

基幹サービスのデータセンターでの運用について

秋山 剛志

京都教育大学 情報処理センター

akiyama@kyokyo-u.ac.jp

概要：大学にとって電子メールや Web サービスの重要性が高くなってきている。地震や台風などの災害発生時に電子メールや Web サービスが情報発信・連絡ツールとして重要な役割を果たすことがわかったため、これらのサービスを災害時に継続運用する必要性が高まった。小規模大学においては、大学内で非常用発電設備など情報システムのサービスを継続運用させるための設備を備えることは費用的に難しい。そこで本学では電子メールや Web サービスなどの基幹サービスサーバを商用データセンターへ移設し「Kyo2 Cloud Center」として平成 23 年 9 月より運用を始めた。本稿ではデータセンターでの運用を開始した背景や実際の運用状況について述べる。

1 はじめに

ネットワーク環境や IT 機器の発達により電子メールが就職活動やレポートの提出などに使われるようになり、大学から外部に情報を発信するツールとして Web サービスが使われるようになってきた。2011 年 3 月 11 日に発生した東日本大震災において、固定電話や携帯電話での通話が制限される中、電子メールや Web, SNS といったインターネットを使用したサービスが連絡ツールとして活躍した^[1]。これによって災害発生時におけるインターネットを使用したサービスの有効性が証明されたのである。このような状況から電子メールや Web サービスの重要性が高くなってきた。

本学では、平成 20 年より学舎の耐震改修工事が行われ情報処理センターの停電が頻繁に発生した。耐震改修工事終了後も 1 年間に数日は電源工事や設備点検のため停電が発生している。電子メールや Web サービス用のサーバには瞬停対策の UPS を備えているが、自家発電設備がないため 5 分以上の停電には対応できない。そのため計画停電のたびに全サーバとネットワークをシャットダウンしていたが、シャットダウン・起動作業だけで 3 時間以上の時間が必要であった。電子メールについては、送信元サーバで SPAM 対策のため再送回数を少なく設定しているものもありシステム停止中に送信された電子メールが受信できない事態が発生した。そのため、停電によるシステム停止が発生するたびに学内から停電時でも電子メールや Web などのシステムを停止しないようにしてほしいとの要望が多数寄せられるようになった。

これらの要望を受けて停電時の継続運用を行うため、情報処理センターを中心に施設課と相談し自家発電設備の導入を検討した。しかし、電子メールや Web サービスに必要なサーバとネットワーク機器には約 7kVA の電力が必要となり、その容量を賄う自家発電設備を設置するには多額の設置費用とメンテナンス費用が必要となる。また、停電が発生してから発電機を起動し電力を安定供給できるまで約 5 分程度の時間が必要となる。(導入を検討したディーゼル式発電機の場合、短時間で安定供給可能なものもあるが価格が高額である。) 発電機からの電力が安定するまでは UPS により電力供給しなければならないが、瞬停対策に導入している UPS では 5 分間供給することが難しい。そのため、自家発電設備の導入については見送ることとなった。

次に商用データセンターサービスの利用について検討した。これまで商用データセンターサービスの利用については(1)大学データセンター間に高速なネットワークが必要、(2)学外にメールや認証情報などのデータを置くことに対しセキュリティ的な面での懸念、(3)データセンターの利用料金が高額などの理由により小規模な大学では導入が困難であった。しかし、静岡大学の「SUCCES」におけるプライベートクラウド事例^[2]や国立情報学研究所の学術情報ネットワーク(SINET4)を利用することによりネットワーク費用を抑えられる等、データセンターでの運用について環境が整ってきた。

2 データセンターでの運用検討

ネットワーク環境や仮想化技術の発達によりサーバの運用形態は多様化している。その中でも近年増加しているのがクラウドサービスである。クラウドサービスには SaaS や PaaS 等クラウド環境でサービスを提供するパブリッククラウドと自機関で構築したクラウド環境を利用するプライベートクラウドある。静岡大学の「SUCCES」ではパブリッククラウドとプライベートクラウドを様々な面から分析しサービスにあわせた使い分けをしている。^[3] 本学では仮想化サーバを使用したプライベートクラウド環境を構築し、データセンターで運用することを検討した。

2.1 BCP の観点から見た運用

BCP（事業継続計画）とは「事業中断の原因となるさまざまなリスクを想定し、これらを未然に回避、あるいは被害を受けても速やかに復旧できるように方針や行動手順」^[4]のことである。一般企業や自治体では策定されていることが多いが、大学などの教育機関で策定されているところは少ない。近年、教育機関においても一般企業と同様に事業の継続性を求められることが多くなった。これは災害発生時に学生の安否確認や被災学生に対するケアなど教育機関として学生に対するサービスが重要視されるようになったためである。

現時点で本学に規定された事業継続計画はなく、国立大学法人京都教育大学危機管理規定^[5]によると学内に危機管理委員会を置き「教職員・学生並びに近隣住民の安全確保を図るとともに本学の社会的な責任を果たす」ためガイドラインやマニュアルの策定を行うと規定されている。しかし、ガイドラインやマニュアルの整備は遅れているのが現状である。

想定されるリスクとして地震・雷・水害・台風・火災・テロ・事故・パンデミックなどの状況が考えられる。

商用データセンターではこのような事態に対し対応できるような対策を講じている。例えば地震が発生した場合、耐震や免震構造によって強い揺れから建物を守り、停電時には非常用バッテリーと自家発電設備により商用電源停止時にも電力の供給を可能としている。また、台風やゲリラ豪雨などで発生する水害対策として基礎部分を高く設置することにより建物内に水が浸入しないように建設

されていることが多い。

災害発生時において電子データの保護は重要である。富士通株式会社が 2010 年に行った災害対策キャンペーンアンケート（有効回答数 4667、対象は富士通製品を使用中の企業・自治体・教育研究機関など）^[6]によるとデータのバックアップを日常的に取得している機関は 93%に対しバックアップデータを遠隔地等の 2 拠点で分散している機関は 29%にとどまった。また、システム拠点を分散している機関は 20%のみであった。この結果より 7 割程度の機関がバックアップの取得は行っているが、オンプレミス運用を行っているため拠点にダメージを受けてバックアップデータが損失すると事業の継続が難しくなるのである。これらのことから様々なリスクへの対策を講じているデータセンターへシステムを分散配置することは BCP の有効な手段である。

2.2 セキュリティの観点から見た運用

大学には学生の成績データやメールアドレスなど様々な個人情報が保管されており厳重に管理されている。電子化されたデータも多数あり情報漏洩の防止が重要課題となっている。

電子データが漏洩する原因として次のものが考えられる。

- (1) 内部の人間が故意に外部へ流出させる
- (2) 内部の人間が自宅など別の場所へデータを移動させ、移動させたデータが流出する
- (3) ネットワークを経由し外部から侵入されてデータを盗まれる
- (4) 保管場所に侵入されてデータを保存している媒体もしくは機械を盗まれる

(1)と(2)については、適切なアクセス権限の設定やセキュリティ講習・セキュリティポリシーなどの対策が必要である。また、(2)についてはデータの持ち出し制限だけでなく VDI（Virtual Desktop Infrastructure）の利用によってデータそのものを持ち出せないようにすることによりリスクを軽減することができる。(3)についてもファイアウォールや侵入検知システムなどの整備、セキュリティホールのパッチ適応などを適切に行うことやネットワークに不正な端末を接続させない対策が必要となる。(4)については保管している部屋の入退室管理や施錠、防犯カメラの設置などが必要となる。

本学のサーバ室には監視カメラ等はなく建物

は日中解錠されており誰でも入館が可能である。サーバ室にはテンキー式の電気錠が備えられており常時施錠されている。また、事務電算用サーバ室は事務局内に設けられており日中建屋の施錠はされていない。サーバ室には録画はされていないが監視カメラが設置されている。サーバ室は常時施錠されているが1階に設置されており道路に面して窓があるため侵入される可能性がある。一方、データセンターでは身分証の確認を徹底するなどの他に生体認証を使用し部外者の侵入を防止している。さらにPCや携帯電話の持ち込み制限を行っておりデータを持ち出すことは不可能となっている。また、館内には防犯カメラが設置されており常時警備員による監視と録画行われている。サーバ室には窓もなく外部から侵入できないように対策されている。

2.3 学生サービスの観点から見た運用

ネットワーク環境やPC・携帯電話・スマートフォンに普及により多くの学生がSNSや電子メール・Webなどのサービスを利用している。これらのサービスは災害発生時にも非常に有効である。本学では東日本大震災の際に電子メールを使用し全教職員と学生に対して被災状況の確認を実施した。このように大地震や大水害などの災害が発生し交通手段に支障が出た場合、電子メールによって安否確認や連絡事項の伝達、大学からの情報提供、長期にわたって通学に支障がでる場合は遠隔講義システムを利用した授業の実施などが考えられる。

学生生活において、大学の電子メールアドレスは授業の課題提出、就職活動、クラブ活動の連絡などに使用され欠かせないものとなっている。教職員にとっても他の教職員や学会・学生との連絡手段として使用されている。大学のWebでは、大学案内だけでなく財務諸表などの公開情報、受験の情報、公開講座や講演会のお知らせなど様々な情報が公開されている。また、教務システムではシラバスや休講情報を携帯電話や自宅のPCから確認することもでき、設定をすれば登録している授業が休講になった際に電子メールで通知するサービスもある。これらのことから学生生活全般において電子メール・Webサービスは重要なものであり、継続的な運用が必要なことがわかる。

3 データセンターでの運用

データセンターで運用を開始するにあたり長期間にわたってシステムが停止しないようシステムの設計を行った。2011年9月に京都の藤森キャンパスから直線距離で約360km離れた商用データセンターに「Kyo2 Cloud Center」を開設した。図1にデータセンターの外観図を示す。



図1 データセンター外観図（富士通株式会社提供）

このデータセンターは弾性すべり支承と積層ゴムを使用した免震構造となっており阪神大震災・新潟県中越沖地震クラスの地震にも耐えられるよう設計されている。また、大容量のUPSとガスタービン式発電機2基を設置している。これらの設備により停電が発生しても備蓄している燃料で3日間は運用が可能となっている。また、受電設備も変電所の異なる2系統で受電しているため変電所でのトラブルにも対応が可能となっている。このデータセンターでは、品質マネジメントのISO9001、環境マネジメントのISO14001、ITサービスマネジメントのISO20000、情報セキュリティマネジメントのISO27001を取得している。

火災への対策として図2のようにサーバ室には窒素ガス消火設備や超高感度煙センサを備え万が一火災が発生した場合でも即座に対応できるようになっている。



図2 火災への対策（富士通株式会社提供）

今回はラック 1 台に 100V 6kVA の電源容量で契約を行っている。図 3 に Kyo2 Cloud Center の全景を示す。

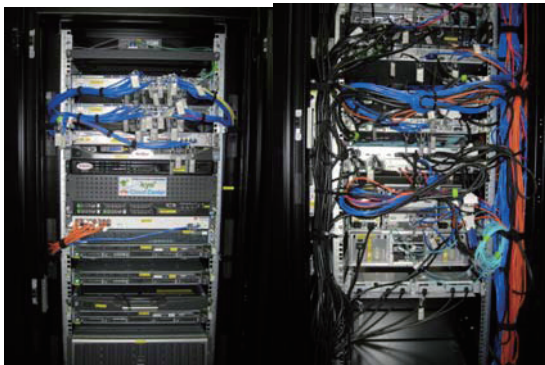


図 3 Kyo2 Cloud Center

3.1 データセンターで運用するサービス

費用の問題から最低限 Web と電子メール (Webmail 含む) のサービスが継続できるように学外・学内向け Web サーバ, メールサーバ, Webmail サーバ, SPAM 対策サーバ, 学外・学内向け DNS サーバ, ファイアウォールサーバ, VPN サーバ, LDAP 認証サーバをデータセンターへ移行した。2010 年に行ったシステムリプレースの際に仮想化を行い物理サーバの台数を減らしていたため, 情報処理センターのサーバ室で運用していた物理サーバ 4 台とファイルサーバ 1 台を移設することにより Web と電子メールサービスをデータセンター運用へ移行することができた。表 1 に移設した機器の一覧を示す。

機種名	消費電力	重量	備考
Fujitsu SPARC ENTERPRISE T5140	769W	18kg	外部DNS, 外部Web
Fujitsu SPARC ENTERPRISE T5140	769W	18kg	WebMailサーバ
Fujitsu SPARC ENTERPRISE T5140	769W	18kg	内部DNS, SMTP, 認証, 内部Web
McAfee EWS3300	670W	20kg	SPAM対策装置(アプライアンス)
McAfee EWS3300	670W	20kg	SPAM対策装置予備(アプライアンス)
Fujitsu ETERNUS NR1000F2040	436W	27kg	NAS(CIFSおよびNFS)
Fujitsu ETERNUS DS14Mk2	440W	37kg	NAS用ディスクシェルフ
Fujitsu PRIMERGY RX200S5	604W	19.6kg	NAS用ウイルスチェックサーバ
Checkpoint IP390G	162W	10.9kg	ファイアウォール

表 1 移設機器一覧

ネットワーク機器については Cisco 社 Catalyst3750X を新規購入し 10Gbps のネットワークに対応している。(現時点では 1Gbps で使用) 表 2 に新規購入した機器の一覧を示す。

機種名	消費電力	重量	備考
Cisco Catalyst3750X	98.7W	7kg	L3スイッチ
Cisco Catalyst3750X	98.7W	7kg	L3スイッチ
Cisco ASA5510	190W	9.7kg	VPNサーバ
Netgear CM4116	20W	5kg	シリアルコンソールサーバ
APC RackmountPDU	-	-	Switched PDU

表 2 購入機器一覧

メールデータと Webmail のアドレス帳や個人設定などはデータセンターに設置したファイルサーバに保存されている。データセンターには大学と接続するネットワーク以外にインターネットへ接続をしている。Web およびメールに必要なシステムをすべてデータセンター内で運用しているため, 大学のキャンパスとデータセンターの距離が離れていることによる遅延によってサービスが遅くなるといった影響はでていない。

3.2 ネットワーク

データセンターで運用するためには大学のキャンパスとの間を高速なネットワークで接続する必要がある。通常は専用回線を使用して接続するが 1Gbps の専用線を長距離借用すると利用料が高額になる。今回は回線費用を抑えるために SINET4 の L2VPN サービスを利用した。これは各拠点最寄りの SINET アクセスポイント同士で L2VPN によるトンネリングを行いプライベートなネットワークを構築するものである。これを利用することにより藤森キャンパス側の回線は既存の回線が使用できるため, データセンターと SINET アクセスポイント間の回線を用意するだけでデータセンターとキャンパスの間を接続することができた。図 4 にネットワーク構成を示す。

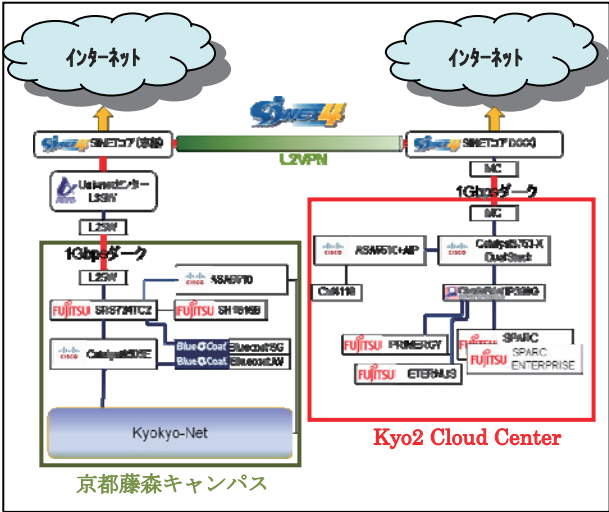


図 4 ネットワーク構成

データセンター側からインターネットへアクセスできるようにルータを設置しているため, 藤森キャンパス・データセンターどちらで障害が発生してもサービスが継続できるようにしている。

3.3 障害に対する対策

データセンターでは大型の空調機でサーバ室の温度管理を行っている。サーバラックには各所に温度センサが取り付けられており常時温度の監視がされている。また、省エネ効率を上げるため図5に示すようにサーバ室の熱・風量・風流を測定分析し空調効率を最適化している。

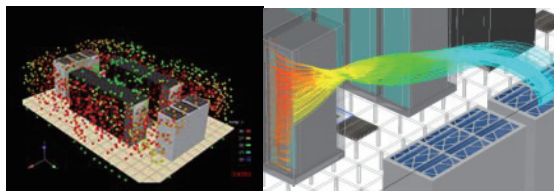


図5 空調の最適化の分析例 (富士通株式会社提供)

サーバは、搭載されている監視ボードにより監視され、ハードウェア障害が発生した場合には電子メールで通知されるように設定している。データセンターにはサーバの保守部品とCEが常駐しており障害発生時に即時対応が可能な体制となっている。

ネットワーク機器やファイアウォールサーバなどのアプライアンスサーバについてはハードウェアの監視機能を備えていない。そのため、これらの機器に障害が発生した場合は予備機に切り替えて運用を行う。また、現地に行かなくてもリモートから電源の投入・切斷・再起動操作が行えるようにAPC社のSwitched Rackmount PDUを使用している。これはネットワーク経由で各コンセント単位の通電状態を制御できる。一部機器についてはシリアル通信による設定変更が必要なため、それらの機器についてはOpengear社のシリアルコンソールサーバを接続している。

3.4 セキュリティ対策

このデータセンターはI.S.Rating社のセキュリティ評価で最高評価となるAAAisを取得している。入館には事前申請が必要となり受付で対面による本人確認を行っている。また、サーバ室の建屋に入館するためには金属探知機を通り館内数ヶ所に設置してある生体認証によって開閉される扉を通過しなければならない。サーバ室前室は図6に示すように入室用と退室用の部屋が分かれており入館時に渡されるRFIDと画像センサによって人数を確認し全員の生体認証が完了するまでサーバ室側のドアが開閉しないようになっている。

また、このRFIDタグにより館内で位置情報を管理し許可されていない場所に侵入できないようになっている。

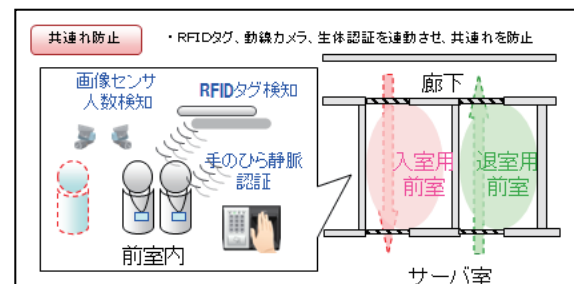


図6 RFID および生体認証 (富士通株式会社提供)

機器を搭載しているラックは電気錠によって施錠されており解錠には生体認証が必要となる。ラックの施錠状態はデータセンターのサーバにて集中管理されており、あらかじめ登録されたラックのみ解錠できるようになっている。これらの設備で不正侵入やデータの流出を防止している。

ネットワークについては、藤森キャンパスとL2VPNによってプライベートなネットワークを構築している。データセンターに設置していても学内LANと同等のネットワークであるため、外部に通信内容が漏れることはない。外部ネットワークとの間にはファイアウォールを設置しセグメントを分割しているため外部から侵入されるリスクは低くなっている。

3.5 バックアップ

本学では2010年2月のシステム更新よりテープ装置によるバックアップを廃止し、ファイルサーバへバックアップを取得するように変更した。これはサーバのディスク容量が増加しバックアップするためのテープ装置とテープの費用が高額になるためである。ファイルサーバを2台使用し2台の間でデータを同期することによりバックアップしている。

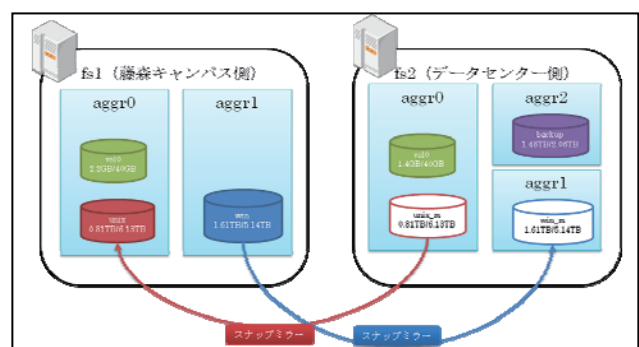


図7 バックアップ構成

藤森キャンパスに設置している Windows サーバは、藤森キャンパスに設置しているファイルサーバに 1 週間に 1 回フルバックアップを取得し、ファールサーバの同期機能によってデータセンターのファイルサーバへバックアップしている。UNIX サーバについては、直接データセンターに設置しているファイルサーバへ 1 週間に 1 回のフルバックアップを行っている。

4 まとめ

データセンターでの運用が開始され、電子メール・Web サービスは藤森キャンパスが停電しても無停止で運用することが可能となった。また、災害発生時でも災害に強いデータセンターとの分散配置とバックアップデータの分散化によってサービスを継続することが可能となり、電子メールを利用した安否確認や Web を通した情報提供など重要な役割を果たすことができるようになった。

今回は、電子メールと Web の基幹サービスを行うサーバのみをデータセンターに移設し運用を行っている。データセンターでの運用について運用体制やパフォーマンスなどの検証を行いサービスの安定稼働と最適化を行っていく。また、他のサーバについてもサービスの内容と重要度を検証し、データセンターでの運用について検討を進める。データセンターとインターネット・藤森キャンパスを結ぶ回線について、現在は 1 回線しかなく回線に障害が発生した場合はサービスが停止してしまう。そのためバックアップ回線の検討が今後の課題となる。

現在のデータセンターはコロケーション契約のため、運用・監視についてはすべて藤森キャンパスにて行っている。そのため、情報処理センターでの業務量は減少しなかった。今後、運用の状況を検証し、監視業務の委託や SaaS, DaaS, PaaS, IaaS（今回導入したデータセンターで IaaS サービスを行っているためネットワークを接続するだけで学内 LAN への接続が可能）サービスを利用するなどパブリッククラウドの導入と運用業務の軽減をはかるための検討を行う。

参考文献

- [1] 齊藤貴之ほか, 「IT で実現する震災・省電力 BCP 完全ガイド システム視点で事業継続計画を見直す」, pp.44-45, 日経 BP 社, 2011
- [2] 静岡大学情報基盤センター, 「静岡大学情報基盤センター広報 Vol.1」, pp.21-27, 静岡大学情報基盤センター, 2009
- [3] クラウドコンピューティング研究会, 「進化するクラウド情報基盤 静岡大学クラウド情報基盤稼働 1 年間の実績と評価」, pp.77-82, 静岡学術出版, 2011
- [4] 昆正和, 「実践 BCP 策定マニュアルー事業継続マネジメントの基礎」, p.16, オーム社, 2009
- [5] 京都教育大学, 「国立大学法人京都教育大学危機管理規定」, pp1-2, 京都教育大学, 2007
- [6] 富士通株式会社, 「お客様の中枢をになう情報システムを災害から守る」, pp28-36, 富士通株式会社, 2011