# 分散キャンパスを利用したファイルバックアップシステム

# File backup system taking advantage of remotely distributed campuses

野口 宏 †, 大瀧 保広 †, 鎌田 賢 †‡

Hiroshi NOGUCHI†, Yasuhiro OHTAKI†, Masaru KAMADA†‡

noguchi@mx.ibaraki.ac.jp, y.ohtaki@mx.ibaraki.ac.jp, m.kamada@mx.ibaraki.ac.jp

茨城大学 IT 基盤センター †
茨城大学 工学部 ‡
Center for Information Technology, Ibaraki University†
Faculty of Engineering, Ibaraki University‡

概要

東日本大震災において，茨城大学では人的な被害や ICT 機器自体には大きな被害が無かったものの，停電と建物内立ち入り禁止が長時間に渡り続いた．同規模の地震への対策を考える時、今回の震災でも懸念された建物倒壊という事態を想定しておく必要がある．本学では分散キャンパス構成になっているため，一つのキャンパスにおいて建物倒壊が起こったとしても，他のキャンパスの建物も同時に倒壊する可能性は低いと考えられる．そこで一般には通信・運営コストの面で不利な分散キャンパスという立地を逆手にとって，ファイルシステムのバックアップをほぼリアルタイムで他キャンパス相互に配置する分散バックアップシステムを設計・構築し，その評価を行った．

キーワード

災害対策, 分散バックアップ

## 1 はじめに

昨年 3 月 11 日に発生した東日本大地震では，茨城大学 (以下、「本学」と略) では人的な被害は少なかったものの，ICT 基盤は多くの被害を受けた．本学では日立, 水戸, 阿見の 3 地区に大きなキャンパスを有する (図 1)．各キャンパスにおける最大震度はそれぞれ 6 強, 6 弱, 6 弱であった．震源から最も遠い阿見キャンパスでは 5, 7 階に PC が設置してあったため，殆どの PC が転倒し中には机と共に転倒しているものもあった．幸いにも，サーバ類は収納したラックが床にボルトで固定されていたため転倒することはなかった．

停電期間は日立, 水戸, 阿見各キャンパスにおいてそれぞれ 3 日間, 2 日間, 2 日間であった．この長時間にわたる停電のため ICT 基盤は麻痺状態となっていた．

特に情報提供の要となる本来の大学の Web サーバ (以

図- 1: 茨城大学 3 大キャンパス

下,「本 Web」と略) が機能しなかった．地震発生が後期日程入試の前日であったこともあり，前期日程試験合格の入学手続き者や後期日程入試志願者に対して大学として早急な情報発信が必要であったが, それができない状況となった．震災前から学外組織に委託して開設してあった携帯電話向けの入試広報用 Web サイトはあったが，一般の方々には URL が知られておらず，検索エンジンでも上位には入っていなかったため，本学は Web での情報提供を全く行っていないように見えていた．

そこで初期対応として VIOPS(仮想化インフラストラクチャ・オペレーターズグループ) を通じて Web サーバを提供するボランティアに依頼し，クラウド上に本学の Web サーバ (以下,「仮 Web」と略) を構築し [4][5]，更に本 Web の URL で参照できるように仮の DNS サーバも構築した．本 Web 及び本学の DNS が復旧した後に JP DNS の設定を元に戻して頂いたが，DNS の『浸透問題』[6] が発生し，本 Web からの情報提供を充分に行うことができなかった．

サーバの停止期間が長引いた最大の要因は，サーバが設置された建物が甚大な被害を受けたことである．建物によっては 1 週間以上立ち入り禁止が続いた．特に震源地に近かった日立キャンパスでは，外壁が破壊された建物が多く，単独での立ち入りが更に 1ヶ月以上にわたり禁止されることとなった．サーバ室の通電チェックとサーバ類の再稼働作業は，建物倒壊の怖れがないことを確認できない状況のまま行われた．サーバ類は UPS に接続されていたため幸いデータの消失等は無かったが，データの保全が確認できるまで続いた恐怖は忘れられない．

同規模の地震への対策を考えるとき，今回の震災でも懸念された建物倒壊という事態を想定しておく必要がある．そこで我々は，建物倒壊時にも比較的短時間でサービスを再構成できるシステムを現行のネットワークトラフィックに影響が出ない形で実現できることを示すことを目的とし，震災時の対応の問題点を分析し，計算機システム及びネットワーク基盤の更新を機に対策を取り入れたシステムの設計・構築を行い，その評価を行った．

建物倒壊時には建物内に設置されたサーバの復旧は考えられないため，新サーバへの切り替え及びその前提となるデータ保全は必然となる．まず当該サーバに関連するデータは全て短い時間間隔で日頃から他のキャンパスでバックアップ保存するものとした．次にバックアップを所有しているキャンパスにおいて，システムの再稼働を実施する．この際，データを保存してあるネットワークドライブの IP アドレス等が変更になる．このため，セカンダリ DNS の外部委託を行いサーバ切り替えを確実に行えるようにする．このようにして，一般には通信・運営コストの面で不利と考えられる分散キャンパス環境を逆手に取り、分散バックアップシステムの構築を行った．

構成したバックアップシステムは，ほぼリアルタイムでファイルシステムのバックアップを他キャンパスに相互に配置するものである．同一学内であるためバックアップの際に暗号化等を行う必要もなく，ネットワークトラフィックを必要以上に増やすことがない．また，暗号化を行っていないため，すぐにシステムの再起動が可能となっている．

本論文は以下のように構成されている．2 章では震災時対応の問題点の分析について述べる。3 章では、幾つかの分散バックアップシステムの形態について比較・検討する．4 章で，本学が構築したバックアップシステムについて述べ、5 章で本システムが学内ネットワークに与える影響について分析・評価を行った．6 章はまとめである．

## 2　震災時対応と問題点の分析

### 2.1　対応の詳細

前述の通り，災害発生後に大学として早急に情報発信をすることが必要であったため，仮 Web を構築した．本 Web の URL でアクセスできるように DNS の設定を変更する必要があったが，本学の DNS サーバは停電のためまだ電源投入ができなかった．そこで仮 Web の A レコードを SINET の DNS に登録して頂くと同時に,「ibaraki.ac.jp」のネームサーバが SINET にあることを「jp」を管理している DNS サーバに登録して頂いた．これにより，仮 Web を本学の通常の URL で参照できるようになった．

震災の 3 日後，復電した日立キャンパスにおいて，倒壊の恐れがあるため立ち入り禁止となっていた IT 基盤センターのある建物の中で，火災の発生の怖れが無いことを確認の上サーバ室への通電が進められ，本 Web や DNS サーバの起動が行われた．まだ余震が続き，建物倒壊や再度停電が発生するかもしれない状況ではあったが，仮 Web から本 Web へ情報発信の拠点を戻すという決定がなされた．この決定を受け，SINET に向いていた DNS を本学の DNS に戻すとともに，VIOPS へ仮 Web の利用期限を申請した．これは DNS の TTL を考慮してものである．つまり，DNS のキャッシュサーバから仮 Web の登録が消失するまでは仮 Web のアドレスを答えてしまい，本 Web を閲覧できない可能性がある．

## 2.2 生じた問題

### 2.2.1 情報発信インタフェースの変更の問題

平常時以上に迅速できめ細かい情報発信が必要であったにもかかわらず，仮 Web における情報発信には困難を伴うこととなった．

本 Web 上のコンテンツは CMS 上に構築されていたため、コンテンツ管理者は平常時には CMS のインタフェースを利用してコンテンツの更新を行っていた．しかし仮 Web では本 Web と同じ環境を再現したわけではないため、同じ CMS は当然用意されておらず，情報を更新するには仮 Web 上のコンテンツを直接編集しなければならなかった．CMS によるコンテンツ管理に慣れていたコンテンツ管理者にとって，これは大変困難な状況であった．幸い、簡単な HTML を直に記述できる者を 2 名確保できたため，最低限の情報発信を行うことはできた．

### 2.2.2 DNS 切り替えに関する問題

前述の通り，仮 Web を実運用するにあたって SINET に DNS を依頼していた．本 Web を実運用に戻した段階で，本学 DNS の設定においてシリアル番号を新しいものと交換した．このことによりキャッシュサーバに蓄積されたデータは TTL に指定した 12 時間以内に順次置き換えられるはずであった．

しかし現実には，DNS の浸透問題により，遥かに長いほぼ 1 週間データが書き換えられなかった DNS があった．本学の Web サイトの参照のために同じ URL を指定しても，一方は本 Web をもう一方は仮 Web を見ているという状況が発生していた．スマートフォンの通信機能を利用し試したところ，高々40 分程度バスで移動しただけであるにもかかわらず接続するごとに仮 Web と本 Web が交互に表示されていた．

## 2.3 教訓

### 2.3.1 大規模なデータ消失を想定したバックアップ

被災前までは，小規模なデータの喪失に対する覚悟はあったものの，大規模なデータの喪失に関して切迫した危機感を皆持っていなかった．そのためバックアップも同一サーバ内あるいは同一サーバ室内の別のサーバにバックアップをとる程度であった．しかし建物倒壊が起こった場合は，これらのバックアップデータも同時に喪失してしまう．建物倒壊が現実味のある危険性として認識された今，喪失すると大学の運営が成り立たなくなるようなデータについても可用性を如何にして維持するかについて真剣に考えなければならない．

### 2.3.2 緊急時にも平常時と同じ環境が提供できること

震災時の大混乱の中，全く異なる環境で平常時以上の情報発信を行うことは非常な困難を伴う．平常時に利用する環境として，使い易い環境を提供し業務効率を高めておくことはもちろん重要である．しかしながら，日頃使い慣れた環境と同じ環境を，緊急時になってから改めてゼロから整えることは大変困難であるということを痛感した．特に緊急時の混乱の中では，同等の機能を持つがインタフェースは異なるツールでは意味がなく，ほとんど同じインタフェースを持つツールであることが重要である．すなわち，緊急時に平常時と同じ環境を如何に迅速に再構築するかよく検討しておく必要がある．

2.2.1 節で示した通り，Web コンテンツを構築するためのツールとしての CMS 等も，緊急時に異なる Web 上に異なる CMS しか用意できなかった場合は，コンテンツの作成作業も困難なものとなる．そのため，バックエンドの DBMS を含めた CMS が，緊急時にも提供できるような環境を提供できるようにする必要がある．

### 2.3.3 耐故障性のある DNS を構築すること

仮 Web のデータが TTL に指定したよりも遥かに長い時間残り続けた問題は，後日 DNS の浸透問題によって生じていたことが判明した．本 Web が本格稼働に入った際に，SINET における本学の DNS データを削除すれば，この問題を防ぐことができた可能性がある．

DNS に関しては，日頃より分散システムを意識し，耐故障性のあるシステムを目指すことが必要である．建物倒壊が起こった場合は，それまで運用していたサーバとは別の新サーバを稼働させるしかなく，その時に従来と連続性のあるサービスを提供するには DNS の速やかな切り替えが必須である．一つの方法として，当初から SINET のセカンダリ DNS サービスを受けていれば，本学の DNS サーバが復旧した時点で速やかに正しいデータに更新されたと思われる．

以上を総合すると，建物倒壊を想定した対策としては，緊急時に完全に新しいサーバの運用を開始することを想定し，平常時とまったく同じ環境を再構築するに必要十分なバックアップを，安全な場所に，かつ日常のシステム運用に大きな影響を及ぼすことなく取得する必要があることがわかる．

# 3 分散バックアップ

今回の震災のような大規模災害を考慮すると，バックアップの保管場所は，なるべく地理的に離れた場所に保管することが望ましいのは明らかである．選択肢としては以下の 3 つが考えられる．

1. 自組織内の別の場所に保管する,
2. 自組織外のデータセンタ等に保管する
3. 他組織と共同で互いに保管

以下では，それぞれのアプローチをとった場合の利点と欠点について検討する．

### 3.1 自組織内

自組織内でなるべく離れた建物にバックアップを保管する．キャンパスが一つであったり，複数でも余り離れていない場合には，今回のような広域災害に対しては無力であるが，地理的に大きく離れたキャンパスを有する場合には特に有効である．

自組織内でバックアップデータを保管することの利点としては，バックアップデータの取得, 移動, 保管において，自組織のネットワーク及びサーバで処理が完結することがあげられる．このことより，自組織の平常時の運用に影響を与えないようにバックアップや転送のスケジューリングを行うことが可能である．また，第三者がバックアップデータに触れる危険性がほとんどないため，第三者に対してデータの機密性を確保するための暗号化処理が必ずしも必要ではない．

ユーザデータよりはシステムの継続性に着目し OS イメージのバックアップを遠隔の自組織内に取り BCP 対策を行う場合 [3] も，自組織内であること及びバックアップ先でのシステムの起動を考慮し暗号化処理はされていない．

### 3.2 データセンタ

データセンタは通常耐震対策を行っているので，震災においてデータが喪失する危険性はほとんどない．

しかしデータセンタは通常自組織外にあるため，データセンタへのバックアップデータの保管のために，データセンタのネットワーク接続点にトラフィックが集中し，ボトルネックとなる恐れがある．またデータセンタの利用に当たっては，借用料等に加えて通信回線費が別途必要となる．

### 3.3 他組織と共同

東日本大震災以降，自組織のバックアップデータを他の組織と相互に保管しあうシステムを検討する大学が出てきている [1][2]．この方式では自組織全体が壊滅的な損害を受けたとしても，他組織に保管されたバックアップデータは損失を免れる可能性が高い．しかし同時に解決されなければならない問題点がいくつかある．

まず始めに，他組織が準備しなければならないストレージの容量が非常に大きくなることが予想される．重要なシステムのバックアップファイルは複数世代保管することが一般的であることを考えると，元データよりはるかに大きな容量が必要となるであろう．

次に，ネットワークトラフィックの観点からは，自組織とバックアップデータを保管する他組織の間のネットワークに，定期的にバックアップデータが流れることになる．システムのフルバックアップを送信する場合には大量のデータが瞬間的に送られることになるため，日常の他の通信に影響が出ないようにしなければならない．また，ファイルシステムのバックアップのように，前回のバックアップからの更新差分のみをバックアップするのが一般的である場合には，送信されるバックアップデータのサイズはフルバックアップに比べれば遥かに小さくなるものの，差分を求める頻度によっては日常業務の最中に定常的にバックアップデータの送信が行われることになる．いずれにしても複数の組織の間で，バックアップタイミングのスケジュール調整が必要となることは明らかである．

最後に，大学の運営にかかわるような重要なデータを他組織に保管する上で，暗号化は必須である．暗号化されていることにより，バックアップデータの差分を求める等の処理ができなくなるため，平文で保管する場合に比べると効率はどうしても悪くなる．暗号化されたデータのサイズは，基本的に元となるバックアップデータのサイズと同じである．複数拠点に分散してバックアップデータを配置する場合には，秘密分散法の利用等により，一拠点あたりのデータサーズを元データより小さくすることこは可能である．平文で保管する場合に比べて必要となる容量の点では大きな問題はないが，暗号化や復号の処理のための計算機資源を必要とすることには注意しなければならない．

## 4 茨城大学でのバックアップシステム

### 4.1 計算機システム及びネットワークの概要

まず始めに，分散バックアップシステムを導入する本学のキャンパスの地理的な関係及びキャンパスネットワークとサーバの構成を整理する．

本学は図 1 に示した通り大キャンパスが日立, 水戸, 阿見の 3 地区にある．キャンパス間の距離は日立-水戸間が約 30km, 水戸-阿見間が約 50km である．今回の震災では，冒頭にも述べたように各キャンパスでの震度の差があり，被害状況にも有意な差があった．同様の地震に見舞われても，万一にも 2 つ以上のキャンパスが同時に壊滅するとは考えにくい．そこで本学においては，

自組織内の他のキャンパスにバックアップを置くことは震災を考慮しても有効であると思われる．

本学の計算機システムやネットワークシステムを管理する IT 基盤センターは日立キャンパスにあるため，本学のネットワークとしての入り口は日立キャンパスとなっている (図 2)．このため，ファイアウォール等は日立キャンパスに設置されている．また，本学では SINET の共同調達に当初から参加している．各キャンパスの入り口に L3 スイッチを配置し広域イーサネットを利用して通信帯域 1Gbps で接続しているため，キャンパス間ネットワークはスター型となっている．附属学校 3 校や 3 研究センターは，通信帯域は 100Mbps ではあるが同じ広域イーサネット経由で接続している．

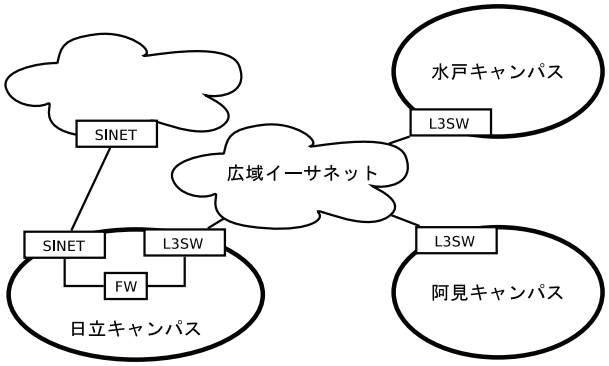



図- 2: キャンパス間ネットワーク

本学には 5 学部があり 1 年次生のほとんどは水戸キャンパスで修学しているが，工学部と農学部の 2 年次以降はそれぞれ日立, 阿見キャンパスにおいて修学している．

各キャンパスに学生用のサーバ (以下,「キャンパスサーバ」と略) を配置し，電子メールはもちろん演習用に学内に限った Web 頁の構築演習を行っている．1 年から 2 年に進級した際に，電子メールアドレスや作成した Web 頁の URL が変わってしまうのは，不要な混乱を招くだけと思われることから，アカウントは卒業までに一番長く修学するキャンパスのキャンパスサーバ上に入学と同時に発行している．つまり，工学部及び農学部学生用のキャンパスサーバはそれぞれ日立及び阿見キャンパスにあり，1 年次からそれを利用する．

次にバックアップの対象となるデータについて述べる．キャンパスサーバ上の各ユーザのデータは，ホームディレクトリに保管される．電子メールもホームディレクトリ配下に Maildir 形式で保存されるため，基本的にはユーザデータのバックアップはホームディレクトリのみを対象とすればよい．

茨城県は雷の発生等も多く，その影響で停電することも稀ではない．キャンパスが離れているため停電は基本的にキャンパス毎である．PC へのログインやネットワーク利用等における認証等が他キャンパスの停電によって影響されないよう，認証サーバ等は各キャンパスに設置してある．教職員が学内外へ情報提供するために Web を利用する基盤としての仮想サーバの提供も行っており，本学としての Web サーバも仮想サーバとして提供している．更に，仮想サーバのバックエンドとなる DBMS も複数用意している．

また，本学のネットワークとしての入り口が日立キャンパスであるため，上述の仮想サーバを含む主要サーバも日立キャンパスに設置されている．

平成 24 年 3 月に教育用計算機及びネットワークシステムのリプレースを行った．基本的にはこれまでのシステム構成は変更していないが，サーバのほとんどを VMware 上の仮想機械とした．更にディスクシステムも仮想化に対応するため，前システムでは各主要サーバ毎に用意していた NetAppp 社のディスクを，各キャンパスに 1 台ずつの EMC 社の VNX5300 に変更した．ディスクの大容量化により，各ユーザのホームディレクトリ以下の容量を表 1 に示した通りに増やすことが可能となった．

表- 1: ユーザのディスク容量

| 種別 | 容量 (前) | 容量 (現) |
|---|---|---|
| 教職員 | 250MB | 3GB |
| 学生 | 120MB | 1GB |

また，平成 24 年度末に全学的に無線 LAN 環境を整備し，アクセスポイント 320 台を各建屋の各階に 1 台以上配置した．無線 LAN システムは Aruba 社製のコントローラタイプのものであるため，他のシステムと同様に停電等を考慮し各キャンパスにコントローラを設置し，それぞれをキャンパス間接続用 L3 スイッチに直結している．

## 4.2 分散バックアップシステム

本学におけるバックアップの対象は，主に学生演習等による成果物や電子メールデータである．いわゆるネットショッピングにおけるトランザクションデータの様なクリティカルなデータではないが，大量のデータ量が対象となる．現時点での総データ量はリプレース直後ということもあり 2.5T バイト程度であるが，将来的にはその 10 倍程度になると見込まれる．

システムリプレースの際，各キャンパスに設置したディスクシステムを論理的に分割し，次の 4 つに分類した．

0. 実データ
1. 実データのバックアップ
2. 他キャンパスのバックアップ

3. 他システムのバックアップ

項番 1 はディスクシステムの耐故障性を通常の冗長化で向上させるためのもので，項番 2 は他キャンパスのデータのバックアップを保管するためのものである．項番 1 のバックアップは，EMC VNX5300 の機能を利用し，実データに変更があった際にはリアルタイムで反映される．

他のキャンパスへ保管する項番 2 のバックアップに関しても，EMC VNX5300 の機能を利用し 10 分間隔で変更が反映される．電子メールや受講学生の成果物という観点からは，本研究で実現したような短い間隔でのバックアップが必要と思われる．震災時に同時に 2 つのキャンパスで建物倒壊等の被害はないと考えているため，このバックアップは他の 1 つのキャンパスのみとした．

項番 3 は，別途購入した学内システムのバックアップデータを保管するための領域である．

工学部及び農学部の 1 年生のデータはそれぞれ日立及び阿見キャンパスにあるため，日常的に異なるキャンパス間の通信が発生している．例えば，水戸キャンパスにいる農学部 1 年生がホームディレクトリのファイルを更新すると，図 3 に示すようにデータを書き込む際に水戸-阿見間の通信が発生し，更にそのデータのバックアップを取るために阿見-日立間の通信が発生することになる．電子メールに関しても，同様の通信が発生することになる．

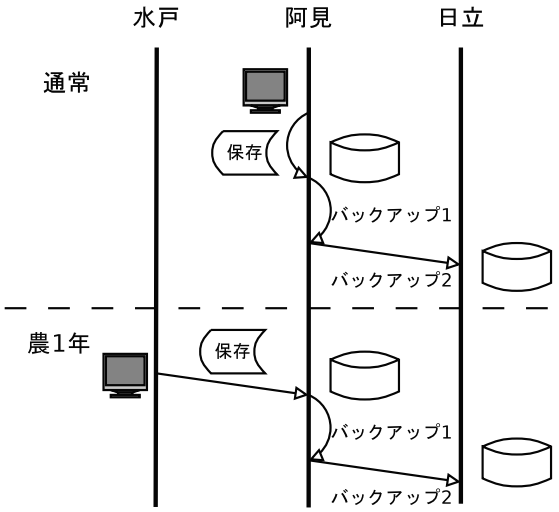



図- 3: 保存したファイルのバックアップ

なお，キャンパス間のバックアップについては暗号化処理を行っていない．これは次の理由からである．

1. バックアップを作成するシステムも保管するシステムも共に IT 基盤センターの管轄下にあるため
2. 平常時のバックアップ作成負荷を低く抑えるため
3. 緊急時の復旧作業を簡素にしておくため

また，圧縮も行っていないため，バックアップのデータはそのまま実データとして利用することができる．例えば，dump コマンドを用いた差分バックアップのような場合には，実データとしてそのまま利用できず，データの復元の際にマスタに差分を当てていく作業及びそのためのディスクが必要となってしまう．

また，将来的には総データ量は 25T バイト程度までを想定しているが，バックアップの際の送信対象は差分であるため，総データ量が現時点での 10 倍になったとしてもトラフィックはそれ程増加しないと考えられる．dump コマンドを用いた差分バックアップの場合のようにマスタとして全てを送る必要がある場合は，その都度総データを送信する必要が生じてしまう．

本学が採用した方式では，仮にいずれかのキャンパスにおいて建物倒壊等でシステムが利用できなくなった際も，そのシステムのイメージを VMware 上で動かした後にバックアップをマウントするだけで容易にシステムを再現することができる．

更に本学では，ユーザデータだけではなく，2.3.2 節にも示した通り，Web の CMS 及びバックエンドの DBMS も対象としている．これにより，建物倒壊が起こったとしても，Web サーバはもちろん CMS 環境の提供も可能となっている．

### 4.3 セカンダリ DNS

建物倒壊を免れた他キャンパスに新サーバを復旧させた場合，DNS の迅速な切り替えが必須である．これまでは DNS はプライマリ及びセカンダリともに本学内に設置していたが，前述のように DNS の浸透問題が発生した．

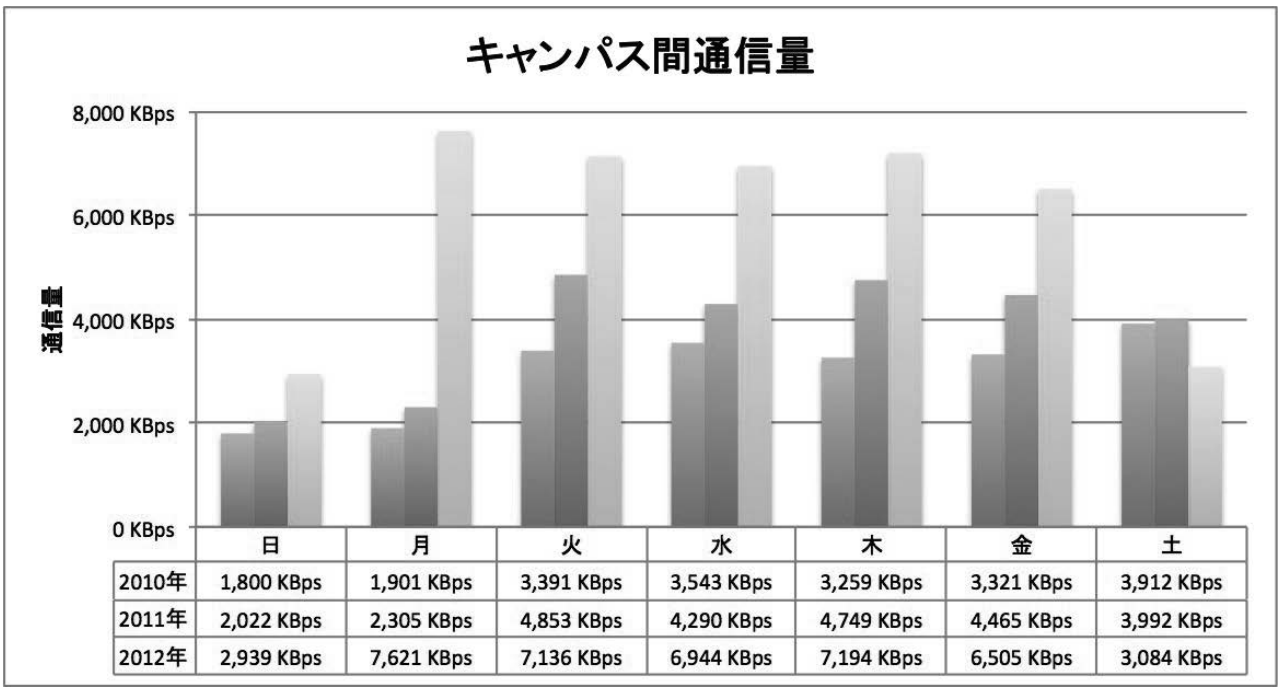
そこで被災時にも速やかに DNS のデータを更新できるように，SINET の提供するセカンダリ DNS サービスを利用することにした．災害時に本学の DNS サーバが被災しても，本学のデータを持つ DNS サーバをあわてて構築する必要がなくなっただけでなく，本学の DNS サーバが復旧した際にも DNS の浸透問題が発生しないことが保証されることになった．

## 5 分析及び評価

### 5.1 トラフィックへの影響

まず始めに，本分散バックアップシステムによってキャンパス間ネットワークのトラフィックにどの程度の影響を与えているかを調査した．

本システムでバックアップの対象となっているのは，全ユーザのホームディレクトリ以下のデータ, Web の仮想ホストのデータ及び DBMS のデータ等計算機システ




| | 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|---|
| 2010年 | 1,800 KBps | 1,901 KBps | 3,391 KBps | 3,543 KBps | 3,259 KBps | 3,321 KBps | 3,912 KBps |
| 2011年 | 2,022 KBps | 2,305 KBps | 4,853 KBps | 4,290 KBps | 4,749 KBps | 4,465 KBps | 3,992 KBps |
| 2012年 | 2,939 KBps | 7,621 KBps | 7,136 KBps | 6,944 KBps | 7,194 KBps | 6,505 KBps | 3,084 KBps |

図- 4: 3 年間のトラフィックの比較

ム上のユーザデータの全てである．システムリプレース直後のため，現時点での対象となるデータ量は 2.5T バイト程度である．比較を行ったのは，現在のシステムの運用が安定してきた 6 月の 2 週間分と過去 2 年間 MRTG で計測していたトラフィックデータである．曜日毎に平均を取ったものを，図 4 に示す．

一見してわかるように月曜日および土曜日が特異である．月曜日および土曜日の特異な傾向の変化は，本学のカリキュラム上の変化によるものであることがわかっている．

月曜日に関しては，本年度より PC を利用する講義が増えたという事情がありトラフィックが増大したものである．昨年度より工学部及び農学部学生に対する教養科目「情報処理概論」が，2 年次開講から 1 年次開講へと移行している．年次進行のために 1, 2 年生の両方に対して講義を開講する必要が生じたため，PC を利用する講義数が一時的に増加することとなったが，この増加分がこれまで PC を利用する講義の少なかった月曜日に集中して開講されるようになった．1 年生の PC 利用が増えると，キャンパス間の通信が増えることは 4 章でも述べた通りである．

一方，土曜日の通信が少なく見えるのは，むしろ 2010 年と 2011 年の通信が多かったことが原因である．2010 年は建物改修, 2011 年には震災の影響等で，一部の学部で土曜日に平日と同じ様に開講しており，その通信が発生していた．今年度は土曜日の開講がなくなったためトラフィックが減少した様に見える．

月曜日と土曜日を除くと，それ以外の平日は同様の傾向を示しており，2012 年は 2011 年の約 1.5 倍程度のトラフィックになっている．

トラフィック増加の要因としては，本バックアップシステム以外に，2012 年 3 月に整備した無線 LAN システムがある．昨年度までは研究室で設置された無線 LAN しかなかったため，学生は研究室に配属されるまで無線 LAN をほとんど利用することがなかった．今年度からは学内のほぼ至る所で無線 LAN が利用できるようになったことにより，現在では，毎日最大 500 デバイス程度が同時に接続されるようになっている．1 年生でも PC やスマートフォンを無線 LAN に接続する利用者は確実に増え続けている．

来年度以降「情報処理概論」の重複開講が解消されたとしても無線 LAN の利用等でトラフィックが増え続けて行くことは間違いない．しかし，現在の広域イーサネットへの契約帯域が 1Gbps であることから，本学としては現時点では余裕のある通信量であるということができる．これにより，キャンパス間ネットワークに支障を与えず，バックアップシステムが安定して運用できていると思われる．

## 5.2 バックアップデータの形式

次に，バックアップデータの形式について検討する．

前述のように，本システムではデータの圧縮や暗号化等をしておらず，実データと同じ状態で保存している．このため，停止したシステムを VMware 上で動かしバックアップをマウントするだけで容易にシステムを

再現することができる．災害からの復旧時に，複雑な処理をすること無しにシステムを容易に再現できるのはきわめて重要な条件と思われる．

バックアップデータを暗号化して保存する場合，共有鍵暗号方式であればデータ量は暗号化前のものと同じことも考えられる．しかし，本研究の方式と同じく差分データをバックアップした場合は，復元の際に各差分を復号し，基本となる全データへ差分を適用する必要がある．これには多大な手間が必要となる．更に，差分の適用回数を減らすためには，ある一定期間毎に基本となる全データをバックアップ先へ送る必要が生じる．仮に全データを 2.5T バイトとすると，1Gbps の通信帯域を専用に利用できたと仮定しても約 5.6 時間要する．これは本学にとっては現実的とは考えられず，ネットワークではなく別の手段を考える必要がある．もしくは，災害時に提供しなければならない Web コンテンツ及び CMS 関連のデータ等の必要最小限のデータに限ってバックアップを考えなければならない．

西村らの方法は，データの広域分散配置により東日本大震災よりもより甚大な災害にも堪えうる有用な方法であると筆者らも着目しているが，前段落で言及した通り本手法はキャンパスが地理的に分散している状況でのみ実現可能であるがゆえに，差分の適用の問題及び基本となる全データの送信問題を生じないものとなっている．更に，全データに関しては，分散した拠点数分の送信が必要となり，実現のためにはより広帯域が必要となる．もしくは，前段落で言及した通り，必要最小限のデータに限ってバックアップを考えなければならない．

## 6　まとめと今後の課題

東日本大震災で得られた教訓を基に，平常時には様々な面で不利と思われてきた分散キャンパスという立地を逆手に取って，分散バックアップシステムを構築することができた．本研究で実現したシステムでは，ユーザデータの全てに関して他キャンパスにバックアップを取っているが，そのための通信量は現時点での利用に影響の出るものではない．

バックアップデータは実データと同じ形式であるため，新しいサーバを稼働させた際にバックアップデータをそのままマウントすることができ，比較的容易にシステムの再構築が可能なシステムとなっている．

また，バックアップデータは学内に配置されるため，データのセキュリティを確保し易いという利点もある．

以上から，効率の良く安全で復旧が容易なバックアップシステムを構築することができた．これにより，建物倒壊の被害に遭遇しても，他のキャンパスで容易に再稼働することが可能となった．

分散キャンパスを有する大学は，基盤設備のキャンパス毎の調達やキャンパス間通信回線のコストが固定費となって常に苦しんできた．本報告では，固定費の範囲内でキャンパス間での分散バックアップが可能となった一例を報告した．また，単一キャンパスからなる大学では，データセンタとの間の通信回線コストが新規に必要となるが，遠隔地の信頼できるデータセンタを利用すれば同様のシステムを構築することが可能である．

今後の課題として，次の 2 つを考えている．第 1 の課題は，現在バックアップの間隔を 10 分としているが，その間隔を変えた際にどの様にネットワークへ影響が生じるかの調査である．第 2 の課題は，現在は，他キャンパスへのバックアップの対象を教育用計算機のデータのみに限っているが，他のシステムのバックアップを受け入れることで大学としての BCP に貢献していくことである．その際にも第 1 の課題に示したバックアップの間隔を変更して，システムの評価を行いたいと考えている．

## 参考文献

[1] 西村浩二: 電子情報の大学間相互保持に向けた遠隔バックアップ技術の研究, 学際大規模情報基盤共同利用・共同研究拠点 第 2 回シンポジウム 講演予稿 2011 年 1 月

[2] 熊谷悠平 他: 認証フェデレーションに基づく分散ファイル管理システムの提案, 情報処理学会 インターネットと運用技術研究会, Vol.2012-IOT-18 No.8, 2012 年 6 月

[3] 岩井真依 他: BCP 対策に向けたサービス無停止バックアップの実証実験, 情報処理学会 インターネットと運用技術研究会, Vol.2012-IOT-17 No.21, 2012 年 5 月

[4] 鈴木 宏康: cloudpack における AWS による DR, http://www.cloudpack.jp/topics/20110630.html, 技術評論社「G-CLOUD Magazine 2011 Summer」, 2011

[5] 茨城大学様からの御礼状のご紹介, http://www.viops.jp/2011/03/post-12.html, 2011 年 3 月

[6] 森下泰宏, 民田雅人: DNS 浸透の都市伝説を斬る ～ ランチのおともに DNS～, http://jprs.jp/tech/material/iw2011-lunch-L1-01.pdf, Internet Week 2011