東日本大震災にみる情報セキュリティと企業行動

田川義博[1]

概 要

2011年3月11日に発生した東日本大震災では,巨大地震,巨大津波,原発事故によって甚大な人的・物的被害が発生した.主たる被災地である岩手,宮城,福島の東北3県は,現時点いまだ復旧過程にあり,本格復興に向けた動きはこれからである.今回の大震災では,インフラ設備や企業の生産設備に大きな被害が発生するとともに,通信ネットワークの脆弱性が露わになった.

また,インターネットを活用してICT企業やNPO・ボランティアが,被災地・被災者支援に貢献した一方で,インターネットを利用して流言・デマが流され,加えて大震災に便乗する形でウイルス攻撃等がみられた.

本論では,大震災においてみられた事例を分析しつつ,情報セキュリティの問題,企業行動に係る問題,さらには今回の大震災がリスクの基本問題および今後の情報セキュリティ問題に対して与える示唆について考える.

1. はじめに

2011 年 3 月 11 日に発生した東日本大震災では,マグニチュード 9.0 の巨大地震と巨大地震が引き起こした巨大津波によって,甚大な人的・物的被害が発生した.また,福島原発の水素爆発や放射線物質の拡散によって,周辺市町村の住民の居住地からの避難が現時点でも続いており,また避難地域における復旧活動の停止が続いている.

本論では,このような東日本大震災における発生事象のうち,まず第一に全体的な発生事象・局面推移に触れた後,第二に情報セキュリティに関してみられたさまざま事象を分析する.ついで第三に今回の大震災における企業行動について述べる.そして第四に今回の大震災のリスクの基本論および今後の情報セキュリティ問題へ与える示唆について考える.

2. 東日本大震災の全体事象

2.1 全体事象

[1] 情報セキュリティ大学院大学セキュアシステム研究所客員研究員

東日本大震災では,自然災害である巨大地震と巨大津波によって,東日本の太平洋沿岸の市町村で多数の死者・行方不明者が出た.また,建物の倒壊・流出,電気・ガス・水道・道路・鉄道・港湾設備などのインフラ設備および生産設備に大きな被害が発生した.

これとともに,情報セキュリティに密接に関係する通信ネットワークが,広い範囲で可用性を喪失した.加えて地震・津波によって,原発事故が発生し,近隣住民が居住地から避難を余儀なくされるとともに,放射線物質の拡散・汚染によって農畜漁産物が出荷停止に追い込まれた.これらの状況は,いまだ終息していない.

東北・関東では,多くの企業が生産中断に追い込まれ,多くのサプライ・チェーンが寸断したことで,国内だけではなくグローバルにもその影響が及んだ.このことで,経済活動がグローバル化していることを再認識させられた.

また首都圏では,多くの帰宅困難者や液状化現象の発生し,東京電力管内では計画停電が実施された.さらに,より広範な地域において,買いだめや消費に関する自粛ムードが広がった.以上のような事象を概観したのが,図表 1 である.

図表 1　東日本大震災における発生事象

＜自然災害	（被災地,被災地外）	人災・2 次被害　＞
＊巨大地震		
＊巨大津波	＊原発事故	[人々の冷静な行動・支え合い]
・死者・行方不明者	・放射線物質汚染（大気,水,土壌）	・水等摂取制限
・家屋の倒壊・流失	・避難指示,農畜漁産物出荷停止	・風評被害
・電気・ガス・上下水道:可用性喪失		・計画停電
・道路・鉄道・空港・港湾・漁船・養殖設備:可用性喪失		・液状化現象
・通信・放送:可用性喪失		・帰宅困難者
・産業設備・流通網（店舗等）:可用性喪失,ガソリン不足		・買いだめ
・被災地での地盤沈下現象		・自粛ムード

注:網掛けは原発事故関連の事象

2.2 巨大地震発生以降の重点取り組み事項の局面推移

3 月 11 日の大震災発生以降,さまざまな主体が懸命に支援・復旧活動を行なってきたが,時間の経過とともに活動の重点が変化しており,それに伴い活動の主体も変化している.

発災直後は,緊急地震速報や巨大津波来襲に対処する避難勧告・避難指示の発出,住民の高台への避難,ついで生存者救助,避難所開設などが焦点となり,被災者への緊急支援,医療・介護の応急措置などが行なわれた.他方で,インフラ復旧,流通網・生産再開への取り組みが行なわれ,金融財政もこの取り組みを支えた.

その後の被災者への生活支援では,大量のボランティアが活動した.また仮設住宅の建設が進むなかで,現在は雇用確保など生活安定策の実施,被災地の復旧・復興計画の作

成,予算措置などに重点が移っている.将来的には,被災者がよりよく生きるための支援,被災者が未来へ希望がもてる支援が求められる.

もっとも,原発事故に関しては,放射線物質拡散による土壌・水質・農畜漁産物汚染問題が終息いない.また一部で土壌に含まれている放射線物質の除染が始まっているが,避難生活は現時点でも継続しており,原発事故の悪影響は,現時点でも続いている.

この局面推移を概観したのが,図表 2 である.

図表 2　巨大地震発生からの重点取り組み事項の局面推移

＊現在の中心は 8・9 局面,4 は依然継続中.これから 10・11 局面へ.

(1)巨大地震(2011.3.11 14:46 分頃)・巨大津波来襲
➔気象庁・防災機関・自治体の被災地住民への情報伝達
(緊急地震速報,避難勧告・指示)
(2)死者・行方不明者発生,甚大な物的被害の発生,原発事故発生
➔生存者救助,避難所等への避難誘導,原発緊急対応(東電)
➔主として,自衛隊,警察,消防,自治体.海外からの支援も
(3)被災者への緊急支援,医療・介護の応急措置,被害状況把握
➔主として,自治体,医療機関,自衛隊・米軍.海外からの支援も
(4)原発事故への対処:現在も継続中の取り組み
➔東電,(外国を含む)メーカー,政府(指示・監督),外国政府・IAEA
(5)経済,産業活動,金融などへの影響評価と対処策の実施
➔主として,政府,日銀,金融機関,経済団体,企業
(6)インフラ復旧,流通網回復,生産設備(漁業等を含む)復旧
➔主として,事業者および行政機関
(7)被災者への生活支援,医療・介護支援,避難所の移転・統合など
➔主として,自治体,ボランティア(プロボノを含む)
注:プロボノとは専門技能・知識を活用してボランティア活動をする人のこと.
(8)仮設住宅への入居,教育,雇用・仕事など生活の安定策,ガレキ撤去
➔主として,県・自治体,政府,企業
(9)被害補償,義援金の支給基準・配布,生保・損保保険金の支給
➔東電,義援金配布団体,政府,自治体,保険会社
(10)復旧・復興を支援する補正予算,新たな企業立地・雇用創出,除染
➔政府,国会,自治体,企業,有識者,地域住民
(11)被災者がよりよく生きるための支援:文化,娯楽,安らぎ,きずな
(注:ニューヨークの 9.11 被災時は,買い物するとブロードウエーのチケットが貰える施策が行なわれ,街の雰囲気が変わった.)

3. 情報セキュリティに関する事象

3.1 通信ネットワーク(conduit)の可用性

今回の大震災では,情報システムよりも,通信ネットワークの可用性喪失が大きな問題となったが,状況は被災地と被災地外では全く異なる.

また,津波被害が集中した岩手,宮城,福島の東北 3 県でも,巨大地震・巨大津波に襲われた太平洋沿岸地域と,巨大津波が来襲しなかった内陸部では,同じ県内でも状況は大きく異なる.

被災地は,固定電話,携帯電話の音声通話・メールおよびインターネットがほぼ利用できなくなった.これは地震・津波のために,通信回線,交換局,基地局などの通信ネットワークを構成する設備が損壊・流失したことに加えて,停電による電源喪失および輻輳発生によって通信規制がかけられたためである.停電の影響は岩手県と宮城県の内陸部に,また通信規制は被災地外にもその影響が及んだ.

まず通信ネットワークへの具体的な被害は以下の通り[2]であるが,各事業者の懸命な復旧作業により,4 月末までに原発事故避難地域など一部を除き,おおむね復旧した.

① NTT 東日本の固定回線については,385 ビルが機能停止,沿岸部の架空ケーブルが 6,300km損壊・流失,中継伝送路が 90 ルート切断,沿岸部の電柱が 65 千本折損・流失した.この結果,190 万のアクセス回線が被災した.

② 携帯電話・PHS 基地局は,基地局と交換機の間のエントランス回線に NTT 東日本の伝送路を利用しているため,この伝送路の被災および長時間の停電によりバッテリー等が枯渇したことで,約29千基地局が機能停止した.

つぎに,利用が発災直後から急増したために輻輳が発生したことによって,

③ 固定電話の音声発信に関して,最大 80～90%の通信規制がかけられた.

④ 携帯電話では,音声では最大 70～95%の通信規制がかけられたのに対して,パケットに関しては,ドコモで最大 30%の通信規制がかけられたものの,他の事業者は通信規制をかけなかったため,音声に比べ比較的疎通しやすかった.ただし,各社ともメールサーバーの輻輳により,送信メールの到着には,通常よりも長い時間を要した.

これらとともに停電のため,テレビ放送が視聴できなくなった.加えて,津波による設備流失や停電のため防災行政無線の多くが損壊し,発災直後から,または一回目の津波の高さを伝えたのちに,二回目以降のより高い津波の情報を伝えることができなかった.このように通信手段が壊滅状態になったために,避難の呼びかけが十分に行なえなかった.加えて避難の呼びかけを聞いても,避難しなかった住民が多数したことが,犠牲者を増やすことにつながったのではないか,との指摘もある.[3]

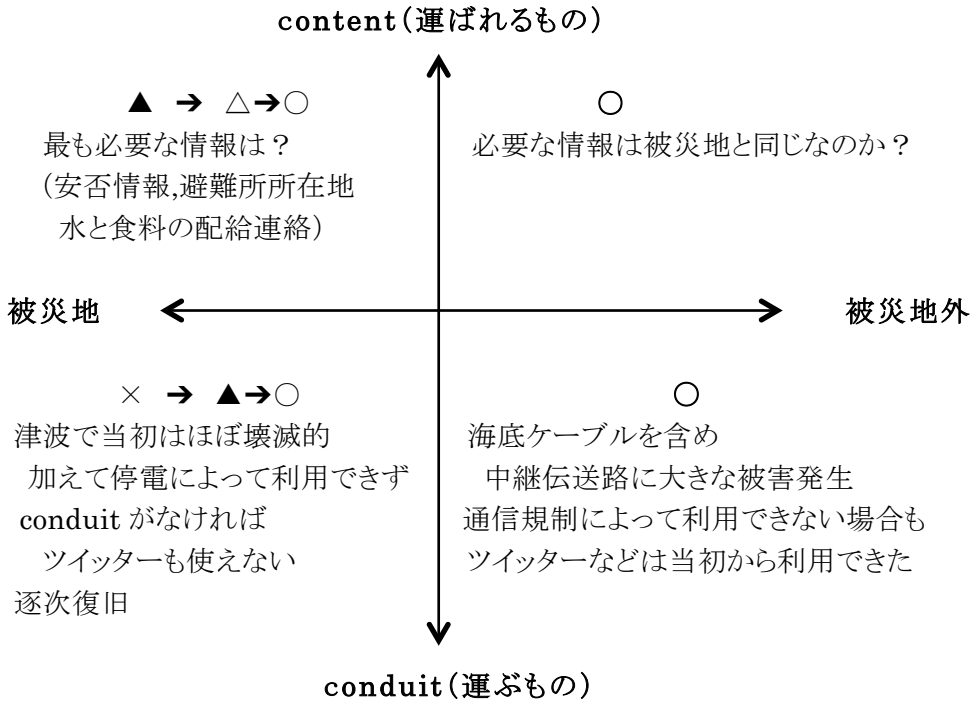
今回の大震災では,固定電話や携帯電話は利用できなかったが,ツイッターなどインターネット系のサービスは利用できたとの声が多い.しかし,通信・コミュニケーションでは conduit と content の両方が必要である.すなわち.,通信・放送ネットワークのような conduit(運ぶもの)が利用可能であってこそ,content(運ばれるもの)が利用できるのである. この被災地と被災地外の状況の違いを,conduit と content の軸に分けてみたのが,図表 3 である.

---

[2] 出典:「知識情報社会の実現に向けた ICT 政策の在り方:中間報告」総務省情報通信審議会,2011 年 7 月 25 日.

[3] この避難の呼びかけがあっても,避難をしない人々が多数いることに関しては,以下の文献を参照.
河田恵昭[2010]『津波災害』. 広瀬弘忠[2004]『人はなぜ逃げおくれるのか』.

図表 3　被災地と被災地外:conduit とcontent の関わり方



注:×　可用性喪失　▲ほぼ可用性喪失　△　可用性一部喪失　○　可用性確保

3.2 被災地における情報の可用性

3.1 で述べたように,主として津波により被災した地域では,発災直後,通信設備の損壊・流失,停電,通信規制によって,通信ネットワークやテレビ放送が,ほとんど利用できなくなった.すなわち生存者救助,被災者の避難,被災者支援活動,安否確認,また,さまざまなインフラ設備や生産設備の被害状況の把握と復旧活動を行なうために,最も必要とされる時期に,緊急情報を伝える conduit がほぼ壊滅状態になった.被災地の沿岸部では,電池利用のラジオや壁新聞,伝言板などの非電子的手段が役立ったとの声が多い.

発災直後のような緊迫した状況において,関係機関が刻々と変化する状況に対して,可能な限り迅速かつ的確に対応するには,情報が不可欠であるが,個別の事象は別として,実際にどのような状況であったのかについては,現時点でも必ずしも全体を概観できる発表はなされていない.

実際の被災地の状況を推測するために,iSPP(情報支援プロボノ・プラットフォーム)[4]が岩手,宮城,福島の 3 県の住民を対象に,2011 年 7 月に行なったインターネットによるアンケート調査(110 市町村,有効回答者数 2,815 名)と,現地の iSPP 関係者による面接調査(42 市町村,回答者数 186 名)の結果をみてみよう.この調査の特徴は,インターネット調査と個

[4] iSPP(情報支援プロボノ・プラットフォーム)の概要については,以下の URL を参照.
http://www.ispp.jp/

別面接調査の両方を行なったこと,多くの市町村の住民を対象としていること,甚大な被害が発生した沿岸部と,沿岸部ほどの被害が発生しなかった内陸部に分けて分析していることである.

また,インターネット調査の有効回答数 2,815 名のうち,内陸部の回答者数が 2,141 名であるのに対して,沿岸部の回答者数が 674 名と割合が小さいのは,被災地の生活状況およびインターネットの普及状況から肯ける.一方で,個別面接を行なう対象者を得ることが困難と思われる沿岸部で,186 名中 112 名の面談調査が行なえたことは, iSPP の関係者の努力の賜物であると思われ,それだけにこの調査の価値があるといえる.

調査目的は,「東日本大震災に際し,被災地住民が,震災発生以降,必要な情報をどのように入手・発信・活用できたか,あるいはできなかったか,それらの要因は何であったか」を探り,「今後の災害時の情報施策立案に資するデータを得る」ことと「具体的に有用な新たなサービス,システムの提案を行なう」ことである.

調査結果で明らかになったことは,沿岸部住民の圧倒的な声は「使えなかった」である.沿岸部住民からは,「固定電話,携帯電話,テレビ,インターネット,ツイッターなどすべて無力であった.」,「電源喪失に対する備えがなかった.」,「東京ではツイッター,SNS などが活躍した.しかしこれは首都圏の話がメインで,被災地では事実とは限らない.」というコメントがあった.

これに対して,内陸部住民は,「ツイッターによって災害情報やインフラ関係の様々な情報を得ることができた（岩手県）」,「伝言ダイヤルがつながらなかった.電話がつながらなかった.情報が錯そうしていた.（岩手県）」,「ライフラインがすべて止まっていたので,せめて携帯電話の使用が可能であったらよかった.（宮城県）」,「自宅の辺りでは停電していなかったので,直後からテレビやラジオは視聴できた.（福島県）」と回答しており,状況は大きく異なる.また,個別の情報源としては,携帯電話に不満が集中している.

この調査結果を読み取るときに,注意すべき点が二つあるように思われる.

第一に,沿岸部,内陸部で状況が異なるが,通信・放送サービスの可用性喪失の原因が,通信設備自体が地震・津波で損壊・流失した場合,停電になり予備電源も利用できなくなった場合,輻輳発生のため通信規制がかけられた場合のそれぞれで,正常化するまでの時間の長さが異なることである.一番早く正常化するのは,通信規制が解除された場合であり,ついで電気が使えるようになった場合である.最後まで残るのは,通信設備が損壊・流失した場合である.この場合には,通信設備自体を復旧しなければならないため,時間がかかる.

二つ目は,携帯電話が利用できなかったことに,不満が集中したことである.大震災の発生によってさまざまなインフラや設備が損壊・流失したが,情報が途絶または混乱しているなかで,場所ごとに利用可能な通信手段が,何であるかについての情報もなかった.このため,日ごろから携帯電話に大きく依存して生活している住民が,携帯電話を最も利用したい緊急時に,利用できないことに大きな不満を持つことは,当然のことである.

この二つの注意点が企業の情報セキュリティに関して意味することは,まず第一に情報システムの可用性喪失の時間の長さは,喪失原因によって異なることである.予備電源の利用可能時間を超えて停電が続けば,情報システムの可用性が喪失する.また,情報システム自体が損壊した場合には,その情報システム自体の復旧にどの程度の時間を要するか,または代替手段をどの程度すみやかに利用できるかによって,企業全体の復旧のスピードが大きく変わる.

ついで第二に企業活動において,情報システムに対する依存度が高くなればなるほど,情報システムの可用性喪失に対して,経営者,社員から大きな不満が出ることを,この調査結果は示唆しているように思われる.すなわち,情報システムと情報を活用して,企業活動を行なえば行なうほど,情報システムが利用できなければ,大きな悪影響が生ずる.したがって,情報システムの可用性に関して,予防策を講ずるとともに,被災した場合にはすみやかな復旧を図ることが強く求められるといえよう.

また,野村総研が 2011 年 3 月 19 日から 20 日に,関東圏居住者3, 224名に対して,自社のパネルを利用したインターネットによる「震災に伴うメディア接触動向に関する調査」を実施し,その結果を3月 29 日に公表した.この調査では,震災情報を入手するに当たって,どのメディア(情報源)を重視したか,またインターネットを含むそれぞれのメディアに対する信頼度が,どのように変化したかを調査している.

この調査によれば,重視しているメディアとしては,「NHK テレビ」が 80.5%と圧倒的に高い.ついで「民放テレビ」(56.9%),「インターネットのポータルサイト」(43.2%),「新聞」(36.3%),以下インターネット系,ラジオ放送が続いている.また,信頼度の変化に関して,「信頼度が上昇した」とする割合は,「NHK」(28.8%),「ポータルサイト」(17.5%),「ソーシャルメディアでの個人の情報発信」(13.4%)となっている.

ここで注目すべきことは,「ソーシャルメディアでの個人の情報発信」に関して,「信頼度が上昇した」との回答が 13.4%と,上昇原因の第 3 位になっている一方で,「信頼度が低下した」との回答も9.0%と,低下原因の第3位になっていることである.これはソーシャルメディアの利用に関して,回答者の実体験に左右されているためであると推測される.すなわち,ソーシャルメディアを利用したことで,安否確認などの有益な情報を得られた人と,4.5 で述べるように,チェーンメールやツイッター上の流言・デマで混乱を経験した人とが両方存在しているため,意見が分かれたものと考えられる.

3.3 情報システムおよび情報の可用性確保に対する取り組み事例

被災地の県や市町村のウエブサイトが,地震,津波とそれに引き続く停電によって,可用性を喪失するケースが発生した.また情報入手手段が限られるなかで,県や市町村の利用できたウエブサイトに対してアクセスが集中し,可用性喪失の恐れが生じた.

これに対して,ICT 企業や NPO・ボランティアがミラーサイトを短時間で立ち上げたことで,トラヒックの分散が図られ,可用性喪失を防ぐことができた事例があった.[5] また被災地・被災者情報提供のために,インターネット上で以下のような支援サイトが多数立ち上げられた.

1) Google: 「グーグル・クライシス・レスポンス」を立ち上げて,被災者の所在探しを支援する「パーソン・ファインダー」,ボランティア募集情報,義援金・寄付金の受付,災害情報や放射能に関する医学情報などの情報提供を行なった.[6]
2) sinsai.info(震災復興支援サイト):ツイッターに投稿された情報を自動的に収集して,ボランティアが人手でその情報の信頼度を判断して,情報を整理.被害状況,安否確認情報[7],避難所情報,ボランティア募集情報,雇用情報などを地図上に表示するサービスを

[5] 出典:白井良 ITPro2011 年 4 月 12 日.

[6] 出典:日経新聞,2011 年 4 月 3 日.

[7] 本文の例以外に,固定電話(災害伝言ダイヤル),携帯電話(災害伝言板),インターネット(東西 NTT の災害

提供した.そのサービス提供のために,OSS(オープン・ソース・ソフトウエア)であるUshahidiを利用,また,無償で提供されたAmazon Web Servicesを利用した.なお,このサイトは震災後 4 時間未満で立ち上げ活動をスタートさせた.

3) 支援ニーズの引き合わせ(マッチング)サイトが多く立ちあげられた.例:「お願いタイガー! 災害版」,「がんばれ!!日本 がんばれ!!東北」,「仮住まいの輪」,「子供の学び支援ポータルサイト」[8]

上記事例に加えて,ヤフー,ミクシィ,日本マイクロソフト,ウエザーニュースなどのウエブサイトでも,数多くの震災関連情報の提供が行なわれた.

このような被災地・被災者支援活動では,企業,NPO,プロボノが活躍して,数多くのサイトが立ちあがった.しかし現在では,「一部大手企業によるものは別として,多くがボランティアや義援金といった「共感」に依存してきた.それが減ってきた現在,支援継続が難しくなっているのも事実.」との指摘があり,サイト運営手法の見直しを迫られているのが実情のようである.[9]

3.4 ICT 企業によるクラウドサービスの提供

富士通,NEC,日本 IBM,ニフティ,日本マイクロソフト,日本ユニシス,日立情報システム,IIJ,NTT コミュニケーションズ,NTTPC コミュニケーションズなど多数の ICT 企業が,被災自治体や被災地・被災者支援を行なう NPO に対して,無償でクラウドサービスを提供した.IPA 調査[10]では,「東日本大震災での緊急支援に役立てられたクラウドサービス」は 76 件にのぼっている.この中には発災後数日でサービスを立ちあげた例がいくつもある.また,提供期間は3か月,6か月のものが多いが,自治体向けなどには期限の定めのないものもある.

上記事例は,大震災などの緊急時の情報システムの可用性確保や,切実に必要とされる情報を提供するために,サービス開始までに要する時間の短いクラウドサービスが,大きな役割を果たす可能性を示したものといえる.今後はクラウドサービスが,政府機関や企業のBCP(Business Continuity Plan:事業継続計画)[11]遂行上の有力な手段ともなり得ることを,印象づけたといえる.

3.5 震災に便乗したウイルス攻撃

3.3 および 3.4 で述べたように,ICT が被災地・被災者支援などに役立った「光の面」がみられた一方で,以下のような「影の面」の事象が発生している.[12]

①震災発生直後,「Most Recent Earthquake in Japan」という用語の検索結果から,不正ウエブサイトに誘導する SEO ポイズニングが確認されている.

用ブロードバンド伝言板,赤十字国際委員会のファミリーリンク),放送(NHK 安否情報の放送)でも,安否確認をすることができた.もっとも,利用は期待ほどではなかったとの声がある.

8 2),3)の出典:朝日新聞,2011 年 4 月 10 日,日経新聞,2011 年 5 月 4 日.

9 出典:「IT ベンチャーの震災復興支援:サイト運営手法に転機」,日経ビジネス,2011 年 9 月 5 日号.

10 IPA(独立行政法人情報処理推進機構)「震災時の緊急支援に役立てられたクラウドサービスの事例と復旧・復興に向けたクラウドサービスの安全利用に関する資料」,2011 年 6 月 20 日.

11 BCPについては 4.3 参照.

12 出典:IPA およびセキュリティ会社等の各種発表資料.

② 検索結果で表示されたサイトにアクセスして,その指示に従っていくと,「Internet Security Essentials」という偽セキュリティソフトを,ダウンロードすることになる.この偽ソフトはトロイの木馬で,ユーザの個人情報やクレジットカード番号を窃取することを目的としている.また,「TROJ_FAKEAV」という偽セキュリティソフトの感染報告が,相当数あった.さらに 3 月下旬には,SQL インジェクションによって正規サイトを改ざんする攻撃があり,通称「LizaMoon」によって,全世界で 10 万サイト以上の改ざんが確認されたとの報告もある.

③ 被災者支援のために,世界中の団体・企業などが義援金を募っていたが,この動きに便乗して,義援金名目で金銭をだまし取ろうとするフィッシング詐欺サイトが確認されている.トレンドマイクロによれば,4 月 14 日時点約 75 のフィッシング詐欺サイトがあった.

④ 震災関連の情報提供を装って,ウイルスに感染させようとして,送付されたメールも多数あった.このなかには,受信者の気になるキーワードを含むメールを送付して,添付ファイルを開かせようとするもの,また政府機関や災害対策に関係ありそうな組織名やメールアドレスを詐称して,一見ウイルスとは思えないファイルを添付して,添付ファイルを開くとウイルスに感染させるものなどがあった.

メールの表題例としては,「被ばくに対する防護対策について」,「福島原発最新状況」,「放射能被ばくに関する基礎知識第 1 報.doc」などがある.また,これらのマルウエア送付の犯人をいくつかの手がかりから,推測・追跡することも行なわれているが,決定的なものはないようである.

⑤ 傾向としては,大震災発生直後は義援金をかたるフィッシングが横行していたが,2 週間を過ぎるころから,大震災に便乗したウイルスメールが報告され始めた.

⑥ 震災に乗じて,企業・公的機関をターゲットにする標的型攻撃もみられた.トレントマイクロの 4 月 7 日発表によると,法人を中心に 40 件を超えている.

3.6 今後の緊急時における通信確保策

今回の大震災において,通信ネットワークの可用性が大きく損なわれたことに対する,今後の対策の在り方を検討するため,総務省において「大規模災害等緊急事態における通信確保の在り方に関する検討会」が 4 月上旬に設置され,7 月 29 日に「中間とりまとめ」が公表された.

この検討会では,緊急時の輻輳状態への対応の在り方,基地局や中継局が被災した場合等における通信手段確保の在り方,今後のネットワークインフラの在り方,今後のインターネット利用の在り方の4つの事項についてさまざまな対策の検討が行われ,アクションプランが提示されている.

また,総務省情報通信審議会は,「知識情報社会の実現にむけた情報通信政策の在り方:東日本大震災および日本再生に向けた ICT 総合戦略:中間とりまとめ」を, 7 月 25 日に公表した.この中間とりまとめでは, ICT に期待されている役割を果たす前提として,「通信インフラ等の耐災害性の強化」が,今後の具体的施策として取り上げられている.さらに,この耐災害性の強化施策として,「通信インフラ等の耐災害性の強化・再構築」,「冗長性の高い情報提供基盤の構築」がうたわれている.

これらの総務省の検討にみられるように,大震災のような緊急時において通信ネットワークの可用性をいかに確保するかが,情報システムと情報の可用性確保とともに大きな課題で

ある.情報通信審議会において,通信ネットワークの可用性確保策が検討されたことは,企業においてもコンピュータシステムだけではなく,通信ネットワークの可用性についても併せて検討しなければならないことを,示唆しているように思われる.今後,通信ネットワークを多用するクラウドサービスが普及した場合に,この通信側の可用性確保が,一層重要な課題になることは容易に想像できる.

4. 東日本大震災における企業行動

4.1 企業の被災・復旧状況

社団法人日本情報システム・ユーザ協会(JUAS)が,2011 年 5 月に行なった調査によれば,回答のあった企業 129 社の 4 分の 3 が,また製造業では 9 割弱が直接・間接の被害があったと回答している.

また今回の大震災で特徴的なこととして,たとえば自動車生産において,特定の部品を生産する企業が被災したことで,国内だけではなく,米国のGM のルイジアナ工場のような海外の工場での生産もストップした.[13]

この事例で自動車生産においては,特定の部品の生産が特定企業に集中している現状が明らかになった.他の産業においても,

① 半導体製造に使われるシリコンウエハーの日本企業のシェアは 60%で,そのうち今回の大震災で被災した信越化学白河工場だけで,世界シェアの 20%を占めている.[14]

② 三菱ガス化学と日立化成の 2 社で市場の約 90%を占めているが,両工場とも被災した.[15]

③ クレハのポリマーは,アップルの iPod 用の小型バッテリーの 70%に使われているが,工場が被災した.

このようなオンリーワン企業が日本にあることは,日本の部品メーカーの国際競争力が強いことを示していると同時に,いったん災害が発生した場合には,グローバル・サプライ・チェーンが寸断する脆弱性があることも示している.

サプライ・チェーンが長く延びている製品の場合には,一次部品や二次部品のメーカー数を一定数確保していたとしても,そのさらなる上流工程の部品メーカーが、裾野の広い部品生産体制になっておらず,特定メーカーに集中している場合には,その特定のメーカー,工場の生産がストップしてしまうと,影響は下流工程全体に及ぶ.さらに,いわゆるカンバン方式といわれるリーン生産方式を取っているケースでは,短時間で下流工程にその響が及ぶため,早期に完成品の生産が止まってしまう事態になる.これらは,個別企業の生産停止の事例である.

---

13 出典:ウイリー・シー「日本企業なくして世界のモノづくりは成り立たない」日経ビジネスオンライン, 2011 年 4 月 21 日.

14 出典:小久保重信「震災発生から 3 週間 回復しない電子部品供給」日経ビジネスオンライン, 2011 年 4 月 5 日号.

15 (イ)と(ウ)の出典:「日本と世界の供給網 壊れた鎖」英エコノミスト,2011 年 4 月 2 日号.

大震災によるマクロ的な生産活動への影響に関しては,経済産業省によって,製造業および小売・サービス業 123 社を対象に調査が行なわれている.この調査によれば,2011 年 6 月時点で全体の 80%の企業が,震災前の生産水準を回復している.一方で.,震災によって,海外顧客からの取引減少や契約打ち切りの影響を受けた企業が,製造業(52 社)の 3 分の 1に及ぶ.取引減少や契約打ち切りの理由は,十分な供給量が確保できない(47%),原発事故に対する過剰反応(41%)である.

他方,取引先の被災で部品の調達先を変えた企業のうちで,もとの調達先に戻すと回答した企業が 83%,引き続き国内の代替先から調達すると回答した企業が 58%である.他方 42%の企業は、「引き続き海外の代替先から調達」すると回答している.[16]

このように,産業活動は回復しつつあるが,上記の国内外企業のサプライ・チェーンの見直し動向については,情報システムなり,情報セキュリティの視点からも注視する必要がある.というのも,サプライ・チェーンの見直しは,企業間の取引の継続性を確保することが契機になっているので,情報システムの面からも事業継続性について貢献することが求められているからである.

4.2 生産再開に向けた取り組み

4.1 で述べたように,生産活動に広範かつ深刻な被害が発生した.もし生産再開が長引けば,グローバル・サプライ・チェーンに大きな悪影響が発生する.と同時に生産再開が遅れれば,国内外の競争メーカーが被災企業の供給ストップを補うような増産を行ない,被災企業が生産再開したとしても,需要が他企業にシフトして戻ってこないということも十分にあり得る.

発災直後から,各企業では社員の安否確認や被災地・被災者支援に併せて,上記のようなサプライ・チェーンの中断に対処するため,ボトルネックとなる部品の生産再開に向けて,下流工程の企業から上流工程の企業へ大量の人員が投入された.

この結果,たとえば自動車生産に関しては,震災後 3 ヶ月時点でかなりの生産水準に回復して,生産正常化のめどがついた.また,食品などの生活物資も供給不足が解消しつつあった.ただし,製紙業界やビール業界では,その時点では全面復旧はまだ見通せていなかった.[17]

このなかにあって,通信ネットワークの損壊に関しては,前述したように 4 月末までにほぼ復旧し,東北新幹線も 4 月 29 日に全線で運転を再開した.さらにこれより早く,かなりの店舗が営業を開始したのが,コンビニなどの流通業界である.震災直後の営業休止店舗数と震災発生後のほぼ 10 日後の 3 月 23 日現在での営業休止店舗数を比較すると,たとえば,セブンイレブンジャパンは約 600 対約 90 店舗,ローソンは約 390 対約 80 店舗,ファミリーマートは約 250 対約 60 店舗となっている.このようにかなり早いスピードで営業再開ができたのは,マスメディアでも大きく報道されたように,コンビニ店舗の営業再開に向けての懸命の取り組みが報われた結果といえよう.[18]

---

16 出典 朝日新聞,2011 年 8 月 2 日.

17 出典:日経新聞,2011 年 6 月 12 日.朝日新聞,2011 年 6 月 11 日.

18 出典:日経新聞,2011 年 3 月 24 日.

他方で,放射線物質汚染問題が食料品だけではなく工業製品にも広がって,出荷時や輸出時に証明書添付を要求される事態も発生している.また,東京電力のサービス地域では,電力使用制限令が発出されて,大幅な節電が求められ,各企業の経営に大きな負担となったが,各企業は目標の 15%節電を上回る実績を上げている.

また,生産拠点および情報システムを,分散する動きも出ている.情報システムの分散の動きに特徴的なのは,クラウドサービスを利用する動きである.4.3 で述べるように,今後事業の効率化とリスク分散の両面から,クラウドサービス利用が進展することが想定される.

ただし,企業のクラウドサービス利用に関して一番大きな不安要素は,情報セキュリティである.とはいえ,クラウドサービスは,普及に向かう立ちあがり段階にあるために,情報セキュリティの実態・課題が十分に解明されているとはいえない.今後の情報セキュリティに関する検討や実例の蓄積を通して,クラウドサービスの利点と注意点について,バランスが良く,実務的に役立つ知見が得られることが,クラウドサービスの普及にとって重要になる.[19]

4.3 BCP(Business Continuity Plan:事業継続計画)

今回の大震災において発生した事態は,BCPの観点からどのように評価できるであろうか.この BCP というのは,大地震などの緊急事態が発生した場合に,事業資産の損害を最小化しつつ,中核となる事業の継続・早期回復を可能にするため,平時から緊急時の対応を事前に定めておくことである.

日本企業でも大企業を中心に,すでにかなりの割合の企業が BCP を作成済みである.しかし,現在のBCPは自社を対象としている場合が多い.これに対して,取引先を対象として BCP を策定していた企業はわずか 6.7%にとどまっており,現実のサプライ・チェーンの広がりに十分に対応しているとはいえない状況にある.[20]

もっとも,BCPによる対処が必ずしも浸透していなかったからといって,生産再開が大きく立ち遅れたというわけでは必ずしもない.BCPでは取引先が対象になっていなかったとしても,実際には上流工程の企業に対して,下流工程企業から多くの人的・物的な支援が行なわれたことは前述した.加えて,たとえば仙台市のガス供給の再開に向けて,全国から多くのガスマンが現地に入り込み,懸命の復旧作業を行なったことが大きく報じられたように,取引先ではない他企業から支援の手が差し伸べられた事例は,多数に上るものと推測される.

さらに,東北新幹線の復旧においても,新幹線建設を請負った建設会社だけではなく,JR西やJR東海,さらには京浜急行や西日本鉄道も,震災直後から復旧作業に協力するなど,一日当たり約 8,500 人規模の人的支援が行なわれた.この結果,東北新幹線は,震災発生 49 日後の 4 月 29 日に全線開通した.阪神・淡路大震災時の山陽新幹線の 81 日後,2004 年中越地震発生時の 66 日後の運転再開に比べると,49 日後というのは比較的短期間での復旧であることが分かる.[21]

---

19 クラウドサービスの概要については,以下のサイトを参照.
http://lab.iisec.ac.jp/~hayashi/FRI2.pdf

20 出典:NTTデータ経営研究所が,gooリサーチのビジネスモニター1020 人に対して,2011 年 6 月に行なった「東日本大震災を受けた企業の事業継続に係る意識調査」結果.

21 出典:梅原淳「震災からの鉄道復旧物語」エコノミスト,2011 年 7 月 19 日号.

前述したように,通信ネットワーク,コンビニなどの流通網なども,同様に比較的早期の復旧・サービス再開となっている.今回の大震災における復旧活動では,前述したように,事前の BCP が効果を発揮したというよりも,発災後の各企業の実際の取り組み（いわば「現場力」）が成果をあげたといえるのはないだろうか.

しかしだからBCPが必要ないということではなく,BCPがあれば,緊急時の日本企業の事業継続性に関する信頼が高まるとともに,さらに早期の生産再開につながるものと考えられる.実務的にはたとえば,復旧活動のための輸送手段や燃料は各企業等の奪い合いになるため,一刻も早く行動に移りそれらの資源を確保することが,その後の復旧のスピードを左右する.したがって,事前に BCP を作成しておけば,直ちに状況を判断して行動することができるので,BCPは不可欠のものであるとの指摘がある.[22]

なおこの際に,取引先や社会に対して安心感と信頼感を与えるために,被害状況,復旧への取り組み状況,復旧状況なり復旧見通しを,積極的に発信していくことが重要である.
積極的な情報発信が,取引先との継続的取引につながるのである.

いままでみてきたように,大震災の発生時のような緊急時には,生産活動を現地で再開するか,代替地で生産活動を行なうかなど手段の違いはあるが,いずれにしても早期に生産再開することが,グローバル・サプライ・チェーンにおいて重要な役割を果たしている企業の責務である.またこの対応に失敗すれば,需要が国内外の他企業にシフトすることにもなるので,経営上大きな打撃を受けることになる.

既存の取引先と継続的な取引関係を築くうえでも,また,将来的な販路を拡大にとっても,自社製品・サービスの品質や価格に加えて,緊急時において,生産活動を継続できることが,また生産活動がストップした場合でも早期に再開できることが,取引継続・新規顧客獲得にとってきわめて重要であることを,今回の大震災で再認識させられたのではないだろうか.

BCPへの取り組みはヨーロッパが先行していたが,日本でも 2000 年代に入ってから検討が始まり,2005 年に経済産業省や内閣府から「事業継続計画（BCP）策定ガイドライン」が公表されている.このうち,経済産業省のガイドラインでは,「情報システムへの依存が増大するなかで,情報システムが事業の停止に直結するリスクになっている」.また,「海外企業にとって,日本の自然災害リスクは脅威に映っている」と述べられている.

2001 年の 9.11 同時多発テロ発生以降,米国では企業取引を行なう際に,品質や財務状況をお互いに公開することに加えて,BCPの実効性を相互に確認することが,取引の前提条件になったようだ.たとえば,インテルは日本を含む世界中の取引先に対して,BCPの開示や査察チームによる現地確認を行なっているといわれている.

今回の大震災の被災状況,復旧状況をふまえて,多くの企業は自社のBCPを見直す動きを示している.この見直しに関しては,個々の計画項目の見直しに加えて,サプライ・チェーンの一部の寸断が,自社の経営活動なり生産活動に大きな影響を及ぼすことが明確になったので,対象範囲を取引先に拡大することも,重要ではないかと思われる.もっとも,事前にあれもこれもと計画することは,マンパワーやコストに響くので,自ずと限界がある.この問題については 5 章で考察する.

---

[22] 伊藤毅「これからの事業継続マネジメント～震災をふまえた実践的 BCM へ～」富士通総研セミナー,2011 年 9 月 22 日. なお,伊藤氏は富士通総研のBCM事業部長.

4.4 震災発生後における企業行動

前述したように,各企業は自社の復旧活動および他社への復旧支援を積極的に行なったのであるが,震災発生後における企業行動に関しては,この他にもいくつか注目すべき事象がみられた.

まず第一に,ICT 企業が被災地・被災者支援に積極的に取り組んだことがあげられる.3.3 および 3.4 で述べたように,ICT企業は被災地・被災者のための支援サイトを多く立ち上げた.また,自治体等のウエブサイトの可用性喪失を防ぐために,ミラーサイトを迅速に立ち上げるなど,情報システムの可用性および情報の可用性を向上させるために,大いに貢献した.この貢献は,いわばプロボノ的な貢献といえよう.

ついで第二に,多くの企業が自社社員のボランティア活動について,側面から援助を行なったことがあげられる.企業のボランティア支援の全体像について公表されたものはないが,たとえばNTTデータは,3.3 2)で述べた sinsai.info の活動の総副責任者である自社社員を含め,約 40 人の社員が勤務時間内に sinsai.info の活動を行なうことを認めていた.[23]また,三菱商事などは,ローテンション的に社員を被災地に派遣している.

さらに第三に,企業の社会において果たす役割について述べておきたい.被災地では.,道路などの通行不能,トラックなどの燃料不足,店舗の損壊・流失などのために,生活物資の供給が途絶して,食糧・水などの基礎的な物資が大きく不足した.この事態に対処するために 4.2 で述べたように,コンビニ業界では仮店舗・移動店舗を含め,震災発生後 10 日余りで多くの店舗の営業再開にこぎつけた.まだ商品の棚に十分に商品が置かれていない状況であっても,コンビニを訪れた被災者が店舗再開に対して,店員にお礼を言って,うれしそうに買い物をしたことが報道された.

近年,企業の社会的責任(CSR:Corporate Social Responsibility)の重要性が叫ばれており,各企業は環境問題への取り組みも含めて,積極的に活動を展開している.しかし,今回のコンビニの事例をみると,企業の最大の社会的な存在価値(レゾンデートル)は,事業活動そのものであるという感を深くする.「利益を挙げて,税金を払うのが最大の社会貢献だ」という指摘も以前からある.企業の存在価値は,まず社会的に役立つ商品・サービスの生産・提供という本業をしっかりと行なうこと,ついで,社会的に必要であるが十分に対処できていない社会的課題に関して,負の外部性を発生させる主体,または良き企業市民としてその解決に貢献することではないだろうか.

2003 年の経済同友会の「第 15 回企業白書」では,「なぜ CSR は企業の持続的発展や競争力向上に結びつくのか」との問題提起を行なっている.この問題に対して,社会的なニーズに照らし,将来のリスク要因を提言する「リスクマネジメント」と,社会的ニーズに対応あるいはそれを発掘し,イノベーションによって,いち早く価値創造・新市場創造・企業革新に結び付ける「ビジネス・ケース」がそのキーワードであるとしている.

今回の大震災でみられた上記の三つの企業行動の特徴点は,今後の日本企業のミッション設定,経営方針,戦略構築,実際行動に影響を与えることが考えられ,企業行動が社会とのつながりをより広くかつ深くする方向に向かえば,市場機能の活用や政策・法制度機能の活用と並んで,企業の自律的な行動が,社会的な合意形成やガバナンスの維持向上に

[23] 出典 高橋信頼,ITPro2011 年 5 月 9 日.

大いに資するのではないかと考えられる.[24]

また,このような企業行動の変化は,情報セキュリティ施策にも影響を及ぼすのではないだろうか.4.5 において,大震災発生時にインターネット上で飛び交った流言・デマに,企業がどのように対処したかについて述べて,6.2 の今後の情報セキュリティの対象範囲を考える際のヒントにしたい.

4.5 流言・デマへの対処

今回の大震災は,インターネットとりわけソーシャルメディアが多く使われた,最初の大災害である.3. 3や3. 4 で述べたように,被災地・被災者支援にインターネットが大きく貢献した.しかし一方で,チェーンメールやツイッターを利用して,大量の流言・デマが流されて,人々の不安を煽った事象も発生している.

被災地・被災者支援や復旧活動などをスムーズに行なうために,情報が共有されていることが,ぜひとも必要なことである.しかし,流言・デマが広まることで,間違った情報が共有されることになると,切実に求められている支援活動や復旧活動の妨げになる.

たとえば,特定の場所で何かの物資が不足しているので,すぐに送ってほしいというような流言・デマが流されたとする.もしこれを信じた善意の人が実際の行動に走ると,必要な所に必要な物資が送られずに,その物資が足りている所へ支援物資が送られてしまうような事象が発生する.したがって,流言・デマの悪影響を最小化するために,誰がどのようにこの流言・デマに対処すればよいかが問われることになる.

発災後発生した千葉のコスモ製油所の火災は,なかなか鎮火せず,長時間燃え続けたことが,テレビでも大きく報道された.この火災に関して,チェーンメールやツイッターで以下のような書き込みがなされ,これを信じた善意の人によっても,これらが転送され,流言・デマ情報が拡散した.

例:千葉のみなさん!コスモ石油の火災で有害物質が雲に付着しています.雨が降ったら危険なので肌を露出しないでください. 長袖・カッパの着用,カサを忘れないようにとの事です.できるだけ多くの人に伝えてください.

インターネット時代の流言・デマの特徴は,情報の拡散するスピードが速いことである.図表 4 で示すように,荻上チキが「うわさ屋」とよぶ,ツイッター上で自らつぶやいた数(公式リツイートされた数は含まれていない)が,震災発生当日 19 時には 606 件であったものが,2 時間後の 21 時には 2,786 件と急増している.

これに対して,翌 12 日の 14 時半ごろにコスモ石油が,ウエブ上で公式に流言内容を否定した.さらに,16 時台には船橋市や浦安市もウエブサイトやツイッター上で流言内容を否定した.この結果,15 時ごろから流言の内容に対して懐疑的なコメントやソースのリンクを貼って流言・デマを明確に否定する発信が急増する一方で,流言・デマ件数が減少した.この結

---

[24] このガバナンスのあり方については,以下の文献を参照.「企業における情報セキュリティの実効性あるガバナンス制度のあり方」(2006～2008 年度科学技術振興機構公募研究)..
www.ristex.jp/examin/infosociety/gobernance/security.html

果,12 日の夜には流言・デマはほぼ終息した.[25]

図表 4 を見ると,流言・デマが急速に広まる一方で,否定的な発表がなされると急激に流言が減少したことが見て取れる.またテレビ報道で,コスモ製油所火災が大きく報道され,おそらくは鎮火したことも報道されたので,流言・デマの縮小のスピードも速かったのではないかと推測される.

もっとも,テレビ報道は真実を伝えていない,インターネットでこそ正しい情報が流れていると主張されることがあり,これがインターネット上での流言・デマが発生する背景の一つとなっている.

なお,注目すべき事象としては,流言を否定する発信,いわゆる「中和情報」も多く流されたことで,これが終息に寄与したと考えられる.

図表 4:コスモ石油に関する流言・デマの推移

日時	A うわさ屋	B 懐疑的	C 検証屋	B+C
11 日 19 時	606	12	0	12(1.9%)
21 時	2,785	32	1	33(1.2%)
23 時	2.958	22	0	22(0.7%)
12 日 8 時	221	70	2	72(24.6%)
11 時	312	54	0	54(14.8%)
13 時	1,010	206	67	273(21.3%)
14 時	1,331	443	324	767(36.6%)
15 時	1,605	1,372	1,113	2,485(60.8%)
17 時	1,010	5.817	1,604	7421(88.0%)
21 時	100	551	211	762(88.4%)
13 日 8 時	10	88	16	104(91.2%)

出典:荻上チキ[2011]『検証 : 東日本大震災の流言・デマ』
p43 から抜粋して作成.

流言・デマ[26]が拡散するのは,重要さと情報の曖昧さの積であるとか,災害時には情報の需要が増えるのに反して,情報の供給が減少するので,そのギャップを埋めるために憶測を含む流言が広がるとか説明されている.もしそうであれば,正しい情報を提供することで,需給ギャップを埋める必要があり, 荻上が指摘するように,確かな情報を行政,マスメディア,専

[25] 出典:荻上チキ[2011]『検証　東日本大震災の流言・デマ』 p 31～45.

[26] 荻上は,流言とデマの違いについて,流言は「根拠が不確かでありながらも広がってしまう情報」であり,デマは「政治的な意図を持ち,相手を貶めるために流される情報」であるとしている.荻上は,この区分は実際の対処の際には重要ではないとしている.流言・デマが広がるときに,「なぜそんなウソをつく人がいるのか」という発信意図を問題にするが,重要なのはそれを信じた人・広げた人がいることで,それを信ずる集団的な心理や情報環境こそ注目すべきであると指摘している.傾聴すべき意見と思われる.

門家,NPO,企業が提供することが重要になる.

5.リスク対処の基本問題

5.1 どこまで発生事象を想定するか

リスク対処には,回避,低減,移転によってリスクを減らす,それでも残るリスクは受容する,この4つの対処方法があるとされている.また,リスクの大きさは発生確率とそのリスクが顕在化したときに発生する損害の大きさの積であるとされている.このリスクというのは,望ましくないマイナスの事象であることが,暗黙的に前提とされている.

これに対して酒井泰弘は,リスクは避けるものであるが,ときには挑むものであると指摘しており,リスクに以下のような定義を与えている.[27]

> リスクとは,ひとつの行為から出る結果がひとつとは限らず,一般に複数個の結果が生まれることを指す.これらの複数個の結果の中で,実際のどの結果が生まれるかは,そのときの状態や条件次第である.
>
> 重要な点は,リスクが人間の生活維持や社会経済に対して,プラスとマイナスの両側面を持つことである.そして,リスクが大きいというのは,複数の結果の間における＜変動幅や範囲＞が大きく,また各結果自体の＜規模やレベル＞が大きいことを意味する.

また酒井は「欧米人と比較して,日本人は天災をいわば運命として甘受する民族であり,大震災の悪夢から大いに学び,リスク対策を積極的に採ることが苦手な民族である」とも述べている.この当否の判断はともかくとして,今回の巨大地震,巨大津波,さらに原発事故のように,発生する確率は低いものの,いったん発生すると甚大な被害が発生するリスクにどう対処すべきかという大問題がある.

さらに,2008年の米国に端を発した金融危機の発生時には,リスクを分散したつもりでも,実際はどこにリスクが分散されたが分からなくなるほど,広範囲にかつ複雑にリスクが分散されたため,大きな信用不安を引き起こした.この渦中で,相次いで破たんの危機に陥った巨大金融機関に対する救済策が実施されたが,リーマン・ブラザースのように実際に破たんした例も生じた.

科学技術が高度に発達し,産業活動に利用されていること,グローバル市場経済化が進展したことなどから,企業にとっても,社会にとっても,政府にとっても,リスクの所在と大きさが従来よりも想定しにくくなっている.

このような状況のなかで,企業はどんなリスクを,どこまで考慮に入れて,経営を行なえばよいかの判断が,従来にも増して難しくなっている.フィリップ・コトラーは,先の見通しがつきにくく,次々と顕在化する結果生じる「カオス,リスク,不確実性こそが,業界,市場,企業のいまの通常状態(ニューノーマル)」[28]であると述べている.

ただし,このようなカオス,リスク,不確実性は,企業に対して損害を与える可能性があると同時に,新たな機会を与えるものであることも,理解しなければならない.すなわち,リスクには,

---

27 出典:酒井泰弘[2006]『リスク社会を見る目』p 49.

28 出典:フィリップ・コトラー,ジョン・キャスリオーネ[2008]『カオティックス (CHAOTICS)』.

それを防止すること,および顕在化した場合に損害を最小化することが,経営上求められる.その一方で,リスクテイクの側面があり,それを追求することも経営上は重要である.

フランク・ナイトは,確率的状況を先験的確率(二つのサイコロを同時に投げるときに,目の和が 7 になるような確率),統計的確率(人間の平均寿命や交通事故など,実際の経験データから決まる確率)および推定と呼ばれる三つに分けている.この最後の推定というのは,推定の基礎が未経験の事柄であるか,大数の法則が成立しない特異事象であるため,確率そのものが分からない場合を指している.[29]

リスクについての前述した酒井の定義も併せ考えると,今回の巨大地震・巨大津波は 100 年に 1 回とか 1000 年に 1 回といわれているので,統計的確率ともいえるが,発生確率が低くまたタイムスパンが非常に長いため,むしろ推定に近いものではないだろうか.

また,福島原発事故に関して,ウルリッヒ・ベックは以下のように指摘している.

①原子力の危険は技術によって最小限に抑えられるだけで,ゼロにできるわけではない.
②原子力の宣伝係や専門家は,「安全性のパラドックス」に陥っていた.「安全よりももっと安全になる」と強調するように強いられている.しかし,これによって公衆の知覚が敏感になり,災害が起こらずとも,その兆候があっただけで,安全性の主張は反駁されることになる.
③原子力の惨事が起こることは,統計的には「可能性が低い」のかもしれない.しかし,原子核が融合すれば何が起こるかを,われわれは良く知っている.不確実なのは,それが起こるかどうかであり,起こった場合にどうなるかの方は,科学的な知見から確実である.[30]

まさにベックの指摘するとおり,原子力の安全神話を作り上げたために,「最悪に備える(Prepare for the Worst)原則」をふまえて,事前検討および対策を実施することができなかったことが,福島原発事故で明らかになったものと思われる.米国が核戦争に備えた対応をしており,日本はその対応は行っていないという差を考慮に入れたとしても,米軍が重装備で訓練を積んだ部隊を送りこんだり,無人の装置が活躍したりしたことを考えれば,「最悪に備える原則」遵守の度合いが,日米で大きく異なると思わざるを得ない.

この点に関して,政府の福島原発事故検証委員会座長の畑村洋太郎は,「ありうることは起こる」として,「全体像」を把握すること,「仮想演習(前提となる条件が変わった場合に何が起こるかを,先に考えておくこと)」,「逆演算(事故 C が起こったときには,その前に B が,さらにその前に A が起こったはずというように,時間軸を遡って考えること)」の習慣をつけることを勧めている.畑村は,「逆演算だけが,不想定を発見する」としている.[31]この不想定(想定しなかったこと)を発見することは,想定外を発見することである.

しかし発生確率が低く,いつ起こるか分からない事象を想定して,予防策を講ずることは対策に費用がかかり過ぎるので,ここは想定することを止めようという判断は,あり得ることである.この場合に,予防にだけ費用をかけるのではなく,かりに被害が発生した場合に,会社

---

29 出典:酒井泰弘[2007]「経済学におけるリスクとは」橘木,長谷部,今田,益永(編)『リスク学入門 1:リスク学とは何か』 p 62.

30 出典:ウルリッヒ・ベック[2011]「この機会に一福島,あるいは世界リスク社会における日本の未来」ウルリッヒ・ベック,鈴木宗徳,伊藤美登里編著『リスク化する日本社会』p 3 ~ 4.

31 出典:畑村洋太郎[2011]『「想定外」を想定せよ!失敗学からの提言』 p 131~137

資産への被害を最小限に抑えて,あらかじめ考えていた対策を実行して,可能な限り早期に復旧させるというような,発想法が重要である.[32]

5.2 発生事象への対処:マニュアルの有効性と限界

巨大津波に襲われた岩手県の釜石市にある釜石東中学校では,生徒が小学生やお年寄りを誘導しながら,避難場所よりももっと高い場所に避難することで助かった.この事例はマニュアルの限界を示すものである.

釜石東中学校では,群馬大学の片田教授の指導による防災教育を受けていた.この防災教育では,「津波が来たら避難場所に逃げましょう」と教えるのではなくて,「想定外の状況にも一人ひとりが対応し,自分の命を守るためにどうすべきか,自分で考えて判断し,行動する力をつけることを,防災教育理論の柱」にした.また,中学生たちには,「逃げるだけではなく,周りを助ける人になれ」とも伝えていた.[33]

さらに,具体的な事項としては,「ハザードマップを信じるな」と教えていた.これは,事前の被害想定を地図上の表示したハザードマップを信じていたら,想定外の巨大な津波が来襲したときに,被害にあうからである.すなわち,想定外を想定して行動することの大切さを強調したのである.この防災教育は実際の成果を生み,釜石東中学校の生徒は,自分で状況を判断かつ行動して,小学生やお年寄りを助けつつ,想定よりも高い場所に避難して,助かったのである.

一方,石巻市の大川小学校の事例は,しっかりとしたマニュアルがあれば,多くの犠牲者を出さなくてもすんだのではないかと推測され,マニュアルの有効性を示す事例であるように思える.すなわち,地震発生後に生徒は校庭に集められたが,避難場所が明確でなかったことや,教師たちが避難方針を決められないまま,地震発生から 1 時間以上生徒は校庭にいた.このように時間だけが経過して,ようやく避難を開始した直後に津波に襲われて,結果として生存者がほとんどいない惨事となった.もしかりに,避難場所が事前に避難マニュアルにおいて指定されていれば,ひとまずはそこへ移動して様子を見て,さらに安全な場所へ移動することも,できたのではないかと考えられる.

この二つの事例は,企業の BCP 作成時や実際の緊急時において,どう状況を判断して,行動するかという問題に大きなヒントになるのではないだろうか.BCP 作成時には,何をどこまで想定して,どう行動するかについて考え,訓練も行っておく.[34]また緊急事態発生時には,BCP を墨守するスタンスではなく,BCP が想定していない事態の発生についても,対応策を柔軟に判断しかつ行動するという,いわばマニュアルを整備しつつ,その限界も理解したうえで,判断・行動することが求められるのではないだろうか.

---

[32] この点の考え方については,5. 3 参照.

[33] 出典:注 31,畑村前掲書,p102～119.
片田敏孝「防災教育 「想定外」に備えた指導を」,朝日新聞,2011 年 9 月 14 日.

[34] この訓練の重要性は,多くの人が指摘するところである.たとえば,河田恵昭は,「知識が行動に結びつくには,行動を起こすことに対する意識上の障壁を低くすることが大切である」としたうえで,「阪神・淡路大震災のもっとも重要な教訓の一つは『災害時には日ごろからやり慣れていることしかできない』ということである.」と述べている. 出典 : 注 3 河田前掲書 p 165.

5.3 発生事象への対処:予防か減災か

巨大津波の来襲で,岩手県宮古市田老地区にある「万里の長城」とも呼ばれていた巨大堤防が倒壊した.田老地区には高さ 10mの新旧 3 つの堤防があったが,海岸に正面から立ちはだかる形で構築されていた新しい二つの巨大な堤防は,大きく破壊された.津波が来襲したときに津波の勢いを逃がす方向に構築されていた以前からの堤防は,ほぼ破壊を免れた.[35]

この以前からの堤防は,津波を海岸線で食い止めるのではなく,海岸線を超える浸水を想定しつつ,避難時間に余裕を持たせるために構築されたとされている.ハードで対処,ソフトでも対処というこの考え方は,被害の発生を防ぐ「防災の発想」ではなく,被害の程度を軽減するという「減災の発想」に基づいているとされている.筆者も現地でこれらの堤防を見て,その対照的な結末に強い印象を受けた.

2011 年 9 月 28 日に公表された内閣府中央防災会議の「東北地方太平洋沖地震を教訓とした地震・津波対策に関する専門調査会」報告書では,津波に関して「A 発生頻度は極めて低いものの,甚大な被害をもたらす最大クラスの津波」と「B 発生頻度が高く,津波高は低いものの大きな被害をもたらす津波」の2つに分けて,それぞれに適した対処策を提言している.

A タイプの津波に関しては,被害の最小化を主眼とする減災の考え方に基づくことを基本スタンスとして,「住民等の生命を守ることを最優先とし,住民の避難を軸にとりうる手段を尽くした,総合的な津波対策を確立」することが,提言されている.また,B タイプの津波に関しては,「人命保護に加えて,住民財産の保護,地域の経済活動の安定化,効率的な生産拠点の確保の観点」からの対策が,提言されている.

核戦争が発生して,通信ネットワークに大きな被害が発生したとしても,全く途絶するのではなく,なんとか最小限の通信が行なえるようにするための通信方式として,パケット通信方式が採用されて,インターネットの発展につながった.まさに,これも減災の発想に基づくものといえよう.この減災の思想は,『セキュリティ経営』[36]において底流になっている resilience (復元力) の発想につながるものである.

6. 今後の情報セキュリティ問題への示唆

6.1 情報セキュリティとナショナル・セキュリティの接近

2010 年 11 月に入ってから,WikiLeaks[37]は米国政府の外交公電情報を,ニューヨークタイムズなど欧米メディアに提供した.情報提供を受けた各社は,自身で内容のチェックを行なった後,紙上で外交公電の内容を報道し,大きな波紋・反響を引き起こした.

日本でも朝日新聞社が,2011 年 5 月に入ってから,WikiLeaks から提供された何件かの情報について,自社のチェックを経て紙上で報道した.公開された 2008 年 3 月 18 日付の外交公電では,原発について地震など既存の脅威に関しては,日本は備えと能力向上を向

35 出典:注 31,畑村前掲書,p21～27.

36 林紘一郎・田川義博・浅井達雄『セキュリティ経営』近刊.

37 WikiLeaks はいわゆる告発サイトとして,2006 年にジュリアン・アサンジなどによって設立された組織.

上させてきたと肯定的に評価している.しかし一方で,原発に対するテロ対策については不十分であると受け取られる表現があり,原発に関する米国政府の関心が,自然災害というよりもテロ攻撃にあることをうかがわせる.

また,「福島原発事故で冷却機能が壊されれば,原発は制御不能とテロリストが知ってしまった.核兵器を入手しなくても,原発を使って放射性物質をまき散らすことが可能と,彼らが考えることを懸念している.」との発言が報じられている.[38]

9.11 以降,電力,通信,交通などの重要インフラに関するリアル空間とサイバー空間におけるテロ攻撃からの防御が,重要なナショナル・セキュリティ問題になっている.

情報セキュリティがナショナル・セキュリティと密接につながっていることを示唆するものとして,ジョージ W ブッシュ米前大統領が「私の履歴書」(2011 年 4 月 25 日付日経新聞)で述べた事件がある.2007 年に,シリアが建設中のプルトニウム生産が可能な原子炉施設に対して,イスラエル空軍による電撃空爆が行なわれた.ブッシュ前大統領は,イスラエル首相からの当該施設に対する米空軍による爆撃依頼を断ったが,イスラエル空軍が爆撃したと述べている.この「私の履歴書」で述べられていないことは,空爆の前夜にシリアのレーダー・システムが無力化されており,空爆時にシリア側からの反撃等は行なわれなかったことである.この無力化が,どのような手段で行なわれたかは明らかではないが,電子システムであるレーダー・システムへの攻撃は空爆に先立って行なわれており,リアル空間とサイバー空間の軍事的行動が密接に連動していることがみてとれる.[39]

また,サイバー攻撃,特定の組織への攻撃として行われる事例が増加している.米国の国防省や軍需生産企業への組織的とみられる標的型のサイバー攻撃も目立つ.この事態に対して.,米国では大統領が現状評価[40]を行なったうえで,対応策を呼びかけている.加えて 2011 年 7 月には,国防総省がサイバー空間を,軍事作戦領域に追加するとともに,対応策強化の戦略方針を打ち出した.[41]

日本の防衛省も2011年の防衛白書において,サイバー攻撃が国家安全保障に重大な影響を及ぼし得るとの認識のもとに,サイバー空間の脅威に関して引き続き注視する方針を表明した.

6.2 「情報」の CIA(機密性,完全性,可用性)の対象拡大

情報セキュリティは伝統的には,情報資産(情報システムとその中にある情報)に関する CIA を,脅威から守ることであるとされている.この重要性は現在でもいささかも揺るがないが,情報セキュリティ対策としては,必要十分条件ではなくなりつつあるように思える.

---

38 出典:ケニス・ルアンゴ米パートナーシップ・フォー・グローバルセキュリティ理事長の発言,日経新聞,2011 年 4 月 22 日.

39 この密接な連動については,以下を参照.“Cyber war skips the battlefield. Systems that people rely upon, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country’s traditional defenses.” Source: Clarke, A. Richard and Robert K. Knake[2010] “Cyber War”

40 “ Cyber Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure” White House, May 2009

41 “Department of Defense Strategy for Operating in Cyberspace” July 2011

ここでは,三つの視点からこの問題を考えてみたい.

まず第一に,企業経営において ICT 依存が深まるにつれ,情報システムと情報の保護に加えて,その情報システムと情報をどのように企業活動に活用して,企業業績向上につなげていくかが,大きな経営課題である.したがって,活用しやすい情報システムの構築,活用しやすい情報の整備が重要な経営課題となる.この保護と活用が表裏一体となってこそはじめて,情報セキュリティが企業経営の重要課題になるのではないだろうか.

3.2 で述べたように企業活動において,情報システムと情報の活用が重要になればなるほど,また情報システムと情報への依存度が高まれば高まるほど,情報システムと情報が利用できなくなると,経営者と社員,さらには取引先や顧客などのステークホルダーの支障・不満が大きくなる.

さらに,最も利用したい緊急時に,情報システムや情報が利用できないことに大きな不満が出ることは,当然のことである.この意味では,情報システムと情報利用に関する BCP 作成と,緊急時の想定外の発生事象に対する柔軟な判断に基づく迅速・的確な行動が,情報セキュリティ担当者の重要な責務であろう.

第二に,インターネットでの情報発信が盛んに行われることが,情報セキュリティへ与える影響の問題がある.ソーシャルメディアを含めて,インターネットでの情報発信のハードルが技術的にもコスト的にも低くなっており,情報発信を専門にする人々以外の一般人が,活発に情報発信するようになっている.インターネットは,「万人」だけではなく「蛮人」にも開かれているため,4.5 で見たような流言・デマだけではなく,特定の組織・個人に損害を与える目的で,情報発信する事例も数多くみられる.

このような外部者の企業・社員に対する好ましくない情報が,企業の関与しないところで流されている.いわば標的型サイバー攻撃の情報版であるといえる.

したがって情報セキュリティは,自社を中心とする情報システムだけを対象とするだけではなく,外部のネットワークで流通している情報についても対象としなければ,自社ブランドや信用に悪影響が生ずる恐れが大きい.

この点についていえば,情報の完全性は,情報システムにある情報が「改ざん」されないことであると理解されているが,外部のネットワークで流通する自社に関する情報は,それ自体が「虚偽情報」であり,改ざん以前の問題であるといえる.

第三に,ブログやツイッターで,社員が自社の機密情報や自社の信用を低下させる書き込みをしたりするケースも数多くみられる.今後,スマートフォン利用が一般化し,クラウドに直接つながるようになると,自社の情報システムでの情報の流れの検知だけでは情報セキュリティ対策としては十分ではなくなる.このため,私的な好ましくない利用の問題に加えて,スマートフォンを社員がビジネスで利用する際の情報セキュリティ・ポリシーをどうするかも問われるようになる.これも「情報」の管理に関する問題である.

また,従来携帯電話系の情報セキュリティは比較的しっかり守られていたため,問題になることが少なかった.しかし,現時点では Android 系を始めとして,脆弱性を狙ったウイルス攻撃などの事例が多くみられる.今後対策は進むと思われるが,セキュリティ・ポリシーの問題に加えて,この問題にも注意を払う必要がある.このことは,情報セキュリティの対象が情報ネットワークに止まらず,コンピュータ以外の端末系にも広がることを意味している.

6.3 相互連携・協力に基づく対処

インターネットを使って企業や政府の機密情報を盗み取ろうとする,サイバーインテリジェンスと呼ばれるスパイ活動が,活発化している.これに対して,警察庁は国と契約関係のある防衛関連企業や先端技術企業約 4, 000社と「不正プログラム対策協議会」を設立して,対策を進めようとしている.[42]

また,内閣府の情報セキュリティ政策会議でも,安全強化策の議論が行なわれている.さらに,海外からのサイバー攻撃に対する対策も,検討されている.このように,官民連携のもとで,海外機関との連携も行いつつ,高度化するサイバー攻撃への対策など,安全保障や企業の競争力に直結する情報セキュリティ対策を進める機運が高まっている.

2011 年 7 月の刑法改正によって「ウイルス作成罪」が新設されたため,今後はサイバー犯罪条約を活用するなど対策の幅が広がるであろう.

また,BCP に関しては,各企業で見直しが進むと思われるが,図表 1 でみたように今回の大震災では,地域全体で大きな被害が発生している.この観点からは,4 章でみたような企業間の協力に加えて,行政,NPO,住民などと連携して,いわば社会生活・産業活動全体の継続計画ともいうべき地域ぐるみの対策が,立案され,実行されることが期待される.もし,これが実現できたなら,日本はより resilient な社会に近づくことになるであろう.[43]

参考文献

[1] ウルリッヒ・ベック,鈴木宗徳,伊藤美登里(編著)『リスク化する日本社会』岩波書店 2011 年
[2] 荻上チキ『検証　東日本大震災の流言・デマ』光文社 2011 年
[3] 河田恵昭『津波災害―減災社会を築く』岩波書店 2010 年.
[4] 酒井泰弘『リスク社会を見る目』岩波書店 2006 年.
[5] 立入勝義『検証　東日本大震災　そのときソーシャルメディアは何を伝えたか』
[6] 畑村洋太郎『「想定外」を想定せよ!失敗学からの提言』ＮＨＫ出版 2011 年
[7] 林紘一郎,田川義博,浅井達雄『セキュリティ経営』勁草書房, 近刊.
[8] 広瀬弘忠『人はなぜ逃げおくれるのか』集英社 2004 年
[9] 橘木俊詔・長谷部恭男・今田高俊・益永茂樹『リスク学入門 1』岩波書店 2007 年
[10] Kotler, Phillip and John A. Caslione “CHAOTICS: The Business of Managing and Markething in the Age of Turbulence” AMACOM 2009. 斉藤慎子訳『カオティックス』東洋経済新報社 2009 年
[11] Clarke, Richard A. and Robert K. Knake“Cyber War:The Nest Threat To National Security And What To Do About It” Harper Collins Publishers 2010 北川知子・峯村利哉訳 『サーバー戦争:見えない軍拡が始まった』徳間書店 2011 年

[42] 出典:日経新聞,2011 年 8 月 4 日夕刊.

[43] 5.3 で紹介した 2011 年 9 月 28 日に公表された内閣府中央防災会議の「東北地方太平洋沖地震を教訓とした地震・津波対策に関する専門調査会」報告書が,このような包括的な対応策のスタートになるものと考えられる.