

 **Endpoint Manager** Cloud

利用ガイド

ビジネスプラス An-319 / 第 52 版 / 2024 年 4 月 5 日

MOTEX

まえがき	5
第 1 章 エンドポイントマネージャーの使い方	6
1-1 利用前に準備する	8
1-2 管理コンソール画面の見方	27
1-3 管理コンソールのログイン/ログアウト	36
1-4 アカウント/ロールを管理する	40
機能権限	40
アカウントを管理する	47
ロールを管理する	60
操作履歴を確認する	67
1-5 セキュリティを管理する	71
パスワードポリシーを設定する	71
2 要素認証を設定する	73
IP アドレス制限をする	81
第 2 章 リストで情報を確認する	87
2-1 デバイス情報を管理する	88
管理できる項目一覧	88
デバイス情報を確認する	94
デバイスの最新情報を取得する	98
デバイス情報を編集/削除する	99
任意項目表示名を設定/編集する	107
周辺機器情報を追加する	111
2-2 操作ログ情報を確認する	117
取得できる項目一覧	117
操作ログ情報の取得設定をする	119
操作ログを確認する	124
2-3 リモート操作を実行する	126
リモート操作を実行する	127
リモート操作の実行結果を確認する	144

2-4 アプリ情報を確認する	148
2-5 プロファイル情報を確認する	151
2-6 アラート情報を確認する	154
第3章 レシピで操作を自動実行する	156
3-1 レシピ一覧を管理する	158
レシピを作成する	158
レシピの有効/無効を設定する	164
レシピを任意のタイミングで実行する	166
レシピの実行履歴を確認する	173
レシピを編集/削除する	175
3-2 アクションを実行する	180
プロフィールを配信する	180
プロフィール配信の流れ	182
プロフィールの配信結果を確認する	209
登録したプロフィールを削除する	213
アプリを配信する	215
アプリ配信の流れ	217
デバイス側での操作	236
アプリの配信結果を確認する	238
登録したアプリを削除する	242
プロビジョニングプロフィールを配信する	244
プロビジョニングプロフィール配信の流れ	246
プロビジョニングプロフィールの配信結果を確認する	255
プロビジョニングプロフィールを削除する	259
メッセージ/アンケートを配信する	261
メッセージ/アンケート配信の流れ	262
デバイス側での操作	275
メッセージ/アンケートの配信結果を確認する	285
アンケートの回答内容を資産情報に反映する	289
メッセージ/アンケートを削除する	293

アラートを設定する	295
アラート設定の流れ	296
デバイスへの通知設定をする	306
アラートを確認する	309
操作ログ／位置情報を一括出力する	315
一括出力設定の流れ	315
出カデータをダウンロードする	322
第 4 章 デバイスの位置情報を確認する	327
4-1 位置情報の取得設定をする	328
4-2 最新の位置情報を確認する	336
第 5 章 レポートを確認する	340
5-1 デバイスの利用状況を確認する	341
5-2 Windows アップデートを確認して対策する	348
第 6 章 ルール設定をする	359
6-1 デバイス設定をする	360
グループを管理する	362
業務時間を設定する	370
取得する情報を設定する	372
PC 操作ログ設定をする	375
6-2 Apple サービス設定をする	379
MDM 証明書を管理する	380
iOS デバイスにアプリを配信する	384
アプリ配信設定を利用する	385
アプリ配信設定を追加する	386
アプリ配信対象のデバイスを追加する	425
デバイス側での操作	428
アプリ配信結果を確認する	430
登録したアプリを削除する	437
アプリカタログを利用する	439

LANSCOPE Client でアプリカタログを利用する	440
Web クリップでアプリカタログを利用する	463
デバイス側で表示されるエラーメッセージ	489
macOS デバイスにアプリを配信する	490
アプリ配信設定を追加する	490
アプリ配信対象のデバイスを追加する	494
アプリ配信結果を確認する	496
6-3 記録メディア制御設定をする	502
記録メディア全体の制御設定をする	502
記録メディアを制御する	503
特定の記録メディアを除外する	505
デバイスごとに個別で制御設定する	526
6-4 配信設定をする	529
ファイル配信設定をする	529
ファイル配信設定を追加する	530
配信対象のデバイスを追加する	547
配信結果を確認する	549
アップデート管理の設定をする	552
プロキシ設定を適用する	552
アップデート管理の設定をする	559
6-5 アプリ設定をする	576
アプリの管理レベルを設定する	576
アプリの利用を禁止するときに必要な設定をする	578
新規アプリの管理レベル初期設定	580
未インストールアプリの管理レベルを設定する	581
第 7 章 仕様	584
7-1 情報取得/設定 (ポリシー) 反映のタイミング	585
7-2 記録メディア別制御一覧	592

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
Android Enterprise 利用ガイド	Android Enterprise の操作手順
Apple Business Manager 利用ガイド	自動デバイス登録 (DEP)、アプリ一括配信 (VPP) の操作手順

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

- 本書で使用される各社の社名および製品名は、各社の商標または登録商標です。
- 本書に含まれる文章や画像などの著作権は、一部を除き、エムオーテックス株式会社が所有します。
- 本書のすべてまたは一部をエムオーテックス株式会社の許諾なく複製し、頒布その他の行為を行うことはできません。また、本書の内容・構成をエムオーテックス株式会社の許諾なく改変し、改変したものを複製し、頒布その他の行為を行うことはできません。
- 本ソフトウェアの仕様ならびに本書の記載内容は、予告なしに変更することがあります。
- MOTEX はエムオーテックス株式会社の略称です。

第1章 エンドポイントマネージャーの使い方

LANSCOPE エンドポイントマネージャー クラウド版は、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。

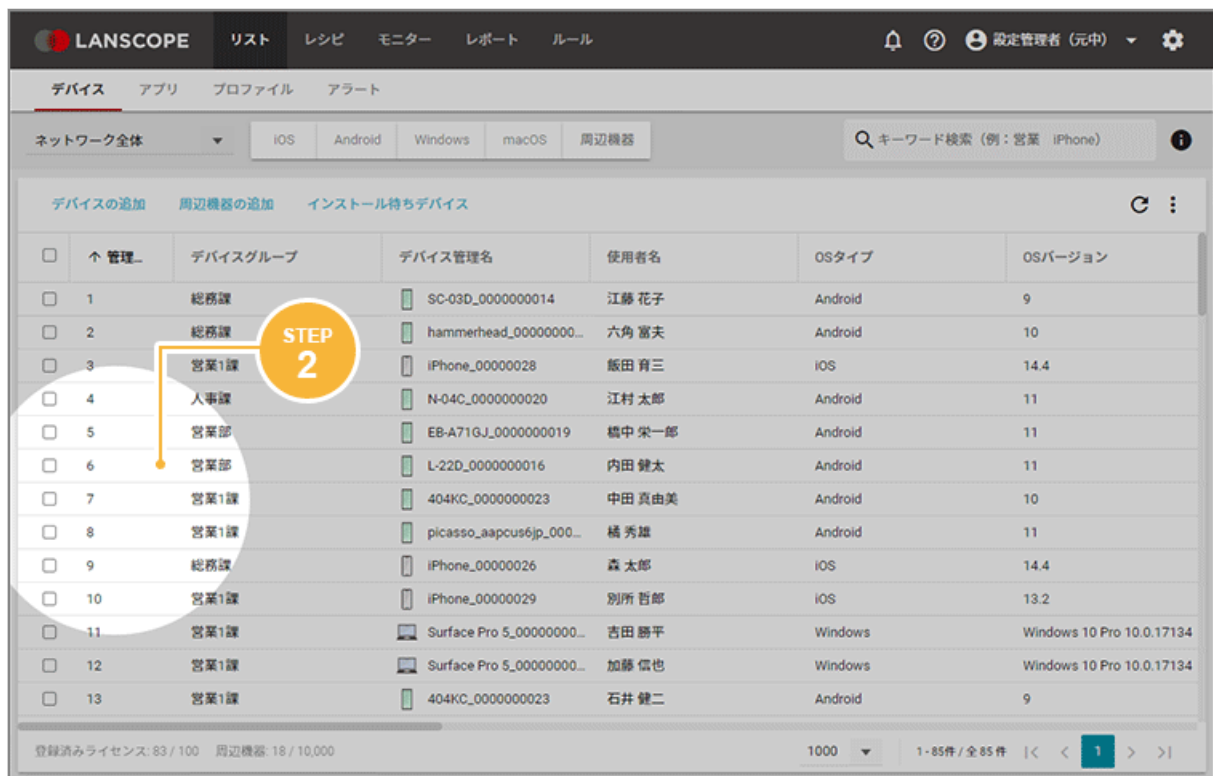
1. 目的を選択します。

デバイスや設定を確認するときは一覧表示の「リスト」、稼働状況を確認するときは「レポート」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 利用前に準備する

iOS

Android

Windows

macOS

エンドポイントマネージャーを利用するために、必要な設定があります。必要に応じて、デバイス側で設定します。

■ iOS

ドメイン/ポート番号の許可

プロキシ環境や閉域網を利用しているデバイスを管理する場合、指定したドメイン名/ポート番号を許可する設定が必要です。

許可設定には、「* (ワイルドカード)」を利用して設定する方法と、許可する必要があるドメイン名/ポート番号を個別に設定する方法があります。ただし、ドメイン名などは追加/変更の可能性があるため、ワイルドカードを利用した設定をおすすめします。

ワイルドカードを利用する場合

1. 管理コンソールを閲覧するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.amazonaws.com	TCP/443	outbound
*.google.com		
*.lanscopean.com		
*.motex.co.jp		
*.virtualearth.net		
cdn.auth0.com		
code.getmdl.io		
fonts.googleapis.com		
fonts.gstatic.com		
stats.g.doubleclick.net		
www.bing.com		
www.google-analytics.com		
www.lanscope.jp		
*.apple.com		

2. デバイスを管理するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.amazonaws.com	TCP/443	outbound
*.lanscopean.com		
setup.icloud.com		
aia.entrust.net	TCP/80	
*.apple.com	TCP/ 80,443,2197,52 23	
	UDP/123	
17.0.0.0/8 (*1)	TCP/ 443,2197,5223	outbound/ inbound

*1 : 詳細は、<https://support.apple.com/ja-jp/HT203609> を参照してください。

ドメイン名／ポート番号を個別に設定する場合

1. 管理コンソールを閲覧するために、次のドメイン名／ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
ユーザーサブドメイン.lanscopean.com	TCP/443	outbound
*.virtualearth.net		
api.androidenterprise.lanscopean.com		
api.assetmanagement.lanscopean.com		
api.auth2.lanscopean.com		
api.configuration2.lanscopean.com		
api.darwinapp.lanscopean.com		
api.darwinprofile.lanscopean.com		
api.dep.lanscopean.com		
api.distribution.lanscopean.com		
api.group3.lanscopean.com		
api.ios.clients.lanscopean.com		
api.it-asset-client.lanscopean.com		
api.location.lanscopean.com		
api.log.lanscopean.com		
api.log.report.lanscopean.com		
api.operation-logs.lanscopean.com		
api.person2.lanscopean.com		

ドメイン名	ポート番号	通信方向
api.recipe2.lanscopean.com		
api.rule.lanscopean.com		
api.vpp.lanscopean.com		
api.windows.installer.lanscopean.com		
apis.google.com		
business.apple.com		
cdn.auth0.com		
code.getmdl.io		
console-operationlogs.lanscopean.com		
console-operationlogs-export.lanscopean.com		
darwinapp-distribution.lanscopean.com		
darwinmacapp.lanscopean.com		
faq.motex.co.jp		
fonts.googleapis.com		
fonts.gstatic.com		
identity.apple.com		
integration.lanscopean.com		
itunes.apple.com		
login.lanscopean.com		
lspan-configuration-apps-prod.s3.ap-northeast-1.amazonaws.com		
lspan-configuration-apps-prod.s3.ap-northeast-1.amazonaws.com		
lspan-configuration-iosmdmcertificate-prod.s3.ap-northeast-1.amazonaws.com		
lspan-configuration-messages-prod.s3.ap-northeast-1.amazonaws.com		
lspan-configuration-provisioningprofile-prod.s3.ap-northeast-1.amazonaws.com		
lspan-darwinprofile-prod.s3.ap-northeast-1.amazonaws.com		
lspan-dep-prod.s3.ap-northeast-1.amazonaws.com		
lspan-logs-output-location-data-ap-northeast-1-prod.s3.ap-northeast-1.amazonaws.com		

ドメイン名	ポート番号	通信方向
lspan-logs-output-operation-data-ap-northeast-1-prod.s3.ap-northeast-1.amazonaws.com		
lspan-recipe-action-data-prod.s3-ap-northeast-1.amazonaws.com		
maps.google.com		
notification.lanscopean.com		
pub.contract2.lanscopean.com		
r.bing.com		
recordingmedia.lanscopean.com		
redirect.lanscopean.com		
resource.lanscopean.com		
rvy8zpzmu.execute-api.ap-northeast-1.amazonaws.com		
stats.g.doubleclick.net		
tryweb2.motex.co.jp		
vpp.itunes.apple.com		
www.bing.com		
www.google-analytics.com		
www.lanscope.jp		

2. デバイスを管理するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.apps.apple.com	TCP/443	outbound
api.ios.clients.lanscopean.com		
appldnld.apple.com		
attachment.clients.lanscopean.com		
deviceenrollment.apple.com		
deviceservices-external.apple.com		
gdmf.apple.com		
installer.ios.clients.lanscopean.com		
iprofiles.apple.com		
lspan-configuration-apps-prod.s3-ap-northeast-1.amazonaws.com		

ドメイン名	ポート番号	通信方向
lspan-configuration-apps-prod.s3.ap-northeast-1.amazonaws.com		
lspan-global-settings.clients.lanscopean.com		
lspan-ios-errorreport-ap-northeast-1-prod.s3-ap-northeast-1.amazonaws.com		
m.ios.clients.lanscopean.com		
mdmenrollment.apple.com		
mesu.apple.com		
s.ios.clients.lanscopean.com		
setup.icloud.com		
template.clients.lanscopean.com		
time.apple.com	UDP/123	
time-ios.apple.com		
aia.entrust.net	TCP/80	
*.itunes.apple.com	TCP/80,443	
*.push.apple.com	TCP/ 80,443,2197,5223	
gateway.push.apple.com	TCP/ 443,2197,5223	outbound/ inbound
17.0.0.0/8 (*1)		

*1 : 詳細は、<https://support.apple.com/ja-jp/HT203609> を参照してください。

■ Android

ドメイン/ポート番号の許可

プロキシ環境や閉域網を利用しているデバイスを管理する場合、指定したドメイン名/ポート番号を許可する設定が必要です。

許可設定には、「* (ワイルドカード)」を利用して設定する方法と、許可する必要があるドメイン名/ポート番号を個別に設定する方法があります。ただし、ドメイン名などは追加/変更の可能性があるため、ワイルドカードを利用した設定をおすすめします。

ワイルドカードを利用する場合

1. 管理コンソールを閲覧するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.amazonaws.com	TCP/443	outbound
*.lanscopean.com		
*.motex.co.jp		
*.pki.goog		
*.virtualearth.net		
cdn.auth0.com		
code.getmdl.io		
fonts.googleapis.com		
fonts.gstatic.com		
stats.g.doubleclick.net		
www.bing.com		
www.google-analytics.com		
www.lanscope.jp		
*.google.com		
	UDP/ 5228,5229,523 0	
*.android.com	TCP/ 443,5228,5229, 5230	
*.googleapis.com	TCP/ 443,5228,5229, 5230,5235,523 6	

2. デバイスを管理するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.lanscopean.com	TCP/443	outbound
omahaproxy.appspot.com		
*.android.com	TCP/ 443,5228,5229, 5230	
*.googleusercontent.com		
*.ggpht.com	TCP/443	

ドメイン名	ポート番号	通信方向
*.gstatic.com	UDP/ 5228,5229,523 0	
*gvt1.com		
*gvt2.com		
*gvt3.com		
google-analytics.com		
*.google.com	TCP/ 443,5228,5229, 5230 UDP/ 5228,5229,523 0	
*.googleapis.com	TCP/ 443,5228,5229, 5230,5235,523 6	

ドメイン名／ポート番号を個別に設定する場合

1. 管理コンソールを閲覧するために、次のドメイン名／ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
ユーザーサブドメイン.lanscopean.com	TCP/443	outbound
*.gstatic.com		
*.virtualearth.net		
accounts.google.*		
accounts.google.com		
ajax.googleapis.com		
api.androidenterprise.lanscopean.com		
api.assetmanagement.lanscopean.com		
api.auth2.lanscopean.com		
api.configuration2.lanscopean.com		
api.darwinapp.lanscopean.com		
api.darwinprofile.lanscopean.com		
api.dep.lanscopean.com		
api.distribution.lanscopean.com		
api.group3.lanscopean.com		

ドメイン名	ポート番号	通信方向
api.ios.clients.lanscopean.com		
api.it-asset-client.lanscopean.com		
api.location.lanscopean.com		
api.log.lanscopean.com		
api.log.report.lanscopean.com		
api.operation-logs.lanscopean.com		
api.person2.lanscopean.com		
api.recipe2.lanscopean.com		
api.rule.lanscopean.com		
api.vpp.lanscopean.com		
api.windows.installer.lanscopean.com		
apis.google.com		
cdn.auth0.com		
clients1.google.com		
code.getmdl.io		
console-operationlogs.lanscopean.com		
console-operationlogs-export.lanscopean.com		
crl.pki.goog		
darwinapp-distribution.lanscopean.com		
darwinmacapp.lanscopean.com		
enterprise.google.com		
faq.motex.co.jp		
fonts.googleapis.com		
fonts.gstatic.com		
gds.google.com		
google.com		
integration.lanscopean.com		
lh3.googleusercontent.com		
login.lanscopean.com		
lspan-configuration-messages-prod.s3.ap-northeast-1.amazonaws.com		
lspan-logs-output-location-data-ap-northeast-1-prod.s3.ap-northeast-1.amazonaws.com		

ドメイン名	ポート番号	通信方向
lspan-logs-output-operation-data-ap-northeast-1-prod.s3.ap-northeast-1.amazonaws.com		
lspan-recipe-action-data-prod.s3-ap-northeast-1.amazonaws.com		
maps.google.com		
myaccount.google.com		
notification.lanscopean.com		
notifications.google.com		
ocsp.pki.goog		
ogs.google.com		
partner.android.com		
payments.google.com		
play.google.com		
play-lh.googleusercontent.com		
pub.contract2.lanscopean.com		
r.bing.com		
recordingmedia.lanscopean.com		
redirect.lanscopean.com		
resource.lanscopean.com		
rvy8zpzmu.execute-api.ap-northeast-1.amazonaws.com		
stats.g.doubleclick.net		
tryweb2.motex.co.jp		
www.bing.com		
www.google.com		
www.google-analytics.com		
www.lanscope.jp		
fcm.googleapis.com	TCP/ 443,5228,5229, 5230	outbound/ inbound

2. デバイスを管理するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.googleapis.com	TCP/443	outbound

ドメイン名	ポート番号	通信方向
accounts.google.[country]		
accounts.google.com		
api.android.clients.lanscopean.com		
attachment.clients.lanscopean.com		
clients1.google.com		
clients2.google.com		
clients3.google.com		
clients4.google.com		
clients5.google.com		
clients6.google.com		
connectivitycheck.android.com		
lspan-android-errorreport-ap-northeast-1-prod.s3-ap-northeast-1.amazonaws.com		
lspan-global-settings.clients.lanscopean.com		
omahaproxy.appspot.com		
pki.google.com		
template.clients.lanscopean.com		
www.google.com		
*.gppht.com	TCP/443	
*.gvt1.com	UDP/ 5228,5229,5230	
*.gvt2.com		
*.gvt3.com		
*gstatic.com		
android.clients.google.com		
android.com		
dl.google.com		
dl-ssl.google.com		
google-analytics.com		
googleusercontent.com		
play.google.com	TCP/ 443,5228,5229, 5230	

ドメイン名	ポート番号	通信方向
	UDP/ 5228,5229,5230	
android.googleapis.com	TCP/ 443,5228,5229, 5230	outbound/ inbound
fcm.googleapis.com		
gcm-http.googleapis.com		
fcm-xmpp.googleapis.com	TCP/ 443,5228,5229, 5230,5235,5236	
gcm-xmpp.googleapis.com		

■ Windows

ドメイン/ポート番号の許可

プロキシ環境や閉域網を利用しているデバイスを管理する場合、指定したドメイン名/ポート番号を許可する設定が必要です。

許可設定には、「* (ワイルドカード)」を利用して設定する方法と、許可する必要があるドメイン名/ポート番号を個別に設定する方法があります。ただし、ドメイン名などは追加/変更の可能性があるため、ワイルドカードを利用した設定をおすすめします。

ワイルドカードを利用する場合

1. 管理コンソールを閲覧するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.amazonaws.com	TCP/443	outbound
*.google.com		
*.lanscopean.com		
*.motex.co.jp		
*.virtualearth.net		
cdn.auth0.com		
code.getmdl.io		
fonts.googleapis.com		
fonts.gstatic.com		
stats.g.doubleclick.net		
www.bing.com		

ドメイン名	ポート番号	通信方向
www.catalog.update.microsoft.com		
www.google-analytics.com		
www.lanscope.jp		

2. デバイスを管理するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.amazonaws.com	TCP/443	outbound
*.dl.delivery.mp.microsoft.com		
*.do.dsp.mp.microsoft.com		
*.download.microsoft.com		
*.download.windowsupdate.com		
*.emdl.ws.microsoft.com		
*.lanscopean.com		
*.mp.microsoft.com		
*.update.microsoft.com		
*.windowsupdate.com		
login.live.com		
ntservicepack.microsoft.com		

ドメイン名/ポート番号を個別に設定する場合

1. 管理コンソールを閲覧するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
ユーザーサブドメイン.lanscopean.com	TCP/443	outbound
*.virtualearth.net		
*.windows.clients.lanscopean.com		
api.androidenterprise.lanscopean.com		
api.assetmanagement.lanscopean.com		
api.auth2.lanscopean.com		
api.configuration2.lanscopean.com		
api.darwinapp.lanscopean.com		
api.darwinprofile.lanscopean.com		
api.dep.lanscopean.com		

ドメイン名	ポート番号	通信方向
api.distribution.lanscopean.com		
api.group3.lanscopean.com		
api.ios.clients.lanscopean.com		
api.it-asset-client.lanscopean.com		
api.location.lanscopean.com		
api.log.lanscopean.com		
api.log.report.lanscopean.com		
api.operation-logs.lanscopean.com		
api.person2.lanscopean.com		
api.recipe2.lanscopean.com		
api.rule.lanscopean.com		
api.vpp.lanscopean.com		
api.windows.installer.lanscopean.com		
apis.google.com		
cdn.auth0.com		
code.getmdl.io		
console-operationlogs.lanscopean.com		
console-operationlogs-export.lanscopean.com		
darwinapp-distribution.lanscopean.com		
darwinmacapp.lanscopean.com		
faq.motex.co.jp		
fonts.googleapis.com		
fonts.gstatic.com		
integration.lanscopean.com		
login.lanscopean.com		
lspan-configuration-messages-prod.s3.ap-northeast-1.amazonaws.com		
lspan-logs-output-location-data-ap-northeast-1-prod.s3.ap-northeast-1.amazonaws.com		
lspan-logs-output-operation-data-ap-northeast-1-prod.s3.ap-northeast-1.amazonaws.com		
lspan-recipe-action-data-prod.s3.ap-northeast-1.amazonaws.com		

ドメイン名	ポート番号	通信方向
lspix-distribution-distributions-prod.s3.amazonaws.com		
lspix-installer-install-tools-prod.s3.amazonaws.com		
lspix-log-alert-report.lanscopean.com		
lspix-log-export.lanscopean.com		
maps.google.com		
notification.lanscopean.com		
pub.contract2.lanscopean.com		
r.bing.com		
recordingmedia.lanscopean.com		
redirect.lanscopean.com		
resource.lanscopean.com		
rvy8zpzmu.execute-api.ap-northeast-1.amazonaws.com		
stats.g.doubleclick.net		
tryweb2.motex.co.jp		
windowsupdate.lanscopean.com		
www.bing.com		
www.catalog.update.microsoft.com		
www.google-analytics.com		
www.lanscope.jp		

2. デバイスを管理するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.dl.delivery.mp.microsoft.com	TCP/443	outbound
*.do.dsp.mp.microsoft.com		
*.download.microsoft.com		
*.download.windowsupdate.com		
*.emdl.ws.microsoft.com		
*.mp.microsoft.com		
*.update.microsoft.com		
*.windowsupdate.com		
api.windows.clients.lanscopean.com		
api.windows.x.clients.lanscopean.com		

ドメイン名	ポート番号	通信方向
attachment.clients.lanscopean.com		
login.live.com		
lspan-windows-errorreport-ap-northeast-1-prod.s3-ap-northeast-1.amazonaws.com		
lspan-windows-updater-ap-northeast-1-prod.s3-ap-northeast-1.amazonaws.com		
lspc-client-setting-merged-prod.s3.amazonaws.com		
ntservicepack.microsoft.com		
template.clients.lanscopean.com		

■ macOS

ドメイン/ポート番号の許可

プロキシ環境や閉域網を利用しているデバイスを管理する場合、指定したドメイン名/ポート番号を許可する設定が必要です。

許可設定には、「* (ワイルドカード)」を利用して設定する方法と、許可する必要があるドメイン名/ポート番号を個別に設定する方法があります。ただし、ドメイン名などは追加/変更の可能性があるため、ワイルドカードを利用した設定をおすすめします。

ワイルドカードを利用する場合

1. 管理コンソールを開覧するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.amazonaws.com	TCP/443	outbound
*.google.com		
*.lanscopean.com		
*.motex.co.jp		
*.virtualearth.net		
cdn.auth0.com		
code.getmdl.io		
fonts.googleapis.com		
fonts.gstatic.com		
stats.g.doubleclick.net		
www.bing.com		

ドメイン名	ポート番号	通信方向
www.google-analytics.com		
www.lanscope.jp		
*.apple.com	TCP/ 80,443,2197,52 23	

2. デバイスを管理するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.apple.com	TCP/ 80,443,2197,52 23 UDP/123	outbound
*.amazonaws.com	TCP/443	
*.lanscopean.com		
*.mzstatic.com		
aia.entrust.net	TCP/80	
*.google.com	TCP/ 443,5228,5229, 5230 UDP/ 5228,5229,523 0	
*.googleusercontent.com	TCP/ 443,5228,5229, 5230	
17.0.0.0/8 (*1)	TCP/ 443,2197,5223	outbound/ inbound

*1：詳細は、<https://support.apple.com/ja-jp/HT203609> を参照してください。

ドメイン名/ポート番号を個別に設定する場合

1. 管理コンソールを閲覧するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
ユーザーサブドメイン.lanscopean.com	TCP/443	outbound
*.virtualearth.net		
api.androidenterprise.lanscopean.com		

ドメイン名	ポート番号	通信方向
api.assetmanagement.lanscopean.com		
api.auth2.lanscopean.com		
api.configuration2.lanscopean.com		
api.darwinapp.lanscopean.com		
api.darwinprofile.lanscopean.com		
api.dep.lanscopean.com		
api.distribution.lanscopean.com		
api.group3.lanscopean.com		
api.ios.clients.lanscopean.com		
api.it-asset-client.lanscopean.com		
api.location.lanscopean.com		
api.log.lanscopean.com		
api.log.report.lanscopean.com		
api.operation-logs.lanscopean.com		
api.person2.lanscopean.com		
api.recipe2.lanscopean.com		
api.rule.lanscopean.com		
api.vpp.lanscopean.com		
api.windows.installer.lanscopean.com		
apis.google.com		
cdn.auth0.com		
code.getmdl.io		
console-operationlogs.lanscopean.com		
console-operationlogs-export.lanscopean.com		
darwinapp-distribution.lanscopean.com		
darwinmacapp.lanscopean.com		
darwinmacapp-pkg-distribution-plists-prod.s3-ap-northeast-1.amazonaws.com		
faq.motex.co.jp		
fonts.googleapis.com		
fonts.gstatic.com		
identity.apple.com		

ドメイン名	ポート番号	通信方向
integration.lanscopean.com		
login.lanscopean.com		
lspix-log-alert-report.lanscopean.com		
lspix-log-export.lanscopean.com		
lspan-configuration-iosmdmcertificate-prod.s3.ap-northeast-1.amazonaws.com		
lspan-configuration-messages-prod.s3.ap-northeast-1.amazonaws.com		
lspan-dep-prod.s3.ap-northeast-1.amazonaws.com		
lspan-logs-output-location-data-ap-northeast-1-prod.s3.ap-northeast-1.amazonaws.com		
lspan-logs-output-operation-data-ap-northeast-1-prod.s3.ap-northeast-1.amazonaws.com		
lspan-recipe-action-data-prod.s3-ap-northeast-1.amazonaws.com		
maps.google.com		
notification.lanscopean.com		
pub.contract2.lanscopean.com		
r.bing.com		
recordingmedia.lanscopean.com		
redirect.lanscopean.com		
resource.lanscopean.com		
rvy8zpzmu.execute-api.ap-northeast-1.amazonaws.com		
stats.g.doubleclick.net		
tryweb2.motex.co.jp		
www.bing.com		
www.google-analytics.com		
www.lanscope.jp		

2. デバイスを管理するために、次のドメイン名/ポート番号の許可設定をします。

ドメイン名	ポート番号	通信方向
*.apps.apple.com	TCP/443	outbound
*.mzstatic.com		

ドメイン名	ポート番号	通信方向
clients2.google.com (*1)		
clients2.googleusercontent.com (*1)		
deviceenrollment.apple.com		
deviceservices-external.apple.com		
gdmf.apple.com		
iprofiles.apple.com		
itunes.apple.com		
lspan-alltypes-settings-ap-northeast-1-prod.s3.ap-northeast-1.amazonaws.com		
lspan-mac-errorreport-ap-northeast-1-prod.s3.ap-northeast-1.amazonaws.com		
lspc-client-setting-merged-prod.s3.ap-northeast-1.amazonaws.com		
m.mac.clients.lanscopean.com		
mac-clients.lanscopean.com		
macclients.lanscopean.com		
mdmenrollment.apple.com		
mesu.apple.com		
ppq.apple.com		
s.mac.clients.lanscopean.com		
time.apple.com		
time-macos.apple.com		
aia.entrust.net	TCP/80	
*.itunes.apple.com	TCP/80,443	
*.push.apple.com	TCP/ 80,443,2197,5223	
gateway.push.apple.com	TCP/ 443,2197,5223	outbound/ inbound
17.0.0.0/8 (*2)		

*1 : 設定しても Web ブラウザーの拡張機能を利用できない場合は、追加でドメイン名/ポート番号の許可が必要です。詳細は、<https://support.google.com/chrome/a/answer/6334001?hl=ja> を参照してください。

*2 : 詳細は、<https://support.apple.com/ja-jp/HT203609> を参照してください。

1-2 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。

LANSCOPE リスト レシビ モニター レポート ルール

デバイス アプリ プロファイル アラート

1 メニューを選択

ネットワーク全体 iOS Android Windows macOS 周辺機器

キーワード検索 (例: 営業 iPhone)

デバイスの追加 周辺機器の追加 インストール待ちデバイス

管理	デバイスグループ	デバイス管理名	ユーザー名	OSタイプ	OSバージョン
1	総務課	SC-03D_0000000014	江藤 花子	Android	9
2	総務課	hammerhead_00000000...	六角 富夫	Android	10
3	営業1課	iPhone_000000028	飯田 育三	iOS	14.4
4	人事課	N-04C_0000000020	江村 太郎	Android	11
5	営業1課	EB-A71GJ_0000000019	橋中 栄一郎	Android	11
6	営業1課	L-22D_0000000016	内田 健太	Android	11
7	営業1課	404KC_0000000023	中田 真由美	Android	10
8	営業1課	picasso_aapcuse6jp_000...	橋 秀雄	Android	11
9	総務課	iPhone_000000026	森 太郎	iOS	14.4
10	営業1課	iPhone_000000029	別所 首郎	iOS	13.2
11	営業1課	Surface Pro 5_00000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134
12	営業1課	Surface Pro 5_00000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134
13	営業1課	404KC_0000000023	石井 健二	Android	9

登録済みライセンス: 83 / 100 周辺機器: 18 / 10,000

1000 1-85件 / 全85件



Android SC-03D_0000000014 - デバイス詳細

管理No. 1

デバイスグループ: 総務課 | ユーザー名: 江藤 花子 | 電話番号: 090xxxxxxx | アカウントのメールアドレス: at10.motex@gmail.com | 最終稼働: 7時間前

管理情報 管理情報更新日時: 2024/01/17 17:37:23

3 確認

基本情報

デバイス管理名: SC-03D_0000000014 | デバイスタイプ: スマートフォン

ユーザー名: 江藤 花子 | 使用者の社員コード: .

使用者の組織名: 総務課

管理者名: 江藤 花子 | 管理者の組織名: 総務課

管理者の組織コード: 00012SOUMU

使用状況

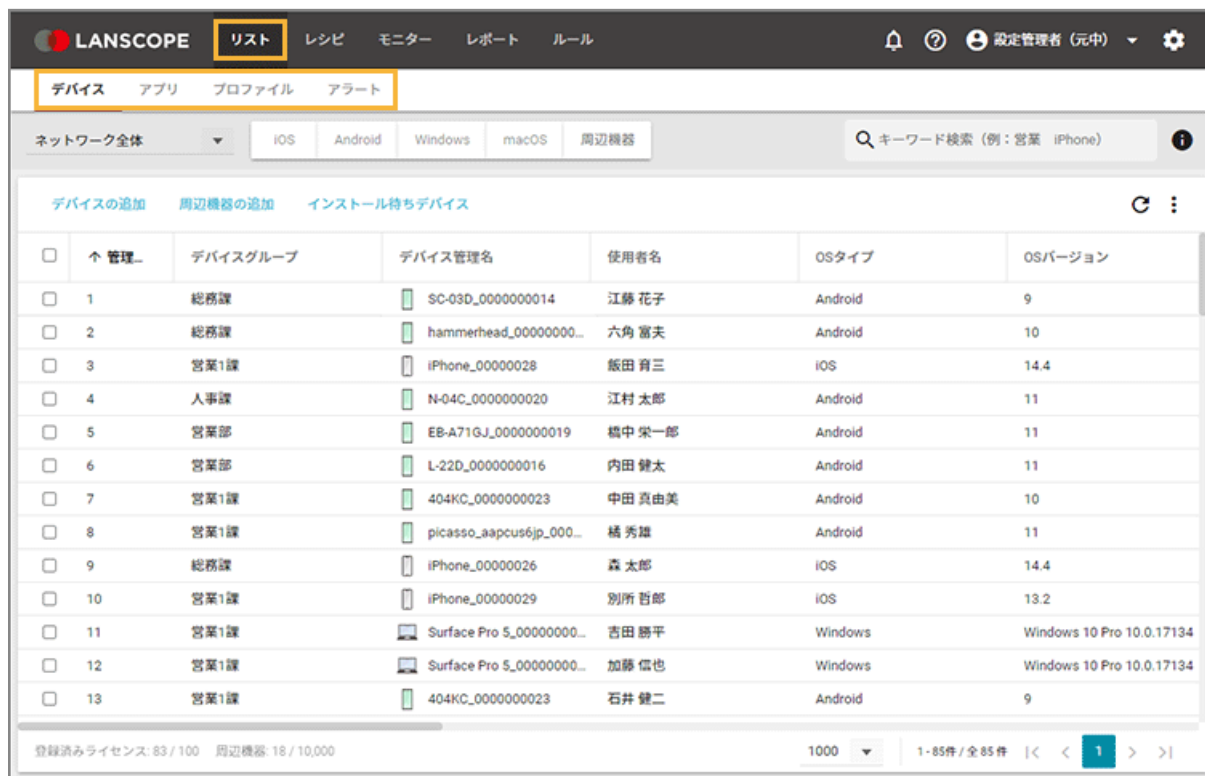
閉じる

■ 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

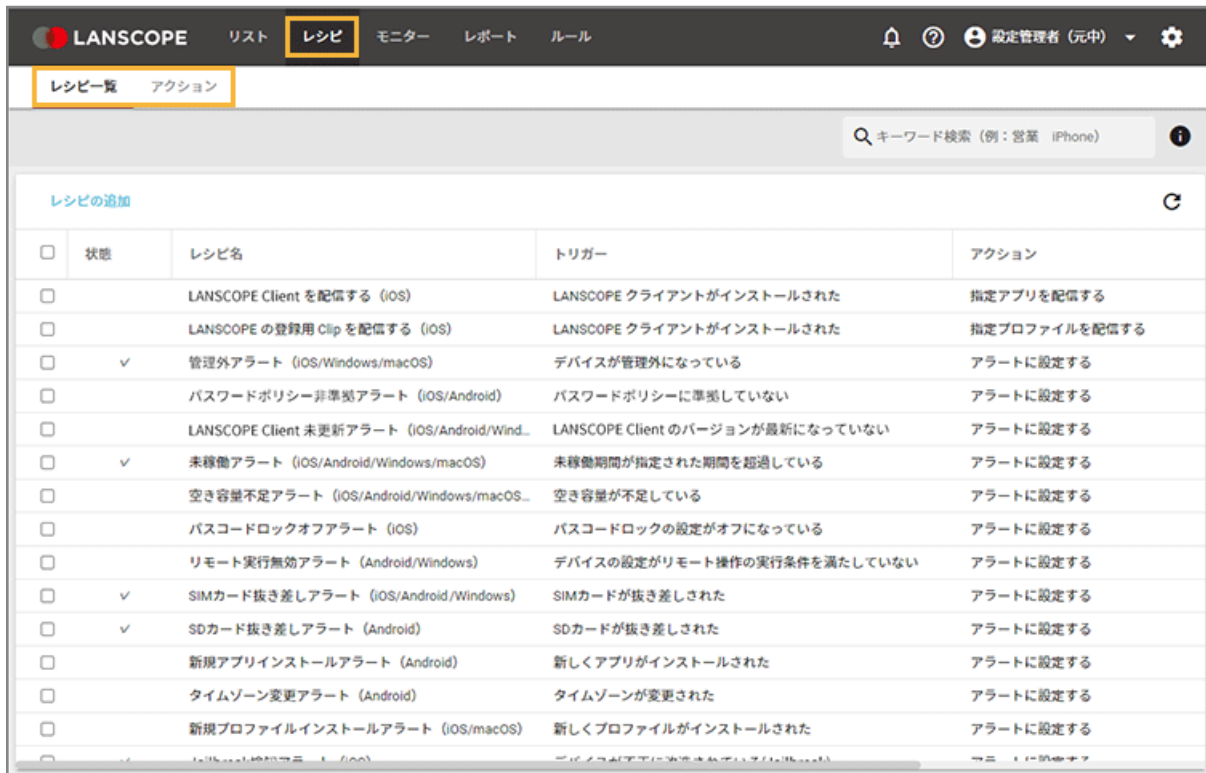
デバイス情報や、インストールアプリ情報／アカウント情報など、さまざまな情報を一覧で確認できます。デバイスの一覧からデバイスを選択し、詳細情報の確認やリモート操作ができます。



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、各デバイスのインベントリ情報の確認や、リモート操作ができます。
アプリ	各 OS のインストールアプリ情報を、アプリごとに確認できます。
プロファイル	iOS/macOS デバイスにインストールされているプロファイル情報を、プロファイルごとに確認できます。
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

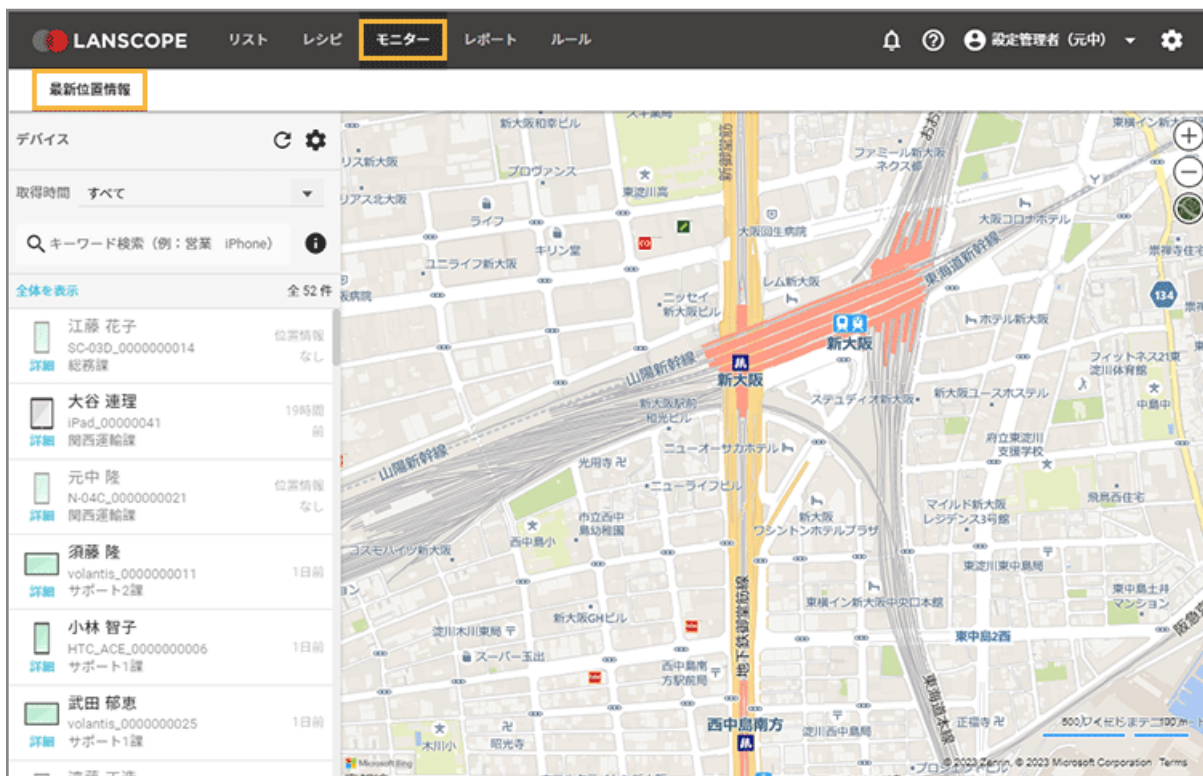
設定した条件に一致したデバイスに対し、アプリやメッセージ配信など指定したアクションを自動実行します。このトリガーとアクションの組み合わせを、レシピとして登録します。



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。
アクション	個別に設定が必要なアクションの設定を行います。

モニター

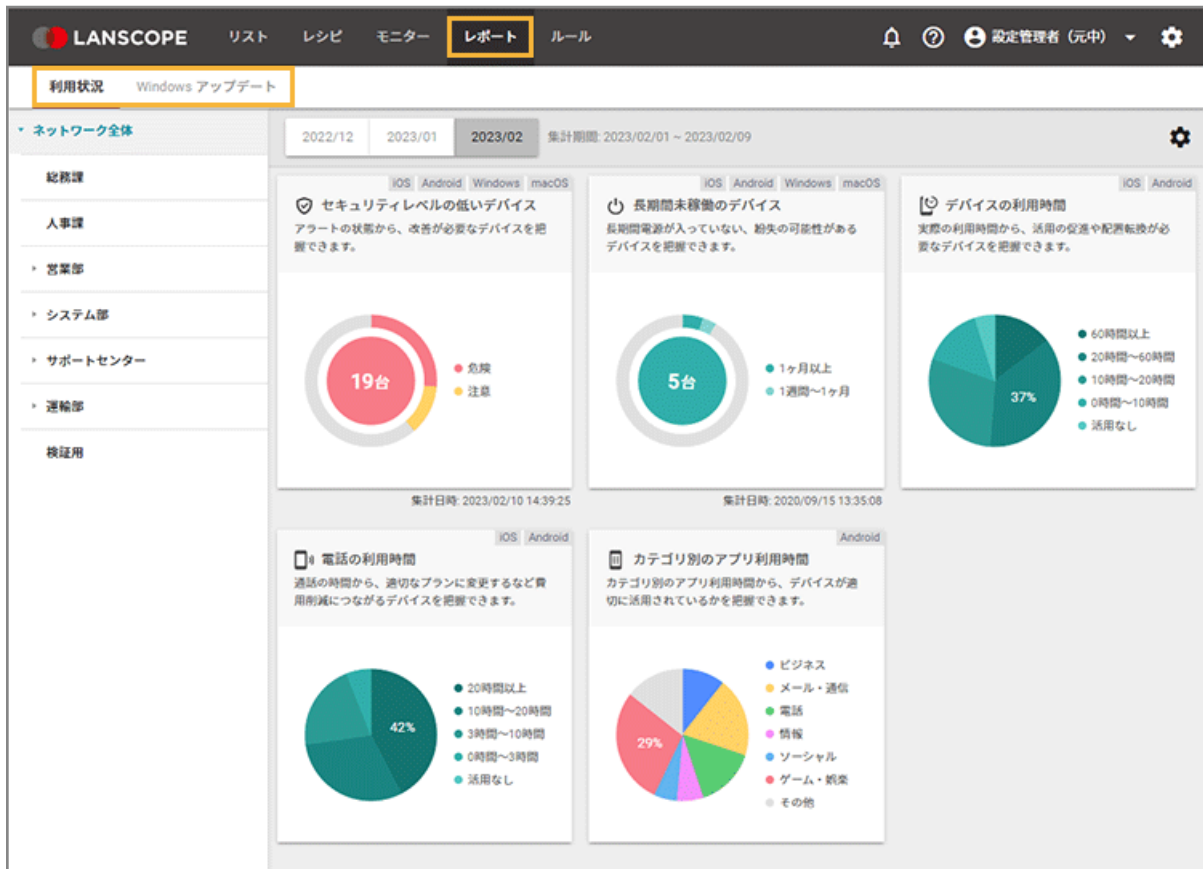
デバイスの最新位置情報を確認できます。1つの地図内に、最大 100 台の最新の位置情報を表示できます。



メニュー	内容
最新位置情報	デバイスの位置情報サービスを利用し、現在位置を地図上で確認できます。

レポート

取得した操作ログ/資産情報のデータや Windows アップデートの情報から、レポートを自動作成できます。導入デバイス/業務アプリが本来の目的で活用できているかを視覚的に確認できます。



メニュー	内容
利用状況	取得した操作ログや資産情報のデータから、レポートを自動作成できます。
Windows アップデート	Windows アップデートのレポートを確認して、サポートが終了する OS や、未適用の月例パッチのインストール設定ができます。

ルール

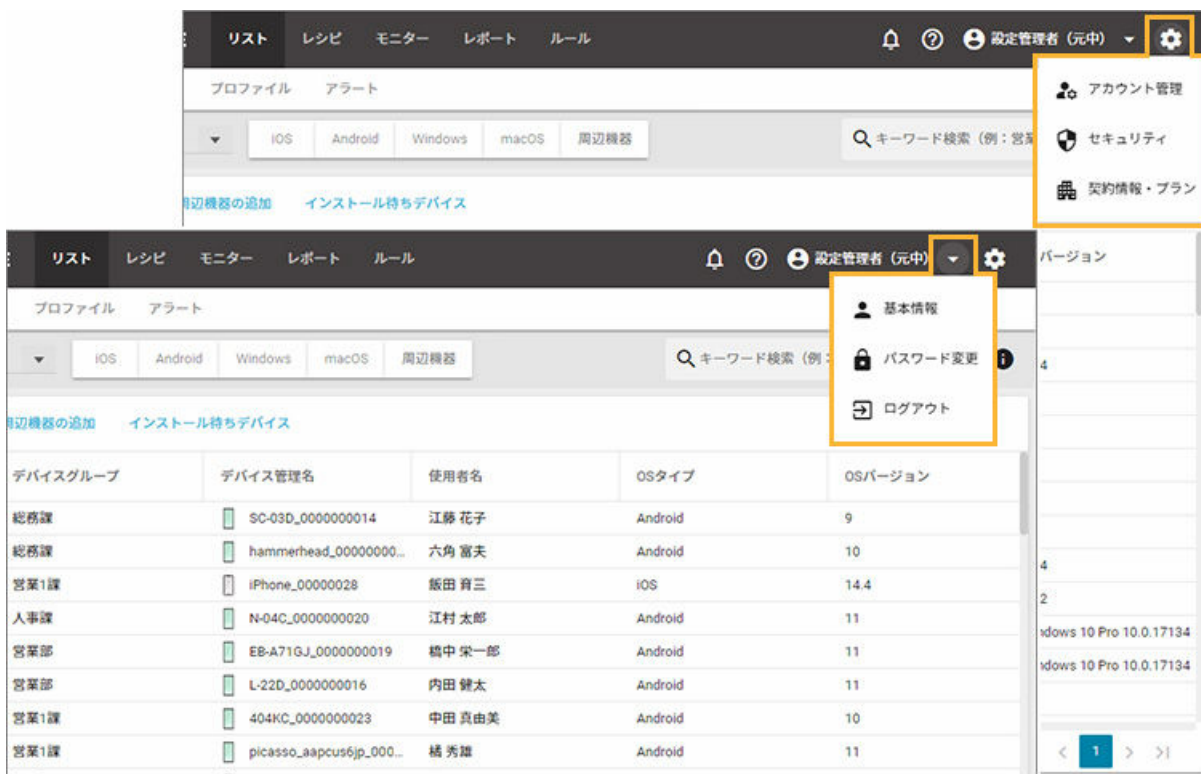
エンドポイントマネージャーを利用/運用するために必要な設定ができます。



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 証明書設定」「DEP 設定」「VPP 設定」「アプリカタログ設定」「アプリ配信設定」「パスワード一括設定」ができます。 「DEP 設定」「VPP 設定」「パスワード一括設定」の詳細は、An-353「Apple Business Manager 利用ガイド」を参照してください。
Android Enterprise 設定	Android Enterprise を利用する場合に必要な設定ができます。 詳細は、An-347「Android Enterprise 利用ガイド」を参照してください。
記録メディア制御	Windows/macOS デバイスの記録メディア制御に必要な「全体設定」「デバイス毎の設定／一時利用」を設定できます。
配信設定	Windows デバイスへの配信に必要な「ファイル配信設定」「OS アップデート」を設定できます。
アプリ設定	インストール情報を取得したアプリの利用レベルを設定できます。

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	アカウント設定の確認や、アカウントで利用するロールの設定、管理コンソールの操作履歴の確認ができます。
	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、IP アドレス制限ができます。
	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。



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。



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。



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。



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。



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。



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。



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 

設定画面が表示されます。

10 

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。

11 

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。

1-3 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。

The screenshot shows the 'パスワードリセット' (Reset Password) page of the Lanscope Endpoint Manager. At the top is the Lanscope logo. Below it, the title 'パスワードリセット' is displayed. A message reads: 'アカウントとして登録されているメールアドレスを入力してください。パスワードを再設定する URL がメールで送信されます。' (Please enter the email address registered as your account. The URL to reset your password will be sent via email.) There is a text input field labeled 'メールアドレス' (Email Address). Below the field is a blue button labeled '送信' (Send). At the bottom, there is a link labeled 'ログイン画面に戻る' (Return to login screen).

→ 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。

The screenshot shows the login page of the Lanscope Endpoint Manager. At the top is the Lanscope logo. Below it, there are two text input fields: 'アカウント' (Account) and 'パスワード' (Password). The password field has an eye icon to toggle visibility. Below the fields is a link labeled 'パスワードの設定はこちら' (Click here to set password). At the bottom is a blue button labeled 'ログイン' (Login).

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。



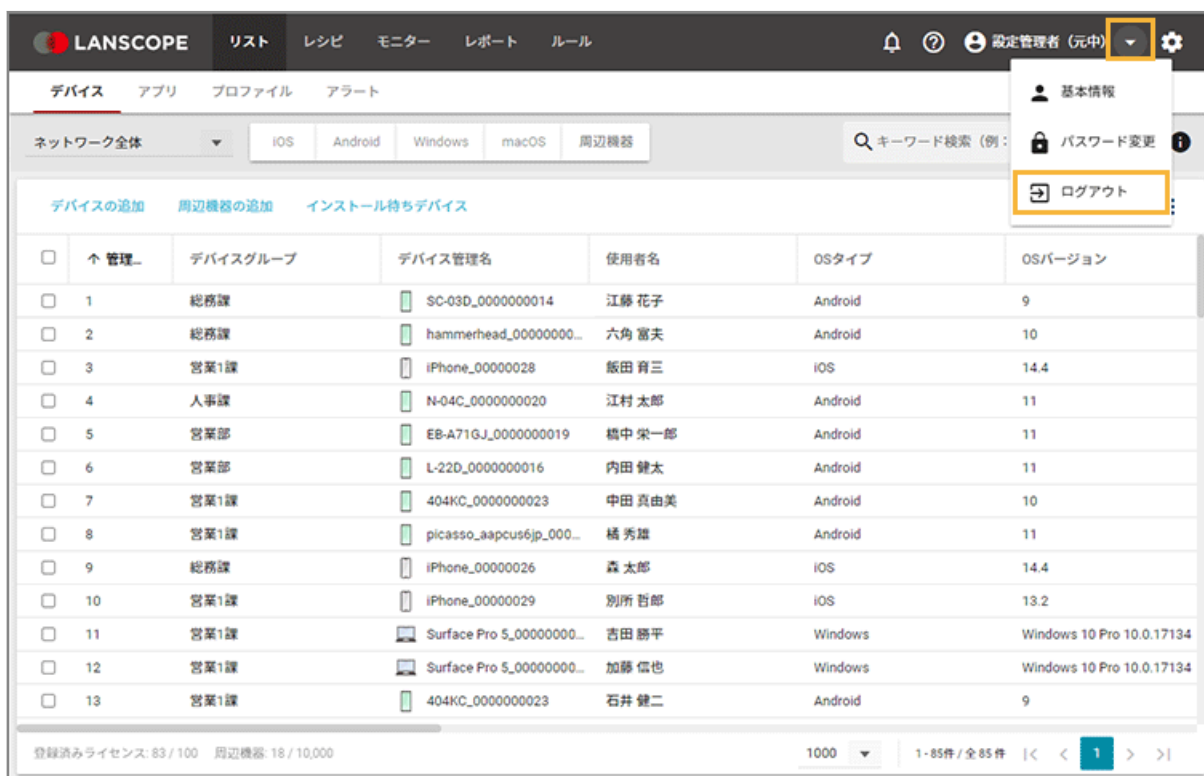
3. 認証デバイスで認証アプリを起動し、認証コードを確認します。
4. 認証コードを入力し、[認証] をクリックします。



■ 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。

1-4 アカウント／ロールを管理する

iOS

Android

Windows

macOS

管理コンソールのアカウント／ロールを管理したり、アカウントの操作履歴を確認したりします。ロールでは、機能権限を設定できます。

- [機能権限](#)
- [アカウントを管理する](#)
- [ロールを管理する](#)
- [操作履歴を確認する](#)

機能権限

iOS

Android

Windows

macOS

機能権限を設定すると、該当ロールを適用したアカウントでは、設定した機能だけを利用させることができます。ロール名「システム管理者」はデフォルトで設定されているロールで、すべての権限が付与されています。

機能権限	詳細
—	<p>ポイント</p> <p>次の権限以外を付与した場合、確認／設定ができます。</p> <ul style="list-style-type: none"> • 「リモートロックを実行できる」 • 「リモートワイプを実行できる」 <ul style="list-style-type: none"> • [リスト] > [デバイス] [アプリ] [プロファイル] で、画面を確認できます。 • [リスト] > [デバイス] で、デバイス情報をエクスポートできます。 • 「デバイス詳細」画面で、「管理情報」「デバイスグループ」「デバイス情報」「ネットワーク」「セキュリティ」「インストールアプリ」「プロファイル (iOS・macOS)」「Microsoft Office (Windows)」「クライアント」情報を確認できます。 • [ルール] > [デバイス設定] > [基本設定] で、各 OS の「デバイス使用者への設定情報表示 (iOS/Android/Windows)」「デバイス情報取得設定」を設定できます。 • [ルール] > [アプリ設定] で、アプリのレベル設定ができます。
アカウント管理ができる	<ul style="list-style-type: none"> • [契約情報] を確認できます。 • [パスワード変更] で、アカウントパスワードを変更できます。

機能権限	詳細
	<ul style="list-style-type: none"> • [アカウント管理] > [アカウント] で、アカウントの作成／編集ができます。 • [アカウント管理] > [ロール] で、ロールの作成／編集ができます。 • [アカウント管理] > [操作履歴] で、管理コンソールの操作履歴を確認できます。 • [セキュリティ] > [パスワードポリシー] で、アカウントのパスワードポリシーを設定できます。 • [セキュリティ] > [2 要素認証] で、ログイン時の 2 要素認証を設定できます。 • [セキュリティ] > [IP アドレス制限] で、管理コンソールのアクセス制限ができます。
運用設定ができる	<ul style="list-style-type: none"> • [ルール] > [デバイス設定] > [基本設定] の「共通」を設定／変更できます。 • [ルール] > [デバイス設定] > [デバイスグループ設定] で、デバイスグループの作成／編集ができます。 • [ルール] > [デバイス設定] > [基本設定] の [iOS] で、「デバイス表示設定」を設定できます。 • [ルール] > [デバイス設定] > [基本設定] の [Android] で、「マルチユーザー機能制御」を設定できます。 • [ルール] > [デバイス設定] > [基本設定] の [Windows] で、「アンインストール防止設定」を設定できます。 • [レシピ] で、次のアクションを利用した、レシピの作成／編集／実行ができます。 <p>アクション</p> <ul style="list-style-type: none"> • 管理者にメールでお知らせする <div style="background-color: #ffe6e6; padding: 10px; margin: 10px 0;"> <p>注意</p> <p>トリガー設定が含まれている権限も同時に設定してください。</p> </div> <ul style="list-style-type: none"> • [ルール] > [Android Enterprise 設定] で、Android Enterprise の利用申請ができます。
資産情報を管理できる	<ul style="list-style-type: none"> • [リスト] > [デバイス] で、デバイス／周辺機器の追加や、デバイス情報の登録／編集／削除ができます。 • [リスト] > [デバイス] で、デバイス情報をインポートできます。 • [リスト] > [デバイス] で、任意項目表示名の設定／編集ができます。 • [レシピ] で、レシピの作成／編集／実行／削除ができます。

機能権限	詳細
	<ul style="list-style-type: none"> • [レシピ] の作成／編集から、次のトリガー／アクションを選択できます。 <p>トリガー</p> <ul style="list-style-type: none"> • LANSCOPE クライアントがインストールされた • パスワードポリシーに準拠していない • デバイスが管理外になっている • LANSCOPE Client のバージョンが最新になっていない • 任意のタイミングで実行する • 定期的に行う • 未稼働期間が指定された期間を超過している • 指定したアプリがインストールされている • 指定したアプリがインストールされていない • パスコードロックの設定がオフになっている • デバイスが不正に改造されている (root 化／Jailbreak) • SIM カードが抜き差しされた • デバイスの設定がリモート操作の実行条件を満たしていない • iOS のバージョンが指定した範囲外になっている • Android のバージョンが指定した範囲外になっている • もうすぐリース切れになる • ログが取得されない設定になっている • 空き容量が不足している • 新しくプロファイルがインストールされた • 位置情報が取得されない設定になっている <p>アクション</p> <ul style="list-style-type: none"> • 指定プロファイルを配信する • 指定アプリを配信する • 指定プロビジョニングプロファイルを配信する • 指定 VPP アプリを配信する • メッセージを配信する • アンケートを配信する • アラートレポートを送信する

機能権限	詳細
	<ul style="list-style-type: none"> • 指定プロファイルを取り除く • 指定アプリをアンインストールする • 指定プロビジョニングプロファイルを取り除く • 指定 VPP アプリをアンインストールする <ul style="list-style-type: none"> • [ルール] > [Apple サービス設定] > [MDM 証明書設定] で、登録/更新/削除ができます。 • [ルール] > [Apple サービス設定] > [iOS 設定] > [DEP 設定] で、DEP 登録と DEP に関わる設定ができます。 • [ルール] > [Apple サービス設定] > [iOS 設定] > [VPP 設定] で、VPP 登録と VPP に関わる設定ができます。 • [ルール] > [Apple サービス設定] > [iOS 設定] > [基本設定] で、デバイスにインストールするアプリに関わる設定ができます。 • [ルール] > [Apple サービス設定] > [iOS 設定] > [アプリ配信設定] で、デバイスにアプリをインストール/アンインストールする設定ができます。 • [ルール] > [Apple サービス設定] > [macOS 設定] > [DEP 設定] で、DEP 登録と DEP に関わる設定ができます。
<p>ファイル配信設定ができる</p> <p>Windows</p>	<ul style="list-style-type: none"> • [ルール] > [配信設定] > [ファイル配信設定 (Windows)] で、アプリやファイルの配信設定の追加/編集/削除ができます。また、配信結果を確認できます。
<p>資産系アラートが設定できる</p>	<ul style="list-style-type: none"> • [レシピ] で、レシピの作成/編集/実行/削除ができます。 • [レシピ] の作成/編集から、次のトリガー/アクションを選択できます。 <p>トリガー</p> <ul style="list-style-type: none"> • パスワードポリシーに準拠していない • デバイスが管理外になっている • LANSKOPE Client のバージョンが最新になっていない • 未稼働期間が指定された期間を超過している • 指定したアプリがインストールされている • 指定したアプリがインストールされていない • パスコードロックの設定がオフになっている • デバイスが不正に改造されている (root 化/Jailbreak) • 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 • iOS のバージョンが指定した範囲外になっている

機能権限	詳細
	<ul style="list-style-type: none"> Android のバージョンが指定した範囲外になっている SIM カードが抜き差しされた もうすぐリース切れになる ログが取得されない設定になっている 空き容量が不足している 新しくプロファイルがインストールされた 位置情報が取得されない設定になっている <p>アクション</p> <ul style="list-style-type: none"> アラートに設定する <ul style="list-style-type: none"> 「デバイス情報」カテゴリのトリガーで、アラート設定のレシピを作成できます。 [ルール] > [デバイス設定] > [基本設定] の [Android] で、「デバイスへの通知設定」の「資産アラートの通知」を設定できます。
<p>資産系アラートを確認できる</p>	<ul style="list-style-type: none"> 「デバイス詳細」画面の「アラート」で、「デバイス情報」カテゴリがトリガーのアラートを確認できます。 [リスト] > [アラート] で、「デバイス情報」カテゴリのアラートを確認できます。 [レポート] > [利用状況] で、「セキュリティレベルの低いデバイス」レポートを確認できます。
<p>リモート操作の結果を通知できる</p>	<ul style="list-style-type: none"> [レシピ] で、レシピの作成／編集／実行／削除ができます。 [レシピ] の作成／編集から、次のトリガー／アクションを選択できます。 <p>トリガー</p> <ul style="list-style-type: none"> リモートロックの実行が成功した <p>アクション</p> <ul style="list-style-type: none"> 管理者にメールでお知らせする
<p>紛失モード・パスコードオフを実行できる</p>	<ul style="list-style-type: none"> 「デバイス詳細」画面の「リモート操作」で、「紛失モード」「パスコードオフ」を実行できます。 iOS 「デバイス詳細」画面の「リモート操作」で、「パスワードを再設定」を実行できます。 Android
<p>操作ログの取得設定ができる</p> <p>iOS Android</p>	<ul style="list-style-type: none"> [ルール] > [デバイス設定] > [基本設定] で、「デバイスへの通知設定 (iOS/Android)」を設定できます。

機能権限	詳細
デバイスの PC 操作ログ 設定ができる  	<ul style="list-style-type: none"> • [ルール] > [デバイス設定] > [PC 操作ログ設定] で、ルールの追加/閲覧/編集/削除ができます。
操作ログを確認できる  	<ul style="list-style-type: none"> • 「デバイス詳細」画面で、操作ログを確認できます。 • [レポート] > [利用状況] で、「デバイスの利用時間」「電話の利用時間」「カテゴリ別のアプリ利用時間」レポートを確認できます。 • [レシピ] で、レシピの作成/編集/実行/削除ができます。 • [レシピ] の作成/編集から、次のトリガー/アクションを選択できます。 <p>トリガー</p> <ul style="list-style-type: none"> • 定期的に行う <p>アクション</p> <ul style="list-style-type: none"> • 操作ログを一括で出力する <ul style="list-style-type: none"> • [レシピ] > [アクション] の「操作ログを一括で出力する」で、出力データをダウンロードできます。
記録メディアの制御設定 ができる  	<ul style="list-style-type: none"> • [ルール] > [記録メディア制御] で、記録メディアを許可/読み取り専用/禁止に設定できます。
Windows の更新設定が できる 	<ul style="list-style-type: none"> • [レポート] > [Windows アップデート] で、「OS のサポートが終了しているデバイス」「月例パッチ（サーバー）が未適用のデバイス」「月例パッチ（クライアント）が未適用のデバイス」レポートを確認できます。 • [ルール] > [配信設定] > [OS アップデート（Windows）] で、アップデート状況を確認し、インストール設定ができます。
操作系アラートが設定 できる	<ul style="list-style-type: none"> • [レシピ] で、レシピの作成/編集/実行/削除ができます。 • [レシピ] の作成/編集から、次のトリガー/アクションを選択できます。 <p>トリガー</p> <ul style="list-style-type: none"> • 新しくアプリがインストールされた • 指定したアプリが実行された • 不正な Web サイトが閲覧された • SD カードが抜き差しされた • タイムゾーンが変更された

機能権限	詳細
	<p>アクション</p> <ul style="list-style-type: none"> アラートに設定する <ul style="list-style-type: none"> [ルール] > [デバイス設定] > [基本設定] の [Android] で、「デバイスへの通知設定」の「資産アラートの通知」を設定できます。
<p>操作系アラートを確認できる</p>	<ul style="list-style-type: none"> 「デバイス詳細」画面の「アラート」で、「操作ログ情報」カテゴリがトリガーのアラートを確認できます。 [リスト] > [アラート] で、「操作ログ情報」カテゴリのアラートを確認できます。 [レポート] > [利用状況] で、「セキュリティレベルの低いデバイス」レポートを確認できます。
<p>位置情報の取得設定ができる</p>	<ul style="list-style-type: none"> [ルール] > [デバイス設定] > [基本設定] で、「位置情報ログ取得設定 (iOS/Android/Windows)」を設定できます。
<p>位置情報を確認できる</p>	<ul style="list-style-type: none"> 「デバイス詳細」画面の「位置情報 (iOS/Android/Windows)」で、移動履歴を確認できます。 [モニター] > [最新位置情報] を確認できます。 [レシピ] で、レシピの作成/編集/実行/削除ができます。 [レシピ] の作成/編集から、次のトリガー/アクションを選択できます。 <p>トリガー</p> <ul style="list-style-type: none"> 定期的に行う <p>アクション</p> <ul style="list-style-type: none"> 位置情報を一括で出力する <ul style="list-style-type: none"> [レシピ] > [アクション] の「位置情報を一括で出力する」で、出力データをダウンロードできます。
<p>リモートロックを実行できる</p>	<ul style="list-style-type: none"> 「デバイス詳細」画面の「リモート操作」で、リモートロックを実行できます。
<p>リモートワイプを実行できる</p>	<ul style="list-style-type: none"> 「デバイス詳細」画面の「リモート操作」で、リモートワイプを実行できます。
<p>デバイスポリシーが管理できる</p> <p>Android</p>	<ul style="list-style-type: none"> [ルール] > [Android Enterprise 設定] > [基本設定] で、デバイスポリシーを設定できます。
<p>アプリポリシーが管理できる</p> <p>Android</p>	<ul style="list-style-type: none"> [ルール] > [Android Enterprise 設定] > [基本設定] で、アプリポリシーを設定できます。

機能権限	詳細
キオスクモードが管理できる Android	<ul style="list-style-type: none"> • [ルール] > [Android Enterprise 設定] > [基本設定] で、キオスクモードを設定できます。
Android Enterprise にデバイスを登録できる Android	<ul style="list-style-type: none"> • [ルール] > [Android Enterprise 設定] > 「デバイス登録」で、Android Enterprise にデバイスを登録できます。
ヘルプを表示できる	<ul style="list-style-type: none"> • ユーザー様向けページを表示できます。

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：

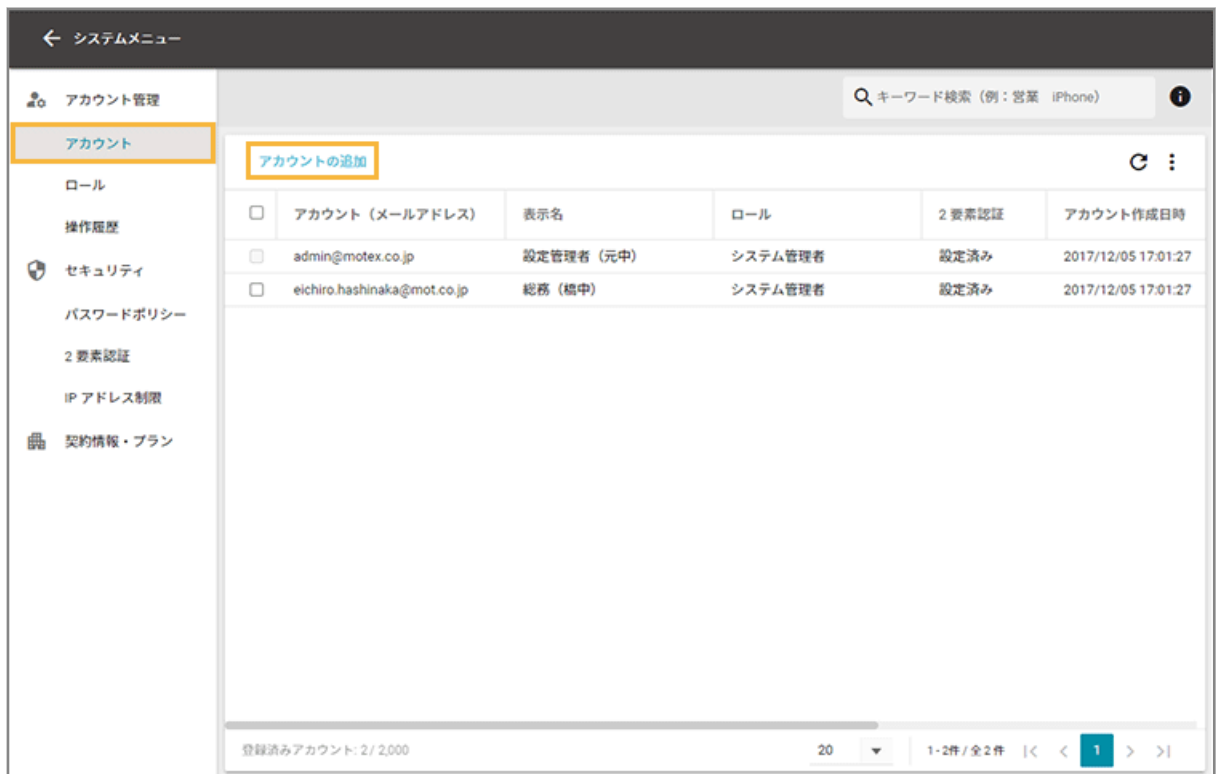
100 ライセンス保有している場合、「 $100 \div 5 + 4$ 」 = 24 アカウントを作成できます。

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。

アカウントの追加

アカウント (メールアドレス) *

 アカウントを識別するために使用されるメールアドレスです。このメールアドレスは変更できません。

表示名 *

ロール *
 選択

パスワード *

 16～64文字以下の半角英数記号で入力してください。
 英小文字、英大文字、数字、記号 (@#\$%&* など) の4種のうち、3つ以上を含む、かつ同じ文字の連続は2つ以下の値を入力してください。

パスワード確認用 *

[ランダムなパスワードを自動で生成する](#)

アクセス許可

- ネットワーク全体
 - 総務課
 - 人事課
 - ▶ 営業部
 - ▶ システム部
 - ▶ サポートセンター
 - ▶ 運輸部
 - 検証用

アカウント情報をメールで送信する
 作成するアカウントの情報を入力されたメールアドレスに送信します。

送信されるメッセージ [↑](#)

haruka.tokunaga様

現在、社内で利用しているスマートフォン、タブレットPCを LANSCOPE で管理をすることになりました。
 本日から LANSCOPE の管理コンソールが利用可能です。

 コンソールURL : <https://motex-items.lanscope.com/ids/>
 アカウント : haruka.tokunaga@motex.co.jp
 パスワード :

※ パスワードは、ログイン後に変更できます。

 ご不明な点がございましたら、設定管理者 (元中) (admin@motex.co.jp) までご連絡下さい。
 ※ このメールは配信専用です。返信はできませんのでご了承ください。

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

ロールを選択します。

ロールについては、[機能権限](#)を参照してください。

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。

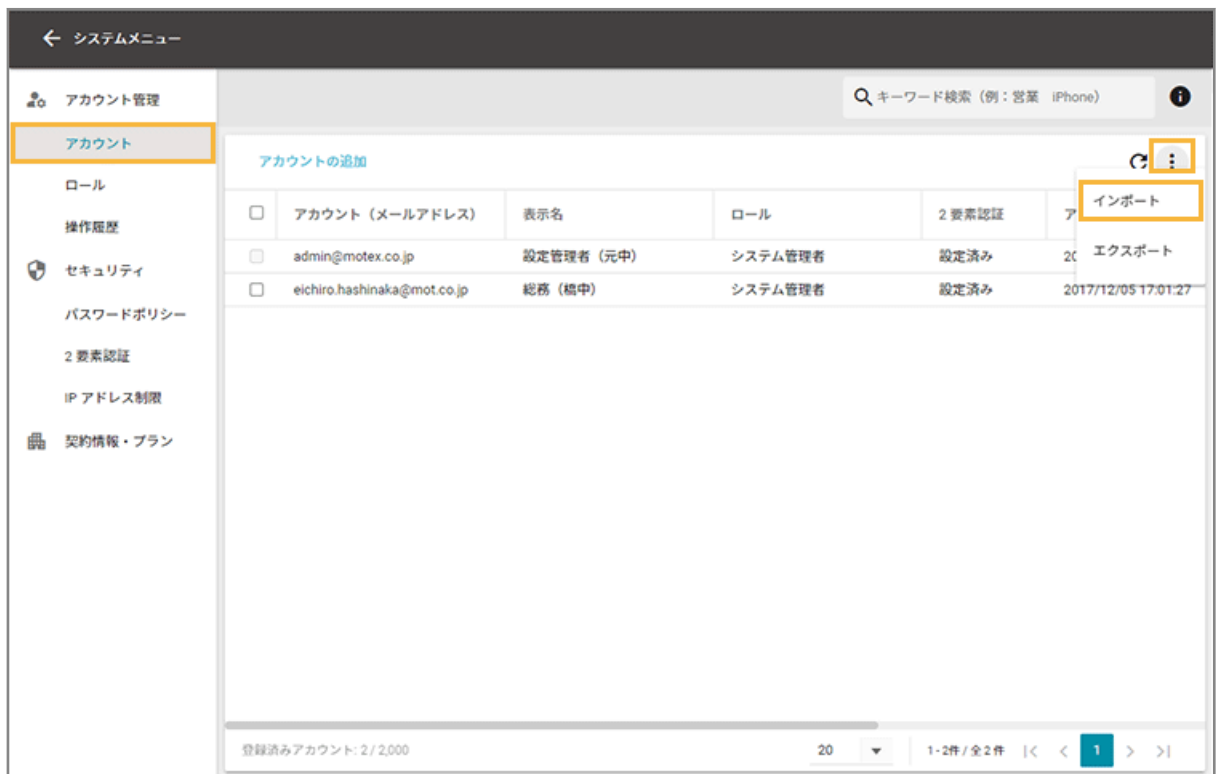
→ アカウントが追加されます。

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

ロールを設定します。

ロールの作成は、[機能権限](#)を参照してください。

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。

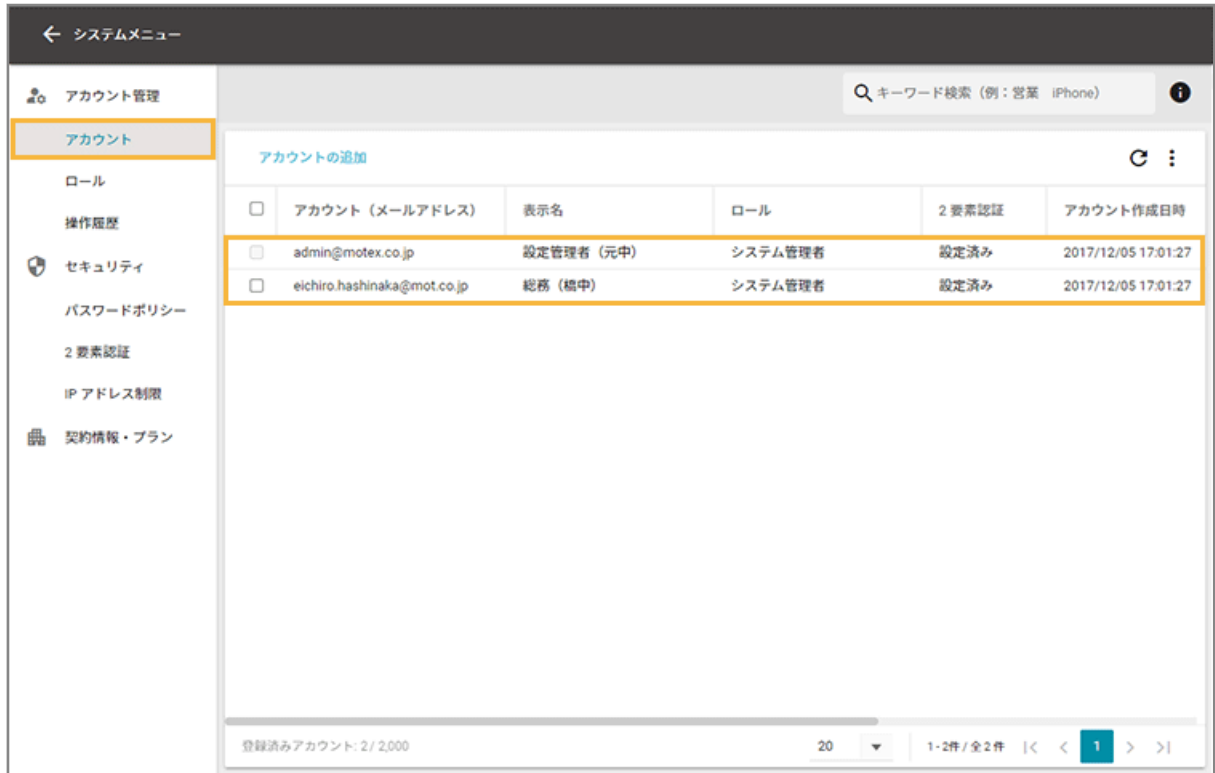
注意

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。

総務 (橋中) (eichiro.hashinaka@mot.co.jp) - アカウント詳細

基本情報 キャンセル 保存

アクセス許可

パスワード

2要素認証

アカウント (メールアドレス) ⓘ
eichiro.hashinaka@mot.co.jp

表示名 *
総務 (橋中)

ロール *
選択

システム管理者 ×

作成日時
2017/12/05 17:01:27

最終ログイン日時
-

閉じる

→ 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

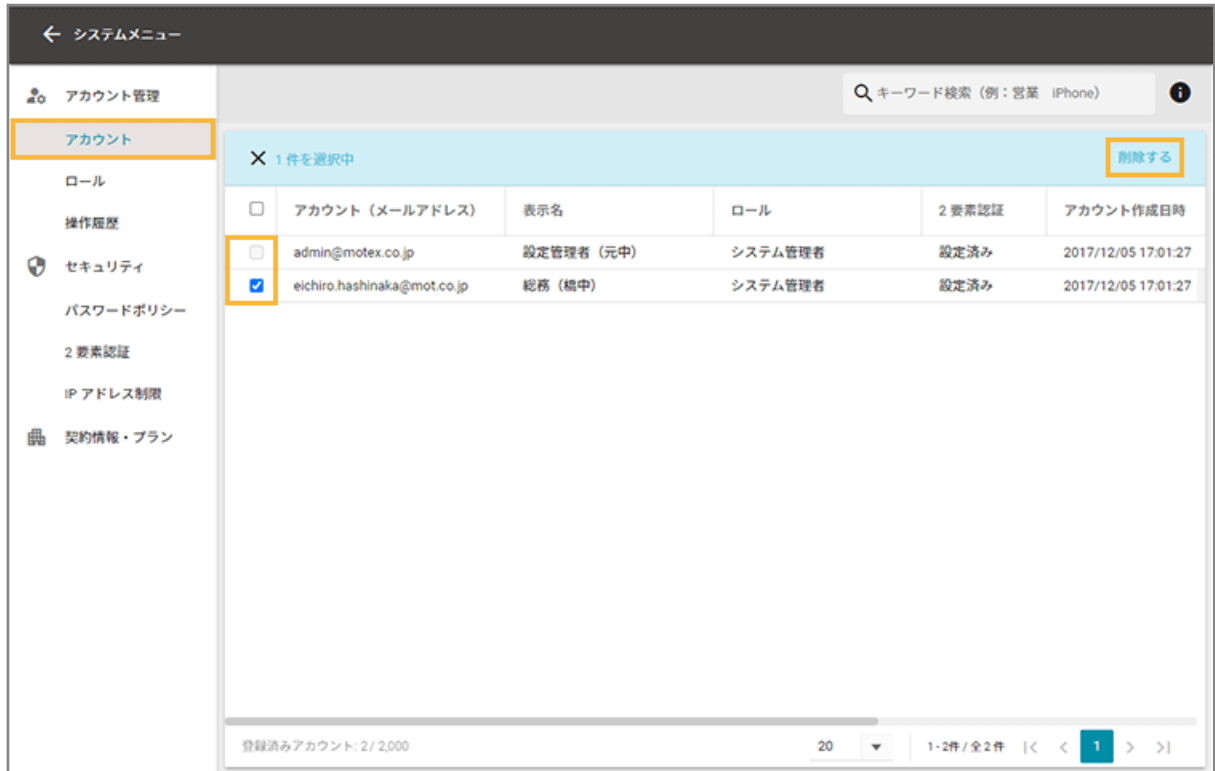
注意

ログインアカウント（メールアドレス）は削除できません。

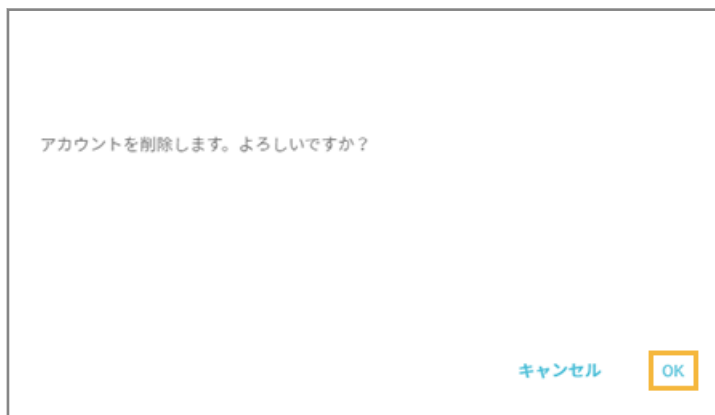
1.  をクリックし、[アカウント管理] をクリックします。




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。

ロールを管理する

iOS Android Windows macOS

アカウントに設定するロールの作成／編集／削除ができます。

■ ロールを追加する

ポイント

- ロールの作成では、必ず 1 つは機能権限を選択してください。機能権限が付与されていないロールを適用したアカウントではログインできません。
- 作成できるロール数に上限はありません。

1.  をクリックし、[アカウント管理] をクリックします。



2. [ロール] をクリックし、[ロールの追加] をクリックします。



3. ロール名を入力し、付与する機能権限をチェックして、[追加] をクリックします。

ロールの追加

ロール名 *

すべてチェック すべてはずす

機能権限

- アカウント管理ができる
- 運用設定ができる
- 資産情報を管理できる
- ファイル配信設定ができる (Windows)
- 資産系アラートが設定できる
- 資産系アラートを確認できる
- リモート操作の結果を通知できる
- 紛失モード・パスコードオフを実行できる
- 操作ログの取得設定ができる (iOS / Android)
- デバイスの PC 操作ログ設定ができる (Windows / macOS)
- 操作ログを確認できる (iOS / Android)
- 操作ログを確認できる (Windows / macOS)
- 使用状況を確認できる (Windows / macOS)
- レポートの集計設定ができる (Windows / macOS)
- 記録メディアの制御設定ができる (Windows / macOS)
- Windowsの更新設定ができる
- 操作系アラートが設定できる
- 操作系アラートを確認できる
- 位置情報の取得設定ができる
- 位置情報を確認できる
- リモートロックを実行できる
- リモートワイプを実行できる
- デバイスポリシーが管理できる
- アプリポリシーが管理できる
- キオスクモードが管理できる
- Android Enterpriseにデバイスを登録できる
- ヘルプを表示できる

キャンセル 追加

→ ロールが追加されます。

■ ロール情報を編集する

注意

事前に設定されているロール名「システム管理者」は、編集できません。

1.  をクリックし、[アカウント管理] をクリックします。



2. [ルール] をクリックし、編集するルールをクリックします。



3. [編集] をクリックします。

ロールの編集

編集

ロール名
資産管理担当者用

機能権限
資産情報を管理できる / 資産系アラートが設定できる / 資産系アラートを確認できる

閉じる

4. 内容を編集し、[保存] をクリックします。

ロールの編集

キャンセル 保存

ロール名*
資産管理担当者用

すべてチェック すべてはずす

機能権限

- アカウント管理ができる
- 運用設定ができる
- 資産情報を管理できる
- ファイル配信設定ができる (Windows)
- 資産系アラートが設定できる
- 資産系アラートを確認できる
- リモート操作の結果を通知できる
- 紛失モード・パスコードオフを実行できる
- 操作ログの取得設定ができる (iOS / Android)
- デバイスのPC 操作ログ設定ができる (Windows / macOS)
- 操作ログを確認できる (iOS / Android)
- 操作ログを確認できる (Windows / macOS)
- 使用状況を確認できる (Windows / macOS)
- レポートの集計設定ができる (Windows / macOS)
- 記録メディアの制御設定ができる (Windows / macOS)
- Windowsの更新設定ができる
- 操作系アラートが設定できる
- 操作系アラートを確認できる
- 位置情報の取得設定ができる
- 位置情報を確認できる
- リモートロックを実行できる
- リモートワイプを実行できる
- デバイスポリシーが管理できる
- アプリポリシーが管理できる
- キオスクモードが管理できる
- Android Enterpriseにデバイスを登録できる
- ヘルプを表示できる

閉じる

→ 編集内容が保存されます。

■ ロールを削除する

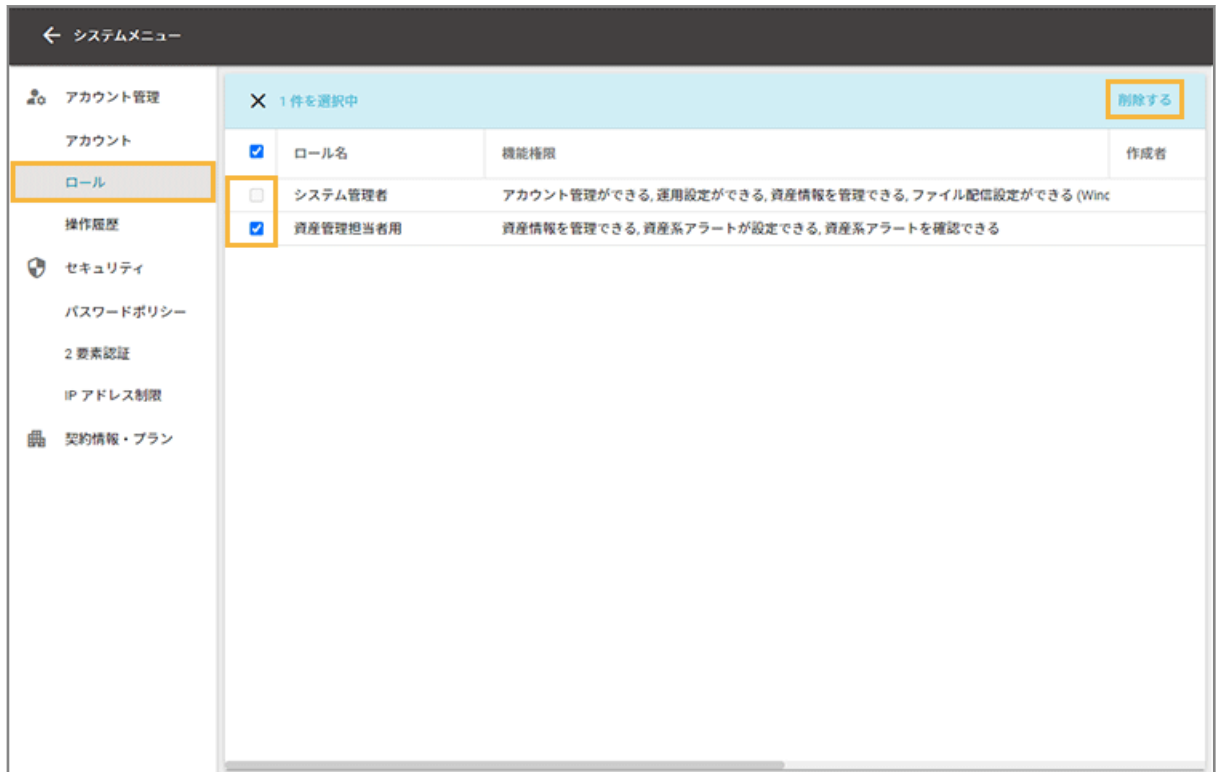
注意

事前に設定されているロール名「システム管理者」は、削除できません。

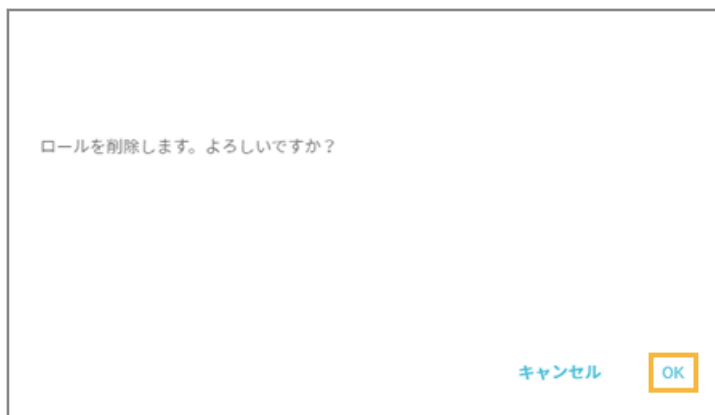
1.  をクリックし、[アカウント管理] をクリックします。



2. [ルール] をクリックし、削除するルールをチェックして、[削除する] をクリックします。



3. [OK] をクリックします。



→ ルールが削除されます。

操作履歴を確認する

アカウントが管理コンソールでどのような操作をしたかを確認します。

ポイント

- 「アカウント管理ができる」の機能権限をもつロールを適用しており、「ネットワーク全体」のアクセス許可があるアカウントで確認できます。
- 操作履歴の保存期間は 367 日です。


注意

- ネットワークの通信状況によっては、一部の操作履歴を記録できないことがあります。
- アカウントがロックアウトされている間のログイン操作は、操作履歴として記録されません。
- IPv6 を有効にしているネットワークから管理コンソールにアクセスした場合、ログイン/ログアウト操作の「アクセス元 IP アドレス」に、IPv6 形式の IP アドレスが記録されることがあります。

1.  をクリックし、[アカウント管理] をクリックします。



2. [操作履歴] をクリックし、操作履歴を確認します。

- 表示できる操作履歴は、最大 10,000 件です。
- 特定の期間を確認する場合は、期間を指定し、 をクリックします。

日時	アカウント (メールアドレス)	表示名	画面	操作
2023/07/11 10:54:52	admin@motex.co.jp	設定管理者 (元中)		ロ
2023/07/11 10:55:04	admin@motex.co.jp	設定管理者 (元中)	リスト > デバイス	開
2023/07/11 10:56:04	admin@motex.co.jp	設定管理者 (元中)	ルール > デバイス設定	開
2023/07/11 10:57:04	admin@motex.co.jp	設定管理者 (元中)	ルール > MDM 証明書設定	開
2023/07/11 10:58:04	admin@motex.co.jp	設定管理者 (元中)	ルール > MDM 証明書設定 > MDM 証明書...	更
2023/07/11 11:03:28	yuzo.motogishi@mot.co.jp	システム (元岸)		ロ
2023/07/11 11:03:32	yuzo.motogishi@mot.co.jp	システム (元岸)	リスト > デバイス	開
2023/07/11 11:03:40	yuzo.motogishi@mot.co.jp	システム (元岸)	リスト > デバイス > デバイス詳細 > 管理情...	開
2023/07/11 11:12:45	yuzo.motogishi@mot.co.jp	システム (元岸)		ロ
2023/07/11 13:30:11	mayumi.nakata@mot.co.jp	営業 (中田)		ロ
2023/07/11 13:33:20	mayumi.nakata@mot.co.jp	営業 (中田)	リスト > デバイス	開
2023/07/11 13:50:35	mayumi.nakata@mot.co.jp	営業 (中田)		ロ
2023/07/11 14:18:23	admin@motex.co.jp	設定管理者 (元中)	リスト > デバイス	開
2023/07/11 14:18:26	admin@motex.co.jp	設定管理者 (元中)	リスト > デバイス > デバイス詳細 > リモ...	開

3. 表示されている操作履歴をダウンロードする場合、 をクリックします。


- ダウンロードできる操作履歴は、最大 10,000 件です。
- 検索／並び替えした状態でダウンロードします。

日時	アカウント (メールアドレス)	表示名	画面	操作
2023/07/11 10:54:52	admin@motex.co.jp	設定管理者 (元中)		ロ
2023/07/11 10:55:04	admin@motex.co.jp	設定管理者 (元中)	リスト > デバイス	開
2023/07/11 10:56:04	admin@motex.co.jp	設定管理者 (元中)	ルール > デバイス設定	開
2023/07/11 10:57:04	admin@motex.co.jp	設定管理者 (元中)	ルール > MDM 証明書設定	開
2023/07/11 10:58:04	admin@motex.co.jp	設定管理者 (元中)	ルール > MDM 証明書設定 > MDM 証明書...	更
2023/07/11 11:03:28	yuzo.motogishi@mot.co.jp	システム (元岸)		ロ
2023/07/11 11:03:32	yuzo.motogishi@mot.co.jp	システム (元岸)	リスト > デバイス	開
2023/07/11 11:03:40	yuzo.motogishi@mot.co.jp	システム (元岸)	リスト > デバイス > デバイス詳細 > 管理情...	開
2023/07/11 11:12:45	yuzo.motogishi@mot.co.jp	システム (元岸)		ロ
2023/07/11 13:30:11	mayumi.nakata@mot.co.jp	営業 (中田)		ロ
2023/07/11 13:33:20	mayumi.nakata@mot.co.jp	営業 (中田)	リスト > デバイス	開
2023/07/11 13:50:35	mayumi.nakata@mot.co.jp	営業 (中田)		ロ
2023/07/11 14:18:23	admin@motex.co.jp	設定管理者 (元中)	リスト > デバイス	開
2023/07/11 14:18:26	admin@motex.co.jp	設定管理者 (元中)	リスト > デバイス > デバイス詳細 > リモ...	開

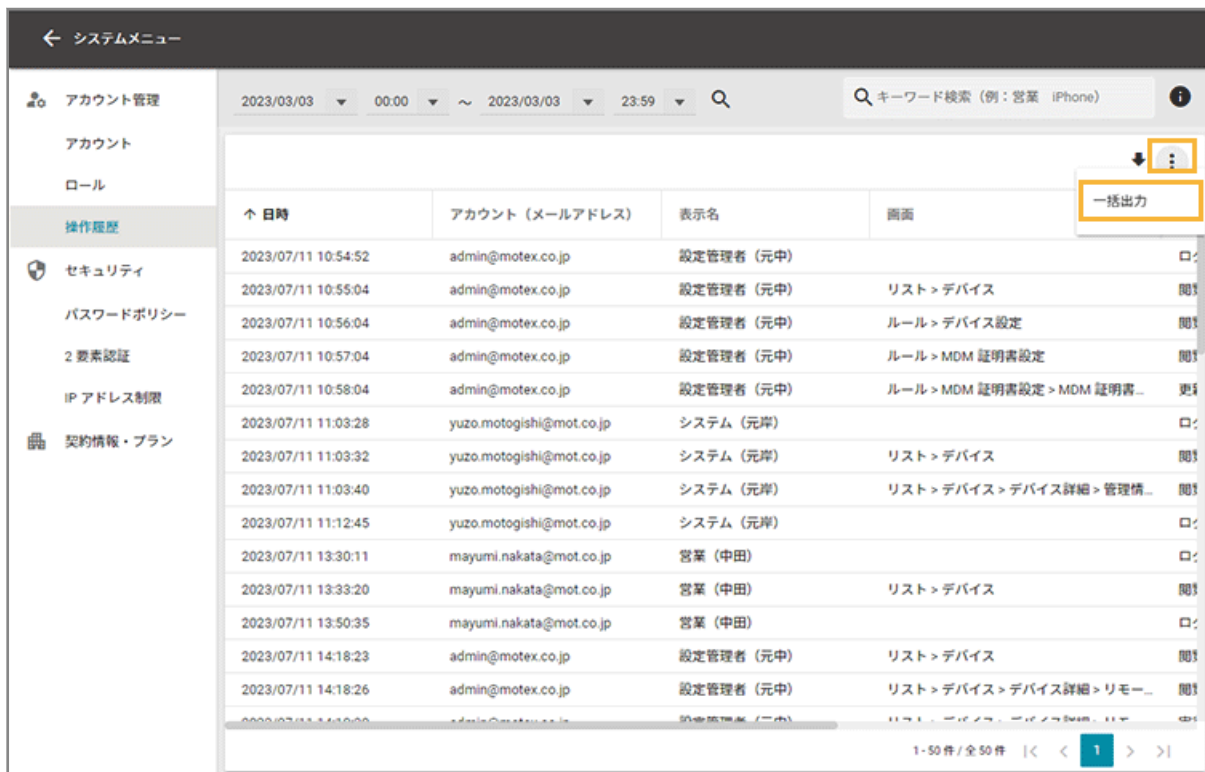
→ CSV ファイルのダウンロードが完了します。

4. 指定した期間のすべての操作履歴をダウンロードする場合は、次の操作をします。

ダウンロードできる操作履歴は、最大 1,000,000 件です。

(1)  をクリックし、[一括出力] をクリックします。

操作履歴の一括出力は、複数のアカウントで同時に実行することができません。



(2) 出力期間を選択し、[ファイル出力] をクリックします。



(3) ファイル出力が完了したら、[ダウンロード] をクリックします。

ダウンロードの有効期限は、7 日です。



→ zip ファイルのダウンロードが完了します。


1-5 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](#)
- [IPアドレス制限をする](#)

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。

パスワードポリシー キャンセル **保存**

パスワード強度 *

弱い
パスワードの最小文字数: 8 ~ 16
使用しなければならない文字の種類: 問わない

標準
パスワードの最小文字数: 8 ~ 16
使用しなければならない文字の種類: 英小文字、英大文字、数字を含む

強い
パスワードの最小文字数: 8 ~ 16
使用しなければならない文字の種類: 英小文字、英大文字、数字、記号 (@#%*&* など) の4種のうち、3つ以上を含む

非常に強い
パスワードの最小文字数: 10 ~ 16
使用しなければならない文字の種類: 英小文字、英大文字、数字、記号 (@#%*&* など) の4種のうち、3つ以上を含む、かつ同じ文字の連続は2つ以下

パスワードの最小文字数 *

16文字

パスワードの有効期間

設定する

有効期間 (日) (1~365日) *

20

以前使用したパスワードの再使用

制限する

禁止するパスワードの世代数 *

2世代前

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。

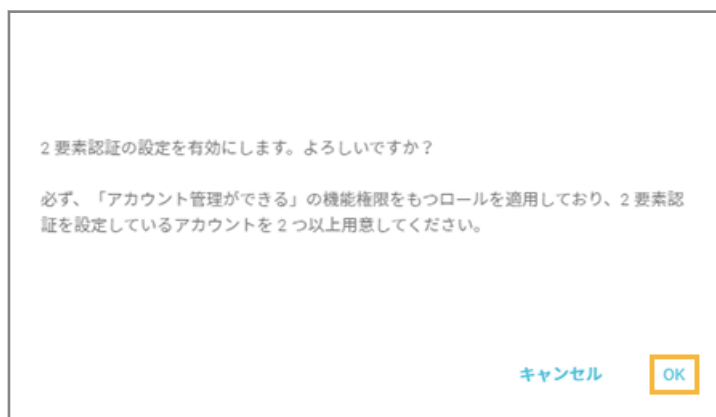
1.  をクリックし、[セキュリティ] をクリックします。



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스에 인증 앱을 설치합니다.

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。



LANSCOPE
Endpoint Manager

アカウント

パスワード

パスワードの設定はこちら

ログイン

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。



LANSCOPE
Endpoint Manager

新しいパスワードの設定

初めてのログインのため、パスワードを変更する必要があります。

新しいパスワード

新しいパスワード確認用

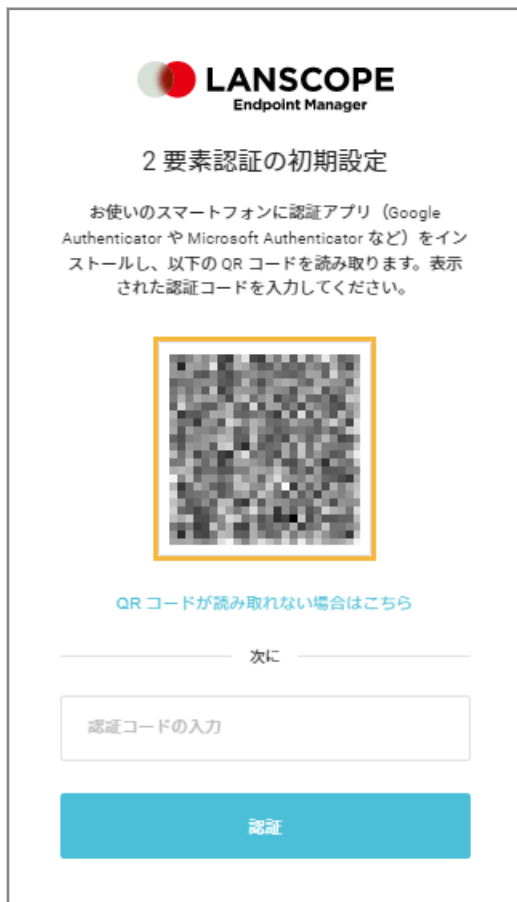
ランダムなパスワードを自動で生成する

パスワードを変更する

- (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。

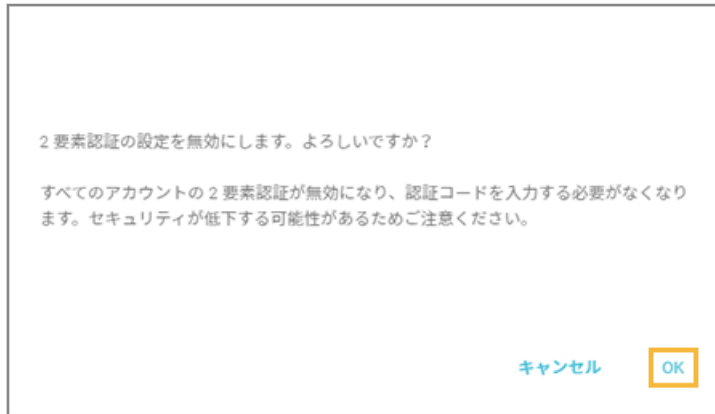
1.  をクリックし、[セキュリティ] をクリックします。



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。

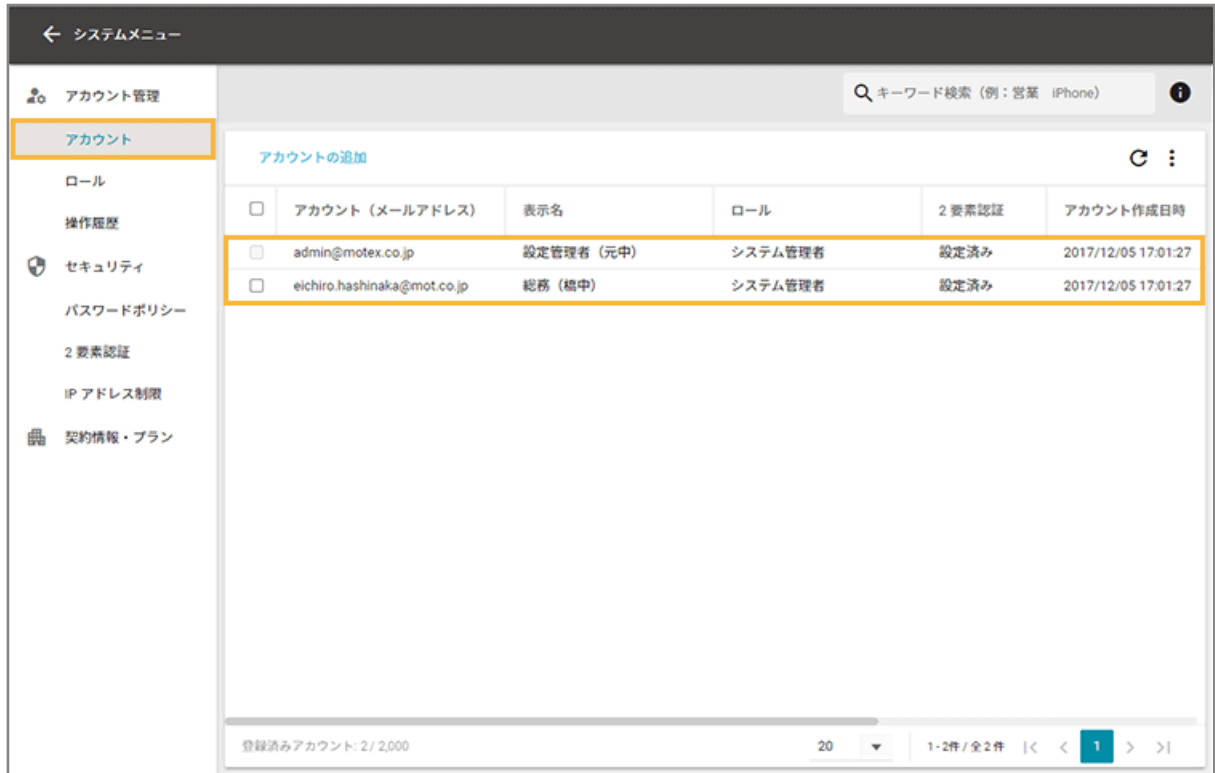
■ 2要素認証を初期化して認証デバイスを変更する

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。



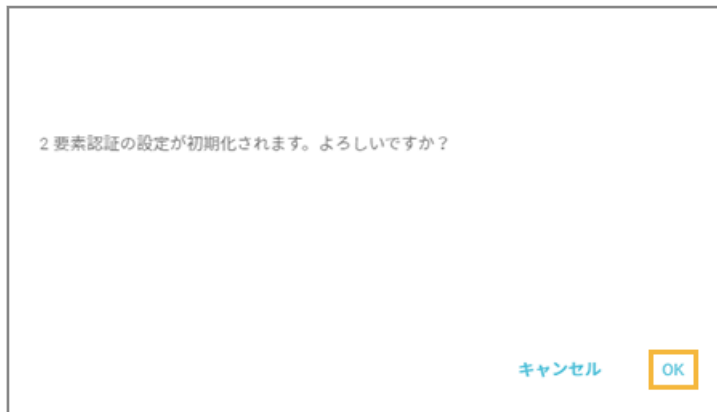
2. [アカウント] をクリックし、初期化するアカウントをクリックします。



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。

IP アドレス制限をする

管理コンソールにアクセスできる IP アドレスを制限します。

ポイント


IP アドレスを 1 件以上追加すると、管理コンソールのアクセス制限が有効になります。IP アドレスを追加していない場合は、アクセス制限は無効です。

■ IP アドレスを追加する

IP アドレスを追加して、管理コンソールのアクセス制限を有効にします。

ポイント

- 必ずアクセス中の IP アドレスを追加してください。追加しなかった場合は、自動的にログアウトし、ログインできなくなります。
- IP アドレスは、最大 100 件追加できます。

1.  をクリックし、[セキュリティ] をクリックします。



2. [IP アドレス制限] をクリックし、[IP アドレスの追加] をクリックします。




3. IP アドレスを入力し、[追加] をクリックします。

複数の IP アドレスを追加する場合は、[IP アドレスを追加] をクリックして入力します。



→ IPアドレスの追加が完了します。

■ IPアドレス情報を編集する

1.  をクリックし、[セキュリティ] をクリックします。



2. [IPアドレス制限] をクリックし、編集する IP アドレスをクリックします。



3. [編集] をクリックします。

IP アドレスの編集

編集

IP アドレス
192.168.1.1

メモ
.

閉じる

4. IP アドレス情報を編集して、[保存] をクリックします。

IP アドレスの編集

キャンセル 保存

IP アドレス *

IPv4 形式のグローバル IP アドレスで指定してください。
範囲指定する場合は CIDR 表記 (203.0.113.xxx/1~32) で指定してください。

メモ


閉じる

→ IP アドレス情報の編集が完了します。

■ IP アドレスを削除する

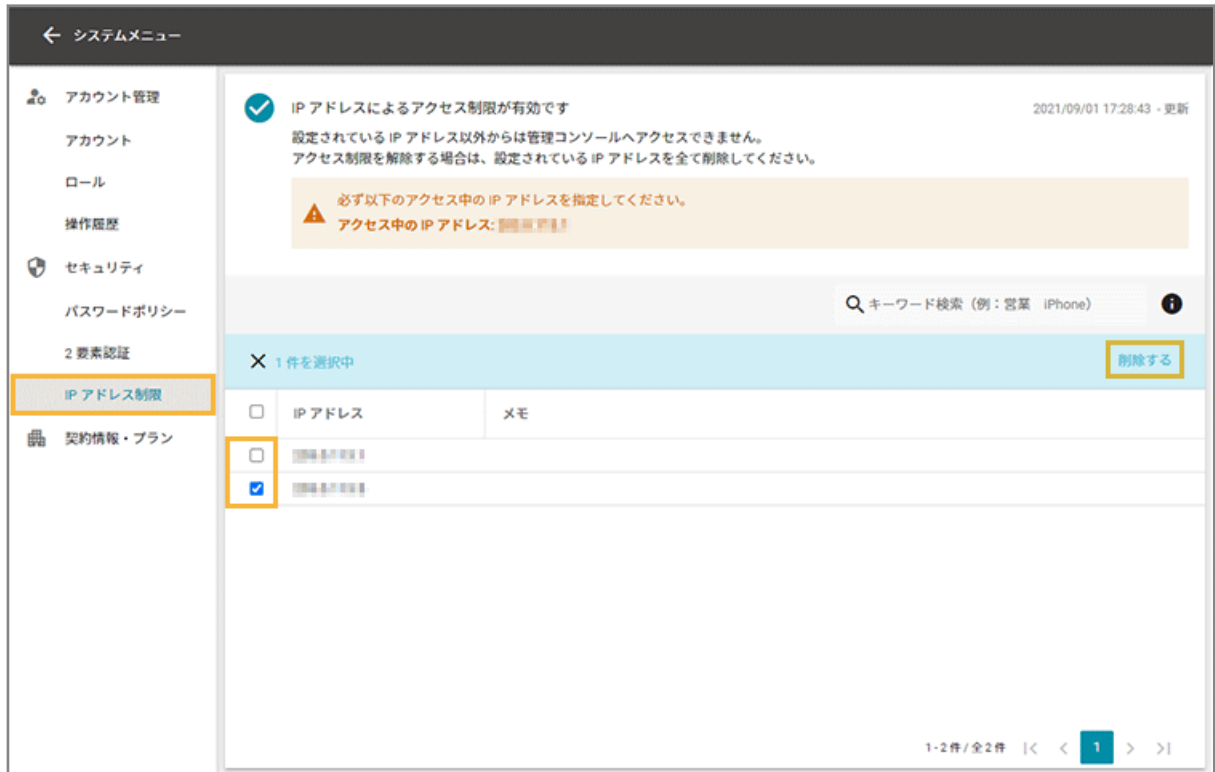
ポイント

- すべての IP アドレスを削除すると、管理コンソールのアクセス制限が無効になります。
- 管理コンソールのアクセス制限を続ける場合は、アクセス中の IP アドレスを削除しないでください。削除すると、自動的にログアウトし、ログインできなくなります。

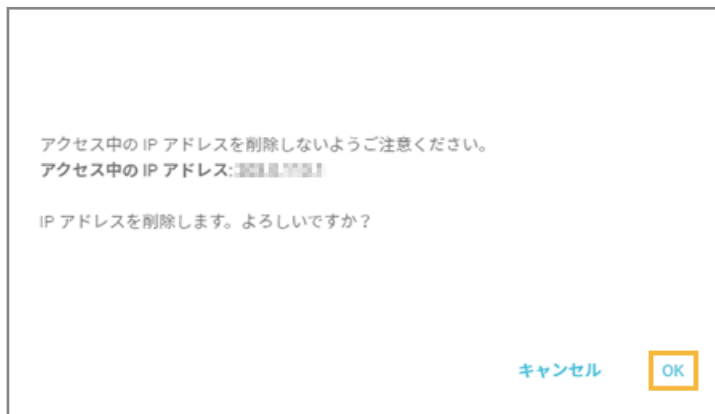
1.  をクリックし、[セキュリティ] をクリックします。



2. **【IP アドレス制限】** をクリックし、削除する IP アドレスをチェックして、**【削除する】** をクリックします。



3. **【OK】** をクリックします。



→ IP アドレスの削除が完了します。

第2章 リストで情報を確認する

iOS

Android

Windows

macOS

デバイス情報や、インストールアプリ情報／アカウント情報など、さまざまな情報を一覧で確認できます。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 操作ログ情報を確認する](#)
- [2-3 リモート操作を実行する](#)
- [2-4 アプリ情報を確認する](#)
- [2-5 プロファイル情報を確認する](#)
- [2-6 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、デバイスや周辺機器などの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](#)
- [デバイスの最新情報を取得する](#)
- [デバイス情報を編集／削除する](#)
- [任意項目表示名を設定／編集する](#)
- [周辺機器情報を追加する](#)

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	<p>基本情報</p> <p>デバイス管理名／デバイスタイプ／Apple ID／使用者名／使用者の社員コード／使用者の組織名／管理者名／管理者の組織名／管理者の組織コード</p> <p>使用状況</p> <p>使用場所／使用者タイプ／使用状況タイプ</p> <p>導入状況</p> <p>導入日／導入責任者／導入金額／導入タイプ／期限（リース／償却）／月額費用／購入先／補償内容</p> <p>棚卸し状況</p> <p>前回棚卸し実施日／前回棚卸し実施者／前回棚卸し実施結果</p> <p>任意項目</p> <p>任意項目 1～20</p>

「デバイス詳細」画面の項目	項目名
デバイスグループ	デバイスグループ
デバイス情報	<p>システム</p> <p>OS バージョン／監視モード／位置情報サービス／LANSCOPE Client 位置情報利用許可／正確な位置情報／紛失モード／iPhone を探す／おやすみモード／アクティベーションロック／iCloud バックアップ／最新 iCloud バックアップ日時／iTunesStore アカウント状態／iTunesStoreIdHash</p> <p>ハードウェア</p> <p>デバイス名／モデル名／シリアル番号／UDID／ストレージ使用容量／通信方式／IMEI／MEID／モデムファームウェア／Exchange デバイス ID／電池残量</p>
ネットワーク	電話番号／MAC アドレス（Wi-Fi）／MAC アドレス（Bluetooth）／加入キャリア／現在のキャリア／キャリア設定バージョン／ICCID／インターネット共有／ローミング／データローミング／音声通話ローミング／カントリーコード／ネットワークコード／SIM カントリーコード／SIM ネットワークコード／現在のカントリーコード／現在のネットワークコード
セキュリティ	Jailbreak／パスコードロック／パスコードポリシー（プロファイル）／パスコード要求までの猶予時間（秒）／ハードウェアの暗号化方式
インストールアプリ	アプリ名／バージョン／管理アプリ／デベロッパー／カテゴリー／アプリケーション ID／アプリサイズ
プロファイル	プロファイル名／作成者／アプリケーション ID／概要
位置情報	移動履歴（地図表示／一覧表示）
操作ログ	時刻／分類／利用時間／内容
アラート	アラート（トリガー）名／アラートレベル
リモート操作	実行履歴（設定日時／実行者／内容／状態／実行日時／メッセージ／電話番号／詳細）
クライアント	MDM 構成プロファイルインストール日時／LANSCOPE クライアント最終稼働日時／LANSCOPE Client インストール日時／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。

■ Android

「デバイス詳細」画面の項目	項目名
管理情報	<p>基本情報</p> <p>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/使用者の組織名/管理者名/管理者の組織名/管理者の組織コード</p> <p>使用状況</p> <p>使用場所/使用者タイプ/使用状況タイプ</p> <p>導入状況</p> <p>導入日/導入責任者/導入金額/導入タイプ/期限（リース/償却）/月額費用/購入先/補償内容</p> <p>棚卸し状況</p> <p>前回棚卸し実施日/前回棚卸し実施者/前回棚卸し実施結果</p> <p>任意項目</p> <p>任意項目 1~20</p>
デバイスグループ	デバイスグループ
デバイス情報	<p>システム</p> <p>OS バージョン/CPU 名/CPU 周波数/メモリ/アカウントのメールアドレス 1~3 (*1) /Android Enterprise デバイス/タイムゾーン/国コード</p> <p>ハードウェア</p> <p>製品名/製造元/ホスト名/モデル名/シリアル番号/内部ストレージ使用容量/外部ストレージ使用容量/IMEI/基盤名/ハードウェア名/ブランド名</p>
ネットワーク	電話番号/MAC アドレス (Wi-Fi) (*2) /Wi-Fi 状態/IP アドレス/デフォルトゲートウェイ/サブネットマスク/DHCP IP アドレス/サーバーアドレス/DNS サーバー/SSID/ネットワーク認証種別/MAC アドレス (Bluetooth) (*3) /Bluetooth アダプタ名/加入キャリア/現在のキャリア/SIM のシリアル番号/SIM の状態/SIM の国コード/
セキュリティ	root 化/パスワードポリシー/USB デバッグ
インストールアプリ	アプリ名/バージョン/プリインストールアプリ/カテゴリ/デベロッパー/パッケージ名/インストール日時
位置情報	移動履歴（地図表示/一覧表示）
操作ログ	時刻/分類/利用時間/内容/詳細 1/詳細 2/カテゴリ/アラート
アラート	アラート（トリガー）名/アラートレベル
リモート操作	実行履歴（設定日時/実行者/内容/状態/実行日時/詳細）
Android Enterprise (*4)	適用されているポリシー/登録日時/ポリシー適用日時/管理モード

「デバイス詳細」画面の項目	項目名
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)

*1 : Google/Exchange アカウントに登録されているメールアドレス情報を取得します。

*2 : [リスト] > [デバイス] 画面で確認する場合は、表示列に「MAC アドレス (NIC)」を追加してください。

*3 : Android 7 以上のデバイスでは、取得できません。

*4 : Android デバイスを、Android Enterprise デバイスとして登録した場合にだけ、表示されます。

■ Windows

「デバイス詳細」画面の項目	項目名
管理情報	<p>基本情報</p> <p>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/使用者の組織名/管理者名/管理者の組織名/管理者の組織コード</p> <p>使用状況</p> <p>使用場所/使用者タイプ/使用状況タイプ</p> <p>導入状況</p> <p>導入日/導入責任者/導入金額/導入タイプ/期限 (リース/償却) /月額費用/購入先/補償内容</p> <p>棚卸し状況</p> <p>前回棚卸し実施日/前回棚卸し実施者/前回棚卸し実施結果</p> <p>任意項目</p> <p>任意項目 1~20</p>
デバイスグループ	デバイスグループ
デバイス情報	<p>システム</p> <p>OS バージョン/OS アーキテクチャ/Windows バージョン (*1) /CPU 名/CPU 周波数/メモリ/ドメイン・ワークグループ名/ログオンユーザー名/ログオンユーザー SID</p> <p>ハードウェア</p> <p>コンピューター名/NetBIOS 名/デバイス名/製品名/製造元/シリアル番号/モデル名/モデムファームウェア/IMEI/システムドライブ/ファイルシステム/ボリューム名/国番号/ストレージ使用容量/プロセッサ数/CPU コア数/ドライブ数/フルネーム</p>

「デバイス詳細」画面の項目	項目名
	(表示名) / Windows プロダクト ID / モデム / SCSI 機器 / BIOS バージョン / Windows サービスパック / Internet Explorer バージョン / IE サービスパック / ドライブ情報 (*2)
ネットワーク	電話番号 / Wi-Fi 状態 / Bluetooth 状態 / NIC 情報 (NIC 名 / NIC の種別 / MAC アドレス / IP アドレス / サブネットマスク / デフォルトゲートウェイ / DNS サーバー) / 現在のキャリア / SIM の状態 / ICCID
セキュリティ	ファイアウォール状態 / Windows アップデート / アンチウイルス状態 / アンチウイルス更新ステータス / リモートワイプ実行可否 / BitLocker 回復キー (*3) / Defender パターンバージョン / Defender エンジンバージョン / Defender バージョン / CylancePROTECT バージョン / CylancePROTECT モード / Deep Instinct バージョン / Deep Instinct 連携設定
インストールアプリ	アプリ名 / バージョン / デベロッパー / パッケージ名 / インストール日時 / アプリ種別
Microsoft Office	Microsoft Office 情報一覧 (*4)
位置情報	移動履歴 (地図表示 / 一覧表示) (*5)
レポート	業務時間内外のデバイス利用状況 / カテゴリ別のアプリ利用状況 / アプリ利用時間ランキング / Web アクセス時間ランキング
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 (*6)

*1 : Windows 11 / 10 以外では取得できません。

*2 : 最大 26 項目表示します。

*3 : リモートワイプができないデバイスは、情報を取得できない場合があります。

*4 : パッケージとしてインストールされている Microsoft Office 2016 / 2013 / 2010 / 2007 の情報を取得します。

Microsoft 365 の情報は取得できません。

*5 : Windows Server OS では、位置情報を取得できません。

*6 : 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	<p>基本情報</p> <p>デバイス管理名/デバイスタイプ/Apple ID/使用者名/使用者の社員コード/使用者の組織名/管理者名/管理者の組織名/管理者の組織コード</p> <p>使用状況</p> <p>使用場所/使用者タイプ/使用状況タイプ</p> <p>導入状況</p> <p>導入日/導入責任者/導入金額/導入タイプ/期限（リース/償却）/月額費用/購入先/補償内容</p> <p>棚卸し状況</p> <p>前回棚卸し実施日/前回棚卸し実施者/前回棚卸し実施結果</p> <p>任意項目</p> <p>任意項目 1~20</p>
デバイスグループ	デバイスグループ
デバイス情報	<p>システム</p> <p>OS バージョン/CPU 名/CPU 周波数/メモリ/ドメイン・ワークグループ名/ログオンユーザー名/iTunesStore アカウント状態/iTunesStoreIdHash</p> <p>ハードウェア</p> <p>デバイス名/製品名/製造元/モデル名/ホスト名/シリアル番号/UDID（ハードウェア UUID）/ストレージ使用容量/CPU コア数/BIOS バージョン</p>
ネットワーク	MAC アドレス（Wi-Fi）/MAC アドレス（イーサネット）/MAC アドレス（Bluetooth）/NIC 情報（MAC アドレス/IP アドレス/サブネットマスク/デフォルトゲートウェイ/DNS サーバー）
セキュリティ	ファイアウォール状態/System Integrity Protection/FileVault/パーソナル復旧キー設定/パーソナル復旧キー/所属団体の復旧キー設定
インストールアプリ	アプリ名/バージョン/カテゴリー/デベロッパー/アプリケーション ID/アプリサイズ
プロファイル	プロファイル名/作成者/アプリケーション ID/概要
レポート	業務時間内外のデバイス利用状況/カテゴリ別のアプリ利用状況/アプリ利用時間ランキング/Web アクセス時間ランキング
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/

「デバイス詳細」画面の項目	項目名
	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。

■ 周辺機器

「デバイス詳細」画面の項目	項目名
管理情報	<p>基本情報</p> <p>デバイス管理名/デバイスタイプ/Apple ID/使用者名/使用者の社員コード/使用者の組織名/管理者名/管理者の組織名/管理者の組織コード</p> <p>使用状況</p> <p>使用場所/使用者タイプ/使用状況タイプ</p> <p>導入状況</p> <p>導入日/導入責任者/導入金額/導入タイプ/期限(リース/償却)/月額費用/購入先/補償内容</p> <p>棚卸し状況</p> <p>前回棚卸し実施日/前回棚卸し実施者/前回棚卸し実施結果</p> <p>任意項目</p> <p>任意項目 1~20</p>
デバイスグループ	デバイスグループ

デバイス情報を確認する

iOS
Android
Windows
macOS

デバイスや周辺機器の詳細情報を確認できます。

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。

	管理	デバイスグループ	デバイス管理名	ユーザー名	OSタイプ	OSバージョン
<input type="checkbox"/>	1	総務課	SC-03D_0000000014	江藤 花子	Android	9
<input type="checkbox"/>	2	総務課	hammerhead_00000000...	六角 富夫	Android	10
<input type="checkbox"/>	3	営業1課	iPhone_000000028	飯田 育三	iOS	14.4
<input type="checkbox"/>	4	人事課	N-04C_0000000020	江村 太郎	Android	11
<input type="checkbox"/>	5	営業部	EB-A71GJ_0000000019	橋中 栄一郎	Android	11
<input type="checkbox"/>	6	営業部	L-22D_0000000016	内田 健太	Android	11
<input type="checkbox"/>	7	営業1課	404KC_0000000023	中田 真由美	Android	10
<input type="checkbox"/>	8	営業1課	picasso_aapcus6jp_000...	橘 秀雄	Android	11
<input type="checkbox"/>	9	総務課	iPhone_000000026	森 太郎	iOS	14.4
<input type="checkbox"/>	10	営業1課	iPhone_000000029	別所 哲郎	iOS	13.2
<input type="checkbox"/>	11	営業1課	Surface Pro 5_00000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	12	営業1課	Surface Pro 5_00000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	13	営業1課	404KC_0000000023	石井 健二	Android	9

3. 詳細情報を確認します。

管理No. 3

iPhone_00000028 - デバイス詳細

デバイスグループ	ユーザー名	電話番号	Apple ID	最終稼働
営業1課	飯田 育三	080xxxxxxx	-	28分前

管理情報更新日時: 2024/01/17 17:27:15

基本情報

デバイス管理名	デバイスタイプ
iPhone_00000028	スマートフォン
Apple ID	
-	
ユーザー名	使用者の社員コード
飯田 育三	-
使用者の組織名	
-	
管理者名	管理者の組織名
-	-
管理者の組織コード	
-	

管理情報

利用者の名前や所属部署など、エンドポイントマネージャーで自動取得できない項目を管理/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。

デバイス情報

エンドポイントマネージャーで自動取得できるデバイスのハードウェア情報を確認できます。

ネットワーク

加入キャリアや Wi-Fi の MAC アドレスなど、ネットワークに関連する情報を確認できます。

セキュリティ

セキュリティに関する情報を確認できます。

インストールアプリ

デバイスにインストールされているアプリ情報を一覧で確認できます。

プロファイル iOS macOS

デバイスにインストールされているプロファイル情報を一覧で確認できます。

注意

macOS デバイスから取得できるプロファイル情報は、デバイスプロファイルだけです。ユーザープロファイルは取得できません。

Microsoft Office Windows

デバイスにインストールされている Microsoft Office 情報を一覧で確認できます。

注意

パッケージとしてインストールされている Microsoft Office 2016/2013/2010/2007 の情報を取得します。

Microsoft 365 の情報は取得できません。

位置情報 iOS Android Windows

デバイスの 1 日の移動履歴を確認できます。

位置情報のデータは一括出力できます。詳細は、[操作ログ/位置情報を一括出力する](#)を参照してください。

操作ログ iOS Android

デバイスの 1 日の操作ログを確認できます。取得できるログは OS によって異なります。

操作ログのデータは一括出力できます。詳細は、[操作ログ/位置情報を一括出力する](#)を参照してください。

レポート Windows macOS

デバイスやアプリの利用状況などを確認できます。

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。

Android Enterprise Android

Android Enterprise の適用ポリシーや、ポリシー適用時間などの情報を確認できます。Android デバイスを、Android Enterprise デバイスとして登録した場合にだけ、表示されます。

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。

デバイスイメージの設定

デバイスイメージを表示する

「デバイスタイプ」を設定すると、「デバイス管理名」列にデバイスイメージを表示させることができます。

サンプルイメージ	デバイスグループ	デバイス管理名	デバイスタイプ	OSタイプ
	ネットワーク全体	MacBook_00000085	ノート	macOS
	ネットワーク全体	iPhone_00000028	スマートフォン	iOS
	ネットワーク全体	iPad_00000034	タブレット	iOS
	ネットワーク全体	Windows_M3400WU	デスクトップ	Windows
	ネットワーク全体	Android_000000012	タブレット	Android
	ネットワーク全体	Windows_00000053	ノート	Windows
	ネットワーク全体	iMac_00021243	デスクトップ	macOS
	ネットワーク全体	SC-03D_000000014	スマートフォン	Android
	ネットワーク全体	Windows_00000040	タブレット	Windows
	ネットワーク全体	本社7階営業部_プリンター	プリンター	周辺機器
	ネットワーク全体	東京事業所2階ルーター	ルーター/HUB	周辺機器
	ネットワーク全体	本社キーボード_00001	入力機器	周辺機器
	ネットワーク全体	名古屋支社_タブレット0004	スマートデバイス	周辺機器
	ネットワーク全体	本社マウス_00001		周辺機器
	ネットワーク全体	廃棄用PC_00005	パソコン	周辺機器
	ネットワーク全体	DVDドライブ_00004	その他の機器	周辺機器

閉じる

デバイスの最新情報を取得する

iOS

Android

Windows

macOS

注意

- 次のデバイスは、取得対象外です。
 - Ver.5.5.3.0 未満の LANSCOPE Client をインストールしている Windows デバイス
 - Ver.3.2.4.0 未満の LANSCOPE Client をインストールしている Android デバイス
 - 周辺機器
- macOS デバイスでは、次のデバイス情報は取得対象外です。
CPU 名/CPU 周波数/CPU コア数/製造元/ログオンユーザー名/メモリ/ドメイン・ワークグループ名/
BIOS バージョン/NIC 情報 (NIC の種別/MAC アドレス/IP アドレス/デフォルトゲートウェイ/サブネット
マスク/DNS サーバー) /LANSCOPE Client バージョン
- 取得処理の実行後、次の取得処理ができるのは 10 分以上経過したあとです。
- 取得処理の実行後、コンソールに表示されるまでにはタイムラグがあります。数分経過したあとにリロードしてください。

1. [リスト] の [デバイス] をクリックします。



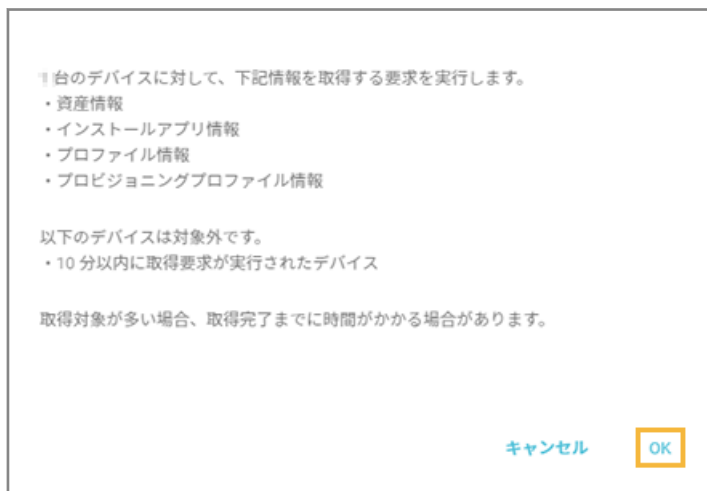
2. デバイスをチェックし、[最新情報を取得] をクリックします。

ネットワーク全体		iOS	Android	Windows	macOS	周辺機器	検索
X 1件を選択中		アクション実行		最新情報を取得	削除する		
<input type="checkbox"/>	↑ 管理	デバイスグループ	デバイス管理名	使用者名	OSタイプ	OSバージョン	
<input type="checkbox"/>	1	総務課	SC-03D_0000000014	江藤 花子	Android	9	
<input type="checkbox"/>	2	総務課	hammerhead_00000000...	六角 富夫	Android	10	
<input checked="" type="checkbox"/>	3	営業1課	iPhone_0000000028	飯田 育三	iOS	14.4	
<input type="checkbox"/>	4	人事課	N-04C_0000000020	江村 太郎	Android	11	
<input type="checkbox"/>	5	営業部	EB-A71GJ_0000000019	橋中 栄一郎	Android	11	
<input type="checkbox"/>	6	営業部	L-22D_0000000016	内田 健太	Android	11	
<input type="checkbox"/>	7	営業1課	404KC_0000000023	中田 真由美	Android	10	
<input type="checkbox"/>	8	営業1課	picasso_aapcus6jp_000...	橋 秀雄	Android	11	
<input type="checkbox"/>	9	総務課	iPhone_0000000026	森 太郎	iOS	14.4	
<input type="checkbox"/>	10	営業1課	iPhone_0000000029	別所 哲郎	iOS	13.2	
<input type="checkbox"/>	11	営業1課	Surface Pro 5_00000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134	
<input type="checkbox"/>	12	営業1課	Surface Pro 5_00000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134	
<input type="checkbox"/>	13	営業1課	404KC_0000000023	石井 健二	Android	9	

登録済みライセンス: 83 / 100 周辺機器: 18 / 10,000 1000 1-85件 / 全 85件 < 1 >

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。



→ チェックしたデバイスの最新情報が取得されます。

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組織名）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。

第2章 リストで情報を確認する

<input type="checkbox"/>	管理	デバイスグループ	デバイス管理名	使用者名	OSタイプ	OSバージョン
<input type="checkbox"/>	1	総務課	SC-03D_0000000014	江藤 花子	Android	9
<input type="checkbox"/>	2	総務課	hammerhead_00000000...	六角 富夫	Android	10
<input type="checkbox"/>	3	営業1課	iPhone_000000028	飯田 育三	iOS	14.4
<input type="checkbox"/>	4	人事課	N-04C_0000000020	江村 太郎	Android	11
<input type="checkbox"/>	5	営業部	EB-A71GJ_0000000019	橋中 栄一郎	Android	11
<input type="checkbox"/>	6	営業部	L-22D_0000000016	内田 健太	Android	11
<input type="checkbox"/>	7	営業1課	404KC_0000000023	中田 真由美	Android	10
<input type="checkbox"/>	8	営業1課	picasso_aapcus6jp_000...	橘 秀雄	Android	11
<input type="checkbox"/>	9	総務課	iPhone_000000026	森 太郎	iOS	14.4
<input type="checkbox"/>	10	営業1課	iPhone_000000029	別所 哲郎	iOS	13.2
<input type="checkbox"/>	11	営業1課	Surface Pro 5_00000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	12	営業1課	Surface Pro 5_00000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	13	営業1課	404KC_0000000023	石井 健二	Android	9

3. [管理情報] の [編集] をクリックします。

管理No. 3

デバイスグループ: 営業1課 | 使用者名: 飯田 育三 | 電話番号: 080xxxxxxx | Apple ID: - | 最終稼働: 28分前

管理情報更新日時: 2024/01/17 17:27:15

管理情報 [編集]

基本情報

デバイス管理名	デバイスタイプ
iPhone_000000028	スマートフォン
Apple ID	-
使用者名	使用者の社員コード
飯田 育三	-
使用者の組織名	-
管理者名	管理者の組織名
-	-
管理者の組織コード	-

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。

ネットワーク全体 ▼ iOS Android Windows macOS 周辺機器 🔍 キーワード検索 (例: 営業 iPhone) ⓘ

デバイスの追加 周辺機器の追加 インストール待ちデバイス

<input type="checkbox"/>	↑ 管理...	デバイスグループ	デバイス管理名	使用者名	OSタイプ	
<input type="checkbox"/>	1	総務課	SC-03D_0000000014	江藤 花子	Android	
<input type="checkbox"/>	2	総務課	hammerhead_00000000...	六角 富夫	Android	
<input type="checkbox"/>	3	営業1課	iPhone_000000028	飯田 育三	iOS	
<input type="checkbox"/>	4	人事課	N-04C_0000000020	江村 太郎	Android	
<input type="checkbox"/>	5	営業部	EB-A71GJ_0000000019	橋中 栄一郎	Android	
<input type="checkbox"/>	6	営業部	L-22D_0000000016	内田 健太	Android	
<input type="checkbox"/>	7	営業1課	404KC_0000000023	中田 真由美	Android	
<input type="checkbox"/>	8	営業1課	picasso_aapcus6jp_000...	橘 秀雄	Android	
<input type="checkbox"/>	9	総務課	iPhone_000000026	森 太郎	iOS	14.4
<input type="checkbox"/>	10	営業1課	iPhone_000000029	別所 哲郎	iOS	13.2
<input type="checkbox"/>	11	営業1課	Surface Pro 5_00000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	12	営業1課	Surface Pro 5_00000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	13	営業1課	404KC_0000000023	石井 健二	Android	9

登録済みライセンス: 83 / 100 周辺機器: 18 / 10,000 1000 1-85件 / 全 85件 < > 1 >

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。

エクスポート

現在指定されている条件のデバイスの情報をエクスポートします。
出力されるファイルの形式はカンマ区切り(CSV)です。

- ダウンロードするファイルのエンコードを選択
Shift_JIS
- エクスポートする項目を選択 (18 件)
すべてチェック 表示中の列をチェック すべてははずす
 - 共通
 - 管理情報
 - デバイス情報
 - セキュリティ情報
 - ネットワーク
 - 位置情報
 - クライアント
- ファイルのダウンロード
エクスポート対象の件数によっては、ダウンロードが完了するまでに時間がかかる場合がございます。
ダウンロードを実行すると今回選択した項目の設定値が保存されます。
ダウンロード

閉じる

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が必要なため、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。

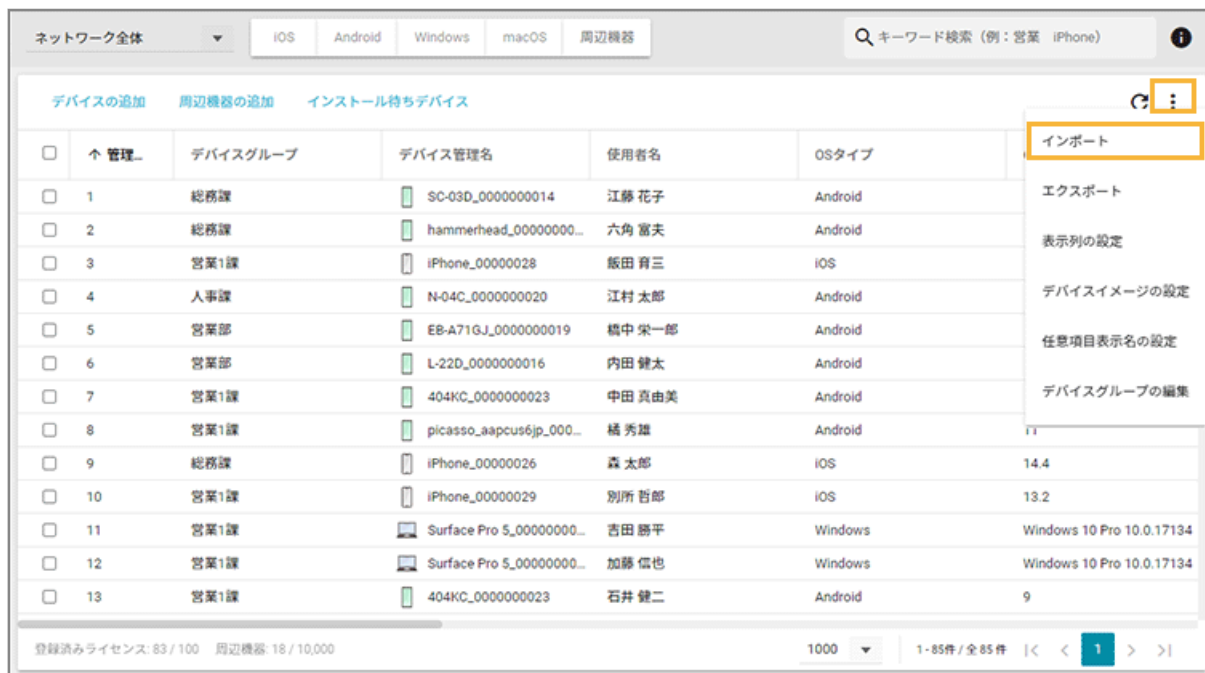
1. 各デバイスの情報を編集し、上書き保存します。

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。



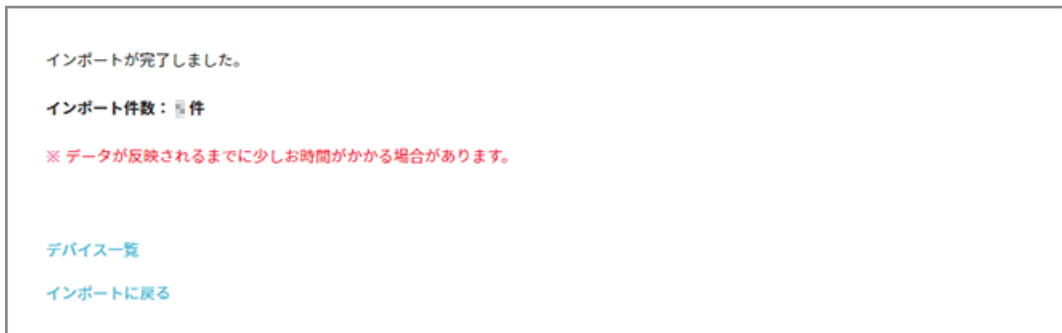
→ 「関連づける列名」が自動的に選択されます。

「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-305「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。

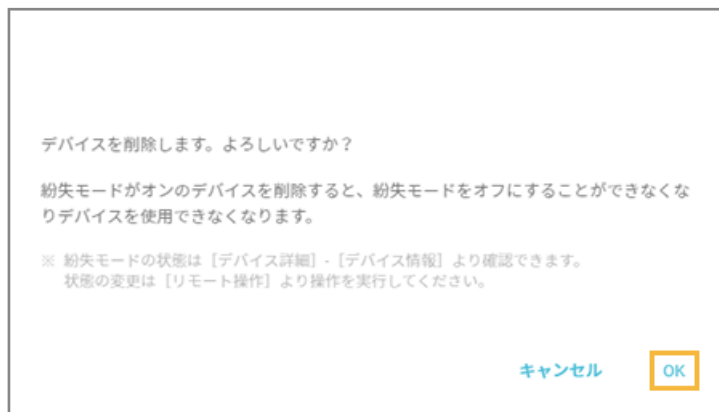


2. デバイスをチェックし、[削除する] をクリックします。

<input type="checkbox"/>	↑ 管理...	デバイスグループ	デバイス管理名	使用者名	OSタイプ	OSバージョン
<input type="checkbox"/>	1	総務課	SC-03D_0000000014	江藤 花子	Android	9
<input type="checkbox"/>	2	総務課	hammerhead_00000000...	六角 富夫	Android	10
<input checked="" type="checkbox"/>	3	営業1課	iPhone_000000028	飯田 育三	iOS	14.4
<input type="checkbox"/>	4	人事課	N-04C_0000000020	江村 太郎	Android	11
<input type="checkbox"/>	5	営業部	EB-A71GJ_0000000019	橋中 栄一郎	Android	11
<input type="checkbox"/>	6	営業部	L-22D_0000000016	内田 健太	Android	11
<input type="checkbox"/>	7	営業1課	404KC_0000000023	中田 真由美	Android	10
<input type="checkbox"/>	8	営業1課	picasso_aapcus6jp_000...	橘 秀雄	Android	11
<input type="checkbox"/>	9	総務課	iPhone_000000026	森 太郎	iOS	14.4
<input type="checkbox"/>	10	営業1課	iPhone_000000029	別所 哲郎	iOS	13.2
<input type="checkbox"/>	11	営業1課	Surface Pro 5_00000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	12	営業1課	Surface Pro 5_00000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	13	営業1課	404KC_0000000023	石井 健二	Android	9

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。

任意項目表示名を設定／編集する

iOS **Android** Windows macOS

任意項目を利用し、デバイスや周辺機器の自動取得できない情報を管理できます。デバイス情報の紐づけに必要な項目がある場合、項目を設定します。任意項目は、「デバイス詳細」画面の「管理情報」で確認できます。

次の項目は、あらかじめ用意されているため、設定する必要はありません。


デバイス管理名	デバイスタイプ	Apple ID (*1)	使用者名	使用者の社員コード
---------	---------	---------------	------	-----------

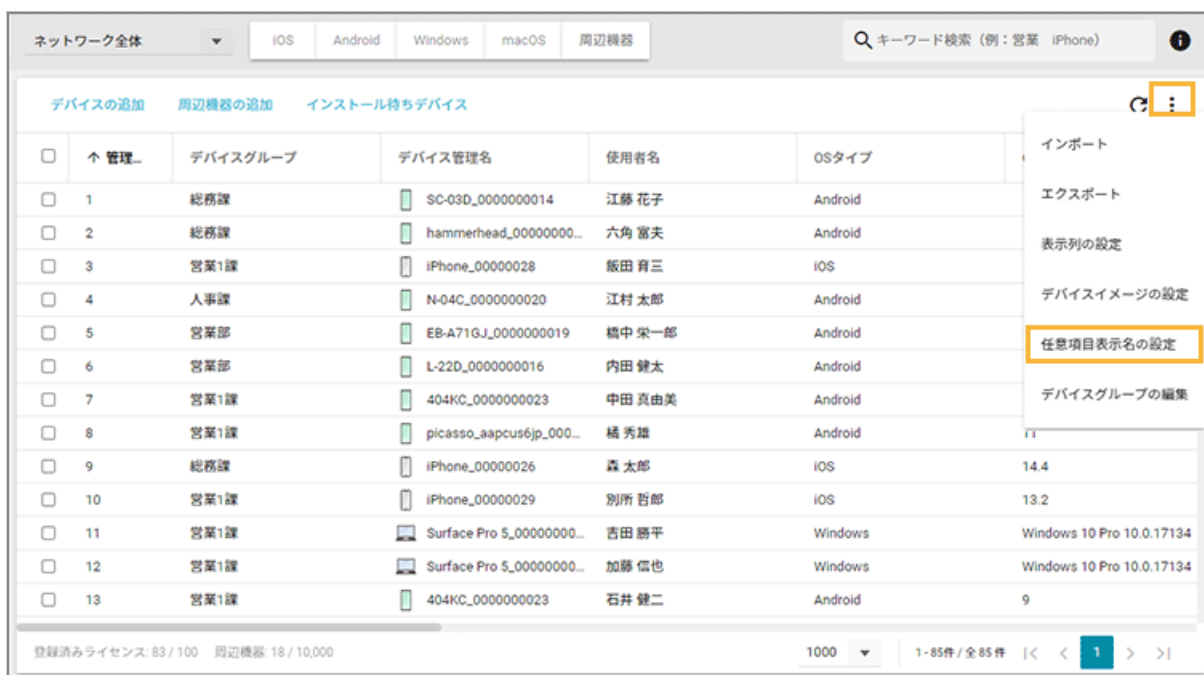
使用者の組織名	管理者名	管理者の組織名	管理者の組織コード	使用場所
使用者タイプ	使用状況タイプ	導入日	導入責任者	導入金額
導入タイプ	期限（リース／償却）	月額費用	購入先	補償内容
前回棚卸し実施日	前回棚卸し実施者	前回棚卸し実施結果		

*1 : iOS/macOS の設定項目です。

1. [リスト] の [デバイス] をクリックします。



2.  をクリックし、[任意項目表示名の設定] をクリックします。



3. [編集] をクリックします。

任意項目表示名の設定

編集

任意項目1の表示名 任意項目1	任意項目2の表示名 任意項目2
任意項目3の表示名 任意項目3	任意項目4の表示名 任意項目4
任意項目5の表示名 任意項目5	任意項目6の表示名 任意項目6
任意項目7の表示名 任意項目7	任意項目8の表示名 任意項目8
任意項目9の表示名 任意項目9	任意項目10の表示名 任意項目10
任意項目11の表示名 任意項目11	任意項目12の表示名 任意項目12
任意項目13の表示名 任意項目13	任意項目14の表示名 任意項目14
任意項目15の表示名 任意項目15	任意項目16の表示名 任意項目16

閉じる

4. 任意項目表示名を入力し、[保存] をクリックします。

任意項目表示名の設定

キャンセル **保存**

・重複する項目名やシステムで使用されている項目名は設定できません。


任意項目1の表示名 *	任意項目2の表示名 *
任意項目1	任意項目2
任意項目3の表示名 *	任意項目4の表示名 *
任意項目3	任意項目4
任意項目5の表示名 *	任意項目6の表示名 *
任意項目5	任意項目6
任意項目7の表示名 *	任意項目8の表示名 *
任意項目7	任意項目8
任意項目9の表示名 *	任意項目10の表示名 *
任意項目9	任意項目10
任意項目11の表示名 *	任意項目12の表示名 *
任意項目11	任意項目12
任意項目13の表示名 *	任意項目14の表示名 *
任意項目13	任意項目14
任意項目15の表示名 *	任意項目16の表示名 *
任意項目15	任意項目16

閉じる

5. [閉じる] をクリックします。

6.  をクリックします。

ネットワーク全体 ▼ iOS Android Windows macOS 周辺機器 🔍 キーワード検索 (例: 営業 iPhone) ⓘ

デバイスの追加 周辺機器の追加 インストール待ちデバイス  ⓘ

<input type="checkbox"/>	管理	デバイスグループ	デバイス管理名	ユーザー名	OSタイプ	OSバージョン
<input type="checkbox"/>	1	総務課	SC-03D_0000000014	江藤 花子	Android	9
<input type="checkbox"/>	2	総務課	hammerhead_00000000...	六角 富夫	Android	10
<input type="checkbox"/>	3	営業1課	iPhone_0000000028	飯田 育三	iOS	14.4
<input type="checkbox"/>	4	人事課	N-04C_0000000020	江村 太郎	Android	11
<input type="checkbox"/>	5	営業部	EB-A71GJ_0000000019	橋中 栄一郎	Android	11
<input type="checkbox"/>	6	営業部	L-22D_0000000016	内田 健太	Android	11
<input type="checkbox"/>	7	営業1課	404KC_0000000023	中田 真由美	Android	10
<input type="checkbox"/>	8	営業1課	picasso_aapcus6jp_000...	橘 秀雄	Android	11
<input type="checkbox"/>	9	総務課	iPhone_0000000026	森 太郎	iOS	14.4
<input type="checkbox"/>	10	営業1課	iPhone_0000000029	別所 哲郎	iOS	13.2
<input type="checkbox"/>	11	営業1課	Surface Pro 5_00000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	12	営業1課	Surface Pro 5_00000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	13	営業1課	404KC_0000000023	石井 健二	Android	9

登録済みライセンス: 83 / 100 周辺機器: 18 / 10,000 1000 ▼ 1 - 85件 / 全 85件 < > 1 >

→ 変更内容が反映されます。

周辺機器情報を追加する

プリンターやルーターなどの自動取得できない周辺機器情報を、任意で追加して手動で管理できます。

追加した情報を編集／削除する場合は、他のデバイスと同様に管理コンソールで編集／削除できます。詳細は、[デバイス情報を編集／削除する](#)を参照してください。

■ 周辺機器情報を1台ずつ追加する

1. [リスト] の [デバイス] をクリックします。



2. [周辺機器の追加] をクリックします。

<input type="checkbox"/>	↑ 管理...	デバイスグループ	デバイス管理名	使用者名	OSタイプ	OSバージョン
<input type="checkbox"/>	1	総務課	SC-03D_0000000014	江藤 花子	Android	9
<input type="checkbox"/>	2	総務課	hammerhead_00000000...	六角 富夫	Android	10
<input type="checkbox"/>	3	営業1課	iPhone_000000028	飯田 育三	iOS	14.4
<input type="checkbox"/>	4	人事課	N-04C_0000000020	江村 太郎	Android	11
<input type="checkbox"/>	5	営業部	EB-A71GJ_0000000019	橋中 栄一郎	Android	11
<input type="checkbox"/>	6	営業部	L-22D_0000000016	内田 健太	Android	11
<input type="checkbox"/>	7	営業1課	404KC_0000000023	中田 真由美	Android	10
<input type="checkbox"/>	8	営業1課	picasso_aapcus6jp_000...	橘 秀雄	Android	11
<input type="checkbox"/>	9	総務課	iPhone_000000026	森 太郎	iOS	14.4
<input type="checkbox"/>	10	営業1課	iPhone_000000029	別所 哲郎	iOS	13.2
<input type="checkbox"/>	11	営業1課	Surface Pro 5_00000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	12	営業1課	Surface Pro 5_00000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	13	営業1課	404KC_0000000023	石井 健二	Android	9

3. [一台ずつ追加] をクリックします。

周辺機器の追加

追加方法を選択してください。

一台ずつ追加

一括インポート追加

[閉じる](#)

4. 基本情報を入力し、[保存] をクリックします。

その他の項目を追加する場合は、[詳細項目を表示する] をクリックして入力します。

項目	値
デバイスグループ	所属するデバイスグループ 事前に設定しておいたグループを指定します。
デバイス管理名	周辺機器を特定できる任意のデバイス管理名
使用者名	周辺機器を特定できる任意の使用者名
デバイスタイプ	周辺機器の種類 パソコン/プリンター/ルーター/HUB/入力機器/スマートデバイス/その他の機器の中から選択します。

周辺機器の追加

追加方法を選択してください。

一台ずつ追加 一括インポート追加

基本情報

デバイスグループ*
ネットワーク全体

デバイス管理名*
USBメモリ

使用者名

使用者の社員コード

デバイスタイプ

▼ 詳細項目を表示する

キャンセル 保存

→ 周辺機器情報が追加されます。

■ 周辺機器情報を一括で追加する

1. [リスト] の [デバイス] をクリックします。



2. [周辺機器の追加] をクリックします。

ネットワーク全体 ▼ iOS Android Windows macOS 周辺機器 🔍 キーワード検索 (例: 営業 iPhone) ⓘ

デバイスの追加 周辺機器の追加 インストール待ちデバイス 🔄 ⋮

<input type="checkbox"/>	↑ 管理...	デバイスグループ	デバイス管理名	使用者名	OSタイプ	OSバージョン
<input type="checkbox"/>	1	総務課	SC-03D_0000000014	江藤 花子	Android	9
<input type="checkbox"/>	2	総務課	hammerhead_00000000...	六角 富夫	Android	10
<input type="checkbox"/>	3	営業1課	iPhone_000000028	飯田 育三	iOS	14.4
<input type="checkbox"/>	4	人事課	N-04C_0000000020	江村 太郎	Android	11
<input type="checkbox"/>	5	営業部	EB-A71GJ_0000000019	橋中 栄一郎	Android	11
<input type="checkbox"/>	6	営業部	L-22D_0000000016	内田 健太	Android	11
<input type="checkbox"/>	7	営業1課	404KC_0000000023	中田 真由美	Android	10
<input type="checkbox"/>	8	営業1課	picasso_aapcus6jp_000...	橘 秀雄	Android	11
<input type="checkbox"/>	9	総務課	iPhone_000000026	森 太郎	iOS	14.4
<input type="checkbox"/>	10	営業1課	iPhone_000000029	別所 哲郎	iOS	13.2
<input type="checkbox"/>	11	営業1課	Surface Pro 5_00000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	12	営業1課	Surface Pro 5_00000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	13	営業1課	404KC_0000000023	石井 健二	Android	9

登録済みライセンス: 83 / 100 周辺機器: 18 / 10,000 1000 ▼ 1-85件 / 全 85 件 |< < 1 > >|

3. [一括インポート追加] をクリックします。

周辺機器の追加

追加方法を選択してください。

一台ずつ追加 一括インポート追加

閉じる

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。

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

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。

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。



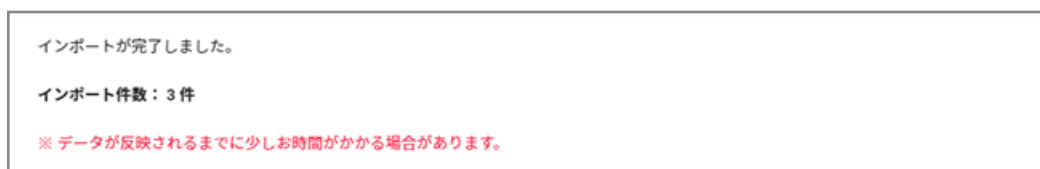
→ 「関連づける列名」が自動的に選択されます。

「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. プレビューを確認し、[インポート] をクリックします。



→ 周辺機器情報が追加されます。



2-2 操作ログ情報を確認する

iOS

Android

ポイント

操作ログは、一括出力できます。詳細は、[操作ログ／位置情報を一括出力する](#)を参照してください。

- [取得できる項目一覧](#)
- [操作ログ情報の取得設定をする](#)
- [操作ログを確認する](#)

取得できる項目一覧

iOS

Android

■ iOS

iOS で取得できる操作ログ情報は、次のとおりです。

操作ログ	デバイス詳細項目	
	分類	内容
電話利用ログ	電話	発信／着信／不在着信
デバイス活用ログ	環境	デバイス活用

■ Android

Android で取得できる操作ログ情報は、次のとおりです。

操作ログ	デバイス詳細項目			
	分類	内容	詳細 1	詳細 2
電話利用ログ	電話	発信／着信／不在着信	発着信先電話番号	相手先名
アプリ利用ログ	アプリ	アプリ利用	アプリ名称	アプリケーション ID
アプリインストールログ	環境	新規アプリインストール	アプリ名称	アプリケーション ID

操作ログ	デバイス詳細項目			
	分類	内容	詳細 1	詳細 2
アプリアンインストールログ		アプリアンインストール	—	アプリケーション ID
外部メディアの認識ログ		外部メディアの認識	メディアのパス (file:///storage/sdcard1 など)	—
外部メディアの取り外しログ		外部メディアの取り外し	メディアのパス (file:///storage/sdcard1 など)	—
タイムゾーン変更ログ		タイムゾーン変更	変更後のタイムゾーン (Asia/Tokyo など)	—
デバイス管理者設定ログ		デバイス管理者設定	"LANSCOPE Client がデバイス管理者に登録されました。" "LANSCOPE Client がデバイス管理者から解除されました。"	—
使用履歴へのアクセス設定ログ		使用履歴へのアクセス設定	"LANSCOPE Client が使用履歴にアクセスできるアプリに登録されました。" "LANSCOPE Client が使用履歴にアクセスできるアプリから解除されました。"	—
LANSCOPE Client のアンインストールを検知したログ		LANSCOPE Client のアンインストール	"LANSCOPE Client をアンインストールする操作を検知しました。"	—
デバイス管理者設定を解除する操作を検知したログ		デバイス管理者設定	"LANSCOPE Client をデバイス管理者から解除する操作を検知しました。"	—
ユーザー補助設定をオフにする操作を検知したログ		ユーザー補助設定	"LANSCOPE Client サービスがユーザー補助アプリから解除する操作を検知しました。"	—
ユーザー補助設定ログ		ユーザー補助設定	"LANSCOPE Client がユーザー補助アプリに登録されました。"	—

操作ログ	デバイス詳細項目			
	分類	内容	詳細 1	詳細 2
			"LANSCOPE Client がユーザー補助アプリから解除されました。"	
ユーザーの切り替えを検知したログ		ユーザー切り替え	"LANSCOPE Client が管理しているユーザーでログインされました。" "LANSCOPE Client が管理していないユーザーでログインされました。"	—

操作ログ情報の取得設定をする

iOS

Android

操作ログ情報を取得するために、管理コンソール/デバイスで必要な設定をします。

ステップ :

1. [デバイスの操作ログ取得設定をする](#)
2. [デバイス側で設定する](#)

ステップ 1 : デバイスの操作ログ取得設定をする

管理コンソールで、取得する情報やパスワードポリシーを設定します。

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	共通	iOS	Android	Windows	macOS
メモ	○	○	○	○	○
業務時間設定	○	—	—	—	—
LANSCOPE Client アップデート設定	—	—	○	—	○
デバイス表示設定 (*1) (*2)	—	○	—	—	—

設定		共通	iOS	Android	Windows	macOS
デバイス使用者への設定情報表示 (*3)		—	○	○	○	—
デバイス情報取得設定	インストールアプリ情報	—	○	○	○	○
	プロファイル情報	—	○	—	—	○
操作ログ取得設定	電話利用ログ	—	○	○	—	—
	デバイス活用ログ	—	○	—	—	—
	アプリ利用ログ	—	—	○ (*4)	—	—
	環境変更操作ログ	—	—	○	—	—
位置情報ログ取得設定		—	○	○	○ (*5)	—
デバイスへの通知設定	LANSCOPE Client 停止時の起動通知	—	○	—	—	—
	資産アラートの通知	—	—	○ (*6)	—	—
	操作アラートの通知	—	—	○ (*6) (*7)	—	—
アンインストール防止設定		—	—	—	○	○
パスワードポリシー設定		—	○	○ (*8) (*9)	—	○
マルチユーザー機能制御		—	—	○ (*8)	—	—

*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。位置情報ログを取得するための設定ではありません。

*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：LANSCOPE Client 側で、環境設定で設定されている内容を確認できます。

*4：アプリを禁止設定する場合、アプリ利用ログは「取得する」に設定してください。詳細は、[アプリの利用を禁止するときに必要な設定をする](#)を参照してください。

*5：Windows Server OS は、位置情報取得機能に未対応です。

*6：事前にアラートに設定するためのレシピ作成が必要です。詳細は、[アラート設定の流れ](#)を参照してください。

*7：アプリを禁止設定する場合、「操作アラートの通知」の「不許可・禁止したアプリが実行された」を「通知する」に設定してください。詳細は、[アプリの利用を禁止するときに必要な設定をする](#)を参照してください。

*8：Android Enterprise デバイスには適用できません。Android Enterprise デバイスに適用するポリシーは、[ルール] > [Android Enterprise 設定] で設定します。詳細は、An-347「Android Enterprise 利用ガイド」を参照してください。

*9 : Android 10 以上のデバイスには適用されません。

4. [保存] をクリックします。

ステップ 2 : デバイス側で設定する

デバイス側の設定を確認します。

iOS の場合

iOS の設定方法は、An-301「初期設定ガイド for iOS/iPadOS」を参照してください。

iOS で操作ログ情報を取得するための条件は、次のとおりです。

- LANSCOPE Client (アプリ) がデバイスにインストールされ、登録されている。
- デバイスの位置情報サービスがオンで、LANSCOPE の設定で [常に] を設定している。
- バックグラウンドで LANSCOPE Client が起動している。





ポイント

LANSCOPE Client がバックグラウンドで終了している場合、操作ログを取得できません。

ただし、位置情報機能を利用する場合、位置情報取得の条件によって、LANSCOPE Client が自動起動するタイミングがあります。自動起動した場合には、操作ログも取得されます。位置情報取得の条件については、[iOS の場合](#)を参照してください。

Android の場合

Android の設定方法は、An-302「初期設定ガイド for Android」を参照してください。

Android で操作ログ情報を取得するための条件は、次のとおりです。

- LANSCOPE Client (アプリ) がデバイスにインストールされ、登録されている。
- 「使用履歴へのアクセス」が有効になっている。
- 「アクセス設定」が有効になっている。
- 「電池の最適化例外設定」が有効になっている。



操作ログを確認する

iOS

Android

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。

第2章 リストで情報を確認する

ネットワーク全体 ▼ iOS Android Windows macOS 周辺機器 🔍 キーワード検索 (例: 営業 iPhone) ⓘ

デバイスの追加 周辺機器の追加 インストール待ちデバイス ↻ ⋮

<input type="checkbox"/>	↑ 管理...	デバイスグループ	デバイス管理名	使用者名	OSタイプ	OSバージョン
<input type="checkbox"/>	1	総務課	SC-03D_0000000014	江藤 花子	Android	9
<input type="checkbox"/>	2	総務課	hammerhead_00000000...	六角 富夫	Android	10
<input type="checkbox"/>	3	営業1課	iPhone_000000028	飯田 育三	iOS	14.4
<input type="checkbox"/>	4	人事課	N-04C_0000000020	江村 太郎	Android	11
<input type="checkbox"/>	5	営業部	EB-A71GJ_0000000019	橋中 栄一郎	Android	11
<input type="checkbox"/>	6	営業部	L-22D_0000000016	内田 健太	Android	11
<input type="checkbox"/>	7	営業1課	404KC_0000000023	中田 真由美	Android	10
<input type="checkbox"/>	8	営業1課	picasso_aapcus6jp_000...	橘 秀雄	Android	11
<input type="checkbox"/>	9	総務課	iPhone_000000026	森 太郎	iOS	14.4
<input type="checkbox"/>	10	営業1課	iPhone_000000029	別所 哲郎	iOS	13.2
<input type="checkbox"/>	11	営業1課	Surface Pro 5_00000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	12	営業1課	Surface Pro 5_00000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	13	営業1課	404KC_0000000023	石井 健二	Android	9

登録済みライセンス: 83 / 100 周辺機器: 18 / 10,000 1000 1-85件 / 全 85 件 |< < 1 > >|

3. [操作ログ] をクリックし、操作ログ情報を確認します。

Android 404KC_0000000023 - デバイス詳細 管理No. 7

デバイスグループ: 営業1課 使用者名: 中田 真由美 電話番号: 060xxxxxxx アカウントのメールアドレス: at35.motex@gmail.com 最終稼働: 7時間前

管理情報 < 2023/03/07 > > すべて > 🔍 キーワード検索 (例: 営業 iPhone) ⓘ

時刻	分類	利用時間	内容	詳細1	詳細2	カ
08:44:36	アプリ	00:00:02	アプリ利用	省電力ナビ	jp.kyocera.ecomode	
08:45:42	アプリ	00:00:05	アプリ利用	省電力ナビ	jp.kyocera.ecomode	
08:48:26	アプリ	00:00:41	アプリ利用	Gmail	com.google.android.gm	通
08:49:00	アプリ	00:03:32	アプリ利用	ビジネスナビタイム動..	com.navitime.twende	
09:02:25	アプリ	00:03:06	アプリ利用	名刺管理アプリEight(無..	net.eightcard	ビ
10:00:25	アプリ	00:00:25	アプリ利用	省電力ナビ	jp.kyocera.ecomode	
10:04:21	アプリ	00:00:04	アプリ利用	HOME	au.android.apps.oceanh...	
10:32:25	アプリ	00:00:01	アプリ利用	Androidシステム	android	
11:01:18	アプリ	00:00:48	アプリ利用	電話帳	com.android.contacts	
11:03:00	アプリ	00:03:06	アプリ利用	産経ニュース	com.msn.jp.sankei.new...	
11:06:11	アプリ	00:00:06	アプリ利用	HOME	au.android.apps.oceanh...	

1-126件 / 全 126 件 |< < 1 > >| 閉じる

2-3 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。
	紛失モード（*1）	遠隔でロックをかけ、デバイス側から解除できないようにします。ロック時にデバイスにメッセージや連絡先（電話番号）を表示できます。また、位置情報の取得もできます。
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。（*2）（*3）（*4）
	リモートワイプ（*5）	遠隔でデバイスを初期化します。
	パスワードを再設定（*6）	デバイスのパスワードを再設定します。
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（*7）	「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。（*8） 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：「監視モード」がオンになっているデバイスにだけ対応しています。条件を満たしていない場合、「紛失モード」は表示されません。

*2：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。

*3：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。

*4：Android Enterprise デバイスでは、ロック解除パスワードの上書き設定はできません。

*5：Android Enterprise デバイスでは、キャンセル操作はできません。

*6：Android Enterprise デバイスにだけ、対応しています。

*7 : Windows 11 Home/Windows 10 Home には対応していません。

*8 : 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
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-302「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-303「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。

管理	デバイスグループ	デバイス管理名	ユーザー名	OSタイプ	OSバージョン
<input type="checkbox"/>	3 営業1課	iPhone_00000028	飯田 育三	iOS	14.4
<input type="checkbox"/>	9 総務課	iPhone_00000026	森 太郎	iOS	14.4
<input type="checkbox"/>	10 営業1課	iPhone_00000029	別所 哲郎	iOS	13.2
<input type="checkbox"/>	16 営業部	iPhone_00000030	佐藤 新	iOS	14.2
<input type="checkbox"/>	17 営業1課	iPhone_00000031	鈴木 一	iOS	14.1
<input type="checkbox"/>	18 営業2課	iPhone_00000032	佐竹 信弘	iOS	13.5.1
<input type="checkbox"/>	19 営業2課	iPhone_00000033	石川 忍	iOS	14.4
<input type="checkbox"/>	21 営業1課	iPad_00000034	小林 哲司	iOS	14.2
<input type="checkbox"/>	27 営業2課	iPhone_00000027	島山 哲夫	iOS	14.3
<input type="checkbox"/>	32 システム1課	iPad_00000035	細川 孝信	iOS	13
<input type="checkbox"/>	33 システム1課	iPad_00000042	横口 掲羽	iOS	14.2
<input type="checkbox"/>	34 システム1課	iPad_00000036	北井 清二	iOS	13.5.1
<input type="checkbox"/>	35 システム部	iPad_00000043	上野 卓	iOS	14

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。

iPhone_00000028 - デバイス詳細

管理No. 3

デバイスグループ: 営業1課 | 使用人名: 飯田 育三 | 電話番号: 080xxxxxxx | Apple ID: - | 最終稼働: 28分前

リモート操作を実行する ▼

- リモートロックを実行
- リモートワイプを実行 7:12に実行されました。
- パスコードオフを実行 11:53:55 (元時)

内容 リモートロック
 状態 成功
 実行日時 2017/12/01 15:38:12
 メッセージ -
 電話番号 -
 詳細 デバイスをロックしました。

リモートロック:リジェクト
 2017/11/30 16:56:46 に実行されました。

リモートワイプ:成功
 2017/11/30 16:45:55 に実行されました。

リモートワイプ:成功
 2017/11/30 16:45:55 に実行されました。

- 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。

リモートロックの実行

リモートロックを実行することで第三者による不正使用を防ぐことができます。

カスタムメッセージ

リモートロックが実行されたデバイスの画面にメッセージや連絡先を表示します。
連絡先を入力した場合は発信ボタンが表示され、入力した連絡先への発信のみ操作が可能な状態になります。

メッセージ

電話番号

① 注意事項 ▾

キャンセル 実行

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。

リモートワイプの実行

リモートワイプを実行することでデバイス内のすべてのデータを初期化できます。
消去されたデータを復元することはできません。
また、LANSCOPE の機能も使用できなくなります。

ログインしている管理コンソールのパスワードを入力し、実行してください。

ログインパスワード *

初期設定時にクイックスタートをスキップする

キャンセル 実行

[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。

パスコードオフの実行

パスコードをオフに設定します。現在のパスコードロックは削除されます。

キャンセル **実行**

- 紛失モードの場合

- 紛失モードオン

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

紛失モードオンの実行

紛失モードをオンにします。
オフにするまでデバイスのロック画面を解除できなくなります。
また、【リモート操作を実行する】メニューから【位置情報取得】が実行できます。
※ デバイスの位置情報サービス設定がオフの場合や LANSOPE Client がインストールされていない場合でも、リモートで位置情報が取得できます。

カスタムメッセージ

メッセージ

ロック画面の上段に表示されます。

電話番号

ロック画面の中段に表示されます。

脚注

ロック画面の下段に表示されます。

① 注意事項 ▾

キャンセル **実行**

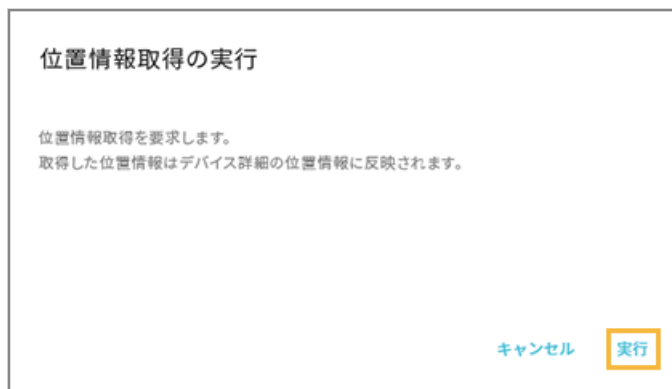
注意

デバイスの紛失モードの状態がオンの場合、次の挙動になります。

- リモートロックができません。
- 紛失モードをオフにするまで、デバイスのロック画面を解除できません。
- 紛失モードがオンになっている場合でも、パスコードオフは実行できます。パスコードオフ実行後の画面は、紛失モードオフ後に確認できます。
- リモートワイプはできますが、リモートワイプ後、紛失モードはオフになり、再アクティベートできる状態になります。
- 紛失モードがオンになると、LANSCOPE Client は停止します。そのため、「標準位置情報サービス」を利用した定期間隔での位置情報取得はできなくなります。ただし、「大幅変更位置情報サービス」で、一度位置情報を取得した場合、LANSCOPE Client が自動復帰後は「標準位置情報サービス」で取得します。
- LANSCOPE Client はバックグラウンドで動作できません。そのため、「メッセージ・アンケートの通知」は表示されません。
- アプリ配信/VPP アプリ配信はできません。
- 管理コンソールから紛失モードオンのデバイスを削除すると、そのデバイスの紛失モードをオフにできないため、ロック解除できず、デバイスを利用できなくなります。必ず、紛失モードをオフにしてからデバイスを削除してください。
- Wi-Fi だけで通信するデバイスを再起動すると、Wi-Fi に接続できず、紛失モードをオフにできなくなります。紛失モードをオフにする場合は、デバイスを初期化し、エンドポイントマネージャーに再登録してください。

- **位置情報取得**

[実行] をクリックします。



ポイント

- 位置情報の取得は、紛失モードオンの状態だけで実行できます。
- 取得した位置情報は、次の画面で確認できます。
 - 最新位置情報：[モニター] > [最新位置情報]
 - 移動履歴：[リスト] > [デバイス] の「デバイス詳細」画面の「位置情報」紛失モードで取得した位置情報は、グレーのアイコンで表示されます。

紛失モードオフ

[実行] をクリックします。



ポイント

- 紛失モードオンの状態だけで実行できます。
- 紛失モードオンの状態で「位置情報取得の実行」を1度でも行ったことがある場合、紛失モードオフの実行後、ロック画面に「このデバイスの位置は、前回×××年×月×日×：×に位置情報が共有されました」と表示されます。

■ Android の場合

ポイント

Android Enterprise デバイスでリモート操作する場合、An-347「Android Enterprise 利用ガイド」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. OS をクリックし、デバイスをクリックします。

	↑ 管理	デバイスグループ	デバイス管理名	使用者名	OSタイプ	OSバージョン
<input type="checkbox"/>	1	総務課	SC-03D_0000000014	江藤 花子	Android	9
<input type="checkbox"/>	2	総務課	hammerhead_00000000...	六角 富夫	Android	10
<input type="checkbox"/>	4	人事課	N-04C_0000000020	江村 太郎	Android	11
<input type="checkbox"/>	5	営業部	EB-A71GJ_0000000019	橋中 栄一郎	Android	11
<input type="checkbox"/>	6	営業部	L-22D_0000000016	内田 健太	Android	11
<input type="checkbox"/>	7	営業1課	404KC_0000000023	中田 真由美	Android	10
<input type="checkbox"/>	8	営業1課	picasso_aapcus6jp_000...	橘 秀雄	Android	11
<input type="checkbox"/>	13	営業1課	404KC_0000000023	石井 健二	Android	9
<input type="checkbox"/>	14	営業2課	404KC_0000000018	平尾 晋作	Android	9
<input type="checkbox"/>	15	営業2課	404KC_0000000007	佐藤 理恵子	Android	10
<input type="checkbox"/>	28	システム部	SO-02C_0000000015	元岸 雄三	Android	11
<input type="checkbox"/>	30	システム1課	GP2_0000000002	中島 雄二	Android	11
<input type="checkbox"/>	31	システム1課	FAR7_0000000004	共有タブレット (システム部...	Android	9

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。

Android SC-03D_0000000014 - デバイス詳細

管理No. 1

デバイスグループ: 総務課 | 使用者名: 江藤 花子 | 電話番号: 090xxxxxxx | アカウントのメールアドレス: at10.motex@gmail.com | 最終稼働: 4時間前

管理情報

- デバイスグループ
- デバイス情報
- ネットワーク
- セキュリティ
- インストールアプリ
- 位置情報
- 操作ログ
- アラート
- リモート操作**
- クライアント

リモート操作を実行する ▼

- リモートロックを実行
- リモートワイブを実行

設定日時: 2017/12/01 15:37:55
 実行者: 設定管理者 (元中)
 内容: リモートロック
 状態: 成功
 実行日時: 2017/12/01 15:38:12
 詳細: デバイスをロックしました。

リモートロック:リジェクト
 2017/11/30 16:56:46 に実行されました。

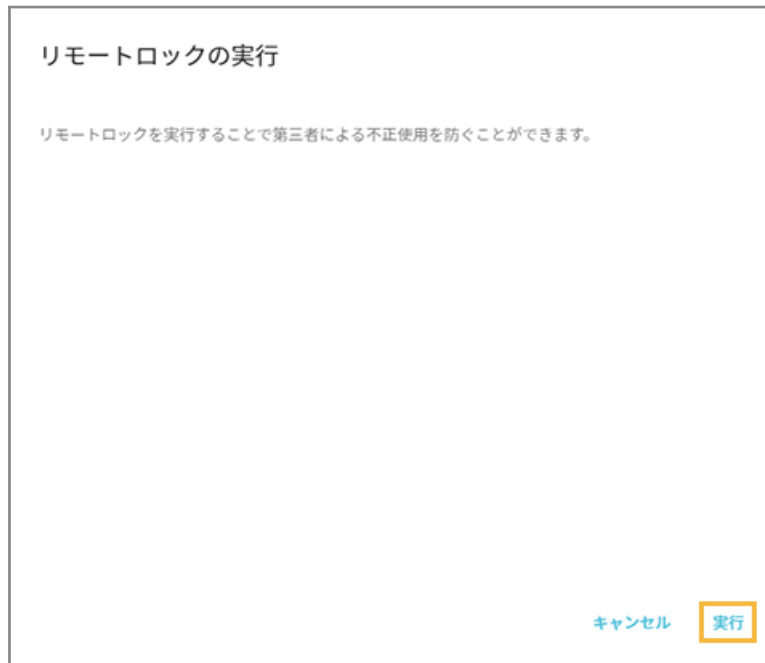
リモートワイブ:成功
 2017/11/30 16:45:55 に実行されました。

リモートワイブ:成功
 2017/11/30 16:45:55 に実行されました。

- リモートロックの場合

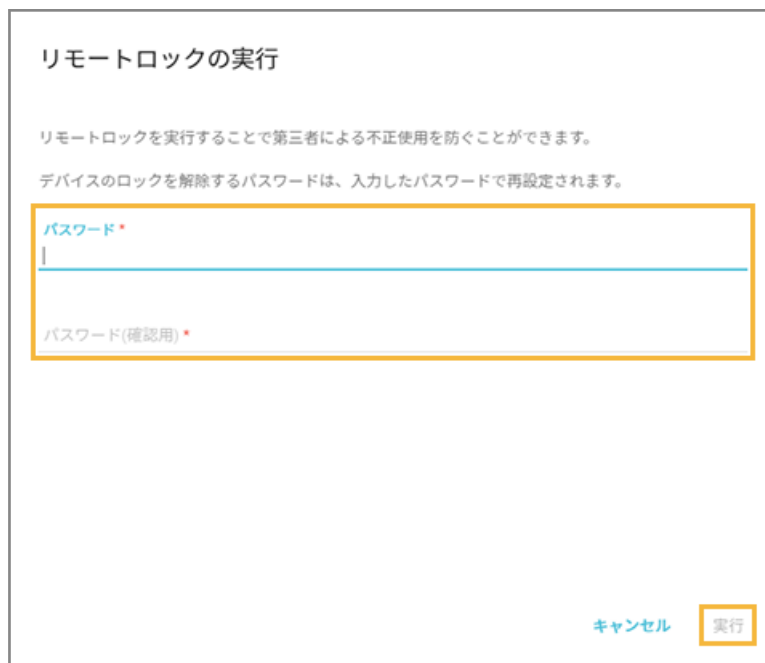
Android 11 以上の場合

[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。

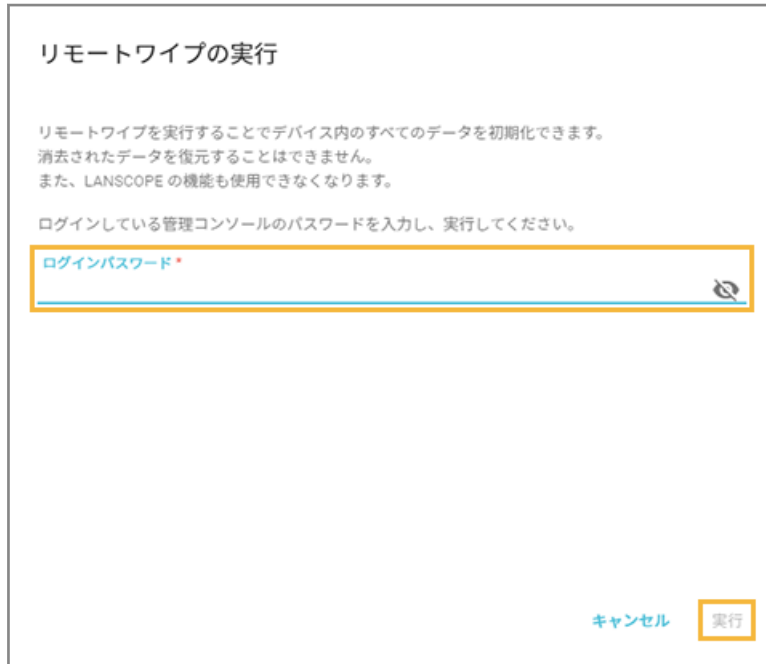


注意

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。

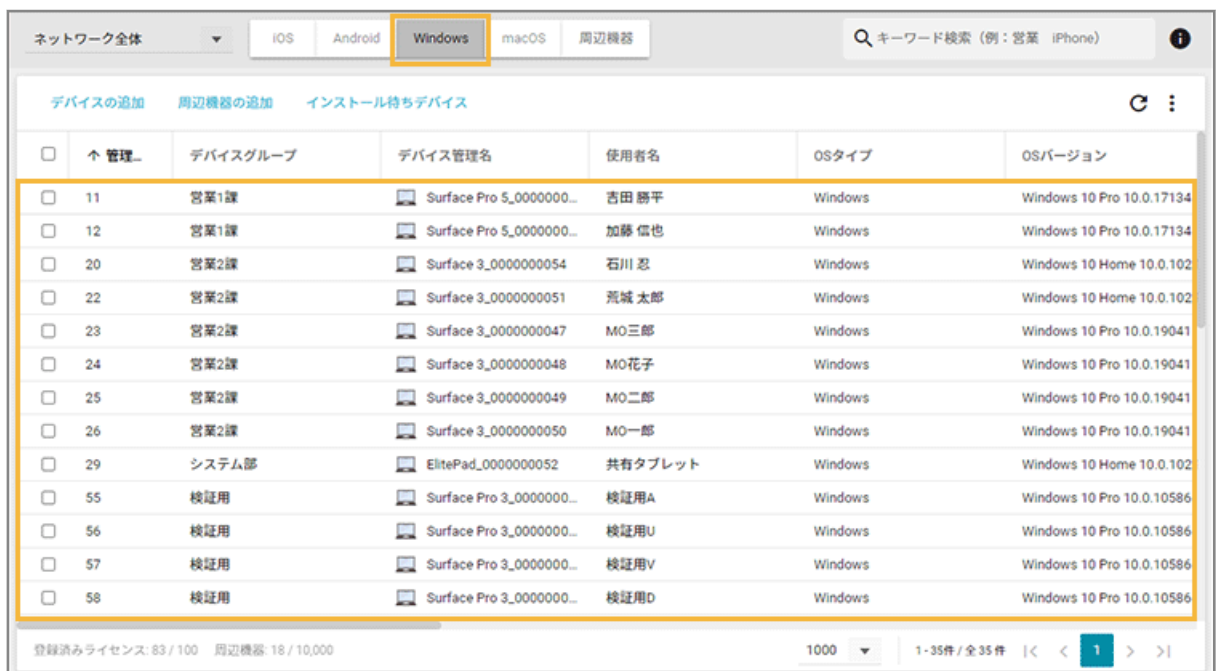


■ Windows の場合

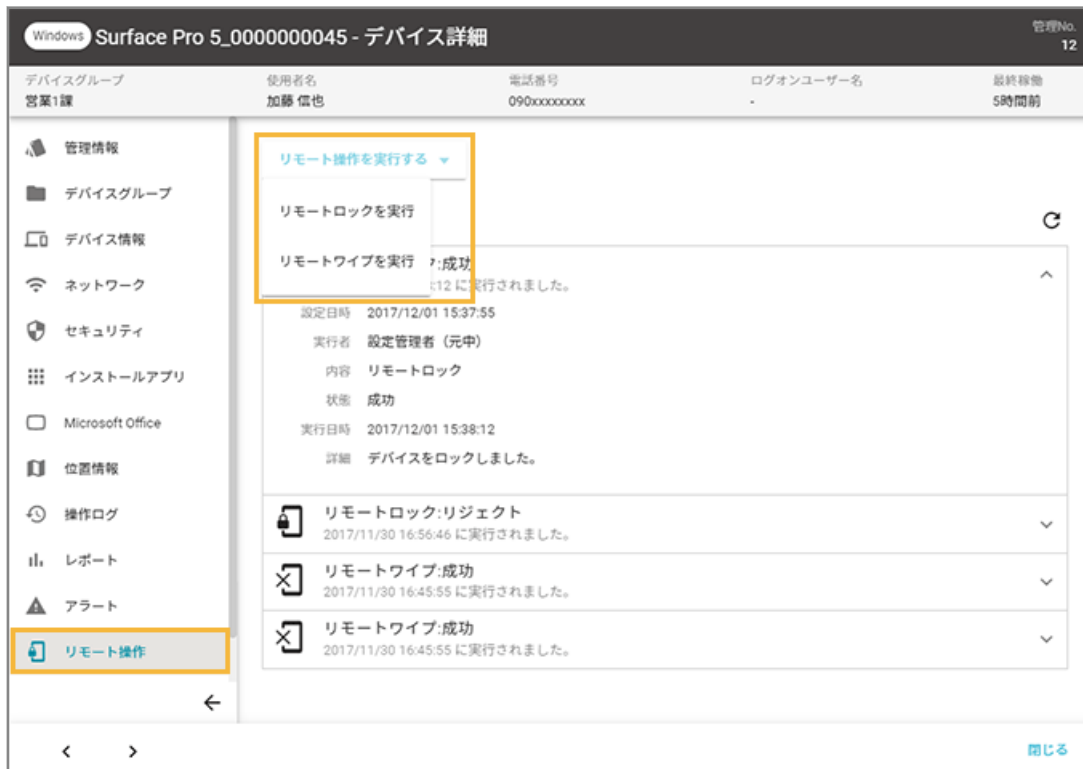
1. [リスト] の [デバイス] をクリックします。



2. OS をクリックし、デバイスをクリックします。

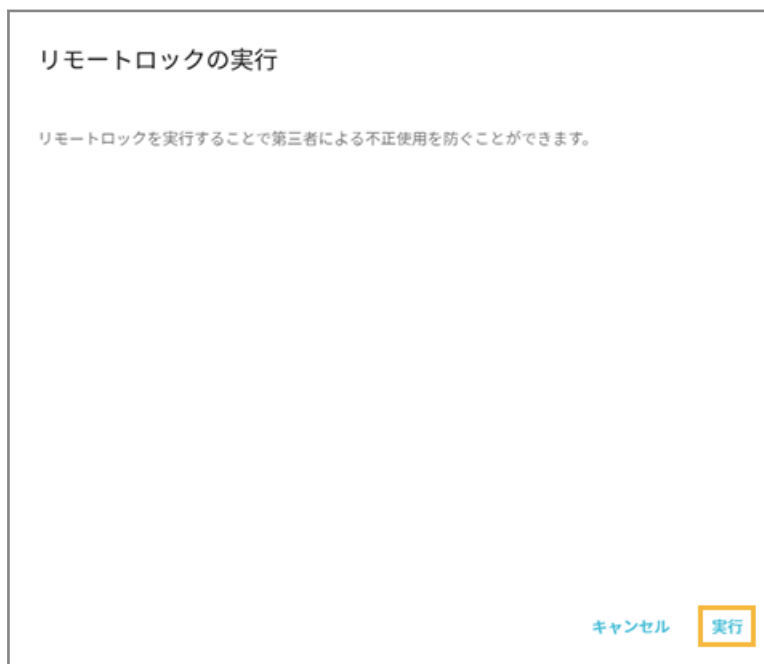


3. **「リモート操作」** をクリックし、**「リモート操作を実行する」** をクリックして、リモート操作を選択します。



- 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。

リモートワイプの実行

リモートワイプを実行し、デバイスに保存されたデータにアクセスできないようにします。
保存されたデータにアクセスするためには、回復キーを入力する必要があります。
また、LANSCOPE の機能も使用できなくなります。

ログインしている管理コンソールのパスワードを入力し、実行してください。

ログインパスワード *

キャンセル 実行

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-303「初期設定ガイド for Windows」を参照してください。

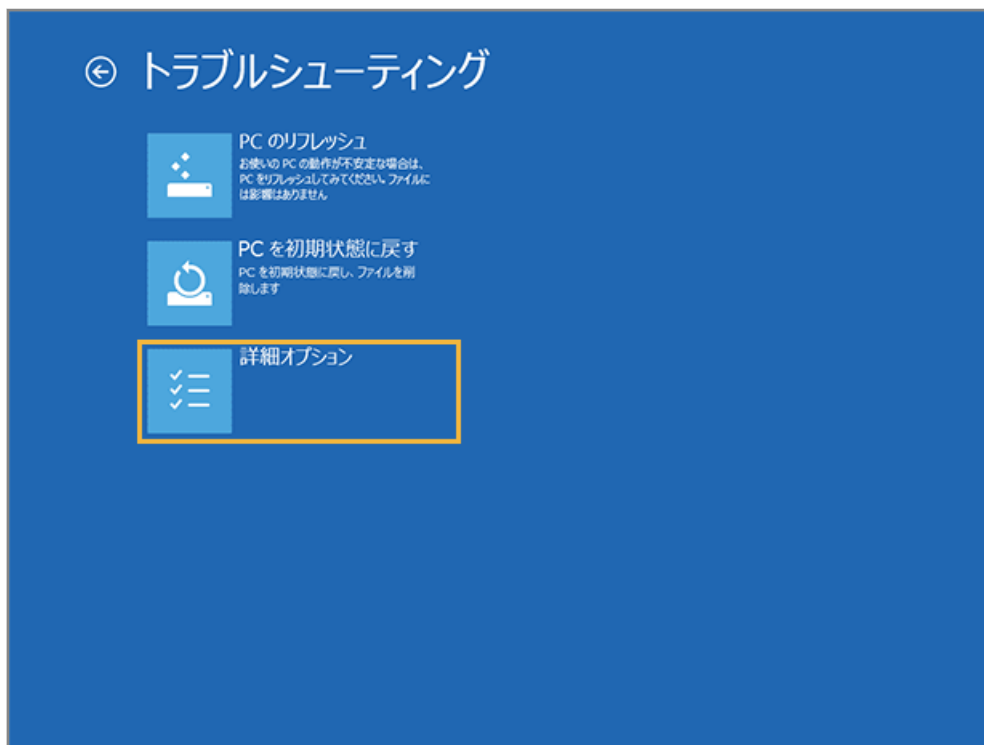
1. デバイスの電源を入れると、次の画面が表示されます。保存していたパスワード（回復キー）を入力し、[Enter] キーを押します。



2. **【トラブルシューティング】をクリックします。**



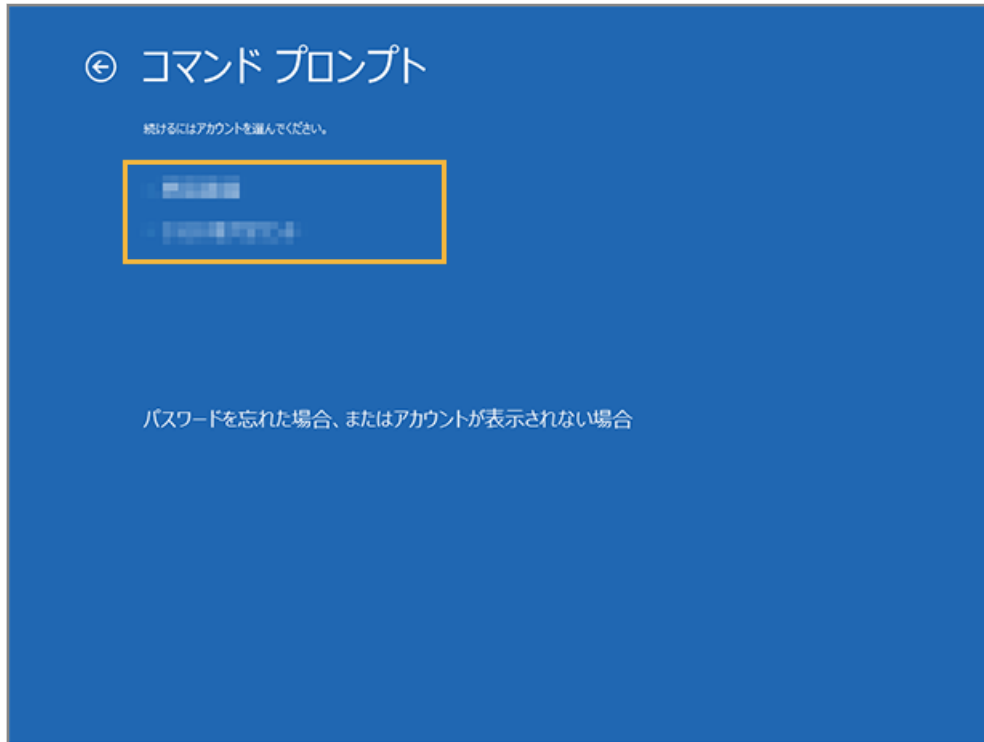
3. **【詳細オプション】をクリックします。**



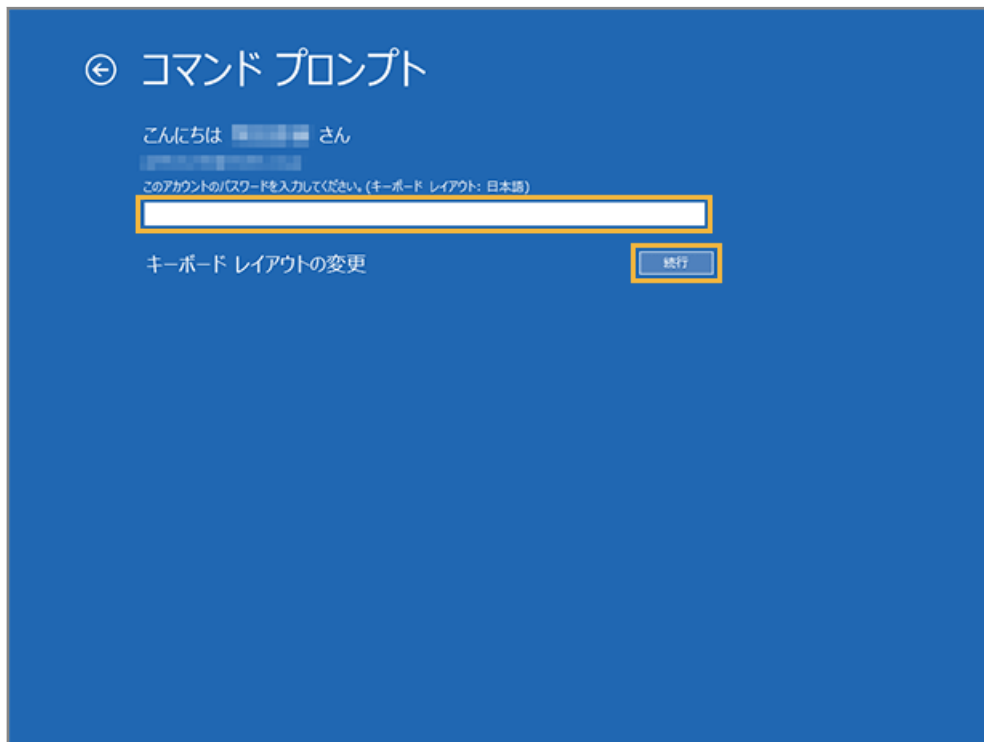
4. [コマンドプロンプト] をクリックします。



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
```

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>manage-bde.exe c: -off
BitLocker ドライブ暗号化: 構成ツール Version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

暗号化の解除は現在実行中です。

C:\Windows\system32>
```

→ 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
```

```
暗号化の解除は現在実行中です。

C:\Windows\system32>manage-bde.exe c: -status
BitLocker ドライブ暗号化: 構成ツール Version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

ボリューム C: []
[OS ボリューム]

サイズ: 59.66 GB
BitLocker のバージョン: 2.0
変換状態: 暗号化の解除を実行中です
暗号化された割合: 32.5%
暗号化の方法: AES 128
保護状態: 保護はオフです
ロック状態: ロック解除
識別子フィールド: 不明
キーの保護機能:
    パスワード
    数字パスワード
```

→ 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
```

```
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>manage-bde.exe c: -status
BitLocker ドライブ暗号化: 構成ツール Version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

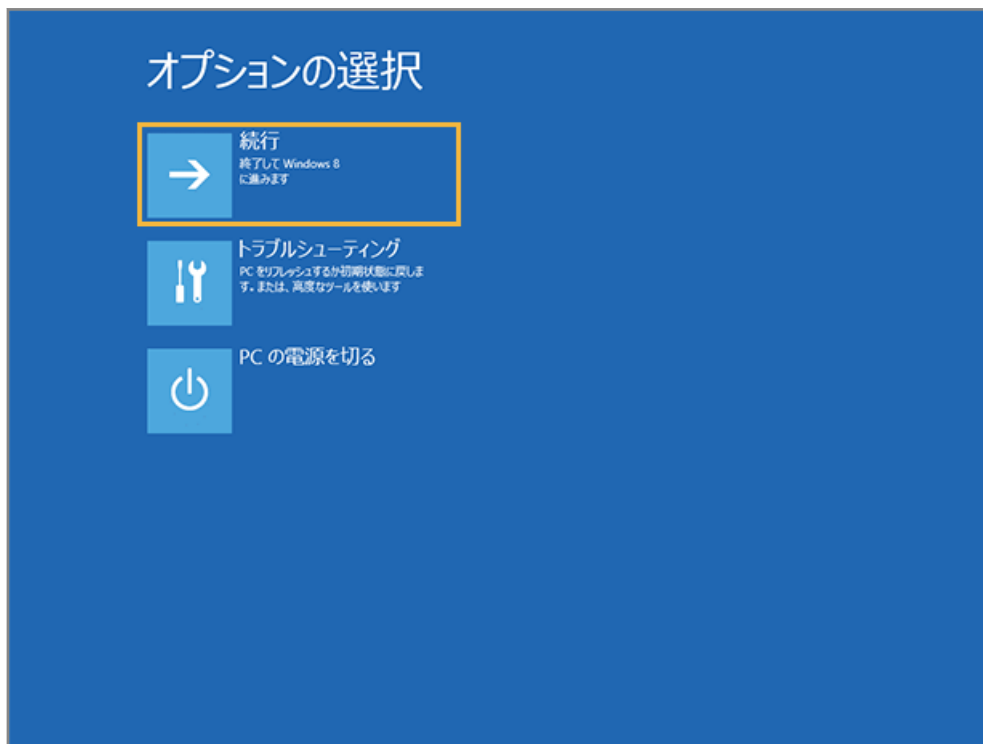
ボリューム C: [ ]
[OS ボリューム]

サイズ: 59.66 GB
BitLocker のバージョン: なし
変換状態: 暗号化は完全に解除されています
暗号化された割合: 0.0%
暗号化の方法: なし
保護状態: 保護はオフです
ロック状態: ロック解除
識別子フィールド: なし
キーの保護機能: 見つかりません

C:\Windows\system32>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。



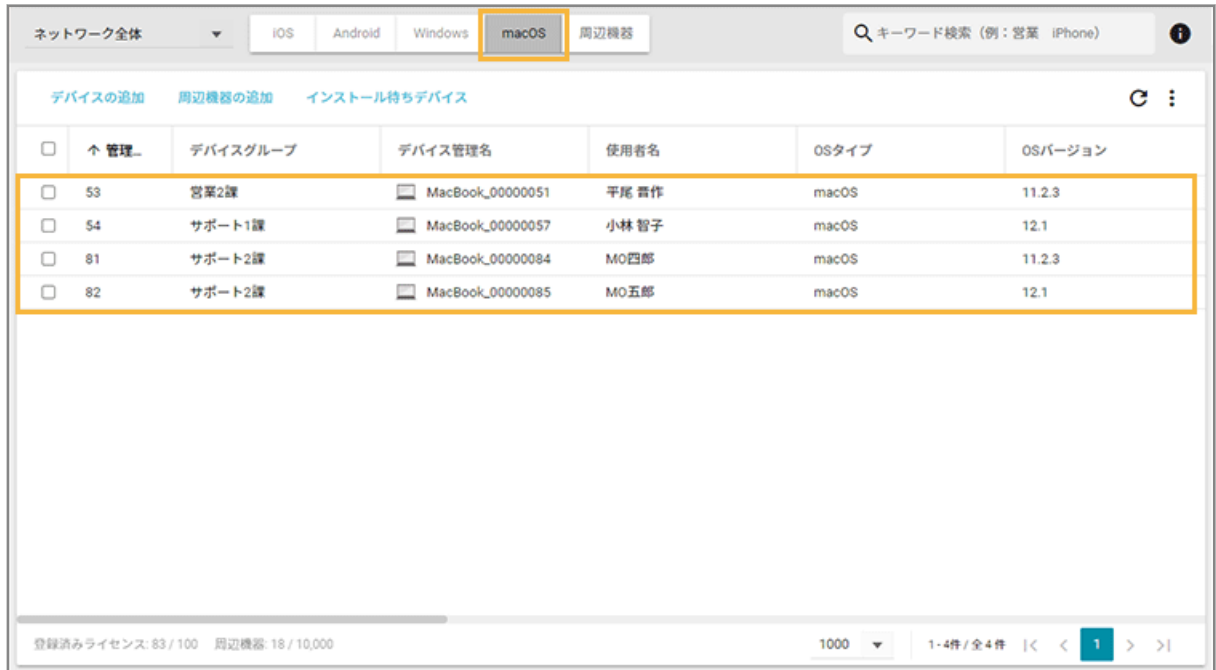
→ デバイス復旧が完了します。

■ 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。

リモートロックの実行

リモートロックを実行することで第三者による不正使用を防ぐことができます。

ロック解除 PIN コード

Mac デバイスのロックを解除する際に必要となります。
一度リモートロックを実行すると Mac デバイスはネットワークに接続できなくなり、この PIN コード以外でのロック解除ができなくなります。
必ずメモを取るなどして PIN コードを紛失しないようにしてください。

カスタムメッセージ

リモートロックが実行されたデバイスの画面にメッセージを表示します。

キャンセル

- 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。

リモートワイプの実行

リモートワイプを実行することでデバイス内のすべてのデータを初期化できます。
消去されたデータを復元することはできません。
また、LANSCOPE の機能も使用できなくなります。

ロック解除 PIN コードの入力

Mac デバイスの初期化を開始する際に必要となります。
リモートワイプを実行するとデバイスは再起動され PIN コードの入力画面が表示されます。
PIN コードが入力され初期化されるまでの間はネットワークに接続できなくなり操作を行えません。
必ずメモを取るなどして PIN コードを紛失しないようにしてください。

ログインしている管理コンソールのパスワードを入力し、実行してください。

キャンセル

リモート操作の実行結果を確認する

iOS

Android

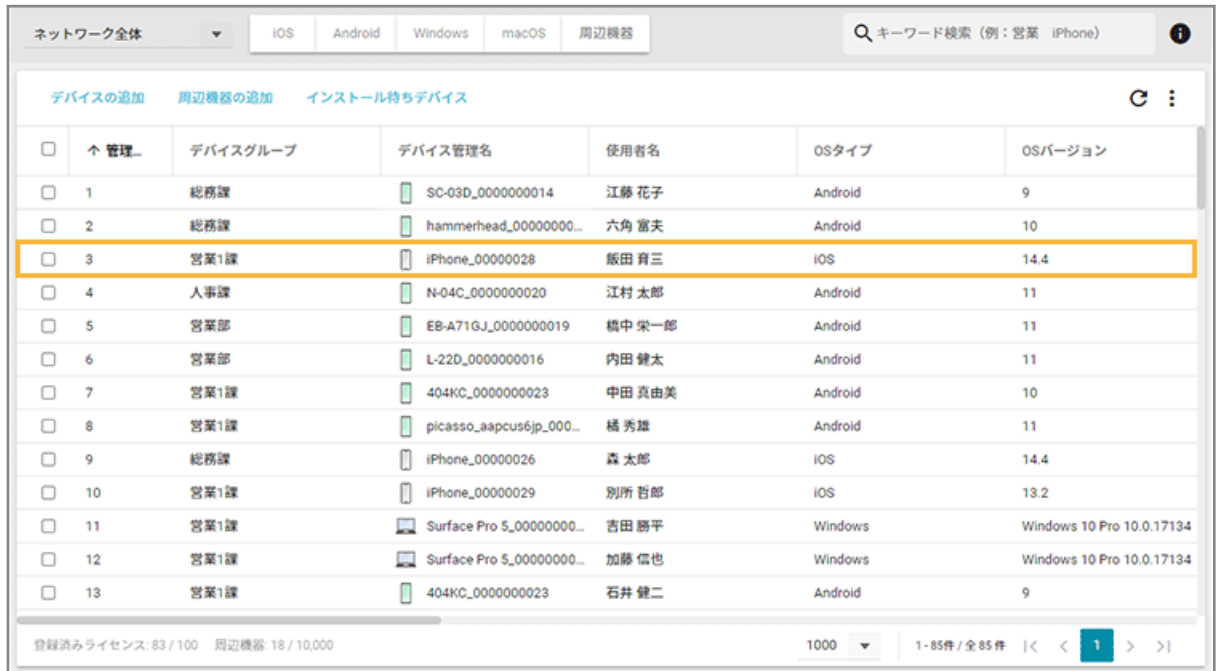
Windows

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。
	(紛失モードオンの場合) デバイスの紛失モードをオンにしました。
	(位置情報取得の場合) デバイスの位置情報を取得しました。
	(紛失モードオフの場合) デバイスの紛失モ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。(*)

OS	デバイスの状態	実行履歴の状態	対処方法
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-301 「初期設定ガイド for iOS/iPadOS」
- An-302 「初期設定ガイド for Android」
- An-303 「初期設定ガイド for Windows」
- An-304 「初期設定ガイド for macOS」

2-4 アプリ情報を確認する

iOS

Android

Windows

macOS

「どのアプリ」が「どのデバイス」にインストールされているかを確認できます。

1. [リスト] の [アプリ] をクリックします。



2. OS を選択します。



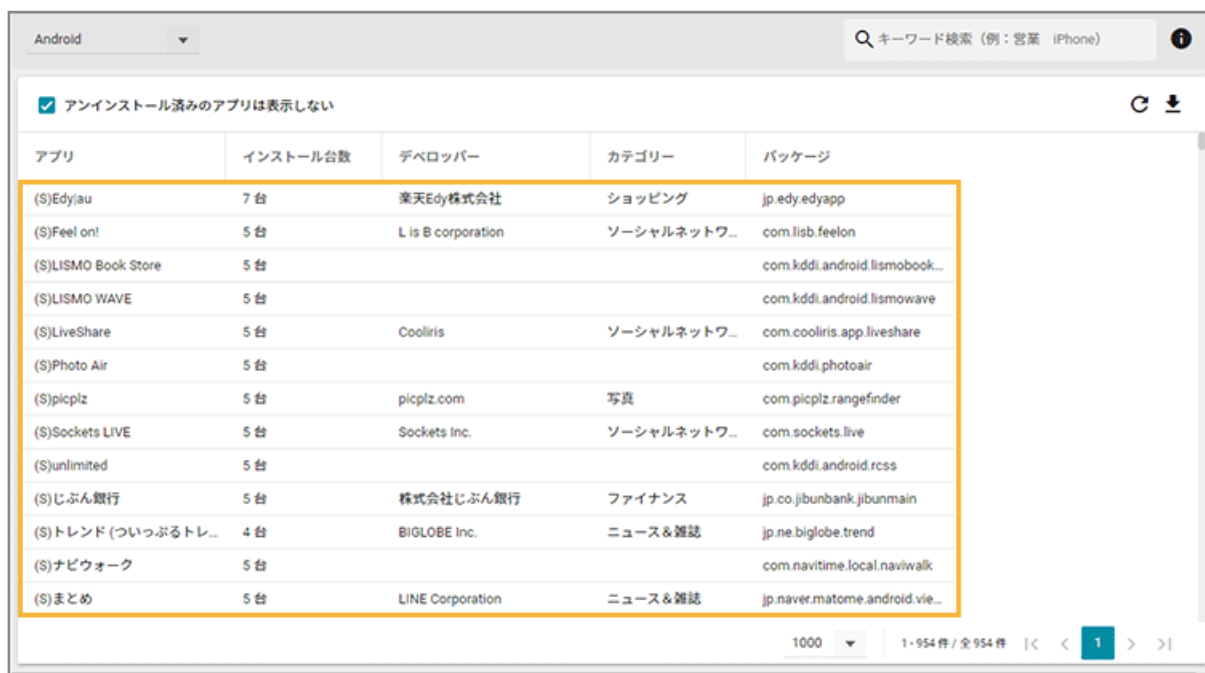
OS によって、取得できるアプリ情報は異なります。

OS	アプリ情報
iOS (*1)	アプリ名/管理アプリ (*2) /インストール台数/デベロッパー/カテゴリ (*3) /アプリケーション ID
Android	アプリ名/インストール台数/デベロッパー/カテゴリ (*4) /パッケージ名
Windows	アプリ名/インストール台数/デベロッパー/アプリ種別 (デスクトップアプリ/ストアアプリ) (*5) /パッケージ名
macOS	アプリ名/インストール台数/デベロッパー/カテゴリ (*6) /アプリケーション ID

*1 : プリインストールアプリの情報は取得されません。

- *2 : 管理アプリとは、エンドポイントマネージャーからアプリ配信機能で配信し、インストールしたアプリを指します。
- *3 : App Store のカテゴリ情報を取得します。In-House（自社開発）アプリの場合、カテゴリが組み込まれていれば、その情報を取得します。
- *4 : Google Play ストアのカテゴリ情報を取得します。In-House（自社開発）アプリの場合、カテゴリが組み込まれていれば、その情報を取得します。
- *5 : デスクトップアプリはコントロールパネルの「プログラムと機能」の情報、ストアアプリは Microsoft ストアからインストールしたアプリの情報を取得します。
- *6 : App Store のカテゴリ情報を取得します。App Store 以外（.dmg ファイルからインストールするなど）のアプリについてはカテゴリは表示されません。

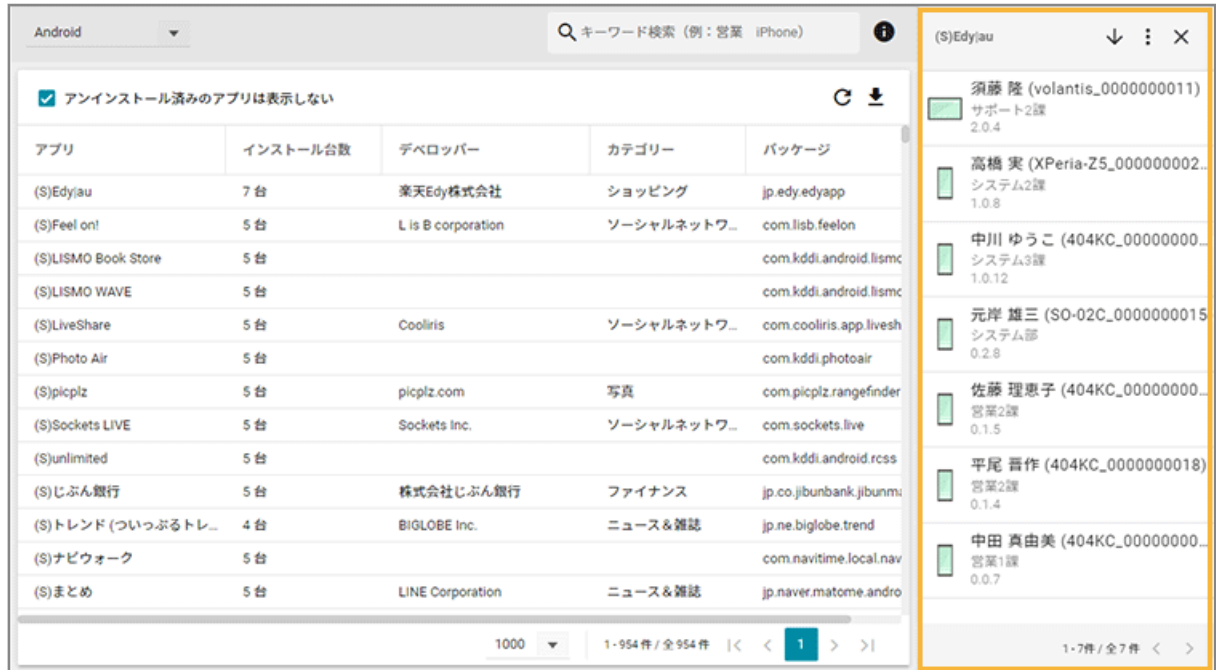
3. アプリをクリックします。



アプリ	インストール台数	デベロッパー	カテゴリ	パッケージ
(S)Edy!au	7 台	楽天Edy株式会社	ショッピング	jp.edy.edyapp
(S)Feel on!	5 台	L is B corporation	ソーシャルネットワ...	com.lisb.feelon
(S)LISMO Book Store	5 台			com.kddi.android.lismobook...
(S)LISMO WAVE	5 台			com.kddi.android.lismowave
(S)LiveShare	5 台	Cooliris	ソーシャルネットワ...	com.cooliris.app.liveshare
(S)Photo Air	5 台			com.kddi.photoair
(S)picplz	5 台	picplz.com	写真	com.picplz.rangefinder
(S)Sockets LIVE	5 台	Sockets Inc.	ソーシャルネットワ...	com.sockets.live
(S)unlimited	5 台			com.kddi.android.rcss
(S)じぶん銀行	5 台	株式会社じぶん銀行	ファイナンス	jp.co.jibunbank.jibunmain
(S)トレンド(ついっふるトレ...	4 台	BIGLOBE Inc.	ニュース&雑誌	jp.ne.biglobe.trend
(S)ナビウォーク	5 台			com.navitime.local.naviwalk
(S)まとめ	5 台	LINE Corporation	ニュース&雑誌	jp.naver.matome.android.vie...

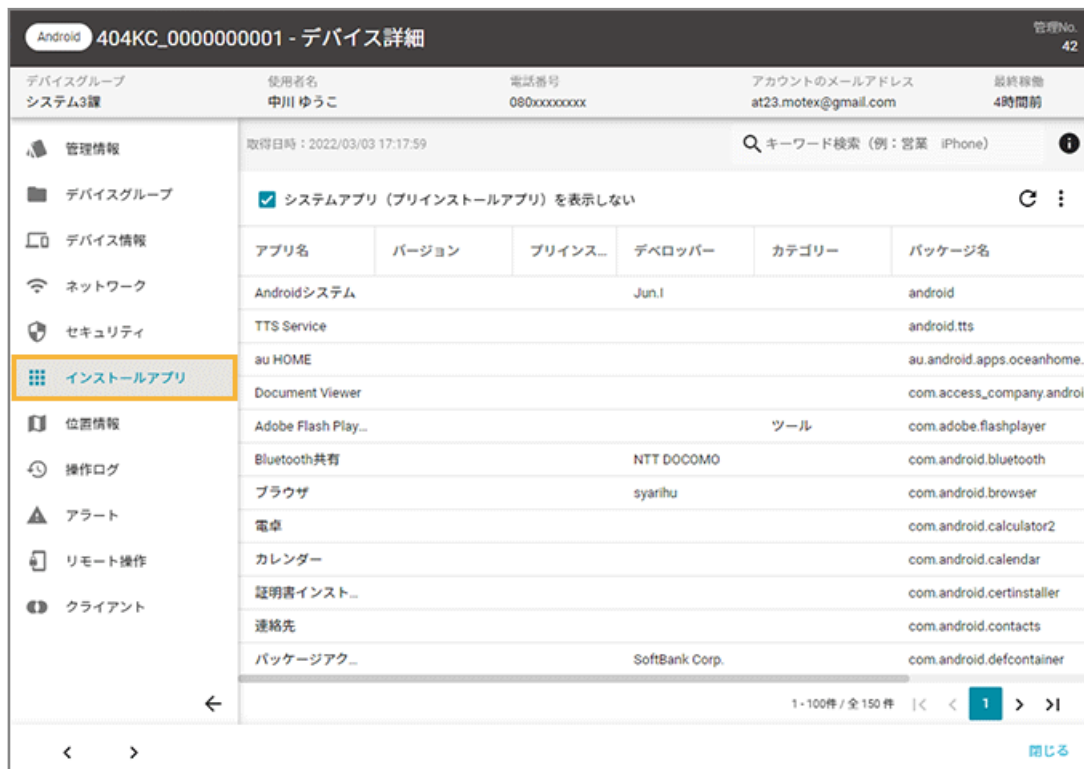
→ 選択したアプリがインストールされているデバイスが、画面右側に一覧表示されます。

4. デバイスをクリックします。



→ 「デバイス詳細」画面の「インストールアプリ」が表示されます。

5. インストールしているアプリを確認します。



2-5 プロファイル情報を確認する

iOS

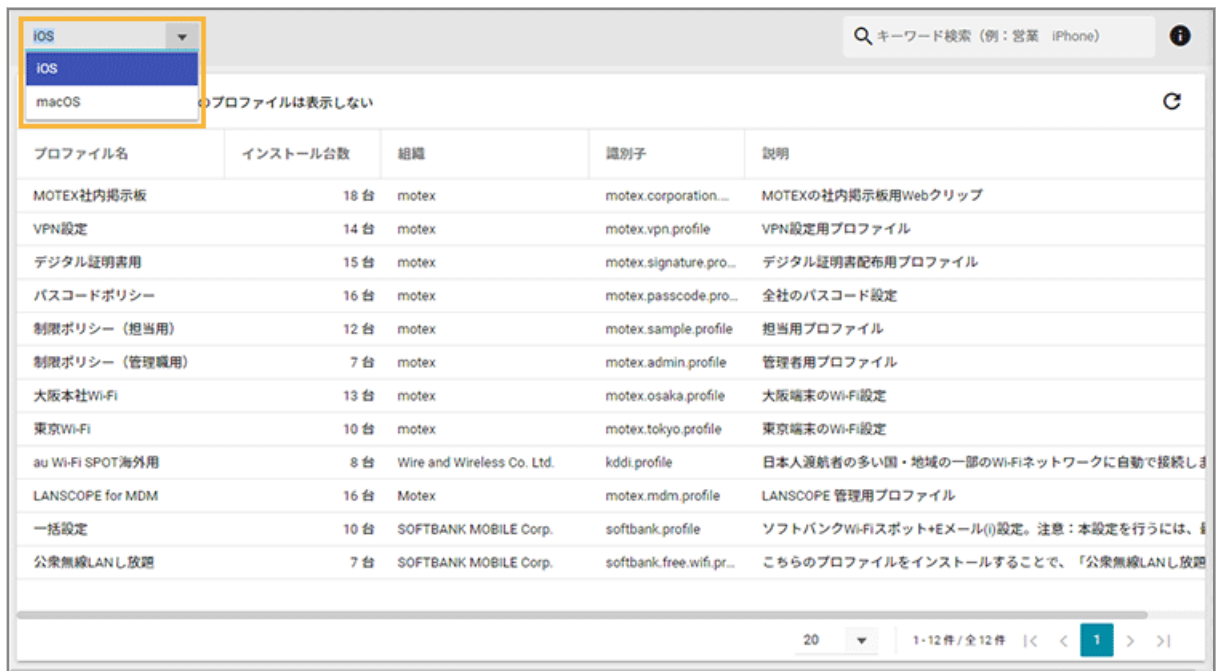
macOS

「どのプロファイル」が「どのデバイス」にインストールされているかを確認できます。

1. [リスト] の [プロファイル] をクリックします。



2. OS を選択します。



3. プロファイルをクリックします。

プロファイル名	インストール台数	組織	識別子	説明
MOTEX社内掲示板	18台	motex	motex.corporation...	MOTEXの社内掲示板用Webクリップ
VPN設定	14台	motex	motex.vpn.profile	VPN設定用プロファイル
デジタル証明書用	15台	motex	motex.signature.pro...	デジタル証明書配布用プロファイル
パスコードポリシー	16台	motex	motex.passcode.pro...	全社のパスコード設定
制限ポリシー (担当用)	12台	motex	motex.sample.profile	担当用プロファイル
制限ポリシー (管理職用)	7台	motex	motex.admin.profile	管理者用プロファイル
大阪本社Wi-Fi	13台	motex	motex.osaka.profile	大阪端末のWi-Fi設定
東京Wi-Fi	10台	motex	motex.tokyo.profile	東京端末のWi-Fi設定
au Wi-Fi SPOT海外用	8台	Wire and Wireless Co. Ltd.	kddi.profile	日本人源航者の多い国・地域の一部のWi-Fiネットワークに自動で接続し
LANSCOPE for MDM	16台	Motex	motex.mdm.profile	LANSCOPE 管理用プロファイル
一括設定	10台	SOFTBANK MOBILE Corp.	softbank.profile	ソフトバンクWi-Fiスポット+Eメール(i)設定。注意：本設定を行うには、
公衆無線LANし放題	7台	SOFTBANK MOBILE Corp.	softbank.free.wifi.pr...	こちらのプロファイルをインストールすることで、「公衆無線LANし放題

→ 選択したプロファイルがインストールされているデバイスが、画面右側に一覧表示されます。

4. デバイスをクリックします。

プロファイル名	インストール台数	組織	識別子	説明
MOTEX社内掲示板	18台	motex	motex.corporation...	MOTEXの社内掲示板用V
VPN設定	14台	motex	motex.vpn.profile	VPN設定用プロファイル
デジタル証明書用	15台	motex	motex.signature.pro...	デジタル証明書配布用フ
パスコードポリシー	16台	motex	motex.passcode.pro...	全社のパスコード設定
制限ポリシー (担当用)	12台	motex	motex.sample.profile	担当用プロファイル
制限ポリシー (管理職用)	7台	motex	motex.admin.profile	管理者用プロファイル
大阪本社Wi-Fi	13台	motex	motex.osaka.profile	大阪端末のWi-Fi設定
東京Wi-Fi	10台	motex	motex.tokyo.profile	東京端末のWi-Fi設定
au Wi-Fi SPOT海外用	8台	Wire and Wireless Co. Ltd.	kddi.profile	日本人源航者の多い国・
LANSCOPE for MDM	16台	Motex	motex.mdm.profile	LANSCOPE 管理用プロフ
一括設定	10台	SOFTBANK MOBILE Corp.	softbank.profile	ソフトバンクWi-Fiスポッ
公衆無線LANし放題	7台	SOFTBANK MOBILE Corp.	softbank.free.wifi.pr...	こちらのプロファイルを

デバイス	OS
鈴木 一 (iPhone_00000031)	iPhone
森 太郎 (iPhone_00000026)	iPhone
別所 哲郎 (iPhone_00000029)	iPhone
飯田 育三 (iPhone_00000028)	iPhone
島山 哲夫 (iPhone_00000027)	iPhone
小林 哲司 (iPad_00000034)	iPad
細川 孝信 (iPad_00000035)	iPad
石川 忍 (iPhone_00000033)	iPhone
佐竹 信弘 (iPhone_00000032)	iPhone
北井 清二 (iPad_00000036)	iPad

→ 「デバイス詳細」画面の「プロファイル」が表示されます。

5. インストールしているプロファイルを確認します。

iPhone_0000031 - デバイス詳細

管理No. 17

デバイスグループ: 営業1課 | 使用人名: 鈴木一 | 電話番号: 080xxxxxxx | Apple ID: - | 最終稼働: 2日前

取得日時: 2022/03/03 17:17:59

8件のプロファイルがインストールされています

制限ポリシー (管理職用)	
motex 管理者用プロファイル	motex.admin.profile
MOTEX社内掲示板	
motex MOTEXの社内掲示板用Webクリップ	motex.corporation.web.profile
パスコードポリシー	
motex 全社のパスコード設定	motex.passcode.profile
デジタル証明書用	
motex デジタル証明書配布用プロファイル	motex.signature.profile
東京Wi-Fi	
motex 東京端末のWi-Fi設定	motex.tokyo.profile
VPN設定	
motex VPN設定用プロファイル	motex.vpn.profile
公衆無線LANし放題	
SOFTBANK MORII E Com	softbank-free-wifi.profile

閉じる

2-6 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。

発生していないアラートは表示しない

警告レベル	アラート	アラート台数
危険	未稼働期間が指定された期間を超過している	5台
注意	空き容量が不足している	2台
危険	パスコードロックの設定がオフになっている	4台
危険	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	3台
注意	SIMカードが抜き差しされた	2台
注意	iOSのバージョンが指定した範囲外になっている	2台
注意	もうすぐリース切れになる	1台
危険	SDカードが抜き差しされた	1台
危険	指定したアプリが実行された	1台
危険	新しくアプリがインストールされた	1台
危険	位置情報が取得されない設定になっている	1台
注意	LANSCOPE Client のバージョンが最新になっていない	1台

20 | 1-12件/全12件 | < < 1 > > |

→ 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。

警告レベル	アラート	アラート台数
危険	未稼働期間が指定された期間を超過している	5台
注意	空き容量が不足している	2台
危険	パスコードロックの設定がオフになっている	4台
危険	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	3台
注意	SIMカードが抜き差しされた	2台
注意	iOSのバージョンが指定した範囲外になっている	2台
注意	もうすぐリース切れになる	1台
危険	SDカードが抜き差しされた	1台
危険	指定したアプリが実行された	1台
危険	新しくアプリがインストールされた	1台
危険	位置情報が取得されない設定になっている	1台
注意	LANSCOPE Client のバージョンが最新になっていない	1台

デバイス名	所属
吉田 勝平 (Surface Pro 5_0000...	営業1課
MO一郎 (Surface 3_000000005)	営業2課
小林 智子 (HTC_ACE_00000000)	サポート1課
北里 智子 (FAR7_0000000012)	システム管理課
MO五郎 (MacBook_00000085)	サポート2課

→ 「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。

Windows Surface Pro 5_0000000044 - デバイス詳細 管理No. 11

デバイスグループ 営業1課	使用人名 吉田 勝平	電話番号 090xxxxxxx	ログオンユーザー名 -	最終稼働 6時間前
------------------	---------------	--------------------	----------------	--------------

- 管理情報
- デバイスグループ
- デバイス情報
- ネットワーク
- セキュリティ
- インストールアプリ
- Microsoft Office
- 位置情報
- 操作ログ
- レポート
- ⚠️ アラート
- リモート操作

- 危険 未稼働期間が指定された期間を超過している
- 危険 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

閉じる

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。

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。

- [3-1 レシピ一覧を管理する](#)
- [3-2 アクションを実行する](#)

登録済みのレシピ

レシピ名	内容	iOS	Android	Windows	macOS
LANSCOPE Client を配信する	MDM 構成プロファイルがインストールされたら、アプリ配信機能で LANSCOPE Client を配信します。	○	×	×	×
LANSCOPE の登録用 Clip を配信する	MDM 構成プロファイルがインストールされたら、プロファイル配信機能で登録用 Clip を配信します。	○	×	×	×
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。（*）	○	×	○	○
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。	○	○	×	×
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。	○	○	○	○
未稼働アラート	30 日間未稼働の場合にアラート（危険）にします。	○	○	○	○
空き容量不足アラート	空き容量が 25%以下になった場合にアラート（危険）にします。	○	○	○	○
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。	×	○	○	×
SIM カード抜き差しアラート	SIM の状態が変更された場合にアラート（危険）にします。	○	○	○	×

レシピ名	内容	iOS	Android	Windows	macOS
SDカード抜き差しアラート	SDカードが抜き差しされた場合にアラート（危険）にします。	×	○	×	×
新規アプリインストールアラート	新規にアプリがインストールされた場合にアラート（注意）にします。	×	○	×	×
タイムゾーン変更アラート	タイムゾーンが変更された場合にアラート（注意）にします。	×	○	×	×
新規プロファイルインストールアラート	プロファイルがインストールされた場合にアラート（注意）にします。	○	×	×	○
位置情報サービス無効アラート	デバイス側で位置情報が取得されない設定になっている場合にアラート（危険）にします。	×	○	○	×
Jailbreak 検知アラート	Jailbreak されている場合にアラート（危険）にします。	○	×	×	×
root 化検知アラート	root 化されている場合にアラート（危険）にします。	×	○	×	×

* : 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 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。

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](#)
- [レシピを任意のタイミングで実行する](#)
- [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

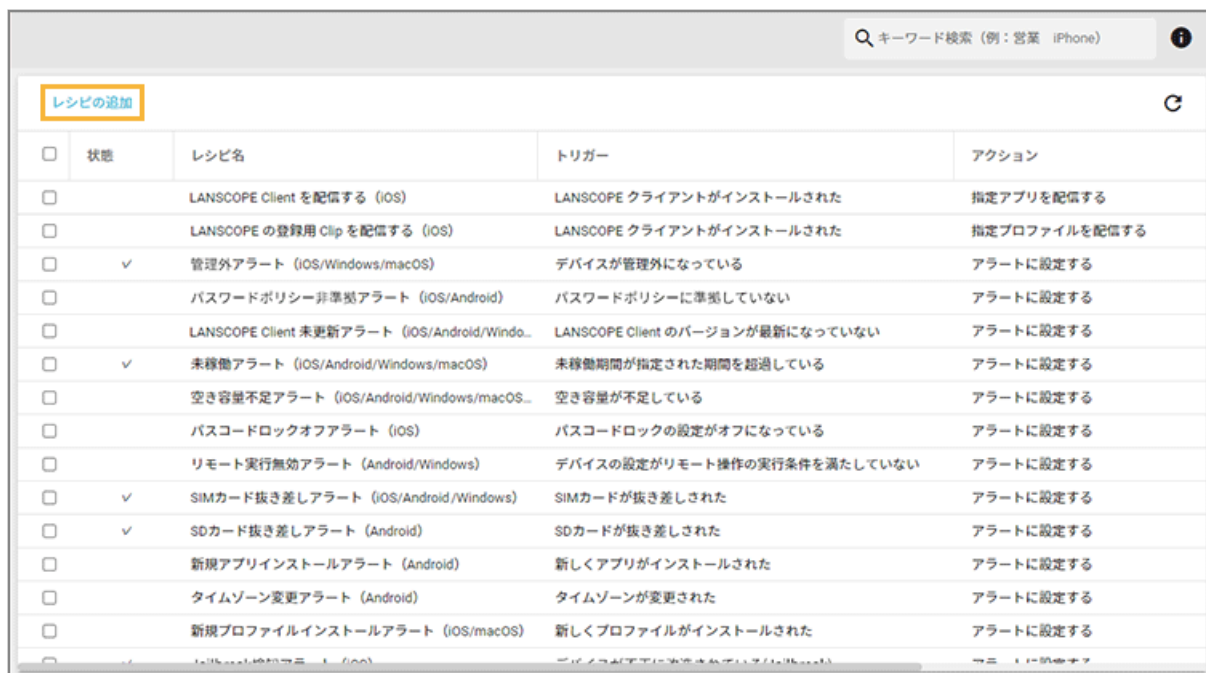
iOS Android Windows macOS

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ることで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。

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、[任意のタイミングで実行する] をクリックします。

トリガー	iOS	Android	Windows	macOS
リモートロックの実行が成功した	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LANSCOPE クライアントがインストールされた	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
パスワードポリシーに準拠していない	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
デバイスが管理外になっている	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LANSCOPE Client のバージョンが最新になっていない	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
任意のタイミングで実行する	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
定期的に行う	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
未稼働期間が指定された期間を超過している	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
新しくアプリがインストールされた	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

カテゴリー

選択すると、トリガーをカテゴリー別で表示できます。

トリガー

アクションを実行するきっかけになる条件です。

- 「任意のタイミングで実行する」を設定すると、管理者のタイミングでアクションを実行できます。
- 資産アラートに設定できるトリガーを選択したレシピは、最大 20 件作成できます。
- [定期的に行う] のトリガーを選択したレシピは、最大 50 件作成できます。

対応 OS

トリガーの対応 OS を「○」「×」で表示します。


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。

レシピのトリガーを選択 トリガー選択

トリガー *
任意のタイミングで実行する

レシピを実行する対象の絞り込み

 デバイスグループ (0 件)
選択

 デバイス (0 台)
選択

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. アクションを選択します。ここでは、[指定プロファイルを配信する] をクリックします。



対応 OS

アクションの対応 OS を「○」「×」で表示します。

8. 配信するプロファイルをチェックし、[選択] をクリックします。

プロファイルは、最大 10 件登録できます。



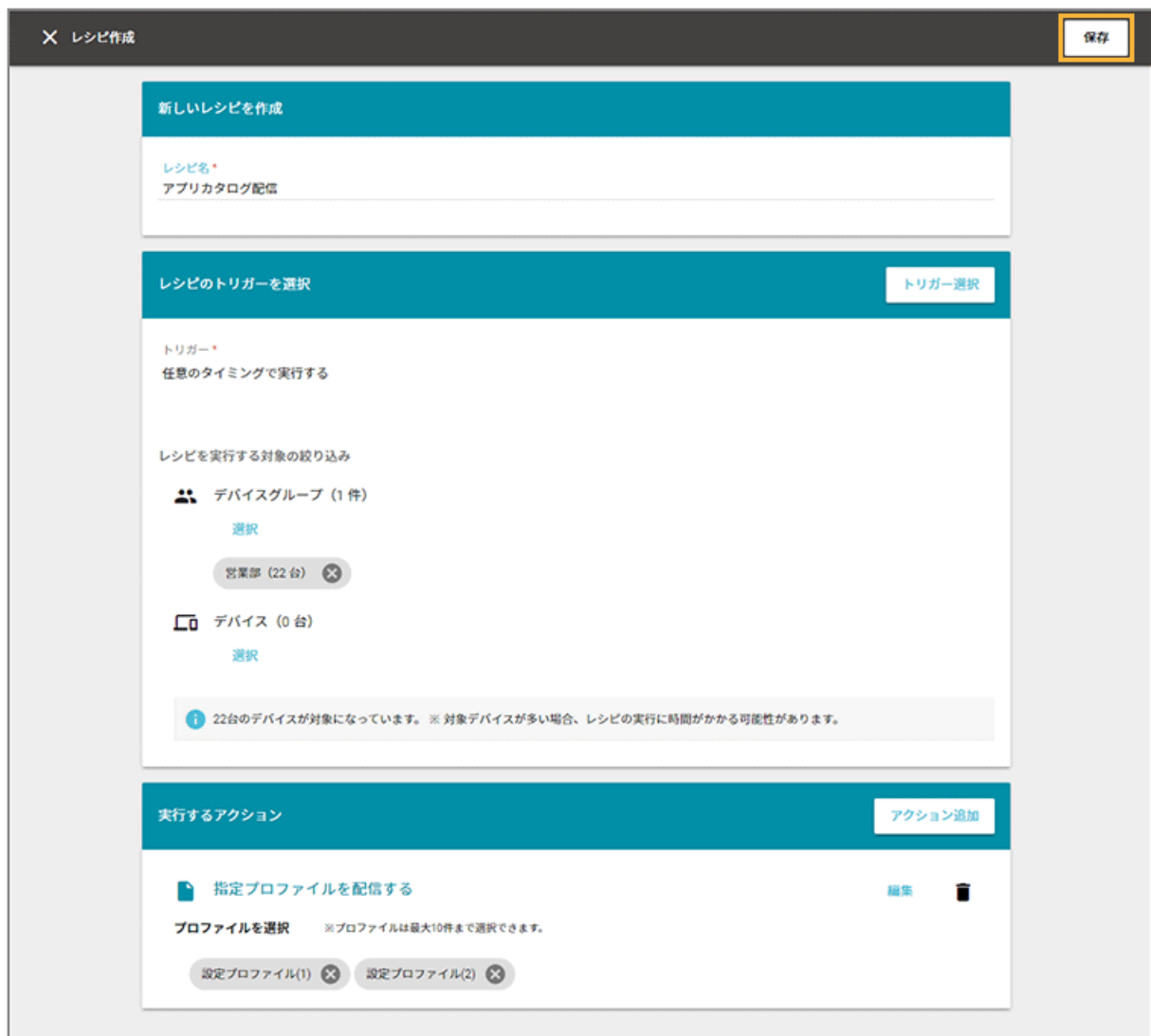
選択したアクションによって、設定項目は異なります。

アクション	設定項目
管理者にメールでお知らせする	配信先メールアドレス
指定プロファイルを送信する・取り除く	プロファイルを選択 (*)
指定アプリ (VPP アプリ) を送信する・アンインストールする	アプリを選択 (*)
指定プロビジョニングプロファイルを送信する・アンインストールする	プロビジョニングプロファイルを選択 (*)
メッセージを送信する	メッセージを選択 (*)
アンケートを送信する	アンケートを選択 (*)
アラートに設定する	アラートレベルを選択
アラートレポートを送信する	通知するアラート種別の選択、配信先メールアドレス
位置情報・操作ログを一括で出力する	出力設定を選択 (*)

* : [リスト] > [アクション] で、事前に設定が必要なアクションです。

9. 複数のアクションを設定する場合、手順 6～手順 8 を繰り返します。

10. 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。

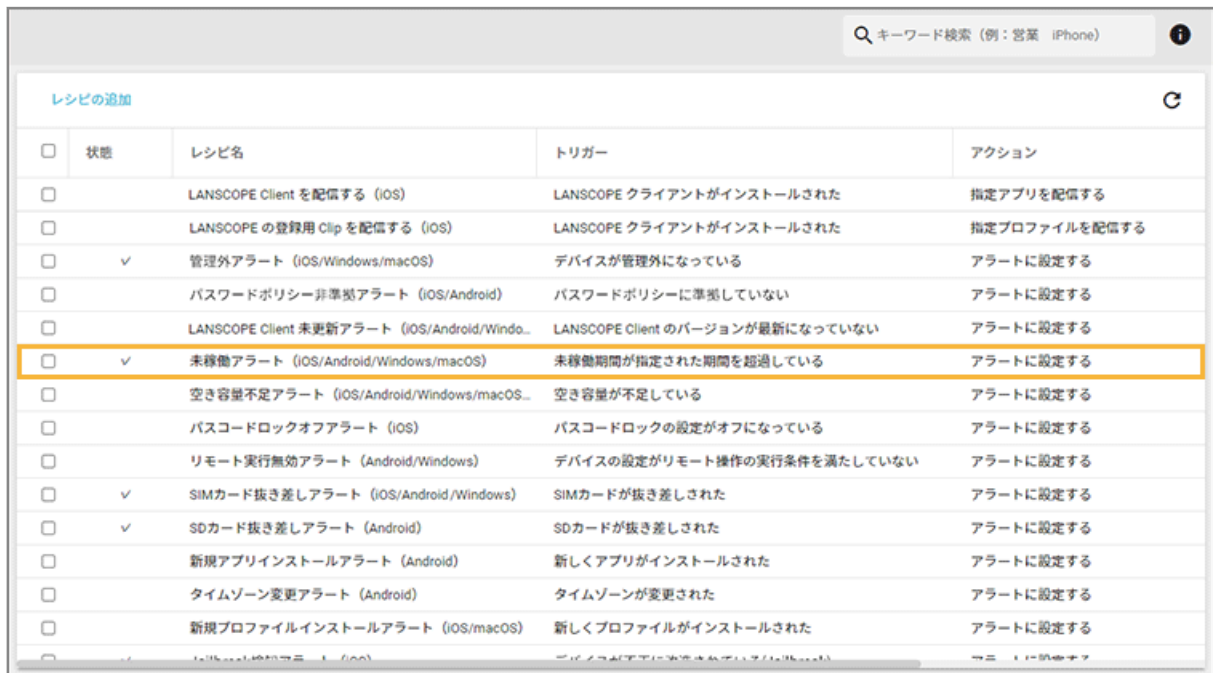
「有効」「無効」の表示は、次のとおりです。

「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。



<input type="checkbox"/>	状態	レシピ名	トリガー	アクション
<input type="checkbox"/>		LANSCOPE Client を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定アプリを配信する
<input type="checkbox"/>		LANSCOPE の登録用 Clip を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定プロフィールを配信する
<input type="checkbox"/>	✓	管理外アラート (iOS/Windows/macOS)	デバイスが管理外になっている	アラートに設定する
<input type="checkbox"/>		パスワードポリシー非準拠アラート (iOS/Android)	パスワードポリシーに準拠していない	アラートに設定する
<input type="checkbox"/>		LANSCOPE Client 未更新アラート (iOS/Android/Windows)	LANSCOPE Client のバージョンが最新になっていない	アラートに設定する
<input type="checkbox"/>		未稼働アラート (iOS/Android/Windows/macOS)	未稼働期間が指定された期間を超過している	アラートに設定する
<input type="checkbox"/>		空き容量不足アラート (iOS/Android/Windows/macOS)	空き容量が不足している	アラートに設定する
<input type="checkbox"/>		パスワードロックオフアラート (iOS)	パスワードロックの設定がオフになっている	アラートに設定する
<input type="checkbox"/>		リモート実行無効アラート (Android/Windows)	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	アラートに設定する
<input type="checkbox"/>	✓	SIMカード抜き差しアラート (iOS/Android/Windows)	SIMカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>	✓	SDカード抜き差しアラート (Android)	SDカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>		新規アプリインストールアラート (Android)	新しくアプリがインストールされた	アラートに設定する
<input type="checkbox"/>		タイムゾーン変更アラート (Android)	タイムゾーンが変更された	アラートに設定する
<input type="checkbox"/>		新規プロフィールインストールアラート (iOS/macOS)	新しくプロフィールがインストールされた	アラートに設定する

レシピを任意のタイミングで実行する

iOS

Android

Windows

macOS

■ レシピを今すぐ実行する

保存済みのレシピを、管理者のタイミングですぐに実行できます。

ステップ：

1. [トリガーを \[任意のタイミングで実行する\] に設定する](#)
2. [レシピを実行する](#)

ステップ 1： トリガーを [任意のタイミングで実行する] に設定する

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。

レシピの追加

検索 キーワード検索 (例: 営業 iPhone)

状態	レシピ名	トリガー	アクション
<input type="checkbox"/>	LANSCOPE Client を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定アプリを配信する
<input type="checkbox"/>	LANSCOPE の登録用 Clip を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定プロファイルを配信する
<input checked="" type="checkbox"/>	アプリカタログ配信	LANSCOPE クライアントがインストールされた	指定プロファイルを配信する
<input checked="" type="checkbox"/>	管理外アラート (iOS/Windows/macOS)	デバイスが管理外になっている	アラートに設定する
<input type="checkbox"/>	パスワードポリシー非準拠アラート (iOS/Android)	パスワードポリシーに準拠していない	アラートに設定する
<input type="checkbox"/>	LANSCOPE Client 未更新アラート (iOS/Android/Windows)	LANSCOPE Client のバージョンが最新になっていない	アラートに設定する
<input checked="" type="checkbox"/>	未稼働アラート (iOS/Android/Windows/macOS)	未稼働期間が指定された期間を超過している	アラートに設定する
<input type="checkbox"/>	空き容量不足アラート (iOS/Android/Windows/macOS)	空き容量が不足している	アラートに設定する
<input type="checkbox"/>	パスコードロックオフアラート (iOS)	パスコードロックの設定がオフになっている	アラートに設定する
<input type="checkbox"/>	リモート実行無効アラート (Android/Windows)	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	アラートに設定する
<input checked="" type="checkbox"/>	SIMカード抜き差しアラート (iOS/Android/Windows)	SIMカードが抜き差しされた	アラートに設定する
<input checked="" type="checkbox"/>	SDカード抜き差しアラート (Android)	SDカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>	新規アプリインストールアラート (Android)	新しくアプリがインストールされた	アラートに設定する
<input type="checkbox"/>	タイムゾーン変更アラート (Android)	タイムゾーンが変更された	アラートに設定する
<input type="checkbox"/>	新規プロファイルインストールアラート (iOS/macOS)	新規プロファイルがインストールされた	アラートに設定する

3. [編集] をクリックします。

← アプリカタログ配信

編集

このレシピを有効にする

アプリカタログ配信

LANSCOPE クライアントがインストールされた

レシピを実行する対象の絞り込み

デバイスグループ (1 件)
ネットワーク全体 (85 台)

85台のデバイスが対象になっています。 ※ 対象デバイスが多い場合、レシピの実行に時間がかかる可能性があります。

レシピで実行するアクション

指定プロファイルを配信する
アプリカタログ - 実行状況

レシピの実行履歴

[すべての実行履歴を確認する](#)

4. [トリガー選択] をクリックします。



5. [任意のタイミングで実行する] をクリックします。



6. [保存] をクリックします。



ステップ 2： レシピを実行する

1. トリガーを「任意のタイミングで実行する」に変更したレシピをクリックします。



検索: キーワード検索 (例: 営業 iPhone)

レシピの追加

<input type="checkbox"/>	状態	レシピ名	トリガー	アクション
<input type="checkbox"/>		LANSCOPE Client を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定アプリを配信する
<input type="checkbox"/>		LANSCOPE の登録用 Clip を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定プロフィールを配信する
<input type="checkbox"/>	✓	アプリカタログ配信	任意のタイミングで実行する	指定プロフィールを配信する
<input type="checkbox"/>	✓	管理外アラート (iOS/Windows/macOS)	デバイスが管理外になっている	アラートに設定する
<input type="checkbox"/>		パスワードポリシー非準拠アラート (iOS/Android)	パスワードポリシーに準拠していない	アラートに設定する
<input type="checkbox"/>		LANSCOPE Client 未更新アラート (iOS/Android/Windows)	LANSCOPE Client のバージョンが最新になっていない	アラートに設定する
<input type="checkbox"/>	✓	未稼働アラート (iOS/Android/Windows/macOS)	未稼働期間が指定された期間を超過している	アラートに設定する
<input type="checkbox"/>		空き容量不足アラート (iOS/Android/Windows/macOS)	空き容量が不足している	アラートに設定する
<input type="checkbox"/>		パスワードロックオフアラート (iOS)	パスワードロックの設定がオフになっている	アラートに設定する
<input type="checkbox"/>		リモート実行無効アラート (Android/Windows)	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	アラートに設定する
<input type="checkbox"/>	✓	SIMカード抜き差しアラート (iOS/Android/Windows)	SIMカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>	✓	SDカード抜き差しアラート (Android)	SDカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>		新規アプリインストールアラート (Android)	新しくアプリがインストールされた	アラートに設定する
<input type="checkbox"/>		タイムゾーン変更アラート (Android)	タイムゾーンが変更された	アラートに設定する
<input type="checkbox"/>		新規プロフィールインストールアラート (iOS/macOS)	新しいプロフィールがインストールされた	アラートに設定する

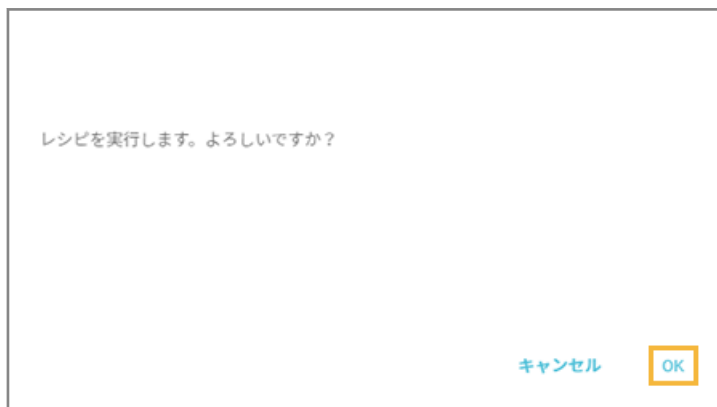
2.  をクリックします。

ポイント

レシピが無効の状態では、 は表示されません。「このレシピを有効にする」を  (有効) にしてください。



3. [OK] をクリックします。



→ レシピが実行されます。

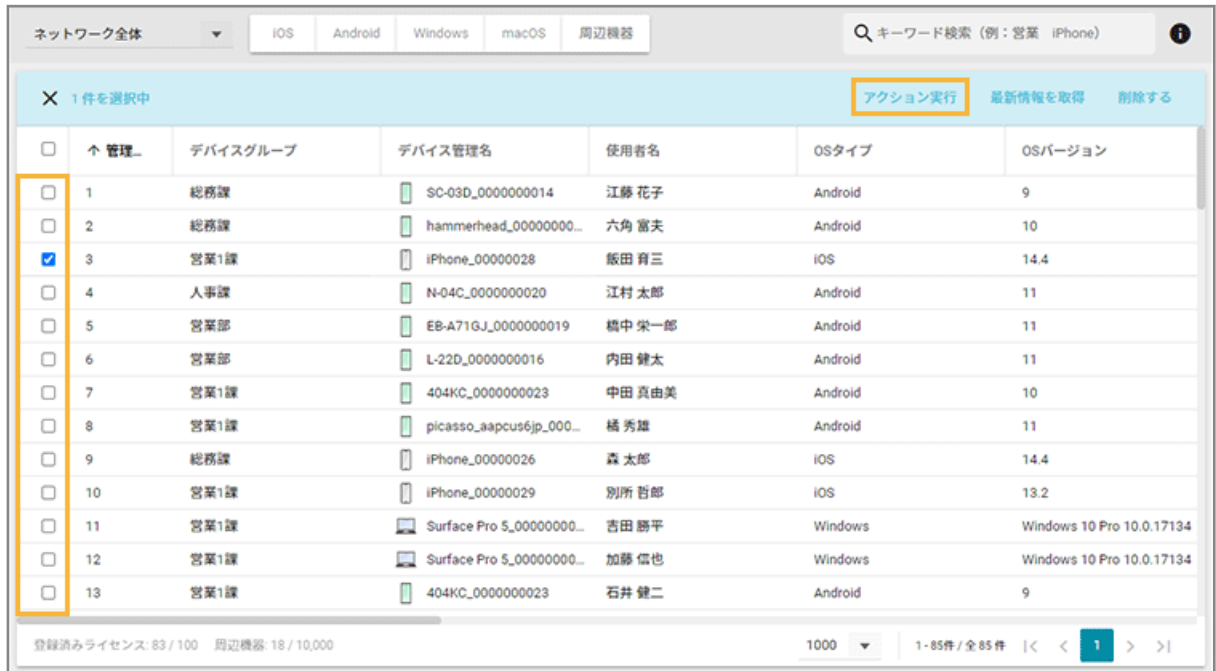
■ リストからアクションを実行する

選択したデバイスに対して、任意のタイミングでアクションを実行するレシピを作成できます。

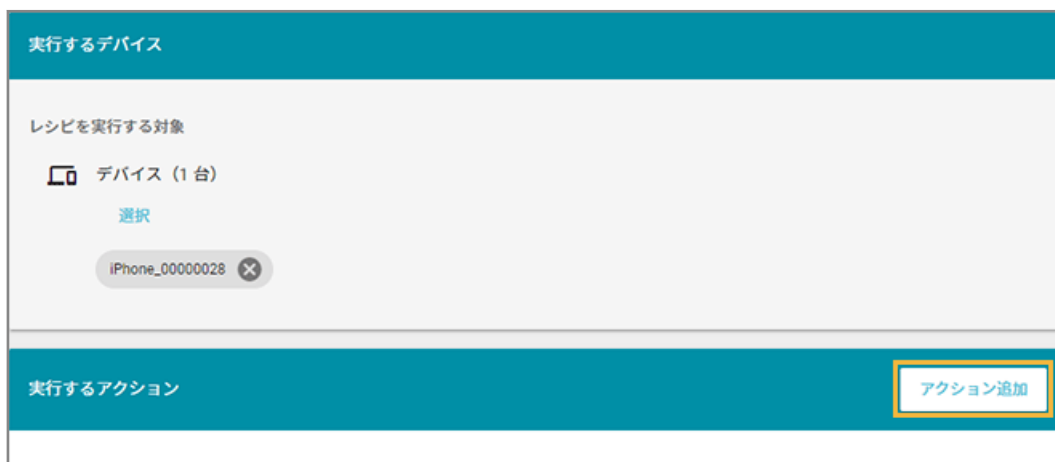
1. [リスト] の [デバイス] をクリックします。



2. デバイスをチェックし、[アクション実行] をクリックします。



3. [アクション追加] をクリックします。



4. アクションを選択します。

ここでは、[指定プロファイルを配信する] をクリックします。



→ 項目を設定し、[追加] をクリックして、「アクション実行」画面に戻ります。

5. [実行] をクリックします。



→ アクションが実行されます。

6. 実行結果を確認します。



→ [レシピとして保存する] をチェックすると、レシピが保存されます。

レシピの実行履歴を確認する



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。

状態	レシピ名	トリガー	アクション
<input type="checkbox"/>	LANSCOPE Client を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定アプリを配信する
<input type="checkbox"/>	LANSCOPE の登録用 Clip を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定プロファイルを配信する
<input checked="" type="checkbox"/>	管理外アラート (iOS/Windows/macOS)	デバイスが管理外になっている	アラートに設定する
<input type="checkbox"/>	パスワードポリシー非準拠アラート (iOS/Android)	パスワードポリシーに準拠していない	アラートに設定する
<input type="checkbox"/>	LANSCOPE Client 未更新アラート (iOS/Android/Windows)	LANSCOPE Client のバージョンが最新になっていない	アラートに設定する
<input checked="" type="checkbox"/>	未稼働アラート (iOS/Android/Windows/macOS)	未稼働期間が指定された期間を超過している	アラートに設定する
<input type="checkbox"/>	空き容量不足アラート (iOS/Android/Windows/macOS)	空き容量が不足している	アラートに設定する
<input type="checkbox"/>	パスワードロックオフアラート (iOS)	パスワードロックの設定がオフになっている	アラートに設定する
<input type="checkbox"/>	リモート実行無効アラート (Android/Windows)	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	アラートに設定する
<input checked="" type="checkbox"/>	SIMカード抜き差しアラート (iOS/Android/Windows)	SIMカードが抜き差しされた	アラートに設定する
<input checked="" type="checkbox"/>	SDカード抜き差しアラート (Android)	SDカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>	新規アプリインストールアラート (Android)	新しくアプリがインストールされた	アラートに設定する
<input type="checkbox"/>	タイムゾーン変更アラート (Android)	タイムゾーンが変更された	アラートに設定する
<input type="checkbox"/>	新規プロファイルインストールアラート (iOS/macOS)	新しくプロファイルがインストールされた	アラートに設定する

3. [すべての実行履歴を確認する] をクリックします。

このレシピを有効にする 

未稼働アラート (iOS/Android/Windows/macOS)

未稼働期間が指定された期間を超過している

未稼働期間 (日) (1 ~ 90 日)
30

レシピを実行する対象の絞り込み

-  デバイスグループ (1 件)
 - ネットワーク全体 (85 台)

 85台のデバイスが対象になっています。 ※ 対象デバイスが多い場合、レシピの実行に時間がかかる可能性があります。

レシピで実行するアクション

-  アラートに設定する
危険

レシピの実行履歴

[すべての実行履歴を確認する](#)

2018/09/15 13:58:34

2018/09/15 13:53:30

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。

ポイント

次のアクションを設定したレシピの場合、各アクションの画面で配信状況を確認できます。

- 指定プロファイルを配信する／取り除く
- 指定アプリ（VPP アプリ）を配信する／アンインストールする
- 指定プロビジョニングプロファイルを配信する／アンインストールする
- メッセージを配信する
- アンケートを配信する

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、トリガーを [LANSCOPE クライアントがインストールされた] から [任意のタイミングで実行する] 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。

The screenshot shows the 'レシピの追加' (Add Recipe) screen. A search bar at the top right contains the text 'キーワード検索 (例: 営業 iPhone)'. Below the search bar is a table of recipes. The third row, 'アプリカタログ配信', is highlighted with a yellow border. The table has columns for '状態' (Status), 'レシピ名' (Recipe Name), 'トリガー' (Trigger), and 'アクション' (Action).

状態	レシピ名	トリガー	アクション
<input type="checkbox"/>	LANSCOPE Client を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定アプリを配信する
<input type="checkbox"/>	LANSCOPE の登録用 Clip を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定プロフィールを配信する
<input checked="" type="checkbox"/>	アプリカタログ配信	LANSCOPE クライアントがインストールされた	指定プロフィールを配信する
<input checked="" type="checkbox"/>	管理外アラート (iOS/Windows/macOS)	デバイスが管理外になっている	アラートに設定する
<input type="checkbox"/>	パスワードポリシー非準拠アラート (iOS/Android)	パスワードポリシーに準拠していない	アラートに設定する
<input type="checkbox"/>	LANSCOPE Client 未更新アラート (iOS/Android/Windows)	LANSCOPE Client のバージョンが最新になっていない	アラートに設定する
<input checked="" type="checkbox"/>	未稼働アラート (iOS/Android/Windows/macOS)	未稼働期間が指定された期間を超過している	アラートに設定する
<input type="checkbox"/>	空き容量不足アラート (iOS/Android/Windows/macOS)	空き容量が不足している	アラートに設定する
<input type="checkbox"/>	パスワードロックオフアラート (iOS)	パスワードロックの設定がオフになっている	アラートに設定する
<input type="checkbox"/>	リモート実行無効アラート (Android/Windows)	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	アラートに設定する
<input checked="" type="checkbox"/>	SIMカード抜き差しアラート (iOS/Android/Windows)	SIMカードが抜き差しされた	アラートに設定する
<input checked="" type="checkbox"/>	SDカード抜き差しアラート (Android)	SDカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>	新規アプリインストールアラート (Android)	新しくアプリがインストールされた	アラートに設定する
<input type="checkbox"/>	タイムゾーン変更アラート (Android)	タイムゾーンが変更された	アラートに設定する
<input type="checkbox"/>	新規プロフィールインストールアラート (iOS/macOS)	新しくプロフィールがインストールされた	アラートに設定する

3. [編集] をクリックします。



4. [トリガー選択] をクリックします。



5. [任意のタイミングで実行する] をクリックします。



→ 「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。

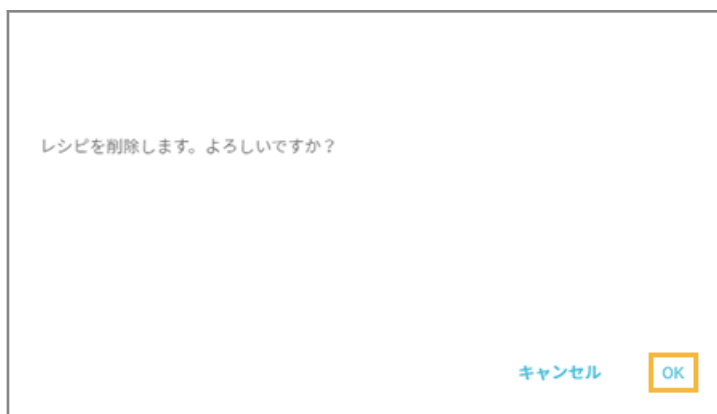
1. [レシピ] の [レシピ一覧] をクリックします。



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。

3-2 アクションを実行する

iOS

Android

Windows

macOS

- [プロフィールを配信する](#)

デバイスに適用するプロフィールを配信できます。

- [アプリを配信する](#)

デバイスにアプリを配信します。

- [プロビジョニングプロフィールを配信する](#)

プロビジョニングプロフィールを配信できます。

- [メッセージ/アンケートを配信する](#)

デバイスにメッセージやアンケートを配信できます。

- [アラートを設定する](#)

アラート設定することで、ルールに抵触したデバイスを発見しやすくなります。デバイス使用者や管理者への通知もできます。

- [操作ログ/位置情報を一括出力する](#)

取得した操作ログ/位置情報を一括出力できます。

プロフィールを配信する

iOS

macOS

デバイスに適用するプロフィールを配信できます。

ポイント

- プロファイルのペイロードの仕様については、Apple 社のヘルプページを確認してください。

<https://support.apple.com/ja-jp/apple-configurator>

- エンドポイントマネージャーは、プロファイルの配信を指示します。デバイスにプロファイルを配信/適用するときの動作は、Apple 社が提供するプログラムやサービスの仕様に依存します。

構成プロファイルとは

iOS/macOS デバイスには、「プロファイル」という設定ファイル（拡張子：.mobileconfig）をインストールできます。あらかじめ設定を組み込んだプロファイルを iOS/macOS デバイスにインストールして、設定を反映できます。

プロファイル配信機能

エンドポイントマネージャーは、複数のデバイスに遠隔操作で、プロファイルの配信（インストール）／取り除き（アンインストール）ができます。

エンドポイントマネージャーを利用しない場合、macOS デバイス上で動作する Apple Configurator を利用して、1 台ずつプロファイルを適用します。

プロファイルの作成方法

プロファイルは、Apple 社が提供する「Apple Configurator」を利用して作成します。

次のプロファイルは、エンドポイントマネージャーの管理コンソールで設定できる／登録済みのため、Apple Configurator は必要ありません。

<p>管理コンソールで設定できるプロファイル (*1)</p>	<ul style="list-style-type: none"> ● パスワードポリシー (*2) (*3) ● 制限 ● Wi-Fi ● VPN ● FileVault ● 証明書 ● Web クリップ
<p>管理コンソールに登録済みのプロファイル (*3)</p>	<ul style="list-style-type: none"> ● カメラの利用を禁止するための設定プロファイル ● スクリーンショットを禁止するための設定プロファイル ● Siri を禁止するための設定プロファイル ● App Store を禁止するための設定プロファイル ● アプリ内の課金を禁止するための設定プロファイル ● iCloud 利用に関して以下項目を禁止するための設定プロファイル <ul style="list-style-type: none"> ● iCloud バックアップ ● iCloud と書類データ ● 管理対象 App が iCloud にデータを保存 ● iCloud での写真共有 ● iTunes Store を禁止するための設定プロファイル ● Safari を禁止するための設定プロファイル

*1 : 「制限」ペイロードなど、作成できるプロファイルは Apple Configurator と異なります。

*2: 「パスコード」ペイロードの「入力を失敗できる回数」で設定した回数よりも1回少ない失敗回数で、デバイスが初期化される場合があります。

*3: パスワードポリシーは、[ルール] > [デバイス設定] > [基本設定] で設定できます。詳細は、[取得する情報を設定する](#)を参照してください。

プロフィール配信の流れ

iOS

macOS

エンドポイントマネージャーで作成したプロフィールを利用する場合と、Apple Configuratorで作成したプロフィールを利用する場合で、プロフィール配信の流れが異なります。

ここでは、iOS デバイスにプロフィールを配信する場合を例に説明します。

ポイント

- レシピを作成すると、プロフィール配信/配信したプロフィールの取り除きができます。レシピで設定したトリガーのタイミングで、配信/取り除きが実行されます。デバイスにパスコードが設定されている場合、画面ロック解除後にプロフィールが配信されます。
- 配信したプロフィールは、デバイスから取り除くことはできません。プロフィールの配信と同様に、レシピを利用して取り除きます。エンドポイントマネージャーの配信以外でインストールしたプロフィールは、エンドポイントマネージャーからは取り除くことはできません。

■ エンドポイントマネージャーでプロフィールを作成する場合

エンドポイントマネージャーの管理コンソールで、Apple 社が提供する一部のペイロード(制限/Wi-Fi/VPN/FileVault/証明書/Web クリップ) プロフィールを作成し、配信設定ができます。

ステップ:

1. [プロフィールを作成する](#)
2. [登録済みのプロフィールを確認する](#)
3. [プロフィールを配信する/取り除く](#)

ステップ 1: プロフィールを作成する

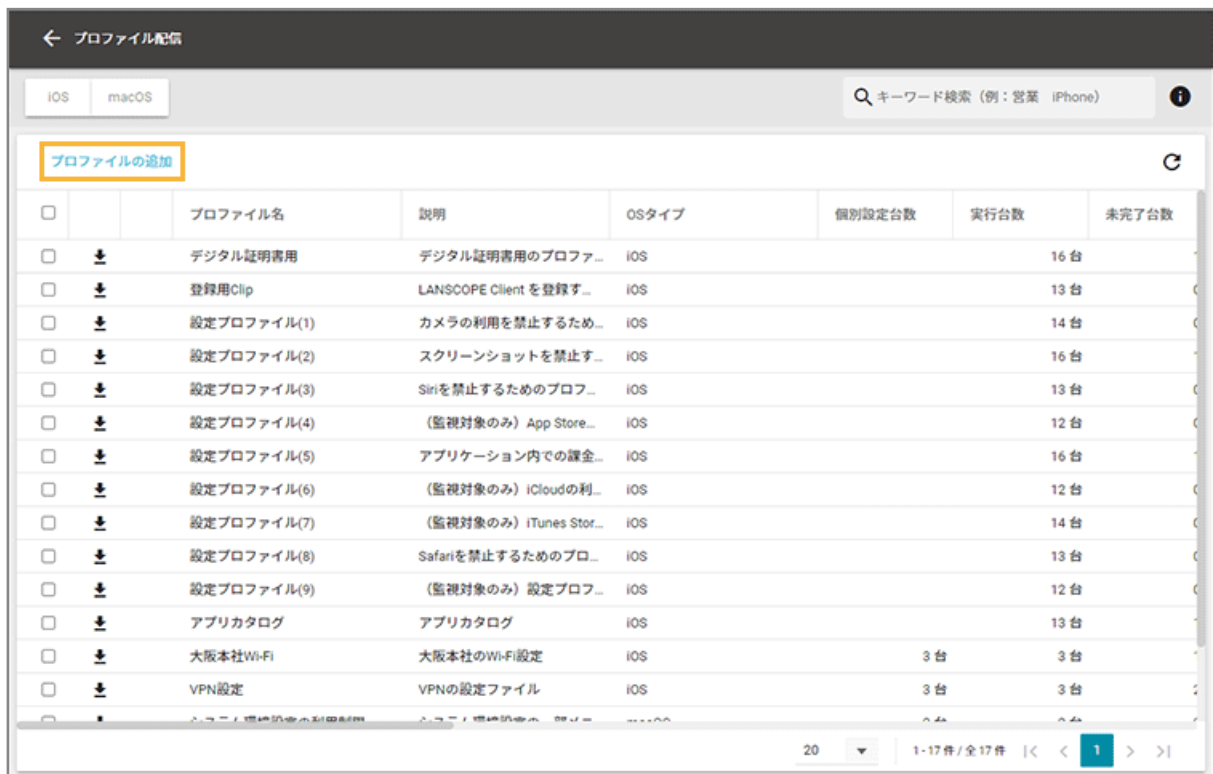
1. [レシピ] の [アクション] をクリックします。



2. [プロフィールを設定する] をクリックします。



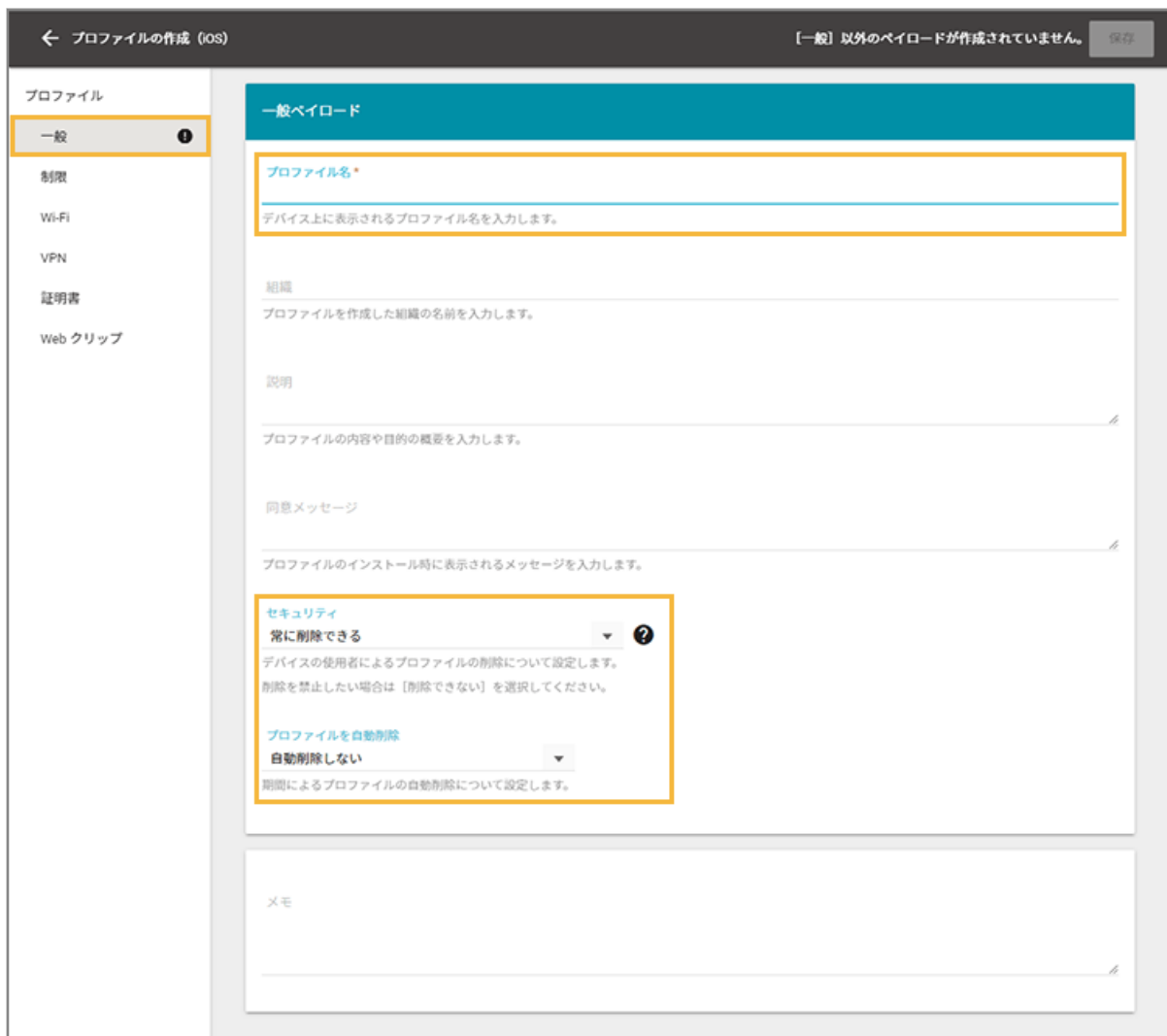
3. [プロフィールの追加] をクリックします。



4. [iOSのプロファイルを作成する] をクリックします。



5. [一般] をクリックし、プロフィール名などを設定します。



プロフィール名

プロフィールの表示名を設定します。ここで設定した名前はデバイス上に表示されます。

セキュリティ

デバイス側からプロファイルを削除するタイミングについて、「常に削除できる」「認証すれば削除できる」「削除できない」から選択します。

「常に削除できる」「認証すれば削除できる」を選択しても、エンドポイントマネージャーから配信したプロファイルは、デバイスからは削除できません。削除する場合、エンドポイントマネージャーからプロファイルを取り除きます。

プロファイルを自動削除

自動でプロファイルを削除するタイミングについて、「自動削除しない」「指定した日に自動削除する」「一定期間後、自動削除する」から選択します。

6. 必要に応じて、各ペイロードを設定します。

The screenshot shows the 'Profile Creation (iOS)' interface. On the left, a sidebar lists various settings: '一般' (General), '制限' (Restrictions), 'Wi-Fi', 'VPN', '証明書' (Certificates), and 'Web クリップ' (Web Clips). The '制限' (Restrictions) option is highlighted with a yellow border. The main area is titled '一般ペイロード' (General Payload) and contains several input fields: 'プロファイル名' (Profile Name), '組織' (Organization), '説明' (Description), and '同意メッセージ' (Consent Message). Below these is a 'セキュリティ' (Security) dropdown menu currently set to '常に削除できる' (Always deletable). A '保存' (Save) button is visible in the top right corner.

7. [保存] をクリックします。

→ プロファイルが作成されます。

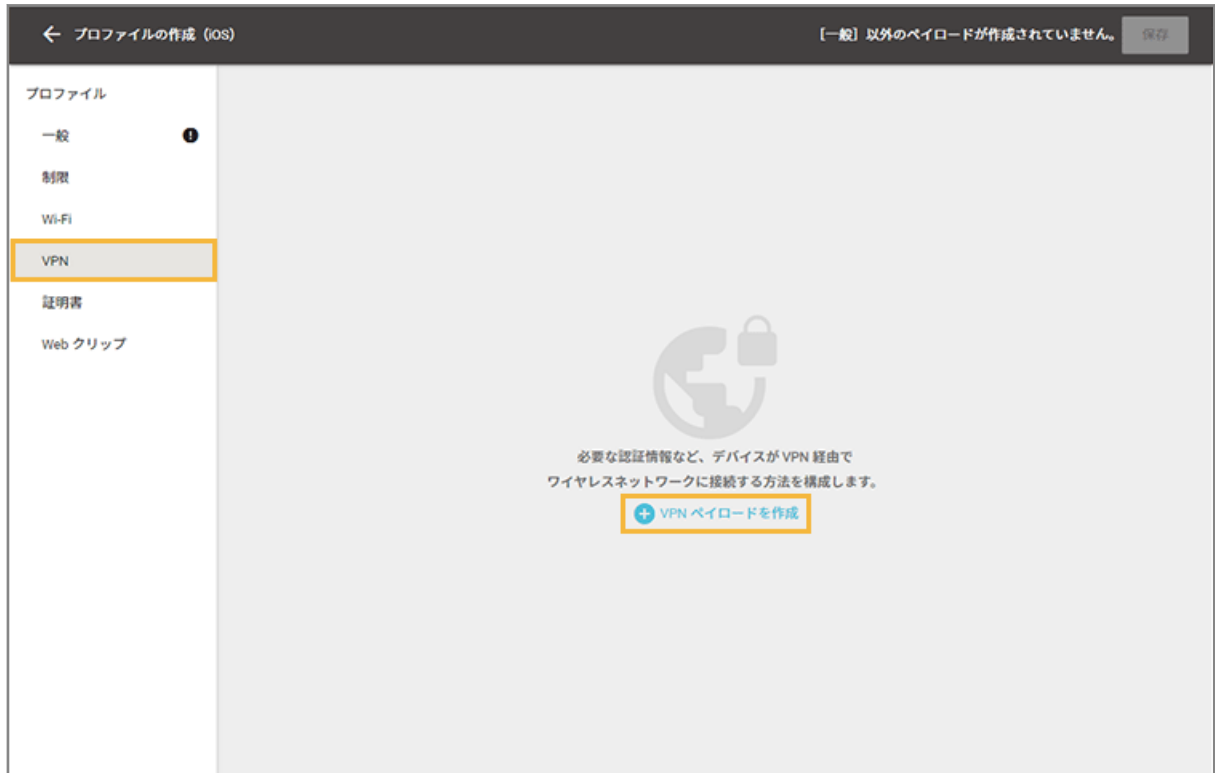
Wi-Fi/VPN の個別設定を利用する場合

Wi-Fi/VPN 接続用のユーザー名/パスワードがデバイスごとに異なる場合、アカウント/パスワードを含む CSV ファイルをインポートすることで、1つのプロファイル作成で配信できます。

ポイント

個別設定を利用する場合、作成できるペイロードは1つです。

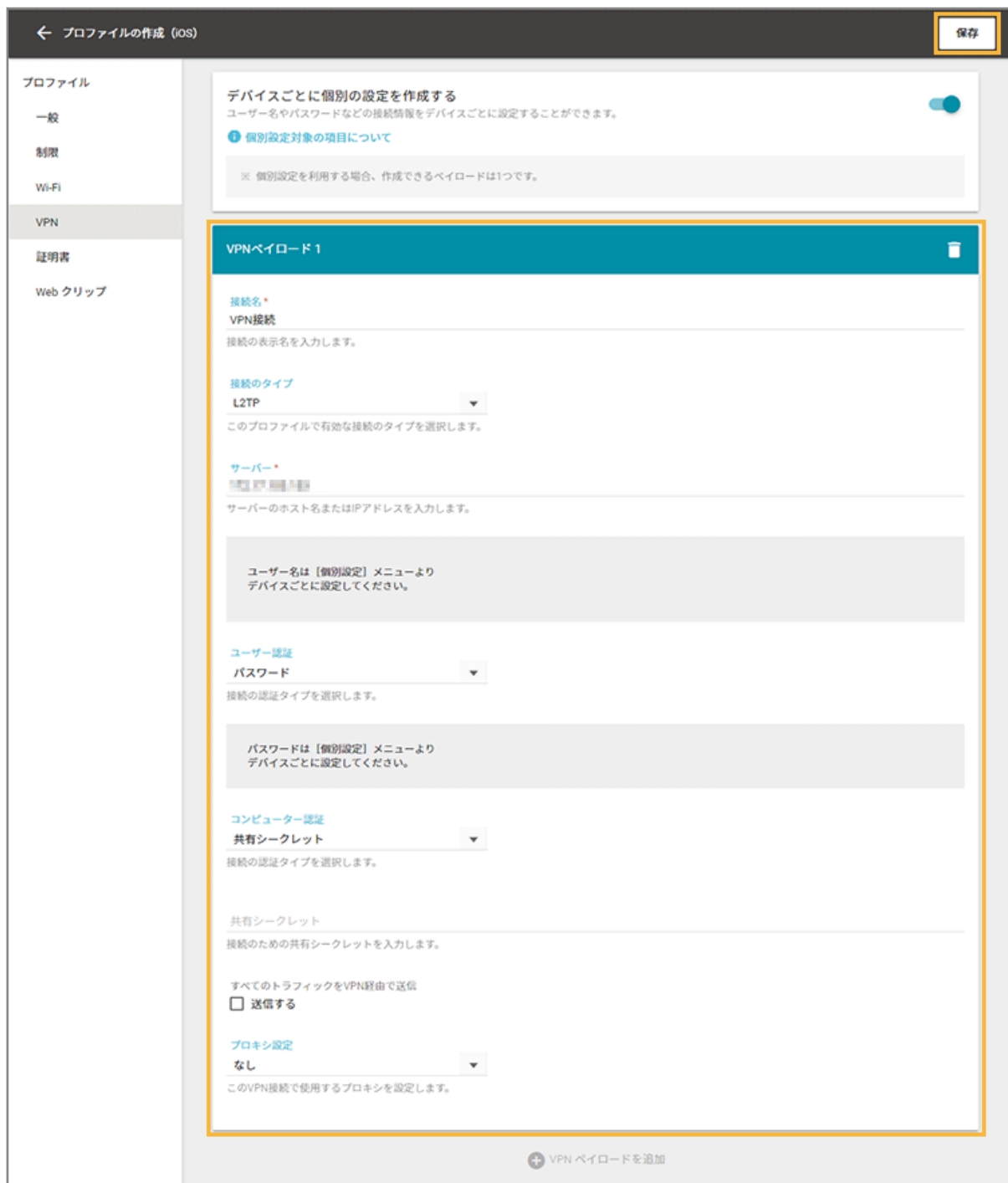
1. [VPN] をクリックし、[VPN ペイロードを作成] をクリックします。



2. 「デバイスごとに個別の設定を作成する」を に切り替えます。

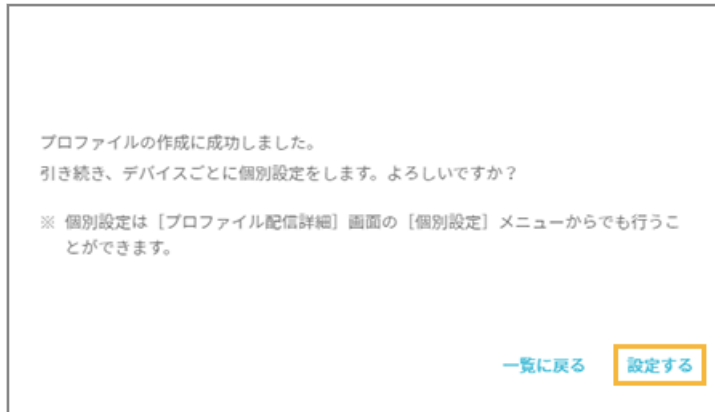


3. 必要な項目を入力し、[保存] をクリックします。

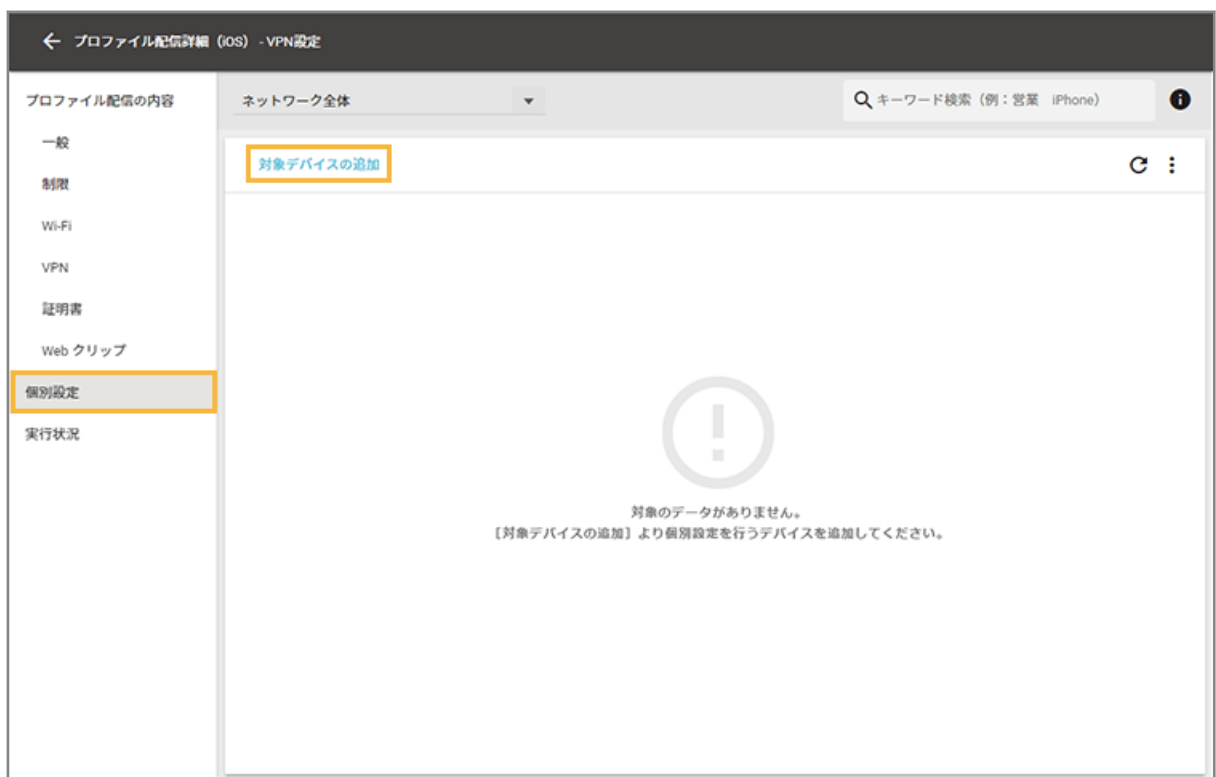


4. [設定する] をクリックします。

[一覧に戻る] をクリックしても、[レシピ] > [アクション] の「プロフィールを設定する」画面で作成したプロフィールをクリックすれば、次の手順に進めます。



5. [対象デバイスの追加] をクリックします。



6. デバイスをチェックし、「選択」をクリックします。

ポイント

「個別設定デバイスを選択」画面では、次のデバイスが表示されます。

- MDM 構成プロファイルをインストール済みのデバイス ([リスト] の [デバイス] 画面に表示されるデバイス)
- カスタムインストールで情報を登録したデバイス ([リスト] の [デバイス] 画面で [インストール待ちデバイス] に表示されるデバイス)
- DEP を利用する場合で、Apple Business Manager サイトと同期し、[DEP 設定] の「DEP デバイス」画面に表示されるデバイス

個別設定対象のデバイスを選択

ネットワーク全体 Q キーワード検索 (例: 営業 iPhone) ⓘ

× 3件を選択中 選択

<input type="checkbox"/>	↑ 管理...	デバイスグループ	デバイス管理名	ユーザー名	OSタイプ
<input type="checkbox"/>	3	営業1課	iPhone_00000028	飯田 育三	iOS
<input type="checkbox"/>	9	総務課	iPhone_00000026	森 太郎	iOS
<input type="checkbox"/>	10	営業1課	iPhone_00000029	別所 哲郎	iOS
<input checked="" type="checkbox"/>	16	営業部	iPhone_00000030	佐藤 新	iOS
<input type="checkbox"/>	17	営業1課	iPhone_00000031	鈴木 一	iOS
<input type="checkbox"/>	18	営業2課	iPhone_00000032	佐竹 信弘	iOS
<input checked="" type="checkbox"/>	19	営業2課	iPhone_00000033	石川 忍	iOS
<input type="checkbox"/>	21	営業1課	iPad_00000034	小林 哲司	iOS
<input type="checkbox"/>	27	営業2課	iPhone_00000027	富山 哲夫	iOS
<input type="checkbox"/>	32	システム1課	iPad_00000035	細川 孝信	iOS
<input type="checkbox"/>	33	システム1課	iPad_00000042	横口 揚羽	iOS
<input type="checkbox"/>	34	システム1課	iPad_00000036	北井 清二	iOS
<input type="checkbox"/>	35	システム部	iPad_00000043	上野 卓	iOS

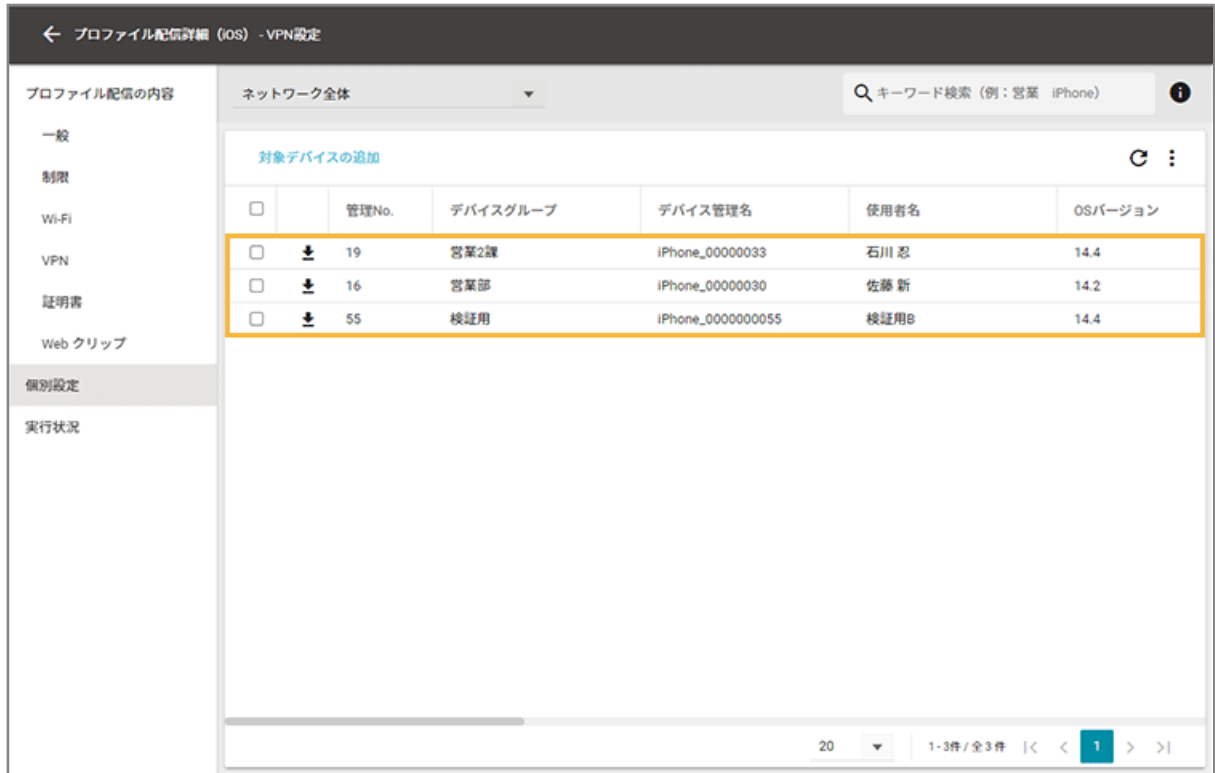
1000 1・20件 / 全20件 |< < 1 > >|

キャンセル

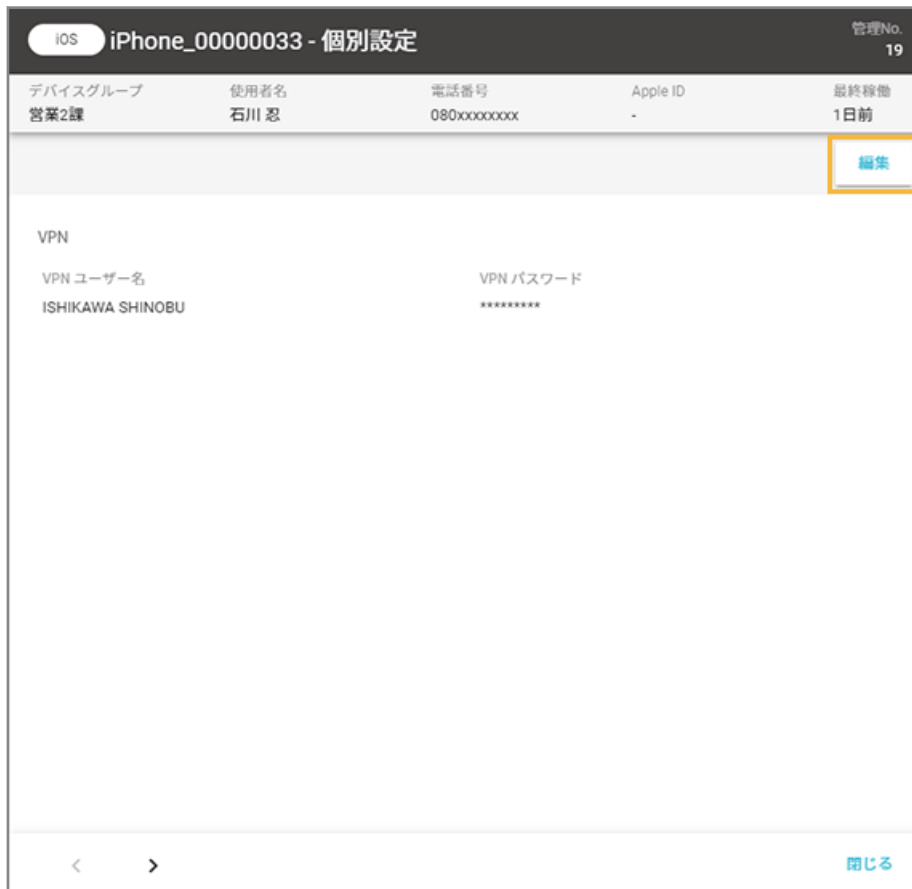
7. デバイスをクリックします。

ポイント

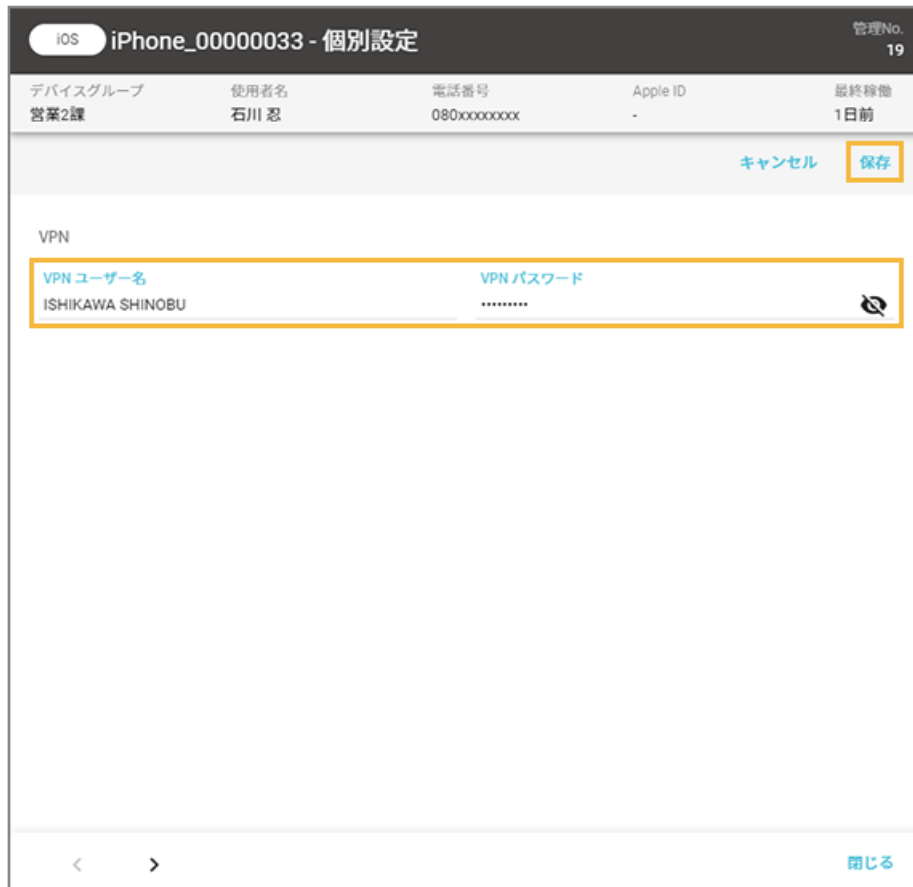
対象デバイスを選択し、エクスポート／インポートすることで、一括設定もできます。



8. [編集] をクリックします。



9. 内容を編集し、[保存] をクリックします。



→ 個別設定が完了します。

ステップ 2： 登録済みのプロファイルを確認する

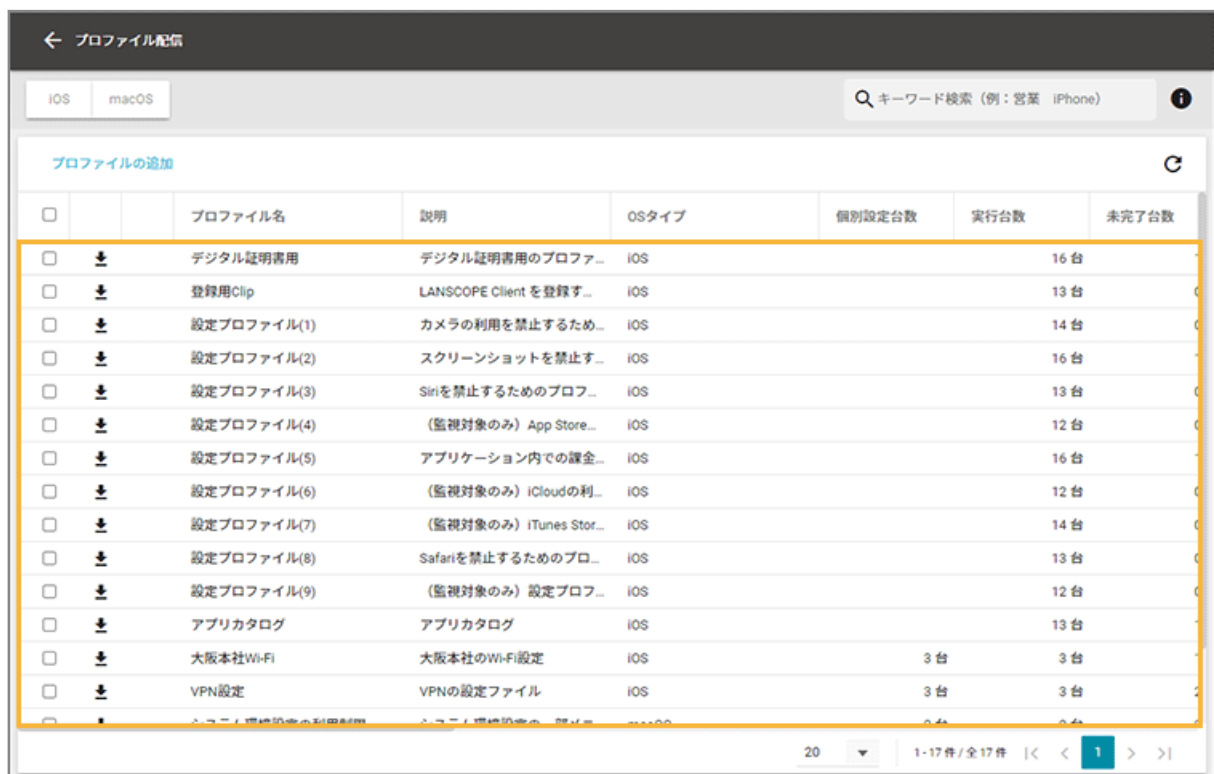
1. [レシピ] の [アクション] をクリックします。



2. [プロファイルを設定する] をクリックします。



3. プロファイルをクリックします。



4. [プロフィール配信の内容] で、設定内容を確認します。



ステップ 3： プロファイルを配信する／取り除く

ここでは、デバイスに LANSCOPE クライアントがインストールされたら、指定したプロファイルを自動配信する場合を例に説明します。

すでに LANSCOPE クライアントがインストールされている場合は、任意のトリガーを選択してください。

注意

Wi-Fi/VPN の個別設定を含む構成プロファイルを配信する場合、「ネットワーク全体」をレシピの実行対象に選択しても、個別設定を含むデバイスにだけ配信されます。

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。

状態	レシピ名	トリガー	アクション
<input type="checkbox"/>	LANSCOPE Client を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定アプリを配信する
<input type="checkbox"/>	LANSCOPE の登録用 Clip を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定プロフィールを配信する
<input checked="" type="checkbox"/>	管理外アラート (iOS/Windows/macOS)	デバイスが管理外になっている	アラートに設定する
<input type="checkbox"/>	パスワードポリシー非準拠アラート (iOS/Android)	パスワードポリシーに準拠していない	アラートに設定する
<input type="checkbox"/>	LANSCOPE Client 未更新アラート (iOS/Android/Windows)	LANSCOPE Client のバージョンが最新になっていない	アラートに設定する
<input checked="" type="checkbox"/>	未稼働アラート (iOS/Android/Windows/macOS)	未稼働期間が指定された期間を超過している	アラートに設定する
<input type="checkbox"/>	空き容量不足アラート (iOS/Android/Windows/macOS)	空き容量が不足している	アラートに設定する
<input type="checkbox"/>	パスコードロックオフアラート (iOS)	パスコードロックの設定がオフになっている	アラートに設定する
<input type="checkbox"/>	リモート実行無効アラート (Android/Windows)	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	アラートに設定する
<input checked="" type="checkbox"/>	SIMカード抜き差しアラート (iOS/Android/Windows)	SIMカードが抜き差しされた	アラートに設定する
<input checked="" type="checkbox"/>	SDカード抜き差しアラート (Android)	SDカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>	新規アプリインストールアラート (Android)	新しくアプリがインストールされた	アラートに設定する
<input type="checkbox"/>	タイムゾーン変更アラート (Android)	タイムゾーンが変更された	アラートに設定する
<input type="checkbox"/>	新規プロフィールインストールアラート (iOS/macOS)	新しくプロフィールがインストールされた	アラートに設定する

3. 次のように設定し、[アクション追加] をクリックします。

項目	値
レシピ名	任意のレシピ名
トリガー	[LANSCOPE クライアントがインストールされた]
デバイスグループ	配信するデバイスグループまたはデバイス
デバイス	

新しいレシピを作成

レシピ名*

制限プロファイルの配信 (営業部用)

レシピのトリガーを選択 トリガー選択

トリガー*

LANSCOPE クライアントがインストールされた

レシピを実行する対象の絞り込み

 デバイスグループ (0 件)
選択

 デバイス (0 台)
選択

実行するアクション アクション追加

4. [指定プロファイルを配信する] をクリックします。

配信したプロファイルを取り除く場合、[指定プロファイルを取り除く] をクリックします。

アクションを選択してください

iOS
Android
Windows
macOS

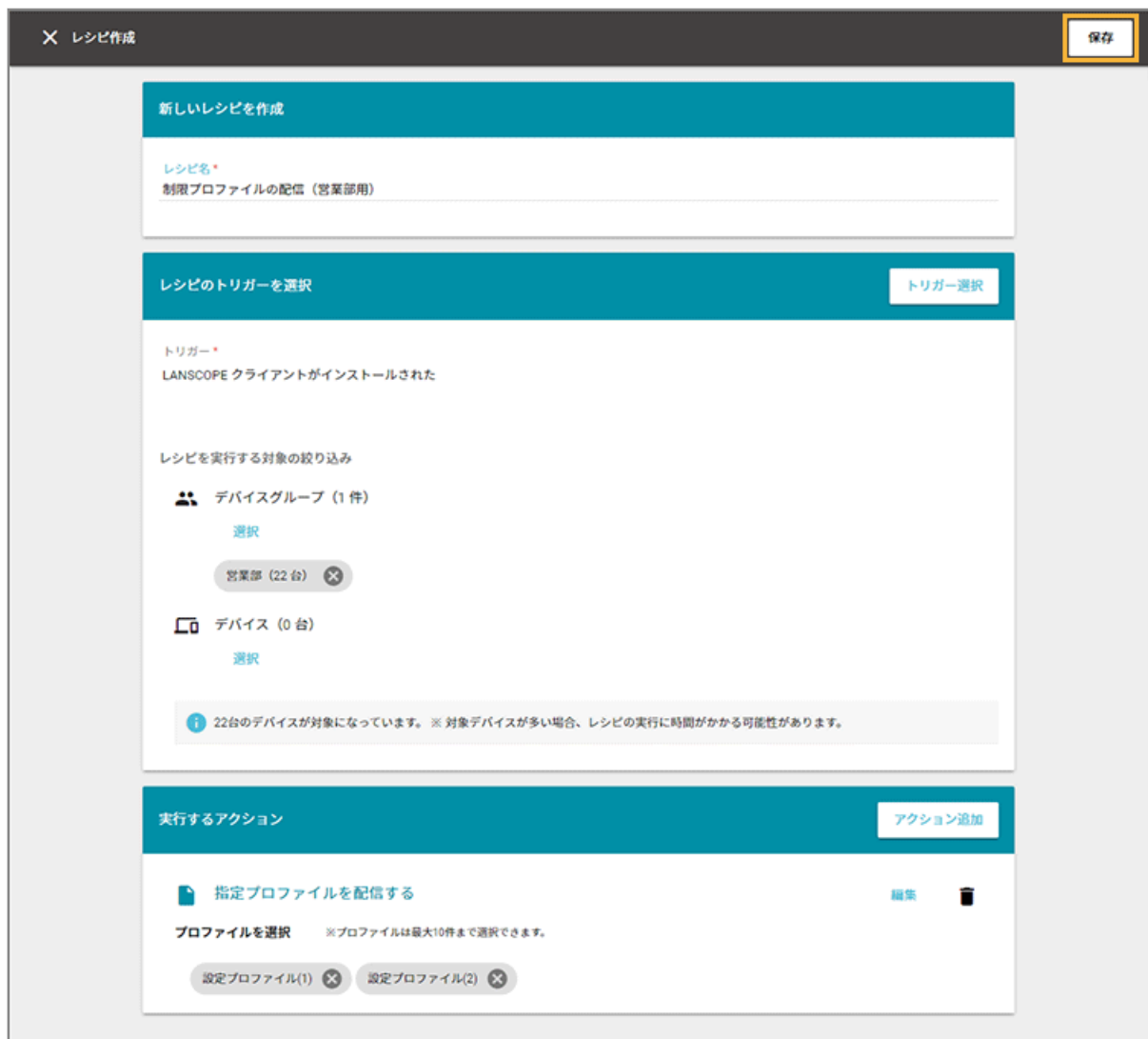
 管理者にメールでお知らせする	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 指定プロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
 指定アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 指定プロビジョニングプロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 指定 VPP アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 メッセージを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
 アンケートを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
 アラートに設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 アラートレポートを送信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 指定プロファイルを取り除く	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

5. プロファイルをチェックし、[選択] をクリックします。

プロファイルは、最大 10 件選択できます。



6. 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。

■ Apple Configurator でプロファイルを作成する場合

Apple 社が提供するすべてのペイロードプロファイルを作成できます。

ステップ：

1. [プロファイルを作成する](#)
2. [プロファイルをエンドポイントマネージャーに登録する](#)
3. [登録済みのプロファイルを確認する](#)
4. [プロファイルを配信する／取り除く](#)

ステップ 1： プロファイルを作成する

Apple Configurator でプロファイルを作成します。

ポイント

- Apple Configurator は、App Store で無料ダウンロードできます。
- プロファイル作成の詳細については、Apple Configurator のヘルプページを参照してください。

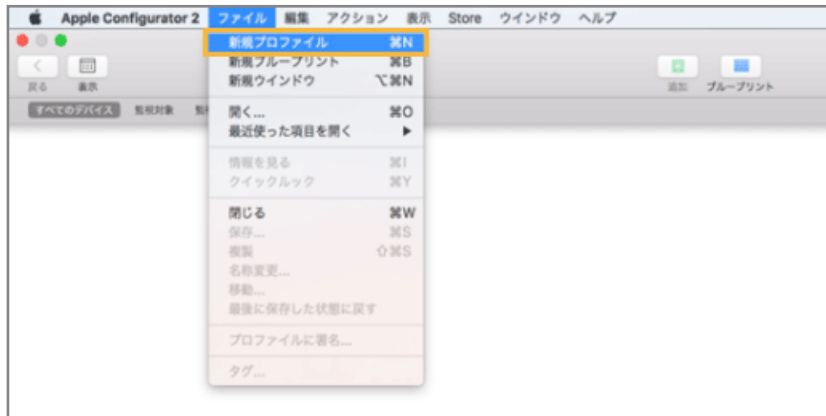
<https://support.apple.com/ja-jp/apple-configurator>

1. Apple Configurator を起動します。

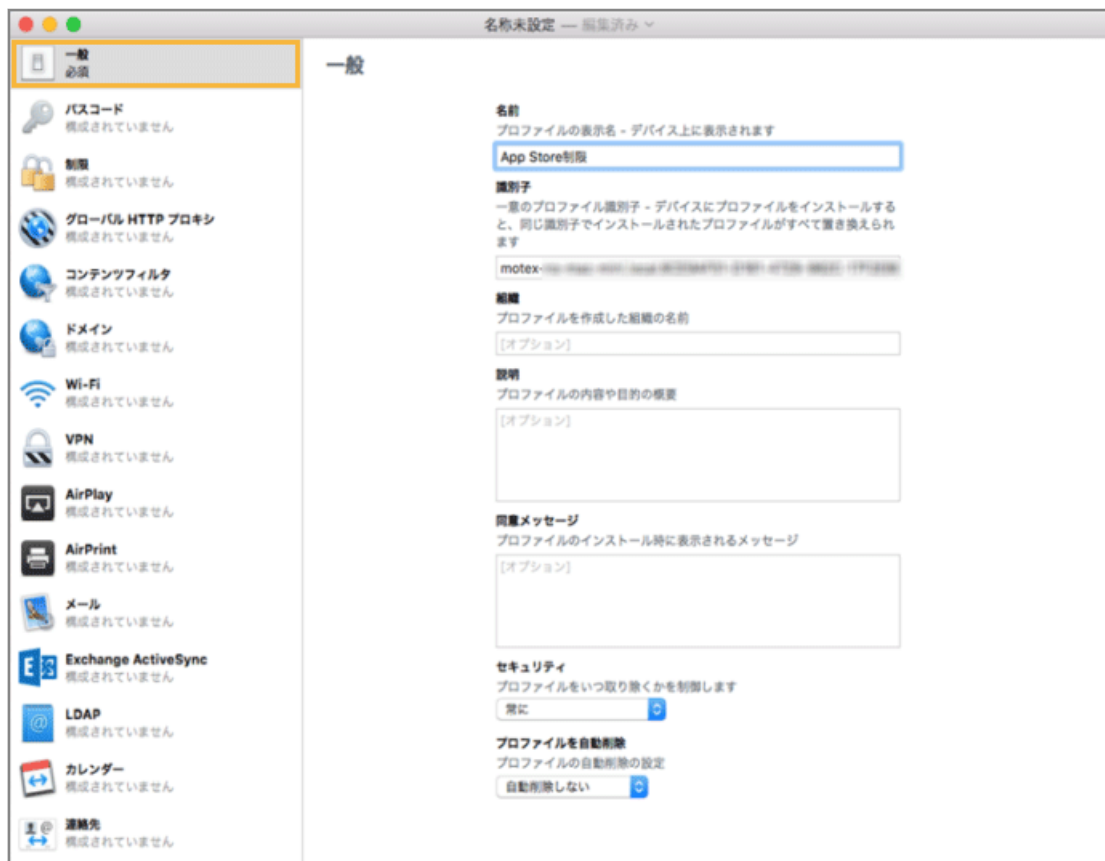


→ 「使用許諾契約」画面が表示された場合は、「同意する」をクリックします。

2. [ファイル] > [新規プロファイル] をクリックします。



3. [一般] をクリックし、プロファイル名などを設定します。



名前

プロファイルの表示名を設定します。ここで設定した名前はデバイス上に表示されます。

セキュリティ

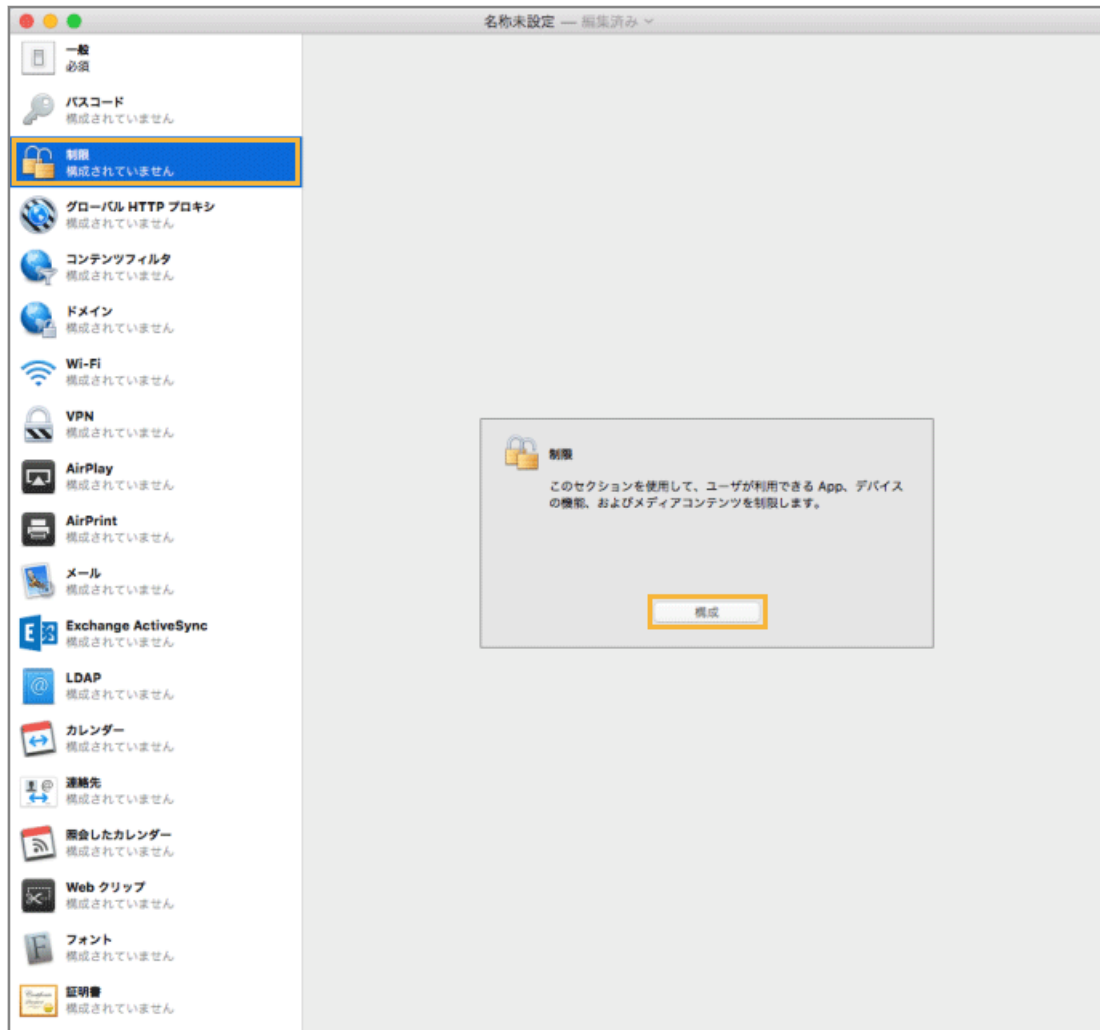
デバイス側からプロファイルを削除するタイミングについて、「常に」「認証時」「取り除かない」から選択します。

「常に」「認証時」を選択しても、エンドポイントマネージャーから配信した構成プロファイルは、デバイスからは削除できません。削除する場合、エンドポイントマネージャーからプロファイルを取り除きます。

プロファイルを自動削除

自動でプロファイルを削除するタイミングについて、「自動削除しない」「指定日」「一定期間後」から選択します。

4. 設定するペイロードをクリックし、[構成] をクリックします。



注意

ペイロードの設定名の横に「(監視対象のみ)」と記載されている場合、監視対象 (監視モード) のデバイスにだけ適用できるプロファイルを指します。監視対象ではないデバイスに配信した場合、配信に失敗します。

5. [ファイル] > [保存] を選択し、プロファイルを保存します。

プロファイルに署名する場合、[ファイル] > [プロファイルに署名] を選択し、ポップアップメニューから証明書を選択して、[OK] をクリックします。

ステップ 2： プロファイルをエンドポイントマネージャーに登録する

Apple Configurator で作成したプロファイルを終端ポイントマネージャーに登録します。

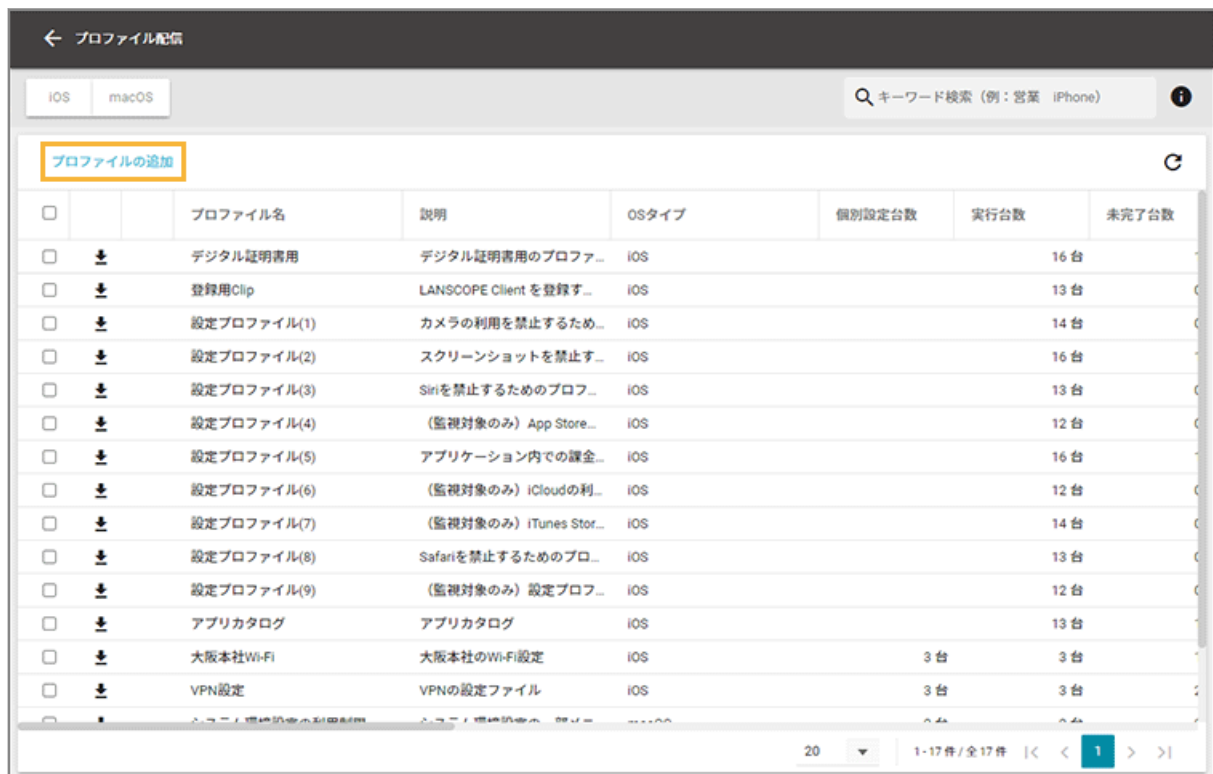
1. [レシピ] の [アクション] をクリックします。



2. [プロフィールを設定する] をクリックします。



3. [プロフィールの追加] をクリックします。



4. [iOSのプロファイルをアップロードする] をクリックします。



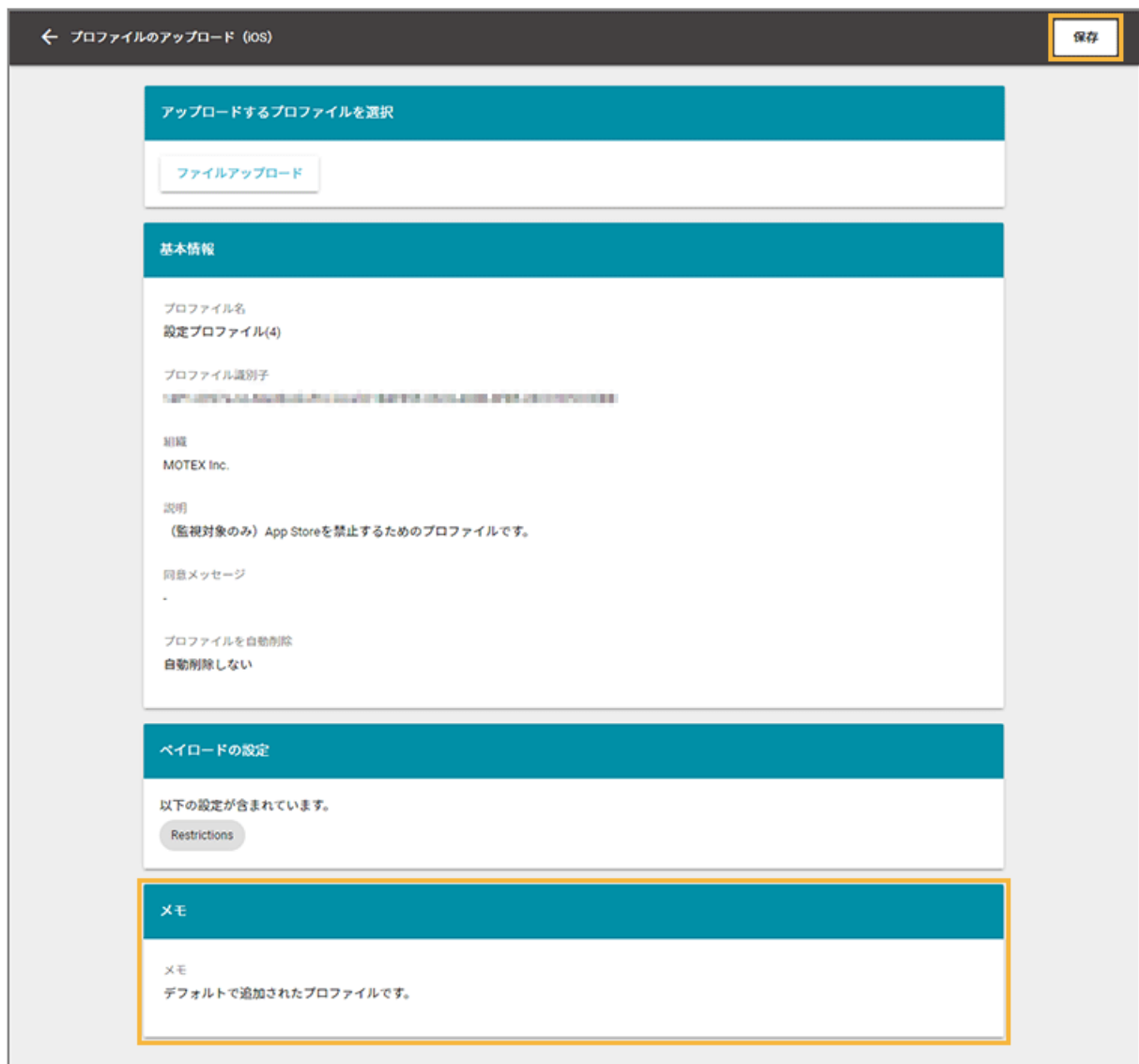
5. **【ファイルアップロード】をクリックし、作成したプロフィールを選択します。**

プロフィールの拡張子は「.mobileconfig」です。



→ 読み込みが完了すると、プロフィール情報が管理コンソールに表示されます。

6. **必要に応じてメモを入力し、【保存】をクリックします。**



注意

暗号化されたプロファイルの場合、「このプロファイルは暗号化されているため、設定内容を表示できません。」と表示され、「ペイロードの設定」の内容を読み込めません。

→ 「プロフィール追加」画面に、登録したプロファイルが追加されます。

ステップ 3： 登録済みのプロファイルを確認する

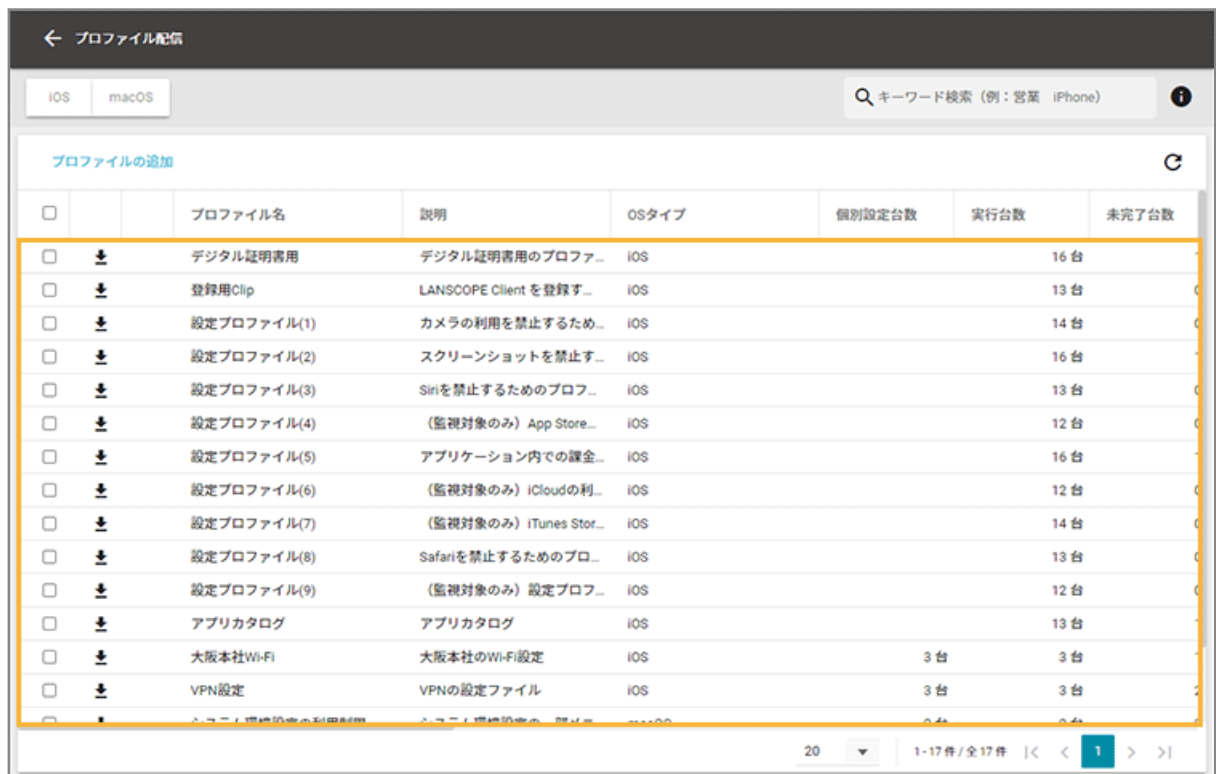
1. [レシピ] の [アクション] をクリックします。



2. [プロフィールを設定する] をクリックします。



3. プロファイルをクリックします。



4. [プロフィール配信の内容] で、設定内容を確認します。



ステップ4： プロファイルを配信する／取り除く

ここでは、デバイスにLANSCOPEクライアントがインストールされたら、指定したプロファイルを自動配信する場合を例に説明します。

すでにLANSCOPEクライアントがインストールされている場合は、任意のトリガーを選択してください。

注意

Wi-Fi/VPNの個別設定を含む構成プロファイルを配信する場合、「ネットワーク全体」をレシピの実行対象に選択しても、個別設定を含むデバイスにだけ配信されます。

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。

状態	レシピ名	トリガー	アクション
<input type="checkbox"/>	LANSCOPE Client を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定アプリを配信する
<input type="checkbox"/>	LANSCOPE の登録用 Clip を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定プロフィールを配信する
<input checked="" type="checkbox"/>	管理外アラート (iOS/Windows/macOS)	デバイスが管理外になっている	アラートに設定する
<input type="checkbox"/>	パスワードポリシー非準拠アラート (iOS/Android)	パスワードポリシーに準拠していない	アラートに設定する
<input type="checkbox"/>	LANSCOPE Client 未更新アラート (iOS/Android/Windows)	LANSCOPE Client のバージョンが最新になっていない	アラートに設定する
<input checked="" type="checkbox"/>	未稼働アラート (iOS/Android/Windows/macOS)	未稼働期間が指定された期間を超過している	アラートに設定する
<input type="checkbox"/>	空き容量不足アラート (iOS/Android/Windows/macOS)	空き容量が不足している	アラートに設定する
<input type="checkbox"/>	パスコードロックオフアラート (iOS)	パスコードロックの設定がオフになっている	アラートに設定する
<input type="checkbox"/>	リモート実行無効アラート (Android/Windows)	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	アラートに設定する
<input checked="" type="checkbox"/>	SIMカード抜き差しアラート (iOS/Android/Windows)	SIMカードが抜き差しされた	アラートに設定する
<input checked="" type="checkbox"/>	SDカード抜き差しアラート (Android)	SDカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>	新規アプリインストールアラート (Android)	新しくアプリがインストールされた	アラートに設定する
<input type="checkbox"/>	タイムゾーン変更アラート (Android)	タイムゾーンが変更された	アラートに設定する
<input type="checkbox"/>	新規プロフィールインストールアラート (iOS/macOS)	新しくプロフィールがインストールされた	アラートに設定する

3. 次のように設定し、[アクション追加] をクリックします。

項目	値
レシピ名	任意のレシピ名
トリガー	[LANSCOPE クライアントがインストールされた]
デバイスグループ	配信するデバイスグループまたはデバイス
デバイス	

新しいレシピを作成

レシピ名*

制限プロファイルの配信 (営業部用)

レシピのトリガーを選択 トリガー選択

トリガー*

LANSCOPE クライアントがインストールされた

レシピを実行する対象の絞り込み

 デバイスグループ (0 件)
選択

 デバイス (0 台)
選択

実行するアクション アクション追加

4. [指定プロファイルを配信する] をクリックします。

配信したプロファイルを取り除く場合、[指定プロファイルを取り除く] をクリックします。

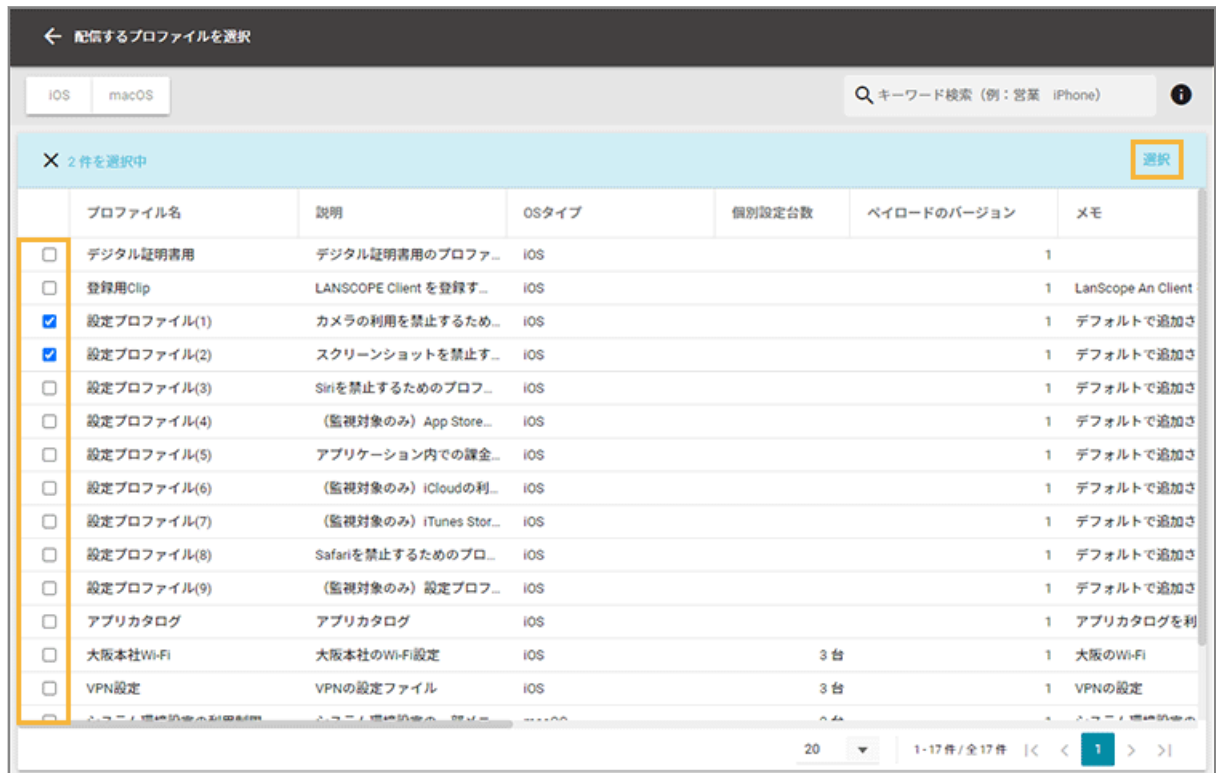
アクションを選択してください

iOS
Android
Windows
macOS

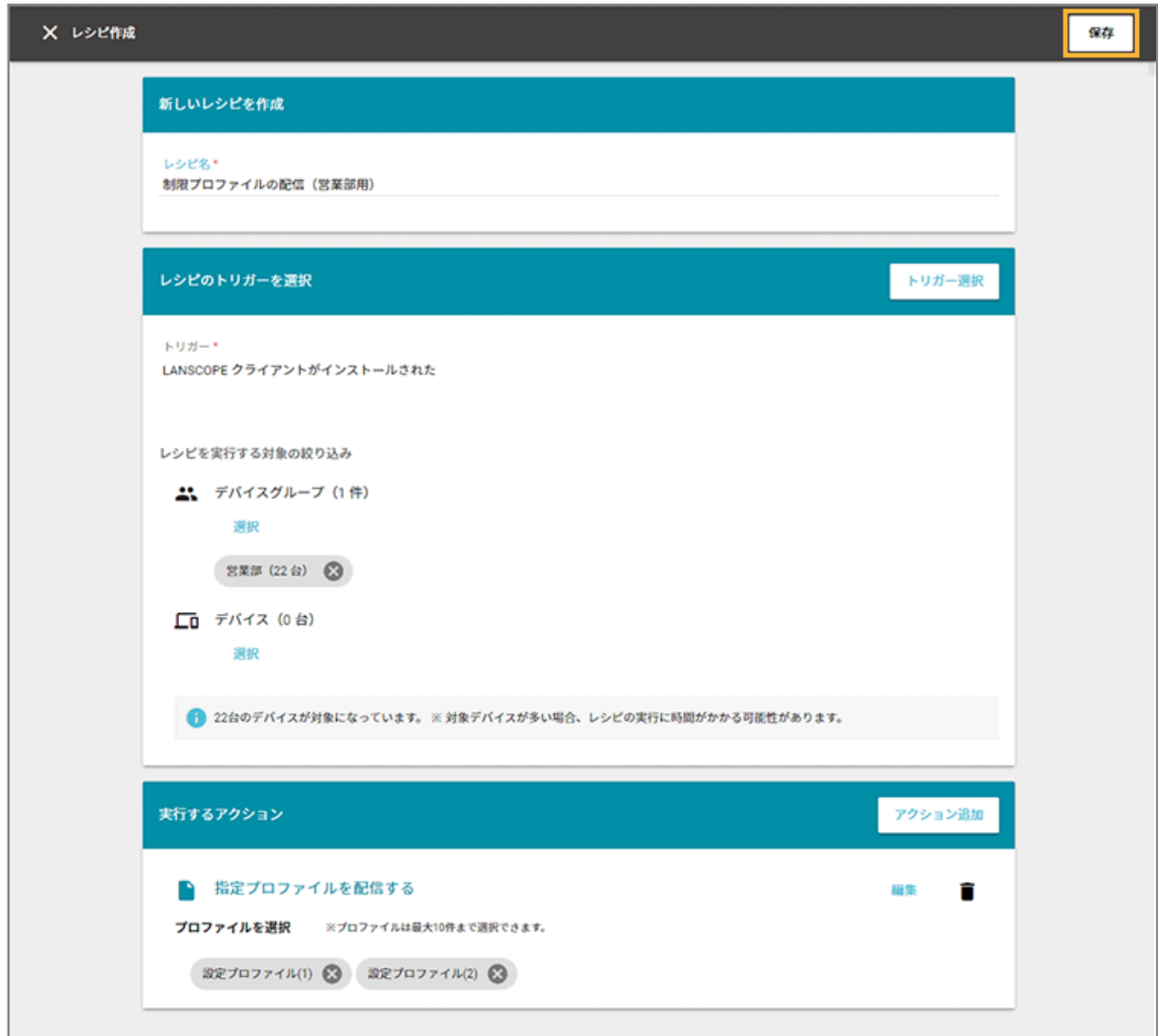
 管理者にメールでお知らせする	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 指定プロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
 指定アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 指定プロビジョニングプロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 指定 VPP アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 メッセージを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
 アンケートを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
 アラートに設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 アラートレポートを送信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 指定プロファイルを取り除く	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

5. プロファイルをチェックし、[選択] をクリックします。

プロファイルは、最大 10 件選択できます。



6. 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。

プロファイルの配信結果を確認する

iOS

macOS

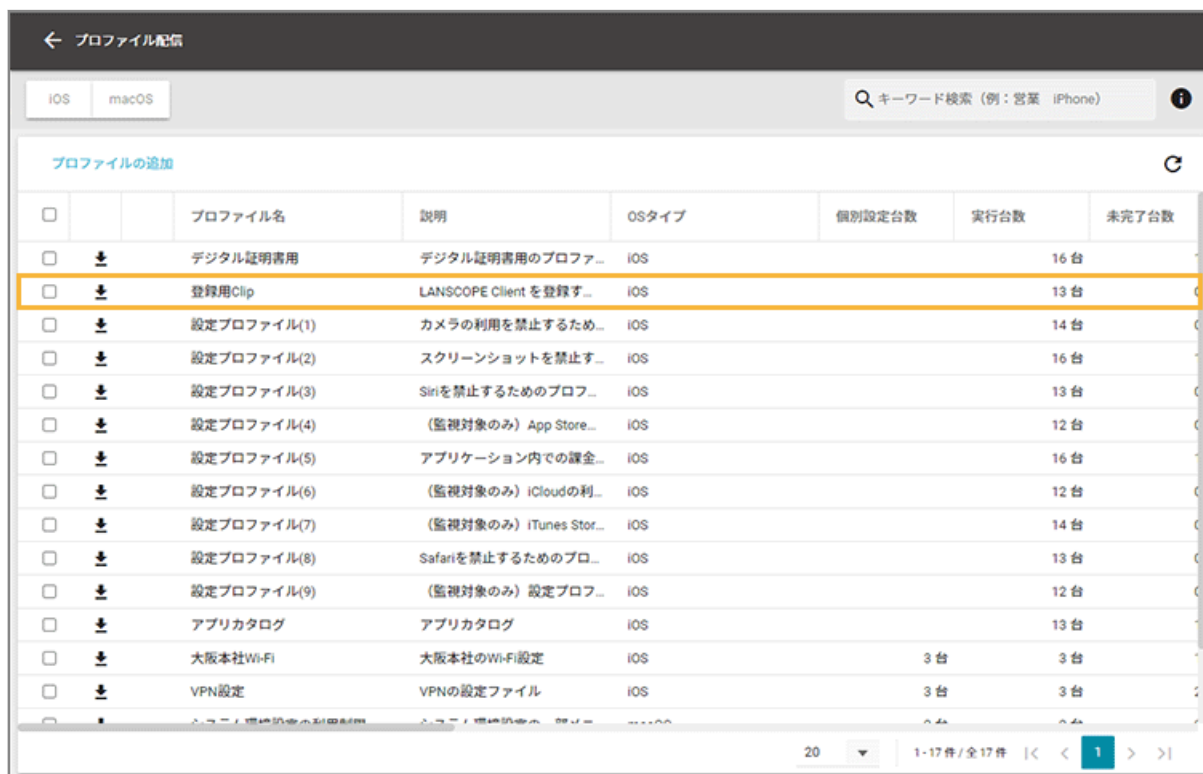
1. [レシピ] の [アクション] をクリックします。



2. [プロフィールを設定する] をクリックします。



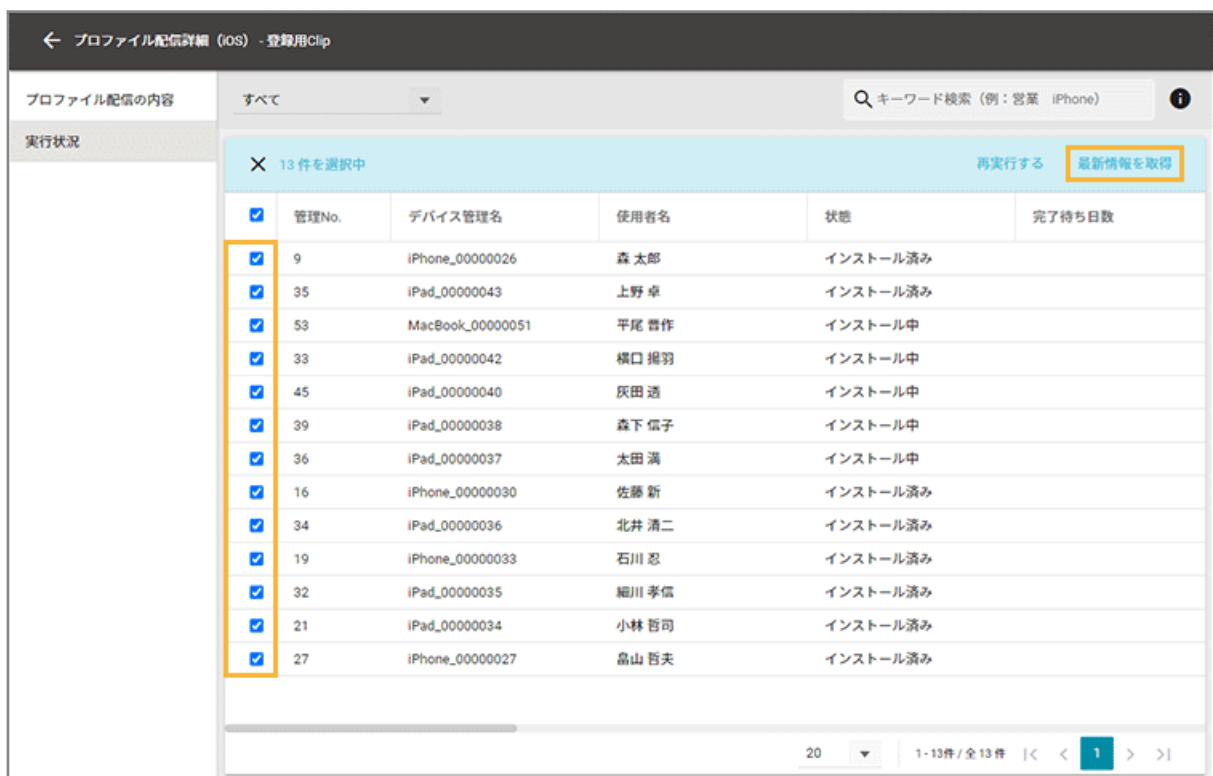
3. プロファイルをクリックします。



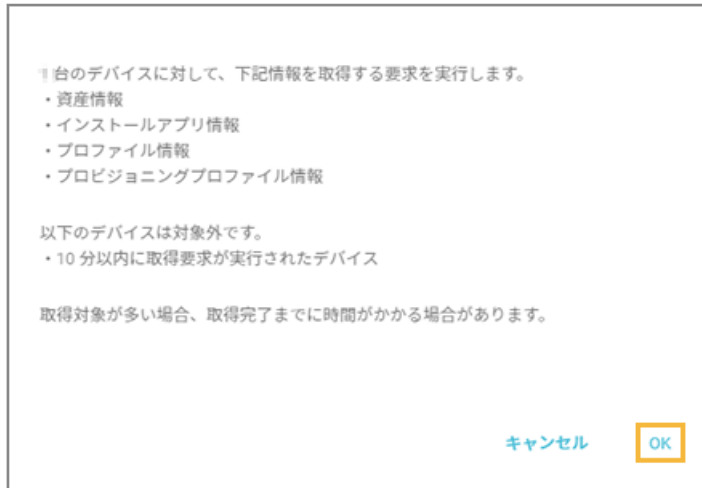
4. [実行状況] をクリックします。



5. デバイスをチェックし、[最新情報を取得] をクリックします。



6. [OK] をクリックします。



7. 各デバイスの配信状態を確認します。

管理No.	デバイス管理名	使用者名	状態	完了待ち日数
9	iPhone_00000026	森 太郎	インストール済み	
35	iPad_00000043	上野 卓	インストール済み	
53	MacBook_00000051	平尾 晋作	インストール中	5日
33	iPad_00000042	横口 翔羽	インストール済み	
45	iPad_00000040	灰田 透	インストール済み	
39	iPad_00000038	森下 信子	インストール済み	
36	iPad_00000037	太田 満	インストール済み	
16	iPhone_00000030	佐藤 新	インストール済み	
34	iPad_00000036	北井 清二	インストール済み	
19	iPhone_00000033	石川 忍	インストール済み	
32	iPad_00000035	細川 孝信	インストール済み	
21	iPad_00000034	小林 哲司	インストール済み	
27	iPhone_00000027	島山 哲夫	インストール済み	

管理 No.

配信されたデバイスの管理 No.が表示されます。

デバイス管理名

配信されたデバイスのデバイス管理名が表示されます。

使用者名

配信されたデバイスの使用者名が表示されます。

状態

- インストール済み

「指定プロファイルを配信する」を実行後、デバイスへインストール済みの状態のときに表示されます。

- インストール中

「指定プロファイルを配信する」を実行後、まだデバイスにインストールされていない状態のときに表示されます。

再配信する場合、デバイスをチェックし、[再実行する]をクリックします。



- アンインストール中

「指定プロファイルを取り除く」を実行後、まだデバイスにインストールされている状態のときに表示されます。

- アンインストール済み

「指定プロファイルを取り除く」を実行後、デバイスからアンインストール済みの状態のときに表示されます。

完了待ち日数

「状態」が「インストール中」「アンインストール中」の場合、「最新配信日時」からの経過日数が表示されます。「状態」が「インストール済み」「アンインストール済み」の場合、空欄です。

実行方法

- レシピ

レシピによるプロファイル配信/取り除きの場合

- 直接実行

[リスト] > [デバイス] でデバイスを選択し、アクション実行した場合

レシピ名

「実行方法」が「レシピ」の場合、レシピ名が表示されます。「実行方法」が「直接実行」の場合、空欄です。

登録したプロファイルを削除する

iOS

macOS

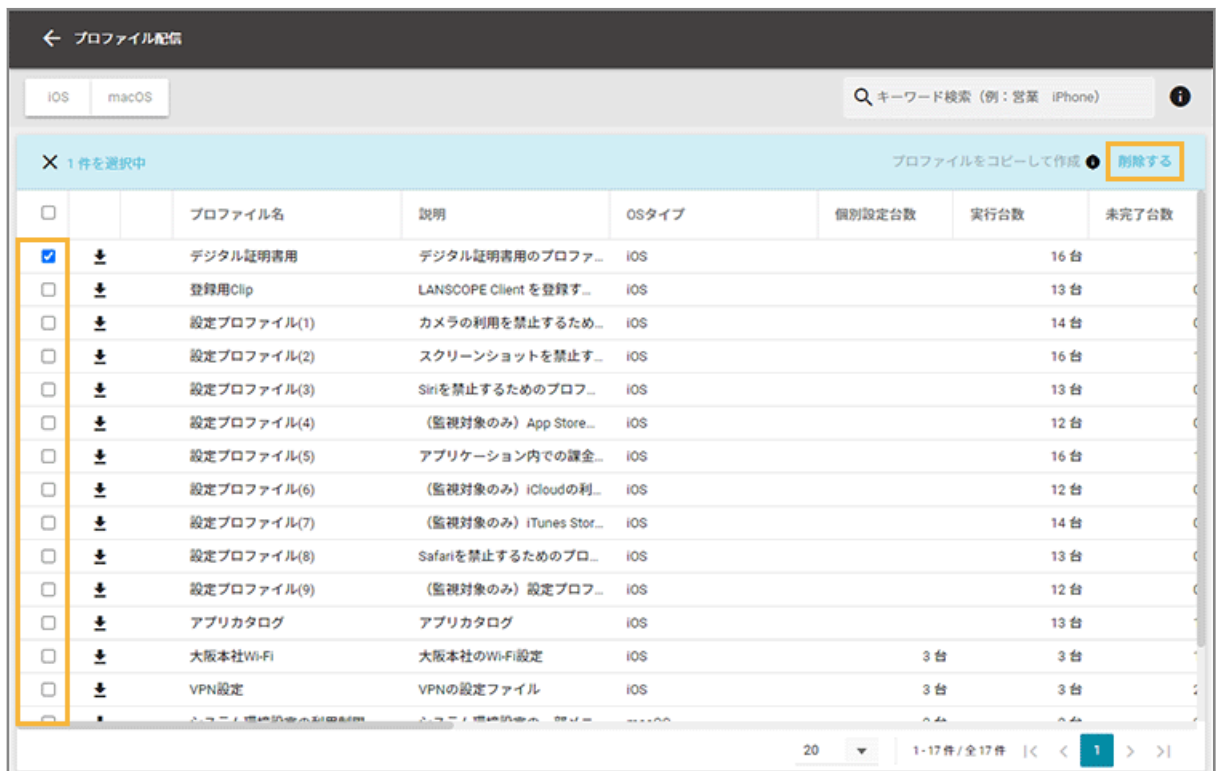
1. [レシピ] の [アクション] をクリックします。



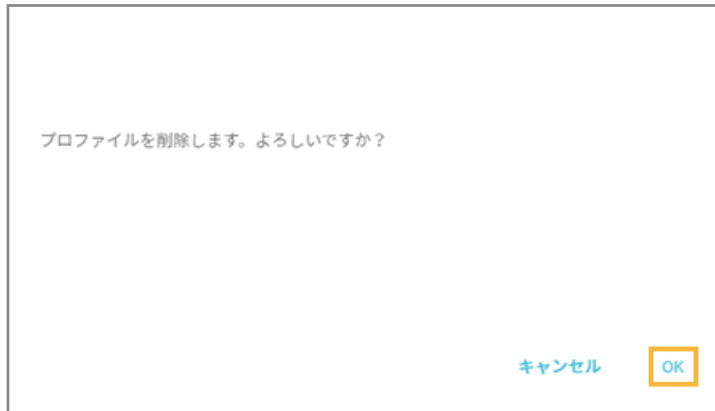
2. [プロフィールを設定する] をクリックします。



3. プロファイルをチェックし、[削除する] をクリックします。



4. [OK] をクリックします。



→ プロファイルが削除されます。

レシピに設定しているプロフィールを削除した場合

レシピには「対象が削除された可能性があります。」と表示されます。



アプリを配信する

IOS

デバイスにアプリを配信します。

ポイント

iOS デバイスにアプリを配信する場合は、Apple サービス設定のアプリ配信をおすすめします。

詳細は、[アプリ配信設定を利用する](#)を参照してください。

アプリ配信の方法

エンドポイントマネージャーでのアプリ配信の方法は、次のとおりです。

レシピを利用する

管理者からアプリを配信します。利用者が「インストール」をタップすると、アプリがインストールされます。



アプリカタログを利用する

管理者がアプリカタログに公開したアプリを、利用者は必要なアプリを任意のタイミングでインストールできます。

設定方法は、[アプリカタログを利用する](#)を参照してください。



アプリ配信/VPP アプリ配信

iOS デバイスに、「App Store に公開されている無償アプリ（以下、App Store アプリ（無償）」）「In-House（自社開発）アプリ」を配信し、デバイス使用者にインストールを促すことができます。また、配信したアプリのアンインストールもできます。

VPP 機能を利用すると、「VPP ストアで購入したアプリ」の配信/アンインストールができます。詳細は、An-353「Apple Business Manager 利用ガイド」を参照してください。

機能と配信方式	アプリ配信機能		VPP アプリ配信機能 デバイスベース方式
対応 OS バージョン	iOS 12 以上/iPadOS 13 以上		iOS 12 以上/iPadOS 13 以上
配信対象	App Store アプリ（無償）	In-House（自社開発）アプリ	VPP アプリ（有償/無償）
Apple ID	必要	不要	不要
App Store が禁止されている場合のアプリ配信（*1）	可（*2）	可	可
サイレントインストール	不可 Apple ID 入力のダイアログが表示される	可 「監視モード」の設定が必要（*3）	可 「監視モード」の設定が必要（*3）

*1：プロファイルで「App Store」の使用を許可していない（アプリのインストールを禁止している）場合のアプリ配信です。

*2：バックグラウンドで起動している LANSCOPE Client などのアプリはアップデートできないことがあります。

*3：デバイスに「監視モード」を設定するには、Apple Configurator を利用して設定するか、自動デバイス登録（DEP）機能を利用して設定してください。DEP 機能を利用した場合、「監視モードに設定する」の項目を有効にした DEP プロファイルをデバイスに割り当て、アクティベーションしてください。

アプリ配信の流れ

iOS

「App Store アプリ（無償）」を配信する場合と、「In-House（自社開発）アプリ」を配信する場合で、アプリ配信の流れが異なります。

■ App Store アプリ（無償）を配信する場合

ステップ：

1. [App Store アプリ（無償）の情報を登録/更新する](#)
2. [アプリを配信する/アンインストールする](#)

ステップ 1： App Store アプリ（無償）の情報を登録/更新する

App Store アプリ（無償）の情報を登録する

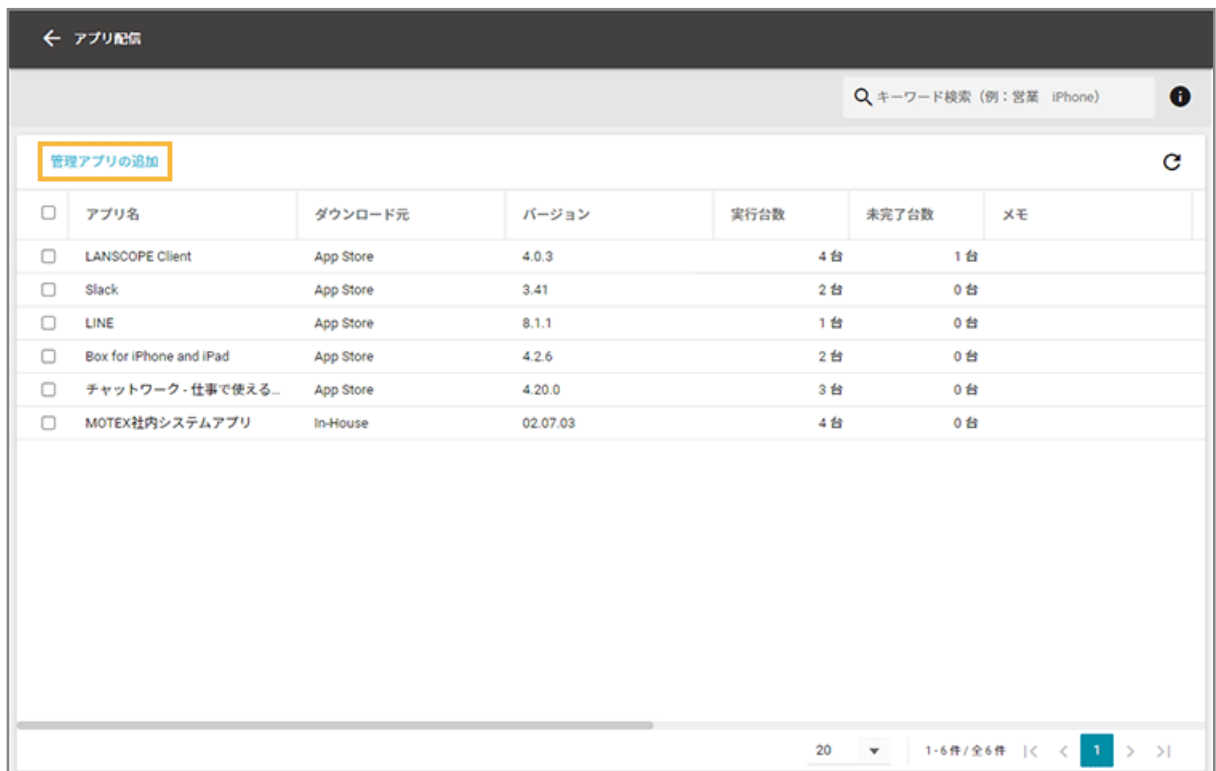
1. [レシピ] の [アクション] をクリックします。



2. [アプリを設定する] をクリックします。



3. [管理アプリの追加] をクリックします。



4. [App Store] をクリックします。



5. アプリ名/アプリ ID/キーワードなどで配信するアプリを検索し、アプリをクリックします。



→ 選択したアプリの基本情報が表示されます。

6. 必要に応じてメモを入力し、[保存] をクリックします。



→ アプリが追加されます。

App Store アプリ（無償）の情報を更新する

App Store に新しいバージョンのアプリが公開された場合、管理コンソールに登録しているアプリも最新バージョンに更新します。

ポイント

管理コンソールのアプリを更新すると、古いバージョンのアプリを使用しているデバイスを確認できます。詳細は、[アプリの配信結果を確認する](#)を参照してください。

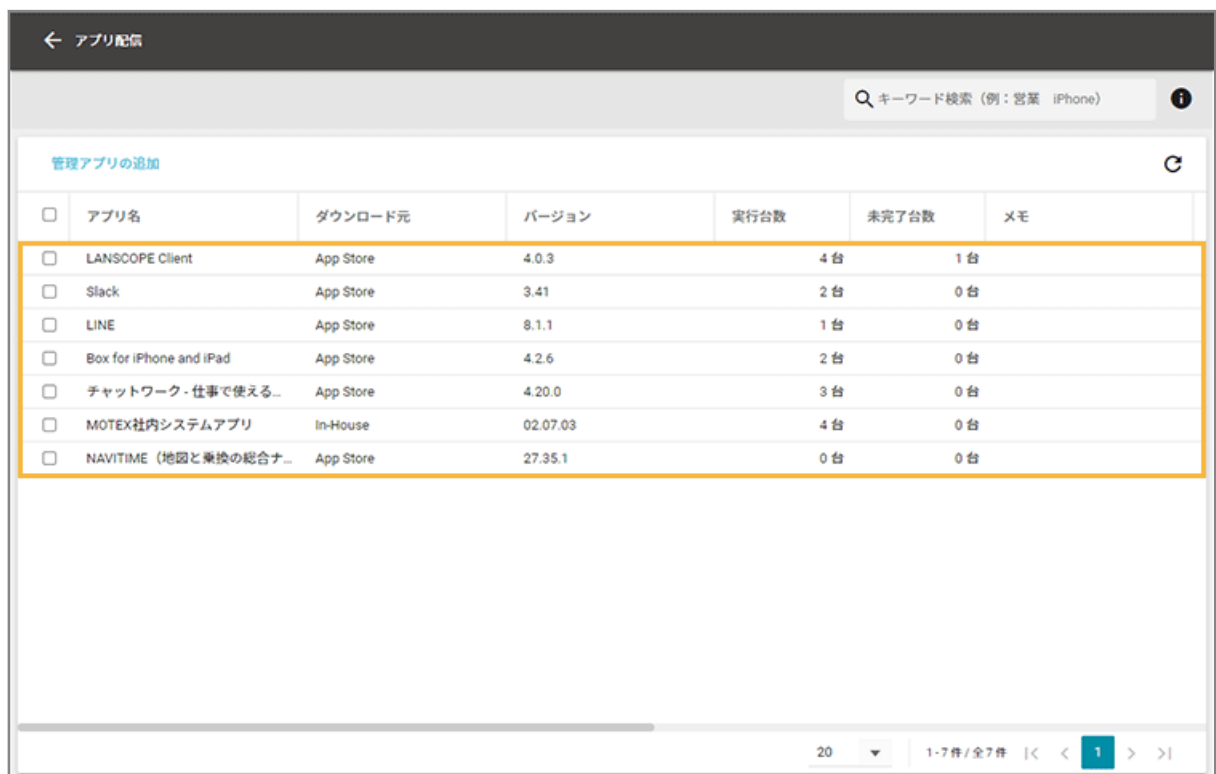
1. [レシピ] の [アクション] をクリックします。



2. [アプリを設定する] をクリックします。



3. アプリをクリックします。



4. [編集] をクリックします。



5. [取得] をクリックします。



→ アプリが更新されます。

6. [保存] をクリックします。

ステップ2： アプリを配信する／アンインストールする

ここでは、デバイスに LANSCOPE クライアントがインストールされたら、指定したアプリを自動配信する場合を例に説明します。

すでに LANSCOPE クライアントがインストールされている場合は、任意のトリガーを選択してください。

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. 次のように設定し、[アクション追加] をクリックします。

項目	値
レシピ名	任意のレシピ名
トリガー	[LANSCOPE クライアントがインストールされた]
デバイスグループ	配信するデバイスグループまたはデバイス
デバイス	

新しいレシピを作成

レシピ名*

乗り換え案内アプリの配信

レシピのトリガーを選択 トリガー選択

トリガー*

LANSCOPE クライアントがインストールされた

レシピを実行する対象の絞り込み

 デバイスグループ (0 件)
選択

 デバイス (0 台)
選択

実行するアクション アクション追加

4. [指定アプリを配信する] をクリックします。

配信したアプリをアンインストールする場合、[指定アプリをアンインストールする] をクリックします。

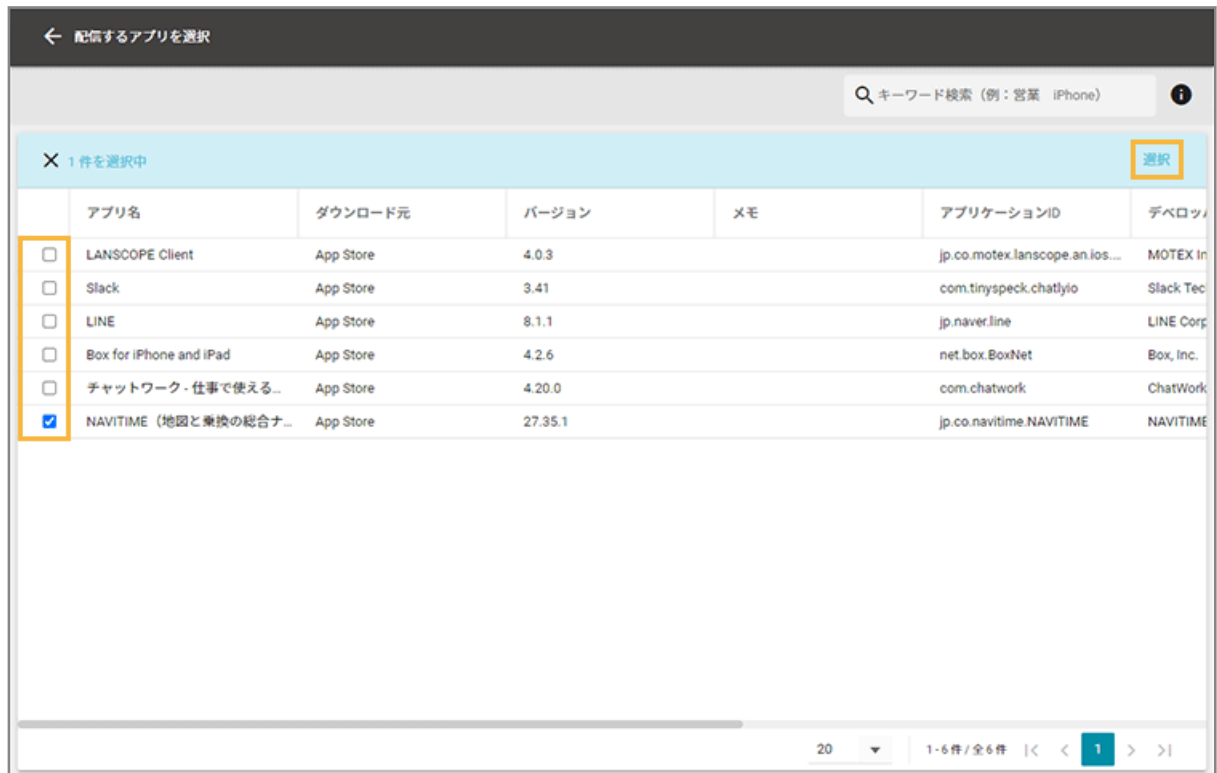
アクションを選択してください

iOS
 Android
 Windows
 macOS

 管理者にメールでお知らせする	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 指定プロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
 指定アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 指定プロビジョニングプロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 指定 VPP アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 メッセージを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
 アンケートを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
 アラートに設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 アラートレポートを送信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 指定プロファイルを取り除く	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

5. アプリをチェックし、[選択] をクリックします。

アプリは、最大 10 件選択できます。



6. 内容を確認し、[保存] をクリックします。

× レシピ作成

新しいレシピを作成

レシピ名*

乗り換え案内アプリの配信

トリガーを選択

トリガー*

LANSCOPE クライアントがインストールされた

レシピを実行する対象の絞り込み

デバイスグループ (1件)

選択

営業部 (22台)

デバイス (0台)

選択

22台のデバイスが対象になっています。 ※ 対象デバイスが多い場合、レシピの実行に時間がかかる可能性があります。

実行するアクション

アクション追加

指定アプリを配信する

アプリを選択

※アプリは最大10件まで選択できます。

NAVITIME (地図と乗換の総合ナビ)

編集

保存

→ レシピが作成されます。

■ In-House（自社開発）アプリを配信する場合

In-House（自社開発）アプリには、プロビジョニングプロファイルが含まれています。プロビジョニングプロファイルには有効期限があり、1年ごとに更新が必要です。有効期限が切れると、In-House（自社開発）アプリを利用できなくなるため、次のいずれかの方法でデバイスのプロビジョニングプロファイルを更新してください。

- [In-House（自社開発）アプリの情報を更新して、デバイスに配信する](#)
- [プロビジョニングプロファイルを更新して、デバイスに配信する](#)

有効期限の確認方法は、[プロビジョニングプロファイルの有効期限を確認する](#)を参照してください。

ステップ：

1. [In-House（自社開発）アプリの情報を登録／更新する](#)
2. [アプリを配信する／アンインストールする](#)

ステップ 1 : In-House (自社開発) アプリの情報を登録/更新する

In-House (自社開発) アプリの登録/更新には、「マニフェストファイル」と「アプリファイル」を利用します。

注意

マニフェストファイル (拡張子 : .plist)

「manifest.plist」ファイルに記載される「Display Image URL」と「Full Size Image URL」の値には、接続できる URL を設定してください。

アプリファイル (拡張子 : .ipa)

アプリファイルのファイルサイズが 4GB を超える In-House (自社開発) アプリは登録できません。

In-House (自社開発) アプリの情報を登録する

1. [レシピ] の [アクション] をクリックします。



2. [アプリを設定する] をクリックします。



3. [管理アプリの追加] をクリックします。

<input type="checkbox"/>	アプリ名	ダウンロード元	バージョン	実行台数	未完了台数	メモ
<input type="checkbox"/>	LANSCOPE Client	App Store	4.0.3	4台	1台	
<input type="checkbox"/>	Slack	App Store	3.41	2台	0台	
<input type="checkbox"/>	LINE	App Store	8.1.1	1台	0台	
<input type="checkbox"/>	Box for iPhone and iPad	App Store	4.2.6	2台	0台	
<input type="checkbox"/>	チャットワーク - 仕事で使える...	App Store	4.20.0	3台	0台	
<input type="checkbox"/>	MOTEX社内システムアプリ	In-House	02.07.03	4台	0台	

4. [In-House] をクリックします。

5. マニフェストファイルとアプリファイルをアップロードします。

(1) マニフェストファイルの [ファイルアップロード] をクリックし、ファイルを選択します。

ポイント

Xcode9 で In-House (自社開発) アプリを開発した場合、「manifest.plist」ファイルを選択してください。

→ 基本情報が表示されます。

(2) アプリファイルの【ファイルアップロード】をクリックし、ファイルを選択します。

→ 基本情報の「ファイルサイズ」と「有効期限」が表示されます。

6. 必要に応じてメモを入力し、【保存】をクリックします。

← In-Houseアプリの追加

保存

アプリ情報の取得

マニフェストファイル

ファイルアップロード FeedbackApp.plist

アプリファイル

ファイルアップロード FeedbackApp.ipa

基本情報

アプリケーション名
MOTEX社内システムアプリ

アプリケーションID
jp.co.motex.house

バージョン
02.07.03

カテゴリ
software

ファイルサイズ
691.46 KB

有効期限
2020/06/19 13:05:20

メモ

メモ

→ アプリが追加されます。

In-House（自社開発）アプリの情報を更新する

配信した In-House（自社開発）アプリをアップデートする場合、登録時と同じ「アプリケーション名」「アプリケーション ID」のファイルで更新します。

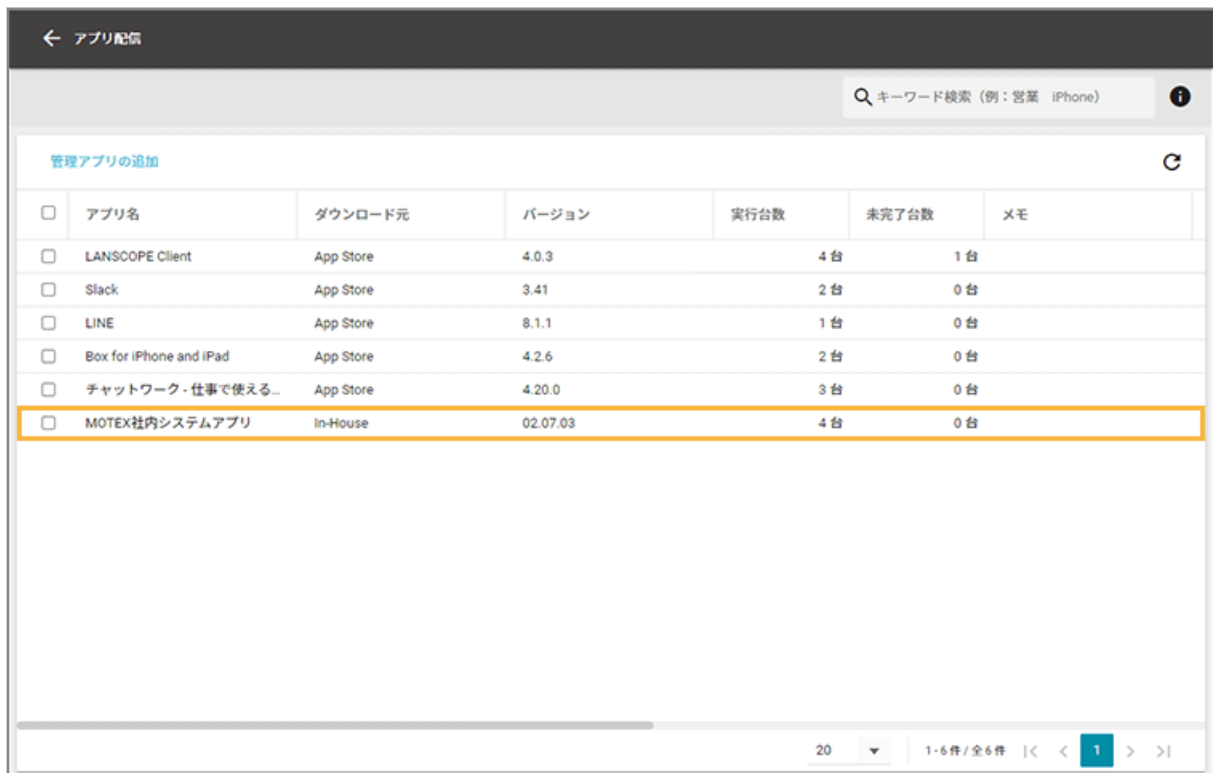
1. 【レシピ】の【アクション】をクリックします。



2. [アプリを設定する] をクリックします。



3. 更新する In-House (自社開発) アプリをクリックします。



4. [編集] をクリックします。



5. マニフェストファイルとアプリファイルを更新します。



(1) マニフェストファイルの [ファイルアップロード] をクリックし、ファイルを選択します。

ポイント

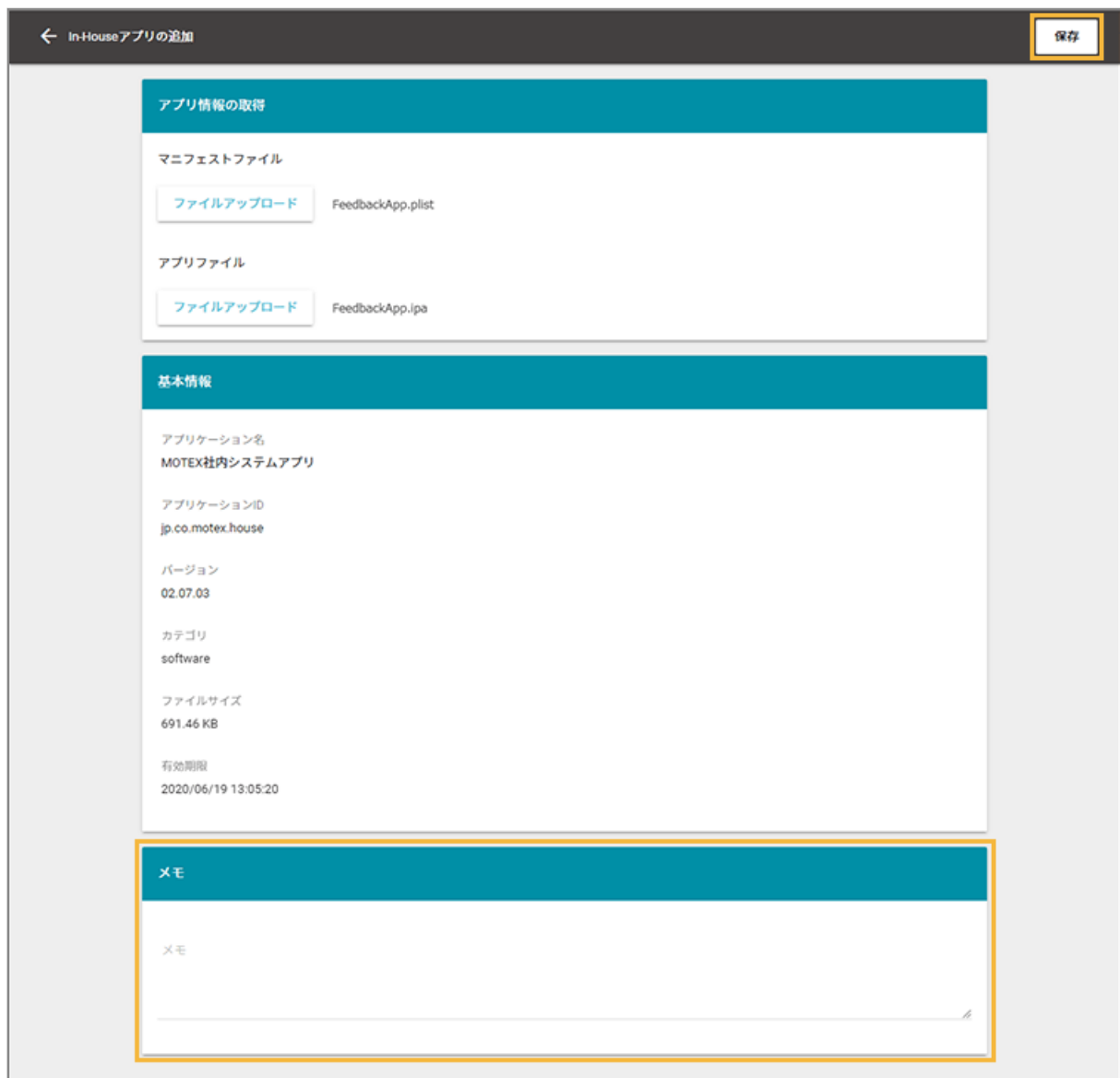
Xcode9 で In-House（自社開発）アプリを開発した場合、「manifest.plist」ファイルを選択してください。

→ 基本情報が更新されます。

(2) アプリファイルの [ファイルアップロード] をクリックし、ファイルを選択します。

→ 基本情報の「ファイルサイズ」と「有効期限」が更新されます。

6. 必要に応じてメモを入力し、[保存] をクリックします。



7. 更新後、アプリを再配信します。

ステップ 2： アプリを配信する／アンインストールする

ここでは、デバイスに LANSCOPE クライアントがインストールされたら、指定したアプリを自動配信する場合を例に説明します。

すでに LANSCOPE クライアントがインストールされている場合は、任意のトリガーを選択してください。

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。

状態	レシピ名	トリガー	アクション
<input type="checkbox"/>	LANSCOPE Client を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定アプリを配信する
<input type="checkbox"/>	LANSCOPE の登録用 Clip を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定プロフィールを配信する
<input checked="" type="checkbox"/>	管理外アラート (iOS/Windows/macOS)	デバイスが管理外になっている	アラートに設定する
<input type="checkbox"/>	パスワードポリシー非準拠アラート (iOS/Android)	パスワードポリシーに準拠していない	アラートに設定する
<input type="checkbox"/>	LANSCOPE Client 未更新アラート (iOS/Android/Windows)	LANSCOPE Client のバージョンが最新になっていない	アラートに設定する
<input checked="" type="checkbox"/>	未稼働アラート (iOS/Android/Windows/macOS)	未稼働期間が指定された期間を超過している	アラートに設定する
<input type="checkbox"/>	空き容量不足アラート (iOS/Android/Windows/macOS)	空き容量が不足している	アラートに設定する
<input type="checkbox"/>	パスワードロックオフアラート (iOS)	パスワードロックの設定がオフになっている	アラートに設定する
<input type="checkbox"/>	リモート実行無効アラート (Android/Windows)	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	アラートに設定する
<input checked="" type="checkbox"/>	SIMカード抜き差しアラート (iOS/Android/Windows)	SIMカードが抜き差しされた	アラートに設定する
<input checked="" type="checkbox"/>	SDカード抜き差しアラート (Android)	SDカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>	新規アプリインストールアラート (Android)	新しくアプリがインストールされた	アラートに設定する
<input type="checkbox"/>	タイムゾーン変更アラート (Android)	タイムゾーンが変更された	アラートに設定する
<input type="checkbox"/>	新規プロフィールインストールアラート (iOS/macOS)	新しくプロフィールがインストールされた	アラートに設定する

3. 次のように設定し、[アクション追加] をクリックします。

項目	値
レシピ名	任意のレシピ名
トリガー	[LANSCOPE クライアントがインストールされた]
デバイスグループ	配信するデバイスグループまたはデバイス
デバイス	

新しいレシピを作成

レシピ名*

バックアップアプリの配信

レシピのトリガーを選択 トリガー選択

トリガー*

LANSCOPE クライアントがインストールされた

レシピを実行する対象の絞り込み

 デバイスグループ (0 件)
選択

 デバイス (0 台)
選択

実行するアクション アクション追加

4. [指定アプリを配信する] をクリックします。

配信したアプリをアンインストールする場合、[指定アプリをアンインストールする] をクリックします。

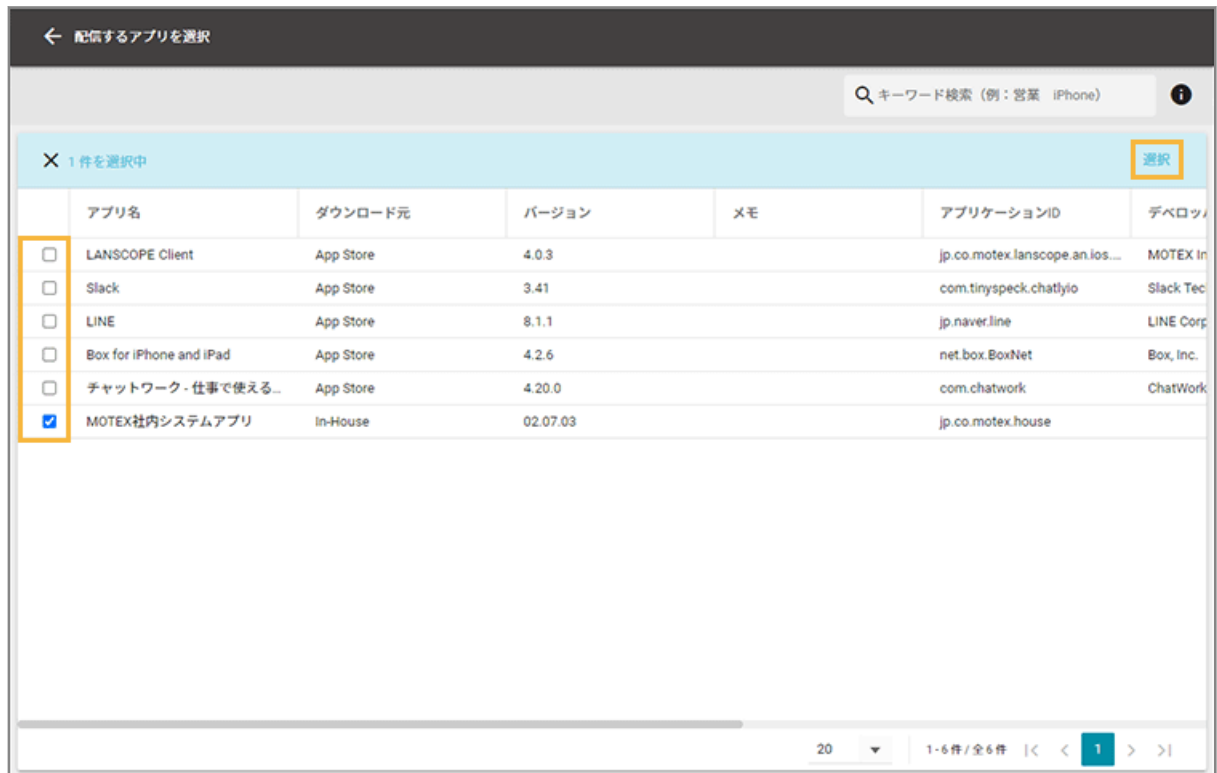
アクションを選択してください

iOS Android Windows macOS

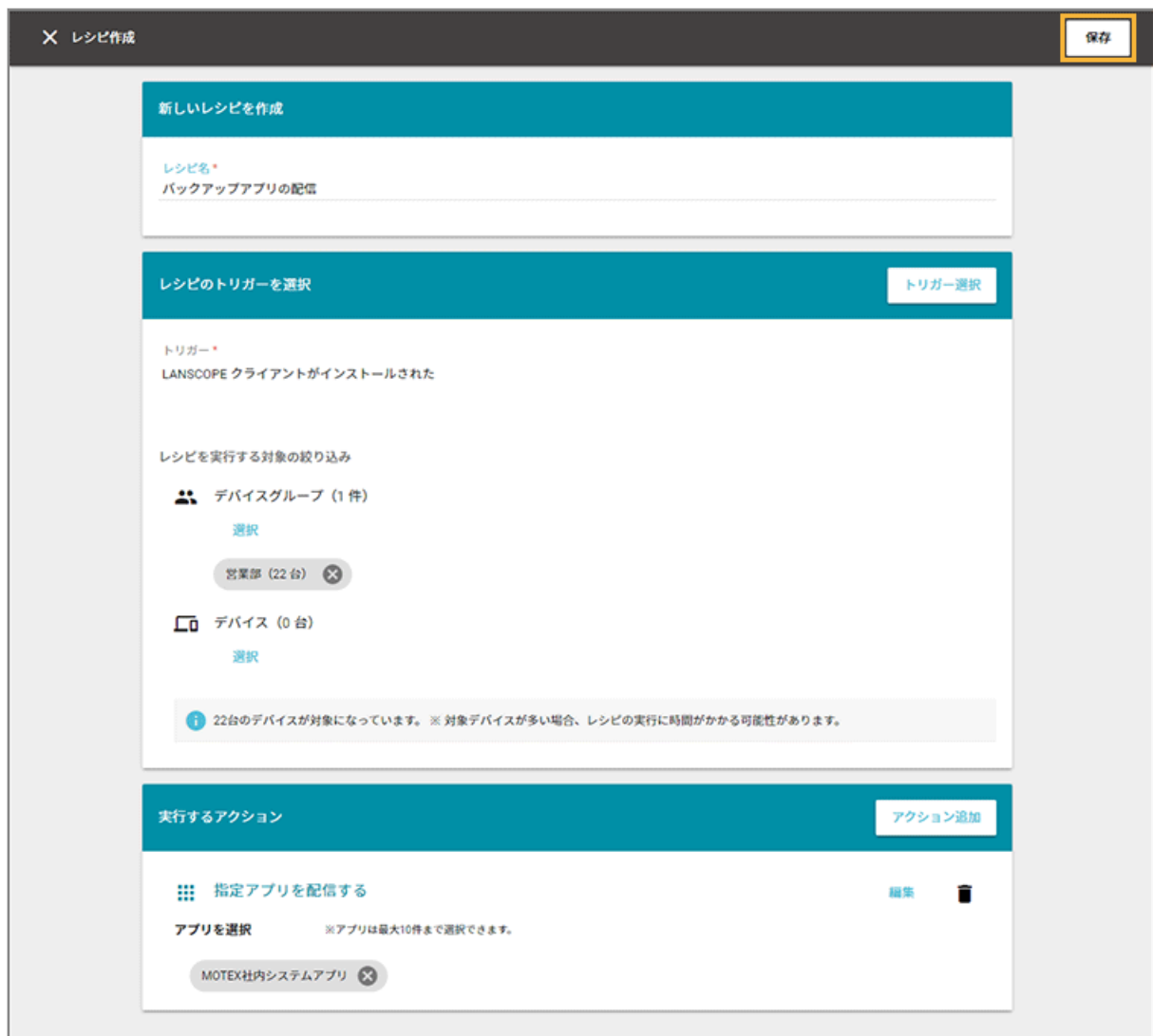
 管理者にメールでお知らせする	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 指定プロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
 指定アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 指定プロビジョニングプロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 指定 VPP アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 メッセージを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
 アンケートを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
 アラートに設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 アラートレポートを送信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 指定プロファイルを取り除く	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

5. アプリをチェックし、[選択] をクリックします。

アプリは、最大 10 件選択できます。



6. 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。

デバイス側での操作

iOS

OSバージョンやデバイスの設定により、画面表記や手順は異なります。

App Store アプリ（無償）の場合

アプリが配信されると、デバイス側にインストールダイアログが表示されます。[インストール] をタップし、インストールします。

ポイント

Apple ID のパスワードの入力を求められた場合、パスワードを入力し、インストールを実行します。



In-House（自社開発）アプリの場合

アプリが配信されると、デバイス側にインストールダイアログが表示されます。[インストール] をタップし、インストールします。

ポイント

デバイスが「監視モード」に設定されている場合、ダイアログは表示されず、サイレントでインストールが開始します。



アプリの配信結果を確認する

iOS

1. [レシピ] の [アクション] をクリックします。



2. [アプリを設定する] をクリックします。



3. アプリをクリックします。

← アプリ配信

キーワード検索 (例: 営業 iPhone)

管理アプリの追加

<input type="checkbox"/>	アプリ名	ダウンロード元	バージョン	実行台数	未完了台数	メモ
<input type="checkbox"/>	LANSCOPE Client	App Store	4.0.3	4台	1台	
<input type="checkbox"/>	Slack	App Store	3.41	2台	0台	
<input type="checkbox"/>	LINE	App Store	8.1.1	1台	0台	
<input type="checkbox"/>	Box for iPhone and iPad	App Store	4.2.6	2台	0台	
<input type="checkbox"/>	チャットワーク - 仕事で使える...	App Store	4.20.0	3台	0台	
<input type="checkbox"/>	MOTEX社内システムアプリ	In-House	02.07.03	4台	0台	
<input type="checkbox"/>	NAVITIME (地図と乗換の総合ナ...	App Store	27.35.1	0台	0台	

20 1-7件/全7件 |< < 1 > >|

4. [実行状況] をクリックします。

NAVITIME (地図と乗換の総合ナビ) - アプリ配信詳細

アプリ配信の内容

管理アプリの編集

実行状況

アプリ情報の取得

App Store の URL
<https://apps.apple.com/jp/app/navitime-%E5%9C%B0%E5%9B%B3%E3%81%A8%E4%B9%97%E6%8F%9B%E3%81%AE%E7%B7%8F%E5%90%88%E3%83%8A%E3%83%93/id365876050?uo=4>

取得

基本情報

アプリ名
NAVITIME (地図と乗換の総合ナビ)

アプリケーションID
jp.co.navitime.NAVITIME

バージョン
27.35.1

デベロッパー
NAVITIME JAPAN CO.,LTD.

閉じる

5. デバイスをチェックし、[最新情報を取得] をクリックします。

NAVITIME (地図と乗換の総合ナビ) - アプリ配信詳細

アプリ配信の内容 未完了のデバイスが1台あります。

実行状況

すべて

× 4件を選択中 再実行する 最新情報を取得

<input checked="" type="checkbox"/>	管理No.	デバイス管理名	使用者名	最終実行操作	状態
<input checked="" type="checkbox"/>	18	iPhone_00000032	佐竹 信弘	インストール	インストール中
<input checked="" type="checkbox"/>	34	iPad_00000036	北井 清二	インストール	インストール済み (管理外) ⓘ
<input checked="" type="checkbox"/>	3	iPhone_00000028	飯田 育三	インストール	インストール済み (配信バージョンと...)
<input checked="" type="checkbox"/>	33	iPad_00000042	横口 播羽	インストール	インストール済み (管理外) ⓘ

20 1-4件/全4件 |< < 1 > >|

[閉じる](#)

6. [OK] をクリックします。

1台のデバイスに対して、下記情報を取得する要求を実行します。

- ・資産情報
- ・インストールアプリ情報
- ・プロフィール情報
- ・プロビジョニングプロフィール情報

以下のデバイスは対象外です。

- ・10分以内に取得要求が実行されたデバイス

取得対象が多い場合、取得完了までに時間がかかる場合があります。

[キャンセル](#) OK

7. 各デバイスの配信状態を確認します。



状態

- インストール済み
[指定アプリを配信する] を実行後、デバイスへインストール済みの状態のときに表示されます。
- インストール済み (配信バージョンと異なる)
配信バージョンと異なるバージョンのアプリがインストールされている場合に表示されます。
再配信する場合、デバイスをチェックし、[再実行する] をクリックします。



- インストール済み (管理外)
[指定アプリを配信する] を実行したが、すでに App Store から手動でインストール済みの状態のときに表示されます。
- インストール中

「指定アプリを配信する」を実行後、まだデバイスにインストールされていない状態のときに表示されます。

再配信する場合、デバイスをチェックし、「再実行する」をクリックします。



- アンインストール済み

「指定アプリをアンインストールする」を実行後、デバイスからアンインストール済みの状態のときに表示されます。

- アンインストール中

「指定アプリをアンインストールする」を実行後、まだデバイスにインストールされている状態のときに表示されます。

- 実行不可（管理外のアプリ）

管理外のアプリ（アプリ配信によりインストールしていないアプリ）をアンインストール指示した場合には表示されます。

完了待ち日数

「状態」が「インストール中」「アンインストール中」の場合、「最新配信日時」からの経過日数が表示されます。「状態」が「インストール済み」「アンインストール済み」の場合、空欄です。

実行方法

- レシピ

レシピによるアプリ配信の場合に表示されます。

- 直接実行

「リスト」>「デバイス」でデバイスを選択し、アクションを実行した場合に表示されます。

レシピ名

「実行方法」が「レシピ」の場合、レシピ名が表示されます。「実行方法」が「直接実行」の場合は空欄です。

登録したアプリを削除する

iOS

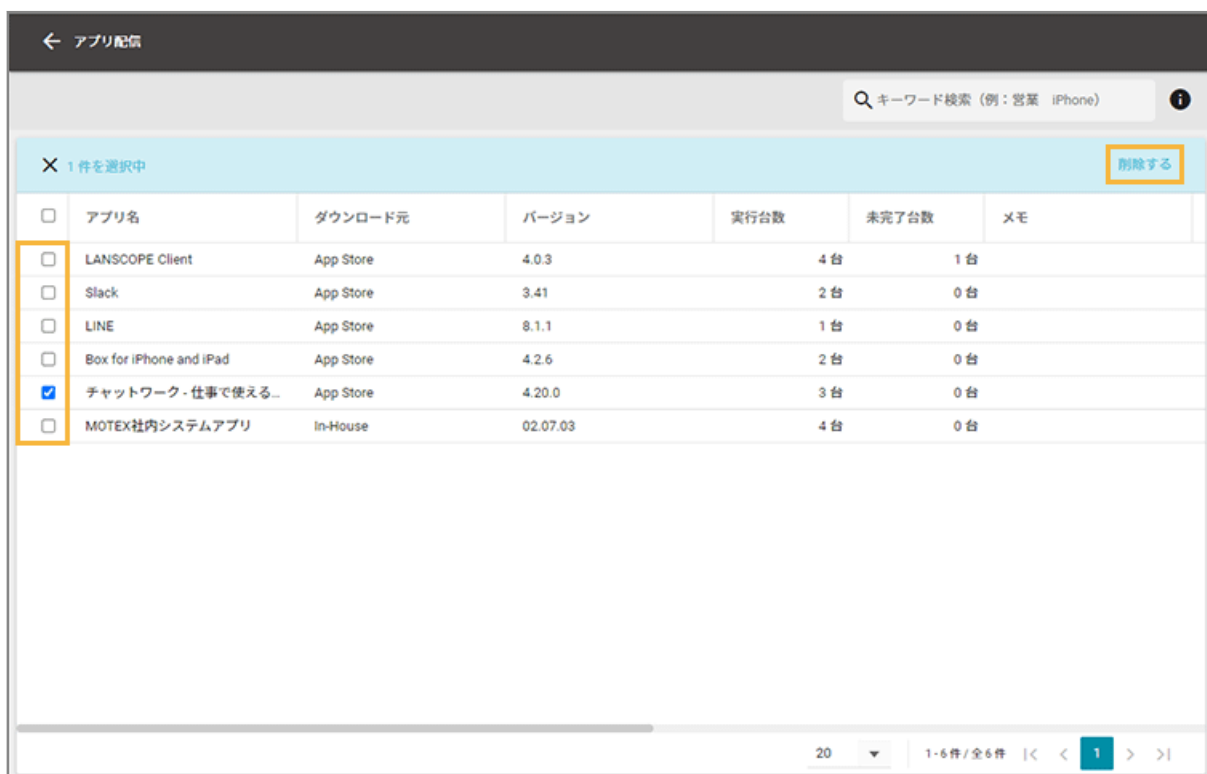
1. [レシピ] の [アクション] をクリックします。



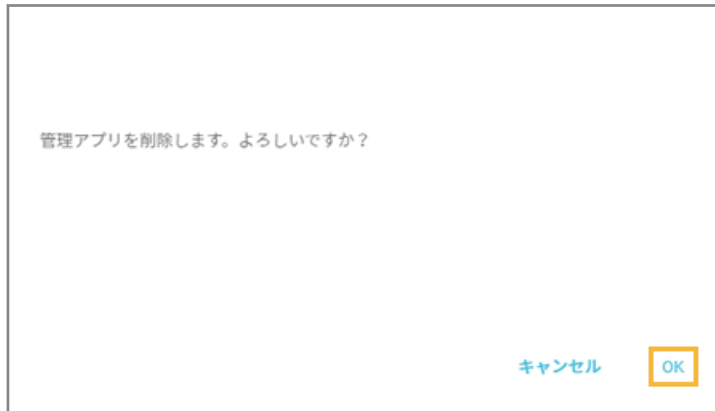
2. [アプリを設定する] をクリックします。



3. アプリをチェックし、[削除する] をクリックします。



4. [OK] をクリックします。



→ アプリが削除されます。

レシピに設定しているアプリを削除した場合

レシピには「対象が削除された可能性があります。」と表示されます。



プロビジョニングプロファイルを配信する

iOS

プロビジョニングプロファイルを配信できます。

プロビジョニングプロファイル配信とは

プロビジョニングプロファイルは、iOS デバイスで、In-House（自社開発）アプリが動作するために必要な情報をまとめて定義したファイルです。

プロビジョニングプロファイル作成に必要なもの

プロビジョニングプロファイルを作成するには、Apple Developer Enterprise Program 専用の Apple ID が必要です。「Apple Developer - Member Center」にアクセスするときに、ログイン ID/パスワードとして Apple ID の情報を求められます。

プロビジョニングプロファイルの有効期限を確認する

プロビジョニングプロファイルには有効期限があり、1年ごとに更新が必要です。有効期限が切れると、In-House（自社開発）アプリを利用できなくなるため、有効期限前にデバイスのプロビジョニングプロファイルを更新してください。

- 登録時の有効期限は、「アプリ詳細」画面で確認できます。
 - [レシピ] > [アクション] で、[アプリを設定する] をクリックします。
 - 「アプリ一覧」画面で、In-House（自社開発）アプリをクリックし、「In-House アプリ配信の内容」の「基本情報」で「有効期限」を確認します。



- 更新後の有効期限は、「プロビジョニングプロファイル配信」画面で確認できます。
 - [レシピ] > [アクション] で、[プロビジョニングプロファイルを設定する] をクリックします。
 - 「有効期限」欄を確認します。

<input type="checkbox"/>	管理名	プロファイル名	有効期限	実行台数	未完了台数	メモ
<input type="checkbox"/>	MOTEX社内システムアプリ	MOTEX社内システムアプリ	2023/07/28 17:30:34	16 台	0 台	
<input type="checkbox"/>	MOTEXお客様番号アプリ	MOTEXお客様番号アプリ	2023/03/31 23:11:28	12 台	1 台	

プロビジョニングプロファイル配信の流れ

iOS

ポイント

- レシピを作成すると、プロビジョニングプロファイル配信／配信したプロファイルのアンインストールができません。レシピで設定したトリガーのタイミングで、配信／アンインストールが実行されます。
デバイスにパスコードが設定されている場合、画面ロック解除後にプロビジョニングプロファイルが配信されません。
- 配信したプロビジョニングプロファイルは、デバイスからアンインストールできません。プロビジョニングプロファイルの配信と同様に、レシピを利用してアンインストールします。エンドポイントマネージャーの配信以外でインストールしたプロビジョニングプロファイルは、エンドポイントマネージャーからはアンインストールできません。

ステップ：

1. [プロビジョニングプロファイルの登録／編集](#)
2. [プロビジョニングプロファイルを配信する／アンインストールする](#)

ステップ 1： プロビジョニングプロファイルの登録／編集

プロビジョニングプロファイルを登録する

1. Apple 社の公式サイト「Apple Developer - Member Center」で、あらかじめプロビジョニングプロファイルを作成します。
2. [レシピ] の [アクション] をクリックします。



3. [プロビジョニングプロファイルを設定する] をクリックします。



4. [プロビジョニングプロファイルの追加] をクリックします。

<input type="checkbox"/>	管理名	プロファイル名	有効期限	実行台数	未完了台数	メモ
<input type="checkbox"/>	MOTEX社内システムアプリ	MOTEX社内システムアプリ	2023/07/28 17:30:34	16台	0台	
<input type="checkbox"/>	MOTEXお客様番号アプリ	MOTEXお客様番号アプリ	2023/03/31 23:11:28	12台	1台	

5. [ファイルをアップロード] をクリックし、プロビジョニングプロファイルを選択します。

プロビジョニングプロファイルの拡張子は「.mobileprovision」です。



6. [保存] をクリックします。

← プロビジョニングプロファイルの追加 保存

アップロードするプロビジョニングプロファイルを選択

ファイルアップロード xxx_lanscopean.mobileprovision

基本情報

管理名*
xxx_lanscopean

プロフィール名
[REDACTED]

プロフィール識別子
xxx_lanscopean

UUID
[REDACTED]

有効期限
[REDACTED]

メモ

メモ

プロビジョニングプロファイルを編集する

注意

編集できる項目は、管理名とメモだけです。プロビジョニングプロファイルのファイル自体の更新をする場合、追加で登録してください。

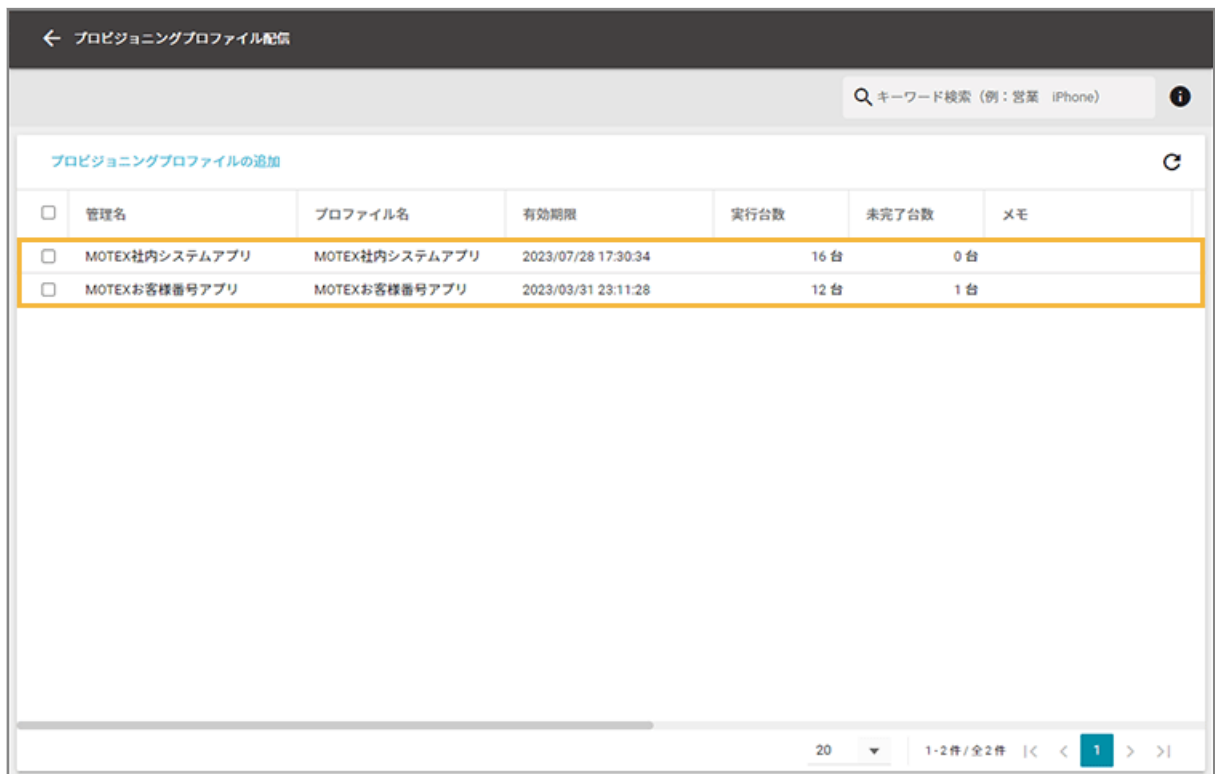
1. [レシピ] の [アクション] をクリックします。



2. [プロビジョニングプロファイルを設定する] をクリックします。



3. プロビジョニングプロファイルをクリックします。



4. [編集] をクリックし、内容を編集します。

MOTEX社内システムアプリ - プロビジョニングプロフィール配信詳細

配信の内容	プロビジョニングプロフィールの編集	編集
実行状況	<p>基本情報</p> <p>管理名 MOTEX社内システムアプリ</p> <p>プロフィール名 MOTEX社内システムアプリ</p> <p>プロフィール識別子 jp.co.motex.house</p> <p>UUID 34862c29-4049-4944-9c95-f0d88ea218fa</p> <p>有効期限 2023/04/22 17:30:34</p> <p>メモ</p> <p>メモ .</p>	閉じる

5. [保存] をクリックします。

MOTEX社内システムアプリ - プロビジョニングプロフィール配信詳細

配信の内容	プロビジョニングプロフィールの編集	キャンセル	保存
実行状況	<p>基本情報</p> <p>管理名 * MOTEX社内システムアプリ</p> <p>プロフィール名 MOTEX社内システムアプリ</p> <p>プロフィール識別子 jp.co.motex.house</p> <p>UUID 34862c29-4049-4944-9c95-f0d88ea218fa</p> <p>有効期限 2023/04/22 17:30:34</p> <p>メモ</p> <p>メモ</p>	閉じる	

ステップ2： プロビジョニングプロファイルを配信する／アンインストールする

ここでは、任意のタイミングでプロビジョニングプロファイルを配信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. 次のように設定し、[アクション追加] をクリックします。

項目	値
レシピ名	任意のレシピ名
トリガー	[任意のタイミングで実行する]
デバイスグループ	配信するデバイスグループまたはデバイス
デバイス	

新しいレシピを作成

レシピ名*
 プロビジョニングプロファイル配信

レシピのトリガーを選択 トリガー選択

トリガー*
 任意のタイミングで実行する

レシピを実行する対象の絞り込み

- 👤 デバイスグループ (0 件)
選択
- 📱 デバイス (0 台)
選択

実行するアクション アクション追加

4. [指定プロビジョニングプロファイルを配信する] をクリックします。

配信したプロビジョニングプロファイルをアンインストールする場合、[指定プロビジョニングプロファイルをアンインストールする] をクリックします。

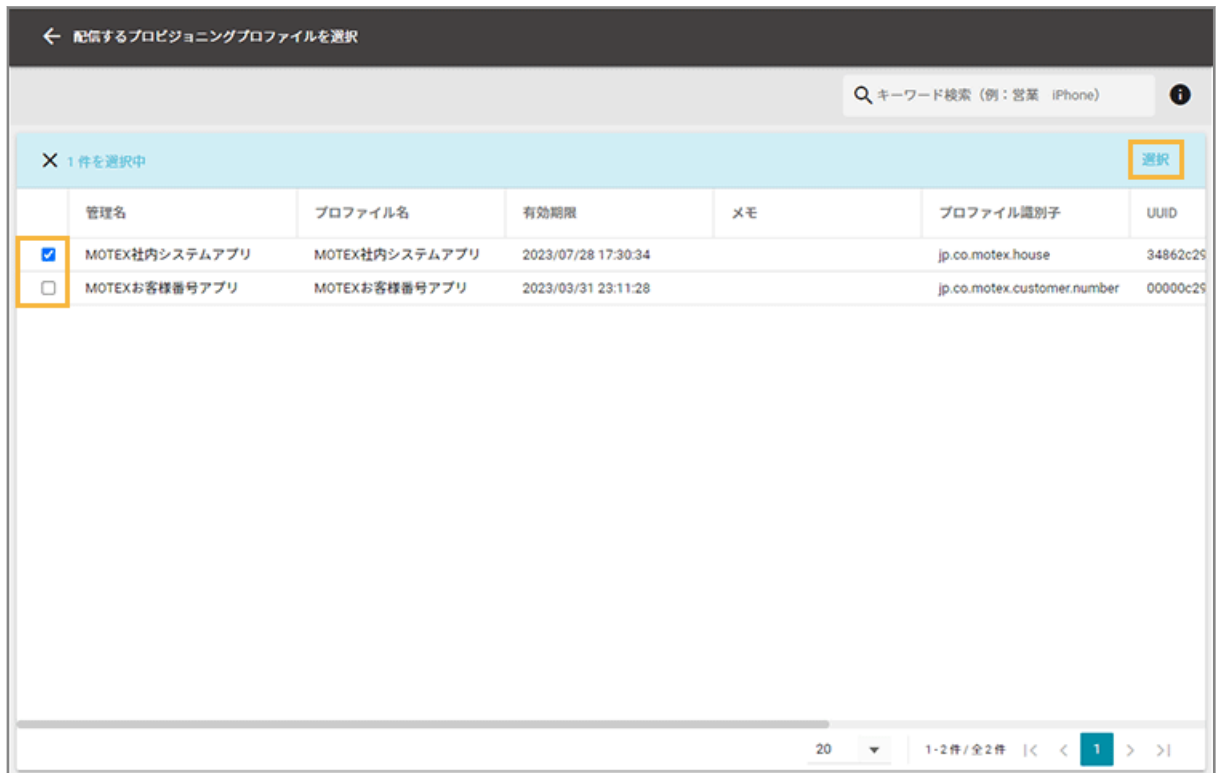
アクションを選択してください

iOS
Android
Windows
macOS

管理者にメールでお知らせする	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定プロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
指定アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
指定プロビジョニングプロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
指定 VPP アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
メッセージを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
アンケートを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
アラートに設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
アラートレポートを送信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定プロファイルを取り除く	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

5. プロビジョニングプロファイルをチェックし、[選択] をクリックします。

プロビジョニングプロファイルは、最大 10 件選択できます。



6. 内容を確認し、[保存] をクリックします。

× レシピ作成 保存

新しいレシピを作成

レシピ名*
プロビジョニングプロファイル配信

レシピのトリガーを選択 トリガー選択

トリガー*
任意のタイミングで実行する

レシピを実行する対象の絞り込み

👤 デバイスグループ (1 件)
選択
営業部 (22 台) ×

📱 デバイス (0 台)
選択

📌 22台のデバイスが対象になっています。 ※ 対象デバイスが多い場合、レシピの実行に時間がかかる可能性があります。

実行するアクション アクション追加

📄 指定プロビジョニングプロファイルを配信する 編集 🗑️

プロビジョニングプロフ ※プロビジョニングプロファイルは最大10件まで選択できます。
ファイルを選択

MOTEX社内システムアプリ ×

→ レシピが作成されます。

プロビジョニングプロファイルの配信結果を確認する

iOS

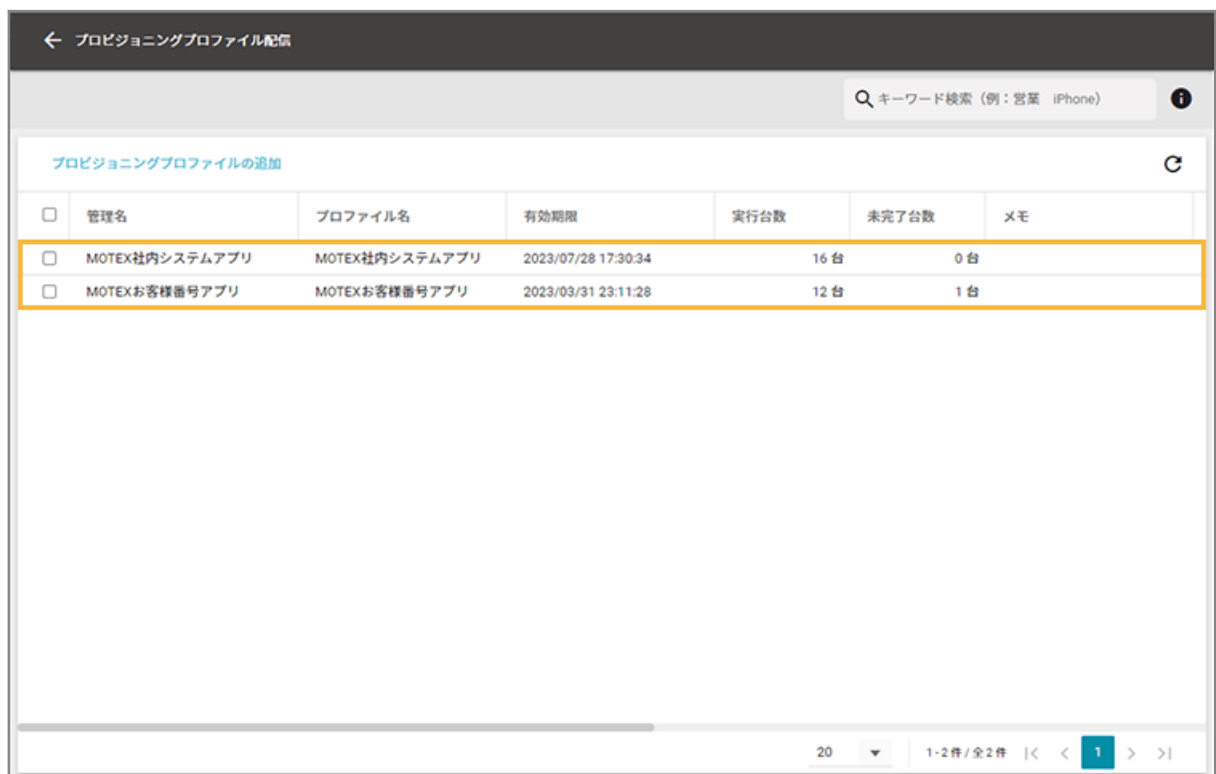
1. [レシピ] の [アクション] をクリックします。



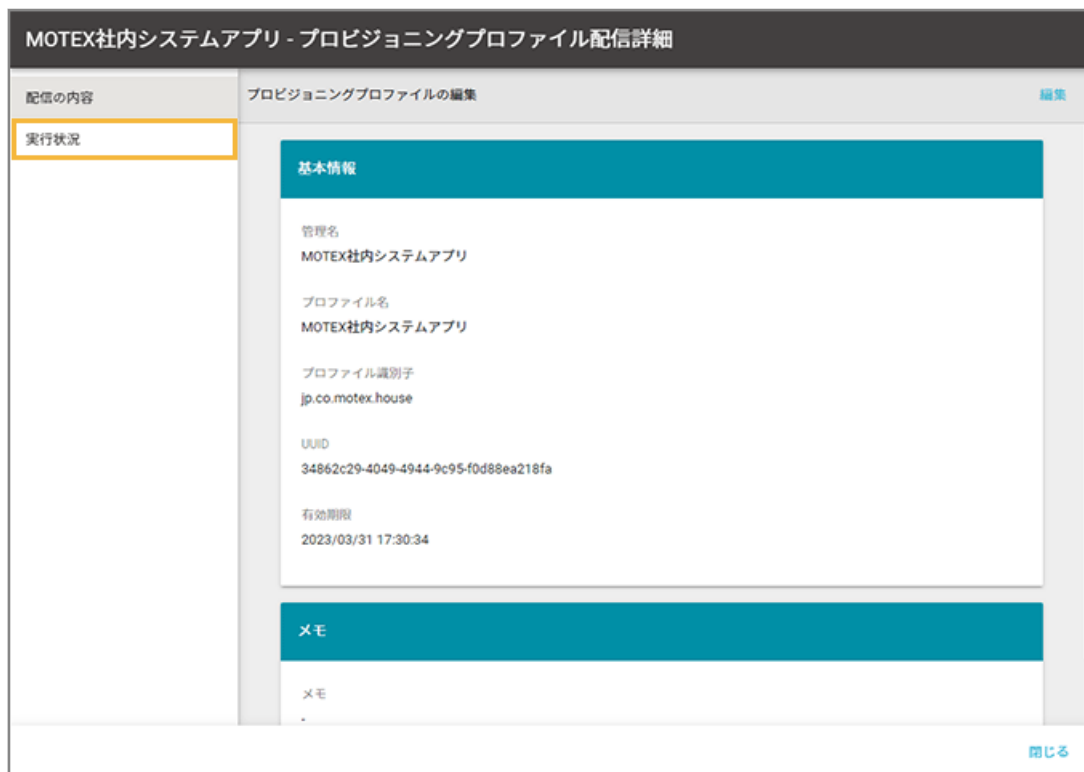
2. [プロビジョニングプロファイルを設定する] をクリックします。



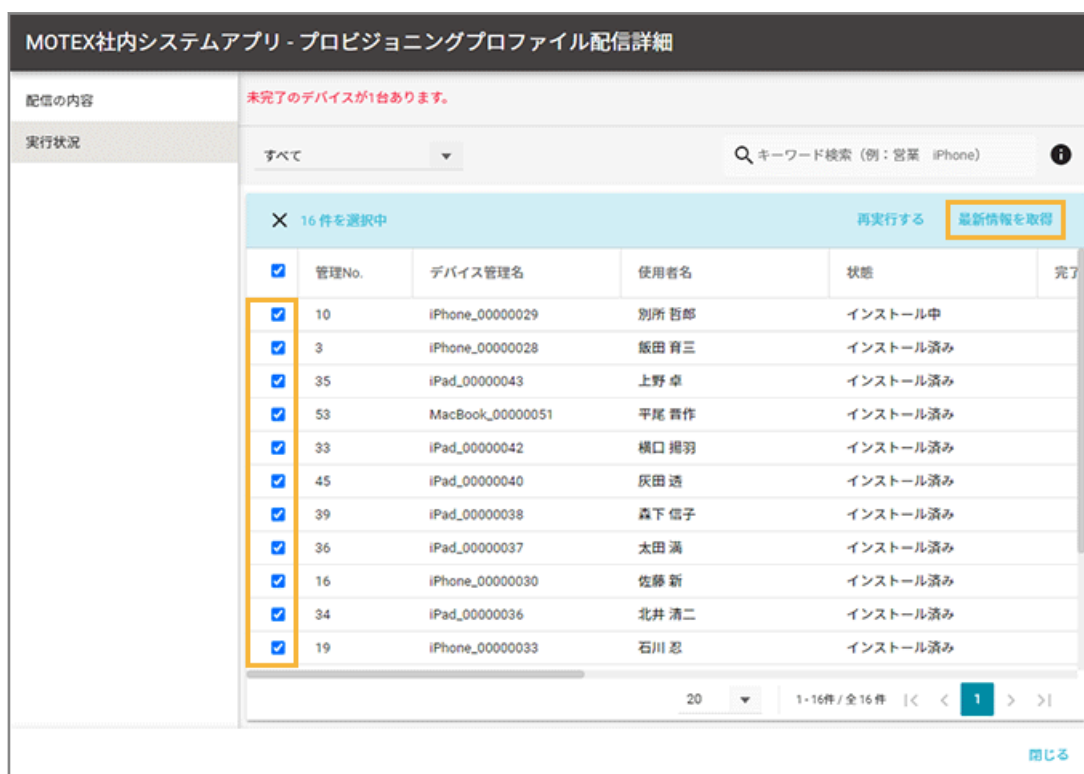
3. プロビジョニングプロファイルを選択します。



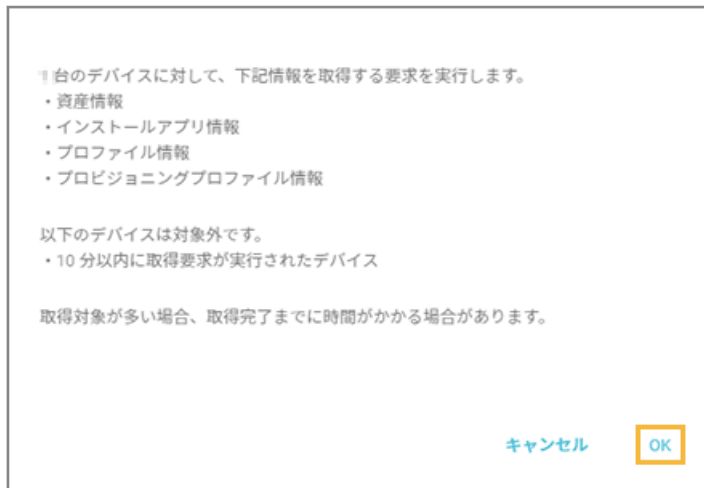
4. [実行状況] をクリックします。



5. デバイスをチェックし、[最新情報を取得] をクリックします。



6. [OK] をクリックします。



7. 各デバイスの配信状態を確認します。

MOTEX社内システムアプリ - プロビジョニングプロファイル配信詳細

配信の内容 未完了のデバイスが1台あります。

実行状況 すべて キーワード検索 (例: 営業 iPhone) 完了

<input type="checkbox"/>	管理No.	デバイス管理名	使用者名	状態
<input type="checkbox"/>	10	iPhone_00000029	別所 哲郎	インストール中
<input type="checkbox"/>	3	iPhone_00000028	飯田 育三	インストール済み
<input type="checkbox"/>	35	iPad_00000043	上野 卓	インストール済み
<input type="checkbox"/>	53	MacBook_00000051	平尾 晋作	インストール済み
<input type="checkbox"/>	33	iPad_00000042	横口 掲羽	インストール済み
<input type="checkbox"/>	45	iPad_00000040	灰田 透	インストール済み
<input type="checkbox"/>	39	iPad_00000038	森下 信子	インストール済み
<input type="checkbox"/>	36	iPad_00000037	太田 満	インストール済み
<input type="checkbox"/>	16	iPhone_00000030	佐藤 新	インストール済み
<input type="checkbox"/>	34	iPad_00000036	北井 清二	インストール済み
<input type="checkbox"/>	19	iPhone_00000033	石川 忍	インストール済み

20 1-16件 / 全16件 < 1 >

閉じる

状態

- インストール済み

「指定プロビジョニングプロファイルを配信する」を実行後、デバイスへインストール済みの状態のときに表示されます。

- インストール中

「指定プロビジョニングプロファイルを配信する」を実行後、まだデバイスにインストールされていない状態のときに表示されます。

再配信する場合、デバイスをチェックし、[再実行する]をクリックします。



- アンインストール済み

「指定プロビジョニングプロファイルを取り除く」を実行後、デバイスからアンインストール済みの状態のときに表示されます。

- アンインストール中

「指定プロビジョニングプロファイルを取り除く」を実行後、まだデバイスにインストールされている状態のときに表示されます。

完了待ち日数

「状態」が「インストール中」「アンインストール中」の場合、「最新配信日時」からの経過日数が表示されます。「状態」が「インストール済み」「アンインストール済み」の場合、空欄です。

実行方法

- レシピ

レシピによるプロビジョニングプロファイル配信／取り除きの場合

- 直接実行

[リスト] > [デバイス] でデバイスを選択し、アクション実行した場合

レシピ名

「実行方法」が「レシピ」の場合、レシピ名が表示されます。「実行方法」が「直接実行」の場合、空欄です。

プロビジョニングプロファイルを削除する

iOS

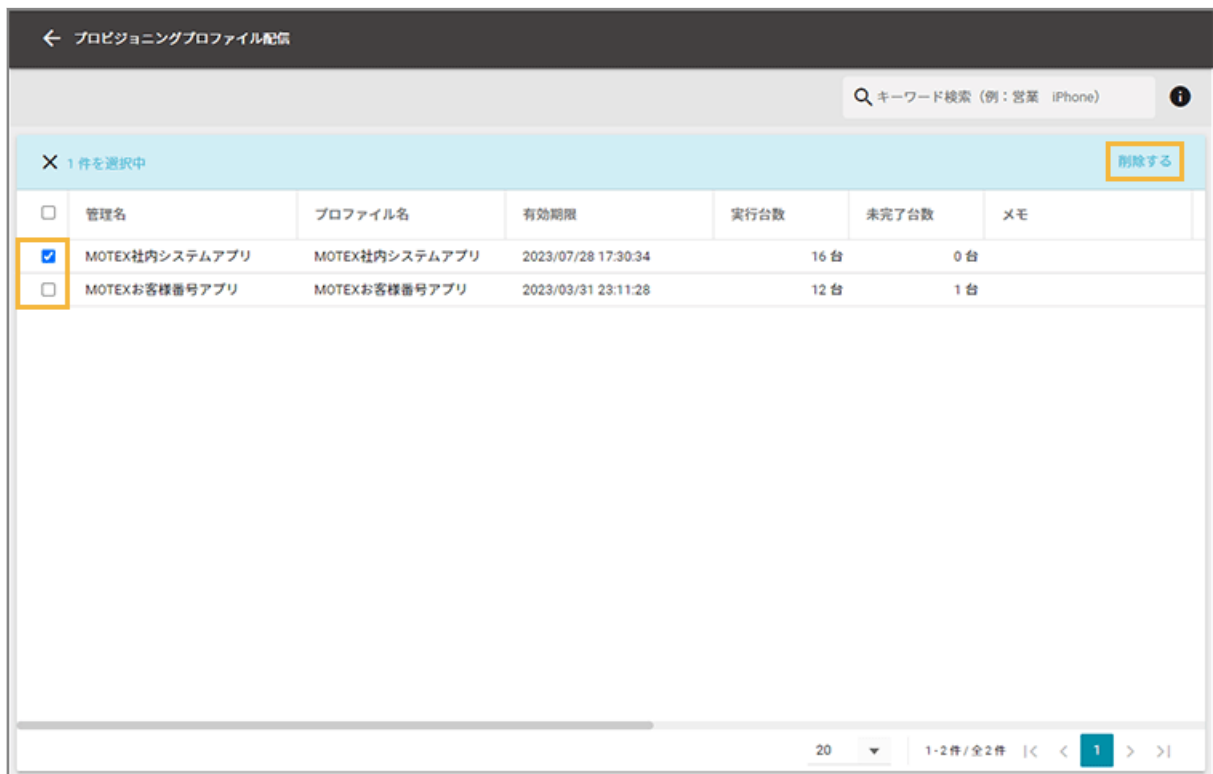
1. [レシピ] の [アクション] をクリックします。



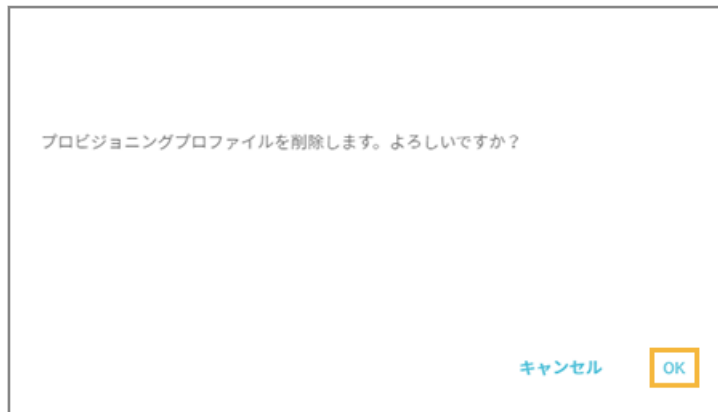
2. [プロビジョニングプロファイルを設定する] をクリックします。



3. プロビジョニングプロファイルをチェックし、[削除する] をクリックします。



4. [OK] をクリックします。



→ プロビジョニングプロファイルが削除されます。

メッセージ/アンケートを配信する

iOS

Android

Windows

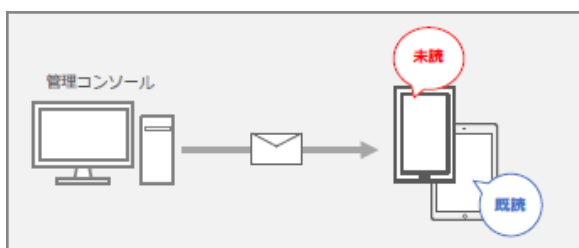
デバイスにメッセージやアンケートを配信できます。

複数デバイスに一括で配信して、情報を共有できます。また、ファイルのアップロードもできます。

アンケート機能では、管理者からアンケートを送信し、回答を要求できます。社員番号や所属部署など、エンドポイントマネージャーで自動取得できない情報をアンケートで収集し、デバイス情報に反映できます。反映した情報は、[リスト] > [デバイス] で確認できます。

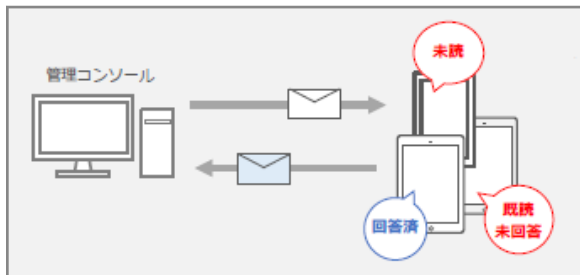
メッセージ機能

デバイス使用者に対して、管理者からメッセージを送信できます。送信対象のデバイスは、管理コンソールから一括選択したり、あらかじめ設定したグループを選択したり、柔軟に設定できます。また、未読/既読のステータスも確認できます。



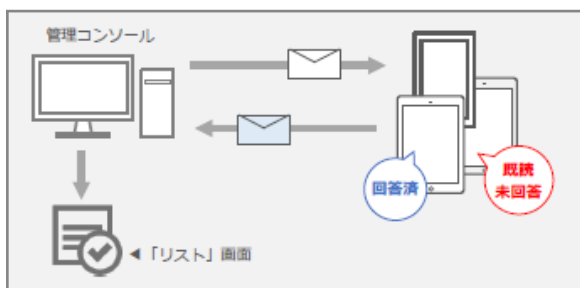
アンケート機能：管理者が任意の質問/情報をデバイス使用者から収集する場合

デバイス使用者に対して、管理者が自由に質問を設定し、回答を要求できます。質問の回答は、管理者が設定した選択肢/日付選択/自由記述の中から設定できます。また、回答は管理コンソールから一覧で確認できます。



アンケート機能：収集した情報を「リスト」に反映させる場合

エンドポイントマネージャーで自動収集できない項目（所属グループの情報／利用者の名前など）をアンケートで質問し、デバイス使用者の回答を「リスト」の「デバイス情報」に反映できます。



メッセージ／アンケート配信の流れ

iOS

Android

Windows

配信後、デバイス上のLANSCOPE Clientで、配信されたメッセージやアンケートを確認できます。

ステップ：

1. [メッセージ／アンケートを作成する](#)
2. [メッセージ／アンケートを配信する](#)

ステップ1：メッセージ／アンケートを作成する

メッセージの作成

1. [レシピ] の [アクション] をクリックします。



2. [メッセージを設定する] をクリックします。

アクションを選択してください

	IOS	Android	Windows	macOS
プロファイルを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
アプリを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
プロビジョニングプロファイルを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VPP アプリを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
メッセージを設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
アンケートを設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
操作ログを一括で出力する	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
位置情報を一括で出力する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>

3. [メッセージの追加] をクリックします。

← メッセージ配信

キーワード検索 (例: 営業 iPhone) ⓘ

メッセージの追加 ↻

<input type="checkbox"/>	件名	添付ファイル数	配信台数	未読台数	最終更新者	最終更新日時
<input type="checkbox"/>	【お知らせ】iOSのアップデートについて	0個	17台	7台	設定管理者 (元中)	2018/04/10 13

20 1-1件/全1件 << 1 >>

4. メッセージを入力し、[保存] をクリックします。



件名

メッセージの件名です。

本文

メッセージの本文です。

ポイント

- 本文に「http」「https」から始まる URL が含まれる場合、デバイス側にハイパーリンクで表示されます。
- iOS で、Safari を利用禁止にしている場合、ハイパーリンクにはなりません。

ファイル添付

クリックすると、添付するファイルを選択できます。

→ メッセージが追加されます。

アンケートの作成

1. [レシピ] の [アクション] をクリックします。

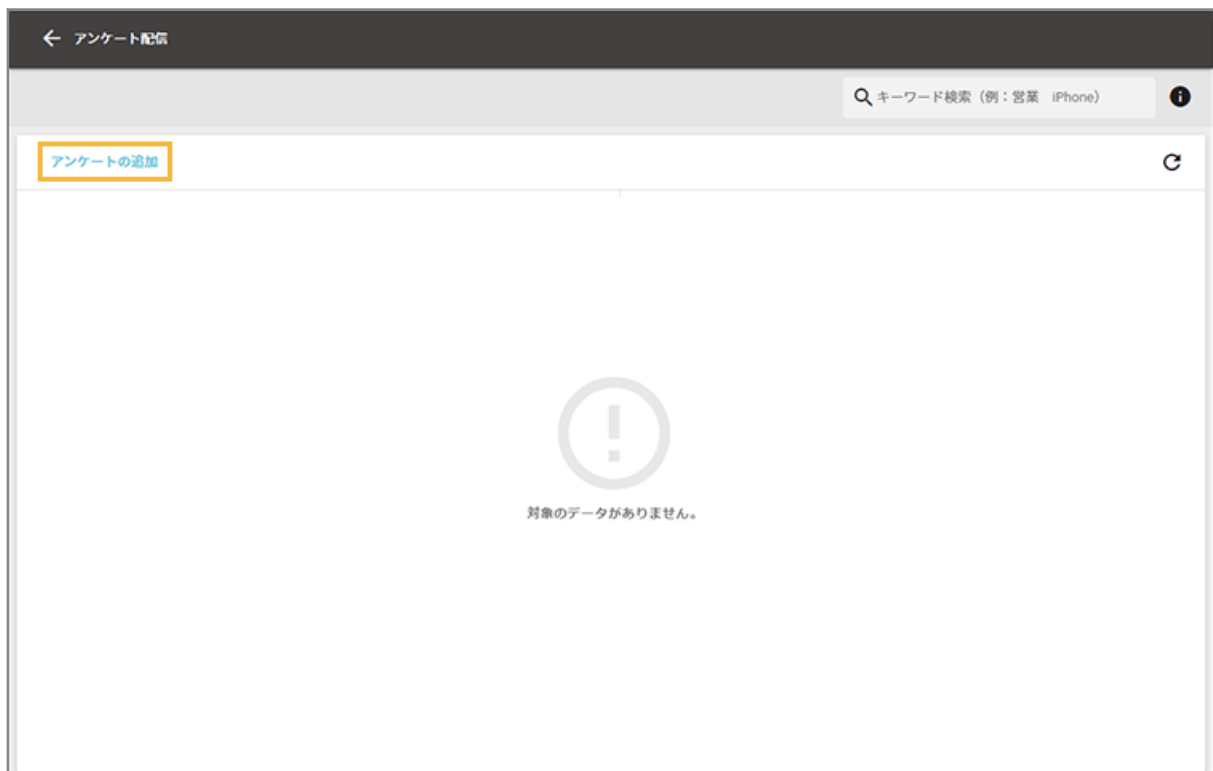


2. [アンケートを設定する] をクリックします。

アクションを選択してください

	IOS	Android	Windows	macOS
 プロファイルを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
 アプリを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 プロビジョニングプロファイルを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 VPP アプリを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 メッセージを設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
 アンケートを設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
 操作ログを一括で出力する	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 位置情報を一括で出力する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>

3. [アンケートの追加] をクリックします。



4. メッセージを入力します。

← アンケートの追加 保存

メッセージ

件名*
所属部署情報の回答のお願い

本文*
ご自身のお名前、所属部署情報などのヒアリングです。「資産権却ルール」の資料を確認の上、アンケートに回答してください。不明点は情報システム部（内線500）までご連絡ください。

ファイル添付

1 / 5 個

資産権却ルール.pptx ×

+ ここに設問を追加

件名

アンケートの件名です。

本文

アンケートの本文です。

ポイント

- 本文に「http」「https」から始まる URL が含まれる場合、デバイス側にハイパーリンクで表示されます。
- iOS で、Safari を利用禁止にしている場合、ハイパーリンクにはなりません。

ファイル添付

クリックすると、添付するファイルを選択できます。

5. **【ここに設問を追加】** をクリックします。

← アンケートの追加 保存

メッセージ

件名*
所属部署情報の回答のお願い

本文*
ご自身のお名前、所属部署情報などのヒアリングです。「資産権即ルール」の資料を確認の上、アンケートに回答してください。不明点は情報システム部（内線500）までご連絡ください。

ファイル添付

1 / 5 個

資産権即ルール.pptx ×

+ここに設問を追加

→ 画面下部に設問の入力フォームが表示されます。

6. 設問の内容を入力します。

← アンケートの追加 保存

1 / 5 個

資産権即ルール.pptx ×

+ここに設問を追加

設問1 回答必須

デバイス管理情報を元に設問を作成

対象項目
デバイス管理名 ▼

設問
デバイス管理名 回答の形式
自由回答（テキスト記述） ▼

説明
ご自身の使命を入力してください。

↑ ↓

+ここに設問を追加

回答必須

チェックすると、回答必須の設問にできます。

デバイス管理情報を元に設問を作成

チェックすると、デバイス管理情報の項目をアンケートの設問に設定できます。表示された「対象項目」で選択します。

設問

設問を入力します。[デバイス管理情報の項目を元に設問を作成] をチェックした場合、「対象項目」で選択したデバイス管理情報の項目が自動入力されます。

説明

設問に説明が必要なときに入力します。

回答の形式

[デバイス管理情報の項目を元に設問を作成] をチェックした場合、設定できる回答形式は対象のデバイス管理情報の項目によって異なります。

- ツリー選択

管理コンソールで設定されている「グループ」情報を、デバイス使用者がツリーから選択します。[デバイス管理情報を元に設問を作成] をチェックし、対象項目を [デバイスグループ] を選択した場合に表示されます。

設問1 ☑ 回答必須

デバイス管理情報を元に設問を作成 ?

対象項目
デバイスグループ

設問
デバイスグループ

回答の形式
ツリーから選択

説明

↑ ↓ 🗑️

- 自由回答（テキスト記述）

デバイス使用者が自由に文字入力を行います。

- 日付選択

デバイス使用者が日付を選択します。

- 選択肢から回答

管理者が設定した選択肢をデバイス使用者が選択します。

7. さらに設問を追加する場合、[ここに設問を追加] をクリックします。

設定できる設問は、最大 10 件です。設問を複数設定した場合、[↑][↓] をクリックすると、設問の順番を変更できます。

8. [保存] をクリックします。

→ アンケートが追加されます。

メッセージ/アンケートの編集

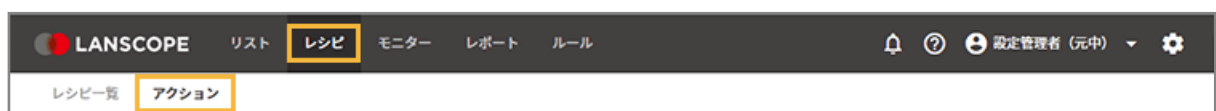
デバイスに配信前のメッセージ/アンケートは編集できます。ここでは、メッセージの編集を例に説明します。

注意

次のメッセージ/アンケートは、編集できません。

- デバイ스에 配信済み
- 레시피의 액션에 設定済み

1. [レシピ] の [アクション] をクリックします。



2. [メッセージを設定する] をクリックします。

アクションを選択してください

	IOS	Android	Windows	macOS
プロファイルを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
アプリを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
プロビジョニングプロファイルを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VPP アプリを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
メッセージを設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
アンケートを設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
操作ログを一括で出力する	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
位置情報を一括で出力する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>

3. メッセージを選択します。

← メッセージ配信

🔍 キーワード検索 (例: 営業 iPhone) ⓘ

メッセージの追加 ↻

<input type="checkbox"/>	件名	添付ファイル数	配信台数	未読台数	最終更新者	最終更新日時
<input type="checkbox"/>	【お知らせ】iOSのアップデートについて	0 個	17 台	7 台	設定管理者 (元中)	2018/04/10 1:
<input type="checkbox"/>	スマートデバイスの利用に関して	1 個	51 台	12 台	設定管理者 (元中)	2018/04/10 1:

20 ▾ 1-2件 / 全2件 |< < 1 > >|

4. [メッセージの内容] をクリックし、[編集] をクリックします。



5. 内容を編集し、[保存] をクリックします。



→ 編集内容が保存されます。

6. [閉じる] をクリックします。

ステップ2： メッセージ/アンケートを配信する

ここでは、任意のタイミングでメッセージを配信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. 次のように設定し、[アクション追加] をクリックします。

項目	値
レシピ名	任意のレシピ名
トリガー	[任意のタイミングで実行する]
デバイスグループ	配信するデバイスグループまたはデバイス
デバイス	

新しいレシピを作成

レシピ名*
 iOSのアップデートについて

レシピのトリガーを選択 トリガー選択

トリガー*
 任意のタイミングで実行する

レシピを実行する対象の絞り込み

- デバイスグループ (0 件)
選択
- デバイス (0 台)
選択

実行するアクション アクション追加

4. [メッセージを配信する] をクリックします。

アンケートの場合、[アンケートを配信する] をクリックします。

アクションを選択してください

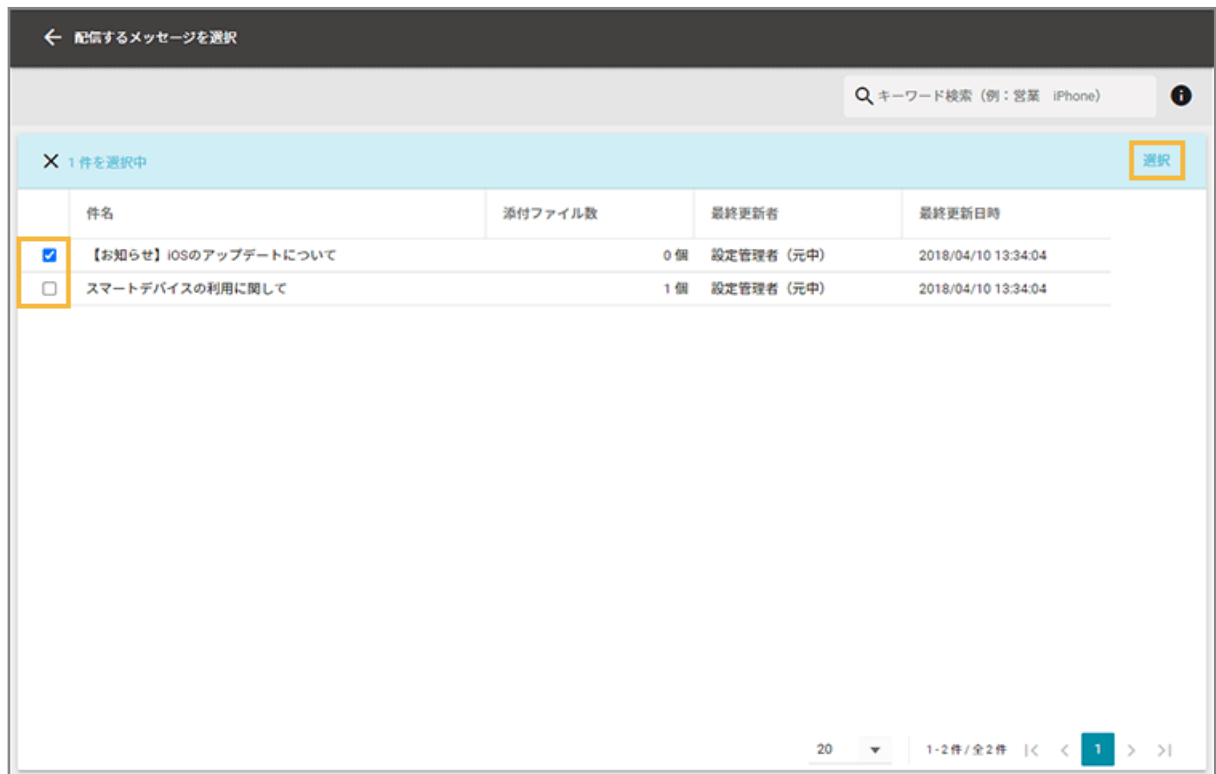
	iOS	Android	Windows	macOS
管理者にメールでお知らせする	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定プロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
指定アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
指定プロビジョニングプロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
指定 VPP アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
メッセージを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
アンケートを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
アラートに設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
アラートレポートを送信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定プロファイルを取り除く	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

5. メッセージをチェックし、[選択] をクリックします。

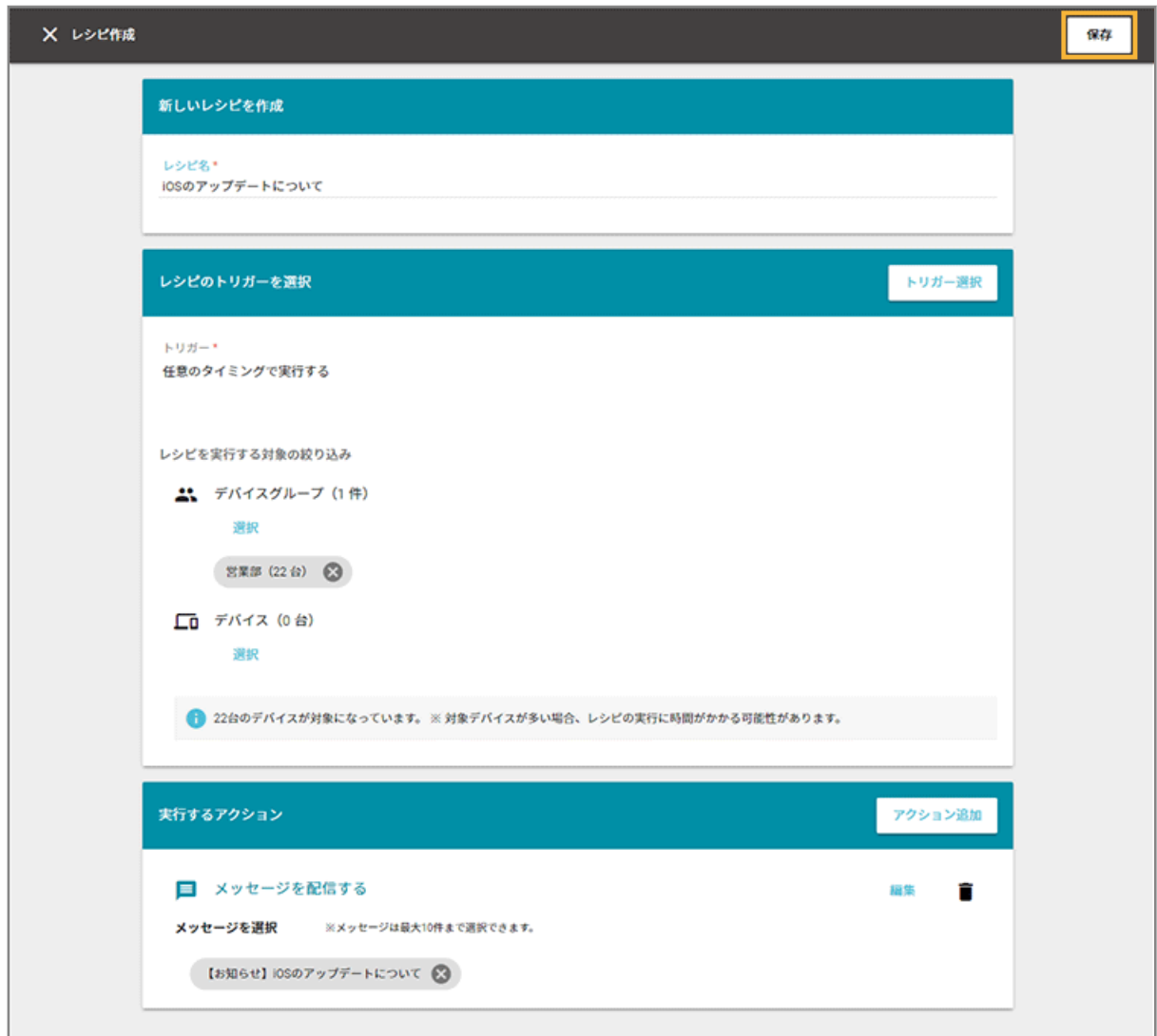
メッセージは、最大 10 件選択できます。

注意

他のレシピに設定されているメッセージ/アンケートは選択できません。



6. 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。

デバイス側での操作

iOS

Android

Windows

メッセージ/アンケートの受信通知設定をし、メッセージ/アンケートを確認します。

■ デバイス側で受信通知設定をする

メッセージ/アンケートを配信したときに、デバイス側でメッセージ/アンケートの受信が分かるように通知設定ができます。

iOS の場合

デバイスの [設定] > [通知] > [LANSCOPE] で、通知設定ができます。

ここでは、iOS 15 を例に説明します。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

デバイスの位置情報サービスがオフ、または LANSCOPE Client が終了している場合、バッジの表示は更新されません。

1. [LANSCOPE Client] をタップします。



2. iOS デバイスの設定により、次のように通知されます。

通知設定	表示		
	<p>App アイコンにバッジを表示</p>		
	<p>ロック画面に表示</p>	<p>履歴に表示</p>	<p>バナーとして表示</p>



Android の場合

ここでは、Android 11 を例に説明します。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。

ステップ：

1. [「LANSCOPE Client」の通知設定をする](#)
2. [ロック画面の通知設定をする](#)

ステップ 1： 「LANSCOPE Client」の通知設定をする

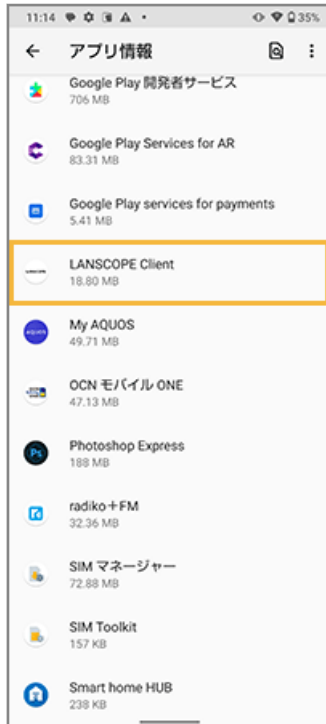
1. [設定] アプリをタップし、[アプリと通知] をタップします。



2. [アプリをすべて表示] をタップします。



3. [LANSCOPE Client] をタップします。



4. [通知] をタップします。



5. 通知をオンにします。



→ 通知設定が完了します。

ステップ2： ロック画面の通知設定をする

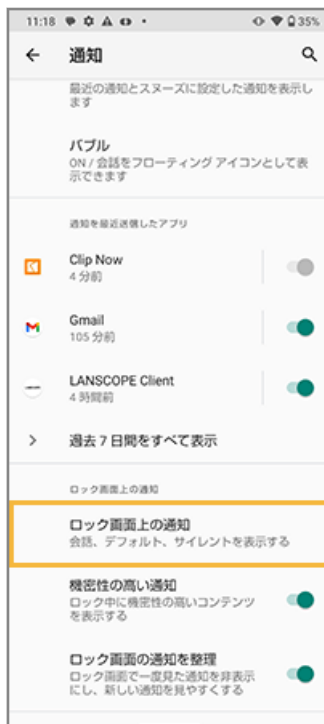
1. [設定] アプリをタップし、[アプリと通知] をタップします。



2. [通知] をタップします。



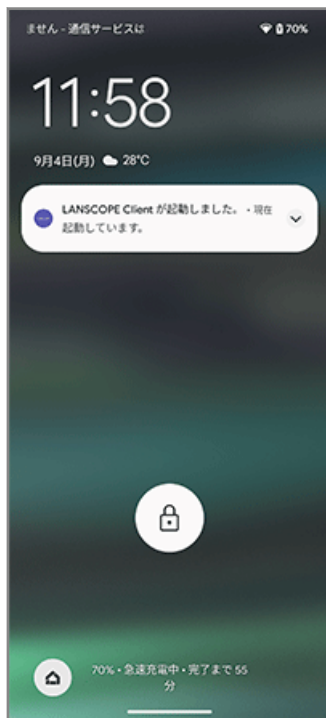
3. [ロック画面上の通知] をタップします。



4. [会議、デフォルト、サイレントを表示する] をタップします。



5. ロック画面に通知が表示されます。



→ ロック画面の通知設定が完了します。

Windows の場合

通知領域の上にメッセージが表示されます。設定は必要ありません。

未読のメッセージや未回答のアンケートがある場合、LANSCOPE Client 起動時、または 12 時間ごとに通知が再表示されます。



■ デバイスでメッセージ/アンケートを確認する

配信したメッセージやアンケートは、デバイスの LANSCOPE Client で確認できます。

1 度回答したアンケートに対して、再度回答することもできます。

iOS/Android の場合

1. LANSCOPE Client をタップします。



2. 画面下部の [メッセージ・アンケート] をタップし、確認したいメッセージやアンケートをタップします。



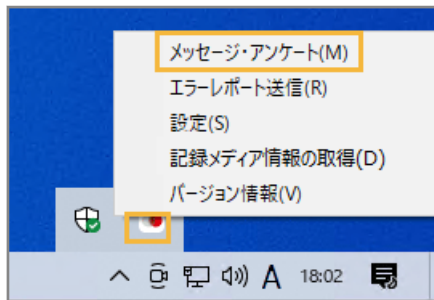
3. アンケートの場合、[次へ] をタップし、質問を確認します。

添付ファイルがある場合、本文下のリンクをタップし、ダウンロードできます。



Windows の場合

1. デスクトップを表示し、タスクバーの通知領域にある LANSCOPE Client のアイコンを右クリックし、[メッセージ・アンケート] をクリックします。



2. 確認するメッセージやアンケートをクリックします。

3. アンケートの場合、[次へ] をクリックし、質問を確認します。

添付ファイルがある場合、本文下のリンクをタップし、ダウンロードできます。

メッセージ/アンケートの配信結果を確認する

iOS

Android

Windows

ここでは、メッセージを例に説明します。

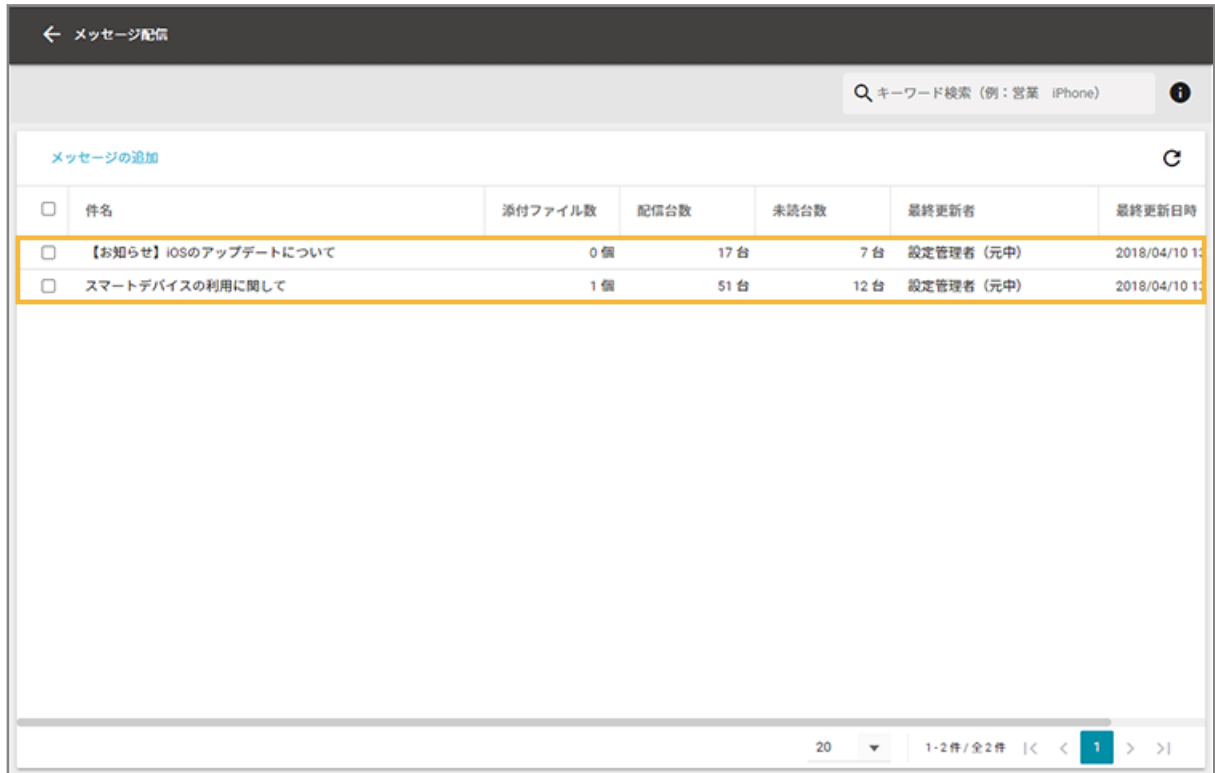
1. [レシピ] の [アクション] をクリックします。



2. [メッセージを設定する] をクリックします。



3. メッセージをクリックします。



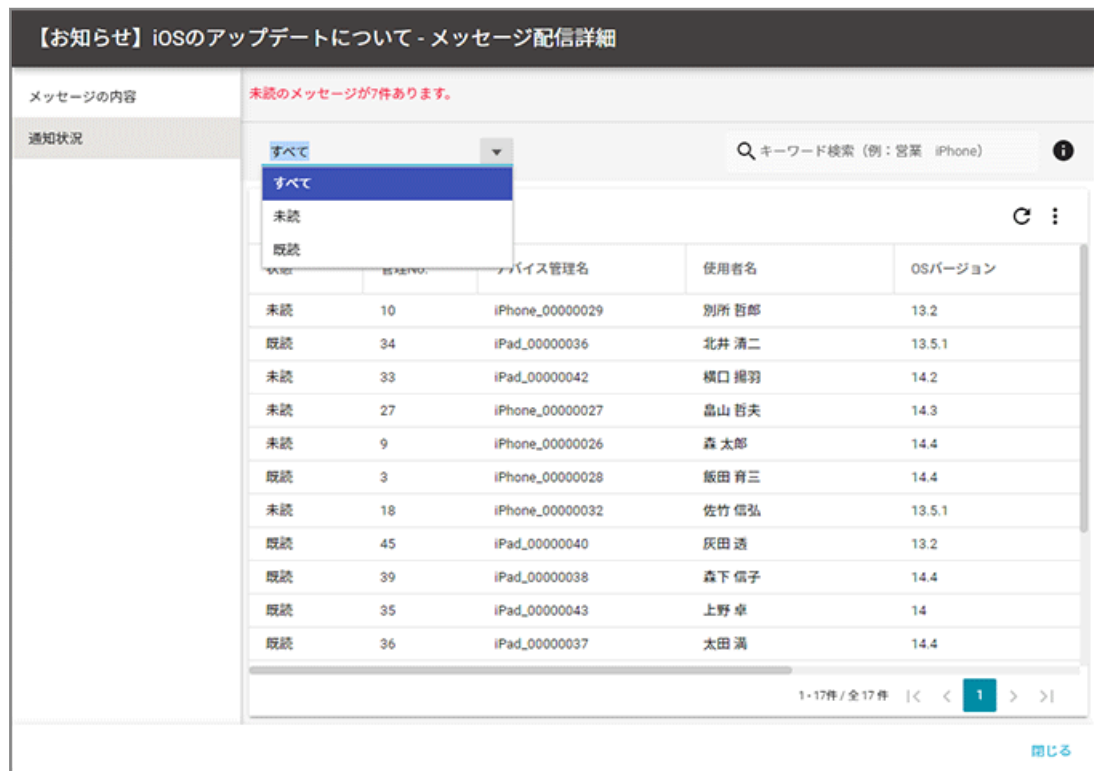
4. [通知状況] をクリックします。



5. 配信結果を確認します。

- メッセージの場合

「すべて」「未読」「既読」から選択し、ステータスごとに確認できます。



状態

- 未読
デバイスでメッセージを未開封で、確認していない状態のときに表示されます。
- 既読
デバイスでメッセージを開封済みで、確認した状態のときに表示されます。

管理 No.

配信されたデバイスの管理 No.が表示されます。

デバイス管理名

配信されたデバイスのデバイス管理名が表示されます。

ユーザー名

配信されたデバイスのユーザー名が表示されます。

配信日時

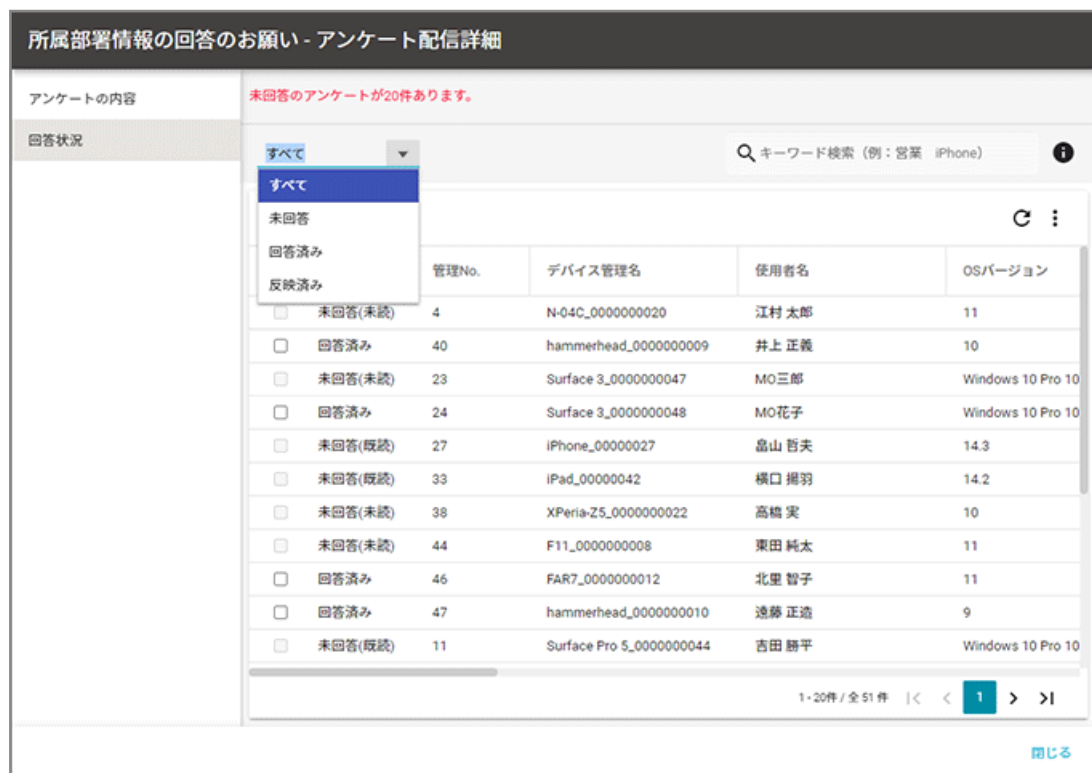
メッセージを配信した日時が表示されます。

確認日時

「状態」が「既読」の場合、デバイスからメッセージを開いた日時が表示されます。「状態」が「未読」の場合、空欄です。

- アンケートの場合

「すべて」「未回答」「回答済み」「反映済み」から選択し、ステータスごとに確認できます。



状態

- 未回答（未読）

デバイスでアンケートを未開封で、確認していない状態のときに表示されます。
- 未回答（既読）

デバイスでアンケートを開封済みで、回答を送信していない状態のときに表示されます。
- 回答済み

デバイスでアンケートの回答を送信した状態のときに表示されます。
- 反映済み

アンケートの回答をデバイス情報に反映済みの状態のときに表示されます。

管理 No.

配信されたデバイスの管理 No.が表示されます。

デバイス管理名

配信されたデバイスのデバイス管理名が表示されます。

使用者名

配信されたデバイスの使用者名が表示されます。

(アンケート本文)

「状態」が「回答済み」の場合、各設問に対する回答が表示されます。「状態」が「未回答」の場合、空欄です。

ポイント

1度回答したアンケートに対して、デバイスから再度回答を送信した場合、回答内容は上書きされません。

配信日時

アンケートを配信した日時が表示されます。

回答日時

「状態」が「回答済み」の場合、デバイスからアンケートの回答を送信した日時が表示されます。「状態」が「未回答」の場合、空欄です。

アンケートの回答内容を資産情報に反映する

iOS

Android

Windows

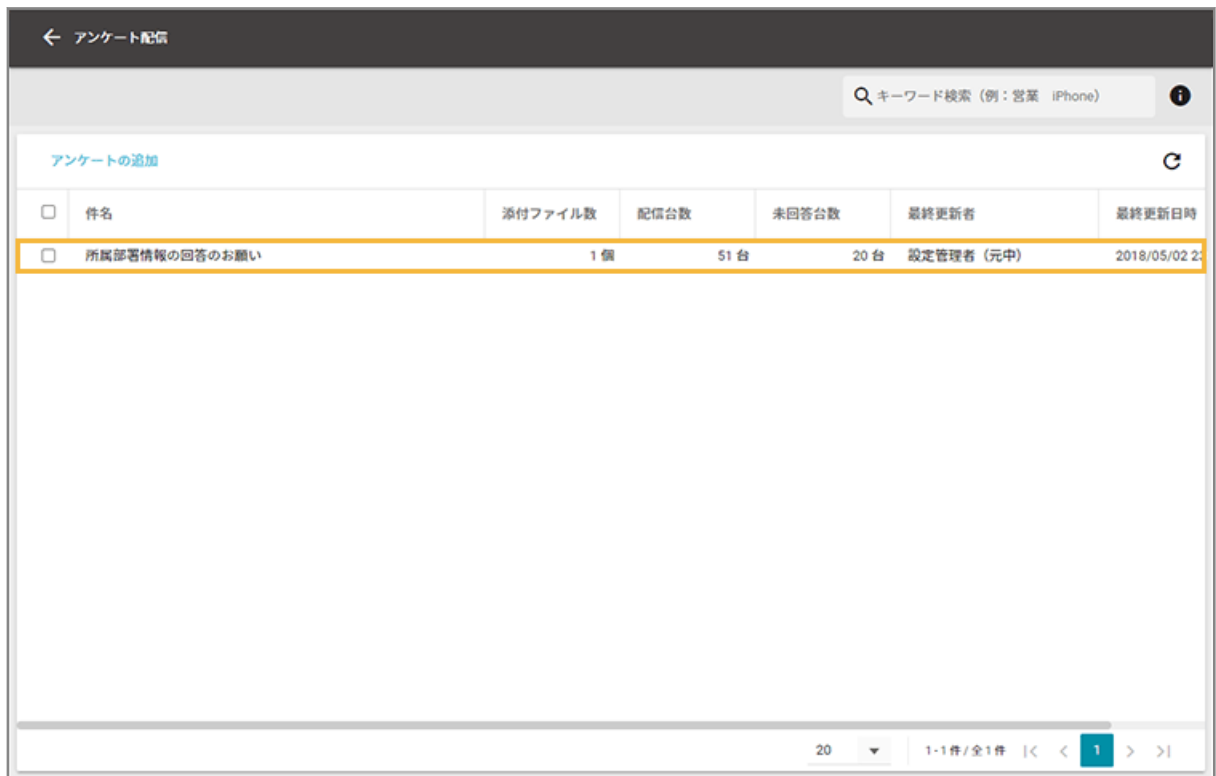
1. [レシピ] の [アクション] をクリックします。



2. [アンケートを設定する] をクリックします。



3. アンケートをクリックします。



4. [回答状況] をクリックします。



5. 回答内容に不備があった場合は、編集します。

(1) デバイスをクリックします。

所属部署情報の回答のお願い - アンケート配信詳細

アンケートの内容 未回答のアンケートが20件あります。

回答状況 回答済み

キーワード検索 (例: 営業 iPhone)

<input type="checkbox"/>	状態	管理No.	デバイス管理名	使用者名	OSバージョン
<input type="checkbox"/>	回答済み	40	hammerhead_0000000009	井上 正義	10
<input type="checkbox"/>	回答済み	24	Surface3_0000000048	MO花子	Windows 10 Pro 10
<input type="checkbox"/>	回答済み	46	FAR7_0000000012	北里 智子	11
<input type="checkbox"/>	回答済み	47	hammerhead_0000000010	速藤 正造	9
<input type="checkbox"/>	回答済み	29	ElitePad_0000000052	共有タブレット	Windows 10 Home
<input type="checkbox"/>	回答済み	26	Surface3_0000000050	MO一郎	Windows 10 Pro 10
<input type="checkbox"/>	回答済み	31	FAR7_0000000004	共有タブレット (システム部...	9
<input type="checkbox"/>	回答済み	35	iPad_0000000043	上野 卓	14
<input type="checkbox"/>	回答済み	10	iPhone_0000000029	別所 哲郎	13.2
<input type="checkbox"/>	回答済み	37	SC-03D_0000000005	青山 秀則	9
<input type="checkbox"/>	回答済み	42	404KC_0000000001	中川 ゆうこ	11

1 - 20件 / 全31件

閉じる

(2) [編集] をクリックします。

iOS iPhone_00000033 - アンケート回答詳細 管理No. 19

デバイスグループ	使用者名	電話番号	Apple ID	最終稼働
営業2課	石川 忍	080xxxxxxx	-	1日前

編集

設問1 デバイス管理名
石川 忍 iPhone_00000033

設問2 デバイスグループ
営業2課

設問3 選択肢から回答
選に1回

閉じる

(3) アンケート内容を修正し、[保存] をクリックします。

デバイスグループ	使用者名	電話番号	Apple ID	最終稼働
営業2課	石川 忍	080xxxxxxxx	-	1日前

キャンセル 保存

設定1 デバイス管理名 *
石川 忍 iPhone_00000033

設定2 デバイスグループ *
営業2課

設定3 選択肢から回答
週に1回

閉じる

→ アンケート回答が修正されます。

6. デバイスをチェックし、[資産情報に反映] をクリックします。

所属部署情報の回答のお願い - アンケート配信詳細

アンケートの内容 未回答のアンケートが20件あります。

回答状況 回答済み キーワード検索 (例: 営業 iPhone)

× 20件を選択中 資産情報に反映

<input checked="" type="checkbox"/>	状態	管理No.	デバイス管理名	使用者名	OSバージョン
<input checked="" type="checkbox"/>	回答済み	40	hammerhead_0000000009	井上 正義	10
<input checked="" type="checkbox"/>	回答済み	24	Surface_3_0000000048	MO花子	Windows 10 Pro 10
<input checked="" type="checkbox"/>	回答済み	46	FAR7_0000000012	北里 智子	11
<input checked="" type="checkbox"/>	回答済み	47	hammerhead_0000000010	逸藤 正造	9
<input checked="" type="checkbox"/>	回答済み	29	ElitePad_0000000052	共有タブレット	Windows 10 Home
<input checked="" type="checkbox"/>	回答済み	26	Surface_3_0000000050	MO一郎	Windows 10 Pro 10
<input checked="" type="checkbox"/>	回答済み	31	FAR7_0000000004	共有タブレット (システム部...	9
<input checked="" type="checkbox"/>	回答済み	35	iPad_0000000043	上野 卓	14
<input checked="" type="checkbox"/>	回答済み	10	iPhone_0000000029	別所 哲郎	13.2
<input checked="" type="checkbox"/>	回答済み	37	SC-03D_0000000005	青山 秀則	9
<input checked="" type="checkbox"/>	回答済み	42	404KC_0000000001	中川 ゆうこ	11

1 - 20件 / 全31件 | < > 1 > > | 閉じる

7. [OK] をクリックします。

資産情報の反映を実行します。よろしいですか？

キャンセル OK

→ 資産情報に反映されます。反映された情報は、[リスト] の「デバイス」画面で確認できます。

メッセージ/アンケートを削除する

iOS

Android

Windows

ここでは、メッセージの削除を例に説明します。

ポイント

- デバイスへ配信済みのメッセージ/アンケート、レシピに設定されているメッセージ/アンケートも削除できません。ただし、デバイスへ配信済みの場合、メッセージ/アンケート削除後は配信結果を確認できません。
- 管理コンソールでメッセージ/アンケートを削除すると、デバイスに配信されたメッセージ/アンケートも削除されます。

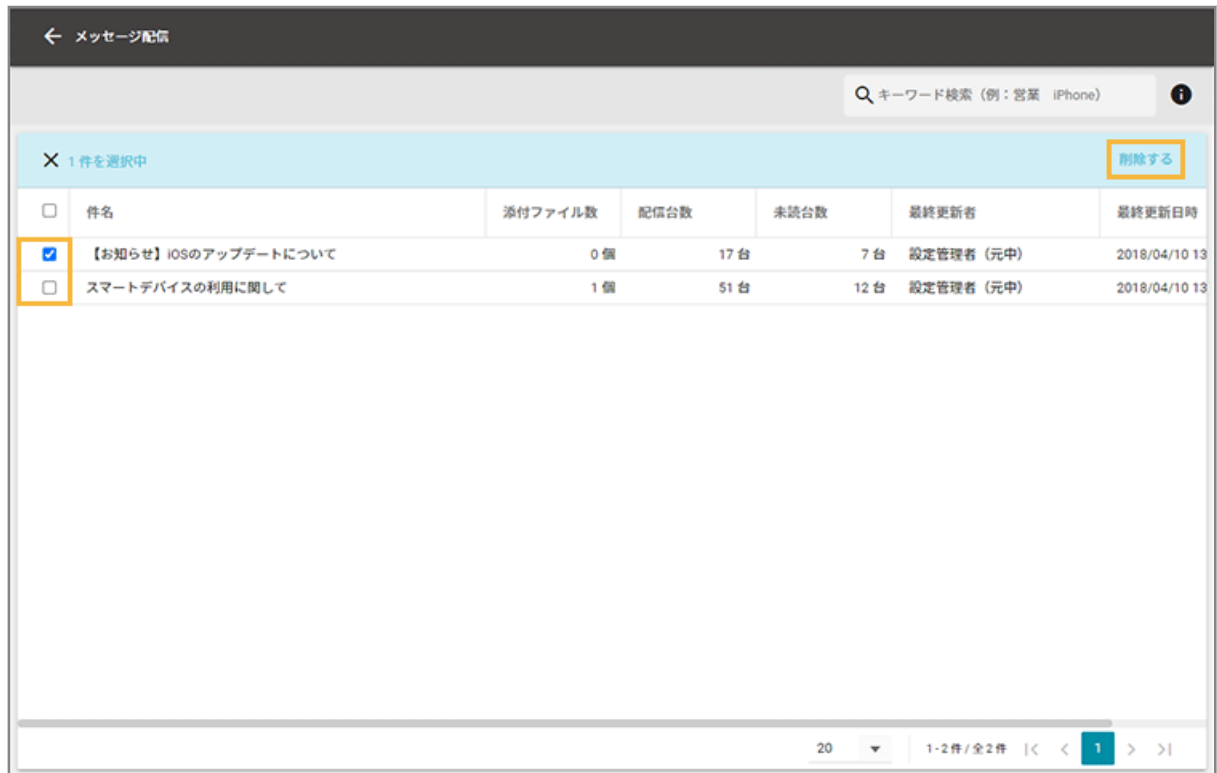
1. [レシピ] の [アクション] をクリックします。



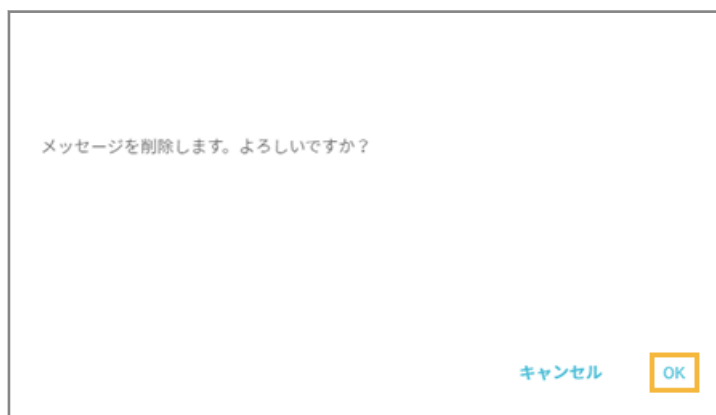
2. [メッセージを設定する] をクリックします。



3. メッセージをチェックし、[削除する] をクリックします。



4. [OK] をクリックします。



→ メッセージが削除されます。

アラートを設定する

iOS Android Windows macOS

アラート設定することで、ルールに抵触したデバイスを発見しやすくなります。デバイス使用者や管理者への通知もできます。

- [アラート設定の流れ](#)

アラート設定を作成し、アラート発生時にデバイス管理者へ通知する設定をします。

- [デバイスへの通知設定をする](#)

ルールに抵触した場合、デバイスに通知できます。

- [アラートを確認する](#)

アラートが発生しているデバイスや、アラート内容を確認できます。

アラート設定の流れ

iOS

Android

Windows

macOS

アラート設定を作成し、アラート発生時にデバイス管理者へ通知する設定をします。

ステップ：

1. [アラートを設定する](#)
2. [アラートレポートを送信する](#)

ステップ 1： アラートを設定する

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。登録済みのレシピも編集できます。

ポイント

- アラート設定では、「危険」「注意」「警告なし」のアラートレベルを設定できます。
- デバイスグループやデバイスごとにレベルを変更する場合、レベルごとのレシピを作成してください。

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。**

状態	レシピ名	トリガー	アクション
<input type="checkbox"/>	LANSCOPE Client を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定アプリを配信する
<input type="checkbox"/>	LANSCOPE の登録用 Clip を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定プロフィールを配信する
<input checked="" type="checkbox"/>	管理外アラート (iOS/Windows/macOS)	デバイスが管理外になっている	アラートに設定する
<input type="checkbox"/>	パスワードポリシー非準拠アラート (iOS/Android)	パスワードポリシーに準拠していない	アラートに設定する
<input type="checkbox"/>	LANSCOPE Client 未更新アラート (iOS/Android/Windows)	LANSCOPE Client のバージョンが最新になっていない	アラートに設定する
<input checked="" type="checkbox"/>	未稼働アラート (iOS/Android/Windows/macOS)	未稼働期間が指定された期間を超過している	アラートに設定する
<input type="checkbox"/>	空き容量不足アラート (iOS/Android/Windows/macOS)	空き容量が不足している	アラートに設定する
<input type="checkbox"/>	パスコードロックオフアラート (iOS)	パスコードロックの設定がオフになっている	アラートに設定する
<input type="checkbox"/>	リモート実行無効アラート (Android/Windows)	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	アラートに設定する
<input checked="" type="checkbox"/>	SIMカード抜き差しアラート (iOS/Android/Windows)	SIMカードが抜き差しされた	アラートに設定する
<input checked="" type="checkbox"/>	SDカード抜き差しアラート (Android)	SDカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>	新規アプリインストールアラート (Android)	新しくアプリがインストールされた	アラートに設定する
<input type="checkbox"/>	タイムゾーン変更アラート (Android)	タイムゾーンが変更された	アラートに設定する
<input type="checkbox"/>	新規プロフィールインストールアラート (iOS/macOS)	新しくプロフィールがインストールされた	アラートに設定する

3. 次のように設定し、[アクション追加] をクリックします。

項目	値
レシピ名	任意のレシピ名
トリガー	任意のトリガー
デバイスグループ	配信するデバイスグループまたはデバイス
デバイス	

新しいレシピを作成

レシピ名*

管理外アラート (iOS/Windows/macOS)

トリガー選択

トリガー*

デバイスが管理外になっている

レシピを実行する対象の絞り込み

デバイスグループ (0件)

選択

デバイス (0台)

選択

アクション追加

アラート設定できるトリガーは、次のとおりです。

カテゴリー	トリガー	詳細設定
デバイス情報	パスワードポリシーに準拠していない (*1)	[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。
	注意 Android Enterprise デバイスは非対応です。	
	デバイスが管理外になっている (*1)	—
	LANSCOPE Client のバージョンが最新になっていない (*1)	—
	未稼働期間が指定された期間を超過している (*1)	「レシピ作成」画面で、「未稼働期間 (日) (1 ~90 日)」を設定します。
	指定したアプリがインストールされている (*1)	<ul style="list-style-type: none"> ● [ルール] > [アプリ設定] で、アプリのレベル設定が必要です。 ● 「レシピ作成」画面で、指定アプリのアプリ管理レベルを設定します。
指定したアプリがインストールされていない (*1)		

カテゴリー	トリガー	詳細設定
	パスコードロックの設定がオフになっている (*1)	—
	デバイスが不正に改造されている (root化/Jailbreak) (*1)	—
	iOS のバージョンが指定した範囲外になっている (*1)	「レシピ作成」画面で、「OS バージョン (下限)」と「OS バージョン (上限)」を設定します。
	Android のバージョンが指定した範囲外になっている (*1)	
	SIM カードが抜き差しされた (*2)	—
	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 (*1)	—
	もうすぐリース切れになる (*1)	<ul style="list-style-type: none"> 各デバイス情報「期限 (リース/償却)」の登録が必要です。 「レシピ作成」画面で、「リース期限 (日) (0~365 日)」を設定します。
	ログが取得されない設定になっている (*1)	—
	空き容量が不足している (*1)	「レシピ作成」画面で、「空き容量 (%) (1~100%)」を設定します。
	新規プロファイルがインストールされた (*2)	—
操作ログ情報	新しくアプリがインストールされた (*2)	—
	指定したアプリが実行された (*2)	<ul style="list-style-type: none"> [ルール] > [アプリ設定] で、アプリのレベル設定が必要です。 「レシピ作成」画面で、指定アプリのアプリ管理レベルを設定します。
	SD カードが抜き差しされた (*2)	—
	タイムゾーンが変更された (*2)	—
位置情報	位置情報が取得されない設定になっている (*1)	—

*1 : アラートが検知されると期限なく表示されます。アラートが解消されると、1 日以内に非表示になります。

*2 : アラートが検知されてから 7 日間表示されます。

4. [アラートに設定する] をクリックします。



5. 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。



6. 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。

ステップ 2： アラートレポートを送信する

アラートが発生したデバイス数を記載したアラートレポート（メール）を、定期的にデバイス管理者へ送信できます。

アラートレポート（メール）のサンプル

LANSCOPE のアラートレポートを通知します。

詳細は LANSCOPE のアラートで確認できます。

<https://motex-cloud.lanscopean.com/#/list/alerts>

※以下の情報はメール送信時の情報です。アラートの情報は随時更新されるため、内容に差異がある場合がございます。

設定者: MO 太郎

通知対象: [危険] 警告と [注意] 警告を通知

対象部署: ネットワーク全体

通知条件: 警告がない場合も通知

 集計日: 20xx/04/17

危険警告発生台数: 4 / 16 台

注意警告発生台数: 2 / 8 台

【危険】

- ・デバイスが管理外になっている: 4 台

【注意】

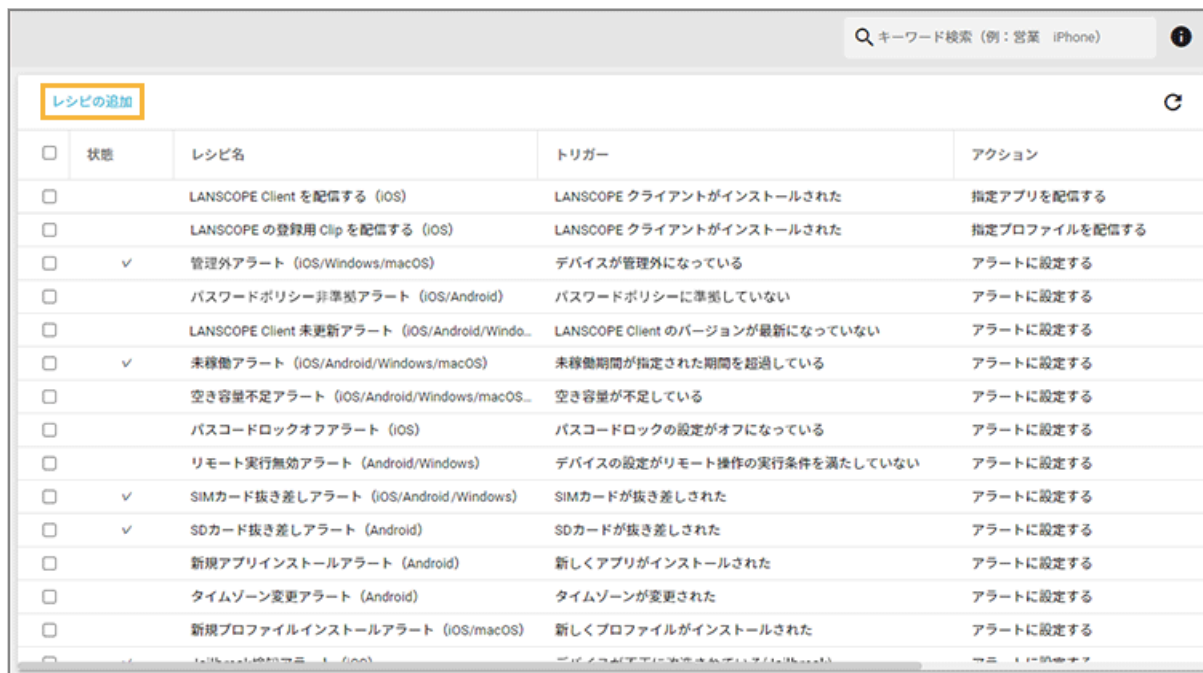
- ・LANSCOPE Client のバージョンが最新になっていない: 2 台

 ※このメールは配信専用です。返信はできませんのでご了承ください。

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. 次のように設定し、[アクション追加] をクリックします。

項目	値
レシピ名	任意のレシピ名
トリガー	[定期的に行う] を選択し、実行タイミングを設定 いますぐアラートレポートを送信するときは、[任意のタイミングで 実行する]
デバイスグループ	配信するデバイスグループまたはデバイス
デバイス	

新しいレシピを作成

レシピ名 *

アラートレポートの送信

レシピのトリガーを選択 トリガー選択


トリガー *


定期的に行う

周期
毎日 ▼

時刻
00 ▼ : 00 ▼

レシピを実行する対象の絞り込み

 デバイスグループ (0 件)
選択

 デバイス (0 台)
選択

実行するアクション アクション追加

4. [アラートレポートを送信する] をクリックします。

アクションを選択してください

	IOS	Android	Windows	macOS
管理者にメールでお知らせする	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定プロファイルを配信する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
指定アプリを配信する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
指定プロビジョニングプロファイルを配信する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
指定 VPP アプリを配信する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
メッセージを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
アンケートを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
アラートに設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
アラートレポートを送信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定プロファイルを取り除く	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>

5. 項目を設定し、[設定] をクリックします。

アラートレポートを設定してください

警告種別*

危険と注意 危険のみ

送信先メールアドレス +

1 / 10 個*

アラートがない場合でもアラートレポートを送信する

送信する

デバイスごとのアラート詳細をメールに添付する

添付する

設定

警告種別

通知する警告種別を「危険と注意」「危険のみ」から選択します。

送信先メールアドレス

送信先メールアドレスを入力し、[+] をクリックします。送信先メールアドレスは、10 個まで設定できます。

アラートがない場合でもアラートレポートを送信する

チェックすると、アラートがない場合でもアラートレポートが送信されます。

デバイスごとのアラート詳細をアラートメールに添付する

チェックすると、デバイスごとのアラート詳細ファイルが添付されます。

6. 内容を確認し、[保存] をクリックします。

× レシピ作成 保存

新しいレシピを作成

レシピ名*
アラートレポートの送信

レシピのトリガーを選択 トリガー選択

トリガー*
定期的に行う

周期
毎日

時刻
00 : 00

レシピを実行する対象の絞り込み

👤 デバイスグループ (1件)
選択
営業部 (22台) ✕

📱 デバイス (0台)
選択

ⓘ 22台のデバイスが対象になっています。 ※ 対象デバイスが多い場合、レシピの実行に時間がかかる可能性があります。

実行するアクション アクション追加

⚠️ アラートレポートを送信する 編集 🗑️

警告種別
危険と注意


送信先メールアドレス
1 / 10 個
hara.h.k@nissai.com

アラートがない場合でもアラートレポートを送信する
送信する



デバイスごとのアラート詳細を添付する
添付する

→ レシピが作成されます。

トリガーで「任意のタイミングで実行する」を選択した場合、次の操作でレシピを実行します。

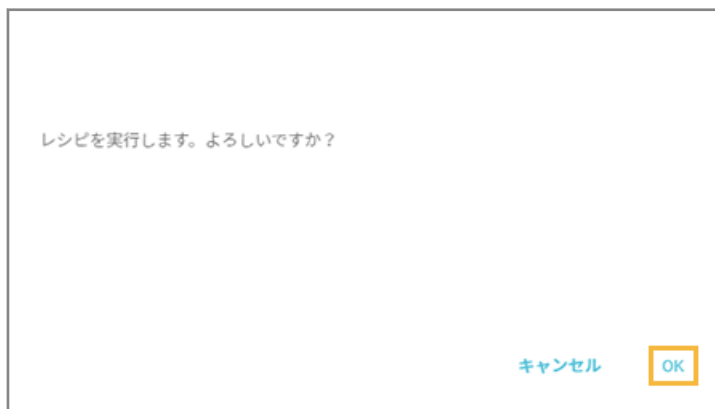
1. 「レシपी一覧」画面で作成したレシピを選択し、 をクリックします。

ポイント

レシピが無効の状態では、 は表示されません。「このレシピを有効にする」を  (有効) にしてください。



2. [OK] をクリックします。



デバイスへの通知設定をする

Android

ルールに抵触した場合、デバイスに通知できます。

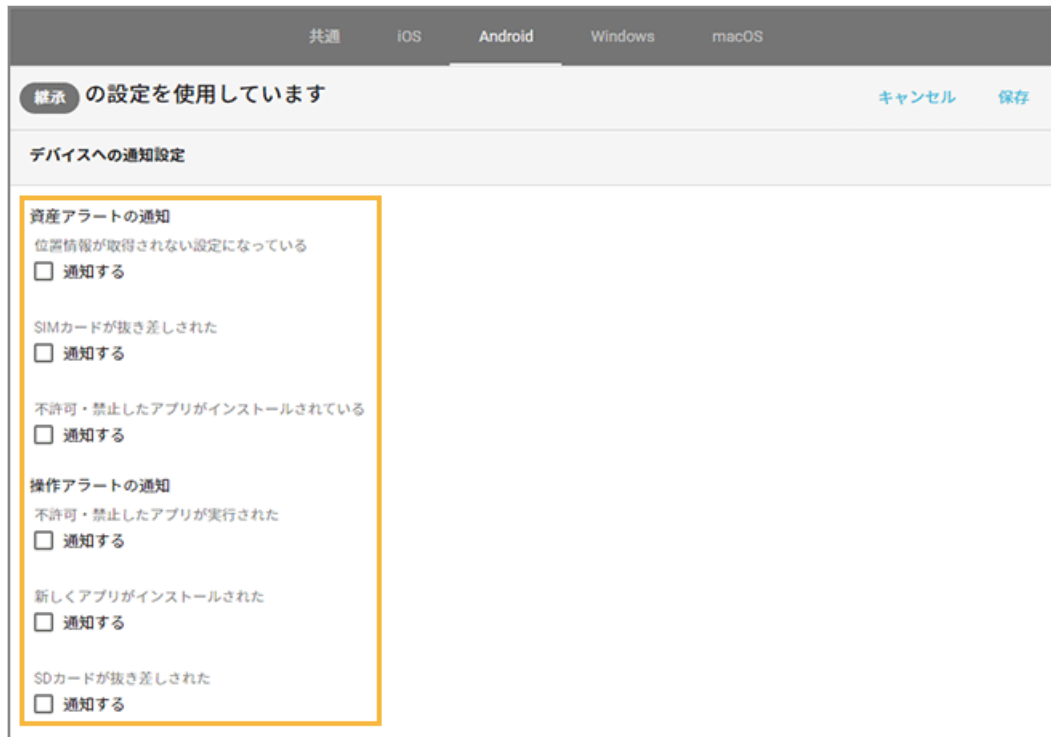
1. [ルール] の [デバイス設定] > [基本設定] をクリックします。



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



3. 「デバイスへの通知設定」で、デバイスへ通知する項目をチェックします。



資産アラートの通知

- 位置情報が取得されない設定になっている
資産情報取得タイミングで、位置情報の設定がオフになっている、またはオンになっていても高精度モード以外の設定になっている場合に通知します。
- SIM カードが抜き差しされた
資産情報取得タイミングで、SIM カードの情報が変更になった場合に通知します。
- 不許可・禁止したアプリがインストールされている
資産情報取得タイミングで、不許可・禁止設定されたアプリがインストールされている場合に通知しません。

操作アラートの通知

- 不許可・禁止したアプリが実行された
デバイスで、不許可・禁止アプリを起動したタイミングで通知します。
- 新しくアプリがインストールされた
デバイスで、新しくアプリをインストールしたタイミングで通知します。
- SD カードが抜き差しされた
デバイスで、SD カードを抜き差ししたタイミングで通知します。

4. [保存] をクリックします。

■ デバイスの通知画面

デバイスへの通知設定では、次のアラート画面が表示されます。

資産アラートの通知

項目	画面表示
位置情報が取得されない設定になっている	 <p>資産アラート</p> <p>以下の資産アラートを検知しました。 ・位置情報無効 GPS / Wi-Fi・モバイルネットワークのデータを使用した位置情報設定が無効になっています。</p>
SIM カードが抜き差しされた	 <p>資産アラート</p> <p>以下の資産アラートを検知しました。 ・SIMカード変更（電話番号が変更されました）</p>
不許可・禁止したアプリがインストールされている	 <p>資産アラート</p> <p>以下の資産アラートを検知しました。 ・不許可・禁止アプリインストール YouTube</p>

操作アラートの通知

項目	画面表示
不許可・禁止したアプリが実行された	 <p>不許可アプリ起動アラート</p> <p>不許可アプリの起動を検知しました。 Chrome</p>
新しくアプリがインストールされた	 <p>新規アプリインストールアラート</p> <p>新規アプリインストールを検知しました。</p>
SD カードが抜き差しされた	 <p>SDカード抜き差しアラート</p> <p>SDカードの抜き差しを検知しました。</p>

アラートを確認する

iOS

Android

Windows

macOS

アラートが発生しているデバイスや、アラート内容を確認できます。

■ 「デバイス」画面で確認する

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。

<input type="checkbox"/>	↑ 管理...	デバイスグループ	デバイス管理名	ユーザー名	OSタイプ	OSバージョン
<input type="checkbox"/>	1	総務課	SC-03D_0000000014	江藤 花子	Android	9
<input type="checkbox"/>	2	総務課	hammerhead_00000000...	六角 富夫	Android	10
<input type="checkbox"/>	3	営業1課	iPhone_0000000028	飯田 育三	iOS	14.4
<input type="checkbox"/>	4	人事課	N-04C_0000000020	江村 太郎	Android	11
<input type="checkbox"/>	5	営業部	EB-A71GJ_0000000019	橋中 栄一郎	Android	11
<input type="checkbox"/>	6	営業部	L-22D_0000000016	内田 健太	Android	11
<input type="checkbox"/>	7	営業1課	404KC_0000000023	中田 真由美	Android	10
<input type="checkbox"/>	8	営業1課	picasso_aapcu56jp_000...	橋 秀雄	Android	11
<input type="checkbox"/>	9	総務課	iPhone_0000000026	森 太郎	iOS	14.4
<input type="checkbox"/>	10	営業1課	iPhone_0000000029	別所 哲郎	iOS	13.2
<input type="checkbox"/>	11	営業1課	Surface Pro 5_00000000...	吉田 勝平	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	12	営業1課	Surface Pro 5_00000000...	加藤 信也	Windows	Windows 10 Pro 10.0.17134
<input type="checkbox"/>	13	営業1課	404KC_0000000023	石井 健二	Android	9

3. [アラート] をクリックし、アラート情報を確認します。



■ 「アラート」画面で確認する

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。

発生していないアラートは表示しない

警告レベル	アラート	アラート台数
危険	未稼働期間が指定された期間を超過している	5台
注意	空き容量が不足している	2台
危険	パスコードロックの設定がオフになっている	4台
危険	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	3台
注意	SIMカードが抜き差しされた	2台
注意	iOSのバージョンが指定した範囲外になっている	2台
注意	もうすぐリース切れになる	1台
危険	SDカードが抜き差しされた	1台
危険	指定したアプリが実行された	1台
危険	新しくアプリがインストールされた	1台
危険	位置情報が取得されない設定になっている	1台
注意	LANSCOPE Client のバージョンが最新になっていない	1台

20 1-12件/全12件 < > 1 > >|

→ 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。

発生していないアラートは表示しない

警告レベル	アラート	アラート台数
危険	未稼働期間が指定された期間を超過している	5台
注意	空き容量が不足している	2台
危険	パスコードロックの設定がオフになっている	4台
危険	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	3台
注意	SIMカードが抜き差しされた	2台
注意	iOSのバージョンが指定した範囲外になっている	2台
注意	もうすぐリース切れになる	1台
危険	SDカードが抜き差しされた	1台
危険	指定したアプリが実行された	1台
危険	新しくアプリがインストールされた	1台
危険	位置情報が取得されない設定になっている	1台
注意	LANSCOPE Client のバージョンが最新になっていない	1台

20 1-12件/全12件 < > 1 > >|

未稼働期間が指定された期間... : ×

警告レベル: 危険

-  吉田 勝平 (Surface Pro 5_0000...)
営業1課
-  MO一郎 (Surface 3_000000005...)
営業2課
-  小林 智子 (HTC_ACE_00000000...)
サポート1課
-  北星 智子 (FAR7_0000000012...)
システム管理課
-  MO五郎 (MacBook_00000085...)
サポート2課

1-5件/全5件 < >

→ 「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。



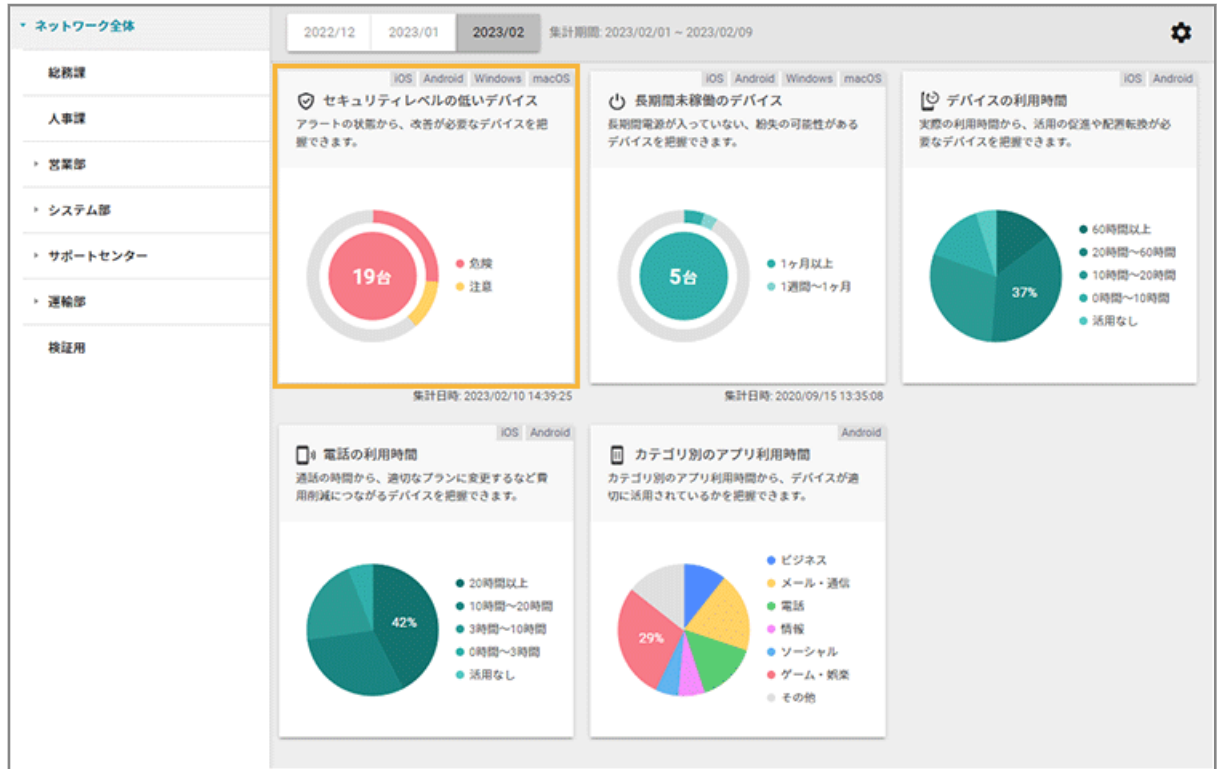
■ 「レポート」画面で確認する

1. [レポート] の [利用状況] をクリックします。



2. レポートをクリックします。

ここでは、例として「セキュリティレベルの低いデバイス」レポートをクリックします。



3. デバイスをクリックします。

セキュリティレベルの低いデバイス

アラートの状態から、改善が必要なデバイスを把握できます。

ネットワーク全体 集計日時: 2023/03/23 09:28:47

19台

- 危険 (13)
- 注意 (6)

配下のグループ

管理No.	デバイス管理名	使用者名	セキュリティ警告レベル
82	MacBook_000000085	MO五郎	危険
49	HTC_ACE_0000000006	小林 智子	危険
48	volantis_0000000025	武田 郁恵	危険
39	iPad_000000038	森下 信子	危険
32	iPad_000000035	細川 孝信	危険
27	iPhone_000000027	畠山 哲夫	危険
24	Surface 3_0000000048	MO花子	危険
20	Surface 3_0000000054	石川 忍	危険
19	iPhone_000000033	石川 忍	危険
18	iPhone_000000032	佐竹 信弘	危険
14	404KC_0000000018	平尾 晋作	危険
9	iPhone_000000026	森 太郎	危険
6	L-22D_0000000016	内田 健太	危険
43	iPad_000000039	山岡 節女	注意

4. アラート情報を確認します。



操作ログ／位置情報を一括出力する

iOS Android Windows

取得した操作ログ／位置情報を一括出力できます。

- [一括出力設定の流れ](#)

取得した操作ログ／位置情報を、アクションで出力設定し、レシピで出力データを作成できます。

- [出力データをダウンロードする](#)

作成した出力データをダウンロードします。

操作ログ／位置情報の出力項目

ログ	出力項目
操作ログ	管理 No./デバイスグループ/使用者名/デバイス管理名/日時/分類/利用時間/内容 /詳細 1/詳細 2/アラート/時差
位置情報	管理 No./デバイスグループ/使用者名/デバイス管理名/日時/住所/取得タイプ/ LANSCOPE Client 状態/緯度/経度/時差

一括出力設定の流れ

iOS Android Windows

取得した操作ログ／位置情報を、アクションで出力設定し、レシピで出力データを作成できます。

ステップ：

1. [出力設定をする](#)
2. [出力データを作成する](#)

ステップ 1： 出力設定をする

出力設定は、アクションで設定します。ここでは、取得した位置情報の出力内容を設定します。

1. **【レシピ】の【アクション】をクリックします。**



2. **【位置情報を一括で出力する】をクリックします。**



3. **【設定の追加】をクリックします。**

<input type="checkbox"/>	設定名	出力期間	更新者	更新日時
<input type="checkbox"/>	位置情報ログ一括出力 (当月)	当月	設定管理者 (元中)	2018/06/14 13:12:25

4. 出力内容を設定します。

出力する内容を設定してください ⓘ

設定名 *

出力期間
 前月 当月 期間指定 2023/02/01 ~ 2023/03/23

メモ

設定名

設定名を入力します。

出力期間

「前月」「当月」「期間設定」から選択します。「期間設定」で指定できる期間は、最長3か月です。

注意

- 直近のログを出力できるまでにはタイムラグがあります。数分経過したあとにアクションを実行してください。
- 当日の9時から12時までのログについては、12時の定期処理完了後に出力可能になります。13時以降にアクションを実行してください。

メモ

必要に応じて入力します。

5. [保存] をクリックします。

→ 出力設定が完了します。

ステップ2： 出力データを作成する

位置情報の一括出力は、レシピで設定できます。操作ログの一括出力も同様の手順です。

1. [レシピ] の [レシピー覧] をクリックします。



2. [レシピの追加] をクリックします。



3. 次のように設定し、[アクション追加] をクリックします。

項目	値
レシピ名	任意のレシピ名
トリガー	[定期的に実行する] を選択し、実行タイミングを設定 いますぐ出力データを作成するときは、[任意のタイミングで実行する]
デバイスグループ	配信するデバイスグループまたはデバイス
デバイス	

新しいレシピを作成

レシピ名*

営業部/位置情報出力 (1ヶ月)

レシピのトリガーを選択 トリガー選択

トリガー*

定期的に行う

周期
毎月

すべてチェック すべてはずす

日

1日 2日 3日 4日 5日 6日 7日 8日 9日 10日 11日

12日 13日 14日 15日 16日 17日 18日 19日 20日 21日 22日

23日 24日 25日 26日 27日 28日 29日 30日 31日

時刻
00 : 00

レシピを実行する対象の絞り込み

デバイスグループ (0件)
選択

デバイス (0台)
選択

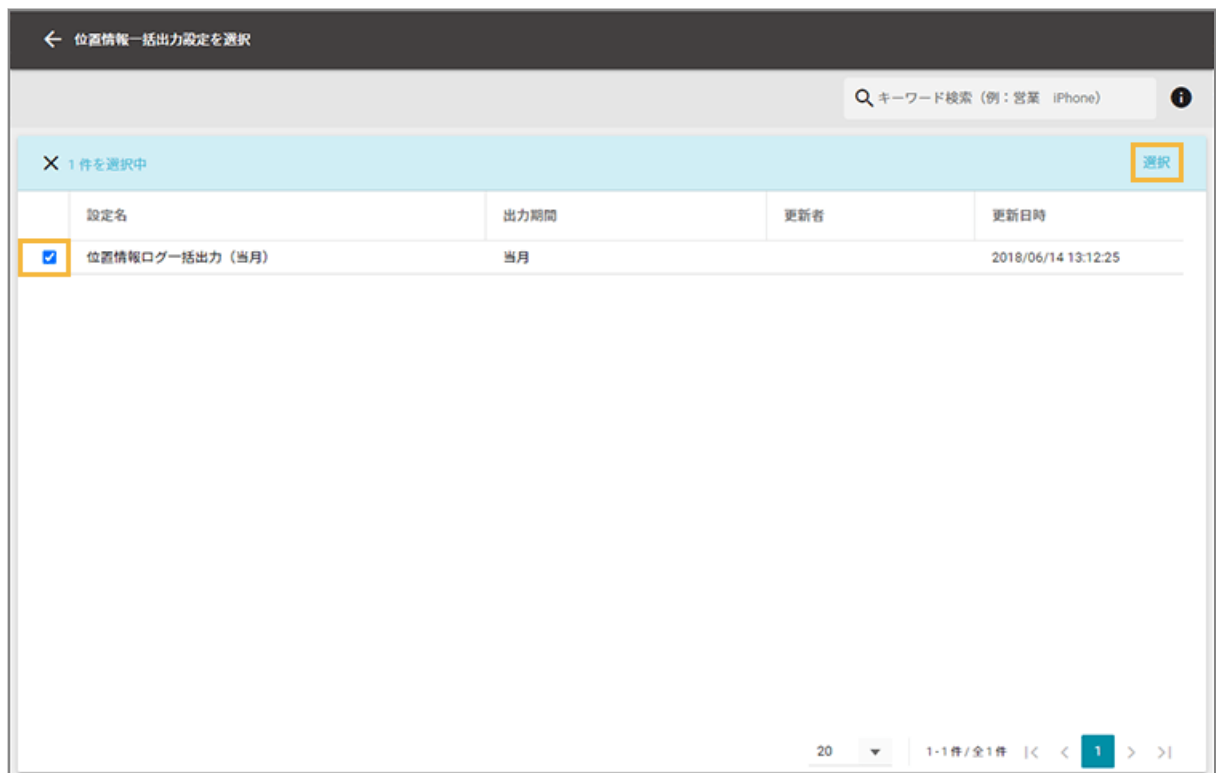
実行するアクション アクション追加

4. [位置情報を一括で出力する] をクリックします。



5. 出力設定をチェックし、[選択] をクリックします。


設定は最大 10 件選択できます。





6. 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。

トリガーで「任意のタイミングで実行する」を選択した場合、次の操作でレシピを実行します。

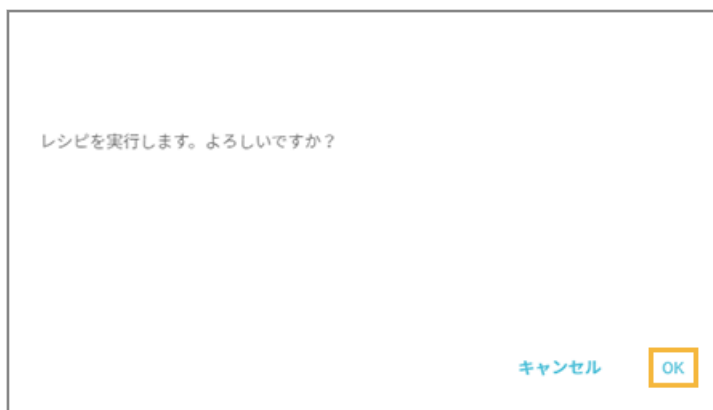
1. 「レシピ一覧」画面で作成したレシピを選択し、 をクリックします。

ポイント

レシピが無効の状態では、 は表示されません。「このレシピを有効にする」を  (有効) にしてください。



2. [OK] をクリックします。



出力データをダウンロードする

iOS

Android

Windows

作成した出力データをダウンロードします。

■ 一括出力設定からダウンロードする

ここでは、位置情報の出力データをダウンロードします。

ポイント

出力データ作成後、ダウンロードできる期間は7日間です。

1. [レシピ] の [アクション] をクリックします。



2. [位置情報を一括で出力する] をクリックします。

アクションを選択してください

	IOS	Android	Windows	macOS
 プロファイルを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
 アプリを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 プロビジョニングプロファイルを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 VPP アプリを設定する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 メッセージを設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
 アンケートを設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
 操作ログを一括で出力する	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 位置情報を一括で出力する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>

3. ダウンロードする出力設定をクリックします。

← 位置情報一括出力設定


設定の追加 ↻

<input type="checkbox"/>	設定名	出力期間	更新者	更新日時
<input type="checkbox"/>	位置情報ログ一括出力 (当月)	当月	設定管理者 (元中)	2018/06/14 13:12:25


20 ▾ | 1-1件 / 全1件 | << < 1 > >>

4. [実行履歴] をクリックします。

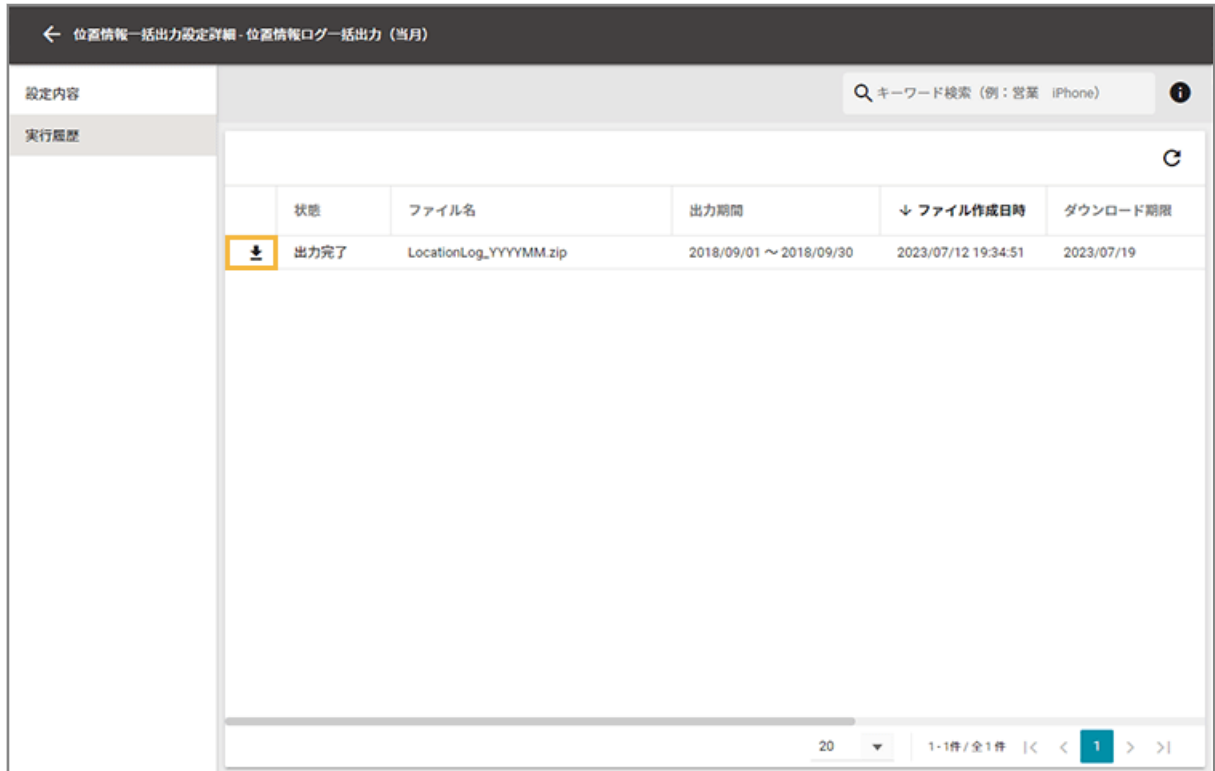


5.  をクリックします。

ポイント

状態が「出力完了」になると、 が表示されます。

第3章 レシピで操作を自動実行する



→ 出力された位置情報がダウンロードされます。

位置情報一括出力データ.xlsx - Excel

管理No.	デバイスグループ	使用名	デバイス管理名	日時	住所	取得タイプ	AnClient状態	緯度	経度	時差
1	総務部	内田 健太	内田 健太	2020/11/12 10:06	大阪府大阪市淀川区西中島	-	-	34.000000	135.000000	UTC+09:00
2	1 総務部	内田 健太	内田 健太	2020/11/12 14:44	大阪府大阪市淀川区西中島	-	-	34.000000	135.000000	UTC+09:00
3	1 総務部	内田 健太	内田 健太	2020/11/12 14:47	大阪府大阪市淀川区西中島	-	-	34.000000	135.000000	UTC+09:00
4	1 総務部	内田 健太	内田 健太	2020/11/12 14:50	大阪府大阪市淀川区西中島	-	-	34.000000	135.000000	UTC+09:00
5	1 総務部	内田 健太	内田 健太	2020/11/12 14:53	大阪府大阪市淀川区西中島	-	-	34.000000	135.000000	UTC+09:00
6	1 総務部	内田 健太	内田 健太	2020/11/12 14:56	大阪府大阪市淀川区西中島	-	-	34.000000	135.000000	UTC+09:00
7	1 総務部	内田 健太	内田 健太	2020/11/12 14:59	大阪府大阪市淀川区西中島	-	-	34.000000	135.000000	UTC+09:00
8	1 総務部	内田 健太	内田 健太	2020/11/12 15:44	大阪府大阪市淀川区西中島	-	-	34.000000	135.000000	UTC+09:00
9	1 総務部	内田 健太	内田 健太	2020/11/12 18:05	大阪府大阪市淀川区西中島	-	終了	34.000000	135.000000	UTC+09:00
10	1 総務部	内田 健太	内田 健太	2020/11/26 9:15	大阪府大阪市淀川区西中島	-	終了	34.000000	135.000000	UTC+09:00
11	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 11:41	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00
12	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 11:44	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00
13	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 11:47	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00
14	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 11:50	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00
15	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 11:53	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00
16	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 11:56	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00
17	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 11:59	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00
18	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 12:02	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00
19	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 12:05	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00
20	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 12:08	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00
21	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 12:11	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00
22	70 東日本営業部	茂礼手 太郎	茂礼手 太郎	2020/12/23 12:11	東京都品川区東大井	-	-	35.000000	139.000000	UTC+09:00

■ 出力データの内容

操作ログ

iOS

Android

項目名	属性	最大文字数	最大バイト長	ダブルクォーテーション
管理 No.	数値型	6	6	有
デバイスグループ	文字列	80	320	有
使用者名	文字列	50	200	有
デバイス管理名	文字列	50	200	有
日時	日付時刻型	19	19	有
分類	文字列	3	12	有
利用時間	日付時刻型	8	8	有
内容	文字列	12	48	有
詳細 1	文字列			有
詳細 2	文字列			有
カテゴリー	文字列	6	24	有
アラート	文字列	12	48	有
時差	文字列	9	36	有

位置情報

iOS

Android

Windows

項目名	属性	最大文字数	最大バイト長	ダブルクォーテーション
管理 No.	数値型	6	6	有
デバイスグループ	文字列	80	320	有
使用者名	文字列	50	200	有
デバイス管理名	文字列	50	200	有
日時	日付時刻型	19	19	有
住所	文字列			有
取得タイプ	文字列	7	28	有
LANSCOPE Client 状態	文字列	2	8	有
緯度	文字列	17	17	有
経度	文字列	17	17	有
時差	文字列	9	36	有

第 4 章 デバイスの位置情報を確認する

iOS

Android

Windows

デバイスの最新位置情報を確認できます。1 つの地図内に、最大 100 台の最新の位置情報を表示できます。

- [4-1 位置情報の取得設定をする](#)

各デバイスの位置情報を取得する設定をします。

- [4-2 最新の位置情報を確認する](#)

デバイスの位置情報サービスを利用し、現在位置を地図上で確認できます。

4-1 位置情報の取得設定をする

iOS

Android

Windows

各デバイスの位置情報を取得する設定をします。

管理者が設定した時間間隔で位置情報を自動取得し、1日の行動を時系列で確認できます。電源が切れる前の位置情報も自動取得するため、万が一の紛失時もデバイスの発見に役立ちます。

ステップ：

1. [管理コンソールの設定](#)
2. [デバイス側での設定](#)

ステップ 1： 管理コンソールの設定

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. 「位置情報ログ取得設定」で、[取得する] をチェックし、取得内容を設定します。



取得間隔

1分/3分/10分/30分/1時間/3時間の中から選択します。

業務時間のみ取得する

[デバイス設定] > [基本設定] > [共通] で設定した業務時間内だけの位置情報を取得します。

デバイス使用者に位置情報を開示する iOS

取得した位置情報をデバイスの LANSCOPE Client で確認できます。

高精度で取得されない設定になっているデバイスに警告する Android

取得設定が高精度になっていないデバイスに警告を表示します。高精度以外の設定に変更した、またはスクリーンをオンにしたタイミングで表示されます。



省電力設定 Android

デバイス上で振動を検知した場合だけ、位置情報を取得します。

注意

位置情報の精度が低下する場合があります。

4. [保存] をクリックします。

ステップ 2： デバイス側での設定

iOS の場合

取得するための条件は、次のとおりです。

- LANSCOPE Client (アプリ) を iOS デバイスにインストールし、登録している。
- デバイスの位置情報サービスがオンで、LANSCOPE の設定で [常に] を設定している。



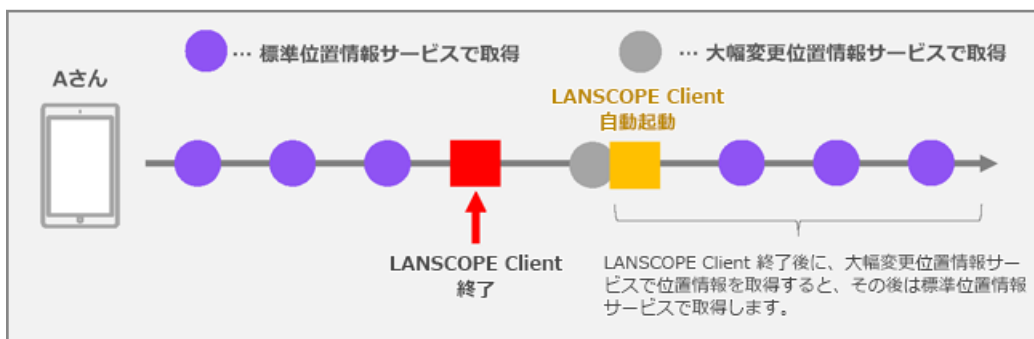


LANSCOPE Client が終了した場合

LANSCOPE Client が「バックグラウンドで起動している場合」「終了している場合」では取得の仕組みが異なります。

状態	取得の仕組み	精度
バックグラウンドで起動している	標準位置情報サービス 設定間隔どおりに位置情報を取得できます。	良い
終了している	大幅変更位置情報サービス (*) 基地局や Wi-Fi のアクセスポイントのエリアが変更され、且つ大幅に位置が変更した場合に取得します。	悪い

* : 「大幅変更位置情報サービス」で位置情報を取得した場合、LANSCOPE Client の自動復帰後は「標準位置情報サービス」で取得します。



位置情報使用時のステータスバー表示

iOS 16.4 以上の場合、LANSCOPE Client が位置情報を使用するため、ステータスバーが青く表示されます。

位置情報設定のダイアログ表示

iOS 13 以上の場合、「位置情報の使用を許可したままにしますか?」というダイアログが定期的に表示されます。

- [常に許可] を選択した場合

エンドポイントマネージャーの仕様どおりに位置情報を取得できます。



- ["使用中のみ許可"に変更] を選択した場合

青い時刻をタップし、位置情報の設定を [常に] に変更してください。





Android の場合

Android 9 以上の場合

[位置情報の使用] をオン、[Google 位置情報の精度] > [位置情報の精度を改善] をオンに設定します。





Android 9 未満の場合

[位置情報モード] > [高精度] に設定します。



注意

[バッテリー節約 (電池節約)] [端末 (機器) のみ] でも位置情報は取得できますが、精度が低下する場合があります。

ポイント

「Wi-Fi 詳細設定」で、スリープ時の Wi-Fi 接続の設定を変更できます。位置情報を正確に取得する場合、スリープ状態時に Wi-Fi を「使用する」に設定します。



Windows の場合

注意

Windows Server OS は、位置情報取得機能に未対応です。

Windows 11 の場合

次の項目を有効にします。

- [スタートボタン] > [設定] > [プライバシーとセキュリティ] > [位置情報] > [位置情報サービス]
- [スタートボタン] > [設定] > [ネットワークとインターネット] > [Wi-Fi]

Windows 10 の場合

次の項目を有効にします。

- [スタートボタン] > [設定] > [プライバシー] > [位置情報] > [変更] > [このデバイスの位置情報]
- [スタートボタン] > [設定] > [ネットワークとインターネット] > [Wi-Fi]

4-2 最新の位置情報を確認する

iOS

Android

Windows

デバイスの位置情報サービスを利用し、現在位置を地図上で確認できます。

ポイント

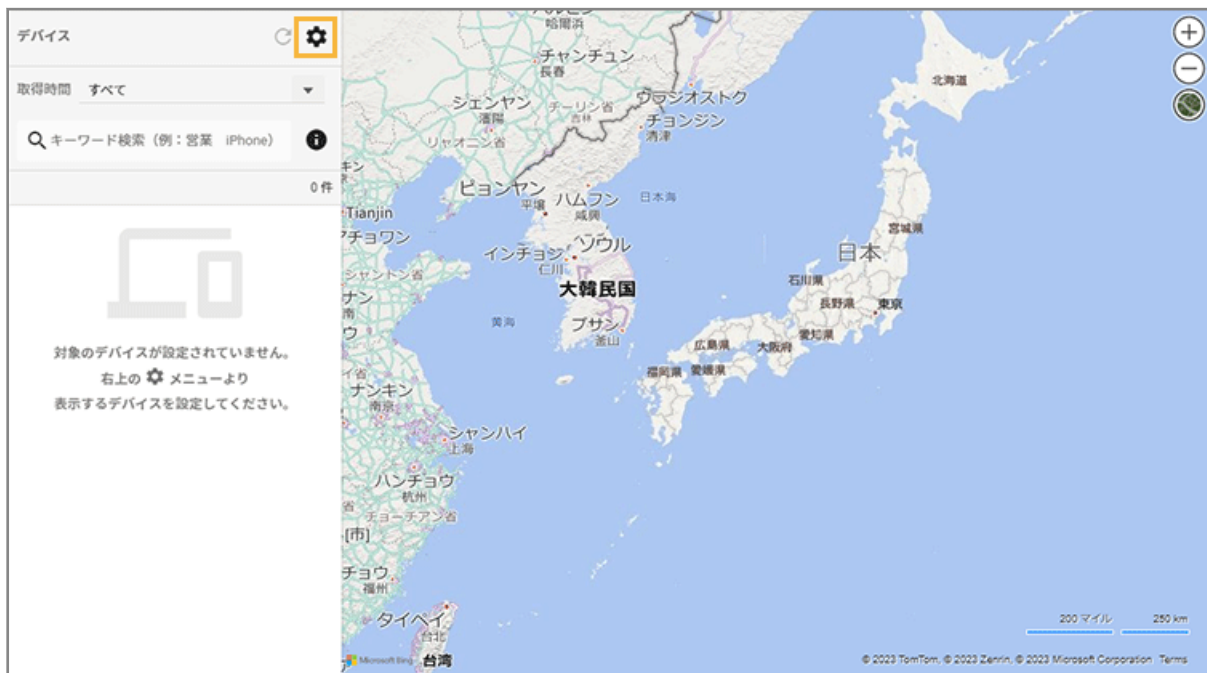
位置情報は、デバイスの設定／通信状況／ハードウェアの性能／OSの動作に依存します。

1. [モニター] の [最新位置情報] をクリックします。



2. 表示するデバイスを選択します。

- (1)  をクリックします。



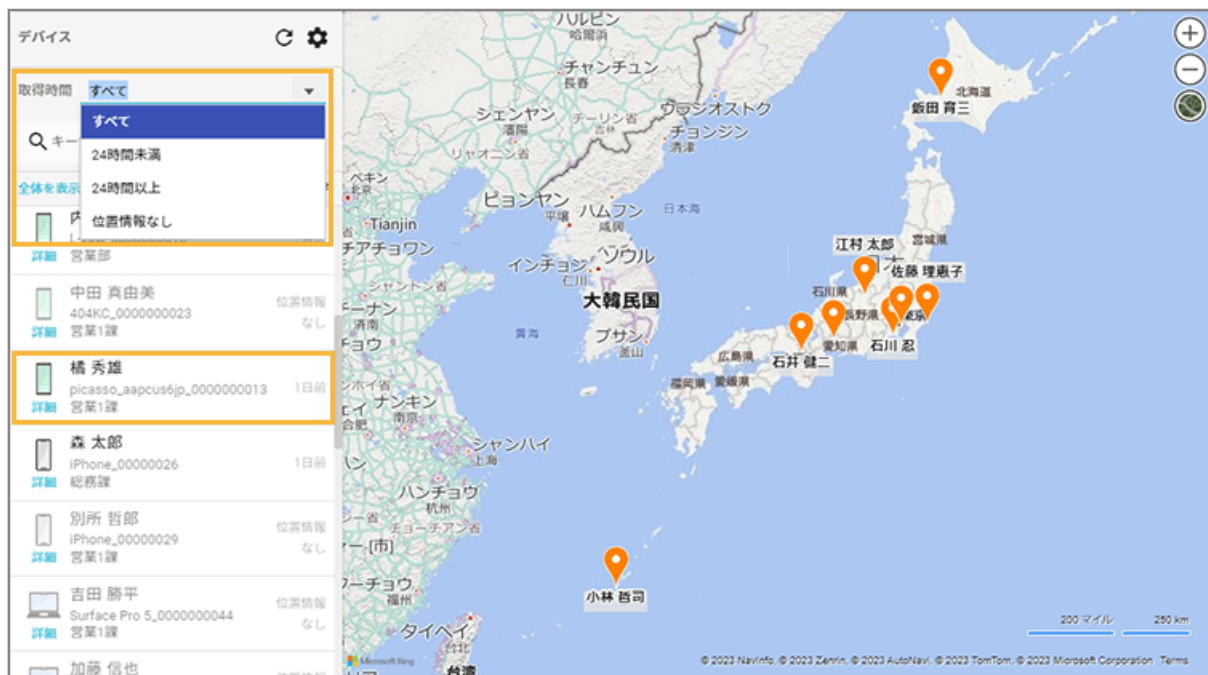
- (2) デバイスをチェックし、[選択] をクリックします。



3. 確認するデバイスを選択します。

[▼] をクリックすると、取得時間でデバイスを絞り込みます。

取得時間	概要
全て	選択しているすべてのデバイスを表示します。
24 時間未満	位置情報の取得から 24 時間未満のデバイスを表示します。
24 時間以上	位置情報の取得から 24 時間以上経過しているデバイスを表示します。
不明	位置情報が取得できていないデバイスを表示します。



→ 選択したデバイス周辺が拡大表示されます。

4. 該当デバイスの情報を確認する場合、 にマウスポインターを合わせます。



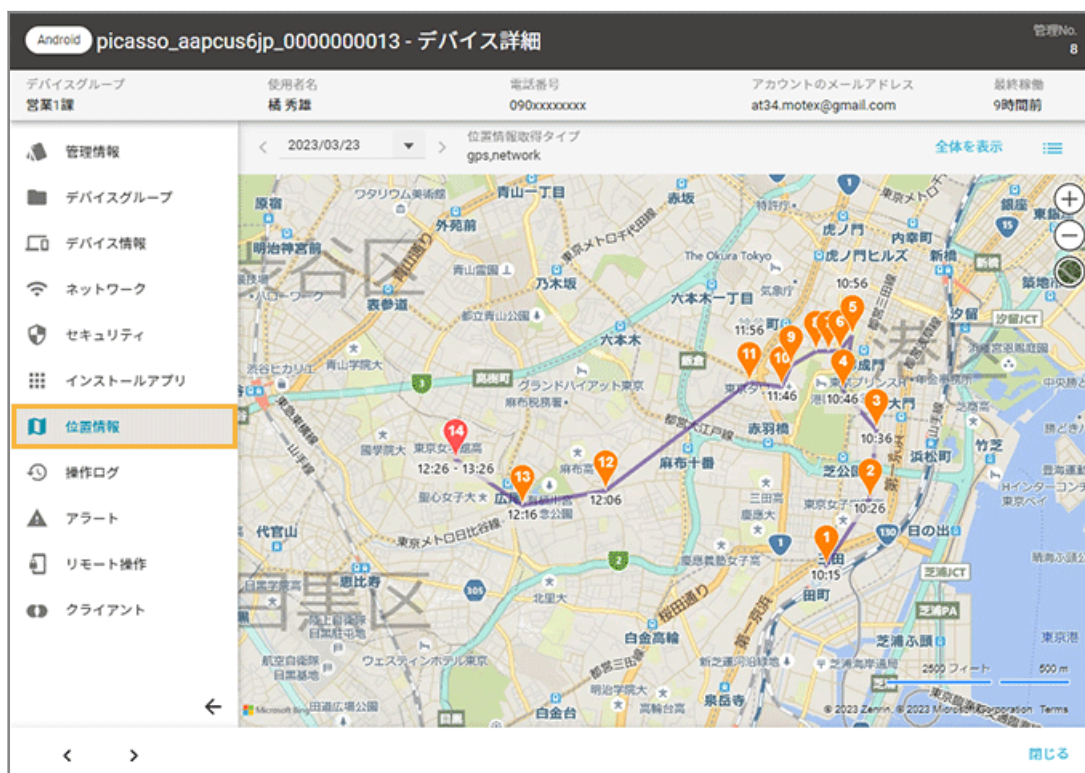
5. デバイスの詳細情報を確認する場合、次の操作をします。

- (1) デバイスの [詳細] をクリックします。

第4章 デバイスの位置情報を確認する



(2) デバイスの移動履歴を確認します。



→ 管理者が設定した時間間隔で位置情報を取得し、1日の行動が時系列で表示されます。

第 5 章 レポートを確認する

iOS

Android

Windows

macOS

取得した操作ログ／資産情報のデータや Windows アップデートの情報から、レポートを自動作成できます。導入デバイス／業務アプリが本来の目的で活用できているかを視覚的に確認できます。

- [5-1 デバイスの利用状況を確認する](#)

取得した操作ログや資産情報のデータから、デバイスの利用状況をレポートで確認できます。

- [5-2 Windows アップデートを確認して対策する](#)

Windows アップデートのレポートを確認して、サポートが終了する OS や、未適用の月例パッチのインストール設定ができます。

5-1 デバイスの利用状況を確認する

iOS

Android

Windows

macOS

取得した操作ログや資産情報のデータから、デバイスの利用状況をレポートで確認できます。

■ 表示できるレポートとカスタマイズ方法を確認する

表示できるレポート

レポート	対応 OS	内容
セキュリティレベルの低いデバイス	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="background-color: #333; color: white; padding: 2px 5px;">iOS</div> <div style="background-color: #4CAF50; color: white; padding: 2px 5px;">Android</div> <div style="background-color: #2196F3; color: white; padding: 2px 5px;">Windows</div> <div style="background-color: #607D8B; color: white; padding: 2px 5px;">macOS</div> </div>	アラートの状態から、改善が必要なデバイスを把握できます。「危険」「注意」に分類して表示します。
長期間未稼働のデバイス	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="background-color: #333; color: white; padding: 2px 5px;">iOS</div> <div style="background-color: #4CAF50; color: white; padding: 2px 5px;">Android</div> <div style="background-color: #2196F3; color: white; padding: 2px 5px;">Windows</div> <div style="background-color: #607D8B; color: white; padding: 2px 5px;">macOS</div> </div>	<p>長期間電源が入っていない、紛失の可能性があるデバイスを把握できます。</p> <p>操作ログをもとに、デバイスの未使用期間を「1ヶ月以上」「1週間～1ヶ月」に分類して表示します。</p>
デバイスの利用時間	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="background-color: #333; color: white; padding: 2px 5px;">iOS</div> <div style="background-color: #4CAF50; color: white; padding: 2px 5px;">Android</div> </div>	<p>実際の利用時間から、活用の促進や配置変換が必要なデバイスを把握できます。</p> <p>操作ログをもとに、1か月当たりのデバイスの利用時間を「60時間以上」「20時間～60時間」「10時間～20時間」「0時間～10時間」「活用なし」に分類して表示します。</p>
電話の利用時間	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="background-color: #333; color: white; padding: 2px 5px;">iOS</div> <div style="background-color: #4CAF50; color: white; padding: 2px 5px;">Android</div> </div>	<p>通話の時間から、適切なプランに変更するなど費用削減につながるデバイスを把握できます。</p> <p>操作ログをもとに、1か月当たりの電話の利用時間を「20時間以上」「10時間～20時間」「3時間～10時間」「0時間～3時間」「活用なし」に分類して表示します。</p>
カテゴリ別のアプリ利用時間	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="background-color: #4CAF50; color: white; padding: 2px 5px;">Android</div> </div>	<p>カテゴリ別のアプリ利用時間から、よく利用されているアプリのカテゴリを把握できます。</p> <p>操作ログをもとに、1か月当たりのカテゴリ別のアプリ利用時間を「ビジネス」「メール・通信」「電話」「情報」「ソーシャル」「ゲーム・娯楽」「その他」のカテゴリに分類して表示します。</p>

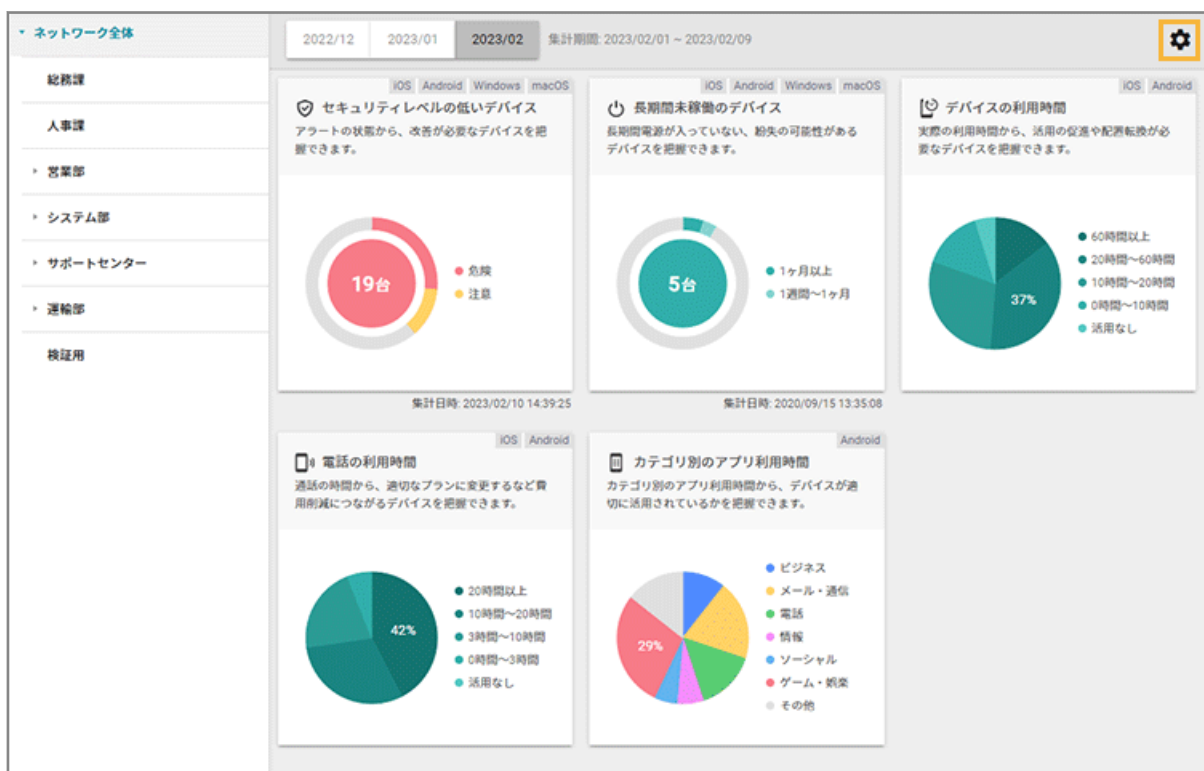
表示するレポートのカスタマイズ

初期設定では、すべてのレポートが表示されます。必要なレポートを選択して、表示するレポートをカスタマイズできます。

1. [レポート] の [利用状況] をクリックします。



2.  をクリックします。



3. 表示するレポートだけをチェックし、[適用] をクリックします。



■ デバイスの利用状況を確認する

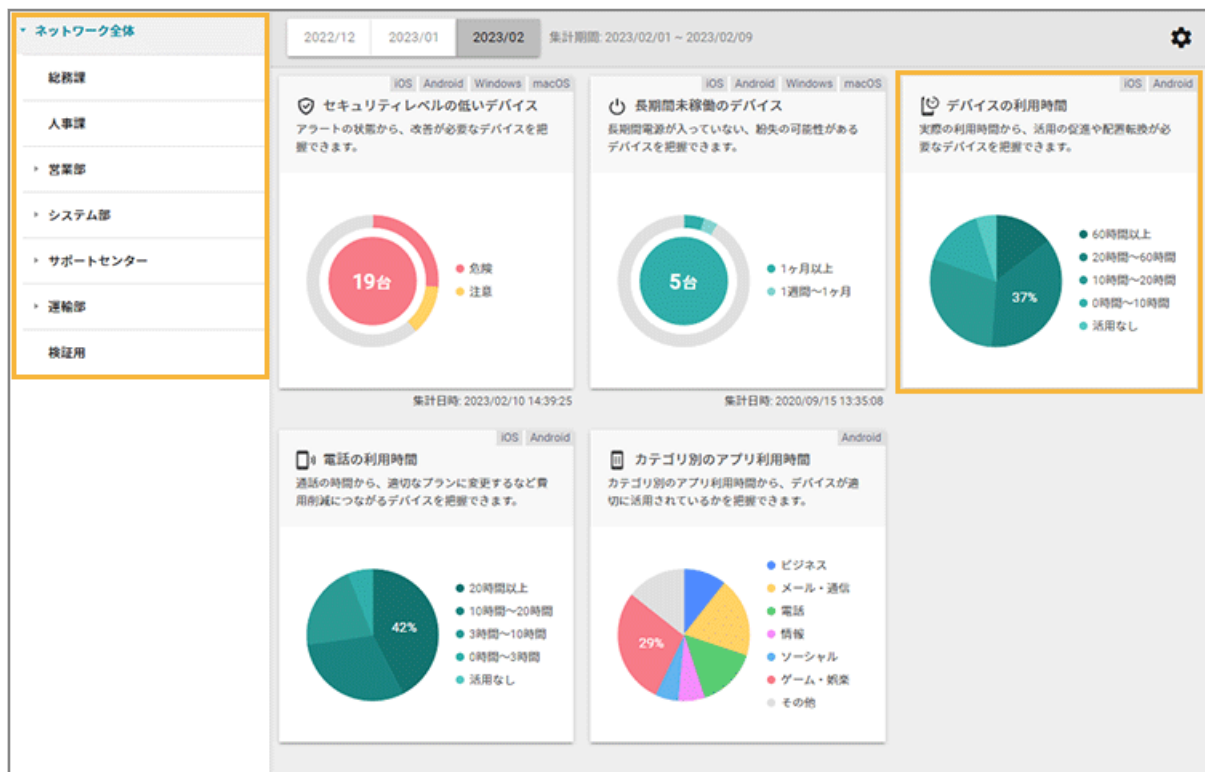
取得した操作ログや資産情報のデータから、デバイスの利用状況をレポートで確認できます。

ここでは、例として「デバイスの利用時間」レポートを確認します。

1. [レポート] の [利用状況] をクリックします。



2. デバイスグループをクリックし、「デバイスの利用時間」レポートをクリックします。



3. デバイスグループを選択します。



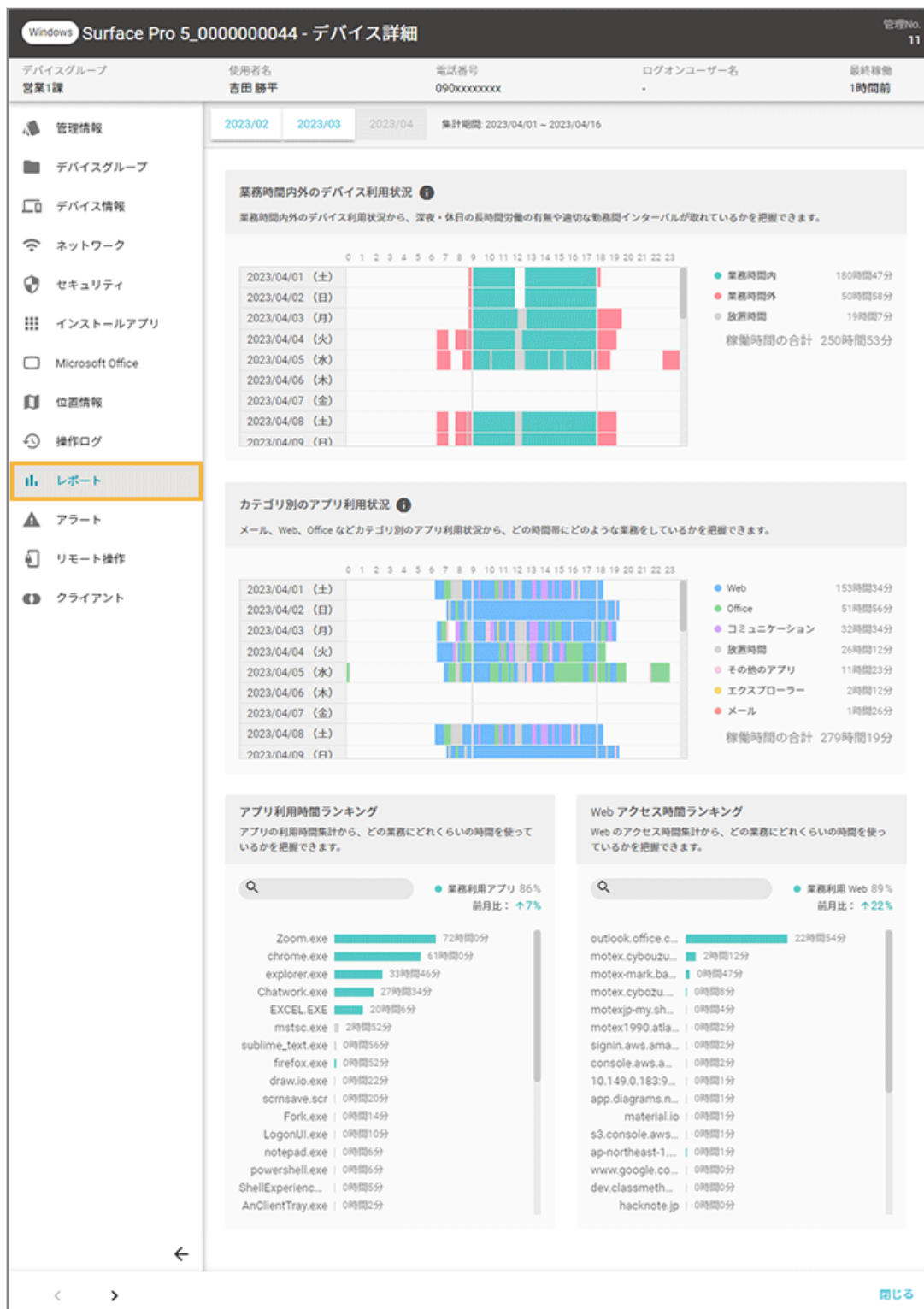
→ 選択したデバイスグループに紐づくデバイスが表示されます。

4. デバイスをクリックします。



→ 「デバイス詳細」画面が表示されます。

5. [レポート] をクリックし、個人レポートを確認します。



業務時間内外のデバイス利用状況

デバイスの電源がオンになっている状態を取得し、集計します。

業務時間内外のデバイス利用状況から、深夜/休日の長時間労働の有無や適切な勤務間インターバルが取れているかを把握できます。

カテゴリ別のアプリ利用状況

アプリを利用している状態を取得し、集計します。

メール/Web/Office などカテゴリー別のアプリ利用状況から、どの時間帯にどのような業務をしているかを把握できます。

アプリ利用時間ランキング

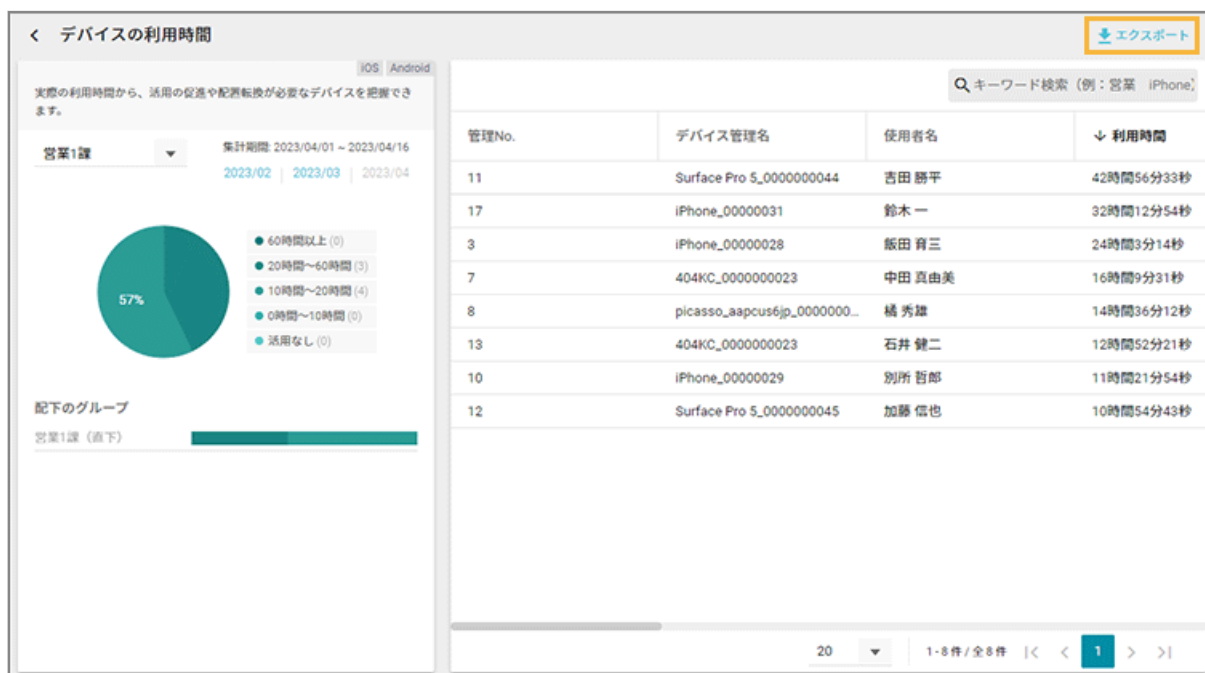
アプリの利用時間集計から、どの業務にどれくらいの時間を使っているかを把握できます。

Web アクセス時間ランキング

Web のアクセス時間集計から、どの業務にどれくらいの時間を使っているかを把握できます。

→ [閉じる] をクリックします。

6. デバイス一覧をエクスポートする場合、 をクリックします。



デバイスの利用時間

実際の利用時間から、活用の促進や配置転換が必要なデバイスを把握できます。

OS: iOS / Android

集計期間: 2023/04/01 ~ 2023/04/16

2023/02 | 2023/03 | 2023/04

営業1課

57%

- 60時間以上 (0)
- 20時間~60時間 (3)
- 10時間~20時間 (4)
- 0時間~10時間 (0)
- 活用なし (0)

配下のグループ

営業1課 (直下)

管理No.	デバイス管理名	利用者名	↓ 利用時間
11	Surface Pro 5_0000000044	吉田 勝平	42時間56分33秒
17	iPhone_000000031	鈴木 一	32時間12分54秒
3	iPhone_000000028	飯田 育三	24時間3分14秒
7	404KC_0000000023	中田 真由美	16時間9分31秒
8	picasso_aapcus6jp_0000000...	橋 秀雄	14時間36分12秒
13	404KC_0000000023	石井 健二	12時間52分21秒
10	iPhone_000000029	別所 哲郎	11時間21分54秒
12	Surface Pro 5_0000000045	加藤 信也	10時間54分43秒

20 1-8件 / 全8件 |< < 1 > >|

→ CSV ファイルがエクスポートされます。

5-2 Windows アップデートを確認して対策する

Windows

Windows アップデートのレポートを確認して、サポートが終了する OS や、未適用の月例パッチのインストール設定ができます。WSUS で OS/月例パッチを配信後、社内ネットワークに接続できないなどの理由で適用できなかったデバイスに対して、エンドポイントマネージャーで配信設定をします。

プロキシサーバーを経由する環境でインストール設定を実行する場合、事前にプロキシの設定が必要です。詳細は、[プロキシ設定を適用する](#)を参照してください。

■ OS のサポートが終了しているデバイスを確認してインストール設定をする

デバイスの OS バージョンを確認できます。OS をアップデートしたい場合は、インストール設定もできます。

注意

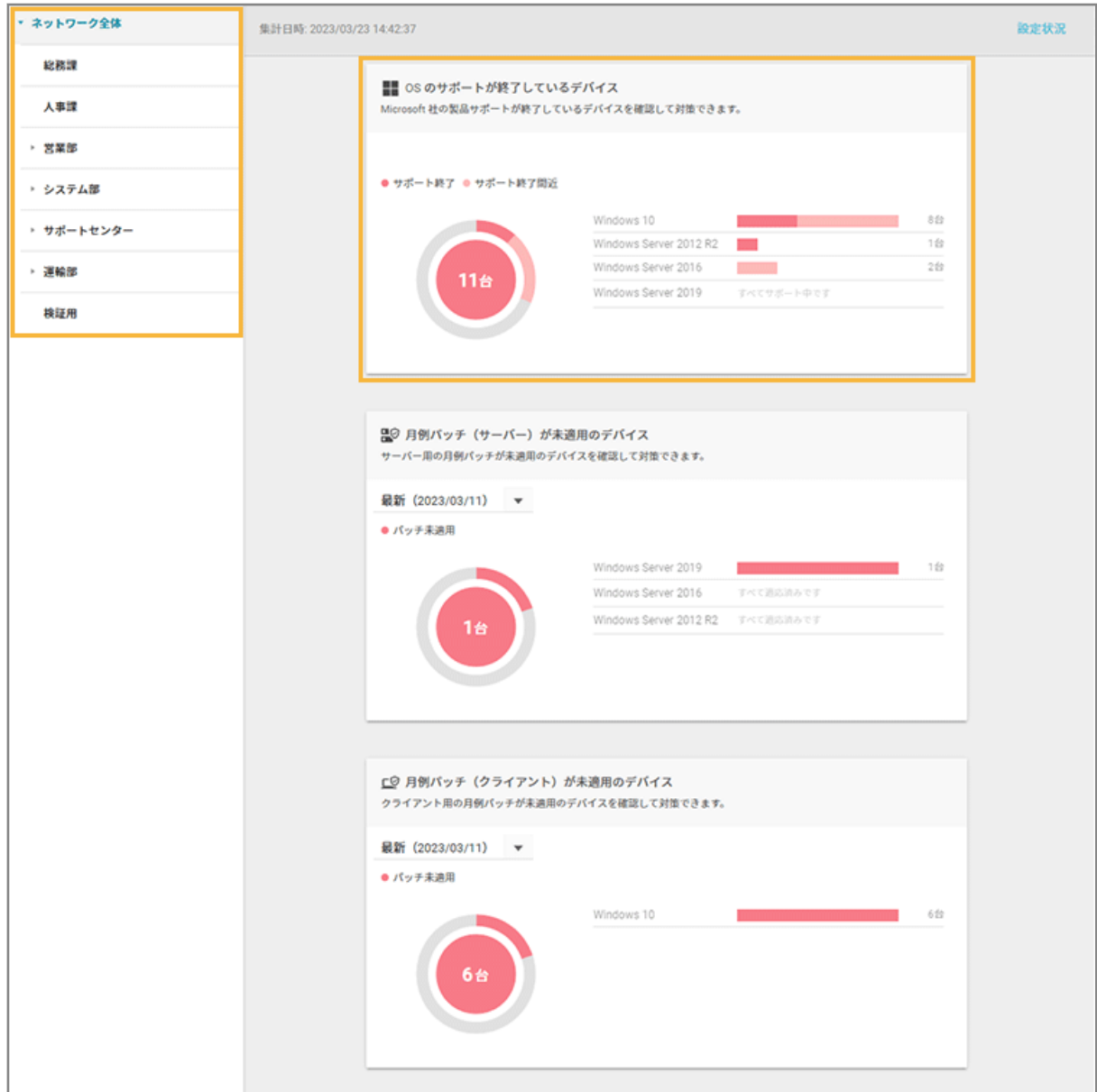
Microsoft 社が最新の OS を公開してから MOTEX が動作確認や対応バージョンをリリースするまでの間は、次の制限事項があります。

- エンドポイントマネージャーで最新の OS を配信できません。
- エンドポイントマネージャー以外の機能で OS を配信した場合、デバイスの Windows バージョン情報が更新されません。MOTEX の動作確認完了後に、正しい Windows バージョン情報を確認できるようになります。

1. **【レポート】の【Windows アップデート】をクリックします。**



2. **デバイスグループをクリックし、「OS のサポートが終了しているデバイス」レポートをクリックします。**



3. OS のサポート状況を確認します。

← OS サポートの詳細

ネットワーク全体 ▼ すべて ▼ サポート中のデバイスも表示する

🔍 キーワード検索 (例: 営業 iPhone) ⓘ

🔄 ⋮

<input type="checkbox"/>	↓ 状態	サポート終了日	管理No.	デバイスグループ	デバイス管理名	OSバージョン	Windows
<input type="checkbox"/>	サポート終了	2020/11/10	11	営業1課	Surface Pro 5_0000000044	Windows 10 Pro 10.0.17134	1803
<input type="checkbox"/>	サポート終了	2020/11/10	12	営業1課	Surface Pro 5_0000000045	Windows 10 Pro 10.0.17134	1803
<input type="checkbox"/>	サポート終了	2020/11/10	20	営業2課	Surface 3_0000000054	Windows 10 Home 10.0.10240	20H1
<input type="checkbox"/>	サポート終了	2020/11/10	76	検証用	Surface Pro 3_0000000053	Windows Server 2012R2	
<input type="checkbox"/>	サポート終了間近	2021/12/11	22	営業2課	Surface 3_0000000051	Windows 10 Home 10.0.10240	1507
<input type="checkbox"/>	サポート終了間近	2021/12/11	23	営業2課	Surface 3_0000000047	Windows 10 Pro 10.0.19041	2004
<input type="checkbox"/>	サポート終了間近	2021/12/11	24	営業2課	Surface 3_0000000048	Windows 10 Pro 10.0.19041	2004
<input type="checkbox"/>	サポート終了間近	2021/12/11	25	営業2課	Surface 3_0000000049	Windows 10 Pro 10.0.19041	2004
<input type="checkbox"/>	サポート終了間近	2021/12/11	26	営業2課	Surface 3_0000000050	Windows 10 Pro 10.0.19041	2004
<input type="checkbox"/>	サポート終了間近	2021/12/11	77	検証用	Surface Pro 3_0000000053	Windows Server 2016	
<input type="checkbox"/>	サポート終了間近	2021/12/11	78	検証用	Surface Pro 3_0000000053	Windows Server 2016	

1-11件/全11件 |< < 1 > >|

状態

- サポート終了
Microsoft 社の製品サポートが終了しています。
- サポート終了間近
Microsoft 社の製品サポートが 180 日間以内に終了します。

4. OS をアップデートする場合は、デバイスをチェックし、[インストール設定] をクリックします。

第5章 レポートを確認する

← OSサポートの詳細

ネットワーク全体 ▼ すべて ▼ サポート中のデバイスも表示する

🔍 キーワード検索 (例: 営業 iPhone) ⓘ

✕ 3件を選択中 インストール設定

<input type="checkbox"/>	状態	サポート終了日	管理No.	デバイスグループ	デバイス管理名	OSバージョン	Windows
<input checked="" type="checkbox"/>	サポート終了	2020/11/10	11	営業1課	Surface Pro 5_0000000044	Windows 10 Pro 10.0.17134	1803
<input checked="" type="checkbox"/>	サポート終了	2020/11/10	12	営業1課	Surface Pro 5_0000000045	Windows 10 Pro 10.0.17134	1803
<input checked="" type="checkbox"/>	サポート終了	2020/11/10	20	営業2課	Surface 3_0000000054	Windows 10 Home 10.0.10240	20H1
<input type="checkbox"/>	サポート終了	2020/11/10	76	検証用	Surface Pro 3_0000000053	Windows Server 2012R2	
<input type="checkbox"/>	サポート終了間近	2021/12/11	22	営業2課	Surface 3_0000000051	Windows 10 Home 10.0.10240	1507
<input type="checkbox"/>	サポート終了間近	2021/12/11	23	営業2課	Surface 3_0000000047	Windows 10 Pro 10.0.19041	2004
<input type="checkbox"/>	サポート終了間近	2021/12/11	24	営業2課	Surface 3_0000000048	Windows 10 Pro 10.0.19041	2004
<input type="checkbox"/>	サポート終了間近	2021/12/11	25	営業2課	Surface 3_0000000049	Windows 10 Pro 10.0.19041	2004
<input type="checkbox"/>	サポート終了間近	2021/12/11	26	営業2課	Surface 3_0000000050	Windows 10 Pro 10.0.19041	2004
<input type="checkbox"/>	サポート終了間近	2021/12/11	77	検証用	Surface Pro 3_0000000053	Windows Server 2016	
<input type="checkbox"/>	サポート終了間近	2021/12/11	78	検証用	Surface Pro 3_0000000053	Windows Server 2016	

1-11件/全11件 |< < 1 > >|

5. 項目を設定し、[実行] をクリックします。

設定名

設定名を入力します。[ルール] > [配信設定] > [OS アップデート (Windows)] > [設定状況] 画面で表示されます。

インストールするデバイス

インストールするデバイス名です。デバイスの詳細情報を確認できます。

インストールする OS アップデート

デバイスにインストールする OS バージョンです。

インストール設定

- インストールタイミング

インストールするタイミングを選択します。

- [すぐにインストールする]

実行完了後、すぐにインストールされます。

- [時刻を指定してインストールする]

実行完了後、指定した時刻にインストールされます。すでに指定時刻を過ぎていた場合、すぐにインストールされます。

- [日時を指定してインストールする]

実行完了後、指定した日時にインストールされます。すでに指定日時を過ぎていた場合、すぐにインストールされます。

- オプション

- [クライアント側からインストールを選択できるようにする]

クライアントにインストール確認のメッセージが表示されます。タスクバーの通知領域にアイコンが表示され、クライアント側のタイミングでファイルの実行を選択できます。

- 通知

- [インストール前にポップアップで通知する]

インストール前に、入力した内容をデバイスにポップアップで通知できます。

→ インストール設定が完了します。

実行状況は、[設定状況] をクリック、または [ルール] > [配信設定] > [OS アップデート (Windows)] > [設定状況] で確認できます。詳細は、[実行状況を確認する](#)を参照してください。

■ 月例パッチが未適用のデバイスを確認してインストール設定をする

クライアント/サーバーの月例パッチの適用状況を確認できます。月例パッチを適用したい場合は、インストール設定もできます。

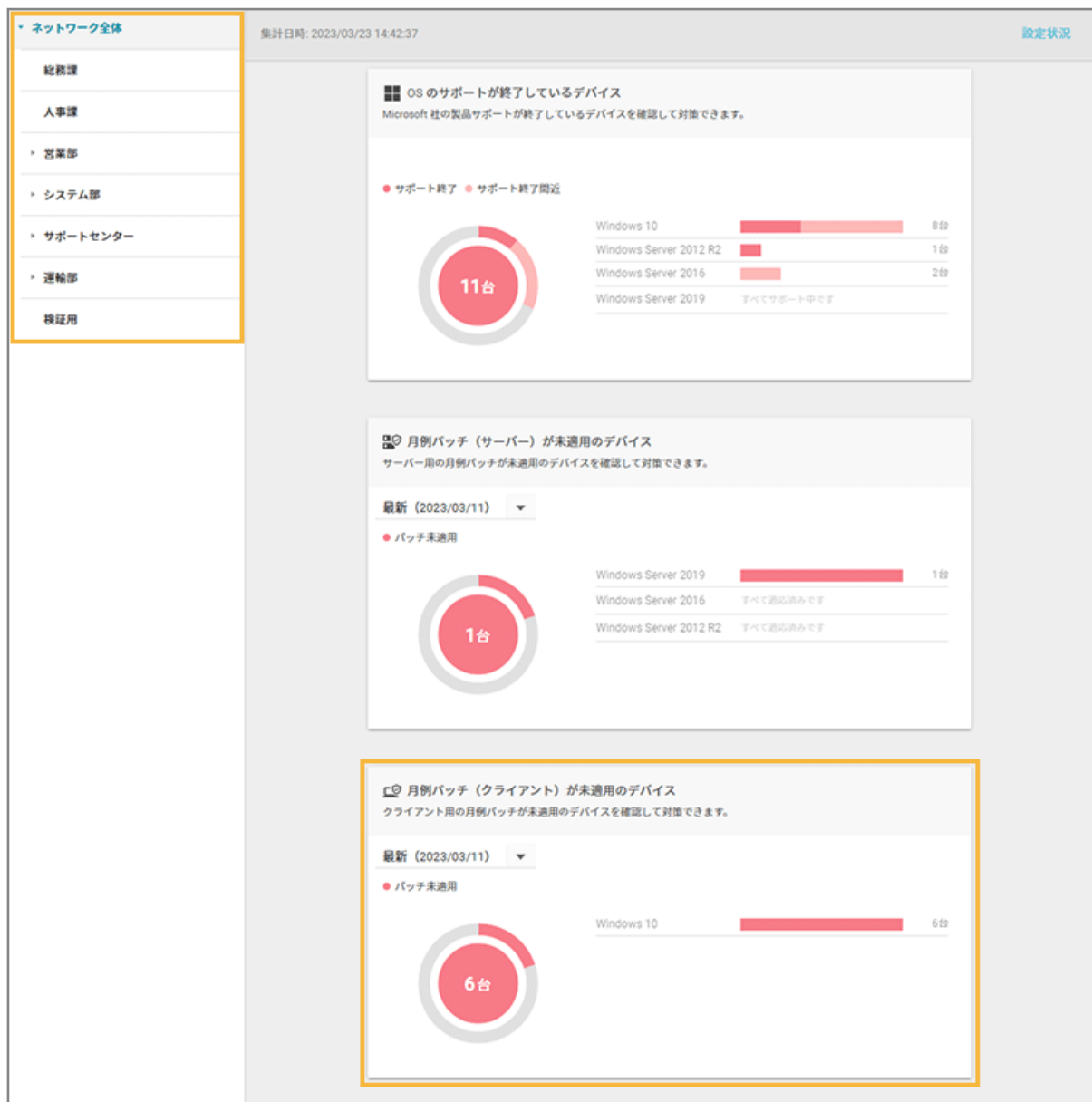
すでに作成している設定は、[設定状況] をクリックして確認できます。

ここでは、例としてクライアントの月例パッチを確認します。

1. [レポート] の [Windows アップデート] をクリックします。



2. デバイスグループをクリックし、「月例パッチ (クライアント) が未適用のデバイス」レポートをクリックします。



3. 月例パッチの適用状況を確認します。

月例パッチは、過去にリリースされた更新を含む、累積更新プログラムが表示されます。

注意

MOTEX で動作検証する前の更新プログラムを適用した場合、最新の月例パッチが「未適用」と表示される場合があります。

月例パッチの詳細

ネットワーク全体 | 最新 (2023/03/11) | サーバー | クライアント | 適用済みのデバイスも表示する | キーワード検索 (例: 営業 IP) | 検索

<input type="checkbox"/>	↓ 状態	適用された月例パッチ	管理No.	デバイスグループ	デバイス管理名	OSバージョン	Wi
<input type="checkbox"/>	未適用	2023/06/13	20	営業2課	Surface 3_0000000054	Windows 10 Home 10.0.10240	20
<input type="checkbox"/>	未適用	2023/02/13	22	営業2課	Surface 3_0000000051	Windows 10 Home 10.0.10240	19
<input type="checkbox"/>	未適用	2023/02/13	11	営業1課	Surface Pro 5_0000000044	Windows 10 Pro 10.0.17134	18
<input type="checkbox"/>	未適用	2023/02/13	12	営業1課	Surface Pro 5_0000000045	Windows 10 Pro 10.0.17134	18
<input type="checkbox"/>	未適用	2023/02/13	23	営業2課	Surface 3_0000000047	Windows 10 Pro 10.0.19041	20
<input type="checkbox"/>	未適用	2023/02/13	24	営業2課	Surface 3_0000000048	Windows 10 Pro 10.0.19041	20

1-6件 / 全6件 | < < 1 > > |

状態

- 未適用

月例パッチが未適用です。

- 適用済み

月例パッチが適用されています。過去の月例パッチも適用済みになります。

4. 月例パッチを適用する場合は、デバイスをチェックし、[インストール設定] をクリックします。

← 月例バッチの詳細

ネットワーク全体 ▼ 最新 (2023/03/11) ▼ サーバー クライアント 適用済みのデバイスも表示する 🔍 キーワード検索 (例: 営業 IP) ⓘ

× 3件を選択中 インストール設定

<input checked="" type="checkbox"/>	↓ 状態	適用された月例バッチ	管理No.	デバイスグループ	デバイス管理名	OSバージョン	Wi
<input checked="" type="checkbox"/>	未適用	2023/06/13	20	営業2課	Surface 3_0000000054	Windows 10 Home 10.0.10240	20
<input type="checkbox"/>	未適用	2023/02/13	22	営業2課	Surface 3_0000000051	Windows 10 Home 10.0.10240	15
<input type="checkbox"/>	未適用	2023/02/13	11	営業1課	Surface Pro 5_0000000044	Windows 10 Pro 10.0.17134	18
<input type="checkbox"/>	未適用	2023/02/13	12	営業1課	Surface Pro 5_0000000045	Windows 10 Pro 10.0.17134	18
<input checked="" type="checkbox"/>	未適用	2023/02/13	23	営業2課	Surface 3_0000000047	Windows 10 Pro 10.0.19041	20
<input checked="" type="checkbox"/>	未適用	2023/02/13	24	営業2課	Surface 3_0000000048	Windows 10 Pro 10.0.19041	20

1-6件 / 全6件 |< < 1 > >|

5. 項目を設定し、[実行] をクリックします。



設定名

設定名を入力します。[ルール] > [配信設定] > [OS アップデート (Windows)] > [設定状況] 画面で表示されます。

インストールするデバイス

インストールするデバイス名です。デバイスの詳細情報を確認できます。

インストールする月例パッチ

インストールする月例パッチを選択します。

インストール設定

- インストールタイミング

インストールするタイミングを選択します。

- [すぐにインストールする]

実行完了後、すぐにインストールされます。

- [時刻を指定してインストールする]

実行完了後、指定した時刻にインストールされます。すでに指定時刻を過ぎていた場合、すぐにインストールされます。

- [日時を指定してインストールする]

実行完了後、指定した日時にインストールされます。すでに指定日時を過ぎていた場合、すぐにインストールされます。

- オプション

- [クライアント側からインストールを選択できるようにする]

クライアントにインストール確認のメッセージが表示されます。タスクバーの通知領域にアイコンが表示され、クライアント側のタイミングでファイルの実行を選択できます。

- 通知

- [インストール前にポップアップで通知する]

インストール前に、入力した内容をデバイスにポップアップで通知できます。

→ インストール設定が完了します。

実行状況は、[設定状況] をクリック、または [ルール] > [配信設定] > [OS アップデート (Windows)] > [設定状況] で確認できます。詳細は、[実行状況を確認する](#)を参照してください。

第6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を利用/運用するために必要な設定ができます。

- [6-1 デバイス設定をする](#)

エンドポイントマネージャーを利用/運用するためのデバイス設定をします。

- [6-2 Apple サービス設定をする](#)

iOS/macOS デバイスの管理に必要な設定をします。

- Android Enterprise 設定をする

詳細は、An-347「Android Enterprise 利用ガイド」を参照してください。

- [6-3 記録メディア制御設定をする](#)

記録メディア制御に必要な設定をします。

- [6-4 配信設定をする](#)

Windows デバイスへの配信に必要な設定をします。

- [6-5 アプリ設定をする](#)

インストール情報が取得されたアプリの利用レベルを設定します。

6-1 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](#)
- [業務時間を設定する](#)
- [取得する情報を設定する](#)
- [PC 操作ログ設定をする](#)

基本設定

次の設定を確認／作成できます。

設定	共通	iOS	Android	Windows	macOS
メモ	○	○	○	○	○
業務時間設定	○	—	—	—	—
LANSCOPE Client アップデート設定	—	—	○	—	○
デバイス表示設定 (*1) (*2)	—	○	—	—	—
デバイス使用者への設定情報表示 (*3)	—	○	○	○	—

設定		共通	iOS	Android	Windows	macOS
デバイス情報取得設定	インストールアプリ情報	—	○	○	○	○
	プロファイル情報	—	○	—	—	○
操作ログ取得設定	電話利用ログ	—	○	○	—	—
	デバイス活用ログ	—	○	—	—	—
	アプリ利用ログ	—	—	○ (*4)	—	—
	環境変更操作ログ	—	—	○	—	—
位置情報ログ取得設定		—	○	○	○ (*5)	—
デバイスへの通知設定	LANSCOPE Client 停止時の起動通知	—	○	—	—	—
	資産アラートの通知	—	—	○ (*6)	—	—
	操作アラートの通知	—	—	○ (*6) (*7)	—	—
アンインストール防止設定		—	—	—	○	○
パスワードポリシー設定		—	○	○ (*8) (*9)	—	○
マルチユーザー機能制御		—	—	○ (*8)	—	—

*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。位置情報ログを取得するための設定ではありません。

*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：LANSCOPE Client 側で、環境設定で設定されている内容を確認できます。

*4：アプリを禁止設定する場合、アプリ利用ログは「取得する」に設定してください。詳細は、[アプリの利用を禁止するときに必要な設定をする](#)を参照してください。

*5：Windows Server OS は、位置情報取得機能に未対応です。

*6：事前にアラートに設定するためのレシピ作成が必要です。詳細は、[アラート設定の流れ](#)を参照してください。

*7：アプリを禁止設定する場合、「操作アラートの通知」の「不許可・禁止したアプリが実行された」を「通知する」に設定してください。詳細は、[アプリの利用を禁止するときに必要な設定をする](#)を参照してください。

*8：Android Enterprise デバイスには適用できません。Android Enterprise デバイスに適用するポリシーは、[ルール] > [Android Enterprise 設定] で設定します。詳細は、An-347「Android Enterprise 利用ガイド」を参照してください。

*9：Android 10 以上のデバイスには適用されません。

PC 操作ログ設定

次の設定を確認／作成できます。

設定		Windows	macOS
通信機器接続	Wi-Fi 接続ログ	○	—
	Bluetooth 接続ログ	○	—
	有線接続ログ	○	—
アプリ禁止	アプリ禁止	○	—
	通知	○	—
省電力		○	—

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。

2 項目の関連づけ

選択されたファイル：group_202302161124.csv

選択されたファイルの列名と LANSCOPE の管理項目を関連づけます。
関連づけされていない項目はインポートされません。

項目名	関連づける列名
グループ名 *	
グループコード *	
上位グループコード *	

自動選択

<

>

ファイルの列名
グループ名
グループコード
上位グループコード

※ 作成可能なグループの階層は、最大で5階層です。

→ 「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。

3 洗い替えオプションの選択

登録済みのグループが読み込むファイルに記載されていない場合は削除する。

※ 削除されたグループ配下のデバイスは、ネットワーク全体配下に移動します。

キャンセル インポート

- (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。



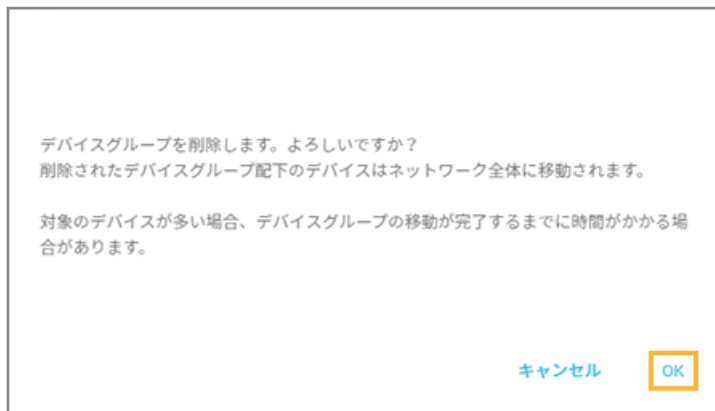
2. デバイスグループをクリックし、[削除] をクリックします。

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。

業務時間を設定する

iOS

Android

業務時間を設定をすると、設定した時間帯の位置情報／操作ログを取得できます。

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、[共通] をクリックして、[作成] をクリックします。



3. 「業務時間設定」で、次の項目を設定します。

The screenshot shows a settings page for business hours. At the top, there are tabs for '共通' (Common), 'iOS', 'Android', 'Windows', and 'macOS'. Below the tabs, there's a header with '継承' (Inheritance) and 'の設定を使用しています' (Using the settings of...), and buttons for 'キャンセル' (Cancel) and '保存' (Save). The main section is titled '業務時間設定' (Business Hours Setting). It contains several fields: '開始時刻' (Start Time) with a dropdown set to '00' and a time selector set to ': 00'; '終了時刻' (End Time) with a dropdown set to '23' and a time selector set to ': 59'; 'タイムゾーン' (Time Zone) with a dropdown set to '(UTC+09:00) 大阪、札幌、東京'; '業務曜日' (Business Days) with checkboxes for '日' (Sun), '月' (Mon), '火' (Tue), '水' (Wed), '木' (Thu), '金' (Fri), and '土' (Sat), where Mon-Fri are checked; '休日設定' (Holiday Setting) with a '設定する' (Set) button; and '業務日設定' (Business Day Setting) with a '設定する' (Set) button.

メモ

設定内容の説明などを必要に応じて入力します。

開始時刻

業務の開始時刻（管理開始の時刻）を入力します。

終了時刻

業務の終了時刻（管理終了の時刻）を入力します。

業務曜日

業務の曜日（管理する曜日）をチェックします。

休日設定

チェックすると、管理しない日付を指定して設定できます。

業務日設定

チェックすると、管理する日付を指定して設定できます。

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	共通	iOS	Android	Windows	macOS
メモ	○	○	○	○	○
業務時間設定	○	—	—	—	—
LANSCOPE Client アップデート設定	—	—	○	—	○
デバイス表示設定 (*1) (*2)	—	○	—	—	—
デバイス使用者への設定情報表示 (*3)	—	○	○	○	—
デバイス情報取得設定	インストールアプリ情報	—	○	○	○
	プロファイル情報	—	○	—	○
操作ログ取得設定	電話利用ログ	—	○	○	—
	デバイス活用ログ	—	○	—	—
	アプリ利用ログ	—	—	○ (*4)	—
	環境変更操作ログ	—	—	○	—
位置情報ログ取得設定	—	○	○	○ (*5)	—
デバイスへの通知設定	LANSCOPE Client 停止時の起動通知	—	○	—	—
	資産アラートの通知	—	—	○ (*6)	—

設定	共通	iOS	Android	Windows	macOS
操作アラートの通知	—	—	○ (*6) (*7)	—	—
アンインストール防止設定	—	—	—	○	○
パスワードポリシー設定	—	○	○ (*8) (*9)	—	○
マルチユーザー機能制御	—	—	○ (*8)	—	—

*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。位置情報ログを取得するための設定ではありません。

*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：LANSCOPE Client 側で、環境設定で設定されている内容を確認できます。

*4：アプリを禁止設定する場合、アプリ利用ログは「取得する」に設定してください。詳細は、[アプリの利用を禁止するときに必要な設定をする](#)を参照してください。

*5：Windows Server OS は、位置情報取得機能に未対応です。

*6：事前にアラートに設定するためのレシピ作成が必要です。詳細は、[アラート設定の流れ](#)を参照してください。

*7：アプリを禁止設定する場合、「操作アラートの通知」の「不許可・禁止したアプリが実行された」を「通知する」に設定してください。詳細は、[アプリの利用を禁止するときに必要な設定をする](#)を参照してください。

*8：Android Enterprise デバイスには適用できません。Android Enterprise デバイスに適用するポリシーは、[ルール] > [Android Enterprise 設定] で設定します。詳細は、An-347「Android Enterprise 利用ガイド」を参照してください。

*9：Android 10 以上のデバイスには適用されません。

4. [保存] をクリックします。

PC 操作ログ設定をする

Windows

Windows デバイスの制御に必要な操作ログの取得設定をします。

注意

取得した操作ログは、閲覧できません。

1. [ルール] の [デバイス設定] > [PC 操作ログ設定] をクリックします。



2. デバイスグループをクリックし、[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。

各設定は項目タブをクリックして切り替えます。



通信機器接続

通信機器（Wi-Fi/Bluetooth）のへの接続を禁止に設定できます。

アプリ禁止

プログラム名/ハッシュ値でアプリの起動を禁止できます。

注意

ストアアプリで実行ファイル名（EXE）が「WWAHost.exe」の場合だけ、実行ファイル名ではなくアプリ名を指定してください。実行ファイル名が「WWAHost.exe」のストアアプリが複数あるためです。

指定できるアプリ名は、[リスト] > [アプリ] に表示される「アプリ」と同じです。

省電力

Windowsの省電力設定ができます。

対象のデバイスに省電力のルールを適用すると、電源オプションの電源プランは「in-house power saving」に変更されます。

6-2 Apple サービス設定をする

iOS

macOS

iOS/macOS デバイスの管理に必要な設定をします。



- MDM 証明書設定

- [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。

- iOS 設定

- DEP 設定をする

自動デバイス登録 (DEP) を利用するために必要な設定をします。詳細は、An-353「Apple Business Manager 利用ガイド」を参照してください。

- VPP 設定をする

アプリの一括配信 (VPP) を利用するために必要な設定をします。詳細は、An-353「Apple Business Manager 利用ガイド」を参照してください。

- [iOS デバイスにアプリを配信する](#)

- [アプリ配信設定を利用する](#)

iOS デバイスのアプリ配信に必要な設定をします。

- [アプリカタログを利用する](#)

管理者がアプリカタログに公開したアプリを、利用者は必要なアプリを任意のタイミングで iOS デバイスにインストールできます。iOS デバイスに LANSCOPE Client をインストールしない場合、Web クリップを利用します。

- macOS 設定

- DEP 設定をする

自動デバイス登録 (DEP) を利用するために必要な設定をします。詳細は、An-353「Apple Business Manager 利用ガイド」を参照してください。

- [macOS デバイスにアプリを配信する](#)

macOS デバイスのアプリ配信に必要な設定をします。

- パスワード一括変更設定をする

自動デバイス登録 (DEP) を利用して管理している macOS デバイスのパスワードを一括で変更できます。詳細は、An-353「Apple Business Manager 利用ガイド」を参照してください。

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。MDM 証明書の有効期限が切れる 30 日前から、管理コンソールに有効期限切れのメッセージが表示されます。

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。DEP (Device Enrollment Program) を利用している場合、デバイスの初期化が必要です。
- MDM 証明書登録用の Apple ID が必要です。次の Apple ID とは別の Apple ID を準備してください。
 - Apple Business Manager のログインに利用している管理対象 Apple ID
 - iOS デバイスに LANSCOPE Client をインストールするための Apple ID

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。

MDM 証明書の登録・更新

MDM 証明書は、iOS デバイス または Mac デバイスを LANSCOPE で管理するために必要となる証明書です。
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。

注意事項
Apple ID を紛失して MDM 証明書を更新できなくなった場合は、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。

- ### 1 CSR ファイルのダウンロード

ベンダー署名付き CSR ファイルをダウンロードします。
追加でベンダー署名付き CSR ファイルが必要な場合は、MDM 証明書を保存したあとにダウンロードしてください。

[ダウンロード](#)
- ### 2 MDM 証明書ファイルの作成 および ダウンロード

手順 1 でダウンロードしたベンダー署名付き CSR ファイルを使用し、
Apple 管理サイト Apple Push Certificates Portal にて MDM 証明書を作成 および ダウンロードします。

[Apple Push Certificates Portal](#)

Apple Push Certificates Portal でのダウンロード手順はこちらをご確認ください。
[マニュアル](#)
- ### 3 MDM 証明書ファイルのアップロード

手順 2 でダウンロードした MDM 証明書をアップロードします。
ファイルの読み込みが完了すると、有効期限が表示されます。

[ファイル選択](#)
- ### 4 有効期限通知メールの設定

有効期限が切れる前にメールで通知する

計 4 回（期日の 30 日前 / 7 日前 / 前日 / 当日）設定したメールアドレス宛に送信されます。
（送信元アドレス：an_report2@LANSCOPE.onmicrosoft.com）

[通知先メールアドレス *](#)

[テスト送信](#)
- ### 5 Apple ID や電話番号などの設定

MDM 証明書を更新するには、登録時に使用した Apple ID が必要です。
Apple ID や 2 ファクタ認証で使用している電話番号など、メモしておくことをおすすめします。

例) Apple ID : sample@motex.co.jp 電話番号 : 09012345678

[メモ](#)

Apple ID : sample@motex.co.jp パスワード : sample123

[閉じる](#) [保存](#)

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。

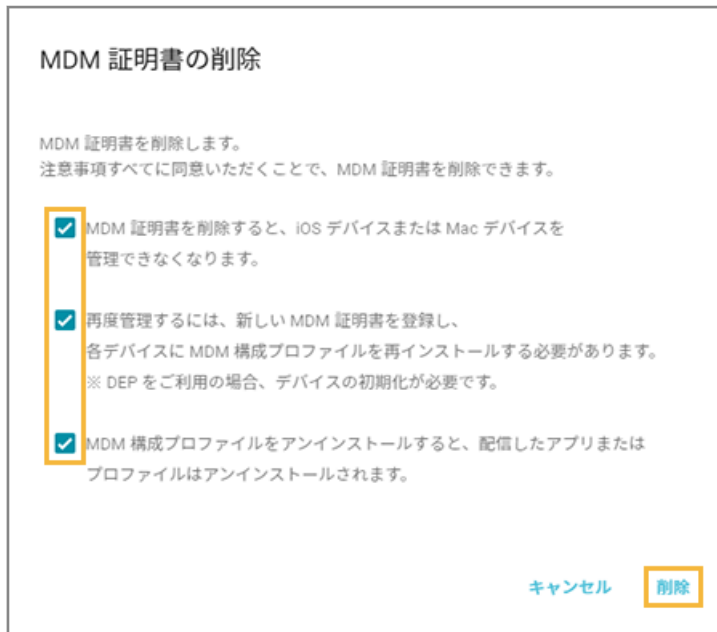
1. [ルール] の [Apple サービス設定] > [MDM 証明書設定] をクリックします。



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。



iOS デバイスにアプリを配信する

iOS

iOS デバイスにアプリを配信します。

アプリ配信の方法

エンドポイントマネージャーでのアプリ配信の方法は、次のとおりです。

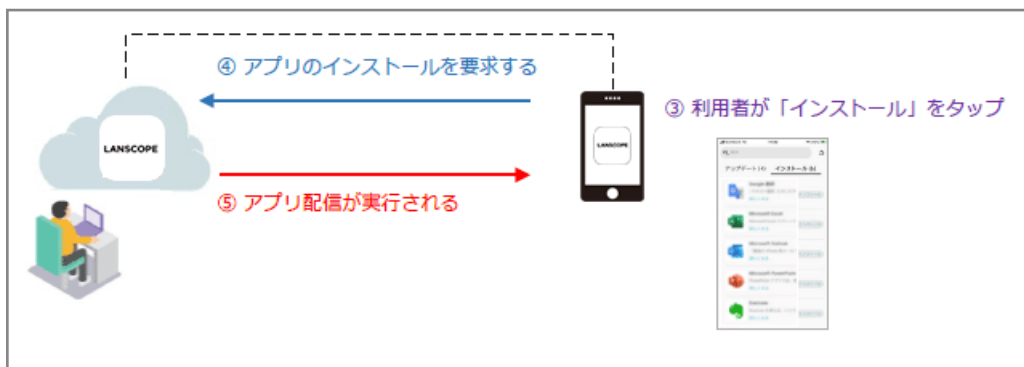
アプリ配信設定を利用する

管理者からアプリを配信します。利用者が「インストール」をタップすると、アプリがインストールされます。



アプリカタログを利用する

管理者がアプリカタログに公開したアプリを、利用者は必要なアプリを任意のタイミングでインストールできます。



アプリ配信/VPP アプリ配信

iOS デバイスに、「App Store に公開されている無償アプリ（以下、App Store アプリ（無償）」「In-House（自社開発）アプリ」を配信し、デバイス使用者にインストールを促すことができます。また、配信したアプリのアンインストールもできます。

VPP 機能を利用すると、「VPP ストアで購入したアプリ」の配信/アンインストールができます。詳細は、An-353「Apple Business Manager 利用ガイド」を参照してください。

機能と配信方式	アプリ配信機能		VPP アプリ配信機能 デバイスベース方式
対応 OS バージョン	iOS 12 以上/iPadOS 13 以上		iOS 12 以上/iPadOS 13 以上
配信対象	App Store アプリ（無償）	In-House（自社開発）アプリ	VPP アプリ（有償/無償）
Apple ID	必要	不要	不要
App Store が禁止されている場合のアプリ配信（*1）	可（*2）	可	可
サイレントインストール	不可 Apple ID 入力のダイアログが表示される	可 「監視モード」の設定が必要（*3）	可 「監視モード」の設定が必要（*3）

*1：プロファイルで「App Store」の使用を許可していない（アプリのインストールを禁止している）場合のアプリ配信です。

*2：バックグラウンドで起動している LANSCOPE Client などのアプリはアップデートできないことがあります。

*3：デバイスに「監視モード」を設定するには、Apple Configurator を利用して設定するか、自動デバイス登録（DEP）機能を利用して設定してください。DEP 機能を利用した場合、「監視モードに設定する」の項目を有効にした DEP プロファイルをデバイスに割り当て、アクティベーションしてください。

アプリ配信設定を利用する

iOS

iOS デバイスにアプリを配信します。

- [アプリ配信設定を追加する](#)
- [アプリ配信対象のデバイスを追加する](#)
- [デバイス側での操作](#)
- [アプリ配信結果を確認する](#)
- [登録したアプリを削除する](#)

アプリ配信設定を追加する

iOS

「App Store アプリ（無償）」を配信する場合と、「In-House（自社開発）アプリ」を配信する場合で、アプリ配信の流れが異なります。

■ App Store アプリ（無償）を配信する場合

ステップ：

1. [App Store アプリ（無償）の情報を登録／更新する](#)
2. [Managed App Configuration の設定を追加／更新する](#)
3. [アプリを配信／アンインストールする](#)

ステップ 1： App Store アプリ（無償）の情報を登録／更新する

App Store アプリ（無償）の情報を登録する

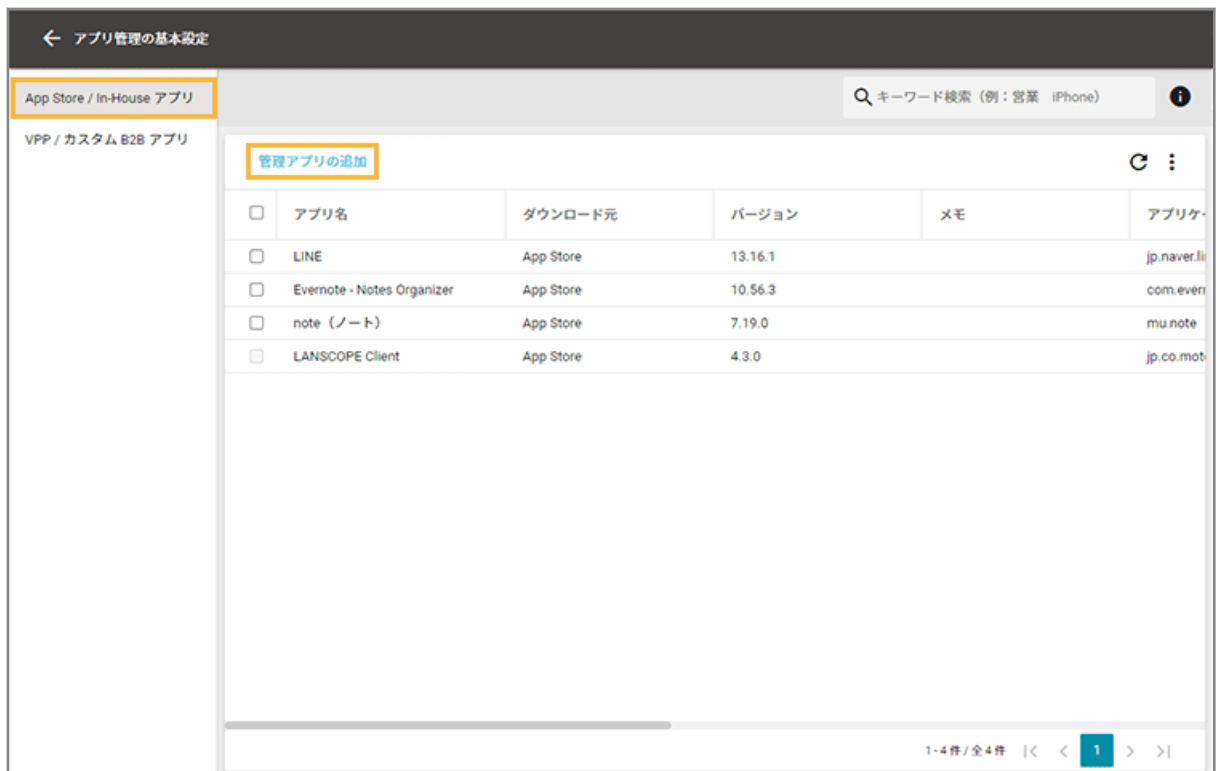
1. **【ルール】** の **【Apple サービス設定】** > **【iOS 設定】** をクリックします。



2. **【基本設定】** をクリックします。



3. [App Store/In-House アプリ] をクリックし、[管理アプリの追加] をクリックします。



4. [App Store] をクリックします。



5. アプリ名/アプリ ID/キーワードなどで配信するアプリを検索し、アプリをクリックします。



→ 選択したアプリの基本情報が表示されます。

6. 必要に応じてメモを入力し、[保存] をクリックします。



→ アプリが追加されます。

App Store アプリ（無償）の情報を更新する

App Store に新しいバージョンのアプリが公開された場合、管理コンソールに登録しているアプリも最新バージョンに更新します。

ポイント

管理コンソールのアプリを更新すると、古いバージョンのアプリを使用しているデバイスを確認できます。詳細は、[アプリ配信結果を確認する](#)を参照してください。

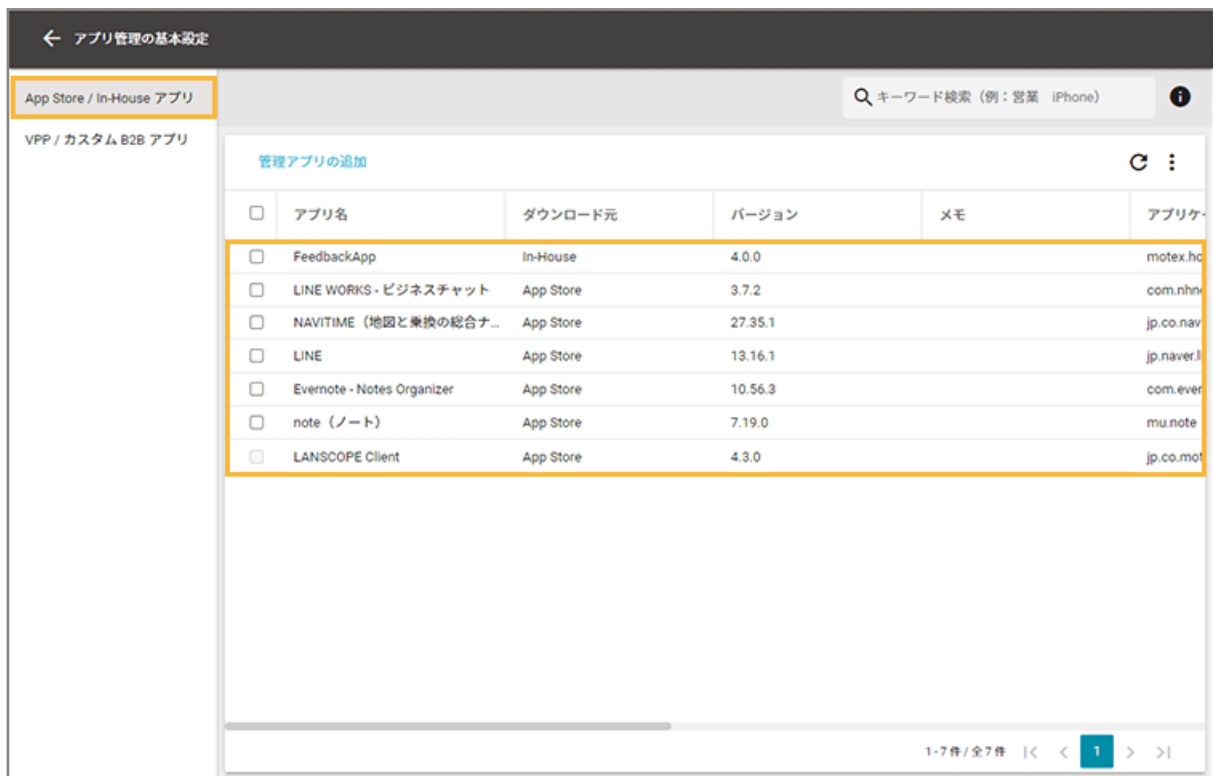
1. **【ルール】** の **【Apple サービス設定】** > **【iOS 設定】** をクリックします。



2. **【基本設定】** をクリックします。



3. **【App Store/In-House アプリ】** をクリックし、**アプリ** をクリックします。



4. **【編集】** をクリックします。



5. [取得] をクリックします。



→ アプリのバージョンが更新されます。

6. [保存] をクリックします。

ステップ 2 : Managed App Configuration の設定を追加／更新する

アプリを利用するときに必要な設定をあらかじめ追加する場合は、Managed App Configuration の設定をします。追加／更新した設定は、アプリのインストール時にデバイスに適用されます。

LANSCOPE Client を配信する場合は、すでに Managed App Configuration が設定されているため、この手順は必要ありません。

注意

- Managed App Configuration の設定項目に入力する情報は、アプリの開発元に確認してください。
- デバイスにインストールしたあとのアプリの動作は、アプリの開発元に確認してください。
- Managed App Configuration の設定が適用されたデバイスをバックアップ／復元すると、Managed App Configuration の設定は解除されます。

Managed App Configuration の設定を追加する

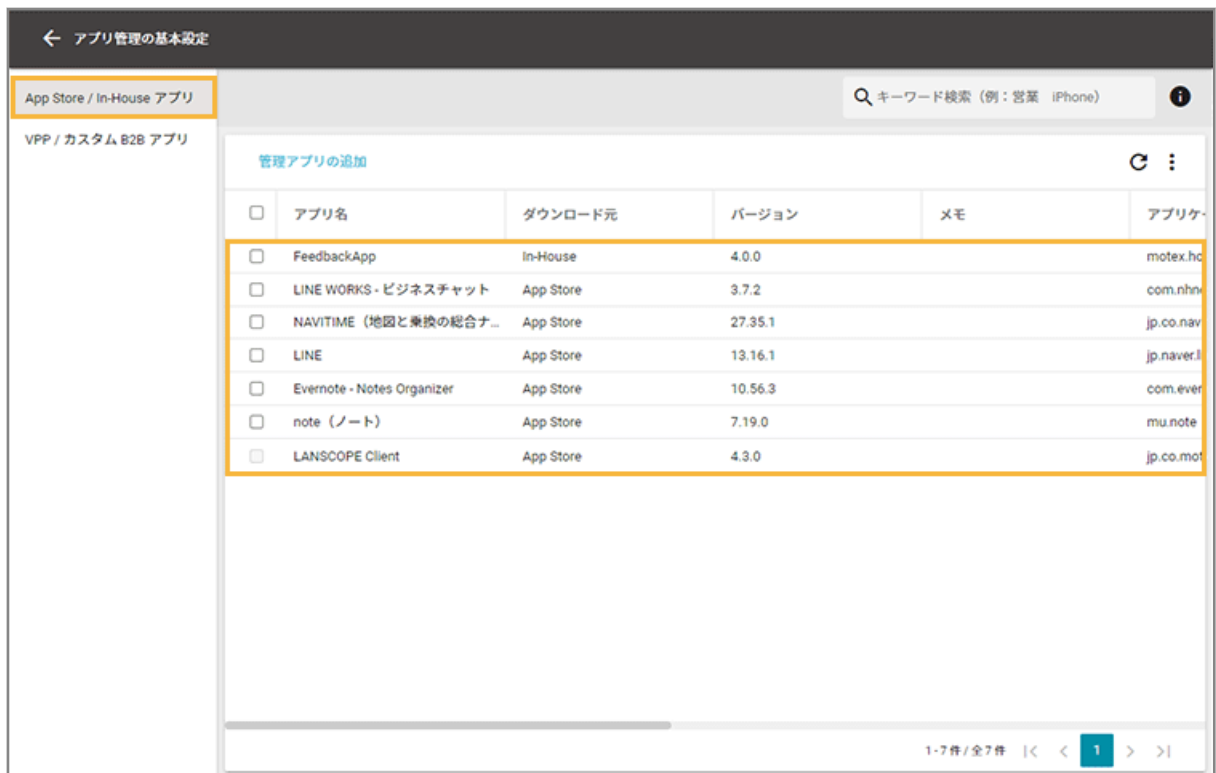
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



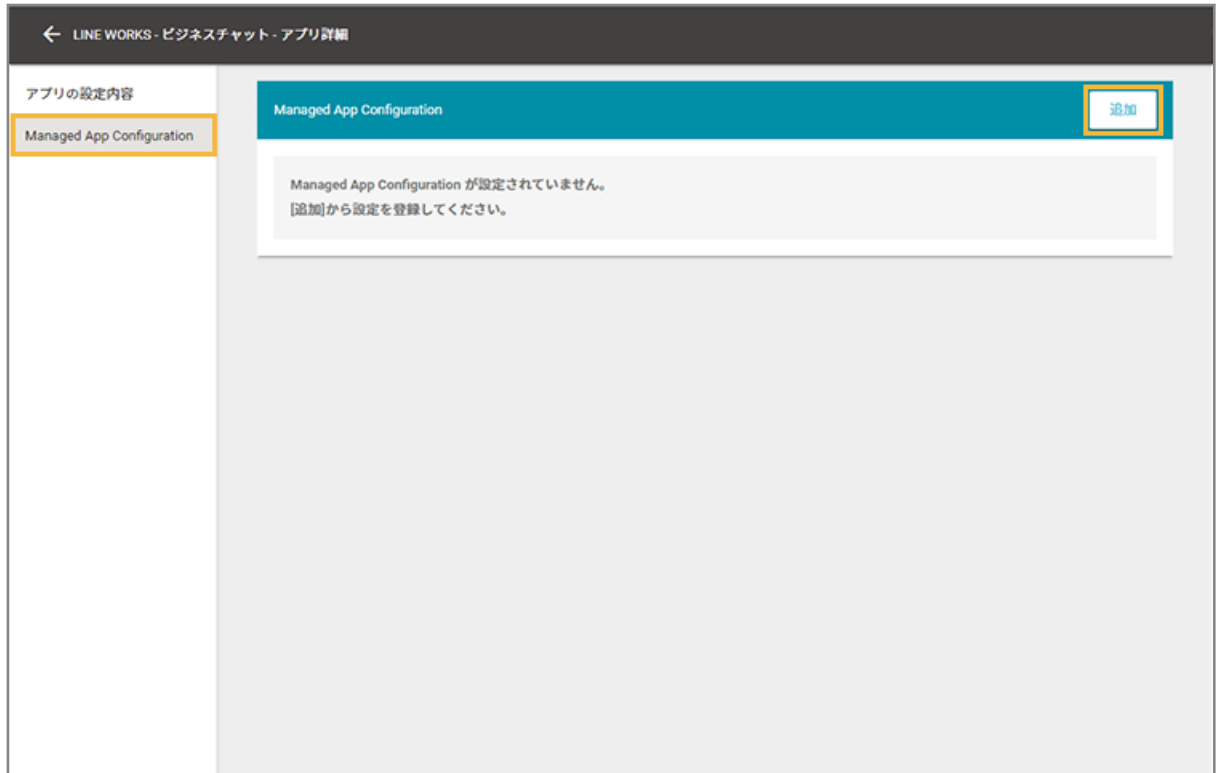
2. [基本設定] をクリックします。



3. [App Store/In-House アプリ] をクリックし、アプリをクリックします。

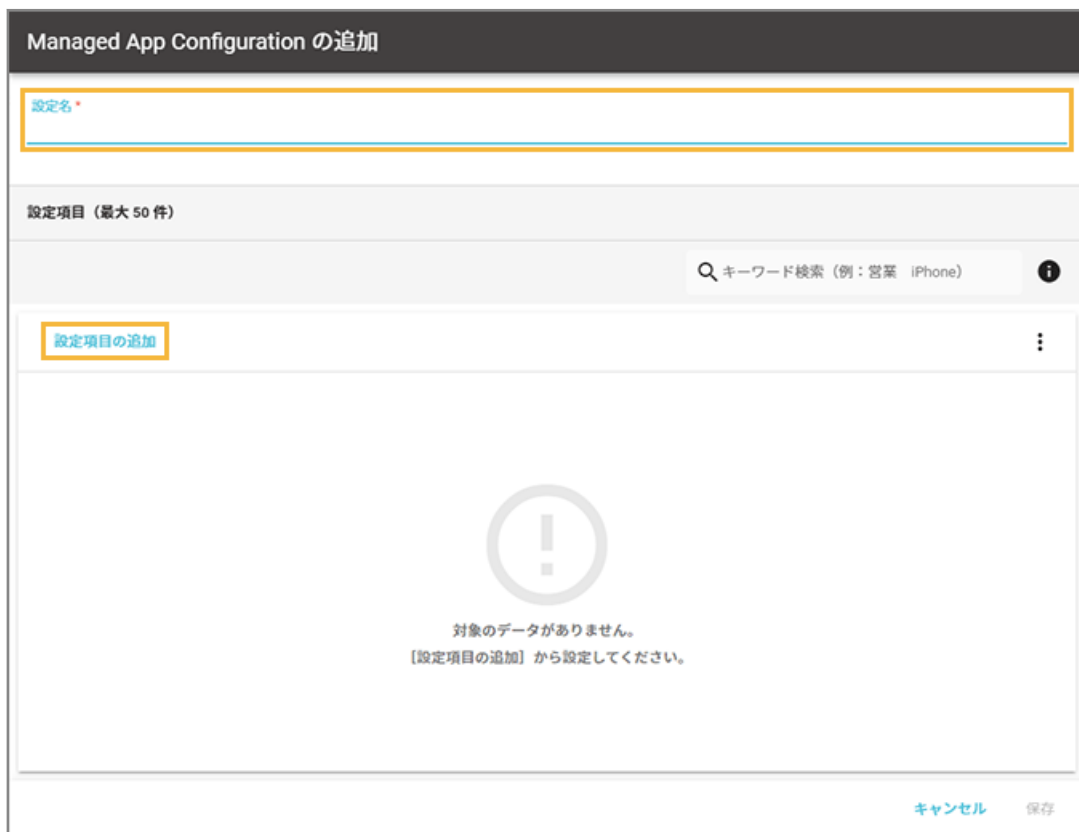


4. [Managed App Configuration] をクリックし、[追加] をクリックします。



5. 設定名を入力し、[設定項目の追加] をクリックします。

⋮ の [インポート] で、一括で追加できます。



6. キー名／値の種類／値を入力します。

← 設定項目の追加

パスワードなど重要な情報を設定するのは避けてください。

キー名 *

メモ

値の種類
文字列

値 *

キャンセル 保存

キー名

アプリの開発元に確認した情報を入力します。入力できる文字数は、80文字以内です。

値の種類

入力する値の種類を選択します。

値

アプリの開発元に確認した情報を入力します。入力できる文字数は、1,000文字以内です。配列の場合、追加できる値は10個以内で、1つの値に入力できる文字数は、100文字以内です。

7. [保存] をクリックします。

→ 「Managed App Configuration の追加」画面に戻ります。

8. 内容を確認し、[保存] をクリックします。

Managed App Configuration の追加

設定名 *
[全社用]ログイン制御設定

設定項目 (最大 50 件)

🔍 キーワード検索 (例: 営業 iPhone) ⓘ

設定項目の追加 ⋮

<input type="checkbox"/>	キー名	値の種類	値 1	値 2
<input type="checkbox"/>	LineworksAuthCode	文字列	xlHD5IU6B8Rwxy	

キャンセル **保存**

→ Managed App Configuration の設定が保存されます。

Managed App Configuration の設定を更新する

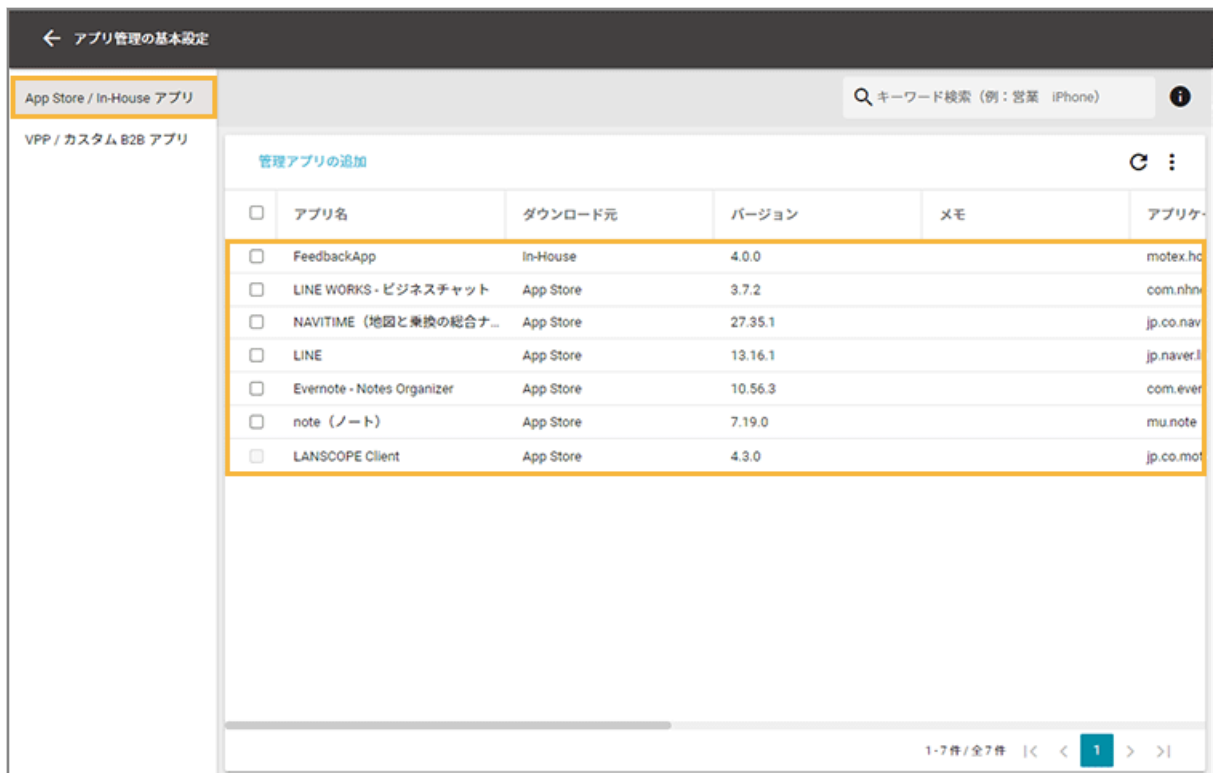
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。




2. [基本設定] をクリックします。

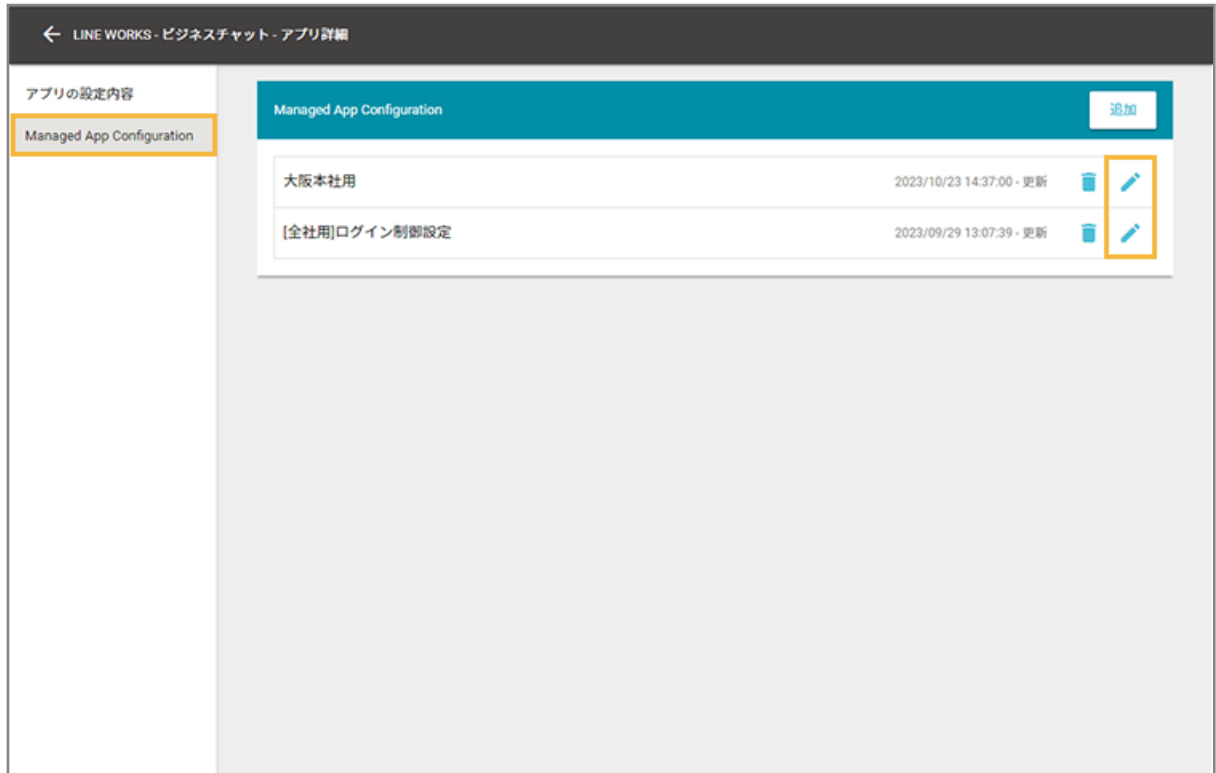


3. [App Store/In-House アプリ] をクリックし、アプリをクリックします。




4. [Managed App Configuration] をクリックし、 をクリックします。

設定を削除する場合は、 をクリックします。



5. 設定項目をクリックします。

- 設定項目を追加する場合は、[設定項目の追加] をクリックします。
- 設定項目を削除する場合は、設定項目をチェックし、[削除する] をクリックします。
-  の [インポート] で、一括で追加/編集できます。

Managed App Configuration の編集

設定名 *
[全社用]ログイン制御設定

設定項目 (最大 50 件)

🔍 キーワード検索 (例: 営業 iPhone) ⓘ

設定項目の追加 ⋮

<input type="checkbox"/>	キー名	値の種類	値 1	値 2
<input type="checkbox"/>	パスワード	文字列	パスワード	

キャンセル 保存

6. キー名/値の種類/値を編集します。

← 設定項目の編集

パスワードなど重要な情報を設定するのは避けてください。

キー名 *
パスワード

メモ

値の種類
文字列

値 *
パスワード

キャンセル 保存

キー名

アプリの開発元に確認した情報を入力します。入力できる文字数は、80文字以内です。

値の種類

入力する値の種類を選択します。

値

アプリの開発元に確認した情報を入力します。入力できる文字数は、1,000文字以内です。配列の場合、追加できる値は10個以内で、1つの値に入力できる文字数は、100文字以内です。

7. [保存] をクリックします。

→ 「Managed App Configuration の編集」画面に戻ります。

8. 内容を確認し、[保存] をクリックします。

設定項目の追加	キー名	値の種類	値 1	値 2
<input type="checkbox"/>	キー名	値の種類	値 1	値 2
<input type="checkbox"/>	[Redacted]	文字列	[Redacted]	[Redacted]

→ Managed App Configuration の設定が保存されます。

ステップ 3： アプリを配信／アンインストールする

ここでは、デバイスにアプリを配信する場合を例に説明します。

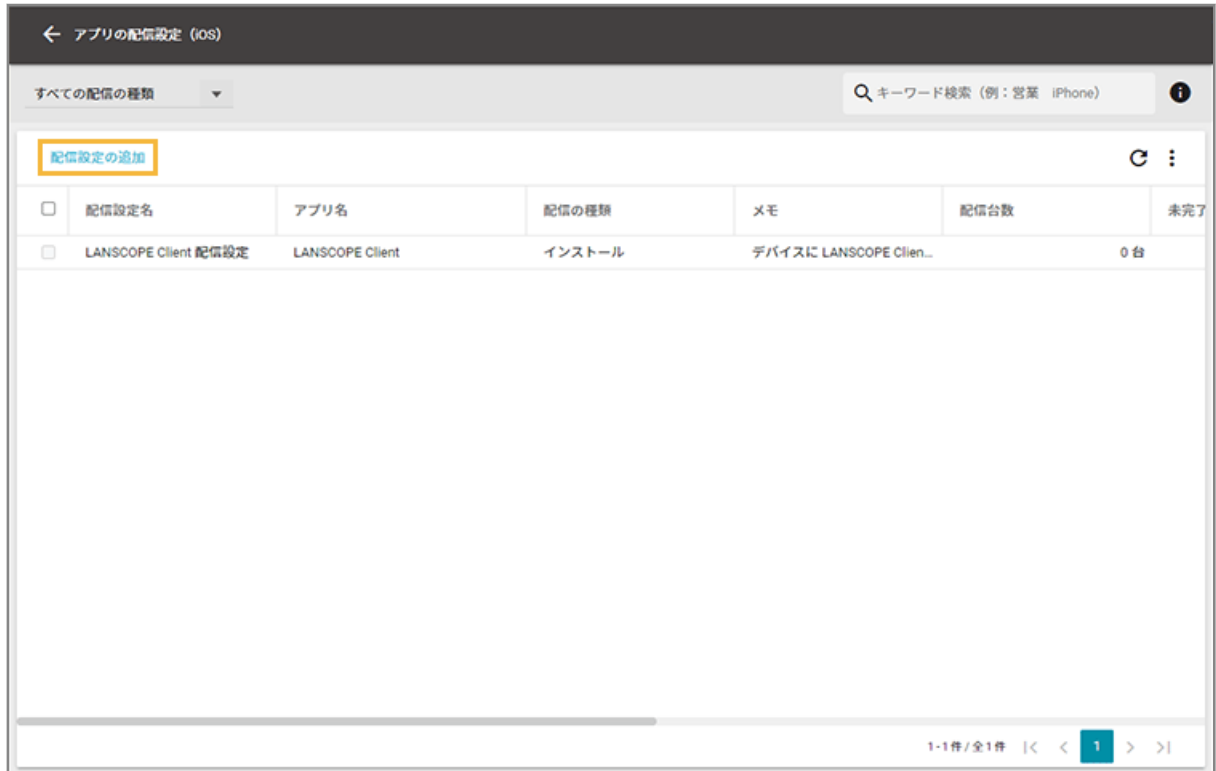
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



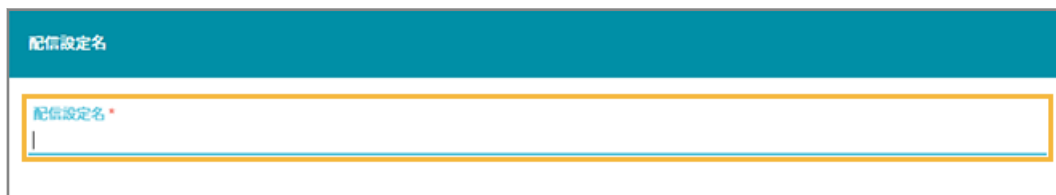
2. [アプリ配信設定] をクリックします。



3. [配信設定の追加] をクリックします。



4. 配信設定名を入力します。



5. [インストール] を選択し、[App Store/In-House アプリを選択] をクリックします。

アプリをアンインストールする場合は、[アンインストール] を選択します。



6. アプリをチェックし、[選択する] をクリックします。



→ 配信アプリが追加されます。

7. Managed App Configuration を設定する場合は、次の操作をします。

(1) [Managed App Configuration の選択] をクリックします。



(2) 設定する Managed App Configuration の [選択] をクリックします。



→ Managed App Configuration の設定が追加されます。

8. MDM 構成プロファイルのインストール後に自動配信する場合は、[MDM 構成プロファイルがインストールされたら配信する] をチェックし、対象のデバイスグループを選択します。



9. 必要に応じてメモを入力し、[保存] をクリックします。

→ アプリ配信設定の追加が完了します。

■ In-House（自社開発）アプリを配信する場合

In-House（自社開発）アプリには、プロビジョニングプロファイルが含まれています。プロビジョニングプロファイルには有効期限があり、1年ごとに更新が必要です。有効期限が切れると、In-House（自社開発）アプリを利用できなくなるため、次のいずれかの方法でデバイスのプロビジョニングプロファイルを更新してください。

- [In-House（自社開発）アプリの情報を更新して、デバイスに配信する](#)
- [プロビジョニングプロファイルを更新して、デバイスに配信する](#)

有効期限の確認方法は、[プロビジョニングプロファイルの有効期限を確認する](#)を参照してください。

ステップ：

1. [In-House（自社開発）アプリの情報を登録／更新する](#)
2. [Managed App Configuration の設定を追加／更新する](#)
3. [アプリを配信／アンインストールする](#)

ステップ 1 : In-House (自社開発) アプリの情報を登録/更新する

In-House (自社開発) アプリの登録/更新には、「マニフェストファイル」と「アプリファイル」を利用します。

注意

マニフェストファイル (拡張子 : .plist)

「manifest.plist」ファイルに記載される「Display Image URL」と「Full Size Image URL」の値には、接続できる URL を設定してください。

アプリファイル (拡張子 : .ipa)

アプリファイルのファイルサイズが 4GB を超える In-House (自社開発) アプリは登録できません。

In-House (自社開発) アプリの情報を登録する

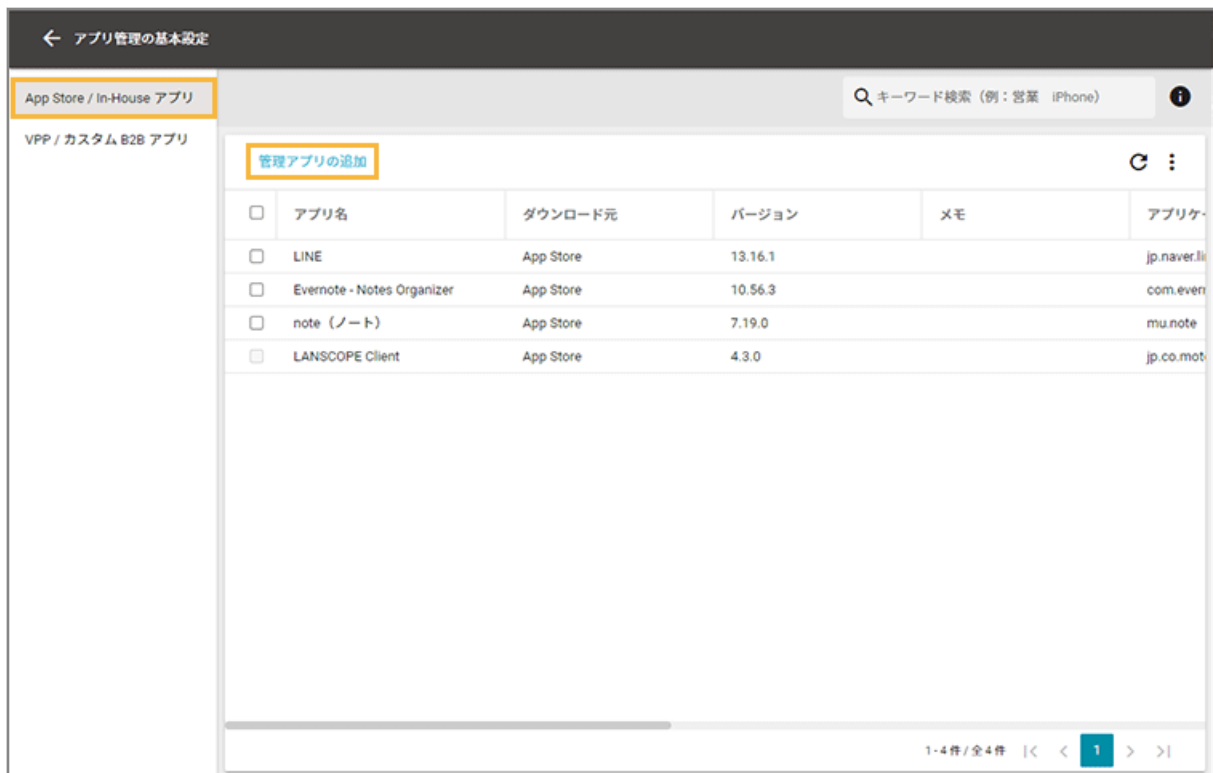
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



2. [基本設定] をクリックします。



3. [App Store/In-House アプリ] をクリックし、[管理アプリの追加] をクリックします。



4. [In-House] をクリックします。



5. マニフェストファイルとアプリファイルをアップロードします。



(1) マニフェストファイルの [ファイルアップロード] をクリックし、ファイルを選択します。

ポイント

Xcode9 で In-House (自社開発) アプリを開発した場合、「manifest.plist」ファイルを選択してください。

→ 基本情報が表示されます。

(2) アプリファイルの [ファイルアップロード] をクリックし、ファイルを選択します。

→ 基本情報の「ファイルサイズ」と「有効期限」が表示されます。

6. 必要に応じてメモを入力し、[保存] をクリックします。

← In-House アプリの追加

アプリ情報の取得

マニフェストファイル

manifest.plist

アプリファイル

FeedbackApp.ipa

基本情報

アプリ名
FeedbackApp

アプリケーションID
motex.hoshino.test

バージョン
4.0.0

カテゴリ
software

ファイルサイズ
49.66 KB

有効期限
2023/11/11 12:57:57

アプリカタログ設定

説明

アプリカタログに表示する説明を入力します。

アイコン
アプリカタログに表示するアイコンを選択します。
インストール後はアプリファイル内に設定されているアイコンが表示されます。
※推奨サイズ 180px x 180px

メモ

→ アプリが追加されます。

In-House（自社開発）アプリの情報を更新する

配信した In-House（自社開発）アプリをアップデートする場合、登録時と同じ「アプリケーション名」「アプリケーション ID」のファイルで更新します。

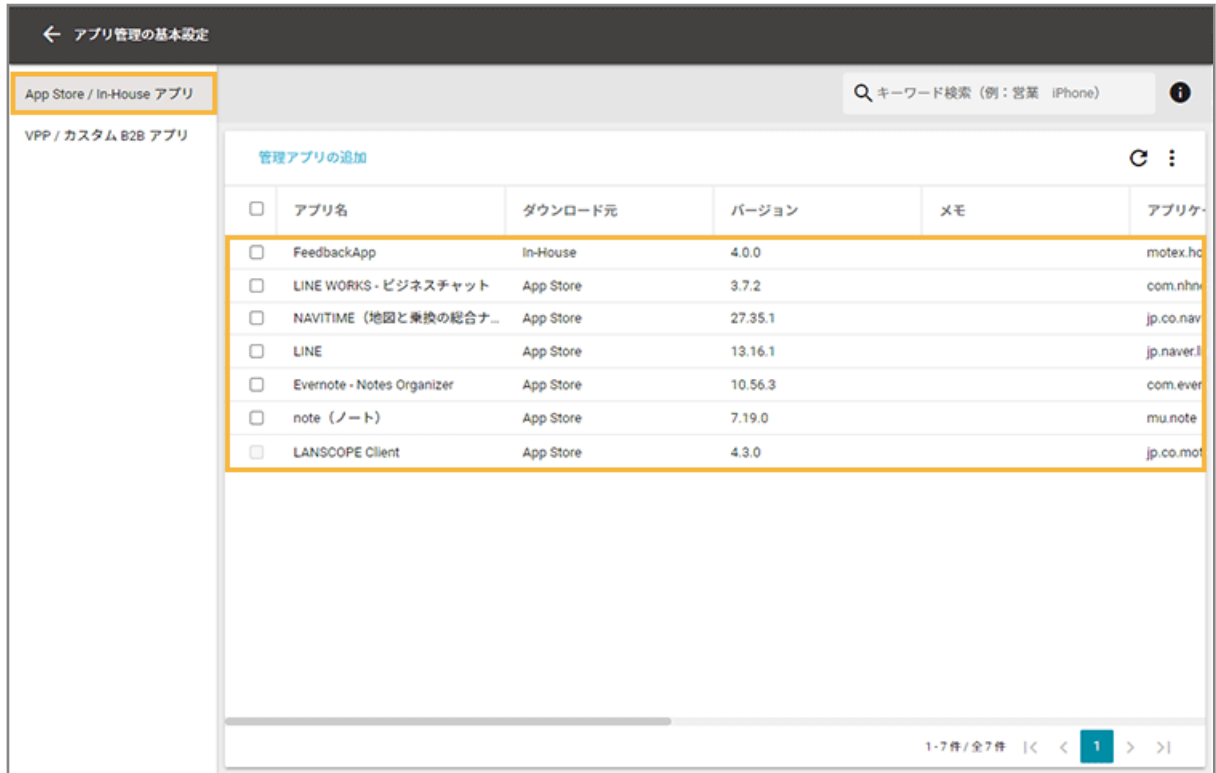
1. **【ルール】** の **【Apple サービス設定】** > **【iOS 設定】** をクリックします。



2. **【基本設定】** をクリックします。



3. **【App Store/In-House アプリ】** をクリックし、**アプリ** をクリックします。



4. [編集] をクリックします。



5. マニフェストファイルとアプリファイルを更新します。



(1) マニフェストファイルの [ファイルアップロード] をクリックし、ファイルを選択します。

ポイント

Xcode9 で In-House（自社開発）アプリを開発した場合、「manifest.plist」ファイルを選択してください。

→ 基本情報が更新されます。

(2) アプリファイルの [ファイルアップロード] をクリックし、ファイルを選択します。

→ 基本情報の「ファイルサイズ」と「有効期限」が更新されます。

6. [保存] をクリックします。



ステップ 2 : Managed App Configuration の設定を追加／更新する

アプリを利用するときに必要な設定をあらかじめ追加する場合は、Managed App Configuration の設定をします。追加／更新した設定は、アプリのインストール時にデバイスに適用されます。

注意

- Managed App Configuration の設定項目に入力する情報は、アプリの開発元に確認してください。
- デバイスにインストールしたあとのアプリの動作は、アプリの開発元に確認してください。
- Managed App Configuration の設定が適用されたデバイスをバックアップ／復元すると、Managed App Configuration の設定は解除されます。

Managed App Configuration の設定を追加する

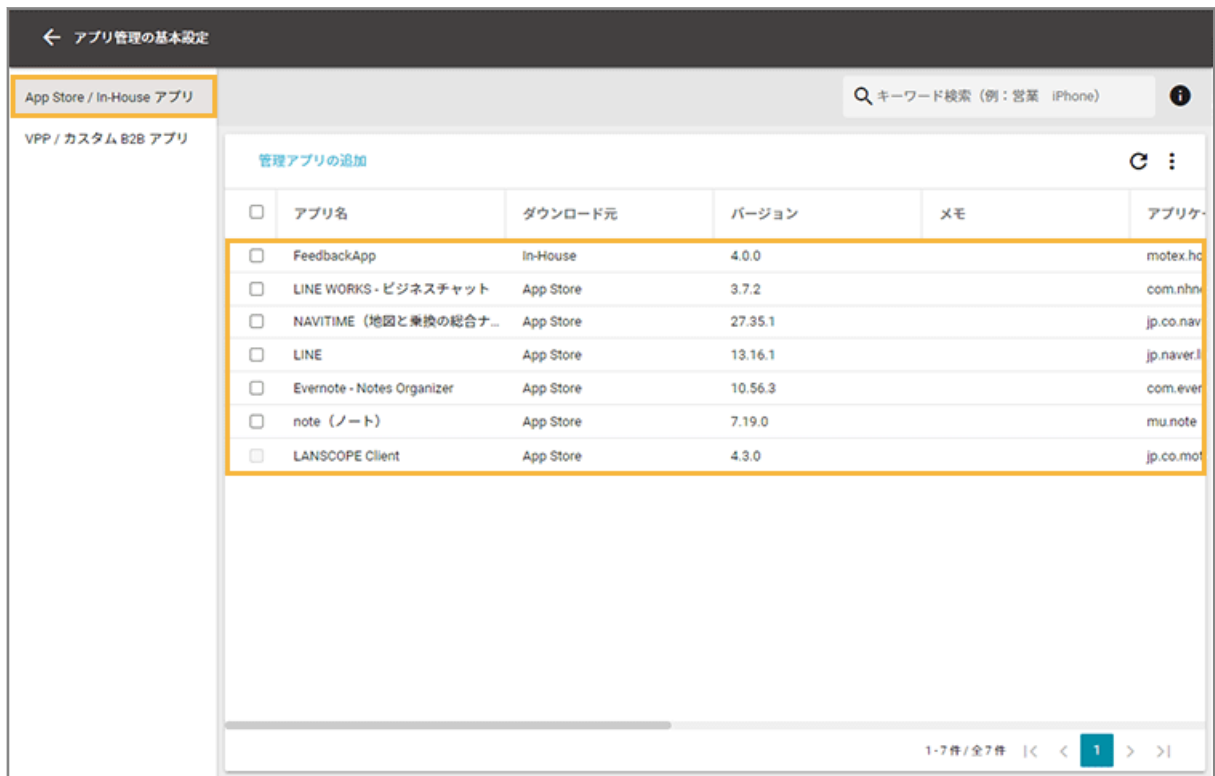
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



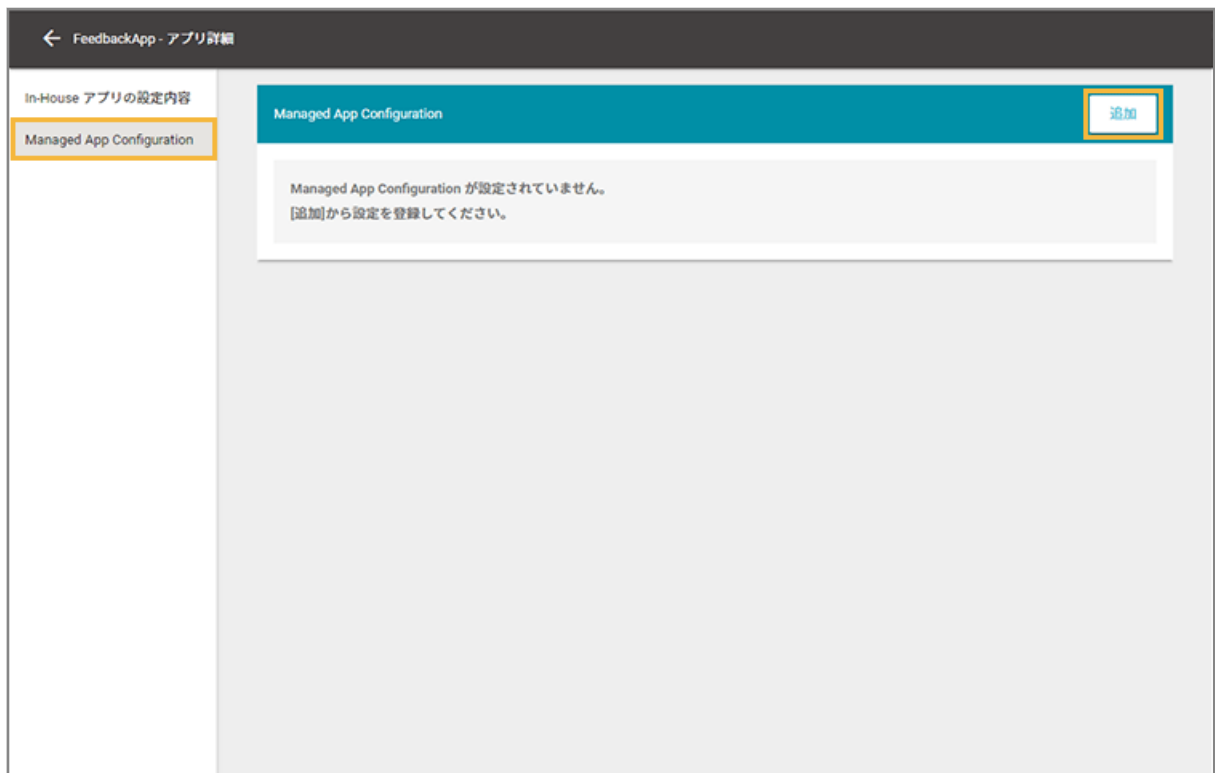
2. [基本設定] をクリックします。



3. [App Store/In-House アプリ] をクリックし、アプリをクリックします。



4. [Managed App Configuration] をクリックし、[追加] をクリックします。



5. 設定名を入力し、[設定項目の追加] をクリックします。

⋮ の [インポート] で、一括で追加できます。

Managed App Configuration の追加

設定名 *

設定項目 (最大 50 件)

キーワード検索 (例: 営業 iPhone)

設定項目の追加

対象のデータがありません。
【設定項目の追加】から設定してください。

キャンセル 保存

6. キー名/値の種類/値を入力します。

← 設定項目の追加

パスワードなど重要な情報を設定するのは避けてください。

キー名 *

メモ

値の種類
文字列

値 *

キャンセル 保存

キー名

アプリの開発元に確認した情報を入力します。入力できる文字数は、80 文字以内です。

値の種類

入力する値の種類を選択します。

値

アプリの開発元に確認した情報を入力します。入力できる文字数は、1,000 文字以内です。配列の場合、追加できる値は 10 個以内で、1 つの値に入力できる文字数は、100 文字以内です。

7. [保存] をクリックします。

→ 「Managed App Configuration の追加」画面に戻ります。

8. 内容を確認し、[保存] をクリックします。

キー名	値の種類	値 1	値 2
<input type="checkbox"/> LineworksAuthCode	文字列	xIHd5IU868Rwxy	

→ Managed App Configuration の設定が保存されます。

Managed App Configuration の設定を更新する

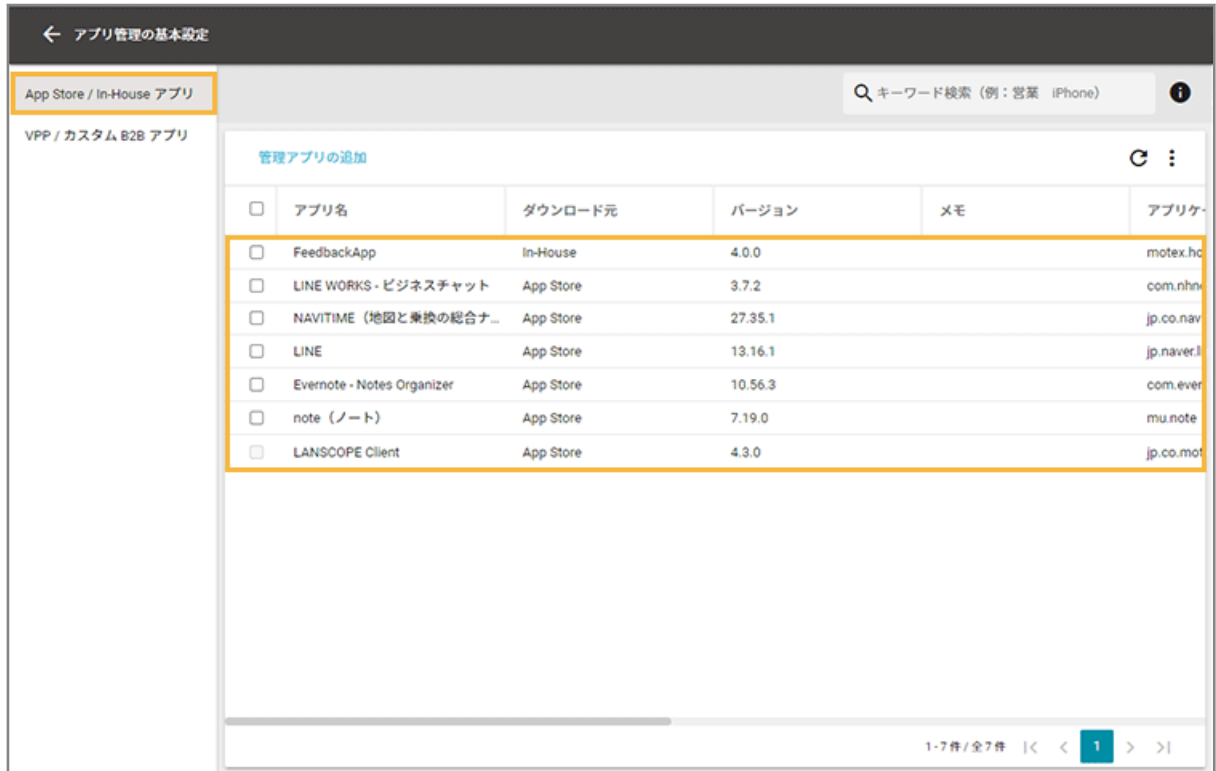
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。





2. [基本設定] をクリックします。

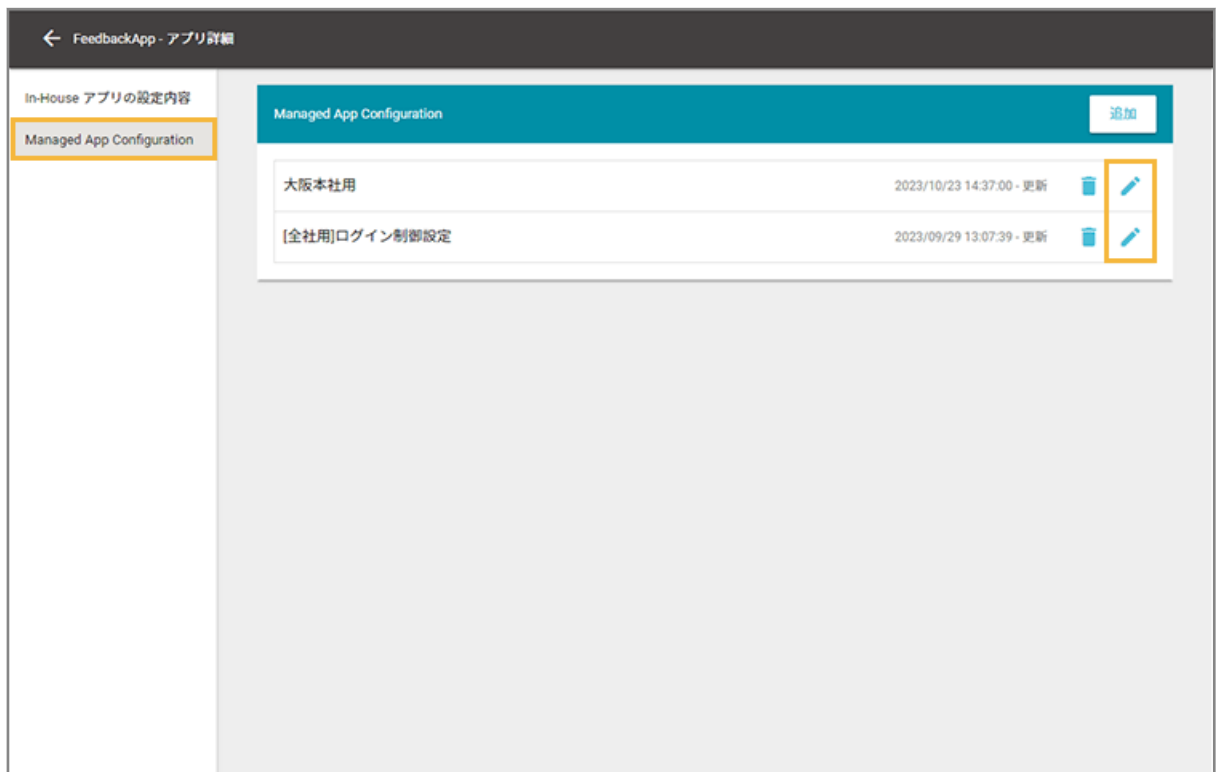


3. [App Store/In-House アプリ] をクリックし、アプリをクリックします。




4. [Managed App Configuration] をクリックし、 をクリックします。

設定を削除する場合は、 をクリックします。



5. 設定項目をクリックします。

- 設定項目を追加する場合は、[設定項目の追加] をクリックします。
- 設定項目を削除する場合は、設定項目をチェックし、[削除する] をクリックします。
-  の [インポート] で、一括で追加／編集できます。

Managed App Configuration の編集

設定名*
[全社用]ログイン制御設定

設定項目 (最大 50 件)

キーワード検索 (例: 営業 iPhone) ⓘ

設定項目の追加 ⓘ

<input type="checkbox"/>	キー名	値の種類	値 1	値 2
<input type="checkbox"/>	password_authentication	文字列	パスワード制御設定	

キャンセル 保存

6. キー名／値の種類／値を編集します。

キー名

アプリの開発元に確認した情報を入力します。入力できる文字数は、80文字以内です。

値の種類

入力する値の種類を選択します。

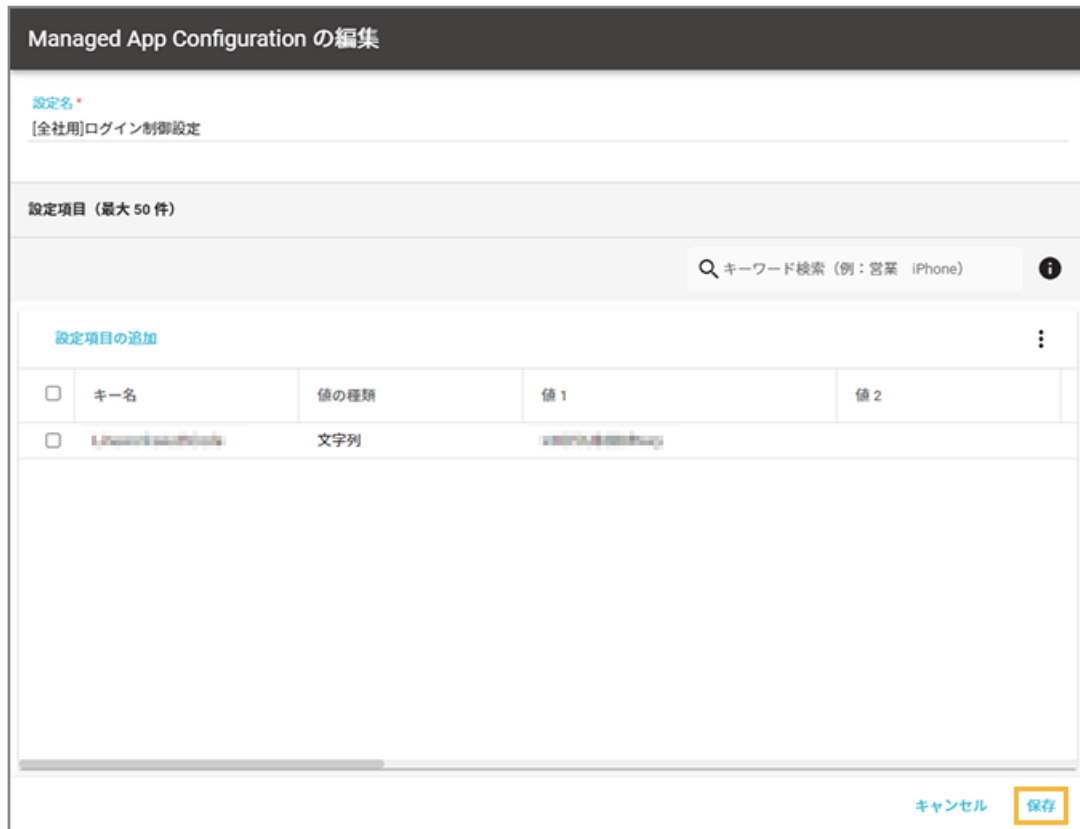
値

アプリの開発元に確認した情報を入力します。入力できる文字数は、1,000文字以内です。配列の場合、追加できる値は10個以内で、1つの値に入力できる文字数は、100文字以内です。

7. [保存] をクリックします。

→ 「Managed App Configuration の編集」画面に戻ります。

8. 内容を確認し、[保存] をクリックします。



→ Managed App Configuration の設定が保存されます。

ステップ 3： アプリを配信／アンインストールする

ここでは、デバイスにアプリを配信する場合を例に説明します。

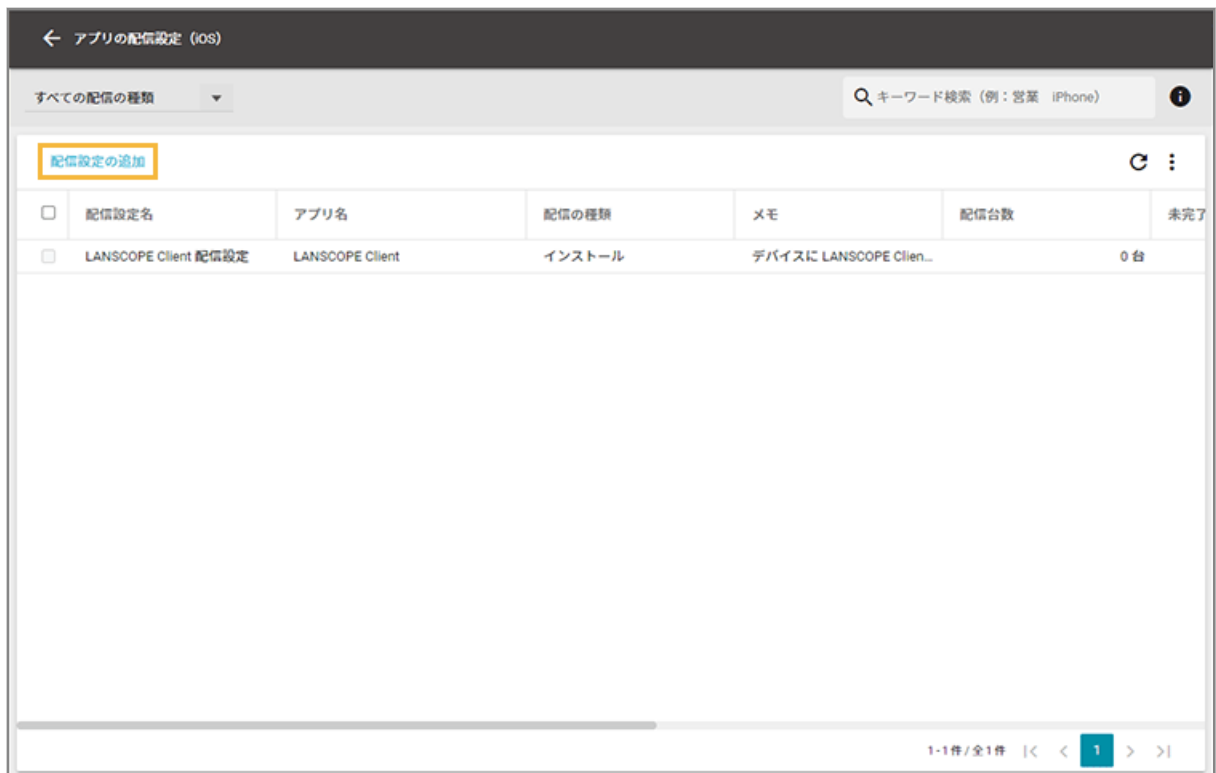
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



2. [アプリ配信設定] をクリックします。



3. [配信設定の追加] をクリックします。



4. 配信設定名を入力します。

配信設定名

配信設定名 *

5. **【インストール】** を選択し、**【App Store/In-House アプリを選択】** をクリックします。
 アプリをアンインストールする場合は、**【アンインストール】** を選択します。

アプリ配信設定

配信の種類

インストール
 アンインストール

配信アプリを選択
 選択できるアプリは最大10件です。

App Store / In-House アプリを選択 VPP / カスタム B2B アプリを選択

6. **アプリをチェックし、【選択する】** をクリックします。

App Store / In-House アプリを選択

キーワード検索 (例: 営業 iPhone) ⓘ

× 1件を選択中 管理アプリの追加 **選択する**

<input type="checkbox"/>	アプリ名	ダウンロード元	バージョン	メモ
<input checked="" type="checkbox"/>	FeedbackApp	In-House	4.0.0	
<input type="checkbox"/>	NAVITIME (地図と乗換の総合ナ...	App Store	27.35.1	
<input type="checkbox"/>	LINE	App Store	13.16.1	
<input type="checkbox"/>	Evernote - Notes Organizer	App Store	10.56.3	
<input type="checkbox"/>	note (ノート)	App Store	7.19.0	
<input type="checkbox"/>	LANSCOPE Client	App Store	4.3.0	

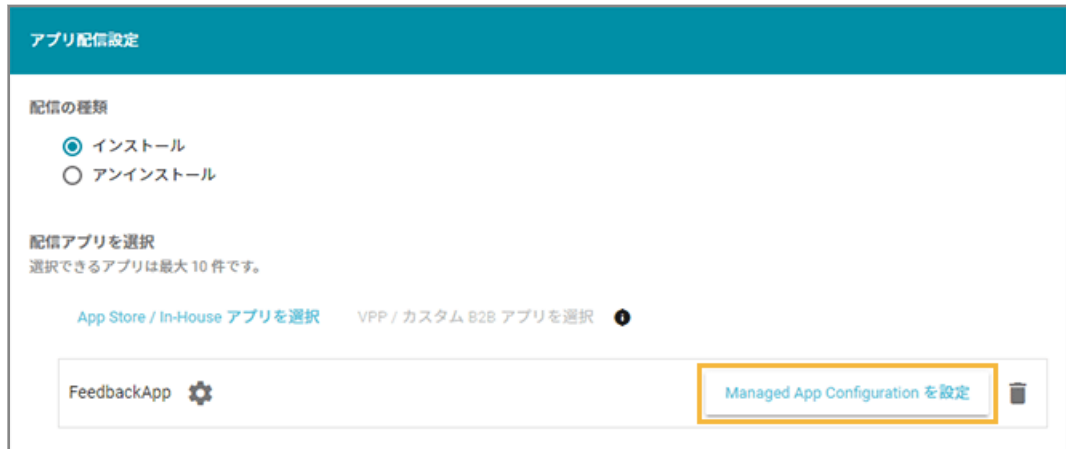
1-6件 / 全6件 < < 1 > >

閉じる

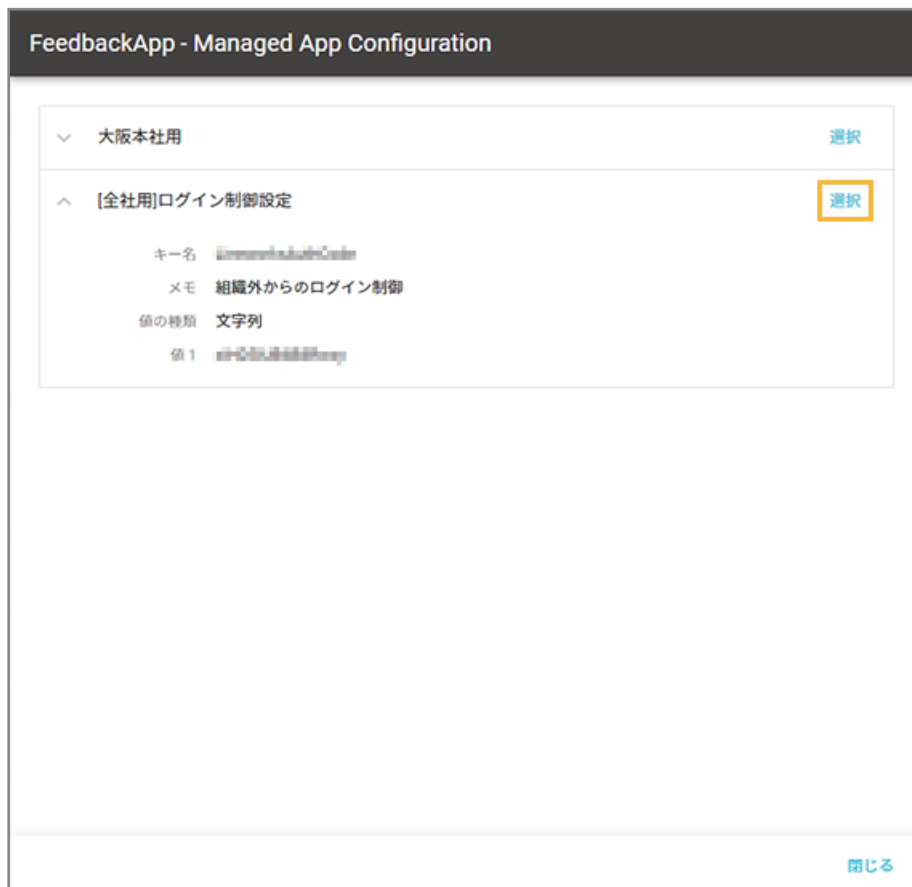
→ 配信アプリが追加されます。

7. **Managed App Configuration** を設定する場合は、次の操作をします。

(1) [Managed App Configuration の選択] をクリックします。



(2) 設定する Managed App Configuration の [選択] をクリックします。




→ Managed App Configuration の設定が追加されます。

8. MDM 構成プロファイルのインストール後に自動配信する場合は、[MDM 構成プロファイルがインストールされたら配信する] をチェックし、対象のデバイスグループを選択します。

オプション

MDM 構成プロファイルがインストールされたら配信する

対象グループを選択*

 デバイスグループ (0 件)

9. 必要に応じてメモを入力し、[保存] をクリックします。

← 配信設定の追加 (iOS)

配信設定名

配信設定名*

配信設定




アプリ配信設定

配信の種類

インストール
 アンインストール

配信アプリを選択
選択できるアプリは最大 10 件です。


App Store / In-House アプリを選択 VPP / カスタム B2B アプリを選択 ⓘ


FeedbackApp  [全社用]ログイン制御設定  

オプション

MDM 構成プロファイルがインストールされたら配信する

対象グループを選択*

 デバイスグループ (1 件)

ネットワーク全体 (3 台) 

メモ

→ アプリ配信設定の追加が完了します。

アプリ配信対象のデバイスを追加する

iOS

配信対象のデバイスを追加して、アプリの配信設定を実行します。

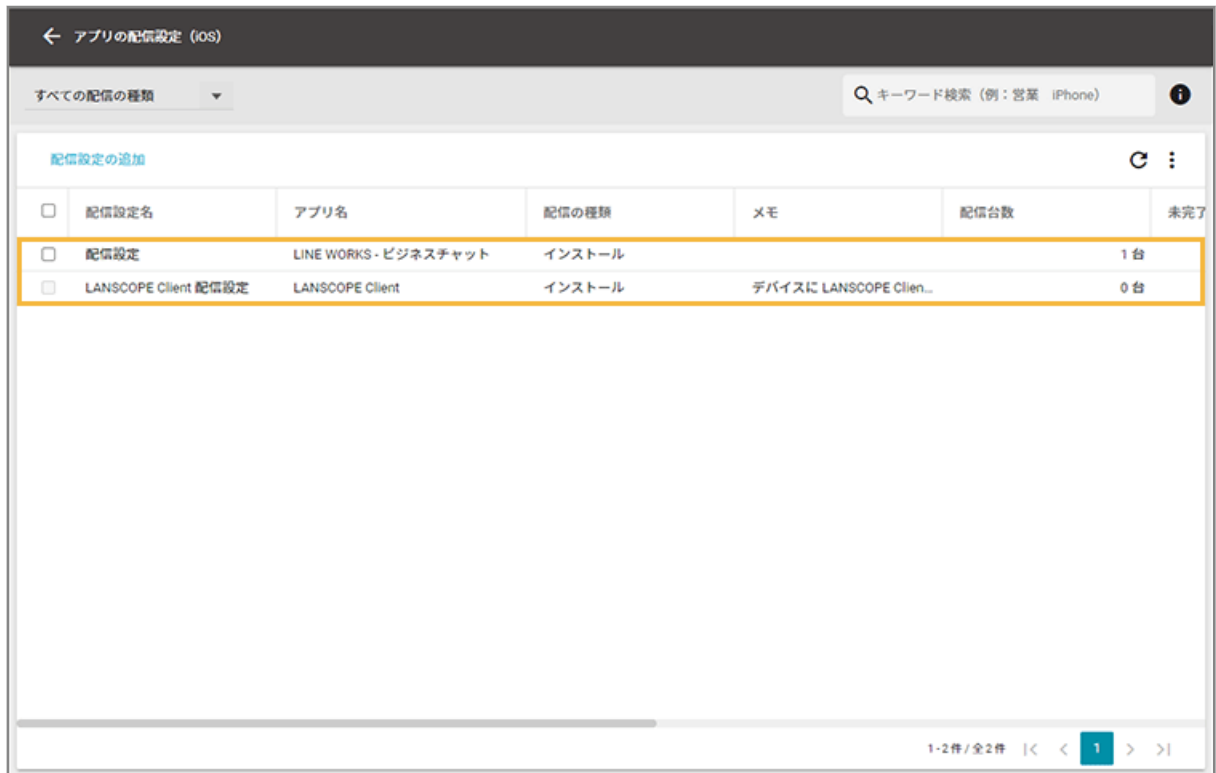
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



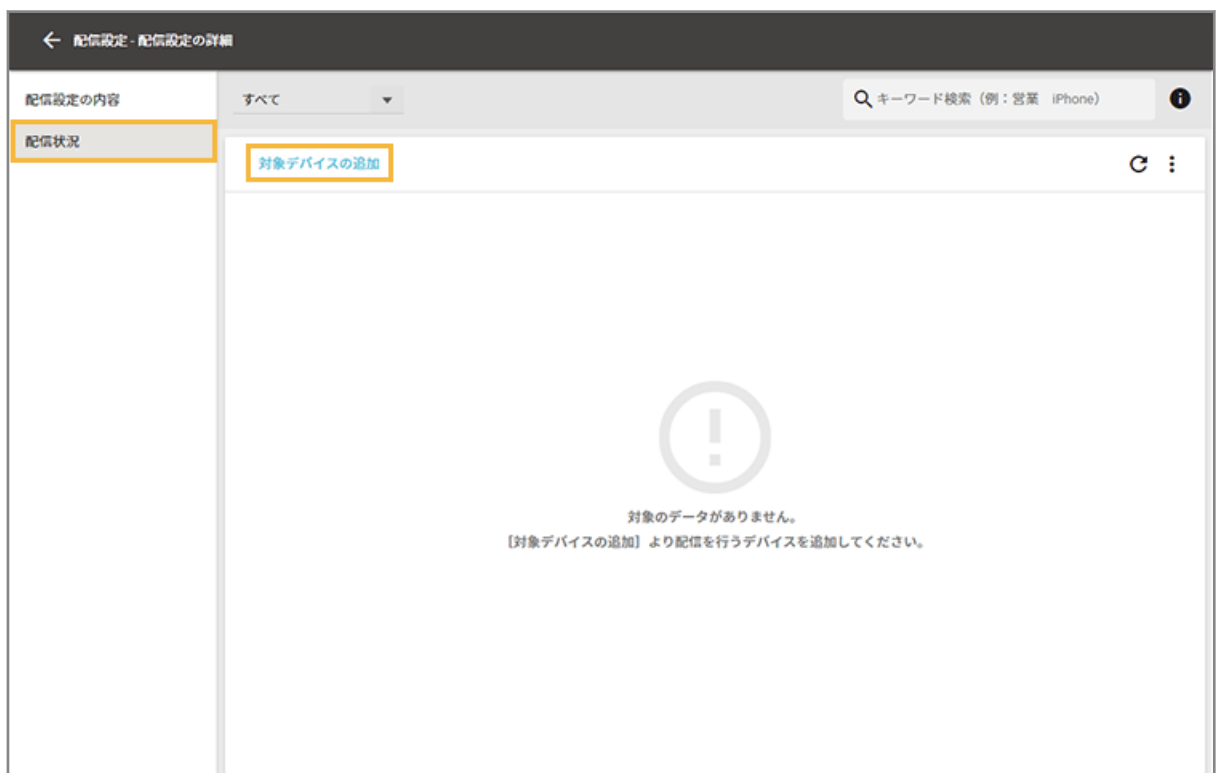
2. [アプリ配信設定] をクリックします。



3. アプリの配信設定をクリックします。



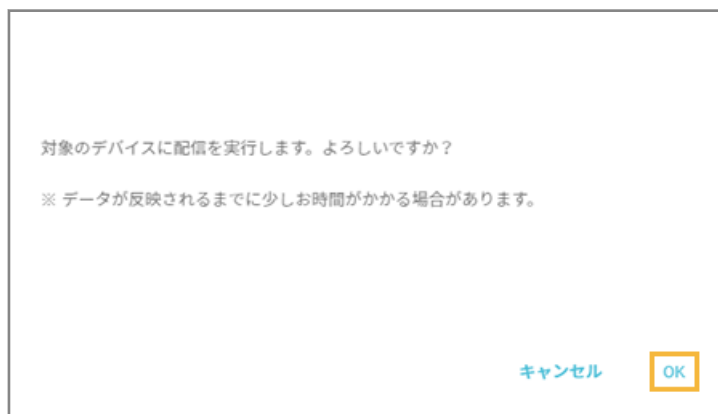
4. [配信状況] をクリックし、[対象デバイスの追加] をクリックします。



5. 配信対象のデバイスをチェックし、[追加] をクリックします。



6. [OK] をクリックします。



→ 対象デバイスに、アプリの配信設定が実行されます。

デバイス側での操作

iOS

OSバージョンやデバイスの設定により、画面表記や手順は異なります。

App Store アプリ（無償）の場合

アプリが配信されると、デバイス側にインストールダイアログが表示されます。[インストール] をタップし、インストールします。

ポイント

Apple ID のパスワードの入力を求められた場合、パスワードを入力し、インストールを実行します。



In-House（自社開発）アプリの場合

アプリが配信されると、デバイス側にインストールダイアログが表示されます。[インストール] をタップし、インストールします。

ポイント

デバイスが「監視モード」に設定されている場合、ダイアログは表示されず、サイレントでインストールが開始します。



アプリ配信結果を確認する

iOS

アプリ配信の結果を確認し、必要に応じて再配信します。

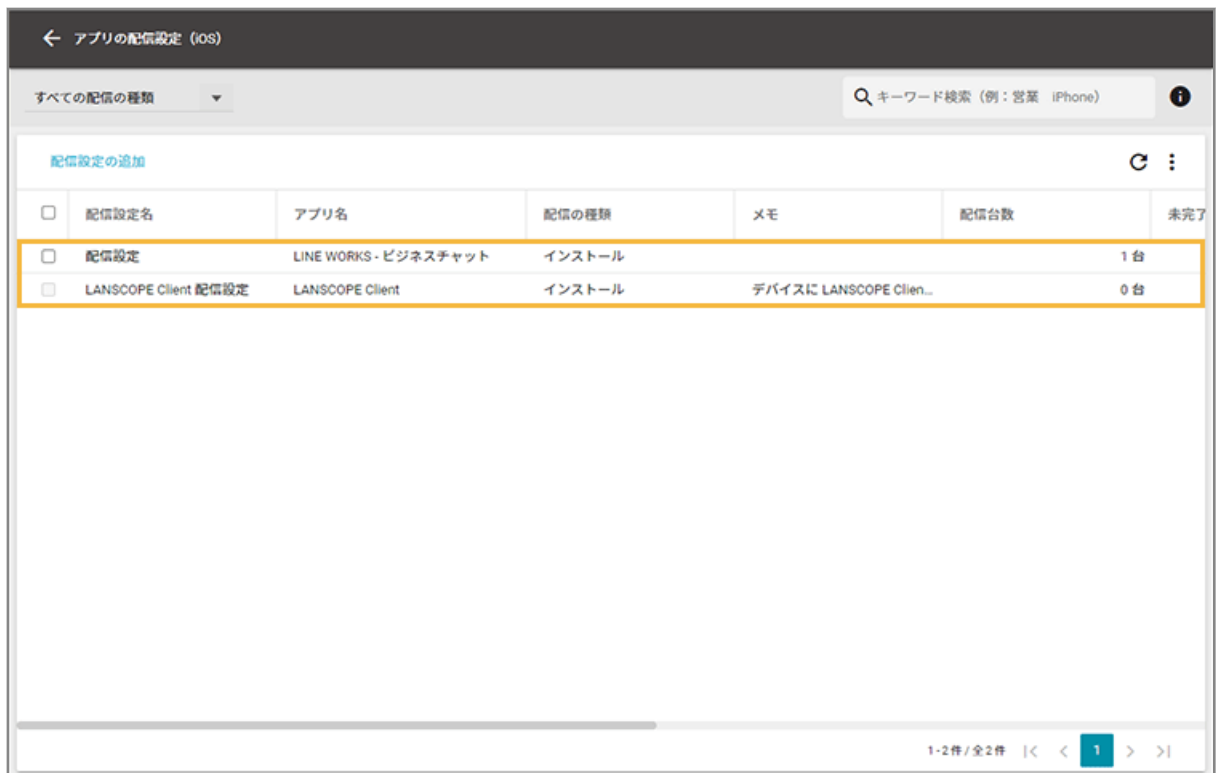
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



2. [アプリ配信設定] をクリックします。



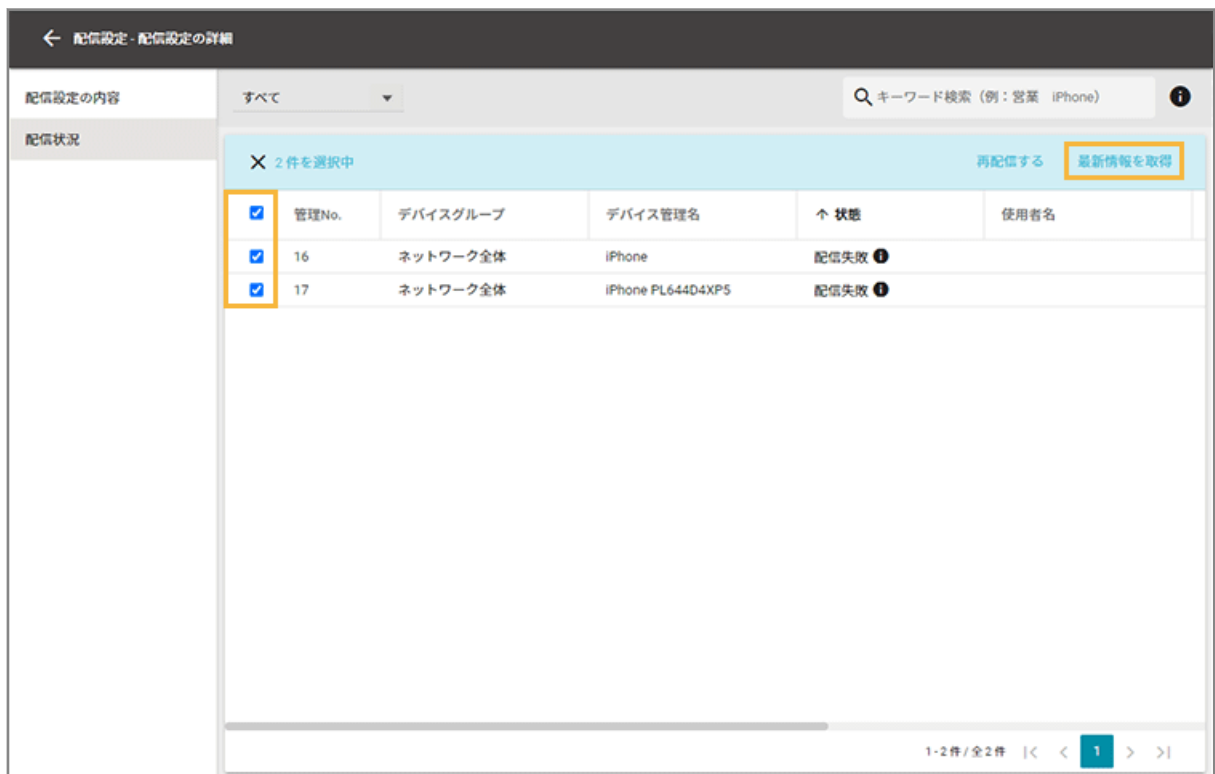
3. アプリの配信設定をクリックします。



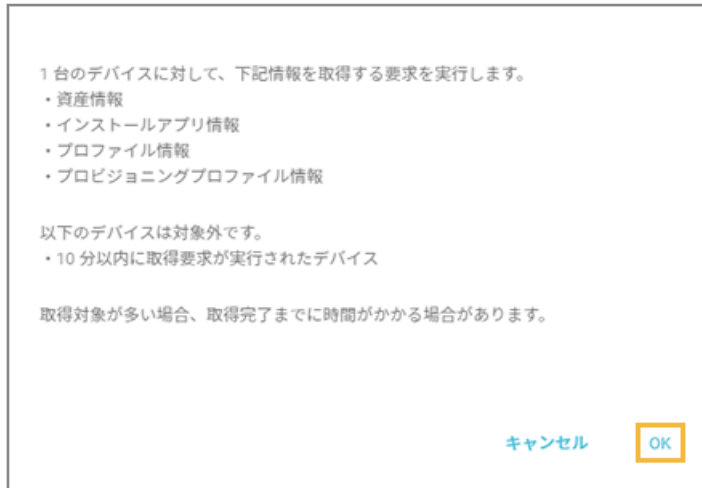
4. [配信状況] をクリックします。



5. デバイスをチェックし、[最新情報を取得] をクリックします。



6. [OK] をクリックします。



7. 各デバイスの配信状態を確認します。

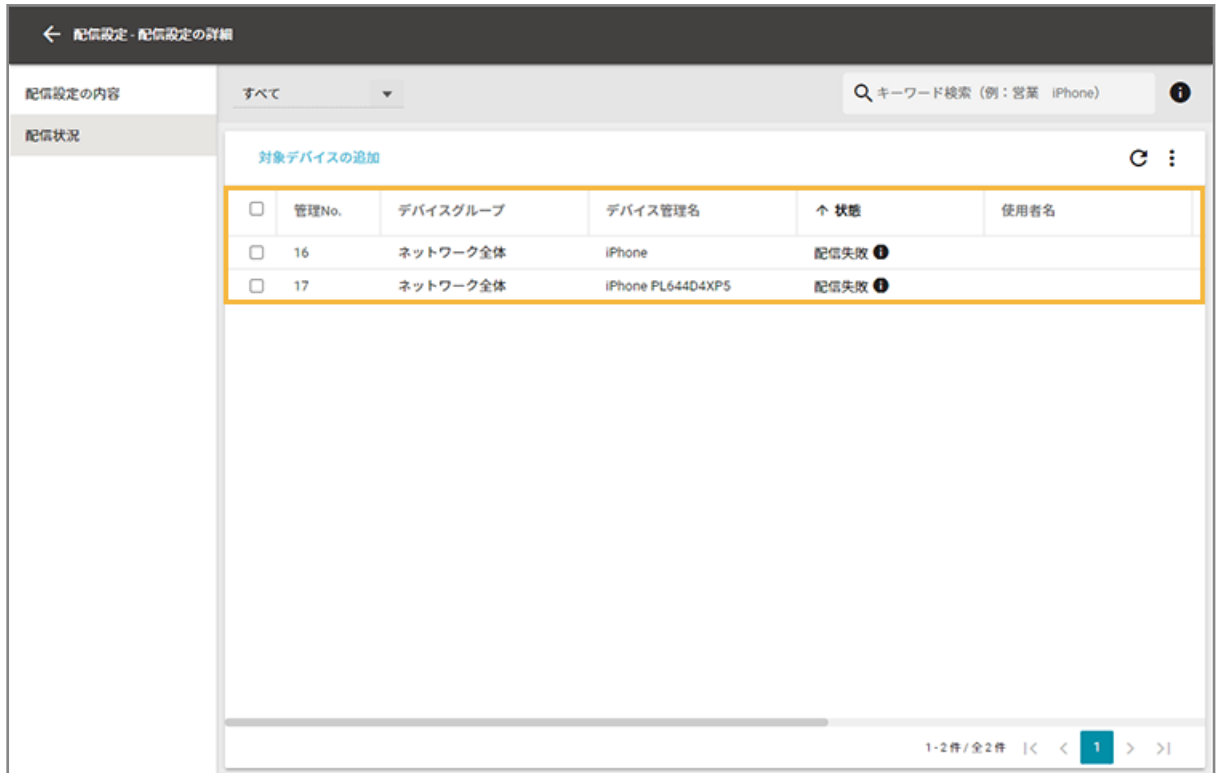


状態

- 配信中
アプリが配信中の状態のときに表示されます。
- 配信完了
アプリが配信された状態のときに表示されます。
- 配信失敗
アプリの配信に失敗した状態のときに表示されます。再配信、または 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。

8. 複数のアプリの配信結果を確認する場合は、次の操作をします。

(1) デバイスをクリックします。



(2) 配信状態／インストール状態を確認します。



配信状態

- 配信中
配信設定の適用後、アプリを配信中のときに表示されます。
- 配信完了
配信設定の適用後、アプリが配信されたときに表示されます。
- 配信失敗
次のエラーが発生したときに表示されます。

配信状態	概要
配信失敗（管理外）	デバイスが管理外になっているため、配信できません。
配信失敗（不明なエラー）	発生した場合、サポートセンターにお問い合わせください。
配信失敗（削除された管理アプリ）	管理アプリが削除されているため、配信できません。
配信失敗（アプリが存在しない）	発生した場合、サポートセンターにお問い合わせください。

配信状態	概要
配信失敗（アプリの有効期限切れ）	管理アプリの有効期限が切れているため、更新が必要です。
配信失敗（iOS アプリではない）	iOS デバイスにインストールできないアプリのため、配信できません。
配信失敗（デバイスがない）	デバイス上で MDM 構成プロファイルがアンインストールされているため、配信できません。
配信失敗（シリアル No がない）	発生した場合、サポートセンターにお問い合わせください。
配信失敗（アプリのサポート外 OS バージョン）	配信しようとしているデバイスの OS バージョンに、アプリが対応していないため、配信できません。

インストール状態

- 未インストール

アプリがインストールされていないか、アンインストールされた状態のときに表示されます。

- インストール済み

アプリがインストールされたか、アンインストールされていない状態のときに表示されます。

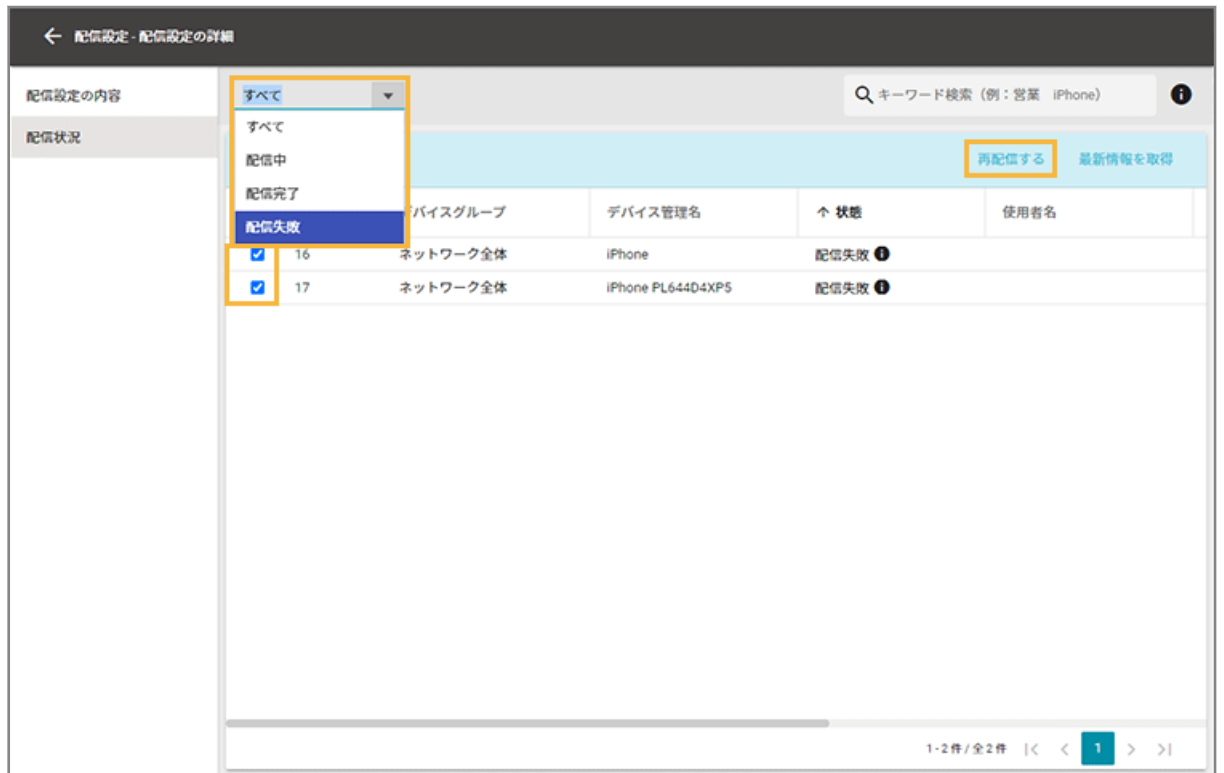
バージョン

デバイスにインストールされているアプリのバージョンが表示されます。

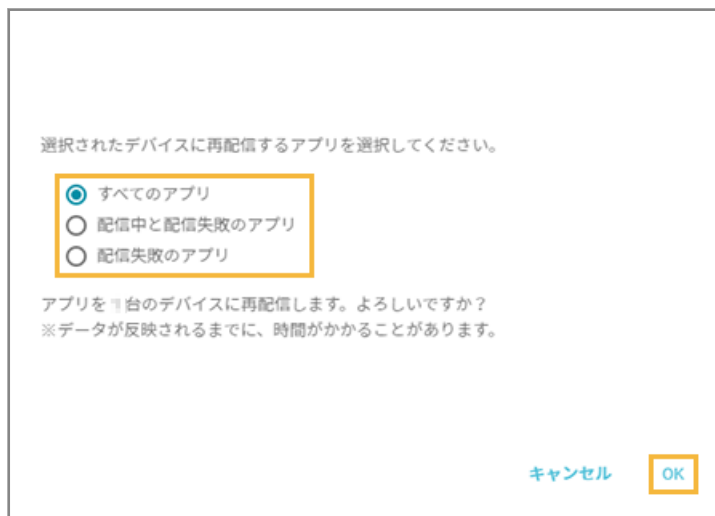
デバイス側でアプリをインストールすると、配信したアプリのバージョンに更新されます。

9. 再配信する場合は、次の操作をします。

- (1) 配信対象の「状態」を選択し、デバイスをチェックして、[再配信する] をクリックします。



(2) 再配信するアプリを選択し、[OK] をクリックします。



→ 再配信が実行されます。

登録したアプリを削除する

iOS

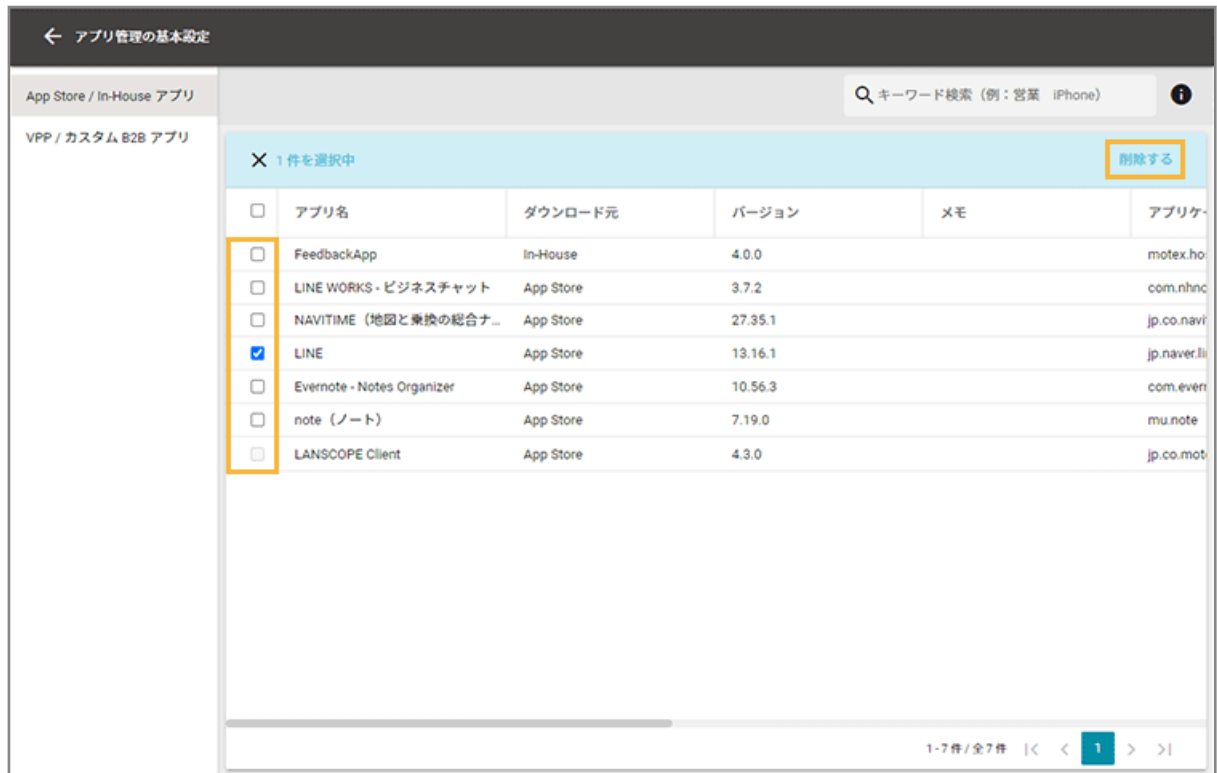
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



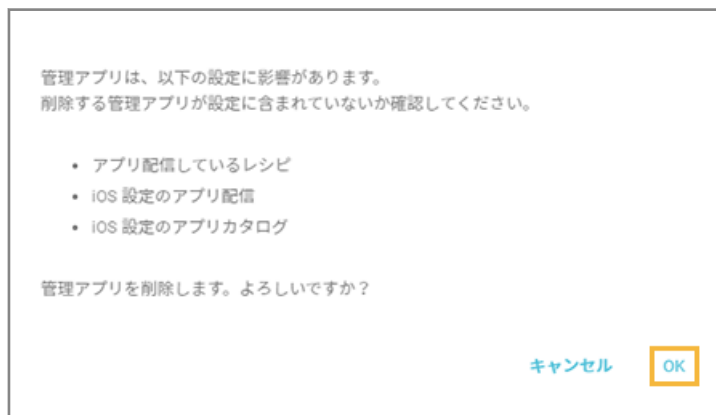
2. [基本設定] をクリックします。



3. アプリをチェックし、[削除する] をクリックします。



4. [OK] をクリックします。



→ アプリが削除されます。

アプリカタログを利用する

iOS

管理者がアプリカタログに公開したアプリを、利用者は必要なアプリを任意のタイミングで iOS デバイスにインストールできます。iOS デバイスに LANSCOPE Client をインストールしない場合、Web クリップを利用します。

VPP アプリ配信を利用する場合、An-353「Apple Business Manager 利用ガイド」を参照してください。

- [LANSCOPE Client でアプリカタログを利用する](#)
- [Web クリップでアプリカタログを利用する](#)

- [デバイス側で表示されるエラーメッセージ](#)

LANSCOPE Client でアプリカタログを利用する

iOS

LANSCOPE Client でアプリカタログを利用できます。

ステップ :

1. [公開するアプリを登録する](#)
2. [Managed App Configuration の設定を追加/更新する](#)
3. [アプリカタログにアプリを公開する](#)
4. [デバイス側での操作](#)

ステップ 1 : 公開するアプリを登録する

アプリを公開するには、事前に管理コンソールでアプリの登録が必要です。

App Store アプリ（無償）の情報を登録する

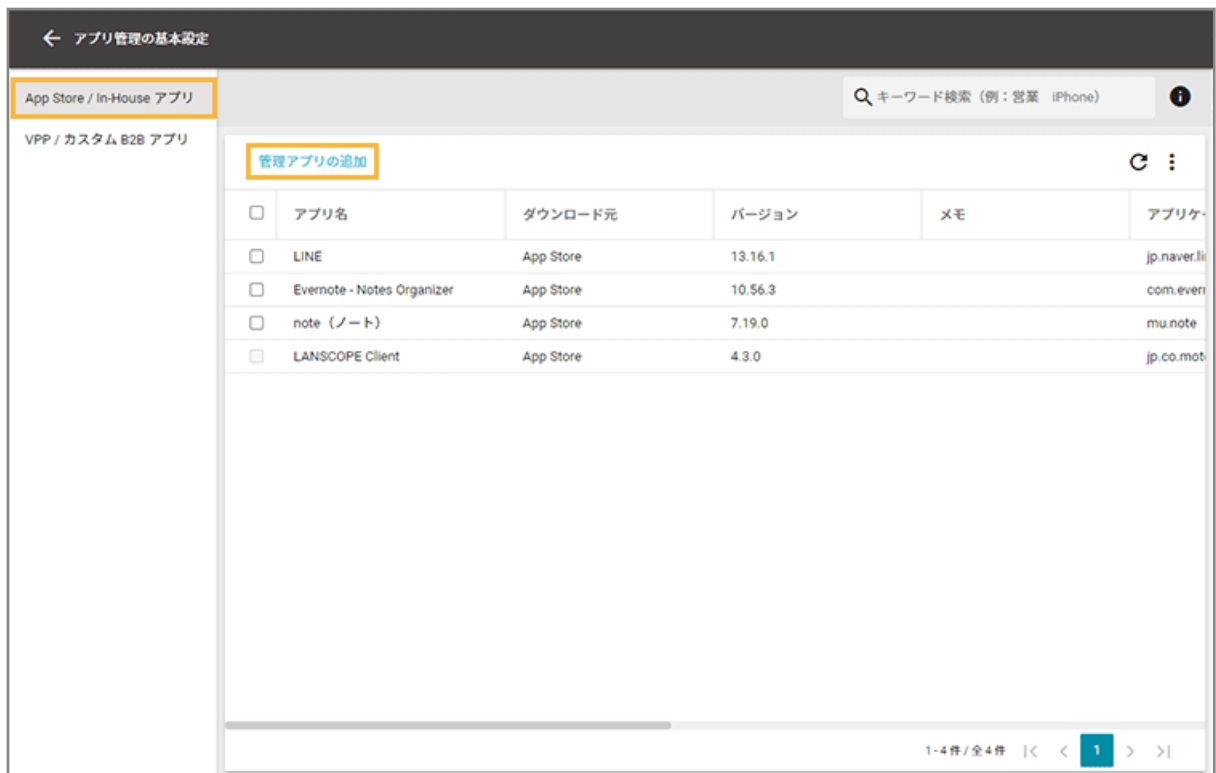
1. **【ルール】 の【Apple サービス設定】 >【iOS 設定】 をクリックします。**



2. **【基本設定】 をクリックします。**



3. [App Store/In-House アプリ] をクリックし、[管理アプリの追加] をクリックします。



4. [App Store] をクリックします。



5. アプリ名/アプリ ID/キーワードなどで配信するアプリを検索し、アプリをクリックします。



→ 選択したアプリの基本情報が表示されます。

6. 必要に応じてメモを入力し、[保存] をクリックします。



→ アプリが追加されます。

In-House（自社開発）アプリの情報を登録する

In-House（自社開発）アプリには、プロビジョニングプロファイルが含まれています。プロビジョニングプロファイルには有効期限があり、1年ごとに更新が必要です。有効期限が切れると、In-House（自社開発）アプリを利用できなくなるため、次のいずれかの方法でデバイスのプロビジョニングプロファイルを更新してください。

- [In-House（自社開発）アプリの情報を更新して、デバイスに配信する](#)
- [プロビジョニングプロファイルを更新して、デバイスに配信する](#)

有効期限の確認方法は、[プロビジョニングプロファイルの有効期限を確認する](#)を参照してください。

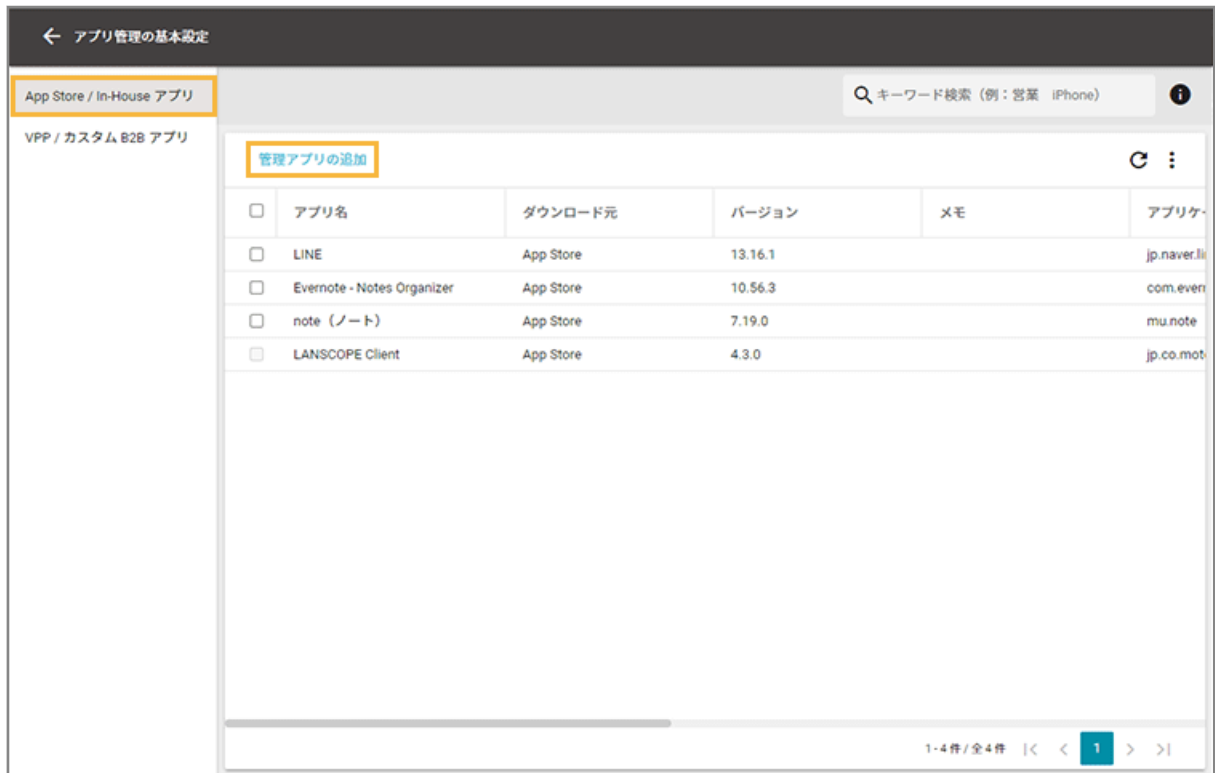
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



2. [基本設定] をクリックします。



3. [App Store/In-House アプリ] をクリックし、[管理アプリの追加] をクリックします。



4. [In-House] をクリックします。



5. マニフェストファイルとアプリファイルをアップロードします。



(1) マニフェストファイルの [ファイルアップロード] をクリックし、ファイルを選択します。

ポイント

Xcode9 で In-House（自社開発）アプリを開発した場合、「manifest.plist」ファイルを選択してください。

→ 基本情報が表示されます。

(2) アプリファイルの [ファイルアップロード] をクリックし、ファイルを選択します。

→ 基本情報の「ファイルサイズ」と「有効期限」が表示されます。

6. アプリカタログに表示する In-House（自社開発）アプリのアイコンを登録する場合は、[ファイルを選択] をクリックして、アイコンファイルを選択します。

アプリをインストール後にデバイスのホーム画面に表示されるアイコンは、In-House アプリのアプリファイル内に設定されたアイコンです。



→ プレビューが表示されます。

7. 必要に応じてメモを入力し、[保存] をクリックします。

← In-House アプリの追加

アプリ情報の取得

マニフェストファイル

manifest.plist

アプリファイル

FeedbackApp.ipa

基本情報

アプリ名
FeedbackApp

アプリケーションID
motex.hoshino.test

バージョン
4.0.0

カテゴリ
software

ファイルサイズ
49.66 KB

有効期限
2023/11/11 12:57:57

アプリカタログ設定

説明

アプリカタログに表示する説明を入力します。

アイコン
アプリカタログに表示するアイコンを選択します。
インストール後はアプリファイル内に設定されているアイコンが表示されます。
※推奨サイズ 180px x 180px

メモ

→ アプリが追加されます。

ステップ 2 : Managed App Configuration の設定を追加／更新する

アプリを利用するときに必要な設定をあらかじめ追加する場合は、Managed App Configuration の設定をします。追加／更新した設定は、アプリのインストール時にデバイスに適用されます。

LANSCOPE Client を公開する場合は、すでに Managed App Configuration が設定されているため、この手順は必要ありません。

ここでは、App Store アプリ（無償）の Managed App Configuration を設定する場合を例に説明します。

注意

- Managed App Configuration の設定項目に入力する情報は、アプリの開発元に確認してください。
- デバイスにインストールしたあとのアプリの動作は、アプリの開発元に確認してください。
- Managed App Configuration の設定が適用されたデバイスをバックアップ／復元すると、Managed App Configuration の設定は解除されます。

Managed App Configuration の設定を追加する

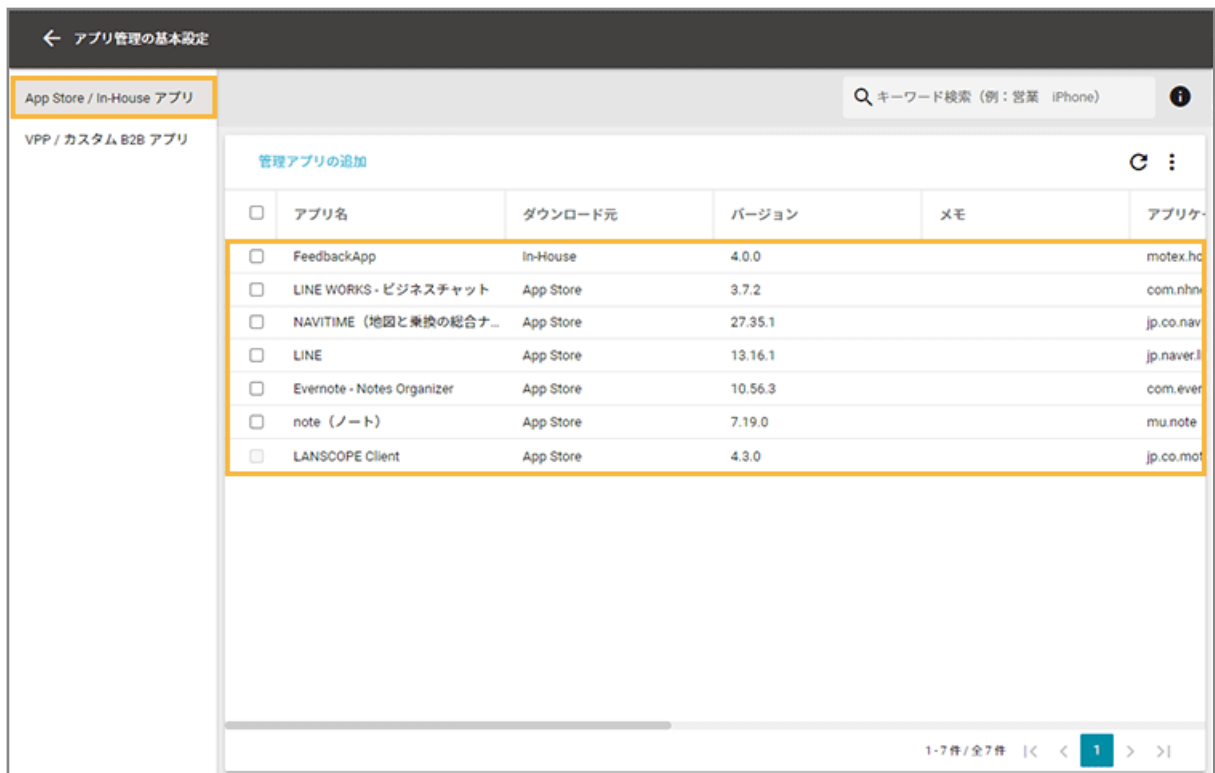
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



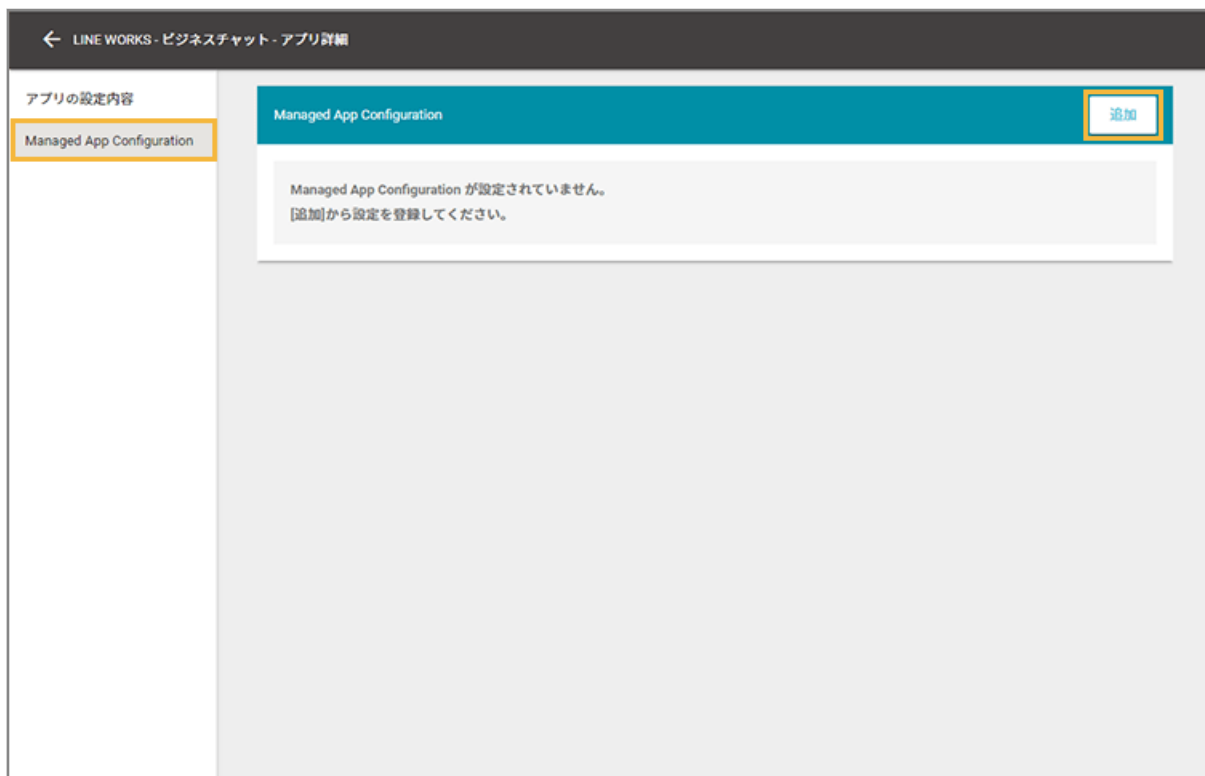
2. [基本設定] をクリックします。



3. [App Store/In-House アプリ] をクリックし、アプリをクリックします。

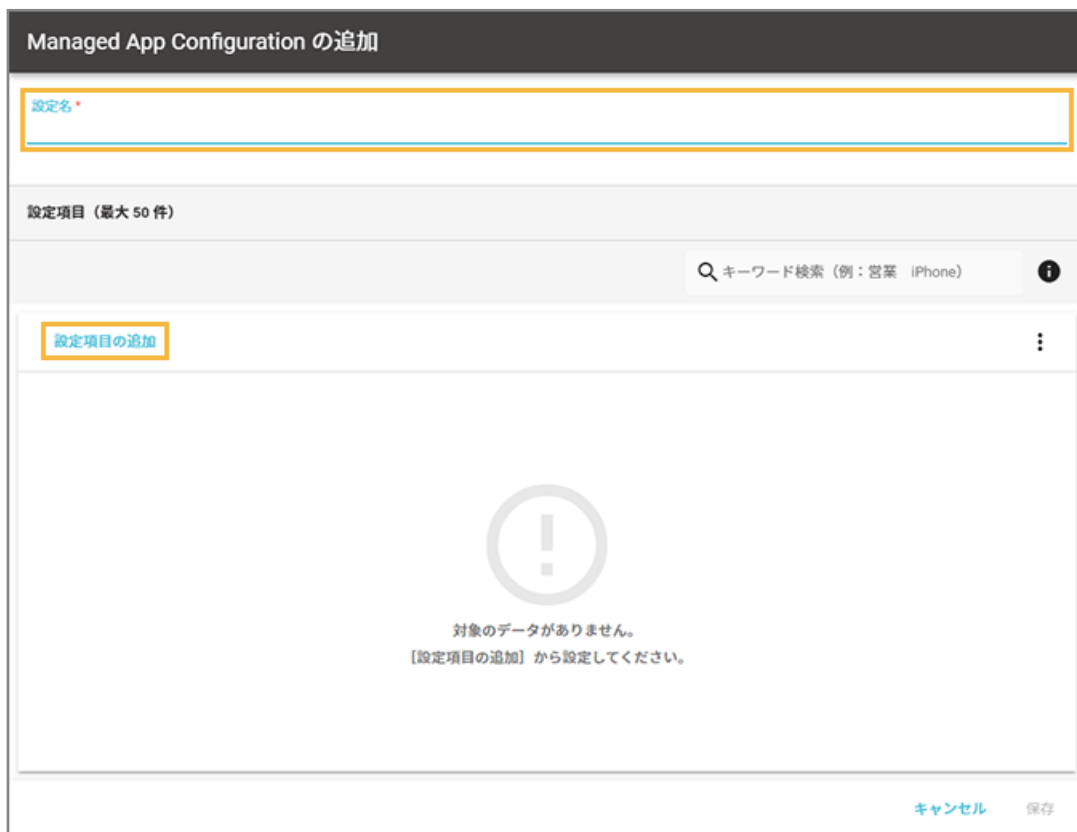


4. [Managed App Configuration] をクリックし、[追加] をクリックします。



5. 設定名を入力し、[設定項目の追加] をクリックします。

⋮ の [インポート] で、一括で追加できます。



6. キー名／値の種類／値を入力します。

← 設定項目の追加

パスワードなど重要な情報を設定するのは避けてください。

キー名 *

メモ

値の種類
文字列

値 *

キャンセル 保存

キー名

アプリの開発元に確認した情報を入力します。入力できる文字数は、80文字以内です。

値の種類

入力する値の種類を選択します。

値

アプリの開発元に確認した情報を入力します。入力できる文字数は、1,000文字以内です。配列の場合、追加できる値は10個以内で、1つの値に入力できる文字数は、100文字以内です。

7. [保存] をクリックします。

→ 「Managed App Configuration の追加」画面に戻ります。

8. 内容を確認し、[保存] をクリックします。

Managed App Configuration の追加

設定名*
[全社用]ログイン制御設定

設定項目 (最大 50 件)

キーワード検索 (例: 営業 iPhone)

設定項目の追加

キー名	値の種類	値 1	値 2
<input type="checkbox"/> LineworksAuthCode	文字列	xIHD5IU6B8Rwxy	

キャンセル 保存

→ Managed App Configuration の設定が保存されます。

Managed App Configuration の設定を更新する

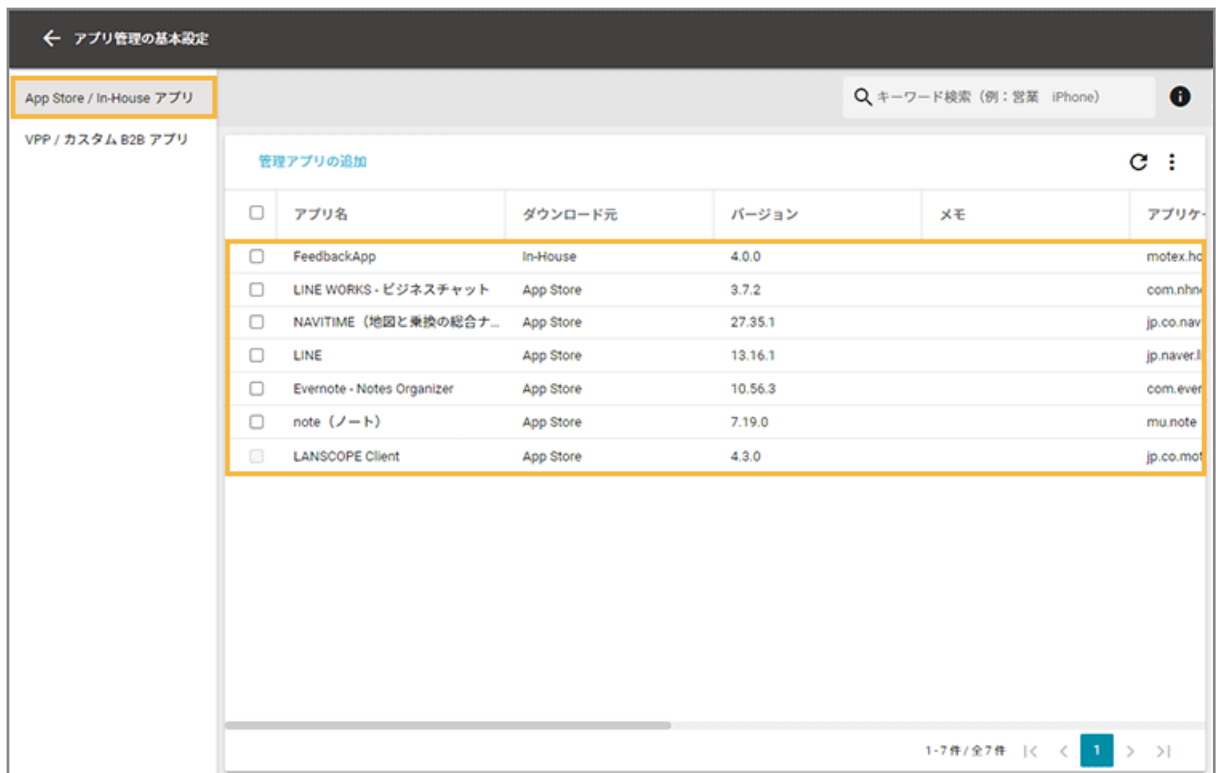
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。





2. [基本設定] をクリックします。

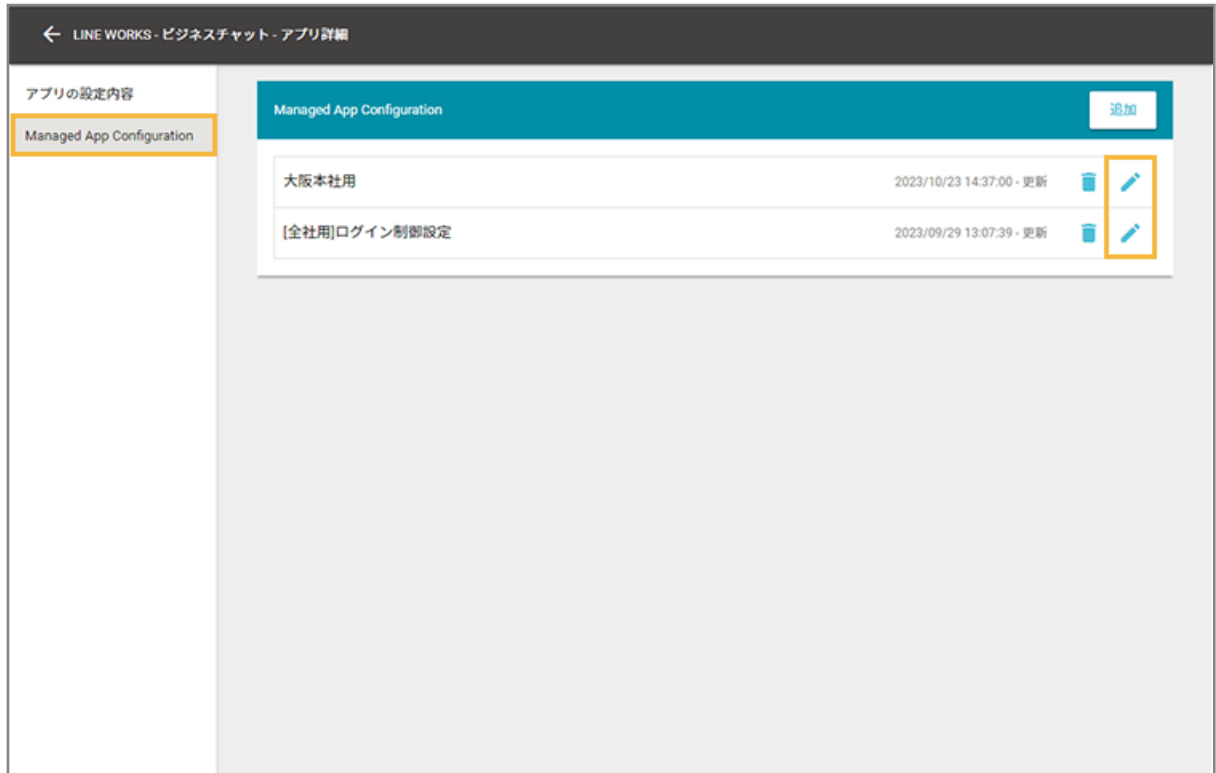


3. [App Store/In-House アプリ] をクリックし、アプリをクリックします。




4. [Managed App Configuration] をクリックし、 をクリックします。

設定を削除する場合は、 をクリックします。



5. 設定項目をクリックします。

- 設定項目を追加する場合は、[設定項目の追加] をクリックします。
- 設定項目を削除する場合は、設定項目をチェックし、[削除する] をクリックします。
-  の [インポート] で、一括で追加／編集できます。

Managed App Configuration の編集

設定名 *
[全社用]ログイン制御設定

設定項目 (最大 50 件)

🔍 キーワード検索 (例: 営業 iPhone) ⓘ

設定項目の追加 ⋮

<input type="checkbox"/>	キー名	値の種類	値 1	値 2
<input type="checkbox"/>	パスワード	文字列	パスワード	

キャンセル 保存

6. キー名／値の種類／値を編集します。

← 設定項目の編集

パスワードなど重要な情報を設定するのは避けてください。

キー名 *
パスワード

メモ

値の種類
文字列

値 *
パスワード

キャンセル 保存

キー名

アプリの開発元に確認した情報を入力します。入力できる文字数は、80 文字以内です。

値の種類

入力する値の種類を選択します。

値

アプリの開発元に確認した情報を入力します。入力できる文字数は、1,000 文字以内です。配列の場合、追加できる値は 10 個以内で、1 つの値に入力できる文字数は、100 文字以内です。

7. [保存] をクリックします。

→ 「Managed App Configuration の編集」画面に戻ります。

8. 内容を確認し、[保存] をクリックします。

Managed App Configuration の編集

設定名 *
[全社用]ログイン制御設定

設定項目 (最大 50 件)

キーワード検索 (例: 営業 iPhone)

設定項目の追加

<input type="checkbox"/>	キー名	値の種類	値 1	値 2
<input type="checkbox"/>	password	文字列		

キャンセル 保存

→ Managed App Configuration の設定が保存されます。

ステップ 3： アプリカタログにアプリを公開する

アプリカタログにアプリを登録して公開します。

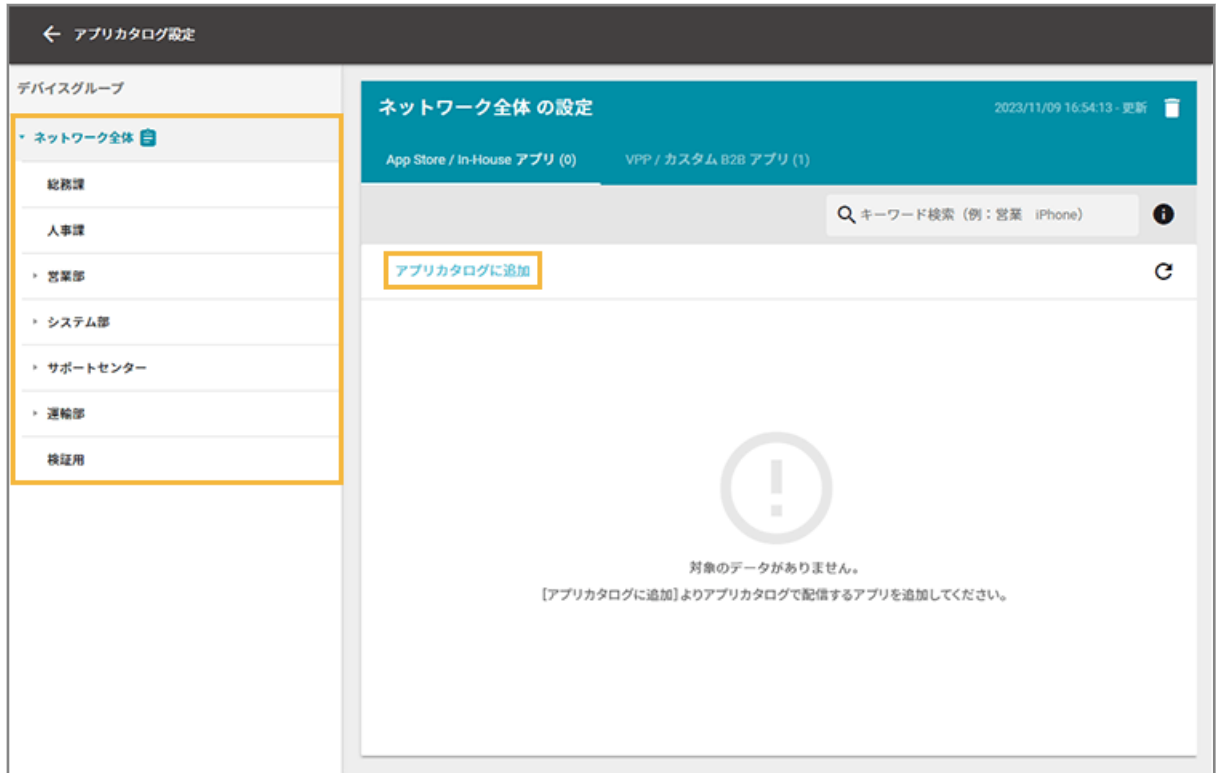
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



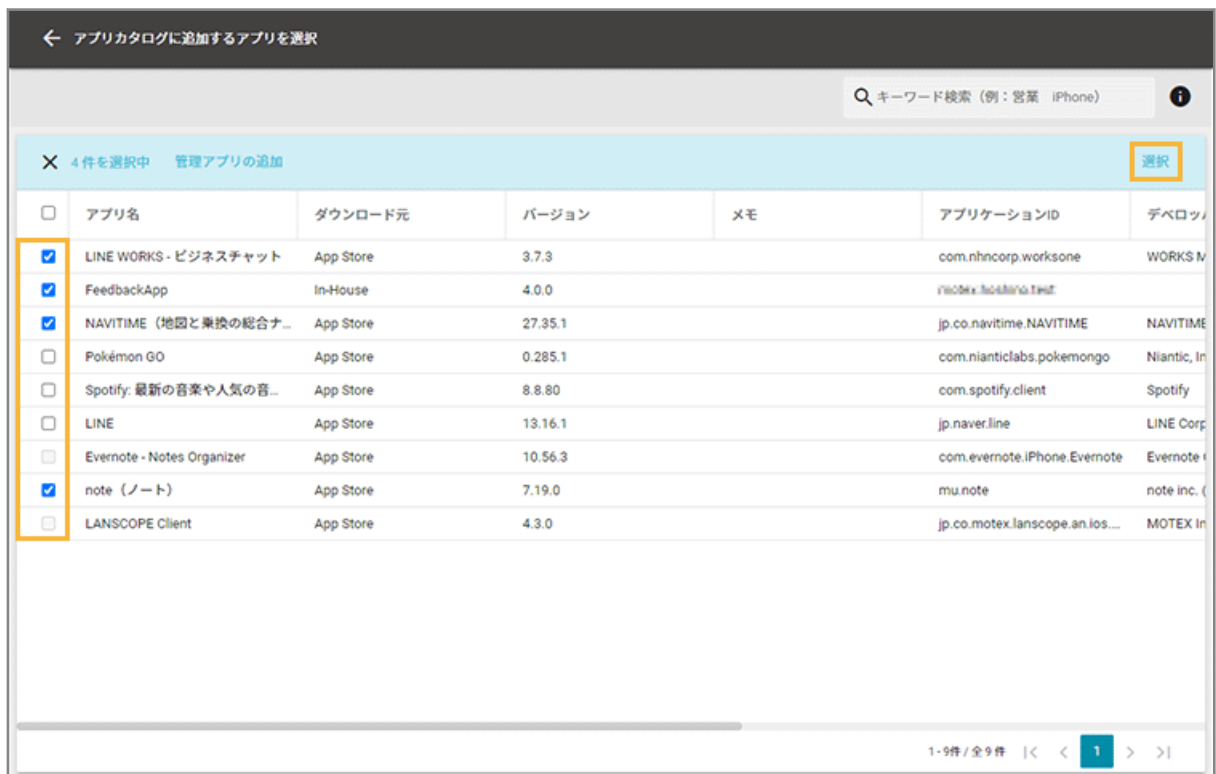
2. [アプリカタログ設定] をクリックします。



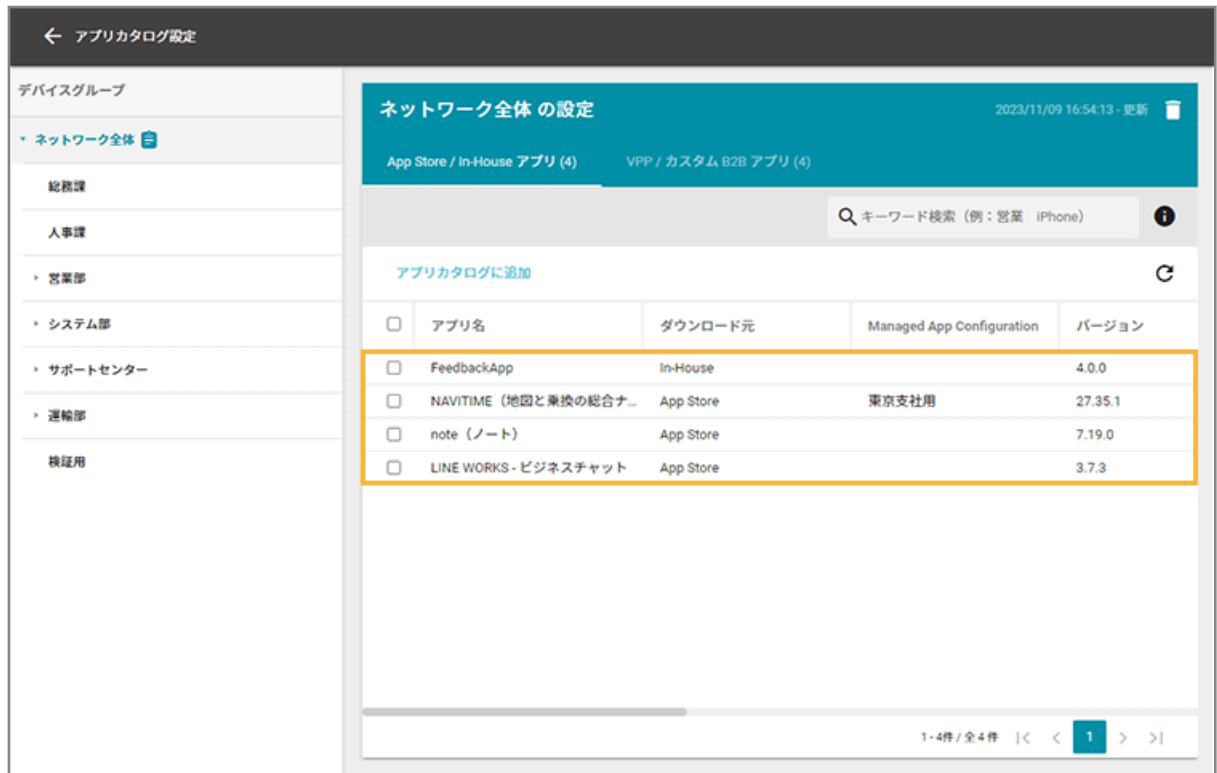
3. アプリを公開するグループをクリックし、[アプリカタログに追加] をクリックします。



4. アプリをチェックし、[選択] をクリックします。



5. 選択したアプリが一覧に追加されたことを確認します。

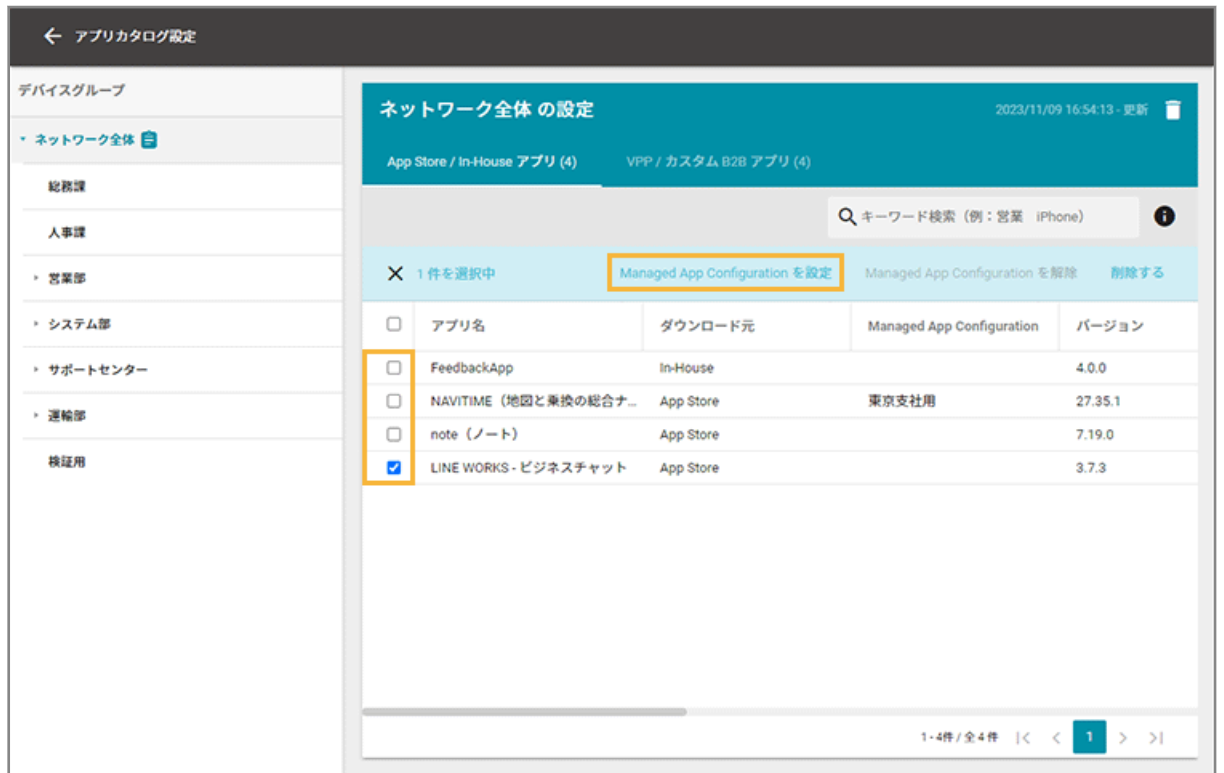


→ 公開完了です。

6. Managed App Configuration の設定を追加する場合は、次の操作をします。

(1) アプリをチェックし、[Managed App Configuration を設定] をクリックします。

すでに設定された Managed App Configuration の設定を解除する場合は、[Managed App Configuration を解除] をクリックし、[OK] をクリックします。



(2) 設定する Managed App Configuration の [選択] をクリックします。



→ Managed App Configuration の設定が追加されます。

ステップ4： デバイス側での操作

ポイント

- LANSCOPE Client Ver.3.3.1.0 以上が対象です。LANSCOPE Client のインストール方法は、An-301「初期設定ガイド for iOS/iPadOS」を参照してください。
- アップデート版の公開タイミングは、ストアにアプリ公開後 24 時間以内です。アプリカタログに最新バージョンが自動で表示されます。
- アップデート待ちのアプリがある場合、LANSCOPE Client アイコンにアプリ数がバッジ表示され、カタログアイコンには「NEW」と表示されます。バッジの表示数は、「メッセージ・アンケートの未読数」+「アップデート待ちのアプリの数」の合計です。

1. [LANSCOPE Client] をタップします。



2. [カタログ] をタップします。



3. アプリを選択し、利用者のタイミングで実行します。





Web クリップでアプリカタログを利用する

iOS

アプリカタログ用の Web クリップを配信して、アプリカタログを利用します。

LANSCOPE Client をインストールしない場合や、アプリカタログ用にアイコンを変更する場合に有効です。

ステップ :

1. [アプリカタログ用の Web クリップを配信する](#)
2. [公開するアプリを登録する](#)
3. [Managed App Configuration の設定を追加／更新する](#)
4. [アプリカタログにアプリを公開する](#)
5. [デバイス側での操作](#)

ステップ 1 : アプリカタログ用の Web クリップを配信する

レシピ機能を利用して、アプリカタログの利用に必要な Web クリップを配信します。

ここでは、デバイスに LANSCOPE クライアントがインストールされたら、アプリカタログの利用に必要なプロファイルを自動配信する場合を例に説明します。

すでに LANSCOPE クライアントがインストールされている場合は、任意のトリガーを選択してください。

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。

状態	レシピ名	トリガー	アクション
<input type="checkbox"/>	LANSCOPE Client を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定アプリを配信する
<input type="checkbox"/>	LANSCOPE の登録用 Clip を配信する (iOS)	LANSCOPE クライアントがインストールされた	指定プロフィールを配信する
<input checked="" type="checkbox"/>	管理外アラート (iOS/Windows/macOS)	デバイスが管理外になっている	アラートに設定する
<input type="checkbox"/>	パスワードポリシー非準拠アラート (iOS/Android)	パスワードポリシーに準拠していない	アラートに設定する
<input type="checkbox"/>	LANSCOPE Client 未更新アラート (iOS/Android/Windows)	LANSCOPE Client のバージョンが最新になっていない	アラートに設定する
<input checked="" type="checkbox"/>	未稼働アラート (iOS/Android/Windows/macOS)	未稼働期間が指定された期間を超過している	アラートに設定する
<input type="checkbox"/>	空き容量不足アラート (iOS/Android/Windows/macOS)	空き容量が不足している	アラートに設定する
<input type="checkbox"/>	パスワードロックオフアラート (iOS)	パスワードロックの設定がオフになっている	アラートに設定する
<input type="checkbox"/>	リモート実行無効アラート (Android/Windows)	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	アラートに設定する
<input checked="" type="checkbox"/>	SIMカード抜き差しアラート (iOS/Android/Windows)	SIMカードが抜き差しされた	アラートに設定する
<input checked="" type="checkbox"/>	SDカード抜き差しアラート (Android)	SDカードが抜き差しされた	アラートに設定する
<input type="checkbox"/>	新規アプリインストールアラート (Android)	新しくアプリがインストールされた	アラートに設定する
<input type="checkbox"/>	タイムゾーン変更アラート (Android)	タイムゾーンが変更された	アラートに設定する
<input type="checkbox"/>	新規プロフィールインストールアラート (iOS/macOS)	新しくプロフィールがインストールされた	アラートに設定する

3. 次のように設定し、[アクション追加] をクリックします。

項目	値
レシピ名	任意のレシピ名
トリガー	[LANSCOPE クライアントがインストールされた]
デバイスグループ	配信するデバイスグループまたはデバイス
デバイス	

新しいレシピを作成

レシピ名*
アプリカタログ配信

レシピのトリガーを選択 トリガー選択

トリガー*
LANSCOPE クライアントがインストールされた

レシピを実行する対象の絞り込み

 デバイスグループ (0 件)
選択

 デバイス (0 台)
選択

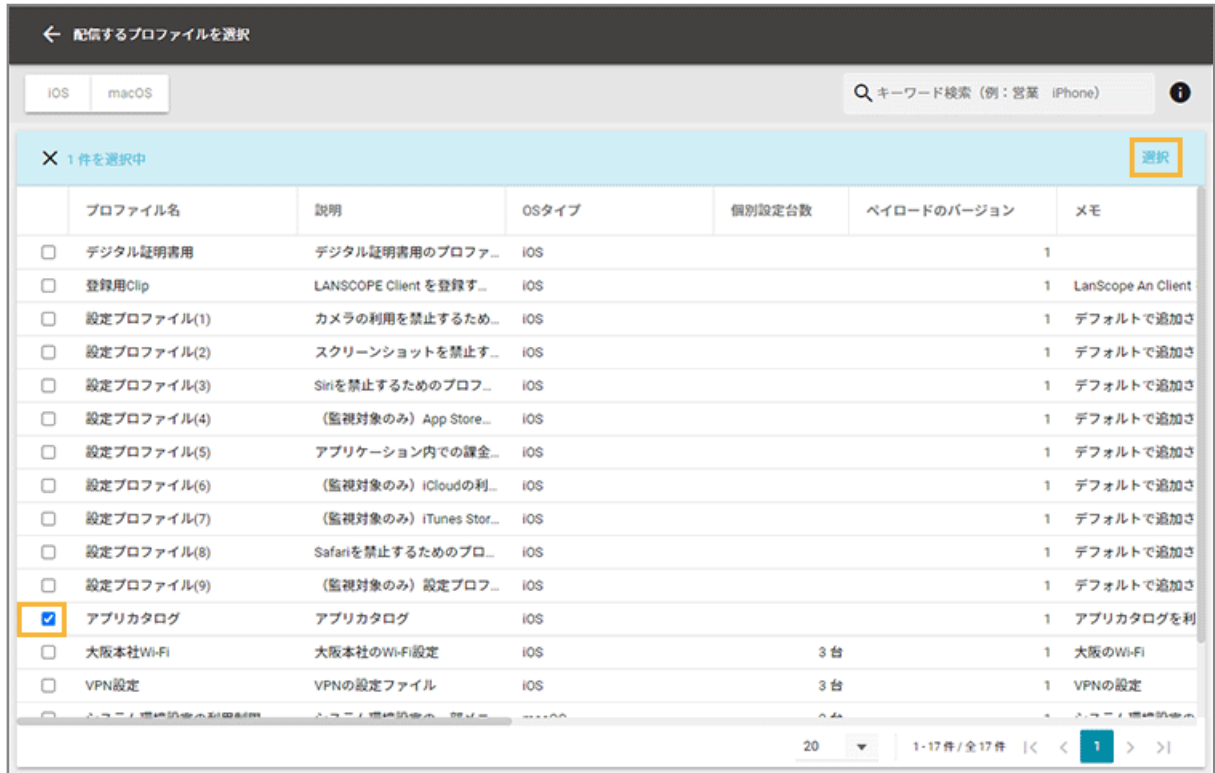
実行するアクション アクション追加

4. [指定プロファイルを配信する] をクリックします。

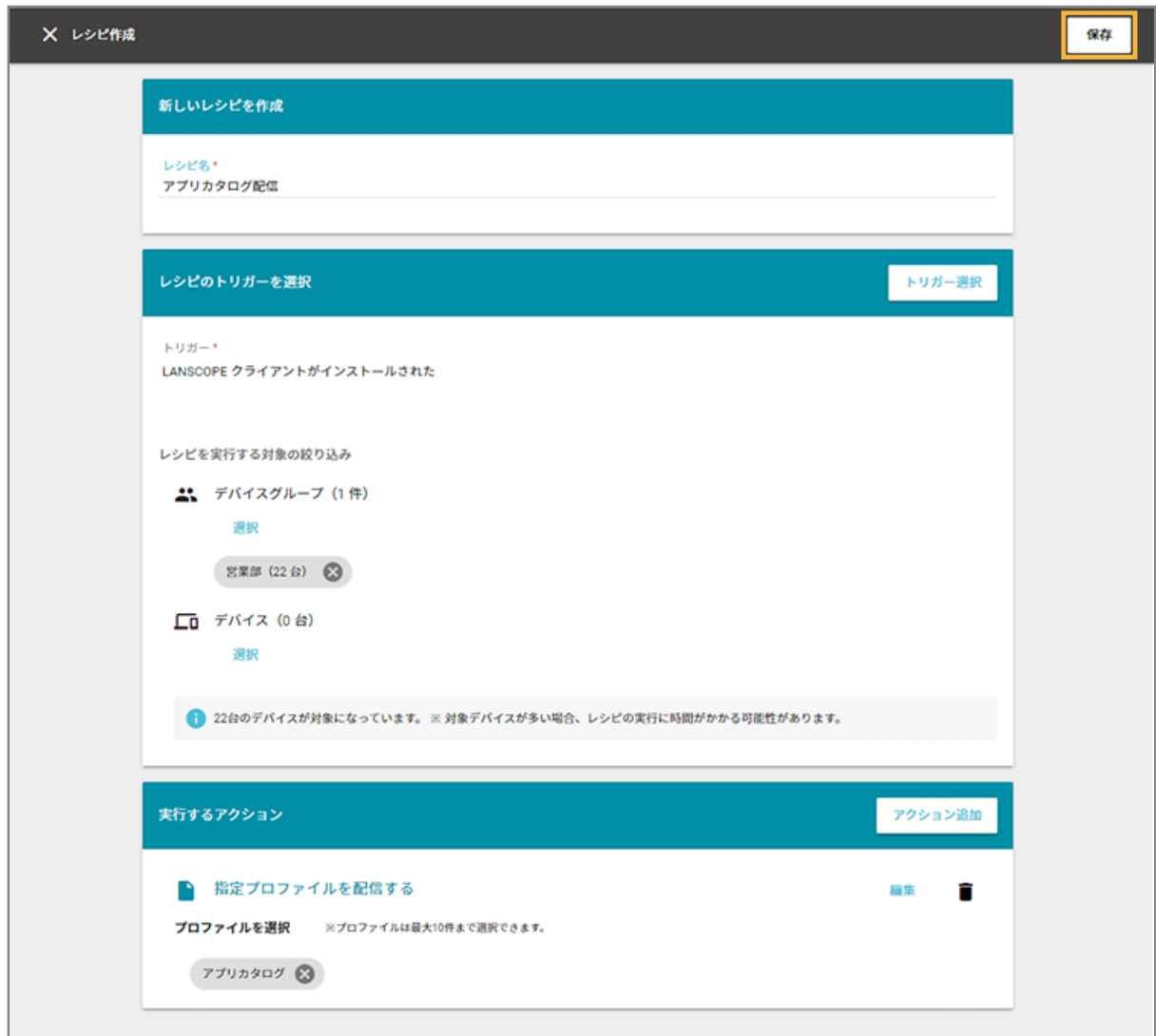
アクションを選択してください

	iOS	Android	Windows	macOS
 管理者にメールでお知らせする	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 指定プロファイルを配信する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
 指定アプリを配信する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 指定プロビジョニングプロファイルを配信する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 指定 VPP アプリを配信する	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 メッセージを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
 アンケートを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
 アラートに設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 アラートレポートを送信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 指定プロファイルを取り除く	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>

5. 「アプリカタログ」をチェックし、[選択] をクリックします。



6. 内容を確認し、[保存] をクリックします。



→ 配信設定が完了します。

ステップ 2： 公開するアプリを登録する

アプリを公開するには、事前にアプリの登録が必要です。

App Store アプリ（無償）の情報を登録する

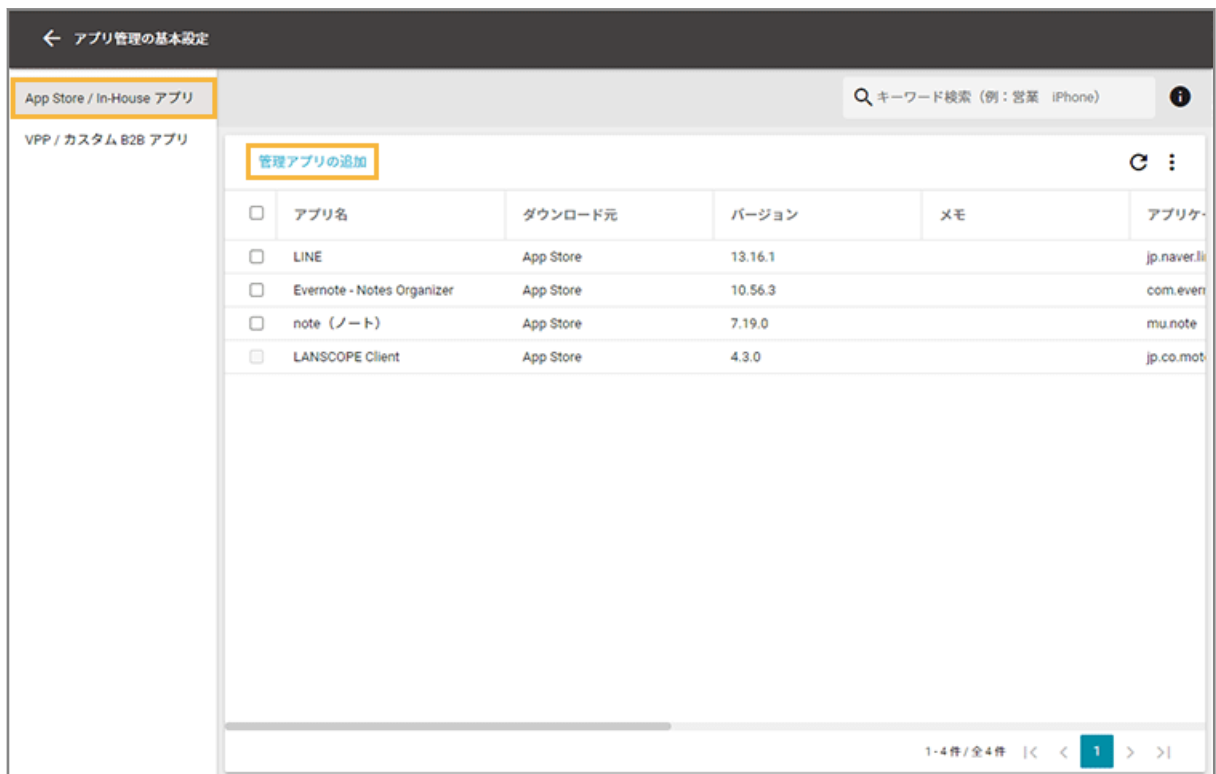
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



2. **【基本設定】** をクリックします。



3. **【App Store/In-House アプリ】** をクリックし、**【管理アプリの追加】** をクリックします。



4. **【App Store】** をクリックします。



5. アプリ名/アプリ ID/キーワードなどで配信するアプリを検索し、アプリをクリックします。



→ 選択したアプリの基本情報が表示されます。

6. 必要に応じてメモを入力し、[保存] をクリックします。



→ アプリが追加されます。

In-House（自社開発）アプリの情報を登録する

In-House（自社開発）アプリには、プロビジョニングプロファイルが含まれています。プロビジョニングプロファイルには有効期限があり、1年ごとに更新が必要です。有効期限が切れると、In-House（自社開発）アプリを利用できなくなるため、次のいずれかの方法でデバイスのプロビジョニングプロファイルを更新してください。

- [In-House（自社開発）アプリの情報を更新して、デバイスに配信する](#)
- [プロビジョニングプロファイルを更新して、デバイスに配信する](#)

有効期限の確認方法は、[プロビジョニングプロファイルの有効期限を確認する](#)を参照してください。

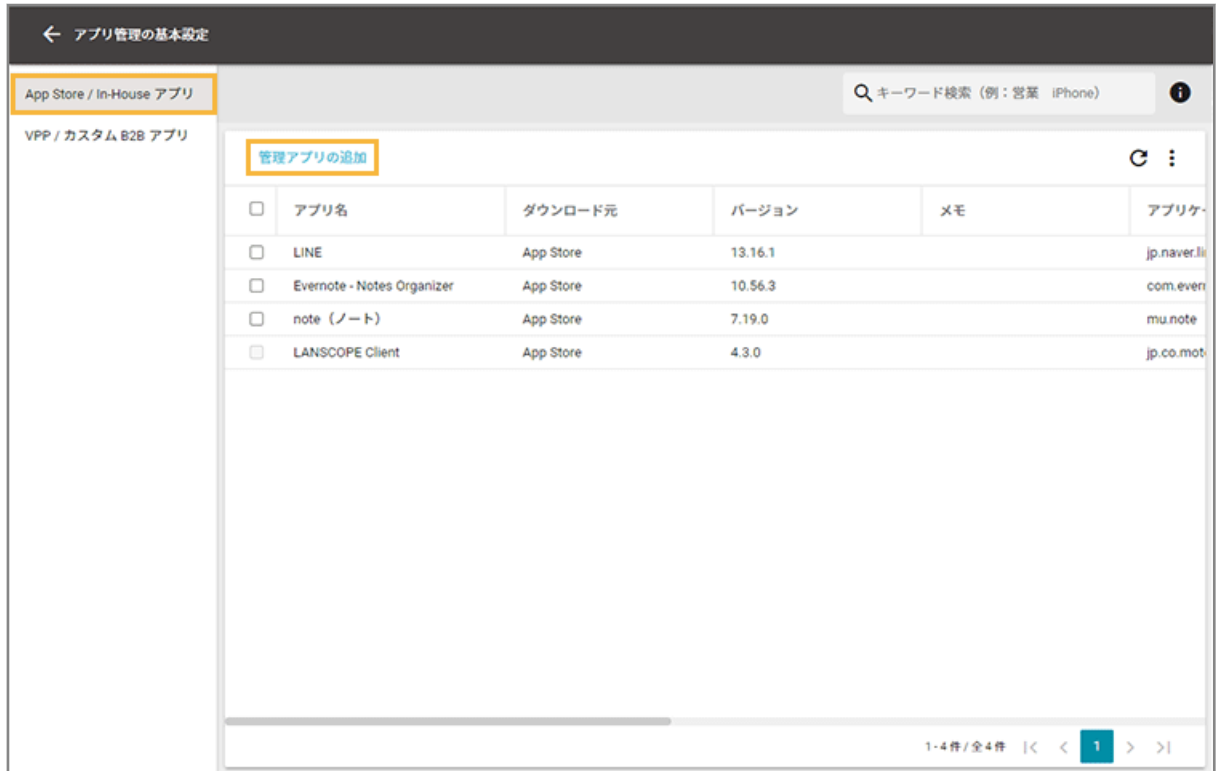
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



2. [基本設定] をクリックします。



3. [App Store/In-House アプリ] をクリックし、[管理アプリの追加] をクリックします。



4. [In-House] をクリックします。



5. マニフェストファイルとアプリファイルをアップロードします。



(1) マニフェストファイルの [ファイルアップロード] をクリックし、ファイルを選択します。

ポイント

Xcode9 で In-House（自社開発）アプリを開発した場合、「manifest.plist」ファイルを選択してください。

→ 基本情報が表示されます。

(2) アプリファイルの [ファイルアップロード] をクリックし、ファイルを選択します。

→ 基本情報の「ファイルサイズ」と「有効期限」が表示されます。

6. アプリカタログに表示する In-House（自社開発）アプリのアイコンを登録する場合は、[ファイルを選択] をクリックして、アイコンファイルを選択します。

アプリをインストール後にデバイスのホーム画面に表示されるアイコンは、In-House アプリのアプリファイル内に設定されたアイコンです。



→ プレビューが表示されます。

7. 必要に応じてメモを入力し、[保存] をクリックします。

← In-House アプリの追加

アプリ情報の取得

マニフェストファイル

manifest.plist

アプリファイル

FeedbackApp.ipa

基本情報

アプリ名
FeedbackApp

アプリケーションID
motex.hoshino.test

バージョン
4.0.0

カテゴリ
software

ファイルサイズ
49.66 KB

有効期限
2023/11/11 12:57:57

アプリカタログ設定

説明

アプリカタログに表示する説明を入力します。

アイコン
アプリカタログに表示するアイコンを選択します。
インストール後はアプリファイル内に設定されているアイコンが表示されます。
※推奨サイズ 180px x 180px

メモ

→ アプリが追加されます。

ステップ 3 : Managed App Configuration の設定を追加／更新する

アプリを利用するときに必要な設定をあらかじめ追加する場合は、Managed App Configuration の設定をします。追加／更新した設定は、アプリのインストール時にデバイスに適用されます。

LANSCOPE Client を公開する場合は、すでに Managed App Configuration が設定されているため、この手順は必要ありません。

ここでは、App Store アプリ（無償）の Managed App Configuration を設定する場合を例に説明します。

注意

- Managed App Configuration の設定項目に入力する情報は、アプリの開発元に確認してください。
- デバイスにインストールしたあとのアプリの動作は、アプリの開発元に確認してください。
- Managed App Configuration の設定が適用されたデバイスをバックアップ／復元すると、Managed App Configuration の設定は解除されます。

Managed App Configuration の設定を追加する

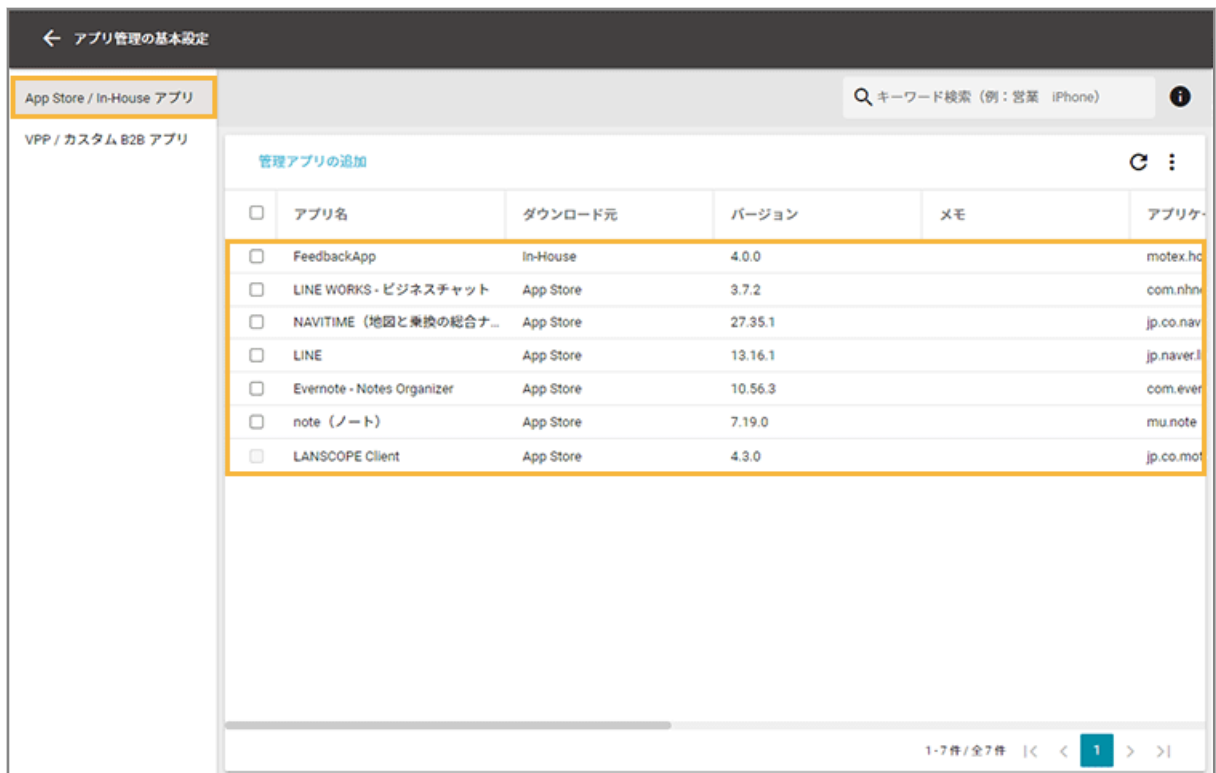
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



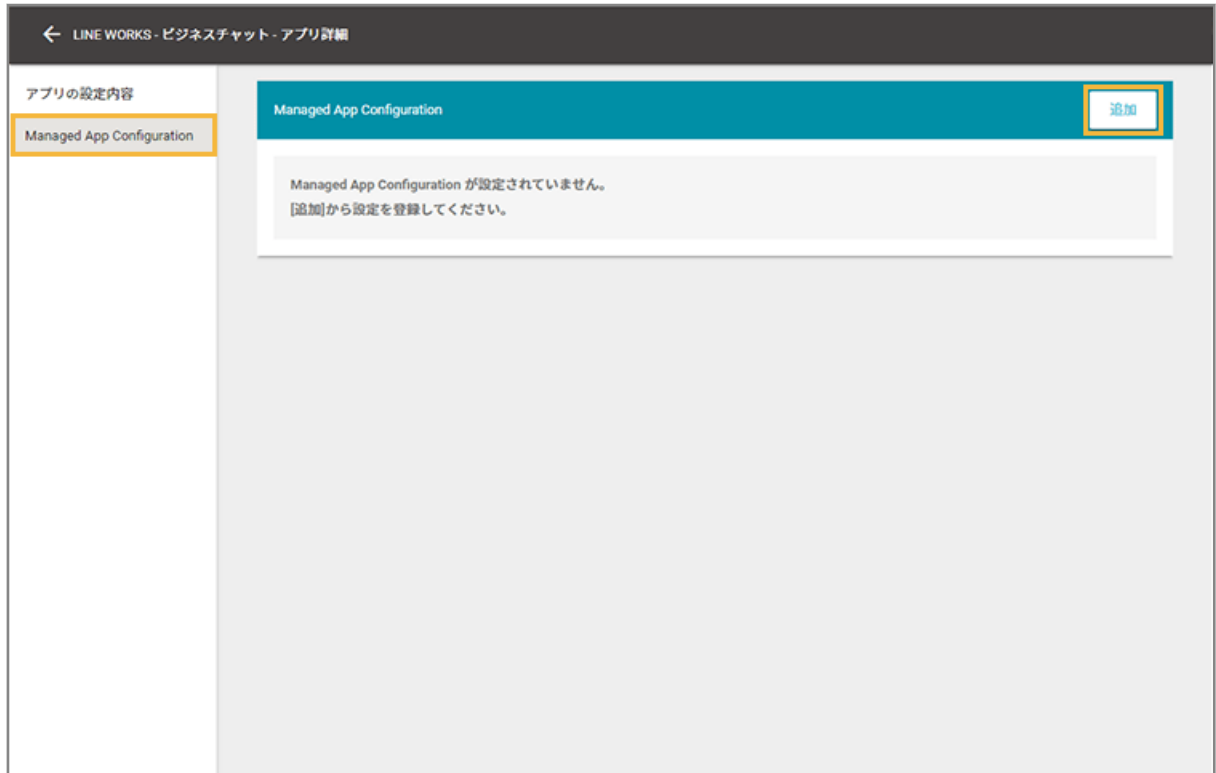
2. [基本設定] をクリックします。



3. [App Store/In-House アプリ] をクリックし、アプリをクリックします。

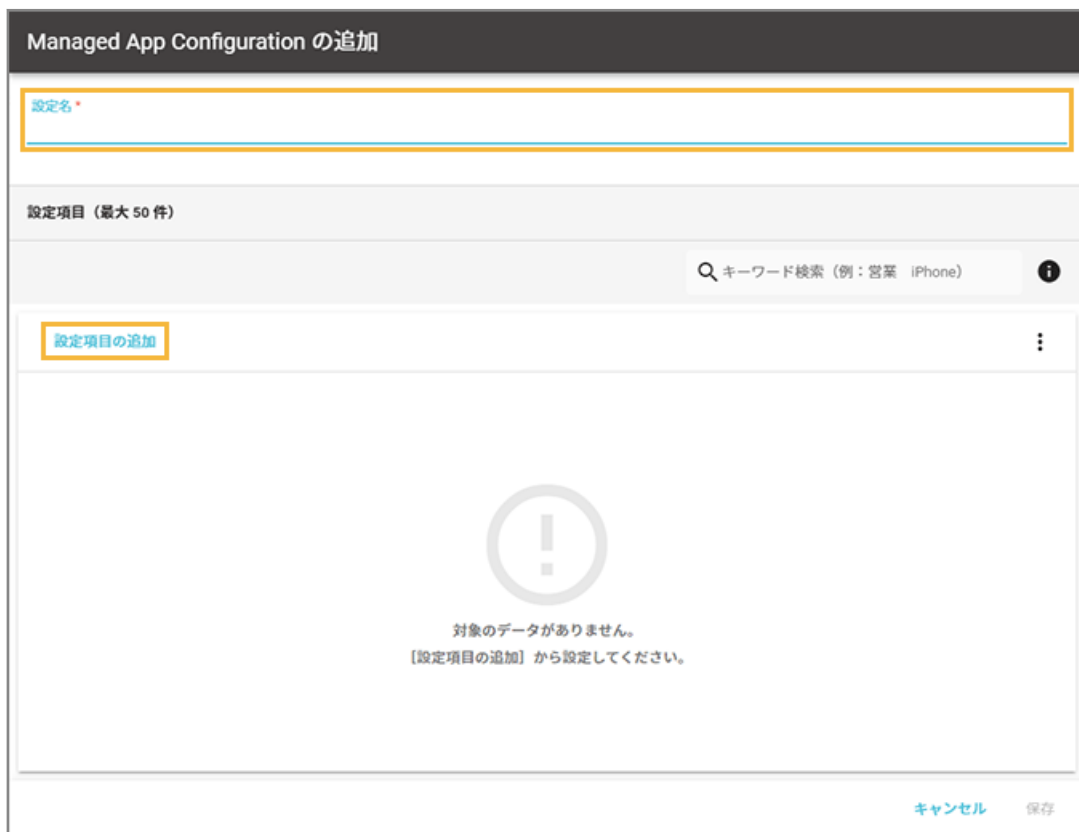


4. [Managed App Configuration] をクリックし、[追加] をクリックします。



5. 設定名を入力し、[設定項目の追加] をクリックします。

⋮ の [インポート] で、一括で追加できます。



6. キー名／値の種類／値を入力します。

キー名

アプリの開発元に確認した情報を入力します。入力できる文字数は、80文字以内です。

値の種類

入力する値の種類を選択します。

値

アプリの開発元に確認した情報を入力します。入力できる文字数は、1,000文字以内です。配列の場合、追加できる値は10個以内で、1つの値に入力できる文字数は、100文字以内です。

7. [保存] をクリックします。

→ 「Managed App Configuration の追加」画面に戻ります。

8. 内容を確認し、[保存] をクリックします。

→ Managed App Configuration の設定が保存されます。

Managed App Configuration の設定を更新する

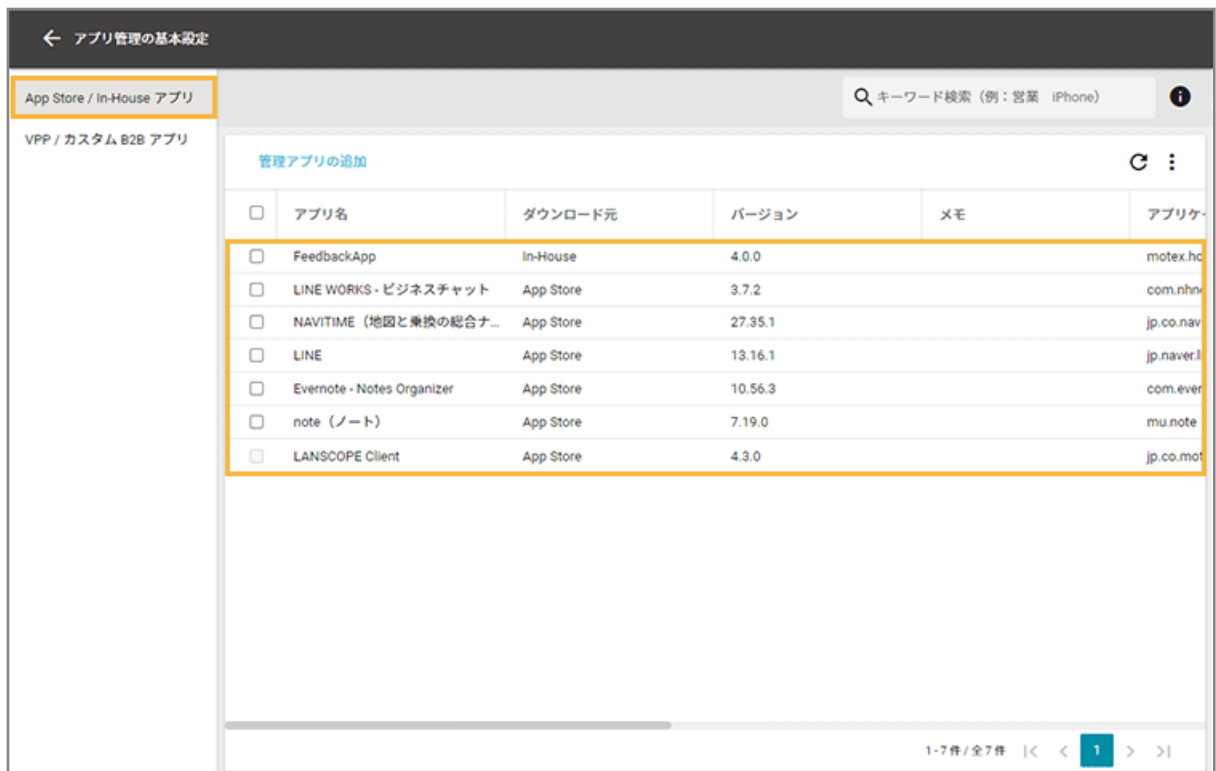
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。




2. [基本設定] をクリックします。

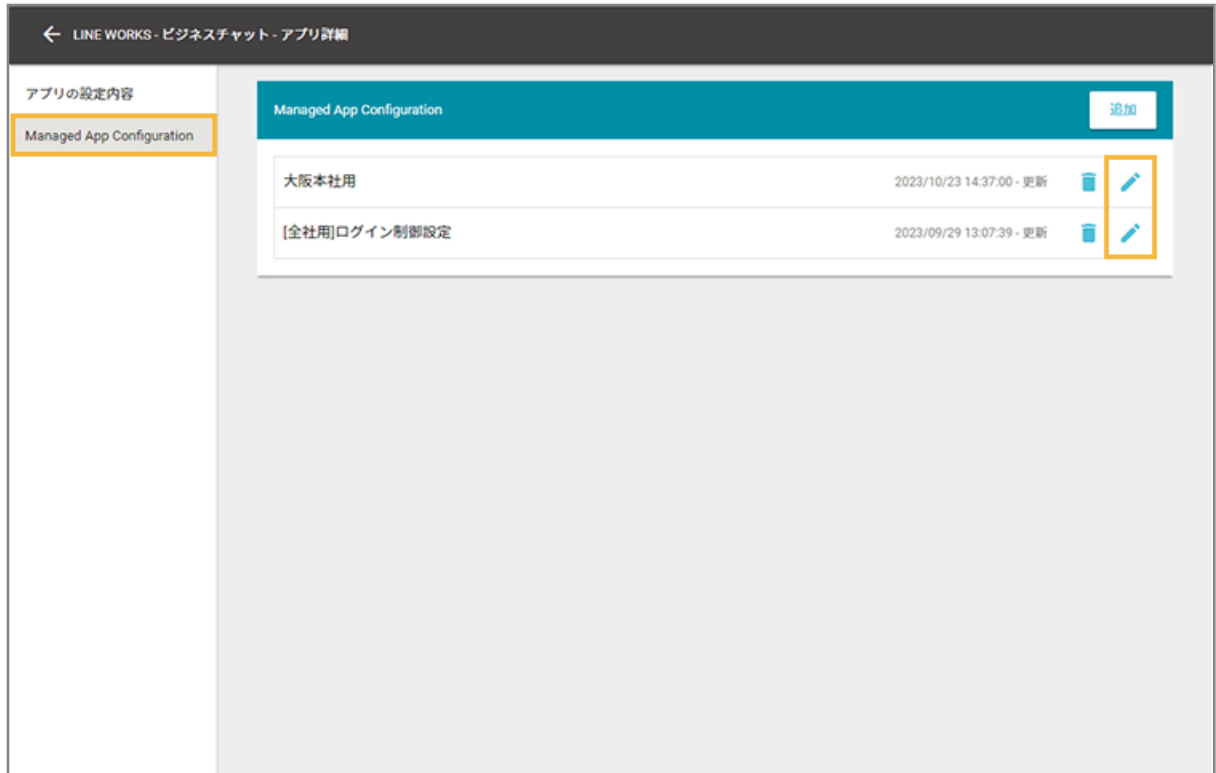


3. [App Store/In-House アプリ] をクリックし、アプリをクリックします。



4. [Managed App Configuration] をクリックし、 をクリックします。

設定を削除する場合は、 をクリックします。



5. 設定項目をクリックします。

- 設定項目を追加する場合は、[設定項目の追加] をクリックします。
- 設定項目を削除する場合は、設定項目をチェックし、[削除する] をクリックします。
- の [インポート] で、一括で追加/編集できます。

Managed App Configuration の編集

設定名 *
[全社用]ログイン制御設定

設定項目 (最大 50 件)

キーワード検索 (例: 営業 iPhone) ⓘ

設定項目の追加 ⓘ

<input type="checkbox"/>	キー名	値の種類	値 1	値 2
<input type="checkbox"/>	パスワード	文字列	パスワード	

キャンセル 保存

6. キー名/値の種類/値を編集します。

← 設定項目の編集

パスワードなど重要な情報を設定するのは避けてください。

キー名 *
パスワード

メモ

値の種類
文字列

値 *
パスワード

キャンセル 保存

キー名

アプリの開発元に確認した情報を入力します。入力できる文字数は、80 文字以内です。

値の種類

入力する値の種類を選択します。

値

アプリの開発元に確認した情報を入力します。入力できる文字数は、1,000 文字以内です。配列の場合、追加できる値は 10 個以内で、1 つの値に入力できる文字数は、100 文字以内です。

7. [保存] をクリックします。

→ 「Managed App Configuration の編集」画面に戻ります。

8. 内容を確認し、[保存] をクリックします。

設定項目の追加	キー名	値の種類	値 1	値 2
<input type="checkbox"/>	パスワード	文字列		

→ Managed App Configuration の設定が保存されます。

ステップ 4： アプリカタログにアプリを公開する

アプリカタログにアプリを登録して公開します。

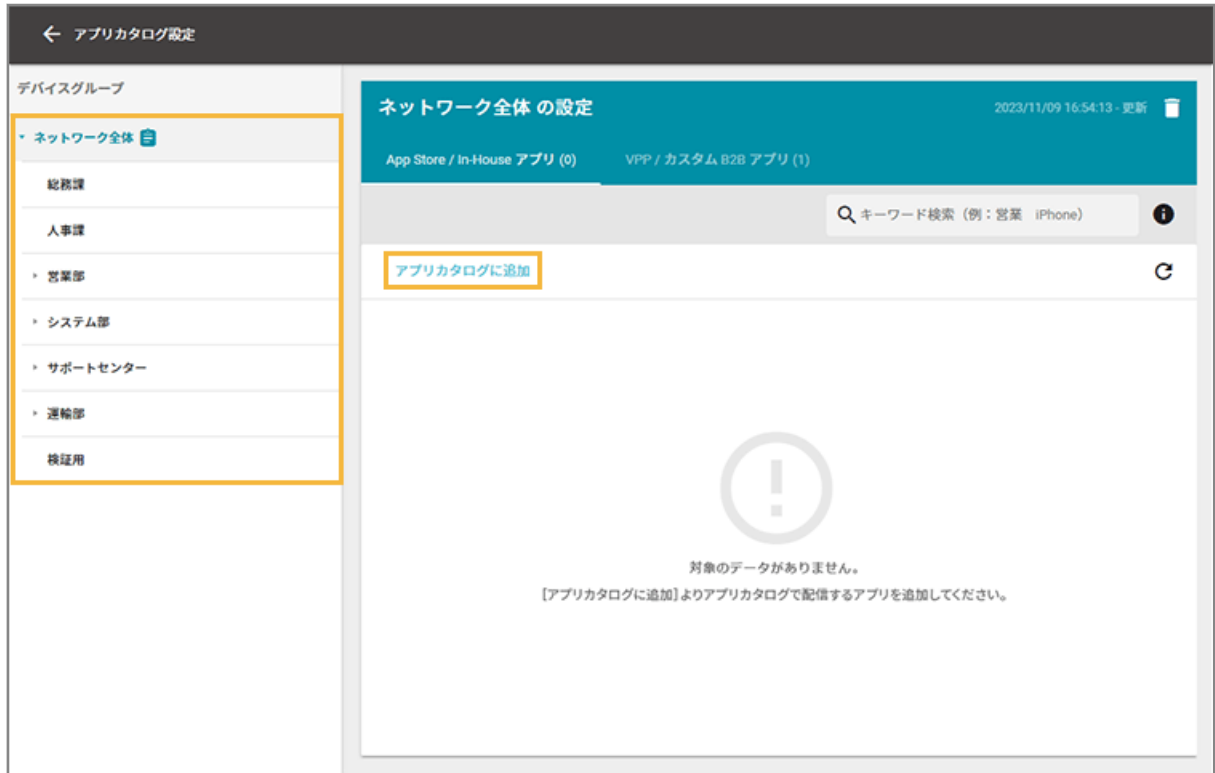
1. [ルール] の [Apple サービス設定] > [iOS 設定] をクリックします。



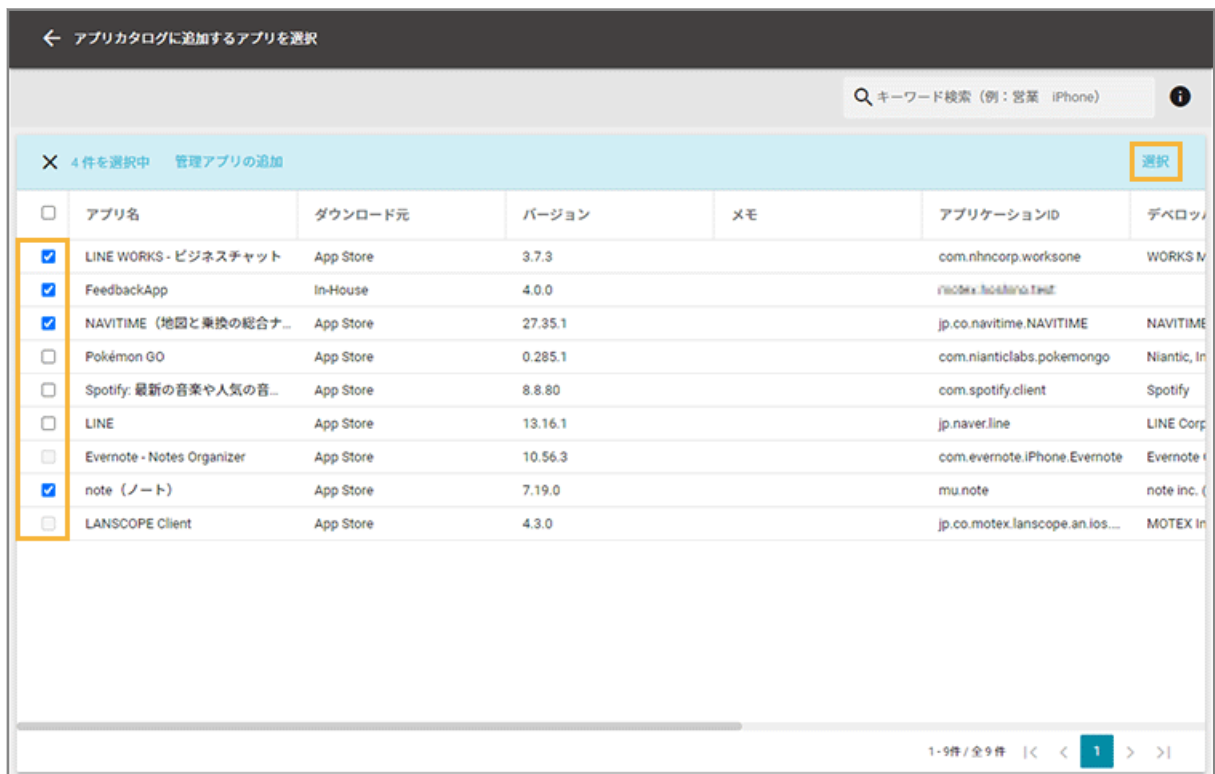
2. [アプリカタログ設定] をクリックします。



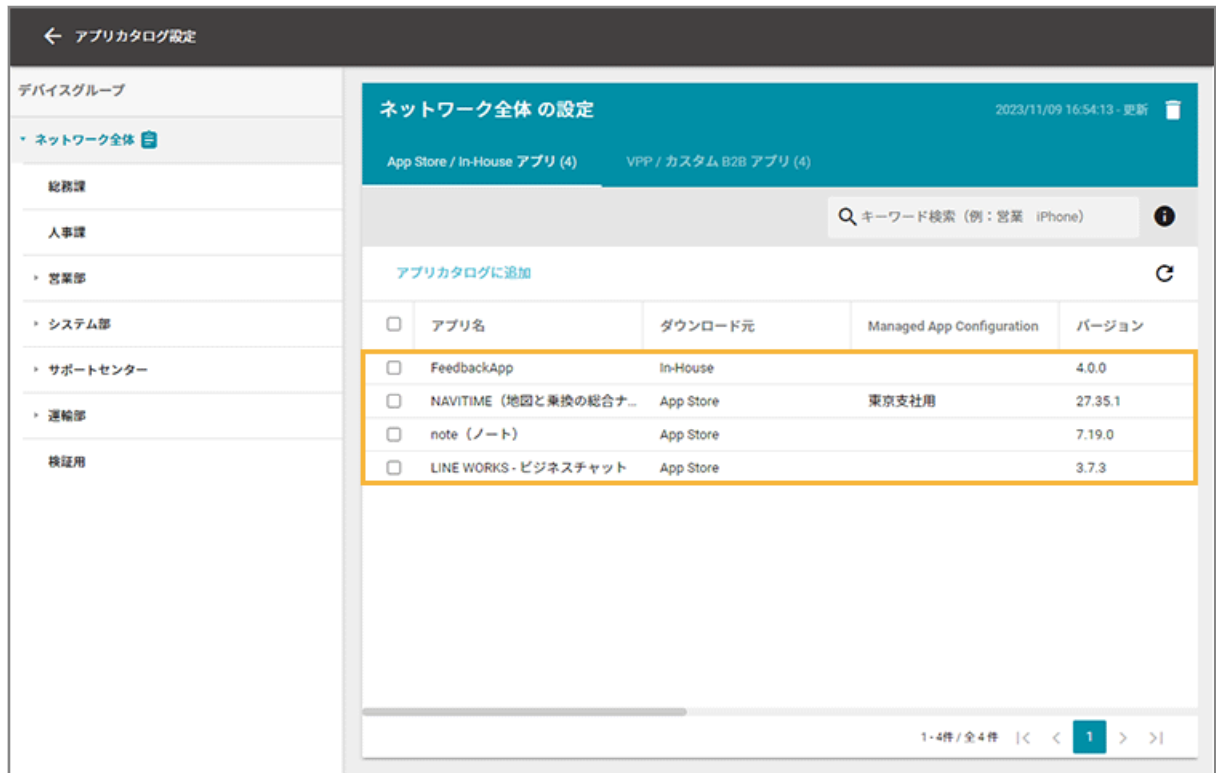
3. アプリを公開するグループをクリックし、[アプリカタログに追加] をクリックします。



4. アプリをチェックし、[選択] をクリックします。



5. 選択したアプリが一覧に追加されたことを確認します。

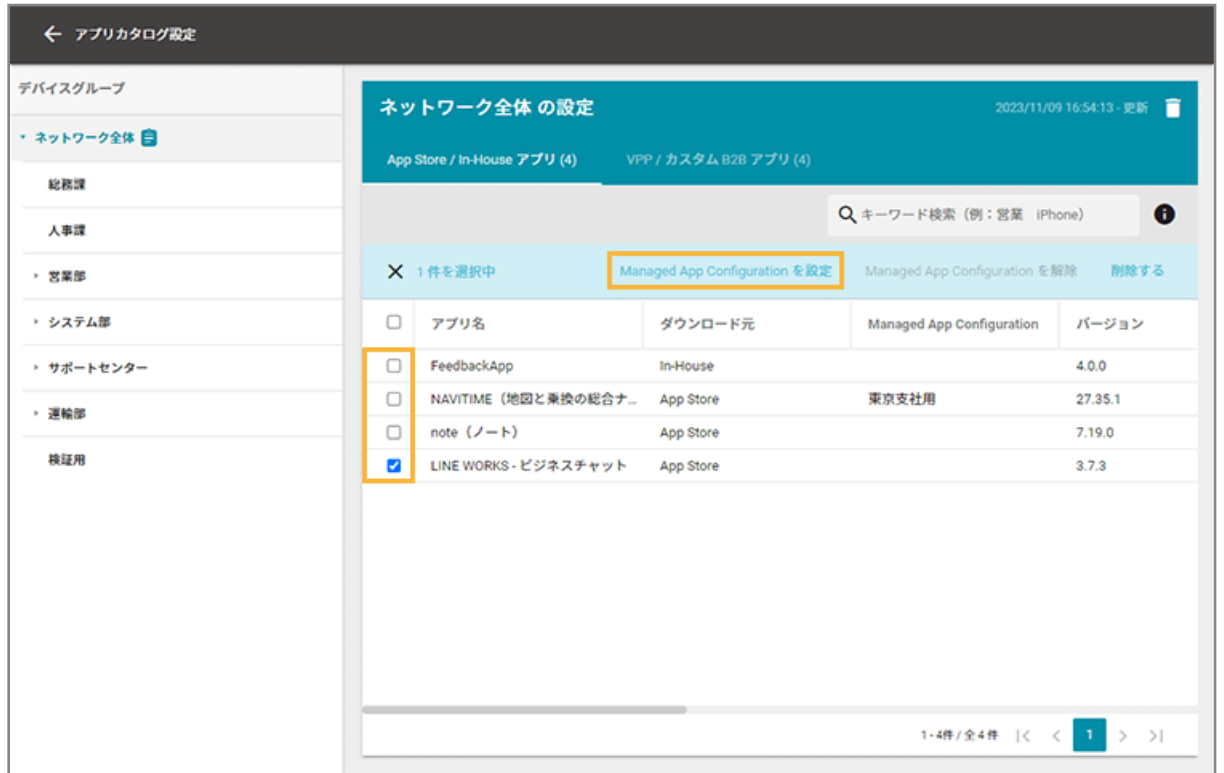


→ 公開完了です。

6. Managed App Configuration の設定を追加する場合は、次の操作をします。

(1) アプリをチェックし、[Managed App Configuration を設定] をクリックします。

すでに設定された Managed App Configuration の設定を解除する場合は、[Managed App Configuration を解除] をクリックし、[OK] をクリックします。



(2) 設定する Managed App Configuration の [選択] をクリックします。



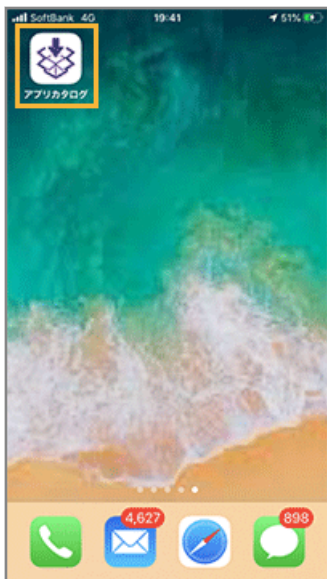
→ Managed App Configuration の設定が追加されます。

ステップ5： デバイス側での操作

ポイント

アップデート版の公開タイミングは、ストアにアプリが公開されてから24時間以内です。アプリカタログに最新バージョンが自動で表示されます。

1. [アプリカタログ] をタップします。



2. アプリを選択し、利用者のタイミングで実行します。





デバイス側で表示されるエラーメッセージ

iOS

アプリのインストール/アップデートで、デバイスにエラーメッセージが表示された場合、次の対応方法を確認してください。

エラーメッセージ	対応方法
契約期間が終了しています。	継続して利用する場合、契約を更新してください。
MDM 証明書が登録されていません。	MDM 証明書を登録してください。
MDM 証明書の有効期限が切れています。	MDM 証明書を更新してください。
デバイスが削除されています。	デバイスが管理コンソールから削除されています。再度、デバイスを登録してください。
MDM 構成プロファイルが削除されています。	再度、MDM 構成プロファイルをインストールしてください。
カタログが作成されていません。	アプリカタログが作成されていません。アプリカタログを作成してください。
カタログからアプリが削除されています。	アプリカタログから該当のアプリが削除されています。再度、アプリカタログにアプリを登録してください。
VPP トークンが登録されていません。	VPP トークンを登録してください。
VPP トークンの有効期限が切れています。	VPP トークンを更新してください。
VPP アプリのライセンスが不足しています。	Apple Business Manager で VPP アプリのライセンスを追加購入してください。
ご利用のデバイスの OS バージョンに対応していません。	アプリでサポートしている OS バージョンを確認してください。

エラーメッセージ	対応方法
プロビジョニングプロファイルの有効期限が切れています。	In-House アプリのプロビジョニングファイルの有効期限が切れているため、プロビジョニングファイルを更新してください。

macOS デバイスにアプリを配信する

macOS

macOS デバイスにアプリを配信します。

- [アプリ配信設定を追加する](#)
- [アプリ配信対象のデバイスを追加する](#)
- [アプリ配信結果を確認する](#)

アプリ配信設定を追加する

macOS

macOS デバイスにアプリを配信するための設定を追加します。

注意

- App Store アプリには対応していません。
- 配信できるアプリの拡張子は、「.pkg」です。
- アプリによっては、デバイスにインストールできない場合があります。配信対象のデバイスにアプリを配信する前に、一部のデバイスに配信をテストし、問題なくインストールできることを確認してください。

ステップ :

1. [配信アプリを準備する](#)
2. [アプリ配信設定を追加する](#)

ステップ 1 : 配信アプリを準備する

1. 配信するアプリを、デバイスがアクセスできるオンラインストレージに配置します。

HTTPS でアクセスできるオンラインストレージに配置します。

配置したオンラインストレージの URL を管理コンソールで設定し、デバイス側でインストールできるようにします。

注意

パブリックアクセス可能なオンラインストレージに配置する必要があります。情報漏えいのリスクがあるため、機密ファイルを配置しないように注意してください。

ステップ 2： アプリ配信設定を追加する

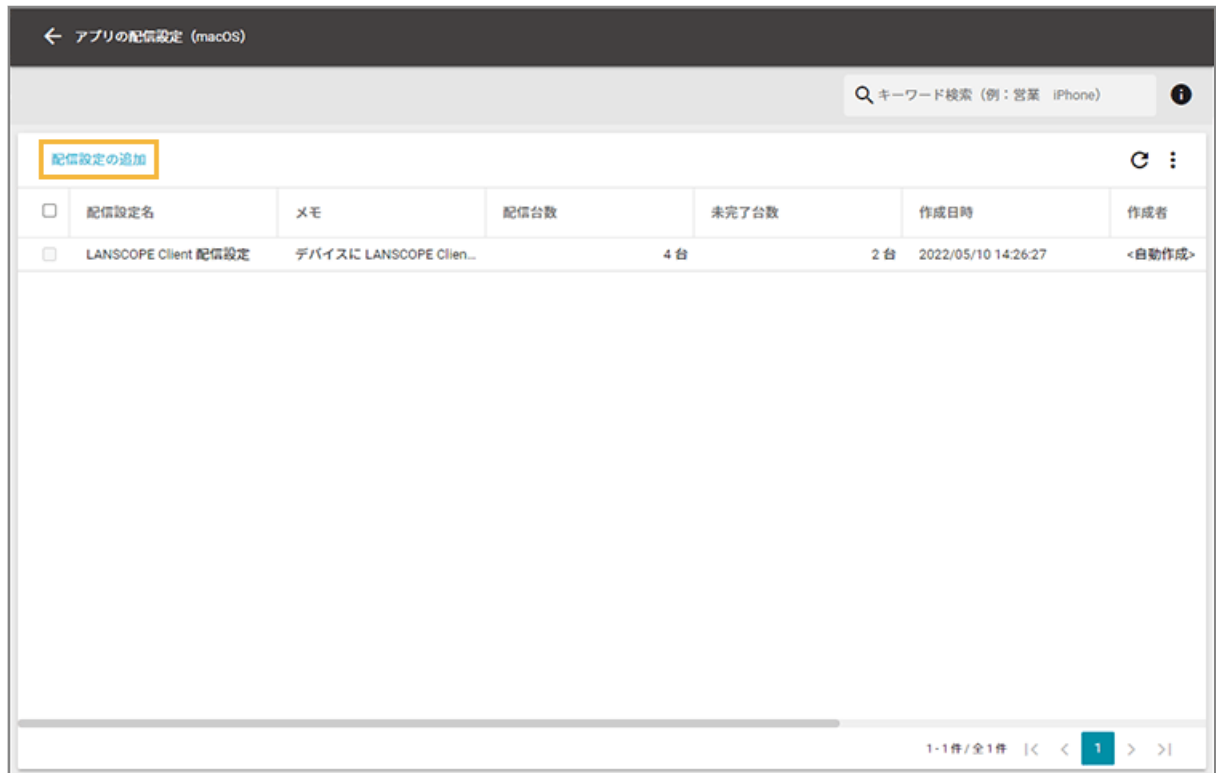
1. [ルール] の [Apple サービス設定] > [macOS 設定] をクリックします。



2. [アプリ配信設定] をクリックします。



3. [配信設定の追加] をクリックします。



4. 配信設定名を入力します。

配信設定名

配信設定名 *

5. アプリを配置したオンラインストレージの URL を入力します。

アプリ配信設定

配信アプリを選択

URL *

HTTPS でアクセス可能で [pkg] 拡張子のファイルがダウンロードできるダウンロードリンクを設定してください。

6. [ハッシュ値を計算する] をクリックし、オンラインストレージに配置した配信アプリと同じファイルを選択します。

ハッシュ値の設定 *

ファイルが正しいかをチェックするために、ハッシュ値を計算してファイルの同一性を確認します。
 配信するファイルを選択すると、ハッシュ値を計算します。
 ※ ファイルはハッシュ値を計算するためだけに使用され、LANSCOPE エンドポイントマネージャー クラウド版のストレージに保存されることはありません。
 ※ 計算が完了するまでに時間がかかる場合があります。

ハッシュ値を計算する

→ ハッシュ値が計算されます。

デバイスに配信アプリをインストールするとき、配信アプリのファイルが同じものかどうかを確認するために使用します。

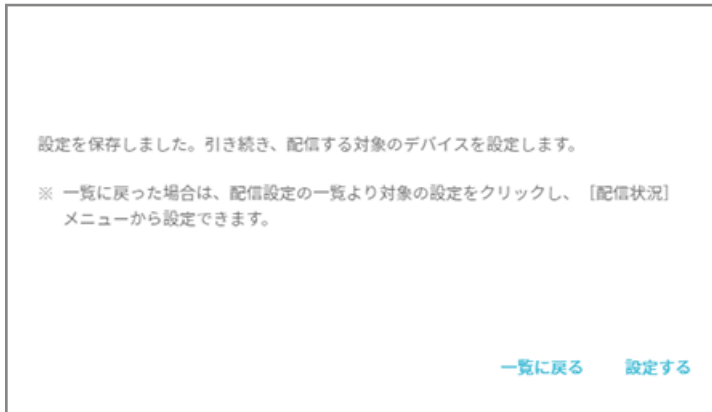
7. MDM 構成プロファイルのインストール後に自動配信する場合は、[MDM 構成プロファイルがインストールされたら配信する] をチェックし、対象のデバイスグループを選択します。

The screenshot shows a configuration screen with a yellow border. At the top, under the heading "オプション" (Options), there is a checked checkbox labeled "MDM 構成プロファイルがインストールされたら配信する" (Distribute when MDM configuration profile is installed). Below this, the text "対象グループを選択*" (Select target group*) is followed by "デバイスグループ (0 件)" (Device groups (0 items)). A "選択" (Select) button is highlighted with a yellow box.

8. 必要に応じてメモを入力し、[保存] をクリックします。

The screenshot shows a detailed configuration screen with a dark header bar containing a back arrow, the text "配信設定の追加" (Add distribution settings), and a "保存" (Save) button highlighted with a yellow box. The main content area has a teal header "アプリ配信設定" (Application distribution settings). Under "配信アプリを選択" (Select distribution app), there is a "URL*" field with a placeholder and a note: "HTTPS でアクセス可能で [pkg] 拡張子のファイルがダウンロードできるダウンロードリンクを設定してください。" (Set a download link that can be accessed via HTTPS and can download files with the [pkg] extension). Below this is a "ハッシュ値の設定*" (Hash value settings*) section with explanatory text and a "ハッシュ値を計算する" (Calculate hash value) button. A SHA256 hash is displayed. At the bottom, under "オプション" (Options), there is a checked checkbox "MDM 構成プロファイルがインストールされたら配信する" (Distribute when MDM configuration profile is installed). Below it, "対象グループを選択*" (Select target group*) shows "デバイスグループ (1 件)" (Device groups (1 item)) with a "選択" (Select) button and a selected item "ネットワーク全体 (4 台)" (All network devices (4 devices)) with a close icon. A "メモ" (Memo) field is highlighted with a yellow box at the bottom.

→ アプリ配信設定の追加が完了します。



アプリ配信対象のデバイスを追加する

macOS

配信対象のデバイスを追加して、アプリの配信設定を実行します。

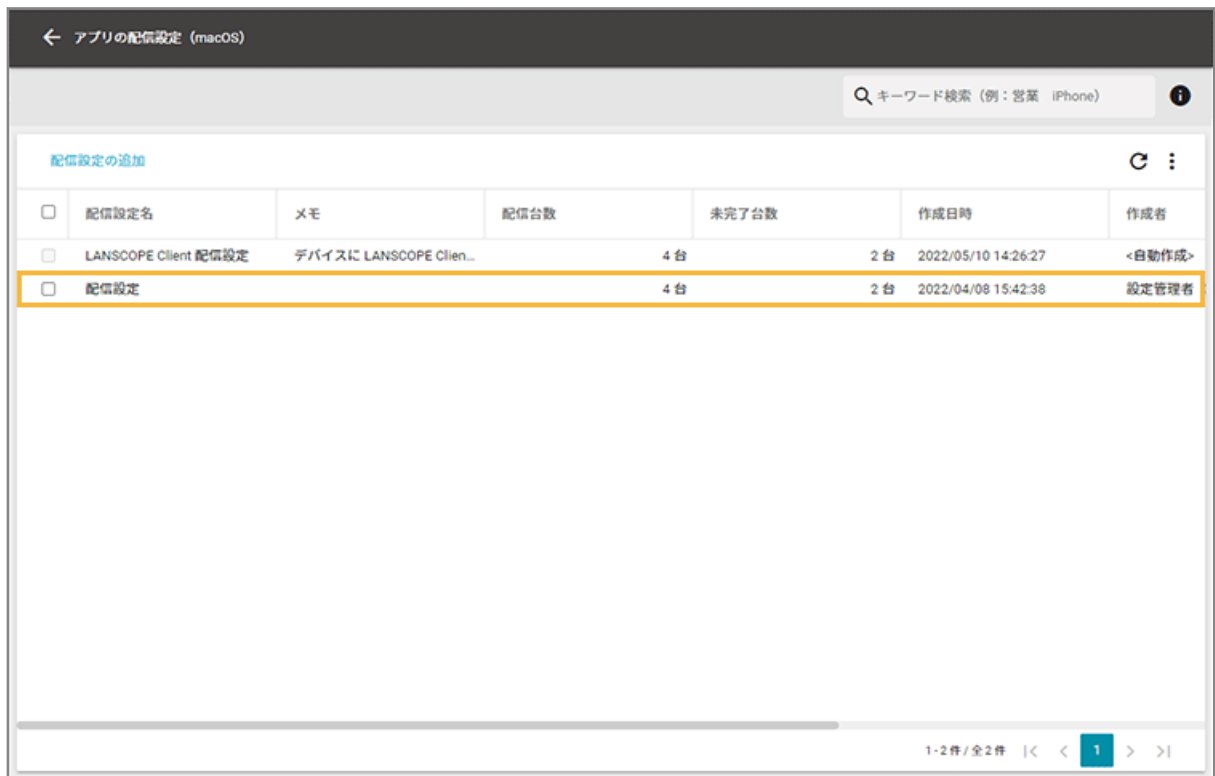
1. 【ルール】 の【Apple サービス設定】 > 【macOS 設定】 をクリックします。



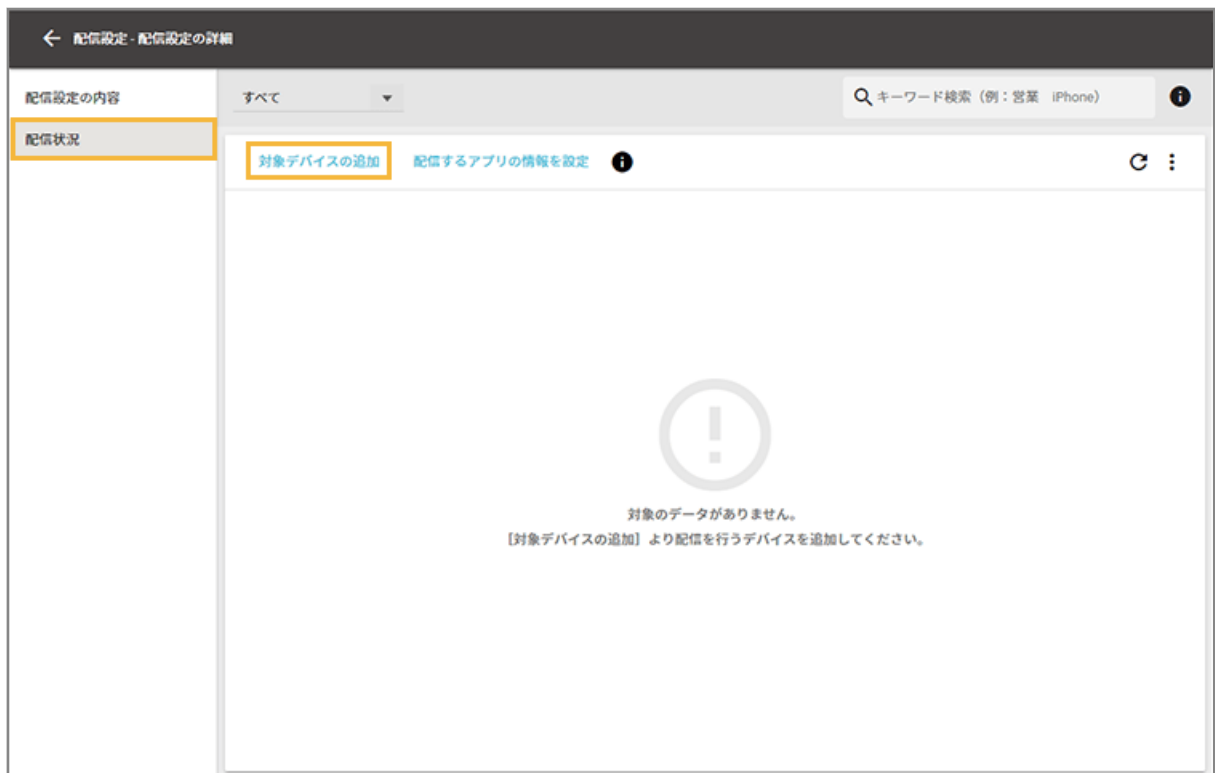
2. 【アプリ配信設定】 をクリックします。



3. アプリの配信設定をクリックします。



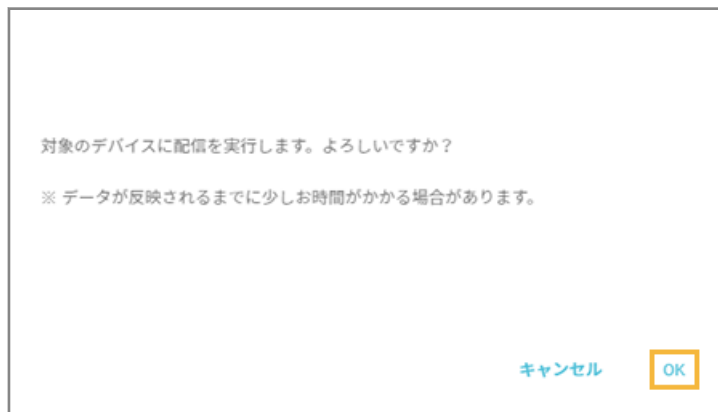
4. [配信状況] をクリックし、[対象デバイスの追加] をクリックします。



5. 配信対象のデバイスをチェックし、[追加] をクリックします。



6. [OK] をクリックします。



→ 対象デバイスに、アプリの配信設定が実行されます。

アプリ配信結果を確認する

macOS

アプリ配信の結果を確認し、必要に応じて再配信します。

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



2. [アプリ配信設定] をクリックします。



3. アプリの配信設定をクリックします。

← アプリの配信設定 (macOS)

キーワード検索 (例: 営業 iPhone)

配信設定の追加

<input type="checkbox"/>	配信設定名	メモ	配信台数	未完了台数	作成日時	作成者
<input type="checkbox"/>	LANSCOPE Client 配信設定	デバイスに LANSCOPE Clie...	4 台	2 台	2022/05/10 14:26:27	<自動作成>
<input type="checkbox"/>	配信設定		4 台	2 台	2022/04/08 15:42:38	設定管理者

1-2件 / 全2件 |< < 1 > >|

4. [配信状況] をクリックし、[配信するアプリの情報を設定] をクリックします。

配信したアプリがデバイスにインストールされていることを確認するため、アプリの情報を紐づけます。紐づけたアプリのバージョンから、インストール状況を確認できます。

← 配信設定 - 配信設定の詳細

配信設定の内容

配信状況

すべて

キーワード検索 (例: 営業 iPhone)

対象デバイスの追加

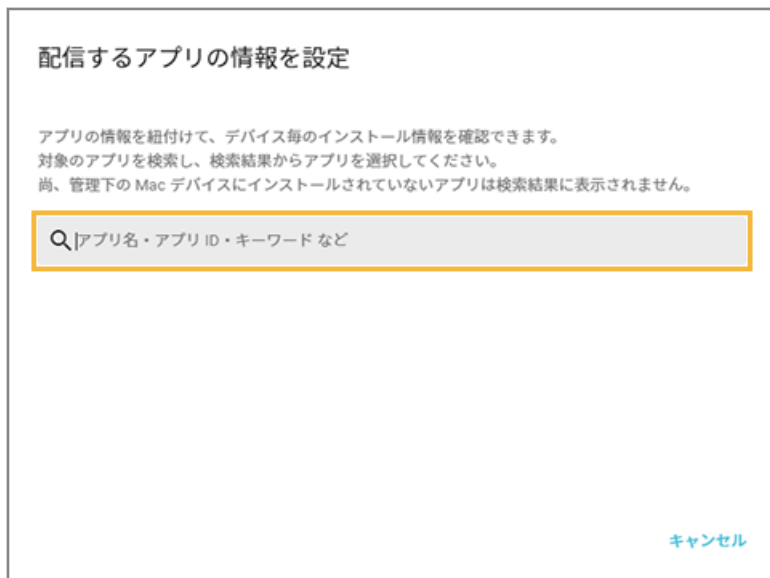
配信するアプリの情報を設定

対象のデータがありません。
[対象デバイスの追加] より配信を行うデバイスを追加してください。

5. アプリを検索し、選択します。

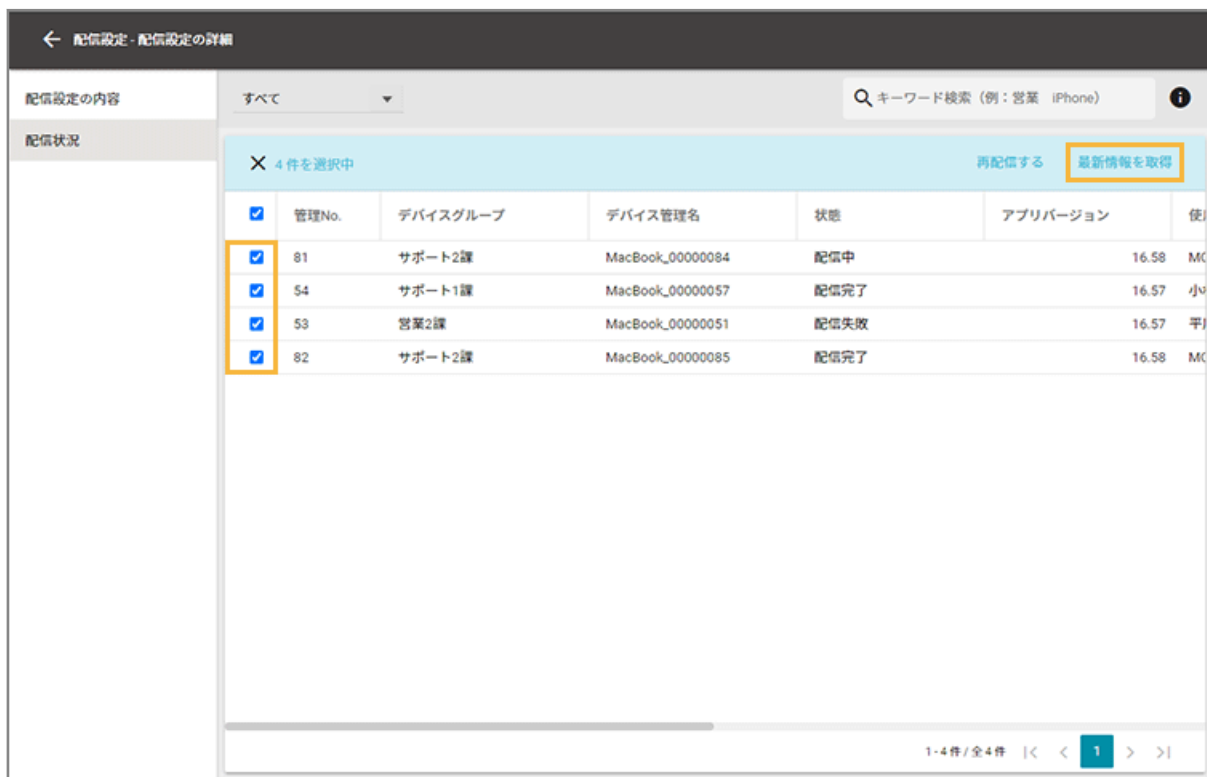
[リスト] > [アプリ] 画面で表示されるアプリから選択します。

すでにアプリの情報を設定している場合は、「基本情報」画面が表示されます。[変更] をクリックすると、アプリ情報を再設定できます。

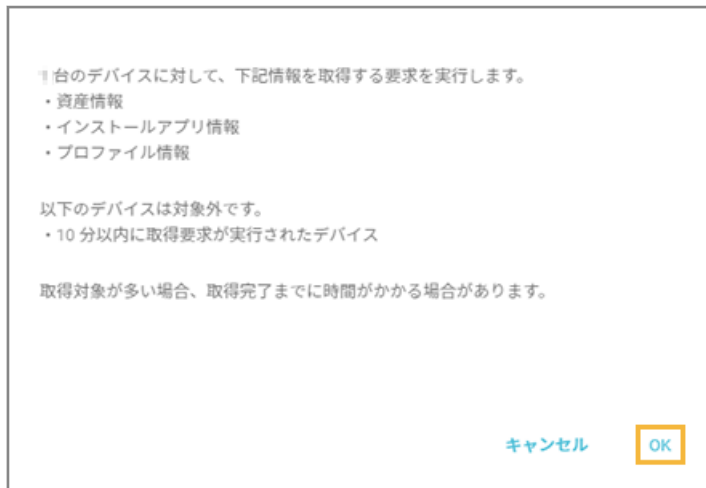


→ 「配信設定の詳細」画面に戻ります。

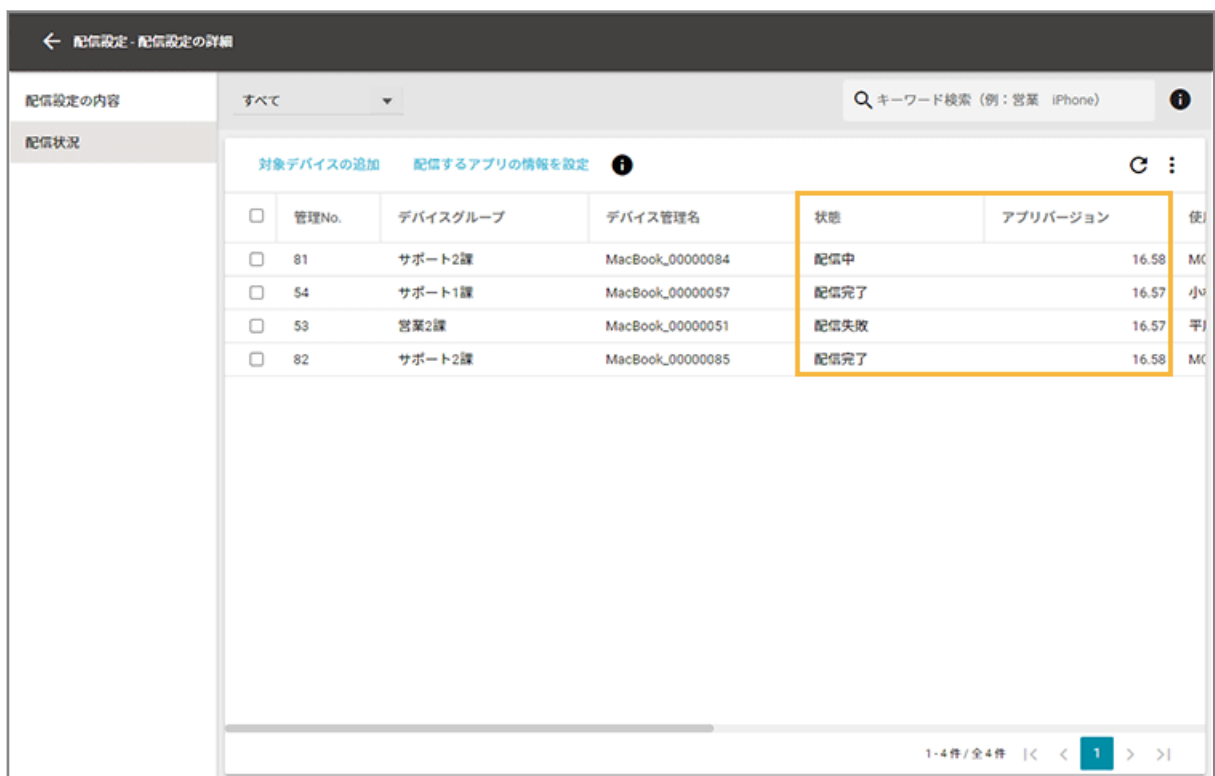
6. デバイスをチェックし、[最新情報を取得] をクリックします。



7. [OK] をクリックします。



8. 状態／アプリバージョンを確認します。



状態

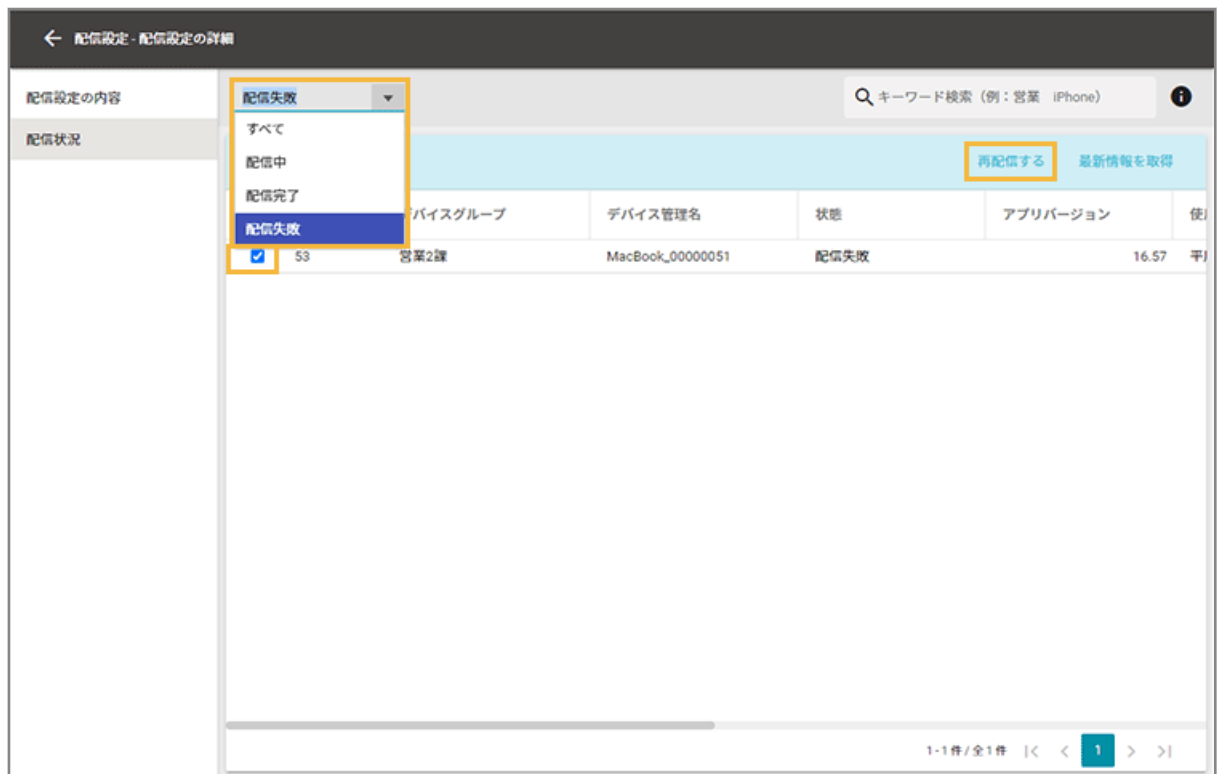
- 配信中
アプリが配信中の状態のときに表示されます。
- 配信完了
アプリが配信された状態のときに表示されます。
- 配信失敗
アプリの配信に失敗した状態のときに表示されます。再配信、または MDM 構成プロファイルを再インストールする必要があります。

アプリバージョン

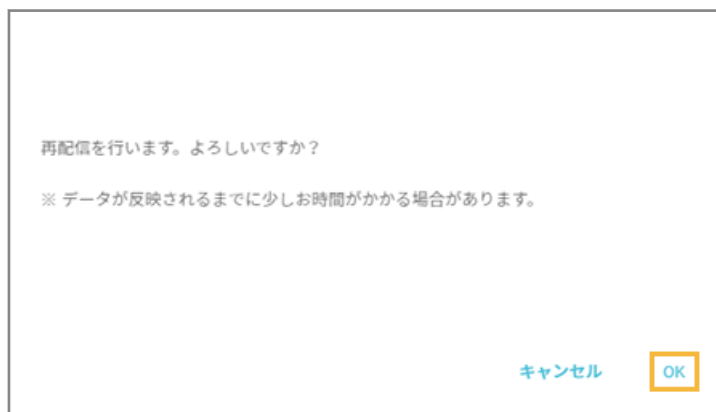
[配信するアプリの情報を設定] で設定したアプリのバージョンが表示されます。

デバイス側でアプリをインストールすると、配信したアプリのバージョンに更新されます。

9. 再配信する場合、配信対象の「状態」を選択し、デバイスをチェックして、[再配信する] をクリックします。



10. [OK] をクリックします。



→ 再配信が実行されます。

6-3 記録メディア制御設定をする

Windows macOS

記録メディア制御に必要な設定をします。WPD 機器や、USB/SD カードなどの記憶領域を持つ記録メディアを許可/読み取り専用/禁止に設定することで、機密資料の閲覧/持ち出しなどを未然に防止するサポートをします。

注意

マウスやキーボードなどの記憶領域を持たない機器は制御対象外です。



- [記録メディア全体の制御設定をする](#)
- [デバイスごとに個別で制御設定する](#)

記録メディア全体の制御設定をする

Windows macOS

デバイスグループごとに、記録メディア全体の制御設定をします。

- [記録メディアを制御する](#)
- [特定の記録メディアを除外する](#)

記録メディアを制御する

Windows macOS

デバイスグループごとに、記録メディアの許可/読み取り専用/禁止を設定をします。

1. [ルール] の [記録メディア制御] > [全体設定] をクリックします。



2. デバイスグループをクリックし、[編集] をクリックします。



3. 全体設定で、記録メディアの制御設定を選択します。



全体設定

- 許可する（書き込み/読み取り可）
接続されたすべての記録メディアを許可します。
- 読み取り専用にする
接続されたすべての記録メディアを読み取り専用にします。
- 禁止する
接続されたすべての記録メディアを禁止します。

除外設定

全体設定で「読み取り専用にする」「禁止する」を選択した場合、除外する記録メディアを設定できます。詳細は、[特定の記録メディアを除外する](#)を参照してください。

4. 禁止時にポップアップで通知する場合、共通設定の「通知する」をチェックし、「タイトル」「メッセージ」を入力します。

ネットワーク全体 の設定 キャンセル 保存

指定したキーワードをフレンドリーネーム/デバイスの説明と紐付けて許可する

[許可するキーワードの設定](#)

共通設定

禁止時にポップアップで通知する

通知する

タイトル*
禁止通知 - 記録メディアの閲覧禁止

メッセージ*
記録メディアのアクセスは、本内ポリシーによって禁止されています。
%URL%。

[過去に入力された通知設定から引用](#)

※ メッセージに以下のキーワードを入力すると、禁止時の各情報に変換されます。

%TIME%	: 抵触時の日時
%MEDIA%	: 記録メディアの情報

5. 「保存」をクリックします。



→ 記録メディア制御の設定が保存されます。

特定の記録メディアを除外する

Windows macOS

デバイスグループごとに、記録メディア制御の除外設定をします。除外設定は、全体設定で「読み取り専用にする」または「禁止する」を選択した場合に設定できます。

記録メディア情報を設定する	指定した記録メディアを許可／読み取り専用を設定します。
ベンダー ID／プロダクト ID で設定する	指定したメーカー／製品番号を許可／読み取り専用を設定します。大量の記録メディアを設定するときに利用します。
キーワードで許可設定する	指定したキーワードをフレンドリーネーム／デバイスの説明と紐づけて許可します。シリアル No が存在しない記録メディアを許可するときに利用します。

■ 記録メディア情報を設定する

周辺機器接続ログから記録メディアを追加する

1. [ルール] の [記録メディア制御] > [全体設定] をクリックします。



2. デバイスグループをクリックし、[編集] をクリックします。



3. 除外設定の [設定する] をチェックし、[記録メディアの個別設定] をクリックします。



4. [ログから選択して追加] をクリックします。

× 記録メディアの個別設定

ログから選択して追加 手動入力して追加

<input type="checkbox"/>	シリアル No	ベンダー ID	プロダクト ID	許可	読み取り専用	メモ
<input type="checkbox"/>	XXXXXXXXXXXXXXXXXXXX			○	-	
<input type="checkbox"/>	XXXXXXXXXXXXXXXXXXXX			-	○	
<input type="checkbox"/>	XXXXXXXXXXXX	0x0457	0x0151	○	-	
<input type="checkbox"/>	XXXXXXXXXXXX	0x0457	0x0151	-	○	
<input type="checkbox"/>	XXXXXXXXXXXX	0x0457	0x0151	○	-	

登録済み設定数: 5 / 10,000

1-5 件 / 全 5 件 |< < 1 > >|

5. 記録メディアをチェックし、[許可して追加] または [読み取り専用にして追加] をクリックします。
- 周辺機器接続ログは、最大 10,000 件取得できます。
 - 記録メディアは、最大 100 件選択できます。

← ログから選択して追加

ネットワーク全体 ▼ 期間: 2023/03/03 00:00 ~ 15:50 🔍 キーワード検索 (例: 営業 iPhone) ⓘ

× 1件を選択中 許可して追加 読み取り専用にして追加

	日時	ログオンユーザー名	デバイス管理名	シリアル No	ベンダー名
<input checked="" type="checkbox"/>	2023/03/03 08:01:37	goro.mo	MacBook_00000085	XXXXXXXXXXXXXXXXXXXX	Kingston
<input type="checkbox"/>	2023/03/03 08:54:17	kappei.yoshida	Surface Pro 5_0000...	XXXXXXXXXXXXXXXXXXXX	SHARP Corporation
<input type="checkbox"/>	2023/03/03 08:54:17	goro.mo	MacBook_00000085	XXXXXXXXXXXXXXXXXXXX	SHARP Corporation
<input type="checkbox"/>	2023/03/03 08:58:49	kappei.yoshida	Surface Pro 5_0000...	XXXXXXXXXXXXXXXXXXXX	I-O DATA
<input type="checkbox"/>	2023/03/03 08:58:49	goro.mo	MacBook_00000085	XXXXXXXXXXXXXXXXXXXX	I-O DATA
<input type="checkbox"/>	2023/03/03 09:01:20	kappei.yoshida	Surface Pro 5_0000...	XXXXXXXXXXXXXXXXXXXX	I-O DATA
<input type="checkbox"/>	2023/03/03 09:01:20	goro.mo	MacBook_00000085	XXXXXXXXXXXXXXXXXXXX	I-O DATA
<input type="checkbox"/>	2023/03/03 09:03:31	kappei.yoshida	Surface Pro 5_0000...	XXXXXXXXXXXXXXXXXXXX	Logitech
<input type="checkbox"/>	2023/03/03 09:03:31	goro.mo	MacBook_00000085	XXXXXXXXXXXXXXXXXXXX	Logitech

1-9件 / 全9件 |< < 1 > >|

注意

「シリアル No」がない記録メディアは選択できません。

→ 「記録メディアの個別設定」画面に戻ります。

6. 「記録メディアの個別設定」画面を閉じます。

7. [保存] をクリックします。



→ 記録メディア制御の設定が保存されます。

手動入力して記録メディアを追加する

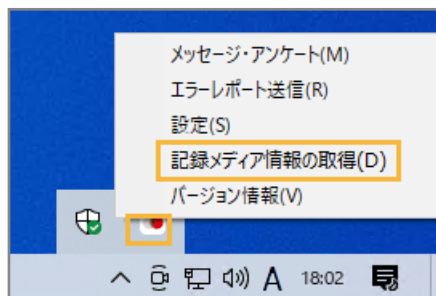
ステップ：

1. [記録メディア情報を取得する](#)
2. [記録メディアを設定する](#)

ステップ 1： 記録メディア情報を取得する

LANSCOPE クライアントをインストールしているデバイスで、記録メディア情報を取得します。

1. タスクバーの通知領域の LANSCOPE Client を右クリックし、[記録メディア情報の取得] をクリックします。



2. 記録メディアの種類を選択し、デバイスに接続します。



SD メモリカード

PC カード／PC 内蔵の SD メモリカードを接続する場合に選択します。

USB 接続機器

USB メモリや、USB 接続するマルチカードリーダー／SD メモリカードなど、接続形態が USB の記録メディアを接続する場合に選択します。

→ 記録メディア情報が取得されます。

3. 記録メディア情報を確認します。



クリックした列の取得情報をコピーします。

[CSV エクスポート]

一覧に表示されているすべての取得情報を CSV ファイルでエクスポートします。

エクスポートした CSV ファイルは、制御区分を編集し、一括設定に利用できます。詳細は、[記録メディアを一括で設定する](#)を参照してください。

[まとめてコピー]

一覧に表示されているすべての取得情報をコピーします。コピーした取得情報は、テキストエディターなどにペーストして確認します。

ステップ 2： 記録メディアを設定する

1. [ルール] の [記録メディア制御] > [全体設定] をクリックします。



2. デバイスグループをクリックし、[編集] をクリックします。



3. 除外設定の [設定する] をチェックし、[記録メディアの個別設定] をクリックします。



4. [手動入力して追加] をクリックします。

× 記録メディアの個別設定

ログから選択して追加 **手動入力して追加** ⋮

<input type="checkbox"/>	シリアル No	ベンダー ID	プロダクト ID	許可	読み取り専用	メモ
<input type="checkbox"/>	XXXXXXXXXXXXXXXXXXXX			○	-	
<input type="checkbox"/>	XXXXXXXXXXXXXXXXXXXX			-	○	
<input type="checkbox"/>	XXXXXXXXXXXX	0x0457	0x0151	○	-	
<input type="checkbox"/>	XXXXXXXXXXXX	0x0457	0x0151	-	○	
<input type="checkbox"/>	XXXXXXXXXXXX	0x0457	0x0151	○	-	

登録済み設定数: 5 / 10,000 1-5件 / 全5件 |< < 1 > >|

5. 記録メディア情報を入力し、制御設定を選択して、[保存] をクリックします。

← 手動入力して追加 保存

Windows デバイスに記録メディアを接続し、取得した情報を追加します。
タスクバーの通知領域にある LANSCOPE Client のアイコンを右クリックし「記録メディア情報の取得」を利用してください。

シリアル No.*
記録メディアの「シリアル No」を指定してください。

ベンダー ID
記録メディアの「ベンダー ID」を指定してください。

プロダクト ID
記録メディアの「プロダクト ID」を指定してください。

メモ

制御設定*
 許可 読み取り専用

→ 「記録メディアの個別設定」画面に戻ります。

6. 「記録メディアの個別設定」画面を閉じます。

7. [保存] をクリックします。

ネットワーク全体の設定 キャンセル 保存

全体設定

グループで管理しているデバイス全体に対して読み取り専用/禁止に関する設定をします。

許可する (書き込み/読み取り可)
 読み取り専用にする
 禁止する

除外設定
禁止または読み取り専用の設定をしている場合に、除外する記録メディアを設定する

設定する

指定した記録メディア毎に許可/読み取り専用にする

記録メディアの個別設定

▼ その他の設定

→ 記録メディア制御の設定が保存されます。

記録メディアを一括で設定する

1. [ルール] の [記録メディア制御] > [全体設定] をクリックします。



2. デバイスグループをクリックし、[編集] をクリックします。



3. 除外設定の [設定する] をチェックし、[記録メディアの個別設定] をクリックします。



4.  をクリックし、[エクスポート] をクリックします。

× 記録メディアの個別設定

ログから選択して追加 手動入力して追加

<input type="checkbox"/>	シリアル No	ベンダー ID	プロダクト ID	許可	読み取り専用	
<input type="checkbox"/>	XXXXXXXXXXXXXXXXXXXX			○	-	 インポート エクスポート
<input type="checkbox"/>	XXXXXXXXXXXXXXXXXXXX			-	○	
<input type="checkbox"/>	XXXXXXXXXXXXXXXXXXXX	0x0457	0x0151	○	-	
<input type="checkbox"/>	XXXXXXXXXXXXXXXXXXXX	0x0457	0x0151	-	○	
<input type="checkbox"/>	XXXXXXXXXXXXXXXXXXXX	0x0457	0x0151	○	-	

登録済み設定数: 5 / 10,000 1-5件 / 全5件 < < 1 > >

→ CSV ファイルがエクスポートされます。

5. 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。

- 記録メディアは、最大 10,000 件追加できます。
- 「ベンダー ID」「プロダクト ID」「シリアル No」「制御区分」「メモ」を入力します。
 - 「ベンダー ID」「プロダクト ID」「シリアル No」を入力した場合、USB メモリが制御されます。
 - 「シリアル No」だけを入力した場合、SD カードが制御されます。

6.  をクリックし、[インポート] をクリックします。



7. 管理コンソールの記載に従って、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。



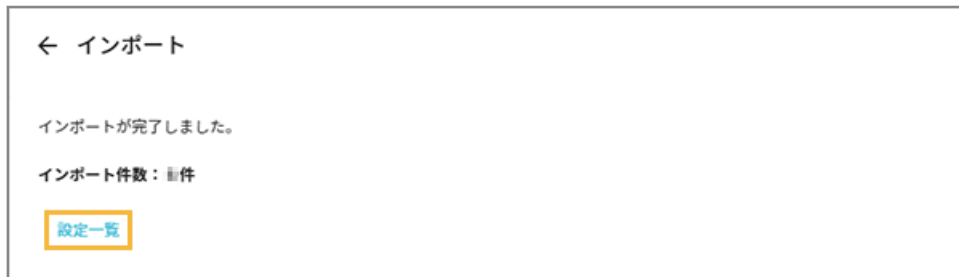
→ 「関連づける列名」が自動的に選択されます。

「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] をクリックします。

→ インポートが完了します。

8. [設定一覧] をクリックします。



→ 「記録メディアの個別設定」画面に戻ります。

9. 「記録メディアの個別設定」画面を閉じます。

10. [保存] をクリックします。



→ 記録メディア制御の設定が保存されます。

■ ベンダー ID/プロダクト ID で設定する

1. [ルール] の [記録メディア制御] > [全体設定] をクリックします。




2. デバイスグループをクリックし、[編集] をクリックします。



3. 除外設定の「設定する」をチェックし、「その他の設定」の「ベンダー ID/プロダクト ID の設定」をクリックします。



4. [追加] をクリックします。

- ベンダー ID/プロダクト ID の設定は、最大 1,000 件追加できます。
-  の [インポート] で、一括で追加できます。

× ベンダー ID/プロダクト ID の設定

追加

<input type="checkbox"/>	ベンダー ID	プロダクト ID	許可	読み取り専用	メモ	↓ 更新日時
<input type="checkbox"/>	0x0411	0x0098	○	-	営業部_USB	2021/02/02 11:3
<input type="checkbox"/>	0x196D	0x0300	○	-	サポート部_USB	2021/02/02 11:3
<input type="checkbox"/>	0x0457	0x0151	○	-	貸出用_USB	2021/02/02 11:3
<input type="checkbox"/>	0x048B	0x0CB5	○	-	I-O DATA_Secure UFD MOT U...	2021/02/02 11:3

登録済み設定数: 4 / 1,000

1-4件 / 全4件 |< < 1 > >|

5. 項目を入力し、[保存] をクリックします。

→ 「ベンダー ID/プロダクト ID の設定」画面に戻ります。

6. 「ベンダー ID/プロダクト ID の設定」画面を閉じます。

7. [保存] をクリックします。

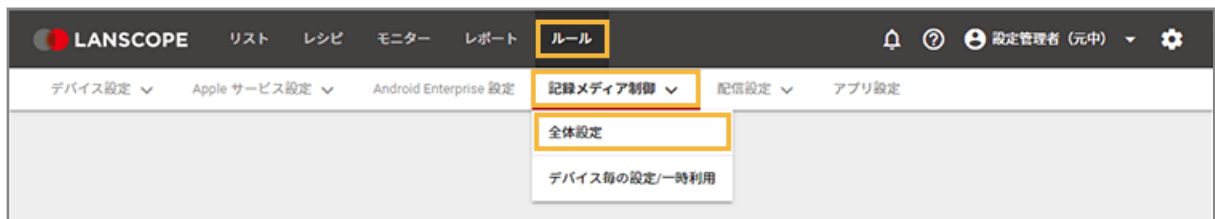
→ ベンダー ID/プロダクト ID の設定が保存されます。

■ キーワードで許可設定する

注意

「USB Composite Device」や「複合デバイス」など、さまざまな記録メディアで共通して保有するキーワードでの設定は、予期しない記録メディアまで許可されることがあります。そのため、キーワードでの設定ではなく、ベンダーID/プロダクトIDで制御設定してください。

1. [ルール] の [記録メディア制御] > [全体設定] をクリックします。



2. デバイスグループをクリックし、[編集] をクリックします。



3. 除外設定の [設定する] をチェックし、[その他の設定] の [許可するキーワードの設定] をクリックします。



4. [追加] をクリックします。

キーワードの設定は、最大 100 件追加できます。



5. キーワードを入力し、[保存] をクリックします。

ポイント

- キーワードには、フレンドリーネームでの設定をおすすめします。フレンドリーネームはデバイス製品名を取得するため、入力したキーワードと紐づけやすくなります。
- 接続時にドライバーを読み込むポータブルデバイスは、接続時のログからドライバーの読み込み前と読み込み後の2つのフレンドリーネームを確認し、設定してください。
- デバイスの説明は、[ログ] > [検索] で周辺機器接続ログを検索して確認できます。
macOS ではデバイスの説明の情報が存在しないため、他のキーワードを設定してください。

← 許可するキーワードの設定

保存

キーワード *

記録メディアの「フレンドリーネーム」または「デバイスの説明」と紐付けます。
(フレンドリーネームとの紐付けを推奨します)

メモ

→ 「許可するキーワードの設定」画面に戻ります。

6. 「許可するキーワードの設定」画面を閉じます。

7. [保存] をクリックします。



→ 許可するキーワードの設定が保存されます。

デバイスごとに個別で制御設定する

Windows macOS

デバイスごとに、個別で制御/一時利用を設定をします。

ポイント

「デバイス毎の設定/一時利用」は、「全体設定」の設定よりも優先されます。

1. 【ルール】の【記録メディア制御】>【デバイス毎の設定/一時利用】をクリックします。



2. 【制御対象デバイスの追加】をクリックします。

- 制御対象デバイスは、最大 100,000 件表示できます。
- 制御対象デバイスの設定は、最大 10,000 件追加できます。

キーワード検索 (例: 営業 iPhone)

制御対象デバイスの追加

<input type="checkbox"/>	管理No.	デバイスグループ	デバイス管理名	ログオンユーザー名	制御設定	一時利用設定
<input type="checkbox"/>	82	サポート2課	MacBook_00000085	goro.mo	<input type="radio"/> 許可	
<input type="checkbox"/>	23	営業2課	Surface 3_0000000047	saburo.mo		- 期限切れ (2023/03/26 09:00)
<input type="checkbox"/>	26	営業2課	Surface 3_0000000050	ichiro.mo	<input type="radio"/> 許可	
<input type="checkbox"/>	25	営業2課	Surface 3_0000000049	jiro.mo	<input type="checkbox"/> △ 読み取り専用	

登録済み設定数: 4 / 10,000

20 1・4件 / 全4件 |< < 1 > >|

3. デバイスをチェックし、[制御設定] または [一時利用設定] をクリックします。

制御対象デバイスは、最大 100 件選択できます。

制御対象デバイスの追加

ネットワーク全体 Windows macOS

キーワード検索 (例: 営業 iPhone)

× 1 件を選択中

制御設定 一時利用設定

<input type="checkbox"/>	管理No.	デバイスグループ	デバイス管理名	使用者名	ログオンユーザー名
<input type="checkbox"/>	82	サポート2課	MacBook_00000085	MO五郎	goro.mo
<input checked="" type="checkbox"/>	81	サポート2課	MacBook_00000084	MO四郎	shiro.mo

20 1・2件 / 全2件 |< < 1 > >|

キャンセル

制御設定

接続されたすべての記録メディアを許可/読み取り専用/禁止に設定します。

一時利用設定

一時許可／一時読み取り専用にする期間を設定します。

4. 制御設定を選択し、[追加] をクリックします。



→ 「デバイス毎の設定/一時利用」画面に戻り、設定内容が表示されます。

6-4 配信設定をする

Windows

Windows デバイスへの配信に必要な設定をします。



- [ファイル配信設定をする](#)
Windows デバイスのファイル配信／実行に必要な設定をします。
- [アップデート管理の設定をする](#)
OS サポートの管理や月例パッチ／更新プログラムのインストールに必要な設定をします。

ファイル配信設定をする

Windows

Windows デバイスのファイル配信／実行に必要な設定をします。

ポイント

大量デバイスへの配信や大容量アプリを配信する場合、ネットワーク帯域に応じて一度に配信する台数を調整し、ネットワークやサーバーアクセスの負荷を分散する必要があります。[設定をコピーして作成] で配信設定をコピーして配信時刻を調整するなど、簡便に設定できます。

- [ファイル配信設定を追加する](#)

- [配信対象のデバイスを追加する](#)
- [配信結果を確認する](#)

ファイル配信設定を追加する

Windows

Windows デバイスのファイル配信/実行に必要な設定をします。

注意

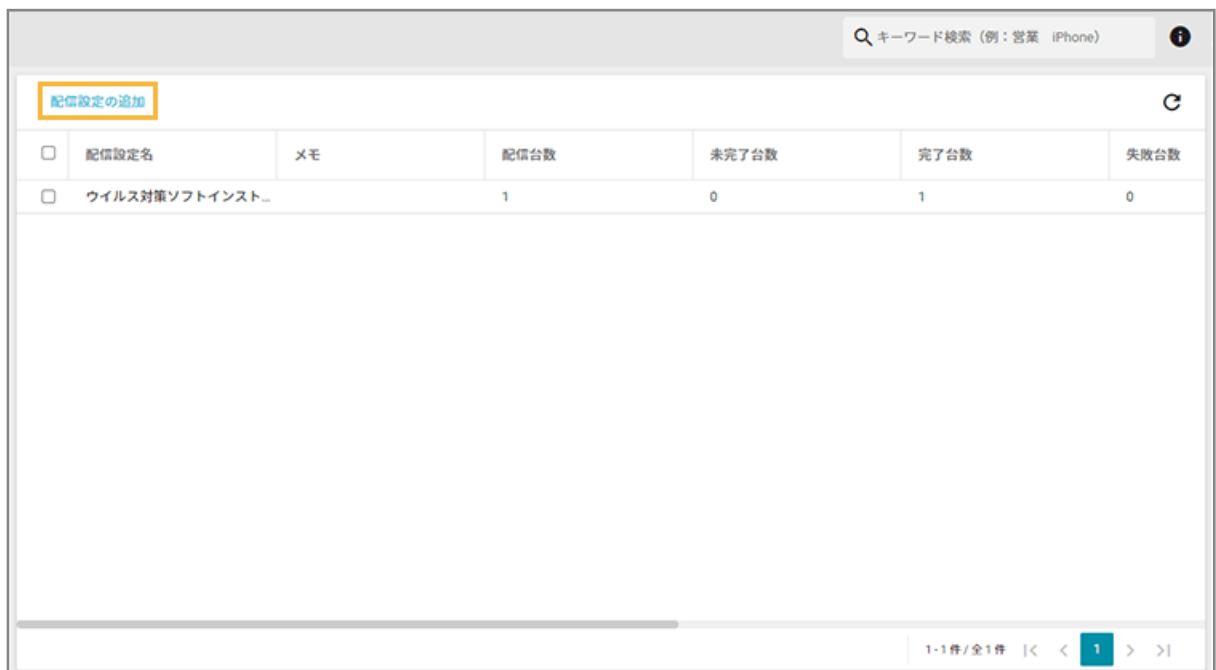
異なる配信設定で、同じファイル名のファイルを配信した場合は、上書き保存されます。

■ 社内ネットワーク上の共有フォルダーからの配信設定を追加する

1. [ルール] の [配信設定] > [ファイル配信設定 (Windows)] をクリックします。



2. [配信設定の追加] をクリックします。



3. 配信設定名を入力し、[配信ファイルの追加] をクリックします。

配信設定名

配信設定名 *

配信ファイル設定

配信ファイル (0) [配信ファイルの追加](#)

ファイルが追加されていません。
[配信ファイルの追加] から、配信するファイルを追加してください。

4. [社内ネットワーク上の共有フォルダー] をクリックします。

ダウンロード元を選択

追加するファイルのダウンロード元を選択してください。

社内ネットワーク上の共有フォルダー
デバイスがアクセスできるネットワーク上の共有フォルダーに配置したファイルを配信します。

オンラインストレージ
HTTPS でアクセスできるオンラインストレージに配置したファイルを配信します。

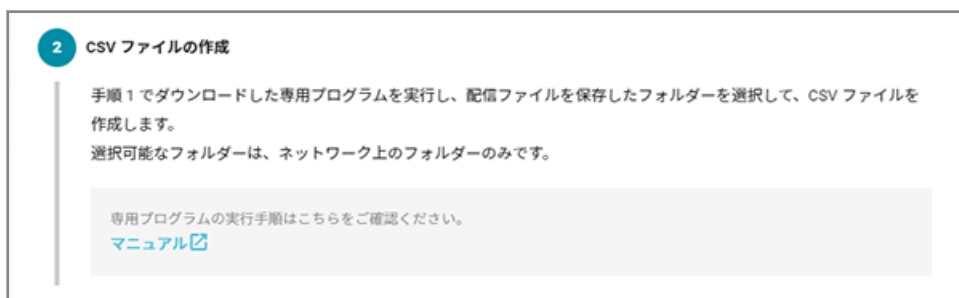
閉じる

5. 管理コンソールに記載の手順に従って、ファイルを追加します。

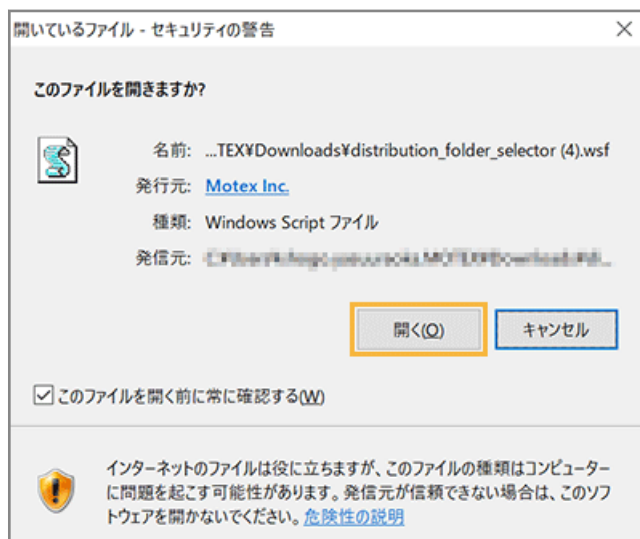
- (1) [専用プログラムをダウンロード] をクリックします。



(2) CSV ファイルを作成します。



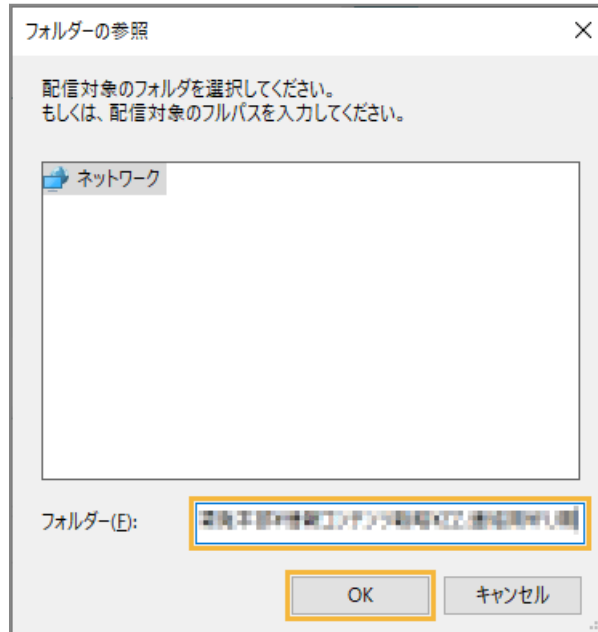
1. ダウンロードしたファイルを実行し、[開く] をクリックします。



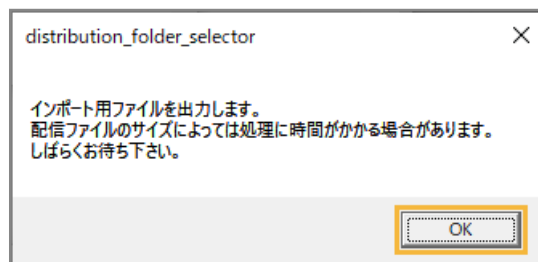
2. 配信ファイルを保存したフォルダーパスを選択、または入力し、[OK] をクリックします。

注意

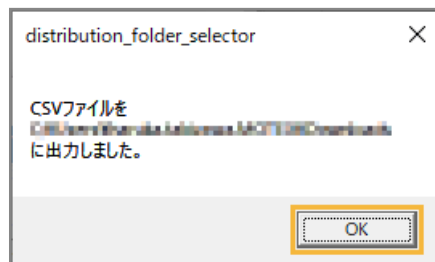
デバイスがアクセスできる社内ネットワーク上の共有フォルダーを指定してください。



3. [OK] をクリックします。



4. [OK] をクリックします。



→ 「distribution_folder_selector.wsf」と同じ階層に、「distribution_files.csv」が出力されます。


- (3) [ファイル選択] をクリックし、「distribution_files.csv」をアップロードして、[追加] をクリックします。



→ 配信ファイルが追加されます。

6. 配信ファイルを実行する場合は、[実行ファイルに設定] をチェックします。

ポイント

- 配信しないファイルは、 をクリックして削除できます。
- 実行ファイルは、必要に応じて、実行パラメーター／実行する順番を設定できます。



7. 配信設定をします。

配信設定

配信先

フォルダー*

LANSCOPE Client インストールフォル... ▼

設定したフォルダーがデバイスに無い場合、新たにフォルダーを作成し配信します。

ファイルサーバーへのアクセスアカウント

ユーザー名

ドメイン環境の場合は「ドメイン名#ユーザー名」の形で入力してください。

パスワード 🔒

配信タイミング

すぐに配信する

日時を指定して配信する

オプション

BITSサービスが無効の場合、有効に変更する

一台あたりの通信帯域を制限する

配信後のストレージ空き容量で制限する

通知

配信後にポップアップで通知する

配信先

デバイスのどのフォルダーに配信するかを設定できます。LANSCOPE Client がアクセスできるフォルダーを設定します。LANSCOPE Client インストールフォルダーの設定をおすすめします。

ファイルサーバーへのアクセスアカウント

ファイルサーバーにアクセスできるユーザー名/パスワードを入力します。ファイルサーバーにアクセスできない場合、ここで設定した権限でアクセスします。

配信タイミング

- すぐに配信する

配信対象のデバイスを追加したあと、すぐに配信されます。
- 日時を指定して配信する

指定した日時に配信されます。すでに指定日時を過ぎていた場合、すぐに配信されます。

オプション

- BITS サービスが無効の場合、有効に変更する

BITS サービスが無効の場合、配信できません。チェックすると、自動で BITS サービスが開始されます。
- 一台あたりの通信帯域を制限する

端末 1 台に対して、配信ファイルをダウンロードするときの最大通信帯域を制限できます（0 を指定すると、無制限になります）。

- 配信後のストレージ空き容量で制限する
 - 指定サイズを下回る場合は配信しない
クライアント HDD の空き容量が、配信後に指定したサイズを下回る場合、配信されません。
 - 一定の割合を下回る場合は配信しない
クライアント HDD の空き容量が、配信後に指定した割合を下回る場合、配信されません。

通知

- 配信後にポップアップで通知する
入力した内容を、配信後にデバイスにポップアップで通知できます。

8. 実行ファイルがある場合、実行設定をします。

実行設定

実行タイミング

すぐに実行する
 時刻を指定して実行する
 日時を指定して実行する

実行権限

localsystem
localsystem 権限で実行されます。ユーザー対話画面が不要な場合に選択します。
クライアント PC がログオフの状態でも実行されます。

ログオンユーザー
配信時にログオンしているユーザーの権限で実行されます。
クライアント PC がログオフの状態では実行されません。

管理者ユーザー
指定したユーザーの権限で実行されます。
基本的には Administrator ユーザーを指定しますが、任意ユーザーの指定も可能です。
クライアント PC がログオフの状態でも実行されます。

オプション

ログオン後の一定時間は実行しない
 クライアント側から実行を選択できるようにする
 すべてのファイル実行後に再起動/シャットダウンする
 再起動後に配信したファイル/フォルダーを削除する

通知

実行前にポップアップで通知する
 実行後にポップアップで通知する

実行タイミング

- すぐに実行する
配信完了後、すぐに実行されます。
- 時刻を指定して実行する

配信完了後、指定した時刻に実行されます。すでに指定時刻を過ぎていた場合、すぐに実行されます。

- 日時を指定して実行する

配信完了後、指定した日時に実行されます。すでに指定日時を過ぎていた場合、すぐに実行されます。

実行権限

- localsystem

localsystem 権限で実行されます。ユーザー対話画面が不要な場合に選択します。クライアント PC がログオフの状態でも実行されます。

- ログオンユーザー

配信時にログオンしているユーザー権限で実行されます。クライアント PC がログオフの状態では実行できません。

- 管理者ユーザー

指定したユーザー権限で実行されます。基本的には Administrator ユーザーを指定しますが、任意ユーザーの指定もできます。クライアント PC がログオフの状態でも実行されます。

オプション

- ログオン後の一定時間は実行しない

ログオン後にクライアント処理の多いタイミングは避けて実行できます。

- クライアント側から実行を選択できるようにする

クライアントに実行確認のメッセージが表示されます。タスクバーの通知領域にアイコンが表示され、クライアント側のタイミングでファイルの実行を選択できます。

- すべてのファイル実行後に再起動/シャットダウンする

再起動が必要なインストーラーの場合、PC を再起動/シャットダウンができます。

- 再起動後に配信したファイル/フォルダーを削除する

配信したファイル/フォルダーが不要の場合、再起動後に削除できます。

通知

- 実行前にポップアップで通知する

入力した内容を、実行前にデバイスにポップアップで通知できます。

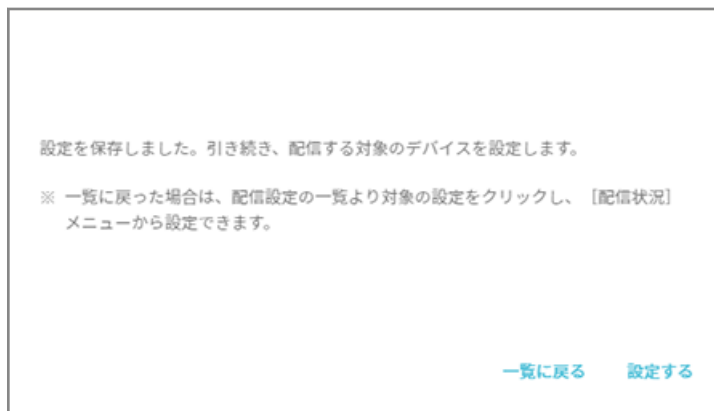
- 実行後にポップアップで通知する

入力した内容を、実行後にデバイスにポップアップで通知できます。

9. [保存] をクリックします。



→ ファイル配信設定が完了します。



■ オンラインストレージからの配信設定を追加する

ステップ：

1. [配信ファイルを準備する](#)
2. [オンラインストレージからの配信設定を追加する](#)

ステップ 1： 配信ファイルを準備する

1. 配信するファイルを、デバイスがアクセスできるオンラインストレージに配置します。

HTTPS でアクセスできるオンラインストレージに配置します。

配置したオンラインストレージの URL を管理コンソールで設定し、デバイス側でインストールできるようにします。

注意

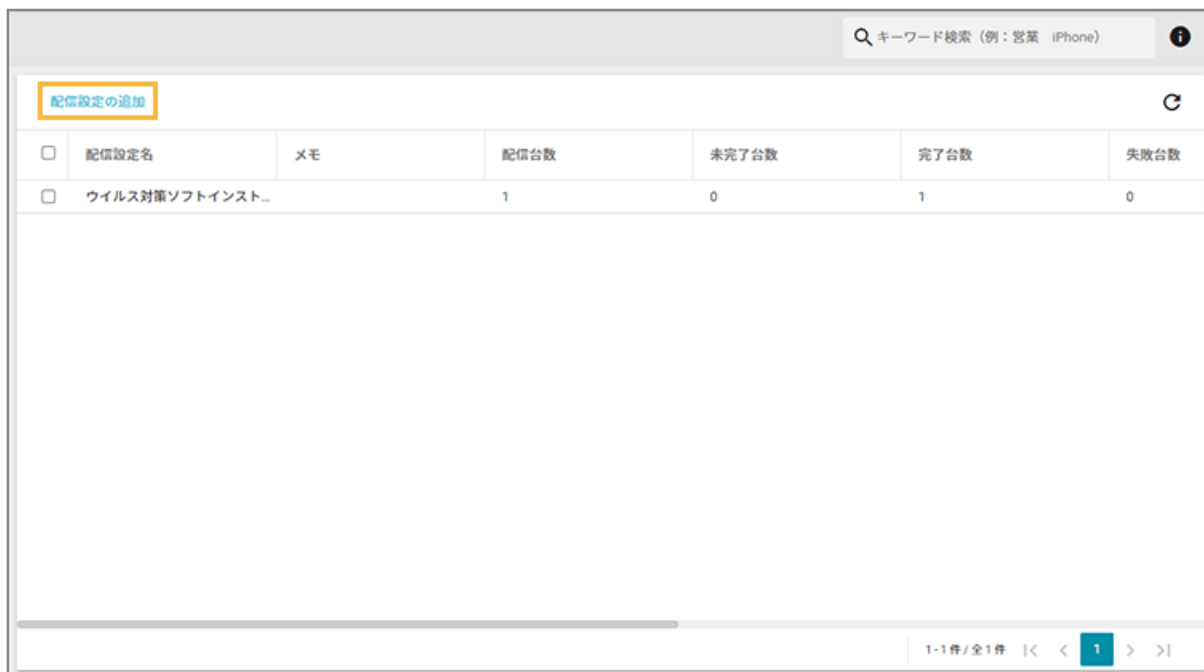
パブリックアクセス可能なオンラインストレージに配置する必要があります。情報漏えいのリスクがあるため、機密ファイルを配置しないように注意してください。

ステップ 2： オンラインストレージからの配信設定を追加する

1. [ルール] の [配信設定] > [ファイル配信設定 (Windows)] をクリックします。



2. [配信設定の追加] をクリックします。



3. 配信設定名を入力し、[配信ファイルの追加] をクリックします。

The screenshot shows a configuration interface with two main sections. The top section, titled '配信設定名' (Distribution Setting Name), contains a text input field with a red asterisk indicating a required field. The bottom section, titled '配信ファイル設定' (Distribution File Setting), shows '配信ファイル (0)' (Distribution Files (0)) and a button labeled '配信ファイルの追加' (Add Distribution File). Below the button, a message states: 'ファイルが追加されていません。 [配信ファイルの追加] から、配信するファイルを追加してください。' (No files have been added. Please add files to be distributed from [Add Distribution File]).

4. [オンラインストレージ] をクリックします。

The screenshot shows a dialog box titled 'ダウンロード元を選択' (Select Download Source). It contains the instruction: '追加するファイルのダウンロード元を選択してください。' (Please select the download source for the files to be added). There are two radio button options: '社内ネットワーク上の共有フォルダー' (Shared folder on the corporate network) and 'オンラインストレージ' (Online storage). The 'オンラインストレージ' option is selected and highlighted with an orange border. Below the options, there is a '閉じる' (Close) button at the bottom right.

5. 配信ファイルを配置したオンラインストレージの URL を入力します。

- 配信ファイルは、最大 10 件追加できます。
- 1 つの URL につき、1 つのファイルを配信できます。
- フォルダー、リダイレクトされる URL、クッションページがある URL は配信できません。



ポイント

配信ファイルが 11 件以上の場合、1 つの zip ファイルにまとめて配信できます。同じ配信設定に、zip ファイル解凍用の bat ファイルを追加し、配信してください。

配信方法は、次のとおりです。

1. 配信ファイルを 1 つの zip ファイルにまとめ、ファイル名を「delivery.zip」に変更します。
2. 拡張子が「.bat」の、zip ファイル解凍用の bat ファイルを作成します。
3. zip ファイル解凍用の bat ファイルに、次の内容をコピーアンドペーストして保存します。


zip ファイルの中に実行したいファイルがある場合、「実行したいファイル名」を編集します。

```
@echo off
cd C:\Program Files (x86)\MOTEX\LanScope Client\Distribution
powershell -windowstyle hidden Expand-Archive -Path "delivery.zip"
if exist ".\delivery\実行したいファイル名" (
start "" ".\delivery\実行したいファイル名"
)
```

4. zip ファイル/bat ファイルをオンラインストレージに配置します。
5. オンラインストレージの URL を、配信設定に追加します。
6. bat ファイルを実行ファイルに設定して、配信します。


6. **【ハッシュ値を計算する】をクリックし、オンラインストレージに配置した配信ファイルと同じファイルを選択します。**

ポイント


- 配信しないファイルは、 をクリックして削除できます。
- 実行ファイルは、必要に応じて、実行パラメーター／実行する順番を設定できます。

配信ファイル設定

配信ファイル (1) 配信ファイルの追加

<small>"/ Lanscope/lanclient/lanclient.exe" 部署別インストールフォルダコンテナ配属した 運用機/OS/lanclient.exe LANSCOPE Client</small>	193 Bytes	<input checked="" type="checkbox"/> 実行ファイルに設定	
--	-----------	---	---

配信後に実行するファイル (1) 実行する順番の並び替え

1	<small>"/ Lanscope/lanclient/lanclient.exe" 部署別インストールフォルダコンテナ配属した 運用機/OS/lanclient.exe</small> 実行パラメーター <Distribution File Name> 
---	---

9. 配信設定をします。

配信設定

配信先

フォルダー*

LANSCOPE Client インストールフォル... ▼

設定したフォルダーがデバイスに無い場合、新たにフォルダーを作成し配信します。

配信タイミング

すぐに配信する

日時を指定して配信する

オプション

BITSサービスが無効の場合、有効に変更する

一台あたりの通信帯域を制限する

配信後のストレージ空き容量で制限する

通知

配信後にポップアップで通知する

配信先

デバイスのどのフォルダーに配信するかを設定できます。LANSCOPE Client がアクセスできるフォルダーを設定します。LANSCOPE Client インストールフォルダーの設定をおすすめします。

配信タイミング

- すぐに配信する
 - 配信対象のデバイスを追加したあと、すぐに配信されます。

- 日時を指定して配信する

指定した日時に配信されます。すでに指定日時を過ぎていた場合、すぐに配信されます。

オプション

- BITS サービスが無効の場合、有効に変更する

BITS サービスが無効の場合、配信できません。チェックすると、自動で BITS サービスが開始されます。

- 一台あたりの通信帯域を制限する

端末 1 台に対して、配信ファイルをダウンロードするときの最大通信帯域を制限できます (0 を指定すると、無制限になります)。

- 配信後のストレージ空き容量で制限する

- 指定サイズを下回る場合は配信しない

クライアント HDD の空き容量が、配信後に指定したサイズを下回る場合、配信されません。

- 一定の割合を下回る場合は配信しない

クライアント HDD の空き容量が、配信後に指定した割合を下回る場合、配信されません。

通知

- 配信後にポップアップで通知する

入力した内容を、配信後にデバイスにポップアップで通知できます。

10. 実行ファイルがある場合、実行設定をします。

実行設定

実行タイミング

すぐに実行する
 時刻を指定して実行する
 日時を指定して実行する

実行権限

localsystem
localsystem 権限で実行されます。ユーザー対話画面が不要な場合に選択します。
クライアント PC がログオフの状態でも実行されます。

ログオンユーザー
配信時にログオンしているユーザーの権限で実行されます。
クライアント PC がログオフの状態では実行されません。

管理者ユーザー
指定したユーザーの権限で実行されます。
基本的には Administrator ユーザーを指定しますが、任意ユーザーの指定も可能です。
クライアント PC がログオフの状態でも実行されます。

オプション

ログオン後の一定時間は実行しない
 クライアント側から実行を選択できるようにする
 すべてのファイル実行後に再起動/シャットダウンする
 再起動後に配信したファイル/フォルダーを削除する

通知

実行前にポップアップで通知する
 実行後にポップアップで通知する

実行タイミング

- すぐに実行する
配信完了後、すぐに実行されます。
- 時刻を指定して実行する
配信完了後、指定した時刻に実行されます。すでに指定時刻を過ぎていた場合、すぐに実行されます。
- 日時を指定して実行する
配信完了後、指定した日時に実行されます。すでに指定日時を過ぎていた場合、すぐに実行されます。

実行権限

- localsystem
localsystem 権限で実行されます。ユーザー対話画面が不要な場合に選択します。クライアント PC がログオフの状態でも実行されます。
- ログオンユーザー
配信時にログオンしているユーザー権限で実行されます。クライアント PC がログオフの状態では実行できません。
- 管理者ユーザー
指定したユーザー権限で実行されます。基本的には Administrator ユーザーを指定しますが、任意ユーザーの指定もできます。クライアント PC がログオフの状態でも実行されます。

オプション

- ログオン後の一定時間は実行しない
ログオン後にクライアント処理の多いタイミングは避けて実行できます。
- クライアント側から実行を選択できるようにする
クライアントに実行確認のメッセージが表示されます。タスクバーの通知領域にアイコンが表示され、クライアント側のタイミングでファイルの実行を選択できます。
- すべてのファイル実行後に再起動/シャットダウンする
再起動が必要なインストーラーの場合、PC を再起動/シャットダウンができます。
- 再起動後に配信したファイル/フォルダーを削除する
配信したファイル/フォルダーが不要の場合、再起動後に削除できます。

通知

- 実行前にポップアップで通知する
入力した内容を、実行前にデバイスにポップアップで通知できます。
- 実行後にポップアップで通知する
入力した内容を、実行後にデバイスにポップアップで通知できます。

11. [保存] をクリックします。

← 配信/実行設定の追加

保存

配信設定名

配信設定名 *

配信設定

配信ファイル設定

配信ファイル (1) 配信ファイルの追加

193 Bytes 実行ファイルに設定

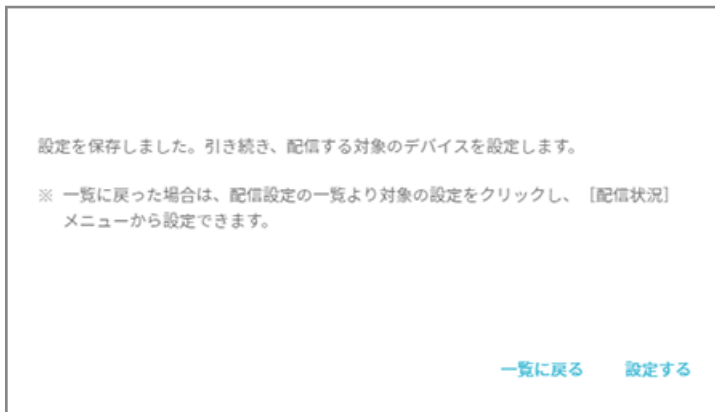
配信後に実行するファイル (1) 実行する順番の並び替え

1 実行パラメーター <Distribution File Name>

配信設定

配信先

→ ファイル配信設定が完了します。



配信対象のデバイスを追加する

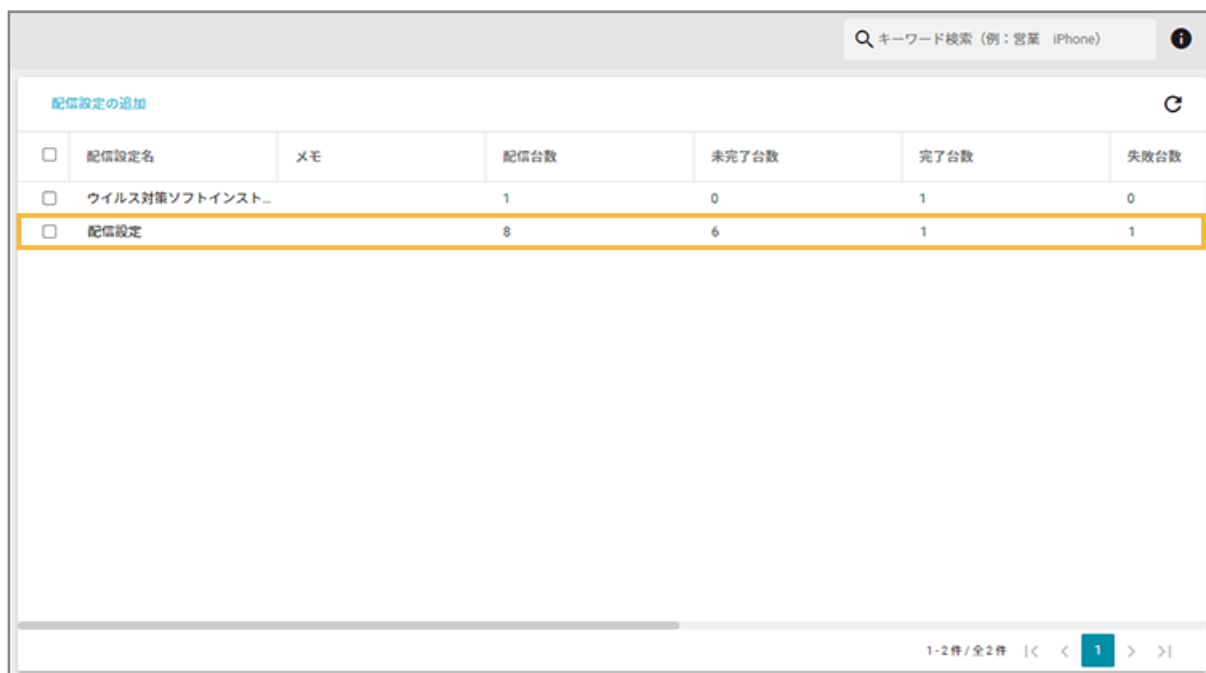
Windows

配信設定に、配信対象のデバイスを追加します。

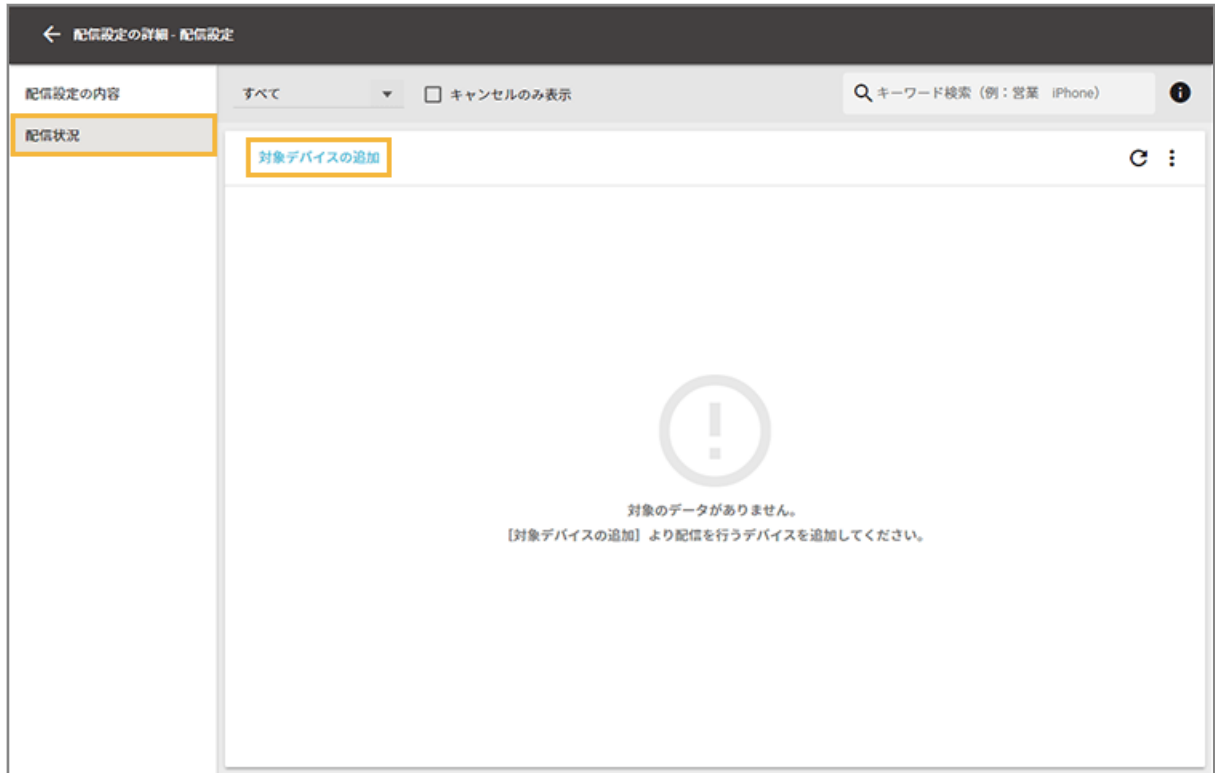
1. 【ルール】の【配信設定】>【ファイル配信設定 (Windows)】をクリックします。



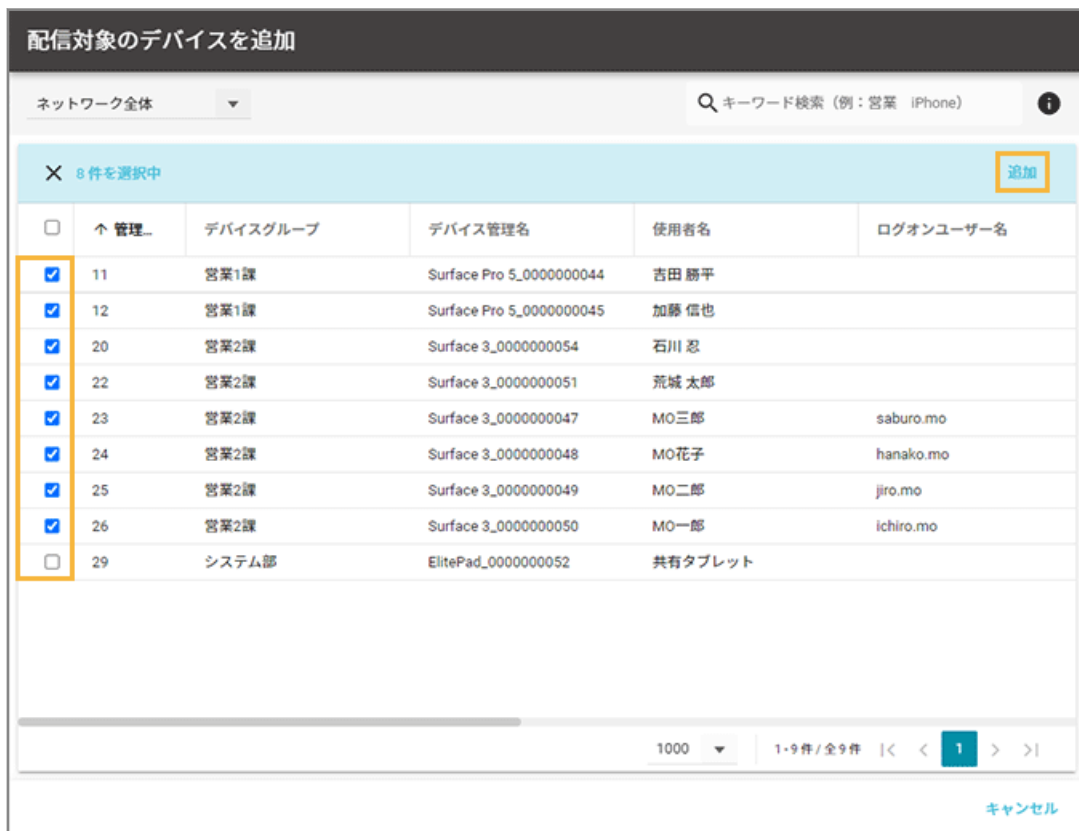
2. 配信設定をクリックします。



3. 【配信状況】をクリックし、【対象デバイスの追加】をクリックします。



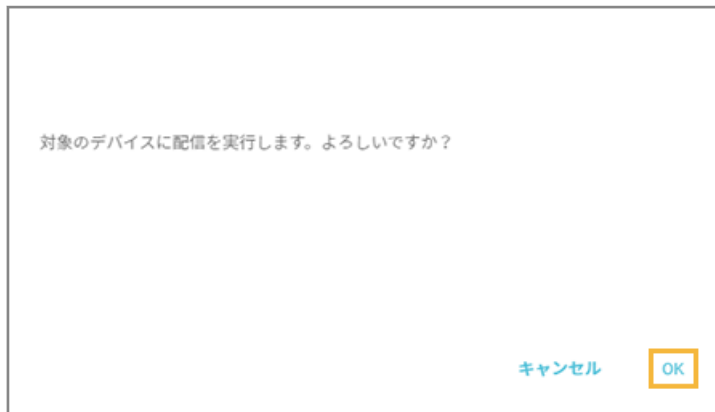
4. 配信対象のデバイスをチェックし、[追加] をクリックします。



→ 配信対象のデバイスが追加されます。

5. [OK] をクリックします。

実行設定で [すぐに実行] を選択している場合に表示されます。



配信結果を確認する

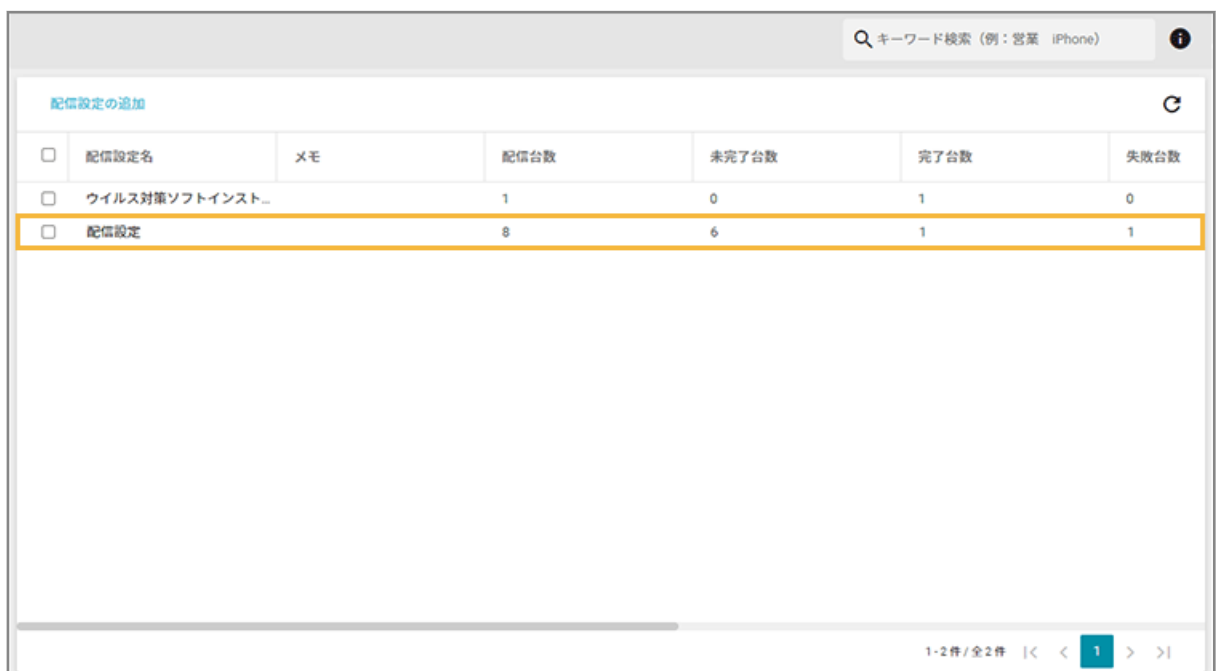
Windows

ファイル配信／実行の結果を確認し、必要に応じて再配信します。

1. [ルール] の [配信設定] > [ファイル配信設定 (Windows)] をクリックします。



2. 配信設定をクリックします。




3. 【配信状況】をクリックし、状態を確認します。

<input type="checkbox"/>	管理No.	デバイスグループ	デバイス管理名	状態	キャンセル	使用者名
<input type="checkbox"/>	11	営業1課	Surface Pro 5_0000000044	実行完了		吉田 勝平
<input type="checkbox"/>	12	営業1課	Surface Pro 5_0000000045	設定通知前	キャンセル	加藤 信也
<input type="checkbox"/>	20	営業2課	Surface 3_0000000054	設定通知前	キャンセル	石川 忍
<input type="checkbox"/>	22	営業2課	Surface 3_0000000051	設定通知前	キャンセル	荒城 太郎
<input type="checkbox"/>	23	営業2課	Surface 3_0000000047	設定通知前	キャンセル	MO 三郎
<input type="checkbox"/>	24	営業2課	Surface 3_0000000048	設定通知前	キャンセル	MO 花子
<input type="checkbox"/>	25	営業2課	Surface 3_0000000049	設定通知前	キャンセル	MO 二郎
<input type="checkbox"/>	26	営業2課	Surface 3_0000000050	配信失敗		MO 一郎

状態

- 設定通知前
配信設定がデバイスに適用されていないときに表示されます。
- 設定通知完了
配信設定がデバイスに適用されたときに表示されます。
- 配信中
配信設定の適用後、配信ファイルを配信中のときに表示されます。
- 配信失敗 (*)
配信設定の適用後、配信ファイルの配信に失敗したときに表示されます。
- 配信完了
配信設定の適用後、配信ファイルが配信されたときに表示されます。
- 実行中
配信設定の適用後、配信ファイルを実行中のときに表示されます。
- 実行失敗 (*)
配信設定の適用後、配信ファイルの実行に失敗したときに表示されます。
- 実行完了
配信ファイルが実行されたときに表示されます。

* :  が表示され、エラー内容を確認できます。


- BITS のダウンロードジョブを作成できませんでした。

システム権限だけがアクセスできるフォルダーに配信したとき、または配信先に同じファイル名のファイルが存在するときに表示されます。配信先をログオンユーザーがアクセスできるフォルダーに変更するか、配信先のフォルダーから同じファイル名のファイルを削除して、再度配信設定を実行する必要があります。

- 要求された操作には管理者権限が必要です。

ファイルの実行権限がないときに表示されます。実行権限を localsystem 権限、またはビルトイン Administrator 権限にして再度配信設定を実行する必要があります。

4. 再配信する場合、デバイスをチェックし、[再配信する] をクリックします。

<input type="checkbox"/>	管理No.	デバイスグループ	デバイス管理名	状態	キャンセル	使用者名
<input type="checkbox"/>	11	営業1課	Surface Pro 5_0000000044	実行完了		吉田 勝平
<input checked="" type="checkbox"/>	12	営業1課	Surface Pro 5_0000000045	設定通知前	キャンセル	加藤 信也
<input checked="" type="checkbox"/>	20	営業2課	Surface 3_0000000054	設定通知前	キャンセル	石川 忍
<input checked="" type="checkbox"/>	22	営業2課	Surface 3_0000000051	設定通知前	キャンセル	荒城 太郎
<input checked="" type="checkbox"/>	23	営業2課	Surface 3_0000000047	設定通知前	キャンセル	MO三部
<input checked="" type="checkbox"/>	24	営業2課	Surface 3_0000000048	設定通知前	キャンセル	MO花子
<input checked="" type="checkbox"/>	25	営業2課	Surface 3_0000000049	設定通知前	キャンセル	MO二郎
<input checked="" type="checkbox"/>	26	営業2課	Surface 3_0000000050	配信失敗 		MO一郎

5. [OK] をクリックします。

再配信を行います。よろしいですか?

キャンセル

→ 再配信が実行されます。

アップデート管理の設定をする

Windows

OS サポートの管理や月例パッチ／更新プログラムのインストールに必要な設定をします。デバイスグループごとにアップデート状況を確認できます。サポートが終了する OS や未適用の月例パッチがある場合は、インストール設定ができません。

- [プロキシ設定を適用する](#)

プロキシサーバーを経由する環境でインストール設定を実行する場合、事前にプロキシの設定が必要です。

- [アップデート管理の設定をする](#)

アップデート状況を確認し、OS サポートの管理や月例パッチ／更新プログラムのインストールに必要な設定をします。

プロキシ設定を適用する

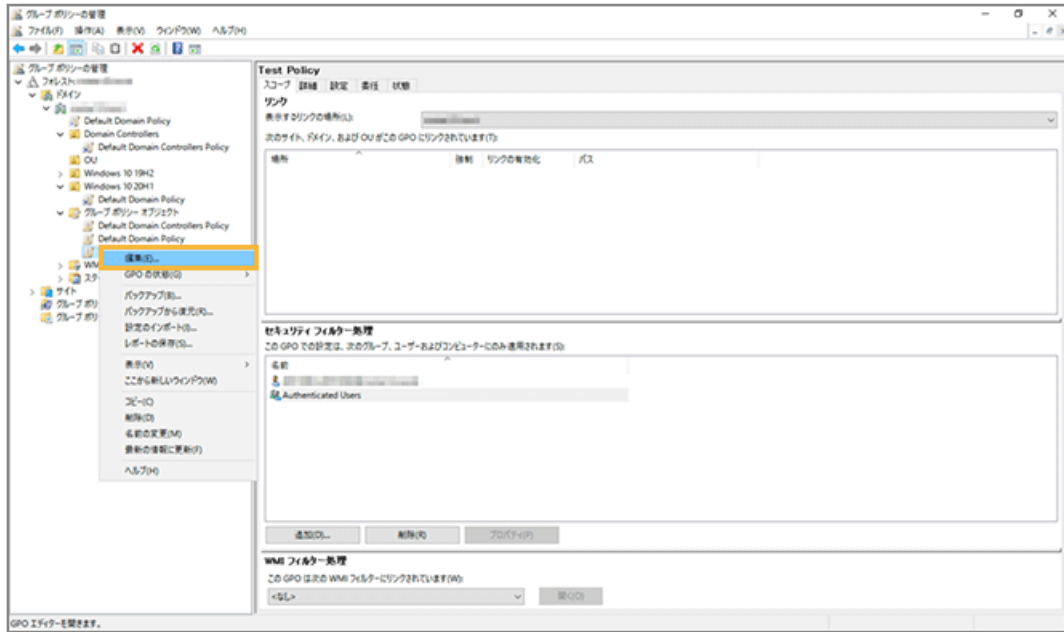
Windows

プロキシサーバーを経由する環境でインストール設定を実行する場合、事前にプロキシの設定が必要です。

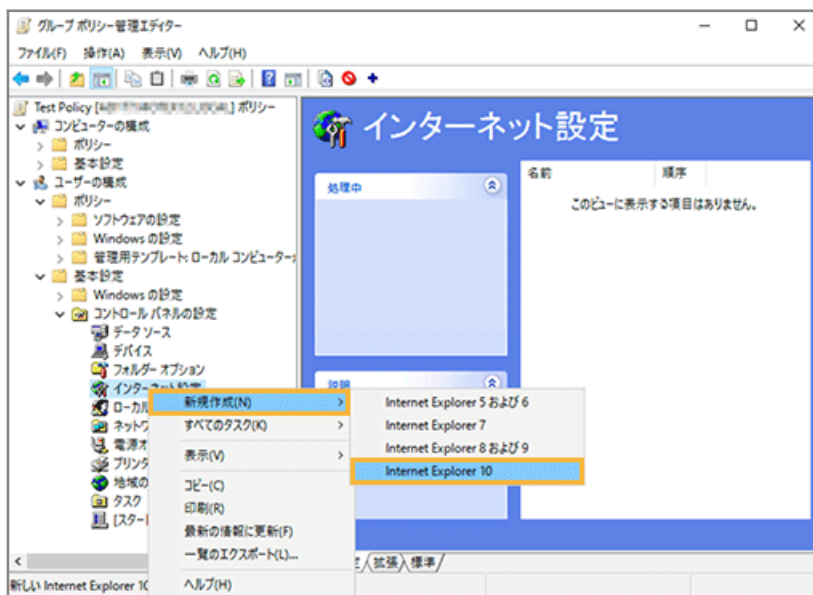
■ Windows 11／10 のデバイスにプロキシ設定を適用する

グループポリシーを利用して、Internet Explorer 10 のプロキシ設定をデバイスに適用します。

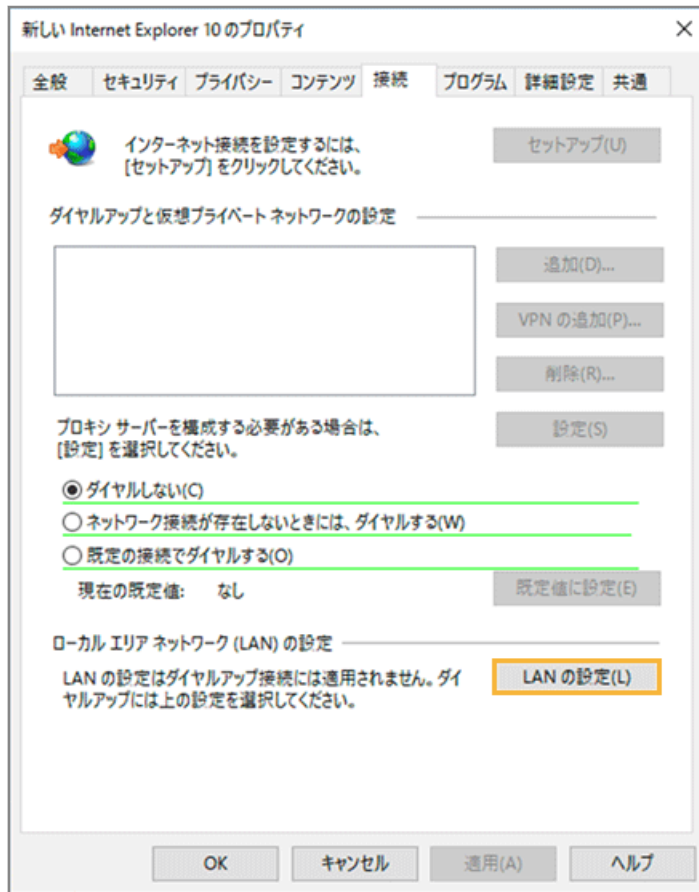
1. **ドメインコントローラーにドメイン管理者ユーザーでログオンします。**
2. **[スタート] > [すべてのプログラム] > [管理ツール] > [グループポリシーの管理] をクリックします。**
3. **[フォレスト] > [ドメイン] > [ドメイン名] > [グループポリシーオブジェクト] で、グループポリシーオブジェクトを作成します。**
4. **作成したグループポリシーオブジェクトを右クリックし、[編集] をクリックします。**



5. [ユーザーの構成] > [基本設定] > [コントロールパネルの設定] > [インターネット設定] を右クリックし、[新規作成] > [Internet Explorer 10] をクリックします。



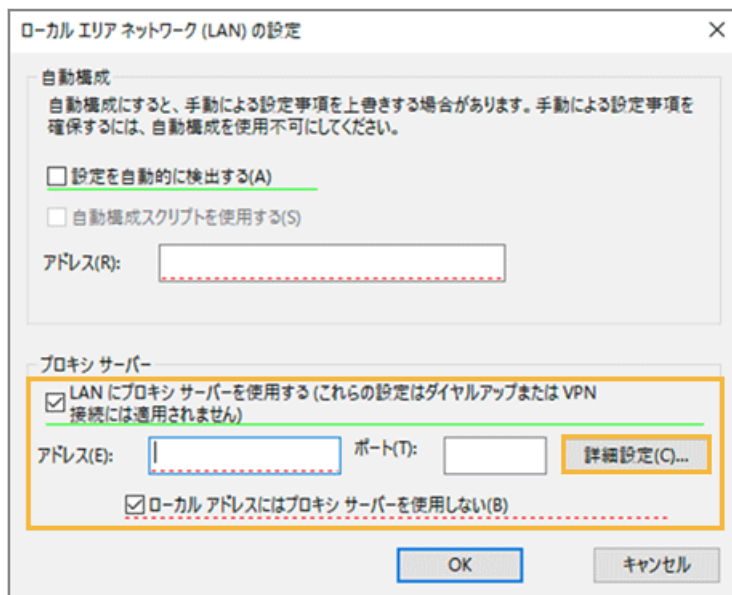
6. [接続] タブの [LAN の設定] をクリックします。



7. 次のように設定し、[詳細設定] をクリックします。

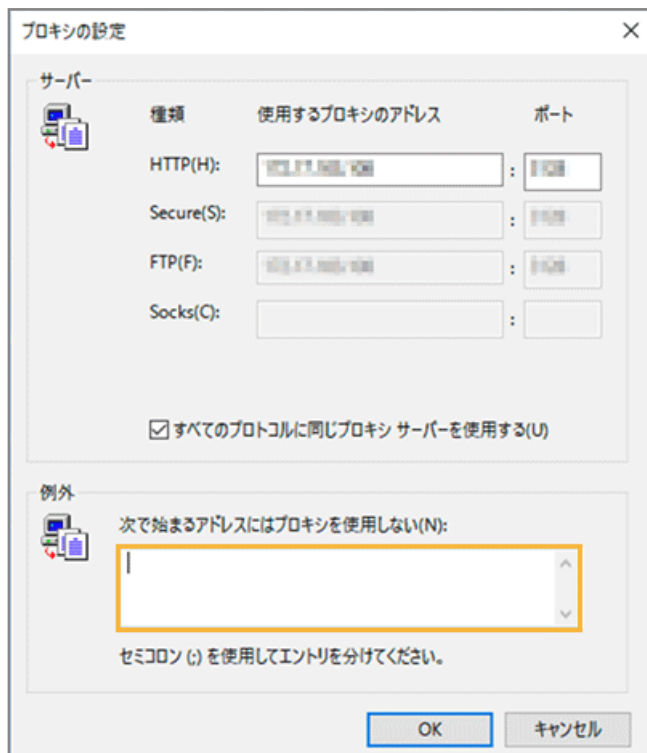
設定項目に表示される緑の実線は「配布」、赤の破線は「配布しない」を表しています。

項目	値
LAN にプロキシサーバーを使用する	チェック
アドレス	プロキシサーバーの IP アドレス
ポート	プロキシサーバーのポート
ローカルアドレスにはプロキシサーバーを使用しない	チェック



8. 「例外」に次の内容を入力して、[OK] をクリックします。

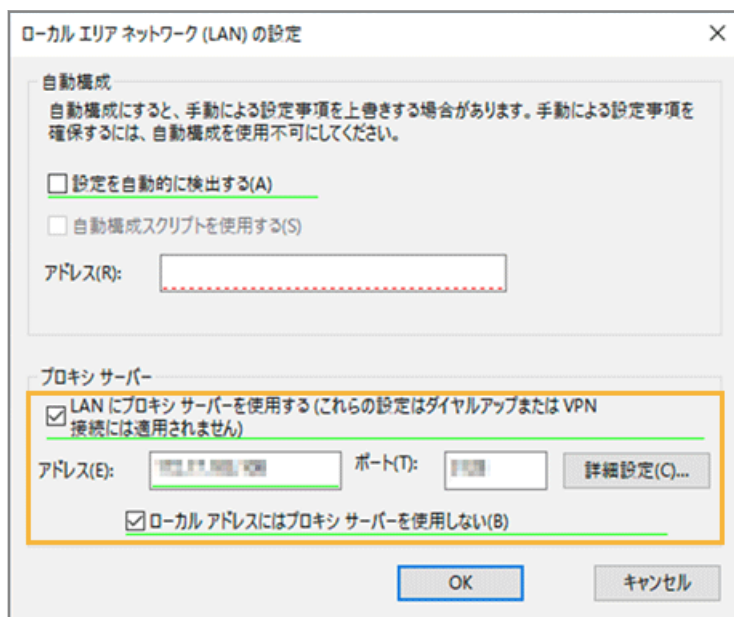
```
update.microsoft.com;*.update.microsoft.com;download.windowsupdate.com;*.download.window
supdate.com;download.microsoft.com;*.download.microsoft.com;windowsupdate.com;*.window
supdate.com;ntservicepack.microsoft.com;login.live.com;mp.microsoft.com;*.mp.microsoft.co
m;*.do.dsp.mp.microsoft.com;*.dl.delivery.mp.microsoft.com;*.emdl.ws.microsoft.com
```



9. [F6] キーを押して、手順 7 で設定した項目を配布対象にします。

注意

- プロキシ設定を完了するためには、プロキシサーバーの赤い破線がある項目を緑の実線にして、デバイスに配布する必要があります。
- 緑の実線が表示されている項目の設定が配布され、デバイスに適用されます。必要な項目だけを緑の実線にしてください。



→ 設定した項目に、緑の実線が表示されます。

10. [OK] をクリックします。

11. 作成したグループポリシーオブジェクトをデバイスに適用します。

→ プロキシ設定の適用が完了します。

■ Windows 10 未満のデバイスにプロキシ設定を適用する

グループポリシーを利用して、WinHTTP のプロキシ設定をデバイスに適用します。

1. ドメインコントローラーにドメイン管理者ユーザーでログオンします。

2. コマンドプロンプトを管理者として起動します。

[スタート] > [すべてのプログラム] > [アクセサリ] (または [Windows システムツール]) > [コマンドプロンプト] を右クリックし、[管理者として実行] をクリックして起動します。

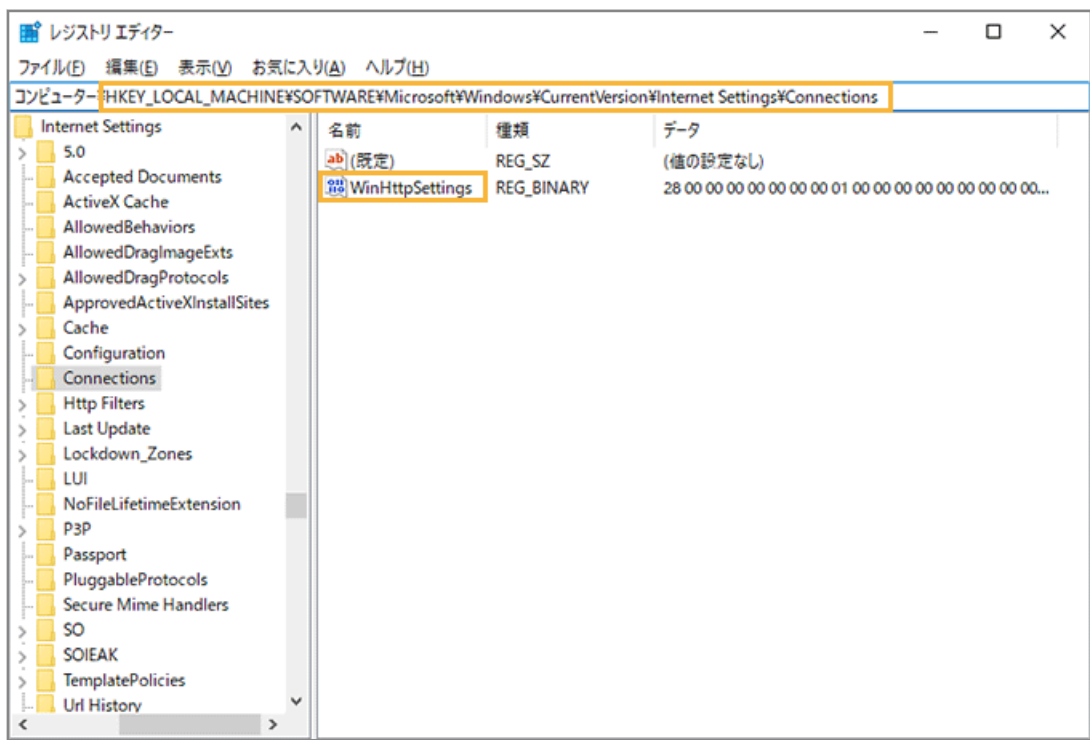
「ユーザーアカウント制御」画面が表示された場合は許可します。

3. 次のコマンドを実行します。

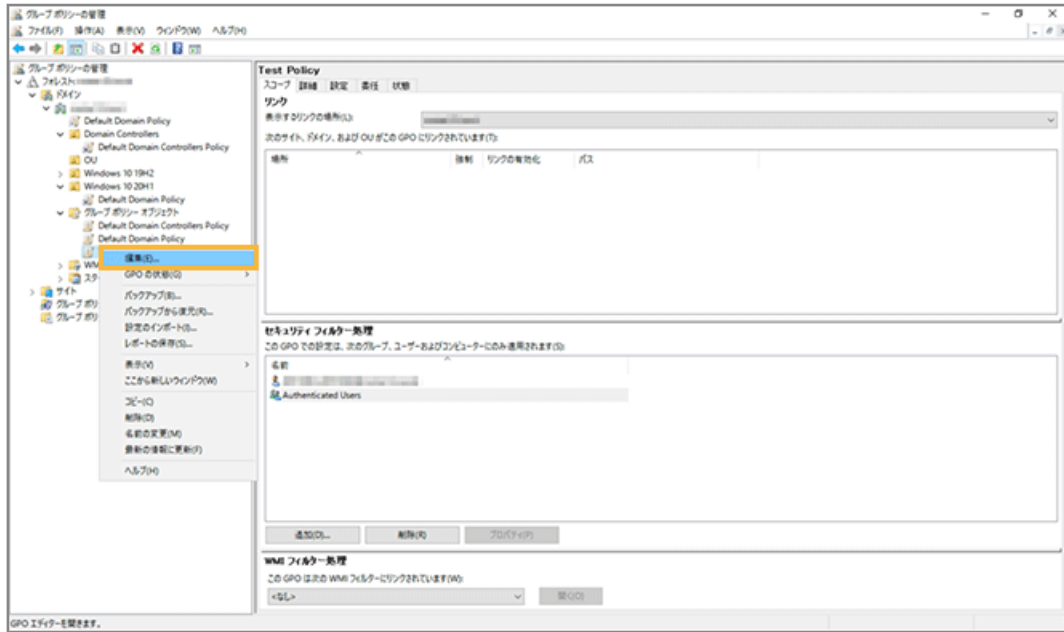
```
netsh winhttp set proxy プロキシサーバーのIPアドレス "update.microsoft.com;*.update.microsof
t.com;download.windowsupdate.com;*.*.download.windowsupdate.com;download.microsoft.com;*.*.d
ownload.microsoft.com;windowsupdate.com;*.*.windowsupdate.com;ntservicepack.microsoft.com;
login.live.com;mp.microsoft.com;*.*.mp.microsoft.com"
```

4. レジストリエディターを起動して、次の内容をコピーします。

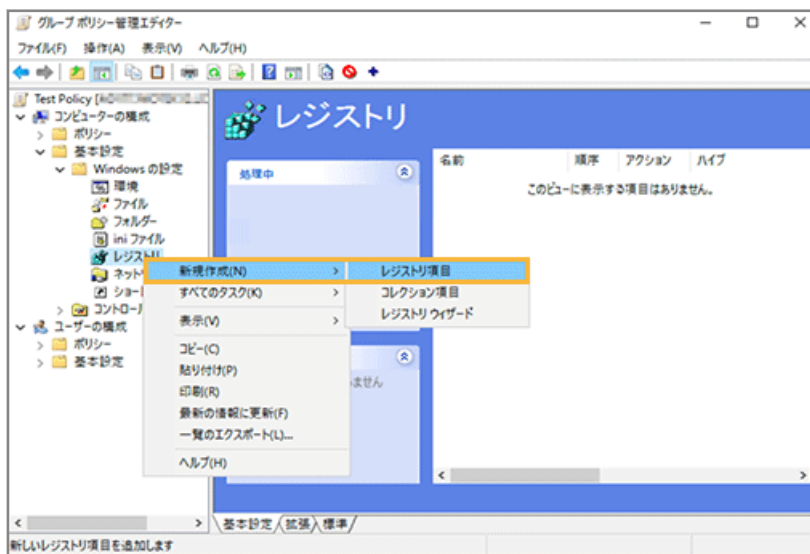
項目	値
レジストリパス	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
名前	WinHttpSettings



5. [スタート] > [すべてのプログラム] > [管理ツール] > [グループポリシーの管理] をクリックします。
6. [フォレスト] > [ドメイン] > [ドメイン名] > [グループポリシーオブジェクト] で、グループポリシーオブジェクトを作成します。
7. 作成したグループポリシーオブジェクトを右クリックし、[編集] をクリックします。



8. [コンピューターの構成] > [基本設定] > [Windows の設定] > [レジストリ] を右クリックし、[新規作成] > [レジストリ項目] をクリックします。



9. [全般] タブで次のように設定し、[OK] をクリックします。

項目	値
アクション	更新
キーのパス	手順 4 でコピーしたレジストリパス
値の名前	手順 4 でコピーした名前

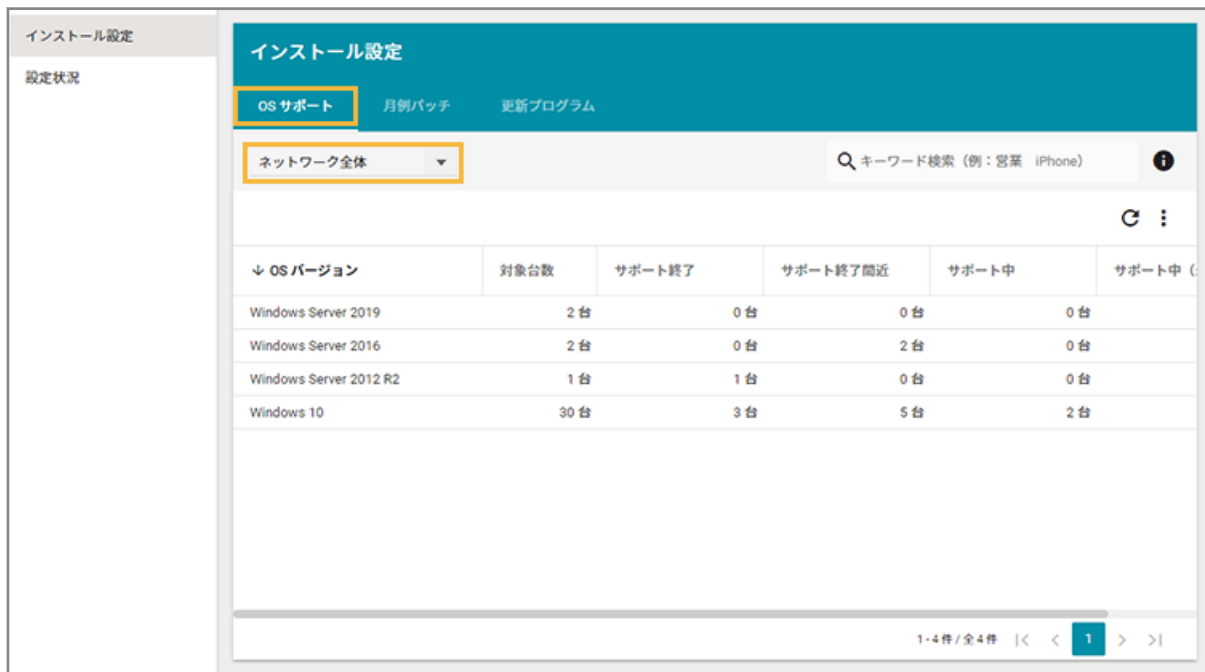
注意

- Microsoft 社が最新の OS を公開してから MOTEX が動作確認や対応バージョンをリリースするまでの間は、次の制限事項があります。
 - エンドポイントマネージャーで最新の OS を配信できません。
 - エンドポイントマネージャー以外の機能で OS を配信した場合、デバイスの Windows バージョン情報が更新されません。MOTEX の動作確認完了後に、正しい Windows バージョン情報を確認できるようになります。
- インストール設定をする場合、Active Directory のグループポリシー「インターネット上の Windows Update に接続しない」を「無効」に設定してください。「有効」に設定していると、Microsoft アップデートサーバーにアクセスできず、インストールできません。

1. [ルール] の [配信設定] > [OS アップデート (Windows)] をクリックします。



2. [OS サポート] をクリックし、デバイスグループを選択します。



3. サポート状況を確認する OS バージョンをクリックします。

インストール設定

OS サポート 月例パッチ 更新プログラム

ネットワーク全体

キーワード検索 (例: 営業 iPhone)

OS バージョン	対象台数	サポート終了	サポート終了間近	サポート中	サポート中 ()
Windows Server 2019	2 台	0 台	0 台	0 台	
Windows Server 2016	2 台	0 台	2 台	0 台	
Windows Server 2012 R2	1 台	1 台	0 台	0 台	
Windows 10	30 台	3 台	5 台	2 台	

1-4 件 / 全 4 件 |< < 1 > >|

4. OS のサポート状況を確認します。

OS サポートの詳細

ネットワーク全体 Windows 10

サポート中のデバイスも表示する

キーワード検索 (例: 営業 iPhone)

状態	サポート終了日	管理No.	デバイスグループ	デバイス管理名	OSバージョン	Window
サポート終了	2020/11/10	11	営業1課	Surface Pro 5_0000000044	Windows 10 Pro 10.0.17134	1803
サポート終了	2020/11/10	12	営業1課	Surface Pro 5_0000000045	Windows 10 Pro 10.0.17134	1803
サポート終了	2020/11/10	20	営業2課	Surface 3_0000000054	Windows 10 Home 10.0.10240	20H1
サポート終了間近	2021/12/11	22	営業2課	Surface 3_0000000051	Windows 10 Home 10.0.10240	1507
サポート終了間近	2021/12/11	23	営業2課	Surface 3_0000000047	Windows 10 Pro 10.0.19041	2004
サポート終了間近	2021/12/11	24	営業2課	Surface 3_0000000048	Windows 10 Pro 10.0.19041	2004
サポート終了間近	2021/12/11	25	営業2課	Surface 3_0000000049	Windows 10 Pro 10.0.19041	2004
サポート終了間近	2021/12/11	26	営業2課	Surface 3_0000000050	Windows 10 Pro 10.0.19041	2004
サポート中	2022/07/11	29	システム部	ElitePad_0000000052	Windows 10 Home 10.0.10240	20H1
サポート中	2022/07/11	55	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	1511
サポート中 (最新)	2022/11/18	56	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	20H1
サポート中 (最新)	2022/11/18	57	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	20H1
サポート中 (最新)	2022/11/18	58	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	20H1
サポート中 (最新)	2022/11/18	59	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	20H1

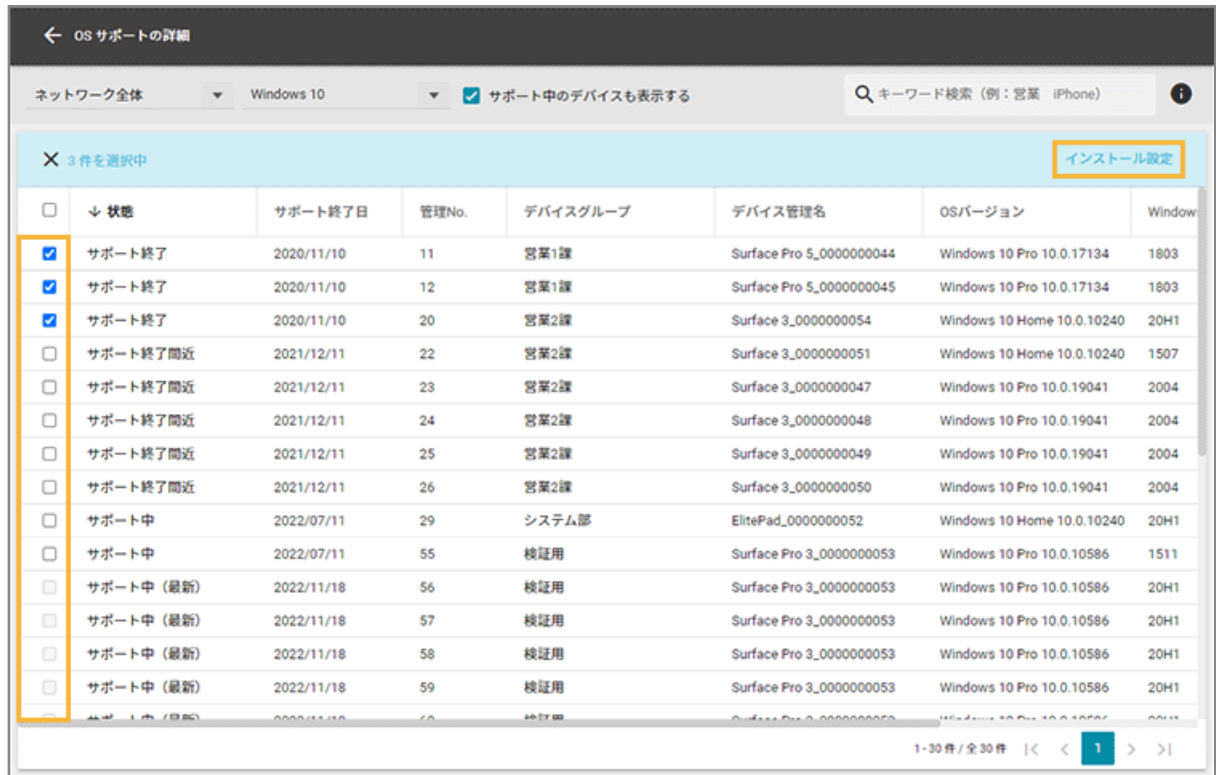
1-30 件 / 全 30 件 |< < 1 > >|

状態

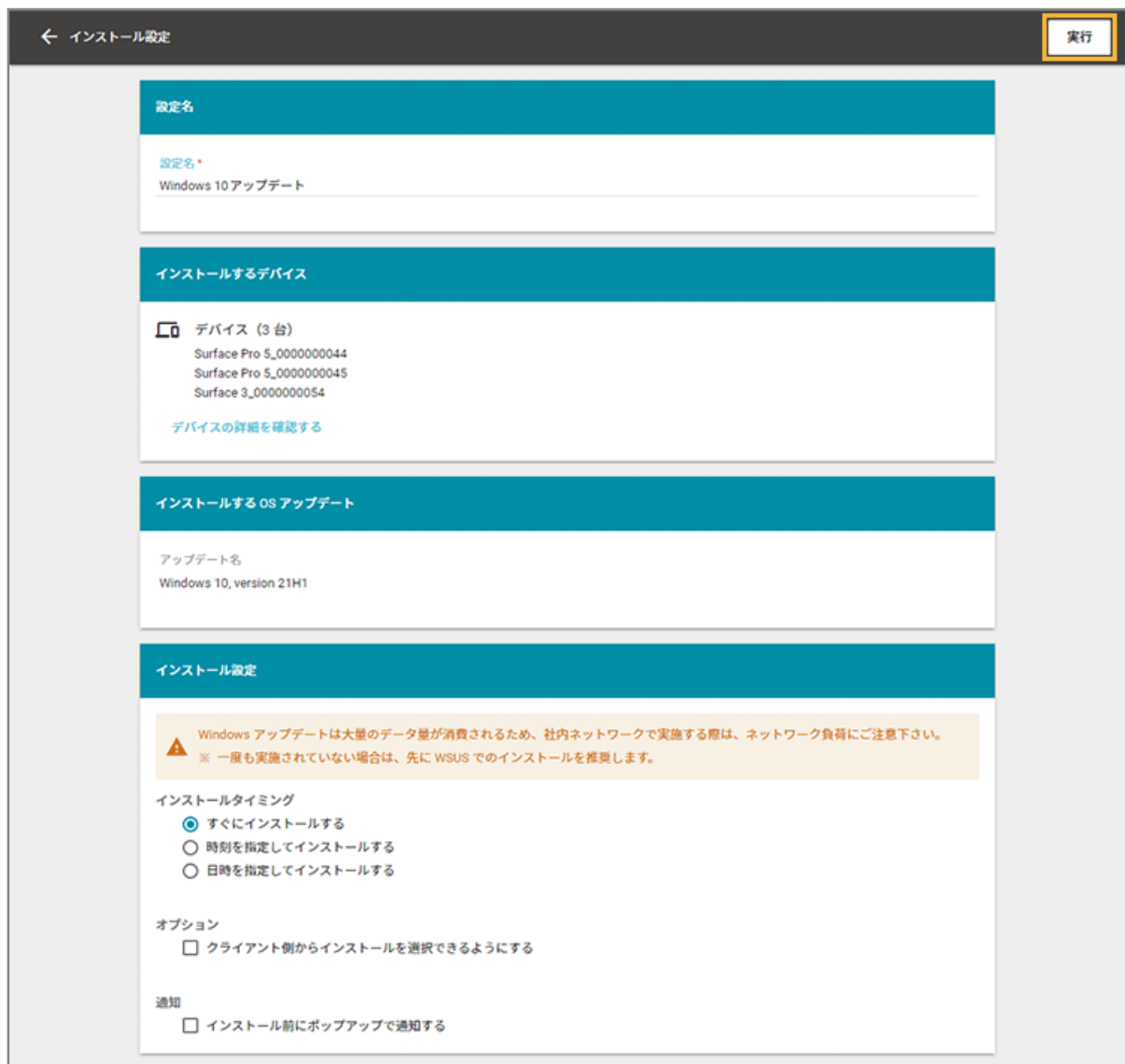
- サポート終了
Microsoft 社の製品サポートが終了しています。
- サポート終了間近
Microsoft 社の製品サポートが 180 日間以内に終了します。

5. デバイスをチェックし、[インストール設定] をクリックします。

OS がサポート終了 / 終了間近のデバイスだけを確認する場合は、[サポート中のデバイスも表示する] のチェックを外します。



6. 項目を設定し、[実行] をクリックします。



設定名

設定名を入力します。[ルール] > [配信設定] > [OS アップデート (Windows)] > [設定状況] 画面で表示されます。

インストールするデバイス

インストールするデバイス名です。デバイスの詳細情報を確認できます。

インストールする OS アップデート

デバイスにインストールする OS バージョンです。

インストール設定

- インストールタイミング

インストールするタイミングを選択します。

- [すぐにインストールする]

実行完了後、すぐにインストールされます。

- [時刻を指定してインストールする]

実行完了後、指定した時刻にインストールされます。すでに指定時刻を過ぎていた場合、すぐにインストールされます。

- [日時を指定してインストールする]

実行完了後、指定した日時にインストールされます。すでに指定日時を過ぎていた場合、すぐにインストールされます。

- オプション

- [クライアント側からインストールを選択できるようにする]

クライアントにインストール確認のメッセージが表示されます。タスクバーの通知領域にアイコンが表示され、クライアント側のタイミングでファイルの実行を選択できます。

- 通知

- [インストール前にポップアップで通知する]

インストール前に、入力した内容をデバイスにポップアップで通知できます。

→ インストール設定が完了します。

月例パッチを確認してインストール設定をする

1. [ルール] の [配信設定] > [OS アップデート (Windows)] をクリックします。



2. [月例パッチ] をクリックし、デバイスグループを選択します。



3. インストールする月例パッチをクリックします。



4. 月例パッチの適用状況を確認します。

注意

MOTEX で動作検証する前の更新プログラムを適用した場合、最新の月例パッチが「未適用」と表示される場合があります。

<input type="checkbox"/>	状態	適用された月例パッチ	管理No.	デバイスグループ	デバイス管理名	OSバージョン	W
<input type="checkbox"/>	未適用	2023/06/13	20	営業2課	Surface 3_0000000054	Windows 10 Home 10.0.10240	2
<input type="checkbox"/>	未適用	2023/02/13	22	営業2課	Surface 3_0000000051	Windows 10 Home 10.0.10240	1
<input type="checkbox"/>	未適用	2023/02/13	11	営業1課	Surface Pro 5_0000000044	Windows 10 Pro 10.0.17134	1
<input type="checkbox"/>	未適用	2023/02/13	12	営業1課	Surface Pro 5_0000000045	Windows 10 Pro 10.0.17134	1
<input type="checkbox"/>	未適用	2023/02/13	23	営業2課	Surface 3_0000000047	Windows 10 Pro 10.0.19041	2
<input type="checkbox"/>	未適用	2023/02/13	24	営業2課	Surface 3_0000000048	Windows 10 Pro 10.0.19041	2
<input type="checkbox"/>	未適用	2023/02/13	79	検証用	Surface Pro 3_0000000053	Windows Server 2019	
<input type="checkbox"/>	適用済み	2023/03/11	29	システム部	ElitePad_0000000052	Windows 10 Home 10.0.10240	2
<input type="checkbox"/>	適用済み	2023/03/11	55	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	1
<input type="checkbox"/>	適用済み	2023/03/11	56	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	2
<input type="checkbox"/>	適用済み	2023/03/11	57	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	2
<input type="checkbox"/>	適用済み	2023/03/11	58	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	2
<input type="checkbox"/>	適用済み	2023/03/11	59	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	2
<input type="checkbox"/>	適用済み	2023/03/11	60	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	2

状態

- 未適用

月例パッチが未適用です。

- 適用済み

月例パッチが適用されています。過去の月例パッチも適用済みになります。

5. デバイスをチェックし、[インストール設定] をクリックします。

月例パッチが未適用のデバイスだけを確認する場合は、[適用済みのデバイスも表示する] のチェックを外します。

第6章 ルール設定をする

← 月例バッチの詳細

ネットワーク全体 ▼ 最新 (2023/03/11) ▼ サーバー クライアント 適用済みのデバイスも表示する 🔍 キーワード検索 (例: 営業 IP) ⓘ

× 3 件を選択中 インストール設定

<input checked="" type="checkbox"/>	↓ 状態	適用された月例バッチ	管理No.	デバイスグループ	デバイス管理名	OSバージョン	W
<input checked="" type="checkbox"/>	未適用	2023/06/13	20	営業2課	Surface 3_0000000054	Windows 10 Home 10.0.10240	2
<input type="checkbox"/>	未適用	2023/02/13	22	営業2課	Surface 3_0000000051	Windows 10 Home 10.0.10240	1
<input type="checkbox"/>	未適用	2023/02/13	11	営業1課	Surface Pro 5_0000000044	Windows 10 Pro 10.0.17134	1
<input type="checkbox"/>	未適用	2023/02/13	12	営業1課	Surface Pro 5_0000000045	Windows 10 Pro 10.0.17134	1
<input checked="" type="checkbox"/>	未適用	2023/02/13	23	営業2課	Surface 3_0000000047	Windows 10 Pro 10.0.19041	2
<input checked="" type="checkbox"/>	未適用	2023/02/13	24	営業2課	Surface 3_0000000048	Windows 10 Pro 10.0.19041	2
<input type="checkbox"/>	未適用	2023/02/13	79	検証用	Surface Pro 3_0000000053	Windows Server 2019	
<input type="checkbox"/>	適用済み	2023/03/11	29	システム部	ElitePad_0000000052	Windows 10 Home 10.0.10240	2
<input type="checkbox"/>	適用済み	2023/03/11	55	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	1
<input type="checkbox"/>	適用済み	2023/03/11	56	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	2
<input type="checkbox"/>	適用済み	2023/03/11	57	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	2
<input type="checkbox"/>	適用済み	2023/03/11	58	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	2
<input type="checkbox"/>	適用済み	2023/03/11	59	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	2
<input type="checkbox"/>	適用済み	2023/03/11	60	検証用	Surface Pro 3_0000000053	Windows 10 Pro 10.0.10586	2

1-35 件 / 全 35 件 |< < 1 > >|

6. 項目を設定し、[実行] をクリックします。

← インストール設定 実行

設定名

設定名*
セキュリティ更新プログラム配信

インストールするデバイス

📁 デバイス (3 台)
Surface_3_0000000054
Surface_3_0000000047
Surface_3_0000000048
[デバイスの詳細を確認する](#)

インストールする月例パッチ

月例パッチ
2023/03/11

説明
Windows 10 2004 64 ビット [説明ページ](#)
Windows 10 20H1 64 ビット [説明ページ](#)
[全て表示する](#)

インストール設定

⚠️ 月例パッチは大量のデータ量が消費されるため、社内ネットワークで実施する際は、ネットワーク負荷にご注意下さい。
※ 一度も実施されていない場合は、先に WSUS でのインストールを推奨します。

インストールタイミング

すぐにインストールする
 時刻を指定してインストールする
 日時を指定してインストールする

オプション

クライアント側からインストールを選択できるようにする

通知

インストール前にポップアップで通知する

設定名

設定名を入力します。[ルール] > [配信設定] > [OS アップデート (Windows)] > [設定状況] 画面で表示されます。

インストールするデバイス

インストールするデバイス名です。デバイスの詳細情報を確認できます。

インストールする月例パッチ

インストールする月例パッチを選択します。

インストール設定

- インストールタイミング

インストールするタイミングを選択します。

- [すぐにインストールする]
実行完了後、すぐにインストールされます。
- [時刻を指定してインストールする]
実行完了後、指定した時刻にインストールされます。すでに指定時刻を過ぎていた場合、すぐにインストールされます。
- [日時を指定してインストールする]
実行完了後、指定した日時にインストールされます。すでに指定日時を過ぎていた場合、すぐにインストールされます。
- オプション
 - [クライアント側からインストールを選択できるようにする]
クライアントにインストール確認のメッセージが表示されます。タスクバーの通知領域にアイコンが表示され、クライアント側のタイミングでファイルの実行を選択できます。
 - 通知
 - [インストール前にポップアップで通知する]
インストール前に、入力した内容をデバイスにポップアップで通知できます。
→ インストール設定が完了します。

更新プログラムを確認してインストール設定をする

ポイント

エンドポイントマネージャーは、インストール設定をデバイスに適用します。インストール設定が適用されたデバイスに更新プログラムをダウンロード/インストールするときの動作は、Windows Update を利用するため、OS の動作に依存します。

注意

インストール設定をする場合、Active Directory のグループポリシー「インターネット上の Windows Update に接続しない」を「無効」に設定してください。「有効」に設定していると、Microsoft アップデートサーバーにアクセスできず、インストールできません。

1. [ルール] の [配信設定] > [OS アップデート (Windows)] をクリックします。



2. **【更新プログラム】** をクリックし、**更新プログラム** を検索します。



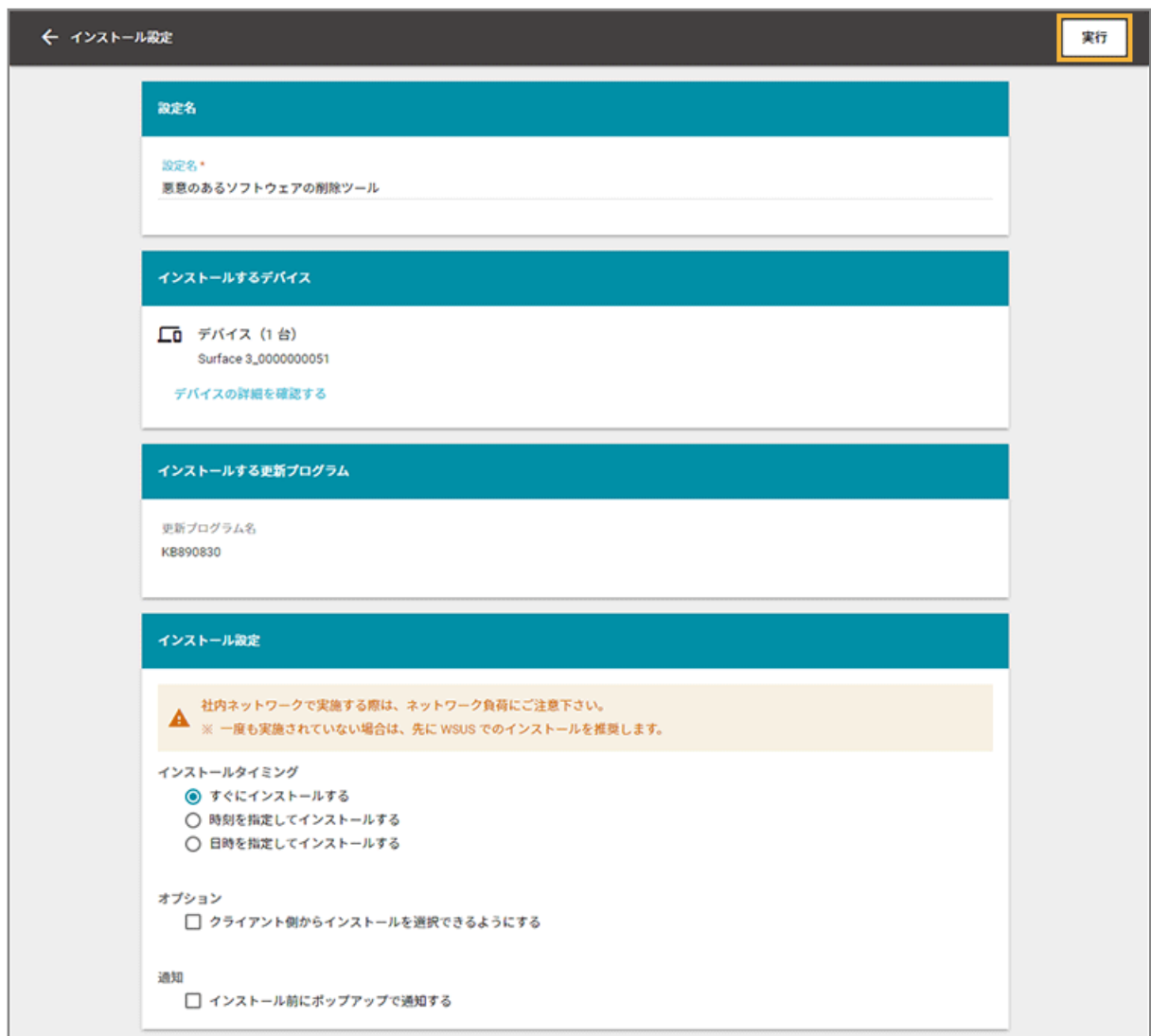
3. **更新プログラム** を適用できるデバイスを確認します。



4. **デバイス** をチェックし、**【インストール設定】** をクリックします。



5. 項目を設定し、[実行] をクリックします。



設定名

設定名を入力します。[ルール] > [配信設定] > [OS アップデート (Windows)] > [設定状況] 画面で表示されます。

インストールするデバイス

インストールするデバイス名です。デバイスの詳細情報を確認できます。

インストールする更新プログラム

デバイスにインストールする更新プログラムです。

インストール設定

- インストールタイミング

インストールするタイミングを選択します。

- [すぐにインストールする]

実行完了後、すぐにインストールされます。

- [時刻を指定してインストールする]

実行完了後、指定した時刻にインストールされます。すでに指定時刻を過ぎていた場合、すぐにインストールされます。

- [日時を指定してインストールする]

実行完了後、指定した日時にインストールされます。すでに指定日時を過ぎていた場合、すぐにインストールされます。

- オプション

- [クライアント側からインストールを選択できるようにする]

クライアントにインストール確認のメッセージが表示されます。タスクバーの通知領域にアイコンが表示され、クライアント側のタイミングでファイルの実行を選択できます。

- 通知

- [インストール前にポップアップで通知する]

インストール前に、入力した内容をデバイスにポップアップで通知できます。

→ インストール設定が完了します。

■ 実行状況を確認する

OS サポート/月例パッチ/更新プログラムの実行状況を確認できます。

1. [ルール] の [配信設定] > [OS アップデート (Windows)] をクリックします。



2. [設定状況] をクリックします。



3. 設定をクリックします。



4. [実行状況] をクリックし、実行状況を確認します。

実行状況	管理No.	デバイスグループ	デバイス管理名	使用者名	OSバージョン
実行中	26	営業2課	Surface 3_0000000050	MO一郎	Windows 10
実行中	29	システム部	ElitePad_0000000052	共有タブレット	Windows 10
実行失敗	55	検証用	Surface Pro 3_0000000053	検証用A	Windows 10
実行完了	11	営業1課	Surface Pro 5_0000000044	吉田 勝平	Windows 10
実行完了	12	営業1課	Surface Pro 5_0000000045	加藤 信也	Windows 10
実行完了	20	営業2課	Surface 3_0000000054	石川 忍	Windows 10
実行完了	22	営業2課	Surface 3_0000000051	荒城 太郎	Windows 10
実行完了	23	営業2課	Surface 3_0000000047	MO三郎	Windows 10
実行完了	24	営業2課	Surface 3_0000000048	MO花子	Windows 10
実行完了	25	営業2課	Surface 3_0000000049	MO二郎	Windows 10

実行状況

- 設定通知前
インストール設定がデバイスに適用されていないときに表示されます。
- 設定通知完了
インストール設定がデバイスに適用されたときに表示されます。
- 実行中
インストール設定の適用後、ダウンロード／インストール中のときに表示されます。
- 実行失敗
インストール設定の適用後、ダウンロード／インストールに失敗したときに表示されます。失敗した場合は、再度インストール設定を実行する必要があります。
- 実行完了
OS／月例パッチがデバイスに適用されたときに表示されます。

エラー詳細

- 空き容量が足りません。
デバイスがインストールに必要な空き容量が足りないときに表示されます。OS のインストールの場合は 6,144MB、月例パッチのインストールの場合は 2,048MB の空き容量が必要です。
- Microsoft 社によりダウンロード URL が変更されている可能性があります。再度配信設定を行ってください。

月例パッチのインストール設定がデバイスに適用されてからダウンロードするまでの間に、Microsoft 社がダウンロード URL を変更した場合に表示されます。

- 実行に失敗しました。

デバイスが月例パッチのダウンロード/インストールに失敗したときに表示されます。

- 他の更新プログラムを適用中です。

デバイスが他の OS/更新プログラムを適用中のときに表示されます。

- 適用可能な更新プログラムが存在しません。

デバイスがインストール設定をした OS/更新プログラムを適用できないときに表示されます。

- 更新プログラムのダウンロードに失敗しました。

デバイスが OS/更新プログラムのダウンロードに失敗したときに表示されます。

- 更新プログラムのインストールに失敗しました。

デバイスが OS/更新プログラムのインストールに失敗したときに表示されます。

6-5 アプリ設定をする

iOS

Android

Windows

macOS

インストール情報が取得されたアプリの利用レベルを設定します。

レベルを設定すると、レシビ機能を利用して、アラート設定や管理者への通知ができます。

「アプリ設定」では、インストール情報を取得したアプリの利用レベル（「必須」「許可」「未設定」「不許可」「禁止（*）」を設定できます。

*：「禁止」設定ができるのは、Android だけです。

注意

Android Enterprise デバイスには適用できません。Android Enterprise デバイスに適用するポリシーは、[Android Enterprise 設定] で設定します。

詳細は、An-347「Android Enterprise 利用ガイド」を参照してください。

- [アプリの管理レベルを設定する](#)
- [アプリの利用を禁止するときに必要な設定をする](#)
- [新規アプリの管理レベル初期設定](#)
- [未インストールアプリの管理レベルを設定する](#)

アプリの管理レベルを設定する

iOS

Android

Windows

macOS

インストールアプリ情報を取得したアプリごとに、管理レベルを設定できます。

Android の場合、管理レベルを「禁止」に設定すると、アプリの利用を禁止できます。

1. [ルール] の [アプリ設定] をクリックします。



2. グループをクリックし、表示する OS をクリックします。

[▼] をクリックすると、表示するアプリを管理レベルで絞り込みます。管理レベルを設定していないアプリを表示する場合、[未設定] を選択します。さらに絞り込む場合は、「アプリ名」や「カテゴリー」を入力し、検索します。



3. アプリをチェックし、[管理レベルの変更] をクリックします。

アプリを複数選択した場合、同じレベルに設定されます。



4. 管理レベルを選択し、[設定] をクリックします。

注意

「禁止」設定ができるのは、Android だけです。



→ 管理レベルが設定されます。

アプリの利用を禁止するときに必要な設定をする

Android

アプリの利用を禁止する場合、アプリレベルの設定以外に「操作ログ取得設定」と「デバイスへの通知設定」が必要です。

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、[Android] をクリックして、[作成] をクリックします。



3. 「操作ログ取得設定」で、「アプリ利用ログ」の「取得する」をチェックします。



ポイント

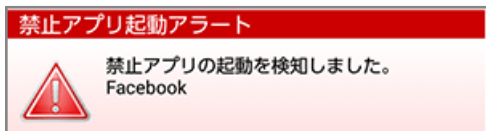
「業務時間のみ取得する」が「有効」の場合、業務時間だけが禁止されます。

4. 「デバイスへの通知設定」で、「操作アラートの通知」の「不許可・禁止したアプリが実行された」の「通知する」をチェックします。



5. [保存] をクリックします。

→ デバイスで「禁止」設定のアプリを起動すると、画面に「禁止アプリ起動アラート」が表示され、強制的にアプリ起動を禁止します。



新規アプリの管理レベル初期設定



新規でアプリがインストールされたときに、自動的に割り当てられるアプリ共通の管理レベルの初期設定を、グループごとに設定できます。

1. [ルール] の [アプリ設定] 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、[変更] をクリックします。



3. アプリ管理レベルを選択し、[保存] をクリックします。

注意

「禁止」設定ができるのは、Android だけです。



→ 管理レベルの初期設定が完了します。

未インストールアプリの管理レベルを設定する



「アプリ設定」画面には、インストールアプリ情報を取得したことがあるアプリしか表示されません。インストールしていないアプリの管理レベルは、次のように設定します。

ポイント

インストールしていないアプリの管理レベルを追加しても、「アプリ設定」画面にアプリ名は表示されません。デバイスにアプリがインストールされたときに、アプリ名が表示されます。

1. [ルール] の [アプリ設定] をクリックします。



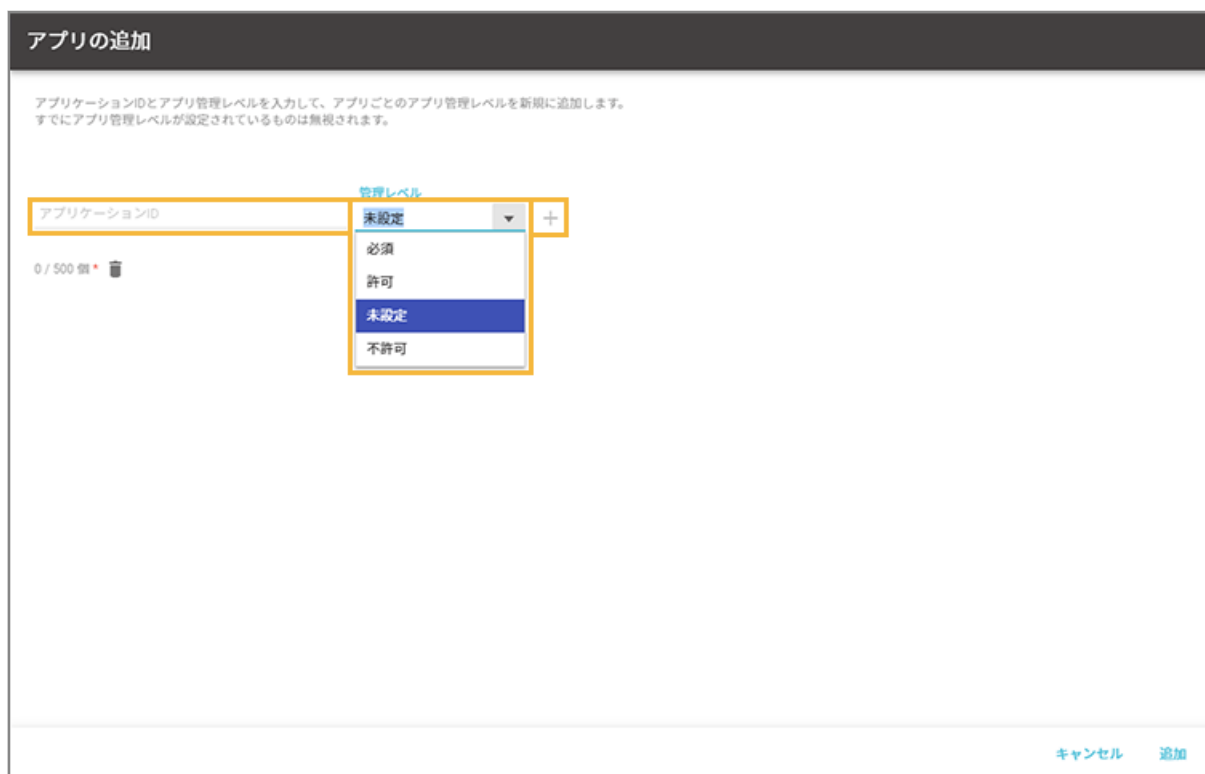
2. グループをクリックし、OS をクリックして、[アプリ管理レベルの追加] をクリックします。



3. 「アプリケーション ID (パッケージ名)」を入力し、「管理レベル」を選択して、[+] をクリックします。

注意

「禁止」設定ができるのは、Android だけです。



4. [追加] をクリックします。

→ 未インストールアプリの管理レベルが設定されます。

第7章 仕様

- [7-1 情報取得／設定（ポリシー）反映のタイミング](#)
- [7-2 記録メディア別制御一覧](#)

7-1 情報取得／設定（ポリシー）反映のタイミング

■ iOS の場合

デバイスからサーバーに、MDM 構成プロファイルで取得した情報をおくるタイミング

確認画面	取得情報	デバイスからサーバーに取得情報をおくるタイミング
デバイス詳細	デバイス情報／ネットワーク／セキュリティ	<ul style="list-style-type: none"> MDM 構成プロファイルインストール後 【最新情報を取得】実行後 12 時間に 1 回の定期通信
	インストールアプリ／プロファイル	<ul style="list-style-type: none"> 【最新情報を取得】実行後 12 時間に 1 回の定期通信 【ルール】で取得設定を変更後
クライアント	MDM 構成プロファイルインストール日時	インストール成功時（上書きインストールした場合も同様）
	LANSCOPE Client インストール日時	LANSCOPE Client 登録成功時（アンインストール後、再インストールして登録した場合も同様）
	LANSCOPE クライアント最終稼働日時	<ul style="list-style-type: none"> 【最新情報を取得】実行後 12 時間に 1 回の定期通信 【ルール】の基本設定変更時（*） LANSCOPE Client 再起動時
	MDM 構成プロファイル最終通信日時	<ul style="list-style-type: none"> 【最新情報を取得】実行後 12 時間に 1 回の定期通信
	LANSCOPE Client 最終通信日時	<ul style="list-style-type: none"> 12 時間に 1 回の定期通信 【ルール】の基本設定変更時（*） LANSCOPE Client 再起動時
モニター	最新位置情報	5 分に 1 回

* : LANSCOPE Client をインストールしたデバイスが対象です。

デバイスからサーバーに、LANSCOPE Client で取得した情報をおくるタイミング

注意

LANSCOPE Client が終了している場合、情報を取得できません。

確認画面	取得情報	デバイスからサーバーに取得情報をおくるタイミング
デバイス詳細	位置情報／操作ログ	5 分に 1 回
	位置情報サービス／LANSCOPE Client 位置情報利用許可	<ul style="list-style-type: none"> ● [最新情報を取得] 実行後 ● 12 時間に 1 回の定期通信
	Jailbreak	<ul style="list-style-type: none"> ● LANSCOPE Client 再起動時に取得
	LANSCOPE Client バージョン	

設定が管理対象デバイスに反映されるまでの時間

設定画面	設定	設定が管理対象デバイスに反映されるまでの時間
ルール	業務時間設定	<ul style="list-style-type: none"> ● [ルール] の基本設定変更時
	デバイス使用者への設定情報表示	<ul style="list-style-type: none"> ● 12 時間に 1 回の定期通信 ● LANSCOPE Client 再起動時 (*)
	デバイス情報取得設定	<ul style="list-style-type: none"> ● [ルール] の基本設定変更時 ● 12 時間に 1 回の定期通信
	操作ログ取得設定	<ul style="list-style-type: none"> ● [ルール] の基本設定変更時
	位置情報ログ取得設定	<ul style="list-style-type: none"> ● 12 時間に 1 回の定期通信
	デバイスへの通知設定	<ul style="list-style-type: none"> ● LANSCOPE Client 再起動時 (*)
	パスワードポリシー設定	<ul style="list-style-type: none"> ● [ルール] の基本設定変更時 ● 12 時間に 1 回の定期通信

* : LANSCOPE Client を終了後に再起動した場合や、「大幅変更位置情報サービス」で位置情報を取得し、LANSCOPE Client が自動起動した場合が対象です。

アクションが実行されるタイミング

トリガーに該当する情報が、デバイスからサーバーに届いている状態を始点とします。

設定画面	その他	アクションが実行されるタイミング
レシピ (アクション)	管理者にメールでお知らせする	即時
	指定プロファイルを配信する	即時 (*1)

設定画面	その他	アクションが実行されるタイミング
	指定アプリを配信する	即時
	メッセージを配信する	即時 (*2)
	アンケートを配信する	即時 (*2)
	アラートに設定する	即時
デバイス詳細	リモートロック/リモートワイプ	即時 (*2)

*1 : パスコード設定で画面をロックしている場合、ロックが解除されたタイミングで配信されます。

*2 : 実行後の状態は、管理コンソールに即時反映されます。

■ Android の場合

デバイスからサーバーに取得情報をおくるタイミング

確認画面	取得情報	デバイスからサーバーに取得情報をおくるタイミング	
デバイス詳細	デバイス情報/ネットワーク/セキュリティ	<ul style="list-style-type: none"> ● デバイスの起動後、15 分以内 ● [最新情報を取得] 実行後 ● 12 時間に 1 回の定期通信 ● [ルール] の基本設定変更時 	
	インストールアプリ		
	位置情報/操作ログ		5 分に 1 回
	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	1 時間に 1 回、またはデバイス再起動から 10 分後
	LANSCOPE クライアント最終稼働日時	<ul style="list-style-type: none"> ● デバイスの起動後、15 分以内 ● [最新情報を取得] 実行後 ● 12 時間に 1 回の定期通信 ● [ルール] の基本設定変更時 	
	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）		
モニター	最新位置情報	5 分に 1 回	

設定が管理対象デバイスに反映されるまでの時間

設定画面	設定	設定が管理対象デバイスに反映されるまでの時間
ルール	業務時間設定	<ul style="list-style-type: none"> ● [ルール] の基本設定変更時

設定画面	設定	設定が管理対象デバイスに反映されるまでの時間
	LANSCOPE Client アップデート設定	<ul style="list-style-type: none"> 12 時間に 1 回の定期通信 LANSCOPE Client 再起動時
	デバイス使用者への設定情報表示	
	デバイス情報取得設定	
	操作ログ取得設定	
	位置情報ログ取得設定	
	デバイスへの通知設定	
	パスワードポリシー設定	
	マルチユーザー機能制御	

アクションが実行されるタイミング

トリガーに該当する情報が、デバイスからサーバーに届いている状態を始点とします。

設定画面	その他	アクションが実行されるタイミング
レシピ (アクション)	管理者にメールでお知らせする	即時
	メッセージを配信する	即時 (*)
	アンケートを配信する	即時 (*)
	アラートに設定する	即時
デバイス詳細	リモートロック/リモートワイプ	即時 (*)

* : 実行後の状態は、管理コンソールに即時反映されます。

■ Windows の場合

デバイスからサーバーに取得情報をおくるタイミング

確認画面	取得情報	デバイスからサーバーに取得情報をおくるタイミング
デバイス詳細	デバイス情報/ネットワーク/セキュリティ	<ul style="list-style-type: none"> デバイスの起動後、10 分以内 [最新情報を取得] 実行後 12 時間に 1 回の定期通信
	インストールアプリ/Microsoft Office (*1)	
	位置情報	5 分に 1 回 (*2)
	操作ログ	5 分に 1 回
	クライアント	LANSCOPE クライアントインストール日時

確認画面	取得情報	デバイスからサーバーに取得情報をおくるタイミング
	LANSCOPE クライアントバージョン	12 時間に 1 回の定期通信
	LANSCOPE クライアント最終稼働日時	5 分に 1 回
モニター	最新位置情報	5 分に 1 回 (*2)

*1 : パッケージとしてインストールされている Microsoft Office 2016/2013/2010/2007 の情報を取得します。

Microsoft 365 の情報は取得できません。

*2 : Windows Server OS は、位置情報取得機能に未対応です。

設定が管理対象デバイスに反映されるまでの時間

設定画面	設定	設定が管理対象デバイスに反映されるまでの時間
ルール	業務時間設定	設定後、10 分程度
	デバイス使用者への設定情報表示	
	デバイス情報取得設定	
	位置情報ログ取得設定	
	アンインストール防止設定	
	PC 操作ログ設定	
	記録メディア制御設定	
	配信設定	

アクションが実行されるタイミング

トリガーに該当する情報が、デバイスからサーバーに届いている状態を始点とします。

設定画面	その他	アクションが実行されるタイミング
レシピ (アクション)	管理者にメールでお知らせする	即時
	メッセージを配信する	5 分以内 (*)
	アンケートを配信する	5 分以内 (*)
	アラートに設定する	5 分以内
デバイス詳細	リモートロック/リモートワイプ	5 分以内 (*)

* : 実行後の状態は、管理コンソールに即時反映されます。

■ macOS の場合

デバイスからサーバーに、MDM 構成プロファイルで取得した情報をおくるタイミング

確認画面	取得情報	デバイスからサーバーに取得情報をおくるタイミング
デバイス詳細	デバイス情報/ネットワーク/セキュリティ	<ul style="list-style-type: none"> MDM 構成プロファイルインストール後 [最新情報を取得] 実行後 12 時間に 1 回の定期通信
	インストールアプリ/プロファイル	<ul style="list-style-type: none"> [最新情報を取得] 実行後 12 時間に 1 回の定期通信 [ルール] で取得設定を変更後
クライアント	MDM 構成プロファイルインストール日時	インストール/上書きインストール成功時
	LANSCOPE Client インストール日時	インストール成功時（アンインストール後、再インストールして登録した場合も同様）
	LANSCOPE クライアント最終稼働日時	<ul style="list-style-type: none"> [最新情報を取得] 実行後 12 時間に 1 回の定期通信
	MDM 構成プロファイル最終通信日時	
	LANSCOPE Client 最終通信日時	5 分に 1 回

デバイスからサーバーに、LANSCOPE Client で取得した情報をおくるタイミング

注意

LANSCOPE Client が終了している場合、情報を取得できません。

確認画面	取得情報	デバイスからサーバーに取得情報をおくるタイミング
デバイス詳細	デバイス情報/ネットワーク	<ul style="list-style-type: none"> LANSCOPE Client インストール後
	LANSCOPE Client バージョン	<ul style="list-style-type: none"> 1 時間に 1 回
	操作ログ	5 分に 1 回

設定が管理対象デバイスに反映されるまでの時間

設定画面	設定	設定が管理対象デバイスに反映されるまでの時間
ルール	業務時間設定	<ul style="list-style-type: none"> 12 時間に 1 回の定期通信

設定画面	設定	設定が管理対象デバイスに反映されるまでの時間
	デバイス情報取得設定	<ul style="list-style-type: none"> • [ルール] の基本設定変更時
	アンインストール防止設定	
	パスワードポリシー設定	
	PC 操作ログ設定	設定後、10 分程度
	記録メディア制御設定	

アクションが実行されるタイミング

トリガーに該当する情報が、デバイスからサーバーに届いている状態を始点とします。

設定画面	その他	アクションが実行されるタイミング
レシピ (アクション)	管理者にメールでお知らせする	即時
	アラートに設定する	即時
デバイス詳細	リモートロック/リモートワイプ	即時 (*)

* : 実行後の状態は、管理コンソールに即時反映されます。

7-2 記録メディア別制御一覧

ポイント

デバイスに WPD 機器を接続すると、デバイス特有の動作をする場合があるため、ご利用前に動作を確認してください。

たとえば、MTP モードでは「読み取り専用」および「操作ログの取得が可能」であっても、PTP モードに変更するといずれも「不可能」になる WPD 機器もあります。

■ Windows の場合

対象デバイス	接続形態／モード	LANSCOPE エンドポイント マネージャ オン プレミス版で の種別	禁止	読み取 り専用	ログ取 得	
CD-ROM/R/RW	USB/IEEE1394	CD/DVD	○	○	○	
	オンボード (ATAPI/SATA/SCSI など)		— (*1)	○	○	
DVD-ROM/-R/ +R/-RW/+RW /RAM	USB/IEEE1394	CD/DVD	○	○	○	
	オンボード (ATAPI/SATA/SCSI など)		— (*1)	○	○	
FD	USB	FD	○	○	○	
	オンボード		— (*1)	○	○	
MO	USB	USB 接続機 器	○	○	○	
	オンボード	その他機器	—	—	○	
HDD	USB	USB 接続機 器	○	○	○	
	UASP		○	○	○	
	IEEE1394		その他機器	○	○	○
	PC カード	SCSI		—	○	○
		eSATA		—	○	○
	PCI ボード (*2)	SCSI		—	—	○
eSATA		—	—	○		

対象デバイス	接続形態/モード		LANSCOPE エンドポイントマネー ジャー オン プレミス版で の種別	禁止	読み取 り専用	ログ取 得		
HUB	USB		USB 接続機 器	—	—	—		
各種メモリ	IEEE1394	メモリスティック	その他機器	○	○	○		
		PC カード		コンパクトフラッ シュ	○	○	○	
				スマートメディア	○	○	○	
				SD メモリカード	○	○	○	
				MMC(マルチメディ アカード)	○	○	○	
	PC 内蔵	マルチカードリー ダー		○	○	○		
		メモリカード(Sony 社製 PC)		—	○	○		
		SD メモリカード		○	○	○		
	USB	マルチカードリー ダー		USB 接続機 器	○	○	○	
		USB メモリ			○	○	○	
		SD メモリカード			○	○	○	
		MMC(マルチメディ アカード)			○	○	○	
	Android デバイス (スマートフォン/ タブレット) (*3)	USB		カードリーダー モード、microSD モードなど	USB 接続機 器	○	○	○
				MTP モード、PTP モードなど		○	○	○
—		—	△ (*4)	—	—			
独自ドライバーの インストールを行 う製品 (Galaxy で 確認)		USB 接続機 器	△ (*5)	—	—			
			△ (*6)	—	—			
スマートデバイス 管理用ソフトウェ	—	—	△ (*6)	—	—			

対象デバイス	接続形態／モード		LANSCOPE エンドポイント マネージャ オン プレミス版で の種別	禁止	読み取 り専用	ログ取 得
		アをインストール する製品(Xperia で 確認)				
	Bluetooth		通信デバイス	○	—	○
	無線 LAN			○(*7)	—	○
iPhone、iPad	USB	iTunes あり	USB 接続機 器	○	△(*4)	○
		iTunes なし		○	○	○
	Bluetooth		通信デバイス	○	—	○
	無線 LAN			○(*7)	—	○
携帯音楽プレー ヤー	USB		USB 接続機 器	○	○	○
イメージキャ ナー				—	—	—
Web カメラ				—	—	—
デジタルカメラ				△(*8)	○	○
フィーチャーフォ ン				○	○	○
PC	赤外線		通信デバイス	○	—	○
	Bluetooth			○	—	○
	USB リンクケーブル		USB 接続機 器、CD/DVD	○	—	—
	LAN ケーブル		通信デバイス	—	—	—

*1：内蔵 CD／内蔵 DVD／内蔵 FD は読み取り専用になります。

*2：禁止／読み取り専用を対象とした場合、OS を起動する HDD アクセスが不可能となるため、制御対象外です。

*3：一部の機種では、制御できない場合があります。

*4：アプリ禁止により、読み書きを禁止できます。

*5：初回接続時に行われるドライバーインストールの状況によって、禁止できないことがあります。2 回目以降の接続時は禁止できます。

*6：インストーラー実行時に、禁止できない場合があります。

*7：スマートフォン側に、FTP/Web サーバーとして動作するアプリをインストールすると、無線 LAN を使用してファイルを持ち出される場合があります。

*8：一部の機種では、禁止設定時でも、デジタルカメラの動きによって読み取り専用で接続される場合があります。

■ macOS の場合

対象デバイス	接続形態/モード		LANSCOPE エンドポイント マネージャ オン プレミス版で の種別	読み書き 禁止	読み取 り専用	ログ取 得
CD-ROM/R/RW (*1)	USB		CD/DVD	○	○	○
	オンボード (SATA など)			○	○	○
DVD-ROM/-R/ +R/-RW/+RW /RAM (*1)	USB		CD/DVD	○	○	○
	オンボード (SATA など)			○	○	○
HDD	USB		その他機器	○	○	○
	UASP			○	○	○
各種メモリ	PC 内蔵	SD メモリカード	その他機器	○	○	○
	USB	USB メモリ	その他機器	○	○	○
		SD メモリカード (*2)		○	○	○
Android デバイス (スマートフォン/ タブレット) (*1)	USB	カードリーダー モード、microSD モードなど	その他機器	○	○	○
デジタルカメラ	USB		その他機器	△ (*3)	○	○

*1：一部の機種では、制御できない場合があります。

*2：除外設定をする場合は、SD メモリカードリーダーを接続したあとに、SD メモリカードを挿入してください。利用できない場合は、SD メモリカードリーダーを接続したまま、SD メモリカードを挿入し直してください。

*3：一部の機種では、禁止設定時でも、デジタルカメラの動きによって読み取り専用で接続される場合があります。

MOTEX

© MOTEX Inc.