



# ツールを活用してAD管理者IDの 管理・監視を効率的に

ゾーホージャパン株式会社 ManageEngine & WebNMS事業

# Agenda

---

## 1. 特権アカウントの洗い出し

(ADManager Plus)

## 2. 「申請/承認フロー」を使用した特権ID管理

(Password Manager Pro)

## 3. イベントログの可視化と検知

(ADAudit Plus/EventLog Analyzer)

## 4. まとめ

# Agenda

1. 特権アカウントの洗い出し  
(ADManager Plus)

2. 「申請/承認フロー」を使用した特権ID管理  
(Password Manager Pro)

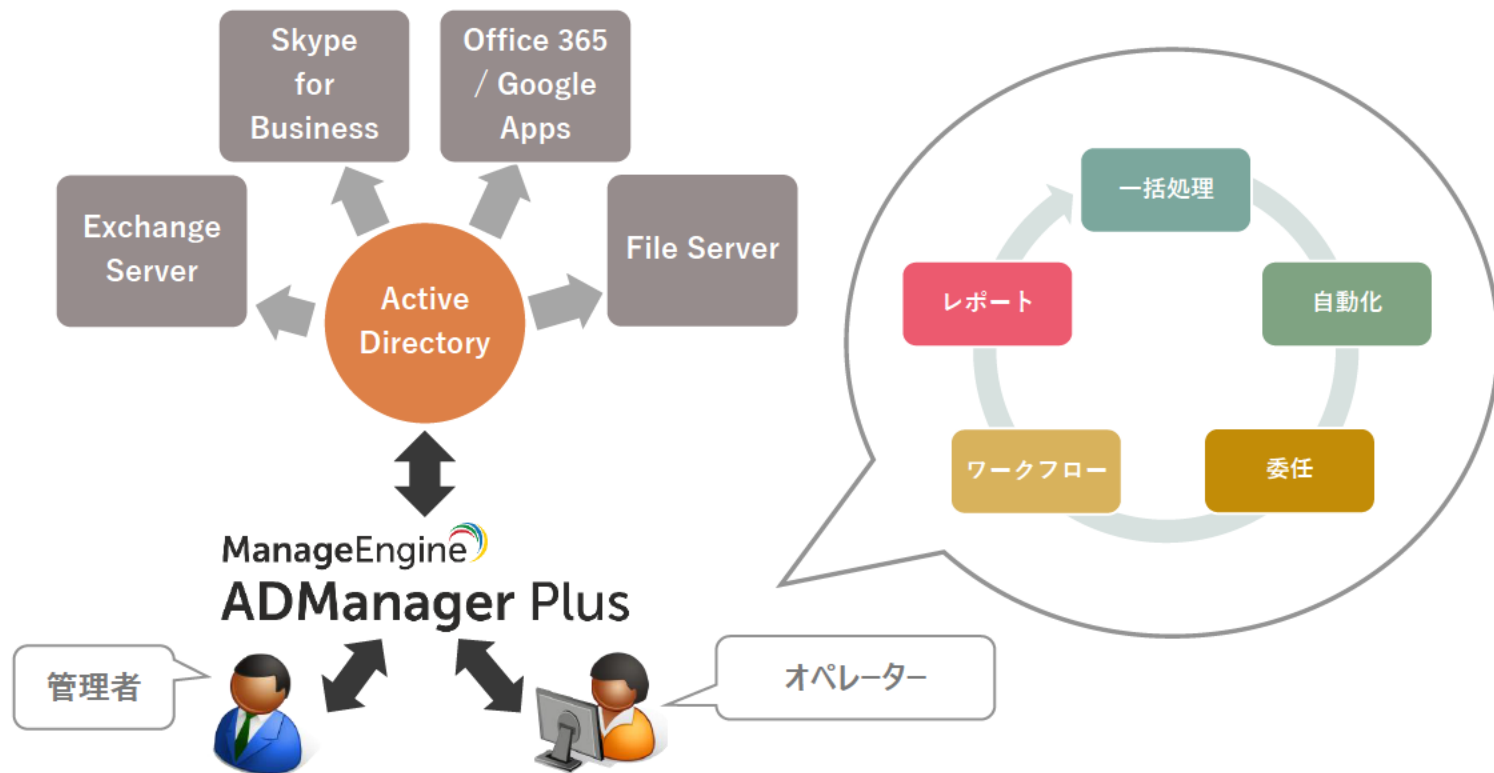
3. イベントログの可視化と検知  
(ADAudit Plus/EventLog Analyzer)

4. まとめ

# 1. 特権アカウントの洗い出し

## ADManager Plus

- Active Directory をより簡単に操作できる **Active Directory 管理 & レポートツール**
- Active Directory の操作権限を適切な担当者に **委任** することが可能





# 1. 特権アカウントの洗い出し

## ADManager Plus

ADオブジェクトなどの新規作成、一括更新、削除といった管理作業をGUI、CSVインポートで簡単操作



Office 365  
Google Apps

- ✓ AD + クラウドアカウントの作成
- ✓ Office 365 ライセンス割当て



Active Directory  
Exchange Server

- ✓ オブジェクト作成、更新
- ✓ 所属グループの変更
- ✓ メールの管理
- ✓ パスワード管理



File Server

- ✓ フォルダーアクセス権の変更

ADManager Plus ようこそ admin [ログアウト](#), [私のアカウント](#), [ジャンプ](#) ライセンス | ヘルプ | トークバック  
 AD オブジェクトの検索 ドメイン設定 | AD エクスポート

ホーム AD管理 **レポート** オペレーター ワークフロー 自動化 管理 サポート

ユーザー レポート パスワード レポート グループ レポート コンピューター レポート Exchange レポート GPOLレポート OUIレポート 他のレポート

エクスポート スケジュール

**選択したグループに所属しているユーザー** 入力情報 スケジュール

指定したグループに所属するすべてのユーザーを表示 [詳しい情報...](#)

ドメインの選択:    
 グループ:  [選択](#)   
 入れ子のグループを除く [詳細グループメンバーに関するレポート](#)

所属するグループ:  生成日: 2018-04-18 16:27:57 列の編集

クイック検索

	表示名 ▲	SAMアカウント名	アカウントの状態	作成日時	変更日時	所属するグループ	プライマリグループ
<input type="checkbox"/>	homura	homura	有効	2016-09-21 16:11:33	2018-03-14 13:44:27	Domain Users; 1G; 2G	Domain Users

1ページの表示件数:  1 - 1 / 1

# 選択したグループに所属しているユーザーのレポート



入力情報

スケジュールレポート

最近ログオンしていないユーザー

指定日数以内にログオンしていないユーザーを表示 [詳しい情報...](#)

ドメインを選択:  me-develop.local

manageengine.yokohama

OUを選択: 契約社員[me-de... [詳細情報](#) [OUを追加](#)

希望の時間範囲を選択:

一度もログオンしていないユーザーを除外する

無効ユーザーを除外する

作成 停止

生成日: 2018-04-16 12:10:06

列の編集

削除する リクエストを作成

クイック検索

1ページの表示件数: 100 1 - 9 / 9

	姓	名	表示名	SAMアカウント名	作成日時	ユーザーの最終ログオン日時	アカウントの状態	電子メールアドレス	説明	プライマリグループ
<input type="checkbox"/>	goro	saito	斉藤	saito	2018-02-26 14:33:19	0	有効	saito@me.test	-	Domain Users
<input type="checkbox"/>	hanako	tanaka	田中	tanaka	2018-02-26 14:33:20	0	有効	tanaka@me.test	-	Domain Users
<input type="checkbox"/>	ichiro	sato	佐藤	sato	2018-02-26 14:33:20	0	有効	sato@me.test	-	Domain Users
<input type="checkbox"/>	saburo	yoshida	吉田	yoshida	2018-02-26 14:33:20	0	有効	yoshida@me.test	-	Domain Users
<input type="checkbox"/>	siro	watabe	渡部	watabe	2018-02-26 14:33:20	0	有効	watanabe@me.test	-	Domain Users
<input type="checkbox"/>	taro	yamada	山田	yamada	2018-02-26 14:33:20	0	有効	yamada@me.test	-	Domain Users
<input type="checkbox"/>	yasuko	matsuda	松田	matsuda	2018-02-26 14:33:19	0	有効	matsuda@me.test	-	Domain Users
<input type="checkbox"/>	yoshiko	takada	高田	takada	2018-02-26 14:33:19	0	有効	takada@me.test	-	Domain Users
<input type="checkbox"/>	内田	健	内田	uchida	2018-02-28 17:04:15	0	有効	uchida@me-develop.local	-	Domain Users

1ページの表示件数: 100 1 - 9 / 9

# Agenda

---

1. 特権アカウントの洗い出し  
(ADManager Plus)

2. 「申請/承認フロー」を使用した特権ID管理  
(Password Manager Pro)

3. イベントログの可視化と検知  
(ADAudit Plus/EventLog Analyzer)

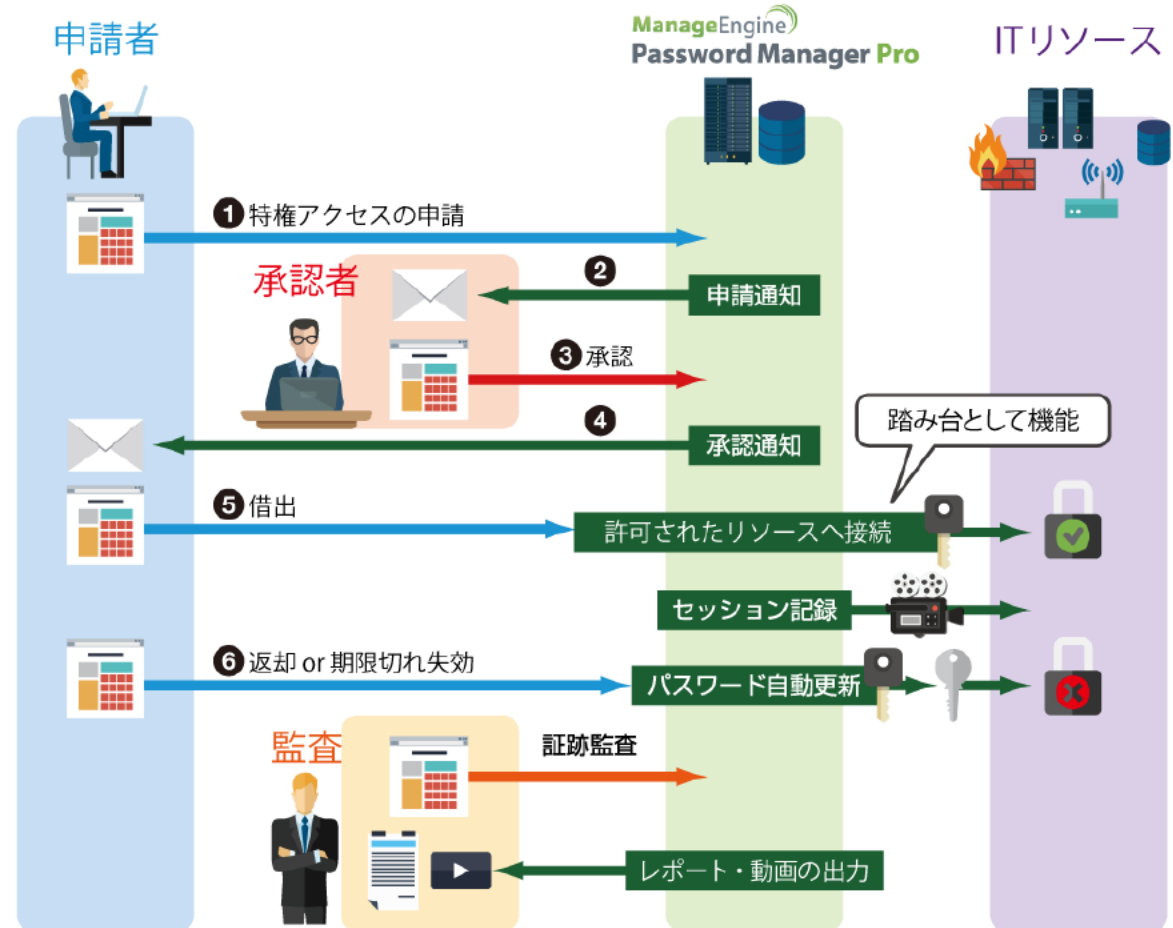
4. まとめ

## 2. 「申請/承認フロー」を使用した特権ID管理

### Password Manager Pro

#### 特権IDによるサーバー/NW機器のアクセス利用を管理

- ワークフロー機能によるパスワードの払い出し
- 踏み台機能による、証跡の管理
- パスワード自動変更によって不正アクセスを抑止





## Password Manager Pro

Password Manager Proは、特権IDアクセスの制御、管理、監視および監査を実現できるツールです。主に以下の3つの機能を提供しています。:

- 特権アカウントの管理
- リモートアクセスの管理
- セッションの管理

## ログイン

Username

Password

Log on to

[Forgot Password?](#)

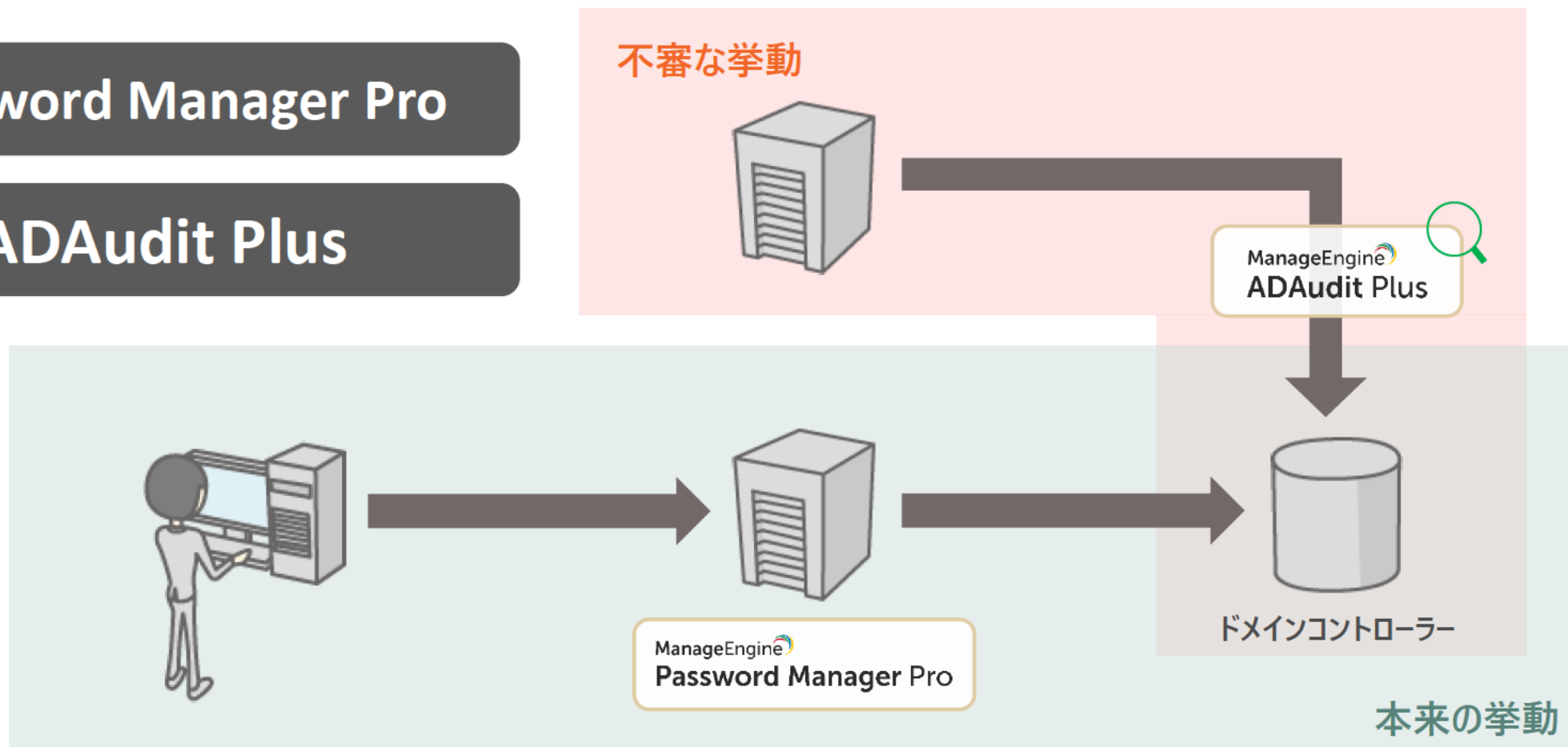
© 2017 Zoho Corp., All rights reserved.

Windows のライセンス認証  
コントロールパネルの [システム] を開き、Windows のライセンス認証を行ってください。

## 2. 「申請/承認フロー」を使用した特権ID管理

Password Manager Pro

ADAudit Plus



# Agenda

1. 特権アカウントの洗い出し  
(ADManager Plus)

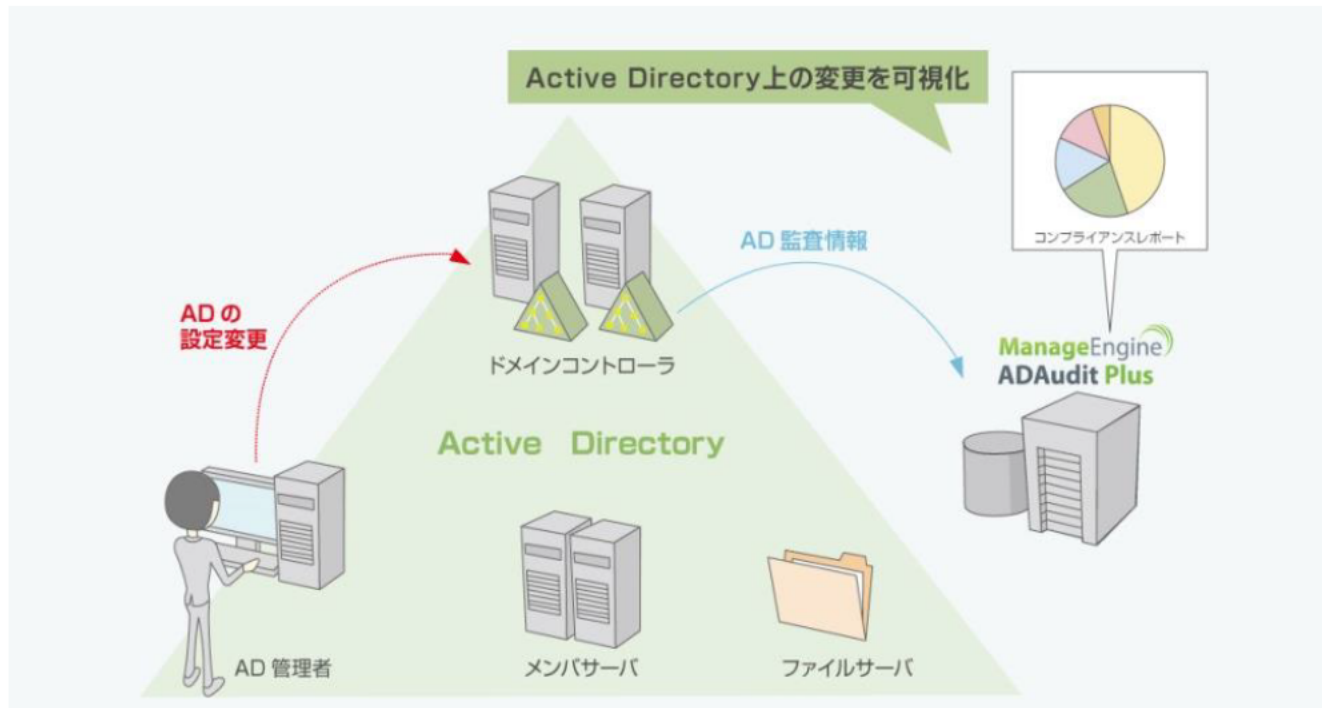
2. 「申請/承認フロー」を使用した特権ID管理  
(Password Manager Pro)

3. イベントログの可視化と検知  
(ADAudit Plus/EventLog Analyzer)

4. まとめ

# 3. イベントログの可視化と検知

## ADAudit Plus



全世界**3,500社**以上の企業や組織で利用されている、WebベースのActive Directory監査ツール

ユーザー

グループ

グループポリシー

変更情報を一元管理

# 3. イベントログの可視化と検知

1

導入・運用

- インストールから監査開始まで**およそ10分**
- **エージェントレス**でイベントログを取得可能

2

機能

- Active Directoryの監査ログを**可視化**
- リアルタイムアラート通知

3

コスト

- **ドメインコントローラー数**に基づく価格設定
- 年間398,000円(2ドメインコントローラー)からご用意



Active Directory Cloud Directory

(ドメインmetech.local) 監査ログのクリア

(3/19/2018 04:36:56 午後から4/18/2018 04:36:56 午後)

期間  時間

フォーマットの選択 ★ 追加 表示

監査ログのクリア

高度な検索

1-2 of 2 25 項目の追加/除外

日時	ロケーション	実行ユーザー名	実行者ユーザードメイン	メッセージ
4/18/2018 04:36:51 午後	maeda-windows1.metech.local	mihirom	METECH	The audit log was cleared by mihirom
4/18/2018 04:35:32 午後	maeda-windows1.metech.local	administrator	METECH	The audit log was cleared by administrator

1-2 of 2 25

- ユーザーログオンレポート
- ローカルログオン/ログオフ
- ADFS監査
- アカウント管理
- ユーザー管理
- グループ管理
- コンピューター管理
- 組織単位 (OU) の管理
- GPO管理
- 高度なGPOレポート
- その他のADオブジェクトの変更
- アクセス許可の変更
- DNSの変更
- 設定監査
- リムーバブルストレージ監査
- ドメイン オブジェクト変更
- LAPS監査
  - LAPS パスワードの読み取り
  - LAPS パスワード有効期限の変更
- プロフィール別レポート

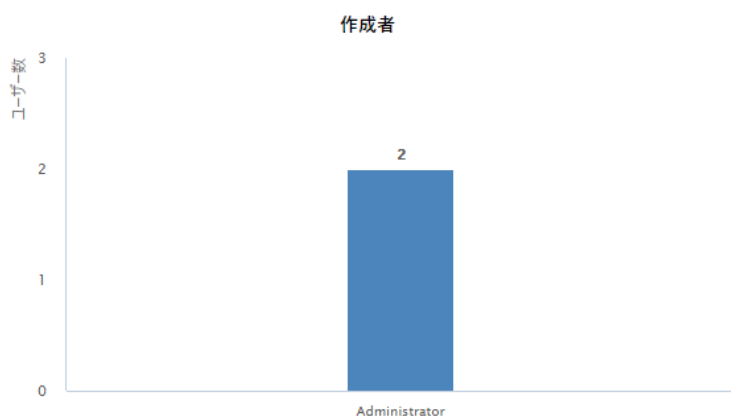
### LAPS パスワード有効期限の変更

(8/21/2017 04:50:44 午後から9/20/2017 04:50:44 午後)

期間  時間

フォーマットの選択 ★ 追加 もっと

#### LAPS パスワード有効期限の変更



高度な検索 1-2 of 2 25 項目の追加/除外

新規アカウント名	実行ユーザー名	更新時間	ドメインコントローラー	変更済み属性	新しい値	古い値	備考
M-WIN10	Administrator	9/20/2017 04:50:02 午後	maeda-windows1.metech.local	ms-Mcs-AdmPwdExpirationTime	9/21/2017 04:42:30 午後	9/20/2017 04:42:30 午後	コンピューターの変更
M-WIN10	Administrator	9/20/2017 04:43:07 午後	maeda-windows1.metech.local	ms-Mcs-AdmPwdExpirationTime	9/20/2017 04:42:30 午後	-	Computer Attribute Added

1-2 of 2 25

ユーザーログオンレポート

- ログオン失敗 **NEW**
- ログオン失敗 (ユーザー別)
- 無効なパスワードによる失敗
- コンピュータへの初回、最新ログオン
- 無効なユーザー名による失敗
- ログオン活動 (ドメインコントローラ別)
- ログオン活動 (IPアドレス別)
- ドメインコントローラ ログオン活動
- メンバーサーバ ログオン活動
- ワークステーション ログオン活動
- ユーザーログオン活動
- 最近のユーザーログオン活動
- ワークステーションの最終ログオン
- ユーザーの最終ログオン
- 複数のコンピュータにログオンしたユーザー

- ローカルログオン/ログオフ
- ADFS監査
- アカウント管理
- ユーザー管理
- グループ管理
- コンピュータ管理
- 組織単位 (OU) の管理
- GPO管理
- 高度なGPOレポート
- その他のADオブジェクトの変更
- アクセス許可の変更
- 設定監査
- 組織単位 (OU) の管理
- GPO管理

ログオン失敗

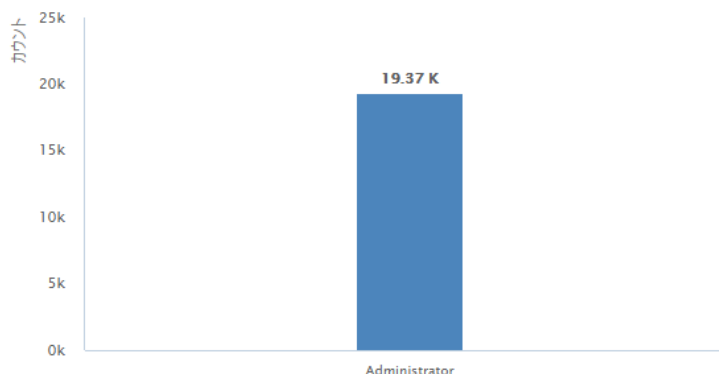
(2017-09-19 4:04:33 午後から2017-09-20 4:04:33 午後)

期間 最新 24 時間 時間 非ビジネス

フォーマットの選択 ★ 追加 もっと

ログオン失敗

トップ ユーザーのログオン失敗



高度な検索

1-25 of 19369 25 項目の追加/除外

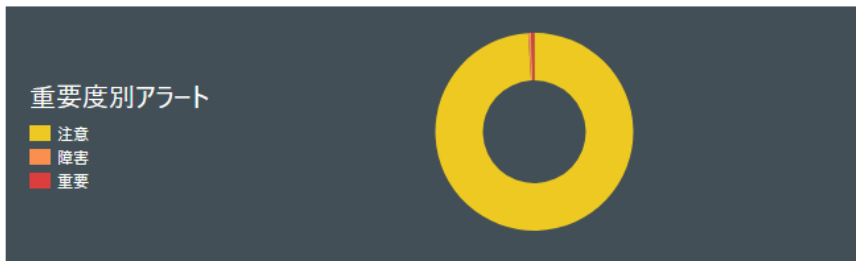
ユーザー名	クライアント ホスト名	ドメインコントローラ	ログオン時間	イベントタイプ	失敗理由	ログオンサービス	アナライザ詳細
Administrator	demo-ela.me-develop.local	DEMO-AD	2017-09-20 8:59:55 午前	失敗	無効なパスワード	krbtgt/me-develop	詳細
Administrator	demo-ela.me-develop.local	DEMO-AD	2017-09-20 8:59:55 午前	失敗	無効なパスワード	krbtgt/me-develop	詳細
Administrator	demo-ela.me-develop.local	DEMO-AD	2017-09-20 8:59:55 午前	失敗	無効なパスワード	krbtgt/me-develop	詳細
Administrator	demo-ela.me-develop.local	DEMO-AD	2017-09-20 8:59:55 午前	失敗	無効なパスワード	krbtgt/me-develop	詳細
Administrator	demo-ela.me-develop.local	DEMO-AD	2017-09-20 8:59:55 午前	失敗	無効なパスワード	krbtgt/me-develop	詳細

認証回数の調査 (休日などアカウントが使用されないはずの期間に認証が行われていないか)

- すべてのアラート
- プロフィール別アラート
  - metech.local

アーカイブアラート | [\[表示\] すべてのアラート](#)  
(開始 9/19/2017 04:11:21 午後 終了 9/20/2017 04:11:21 午後)

最新 24 時間



✕

**重要 1**

[重要アラートをフィルターする](#)

!!

**障害 1**

[障害アラートをフィルターする](#)

!

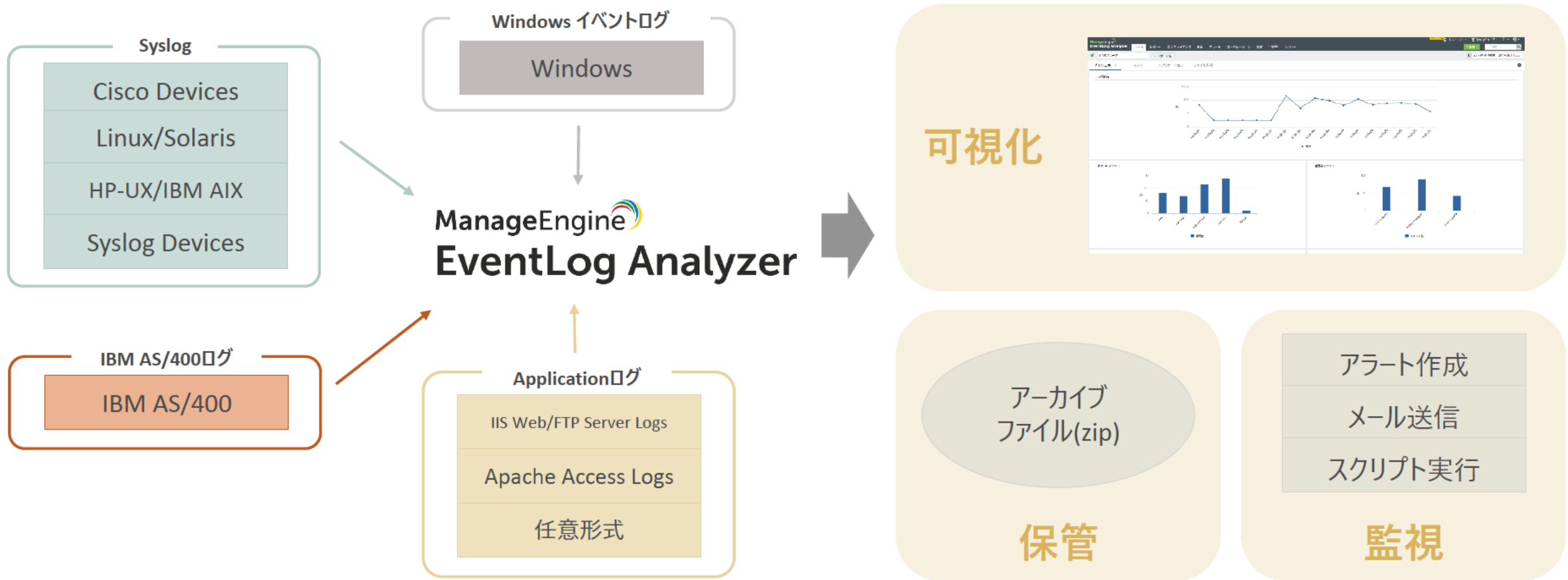
**注意 202**

[注意アラートをフィルターする](#)

除外 削除 1-25 of 204 25

<input type="checkbox"/>	ソース	ドメイン名	基準	生成時間	アラートメッセージ	しきい値
<input type="checkbox"/>	maeda-windows1.metech.local	metech.local	注意	9/20/2017 04:02:15 午後	M-WINSECにおいてユーザーAdministratorがログインに失敗しました。理由:無効なパスワード	-
<input type="checkbox"/>	maeda-windows1.metech.local	metech.local	重要	9/20/2017 03:57:09 午後	administratorがシステム監査ログをクリアしました	-
<input type="checkbox"/>	maeda-windows1.metech.local	metech.local	注意	9/20/2017 03:51:56 午後	M-WINSECにおいてユーザーAdministratorがログインに失敗しました。理由:無効なパスワード	-
<input type="checkbox"/>	maeda-windows1.metech.local	metech.local	注意	9/20/2017 03:41:32 午後	M-WINSECにおいてユーザーAdministratorがログインに失敗しました。理由:無効なパスワード	-
<input type="checkbox"/>	maeda-windows1.metech.local	metech.local	注意	9/20/2017 03:31:24 午後	M-WINSECにおいてユーザーAdministratorがログインに失敗しました。理由:無効なパスワード	-
<input type="checkbox"/>	maeda-windows1.metech.local	metech.local	注意	9/20/2017 03:21:19 午後	M-WINSECにおいてユーザーAdministratorがログインに失敗しました。理由:無効なパスワード	-
<input type="checkbox"/>	maeda-windows1.metech.local	metech.local	注意	9/20/2017 03:11:19 午後	M-WINSECにおいてユーザーAdministratorがログインに失敗しました。理由:無効なパスワード	-
<input type="checkbox"/>	maeda-windows1.metech.local	metech.local	注意	9/20/2017 03:11:19 午後	M-WINSECにおいてユーザーAdministratorがログインに失敗しました。理由:無効なパスワード	-
<input type="checkbox"/>	maeda-windows1.metech.local	metech.local	注意	9/20/2017 03:07:26 午後	M-WINSECにおいてユーザーAdministratorがログインに失敗しました。理由:無効なパスワード	-
<input type="checkbox"/>	maeda-windows1.metech.local	metech.local	注意	9/20/2017 03:01:18 午後	M-WINSECにおいてユーザーAdministratorがログインに失敗しました。理由:無効なパスワード	-
<input type="checkbox"/>	maeda-windows1.metech.local	metech.local	障害	9/20/2017 03:01:12 午後	METECH\administratorがドメインのローカルセキュリティグループAdministratorsにメンバーtestuserを追加しました	-

# 3. イベントログの可視化と検知





### 3. イベントログの可視化と検知

	ADAudit Plus	EventLog Analyzer
収集ログ	<ul style="list-style-type: none"><li>● Windowsイベントログ</li></ul>	<ul style="list-style-type: none"><li>● Windowsイベントログ</li><li>● Syslog</li><li>● アプリケーションログ</li></ul>
管理形態	<ul style="list-style-type: none"><li>● ドメインごと</li></ul>	<ul style="list-style-type: none"><li>● ホストごと</li></ul>
製品の強み	<ul style="list-style-type: none"><li>● レポート数が多く細分化</li><li>● Active Directory運用の監査に特化</li></ul>	<ul style="list-style-type: none"><li>● 複数種類ログの一括保管</li><li>● 生ログの保管</li><li>● 条件指定による検索</li></ul>

# Agenda

## 1. 特権アカウントの洗い出し

(ADManager Plus)

## 2. 「申請/承認フロー」を使用した特権ID管理

(Password Manager Pro)

## 3. イベントログの可視化と検知

(ADAudit Plus/EventLog Analyzer)

## 4. まとめ

# 4. まとめ

1

ManageEngine  
**ADManager Plus**

- Active Directory ID管理ソフト
- Active Directoryアカウントの棚卸を効率化

2

ManageEngine  
**Password Manager Pro**

- 申請/承認フローを使用した特権ID管理
- 特権IDの運用自動化/操作画面の録画に対応

3

ManageEngine  
**ADAudit Plus**  
ManageEngine  
**EventLog Analyzer**

- Active Directoryの監査ログを可視化
- リアルタイムアラート通知に対応
- ログの保管に特化した統合ログ管理

# 4. まとめ

製品に関する詳細な説明・デモをご希望の方

オンライン相談

にお申し込みください。

[https://www.manageengine.jp/online\\_meeting/](https://www.manageengine.jp/online_meeting/)

## お申し込みフォーム

次のフォームに必要事項をご記入の上、送信してください。

必須 会社名	<input type="text"/>
必須 部署名	<input type="text"/>
必須 役職	<input type="text"/>
必須 氏名	姓: <input type="text"/> 名: <input type="text"/>
必須 電話番号	<input type="text"/> 半角でご記入ください
必須 メールアドレス	<input type="text"/> 半角でご記入ください
必須 対象製品	<div style="border: 1px solid #ccc; padding: 2px;"><p>ADAudit Plus ADManager Plus ADSelfService Plus Applications Manager Desktop Central EventLog Analyzer</p></div> 「Ctrl」キーで複数選択できます

## 購入相談専用窓口 オンライン相談

ManageEngineでは、製品の詳細を知りたい方向けに「オンライン相談」のお申込みを受け付けております。お気軽にご利用ください。

こんな方におすすめです

製品導入を検討するため、説明を受けたい。

実際の画面や使用感を見たい。

口頭で細かいニュアンスの質問をしたい。



訪問説明とほぼ同じ内容をご提供できます！

お申し込みフォーム



ご清聴ありがとうございました。