

ビジネス・コンシェル デバイスマネジメント ご提案資料

ソフトバンクは、お客さまのプライバシーを 最優先に考えます

ソフトバンクは、お客さまからパーソナルデータをお預かりし、
社会課題の解決や、お客さまの生活を向上するための取り組みに役立てております。
パーソナルデータの取り扱いには細心の注意を払い、適切に保護しています。

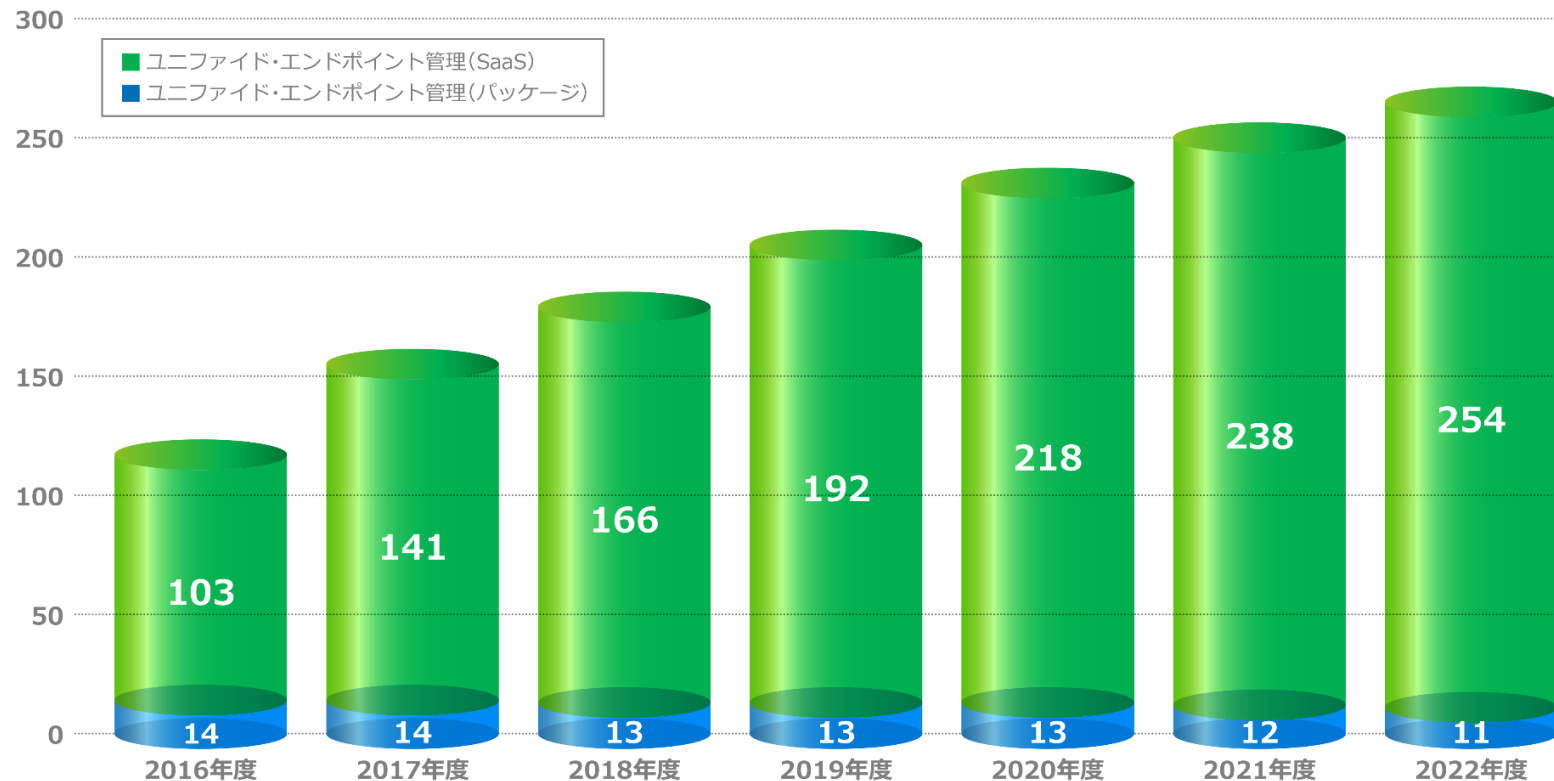
※詳細はこちら
プライバシーセンター

<https://www.softbank.jp/privacy/>

ソフトバンク株式会社

MDM（Mobile Device Management）とは
複数台のスマートフォンおよびタブレット端末をリモートで一元管理・運用できるサービス。
スマホが普及し、業務利用する企業も増えているため、
デバイスのセキュリティを担保するためにMDMを検討・導入する企業が増えています。

（単位：億円）



出展：ITR「ITR MARKET VIEW ユニファイド・エンドポイント管理市場2018」 ※2018年以降は予測値となります。

多種多様なデバイスを
社員が利用しているため
一括管理が必須



紛失や盗難、あるいは
ウイルスに感染した際の
情報漏洩対策が必要



業務利用端末のため
私的利用はさせたくない



ビジネス・コンシェル デバイスマネジメントで課題を解決

ソフトバンクが自社開発したクラウド型のMDMサービス



ビジネス・コンシェル デバイスマネジメントが 政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されました。

1400項目を超える厳しい政府の管理基準、高いセキュリティ水準を順守している証明となります。
お客様による導入検討時のセキュリティチェックの短縮・工数低減にもお役立てください。

ISMAPとは

ISMAP（Information System Security Management and Assessment Program、通称：イスマップ）は、政府が求めるセキュリティ基準を満たしたクラウドサービスを評価・登録することにより、政府のクラウドサービスの調達におけるセキュリティ水準を確保し、円滑な導入を進めることを目的とした制度です。行政機関は原則として、ISMAPに登録されたクラウドサービスから調達を行うこととされています。詳細については以下よりご確認ください。

https://www.ismap.go.jp/csm?id=cloud_service_list



レビューサイト（ITreview）でお客様より高評価を獲得

- ★ **ビジネス・コンシェル デバイスマネジメントは、ITreview※にて管理画面のわかりやすさや手厚いサポートが評価され、高評価を獲得しています。**



★★★★★ 画面レスポンスが改善された

他社MDMも複数運用したことがありますが、画面がわかりやすいと思います。また直近のアップデートでログイン後すぐに表示されるダッシュボード画面のロードが早くなりレスポンスが改善されたと思います。操作に困ったときにメールと電話でサポートが受けられますが、その品質にも満足しています。2000台近いiOSデバイスの運用管理、キッティング工数を削減することができました。デバイス単価での課金なので、運用状況に応じてコストコントロールができることもメリットだと思います。



★★★★★ MDMに非常に有用です。

情報システム部がないので総務部のスタッフが兼任しており、IT機器の管理は非常に大変です。営業担当者が使用するiPadを250台ほど管理していますが、機器情報、使用者情報を登録できて管理がしやすいです。管理画面でセキュリティのチェックやインストールしているアプリが確認でき、監視面でも役立っています。1つの管理画面で全部、個別のiPadに設定を施せるので、都度、実物を本社に送る必要がなくなるのもいいと思います。キャリア純正サービスというのもポイントでした。

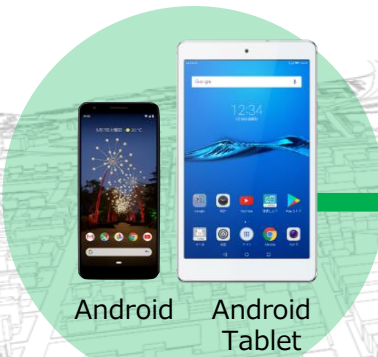


他のレビューを読みたい方はこちら (<https://www.itreview.jp/products/business-concier-device-management/reviews>)

※ ITreviewとは、アイティクラウド株式会社が運営する、ビジネス向けソフトウェア・クラウドサービスのレビューが集まるWebサイトです。現在、約4万件もの国内レビューが掲載されており、実際の利用ユーザの口コミ評価をもとに検討製品が自社にマッチするのかが判断することができます。

特徴①デバイスとユーザの一元管理

モバイルとユーザを一括管理でき、簡易な導入と運用が可能



デバイスを回収することなくリモートからセキュリティ設定可能

セキュリティ設定

パスワードの設定
アプリやカメラ、テザリングの制限など
リモートから設定することが可能



ウイルス対策

Android、PCにはトレンドマイクロ社の
アンチウイルス機能を提供



認証

SaaSログイン時の多要素認証
私用デバイスからのアクセスも制御
することが可能



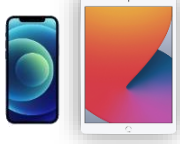
セキュリティだけではないリモート機能および代行操作により
デバイス運用の負荷を軽減

業務に必要なアプリを配信

ステータスにより配信状況も確認可能



※画像はiOS



iOS

アプリ配信
+ アプリカタログ



Android

アプリ配信
+ Playストア
ホワイトリスト化

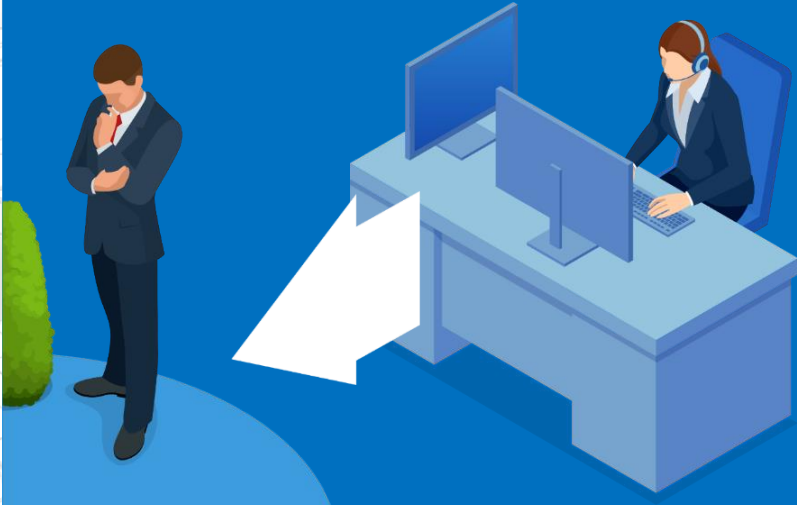


PC

ソフトウェア
配信

万が一に備えて
24時間365日のヘルプデスクも完備※

紛失、盗難時の情報漏洩をふせぐため
リモートロック、ワイプ操作も代行



提供サービス一覧（基本サービス）

	提供機能	iOS	Android	4Gケータイ	PC	
					Windows	Mac
基本サービス	[1] ダッシュボード機能	○	○	○	○	○
	[2] グループ管理機能	○	○	○	○	○
	[3] デバイス利用者情報登録	○	○	○	○	○
	[4] 言語設定機能（日/英）	○	○	○	○	○
	[5] 対象デバイスの設定情報収集	○	○	○	○	○
	[6] デバイス遠隔設定	○	○	○	○	—
	[7] かんたん一括設定	○	—	—	—	—
	[8] アカウント一括登録設定	○	—	—	—	—
	[9] デフォルトプロファイル配信機能	○	—	—	—	—
	[10] セキュリティポリシー設定	○	○	○	○	—
	[11] MDMプロファイル削除検知機能	○	—	—	—	—
	[12] プロビジョニングプロファイル配信	○	—	—	—	—
	[13] アプリケーション制御	○	○	○	○	—
	[14] 位置情報取得	○	○	○	○※1	—
	[15] root化検知	—	○	—	—	—

	提供機能	iOS	Android	4Gケータイ	PC	
					Windows	Mac
基本サービス	[16] アンチウイルス	—	○	○	○	○
	[17] Managed Apps機能	○	○	○	—	—
	[18] BizConPlace機能	○	○	○	—	—
	[19] BC Location機能 ※4 ※5	○	—	—	—	—
	[20] PC向け遠隔消去機能	—	—	—	○	—
	[21] Automated Device Enrollment (ADE (旧DEP)) / ゼロタッチ対応	○	○	—	—	—
	[22] Android Enterprise機能	—	○	—	—	—
	[23] アプリカタログ機能	○	—	—	—	—
	[24] 強制OSアップデート機能	○	△※1	—	—	—
	[25] 遠隔消去・ロック※2	—	—	—	—	○
	[26] 証明書発行/配布機能※3	○	○	—	○	—
	[27] シングルサインオン機能※3	○	○	○	○	○

※1 Android Enterprise（Fully managed device）でのみ
アップデートの実行タイミングを設定可能

※2 本機能は、M62/M63から始まるDMコードの環境のみ利用可能です。

※3 本機能は、M6から始まるDMコードの環境のみ利用可能です。
※4 本機能は、M7から始まるDMコードの環境では使用できません。
※5 本機能は、オプションの申し込み（無料）が必要となります。

	提供機能	iOS	Android	4Gケータイ	PC	
					Windows	Mac
基本サービス	[28] 紛失時リカバリーサービス					
	紛失モード	○	—	—	—	—
	遠隔消去・ロック	○	○	○	—	—
	パスコード一時解除	○	○	○	—	—
	ヘルプデスク	○	○	○	—	—

提供サービス一覧（オプションサービス）

	提供機能	iOS	Android	4Gケータイ	PC	
					Windows	Mac
オプションサービス	[1] Webフィルタリングサービス	○	○	—	—	—
	[2] Managed Appsサービス（PC）	—	—	—	○	—
	[3] シングルサインオン機能※1					
	SSO無制限	○	○	○	○	○
	多要素認証	○	○	○	○	○
	多要素認証Pro	○	○	○	○	○
	ライフサイクル管理	○	○	○	○	○
	[4] Managed Apps容量拡張	○	○	—	—	—
	[5] デバイスコントロール for Microsoft 365	○	—	—	—	—
	[6] PC操作ログ	—	—	—	○※2	—

※1 本機能は、M6から始まるDMコードの環境のみ利用可能です。

※2 本機能は、M5、M6から始まるDMコードの環境のみ利用可能です。

1デバイスから申込可能、無料トライアル実施中

デバイス	基本サービス＋紛失時リカバリー (月額)
iOS	500円/ID
Android	500円/ID
4Gケータイ	200円/ID
PC(Windows)	400円/ID
PC(Mac)	400円/ID

※オプションサービスは基本サービスのデバイス数と同数でのご契約となります。
※最低利用期間は 1 カ月となります。
※月額使用料：初月無料です。
※表示金額は全て税抜です。
※無料オプションサービスについてもご利用時にはお申込みが必要となります。

1デバイスから申込可能、無料トライアル実施中

デバイス	オプションサービス（月額）						
	シングルサインオン機能オプション				Web フィルタリング	Managed Apps 容量拡張	PC操作 ログ
	SSO 無制限	多要素 認証	多要素 認証Pro	ライフサイクル管理			
iOS	400円/ID	500円/ID	1,000円/ID	1,000円/ID	200円/ID	100円/ID	—
Android							—
4Gケータイ					—	—	—
PC (Windows)					—	—	500円/ID
PC (Mac)					—	—	—

※オプションサービスは基本サービスのデバイス数と同数でのご契約となります。
※最低利用期間は1カ月となります。
※月額使用料：初月無料です。
※表示金額は全て税抜です。
※無料オプションサービスについてもご利用時にはお申込みが必要となります。

■シングルサインオン機能
※ご契約はデバイス数単位となります。
※Mac、4Gケータイにつきましては、デバイス証明書を利用したデバイス認証はご利用いただけません。
※オプションサービスは基本サービスの契約ID数と同数でのご契約となります。
※シングルサインオン機能はM6から始まるDMコードにてご利用いただくことができます。
※「ライフサイクル管理」には「SSO無制限」が含まれております。（セットでのご提供のみ）
※多要素認証と多要素認証Proは併用できません。

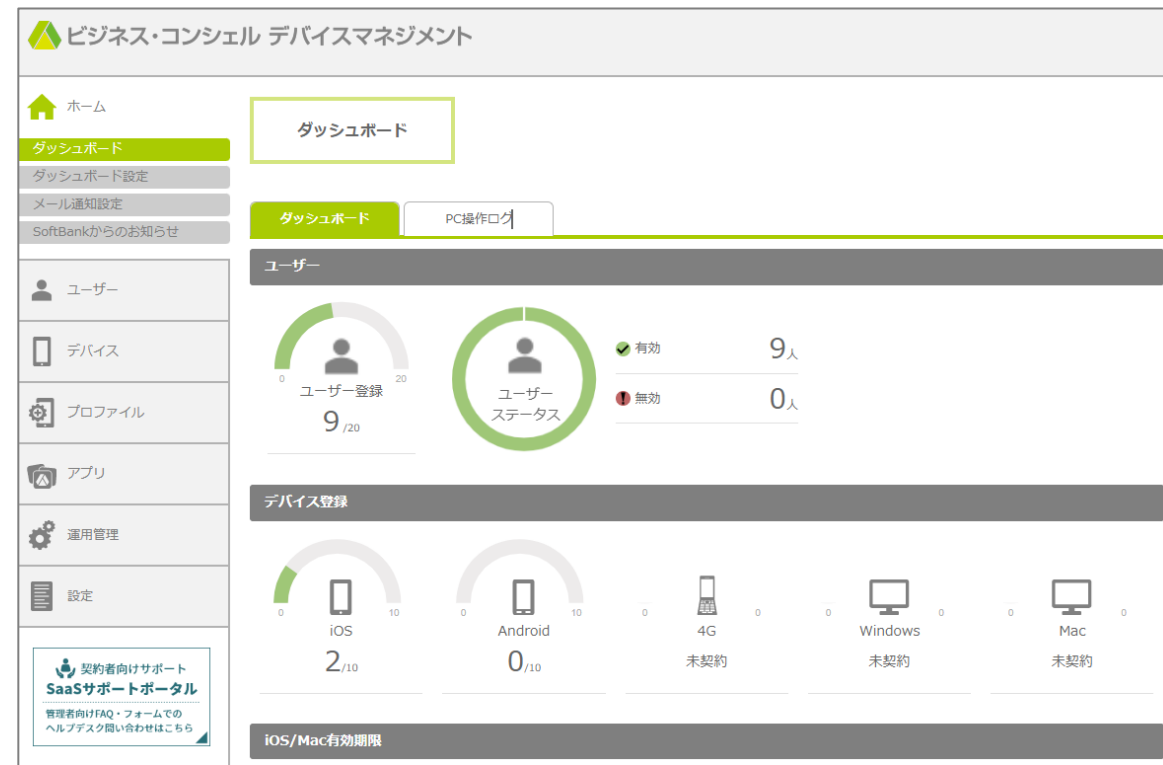
基本サービス [デバイス共通機能]

デバイス情報のサマリーを一覧で表示

デバイスの状況をわかりやすいグラフで表示し、ステータス確認が可能。

表示項目

- デバイス登録
- ステータス
- セキュリティポリシー違反…など



ユーザ登録をすることで、ユーザと利用デバイスを紐付けて管理可能

BCDM管理画面

ユーザー詳細

登録済のユーザー情報を表示します。

BCDM太郎の情報

ユーザーID	氏名	メールアドレス
bcdm.taro@test.com	BCDM太郎	bcdm.taro@test.com

ユーザー情報

SaaSアプリ

デバイス

所属グループ

SaaSアプリ

ユーザーが利用可能なアプリケーションがわかる

デバイス

ユーザーが利用しているデバイスがわかる

所属グループ

ユーザーが所属しているグループがわかる

言語設定	日本語
権限	ユーザー管理者
レポート	表示
国・地域	日本
ステータス	有効 詳細ステータス: ACTIVE
社員番号	

ユーザ情報を別で管理する必要がなく、BCDMひとつでユーザ情報もデバイス情報も管理ができる

表示項目

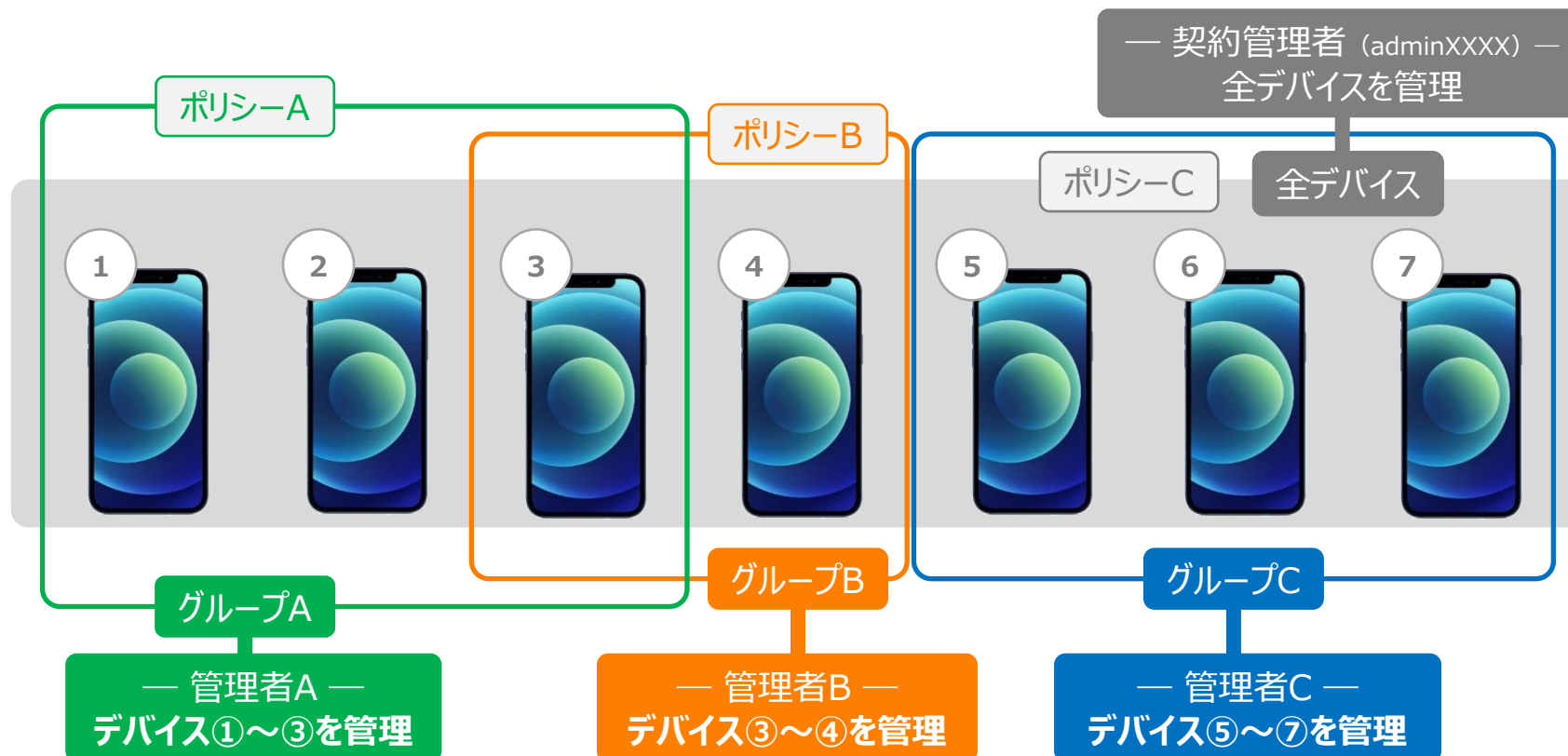
- 氏名
- ユーザのアカウントID/パスワード
- 連絡先
- デバイス情報
- 所属グループ
- 利用可能SaaSアプリなど

デバイスをグループごとに管理可能

1デバイスに複数のグループ設定ができ、グループごとに管理者の設定が可能です。

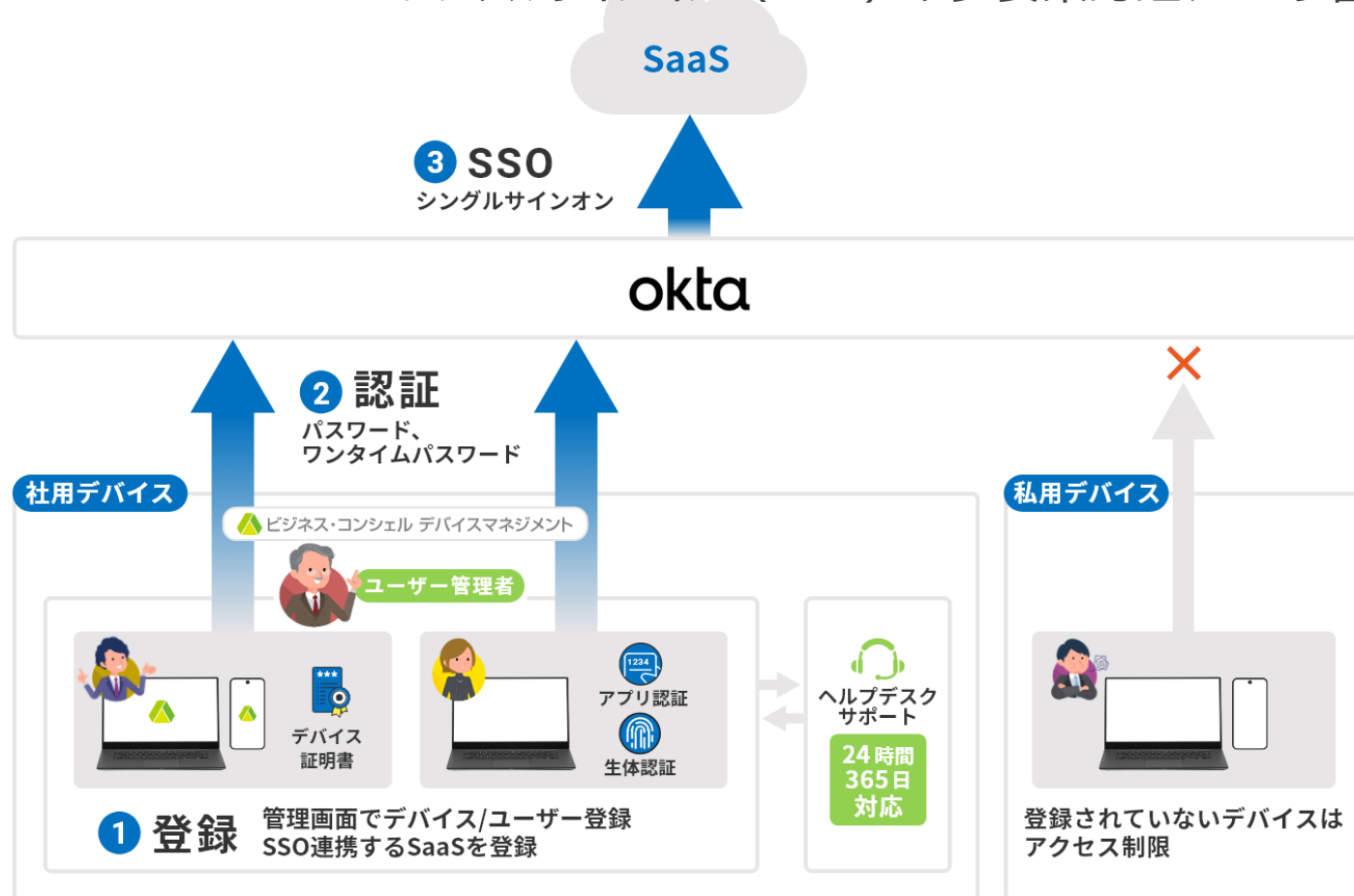
登録グループごとにセキュリティポリシーの設定が可能です。

登録グループは1,000グループ、階層は4階層まで設定可能です。



SaaS利用時に必要となる、安全な認証と便利なSSOを提供します

BCDMのシングルサインオン機能はOktaの機能を実装しており、
Oktaのシングルサインオン（SSO）や多要素認証、ユーザ管理などの機能をご利用いただけます



■ 基本機能

- 指定の5つのSaaSでシングルサインオン
- デバイス証明書によるアクセス制御
- Okta Verifyによるワンタイムパスワード
- パスワード・アクセスポリシーの設定など

※指定の5つのSaaSは Google Workspace、Zoom、LINE WORKS、PrimeDrive、BCDM となります。

事 項	詳 細
利用環境	・本機能は、M6から始まるDMコードの環境のみ利用可能です。
利用できるデバイス	・iOS,Android（Android Enterprise且つOS7.0以上）,Windowsとなります。
利用価格	・基本サービスに含まれる為、無料となります。
証明書の失効方法	・リモートワイプもしくはデバイス削除を実施すると、自動で証明書が失効されます。また証明書削除画面にて証明書削除を実施された場合も証明書が自動で削除されます。
証明書の更新方法	・更新のタイミングで自動で発行、削除が実施されます。
証明書の有効期限	・3年+1か月となります。
CA局証明書の有効期限	・2029年3月12日までとなります。（弊社対応により新規CA局を設置します。）
OCSP※1の利用	・利用可能です。
CRL※2,OCSP反映間隔	・最大で24時間となります。

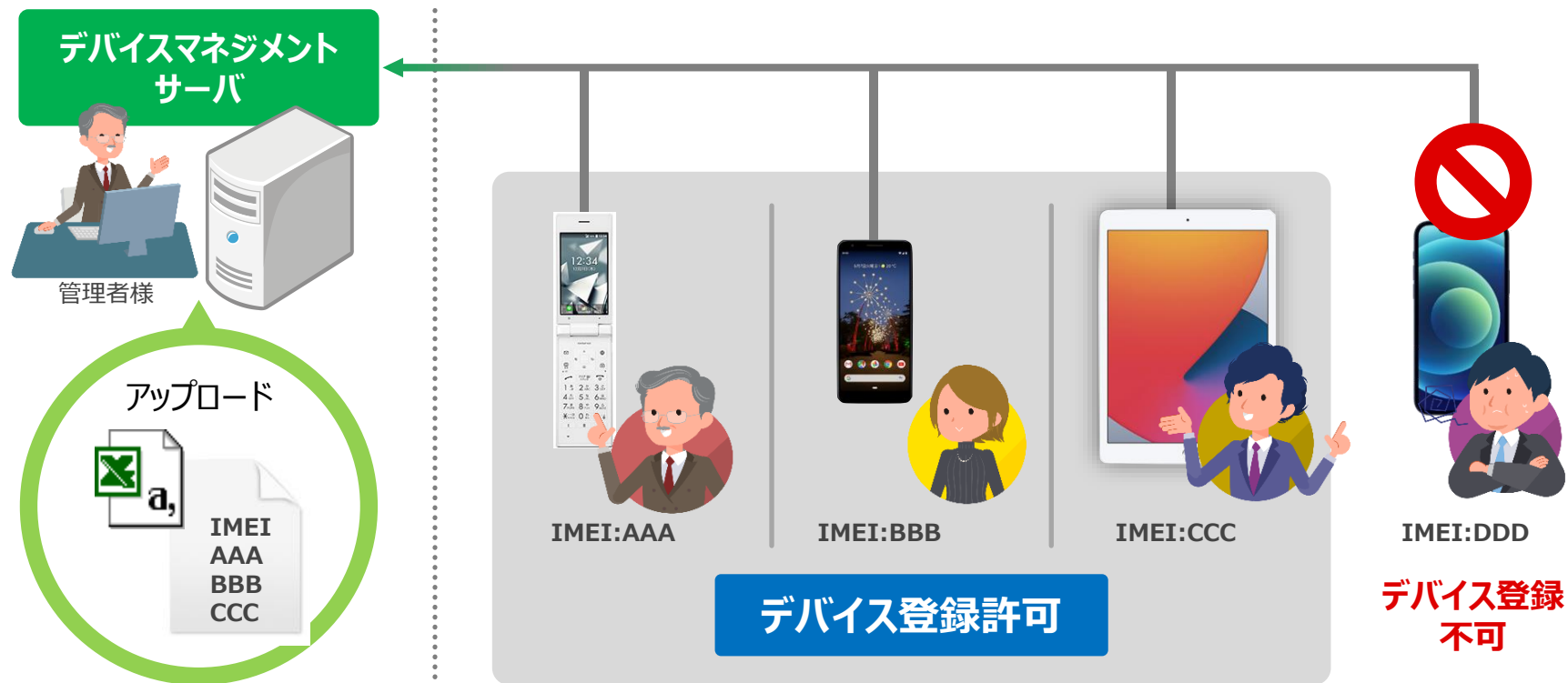
※1 OCSP(Online Certificate Status Protocol)・・・TCP/IPネットワークを通じてデジタル証明書（公開鍵証明書）の有効性を問い合わせる手順を定めたプロトコル（通信規約）

※2 CRL（Certificate Revocation List）・・・証明書の失効情報（シリアル番号と失効日）が記載されている認証局（CA）毎に作成・更新されるリスト

事 項	詳 細
証明書の配布方法	・ユーザと利用デバイスを紐づけることで、証明書がデバイスに自動配付されます。
メンテナンス	・毎月第3火曜日の20時から22時はサイバートラスト社のメンテナンスがあります。 メンテナンス中は証明書発行処理が停止します。
その他	・VPN装置等で証明書を利用する場合は、OUに含まれるDMコードを必ず接続判定条件に加えてください。

登録許可デバイスの指定が可能

デバイスのIMEIやserialを指定することで、MDMの登録を許可するデバイスを指定できます。
指定外のデバイスがデバイス登録を行っても、デバイス登録できません。

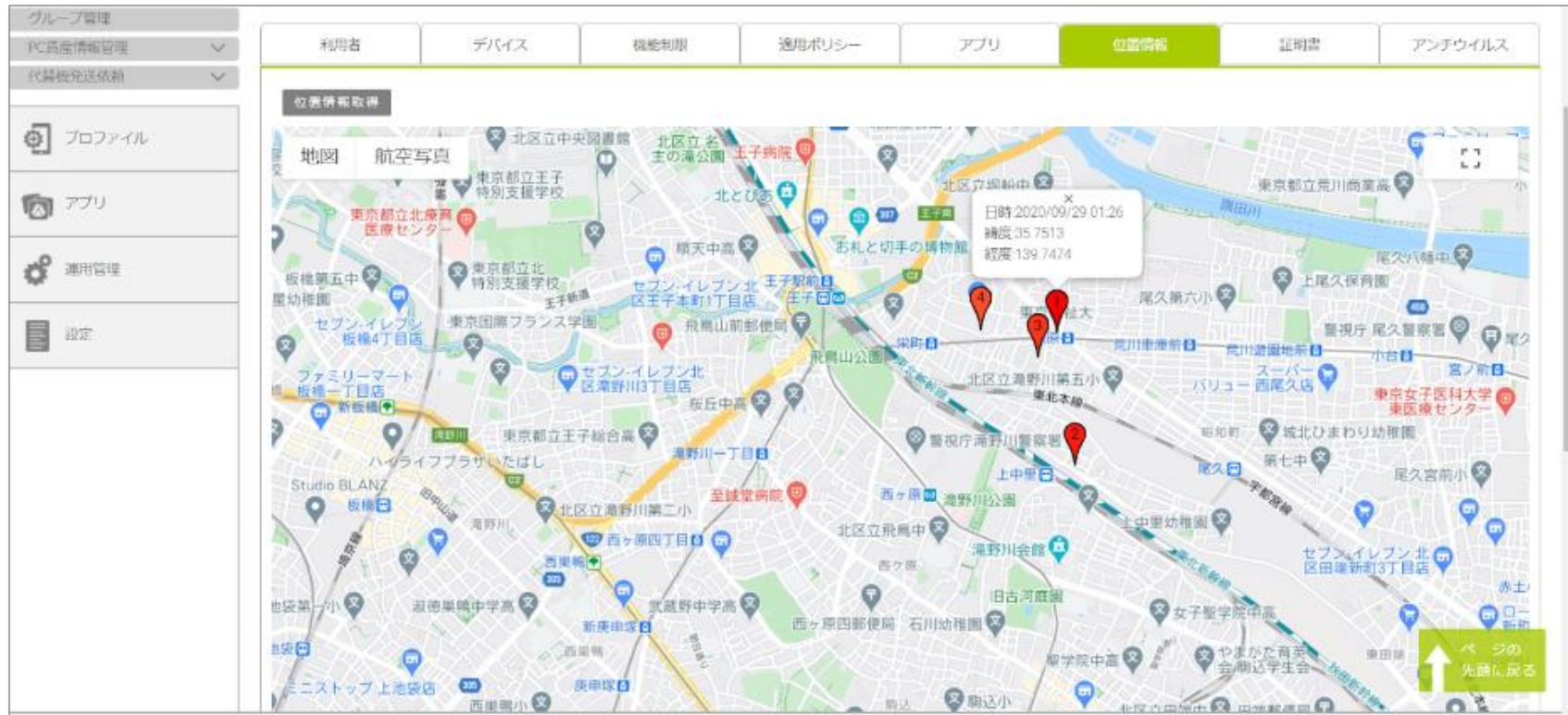


※運用管理のデバイス登録制御の設定が完了する前にデバイス登録が完了しているデバイスは登録可否チェック対象外となります。

※iOSでIMEIを持たない場合は、serialで指定できます。

デバイスの最新位置情報の取得が可能

デバイス毎に現在位置を地図上で確認できます。更に、iOSは基地局移動、Androidは予め設定した時間間隔、Windowsは15分間隔に応じて位置情報を自動取得するため、1日の行動を時系列で確認できます。



※AndroidはAndroid Enterprise (Fully managed device) のみ本機能をご利用頂けます。

※ Windowsは、M6から始まるDMコードの環境のみ利用可能です。

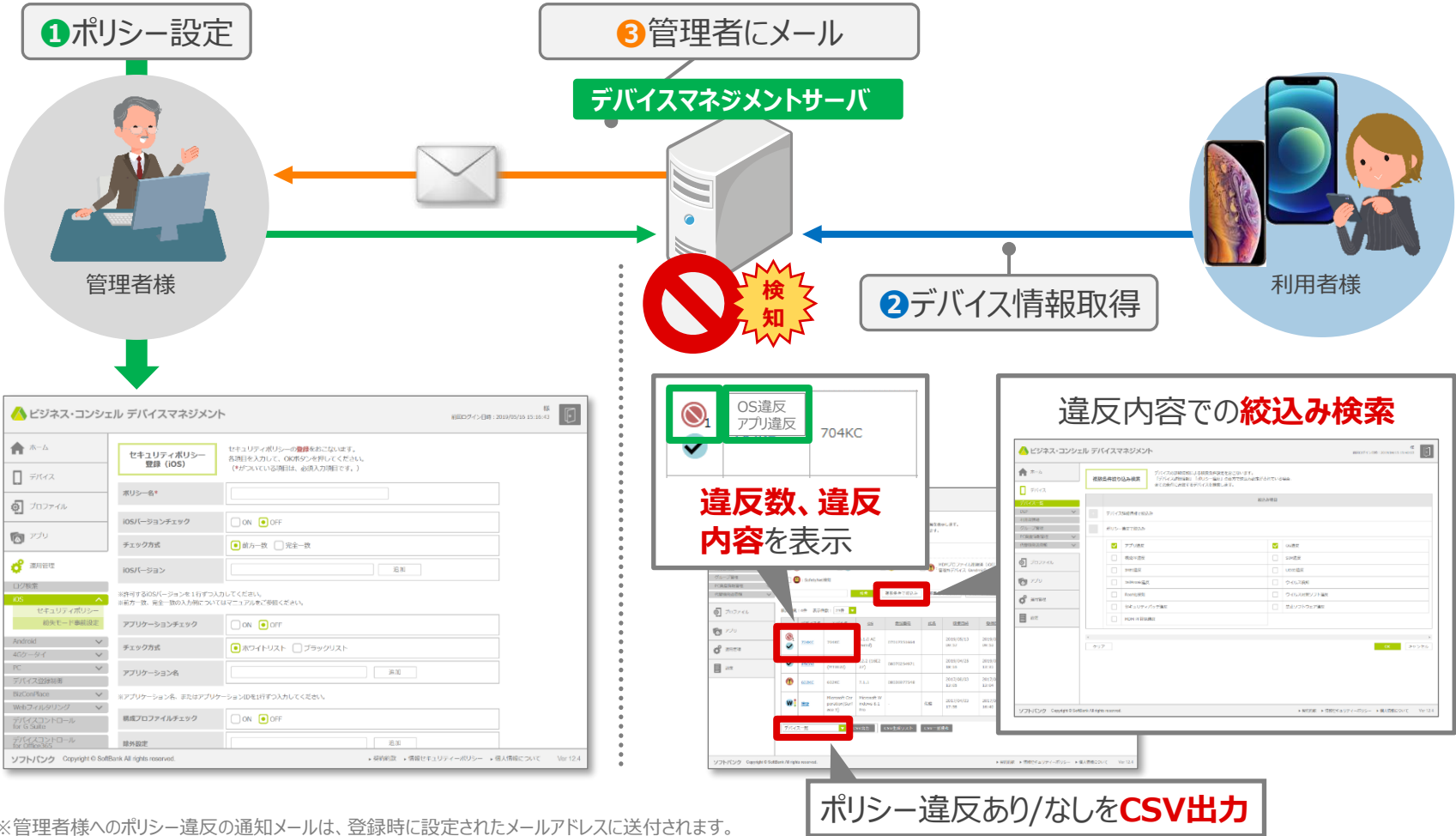
※iOSは紛失モード、BizConPlace/ArrowPortalでも位置情報が取得できますが、位置情報履歴を取得することはできません。

※iOSの位置情報機能は「BC Location」のスライドでもご紹介しております。

	内 容
iOS	位置情報履歴を取得するには、BC Locationが必要となります。 ※BC LocationをエンタープライズAppでご利用される場合、契約者にて米国Apple社とApple Developer Enterprise Programの契約を行う必要があります。 ※本機能をご利用いただくには、申し込みが必要です。
	Wi-Fiモデルは対象外です。海外キャリア端末ご利用時、海外ローミングご利用時は、位置情報機能はサポート対象外となります。（日本以外の国の地図は表示されません）
	BC LocationのApp StoreアプリをManaged Appsで配布する場合は、BC Locationが取得した認証キーによる自動認証にて使用可能です。 App Storeから直接インストールした場合は、手動認証（初回）のためBizConID、パスワードが必要となります。
	対象デバイスの設定で位置情報サービスが許可されている必要があります。また、アプリの「位置情報の利用を許可」設定で「Appの使用中は許可」が選択されている必要があります。
	デバイスが電源オフや圏外などの間は動作しません。
	バックグラウンドからBC Locationを削除すると、機能は停止します。ただしiOS 8以降は、基地局移動を検知すると位置情報の取得を再開します。
	取得する位置情報の精度は、対象デバイスの位置情報の精度に依存します。 BC Locationの位置情報送信間隔、および管理サイトの位置情報取得日時は、対象デバイスの状況や通信環境によってずれが生じることがあります。また、本機能は、対象デバイスの位置情報の正確性を保証するものではありません。
Android	位置情報履歴を取得するには、BCAgent（バージョン：v4.03.13以上）が必要となります。
	位置情報はあくまでも目安として利用してください。実際の位置とは異なる場合があります。
	位置情報を取得するには、位置情報を取得するためのポリシーをデバイスに適用しておく必要があります。
	デバイスの位置情報サービスが有効になっている必要があります。GPSのみオンになっていると、屋内では位置情報を取得できない場合があります。位置情報を取得しやすくするためには、デバイスの「設定」-「位置とセキュリティ」をタップし、「Wi-Fi/モバイル接続時の位置情報」と「GPS機能を使用」にチェックを入れてください。Android OS 9以降では、「Google位置情報の精度」を有効にしてください。
	2018年以降に発売されているデバイスが位置情報サービスの推奨機種です。

	内 容
Windows	本機能はM6から始まるDMコードのみでご利用いただける機能となります。
	位置情報はあくまでも目安として利用してください。実際の位置とは異なる場合があります。
	GPSのみオンになっていると、屋内では位置情報を取得できない場合があります。 Wi-Fi機能をONにしてご利用いただくことを推奨します。
	対象デバイスの設定で位置情報サービスが許可されている必要があります。
	デバイスが電源オフや圏外などの間は動作しません。

ポリシー違反を管理者にメール通知することが可能

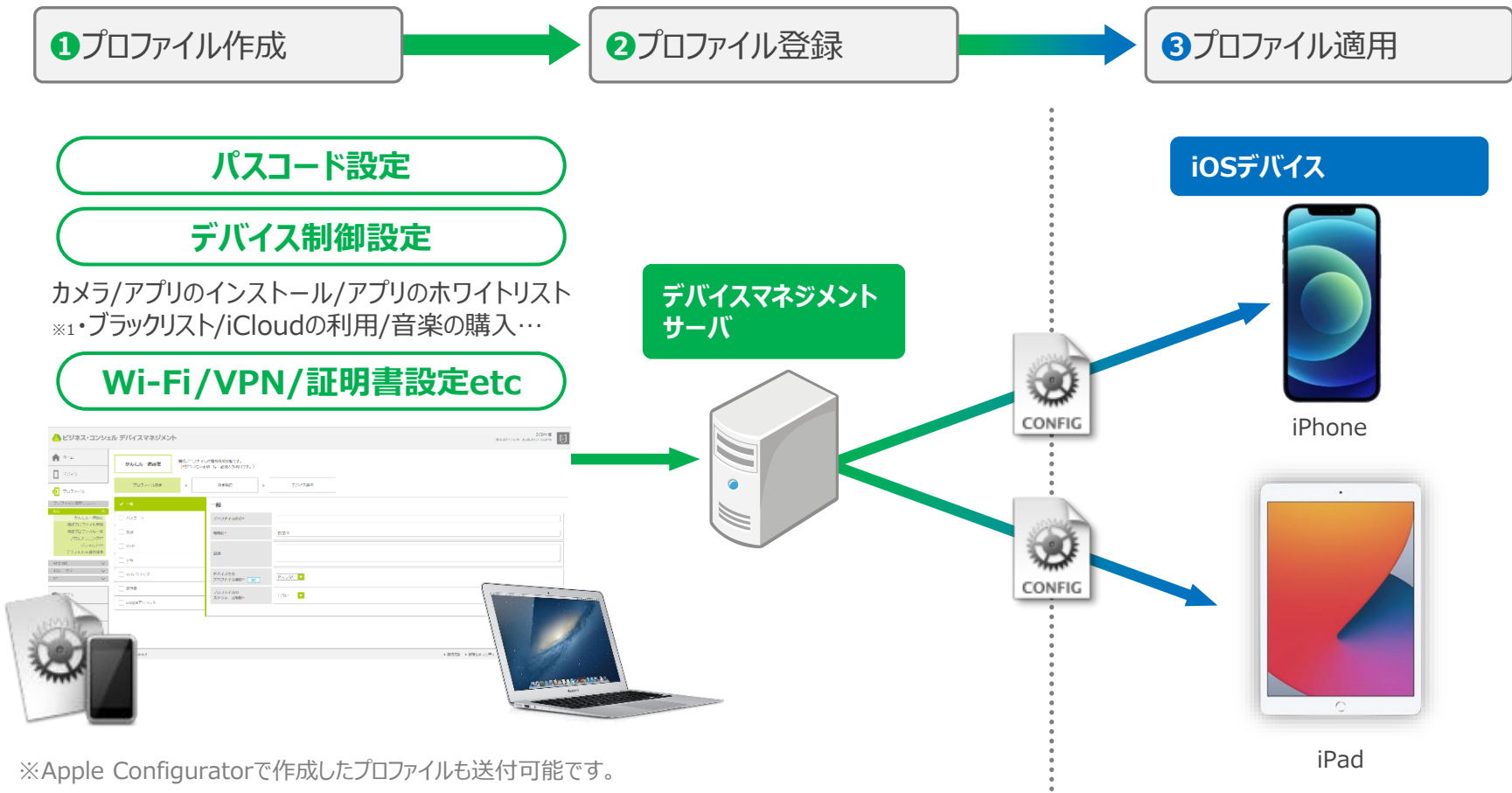


基本サービス [iOS]

収集可能なデバイス情報の項目一覧

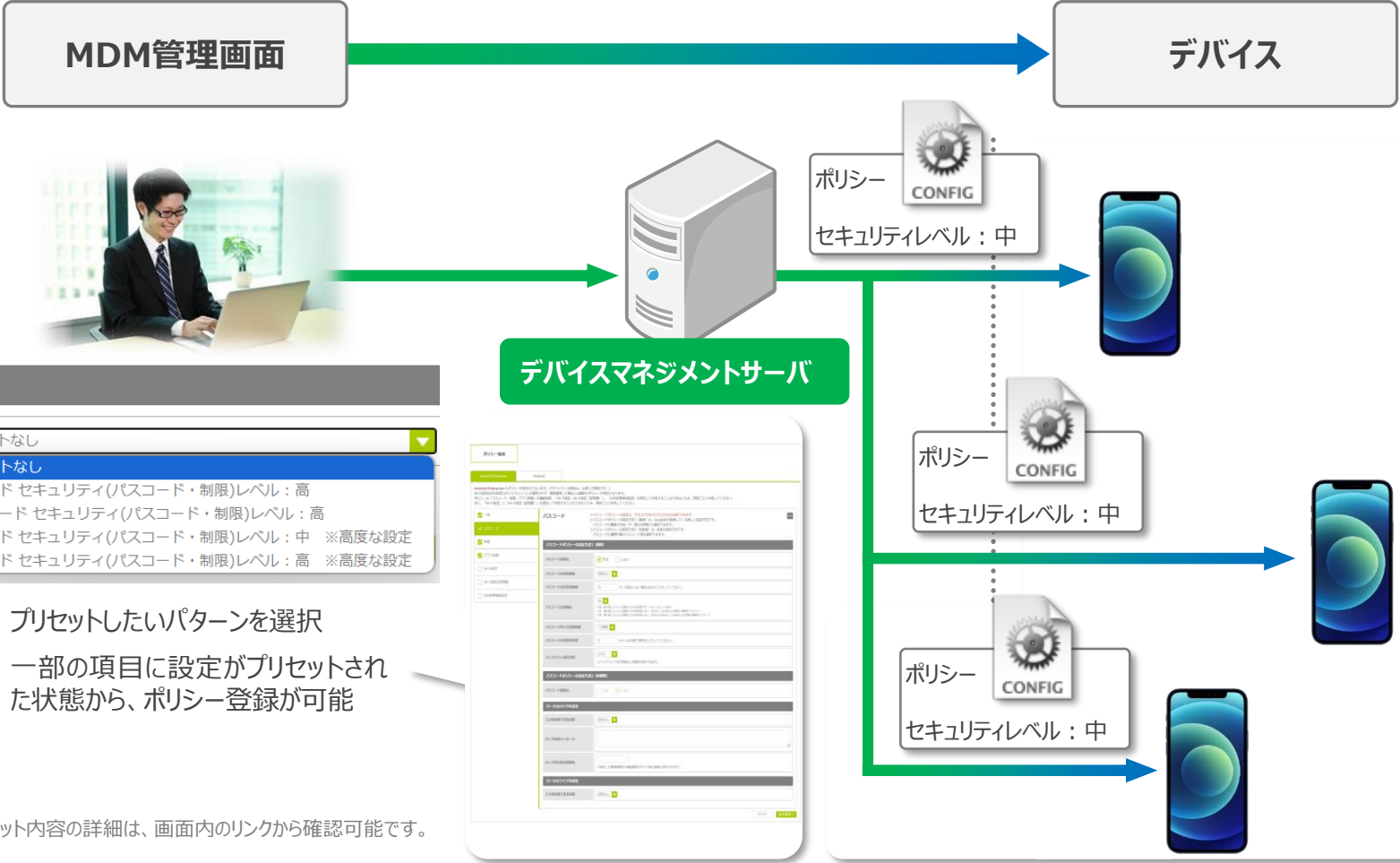
デバイス情報	- 電話番号 - デバイス情報の収集日時 - デバイス名 - モデル名および番号 - iOSおよびビルドバージョン - パスコードの設定有無 - デバイス登録日時 - デバイスの監視 - SIMキャリアのネットワーク - 現在のキャリアのネットワーク - UDID(デバイス識別番号)	- 容量 - 使用可能な空き領域 - キャリア設定のバージョン - シリアル番号 - Wi-FiのMACアドレス - BluetoothのMACアドレス - IMEI(携帯端末識別番号) - ICCID(SIMカード番号) - モデムのファームウェア - バッテリー残量 - ハードウェア暗号化機能	- EASデバイス識別子 - ローミング中 - データローミング設定 - 音声通話ローミング - iTunesStoreアカウント - 位置情報サービス - アクティベーションロック - おやすみモード - インターネット共有（テザリング） - iCloudバックアップ最終日時 - iCloudバックアップ設定有無
プロファイル情報	- プロファイル名 - 識別子 - 組織	- 削除可否 - 削除用パスワード - MDMから導入	暗号化
証明書情報	- コモンネーム - 発行者名	- 有効開始日 - 有効期限	秘密鍵
アプリケーション情報	- インストールされているアプリケーション（アプリケーションID、名前、バージョン、サイズ、データサイズ） - インストールされているプロビジョニングプロファイル		
位置情報	位置情報（最大100件）、位置情報の取得日時、緯度、経度、精度、電池		

遠隔からプロファイルの適用が可能



※構成プロファイルで設定可能な項目に従います。詳細な遠隔設定項目はAppendixをご覧ください。
※1 アプリのホワイトリストを設定する際、アプリカタログをご利用中の場合はアプリカタログも併せて指定してください。

BCDMおすすめのセキュリティレベルのポリシーが
プリセット（初期設定）された状態からポリシー登録可能



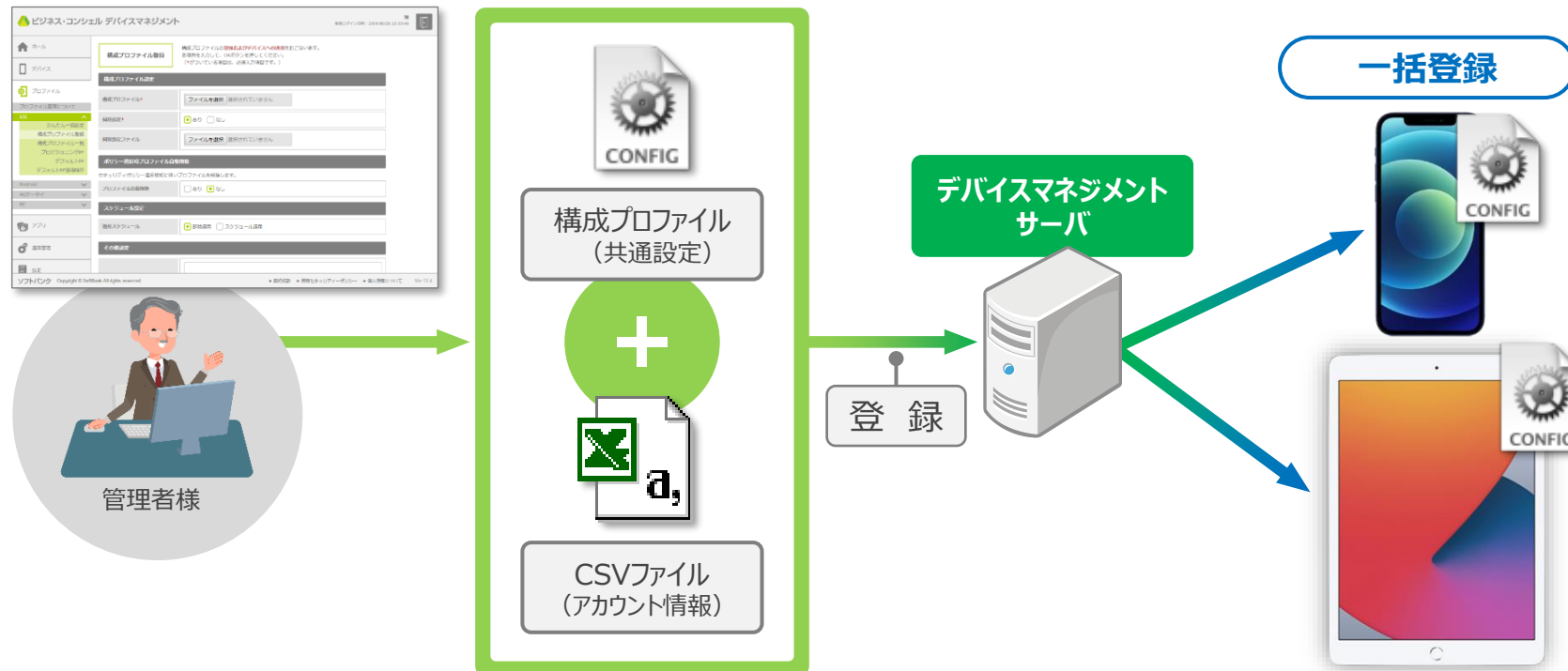
アカウント（Exchange ActiveSync/VPN/Google/メール）の一括設定可能

共通設定

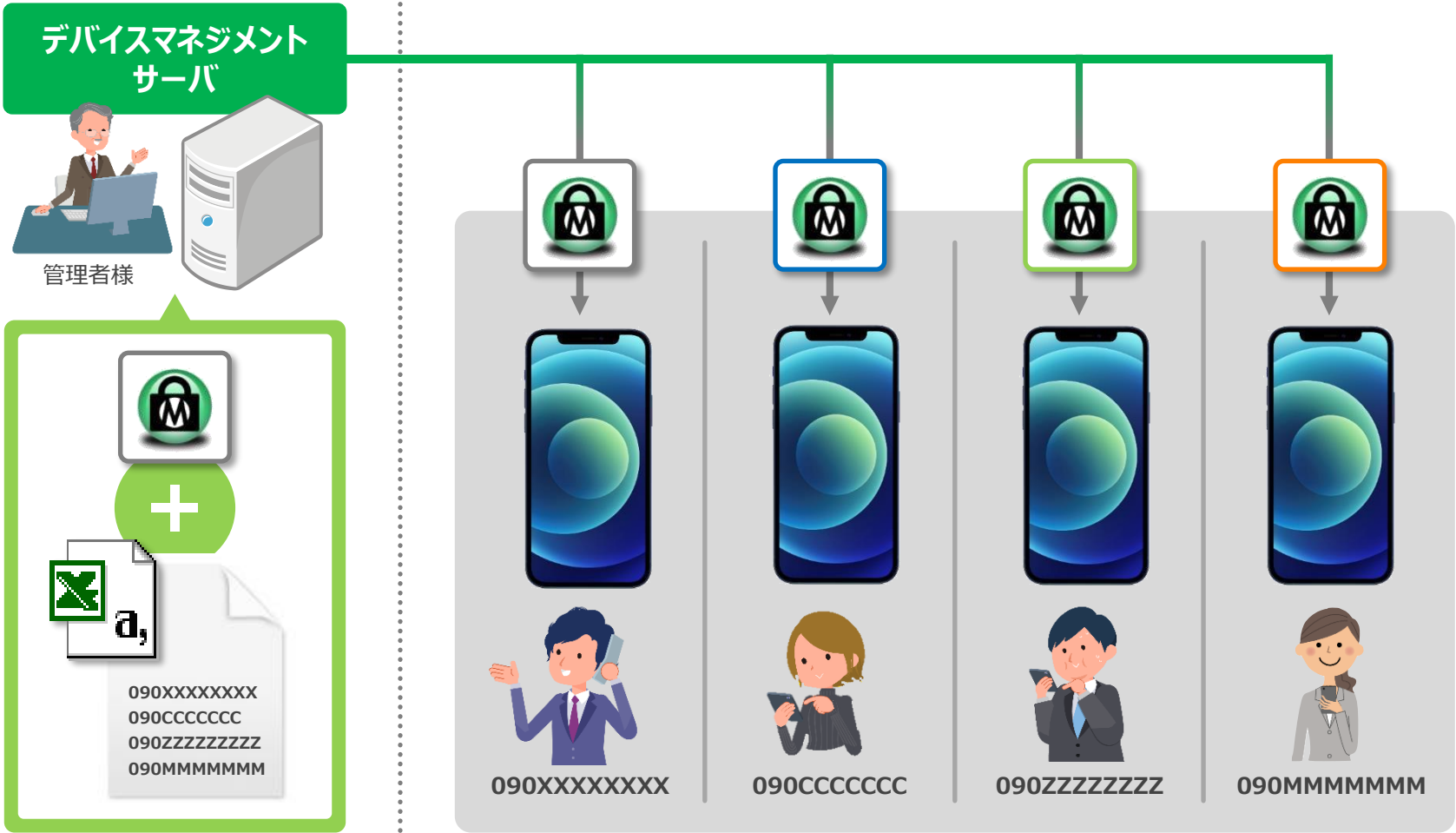
Exchange ActiveSyncサーバホスト（サーバ）、SSL使用等の共通設定情報

個別設定

アカウント、メールアドレス、PW等の個別設定情報

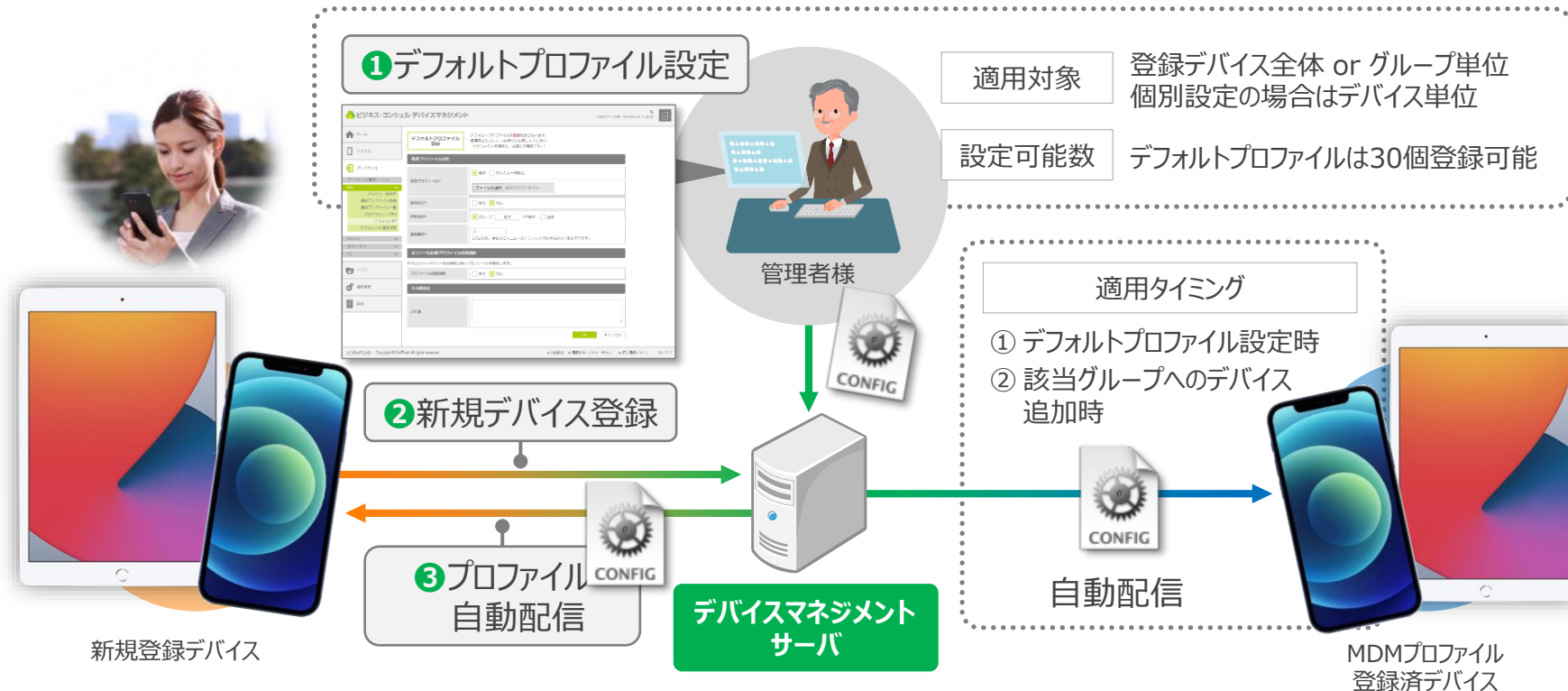


CSVファイルを組み合わせることでユーザーごとにURL配布が可能



構成プロフィールの自動配信が可能

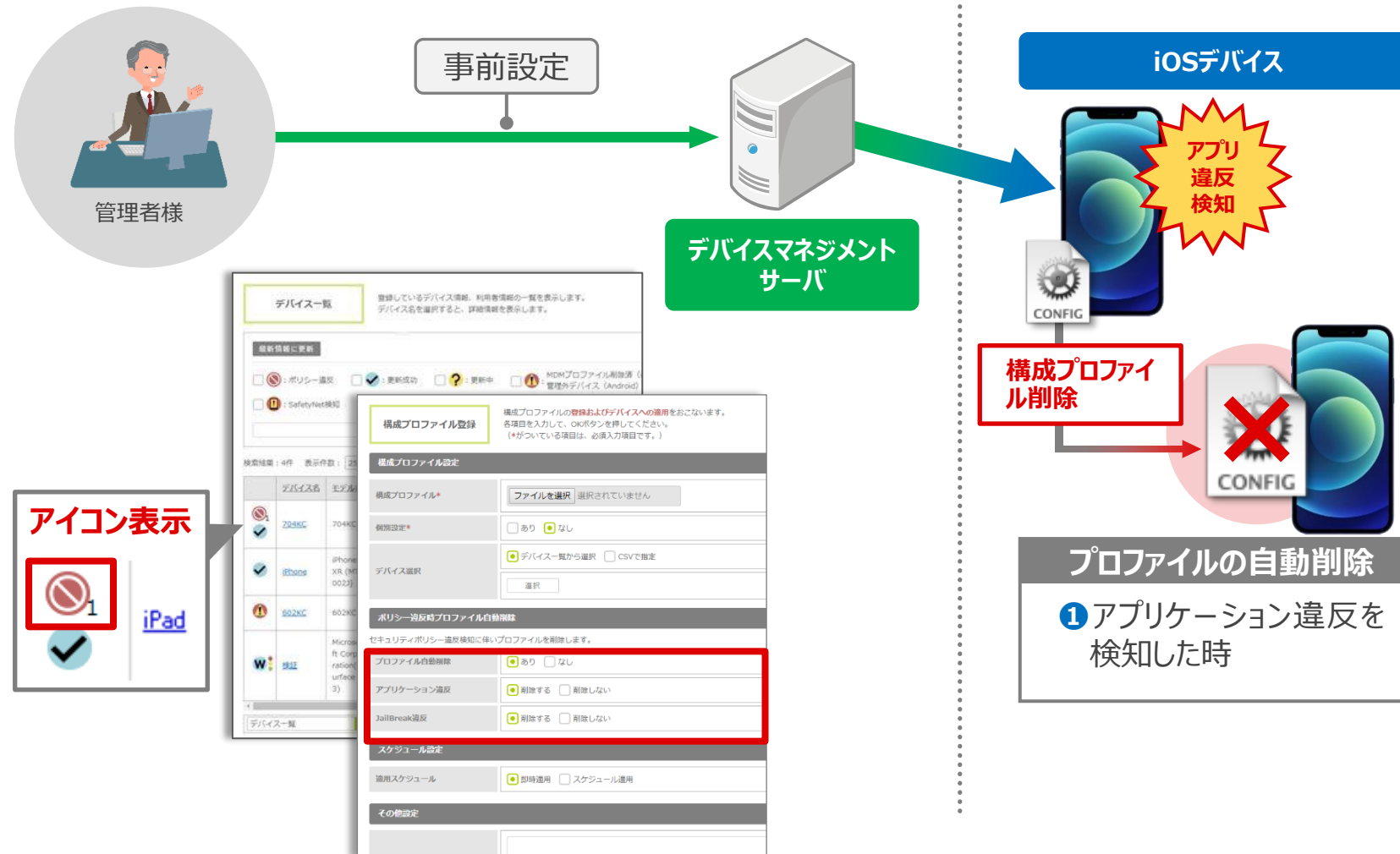
自動配信させたいプロフィールを事前に設定する事で、
デバイス登録時やグループ追加時に、該当プロフィールを自動で配信する事が出来ます。
また、配信対象となるMDMプロフィール登録済みデバイスに対しても自動配信が可能です。



※デフォルトプロフィールを複数設定した場合、設定時に指定する適用順序に従い、デバイスへ適用されます。

項 目	内 容
設定可能なプロファイルの種類について	以下2項目となります ① 「かんたん一括設定」より作成されたプロファイル ② Apple Configuratorより作成されたプロファイル
グループ単位で設定したデフォルトプロファイル配信について	新規デバイス登録時にグループ単位で設定したデフォルトプロファイルを適用させるには、デバイス登録前に該当グループへデバイス情報をあらかじめCSV登録しておく必要があります。
適用済デフォルトプロファイルの削除について	グループ設定済のデバイスを別グループへ変更した場合、旧グループにて適用されたデフォルトプロファイルは自動削除されません。

アプリケーション違反を検知後、設定した構成プロファイルを削除



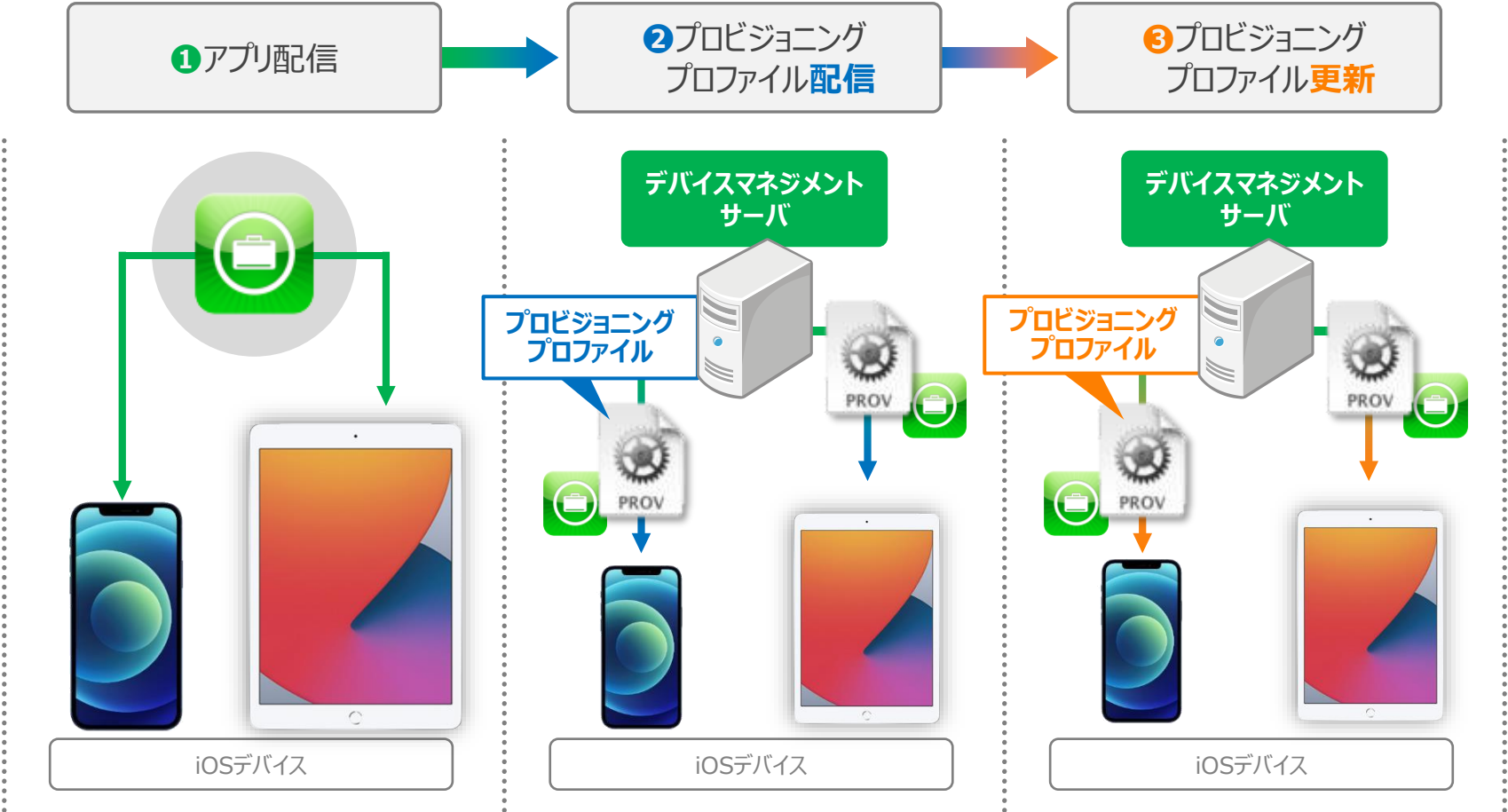
MDM管理対象から外れたデバイスの検知が可能



※MDMプロファイルとは、MDM管理対象とするためにiPhone、iPadに設定するプロファイルです。MDMプロファイルを削除するとMDM管理対象から外れます。

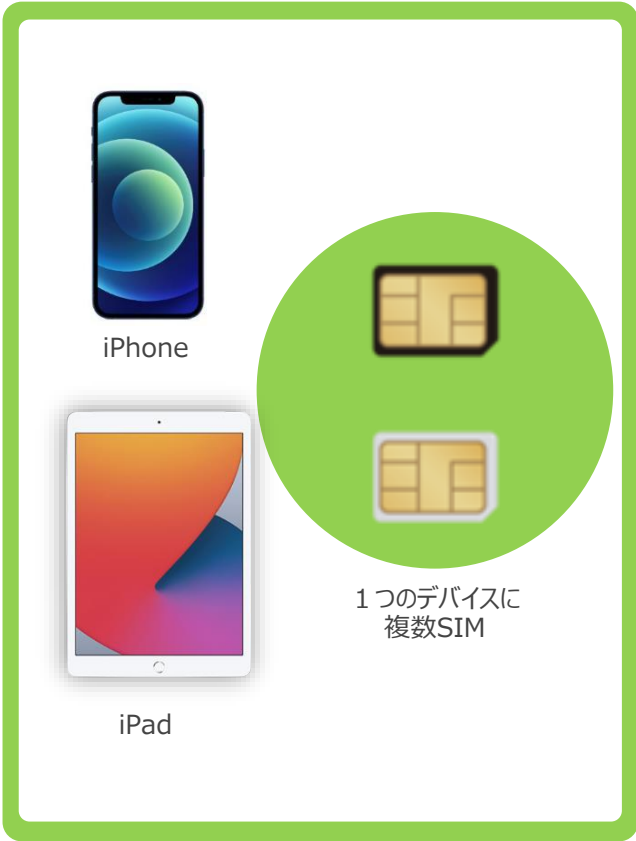
※MDMプロファイルが削除されたことを管理サーバが検知するタイミングには、定期検知（1回/日）と即時検知があります。

プロビジョニングプロファイルの配信が可能



※管理画面から更新作業をおこなうには、アプリ配布/Managed Appsによるアプリ配信のあとに、管理サーバからプロビジョニングプロファイルの登録配信が必須になります。

複数SIM対応のiOSデバイスにて
2枚までのSIM情報(電話番号等)を表示可能



利用者詳細情報 画面

利用者詳細情報					
対象者の登録情報を表示します。 パスコードの一時解除、利用者の変更、デバイス情報の削除もおこなえます。					
デバイス名	モデル名	電話番号 1	電話番号 2	氏名	シリアル
iPhone	(MLJD3J)	08012341234 (ラベルA)	08012345678 (ラベルB)		

デバイス一覧 画面

検索結果：1件 表示件数：100件

	デバイス名	モデル名	OS	電話番号 1	電話番号 2	氏名	収集日時	登録日時
	iPhone	(MLJD3J)	16.4 (20E247)	08012341234 (ラベルA)	08012345678 (ラベルB)		2023/04/05 11:01	2023/04/05 10:58

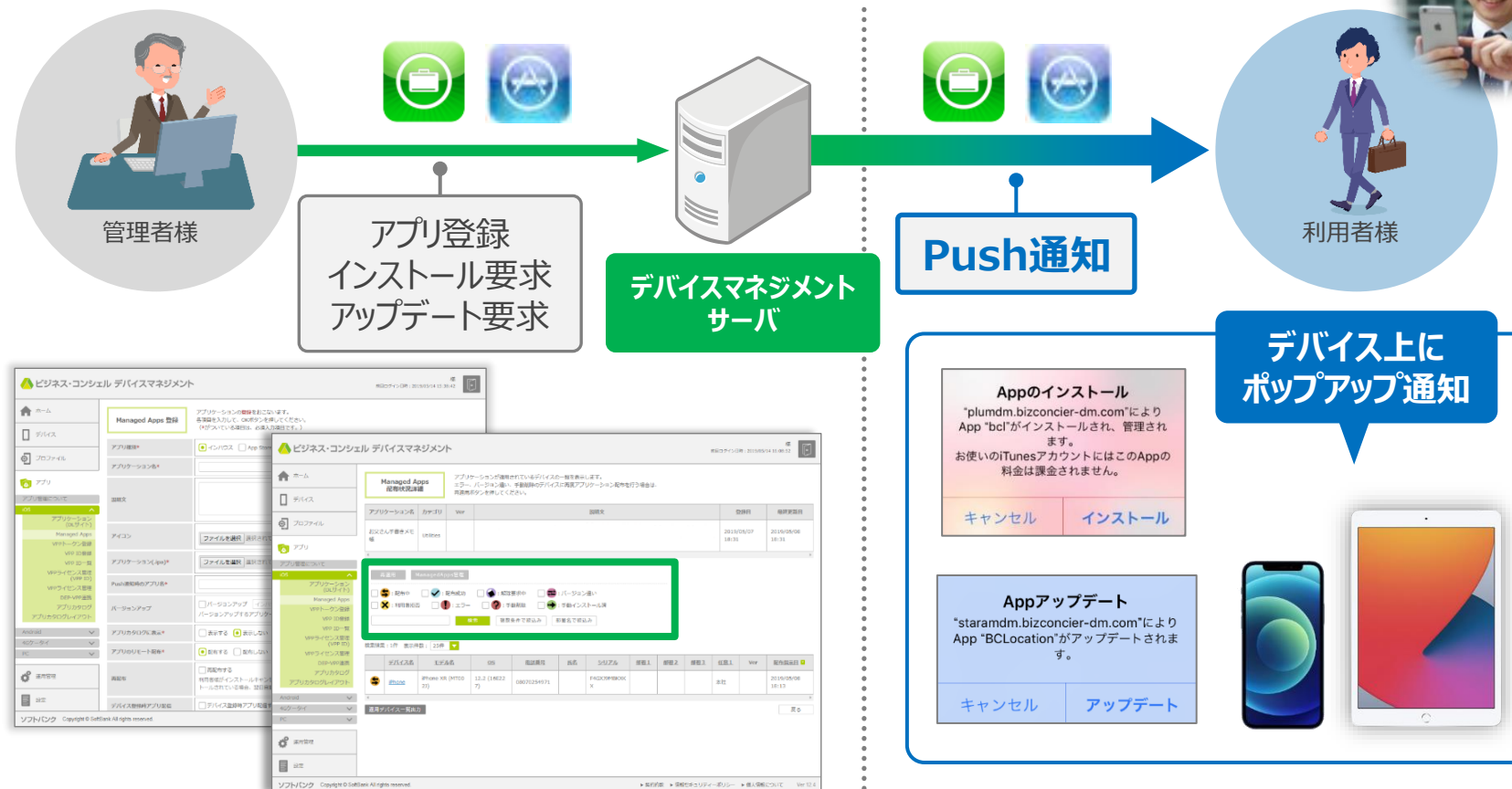
利用者詳細情報 SIM画面

SIM情報		
電話番号	08012341234	08012345678
形式	物理SIM	eSIM
名称	ラベルA	ラベルB
キャリア		KDDI
キャリア設定のバージョン	51.0.1	51.0
ローミング中	いいえ	いいえ
音声回線		優先
データ通信		優先

SIM情報セクションにはSIM毎に情報が表示されます。

- 電話番号
 - SIM形式
 - 名称
 - キャリア
 - キャリア設定のバージョン
 - ローミング中
 - 音声回線
- データ通信
 - ICCID
 - IMEI
 - EID
 - スロット

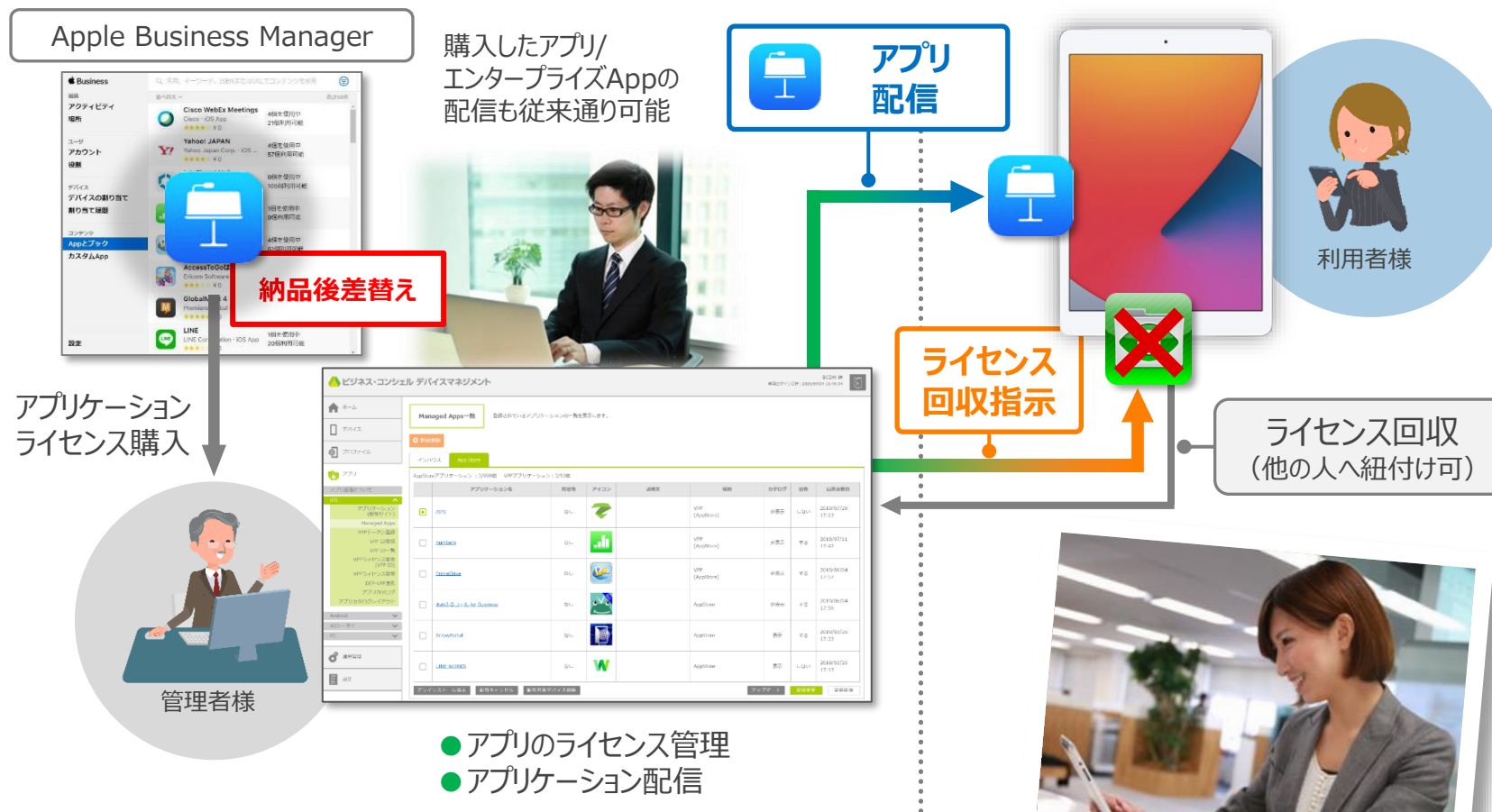
エンタープライズApp/App StoreアプリをリモートからPush配信 アプリ配布状況を管理画面で確認可能



※2013年4月15日以降にMDMにデバイス登録されたデバイスが対象です。

※複数のアプリを一括で配信することも可能です。

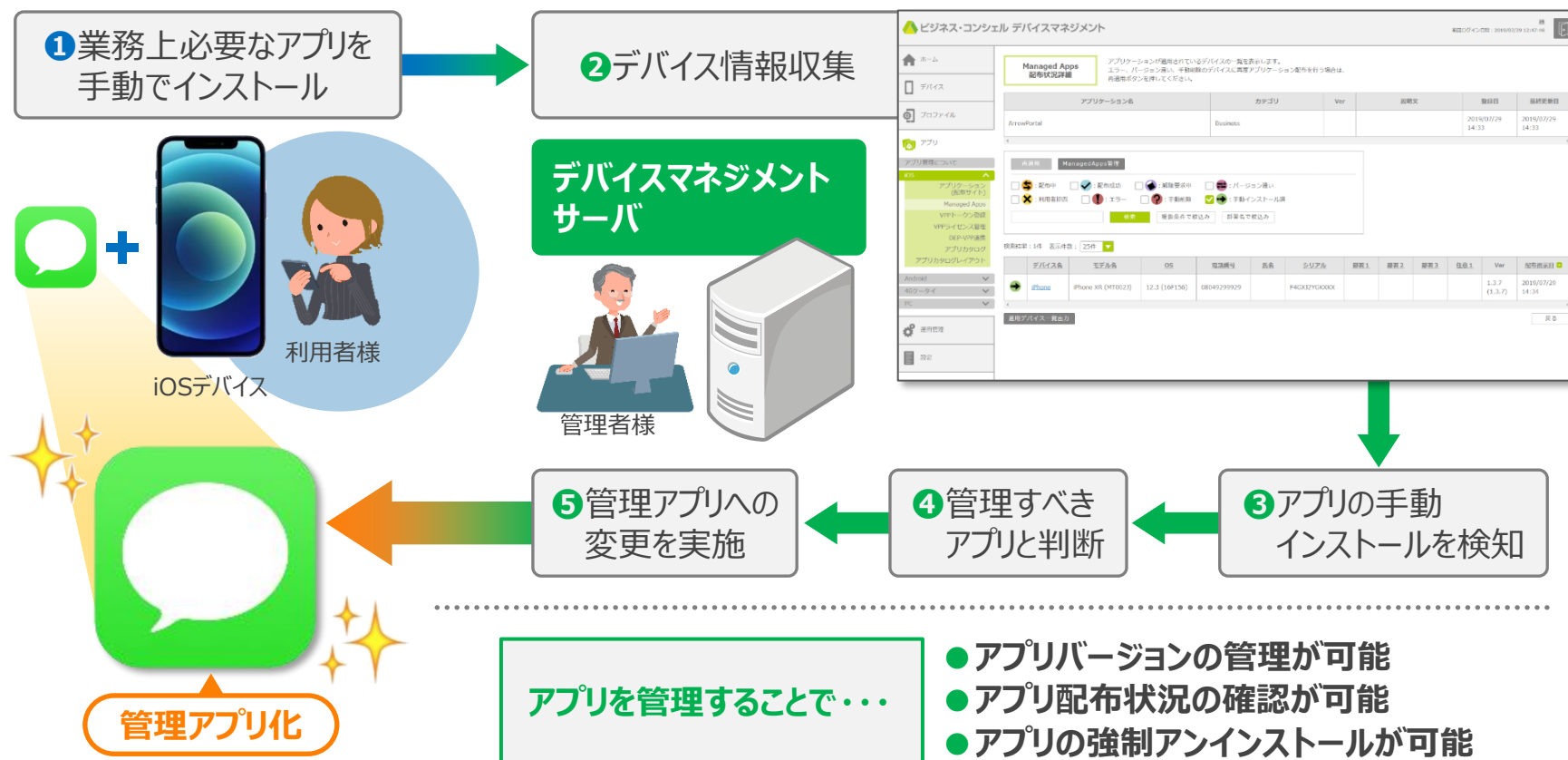
購入済Appから購入したアプリの配信/ライセンス管理が可能



※動作確認iOSバージョンについてはAppendixをご覧ください。

※購入済App(無料アプリでも「購入済」と表記します)とはApple社が提供する「Volume Purchase Program」を示します。

利用者が手動インストールしたアプリを、後から管理アプリに変更



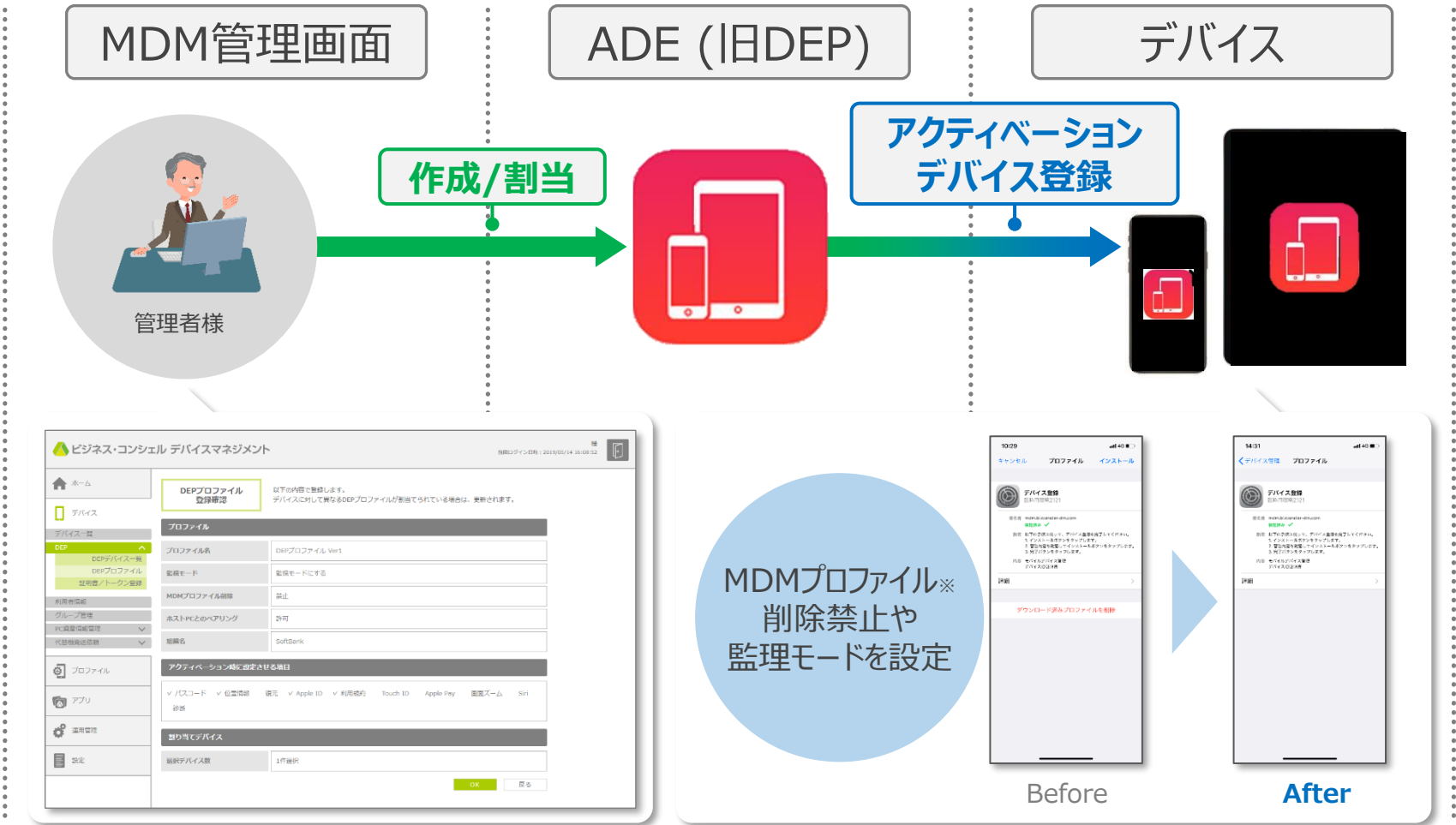
※本機能は、購入済App(無料アプリでも“購入済”と表記します)、エンタープライズAppには適用できません。

項 目	内 容
アプリ登録	アプリをMDMに登録することができます。
デバイス登録時アプリ配信	事前に設定をしておくと、新規デバイス登録時にアプリを自動で配信できます。
アプリインストール	アプリケーションのインストール通知を配信します。
複数アプリインストール	指定したApp Store(無償)・購入済Appを配信できます。
アプリアップデート	アプリケーションのアップデート通知を配信します。
アプリアンインストール	管理サーバからインストール通知したアプリケーションを、デバイス上から強制削除することができます。
アプリ配布キャンセル	アプリケーションの配信指示をキャンセルをすることができます。
アプリ配布対象デバイスの削除	インストール未完了のデバイス情報を管理サーバから削除することができます。
アプリの再適用	インストール未完了のデバイスに対して、インストール通知を再適用することができます。

項 目	内 容
登録可能なアプリの個数	エンタープライズAppは最大50個登録でき、ファイル1個あたりの容量上限は40MBになります。App Storeの無料アプリケーションは最大999個登録できます。また購入済App(無料アプリでも“購入済”と表記します) は、最大150個登録できます。
Apple IDでのサインインが必要	App Storeのアプリケーションをインストールする際は各デバイスごとにApple IDのサインインが求められますので、事前にご用意下さい。 ※購入済App(無料アプリでも“購入済”と表記します)利用時は不要となります。
手動インストール済みアプリをManaged Appsに変更	デバイスに手動インストール済のアプリケーションに対して、MDMから管理することが出来ます。
エンタープライズAppについて	エンタープライズAppをご利用になる場合は、お客様とApple社との間でADEP (Apple Developer Enterprise Program) のご契約が必要になります。
有料アプリケーションについて	有料アプリケーションを配信する場合は、Apple社が提供する「Apple Business Manager (ABM)」の登録が必要となります。
デバイス登録時アプリ配信の適用範囲	新規登録デバイス全体、もしくはグループ単位での設定が可能です。 既にデバイス登録済みのデバイスは適用範囲に含まれません。
デバイス登録時アプリ配信のグループへの配信について	新規デバイス登録時にアプリをグループへ配信させるには、デバイス登録前にあらかじめアプリを配信したいデバイスの情報を該当グループへ登録しておく必要があります。
アプリケーションの階層表示について	既存アプリの別バージョンを登録するとアプリ単位で別バージョンを階層表示できますが、App Storeのアプリの場合別バージョンを登録できないため、階層表示で表示できるアプリは一つだけになります。

分 類	項 目	内 容
管理者	管理対象Apple IDの取得	Apple社が提供する「Apple Business Manager」へアクセスし、アプリを購入するための企業向けApple IDを作成下さい。
	利用者毎のデバイス シリアル番号一覧の登録	Managed Appsから配布するには、事前に配布対象デバイスのシリアル番号の登録が必要です。シリアル登録はデバイス登録済みのリストから選択可能です。
	アプリ配布	MDM管理サイトのManaged Appsからアプリ配信を実施下さい。
利用者	アプリインストールの確認	App Storeアプリのインストールの確認画面がポップアップ表示されます。同意してインストールを実施してください。※監理モードの場合はサイレントでインストールされます。
その他	ライセンスの割当方法	デバイス単位・グループ単位でのライセンス割当のみとなります。

アクティベーションと同時にデバイス登録が可能



※ MDMプロファイルとは、MDM管理対象とするためにiPhone、iPadに設定するプロファイルです。ADE (旧DEP)を利用して設定した場合は「ADE (旧DEP)プロファイル」と呼ばれます。

設定項目一覧①

監理モード	端末を監理モードにすることが選択可能です。
MDMプロファイル※削除	端末にインストールされるMDMプロファイルを削除不可にすることが可能です。
ホストPCとのペアリング	PCとのペアリングの可否を設定可能です。
共有iPadの設定	デバイスを共有iPadに設定することが可能です。

※共有iPadについては別スライドに詳細を記載しています。

設定項目一覧②

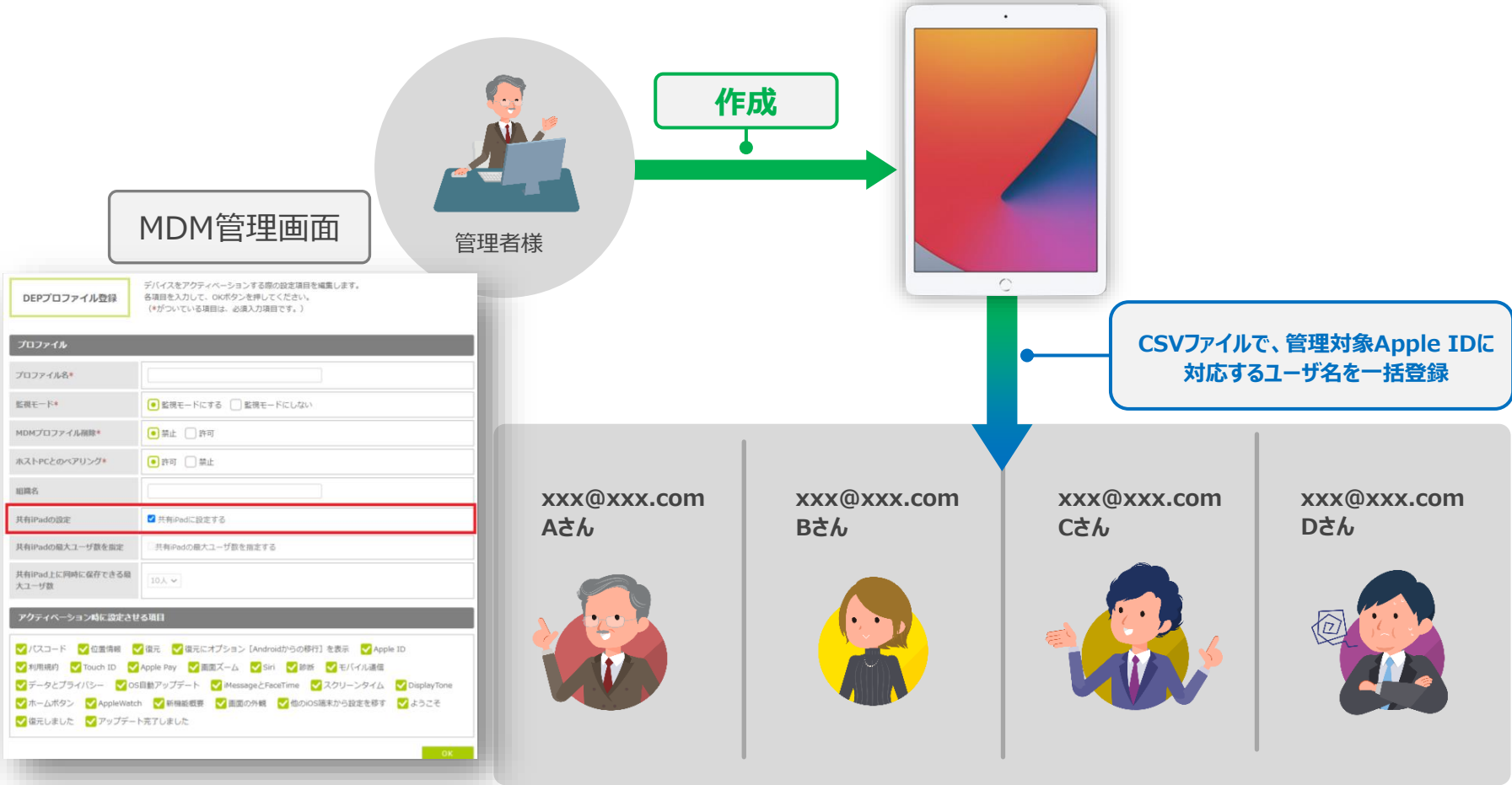
アクティベーション時に 設定させる項目	下記の項目について、アクティベーション時に設定を可能とするか、スキップさせるか設定可能です。 • パスコード • 位置情報 • 復元 • 復元にオプション(Androidからの移行)を表示 • Apple ID • 利用規約 • Touch ID • Apple pay • 拡大表示 • Siri • 診断 • モバイル通信 • データとプライバシー • OS自動アップデート • iMessageとFaceTime • スクリーンタイム • Display Tone • ホームボタン • AppleWatch • 新機能概要 • 画面の外観 • 他のiOS端末から設定を移す • ようこそ • 復元しました • アップデート完了しました
------------------------	---

※MDMプロファイルとは、MDM管理対象とするためにiPhone、iPadに設定するプロファイルです。ADE (旧DEP)を利用して設定した場合は「ADE (旧DEP)プロファイル」と呼ばれます。

MDMプロファイル(ADE (旧DEP)プロファイル)を削除するとMDM管理対象から外れます。

※「アクティベーション時に設定させる項目」は、「共有iPadの設定」にチェックが入っている場合は無効になります。

複数のユーザが 1 台のiPadを共有して各ユーザごとに
個人の領域をもちながら利用することが可能



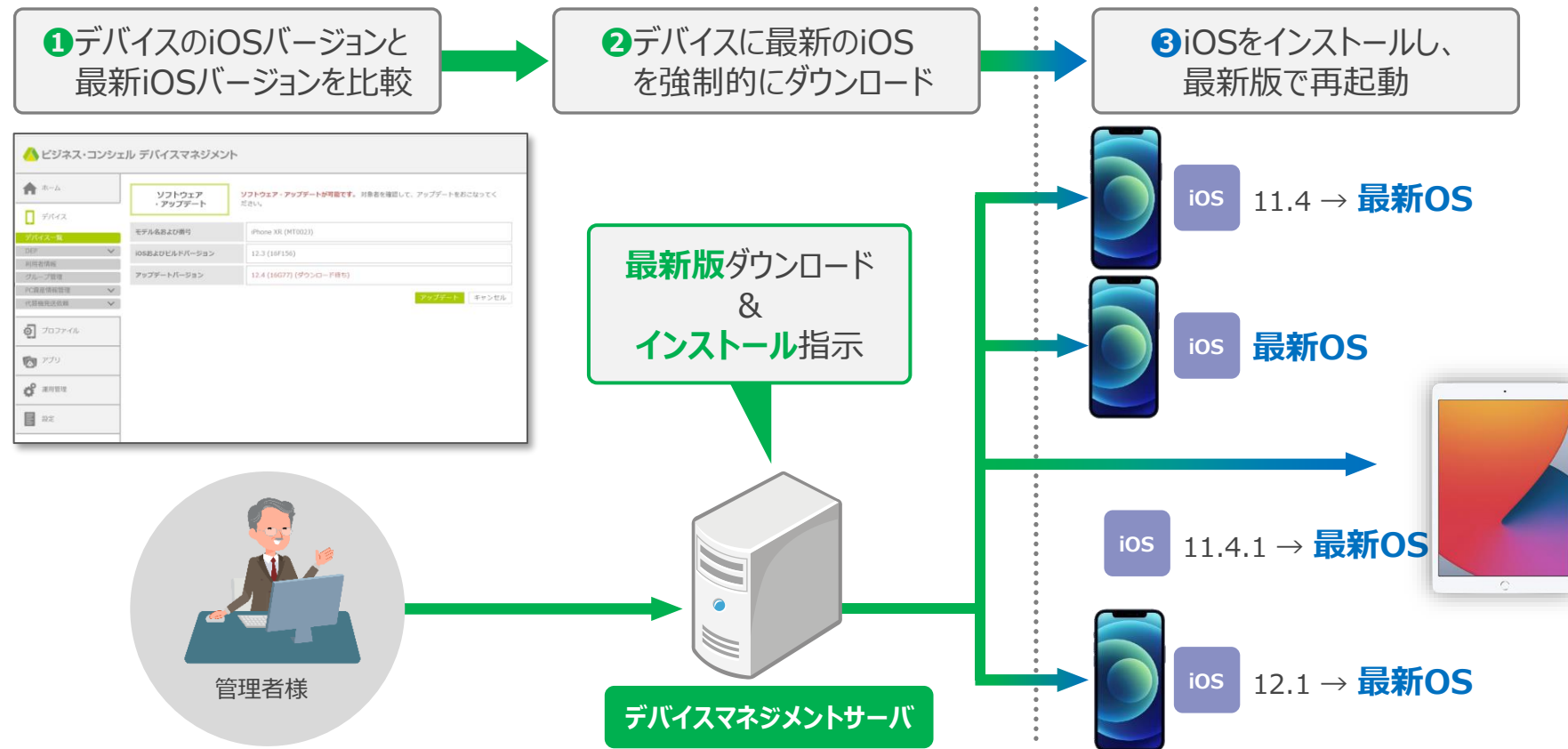
項 目	内 容
ABM登録	事前にApple Business Managerへの登録が必要となります。
ADE (旧DEP)対応端末	購入した端末がADE (旧DEP)に対応している必要があります。詳しくは端末購入元にお問い合わせください。
ID管理併用不可	本機能とID管理機能を同時に利用することはできません。
Apple Configurator 利用不可	ADE (旧DEP)端末はApple Configuratorを利用することができません。
スキップ項目	ADE (旧DEP)プロファイルでスキップできる項目は国または地域を選択で「日本」を選択した場合の項目になります。
監理モードのみ有効な項目	「MDMプロファイル削除禁止」「ホストPCとのペアリング許可」は監理モードにしたときのみ有効となります。

項 目	内 容
管理対象Apple ID	共有iPadを利用するには、Apple社のApple Business Manager（ABM）サイトで組織が発行および所有する管理対象Apple IDが必要です。ユーザは管理対象Apple IDに紐づきます。また、共有iPadに設定するデバイスは、最低32GBのストレージ容量が必要です。
最大ユーザ数とデータの削除	アクティベーション時に、共有iPad上に同時にデータを保存できる最大ユーザ数が設定されます。現在は10名で固定となっています。共有iPadを使用中のユーザが、共有iPad上に同時に保存できる最大ユーザ数を超えた場合、サインインした履歴が一番古いユーザからデバイスのローカルデータが削除されます。iCloudに同期されたデータは削除されません。同期が完了したユーザが存在しない場合、新しいユーザのサインインはエラーとなります。共有iPadを使用する際には、iCloudへのデータの同期と、ユーザが毎回同じ共有iPadを使用することを強く推奨します。
パスコード一時解除不可	共有iPadに対しては、パスコード一時解除機能を利用できません。
配布可能アプリ種別	Apple社の仕様により、共有iPadに対してManaged Apps機能で配布できるアプリはエンタープライズApp及び購入済App(無料アプリでも“購入済”と表記します)のみです。App Storeアプリは配布できません。また、ユーザ（管理対象Apple ID）単位ではなくデバイス単位での配布となります。
「ゲスト」利用不可	共有iPadに設定したデバイスのログイン画面に表示される「ゲスト」ボタンを押下することで、管理対象AppleIDやパスワードを用いずにサインインする「一時セッション」は、BCDMでは使用できません。
構成プロファイル配布対象	構成プロファイルの配布対象となるユーザは、共有iPadから取得したもののみとなります。管理画面からユーザ（および管理対象Apple ID）を登録しただけでは配布対象とはならず、対象のユーザが共有iPad上にサインインする必要があります。
デバイス登録削除不可	共有iPadに設定された状態で、デバイス登録削除を行うことはできません。 Apple社の仕様により、デバイスの「設定」-「一般」-「リセット」が無効化されて非表示となり、デバイス側での初期化が行えなくなります。 ※紛失リカバリーオプションに加入していただくことでBCDMからリモートワイプをすることが可能です。 ※解約時や端末返却時、非共有iPadに戻す際はリモートワイプが必要です。

インストールさせたいアプリケーションのみ表示させる カタログ機能を提供



最新版iOSのダウンロードおよびインストールを強制的に実施させることが可能



※この機能のご利用には、あらかじめデバイスを監理モードにしておく必要があります。

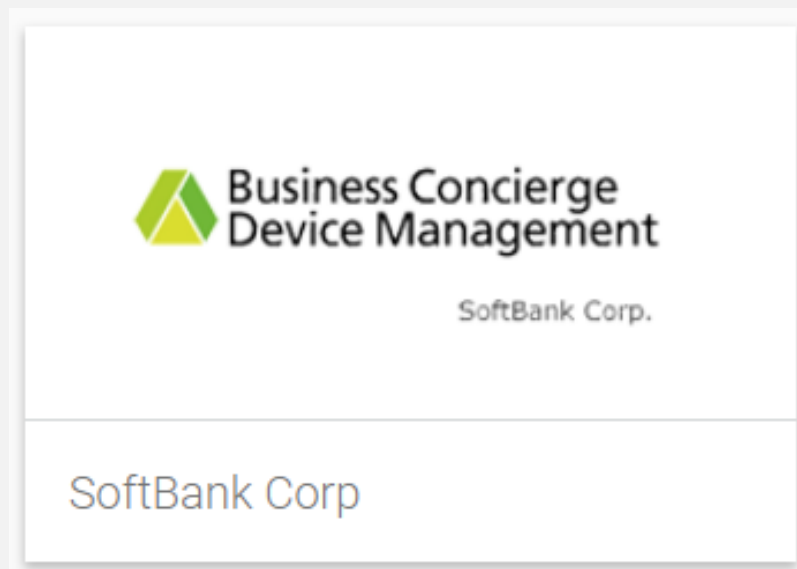
※本機能はデバイスのiOSバージョンが11.4以降で有効になります。

※複数台のデバイスに一括で実施することも可能です。

事 項	詳 細
初期設定	MDM証明書取得には、Safariをご用意ください。(WindowsにてGoogle Chrome使用でも可) なお、MDM証明書はInternet Explorerからでは取得できません。
詳細な機能制限	かんたん一括設定の対象項目外の機能制限や設定を行いたい場合はApple Configuratorを利用可能なMacが必要となります
MDM証明書の更新	1年に1回、MDM証明書の有効期限が切れる前に更新が必要となります。その際、申請時に使用したApple IDとパスワードが必要となりますので、忘れないように管理して下さい。有効期限が切れたままの状態では、端末と管理サイトの疎通が取れず、iOS関連の操作ができません。
MDM証明書用のApple ID取得	個人のApple IDを使用すると、管理者が変更になった等の理由からMDM証明書の更新が煩雑になる懸念があります。その為、MDM証明書専用のApple IDを新しく取得することを推奨します。
MDM証明書の無効化	作成したMDM証明書は絶対に無効化（Revoke）しないでください。無効化すると、全ての導入作業を最初からやり直す必要があります。
初回ログイン時に管理者メールアドレスのメーリングリスト設定	ポリシー違反通知やMDM証明書有効期限通知のメールは、設定された管理者メールアドレスに送信されます。 そのため初回ログイン時に、管理者メールアドレスを関係者が含まれたメーリングリストに設定しておくことを推奨します。
Ver1.3.2以降のBizConPlace	位置情報の定期取得には、Ver1.3.2以降のBizConPlaceが必要となります。

基本サービス [Android]

GoogleがAndroid端末をより安全に利用するために
リリースした**企業向けのモバイル管理プログラム**



EMM※ソリューションに組み込むことで利用可能

※EMMとは「Enterprise Mobility Management」の略であり、社内で扱うスマートデバイスを総合的に管理するツールです。

Android Enterpriseは3つの管理タイプから選択が可能

Work profile



個人所有端末

デバイスに
個人領域と仕事領域を構成

Fully managed device



会社所有端末

デバイスを
仕事専用端末として構成

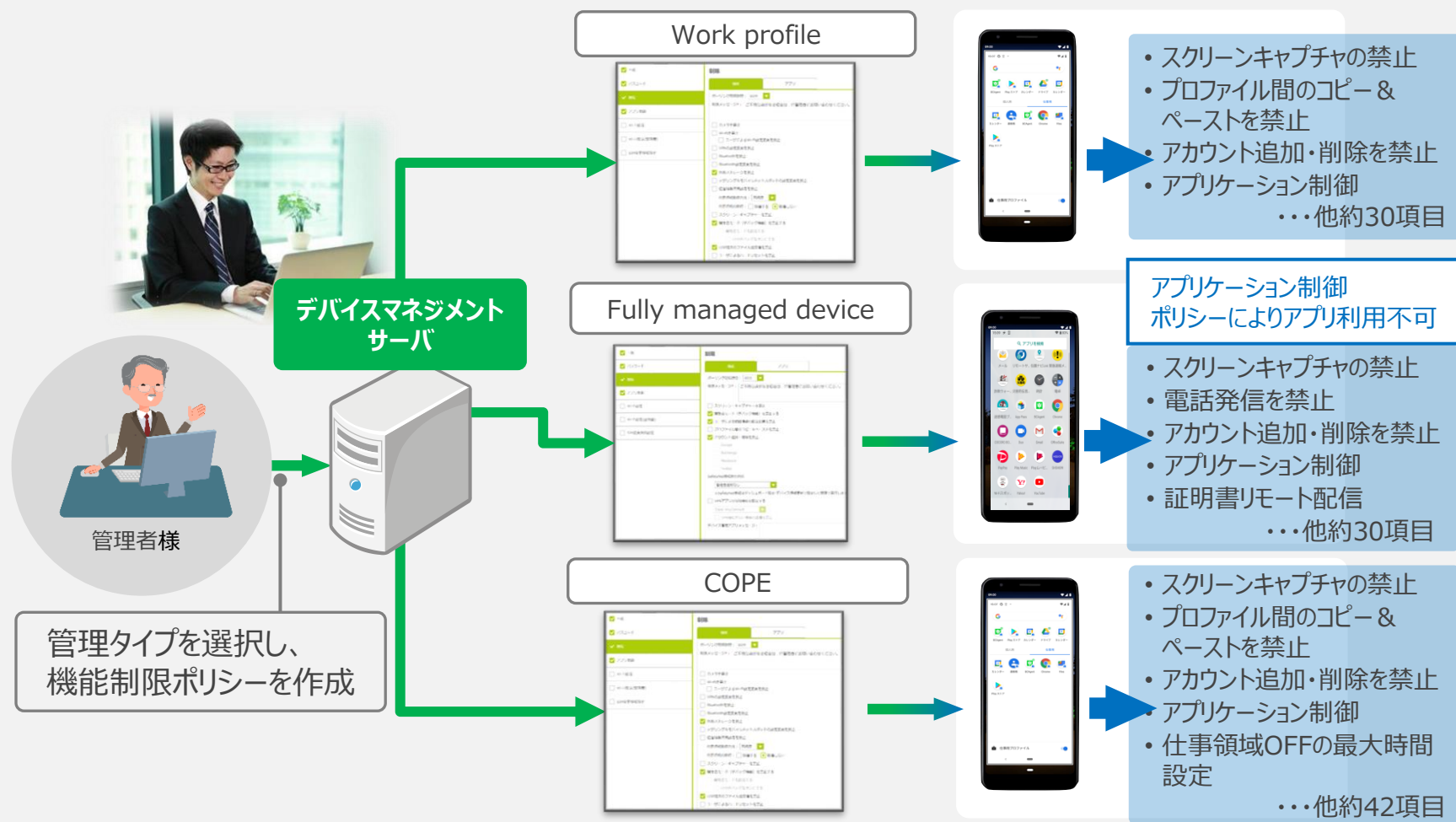
COPE



会社所有端末

デバイスに
個人領域と仕事領域を構成

管理タイプごとに適した制限ポリシーを遠隔から適用可能



※機能制限ポリシーの一覧はAppendixを参照してください。

BCDMおすすめのセキュリティレベルのポリシーが
プリセット（初期設定）された状態からポリシー登録可能

MDM管理画面

デバイス



デバイスマネジメントサーバ

ポリシー
セキュリティレベル：中



ポリシー
セキュリティレベル：中



ポリシー
セキュリティレベル：中



プリセットパターン選択

プリセットパターン ?

プリセットなし
プリセットなし
セキュリティレベル：中
セキュリティレベル：高
セキュリティレベル：中 ※高度な設定
セキュリティレベル：高 ※高度な設定

※末尾が「※高度な設定」のプリセット
画面下部の「プリセット内容説明用フ
プリセット内容説明用ファイルへのリンク

- プリセットしたいパターンを選択
- 一部の項目に設定がプリセットされた状態から、ポリシー登録が可能

※本機能はAndroid Enterpriseが対象です。

※プリセット内容の詳細は、画面内のリンクから確認可能です。

収集可能なデバイス情報の項目一覧：Android

デバイス情報	- デバイス名 - モデル名 - SIMキャリアのネットワーク - 現在のキャリアのネットワーク - ICCID - 電話番号	- IMEI - Android OSバージョン - Wi-FiのMACアドレス/UUI (※2) - BluetoothのMACアドレス - C2DM/GCM/FCMの利用状況 - APN名および利用状況 (※1)	- エージェントバージョン - Googleアカウント (※3) - Android Enterprise - ビルド番号 - 非正規利用(旧SafetyNet)検知 (※3)
リモート設定情報	ポリシー名および適用日時		
セキュリティ情報	- パスコードの義務化 - パスコードの種類 - 最小のパスコード長 - カメラの使用情報 - Wi-Fiの使用情報 - Bluetoothの利用情報	- 外部メモリの使用情報 - テザリングの利用情報 - ローカルロック - 外部メモリ消去 - ローカルワイプ - 位置情報取得情報	- Wi-Fi/モバイル接続時の位置情報の義務化 - GPS設定義務化情報 - ポーリング間隔時間
アプリケーション情報	インストールされているアプリケーション (名前、バージョン、パッケージ名)		
位置情報	- 位置情報 - 経度	位置情報の取得日時	緯度
アンチウイルス	- ソフトウェアバージョン - パターンファイルバージョン - パターンファイル更新日時	- 前回通知日時 - 前回通知からの時間 - Root化検知情報および検知日時	ウィルス検知情報および検知日時

※1 APN名および利用状況はOS4.2以降では取得できません。
※2 デバイス情報のWi-FiのMACアドレスはAndroid 6.0以降は取得できません。
※3 Android Enterprise登録デバイスのみ取得します。

Google Play アプリのサイレントインストールが可能 Playストアにも管理者が承認したアプリのみ表示



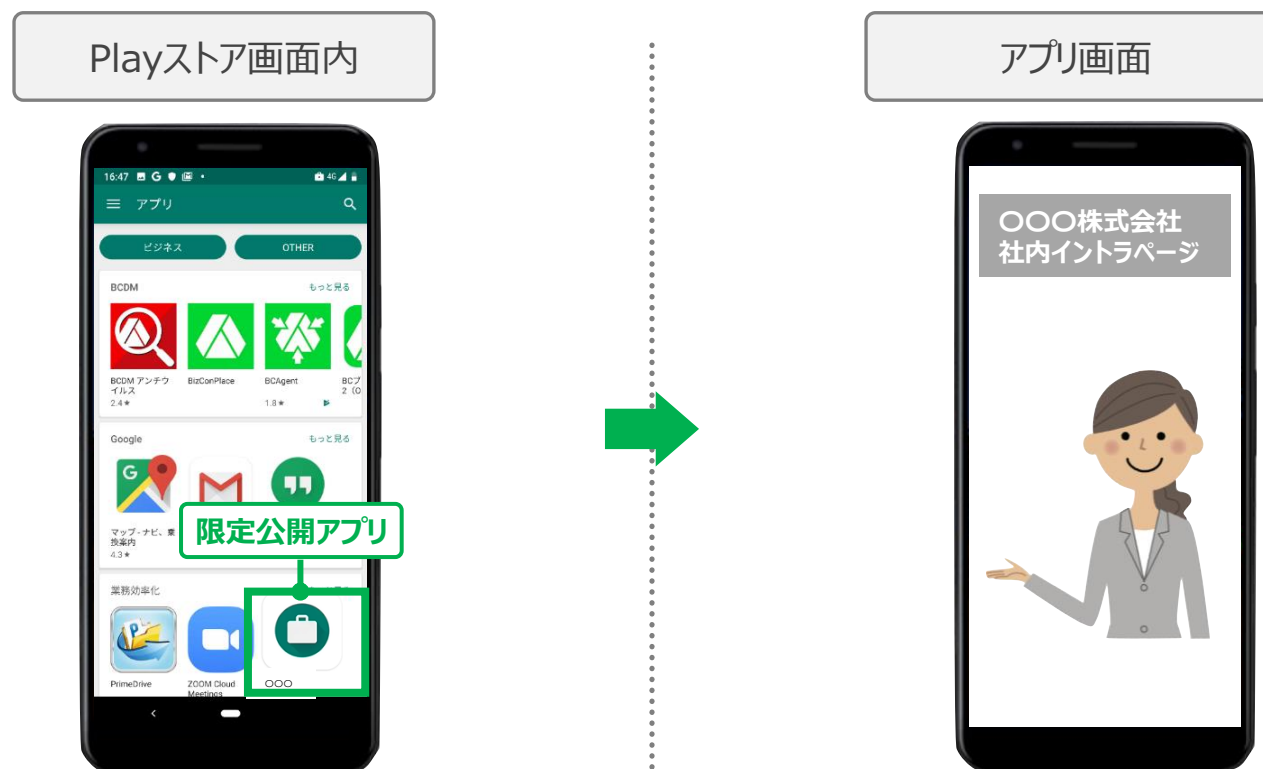
※Work profileとCOPEの場合、仕事領域のみアプリがインストールされます。

※デバイス上のPlayストア内には、管理者様が指定したアプリのみ表示されます。

※Playストアの有料アプリは対象外となります。アプリ内課金も制限されます。

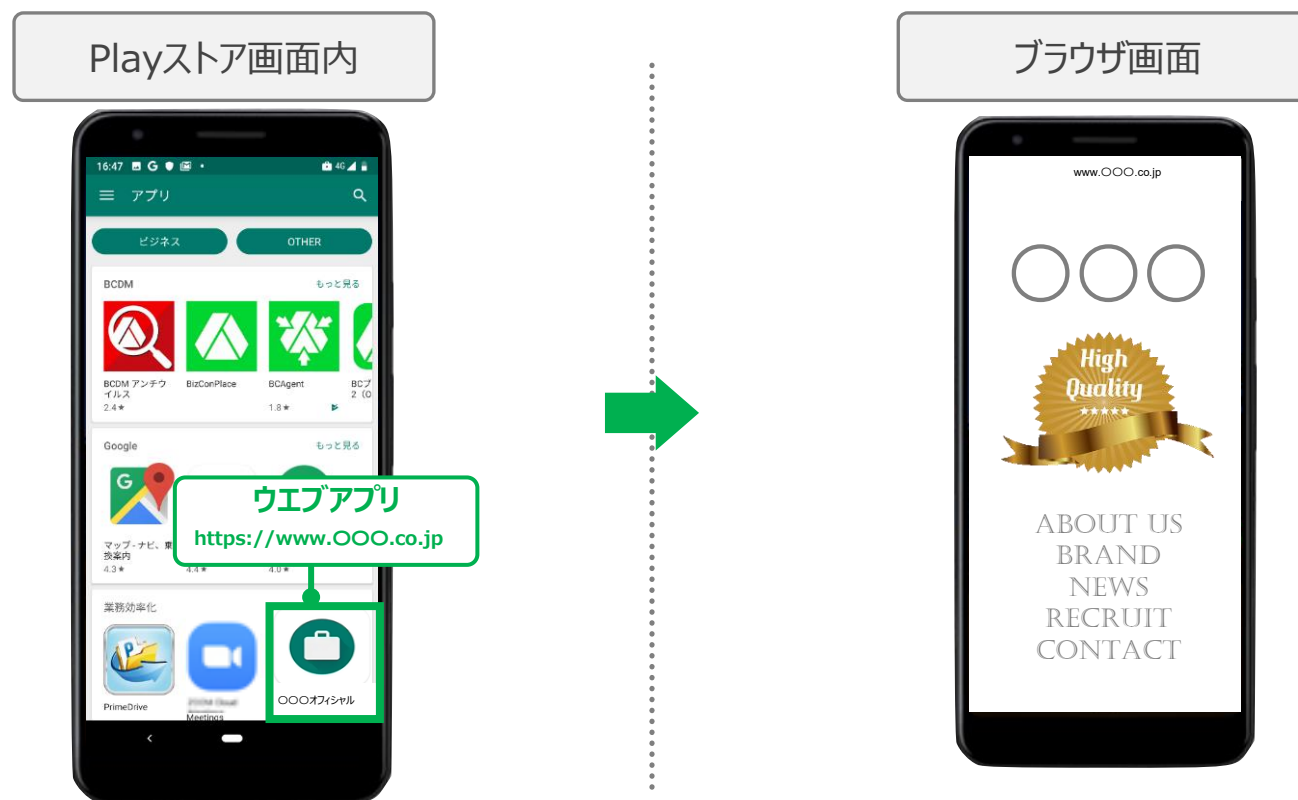
※利用者ごとにGoogle Playの表示内容を変更することはできません

社内限定の業務用アプリを「限定公開アプリ」としてGoogle Play ストアにアップロードし、サイレントインストールさせることができます。



- ※ Work profileとCOPEの場合、仕事領域のみアプリがインストールされます。
- ※ デバイス上のPlayストア内には、管理者様が指定したアプリのみ表示されます。
- ※ Playストアの有料アプリは対象外となります。アプリ内課金も制限されます。
- ※ 利用者ごとにGoogle Playの表示内容を変更することはできません
- ※ 限定公開アプリとウェブアプリ合わせて1日に最大15件のPlayストアへのアップロード制限があります。

Webページのショートカットを、Playストアにアップし
アプリのようにホーム画面に表示できる「ウェブアプリ」という機能があり
サイレントインストールさせることができます。



※ Work profileとCOPEの場合、仕事領域のみアプリがインストールされます。
※ デバイス上のPlayストア内には、管理者様が指定したアプリのみ表示されます。
※ Playストアの有料アプリは対象外となります。アプリ内課金も制限されます。
※ 限定公開アプリとウェブアプリ合わせて1日に最大15件のPlayストアへのアップロード制限があります。

ゼロタッチ登録を利用することで端末を簡単にセットアップ



ゼロタッチポータルでMDMを割り当て。パラメータを設定することでデバイス登録情報を自動反映することも可能です。

デバイスの電源をオンにすると、アクティベーション時に自動的にMDMのAgentがインストールされアクティベーションの簡素化を実現できます。

ゼロタッチポータルでデバイスとMDMの割り当てを解除しない限り、初期化してもアクティベーション時にMDMのAgentが自動的にインストールされます。

※ゼロタッチ登録とは2017年9月Googleが開始した新しい登録方式です。

※ゼロタッチを使用するにはBCDMとは別に「Android ゼロタッチ登録サービス」への申込が必要です。

※ゼロタッチが利用できるデバイスはOS8以上でゼロタッチ対応済のデバイスとなります。

※ゼロタッチ登録を使用した場合、Fully managed deviceもしくはCOPE（OS11以降～）のみの登録となります。Work profileの登録はできません。

※アクティベーションを実施する前に、ゼロタッチポータルでデバイスとAgentの紐付け作業とBCDM環境でAndroid Enterpriseの登録が必要です。

※ゼロタッチポータルでの作業はお客様作業となります。

トレンドマイクロ アンチウイルスを基本サービスとして提供

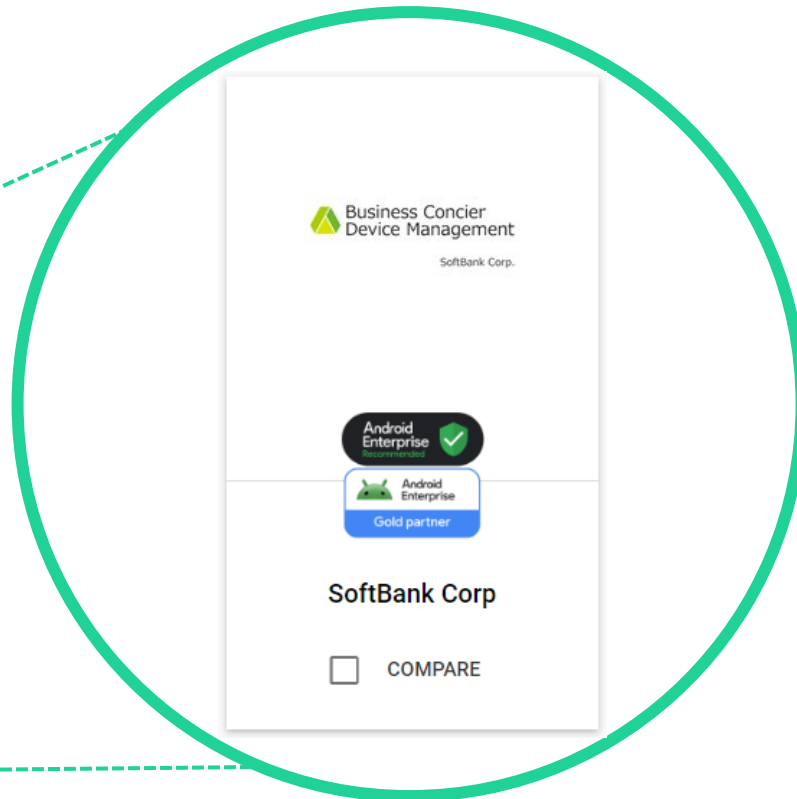
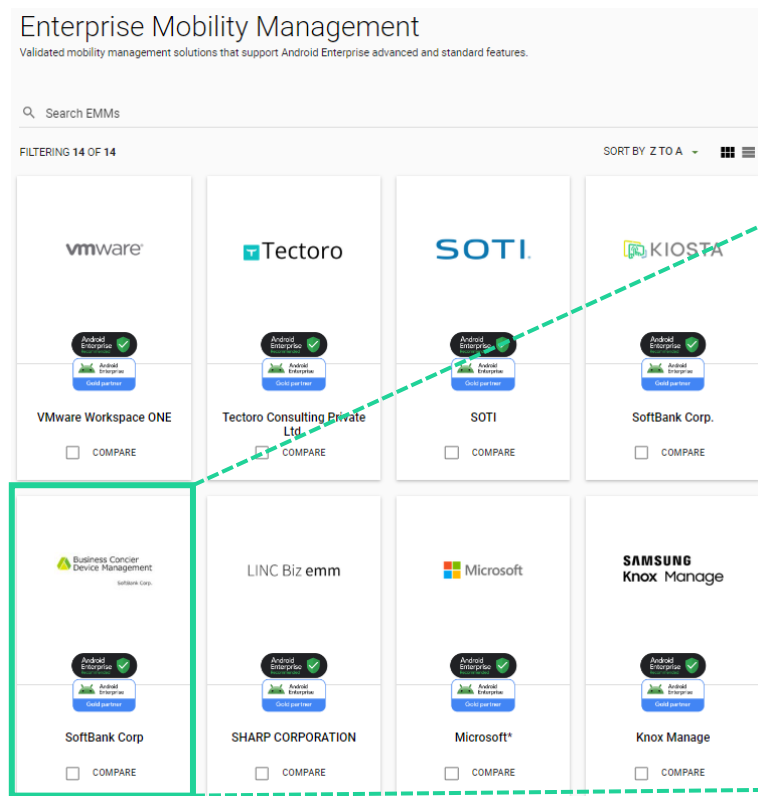


※動作確認デバイスについては右記サイトをご覧ください。(https://tm.softbank.jp/outsourcing/concierge/dm/device/android_s_for_work/)

※デバイスがウイルス感染またはroot化された場合、お客様でご対応いただけます。

機能名	概要	詳細
不正アプリ対策	不正アプリ、または偽アプリによる攻撃を防御する	デバイスにインストールされているアプリケーションが、ウイルスに感染していないかをスキャンします。ウイルスに感染している危険性がある場合は、デバイスに警告が表示され管理サイトにも通知されます。
アプリ権限チェック	アプリが不要な権限(プライバシー情報へのアクセス、外部への送信)を保持しているか確認する	デバイスにインストールされているアプリが、個人情報を漏えいする可能性がないかをスキャンします。アプリ権限チェックにはリアルタイム検索と手動検索の2種類あります。
Web脅威対策	不正な動作や内容が検知されたWebサイトへのアクセスをブロックできる機能	アクセスしようとしているサイトに不正な動作や内容が検知された場合に、該当サイトへのアクセスをブロックします。
Root化検知	Android OSを不正に改ざんし、特権的な権限を取得する行為（Root化）を確認する	デバイスに対して、root化（Android OSを不正に改ざんし、セキュリティなどの理由から制限されている操作を可能にすること）が行われていないかを検知します。root化が検知されると、管理サイトに通知されます。
パターンファイルの更新	BCDM Antivirus アプリ が搭載する検索機能にて利用するパターンファイルを更新する	不正アプリ対策に使うパターンファイルを最新に保つために、パターンファイルが更新されているかどうかをトレンドマイクロ社のサーバにアクセスして確認します。更新されている場合は、パターンファイルをデバイスにダウンロードします。
ログ収集および送信機能	本アプリの調査に利用するログを収集、及び送信する	BCDM AntiVirusが正しく動作しなくなった場合に、その原因の調査に必要な情報（ログ）を収集し、開発元のトレンドマイクロ社に送信します。

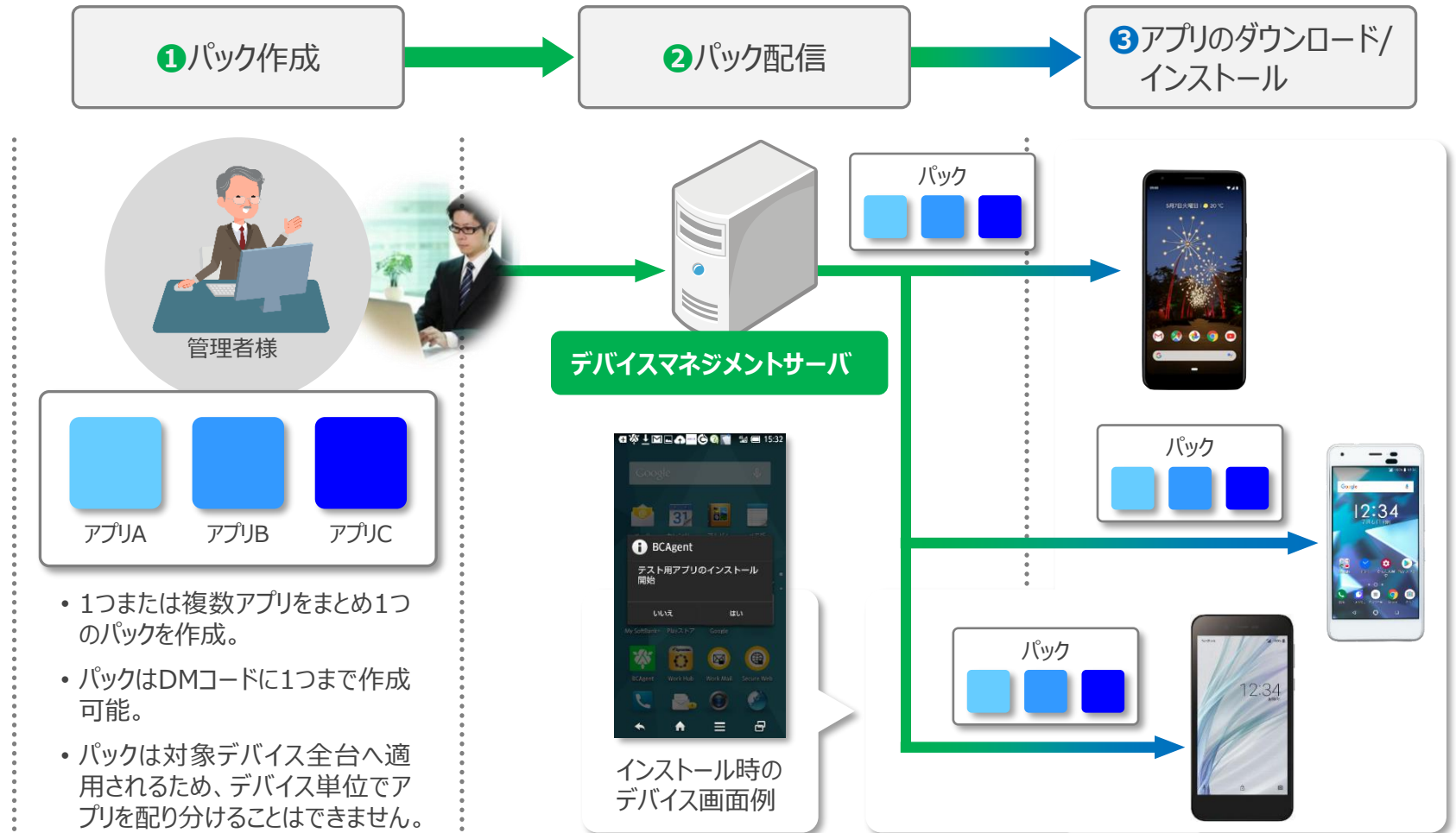
Googleからの厳しい要件を満たし、通信事業者として世界で初めて
「**Android Enterprise Recommended**」を取得
また、2023年6月に**Google Gold partner**に認定



項目	内容
同時利用の制限	ソフトバンク法人コンシェルサービスのアプリコンシェルサービス及びMDM機能を有するその他アプリと同時利用はできません。
パケット対応プラン 加入推奨	MDMエージェントソフトは定期的にサーバとポーリング通信をするため、パケット利用に対応したプランに加入しておくことを強く推奨します。
対応機種	Android OS7以降でAndroid Enterpriseに対応している端末が対象となります。 動作確認済デバイスの詳細については以下サイトをご覧ください。 (https://tm.softbank.jp/outsource/concierge/dm/device/android_s_for_work/)
Android Enterpriseの 登録方法について	Android Enterpriseの登録方法は「Android Enterprise企業登録」と「Google Workspaceトークン登録方式」の2種類あります。 「Android Enterprise企業登録」は、managed Google domain方式とmanaged Google Play Account方式の2種類あります。 <managed Google domainの場合> ・ビジネス用のお客様ドメインのメールアドレスを利用して管理者アカウントを作成する方法です。 <managed Google Play Accountの場合※> * Google非推奨 ・管理用として個人で取得できる無償のGmailアカウントを1つご用意いただく必要があります。 <トークン登録の場合> ・お客様にビジネス用のGoogleドメインおよびGoogleアカウントをご用意いただく必要があります。 個人で取得できる無償のGmailアカウントは利用することはできません。 ・ 端末上でGoogle Workspaceを利用すること並びに企業用Playストアのみを利用することを前提とされている場合は、こちらの方式をご利用いただく必要があります。
BCDM AntiVirusアプリについて	・ Work profile、COPEでデバイス登録をした場合、基本サービスとして提供するBCDM AntiVirusアプリを利用することはできません。 ・ バッテリーセーバー、省電力モード、その他電池消費を防ぐ機能が有効になっているデバイスではBCDM AntiVirusアプリが正常に動作しない可能性があるため、設定しないようお願いします。
ゼロタッチ登録	・ ゼロタッチポータルを利用するにはBCDMとは別に「Android ゼロタッチ登録サービス」へのお申込が必要です。 ・ ゼロタッチが利用できるデバイスはOS 8以上でゼロタッチ登録が可能なデバイスとなります。 ・ ゼロタッチ登録を利用した場合、Fully managed deviceもしくはCOPE（OS11以降～）のみの登録となります。 Work profileでのご利用はできません。 ・ アクティベーションを実施する前に、ゼロタッチポータルサイトでデバイスとAgentの紐付け作業とBCDM環境でAndroid Enterprise登録が必要です。
MDMを既存で ご利用中の場合	既に従来型（レガシー）の方法で管理しているデバイスに対して、Android Enterprise機能を利用したい場合、BCAgentの削除および再インストールが必要となります。 Fully managed device及びCOPEの場合、デバイス全体を仕事領域にするためデバイス初期化が必要となります。

※無償のGmailアカウントを取得し、managed Google Play Account方式にてトークン登録を実施をしている場合、登録に使用しているGmailアカウント(管理アカウント)がGoogle社でポリシー違反と判断されたケースにおいてアカウントの凍結、削除(もしくは凍結後、削除)がGoogle社によって実施されることがあります。
また1つのアカウントが削除されても、他の紐づいているアカウントで継続して利用できるように管理アカウントを複数設定してご利用ください。

インハウスアプリの遠隔Push配信が可能



項 目	内 容
配布可能アプリ	インハウスアプリのみで、Google Play ストア アプリは対象外となります。
配布方法	iOS版Managed Appsと異なり、アプリ単位での配布はできません。 配布はパック単位となり、1つまたは複数のアプリをまとめたパックを作成し、配布します。
アプリ登録上限	登録可能上限は40MB、30個までとなります。
アプリ数配布上限	配布上限は10個までとなります。
配布対象デバイス	Ver2.26.01以降のBCAgentがインストールされたデバイスが対象で、 2015年4月13日以降にデバイス登録したデバイスへの配布が可能です。 2015年4月13日より前にデバイス登録したデバイスは、BCAgentのバージョンアップが必要になります。
ステータス管理	iOS向けManaged Appsと異なり、配布後のステータス管理はできません。

項 目	アプリケーション配布	Managed Apps (パック型リモート配信)	Google Play アプリ配信 (Android Enterprise)
配信方法	アプリ配布サイトに掲載し 指定リンクからダウンロード	リモート配信	サイレントリモート配信
対象アプリ	インハウス/Google Play	インハウスのみ	Google Playのみ
配布単位	アプリ単位	パック単位 1DMコード：1パックまで 1パック：アプリ10個まで	アプリ単位
登録上限 (通常)	40MB、30個まで	40MB、30個まで	1,000 (※1)
登録上限 (Managed Apps容量拡張)	—	600MB、30個まで	—
ステータス管理	—	配布開始～配布完了まで	常時
バージョンアップ	上書き可能	アプリ削除後に再配信	アプリが登録済の場合、 アプリの更新可 (※2)
インストール開始/終了 メッセージ指定	指定不可	指定可能	指定不可

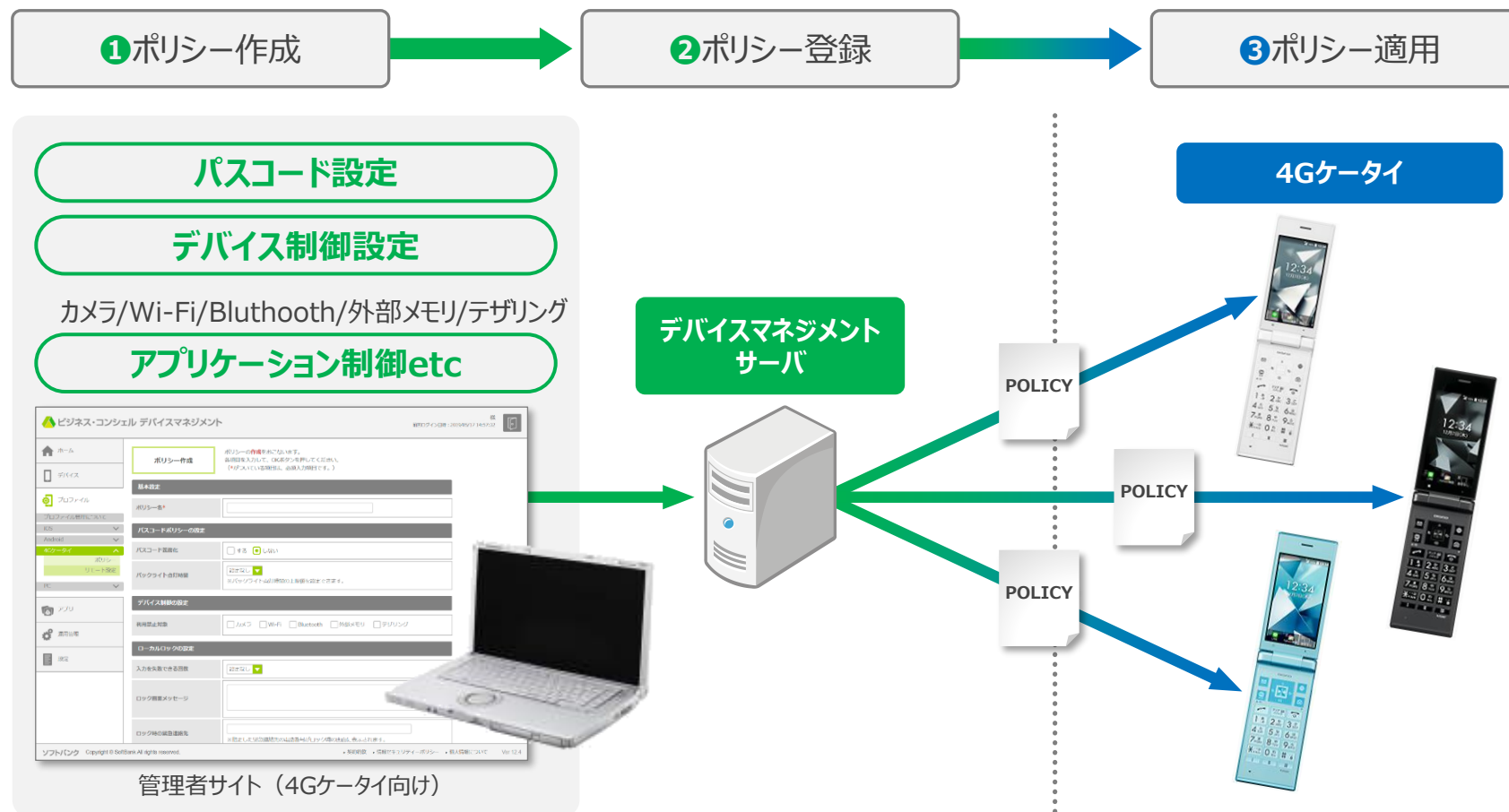
※1 限定公開アプリとウェブアプリ合わせて1日に最大15件のPlayストアへのアップロード制限があります。

※2 更新タイミングはデバイスのPlayストアの「アプリの自動更新の設定」または「管理画面側の設定内容」によります。

※2 更新時にはPlayストアレイアウトにアプリを表示しておく必要があります。

基本サービス [4Gケータイ]

遠隔からのポリシー適用可能



※詳細な遠隔設定項目はAppendixをご覧ください。

※4Gケータイの場合、FCMサービスが利用できないためポーリング（定期）通信での適用となります。

リモートからWi-Fi設定/Wi-Fiアクセス制御が可能

1つの設定ファイル内に最大3個のWi-Fiを設定することができます。

リモート設定は1つのデバイスに対して複数の設定ファイルを作成し、配信することが可能です。

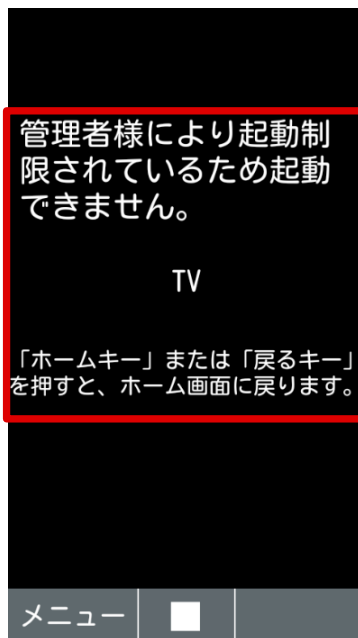
また、接続を許可するWi-Fiアクセスポイントを設定することができます。



指定アプリの起動制御、アンインストール指示が可能

アプリケーション制御

指定したアプリケーションの
起動を制御



アンインストール指示

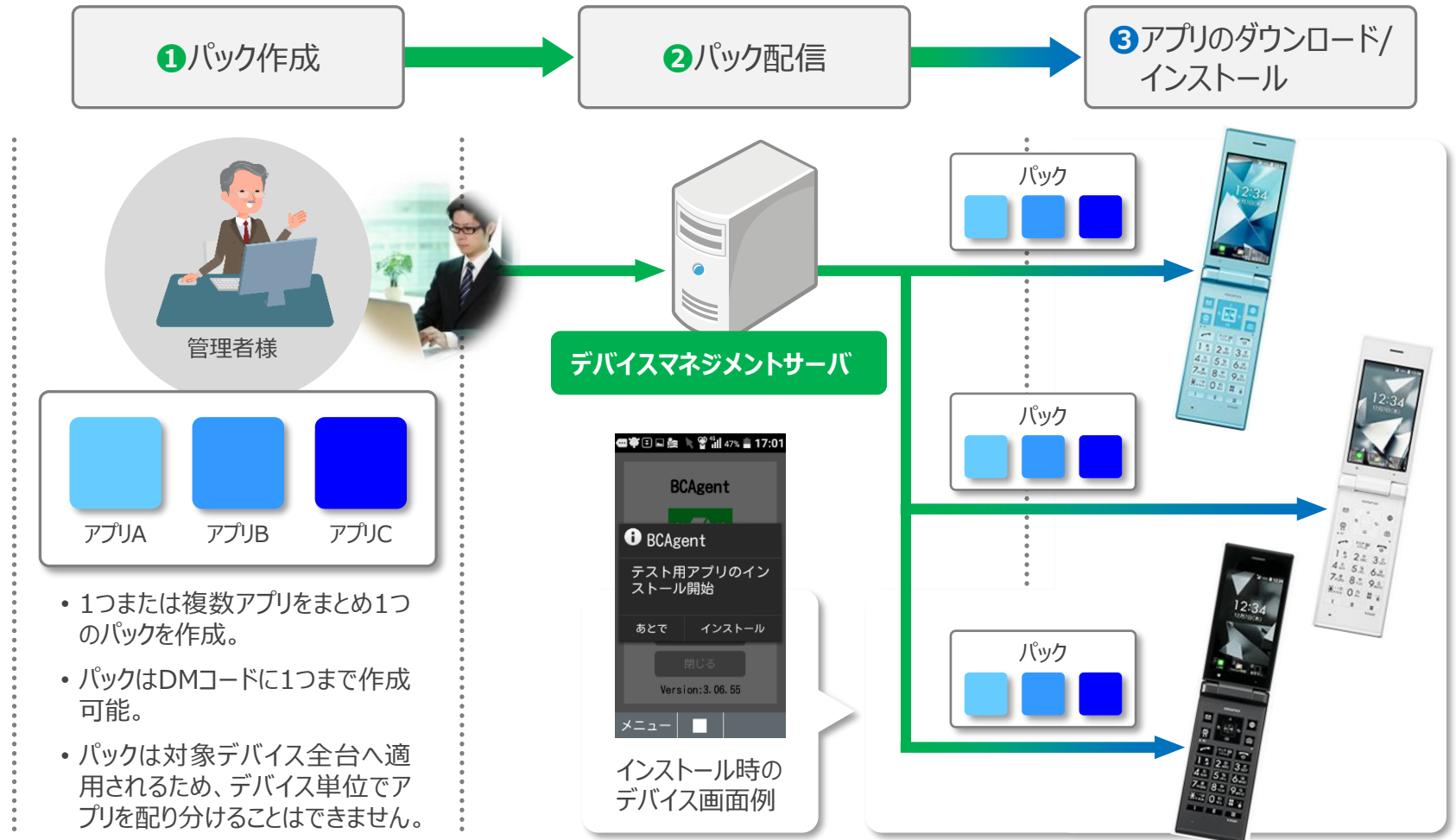
指定したアプリケーションのアンインストールを誘導



※アプリの仕様によりアプリケーション制御がかからない場合がありますので、お客様のデバイスにて動作確認を実施の上、ご利用ください。

※アンインストール指示は、デフォルトアプリは対象外となりますので、MDM等の機能でインストールさせたアプリが対象となります。

インハウスアプリの遠隔Push配信が可能



項 目	内 容
配布可能アプリ	インハウスアプリのみとなります。
配布方法	iOS版Managed Appsと異なり、アプリ単位での配布はできません。 配布はパック単位となり、1つまたは複数のアプリをまとめたパックを作成し、配布します。
登録上限	登録可能上限は40MB、30個までとなります。
配布上限	配布上限は10個までとなります。
配布対象デバイス	BCAgentがインストールされたデバイスが対象です。
ステータス管理	iOS向けManaged Appsと異なり、配布後のステータス管理はできません。
配布間隔	4Gケータイの場合、FCMサービスが利用できないため定期通信（ポーリング）での配布となります。

基本サービス [PC管理]

特徴① セキュリティ機能が盛りだくさん

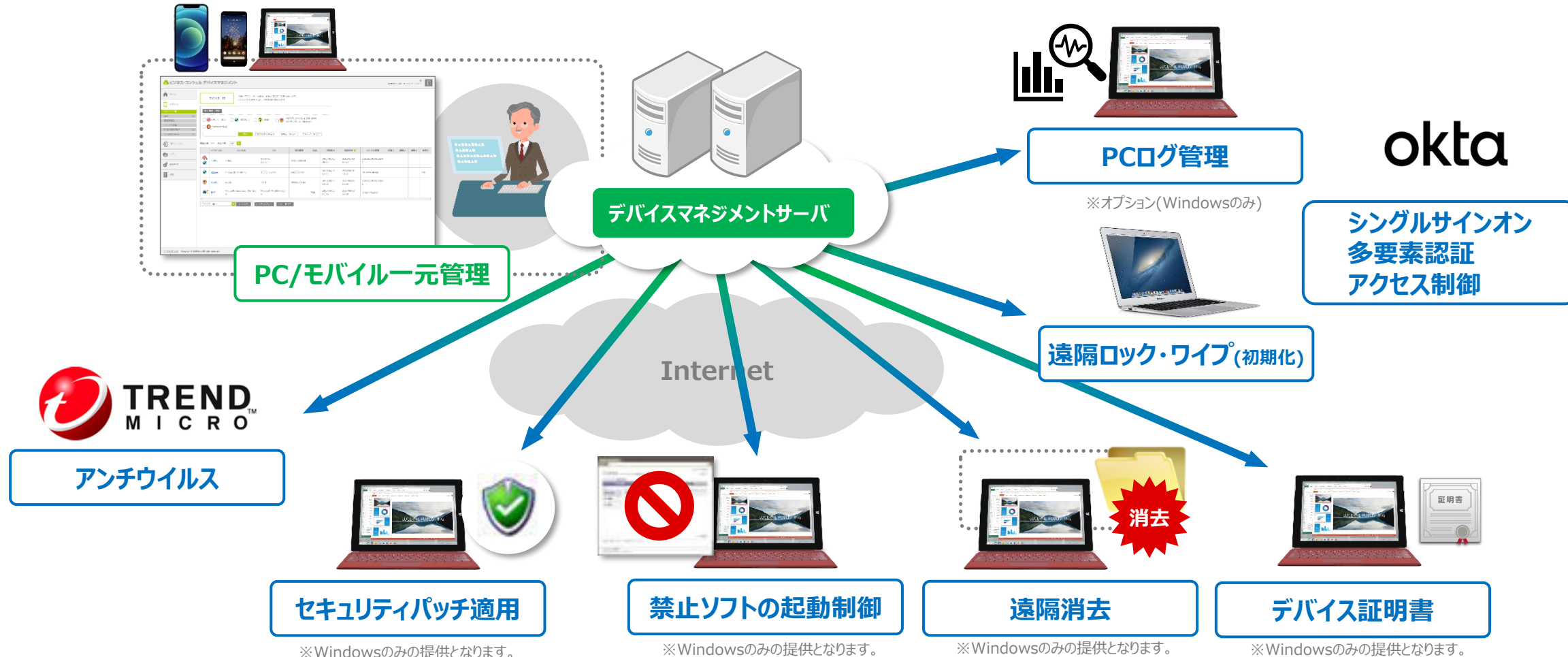
Windows

Mac

SoftBank

PC向け必須セキュリティ機能をワンパッケージにて提供

たくさんのサービスを導入しなくてもPC管理サービス1つで解決



スマートフォンとPCを同一コンソールで管理可能



管理者様

ビジネス・コンシェル デバイスマネジメント

デバイス一覧

登録しているデバイスの機能、利用状況等の一覧を表示します。
デバイスを追加する、詳細情報を表示します。

☐ 最新バージョンへ更新
 ☐ 更新成功
 ☐ 更新中
 ☐ MDMプロファイル無効化
 ☐ 管理外デバイス (Android)

☐ SafetyNet検出

検索結果: 7件 表示件数: 25件

デバイス名	モデル名	OS	出荷量	品名	登録日時	削除日時	シリアル	更新1	更新2	更新3	圧迫1
iPhone	iPhone X (18099)	12.1.1 (18A203)	00047030877		2019/07/03 13:59	2019/07/03 13:59	FL17W43QCL				
Pixel 3a XL	Pixel 3a XL	9 AE (wmd)	000130000181		2019/06/27 14:54	2019/06/27 14:52	0058080001102467				
Pixel 3a	Pixel 3a	9 AF (wmd)	00042525403		2019/06/27 16:39	2019/06/27 14:45	0058080001102468				
iPhone	iPhone XR (MT002)	12.3 (18F156)	00049296628		2019/06/19 18:00	2019/06/12 10:18	F46X22Y90K				
704KC	704KC	8.1.0 AF (wmd)	000117351664		2019/06/28 00:21	2019/06/03 09:27	0058080001102365				
502KC	502KC	7.1.1	000136077548		2017/08/03 13:05	2017/08/03 13:04	0058080001102366				
Microsoft Corporation	Microsoft Windows 8.1 Pro			登録	2017/04/03 17:58	2017/04/03 16:40	0058080001102367				



管理デバイス (PC)

管理可能な情報

デバイス情報
資産管理情報

セキュリティパッチ(※)
アンチウイルス情報

インストール
ソフトウェア(※)

Windows Update
設定状況(※)

※一部Windowsのみの提供となります。

情報取得可能項目①

デバイス情報	• 収集日時 • コンピュータ名 • ログオンユーザ名 • 参加ドメイン	• メーカー名 • モデル名 • マシンシリアル番号 • 起動日時	• CPU情報 • メモリ情報
ネットワーク情報	• ネットワークアダプタ • MACアドレス • WINS使用	• DHCP情報 • IPアドレス • サブネットマスク	• デフォルトGW • DNS
OperationSystem InternetExplorer	• OS • OSバージョン • OSビルド番号 • サービスパック	• ファイアウォール設定 • 設定使用者 • 設定所属組織 • プロダクトID	• システムディレクトリ • インストール日
プリンター情報	• プリンター名 • ドライバー名 • ドライバーパス	• ドライバーバージョン • プリントプロセッサ名 • プリンター種別	• 解像度 • ポート名

情報取得可能項目②

セキュリティ情報	• AntiVirusプロファイルバージョン • HotFixプロファイルバージョン • MSIEOfficeプロファイルバージョン • Adobeプロファイルバージョン	• オプション製品プロファイルバージョン • JAVAプロファイルバージョン • Webブラウザプロファイルバージョン • Webサーバプロファイルバージョン	• セキュリティパッチ種別 • サポート技術コード
ソフトウェア情報	• 製品名 • 製品バージョン • 会社名 • 禁止ソフトウェア • ソフトウェアID	• パス名 • ファイル名 • ファイルバージョン • ファイルサイズ • ファイル更新	
自動更新設定	• WindowsUpdate自動設定 • WSUSサーバ有無 • WindowsUpdate更新方法 • インストール時間	• インストール日 • サーバ名 • ステータスサーバ名	
位置情報 ※M6のみ	• 位置情報		

情報取得可能項目

デバイス情報	- 収集日時 - コンピュータ名	- ログオンユーザ名 - モデル名	- CPU情報 - メモリ情報
ネットワーク情報	- MACアドレス - WINS使用 - DHCP情報	- IPアドレス - サブネットマスク - デフォルトGW	- DNS - OS言語
Operation System Internet Explorer	OS	OSバージョン	
プリンター情報	- 製品バージョン - パス名	- ファイル名 - ファイルサイズ	ファイル更新

情報取得可能項目

デバイス情報	• 収集日時 • デバイス名 • モデル名および番号 • OSおよびビルドバージョン • デバイス登録日時 • UDID • 容量 • メモリ情報	• 使用可能な空き領域 • シリアル • Wi-FiのMACアドレス • BluetoothのMACアドレス • ローカルホスト名 • iTunesStoreアカウント有効/無効 • アクティベーションロック有効/無効	• ソフトウェアアップデート設定有効/無効 - アップデートを確認 - AppStoreからのアプリケーションアップデートをインストール - macOSアップデートをインストール - システムデータファイルとセキュリティアップデートをインストール - 新しいアップデートがある場合はダウンロード • System Integrity Protection有効/無効
プロファイル	• プロファイル名 • 識別子 • 組織	• 説明 • 削除可否 • 削除用パスワード	• 暗号化
アプリ	• アプリケーション名 • アプリバージョン	• アプリ容量 • アプリケーションID	
証明書	• コモンネーム（CN） • 発行者名	• 発行開始日 • 有効期限	• 秘密鍵

資産情報もデバイスマネジメントで一元管理が可能

資産情報登録

利用

資産情報

デバイス

ネットワーク

コンピュータ名	
資産管理番号	
資産区分	
機器名称	
機器管理番号	
設置場所(郵便番号)	
設置場所(住所1)	
設置場所(住所2)	
設置場所(住所3)	
保証期間開始日	
保証期間終了日	

リース・レンタル会社名	
契約番号	
リース管理番号	
リース・レンタル開始日	
リース・レンタル終了日	
契約金額	
支払日	
初回支払金額	
支払金額1	
支払金額2	
支払金額3	
支払金額4	
支払金額5	

- リース/レンタル会社名
- リース管理番号
- 資産区分
- 機器管理番号
- レンタル終了日
- 保証期間終了日
- 契約番号
- 資産管理番号
- 機器名称
- レンタル開始日
- 保証期間開始日

資産情報一覧

ビジネス・コンシェル デバイスマネジメント

最新ログイン日時: 2019/05/15 15:31:13

ホーム

デバイス

デバイス一覧

PC資産情報一覧

登録しているデバイスの資産情報を表示します。

検索

検索条件で絞り込み

検索名で絞り込み

グループで絞り込み

検索結果: 1件 表示件数: 25件

	コンピュータ名	機器管理番号	リース管理番号	資産管理番号	IPアドレス
☐	保証				126.167.8.94

プリンタCSV出力

ソフトウェアCSV出力

ソフトウェアCSV出力

資産情報CSV出力

資産情報一括出力

CSVファイルに一括出力

CSVファイル

デスクトップPC

ノートPC

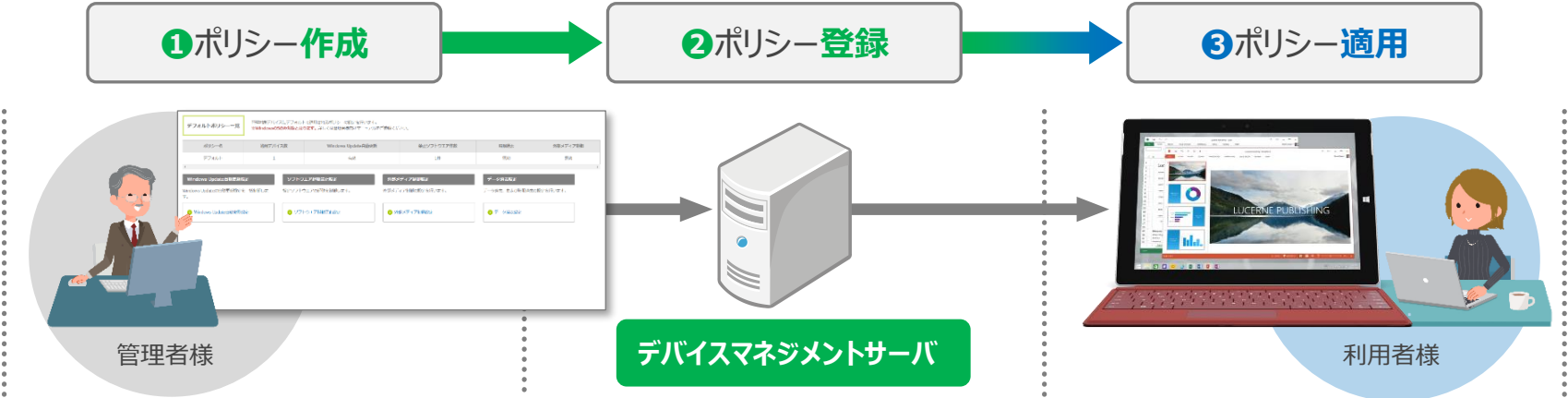
タブレット

※登録できる情報の詳細につきましてはAppendixをご覧ください。

© SoftBank Corp. All Rights Reserved.

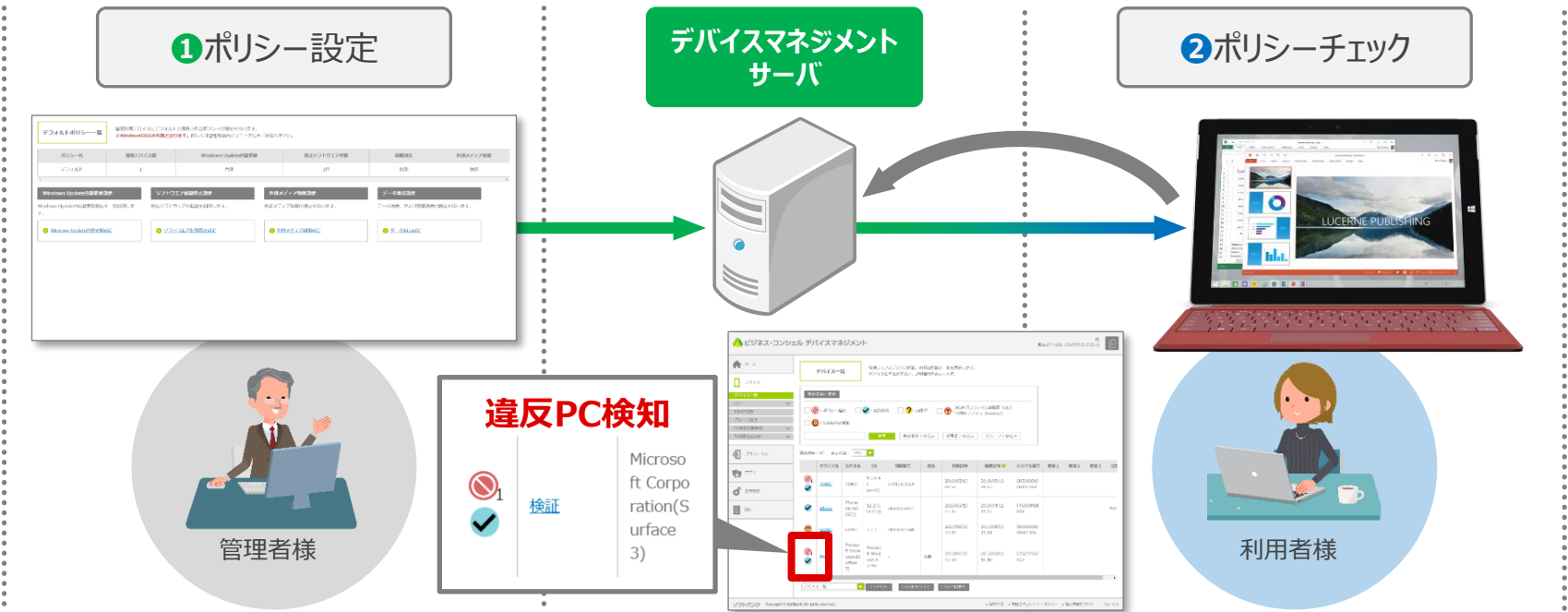
85

リモートからポリシー設定可能



ポリシー設定項目	詳細	備考（制限事項など）
WindowsUpdate自動設定	- WindowsUpdate更新方法の統一化 - 設定上書きスケジュール指定	ローカルでの設定変更抑止が不可能（WSUSのような事が不可）
ソフトウェア起動禁止設定	- グレーゾーンアプリのデフォルト禁止 - 個別によるアプリ選択 - 禁止アプリ起動時のポップアップメッセージ設定	
データ消去設定	- マイドキュメントとデスクトップの消去有無設定 - 任意フォルダ/ファイル5個までの消去設定	デバイス単位で設定可能
Chromeポリシー設定	Webブラウザ「Chrome」のポリシー設定	

セキュリティポリシー違反PCの検知と確認が可能



セキュリティポリシー項目	内容
ウイルス対策ソフト違反	最新のアンチウイルス対策ソフト以外がインストールされたPCを検知
セキュリティパッチ違反	最新のHotFixがインストールされていないPCを検知
禁止ソフトウェア違反	指定した禁止ソフトウェア一覧に該当するソフトウェアがインストールされたPCを検知

Windows PCに対してパスワードのポリシーを設定

ホーム

デバイス

プロフィール

プロフィール管理について

iOS

Android

4Gケータイ

Windows

デフォルトポリシー

個別ポリシー

外部メディア登録

アプリ

運用管理

設定

契約者向けサポート

SaaSサポートポータル

管理者向けFAQ・フォームでのヘルプデスク問い合わせはこちら

パスワードポリシー設定

パスワードポリシーの設定を行います。

基本設定

設定確認

登録

パスワードポリシー設定

設定しない

設定する

最小文字数の設定

設定しない

設定する

最小文字数

1

※1~14文字の間で数字を入力してください。

変更禁止期間の設定

設定しない

設定する

変更禁止期間

1

日

※1~998の間で数字を入力してください。

有効期間の設定

設定しない

設定する

有効期間

1

日

※1~999の間で数字を入力してください。

履歴記録数の設定

設定しない

設定する

履歴記録数

1

※1~24の間で数字を入力してください。

パスワード制御方法

設定確認周期

1時間

デフォルトポリシーへ

設定確認へ

パスワードポリシーの設定
を入力しポリシーを適用

ローカル セキュリティ ポリシー

ファイル(E) 操作(A) 表示(V) ヘルプ(H)

セキュリティの設定

アカウント ポリシー

パスワードのポリシー

アカウント ロックアウトのポリシー

ローカル ポリシー

セキュリティが強化された Windows ファイル

ネットワーク リスト マネージャー ポリシー

公開キーのポリシー

ソフトウェアの制限のポリシー

アプリケーション制御ポリシー

IP セキュリティポリシー (ローカル コンピュータ

監査ポリシーの詳細な構成

ポリシー

パスワードの長さ

パスワードの変更禁止期間

パスワードの有効期間

パスワードの履歴を記録する

暗号化を元に戻せる状態でパスワードを保存する

複雑さの要件を満たす必要があるパスワード

セキュリティの設定

0文字以上

0日

42日

0回

無効

有効

Windowsのポリシーに適用

設定したポリシーに違反する
パスワードには変更不可

パスワードの変更

パスワードを更新できませんでした。新しいパスワードとして指定された値は、パスワードの長さ、複雑さ、または履歴に関するドメインの要件を満たしていません。

OK

外部メディアデータの読取/書込を制御

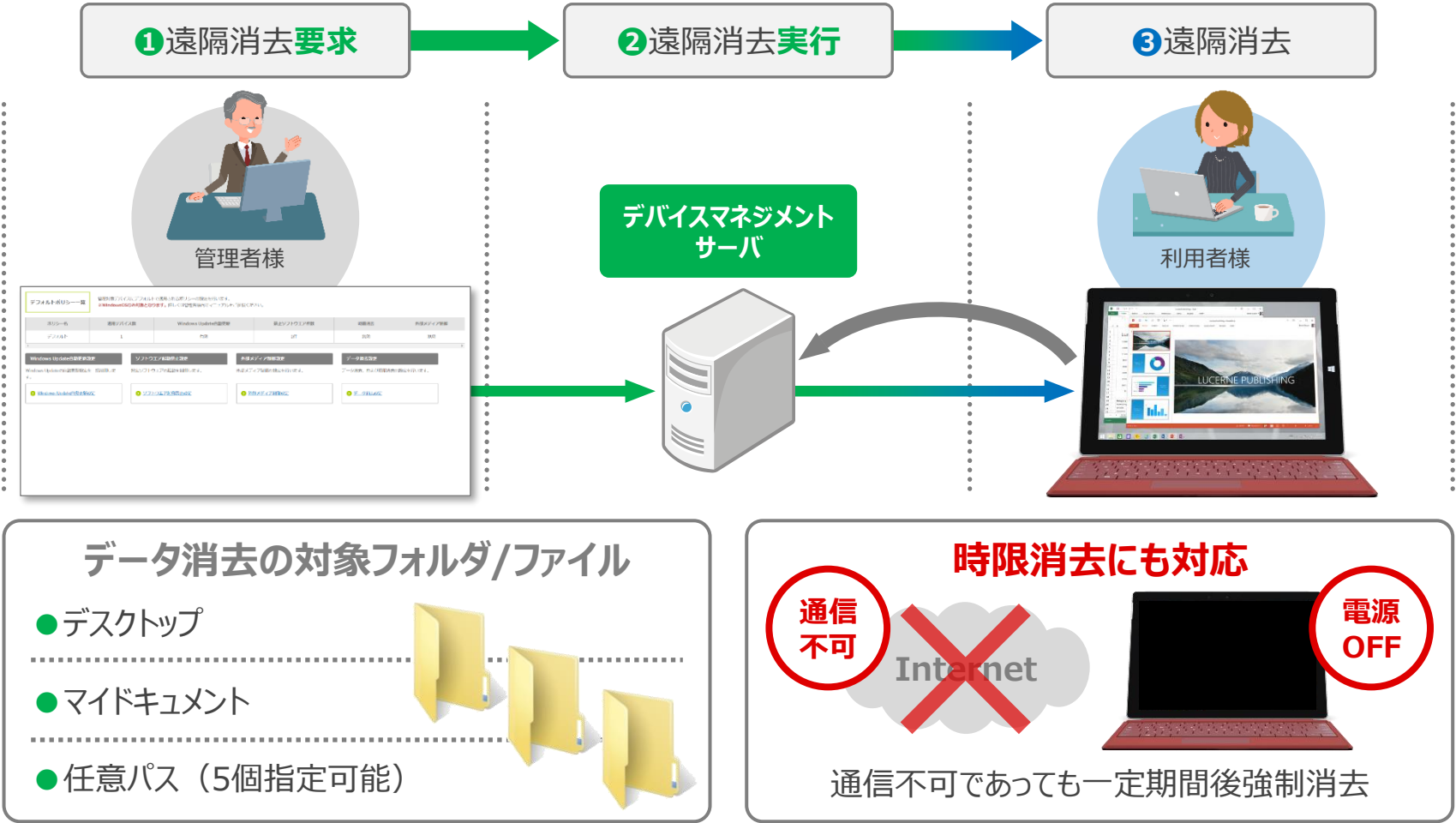


ソフトウェアの一括配布/インストールが可能

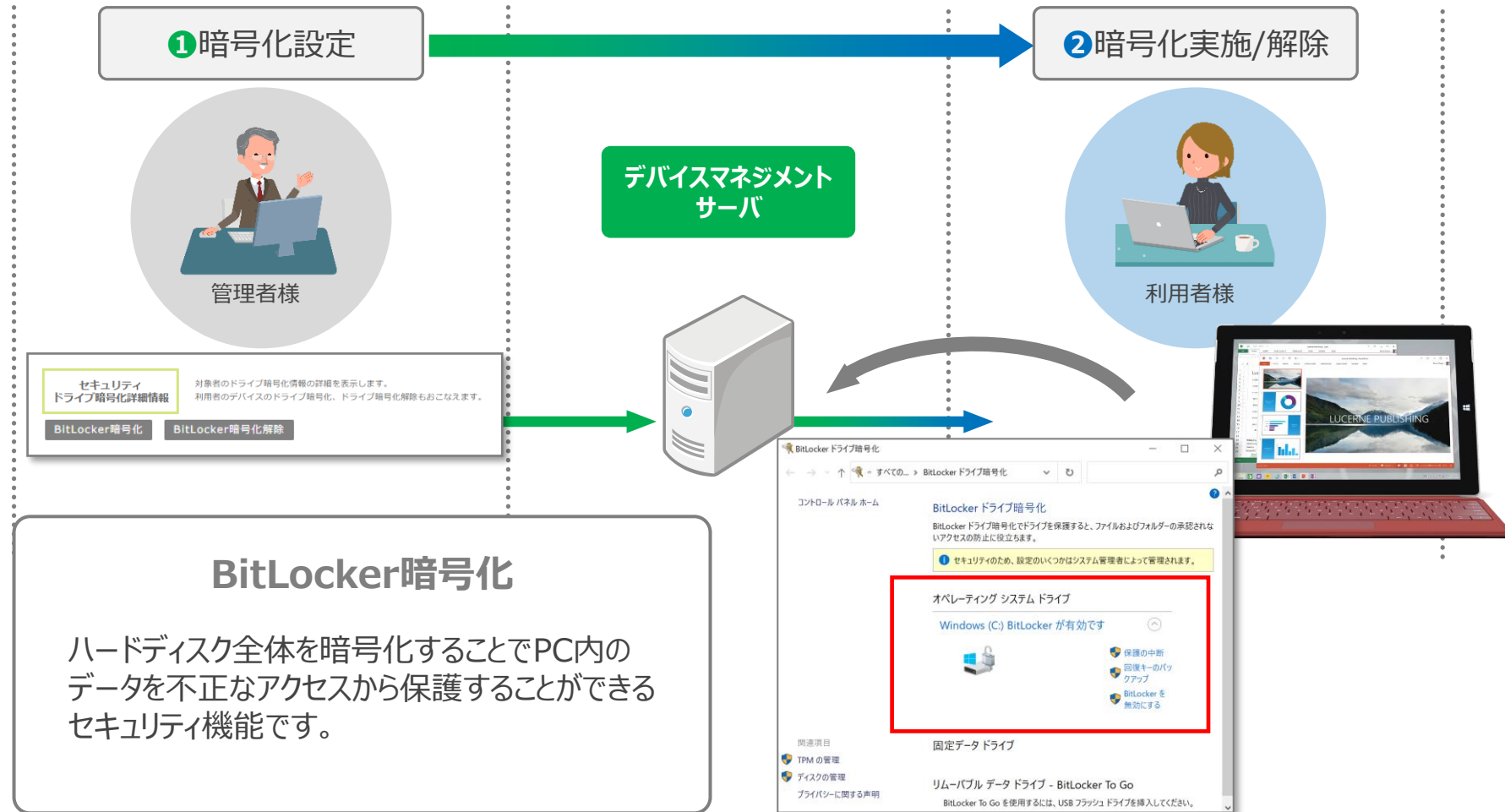


※ご利用には、オプション：ManagedAppsサービス（無償）のお申し込みが必要です。
※配信できるファイルの数、種類、サイズには制限があります。

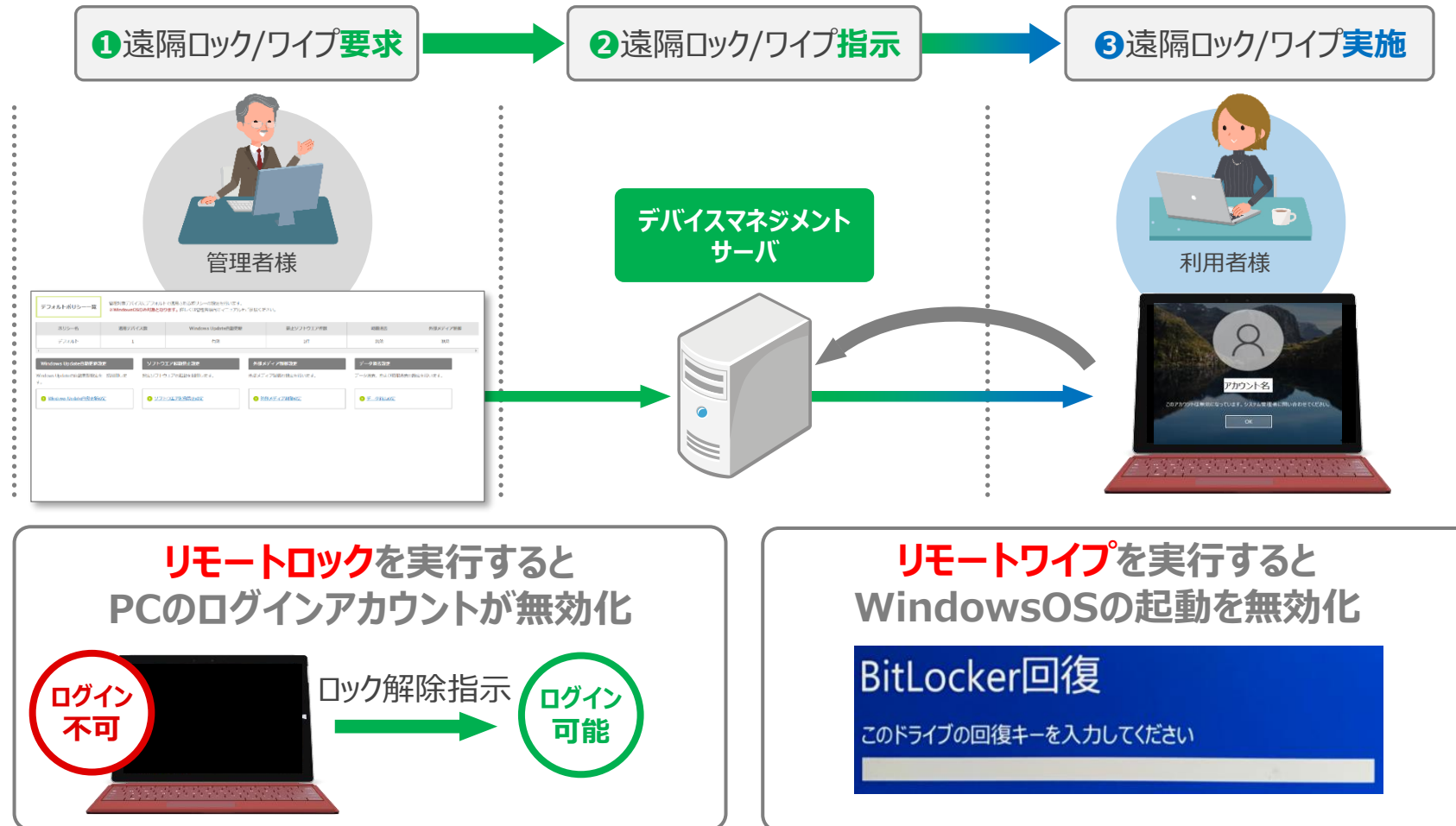
リモートから指定フォルダ/ファイルのデータ消去が可能



BitLocker暗号化/暗号化解除の設定変更が可能



リモートからロック/ワイプが可能



※本機能はWindows10 Pro・Enterprise/Windows11 Pro・EnterPriseが対象です。

項目 1	項目 2	詳 細
消去対象	消去対象フォルダ設定	マイドキュメント、デスクトップ、任意指定（5つまで）
	データ消去方式	ランダムデータを2回、0を1回書き込み
	データ消去時間	PCスペックに依存（参考値：1GBあたり60～90秒）
	消去対象外ファイル①	Windowsの起動や本プログラムの実行に必要なファイルは消去対象外。 （消去の対象外となるもの：Windowsフォルダ、OSの起動に必要なフォルダ、システムファイルフォルダ、本プログラムインストールフォルダ等） CドライブまたはDドライブを消去対象指定しても同様。
	消去対象外ファイル②	消去実行時にファイルが利用中の場合は消去不可。 ※例外としてMicrosoftのWord、Excel、Power Point、およびPDFファイルは開いている状態でも消去することが可能。
時限消去	時限消去機能	専用エージェントから管理サーバへのポーリングが一定期間有効にならなかった場合、データ消去を実行する機能。 ※PCの時刻を12時間以上変更した場合もデータ消去されます。
	時限消去期間設定	管理画面にて1～365日の間で設定（1日単位）
	時限消去ガードタイム	時限消去実行直前に5分間の猶予期間あり、データ消去の実行日時になっても、PCの起動から5分以内にネットワークに接続して管理サーバとの接続が成功すると、データ時限消去はリセットされる。 PCを紛失して管理サーバにて消去命令を発行している場合は、消去命令を受信することでデータ消去が実行される。

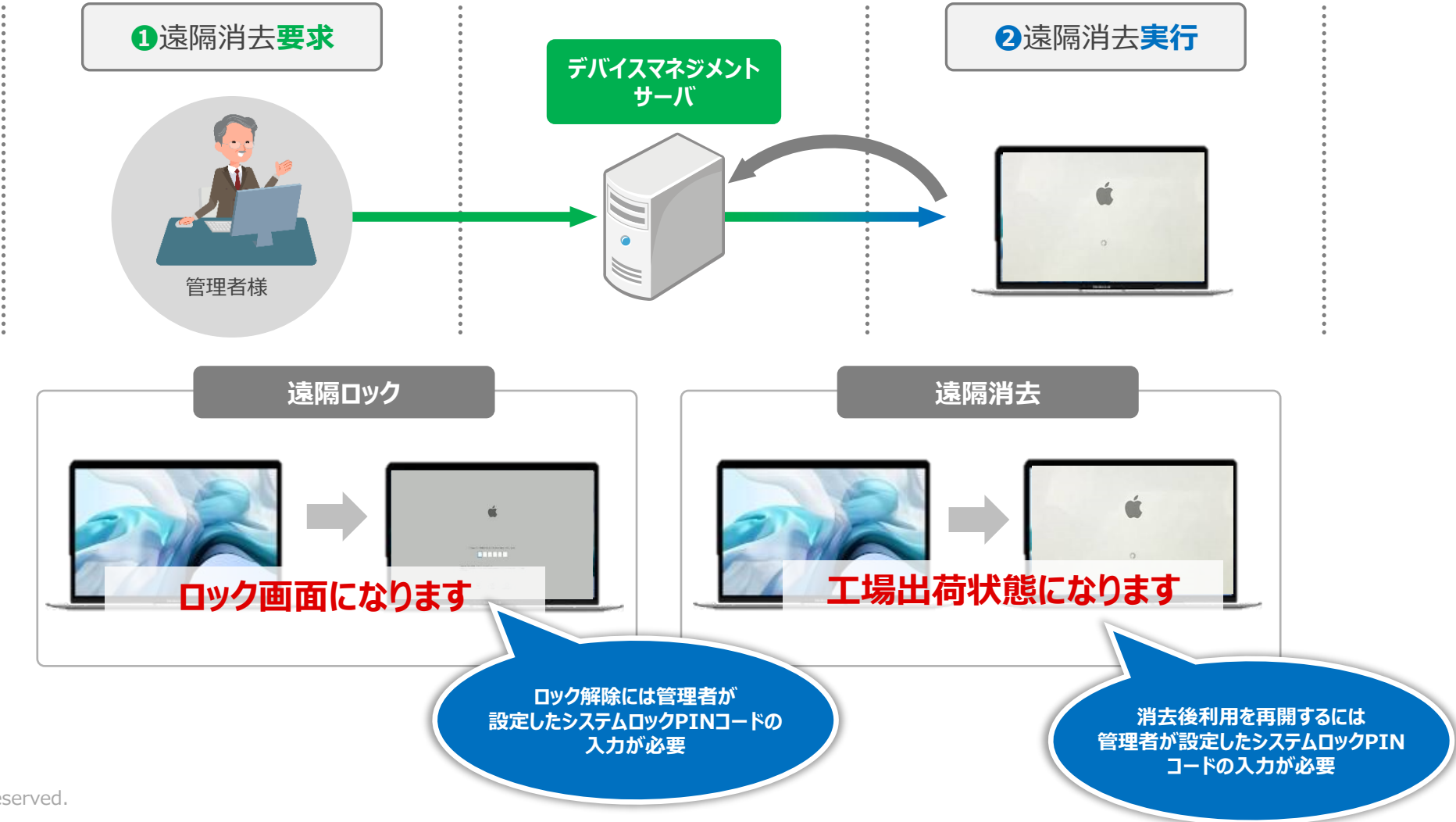
トレンドマイクロ アンチウイルスを基本サービスとして提供



提供機能	Windows	Mac
ウイルス対策、スパイウェア対策	○	○
スキャン	○	○
不正サイト接続ブロック	○	○
Webレピュテーション・URLフィルタ	○	○

※機能詳細につきましてはAppendixをご覧ください。

遠隔からのロック/消去が可能のためデバイス紛失時も安心



項目	詳細
初期設定	- Mac PCを管理するには、iOSを管理する際と同様にMDM証明書の取得が必要となります。 ※既にiOSを管理されていて、MDM証明書を登録済みの場合は不要です。 - MDM証明書はInternet Explorerからでは取得できません。
MDM証明書の更新	1年に1回、MDM証明書の有効期限が切れる前に更新が必要となります。その際、申請時に使用したApple IDとパスワードが必要となりますので、忘れないように管理して下さい。有効期限が切れたままの状態では、端末と管理サイトの疎通が取れず、Mac関連の操作ができません。
MDM証明書用のApple ID取得	個人のApple IDを使用すると、管理者が変更になった等の理由からMDM証明書の更新が煩雑になる懸念があります。その為、MDM証明書専用のApple IDを新しく取得することを推奨します。
初回ログイン時に管理者メールアドレスのメーリングリスト設定	MDM証明書有効期限通知のメールは、設定された管理者メールアドレスに送信されます。そのため初回ログイン時に、管理者メールアドレスを関係者が含まれたメーリングリストに設定しておくことを推奨します。
MDM証明書の無効化	作成したMDM証明書は絶対に無効化（Revoke）しないでください。無効化すると、全ての導入作業を最初からやり直す必要があります。
遠隔ロック	- 遠隔ロックを実行した場合、管理サイトからキャンセルすることはできません。 - 遠隔ロック中は情報を更新することができません。そのためロック実施時、保存していない作業データが消えてしまう可能性があります。
遠隔消去	- 遠隔消去を実行すると、MDMプロファイルや全ての構成プロファイルの設定情報がデバイスから削除されるため、管理サイトからの命令は一切受け付けなくなります。また、ダッシュボード画面の「情報更新待ちデバイス」の欄に表示されるようになります。 - T2チップ搭載のMacデバイスは、遠隔消去のご利用ができません。
遠隔消去キャンセル	遠隔消去をキャンセルしても、必ずしもキャンセルの実行結果が保証されるものではありません。対象デバイスが圏外にいたり、電源が入っていなかったりする場合は、キャンセルが実行されません。必ず「ログ検索」画面でキャンセルの実行結果を確認してください。
ネットワーク設定	ネットワーク設定が正しくされていない場合、遠隔消去が正しく動作せず、消去が実行されません。詳細はネットワーク要件をご参照ください。

基本サービス

[BizConPlace/BC Location]

専用アプリで利用者様とのコミュニケーションを促進

The screenshot shows the BizConPlace app interface. It includes a header with the date '2013年9月11日' and the title 'ビジネス・コンシェル'. Below the header, there are several sections: 'NAME' (listing users like 1210591, 小林 隆, コンシェル開発部, 第1課), 'ムービー' (video player), and 'お知らせ' (notice). The 'お知らせ' section contains icons for 'BCブラウザ', 'iPadGIVE', and 'OCR (練習)'. Red arrows point from callout boxes to specific features on the screen.

利用者情報

利用者情報の閲覧、編集が可能
(管理者が許可した場合のみ)

インフォメーション

管理者様よりメッセージ送信する
欄閲覧のみ可能

掲示板

掲示板を閲覧/記載内容について
利用者が、コメント返信可能

動画再生

動画をミニ画面、フル画面で再生
可能

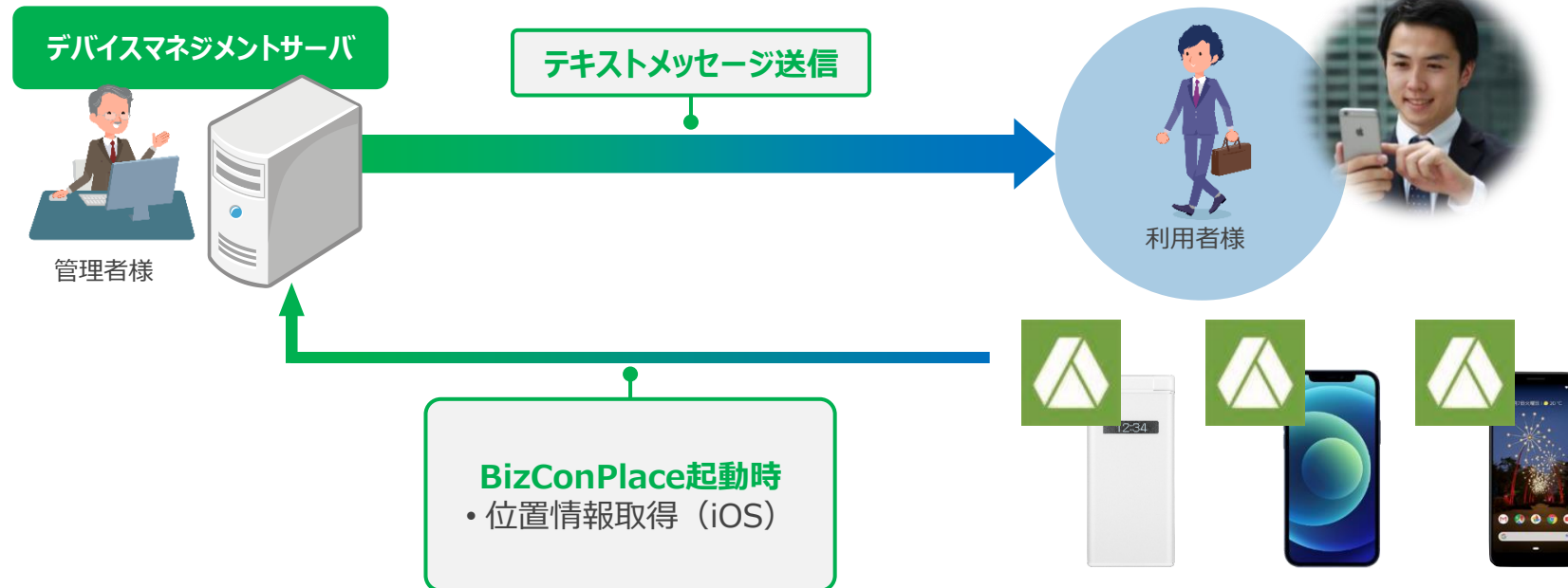
お知らせ

提供アプリケーションの起動アイ
コンが表示されます
(内容を変更することはできません)

※エンタープライズAppをご利用になる場合は、お客様とApple社との間でADEP (Apple Developer Enterprise Program) のご契約が必要になります。

メッセージPush送信、位置情報取得が可能

テキストメッセージをデバイスに送信することができます。
デバイス利用者がBizConPlace起動した際に位置情報（iOS）を取得し、管理サーバに送信します。



※エンタープライズAppをご利用になる場合は、お客様とApple社との間でADEP（Apple Developer Enterprise Program）のご契約が必要になります。

※Android 6以降の場合、メッセージPush送信機能はご利用できません。その他の注意事項は、以下サイトをご覧ください。

(<http://tm.softbank.jp/outsource/concierge/dm/device/>)

※Androidデバイスは、位置情報及びroot化検知はBizConPlaceではおこないません。

位置情報は管理ソフト（BCAgent）を利用し取得可能、root化検知は基本サービスのアンチウイルスソフトをインストールすることで検知することができます。

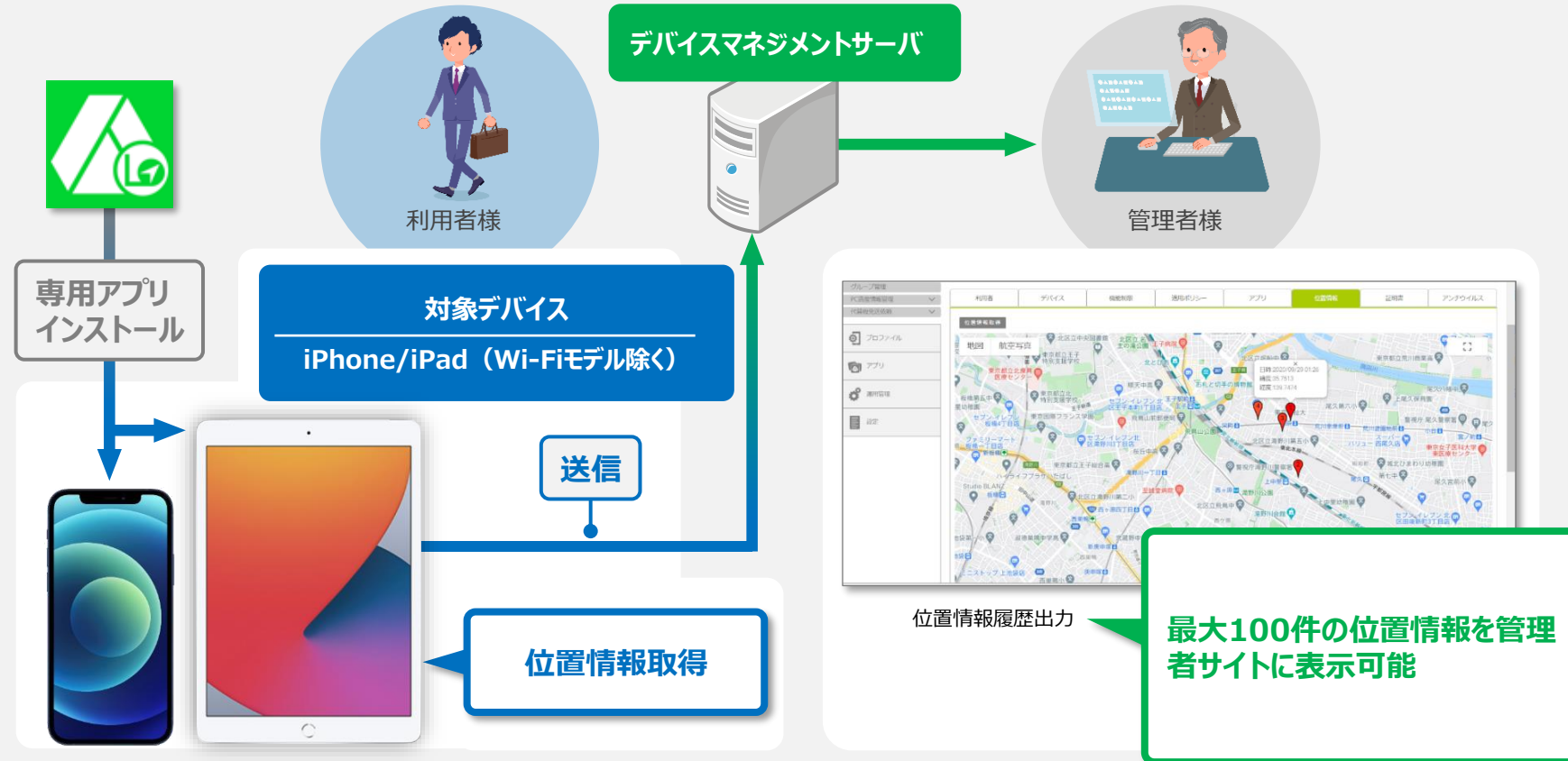
利用者様向け「安否確認」が可能

管理者様にて安否確認モードをONに設定すると、
利用者様がBizConPlaceアプリを起動時に安否確認が可能となります。
報告状況の確認は、CSVファイルにて行えます。



デバイスの位置情報取得が可能

基地局移動時※に位置情報を自動取得するため、1日の行動を時系列で確認できます。



※本機能を利用するにあたり、iOS : BC Locationが必要となります。

※本機能をご利用いただくには、申込が必要です。

※エンタープライズAppを提供するには、お客様とApple社との間で ADEP (Apple Developer Enterprise Program) (有料) が必要です。

内 容

iPhone/iPad向けのアプリです。Wi-Fiモデルは対象外です。
海外キャリア端末ご利用時、海外ローミングご利用時は、位置情報機能はサポート対象外となります。
(日本以外の国の地図は表示されません)

BC LocationのApp StoreアプリをManaged Appsで配布する場合は、BC Locationが取得した認証キーによる自動認証にて使用可能です。
App Storeから直接インストールした場合は、手動認証（初回）のためBizConID、パスワードが必要となります。

対象デバイスの設定で位置情報サービスが許可されている必要があります。また、アプリの「位置情報の利用を許可」設定で「Appの使用中は許可」が選択されている必要があります。

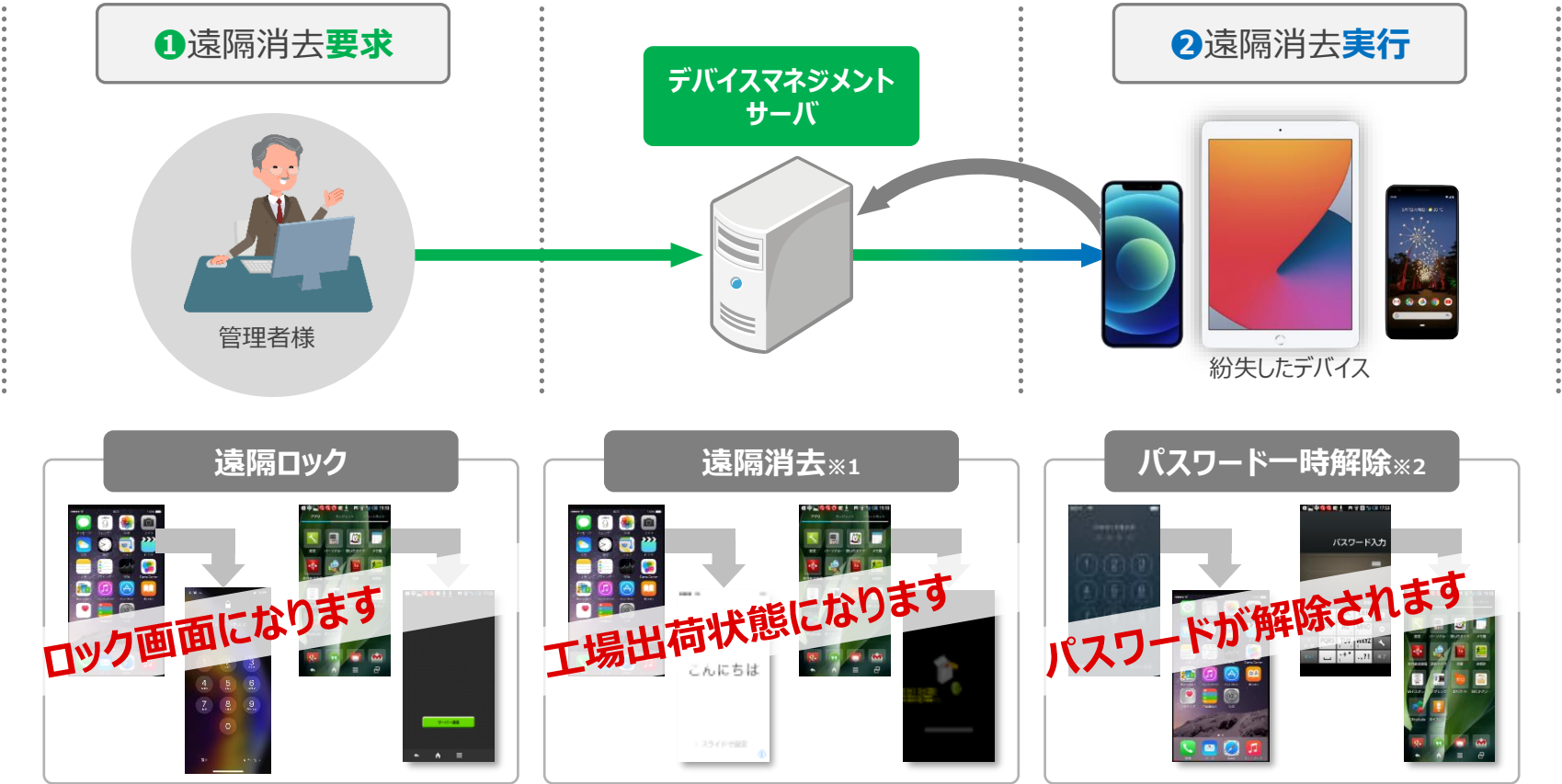
デバイスが電源オフや圏外などの間は動作しません。

バックグラウンドからBC Locationを削除すると、機能は停止します。ただしiOS 8以降は、基地局移動を検知すると位置情報の取得を再開します。

取得する位置情報の精度は、対象デバイスの位置情報の精度に依存します。
BC Locationの位置情報送信間隔、および管理サイトの位置情報取得日時は、対象デバイスの状況や通信環境によって、ずれが生じることがあります。また、本機能は、対象デバイスの位置情報の正確性を保証するものではありません。

紛失時リカバリーサービス

遠隔からのロック/消去、パスワード一時解除が可能



※1 回線停止後にデバイスに遠隔消去を行っても実行されません。また、回線を復旧させた後に遠隔消去を行っても、実行されるのはデバイスを再起動させた後となりますのでご注意ください。

※2 Androidは機能制御ポリシー（パスコード系の制御）が適用されている場合のみ有効となります。iOSの場合は、“パスワード”は“パスコード”と読み替えます。

紛失したデバイスにメッセージ・折り返し連絡先を表示して
操作ロックをかけ、位置情報の取得が可能



※本機能は、監理モードのデバイスのみ利用可能です。
※サウンド再生はiOS10.3以降のみ利用可能です。
※iPadは折り返し電話が出来ません。

管理者/利用者向けヘルプデスクをご提供、英/中対応可

管理者様向け電話サポートを行います。

遠隔ロック、遠隔消去、パスワード一時解除の操作代行を行います。

デバイスに関する一般的な問合せの対応も行います（日本利用のみ）。



OS	モデル	購入方法	ワイプ/ロック パスコード一時解除パス ワードリセット 操作代行	回線停止 代行※1	一般 問合せ ※2	月次 レポート	フリー コール ※3
iOS	Wi-Fi + Cellular	レンタル	○	○	○	○	○
		レンタル以外	○	○	○	○	○
		他キャリア（国内）	○	—	—	○	○
		海外キャリア	○	—	—	—	○
	Wi-Fi※4		○	—	○	○	○
Android/ 4Gケータイ	4G	レンタル	○	○	○	○	○
		レンタル以外	○	○	○	○	○
		他キャリア（国内）	○	—	—	○	○
		海外キャリア	○	—	—	—	○

※1：交換機暗証番号4桁をご提示いただきます。

※2：ソフトバンク製端末に限ります。

※3：海外からヘルプデスクにおかけの場合、無料通話可能な国、キャリアは限られます。

※4：デバイスの特定に際して「シリアル番号」を使用します。利用者情報登録で使用するCSVファイルや構成プロファイル配布時のCSVファイル（デバイス毎の情報を指定する際）には、「シリアル番号」を記述してください。
また、サービスデスクで操作代行するにあたり、「シリアル番号」でのご申告が必要になります。

オプション

[シングルサインオン機能]

連携可能SaaS数の多さが強み！数が増えても安心

SSO無制限

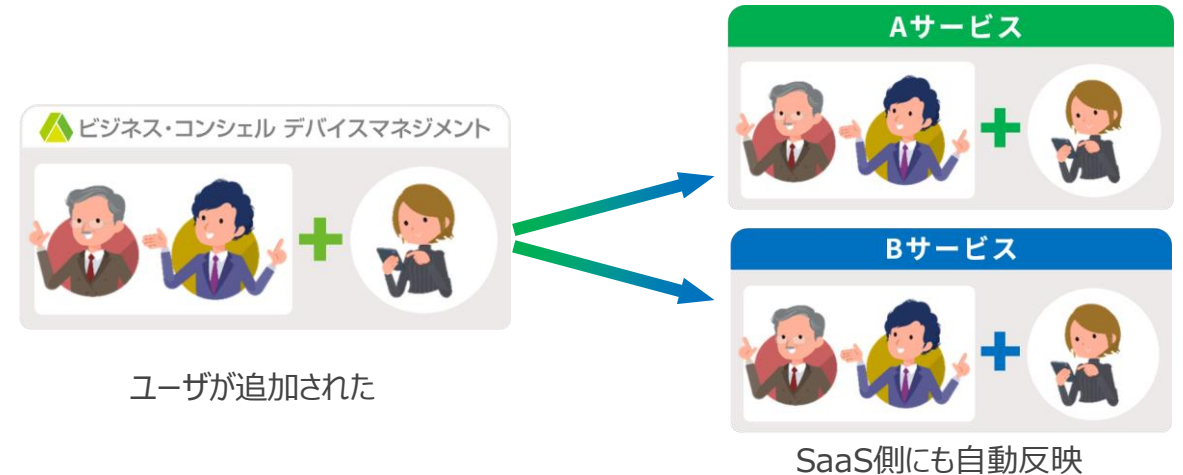
5つのSaaS以外でご利用いただきたい方向け
7,000以上のSaaSを数量無制限で連携いただくことができます。



- ✓ 利用したいSaaSが増えても安心
- ✓ SaaSごとに利用していた認証ツールを一つに統一できる

ライフサイクル管理

BCDMのユーザ情報と連携し、従業員の入退社などによる
SaaSのアカウント作成、変更、削除（プロビジョニング）を
自動化することができます



- ✓ アカウント管理の運用工数削減
- ✓ 不要なアカウント払い出しがなくなりコスト削減
- ✓ 権限の付与間違い、削除漏れがなくなり安全

※5つのSaaSはGoogleWorkspace、Zoom、LINE WORKS、PrimeDrive、BCDM、を指します。
※SSO無制限、ライフサイクル管理の対応アプリはOkta社のOINカタログよりご確認ください。
Okta Integration Network (OIN) <https://www.okta.com/integrations/>

オプション加入で多要素認証がさらに便利に

多要素認証

生体認証、プッシュ認証でさらに認証を簡単、強化したい方へ

■ プッシュ認証

本人以外が不正にログイン

利用者本人に確認

ログイン失敗



- ✓ 顔認証でスマホでも簡単ログイン
- ✓ プッシュ認証でフィッシング耐性が強化できる

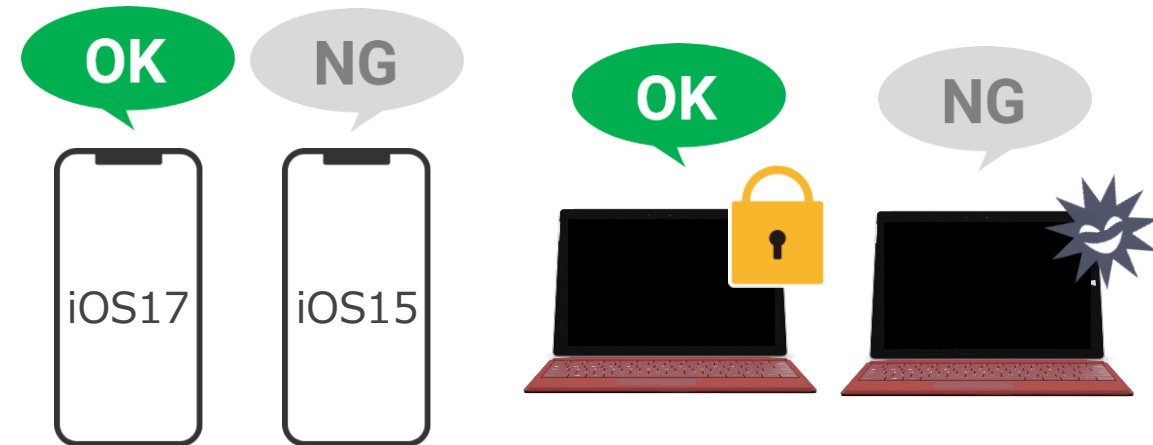


多要素認証Pro

デバイス情報を用いたアクセス制御

BYODや社外の人などBCDM登録外デバイスを利用したい方へ

- デバイス認証（OSバージョンによる認証）
- Microsoft Windows Security Center連携
- iOS16以上は認証許可とする
- エンドポイントの基準を満たしたデバイスは認証許可



- ✓ 外部社員のSaaS利用も許可したい
- ✓ 問題のあるデバイスは許可しないことでセキュリティ強化

オプション

[Webフィルタリングサービス]

専用ブラウザ「BCブラウザ」でURLフィルタリングを実現



- 専用アプリ「BCブラウザ」と連携して利用者様のアクセスログ検索/出力
- 業務上不適切なWebページには規制画面表示

※URLフィルタリングはネットスター株式会社様より技術提供を受けています。

※BCブラウザを用いたブラウジングでは、アクセスするサイトによってはsafariと同様のアクセス結果を得ることができない場合があります。

※本サービスのご導入においては、トライアルにて事前に動作検証の実施を推奨します。

※App Store版とエンタープライズApp版がありますが、

エンタープライズAppをご利用になる場合は、お客様とApple社との間でADEP（Apple Developer Enterprise Program）のご契約が必要になります。

提供機能	内 容	iOS	Android
Webアクセスのサマリログレポート	前日分までのアクセスログを集計し、サマリレポートとして画面表示します。	○	○
端末ごとのアクセスログ検索	端末ごとにアクセスした履歴を画面に表示します。	○	○
フィルタリングルールの設定	規定のポリシー（6パターン）に合わせてフィルタリングルールを1つ選択できます。	○	○
除外、規制URLの設定	見たいサイト、見せたくないサイトを管理者様がカスタマイズすることが出来ます。（300件まで）	○	○
ブックマーク配信	管理者様が設定したブックマークを利用者様の端末で共有することが可能です。（50件まで）	○	○
コンテンツ内の文字から検索	どのようなキーワードを入力してWebページを閲覧しているのかランキング表示します。	○	○
履歴保存/初期化設定の強制化	履歴の保存/初期化の設定を管理者様側で強制することができます。	○	○
フォームデータの保存（※1）	過去に入力したフォームデータの保存するか設定することができます。	○	—
プリンタの利用（※1）	BCブラウザからプリンターを使用させるか設定することができます。	○	—
長押しメニュー利用制限（※1）	BCブラウザ上でテキストや画像のコピーを制限することができます。	○	—
書き込み規制（※1）	掲示板等への書き込みを制限することができます。	○	—
セーフサーチ機能（※1）	セーフサーチ機能の有効/無効を設定することができます。	○	—
アクセスログダウンロード	管理画面に表示されるアクセス先のログのCSV出力が可能です。アクセスログは過去1年分の履歴が保管されますが、一度にCSV出力できる件数には制限があります。	○	○

※1 BCブラウザver3.0以降（iOS）のアプリに設定が反映されます。

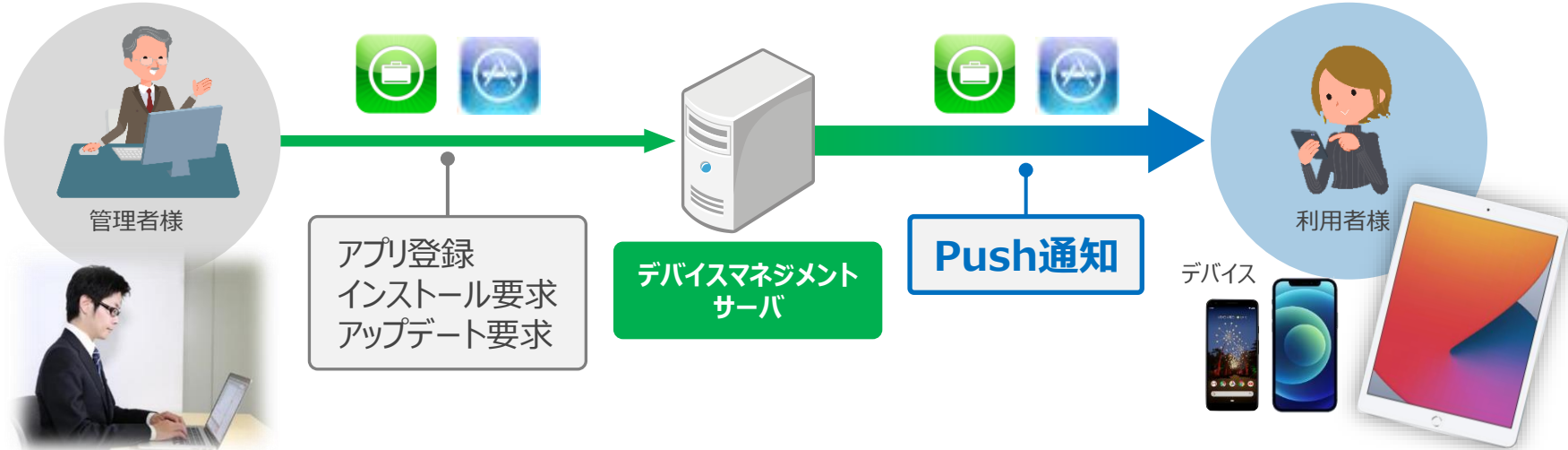
提供機能	内 容	iOS	Android
アプリケーション区分	App Store版、インハウス版をご提供します。 ※ Apple社では、「インハウスアプリ」の正式名称は「エンタープライズApp」となります。	○	—
履歴、Cookieの自動削除	履歴とCookieの削除タイミングを指定することができます。 不特定多数で使う共有端末で情報が残ることを防止します。	○	○
キャッシュ	設定したタイミングにおいて、設定内容を自動初期化すること可能です。	○	○
Basic認証 Digest認証	Basic認証/Digest認証に対応できます。	○ App Store版は Ver2.0.以降	○
規制画面での カテゴリ表示	規制画面が表示された場合に、どのカテゴリに該当したのかを表示します。	○	○
サイト内検索	サイト内検索が可能です。(iOS版のみ)	○	—
URLスキーム	スキーマ部分に「bcdmweb」または「bcdmwebs」と記載すれば、他のアプリのURLリンクから、直接BCブラウザが起動します。	○ App Store版は Ver2.2.以降	—
クライアント証明書登録	BCブラウザアプリからクライアント証明書の登録が可能です。	○ Ver3.0以降	—

事 項	詳 細
JavaScript	JavaScriptのwindow.open()及びwindow.opener()には対応しておりません。
IPv6	IPv6形式のURLには対応しておりません。
SplitView	iPadのSplitView機能には対応しておりません。
Web認証が必要なWi-fiサービス	Web認証が必要なWi-fiサービスを利用する場合は以下の注意事項があります。 • Wi-fiサービスのログイン画面のアクセスはHTTPの通信で行なってください。 • Wi-fiサービスのログイン画面へアクセスした際に証明書のセキュリティ警告が表示されることがあります。 • Wi-fiサービスのログイン画面の表示に数十秒時間を要する場合があります。
Ajaxを使用したPOST通信	Ajaxを使用したPOST通信のサイトでは、書き込み規制機能による制御ができません。
フォームデータの保存機能	一部サイトではフォームデータの保存機能が使えない場合があります。
事前検証のお願い	サイトによっては、表示や動作が異なることがあります。また、正常に動作しない場合もあります。社内・業務サイトをご利用の場合は事前の検証をお願い致します。

オプション

[Managed Apps容量拡張]

Managed Appsで配信できるインハウスアプリ※容量を有償で拡張



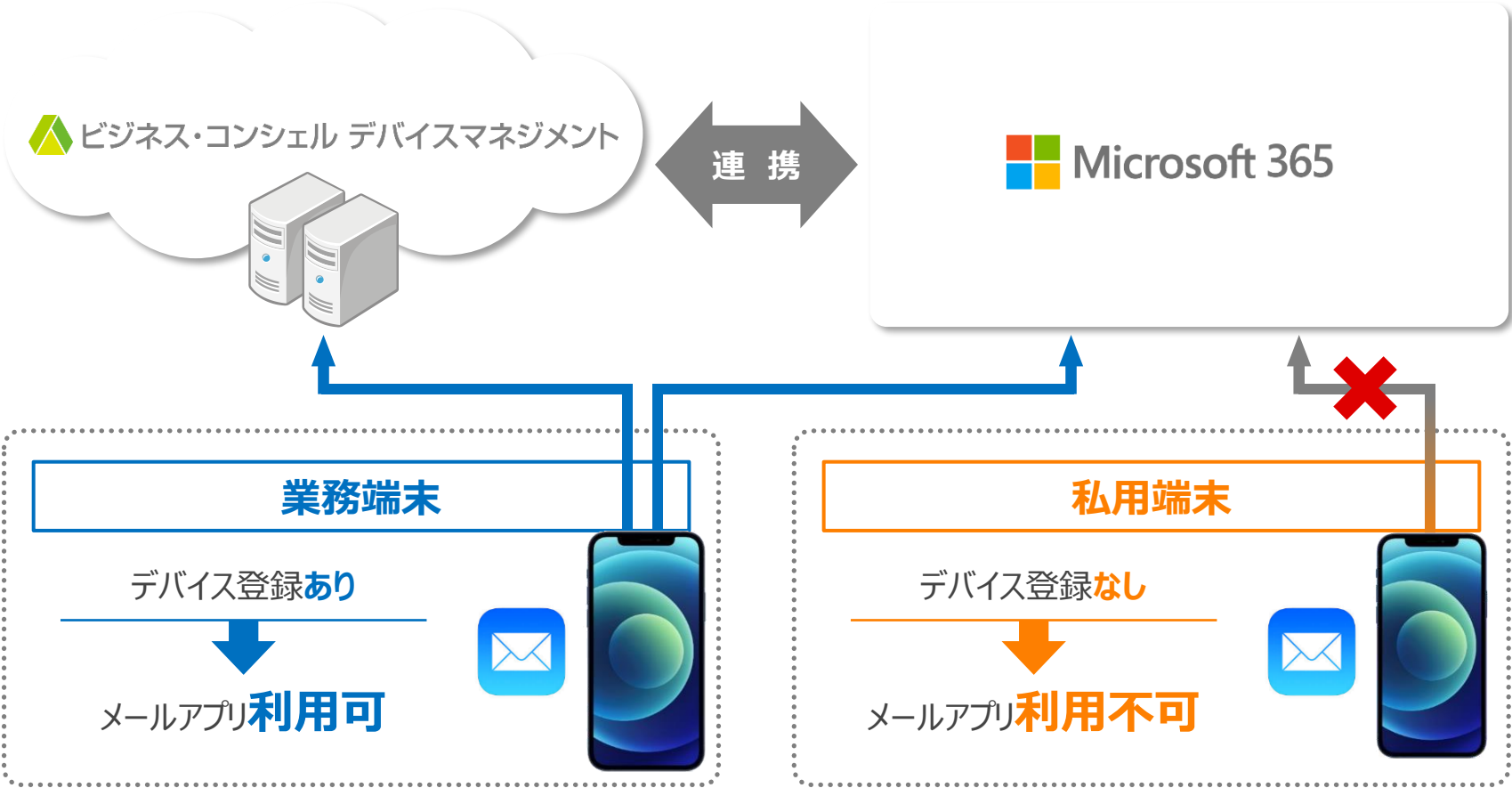
	Managed Apps 容量拡張	Managed Apps
インハウスアプリ登録上限容量	600MBまで : 100円/ID	40MBまで : 無償
インハウスアプリ登録上限数	iOS : 50個 Android : 30個	iOS : 50個 Android : 30個

※ Apple社では、「インハウスアプリ」の正式名称は「エンタープライズApp」となります。

オプション

[デバイスコントロール for Microsoft 365]

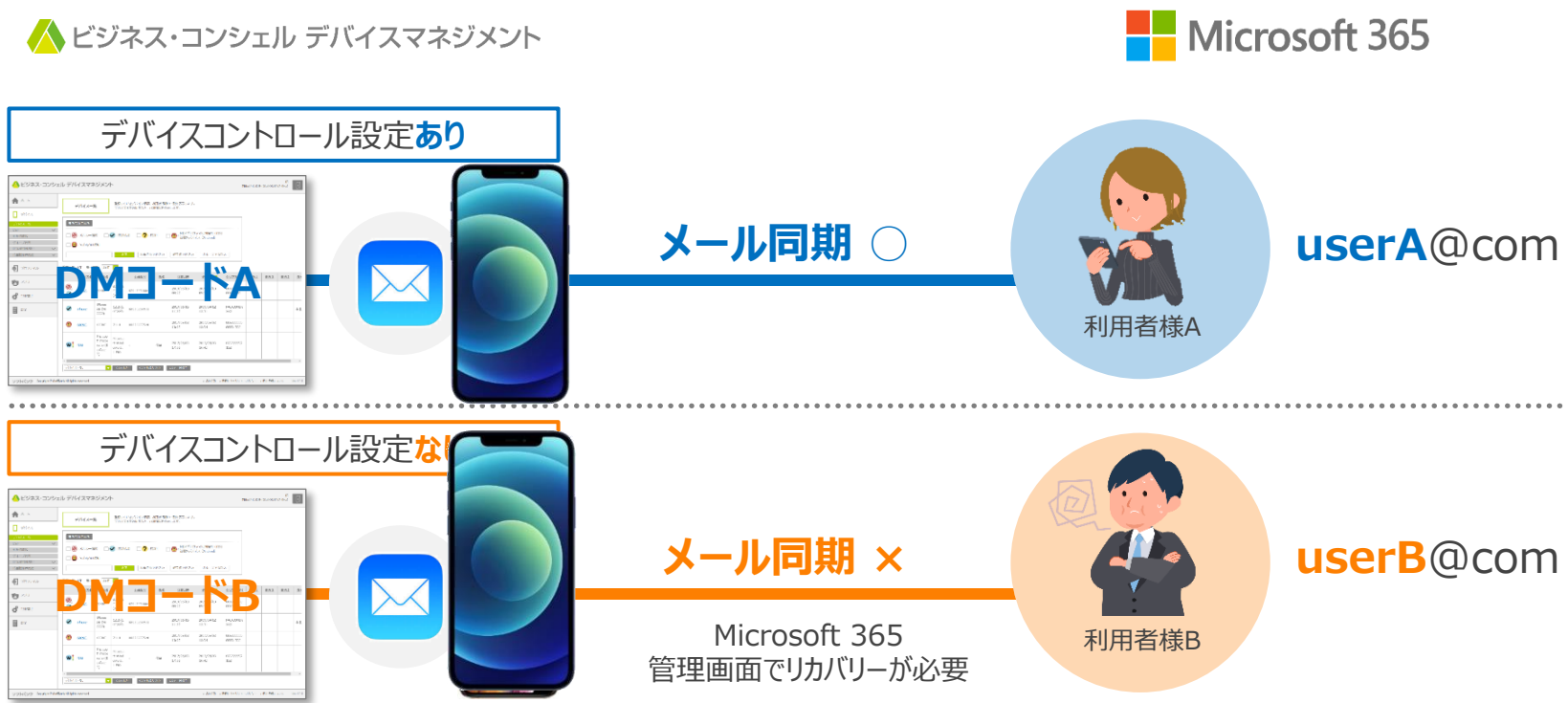
メールアプリの同期を業務端末だけに制限



※ご利用時には別途Microsoft 365のご契約が必要です。
※iOS動作確認バージョンについてはAppendixをご覧ください。

複数DMコードご契約の場合、他DMコードの端末に影響あり

同ドメインを利用するデバイスを複数のDMコードに登録している場合、
デバイスコントロール未設定のDMコードに登録されているデバイスはメール同期不可となり、
Microsoft 365管理画面でリカバリーが必要となります。



オプション

[PC操作ログサービス]

PCの操作ログを取得しダッシュボードで確認可能



各種ログ取得に対し
禁止操作として
管理者に通知可能



操作ログ検索

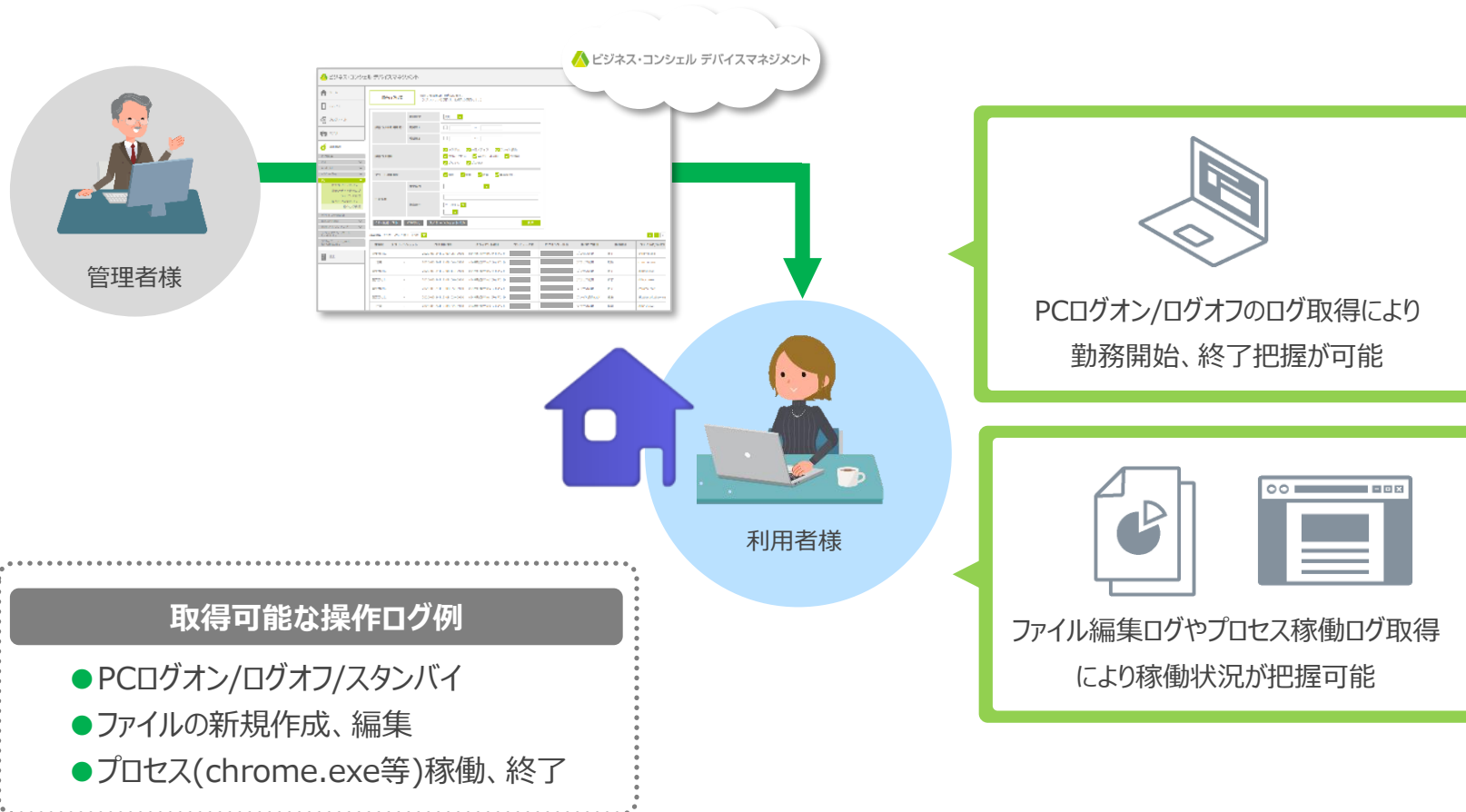
取得した操作ログを検索します。
(*がついている項目は、必須入力項目です。)

操作ログの取得期間*	期間指定	今日 ▼
	時間帯1	~
	時間帯2	~
	操作ログ種別	☒ システム ☒ 外部メディア ☒ ファイル操作 ☒ Webアクセス ☒ Webメール送信 ☒ PC稼働 ☒ プリンタ ☒ プロセス ☒ アクティブウィンドウ
アラートの重要度		☒ 緊急 ☒ 警告 ☒ 注意 ☒ 重要度なし
任意条件	検索項目	▼
	検索条件	と一致する ▼ ▼

取得可能なログ

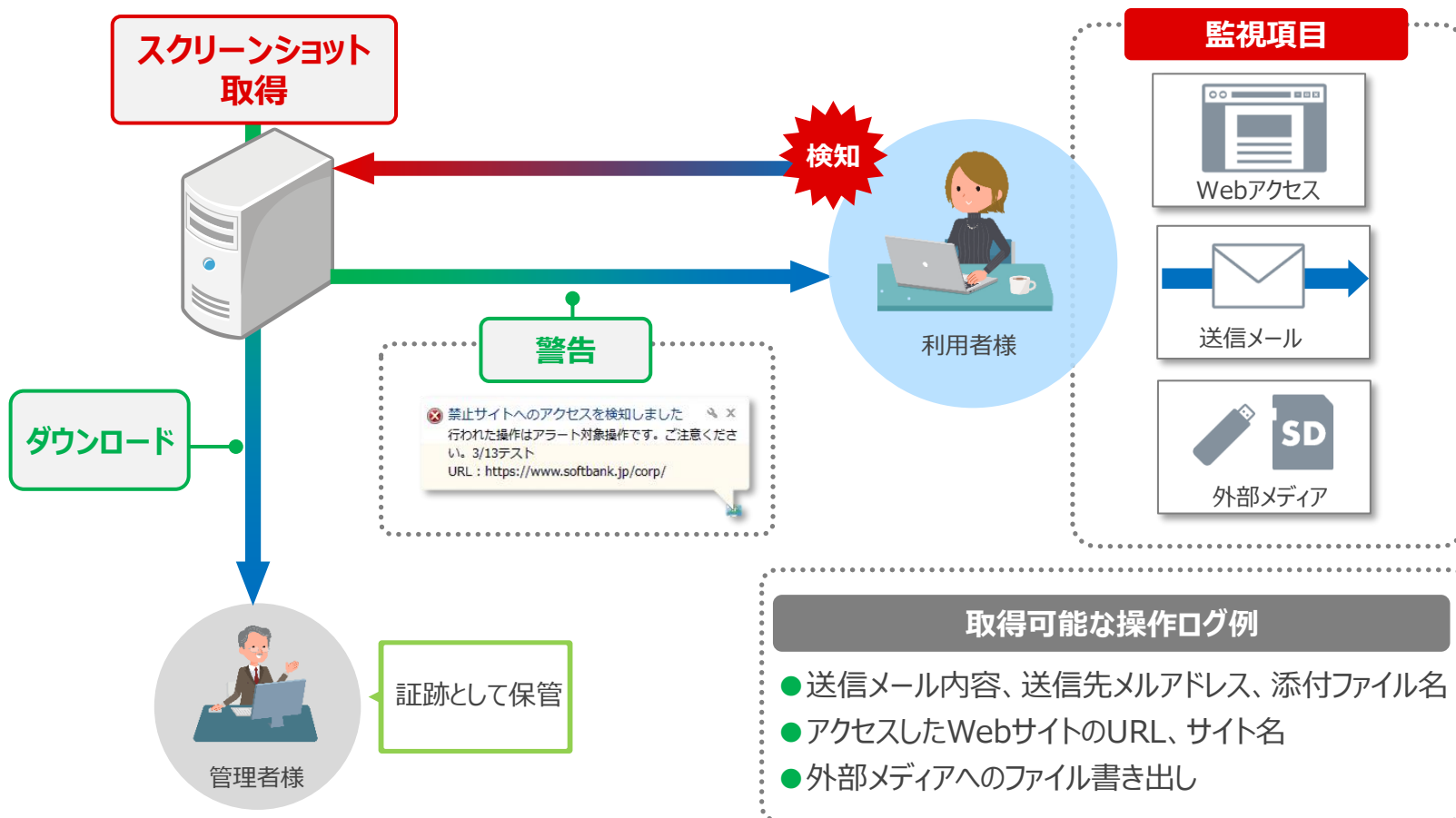
- システムログ
- 外部メディアの挿入
- ファイル操作ログ
- Webアクセスログ
- Webメール送信ログ
- PC稼働ログ
- プリンタ履歴ログ
- プロセスログ
- アクティブウィンドウログ

テレワーク時に従業員の勤務実態を確認可能



不正操作の抑制・監視に利用可能

ポリシー違反の場合は利用者への警告表示や違反画面のスクリーンショットを取得することができます。



ログ種別	機能	内容
システム	取得ログ	操作ログに関するシステムアラート情報を取得できます。 ・操作種別：空き容量低下（*1） / ログ未収集判定/Web プラグイン不正停止/ システム日時変更 ・システムログ情報
	アラート機能	・Windows クライアントのインストールドライブの残容量が設定以下になった場合 ・指定した日数以上、ログが取得されなかった場合 ・Windows クライアントのシステム時刻が不正な時刻に変更された場合 ・Web プラグインが不正に停止された場合
外部メディア	取得ログ	外部メディアの挿入/ 取り出し、ファイル書き出し操作ログを取得できます。 ・操作種別：外部メディア挿入/ 外部メディア取り出し/ 書き出し（*2） ・ファイル名 ・ファイルパス ・ファイルサイズ ・登録済メディアかどうか ・ベンダ名 ・製品名 ・シリアル番号 ・ベンダID ・製品ID
	アラート機能	・未登録外部メディアを挿入した場合 ・未登録外部メディアへの書き出し操作を行った場合

*1 インストールドライブの空き容量低下です。

*2 外部メディア上のファイルを削除した場合は、外部メディアログの書き出しログとして取得されません。

ログ種別	機能	内容
ファイル操作	取得ログ	取得対象ファイルの新規作成、操作内容、外部メディアへの書き出しなどのファイル操作ログを取得できます。 ・操作種別：新規作成/ 削除/ 編集/ 上書き保存/ ファイル名変更/ 移動/ コピー ・ファイル名 ・ファイルパス ・ファイルサイズ ・ブラウザ名/ プロセス名 ・変更前ファイル名 ・コピー、移動元ファイルパス ・ドライブ情報
	アラート機能	・ファイル名に特定のキーワードが含まれるファイルへの操作を行った場合
Webアクセス	取得ログ	アクセスしたWebサイトのURL、サイト名や、SNSサイト（Ameba / Facebook / Google+ / mixi / Twitter）への書き込み情報を取得できます。 ・操作種別：Web アクセス/SNS 書き込み ・ブラウザ名 ・サイト名 ・URL ・ドメイン ・SNS サイト名 ・SNS 書き込み内容
	アラート機能	・SNS サイト（Ameba / Facebook / Google+ / mixi / Twitter）への書き込みを行った場合 ・指定時間外にWeb サイトへのアクセスを行った場合 ・特定のキーワード（URL、ドメイン名、サイト名）が含まれたWeb サイトへのアクセスを行った場合

ログ種別	機能	内容
Webメール送信	取得ログ	Web メール（Gmail / Outlook.com / Yahoo! メール）を送信した際の送信先のメールアドレス、メール内容、添付ファイル名を取得できます。 ・操作種別：送信 ・添付ファイル名 ・ブラウザ名 ・メールサービス ・件名 ・本文 ・送信先メールアドレス（TO） ・送信先メールアドレス（CC） ・送信先メールアドレス（BCC）
	アラート機能	・Web メール（Gmail / Outlook.com / Yahoo! メール）を送信した場合
PC稼動	取得ログ	PC 稼働状況を取得できます。 ・操作種別：電源ON/ 電源OFF/ ログオン/ ログオフ/ スタンバイ（*1） / 復帰/ 稼働中（*2） / スタンバイ中（*2） / 時間外利用 ・前回利用開始日時 ・PC 利用時間
	アラート機能	・業務時間外にPC を利用した場合

*1 スタンバイには、スリープと休止が含まれます。

*2 1日中ずっと稼働している場合やスタンバイの場合、1 日 1 回、〔稼働中〕、または〔スタンバイ中〕のログが取得されます。

ログ種別	機能	内容
プロセス	取得ログ	プロセス起動・終了のログを取得できます。 ・操作種別（起動、終了）、プロセス名、対象のプロセスの実行ファイルのファイルパス、対象プロセスの説明
	アラート機能	・特定のキーワードが含まれたプロセスの起動に対するアラート通知 ・指定時間外のプロセス起動
プリンターログ	取得ログ	プリンター操作ログを取得できます。 ・プリンター操作種別、印刷したドキュメント名、一度の印刷で出力した枚数、プリンター名、IPアドレス
	アラート機能	・ドキュメント名に特定のキーワードが含まれるプリンター操作に対するアラート通知 ・指定枚数以上の印刷

ログ種別	機能	内容
アクティブ ウィンドウ	取得ログ	クライアントPCで現在アクティブ表示のウィンドウの情報を取得できます。 ・ウィンドウタイトル、ウィンドウプロセス名
	アラート機能	・特定のキーワードが含まれたアクティブウィンドウログ取得に対するアラート通知 ・アクティブウィンドウログ取得時のアラート通知

項目	内容
ログ取得サービス利用について	・本サービスはパブリッククラウドサービスを利用しています。 ・本サービスを利用するには、管理対象のPCがインターネットに接続されている必要があります。 ※インターネットに接続されていない状態で取得したログは、管理対象のPCに保存されます。 ※管理対象PC側に蓄積されたログが設定された容量を超えた場合、古いものから削除、またはログ取得が停止します。（管理画面にて設定可能） ・通信ポート「443/TCP」を許可する必要があります。
ログの反映について	・操作ログは以下のタイミングで管理画面サーバへ送信されます。 -管理対象PC起動時に未送信ログがあれば送信されます。以降は30分間隔で送信されます。 -管理対象PC側に蓄積されたログが100KBを超える場合は超えた時点で送信が行われます。 ※管理対象PCシャットダウンおよびスリープ状態ではログの送信は行われません。 - 未送信状態のログがある場合、次回起動時に送信されます。 ※パブリッククラウドサービスを利用しているため、状況によってはログの反映が遅延する場合がございます。
ログの監視の定義とロジックについて	・本サービスは管理対象端末にインストールされたエージェントソフトに対しポリシーを適用し、設定されたポリシー内容に応じて管理対象PCの監視、および必要に応じてアラートを表示します。
アラート発生時のログについて	・アラート発生時に取得したログについては即時反映し、以降は30分間隔で蓄積されたログが送信され管理画面に反映されます。

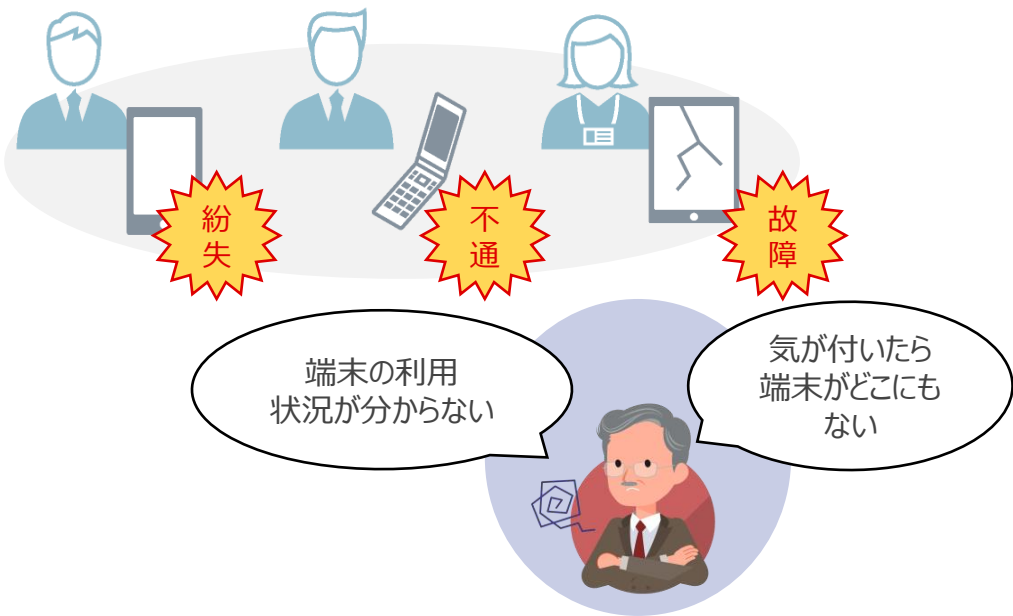
項目	内容
ログのイベント時刻について	・ログのイベント時刻は、一部を除いて管理対象PC側で操作を行った時刻で記録されます。 ※「ログ未収集アラート」については、管理対象PC側ではなく、ログの収集が行われていないことをサーバ側で検知するため、サーバ側の時間を検知時間としています。
サービスの仕様変更に伴うログの取得について	・Webメール送信などに関する取得ログについて、クライアント側の仕様変更やブラウザ仕様変更により正常に取得できなくなる場合があります。 ・Windows OS のバージョンアップ等の仕様変更によりログの取得が正常に機能しなくなる場合があります。
ログのバックアップについて	・ログデータのバックアップはサービスに含まれておりません。 - 必要に応じてお客様にてCSVファイルを書き出した後に別途保存していただく必要があります。
ログの保存期間について	・操作ログの保持期間は365日となります。

導入事例

導入事例：端末の利用状況確認

業種/契約ID 介護・福祉 / 1,600ID

導入前 個別管理



背景・課題 端末は個別で管理をまかせていたので、気が付いたら端末を紛失していたということがあった。

機能 デバイス一覧・デバイス情報更新

導入後 BCDMによる管理集約



効果 BCDMで端末を管理することにより、端末の利用頻度が見える化し、利用されていない端末について管理者側から確認ができるようになり、端末の所在や利用有無を管理できるようになった。

導入事例：パスコード設定・リモートワイプによる情報漏洩対策

業種/契約ID

食品製造業 / 60ID

導入前

情報漏洩リスクあり



社用端末紛失

悪意ある第三者

端末を紛失してしまった…

管理者様

情報漏洩を防ぐ方法がない…
何か対策を考えなければいけない…

端末を紛失してしまった場合、情報漏洩を防ぐ手立てがなく、
情報漏洩のリスクがあった

機能

デフォルトPF・リモートワイプ

導入後

情報漏洩防止に成功

6桁以上のパスコード設定済みの端末

悪意ある第三者

パスコードがかかっていてロック解除ができない！

端末紛失発覚

管理画面からリモートワイプを実施

端末を初期化して情報漏洩を防げた！

効果

端末を紛失してしまっても、事前にデフォルトPFにて全端末に6桁以上のパスコードを設定していた為、情報漏洩リスクの軽減につながった。さらに、遠隔から端末を初期化することで、確実に情報漏洩を防ぐことができた。

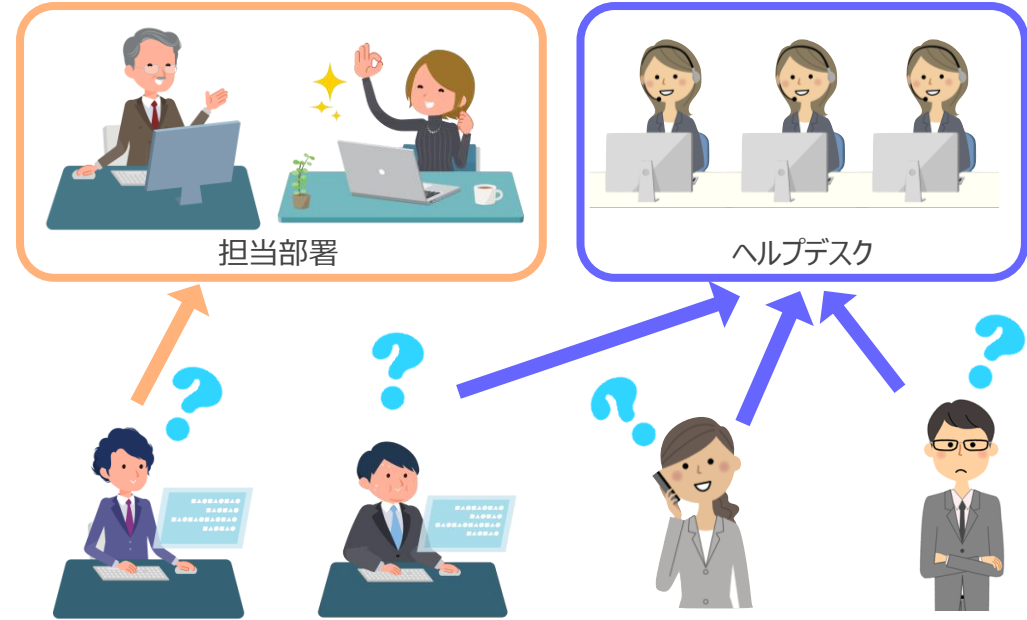
導入事例：ヘルプデスク対応による工数削減

業種/契約ID 製造業 / 80ID

機能 24時間365日ヘルプデスク

導入前 社内問合せが担当部署に集中

導入後 ヘルプデスクへ問合せ集約し、工数削減



背景・課題 社用携帯やPCに関する問合せ窓口は全て社内の担当部署となっており、日々問合せが多く工数がかかっていた

効果 社用携帯に関する事は社員から直接ソフトバンクヘルプデスクへ問合せするようにしたことで、担当部署の工数が削減され、その他業務への集中時間を捻出できるようになった

導入事例：ADE（旧DEP）によるキッティングの効率化

業種/契約ID ITソリューション / 520ID

導入前 iOS端末に1台1台インストール作業



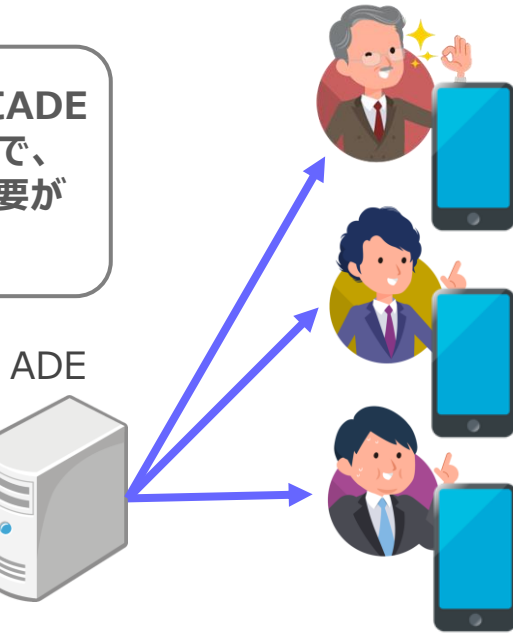
デバイス登録を行ってから
利用者に渡したいけど
1台1台作業を行うから
時間と手間がかかって大変...

背景・課題 デバイス登録を行う際、1台1台手動で行う必要があるため工数がかかり、利用者がすぐにBCDMに登録済みの端末を利用することができない。

機能 Automated Device Enrollment (旧DEP)

導入後 事前準備のみですぐに利用可能

端末のシリアル番号を事前にADE
として一括で登録しておくことで、
1台1台デバイス登録する必要が
なくなり、作業効率UP！



効果 Appleの提供しているADEの機能を利用することでアクティベーション時に自動でデバイス登録されるため工数削減につながり、ユーザが端末をすぐに利用できる。

導入事例：PC操作ログの活用

業種/契約ID ITサービス / 300ID

導入前 セキュリティ外部監査に苦慮

監査項目が何百項目もあり点検が大変…

項目毎に何をどう対策したら良いかわからない…

従業員の端末の操作ログの提示も必要です！



管理者様



セキュリティ監査法人

背景・課題

セキュリティ外部監査を実施するのが初めてで、項目数の多さもありましたが、各監査項目に対して、具体的にどう対応を行えば良いのか等点検に非常に苦労した。

機能 基本機能・PC操作ログ

導入後 セキュリティ外部監査対応を無事完了

BCDM導入済みだったから対策済みと報告できた！追加対策もBCDMで簡単に設定できた！

セキュリティ対策万全です！



管理者様

操作ログデータ提出



セキュリティ監査法人

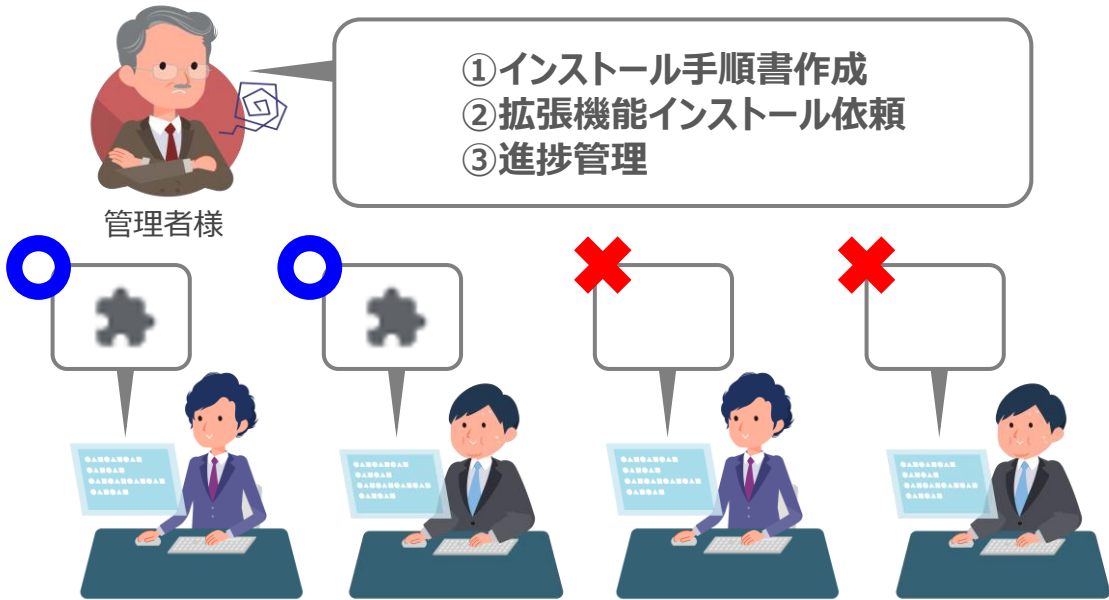
効果

BCDMを導入済みだったため対策済みと報告できたものや、追加対策が必要であってもBCDMの設定で簡単に対応できたものがあつた。業務端末のログ取得を要求する項目へも対応ができた。

導入事例：Chromeポリシー設定（拡張機能自動インストール）

業種/契約ID ITサービス / 300ID

導入前 PC所有者1人1人に対応



背景・課題 セキュリティ外部監査実施時に、セキュリティ対策として推奨されたChrome拡張機能をインストールするにあたり、PC所有者1人1人に対応を依頼・完了したか管理する必要があった。

機能 Chromeポリシー設定（拡張機能自動インストール）

導入後 リモートで拡張機能を一括インストール



効果 BCDMから一括で拡張機能インストール指示を出すことで、漏れなく全ての端末に拡張機能がインストールされ、セキュリティがより強固になった。

Appendix

デバイスマネジメントでは、以下の通信ポートを使用します。モバイルゲートウェイ・Wi-Fi・VPNなどの閉域サービス、プロキシ、i-FILTER・ZScaler等によるクラウドプロキシ等を使用している場合は、ネットワーク管理者の方にご相談の上、お客様のネットワーク機器側にて開放または除外設定が必要となります。

また、ご利用にあたってのネットワーク要件は、お客様の環境ごとに異なりますので、設定が必要な際は当社までお問い合わせください。

事 項		BCDM側	Apple / Google側 (プロキシ不可)	その他
B C D M ネ ッ ト ワ ー ク 要 件	iOS / macOS	- tcp/80, 443 - tcp/8080 (Webフィルタリングオプション) ※収容しているサーバ・ご契約オプションにより変わりますので、詳細は当社までお問合せください。	- tcp/80, 443, 5223 - tcp/udp 123 ※Apple社により予告なく変更の可能性があります。 ※通信要件の詳細につきましては当社までお問い合わせください。	- インターネット接続が必須です。 - 外部DNS参照が必須です。 - Zscaler等のクラウドプロキシ もしくは宅内設置のプロキシ経由では、 プロキシ除外(バイパス)が必要です。 なお、BCDM側は、プロキシ利用可能ですが、 SSLインターセプトするプロキシ (Zscaler等)はサポート外となりますので、 除外指定してください。
	Android / 4Gケータイ	- tcp/80, 443 - tcp/8080 (Webフィルタリングオプション) ※収容しているサーバ・ご契約オプションにより変わりますので、詳細は当社までお問合せください。	- tcp/443 - tcp/5228, 5229, 5230 - IPアドレスはGoogle社で非公開です。 ※Google社により予告なく変更の可能性があります。	【Android BCDM AntiVirus】 tcp/80, 443, 22 【Windows/macOS VBBSS】
	Windows	- tcp/80, 443 ※収容しているサーバ・ご契約オプションにより変わりますので、詳細は当社までお問合せください。	なし	- tcp/80, 443 (WAN側) tcp/21112, 61116 (LAN側) udp/61117, 61118, 61119 (LAN側) - 通信要件の詳細につきましては当社までお問い合わせください。

お問い合わせ に必要な情報

- DMコード (必須)
- ご契約オプション

ご契約オプションが不明であれば、当社で現在ご契約のオプションを調べ、その範囲でお答えします。
新たに下記のオプションを申し込まれた場合も、通信先が追加になりますので、お問い合わせください。

- 紛失時リカバリー
- Webフィルタリング
- Managed Apps容量拡張
- ほかのOSのID追加 (iOSデバイスのみの環境にAndroidデバイスを追加する等)

IPアドレス・FQDN・ポートは、DMコードやご利用オプションにより通信先が異なりますので、ここでは公開しておりません。
そのため、当社に通信要件詳細をお問い合わせいただき、お客様のネットワークご担当者様に機器側の設定を依頼してください。

複数DMコードをお持ちのお客様は、DMコードごとに当社にお問い合わせいただき、設定の流用はされないようお願いいたします。

通信要件に沿って機器側で設定しない場合、
デバイス登録ができない・デバイスの最新情報が取得できない・アプリが配れない・プロファイルが配れない・リモートワイプ指示ができないなど、
トラブルが発生する可能性があります。(一部のデバイスのみ該当し、全台では発生しない場合もあります。)

かんたん一括設定の項目一覧

一 般	・ プロファイル名称 ・ 組織名 ・ 説明 ・ デバイスでのプロファイル削除（認証時、許可しない） ・ プロファイルのスケジュール削除（しない、指定日、一定期間後）
パスコード	・ 起動時にパスコードを要求 ・ 簡単なパスコードの使用（許可、禁止） ・ パスコードに英数字を含める（必要、不要） ・ パスコードの最小桁数（1 ～ 16） ・ 英数字以外に使用できる文字の最小数（1 ～ 4） ・ パスコードの有効期限（1 ～ 730） ・ スリープまでの時間の範囲（1 ～ 5分、10分、15分） ・ この数までパスコード再利用禁止（1 ～ 50） ・ パスコードロックまでの時間の範囲（即時、1分、5分、15分、1時間、4時間） ・ 連続してパスコードを間違えるとデータを削除（2 ～ 10）
制 限	【機能】 ・ カメラの使用を許可 ・ Facetimeを許可（SV） ・ スクリーンショットと画面収録を許可 ・ AirPlay、"クラスルーム"による画面の閲覧、および画面共有の許可 ・ "クラスルーム"にプロンプトなしでのAirPlayと"画面を表示"の実行を許可（SV） ・ Airdropを許可（SV） ・ iMessageを許可（SV） ・ Apple Musicを許可（SV） ・ Radioを許可（SV） ・ デバイスのロック中でも音声ダイヤルを許可 ・ Siriを許可 ・ デバイスのロック中でもSiriを許可 ・ Siriの不適切な単語フィルタを有効にする（SV） ・ Siriにユーザ生成コンテンツを表示（SV） ・ Siriの検索候補を許可 ・ Apple Booksを許可（SV） ・ Appのインストールを許可（SV） ・ App StoreからのAppのインストールを許可（iOS9）（SV） ・ Appの自動ダウンロードを許可（iOS9）（SV） ・ Appの削除を許可（SV）

かんたん一括設定の項目一覧

制 限	- システムAppの削除を許可（SV） - App Clipを許可（SV） - App内課金を許可 - 購入時に常にiTunes Storeパスワードを要求 - iCloudバックアップを許可 - iCloud書類とデータを許可（SV） - iCloudキーチェーンを許可 - 管理対象AppがiCloudにデータを保存することを許可 - エンタープライズブックのバックアップを許可 - エンタープライズのメモとハイライトの同期を許可 - 共有アルバムを許可 - iCloud写真を許可 “マイフォストリーム”を許可(許可しないとデータ損失の可能性あり) - ローミング中の自動同期を許可 “ファイル”AppでUSBドライブへのアクセスを許可（SV） “ファイル”Appでネットワークドライブへのアクセスを許可（SV） - 強制的に暗号化バックアップ - Appからのトラッキング要求を禁止 “すべてのコンテンツと設定を消去”を許可（SV） - 信頼されていないTLS証明書の受け入れをユーザに許可 - 証明書信頼設定の自動アップデートを許可 - 構成プロファイルのインストールを許可（SV） - VPN構成の追加を許可（SV） - 日付と時刻を強制的に自動設定（SV） - Wi-Fiの電源を強制的にオン（SV）	- アカウント設定の変更を許可（SV） - Bluetooth設定の変更を許可（SV） - モバイルデータ通信App設定の変更を許可（SV） - モバイルデータ通信プラン設定の変更を許可（SV） - eSIM設定の変更を許可（SV） - デバイス名の変更を許可（iOS9）（SV） “友達を探す”設定の変更を許可（SV） - 通知設定の変更を許可（SV） - パスコードの変更を許可（iOS9）（SV） - Touch IDの指紋/Face IDの顔の変更を許可（SV） - スクリーンタイムを許可（SV） - 壁紙の変更を許可（SV） - インターネット共有設定の変更を許可（SV） “友達を探す”を許可（SV） “探す”の“デバイスを探す”を許可（SV） - デバイスのロック中もUSBアクセサリを許可（SV） - Configurator以外のホストとのペアリングを許可（SV） - 管理対象外出力先で管理対象ソースからの書類を許可 - 管理対象出力先で管理対象外ソースからの書類を許可 - AirDropを管理対象外の出力先とみなす（iOS9） - Handoffを許可 - Appleへの診断情報と使用状況データの送信を許可 - Touch ID/Face IDによるデバイスロック解除を許可 - パスワードの自動入力を許可（SV） - 自動入力の前にTouch ID/Face IDによる認証を要求（SV）
-----	---	---

かんたん一括設定の項目一覧

制 限	• Apple Watchの手首検出を強制 • Apple Watchとのペアリングを許可（SV） • 最初のAirPlayペアリングでパスコードを要求 • Wi-FiペイロードによってインストールされたWi-Fiネットワークのみに接続（SV） • 近くのデバイスの新規設定を許可（SV） • 近接通信に基づくパスワード共有要求を許可（SV） • パスワードの共有を許可（SV） • AirPrintを許可（SV） • iBeaconを使ったAirPrintプリンタの検出を許可（SV） • キーチェーンへのAirPrint資格情報の保存を許可（SV） • 証明書が信頼されていない出力先へのAirPrintを禁止（SV） • 予測表示キーボードを許可（SV） • キーボードショートカットを許可（SV） • なぞり入力キーボードを許可（SV） • 自動修正を許可（SV） • スペルチェックを許可（SV） • 定義を許可（SV） • 音声入力を許可（SV） • ロック画面でのWallet通知を許可 • ロック画面にコントロールセンターを表示 • ロック画面に通知センターを表示 • ロック画面に今日表示を表示 • ソフトウェア・アップデートの遅延〇日間（SV）	【アプリケーション】 • YouTubeの使用を許可（～iOS5） • iTunes Storeの使用を許可（SV） • Podcastの使用を許可（SV） • Game Centerの使用を許可（SV） • マルチプレイヤーゲームを許可（SV） • Game Centerの友達の追加を許可（SV） • Safariの使用を許可 • 自動入力を有効にする • 強制的に詐欺警告 • JavaScriptを有効にする • ポップアップを開かない • Cookieの受け入れ（しない、現在のWebサイトからのみ、常に） • Appの使用を制限 （すべてのAppを許可、以下のAppを禁止、以下のAppのみ許可） 【メディアコンテンツ】 • レーティングの地域（オーストラリア、カナダ、フランス、ドイツ、アイルランド、日本、ニュージーランド、イギリス、アメリカ） • 許可されるコンテンツレーティング 映画（映画を許可しない、G、PG12、R15+、R18+、すべての映画を許可）※ テレビ番組（テレビ番組を許可しない、0+、9+、12+、18+、すべてのテレビ番組を許可）※App（Appを許可しない、4+、9+、12+、17+、すべてのAppを許可） • 不適切なミュージック、Podcast、iTunes Uメディアの再生を許可(iOS13)（SV） • Apple Booksで不適切な性的描写のあるブックの閲覧を許可
-----	--	---

かんたん一括設定の項目一覧

Wi-Fi	- SSID - 非公開ネットワーク（有効、無効） - ワイヤレスネットワークへの自動接続（有効、無効） - キャプティブネットワーク検出(iOS10)（有効、無効） - 関連付けを回避するためのMACランダム化(有効、無効) - プロキシ設定（なし、手動、自動）	- セキュリティの種類 - なし - WEP - WPA/WPA2パーソナル - WPA2パーソナル（Apple TVを除くiOS8以降） - 任意（パーソナル）
VPN	- 接続名（デバイス上に表示） - 接続のタイプ - IPSec - L2TP - PPTP - Cisco AnyConnect - Cisco Legacy AnyConnect - Juniper SSL - Pulse Secure - F5 SSL - SonicWall Mobile Connect	- Aruba VIA - Check Point Mobile VPN - カスタムSSL - F5 Access - サーバのホスト名またはIPアドレス - ユーザアカウント(CSV) - Per-App VPN - ユーザ認証(パスワード、証明書、パスワード+証明書) - パスワード - プロキシ設定（なし、手動自動）
Webクリップ	- ラベル - URL - Webクリップの削除（許可、禁止）	- アイコン(59x60pixel) - アイコンの表示設定（視覚エフェクトあり、視覚エフェクトなし） - フルスクリーン（有効、無効）
証明書	- 証明書 - 証明書名（CSV）	パスワード（CSV）
Googleアカウント	- アカウントの説明（CSV） - アカウント名（CSV）	- メールアドレス（CSV） - 通信サービスルール（CSV）

かんたん一括設定の項目一覧

Exchange Active Sync	• アカウント名非公開ネットワーク（有効、無効） • Exchange ActiveSyncホスト • SSLを使用 • ユーザ（CSV） • メールアドレス（CSV） • 認証にOauthを使用 • パスワード（CSV） • 以前のパスワードを上書き • 過去のメールを同期（日数）（制限なし、1日、3日間、1週間、2週間、1カ月） • 認証資格情報名 • 認証資格情報（値なし）	• メッセージの移動を許可 • 最近使ったアドレスの同期を許可 • Mail Dropを許可 • “メール”でのみ使用 • S/MIME署名を有効にする • ユーザによるS/MIME署名の有効化/無効化を許可 • S/MIME暗号化をデフォルトで有効にする • ユーザによるS/MIME暗号化の有効化/無効化を許可 • メッセージごとの暗号化切り替えを有効にする • 有効なサービス（メール、連絡先、カレンダー、リマインダー、メモ） • アカウントの変更（メール、連絡先、カレンダー、リマインダー、メモ） • 通信サービスルール
メール	• アカウントの説明（CSV） • アカウントの種類（IMAP、POP） • パスの接頭辞 • ユーザ表示名（CSV） • メールアドレス（CSV） • ユーザがこのアカウントからメッセージを移動することを許可 • 最近使ったアドレスの同期を許可 • Mail Dropを許可 • “メール”でのみ使用 • S/MIME署名を有効にする • ユーザによるS/MIME署名の有効化/無効化を許可 • S/MIME暗号化をデフォルトで有効にする • ユーザによるS/MIME暗号化の有効化/無効化を許可 • メッセージごとの暗号化切り替えを有効にする	【受信メール】 • メールサーバとポート • ユーザ名(CSV) • 認証のタイプ（パスワード、MD5チャレンジ応答、NTLM、HTTP MD5ダイジェスト） • パスワード(CSV) • SSLを使用 【送信メール】 • メールサーバとポート • ユーザ名(CSV) • 認証のタイプ（パスワード、MD5チャレンジ応答、NTLM、HTTP MD5ダイジェスト） • パスワード(CSV) • 送信パスワードを受信パスワードと同じにする • SSLを使用

かんたん一括設定の項目一覧

グローバル HTTP プロキシ※	・ プロキシタイプ（手動、自動） ・ プロキシサーバとポート ・ ユーザ名	・ パスワード ・ キャプティブネットワークにアクセスするためのプロキシのバイパスを許可
DNS プロキシ	・ AppバンドルID ・ プロバイダバンドルID	・ プロバイダ構成
モバイル通信※	・ 構成するAPNのタイプ（デフォルトAPN、データAPN、デフォルトAPNとデータAPN） ・ デフォルトAPN名 ・ デフォルトAPNの認証タイプ（PAP、CHAP）	・ デフォルトAPNのユーザ名 ・ デフォルトAPNのパスワード ・ デフォルトAPN対応IPバージョン（-、IPv4、IPv6、IPv4とIPv6）

※ 誤った設定のプロファイルをデバイスに配布すると、デバイスが機能しなくなることがあります。ご注意ください。

デバイスに設定可能な項目一覧：Android

機能制御	パスコード	- パスコードの要求 - パスコードの有効期限 - パスコードの種類 - バックライト点灯時間 - ローカルワイプまでのパスコード入力失敗回数 - ローカルロックまでのパスコード入力失敗回数 - 外部メモリ消去までのパスコード入力失敗回数	
	デバイスの制御	- カメラ使用制御 - Wi-Fi使用制御 - Bluetooth使用制御	- 外部メモリ使用制御 - テザリング使用制御
	GPS設定	位置情報の取得制御	位置情報取得義務化の設定
	その他	ポーリング間隔時間の設定	

デバイスに設定可能な項目一覧：Android Enterprise

Fully managed device

制 御	パスコード	・ パスコード義務化・パスコードの有効期限 ・ パスコード設定有効期限 ・ パスコードの種類・バックライト点灯時間	・ パスコードの再入力時間間隔 ・ パスコードの再利用回数 ・ ローカルワイプまでのパスコード入力失敗回数 ・ ローカルロックまでのパスコード入力失敗回数
	機 能	・ ポーリング間隔時間 ・ 制限メッセージの設定 ・ カメラ使用制御 ・ Wi-Fi使用制御 ・ VPNの設定変更を禁止 ・ Bluetoothを禁止 ・ Bluetooth設定変更を禁止 ・ 外部ストレージを禁止 ・ デザリング & モバイルホットスポットの設定変更を禁止 ・ 位置情報共有設定を禁止 ・ スクリーン・キャプチャーを禁止 ・ 開発者モード（デバッグ機能）を禁止する ・ USB経由のファイル送受信を禁止 ・ ユーザによるハードリセットを禁止 ・ ユーザによる緊急速報メールの設定変更を禁止 ・ ユーザによる認証情報の設定変更を禁止	・ USB経由のファイル送受信を禁止 ・ 強制的に時刻自動設定をオンにする ・ Time Zone設定を「タイムゾーンの自動設定」にする ・ 電話発信を禁止（緊急電話を除く） ・ SMS送受信を禁止 ・ モバイルネットワークの設定変更を禁止 ・ データローミングを設定オフ ・ NFCを利用したAndroidビームの禁止 ・ アカウント追加・削除を禁止 ・ セーフモードの禁止 ・ システムアップデートの実行タイミングの設定を可能とする。 ・ ロック画面の表示を禁止 ・ ファクトリリセットの保護を有効にする ・ 非正規利用(旧SafetyNet)検知時の対応 ・ VPNアプリの常時接続を設定する（Cisco AnyConnectのみ） ・ デバイス管理アプリメッセージを追加する
	アプリ	・ 起動時権限設定 ・ アプリ確認の無効化を禁止 ・ アプリ管理の設定変更を禁止 ・ アプリインストール禁止	・ 非Google Play アプリ（第三者アプリ）のインストール禁止 ・ アプリアンインストール許可 ・ 指定したアプリをアンインストール禁止
	アプリ制御	・ アプリ指定	
	SIM変更検知	・ デバイスロック	・ SIMカードの変更検知

デバイスに設定可能な項目一覧：Android Enterprise **Work profile**

制 御	パスコード	• パスコード義務化・パスコードの有効期限 • パスコード設定有効期限 • パスコードの種類・バックライト点灯時間	• パスコードの再入力時間間隔 • パスコードの再利用回数 • ローカルワイプまでのパスコード入力失敗回数 • ローカルロックまでのパスコード入力失敗回数
	機 能	• ポーリング間隔時間 • 制限メッセージの設定 • スクリーン・キャプチャーを禁止 • 開発者モード（デバッグ機能）を禁止する • ユーザによる認証情報の設定変更を禁止	• プロファイル間のコピー & ペーストを禁止 • SMS送受信を禁止 • アカウント追加・削除を禁止 • VPNアプリの常時接続を設定する（Cisco AnyConnectのみ） • ワイプ時メッセージの追加をする • デバイス管理アプリメッセージを追加する
	アプリ	• 起動時権限設定 • アプリ確認の無効化を禁止 • 非Google Play アプリ（第三者アプリ）のインストール設定 • アプリ管理の設定変更を禁止 • アプリインストール禁止	• アプリアンインストール許可 • 指定したアプリをアンインストール禁止 • 指定したクロスプロファイルアプリを利用許可
	アプリ制御	• アプリ指定	
	SIM変更検知	• デバイスロック	• SIMカードの変更検知

デバイスに設定可能な項目一覧：Android Enterprise

COPE

制 御	パスコード	- パスコード義務化・パスコードの有効期限 - パスコード設定有効期限 - パスコードの種類・バックライト点灯時間	- パスコードの再入力時間間隔 - パスコードの再利用回数 - ローカルワイプまでのパスコード入力失敗回数 - 入力失敗時のローカルワイプ領域 - ローカルロックまでのパスコード入力失敗回数 - 入力失敗時のローカルロック領域
	機 能	- ボーリング間隔時間 - 制限メッセージの設定 - カメラ使用制御 - 外部ストレージを禁止 - スクリーン・キャプチャーを禁止 - 開発者モード（デバッグ機能）を禁止する - USB経由のファイル送受信を禁止 - ユーザによる認証情報の設定変更を禁止 - プロフィール間のコピー & ペーストを禁止	- アカウント追加・削除を禁止 - ロック画面の表示を禁止 - ファクトリーリセットの保護を有効にする - 非正規利用(旧SafetyNet)検知時の対応 - VPNアプリの常時接続を設定する（Cisco AnyConnectのみ） - ワイプ時メッセージの追加をする - デバイス管理アプリメッセージを追加する - 仕事領域OFFの最大時間設定
	アプリ	- 起動時権限設定 - Google Playプロテクトの無効化を禁止 - 非Google Play アプリ（第三者アプリ）のインストール設定 - アプリ管理の設定変更を禁止	- アプリインストール禁止 - アプリアンインストール許可 - 指定したアプリをアンインストール禁止 - 指定したクロスプロフィールアプリを利用許可
	個人領域のPlayストア	- 個人領域のPlayストアを制御 - 指定したアプリのみを表示 - 指定したアプリを非表示	
	アプリ制御	アプリ指定	
	SIM変更検知	デバイスロック	SIMカードの変更検知

managed Google Play Account方式でデバイス登録された場合、
制御ポリシーの「アカウント追加・削除禁止」のチェックを外した設定を適用頂くことで、
デバイスへアカウントを登録頂くことが可能となります。

但し、個人用アカウント（Google Workspace・Gmail含む）を追加されると
企業用Playストアだけでなく個人用のPlayストアが開放されるため、
利用者が自由にアプリをインストールできるようになりますので、ご注意ください。（下表 1）
※アカウントを追加されますと、Playストア上でデバイス登録されているアカウントごとに表示を切り替えることが
できるようになります。

Google Workspaceの利用並びに、企業用Playストアのみの利用を前提とされている場合は、
Google Workspaceのトークン登録方式の導入をご検討ください。（下表3）

●登録方式とGoogle Workspaceの同期有無によるPlayストアの差分について

	キッティング方法	Google Workspace 同期有無	企業専用Playストア (managed Google Play)	Playストア/企業専用Playストア
1	managed Google Play Account方式	あり	企業専用Playストアが利用可能	Playストアが利用可能
2	managed Google Play Account方式	なし	企業専用Playストアが利用可能	提供無
3	Google Workspaceトークン方式	あり	提供無	企業専用Playストアが利用可能



デバイスに設定可能な項目一覧：4Gケータイ

機能制御	パスコード	• パスコードの要求 • パスコードの有効期限 • パスコードの種類 • バックライト点灯時間 • ローカルワイプまでのパスコード入力失敗回数 • ローカルロックまでのパスコード入力失敗回数
	デバイスの制御	• カメラ使用制御 • Wi-Fi使用制御 • Bluetooth使用制御 • 外部メモリ使用制御 • テザリング使用制御
	GPS設定	• 位置情報の取得制御
	その他	• ポーリング間隔時間の設定

アンチウイルス機能一覧：Windows

不正サイト接続ブロック	毎日リアルタイムで監視・更新されているトレンドマイクロの不正Webサイトの評価データベース情報を基に、フィッシング詐欺やウイルスが仕込まれているWebサイトなど、危険なWebサイトへのアクセスを未然にブロック。 ※改ざんされたWebも検索対象。
Webレピュテーション・URLフィルタ	業務上必要のないWebサイトへのアクセス制御。 フィルタの強度、ルール、時間帯等を設定することで、お客様のビジネス環境に応じて柔軟に規制対象のWebサイトを設定可能。
スキャンパフォーマンスコントロール	PC負荷が少ないときにスキャンを行うことにより、利用アプリケーションへの影響を少なくする。
その他の機能	• ウイルス対策 • スパイウェア対策 • 不正侵入防止 • POP3メール検索 • 挙動監視,脆弱性診断 • スマートスキャン • インスタントメッセージコンテンツフィルタ • 大規模感染防止 • Webインストール • エージェントアンインストール/アンロード防止パスワード設定
Webによるクライアント管理	—
グループごとのセキュリティ設定	—
その他機能	• ダッシュボードによる脅威/管理情報のサマリー表示 • ワンタイムレポート • 日、週、月ごとのスケジュールレポート • メールでの自動通知

アンチウイルス機能一覧：Mac

不正サイト接続ブロック	毎日リアルタイムで監視・更新されているトレンドマイクロの不正Webサイトの評価データベース情報を基に、フィッシング詐欺やウイルスが仕込まれているWebサイトなど、危険なWebサイトへのアクセスを未然にブロック。 ※改ざんされたWebも検索対象。
Webレピュテーション・URLフィルタ	業務上必要のないWebサイトへのアクセス制御。 フィルタの強度、ルール、時間帯等を設定することで、お客様のビジネス環境に応じて柔軟に規制対象のWebサイトを設定可能。
スキャンパフォーマンスコントロール	PC負荷が少ないときにスキャンを行うことにより、利用アプリケーションへの影響を少なくする。
その他の機能	• ウイルス対策 • スパイウェア対策
Webによるクライアント管理	—
グループごとのセキュリティ設定	—

資産情報入力項目：Windows

利用者情報	・ 氏名 ・ 社員番号	・ 部署名1～4 ・ 任意1～4
資産情報	・ コンピュータ名 ・ リース・レンタル会社名 ・ 契約番号 ・ リース管理番号 ・ 資産管理番号 ・ 資産区分 ・ 機器名称 ・ 機器管理番号 ・ レンタル開始日	・ レンタル終了日 ・ 保証期間開始日 ・ 保証期間終了日 ・ 設置場所（郵便番号） ・ 設置場所（住所） ・ 設置場所（ビル） ・ 設置場所（階数） ・ 貸出PCIP設定区分 ・ 貸出部署

資産情報入力項目：Macデバイス

利用者情報	- 氏名 - 社員番号	- 部署名1～4 - 任意1～4	
資産情報	- コンピュータ名 - リース・レンタル会社名 - 契約番号 - リース管理番号 - 資産管理番号 - 資産区分 - 機器名称 - 機器管理番号 - レンタル開始日	- レンタル終了日 - 保証期間開始日 - 保証期間終了日 - 設置場所（郵便番号） - 設置場所（住所） - 設置場所（ビル） - 設置場所（階数） - 貸出PCIP設定区分 - 貸出部署	- 料金負担部署 - 利用用途 - 契約金額 - 支払日 - 初回支払金額 - 支払金額1～5 - メモ1～20

資産情報入力項目：Mac

利用者情報	- 氏名 - 社員番号	- 部署名1～4 - 任意1～4	システムロックPINコード
資産情報	- コンピュータ名 - 資産管理番号 - 資産区分 - 機器名称 - 機器管理番号 - 設置場所（郵便番号） - 設置場所（住所1～3） - 保証期間開始日	- 保証期間終了日 - リース・レンタル会社名 - 契約番号 - リース管理番号 - リース・レンタル開始日 - リース・レンタル終了日 - 契約金額	- 支払日 - 初回支払金額 - 支払金額1～5 - 貸出部署 - 料金負担部署 - 利用用途 - メモ1～20

M5・M6環境のみご利用いただける機能一覧		
共通	ダッシュボード機能	デバイス情報のサマリーをグラフで表示
	セキュリティ監査レポート	リモートロックおよびリモートワイプの実施回数・割合、セキュリティポリシー違反状況などをグラフ化したレポートをダウンロード可能
	証明書発行/配布機能	サイバートラスト社の証明書発行/配布が可能 ※M6環境のみ
iOS	ID管理サービス (MAM新規受付停止)	ID管理サイトにて作成したIDとPassでデバイス登録が可能
	ADE (旧DEP)機能	・アクティベーションと同時にデバイス登録が可能 ・ID管理サービスをご契約の場合は利用不可
	アプリカタログ機能	インストールさせたいアプリケーションのみ表示させるカタログ機能
Android	Android Enterprise	管理タイプごとに適した制限が可能 Google Play アプリのサイレントインストールが可能
4Gケータイ	各種基本サービス	対象デバイスの設定情報収集／デバイス遠隔設定／リモート設定／アンチウイルス機能／アプリケーション制御／Managed Apps
Windows	PC操作ログ	PCの各種操作ログを取得し、管理画面から閲覧可能とする機能
	位置情報取得	端末の位置情報を取得し、管理画面で確認できる機能 ※M6環境のみ
Mac	遠隔ロック・消去	Mac PCを遠隔からロック、消去する機能 ※M62/M63環境のみ

■ 2024年2月29日より新規でBCDMをご契約いただくお客様

- ご利用条件を満たした場合には、シングルサインオン機能（基本サービス）をご利用いただけます。
- オプションは申し込みが必要です。

■ 2024年2月29日以前にBCDMをご契約のお客様

- 「シングルサインオン機能」の利用開始には、**お客様による申請**が必要となります。

お申し込み方法

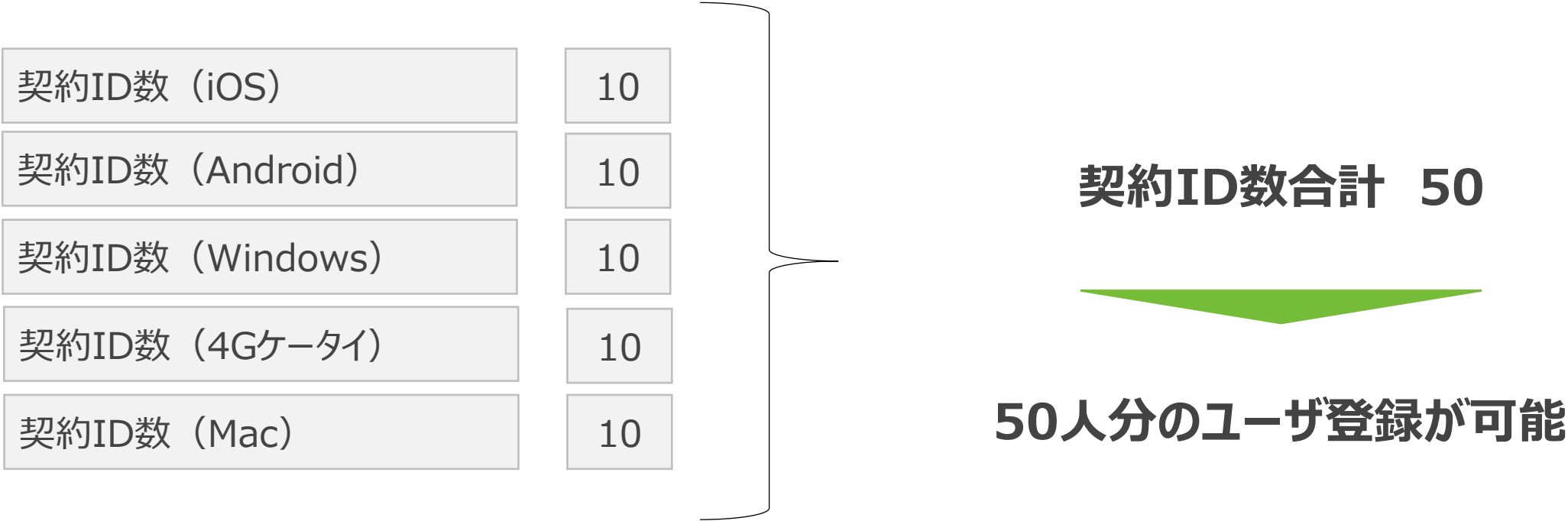
- お客様にて専用フォーム（Googleフォーム）にアクセスし、フォームに記載の案内事項と注意事項をご確認の上、フォームに必要事項を記入し、申請ください。
- ご利用対象のお客様へは専用フォームのリンクを2024/6/10「SoftBankからのお知らせ」（メールおよび管理画面のお知らせ）にてご案内しております。

■ ご利用条件（共通）

- シングルサインオン機能を利用できるユーザーの上限数は、1DMコードあたりのご契約IDの合計数です。
- 外部ディレクトリ（ADなど）との連携はできません。
- ソフトバンク株式会社の海外現地法人よりご契約のお客様は、シングルサインオン機能をご利用いただけません。
- 基本サービスに含まれる4つのSaaS（Google Workspace、Zoom、LINE WORKS、PrimeDrive）をシングルサインオンで連携する場合、各SaaSを別途ご契約いただく必要があります。
- 本機能を利用するには米国Okta社が定める以下の規約に同意いただく必要があります。お客様が本機能を利用することによって規約の内容に同意したものと判断いたしますので、内容を確認ください。
 - [Okta Inc. Minimum Customer Agreement Terms](#)
 - [DATA PROCESSING ADDENDUM](#)

BCDMの契約ID数合計 = ユーザ登録可能なID数となります

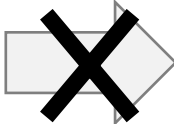
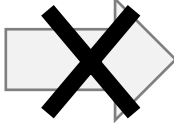
※例：BCDMの各デバイス種別を10ずつ契約した場合



- シングルサインオンオプション（「SSO無制限」「多要素認証」「多要素認証Pro」「ライフサイクル管理」）について下記にご留意ください。
- **シングルサインオンオプションは契約後に解約ができません。**
- オプションサービスは基本サービスの契約ID数と同数でのご契約となります。
- **1DMコードあたりのご契約ID数の合計数が、2,500ID以上のご契約でシングルサインオン機能をご利用希望の場合は、事前にご相談ください。**
- 多要素認証と多要素認証Proは併用できません。
- 多要素認証と多要素認証Proは併用できません。
- 「ライフサイクル管理」には「SSO無制限」が含まれております。（セットでのご提供のみ）
- **多要素認証Proから多要素認証、ライフサイクル管理からSSO無制限へ変更はできません。**
- **トライアル終了後、本契約の際にトライアル環境を引き継ぐ場合、シングルサインオンオプションを解除することはできません。**
シングルサインオンオプションの継続利用が不要な場合には、新規DMコードにてご契約をお願いします。
- 多要素認証と多要素認証Proの設定は弊社にて対応します。
お客様のご希望の設定内容を確認するため、専用のヒアリングシートをお渡ししますのでご記入をお願いいたします。
- ・レンタルオプションのBプラン、Cプランをご契約中の場合、シングルサインオンオプションはご利用いただけません。
シングルサインオンオプションをご利用希望の場合、D/E/Fプランへ変更していただく必要がありますが、BプランについているWebフィルタリング機能、CプランについているManaged Apps容量拡張機能はD/E/Fプランに含まれませんのでご注意ください。
- 基本サービスで提供している5アプリの内、LINE WORKS、PrimeDrive、BCDMはライフサイクル管理オプションに対応していません。

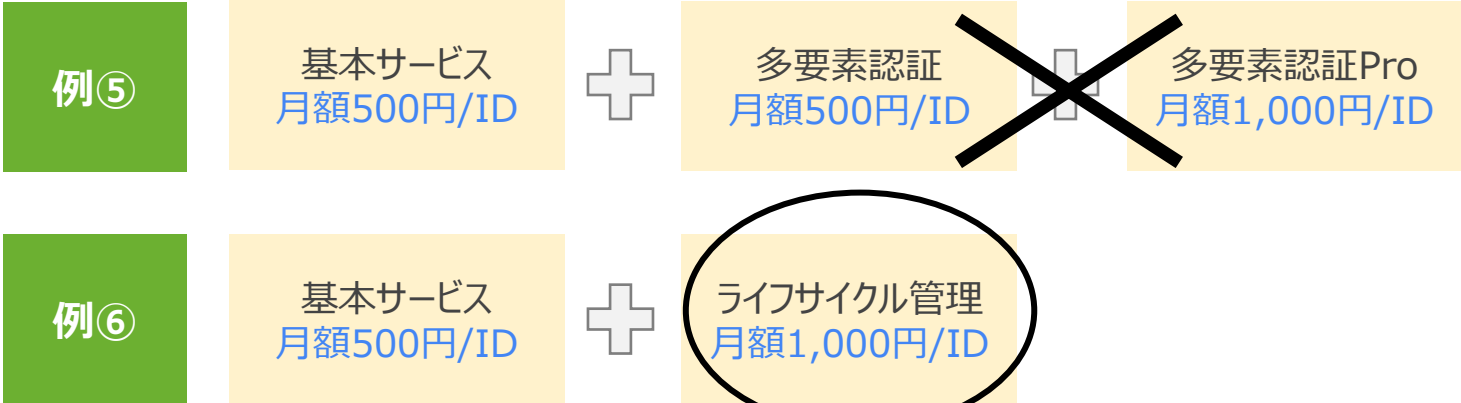
補足：オプション申込条件（１）オプションのみ削除は不可

シングルサインオンオプションのみ削除することは出来ません（例①～④は全て不可）

	変更前			変更後	
例①	基本サービス 月額500円/ID	+	SSO無制限 月額400円/ID		基本サービス 月額500円/ID + 解除
例②	基本サービス 月額500円/ID	+	ライフサイクル管理 月額1,000円/ID		基本サービス 月額500円/ID + 解除
例③	基本サービス 月額500円/ID	+	多要素認証 月額500円/ID		基本サービス 月額500円/ID + 解除
例④	基本サービス 月額500円/ID	+	多要素認証Pro 月額1,000円/ID		基本サービス 月額500円/ID + 解除

補足：オプション申込条件（2） 排他条件

- 多要素認証と多要素認証Proは同時契約は不可となります（例⑤）
- ライフサイクル管理はSSO無制限とセットでの提供のみとなります（例⑥）



共通	シングルサインオン 機能(オプション) ※オプション加入後 削除はできません	☒	SSO無制限		$(a + b + c + d + e) \times 400$ 円；月額	400円
		☐	多要素認証	(☐ 多要素認証 ☐ 多要素認証Pro)	選択すると金額が表示されます	
		☒	ライフサイクル管理	※ライフサイクル管理のご利用には、SSO無制限の加入が必要です	$(a + b + c + d + e) \times 600$ 円；月額	600円

月額1,000円/IDには、
SSO無制限+ライフサイクル管理が含まれます。
申込書上では、両方にチェックをお願いします。

補足：オプション申込条件（3） 加入オプション変更が可能なパターン

- 上位オプションへの変更は可です（例⑦、例⑨）
- 下位オプションへの変更は不可です（例⑧、例⑩）

	変更前				変更後		
例⑦	基本サービス 月額500円/ID	+	SSO無制限 月額400円/ID	→	基本サービス 月額500円/ID	+	ライフサイクル管理 月額1,000円/ID
例⑧	基本サービス 月額500円/ID	+	ライフサイクル管理 月額1,000円/ID	✗	基本サービス 月額500円/ID	+	SSO無制限 月額400円/ID
例⑨	基本サービス 月額500円/ID	+	多要素認証 月額500円/ID	→	基本サービス 月額500円/ID	+	多要素認証Pro 月額1,000円/ID
例⑩	基本サービス 月額500円/ID	+	多要素認証Pro 月額1,000円/ID	✗	基本サービス 月額500円/ID	+	多要素認証 月額500円/ID

シングルサインオン機能オプション（D,E,Fプラン）に加入後、変更可能なパターンは以下です。

- DプランからE、Fプランへの変更は可、その他の変更は不可

		変更後						
		基本	Aプラン	Bプラン	Cプラン	Dプラン	Eプラン	Fプラン
変更前	Dプラン	NG	NG	NG	NG		OK	OK
	Eプラン	NG	NG	NG	NG	NG		NG
	Fプラン	NG	NG	NG	NG	NG	NG	

 SoftBank