災害時に備えた分散キャンパスによる情報基盤の整備

Construction of robust information infrastructures for disaster in decentralized campus

伊藤智博[†,†‡]，高野勝美[†,†‡]，田島靖久[‡,†‡]，吉田浩司[‡,†‡]
Tomohiro Ito[†,†‡], Katsumi Takano[†,†‡], Yasuhisa Tajima[‡,†‡], Hiroshi Yoshida[‡,†‡]
tomohiro_ito@ieee.org, ktakano@ieee.org, tajima@sci.kj.yamagata-u.ac.jp, yoshida@ncsc.yamagata-u.ac.jp

† 山形大学大学院理工学研究科
‡ 山形大学基盤教育院
† ‡ 山形大学情報ネットワークセンター
992-8510 米沢市城南 4-3-16

† Graduate School of Science and Engineering, Yamagata University,
‡ Institute of Arts and Sciences, Yamagata University
† ‡ Networking and Computing Service Center, Yamagata University
4-3-16 Johnan, Yonezawa 992-8510 Japan

概要

山形大学では，ネットワークを安定に運用するために様々な試みがなされてきた．2011 年 3 月 11 日に発生した東日本大震災以前には，比較的安価な商用 ISP によるバックアップ回線を準備し，ファイアウォールの複数 ISP 接続機能と DNS のラウンドロビン機能によるインバウンド通信の冗長化技術を構築していた．震災による停電によって，この冗長化構成が施されたサーバについては，学外から本学のサービスを利用することができた．一方，この冗長化技術だけでは，学内から学外への通信はできなかったため，震災後，アウトバウンド通信の冗長化技術を導入した．本稿では，震災前，震災時および震災後に実施した情報基盤を取り囲む様々な対応について報告する．

キーワード

ネットワーク，冗長化， WAN リンクロードバランシング，シボレス認証

1. はじめに

学内 LAN(Local Area Network)を始めとする情報基盤は，大学において日夜停止することなく運用されるネットワークであり，教育研究や業務などで広く利用されている．履修登録システムの Web 化や IC カードによる出席管理，キャンパス間の内線電話の VoIP 化などの様々な分野において，情報基盤が必要不可欠になってきている[1]．また，ブロードバンドネットワークの普及や公衆無線 LAN，WiMAX などの普及により，インターネットへの接続で

きる場所が広がりを見せており，ネットワークインフラが教育や生活の中で重要な位置づけになってきている．大規模災害時には，学生への情報発信や安否確認などでもインターネットが利用されるなど，情報基盤は教育や業務のみならず，大規模災害発生時の緊急用連絡手段としても必要不可欠な存在となっている[2],[3].

本学における学内 LAN システムである山形大学情報通信ネットワークシステムには，障害が発生したときのことを想定していくつかの試みがなされてきた. 一般に，障害に強いネットワーク構成するためには，Border Gateway Protocol (BGP)によるマルチホームを構成することが多い．本学では，表 1 に示すように，複数の冗長化方式を費用面および運用面から検討した．一般的な BGP によるマルチホーム接続は，インバウンド／アウトバウンド通信を相互に冗長化できるなど利点が大きい．しかし，高価な商用 ISP の回線が必要になることや経路障害を自力で解決できる人材の育成が必要になることから，BGP の導入には至らなかった．地理的負荷分散装置などによってもインバウンド／アウトバウンド通信を冗長化することが可能であるが，機器の導入費用が高額なことから，断念した．あくまで，一時的な障害発生時に，重要な通信（DNS サービスやメールの受信）のみを可能にすればよいと考えると，高額な回線費用や機器の導入，運用面での人的なコストの増大を行ってまで，BGP などによるインバウンド／アウトバウンドの通信の冗長化は不要であると判断した．そこで，緊急時の通信の確保のために比較的安価な商用 ISP によるバックアップ回線を準備し，ファイアウォールの複数 ISP 機能と DNS のラウンドロビン機能によるインバウンド通信の冗長化技術を取り入れた．特に，本学は，50km 以上離れた場所に複数のキャンパス（山形市，米沢市，鶴岡市）を有する分散キャンパスである．この分散キャンパスを活用して，複数のキャンパスに DNS サーバを配置したり，メールのトランスポートサーバを複数回線に接続したり，様々な手法で，緊急時のバックアップ機能について試みてきた.

2011 年 3 月 11 日に発生した東日本大震災においては，本学の情報基盤の要となっている小白川キャンパスが停電になり，インターネットと接続している主回線が停止した．震災以前には，長時間の障害を想定していなかったため，インバウンド通信における冗長化や負荷分散技術の運用が導入されていた．震災以降は，長時間の障害が発生することを想定して，アウトバウンドの通信における冗長化技術が試験的に導入された．さらに，大規模震災時の安否確認システムとして，学術認証フェデレーション（学認）[4]で採用されているシボレス認証を利用して構築した．本稿では，震災前，震災時および震災後に実施した情報基盤を取り囲む様々な対応について報告する.

以下，第 2 節では，震災前に試みられてきた情報基盤の障害対応および冗長化構成について述べ, 第 3 節では, 震災後に導入された情報通信基盤の冗長化構成について述べる.

表 1 冗長化方式の違いによる効果および費用面，運用面から導入検討事項

検討項目	冗長化方式		
	マルチホーム／BGP	地理的負荷分散	DNS ラウンドロビン
冗長回線費用 a)	数十万円～/月	数万円/月	数万円/月
機器導入費用	500 万円程度 b)	1000 万円以上 c)	0 円 d)
効果および利点	・インバウンド／アウトバウンドの通信が冗長化 ・インバウンド／アウトバウンドの通信が等価であるため IP 認証にも対応	・インバウンド通信が冗長化 ・回線が低価格 ・回線障害時に DNS の自動変更が可能 ・設計次第では，アウトバンドの冗長化も可能	・一部の回線に障害が発生したときに，ラウンドロビンによるインバウンド通信が可能 ・回線が低価格 ・短期間で導入可能
欠点・運用面の問題	・回線費用が高い ・導入機器が高価 ・経路障害は自力で解決することが前提のため，運用コストが増大および長期的な人材の育成が必要 ・機器の調達が必要なため導入までの期間が長い	・導入機器が高価 ・インバウンド／アウトバウンド通信時の IP アドレスが異なる場合があるため，IP 認証には対応不可能 ・機器の調達が必要なため導入までの期間が長い	・回線障害時に DNS の手動変更必要 ・アウトバウンド通信の冗長化が難しい ・インバウンド／アウトバウンド通信時の IP アドレスが異なる場合があるため，IP 認証には対応不可能

a) バックアップ回線のため，帯域は，10 Mbps 程度で算出. b) CISCO 社製 ASR 1002（フルルート対応，スループット数 Gbps）を導入したと仮定. c) F5 社製 BIG-IP Local Traffic Manager に Global Traffic Manager モジュールを導入したと仮定.
d) 本学で導入済みのファイアウォールは，導入時より，複数 ISP 機能に対応していたので，費用負担は発生しない.

2. 震災前の情報基盤

2011 年 3 月 11 日に発生した東日本大震災前に，障害発生時を想定して，複数回線の引き込みや DNS サーバの複数回線による冗長化などの様々な実証実験が試みられてきた．震災時および震災後の情報基盤の整備は，この実証実験の試みを基盤として，今後の大規模災害に備えるために拡張されたものであるので，本節では震災前までの情報基盤の概要と試みされてきた冗長化技術について述べる．

2.1. ネットワークの構成

2011 年 3 月 11 日の時点での本学におけるキャンパス内ネットワークは，図 1 に示すように，小白川キャンパスを中心としたスターネットワークによって，4 つのキャンパスを接続している．キャンパス間の通信は，1Gbps の 1 対 1 接続の専用線とイーサーネット網による 100Mbps のサービス回線の 2 つの回線に接続されている．平常時には，キャンパス間のデータ通信は前者の専用回線を利用し，後者は VoIP によるキャンパス間の内線電話などに利用されている．どちらか一方の回線が遮断されたときは，自動的にもう一方の回線に切り替わるように冗長化されている．通常のインターネットへのアクセスは，主回線である専用線を使用して，東北学術研究インターネットコミュニティ(TOPIC)に接続している．主回線に障害が発生したときを想定して，バックアップ用の回線として，米沢キャンパス内に商用 ISP，地域 IP 網経由の SINET の回線が引き込まれている．また，研究用の回線として，JGN2plus を経由して WIDE プロジェクトに接続している[5][6]．それぞれの回線の特徴を下記に示す．

[専用線による TOPIC への接続(回線 A)]
接続：小白川キャンパスから専用線にて TOPIC に接続
回線速度： 最大 約 100Mbps
備考：2011 年 3 月 30 日より SINET4-山形 DC に 10Gbps の専用線接続に変更．

[商用 ISP による接続（回線 B）]
接続：米沢キャンパスから商用 ISP に接続
回線速度： ベストエフォート 20Mbps
備考：DNS のバックアップ用および研究用回線

[JGN 経由による WIDE プロジェクト接続（回線 C）]
接続：小白川キャンパスから JGN2plus への接続
回線速度： 最大 約 1.0Gbps
備考：研究用回線，JGN2plus プロジェクトの終了および山形 AP の廃止に伴い 2011 年 3 月 9 日に停止

[地域 IP 網経由による SINET4 接続（回線 D）]
接続：米沢キャンパスから地域 IP 網に接続
回線速度： ベストエフォート 100Mbps
備考：主に研究利用のための回線

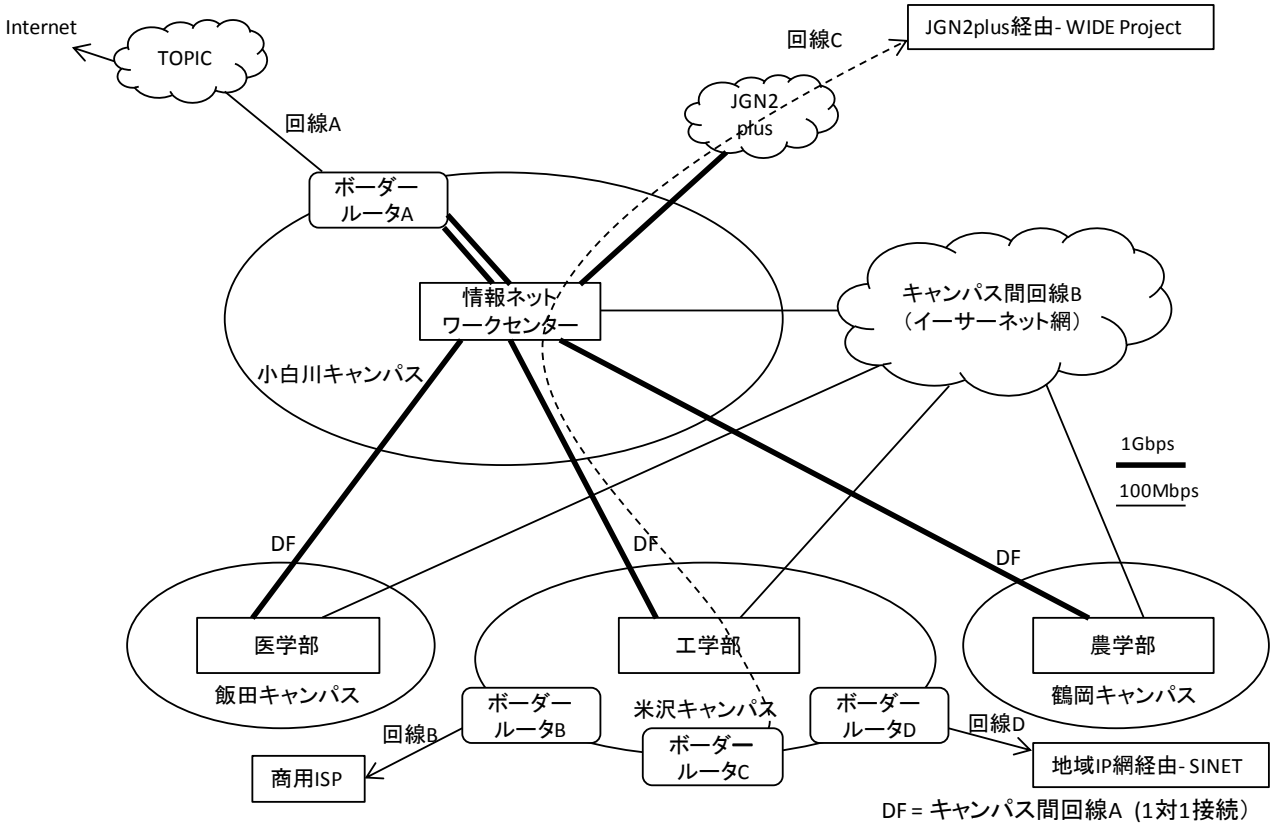

図 1 外部回線およびキャンパス間回線の構成

2.2. DNS サーバの分散配置

DNS サーバが停止または回線障害で通信不能になった場合，外部機関の利用者から本学のサーバの名前解決ができなくなり，本学の外部利用者のサービスが全て停止することになる．そこで，本学では，表 2 に示すように，DNS コンテンツサーバを 3 つのキャンパスに分散配置し，トップドメインの名前空間および PI アドレスの逆引きレコードの要求に応答できるようになっている．すなわち，主回線である回線 A に障害が発生しても，バックアップ回線である回線 B によって DNS コンテンツサーバに通信ができるため，外部利用者への DNS サービスを提供できるようになっている．また，複数キャンパスに配置したことによって，キャンパス間接続用のコアスイッチなどに障害が発生した場合でも DNS サービスを継続できるようになっている．

表 2 DNS サーバの配置構成

サーバ名	設置キャンパス	接続回線
dns0	小白川	回線 A
dns1	飯田	回線 A
dns2	米沢	回線 A
dns4	米沢	回線 B

2.3. バックアップ回線によるリモート接続

ブロードバンドネットワークの普及に伴い，これを経由した学外から学内 LAN への接続サービスの利用を求める要望が出てきた．この要望に対応するために，2005 年から本学の工学部を対象に，IPSec VPN によるリモート接続サービスが試験的に展開された．導入当初より，主回線の障害時に，リモートからの障害対応ができなくなる問題があったため，VPN 装置は，バックアップ回線（回線 B）を使用して，学外からのリモート接続サービスを提供することにした．すなわち，主回線や上位 ISP である TOPIC に障害が発生した場合でも，学内 LAN に接続し，リモートから障害対応およびインシデントなどへの初期対応が可能になっている．

2.4. 認証情報の分散配置

認証サービスは，計算機の利用やリモート接続，e-ラーニングなどのコンテンツ利用など様々なサービスを展開するために必要不可欠なもとのなっている．同一拠点に複数の認証サーバを配置して同期したとしても落雷や火災などによって，複数台のサーバが同時に故障し認証サービスの継続性が失われることが予想される．本学の学術研究用アカウントの認証システムは，Active Directory を採用し，ドメインコントローラーを複数キャンパスに分散配置することによって，認証サービスの継続性を保っている．

2.5. インバウンド通信の冗長化

複数回線を用いた冗長化方式としては，一般的な BGP によるマルチホーム接続が行われているが，本学では，運用面やコスト面の問題から導入されていない．そこで，1 つのホスト名のサーバに対して，A レコードや MX レコードに複数回線の IP アドレスを登録する DNS ラウンドロビンによる冗長化方式を採用し，図 2 に示すように構築した．具体的には，ファイアウォールに，回線 A，B，D の 3 つの外部回線を接続する．ファイアウォールの内部ネットワークは，プライベート IP が採用され，物理サーバが接続されている．外部機関からのインバウンド通信は，ファイアウォールの Network Address Translation (NAT)機能によって接続される．また，ファイアウォールのデフォルトゲートウェイのメトリックは，小さい方から回線 A，回線 B，回線 D の順番になるように設定された．アウトバウントの通信は，経路テーブルの回線コストの小さい方から選択されるため，回線 A のみによる通信となる．一方，インバウンドの通信は，ファイアウォールのセッション管理機能により，経路テーブルの回線コストに関わらずリクエストを受信した回線による通信となる．

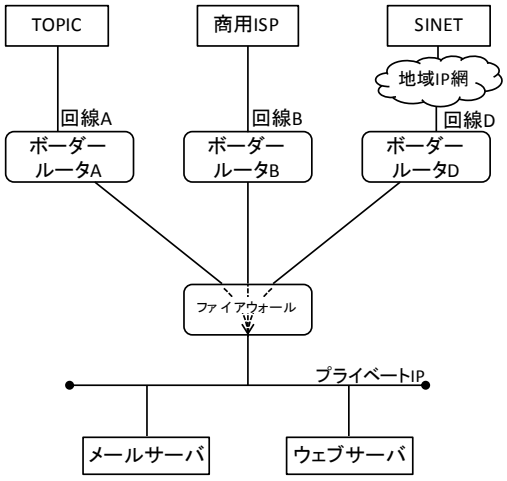

図 2　インバウンド通信の冗長化構成

実施したサービスとしては，工学部の教職員向けのメールサービスとバーチャルウェブホスティングサービスが， DNS ラウンドロビンによって冗長化されている．この手法の問題点としては，リンクの状態を監視して DNS サーバの登録情報を自動的に変更できないため，障害の発生している回線を選択した場合に，通信ができなくなる．この問題を解決する手段として，地理的負荷分散機能や WAN リンクロードバランシング機能があるが，

専用のネットワーク装置を必要とし，ハードウェア的にもライセンス的にも高価な装置であるため導入を断念した.

2.6. 重みつき DNS ラウンドロビン

DNS ラウンドロビンを用いることによって，冗長化および回線負荷の軽減は可能である．しかし，回線の容量に関わらず均等に回線が選択されるため，大容量の通信を行った場合，回線容量の低い回線は，回線帯域が飽和するなどの問題がある．この問題を解決する 1 つの手段として，重みつき DNS ラウンドロビンを採用した．具体的には，回線 A と回線 D を使用して，本学の Anonymous FTP サーバを利用して，重みつき負荷分散について試験的に運用した．一般に DNS サーバに利用されているアプリケーションとして，BIND，djbdns，Microsoft DNS Server などがあるが，重みつきの DNS レコードを取りあつかうことができない．また，地理的負荷分散装置に搭載されている Global Server Load Balancing (GSLB)や Global Traffic Manager (GTM)などの機能を利用することによって重みつき DNS ラウンドロビンは可能であるが, これらの機能を有するシステムは, 高価なライセンスや通信機器が必要であるため，予算的な理由により断念した．実験的であるため，図 3 に示すように，2 台の DNS サーバを立ち上げ，それぞれのサーバの A レコードに，回線 A と回線 D の A レコードを登録した．具体的には，DNS サーバ 1(DNS1)には，回線 A の IP アドレスを，DNS サーバ 2(DNS2)には，回線 D の IP アドレスを登録した．次に，負荷分散装置の DNS サービスに関する負荷分散先のリアルサーバの比が DNS1:DNS2 = 1:10 になるように設定した. このように設定することによって，回線帯域の異なるインバウンド通信の回線の帯域使用率の平滑化が可能になった.

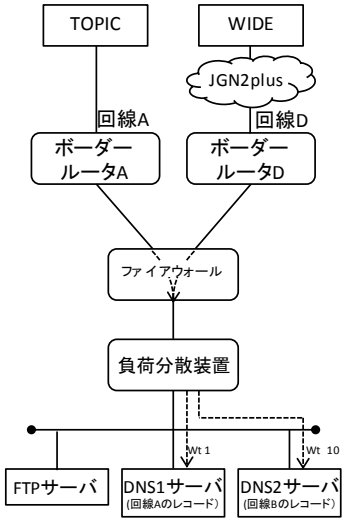

図 3　重みつき DNS ラウンドロビンの構成

3. 震災時および震災後の情報基盤

震災前の情報基盤の冗長化への試みは，前節で述べたとおりであるが，大規模災害を想定した冗長構成ではないため，様々な対応が必要となったので，本節では震災直後の状況やその後の対応について述べる.

3.1. 震災発生直後の状況

東日本大震災の発生直後に，東北地方では，停電が発生し，本学の主回線を収容している小白川キャンパスが停電となった．これに伴い，本学の外部接続用のボーダールータや DNS サーバ, コアスイッチなど停止により，主回線による外部接続が不可能になった．米沢キャンパスでは幸い停電が発生しなかったので，バックアップ回線は正常に利用でき，DNS サービス，リモート接続，インバウンド冗長化によって構成されていたメールサービスは，正常に動作していた．インバウンド冗長化によって構成されたウェブサービスについて，ラウンドロビンのため，エラーになることもあったが，ウェブの閲覧は可能であった. 一方, メールの送信サービスについては, 主回線のみによる送信を想定していたため，小白川キャンパスが復電した 3 月 14 日の朝までは, 全く送信できない状況であった．工学部のネットワークトポロジーの変更によりバックアップ回線によるメールの送信も可能であったが，主回線が回復したときの影響や想定外の障害の発生による全学のネットワーク機能の停止のリスクを考慮して，メールの送信機能の緊急復旧作業は実施しなかった.

3.2. 計画停電への対応

震災後, 東北電力管内でも 3 月 16 日より計画停電が予定された．実際には，計画停電は行われなかったが，初日の計画停電の対象エリアに，米沢キャンパスが含まれていたことや震災後の経過日数が少なく緊急時の情報発信サービスの必要性が高いことから，緊急対応として，外部サービスへの移行作業を実施した．具体的には，3 月 15 日の夕方より, アカマイサービスに工学部の緊急用ホームページのみを移行した．移行作業は，3 月 16 日の午前 1 時に完了した． 4 月 7 日に発生した最大震度 6 強の余震による停電では，山形市が停電になったため，主回線との通信が切断され，本学と学外との通信は不能になったが，工学部の緊急用ホームページはアカマイサイトに移行していたので，問題なく閲覧できた.

3.3. アウトバウンド通信の冗長化

本学の主回線に障害が発生した場合に，工学部のメールの受信は可能であるが, 送信ができない問題があった. この問題を解決するためには，アウトバウンド回線の冗長化が必要となる．アウトバンド通信を冗長化する方法としては, 複数キャンパスを活用して BGP によるマルチホーム化を行うことが，IP 認証によるサービスへの影響がないことや全学的なインバウンド通信を含めて冗長化できることなどから有効であろう. しかし, この手法は, 冗長化のための商用回線の調達が必要であるため，予算面や運用面を考慮すると早急に実施できるものではない. 一方，ICMP を用いて回線のリンク状態を監視し，障害発生時には，NAT 機能を用いて切り替える WAN リンクロードランシング方式がある．工学部には，WAN リンクモニタリング機能を有している UTM 装置（FortiGate; フォーティネットジャパン株式会社）が設置されている. この方式を採用する場合，新たな設備投資が発生しないことや構成変更によるネットワークの停止を伴わずに実施できること，比較的短い時間で実施できることから，WAN リンクロードランシング方式による冗長化を実施した.

具体的な構成は，図 4 に示すように，通常時のアウトバウンド通信は，小白川キャンパスに設置されたボーダールータ A を経由して，主回線からインターネットにアクセスする．もし，小白川キャンパスが停電などによって機能停止した場合，ICMP による死活監視機能が障害を検知し，工学部のアウトバウンド通信は，自動的にバックアップ回線に切り替わる．これによって，工学部の通信は，メールの送信のみならず，ウェブの閲覧なども障害発生時に継続的に利用できるようになっている.

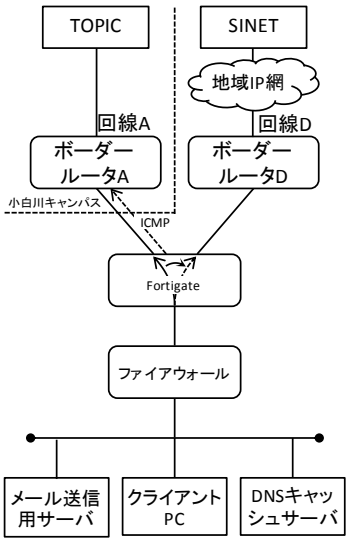

図 4 アウトバウンド通信の冗長化構成

3.4. 安否確認システムの構築

震災から数日経過し，電話回線などの通信網の規制が解除されるにつれて，学生などの安否確認の要請が高まり，インターネット経由による安否確認システムの構築が必要となった．重要なポイントは，短期間で安否確認システムを構築することであった．幸い震災による被害は少なく，認証システムやデータベースサービス，ウェブサービス，メールシステム，学認用 Shibboleth IdP サービスへの被害はなかったため，十分なリソースが利用できることが確認できた．認証サービスは，既に運用を開始している学認用 Shibboleth IdP サーバを利用することによって，開発期間の短縮を図った．さらにウェブサービスは，学認に提供しているサービスプロバイダー(SP)である科学技術の学術情報共有のための双方向コミュニケーションサービスのサイトを機能拡張することによって，新規のデジタル証明書の取得やシボレス SP の新規インストール作業などの時間を短縮した.

開発されたシステムは，図 5 に示すように，利用者はウェブサーバに接続し，認証要求のため，本学の IdP サーバにリダイレクトされる．認証が完了するとウェブサーバにリダイレクトされ，安否情報を送信する．送信された安否情報は，安否確認者にメールが送信されると同時に，データベース内に記録される．安否確認者は，メールの受信または Access などのデータベースソフトウェアを使用して, ODBC 経由でデータベースを参照して，安否情報を確認できる．学認の IdP システムおよび既存の SP を利用したことによって，安否確認システムの開発は，6 時間程度で完了した.

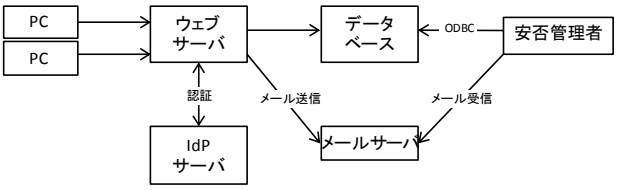

図 5 安否確認システムの概略図

4. まとめ

震災前に実施した様々な障害対応機能を基盤に，震災を踏まえて，災害時に備えた分散キャンパスによる情報基盤の整備を行った．震災前は，インバウンドの通信を中心に冗長化を試みており，それなりの効果があった. しかし，アウトバンドの通信については，全く対応していない冗長化システムであった．震災によって発生した 2 日以上の停電を考慮すると，大規模災害に備えたアウトバンド通信の冗長化システムの構築が必要不可欠であると判断した. 比較的安価な商用回線や地域 IP 網を利用

して，WAN リンクロードランシング方式によるアウトバウンド回線の冗長化システムを米沢キャンパス内に導入した．また，震災による情報基盤への障害や故障が小さかったことや学内でフラットに利用できるシボレス認証を既に採用していたことが幸いして，短時間で安否確認システムの構築することができた．長期的な運用を見つめると BGP によるマルチホーム接続が適切な選択であろうが，短期間で，震災に備える手段としては，安価な ISP 回線と WAN リンクロードランシング方式による冗長化構成も１つの解決策になるであろう．

今後の課題としては，現在，インバウンドおよびアウトバウンドの冗長化構成は，工学部のみであるため，全学規模の冗長化構成を進めることが必要であろう．

謝辞

IPv6 ネットワークを提供していただきました JGN2plus および WIDE プロジェクトの皆様に深く感謝申し上げます．計画停電の対応のために，「アカマイ」東日本大地震緊急配信無償提供プログラムを提供していただきましたアカマイ・テクノロジーズ合同会社様に深く感謝申しあげます．震災時の緊急対応を進めるにあたり，ご指導・ご協力を賜りました情報担当副学長，情報系センター，工学部執行部の皆様に深く感謝申しあげます．

参考文献

[1] 清水さや子，横田賢史，戸田勝善，吉田次郎：東京海洋大学における IC カード学生証の運用・評価および今後の展開，学術情報処理研究誌，No.13，pp. 64-73 (2009).

[2] 越後 博之，湯瀬 裕昭，千川 剛史，沢野 伸浩，高畑 一夫，柴田 義孝：大規模分散環境におけるロバストネスを考慮した広域災害情報共有システム，情報処理学会論文誌，Vol. 48，No. 7，pp. 2340-2350 (2007).

[3] 長谷川孝博，井上春樹，八巻直一：低コスト運用でユーザフレンドリな安否情報システムの開発，学術情報処理研究誌，No.13，pp. 91-98 (2009).

[4] 学術認証フェデレーション，https://www.gakunin.jp/

[5] 山本成一，金海好彦，中村一彦，三宅喬，長谷部克幸，太田善之，田中仁，美甘幸路，櫨山寛章，小林和真，下條真司 : JGN2plus における運用 安定性とチャレンジ,テストベッドネットワークに対する運用面からの試み, 電子情報通信学会技術研究報告, Vol. 108, No. 223，IA2008，pp.33-38 (2008).

[6]JGN2plus，https://www.jgn.nict.go.jp/jgn2plus_archive/