Vol.2010-IOT-10 No.4
2010/7/16

システム統合と運用管理に配慮したサーバの仮想化と統合認証系を有する計算機システム

桝田秀夫[†1]　村田和義[†1]　渋谷雄[†1]
若杉耕一郎[†2]　黒江康明[†2]

京都工芸繊維大学の新計算機システム (System8) では，すべてのサーバを仮想化し，物理的に 12 台のサーバで 40 個以上のゲスト OS を稼動させ，上位に冗長化された負荷分散装置を配し，サービス毎に複数のゲスト OS を稼動させることでメンテナンスによる停止を最小化するように工夫した．また，教職員から学生までを統一的に管理する認証系を準備し，Web SSO の 1 つである Shibboleth 認証を導入し，パスワード変更から WebMail，Moodle，情報コンセントの Web 認証といった Web サービスに対して SSO を可能とした．

Campus Computer System that realizes at Service Integration and Low Management Cost by Virtual Machine Technology

Hideo Masuda ,[†1] Kazuyoshi Murata ,[†1]
Yu Shibuya ,[†1] Koichiro Wakasugi [†2]
and Yasuaki Kuroe [†2]

We have replaced our Campus Computer System in this March. Our new system has two new features: (1) All services are running on Virtual Machine (VMware Infrastructure) including DNS, E-Mail, Web, e-Learning, Remote access, File server and Network boot servers. Moreover, each service is provided by more than one guest OS and load balancer, so we are easy to maintain the OS image because the service is still available if one guest OS is shutdown for maintenance. Thus, our system consists of only 12 real servers mounted only 4 racks and over 200 PCs are booted from Network boot servers. (2) All members ' electric Identities are provided from our new system. Moreover, a several systems are shibbolized (Web-based Single Sign On system produced by Internet2) such as changing password, checking own resources, accessing e-Learning system and using network outlets.

1. はじめに

京都工芸繊維大学情報科学センターでは 2006 年 3 月に Windows PC と UNIX サーバによる電子計算機システム (System7) が導入されていた[1)] が，2010 年 3 月に更新時期を迎えた．

本報告では，2010 年 3 月から稼動している新システム (System8) の設計や構成について述べる．新システムは，NEC 社の Express5800/R120a-2 サーバ 14 台と，SAN ストレージの iStorage D8-3010，および Mate タイプ ME (MY30A/E-7) パソコン 216 台などで構成されている．

2. システム更新の目標

2.1 柔軟性のあるシステム構成

大学のネットワークが整備されインターネットとの接続が開始された頃は，研究室や学科といった単位で独自にサーバを構築して，学内外にむけてサービスを提供することが一般的であった．しかし，インターネットが急速に普及し，重要なインフラとして教育・研究活動に利用されるようになり，サービスの継続性が重要となってきた．さらに，インターネットを経由した様々な攻撃は多種多様でかつ頻発しており，高度に専門的な知識を持たなければ容易に侵入され，被害者としてではなく加害者になりかねない情勢となってきており，きちんとした管理が必須となってきている．

また，以前のシステムでは，端末パソコンとして，CAD の稼動の為に必要な高性能パソコンとそれ以外の廉価版パソコンの二系列で構成していたが，演習室の移動や再編により台数の辻褄があわなくなったり，保守が複雑になるといった問題があった．さらに，サーバシステムも，適材適所と考えて 1U のものと 2U のもの，SATA HDD のものと SCSI HDD のものを混在して導入したため，情勢にあわせた運用の再編に柔軟に対応できなかった．

4 年間のレンタル期間において，安定的な運用体制が必要とされるが，セキュリティ対策

†1 京都工芸繊維大学 情報科学センター
Center for Information Science, Kyoto Institute of Technology
†2 京都工芸繊維大学 大学院工芸科学研究科 設計工学系 情報工学部門
Department of Information Science, Graduate School of Science and Technology, Kyoto Institute of Technology

の変化や学内での ICT を使ったサービスの増大に適時に対応できる仕組みも望まれる．

その為には，出来る限りハードウェアの種類を絞り込み，仮想化技術などを用いて，柔軟な再編体制がとれる構成が望ましい．

2.2 クライアント PC の運用管理コストの削減

本学は，学生数 4500 人程度の理系単科大学であるが，以前のシステムでの端末数は管理用を含めて 165 台であり，非常に少ない状態であった．また，演習に利用できる部屋は，端末パソコンが 70 台の部屋と 41 台の部屋の合計 2 つしかなく，課程によっては導入時教育を二回に分けて実施しなければならない場合も発生していた．学内に働きかけることにより，部屋の床面積の追加措置を得ることができたが，管理するスタッフの人数は微減となってしまった．その為，端末パソコン数を単純に増加させても，定常的な更新作業などの管理の手間が削減できる仕組みであることが必須となる．

また，以前のシステムでは，端末パソコンを収容するハブは，非インテリジェント型のハブであったため，ネットワーク障害の検出に問題があった．特に，OS イメージを更新する際に，演習室のパソコンに Multicast などで配信を行うと一部のパソコンで更新に失敗するといった，ネットワークに起因すると思われるトラブルも発生し，少ないスタッフでの運用に不安があった．従って，ネットワーク装置の遠隔管理機能などを用いてできるだけ現地に行かずに問題判別できる機構が望まれる．

さらに，アプリケーションのライセンス料も懸念事項となる．以前のシステムでは，ライセンスサーバによる管理ができるアプリケーションはそれを積極的に採用することにより，演習室 1 つ分のライセンスを確保するだけで演習から自習までの利用が可能であったが，そうではないアプリケーションは，利用できる端末パソコンの場所が限定されたり，必要数以上のライセンスを確保する必要があった．このようなアプリケーションを，必要最低限のライセンス数で運用管理できる仕組みも望まれる．

2.3 電子メールシステムの増強

電子メールは，非常に手軽なプッシュ型の情報伝達手段である．しかしながら，非常に多くの迷惑メールが流通しており，その対応が急務となっている．以前のシステムでは，Greet-Pause や Envelope の DNS 解決確認といった機械的に実行可能な迷惑メール対策[2] は施していたが，それでもかなりの数の迷惑メールが流入してしまっている．また，SpamAssassin のように電子メールの中身にまで踏み込むタイプの迷惑メール対策システムは，プライバシーの観点からも，それぞれ個人の判断を重視するべきであり，さらに誤判定に対する救済手段を設けておく必要がある．従来は，Thunderbird などの MUA での個別対策を依頼していたが，やはりサーバ側での一括対応への期待も強い．そのような個人毎にするべき設定を，管理者を介在させて実施することは，手間が膨大となるため，ツールとして提供する必要がある．

そのような，各種フィルタ処理に対して，個人毎の制御が可能な電子メールシステムが望まれる．

2.4 統合認証システムの導入

さまざまな情報の流通を，ネットワークを介して実施できるようになってきており，とりわけ Web を用いたシステムは非常に多くなってきている．本学でも，財務会計システムや学務履修登録システム，シラバスシステムや事務情報ポータルなど，教育研究だけでなく事務システムも Web 化が進んでいる．これらのシステムへのアクセスは，当然ながら利用者認証が必須であるが，それぞれのシステムが，導入時期も異なり，ばらばらの認証情報を有している状況である．また，本センターの本務は教育研究に関わるものとされており，事務の情報化は別組織 (情報課) が掌握していたため，統一がなされておらず，アカウントも教員と学生はセンターで管理していたが，職員は別となっていた．さらに，教員や学生のアカウント管理も，元となるデータは総務課人事係や学務課が持っており，データのやりとりに手間隙がかかっていた．

そこで，アカウント情報についてはこの垣根を取り払い，本センター側で全学規模の統合認証システムを導入し，すべての構成員を登録可能なシステムとすることとした．その為には，必要な属性を持つアカウントを切り出して提供できる仕組みや，Web システム間でのシングルサインオン (SSO) が可能となる仕組みが求められる．

さらに，広範囲のシステムで利用可能なアカウントになれば，そのアカウントの重要性は飛躍的に高まる．その為の利用者教育の充実も必須な要求となる．

3. システムの構成

3.1 負荷分散+仮想化システムの活用

図 1 は，新しいシステムのサーバシステム群の概要である．サーバはすべて VMware Infrastructure 上で仮想化されており，さらにメールや DNS などのサービス毎に別々の物理サーバに跨った複数のゲスト OS による冗長化構成となっている．物理サーバのサイジングとしては，センターとして提供するサービスについては，1 つの論理サーバに 64bit CPU を 2 コア以上と 4Gbyte 以上のメモリを割り当てられることを仕様書でうたい，Quad Core の Intel 社 Xeon X5570 を 2 つ搭載した物理サーバにメインメモリを 32GByte 搭載したも

Vol.2010-IOT-10 No.4
2010/7/16

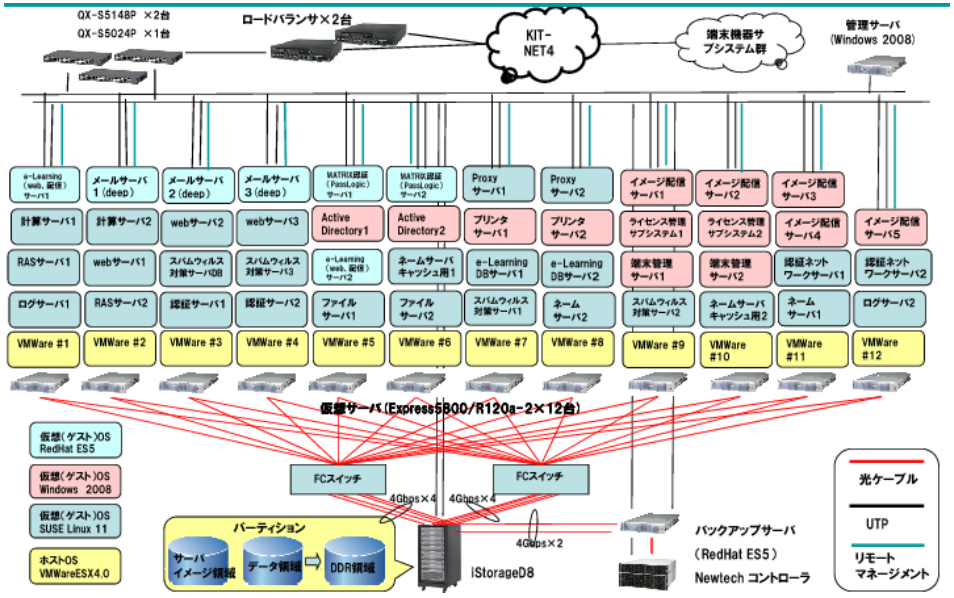

図 1 システム構成概略図

のを合計 12 台で構成している．

サーバ OS としては，基本的に Novell 社の SUSE Linux Enterprise Server[6] を採用した．これは，SUSE Linux が，ライセンス (サポート) 体制として，物理サーバ 1 台あたりで規定されておりゲスト OS の数に依存しないため，仮想化環境で多数のゲスト OS を稼動させる場合に好都合であったからである．ただし，稼動させるサービスの都合上，Windows Server や Red Hat Enterprise Linux Server も導入している．

また，複数のゲスト OS 上で稼動するサービスは，上位に負荷分散冗長化装置として A10 Networks 社の AX2200 を経由させることで，あるゲスト OS が停止してもサービスを継続できるようになっている．AX2200 自体も二重化しており，サービスの停止時間の極小化をはかっている．

さらに，すべての物理サーバは，異なる FC スイッチを経由する複数のパスで iStorage D8 に Fibre Channel で接続されており，ゲスト OS をどの物理サーバ上で動かすことも可能としている．iStorage D8 は，300GByte の SAS HDD を 80 個と 1TByte の SATA HDD を 10 個を装備している．この HDD 群を，常用領域は SAS HDD を RAID1+0 で構成した約 10TByte の領域とし，SATA HDD は RAID6 で構成して DDR (Dynamic Data Replication) 機能用の領域とすることにより，ランダムアクセスの高性能化とサーバフリーバックアップが可能となっている．

これらの仕組みにより，ゲスト OS 単位でのメンテナンスによるサービスの中断を最小限にすることが可能となり，また，物理サーバ自体の障害に対しても，他の物理サーバ上のゲスト OS がバックアップすることができ， 場合によっては別の物理サーバ上でゲスト OS を再稼働させることも可能となる．

さらに，運用中にサービスの追加が必要になった場合でも，仮想化技術を用いているので，物理サーバの数に大きく制限されることなく，リソースの割当の見直しをするだけで追加が容易となる．

表 1 主要アプリケーション

オフィススイート	Microsoft Office 2007 Professional , OpenOffice.org 3.2
CAD	Pro/ENGINEERING
図画処理	Adobe Illustrator CS2 , Adobe Photoshop Elements 7
数式処理	Mathematica
ウィルス対策	Symmantec Protection Suite Enterprise
データ解析	gnuplot, Octave, SciLab
開発環境	Eclipse, Java6 SDK
文書処理	日本語 pLaTeX
端末エミュレータ	putty
Web ブラウザ	Internet Explorer 7, Firefox3
メーラ	Thunderbird3
PDF	Adobe Reader, PrimoPDF, PDFCreator
メディアプレイヤ	Windows Media Player, Adobe Flash Player, Real Player, Quick Time, iTunes

3.2 ネットワークブートとネットワーク装置

端末パソコンは，すべて共通仕様とし，Intel-VT に対応した Core2Duo E8400 (3GHz) と 4GByte のメモリ，80GByte の HDD を持つ機種で統一した上で，Windows Vista (SP2) Bussiness [*1]を Citrix Provisioning Server (旧 Ardence)[7] と呼ばれるネットワークブートシステム上で稼動させている．さらに，ReadCache[8] と呼ばれる仕組みを併せて採用することにより，ローカルディスクをキャッシュとして利用し，ネットワークやブートサーバへの負荷を軽減するようにしている．表 1 は，導入している主要アプリケーションのリストで

⋆1 調達時期が 2009 年 10 月落札というタイミングであったため，Windows7 はぎりぎり間に合わなかった．

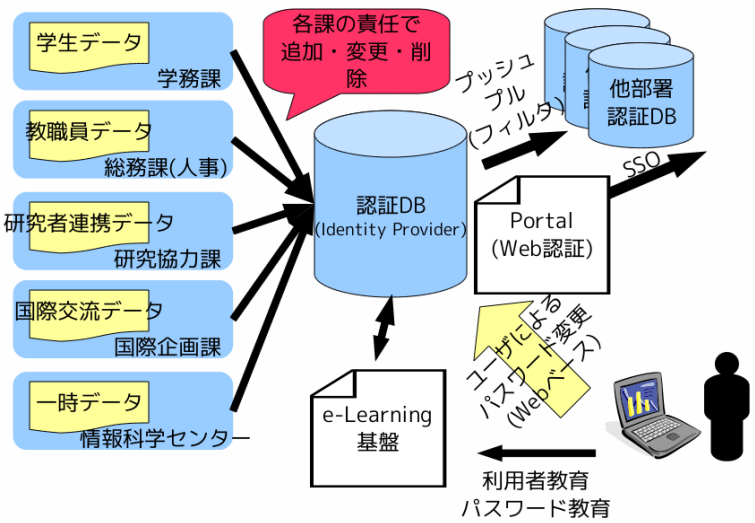

図 2 認証システムの考え方

ある．

また，OpenSUSE Linux 11.1 をディスクレス稼動できる仕組みも準備しており，デュアルブートとしている．このディスクレスシステムは，文献[3] を参考として構築している．

端末パソコンは，情報科学センター演習室 (70 台)，情報科学センター自習室 (25 台)，5 号館情報科学演習室 (71 台)，図書館 1F (24 台)，図書館 3F (10 台)，就職資料室 (5 台)，学務課ロビー (5 台)，管理室 (6 台) と 8 箇所に分散配置している．これらのネットワーク接続については，昨年度に導入した本学情報ネットワークインフラである KITnet4[4] の装置に直収することを基本とした．ただし，部局スイッチから離れている 5 号館の演習室のみは，4 本の 1000baseT をリンクアグリゲーションした 48 ポートのマネジメント機能付きスイッチ (2 台) を経由して収容している．特に今回のシステムではネットワークブートを採用しているので，端末毎の稼動状況やリンクの状態について統計情報の入手や遠隔監視が可能となっていることは重要な要件であったと考えている．

3.3 分散管理が可能な統合認証システム

本学では，各構成員の属性によって，その管理の掌握部署が異なっている．学生は学務課，教員は総務課，留学生は国際企画課，共同研究者は研究協力課と分散している．どのような条件であればアカウントを発行するのかといったポリシーも明確化されていなかったので，その整理を実施した上で，各課が掌握している「人」に対して責任を持って管理できる機能を持たせた．

また，以前のシステムでは，教員と学生のみを全員登録し，それ以外については，「研究目的利用者」として随時登録としていたが，一部の事務職員を登録していたり，来訪者などの一時的にしか利用しない利用者など，多様な利用者を登録する必要が多くなってきた．さらに，全学生のアカウントを管理している唯一のデータベースとなっていたので，履修登録システムなどへの活用が期待されていた．

そこで，教職員と学生のすべての構成員を登録したデータベースとして統合認証システムを構築し，学内の必要な箇所に，必要な属性のアカウントのみ提供できるようにした (図 2)．また，LDAP, RADIUS, Windows Active Directory の認証サービスも提供している．これにより，学内のすべての構成員を電子的に認証できる基盤となることができた．

3.4 初期教育と利用サービスの選択

今回のシステムでは，利用者は，本センターのアカウントを保有すれば，Windows パソコン，e-Learning システム，電子メール，オンデマンド印刷，情報コンセント，遠隔計算サービス，リモートアクセス，が利用可能となる．アカウントの配布をスムースにする為に，新規の利用者の情報が入手できたタイミングですべてのアカウントを作成しシステムに登録している．しかしながら，すべての利用者がアカウントを受領してから，すぐに使用するとは限らないし，すべてのサービスを使うとも限らない．さらに，通常，大学組織として利用規程などを提供しており，利用者にはそれに同意させてから使用させるべきではあるが，単純に規程の文書を一緒に配布するだけでは実効性に欠ける．

そこで，本システムでは配布時に使用できるサービスは最低限とし，その後 e-Learning システムでアカウントの利用方法に関するコンテンツを参照した上でオンラインテストを受講させて，合格した場合にのみ，他の各種サービスを有効化できる，という仕組みを導入した (図 3)．オンラインテストは，本学で以前から利用している Moodle[5] を用い，特定のコース内の小テストへの合格をもって判定するようになっている．これにより，オンラインテストに合格できる程度には教育ができていることが担保でき，また利用者が積極的に有効にしないサービスは無効化の状態のままとなるので，不正利用の心配を軽減できている．

3.5 パスワード再発行手続き

全構成員にアカウントを配布すれば，パスワードの再発行要求もそれなりの数で発生することは避けられない．組織によっては，パスワードの再発行に対して課金するといった対応

図 3 利用者認証ポータルの例

も取られているが，金銭のやりとりは，やはり国立大学法人になったとは言えハードルが高い．

そこで，教育的な観点を重視し，パスワード再発行手続きに際して，再発行の理由に加えて再発防止策を記述させることで，安易に再発行することに頼ることなく，本人に自覚を促すように工夫している．再発行を繰り返した場合は，センター教員による直接指導なども規定している．

3.6 Shibboleth SSO

Shibboleth[9] とは，Internet2 で開発されている，認証フェデレーション技術である．Shibboleth は，Identity Provider(IdP) と Service Provider(SP) から構成され，IdP で認証された利用者は，IdP から属性情報を入手することができ，その後 SP にアクセスした際に，その属性情報を元に認可が行える．

この技術により，認証作業を IdP に一元化することが可能となり，Single Sign On が実現できる．現時点では，パスワード変更，利用サービス登録，Web メール，Moodle (e-Learning システム)，情報コンセント利用者認証については，Shibboleth 対応ができている．

3.7 統合電子メールシステム

電子メールシステムには，DEEPSoft 社の DEEPMail を採用している．DEEPMail は，Linux, FreeBSD, Solaris などの UNIX 系 OS 上で動作するアプリケーションであり，今回のような仮想化環境に導入することに都合が良い．これにより，IMAP4，POP3，WebMail のいずれでもメールボックスにアクセスできることや，SPAMBlock や AntiVirus システム (Sophos 社 Pure Message) との連携もはかれている．IMAP4, POP3, SMTP, WebMail は，すべて独立した SSL 証明書による通信路暗号化を施している．SSL 処理は AX2200 にオフロードし，また，証明書は，NII の証明書自動発行検証プロジェクト[10] のものを利用させて戴いている．さらに，SPAMBlock に関しては，利用者によって有効にするまでは機能しないように初期設定をすることで，利用者が明示的に判断できる余地を盛り込んでいる．

4. 現在の運用状況と考察

4.1 消 費 電 力

仮想化計算機システムを採用する理由として，システムの負荷を集約して機器数を減らすことから消費電力の低減できることが挙げられている．今回のシステムでも，以前のシステムでは 35 台のサーバ計算機があったが，14 台のサーバ計算機[*1] に台数を集約することができており，設置面積もラック 6 個分から 4 個分に減少している．

表 2 は，前システム (System7) と現システム (System8) で，分電盤のブレーカ付近に AC クランプメータを挿入し，電流を測定した結果である．電流値は変動があるが，目視で概ね中央値を記録した．端末 PC は，ログオン待ち状態を平常時，ブート時のピーク電流を最大として記録している．

消費電流を単純に電力と考えれば，サーバに関しては約 22%の増大，ということになる．しかしながら，今回のシステムではネットワークブートサーバ，Web メールシステム，仮想サーバシステムなどが増強されていることや，すべてのサービスに付いて，複数のサーバインスタンスを稼動させているため，単純な比較はできない．もし以前のシステムで同様の冗長性 (二重化) を提供するとすれば，35 台のうち約 20 台分の機器が必要になると考えられ，単純な消費電流の比較では約 1.6 倍となり，機能に対しては省電力化がはかれていると

⋆1 1 台はコンソール処理専用，1 台は外部バックアップ装置である．

表 2 前システムと現システムの電力消費量比較

システム	サーバ (全ラック合計値)	端末 PC+モニタ 平常時 / 最大
System7	69.2 A	0.8 A / 1.5 A (x 165 台)
System8	84.2 A	0.8 A / 1.1 A (x 216 台)

も考えられなくはない.

4.2 起動時間

今回のシステムでは，端末パソコンをネットワークブートで運用している．仮想化計算機システムは I/O 性能が低下すると言われているため，当初はブートサーバは非仮想化環境で稼動させることも検討していた．しかし，実際には仮想化環境のブートサーバであっても，端末パソコンの起動時間は POST (Power On Self Test) を含めても概ね 2 分程度であり，70 台同時起動だとしても 2 分半程度で起動する．これは，ReadCache などのブートサーバの負荷軽減の為のシステムを導入したこともあるが，SAN ストレージに比較的小さな容量の HDD を配し，さらに RAID1+0 構成とすることで，ランダムアクセス時の実効性能に配慮したことと，仮想化ソフトウェア自体の改善が行われていることなどが挙げられると考えられる.

4.3 利用者属性の整理

3.3 節で述べた通り，今回の統合認証システムは，人の情報を管理している”発生源”での入力・更新を想定して構築したが，現在のところ，本システムがすべての情報のマスターデータになるところまでは進め切れておらず，あくまでも各掌握部署が持っている情報を変換して投入する，という運用となっている．また，事務の作業手順上の問題もあり，どうしてもデータの更新遅れが発生してしまうが，現在，事務の業務改善と共に検討しつつある.

また，今回のシステムでは，まずは学内 Web サービスの SSO を想定して Shibboleth IdP を構築した．Shibboleth を採用したことにより，UPKI の学術認証フェデレーション (Gakunin)[11] への参加が期待される．しかしながら，当初の IdP の構築方法の事情により現時点ではすぐには参加できない状況にある．この Gakunin への参加に向けて，利用者属性の整理などを進めることが現在の課題である.

5. おわりに

本稿では，本学の電子計算機システムの更新にあたっての，システムの設計方針や構成について述べ，現状について報告した．サーバシステムを仮想化環境で動作させることや，クライアント PC を統一し，ネットワークブートで稼動させること，さらに統合認証システムにより認証情報の統一化を実現したことなどによる運用コストの削減に注力した.

今後，システムの継続的な運用を続け，発生した問題点を検討・解決し，安定したシステムに向けて改善を続けていく必要があると考えている.

参考文献

1) 桝田 秀夫, 黒江 康明, 若杉 耕一郎: 京都工芸繊維大学における情報教育システムについて, 平成 18 年度情報教育研究集会, pp.537-540 (2006).
2) 岡田 哲治, 桝田 秀夫: Postfix を使った簡易 spam メール対策, 第 20 回情報処理センター等担当者技術研究会 (2008).
3) 桝田 秀夫, 小川 剛史, 町田 貴史, 中澤 篤志, 清川 清, 竹村 治雄 : Diskless Linux を用いた情報教育システムの開発とその評価, 情報処理学会論文誌, Vol.49 No.3 pp.1239-1248 (2008).
4) 桝田 秀夫, 村田 和義, 渋谷 雄: 京都工芸繊維大学における 10Gbps ネットワークインフラの導入について, 情報処理学会 IOT 研究会, IOT6-4 (2009).
5) 桝田 秀夫, 村田 和義, 渋谷 雄: 京都工芸繊維大学における Moodle パイロットシステムについて, 平成 20 年度情報教育研究集会, pp.307-310 (2008).
6) Novell : SUSE Linux Enterprise Server, http://www.novell.com/ja-jp/products/server/.
7) Citrix: Citrix Provisioning Server (PVS), http://www.citrix.co.jp/products/cpros/.
8) CO-CONV: ReadCache システム, http://www.co-conv.jp/product/readcache/.
9) Shibboleth, http://shibboleth.internet2.edu/.
10) UPKI イニシアティブ: UPKI オープンドメイン証明書自動発行検証プロジェクト, https://upki-portal.nii.ac.jp/docs/odcert.
11) UPKI イニシアティブ: 学術認証フェデレーション, https://upki-portal.nii.ac.jp/docs/fed.