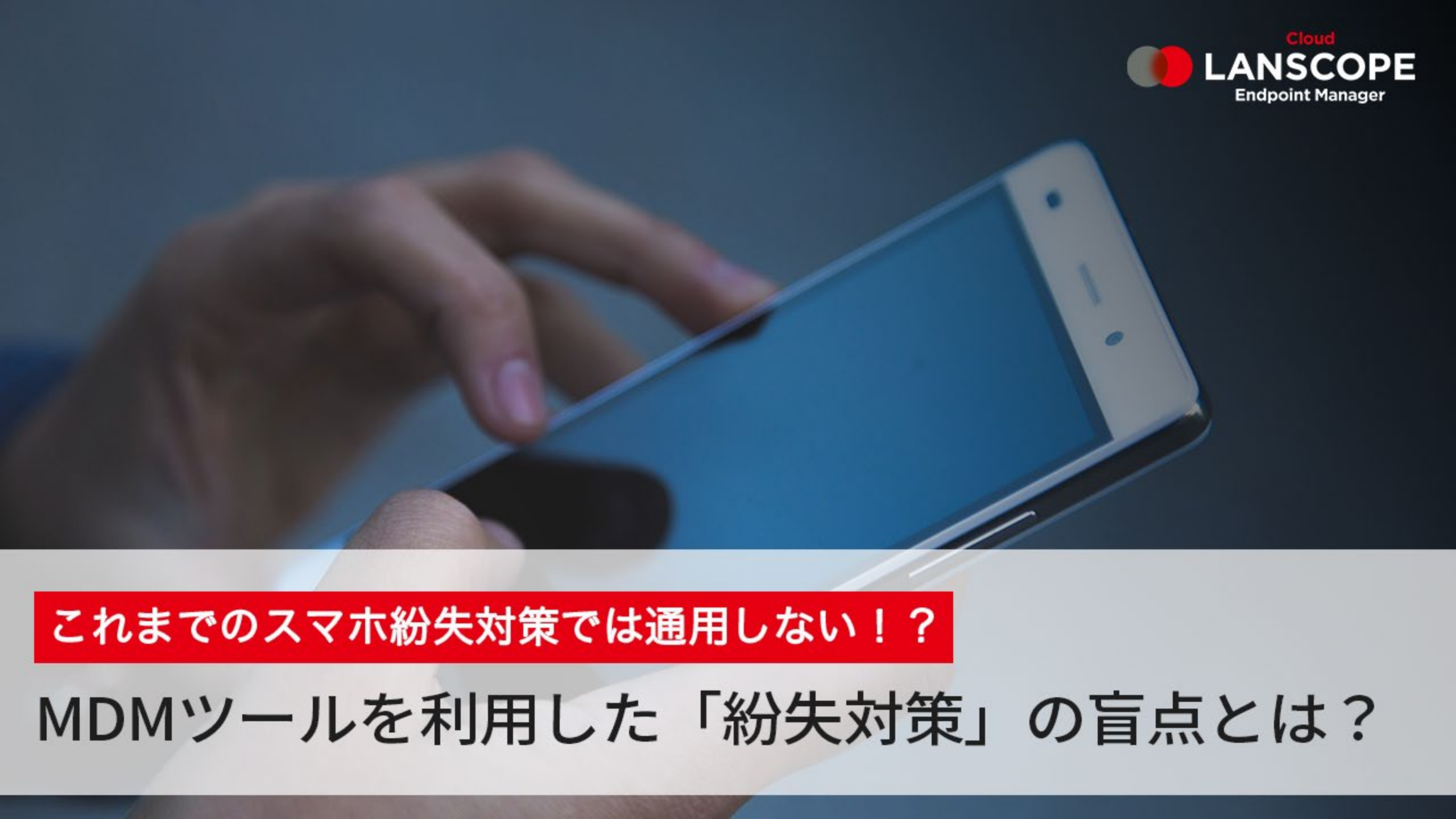




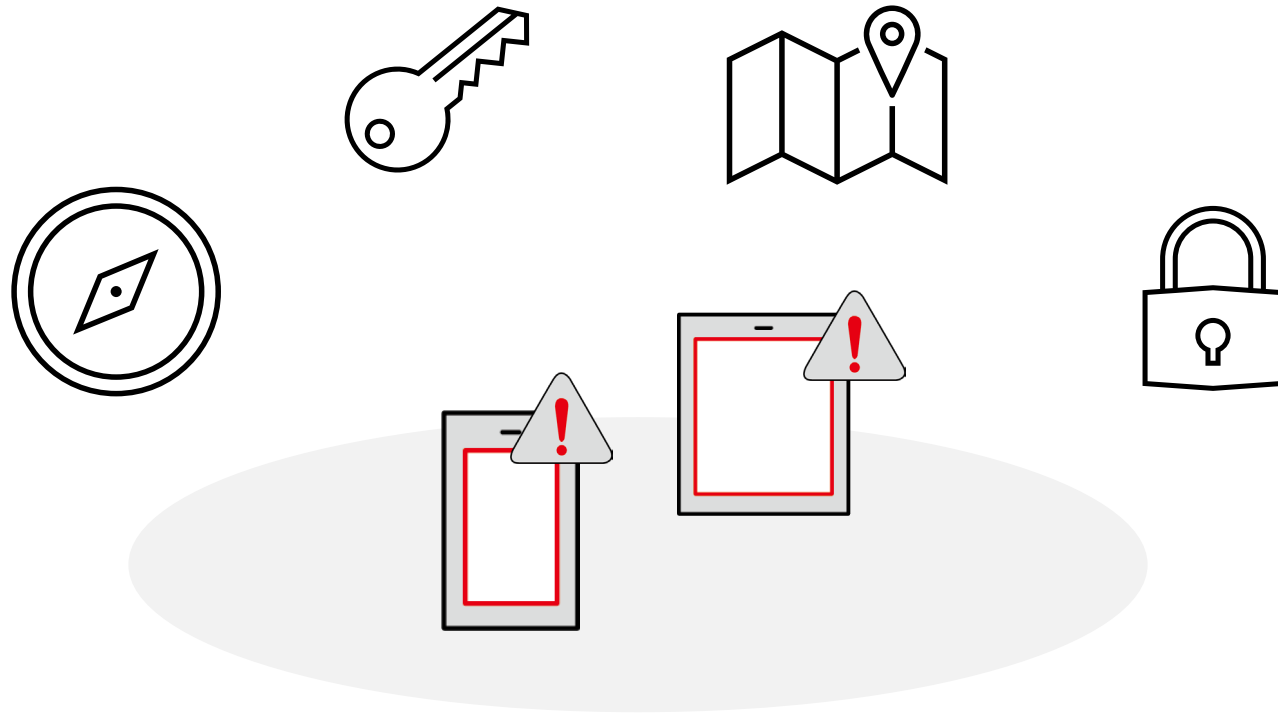
これまでのスマホ紛失対策では通用しない！？

MDMツールを利用した「紛失対策」の盲点とは？

01

モバイルデバイスの紛失対策

モバイルデバイスは持ち運びが容易なため、紛失のリスクが高くなります
そのため、基本的なセキュリティ対策として紛失対策が重要です



紛失は10人に1人が経験！位置情報の取得で3割が発見に成功！

図1 業務用スマートデバイスで以下の経験はありますか？（MA/n=400）※1

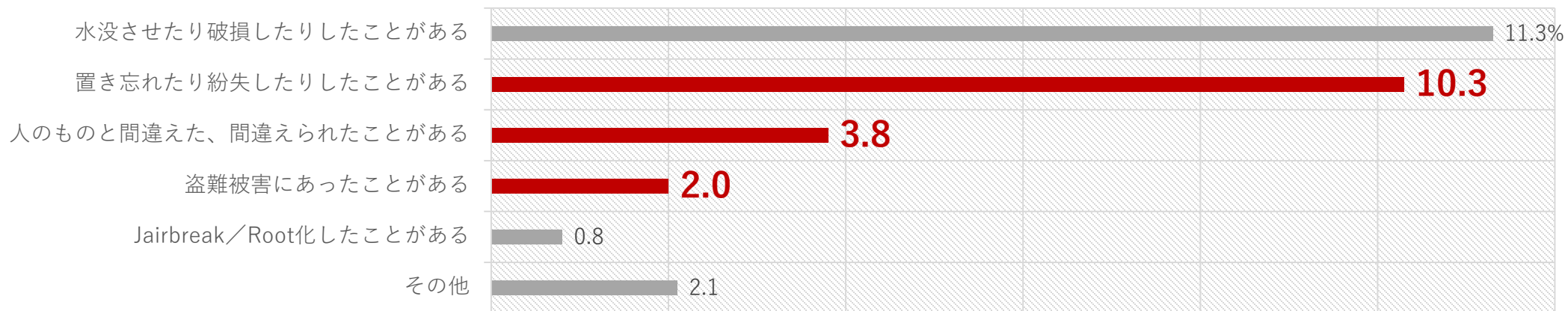
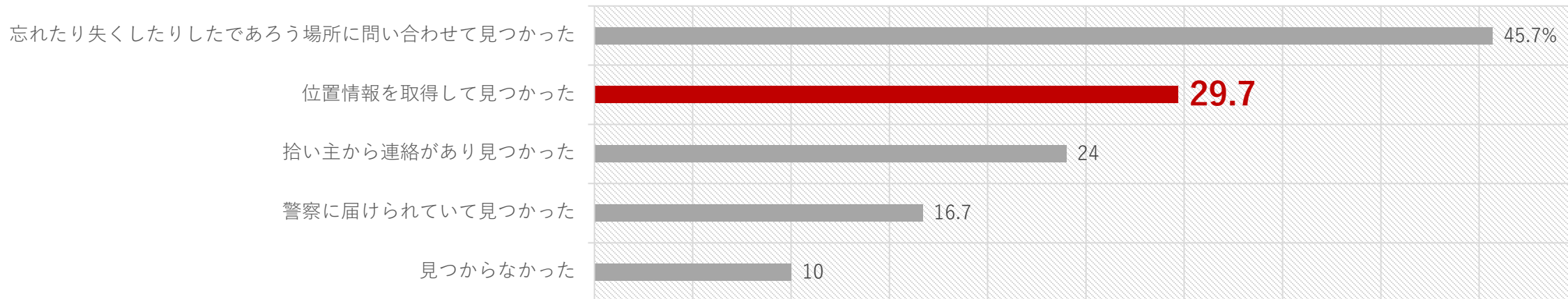


図2 スマートデバイスを忘れたり失くしたりした際、どのようにして見つかりましたか。（MA/n=300）※2



※1 「30代男女のビジネスパーソン600人に聞いた！業務用スマートデバイスの利用実態調査」 エムオーテックス株式会社

※2 「スマートデバイスの紛失実態調査（紛失経験のあるビジネスパーソン300名への調査）」 エムオーテックス株式会社

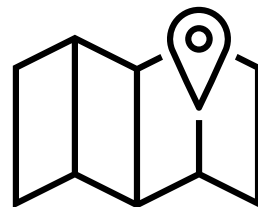
紛失時に備えた事前の対策と、紛失が発生した場合に被害を最小限に抑えるための事後対策が求められます

事前対策



パスワードポリシー

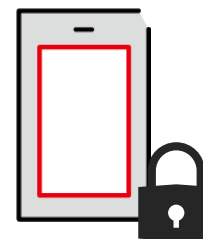
デバイス紛失時にパスワードが設定されていない、または簡単なパスワードが設定されている場合、第三者に容易にロックを解除されてしまいます。紛失時に備え、パスワードの設定を強化しておくことが重要です。



位置情報の取得

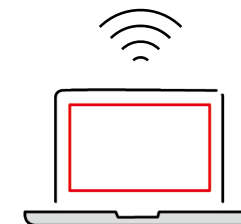
万が一デバイスを紛失した際に、紛失場所を特定して検索できるように位置情報の取得設定を有効にしておきます。

事後対策



リモートロック

遠隔でデバイスをロックし、第三者に拾われて中身を見られないようにします。ロック解除を防止するため、パスワードの再設定やロック解除の禁止も同時に行います。



リモートワイプ

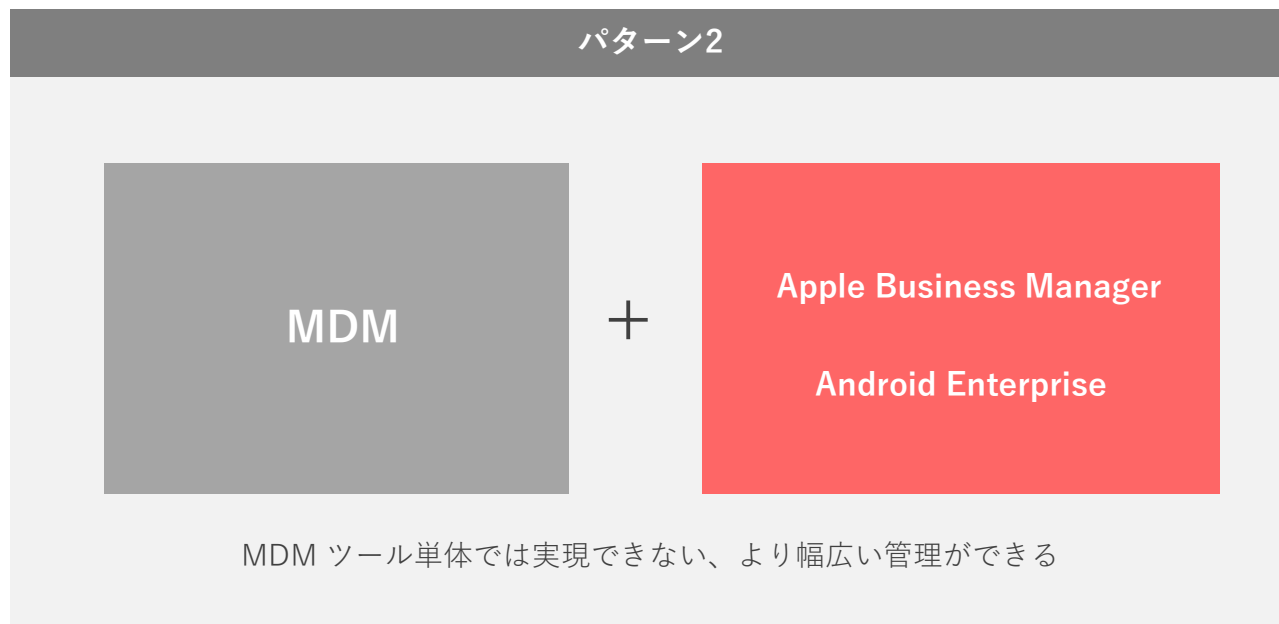
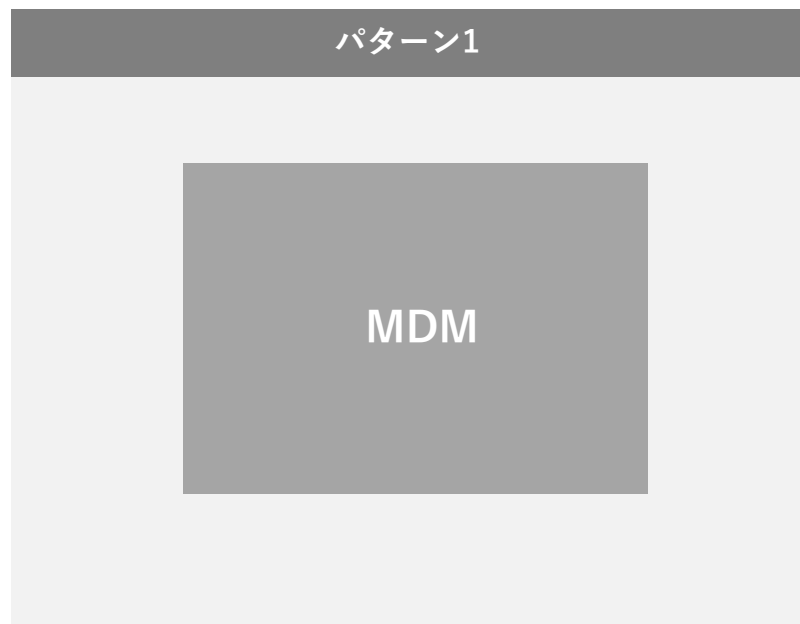
遠隔でデバイス内のデータを消去します。紛失時にデバイスの回収が困難な場合、リモートワイプを実行して情報漏洩のリスクを防ぎます。

iOS・Androidのモバイルデバイス管理は基本的にMDMツールで行います
紛失対策に必要な位置情報の取得、リモートロック・ワイプ、パスワードポリシー機能も備えています

MDM ツール単体の主な機能一覧

機能	iOS	Android
ハードウェア情報の取得	○	○
インストールアプリ情報の取得	○	○
メッセージ・アンケートの配信	○	○
位置情報の取得	○	○
リモートロック・ワイプ	○	○
パスワードポリシー	○	○
アプリ利用ログの取得	×	○
電話利用ログの取得	×	○
プロファイル配信	△	—
アラート設定	○	○
レポート機能	○	○

モバイルデバイス管理は、MDM ツール単体で行うか、
MDM + Apple Business Manager または MDM + Android Enterpriseで行うかの二択となります



紛失対策においては、MDM ツール単体では実現できないことが増えており、
Apple Business Manager・Android Enterpriseの利用が必須となってきています

02

Apple Business Manager ・ Android Enterpriseが 紛失対策に必要な理由

Apple Business Manager (ABM) ・ Android Enterprise (AE) は Apple ・ Google が提供し、
MDM ツールと連携して利用するプログラムで、より高度なデバイス管理を実現します

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)

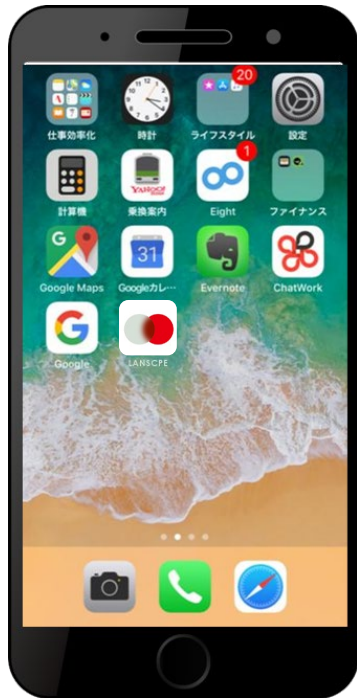
Android Enterprise (AE)

- ✓ MDM と組み合わせて利用する必要がある
- ✓ iOS は利用有無の選択が可能、**Android は Android Enterprise の利用が必須**
- ✓ 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 ツールと連携することで情報漏洩に繋がる機能を制限することが可能

紛失対策においては、紛失モードを利用すると位置情報の強制取得などより強固な対策を実行できます

Apple Business Manager (ABM)



<プロフィールの設定・制御>

- iCloudの利用制限
 - AirDropの制御※
 - App Storeの利用禁止※
 - 指定のWi-Fiのみ許可※
 - iTunesの禁止※
- #### <監視モードの自動適用>
- 紛失モードの利用
 - VPP アプリのサイレントインストール

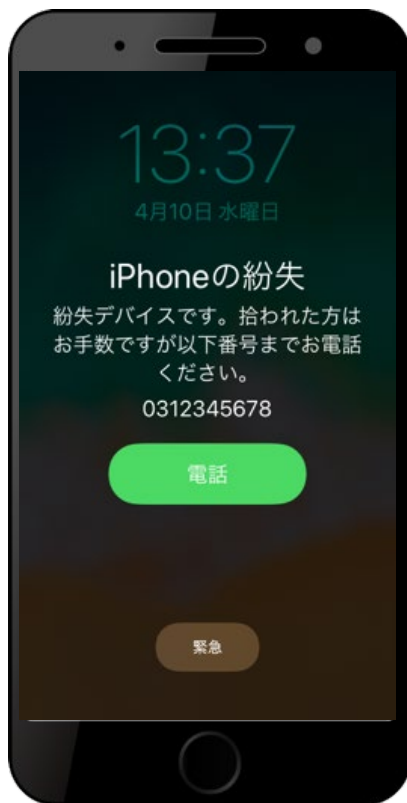
※デバイスを監視モードに設定する必要があります。

Android Enterprise (AE)



- Googleアカウント管理
- 指定のWi-Fiのみ許可
- USBの接続禁止
- 提供元不明アプリ
- 初期化禁止
- テザリング禁止
- リモート再起動
- 紛失モードの利用

Apple Business Manager (ABM) ・ Android Enterprise (AE) の 紛失モードを利用するとより強固な紛失対策が実現できます



紛失モードの主な機能

ロック解除を禁止

紛失時にリモートロックをかけてもロックが解除されると情報漏洩リスクが高くなるため、第三者によるロック解除を禁止します。

画面上へメッセージ表示

デバイスを見つけてくれた人に向けて画面に電話番号やメッセージを表示します。

位置情報の強制取得

位置情報の取得にはデバイス側での設定が必要なためデバイス側で設定変更されると、位置情報が取得できなくなります。紛失モードではデバイス側の設定に関わらず強制的に位置情報を取得できます。

※ OS によって動作は異なります。

紛失対策に必要な機能は MDM ツール単体で利用できるとなっているが
実は Apple Business Manager・Android Enterprise を利用しないと実現できない機能があります

MDM ツール単体の主な機能一覧

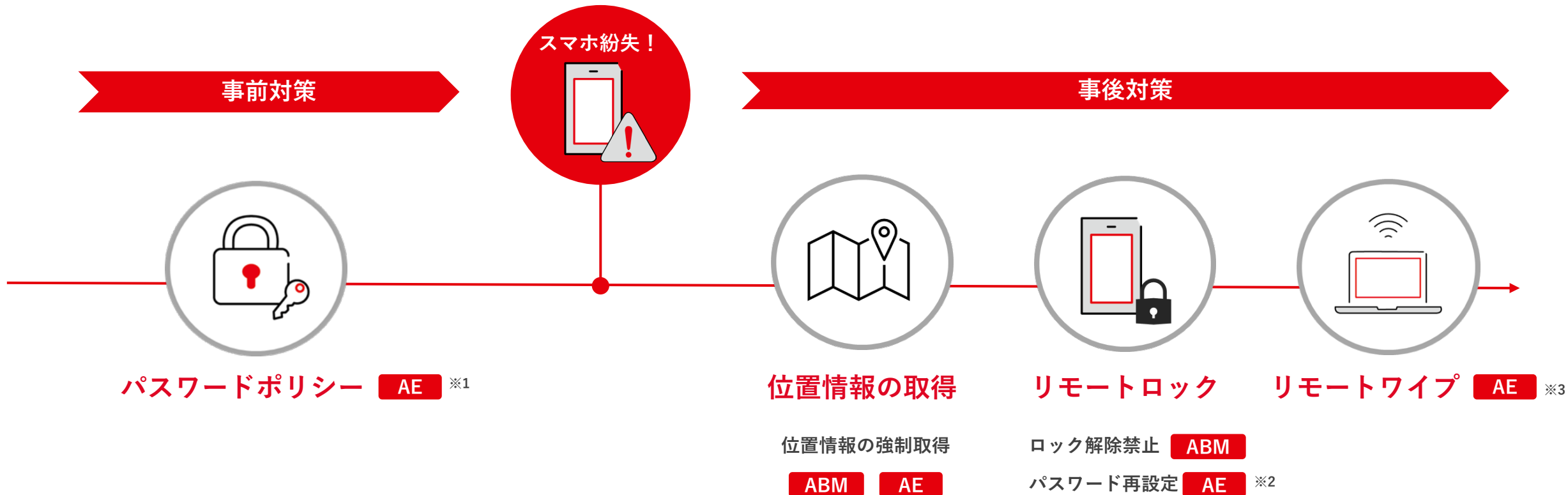
機能	iOS	Android
ハードウェア情報の取得	○	○
インストールアプリ情報の取得	○	○
メッセージ・アンケートの配信	○	○
位置情報の取得	○	○
リモートロック・ワイプ	○	○
パスワードポリシー	○	○
アプリ利用ログの取得	×	○
電話利用ログの取得	×	○
プロファイル配信	△	—
アラート設定	○	○
レポート機能	○	○

紛失対策で利用する機能の利用条件

機能	iOS	Android
位置情報の取得	位置情報の強制取得 ABM（紛失モード）必須	位置情報の強制取得 AE（紛失モード）必須
リモートロック	ロック解除禁止 ABM（紛失モード）必須	ロック時のパスワード上書き Android 11以上 AE 必須
リモートワイプ	-	Android 14以上 AE 必須
パスワードポリシー	-	Android 10以上 AE 必須

MDM ツール単体では使えない機能や、利用条件は今後増える可能性もあります

モバイルデバイスのセキュリティ対策の基本である紛失対策を確実に行うためには
Apple Business Manager (ABM)、Android Enterprise (AE) が必要となります



これからのモバイルデバイスの紛失対策には MDM ツールに加えて
Apple Business Manager (ABM) 、Android Enterprise (AE) を利用するのがベストです

iOS の場合		
機能	MDM単体	MDM + ABM
パスワードポリシー	○	○
位置情報の取得	○	○
位置情報の強制取得	×	○
リモートロック	○	○
ロック解除禁止	×	○
リモートワイプ	○	○

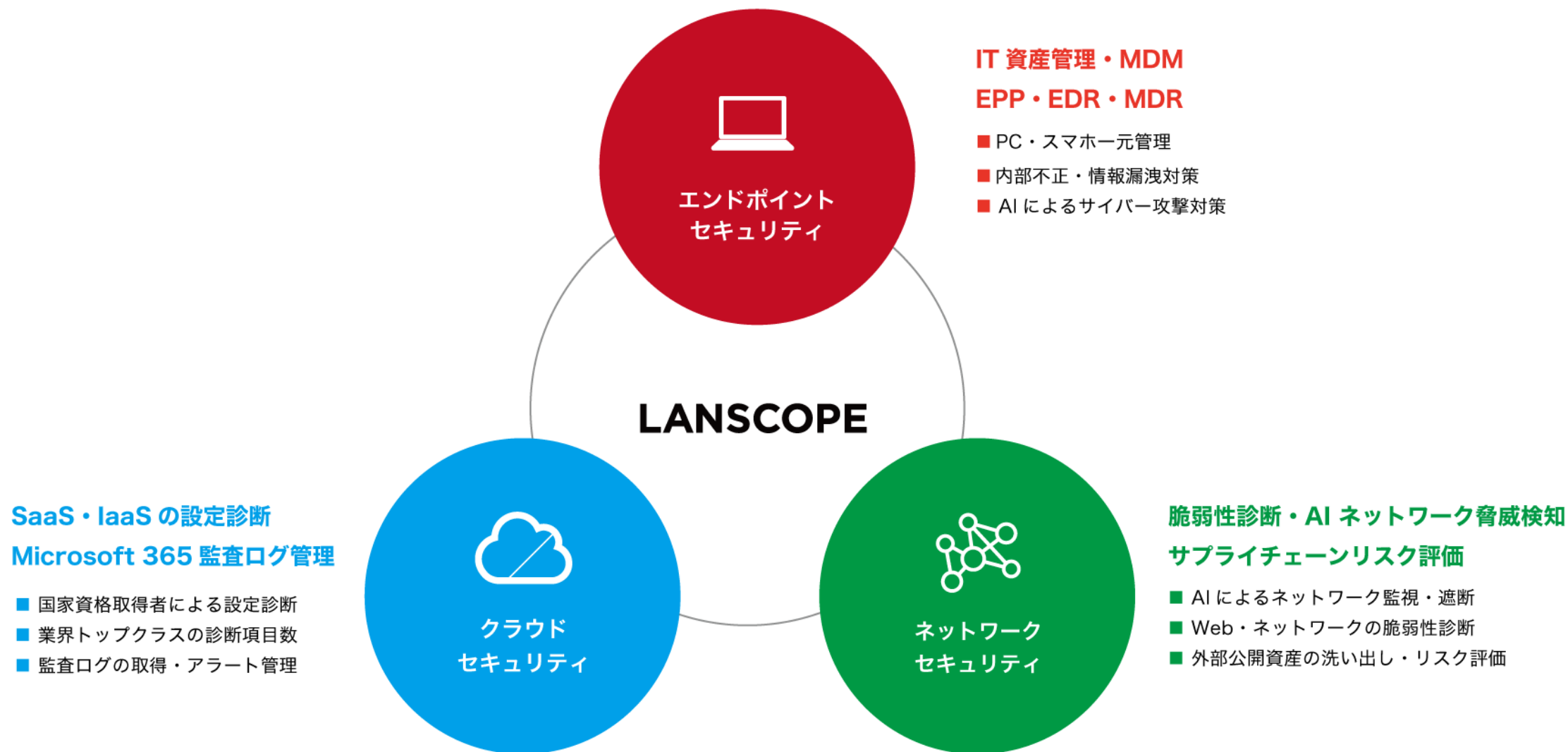
Android の場合		
機能	MDM単体	MDM + AE
パスワードポリシー	△	○
位置情報の取得	○	○
強制取得	×	○
リモートロック	△ Android 14 以上は利用不可	○
ロック解除禁止	×	○
パスワード再設定	△	○
リモートワイプ	△ Android 10 以上は利用不可	○

03

LANSCOPE を活用した紛失対策



Android 15 未満のデバイスは、Android Enterprise を利用しない場合でも、管理下に置くことができますが、パスワードポリシーやリモートワイプなど一部機能が利用できません。当該機能の利用には、Android Enterprise を利用する必要があります。また、Android 15 以上のデバイスの場合、Android Enterprise を利用しない管理ができません（サポート対象外です）。



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



エンドポイントセキュリティ



クラウドセキュリティ



ネットワークセキュリティ

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

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

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」



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。



利用者に依存しがちなパスワードの設定ルールを組織で統一

パスワードの最小文字数 *
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

パスワードの有効期間
☒ 設定する
有効期間 (日) (1 ~ 730 日) *
90

以前使用したパスワードの再使用
☒ 禁止する
再使用禁止回数 *
2回

パスワ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

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。

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。

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

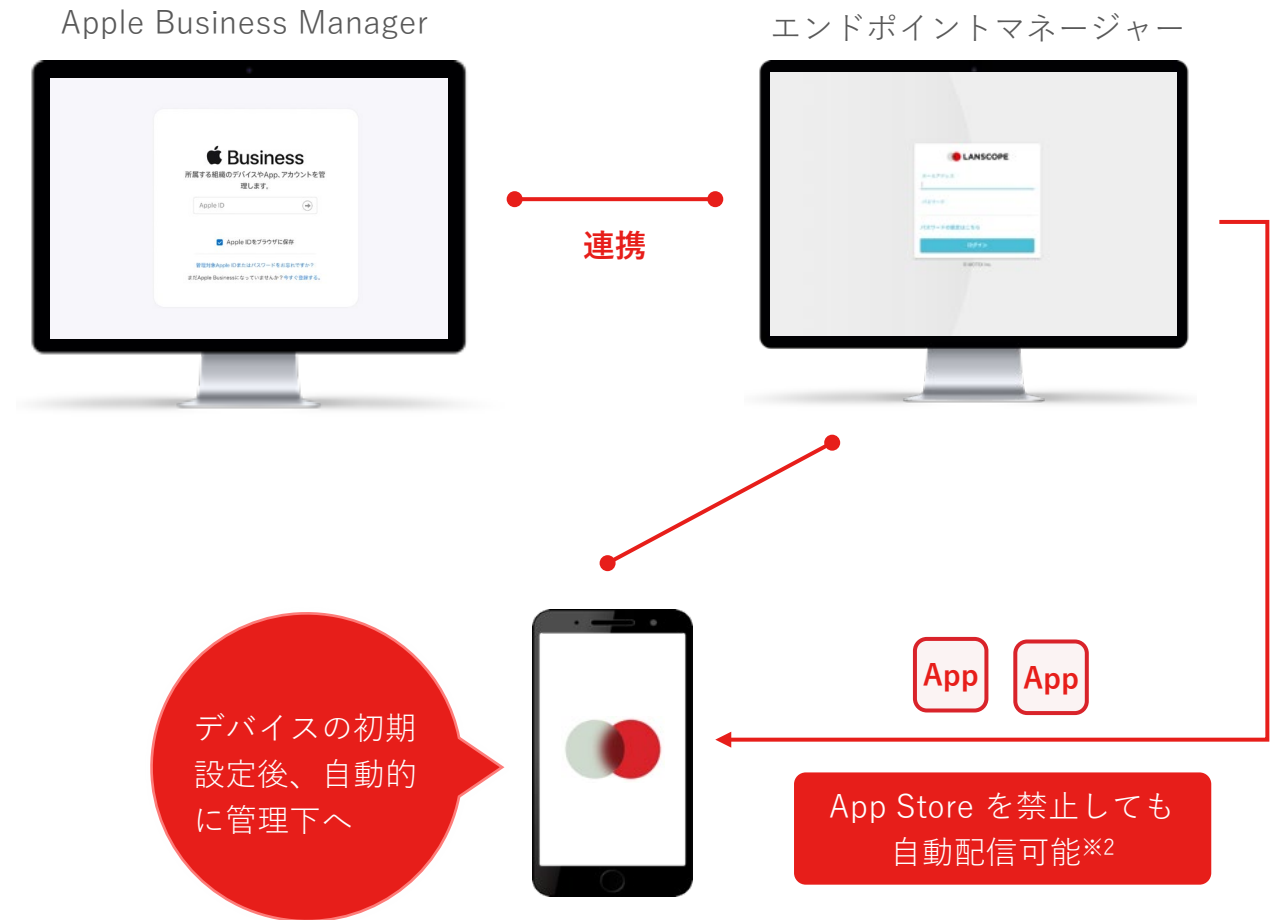
ABM はデバイスを効率的にエンドポイントマネージャーの管理下に置き、アプリの配信やデバイスの利用制御などを実現できる Apple 社が提供するプログラムです。

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、iOS のみ対応しています。

※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 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。

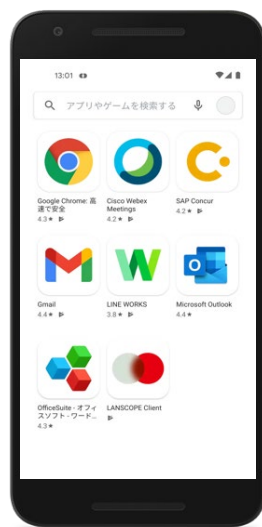
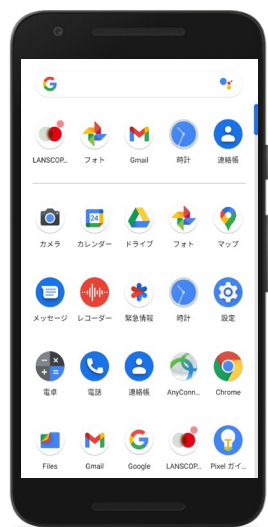
※ オプション機能です。

Full Device Management とキオスクモードの2種類から選択し、デバイスを管理下に置きます

Android 15 以降のデバイスの場合、AE の利用が必須です。Android 15 未満の場合、AE を利用しなくても管理下に置けますが一部機能が利用できません。

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。



許可したアプリのみ
Play ストアに表示

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。



60日間無料体験キャンペーン中

エンドポイントマネージャー クラウド版の体験版は、設定したポリシーや取得した情報を含め、そのまま製品版へのデータ引き継ぎが可能です。また体験版利用中も、弊社サポートセンターにお電話やメールで問い合わせが可能。体験期間中は、マニュアルやオンラインで学べるトレーニング動画も公開しています。

●各種マニュアル・問い合わせが可能



●動画で設定方法を説明

LANSCOPE クラウド版 動画でわかる使い方

初期設定手順



【初期設定手順】iOS・iPadOS 向け インストール手順（約7分）

iOS/iPadOS



【初期設定手順】iOS・iPadOS 向け 自動デバイス登録（DEP）利用時のインストール手順（約12分）

iOS/iPadOS



【初期設定手順】Android 向け インストール手順（約4分30秒）

Android



<https://go.motex.co.jp/l/320351/2017-06-21/c55z>



本資料に関するお問い合わせ

■ マーケティング本部

プロダクトマーケティング部

E-mail product@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

お電話受付時間

E-mailお問い合わせ

0120-968-995（携帯・PHSからは06-6308-8981）

9:30～12:00/13:00～17:30（平日、祝祭日除く）

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。