

大震災の経験から考案した BCP 非常用サーバ

The emergency server for BCP by the experience of the disaster

鵜川義弘†, 福井恵子†, 平井清巳†, 安藤明伸†, 小野元久†, 本田茂広‡
Yoshihiro Ugawa†, Keiko Fukui†, Kiyomi Hirai†, Akinobu Ando†, Motohisa Ono†,
Shigehiro Honda‡

sakura2012@miyakyu-u.ac.jp † ‡

† 宮城教育大学情報処理センター

‡ 三菱スペース・ソフトウェア

† Miyagi University of Education

‡ Mitsubishi Space Software CO., LTD.

概要

東日本大震災のとき、大学のサーバが2日間の停電で全機能が停止する中、携帯やインターネットが使えるれば連絡ができたこと、その後1ヶ月日常生活ができなかったことを踏まえ、東北地方が全停電した状態であっても、Webで広報活動ができ、メールで安否確認が行えるよう大学宛メールから携帯等への“普段使い”の転送が維持され、復旧までの長期蓄積もできる非常用サーバを構築した。

キーワード

東日本大震災, BCP, 業務継続計画, 事業継続計画, クラウドサーバ

1. 大震災の被害状況とBCPの策定

宮城教育大学は東北地方でも震災に近く沿岸寄りにある仙台市に立地し、地域は大きな被害を受けた。

情報処理センターのサーバ室は1階にあり、物理的な被害は軽微であった一方で、2日間の停電により情報処理センターの全機能が停止し、Webサーバやメールサーバが機能しなくなった。メールによる安否確認もできず、入学試験の中止の案内もできなかった[1]。水道、ガス、自家用車にガソリンが自由に手に入るまでの1ヶ月以上

の間は、食料も満足に調達できない不自由な生活だった。

管理者が出張中で仙台に戻れない状況もあり、インフラだけでなく人命に不測の事態も想定する必要性もあった。非常時以前に、あらかじめ被害状況に応じた対応策を決めておく業務継続計画（Business Continuity Plan）を策定する必要性を痛感した[2]。

大震災のときSINETは電源喪失による停止はあったものの別ルートを回るバックアップにより途切れることはなかった。またネットワークインフラを支える複数の企業や組織の災害復旧、災害対応状況を見ると、今後のネットワークは災害時にも強いと考えられ、想定すべき最も重要な危機は電源であると思われる。

業務継続計画では東北地方全停電ですべての機能が停止する場合と、輪番停電などで一部機能が停止する場合があります。後者は発電機や縮退運転モードを持つシステムの導入を計画しているが、本稿では前者について述べる。

2. 非常用サーバの構成

2.1. クラウドサーバ

今回構築した非常用サーバは、東北地方全停電により情報処理センターは機能を停止した状態。一方で携帯各社のネット機能は使える状態を想定し、東北地方と同時に停電する可能性がない離れた地域にクラウドサーバをレンタルし非常用 DNS、Web サーバとメールサーバを構築したものである。

非常用サーバは、まず、サーバ設置地域が東北地方ではないとわかるもの、またデータ転送量に制限がないものを検討した。その結果、仮想4コアCPU、主メモリ4G、ディスク容量400GByteのものを年間5万円以下で契約することができた。

2.2. 非常用モードコントローラ

非常時には携帯から非常用サーバにアクセスし、通常サーバから非常用サーバに切り替えるコントローラ機能を持たせることにした。

非常用モードコントローラにより通常状態と非常状態を切り替える。災害直後など非常時の利用であることから携帯電話からのアクセスが可能なシンプルなインターフェースとした。

非常用モードコントローラはCakePHP[4]をフレームワークとして用いたWebアプリケーションとして開発した。



図-1 非常用モードコントローラログイン画面



図-2 非常用モードコントローラ切替画面

2.3. 非常用 DNS

非常用 DNS により、Web サーバ、メールサーバが通常のものから非常用のサーバへと切り替わる（図-7 非常用 DNS 動作概念図を参照）。

非常用 DNS は通常状態ではセカンダリ DNS として動作する。

非常状態では、セカンダリとして収集している最新のゾーンファイルを元にすべてのAレコードを非常用サーバのIPアドレスに切り替えたゾーンファイルを作成し、そのゾーンファイルを使用したプライマリDNSサーバとして稼働する。

また、非常状態から通常状態に戻した際にDNS情報の伝搬が高速になるようにTTLを元のゾーンファイルより短く変更した。

ゾーンファイルの切り替えプログラムではDNS::ZoneParse Perlモジュールを用いている。

2.4. 非常用 Web サーバ

非常用 Web サーバは非常用の連絡先、安否確認の方法など、非常時に必要な情報を提供するサーバである。

Web サーバについては一部コンテンツのミラーを持つ代替サーバも検討したが、震災後1ヶ月、生活もままならない状況で、通常のコンテンツを流していても、例えば停電時に着信できない内線電話の表記があったり、人が動けない状況では意味がなく、望ましくない状況が生まれる。そこでコンテンツは、被災状況、連絡先、安否確認の方法などの非常用情報を提供する最低限のものとした。コンテンツの更新も、携帯から更新ができるブログ形式のものとした。

他のWebサーバについても同様の状況と考えられ、非常用DNSの設定により大学のトップページだけでなく

URL が .miyakyo-u.ac.jp で終わるすべての Web ページへのアクセスがこのブログへと導かれる。

非常用 Web サーバはパソコンでも携帯からでも見やすい Geeklog [5] を CMS として用いた。ブログ形式であり、万が一の場合に、パソコンとネットの確保が難しい状態でも、携帯電話から更新作業ができる。



図3 本学の通常のホームページ



図4 非常用 Web サーバでのブログホームページ
「非常時には非常時用コンテンツが表示される」

通常時に非常用コンテンツが見えると誤解を生むが、管理者は通常時に非常用コンテンツの準備を行ないたい。そこで Geeklog のソースを変更し管理者としてアクセスした場合は通常時でも非常時用のコンテンツを閲覧/管理できるようにした。

非常用に切り替わっている状態のとき Google 等の検索サイトのロボットがクロールし、誤ったコンテンツを収集しないように robots.txt によりロボットからの収集を禁止した。

2.5. 非常用メールサーバ

非常用メールサーバは、非常時のメールの蓄積と携帯メール等への転送を継続するためのメールサーバからなる (図-8 非常用メールサーバ動作概念図を参照)。

非常用メールサーバに、ユーザのメール領域を含め、通常業務のすべての機能を代替しようとすると非常に大

きなものとなり、ミラー方法、提供方法も複雑になる。今回の大震災では、災害時にも携帯電話やプロバイダーのメールは動作しており大学のサーバ停止中であっても携帯電話や HotMail, YahooMail, Gmail に転送し、それで安否確認を含めて緊急の連絡を見ることができれば、当面不自由はしない。そこで、平常時、大学から携帯や自宅プロバイダー等に転送している状況を自動で学習させ、非常時にその転送ルールに従って転送する機能を持たせた。

一方で、通常のメールサーバが停止中の間は、メールを非常用サーバに蓄積するようにし、復旧後に改めて非常用サーバから再送するような機能を持たせた。

通常状態ではセカンダリメールサーバとして稼働し、非常状態ではセカンダリメールサーバ機能に加え、メール転送機能を行う。

通常状態から非常状態となった時点で、DNS にて非常用サーバを MX レコードに追加した場合、その伝搬期間の間、メールが非常用サーバに届かないことになるため、通常状態でセカンダリメールサーバとして稼働させている。

2.5.1. メール転送状況の学習

非常時に転送するアドレスをわざわざ登録させるページを作っておいたとして、そのことを覚えている人はどれだけいるかわからないし、災害が起こってから転送先を入力してもらうことも考えられない。学内には様々な方法で転送方法が提供されていて全てを網羅して調査することは難しい。そこで“普段”の転送状況を学習させることにした。

本学のメールシステムでは、どのホスト、サーバから送信しても必ずウィルス対策を行うメールサーバを中継してメールが外部または内部に配信される。

この中継用メールサーバのメールログのうち、メールの Message-ID ヘッダを用いて追跡をすることで、あるアドレスに対する転送先のメールアドレスが把握できる。

メーリングリストなどの同報メールの場合、同一の Message-ID で複数の宛先に配信されるため、メールログの検査ではこれを除外した。

また最終転送先が同じ大学内のメールサーバである場合、該当するメールサーバも非常時は停止していることが想定できるため、これも除外する。

非常時に確実に配送するため、同一アドレスからの転送先が複数に変化した場合には、変化分を追記する形にしている (図 5, 図 6)。

これは、単に転送先を変更したのか、procmail, ActiveMail などを用い、条件によって転送先を振り分けているのか、がメールログだけでは分からないためである。

日付	転送元アドレス	転送先アドレス
2012/3/1	転送元アドレス A	転送先アドレス A
2012/3/10	転送元アドレス A	転送先アドレス B
2012/3/15	転送元アドレス A	転送先アドレス A
2012/3/20	転送元アドレス A	転送先アドレス C

図-5 収集した転送先アドレスが変化した様子

転送元アドレス	転送先アドレス
転送元アドレス A	転送先アドレス A, 転送先アドレス B, 転送先アドレス C,

図-6 変化した転送先アドレスを追加した様子

転送先の把握は毎日行うが、当日分のメールログ検査結果だけではその日にメールが届かなかったユーザの転送先が消えてしまうため過去 21 日分（メールログ三世代分）の検査結果をまとめ、転送先データベースを構築している。登録件数から見る限り、転送先を元々設定していない者を除きほぼ全てのユーザの転送先を把握していると考えている。

転送先データベースは 1 日 1 度非常用サーバに転送している。

2.5.2. セカンダリメールサーバとメール転送

セカンダリメールサーバでは、大学宛のメールを静的に大学の外部メールサーバに配送する。

ホスト名で配送先メールサーバを指定した場合、非常状態で配送先が自分自身となりループを発生させてしまうため、配送先のメールサーバは IP アドレスで指定する。

メールの転送は postfix の `virtual_alias_maps` 機能を用いて行う。通常状態では `virtual_alias_maps` 機能を無効にし、非常状態で `virtual_alias_maps` 機能を有効にすることで、メール転送機能の有効、無効を切り替える。

一日一度、転送された最新の転送先データベースを元に Alias ファイルを作成する。作成する際に転送元アドレスを転送先アドレスに加える。

転送元アドレスへの配送は、配送先サーバが停止しているため、非常用サーバの中のキューにたまり、配送先となる大学のメールサーバが復活した後に配送される。

この方法の欠点として、非常状態から通常状態に戻った後、本来のサーバで同一の転送が行われるため、転送メールが合計 2 通になることである。緊急性を重要視し、

この欠点は無視した。

学内のメールサーバの内、独自に MX を持つサーバに関しては、指定した IP アドレスのメールサーバでは 3rd party relay とみなされ配送エラーが発生する。そこでセカンダリ DNS サーバとして収集しているゾーンファイルを検索し、独自に MX レコードを持つドメイン名を抽出し、静的配送マップに追加する処理を追加した。

3. その他

本学では通常時は広報・危機管理係が Web ページを管理しているが、震災時には、総務部に設置された災害対策本部が様々な情報を収集し発信を行っていた。

非常用サーバは情報処理センターが設置したものであるが、災害対策本部や広報・危機管理係が内容を管理、普段から非常用連絡先、安否確認の方法などの情報を蓄積できるよう、情報処理センターと大学との役割分担に関して調整が必要であった[3]。

非常モードでは、学内の Web サーバの全てが非常用 Web サーバに切り替わる。各組織で、非常時に必要な情報を広報・危機管理係に集め準備することが必要である。

未曾有の災害と言えども時がたてば記憶も薄れ対策が疎かになる。1 年に 1 度は必ずある電源設備点検時等のタイミングで切替訓練を行なう計画である。訓練に伴うアナウンスでは、学内の Web サーバの全てが非常用 Web サーバに切り替わること。非常モードで転送した先ではメールが重複すること等の注意の他、非常用サーバでは訓練であることを示すことが必要である。

4. 参考文献

- [1] 宮城教育大学情報処理センター被災状況
<http://edb.miyakyo-u.ac.jp/ugawa/20110926/MUE-IPC-311/>
- [2] 宮城教育大学情報処理センター大震災被災状況と業務継続性計画
<http://www.ipc.miyakyo-u.ac.jp/nenpo/no.19pdf/06.pdf>
- [3] 宮城教育大学非常用サーバ案内
<http://staff.miyakyo-u.ac.jp/~ugawa/Center/BCPserver.pdf>
- [4] CakePHP
<http://cakephp.jp/>
- [5] Geeklog オープンソース CMS
<http://www.geeklog.jp/>

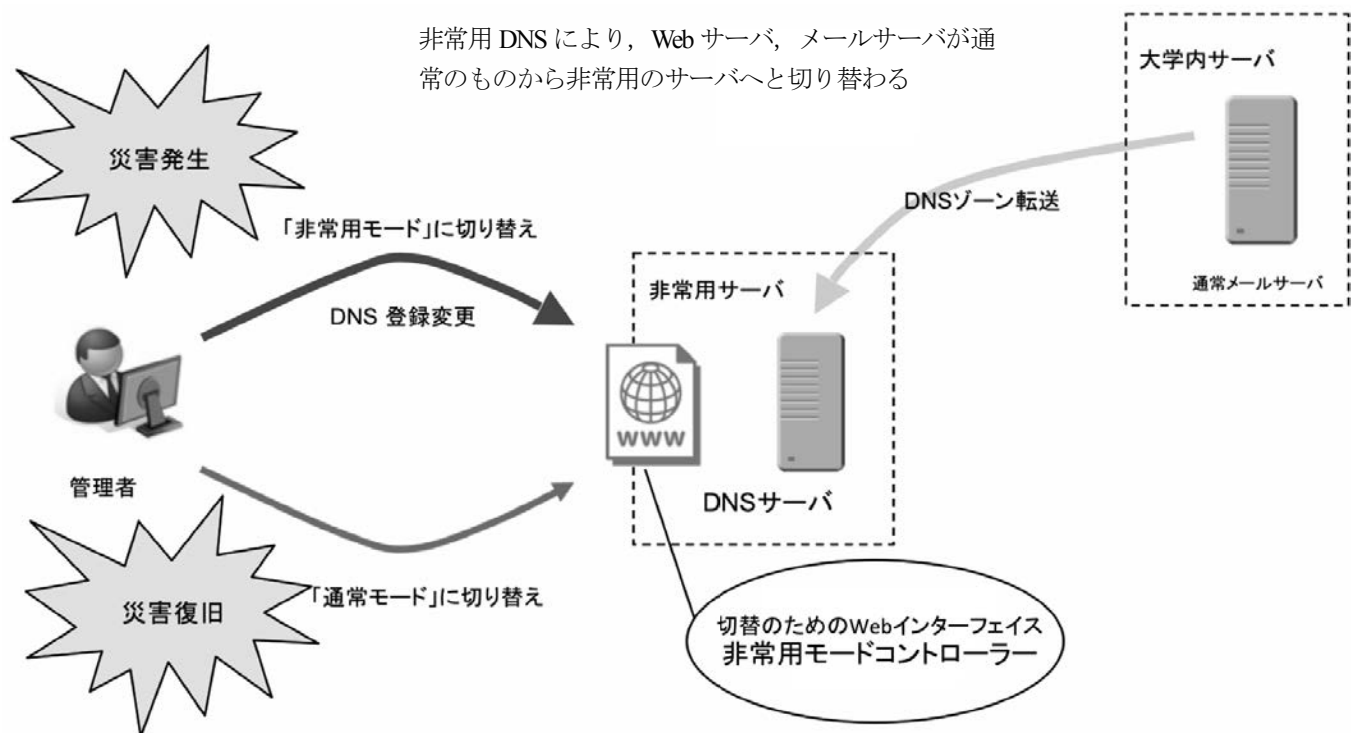


図-7 非常用 DNS 動作概念図

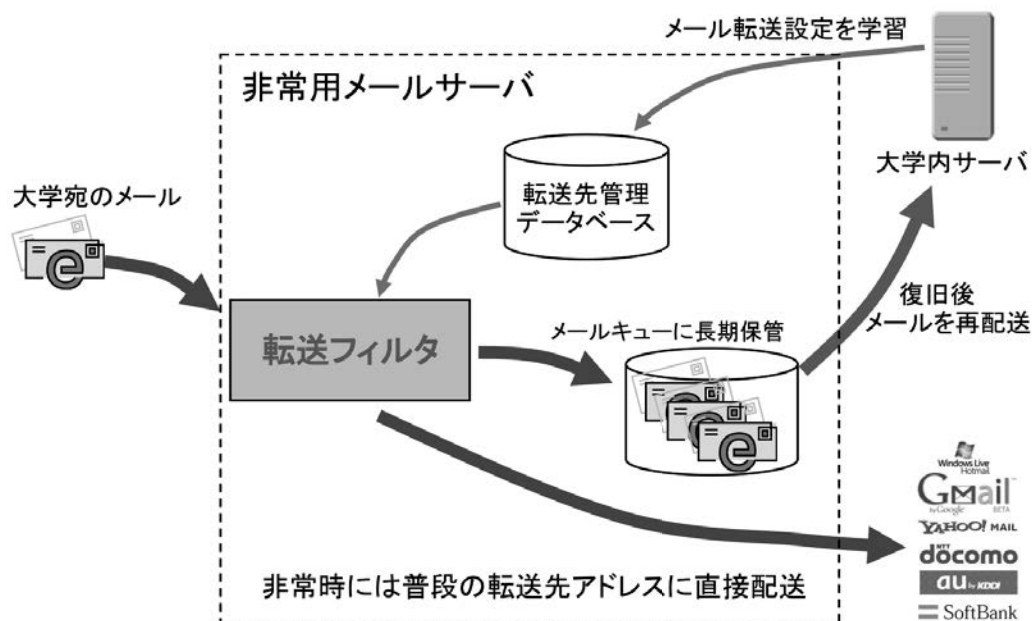


図-8 非常用メールサーバ動作概念図