情報管理 JOHO KANRI
2013
vol.55 no.11
Journal of Information Processing and Management
2 February
http://johokanri.jp/

情報システムリスクから考える事業継続計画（BCP）の考え方

Proposal of BCP (Business Continuity Plan) from threats to information systems

内田 勝也[1]

UCHIDA Katsuya[1]

1 情報セキュリティ大学院大学 名誉教授　E-mail：uchidak@gol.com
1 Professor Emeritus, Institute of Information Security

原稿受理 （2012-12-20）
情報管理 55(11), 810-818, doi: 10.1241/johokanri.55.810 (http://dx.doi.org/10.1241/johokanri.55.810)

著者抄録

情報システムの重要性は益々増大しているが，東日本大震災後の調査でも万一に備えた対応を考える事業継続計画の策定が必ずしも十分ではない。経営トップの無関心や最初から100%完璧な計画の策定を想定しているためとも思われる。本稿では，守るべき情報資産と事業継続を脅かすリスクについて考察した。主なリスクである大規模地震や台風・集中豪雨，テロ，その他（突発的大規模停電）について，事業継続を考える上で必要な事柄を過去の知見から得られた内容について考察した。事業継続計画の文書化に役立ち，机上や実践的訓練に役立てるものと考えている。文書化と訓練の相乗効果が，事業継続計画策定のキーポイントになる。

キーワード

事業継続計画（BCP），情報資産，リスク，脅威，脆弱性，可能性，管理策

1. はじめに：災害時におけるBCPの重要性

近年，組織における情報システムの役割はますます増大してきた。それに連れ，自然災害や人的ミス，外部からの攻撃等により，情報システムが停止に追い込まれる，あるいは，サービス提供が十分できない状況がしばしば見られる。

自然災害では，米国では2005年に巨大なハリケーン「カトリーナ」が，2012年には「サンディ」が上陸し，どちらも情報システムに大きな被害をもたらした。国内では2011年3月に東日本大震災が発生し，大地震に伴う大津波による情報システムへの被害は甚大なものとなった。近い将来，首都圏直下型や東海地震，東南海・南海地震などの発生が危惧されており，さらに，東海，東南海，南海の3地震が連動して発生するとも言われている[1)]。

人為的なミスもある。情報システムの外部委託では，安全・安心を唱っていたクラウドサービスで，基本的な操作ミスにより，6,000社近くの企業等のデータが消失し，データのバックアップをとっていなかった企業等は，日常業務が止まるという大きな影響を受けた[2)]。また，インターネット上では機密

情報や個人情報の漏えいの発覚やDDoS攻撃（分散型サービス妨害攻撃）が増えており，ネットワークを利用した業務に大きな影響を及ぼしている。

情報システムを利用する場合，このような状況を回避するためにはBCP（Business Continuity Plan，事業継続計画）が必要になる。

BCPとは，組織が事故や災害等に遭遇しても，必要な事業を継続し，復旧を果たせるような対応計画を策定することを言う。この計画を策定するため，事故や災害が組織にどのような影響を及ぼすかの分析を行い，リスクや損害を考える。広義のBCPでは，企業・組織全体を考えることもあるが，本稿では，情報システム面からの考察に限定した。

図1に示すように，BCPでも継続的な改善を行うことになるが，①経営者による方針策定，②計画の策定として，どのような災害を想定するのか，事業の優先度や事業への影響評価等を行う，③対応の実施・運用，④関係者の教育・訓練の実施，⑤教育・訓練の結果を評価し，必要があれば是正する，⑥経営者によるレビューを行う。これを継続的に繰り返していく。

2. BCPの策定を妨げるもの

2011年3月の東日本大震災後に，一般社団法人日本情報システム・ユーザー協会（JUAS）がBCPへの取り組みについて，調査を行った[3)~5)]。

情報化が進んだ今日では，情報システムなしに企業経営を行うことは不可能と思われ，情報システムを停止させない，あるいは，停止時間を最小限にするために，BCPの策定は不可欠である。

JUASの調査で，原田[4)]は「東日本大震災で直接被害を受けた企業でも，34%は経営者からのBCP見直しの指示がなく，また，東日本大震災後でもユーザ企業の半数以上がBCPを策定していない」と述べている。

経営者の情報システムへの関心が低ければ，当然ながらBCPへの関心も低い。このような場合，経営者には心理学でいう「正常化バイアス（Normalcy bias）」があるのではないかと，筆者は考えている。すなわち，大きな自然災害等が発生しても，自分の所は，正常に運用することができ，BCPを発動する必要がないと考えているのではないだろうか？

あるいは，経営者の多くが情報システムは，「専門性が高く，自分にはわからない」，情報システム部門に権限委譲しているので問題ないと考えているが，実際には情報システム部門へ「丸投げ」しているのではないだろうか。

もちろん，経営者に専門用語を使って説明している情報システム部門もあり，その辺りにも問題があるかも知れない。

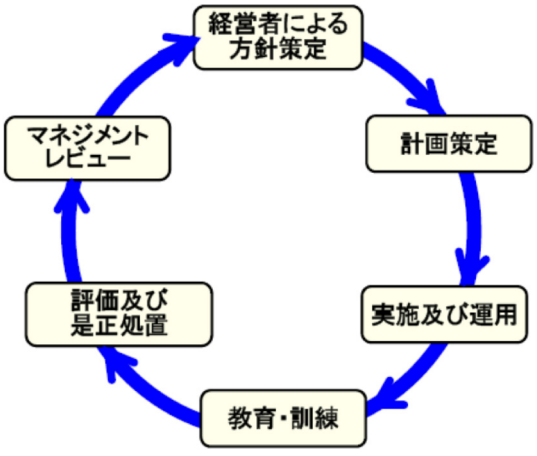

図1　BCPサイクル（継続的改善を行う）

3. BCPにより守るべき情報資産

3.1 情報資産とは

情報システムでは，情報資産を**表1**に示す4種類と考えている。

情報は無形だが，一般的には何らかの形で有形のものに保存される。これら，4種類の情報資産の1つでも欠けると，BCPの運用が困難になる可能性がある。この4種類について考えるべきことを以下に述べる。

表1　情報資産の種類

種　類		特　徴
(1)人間		代替不可能。ただし，同一作業を複数人で行えるが，費用が課題になる
(2)情報	①アナログ	複写可能だが原本と異なる。同一物が複数ある場合とそうでない場合がある
	②デジタル	原本と同じものを複数作成可能。遠隔地での対応も可能
(3)テクノロジー		ソフトウェア，ハードウェア等
(4)設備		複数設備を持つことは可能だが，他の情報資産の準備も必要

(1) 人間：情報システムを動かすだけでなく，データの入力や情報を使って作業する人たちも必要になる。BCPを実行するには，現在の情報システムの一部，または全部を他の場所で運用しなければならないこともあり，そのための要員も必要になる。

2001年9月11日に発生した米国同時多発テロでは，BCP要員が心的外傷後ストレス障害（PTSD）になり，他はすべて揃っていたが，担当者が業務を行えず，復旧ができなかったとの指摘もあった[注1)]。

大企業等では，経営トップが常に陣頭指揮をとれないこともあり，複数の経営者が必要に応じ，陣頭指揮をとれるように考えていた所もある。例えば，経営者の自宅の近辺に住んでいる管理職がその経営者を支える仕組みを構築する。夜間や休祭日等の緊急時に，最も適切に緊急対応が可能な経営者が配下の管理職とともに，BCP対応を行うと定めている。

緊急事態が発生した場合，常に経営トップが陣頭指揮をとれないことも含め，迅速・適切にBCPを行う体制の構築が重要である。

(2) 情報：

① アナログ情報：情報システムではアナログ情報は少なくなってきたが，BCP発動時に運用先のコンピューターで請求書等を決まったフォームに印刷するには，必要な用紙を必要枚数確保しておく必要がある。

② デジタル情報：原則的には原本から複製したデータを遠隔地に保管し，BCP発動時は，それを利用するべきである。費用面や煩雑さ等から，同一場所で保管していたため，全情報が喪失した例は多々ある。3.11東日本大震災では津波，9.11米国同時多発テロではビル崩壊のため，原本だけでなく，複製も喪失した例がある。従来，地震等への対処は，40km以上離れた場所への保管が必須と言われた。これは，大地震を想定したものであるが，当然ながら，大地震に伴う津波では，40km以上の距離でも津波が襲う可能性のある所では意味がない。逆に，テロや火災等では5km程度でも十分対処でき，何を対象にしてBCP対策を考えるかで保管場所も異なる。

最近はクラウドコンピューティングの利用が進展しているが，事業者が全データを破壊した事故も発生しており，利用者側に複製がなく，全情報がなくなった事故も発生している[2),6)]。

(3) テクノロジー：ソフトウェアやハードウェア等も，BCPでは重要だが，完全に同一物を遠隔地に準備することは，一般的には難しい。外部委託でクラウドコンピューティングを利用する場合，代替手段があるかの検討が欠かせない。外部への委託でも，通信回線に問題が起これば処理不能になる。

(4) 設備：電力や水，建物等が該当する。自社システムの場合，費用面から考えると，バックアップセンター，あるいはサブセンターとして運用し，緊急時はBCPで利用する。

電源は自家発電装置や蓄電池も必要になるが，津波，集中豪雨，台風等でビルの地下に水が流れ込めば，すべての電源が冠水し，電源供給が不可能になった例もある。電源を地下に設置する場合，環境を考慮する必要があろう。

大地震では，液状化により地下洞道とビルとの接続部分でケーブルが被害を受けた例もある。

クラウドコンピューティングでも，外部委託先のデータセンターで同じような問題が発生する可能性がある。

3.2 BCP対象業務について

企業等では，最も重要な業務の実行が妨げられた場合，どのような影響を組織全体に及ぼすかを考える必要がある。例えば，大地震やそれに伴う津波を考えると，BCPの策定は意味がないとの指摘もあるが，まずは最低限の対応を考える。絶対に企業活動が止まって困る業種以外は，人間や情報が無事ならば，時間がかかるが，復旧は可能であろう。経営者も含め，すべての従業員が対応できなくなれば，何の意味もない。

また，以下で述べるリスクを考えることにより異なる対応になる。最初から無理だから検討しないことが最悪である。発生可能性のあるリスクについて考えることになるのは当然である。

4. リスクを考える

あらゆる分野で，絶対安全を要求しがちだが，100%の安全は存在しない。時間が流れ，何か行えば，必ず安全を脅かす「リスク」が存在する。

リスクでは以下の5つを考える必要がある。

① 脅威（Threat）
② 脆弱性（Vulnerability）
③ 可能性（Likelihood）
④ 影響（Impact）
⑤ 管理策（Control）

上記は，①雨が降る，②窓が開いている，③室内にあるカーペットが濡れる可能性がある，④カーペットを購入しなおす／修繕する，⑤カーペットが濡れないように，雨が降れば自動的に窓が閉まる仕組みを導入する，と考えるとわかりやすい。

また，リスクの大きさは，脅威，脆弱性，資産価値の3要素のベクトル（または，乗算）で決まる。資産価値が小さいと，リスクも小さくなる。センター試験等では，試験問題は，試験前日までは重要だが，試験終了後は価値が低くなる。リスクの大きさを決める3要素に時間軸を含め4要素で考える必要もある。一度決めたリスクは永久不変ではないので，定期的な見直しが必要になる。

リスクも「費用対効果」を考える必要がある。どのような脅威が存在し，そのリスクの大きさを考えて対応する必要がある。

例えば，米国東部やヨーロッパの大部分では，大地震が発生する可能性はない。大地震による広域災害の想定は不要である。一方，日本や米国東部・南部は，台風やハリケーン被害を考える必要がある。

5. 過去の事例に学ぶリスク

脅威としてどのようなものがあるかを考えるには過去にどのようなことが発生したかを知ることは有用で，「歴史から学ぶ」ことの意義は大きい。

5.1 大規模地震

東日本大震災は記憶に新しいが，1995年1月17日の阪神淡路大震災もいくつかの教訓を残している。

最近のビルは，震度7にも耐えられる構造を持っており，大規模な地震でも建物が崩壊する可能性は少ない。しかし，以下の検証は大切であろう。

(1) 液状化現象：阪神淡路大震災では，洞道とビル間で通信ケーブルが液状化により被害を受けたと聞いている。液状化により，マンホール等が大きくずれると，中を通っているケーブル等に損傷が発生する。近年はこのような液状化を防ぐ方法やケーブルに余裕を持たせ，多少ずれても，ケーブルに損傷がでない工夫も行われるようになった。
(2) 停電・断水：電源や給水設備は，セミナー等で質問をしても，地下階設置の回答が多い。蓄電池等，バックアップ電源も同一場所であれば，津波や洪水等で同時に役立たなくなる可能性がある。

給水設備では屋上まで冷却水を上げ，屋上に設置した給水タンクから供給することもあるが，停電では屋上まで冷却水を上げられず，断水に追い込まれる。さらに，配管や給水タンクが地震の揺

れで壊れ，屋上の給水タンクの水がビル内に溢れたこともある。

阪神淡路大震災で，大手金融機関のデータセンターは無事だったが，周辺地域が断水し，空調用冷却水の供給が断たれ，ビル壁に穴を開け，毎日給水車で必要量の冷却水を確保し，コンピューターを運用した例も聞いている。

最近のサーバー類は従来のメインフレームより単位面積当たりの発熱量は大きいが，空冷式空調で，冷却水を利用しないデータセンターもある。

また，自家発電機（ディーゼル発電機）で，大手のデータセンターでも，3.11東日本大震災までは，燃料は半分程度だったが，3.11以降，満タンにしているとの回答もあった。

一部の中小データセンターは，3.11以降の計画停電時には燃料確保ができないため，データセンターサービスを停止する可能性があると表明した所もある[7),8)]。

(3) タンク火災：1964年の新潟地震以降，大地震の発生時には，多くの場合，タンク火災が発生している。

2009年3月の十勝沖地震では，石油タンクの液面揺動（スロッシング）に起因し，苫小牧の製油所で原油タンクが約8時間炎上した。

東日本大震災でも，千葉県市原市の製油所の液化石油ガス（LPG）タンクが約8日間炎上した。

今後予想される大地震でも大都市圏の近辺にあるコンビナート火災と津波の複合化災害が発生すると大きな被害が想定される。

東京湾岸には，神奈川県に根岸・本牧地区，扇島地区等と千葉県市原市等を中心に，5,000基以上のタンクがあり，これらのタンクの危険性が指摘されている。

(4) 電話／携帯メール：電話や携帯での安否確認や連絡が非常に重要だが，3.11でもいくつかの課題が残った。

携帯電話は固定電話以上につながらなかった。

また，通信量増大防止策として，184（発信者番号非表示）発信扱いとしたため，受信者が184発信拒否設定の電話には接続できなかった。

固定電話の場合，停電時に利用できなくなるものが多い。最近，IP電話の利用が増えているが，停電時に利用できないことが多い。

携帯メールは，「メール問合せ」（**図2**）機能を実行しないとメールが受信できないこともあり，この機能を知らず，新規の受信メールがないと誤認する可能性がある。利用する場合，周知が必要であろう。

(5) インターネット：被災地以外では比較的容易に利用でき，3.11でもSNS（ソーシャルネットワーキングサービス）が被災直後から頻繁に利用され，安否確認や企業からの情報提供に利用されたが，デマ情報やなりすましによる混乱も一部で発生しており[9)]，功罪両面があったと言える。

大地震の場合には多くの状況に対応する対策を考える必要があるが，バックアップデータを遠隔地に保管し，万一に備えるだけの考えもある。

5.2 台風・集中豪雨

地球規模の温暖化現象のためか，集中豪雨や大型の台風等の発生が多くなってきている。

最近の集中豪雨は，大都市圏でも30mm／時間を超える豪雨もかなりの頻度で発生している。都内の

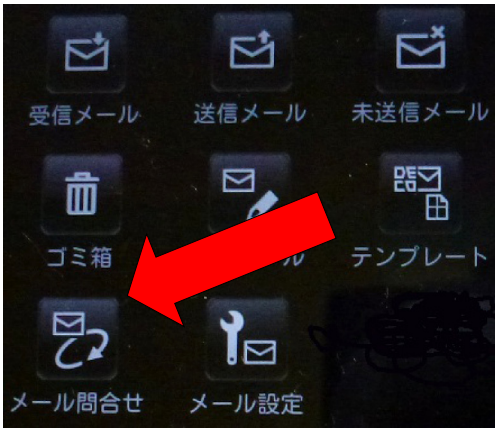

図2　スマートフォンのメール問合せ

神田川下流域では**表2**のような豪雨があった[10]。

これらは，「内水氾濫」と言われ，都市内を流れる中小河川で豪雨の処理ができないと，マンホールや一般家庭の風呂場等から逆流することがある。

道路などに溢れた水の水位が高くなれば，ビルの駐車場スロープ等から，地下に流れ込み，地下の電気施設や給水施設に被害を与える。

実際，1994年9月，伊丹空港ビルが集中豪雨により，地下に雨水が流れ込み，電気系統が被害を受け，ビル機能が麻痺した事故が発生した[11]。

河川氾濫では，「2000年東海豪雨」が有名で，名古屋の総雨量が562mmに達し，年間総雨量1,532mmの3分の1以上が降り，名古屋市の西を流れる新川が名古屋市あし原町で破堤，庄内川は一色大橋の右岸で溢水し，26,000棟以上が床上浸水した（**表3**，**図3**）。

近年，首都圏は大きな河川氾濫がないが，1993年，当時の建設省が200年に1回程度の降雨量「3日間に548mm」で，荒川下流域で破堤が発生すると想定したシミュレーションを行った。最悪は右岸16.75kmの破堤と結論した（**表4**, **図4**）[注2)]。500メートルメッシュで計算したが，最大浸水深度は約6メートルで，被害額は約38兆円に達した。

厳密には，洪水と呼ぶのは適切でないが，シカゴのダウンタウンのビル群の地下階にシカゴ川の水が流れ込み，大きな被害が発生した。「The Great Chicago Flood」と言われ，1992年4月にダウンタウンの各ビルを地下でつないでいた地下道（**図5**）[注3)]にシカゴ川の改修工事に使っていたコンクリートパイルが原因で，シカゴ川の水が溢れ，地下道とつながっていたビルの地下にも水が流れ込み，約1週間都市機能が麻痺した[12]。

表2　神田川下流域の近年の豪雨

年月日	原　因	総雨量	時間最大
1989年8月	集中豪雨	276mm	70mm
1993年8月	台風11号	288mm	47mm
2004年10月	台風22号	284mm	57mm
2005年9月	集中豪雨	263mm	112mm

表3　2000年東海豪雨の被害状況

愛知県計	住家被害									
	全壊		半壊		一部損壊		床上浸水		床下浸水	
	棟	世帯	棟	世帯	棟	世帯	棟	世帯	棟	世帯
	15	20	56	75	167	171	26,531	27,371	38,879	39,963

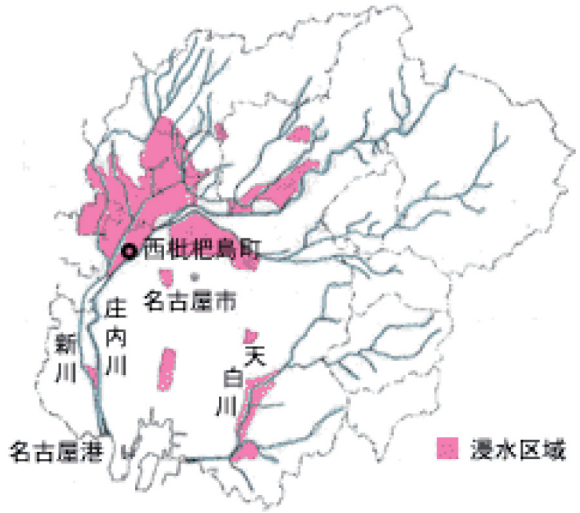

図3　庄内川周辺浸水図

表4　荒川下流被害想定概要

全被害状況	
浸水面積	82.8km^2
浸水区域内人口	1,163,031人
床下浸水戸数	18,085戸
床上浸水戸数	456,052戸
被害額	384,947億円

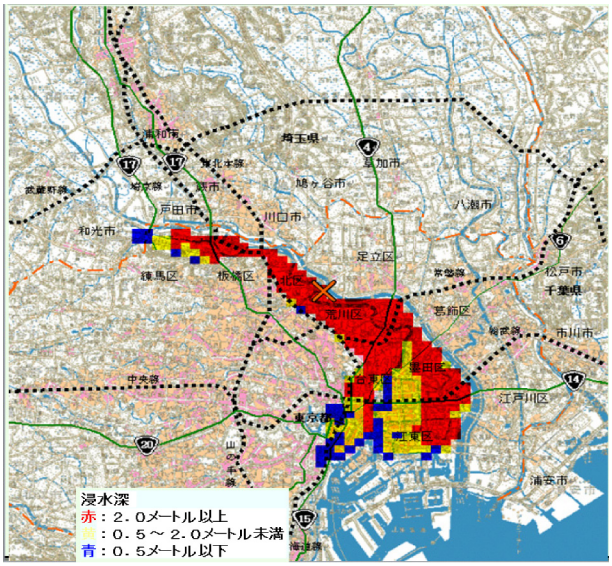

図4　荒川右岸16.75km破堤の被害想定地図

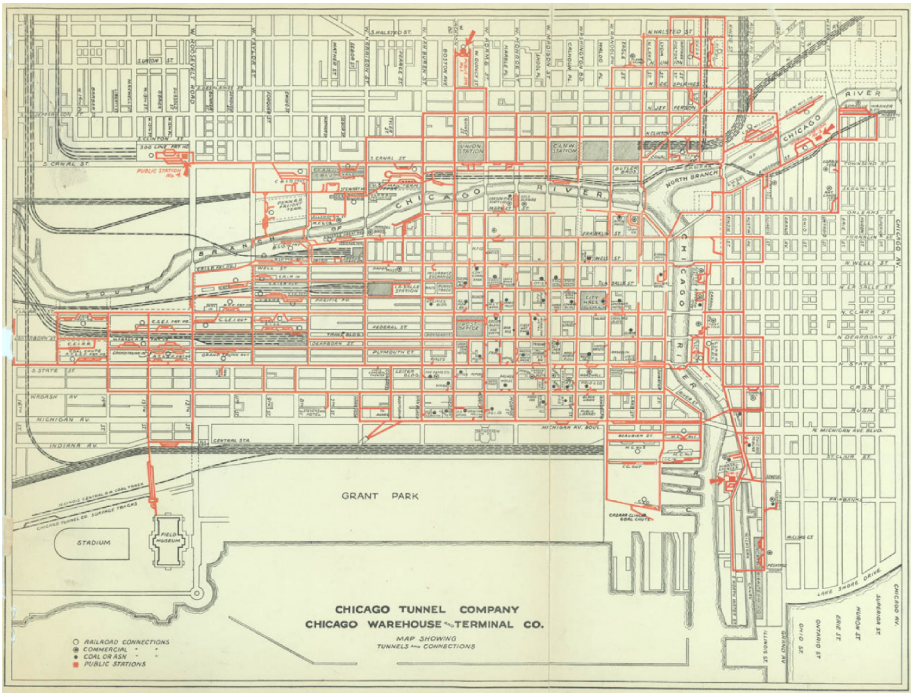

図5　シカゴのダウンタウンの地下道

台風や集中豪雨，河川氾濫等による洪水の被害では，地上だけでなく，地下に被害が及ぶと，地下に設置した設備が被害を受け，ビル機能が麻痺することが多い。国内でも大都市圏では，地下鉄や地下道が発達しており，地下への被害を防止するための止水板等の対策を考えているが，荒川下流破堤の計算では，最大浸水深度は6メートル近くになり，地下への水の流入は避けられないであろう。BCP立案の場合には十分考慮する必要がある。

5.3 その他

国内でのテロは，一連のオウム事件での「地下鉄サリン事件」がある。欧米では大規模なものが発生している。

2001年9月11日「米国同時多発テロ」では，WTCビル内にバックアップデータを保存していた企業も数多くあった。ただ，前述のように，大地震や台風・洪水被害から比べると被害範囲はかなり小さい。

テロではないが，過失や豪雪による大停電が国内で発生している。

(1) 2006年首都圏大停電：2006年8月，東京都江戸川区と千葉県浦安市の間を流れる旧江戸川を横断する東京電力特別高圧送電線「江東線」（27万5,000ボルト）にクレーン船が接触する事故が発生した。これにより，7時38分頃に約122万戸が停電し，さらに品川火力発電所が供給バランスを崩して自動停止したため，約17万戸がさらに停電した。停電が完全に復旧したのは，12時20分であった[13),14)]。

この事故で，日本経済新聞社が計算している「日経平均」等の算出ができなくなったが，電源を自家発電装置に切り換える時点で問題が生じた。

また，旅行サービス業務の受託企業は電力供給再開時に，過電流によりUPS（無停電電源装置）が故障し，再開までに1時間以上を要した。

サービス停止には至らなかったが，停電で正常な終了プロセスを経ずサーバーがダウンし，サーバーのデータベースのクラスター機能の整合性がとれず，1台で稼働させ，ベンダーの支援で復旧をはかった受託企業もあった。

この時はなかったが，自家発電装置の燃料の備蓄量が問題になる可能性は高い。

(2) 豪雪：「2005年新潟豪雪」では，強風雪による絶縁体碍子の塩害と送電線が振動しショートする「ギャロッピング現象」が同時複合的に発生し，最大時約35万戸が停電し，最大31時間停電した。

本稿では，主に自然災害を中心に述べたが，この他にも，「パンデミック」では，人的被害の発生や人間の移動が制限される。また，近年，インターネットに社会が大きく依存しており，大規模なサイバー攻撃等により，コンピューターやネットワークの利用が困難になり，社会活動が停止する事例も海外では発生している[15]。また，国内の通信ネットワーク機器の脆弱性により大規模停止になるとの指摘もあり，機会があれば述べたい。

6. 終わりに

3.11東日本大震災以降，BCP策定の必要性が叫ばれているが，必ずしも十分に浸透していない。ガイドライン通りに行うことの大変さもあると考えている。

本稿では，情報システムに対するリスクを考えることで，それに対応する対策を考えることができると考え，ガイドラインから離れ，従来から気になっている脅威をまとめた。

明確に脅威を考えられれば，それに対応したBCP対策を構築できると考えている。

もちろん，脅威について新たに発生するもの，従来のものの見直しがあったりするが，それらを考慮してリスクを考えることが大切で，リスクは変動すると考える必要がある。

また，BCPは文書化で終わりでなく，訓練を積み重ね，それを知識，知見とすることが大切である。BCPにも完璧はない。訓練（机上，実訓練）を積み重ね，文書を修正する。危機が発生し，「想定外」と言わないためにも，訓練も重要である。

本文の注

注1) 2002年6月に開催されたCSI（Computer Security Institute）主催のNetSec 2002にて，講演者の1人が述べたもので，具体的な企業名等は確認したが，開示されなかった。国内でも大きな災害等が発生するとPTSDになる人がいるので，BCP要員がPTSDになっても不思議ではない。

注2) 実際には，全国主要10河川について，おおむね100年から200年に1度程度発生すると予想される降雨量で，5km程度の間隔で右岸・左岸が破堤した場合の被害想定を行い，洪水氾濫のハザードマップを作成した。

注3) 昔は暖房用石炭を運ぶトロッコ通路で，現在はCATVケーブル等が敷設されている（http://www.structuremag.org/article.aspx?articleID=307）。

参考文献

1) 南海トラフの巨大地震モデル検討会（第1回）. 東海地震，東南海・南海地震について. 2011-08-28. http://www.bousai.go.jp/jishin/chubou/nankai_trough/1/2.pdf, (accessed 2012-11-06).

2) ファーストサーバ株式会社. “6/20に発生した大規模障害に関するお詫びとお知らせ”. ファーストサーバサポートWEB. http://support.fsv.jp/urgent/index.html, (accessed 2012-11-06).

3) 原田俊彦. 第18回企業IT動向調査2012（11年度調査）. 2012-03. http://www.juas.or.jp/servey/it12/it12_press_pp.pdf, (accessed 2012-11-06).
4) 原田俊彦. "不安が大きいソーシャルリスク，BCPの策定企業は半数未満". 日経ITPro. 2012-05-30. http://itpro.nikkeibp.co.jp/article/COLUMN/20120511/396128/, (accessed 2012-11-06).
5) 井上健太郎. "日本企業の大災害対策はそんなに停滞しているのか？". 日経ITPro. 2012-09-07. http://itpro.nikkeibp.co.jp/article/Watcher/20120903/420061/, (accessed 2012-11-06).
6) 動かないコンピュータ グーグルPaaSが停電で2時間停止 一部データで整合性に問題発生. 日経コンピュータ. 2010, no. 753, p. 88-90.
7) 株式会社ソリッドシステムソリューションズ. "東北地方太平洋沖地震の影響に関して". Solid Online Support System. 2011-03-17. https://www.soss.jp/content/2011031701.html, (accessed 2012-11-06).
8) サンファースト株式会社. "東北地方太平洋沖地震の影響について". サンファースト株式会社. 2011-03-29. http://www.sunfirst.co.jp/detail/detailG000000001_43.html#B000000354, (accessed 2012-11-06).
9) ITmedia. "イオングループ企業，取締役なりすましTwitterが原因で炎上「法的措置も」". ITmediaニュース. 2011-04-07. http://www.itmedia.co.jp/news/articles/1104/07/news077.html, (accessed 2012-11-06).
10) 河川整備基金助成事業. 平成17年9月関東地方大雨による市街地浸水災害調査と防災対策研究. http://www3.kasen.or.jp/docs/2005/01/171251003.pdf, (accessed 2012-11-06).
11) "台風は大型化している". 日経BP. http://www.nikkeibp.co.jp/sj/2/special/169/index2.html, (accessed 2012-11-06).
12) Wren, Jon. "The Great Chicago Flood". Structure Magazine. http://www.structuremag.org/article.aspx?articleID=307, (accessed 2012-11-06).
13) 東京電力. 8月14日に首都圏で発生した停電事故について. TEPCO REPORT. 2006, vol. 116.
14) 東京電力. "クレーン船の接触に伴う当社特別高圧送電線損傷による停電事故について". 東京電力. 2006-08-14. http://www.tepco.co.jp/cc/press/06081401-j.html, (accessed 2012-11-06).
15) Krebs, Brian. "Georgian Web Sites Under Attack". The Washington Post. http://voices.washingtonpost.com/securityfix/2008/08/georgian_web_sites_under_attac.html?nav=rss_blog, (accessed 2012-12-19).

Author Abstract

By the investigation after The Great East Japan Earthquake, more than 50% of the companies do not make business continuity plan. By this article, I reviewed threats to information assets that you should have defended and the business continuity. About major threats, that is, large-scale earthquake and typhoon / torrential downpour, terrorism, other (a sudden massive blackout), I explained these contents obtained from past knowledge to give you a necessary image when you thought about business continuity plan. I believe that this article is useful for not only a desktop / practical training but also documentation of the business continuity plan. I am confident that the synergistic effect of documentation and the training becomes the key of the business continuity plan.

Key words

business continuity plan, information asset, risk, threat, vulnerability, likelihood, control