

# 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)

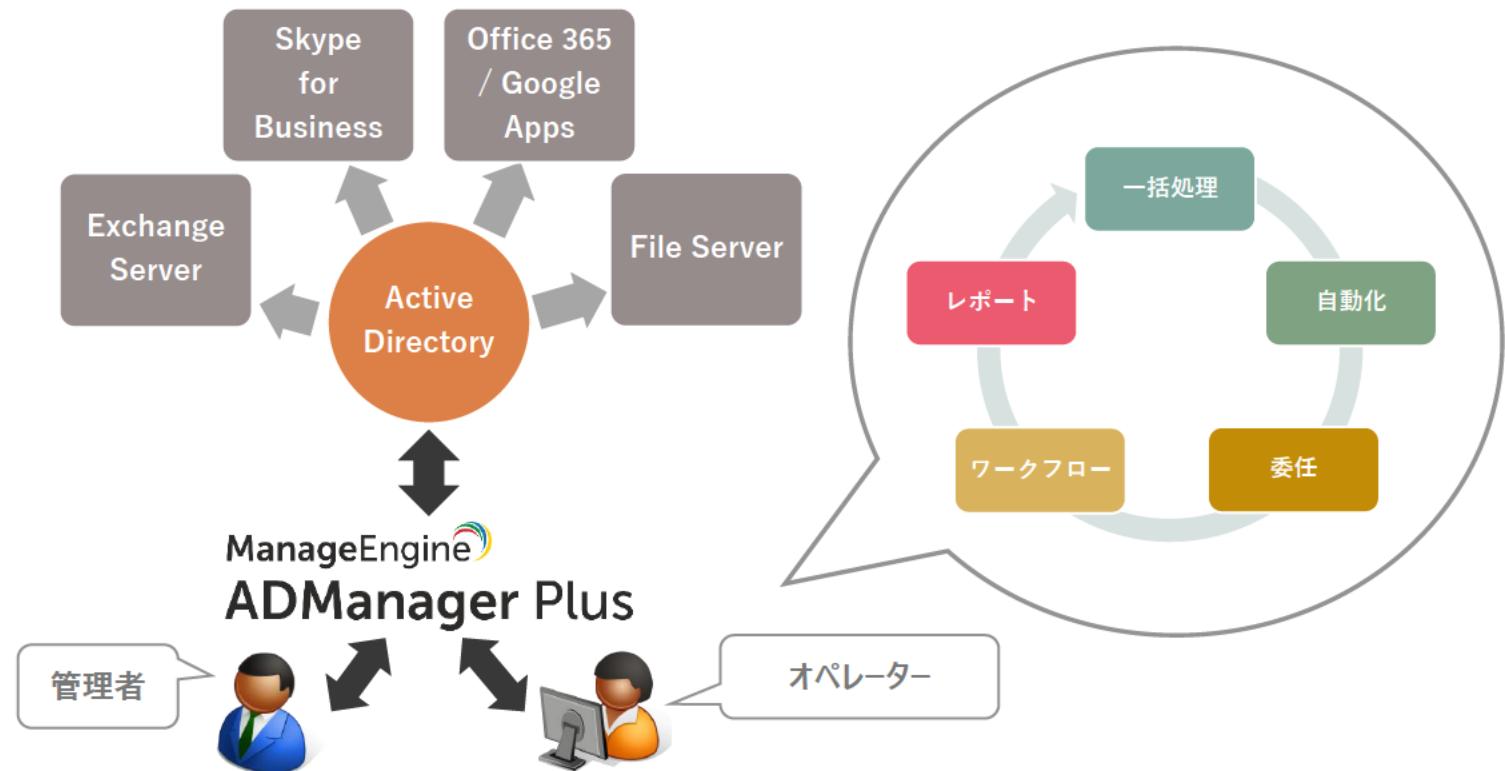
3. イベントログの可視化と検知  
(ADAudit Plus/EventLog Analyzer)

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

[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](#)[ドメイン設定](#) | [AD エクスポート](#)[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](#) [GPO レポート](#) [OU レポート](#) [他のレポート](#)[エクスポート](#) | [PDF](#) | [CSV](#)

## 選択したグループに所属しているユーザー

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...](#)

入力情報

[スケジュール レポート](#)ドメインの選択 : グループ :  [編集](#)[選択](#) 入れ子のグループを除く[作成](#) [停止](#)[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

[グループから削除](#)[操作オプション](#)[リクエストを作成](#)[クリック検索](#)1ページの表示件数 : 

1 - 1 / 1

<input type="checkbox"/>	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	プライマリー 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

ManageEngine

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

GPO レポート

OU レポート

他のレポート

エクスポート | 印刷 |

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...

入力情報

ドメインを選択:  me-develop.local

OUを選択: 設約社員[me-de...詳細情報 [OUを追加]

 manageengine.yokohama希望の時間範囲を選択:  過去 90 日 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 | 署名 | ... | 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	プライマリーグループ
	goro	saito	齊藤	saito	2018-02-26 14:33:19	0	有効	saito@me.test	-	Domain Users
	hanako	tanaka	田中	tanaka	2018-02-26 14:33:20	0	有効	tanaka@me.test	-	Domain Users
	ichiro	sato	佐藤	sato	2018-02-26 14:33:20	0	有効	sato@me.test	-	Domain Users
	saburo	yoshida	吉田	yoshida	2018-02-26 14:33:20	0	有効	yoshida@me.test	-	Domain Users
	siro	watabe	渡部	watabe	2018-02-26 14:33:20	0	有効	watanabe@me.test	-	Domain Users
	taro	yamada	山田	yamada	2018-02-26 14:33:20	0	有効	yamada@me.test	-	Domain Users
	yasuko	matsuda	松田	matsuda	2018-02-26 14:33:19	0	有効	matsuda@me.test	-	Domain Users
	yoshiko	takada	高田	takada	2018-02-26 14:33:19	0	有効	takada@me.test	-	Domain Users
	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)

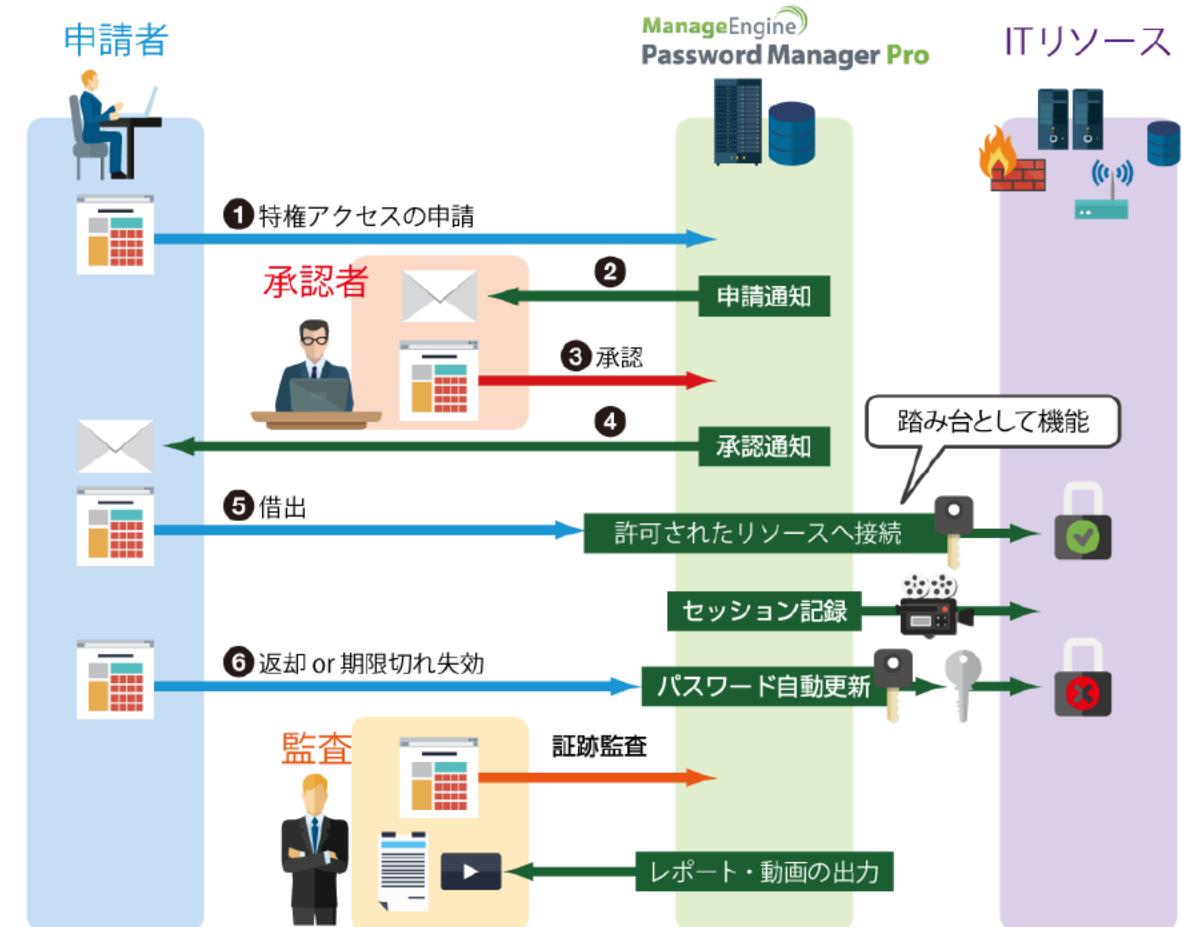
4. まとめ

## 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



ManageEngine Password X

https://demo-pmp.me-develop.local:7272/PassTrixMain.cc

検索

ログイン

Username: demotest

Password: [REDACTED]

Log on to: Local Authentication

Login

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。

English | 中文 | 日本語 | Deutsch | Español | Français | polski

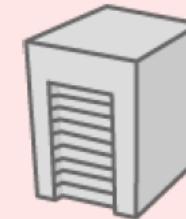
申請者側

## 2. 「申請/承認フロー」を使用した特権ID管理

Password Manager Pro

ADAudit Plus

不審な挙動



ManageEngine  
ADAudit Plus



ManageEngine  
Password Manager Pro

ドメインコントローラー

本来の挙動

# 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)

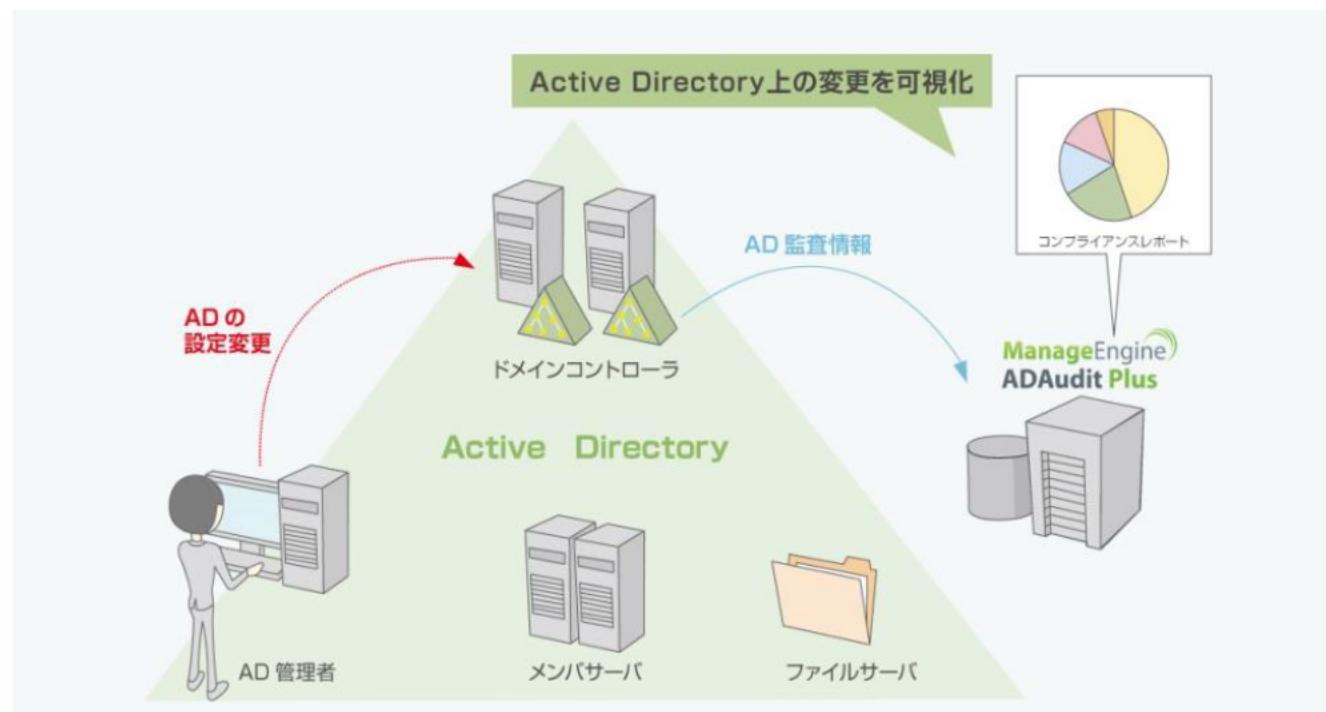
3. イベントログの可視化と検知

(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)からご用意

レポートの検索

ログオン監査

Active Directory変更

GPO変更

コンプライアンス

カスタムレポート

スケジュールレポート

集約レポート



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

最新 30 日間

時間

すべて

フォーマットの選択 ★追加 もつ

## 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 ▲

LAPS監査

ドメイン オブジェクト変更

プロファイル別レポート

WorkGroup

metech.local

アカウントログオン

ローカル ログオン/ログオフ

アカウント作成

ユーザー変更

コンピューターの変更

グループ変更

組織単位 (OU) の管理

GPO管理

詳細追跡

ドメインポリシーの変更

システム イベント

役割の分離の有効

関連あるセキュリティログ

セキュリティログの空き容量不足

イベント記録の不具合

監視対象のセキュリティイベントのパン

システム ログオン

監査ログのクリア

システム時刻の変更

OCSP レスポンダー サービスのセキュ

リティ設定更新

拡張AD監査

ポリシー変更

DNSサーバー監査

ローカル アカウント管理

レポートの検索

ログオン監査 Active Directory変更 GPO変更 コンプライアンス

カスタムレポート スケジュールレポート 集約レポート

ユーザー登録レポート

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)

ドメ  
イン

metech.local

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

プロファイル別レポート

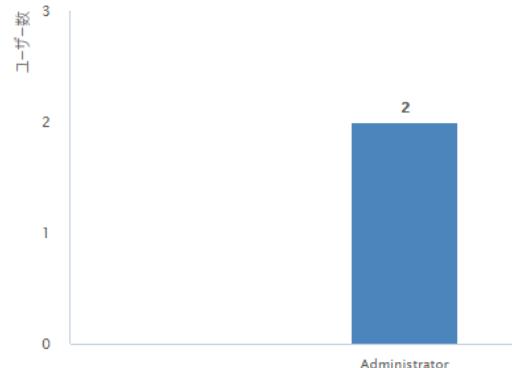
期間 最新 30 日間

時間 すべて

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

## 作成者



Q\* 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 ▾

LAPSによるローカル管理者アカウントのパスワード変更

ManageEngine  
16

レポートの検索

ログオン監査 ▾ Active Directory変更 ▾ GPO変更 ▾ コンプライアンス ▾ マイレポート ▾

カスタムレポート スケジュールレポート 集約レポート

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

コンピューターへの初回、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ー-ログオン活動

メンバーサーバー-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ー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

設定監査

組織単位（OU）の監査

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)

ドメイ...  
イン

me-develop.local

期間

最新 24 時間

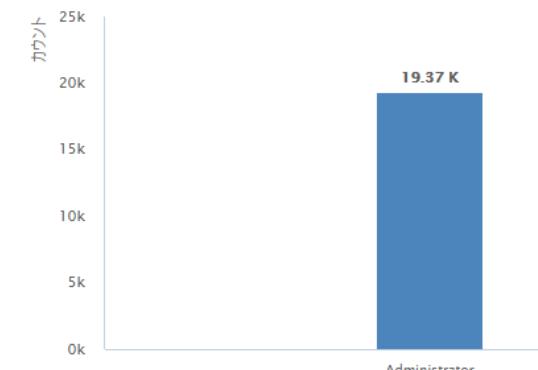
時間

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

 Q\* 高度な検索1-25 of 19369   25  プロジェクトの追加/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ー	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	<input type="button"/> 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	<input type="button"/> 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	<input type="button"/> 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	<input type="button"/> 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	<input type="button"/> 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）

ManageEngine

すべてのアラート

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)

メール通知

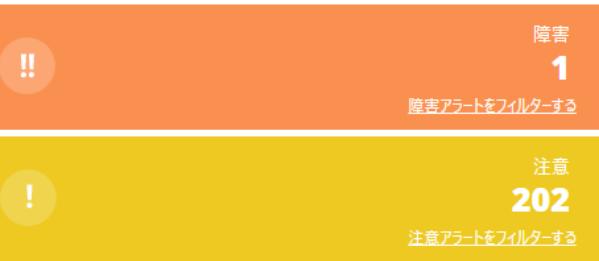
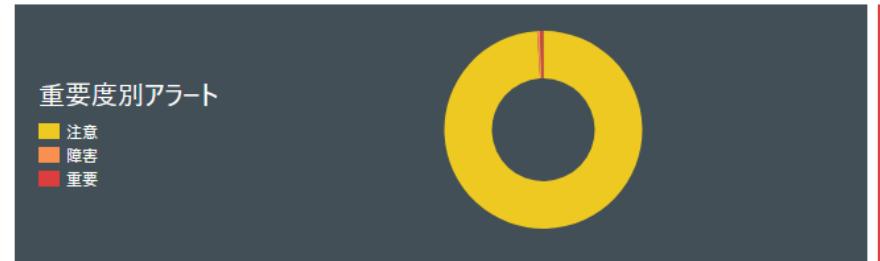
新規アラートプロファイル

アラートプロファイルを表示/変更

プロファイル別アラート

▶ metech.local

最新 24 時間

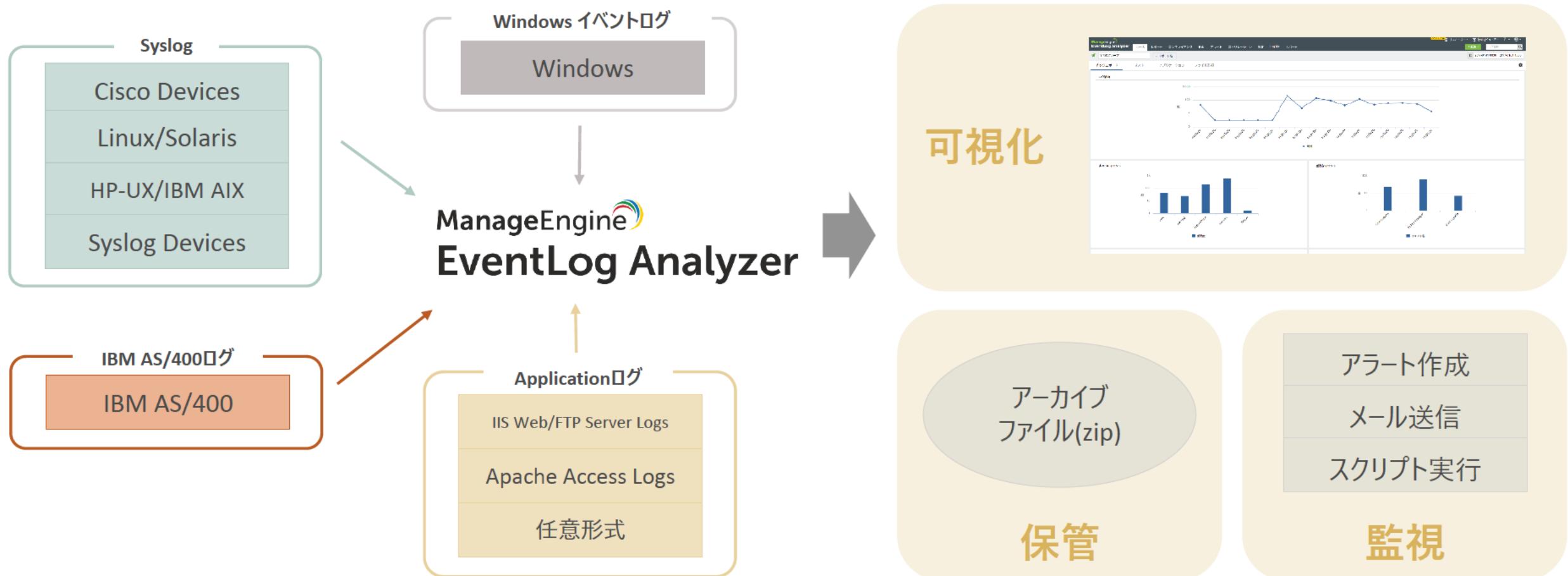


除外 削除

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

収集ログ

管理形態

製品の強み

#### ADAudit Plus

- Windowsイベントログ
- ドメインごと
- レポート数が多く細分化
- Active Directory運用の監査に特化

#### EventLog Analyzer

- Windowsイベントログ
- Syslog
- アプリケーションログ
- ホストごと
- 複数種類ログの一括保管
- 生ログの保管
- 条件指定による検索

# 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	<ul style="list-style-type: none"><li>ADAudit Plus</li><li>ADManager Plus</li><li>ADSelSelfService Plus</li><li>Applications Manager</li><li>Desktop Central</li><li>EventLog Analyzer</li></ul> <p>「Ctrl」キーで複数選択できます</p>



## 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てみたい。

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

A photograph of a person standing in front of a large window, looking out onto a dense city skyline. The sky is clear and blue. The person is positioned on the right side of the frame, facing left. The city below is filled with numerous skyscrapers of various heights and architectural styles.

ご清聴ありがとうございました。