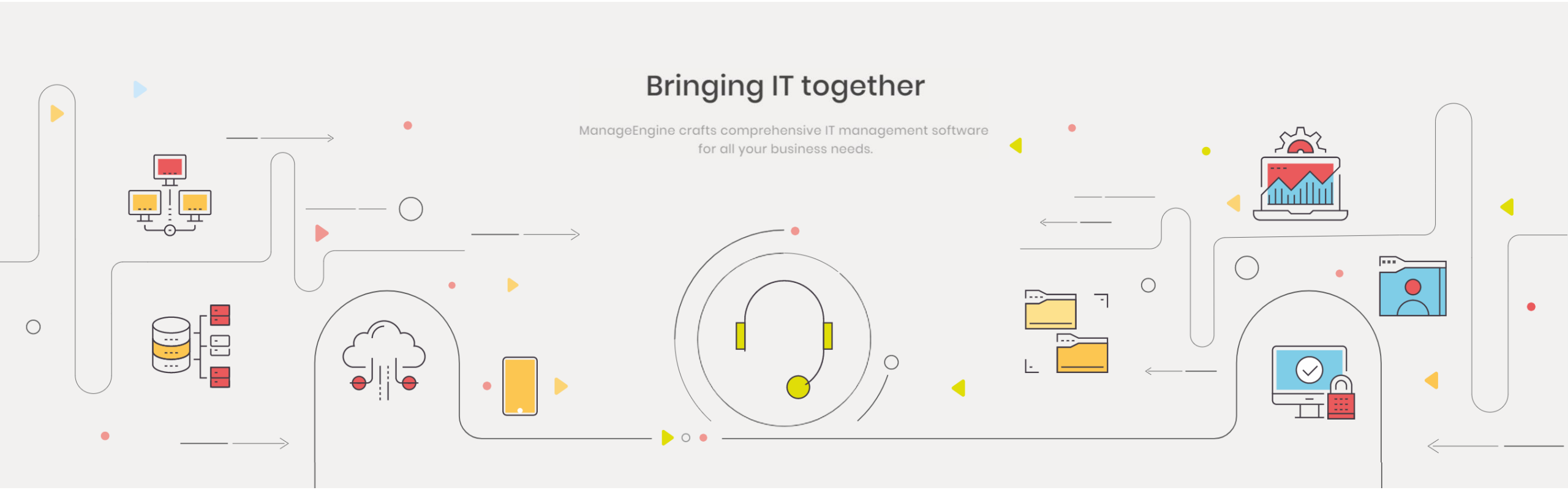
ManageEngine



増えるアクセス、広がるリスクに備える

ファイルサーバーのアクセス権限管理に関するソリューション

ゾーホージャパン株式会社

セキュリティ意識の更なる高まり

満たすべき規格や基準、規則やガイドラインがますます増加

ISO27001
情報セキュリティに関する国際規格

マイナンバーガイドライン
マイナンバーの取り扱いに関するガイドライン

PCI DSS
クレジット業界におけるグローバル
セキュリティ基準

GDPR
EU内の全ての個人のために
データ保護を強化するための規則

Pマーク
個人情報保護マネジメントシステム
JIS Q 15001の認定マーク

NIST SP800-171
米国国防総省による業者に対しての
サイバーセキュリティガイドライン

これに伴いファイルサーバーのアクセス権限管理に関する要件が増加しています

© ZOHO Japan Corporation. All rights reserved.

ファイルサーバー監査を行うにあたり推奨されるステップ

STEP 1

情報資産の棚卸

どんな情報が、どこに、どういう状態で保存されているかを洗い出す

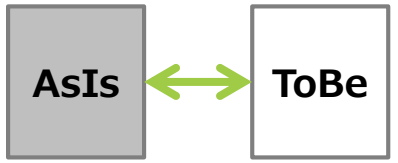
STEP 2

あるべき運用ルールの整理

棚卸した内容を基に、情報資産の種類別に理想的な保存先および保存方法・運用方法を整理

STEP 3

現状の運用との比較



現状とSTEP2を比較し、そのFit&Gapを整理して、規定や運用ルール、システム構成の変更を行う

STEP 4

監査の実施

STEP2で制定した運用ルールとの差異を監査ツールなどで抽出して、機械的、人間的の両面で監査を行う

STEP１～３を飛ばして STEP４から開始しても 適切な監査は行えない

運用面の見直しを合わせて実施することで、より適切な監査を実施

© ZOHO Japan Corporation. All rights reserved.

ファイルサーバーのアクセス権限管理業務に関して

ユーザーに権限を
適切に/スピーディーに/
ミスなく設定したい

ユーザーの権限を
簡単に
棚卸ししたい

どのユーザーで
不正が発生しているのかを
早期に発見したい

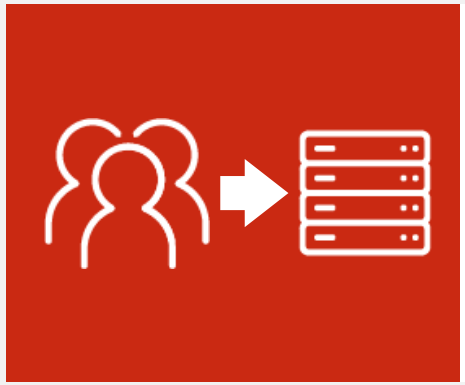
ファイルやフォルダへの
不正なアクセスを
確実に検知したい

セキュリティグループや
ACL設定に対する
不正な変更を
正確に把握したい

多くの企業がファイルサーバーのアクセス権限管理に関して苦労されています

© ZOHO Japan Corporation. All rights reserved.

ファイルサーバーのアクセス権限管理業務に関連するManageEngine製品のご紹介



ファイルサーバーに対するアクセス権限管理の最適化

- ユーザーに適切な権限をスピーディーにミスなく設定
- ユーザーにどんな権限が付与されているのか簡単に権限を棚卸し

ManageEngine
ADManager Plus

認証ログやACL・セキュリティグループの設定および ファイルやフォルダへのアクセス状況の監査

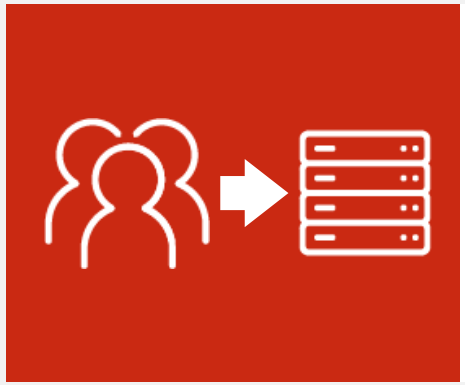
- どのユーザーが異常なアクセスをしているのかを可視化
- ACLやセキュリティグループの設定が不正に変更されていないか可視化
- ユーザーがフォルダ・ファイルへどのような操作をしているのかを可視化

ManageEngine
ADAudit Plus

Windows環境に加えNetAppも含めたファイルサーバーのアクセス権限管理に関連する多彩なラインナップ

© ZOHO Japan Corporation. All rights reserved.

セキュリティグループ・NTFSに関するワークフローとレポート



ファイルサーバーに対するアクセス権限管理の最適化

- ユーザーに適切な権限をスピーディーにミスなく設定
- ユーザーにどんな権限が付与されているのか簡単に権限を棚卸し

ManageEngine
ADManager Plus

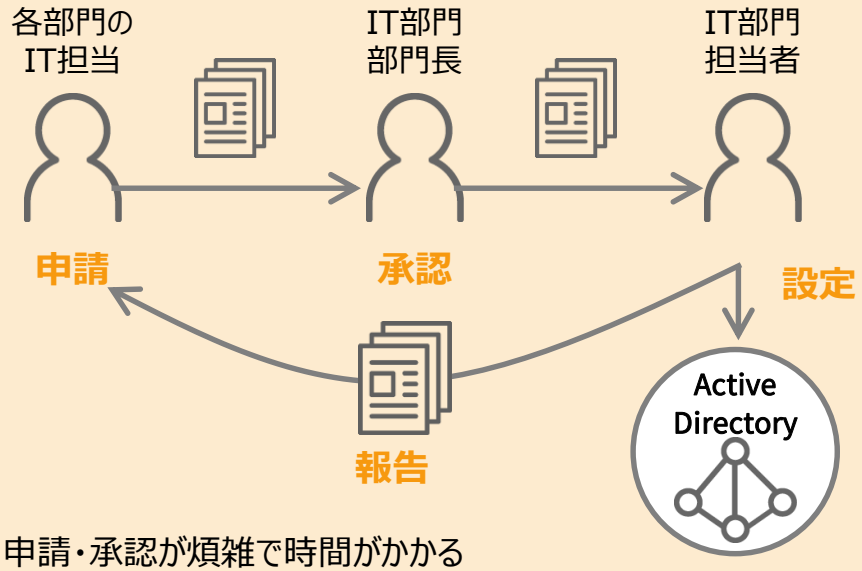
Active Directory の運用に関するお悩み事を解決

© ZOHO Japan Corporation. All rights reserved.

ワークフロー：セキュリティグループ

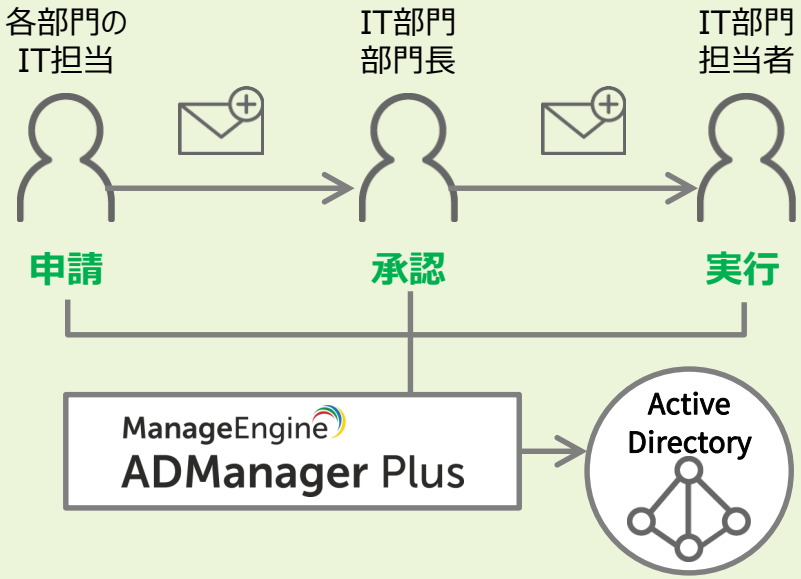
例：アクセス権を付与しているセキュリティグループへの追加/削除を行う場合

Active Directory でのよくある運用



- 申請・承認が煩雑で時間がかかる
- ADのセキュリティグループに対して1つずつ直接メンテナンスを実施
- 使いづらい画面のため操作が複雑で面倒
- 入力ミス・操作ミスが発生する危険性あり

ADManager Plus の場合



- 申請・承認が簡単でスピーディーかつそのまま実行可能
- ワークフローを利用するため、入力ミス・操作ミスが発生しない仕組み
- 1時間後に実行、指定日時に実行など実行スケジュールを設定可能

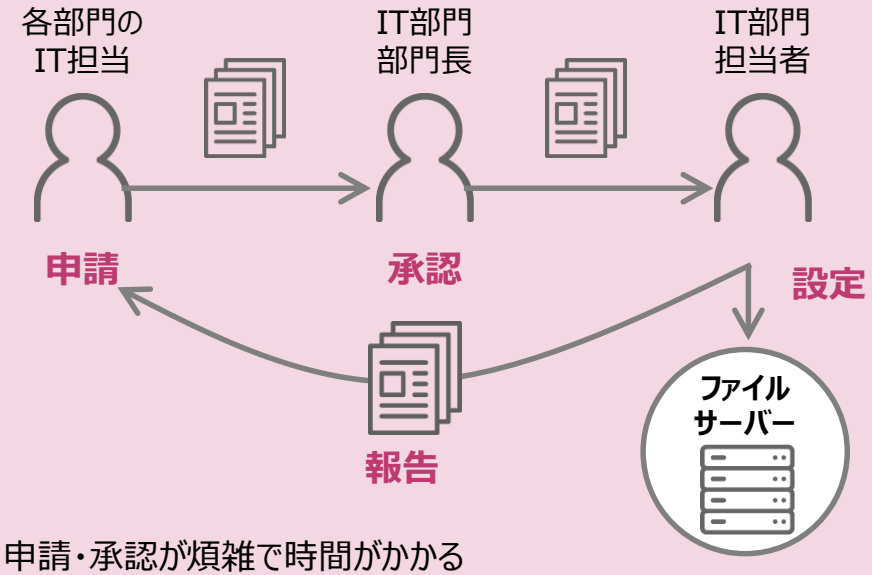
セキュリティグループでの権限申請・承認業務を正確かつスピーディーに

© ZOHO Japan Corporation. All rights reserved.

ワークフロー：NTFS

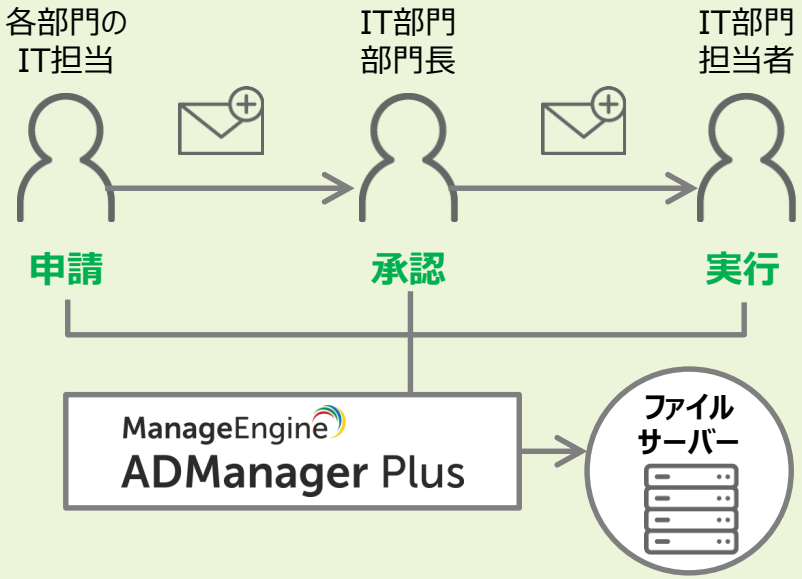
例：アクセス権の変更に承認フローを利用する場合

Active Directory でのよくある運用



- 申請・承認が煩雑で時間がかかる
- 各フォルダやファイルのプロパティからアクセス権限を1つずつ直接作業
- 使いづらい画面のため操作が複雑で面倒
- 入力ミス・操作ミスが発生する危険性あり

ADManager Plus の場合



- 申請・承認が簡単でスピーディーかつそのまま実行可能
- 実際の操作履歴を記録に残すことが可能
- ユーザのアクセスを許可する期間（ 1時間、1日など）も設定可能

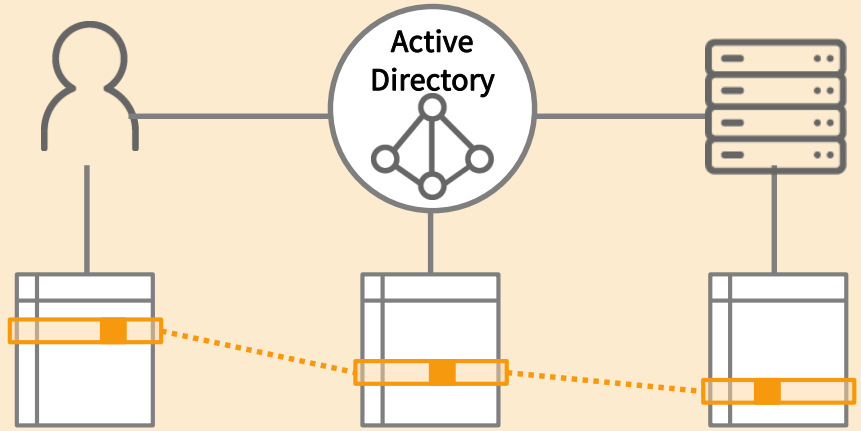
NTFSでの権限申請・承認業務を正確かつスピーディーに

© ZOHO Japan Corporation. All rights reserved.

レポート：セキュリティグループ

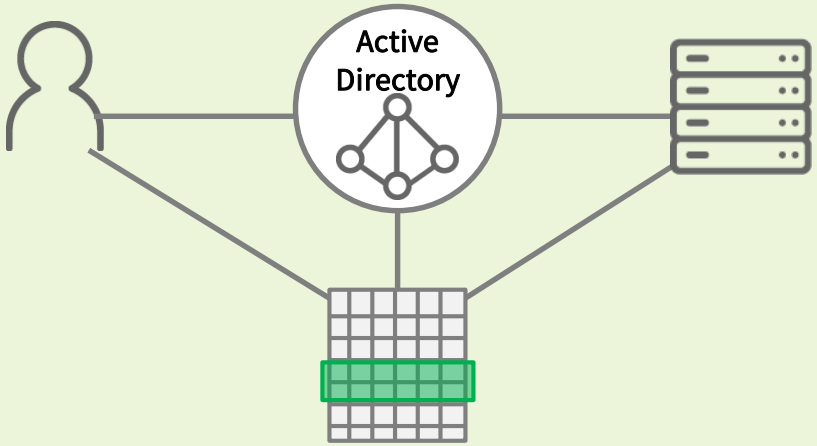
例：セキュリティグループに所属するメンバーを確認する場合

Active Directory でのよくある運用



- セキュリティグループを1つずつ直接確認しExcelなどにまとめる
- 手作業では現実的には調査が難しいほどの膨大な作業量
- 自作ツールや一般公開されているツールを利用するがサポート面が不安
- 設定内容は変化するため、定期的な調査が必要

ADManager Plus の場合



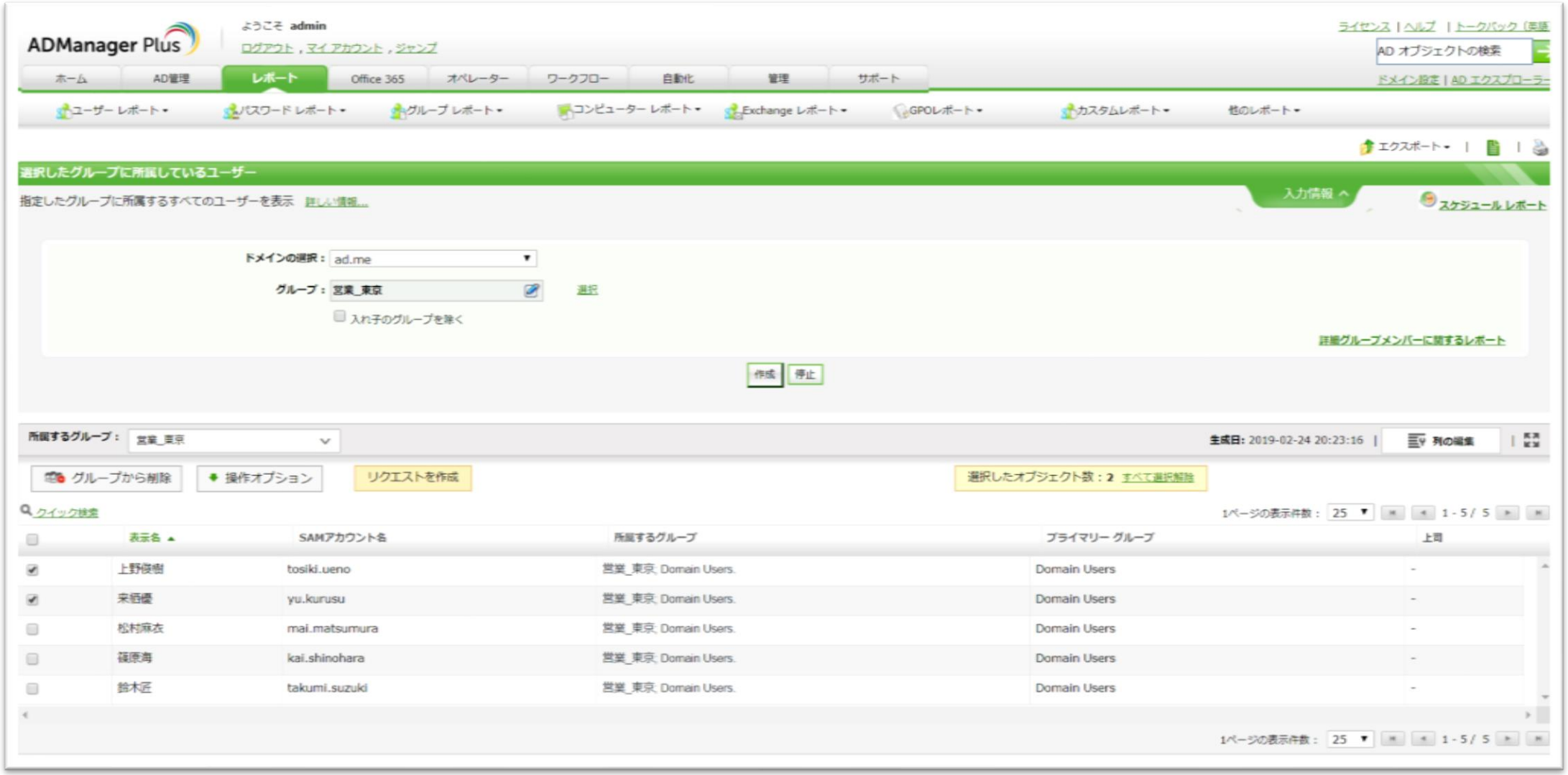
- ユーザ視点/グループ視点など標準で豊富なレポートが利用可能
- レポート作成をスケジュール化することで定期的な調査が容易に
- レポート取得後、ユーザをグループから削除するなど次のアクションをそのまま実行可能

セキュリティグループでの権限設定の棚卸しなどが簡単におこなえます

© ZOHO Japan Corporation. All rights reserved.

レポート：セキュリティグループ

例：選択したグループに所属しているユーザーレポート

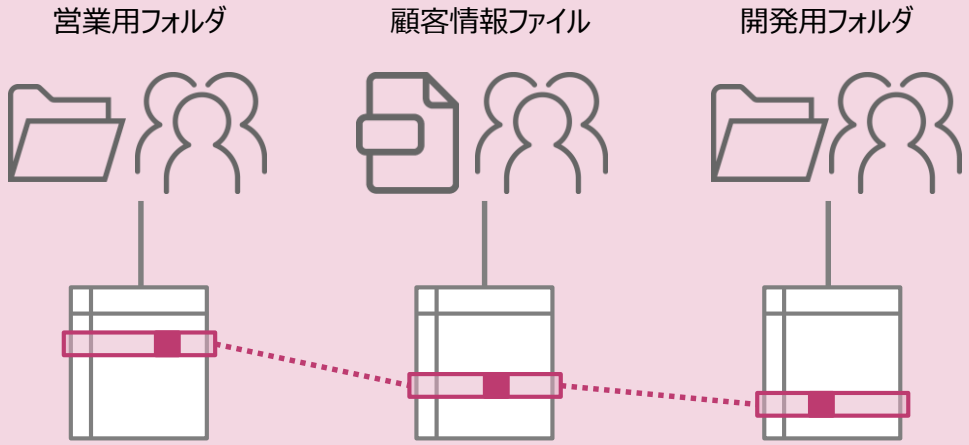


© ZOHO Japan Corporation. All rights reserved.

レポート：NTFS

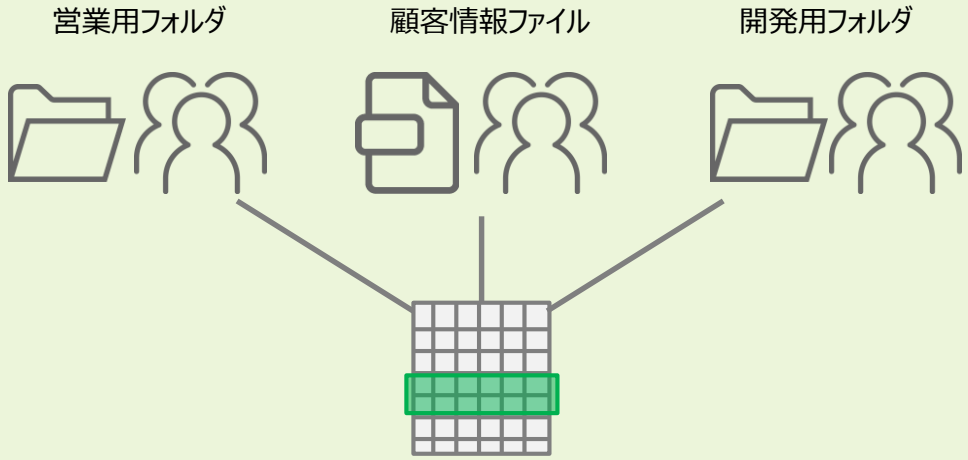
例：任意のフォルダのアクセス許可リスト（ACL）を確認する場合

Active Directory でのよくある運用



- 各フォルダやファイルのプロパティからアクセス権限を1つずつ直接確認
- どのユーザーがどのフォルダにアクセス可能かを個別に調査しExcelなどにまとめる
- 手作業では現実的には調査が難しいほどの膨大な作業量
- 自作ツールや一般公開されているツールを利用するがサポート面が不安
- 設定内容は変化するため、定期的な調査が必要

ADManager Plus の場合



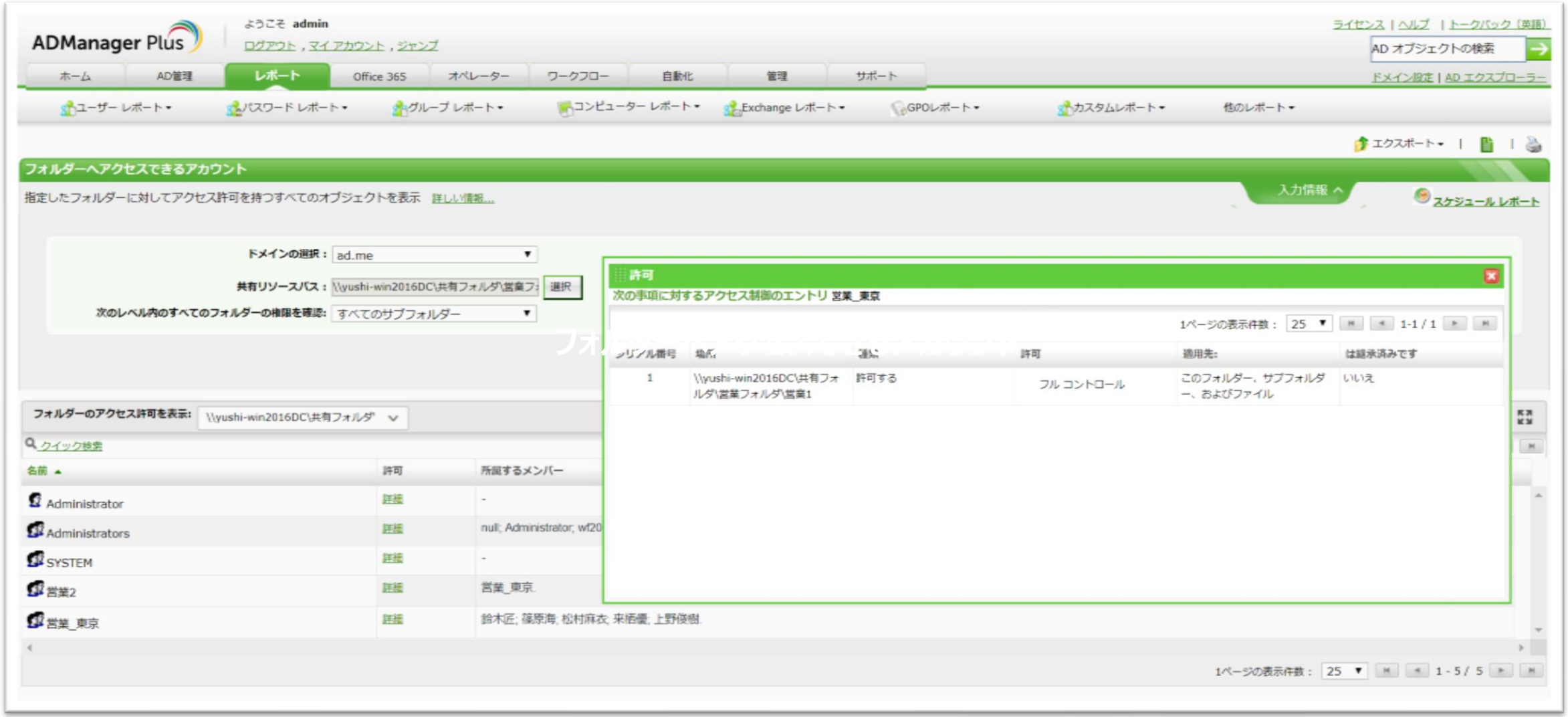
- フォルダ間を移動することなく1つ画面からアクセス権限を確認可能
- レポート作成をスケジュール化することで定期的な調査が容易に
- Excel、CSV、CSVDE、PDF、HTML形式へとエクスポート可能

NTFSでの権限設定の棚卸しなどが簡単におこなえます

© ZOHO Japan Corporation. All rights reserved.

レポート：NTFS

例：フォルダーへアクセスできるアカウントレポート



© ZOHO Japan Corporation. All rights reserved.

ファイルサーバーに対するアクセス状況の可視化とセキュリティ設定の変更監査

認証ログやACL・セキュリティグループの設定およびファイルやフォルダへのアクセス状況の監査

- どのユーザーが異常なアクセスをしているのかを可視化
- ACLやセキュリティグループの設定が不正に変更されていないか可視化
- ユーザーがフォルダ・ファイルへどのような操作をしているのかを可視化

ManageEngine
ADAudit Plus

認証ログの可視化

ファイルサーバーへの認証ログを監視・保管することで外部攻撃や内部不正を早期に検知

セキュリティ設定の変更監査

ACLやセキュリティグループの設定に関する変更管理を監査することで外部攻撃や内部不正を早期に検知

フォルダやファイルへのアクセス状況の可視化

どのユーザーがどのフォルダやファイルにアクセスをしているのかを可視化することで、外部攻撃や内部不正を早期に検知

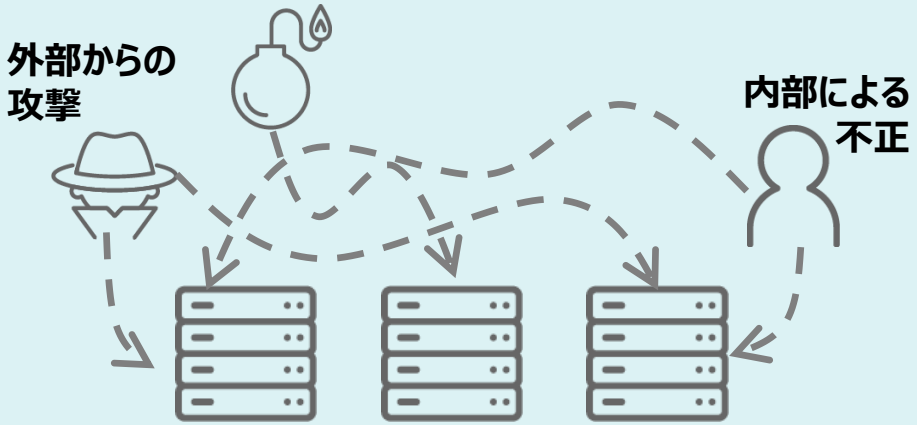
Active Directory監査業務に関するお悩み事を解決

© ZOHO Japan Corporation. All rights reserved.

認証ログの可視化

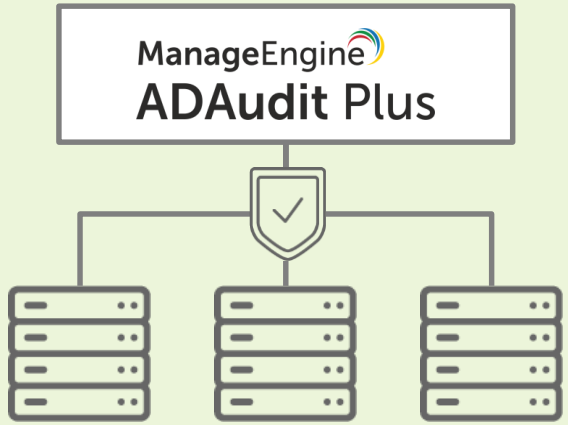
例：攻撃や不正の早期検知のためにファイルサーバーへの認証ログを可視化する場合

Active Directory でのよくある運用



- 標的型攻撃や内部不正が生じているものの検知が難しく発生していることが認識しづらい
- ログが複雑で、解析するには専門的な知識が必要であり、煩雑で手間がかかる
- 被害が発生してから、初めて認識

ADAudit Plus の場合



- 標準で豊富なレポートが利用可能
- 攻撃や不正の兆しを検知することで、被害の発生を未然に防止
- ファイルサーバーへのログオン/ログオン失敗を可視化することで早期に検知

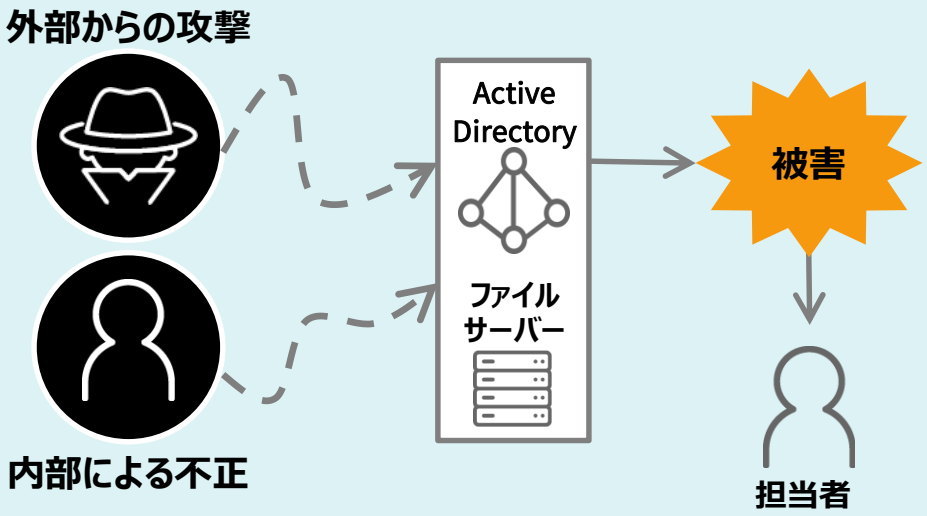
ファイルサーバーへの認証ログを監視・保管することで外部攻撃や内部不正を早期に検知

© ZOHO Japan Corporation. All rights reserved.

セキュリティ設定の変更管理

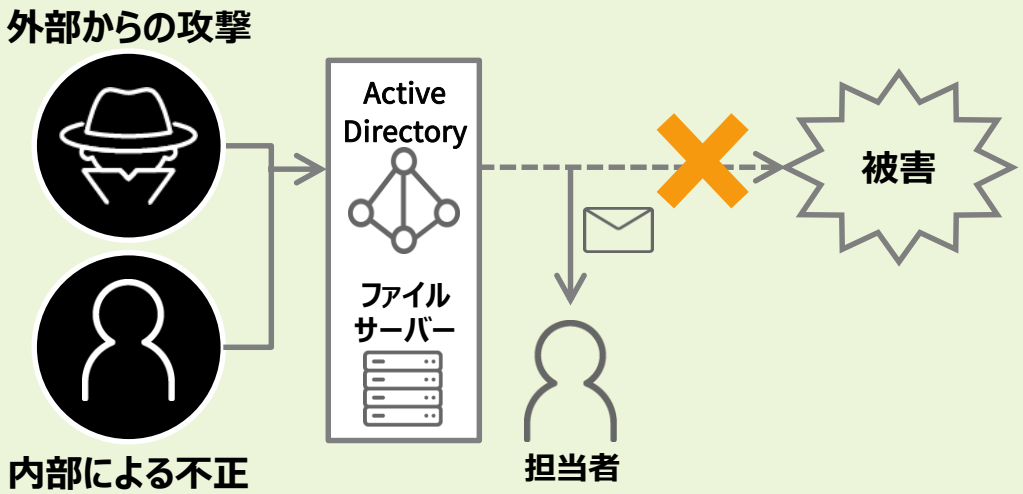
例：ACLやセキュリティグループの設定に関する変更管理を監査する場合

Active Directory でのよくある運用



- ACLやセキュリティグループの設定は頻繁に変更しないため、発生していることが認識しづらい
- 被害が発生してから、初めて認識

ADAudit Plus の場合



- 攻撃や不正の兆しを検知することで、被害の発生を未然に防止
- 変更前と変更後のACLやセキュリティグループの設定を記録し、本来の設定を素早く確認
- ADManager Plusと組み合わせることで、ADManager Plus経由以外でACLやセキュリティグループの設定が変更された場合、即時にアラート

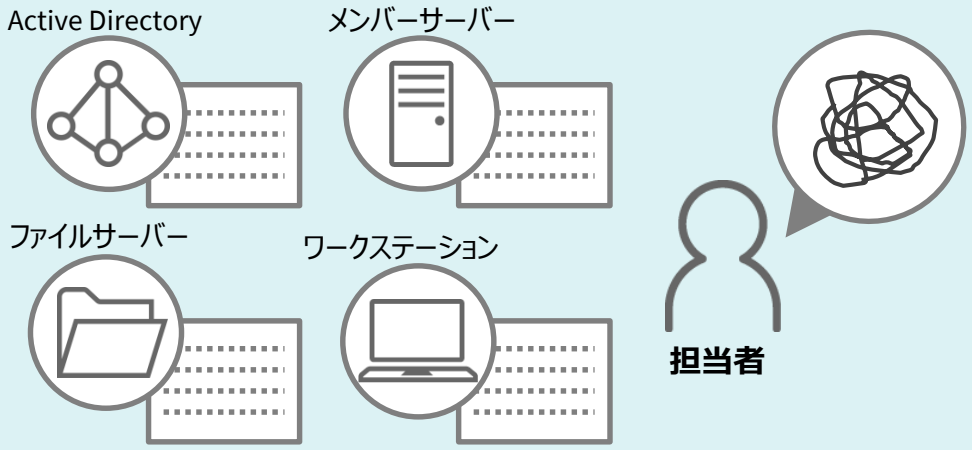
ACL設定の変更管理を監査することで外部攻撃や内部不正を早期に検知

© ZOHO Japan Corporation. All rights reserved.

フォルダやファイルへのアクセス状況の可視化

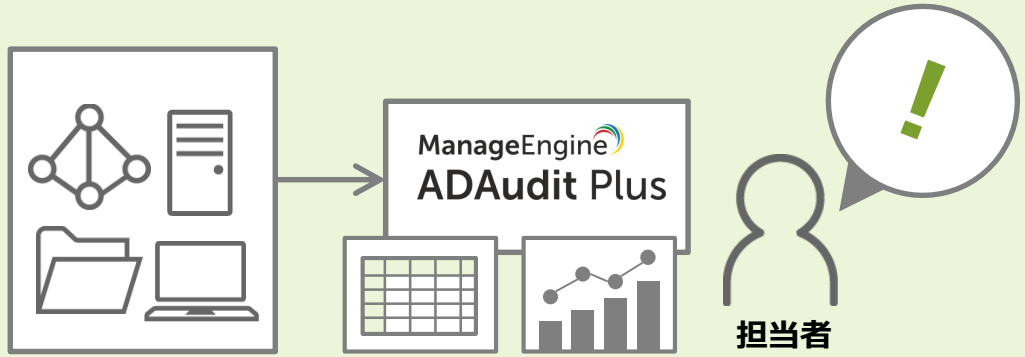
例：ファイルやフォルダに対する参照・変更・複製・移動・削除などの操作を監査する場合

Active Directory でのよくある運用



- 標的型攻撃や内部不正が生じているものの検知が難しく発生していることが認識しづらい
- ログが複雑で、解析するには専門的な知識が必要であり、煩雑で手間がかかる
- 被害が発生してから、初めて認識

ADAudit Plus の場合



- 標準で豊富なレポートが利用可能
- ファイルやフォルダへの参照・変更・複製・移動・削除などのログを可視化することで早期に検知
- 攻撃や不正の兆しを検知することで、被害の発生を未然に防止

フォルダやファイルへのアクセス状況を可視化することで外部攻撃や内部不正を早期に検知

© ZOHO Japan Corporation. All rights reserved.

導入事例：住友金属鉱山

導入の背景/課題

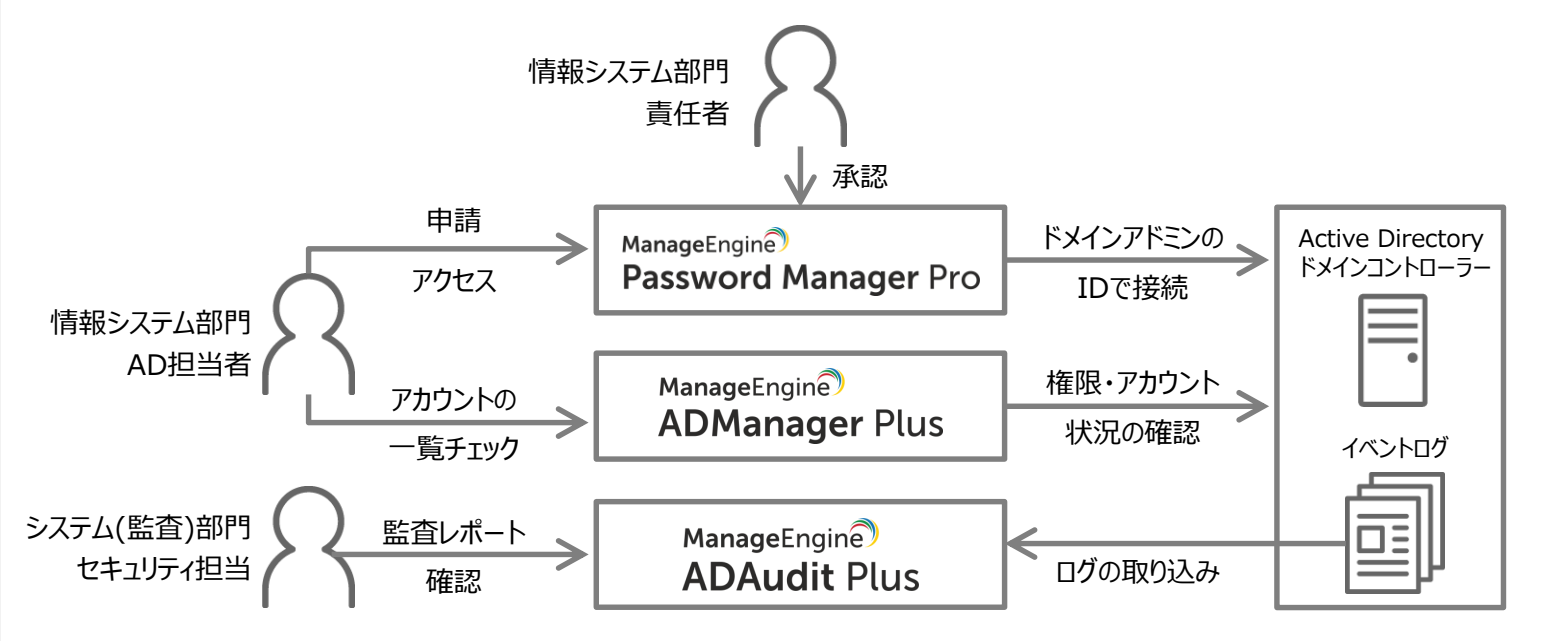
- これまでにも標的型攻撃対策を実施し、Active Directoryのログ監査についても課題意識を持っていた
- JPCERT/CCの文書「ログを活用したActive Directoryに対する攻撃の検知と対策」を受け、対策を行うことに決めた

導入の決め手

- 費用は他の提案と同程度ながら、ツールの使い勝手に大きな優位性を感じたため
- ADAudit PlusはActive Directoryに特化した製品であり、試用版での評価などから容易に活用できそうだという感触が得られたため

導入のメリット

- ADAudit Plusのコンソールで、複数あるドメインコントローラーの情報を一つの画面で確認できるようになった
- 何らかの問題が検知された場合、ADAudit Plusの画面から詳細内容や問題のあった端末を簡単に調べられるようになった
- ログオンエラー状況やログオンが確認されない端末が把握できるようになった



ManageEngineが提供するActive Directoryセキュリティ対策ソリューションマップ　※当事例では「ADAudit Plus」と「ADManager Plus」が採用

住友金属鉱山株式会社

事業内容　資源開発、非鉄金属製錬業、電子材料・機能性材料の製造、その他

URL　www.smm.co.jp/

以前よりきめ細かい監視を実現しつつ、システム保守費80%を削減

© ZOHO Japan Corporation. All rights reserved.

参考費用例

年間ライセンス

- 1年間利用可能な製品ライセンスで、年間保守サポートサービスが含まれています。
- 1年ごとに年間ライセンス契約を更新します。

通常ライセンス

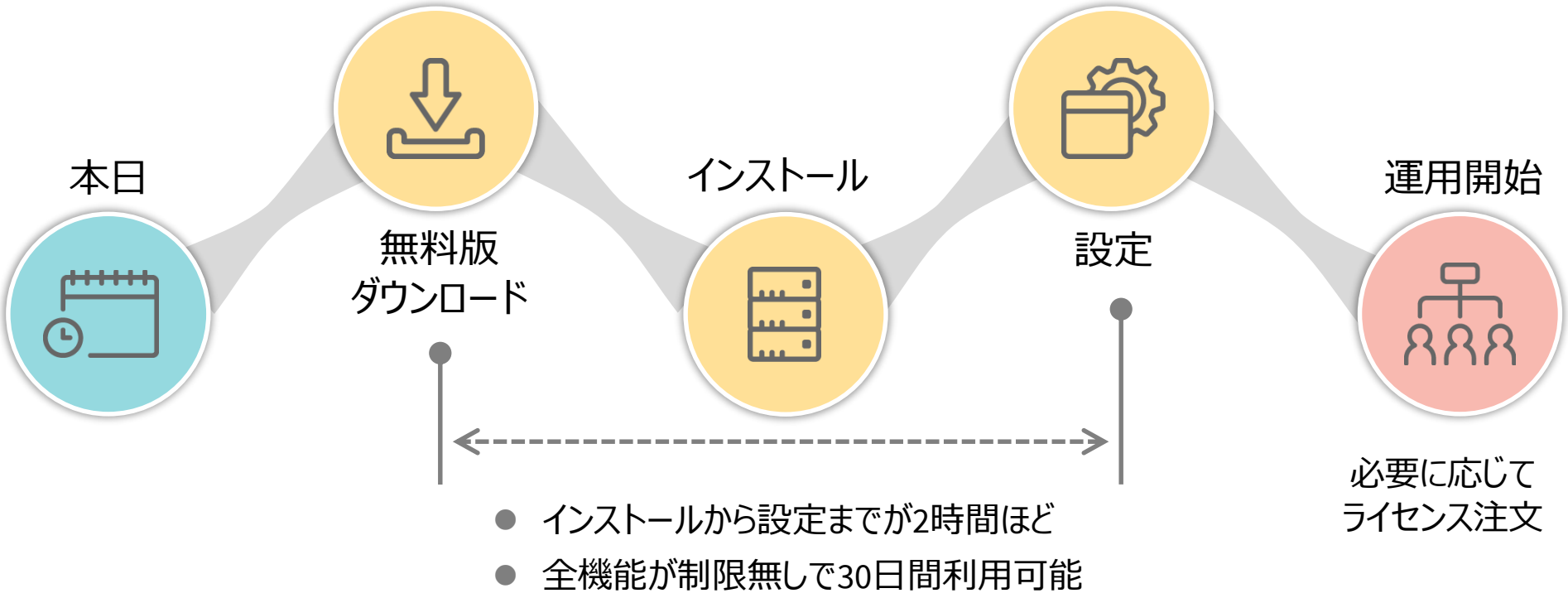
- 無期限の製品ライセンスに、初年度のみの年間保守サポートサービスが含まれています。
- 2年目以降は1年ごとに年間保守サポートサービス契約を更新します。
- 4年以上利用する場合は、価格が抑えられます。

AD ID管理	AD監査・ファイルサーバーレポート
ManageEngine ADManager Plus	ManageEngine ADAudit Plus
1ドメインを1人で管理する場合	ドメインコントローラー2台とファイルサーバー2台の監査レポートを作成する場合
年間ライセンス **年間22.8万円～**	**年間ライセンス** **年間39.8万円～**
通常ライセンス **50.3万円～**	**通常ライセンス** **123.3万円～**

具体的な費用・御見積に関しては、ご連絡ください

© ZOHO Japan Corporation. All rights reserved.

導入ステップ



数ステップで導入できます

© ZOHO Japan Corporation. All rights reserved.

無料版 / 評価版ダウンロード(技術サポート付き)

ADManager Plus
無料版ダウンロード

ADAudit Plus
無料版ダウンロード

ご用意いただくもの

インストールするサーバー×1台

インターネットブラウザー

評価に必要なWebサーバー、データベースサーバーなどはバンドルしています。

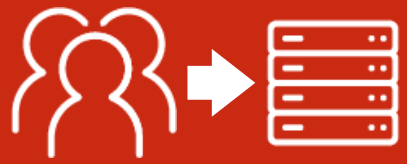
また、評価期間中は、無償で技術サポートを受けられます。評価期間が終了すると、自動で無料版に移行します。
評価版をダウンロードする際は、必ず「ソフトウェアライセンス契約」をご確認ください。

評価期間中は無料でお使いいただけます

© ZOHO Japan Corporation. All rights reserved.

ファイルサーバーのアクセス権限管理の特徴まとめ

ファイルサーバーに対する
アクセス権限管理の最適化



ManageEngine
ADManager Plus

- ユーザーに適切な権限をスピーディーにミスなく設定
- ユーザーにどんな権限が付与されているのか簡単に権限を棚卸し

認証ログやACL・セキュリティ
グループの設定およびファイルや
フォルダへのアクセス状況の監査

ManageEngine
ADAudit Plus

- どのユーザーが異常なアクセスをしているのかを可視化
- ACLやセキュリティグループの設定が不正に変更されていないか可視化
- ユーザーがフォルダ・ファイルへどのような操作をしているのかを可視化

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三丁目6番1号
みなとみらいセンタービル13階

045-319-4612（ManageEngine 営業担当）

https://www.manageengine.jp/

jp-mesales@zohocorp.com

販売元

※ご連絡先を入力してご利用ください

ファイルサーバーのアクセス権限管理の包括的な効率化とセキュリティ向上をサポート

© ZOHO Japan Corporation. All rights reserved.