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 ~iOS~）

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

(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。（2023 年 11 月 7 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、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。

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・検知	P.6
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.9
5-1 脆弱性管理 **テレワーク端末の OS やアプリケーションに対して最新のセキュリティアップデートを適用するよう周知する。**	・メーカーサポートの確認	P.11
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の確認	P.12
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.13
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.14
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.17
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 端末のパスコードポリシーの設定	P.17
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.20

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.21
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.22
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.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。**	・たよれーる DMS の管理者権限の管理	P.25

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 2-4 への対応

3-1-1　アプリケーションの制限・検知

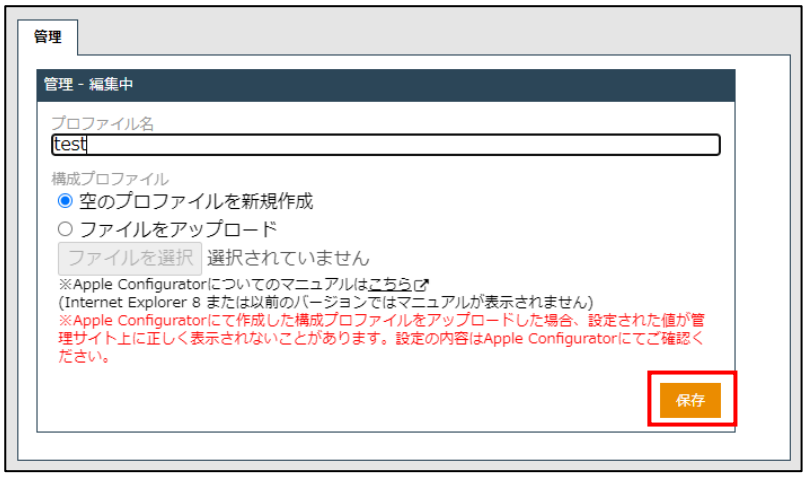
アプリのインストールを業務上必要なものに限定することで、不審なアプリケーションが実行されるリスクを低減することができます。
本項目ではアプリインストールを制限する方法及び検知する方法を記載します。

アプリケーションの利用制限

本手順での設定は、iOS 端末が”監視対象”として配布されている場合のみ機能します。

【手順①】
ポータルのトップ画面から「設定」-「iOS」-「構成ファイルアップロード」を選択し、「＋」ボタンをクリックし、設定セットを作成します。

【手順②】
設定名を入力し「空のプロファイルを新規作成」にチェックを入れ、「保存」をクリックします。

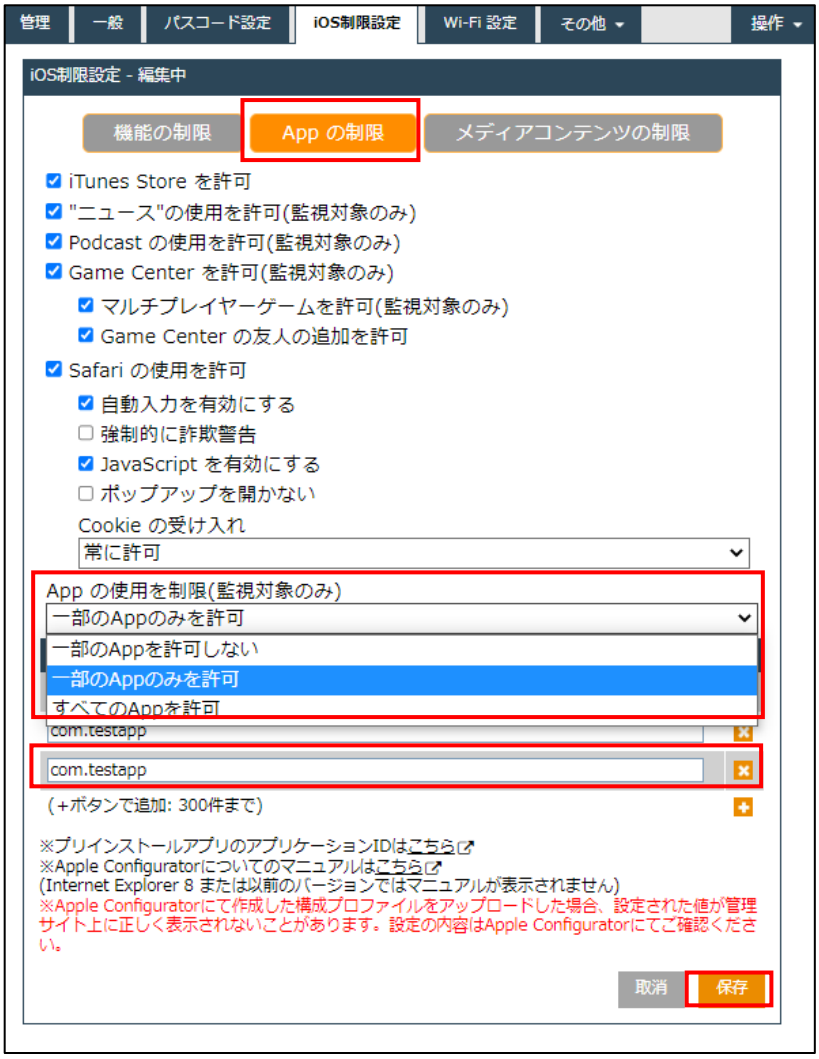


【手順③】

「iOS 制限」のタブに移動し「新規作成」をクリックします。

【手順④】

「App の制限」のタブに移動し、「App の使用を制限」から「一部の App を許可しない(ブラックリスト形式)」または「一部の App のみを許可(ホワイトリスト形式)」を選択し、アプリケーション ID を入力後「保存」をクリックします。



禁止アプリケーションの検知

【手順①】

「設定」-「iOS」-「アプリケーション」-「アプリケーション検知」から「＋」ボタンで設定セットを新規作成します。

【手順②】

設定名を入力し、「インストール非推奨アプリケーション」にアプリケーション名、アプリケーション ID（※）を入力し「保存」をクリックします。

※　アプリケーション ID はアプリベンダーに問い合わせてください。

【参考】

既にインストールされているアプリケーションのアプリケーション ID を調べる場合は「機器」-「対象機器の詳細」-右ペインの「アプリケーション」から、以下のようにアプリケーション ID を表示することが可能です。

3-2　チェックリスト 4-2 への対応

3-2-1　スクリーンロックの設定

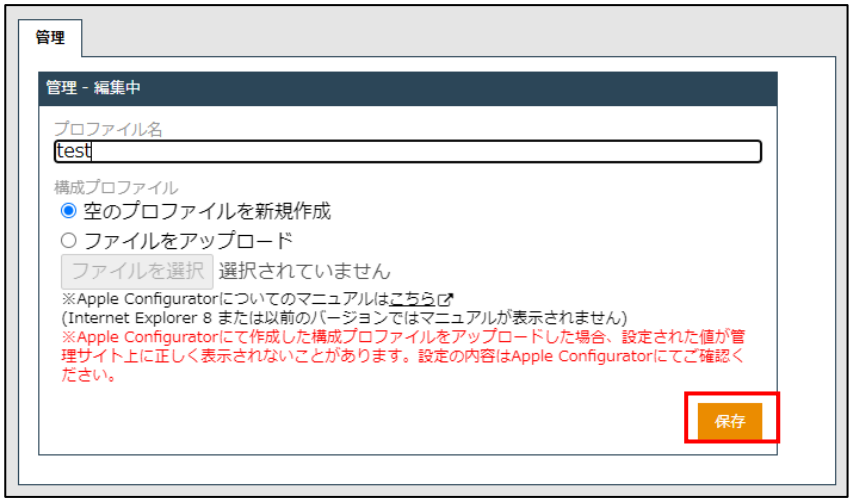
端末のスクリーンロックを設定することにより、**端末紛失時やのぞき見による情報漏えいのリスクを低減します**。この手順と合わせて、各端末のパスコード設定は必ず行ってください。

【手順①】

ポータルのトップ画面から「設定」-「iOS」-「構成ファイルアップロード」を選択し「＋」ボタンをクリックし設定設定セットを新規作成します。

【手順②】

設定名を入力し「空のプロファイルを新規作成」にチェックを入れ「保存」をクリックします。



【手順③】

「パスワード設定」のタブに移動し「新規作成」をクリックします。

【手順④】

「自動ロックまでの最長時間」の時間を選択し、「保存」をクリックします。

3-3　チェックリスト 5-1 への対応

3-3-1　　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）

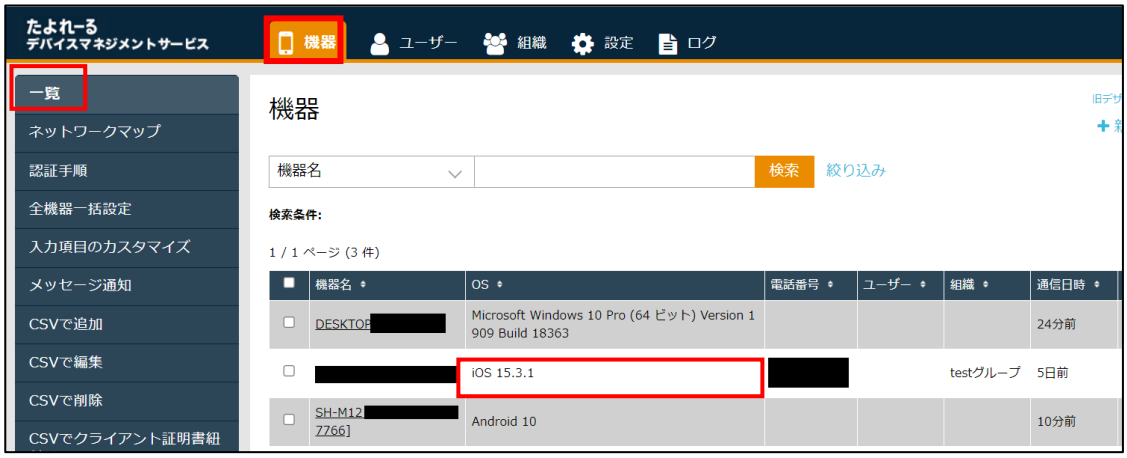
ここでは、たよれーる DMS を利用して、端末の OS バージョンを確認する方法を記載します。

OS バージョン確認方法

【手順①】

「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。

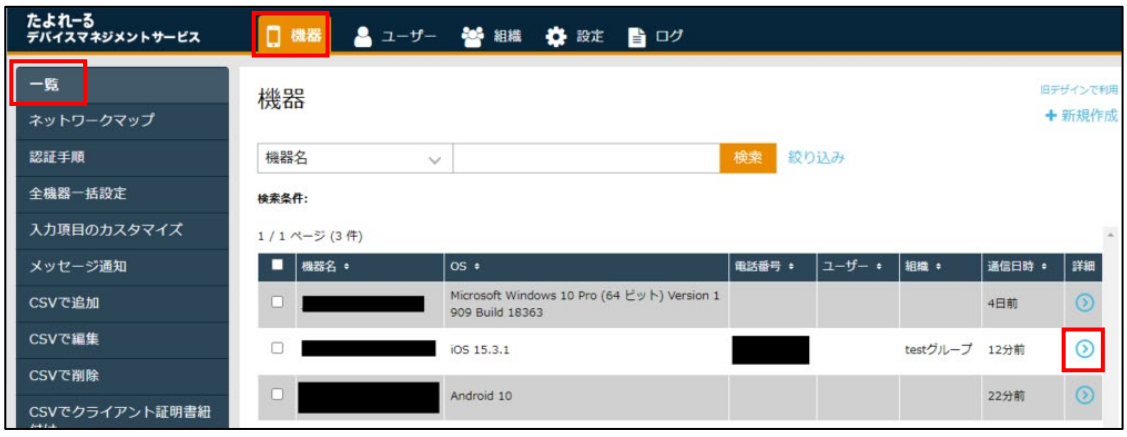
各機器の「OS」に表示されたバージョンから、各機器の OS のバージョンを確認することができます。



アプリケーションバージョン確認方法

【手順①】

「機器」-「一覧」から対象機器の詳細をクリックします。



【手順②】

右ペインに表示されたメニューから「アプリケーション」をクリックすると、インストールされたアプリケーションのバージョンが確認可能です。

3-4　チェックリスト 7-3 への対応

3-4-1　　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」から各ログが確認出来ます。

3-5　チェックリスト 8-1 への対応

3-5-1　　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。

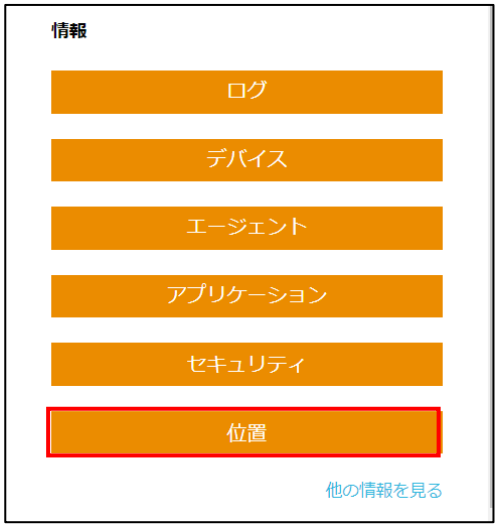
端末位置の確認方法

【手順①】

たよれーる DMS ホーム画面か「機器」から確認対象の機器の詳細情報を表示します。

【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。

3-6　チェックリスト 8-2 への対応

3-6-1　　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。

たよれーる DMS からのリモートロック実行

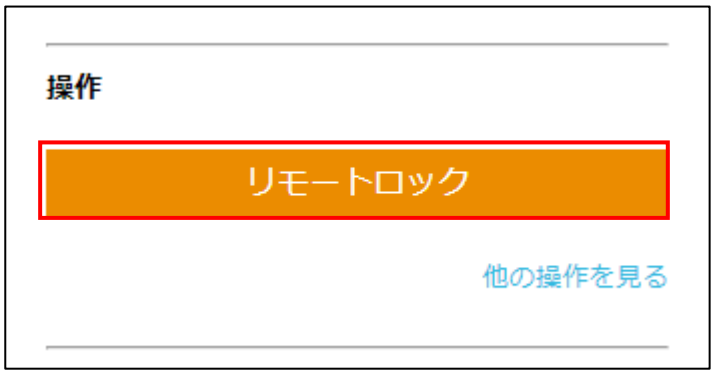
例えば、端末を紛失し、一時的に利用不可としたい場合は、リモートロックを実行します。

【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。

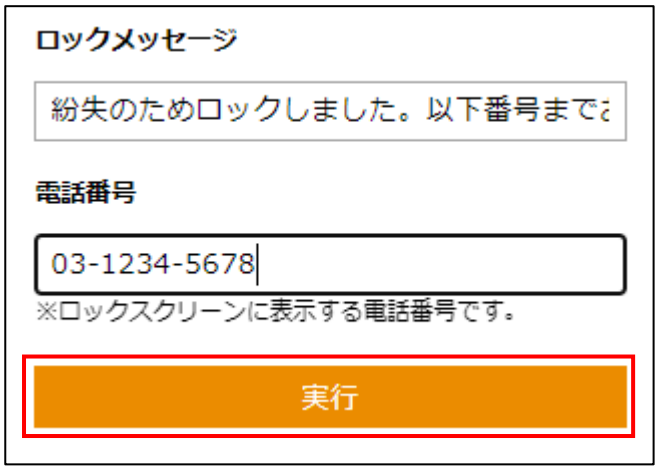
【手順②】

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。



参考:ユーザーロック画面

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】

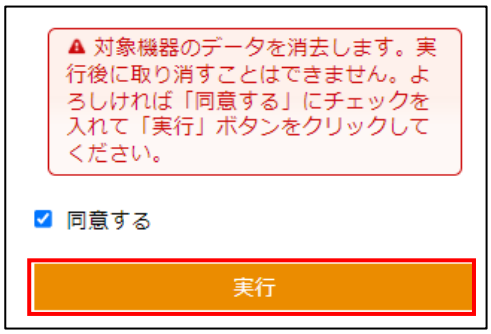
右ペインに表示された「操作」の「他の操作を見る」をクリックします。

【手順③】

リモートワイプをクリックします。

【手順④】

「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。これにより、端末が初期化されます。



3-7　チェックリスト 8-3 への対応

3-7-1　　端末の暗号化

パスコードを設定することにより、データ保護機能が有効化され、保存されているデータが暗号化されます。パスコード設定手順は「設定解説資料（iOS）」を参照してください。

【参考】iPhone でパスコードを設定する - Apple サポート (日本)

3-8　チェックリスト 9-1 への対応

3-8-1　　iOS 端末のパスコードポリシーの設定

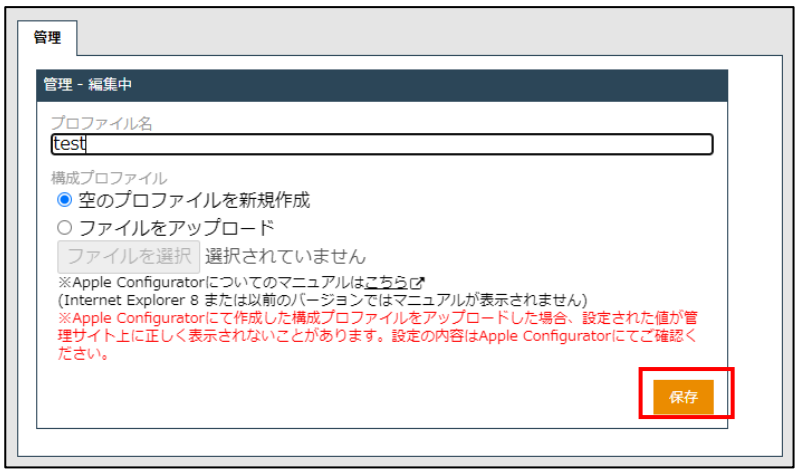
管理者はパスコードポリシーを設定することにより、強度の高いパスコード設定をユーザーに要求できます。**これにより、強度の低いパスワードが使用されるリスクを低減することができます。**

【手順①】

ポータルのトップ画面から「設定」-「iOS」-「構成ファイルアップロード」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】

設定名を入力し「空のプロファイルを新規作成」にチェックを入れ「保存」をクリックします。



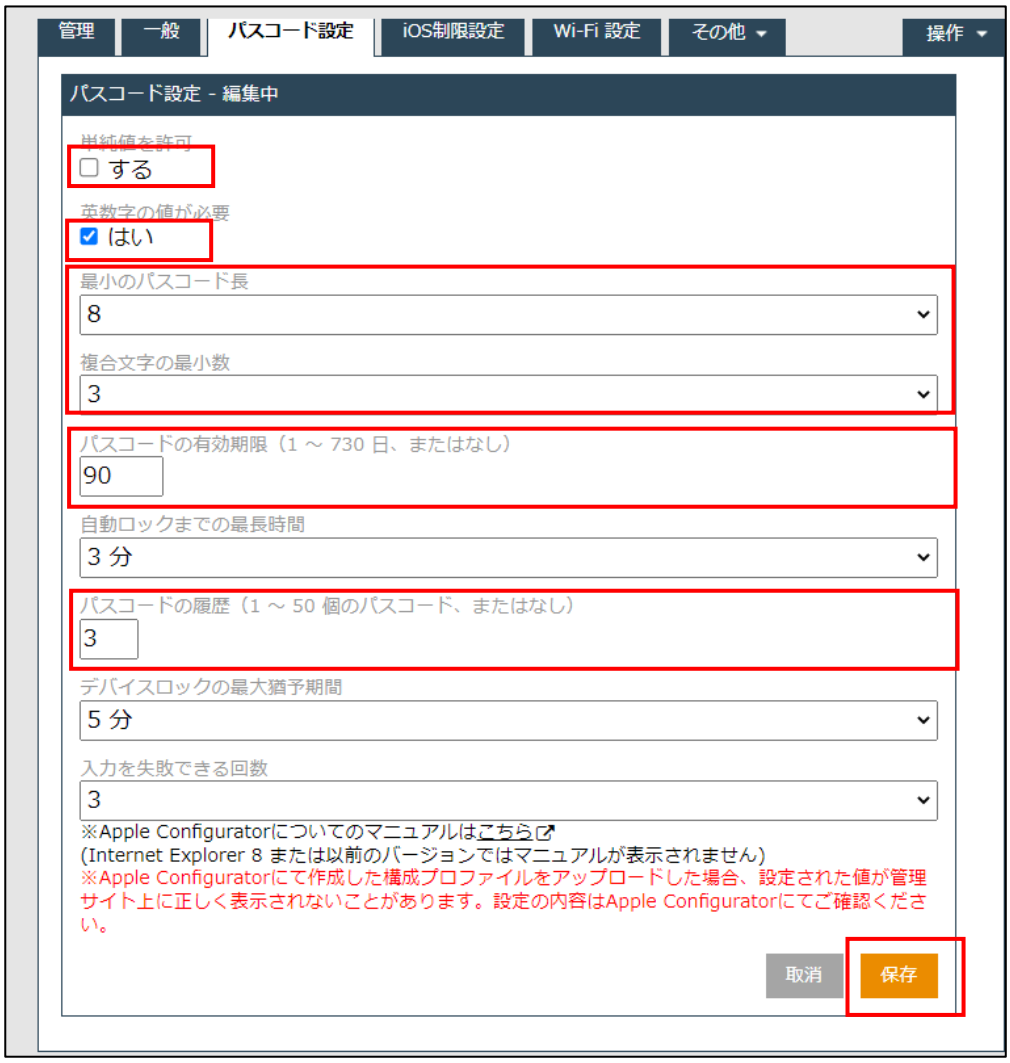
【手順③】

「パスワード設定」のタブに移動し「新規作成」をクリックします。

【手順④】

ポリシーの詳細を設定します。「単純値を許可」はチェックを**外し**、「英数字の値が必要」は「はい」にチェックを入れます。「最小のパスコード長」、「複合文字の最小数」は任意の値を設定します。「複合文字の最小数」は、英文字、数字などの文字の種類数をパスコードに設定することを求めることができます。「パスコードの有効期限」および「パスコードの履歴」についても任意の値（※）を入力します。

※　パスワードの定期変更によるセキュリティ上の効果は薄いという調査結果があります。コンプライアンス上の理由で有効期限の設定が必要な場合は、ユーザーのパスワードの有効期限を設定してください。



3-9　チェックリスト 9-2 への対応

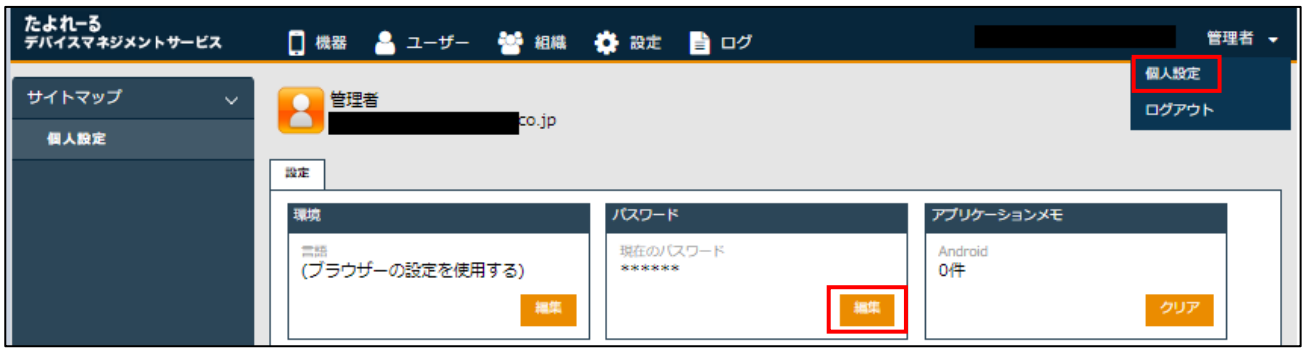
3-9-1　　たよれーる DMS のログインパスワード変更

たよれーる DMS ポータルにアクセスする初期パスワードは、誰が把握しているかわからないので、初期パスワードを速やかに変更することで、**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から、「個人設定」をクリックします。

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。

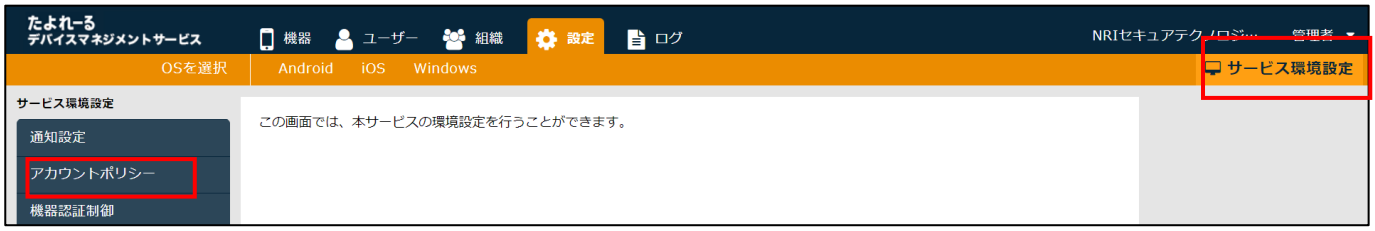
3-10 チェックリスト 9-3 への対応

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。

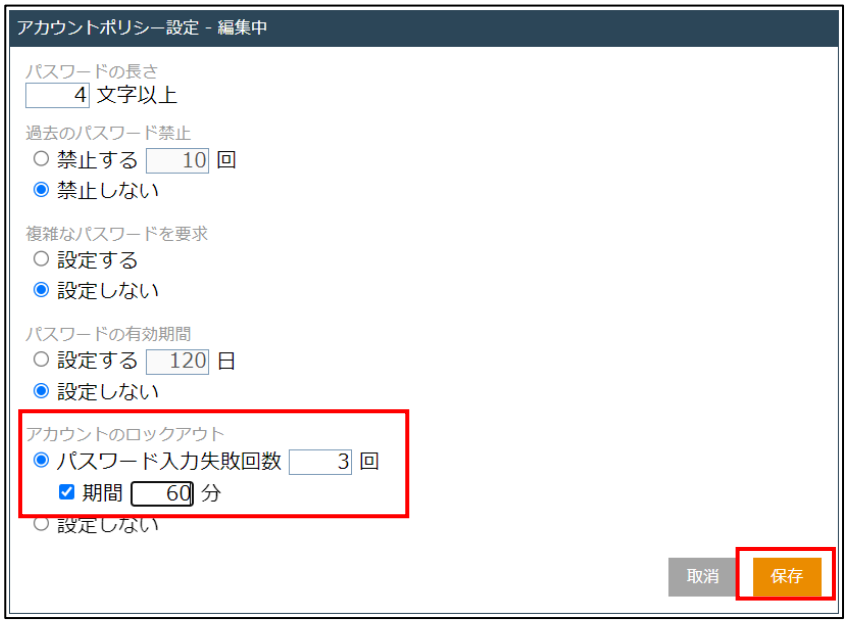


【手順②】

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

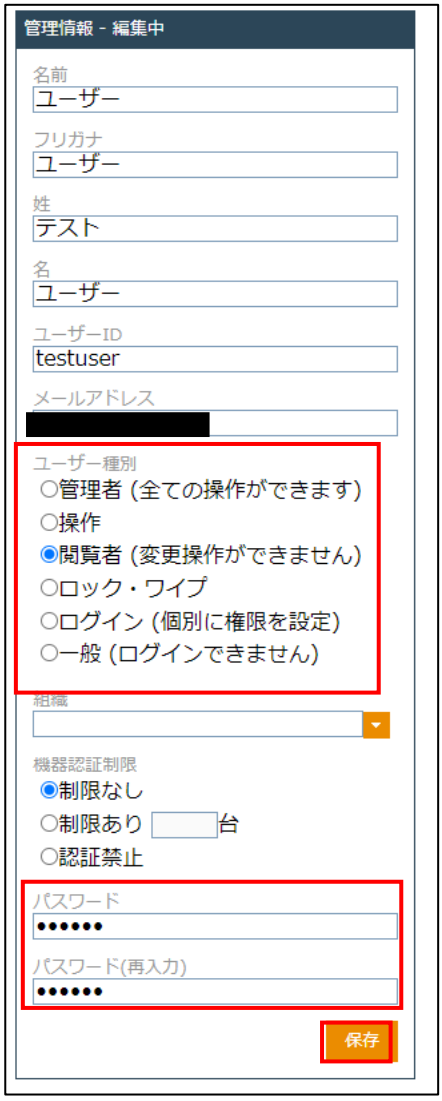
管理者権限を付与するユーザーを限定することで、本製品の設定変更をできるユーザーを必要最小限に抑え、**悪意のあるユーザーにより、意図しない設定変更が行われるリスクを低減することができます。**
たよれーる DMS のユーザーを追加する場合は、以下の手順で、過剰な権限を持つユーザー種別を設定しないようにしてください。

【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。



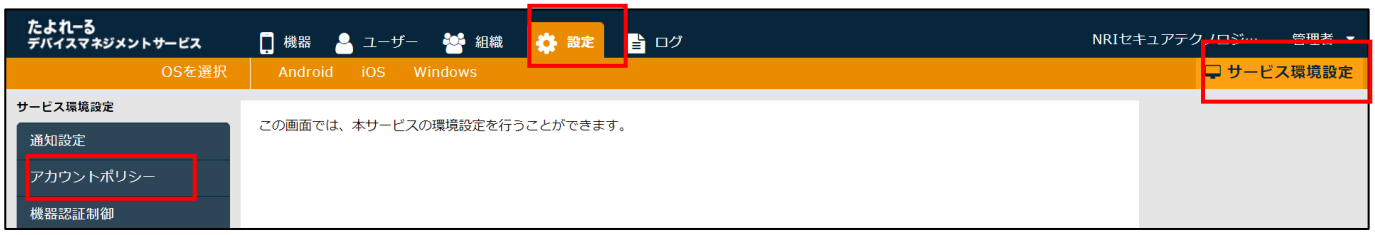
3-12 チェックリスト 10-2 への対応

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

たよれーる DMS 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。

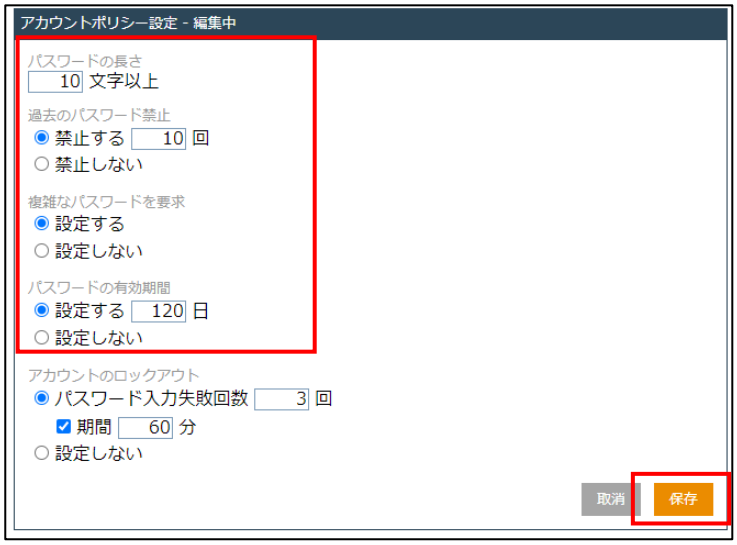


【手順②】

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条件を入力し、「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。

【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、株式会社大塚商会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。