情報システムと災害リスク

畑山 満則
京都大学防災研究所

概要：災害対応においてハード対策を補う被害防止や軽減活動には，必要十分な準備と迅速な意思決定が求められる．情報活用は災害対応活動において一つの大きな役割を果たすことになる．本稿では，被害防止・軽減で利用される情報に着目し，情報伝達・共有を実現するために構築される情報システムについて考察する．

キーワード：災害対応，災害リスク，情報システム

1. はじめに

災害対策基本法第二条第二項において「防災」とは「災害を未然に防止し，災害が発生した場合における被害の拡大を防ぎ，及び被害の復旧を図ること」と定義されている．阪神・淡路大震災以降，災害そのものに堤防や護岸などの構造物をもって立ち向かうハード対策の限界が指摘され，それを補う被害防止，軽減活動（ソフト対策）に注目が集まってきた．東日本大震災においても，防潮堤をはじめとするハード対策は，設計仕様を超える事象にきわめて脆弱であることが再確認されており，ソフト対策を強調する「減災」の意識がさらに高まったといえる．被害防止や軽減には，必要十分な準備（過度な準備は迅速な行動をかえって妨げる場合がある．例えば避難袋に荷物を詰めすぎ，実際にそれを持って避難することが難しくなるなど）と迅速な意思決定が求められるが，そのためには情報の活用が一つの大きな役割を果たすことになる．すなわち，必要な情報を取得することができれば，効果的な減災活動が可能となるといえる．本稿では，被害防止・軽減で利用される情報に着目し，情報伝達・共有を実現するために構築される情報システムについて考察する．

2. 災害リスクとレジリエンシー

災害リスクとはどのように定義されるのであろうか．災害リスクの定義として図1のような Hazard − Exposure − Vulnerability モデルがある．この図において Hazard とは，その場所での災害原因となる自然現象（地震・洪水・津波など）の発生する可能性を示し，Exposure とは，そのような災害に晒されている人や資産を指す．Vulnerability は，災害に対する脆弱性を示すが，これはどの程度の対策ができているかということの裏返しとしてとらえることが多い．この3つの要素の重なりで災害リスクは定義されるのであるが，Hazard は人の力でコントロールすることはできない．つまり Exposure や Vulnerability を変化させることで災害リスクを軽減化させることが可能となる．この観点からみると情報システムは Vulnerability を下げる（災害対応力をあげる）という部分に貢献が期待されるものであるが，同時に情報システムそのものも災害リスクに晒されている資産と解釈することもできる．つまり，情報システムと災害リスクについて述べるならば，この両面からのアプローチが必要となるのである．

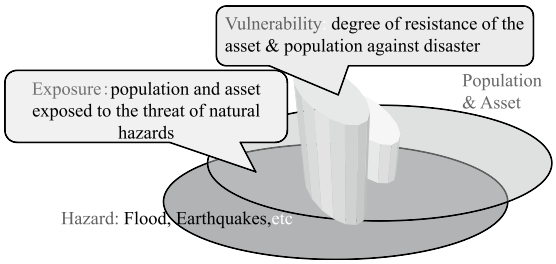

図1. 災害リスク

災害リスクを軽減化させるためにはどのような方式があるのであろうか？ここでは，図2のような災害発生からのインフラやサービスなどの機能水準の推移モデルを用いて考えてみる．このモデルでは，災害発生前の機能水準を100％と考え，災害発生とともに機能低下した水準が元に戻ることで復旧・復興が遂げられると考える（現実には元の水準まで戻らないことや元の水準以上に機能があがることもある）．これを実現するためには，図3に示すような2つの方策が考えられる．すなわち，災害に対する抵抗力を高めて被害を抑止すること，回復力を高めて復旧時間を短

縮することである．これらは災害発生時の対応だけでなく，事前の準備時点からできることをやっておくことが必要である．このように総合的にマネジメントがなされることで，図2に示されるように機能低下を示す三角形を小さくすることが求められるのである．このような状態は，風になびく柳のようなしなやかさをもつ（レジリエンシーの高い）社会と表されている．

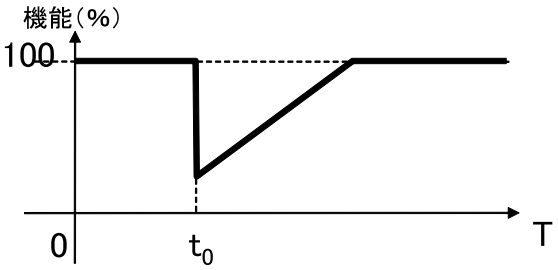

図2. 災害発生からの機能水準の推移モデル

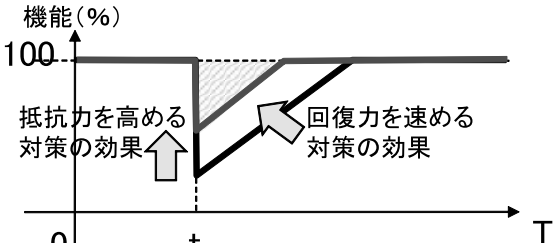

図3. 総合的な対策

3. ICTの高度化と巨大災害

Exposureが正しい情報を取得することは抵抗力や回復力を高めることにつながると考えられる．しかしながら，阪神・淡路大震災まではこれを実現するための技術が伴わないため，遠距離間や不特定多数の対象への情報伝達・情報共有は，テレビ・ラジオや災害対応のための特殊な手段の利用に限定されていた．しかしながらICTの高度化と技術の普及にともない．それ以外の手段を用いた情報伝達・共有の可能性が指摘され，期待が高まっている．しかしながら，これらの期待は部分的に実現されるものの，期待したレベルに対して十分に応えた事例はまだ少ない．ここでは，このような期待と現実のギャップが生まれた背景について述べる．

3.1 災害対応に係る情報通信技術の環境

IT革命は1990年代後半に加速したといわれている．阪神・淡路大震災が発生した1995年の情報通信環境とその後の変遷について，防災情報技術の高度化に大きく係るものを取り上げ振り返る．

(1) PC環境

PC環境は，1995年末にマイクロソフト社からWindows95が発売されたことを契機に大きく変わる．CUI（Character User Interface）からGUI（Graphical User Interface）にインターフェースが変わったことで，個人利用のユーザが格段に増え，コンピュータの利用は特殊なことではなくなった．情報化がなかなか進まないと言われる自治体業務であっても，阪神・淡路大震災発生時にはメインフレームを用いた所謂レガシーシステムが中心であったが，この変化により互換機，共通OSを用いたオープンシステムに急激に移行した．さらに，1990年前後から発売されていたラップトップPCが，可搬性と省スペース性から，多様な業務を様々な場所でこなす必要のある災害対応業務に有効であると認識された．

(2) インターネット

インターネットの民間利用は，阪神・淡路大震災以前から可能であった．1994年にそれまでに比べると格安でインターネット接続サービスを提供する民間プロバイダが現れ，PCの普及とあいまって，またたく間に普及した．

Web上のコンテンツは，ホームページ作成や掲示板を用いたサービスにより増え始めたが，日単位で更新されるブログサービスが普及することで爆発的に増えた．その後は，SNSサービスが始まり多様性を増した．近年では分単位で更新されるマイクロブログが普及し，溢れかえる玉石混合の情報から必要な（有用な）情報を取り出すことが必要となっている．

(3) 通信技術

携帯電話は，阪神・淡路大震災時に固定電話にはない利便性が注目され，その他の社会のトレンドとあいまって急激に普及した．インターネット接続について固定電話からモデムを介して接続する方式から，ADSL，FTTHと利用の中心が変わってき

た．また，公衆無線 LAN サービスも広がり，都市部ではどこでもインターネットに接続できるようになっている（地方はこの限りではない）．携帯電話からのインターネット接続は各通信キャリア独自で整備が進められ，スマートフォンの出現により直接接続が可能となった．

(4) 情報収集デバイス

阪神・淡路大震災時には，使い捨てカメラが利用されたが，デジタルカメラの普及や携帯電話へのデジタルカメラ機能の付加により，簡便に写真撮影可能となった．ハンディタイプ GPS の低価格化，カーナビゲーションの普及なども相まって写真に位置情報を付加することも容易になった．リモートセンシング技術の発達により航空写真や衛星写真から大まかな災害状況を把握することも可能となった．

3.2 震災時での利用

阪神・淡路大震災以降，情報通信環境は大幅な進化をとげた．それに伴い，災害情報の共有技術も大きく進んだが，情報課題はまだ山積している．災害直後数週間の混乱期を想定し，情報の送受信の主体を被災地内外に分類した上で，この課題に対し考察を試みた．

(1) 被災地外での情報共有

阪神・淡路大震災の時に比べて格段に多くの情報がインターネットを通じて公開され，閲覧されるようになった．東日本大震災では，掲示板サイト，ブログ，ツイッターを通して多くの人が情報発信しており，YouTube や USTREAM を通じてテレビの生放送も中継された．震災以前に期待されていた，もしくはそれ以上の効果を発揮したといえるが，逆に追うことができない情報が飛び交い，情報過多の状態となるという課題も見え始めた．

(2) 被災地外と被災地内との情報共有

このカテゴリーでは被災地域在住者の安否を問い合わせる内容が多い．これには被災者が安否情報を発信することが有効であるが，被災者は情報発信するすべを持たないことが多く，情報共有ができない状態に陥りやすい．阪神・淡路大震災では掲示板サービスを使って被災地外から被災地内の人に家族の安否確認を依頼し，確認がなされた事例があったが，その後は，家族や友人が集っていたブログ，SNS が利用されるようになり，東日本大震災では Twitter を用いて確認された例がみられた．Google はパーソンファインダーサービス，避難所名簿共有サービス，YouTube を通じた被災者の動画メッセージによる消息情報チャンネルを提供し，新たな可能性を示した．携帯情報端末が発達しソーシャルサービスが普及した今後は，“通信インフラの確保と電力供給さえなされれば”このカテゴリーの課題はクリアされる可能性が高い．

(3) 被災地内での情報共有

このカテゴリーでは，停電，通信施設の破壊などにより情報通信技術の利用が難しく，東日本大震災でも多くの課題が確認された．緊急地震速報や津波警報が様々なデバイスから取得できるようになったことで大きな進歩を遂げているが，発信された情報に気づかない車や人がいることは多くの災害報道で確認されており，情報活用に関する検討が十分ではなかったということが分かる．また，防災無線から避難を呼び掛けていた人が津波に呑み込まれた事例も報告され情報提供者側の安全確保の問題も考慮すべきことが認識された．被害想定地域にいる人すべてに情報を届けるために取るべき方法について今後新たな手法が必要であろう．

4． 情報システムが持つリスク

2 章で述べたように情報システムを，被害を軽減させるための重要な資産と考えるならば，情報システムそのものが災害リスクをもつことになる．阪神・淡路大震災では，神戸市役所においてサーバーが設置されているフロアが倒壊し，情報を取り出せない状態に陥ったことを受け，その後はシステムを格納する建物やフロアの耐震性を強化，コンピュータそのものの堅牢化，無停電電源装置（UPS）や予備電源の準備といった Vulnerability を下げる対策がなされてきたが，クラウドコンピューティングの台頭とともに，データセンターそのものの移動，分散，つまり Hazard ―Exposure 間の位置関係の見直しによる災害リスク軽減化対策が脚光を浴びている．東日本大震災では，役場ごと津波に流されデータを全損させた自治体が存在した傍らで，クラウド化により情報の回復が

迅速に行われ，効果的な対応を行った自治体も存在する．また，被災地外からも支援の輪に加わることが可能とすることで，災害現場の人的リソース不足を補うことも可能とした．これらにより次の大災害での情報システムの在り方について新たな可能性を示した．以下では，その可能性を実践するために考慮しておくべき3つ課題について考察する．

(1) 新しい技術の持つリスク

クラウドコンピューティングは，これまでの問題を解決する可能性を持つ手段であるが，この技術がもつ独特のリスクが存在することも忘れてはいけない．まず，移行，分散したデータセンターの場所にもハザードが存在するということである．日本国内であれば，多くの場所で地震ハザードは存在する．国外には地震リスクのほとんどない場所も存在するが，国内の法律が適応されず，データ保護の観点から災害リスク以外のリスクに晒される可能性もある．また，利用している場所と同じハザードを持つエリアにデータセンターを置く形では，災害リスク軽減につながらないため，十分に距離のある位置にデータセンターを置く必要があるが，この場合，センターへのアクセスはインターネットへの接続が必要になる．災害時には利用側での通信インフラが途絶し，接続ができない時期がでる場合も多いので，この時間帯では利用できない．インターネットは局所的な切断が全体の安定性に及ぼす影響が小さいところから「災害に強い」と評されることがあるが，切断された先からは当然アクセスできないことを想定しておかなければならない．

(2) 新しいサービスの持つリスク

災害対応システム，特に，命にかかわるシステムでは初期不良は許されない．また，想定しうる利用シナリオがサポートされていないこともあってはならない．しかし，低頻度な巨大災害の対応では，新しい技術は，限定された環境，緊迫した状況で初めて実戦で利用されることが多いため，このような問題を引き起こすことが多い．例えば，携帯電話からの災害伝言版サービスに関しては，中越地震時にキャリア間情報共有ができなかったり，東日本大震災直後にはスマートフォンからの利用ができなかったりといった問題が指摘されている．防災訓練などで問題点の解消に努めていることが多いが，災害時を想定するシナリオが十分に検討されていないと問題点を表出化させることができない可能性がある．

(3) 新しい技術を支える人材の問題

新しい技術やサービスは，技術力の高い人によって支えられている場合が多く，それが付加価値を生んでいる．しかしながら，災害時という緊急性が高く，平常時には経験することのない大量なユーザからのアクセスに対応するためには，人海戦術も必要となる．この問題を避けるためには災害時の専門技術を持つ人員の確保が必要になる．平常時からバックアップ要員を教育しておくことが最良であるが，それが難しい場合は他の機関への応援要請で対応するという方法もある．このようなことを想定し，事前に相互応援協定などを結んでおくことができれば，災害時にあわてることなく対応が可能となる．

5. 情報システムによるレジリエンシー向上

2章で述べたように災害に対するレジリエンシーを高めるために情報システムを積極的に用いることが近年検討されている．BCP（事業継続計画）やBCM（事業継続管理）では，情報の利用は最重要事項に挙げられているが，その性質は，大きく分けてシステムバックアップという側面と災害発生時の情報収集・伝達・管理という側面がある．前者は，平常の事業を目標時間内で復旧し，継続するために重要な役割を果たすため注目を浴びている．バックアップが自動で取られ，電源と通信インフラが回復すれば利用できるようになることからクラウド利用の価値は高い．後者については，災害時に（特に災害直後に）被災地内で利用することが想定されるため，前者と同じコンセプトでのシステム構築では問題が出る場合がある．例えば，安否確認など命にかかわる作業を企業・大学や行政が行うことになる場合，対象となる人が確実に利用できる環境を提供することが求められる．そのためには，ベストエフォートでの成果としてえられるシステムではなく，ギャランティ型のシステムが求められ，そのためにはコストがかかることを考えておかなければならない．

6. おわりに

災害時における情報システムとそのリスクについて考察を行った．災害時の抵抗力を高めたり，回復力を速めたりする（レジリエンシーを強化する）ために情報システムに対する期待は大きいが，それを実現するためには情報システムそのものにも災害リスクがあることを意識しておく必要がある．ICT の進化は非常に速い一方で，阪神・淡路大震災や東日本大震災のような巨大災害の発生頻度は低いことから，情報システムに対する期待は先行しがちである．そのため，被災者を十分に納得させるような成果はまだ多いとは言えないが，阪神・淡路大震災以降の様々な取組から，確実に利用できるシステムが生まれていることも確かである．災害のたびに多くの情報技術者により支援システムの開発と提供がなされているが，その活動と成果に敬意を払う一方で，開発・導入されたシステムそのものの評価（限定された期間内でコストを抑えて開発されたことなどを差し引いた評価）を行い，次に生かすことも重要である．さらに，東日本大震災以降の情報技術の進化と社会への普及度合いなどから，実績あるシステムや可能性を示したサービスを，次の災害時にも確実に稼働できるように，常に見直していくことが必要であると考えている．

最後に東日本大震災における被災地の一日も早い復興を願い，本稿を閉じることにする．