解 説 3

クラウドが支える新しいリスク管理

― BCM/ITDR 災害のリスクマネジメントにおけるクラウドの役割 ―

東日本を急襲した未曾有の大災害の経験により、企業や社会は、リスクマネジメントの見直しが余儀なくされています。これは、IT システムの観点でも同様であり、従来のリスク管理の方法論を再考する必要性が認識されました。今回、震災自体の規模もさることながら、その影響範囲が想定をはるかに超えたことから、今後は、主センターが長期にわたって復旧できない場合に備え、副センターで本格復旧を行えるような方策も検討する必要があるでしょう。また、災害回復期に必要な IT 機能として、コミュニケーション関連機能の重要性が非常に高まっていることが明らかになりました。さらに、こうした災害対策の新しい解決策として、クラウド・コンピューティングの適用が有効であることも、実体験を通じて理解されました。本稿では、今回の災害対応を通じて IBM が得た新たな知見を基に、クラウド時代の新しいリスク管理方法について解説します。

Article 3

Risk Management in the Cloud Computing Era

- BCM/ITDR*: The Role of Cloud Computing in Disaster Risk Management -

The painful experience of the Tohoku earthquake and tsunami on March 11, 2011 forces us to re-consider the scope of risk management. It also impacts on today's IT risk management methodology. For example, the unexpected scale and power of the disaster taught us that we need to prepare a secondary data center to take over from the primary data center permanent base when there has been serious impact on the primary data center.

The experience made us aware of the fact that one of the most important IT functions necessary to recover as quickly as possible after disaster is communication, including messaging and social network services (SNS).

Cloud computing actually proved to be of great value during the disaster, because it facilitated rapid and flexible deployment of crisis response activities.

This article explains a new approach to IT risk management in the cloud computing era based on the findings made during crisis response activities.

* BCM/ITDR refers to Business Continuity Management/IT Disaster Recovery

❶ 災害対策にクラウド・コンピューティングを利用

東日本大震災のダメージを乗り越えて、これからの IT システムはどのように変化すべきでしょうか。その大命題において、災害対策が重要なポイントとなります。まさに「想定外」というべき災害に、IT システムはどう対応するべきなのでしょうか。

まず、これまでの「想定」をどう変更しなくてはならないかということを、距離と時間の軸で考えてみます。従来想定では、甚大被害エリアの範囲はおよそ半径 20 ～ 30km、直線距離での離隔距離は 100km 以内でした。これは、ストレージ・システムのネットワーク同期の限界と同等の範囲でもあり、合理的な離隔距離とされていました。また、被害が甚大であっても、バックアップ・センターでの稼働期間は数週間から1カ月と想定されてきました。その程度で主センターへの復旧作業が開始できるものとされていたからです。これは、多くのバックアップ・センターが、業務範囲や処理容量という点で、縮退運転を前提とした設計がなされてきた根拠となっています。

しかし、今回の東日本大震災の被害エリアの大きさ、大規模な液状化現象、そして原子力発電所事故による広範な避難エリアの設定などによって、これらの想定は大きく覆されました。**表 1** は、被害状況を現時点で分かる範囲でまとめたものです。

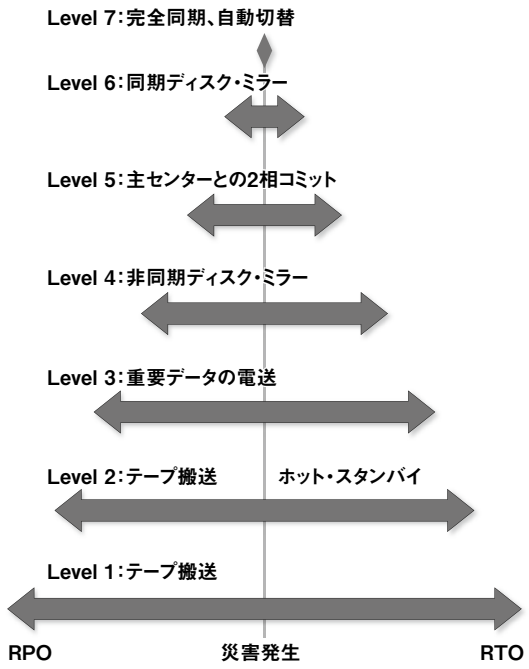
表1. 被害状況のまとめ

	過去の震災規模例（参考）	東日本大震災
震度	震度 7（阪神・淡路大震災 '95）	震度 7（宮城県栗原市）
震源域の想定	60km（FISC 安全対策基準など） ※ FISC：公益財団法人金融情報システムセンター	約 500km 以上となる可能性
最大加速度	818gal（阪神・淡路大震災 '95）	2,933gal
津波被害	奥尻島（北海道南西沖地震 '93） ・稲穂地区 8.5m ・奥尻地区 3.5m ・初松前地区 16.8m	・岩手県・大船渡港 11.8m ・福島県・相馬港 9.3m 以上 ・岩手県・釜石港 9.3m ・宮城県・石巻市鮎川 8.6m 以上 ・宮城県・仙台港 7.2m ・青森県・八戸港 6.2m
津波遡上距離	十勝川 10km 程度 （十勝沖地震 '03）	北上川 50km 以上
火災	・阪神地域で 285 件出火、7,483 棟の焼損棟数（阪神・淡路大震災 '95） ・奥尻島青苗地区で 190 戸、約 51,000 ㎡が焼失（北海道南西沖地震 '93）	1 都 10 県で 324 件発生 ※気仙沼のタンク重油流出、仙台市の製油所、千葉県市原市ほか、地震・津波によるガソリン、軽油などへの引火多数。
液状化	・ポートアイランドほか約 10 ㎢（阪神・淡路大震災 '95） ・水田の埋立地など（新潟県中越沖地震 '04）	千葉県、埼玉県、茨城県など約 42 ㎢
停電	・震災による約 260 万戸の停電（阪神・淡路大震災 '95）	・震災による停電 ※東北電力館内で約 440 万戸、 ※東京電力館内で約 405 万戸 ・原子力発電所の停止による計画停電
発電所の停止	柏崎刈羽原子力発電所を停止（新潟県中越沖地震 '04）	福島第一、第二原子力発電所 常陸那珂、鹿島、大井、五井、東扇島 火力発電所 11 機 水力 福島（14）、栃木（4）、山梨（4） 変電所 9 カ所
原子力発電所事故による影響	NA	半径 20 ～ 30km 圏内の住民に避難指示／屋内退避、その他 関東、甲信越と広範囲にわたる農作物への影響、風評被害など
通信	30 万回線超の電話不通（阪神・淡路大震災'95） 専用線系　約 2 日間 公衆網系　約 1 週間	影響調査中 ※日米ファイバーの損傷 ※台湾・香港ルート損傷など

注 1）内閣府、気象庁、消防庁、経済産業省ほか各ニュース・サイトの情報を基に著者が作成（2011 年 6 月 22 日現在）[1] [2] [3] [4] [5] [6] [7]
注 2）浜岡原子力発電所の停止などは含まない。

まず、これまでの「想定」を大きく変えるべき点と変えるべきでない点を明らかにしなくてはなりません。従来の想定に基づいて検討されてきた業務上の重要度や縮退運転の許容度などは、まったく有効に働かないのでしょうか。答えは、どんな場合にも無効というわけではなく、今回ほどの規模でない災害においては、有効に働くだろうと思われます。東阪の両エリアに分散するなど500km以上の離隔地にバックアップ・センターがあれば、これまで通り、想定された復旧時間でバックアップ・センターを起動することで、短期間（数週間程度）の対応が可能になるでしょう。想定外の事態が発生するのはその後です。これまでの災害対策では、バックアップ・センターにおける縮退運転から通常運転に復旧するためには、主センターの回復を待たなくてはなりません。しかし、主センターが数週間で回復しない場合など、被災からの時間軸を長く取った災害対策の立案が求められます。想定外の建物損傷や原子力発電所事故、余震による立ち入り禁止、液状化によるライフラインの損傷などが発生した今回の大震災はまさにこのケースです。

これまでのITDR（IT Disaster Recovery：ITシステムにおける災害対策案）のフレームワークは、RTO（目標復旧時間）/RPO（目標復旧地点）のバランスの上に成り立っていました。業務データの復旧がどの時点まで求められるか、どのくらい早くシステムが復旧しなくてはならないか、というパラメーターで、業務の重要度とITDRに用いられるコストとのバランスを考慮し、業務領域の絞り込みと最適なテクノロジーを選択します。この原則に変化はありませんが、数週間であれば耐え得る業務の縮退が長期間には耐えられないという事態に備えなくてはなりません。つまり、バックアップ・センターにおける追加の機能回復や、被災エリア外へのシステムの退避が求められるということです。



※米国 Share： http://www.share.org/

図1. 米国ShareによるITDR技術選択基準

これが意味することは、被災からの時間軸をRTOという指標だけで見るのではなく、被災規模の把握により「タイムライン的」な柔軟な対応を計画することが求められているということです。被災直後に必要なRTOの小さなシステムと、数週間後に復旧すべきシステム、それぞれのデータの鮮度などが個別に議論されなくてはなりません。さらに、被災直後の業務復旧においては、基幹業務のデータの同期よりも、コミュニケーションや取引先への連絡など、RPO不問の「データの鮮度」にかかわらない種類の機能中心の回復も重要な要素です。被災からの時間軸に対して柔軟な災害対策計画を立てるためには、一元的なリカバリー技術を中心とする災害対策ではなく、柔軟性の高いクラウド・コンピューティング技術を活用することが鍵となります。

クラウド環境においては、資源を柔軟に変更することができます。例えば、データ同期をしている縮退対応のバックアップ・センターのプロセッサーの処理容量を、主センターの被災状況を判断しながら、通常運転に対応できるよう拡張することもできます。コストという観点では、主センターは被災してすべての資源利用課金が止まっているので、バックアップ・センターでの資源拡張によるコスト負荷は少なくなります。また、データ同期の必要ないシステムは、サービス・イメージ・ライブラリーに保存しておけば、ボタン1つでバックアップ・クラウド・センター上に復元でき、RPO不問の機能回復を図ることができます。こうした対策は、対象となるシステムがクラウドのイメージとして取り扱える状態になっていることが前提となっています。

上記のようなクラウドを活用した災害対策計画にも課題はあります。いざ、災害が発生した時にクラウド全体で資源が枯渇してしまうことはないのか。クラウド上で保管されるサービス・イメージは、データセンター間で可搬性があるのか。さらには、複雑なシステムでは、サーバーをクラウド環境上に置くだけではなく、クラスタリングやチューニングなどのシステム構築作業も莫大になります。

資源予約やクラウドの可搬性を高める標準化など、今後、クラウド事業者が取り組むべき課題となるでしょう。

また、クラウドが提供するAPIを用いたシステム構築の自動化や、アプリケーションの可搬性をより高めるPaaS（Platform as a Service）技術などに関する今後の動向にも注意を払いたいと考えます。

❷ 災害支援におけるクラウドの活用

今回の東北地方太平洋沖地震では、多くの方々が甚大な被害を受けられ、現在も復興の過程にあります。企業や自治体などの活動の根幹を担うITシステムにも、多大な影響がありました。

そうした中で、クラウドを活用して、迅速な支援活動の立ち上げを試みた例が幾つもあります。クラウド・サービス・プロバイダー各社は、相次いでIaaS（Infrastructure as a Service）の無償提供を実施しましたし、PaaSを活用して情報共有アプリケーションを短期間で立ち上げた例もあります。

IBMは、Smart Business Cloud for Enterprise（SBCE）の無償提供と、それを活用したミラーサイト立ち上げ、Sahanaプロジェクトの支援、LotusLiveの無償提供などを実施しました（本誌28ページ以下：インタビュー③参照）[8]。

今回の災害対応でクラウドが活用された理由としては、クラウドの持つ「すぐに使える」という特性が、災害支援活動における緊急性という切実な要件に適合したことが大きいでしょう。

また、実際に使われたアプリケーションは、情報発信、情報共有など、コミュニケーション用途のものが中心となりました。

災害時に、携帯電話を含む電話網がまひする中、IPネットワークは生き残り、ラジオ、テレビに加えて、SNSサイトやTwitterが情報提供・情報交換に活発に使われました。例えば被害を受けた企業は、短期間での業務復旧に取り組みながらも、被害状況や復旧見通しなどの情報を発信することを重視し、これらのメディアを活用しました。ほとんどの企業がホームページを持ち、取引先や、顧客がさまざまなサービスの情報をWebサイトから入手することが当たり前になった現在では、インターネットによる情報発信の手段を失うことは、企業にとって致命的な損失だと認識されているのです。企業のITシステムにおける災害対策は、従来は主に基幹業務のリカバリーを主眼に置いていましたが、今後の対策を考える上でこれは新たな発見でした。

2.1 ミラーサイトの活用

計画停電や放射能に関する情報など、国民生活に深くかかわるライフライン情報を提供するサイトが、通常の10倍以上のアクセスを受けてまひしたため、ミラーサイトによるアクセス分散で対応した例が幾つもあります。

ミラーサイトは、インターネット黎明期から使われていた古典的な方法で、元来はフリー・ソフトウェアなどのファイルのダウンロード・サイトを、複数設けて負荷分散するためのものでした。

企業のWebサイトでは、同一サイト内に複数のWebサーバーを置いて、ロード・バランサー（負荷分散装置）によって負荷分散するのが主流でしたが、今回の震災ではあまりにも急激なトラフィック増のために、サーバー増設が追い付かず、短期間で実施可能な即効性のある手段として、クラウド上でミラーサイトを作る方法が使われました。

ミラーサイトは**図2**のような仕組みで、簡単に作ることができますが、次のような制約があります。

a）CGI（Common Gateway Interface）やサーブレットを使った、サーバー・サイドのアプリケーションには対応できない

b）データベースなどを使った、登録、申し込みなどを行うものには対応できない

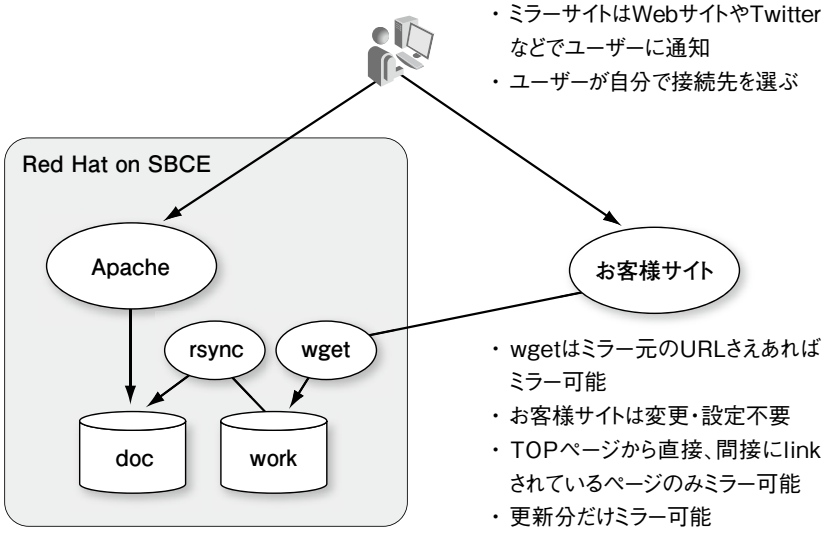


図2. ミラーサイトの仕組

c）CSS や JavaScript などを使った、凝ったページもうまくミラーできない場合がある

また、次のようなちょっとした工夫で、ミラーサイトの立ち上げを効率化できます。

a）Web サイトのどの部分をミラー対象とするかを決めておく
b）ミラー対象のファイル一覧を用意しておく
c）初期ミラー後に更新するファイルを把握しておく
d）絶対パス、URL はできるだけ使わない
e）サイズの大きな画像、データを使わない

ミラーサイト作成で使われるツールは、指定されたページから順にリンクをたどりますが、更新がなくても対象範囲のすべてのファイルの更新状況を調べます。更新範囲が決まっていれば、そこだけ明示的に調べた方が速いのです。

2.2 Sahanaプロジェクトの支援

Sahana（サハナ）は、被災者を支援する活動を行っている行政、NPO（非営利団体）、ボランティア団体などが支援活動をするのに必要なさまざまな情報を集約し活用するために作られた災害時情報共有システムです［9］。

スリランカの津波の際に開発が開始され、現在は2009 年 6 月設立された非営利組織 Sahana Software Foundation がオープンソースで開発を進めています。これまでスマトラ島沖地震、四川大地震、ハイチ地震など世界各地の被災地で利用されました。

今回の東日本大震災の支援のために、現在 “Sahana Japan Team” が、Sahana を日本で利用するための作業を行っていますが、開発環境、テスト環境、デモ環境、本番環境など、幾つもの環境が次々と必要とされるので、IBM の SBCE を無償提供してニーズに柔軟に対応しています。

Sahana は、10 以上のオープンソース・パッケージの組み合わせで、**図 3** のように構成されています。Web サーバーの Apache 上で稼働する、web2py という Python 言語のフレームワークを中心とし、データベースとして PostgreSQL を利用しています。その他、数多くのライブラリーやツールが使われていて、地図情報や Twitter との連携など、幅広い機能を実現しています。

Sahana のアプリケーション本体は、Eden と呼ばれる web2py のアプリケーションとして構成されていて、アプリケーション・リポジトリーから、Bazaar［10］というリビジョン・コントロール・システムを使用して、展開されるようになっています。

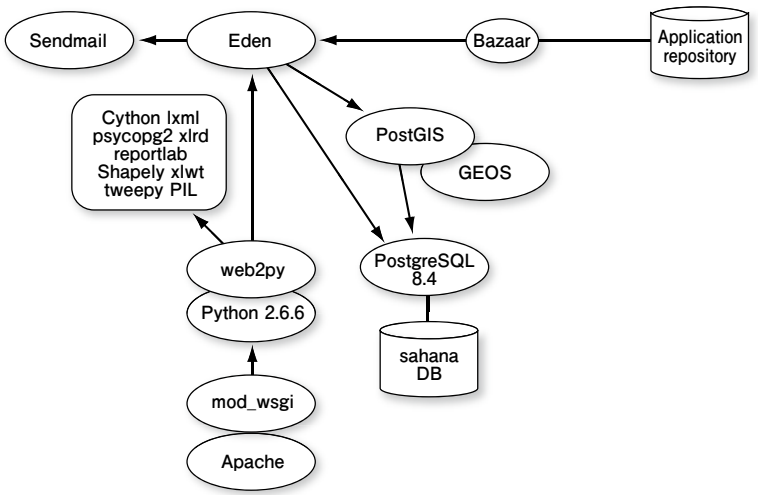


図3. Sahanaの構造

Sahana システムの導入手順のドキュメントは A4 サイズで 4 ページほどになりますが、クラウド上ではひな形となる環境のイメージを作れば、それ以降は短時間で幾つもの環境を次々と作ることができます。運用監視の仕組みや、アプリケーションのリリースの仕組みを組み込んだイメージを用意しておけば、環境を作ってすぐに本番運用に入ることもできます。

多少複雑なパッケージを利用したり、アプリケーション開発を伴うものであっても、クラウドを利用することで、導入・構築の期間と工数を大幅に減らすことができます。

Sahana のプロジェクトでは、活発な開発が続いているため、開発環境で更新されたアプリケーションを、テスト環境、デモ環境、本番環境へと、タイムリーに展開していく必要があるので、クラウド技術が大いに役立っているのです（**図4**）。

このようにして、インフラ面ではクラウドの VM イメージの作成とプロビジョニングの機能を、アプリケーション面では分散ソースコード管理の仕組みをうまく使って、複数環境の一貫性を保ちつつ、短時間で効率よく環境を準備し、運用しています。

❸ 災害時にクラウドを活用するために

今回の経験を踏まえ、クラウドを活用した災害時のリスクマネジメントを考える場合、以下のような項目に沿って、要件を整理しておく必要があります。

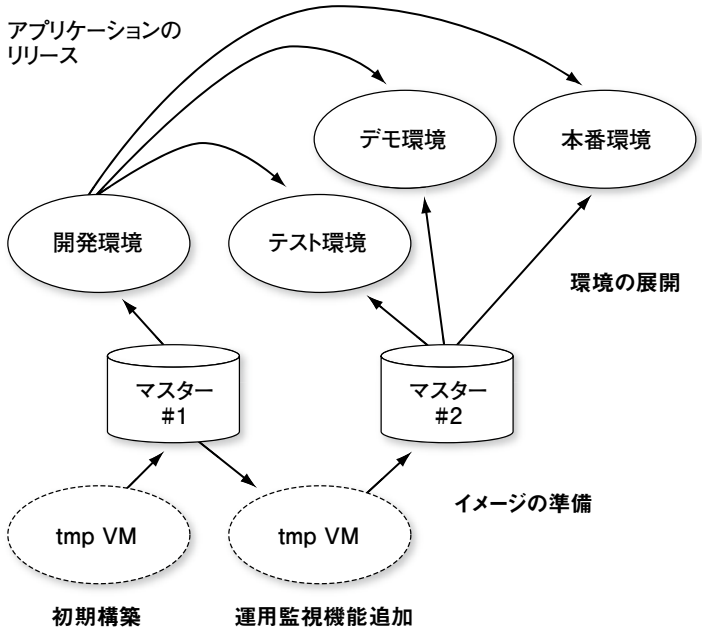


図4. クラウドを使ったSahana環境構築

(1)災害時にすぐに動かすべきIT機能

災害時には、交通や通信が遮断され、企業活動はまひします。限定的な活動のみが可能な中で、必要なIT機能を決定して、迅速に対応する必要があります。

しかし、通常通りの方法で意思決定を行おうとしても、検討に必要な人員が集まらなかったり、承認者と連絡がとれなかったりすることも考えられます。従って、迅速な対応のためには、災害時に動かすべきIT機能をあらかじめ検討しておき、いざという時には限られた人数でも実行に移せるように意思決定しておく必要があります。

(2)災害時に収集・発信すべき情報

企業が業務の復旧計画を作成する上で、災害時の社員やその家族の安否の把握、自社状況の把握と情報発信、顧客や取引先の状況把握などが前提となります。

特に社員とその家族の安否確認は、災害対応の第一歩です。災害発生時にどのような通信手段が使えるかは予想できませんが、少なくとも、複数の異なる手段で、社員とその家族の安否情報を、上司もしくは同僚に伝えることができるように普段から徹底し、実地訓練をしておく必要があります。

(3)災害時に利用できるIT基盤

災害による破壊だけでなく、電力や燃料供給の停滞などの二次的な影響により、自社データセンターや、利用中のクラウド・サービスが継続利用できなくなるかもしれません。

前述の安否確認を例にとると、情報収集用のシステムを自社で用意しておくことも大切ですが、それが災害によって使用不能になった場合に備えて、クラウド上で利用可能なSaaS（Software as a Service）や、IaaS上で簡単に構築できる情報共有サイトなどを利用することも検討しておくべきでしょう。

(4)災害時のIT機能を利用する体制

緊急かつ必要最低限のIT機能を動かすために、自社要員だけで対応できるとは限りません。クラウド・サービスを利用する際に、システムの運用監視や、アプリケーションやデータの更新など、外部のサービスによって代替できるものも検討しておきましょう。

人間の避難訓練と同様に、災害時のIT機能の利用については、普段から被害発生を想定したマニュアルの準備と、運用切り替えの訓練が必要です。

災害発生直後は、マニュアル通りの対応では済まないことが多く、機転を利かせた対応や、個人に依存した非常体制での対応が強いられることも少なくないでしょう。しかし、企業としての災害対応としては、可能な限り短い時間で、組織的な対応ができる体制に移行していくことが必要です。

特に、災害により、直接的、間接的なダメージが大きい場合、災害対策は短期間では終わらず、何カ月といった長期間にわたる場合もあります。

災害後の暫定的なIT機能であっても、稼働させる期間が長期になれば、通常システムと変わらないシステムの運用監視や、アプリケーションのメンテナンスが必要になります。

災害発生直後の暫定的な対応から、長期的な対応、通常運用への復帰と、幾つかの段階に分けて、IT機能の利用・運用形態を決めていく必要があります。

❹ まとめ

未曾有の大災害への対応を通じて、クラウド・コンピューティングがいかに有効に機能したのか、実例に基づいてご紹介しました。今回の大震災は、企業に災害対策の

実体験を与え、リスクマネジメントのスコープの再考を促しています。副センターは、従来にも増して大きな役割を担うことが求められています。災害発生時には、まずコミュニケーション機能の回復が必要です。クラウド・コンピューティングは、災害対策に有効であることが実証され、ITのリスクマネジメントを再定義する上で、重要な位置を占めています。

［参考文献］

［1］ 内閣府：阪神・淡路大震災教訓情報資料集,http://www.bousai.go.jp/1info/kyoukun/hanshin_awaji/earthquake/index.html
［2］ 北海道南西沖地震による奥尻島の津波【1993 年7 月12 日、北海道南西沖奥尻島】,http://www.sozogaku.com/fkd/hf/HA0000618.pdf
［3］ 消防防災博物館、第2 章　阪神･淡路大震災における火災の発生状況と出火原因,http://www.bousaihaku.com/bousaihaku2/images/prev/pdf/h002.pdf
［4］ 国土交通省気象庁：報道発表資料・情報公開,http://www.jma.go.jp/jma/index.html
［5］ 総務省消防庁 :http://www.fdma.go.jp/
［6］ NHK ニュース,http://www.nhk.or.jp
［7］ "東北地方の440 万世帯で停電". 読売新聞. (2011 年3 月11 日). http://www.yomiuri.co.jp/national/news/20110311-OYT1T00857.htm
［8］ 日本IBM：震災復旧・復興支援ポータル,http://www.ibm.com/jp/news/2011/03/earthquake.html
［9］ Sahana Japan Team フリー(自由) ･オープンソース災害時救援情報共有システム,http://www.sahana.jp/
［10］Bazaar, http://bazaar.canonical.com/en/

日本アイ・ビー・エム株式会社
クラウド&スマーター・シティ事業 CTO
ディスティングイッシュト・エンジニア（技術理事）

山下 克司 **Katsushi Yamashita**

［プロフィール］
1987 年、日本 IBM 入社。適用業務パッケージの開発などを経てネットワーク分野のテクニカル・リーダーを務める。2007 年にネットワーク仮想化技術などの貢献を評価されディスティングイッシュト・エンジニアに認定され技術理事に就任。2010 年からはクラウド・コンピューティング事業の技術統括をするチーフ・テクノロジー・オフィサーに就任し、クラウド・コンピューティングの技術面でのリーダーを務める。

日本アイ・ビー・エム株式会社
クラウド&スマーター・シティ事業 .
クラウド・ソリューション
Senior IT Architect / クラウド・マイスター

新島 智之 **Tomoyuki Niijima**

［プロフィール］
1989 年、日本 IBM 入社。さまざまな業種のお客様における、大規模メール・サーバー、放送制御システム、大規模 ERP システムなどの開発プロジェクトで、リード・アーキテクトを務め、最新技術の適用に挑戦し、成功裏のサービスインと安定稼働を実現し続けている。2009 年よりクラウド・コンピューティング関連の業務に従事し、その普及に努めている。