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 ~macOS~）

**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
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。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。**（2022 年 11 月 1 日現在）

(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、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 |
|---|---|---|
| **5-1 脆弱性管理**<br>**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.5 |
| **8-2 データ保護**<br>**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.6 |
| **8-3 データ保護**<br>**テレワーク端末の盗難・紛失時に情報が漏えいしないよう、端末に内蔵されたハードディスクやフラッシュメモリ等の記録媒体の暗号化を実施する。ただし、端末に会社のデータを保管しない場合を除く。** | ・端末のディスクの暗号化状態の確認 | P.9 |
| **9-2 アカウント・認証管理**<br>**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.11 |
| **10-1 特権管理**<br>**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.12 |
| **10-2 特権管理**<br>**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.18 |
| **10-3 特権管理**<br>**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.18 |

# 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や注意事項を記載します。

## 3-1　チェックリスト 5-1 への対応

### 3-1-1　メーカーサポートの確認

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、不正アクセスや HDD 内データを破壊されるなどの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 社の公式 HP（※）を確認するか、macOS 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」を選択後、システムの欄の OS バージョンにより確認できます。


## 3-2　チェックリスト 8-2 への対応

### 3-2-1　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。

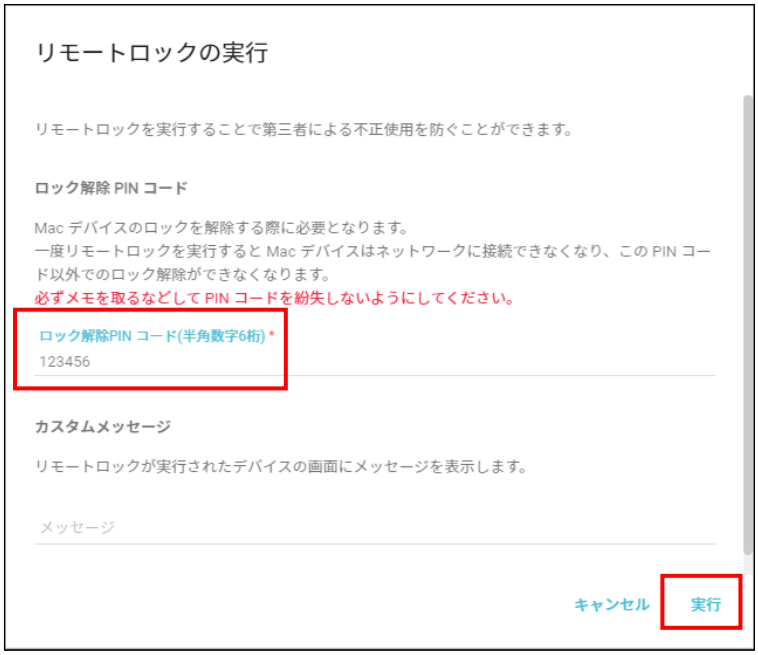
選択後、エンドポイントマネージャーに登録されているデバイスリストが表示されるので、対象のデバイスをクリックします。

**【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】**

ロック解除用の任意の PIN コード（半角数字 6 桁）を入力して、「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使用できなくます。



## 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、ロック解除用の任意の PIN コードとログインパスワードを入力し、「実行」します。

これにより、対象端末のデータが初期化されます。


## 3-3　チェックリスト 8-3 への対応

### 3-3-1　　端末のディスクの暗号化状態の確認

macOS 端末の紛失・盗難があった場合に備え、端末のハードディスクが暗号化されているか確認します。

**【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】**

「セキュリティ」の項目の「File Vault」が ON になっていることを確認します。ON と表示されていれば、ハードディスクが暗号化されています。ON と表示されていない場合は、「設定解説書（macOS）」を参考に、対象の端末で File Vault を有効にしてください。

## 3-4　チェックリスト 9-2 への対応

### 3-4-1　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「▼」をクリックして、「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し、「保存」をクリックします。

# 3-5　チェックリスト 10-1 への対応

## 3-5-1　　エンドポイントマネージャーの管理者権限の付与

システム管理者の権限を付与するユーザーを限定することで、エンドポイントマネージャーの設定変更をできるユーザーを必要最小限に抑えます。これにより、**悪意のあるユーザーからの意図しない設定変更の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としては、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  をクリックして、「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」の「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。

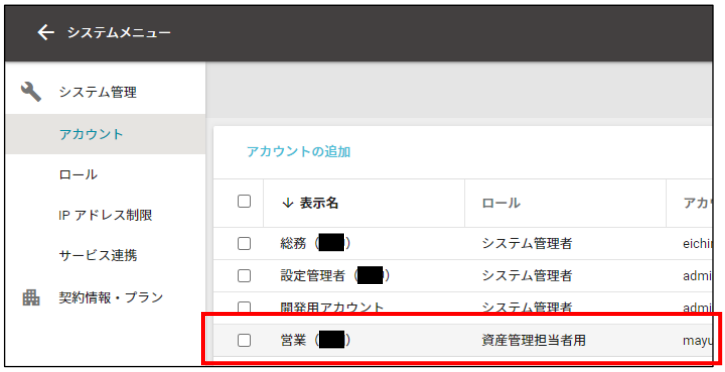
**【手順⑤】**

「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。


## 3-6　チェックリスト 10-2 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。

## 3-7　チェックリスト 10-3 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。