



Cisco IT@Work 事例研究:
既存のネットワーク OS(NOS)ディレクトリ
と新しい企業ディレクトリをマイクロソフト ア
クティブ ディレクトリへ移行する

Cisco Information Technology

May 25, 2005

- 課題

NOS ディレクトリ全てと企業ディレクトリを集約する単一のディレクトリソリューションを導入する

- ソリューション

移行とプロビジョニング プロセスをできる限り自動化した、マイクロソフト アクティブ ディレクトリへの移行

- 成果

投資を16ヶ月で回収: 48ヶ月間の削減見込み総額は 580 万ドル～810 万ドル

- 次のステップ

MeetingMaker と POP メール サーバ ディレクトリの移行

課題: 複数のディレクトリを統合する

Cisco.com

- アプリケーションごとに、異なる NOS と Lightweight Directory Access Protocol (LDAP) ディレクトリを運用してきたシスコ IT

メールサーバ、MeetingMaker カレンダーサーバ、様々な Oracle アプリケーション、Windows、UNIX、Macintosh PC

ラボ環境だけで 50 を超えるディレクトリ!

- ユーザは、複数のユーザアカウントとパスワードを管理しなければならなかった
- 管理者は、様々なシステムを扱えなければならず、また、従業員の入・退社があるたびに複数のディレクトリを更新しなければならなかった
- シスコの開発者は、アプリケーションがアクセスするディレクトリごとに異なるコードを記述しなければならなかった

課題: ディレクトリのコストとメンテナンス要求を軽減する

Cisco.com

IT でも、複数のディレクトリの維持に関連して、様々な問題に直面していた:

- 高い経費

各ディレクトリをサポートするためのトレーニング費用

ライセンス使用料

- 煩雑な SOX 法への準拠

ディレクトリ環境の数が増えるにつれ、各個人が法を適切に遵守することが難しくなる

- 説明責任

問題が起こった場合、どのディレクトリ グループに問題があったのかを特定できない

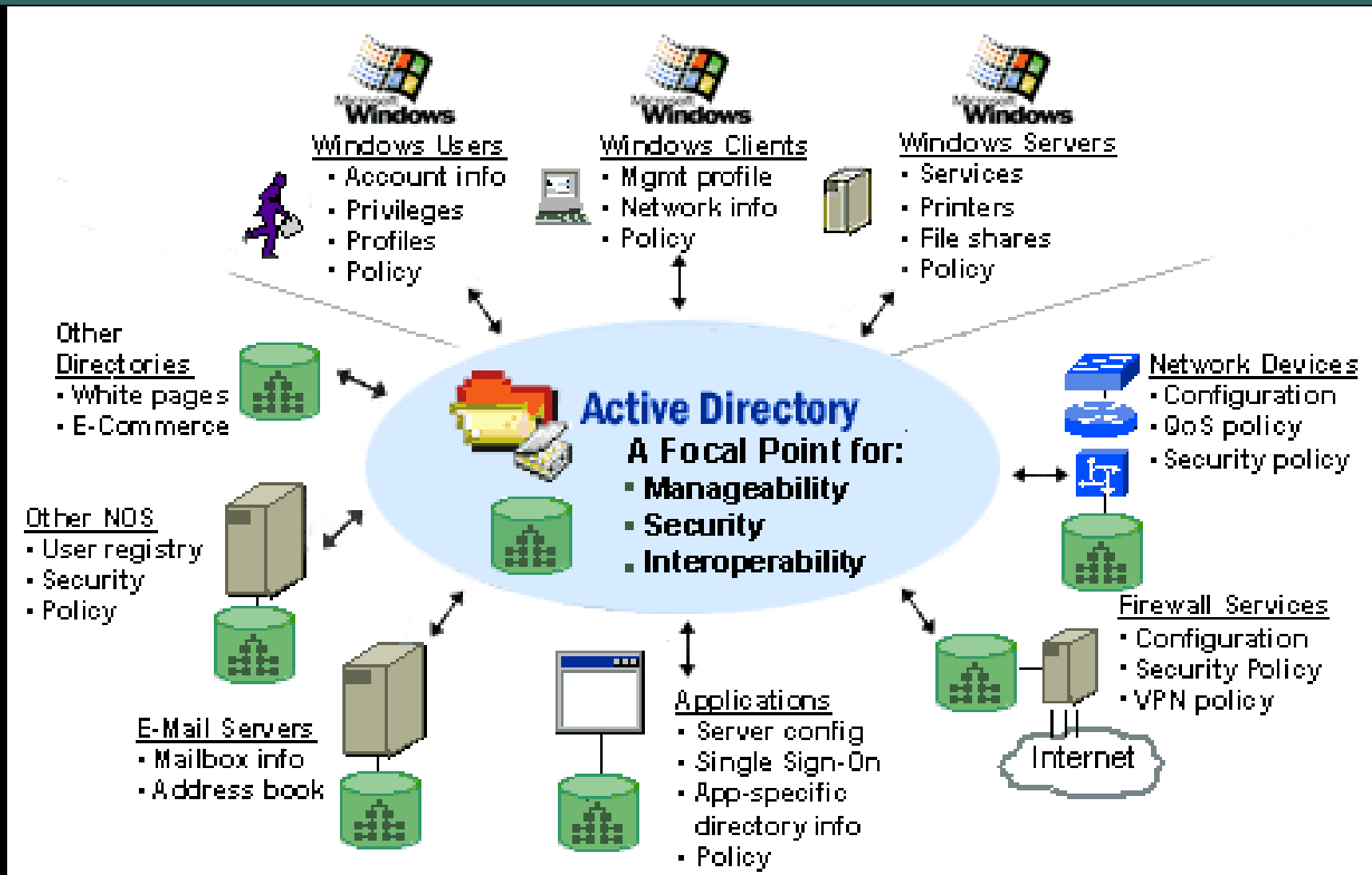
ソリューション: マイクロソフト アクティブ ディレクトリ

Cisco.com

- 単体で、シスコ IT が必要とする機能を全て提供するアクティブ ディレクトリ
 - 企業ディレクトリ
 - NOS ディレクトリ
 - LDAPv3
 - 公開鍵基盤(PKI)と Kerberos セキュリティ サービス
 - ネットワーク デバイス管理機能
- Windows OS 内に構築されるため、別途のライセンス使用料は不要

ソリューション: アクティブディレクトリへの統合

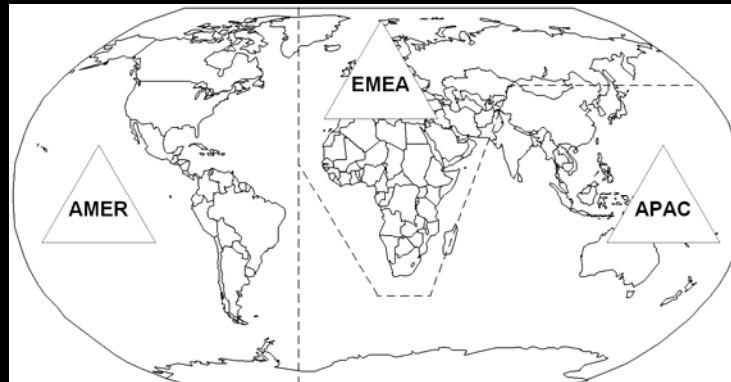
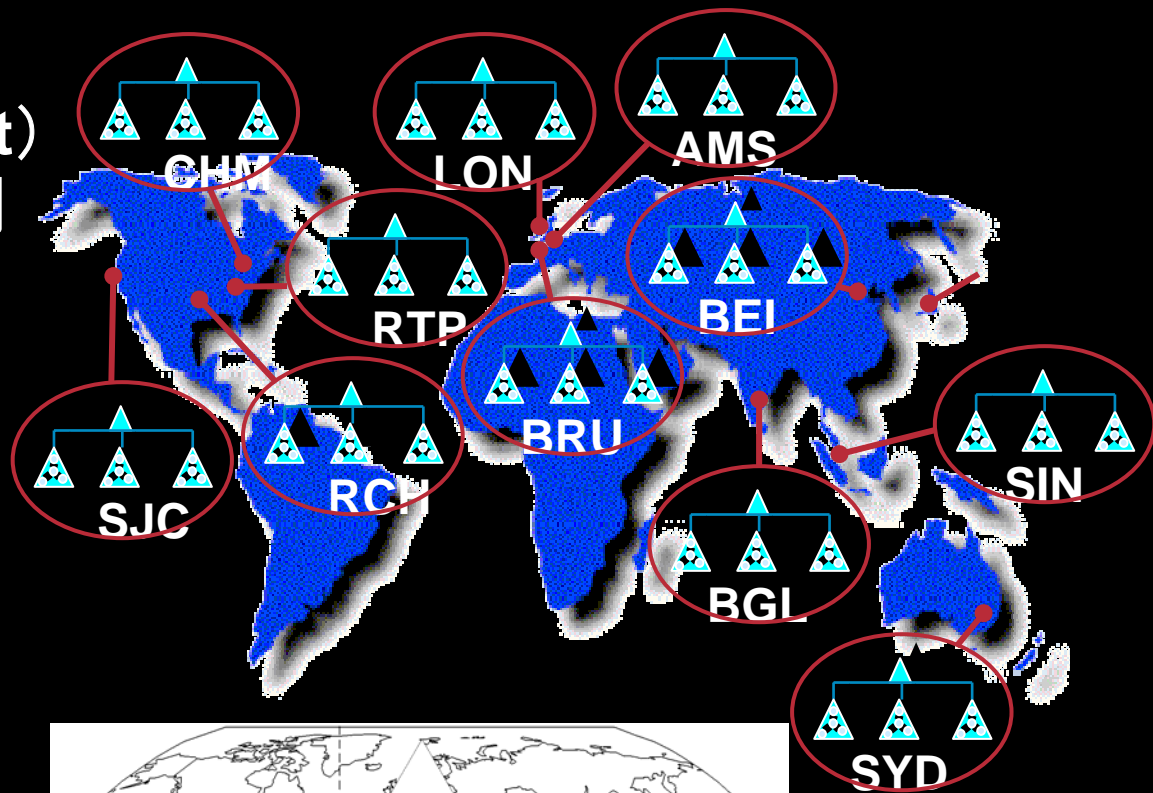
Cisco.com



ソリューション: アーキテクチャ

Cisco.com

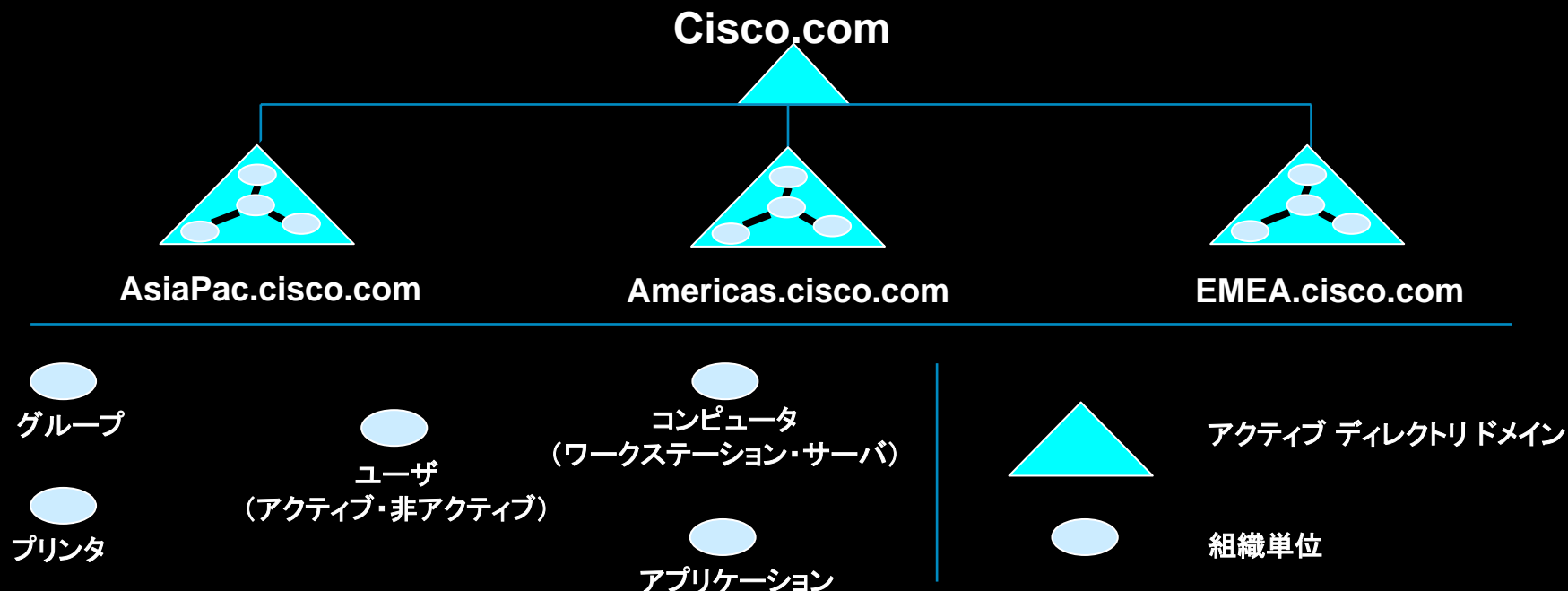
- Cisco all-packet network (CAPnet) 上の12ヶ所に展開
- 広い帯域幅により全世界のシスコユーザへ、迅速な認証応答を実現



ソリューション: 地理的区分に基づいたドメイン

Cisco.com

- 各展開拠点にそれぞれ5つのドメイン コントローラーを配置:
 - ルートドメイン
 - 地理的区分に基づいた3つの子ドメイン
 - 所属する区分の子ドメイン用の冗長ドメイン
- シスコの従業員が他の地域へ移動した場合も移動先で認証が可能
- 場所によっては、認証時間が分単位から秒単位へ大幅に短縮



ソリューション: 自動移行

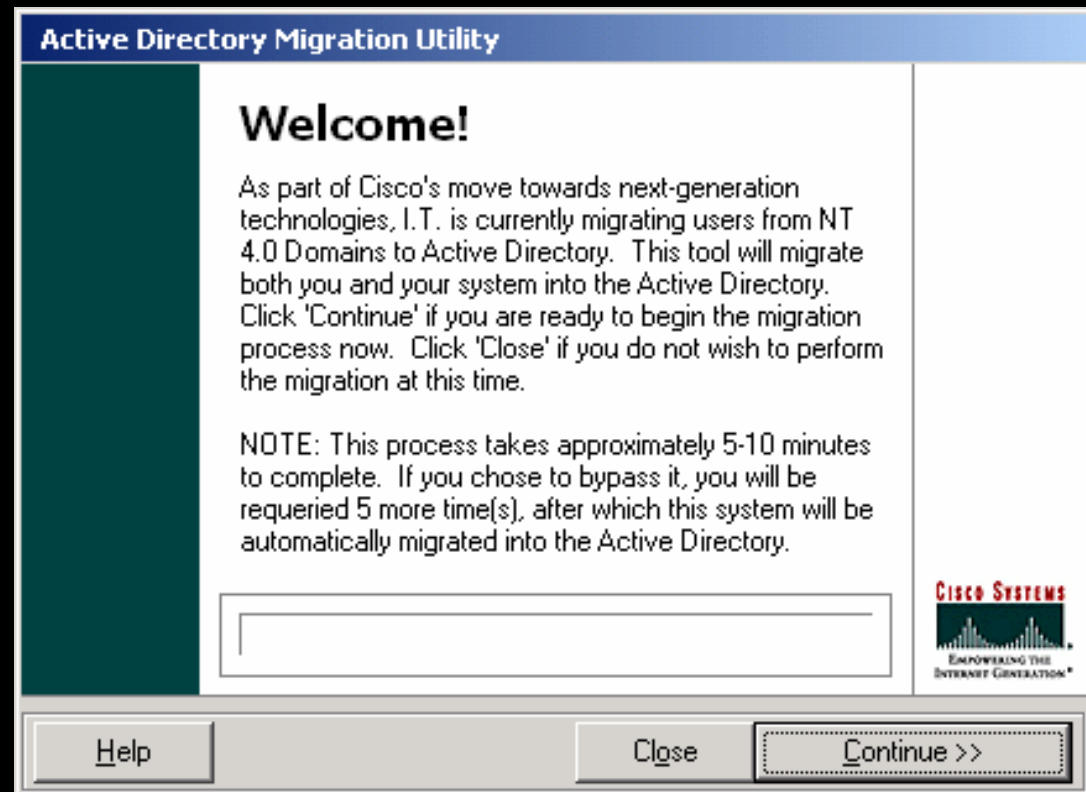
Cisco.com

- 移行を自動的に行うことでビジネスリスクを軽減
- シスコ IT では、以前の Windows NT 4 NOS ディレクトリからの移行を自動化するユーティリティを開発
 - ユーザアカウント情報をアクティブ ディレクトリ内に格納
 - グループアカウントを Windows NT4 からアクティブ ディレクトリへ移行
 - セキュリティ ID (SID) の移行

ソリューション: 自動移行

Cisco.com

- ユーザが Windows NT4 にログインするとスクリプトが起動
 - アクティブ ディレクトリ ユーザアカウントの有効化
 - パスワードの設定
 - など
- シスコ ユーザの 99% はスタッフの介入なしでアクティブ ディレクトリへの移行を完了



ソリューション: 自動プロビジョニング

Cisco.com

- モットーは、「なるべくたくさんのデータをプロビジョニングし、アクティブディレクトリ内にマスター化するデータは最小限にとどめる」
- 15 分から 24 時間間隔で毎日実行される、100 種の自動プロビジョニング スクリプト

従業員 (PeopleSoft HR システムから供給)

グループ

SID ヒストリ

メールボックス

メールエイリアス

プリンター

サイトポロジ

スキーマ拡張

組織単位

ソリューション: ネットワークトポロジー情報の自動更新

Cisco.com

- ネットワークトポロジー情報を提供するディレクトリ サービス

IT スタッフは、トポロジーを参照して、ネットワークリソースへの最短接続経路を見つけ出す

不適切に設定されたサイトトポロジーは、ディレクトリが実行するアプリケーションの可用性に影響する

- アクティブディレクトリでは、トポロジー情報を更新するのに手作業が必要

ネットワーク情報が日々変更されるシスコでは、手作業による更新は非実用的

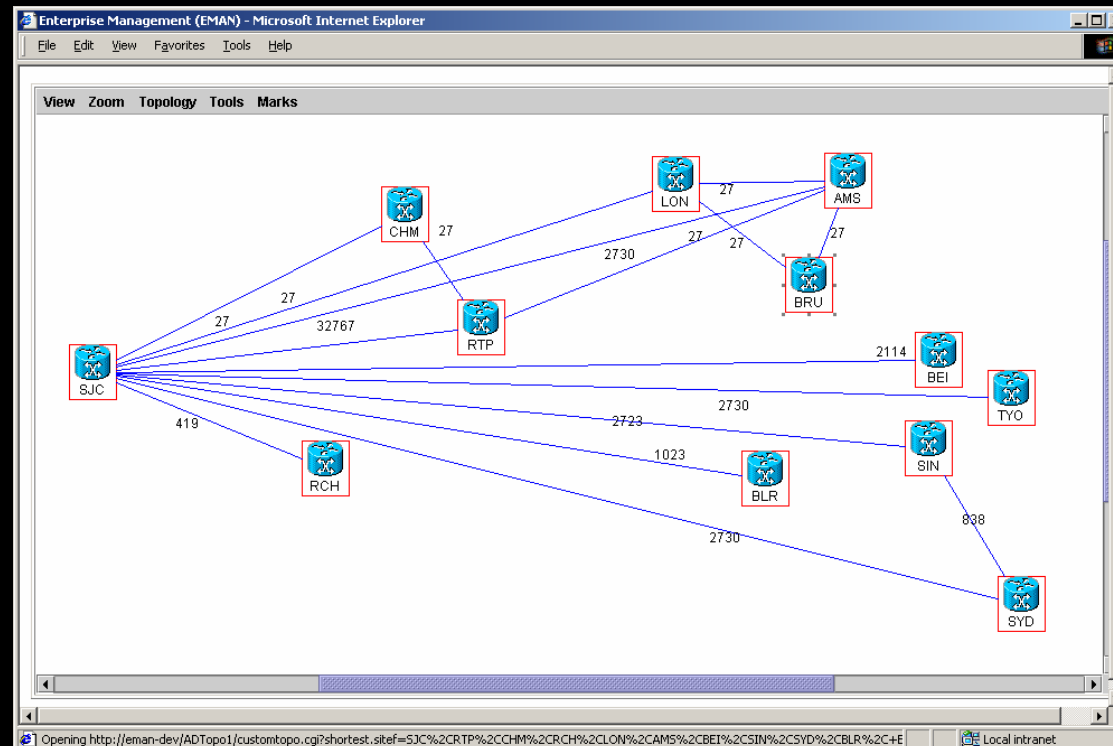
- 自動化に向けたチャレンジがはじまる...

ソリューション: ネットワークトポロジ情報の自動更新

Cisco.com

- シスコ IT では、トポロジ情報を毎日、自動的に更新するスクリプトを開発

スクリプトは、シスコのルータから config ファイルを取り出し、その情報をアクティブディレクトリに書き込む



ソリューション: 複製

Cisco.com

- アクティブ ディレクトリのマルチマスター複製機能により、シスコが管理する 12ヶ所のアクティブ ディレクトリのどこで変更が行われても、他のディレクトリに反映される
- 広い帯域幅を持つ CAPnet サイトにより、複製中も帯域幅の輻輳は回避
- 災害時でも復旧を迅速に行えるように、シスコ IT では、マスターデータをアクティブ ディレクトリではなく、別々のデータベースに保存

リスクを軽減

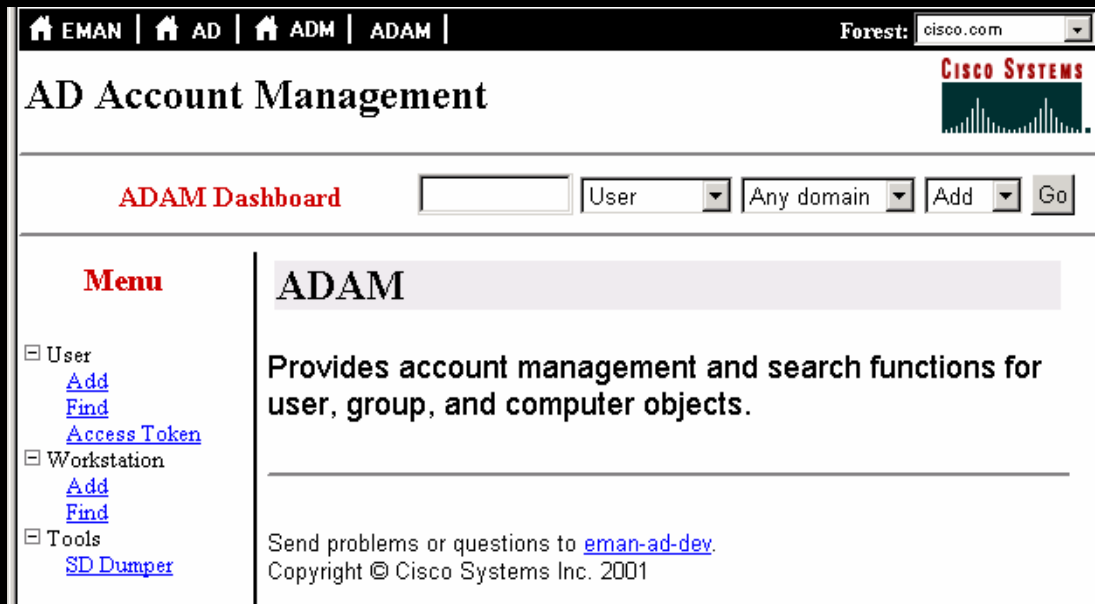
監査を改善

各システム管理者に与える変更権限と、変更頻度を定める際の IT のコントロールを促進

ソリューション: ウェブベース プロキシによる管理

Cisco.com

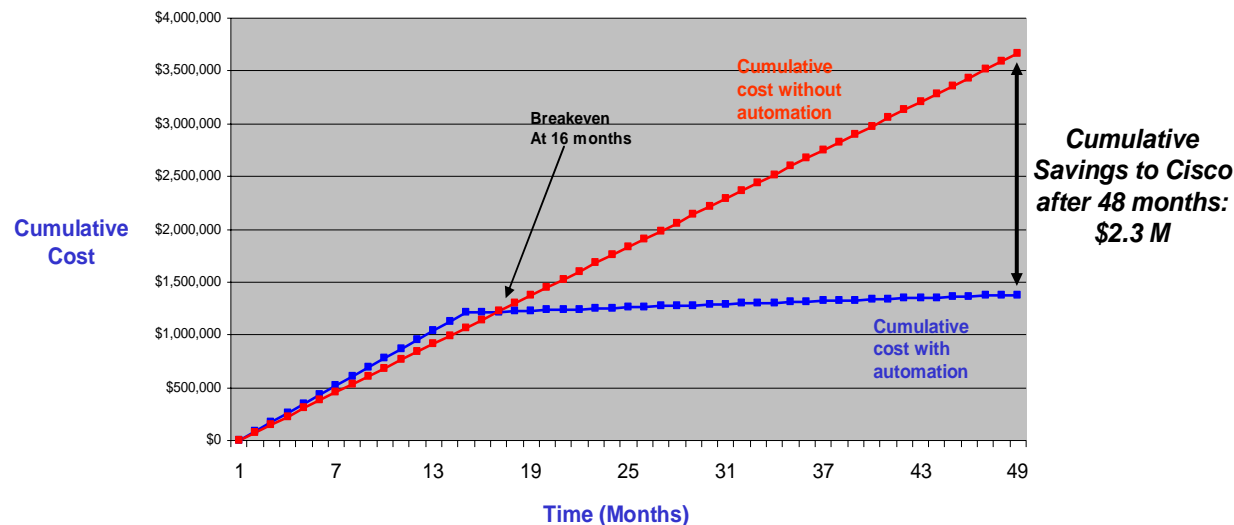
- 1ヶ所のドメインコントローラで行われたローカルな変更により、各サーバの設定が整合性を失い、保守管理が煩雑になる
- シスコ IT では、ウェブベースのプロキシサービスを開発
- ローカルでサーバ設定の変更が行われても、アクティブ ディレクトリ上のデータは保持されるようになった



成果：投資を16ヶ月で回収！

Cisco.com

- 自動移行ユーティリティにより、Windows デスクトップ1台あたり 630 ドルのコストで移行を実現
業界平均は 2100 ～ 3000 ドル（Gartner 調べ）
- 一括移行によるコスト削減額: 150 万ドル
- Windows サービスの 48ヶ月間の運用コスト削減額: 230 万ドル
- UNIX サービスの 48ヶ月間の運用コスト削減額: SunOne に比べ 200 万ドル、Sun Network Information Service (NIS+) に比べ 430 万ドル以上削減



次のステップ: その他のディレクトリの移行

Cisco.com

- MeetingMaker 用ディレクトリ
- POP メールサーバ用ディレクトリ

その他、各ビジネスソリューションに対する Cisco IT の事例研究は、
Cisco IT @ Work をご覧ください
<http://www.cisco.com/jp> (シスコシステムズ→ Cisco IT @ Work)



この文書に記載されている事例は、シスコが自社製品の展開によって得たものであり、
この結果には様々な要因が関連していると考えられるため、
同様の結果を別の事例で得られることを保証するものではありません。

この文書は、明示、黙示に関わらず、商品性の保証や特定用途への適合性を含み、
いかなる保証をも与えるものではありません。

司法権によっては、明示、黙示に関わらず上記免責を認めない場合があります。
その場合、この免責事項は適用されないことがあります。