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
（たよれーる DMS ~Windows~）

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、たよれーる DMS を利用しての具体的な作業内容の解説をすることで、管理者が実施すべき設定作業や利用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「基本サービス」と「オプションサービス」が存在します。（2022 年 11 月 1 日現在）**本資料では「基本サービス」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
2-1 マルウェア対策 **テレワーク端末にウイルス対策ソフトをインストールし、リアルタイムスキャンを有効にする。ウイルス対策ソフトの定義ファイルを自動更新する設定にするか、手動で更新するルールを作成する。**	・Windows Defender の設定	P.6
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.9
4-2 物理セキュリティ **テレワーク端末から離れる際には、スクリーンロックをかけるよう周知する。**	・スクリーンロックの設定	P.11
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.12
7-3 インシデント対応・ログ管理 **テレワーク端末からオフィスネットワークに接続する際のアクセスログを収集する。**	・ポータルへのアクセス	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.14
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.17
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。**	・端末の暗号化	P.22
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。**	・たよれーる DMS のログインパスワード変更	P.23

チェックリスト項目	対応する設定作業	ページ
9-3 アカウント･認証管理 **テレワーク端末やテレワークで利用する各システムに対して一定回数以上パスワードを誤入力した場合、それ以上のパスワード入力を受け付けないよう設定する。**	・たよれーる DMS のアカウントロック回数の設定	P.24
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。**	・たよれーる DMS の管理者権限の付与	P.25
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。**	・たよれーる DMS のログインパスワードポリシーの	P.27
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。**	・たよれーる DMS の管理者権限の管理	P.28

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 2-1 への対応

3-1-1　Windows Defender の設定

Windows Defender を有効化することで、**マルウェアや疑わしいアプリケーションから PC を保護します。**

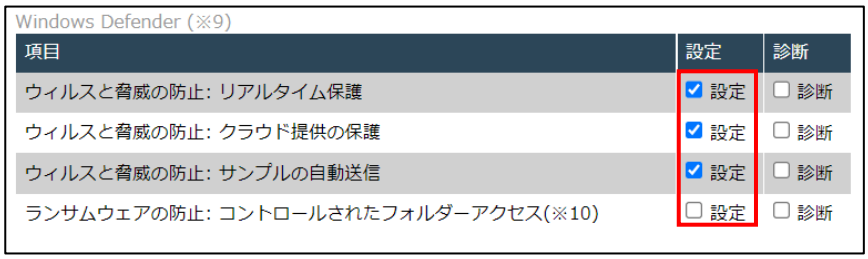
Defender 設定の強制

【手順①】

たよれーる DMS ポータルから「設定」-「Windows」-「システムセキュリティ」を選択し「＋」ボタンから設定セットを新規作成します（既にシステムセキュリティの設定ファイルを作成している場合は設定ファイル名を選択します）。

【手順②】

Defender の設定で有効化したい項目にチェックを付けます。



＜参考＞各項目の説明

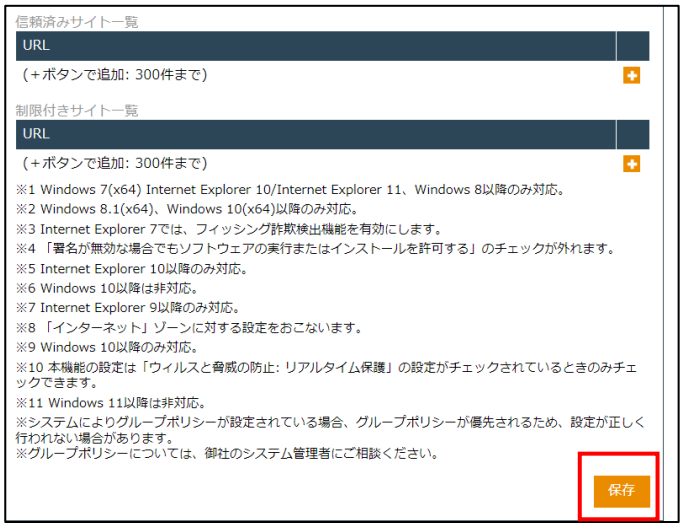
- リアルタイム保護・・・マルウェアなどがインストールまたは実行されそうな場合に、利用者に警告メッセージを表示します。
- クラウド提供の保護・・・Microsoft のクラウド上で新たに発見された脅威情報をリアルタイムに PC に反映します。
- サンプルの自動送信・・・Microsoft 社による分析のため、端末上にあるログを Microsoft 社のクラウドに送信します。
- コントロールされたフォルダーアクセス・・・登録したアプリケーション以外は、登録したフォルダーにアクセスできなくなります。万が一パソコンにランサムウェアが侵入しても、データを暗号化される被害を阻止することができます。利用には事前の設定が必要なため下記 URL を参考に設定してください。

【参考】フォルダーへのアクセス制御で重要なフォルダーを保護する

URL: https://learn.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide

【手順③】

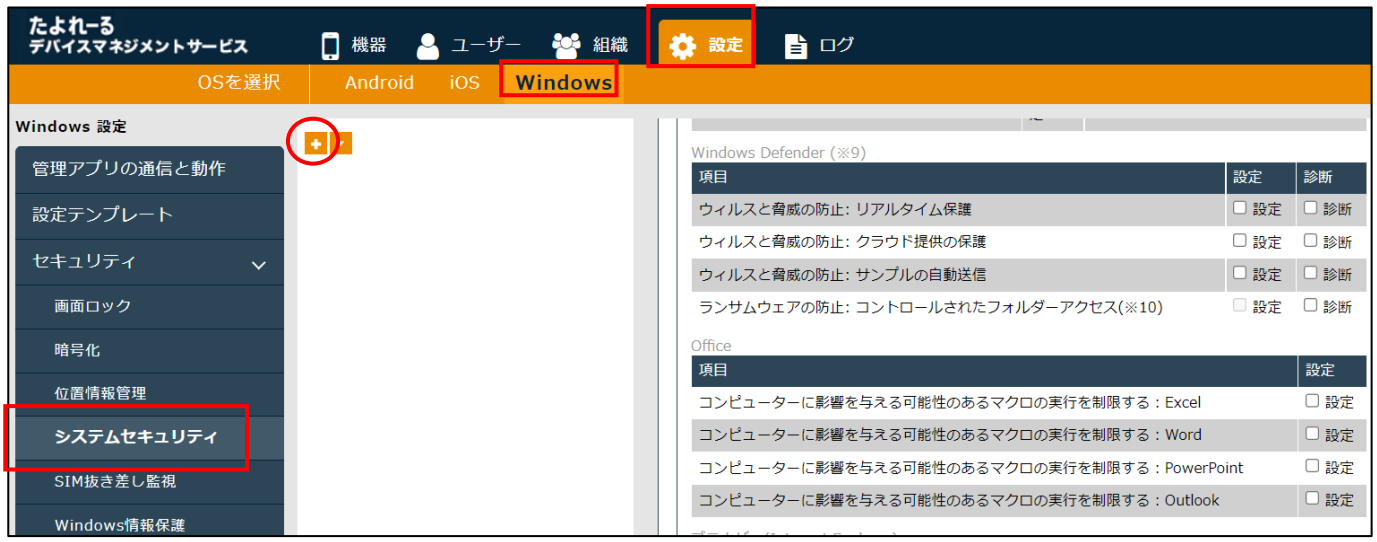
最後に最下部の保存をクリックします。



WindowsUpdate の設定

【手順①】

ポータルのトップ画面から「設定」-「Windows」-「システムセキュリティ」から「＋」ボタンを押し、設定セットを新規作成します（既にシステムセキュリティの設定ファイルを作成している場合は設定ファイル名を選択します）。



【手順②】

「システムセキュリティ」と「Windows Update」の下記項目の「設定」にチェックを入れます。

適用を開始する時刻などの「値」は PC の利用条件によって数値を適宜更新します。

【手順③】

最下部の「保存」をクリックします。

3-2　チェックリスト 2-4 への対応

3-2-1　アプリケーションの制限

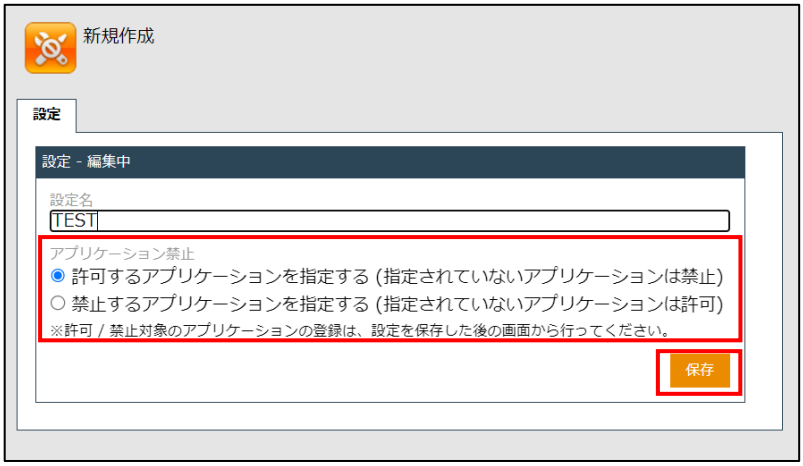
利用可能なアプリケーションを業務上必用なものに限定することで、不審なアプリケーションが実行されるリスクを低減することができます。

【手順①】

「設定」-「Windows」-「アプリケーション」-「アプリケーション禁止」から「＋」ボタンで新規作成を選択します。

【手順②】

設定名を入力し、「許可するアプリケーションを指定する」、または、「禁止するアプリケーションを指定する」を選択し「保存」をクリックします。



【手順③】

対象とするアプリケーションの条件を入力し、チェックをクリックします。

3-3　チェックリスト 4-2 への対応

3-3-1　　スクリーンロックの設定

端末のスクリーンロックを設定することにより、**端末紛失時やのぞき見による情報漏えいのリスクを低減します**。この手順と合わせて、各端末のパスワード設定は必ず行ってください。

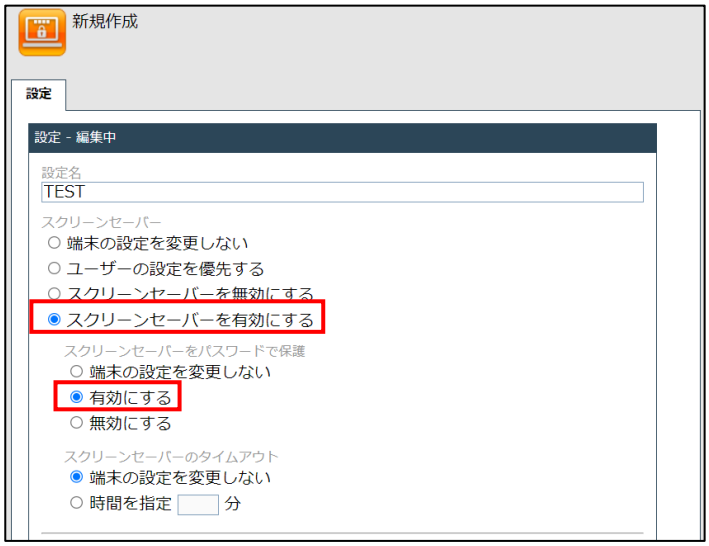
スクリーンセーバーの有効化

【手順①】

「設定」-「Windows」-「セキュリティ」から画面ロックを選択し「＋」ボタンから新規作成を選択します。

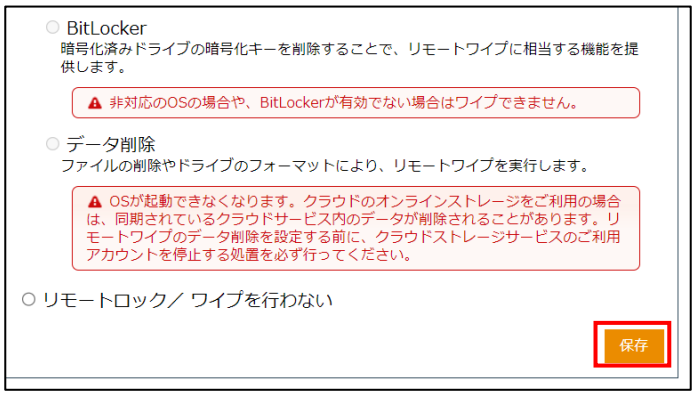
【手順②】

設定名を入力し「スクリーンセーバーを有効にする」にチェックを入れ、「スクリーンセーバーをパスワードで保護」の項目を「有効にする」を選択します。



【手順③】

最下部にある「保存」をクリックします。



3-4　チェックリスト 5-1 への対応

3-4-1　　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。

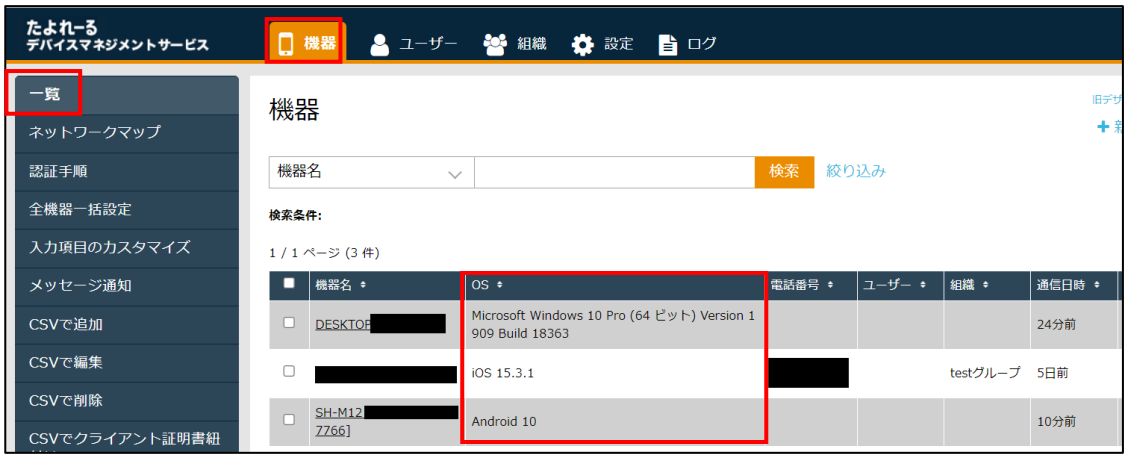
※　Microsoft ライフサイクルポリシー（https://docs.microsoft.com/ja-jp/lifecycle/）

ここでは、たよれーる DMS 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

「機器」-「一覧」を選択から、たよれーる DMS がインストールされた機器の一覧を表示します。

各機器の「OS」に表示されたバージョンから、各機器の OS のバージョンを確認することができます。



3-5　チェックリスト 7-3 への対応

3-5-1　　ポータルへのアクセスの確認

ポータルへのアクセスログを定期的に確認し、不審なユーザーがたよれーる DMS にログインしていないか確認します。

ログの確認方法

ポータルの「ログ」から各ログを確認することができます。

3-6　チェックリスト 8-1 への対応

3-6-1　　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。

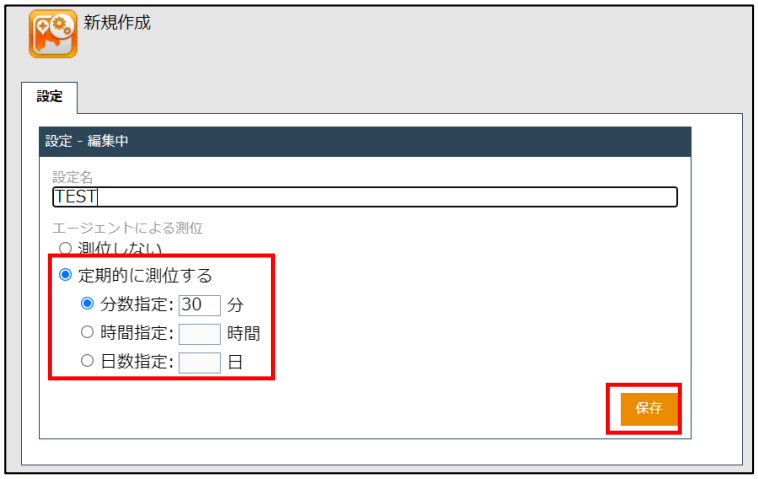
位置情報の取得設定

【手順①】

たよれーる DMS ホーム画面から「設定」-「Windows」-「セキュリティ」-「位置情報管理」を選択、「＋」ボタンをクリックし、設定セットを作成します。

【手順②】

「エージェントによる測位」の選択肢のうち「定期的に測位する」にチェックを入れ、取得間隔（分、時間、日）を指定し、「保存」をクリックします。



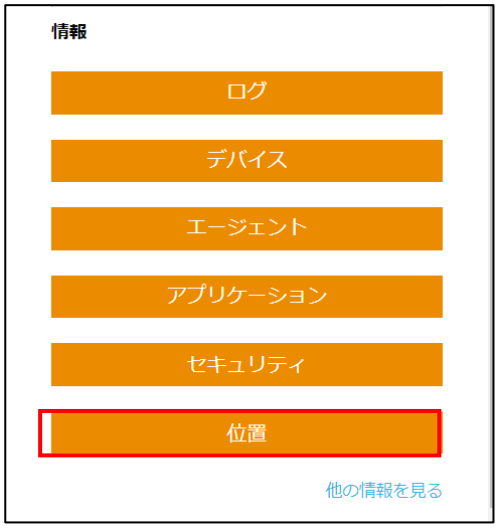
端末位置の確認方法

【手順①】

たよれーる DMS ホーム画面、または「機器」タブから確認対象の機器の詳細欄をクリックします。

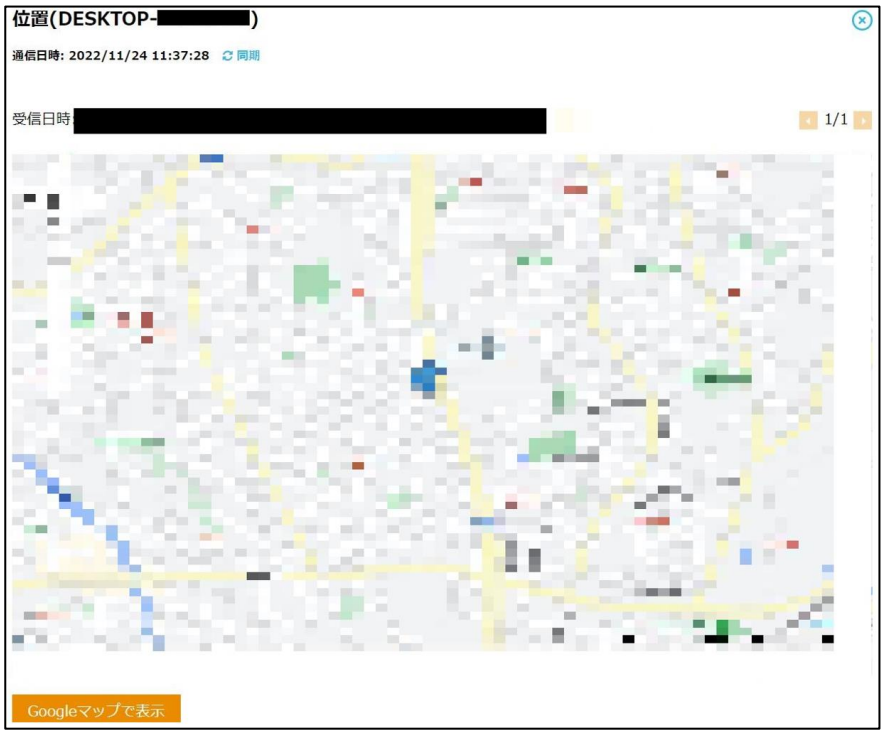
【手順②】

右ペインのメニューから「情報」-「位置」をクリックします。



【手順③】

「位置」を選択後、マップにて現在の端末の位置情報を確認することができます。



3-7　チェックリスト 8-2 への対応

3-7-1　　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）や端末のデータにアクセスできなく（リモートワイプ）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により、第三者から不正操作されるリスクを低減**させることができます。

たよれーる DMS 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】

ホーム画面の「機器」から対象のデバイスの詳細をクリックします。

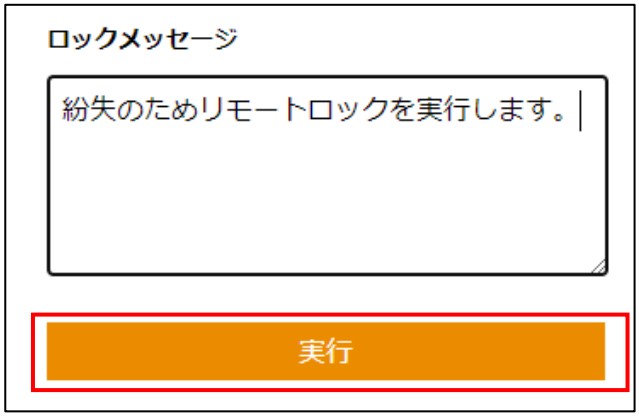
【手順②】

右ペインに表示された「操作」の「リモートロック」をクリックします。

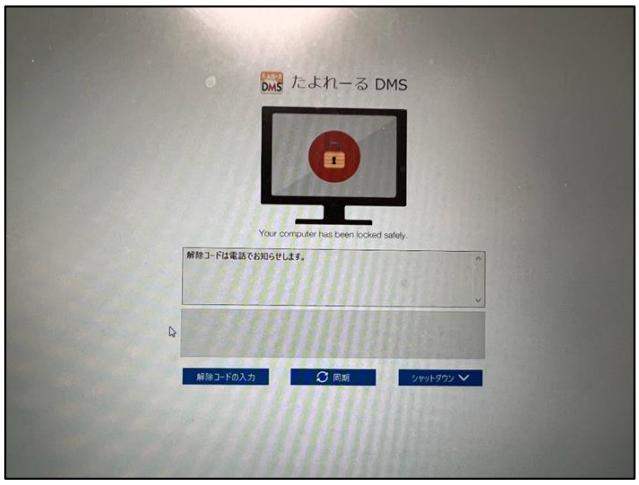
【手順③】

ロックメッセージを入力し、「実行」をクリックします。これにより対象端末をロックすることができます。

解除には解除コードが必要です。この解除コードを対象ユーザーに伝えると、端末側ロックの解除が可能になります。



参考:ユーザーロック画面



リモートロック解除コードの確認

リモートロックを実行した場合、下記手順で確認するコードを入力することで、ロックを解除することができます。

【手順①】

ホーム画面の「設定」-「Windows」-「管理アプリの通信と動作」をクリックします。

【手順②】

エージェント共通管理内の「端末でのリモートロックの解除方法」に記載のパスワードを確認します。

たよれーる DMS からのリモートワイプ実行

【手順①】

ホーム画面の「機器」から対象のデバイスの詳細をクリックします。

【手順②】

右ペインに表示された「操作」の「他の操作を見る」をクリックします。

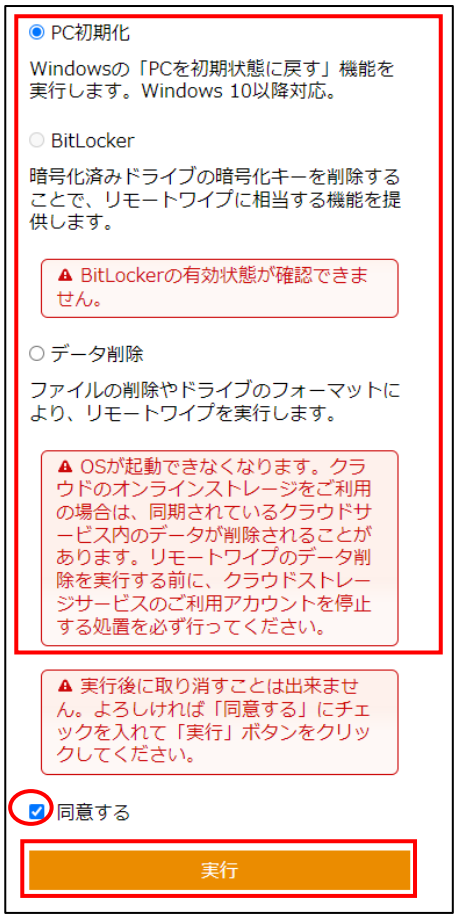
【手順③】

リモートワイプをクリックします。

【手順④】

リモートワイプの実行パターン（PC 初期化、BitLocker、データ削除）を選択し「同意する」にチェックを入れ実行ボタンをクリックします。例えば、端末を紛失し当該端末を破棄する場合は、BitLocker を選択します。

端末を引き続き利用したい場合は PC 初期化またはデータ削除を選択します。



3-8　チェックリスト 8-3 への対応

3-8-1　　端末の暗号化

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るように設定します。

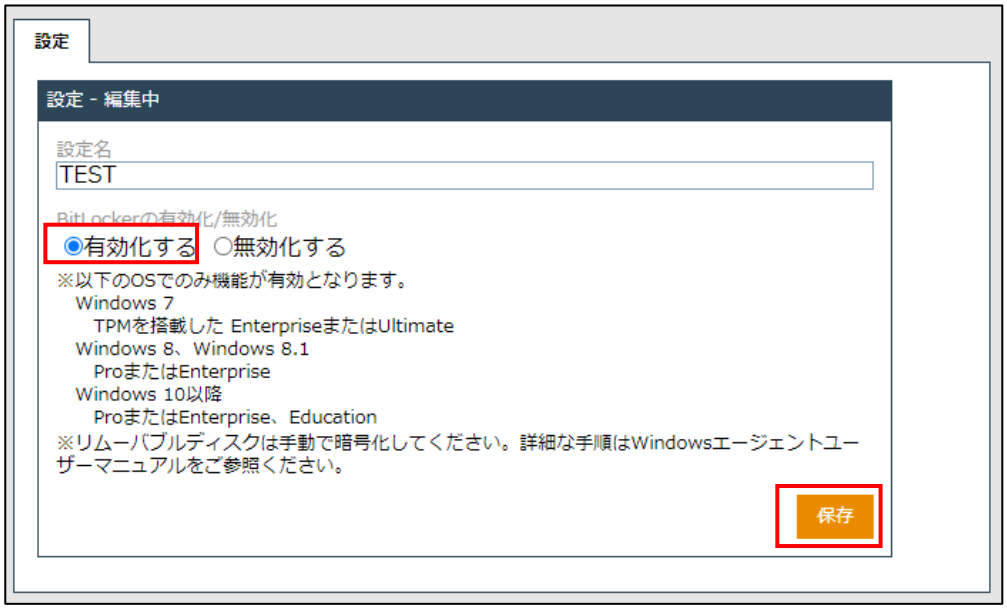
ハードディスクの暗号化

【手順①】

ホーム画面の「設定」-「Windows」-「セキュリティ」-「暗号化」を選択し「＋」ボタンをクリックし設定セットを新規作成します。

【手順②】

設定名を入力後「BitLocker の有効化/無効化」の項目で「有効化する」にチェックを入れ、「保存」ボタンを押します。



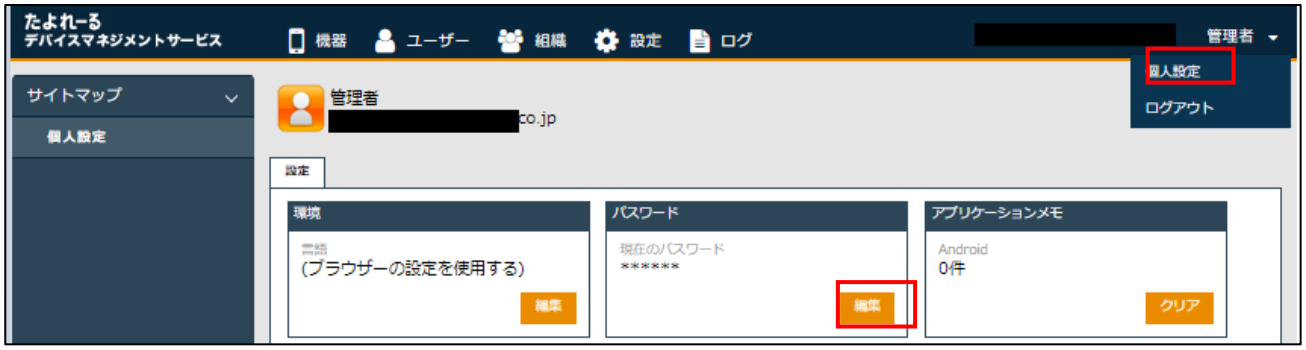
3-9　チェックリスト 9-2 への対応

3-9-1　　たよれーる DMS 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**。

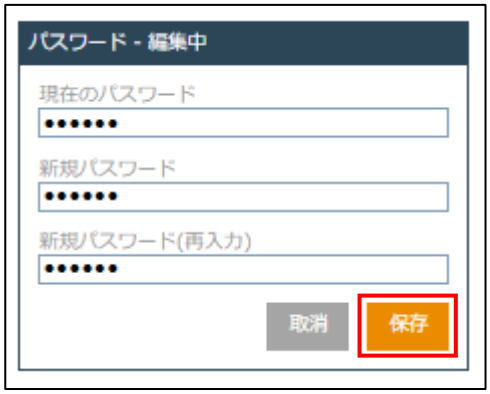
【手順①】

ホーム画面の右上にあるユーザー名のプルダウンを表示させ「個人設定」、パスワードの項目から「編集」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。



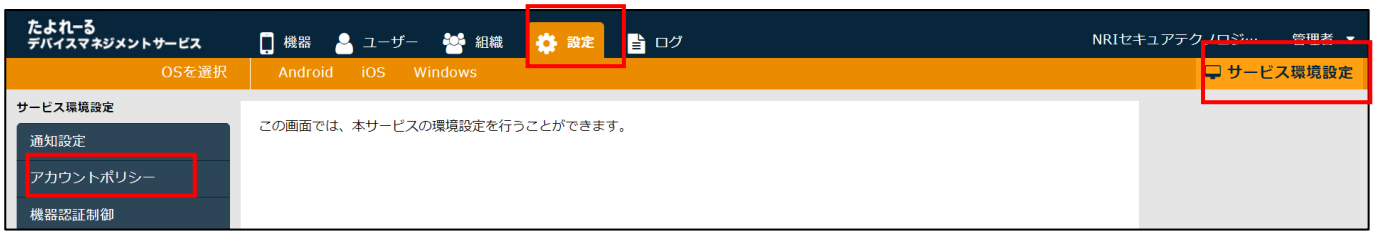
3-10 チェックリスト 9-3 への対応

3-10-1　たよれーる DMS のアカウントロック回数の設定

たよれーる DMS のポータルへのアクセスに対し、ロックアウトの設定を行います。これにより、第三者による不正アクセスのリスクを低減します。

【手順①】

ホーム画面の「設定」-「サービス環境設定」-「アカウントポリシー」をクリックします。

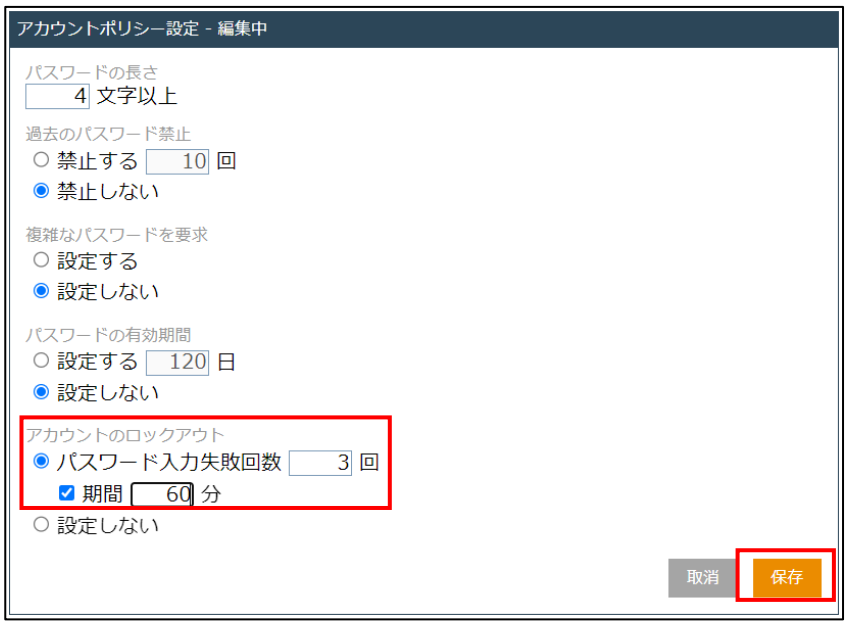


【手順②】

現在のポリシーが表示されるので、「編集」をクリックします。

【手順③】

「アカウントのロックアウト」の項目を選択します。「パスワード入力失敗回数」を入力し、ロックアウトする期間を入力後「保存」をクリックします。



3-11 チェックリスト 10-1 への対応

3-11-1　たよれーる DMS 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。**
たよれーる DMS のユーザーを追加する場合は、以下の手順で、過剰な権限を持つユーザー種別を設定しないようにしてください。

【手順①】
「ユーザー」タブをクリックし「＋」ボタンから新規ユーザーを作成します。

【手順②】

ユーザー情報を入力しユーザー種別から要件に合った権限を選択します。

パスワードを入力し「保存」をクリックします。

3-12 チェックリスト 10-2 への対応

3-12-1　たよれーる DMS のログインパスワードポリシーの設定

システムにログインするためのパスワードの強度を高めることで不正ログインのリスクを低減します。

【手順①】

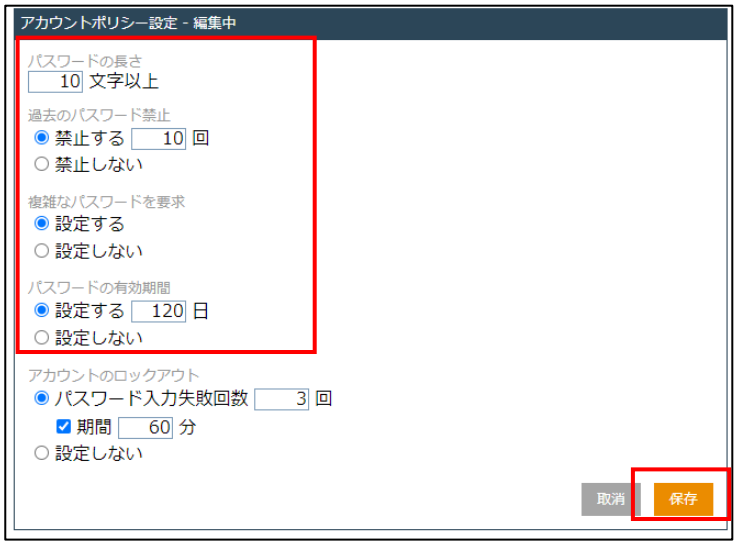
ホーム画面の「設定」-「サービス環境設定」-「アカウントポリシー」をクリックします。

【手順②】

現在のポリシーが表示されるので、「編集」をクリックします。

【手順③】

「パスワードの長さ」「過去のパスワード禁止」「複雑なパスワードを要求」「パスワードの有効期限」に値を入力し「保存」をクリックします。



3-13 チェックリスト 10-3 への対応

3-13-1　たよれーる DMS 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。