E-18

中小企業向け災害即応型簡易データバックアップシステムの検証

Verification of the disaster conformity type simple data backup system for small and medium-sized enterprises

吉田 昌弘 †　大西 克実 †　中野 秀男 ‡
Masahiro Yoshida　Katsumi Onishi　Hideo Nakano

１．はじめに

インターネットの普及とそれに始まるコンピュータおよび通信機器のコモディティ化によって、社会における IT 化は成熟期を迎えた。

多くの人々は、さまざまな生活の記録を画像・音声・文章などの電子データとしてパソコンやスマートデバイスに保存し、電子メールや LINE を代表とするインスタントメッセンジャーで相互にコミュニケーションを取っている。

もちろん、IT 化の波は企業活動にも押し寄せており、以前であれば紙媒体であった事務書類（各種帳簿類、設計資料など）や雑多なメモ類に至るまで電子データとして HDD などの電子媒体に保存されている。

企業のコミュニケーションに目を向けてみるとやり取りの履歴が残るなどのメリットが多い為、企業取引や社内連絡の手段として電子メールが普及し、一人一人にメールアドレスが割り当てられ、頻繁にやり取りが行われている状況となっている。

以上のように、現在では、個人の生活や企業活動と電子データは、切っても切り離せない状態となっており、災害などによる電子データ消失を未然に防ぐバックアップ作業は、ますます重要になっている。

特に企業活動におけるデータ消失は、企業の記憶喪失といってよい状態であり、業務の継続はおろか復旧も困難になり、事業運営自体が危ぶまれることになる。

このような状況の中、2005 年頃から政府では、企業や政府機関における BCP（事業継続計画）の普及に向けて情報システムやデータのバックアップを含めた様々なガイドラインの整備を進めている。

しかし、第３章で述べるとおり、BCP の策定状況は、東日本大震災以降も依然低く、特に中小企業で策定済みの企業は全体の 5.5%となっている。

ますます重要度が増している電子データのバックアップであるが、東日本大震災で明らかになったように適切なバックアップがなされておらず、多くの企業でデータ消失が発生した。

そこで、本研究では、情報担当部門および専任担当者の居ない中小企業をターゲットにしたバックアップシステムを提案することを目的に、自動で定期的にバックアップを行うことはもちろん、災害発生時にも自動で重要データをバックアップする簡易システムを作成してその有効性の検証を行う。

２．BCP（事業継続計画）とは

内閣府では、BCP を以下の様に定義している。

『災害時に特定された重要業務が中断しないこと、また万一事業活動が中断した場合に目標復旧時間内に重要な機能を再開させ、業務中断に伴う顧客取引の競合他社への流出、マーケットシェアの低下、企業評価の低下などから企業を守るための経営戦略。バックアップシステムの整備、バックアップオフィスの確保、安否確認の迅速化、要員の確保、生産設備の代替などの対策を実施する（Business Continuity Plan: BCP）。』[1]

特に IT 部門におけるバックアップシステムの整備については、「ディザスターリカバリ」とも呼ばれる。

３．BCP 対策の現状

３-１ BCP の策定状況

東日本大震災の影響もあり、大企業では、BCP の策定が進む一方、中小企業では、依然 14.0%と策定率が低く、企業規模ごとの格差が開いている。

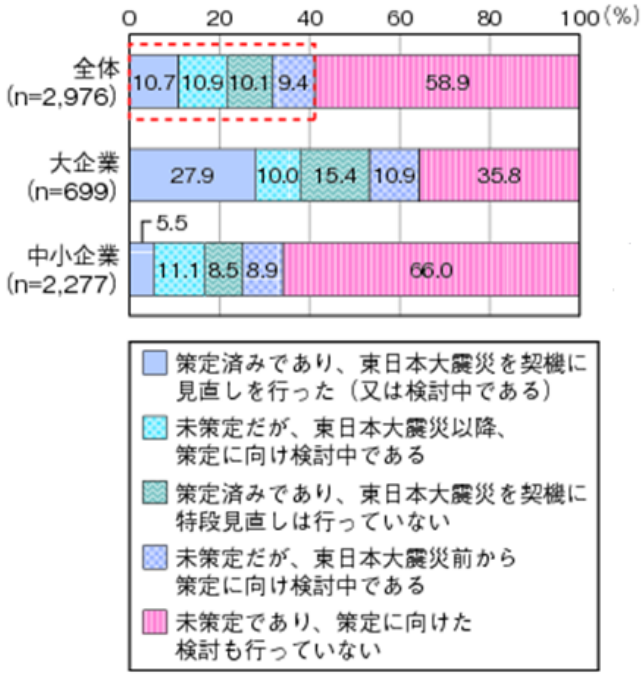

図１　企業の BCP 策定状況(2012 年)[2]

† 大阪市立大学, Osaka City University
‡ 帝塚山学院大学, Tezukayama Gakuin University

3-2 中小企業の現状

中小企業で BCP 策定が進んでいない理由については、以下の表の通りとなっている。

多くの中小企業では、財政的な問題により専門の情報部門や担当者を持てず、BCP 策定やディザスターリカバリ対応を行えていない。

また、「自社には不要」と回答している企業の多くは、対策する必要がないというわけではなく、被災した際には、そのまま廃業する為不要という意味も含まれる。

表 1 中小企業における BCP 未策定の理由[3]

ノウハウがない（策定方法がわからない）	42.1%
自社には不要	35.3%
人手が足りない	33.1%
時間がない	26.3%
コストがかかる	21.6%
その他	6.9%

（複数回答あり）

3-3 中小企業におけるデータバックアップ

多くの中小企業では、安価な DVD や USB メモリへの保存が多く、バックアップタイミングも週に 1、2 度、手作業で個人任せの実施が主流である。比較的規模の大きい企業においてもサーバは自動でバックアップを実施するが、クライアント PC は、個人任せという場合が多い。

特に手作業でのバックアップは、不確実で必要な時に必要なバックアップデータが存在しない、古いデータしか残っていないなどの事故が発生しやすくデータ消失の可能性が高い。

4. 災害発生時の状況分析

本研究では、災害の発生に呼応してバックアップを行うことから災害発生からバックアップ完了までの制約についての考察を行った。

4-1 時間的制約

災害の発生からシステムがダウンするまでの時間的制約を考えることは、データをどれだけバックアップできるかということに関わる重要な視点である。

参考資料として、報知可能な災害として地震と火災の災害の発生から到達までの時間的制約を以下に記載する。

- 地震速報発報から地震到達までの時間
  十数秒～数十秒[4]
- 地震到達から津波到達までの時間
  東日本大震災で最短 30 分
- 火災報知器鳴動から電源消失までの時間
  出火場所により不定

4-2 量的制約

時間的制約から災害の発生からシステムがダウンするまでのデータ転送量が量的制約として求められる。ここでは、100BASE-T のイーサネットの理論値を元に電源消失・ネットワーク不通までの転送量を求め、以下に記載する。（転送量については、100BASE-TX の理想値で試算）

- 地震速報発報から地震到達までの転送量
  約 1GBit～9GBit 程度
- 地震到達から津波到達までの転送量
  約 180GBit 程度
- 火災報知器鳴動から電源消失までの転送量
  出火場所により不定

5. 既存のディザスターリカバリサービス

東日本大震災以降、各社が争ってディザスターリカバリサービスを打ち出しているが、そのほとんどが、システム自体の冗長化や遠隔地へのレプリケーションなどの大規模なシステム構築となっている。

中小企業向けを謳っているバックアップシステムなどについても、導入には 100 万円から 400 万円程度の費用が掛かり、中小零細企業では、到底手が出ない価格設定となっている。

また、バックアップサービスについては、定期バックアップのみであり、被災直前のデータについては、バックアップできない為、被災直前にやり取りしていたメールの内容やデータについては、消失する。

6. 災害即応型簡易バックアップシステムの検討

以上のことから大規模システムを構築できない中小企業に対しては、定期的に自動バックアップを行いながら、被災直前には重要データを退避させるシステムの提供が必要であり、ベストエフォート型のサービスでも良いが安価なシステムが望まれていると言える。

このことから以下の様なシステムの作成を行い、有効性を検証したいと考える。

6-1 システム概要

情報部門および専任担当者が存在しない中小企業をターゲットとして、以下の要件を定める。

(1) バックアップについては、手作業による不確実性を排除するため、定期的な自動バックアップとする。
また、任意の時点でのバックアップを実施できることとする。

(2) 被災情報を取得した際には、自動で緊急バックアップを行う。緊急バックアップは、バックアップ途中でのシステムダウンを考慮し、定期的な自動バックアップのバックアップ先とは別の保存先とする。

(3) バックアップファイルの設定時に以降で述べる重要度分析により重み付けを行い、バックアップ実施時には、重要度の高いファイルから順にバックアップを実施する。

(4) 緊急バックアップ実施のトリガーとなる被災情報の取得については、コストを考慮し、本研究では、安価で利用できるサービスを対象に検討する。
また、緊急バックアップ実施のトリガーインターフェイスを用意することにより、被災情報取得の方式をユーザーがネットワーク経由で自由に選択できるようにする。

(5) データのバックアップ先については、SkyDrive や Dropbox などに代表されるクラウドストレージや FTP サーバ、NAS に転送できるものとする。
また、バックアップ方法の拡張性を考慮して、スクリプトファイル（MS-DOS や WPS など）の実行によるバックアップ方式を用意する。

6-2 重要度分析

データの重要度を判定する為に担当者が、各部門に聞き取りを行ったとしても自部門のデータを最優先でバックアップしてほしいという回答になることが多く、専門知識の無い担当者が、バックアップの優先順位を決めることは、きわめて難しい作業となる。

そこで本研究では、バックアップ対象のファイルを設定する際に以下の手順で重要度分析による重み付けを行い、優先順位を決定するものとする。

(1) 対象のファイルに対して、ファイル内容の確認項目を設け、その項目の入力に対して重要度の重み付けを行う。
(2) データ転送の量的制約から、対象ファイルのファイルサイズに対して重要度の重み付けを行う。（小さいファイルほど優先度が上がるようにする）
(3) 一定期間ごとの対象ファイル対する更新頻度を分析し、頻度の高いものから重要度の重み付けを行う。

6-3 被災情報の取得方法

本研究では、様々な災害の中からデータ消失の直接要因になる可能性があり、ユーザーに対して報知可能な災害として、地震と火災を取り上げる。

被災情報の取得方法に関しては、対象ユーザーが中小の零細企業であることを想定している為、導入や維持のコストが安価であることが絶対条件となる。

そのことから地震と火災の被災情報の取得について考察する。

(1) 地震

地震による被災情報としては、気象庁が 2007 年より一部離島を除いた国内ほぼ全域を対象とした緊急地震速報を運用しており、この速報を受信することで被災情報の取得が可能となる。

緊急地震速報の受信については、テレビ・ラジオ放送や携帯電話、専用ラジオ受信機など様々な利用形態が存在するが、本研究では、インターネットとの親和性が高い、Twitter による緊急地震速報を受信する方式を採用する。

(2) 火災

火災による被災情報としては、システムを設置している建屋の自動火災報知設備からの被災情報の取得を行う。

現状では、自動火災報知設備のベル鳴動を検知する回路を作成して、発報を検知する。

6-4 バックアップ内容

ターゲットである中小の零細企業では、データのほとんどがファイルである為、バックアップ対象については、ファイルを想定することとする。

ただし、高度なバックアップ機能として DB などのバックアップも可能とするスクリプトファイルの実行ができることとする。

6-5 バックアップ先

クラウド・FTP・遠隔地に存在する NAS など幅広いバックアップ先に対応できるようプラグイン方式とし、拡張性を保持する。

また、通常時と緊急時では、バックアップ先を変更できるようにする。

7. 現状の問題点

現時点において、判明している問題点を以下に挙げてみる。今後は、これらの問題について考察し、対応を実施することが今後の課題である。

(1) 地震到達時におけるハードウェア保護

本研究では、災害発生後の被災情報取得をトリガーにバックアップを実施するが、地震到達時の揺れによる HDD 故障に繋がる可能性がある為、その対策が必要となる。

(2) バックアップ先のシステムダウン対応

地震発生時の場合、バックアップ対象のシステムより保存先のネットワーダウンやシステムダウンが発生する可能性がある為、それに対する対策が必要となる。

(3) 重要度分析の手法について

ファイルの重要度をはかる確認項目とその重み付けが不明確であり、客観的な評価基準を構築する必要がある。

(4) 自動火災報知設備からの情報取得方式

法的に問題の無いように自動火災報知設備に回路を追加する方式の検討。

(5) 有効性の評価方法

擬似的被災情報を取得しての評価は可能であるが、本研究は被災時における緊急バックアップを主眼としたシステムの為、実際の災害に対する評価を行う必要があると考える。また、その有効性を評価する指標を定める必要がある。

８．参考文献

[1]　内閣府　「防災情報のページ」
http://www.bousai.go.jp/kyoiku/kigyou/keizoku/index.html
[2]　総務省　平成 24 年版 情報白書
[3]　㈱帝国データバンク　BCP（事業継続計画）についての企業意識調査　2011 年 6 月 27 日
[4]　気象庁　「緊急地震速報とは」
http://www.seisvol.kishou.go.jp/eq/EEW/kaisetsu/Whats_EEW.html
[5]　YOMIURI ONLINE　「地震発生から津波来襲まで最短 30 分」 2011 年 3 月 12 日
http://www.yomiuri.co.jp/science/news/20110312-OYT1T00196.htm
[6]　谷井 成吉　実践マニュアル コンピュータシステム災害復旧の対策 -ディザスターリカバリ対策の構築-　ダイヤモンド社　2006

以　上