Active Directory を 秩序ある状態に保つために

株式会社 ソフィアネットワーク
新井 慎太朗（あらい しんたろう）

自己紹介

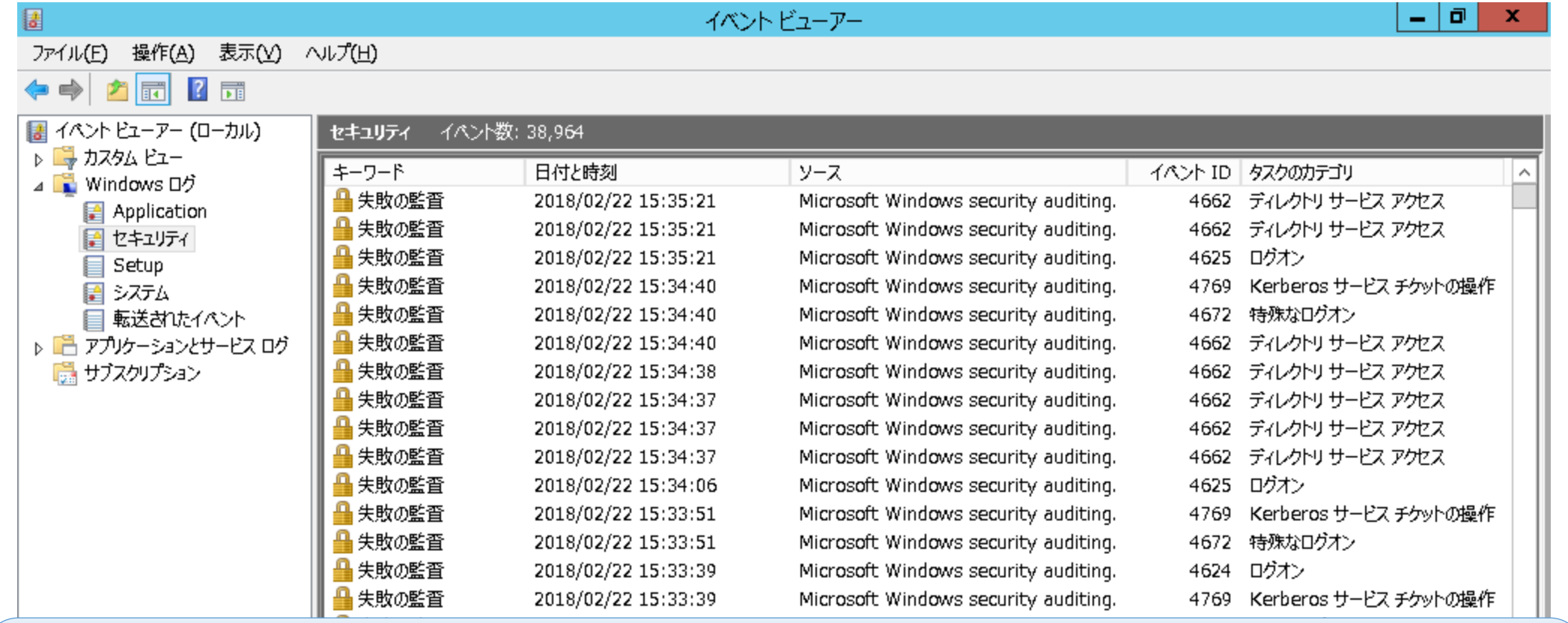
- 新井 慎太朗（あらい　しんたろう）
  - 株式会社 ソフィアネットワーク 所属
    http://www.sophianetwork.co.jp/
  - マイクロソフト認定トレーナー (MCT)
  - Microsoft MVP for Enterprise Mobility

- 主な執筆
  - 徹底攻略 MCP 問題集
    - Windows Server 2016［試験番号:70-740］対応
    - Windows 10［試験番号:70-697］対応
    - Windows 10［試験番号:70-698］対応
  - ひとり情シスのための Windows Server 逆引きデザインパターン -Windows Server 2016対応-

目次

1 章
適切な管理および運用が
できていますか？

まずは、この画面をご覧ください

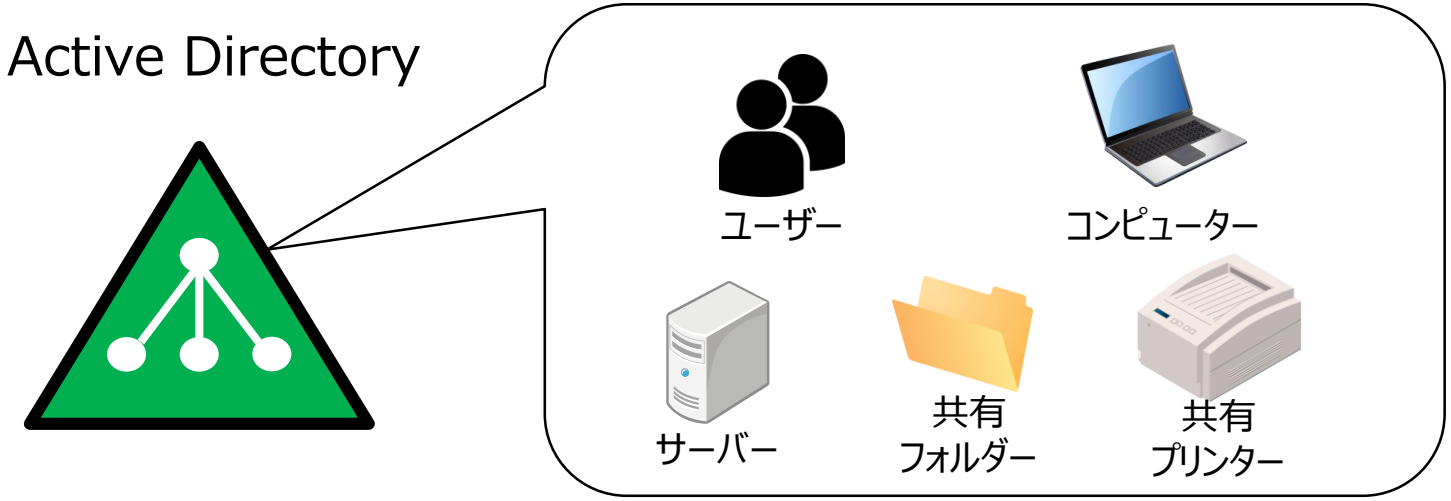


万が一、悪意のあるユーザーから実際に攻撃を受けたとしても
その攻撃の検知や追跡をおこなうことは困難

Active Directory のおさらい

■Active Directory とは

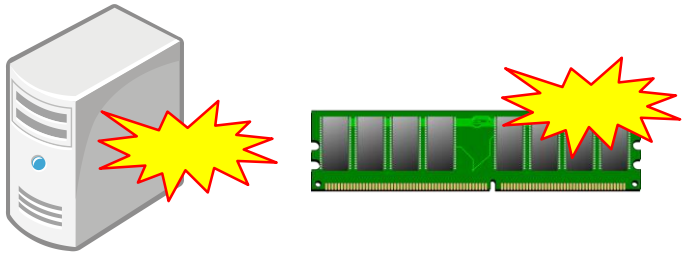
■アカウントやリソースの情報を集中管理する仕組み



管理者権限の情報などの重要な情報が格納されているため、
攻撃者から狙われやすい

Active Directory が受ける攻撃の手口

■攻撃のために悪用される情報の例
- ■OS や Kerberos 認証の脆弱性
- ■メモリに保存された認証情報のハッシュ値

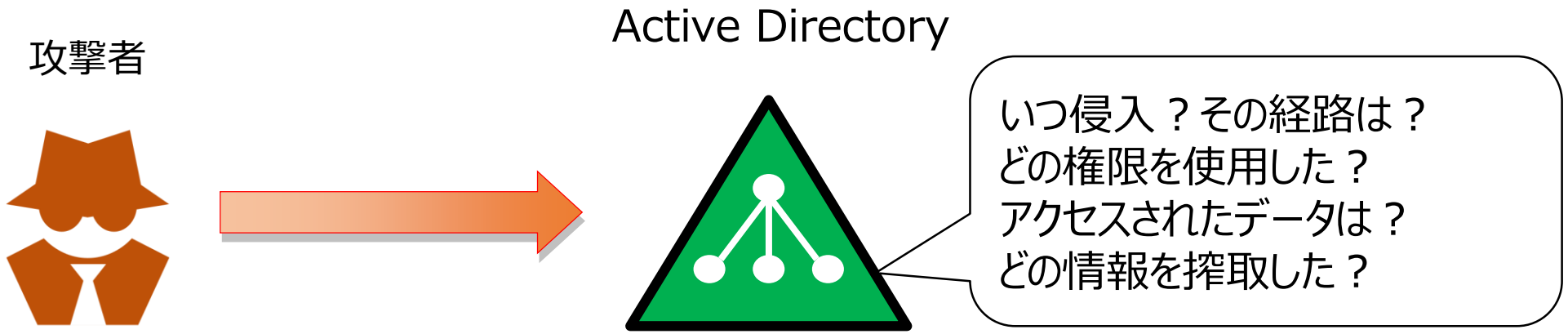


■手口の例
- ■標的型攻撃などによりエンドユーザーの PC へ侵入し、組織内のサーバーやドメインコントローラーへのアクセスを試行

適切な管理および運用ができていないと・・・

■攻撃されたことに気づくまでに時間がかかる

■悪事を追跡することが難しくなる

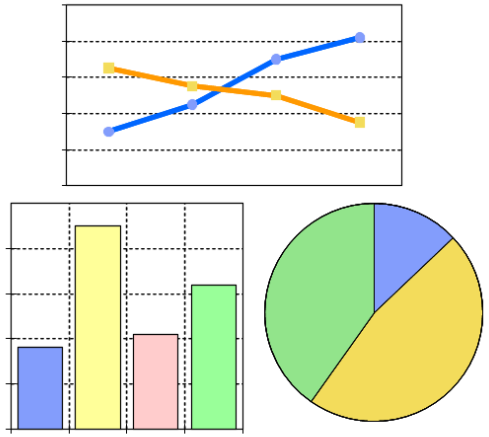


混沌としたアカウントやログの登録状況では、
攻撃を受けたときの被害も大きくなる

2 章
混沌とした状況を
回避するためには？

このような状況を回避するには

- ツール (製品) の導入
  - 現状分析
  - 状況把握のしやすさの向上
  - 秩序ある状態にするための手がかりに

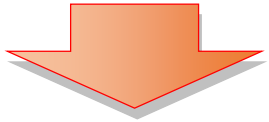


ツールを導入すれば、それで十分か？

■ツールをうまく活用するためには、ベースが重要

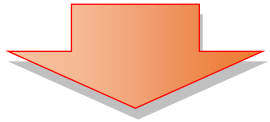
■ベースとなる情報が適切に管理および運用されている前提

ユーザーアカウントの部署や
連絡先などが登録されていない



ログ確認のための連絡が
すぐに取れない

複数の従業員によって
共有アカウントが使用されている



実際にどの従業員の操作なのか
追跡できない

情報が適切に管理/運用されていないと
ツールを入れてもゴミしか出ない

秩序ある状態を保つためには

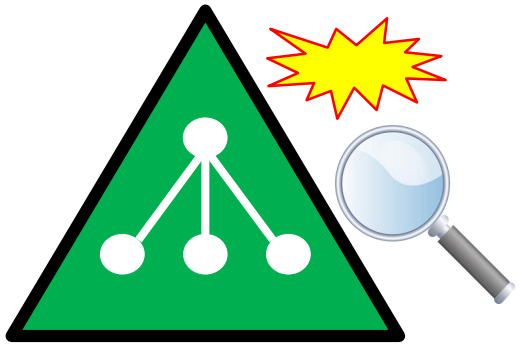
- 必要な情報が適切に登録されていることは大前提
  - ログから検知や追跡をおこなうために必要な情報が登録されているか

- 管理および運用が適切に行われているかどうか
  - 不要なメンバーがグループに登録されていないか
  - 不要なアカウントが放置されていないか
  - 共有アカウントとして利用されていないか

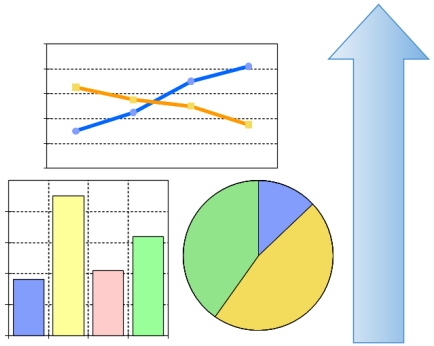
”地道な作業”が重要

“地道な作業”による効果

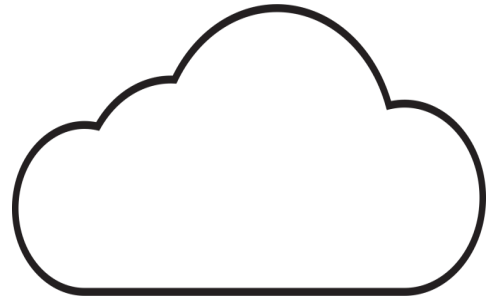
- ■攻撃への素早い検知と適切な対処
- ■ツールの導入によって得られる効果の最大化
- ■クラウド時代への対応



素早い検知と適切な対処



ツール導入効果の最大化



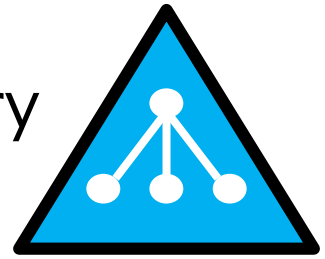
クラウドへのスムーズな対応

3 章
クラウド時代に
対応していくためには？

クラウド時代への対応

■Microsoft が提供するクラウドサービスの例

Azure Active Directory



Office 365

Microsoft Intune

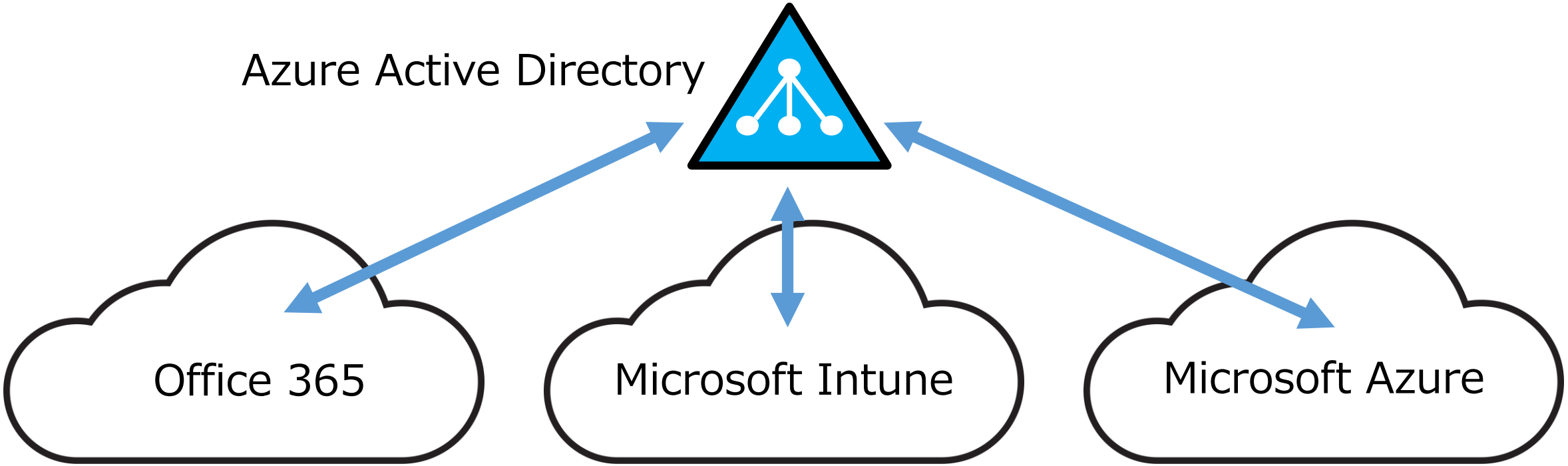
Microsoft Azure

クラウドサービスは、Azure AD を認証/承認基盤として使用

Azure AD とは

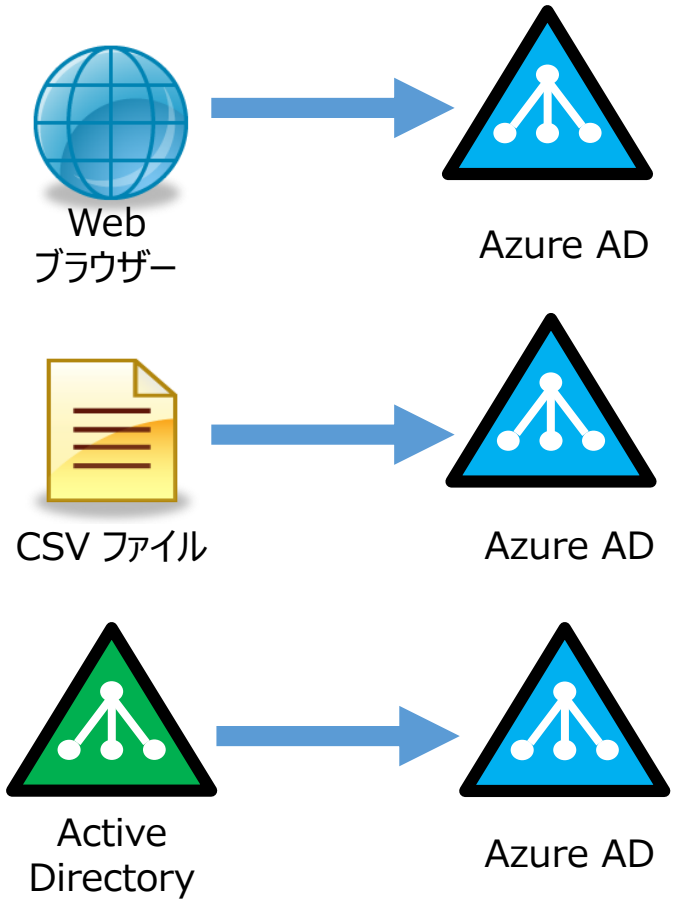
■クラウド上のディレクトリサービス

■クラウドサービスへのアクセスの認証および承認に使用される



Azure AD へのアカウント登録方法

- 手動登録
  - Microsoft Azure 管理ポータルにアクセス
- CSV ファイルを用いた一括登録
  - Windows PowerShell コマンドレットを使用
- オンプレミスの Active Directory を同期
  - Microsoft から提供される同期ツールを使用



Azure AD Connect

■Microsoft から提供される同期ツール

Active Directory を秩序ある状態に保つことは
クラウド対応にも良い効果を生む

４ 章
まとめ

まとめ

■Active Directory を秩序ある状態に保つ意味

- ✓ Active Directory のセキュリティと運用管理のバランスをとる鍵
- ✓ 今後も進んでいくクラウド時代への対応

■そのために今からすべきこと

- ✓ 各組織の Active Directory 環境の見直し
- ✓ Active Directory の情報を整理することが第一歩