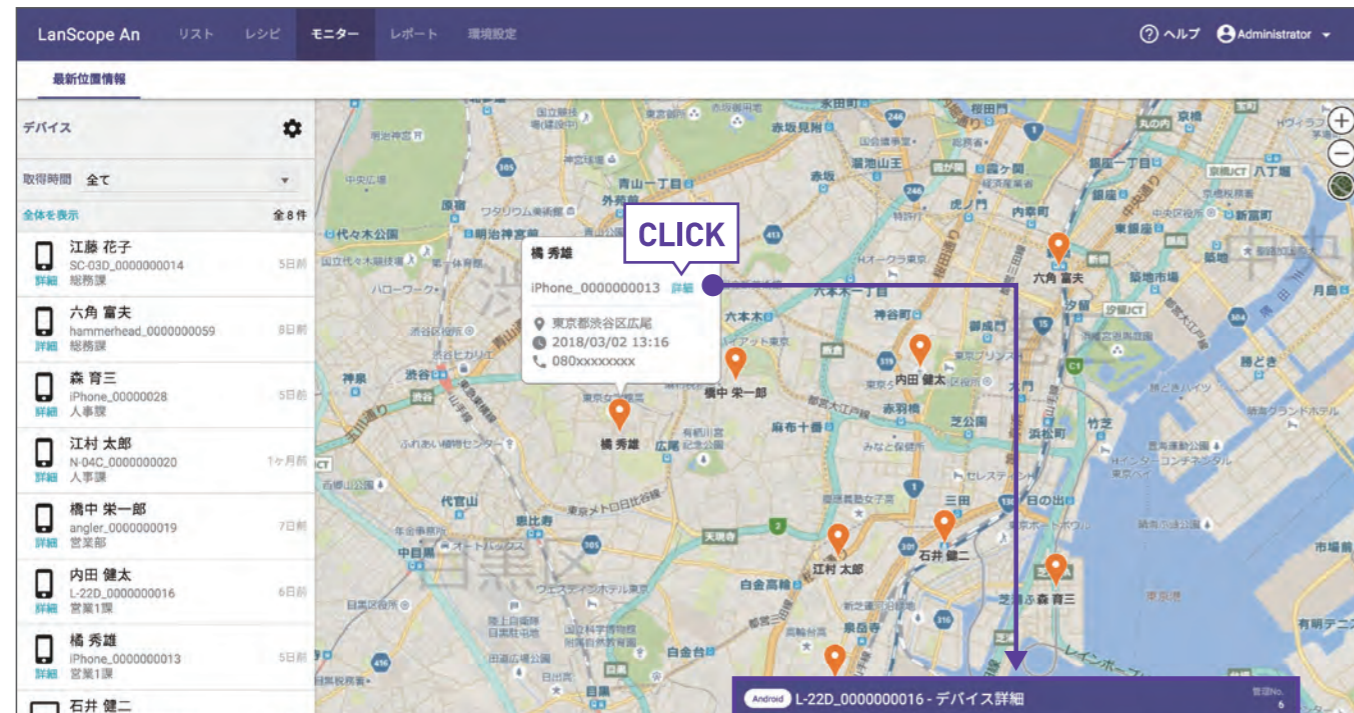
全国30拠点にある
スマートデバイス 800 台をまとめて管理。
手入力によるミスもなくなり助かっています。

スマートフォンの導入で管理しなければならない情報が増え、これまでの手入力でのExcel管理は限界があると感じていました。Anは、最新の資産情報を自動収集してくれるので、わざわざデバイスを1台1台確認する必要がなく、全国の拠点にあるデバイスを一元管理できています。

位置情報を自動取得し、デバイスがどこにあるか一目でわかります。

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

複数デバイスの最新位置情報をまとめて表示



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

デバイスごとに1日の移動履歴を表示 移動履歴管理

01 業務管理

外出時の社員の動きを把握して業務管理ができます。

02 営業支援

複数デバイスの位置を同時に確認。スムーズな営業支援ができます。

03 紛失対策

万が一デバイスを紛失しても所在がすぐに確認できます。



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



User's voice

万が一の紛失、電源がOFFになっていると対策が打てない！でも、LanScope Anなら…

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

紛失の事前対策から、万が一の紛失時の対策を実現します。

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

紛失に備えた事前の対策

パスワードポリシーの一括適用

(iOS、Android 対応)



デバイスの稼働状況を確認



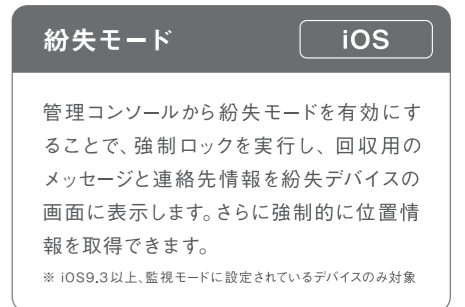
万が一の紛失時の対策

STEP 1 位置情報を確認

(iOS、Android、Windows 8.1以降対応)



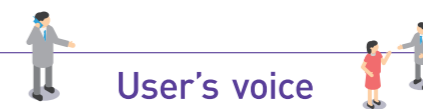
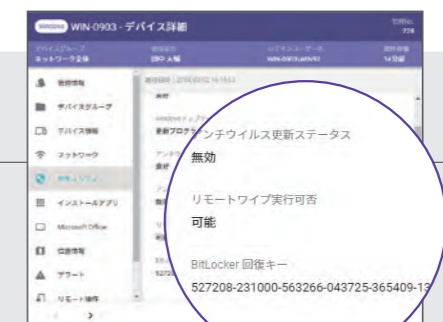
STEP 2 リモートロック・ワイプを実行



PICK UP

BitLockerを利用した紛失対策を実現!

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



User's voice

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

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

豊富なレポートで、デバイスの活用状況を「見える化」します。

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

デバイスの活用状況やルール違反の状況をレポート



レポートはデバイス稼働、セキュリティ警告、デバイス活用、アプリ活用、電話活用の5種類。グラフをクリックすると該当するデバイスを一覧で表示。またデバイスの詳細を確認することができます。

※ 操作ログはiOS・Androidのみに対応。OSによって取得できる内容が異なります。

操作ログ管理の効果

操作ログ

01 現状の把握

導入した目的に沿ってスマートデバイスが活用されているか、判断や分析のための情報として活用できます。

02 不正操作を抑止

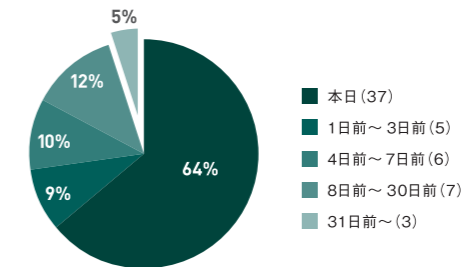
ログを自動取得する＝行動を見られている、という意識をもたらし、不正操作を未然に防ぐことができます。

●取得可能な操作ログ

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

デバイス稼働

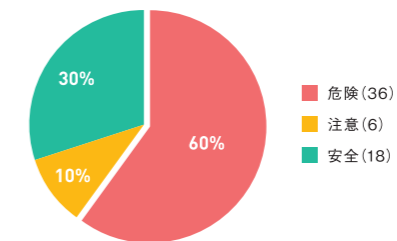
管理しているデバイスを、未稼働(電源が入っていない状態やAnサーバーと通信が取れていない状態)の日数ごとにグラフ化し、デバイスの稼働状況を把握できます。長期間未稼働なデバイスの再配置や紛失防止に役立ちます。



3台のデバイスが1ヶ月以上未稼働...! 紛失していないかチェックしよう!

セキュリティ警告

デバイス利用ルールに違反しているデバイスを「危険」「注意」の警告基準に分けてレポート表示。警告基準は自社の運用に合わせて設定できます。



営業2課で違反が多い! 毎週の朝礼で利用ルールを再徹底しよう!

●警告設定の内容

資産情報に関する警告	iOS	Android	Windows	macOS	操作ログに関する警告	iOS	Android	Windows	macOS
設定期間以上未稼働になっている	○	○	○	○	不許可アプリ起動	—	○	—	—
デバイスが管理外になっている	○	—	○	○	新規アプリインストール	—	○	—	—
不許可アプリがインストールされている	○	○	○	○	不正Webサイトの閲覧*	—	○	—	—
指定したアプリがインストールされていない	○	○	○	○	タイムゾーンの変更	—	○	—	—
LanScope An Clientのバージョンが最新ではない	○	○	○	—	SDカードの抜き差し	—	○	—	—
設定日数以内でリース切れになる	○	○	○	○					
位置情報設定が無効になっている	—	○	○	—					
パスワードポリシーの非準拠	○	○	—	—					
パスワードロックがオフになっている	○	—	—	—					
Jailbreak・root化されている	○	○	—	—					
リモート操作が実行できない状態になっている	—	○	○	—					
SIMカード挿入状態の変化	○	○	—	—					
OSバージョン指定範囲外になっている	○	○	—	—					

※ Android 6.0以降は未対応

PICK UP

iOSの利用ログで費用対効果を把握!

iOSデバイスでも利用ログの取得が可能になりました。電源ON/OFFではなく、実際に利用している時間を把握できるので、使われていないデバイスは回収し、利用頻度の高い部門や利用者、店舗に再貸与するなど、費用対効果の見える化とIT資産の最適な配置ができます。



User's voice

導入デバイス・業務アプリの投資対効果の把握に成功! 報告に役立つ数値がレポートで一目瞭然。

Androidスマートフォンを導入する際に、一番の課題だったのが投資対効果の把握です。アプリの活用レポートは、デバイスや業務アプリが有効活用できているかが視覚的に分かり、報告時にも役立っています。私的利用が多い社員には注意を促すことで、改善を図っています。

「自動化」でデバイス管理にかかる工数を削減します。

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



トリガー

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

アクション

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

トリガー・アクション一覧 レシピ

	設定可能なトリガー			
	iOS	Android	Windows	macOS
リモートロックの実行が成功した	○	○	○	○
An クライアントがインストールされた	○	○	○	×
パスワードポリシーに準拠していない	○	○	×	×
デバイスが管理外になっている	○	×	○	○
LanScope An 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	○	○	○	○
指定したアプリがインストールされている	○	○	○	○
指定したアプリがインストールされていない	○	○	○	○
パスコードロックの設定がオフになっている	○	×	×	×
デバイスが不正に改造されている (Jailbreak/root化)	○	○	—	—
iOSのバージョンが指定した範囲外になっている	○	—	—	—
Androidのバージョンが指定した範囲外になっている	—	○	—	—
SIMカードが抜き差しされた	○	○	×	—
デバイスの設定がリモート操作の実行条件を満たしていない	×	○	○	×
もうすぐリース切れになる	○	○	○	○
ログが取得されない設定になっている	×	○	—	—
空き容量が不足している	○	○	○	○
新規プロファイルがインストールされた	○	—	—	○
新しくアプリがインストールされた	×	○	×	×
指定したアプリが実行された	×	○	×	×
不正なWebサイトが閲覧された	×	○*	×	×
SDカードが抜き差しされた	—	○	×	×
タイムゾーンが変更された	×	○	×	×
位置情報	×	○	○	×
任意のタイミング	○	○	○	○
定期的に行う	○	○	○	○

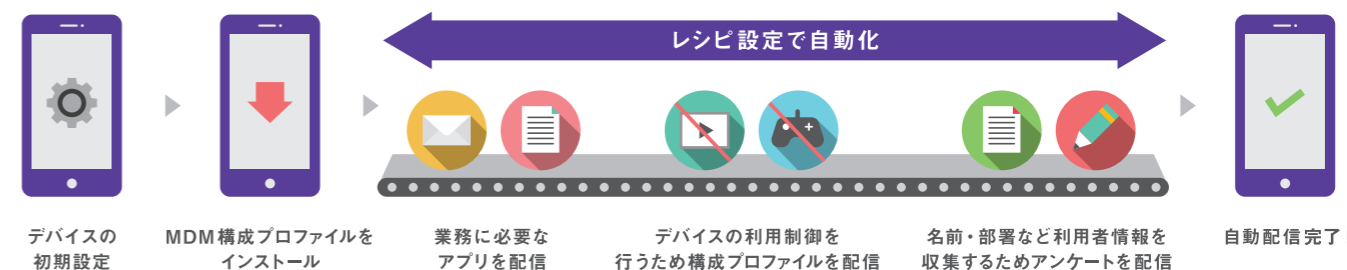
* Android6.0以降は未対応です。

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

おすすめ! iPhone、iPadのキッティング業務を自動化

Anがインストールされたら、業務用アプリや構成プロファイルを自動配信!

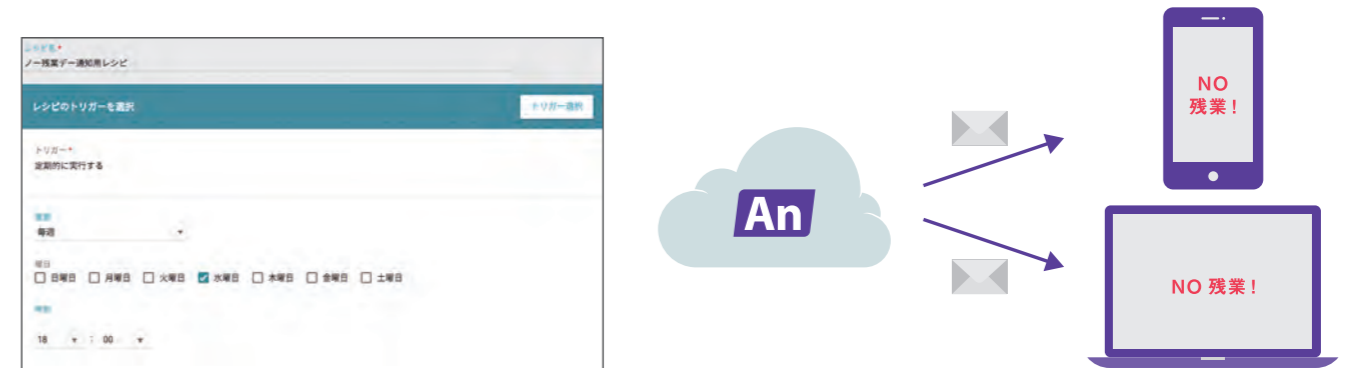
従来はMDM構成プロファイルをインストール後、別途デバイスに対して業務アプリや構成プロファイルの配信設定を行う必要がありました。レシピ機能を利用すれば、MDM構成プロファイルがインストールされたら、業務アプリや構成プロファイルを自動配信できます。



おすすめ! 従業員への通知業務を自動化

毎週水曜日の18時に「ノー残業デー」推進のメッセージを自動配信!

毎日、毎週、毎月の単位で定期的に指定したメッセージを配信できます。その他にも定期的に従業員に、デバイス利用者の変更や部署異動の状況などをヒアリングしている業務があれば、レシピを利用して自動化することができます。



PICK UP

スポット対応の業務を2回目から自動化!

特定のデバイスに対して行ったアクションを、レシピとして保存できます。2回目からは設定した条件でアクションが自動実行されるので、手間のかかる作業を繰り返す必要はありません。



User's voice

LanScope Anは
インストールが簡単!
デバイスのキッティングにも大きく貢献!

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

DEP・VPPの利用で、より幅広いiOSデバイス管理を実現します。

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

構成プロファイル管理

構成プロファイルを利用して、App Storeやカメラ、Safariなどの利用制限、Wi-FiやVPNなどの工数のかかる各種設定を複数のデバイスに一括で配信・適用ができます。インストールした構成プロファイルをアンインストールすることもできるため、遠隔で柔軟に設定変更が可能です。



Device Enrollment Program (DEP)

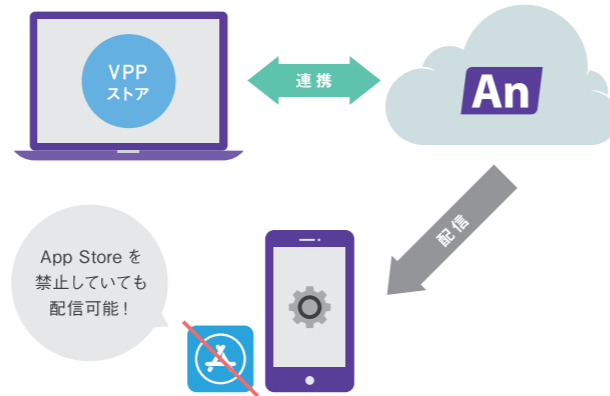
デバイスを自動的にMDMの管理下に配置でき、デバイス登録に必要な工数を削減できます。また監視モードを自動適用できるため、MDM構成プロファイルの削除を禁止したり、VPPを利用したApp Storeアプリのサイレントインストールが可能になるなど、より幅広い管理を実現できます。



Volume Purchase Program (VPP)

VPP (Volume Purchase Program) ストアで購入した無償・有償アプリをデバイスに配信できます。さらにApple IDを設定していないデバイス、App Storeを禁止しているデバイスに対しても配信が可能です。

※ デバイスベース方式に対応しています。
※ オプション機能です。



User's voice

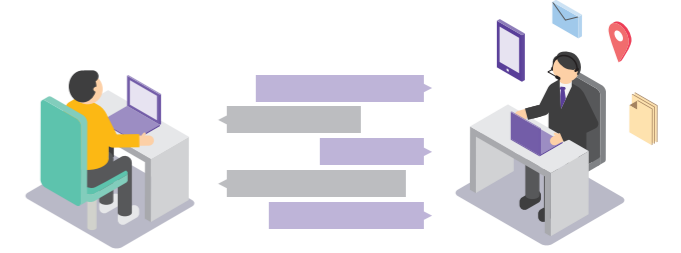
VPPを利用して、業務に必要なアプリのみを一括配信! 店舗に備え付けのiPad1,500台を2人で一元管理。

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

継続利用率90%以上! 充実のサポート体制でお客様を支援

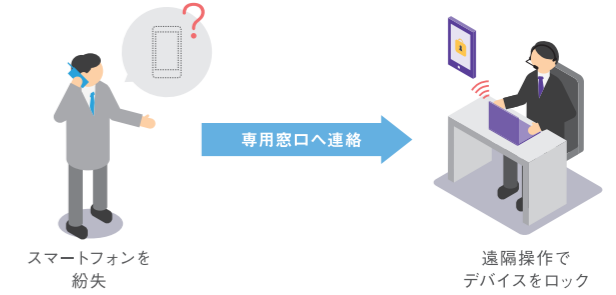
ヘルプデスクサービス

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



24時間365日対応 紛失サポートサービス(オプション)

紛失に気付いたのが深夜だった時、会社と連絡が取れなかった時など対応が遅れる程、情報漏えいのリスクは高まります。本サービスは専用窓口にて電話をいただくと、スタッフがリモートロックもしくはワイプの実行を代行します。



ご検討中のお客様向けコンテンツ

オンラインデモサービス

TEL 03-5460-1372

[受付時間] 9:00~18:00 [営業日] 月~金曜日 ※土日祝日および当社規定の休日を除く。

こんな方におすすめ!!

- 実際の画面を見てみたいけど検証まではちょっと...
- デモを見たいけどあまり時間がない...
- なかなかセミナーに参加できない...

オンラインデモサービスとは...

自席で実際の画面をご覧いただきながら専任スタッフがお電話で、製品をご紹介! 搭載機能はもちろん、どのように管理・活用頂けるのかをご理解いただけます。「実際に操作しながら教えてもらえるので、わかりやすい!」とご好評いただいています。



資料ダウンロード

導入時にご検討いただく際の各種資料をダウンロードいただけます。



60日間無料体験

LanScope Anを今すぐお試しください。60日間無料体験をご用意しています。



簡単お見積

LanScope Anの価格を簡単にご確認いただけます。

<https://www.lanscope.jp/an/>

LanScope An

検索