

フレッツ回線を利用したキャンパス間通信のバックアップ手法とその実践

近堂 徹¹⁾, 吉田 朋彦¹⁾, 西村 浩二¹⁾, 相原 玲二¹⁾

1) 広島大学 情報メディア教育研究センター

tkondo@hiroshima-u.ac.jp

The Practice of the Backup Connection between Campuses using the FLET'S HIKARI access service

Tohru Kondo¹⁾, Tomohiko Yoshida¹⁾, Kouji Nishimura¹⁾, Reiji Aibara¹⁾

1) Information Media Center, Hiroshima University

概要

広島大学ではキャンパス間通信やインターネット接続の高速化や高品質化を目的として、2001年に主要キャンパス間やデータセンターを結ぶ光ファイバケーブルを敷設し、常時活用している。一方で、災害や障害に強いインフラを確保するためには、通信回線を含めた冗長経路等に関する検討が必要となるが、管理運用コストとのトレードオフとなり、常時利用する通信回線と同品質の回線を定常的に確保するのは難しい。そこで本稿では、比較的安価に利用できるフレッツ回線を利用した緊急時のキャンパス間通信のバックアップ手法について述べる。さらに、2018年7月6日から7日にかけて西日本を襲った豪雨により、キャンパス間光ファイバが大きな損傷を受ける事象が発生した。その際に実施した本手法を活用によるバックアップ作業の実践について報告する。

1 はじめに

大学などの高等教育機関におけるキャンパスネットワークは、教育研究活動から事務・管理運営業務に至る様々な活動に対してICTを最大限に活用するための主要インフラとして位置付けられ、停止することなくサービスを提供することが強く求められる。この要求に対して、可能な限りコストをかけずに安定性や可用性を実現・向上させていく必要がある。さらに複数の地区に分散して拠点をもつ組織では、拠点間の通信回線やネットワーク構成、インターネット接続についての検討が必要となる。このように、多くの大学で基幹ネットワークや情報システムにおける耐障害性・耐災害性を向上させる取り組みが行われている[1],[2]。

また、近年大学等でもクラウドコンピューティングを導入する動きが顕著であり、多くの大学でパブリッククラウドを利用した情報サービスが提供されるようになってきた。クラウド利用においてはインターネット接続が前提となるため、ネットワークの切断が各種業務の遂行に大きな影響を与えることは避けられない。このようなことから、耐障害性に優れたネットワーク基盤への要求が明確となっている。

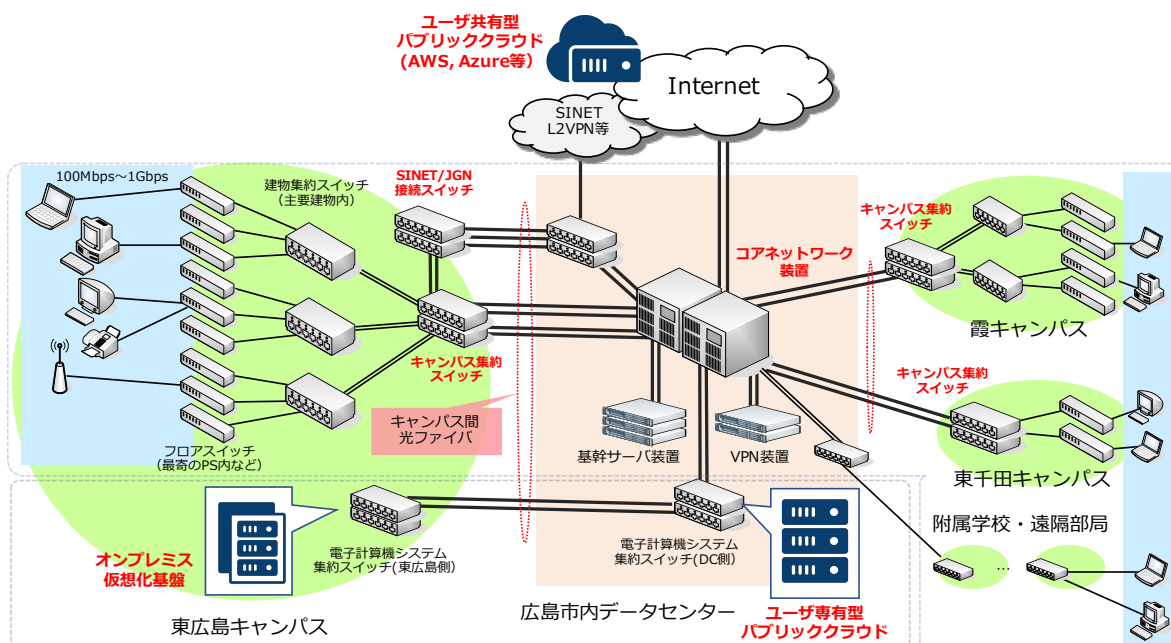
広島大学では2001年に主要キャンパス間やデータセンターを結ぶ光ファイバケーブル（以下、光ファイ

バ）を敷設し、キャンパスネットワークや電子計算機システムのネットワーク接続に常時活用している。一方で、この物理経路に依存した形となり、災害・障害の発生によりファイバを収容する管路が損傷した場合などに受ける影響は非常に大きい。物理経路の異なるバックアップ用ファイバを確保しておくことが望ましいが、経済的制約により実現できなかった。そこで本稿では、比較的安価に利用できるフレッツ回線を利用し、緊急時に必要最低限の通信経路を確保することを目的としたキャンパス間通信のバックアップについて述べる。実際に2018年7月6日から7日にかけて西日本を襲った豪雨により、キャンパス間光ファイバが大きな損傷を受ける事象が発生した。その際に実施した本手法を活用によるバックアップ作業の実践について述べる。

2 広島大学のキャンパスネットワーク

2.1 キャンパスネットワークの変遷

本学のキャンパスネットワークの規模等を明らかにするために、これまでのキャンパスネットワークの変遷について述べる。広島大学のキャンパスネットワークは情報メディア教育研究センター（以下、メディアセンター）が管理・運用を行い、主要3キャンパス（東広島キャンパス、霞キャンパス、東千田キャンパス）、



附属学校（翠地区，東雲地区，三原地区，福山地区）および小規模遠隔部局（呉，竹原，宮島，東京オフィス等）の拠点から構成される。構成員数は、教員約 1,800 人，職員約 3,300 人，学生約 15,000 人（附属学校の児童，生徒約 4,000 人は含まない）の規模である。

広島大学での本格的なキャンパスネットワークは FDDI を基幹に採用した HINET93 (1994 年稼働) に始まり, ATM を基幹に採用した HINET95 (1995 年稼働), Gigabit Ethernet を基幹とする HINET2001 (2001 年稼働) と更新を重ねてきた。いずれにおいても, 原則サブネットを部局単位に割当てを行い, 各部局で管理する体制で運用を行ってきた。2008 年度から運用を開始した HINET2007[3] ではそれまでの管理方法を一新し, 全学整備および一元管理によるキャンパスネットワークを構築・運用してきた。基幹ネットワークだけでなくフロアスイッチ (2018 年 9 月時点で約 550 台) を対象とした整備を実施し, 部局単位でのサブネット管理体制から全学的な一元管理体制へと移行した。HINET2007 の考え方は次節で述べる現行のキャンパスネットワーク (HINET2014) でも同様の機能を引き続き実現しているため, 詳細については後述する。

主要 3 キャンパスおよびデータセンターとの間の通信については、2001 年に敷設した光ファイバを活用している。この光ファイバは、キャンパスネットワークのほかにも電子計算機システム [5] におけるオンプレミス仮想化基盤とデータセンターに設置されたユーザ

専有型パブリッククラウドとの接続や教育用情報端末の内部ネットワークの接続にも利用しており、キャンパス間通信を支える重要インフラとなっている。

2.2 HINET2014

本節では、2014 年 8 月より稼働しているキャンパスネットワーク HINET2014 について紹介する。ネットワーク構成を図 1、主要な機器仕様を表 1 に示す。図 1 には、HINET のほか、電子計算機システム (HUC12) で活用するパブリッククラウド（専有型、共有型）とオンプレミス仮想化基盤の構成も示している。

HINET では、コアスイッチ装置および各キャンパス集約スイッチは全てスタック接続かつリンクアグリゲーションによるアクティブ・アクティブ構成とし、ファイアウォール装置と VPN 装置については HA (High Availability) によるアクティブ・スタンバイ構成としている。これにより、装置やリンクの故障に対する冗長性を確保した。

HINET の主な特徴は以下に示す通りである。

基幹装置のデータセンター設置 HINET2014 では基幹装置の主要部分をデータセンターへ設置している。これにより、対外接続拠点であるデータセンターから各キャンパスが接続される完全なスター型ネットワークとなり、対外接続に対するトラフィックの経路最適化と、特定のキャンパスでの障害に依存しない耐障害性の向上を実現している。レイヤ3機能をデータセンターに集約するこ

表 1 基幹ネットワーク装置の主な機器仕様

機器名称	機種	数量
コアスイッチ装置	Cisco Catalyst 6807-XL	2
ファイアウォール装置	Cisco ASA5585-X / SSP60	2
VPN 装置	Cisco ASA5545-X	2
キャンパス集約スイッチ	Alaxala AX3830 (東広島)	2
	Alaxala A2530S (霞)	2
	Alaxala A2530S (東千田)	2
基幹サーバ装置	DELL PowerEdge R620	3

とにより、キャンパス間およびキャンパス内はすべてレイヤ 2 ネットワークで構成され、各キャンパスに設置される集約スイッチもミドルボックスの L2 スイッチである。データセンターと各キャンパス間は 802.1Q による VLAN を行い、自設の光ファイバを用いて最大 40Gbps (東広島～データセンター) の帯域を確保している。

ゾーニングによるネットワーク設計 HINET では学内外からのアクセス可否パターンおよび利用形態により区別される「ゾーン」という概念を導入している。図 2 にゾーンの概要を示す。構成員の多くが研究室単位でゾーン C を申請し、その中に PC やプリンタ、NAS 等を設置して管理・運用するのが一般的な利用形態となっている。学外公開が前提となるサーバはゾーン A、複数のゾーン C やゾーン D から利用する可能性のあるプリンタや NAS 等の学内限定ホストはゾーン B に設置する形で運用している。構成員はネットワーク利用申請サービスを通して各種の申請を行う。

個別ファイアウォール機能の提供 約 2,000 の個別ファイアウォール (NAPT) 機能と DHCP サーバ機能をキャンパスネットワークの機能として全学的に提供し、管理・維持コストの削減を図っている。2,000 という数字は本学教員等の数を勘定して設定したものであり、1 教員 1 個別ファイアウォール (ゾーン C) の提供が可能となる。また、ゾーン C の管理者によって構成員の ID をネットワーク利用申請サービスで事前登録することにより、特定のゾーン C の機器と直接接続可能な VPN サービスも提供している。

全学的な一元管理体制 全学整備の範囲を基幹ネットワークからフロアスイッチまでとし、約 550 台のフロアスイッチを一元管理としている。ポート総数としては、18,000 ポートとなる。各ポートの物理リソースのみならず VLAN ID、IP アドレスの論理リソースもメディアセンターで一元的に管理

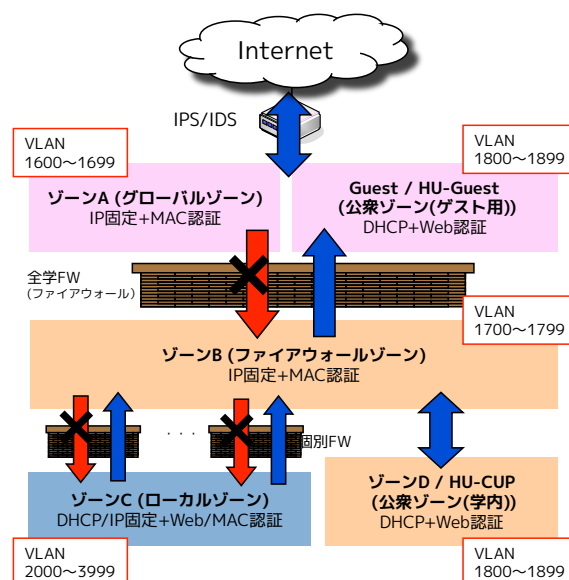


図 2 HINET におけるゾーン構成

し、ネットワーク利用申請サービスからの申請に基づきメディアセンターで一括して設定を行う。

3 キャンパス間通信のバックアップ手法

前章で述べた通り、主要 3 キャンパス間の通信では広島大学が 2001 年に整備した光ファイバ (以下、主回線とする) を利用している。高品質で安定的な通信が可能である一方、多くの通信が主回線に強く依存している状況となっている。特に、HINET では L3 機能をデータセンターに収容したスター型のネットワークとなっているため、大学内の通信であってもサブネットを超える場合はこの経路を往復する形となる。

図 1 にも示している通り、東広島キャンパスとデータセンター間は 2 芯 1 対を 4 ペア利用し、10Gbps × 4 で冗長化、霞・東千田キャンパスとデータセンター間は 2 ペア利用し、10Gbps × 2 での冗長化を行なっている。これにより、機器の障害や計画的作業においては無停止での運用が可能である。しかしながら、通信回線を考慮した冗長化は行われていない。そのため、光ファイバ全体に損傷が発生すると通信断は避けられない。これに対しては、同等の性能を有する通信回線を確保して冗長化を行い、バックアップ回線として利用できる状態しておくなどの対策を行う必要があるが、費用面や運用面での大きなコスト増となる。

そこで広島大学では、緊急時の最低限のキャンパス間通信経路を確保するために、HINET で利用する通信に対して商用回線を利用したバックアップを用意している。その構成を図 3 に示す。商用回線として

NTT 西日本が提供するフレッツ光ネクストスーパーハイスピードタイプ準（ファミリータイプ）を、東広島キャンパスとデータセンターにそれぞれ 2 回線ずつの合計 4 回線を準備している。さらに、キャンパス間の 802.1Q タグを透過させる必要があるため、マイクロリサーチ 社のレイヤ 2VPN 装置である Unified Gate1005（以下、Unified Gate）*1を両端に設置している。Unified Gate は拠点間でタグ VLAN を透過することが可能な製品であり、拠点間は EtherIP もしくは IPsec によるトンネリングを行う。外部接続には PPPoE による商用プロバイダ接続のほか、NTT 西日本が提供するフレッツ・v6 オプションを利用した網内接続にも対応し、高スループットでのレイヤ 2VPN を構築することができる。本手法では、この Unified Gate を 2 セット設置することで 2 つのバックアップ（A 系統と B 系統）を構築し、必要に応じてコアスイッチと東広島キャンパス集約スイッチ間で通信継続が必要な VLAN を主回線からバックアップ回線に割り振ることでキャンパス間通信のバックアップが可能となる。

バックアップ回線切替えのための操作としては

- 事前に、コアスイッチおよびキャンパス集約スイッチに対してバックアップ対象とする VLAN をバックアップ回線用のポートに設定し、シャットダウン状態にしておく
- 切り替え時に、主回線のポートチャネルを shutdown 操作し、バックアップ回線用ポートを noshutdown 操作する

のみである。主回線側のポートチャネルの障害を検知し上記の切替操作を自動化することは可能だが、現時点では手動での切替となっている。

4 2018 年 7 月豪雨災害における実践

4.1 災害の概要

2018 年 7 月 6 日午後から 7 日早朝にかけて、西日本を中心に広範囲に渡って豪雨により土砂崩れや道路崩落などの大規模災害が発生した。この災害により、前節で説明したキャンパス間の光ファイバも大きな損傷を受けた。具体的には広島市内の国道の道路崩落により国道沿いに埋設された情報ボックスが破損し、収容する光ファイバが保護管路から露出し荷重がかかる状

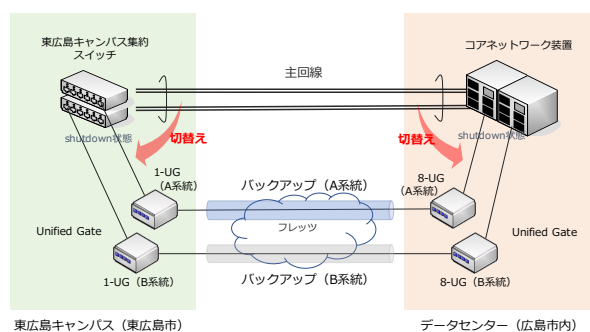


図 3 商用回線を利用したキャンパス間通信のバックアップ構成（東広島 - データセンター間）



図 4 光ファイバを収容する情報ボックス損傷の様子

態となった。メディアセンターで公開している写真を図 4 に示す*2。損傷箇所は 2 箇所、7 月 8 日午後の時点で通信障害等の影響は確認されなかったものの、いつ切断されてもおかしくない状況となった。

4.2 光ファイバの迂回工事計画

7 月 8 日の損傷の報告を受けた後、損傷を受けた箇所を迂回するために臨時の光ファイバを電柱懸架で準備し、光ファイバ経路の変更工事を行うこととなった。調整の結果、広島市安芸区中野東の損傷箇所については 7 月 13 日 21:00 から 23:00（迂回用光ファイバ長：約 410 m）、広島市安芸区の損傷箇所については 7 月 18 日 22:00 から 24:00（迂回用光ファイバ長：約 1,380 m）の時間帯で行われることが決まった。

この光ファイバ迂回工事は、すべての芯線を一旦切断し、その後テープ芯線ごとに融着接続を行う作業となる。迂回工事において最初に復旧させるテープ芯線を工事業者に指定できたため、4 ペアあるうちのひとつを復旧させることで、すべての芯線の復旧を待たずして 10Gbps のキャンパス間通信を復旧させることは

*1 <https://www.mrl.co.jp/product/ugg05/index.html>
(2018-09-08 参照)

*2 https://www.media.hiroshima-u.ac.jp/news/disaster_201807 (2018-09-08 参照)

表2 バックアップ対象 VLAN とその振り分け

系統	VLAN 数	利用用途
A	2	基幹ネットワーク管理用セグメント
	1	外部から参照されるサーバセグメント
	50	事務用ネットワークセグメント
B	3	学生情報システムや全学 e-learning システム

可能となった。しかしながら、最初のテープ芯線が接続されるまでは、東広島地区のネットワークが分断された状態となり、東広島地区でのインターネット利用や他の地区等からのサーバ等へのアクセスができない状態となる。事前の計画では2時間程度の通信断と伝えられた。この対策として、前節で示したバックアップ手法を利用した一部サービスの継続を試みた。

4.3 バックアップ回線の利用

バックアップ回線で確保できる帯域は商用サービスの品質に大きく依存するため、通常のキャンパス間通信の全てをバックアップ回線に流すことは現実的には難しい。そこで、バックアップ対象とする VLAN を限定し、特定の通信のみをバックアップすることで、一部サービスのみを継続する方針とした。具体的なバックアップ対象は表2に示す通りであり、バックアップ対象する通信を収容する VLAN (合計 58VLANs) を平常時のトラフィック量等を考慮し、A 系統と B 系統にそれぞれ割り振った。

広島大学では主要な情報システムはクラウド化を進め、電子メールや各種ウェブサイトへのアクセスは本災害の影響を受けることはなかったが、一部学内に存在するサーバ類や管理運営業務のために優先的に利用が求められる事務用ネットワークをバックアップ対象とした。一方、学内構成員が利用するネットワーク(図2におけるゾーン C やゾーン D)は今回はバックアップ対象とせず、該当時間帯では利用できない旨の広報にて対応した。作業が夜間であったことと全学に対する事前周知等を行なったことにより、大きな混乱はなかった。

4.4 光ファイバ迂回工事による影響とバックアップの効果

迂回工事およびバックアップ作業の流れを13日と18日それぞれで表3にまとめた。作業時間帯は異なるものの、13日と18日の両日で本手法によるバックアップを実施した。13日では最初バックアップの切替に時間を要する結果となった。これは切替操作においてコアネットワーク装置と東広島キャンパス集約スイッチの操作が必要になるが、装置へのアクセスおよび操作に時間を要したためである。

表3 光ファイバ迂回工事およびバックアップ切替の様子

7月13日 21:00-23:00	
21:00	工事業者からの作業開始連絡
21:03	光ファイバ切断(キャンパス間通信の全断)
21:19	バックアップのリンクアップ
22:10	最初の光ファイバの融着完了報告
22:15	バックアップ回線のリンクダウン
22:16	キャンパス間ファイバのリンクアップ
以降	冗長系を含む全光ファイバの融着作業
7月18日 22:00-24:00	
22:00	工事業者からの作業開始連絡
22:04	光ファイバ切断(キャンパス間通信の全断)
22:05	バックアップのリンクアップ
22:45	最初の光ファイバの融着完了報告
22:46	バックアップ回線のリンクダウン
22:46	キャンパス間ファイバのリンクアップ
以降	冗長系を含む全光ファイバの融着作業

バックアップ回線利用中の東広島キャンパス～データセンター間の通信品質(18日分)を図5に示す。2つのバックアップラインについて RTT と連続パケットロス数を計測したものである。なお、RTT については Y 軸は最大 100ms でプロットしている。この結果からもわかるように、バックアップ期間中に通信品質の悪化がみられ、特に B 系統の品質に問題があることがわかる。常時行なっている死活監視でもバックアップを行なっているサーバ類についてもアラートが上がるなど、回線品質の影響により十分な帯域が確保できるアクセスに影響が出ていたものと考えられる。

一方、学外から主要サーバ(学生情報システムや e-learning システム)へのアクセスは、低速ながらも継続してアクセスできることも確認できた。通信経路としての有用性を確認することができたが、品質改善に向けた検討を継続して行う必要がある。

5 まとめ

本稿では、緊急時における商用フレッツ回線を利用したキャンパス間通信のバックアップについて述べた。可用性の確保と維持・運用管理のコストはトレードオフとなるため、冗長化した光ファイバ経路を常時維持することは難しい。比較的安価なフレッツ回線を利用しバックアップ対象とする通信をトリアージ的に必要最低限に絞ることで、緊急的な通信経路の確保を行うことができる。さらに、レイヤ3機能をデータセンターに集約し、VLANID等のレイヤ2の論理リソースを一元管理することで、VLAN単位での選択的バックアップが可能となる。2018年7月の豪雨災害において、損傷したキャンパス間光ファイバの迂回工事に

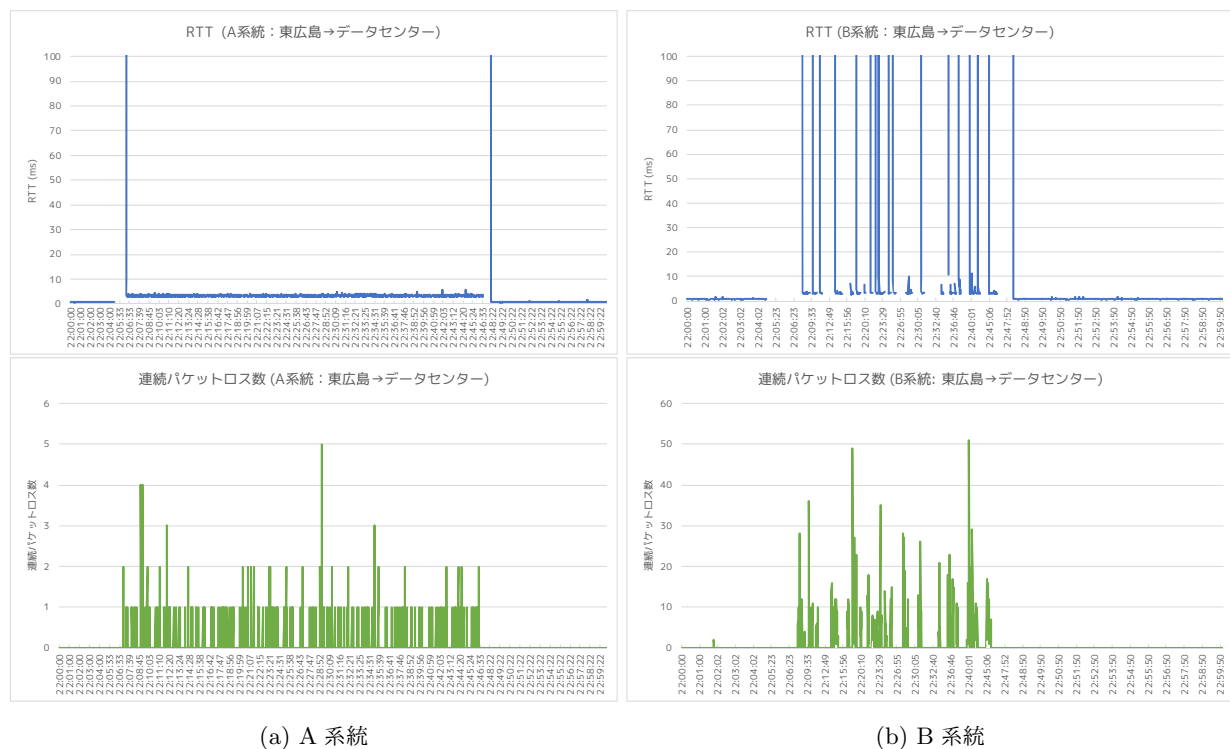


図5 バックアップ期間中の通信品質（7月18日分）

よるキャンパス通信の全断に対して、本バックアップ手法の実践を行い、一定の効果を得ることができたが、通信品質の面での課題は残った。

今後はより品質を考慮しつつ大幅なコスト増にならない回線確保の検討やバックアップ切替の自動化、平常時の活用などを考えていく予定である。また、現時点では特に物理的に距離があるデータセンター～東広島キャンパス間のみをバックアップ対象としているが、今後は他キャンパスへの拡大も検討する。

謝辞

本発表に関する取り組みおよびキャンパスネットワークの運用に尽力頂いている情報メディア教育研究センターおよび財務総務室 情報部 情報化推進グループの関係者各位に感謝致します。

参考文献

- [1] 伊藤智博, 高野勝美, 田島靖久, 吉田浩司, ”災害時に備えた分散キャンパスによる情報基盤の整備”, 学術情報処理研究誌, No.15, pp.5-11, 2011.
- [2] 野口宏, 大瀧保広, 鎌田賢, ”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”, 学術情報処理研究誌, No.16, pp.25-32, 2012.
- [3] 近堂徹, 田島浩一, 岸場清悟, 大東俊博, 岩田則和, 西村浩二, 相原玲二, ”利用者認証機能を備えた大

規模キャンパスネットワークの性能評価”, 第1回 IOT シンポジウム 2008 論文集, pp.121-128, 2008.

- [4] 近堂徹, 田島浩一, 岸場清悟, 吉田朋彦, 岩田則和, 大東俊博, 西村浩二, 相原玲二, ”クラウドコンピューティング活用のための大規模キャンパスネットワーク”, 情報処理学会 インターネットと運用技術シンポジウム (IOTS)2014 論文集, pp.101-108, 2014.
- [5] 近堂徹, 岸場清悟, 西村浩二, 相原玲二, ”パブリッククラウドを利用したスケールアウト型 HPC クラスタの実装”, 情報処理学会研究報告, Vol.2016-IOT-32(26), pp.1-6, 2016.
- [6] 田島 浩一, 岸場 清悟, 近堂 徹, 大東 俊博, 岩田 則和, 西村 浩二, 相原 玲二, ”広島大学におけるセキュリティ脆弱性診断の実施とその評価”, 学術情報処理研究, No.18, pp.16-23, 2014.