認証サーバを基盤とした教育・研究用ネットワークシステムの構築について

白濱　成希*

Construction of Educational Computing System Based on Authentication Server

Naruki SHIRAHAMA

Abstract

We have fully updated the educational computer system in Kitakyushu National College of Technology on March 2011. We adopted two new technologies, cloud computing and virtualization to our system. Cloud computing is the delivery of computing providing computation, software, data access, and storage services. We choose two educational cloud services, one is Google Apps for Education the other is Microsoft Live@Edu. All students, teachers and staff can use Gmail, Google Calendar or Microsoft Outlook Web Apps and Office Web Apps. There are no servers and storages concerning these educational cloud services in our campus. We also reduce hardware cost of existing other services Windows Server or UNIX server using VMware ESXi. The redundant server has six Server OS, and using virtualization technology. We can reduce not only hardware cost but also running cost such as electric power, installation space and management cost. We already achieved the introducing account management system last year. All users have to do is to remind only one password to login Windows/Linux Gmail and WebClass (LMS) and so on. LDAP appliance server AXIOLE can provide us account management system for multi services.

Keywords:　*Cloud computing, Virtualization, Account Management System, LDAP, Active Directory, e-learning.*

1. はじめに

平成23年4月に新しい教育用システムの稼働を開始した。旧システムの稼働開始は平成17年4月であったため実に6年間の稼働となった。本来の予定では5年間の間隔を想定していたが、システムが概ね安定している点と、クライアントOSが確実にWindows7に切り替わるという点を考慮して更新を1年送らせた。

旧システムが本校のニーズを満たしており、特に変更を要求される点はなかったため、旧システムをベースに本校ITセンター教育室が将来必要になると思われる要素を拡充するという方針で仕様策定を開始した。大きな追加は「1. 教育用クラウド」、と「2. 仮想化システム」という2点である。図1に仕様策定にあたり、本校教育システムの構想を示す。図2に示す通りシステムの中核は認証レイヤである。

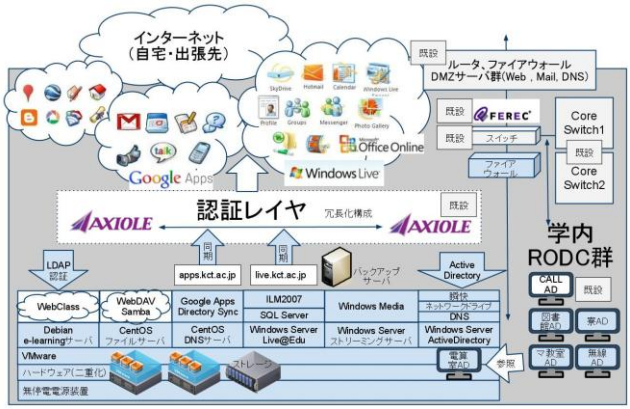

図1. 本校教育システム構想

旧教育用システムでは、はじめて業界標準であるサーバ用19インチラックを採用し、1U型のサーバを導入した。電子計算機室のサーバルームのスペースに限りがあり、これまでのようにタワー型のサーバを導入することは難しいと判断したためである。学内業務のIT化が進むにつれこの傾向は加速し、現在は校内LAN主要サーバ群、Webサーバ群がラックマウントサーバに取り付けられている。今回導入するシステムもラックマウント式を採用した。旧システムではサーバ用途ごとに1台ずつ物理サーバを用意したが、新システムでは仮想化技術を用いることで論理的にサーバを用意することが可能となったため、さらなる集約化を実現した。

「教育用クラウドシステムの導入」もIT教育総合情報センターの長年の達成目標であった。スマートフォン、タブレットとIT技術の普及はさらに加速し、比例する形でe-learningの利用率も上昇している。インターネットにおける連絡手段は未だ電子メールが主役であり、学生の利用率を向上させる電子メールシステムを導入することは、各校IT担当者の共通目標である。教職員と違い、学生は研究室に配属されない限り専用のPCを利用する事は出来ないため、Webメール環境の方が適している。本科・専攻科合わせて1,200名余りの学生が快適に利用出来る環境を考えると、処理能力、メモリ、ストレージ、そしてサーバ設置場所を考えたると、教育用クラウドを利用することがベターなソリューションとして浮上した。教育用クラウドの導入に関しては、電子メールデータが海外企業のサーバにあるということに関して不安視する意見もあるが、本校では学生利用である事と、一年以上かけて議論を行い、他校の導入実績から教育用利用に問題はないと判断した。以上が導入背景である。次節以降で各項目について説明する。

2. 仮想化

2.1 仮想化技術導入経緯

仮想化には様々な利点が挙げられる。本校においてはまず設置スペースの関係からサーバを集約する方がよいと判断した。サーバ数を減らすことで消費電力や空調に関してもコストを削減できる可能性がある。またサーバをファイルとして運用するため管理コストの削減が期待できる。しかしながら物理サーバを1台に集約してしまうと、ハードウェアトラブル時の被害が甚大となる。しかし、完全な2重構成にすると予算面で厳しくかつ、普段の活用割合が低くなる。実際に仮想化を導入する際には上記のバランスを考慮し、最低限必要なパフォーマンス、スケーラビリティを考慮して性能を決定し、2台構成にするのがよいと思われる。今回導入した仮想化用サーバのスペックは、Intel Xeon X5670 (2.93GHz/12コア)、メモリ 64GB以上、1000Base-Tを8ポート以上とした。現在7つの仮想サーバを2台の物理サーバ上で稼働させているが、トラブル発生時には復旧までの間、1台に集約して運用することも可能である。

VMware vSphere 4 Advanced Edition相当以上の機能を持つ仮想化システムが必要であると判断した。特にvMotionは稼動中の仮想サーバのダイナミックな移動のために必須である。vMotionについて説明する。

2.2 vMotion

図2にvMotionの概念図を示す。複数のサーバは物理サーバが構成するリソースプールの上で構築された論理サーバ上で起動する。論理サーバは仮想化されたハードウェアにインストールされている。仮想化されているとはいえ、物理サーバ上のCPUのコアを1個以上割り当てられており、同様にメモリやディスクも物理サーバ上のリソースから割り当てられている。従って仮想化といえども物理的制約がなくなったわけではない。しかしながらリソースプールを物理サーバ2台以上で構成されている場合には、vMotionを用いてダウンタイムなしにサーバを稼働させる事ができる。導入当初のサーバ群であれば、冗長化された2台の物理サーバのうちどちらかのサーバにハードウェアトラブルが発生した時にも、即座に対応できる。

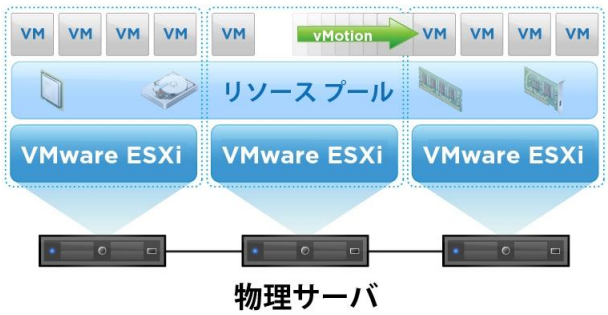

図2. vMotion概念図

2.3 ダウンタイム軽減の必要性

教育用電子計算機システムの利用はミッションクリティカルシステムと言わないまでも、年を追うごとにより少ないダウンタイムが要求されるようになった。年に数度の作業停電時はもちろん、今回の更新にあたっても教育用サーバ群を長期間停止する事に対してクレームがくるようになった。これは本校における教育用システムの利用が、これまでの「授業時間に教室で計算機教育環境を提供する」というものから、「e-learningや電子メールシステムなどネットワークを利用することで時間的空間的制約を超えてサービスを提供する」という形態に進化したことの証左といえる。

しかしながら大学や研究機関等と比較して、高専が教育用電子計算機システムに割り当てる事の出来る予算は極めて少ない。サーバハードウェアの一部にトラブルが発生したと過程しよう。通常主要ハードウェアの保守契約はセンドバック形式で行われる。センドバックとはどのハードウェアにトラブルが発生しているか原因を切り分け、部品を取り外しメーカーに送り、修理後送り返されてくる形態のサポートである。そのため2,3週間かかることも珍しくない。これまではこの形態のサポートであっても問題は少なかった。例えば過去にはActive Directoryサーバに不具合が発生した際、クライアントPCをスタンドアローンで動かして授業を行い対処したという事例がある。だが現在WebClass、電子メールシステムが使えないという状況はとうていされるものではない。今や教育用システムにおいてもサーバの冗長化は必須といえる。

冗長化とは待機系のハードウェアを用意し、主系ハードウェアにトラブルが発生した時に待機系に切り替える事をさす。障害が発生してから待機系を稼働させることをコールドスタンバイ、主系と同じ動作を行っている待機系に即座に切り替える事をホットスタンバイと呼ぶ。一般にホットスタンバイはコールドスタンバイに比べて、同期設定等にコストがかかるため、予算の制約から導入出来ない事が多い。しかしながら今回導入したVMware ESXiのvMotionを利用することでホットスタンバイと同等の環境を構築できた。主系、待機系の区別なくどちらのサーバが停止したとしても、片方のサーバで引き続き運用することが可能である。

2.3 VMware HA

ここで「vMotionで仮想サーバを別の物理サーバに動かすといっても誰が行うのか?』作業担当者が到着するまでの、ダウンタイムは発生するのではないか?」という問題に直面する。しかしながらこの問題もVMware HAで解決する事が可能である。VMware vCenterが導入されている、2台以上のVMware ESXが導入されている、共有ストレージが構成されている、等の条件を満たすことでVMware HAが利用可能となる。VMware HAの動作について説明する。一方のサーバにトラブルが発生したと仮定する。なんらかの理由でサーバの電源断が発生し、サーバが起動しなくなったとしよう。vCenter serverが異常を検知し、共有ストレージ上にある仮想マシンを正常に動作している物理サーバに割り当て、再度サーバが起動する。vCenter Serverが停止中であっても、各ESX

のサービスとしてインスト ールされたエージェント がフェイルオーバー機構を実現する。図3にvCenter Serverの設定画面を示す。本校仮想環境におけるデータセンター、クラスター、ホスト 仮想マシン及びVMware HAの設定を確認することができる。

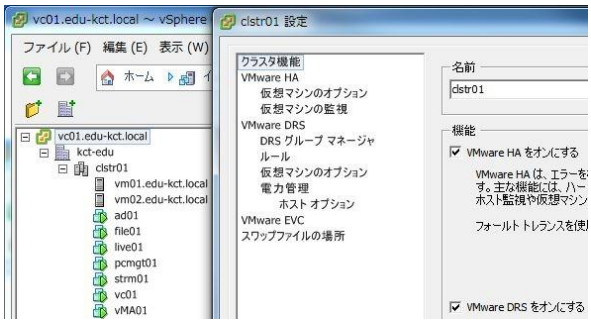

図3 vCenter Server設定画面

図3より VMware DRSの設定を確認する事ができる。DRSとはDistributed Resource Schedulerを意味し、その時の負荷に応じて自動的にvMotionを実行し、負荷を分散する事が可能となる。従ってハードウェアトラブル時にVMware HAによって、別サーバによって移動した仮想サーバは、ハードウェアトラブルから復旧した時に元の構成に戻り 運用される。

2.4 iSCSI

前節でvMotion, VMware HA, VMware DRSについて述べたが、いずれも 高性能な共用ストレージシステムを導入して初めてその性能を発揮するといえる。今回導入したものはSASを14台搭載可能なものとし、4 Gbps Fiber Chanelと 1Gbps iSCSIポート をそれぞれ2系統ずつ有している。RAIDの構成も各レベルの筐体内混在が可能であり、電源・ FABユニットも 冗長化可能かつホット スワップに対応している。今回はiSCSIをストレージに採用している。iSCSIとはSCSIプロトコルをTCP/IPネットワークで利用する規格である。ギガビット・イーサネットの普及により、導入にあたってのコスト パフォーマンスが良好であることが採用の理由である。

2.5 高専での仮想化導入に関する考察

高専において、仮想化システムを導入する意義について考察する。予算も 人的リソースも 限られた高専においては、どの程度の稼働率が求められているかを考慮しなければならない。PC教室用のActive Directoryサーバを運用する程度であれば、サーバの重要性はそれほど 高くなく、ストレージをRAID構成などで運用することでニーズを満たせる。しかしながらそこに、e-learningやWebDAV等のファイルサーバ、電子メールサーバ(本校はクラウド 上で運用)等が稼働すると、要求されるダウンタイムは極めて短いものとなる。ホット スタンバイのための予算がなく、迅速に復旧するための人員も確保出来ない場合、現時点における VMware社が提供する一連の仮想化技術の採用は最善といえる。仮想化技術の利点は耐障害性だけではない。教育用計算機システムは導入年度に全体を設計し、以降は4-6年の間レンタル費用を支出するという 形式であるため、年度途中でのハードウェアの追加・ 削減は一般的に難しいといえる。しかしながら 最初にリソース プールを確保し、サーバを論理的に構築する事ができる仮想化技術は変化に強いシステムであるとも 言える。

3. 教育用クラウドシステム

3.1 教育用クラウド導入経緯

本校では早くから教育用クラウドの導入を検討してきた。教職員の業務用途に対しては導入が見送られたが、教育用途には問題がないであろうという 判断を正式に委員会において決定した。これを受け新システム導入の10ヶ月前から試験的にGoogle Apps for Educationを導入した。従来の教育用サブドメインはeduであったため、新たにappsという サブドメインを決定し、DNSサーバへの登録を行い、あらたにKCT Appsという 名称で試験運用を行った。学生へ電子メール利用を促進するためには、より信頼性があり、使いやすいサービスが必要であったが、Gmailはその要件を満たしている。非常に高機能なメールサービスであり、1人当たりに容量は25GBを超える。優れたspam判定、ラベル/フィルタによるメール管理等は、既に多くのユーザの支持を集めている。ドメインでの運用なので、メーリングリストに相当するグループ機能や、整備された連絡帳などにより、学生の利用率が上昇している。図4にGoogle Appsの設定画面を示す。常時200人前後のユーザが週ごとに使用していることがわかる。

図4. Google Apps ステータス

3.2 高専での教育用クラウド導入に関する考察

すでに多くの大学で教育用クラウドを導入している。Google Apps for Education, Microsoft Live@Edu, Yahoo Mailといった違いはあるが、電子メールのインフラ・ 管理コスト の削減が第一の目的であると思われる。学生数の多い大学ではコスト 削減効果も 大きい。もちろん高専でもその効果は大きい。現在Google Appsでは一人あたり 25GBのメール容量を提供している。学生数を1200と 見積もると30TBとなり、RAID構成まで考慮すると導入検討さえ不可能である。もちろんこの容量が必要であるとはいえないが、容量を気にせずに利用出来るというのは利点であるといえる。メールは全てGoogleのサーバにあり、メールを貯めこんでもローカルのWindowsが重くなるということはなく、検索

も高速である。Google Apps for Businessを採用する企業も増えており、学生がWebメールに慣れておくという効果も期待できる。

導入にあたりGoogle, Microsoft, Yahooと検討したが、機能と使いやすさ、コストの面からGoogleをメインに使用することにした。しかしながらOffice Web Appsの動向や、高専がMicrosoftと提携した事を考慮し、Microsoftも利用可能とした。

4. LDAPによる認証一元管理

4.1 認証一元管理導入経緯

平成17年度の更新からIT教育総合情報センターではアカウントの一元管理を目標に掲げてきた。旧システムではActive Directoryをインストールした Windows Server上でService for UNIXをインストールし、NISを動かすことで、電子メールやWebClassと認証一元化を実現した。しかし認証の重要性が高まると、Windows Serverではなく認証に特化したアプライアンス製品の採用が望まれるようになった。例えばWindows Serverを用いる場合、再起動に要する時間、セキュリティの都合上Windows Updateを行わなければならない時の動作検証、ディスク障害等の要因が無視できなくなったためである。

そこでLDAPアプライアンス製品であるAXIOLEを導入し、全面的に認証サーバとして参照、教育用システムの基礎とした。認証専用の製品を導入したことによって、教育用システムはより安定して運用する事が可能となった。Windows Serverを再起動しても、WebClass等の他の認証に支障をきたさない。何よりユーザのパスワード管理が、各自がWeb上で行えるようになった。例えばユーザがリマインダ用に携帯電話のメールアドレスを設定しておけば、パスワードを忘れた際にもユーザの権限のみでリセットすることができる。管理者グループという概念があるため、IT系の科目を担当する教員に権限を付与することでセンタースタッフの代わりに学生のパスワードリセット作業も依頼できる。

4.2 RODC、WebDAV

今回の導入では各学科のPCの教室も恩恵を受けている。RODCを設置し異なるPCの教室でも同一のアカウント情報持たせ、管理者の負担削減となった。またネットワーク構成の見直しと、トレージサーバの性能向上により学内であればどのPCの教室でも同じホームドライブにアクセスできる。各ユーザのホームドライブはWebDAVとしても提供されているため、学内はもちろん学外からも認証を経由してセキュアにアクセス可能である。

4.3 Rubyによるユーザ登録支援

複数のサービスが認証サーバに依存するため、各システムの設定の整合性を取る必要がある。アカウント情報は認証サーバが持つが、各サービスへのオプション的な項目はCSVやBATファイルでの設定が必要となる。これらの処理は年度末、年度始に集中し大変な負担となっていた。これを緩和するため図5に示すように処理スクリプトを作成し、ユーザ登録支援としている。

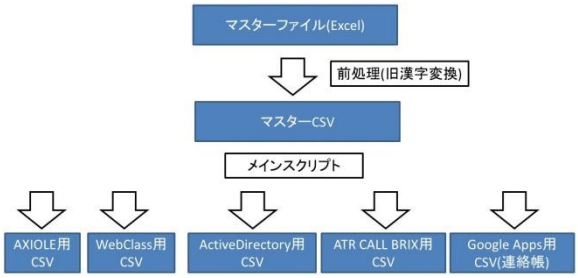

図5 スクリプトによる処理のフローチャート

おわりに

認証基盤を整備することで教育用システムの利便性を大きく高める事を実現した。一つのアカウントで全ての教育用サービスを利用することが可能である。仮想化、クラウドに対応することで機能を高めつつ管理コストを大きく削減している。現在高専機構主導による認証サーバ全高専導入が進められているが、本校教育用システムはその先駆けともいえるものである。

今後の検討課題としてまずパスワード管理ポリシーが挙げられる。また信頼性の高い電子メールの提供を実現したので、今後は学生に電子メールをどれくらいの頻度で利用することを推奨するかを考えていく必要がある。現在急増しているスマートフォンの活用も考慮する必要がある。

参考文献

[1]. 白濱 成希、脇山 正博、桐本 賢太、”教育用システムへのクラウドと仮想化の導入について”、高等専門学校情報処理教育研究発表会論文集第31号、pp217-218、2011

[2]. 一條 博、”LDAPによるネットワークシステム構築(第2版)、工学社、2003

[3]. 青木、後藤、高橋著、まつもと監修、”Rubyレシピブック(第3版)”、ソフトバンク クリエイティブ、2010

（ 2011年11月7日　受理）