

## WHITE PAPER

# 東日本大震災がもたらした事業継続管理の変化 富士通ストレージ ETERNUS を活用したデータ保護のアドバンテージ

Sponsored by: 富士通

鈴木 康介

February 2012

## 調査概要

2011年3月11日、東日本の広範な地域に甚大な被害をもたらした東日本大震災は、これまでの災害対策の考え方を大きく変えるものであった。かつては存在することが重要であった事業継続計画は、その計画内容の有効性と実行に移す際の錬度が問われるものへと変化した。本調査レポートでは、50か所以上の拠点で被災を経験した富士通に取材し、事業継続管理の改善、強化に取り組む国内企業や組織のために、東日本大震災で得られた教訓をどのように生かすべきかを示す。また、後半では、データ保護を中心に考える IT システムの災害対策について、富士通のストレージ ETERNUS を活用する利点を考察する。

## 概況

### 被災のビジネスインパクトを最小限に抑えた事前訓練

富士通では、東北地方や北関東にある多くの工場が被災した。プリンター、デスクトップ PC、PC サーバーを製造する福島県伊達市にある富士通アイソテックの本社工場もその1つである。伊達市は、東京電力福島第一原子力発電所から50キロ離れていたため、避難指示区域に指定されることはなかったものの、阿武隈川の複数の橋梁が通行止めになるなど、地震により大きな被害が出ていた。また、水道などの社会インフラも一時期停止を余儀なくされた。

富士通では、富士通アイソテックの工場施設の生産設備に被害が発生したことを受け、デスクトップ PC の製造業務を島根富士通での代替製造へと移行した。この移行が速やかに行われた鍵は、富士通に事業継続計画が策定されていたのみならず、2008～2010年度（会計年度）までに計40回以上訓練が行われていたことにある。災害模擬訓練、机上読み合わせ訓練、総合訓練などを繰り返し実施していたことで、現場からトップマネジメントまでが災害に直面した場面に何をすべきか、何を判断基準に次の行動を決定すべきか、十分に理解できていたことが現実の移行所要時間を短縮したとみられる。

富士通アイソテックは、地震発生直後の3月11日午後、現地復旧対策本部を設置し、通信手段の確保と情報収集を始めた。それと同時にサプライヤーの被災状況についても調査を開始している。翌12日午前には、島根富士通に代替製造準備を開始する旨の指示を出すと共に、原発事故の影響分析、生産計画の見直しなどを行った。その状況判断の結果、13日午前には早くも代替製造の開始が発令された。そして工場停止から12日後にあたる3月23日には、島根富士通の工場から出荷が開始された。富士通では、事業継続計画がなかった場合、業務再開に必要なリソースの確保に遅れが生じ、実際よりも18日間は復旧が遅れたであろうと評価している。

この富士通アイソテックのケースは切り替えの意思決定がスムーズに行われた例であるが、今回、国内のすべての企業がこのような迅速な対応が取れたわけではない。

たとえば、計画停電の実施予定地域にサーバールームを持っていたある企業では、100%停電になるとは限らない状況で、システムをセカンダリーサイトに切り替えるべきなのか、いつの時点で、どの情報を基に最終判断すべきなのかが分からず、結局、切り替えができなかったケースがあった。また、別の企業の例では、実際にセカンダリーサイトに切り替えした後に、プライマリーへのフェイルバックの時期を判断できずに困惑した話も聞かれた。システム上に仕組みを作り込んでも、状況を判断する責任者が十分に訓練されていない場合、それが機能しないことがあり得ると分かったことは貴重な教訓といえよう。

## 改定が必要となった事業継続計画

東日本大震災では、いくつかの点で事業継続計画が想定していた被災状況と異なり、復旧計画を見直さざるを得ないことが分かったが、中でも多くの企業を悩ませたのは電力供給の問題である。

データセンター事業者の場合、自家発電設備を持つことが通例となっていたため、計画停電で操業を止めたところでは出なかった。富士通においても、館林システムセンター、富士通エフ・アイ・ピーが展開する全国のデータセンターなどは、計画停電や電力供給問題のさなかも、安定稼働を続けることができた。このような本格的な自家発電設備を持たないデータセンターやサーバールームを保有する一般企業では、現在、電力供給の視点を加えた災害対策を策定する必要に迫られている。たとえば、災害対策用セカンダリーサイトを準備する場合、これまで担当技術者が比較的短時間で移動できる距離に置かれることが多かったが、電力供給の問題が明らかになってからは、同一の電力会社から供給を受ける地域を避け、遠距離にセカンダリーサイトを置こうとする企業が増えている。中には、データセンターを東日本、西日本の両地域に持ち、連携させることを検討している企業もある。

また、東日本大震災のような大規模災害においては、道路、鉄道などの交通インフラにも被害が出ること、電力のみならず水道、ガス、通信などのライフラインの復旧にも時間を要することを考慮しなければならない。富士通総研では、富士通社内の被災時の行動記録とさまざまな企業から収集した対応状況の公開情報をベースに災害時における対応行動をベストプラクティスとしてテンプレート化した行動手順書を作成し、大規模災害が発生時にどのように行動すべきか、何を準備しておくべきかを「BCP トータルパック 2011」として提供し始めている（Figure 1 参照）。このサービスを利用するとすでに事業継続計画を策定済みの企業や団体が、自らの事業継続計画とベストプラクティスを比較評価を行い、実効性の観点から計画の見直しを行うことが可能となっている。

FIGURE 1

### コンサルティングサービス「BCP トータルパック 2011」



Source: 富士通総研, 2012

## データセンターアウトソーシングを利用した災害対策の必要性

前述の通り、自家発電設備を持つデータセンターは電力供給に問題があった時期をトラブルなく乗り越えることができた。その実績はデータセンターサービスを災害対策に活用すべきとのユーザー意識の変化に結び付いている。だが、データセンター利用の価値は電力供給問題への対応力だけではない。IT システムの災害対策の重要性が増したといっても、無制限にコストがかけられるわけではなく、適所にアウトソーシングを織り交ぜた災害対策を実施することでコストの最適化を図ることはすべての企業にとって重要なことである。たとえば、ホットスタンバイしておかなくてもよいと判断されるシステムであれば、仮想マシンイメージと業務データをデータセンターに預けておき、必要が生じたときに仮想マシンを起動し、業務を継続するやり方もある。

また、データセンター事業者が用意している高速ネットワークの利用価値も高い。富士通の場合、富士通と富士通エフ・アイ・ピーの主要な 5 つのデータセンター（館林、東京第 1 / 第 2、明石、FIP 横浜、FIP 千里）は 10Gbps を 2 重化した回線で接続されている。複数のデータセンターを利用し、連携させたいニーズがあるユーザーならば、これらの高速ネットワークが利用できることの意義は大きい。

FIGURE 2

### 富士通データセンター



Source: 富士通, 2012

### 富士通ストレージ ETERNUS によるデータ保護

IT システムの災害対策には種々の選択肢があるが、何より必要なことはデータを守ることである。データの保全がなされていれば、たとえ復旧に時間がかかったとしても、業務を再開することはできるであろう。逆にデータを失った場合には、事業の継続そのものが危うくなる。過去には、阪神・淡路大震災の際にもデータを失ったことで事業が再開できなかった例が出ている。

しかし、いくらデータ保護が必須といっても、それにかかるコストは企業にとって負担となることから、運用方式の選択には熟慮が必要となる。リモートバックアップやリモートレプリケーションを災害対策として実施する場合には回線コストの支出が大きくなることも念頭に置かねばならない。本調査レポートで取り上げる富士通ストレージ「ETERNUS DX60 S2/DX80 S2/DX90 S2 ディスクアレイ」と「ETERNUS CS800 デデュープアプライアンス」は費用対効果の高い災害対策を可能にする製品である。以下では、これらの製品によってどのようにコスト最適化が図れるかを考察する。

## ストレージを中心とした災害対策の優位点

ストレージ製品の個別機能を検証する前に、ストレージを中心とした災害対策にどのような利点があるかを考察しておく。

災害対策にはさまざまな方法があり、アプリケーションごとに必要とされるサービスレベルに応じた仕組みを構築することは可能である。また、データベースにもディザスタリカバリ機能があることから、その利用も考えられる。

しかし、個々のシステムにそれぞれ災害対策を施した場合、コスト面で全体最適が図りにくいこともさることながら、災害対策システムの運用が複雑化するという問題が出てくる。東日本大震災で経験した通り、災害発生直後には人員の移動が制限される場合が多く、システムごとの災害対策が、高度な、しかも固有のスキルを持つ技術者によって運用されている場合には、組織内に人的バックアップを準備することが難しくなり、担当者の不在が原因で復旧作業が遅れることが起こり得る。

安全性を高める方法の1つは、災害対策を簡素化し、担当者の不在による影響を受けにくいシステムを構築することである。具体的にはストレージ統合を行い、一元的なデータ管理を実現することである。さらにストレージが組織内で標準化されていれば、運用スキルの教育負担を抑えることができ、災害対策に必要な知識を持つ技術者の配置に冗長性を持たせやすくなる。

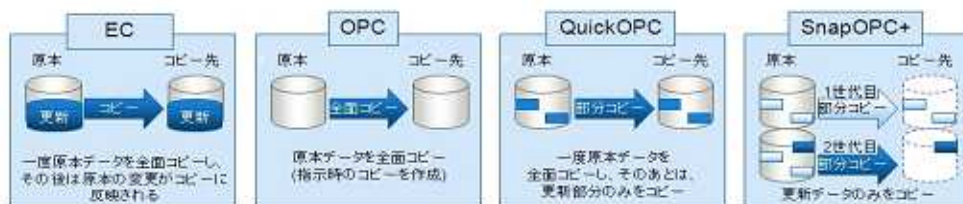
## ETERNUS DX60 S2 / DX80 S2 / DX90 S2 を用いた災害対策

富士通のストレージ製品でエントリークラスに位置付けられるディスクアレイ「ETERNUS DX60 S2 / DX80 S2 / DX90 S2」は、コンパクトな筐体にハイエンドクラスの充実した機能を提供することをコンセプトにしている。このため、災害対策への支出を抑えたいユーザーには有効なソリューションとなる。

### 豊富な動作モードを持つアドバンスト・コピー機能

FIGURE 3

## オンライン中の高速バックアップ / アドバンスト・コピー機能



Source: 富士通, 2012



「アドバンスド・コピー機能」は、サーバーの CPU を使用せずにストレージだけで高速にコピーを作成する機能である。アプリケーションを停止することなく、任意時点の業務ボリュームのデータを、短時間で同じディスクアレイ内の別のボリュームにコピーする。コピー完了後の複製ボリュームは、業務ボリュームと切り離されるため、本番業務を継続しながらある時点の業務ボリュームをテープ装置へバックアップできる。いくつかの動作モードが用意されており、ユーザーはデータの性質に応じた方式を選択できる（Figure 3 参照）。

これらの「アドバンスド・コピー機能」を利用すれば復旧時点目標（Recovery Point Objective：災害や障害の発生から復旧を行う際、どの時点まで遡ってデータを回復させるかの指標）の改善が可能となり、データ損失リスクの低減が図れる。

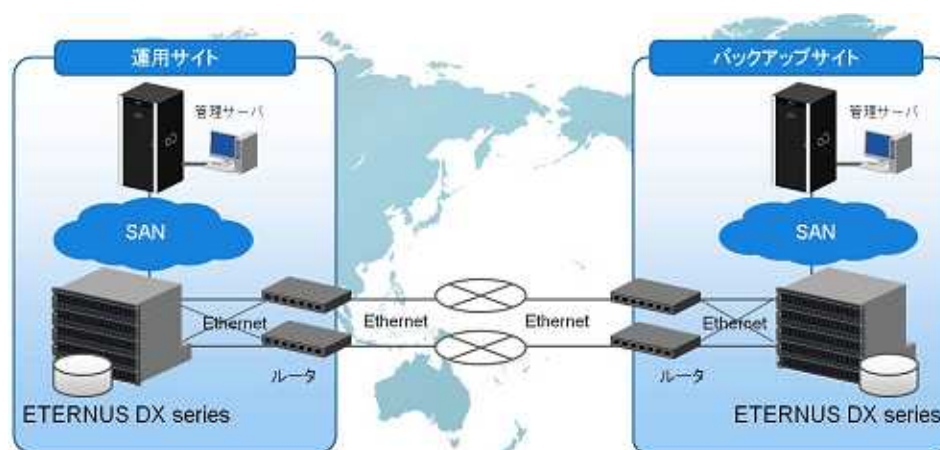
### iSCSI インターフェースによるリモートコピー

さらに「ETERNUS DX90 S2」には「リモート・アドバンスド・コピー機能」が備わっている。これは「アドバンスド・コピー機能」の二重化切り離し方式 EC を拡張した「Remote Equivalent Copy（REC）」を使用し、遠隔地での筐体間コピーを実現する機能である。複数筐体間でのミラーリングやスナップショットの作成、バックアップに適用できるため、災害対策を目的としたデータ保護、迅速なリカバリーを可能にする。「REC」のデータ転送には同期転送モードと非同期転送モードがあり、データの性質やセカンダリーサイトの距離などに応じてモードを選択して使用できる。

「REC」はファイバーチャネル接続でもサポートされているが、災害対策のコストをより低廉にするために、IP ネットワーク接続もサポートされている。ストレージ間を iSCSI インターフェースで接続し、IP 回線を利用することで、導入コストが高額になりがちなファイバーチャネルスイッチや SAN ゲートウェイ装置が不要となり、低コストでの接続が可能になる。また、「ETERNUS DX90 S2」では、同一機種間のみならず、上位機種や旧機種とのレプリケーションや、N 対 1 の統合バックアップにも対応しているため、セカンダリーサイトに本番サイトと同じストレージを置く必要がなく、予算に応じた柔軟なシステム構築が可能となる（Figure 4 参照）。

FIGURE 4

### IP ネットワーク接続のリモートコピー



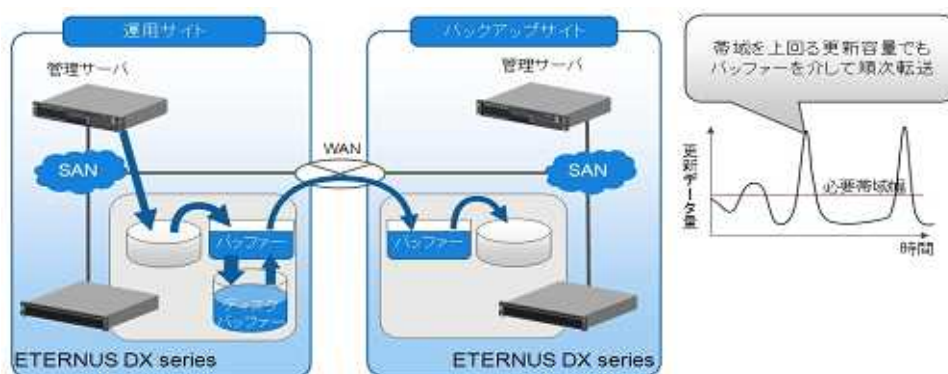
Source: 富士通, 2012

### 低帯域回線を用いて遠隔データ保護を可能にする Disk Buffered REC

回線経由の遠隔データ保護を行う場合、通信回線のコストが高額な負担になるため、低帯域回線を用いたりリモートコピーが可能となれば、ユーザーには大きなメリットになる。「ETERNUS DX90 S2」には、キャッシュメモリの一部を REC バッファとして使用し、複数の REC セッションへの I/O を一定期間 REC バッファに保持したあと、ブロックにまとめてコピーを行う「Consistency モード」がある。このモードは、コピー先の転送順序性を保つように制御される。また、回線不安定などの要因により、キャッシュメモリのバッファだけでは容量が不足する場合は、ディスクをバッファとして使用する「Disk Buffered REC」も提供されている。ディスクを用いることでバッファを大容量化し、一時的な更新データの急増にも対応が可能となっている（Figure 5 参照）。

FIGURE 5

### 低帯域回線を用いたりリモートコピー-Disk Buffered REC



Source: 富士通, 2012

### VMware 連携

現在、セカンダリーサイトにサーバー仮想化技術を導入し、災害対策のコスト削減を試みるユーザーが増えている。アプリケーションのサービスレベルを見極めた上で、それが一時的に縮退運転も許容できるサーバーであれば、本番サイトと同一の装置を準備するよりもコスト面で有利な構成が組める。「ETERNUS DX80 S2/DX90 S2」には「VMware vSphere」の VAAI (vStorage APIs for Array Integration) がサポートされており、仮想サーバー環境でのパフォーマンス向上を図れる。たとえば、VAAI で実装されている機能の 1 つ Full Copy では、データコピーのタスクをディスクアレイの機能を使用して実行するため、データがサーバーを経由せずシステム性能が向上する。実際、この機能は仮想マシンのクローンの作成やライブマイグレーション (Storage vMotion) などに有効である。この他にも、初期化作業を効率化する Block Zeroing、粒度の細かいロック機構を実現する Hardware Assisted Locking、未使用となった領域を未割り当て領域として解放する Thin Provisioning Space Reclamation などの VAAI 機能にも対応している。

エントリークラスの製品でありながら、セカンダリーサイトの統合 SAN ストレージとして仮想サーバーを含む各種 OS のサーバーに対応できることは、非常に高い費用対効果を提供しているといえるであろう。

## デデューブアプライアンス「ETERNUS CS800」による災害対策のコスト削減

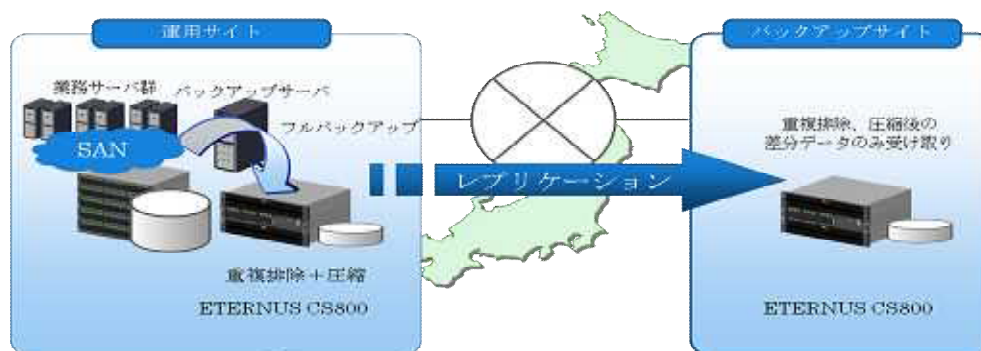
遠隔データ保護における回線コストを下げるもう1つの有効な手段は、データの重複排除（デデューブリケーション）を導入することである。保護対象データは種類/量共にハイペースで増えるので、遠隔データ保護においては、その負荷の増大が深刻な課題になりかねない。回線の帯域を追加するのはストレージ容量を増設するよりも難しいからである。データの増加ペースを抑える意味で重複排除は重要な技術的な選択肢となる。

富士通は、デデューブアプライアンス「ETERNUS CS800」により、重複排除技術を利用した低コストで高速なディスクバックアップの運用を提唱している。富士通では、重複排除のデータ削減効果として、「標準的な企業のデータを毎週フルバックアップ、毎日、差分バックアップした場合、データ量の90%以上の削減が期待できる」としている。削減効果はデータの種別やバックアップ運用により異なるため、削減率を重視するならば、重複排除製品のアルゴリズムに着目すべきと IDC では考えているが、「ETERNUS CS800」の場合、可変長のブロック単位で重複判定を行う、運用現場で実績のあるアルゴリズムを用いているので、その点でも安心である。また、圧縮率の評価だけでなく、富士通では「ETERNUS CS800」の実機の無償トライアルを行っているため、パフォーマンスについても、導入前に検証が行える。

### 「ETERNUS CS800」による災害対策

FIGURE 6

### 低帯域 WAN を利用した ETERNUS CS800 間でのデータ複製



Source: 富士通, 2012

災害対策システムに「ETERNUS CS800」を用いることのメリットは、2拠点での相互レプリケーションや各拠点とデータセンター間での N 対 1 の統合バックアップが低帯域 WAN を通して行いやすくなることである。さらに「ETERNUS CS800」では通信の暗号化もサポートされているため、WAN 利用の際の安全性が高い（Figure 6 参照）。「ETERNUS CS800」は、業界の標準的なバックアップソフトウェア（Symantec NetBackup、Symantec Backup Exec、CA ARCserve Backup、NetVault Backup、NetWorker、ETERNUS SF TSM など）に対応している。このため、ローカルなバックアップ作業はそれらのソフトウェアを利用しながら「ETERNUS CS800」に統合し、拠点間の遠隔レプリケーションを「ETERNUS CS800」の機能を使って行うことで、既存環境に親和性の高い遠隔データ保護システムを容易に構築できる。

## 富士通ストレージ ETERNUS のデータ保護ソリューションの市場機会と課題

現在、国内のあらゆる企業、団体は、東日本大震災の経験を基に、IT システムの災害対策強化の必要性に迫られている。さらに、2012 年 4 月～5 月の発行が想定される ISO 22301 事業継続マネジメントシステム（英文タイトル Societal security - Business continuity management systems - Requirements）が正式発行されれば、災害対策ソリューションのニーズはいっそう高まるであろう。しかし、世界的に景気の先行きが不透明な中で、企業が災害対策の新たな予算を準備することは容易ではない。このような状況の下で、本調査レポートで取り上げた富士通ストレージ ETERNUS による費用対効果の高いデータ保護ソリューションは、多くのユーザーから支持を得るであろう。特にこれまで予算の制限から本格的な遠隔データ保護システムを構築できなかったユーザーに新たな選択肢を提案できる意義は大きい。

一方で、富士通の課題となるのは、災害対策予算が足りず、データを十分に保護できていないユーザーをいかに支援するかであろう。予算を捻出するためには、IT システム全体のコスト最適化を図ることが有効だが、それに何年もかかるようでは災害対策が遅れてしまう。また、現時点で災害対策予算が不十分なユーザーは、コンサルティングなどの有償サービスを利用することも少ないと思われ、ベンダーの支援には難しさもある。しかし、国内で最も多くの災害対策システムの構築実績を持つベンダー、システムインテグレーターとして富士通は、IT システムの事業継続性改善に向けて未対策ユーザーを減らせる最も有力な位置にある。災害対策システム市場の裾野を広げ、国内の災害対策レベルの底上げに向けて富士通の活躍が期待される。

## Copyright Notice

本レポートは、IDC の製品として提供されています。本レポートおよびサービスの詳細は、IDC Japan 株式会社セールス（Tel：03-3556-4761、jp-sales@idcjapan.co.jp）までお問い合わせ下さい。また、本書に掲載される「Source: IDC Japan」および「Source: IDC」と出典の明示された Figure や Table の著作権は IDC が留保します。

Copyright 2012 IDC Japan 無断複製を禁じます。