2020

Password Management

Privileged Account Management
& Remote Access Management
&Privileged Session Management

スタートアップガイド

ManageEngine

Password Manager Pro

2020 年 09 月 04 日発行

目次

1 はじめに

1 - 1 ManageEngine Password Manager Pro について

ManageEngine Password Manager Pro（マネージエンジン パスワードマネージャー プロ）は、「必要な時だけ必要な人だけが使える特権 ID のパスワード」の申請/承認/貸出/返却のワークフロー自動化、オペレーター操作画面録画、パスワード定期変更等を圧倒的な低価格で手軽に実現するソフトウェアです。

Windows、Linux をはじめ、データベースやネットワーク機器、Web アカウント、クラウドアカウントなどの特権 ID のパスワード管理をエージェントレスで実施できます。(注 1)

(注 1):Linux サーバーにインストールした場合、Windows サーバーのパスワード変更にはエージェントが必要です。

1 - 2 本ガイドについて

本ガイドでは Password Manager Pro（PMP）のインストール方法から初期設定の内容について説明しています。

また本ガイドはビルド 10500 を元に作成しています。

1 - 3 本書の目的と対象読者

本書は、Password Manager Pro を購入された方やこれから評価版を試用される方が Password Manager Pro の概要を手早く理解し、ご利用を始めるまでの学習時間を短縮し、製品に慣れるための手がかりとなることを目的としています。

Password Manager Pro 製品のセットアップから実際にパスワード管理を開始するまでの流れ、Password Manager Pro の基礎的な利用方法についてステップ・バイ・ステップでわかりやすく説明しています。

本書でカバーしている範囲は Password Manager Pro の基本的な操作方法です。Password Manager Pro には暗号化 HTML ファイルのエクスポート機能、IP アドレス制御機能、SSH コマンドセット機能など、本書では扱っていない数多くの機能が用意されています。

1 - 4　Password Manager Pro の動作環境

Password Manager Pro をご利用いただくためには、次の条件を満たすシステムが必要です。(注 1)

ハードウェア(最小構成)

CPU	メモリー	ストレージ
Dual Core/Core2Duo	4.0GB　以上	10.0GB　以上

サイジング

リソース数/ユーザー数	CPU	メモリー	ストレージ
小規模 1000 リソース/500 ユーザー以下	DualCore/Core2Duo	4.0GB	10.0GB　以上
中規模 5000 リソース/1000 ユーザー以下	Quad Core 以上	8.0GB	20.0GB　以上
大規模 5000 リソース/1000 ユーザー以上	Octa Core 以上	16.0GB	30.0GB　以上

ソフトウェア

サーバーOS	Windows Server 2012 / 2012 R2 / 2016 / 2019 Ubuntu 9.x 以降、CentOS 4.4 以降、Red Hat Linux 9.0、Red Hat Enterprise Linux 7.x,6.x,5.x
パスワード変更(注 2)	Microsoft .NET framework 4.5.2 以降 Visual Studio 2015 C ++再配布可能パッケージ(2015 以降であれば可)

Web クライアント

Web ブラウザー	Mozilla Firefox, Microsoft Edge, Google Chrome 解像度 1280 x 800 ピクセル以上

データベース

データベース	PostgreSQL（製品バンドル）， Microsoft SQL Server 2008 / 2012 / 2014 / 2016 / 2017 / 2019(注 3)

(注 1): 詳細なシステム要件、管理対象のリソースについては Password Manager Pro 動作環境をご覧ください。

(注 2): パスワード変更を実行するために必要となるモジュールです。

(注 3): Windows Server 2008 以降にインストールされていることが必要です。

2 Password Manager Pro のインストール・アンインストール

Password Manager Pro のインストーラー入手からインストールまでの流れを説明します。

2 - 1 Password Manager Pro のダウンロード

Web ブラウザーで次の URL を開き、ご利用の環境に適したインストーラーをダウンロードします。

https://www.manageengine.jp/products/Password_Manager_Pro/download.html

2 - 2 Password Manager Pro のインストール手順

Windows

1. インストールするマシンのローカル管理者の権限を持つユーザーで Windows にログオンします。

2. ダウンロードしたインストーラーをダブルクリックして起動します。

図 1 インストーラーの起動

3. インストール画面が表示されるので「**Next**」をクリックします。

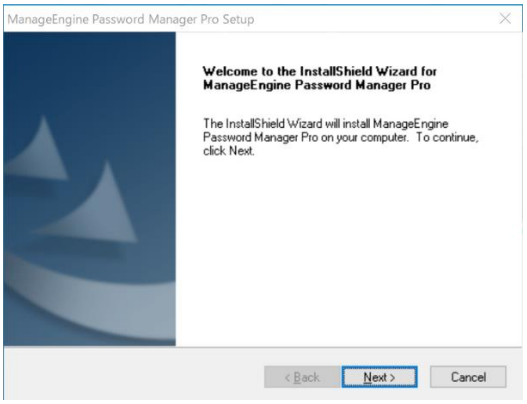


図 2 インストール画面

4. 使用許諾条項をお読みいただき、承諾後に「**Yes**」をクリックします。

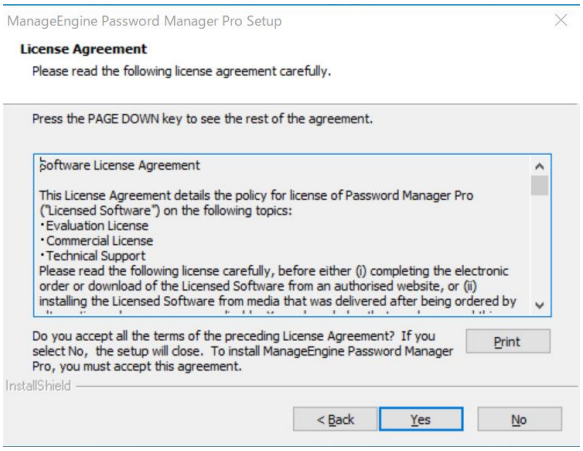


図 3 使用許諾条項

5. インストールフォルダーを選択します。デフォルトは‘C:¥Program Files¥ManageEngine¥PMP’です。

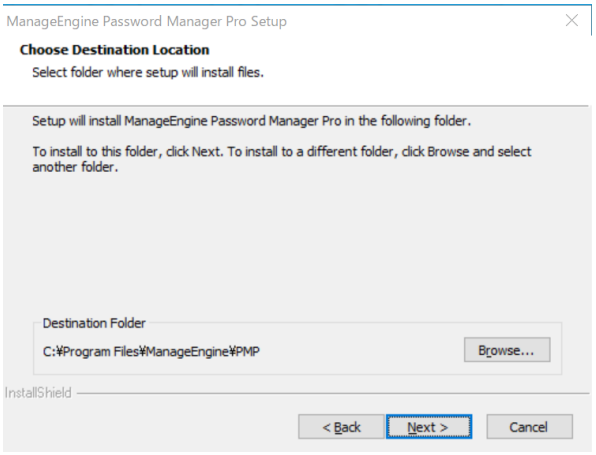


図 4 インストールフォルダーの選択

6. HA 構成(高可用性)を実装する場合にはプライマリーサーバー、セカンダリーサーバーをこちらで指定します。HA 構成を未構成の場合は‘High availability primary server’を選択した状態で「**Next**」をクリックします。

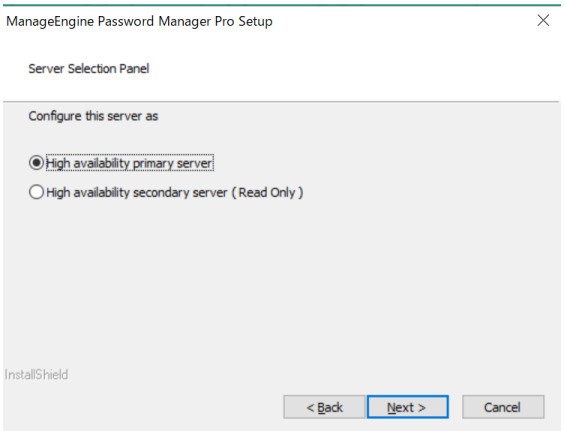


図 5 HA 構成の選択

7. インストールディレクトリをアンチウイルスソフトのスキャン対象から除外する設定を推奨するメッセージが表示されます。「**OK**」をクリックして続行します。

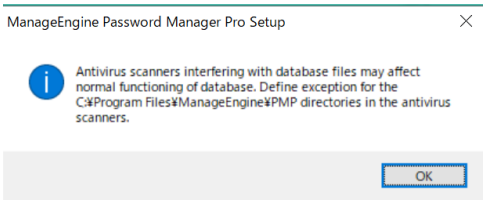


図 6 アンチウイルスソフトのスキャン対象からの除外

8. お客様情報を入力します。E-mail と Country は必須となります。それ以外の項目は任意です。

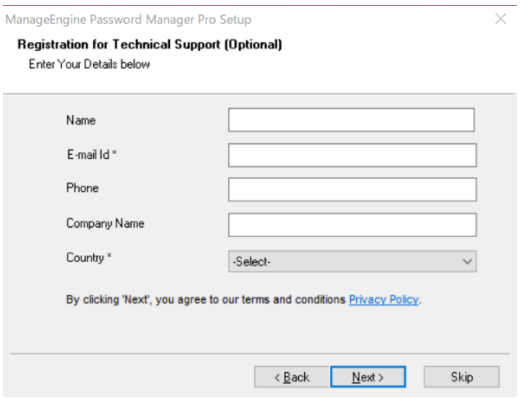


図 7 お客様情報の入力

9. Password Manager Pro をインストールするため、「**Next**」をクリックします。

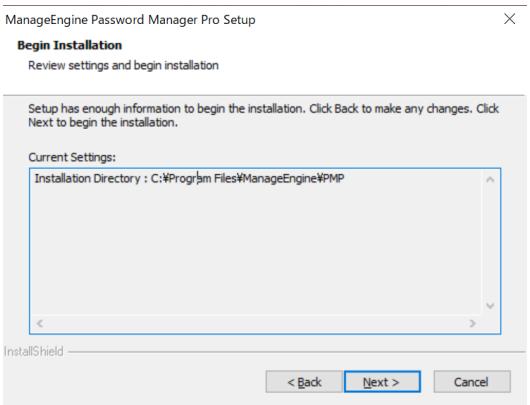


図 8 内容の確認

10. インストールの完了です。必要に応じてチェックボックスを選択し、「**完了**」ボタンをクリックします。

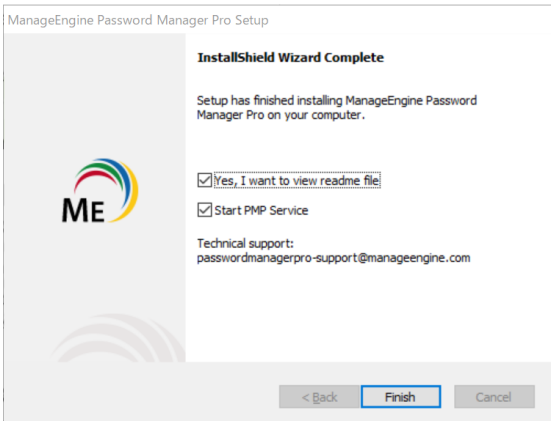


図 9 インストール完了画面

Linux

1. ダウンロードしたインストーラーに実行権限を付与します。

```
chmod 777 ManageEngine_PMP_64bit.bin
```

2. 次のコマンドを実行し、インストーラーを起動します。

```
./ManageEngine_PMP_64bit.bin -i console
```

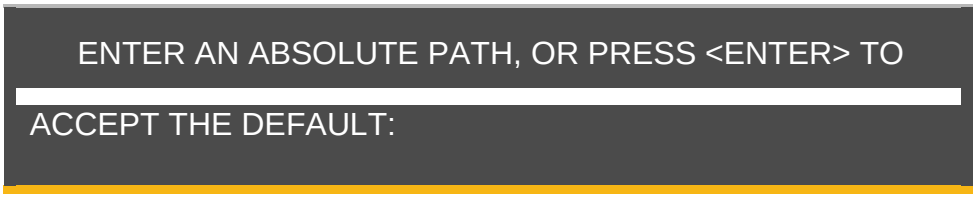
3. Introduction をお読みいただいた上で、PRESS <ENTER> TO CONTINUE にて Enter を押下します。

```
PRESS <ENTER> TO CONTINUE:
```

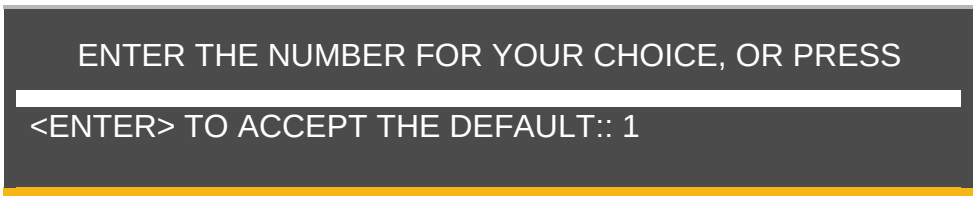
4. License Agreement を適宜 PRESS <ENTER> TO CONTINUE にて Enter を押下しつつ読み進める。最後に以下のメッセージが表示されるため、「Y」を入力します。

```
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y?N): Y
```

5. Choose Installation Folder では PMP フォルダーのインストールディレクトリを決定します。デフォルトのパスで問題ない場合には Enter を押下し、変更する場合にはインストール先の絶対パスを指定します。



6. Server Configuration では HA 構成時のサーバー種別を聞かれます。プライマリサーバーの場合は 1 または Enter、セカンダリーサーバーの場合は 2 を入力してください。単体でのご利用の場合は 1 または Enter を入力してください。



7. Pre-Installation Summary ではインストールの確認がなされます。問題ない場合には Enter を押下してください。

8. Ready To Install ではインストールを実行します。Enter を押下してください。

9. Installation Complete と表示されていればインストールは無事終了しています。Enter を押下してインストールを終了してください。

2 - 3　アンインストール

Windows

1. **コントロールパネル** → **プログラムと機能**　→　**プログラムのアンインストール** を開きます。

2. **ManageEngine Password Manager Pro** を選択し、 **アンインストール** をクリックします。

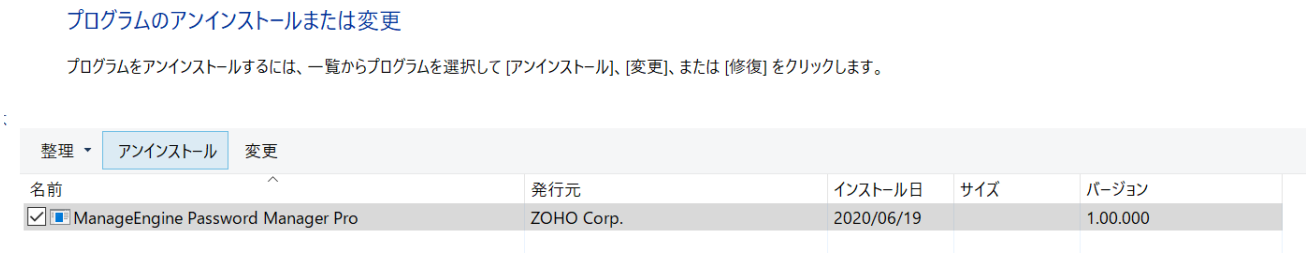


図 10 Password Manager Pro のアンインストール

3. 画面の指示に従い、アンインストール作業を進めます。

メモ：**スタートメニュー** → **ManageEngine Password Manager Pro Server** → **アンインストール** からアンインストールすることもできます。Setup.exe が見つからないと表示される場合は、ダウンロードしたインストーラー ManageEngine_PMP_64bit.exe を指定します。

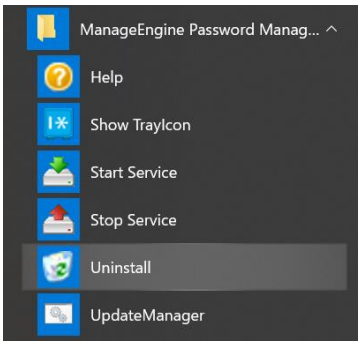


図 11 Password Manager Pro のアンインストール

Linux

1. <PMP>¥bin へ移動します。

2. 次のコマンドを実行し、Password Manager Pro のサービスをアンインストールします。

```
sh pmp.sh remove
```

3. PMP フォルダーを手動で削除します。

3 Password Manager Pro の起動と停止

Password Manager Pro の起動方法を説明します。

3 - 1 サーバーの起動

Windows

1. **コントロールパネル** → **管理ツール** → **サービス**を開き、[**Password Manager Pro**]をクリックします。

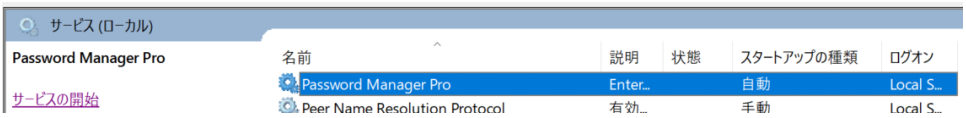


図 12 管理ツールからのサービス停止

2. [**サービスの開始**]をクリックします。

メモ：**スタートメニュー** → **ManageEngine Password Manager Pro** →**Start Service** からサービスを開始することもできます。

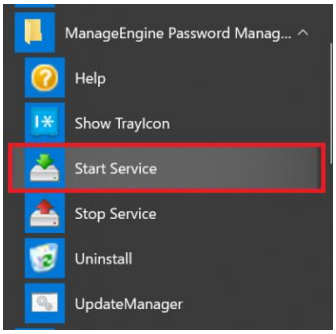


図 13 スタートメニューからのサービス開始

3. Password Manager Pro サービスが起動します。

メモ：今後は Windows の起動時に Password Manager Pro サービスも自動的に起動します。

Linux

以下のコマンドを実行し、サービスを起動させます。

```
/etc/rc.d/init.d/pmp-service start
```

3 - 2 サーバーの停止

Windows

1. **コントロールパネル** → **管理ツール** → **サービス**を開き、[**Password Manager Pro**]をクリックします。

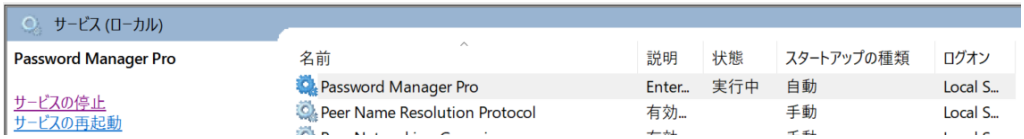


図 14 管理ツールからのサービス停止

2. [**サービスの停止**]をクリックします。

メモ：**スタートメニュー** → **ManageEngine Password Manager Pro** → **Stop Service** からサービスを停止することもできます。

図 14 スタートメニューからのサービス停止

Linux

以下のコマンドを実行し、サービスを停止させます。

```
/etc/rc.d/init.d/pmp-service stop
```

4 Password Manager Pro の初回ログイン時の設定

Password Manager Pro に初めてログインした後に必須となる設定について説明します。

メモ：管理者としてログインした後に「ダッシュボード」タブから必要となる作業が記載されています。

図 15 初期セットアップ項目

4 - 1 Password Manager Pro へのアクセス

1. サービスを起動すると自動的に Web ブラウザーが起動し、ログイン画面が起動します。

2. （Web ブラウザーが起動しない場合）Web ブラウザーを起動しアドレスバーに **https://[*サーバー名*]:[*ポート番号*]** を入力し、移動します。
   例：**https://*PMP-server*:*7272*（デフォルトのポート番号は 7272 です）

メモ：上記の方法でリモートマシン上の Password Manager Pro にアクセスできないときは、Password Manager Pro がインストールされているマシン上の Web ブラウザーから **https://localhost:7272** にアクセスできるかどうかをご確認ください。

3. 管理者として Password Manager Pro にログインするには、初期ユーザー名・パスワードとして「admin」と入力して [**ログイン**]をクリックします。Google Chrome で開く場合には、[サーバー名]にアクセスする(安全ではありません)をクリックしてください。

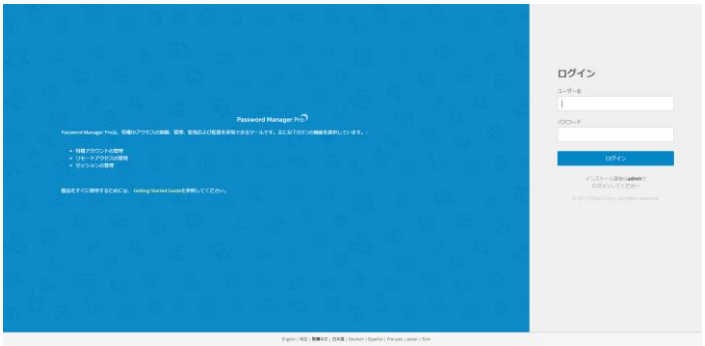


図 16 ログイン画面

4. Password Manager Pro に対して証明書が未適用なためにブラウザーから警告が発生します。自己署名証明書を受け入れてコンソールにアクセスします。

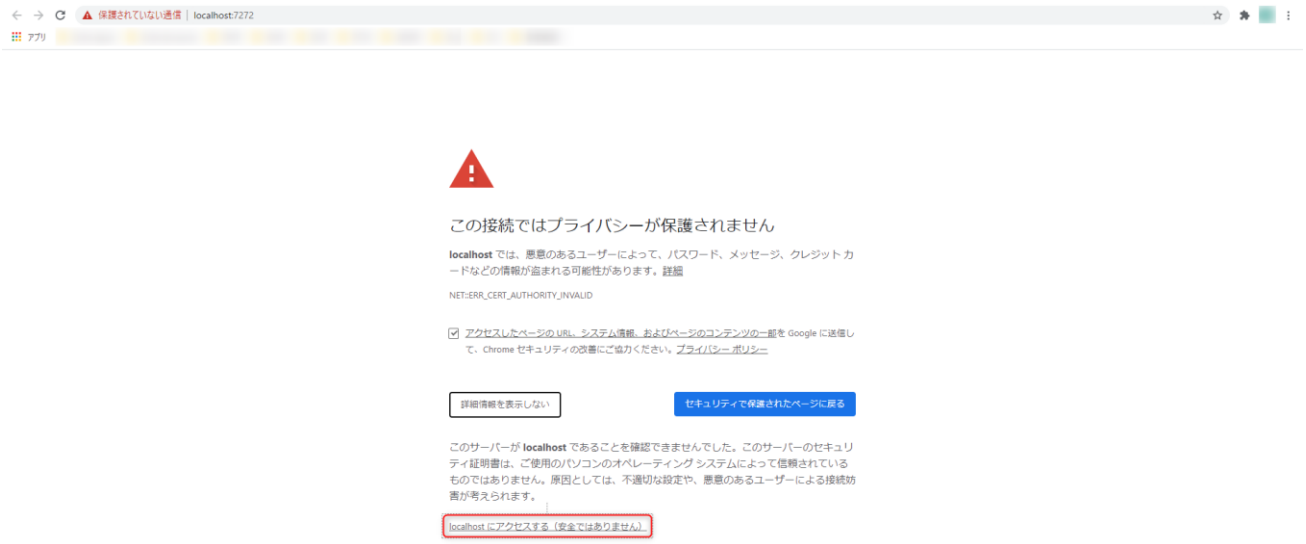


図 17 Password Manager Pro のログイン

メモ：Password Manager Pro では HSTS が実装されており、https 接続を強制します。

4 - 2 メールサーバー設定

1. **管理**タブ → **セットアップ**欄 → **メールサーバー設定** をクリックします。
2. サーバー名、ポート、送信者メールアドレスを指定します。必要に応じてアクセス URL、認証の有無、セキュア接続も指定します。

図 18 メールサーバー設定

3. **「テスト」をクリックし、テストメールが正しく送信されるか確認します。正しく送信された場合にはポップメッセージ「テストメールを×××@○○に送信しました。受信を確認してください」が表示されます。**

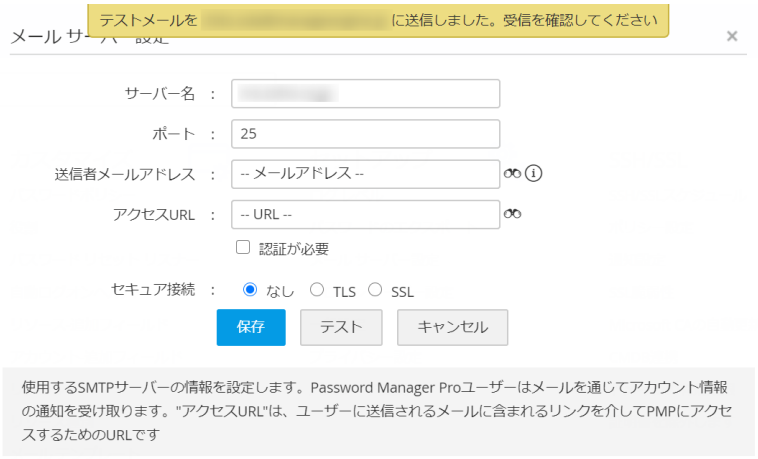


図 19 テストメールの送信

4. 「**保存**」をクリックします。

4 - 2 ライセンスの適用

1. 管理者ユーザーで Password Manager Pro にログインします。

2. 画面右上の人型アイコンをクリックします。

3. 「ライセンス」をクリックします。

4. 受領しているライセンスファイルのパスを指定して「アップグレード」をクリックします。

図 20 ライセンス状況

5. ライセンスの適用に成功した旨のポップアップウィンドウが表示されていることを確認します。

図 21 ライセンス適用に成功

4 - 3 デフォルトの admin, guest のパスワード変更

Password Manager Pro ではセキュリティ上の理由からライセンス適用後にデフォルトユーザー(admin、guest)のパスワード変更を強制します。デフォルトのパスワードポリシーは Strong となります。

図 22 ログインパスワードの変更(admin)

図 23 ログインパスワードの変更(guest)

4 - 4 PMP 暗号化鍵の保管

Password Manager Pro はデータベース、その他機密情報に対して AES-256 による暗号化を施しています。その暗号化鍵(**pmp_key.key**)は**<PMP>¥conf フォルダ**ー に保存されています。ただし、セキュリティ上の理由からライセンスの適用後、保管場所の設定を変更するように強制します。

図 22 PMP 暗号化鍵の保存先パスの変更

以下、pmp_key.key ファイルの保存先を変更する手順となります。

1. Password Manager Pro サーバーにログインします。

2. <PMP>¥conf 配下にある pmp_key.key ファイルを PMP フォルダー外に保存します。

メモ：PMP サーバーから PMP のサービスアカウントで pmp_key.key ファイルにアクセスできる状況であれば、外部サーバーでも保管可能です。ただし、サービス起動毎にデータベースのアクセスのために pmp_key.key ファイルを使用します。通信が取れない状況では PMP が起動できませんのでご注意ください。

3. UI 上で保存先パスを UNC 形式で変更の上、以下のチェックボックスをクリックします。
   □ 私は、PMP のマスター暗号化鍵を保護する必要と方法について理解しました

4. 「ファイルの場所を変更」をクリックします。

5. 「ホームに移動」をクリックします。

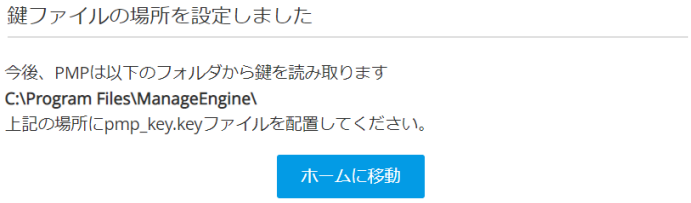


図 25 pmp_key.key ファイルの保存先

4 - 5　SSL/TLS 証明書のインポート

CA 機関から取得された正式な SSL 証明書を本製品に組み込んで利用いただくことも可能です。
以下の手順にて UI 上でインポートできます。

1. 「管理」タブ → 「設定」欄 → サーバー設定へ移動します。

2. 鍵ストアの種別、ファイル名、パスワードを設定の上で保存をクリックします。

図 26 SSL 証明書、ポート番号の設定

5　Password Manager Pro ユーザーの追加

本章では Password Manager Pro へログインするユーザーの追加方法について解説します。
Password Manager Pro ユーザーを Password Manager Pro へ追加する方法は、以下の 3 種類があります。

- 手動で追加
- CSV ファイルからインポート
- Active Directory / Azure AD / LDAP からインポート

5 - 1　手動で追加

1. 「ユーザー」タブをクリックします。

2. 「ユーザー追加」から「手動で追加」をクリックします。

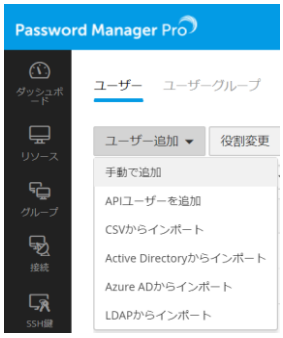


図 27 ユーザーの追加画面

3. 「ユーザー追加」のウィンドウが表示された後に、名、姓、ユーザー名、電子メールをそれぞれ入力します。またパスワード生成方式、パスワードポリシーにて作成するユーザーアカウントのパスワードが準拠するポリシーを選択します。アクセスレベルから作成するユーザーの役割を選択します。その他の項目に関しても適宜入力します。

図 28 手動で追加

5 - 2 CSV ファイルからインポート

CSV ファイル(.txt ファイルも可)から一括でインポートする機能もあります。

1. 「ユーザー」タブをクリックします。

2. 「ユーザー追加」から「CSV からインポート」をクリックします。

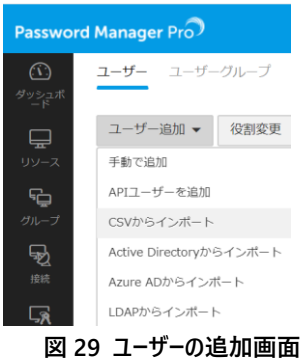


図 29 ユーザーの追加画面

3. ファイルフォーマットを指定し、「参照」から CSV ファイルを指定します。

図 30 CSV ファイルからのインポート

4. 「CSV ファイルからユーザーをインポート」にて各フィールドと対応する列をそれぞれ指定します。

図 31 各フィールド

5. 「完了」をクリックします。

> メモ：名、姓、ユーザー名に日本語等の 2 バイト文字は使用できません。英数字をご利用ください。

5 - 3 Active Directory / Azure AD / LDAP からインポート

Active Directory や Azure AD、LDAP 等のディレクトリサービスと連携する機能もあります。本項では Active Directory を利用したユーザーのインポート機能について解説します。

1. 「ユーザー」タブをクリックします。

図 32 ユーザーの追加画面

2. 「ユーザー追加」から「Active Directory からインポート」をクリックします。

3. 新規ドメインを「追加」し、プライマリドメインコントローラーの FQDN と管理者権限を有するアカウント情報を入力します。

メモ：ドメインのユーザーオブジェクトに対する参照権限を持っているアカウントを指定する必要があります。

4. インポートするユーザー、グループ、OU を指定することも可能です。同期間隔を設定し、「列挙」をクリックしてください。

図 33 Active Directory からインポート

5. グループまたは OU を指定して「インポート」をクリックします。

図 34 グループ/OU 選択画面

6. Active Directory インポート概要からユーザーがインポートされたことを確認します。

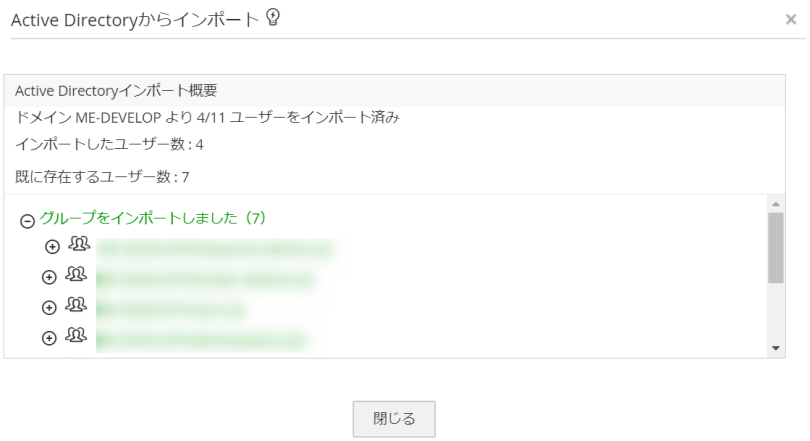


図 35 インポート結果

5 - 4 ユーザーグループの作成

ユーザーをグループ化することで管理を体系化できます。また Active Directory/Azure AD/LDAP からインポートした OU、グループはユーザーグループからまとめて確認できます。以下ユーザーグループを手動で作成する手順を紹介します。

1. 「ユーザー」タブをクリックします。

2. ユーザーグループをクリックします。

図 36 ユーザーグループ画面

3. 「ユーザーグループ追加」をクリックします。

4. グループ名と説明を記載して、「保存して続行」をクリックします。

図 37 ユーザーグループ追加

5. グループに追加したいユーザーを選択し、「グループへ追加」をクリックします。

メモ：ユーザーグループではユーザーをまとめて管理できます。「ユーザー」タブ→「ユーザーグループ」→ユーザーグループのアクションアイコン→ユーザー管理にてグループに対して許可されているアクションを確認できます。デフォルトでは以下の設定項目にチェックがついています。

図 38 ユーザーグループ追加

6 パスワードポリシーの設定

組織にて独自のパスワードポリシーを設定できます。Password Manager Pro ではデフォルトで以下 4 つのパスワードポリシーを用意しています。

- ☐ Low

  …厳格な制約がほとんどないパスワード

- ☐ Medium

  …厳格な制約の少ないパスワード

- ☐ Strong

  …厳格な制約が伴うパスワード

- ☐ Offline Password File

  …オフラインパスワードアクセスポリシー

メモ：デフォルトのパスワードポリシーは編集することができません。

メモ：デフォルトでは Strong が規定として設定されています。 つまり Strong にパスワードポリシーに準拠した形でパスワードを変更します。他のパスワードポリシーを規定とする場合には「既定に設定」のチェックマークをクリックして切り替えます。

図 39 パスワードポリシー画面

6 - 1 パスワードポリシーの定義項目

項目名	解説
ポリシー名	定義するポリシー名を一意の名前で設定します
ポリシーの説明	ポリシーの内容を設定します
最小パスワード長	パスワードの最小文字数を設定します
最長パスワード長	パスワードの最大文字数を設定します
大文字と小文字の混在を強制	パスワードに大文字と小文字を混在させるかどうかを設定します
大文字と小文字の数	パスワードに設定する大文字と小文字の数をそれぞれ設定します
数値を強制	パスワードに数字の設定を強制するか設定します
数字の数	パスワードに設定する数字の数を設定します
特殊文字を強制	特殊文字を混在させるかどうかを設定します ※特殊文字としてカウントされる文字は以下となります。 !#$%&'(=~{+*}<>?_-^¥@[;:,./ ※パスワード自動生成機能によってサポートしている文字は以下となります。 @$-%&*()=^<>!#
特殊文字の数	特殊文字の数を設定します

許可しない文字	パスワードとして許可しない文字を入力します。 ※< >(レスザン グレーターザン)は設定できません。
最初の文字はアルファベットを強制	パスワードの最初の文字をアルファベットで指定するかを設定します
パスワードにログイン名を含めることを許可	アカウント名が含まれるパスワードの設定を許可するかどうかを設定します
最大パスワード経過期間	パスワードの有効期限を定義します。 ここで定義した期間を超えたものは違反としてレポートに表示します
古いパスワードを再利用	過去に設定したパスワードの再利用を許可するかどうかを設定します

6 - 2 パスワードポリシーの設定手順

1. 「管理」タブをクリックします。

2. 「パスワードポリシー」をクリックします。

3. 「ポリシーを追加」をクリックします。

図 40 パスワードポリシー画面

4. 「パスワードのポリシーを追加」にて組織のパスワードポリシーに準拠する形で設定します。

図 41 パスワードポリシー設定画面

5. 「保存」をクリックします。

7 リソース・アカウントの追加

本章では Password Manager Pro が管理するリソース・アカウントの追加方法について解説します。
リソース・アカウントを Password Manager Pro へ追加する方法は、以下の 3 種類があります。

- 手動で追加
- CSV ファイルからインポート
- リソースディスカバリー(Windows/Linux/ネットワーク機器/VMware)

7 - 1 手動で追加

1. 「リソース」タブをクリックします。

2. 「リソース追加」をクリックします。

図 42 リソース追加

3. 各項目を入力して、[保存して続行]をクリックします。 表示名は[リソース名]に、ホスト名/IP アドレスは、[FQDN/IP アドレス]に設定します。また、[リソース種別]、[パスワードポリシー]も最低限設定が必要です。

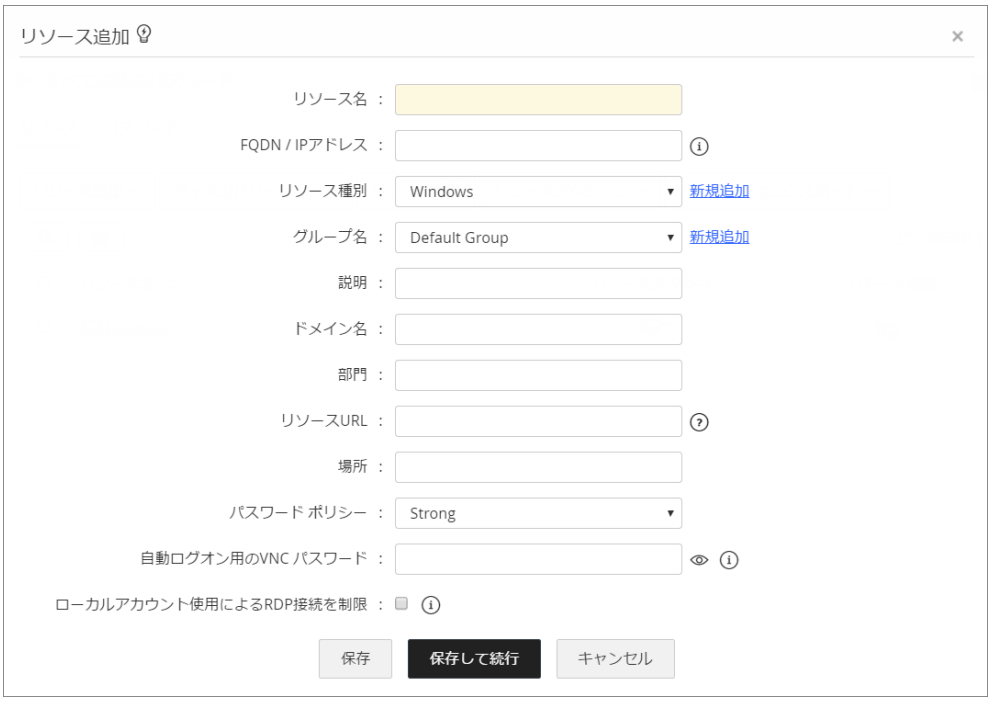


図 43 手動で追加(リソース)

4. アカウント(リソース上の特権 ID)を追加します。複数のアカウントを追加可能です。[ユーザーアカウント]、[パスワード]、[パスワード確認]は必須項目です。

5. [追加]をクリックすると、設定内容が下の一覧に移動します。設定後、[保存をクリックします。

図 44 手動で追加(アカウント)

7 - 2 CSV ファイルからインポート

CSV ファイル(.txt ファイルも可)から一括でインポートする機能もあります。

1. 「リソース」タブをクリックします。

2. 「リソース」追加をクリックします。

図 45 リソース追加

3. 「リソースのインポート」をクリックします。

4. ファイルフォーマットを指定し、「参照」から CSV ファイルを指定します。

図 46 リソースのインポート

5. リソースの各フィールドと CSV ファイルの列を対応させます。

図 47 フィールドのマッピング

メモ：既に存在するリソースはインポートされません。既に存在するリソース情報を上書きする場合には
「既存のリソースを上書き　：　□」のチェックボックスにチェックを入れてください。

7 - 3　リソースディスカバリー(Windows)

1. 「リソース」タブをクリックします。

2. 「リソースディスカバリー」をクリックします。

3. 「Windows」タブからドメイン名、プライマリドメインコントローラーを指定した上で、その資格情報を入力し、「列挙」をクリックしてください。

図 48 リソースディスカバリーの設定画面(Windows)

> メモ：インポートするリソース、グループ/OU を直接指定することもできます。

4. インポート対象のグループ/OU を選択して、「インポート」をクリックします。

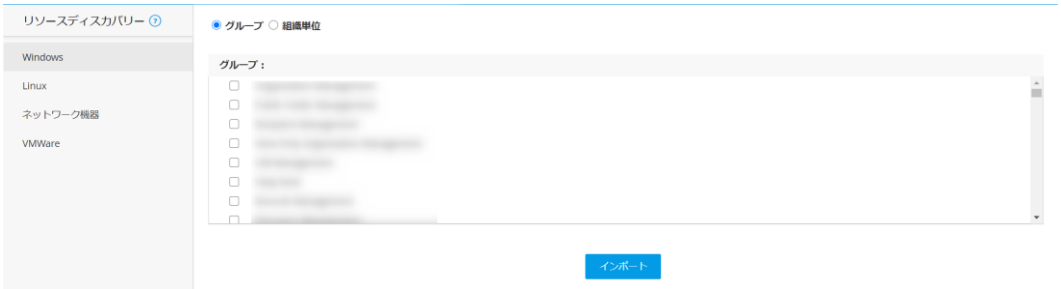


図 49 グループ/OU の選択

5. インポートが成功したことを確認します。

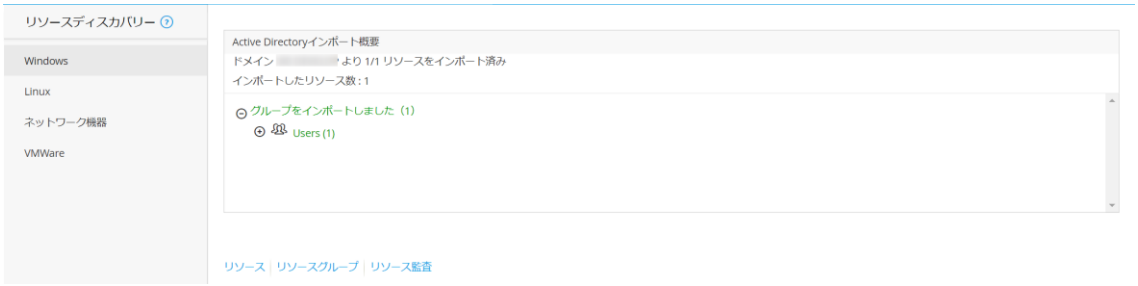


図 50 ディスカバリー結果

7 - 4 リソースディスカバリー(Linux)

1. 「リソース」タブをクリックします。

2. 「リソースディスカバリー」をクリックします。

3. 「Linux」タブをクリックします。

4. IP アドレスの範囲、接続モード、プロファイル、タイムアウトを指定して、「列挙」をクリックします。

図 51 リソースディスカバリーの設定画面(Linux)

5. プロファイルが未作成の場合は、「プロファイル追加」をクリックし、リソース取得に必要な認証情報を追加します。

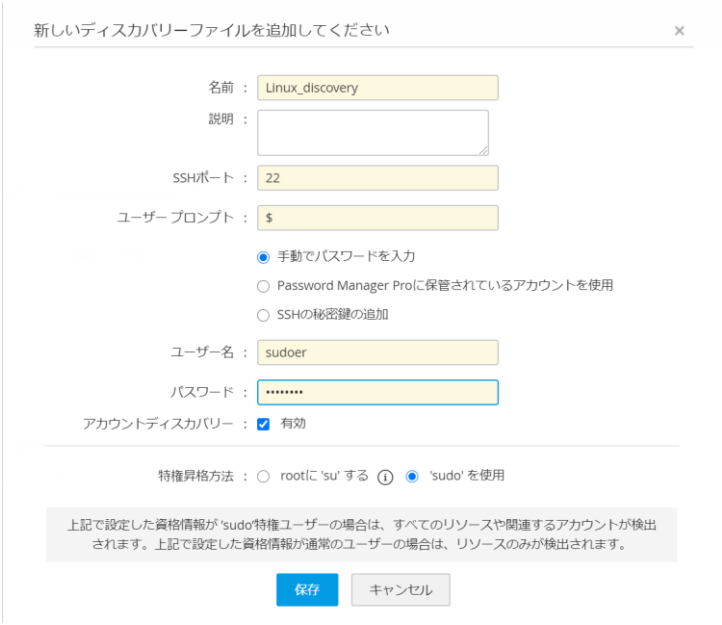


図 52 プロファイルの追加

6. 「ディスカバリーの確認」のポップアップ画面が表示されます。通知先を指定した上で、「続行」をクリックします。

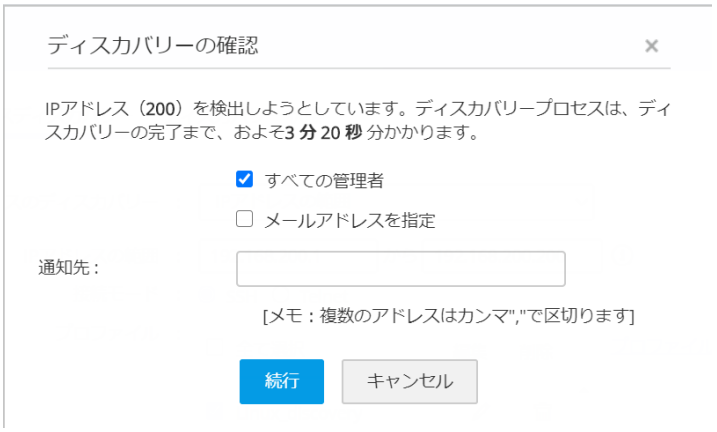


図 53 ディスカバリーの確認

7. 「ディスカバリー状態」タブからディスカバリーの結果を確認できます。

図 54 ディスカバリー結果

7 - 5 リソースディスカバリー(ネットワーク機器)

1. 「リソース」タブをクリックします。

2. 「リソースディスカバリー」をクリックします。

3. 「ネットワーク機器」タブをクリックします。

4. IP アドレスの範囲、プロファイル、タイムアウトを指定して、「列挙」をクリックします。

図 55 リソースディスカバリーの設定画面(ネットワーク機器)

5. プロファイルが未作成の場合は、「プロファイル追加」をクリックし、リソース取得に必要な認証情報を追加します。

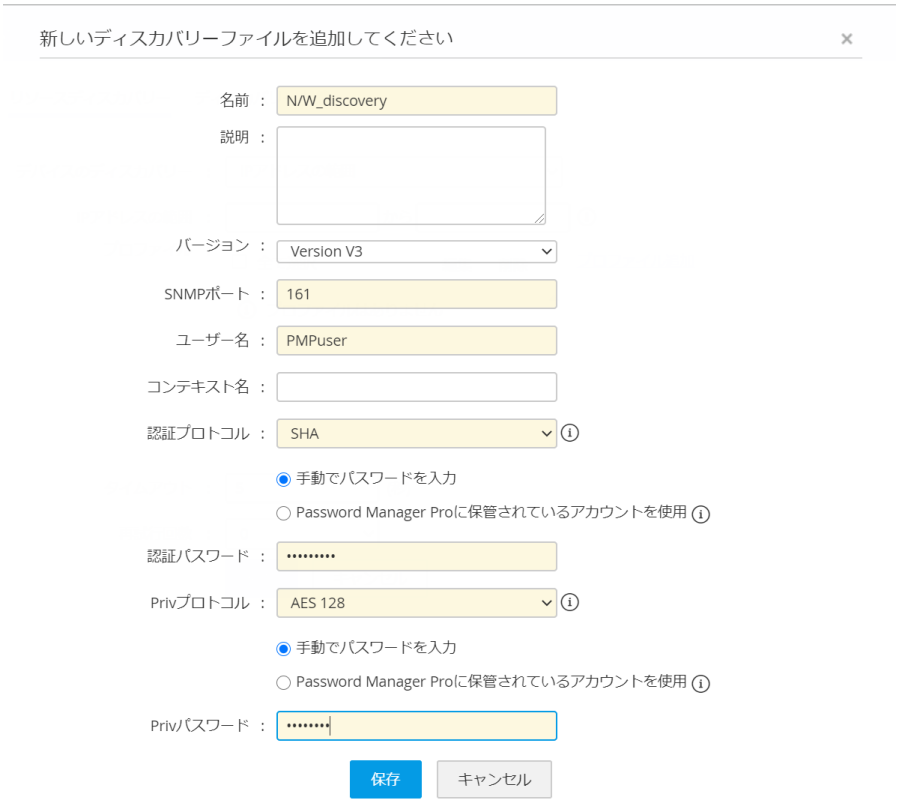


図 56 プロファイル追加

6. 「ディスカバリーの確認」のポップアップ画面が表示されます。通知先を指定した上で、「続行」をクリックします。

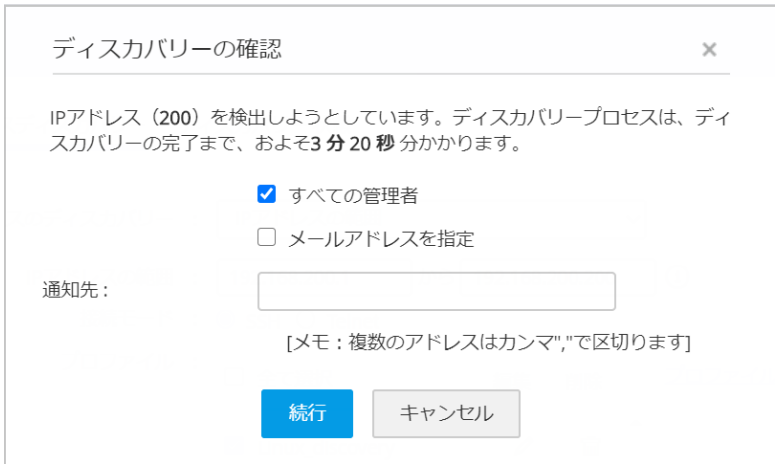


図 57 ディスカバリーの確認

7. 「ディスカバリー状態」タブからディスカバリーの結果を確認できます。

図 58 ディスカバリー結果

7 - 6 リソースディスカバリー(VMware)

1. 「リソース」タブをクリックします。

2. 「リソースディスカバリー」をクリックします。

3. 「VMware」タブをクリックします。

4. IP アドレスの範囲、接続モード、プロファイル、タイムアウトを指定して、「列挙」をクリックします。

図 59 リソースディスカバリーの設定画面(VMware)

5. プロファイルが未作成の場合は、「プロファイル追加」をクリックし、リソース取得に必要な認証情報を追加します。

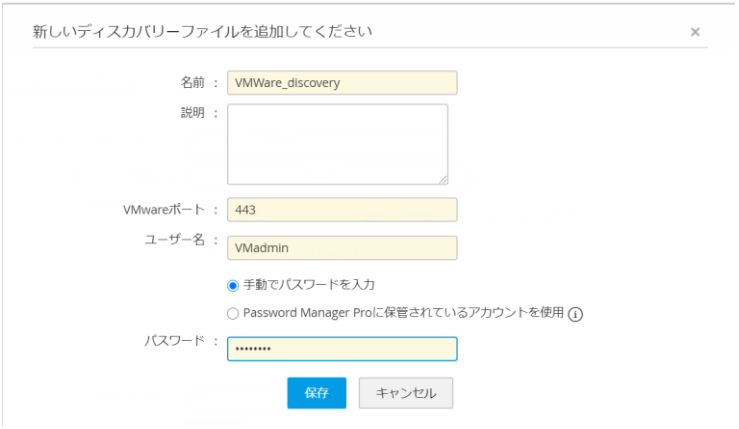


図 60 プロファイル追加

6. 「ディスカバリーの確認」のポップアップ画面が表示されます。通知先を指定した上で、「続行」をクリックします。

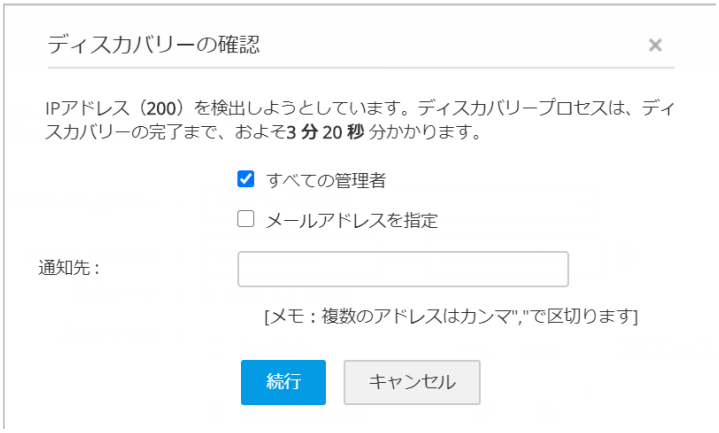


図 61 ディスカバリーの確認

7. 「ディスカバリー状態」タブからディスカバリーの結果を確認できます。

図 62 ディスカバリー結果

8 アクセス制御設定

アクセス制御を実装いただくことで申請承認のワークフローを構築できます。本章ではリソース、アカウント毎にアクセス制御を実装する手順について解説します。

8 - 1　アクセス制御設定項目

1. 承認管理者

   …対象のリソース/アカウントに対して承認者を選択できます。ユーザー単位、またはグループ単位で設定可能です。

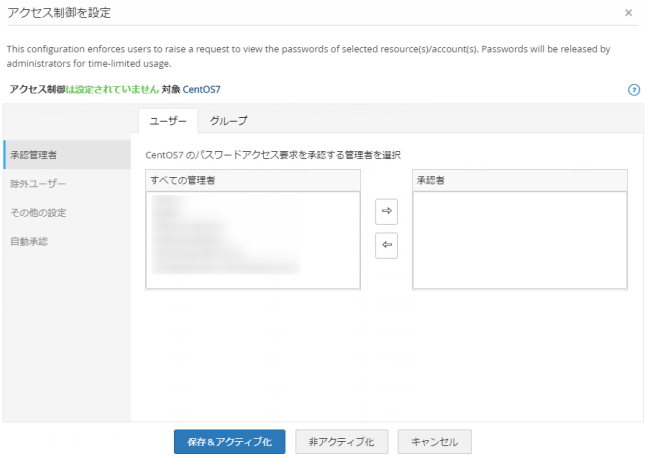


図 63　承認管理者

メモ：多段承認機能はございませんが、承認者にて指定された管理者全員の承認が必要であるように設定可能です。

2. 除外ユーザー

   …アクセス制御を除外するユーザーを指定します。除外ユーザーとして設定されたユーザーは申請承認のフローを経ずにリソース/アカウントに対してアクセスできるようになります。

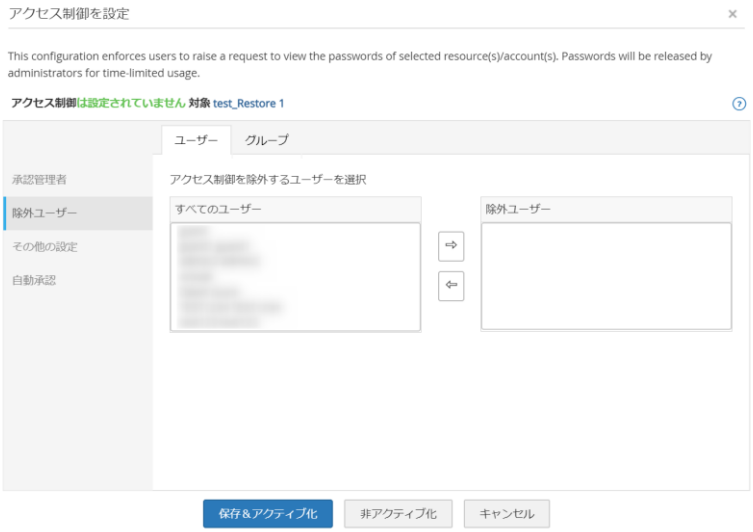


図 64　除外ユーザー

3. その他の設定

   □　デフォルトではチェックされていない設定項目

   ✓　デフォルトでチェックされている設定項目、ただし無効化可能

   ■　デフォルトでチェックされている設定項目、ただし無効化不可能

以下それぞれの設定項目について解説します。

□　パスワード アクセスを承認する管理者は 2 人以上必要(　)管理者

…パスワードが払い出されるまでに必要な承認者の人数です。

メモ：デフォルトで 5 名(01～05)までの承認者を選択できます。 ライセンスが 5 アドミン以上かつ承認者を 5 名以上必要と設定する場合には「管理」タブ→「セットアップ」欄一般設定→「パスワード取得」タブにて

■　最大値(　)承認者(最小「1」から最大「10」の管理者を設定できます)。

最大承認者数を変更してください。ただし、10 名が上限となります。

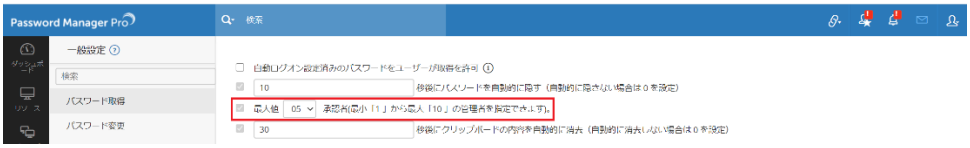


図 65　最大承認者数の変更

✓　パスワードを取得する際に理由の入力を強制

…申請する際のコメント欄にて記載が必須となります。記載なしで申請しようとした際にはエラーとなり申請処理が行われません。

図 66　コメント欄への記載

□　指定された時間の(　)分前に、管理者にリマインドメールを送信

…時刻指定の申請に対して、開始時刻の(　)分前に承認のリマインドメールを管理者に通知します。

□　使用時間終了後、ユーザーに(　)分の延長時間を付与

…排他的使用時間後、セッション終了までの指定した猶予時間を設定します。

□　パスワードは、承認されてから(　)時間後に自働的にチェックイン

…パスワードを払い出した後に申請者がチェックインをし忘れた際にシステムが指定した時間を経過後自動的にチェックインします。

■　承認されない場合、要求は(　)時間後に無効

…承認が下りない申請に対して指定された時間を経過後にその申請を無効化します。

■　パスワードアクセスの排他は最大で(　)分

…排他的に払い出されたパスワードを使用できる時間です。指定された時間を超過した瞬間にセッションは自動的に切れます。

✓ 排他的使用の後(他のユーザーによってチェックインする場合)に、パスワードを変更

…チェックインした後にパスワードを自動的に変更します。

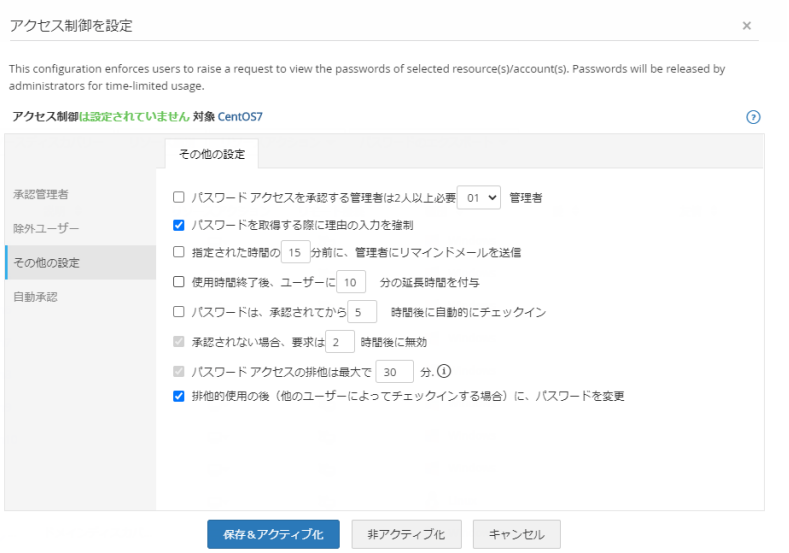


図 67 その他の設定

4. 自動承認

…申請に対してシステムが自動的に承認します。以下 3 つの種類があります。

- 終日

  …こちらの設定により、いかなる時間であっても申請に対しては自動的に承認されます。

- 時間帯指定

  …曜日ごとに自動承認する時間帯を設定できます。一つの曜日で最大 3 つまでの時間帯を設定可能です。例えば土日、祝日にて設定いただけます。

- チケット ID

  …チケット管理システムと連携することで、チケット ID によって自動承認します。

図 68 自動承認

8 - 2　リソース単位でのアクセス制御設定

リソースごとにアクセス制御を設定する方法について紹介します。

1. 「リソース」タブをクリックします。

2. アクセス制御を実装されたいリソースの「リソースアクション」をクリックします。

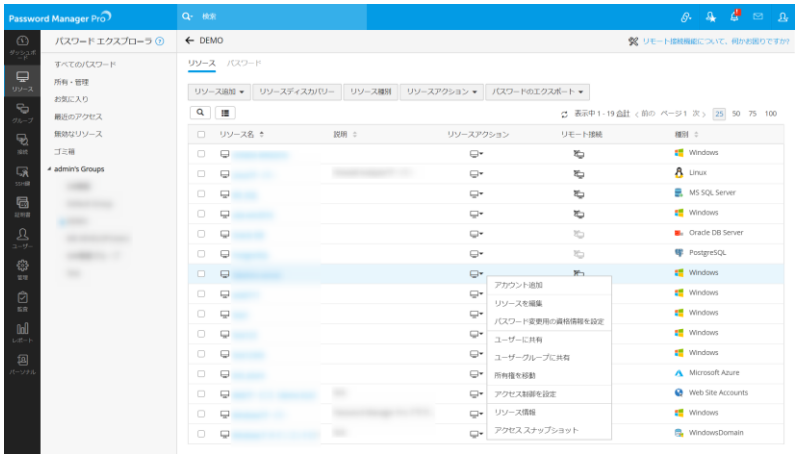


図 69　リソースアクション

3. 「アクセス制御を設定」をクリックします。

4. 8-1 アクセス制御設定項目を参照の上、要件に合った形で設定します。

5. 「保存＆アクティブ化」をクリックします。

> メモ：「非アクティブ化」をクリックすることで、アクセス制御の設定内容を保持したまま無効化することができます。

8 - 3　アカウント単位でのアクセス制御設定

ビルド 10500 以降アカウント単位でアクセス制御を設定することができるようになりました。サーバーの特権 ID に絞ってよりセキュアなアクセス制御を設定することが可能になります。設定方法については以下の通りです。

1. 「リソース」タブをクリックします。

2. アクセス制御を実装したいアカウントを含むリソース名をクリックします。

3. アクセス制御を実装されたいアカウントの「アカウントアクション」アイコンをクリックします。

4. 「アクセス制御を設定」をクリックします。

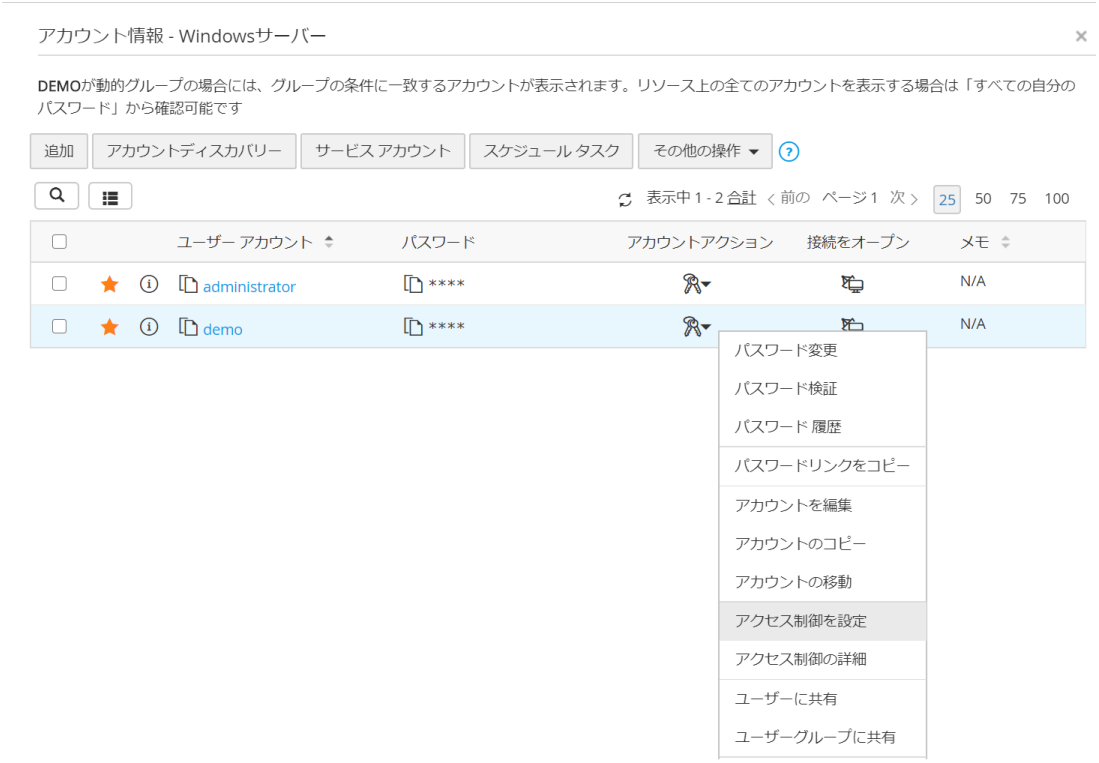


図 70 アクセス制御を設定

5. 8-1 アクセス制御設定項目を参照の上、要件に合った形で設定します。

6. 「保存＆アクティブ化」をクリックします。

7. 設定内容を「アカウントアクション」アイコン→「アクセス制御の詳細」から確認します。

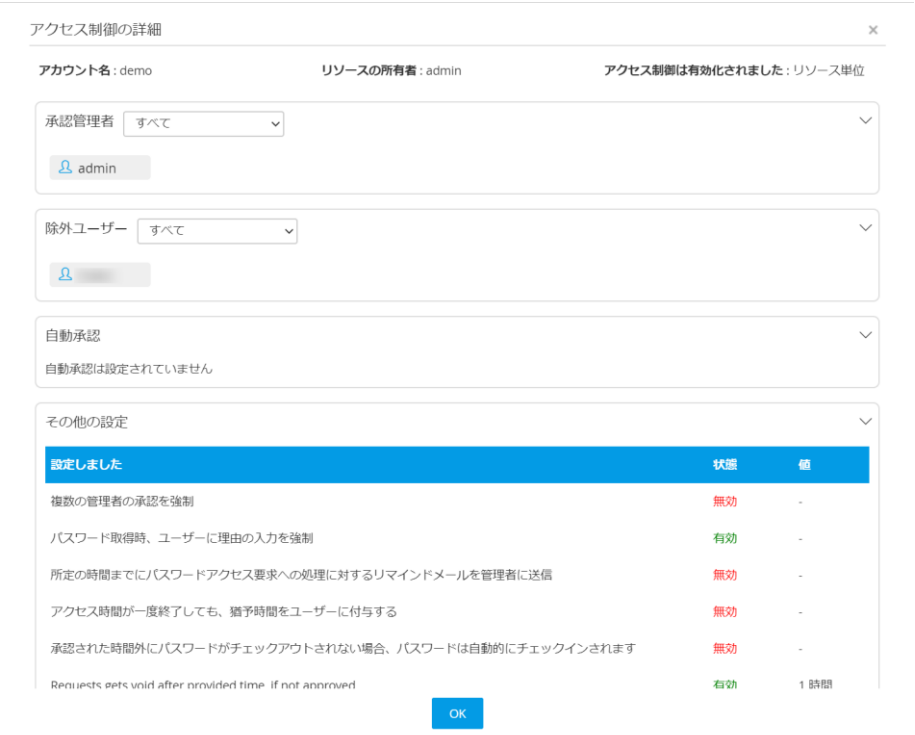


図 71 アクセス制御の詳細

メモ：アカウント単位でのアクセス制御はリソース単位のアクセス制御より優先度が高くなります。例えばあるリソースに対してアクセス制御が既に実装されていたとします。そのリソース内にてあるアカウントのみ特別に別のアクセス制御を実装したいと仮定します。その際にリソースに対して設定したアクセス制御はそのアカウントに対しては適用されず、そのアカウントに対して個別に設定したアクセス制御が適用されます。

9 リソース/リソースグループの共有

リソース/リソースグループを特定のユーザー/ユーザーグループに共有することで共有されたユーザー/ユーザーグループはそのリソースを利用することができるようになります。

リソースの共有する際に管理者は共有するユーザー/ユーザーグループに対してどの程度の権限を与えるのか選択できます。

Password Manager Pro では 3 つの共有レベルを用意しています。

- □ パスワードの表示
  …共有されたパスワードを利用できるようになります。

- □ パスワードの変更
  …共有されたパスワードを利用・変更できるようになります。

- □ フルコントロール
  …共有されたパスワードを利用・変更できるようになります。

9 - 1 リソースを共有

1. 「リソース」タブをクリックします。

2. 共有したいリソースの「リソースアクション」アイコンをクリックします。

3. 「ユーザーに共有」または「ユーザーグループに共有」をクリックします。

図 72 ユーザーに共有

メモ：複数のリソースを一括してユーザー/ユーザーグループに共有することも可能です。その際には各リソースのチェックボックスにチェックを入れ、「リソースアクション」>>共有へと進んでください。

図 73 一括でユーザーに共有

メモ：フルコントロールの権限で共有するためには共有されるユーザーが特権管理者、管理者、パスワード管理者であることが必要です。

4. 「アクセス権の付与」をクリックし、共有権限を選択して共有します。

図 74 アクセス権の付与

5. 共有されたユーザーでログインし、リソースを確認します。

メモ：権限に応じて共有されたリソースに対する実行可能なアクションが異なります。

図 75 パスワードの表示

図 76 パスワードの変更

図 77 パスワードの管理

9 - 2 リソースグループを共有

リソースをまとめてリソースグループとして、グループ単位で共有することも可能です。

1. 「グループ」タブをクリックします。

2. 共有したいリソースグループの「アクション」アイコンをクリックします。

3. 「ユーザーに共有」または「ユーザーグループに共有」をクリックします。

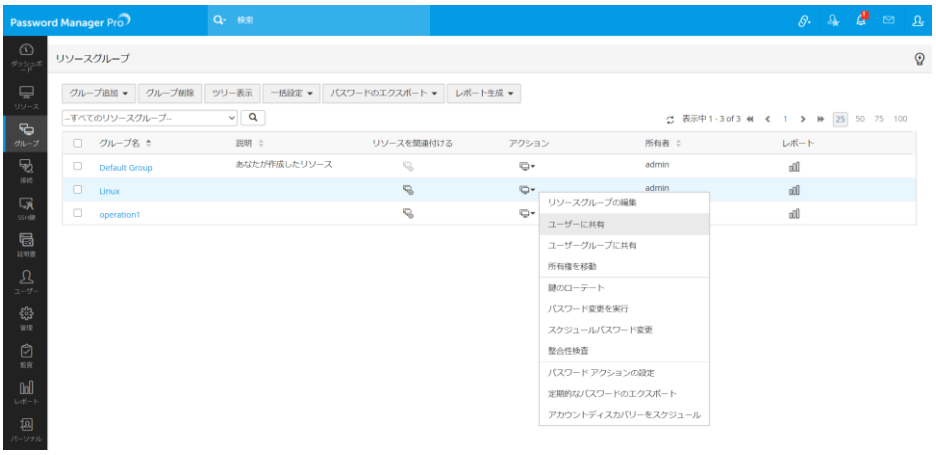


図 78 ユーザーに共有

メモ：複数のリソースグループを一括してユーザー/ユーザーグループに共有することも可能です。

図 79 一括でユーザーに共有

メモ：フルコントロールの権限で共有するためには共有されるユーザーが特権管理者、管理者、パスワード管理者であることが必要です。

4. 「アクセス権の付与」をクリックし、共有権限を選択して共有します。

図 80 アクセス権の付与

5. 共有されたユーザーでログインし、リソースグループを確認します。

図 81 共有されたリソースグループ

9 - 3 アカウントを共有

同じリソースの複数のアカウントをそれぞれ別のユーザーに共有することも可能です。以下の設定ではアカウントごとに共有先を設定します。

1. 「リソース」タブをクリックします。

2. 共有したいアカウントが含まれるリソース名をクリックします。

3. 共有したいアカウントの「アカウントアクション」アイコンをクリックします。

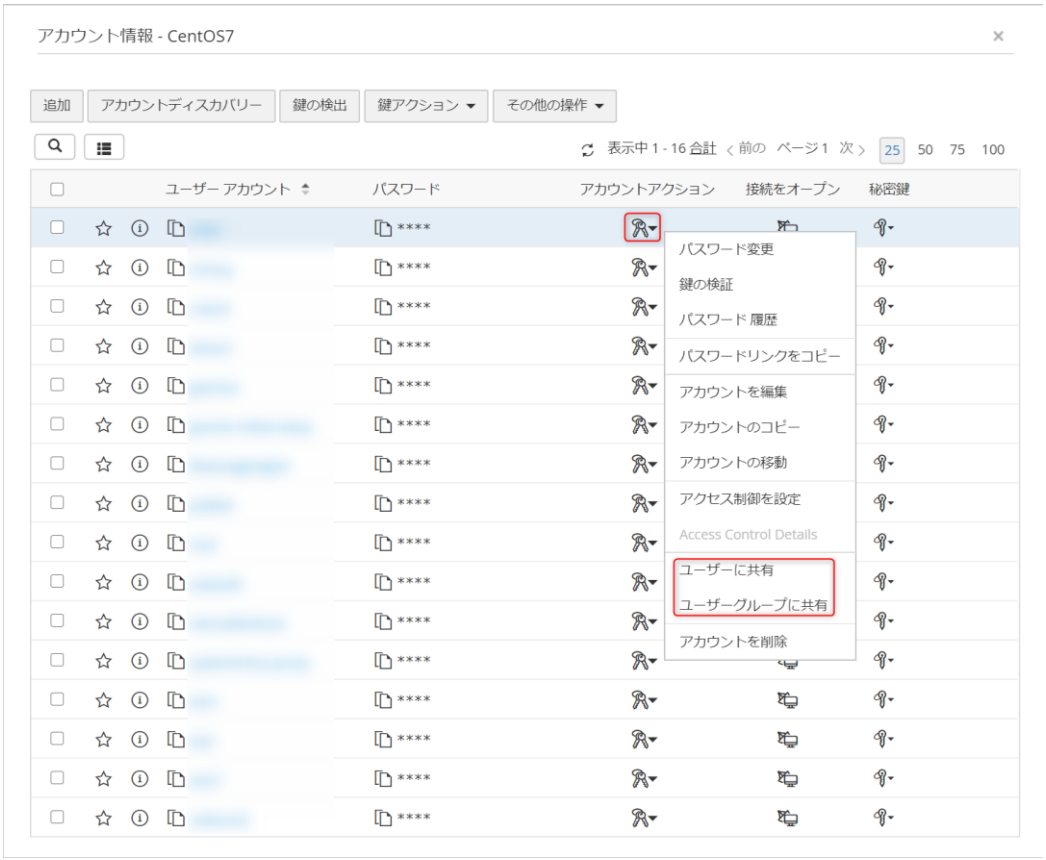


図 82 アカウントアクション

4. 「ユーザーに共有」または「ユーザーグループに共有」をクリックします。

メモ：複数のアカウントを一括してユーザー/ユーザーグループに共有することも可能です。

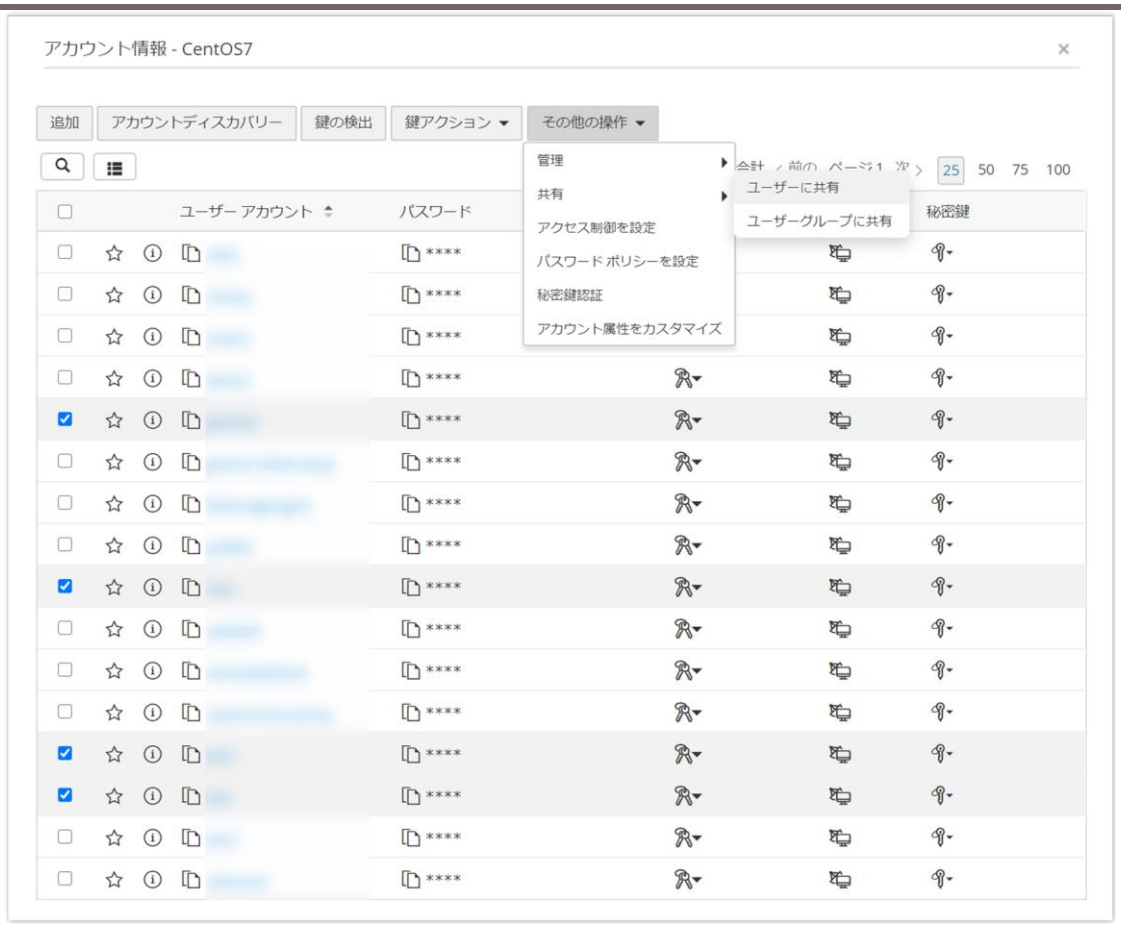


図 83 一括でユーザーに共有

5. 「アクセス権の付与」をクリックし、共有権限を選択して共有します。

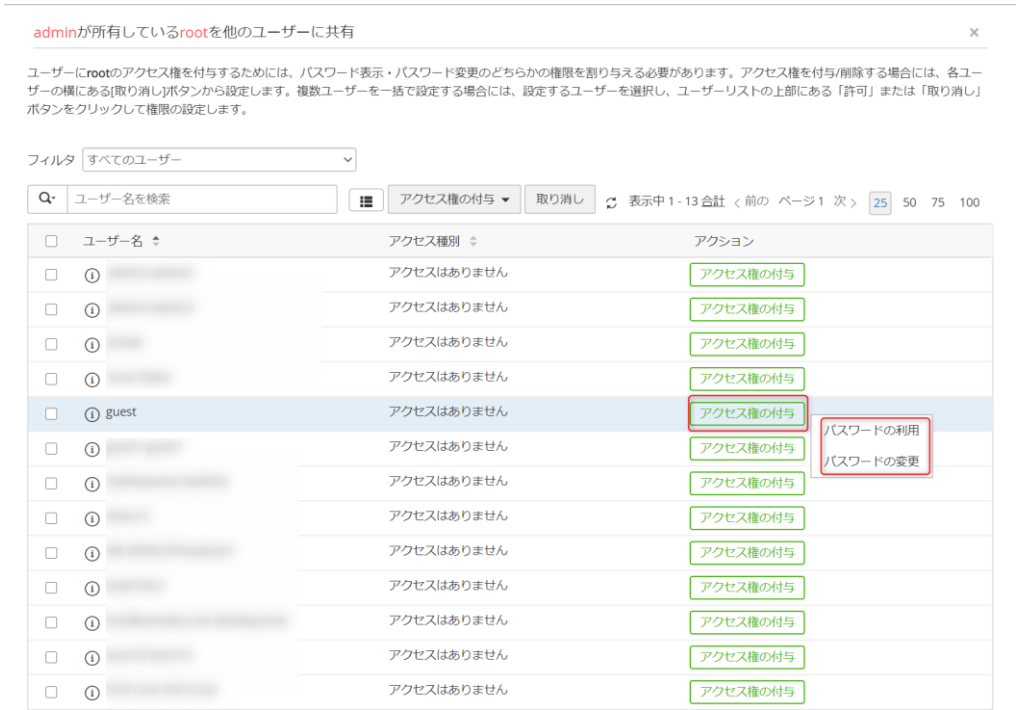


図 84 アクセス権の付与

6. 共有されたユーザーでログインし、リソースグループを確認します。

10 申請・承認のワークフローの流れ

前章まで設定いただけますと申請・承認のワークフローを運用することができます。以下実際のワークフローの流れについて説明します。

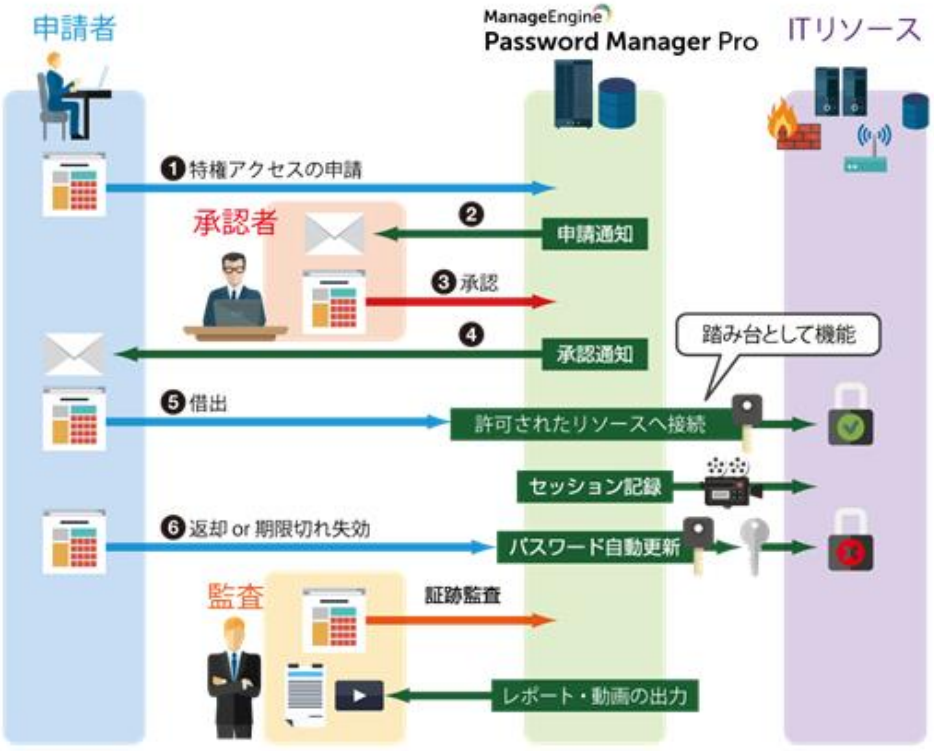


図 85 申請承認のワークフローの概要

１０-１ 申請者からの申請

1. 「リソース」タブをクリックします。

2. 申請したいアカウントを含むリソース名をクリックします。

3. 申請予定のアカウントのパスワード欄にて記載している[要求]をクリックします。

図 86 アカウント情報

4. 任意でコメントを記入し、「送信」をクリックします。即時の承認を求める場合には、「今」を選択します。

図 87 パスワードを要求(今)

5. 日時指定して承認する場合には、「後で」を選択します。

図 88 パスワードを要求(後で)

メモ：デフォルトの設定ではコメントは必須です。こちらの設定を解除するためには、リソース/アカウントに設定されているアクセス制御設定にて「**パスワードを取得する際に理由の入力を強制**」を無効化する必要があります。詳細につきましては 8 アクセス制御の設定をご確認ください。

6. 表示が「承認待ち」に変わります。

図 89 承認待ち

１０-２ 承認者への通知

申請者から申請されると承認者に対してメールが通知されます。その後、Password Manager Pro へログインして、その申請を処理してください。

1. 画面右上のベルアイコンをクリックします。

図 90 パスワードアラート

2. 「1 パスワードアクセス要求」をクリックします。

メモ：「管理」タブ→「管理」欄→パスワードアクセス要求からも確認できます。

１０-３ 承認者の承認/拒否

1. パスワードアクセス要求から申請内容を確認した後に、「要求」をクリックします。

図 91 パスワードアクセス要求

2. 理由を任意で記載し、「承認」または「拒否」をクリックします。

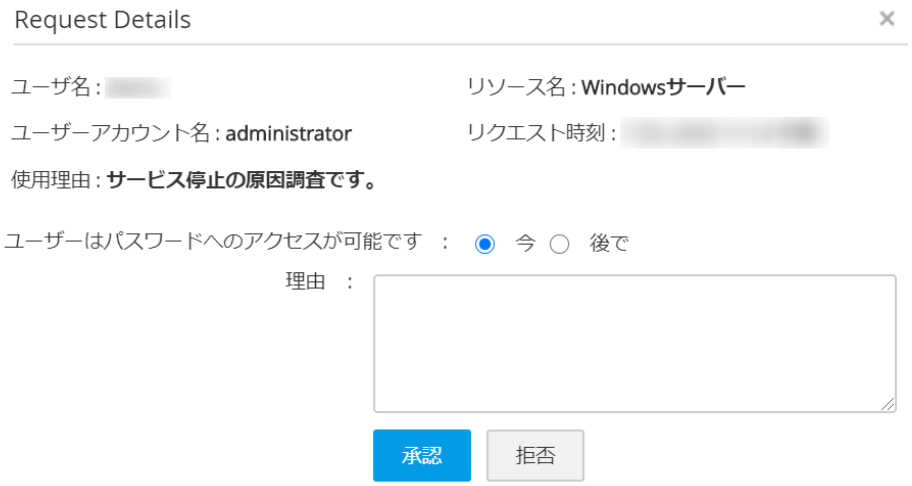


図 92 申請内容

メモ：「後で」を選択して、時刻指定した形で承認することもできます。申請者が指定した時刻とは異なる時刻を指定することもできます。

3. パスワードアクセス要求画面の[アクション]で、表示が[未使用]となります。

図 93 承認後のステータス

メモ：一旦承認した場合でも「チェックイン」ボタンをクリックすることでパスワードを強制的に返却させることができます。

１０-４ 申請者への承認/拒否通知/チェックアウト

申請が承認/拒否された際には申請者に対して通知メールが送信されます。拒否された場合はアカウントのパスワード欄にて記載しているステータスが[要求]へと代わります。以下、承認された際の手順について解説します。

1. 「リソース」タブをクリックします。

2. 申請したアカウントを含むリソース名をクリックします。

3. 申請したアカウントのパスワード欄の「チェックアウト」をクリックします。

図 94 アカウント情報

4. [チェックアウト]すると当該ユーザーアカウントでリソースにアクセス可能となります。

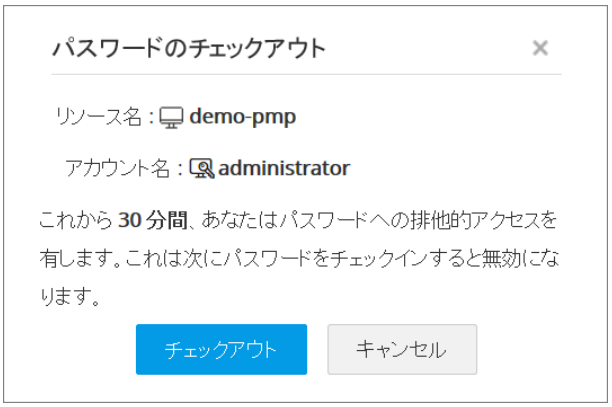


図 95 チェックアウト

5. [パスワード]で、表示が[チェックイン]に変わります。

図 96 パスワードの払い出し

メモ： パスワード欄の＊＊＊＊をクリックすることでパスワードが表示されます。役割が**特権管理者、管理者、パスワード管理者以外**のユーザーに対してパスワードが払い出された際に、パスワードをマスキング(＃ ＃ ＃ ＃)し非表示にすることも可能です。

図 97 パスワードのマスキング

設定方法は以下の通りです。

1. 「管理」タブ>>「セットアップ」欄>>一般設定>>「パスワード取得」タブへと進む
2. 「自動ログオン設定済みのパスワードをユーザーが取得を許可」のチェックを外す
3. 「保存」をクリックします

１０-５ パスワードの借り出し

1.「接続をオープン」欄のマシンアイコンをクリックします。

2.[Windows Remote Desktop]をクリックします。

図 98 接続をオープン

3. 別タブで RDP 接続が開始されます。

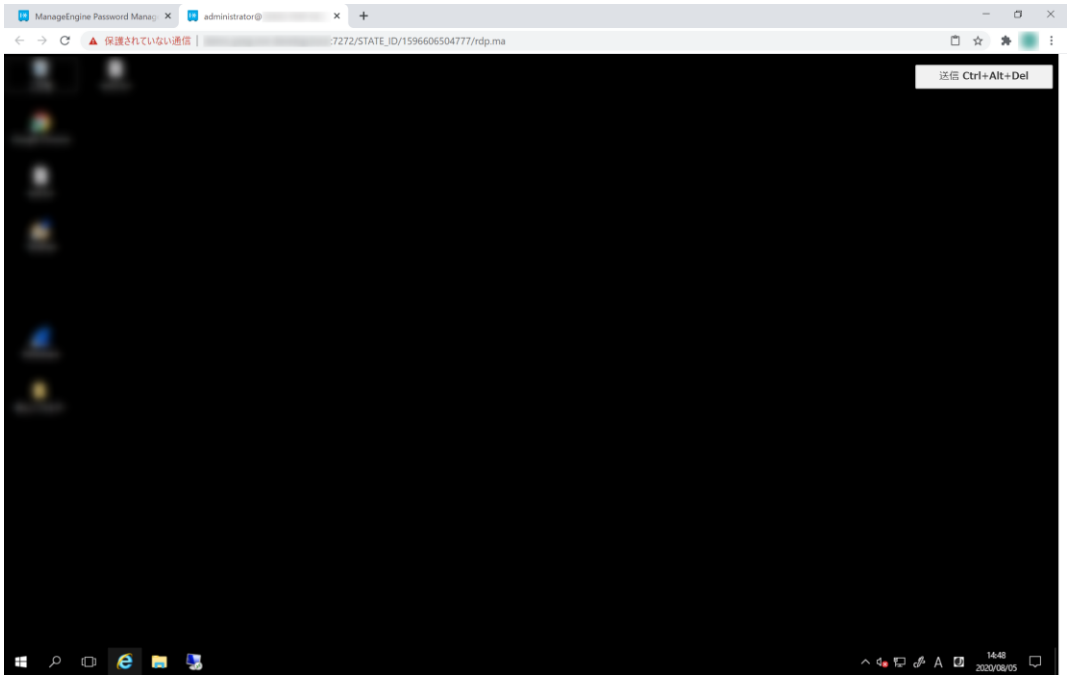


図 99 Windows Remote Desktop セッション

メモ：RDP 接続タブには「アカウント名@FQDN/IP アドレス」が記載されています。FQDN/IP アドレスはリソースを追加した際に設定した内容となります。

メモ：「監査」タブ>>「アクティブなリモートセッション」へ進むと、現時点で実施しているリモートセッションの一覧を確認することができます。あるセッションにて「参加」アイコンをクリックすると、当該のセッションの様子をリアルタイムで確認できます。またユーザーが不審な動作を行った際などに対して管理者は「終了」アイコンをクリックし、セッションを強制的に時刻指定した形で承認することもできます。申請者が指定した時刻とは異なる時刻を指定することもできます。

図 100 アクティブなリモートセッション

１０-６ パスワードの返却

1.[パスワード]で、[チェックイン]をクリックします。

メモ：サーバー側でサインアウトする、またはブラウザーの[×]ボタンをクリックすることでもセッションを終了できます。

図 101 チェックイン

2.[パスワード]で、表示が[要求]に変わります。

図 102 チェックイン後

メモ： チェックイン時に自動的にパスワードを変更させることもできます。アクセス制御設定のデフォルトの設定では変更するにチェックが入っています。変更する場合には以下の手順となります。

1. 当該のリソースの「リソースアクション」アイコンをクリックします。
2. 「アクセス制御を設定」をクリックします。
3. 「その他の設定」タブへ進み、「排他的使用の後(他のユーザーによってチェックインする場合)に、パスワードを変更」のチェックを外します。
4. 「保存＆アクティブ化」をクリックします。

メモ： ブラウザーの拡張機能を利用することで Password Manager Pro の Web コンソールにアクセスすることなく申請承認のワークフローを回すことができます。

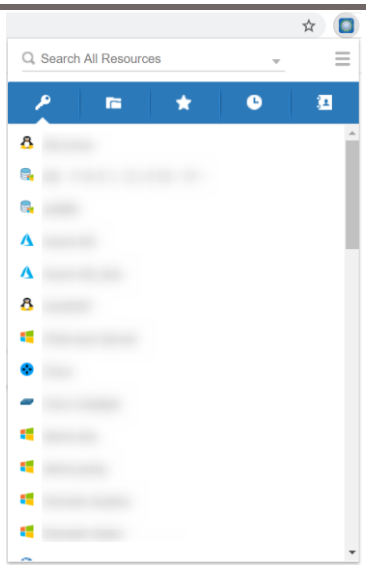


図 103 ブラウザーの拡張機能

またアンドロイド＆iOS それぞれに対応した Password Manager Pro アプリを利用することでスマートデバイス上から申請承認のワークフローを回すことができます。

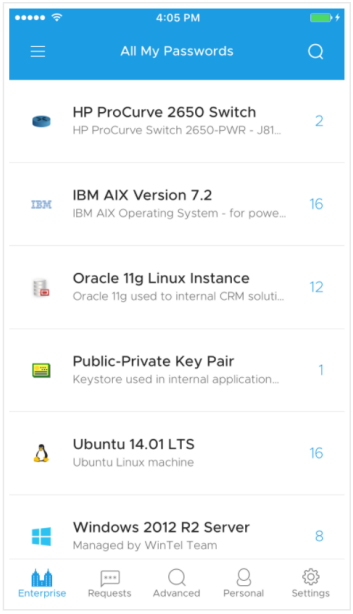


図 104 モバイルアプリ

1 1 記録済みセッションの管理

下記の図のように、Password Manager Pro 経由でパスワード管理対象リソースにリモート接続し、リモート接続時の操作内容をセッション記録として取得可能です。Windows では動画、Linux、DB、ネットワーク機器等ではコマンドをテキストとして取得します。

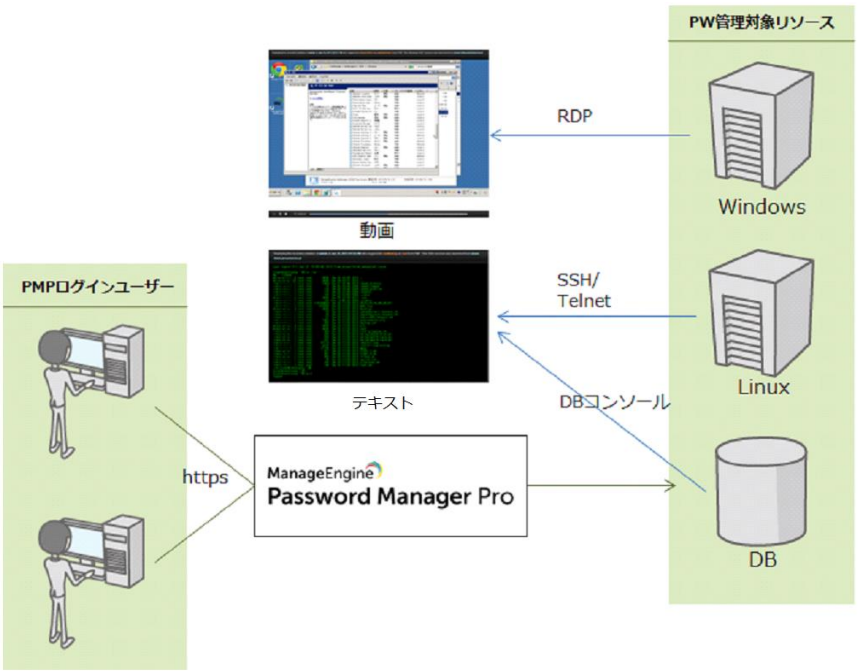


図 105 記録済みセッションの取得

メモ： 動画ファイルは 1 分あたり約 1 MB の容量を消費します。ただし、画面操作がない場合には静止画として取得します。

１１-１ セッションレコーディング設定

「管理」タブ→「設定」欄→セッションレコーディング(「監査」タブ→「記録済みセッション」タブ→セッションレコーディング設定)へ進みますと、セッションレコーディングに関する設定を行えます。

図 106 セッションレコーディング設定

設定内容としては以下の 3 つとなります。

- 各種セッション記録の有効化/無効化
  …デフォルトではチェックボックスにチェックが入っている状態で、有効化されています。チェックを外すことでセッションは開始してもレコーディングはしない設定が可能です。

- 記録済みセッションの保存先
  …UNC 形式で保存先パスを指定可能です。

- 記録済みセッションの保存期間
  …日数単位で保存期間を設定できます。無期限の場合には 0 を入力してください。

メモ： 記録済みセッションのバックアップ保存先を指定し、双方に記録済みセッションファイルを保存可能です。ただし、メインの記録済みセッション保存先のパスに保管できない場合、Password Manager Pro は記録済みセッションのバックアップ保存先に保存されず、デフォルトの保存先(<PMP>¥recorded_files)に保管される仕様です。

１１-２ 記録済みセッションの再生方法

1. 「監査」タブをクリックします。

2. 「記録済みセッション」をクリックします。

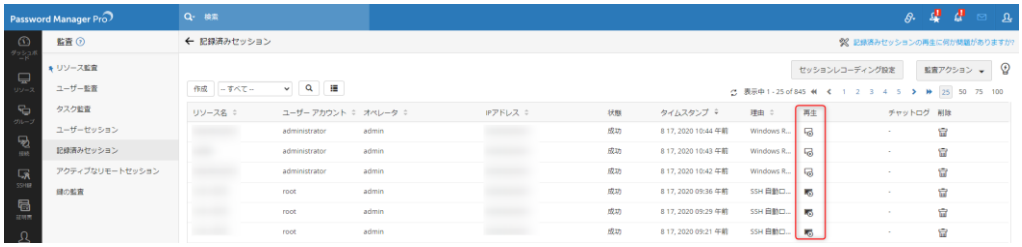


図 107 記録済みセッションの再生

3. 「再生」アイコンをクリックします。

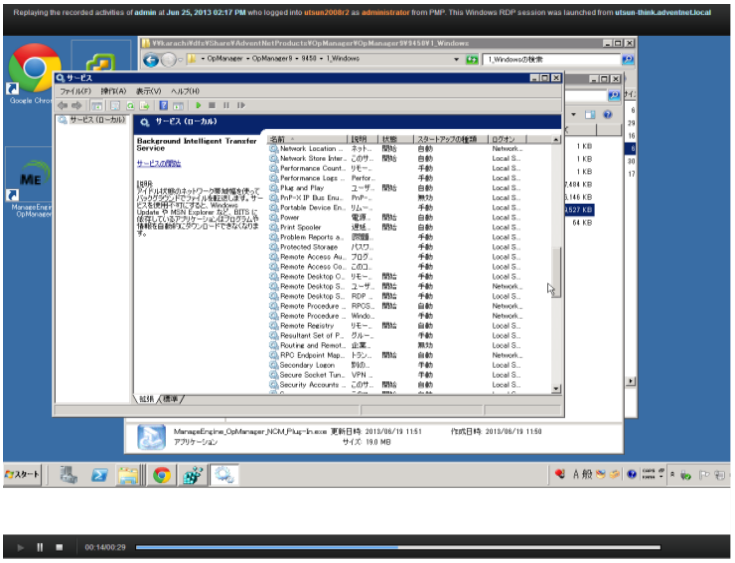


図 108 再生画面(RDP)

メモ： 記録済みセッションファイル(.rdpv ファイル、sshv ファイル等)は生成された Password Manager Pro によって暗号化されています。つまり、Password Manager Pro のコンソール画面でのみ、記録済みセッションを再生することが可能です。また他の Password Manager Pro で再生することは暗号鍵が異なるためできません。

メモ： 管理者は「削除」アイコンをクリックすることで、各々の記録済みセッションファイルを手動で削除できます。ただし、他の管理者の承認が必要です。

１２ 各タブの機能概要

１２-１ ダッシュボードタブ

Password Manager Pro が管理するパスワード、Password Manager Pro ユーザー、SSH 鍵について、サマリーを表示します。ログイン直後に表示され、直観的に利用状況を把握できます。

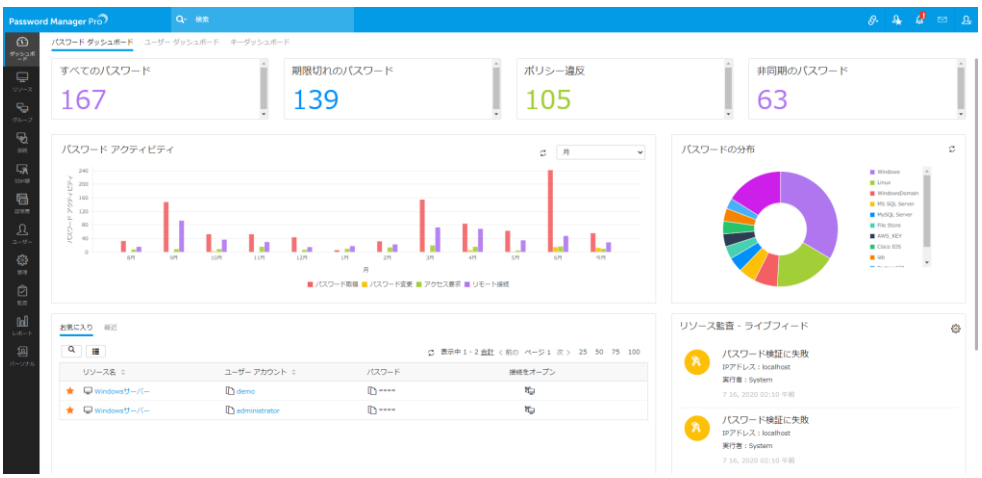


図 109 ダッシュボードタブ

１２-２　リソースタブ

Password Manager Pro で管理しているリソースの一覧を確認できます。パスワード変更やリソースの共有、アクセス制御設定などリソースの設定に関わるものは全てこちらのタブで設定します。

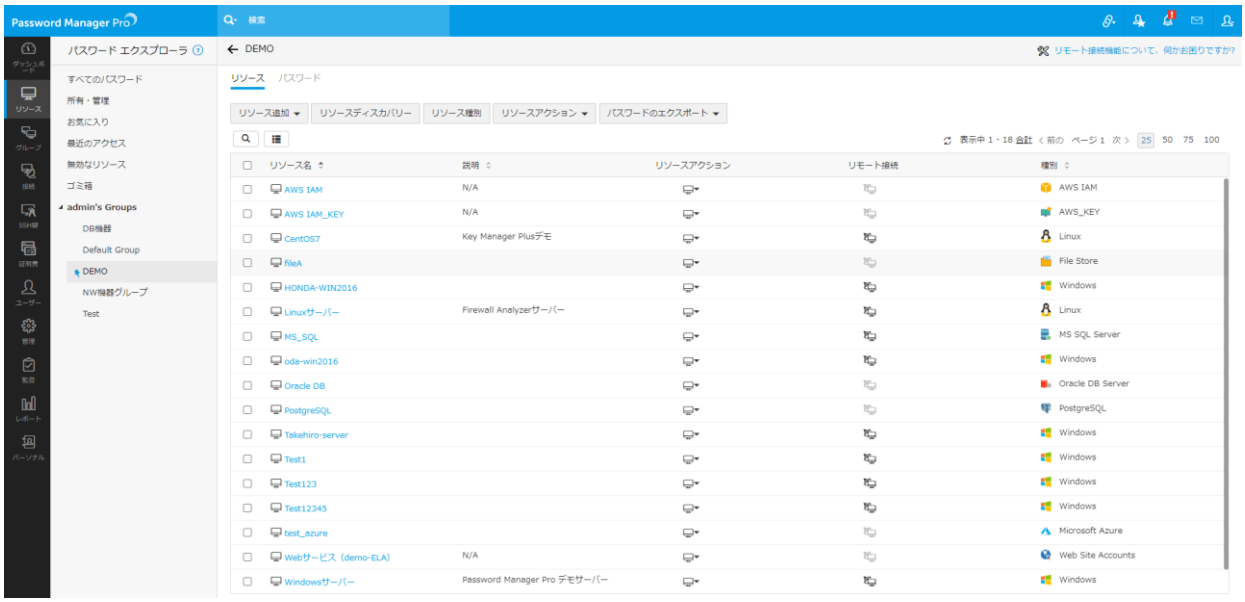


図 110　リソースタブ

１２-３　グループタブ

リソースを管理区分に沿ってまとめることができます。作成されたリソースグループに対してユーザーにまとめて共有し、定期パスワード変更等のアクションを設定できます。

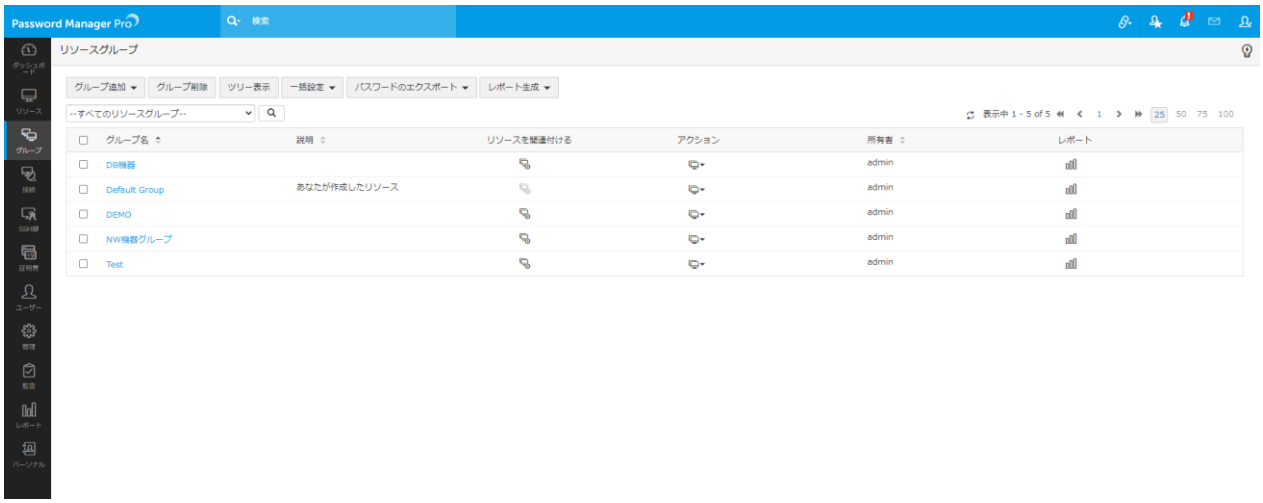


図 111　グループタブ

１２-４　接続タブ

管理対象サーバーに接続する際に利用します。

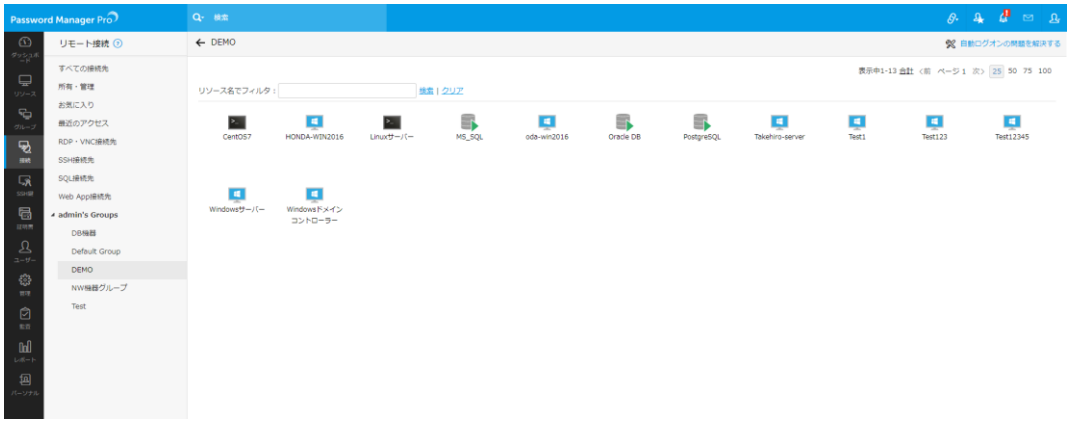

Password Manager Pro
検索
リモート接続
すべての接続先
所有・管理
お気に入り
最近のアクセス
RDP・VNC接続先
SSH接続先
SQL接続先
Web App接続先
admin's Groups
DB機器
Default Group
DEMO
NW機器グループ
Test
DEMO
自動ログオンの問題を解決する
リソース名でフィルタ：
検索 | クリア
CentOS7
HONDA-WIN2016
Linuxサーバー
MS_SQL
oda-win2016
Oracle DB
PostgreSQL
Takehiro-server
Test1
Test123
Test12345
Windowsサーバー
Windowsドメイン
コントローラー

図 112 接続タブ

１２-５　SSH 鍵タブ

SSH 鍵の管理をこちらのタブから行います。SSH 鍵の作成、サーバーへの関連付け等も実施することができます。

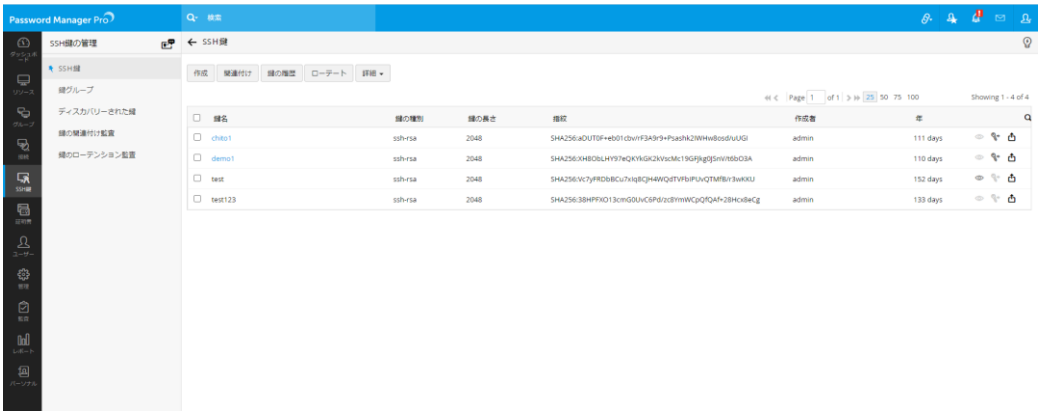


図 113 SSH 鍵タブ

１２-６　証明書タブ

SSL/TLS 証明書の管理をこちらのタブから行います。証明書の保管のみならず、既存の証明書のディスカバリー、CSR の作成、外部 CA との連携による署名等も実行できます。

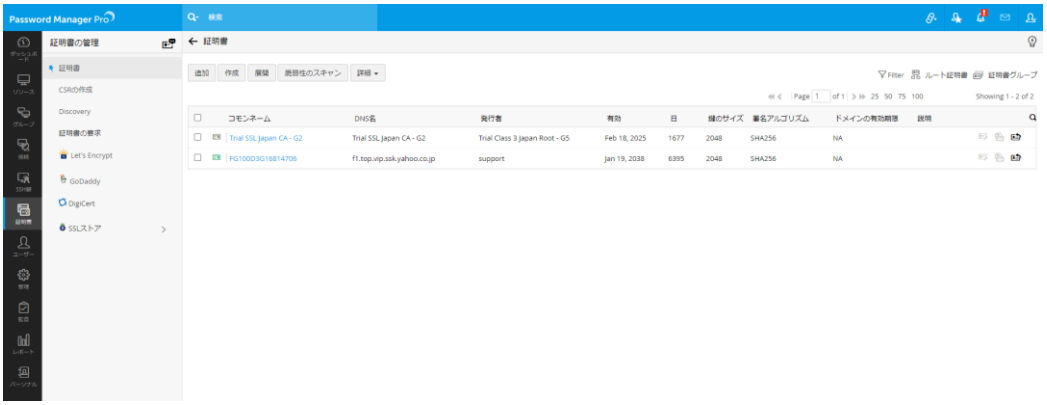


図 114　証明書タブ

メモ：Password Manager Pro ではデフォルトで 25 キー分のライセンスを用意しております。SSH 鍵と証明書はそれぞれ 1 つで 1 キー分のライセンスを消費します。25 キー分以上のライセンスの追加を希望されている場合には、弊社営業部(jp-mesales@zohocorp.com)までお問い合わせください。

１２-７　ユーザータブ

Password Manager Pro へログインするユーザーの管理をこちらのタブにて行います。各ユーザーの編集や役割の変更ができます。また AD、Azure AD と連携してインポートすることもできます。

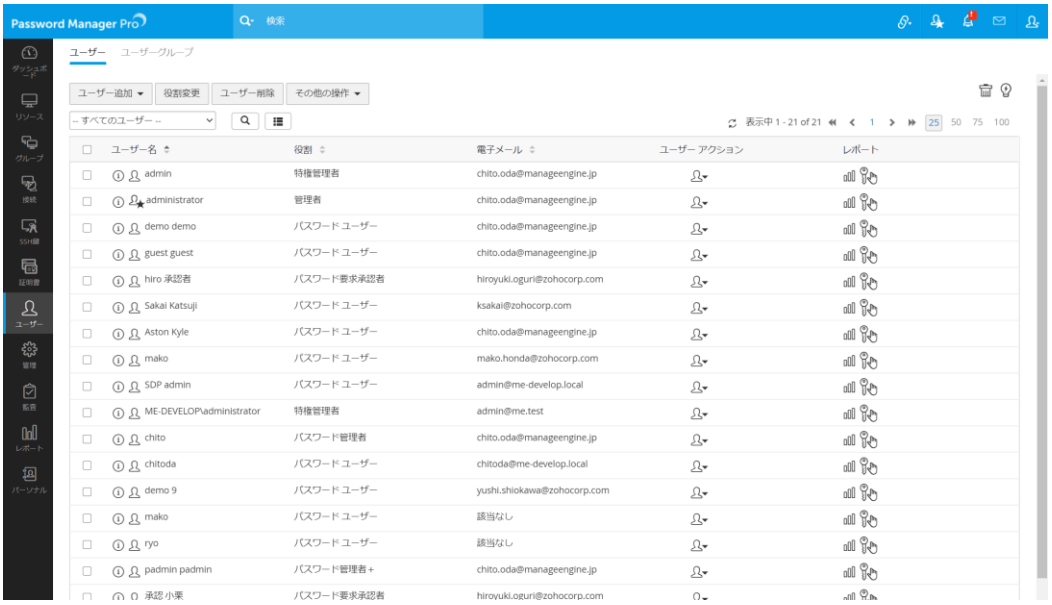


図 115 ユーザータブ

１２-８ 管理タブ

Password Manager Pro に対する各種設定を行います。です。このタブは原則として管理者の方のみ編集可能になります。

1. **認証**
   Password Manager Pro にログインする際の認証方式を強化できます。Active Directory 認証のみならず、RADIUS 認証、LDAP 認証、SAML シングルサインオン、スマートカード認証、二段階認証に対応しております。

2. **カスタマイズ**
   Password Manager Pro を利用するにあたって環境に即したカスタマイズ可能です。パスワードポリシー、ユーザーの役割等を編集できます。

3. **セットアップ**
   製品全体に関わる一般的な設定はこちらから行えます。

4. **SSH/SSL**
   SSH 鍵、SSL/TLS 証明書の管理に関する設定を行えます。

5. **設定**
   製品のバックエンド側の設定を行えます。データベースのバックアップ、HA 構成等もこちらから確認できます。

6. **管理**
   本製品のセキュリティに関する設定やパスワードアクセス要求等を確認できます。

7. **連携**
   サードパーティ製品や他の ManageEngine 製品との連携を実施できます。

8. PMP Agents

Password Manager Pro Agent をダウンロードできます。

図 116 管理タブ

メモ：Password Manager Pro Agent を管理対象サーバーにインストールすることで https 通信によるパスワード管理が可能です。Linux サーバーに Password Manager Pro をインストールし、かつリソースとして Windows OS のパスワード管理を実施したい場合には Agent をインストールする必要があります。その他、パスワード管理に必要なポートの開放ができない場合(リソースが DMZ にある等)でもご利用可能です。

１２-９ 監査タブ

管理対象へのインストール状況の確認や、リモート環境へのインストール、Active Directory 環境における新規加入 PC への自動インストールなどを設定します。

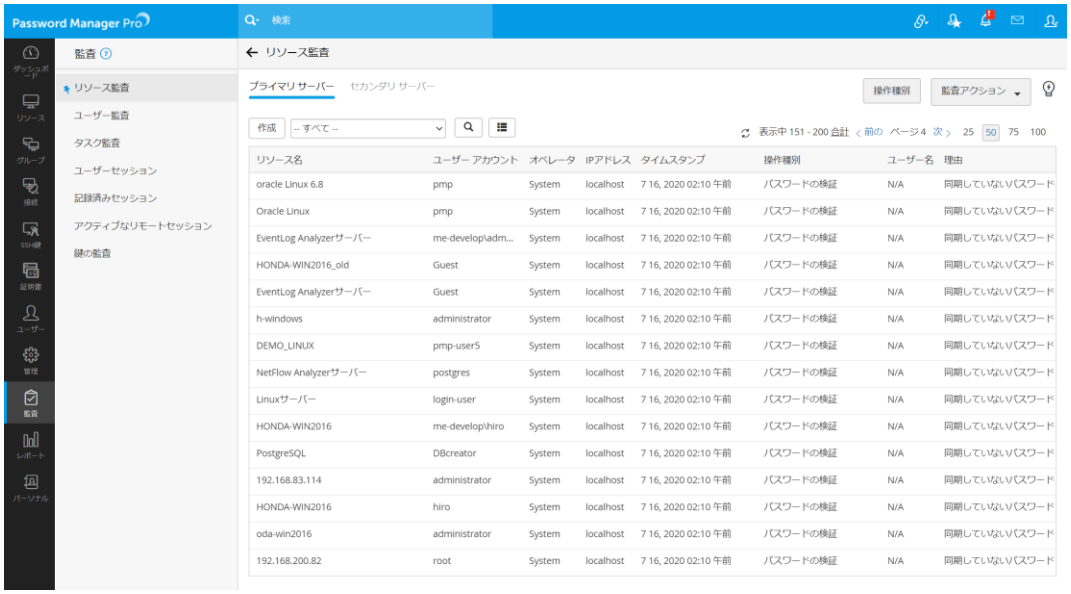


図 117 監査タブ

１２-１０ レポートタブ

定期的にパスワードの利用状況やユーザーの活動状況をレポート化できます。また PCI DSS 等の認証機関に準拠した形式でレポートを出力することができます。クエリレポートによりカスタマイズ可能です。

図 118 レポートタブ

１２-１１ パーソナルタブ

Password Manager Pro ユーザー個人の情報を保管できます。デフォルトで Web アカウント情報、銀行口座、クレジットカード情報、連絡先情報を管理できます。その他のフィールドも個人でカスタマイズ可能です。

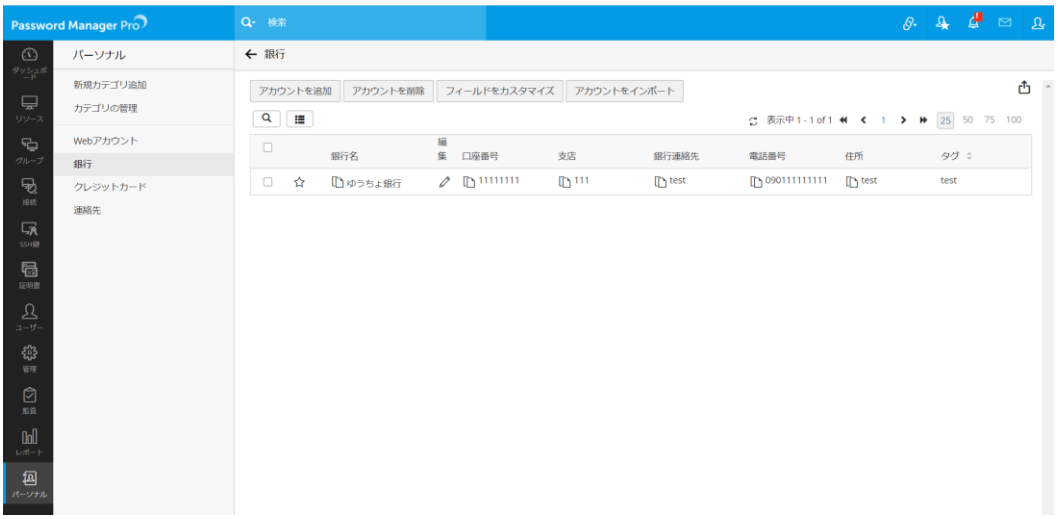


図 119 パーソナルタブ

１２-１２ 権限毎に表示可能なタブ

権限	管理者/特権管理者	パスワード管理者	パスワード監査担当者	パスワードユーザー
ダッシュボード	○	×	○	×
リソース	○	○	○	○
グループ	○	○	×	×
接続	○	○	○	○
SSH 鍵	○	○		
証明書	○	○		

ユーザー	○	×	×	×
管理	○	○	×	×
監査	○	×	○	×
レポート	○	×	○	×
パーソナル	○	○	○	○

メモ：特権管理者と管理者は次の 2 点で異なります。

- 緊急対策
- IP アドレス制御

特権管理者は製品全体のセキュリティ設定に対する権限が付与されている点で管理者よりも高権限です。

１３　製品のお問い合わせ先

評価版の使用期間 / 製品ご購入後の技術サポートは、以下のリンクよりご利用ください。

評価版サポート

https://www.manageengine.jp/support/trial.html

製品ご購入後のサポート

https://www.manageengine.jp/support/purchased.html

Password Manager Pro に関するご質問、ご購入は、下記までお問い合わせください。

製品提供元

ゾーホージャパン株式会社
神奈川県横浜市西区みなとみらい 3-6-1 みなとみらいセンタービル 13 階
Tel: 045-319-4612（ManageEngine 営業担当）
Web サイト: https://www.manageengine.jp/products/Password_Manager_Pro/
E-mail: jp-mesales@zohocorp.com