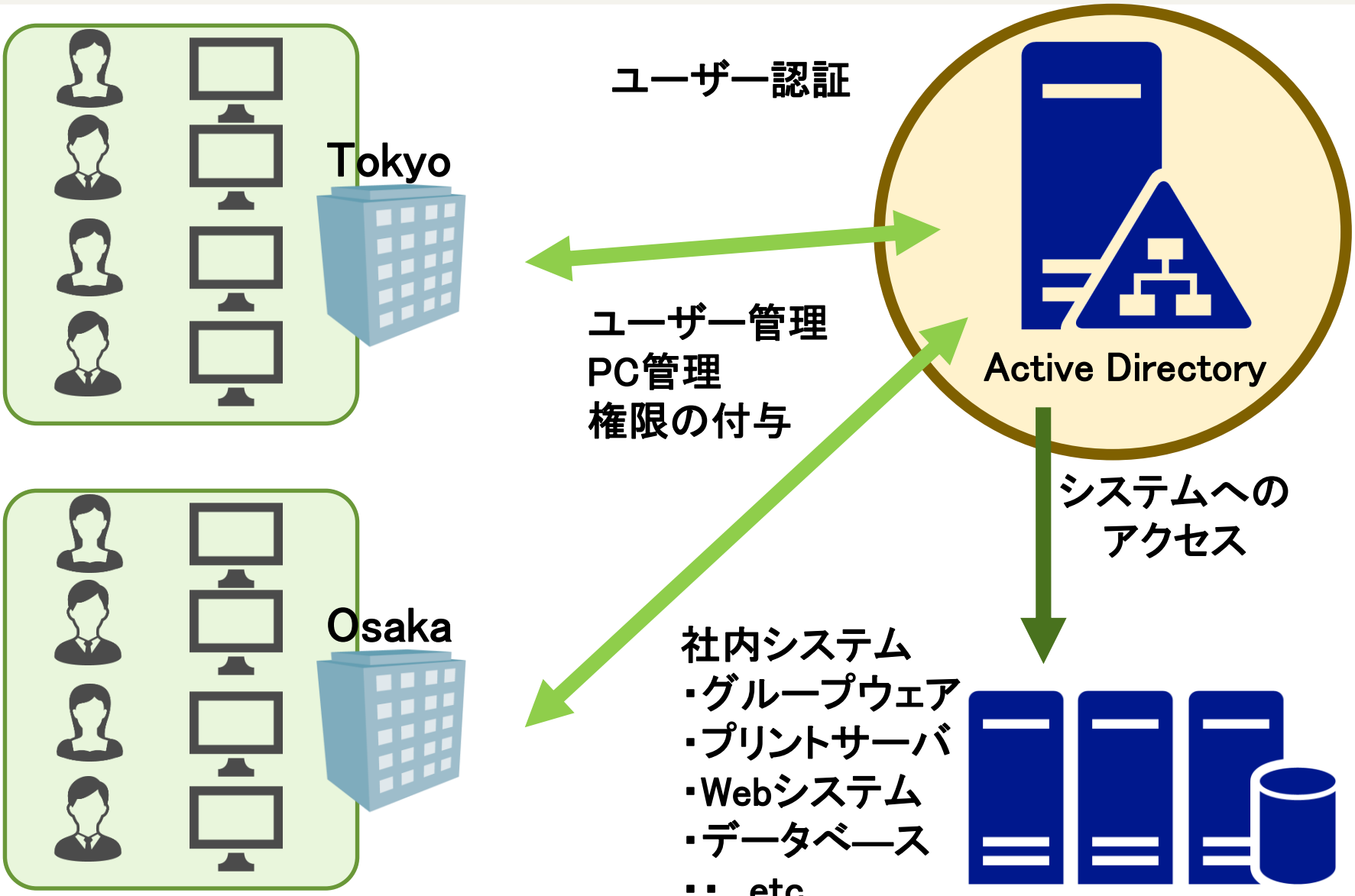
Active Directory運用の実際

～セキュリティの担保と効率的な運用～

株式会社フェス

ADの利用環境



ADにおける運用業務

運用業務の例	頻度	難度
ユーザー/ユーザーグループの 追加/変更/削除	大	低
コンピュータの 追加/変更/削除	大	低
グループポリシー/OUの 追加/変更/削除	中	高
ユーザー/コンピュータの棚卸	小	中
パスワードリセット	大	低
ロックアウト時等の調査	小	中

AD運用における課題・問題①

特権IDの共用

- オペレータや外部委託者による、特権ID「Domain Admins」等のドメイン管理者権限使い回し
  - 作業ミスによるリスク
    - 重要なユーザーやコンピュータの削除　・・等
  - 悪意ある操作/情報漏えいのリスク
    - 管理者権限による操作/重要情報の奪取　・・等

AD運用における課題・問題②

運用工数の増大（エンドユーザー対応）

- ユーザー増加に伴う日々の運用負荷増大
  - 日常的にユーザーアカウント変更や追加に追われる　・・等
  - 不適切なアカウント管理
    - ユーザー退職時に、タイムリーにユーザ削除ができていない　・・等

AD運用における課題・問題②

運用工数の増大（AD管理）

- セキュリティや影響の大きさからシビアな管理が求められるための負荷増
  - OUやグループポリシーの変更に、時間と労力がかかる　・・等
- アカウントが把握できない
  - 不要アカウント、不要コンピュータの棚卸やアカウントの見直し、削除等ができない　・・等
- 特権ID貸し出しの申請、承認に手間がかかる

AD運用における課題・問題③

操作証跡をとっておらず分析ができない

- ADのイベントログがない
  - 短期間しかイベントログを保持できない　・・等
- 分析、調査ができない
  - 膨大なログから、システムへのログオン記録を検索するため、大きな労力と時間が必要　・・等

AD運用のあるべき姿

適切な権限付与

- 必要最低限の権限を、必要なユーザーへ割り当て（特権の管理）

効率的な運用

- ツール導入による、アカウント管理における手作業/Excel/紙運用の廃止

適切な証跡管理

- イベントログを検索可能なシステムへ格納
- ログの可視化／異常検知

ツール適用の例

適切な権限付与

- 必要最低限の権限を、必要なユーザーへ割り当て（特権の管理）

ManageEngine Password Manager Pro

効率的な運用

- ツール導入による、アカウント管理における手作業/Excel/紙運用の廃止

ManageEngine ADManager Plus

適切な証跡管理

- イベントログを検索可能なシステムへ格納
- ログの可視化/異常検知

ManageEngine ADAudit Plus

ManageEngine EventLog Analyzer

フェスのサービス

AD管理の仕組みの構築

- 特権ID管理、運用管理、証跡管理のコンサルティング
  - AD管理経験豊富なコンサルタントが支援
- ツール導入支援
  - 金融・製造・官公庁・物流・教育など多数の導入実績！

AD管理の運用支援

- 初期運用支援
  - ツール導入時の課題解決
- 継続的改善支援
  - ツール導入後の運用改善

実例）
ログ管理ツールに多量のログが表示され、異常か判別できない
→ログの削減方法、ツール上のフィルタリング方法をアドバイス

END

～Thank you～