

高機能高可用性情報ストレージ基盤の耐災害性実証シナリオの構築

Propose a Scenario to Verify Fault-tolerance of High Functionality and High Availability Information Storage Infrastructure on the Assumption of Large Scale Disasters

東日本大震災では、地震や津波により拠点の情報ストレージが損壊、流出して重要なデータが喪失した。一部のデータはクラウド上のストレージに複製されていたが、広域の通信障害の影響で被災地ではインターネットに接続できず、複製データの取得は困難であった。こうして大規模かつ広域な災害の下では、既存の情報ストレージ基盤は十分な耐災害性を持たないことが明らかになった。大規模災害により拠点が被災しても企業や自治体などが必要な災害対応や業務を実施していくためには、発災後も必要なデータを取得できる高可用性情報ストレージ基盤が望まれる。現在、近隣の拠点ストレージ間でデータを複製し合うことで耐災害性を強化した分散ストレージ基盤技術が開発されている。本稿では、分散ストレージ基盤上に構築した情報システムを用いて、ユーザによるシステムの利用や実際の災害による被災状況に基づきストレージ基盤の耐災害性を実証するための、実証シナリオについて提案する。

宗形 聡	Munakata Satoshi
宋 チュウ	Song Chong
手塚 大	Tezuka Masaru

1. はじめに

東日本大震災では、地震による拠点の損壊や津波による浸水により医療情報や住民情報などの重要なデータが情報ストレージから喪失した^{1,2)}。企業や病院、自治体などが被災後に適切な災害対応を実施し、必要な業務を停止させずに継続していくためには、発災後も重要なデータにアクセスして取得できる高可用性情報ストレージ基盤が必要である。

従来、情報ストレージに関する可用性向上の施策としては、拠点の情報ストレージにある複数のディスクにデータを分散して記録する RAID 技術の適用や、情報ストレージから外部記憶媒体への複製と拠点内での保管などの対策が取られることが多い³⁾。しかし、東日本大震災級の大規模災害では、拠点自体が損壊または流出するほどの甚大な被害を受ける。このような場合には、従来の技術や施策では十分なデータの保全が困難となる。

一方、近年新たなストレージ基盤としてクラウドが注目され、震災後は自治体や企業のディザスタリカバリのインフラとして期待されている⁴⁾。ネットワーク経由で

クラウドストレージにバックアップしておくことで、災害により拠点が被災しても重要なデータの喪失を防ぐことができる。しかし、大規模災害が発生すると、多くの基地局や局舎、物理回線の被災だけでなく、輻輳による通信規制や停電による機器の停止などネットワークに関する複合的な問題により広域の通信障害が生じる。そのため、必要なデータを参照したい場合でもインターネットにアクセスできず、クラウド上のデータを取得できないリスクが高まる。データの喪失を防ぐことができて、必要な時に取得できないという状況の下では、クラウドストレージのデータ可用性が十分であるとは言えない。

このような情報ストレージの耐災害性の不備を解決する新たな技術は、将来発生しうる大規模災害からデータを守るために重要な役割を果たすだけでなく、被災した東北地方の復興貢献にも資するものである。(株)日立ソリューションズ東日本（以下、HSE と略す）は、東日本大震災の被災地である仙台市に本社を置く企業として、被災自治体向け住民ニーズ可視化・管理システムなどの提供を通して復興に貢献してきた⁵⁾。今回、大規模災害

にも十分な耐災害性を持つストレージ基盤技術の開発とその実証実験を推進するため、HSE は東北大学および（株）日立製作所と共同で、文部科学省の委託事業「高機能高可用性情報ストレージ基盤技術の開発」に参画している。

開発している高機能高可用性情報ストレージ基盤は、近隣の拠点ストレージ間でデータを複製し合う分散ストレージである。元データを持つ拠点と複製データを持つ拠点が同時に被災してデータを喪失することのないように、複数拠点の同時被災リスクに基づき複製先を決定することを特長としている。また、広域の通信障害が発生した場合には、ユーザが近隣拠点に向向いてストレージからデータを取得できるようにシステムを構築することで、通信障害時のデータ可用性を向上させることが可能である。

HSE は委託事業の中で、高機能高可用性情報ストレージ基盤にデータを格納する災害に強い情報システムの設計・構築と、当該システムを用いた情報ストレージ基盤の耐災害性実証実験を担当している。実証実験では、多くのユーザが利用するシステムを前提に大規模災害が発生した際のストレージ基盤の耐災害性を高い精度で検証することが求められる。本稿では、実際のユーザによるシステムの利用や災害による被災の状況を反映して構築した耐災害性実証シナリオについて報告する。

2. 高機能高可用性情報ストレージ基盤

高機能高可用性情報ストレージ基盤（以下、高可用ストレージ基盤と略す）は、県や市などローカルな地域内で互いに近隣に設置された拠点ストレージ群と遠隔地のクラウドストレージから構成される分散ストレージである。任意の 2 つの拠点ストレージは直接あるいはその他の拠点ストレージを介してネットワークでつながっている。ある拠点のストレージにデータが格納されると、高可用ストレージ基盤はクラウドストレージまたは近隣の拠点ストレージに自動的にデータを複製する。複製処理は、高可用ストレージ基盤のレスポンスに影響するのを防ぐため、非同期で実行される。

複製先となる近隣拠点の選択にはリスクアウェア複製と呼ばれるアルゴリズムが用いられている⁶⁾。リスクアウェア複製とは、元データを持つ拠点と複製データを持つ拠点が同時に被災してデータを失わないように、複数拠点の同時被災リスクに基づいて複製先を決定するアルゴリズムである。

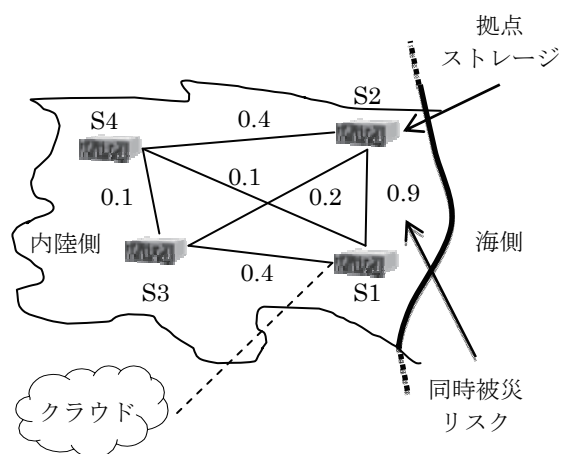


図1 高可用ストレージ基盤とデータ複製

リスクアウェア複製の例を図1に示す。ある地域に4つの拠点ストレージS1～S4が設置されており、それぞれが互いにネットワークでつながっている。この例ではデータの複製数を1として、海溝型地震による津波の被害を想定した場合に任意の2拠点間の同時被災リスクを数値化したものになっている。拠点の同時被災リスクは災害の種類や地理的条件などに基づいて定量化される。

津波による被災のため、図1では沿岸部にある2つの拠点ストレージS1とS2は同時被災リスクが0.9と高く、沿岸部の拠点ストレージS1と内陸部の拠点ストレージS4は0.1と最も低くなっている。そのため、S1に格納された元データの複製先にはS4が選択される。同様に、S2に格納された元データの複製先は同時被災リスクが0.2と最も低いS3が選択される。他の拠点ストレージについても同様にして複製先を選択することができる。

図1では複製数を1としたが、2以上の場合でも同様に複数拠点の同時被災リスクに基づき、リスクの小さい拠点を元データの複製先として選択する。多数の拠点ストレージ間でデータを複製し合う場合、同時被災リスクの設定状況によっては同じリスクとなる複製先が複数存在したり、どの拠点とも同時被災リスクが相対的に小さくなる特定の拠点に複製データが集中したりする可能性が生じる。そのためリスクアウェア複製では、各拠点ストレージの容量などを制約条件としながら、データ喪失リスクの総和が可能な限り小さくなるように各拠点の元データの複製先を決定している。

リスクアウェア複製の適用により、高可用ストレージ基盤の50%の機器が損壊しても90%のデータにアクセスできる可用性が期待される。

3. 高可用ストレージ基盤を用いた災害に強い投薬情報システム

高可用ストレージ基盤の耐災害性を実証するため、高可用ストレージ基盤にデータを格納する上位の情報システムが必要である。本研究では、多数のユーザがシステムを利用することを想定して実証実験をする必要があること、実際の災害時に役に立つシステムで実証することなどを考慮し、ユーザの服薬履歴を管理する投薬情報システム(電子お薬手帳)を上位システムとして選択した。

投薬情報システムは健康管理に支援が必要な高齢者や慢性疾患患者だけではなく、広く一般のユーザから利用されるシステムとして位置付けられる。また、東日本大震災では、被災者への円滑な医療の提供のためにお薬手帳の有無が大変重要であったとの指摘がなされている⁷⁾。こうしたことから、投薬情報システムは実証実験の題材として適切であると言える。

高可用ストレージ基盤にデータを格納する投薬情報システムの全体像を図2に示す。投薬情報システムはユーザから利用される際の利便性を考慮し、Webアプリケーションシステムとした。Webアプリケーションサーバはパブリッククラウド上にあるメインのサーバと、各拠点にある代替サーバから構成される。クライアントはスマートフォンのアプリやPCのブラウザである。拠点ストレージは、ユーザの投薬情報を格納するという役割か

ら、地域の医療機関や調剤薬局に設置されていると見なすことができる。

インターネットに接続できる平常時には、クライアントはクラウド上のメインサーバにアクセスする。これは通常のWebシステムの利用方法と同じである。メインサーバはクライアントからの投薬情報の登録や参照要求を受け付ける。その後メインサーバは元データを格納する拠点ストレージを特定し、そのストレージに対してデータの格納または取得を行う。データが格納された場合には、高可用ストレージ基盤側でリスクアウェア複製により複製先が選択され、自動複製される。偶発的な故障により拠点ストレージが停止している場合には、メインサーバはクライアントの複製データを格納する代替拠点を特定し、代替ストレージに対してデータの格納/取得を試みる。

大規模災害によってインターネット接続が途絶した場合には、ユーザは自身の元データを格納する拠点に直接出向き、拠点のLAN経由で代替サーバにアクセスしてデータを取得する。その際、拠点の被災によってストレージが損壊または流出している場合には、ストレージ群が近隣拠点に設置されている高可用ストレージ基盤の利点を活用し、ユーザは複製データを持つ代替拠点に再度移動し、当該拠点の代替サーバからデータを取得する。

このように、高可用ストレージ基盤を利用した投薬情報システムを構築することによって、大規模災害の被災による拠点ストレージの損壊や流出だけではなく、広域の通信障害にあっても、必要な服薬履歴データにアクセス可能な耐災害性のあるシステムを構築することができる。

4. 投薬情報システムを題材とした耐災害性実証シナリオの構築

高可用ストレージ基盤の耐災害性を検証するため、投薬情報システムを用いた実証実験を実施する。本研究では、システムのユーザが必要とするデータを実用的な時間内に取得できることを十分な耐災害性を持つと定める。実証実験を通して、高可用ストレージ基盤のデータ可用性とユーザがデータを必要としてから取得するまでに要する時間を評価する。評価の精度を高めるためには、ユーザによるシステムの利用や災害時の被災に関してできる限り実際の状況を反映した条件下で実験することが求められる。

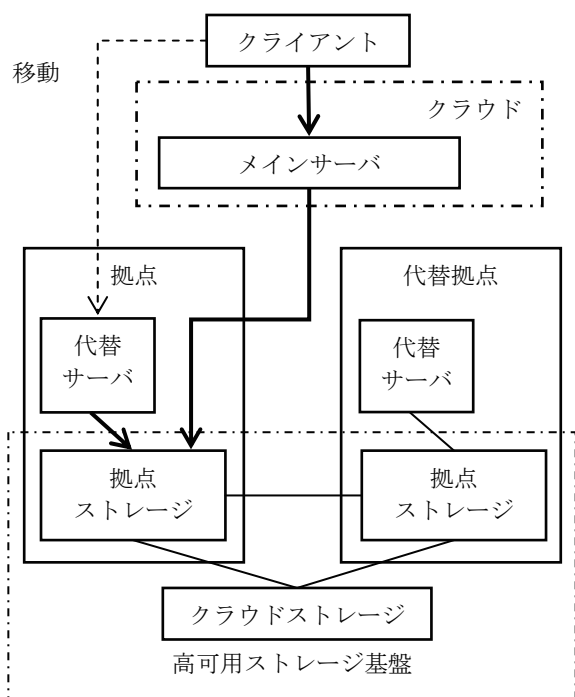


図2 災害に強い情報システムの全体像

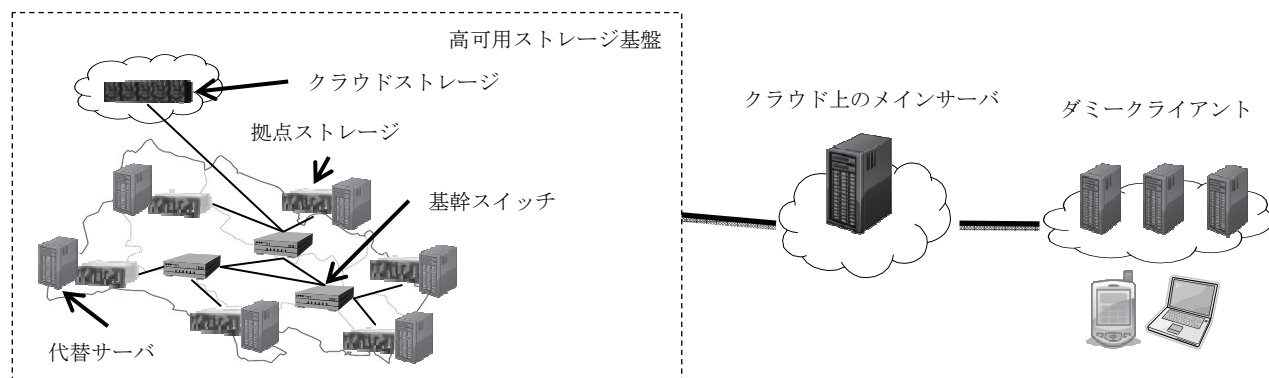


図3 実験構成のイメージ

そこで本研究では、実際に東日本大震災で被災した仙台市に高可用ストレージ基盤が設置された状況を仮定し、仙台市規模の人口となる100万ユーザが平常時や災害時にシステムにアクセスしてデータ登録や参照を行うシミュレーション実験を実施する。仙台市民が平常時や災害時に服薬履歴を登録・参照する状況や、災害発生時の実際の被災状況に基づき、100万ユーザを想定した耐災害性実証シナリオを構築する。

4.1 実験構成

実証シナリオの作成に当たり、まず実証実験の構成を決定した。実験構成のイメージを図3に示す。高可用ストレージ基盤は、仙台市に設置された100台の拠点ストレージとクラウドストレージから構成する。100台の拠点ストレージは、仙台市の各区の人口比率にしがたって各区に設置され、基幹スイッチを通して互いにネットワークにつながっているものとする。100台という数は仙台市の病院、一部の大規模な診療所や調剤薬局にストレージが設置された状況を表している。投薬情報システムは、3章でも述べたように、クラウド上のメインサーバと各拠点の代替サーバがそれぞれ配備される。クライアントには、100万ユーザによるシステムの利用をシミュレートするプログラム(ダミークライアント)を用いる。ダミークライアントは3章に記述した要領で平常時および

災害時に投薬情報システムを利用する。ただし、災害時にユーザが直接拠点に出向いて行う代替サーバへのアクセスは、ダミークライアントからメインサーバではなく代替サーバに直接データ取得要求を送ることで、ユーザが拠点に移動した状況を再現する。また、各ダミークライアントには日常生活を送る行政区が定められており、投薬情報システムを通して登録する元データはかかりつけの医療機関に相当する最寄りの拠点ストレージに格納されるものとする。

4.2 システム利用および災害時の被災対象の推定

次に、ユーザによるシステムの利用タイミングや場所、および大規模災害時の被災対象を推定するため、平常時と災害時のそれぞれについて代表的なシステム利用シナリオを整理した。利用シナリオの分岐ポイントを表1の各列に示す。代表的な利用シナリオは各分岐ポイントの選択肢の組合せとして表現できる。例えば、「平常時の利用でインターネット接続が可能であり、元データを格納する拠点ストレージが故障している場合に、通院後に帰宅してからユーザが所持する端末を用いて服薬履歴を登録する」シナリオや、「地震でインターネットが途絶して元データを格納する拠点ストレージも損壊している場合に、ユーザが近隣の病院に移動し、所持する携帯端末を用いて代替サーバから服薬履歴を参照する」シナリオなどが挙げられる。これらの分岐ポイントから、投薬情報システムの利用場所やタイミングは、病院や自宅で投薬情報を登録、確認するときであると推定される。また、災害時の被災対象にはネットワークや拠点ストレージ、ユーザの携帯端末があると推定される。ただし、ユーザが災害等で携帯端末を紛失した場合には、拠点に設置されたPC等の別端末から代替サーバを利用するなどの手段を提供可能なことから、100万ユーザによるシミュレーションでは携帯端末を被災対象としては考慮しない。

表1. システム利用シナリオの分岐ポイント

発災状況	ネットワーク	拠点ストレージ	携帯端末	場所	
平常	接続	稼働	所持	市内	病院
地震	途絶	故障	紛失		薬局
津波	輻輳	損壊	流出		自宅
火災	規制	流出	—	市外	
水害	停電	停電	—	—	

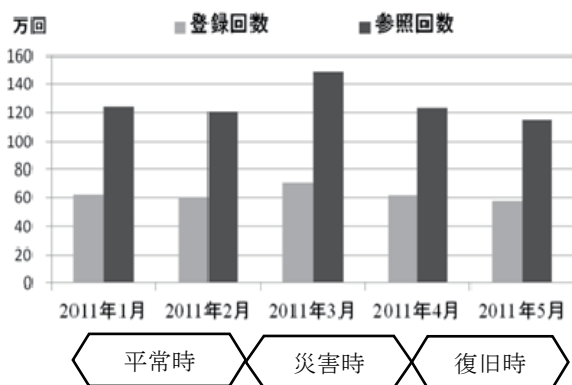


図 4 100 万ユーザの投薬情報システムの利用頻度

4.3 100 万ユーザを想定した実証シナリオ

前節の推定をもとに 100 万ユーザを想定した実証シナリオを作成する。実証期間は、実際に東日本大震災が発生した 2011 年 3 月を含む 2011 年 1 月から 5 月までの 5 か月間とする。

まず、100 万ユーザによる投薬情報システムの利用状況として、実証期間内のシステムへのアクセス頻度を設定する。前節から、通院時に医療機関や自宅で投薬情報を登録、確認する際にユーザはシステムを利用すると推定される。そのため、2011 年 1 月～5 月の宮城県の処方箋発行数から推計した仙台市の処方箋発行数を用いて、100 万ユーザによる各月の投薬情報の登録回数と参照回数を設定した。設定状況を図 4 に示す。1 月と 2 月は震災前の平常時のアクセス頻度を表し、3 月は発災直後のアクセス頻度を表している。4 月～5 月は復旧から平常時に戻る過程の利用状況を表す。このように、平常時、災害時、復旧時の 3 つのシステム利用状況に基づいてデータの可用性と取得時間を評価できるようにした。

各月の登録回数は、処方箋の発行が調剤およびユーザによる投薬履歴の登録につながるとして、仙台市の処方箋発行数の推計値そのものとして設定した。ただし、災害が発生した 3 月の登録回数については、東日本大震災で実施されたお薬手帳持参の被災者に対する処方箋なしの特例調剤の推定発生数を加算している。特例調剤の発生数は、震災で生じた 3 月 11 日～31 日までの仙台市の避難者数と仙台市人口の年齢構成比率から、避難した高齢者、児童、成人の数を推定し、高齢者の 60%、児童の 30%、成人の 10%がそれぞれ特例調剤を受けると仮定して推計している。

各月の参照回数については、登録回数の 2 倍に設定した。ユーザが通院した際、診察時にユーザによる投薬履歴の参照と医師への提示、および処方箋発行後の投薬情報の登録が行われるとすると、各月の参照回数と処方箋発行数（すなわち登録回数）は等しくなる。また、宮城県の外来患者の平均診療間隔が約 11 日であることから、仙台市の外来患者も月当たり 2～3 回通院すると見なせる。そこで今回は、診療と次の診療の間（服用期間）に用法・用量の確認等で 1 回の参照があると仮定した。その結果、月当たりの参照回数は登録回数の 2 倍となる。ただし、3 月の参照回数については、処方箋なしの特例調剤や避難所での服薬指導などにより増加する投薬履歴の参照頻度の推計値を加算した。参照回数の加算値は、3 月の登録回数の加算値の 2.5 倍とした。

次に、100 万ユーザが図 4 に示す頻度でシステムにアクセスする場合に、3 月に生じる大規模災害の被災状況を設定する。表 1 から被災対象にはネットワークや拠点ストレージがあると推定されたが、本稿ではネットワークをさらにインターネットと拠点間ネットワークに分け、

表 2 海溝型地震による高可用ストレージ基盤の損壊状況（3 月、被災直後）

	青葉区設置 拠点数 27	泉区設置 拠点数 21	太白区設置 拠点数 22	宮城野区設置 拠点数 18	若林区設置 拠点数 12
拠点	損壊 7, 残存 20	損壊 8, 残存 13	損壊 8, 残存 14	損壊 16, 残存 2	損壊 11, 残存 1
ネットワーク	損壊拠点と基幹スイッチ間で断絶			基幹スイッチ故障	
インターネット	残存拠点地域のみ接続可			接続不可	

表 3 海溝型地震による高可用ストレージ基盤の損壊状況（4 月、被災 1 ヶ月後）

	青葉区設置 拠点数 27	泉区設置 拠点数 21	太白区設置 拠点数 22	宮城野区設置 拠点数 18	若林区設置 拠点数 12
拠点	損壊 0, 残存 27	損壊 3, 残存 18	損壊 3, 残存 19	損壊 13, 残存 5	損壊 7, 残存 5
ネットワーク	復旧			損壊拠点と基幹スイッチ間で断絶	
インターネット	接続可			接続不可	

各拠点と拠点間ネットワーク、インターネット接続の 3 つとした。

東日本大震災と同様の海溝型地震による被災状況を表 2 と表 3 に示す。その他の大規模災害として、岩手・宮城内陸地震をもたらした内陸型地震による被災状況などを設定することもできる。表 2 は発災直後となる 3 月の被災状況を示し、表 3 は復旧途上の 4 月の被災状況を示している。海溝型地震のため、発災直後となる 3 月は地震や津波の影響で沿岸部の拠点やネットワークが壊滅状態となる。なお、高可用ストレージ基盤の可用性期待値を検証する目的で、発災直後は高可用ストレージ基盤の機器の半分以上が損壊または流出すると設定した。また復旧途上の 4 月では、沿岸部の被災状況は内陸部と比較して復旧の進捗が遅く、沿岸部の多くの拠点は被災した状況が継続するものとした。

被災して拠点が損壊または流出すると、拠点ストレージと代替サーバは使用できなくなる。この場合、損壊拠点到元データを格納しているユーザは複製先拠点ストレージからのデータ取得を試みる。拠点間ネットワークの被災は、基幹スイッチと拠点をつなぐネットワークの断絶と、基幹スイッチ自体の故障の 2 つを考慮する。拠点間ネットワークの被災により高可用ストレージ基盤側でのデータ複製やリストアに影響が生じる。また、インターネット接続が途絶するとユーザはクラウド上のサーバにアクセスできなくなるため、拠点まで直接移動して代替サーバからデータを取得する必要がある。さらに高可用ストレージ基盤側でクラウドストレージへのデータ複製やリストアもできなくなる。

4.4 可用性およびデータ取得時間の評価

これまで記述してきた 100 万ユーザによる投薬情報システムの利用状況、および災害による被災状況を設定に基づき、高可用ストレージ基盤のデータ可用性と取得時間を評価する。

データ可用性については、ダミークライアントが実証期間の 2011 年 1 月～5 月までの各月に投薬情報システムに要求するデータ参照の成否で判定する。ダミークライアントによる n 月の失敗した参照リクエスト数を $r(n)$ 、 n 月の参照リクエストの総数を $R(n)$ とするとき、 n 月の可用性指標 $A(n)$ を以下のように定める。

$$A(n) = (1 - r(n)/R(n)) \quad (n=1, \dots, 5).$$

ここで、失敗した参照リクエストとは、拠点の被災によって元データや複製データが喪失したなどの理由で、ダミークライアントが投薬情報を取得できなかったリクエ

ストを意味する。データ可用性の目標水準は、高可用ストレージ基盤の機器の 50% が損壊する 3 月 ($n=3$) であっても、 $A(n) \geq 0.9$ を満たすことである。

データ取得時間については、クラウド上のメインサーバにアクセスできる平常時の場合には、投薬情報システムの応答時間として計算する。災害でインターネットが途絶した場合には、代替サーバの応答時間とデータ格納拠点までの移動時間を含めた時間として計算する。この際、日常生活を送る行政区内の最寄り拠点や複製先拠点への移動時間は 10 分、隣接する行政区内の複製先拠点への移動時間は 30 分、隣接しない行政区内の複製先拠点への移動時間は 60 分と設定している。

ダミークライアントによる n 月のデータ取得時間(分)を $T(n)$ とすると、

$$T(n) = (1/R(n)) * \sum_i t_i(n) \text{ あるいは } T(n) = \max_i \{t_i(n)\}.$$

ただし、 $t_i(n)$ は n 月の i 回目のデータ取得時間である。実用的な時間内でのデータ取得を考慮すれば、平常時であれば $T(n)$ は数秒～数分以下、災害時であっても数十分～1 時間程度に収まる必要がある。

5. おわりに

本稿では、文部科学省の委託事業「高機能高可用性情報ストレージ基盤技術の開発」の研究成果として、投薬情報システムを題材とした高可用ストレージ基盤の耐災害性実証実験に用いる実証シナリオについて報告した。

委託事業で開発する高可用ストレージ基盤技術の目標は、災害によりストレージ機器の 50% が損壊しても 90% 以上のデータに実用的な時間内にアクセスできることである。本研究では、東日本大震災の被災地である仙台市に高可用ストレージ基盤が設置された状況を仮定し、仙台市人口規模の 100 万ユーザによるシステムの利用や大規模災害による被災状況を想定した実証シナリオとすることで、高可用ストレージ基盤のデータ可用性やユーザによるデータ取得時間を高い精度で検証できる。

今後は、本研究で作成した実証シナリオに沿って、投薬情報システムを用いた高可用ストレージ基盤の耐災害性実証実験を推進していく。

6. 謝辞

本研究の成果は、文部科学省の委託事業「高機能高可用性情報ストレージ基盤技術の開発」の研究成果の一部である。

参考文献

- 1) 地方自治情報センター：東日本大震災における地方公共団体情報部門の被災時の取組みと今後の対応のあり方に関する調査研究, LASDEC 調査研究報告書, (2012).
- 2) 田中博:災害時と震災後の医療 IT 体制 そのグランドデザイン, 情報管理, Vol.54, pp.825-835, (2012).
- 3) 総務省：災害時における情報通信の在り方に関する調査結果, 平成 24 年 3 月総務省報道資料, (2012).
- 4) 総務省：平成 24 年版 情報通信白書, (2012).
- 5) 高梨勝敏 他：避難から復興までのコミュニティ支援システムーコミュニティ形成・維持の要件と段階的開発ー, 情報処理学会デジタルプラクティス, Vol.3, (2012).
- 6) 松本慎也, 他：広域災害向けリスクアウェアデータ複製方式の提案, 電気学会第 55 回情報システム研究会, pp.39-43, (2013).
- 7) 日本薬剤師会, “東日本大震災における活動報告書について”, プレスリリース (平成 23 年度), 2012.



宗形 聡 2003 年入社
研究開発部 研究開発グループ
高可用ストレージ基盤の耐災害性実証実験, および意思決定支援技術の研究開発
satoshi.munakata.tu@hitachi-solutions.com



宋 チュウ 2008 年入社
研究開発部 研究開発グループ
高可用ストレージ基盤の耐災害性実証実験, および RIA 技術の研究開発
chong.song.ty@hitachi-solutions.com



手塚 大 1994 年入社
研究開発部
意思決定, リスク分析, 最適化技術の研究, 開発
masaru.tezuka.fd@hitachi-solutions.com