

Title	国立大学法人北陸先端科学技術大学院大学技術サービス部業務報告集：平成22年度
Author(s)	
Citation	
Issue Date	2011-08
Type	Presentation
Text version	publisher
URL	http://hdl.handle.net/10119/9874
Rights	
Description	

5 業務報告

本学技術サービス部では、関連する教員だけでなく、日頃技術職員と協力して業務を遂行する機会の多い若手研究員及び学生を含む学内の多くの方に技術職員の業務についての理解を深めていただくため、下記のとおり情報系技術職員及びマテリアル系技術職員による平成22年度分の業務報告会を開催しました。

技術職員業務報告会

日時：平成23年7月28日（木） 13：30～17：00

場所：知識科学研究科講義棟 中講義室

発表者（発表順）	発表内容
宇野 宗則 (ナノマテリアルテクノロジーセンター担当)	平成22年度工作室業務報告
能登屋 治 (ナノマテリアルテクノロジーセンター担当)	業務報告 2010年7月 - 2011年6月
東嶺 孝一 (ナノマテリアルテクノロジーセンター担当)	2010年7月から2011年7月までの透過電子顕微鏡に関する業務報告
宮下 夏苗 (情報社会基盤研究センター担当)	JAIST 統合ユーザ環境の運用
須藤 千恵 (情報社会基盤研究センター担当)	平成22年度業務報告およびセンター受付業務の自己解析
福島 清信 (ライフスタイルデザイン研究センター担当)	2010年度業務報告 知識創造支援システム導入作業 他

情報社会基盤研究センター

情報環境システム調達業務と作業報告

中野 裕晶

情報社会基盤研究センター

概要

情報科学センター(平成 23 年 4 月 1 日に情報社会基盤研究センターへ改組)では、学生や教職員が使用するコンピュータ、各種サーバ、ネットワーク機器といった全学サービスの為のシステム(情報環境システム)について 4 年間のレンタル契約をしており、毎年これらシステムの約 1/4 ずつの調達業務を行っている。

2010 年度は、この情報環境システム調達、導入に関する事が主な担当業務となった為、これら以外の技術的業務を行う時間があまり多く取れなかったが、合間を見つけて行った作業と調達、導入業務についての報告を行う。

MRTG による Windows Server のリソース等使用状況のグラフ化

2009 年度末、Windows ターミナルサービスとして提供しているシステムが一新され、VMware + XenApp + SoftGrid という組み合わせによるシステム構成となり、ユーザは用意された約 100 台の Windows Server 2008 の中から自動的に選択された 1 台を、Web ブラウザを起点として利用できるようになった。また、ユーザが作成したファイルやプロファイルは、高速ファイルサーバ内に保存されるようになっており、どの Windows サーバが選択された場合でも同じ環境下で利用できるようになっている。

これら約 100 台の Windows Server の利用者状況やリソースの消費状況は、VMware や XenApp の管理画面で確認することができるが、全台数の使用状況を直感的に一目で確認できない為、今回、MRTG を使ってグラフ化する作業を行った。

ログオンユーザ数や特定のアプリケーションプロセス起動数等については、Windows Server 上で SNMP エージェントが動いていれば取得できるが、CPU 負荷、メモリやハードディスクの使用状況については、SNMP エージェントのアドオンの SNMP Informant を各 Windows Server にインストールすることによってデータを取得できるようにした。また、取得したデータがしきい値を超えた場合に警告メールが送信される設定も行った。

SNMP で取得したデータを MRTG によってグラフ化したものの例を図 1 から図 4 に示す。

今回は MRTG を使用してグラフ化したが、1 枚のグラフに 2 種類のデータしか表示させられない等の制約がある為、今後はより自由度が高いと思われる Cacti や Zabbix 等に移り換えることを検討している。

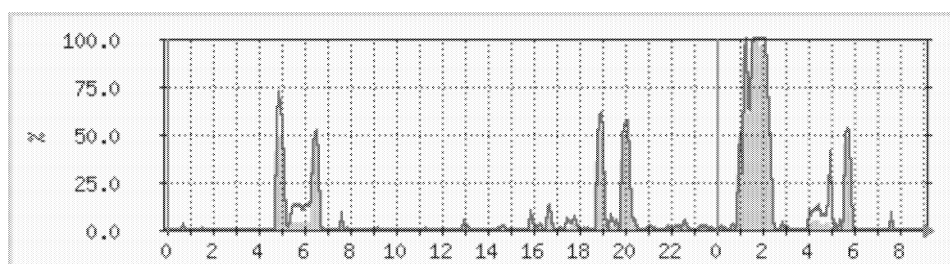


図 1 CPU 負荷状況

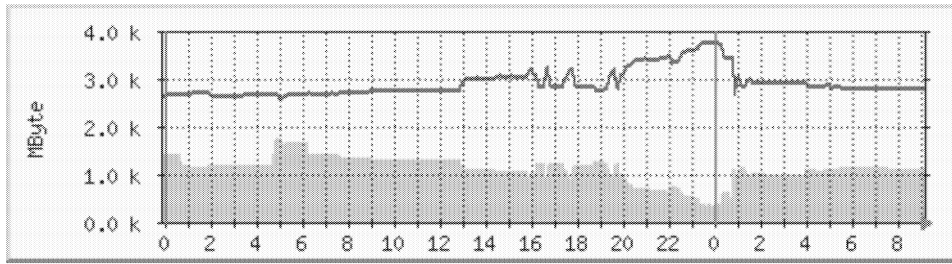


図2 メモリ使用状況

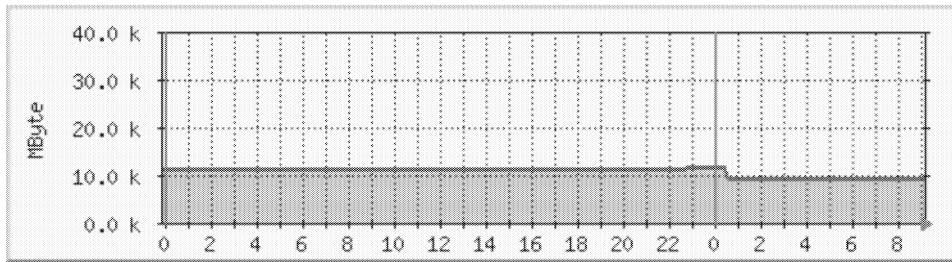


図3 ハードディスク使用状況

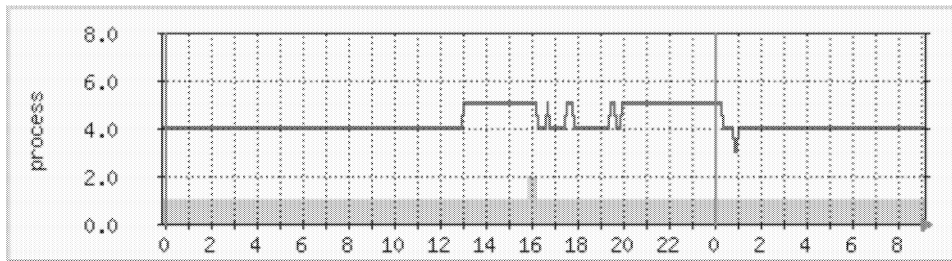


図4 ログオン数とThunderbirdのプロセス数

Mac mini のイメージ作成と展開

本センターでは、教員用や研究室用としてMacを設置しており、Boot CampによるWindows環境の用意、Office等のアプリケーションのインストール、セキュティアップデート等を行った状態で設置している。これらは設置台数が非常に多く、1台ずつ作業を行うことは非常に非効率である。その為、雛形となるディスクイメージを作成し、これを他のMacへ複製することによって全体的な作業量を減らすようにしている。

イメージの複製用ソフトウェアとして、フロントライン社のコピーキャットを使用している。コピーキャットの複製機能には、

- ・ Mac OS用ボリュームのバックアップ & 復元（複製にかかる時間はハードディスク使用量に依存）
- ・ ハードディスク全体の複製（複製にかかる時間はハードディスク容量に依存）

が用意されており、後者を使用すればBoot CampによるWindows用ボリュームを含んだディスクイメージでも複製が可能となる。但し、ディスクイメージを丸ごと複製する機能となるので、コピー元のディスク容量（ディスク使用量ではない）が大きければ大きい程、複製にかかる時間も長くなってしまふ。実際に、FireWire 400を使用して、1台のMac miniに対しての複製にかかった時間は、112GBディスクで3時間45分程度、149GBディスクで5時間弱という結果であった。なお、一度に複数台のMacに対して複製する場合は、1台当りの複製時間が短縮されるようである。

ディスクイメージ複製作業は図5の構成で行っている。コピーキャットDVDを使用して雛形またはイメージ展開先となるMacを起動ディスクとすることもできるが、この場合OSの起動にかなり時間がかかり非効率な為、別途コピーキャットをインストールしたマシンを用意している。雛形、イメージ展開先となるMacについては、ターゲットディスクモードで起動し、コピーキャットインストールMacから外付けハードディスクとして見えるように接続している。複製作業は、朝と夕方開始し、それぞれ夕方、翌朝に複製完了を迎えるようなスケジュールで行っている。

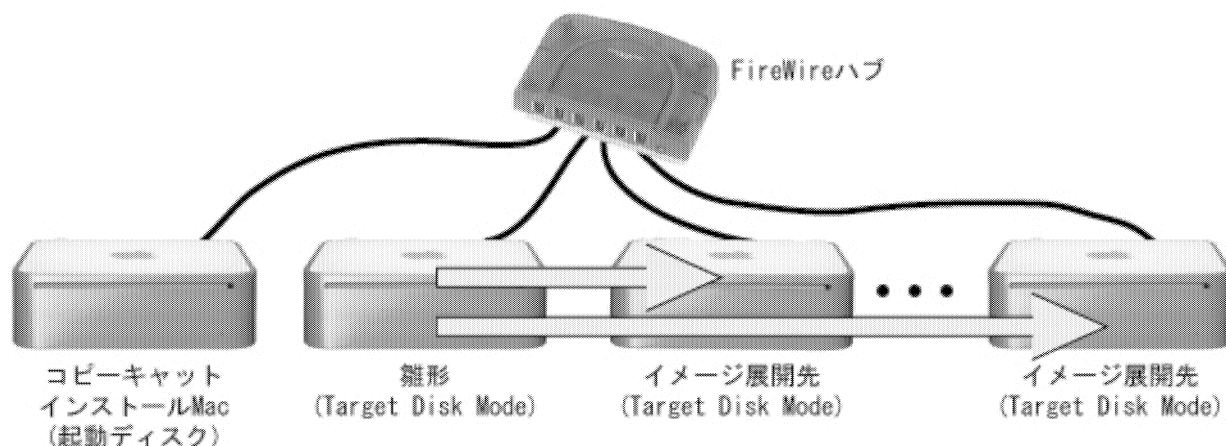


図5 Macのディスクイメージ展開時の構成

ちなみに、Windows用ボリュームを含んだイメージの大量複製を行う場合は上記方法が効率的と思われるが、1台だけの複製を行う場合は、Windows領域の複製にはWincloneというフリーのツールを使う方が、より効率的になるかと思われる。

ネットワークスイッチからの接続機器MACアドレス取得

学内に設置されているほとんどのスイッチはSNMP対応のものを使用しており、以前からこれらスイッチに接続された機器のMACアドレスを一定間隔で記録していた。2009年度末、ネットワーク機器の大幅な更新が行われ、学内設置のほとんどのスイッチがCisco社等のものからD-Link社製のものに置き換えられた。

D-Link社のスイッチでは、MACアドレス情報を取得する為のOIDが今までのものとは異なっていたり、MACアドレス情報がOIDの一部として10進数表示で格納されていたりといった違いがあった為、データ取得用スクリプトの修正が必要となった。スイッチ変更に伴うOID等の変更は表1の通りである。

表1 スイッチ変更に伴うMACアドレス取得に関する変更点

スイッチ	MACアドレス取得OID	取得データの例
Cisco社 Catalyst 3750 シリーズ	.1.3.6.1.2.1.17.4.3.1.1	Hex-STRING: <u>00 09 8A 01 AC E6</u>
D-Link社 DGS-3400 シリーズ	.1.3.6.1.2.1.17.7.1.2.2.1.2	.1.3.6.1.2.1.17.7.1.2.2.1.2.2701. <u>0.9.138.1.172.230</u> = INTEGER: 323

取得された MAC アドレス情報は、現在のところ単純にテキストベースで一定期間保存しているが、今後はデータベースを使用しての管理ができないか検討している。

情報環境システム調達、導入業務

2010 年度の情報環境システム調達に関して、2 月頃から 9 月頃までが調達期間、10 月頃から 2 月頃までが導入期間として進められた。調達期間中には、各社提案システムの確認・比較、導入説明書、仕様書(案)、総合評価基準(案)、仕様書(案)に対する各社からの意見の回答、仕様書、総合評価基準の作成等々を行い、導入期間中には、機器の搬入スケジュール調整、設置場所の調整(電源、空調、ネットワーク等)、各システムについての打合せ、倉庫の整理・管理、レンタル切れ物品の返却、管理作業等を行うことが、おおよその業務内容である。

以上のような過程を経て、2010 年度は以下のシステムの調達、導入が行われた。

- ・ 研究系常用ワークステーションシステム
- ・ 事務系常用ワークステーションシステム
- ・ 高速大容量ファイルサーバシステム
- ・ 図書館情報システム
- ・ 学務システム
- ・ 小規模計算サーバシステム
- ・ セントラルサービスシステム(ファイアウォールシステム、ネットワーク監視システム等々)
- ・ その他周辺機器

最後に

情報環境システム調達業務については慣例的に毎年担当者を交代していく(約 4 年周期)こととなっていたが、諸々の事情により、引き続き 2011 年度も情報環境システム調達業務を担当することとなった。その為、2 月には 2010 年度の導入業務と 2011 年度の調達業務を同時に行うこととなった。

2011 年度も、前年度同様に調達関連以外で技術的作業を行う時間を多く取れないような気がしているが、前年度に行った作業の中でやり残した部分等を含めて、手を付けられそうなところから手を付けていければと考えている。

ファイルサーバの運用と課題について

小坂 秀一

情報社会基盤研究センター

概要

情報社会基盤研究センター(旧情報科学センター)は 1990 年の開学より、利用者である学生教職員に対して世界最高水準の情報環境を提供し、教員の教育研究活動や学生の学習活動に資するため、等質かつ高レベルの情報サービスを展開する基盤の整備を進めている。

ファイルサーバシステムは情報環境の中でも、ユーザの全てのファイルを集中的に保存、管理する JAIST の情報環境の根幹に位置するシステムである。24 時間 364 日動作する可用性と共に最先端の環境を目指してきり限りトライアルなシステムを採用してきた。

それらのシステム中で fs1 は最もトライアルであると共に、運用上でファイルシステムが破損するという障害が重大な問題が発生するなど課題も多い。fs1 の特徴を紹介すると共に、障害の原因調査や再発防止への取り組みなどを紹介する。

1 ファイルサーバ群の概要

現在以下の 5 つのファイルサーバシステムを運用している。fs1 はこれらの中でも学生教職員(主に M1, M2 の学生)にディスク領域をサービスしている最も重要な位置づけに当たるファイルサーバである。

表 1. 運用中のファイルサーバ一覧

システム	サービス 実効容量	用途	利用プロト コル	ファイル システム
fs1	150TB	学生教職員のホームディレクトリ	NFSv4, CIFS	ZFS
fs2	100TB	学生教職員のホームディレクトリ	NFSv3, CIFS	StorFS
fs4	908TB	プロジェクト、大容量ファイル領域	NFSv3, CIFS	GPFS
fs7	266TB	ディスク領域の追加	iSCSI	NTFS, ZFS 等
fs8	12TB	事務職員のホームディレクトリ、共有フォルダ	CIFS, NFSv3	CFS

2 高速大容量ファイルサーバシステム fs1 の特徴について

高速大容量ファイルサーバシステム fs1 は学生、教職員用のホームディレクトリをサービスすることを目的に 2009 年 3 月から運用を開始したシステムである。fs1 は特に可用性が求められるファイルサーバシステムとしては、技術的にトライアルな部分が多いシステムである。

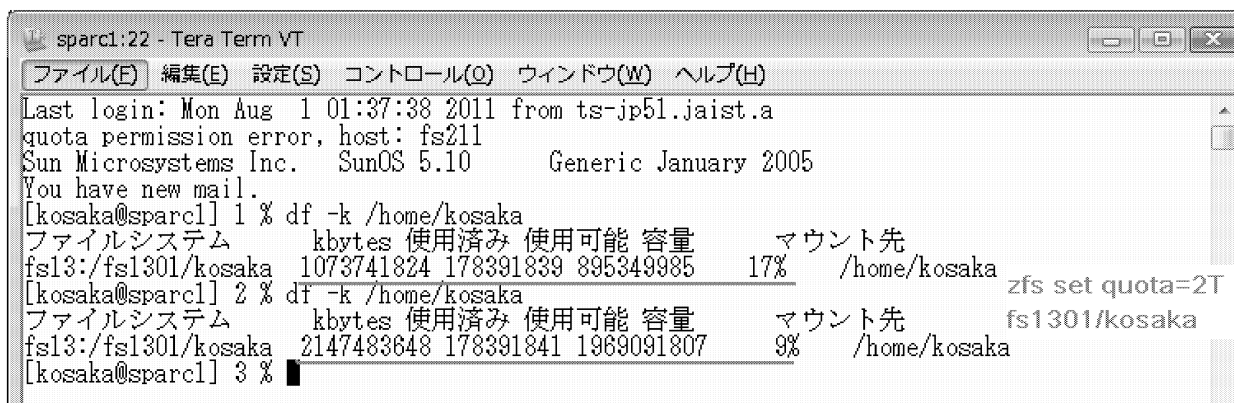


図 1. 高速大容量ファイルサーバシステム fs1

2.1 仮想化による柔軟なボリューム構築

fs1 では従来までの lun 単位で構成されるボリュームではなく、Oracle Solaris ZFS および DELL EqualLogic の仮想ボリュームの採用によりボリュームの仮想化を行っている。

ZFS ではストレージプールのサイズの範囲の中で、ボリュームのサイズ(=quota)を運用中に自由に変更できる。エンドユーザにはこの quota サイズがファイルシステムのサイズとして見えているため、運用中に quota サイズを変更すると一瞬でファイルシステム自体が増えたように見える。

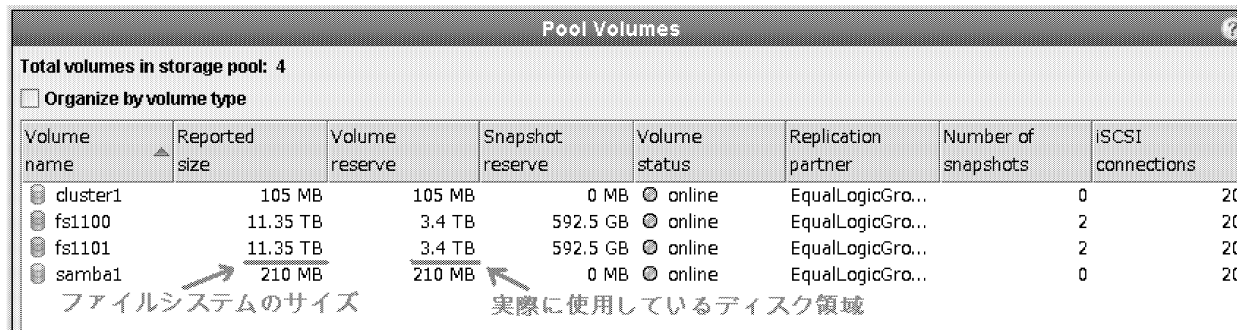


```
sparc1:22 - Tera Term VT
ファイル(E) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
Last login: Mon Aug 1 01:37:38 2011 from ts-jp51.jaist.a
quota permission error, host: fs211
Sun Microsystems Inc. SunOS 5.10 Generic January 2005
You have new mail.
[kosaka@sparc1] 1 % df -k /home/kosaka
ファイルシステム      kbytes 使用済み 使用可能 容量      マウント先
fs13:/fsl301/kosaka 1073741824 178391839 895349985 17%      /home/kosaka
[kosaka@sparc1] 2 % df -k /home/kosaka
ファイルシステム      kbytes 使用済み 使用可能 容量      マウント先      zfs set quota=2T \
fs13:/fsl301/kosaka 2147483648 178391841 1969091807 9%      /home/kosaka
[kosaka@sparc1] 3 %
```

図 2. Quota サイズを 1TB から 2TB に変更した場合の df の出力結果の変化

fs1 では事故防止の観点から quota サイズを 1TB に設定しているが、ユーザからの領域の追加のリクエストにすぐに答えられるようになっている。

また、シン・プロビジョニングという仮想ボリュームの技術によりディスクの容量の仮想化を行っている。このシン・プロビジョニングを利用すると実際に割り当てる物理容量よりも大きなディスク容量を仮想的に設定できる。



Volume name	Reported size	Volume reserve	Snapshot reserve	Volume status	Replication partner	Number of snapshots	iSCSI connections
cluster1	105 MB	105 MB	0 MB	online	EqualLogicGro...	0	20
fs1100	11.35 TB	3.4 TB	592.5 GB	online	EqualLogicGro...	2	20
fs1101	11.35 TB	3.4 TB	592.5 GB	online	EqualLogicGro...	2	20
samba1	210 MB	210 MB	0 MB	online	EqualLogicGro...	0	20

↑ ファイルシステムのサイズ (fs1100, fs1101)

↑ 実際に使用しているディスク領域 (samba1)

図 3. ファイルシステムのサイズと実際に使用しているディスク領域

fs1 ではディスク装置のファームウェアのバージョンアップに活用されている。ディスク装置を運用中にサービスから一旦外し、ファームウェアをアップグレード後に再びサービスに戻す手法を取っている。この時一時的にはあるがディスクの物理容量よりもファイルシステムのサイズが大きい状態になっている。

2.2 NFSv4, Kerberized NFS 対応

NFSv4 および Kerberized NFS に対応することにより本学が NFS をサービスを継続するうえで重要な 2 点のセキュリティ上の課題を解決できた。

- ACL(Access Control List)により CIFS/NFS 間で透過的アクセス権設定が可能になった。本学では Windows のシステムからも Unix のシステムからも同じボリューム・ファイルを参照させているため Windows システム上のアクセス権と Unix システム上でのアクセス権の整合性が課題であった。ACL が利用できるようになることでほぼ Windows でのアクセス権=Unix でのアクセス権を実現できた。
- Kerberized NFS により NFS サービスのセキュリティが協力になりました。データ通信が暗号化されると共に、Kerberos による認証で適切なアクセス権を確保できるようになりました。

2.3 ストレージエリアネットワークに iSCSI を採用

一般的に SAN(Storage Area Network)はファイバチャネルを使われて組まれることが多いが、fs1 ではファイバチャネルの代わりに iSCSI を採用した。これにより一般的なイーサネット用のスイッチングハブが利用でき、別途運用している JAIST ネットワークと同様に扱うことができるため管理運用コストの削減が期待できる。

3 ファイルサーバ fs1 の問題点と改善について

fs1 は先進的なシステムであるが、一方で問題点もいくつかあり、4 月にはファイルシステムの 1 つが破損し過去のバックアップからデータを復旧したという重大な障害が発生した。その障害の原因を調査するとともにいくつか対策や運用の改善を行った。

3.1 障害の発生

2011 年 4 月 14 日(木)19:05 頃知識科学研究科の学生のデータを収容しているグループ 3 がフェイルオーバーした。通常は移動した先でサービスが起動する設計になっているが、M2 の学生のデータを収容しているボリューム fs1300 が破損したためサービスが再開できない状態になった。また、M1 の学生のデータを収容しているボリューム fs1301 も設計上 fs1300/fs1301 の両方が online にならないとサービスしない設計になっているためこちらも参照できない状態になった。

3.2 サービスの仮復旧について

サービスの復旧は破損したボリューム fs1300 の復旧の可否や時期が不透明であったため、まずバックアップデータを利用してサービスを仮復旧することとなった。しかし新たに fs1300/fs1301 のボリュームのバックアップは 3 月 18 日から止まっていたことが新たに判明した。停止していた原因は 3 月 18 日に保守業者が行ったメンテナンスの際に一旦停止させていた設定戻し忘れが原因だったが、そのため 4 月 16 日(土)16:30 頃に 3 月 18 日時点のバックアップデータでのサービスの再開することとなった。

3.3 破損したファイルシステムからのデータの復旧

破損したファイルシステムからのデータの復旧はサポート業者への解析依頼と並行して、Solaris 10 以外で ZFS をサポートしている OS(FreeBSD や Solaris 11 等)でのインポートができないか試みた。その結果、ReadOnly だが Solaris 11 でインポートし、ファイルシステム内のユーザのファイルを読めるようになった。

3.4 最終的な復旧

最終的な復旧作業を 4 月 25 日(月)に行った。この時点でユーザのデータは以下の 2 つにわかれて保存されている。

- 元々のファイルシステム上の 4 月 14 日 19 時までのデータ (以下、データ B とする)
- 3 月 18 日時点のバックアップデータをベースに 4 月 16 日から 4 月 25 日までにユーザが作成した

データが加わったデータ(以下、データ B とする)

どのように 2 つのデータをユーザに公開するか検討した結果、ファイルシステムのデータを再度障害発生した 4 月 14 日 19 時のデータ A に戻し、データ B から仮復旧期間中に生成されたデータのみを抽出し、データ A 上にあるユーザのデスクトップフォルダにコピーすることにした。作業手順を以下の通り行った。

1. ファイルシステムを障害発生時(4 月 14 日 19 時)のデータ A に戻す
2. 仮復旧中のデータ B の中から 4 月 16 日から 4 月 25 日の間に更新があったファイルのみを抽出する
3. データ B から抽出したデータのうち Windows で利用しているデータ(~/.windows 以下)を Windows 環境のユーザのデスクトップフォルダにコピーする
4. データ B から 3 の手順でコピーした Windows で利用しているデータを間引く
5. 4 で生成したデータを Unix 環境のユーザのデスクトップフォルダにコピーする

3.5 ファイルシステムの破損の原因

ファイルシステムの破壊の原因を調査するために別システムで再現試験を行った。現在の設定ではフェイルオーバー時にフェイルオーバーした先のホストの活性時にファイルシステムのインポートや強制インポートを行った際にエラーが発生した場合には再度フェイルオーバーを試みる設定になっている。その際にフェイルオーバーした元のシステムは **panic** リポートすることでインポート処理が停止し、2 重インポートが防げていると考えていたが、再現試験ではファイルシステムの破損を確認することができた。

3.6 システムや運用の改善

今回の障害を受けてシステム的设计の再見直しを行い、下記の項目の改善を実施や検討を行っている。

- これまではフェイルオーバーした先での活性時にエラーが発生した場合には、再度フェイルオーバーを試みたが、ファイルシステムの破壊を招く可能性があるため、活性時に ZFS のインポートエラーが発生した場合にはフェイルオーバーせず停止する設定に変更した
- フェイルオーバーした際にボリュームの破壊が発生しても復旧できるよう、フェイルオーバーした際に ZFS 上で **snapshot** を実施するように変更をした
- メンテナンスの実施手順を事前に作成してもらい大学側でも作業内容の確認したり、作業後の確認作業を行うようにした
- レプリケーションによるバックアップの設定が無効になっていないか確認するチェックスクリプトを定期的に行うようにした
- レプリケーションによるバックアップの日時がすべてのグループで一斉に行われていたが、30 分ずつずらすことで SAN 部分のネットワークの流量が分散するようスケジュールを見直した
- NAS 全体の統計情報が取れるよう Dell EqualLogic SAN HeadQuoters や Zabbix などの運用やその準備を行っている

4 まとめ

今回の障害を受けて前述のような改善を行ったが、これらの多くは運用の開始前に対策されるべきだった内容である。運用開始前に JAIST と納入業者の両者がシステムの構成の確認や運用テストを行い、見直しや修正を充分行っていれば今回の様なファイルシステムの破損という重大な障害は防げたと考えている。それには納入業者の言うことを鵜呑みにするのではなく、我々運用する側である大学の職員が関連ドキュメントを深く読み、システムの構成や動作をしっかりと理解し、保守業者と協調して管理運用を行う必要がある。

ファイル共有ソフトウェアの検出法の更新

上埜 元嗣

情報社会基盤研究センター

概要

本学ではセキュリティポリシーによりファイル共有ソフトウェアの利用を禁止しており、以前より使用者を検出してきた。技術の進歩に伴い検出方法も変わってきており、本年度、機器の更新に伴い検出方法が変わり、現在は運用しながら精度や効率を高めている。本稿ではそれに伴う問題点や課題について述べる。

1 はじめに

2002年より以前から試行していたファイル共有ソフトウェアの検出を正式に始めた。また、2003年にはセキュリティポリシーも策定され、その中でもファイル共有ソフトウェアの使用禁止に関する条項はもりこまれた。ファイル共有ソフトウェアの使用を禁止するためにはファイアーウォールでの通信を遮断することで使用不可とすることも可能であったが行わなかった。当時は技術的にファイル共有ソフトウェアの通信のみを遮断することは難しく、そのほかの通信に支障をきたすことも十分あったうえ、本学は研究機関であるため研究目的での使用もあるためである。そのため、通信の検出からユーザを特定し、ユーザに注意喚起という手段をとっている。検出機器も更新しながら行っており、今年度はちょうど更新した。本稿ではいくつかの機器更新のうち FortiNet 社 FortiGate3950B の更新に伴う問題点や課題について更新作業中であるが報告する。

2 機器の更新

2002年より始めた検出では tcpdump によりネットワークのパケットをキャプチャしその中でファイル共有ソフトウェアの通信に使われる port を使用したパケットをカウントしカウントの多い IPaddress を利用者と断定していた。しかしながら解析しなければならないデータが膨大なことや解析に時間がかかるために即座に検出することができないことが問題であった。その後の機器の更新では Lancop社 Stelth Watch System を導入しネットワークのトラフィック管理によって検出を行った。このシステムでは netflow,sflow によりトラフィックデータを収集し分析までおこなえ、グラフィカルにそのデータを閲覧できた。検出のための作業効率はよくなった。今回の更新ではファイアーウォールとして FortiNet 社 FortiGate3950B 、トラフィック管理として Genie 社 Genie6333-T、パケットキャプチャとして FLUKEnetworks 社、NetworkTimeMachine Express3 を導入した。それぞれはファイル共有ソフトウェアの通信の検出が目的ではなくそれぞれに主の目的があり機能としてファイル共有ソフトウェアの通信の検出が可能である。

2.1 ForiGate3950B

FortiNet 社 FortiGate3950B はファイアーウォールの機器更新に伴い導入された。主な目的はもちろんファイアーウォールであり機能も当然ファイアーウォールとしての機能が充実している。主な特徴としては

- 高性能ハードウェア 最大 20Gbps (本学仕様) のパフォーマンス
- モジュラー型の拡張性
- 複合脅威セキュリティー

2.2 複合脅威セキュリティー

従来はファイヤーウォールとは別にアンチウイルス、アンチスパム、webフィルタリング、IPSなどのシステムを導入しファイヤーウォールと連携させることで制御してきた。FortiGateはファイヤーウォールであるが、それらの機能を持っており、それによりコスト削減、負荷軽減、耐障害性の向上などをうたっている。

これらの機能の一部として1400以上のアプリケーションの通信を認識し制御できる。もちろん、WinnyやShare、BitTorrentなど国内外のファイル共有ソフトウェアの通信を認識できる。ファイル共有ソフトウェアについては約80のソフトウェアを認識できる。



図1. FortiGate3950B Application list

3 設定およびソフトウェアの検出

今回は更新作業の初段階ということからFortiGate3950Bがどれくらい正確にファイル共有ソフトウェアを検出できるかに重点を置いて設定した。

3.1 FortiGate3950Bの設定

以下のポイントを踏まえ設定した。

- 登録されているファイル共有ソフトウェアはすべて検出する
- ファイル共有ソフトウェアの通信は遮断しない
- 通信の検出はログをとる

図2はFortiGate3950Bに対し上記の条件で設定を行っているところである。

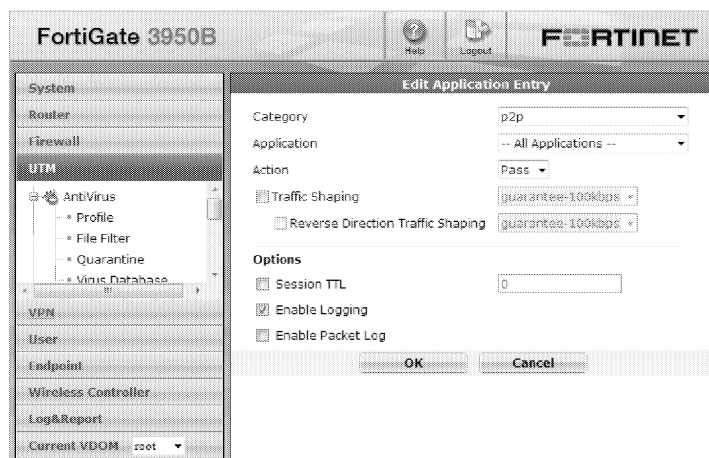


図2. FortiGate3950B Application Control の設定画面

3.2 ログ

ログはFortiGate本体に記録しておくこともできるがサイズの制限があるためログサーバに転送することにした。本学のシステム全般のログを収集しているログサーバに転送する設定をした。図3にて実際のログを示す。

ログからはファイル共有ソフトウェアを使用しているIPアドレスや相手先のIPアドレス、使用ポート、使用ソフトウェアなどが記述されている。このようなログが1日あたり400万行程度あり、それらを1行ずつ分析するわけにはいかないので、集計するプログラムを作成した。

```
2011-07-11 01:00:00 150.65.254.129 (20.6) <166>date=2011-07-11,time=00:59:59,devname=fg39a  
,device_id=FG3K9B3E10700172,log_id=1059028704,type=app-ctrl,subtype=app-ctrl-all,pri=informa  
tion,vd=root,attack_id=0,user=N/A,group=N/A,src=150.65.246.70,src_port=11763,src_i  
nt=vlan3016,dst=90.214.135.56,dst_port=56881,dst_int=vlan3001,src_name=150.65.246.70  
,dst_name=90.214.135.56,profilegroup=N/A,profiletype=N/A,profile=N/A,proto=17,serv  
ice=56881/udp,policyid=11951,serial=1945523475,app_list=p2p,app_type=p2p,app=BitTor  
rent,action=pass,count=1,msg=N/A
```

図3. FortiGate3950B のログ

3.3 集計プログラム

ログデータの中で今回必要なものを挙げる

- 学内で使用している IPaddress(sorce,distnation のどちらの場合も)
- 使用しているファイル共有ソフトウェア
- 検出したログ数
- 接続先の IPaddress 数

今回は、検出の正確さに重点を置いているので、対象がどのようなふるまいをしているかということも重要と考えて検出の確かさを判断する。また、一つ一つのソフトウェアの挙動や複数使用しているかどうかなどの判断のためにも学内で使用している IPaddress とファイル共有ソフトウェアをキーにしてそれぞれの検出数を出した。プログラム言語は perl を使用し、ログサーバ上で実行した。

```
## FortiGate P2P Summary Report ##
IP      P2P_App      Log Count      Distantion_IP_number
-----
150.65.1.130      Sina_TV      3      1
150.65.1.131      Sina_TV      6      1
150.65.1.1      Sina_TV      333      4
150.65.102.103      BitTorrent      267      2
150.65.104.108      BitTorrent      170105      37363
150.65.104.108      BitTorrent.HTTP.Track      881      13
150.65.104.108      Gnutella      7      7
150.65.104.113      Skype      6      5
150.65.104.116      Skype      5      3
150.65.104.57      PPLive      2      2
150.65.105.103      BitTorrent      11      1
150.65.105.103      Thunder      92      12
150.65.105.103      Skype      1      1
150.65.106.118      BitTorrent      20      1
150.65.106.17      Skype      17      13
150.65.108.103      Skype      30      11
150.65.108.108      BitTorrent      2      2
150.65.108.109      Skype      802      15
150.65.108.114      Skype      6      1
150.65.108.120      Skype      1      1
150.65.108.124      Skype      378      14
150.65.108.129      Skype      85      22
150.65.108.152      Skype      6      2
150.65.108.154      Skype      7      2
150.65.108.155      Skype      7      2
150.65.108.167      Skype      21      7
150.65.108.18      BitTorrent      9      1
150.65.108.18      Skype      1473      14
150.65.108.172      Skype      22      10
```

図4. 集計プログラムの出力例

4 分析

集計結果をファイル共有ソフトウェアの使用割合でグラフにしたものを図5に示す。ただし Skype を除いた検出数の多いものをグラフにした。eDonkey、BitTorrent がほとんどの割合を占めることがわかる。また、集計結果の IPaddress から本学 DNS サーバなどファイル共有ソフトウェアをしようしていないはずの IPaddress からファイル共有ソフトウェアの通信を検出していることが分かった。DNS サーバからの検出、BitTorrent、eDonkey についてさらに分析をすすめてみた。

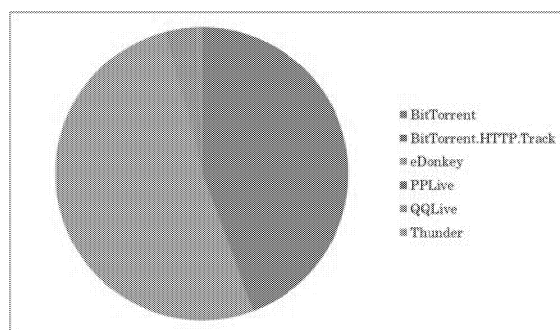


図5. ファイル共有ソフトウェアの割合

4.1 DNS サーバからの検出

本学 DNS サーバから Sina.TV というファイル共有ソフトウェアの通信を検出した。図4でもわかるが、最初の3つの IPaddress(150.65.1.130,150.65.1.131,150.65.1.1)は本学の DNS キャッシュサーバである。実際にファイル共有ソフトウェアを使用している可能性はない。そこで実際のログを確認したところあるきまった IPaddress の 53 番ポートに対してのアクセスであった。やはりそのことからこの検出については DNS のキャッシュサーバとしての通信をそのように誤検出してしまったものと考えられる。

4.2 BitTorrent

BitTorrent を検出した IPaddress では多数のログまた多数の通信先を検出していた。これはファイル共有ソフトウェア通信の特徴である。また、BitTorrent が検出された IPaddress からは BitTorrent 以外のソフトウェアも検出されている。それらのソフトウェアは BitTorrent を使用するものがほとんどである。IPaddress から使用者を特定し使用しているソフトウェアなどを確認してみると BitTorrent を使用しているとは思っていないが、そのほかの検出されたファイル共有ソフトウェアを使用していることを認めている。

4.3 eDonkey

eDonkey も検出割合では BitTorrent と同程度検出されている。しかしながら、特定の IPaddress からの検出が多いわけではなく数多くの IPaddress からの検出が多くまた、それぞれの IPaddress 検出数は少ない。これと検出数の分布が似ているものに Skype があり、IPaddress から使用者に確認を取ると Skype のみの使用ということであった。また、検出時刻なども Skype を使用していた時刻ではないが、常時 Skype を起動しているとのことであった。このことから Skype の何らかの通信を eDonkey と誤検出することが分かった。

5 考察

今回はファイル共有ソフトウェアの通信検出において FortiGate3950B の正確さを検証したわけであるが、以下のことが問題点であることが分かった。

- DNS サーバの特定サイトへの通信を誤検出してしまう。
- eDonkey としての検出はほぼ Skype の何らかの通信を誤検出してしまう。

特定の IPaddress に対する問題点は FortiGate3950B の設定で除外することは可能であり、設定したい。また、eDonkey の問題は Skype の挙動などを調査し何をどう誤認しているかを特定していきたい。統計データの方からも関連性を詳しく長期にわたりだし、Skype との関連が確かであれば Skype と同様の扱いとしたい。

使用率の少ないソフトウェアに関しても検証が必要かと思われる。

6 まとめ

まだ更新作業中であり FortiGate3950B の検出に関する精度を上げていかねばならない。そのほかの機器も同様に活用し、合わせた検出法でさらに精度も上げていきたい。また、当然利用者にはファイル共有ソフトウェアの使用禁止を啓蒙していく必要もあるわけであるが、IPaddress からの利用者の割り出しにコストがかかっている点も改善したい。今回の作業でこれらの課題がわかり、これらの課題に対して作業を進めていきたい。

アカウント作成業務の改善

岡本 忠男

情報社会基盤研究センター

概要

本学の構成員全員が使うユーザアカウントは、その重要性から、本学の構成員になって最初に配布されるものの一つとなっている。このためユーザアカウント作成作業は短時間で正確に行われることが要求される。しかしながら、従来の作業手順にはそれを阻害する要因が多く含まれていたため、アカウントを担当することになったのを機にこれを改善し、ここに報告する。

1 はじめに

1.1 アカウントの概要

本学の全構成員に対して、メール、ターミナルサービス、電子証明書、ホームディレクトリなど、情報社会基盤研究センターが提供するさまざまなサービスを利用するためのユーザアカウント(以下、アカウント)を発行している。アカウントはLDAP(Lightweight Directory Access Protocol)サーバ上に作成し、その一部の項目はAD(Active Directory)と同期されている。ユーザが利用するサービスは必要に応じてそれらを参照し、認証をはじめとする機能の提供を受ける。LDAPサーバ上には、ユーザID、パスワード、氏名、メールアドレス等の個人情報のほか、メールサーバに関する情報、ファイルサーバに関する情報、ADに関する情報など、各システムとの連携に必要な情報が登録されている。

1.2 アカウント作成作業の概要

アカウント作成作業は、構成員番号、氏名、身分等の情報が担当部署から提供され、作成依頼されるところから始まる。担当部署は学生/教職員/研究員等の構成員の種類毎に異なり、複数ある。提供された情報に基づき、以下の段階を経てアカウントが発行され、最終的に構成員の手に渡る。

(1) LDAPサーバ上への登録

アカウント作成依頼を受けたときに提供される情報に、ユーザID/パスワードを付加し、さらに各システムとの連携用の情報も加えてLDIF形式のデータを作成する。それを用いてLDAPサーバに登録する。

(2) ホームディレクトリの作成

ファイルサーバ上にユーザのホームディレクトリを作成し、初期設定ファイルを配置する。ホームディレクトリはNFS(Network File System)とCIFS(Common Internet File System)でマウントされる。

(3) アカウント通知書の作成

構成員に渡すためのアカウント通知書を作成する。これは、はがき大の紙であり、ユーザID、初期パスワード、メールアドレスが記載されている。パスワードを正当なユーザのみに伝えるために、一度はがしたら痕跡の残る目隠しシールを貼っている。

(4) 依頼元に配布物を渡す

アカウント通知書と情報環境システム利用ガイド等のパンフレットをアカウント作成依頼元に渡す。

2 従来の問題点

まず、図1に従来のアカウント作成手順を示す。

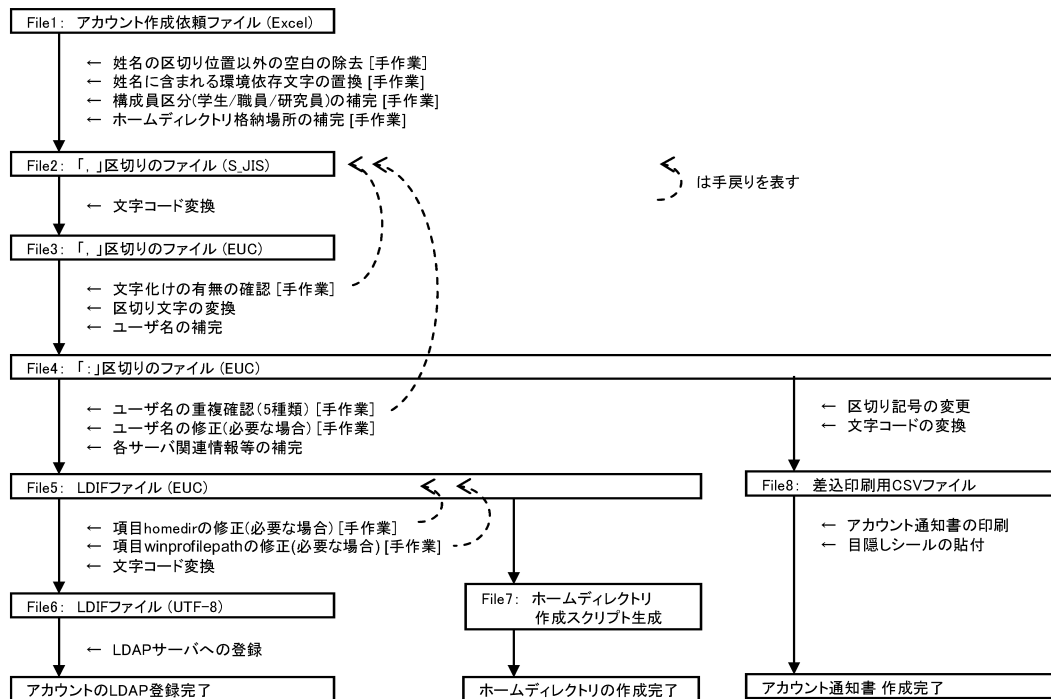


図 1. 従来のアカウント作成手順

従来の作成手順には、次のような問題点が見られた。

(1) 文字コードと区切り文字の変換の多用

手順の中で文字コードの変換作業や、区切り文字の変更作業が何度も見られるが、これは、既存のアカウント作成スクリプトが必要とする入力ファイルのデータ形式に合わせるためのものであり、冗長である。

(2) データ修正タイミングの分散

最初の入力ファイルの時点ではユーザ ID は入力不要な項目である代わりに、手順の途中で手作業でユーザ ID を書き換える必要がある。また、それとは別の項目に関しては、さらにその後に修正する手順が設けられている。このように、項目や条件によってデータ修正のタイミングがまちまちであり、効率が悪い。

(3) 姓名の区切り以外にも含まれる空白文字

学生用アカウント作成依頼データ項目の一つに氏名がある。この氏名の項目は姓と名に分かれておらず、かつ、見栄えのためであろうか、姓名の区切り位置以外にも空白文字が入ったものが送られてくる。例えば、「東京太郎」という氏名データが送られてくるが、これは「東京/太郎」なのか「東/京太郎」なのかそれだけでは判別できない。しかし、LDAP サーバには姓と名を別項目として登録する必要があり、正しく分離することが求められる。このため、氏名のよみがなを頼りに、数百人の空白交じりの氏名データから、姓と名の間の空白文字は残し、余分なものを削除する作業を手でしなくてはならなくなる。この作業にかかる時間は相当なものになる上、手作業のため間違いも発生しやすい。

(4) 氏名に含まれる環境依存文字

氏名には「高」に対する「髙」、「崎」に対する「崎」といった、使用環境によっては文字化けを引き起こす環境依存文字が含まれていることがある。環境依存文字を含んでいると LDAP サーバに氏名を正しく登録できない。目視でチェックを行い入力データの環境依存文字を置換する作業を行うが、チェック漏れが生じることもあり、その場合には作業ステップをさかのぼって再度修正を行う、いわゆる手戻りが発生する。

3 改善の方針

上で述べた問題点を改善するにあたり次の方針で設計を行った。

(1) 手戻りの排除

入力データの不備のチェックタイミングを最初の段階に集約し、訂正すべき事項はすべてこの時点で指摘し、直せるようにする。これにより、手戻りによる作業時間の無駄を排除する。

(2) 手順の整理と無駄な作業の削減

アカウント作成の手順を全体的に整理し、従来の手順で行われている、複数回にわたる文字コード変換や区切り文字変換をはじめとする無駄な手順を削減する。

(3) 目視、手作業に頼る工程の削減

大量の氏名データから目視で環境依存文字を発見する作業や、氏名に含まれる余分な空白を削除する作業といった、正確性を欠きやすい目視と手作業に頼る工程を削減する。

4 改善の実施

4.1 氏名データに含まれる空白に関する依頼元への要請

氏名に空白が過度に含まれ、姓と名の区切り位置が判別できない件について、このデータを送付してくるアカウント作成依頼元に対して聞き取り調査を行ったところ、この部署では「上流工程から受け取っているデータが、既に氏名に過度の空白文字を含んでいる」「手作業で余分な空白文字を削除してから使っている」とのことであった。そこで、余分な空白文字を削除した後のデータを送ってもらうことを提案し、担当者とは合意した。

これにより、この部署からのアカウント作成依頼は、氏名に含まれる空白文字は姓と名の間に入り、かつ、そこにしか入らないという、姓と名の分離可能な前提が成り立つこととなった。

4.2 入力データ形式の変更

従来の入力データファイルでは、最初はユーザ ID の項目がないなど、最初の段階で入力データの不備をチェックすることができないことが分かった。このため、必要な項目すべてを含むデータ形式に設計し直すことにした。また、文字コードと区切り文字は、Microsoft Excel からのデータの取り扱いを容易にするため、それぞれ Shift-JIS、タブを用いた。

4.3 入力データのチェック強化

従来は入力データのチェックはほとんど行われていないため、誤った内容がずっと後の工程で見つかり手戻りが発生した。そこで、今回はそれを防止するために入力データのチェックを強化し、それを最初の工程に配置した。主なチェック項目は次の通りである。

- ・氏名(姓と名を分離可能なように空白が含まれているか)
- ・氏名(環境依存文字の有無)
- ・氏名(日本人として、外国人として適切な内容か)
- ・ユーザ ID(他ユーザ ID やメールアドレス等との重複チェック 5 項目)
- ・ユーザ ID(構成員区分との矛盾の有無)
- ・構成員区分(リストと一致するか)
- ・ホームディレクトリ(リストと一致するか)
- ・必須項目、数値項目の妥当性
- ・その他

入力データファイルに不適切な内容があればエラーとなり、そのファイル内の全エラーを行番号と内容と

共に一括して出力し、訂正を促す。

4.4 手順の整理

LDIF ファイル作成と差込印刷データ作成までの手順を整理し、次の3つの perl スクリプトに集約した。

(1) 入力データの内容チェックと補完

入力データの不備があればその位置と内容を指摘し、初期パスワードや学生のユーザ ID などの空白項目を補完する。

(2) LDIF ファイルの作成

(1)で出力されたファイルをもとに LDIF ファイルを作成する。

(3) 差込印刷用データ作成

(1)で出力されたファイルをもとに、アカウント通知書の日本語版と英語版向けにレコードを振り分けて差込印刷用データを作成する。

図2に、改善後のアカウント作成手順を示す。図1の従来の手順と比べると、変換や修正作業、中間ファイルが削減されているのが分かる。

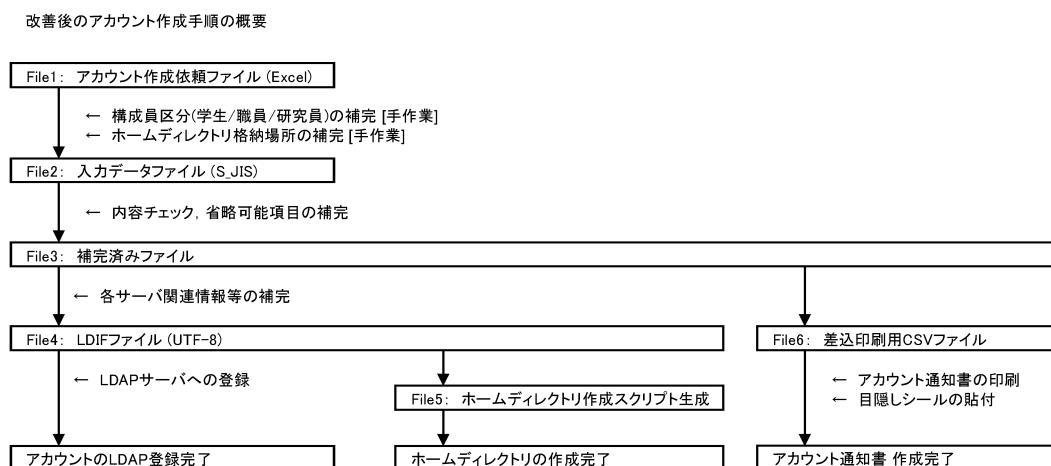


図2. 改善後のアカウント作成手順

5 効果

改善後の手順でアカウント作成を行って約3か月の間に約260のアカウントを作成したが、これまでのところ手戻りは発生していない。また、物理的作業を伴う、印刷や目隠しシール貼り以外に要する時間は、約200の新入生アカウント作成時でも20分間程度にまで短縮された。

6 今後の課題

今回は、新入生アカウントの大量作成時期が迫っていたため、従来のアカウント作成手順の中でも最も非効率的な部分に絞って改善を行った。今後はアカウント削除に関する作業も効率化を図る必要がある。

情報環境更新によるシンクライアント端末の構築と展開

間藤真人

情報社会基盤研究センター

概要

情報環境機器の更新の一部として行われるユーザ用クライアント端末の入れ替え作業について、その端末の性質から来る OS イメージ作成での課題点や展開作業の簡略化の重要性、そして導入機器の微妙な差異によって起こるトラブルとその対応の一例についてを示す。

1 はじめに

本学では、学生及び教職員が研究や事務処理等を行う為の環境として、常用ワークステーションシステムと呼ばれるものを整備しています。各員には基本的に机上作業としてクライアント端末が一台ずつ配布され、その端末より各種の計算機サービスが利用できるようになっています。

当初は Solaris ワークステーションにてサービスを行っていた常用ワークステーションシステムでした。しかし Windows 環境の利用が必須となって来たことにより、シンクライアントを介して Windows サーバを利用する現在の環境となりました。これらの計算機環境は 1/4 ずつ毎年更新を行う事で、常に最新の環境を利用できるようになっていますが、そのため毎年導入作業を行う必要があります。

この導入作業について、計算機環境の概要から必要とされる作業を示し、その際に起こった問題点等をまとめたいと思います。

2 常用ワークステーションシステムの概要

2.1 以前の Solaris ワークステーション端末環境

当初の Solaris ワークステーションを使用した常用ワークステーションシステムでは、人員に限りのあるセンターで全学の環境を管理できるようにと、実行環境とデータの分離を行った環境で構築されていました。

各個人の机上端末には、計算の実行環境のみが存在しており、各個人のデータやアプリケーション等はファイルサーバに保存され、NFS(Network File System)等を介して、参照・利用するというものでした。この方式により、机上端末の故障等のトラブルの際にも、各個人のデータはファイルサーバに保存されているので、机上端末の交換を行うだけで利用再開が可能になり、ユーザ環境への影響も最低限のものとしていました。また、机上端末である Solaris ワークステーション自体も、network boot の機能を使い、ファイルサーバよりディスクイメージを書き戻す事によってインストール作業を完了できるというように、簡素化していました。

以上のように、限られた人員で端末の保守作業を効率よく行えるよう常用ワークステーションシステムは構築されていました。

2.2 現在のシンクライアント端末環境

現在のシンクライアント端末を使用した常用ワークステーション環境でも、その設計思想は受け継がれており、端末自体にはデータを置かないデータレス環境となっています。各個人のデータはファイルサーバにて管理されており、アプリケーションや実行環境は基本的に Windows サーバにて管理されています。

シンクライアント端末本体は、ハードディスクやファンなどの可動部分を持たない設計となっており、機械的な故障が起りにくいものになっています。また端末管理ソフトウェアがあり、そのソフトウェアには集中管理

機能とネットワークを介したイメージ展開機能を持っているので、Solaris ワークステーションの頃のシステムと同様にインストール作業の簡素化を行っています。

ただし、シンクライアント端末は thin(薄い、乏しい、貧弱な) の名の通り、必要最低限な機能のみを持った簡易端末であり、通常の計算機同様に利用する事は想定されていません。逆にデータの保持等が出来ないように、起動時には想定されている初期状態に戻るような仕組み (WriteFilter) が組み込んであります。

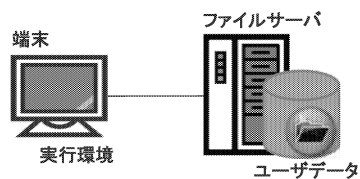


図 1: Solaris ワークステーション環境

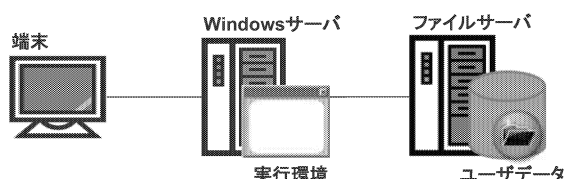


図 2: シンクライアント端末による現環境

3 クライアントイメージの作成

3.1 機能の取捨選択

本学環境のクライアントに必要とされる機能は、「デスクトップ環境をサービスしているサーバに接続出来る」だけである。ただしこの接続機能に関して、研究環境または事務処理環境として利用する上で必須となる機能・性能が幾つかあり、それらに必要なドライバやライブラリの中には、標準では用意されていないものが幾つか存在する。しかしながら、「起動時には初期状態に戻す」というシンクライアントの性質上、必要になった際にインストールを行ってもらうという方法では、毎回その作業が行われる事になるうえ、再起動が必須の作業の場合そもそも作業の完了が不可能である。そのため、必要と考えられる機能については予めセットアップを完了させておく必要があります。

一方、必要最低限の機能しか要求されていないシンクライアント端末は、それに見合っただけの性能しか有していない事が多い。必要な機能をセットアップを行っていく事によって、性能的に余裕が全く無くなっていく事や、場合によっては必要な機能を追加する余裕が無くなってしまいう事さえある。そのため、不要な機能を削除し、必要な機能のみを残し、追加するという作業が必要とされる。

また、ユーザが利用する環境として不便な機能・設定を修正しておく必要もある。出現頻度の高いポップアップウィンドウの抑制などが、これに該当すると考える。

3.2 作業内容

今年度導入のシンクライアント端末は、前年度導入の端末をほぼ同じものであったため、前年度のイメージで上書きする事でそのまま利用する事も可能であったが、幾つかの不具合や要望事項への修正を加えるため、前年度の設定内容を踏襲しつつ、イメージの作成を行った。

以下に、前年度作成以降に判明し、修正を行った項目を幾つか列挙する。

- ユーザパスワードの設定

シンクライアント端末については、ユーザが端末のパスワードを利用する場面が無い場合、自動ログオンが行えれば問題ないと考えていたが、デフォルトではパスワードの有効期限が設定されており、期限が切れるとパスワードの変更を毎回促されるようになることが分かった為、期限を無期限に修正した。また、スクリーンロック時にパスワードを要求されるため、この機能を利用出来ないように設定した。

- USB 機器の認識

USB 機器を新規に接続した際に、ドライバのセットアップが自動的に起動するが、終了時に初期状態に戻るシンクライアントでは、この動作が毎回起こる事になる。そのため、初期状態で必要最低限の機器に関しては認識済にしておくことにした。

- 各種ポップアップメッセージの抑制

通常のポップアップメッセージが毎回出て来るのを煩わしいと思う人も少なくないと思うが、接続先のサーバ上で作業中にシンクライアント側のポップアップウインドウにフォーカスを取られてしまうという現象が判明したため、ポップアップしないように修正した。

- 動画再生用エンコーダの追加

学内で公開している動画コンテンツを再生する際に、シンクライアント側のエンコーダを利用して再生を行える事が判明したため、エンコーダの追加を行った。

4 クライアントの展開

4.1 管理サーバと PXE 機能によるイメージの展開

管理サーバでは、学内のシンクライアント端末にインストールされている管理クライアントソフトと通信を行う事で、各端末の状態の確認やリモートコントロールなどの管理機能を利用することが可能となっています。この管理機能の中に、端末の PXE(Preboot eXecution Environment) 機能を利用したイメージファイルからの OS 展開があります。

この機能を利用した従来の端末イメージの展開方法は以下のようになります。

1. PXE 機能を利用できるように BIOS 設定の変更し、変更後、OS を起動。(端末上での作業)
2. しばらくすると、自動的に管理サーバに端末情報が登録される。
3. 管理サーバより、イメージの展開作業を指示。
4. 端末が自動的に再起動し、イメージ展開作業が始まる。
5. 30 分程度で書き換えが完了し、初期処理を行った後、利用可能な端末が起動する。

この作業のうち端末上で行わなければならない作業は BIOS の設定変更だけであり、以降の作業は基本的に管理サーバ上で行えばよく、なおかつ複数台に対して展開作業を同時に投入する事が出来るため、従来の OS のセットアップ作業と比較するとかなりの簡略化が行われています。毎年、数百台に行う作業となるため、展開作業の簡略化は非常に重要と考えます。

4.2 今年度端末のファイアウォール機能による問題点

今年度導入された端末では、独自のファイアウォール機能がセットアップ済でしたが、この機能によって管理サーバと管理クライアントソフトの通信が遮断されているという、問題がありました。そのため展開方法の 2 が完了せず、以降の作業を行う事が出来ないという状態になりました。

解決策としては、ファイアウォール機能の設定を変更する事や管理クライアントソフトに手動で管理サーバを指定するという方法がありましたが、いずれもマウスによる GUI 操作を伴うもので、数百台に行うには現実的で無い作業でした。

4.3 初期展開機能による解決策

現在使用している管理サーバの機能には、初期展開という機能がありました。この機能は、新規にデータベースに登録された端末に対して、自動的に指定された作業を行うというものです。また、通常管理クライアントソフトからの通信によってデータベース登録を行う以外に、PXE ブートして来た端末をデータベースに登録する機能を有していました。この二つの機能を利用して、PXE ブートして来た新規の端末に対して、イメージの展開を行うという方法を行う事にしました。

この方法はうまく行える事が出来、結果として BIOS の設定完了後に電源投入するだけでイメージの展開が完了するというように、更に作業の簡略化が行えました。

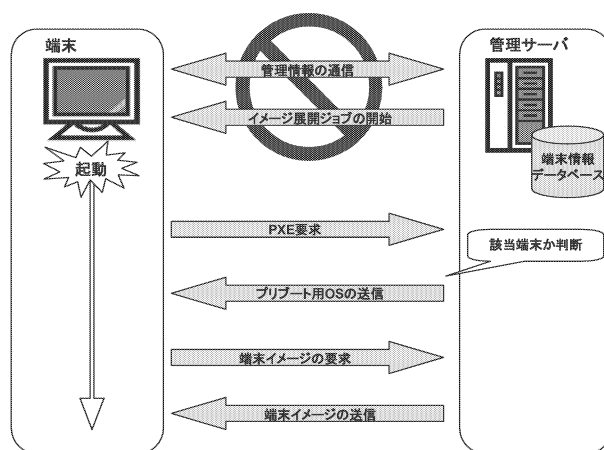


図 3: ファイアウォール機能によって管理情報の通信が遮断されているため、端末情報はデータベースに登録されず、ジョブ送信を行う事も出来ない。初期展開機能を利用してPXE 要求を受けた場合も、情報が登録されていない為、端末の判断にデータベースを利用する事が出来ない。

4.4 初期展開機能の利用

この方法は学内のほぼ全てのネットワークで利用可能なため、今後は端末の配布時に同時にイメージ展開を行うという方法が可能であると思われる。今までは予めイメージ展開を行っておき、その後端末を配布するという方法であったため、イメージ展開用の作業スペースの確保などの場所の問題もあったが、そのスペースの確保が不要になるとも考えられる。

一方 PXE ブートして来た端末全てに対して有効なため、関係の無い普通の PC 等に対しても、イメージの展開作業を行ってしまう危険性がある。初期展開時には幾つかの条件を設定して、無関係の端末に対して作業を行わないようにする必要があるが、端末識別に使えると思われる端末情報のほとんどが、通常の OS 起動後に利用できる情報のため、イメージ展開用に利用されるプリブート時の OS からどの情報が参照できるかなどを、十分に吟味して設定する必要がある。

今年度端末のようなファイアウォールによる通信障害が無いのであれば、通常管理クライアントからのデータベース登録時に初期展開を行うという方法が安全であると考えられるので、そのような方法を利用する方が良いだろう。

5 まとめ

毎年、学生及び教職員用の端末が更新される事になっている。基本的に必要な機能は変わらないが、ハードウェアの他に利用されるサーバの環境によって、必要とされるソフトウェアも微妙に更新されており、端末側のソフトウェアの更新作業が必要とされる。実際、今年度の端末についても既に幾つか修正の要望が出てきている。大規模な修正が必要ならば、管理サーバより全台に対してイメージの書き換えを行う事も可能ではあるが、修正の要望が上がるたびに行うなどというのは現実的でない。これまでのノウハウが幾らかたまってはいるが、一番最初に配布する初期イメージは十分に検証する必要があることは、間違い無い。

そのイメージの展開作業に関して、毎年数百台の規模で行う必要がある。基本的にはマニュアル通りに行う単純作業であるが、数百台規模となると結構大変で時間のかかる作業となっています。だからこそ、作業をより簡略化していく必要があり、そのために便利なツール等があるならば、積極的に利用していきたいと考えます。

情報社会基盤研究センター受付業務の自己解析

須藤 千恵

情報社会基盤研究センター

概要

情報社会基盤研究センター（以下、センター）のサービス業務全般に対する電話、電子メールおよびセンターへ来室による問い合わせの対応（受付業務）を毎日行っており、現在は主にセンターの技術職員が3日に1度の割合で担当している。時期や問い合わせの内容によっては、受付業務のみで1日が経過してしまうことや内容によっては翌日以降も引き続き対応する場合もある。センターのサービス業務が年々増えていく中で、受付業務の効率化は重要であると思われる。ここ数年の受付業務の取り扱い内容について自己解析し、改善できるポイントについて検討した。

1 受付業務

1.1 はじめに

センターのサービス業務全般に対する電話、電子メールおよびセンター来室による問い合わせの対応（受付業務）は、センターおよび利用者にとって重要なサービスである。

現在は、主に技術職員が3日に1度の割合で担当している。

1.2 受付業務の体制

現在の受付業務の体制は以下のとおりである。

1. センター受付スペース（日頃の技術職員の座席とは別のスペース）で対応する
2. センターサービスを担当している2つのグループ（1グループ3人）から職員1人ずつ計2人が受付業務を日替わりで行い、この2人でできる限りの対応をする
3. センター職員向けFAQ（センターサービス運用情報も掲載している）を参考にしながら、対応をする
4. 対応漏れの防止、進捗状況の確認、対応履歴を残すためにWebグループメールシステム「サイボウズメールワイズ」を用いた管理を行う

(ア) 対応管理：電話およびセンター来室での対応履歴、進捗状況の管理

(イ) メール管理：電子メールでの問い合わせ、申請などの対応履歴、進捗状況の管理



図1. サイボウズ メールワイズ（対応管理）

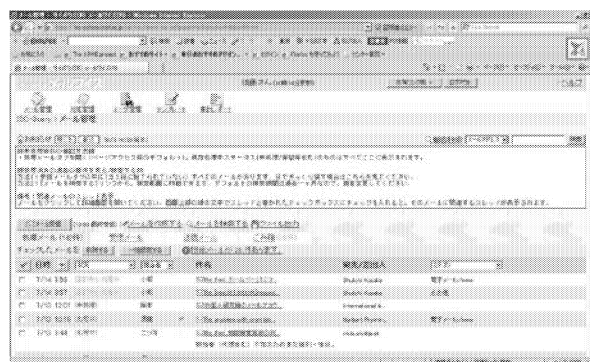


図2. サイボウズ メールワイズ（メール管理）



図3. センター職員向けFAQ

2 集計結果および考察

2.1 集計結果（全体）

「サイボウズ メールワイズ」に入力された対応内容を基に改善ポイントを検討することにした。平成20年度から平成22年度までの3年間の対応件数の集計結果は以下のとおりである。

表1. 対応管理（電話およびセンター来室）

期 間	件 数
平成20年度（2008.4-2009.3）	1,340
平成21年度（2009.4-2010.3）	1,327
平成22年度（2010.4-2011.3）	1,507

表2. メール管理

期 間	件 数
平成20年度（2008.4-2009.3）	1,580※
平成21年度（2009.4-2010.3）	1,627※
平成22年度（2010.4-2011.3）	1,420※

※同一案件も含む

どの年度においても対応管理、メール管理を含めて約3,000件程度（一日あたり平均十数件の対応を行っている）と推測）対応していることがわかる。

2.2 集計結果（カテゴリ別、対応管理）

対応管理のみ（電話およびセンターへ来室）に入力された内容について、以下の11種類のカテゴリに分類し、対応件数の集計を行った。

- 1 ネットワーク
- 2 電子メール/www
- 3 電子証明書
- 4 ユーザ環境
- 5 ソフトウェア
- 6 WorkstationSystem(WS)/TerminalServer(TS)/Thinclient/PC
- 7 並列計算機
- 8 プリンタ/コピー機
- 9 アカウント
- 10 その他
- 11 センター業務外

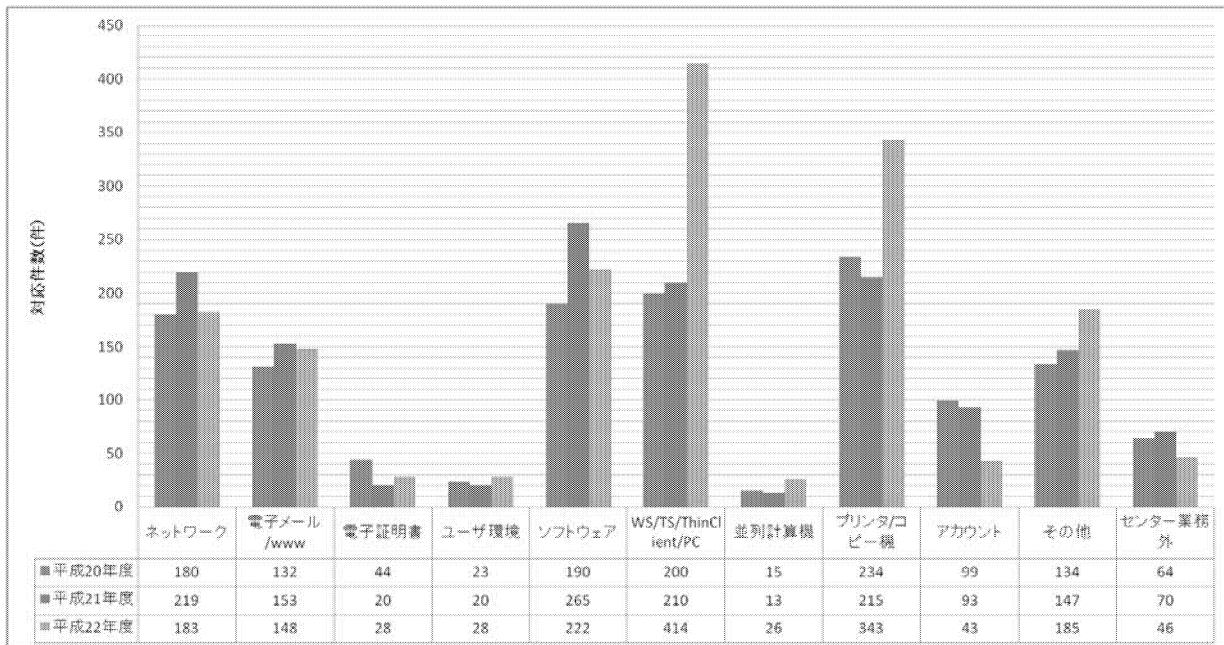


図4. カテゴリ別集計結果（対応管理）

2.3 カテゴリ別の集計結果（対応管理）からの考察

WS/TS/Thinclient/PC とプリンタ/コピー機の取り扱い件数が平成 22 年度に顕著に増えていることがわかる。

WS/TS/Thinclient/PC が平成 22 年度にほぼ倍増（210→414）している点は、平成 22 年 3 月に WindowsTS を更新し、サーバトラブル、使用方法がわからないという問い合わせ（225 件）が増えたことが原因と推測される。

プリンタ/コピー機が平成 22 年度に増加（215 件→343 件）している点は、平成 22 年 3 月に複合機を更新し、コピーカードを貸し出す業務が追加された（52 件）こと、製本サービスを開始し、補助業務、トラブルが多かったこと、また、同じくモノクロプリンタをカラープリンタに更新したことで、トナーおよび感光体交換依頼の対応件数（97 件）が増えたことが原因と推測される。

システムを更新した直後は対応件数が増える傾向があることは推測される（＝効率化を図る上では注目すべきポイント）。ただし、ひたすら件数が多い部分に着目し、件数を減らす努力をすることで効率化につながるということではない。例えば、コピーカードの貸出業務やプリンタトナー/感光体交換依頼は必要な業務であり、この業務に関する効率化は難しい。

そこで、さらに具体的にどのような内容での対応が多かったか、カテゴリ内の内訳について解析した。

今回は、日頃の担当業務であるカテゴリ（プリンタ/コピー機、電子メール/www、ネットワーク）について解析してみた。

プリンタ/コピー機のカテゴリ内で効率化できる点を検討してみると、複合機の製本補助、大判プリンタの印刷補助が挙げられる。既に利用者向けのマニュアルは整備されてはいるが、利用者からの問い合わせがあるため、マニュアルの定期的な見直し、配置場所の再検討が必要であると思われる。

電子メール/www のカテゴリ内では、平成 22 年 3 月に WindowsTS の更新に伴い、電子メール（ソフトウェア）の問い合わせが増えた。主にソフトウェア(Thunderbird)が正常に起動しない、設定ファイルが何らかのトラブルで参照できなくなり、設定ウィザードが起動してしまうなどのトラブルに関する問い合わせが多かった。トラブルの内容に応じて、対応方法は確立されてきたので、利用者に向けて「●●の症状が出たら、××のように対応する」という内容の FAQ やトラブル解決チャートを提供することで効率が高まるのではないかとと思われる。

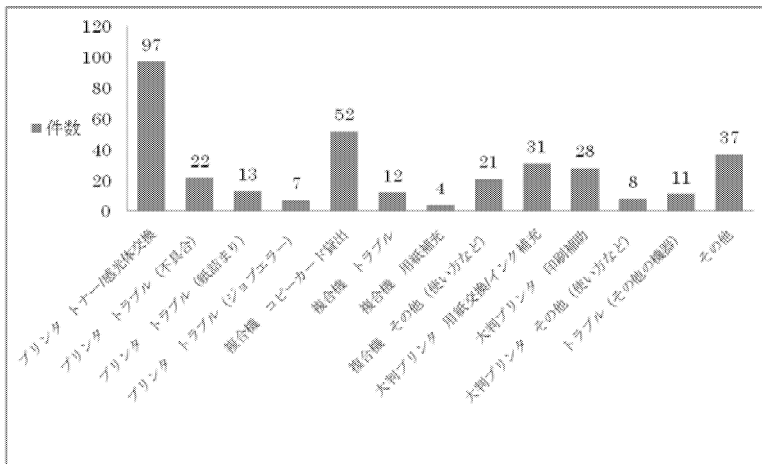


図 5. プリンタ/コピー機の内容別内訳

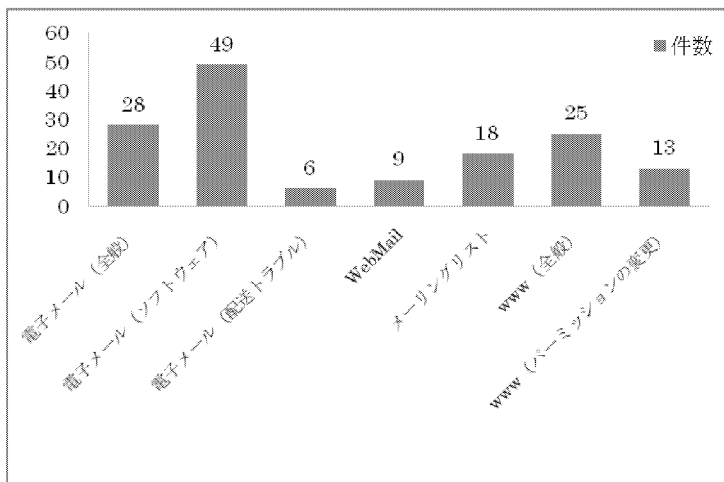


図 6. 電子メール/www の内容別内訳

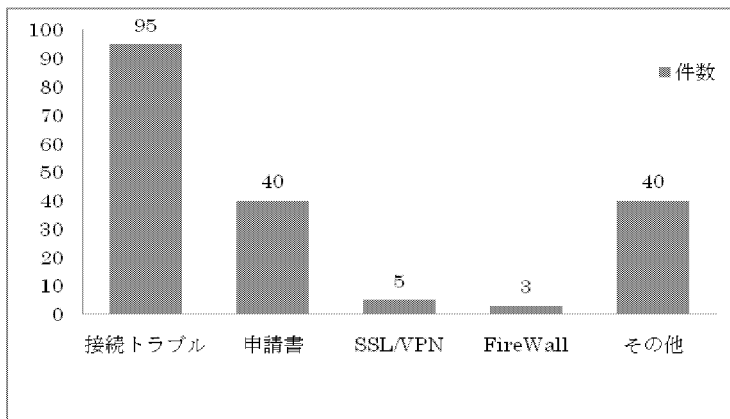


図 7. ネットワークの内容別内訳

表 3. ネットワーク接続トラブルの主な原因

主な原因	件数
DHCP サーバ	22
ケーブル	13
機器の故障	11
設定ミス(端末/MACアドレス)	16
Proxy サーバ	8
その他	25

ネットワークのカテゴリでは、接続トラブルが一番多い。主な原因についても分類してみたところ、DHCP サーバに原因があるケースが一番多く、不正な DHCP サーバが存在していた、DHCP 用の IP アドレスが枯渇

していた、特定の MAC アドレスの機器について使用不可状態になっていたということが挙げられる。その他、LAN ケーブルが利用できる状態ではなかった（経路の途中で接続が切れていた）、ネットワーク機器の故障、利用者の端末の設定ミスなどがあつた。ネットワークの接続トラブルは、よく「インターネットにつながらない」という内容のみで問い合わせしてくるケースが多く、その場合、原因特定までに時間がかかる。トラブル解決チャートを利用者に提供することで、自己解決できたり、問い合わせの際には必要な情報を付加してもらうことで原因究明が容易になり、対応時間が短縮されると思われる。

また、その他のカテゴリでは、以下のような問い合わせが多く、FAQ を充実させることで、利用者自身である程度は自己解決できるとと思われる。

1. 電子証明書

- (ア) 取得後の設定方法（Web ブラウザへのインポート）がわからない

- (イ) 有効期限切れに気づかず、電子証明書が必要なサービスが利用できなくなった

2. WindowsTS

- (ア) ソフトウェアが起動しない

- (イ) フリーズしてしまった

3. ソフトウェア

- (ア) Microsoft キャンパスアグリーメントソフトのライセンス認証に失敗

これらの結果から、改善できるポイントは以下のとおりである。

1. 利用者向けマニュアルの整備

- (ア) 特にシステム更新後、間もないサービスは重点的に

- (イ) 定期的な内容の見直し

- (ウ) 配置場所の見直し

2. FAQ やトラブル解決チャートの充実

- (ア) 定期的に対処履歴を確認しながら充実させる

- (イ) 利用者自身での自己解決を促す

3. 問い合わせに必要な情報の掲載

これらの改善を行うことで、センター受付業務の効率が高まる一方で、ユーザ自身の日常業務の不要な中断を減少させることにもつながるとと思われる。

3 まとめ

センターサービス業務が年々増えていく中で、受付業務の効率化は重要である。今回、受付業務のここ数年の集計、自己解析を行い、改善できるポイントについて検討した。その結果から今後は以下の点を改善することで、受付業務の効率化をもたらすと思われる。

1. 更新したシステムの利用マニュアルの充実

2. ユーザ自身で自己解決できるための FAQ やトラブル解決チャートの充実

3. 問い合わせ時に内容に応じたユーザに提供して欲しい必要な情報の掲載

また、個人的な課題としては、

1. 利用者へのわかりやすい説明スキルの向上

2. 留学生向けの英語表現スキルの向上

について努力していきたいと思う。

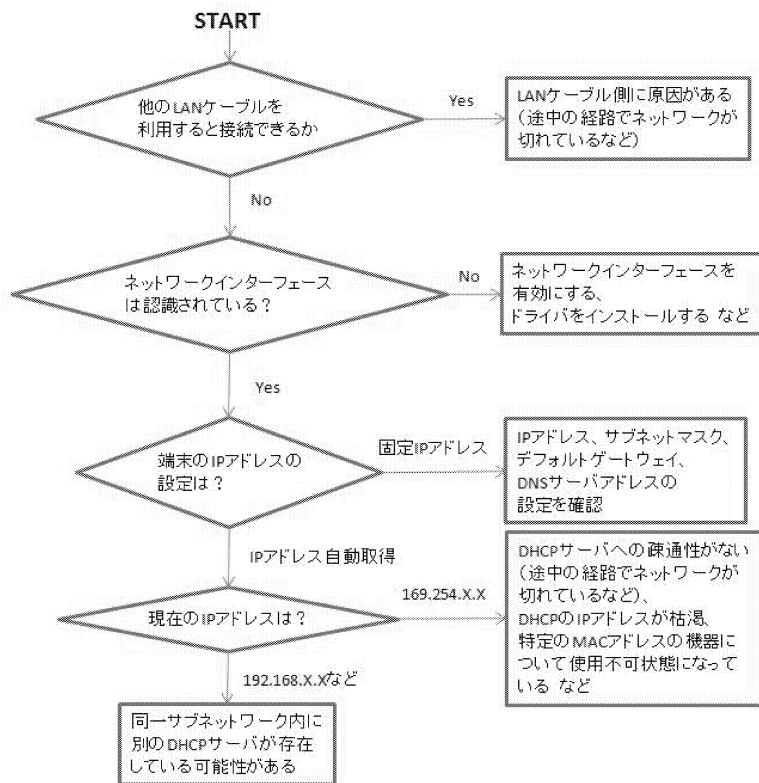


図 8. トラブル解決チャートの例
(Windows 端末がネットワーク接続できない場合)

Microsoft Application Virtualization を使ったアプリケーション配信例

二ツ寺 政友

情報社会基盤研究センター

概要

情報社会基盤研究センターでは、主にターミナルサーバのユーザに対して、Microsoft Application Virtualization を利用して各アプリケーションを配信している。今年春に行われたセンター内のグループ替えでこの業務を担当することになったので、勉強も兼ねてシーケンスの一連の操作を紹介する。そして、技術職員としての全体的なことがらを最後に述べる。

1 Microsoft Application Virtualization

Microsoft Application Virtualization (App-V) は、2006年7月に Microsoft が買収した Softricity 社が作っていた SoftGrid という製品を基にして作られた、アプリケーションを各ユーザのコンピュータに直接インストールすることなく、各ユーザのコンピュータでアプリケーションを利用可能にする機能を提供する製品である。通常は各コンピュータに直接インストールするアプリケーションを、インストールせずに App-V を使って仮想化して一つのパッケージとして作り上げ、それを配下の各コンピュータに配信することで実現している。情報社会基盤研究センターは、「情報環境システム」としてファイルサーバやネットワーク、電子メールシステム、並列計算機群等から各フロア向けのプリンタに至るまで、さまざまな情報機器を全学ユーザ向けに提供している。App-V もこの情報環境システムの一環として導入され、主に Windows ターミナルサーバ (TS) にログインしたユーザが使う各アプリケーションを配信するために使われている。

App-V ではアプリケーションを各々のコンピュータに直接インストールしないため、たとえばアプリケーションをアップデートする必要が生じた際に、以前の TS では一つ一つのコンピュータにログインして同じ作業を台数分行う必要があったようなケースでも、アップデートをかけたアプリケーションを配信し直せば済むため、大幅な省力化を実現できるという利点がある。管理者がログインすべきサーバは、アプリケーションを仮想化する (シーケンスする) ためのサーバと、シーケンスしたアプリケーションを各ユーザ向けに配信するサーバとの2つで済んでしまう。

一方で、シーケンスがうまくいかない、思った状態で配信されない、といった時の解決方法が、その時々での試行錯誤に依存してしまう場合があり、勘を身につけていく必要があったり、どんなアプリケーションでも仮想化できるわけではなく相性の良し悪しがあったりするという難点もある。シーケンス中はマウスの動きやフォルダの開閉といった操作もすべて読み取られており (次の「2 シーケンス実例」参照)、これらがシーケンスの動きを左右することもあるらしい。導入時に業者の技術スタッフから教えられたことなので本当なのだろう。実際にこの報告書を書くにあたりあらためて何種類かのアプリケーションについて、複数回シーケンスを行ったところ、同じ挙動にならなかつたり、一連のシーケンス操作はうまく完了したように見えるのになぜか思うように配信されなかつたり、といったことが続いた。この点については、既に必要なアプリケーションについてはあらかじめ配信 (あるいは仮想化に適さない物については別の方法で供用) を済ませているのでそれほど致命的ではないため安堵している。これから私が修練していけば良いことである。

2 シーケンス実例

今回は PictBear (<http://www.fenrir.co.jp/pictbear/intro/>) というペイントソフトを採りあげる。これは Windows 98 / Me / 2000 / XP / Vista / 7 で動作するフリーソフトであり、一方でターミナルサーバは Windows Server 2008 で動いているため、正しく動作しない可能性はゼロではない。われわれが Windows Server 2008 を使っている以上、ある程度仕方のないことのようなのだ。

2.1 大まかな流れ

大まかな流れは下記の 4 ステップである。

- a. 配信したいアプリケーションを用意する。
- b. シーケンス用に用意した Windows マシン上で、シーケンスするためのアプリケーション（シーケンサ）を起動した状態で、配信したいアプリケーションをインストールする操作を行い、その一連の流れを読み取らせる。
- c. 前の手順で読み取ったファイルを配信用サーバに移す。
- d. 配信に必要な設定を済ませ、配信する。

実際には、b. の際に通常のインストールであればたいの場合に用いる C ドライブの中にある Program Files フォルダではなく、シーケンス用に用意した仮想ドライブ（Q ドライブ）の中に作ったフォルダにインストールする。シーケンス用マシンはシーケンサ以外のアプリケーションをインストールしていない、言わばまっさらのマシンである必要があるため、われわれは VMware 上でこれらのマシンを稼働させ、シーケンスする際には VMware の機能でまっさらな状態のスナップショットへ戻してから行っている。シーケンス用マシンの OS は Windows 7 なり XP なりそれぞれ用意する。今回は Windows 7 64bit 版のマシンでシーケンスした。

2.2 実手順

実際の手順の流れを下記に示す。私たちの環境に依存してこういう操作になる、という部分もあることはご了承ください。

1. 配信したいアプリケーション（PictBear）のインストールに必要なファイル類を、シーケンス用マシン以外の別サーバ等にあらかじめ用意したフォルダの中に保存する。
2. VMware の管理ツールにログインし、シーケンス用マシンの画面を開く（コンソールを開く）。(図 1)
3. コンソールが開いたら、そのマシンを初期状態のスナップショットに戻す（現在のスナップショットまで戻る）。(図 2)
4. いったん VMware のロゴの表示された黒い画面になり、その後、スナップショットを採った時点までシーケンス用マシンの状態が戻る。画面右下の日付でそれを確認できる。

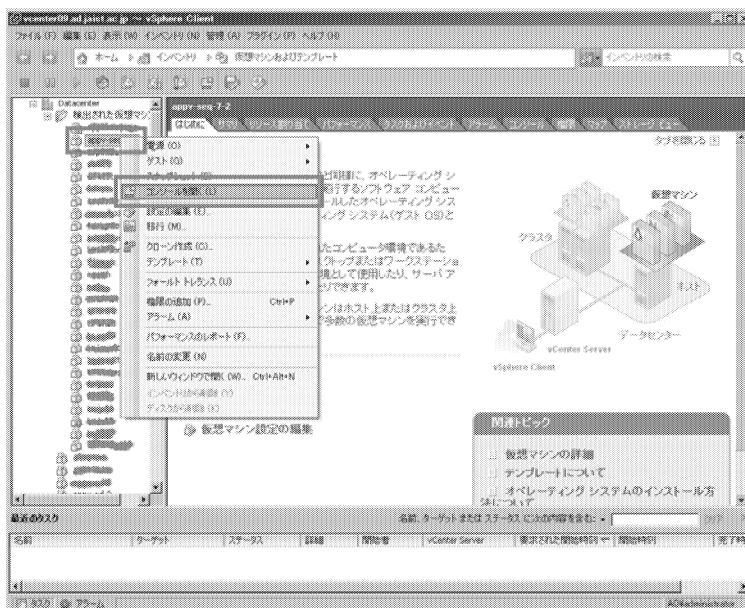


図 1 コンソールを開く

ここから先はコンソールの中、つまり、シーケンス用マシンの中で作業する。

5. あらかじめ「日付と時刻」のショートカットをデスクトップに用意してあり、それをダブルクリックし、日付と時刻をあらためて現在のものにあわせ直す。(図3)

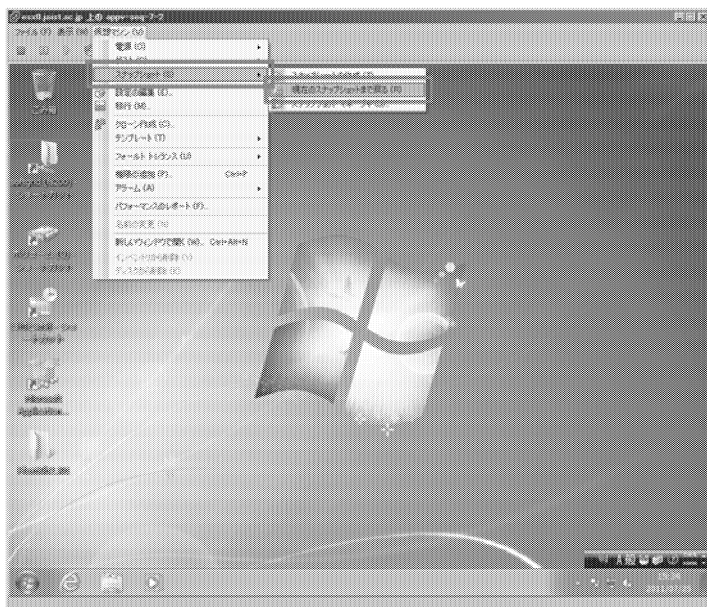


図2 現在のスナップショットまで戻る

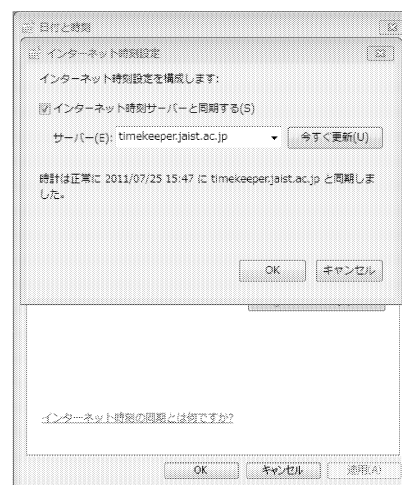


図3 日付と時刻を合わせ直す

6. デスクトップ上と、あらかじめデスクトップ上にショートカットを用意してあるQドライブの中とに、PictB203.J01 という同じ名前のフォルダを作成する。この時のフォルダ名はシーケンサの動作の仕様上、「8文字.3文字」の作りである必要があるので、わかりやすさと文字数の両方を考えて名前をつける。これらのフォルダは後で使う。
7. あらかじめデスクトップ上にショートカットを用意しておいた、PictBear を収めたフォルダを開く。今は開くだけ。
8. シーケンサを起動し、「パッケージの作成」をクリックする。(図4)
9. 次いで開いた画面でパッケージ名を入力し、「次へ」をクリックする。
10. インストールの監視という画面になる。あとはこのアイコン (pb203.exe ファイル) をダブルクリックすれば PictBear のインストールを始められる、という状態にした後で「監視の開始」をクリックする。
11. しばらく待つと、インストール先を指定する画面が表示されるので、Q ドライブの中に作った PictB203.J01 フォルダを選択し「OK」をクリックする。
12. pb203.exe ファイルのアイコンをダブルクリックし、「セキュリティの警告」が表示された場合には「実行」をクリックすると、PictBear のセットアップが始まる。(図5)



図4 パッケージの作成 をクリックする



図5 PictBear のセットアップ開始

13. ここでも再びインストール先を選ぶ画面が表示されるので、Q ドライブの中に作った PictB203.J01 フォルダを選択し「OK」をクリックする。
14. 引き続きセットアップを進めていく。例えば「デスクトップにアイコンを作成」にチェックをつけておいても作業自体にはまったく問題ない。配信対象となるユーザ全員のデスクトップ上にアイコンが出ることになるので考慮は必要。
15. インストールを終えたら、「終了」をクリックする。PictBear のセットアップ画面が閉じられる。
16. シーケンスの「監視の停止」をクリックする。
17. アプリケーションの構成という画面になる。今回はそのまま「次へ」をクリックする。
18. アプリケーションの起動という画面になる。Readme 等のファイルも同時に表示されているので、PictBear だけを選択して「起動」をクリックする。(図 6)

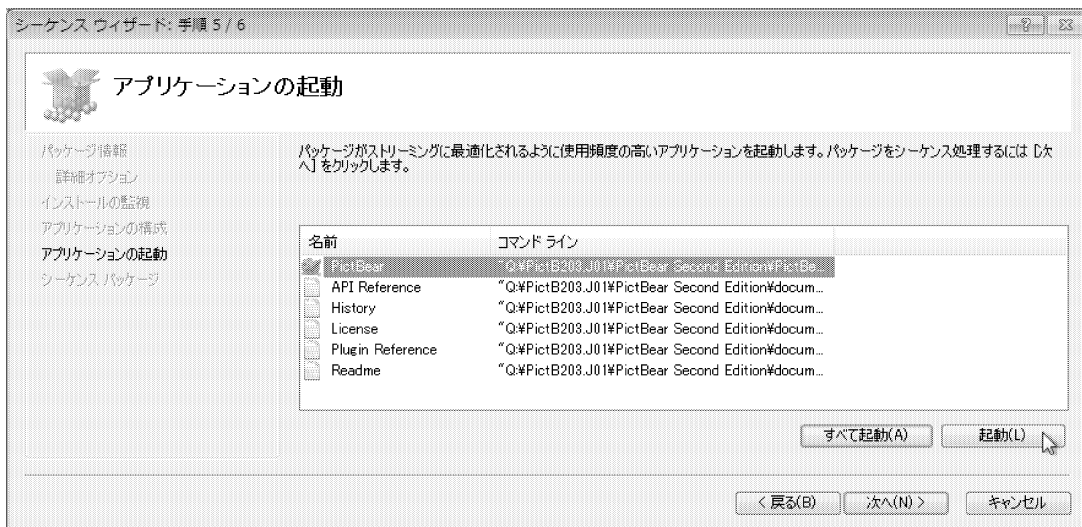


図 6 PictBear だけを選択して起動をクリック

19. PictBear が起動するので、終了させ、アプリケーションの起動の画面の「次へ」をクリックする。
20. シーケンス パッケージという画面になるので、「完了」をクリックする。
21. シーケンスの画面が閉じられる。図 7 のように、「展開」タブを開き、すべての OS を「選択済み」に加える。(図 7)
22. フロッピーディスクの絵のアイコンをクリックして、デスクトップ上に作った PictB203.J01 フォルダにパッケージを保存し、さらにそのフォルダを、配信用サーバ (OS は Windows Server 2008) の C ドライブに作ってある content フォルダの中にコピーする。

ここから先は別途配信用サーバにログインして作業する。



23. 配信用サーバにログインし、Application Virtualization Management Console を起動する。
24. 画面左の列で「アプリケーション」を選択してから、画面右の列で「アプリケーションのインポート」をクリックする。
25. ファイルを選ぶ画面が開くので、先ほど C ドライブの content フォルダにコピーした PictB203.J01 フォルダの中にある PictBear2.03.sprj ファイルを選択し、「開く」をクリックする。

26. アプリケーションのインポートという画面になるので、「アプリケーション ライセンス グループ」を unlimited に、「サーバー グループ」を Default Server Group にし、「説明」欄に必要な応じて入力する。今回は空白のままにしておく。そして「次へ」をクリックする。
27. 作成されたショートカットという画面になるので、今回は「ユーザーの [スタート] メニューに作成する」にのみチェックをつけて「次へ」をクリックする。
28. アクセス許可という画面になるので「追加」をクリックし、開いた画面で、今回配信対象とするグループ isc を追加する。全ユーザに向け配信する場合は Domain Users を追加する。そして「次へ」をクリックする。
29. 概要という画面になるので、「完了」をクリックする。画面が閉じられる。
30. PictBear をシーケンスした際に結果的に一緒についてきてしまった、アプリケーションではないファイルを、Application Virtualization Management Console 上で削除する。Console 画面右の列にある「削除」をクリックすればよい。(図 8)



図 8 Application Virtualization Management Console の画面

31. これで、isc というグループのメンバとなっているユーザに向けた PictBear の配信が始まった。
32. 実際に使用するには、既に TS にログオン中の場合には、画面右下にあるオレンジ色の四角いアイコンをクリックして「Refresh Applications」をクリックし、数秒待つと反映される。「スタート」→「すべてのプログラム」→「Fenrir Inc」→「PictBear」→「PictBear」と選んでいき、PictBear を起動できる。以上で手順は終わりである。操作のためにログインしたサーバ等は必要に応じてログオフや切断等を済ませる。

3 感想

今後さらに回数をこなしてこつを身につける必要があるとまずは感じた。操作そのものは決して難しくないのだけれど、独特のブラックボックス感がある。先にこれを担当している職員からもいろいろと吸収せねばならない。今回の例では例えば、ユーザが実際に PictBear を起動するに当たって（手順 32） PictBear のアイコンの位置を、「スタート」→「すべてのプログラム」→「PictBear」とクリックすれば済むようにきっとできるはずだと思い、手順 27 においてあれこれ試したのだが、結局思うようにできなかった。また別のアプリケーションでは、アプリケーションの機能そのものの部分の他に、ヘルプファイルやプラグイン等も同時にシーケンスして配信し、起動させてみたところ、正しく起動しているのかわからなかった。そのアプリケーションの需要があるかどうかにかかわらず、まだまだこれからいろいろなアプリケーションについてシーケンスを試して習熟していく必要がある。既に配信成功しているアプリケーションのプロパティをのぞいて見て、まねしてみるのも良いだろう。回数をこなしているうちになんとなくわかってきて、ブラックボックス感も薄らいでいくのではないかと期待している。そして今回は手順の紹介のみにとどまったが、次回このような原稿を書く際にはより中身の濃いものを書けるようにしたい。

4 おわりに

ここまでは App-V について述べた。おわりに、自分自身の技術職員としての全体的なことについて記す。現在、大きく四つの課題がある。一つ目は以前の発表でも述べた通り、センターの中での自分の核となる分野を早く確立すること、二つ目はセンターの受付窓口や電話でのやりとりをもっとスマートにできるようになること、三つ目は自分の受け持っている各作業の進捗管理を強化すること、そして四つ目は、センターの枠を超えた技術サービス部に所属する者としての働きに、より積極的に関わっていくことだ。一つ目については、残念ながら未だに方向性を見いだせていない。見つけなければという不安は常にあるものの、日々の目の前の仕事や受付対応で受け取った件に取り組むことでいっぱいとなってしまう。

二つ目のユーザとのやりとりについては、もし自分が逆の立場だったらおもしろくないだろうな、というような返答の仕方を、してしまった後で今の受け答えは良くなかったと気づくことが多いので、そういう返答を減らすように心がけたい。何でもかんでも優しく受け答えをしていれば良いというものではなく、時には不親切な人だと思われることを恐れてはならない時もあるのが実際なので、使い分けることができるのが理想ではある。

三つ目の進捗管理については、現在常に「あれもこれも間に合っていない」状態なので何とかしなければならぬ。サイボウズ等で日々の予定管理はしているものの、自分の個々の仕事の管理にまでは活用できていない。私達の周りには、私達よりもよほど厳密に進捗管理をし、私達よりもよほどたくさんの要求を顧客から受けているであろう業者の方達がいて、私達はそういった方達から工程管理表を受け取る立場でもある。どんな内容が書かれているか思い出しながら、自分に当てはめると良いと思っている。

四つ目については、本学の開催する行事や地元の催し物において科学実験等の実演・展示をするといった、技術サービス部としての動きの時に、ナノマテリアルテクノロジーセンター担当技術職員の方達におんぶにだっこの状態が続いているのを改善したい。現状では打ち合わせに出席したり当日の手伝いに参加したりする程度しかできていないので、いずれはその行事にふさわしい内容の出し物を具体的に探し出して提案し、実行するところまでできるのが望ましい。

以上、担当業務の一つとして App-V のことを、そして、技術サービス部に所属する技術職員としてのことを述べた。こうして書き上げてみると課題ばかりであるとあらためて思い知らされる。日々少しでも成長して行けたらと思う。

JAIST 統合ユーザ環境の運用

宮下 夏苗

情報社会基盤研究センター

概要

当情報社会基盤研究センターは全学生および教職員を利用ユーザと位置づけ、2010年2月より、それまでサービスしていた Windows ターミナルサーバシステムに3つの仮想化技術を取り入れて改良し、メンテナンス作業によるシステム停止、サービス中断を可能な限り抑え、いつでも、誰でも、どこからでも利用可能な、ターミナルサーバクラウド環境としてリリースした。本稿では、このクラウド環境に至るまでの改良の歴史と現状の運用について述べる。

1 はじめに

先端的科学技術教育・研究の推進にあたり、情報およびその処理技術は不可欠の基盤であるといえる。本学では開学当初より、全学ユーザの研究・教育活動に資するべく、情報の生成、蓄積、利用に関するあらゆる局面を支援する統合的情報環境システムを設計、実現してきた。情報社会基盤研究センター(以下センター)は、この情報環境の運用、管理および、先進の技術研究を踏まえた先端的システムを導入、情報環境へと組み込む役割を担っている。ここでは、情報環境システムにおいて、各ユーザに日常の作業空間を提供する統合ユーザ環境の改良と運用について説明する。

2 統合ユーザ環境の変遷

2.1 旧環境と改良(～2006)

2006年以前には、各ユーザが利用する端末として、OSにSun Solarisシリーズを利用したSun Workstationをほぼ一人1台に近い割合で配置してきた。ユーザのホームディレクトリおよび各種ツール類を格納する共有ディレクトリを超高速ネットワークで接続されたファイルサーバに格納し、各ワークステーションからのオートマウント設計とした。

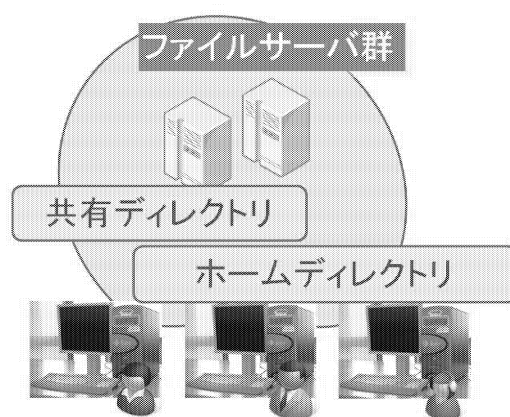


図1 2006年以前

しかしこの環境においては各ユーザに提供する端末一台づつが高価であること、当時増えつつあった

Microsoft Windows 系 OS を動作条件とする研究，教育用ソフトウェアのサポートが困難であることなどの問題があった。

2.2 旧環境と改良 (2006~2010)

前項の問題を踏まえ，2006年にこれまでの環境を改善するべく Windows Terminal Server システムを導入した。各研究室・部課ごとに Windows 2003 Server が動作するターミナルサーバを配備し，ファイルサーバに格納されたホームディレクトリ，共有ディレクトリをこれらターミナルサーバからマウントする設計を追加した。また旧 Solaris 環境の利用も維持するべく共用の Solaris サーバを準備し，これまでの Sun Workstation に代えてユーザがターミナルサーバ，および Solaris サーバに接続するためにシンクライアント端末を配置した。

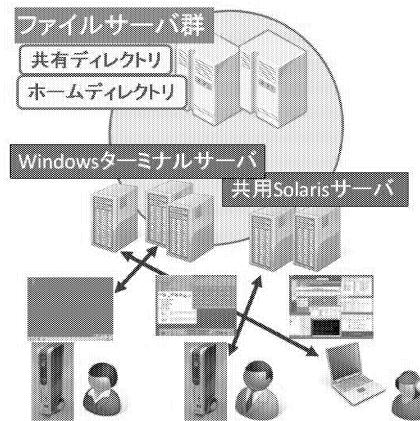


図2 2006年 ~2010年

しかしこの環境においても，各部課・研究室の利用頻度によって，配置した Windows ターミナルサーバの負荷に大きく偏りが生じるという問題があった。また，事務局向けのターミナルサーバにおいては，夜間はまったく利用されないまま電力だけを消費する状況となっていた。さらに，100台以上の物理サーバについてはそれぞれの運用，管理の多くを各研究室に一任していたが，研究室によってはセキュリティアップデートがなされていない，ソフトウェアが古いバージョンのままであるなど管理状況はサーバによってまちまちであった。

2.3 旧環境と改良 (2010~)

前項の問題点を解決するため，2010年2月，Windows Terminal Server 環境に3つの仮想化を導入した JAIST ターミナルサーバクラウド環境を設計，実現した。

2.3.1 サーバ仮想化

サーバ仮想化により，一台の物理ホスト上に複数の仮想ホストを動作させる。これを実現する製品として，すでにセンター内で運用実績があり，導入事例が豊富かつ安定性，操作性に優れていると考えられる VMWare VSphere4.0 を採用した。動作中の仮想ホストを無停止で異なる物理ホストに移動する機能を活用し，物理ホストのメンテナンス性の確保および，物理リソースの負荷分散を実現できた。

2.3.2 セッション仮想化

旧来はユーザ自身が個別のターミナルサーバを指定してセッションを開始していたが，これを一元化し，ユーザのセッション開始要求をゲートウェイが受け付け，負荷分散のもとに適切な接続先ターミナルサーバに割り振る方式に置き換えた。このシステムの構築のため，Citrix XenApp5.0 を利用している。各ユーザのセッション接続状況はゲートウェイにおいて確認することができ，セッショントラブル発生時等に役立てることができる。また，メンテナンスを要するターミナルサーバを負荷分散の対象から外すことで，サー

ビス中のターミナルサーバクラウド内(負荷分散の対象内)のサーバには影響なく、サーバメンテナンスを行える。さらに、各仮想ホストに割り当てられた仮想リソースの現在の利用負荷状況をもとに、ユーザログインを優先的に負荷の低いサーバに割り当てる機能を活用し、仮想リソースの負荷状況に基づいた負荷分散が可能となった。

2.3.3 アプリケーション仮想化

通常 Windows のアプリケーションインストールは各 OS のローカルフォルダにインストールを行う。構造の簡単なものは CIFS 共有を行うファイルサーバ上の共有ディレクトリから起動できる場合もあるが、多くのアプリケーションはローカルフォルダ以外へのインストールを考慮しておらず、その動作は保証されない。

このことは、仮想ホストといっても 100 台あれば 100 台すべてに対してアプリケーションのインストール、アップデートが必要となることを意味する。しかし、一般的に常用されるブラウザ、メールである FireFox, ThunderBird を含め、ソフトウェアのアップデート、セキュリティパッチリリース頻度は少ないとはいえない。その都度全サーバに対してアップデートを行うには、相当の作業コストが要求される。この作業コストを回避するため、Microsoft Application Virtualization に基づいたアプリケーション配信システムを構築した。アプリケーションをパッケージングし、全サーバに配信することで、全体へのインストール適用、アップデートといった作業を劇的に簡略化することができる。また、同じアプリケーションの異なるバージョンを同時に配信する、所有ライセンス数に応じて、同時に利用しているプロセス数の監視・管理を行うといった機能も活用している。

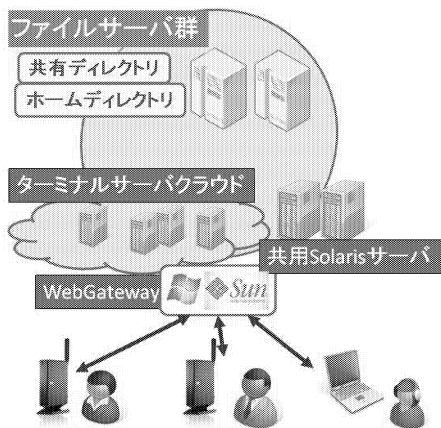


図3 2010年～

3 ターミナルサーバクラウドの障害

構築したターミナルサーバクラウド環境は物理ホストの上に多数の仮想ホストを作成し、さらにこれらの仮想ホストのレイヤでセッション、アプリケーションの仮想化を行うという多段階構成となっている。構成が複雑であるため、一旦障害が発生した場合には障害部位の特定、復旧に時間のかかる場合もある。

一例を挙げると、仮想ホストが突然停止した場合にこれが Windows OS の問題であるのか、Citrix XenApp による障害であるのか、または、ハイパーバイザ、物理障害のレイヤの問題であるのかをまず切り分けなくてはならない。

昨年7月から一年間で起こった障害件数は17件が記録されている。うち、複数台の仮想ホストがサービス中に停止するといった、被害範囲の広い障害も3件発生している。

次章では、この障害対策および監視と、日常のメンテナンスについて述べる。

4 ターミナルサーバクラウドの運用と改良

本システムにおいてシステムのパッチアップデート、物理ファームアップデートなどのメンテナンス要項は、通常の物理サーバの運用に比べ圧倒的に多くなる。また、システムの複雑性から一部に発生した障害を発見しにくく、気づいていれば修復できるような問題であっても、いつ発生したか判らないまま、ユーザからの問い合わせを待つよりない状況も発生した。個々の物理ホスト、仮想ホストの稼動状況、システム状態ばかりでなく、クラウドシステム全体についても動作状況の正常性を適切に監視して、障害の発生を検知する必要がある。この章では、システム運用におけるメンテナンス作業および障害検知と、その改良について述べる。

4.1 仮想ホストのアップデート、パッチ適用

クラウドシステムを構成する仮想ホストは、総計で 150 台近くにもなる。これらのホストに対して、一台づつセキュリティパッチを適用する、HotFix を適用するといった作業は非常に困難である。これらの作業を緩和、軽減する方式として、以下を行っている。

1. WSUS(Windows Server Update Service)
2. リモートスクリプト

4.1.1 WSUS

WSUS は Microsoft の機構で、Windows Update を管理サーバで集中管理し、管理クライアントのパッチ適用状況を確認する、必要なパッチを選択適用させるといった一括処理を可能とするシステムである。2006 年時のターミナルサーバシステムから導入しており、運用実績のある本サービスをこのクラウドサービスに適応するよう構成し、運用している。

しかし、WSUS で適用できるのは Microsoft が提供する一般のアップデートリリースのみである。特殊な障害に対応するための Hotfix や、Microsoft 純正以外のアプリケーションが必要とするパッチアップデートは、この方法で配布することはできない。

4.1.2 リモートスクリプト

WSUS で配布する以外のアップデート適用、その他の仮想ホスト一括操作のために、リモートスクリプトを利用するようにした。最初に考案した方式では、コントロールサーバ上にコマンドを仮想ホスト全台に送信するためのバッチファイルを用意した。コマンドによって、各仮想ホストがコントロールサーバ上に置いたインストーラ実行用バッチファイルをそれぞれ実行し、同じくコントロールサーバ上に置いたインストーラ本体をサイレントインストールオプション付きで起動する。

しかし、一台のインストールに時間がかかる場合など、コントロールサーバ上に用意した仮想ホストへのコマンド送信用バッチファイルに記載した、個々の送信コマンドが正常に完了せず、処理シーケンスがうまく動作しないためにホストでコマンドが正常に実行されないことがあった。

これを克服するため、処理方法を改良した。コントロールサーバ上に仮想ホストへのコマンド送信用バッチファイルを準備することはこれまでと同様であるが、送信したコマンドで直接各々の仮想ホストにインストーラ実行用バッチファイルを実行させるのではなく、各仮想ホストが 1 分ずつ間を置いて実行するよう、各々の仮想ホストにタスクスケジュールを記録する方式へ切り替えた。この処理変更により、コントロールサーバ上の処理は全仮想サーバにコマンドによりタスクスケジュールを設定するだけの簡単な内容となり、処理のシーケンスが停止する問題は起こらない。また、各仮想サーバも自己のタスクに記載された、インストーラのダウンロードおよび実行を各々のサーバが行うこととなり、タスクの実行時間をずらすことでダウンロードが集中することも回避できた。

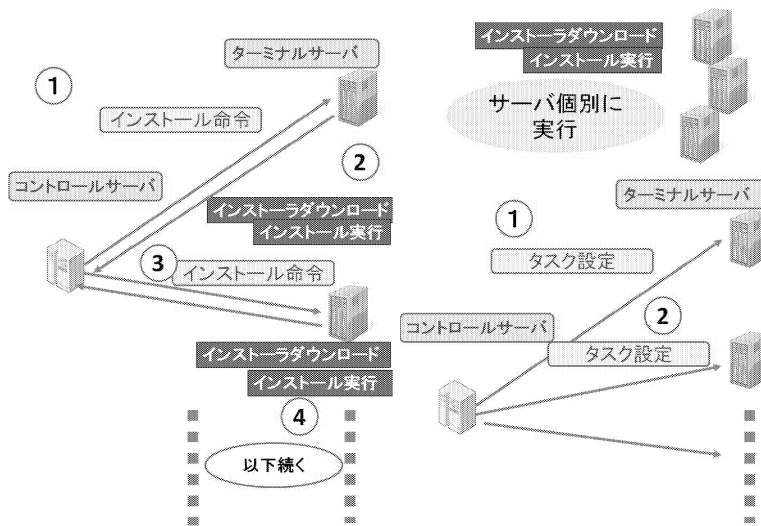


図4 アップデート方式改良前後

4.2 監視

仮想ホストはおろか、当然物理ホストについてもそれが正常に稼動していることを監視し、異常時にはまずサービスへの影響を最小限に抑え、かつ異常を速やかに復旧する必要がある。

センターでは次のような方法により、システムの正常性を監視、維持している。

1. pingman による物理ホスト、仮想ホストの生存監視
2. 仮想ホストの printspooler プロセス動作監視
3. 仮想ホストのローカルホストキャッシュ正常性監視
4. 仮想ホストのターミナルサーバ機能監視
5. 仮想ホストのディスク空き容量監視

pingman による監視は、センタ内に設置した大型ディスプレイに常時 pingman による ping 応答出力結果を出力しており、異常があれば速やかに職員が視認できる環境を構成している。

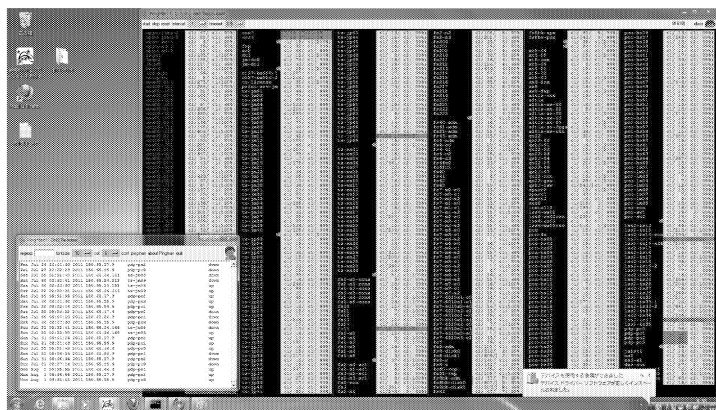


図5 pingman 監視

それ以外については、定期的に監視スクリプトを動作させており、異常を検知するとメールで通知するようになっている。

5 まとめ

本稿では JAIST における歴代のユーザ環境と、その改良、これらに基づいて構築された現在のターミナルサーバクラウドシステムにおける運用とメンテナンスについて述べた。さらに改良すべき点として、現状アップデート作業に利用しているリモートスクリプトの設定が、ある程度人手によるという点がある。スクリプトを洗練させ、人的ミスがより介入しづらいものに改良する必要がある。また、システム自体の障害件数が現状少ないとは言いがたい。より堅牢かつ安定したサービスを行えるよう、システム設計の見直しを含めてシステム全体の改良を図りたい。