

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 ～Windows～）

Ver1.1 (2024.03)

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	3
2	チェックリスト項目に対応する設定作業一覧	4
3	管理者向け設定作業	5
3-1	チェックリスト 5-1 への対応	5
3-1-1	メーカーサポートの確認.....	5
3-2	チェックリスト 8-1 への対応	6
3-2-1	端末位置の把握.....	6
3-3	チェックリスト 8-2 への対応	13
3-3-1	リモートロック・リモートワイプの実行	13
3-4	チェックリスト 8-3 への対応	16
3-4-1	端末暗号化状態の確認.....	16
3-5	チェックリスト 9-2 への対応	17
3-5-1	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	17
3-6	チェックリスト 10-1 への対応	18
3-6-1	エンドポイントマネージャーの管理者権限の付与	18
3-7	チェックリスト 10-2 への対応	24
3-7-1	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	24
3-8	チェックリスト 10-3 への対応	24
3-8-1	エンドポイントマネージャーの管理者権限の管理.....	24

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。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。**（2023 年 11 月 7 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、2023 年 11 月 7 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	対応する設定作業解説	ページ
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。	<ul style="list-style-type: none"> ・ メーカーサポートの確認 	P.5
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。	<ul style="list-style-type: none"> ・ 端末位置の把握 	P.6
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。	<ul style="list-style-type: none"> ・ リモートロック・リモートワイプの実行 	P.13
8-3 データ保護 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。	<ul style="list-style-type: none"> ・ 端末暗号化状態の確認 	P.16
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。	<ul style="list-style-type: none"> ・ 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.17
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。	<ul style="list-style-type: none"> ・ エンドポイントマネージャーの管理者権限の付与 	P.18
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。	<ul style="list-style-type: none"> ・ エンドポイントマネージャーのログインパスワード 	P.24
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。	<ul style="list-style-type: none"> ・ エンドポイントマネージャーの管理者権限の管理 	P.24

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、本製品の利用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

利用する端末の OS 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、Microsoft 社のサイト（※）を確認するか、Windows OS 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。

※ Microsoft ライフサイクルポリシー（<https://docs.microsoft.com/ja-jp/lifecycle/>）

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

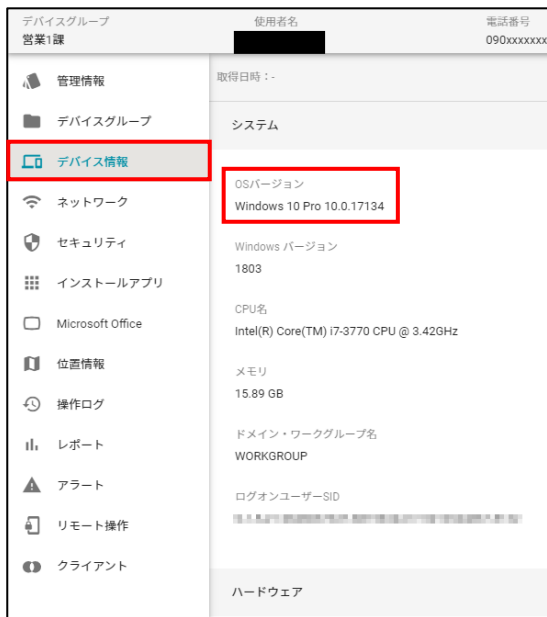
【手順①】

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から対象のデバイスをクリックします。

	↑ ...	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
<input type="checkbox"/>	10	営業1課	██████	iOS	13.2	080xxxxxxx
<input type="checkbox"/>	11	営業1課	██████	Windows	Windows 10 Pro ...	090xxxxxxx
<input type="checkbox"/>	12	営業1課	██████	Windows	Windows 10 Pro ...	090xxxxxxx

【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。



3-2 チェックリスト 8-1 への対応

3-2-1 端末位置の把握

端末の盗難・紛失に備えて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、**紛失・盗難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。



【手順②】

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。「Windows」をクリックし、右側の「作成」をクリックします。



【手順③】

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のみ情報を取得します。



業務時間は、「共通」から編集で設定できます。



端末位置の確認方法

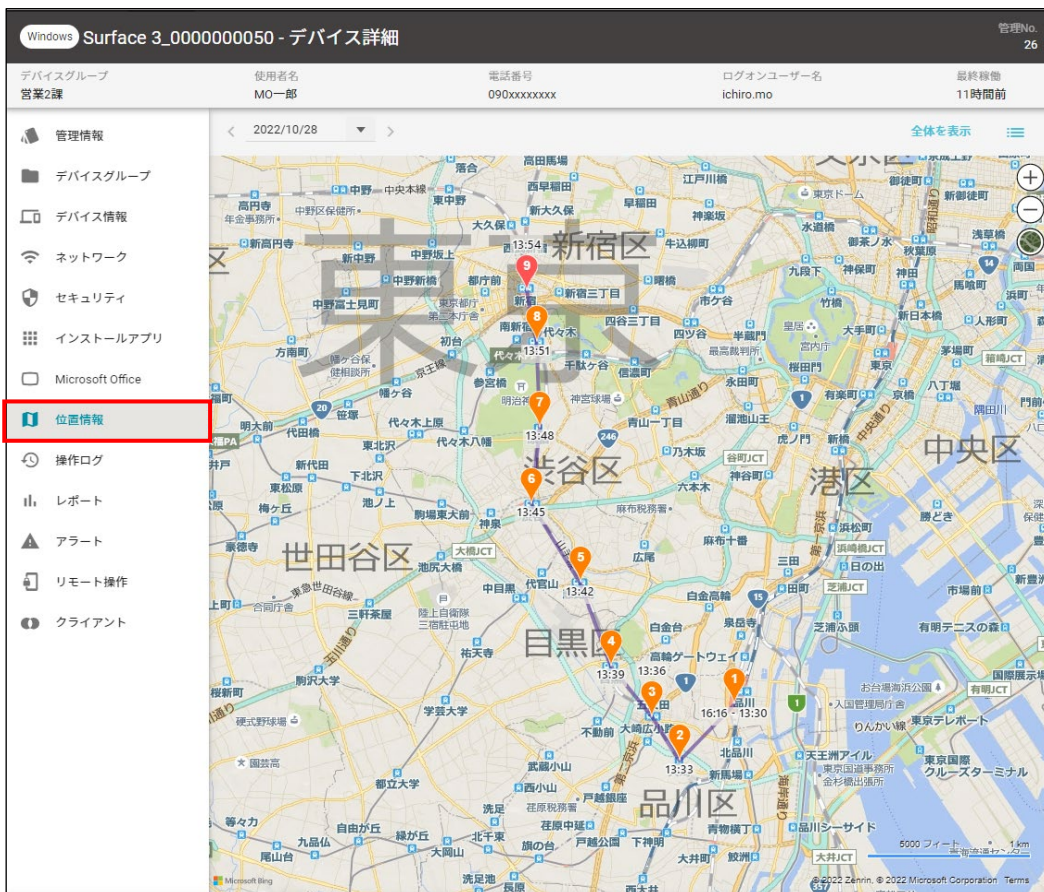
【手順①】

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現在の位置情報を確認できます。



位置情報が取得されない設定の場合の検知

【手順①】

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



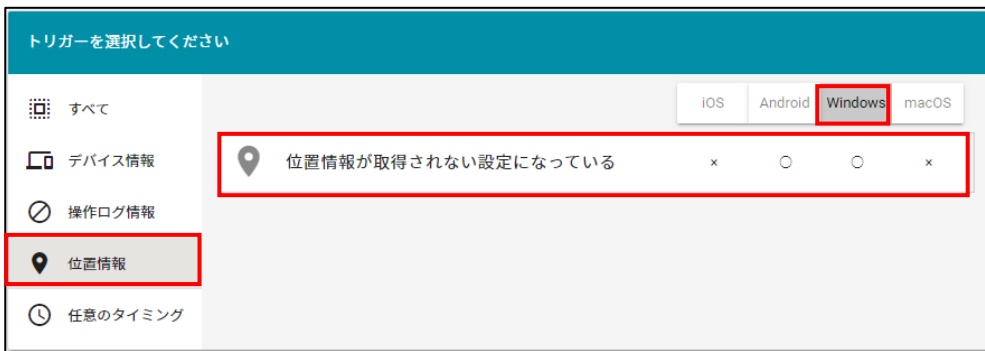
【手順②】

レシピ名に新規にレシピを作成する際の名前を任意で入力後、「トリガー選択」をクリックします。



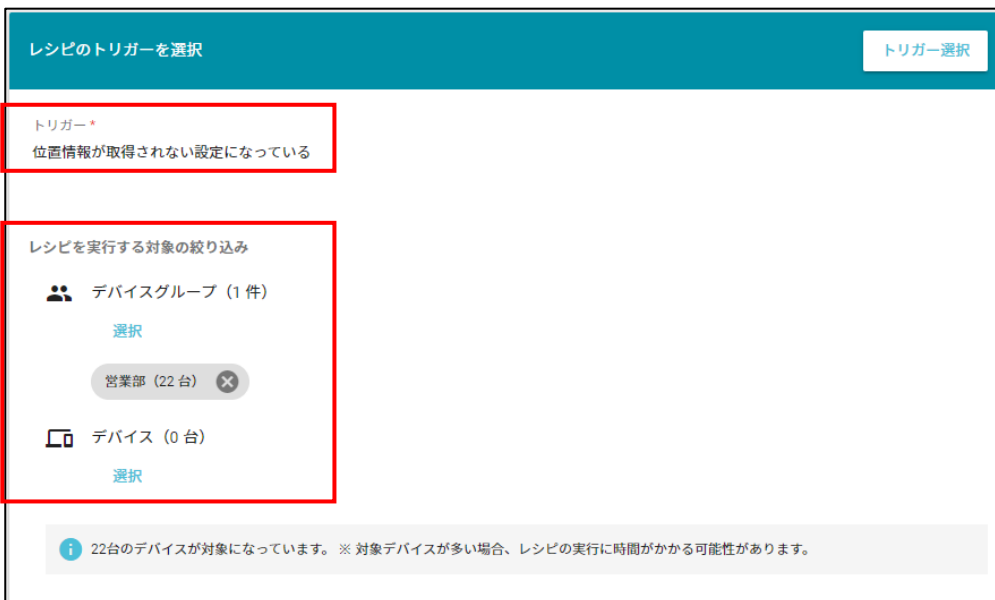
【手順③】

「位置情報」を選択し、画面左の端末を「Windows」にフィルター後、「位置情報が取得されない設定になっている」をクリックします。



【手順④】

トリガーが選択されているかを確認後、対象のデバイスグループもしくはデバイスを選択します。



【手順⑤】

画面下の「アクション追加」からアラートレベルを設定し、「保存」をクリックします。



3-3 チェックリスト 8-2 への対応

3-3-1 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】

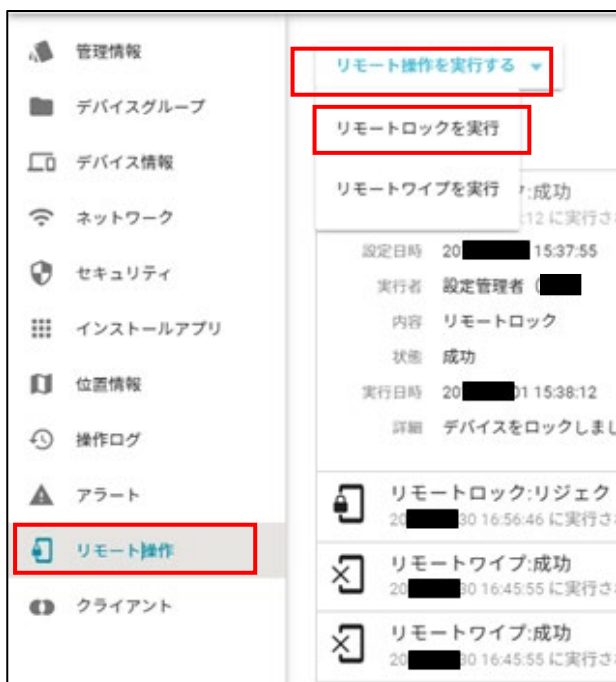
ホーム画面から「リスト」を選択し、「デバイス」を選択します。

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。



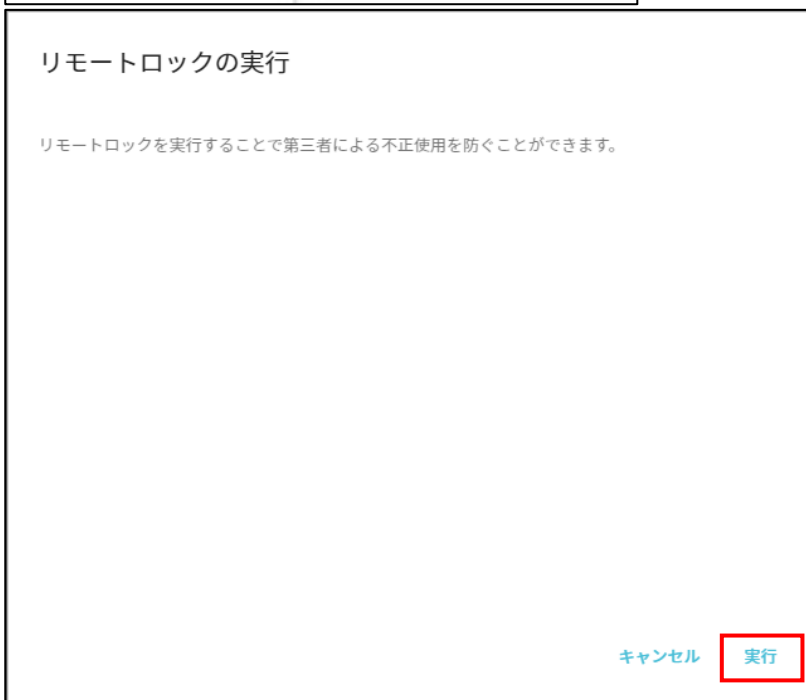
【手順②】

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】

「リモートロックの実行」画面で、「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なります。



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

※ BitLocker を使用した暗号化が無効な場合、リモートワイプの実行はできません。その場合、[端末暗号化状態の確認](#)をしてください。

【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。

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。

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*

キャンセル
実行

3-4 チェックリスト 8-3 への対応

3-4-1 端末暗号化状態の確認

Windows 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。暗号化されていなかった場合は、設定解説書資料（Windows）を参考に、有効化します。

【手順①】

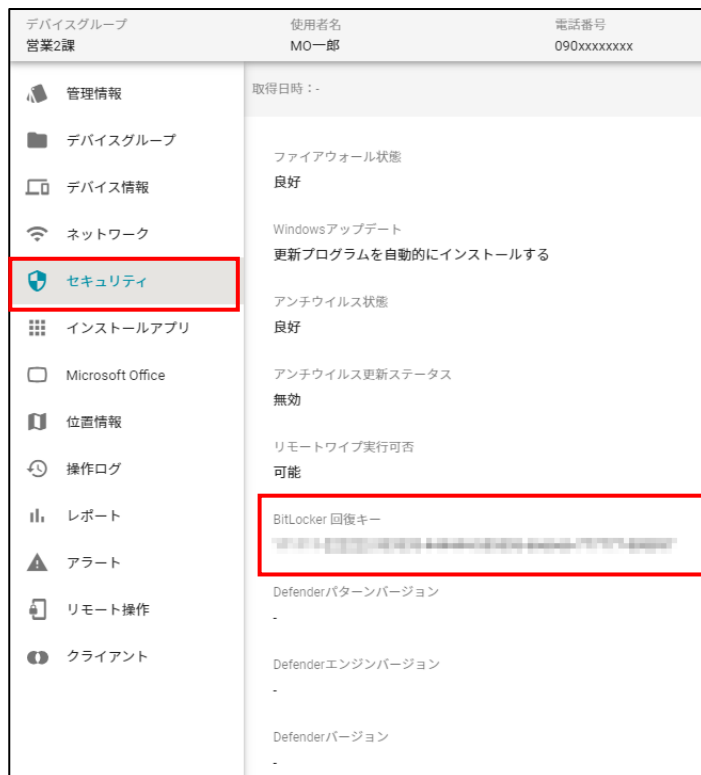
ホーム画面から「リスト」を選択し、「デバイス」を選択します。

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"/>	24	営業2課	MO花子	Windows	Windows 10 Pro ...	
<input type="checkbox"/>	25	営業2課	MO二郎	Windows	Windows 10 Pro ...	
<input type="checkbox"/>	26	営業2課	MO一郎	Windows	Windows 10 Pro ...	090xxxxxxx

【手順②】

「セキュリティ」の項目の「BitLocker 回復キー」に 48 桁の回復キーが表示されていることを確認します。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。表示されていない場合「設定解説資料（Windows）」を参考に、対象の端末で BitLocker を有効にしてください。



3-5 チェックリスト 9-2 への対応

3-5-1 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。

設定管理者 () (admin@xxxxxx.co.jp)

基本情報

パスワード

現在のパスワード *

新しいパスワード *

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。

新しいパスワード確認用 *

閉じる


3-6 チェックリスト 10-1 への対応

3-6-1 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。

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)
- 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											
<ul style="list-style-type: none"> アカウント管理 アカウント <li style="background-color: #eee;">ロール 操作履歴 	<p>ロールの追加</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 5%;"></th> <th style="width: 30%;">ロール名</th> <th style="width: 65%;">機能権限</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>システム管理者</td> <td>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</td> </tr> <tr style="border: 2px solid red;"> <td style="text-align: center;"><input type="checkbox"/></td> <td>資産管理担当者用</td> <td>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</td> </tr> </tbody> </table>		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
	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  をクリックして、「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」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。

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. The 'ロール' (Role) field is set to 'システム管理者' (System Administrator). A red box highlights the '選択' (Select) button. To the right, a modal window titled 'ロールを選択' (Select Role) is displayed, showing a table of roles. The 'システム管理者' role is selected, and its '選択' button is highlighted in red.

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 selection. The '保存' (Save) button is highlighted in red, indicating the final step of the process.

3-7 チェックリスト 10-2 への対応

3-7-1 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。

3-8 チェックリスト 10-3 への対応

3-8-1 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。