Active Directoryによる統合セキュリティ管理

グローバルナレッジネットワーク株式会社
横山 哲也
Microsoft MVP for Windows Server – Directory Services

自己紹介

- 1994年～ ITプロ向けWindows関連教育
- 2003年～ マイクロソフトMVP
- 最近の著書・雑誌記事
  - 実践Active Directory逆引きリファレンス (毎日コミュニケーションズ)
  - ひと目でわかるMicrosoft Windows Server 2003ネットワーク設定・管理術(日経BP)
  - Windows Server 2003完全技術解説(日経BP)
- Twitter ID: yokoyamat

Agenda

- Active Directoryと企業システム
- パスワード
- グループポリシー
- セキュリティ設定の一元管理
- 修正プログラムの一元管理
- ファイルアクセス許可の一元管理

Active Directoryと企業システム

- ワークグループ
- ドメイン
- シングルサインオン
- ディレクトリサービス

ワークグループ

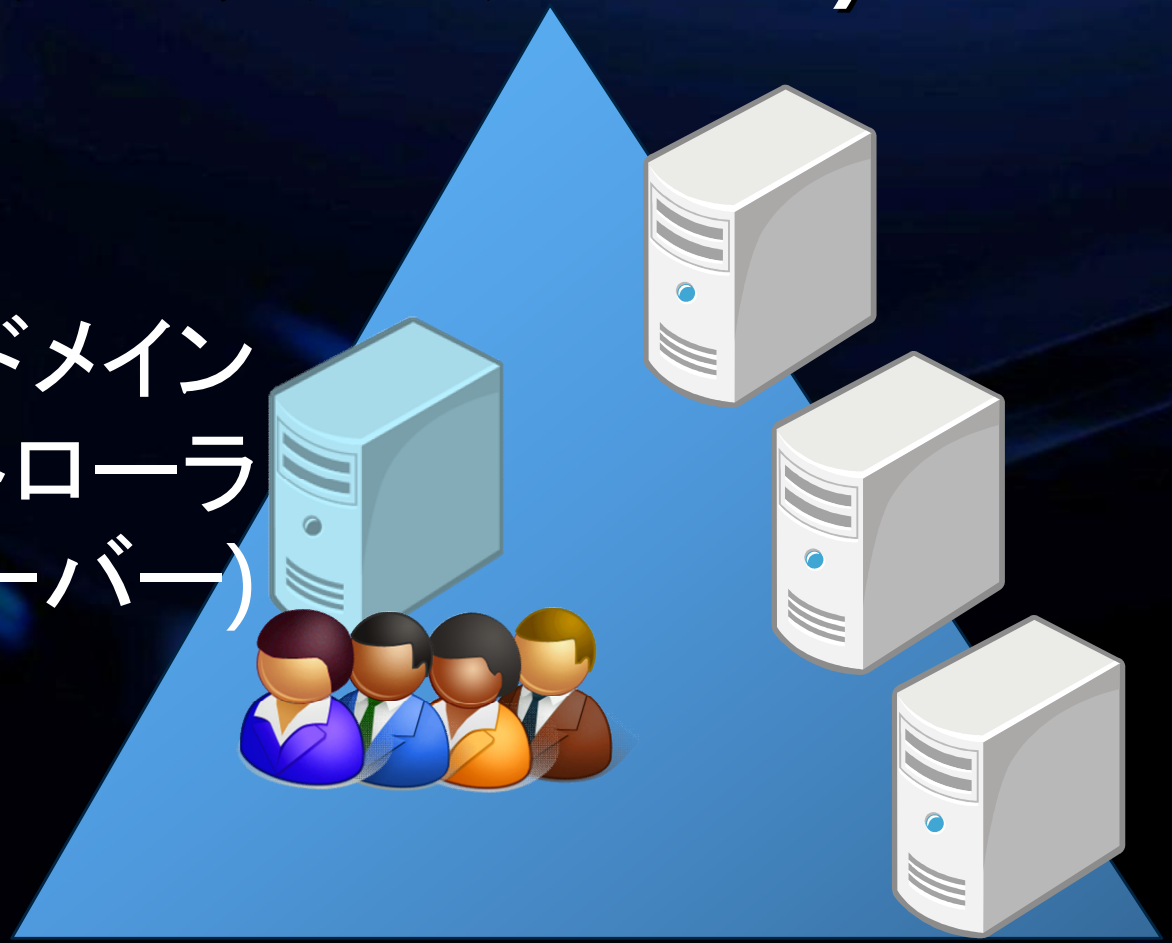
- ユーザー情報をコンピュータ単位で管理
  - レジストリ内のSAM
    (Security Account Manager)
- コンピュータごとにユーザー登録が必要

ドメイン

Active Directoryドメインサービス: AD DS

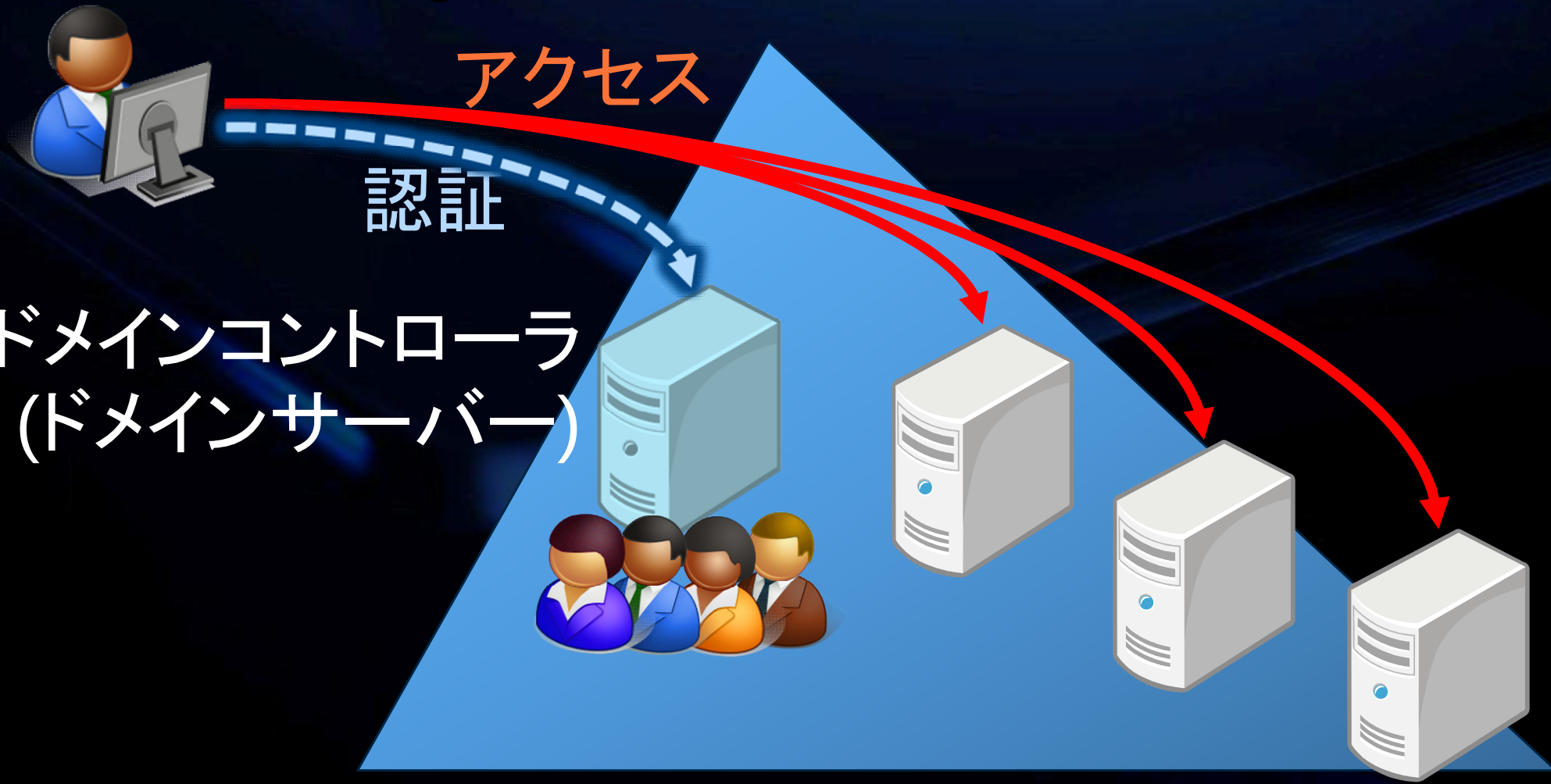
- ユーザー登録データベース
  (ディレクトリデータベース)

ドメイン
コントローラ
(ドメインサーバー)



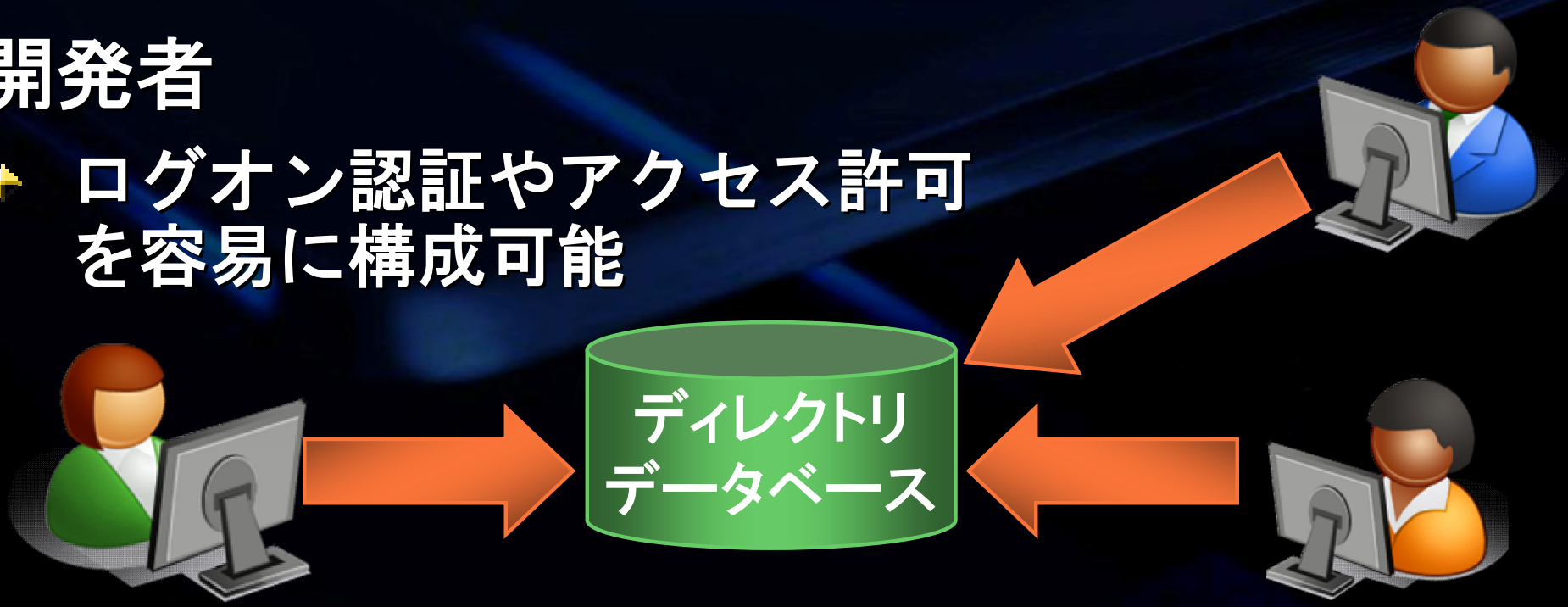
シングルサインオン

- ログオン時の情報で全サーバーを利用可能
- IE/IISやSQL Serverなどの統合認証



ディレクトリサービス

- 利用者
  - ドメイン内のあらゆる資源利用可能
- 管理者
  - ユーザーやコンピュータの一元管理が可能
- 開発者
  - ログオン認証やアクセス許可を容易に構成可能



パスワード

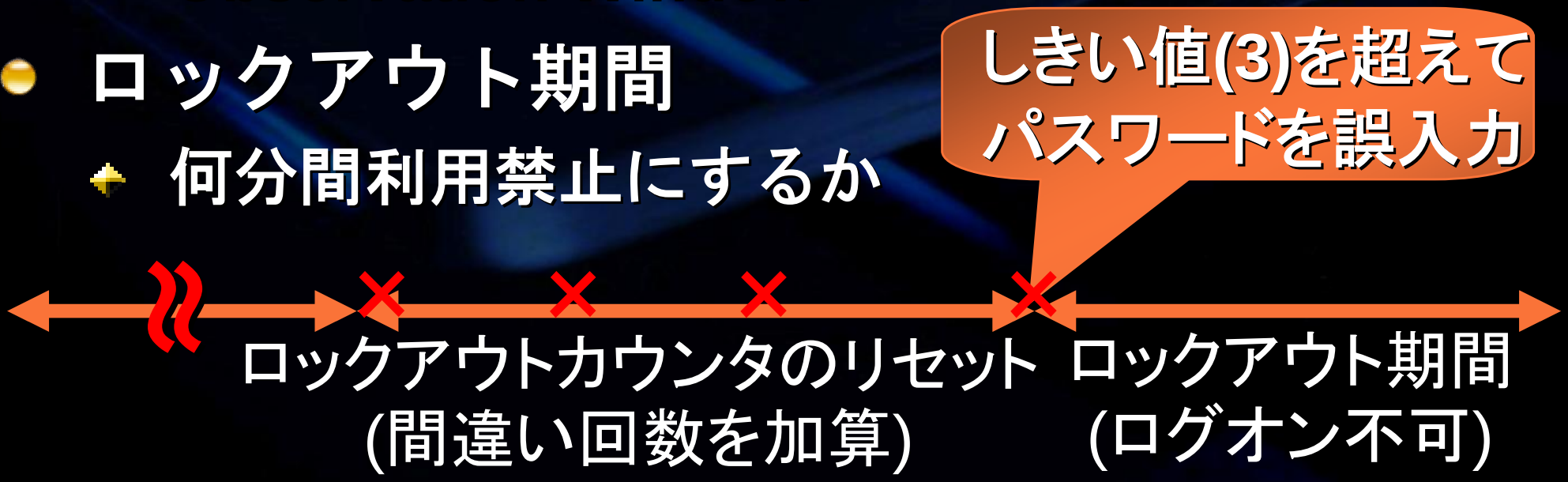
- パスワードポリシー
- ロックアウトポリシー
- パスワードの留意点

パスワードポリシー

- パスワードの長さ(最低長)
- パスワードの有効期間(最長期間)
- パスワードの変更禁止期間(最短期間)
- パスワードの履歴を記録する(再利用制限)
- パスワードは複雑さの要件を満たす
  - 英大文字、小文字、数字、記号のうち3種類
  - ユーザー名と異なる不可
- 暗号化を元に戻せる状態でパスワードを保存
  - UNIXベースのKerberos等の互換用

ロックアウトポリシー

- ロックアウトのしきい値
  - 何回連続して間違えても良いか
- ロックアウトカウンタのリセット
  - 何分間経てば間違えても許されるか
  - Observation Window
- ロックアウト期間
  - 何分間利用禁止にするか



パスワードの留意点

- 利用者への注意
  - 単純な規則にしない(Pa$$w0rd、末尾-1等)
  - 難しいパスワードは使いにくい(P!”#$iAd等)
  - パスワード強度は文字種と長さで決まる
    (人間にとっての難しさではない)
- パスワードポリシー
  - 長いパスワードを使う
  - 複雑さを要求する
- ロックアウトポリシー
  - 本当に必要か検討(ロックアウト攻撃のリスク)

グループポリシー

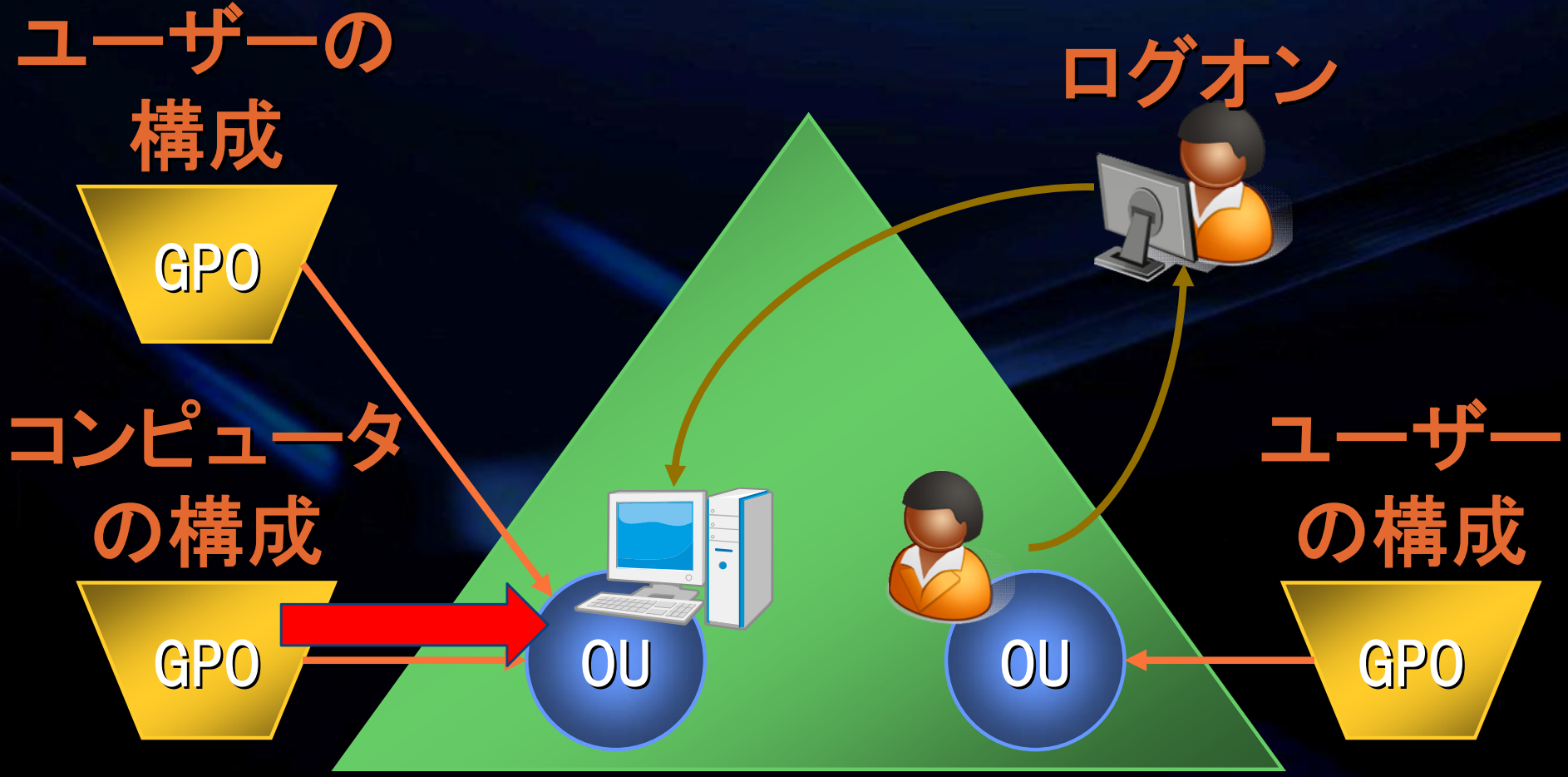
- グループポリシーの意味
- コンピュータの構成
- ユーザーの構成
- ループバックの処理モード

グループポリシーの意味

- システムの構成を利用者に強制
- セキュリティ…放置すると緩くなりがち
  - トラブル1: 厳しすぎて仕事ができない
  - トラブル2: 管理者の裏をかく
- 複雑な構成…利用者による設定が困難
  - トラブル1: 利用者が思っていた設定と違う
  - トラブル2: 環境が違っても融通が利かない
- 基本的な考え方
  - システム管理者が、利用者の代わりに設定

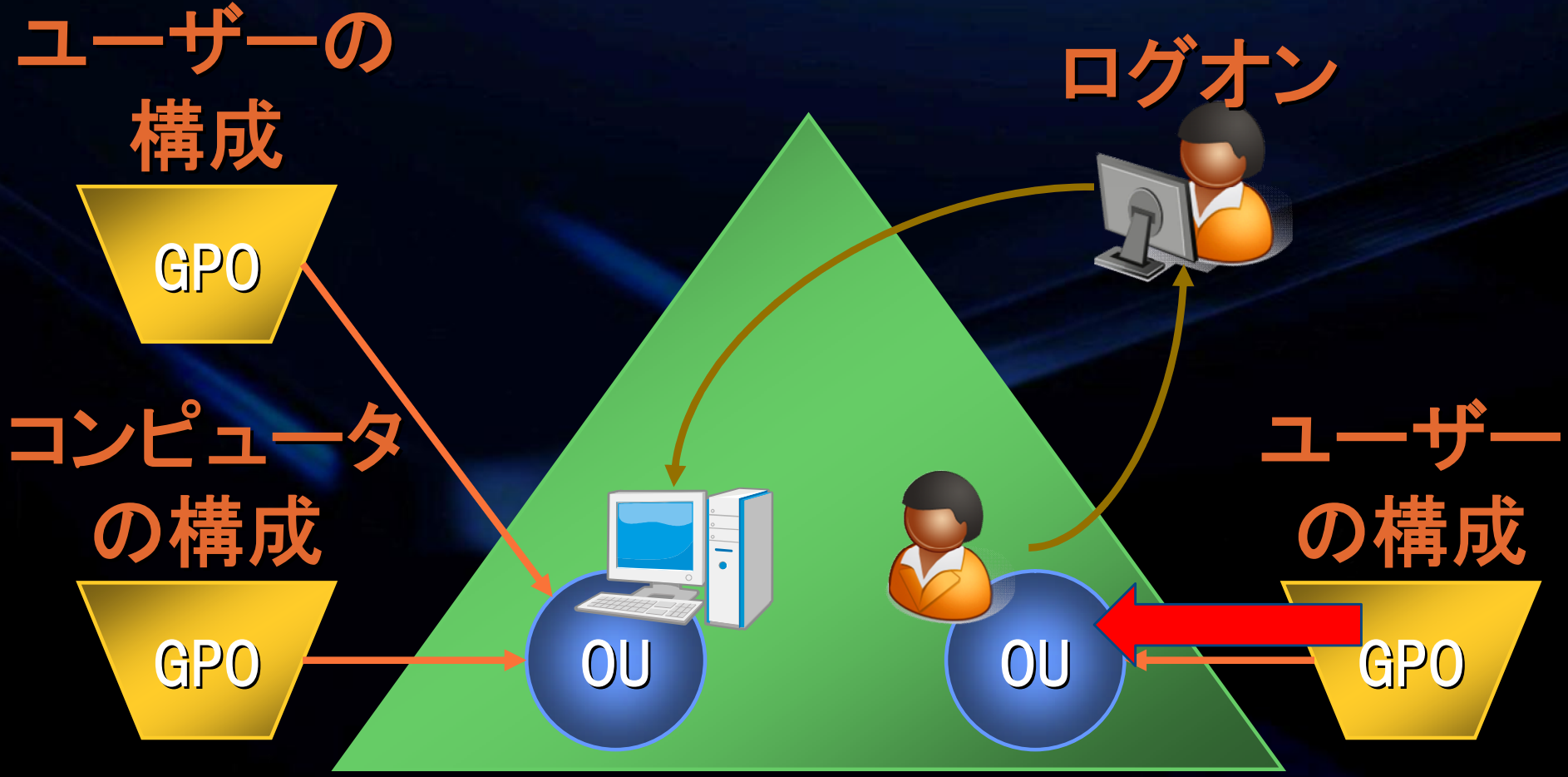
コンピュータの構成

- コンピュータアカウントのある場所に適用
- 例: レガシープロトコルの利用、サービス



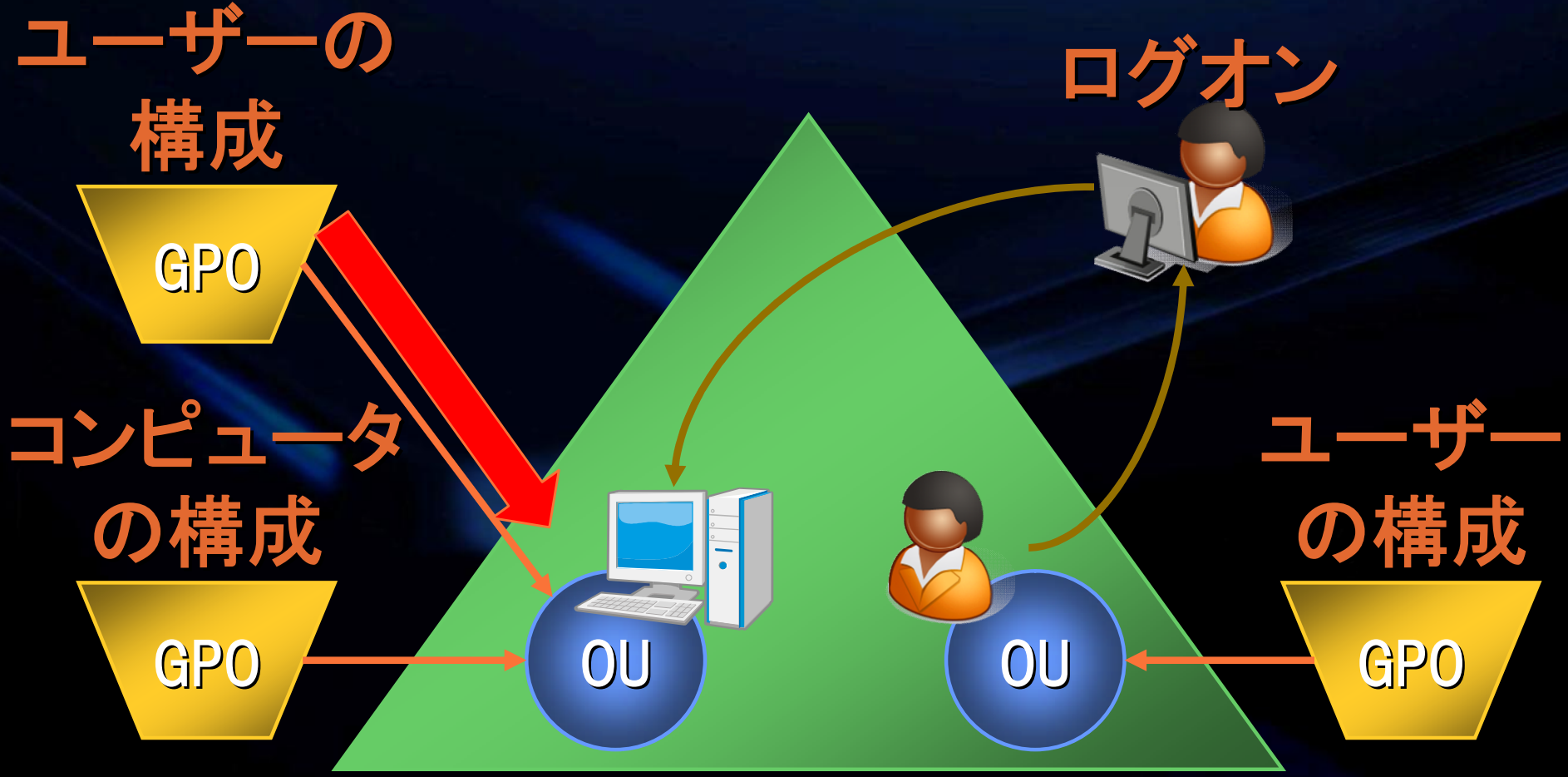
ユーザーの構成

- ユーザーアカウントのある場所に適用
- 例: スクリーンセーバー、エクスプローラ



ループバックの処理モード

- 本来はユーザーのポリシーなのに
  コンピュータに対して割り当て



セキュリティ設定の一元管理

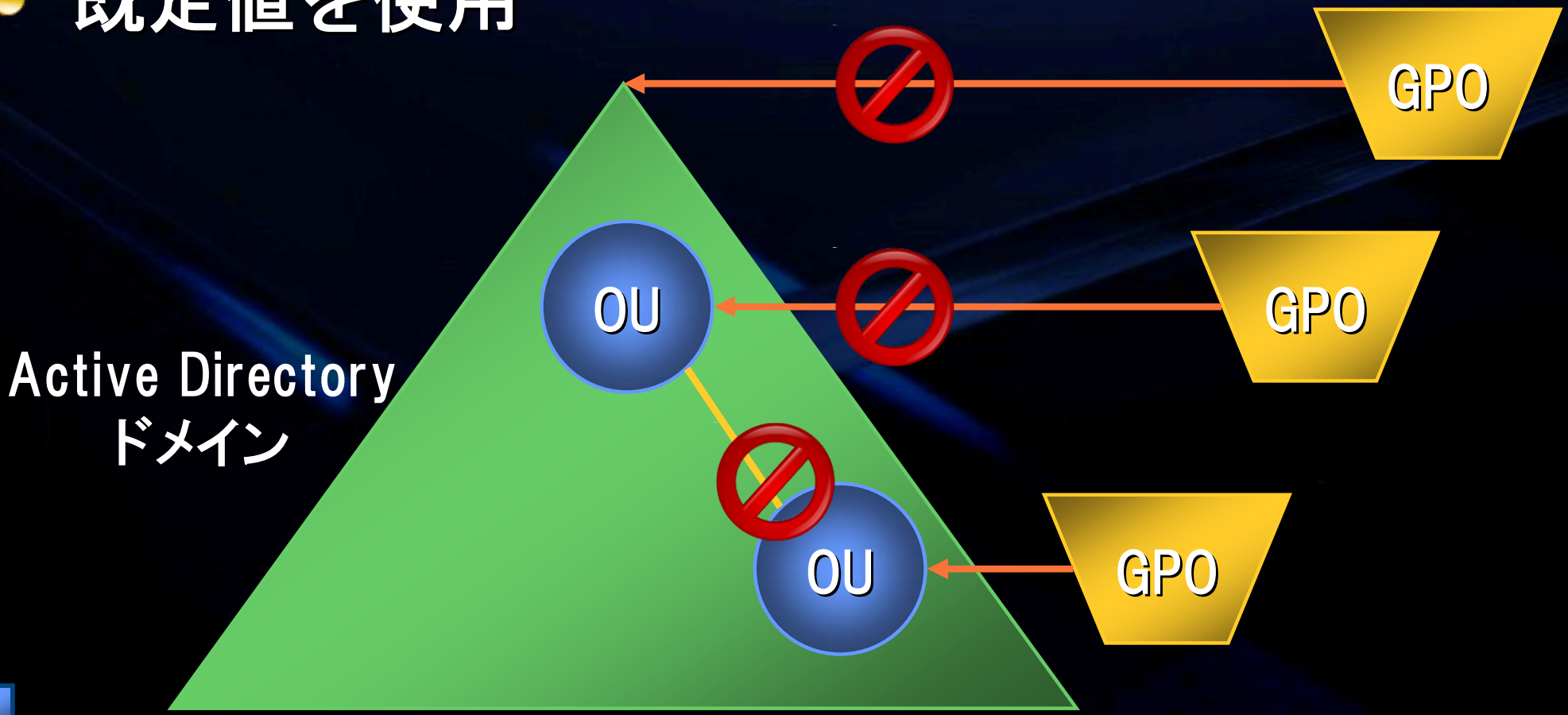
- GPOの継承
- GPOの継承禁止
- GPOの強制
- GPO適用のフィルタリング

GPOの継承

- ユーザー環境の統一(強制)
- コンピュータ設定の統一(強制)
- ソフトウェアの自動インストール
- …

GPOの継承禁止

- 上位OUからの継承を禁止
- 上位GPOが存在しないのと同じ
- 既定値を使用



GPOの強制

- 特定のGPOを優先的に適用
- 競合しない設定は累積
- 継承禁止よりも優先

GPO適用のフィルタリング

- セキュリティフィルタ
  - GPOにACL(アクセス許可)を設定
  - GPOの適用 = 読み取り + 適用
  - 静的フィルタリング
- WMIフィルタ
  - Windows XP以降のクライアント
  - クライアント側でWMIクエリを実行
  - 動的フィルタリング

GPOの適用原則
ベストプラクティス

- なるべく既定値を使う
  - ローカル
    →サイト→ドメイン→上位OU→下位OU
- 強制は全社セキュリティに限定
- 継承禁止は使わない
- セキュリティフィルタリングは禁止に使う
- WMIフィルタリングは必要最小限に留める

修正プログラムの一元管理

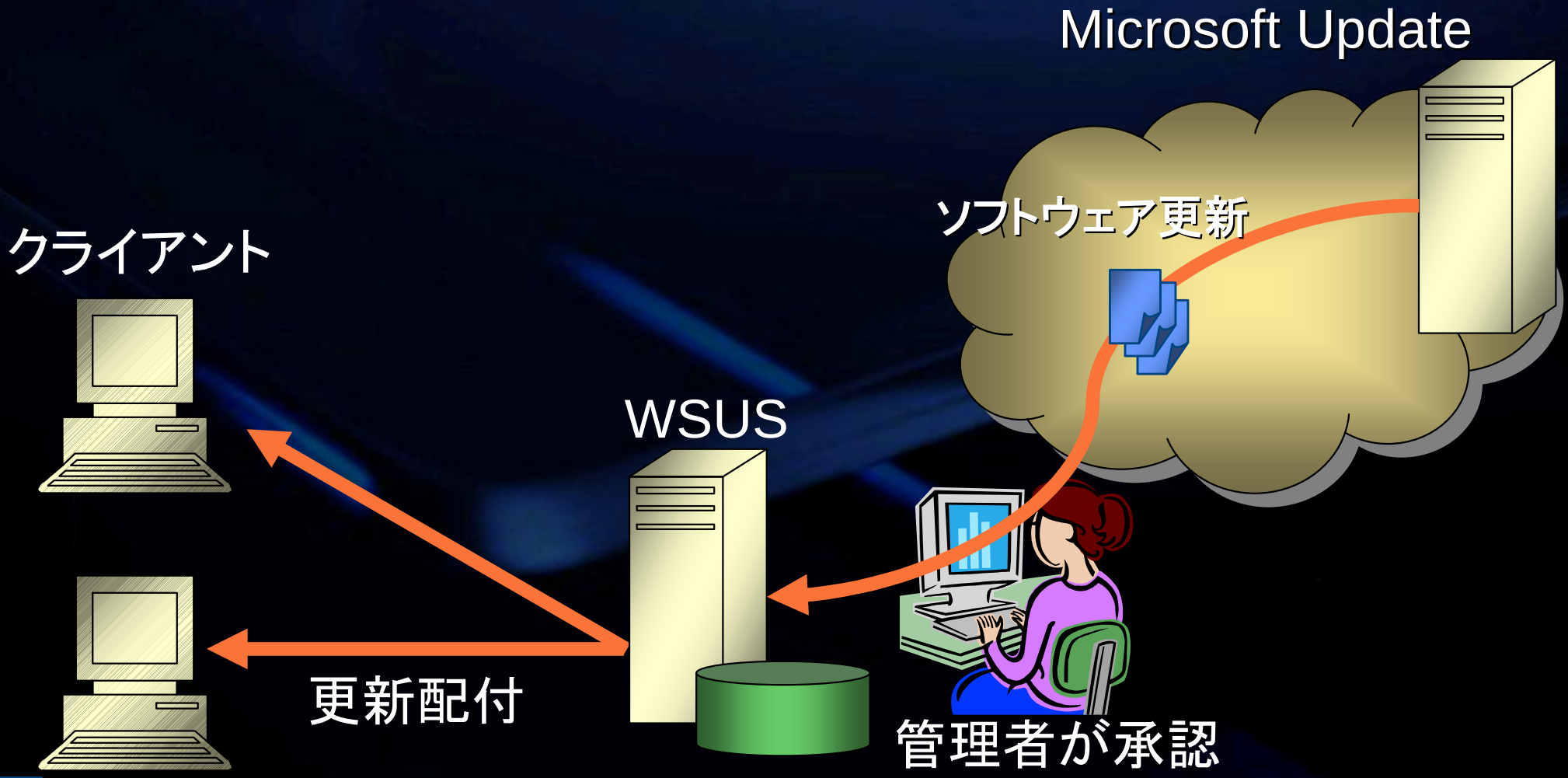
- Windows Update
- Windows Server Update Services
- System Center Configuration Manager

Windows Update
Microsoft Update

- 更新の可否と時刻...利用者個人またはGPO
- 更新内容...選択不可

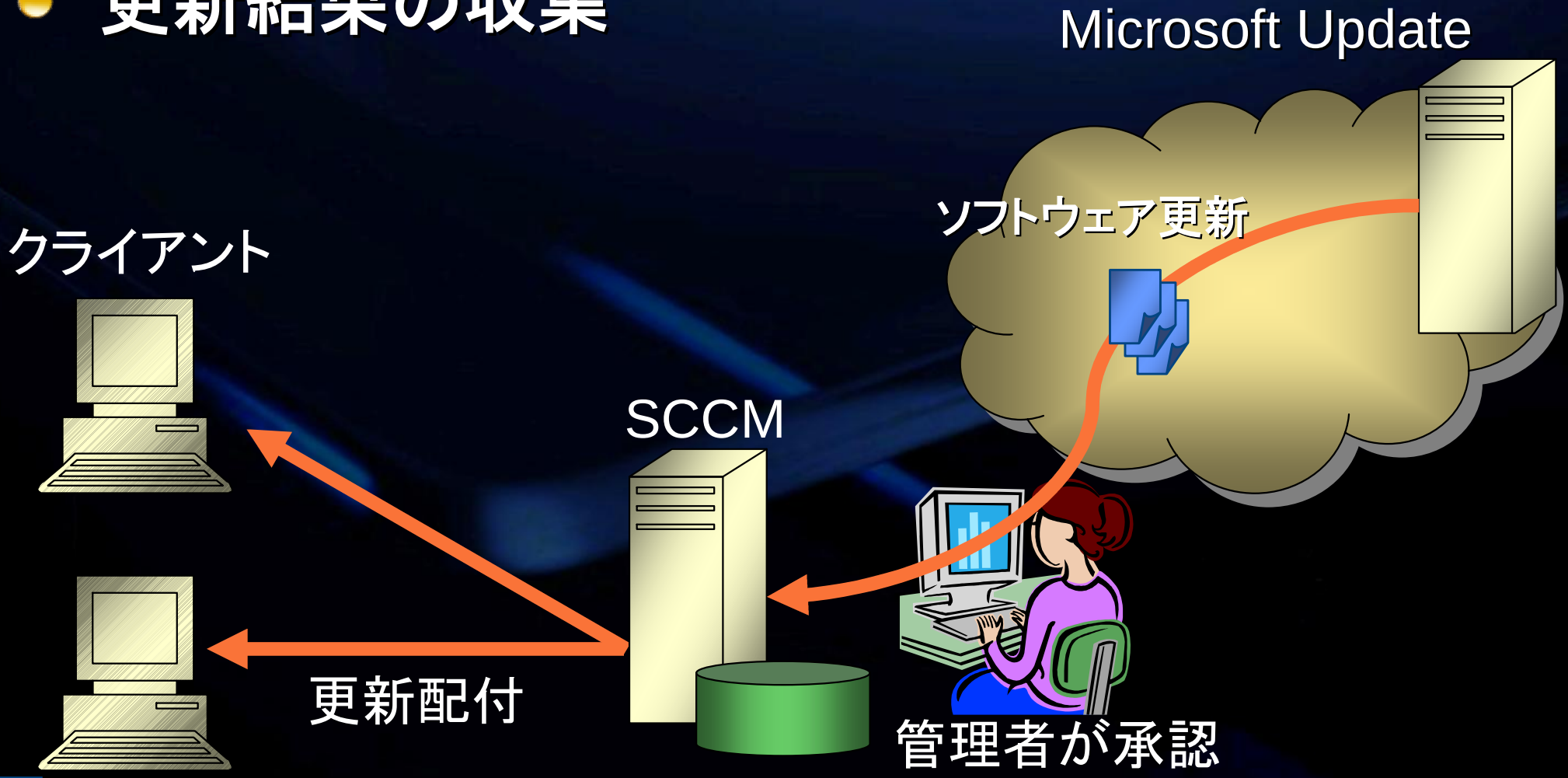
WSUS
Windows Server Update Services

- 適用するかどうかを管理者が判断可能



SCCM
System Center Configuration Manager

- より詳細な条件指定
- 更新結果の収集



ファイルアクセス許可の一元管理

- アクセス許可戦略
- A-G-L-Pポリシー
- A-G-DL-Pポリシー
- A-G-U-DL-Pポリシー
- アクセス許可戦略のまとめ

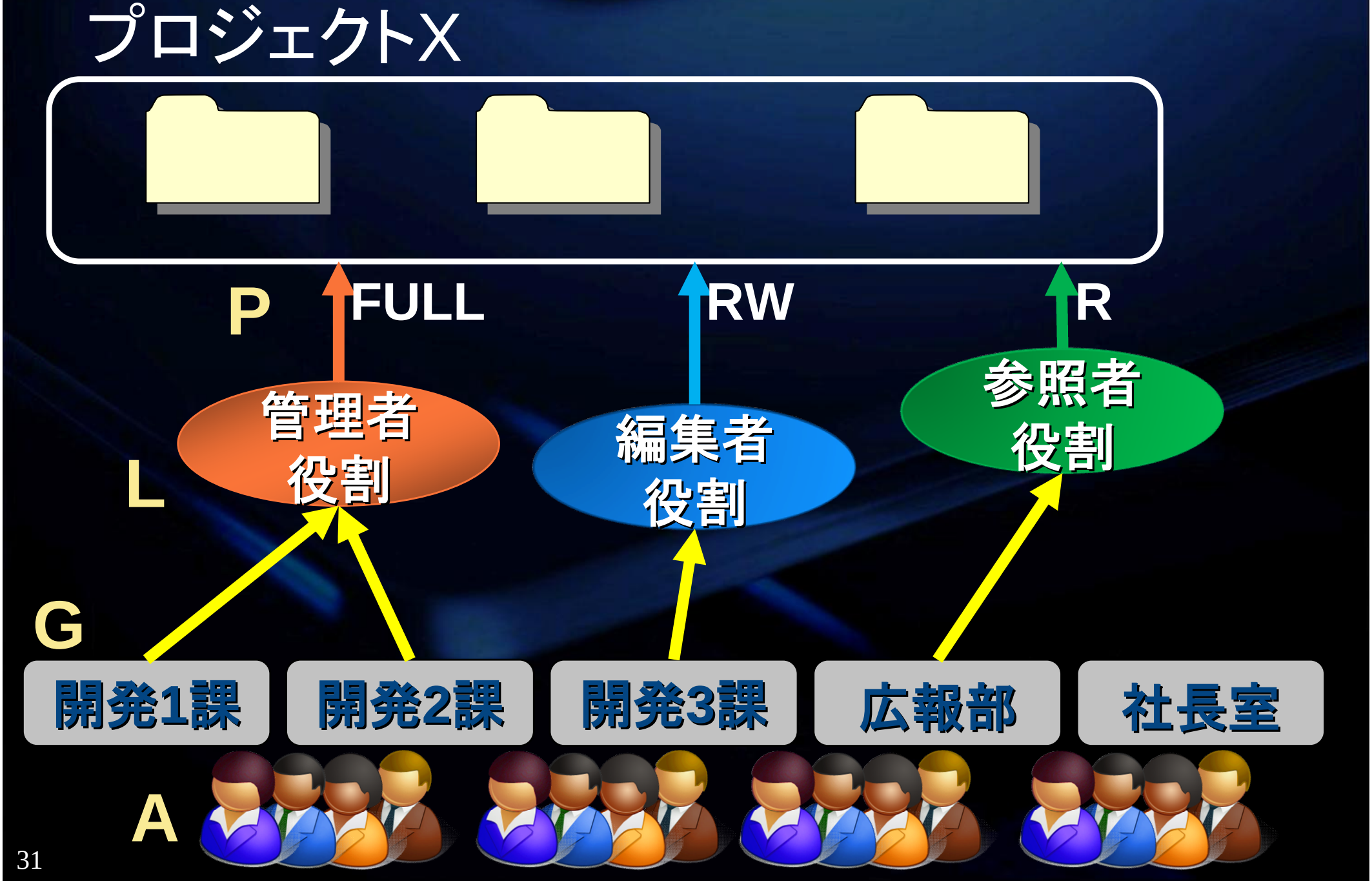
アクセス許可戦略

- ACLの継承を効果的に利用
- ACLの割り当ての原則
  - アクセス許可の変化に対応
  - 役割の変化に対応
- ACLの割り当てポリシー
  - A-G-L-Pポリシー
  - A-G-DL-Pポリシー
  - A-G-U-DL-Pポリシー

A-G-L-Pポリシー

- ポリシー
  - A:アカウントを
  - G:グローバルグループにまとめ
  - L:ローカルグループのメンバとして
  - P:許可(Permission)を与える
- 利点
  - アクセス許可の変化と役割の変化に追従
- 欠点
  - ローカルグループはサーバー毎(GPOでも可)
  - めんどくさい

A-G-L-Pポリシーの意味



A-G-DL-Pポリシー

- ポリシー
  - A:アカウントを
  - G:グローバルグループにまとめ
  - DL:ドメインローカルグループのメンバとして
  - P:許可(Permission)を与える
- 利点
  - アクセス許可の変化と役割の変化に追従
  - Active Directoryのみで構成可能
- 欠点
  - めんどくさい

A-G-U-DL-Pポリシー

- ポリシー
  - A:アカウントを
  - G:グローバルグループにまとめ
  - U:ユニバーサルグループのメンバにしてから
  - DL:ドメインローカルグループのメンバとして
  - P:許可(Permission)を与える
- 利点
  - クロスドメインメンバシップに対応
- 欠点
  - もっとめんどくさい

アクセス許可戦略のまとめ

- ユーザーの集合: グローバルグループ
- 許可の種類: ドメインローカルグループ

- ユニバーサルグループのメンバは
  増えすぎないように

- 継承を効果的に利用
  - ファイルよりもフォルダ
  - 下位よりも上位

まとめ

まとめ

- Active Directoryと企業システム
- パスワード
- グループポリシー
- セキュリティ設定の一元管理
- 修正プログラムの一元管理
- ファイルアクセス許可の一元管理

参考資料

- グローバルナレッジネットワーク株式会社
  http://www.globalknowledge.co.jp/
- 定期開催コース
  - Windows Server 2008システム管理基礎 (前編・後編)
- GKラーニングクラブ
  http://www.globalknowledge.co.jp/gklc