

中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）関連資料

**設定解説資料**  
**（LANSCOPE エンドポイントマネージャー**  
**クラウド版 ~iOS~）**

**Ver1.0** (2023.07)

本書は、総務省の調査研究事業により作成したものです。

本書に関する問い合わせ先（個別のシステムおよび環境に関する御質問については、製品の開発元にお問い合わせください。）

総務省 サイバーセキュリティ統括官室

Email [telework-security@ml.soumu.go.jp](mailto:telework-security@ml.soumu.go.jp)

URL [https://www.soumu.go.jp/main\\_sosiki/cybersecurity/telework/](https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/)

## 目次

<b>1</b>	<b>はじめに</b> .....	<b>3</b>
<b>2</b>	<b>チェックリスト項目に対応する設定作業一覧</b> .....	<b>4</b>
<b>3</b>	<b>管理者向け設定作業</b> .....	<b>5</b>
<b>3-1</b>	<b>チェックリスト 2-4 への対応</b> .....	<b>5</b>
3-1-1	アプリケーションの制限 .....	5
<b>3-2</b>	<b>チェックリスト 5-1 への対応</b> .....	<b>13</b>
3-2-1	メーカーサポートの確認 .....	13
<b>3-3</b>	<b>チェックリスト 8-1 への対応</b> .....	<b>18</b>
3-3-1	端末位置の把握 .....	18
<b>3-4</b>	<b>チェックリスト 8-2 への対応</b> .....	<b>21</b>
3-4-1	リモートロック・リモートワイプの実行 .....	21
<b>3-5</b>	<b>チェックリスト 9-1 への対応</b> .....	<b>25</b>
3-5-1	iOS 端末のパスワードポリシー設定とアラート設定 .....	25
<b>3-6</b>	<b>チェックリスト 9-2 への対応</b> .....	<b>30</b>
3-6-1	エンドポイントマネージャーのログインパスワード変更 .....	30
<b>3-7</b>	<b>チェックリスト 10-1 への対応</b> .....	<b>31</b>
3-7-1	エンドポイントマネージャーの管理者権限の付与 .....	31
<b>3-8</b>	<b>チェックリスト 10-2 への対応</b> .....	<b>37</b>
3-8-1	エンドポイントマネージャーのログインパスワード強度 .....	37
<b>3-9</b>	<b>チェックリスト 10-3 への対応</b> .....	<b>37</b>
3-9-1	エンドポイントマネージャーの管理者権限の管理 .....	37

## 1 はじめに

### (ア) 本書の目的

本書は、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目について、LANSCOPE エンドポイントマネージャー クラウド版（以下エンドポイントマネージャー）を利用した具体的な作業内容の解説をすることで、管理者が利用時に実施すべき作業の理解を助けることを目的としています。

### (イ) 前提条件

本製品のライセンス形態はすべて有償で「ライト A」「ライト B」「ベーシック」が存在します。（2022 年 11 月 1 日現在）利用するライセンス種類により使用可能な機能が異なります。**本資料では「ベーシック」ライセンスの利用を前提としております。**

### (ウ) 本書の活用方法

本書は、中小企業のセキュリティ管理担当者やシステム管理担当者（これらに準ずる役割を担っている方を含みます）を対象として、その方々がチェックリスト項目の具体的な対策を把握できるよう、第 2 章ではチェックリスト項目に紐づけて解説内容と解説ページを記載しています。本書では第 3 章にて管理者向けに設定手順や注意事項を記載しています。

表 1. 本書の全体構成

章題	概要
1 はじめに	本書を活用するための、目的、本書の前提条件、活用方法、免責事項を説明しています。
2 チェックリスト項目と設定解説の対応表	本書で解説するチェックリスト項目と、その項目に対応する設定作業手順および注意事項の解説が記載されたページを記載しています。
3 管理者向け設定作業	対象のチェックリスト項目に対する管理者向けの設定手順や注意事項を解説しています。

### (エ) 免責事項

本資料は現状有姿でご利用者に提供するものであり、明示であると黙示であるとを問わず、正確性、商品性、有用性、ご利用者様の特定の目的に対する適合性を含むその他の保証を一切行つものではありません。本資料に掲載されている情報は、2022 年 11 月 1 日時点の各製品の操作画面を基に作成しており、その後の製品仕様の更新、追加、変更、削除もしくは部分改廃により、画面表示等に差異が生じる可能性があります。本資料は、初期出荷状態の製品を単体動作させている環境を利用して設定手順を解説しています。本製品をご利用者様の業務環境で利用する際には、本資料に掲載している設定により業務環境システムに影響がないかをご利用者様の責任にて確認の上、実施するようにしてください。本資料に掲載されている製品仕様・設定方法について不明点がありましたら、製品提供元へお問い合わせください。

## 2 チェックリスト項目に対応する設定作業一覧

本書で解説しているチェックリスト項目、対応する設定作業解説および注意事項が記載されているページは下記のとおりです。

表 2. チェックリスト項目と管理者向け設定作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
<b>2-4 マルウェア対策</b> スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。	<ul style="list-style-type: none"> <li>・ <a href="#">アプリケーションの制限</a></li> </ul>	P.5
<b>5-1 脆弱性管理</b> テレワーク端末にはメーカーサポートが終了した OS やアプリケーションを利用しないよう周知する。	<ul style="list-style-type: none"> <li>・ <a href="#">メーカーサポートの確認</a></li> </ul>	P.13
<b>8-1 データ保護</b> スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	<ul style="list-style-type: none"> <li>・ <a href="#">端末位置の把握</a></li> </ul>	P.18
<b>8-2 データ保護</b> テレワーク端末の紛失時に備えて MDM 等を導入し、リモートからのデータ消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用する。	<ul style="list-style-type: none"> <li>・ <a href="#">リモートロック・リモートワイプの実行</a></li> </ul>	P.21
<b>9-1 アカウント・認証管理</b> テレワーク端末のログインアカウントや、テレワークで利用する各システムのパスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。	<ul style="list-style-type: none"> <li>・ <a href="#">iOS 端末のパスワードポリシー設定とアラート設定</a></li> </ul>	P.25
<b>9-2 アカウント・認証管理</b> テレワーク端末のログインパスワードや、テレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。	<ul style="list-style-type: none"> <li>・ <a href="#">エンドポイントマネージャーのログインパスワード変更</a></li> </ul>	P.30
<b>10-1 特権管理</b> テレワーク端末やテレワークで利用する各システムの管理者権限は、業務上必要な最小限の人に付与する。	<ul style="list-style-type: none"> <li>・ <a href="#">エンドポイントマネージャーの管理者権限の付与</a></li> </ul>	P.31
<b>10-2 特権管理</b> テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用する。	<ul style="list-style-type: none"> <li>・ <a href="#">エンドポイントマネージャーのログインパスワード強度</a></li> </ul>	P.37
<b>10-3 特権管理</b> テレワーク端末やテレワークで利用する各システムの管理者権限は、必要な作業時のみ利用する。	<ul style="list-style-type: none"> <li>・ <a href="#">エンドポイントマネージャーの管理者権限の管理</a></li> </ul>	P.37

## 3 管理者向け設定作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第2部に記載されているチェックリスト項目のうち、本製品の管理者が実施すべき対策の設定手順を記載します。

### 3-1 チェックリスト 2-4 への対応

#### 3-1-1 アプリケーションの制限

アプリのインストールを業務上必要なものに限定することで、不審なアプリケーションが実行されるリスクを低減することができます。

##### 【手順①】

ホーム画面から「レシピ」を選択し、「アクション」を選択後、「プロフィールを設定する」をクリックします。



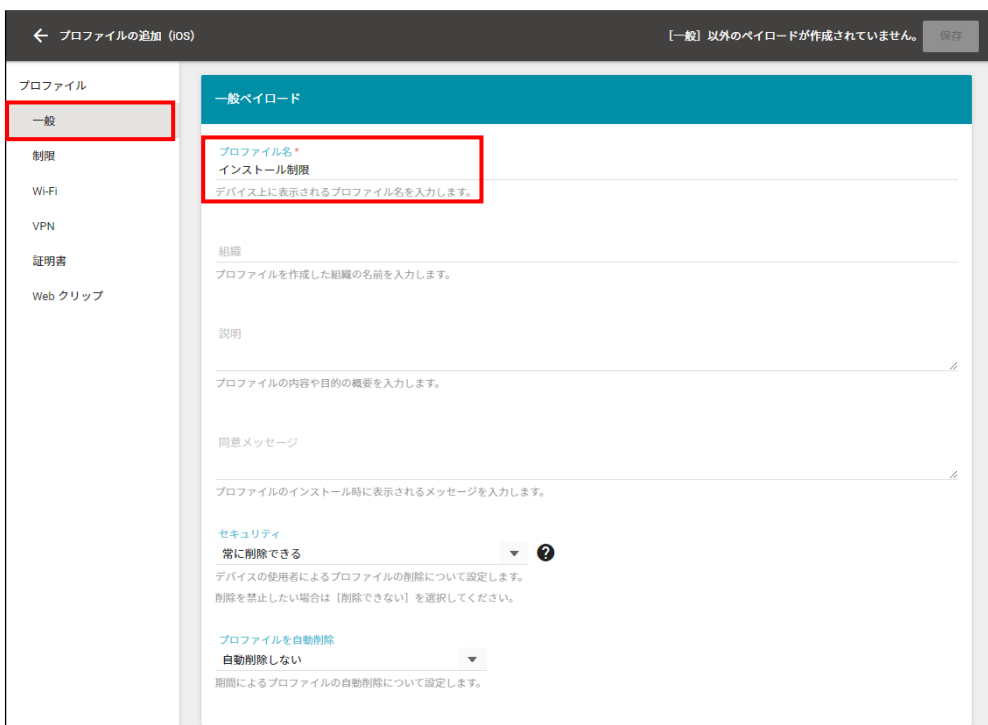
【手順②】

「プロフィールの追加」をクリックし、次の画面で「iOS のプロフィールを作成する」をクリックします。



【手順③】

左側プロフィールメニューの「一般」をクリックし、「プロフィール名」に任意のプロフィール名を入力します。



**【手順④】**

左側プロファイルメニューの「制限」から「制限ペイロードを作成」をクリックします。



【手順⑤】

「制限ペイロード」の「機能」から様々な制限を行うことができます。本手順ではアプリのインストールを許可しない設定とするため、下記項目のチェックを外し、「保存」をクリックします。

- App のインストールを許可する（監視対象のみ）
- App Store からの App のインストールを許可する（監視対象のみ）
- App の自動ダウンロードを許可する（監視対象のみ）



【手順⑥】

プロファイル作成後、ホーム画面から「レシピ」を選択し、「レシピ一覧」から、「レシピの追加」をクリックします。





**【手順⑦】**

任意のレシピ名を入力し、「トリガーを選択」をクリックします。

**【手順⑧】**

トリガーを選択します。（本手順では、トリガーは「任意のタイミングで実行する」を選択）

	すべて	iOS	Android	Windows	macOS
デバイス情報					
操作ログ情報					
位置情報				x	x
任意のタイミング					
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"/>	<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"/>	<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 type="checkbox"/>	x	x
デバイスが管理外になっている	<input type="checkbox"/>	<input type="checkbox"/>	x	<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"/>	<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"/>	<input type="checkbox"/>
定期的に行う	<input type="checkbox"/>	<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"/>	<input type="checkbox"/>
新しくアプリがインストールされた	<input checked="" type="checkbox"/>	x	<input type="checkbox"/>	x	x
指定したアプリがインストールされている	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
指定したアプリがインストールされていない	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

【手順⑨】

レシピを実行する対象の絞り込みを行います。対象の絞り込みは、「デバイスグループ」単位か「デバイス」単位で設定できます。対象を選択後、「選択」をクリックします。



【手順⑩】

「アクション追加」をクリックし、次に表示される画面から「指定プロファイルを配信する」を選択します。



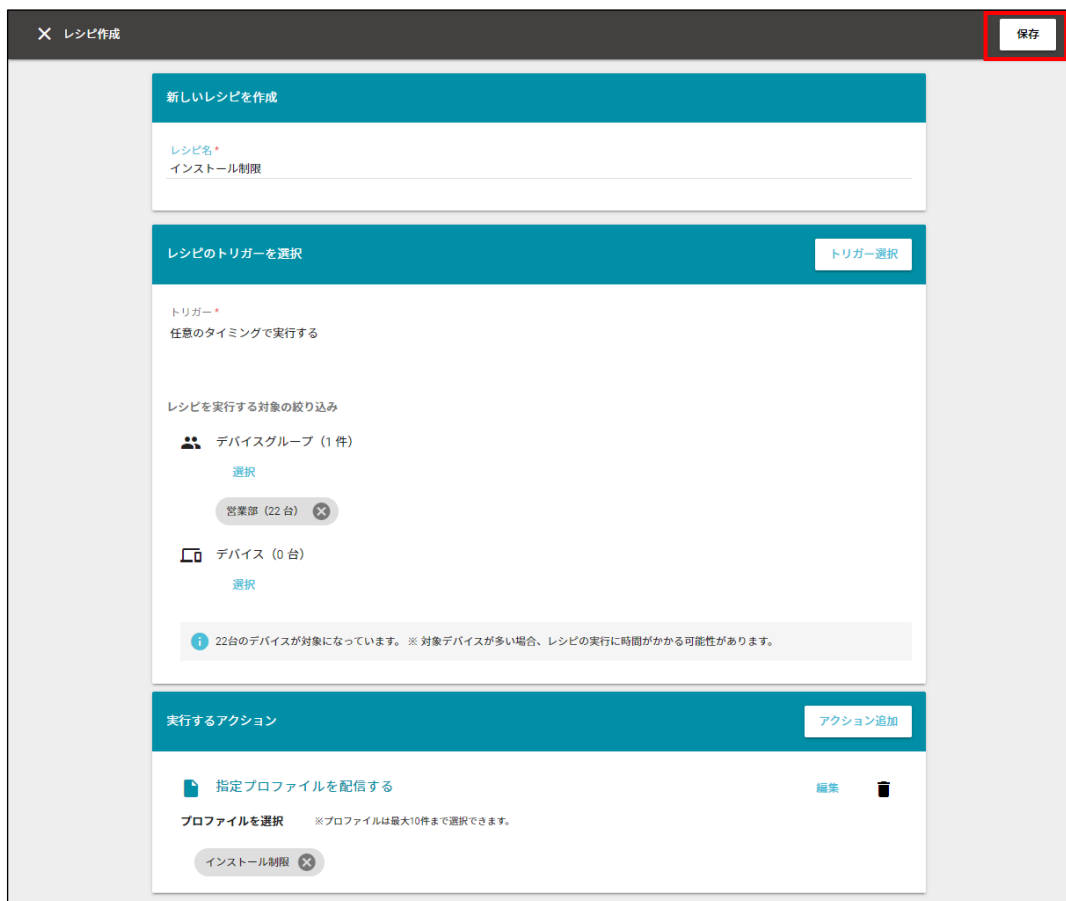
【手順⑪】

作成したプロファイルをチェックし、「選択」をクリックします。（本手順ではインストール制限を選択）



【手順⑫】

「保存」をクリックします。



【手順⑬】

作成したレシピを選択後、「実行アイコン」からレシピを実行します。

状態	レシピ名	トリガー
<input type="checkbox"/>	インストール制限	任意のタイミングで実行する
<input type="checkbox"/>	LANSCOPE登録用Clipを配信する	LANSCOPEクライアントがインストールされた
<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

このレシピを有効にする

**インストール制限**  
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)  
営業部 (22 台)

📌 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。

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  
インストール制限 - 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

レシピを実行します。よろしいですか？

キャンセル OK

「実行状況」を開くと、対象端末への実行状況が確認できます。インストールが完了すると「インストール済み」と表示されます。

このレシピを有効にする

**インストール制限**  
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)  
営業部 (22 台)

📌 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。

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  
インストール制限 **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

管理No.	デバイス管理名	ユーザー名	状態	完了待ち日数	最終実行操作	最終実行日時
2	iPhone		インストール済み		インストール	2022/08/31 13:47:56

## 3-2 チェックリスト 5-1 への対応

### 3-2-1 メーカーサポートの確認

利用する端末の OS やアプリケーションは製品提供元からサポートのあるバージョンを利用します。サポート切れの OS を使用していると不具合や脆弱性が修正されないため、不正アクセスの起点となってしまう恐れがあり、セキュリティ上のリスクとなります。OS のサポート期間については、Apple 社のサイト（※）を確認するか、iOS 端末の取引のある SI ベンダーや代理店に確認してください。

※ Apple サポート公式サイト（<https://support.apple.com/ja-jp>）

ここでは、LANSCOPE を利用して、端末の OS バージョンを確認する方法を記載します。

### OS バージョン確認方法

#### 【手順①】

ホーム画面から「リスト」-「デバイス」をクリックし、エンドポイントマネージャーに登録されているデバイスリストが表示から対象のデバイスをクリックします。

<input type="checkbox"/>	↑ ↓	デバイスグループ	ユーザー名	OSタイプ	OSバージョン	電話番号	LANSCOPE クライアント最終稼働...	デバ
<input type="checkbox"/>	1	総務課	██████	Android	9	090xxxxxxx	2022/10/25 09:30:39	SC-0
<input type="checkbox"/>	2	総務課	██████	Android	10	090xxxxxxx	2022/10/25 09:30:39	hami
<input type="checkbox"/>	3	営業1課	██████	iOS	14.4	080xxxxxxx	2022/10/25 12:32:30	iPhoi
<input type="checkbox"/>	4	人事課	██████	Android	11	080xxxxxxx	2022/10/25 10:17:06	N-04

【手順②】

画面左にある「デバイス情報」をクリックします。、システムの欄に表示されている「OSバージョン」より確認できます。



指定した iOS のバージョン範囲外の時にアラートを上げる方法

【手順①】

ホーム画面から「レシピ」を選択し、「レシピ一覧」から、「レシピの追加」をクリックします。



### 【手順②】

任意のレシピ名を入力後、「トリガーを選択」をクリックし、「iOS」のタブから、「iOS のバージョンが指定した範囲外になっている」を選択します。

The screenshot shows two parts of the interface. On the left, the '新しいレシピを作成' (Create New Recipe) form has 'レシピ名' (Recipe Name) and 'OSバージョン確認' (OS Version Check) highlighted with a red box. Below, the 'レシピのトリガーを選択' (Select Recipe Trigger) section has a 'トリガー選択' (Select Trigger) button highlighted with a red box. On the right, the 'トリガーを選択してください' (Please Select a Trigger) dialog is open, with the 'iOS' tab selected and highlighted with a red box. A table of triggers is shown below, with the row 'iOSのバージョンが指定した範囲外になっている' (iOS version is outside the specified range) highlighted with a red box.

	すべて	iOS	Android	Windows	macOS
指定したアプリがインストールされている	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定したアプリがインストールされていない	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定したアプリが実行された	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
パスワードロックの設定がオフになっている	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
デバイスが不正に改造されている(root化)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
デバイスが不正に改造されている(Jailbreak)	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
<b>iOSのバージョンが指定した範囲外になっている</b>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Androidのバージョンが指定した範囲外になっている	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
SIMカードが抜き差しされた	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SDカードが抜き差しされた	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
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	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

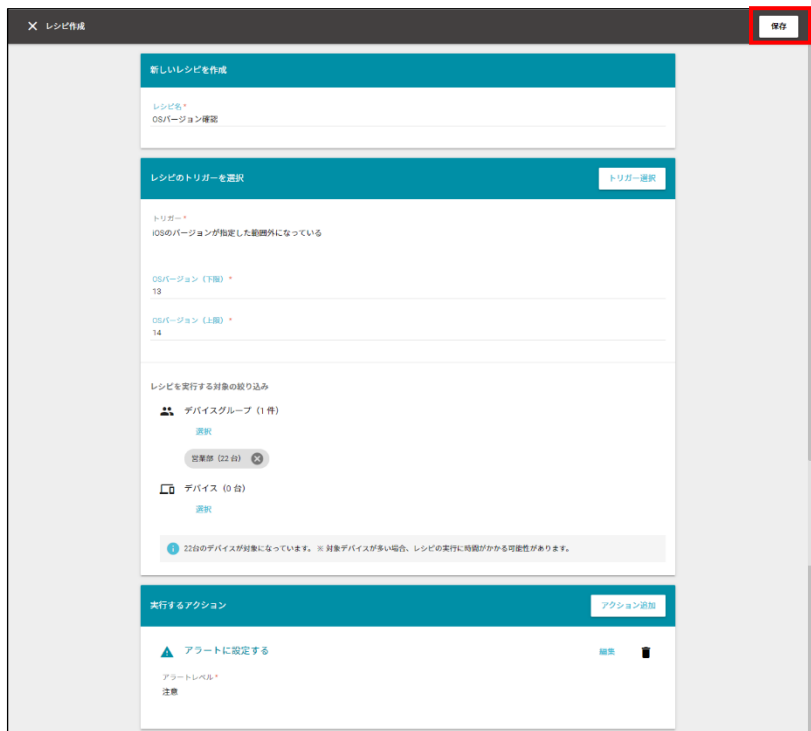
### 【手順③】

OSバージョンの範囲を指定し、「レシピを実行する対象の絞り込み」を設定し、「アクション追加」をクリックします。  
 （下記では、OS のバージョンを 13 から 14 までとし、デバイスグループをレシピの実行対象として設定）

The screenshot shows the '新しいレシピを作成' (Create New Recipe) form. The 'トリガー' (Trigger) is set to 'iOSのバージョンが指定した範囲外になっている' (iOS version is outside the specified range). The 'OSバージョン (下限)' (OS Version (Lower Limit)) is set to 13 and 'OSバージョン (上限)' (OS Version (Upper Limit)) is set to 14, both highlighted with a red box. In the 'レシピを実行する対象の絞り込み' (Filter Recipe Execution Targets) section, 'デバイスグループ (1件)' (Device Group (1 item)) is selected, showing '営業部 (22台)' (Sales Department (22 devices)), highlighted with a red box. The 'アクション追加' (Add Action) button at the bottom right is also highlighted with a red box. A note at the bottom states: '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。' (22 devices are targeted. ※ When the number of target devices is large, it may take time to execute the recipe.)

**【手順④】**

次に、アクションを選択します。ここでは「アラートに設定する」を選択し、アラートレベル（危険/注意/警告なし）を「注意」に設定し、保存します。





【手順⑤】

ホーム画面から「リスト」を選択し、「アラート」から、対象のアラートを確認します。

アラート対象の端末がある場合は、右側に対象端末が表示され、対象端末をクリックするとその端末の詳細画面が開きます。



### 3-3 チェックリスト 8-1 への対応

#### 3-3-1 端末位置の把握

端末の盗難・紛失があった場合に備え、端末の位置情報を検出できるように設定します。端末の位置情報を検出できるように設定することにより、**端末の盗難・紛失時に端末の位置を特定できる可能性が高まり、情報漏洩のリスクを低減することができます。**

端末の位置情報を取得するためには、下記の手順を実施することに加えて、端末側で位置情報を取得する設定を有効にしている必要があります。

#### 位置情報の取得設定

##### 【手順①】

ホーム画面「ルール」から「デバイス設定」を選択し、「基本設定」をクリックします。

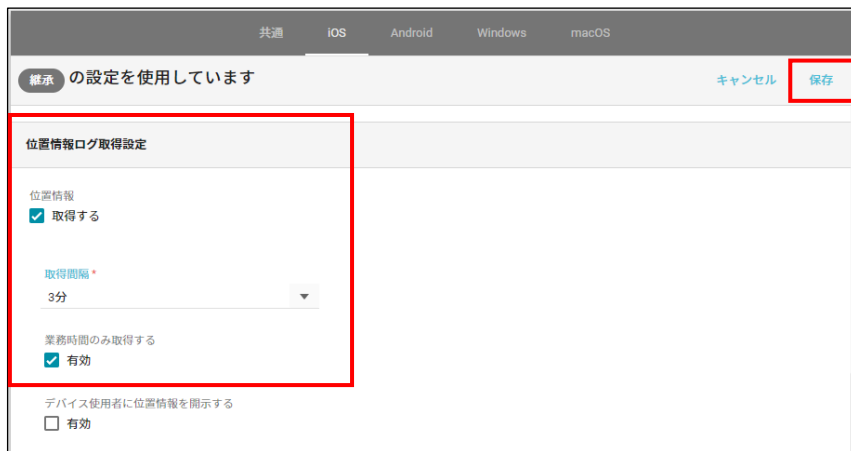


画面左側のデバイスグループから設定を適用するデバイスグループをクリックします。「iOS」をクリックし、右側の「作成」をクリックします。



**【手順②】**

位置情報ログ取得設定欄で、「取得する」にチェックを入れ、取得間隔を指定し、「保存」をクリックします。  
 「業務時間のみ取得する」を有効にした場合は、設定した業務時間内でのみ位置情報を取得します。



業務時間は、同画面の「共通」から「編集」で設定できます。



## 端末位置の確認方法

### 【手順①】

ホーム画面かの「リスト」から、「デバイス」を選択し位置情報を確認したいデバイスをクリックします。

<input type="checkbox"/>	↑...	デバイスグループ	使用者名	OSタイプ	OSバージョン	電話番号
<input type="checkbox"/>	7	営業1課	██████████	Android	10	080xxxxxxxx
<input type="checkbox"/>	8	営業1課	██████████	Android	11	090xxxxxxxx
<input type="checkbox"/>	9	総務課	██████████	iOS	14.4	080xxxxxxxx
<input type="checkbox"/>	10	営業1課	██████████	iOS	13.2	080xxxxxxxx

### 【手順②】

画面左にある「位置情報」を選択後、画面右のマップにて位置情報を確認できます。

## 3-4 チェックリスト 8-2 への対応

### 3-4-1 リモートロック・リモートワイプの実行

端末の紛失・盗難があった場合、遠隔操作で端末のロック（リモートロック）や端末のデータを初期化（リモートワイプ）をすることができます。**紛失・盗難時に端末のリモートロックやリモートワイプを行うことで、第三者に不正操作されるリスクを低減**します。

#### エンドポイントマネージャーからのリモートロック実行

例えば、端末を紛失し、一時的に利用不可としたい場合は、リモートロックを実行します。

#### 【手順①】

ホーム画面から「リスト」を選択し、「デバイス」を選択します。

選択後、エンドポイントマネージャーに登録されているデバイスリストが表示されるので、対象のデバイスをクリックします。

	↑ ↓	デバイスグループ	使用者名	OSタイプ	OSバージョン	電話番号
<input type="checkbox"/>	1	総務課	██████	Android	9	090xxxxxxxx
<input type="checkbox"/>	2	総務課	██████	Android	10	090xxxxxxxx
<input type="checkbox"/>	3	営業1課	██████	iOS	14.4	080xxxxxxxx

【手順②】

画面左にある「リモート操作」を選択後、「リモート操作を実行する」をクリックし、「リモートロックを実行」をクリックします。



【手順③】

「実行」をクリックします。これにより対象端末がロックされます。必要に応じてメッセージや連絡先の電話番号を入力することもできます。

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

注意事項

キャンセル 実行

## エンドポイントマネージャーからのリモートワイプ実行

### 【手順①】

ホーム画面から「リスト」を選択し、「デバイス」を選択します。

選択後、エンドポイントマネージャーに登録されているデバイスリストが表示されるので、対象のデバイスをクリックします。

デバイス	アプリ	プロフィール	アラート			
ネットワーク全体 ▼ iOS Android Windows macOS						
デバイスの追加 インストール待ちデバイス						
<input type="checkbox"/>	↑ ↓	デバイスグループ	使用人名	OSタイプ	OSバージョン	電話番号
<input type="checkbox"/>	1	総務課	██████	Android	9	090xxxxxxx
<input type="checkbox"/>	2	総務課	██████	Android	10	090xxxxxxx
<input type="checkbox"/>	3	営業1課	██████	iOS	14.4	080xxxxxxx

### 【手順②】

画面左にある「リモート操作」を選択後、「リモート操作を実行する」をクリックし、「リモートワイプを実行」をクリックします。

- 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

リモートワイプを実行

設定日時 20███ 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 20███ 15:38:12  
 詳細 デバイスをロックしまし

リモートロック:リジェクト  
 20███ 16:56:46 に実行さ

リモートワイプ:成功  
 20███ 16:45:55 に実行さ

リモートワイプ:成功  
 20███ 16:45:55 に実行さ

【手順③】

「リモートワイプの実行」画面でログインパスワードを入力し、「実行」をクリックします。これにより、対象端末のデータが初期化されます。

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。

確認のためログインパスワードを入力してください。

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



## 3-5 チェックリスト 9-1 への対応

### 3-5-1 iOS 端末のパスワードポリシー設定とアラート設定

管理者はパスワードポリシーを設定することにより、強度の高いパスワード設定をユーザーに要求できます。**これにより、強度の低いパスワードが使用されるリスクを低減することができます。**

#### パスワードポリシー設定

##### 【手順①】

ホーム画面から「ルール」から「デバイス設定」を選択し、「基本設定」をクリックします。

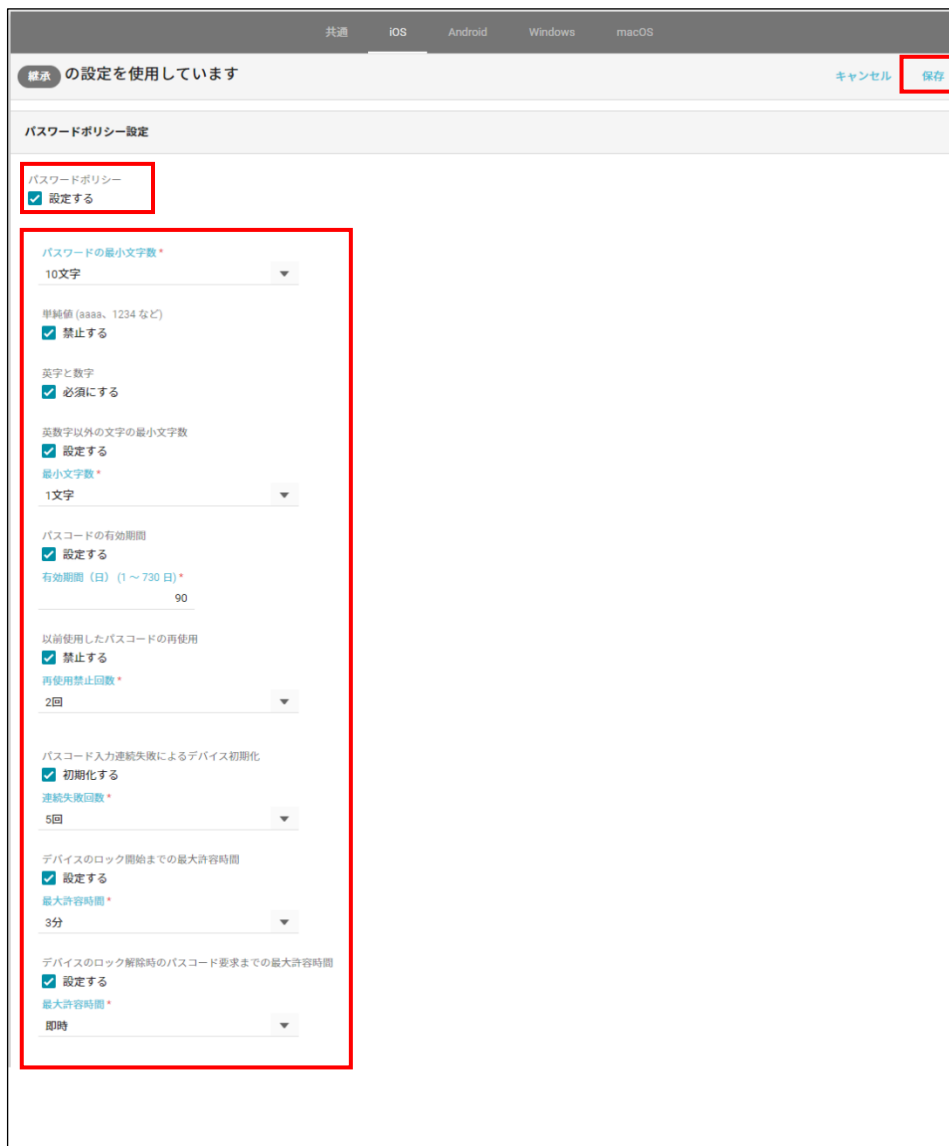


画面左側のデバイスグループから設定を適用するデバイスグループをクリックします。「iOS」をクリックし、右側の「作成」をクリックします。



【手順②】

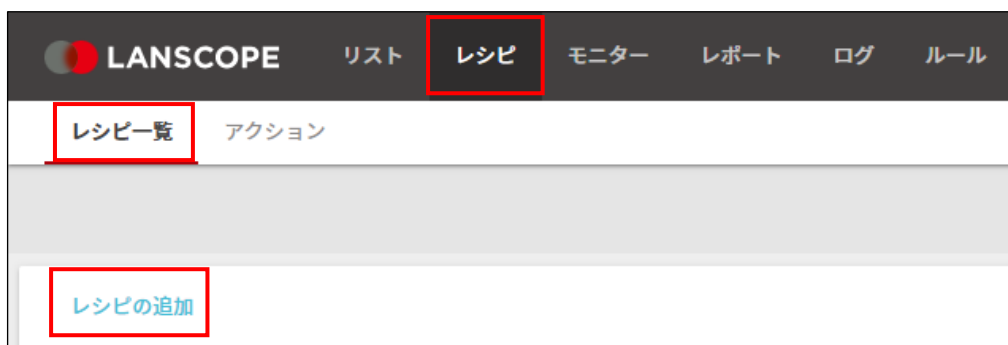
パスワードポリシー設定欄で、「パスワードポリシー」の「設定する」にチェックを入れ、ポリシーを設定し、「保存」をクリックします。



パスワードポリシーに準拠していない端末のアラート設定

【手順①】

ホーム画面から「レシピ」を選択し、「レシピ一覧」から、「レシピの追加」をクリックします。



**【手順②】**

任意のレシピ名を入力し、「トリガーを選択」をクリックし、「パスワードポリシーに準拠していない」を選択します。

The right screenshot shows a table of triggers with the following data:

	iOS	Android	Windows	macOS
リモートロックの実行が成功した	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
LANSCOPE クライアントがインストールされた	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
パスワードポリシーに準拠していない	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
デバイスが管理外になっている	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
LANSCOPE Client のバージョンが最新になっていない	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
任意のタイミングで実行する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
定期的に行う	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
未稼働期間が指定された期間を超過している	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定したアプリがインストールされている	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定したアプリがインストールされていない	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
パスコードロックの設定がオフになっている	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
デバイスが不正に改造されている(Jailbreak)	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
iOSのバージョンが指定した範囲外になっている	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

**【手順③】**

レシピを実行する対象の絞り込みを設定し、「アクション追加」をクリックします。

The screenshot shows the '新しいレシピを作成' screen with the following details:

- レシピ名: パスワードポリシー準拠確認
- トリガー: パスワードポリシーに準拠していない
- 絞り込み:
  - デバイスグループ (1件): 営業部 (22台)
  - デバイス (0台)
- メッセージ: 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。
- アクション追加ボタン

【手順④】

アクションを選択します。ここでは「アラートに設定する」を選択し、アラートレベルを「注意」で設定し、保存しています。



【手順⑤】

ホーム画面から「リスト」を選択し、「アラート」から、対象のアラートと対象端末の台数を確認できます。  
アラート台数がある場合は、対象アラートを選択すると、右側に対象端末が確認できます。

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		
<input type="checkbox"/> 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	位置情報が取得されない設定になっている	3 台
● 危険	iOSのバージョンが指定した範囲外になっている	0 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	0 台
● 危険	SDカードが抜き差しされた	0 台
● 危険	SIMカードが抜き差しされた	0 台
● 危険	タイムゾーンが変更された	0 台
● 注意	未稼働期間が指定された期間を超過している	11 台
● 注意	空き容量が不足している	3 台
● 注意	パスコードロックの設定がオフになっている	0 台
● 注意	パスワードポリシーに準拠していない	0 台

## 3-6 チェックリスト 9-2 への対応

### 3-6-1 エンドポイントマネージャーのログインパスワード変更

初期パスワードは、誰が把握しているかわからないので、速やかにパスワード要件を満たすものに変更することで、**悪意のある第三者から不正アクセスされるリスクを低減します。**

#### 【手順①】

画面右上のログインアカウント隣の「▼」をクリックし、「パスワード変更」をクリックします。



#### 【手順②】

現在のパスワードを入力し、新しいパスワードを入力後、「保存」をクリックします。




## 3-7 チェックリスト 10-1 への対応

### 3-7-1 エンドポイントマネージャーの管理者権限の付与

管理者権限を付与するユーザーを限定することで、本製品の設定変更をできるユーザーを必要最小限に抑え、**悪意のあるユーザーにより、意図しない設定変更が行われるリスクを低減することができます。** エンドポイントマネージャーを利用するユーザーを追加する場合は、利用できる機能権限（ロール）を制限したうえで追加することを推奨します。

エンドポイントマネージャーのデフォルトのロールは、全機能権限を持つシステム管理者のみとなります。以下の手順で、使用者の目的に応じたロールを作成してユーザーに割り当てることができます。

#### 【手順①】

画面右上の「」をクリックし、「システム管理」をクリックします。



画面左側のメニューから「ロール」を選択し、「ロールの追加」をクリックします。



【手順②】

任意のロール名を入力し、付与したい機能権限を選択後、「追加」をクリックします。

以下の画面はロールとして、ログやアラートの確認のみができるロール「資産管理担当者用」を追加しています。

### ロールの追加

ロール名\*

資産管理担当者用

すべてチェック    すべてははずす

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・パスワ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)
- Windows / macOSの使用状況を確認できる
- 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

キャンセル
追加


作成後、ロールの一覧に作成したロールが追加されます。

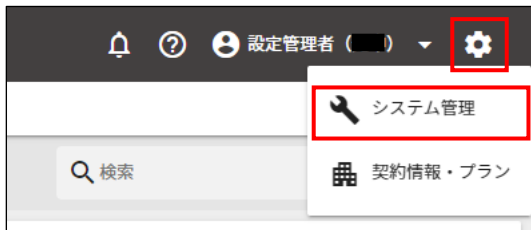
←
システムメニュー

	ロールの追加	
	ロール名	機能権限
<input type="checkbox"/>	システム管理者	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
<input type="checkbox"/>	資産管理担当者用	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



【手順③】

画面右上の  をクリックし、「システム管理」をクリックします。



画面左側のメニューから「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。



【手順④】

「ロール」から「選択」をクリックします。

アカウントの追加

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\*

営業

ロール\*

選択

パスワード\*

半角英字1文字以上、半角数字1文字以上を含んでください。  
半角英数記号8～15文字以下で入力してください。  
パスワードはメールアドレスと異なる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

キャンセル 追加

「ロールを選択」画面で追加したロールをチェックし、「選択」をクリックします。

以下の画面は、【手順②】で追加した「資産管理担当者用」を選択しています。

全権限を付与したいユーザーの場合は、「システム管理者」を選択します。

ロールを選択

× 1件を選択中

選択

<input type="checkbox"/>	ロール名	機能権限
<input type="checkbox"/>	システム管理者	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
<input checked="" type="checkbox"/>	資産管理担当者用	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

【手順⑤】

「ロール」に選択したロールが追加されます。次に、メールアドレスや表示名、パスワードを入力し、アクセス許可するネットワークを選択後、「追加」をクリックします。これによりユーザーが使用できる権限を限定することができます。

### アカウントの追加

**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\***

test

**ロール\***

選択

資産管理担当者用 ×

**パスワード\***

.....

半角英字 1 文字以上、半角数字 1 文字以上を含んでください。  
半角英数記号 8 ~ 15 文字以下で入力してください。  
パスワードはメールアドレスと異なる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

キャンセル 追加

## ロールの変更

### 【手順①】

既存ユーザーをシステム管理者から変更する場合は、アカウント一覧から対象ユーザーをクリックし、「編集」をクリックします。



## 【手順②】

「選択」をクリックし、変更するロールにチェックを入れ、「選択」をクリックします。

The screenshot shows the 'アカウント詳細' (Account Details) page for a user named '営業 ( )' (Employee). The 'ロール' (Role) field is set to '資産管理担当者用' (Asset Management User). A red box highlights the '選択' (Select) button next to the role field. To the right, a 'ロールを選択' (Select Role) dialog is open, showing a table of roles with 'システム管理者' (System Administrator) selected. A red box highlights the '選択' (Select) button in the dialog's top right corner.

ロール名	機能権限
<input checked="" type="checkbox"/> システム管理者	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
<input type="checkbox"/> 資産管理担当者用	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

「保存」をクリックします。これによりアカウントのロールが変更され、アカウントの権限が変更されます。

The screenshot shows the 'アカウント詳細' (Account Details) page after the role has been changed to 'システム管理者' (System Administrator). A red box highlights the '保存' (Save) button in the top right corner of the page.

## 3-8 チェックリスト 10-2 への対応

### 3-8-1 エンドポイントマネージャーのログインパスワード強度

パスワード強度が弱いパスワードを使用した場合、パスワードが解読され、不正アクセスを受けるおそれがあります。そのため、適切なパスワードを設定することが重要です。設定するパスワードは「[中小企業等向けテレワークセキュリティの手引き](#)」の P.96 に記載の「パスワード強度」を参考に設定することを推奨します。

## 3-9 チェックリスト 10-3 への対応

### 3-9-1 エンドポイントマネージャーの管理者権限の管理

作業ミスによるシステムやデータへの悪影響を防ぐために、**一般ユーザーのアカウントを作成し、普段はそのアカウントを利用、管理者用アカウントの利用は最小限に留める**ことを推奨します。