最新 Windows ActiveDirectory/Exchange 環境への安全なシステム移行事例

富士ソフト株式会社

■ 執筆者Ｐｒｏｆｉｌｅ

藪田　義和

2003年 富士ソフト ABC 株式会社　入社

2006年 現在 IT 事業本部 産業システム事業部
大阪事業所　所属
基盤システム構築業務担当

■ 論文要旨 ■

実際に企業情報基盤環境（Windows Active Directory/Exchange）を旧バージョンから最新バージョンへ更新を実施した事例をとりあげる.

Active Directory／Exchange システムは,認証・メール環境を提供する,いわば企業にとって土台となる環境であり,システム停止時の影響は計り知れない.

本書にて,Active Directory／Exchange システム概要を述べ,導入によるセキュリティの向上や旧システムからのバージョンアップによる操作面・機能面の向上などの効果を含めた導入目的を示す.

導入過程で最も重視すべき「既存環境への影響」を念頭に,導入ステップや注意点を取り上げた.また,Exchange で管理するメールデータの移行について,実測値をまとめ,移行結果の考察より作業時にかかる時間を削減するための手段を提唱する.

■ 論文目次 ■

■ 図表一覧 ■

１.はじめに

１.１　当社の概要

当社は 1970 年創立の独立系ソフトウェア会社である.現在全国に 5,000 人以上の従業員を抱え,情報ソフトウェア企業の中でも比較的大規模になっている.創立以来「品質」「納期」「機密保持」を開発ポリシーとし,現在では「国内最大の独立系 SE 集団」として IT に関わるすべての技術サービスを提供している.制御系の開発分野から IT 総合システムインテグレーションまで幅広い情報部門に活躍の場を広げている.

１.２　Active Directory／Exchange システム概要

(1)　Active Directory とは

Microsoft 社が提供しているディレクトリサービスを提供するシステムの総称である.Windows 2000 Server・Windows Sevrer 2003 で提供され,ネットワーク上のユーザー情報やコンピュータ情報など,さまざまな資源を一元的に管理できる.

Active Directory は,インターネット標準技術を採用しており,インターネットとの相互運用性を強化している.具体的には,名前解決サービスとして DNS（Domain Name System）,情報検索用プロトコルとして LDAP,認証プロトコルとして Kerberos 技術を採用している.

Active Directory は「ドメイン」という単位で管理する範囲を定義している.組織で一つのドメインを作成すれば,組織内のユーザー,コンピュータ,グループ,サービスなどを集中して管理することができるようになる.

主な特徴を以下にまとめる.

① Windows におけるユーザー認証サービスを提供する
② 認証サービスを提供するサーバが最低１台必要（ドメインコントローラ）
③ ドメインコントローラでドメイン資源の一元管理が可能
④ DNS サービスが必須

(2)　Exchange とは

Active Directory と同様に Microsoft 社が提供しているメッセージングサーバソフトウェアを指す.Exchange のロードマップは Ver5.0 から Ver5.5,Ver2000 へとバージョンアップが繰り返され,現在 Ver2003 が最新となっている.提供される機能のうちメッセージング機能については,バージョンごとに若干機能のアップグレードはあるもののすべてのバージョンで同様に利用できる.しかし,Exchange 2000 から大きく構成に関する仕組みが変わった.それが Active Directory とのディレクトリ情報連携である.

Exchange 2000 以前のバージョンは,独自でディレクトリデータベースを保持しており Exchange 単独でユーザー情報やメール属性といった情報を管理していたが, Exchange 2000 から Active Directory が提供するディレクトリデータベースを利用している.これにより Exchange にてシステム構成の管理,メールの実データの管理を行い,Active Directory にてその他メールアドレスを含むユーザーアカウントの属性情報を管理するようになり,依存関係がより親密なものになっている.（参照 **図１**）

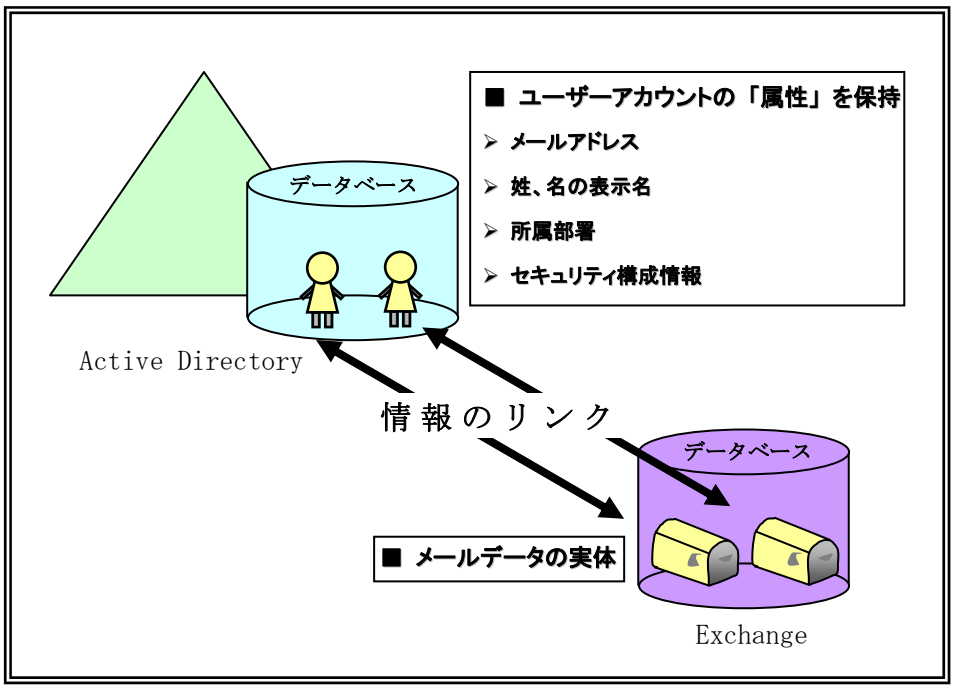

図 1 Active Direcotory と Exchange の連携図

以上から二つのシステムは,切り離して考えることはできない.これは,以降述べる導入・移行時にはもちろんのこと,日常の運用から障害復旧時まですべての管理要素において念頭におくべき重要な事柄である.

２.Active Directory/Exchange システム導入の目的

本章より実際の事例を基に現状の問題点から解決までの導入ステップを紹介する.

２.１　現状の問題点

現状環境として,企業が３拠点にまたがりそれぞれでドメイン運用を行っている.ドメインはユーザー情報を,Exchange はメールデータを管理するシステムであり,昨今の個人情報保護の観点から全社的に管理方針を決定し集中的にセキュア管理を徹底すべきである.セキュリティドメインは Active Directory の前バージョンである Windows NT を OS 基盤として構成する NT ドメインを採用している.更に Exchange についても最新の Ver2003 ではなく,Ver5.5 を使用している.問題点の一つとしてこれら Windows NT と Exchange 5.5 の Microsoft からのサポート切れが挙げられる.サポート切れによりセキュリティパッチの更新や障害時のサポートが受けられなくなり,個人情報を管理する企業基盤としてあまりにも危険な状態であるといえる.

また,最新のアプリケーションソフト（主にウィルス対策ソフト）などが対応しておらず,外部からのウィルスの侵入を防御できない状態となっていることも挙げられる.

２.２　導入の目的

導入目的としては,問題点として挙げたWindows NT,Exchange 5.5のサポート切れによる対応と,３拠点に点在しているドメイン環境を一つのActive Directoryドメインへ集約し,企業としての認証基盤を統一化することにある.それにより,構成・規約・運用といった社内ルールを決定することができる.

またExchange 2003へアップグレードすることにより,最新機能を最大限に活用することができる.その一例としては,外部インターネット環境からの社内メールシステムへの携帯電話やWebブラウザを使用したシームレスなアクセスが実現できることが挙げられる.

３.Active Directory／Exchangeシステムの段階的導入

本章ではNTドメイン／Exchange 5.5環境から段階的にWindows 2003 Active Directory／Exchange 2003環境へ刷新する手段を述べる.全体ステップにて第一に考慮した点は

『既存環境・利用者への影響度』である.その点に注目して,本刷新手段がどの程度有効であるか紹介する.

３.１　Active Directoryの構築

まず第一ステップとして,Active Directoryドメインサーバを構築する.

構築方法として

（１） NTドメインサーバをWindows 2003 Active Directoryにアップグレードする方法

（２） NTドメインとは別にWindows 2003 Active Directoryを新規構築する方法

が考えられる.

（１）の方法は,NTドメインのPDCをWindows 2003へとアップグレードして,現在の環境をそのまま引き継いだWindows 2003 Active Directoryの構築を行う方法である.この場合の特徴としては,ユーザー移行の必要が無く共有フォルダのアクセス権の再設定なども必要が無くなる反面,すべてのリソースが一度にアップグレードされる為に,障害発生時の切り分けが困難となる.また,NTドメインのドメインNetBIOS名を引き継ぐので,今回のような三つのドメインを一つのドメインに統合したい場合,拠点ドメイン名（例：OSAKA）が統合ドメイン名となってしまい,非常に都合が悪い.（この問題を解決するにはNTドメインをアップグレードする前にドメイン名変更の作業が必要になる.）

（２）の方法では,Windows 2003 Active Directoryを新規構築して,既存NTドメインからユーザーや共有フォルダなどの各種リソースを移行する.移行の手間はかかるが,新旧両ドメインの併用が可能となる為,クライアントOSの所属ドメイン変更に時間をかける事が可能となる.また,アプリケーションサーバに関してもドメインのアップグレードと違い,ドメイン／Exchangeのすべての移行が完了してから移行を開始することが可能となるのでスケジュールに余裕を持たせた移行を行うことが可能になる.

今回の事例では,（２）を採用する結果となり,以下の手順をとることにした.

- 既存NTドメインとは別にWindows 2003 Active Directoryを新規構築する.
- NTドメインとWindows 2003 Active Directoryを並行運用するために,新規構築したWindows 2003 Active DirectoryとNTドメインの間には,双方向の信頼関係を結ぶこととする.

● Windows 2003 Active Directory DNS から既存 UNIX 系 DNS サーバへ名前解決の連携を行う.

結果としては同一ネットワークに NT ドメインとは別で Windows 2003 Active Directory を構築するものの,新規で構築したので NT ドメイン環境や利用者への影響は発生しなかった.Windows 2003 Active Directory では DNS サービスが必須であり,ディレクトリの検索は DNS を使用して名前解決を行う.そのためクライアントは必ず DNS 設定を Active Directory 専用に行う必要があるため,それまで設定していた DNS 設定を変更しなければいけない.変更によりこれまでサーバ名などの名前解決に影響する必要があるため,既存の DNS サーバへの名前解決を実施する必要がある.

基盤刷新作業の場合,開発作業ほど納期について優先度が低いといえる.（支払いやリースなど金銭的な事情は別であるが.）このケースで管理者やユーザーから最も求められるものは,既存システムが稼動しつづける事である.極端な話,すべての基盤を刷新するまで 1 年かかろうとも,その間ユーザーの便宜性や操作性が変わらなければ,お客様からのクレームは発生しないであろう.

短期間でアップグレードするのは我々技術者としても最も簡単なアプローチである.しかし,ドメイン規模が大きくなればなるほど,利用している機能が多くなればなるほど,比例的にリスクが大きくなる事を忘れてはいけない.

3.2 ドメインオブジェクトの移行

NT ドメインで使用されているドメインオブジェクトを Windows 2003 Active Directory に移行する必要がある.長期的にドメインオブジェクトの移行を行っていくうえで,考慮しなければいけないのが,NT ドメインに所属している共有リソースである.

移行段階では,所属を Windows 2003 Active Directory に変更したクライアントと,移行が完了していないクライアントが共存することになる.したがって,所属を Windows 2003 Active Directory に変更したクライアントからも今までどおり NT ドメイン所属の共有リソースにアクセスできなければ平常業務に支障を来たすことになる.この問題を解決するキーワードが,SID History である.

SID History とは,ユーザーアカウントを Windows 2003 Active Directory に移行する際に,移行元 NT ドメインで使用していた SecurityID（SID）属性を引き継つげる技術である.

これにより,移行後もあたかも移行元 NT ドメインのユーザーであるかのように共有リソースにアクセスを行うことが可能になるのである.

SID History を付加したユーザー移行を行えるツールの代表的なものに,Active Directory Migration Tool（以下 ADMT と称す）がある.Windows 2000 Active Direcotry から ADMT が使用できたが,最大の難点があった.ユーザーアカウントに付与されているパスワードが移行できないことである.このことは利用者にとって影響度が大きく,多くの企業が別ツールを採用することを余儀なくされた.しかし Windows 2003 Active Direcotry からパスワードも移行可能になり大幅に改善された.よって今回は Windows 2003 Active Direcotry の ADMT を採用することとなった.

即ち以下のような方法となったわけである.

● 移行ツールとして Windows 2003 Active Direcotry の ADMT を採用する.
● SID History を付加したユーザー移行を行う.

この点についても既存環境・利用者への影響を考慮した選択だといえる.共存環境での並行ドメイン運用を選択した以上,旧 NT ドメインに所属する共有リソースに対してアクセスを維持することは必須要件だと考える.

更に ADMT については,Windows 2000 Active Directory ではパスワードが移行できないといった致命的な機能の欠落があったが,Windows 2003 Active Directory の ADMT で補完された.そういった機能が付加したにも関わらず,無償であることも採用の大きな理由の一つになっている.

今回の事例では使用しなかったが,ADMT には,共有リソースのアクセス権の一括変更機能やクライアントの一括ドメイン参加機能なども提供されており,お客様環境での検証作業の実施確認と期間の確保ができたとすれば,大いに活用できる機能であると考えている.

3.3　ADC・Exchange 2003 の構築

Windows 2003 Active Directory を構築し,ユーザーアカウントを移行した後に Exchange 2003 を Active Directory に追加する段階となる.実際の Exchange 2003 の導入は比較的容易であるが,Excahnge 2003 を導入する前に必ず Active Directory Connector（以下 ADC と称す）を導入する必要があり動作を十分に把握する必要がある.

冒頭で述べたとおり,Exchange 5.5 と Exchange 2003 ではディレクトリデータの持ち方が変更され Exchange 2003 ではディレクトリデータを Active Direcoty データベースで保持される仕組みとなっている.このようなデータ保持の仕組みを ADC が橋渡し役となって並行稼動されているシステムを維持することができる.すなわち,Exchange 5.5 で保持しているメール属性に関するデータベースと Active Directory で保持しているディレクトリデータベースをミラーリングすることで整合性をとり,新旧システムを維持できているのである.

しかし,ADC においても Exchange 2000 から利用されているが Exchange 2000 バージョンの ADC を採用した場合,**図２**の構成を採用した際にデータベースの不整合が起きてしまう現象が発生することを確認していた.

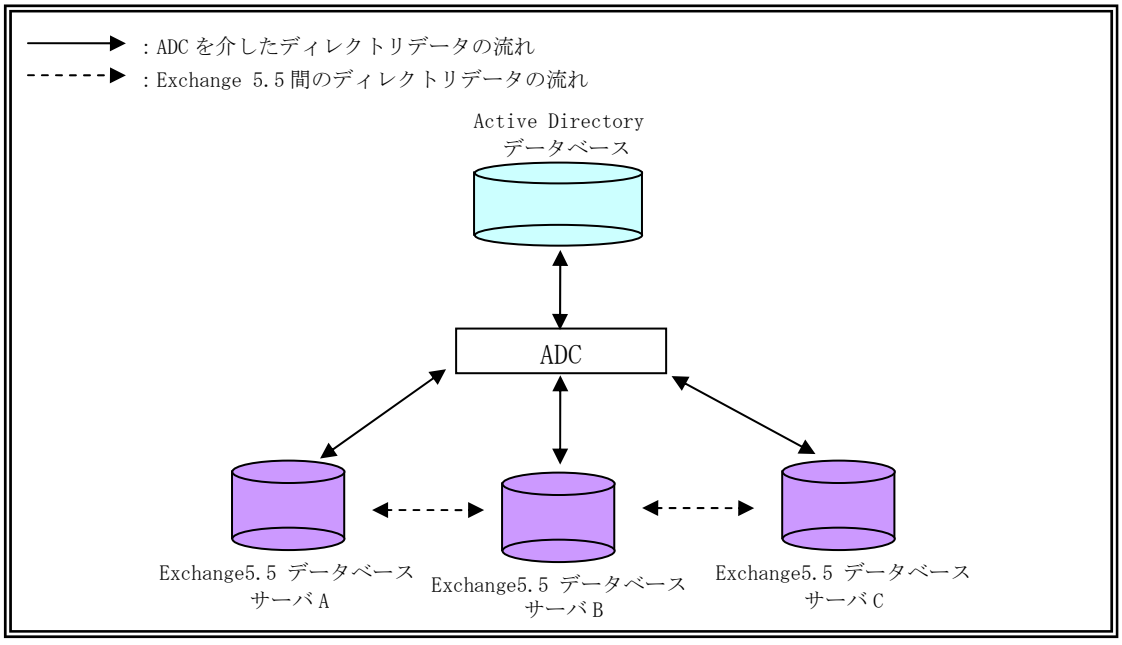

図２ ディレクトリデータの流れ

図のような構成を採用している場合に,例えばサーバ A でディレクトリデータを更新したとする.通常はサーバ A から ADC を介して Active Directory データベースにディレクトリデータが複製されるが,タイミングによりサーバ A からサーバ B へ複製が行われ,サーバ B から ADC にて Active Directory データベースへ複製される.その後サーバ A から ADC を介して Active Directory データベースへ複製される際に,同一データの重複エラーが発生し,ディレクトリデータベースに不整合が発生してしまう.

Exchange 2003 の ADC では同一環境にて検証した結果,こういった不整合は発生しないように修正されていたので,本事例では Exchange 2003 バージョンの ADC を採用した.

こういった現象が本番環境で発生してしまっては,既存システムへの影響に多大な影響を与えてしまう.事前に本番環境と同等のパイロット環境を作成し,様々なシチュエーションを想定し反復して検証を実施する必要がある.こういった事前検証期間は事前に長期的に計画し,作業時に起こり得る現象を網羅することで,本番環境でのトラブルを限りなく０％に近づけることができる.

３.４　メールボックスの移行

管理画面レベルでメールボックスを Exchange 5.5 から Exchange 2003 へ移動する.それをできるのは,Exchange 5.5 と Exchange 2003 が同一の Exchange 5.5 サイトに存在する場合に限るので,Exchange 5.5 サイトごとに Exchange 2003 をインストールする.メールボックスの移動自体は Exchange 標準機能で可能で,比較的問題も少ない.ただし,メールボックス移行時間帯がそのまま利用者の業務が停止する時間帯となることから,メールボックスの総移動時間がお客様にとって重要なポイントとなる.

したがってここでは,５０個のメールボックスを対象に現状のサイズとアイテム数と移動に要した時間について**表１**に結果を示し,それぞれの関連性について考察する.

サイズとはメールボックス自体の容量を指し,キロバイト (KB) 単位で示す.

アイテム数とは,保存メール数,その他 Outlook で使用するオブジェクト総数を指す.

移動時間はメールボックスの移動処理が開始されてから完了するまでの時間を指す.

移動手段については,Exchange 2003 標準の管理ツールから Exchang タスクを使用して,Exchange 5.5 から Exchange 2003 へネットワーク経由で行う方法をとった.

以下に移動元 Exchange 5.5 の基本スペック,移動先 Exchange 2003 の基本スペック,ネットワーク帯域について示す.

【Exchange 5.5 スペック】

・CPU： 500MHz×2　・メモリ： 512MB×1

【Exchange 2003 スペック】

・CPU： 3.0GHz×2　・メモリ： 512MB×2

【ネットワーク帯域】

・100MBase

No.	サイズ (KB)	アイテム総数	移動時間(h)
1	483	193	0:01
2	1,324	288	0:01
3	17,642	248	0:01
4	9,357	118	0:00
5	9,420	222	0:00
6	1,225	315	0:01
7	8,285	140	0:01
8	12,584	201	0:01
9	10,005	1,766	0:02
10	1,092	188	0:01
11	9,605	397	0:01
12	12,095	210	0:00
13	10,566	190	0:00
14	8,243	197	0:01
15	2,536	120	0:00
16	615	17	0:00
17	2,839	56	0:00
18	7,214	288	0:01
19	5,571	196	0:01
20	306	8	0:00
21	20,504	393	0:01
22	18,117	841	0:01
23	3,515	619	0:00
24	135	130	0:00
25	1,316	95	0:00

No.	サイズ (KB)	アイテム総数	移動時間(h)
26	7,168	390	0:01
27	5,658	217	0:01
28	10,446	61	0:00
29	28,989	568	0:01
30	18,441	38,710	0:07
31	15,482	452	0:01
32	1,047	92	0:00
33	20,216	2,008	0:02
34	9,192	14	0:01
35	20,939	502	0:01
36	2,576	69	0:00
37	5,644	333	0:00
38	164	37	0:00
39	4,770	124	0:00
40	161	106	0:00
41	175	177	0:00
42	15,758	443	0:01
43	4,455	43	0:01
44	20,704	701	0:01
45	1,955	876	0:01
46	394	24	0:00
47	927	134	0:00
48	11,954	372	0:01
49	682	47	0:00
50	22,240	217	0:01

表 1 メールボックス移行結果表

＜考察＞

メールボックスサイズ・アイテム数とその移動時間との関連性について,メールボックスの移行時間に大きく影響する要素としては,サイズよりアイテム数が関連性が大きい.

その判断要素となる結果として,No.30 のメールボックスの移動時間が 7 分となっておりその他メールボックスと比較しても飛びぬけて移動時間を要している.また No.9,33 のメールボックスも 2 分かかっており,若干ではあるが他メールボックスより移動時間が長い.それぞれで共通しているのが,アイテム数が多いことから導いた関連性の結論である.

本事例ではメールボックスを移動する際にお客様に対して,極力メールボックスサイズを減らすよう提案していたが,これではサイズの大きいメール（大容量添付ファイルなど）を数メール削除したところで作業時間の削減を実現することはできない.

そういった意味では今後同一の作業を実施する際に大変有効なデータといえる.

本事例におけるメールボックス移行の実際は,お客様の業務が 24 時間フル稼働であったため,利用者がシステムを全く利用しない時間帯はなく,利用頻度が少ない深夜 22:00 以降からメールボックスの移行作業を実施することとなった.そのため,深夜時間帯に利用するユーザーに管理者が事前にシステム停止通知を行う必要があるので,作業者から管理者への作業予定の通知は,可能な限り早めに実施しておくことが望ましい.

しかし,事前通知を行っていたとしても移行作業時間中に,利用者がメールシステムを使用する利用者がでてくることが予想される.ただ,Exchange メールボックス移行プログラムは,たとえ移行中にシステムを利用しても,接続エラーとなって利用者に通知されるだけで移行処理には特に影響がでないため,強制的にセッションを制限する手段はとっていない.

表２に３拠点のユーザー数,メールボックス数,メールデータ量を示し,データ量に対し,メールボックスの総移行時間を示す.

拠点	ユーザー数	メールボックス数	メールデータ量（MB）	移行時間（分）
A	207	203	13,607	約 180
B	171	148	2,655	約 90
C	130	114	3,069	約 90

表 2 メールボックス移行時間一覧表

実際のメールボックス移行には,前述したメールボックス移行結果データから,移行時間はメールデータ量より,メールアイテム数に依存することが判明したため,事前に余分なメール（削除済みアイテム,送信済みアイテム等）は削除して頂くよう通知すべきである.しかし,メールデータは個人情報の主たるものであり,作業者はもとより管理者でも強制的に削除できるようなものではなく,結局は利用者自身に委任される形となるため,対応が難しい問題である.

３.５　NT ドメイン・Exchange 5.5 の撤去

ユーザーの移行,メールボックスの移行が終了したら,いよいよ最終段階である.
NT ドメイン,Exchange 5.5 を撤去して完全な Windows 2003 Active Directory／Exchange 2003 環境の完成である.

Exchange 5.5 に関しては撤去という言葉から,最終的にサーバの電源を落とす作業をイメージしがちだが,実際は Exchange 5.5 の Exchange サービスを停止することで,撤去は可能である.したがって,もしほかのアプリケーションが共存していた場合に,移行する必要はなく今後も活用できる.

Exchange 5.5 を撤去する際の注意点として,ADC で Active Directory と Exchange 5.5 のディレクトリデータを相互連携しているので,必ず ADC を削除しておくことが挙げられる.削除しなければ,Exchange 5.5 を撤去した際にディレクトリデータベースも削除されてしまい,その削除情報が Active Directory に伝播し,ユーザーやグループといった情報が Active Directory から削除されてしまう.

後は NT ドメインに所属しているファイルサーバ／アプリケーションサーバを Windows 2003 Active Directory に変更し,アクセス権を Windows 2003 ドメインユーザーカウント／グループで置き換える.これらの作業は先で述べたとおり ADMT を使って一括で変更することも可能であるが,手作業で行えるレベルであれば手作業で行っても構わない.

４.むすび

本事例では移行期間を設計から導入完了までを７ヶ月で遂行した.内訳としては, 現状調査・要件定義フェーズに２ヶ月,設計・検証フェーズで２ヶ月,導入・移行フェーズで３ヶ月となった.やはり段階的な移行を採用したため,導入・移行フェーズでボリュームが増大したが,移行期間中のパスワード変更やExchangeクライアントの設定変更・ユーザー自身でのメール資産の退避や復旧といった作業は一切発生していない.また,現地での大きなトラ

ブルもなく,お客様に与える業務に差し障る影響は最小限に押さえる事ができた.
事前に作業プランを提示,納得して頂いたことを前提にすると,プロジェクトは成功であったと確信している.

安全な移行を第一目標とし移行する.これはお客様にとっては,現在の業務やシステムへの影響を考えればおのずと最重要ファクターとなる.目標達成のためにシステム導入業者の立場からすれば,既存システム環境を変更するような一点集中型移行より既存システム環境と共存する形で段階的に変更するような長期的移行計画を立てることが肝心となる.
しかし,長期的になってしまうと工数の増加も余儀なくされるが,安全な移行による既存環境へのインパクトとを天秤にかけると,やはり後者を優先すべきだとお客様と業者の間でも一致する.

今後の展望としては,Active Directoryシステムを導入したメリットを活かして,認証を使用するメールシステム以外のアプリケーションシステムの構築・提案が可能になる.昨今のセキュリティ問題対策においてもActive Directoryシステムを中心に機密情報の在り処を明確にし,情報の集中管理化・厳密認証化することを目指す.

最後に,近年Microsoft OSをはじめとするアプリケーションソフトについては改良されつつあり,利便性や操作性については数年前と比較して目を見張るものがある.しかし,結局はそれもひとつのツールに過ぎず,お客様環境により最適な活用手段を我々導入業者が検証を重ね,見出す必要がある.いくら便利な機能があるからといってそれが果たしてお客様環境で安全に活用できるものであるかは,最終的には我々が判断する必要がある.