Vol.2013-CSEC-61 No.20
Vol.2013-IOT-21 No.20
2013/5/10

可用性向上を目指した佐賀大学のネットワーク構成変更

江藤 博文[1]　大谷 誠[1]　廣友 雅徳[2]　松原 義継[1]　只木 進一[1,a)]

概要：大学の教育、研究、診療、そして組織運営にとって、情報ネットワークは不可欠な基盤となっている。大学の情報基盤は、停止することなくサービスを続けることを期待されている。この期待に応えるためにも、情報ネットワークの可用性を少ないコストで向上させる必要がある。佐賀大学では、SINET4 佐賀ノード接続を機会に、可用性向上を目指して対外接続部分の構成変更を、外部サービス及びデータセンターを活用して行った。その内容は、二つの主要キャンパスへの経路の冗長化と、停電・災害時への対応である。また、安全性向上のため、ドメインネームサーバの構成変更を行った。構成の概要と課題について紹介する。

キーワード：インターネット接続, DNS, 可用性, Flex Link

Improving Network Availability in Saga University

Hirofumi Eto[1]　Makoto Otani[1]　Masanori Hirotomo[2]　Yoshitsugu Matsubara[1]
Shin-ichi Tadaki[1,a)]

Abstract: Information network systems have been indispensable for university activities, such as education, research, medical treatments and administration. Thus university information infrastructure has been requested to provide non-stop services. For meeting those requests, information network systems must improve their availability with small amounts of costs. At the opportunity of connecting to the Saga Node of SINET4, Saga university rearranged the structure of the network system, by out-sourcing and utilizing a data center service. The purpose of the rearrangement is to improve the network availability. In other words, the rearrangement installed the redundant routes for our two main campuses and improved the preparation for fails in electric power supply and disasters. The domain name services were also rearranged for improving their safe services. This report describes the outline of the rearrangement and discusses the remaining problems.

Keywords: Internet connection, DNS, availability, Flex Link

1. はじめに：大学におけるネットワークの重要性と現状

大学における教育、研究、大学病院を擁する大学では診療、そして組織業務のいずれをとっても、情報通信技術は必須の基盤である。これらの情報システム化の近年の顕著な特徴は、それらの業務やシステムがインターネットの常時接続無しには成り立たなくなっている点である。また、それらの業務に必要な情報は、電子メールや Web サービスなどという形でインターネット経由で取得・交換されていることも重要な特徴である。つまり、インターネット接続を含む情報ネットワークは、電気や水道のような、大学の基本的活動を支えるライフラインであり、常に安定に稼働していることが求められている。

このように、情報ネットワークは、大学業務を支えるライフラインと期待されているが、それに応える体制の整備は危うい状況のままである。大学において、コンピュータとインターネットは研究としてスタートした。インターネットが業務を支える基盤となった現在でも、研究としてインターネット接続を構築した当初の影響を残し、業務に

[1] 佐賀大学総合情報基盤センター
Computer and Network Center, Saga University
[2] 佐賀大学大学院工学系研究科
Department of Information Science, Saga University
[a)] tadaki@cc.saga-u.ac.jp

対応できる適切な運用体制の整備は遅れている。大学において情報ネットワークを運用する要員は、情報系センターに属する教員や技術職員、あるいは事務情報部署に属する事務職員である。システムエンジニアのような専門職員を有さない場合が多い。つまり、情報システムを 24 時間 365 日運用するための人的体制、勤務体制ではない状況で、基盤的サービスを運用している状況である。そのため、障害発生時には、これらの職員によるボランティア的対応でなんとかやりくりしているのが現状である。

また、大学の情報系センターの建物の中には、現代の情報システムに対応した専用の建物でないものが多い。従って、電源施設や空調施設、あるいは機密性が不十分、あるいは 24 時間 365 日の連続運転に耐えられない場合が多い。更に、複数キャンパスを有する大学のキャンパス間接続には、冗長性などに課題がある場合もある。

近年の基幹ネットワークの高速化と安定化によって、外部のデータセンターやサービスをネットワークを通じて利用することが急速に普及している。情報システムに限らず、サービスは、大規模化によってコスト削減が期待できることも重要である。大学の情報システムについては、災害時の事業継続計画、電源や空調などの設備投資の縮約、さらに運用コスト削減のために、あるいはより良い汎用的サービス活用のために、データセンターやクラウドサービスの活用の検討が進んでいる。実際に、外部メールサービス利用やデータセンターの活用に関するいくつかの事例が報告されている。佐賀大学においても、メールシステムを市内データセンターへ外注し、可用性向上を図るなどの取組を進めてきた [1]。

本稿では、2012 度に佐賀大学にて実施した、可用性と耐性向上を目指したネットワーク構成の変更について報告する。2011 年 4 月に運用を開始した SINET4 では、13 あったノードの無い県の解消が一つの大きなテーマであった [2]。SINET ノードが無い県の一つであった佐賀県にも 2011 年度末にノードが設置され、2012 年秋に佐賀大学の接続を九州大学経由から佐賀ノードへの直接接続に変更した。これを契機に、データセンターを活用した対外接続とキャンパス間接続の冗長化を実施した。同時に、クラウドサービスを活用して、ネームサーバの耐性強化と可用性向上を実施した。

2. 従来のネットワーク構成の課題

2.1 対外接続回線の状況

佐賀大学は、2004 年に佐賀医科大学と旧佐賀大学が統合して発足した、5 学部を擁する地方総合大学である。医学部と附属病院のある鍋島キャンパスとそれ以外の 4 学部 (理工学部、農学部、文化教育学部、経済学部) のある本庄キャンパスが主要なキャンパスである。全学の情報基盤の整備運用を担う総合情報基盤センターは、両校の情報系センターを統合し、本庄キャンパスにメインセンターを、鍋島キャンパスに医学サブセンターを置く構成となった。事務系の情報システムを担う部署 (現在の総務部情報管理課) は、本庄キャンパスの事務局内に主たる場所を有する体制となった。統合以前には、それぞれが九州大学を経由して SINET に接続していたが、統合時に本庄キャンパスからの接続に一本化を行い、鍋島キャンパスは本庄キャンパス経由の SINET 接続となった。研究センター等の遠隔施設や附属学校 4 校は、フレッツグループサービスにより、本庄キャンパスに接続を一本化している。

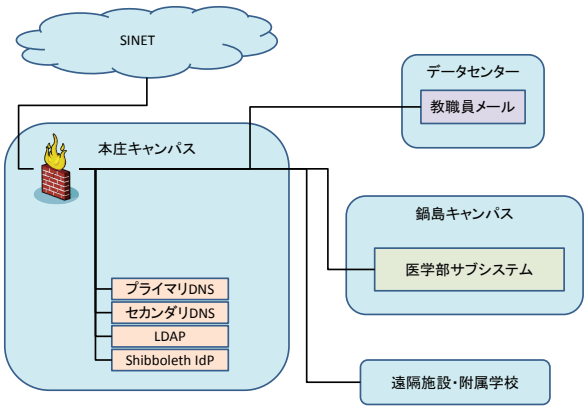


図 1 佐賀大学の従来のネットワーク構成:SINET からの接続は、本庄キャンパスで行い、その下に木構造のネットワークを構築していた。

Fig. 1 Outline of the previous network in Saga University. The whole university network was connected through the Honjo campus and had a tree structure.

2011 年度までの対外ネットワーク接続の概要を図 1 に示す。このようにネットワーク構成は、それぞれのキャンパス内の支線を含めて単純な木構造である。そのため、ネットワークの配送経路管理は、比較的容易であり、障害ポイントの発見も容易であった。一方、この構成では、本庄キャンパスが単一障害点となっており、本庄キャンパスでの停電や障害により、全学がインターネットから切断される状況であった。

例えば、2010 年度以前は、総合情報基盤センターメインセンターの法定点検による停電時には、全学がインターネットから切り離された。各学部は、総合情報基盤センターの停電に加えて自学部の法定点検による停電があるため、年に二度、インターネットから切断されていた。また、落雷や台風、あるいは受電設備の障害で本庄キャンパス全域が停電となり、鍋島キャンパスも含めて全学がインターネットから切り離される事態も発生した。

本庄キャンパスが単一障害点であることの対策として、事前に計画された停電時にネットワークサービスを停止させないための対策を、2010 年 3 月のネットワーク更新時に導入した [3]。主に、夏に行われる電源設備の法定点検を

想定し、その際には外部電源導入により、コアスイッチ、ファイアウォール、DNS、認証システム、利用者用ネットワーク Opengate を無停止でサービス可能とした。なお、教職員用メールサービスはデータセンターへ外注済みであったため、認証サービスの無停止サービスにより、メールサービスも無停止サービスが可能な体制となった。この措置により、総合情報基盤センターの停電時にも、演習室環境などの一部のサービスを除いて、停電を意識しないようになった。

もちろん、このような対策では、急な停電には対応できない。急な停電が発生すれば、本庄キャンパスだけでなく、病院を含む鍋島キャンパスまでインターネットから切断されてしまう。急な停電でも影響範囲をできるだけ小さくするための対策が必要となっていた。

2.2 DNS

ドメインネームシステム (DNS) は、インターネットの初期からあるサービスであり、不可欠なもののひとつである。また、独自のドメインを有する組織は、必ず保有しているサービスである。このサービスにより、名前 (FQDN) と IP アドレスを相互に翻訳し、通信を可能としている。佐賀大学においても、インターネット接続の初期から、プライマリサーバとセカンダリサーバの二重体制で運用を行ってきた。

DNS のサービスには、大きくわけて、二つのサービスが混在している。一つは、組織内部の端末に対して、外部のサーバ等の名前解決を提供する機能である。このサービスでは、組織内部の端末からのリクエストに対する外部からの返答をキャッシュして効率向上を行う。二つ目は、外部からの問い合わせに対して、組織内部のサーバの名前解決を提供する機能である。後者のサービスでは、組織内部の情報を静的に保有する。

近年、上記のキャッシュに悪意ある誤った内容を送り込むことで、端末を悪意あるサイトへと誘導する攻撃が報告されている [4]。組織内部向けと外部向けのサービスを分離し、内部向けサービスが有するキャッシュの汚染を防ぐ運用が必要となっていた。

2011 年 3 月 11 日に多くの犠牲者を出した東日本大震災以降、情報システムを含めた社会基盤の事業継続が関心を集めている。DNS について、事業継続性の観点から考えると、DNS が組織内だけにあることは大きなリスクとなる。災害などで組織内に設置した DNS が一週間程度以上停止する、あるいはインターネットから見えなくなった場合（設定による）、インターネットの世界から当該ドメインが消滅してしまうというリスクが存在する。その対策として、組織外に DNS のバックアップがあることが望ましい。

3. ネットワーク構成の変更

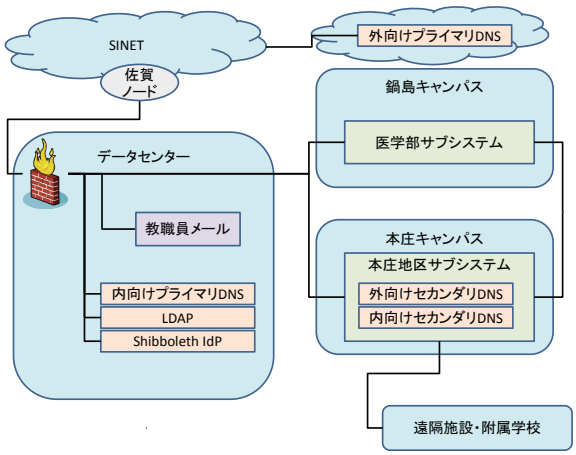


図 2 佐賀大学の現在のネットワーク構成: SINET への接続を佐賀ノードとし、データセンターに接続ポイントを移動した。また、キャンパス間を冗長接続とした。

Fig. 2 Outline of the current network in Saga University. The university network is connected to Saga SINET node through the data center. The connections between the campuses are constructed with redundancy.

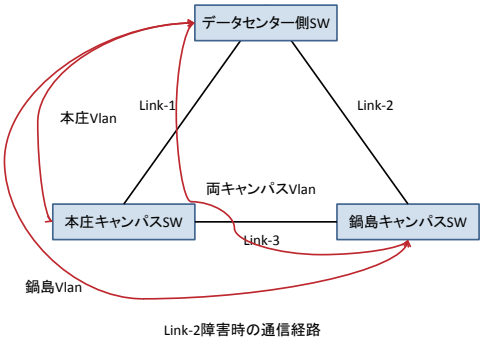
3.1 対外接続

2011 年度末に SINET4 ノードが佐賀市内に設置されたことを受けて、SINET 接続を従来の九州大学経由から佐賀ノードへと 2012 年 9 月に変更を行った。この際に、可用性向上のための対外接続変更を実施した。概要を図 2 に示す。

可用性向上を目指した対外接続変更の第一のポイントは、対外接続ポイントを、従来の本庄キャンパスから市内データセンターへと移動させたことである。電源や空調の安定度が高く、物理的セキュリティレベルの高いデータセンターへと移動させることで、基幹的インターネットサービスの可用性向上を狙った。

基幹的インターネットサービスの可用性向上のためには、対外接続ポイントだけを移動しただけでは不足である。基幹的インターネットサービスを支えるためのサービスも同様以上の可用性が求められる。佐賀大学では、ファイアウォール、認証基盤、及び DNS をデータセンターへ移動することで、可用性向上を図った。前述のように、教職員向けメールサービスはデータセンターへと外注済である。これらの対策により、大学において停電等の障害が発生しても、学外から、メールによる情報交換を継続することが可能となった。

可用性向上を目指した対外接続変更の第二のポイントは、二つのキャンパスとデータセンターを結ぶ接続の冗長化である。従来の接続では、鍋島キャンパスは本庄キャンパス



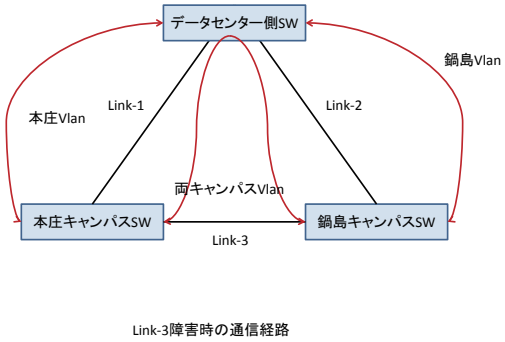


図 3 Flex Link による冗長構成：鍋島キャンパスへの Link-2 が切断した場合には、Link-1 経由で鍋島キャンパスを接続する。

Fig. 3 Redundant structure using flex link mechanism: When the Link-2 connecting Nameshima campus to the data center fails, the Link-1 becomes active for connecting the campus.

図 4 Embedded Event Manager による冗長構成：両キャンパスを結ぶ Link-3 が切断した場合には、spanning tree が有効になる。

Fig. 4 Redundant structure using embedded event manager mechanism: When the Link-2 connecting Nameshima campus to Honjo campus fails, the spanning tree mechanism is activated for connecting both campuses.

の下流となり、本庄キャンパスの障害は鍋島キャンパスのインターネットからの切断を意味していた。今回の変更では、いずれのキャンパスも他方のキャンパスの停電等の影響を受けないように、データセンターへの直接接続とした。また、二つのキャンパスとデータセンターを結ぶ回線の冗長化として、複数のキャリアの回線を活用した三角形の構成とした。これにより、障害やキャリアの工事などによって回線の一つが切断しても、迂回路を使って、両キャンパス間の通信及びインターネット接続を確保した。経路の切り替えは、Flex Link と Embedded Event Manager を用いて制御を行う設定とした。

3.2 Flex Link と Embedded Event Manager による冗長化

Flex Link は、二つのポートでの通信を切り替える冗長構成の方法である [5]。通信経路が二つある場合、通常時に使用するポート側を「アクティブ」、バックアップ時に使用するポートを「スタンドバイ」と呼ぶ。アクティブ側のポートに接続した回線に障害があった場合に、スタンドバイ側に接続した回線に自動的に切り替えることができる。図 2 に示した、佐賀大学の現在のネットワーク構成では、データセンタに設置したスイッチに Flex Link の機能を設定している。

佐賀大学では、各サブネットに対応した vlan を設定し、運用している。学科や建物、事務系、特殊な用途のネットワークなどに vlan が割り当てられている。それらは、本庄キャンパスだけで使われているもの、鍋島キャンパスだけで使われているもの、両キャンパスで使われているものからなる。

Flex Link を使ったネットワーク構成と障害時の経路変更の概念図を図 3 に示す。データセンターに設置したスイッチには、本庄キャンパスで使用する vlan に対しては、本庄キャンパスに直結した Link-1 がアクティブに、鍋島キャンパスへ向かう Link-2 がスタンドバイに設定されている。鍋島キャンパスで使用する vlan に対しては、その逆の設定となっている。

図 3 には、鍋島キャンパスとデータセンターを結ぶ Link-2 が切断した場合の通信経路を示している。Link-2 に障害が発生した場合、データセンターに設置したスイッチが検知する。鍋島キャンパスが使用する vlan のためのリンクが停止したため、Flex Link 機能が、スタンドバイである Link-1 を鍋島キャンパスが使用する vlan に対するアクティブな経路に変更する。これにより、鍋島キャンパスが使用する vlan が、データセンターから本庄キャンパスを経由して、鍋島キャンパスに到達する。このような vlan 情報の変更を可能とするためには、両キャンパスのコアスイッチに許容される vlan が共通でなければならない。

佐賀大学で設定している多くの vlan は、本庄キャンパスの中だけ、あるいは鍋島キャンパスの中だけで使用している。これらの vlan については、データセンターへと通じる Link-1 及び Link-2 に障害がなければ、両キャンパスを結ぶ Link-3 が停止していても支障はなし。しかし、事務系ネットワークや内線電話など、両キャンパスに跨る vlan がいくつかある。これらについては、Link-3 の停止は通信障害となる。Flex Link の機能はデータセンターに設置したスイッチの機能であるため、Link-3 の障害を検知することができない。そこで、本庄キャンパスのコアスイッチに Embedded Event Manager (EEM) を設定することで冗長性を確保している。

Embedded Event Manager は、スイッチ内部でのイベントを検知し、設定変更などを行う仕組みである [6]。本庄キャンパスのコアスイッチには、鍋島キャンパスを直接結ぶ Link-3 のオン・オフのイベントを検知する設定を行っている。

Link-3 の停止を検知すると、本庄キャンパスのコアスイッチは、データセンター設置のスイッチに接続し、Flex Link を解除し、Spanning Tree を有効にする (図 4)。これにより、両キャンパスのそれぞれの vlan、及び両キャンパスに跨る vlan が有効となる。Link-3 の回復を検知すると、Spanning Tree が無効化され、Flex Link が有効となる。

以上のように、Flex Link と EEM を機能を用いることで、データセンターと両キャンパスを結ぶ三角形の経路のうち、一つの経路が切断した場合には、自動で通信を確保することができる。

3.3 DNS

佐賀大学の従来の DNS の構成には、二つの大きな課題があった。内部向けサービスと外部向けサービスの区別が無いことと、二台のサーバのいずれも本庄キャンパスに設置していたことである。対外接続の変更に合わせて、こらも可用性向上を目指した変更を行った。

第一に、内部向けと外部向けを分離し、それぞれを二台ずつの構成とした。学内の端末やサーバには、ネームサーバの名前と IP アドレスが静的に記述されているものが多い。利用者らに、これらを変更してもらうことは、非常に困難である。そのため、二台の新規サーバを構築し、それらを外部向けとした。併せて、部局等が運用するサブドメインの DNS について、その設定内容の精査を行い、改善を行った。

内部向けサービスは、学内からの問い合わせに答える必要がある。そのため、過去の問い合わせをキャッシュして効率化するとともに、必要に応じて再帰問い合わせを行う。また、外部からのキャッシュ汚染の攻撃を防ぐために、ファイアウォールによって外部から隔離した。もちろん、内部の端末やサーバの情報と、学内の部局サブドメインのセカンダリサーバとしての役割も担っている。

外部向けサービスは、学外から、学内の端末やサーバの情報問い合わせに答えるのが役割である。そのため、学内情報を信頼できる内部向け DNS から受け取れば十分である。そのため、再帰問い合わせとキャッシュを停止した。これにより、キャッシュ汚染などの攻撃のリスクを軽減した。

第二に、可用性向上のため、内部向けと外部向け、それぞれのプライマリサーバを本庄キャンパス外に設置した。内部向けプライマリサーバは、データセンターに設置し、本庄キャンパス障害時にも鍋島キャンパスからのインターネット接続を確保した。外部向けプライマリサーバは、学外の仮想サーバサービスを利用して構築し、可用性を向上した。

図 5 に新しい DNS サービスの構成概要を示す。図中の破線は、ゾーン転送の経路を表している。内部向けキャッシュサーバ及び部局サブネットの情報を、外部向け副コンテンツサーバにゾーン転送を行っている。その後、副コンテンツサーバから、クラウド上に設置された主コンテンツサーバに向けて、証明付きでゾーン転送を行い、データの完全性を確認している。

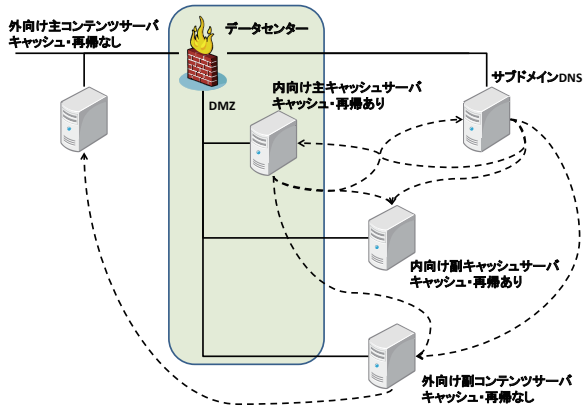


図 5 佐賀大学の現在の DNS 構成: 外部向けコンテンツサーバと内部向けキャッシュサーバへと分離した。破線はゾーン転送の流れを表す。

Fig. 5 Outline of the current DNS configuration in Saga University. The system consists of the content servers for external users and the cache servers for internal users. The broken lines denote the data flow of zone transfer.

4. まとめと今後の課題

情報ネットワークは、大学の活動にとって不可欠な基盤となっている。一方で、大学の情報基盤を担う現状の建物と人員だけで、内部の情報ネットワークとインターネット接続サービスを無停止で運用することは容易ではない。そのため、大学の情報基盤の一部をデータセンターやクラウドサービスに移行することで、コスト削減を図りつつ、可用性を高める試みが行われている。佐賀大学においては、教職員メールのデータセンターへの外注に続いて、SINET4 佐賀ノードへの接続変更を機会に、対外接続ポイントをデータセンターに移動し、更に多重化するなどの、可用性向上を目指した構成変更を実施した。

対外接続ポイントと基幹ネットワークサービスを電源及び空調設備の整ったデータセンターに移動したことで、可用性を大きく向上させることができた。つまり、総合情報基盤センターのメインセンターでの障害時でも、鍋島キャンパスからのインターネット接続と、インターネット側からのメール利用を継続することができるようになった。ま

た、毎年実施しなくてはならない総合情報基盤センターのメインセンターでの法定点検に伴う計画停電に際しても、外部電源によるサービス提供のための電源規模や作業工数を縮小できることが期待される。

対外接続ポイントと基幹ネットワークサービスをデータセンターに移動させることで、安定な電源供給と空調環境によって守ることができた。一方で、ファイアウォール装置がデータセンターへ移動したことで、回線確保の重要度が大きくなった。佐賀大学では、一つのファイアウォール装置に多数のファイアウォール機能を仮想的に持たせることで、機材と運用コストの軽減を図っている。つまり、一つのファイアウォール装置の中に、学内と学外を隔てるファイアウオール機能の他に、いくつかのプライベートネットワークの NAT 機能、セキュリティレベルの異なるネットワークを隔てるファイアウォール機能を持たせている。従って、データセンターへの通信障害は、同一キャンパス内での通信障害を誘発する。そのため、両キャンパスから、常にデータセンター設置のファイアウォール装置が見える必要がある。そのために、Flex Link と EEM を用いて、回線切断時に自動で経路を切り替える仕組みを導入した。なお、ファイアウォール装置は二台の冗長構成となっている。

災害時には、大学の被害状況、復旧へ向けた様々な日程など、大学からの迅速な情報提供が重要である。そのためには、メールだけでなく、大学の公式 Web などの情報交換、情報流通手段を、キャンパス外のデータセンター、あるいは外部サービスへと移行させる必要がある。災害時の体制の整備とともに、検討をする必要がある。

佐賀大学には、5 か所の遠隔研究施設と 4 校の附属学校がある。これらの接続は、本庄キャンパスの下流のままである。これらの組織のネットワーク安定化のためには、接続ポイントをデータセンターへ移行するなどの対策が必要であり、今後の検討課題である。特に、附属学校ネットワークの可用性向上は重要な課題である。

教職員メールサービスは、データセンターに外注済みであり、今回の接続変更により可用性を大きく向上させることができた。一方、学生用メールサービスは、ウィルスメール及び SPAM メール対策はデータセンターを設置する一方、送信及び受信サービスを学内に設置している。メールは大規模災害時の学生への重要な連絡手段であるため、利便性とコスト、学生が主に使用する携帯端末との関係などを考慮した対策が必要である。

謝辞 SINET4 への接続を支援して頂いた、株式会社佐賀 IDC に感謝いたします。また、冗長構成の構築をして頂いたネットワンシステムズ株式会社に感謝いたします。

参考文献

[1] 松原義継, 大谷　誠, 江藤博文, 渡辺健次, 只木進一：プライベートクラウドによる電子メール管理コストの低減とサービスレベルの改善-佐賀大学の事例-，情報処理学会研究報告. IOT, [インターネットと運用技術]， Vol. 2011-IOT-14, No. 8, pp. 1–6 (2011).

[2] 国立情報学研究所：学術情報ネットワーク，http://www.sinet.ad.jp/.

[3] 只木進一，田中芳雄，小野隆久，渡辺健次：情報系センターの停電対策と電源管理，情報処理学会研究報告. IOT, [インターネットと運用技術]， Vol. 2011-IOT-15, No. 8, pp. 1–5 (2011).

[4] サイエンティフィックシステム研究会：情報化された組織のセキュリティマネジメント WG 成果報告書，https://www.ssken.gr.jp/MAINSITE/download/wg_report/info-secmng/.

[5] Cisco Systems: Catalyst 3750 Metro スイッチ ソフトウェアコンフィギュレーション ガイド Cisco IOS Release 12.2(25)EY，http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/sw/cat3750m/cat3750mscg/chapter20/16793_01_20.shtml.

[6] Cisco Systems: Cisco IOS ネットワーク管理コンフィギュレーション ガイド - Embedded Event Manager 概要，http://www.cisco.com/cisco/web/support/JP/docs/CIAN/IOS/IOS15_1M_T/CG/009/nm_eem_overview.html?bid=0900e4b18252971b.