Endpoint Manager Cloud Free

利用ガイド

An-345 / 第 22 版 / 2024 年 2 月 28 日

MOTEX

まえがき

本書は、LANSCOPE エンドポイントマネージャー クラウド版 Free の設定方法について説明します。管理コンソールの操作をサポートします。

製品マニュアルラインナップ

各種マニュアルラインナップは、次のとおりです。

マニュアルの種類	説明
初期設定ガイド for iOS／iPadOS	iOS／iPadOS 向けの初期設定手順
初期設定ガイド for Android	Android 向けの初期設定手順
初期設定ガイド for Windows	Windows 向けの初期設定手順
初期設定ガイド for macOS	macOS 向けの初期設定手順
利用ガイド	管理コンソールの操作手順
アンインストールガイド	LANSCOPE クライアントのアンインストール手順

用語について

- 断りのない限り、本書の「iOS」は「iOS／iPadOS」の双方を指します。

お問い合わせ先

操作方法／トラブル／販売／お取扱いなど

メールまたは電話でお問い合わせください。

https://tryweb2.motex.co.jp/contact/cloud_support.html

商標・著作権

第 1 章　エンドポイントマネージャー Free の使い方

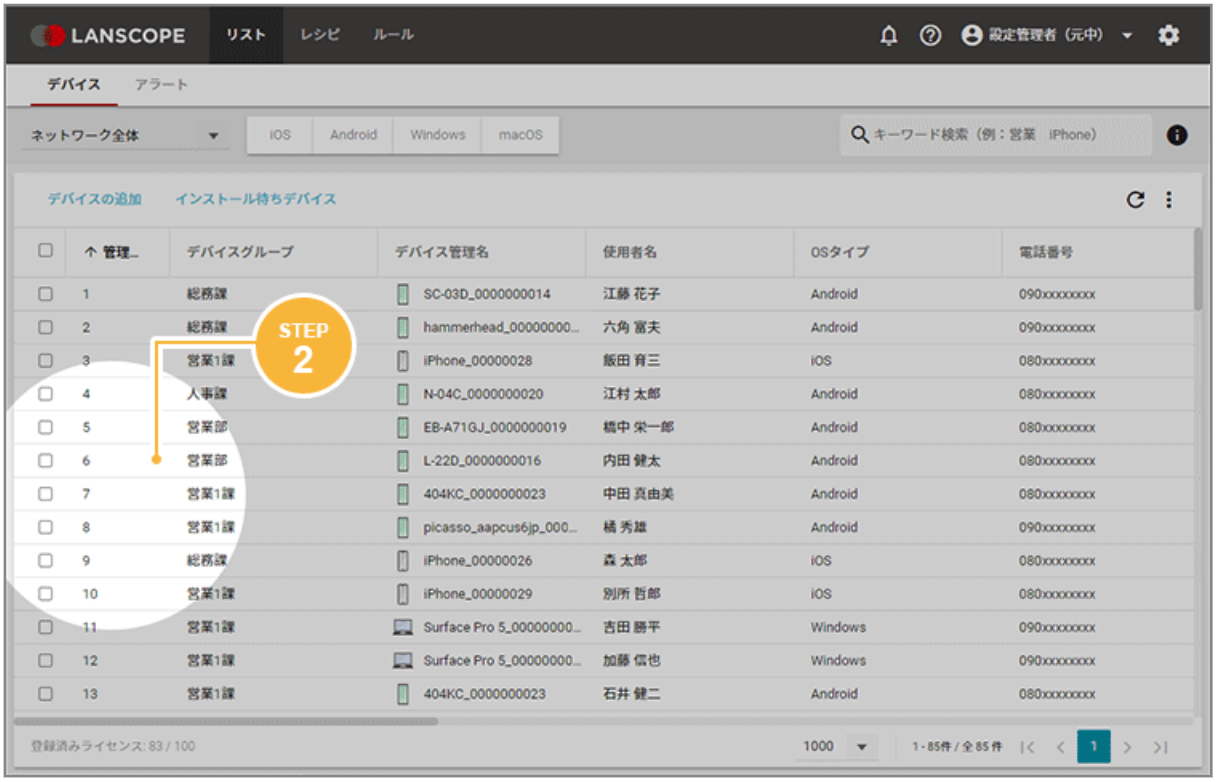
LANSCOPE エンドポイントマネージャー クラウド版 Free は、スマホ／タブレット／PC を一元管理するスマートデバイス管理ツールです。管理コンソールの操作は、基本的に次の「3 STEP」で行います。

1. **目的を選択します。**

   デバイスや設定を確認するときは一覧表示の「リスト」、エンドポイントマネージャー Free の設定をするときは「ルール」など、目的のメニューを選択します。

2. **対象を選択します。**

   OS の絞り込みや検索などを利用し、確認したいデバイスを選択します。

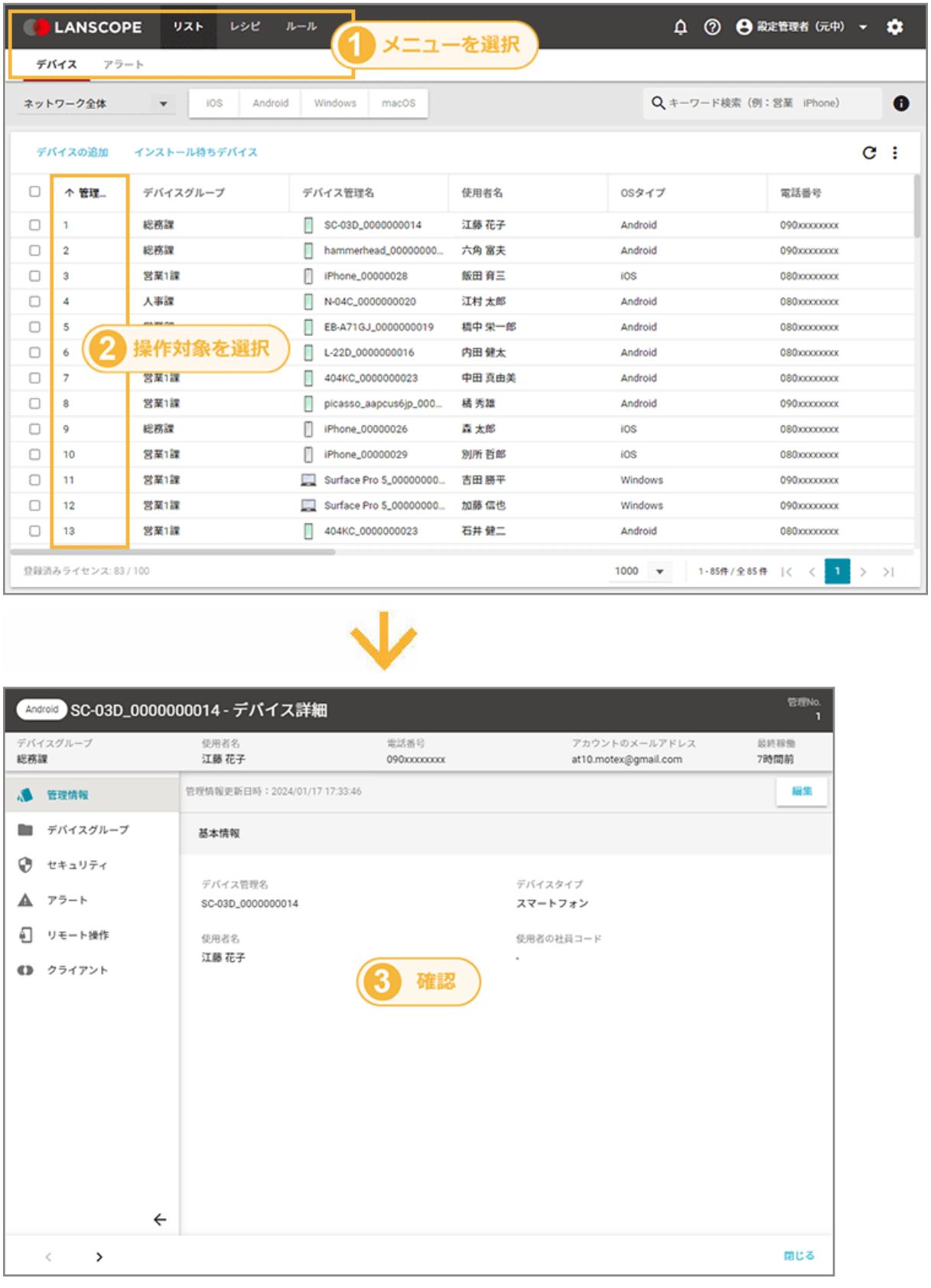


3. 確認／対策をします。

表示された画面で、データ確認や必要な対策の実施などを行います。

1-1　管理コンソール画面の見方

次のように操作します。メニューが変わっても導線は同じです。

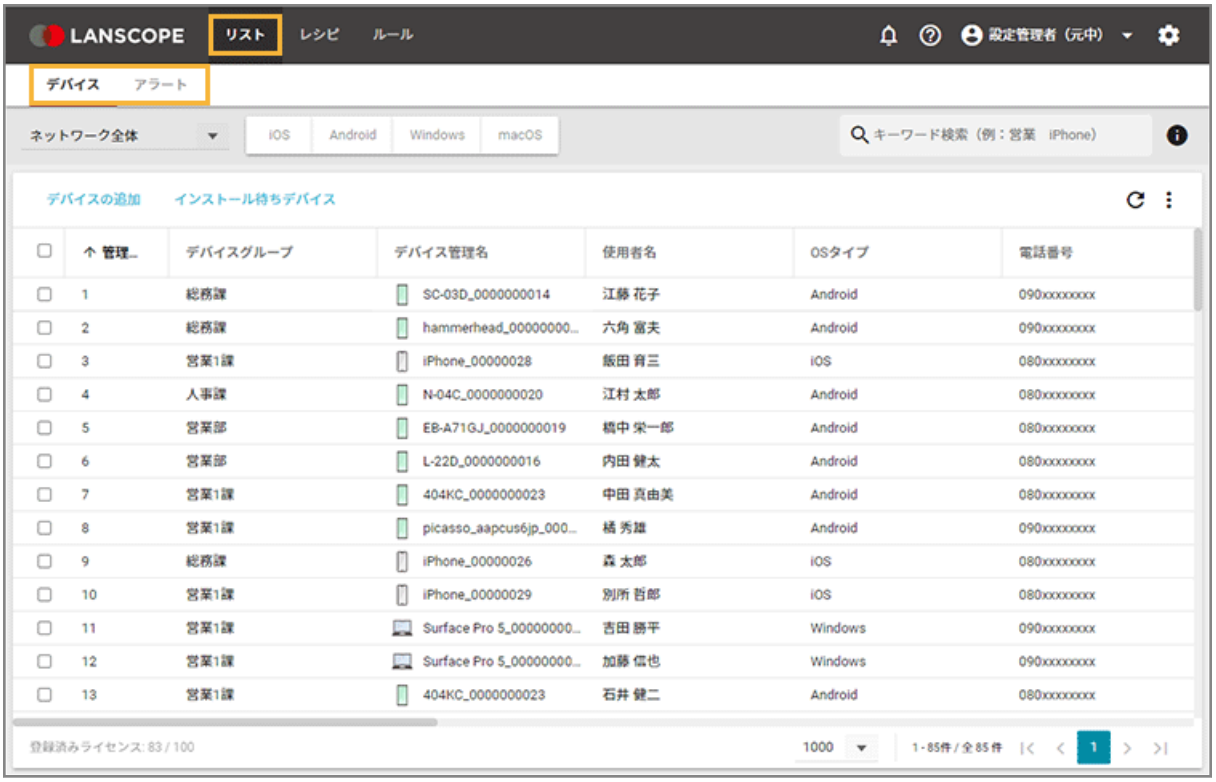


■ 画面構成

管理コンソールの画面構成について、カテゴリーメニューごとに説明します。

リスト

デバイスの一覧からデバイスを選択し、詳細情報の確認やリモート操作ができます。

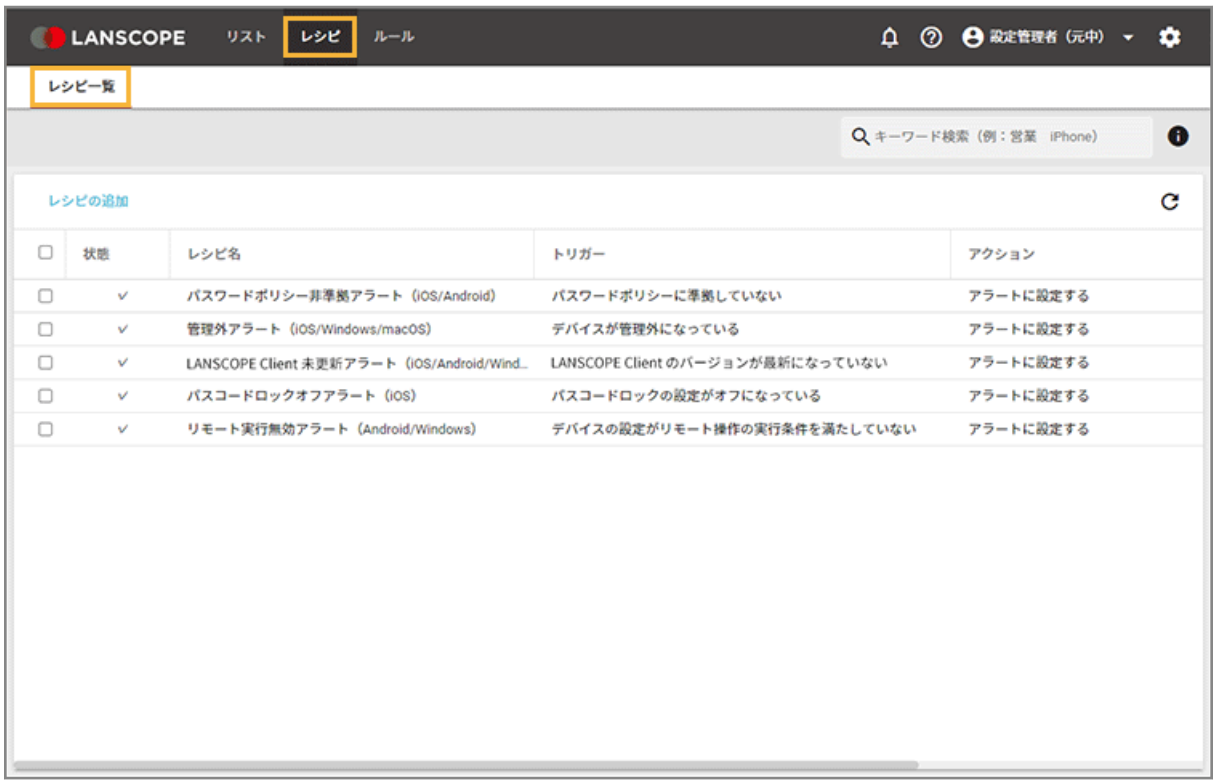


メニュー	内容
デバイス	デバイス情報を一覧で確認できます。また、各デバイスのリモート操作ができます。
アラート	各デバイスで発生しているアラート情報を、アラートごとに確認できます。

レシピ

設定した条件に一致したデバイスに対し、アプリやメッセージ配信など指定したアクションを自動実行します。このトリガーとアクションの組み合わせを、レシピとして登録します。

エンドポイントマネージャー Free では、「アラート設定」だけを利用できます。



メニュー	内容
レシピ一覧	作成したレシピを一覧で確認できます。

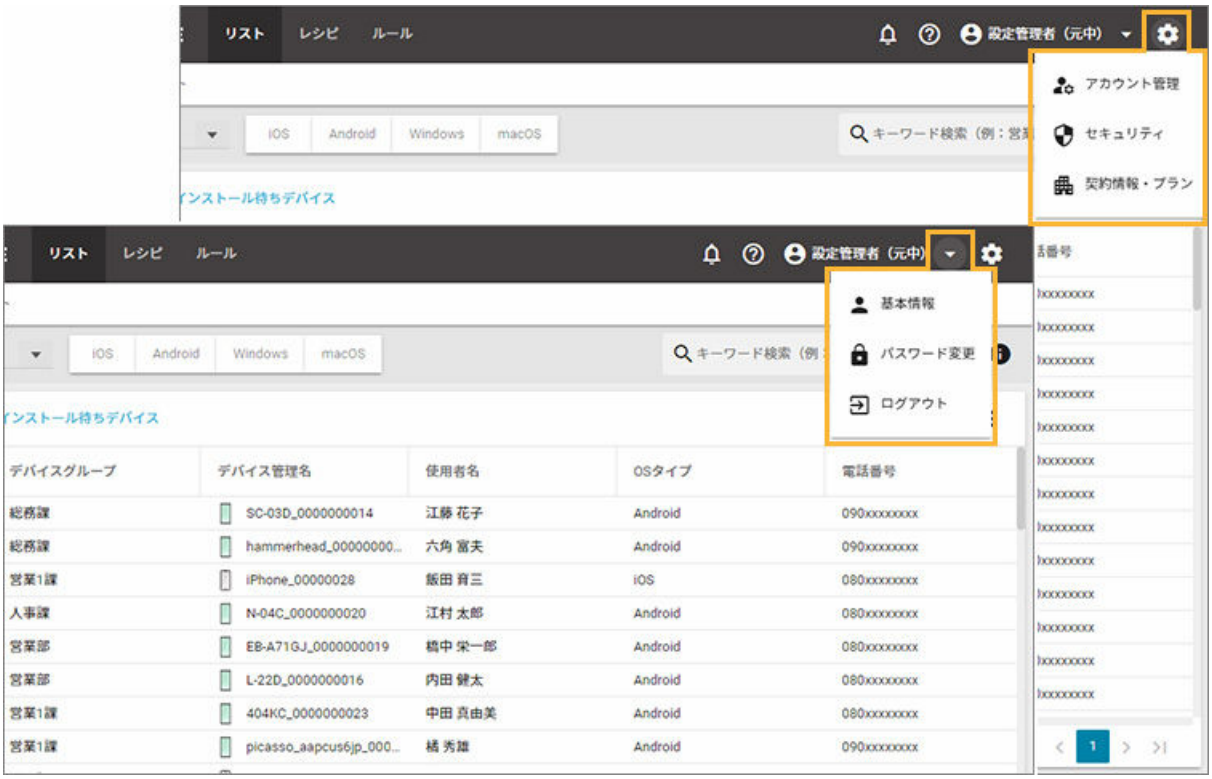
ルール

エンドポイントマネージャー Free を利用／運用するために必要な設定ができます。

メニュー	内容
デバイス設定	エンドポイントマネージャー Free を利用／運用するための各種設定を行います。
Apple サービス設定	iOS／macOS デバイスの管理に必要な MDM 証明書の設定をします。

共通

管理コンソール全体で使用する共通のメニューです。 ／ をクリックすると、メニューが表示されます。



メニュー		内容
システムメニュー	アカウント管理	アカウント設定を確認できます。また、追加設定や変更／削除ができます。
	セキュリティ	管理コンソールのパスワードポリシー設定や、2 要素認証の設定ができます。
	契約情報・プラン	契約情報／契約プラン（契約プラン／利用ライセンス数／契約ライセンス数など）を確認できます。
アカウントメニュー	基本情報	基本情報（登録 ID／契約法人名）を確認できます。
	パスワード変更	現在ログインしているアカウントのパスワードを変更できます。
	ログアウト	管理コンソールからログアウトします。

■ アイコン

管理コンソール画面の機能アイコンについて説明します。

1

リリース情報やメンテナンス情報などをお知らせするウィンドウが表示されます。

2

各種マニュアルや製品に関する FAQ、ユーザー様向けページのリンクが表示されます。

3

アイコン横に、現在のログインユーザー名が表示されます。

4

ログインユーザーのアカウントに関する設定を行います。

5

管理コンソールに関する設定を行います。また、契約情報／プランを確認できます。

6

デバイス／アプリなど、キーワードを入力して検索できます。

7

画面表示を更新できます。

⑧ ⋮

操作できるメニューが表示されます。

⑨

グループ専用のポリシー設定を適用している場合に表示されます。

ポリシーを設定していないデバイスグループは、上位グループに適用されているポリシーが継承されます。

⑩

配下にポリシー設定が割り当てられているグループがある場合に表示されます。

1-2　管理コンソールのログイン／ログアウト

■ 管理コンソールにログインする

初回ログイン

管理コンソールのログイン方法を説明します。

パスワードの再設定も同じ手順です。

1. **納品メールに記載された管理コンソールの URL にアクセスします。**

ポイント

- URL の形式は「https://*********lanscopean.com」です。「***」部分はユーザーごとに異なるため、納品メールを確認してください。
- 納品メールを紛失した場合、管理コンソール（ > ［お問い合わせ］）からお問い合わせください。

2. **［パスワードの設定はこちら］をクリックします。**

3. **納品メールに記載されたアカウント登録しているメールアドレスを入力し、［送信］をクリックします。**

注意

アカウント登録していないメールアドレスを入力して［送信］をクリックした場合、管理コンソールには「メールの送信に成功」と表示されますが、メールは送信されません。

→ 入力したメールアドレス宛に、パスワードをリセットする URL が記載されたメールが届きます。

4. 届いたメールからパスワードの設定を行います。

注意

パスワードの設定は、メール受信後 24 時間以内に行ってください。1 通のメールで変更できるのは、1 回だけです。24 時間以上経過した場合や、設定後に再設定する場合は、再度パスワード設定メールを送信してください。

5. 「アカウント（メールアドレス）」と、手順 4 で設定した「パスワード」を入力して、[ログイン] をクリックします。

ポイント

- 5 ライセンスごとに作成できるアカウントが 1 つ追加されます。
- 管理アカウントの追加／変更／削除は、［リスト］>［アカウント］で設定できます。

注意

ログインに連続 6 回失敗すると、アカウントが 10 分間ロックアウトされます。

2 要素認証有効時のログイン

2 要素認証を有効にしている場合の管理コンソールのログイン方法を説明します。

初回ログイン時は、認証デバイスの設定が必要です。詳細は、2 要素認証を有効にして認証デバイスを設定するを参照してください。

1. **管理コンソールの URL にアクセスします。**
2. **「アカウント」と「パスワード」を入力し、［ログイン］をクリックします。**

   注意

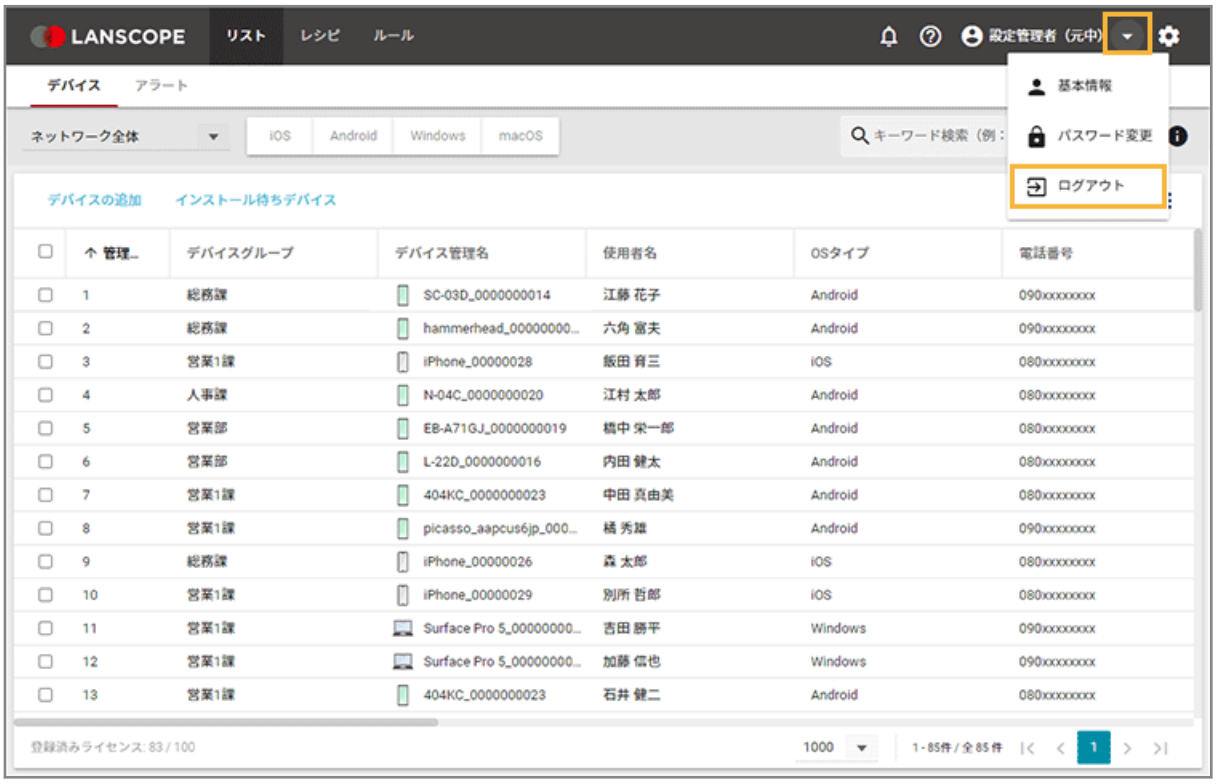
   ログインに連続 6 回失敗すると、アカウントが 10 分間ロックアウトされます。

3. **認証デバイスで認証アプリを起動し、認証コードを確認します。**
4. **認証コードを入力し、［認証］をクリックします。**

■ 管理コンソールからログアウトする

管理コンソールのログアウト方法を説明します。

1. **▼をクリックし、[ログアウト] をクリックします。**



→ 管理コンソールのログイン画面に戻ります。

1-3　アカウントを管理する

iOS Android Windows macOS

管理コンソールにログインするためのアカウント情報を管理できます。

ポイント

アカウント情報をインポート／エクスポートする場合、「ネットワーク全体」のアクセス許可があるアカウントでログインしてください。

注意

アクセス許可の編集と、デバイスグループの編集を同時に行なった場合、タイミングによってはアクセス許可設定が正しく反映されないことがあります。デバイスグループを編集したときは、アカウント情報は数分経ってから編集してください。

■ アカウントを追加する

ポイント

契約ライセンスが 10 ライセンス未満の場合、5 アカウントを作成できます。以降、5 ライセンスにつき、1 アカウントを作成できます。作成できるアカウントの計算方法は「保有ライセンス数」÷5 + 4 です。

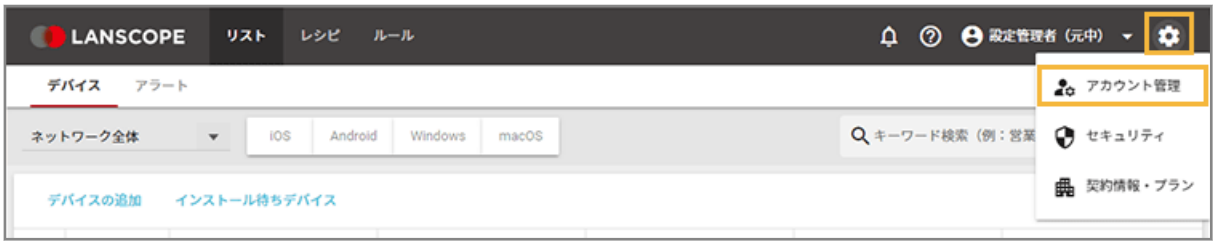
ただし、作成できるアカウントは、最大 2,000 アカウントです。

例：

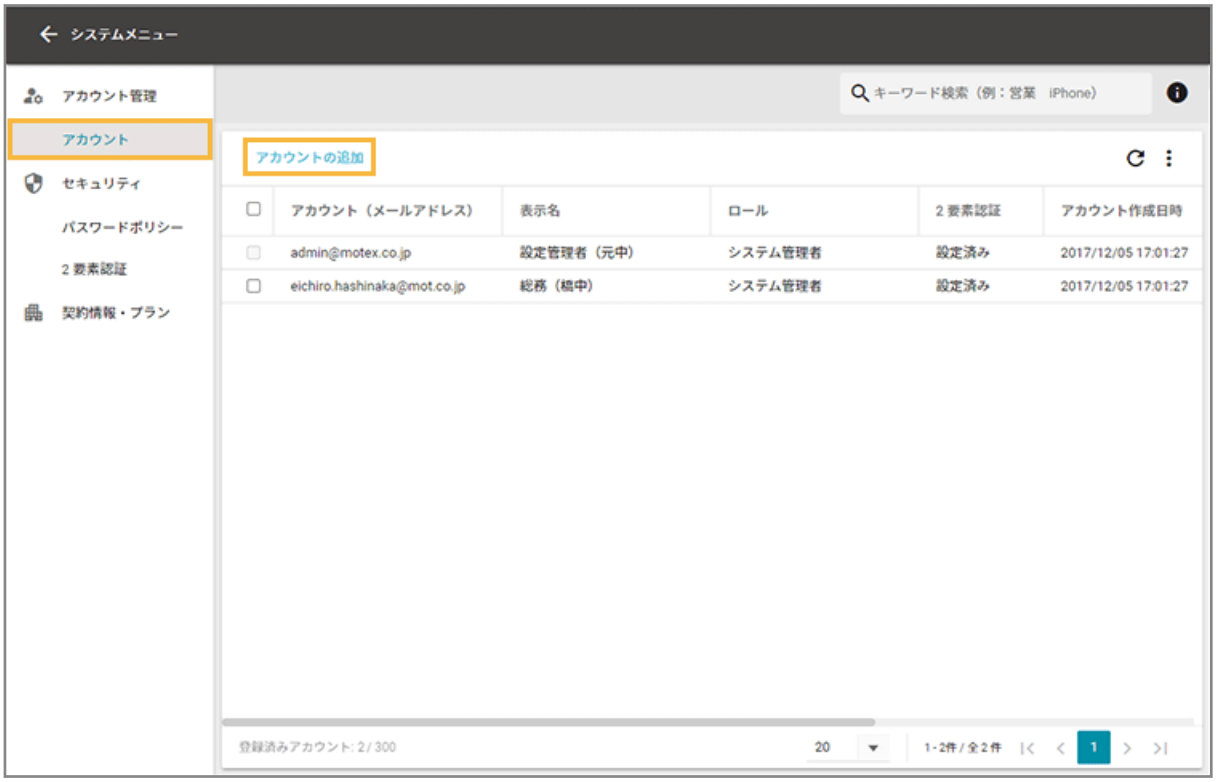
100 ライセンス保有している場合、「100÷5 + 4」= 24 アカウントを作成できます。

アカウントを 1 つずつ追加する

1. **をクリックし、［アカウント管理］をクリックします。**



2. ［アカウント］をクリックし、［アカウントの追加］をクリックします。



3. 必要事項を入力し、［追加］をクリックします。

メールアドレス

ログインするアカウントです。

> **注意**
>
> 無効なメールアドレス、および、すでにアカウントとして設定済みのメールアドレスは使用できません。

表示名

アカウントに表示される名前です。

ロール

「システム管理者」を選択します。

パスワード

ログインパスワードです。[ランダムなパスワードを自動で生成する] をクリックし、自動生成することもできます。

アクセス許可

表示や設定を許可するデバイスグループを選択します。選択したデバイスグループ配下が表示／設定対象になります。

> **注意**
>
> 次の操作は、「ネットワーク全体」のアクセス許可がないと操作できません。
>
> - デバイスグループの編集
> - かんたんインストール

アカウント情報をメールで送信する

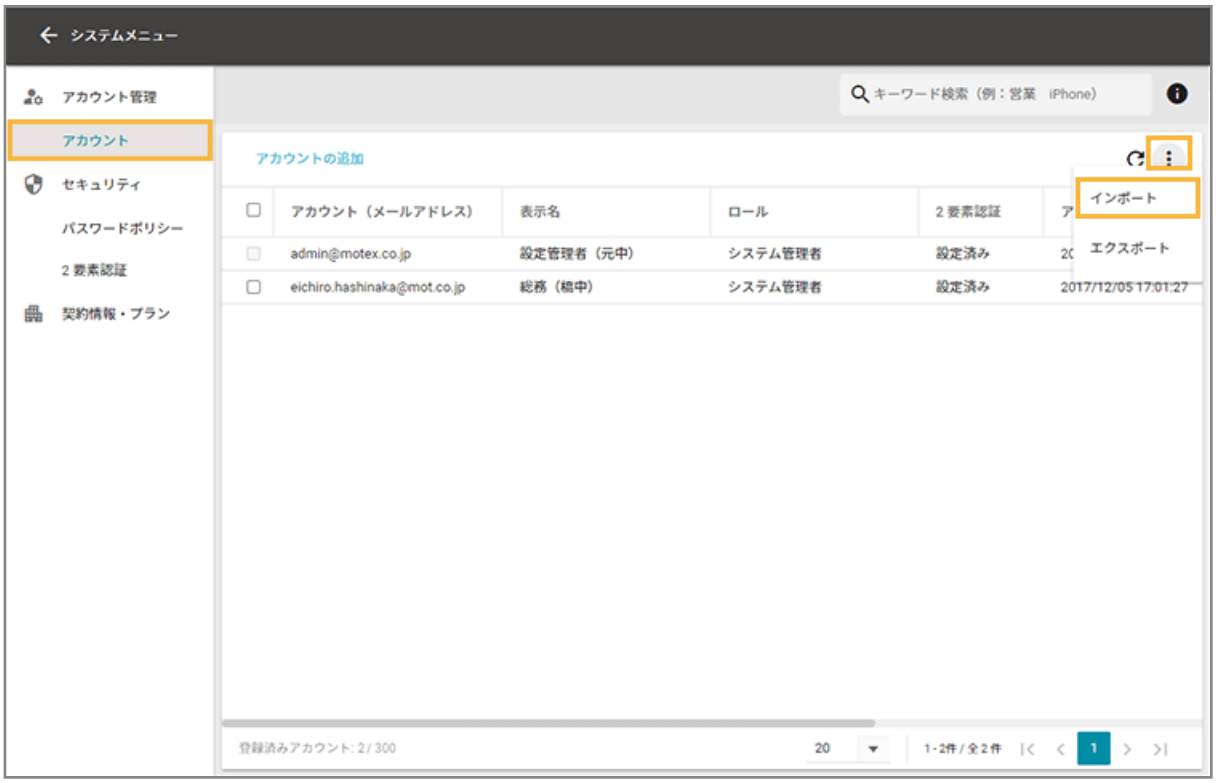
アカウントに設定するメールアドレス宛にアカウント情報を送信できます。チェックすると、送信されるメール本文が表示されます。メールの件名と本文は、編集できません。

→ アカウントが追加されます。

アカウントを一括で追加する

1. **をクリックし、[アカウント管理] をクリックします。**

2. ［アカウント］をクリックし、 ⋮ をクリックして、［インポート］をクリックします。



3. ［新しくアカウントを追加］を選択します。

4. ［テンプレートのダウンロード］をクリックします。

→　CSV ファイルがダウンロードされます。

5. ダウンロードしたファイルを編集し、インポートファイルを作成します。

メールアドレス

ログインするアカウントです。

> **注意**
>
> 無効なメールアドレス、および、すでにアカウントとして設定済みのメールアドレスは使用できません。

表示名

アカウントに表示される名前です。

ロール

「システム管理者」を設定します。

パスワード

ログイン時のパスワードです。8～15 文字以内の半角英数字記号を設定します。

デバイスグループ階層

表示や設定を許可するデバイスグループを設定します。入力したデバイスグループ配下が表示／設定対象になります。

「ネットワーク全体」を設定する場合は、空白にします。

> **注意**
>
> 次の操作は、「ネットワーク全体」のアクセス許可がないと操作できません。
>
> - デバイスグループの編集
> - かんたんインストール

アカウント情報をメールで送信する

アカウントに設定するメールアドレス宛にアカウント情報を送信できます。メールを送信する場合は「1」、送信しない場合は「0」を設定します。メールの件名と本文は、編集できません。

6. ［ファイルを選択］をクリックし、作成したインポートファイルを選択します。

7. ［自動選択］をクリックします。

→ 「関連づける列名」が自動的に選択されます。

「項目名」と「ファイルの列名」の項目が一致していないと自動的に選択されません。その場合は、対応する項目を 1 つずつ紐づけます。

8. ［インポート］をクリックします。

→ アカウントの追加が完了します。

■ アカウント情報を編集する

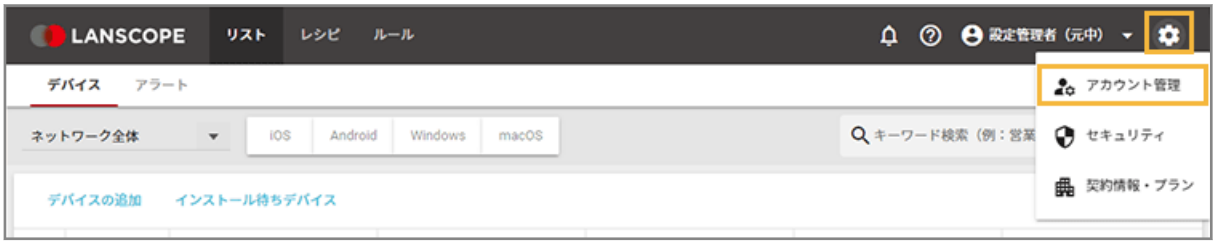
ここでは、アカウントごとに編集する場合を例に説明します。

複数のアカウントを一括で編集する場合は、 ⋮ > ［インポート］ > ［登録されているアカウントの情報を編集］で、登録しているアカウントをエクスポートして編集したファイルをインポートできます。

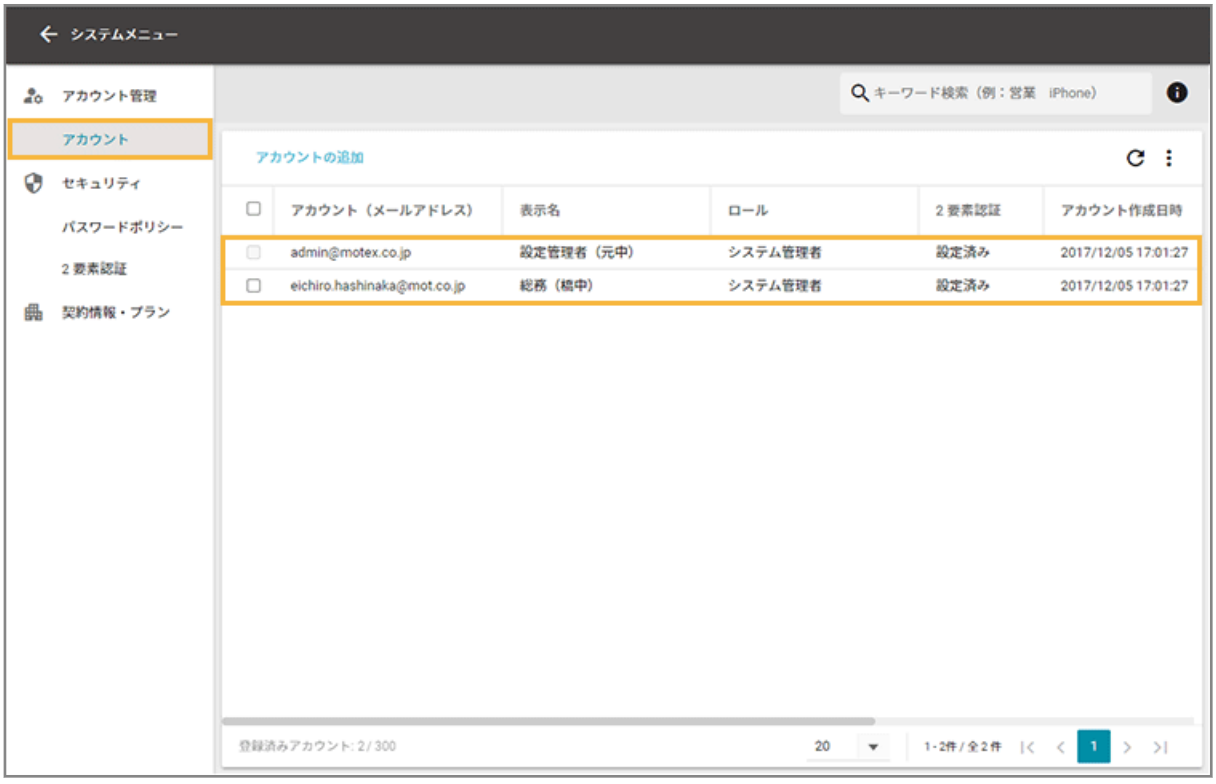
注意

ログインアカウント（メールアドレス）は編集できません。アカウントを新規作成してください。

1. **⚙をクリックし、［アカウント管理］をクリックします。**



2. **［アカウント］をクリックし、編集するアカウントをクリックします。**



3. **基本情報を編集する場合、［基本情報］の［編集］をクリックします。**

4. 編集後、［保存］をクリックします。

→ 基本情報が更新されます。

5. アクセス許可を編集する場合、［アクセス許可］の［編集］をクリックします。

6. 編集後、［保存］をクリックします。

→ アクセス許可の設定が更新されます。

7. パスワードを変更する場合、[パスワード] をクリックし、新しいパスワードを入力して、[保存] をクリックします。

[ランダムなパスワードを自動で生成する] をクリックすると、パスワードを自動生成できます。

→ パスワードが更新されます。

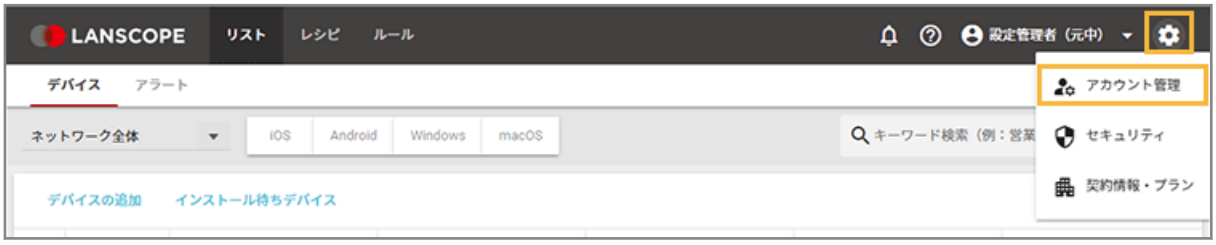
8. ［閉じる］をクリックします。

■ アカウントを削除する

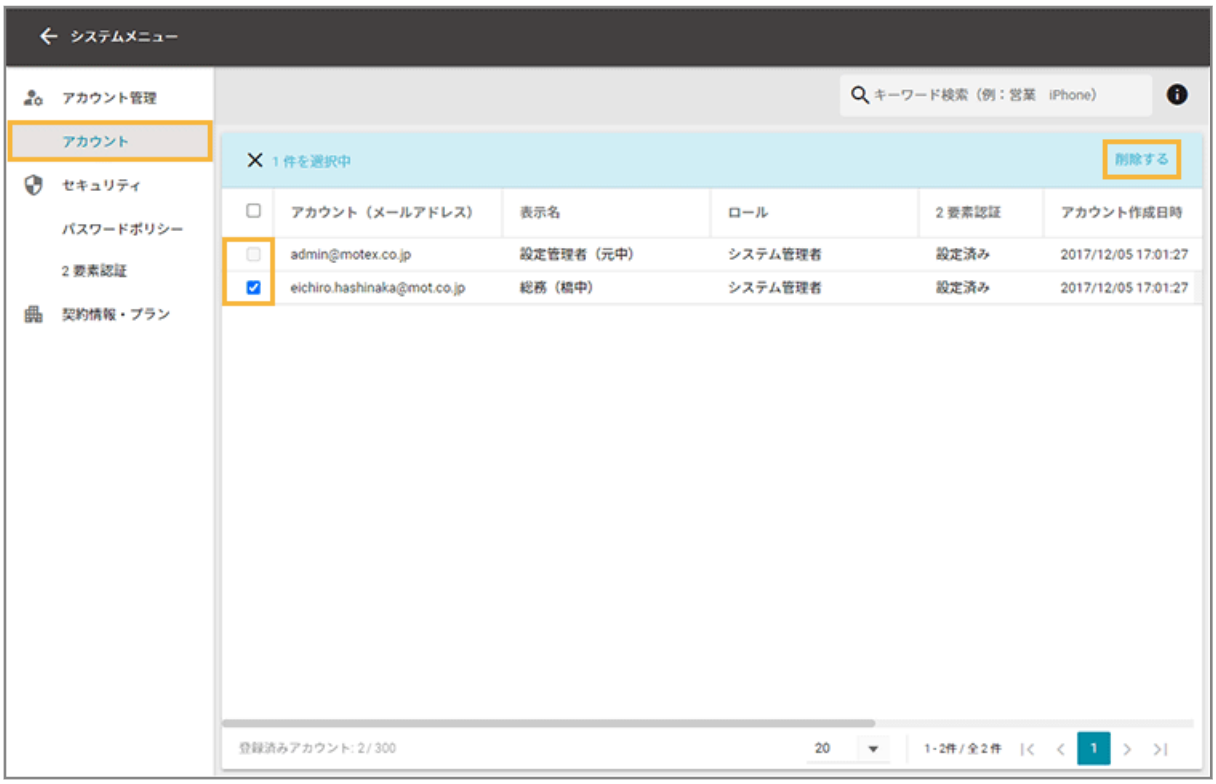
注意

ログインアカウント（メールアドレス）は削除できません。

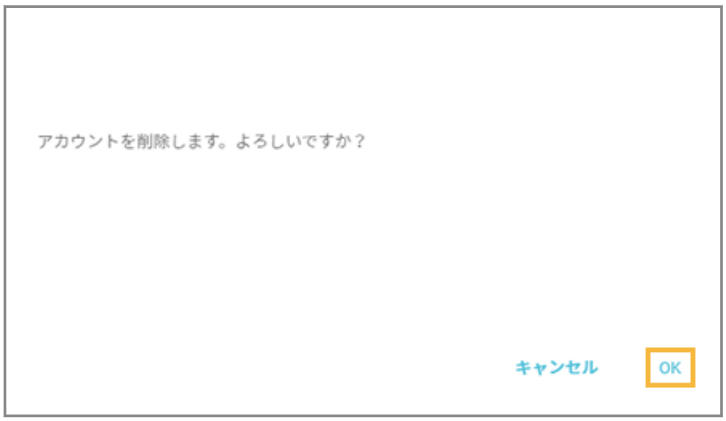
1. をクリックし、［アカウント管理］をクリックします。



2. ［アカウント］をクリックし、削除するアカウントをチェックして、［削除する］をクリックします。



3. ［OK］をクリックします。



→ をクリックし、アカウントが削除されたことを確認します。

1-4　セキュリティを管理する

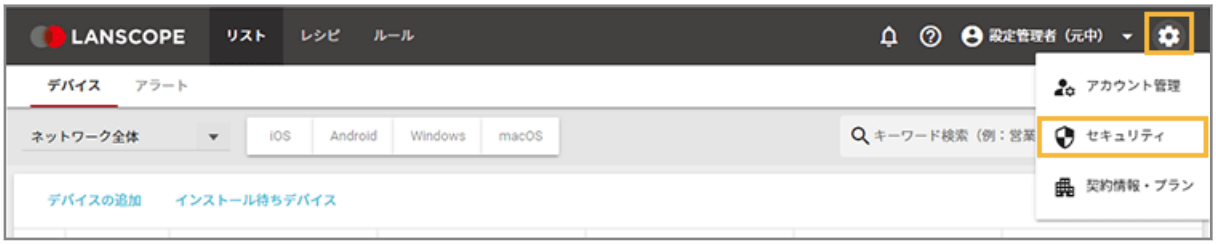
管理コンソールのセキュリティを管理します。

- パスワードポリシーを設定する
- 2 要素認証を設定する

パスワードポリシーを設定する

管理コンソールにログインするための、アカウントのパスワードポリシーを設定します。

1. **をクリックし、［セキュリティ］をクリックします。**



2. **［パスワードポリシー］をクリックし、［編集］をクリックします。**

3. **項目を設定し、［保存］をクリックします。**

パスワード強度

パスワードの文字数や、使用する文字の種類を設定できます。

パスワードの有効期間

同じパスワードを使用できる期間を設定できます。設定した期間を過ぎると、次回ログイン時にパスワードの再設定を求められます。

以前使用したパスワードの再使用

過去に使用していたパスワードを禁止する世代数を設定できます。世代数は、設定が有効になっている期間のパスワード変更、または再設定だけカウントされます。

→ パスワードポリシー設定が完了します。

ポイント

設定／変更した「パスワードの有効期間」は次回ログイン時から、その他の項目は次回パスワード変更／再設定時から適用されます。

2 要素認証を設定する

管理コンソールにログインするときの 2 要素認証を設定します。

■ 2 要素認証を有効にして認証デバイスを設定する

2 要素認証を有効にすると、すべてのアカウントで 2 要素認証を求められます。

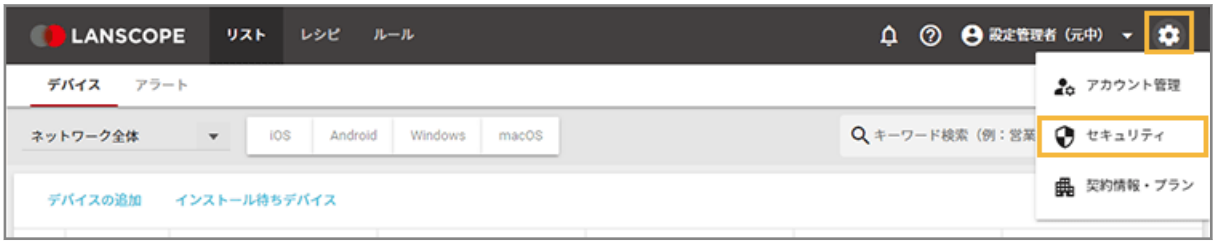
ステップ：

1. 2 要素認証を有効にする
2. 認証アプリをインストールする
3. 認証デバイスを設定する

ステップ 1：　2 要素認証を有効にする

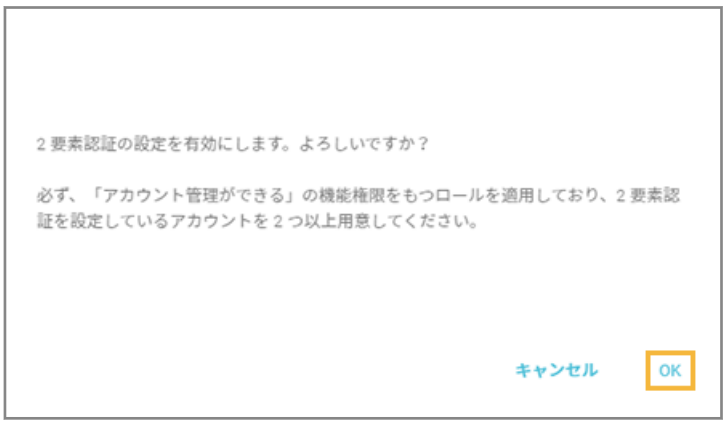
管理コンソールで、すべてのアカウントの 2 要素認証を有効にします。

1. **をクリックし、[セキュリティ] をクリックします。**



2. **[2 要素認証] をクリックし、[認証設定が無効です] を （有効）に切り替えます。**

3. **［OK］をクリックします。**



→ 2 要素認証の有効化が完了します。

ステップ 2： 認証アプリをインストールする

ログインに必要な認証コードを取得するための準備をします。すべての管理者のデバイスでインストールが必要です。

1. **デバイスに認証アプリをインストールします。**

   例：

   - Google Authenticator
   - Microsoft Authenticator

ステップ 3： 認証デバイスを設定する

認証アプリをインストールしたデバイスを、認証デバイスとして管理コンソールに登録します。すべてのアカウントで登録が必要です。

1. **管理コンソールの URL にアクセスします。**

2. **「アカウント」と「パスワード」を入力し、［ログイン］をクリックします。**

3. はじめて管理コンソールにログインする場合は、パスワードを変更する必要があります。

(1) 新しいパスワードを入力し、[パスワードを変更する] をクリックします。

(2) [次へ] をクリックします。

4. ステップ 2 でインストールした認証アプリで、QR コードを読み取ります。

QR コードを読み取れない場合は、［QR コードが読み取れない場合はこちら］をクリックし、表示されたコードを手動で認証アプリに入力してください。

5. 認証アプリに表示された認証コードを入力し、［認証］をクリックします。

→ 認証デバイスの設定が完了します。

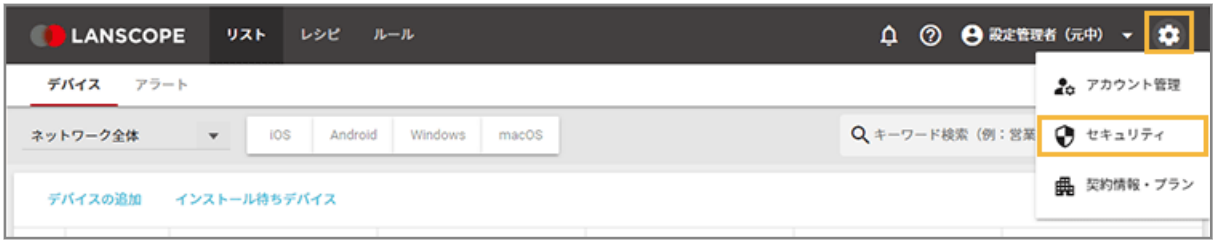
■ 2 要素認証を無効にする

2 要素認証を無効にすると、すべてのアカウントで、ログイン時に認証コードの入力が不要になります。

ポイント

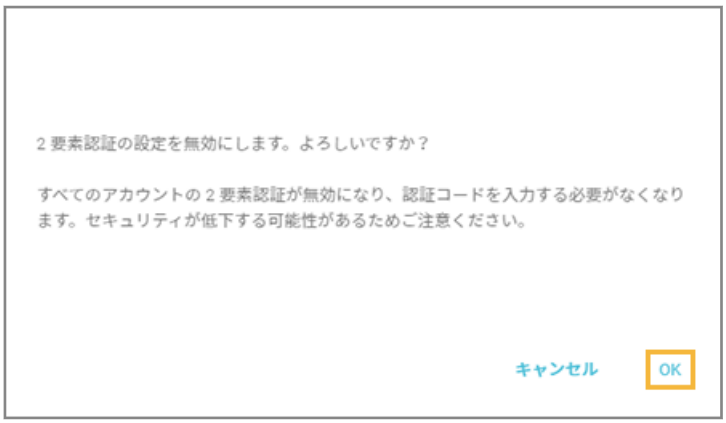
2 要素認証を無効にしても、認証デバイスの設定情報は削除されません。そのため、再度有効にしたとき、認証デバイスの再設定は不要です。

1. **をクリックし、[セキュリティ] をクリックします。**



2. **[2 要素認証] をクリックし、[認証設定が有効です] を （無効）に切り替えます。**

3. **[OK] をクリックします。**

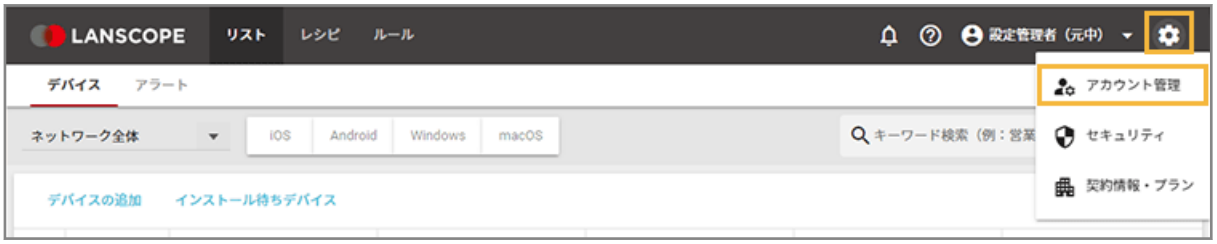


→ 2 要素認証の無効化が完了します。

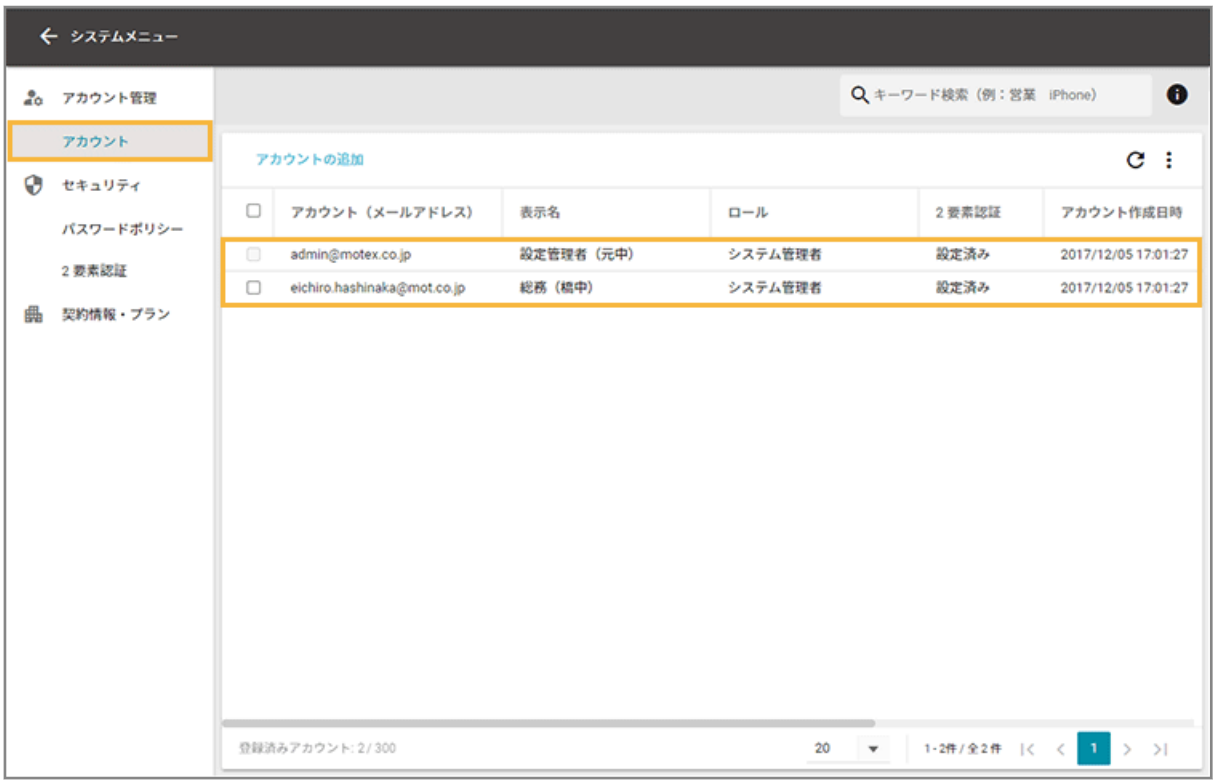
■ 2 要素認証を初期化して認証デバイスを変更する

機種変更などで認証デバイスを変更する場合に、アカウントの 2 要素認証設定を初期化します。

1. **をクリックし、[アカウント管理] をクリックします。**

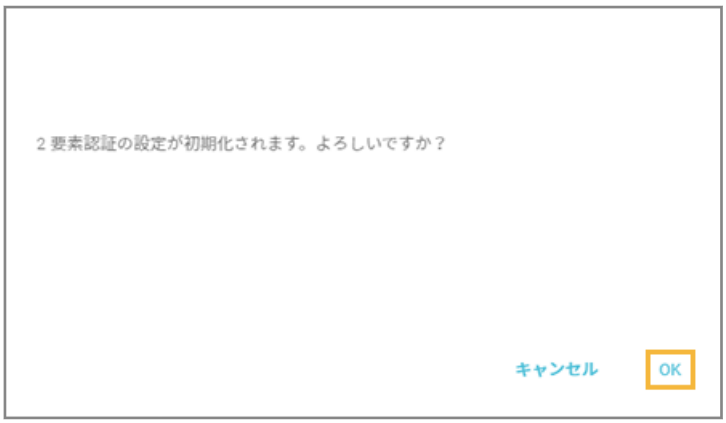


2. **[アカウント] をクリックし、初期化するアカウントをクリックします。**



3. ［2 要素認証］をクリックし、［初期化する］をクリックします。

4. ［OK］をクリックします。



→ 2 要素認証設定の初期化が完了します。次回ログイン時に、認証デバイスを再設定してください。

第 2 章　リストで情報を確認する

iOS Android Windows macOS

デバイスの一覧からデバイスを選択し、詳細情報の確認やリモート操作ができます。

- 2-1 デバイス情報を管理する
- 2-2 リモート操作を実行する
- 2-3 アラート情報を確認する

2-1　デバイス情報を管理する

iOS Android Windows macOS

「デバイス」画面では、デバイス情報の確認や編集／削除など、管理ができます。

- 管理できる項目一覧
- デバイス情報を確認する
- デバイス情報を編集／削除する

管理できる項目一覧

iOS Android Windows macOS

「デバイス詳細」画面で表示される項目は、OS によって異なります。

■ iOS

「デバイス詳細」画面の項目	項目名
管理情報	デバイス管理名／デバイスタイプ／使用者名／使用者の社員コード
デバイスグループ	デバイスグループ
セキュリティ	パスコードポリシー（プロファイル）
アラート	アラート（トリガー）名／アラートレベル
リモート操作	実行履歴（設定日時／実行者／内容／状態／実行日時／メッセージ／電話番号／詳細）
クライアント	MDM 構成プロファイルインストール日時／LANSCOPE クライアント最終稼働日時／MDM 構成プロファイル最終通信日時／MDM 構成プロファイルアンインストール日時（*）

*：アンインストールされた時にだけ表示されます。ネットワークに繋がっていないときにアンインストールされた場合、情報を取得できません。

■ Android

「デバイス詳細」画面の項目	項目名
管理情報	デバイス管理名／デバイスタイプ／使用者名／使用者の社員コード
デバイスグループ	デバイスグループ

「デバイス詳細」画面の項目	項目名
セキュリティ	パスワードポリシー
アラート	アラート（トリガー）名／アラートレベル
リモート操作	実行履歴（設定日時／実行者／内容／状態／実行日時／詳細）
クライアント	LANSCOPE クライアントインストール日時／LANSCOPE クライアントバージョン／LANSCOPE クライアント最終稼働日時／LANSCOPE クライアントの設定（デバイス管理者／使用履歴へのアクセス）

■ Windows

「デバイス詳細」画面の項目	項目名
管理情報	デバイス管理名／デバイスタイプ／使用者名／使用者の社員コード
デバイスグループ	デバイスグループ
デバイス情報	**システム** ログオンユーザー名 **ハードウェア** コンピューター名
アラート	アラート（トリガー）名／アラートレベル
リモート操作	実行履歴（設定日時／実行者／内容／状態／実行日時／詳細）
クライアント	LANSCOPE クライアントインストール日時／LANSCOPE クライアントバージョン／LANSCOPE クライアント最終稼働日時／LANSCOPE クライアントアンインストール日時(*)

*：アンインストールされた時にだけ表示されます。ネットワークに繋がっていないときにアンインストールされた場合、情報を取得できません。

■ macOS

「デバイス詳細」画面の項目	項目名
管理情報	デバイス管理名／デバイスタイプ／使用者名／使用者の社員コード
デバイスグループ	デバイスグループ

「デバイス詳細」画面の項目	項目名
デバイス情報	**システム** ログオンユーザー名 **ハードウェア** ホスト名
アラート	アラート（トリガー）名／アラートレベル
リモート操作	実行履歴（設定日時／実行者／内容／状態／実行日時／詳細）
クライアント	MDM 構成プロファイルインストール日時／LANSCOPE Client インストール日時／LANSCOPE クライアント最終稼働日時／MDM 構成プロファイル最終通信日時／LANSCOPE Client 最終通信日時／LANSCOPE Client バージョン／MDM 構成プロファイルアンインストール日時（*）

*：アンインストールされた時にだけ表示されます。ネットワークに繋がっていないときにアンインストールされた場合、情報を取得できません。

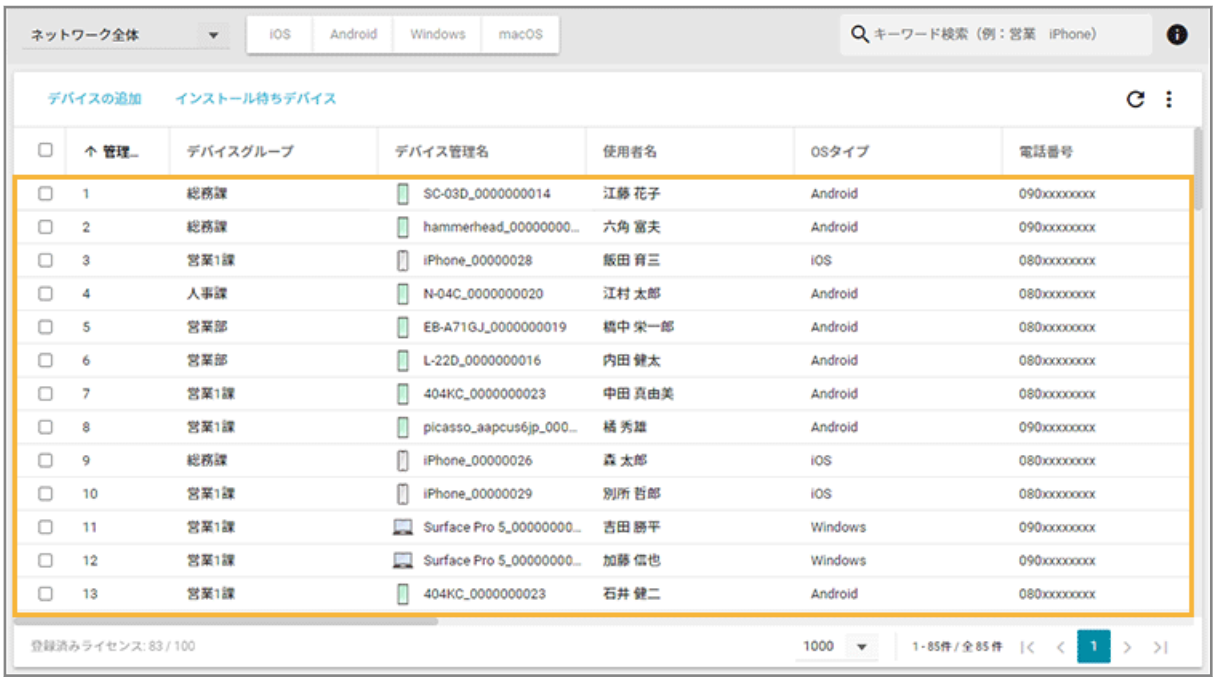
デバイス情報を確認する

iOS Android Windows macOS

1. **［リスト］の［デバイス］をクリックします。**

2. **デバイスをクリックします。**

   デバイスグループや OS で絞り込みができます。



3. 詳細情報を確認します。

管理情報

「使用者名」「使用者の社員コード」を管理／確認できます。

デバイスグループ

デバイスの所属グループを確認できます。

セキュリティ iOS Android

セキュリティに関する情報を確認できます。

アラート

デバイスで発生しているアラート情報を一覧で確認できます。

リモート操作

リモートロック／リモートワイプを実行できます。

クライアント

デバイスをエンドポイントマネージャー Free で管理するために必要なプログラム（MDM 構成プロファイルや LANSCOPE Client）の情報を確認できます。

ポイント

［リスト］>［デバイス］画面で、デバイスイメージ画像の表示／非表示を設定できます。設定を変更する場合は、⋮ >［デバイスイメージの設定］で「デバイスイメージを表示する」の有効／無効を切り替えてください。

デバイス情報を編集／削除する

iOS Android Windows macOS

エンドポイントマネージャー Free で自動取得できない項目（「デバイス詳細」画面の「管理情報」）は、管理コンソールで登録／編集できます。

たとえば、デバイス使用者が変更になった場合、デバイス情報（使用者名や使用者の社員コード）を変更することで、使用者変更後も継続してデバイスを管理できます。

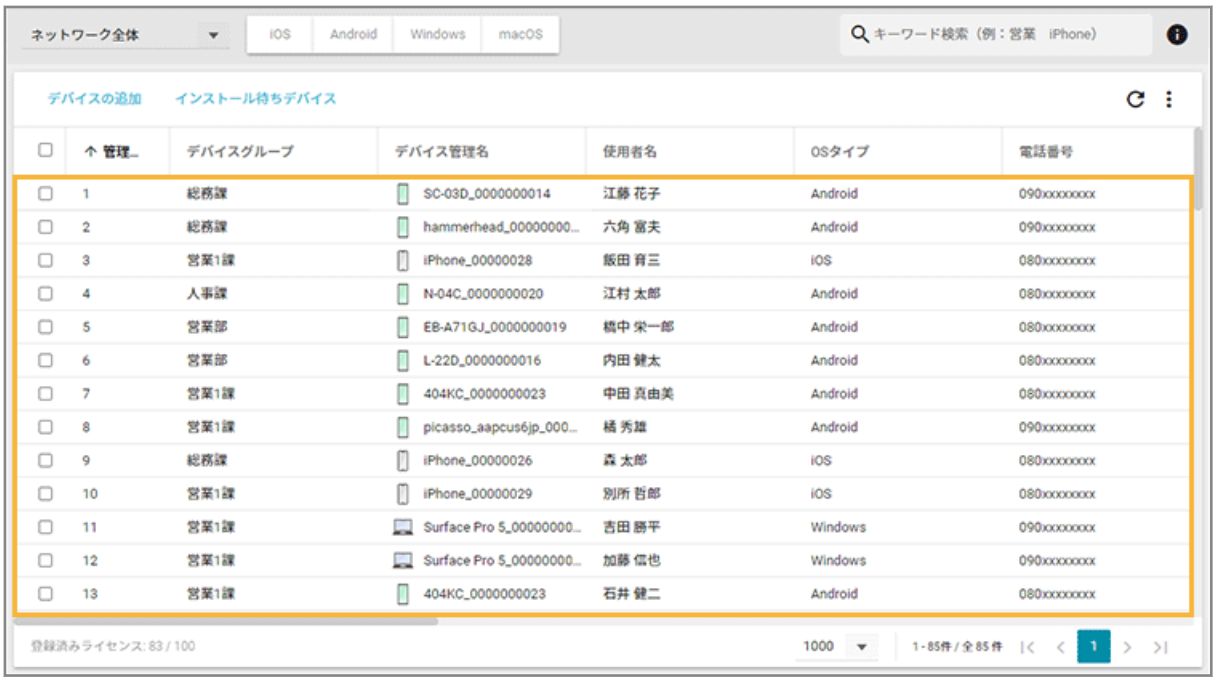
ポイント

管理コンソール上で特定デバイスを表示する場合、おもに「デバイス管理名」と「使用者名」を利用します。そのため、「デバイス管理名」と「使用者名」は、デバイスを特定できる値での登録をおすすめします。

■ デバイス情報を 1 台ずつ編集する

1. **［リスト］の［デバイス］をクリックします。**

2. **デバイスをクリックします。**



3. **［管理情報］の［編集］をクリックします。**

4. 内容を編集し、［保存］をクリックします。

■ デバイス情報を一括で編集する

デバイス情報をエクスポートし、CSV ファイルを編集して、インポートできます。

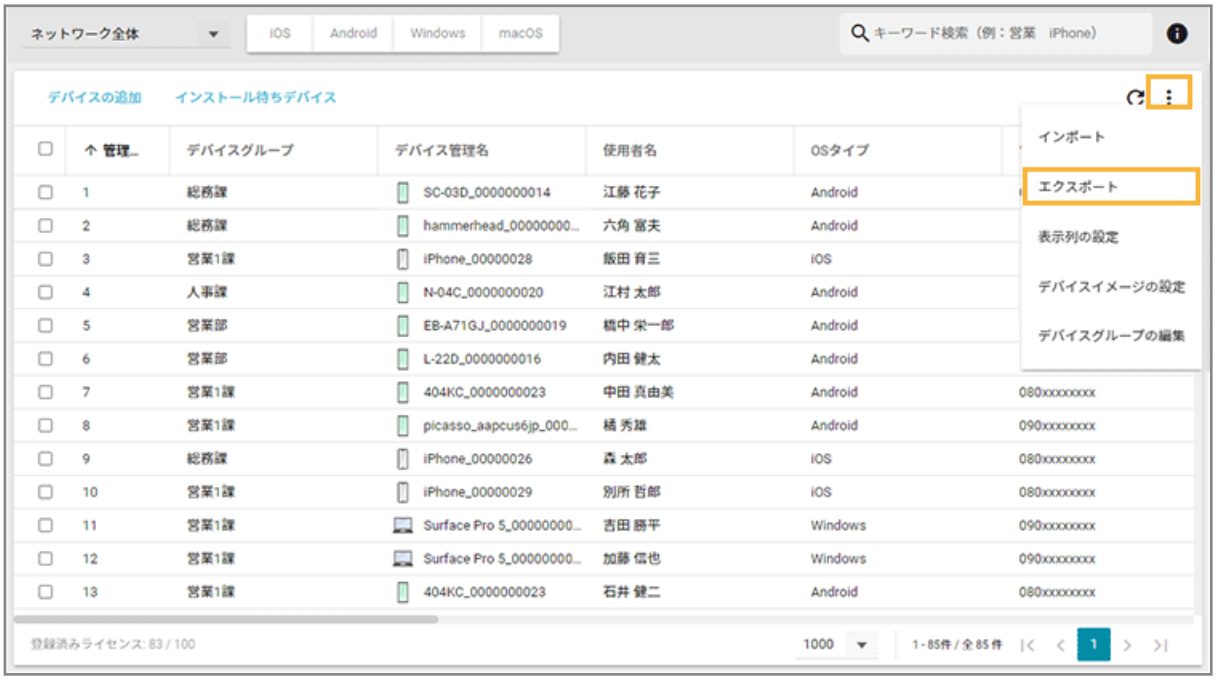
ステップ：

1. デバイス情報をエクスポートする
2. エクスポートしたファイルを編集する
3. 編集したデバイス情報をインポートする

ステップ 1：　デバイス情報をエクスポートする

1. ［リスト］の［デバイス］をクリックします。

2. ⋮ をクリックし、［エクスポート］をクリックします。



3. 管理コンソールに記載の手順に従って設定し、［ダウンロード］をクリックします。

ポイント

エクスポートする項目で、共通の「管理 No.」とデバイス情報の「OS タイプ」は、インポート時にデバイスを紐づけるため、必須項目としてあらかじめチェックされています。

→ CSV ファイルがエクスポートされます。

4. **［閉じる］をクリックします。**

ステップ 2： エクスポートしたファイルを編集する

ポイント

- インポートできるデバイス情報は、「管理情報」と「デバイスグループ」の項目です。
- 「デバイスグループ階層 1」には、ネットワーク全体配下のデバイスグループを入力してください。「デバイスグループ階層 1」が未入力の場合は、自動的にネットワーク全体になります。

注意

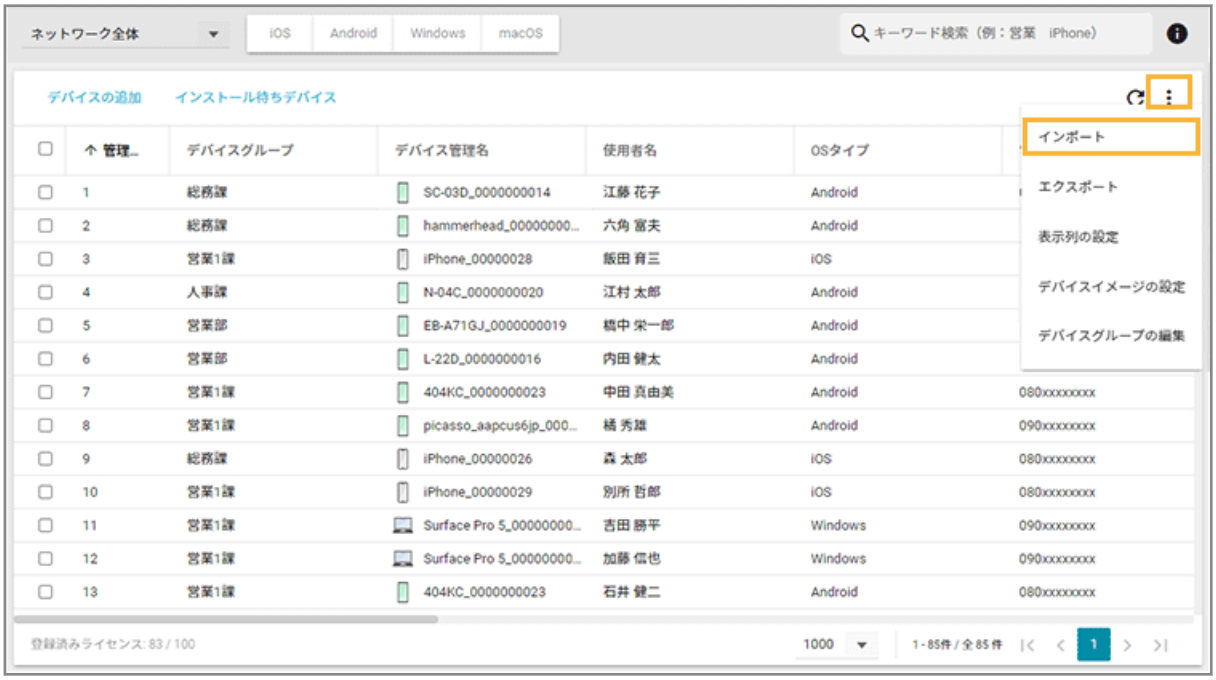
- 「管理 No.」と「OS タイプ」は、インポート時にデバイスの紐づけで必要なため、編集しないでください。
- 項目によっては入力値に制限があります。制限値以外の入力がある場合、インポートに失敗します。

1. **各デバイスの情報を編集し、上書き保存します。**

ステップ 3： 編集したデバイス情報をインポートする

1. **［リスト］の［デバイス］をクリックします。**

2. **⋮ をクリックし、［インポート］をクリックします。**



3. **管理コンソールに記載の手順に従って、インポートします。**

(1) ［ファイルを選択］をクリックし、編集したインポートファイルを選択します。

ファイルの内容が正しく読み込まれない場合は、エンコードを確認します。

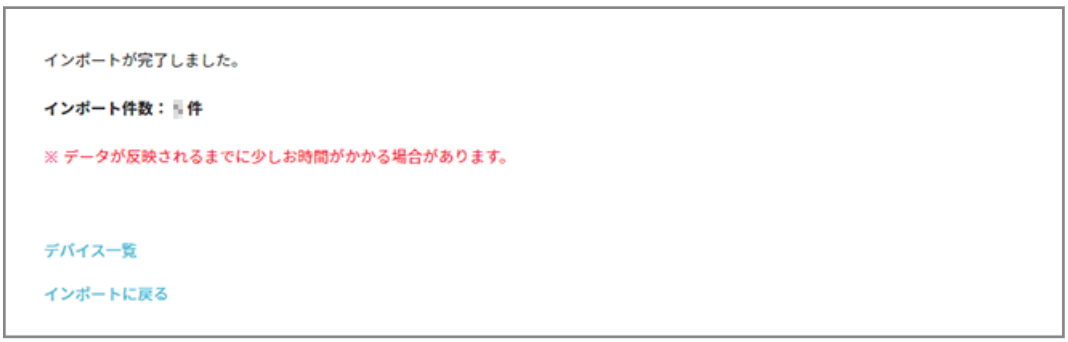
(2) ［自動選択］をクリックします。

→ 「関連づける列名」が自動的に選択されます。

「項目名」と「ファイルの列名」の項目が一致していないと自動的に選択されません。その場合は、対応する項目を 1 つずつ紐づけます。

(3) プレビューを確認し、［インポート］をクリックします。

→「インポート完了」画面が表示されます。



［デバイス一覧］をクリックすると、インポートしたデータを確認できます。

■ デバイス情報を削除する

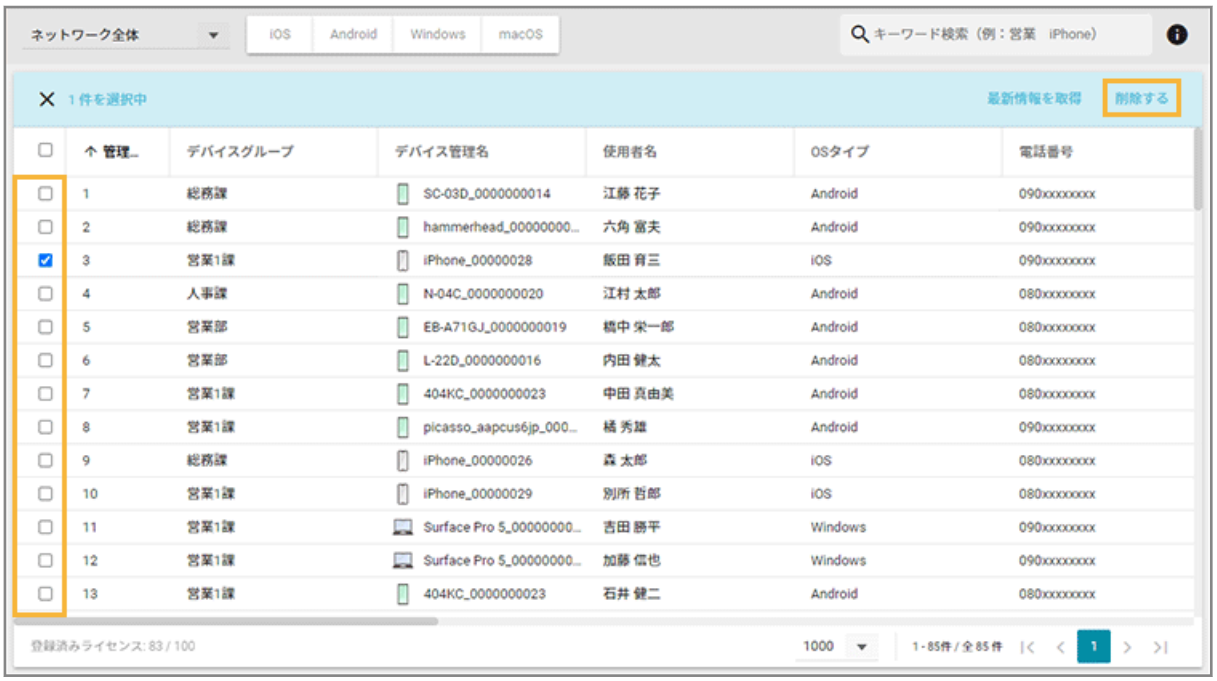
機種変更などで必要なくなったデバイスをエンドポイントマネージャー Free の管理下から外す場合、デバイス情報を削除します。デバイス情報を削除することで、余剰ライセンスができ、新しいデバイスを登録できます。

注意

- デバイスを削除すると、そのデバイスの情報は閲覧できなくなります。
- デバイスを削除しても、デバイスにインストールされている LANSCOPE Client はアンインストールされません。手動でアンインストールしてください。詳細は、 An-337「Free アンインストールガイド」 を参照してください。

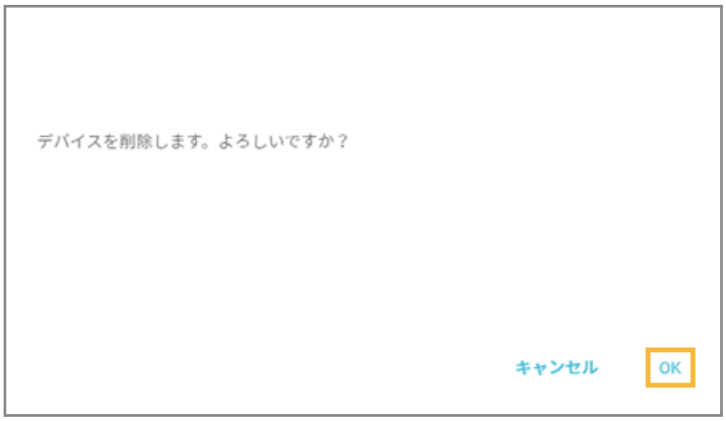
1. ［リスト］の［デバイス］をクリックします。

2. デバイスをチェックし、［削除する］をクリックします。



3. ［OK］をクリックします。

表示される内容は OS タイプによって異なります。



→　デバイスが削除されます。

2-2　リモート操作を実行する

iOS Android Windows macOS

デバイスのロックや初期化など、リモート操作を実行できます。デバイスの紛失時など、情報漏えいなどのセキュリティリスクに備えることができます。

リモート操作一覧

OS によって、実行できるリモート操作や内容は異なります。

OS	リモート操作	内容
iOS	リモートロック	遠隔でロックをかけます。ロック時にデバイス側にメッセージや連絡先（電話番号）を表示できます。
	リモートワイプ	遠隔でデバイスを初期化します。
	パスコードオフ	デバイスに設定されているパスコードロックを解除します。
Android	リモートロック	遠隔で画面ロックをかけます。リモートロック時にパスコードを上書きします。（*1）（*2）
	リモートワイプ	遠隔でデバイスを初期化します。
Windows	リモートロック	遠隔で画面ロックをかけます。
	リモートワイプ（*3）	「BitLocker ドライブ暗号化」機能で暗号化したときに TPM に保存される暗号キーを削除することで、暗号化したデータにアクセスできないようにします。（*4） 回復キーの入力でデータを復元できます。
macOS	リモートロック	遠隔でロックをかけます。
	リモートワイプ	遠隔でデバイスを初期化します。

*1：パスワードが設定済みの場合、ロック解除パスワードの上書き設定はできません。
*2：Android 11 以上のデバイスでは、ロック解除パスワードの設定はできません。
*3：Windows 11 Home／Windows 10 Home には対応していません。
*4：デバイス側で PIN 認証を利用した BitLocker が設定されている場合、リモートワイプはできません。

リモート操作に必要な設定／条件

Android／Windows でのリモート操作には、デバイス側で次の設定が必要です。条件を満たしていない場合、リモート操作はできません。

OS	リモート操作	内容
Android	リモートロック	デバイス管理者に LANSCOPE Client を登録する（*1）
	リモートワイプ	Google Play ストアがインストールされている

OS	リモート操作	内容
Windows	リモートワイプ	TPM が搭載されたデバイスで、BitLocker 機能が有効になっていること (*2)

*1：登録方法は、 An-338「Free 初期設定ガイド for Android」 を参照してください。
*2：BitLocker の設定方法は、 An-341「Free 初期設定ガイド for Windows」 を参照してください。

ポイント

Android／Windows デバイスで条件を満たしていない場合、次のレシピを作成してアラートに設定できます。

トリガー	デバイスの設定がリモート操作の実行条件を満たしていない
アクション	アラートに設定する

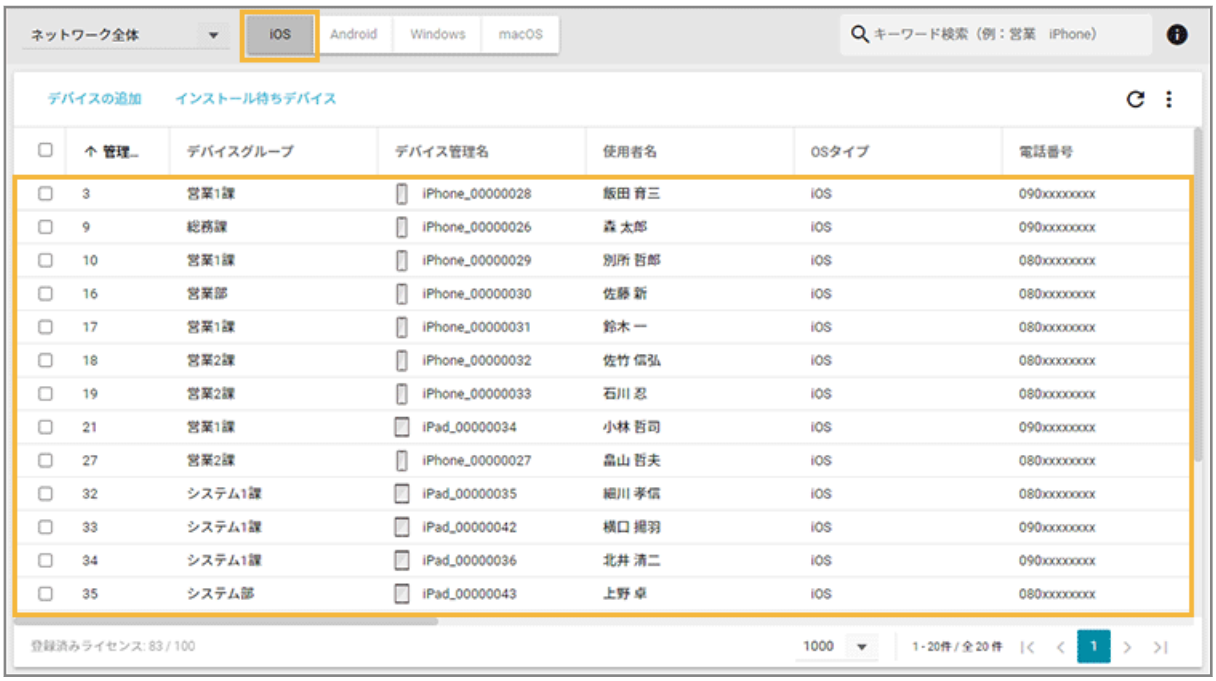
リモート操作を実行する

iOS Android Windows macOS

■ iOS の場合

1. **［リスト］の［デバイス］をクリックします。**

2. **OS をクリックし、デバイスをクリックします。**



3. ［リモート操作］をクリックし、［リモート操作を実行する］をクリックして、リモート操作を選択します。

- リモートロックの場合

  デバイス側にメッセージや連絡先（電話番号）を表示させる場合、「メッセージ」「電話番号」を入力し、［実行］をクリックします。

注意

リモートロック実行時、デバイス側でパスコードの設定をしていない場合、「メッセージ」「電話番号」は表示されません。

- リモートワイプの場合

  ログインしている管理コンソールのアカウントの「ログインパスワード」を入力し、必要に応じて［初期設定時にクイックスタートをスキップする］をチェックして、［実行］をクリックします。

［初期設定時にクイックスタートをスキップする］

チェックすると、初期設定時の「クイックスタート」画面が表示されません。

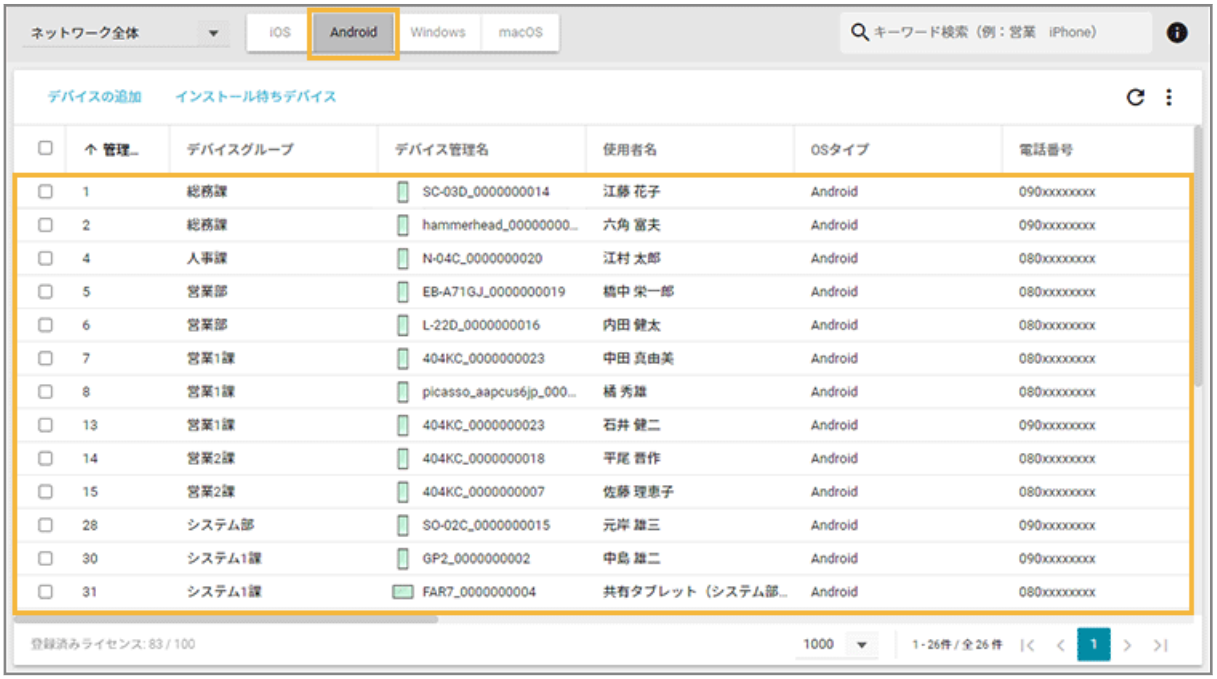
- パスコードオフの場合

  ［実行］をクリックします。

■ Android の場合

1. ［リスト］の［デバイス］をクリックします。

2. OS をクリックし、デバイスをクリックします。



3. ［リモート操作］をクリックし、［リモート操作を実行する］をクリックして、リモート操作を選択します。

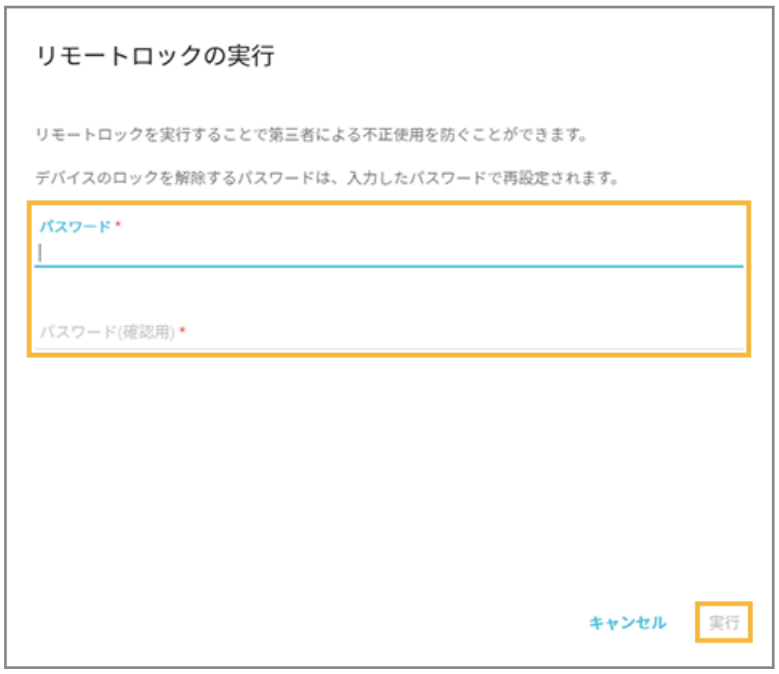
- リモートロックの場合

Android 11 以上の場合

［実行］をクリックします。

Android 11 未満の場合

ロックを解除するための「パスワード」「パスワード（確認用）」を入力し、［実行］をクリックします。



注意

リモートロックを実行するときに、デバイス側でパスワードが設定されていると、ロック解除パスワードを上書き設定できません。

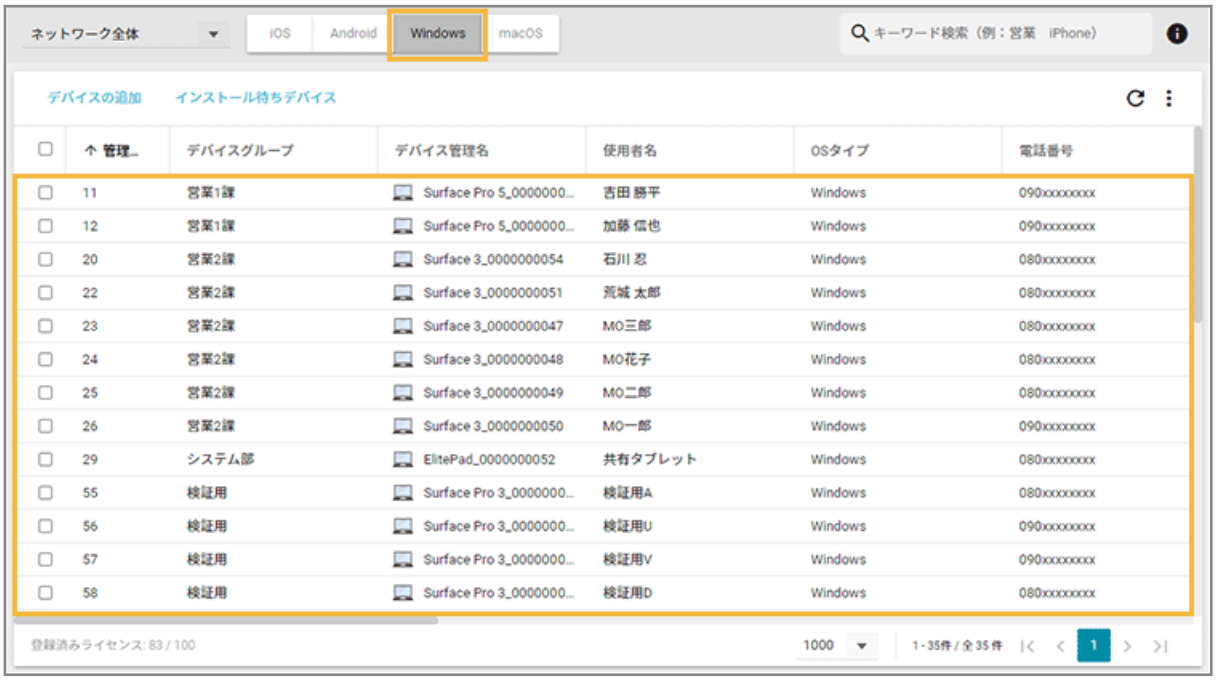
- リモートワイプの場合

  ログインしている管理コンソールのアカウントの「ログインパスワード」を入力し、[実行]をクリックします。

■ Windows の場合

1. **［リスト］の［デバイス］をクリックします。**

2. **OS をクリックし、デバイスをクリックします。**



3. **［リモート操作］をクリックし、［リモート操作を実行する］をクリックして、リモート操作を選択します。**

- リモートロックの場合

  ［実行］をクリックします。

- リモートワイプの場合

  ログインしている管理コンソールのアカウントの「ログインパスワード」を入力し、［実行］をクリックします。

Windows のリモートワイプ実行後の復旧方法

Windows のリモートワイプ実行後、デバイスを復旧する手順です。機種や OS バージョンにより、画面や手順が異なる場合があります。

注意

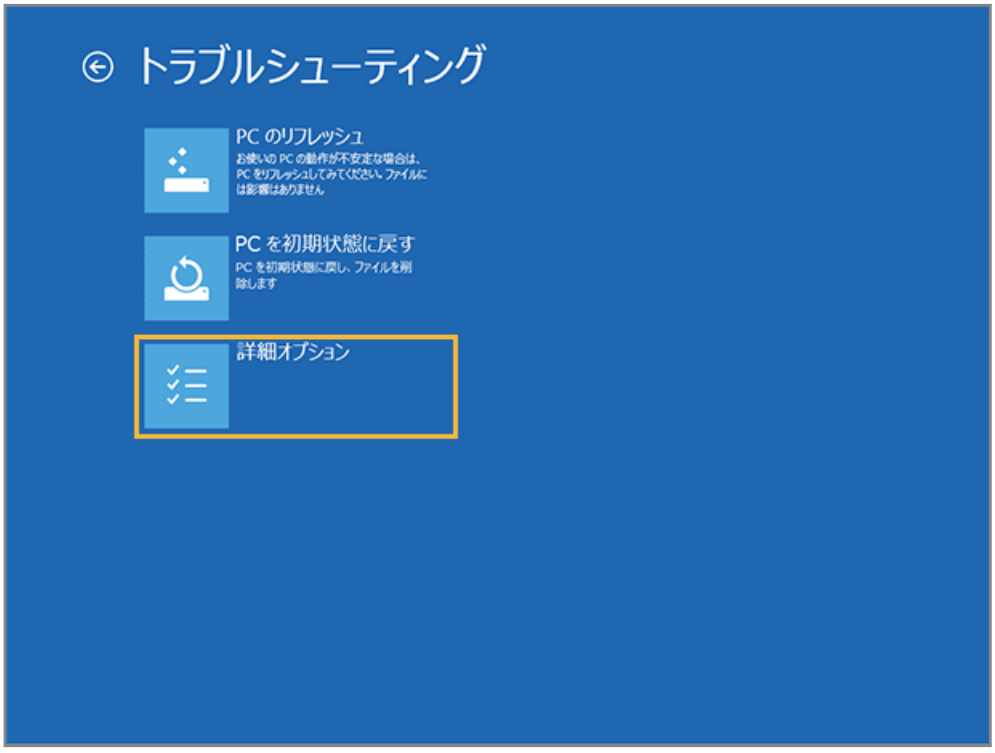
本手順の実行で「BitLocker 暗号化」が解除されます。再度、リモートワイプを実行するには、BitLocker の再設定が必要です。

BitLocker の設定は、 An-341「Free 初期設定ガイド for Windows」 を参照してください。

1. **デバイスの電源を入れると、次の画面が表示されます。保存していたパスワード（回復キー）を入力し、［Enter］キーを押します。**

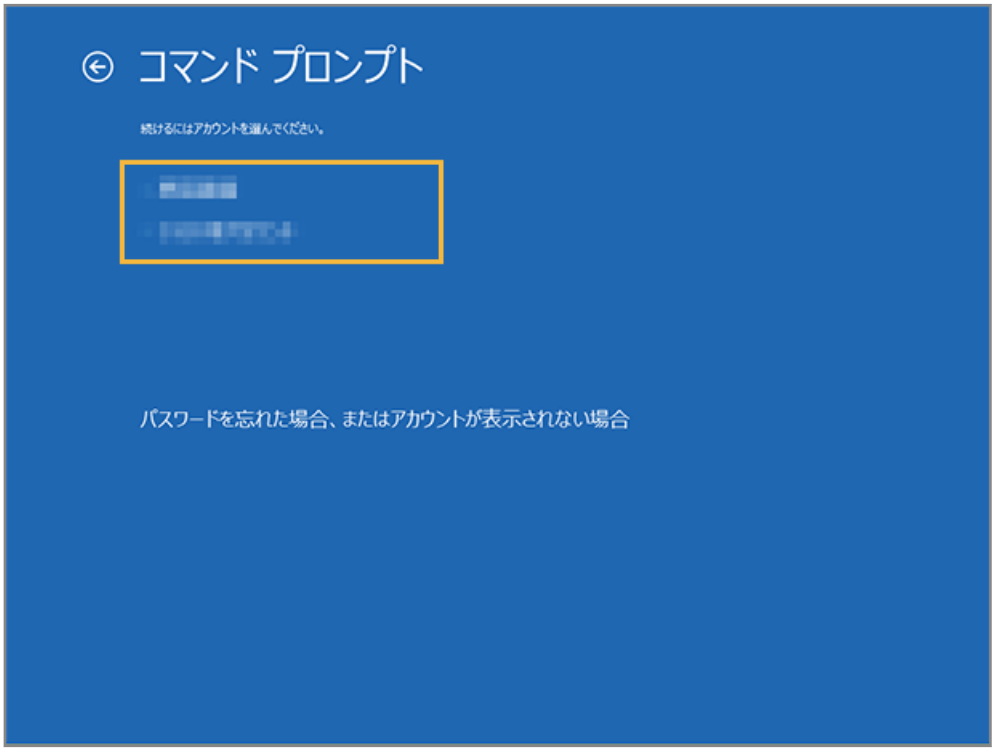
2. **［トラブルシューティング］をクリックします。**

3. ［詳細オプション］をクリックします。

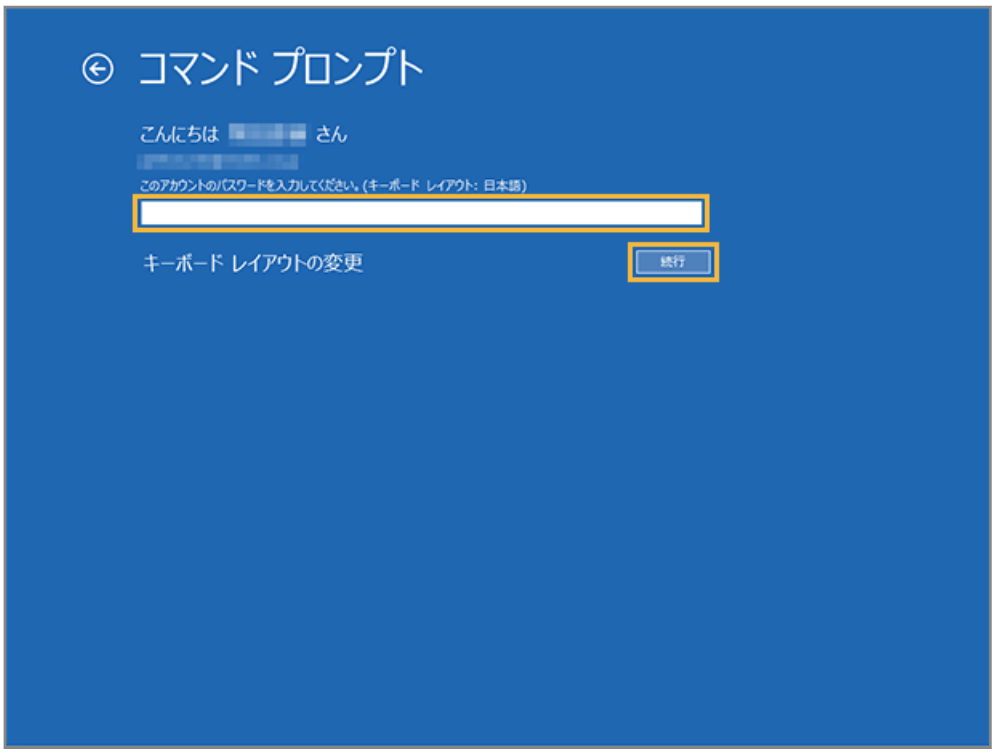


4. ［コマンドプロンプト］をクリックします。

5. 起動するアカウントを選択します。



6. ログインパスワードを入力し、［続行］をクリックします。



→ コマンドプロンプトが起動します。

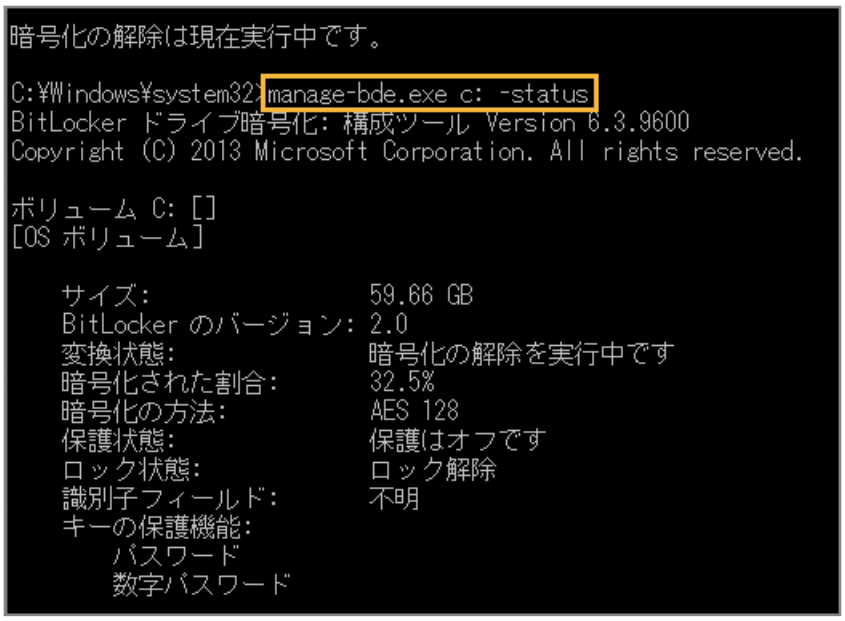
7. コマンドラインに次のコマンドを入力し、[Enter] キーを押します。

```
manage-bde.exe c: -off
```

→ 回復処理が開始されます。

8. コマンドラインに次のコマンドを入力し、[Enter] キーを押します。

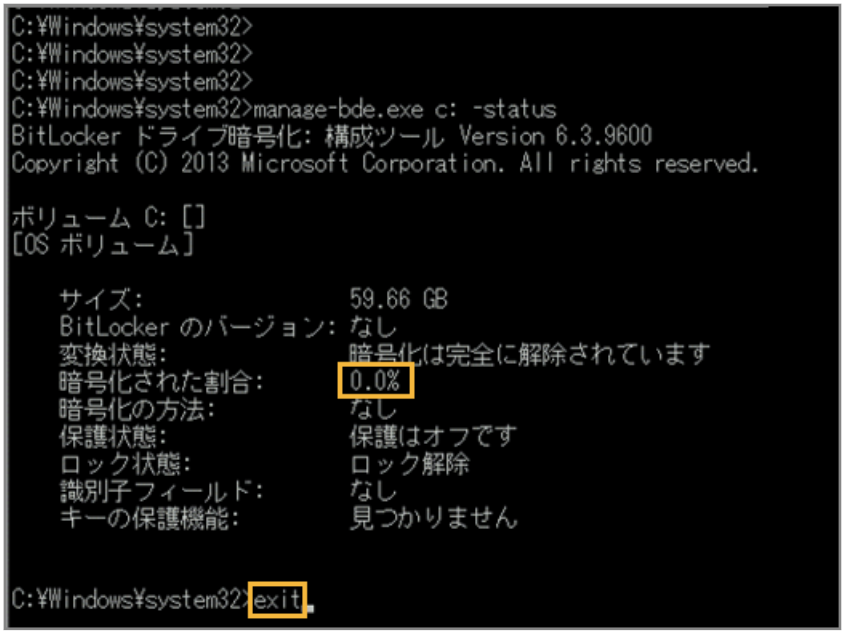
```
manage-bde.exe c: -status
```



→ コマンド実行時に表示される「暗号化された割合」を確認し、0%になるまで待機します（約 10 分程度かかります）。

9. コマンドラインに次のコマンドを入力し、[Enter] キーを押します。

```
exit
```



→ コマンドプロンプトが終了します。

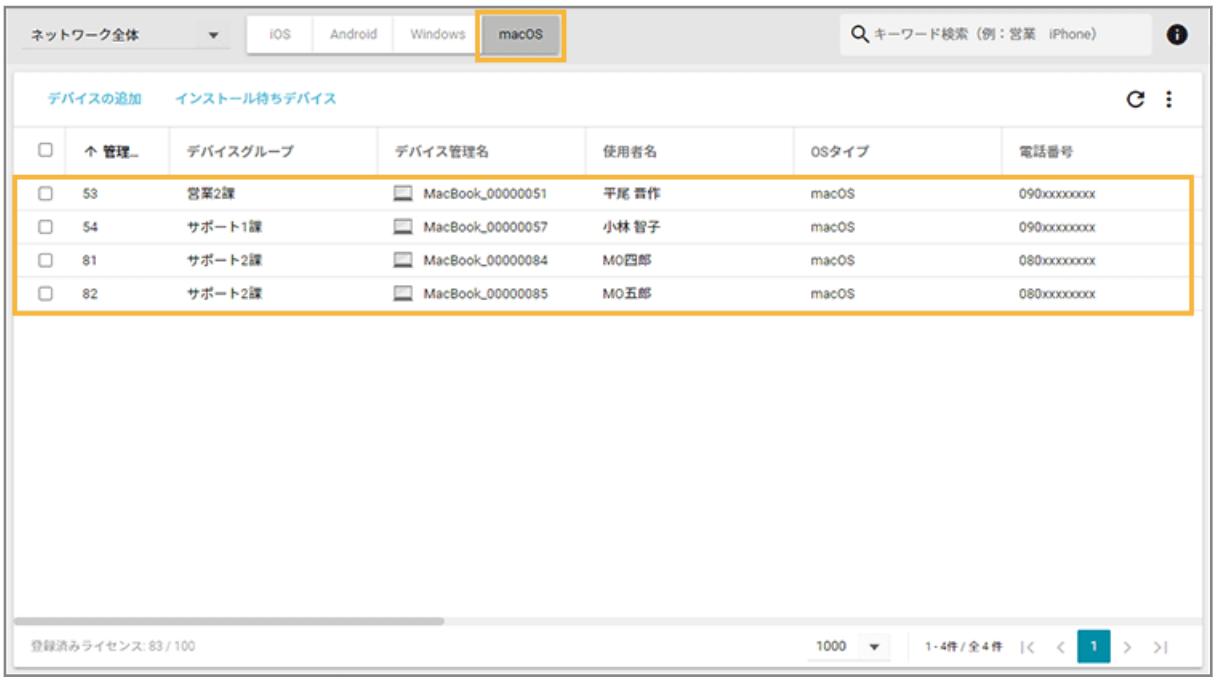
10. [続行] をクリックします。

→ デバイス復旧が完了します。

■ macOS の場合

1. **［リスト］の［デバイス］をクリックします。**

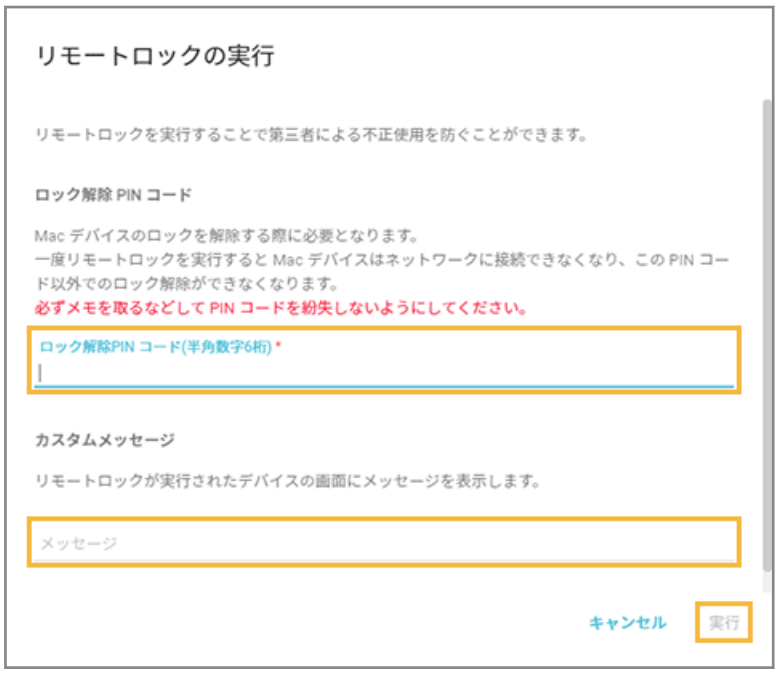
2. **OS をクリックし、デバイスをクリックします。**



3. ［リモート操作］をクリックし、［リモート操作を実行する］をクリックして、リモート操作を選択します。

- リモートロックの場合

  「ロック解除 PIN コード」が表示されている場合は PIN コードを入力し、必要に応じてロック画面に表示するメッセージを入力して、［実行］をクリックします。



- リモートワイプの場合

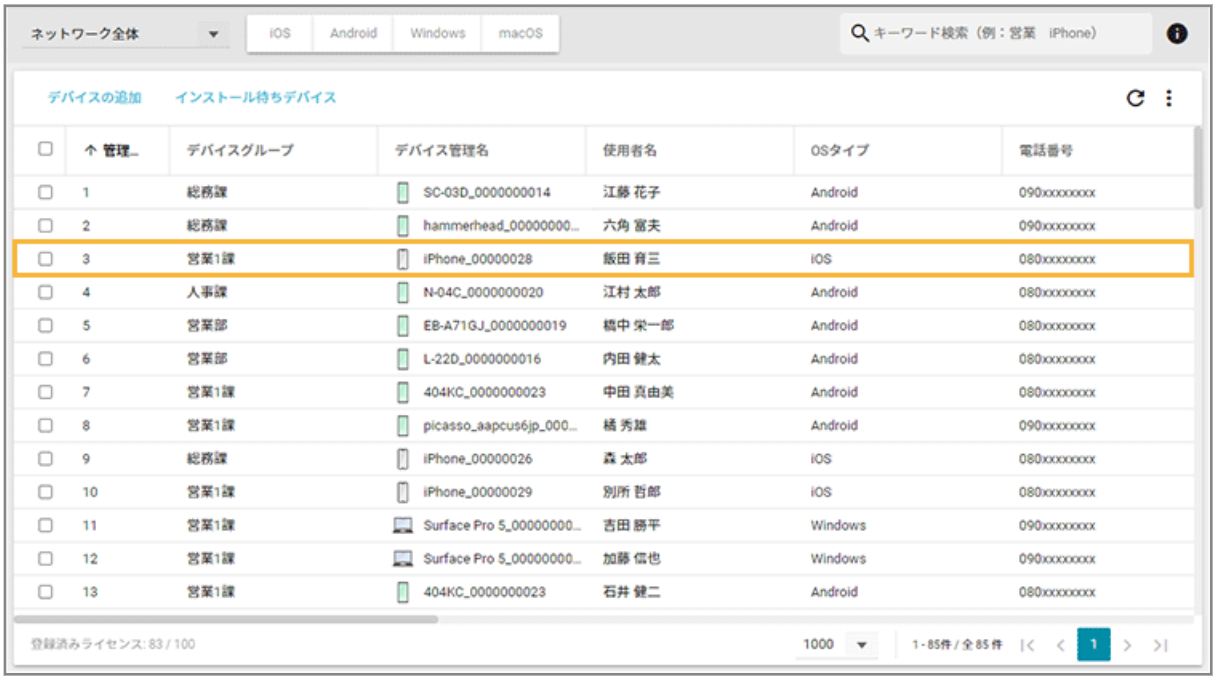
  リモートワイプ後、「ロック解除 PIN コード」が表示されている場合は PIN コードを入力し、ログインしている管理コンソールのアカウントの「ログインパスワード」を入力して、［実行］をクリックします。

リモート操作の実行結果を確認する

iOS Android Windows macOS

1. **［リスト］の［デバイス］をクリックします。**

2. **デバイスをクリックします。**



3. **［リモート操作］をクリックし、「実行履歴」を確認します。**

実行履歴の状態	詳細
待機中	デバイスが通信できる状態になるとリモート操作を実行します。
	リモート操作のキャンセルに失敗しました。
実行中	リモート操作を実行中です。
成功	（リモートロックの場合）デバイスをロックしました。(*)
	（リモートワイプの場合）デバイスのすべてのデータを初期化しました。(*)
	（パスコードオフの場合）デバイスのパスコードをオフにしました。
キャンセル中	リモート操作をキャンセル中です。
キャンセル	リモート操作をキャンセルしました。
リジェクト	別のリモート操作が設定されたため、この操作はリジェクトされました。
失敗	リモート操作の実行に失敗しました。
	リモート操作の実行がタイムアウトしました。

*：キャンセル操作をしても、キャンセル前に実行された場合は、詳細に「キャンセル操作が実行されましたが、すでにデバイスのリモートロック（またはワイプ）操作が完了しました。」と表示されます。

■ トラブルシューティング

デバイスが次の状態の場合、リモート操作が成功しません。デバイス側の設定を確認してください。

OS	デバイスの状態	実行履歴の状態	対処方法
共通	ネットワークに繋がっていない 圏外になっている	待機中	ネットワークに接続してください。 次にネットワークに接続されたタイミングで実行されます。
iOS	MDM 構成プロファイルがインストールされていない	待機中	MDM 構成プロファイルをインストールしてください。(*)
Android	LANSCOPE Client がインストールされていない	待機中	LANSCOPE Client をインストールしてください。(*)
	「デバイス管理者」に LANSCOPE Client が登録されていない	失敗	「デバイス管理者」に LANSCOPE Client を登録してください。(*)
Windows	LANSCOPE Client がインストールされていない	待機中	LANSCOPE Client をインストールしてください。(*)
macOS	MDM 構成プロファイルがインストールされていない	待機中	MDM 構成プロファイルをインストールしてください。(*)

*：設定方法は、各 OS の初期設定ガイドを参照してください。

- An-339「Free 初期設定ガイド for iOS／iPadOS」
- An-338「Free 初期設定ガイド for Android」
- An-341「Free 初期設定ガイド for Windows」
- An-340「Free 初期設定ガイド for macOS」

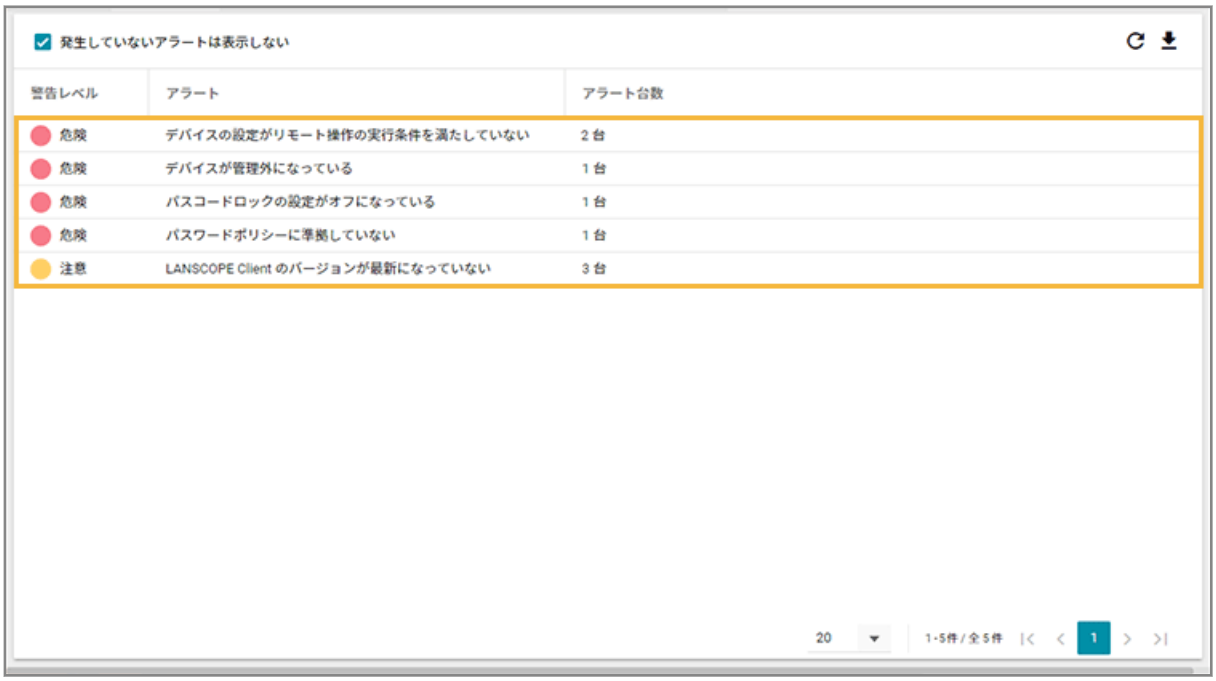
2-3　アラート情報を確認する

iOS Android Windows macOS

「どのアラート」が「どのデバイス」で発生しているかを確認できます。

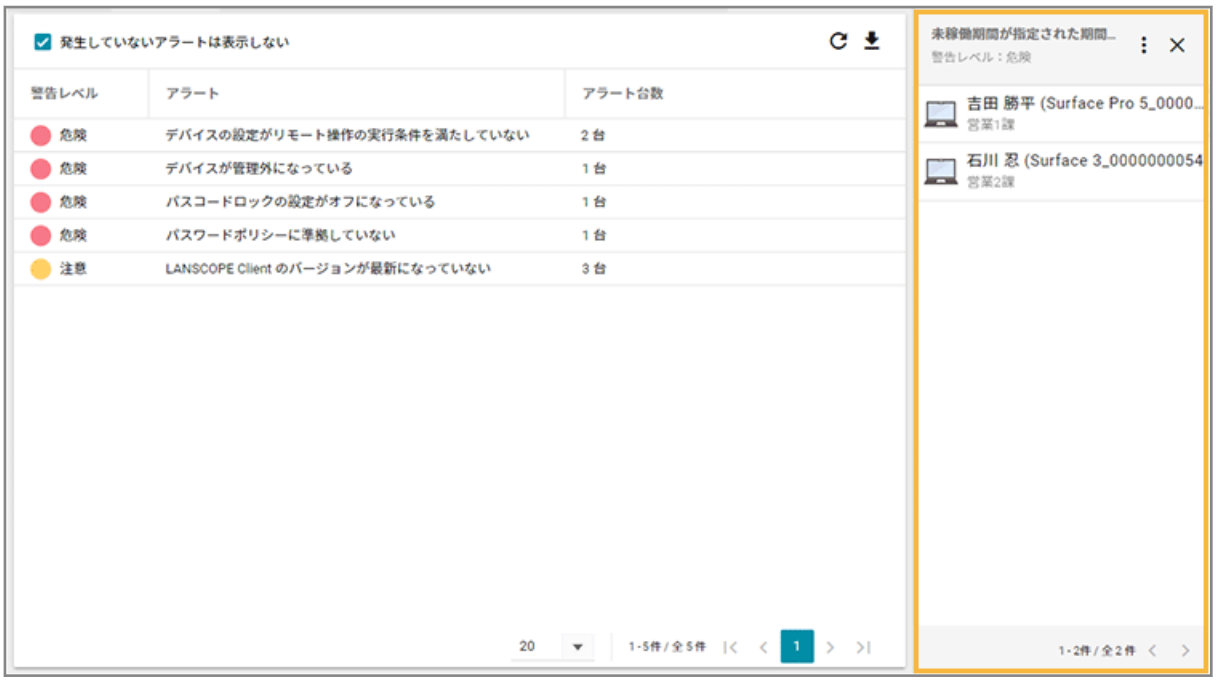
1. **［リスト］の［アラート］をクリックします。**

2. **アラートをクリックします。**



→　選択したアラートを発生しているデバイスが、画面右側に一覧表示されます。

3. **デバイスをクリックします。**



→ 「デバイス詳細」画面の「アラート」が表示されます。

4. デバイスで発生しているアラートを確認します。

第 3 章　レシピで操作を自動実行する

iOS Android Windows macOS

設定した条件に一致したデバイスに対し、アプリやメッセージ配信など指定したアクションを自動実行します。このトリガーとアクションの組み合わせを、レシピとして登録します。

エンドポイントマネージャー Free では、「アラート設定」だけを利用できます。

レシピの利用で、管理者が都度操作を実行する必要がありません。

設定できるトリガー／アクションは、レシピを作成する画面の［トリガー選択］［アクション選択］の一覧で確認できます。OS によって、設定できるトリガー／アクションは異なります。

登録済みのレシピ

レシピ名	内容	iOS	Android	Windows	macOS
管理外アラート	管理外になっている場合にアラート（危険）にします。（*1）	○	×	○	○
パスワードポリシー非準拠アラート	エンドポイントマネージャー Free で設定しているパスワードポリシーの条件に、準拠していない場合にアラート（危険）にします。（*2）	○	○	×	×
LANSCOPE Client 未更新アラート	LANSCOPE Client のバージョンが古い場合にアラート（注意）にします。	○（*3）	○	○	○
パスコードロックオフアラート	デバイス側でパスコードが設定されていない場合にアラート（危険）にします。	○	×	×	×
リモート実行無効アラート	リモート実行に必要な設定がされていない場合にアラート（危険）にします。	×	○	○	×

*1：iOS／macOS は「MDM 構成プロファイル」、Windows は「LANSCOPE Client」がアンインストールされた場合に発生します。ただし、iOS／Windows／macOS は、LANSCOPE Free サーバーと通信が取れていない場合、アラートは発生しません。

*2：［ルール］＞［デバイス設定］＞［基本設定］でパスワードポリシーの設定が必要です。詳細は、取得する情報を設定するを参照してください。

*3：iOS の場合、LANSCOPE Client のインストールは不要のため、設定は必要ありません。

3-1　レシピ一覧を管理する

iOS Android Windows macOS

- レシピを作成する
- レシピの有効／無効を設定する
- レシピの実行履歴を確認する
- レシピを編集／削除する

レシピを作成する

iOS Android Windows macOS

自動化したい業務がある場合、トリガーとアクションを組み合わせてレシピを作成します。トリガーとは、アクションを実行するきっかけになる条件です。

ここでは、管理外のデバイス検知をアラートにする場合を例に説明します。

1. **［レシピ］の［レシピ一覧］をクリックします。**

2. **［レシピの追加］をクリックします。**

3. **「レシピ名」を入力し、［トリガー選択］をクリックします。**

4. トリガーを選択します。ここでは、［デバイスが管理外になっている］をクリックします。

5. レシピを実行する対象を選択します。ここでは、「デバイスグループ」を選択します。

(1) 「デバイスグループ」の［選択］をクリックします。

ポイント

レシピを実行する対象は、「デバイスグループ」「デバイス」、それぞれで設定できます。

(2) 実行対象にするデバイスグループをチェックし、［選択］をクリックします。

6. ［アクション追加］をクリックします。

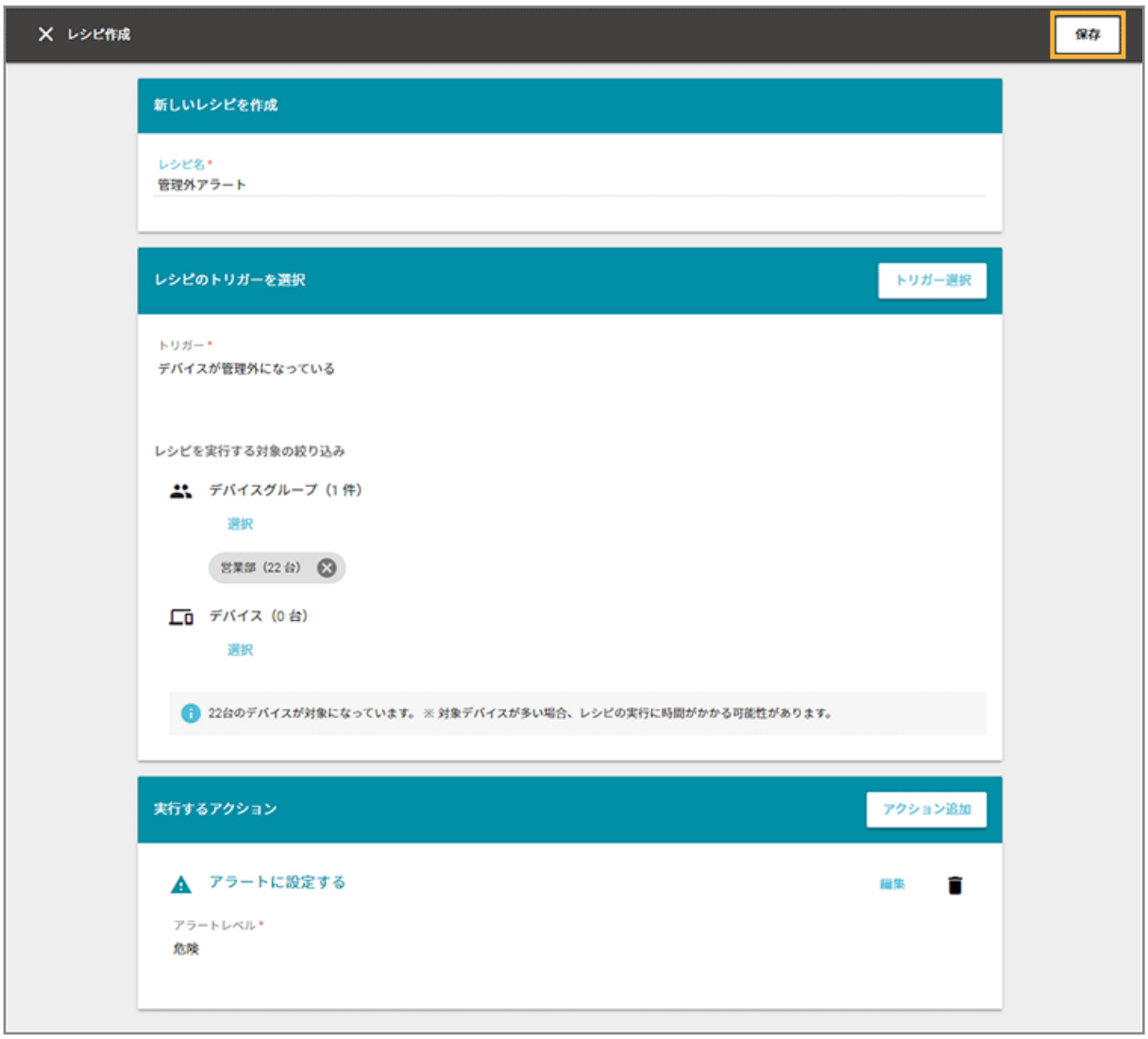
7. ［アラートに設定する］をクリックします。

8. アラートレベルを選択し、［設定］をクリックします。

注意

アラートレベルは「危険」「注意」を選択してください。「警告なし」を選択すると、アラートは設定されません。

9. 内容を確認し、［保存］をクリックします。



→ レシピが作成されます。

レシピの有効／無効を設定する

iOS Android Windows macOS

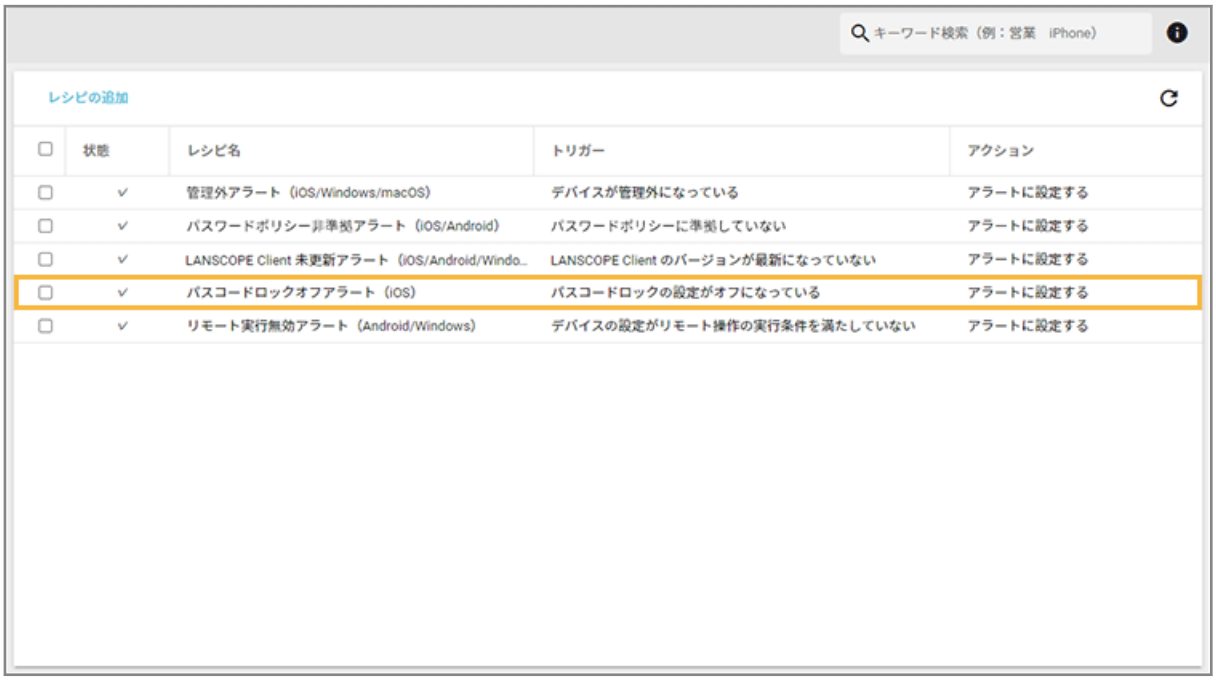
レシピの作成時点では「有効」に設定されます。作成したレシピを利用しない場合、レシピを「無効」にして実行させない設定ができます。

「有効」「無効」の表示は、次のとおりです。

「レシピ一覧」画面の「状態」列	設定アイコン	内容
✓		（有効）トリガーが発生すると、レシピが実行されます。
（空欄）		（無効）トリガーが発生しても、レシピは実行されません。

1. **［レシピ］の［レシピ一覧］をクリックします。**

2. **レシピをクリックします。**



3. **「このレシピを有効にする」を に切り替えます。**

→「レシピを無効にしました。」と表示されます。

4. **をクリックし、「レシピ一覧」画面に戻ります。**

5. **「状態」列の ✓ が消えて、空欄になったことを確認します。**

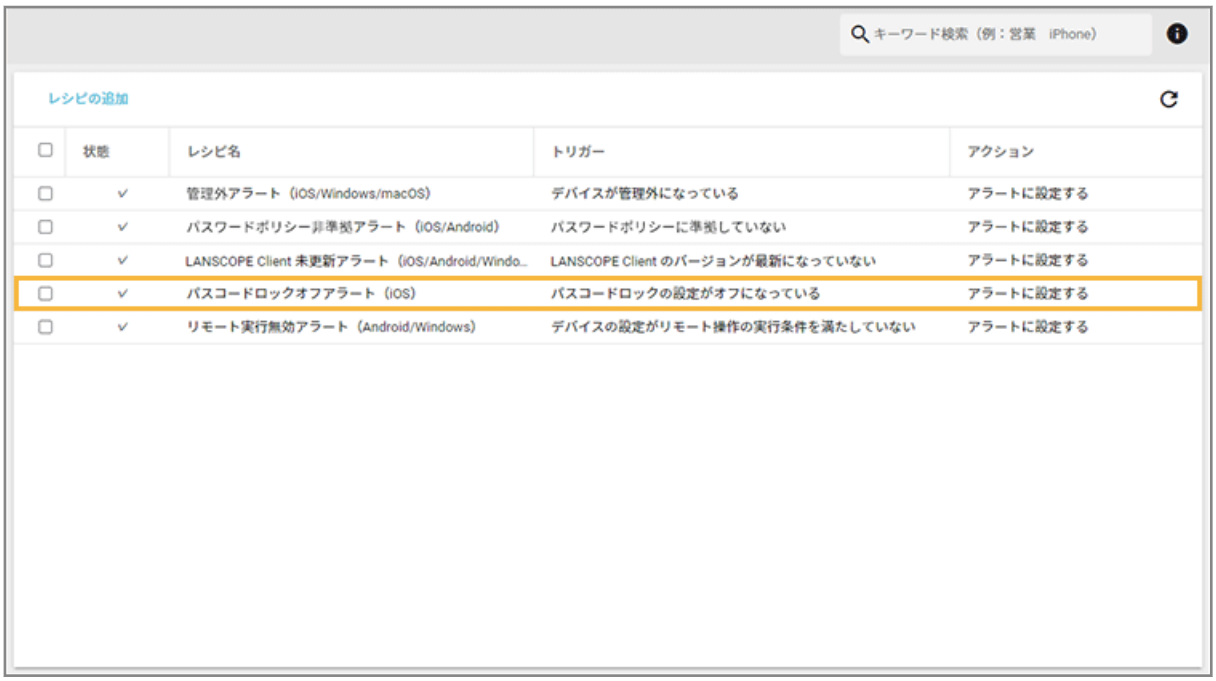
レシピの実行履歴を確認する

iOS Android Windows macOS

レシピが実行された日時を確認できます。

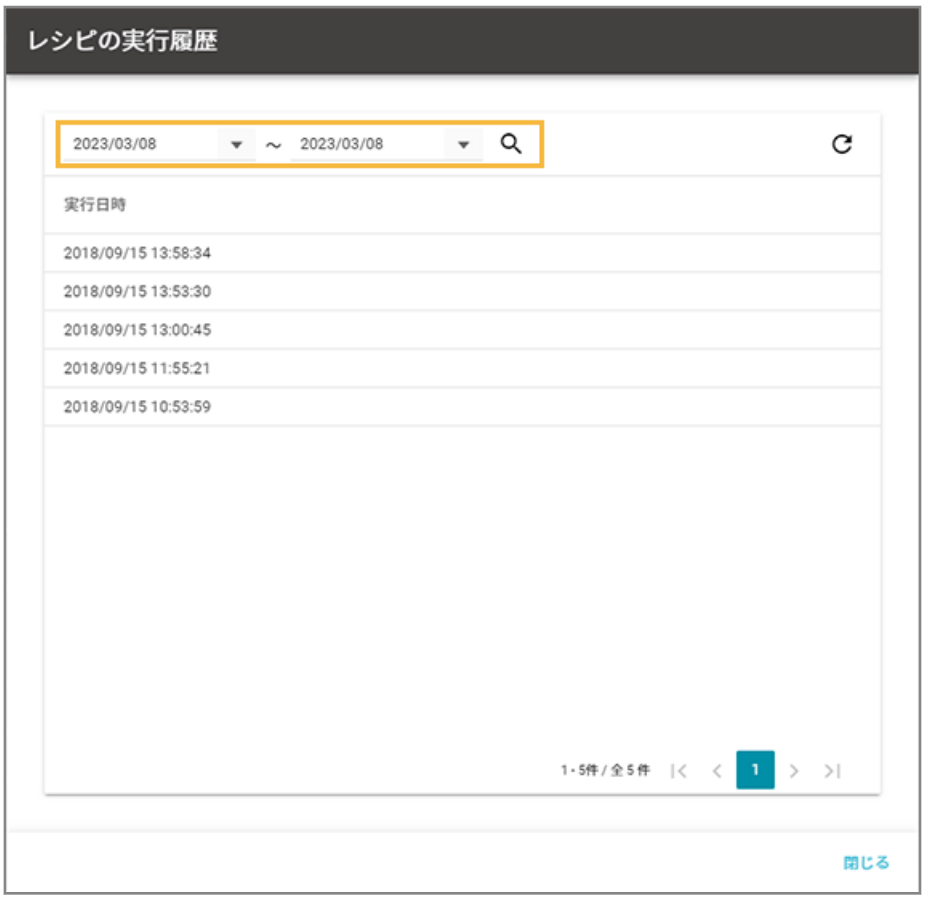
1. **［レシピ］の［レシピ一覧］をクリックします。**

2. **レシピをクリックします。**



3. ［すべての実行履歴を確認する］をクリックします。

4. 実行履歴を表示する期間を設定し、 をクリックします。



→ レシピが実行された日時が、実行されたデバイスの数だけ、表示されます。

レシピを編集／削除する

iOS Android Windows macOS

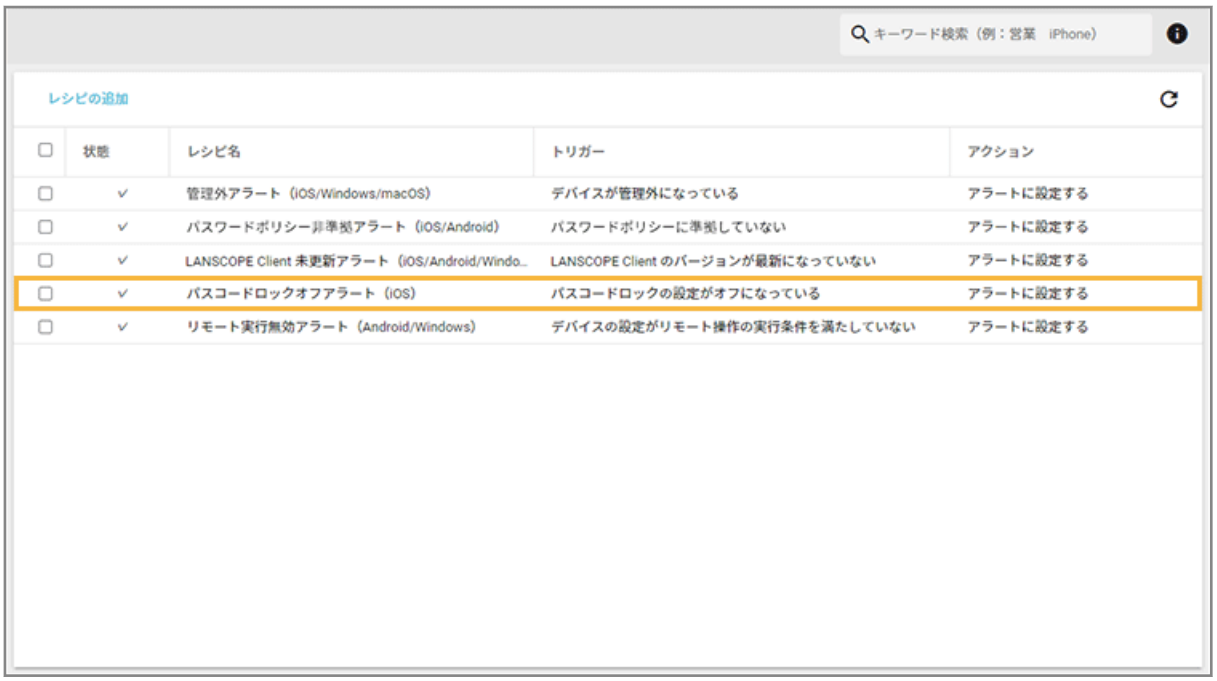
■ レシピを編集する

作成したレシピや登録済みのレシピを編集できます。

ここでは、実行するアクションのアラートレベル［危険］を［注意］に変更します。

1. **［レシピ］の［レシピ一覧］をクリックします。**

2. **レシピをクリックします。**



3. ［編集］をクリックします。

4. 実行するアクション欄の［編集］をクリックします。

5. アラートレベルを［注意］に変更し、［設定］をクリックします。

注意

アラートレベルは「危険」「注意」を選択してください。「警告なし」を選択すると、アラートは設定されません。

→ 「レシピ作成」画面に戻ります。

6. **［保存］をクリックします。**

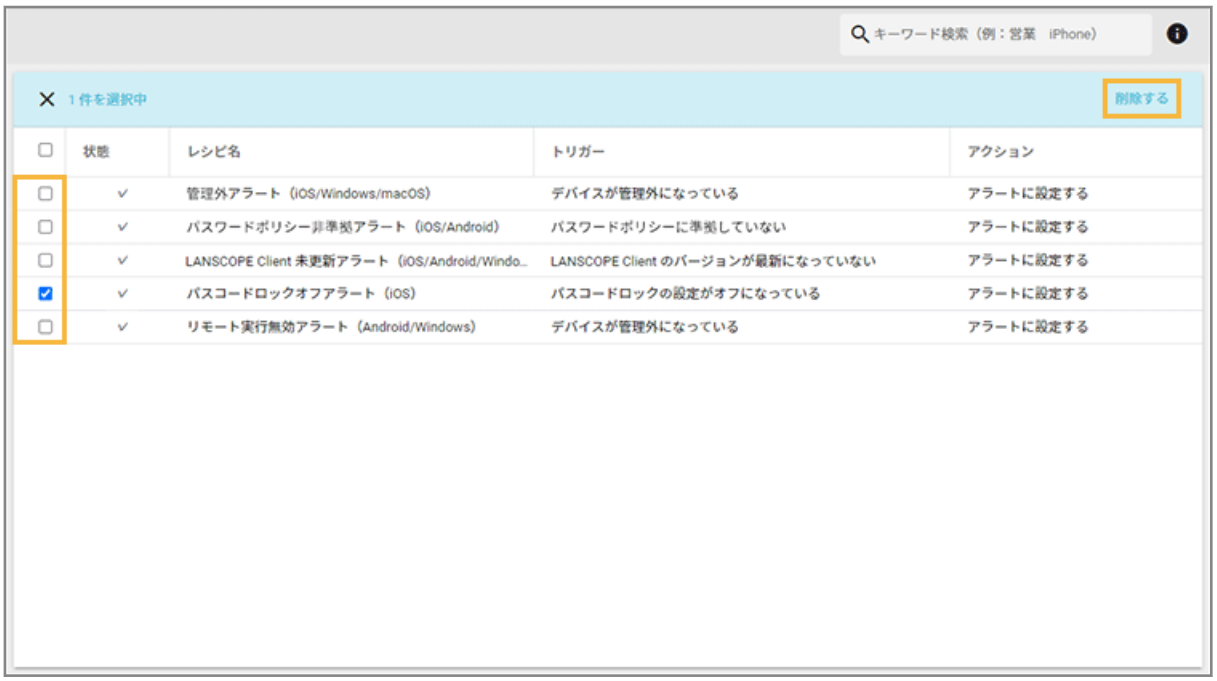
→ 「レシピの更新に成功しました。」と表示され、「レシピ一覧」画面に戻ります。

■ レシピを削除する

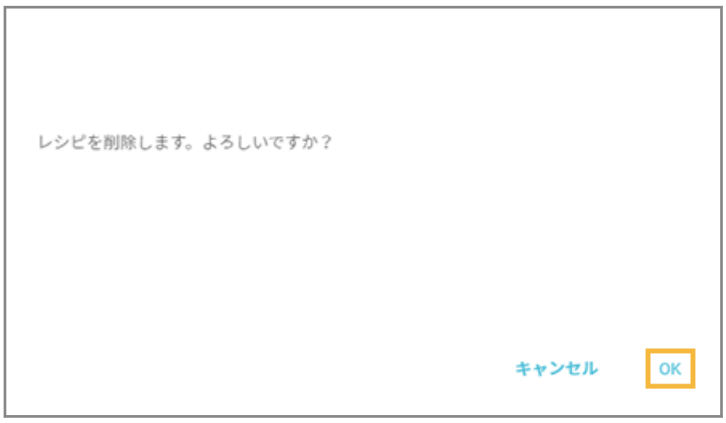
作成したレシピや登録済みのレシピを削除できます。

1. **［レシピ］の［レシピ一覧］をクリックします。**

2. **レシピをチェックし、［削除する］をクリックします。**



3. ［OK］をクリックします。



→　レシピが削除されます。

第 4 章　ルール設定をする

iOS Android Windows macOS

エンドポイントマネージャー Free を利用／運用するために必要な設定ができます。

- 4-1 デバイス設定をする

  エンドポイントマネージャー Free を利用／運用するためのデバイス設定をします。

- 4-2 MDM 証明書を管理する

  iOS／macOS デバイスの管理に必要な MDM 証明書の設定をします。

4-1　デバイス設定をする

iOS Android Windows macOS

エンドポイントマネージャー Free を利用／運用するためのデバイス設定をします。

- グループを管理する
- 取得する情報を設定する

基本設定

次の設定を確認／作成できます。

設定	iOS	Android	Windows	macOS
メモ	○	○	○	○
LANSCOPE Client アップデート設定	―	―	―	○
デバイス表示設定（*1）（*2）	○	―	―	―
アンインストール防止設定	―	―	○	○
パスワードポリシー設定	○	○（*3）	―	○

*1：位置情報を使用しているときのステータスバー表示の設定です。
*2：LANSCOPE Client はデバイス情報取得のために常に起動し、定期的に位置情報を使用しています。

位置情報使用中は、デバイスにステータスバーが表示されます。ステータスバーを非表示に設定した場合、精度が高い位置情報の取得処理が実行されるため、デバイスのバッテリー駆動時間が短くなる可能性があります。

*3：Android 10 以上のデバイスには適用されません。

グループを管理する

iOS Android Windows macOS

グループを設定すると、グループごとに「基本設定」「レシピ作成」ができます。

■ グループを設定する

グループは 5 階層まで作成できます。

グループを手動で設定する

1. **［ルール］の［デバイス設定］>［デバイスグループ設定］をクリックします。**

2. **設定するデバイスグループの上位階層のデバイスグループをクリックし、［追加］をクリックします。**

→ 選択した階層の下に「新しいデバイスグループ」が追加されます。

3. 「新しいデバイスグループ」をダブルクリックし、「デバイスグループ名」と「グループコード」を入力します。

注意

- グループコードには、一意の値を入力してください。
- 入力できる文字の種類に制限はありません（英字／数字／漢字／ひらがな／カタカナ可）。
- 入力できる文字数は、100 文字以内です。

4. **［保存］をクリックします。**

グループを一括で設定する

1. **［ルール］の［デバイス設定］>［デバイスグループ設定］をクリックします。**

2. **⋮ をクリックし、［エクスポート］をクリックします。**

→ CSV ファイルがエクスポートされます。

3. エクスポートしたファイルを編集し、インポートファイルを作成します。

- 「グループ名」「グループコード」「上位グループコード」を入力します。
- 「上位グループコード」が未記入の場合、1 階層目に設定されます。

注意

- グループコードには、一意の値を入力してください。
- 入力できる文字の種類に制限はありません（英字／数字／漢字／ひらがな／カタカナ可）。
- 入力できる文字数は、100 文字以内です。

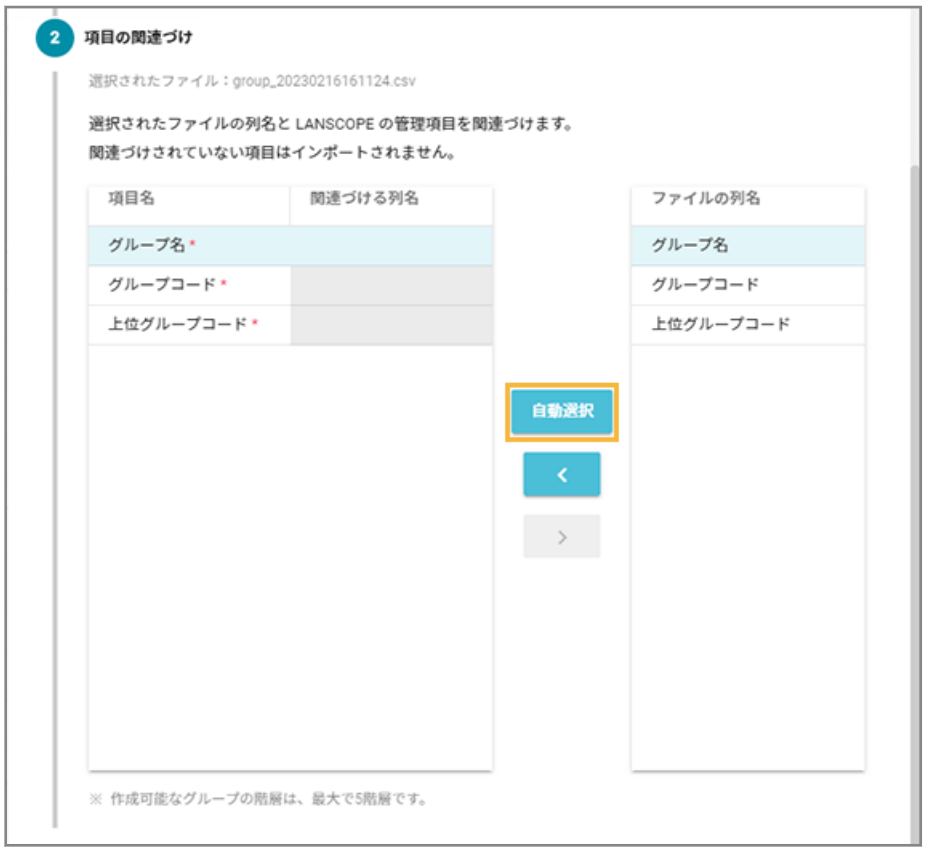
4. ⋮ をクリックし、[インポート] をクリックします。

5. 管理コンソールに記載の手順に従って、インポートします。

(1) ［ファイルを選択］をクリックし、作成したインポートファイルを選択します。

ファイルの内容が正しく読み込まれない場合は、エンコードを確認します。

(2) ［自動選択］をクリックします。



→ 「関連づける列名」が自動的に選択されます。

「項目名」と「ファイルの列名」の項目が一致していないと自動的に選択されません。その場合は、対応する項目を 1 つずつ紐づけます。

(3) インポートファイルに記載されていないグループを管理コンソールから削除する場合は、チェックします。

(4) ［インポート］をクリックします。

→ インポートが完了します。

6. 内容を確認し、［保存］をクリックします。

■ グループを編集する

1. **［ルール］の［デバイス設定］>［デバイスグループ設定］をクリックします。**

2. **デバイスグループ名とグループコードを変更する場合、デバイスグループをダブルクリックします。**

3. **デバイスグループの階層を移動する場合、デバイスグループをドラッグアンドドロップします。**

4. **［保存］をクリックします。**

■ グループを削除する

ポイント

削除したデバイスグループに紐づくデバイスは、「ネットワーク全体」に紐づきます。

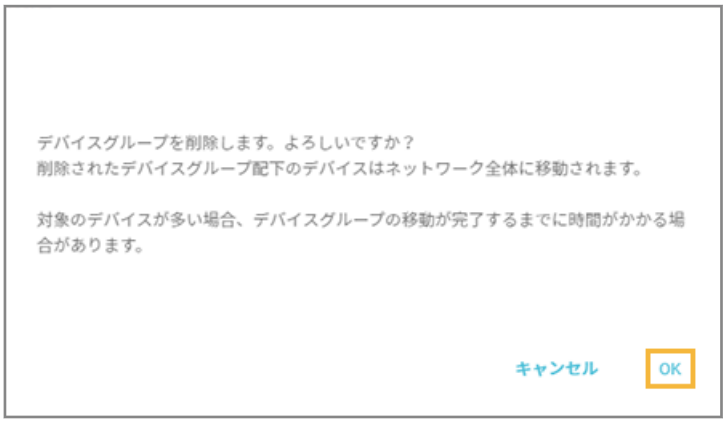
1. **［ルール］の［デバイス設定］>［デバイスグループ設定］をクリックします。**

2. **デバイスグループをクリックし、［削除］をクリックします。**

注意

選択したデバイスグループに紐づく下位のグループも削除されます。

3. **確認し、「OK」をクリックします。**



→ 「デバイスグループ編集」画面に戻ります。

4. **［保存］をクリックします。**

取得する情報を設定する

iOS Android Windows macOS

各 OS ごとに取得する情報や、パスワードポリシーなどを設定します。グループごとに設定することもできます。

1. **［ルール］の［デバイス設定］>［基本設定］をクリックします。**

2. **グループをクリックし、OS をクリックして、［作成］をクリックします。**

3. **次の項目を設定します。設定内容は OS ごとに異なります。**

設定	iOS	Android	Windows	macOS
メモ	○	○	○	○
LANSCOPE Client アップデート設定	―	―	―	○
デバイス表示設定（*1）（*2）	○	―	―	―
アンインストール防止設定	―	―	○	○
パスワードポリシー設定	○	○（*3）	―	○

*1：位置情報を使用しているときのステータスバー表示の設定です。
*2：LANSCOPE Client はデバイス情報取得のために常に起動し、定期的に位置情報を使用しています。

位置情報使用中は、デバイスにステータスバーが表示されます。ステータスバーを非表示に設定した場合、精度が高い位置情報の取得処理が実行されるため、デバイスのバッテリー駆動時間が短くなる可能性があります。

*3：Android 10 以上のデバイスには適用されません。

ポイント

- パスワードポリシーの適用タイミング

  設定後、iOS は 5 分、Android は 10 分以内に適用されます。

- アンインストール用パスワードの適用タイミング

  設定後、10 分以内に適用されます。

4. ［保存］をクリックします。

4-2　MDM 証明書を管理する

iOS macOS

iOS／macOS デバイスの管理に必要な MDM 証明書の設定をします。

■ MDM 証明書を登録する

必須

iOS／macOS デバイスの管理に必要な MDM 証明書をエンドポイントマネージャー Free に登録します。

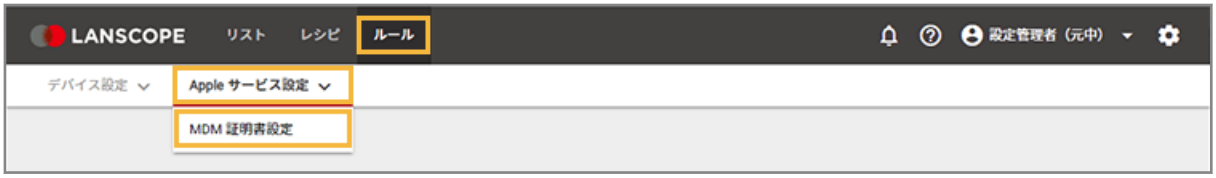
MDM 証明書の有効期限は登録から 1 年で、毎年更新が必要です。

事前に、MDM 証明書をダウンロードするために必要な Apple ID を準備します。

注意

MDM 証明書を更新するときにも同じ Apple ID を使用するため、Apple ID を紛失しないように注意してください。紛失などで Apple ID がわからなくなった場合、デバイスに LANSCOPE クライアントの入れ直しが必要になります。

1. **［ルール］の［Apple サービス設定］>［MDM 証明書設定］をクリックします。**



2. **［MDM 証明書の登録］をクリックします。**

3. **管理コンソールに記載の手順に従って、MDM 証明書を登録します。**

4. ［保存］をクリックします。

→ MDM 証明書の登録が完了します。

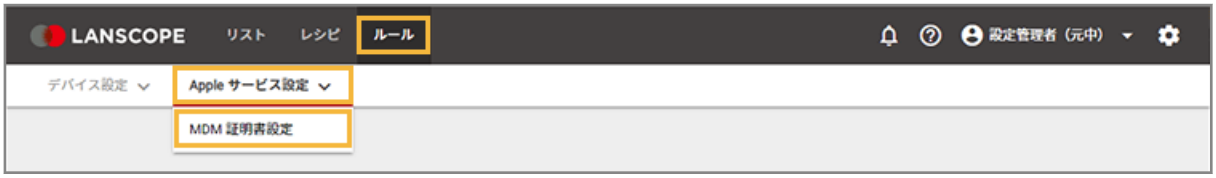
■ MDM 証明書を削除する

MDM 証明書をエンドポイントマネージャー Free から削除します。

注意

- MDM 証明書を削除すると、iOS／macOS デバイスを管理できなくなります。再度管理するときは、新しい MDM 証明書を登録後、新しい MDM 構成プロファイルの再インストールが必要です。
- MDM 構成プロファイルをアンインストールすると、エンドポイントマネージャー Free から配信したアプリ／プロファイルはアンインストールされます。

1. ［ルール］の［Apple サービス設定］>［MDM 証明書設定］をクリックします。



2. ［削除］をクリックします。

3. 注意事項をすべてにチェックし、［削除］をクリックします。


MDM 証明書の削除
MDM 証明書を削除します。
注意事項すべてに同意いただくことで、MDM 証明書を削除できます。
MDM 証明書を削除すると、iOS デバイスまたは Mac デバイスを
管理できなくなります。
再度管理するには、新しい MDM 証明書を登録し、
各デバイスに MDM 構成プロファイルを再インストールする必要があります。
※ DEP をご利用の場合、デバイスの初期化が必要です。
MDM 構成プロファイルをアンインストールすると、配信したアプリまたは
プロファイルはアンインストールされます。
キャンセル
削除