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~）

Ver1.2（2025.03）

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
URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

目次

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）を利用しての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。（2024 年 11 月 5 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「ライト A」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様に提供するものであり、明示であると黙示であることを問わず、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うものではありません。本資料に掲載されている情報は、2024 年 11 月 5 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
2-4 マルウェア対策 **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。**	・アプリケーションの制限	P.5
5-1 脆弱性管理 **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。**	・メーカーサポートの確認	P.13
8-1 データ保護 **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。**	・端末位置の把握	P.18
8-2 データ保護 **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。**	・リモートロック・リモートワイプの実行	P.21
9-1 アカウント・認証管理 **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。**	・iOS 端末のパスワードポリシー設定とアラート設定	P.25
9-2 アカウント・認証管理 **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。**	・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	P.30
10-1 特権管理 **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。**	・エンドポイントマネージャーの管理者権限の付与	P.31
10-2 特権管理 **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。**	・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	P.37
10-3 特権管理 **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。**	・エンドポイントマネージャーの管理者権限の管理	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】

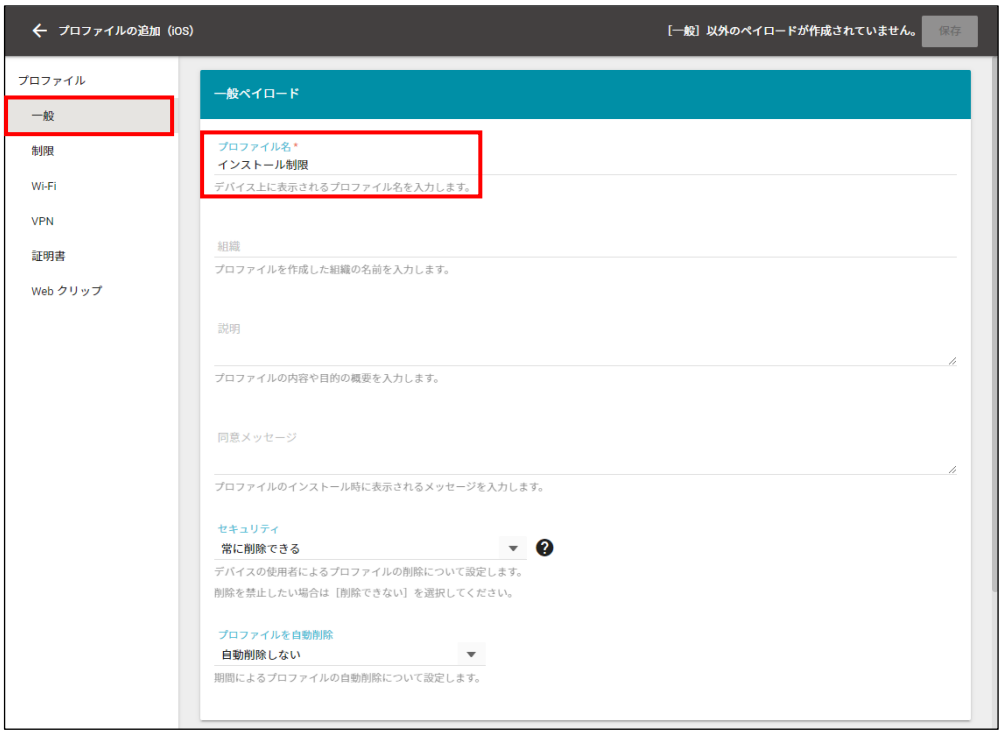
ホーム画面から「レシピ」を選択し、「アクション」を選択後、「プロファイルを設定する」をクリックします。

【手順②】

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

【手順③】

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



【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）

【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】

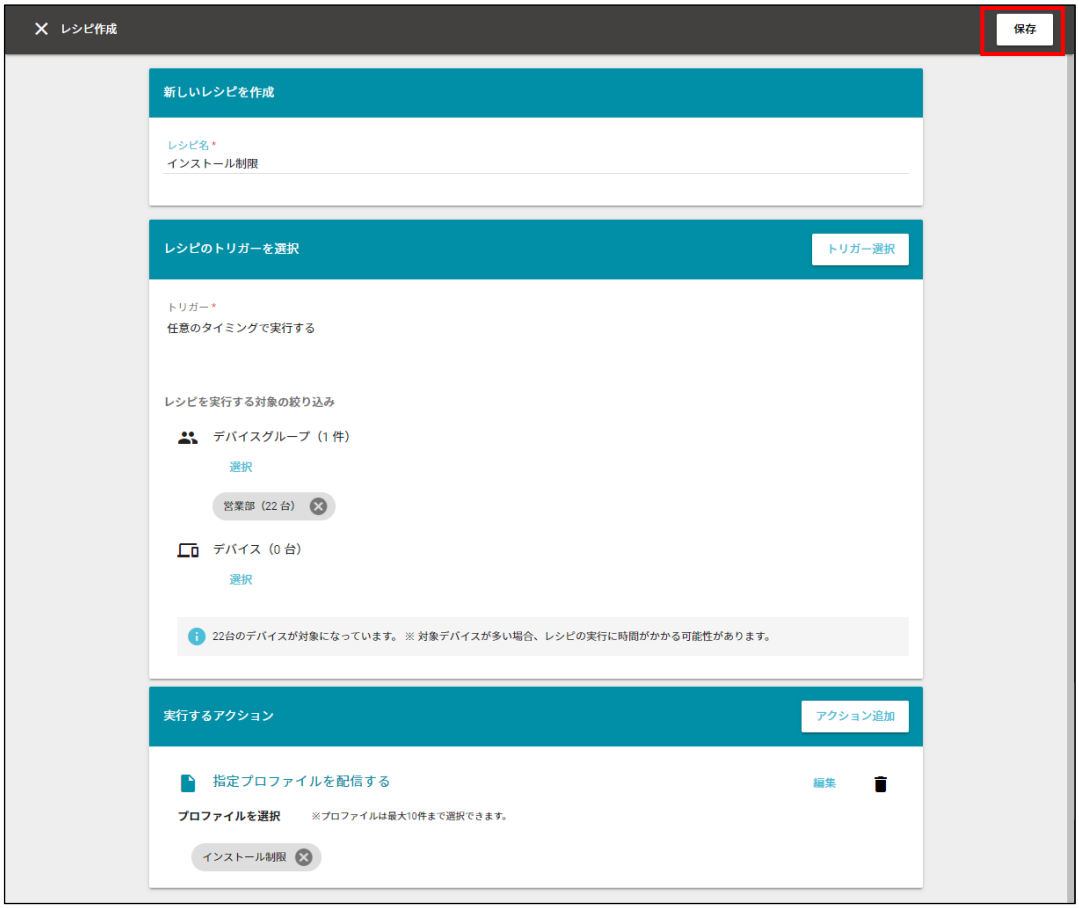
「アクション追加」をクリックし、次に表示される画面から「指定プロファイルを配信する」を選択します。

【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）

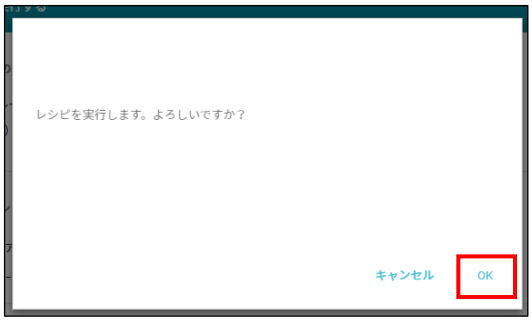
【手順⑫】

「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。



「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。

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。

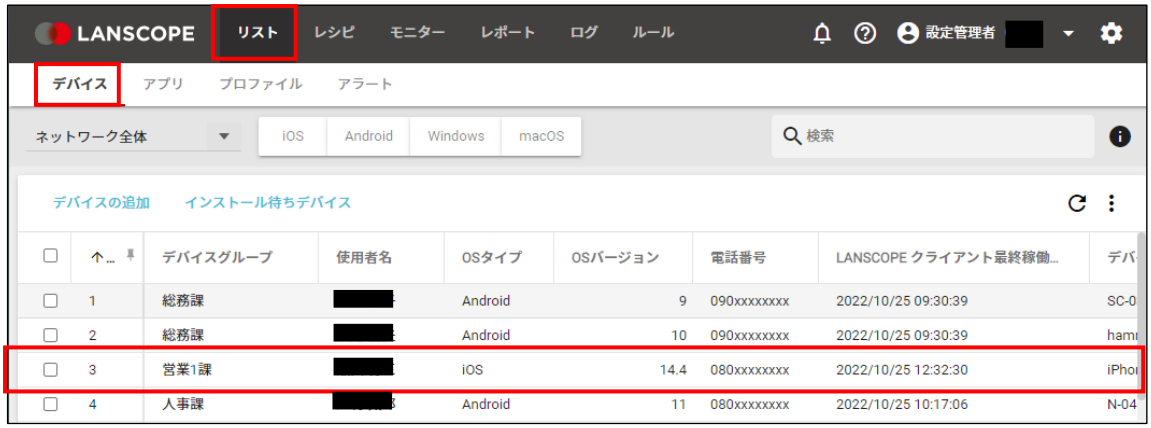
※ Apple サポート公式サイト（https://support.apple.com/ja-jp）

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。



【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。

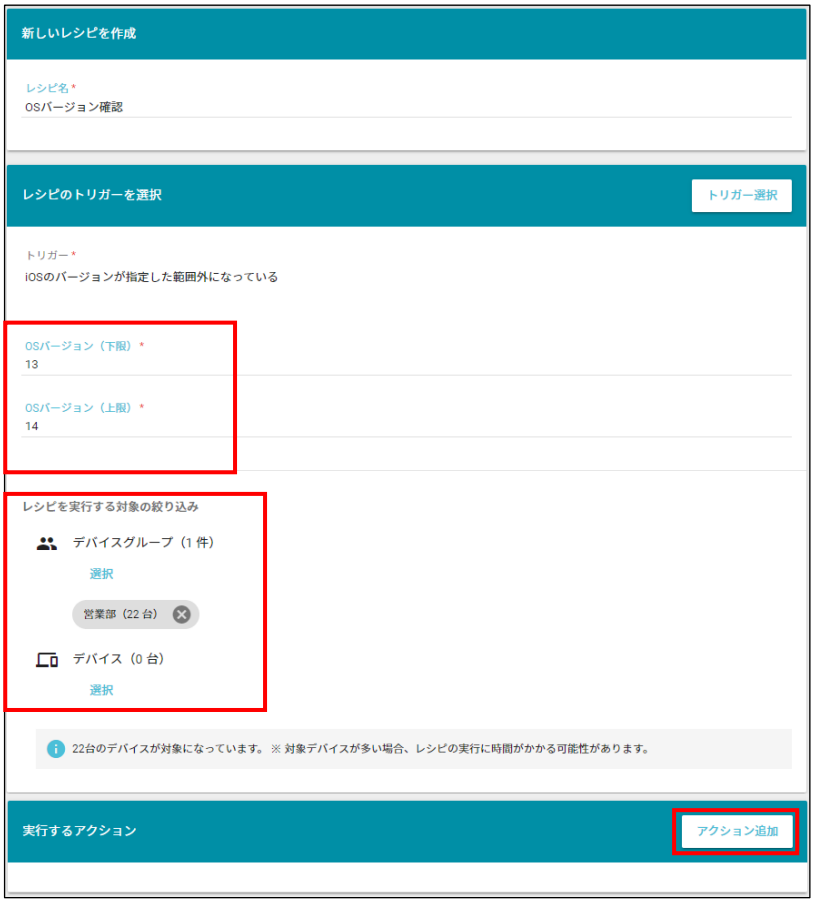
【手順②】

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。

【手順③】

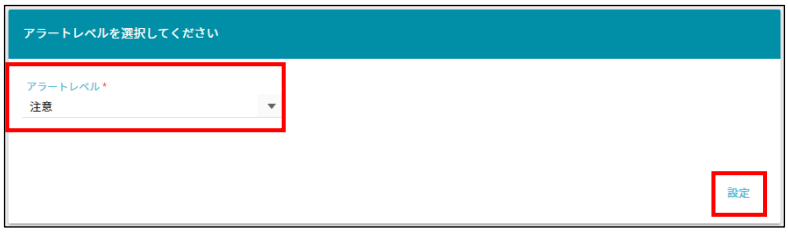
OS バージョンの範囲を指定し、「レシピを実行する対象の絞り込み」を設定し、「アクション追加」をクリックします。

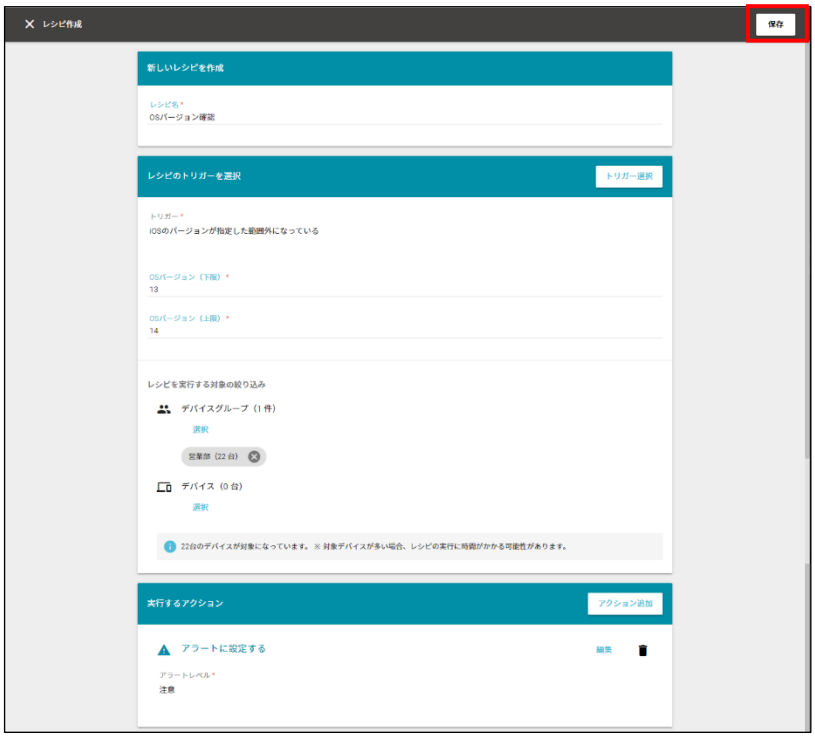
（下記では、OS のバージョンを 13 から 14 までとし、デバイスグループをレシピの実行対象として設定）



【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】

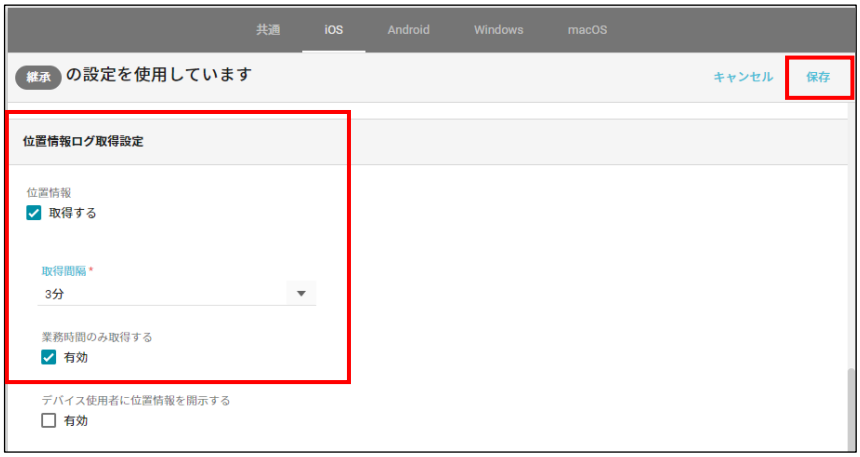
ホーム画面「ルール」から「デバイス設定」を選択し、「基本設定」をクリックします。

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。

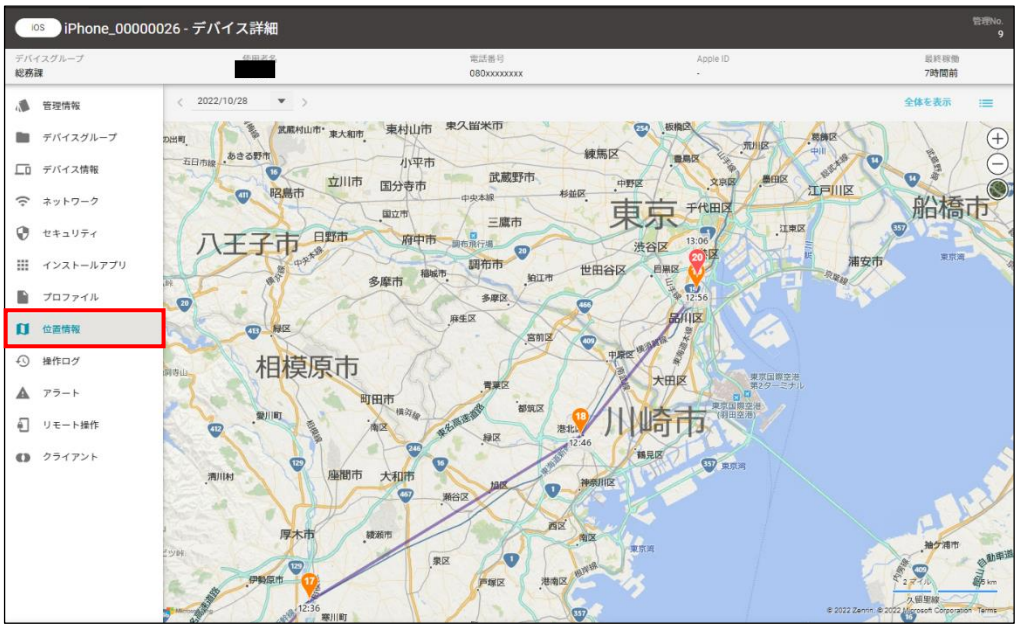
端末位置の確認方法

【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。

【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。

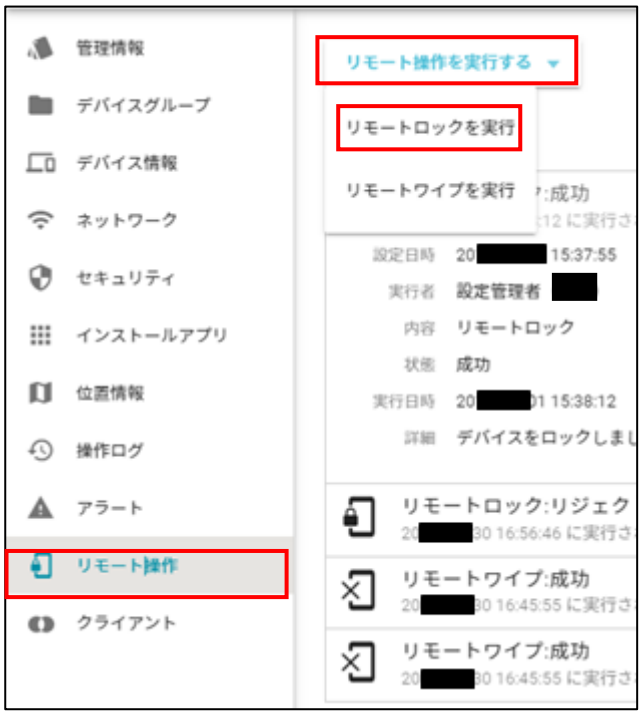
【手順①】

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。

【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。

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

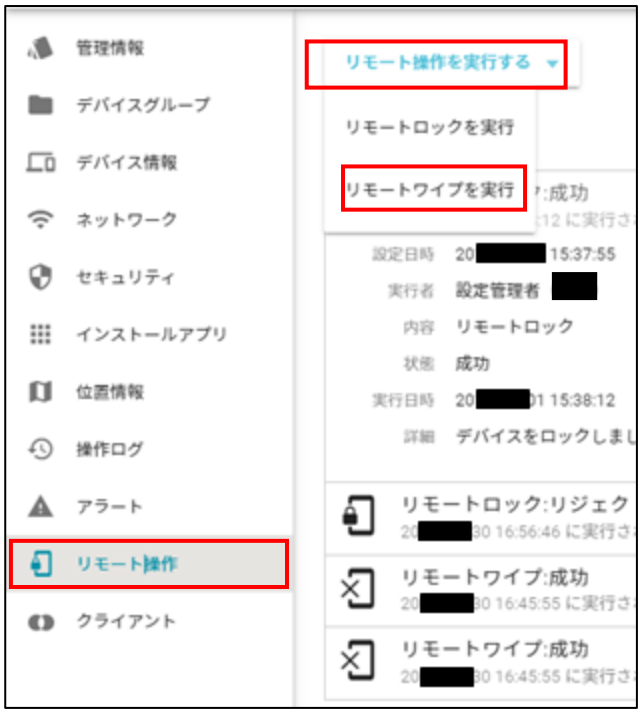
【手順①】

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。

【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。



【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。

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

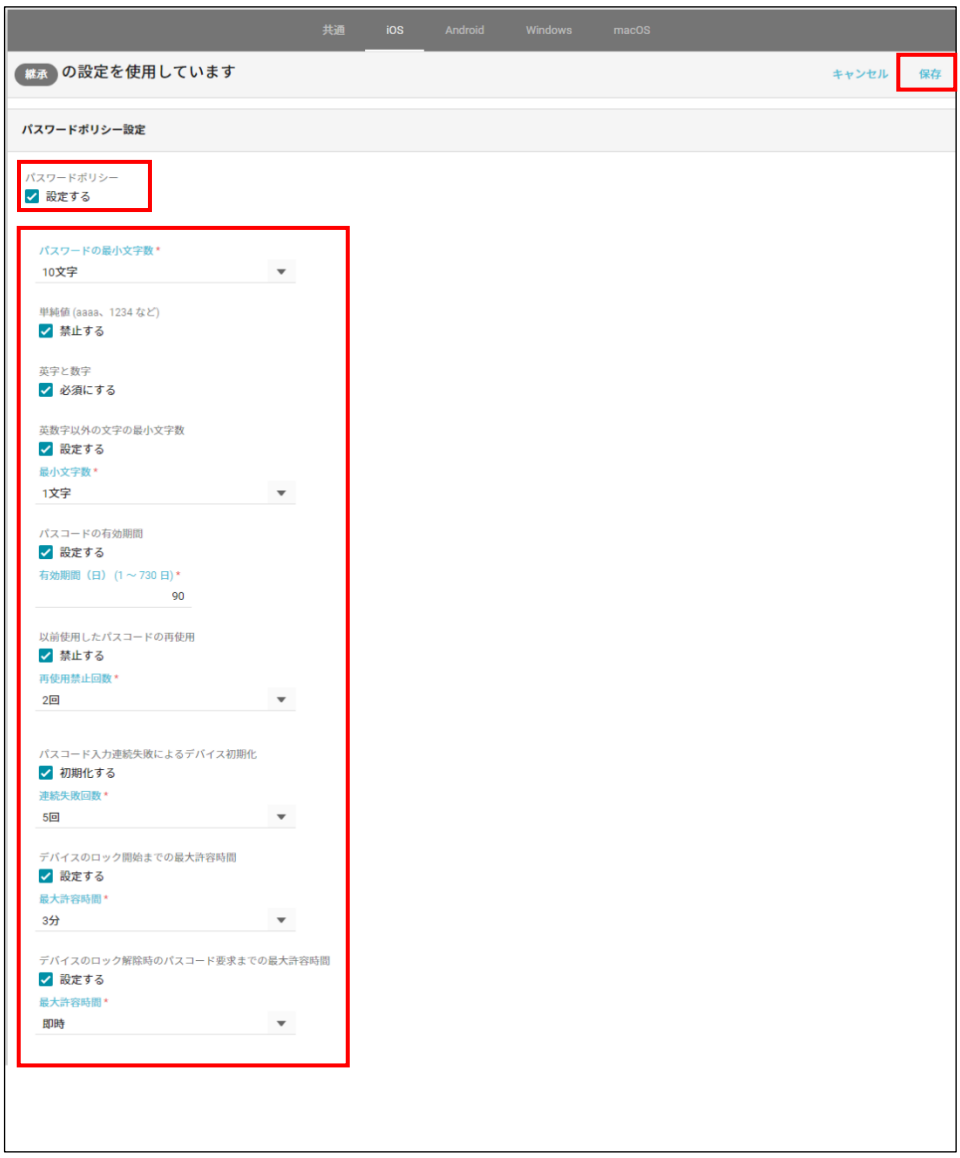
【手順①】

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】

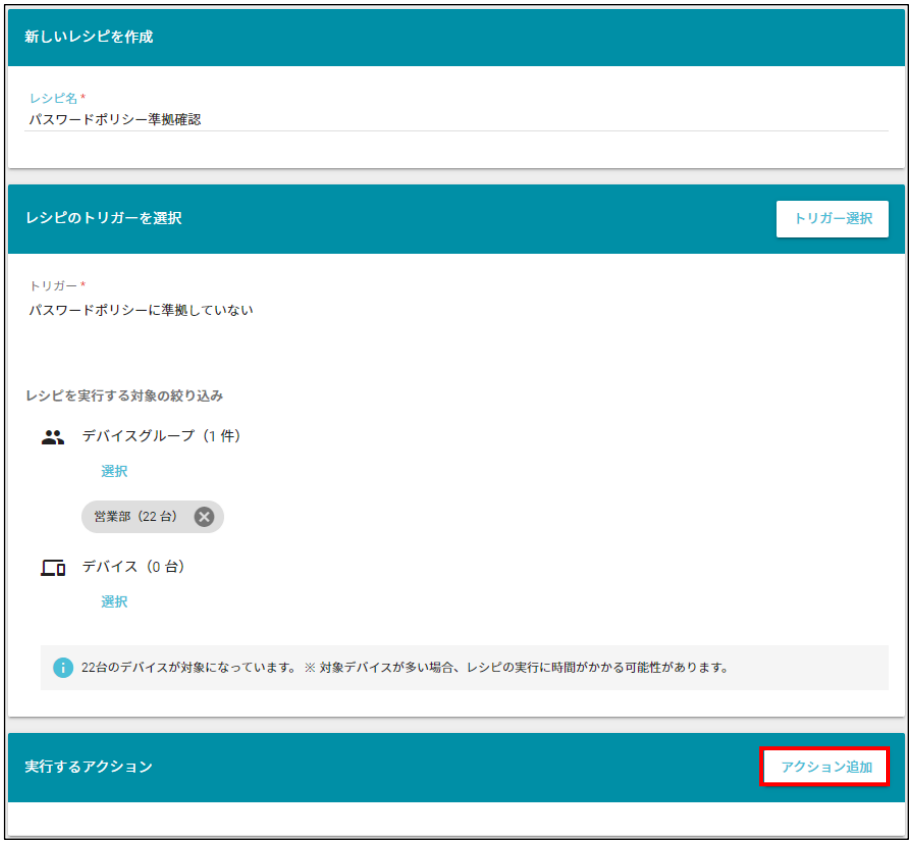
ホーム画面から「レシピ」を選択し、「レシピ一覧」から、「レシピの追加」をクリックします。

【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。

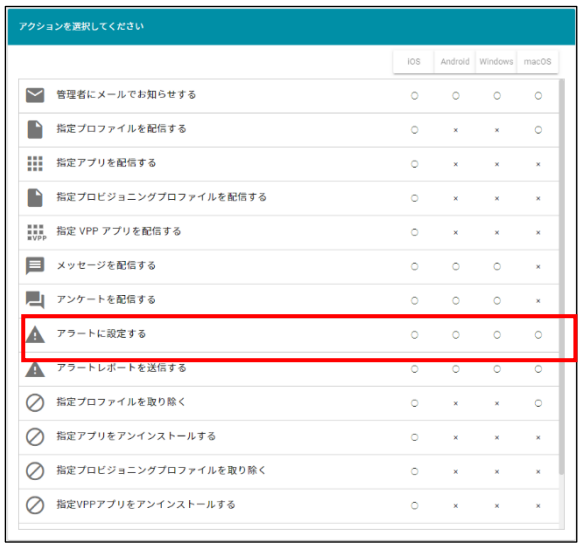
【手順③】

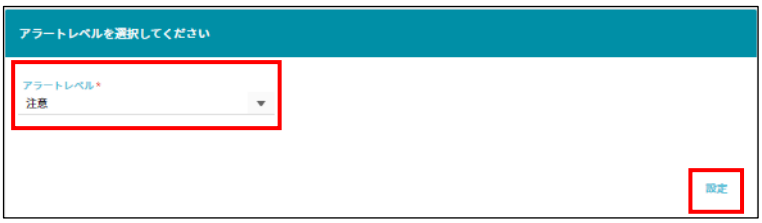
レシピを実行する対象の絞り込みを設定し、「アクション追加」をクリックします。



【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。

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、「アカウント管理」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。

作成後、ロールの一覧に作成したロールが追加されます。

【手順③】

画面右上の  をクリックし、「アカウント管理」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。

「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。

【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。

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。

「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。

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。

【謝辞】

本設定解説資料の策定及び更新を行うにあたっては、エムオーテックス株式会社の関係各所の方々に多大なるご協力をいただきました。この場をお借りして深く御礼申し上げます。