「米国における BCP（事業継続計画）、DR（災害復旧）への対応状況」

渡辺弘美@JETRO/IPA NY

1. 米国連邦政府における BCP、DR 策定状況

(1) 国土安全保障省による政府向けガイドライン

2001 年 9 月 11 日の同時多発テロ以降、度重なるテロリストからのテロ予告に加え、ハリケーン・カトリーナなどの天災による被害を受け、米国政府は、BCP（Business Continuity Planning＝事業継続計画）や DR（Disaster Recovery ＝災害復旧）の重要性を認識し、その対応を余儀なくされている。

① 連邦政府における BCP、DR ガイドライン

現在、連邦政府レベルで、緊急時対応計画活動を規定している大統領発行文書が 3 つ存在する。その中で、最も古いものは、大統領命令（Executive Order＝E.O.） 12656 で、1988 年の冷戦の時代に発令され、現在も有効である。その後、大統領指示事項（Presidential Decision Directive＝PDD） 67 と E.O. 13286 がテロリズムの脅威が高まる中 1998 年と 2003 年にそれぞれ作成されている。

これまでにホワイトハウスより発表された主な BCP/DR 関連文書

大統領発行文書	概要
E.O. 12656： 緊急事態準備責務の任命	E.O. 12656 は、1988 年 11 月 23 日に Ronald Reagan 大統領によって公布され、国家安全緊急事態準備責務を連邦政府の省と機関に任命している。 E.O. 12656 は、国家安全保障緊急事態を、米国の国家安全を深刻に脅かす自然災害、武力攻撃、技術関連緊急事態とその他の緊急事態と定義している。この命令は、直接業務継続に言及していないが、国家安全保障緊急事態に対応し、そこから復旧しなければならない連邦政府の政策作成、計画、手順、準備度合い測定を含んだ準備における役割を明細に述べている。

	E.O. 12656 は、国家安全保障緊急事態準備政策を検討する主な公開討論の場として、国家安全保障会議（National Security Council=NSC）を指定している。 また、この命令は、FEMA（Federal Emergency Management Agency=連邦緊急事態管理庁）長官に適切な動員準備、民間防衛、政府の継続、技術関連災害やその他の問題を含んだ国家安全保障緊急事態準備において NSC の助言者となることを要請している。FEMA はまた、省や機関、州や地方政府と協力して、準備政策の実運用を援助することを要請されている。
PDD 67： 憲法にのっとった政府持続と、政府運営の継続	PDD 67 は、1998 年に Bill Clinton 政権によって、公布され、NSC により機密扱いとされているため、詳細は不明。しかし、国土安全保障会議（Homeland Security Council=HSC）スタッフが作成した機密扱いを受けていない指示事項のファクトシートによると、緊急時対応計画作成活動とは、政府の行政・司法・立法の三府が統治能力を保持し、リーダーシップを継続して示し、防衛と民間の要求に応えるために必要な本質の機能とサービスを提供することを保証するという国家安全保障の最優先度課題である。 PDD 67 ファクトシートによれば、PDD67 には、憲法にのっとった政府機能の持続と、本質的連邦制度を継続するために設計され、政府の持続（enduring constitutional government=ECG）、COG（Continuity of Government）、COOP（Continuity of Operations）という 3 つの政策概念を核とするプログラムに関して記述されているとしている。 また同ファクトシートによれば、PDD67 は、大統領府を含むすべての行政機関が現実味のある COOP 計画を確立すべきとしている。これにより、非常事態に権限の委譲、重要な資源、施設、記録の保管、ビジネス再開のために必要な資源の緊急かつ即時確保、通常運営が再開できるまでの代替仕事場での業務などを保証する継続プログラムが提供されることを求められている。

E.O. 13286： 国家安全保障省（Department of Homeland Security＝DHS）長官への一部機能の移管に伴う、大統領命令と決定の改正	E.O. 13286 は、2003 年 2 月 28 日に George W. Bush 大統領により、公布された。この命令は、E.O. 12656 で FEMA 長官に与えられた権限を、国家安全保障長官に移すことを指示したものである。 DHS は 2003 年 1 月に始動。FEMA はそれまで大統領直轄機関であったが、DHS 設立により、2003 年 3 月より、DHS 配下の組織に組み込まれている。

これらに加えて、COOP（Continuity of Operations＝業務継続）計画作成について、より詳細な内容を指示した連邦準備令（Federal Preparedness Circular=FPC） 65 が FEMA により 2004 年 6 月 15 日に発行されている。

同法令は、大統領府及び各連邦政府機関が、COOP と称して、政府の BCP/DR 作成を進めることを求めている。これに対応し、政府の各省、機関などは、COOP 計画を作成し、緊急事態が発生した場合でも、その計画に基づき、基本的な機能・業務については、稼働を続けることができるよう保証することが要請されている。こうした計画作成には、事が起こった際に、組織全体として、多数の関係者が連携して復旧努力を実施できるよう、組織内の多くの専門家（緊急事態管理、インフォメーション・テクノロジー、物理的安全、人的資源、施設管理など）が携わっている。

FPC 65 は、連邦行政部門の COOP を先導する機関として FEMA を位置づけた。同権限は、先にあげた PDD67 によって、FEMA に与えられたが、2003 年 3 月 1 日、FEMA が DHS の一組織となったことで、DHS 長官に同権限自体は移され（E.O. 13286）、同長官より FEMA に委任される形式をとっている。また、FPC 65 では、FEMA の ONSC（Office of National Security Coordination）が、COOP プログラムを先導する機関に指命されている。FPC 65 は、FEMA の責務を、各行政機関が、実現性が高く、実行可能な COOP 計画を作成し、他の関連機関との調整をし、自機関の COOP 能力の状況を監督、査定する際に使用できるガイダンス、標準を作成することと定義している。

一方、FPC 65 によれば、各々の行政部門機関は、FEMA によるガイダンスに従って機関ごとの COOP プログラムの計画・実施を行うとともに、COOP 活動の調整役として、幹部クラスの連邦政府行政官を任命する責任があるとされている。

他にも FPC 65 には以下の内容が含まれている。

- 非常事態において、きわめて重要なサービスの提供、市民権力の行使、安全の維持、経済の持続をその間保証する『必須機能』を確認することが COOP 計画の基礎であるとしている。
- 11 の分野（①計画と手順、②必須機能、③権限の委任、④継承の順位、⑤代替運営施設、⑥相互運用可能な通信、⑦きわめて重要な記録とデータベース、⑧人的資本、⑨テスト、訓練、実習、⑩監督権と指揮権の委譲、⑪再構成）において、現実味のある業務継続能力の要素を定義している。
- 継続計画を調整するための機関間ワーキンググループを設置することを求めている。

FPC 65 は、Washington D.C.だけではなく、全米にある連邦政府機関に適応される。それは、各々の機関の長に以下を含む責務を負うことを義務付けている。

- 機関の継続計画と手順を作成、承認、維持する。
- COOP 複数年戦略と、プログラム管理計画を作成する。
- 機関の継続計画、緊急時対応スタッフ、必須システムと機器のテスト、訓練を実施する。

上記 FPC 65 に定義されている要素のうち IT に特に関係するものは、⑤代替運営施設、⑥相互運用可能な通信、⑦きわめて重要な記録とデータベースの 3 つである。

FPC65 上の IT に関係するガイダンス

分野	計画に含まれるべき内容
代替運用施設	・すべての機関は、COOP 計画の一部として、代替運営施設を定め、準備しなければならないとしている ・代替運営施設は、可能なかぎり短時間で、少なくとも施設使用開始から 12 時間以内に、必須機能を提供できるだけの能力を持たなくてはならない。 ・代替運営施設は、業務遂行に必要な支援、サービス、インフラストラクチャ・システムを提供できなければならない。 ・代替運営施設は、重要な内外の組織、顧客、一般大衆との相互通信を提供できなければならない。 ・代替運営施設は、コンピュータ機器、ソフトウェア、その他必要な自動データ処理機器を提供できなければならない。
相互運用可能な通信	・すべての必要な通信と IT 能力は、COOP 活動化後できるだけ短時間で、遅くとも、12 間以内に使用

	可能となっていなければならない。 ・ COOP 通信計画（COOP Communication Plan＝CCP）に挙がっている省、機関は、四半期ごとにそれらの代替施設における通信能力をテストしておかなければならない。
重要な記録とデータベース	・ 機関に所属する者は、必須機能を実行するために、電子文書や、ハード・コピー文書、参考文書、記録、インフォメーション・システムにアクセスでき、使用することができなければならない。 ・ 上記を守り、更新していく手順も揃っていなければならない。

② GAO レポート（2005 年 4 月）

このように、FEMA は連邦政府機関における COOP 計画の旗振り役としての位置づけを与えられているものの、それが十分機能せず、各機関では対応がいまだに遅れていることを指摘する声が GAO（Government Accountability Office）から上がっている。

GAO は、同時多発テロ発生後の 2002 年 1 月、機関の継続計画遵守性に関して調査を実施した。その結果、多くの機関とその部署が、継続計画を準備できておらず、準備できているとしている機関でも FEMA のガイダンスに沿ったものではないと判断した。その後、DHS 設立、FEMA の位置づけ変更などを経て、各政府機関がどのように COOP 計画を進めているか調査するため、GAO は再度 2004 年 5 月から 2005 年 1 月にかけて各政府機関の計画を査定、2005 年 4 月には下院政府改革委員会で、その結果を証言として報告している。GAO は以下の 3 点を中心に調査を実施した。

- 主な連邦機関が『必須機能』を確認、確証するために適当な方法をとったか。
- 各機関が GAO の 2002 年の調査以降、FPC 65 に述べられたガイダンスを遵守すべく、改善を行ったか。
- 各機関の COOP 計画が非常事態時のテレワーク導入に取り組んだか。
  （注：2003 年に連邦政府でのテレワーク使用に関して、連邦人材管理局（Office of Personnel Management=OPM）局長が議会で、「職員にプライベートと仕事のバランス配分に柔軟性を与えるだけでなく、テロリストによ

る脅威を含んだ職場の崩壊に対応できる基礎となる」と報告している。GAO も 2004 年に COOP 計画と実施において、テレワークが重要な選択肢となるとの報告をしている。）

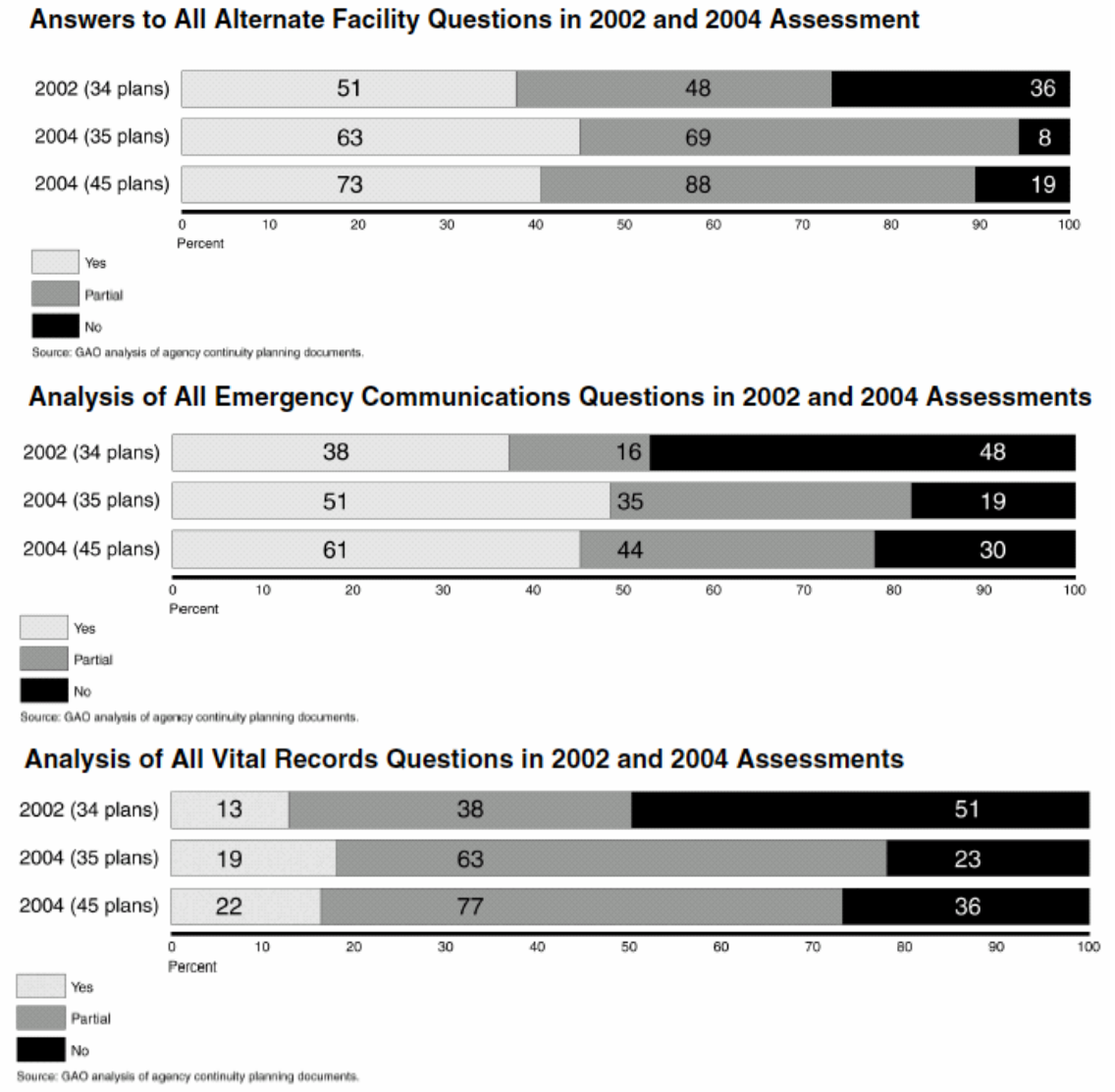
同調査の実施にあたり、GAO は各政府機関の状況を調査するにあたり、FPC 65 のガイダンスに関連する Yes/No または Partial（一部のみ Yes） の三択の質問票を作成し、それに対する回答を求めた。質問票には以下 8 つの項目ごとに 2～8 個の質問が含まれていた。

- 必須機能（essential functions）
- 計画及び手順
- （責任者不在などの際における）命令・指示の継続性
- 権限の委任
- 代替設備
- 緊急時通信手段の多重化
- 重要記録（の扱い・保存など）
- 試験、訓練、実験

その結果、調査対象となった機関の多くが、『必須機能』を確認、確証するために FPC 65 のガイダンスを採用しているとしているが、一方で、その実態を GAO が確認できるような十分な文書を用意できていなかったことが判明した。また、各機関が確認した『必須機能』の数は、3 から 538 まで大きく差があり、特に項目を多数上げた機関は、最重要項目だけではなく、重要性の低い機能までも含めていることなどの問題が明らかになった。

また、IT に関連する代替設備、緊急時通信手段の多重化、重要記録（の扱い・保存など）に対する回答について 2002 年と 2004 年の調査結果を比較したものが次の通りである（対象としたのは、2002 年が 22 の主要機関（省庁、重要な委員会）と配下の部門を含めた 34 機関。2004 年には、総数 45 機関。中段の 2004 (35 plans)は、2002 年に調査した機関に限った場合の結果を示す。1 機関増えているのは、DHS。実際には設問が複数あり、ここに出ているのは、すべての設問の答えを合計したもの。

GAO 調査結果例



また、2004 年 5 月時点の FEMA の継続計画ガイダンスは、テレワークに触れていないが、1 機関の継続計画は非常事態に対応して、テレワーク利用を計画していると示した。加えて 10 機関が COOP 発生時には、テレワークを利用することを計画していると報告したが、文書化はされていなかった

この状況について、GAO は、FEMA による不十分な監督が各機関における COOP 計画の弱点の原因となったとしている。FEMA は、今年後半に稼働開始を計画しているオンライン準備報告システムを使用して、監督を改善するとして、

すでに、機関横断的に実習を実施するなど、各機関が計画を立案し、さらにそれを改善することを援助する取り組みを始めている。

GAO は、最終的にその報告書で、国土安全保障担当大統領補佐官と国土安全保障長官に対し、各機関が非常事態に『必須機能』を提供し続けるために十分な準備ができていることを保証するため必要な事項として、以下 4 点を勧告している。

- 国土安全保障担当大統領補佐官は、現在進められている各機関の『必須機能』の確認と、連邦 COOP 政策の改良スケジュールを立てる。
- 国土安全保障長官は、各機関が『必須機能』を洗い出し、（長期的視野に立った）新たな COOP 計画ガイドラインを作成する一方で、その間に『必須事項』が中断せざるを得ない事態に対応するための短期的な戦略について準備しておくことを、各機関に指示する。
- 国土安全保障長官は、緊急準備即応次官に各機関の COOP 計画の監督に使用する報告データを検証する手順を作り、実施することを指示する。
- 国土安全保障長官は、緊急準備即応次官に、連邦人材管理局（Office of Personnel Management=OPM）のコンサルテーションのもと、COOP 発生時にテレワークを活用する準備をするために機関がとるべきステップに関してのガイダンスを作成するよう指示する。

③　ハリケーン・カトリーナ対応に関する議会公聴会（2006 年 3 月）

こうした GAO の勧告などによって、改善努力が求められてきた政府の COOP であったが、それが機能しないことを示す天災が発生する。2005 年 9 月に米国湾岸州を襲ったハリケーン・カトリーナは、米国の歴史上もっとも大きな自然災害の一つとなった。ハリケーン・カトリーナは米国の大災害に対する準備と対応能力に疑問を抱かせた。また、続いたハリケーン・リタが政府のすべてのレベルにおいて、緊迫した対応と復旧努力の需要を高めた。

この事態を重く見て、2006 年 3 月 8 日、上院国土安全保障・政府問題委員会は公聴会を開き、GAO、国土安全保障省を含んだ関係者、専門家の証言を求めた（ただし、この公聴会の中では、COOP 全般に対するものであり、IT に特化した指摘はなされていない）。

GAO は、非常に多くの人と時間をかけて、ハリケーン・カトリーナとリタに関連した準備、対応、復旧、再建の全フェーズの問題点を調査しており、現在も 40 近い調査活動を実施中であるが、こうした調査を基に公聴会で証言を行った。GAO は、1992 年にハリケーン・アンドリューが南フロリダを襲った時の連邦の対応を調査し、勧告を行っているが、ハリケーン・カトリーナが湾岸を襲う前に、必ずしもその勧告が実施されなかったことを指摘した。

この他、GAO は、主に以下の点などについてコメントした。

- ハリケーン・カトリーナの対応は、以下の 4 つの重要性を浮かび上がらせている。①大災害の前に、対応のための指揮官の役割、責任、権限を明確に定義し、伝達することの重要さ、②国家対応計画（National Response Plan=NRP）を機能させ、大災害へ適応する手順を明確化しておくことの重要さ、③しっかりした事前計画と十分な訓練、演習プログラムの重要さ、④大災害対応と、復旧能力の強力化の重要さである。

- ハリケーン・カトリーナ対応での FEMA のミッション実行能力を理由として、FEMA を解散させ、機能を他の機関に移すべきか、国家安全保障省内に残すべきか、あるいは FEMA として（従来のように）独立機関とすべきかなどといった、組織の位置づけに関する議論が持ち上がっている。しかし、それ以上に FEMA 指導者が、十分な経験、訓練、力量を持っているか否かを見極めて、任命することが、FEMA 自体の位置づけ以上に、FEMA のこれからの成功にとっては重要である。

- 連邦政府は、広範囲の物理的損害と経済的打撃を受けた湾岸地方の長期再建のパートナーとなる。再建における連邦の役割は、交通、健康管理インフラストラクチャと連邦施設などの分野で特に重要になる。長期再建は、どんな基準に基づいて、どこに、何が再建されるべきで、誰が何を負担し、意図した目的どおりに連邦資金が賢明に使われているかをどのように監視するかなど、世論の同意が必要な問題を多く抱えている。

GAO 以外からも専門家が公聴会に召喚され、DHS の対応について、以下のような証言をしている。

上院国土安全保障・政府問題委員会公聴会での証言

証言者	証言内容
Barbara A. Mikulski - U.S. Senator	・ FEMA は、大統領に対しての説明義務と直接パスを保証するために、独立機関に戻るべきである。 ・ 大統領は、専門知識をもった FEMA 長官を任命すべきである。 ・ 以前の改革時に学んだ事を参照するために、1990 年代の改革に関する報告書に再度目を通すべきである。
Bruce P. Baughman - President, National Emergency Management Association - Director, Alabama State Emergency Management Agency	・ FEMA は、その原因がなんであれ、災害対応において、連邦政府の機能を調整する機関であるべきだ。 ・ FEMA 長官は、大統領に直接の報告義務を持つべきである。 ・ 長官は、連邦、州、地方政府レベルで、緊急時管理、もしくはそれに似た仕事の経験があり、管理職レベルの管理経験、政府管理、予算配分の経験があり、人民の安全確保、災害準備、沈静、対応と復旧、指揮と監督などの理解があり、立法プロセスを理解し、権限を行使し、危機において決定を実行に移す実行力が発揮できる人物でなければならない。 ・ 国防総省は、あくまでも支援機関であるべきだ。 ・ 連邦政府は、第一対応者であってはならず、準備、緊急対応、能力維持、緊急事態発生時の特別リソース供給のため、より強力な資金提供に焦点を置くべきだ。 ・ NEMA を含む州、地方政府からの意見に耳を傾け、NRP を改訂すべきだ。 ・ FEMA に十分に人員を配置すべきだ。 ・ Robert T. Stafford Disaster Relief and Emergency Relief 法を改訂すべきだ。
Frank J. Cilluffo - Director, Homeland Security Policy Institute, The George Washington University	・ 国家準備対応システムは、最前線にある州、地方、非政府、民間セクター顧客を支援する最終的な力と成果に基づくべきである。システムは、持ち分を争うのでなく、協力と結合力で進められるべきである。 ・ 国土安全保障省を地域化することは、連邦政府の役割を適切な状況に置いておくという意味と、最残線に必要な力を持たせるという意味でも必要なことである。 ・ 準備は、個人とコミュニティから始まる。

Herman B. Leonard - John F. Kennedy School of Government and Harvard Business School	・ 災害からの損害を最小限に抑える最も良い機会は、まだ事前に防ぎ、鎮静化できる段階にある。可能なうちに、十分な保護を提供しなければならない。 ・ より効果的な対応を準備しなければならない。 ・ 対応能力の特定の弱点に注目しなければならない。 ・ DHS が、米国人の生活と危険に対抗する米国人を保護する展望を持った優れた組織となるよう、支援しなければならない。

こうした意見に対して、同公聴会には、国土安全保障省から Richard L. Skinner 連邦監察官も出席し、証言をしている。同氏は、FEMA は、批判の対象となっているが、ハリケーン・アンドリューから学んだ教訓に基づいて、いくつかの意義ある変更を採用し、ハリケーン・カトリーナの対応を改善することとなった。たとえば、1992 年に有効となった連邦緊急対応計画は、嵐の前に十分な資源を動かしたり、配置させたりできなかったが、ハリケーン・カトリーナに対して、FEMA は、湾岸地域の 16 ヶ所にこれまでの自然災害よりも多くの量の必要物資を事前配備することができたとしている。また、ESF-13（緊急事態支援機能: Emergency Support Function）に基づき、ルイジアナ州とミシシッピ州にいた 2,800 人以上の警官の仕事を調整する機能を果たした。さらに、ハリケーン・アンドリュー襲来時に、FEMA は、犠牲者が被害登録する場所を設置するのに苦労し、電話による登録への対処も非常に遅かったが、今回は、24 の移動センターをテキサス州、アラバマ州、ルイジアナ州、ミシシッピ州に設置し、電話回線も増やすことで迅速な対処を行ったとした。

しかしなら、次に例としてあげるように、ハリケーン・アンドリューの際に問題として認知されていたが、解決されていなかった問題も多くあり、それが今回の対応の遅れなどにも影響したとしている。

- 州、地方能力への期待：
  FEMA はこれまでと同様、州が打ちのめされ、連邦の援助を必要とするタイミングを見極めることができなかった。

- 連邦の指揮と監督：
  連邦の指揮と監督に混乱があり、遅れが生じたり、仕事が重複したりした。

- IT 利用の必要性：
  FEMA はいまだ、資産損失を証明するテクノロジーやデータを使いこなせていない。ハリケーン・アンドリュー時に、資産損害を見極める調査のプロセスが、不十分であることが証明された。FEMA 監視局は、災害が起こ

る前に、特に災害が頻繁に起こる地域における資産状況を管理するデータベースにアクセスできるようにしておくべきと勧告していた。しかし、13年たっても、FEMA はこの情報をフル活用していない。また、FEMA 監視局は、資産管理とその状況を示す統計を示す報告書作成を自動化すべきとしている。

(2) 国土安全保障省による企業支援活動：READY Business

Ready キャンペーンは、国土安全保障省とのパートナーシップで、公共広告機構（Ad Council）によって作成された国による一般向けサービス広告キャンペーンで、米国市民がテロリスト攻撃や、他の緊急事態に備え、対応できるよう教育し、能力を与えることを目的としている。

その中の *Ready Business* は、緊急事態に備えた計画作りや、準備の必要性をビジネス・コミュニティに認識させることを目的としている。*Ready Business* は「準備できている」という状態となるために、ビジネス・オーナーやマネージャーが取るべき処置をリストアップし、その導入のためのステップや、使いやすいテンプレートを提供することにより、ビジネス・オーナーの計画作りを支援している。*Ready Business* の勧告は、後述する米国防火協会によって作成された緊急事態準備と業務継続性標準（Emergency Preparedness and Business Continuity Standard: NFPA）を反映している。

キャンペーンはビジネス・オーナーやマネージャーに①業務継続を計画し、②従業員と話をし、③投資を守るように働きかけている。それぞれのステップで、どのような準備をすべきかを、リストアップしている。

READY Business キャンペーンで掲げられている項目リスト

ステップ	準備
1. 業務継続を計画する (Plan to Stay in Business)	・ 情報収集する ・ 継続計画をたてる ・ 緊急事態計画をたてる ・ 緊急時用たくわえを準備する ・ 避難場所を確認する ・ 防火対策を確認する ・ 緊急医療事態に備える
2. 従業員と話す (Talk to Your People)	・ 仕事仲間を巻き込む ・ 計画を訓練にうつす ・ 準備を啓蒙する

	・ 緊急時通信計画をたてる ・ 従業員健康を守る
3. 投資を守る (Protect Your Investment)	・ 保険適用範囲を確認する ・ ユーティリティ崩壊に備える ・ 施設、建物、工場をまもる ・ 機器を守る ・ 建物の空気の安全を確認する ・ サイバー・セキュリティを強化する

(3) GSA による州政府向けガイドライン：Information on the Intergovernmental Advisory Board (IAB)

一般調達局(General Service Administration=GSA)に設置されている、政府間顧問委員会（Intergovernmental Advisory Board=IAB）は、連邦、州、地方政府の政府間の IT 問題についての知識と理解を広め、IT 政府間問題に関して American Council for Technology（ACT）に助言とガイダンスを提供することをミッションとしている。

ACT とは、1979 年に設立されたインフォメーショ・テクノロジー資源を効果的、能率的に獲得、利用することにおいて、政府に助言する非営利教育機構である。国内の政府 IT コミュニティ組織間、政府と業界間、政府組織と中央の規制、監督機関間の専門的なコミュニケーションを容易にし、促進することを目的としている。

IAB は毎年、IT 関連の報告書を作成し、ACT に提出しており、2004 年には、業務継続に関して”Business Continuity: It’s Not Just an IT Recovery Plan : Intergovernmental and Enterprise Approaches”を作成した。同報告書には、以下の内容が含まれている。

IAB による 2004 年報告書の主な概要

①政府とビジネスは、業務継続性計画に関し、企業的アプローチを取り始めている。	
	▪ 災害復旧と業務継続に関する法律、規制、業界標準の整備は、政府やビジネスの業務継続性の優先度を上げる結果に結びついた。 ▪ 企業的アプローチが成功するためには、災害に対応し、業務を再開するために必要な情報とデータが組織全体に利用可能状態となっていることが必須である。 ▪ システムが企業全体を支えるようになるにつれ、政府は、組織全体におよぶ影響やリスクを考慮せざるを得なくなる。

②計画段階で、政府間や民間セクター・パートナーを業務継続に巻き混むことは、政府に重要な相互依存と資源、施設の共用を可能とすることにつながる。

- 協力は、民間と政府間パートナーを含むべきである。政府は特に計画、バックアップ、代替施設などにかける資源を持たない小規模ビジネスが業務を継続できるよう、主たる役割を果たすことができる。
- 機関やビジネスは、第一レベルの応答者と交わり、協力する方法を知っていなければならない。多くの地方政府は、施設の損害を査定し、復旧プロセスを開始するために、災害時に緊急事態ゾーンにビジネス関係者がアクセスすることを許可する計画を作っている。
- 協力は、災害時に行政管轄体が資源や、施設を共有するのを助ける。
- 協力は、一次連絡先と連絡が取れない場合、業務を展開するために、明確に定義され役割、継承計画、正式の連絡係とバックアップを必要とする。
- 他組織、政府、ビジネスとの相互依存性を知っておかなければならない。
- パートナーは計画段階から巻き込まれるべきである。

③災害対応と緊急時サービスに加えて、日々の業務を再開することと、政府の継続は、業務継続計画の主要素となるべきである。

- 崩壊の影響を未然に防ぐ、もしくは低く抑えるために、さきを見越した対策を取ることは、稼働維持には重要である。対策には、バックアップ戦略や詳細なリスク解析などが含まれる。
- 重要なインフラストラクチャに依存しているものをすべて抑えておかなければならない。バックアップ施設やシステムの地理的多様性は、ある一地点の重要なインフラストラクチャが使用不可能となった時の影響を抑えることができる。
- どのアプリケーションがもっとも重要かを知っておき、それを一番に回復しなければならない。
- エンドユーザーレベルの復旧、再開に焦点をあてなければならない。
- 計画にはテストが必須である。

④政府の多くの人間が、業務継続は、IT オフィスの管轄であるととらえている。事が起これば、システムが停止し、IT ショップがシステムの復旧を行い、ビジネスは継続される。しかしながら、企業全体が IT に頼っているのだから、ビジネス継続は本来は、経営陣を含む組織に所属する全員の関心事であるべきだ。ビジネス継続の企業的視点は、システムを守り、リスクと脆弱さを理解し、崩壊の影響を減らすことにおいて、非常に重要である。それはまた、インフラストラクチャへのアクセスなしに重要なサービスを提供し、ミッションを達成するという、最悪のシナリオを考えることを強いることにもなる。

同報告書では、これに取り組んでいる政府の例を挙げている。たとえば、2002 年の National Association of State CIO のビジネス継続・インフォメーション・セキュリティ部門で賞を受けたノース・カロライナ州が挙げられる。また 2003 年に同賞を受賞している Secure Michigan Initiative というミシガン州のインフォメーション・テクノロジー部門のプロジェクトについても触れられている。

2. 州政府による取り組み

連邦政府だけではなく、州政府や、地方政府も緊急事態に備えて、自らの緊急事態対応計画を作成したり、地元のビジネスに対しての計画作成支援を行っている。以下は、その取り組み例として、（１）ワシントン DC、（２）テキサス州、（３）フロリダ州 Delray Beach 市、（４）南・北カロライナ州における活動を紹介する。

州政府、地方政府の BCP

	地方政府自体のBCP	管轄する地域のビジネス・住民のBCP
（１）ワシントン DC	・ ワシントン DC、District of Columbia Emergency Management Agency（DCEMA）によるビジネスと産業緊急事態管理計画	・ ワシントン DC、DCEMP によるビジネスと産業緊急事態管理計画（前半） ・ DCEMP 作成のコミュニティ向け机上練習問題 ・ Community Emergency Management Plan（CEMP）
（２）テキサス州	・ テキサス州 DIR の業務継続計画作成ガイドライン ・ テキサス州 DIR の Practices for Protecting Information Resources Assets	

（３）フロリダ州 Delray Beach 市	・フロリダ州 Delray Beach 市 MIS の Enterprise Technology Plan	
（４）南北カロライナ州		・南北カロライナ州の Contingency Planning Association of the Carolinas（CPAC）

(1)　ワシントンDC：DC Business and Industry Emergency Management Plan

ワシントンDCでは、DCEMA （District of Columbia Emergency Management Agency）が、緊急事態や災害に対する対応を調整・支援している。DCEMAのミッションは、人命や資産の損失を最小限に抑え、最高水準の緊急事態管理インフラストラクチャを運用、維持することにより、危険から市民と機関を守ることにある。DCEMAは以下の活動を通じて、ミッションを達成するとしている。

- あらゆる緊急事態や災害に対して、緊急対応・復旧活動ができることを保証する計画・手順を作成する。
- 緊急事態や災害発生時の、緊急物資の調整を行う。
- 緊急事態の第一対応者、市の職員、一般市民を訓練する。
- 緊急事態に備えた実習を行う。
- （緊急事態以外においても）あらゆる特別イベントや、それに関連して必要となる道路閉鎖などを調整する。

DCEMA は、BCP/DR に関して、主として以下３つのような取り組みを行っている。

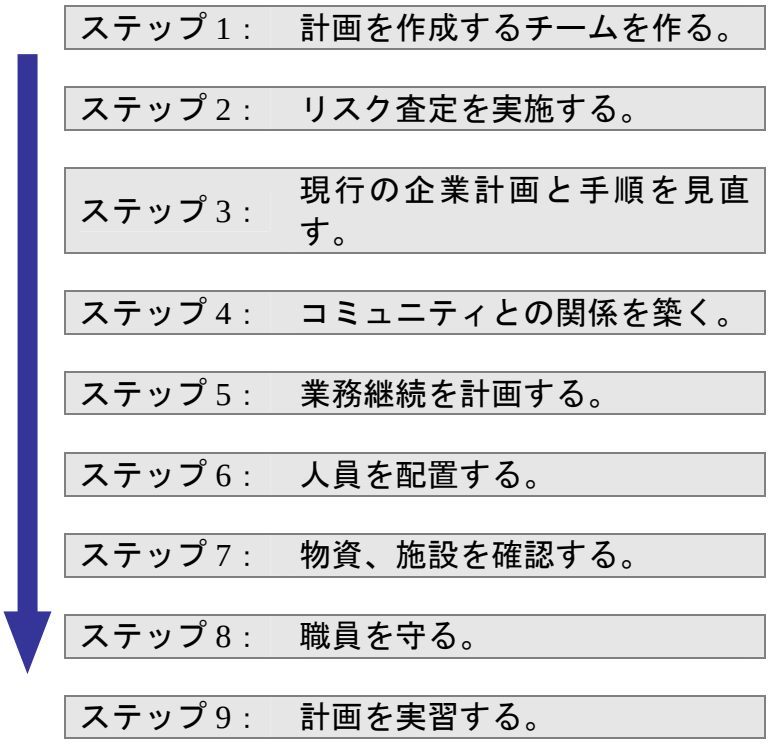
①　DC Business and Industry Emergency Management Plan=BIEMP

DC ビジネスと産業緊急事態管理計画（DC Business and Industry Emergency Management Plan=BIEMP）は、重要な緊急事態管理概念と、地元での緊急時対応がどのようになされるのかをビジネスや産業に理解してもらうために、DCEMA がスポンサーとなり作成された。

BIEMP は、大きく 2 つの部分から構成されており、前半では、あらゆるタイプの緊急事態に対するさまざまな規模のビジネスの緊急事態計画フレームワークを提示している。BIEMP は、以下の 9 ステップを緊急事態管理計画作成の際には考

慮すべきだとしている。特にこの BIEMP の前半部分は、政府機関だけではなく、DC にある民間組織が自身の緊急時計画を作成する際のモデルとして利用することもできるとしている。

BIEMP の緊急事態計画フレームワークの 9 ステップ



後半では、ワシントン DC と連邦政府がどのように緊急事態を管理するのかが記述されている。ワシントン DC は、District Response Plan（DR）を作成しており、ワシントン DC がさまざまな危機に対応する準備をしている。DR は、能力、スキル、物資、権限などで DC 政府内をグルーピングすることにより、機能的な対応組織を構成している。これにより、DR は、資源がどのように投入され、使用され、必要であれば、どのように連邦や地方のパートナーが支援に携わるのかのアウトラインを提示している。

② Community Emergency Management Plan（CEMP）

また、ワシントン DC 政府では、各々のコミュニティに Emergency Preparedness Committee（EPC）を設立し、Community Emergency Management Plan（CEMP）の更新と実習を奨励している。CEMP は、DCEMA 主催の緊急事態管理計画と訓練会議に参加した、ワシントン DC 住民の共同作業で作成された。EPC は、コミュニ

ティと近隣のボランティアを、災害時に組織だったパートナーにまとめあげ、緊急事態発生時の対応を迅速に行うことを目指している。

(2)　テキサス州：BCP ガイドライン

テキサス州では、Department of Information Resources（DIR）の IT セキュリティ部門で、テキサス州政府のための、継続性と緊急時対応計画を扱っている。Information Resources Asset Protection Council（IRAPC）は、州機関と大学がお互いに協力し、情報共有することによって、緊急事態が発生した際の資産保守をどのように行うかについて取り組むフォーラムであった。1997 年に、10 以上の機関と大学の代表が特別 IRAPC チームを作り、業務継続計画作成ガイドライン作りを始めた。DIR は、1997 年にこのチームにより持ち込まれたガイドラインを、州の業務継続計画作成ガイドラインとして発行している。

テキサス州業務継続計画作成ガイドラインの章立て

序章
①範囲と準備度合いを判断する ▪ 業務復旧計画作成を始めるためには、どのような情報が必要なのか。 ▪ どうやってこの情報をベースに計画の範囲を決定するのか。
②業務回復責任 ▪ 計画作成活動においての役割と責任。
③分析と戦略選択 ▪ 影響分析は、崩壊や、災害が起こった場合、機関が何を失う可能性があるのかを詳細に理解することを伴う。 ▪ 影響度合いが計画作成の方向、範囲と、適切な復旧の戦略の主要考慮点となる。復旧計画作りに大事なことは、実際の災害が起きた時に復旧作業を行う人により作成されることである。
④業務継続性テスト ▪ テストは、合格・不合格を決めるためにするのではなく、計画上の改訂が必要な箇所を見つけ出すためにある。
⑤まとめ ▪ 本当の供給停止を含んだ、総合的で、現実的なテスト状況下で、望まれた結果を生み出す上出来の継続計画は、技術面や、ある特殊プロセスからでなく、業務面で構成されたものである。 ▪ 継続計画作成は、経営陣の注目とガイダンスが必要なビジネス・プロセスである。

ガイドラインには、Appendix として、多くのチェックリスト、質問集、計画などのサンプルが記載されている。

また DIR は、Practices for Protecting Information Resources Assets というガイドラインも出している。このガイドラインは、インフォメーション・セキュリティ・リスク管理プログラムを確立、維持し、同時に、その活動を通じて、州の掲げる情報セキュリティ標準を満たそうとする州政府機関と州立の高等教育機関を支援する目的で書かれている。同ガイドラインは、情報保護の専門家や、計画立案者が、州政府や高等教育関連機関が緊急事態への対応に際して、必要となる事項を適切に判断できよう、参照、例、図、テンプレートなどのリスク管理への様々なアプローチを紹介している。また、第 3 章の「重要情報資産保護のためのツールと演習」では、環境管理システムの故障などとともに、悪天候などの自然災害に関する事項にも触れている。

(3) フロリダ州 Delray Beach 市：CITY OF DELRAY BEACH: ENTERPRISE TECHNOLOGY PLAN

フロリダ州 Delray Beach 市では、財務課の Management Information Systems（MIS）部門が年次指導部目標設定会議で市政府機関及びそのスタッフの掲げた市の目標に焦点を合わせ、MIS Enterprise Technology Plan for FY 2005-2009 を作成した。この計画書は、4 つの個別の項目から成っているが、その第 3 項目として、MIS 業務中断/業務継続計画と称し、BCP に特化した項を設けている。

MIS Enterprise Technology Plan for FY 2005-2009 の主な概要

項目	概要
①MIS 戦略計画	この計画は、MIS の内部ガイド、もしくは地図に値する。将来 MIS 部門がどのように成るべきかを定義し、その目標を宣言し、職員に求めるものは何かを明らかにし、どうやってミッションを達成するつもりであるかを宣言する声明文である。
②MIS 戦術計画	この計画では、MIS の職員が、毎年、組織、施設、機器、ハードウェア、ソフトウェア、通信、サービス、緊急時対応計画、新技術などの MIS インフラストラクチャ全体を調査することを義務づけている。この詳細調査は、現状を確認し、ユーザ・ライセンス、サーバ・ライセンス、メンテナンス契約などが更新されていることを保証し、問題を確認し、サービス・ボトルネックを明らかにし、新たにわか

	ったことを発表し、問題を解決し、全体の運用を改善するという勧告を出すことにつながる。
③MIS 業務中断/業務継続計画	MIS のハードウェア、インフラストラクチャ、ソフトウェア・システム、データ・ファイルがシステムのすべての顧客とユーザーの満足のいくように、適切な時間内に復旧できるように、物理的に守られていることを保証するために、業務中断計画と業務継続計画を文書化することを目的としている（後述）。
④MIS プロジェクト作業計画	MIS では、細かい作業に分けられた会計年度内に達成されなければならないプロジェクトの年間スケジュールを準備している。このスケジュールは、また、MIS 部門でのスケジュールされていた作業と、スケジュール外作業をモニターする管理ツールとしても使用されている。

同計画書の「③MIS 業務中断/業務継続計画」によれば、同市では、短期中断と長期中断とに分けてシステム導入や災害時対応計画を行っている。

まず、同市では、主に停電や、機器の故障などに起因する短期業務中断の可能性をできるかぎり抑えられるようにシステムを設計しているとしている。具体的には、フォールト・トレラントな、システムを提供するために、システム二重化などの対策がすでに取られており、加えて新たな対応も検討されているとしている。

一方、市役所と警察署のコンピューター・オペレーション・センターを破壊するような災害は、長期業務中断につながる。最悪のシナリオで、両機関の施設が使用不可能となることを想定し、長期業務継続計画は、このようなタイプの災害の後、どのように市が運営を再開するかに着目したものとなっている。長期業務計画には、以下の項目が含まれている。

- 運営再開に向け、指名された復旧チームと文書化された優先度リストを作る。
- 災害地での職員の安全を確保する。
- 災害地を固め、被害をうけていない資産を守る。
- 損害、復旧努力を行っている適切な人間に連絡を取る。
- 被害状況の詳細記録を残す。
- すべての電話会話、書き物によるやりとり、口頭の会話、被害・復旧費用の記録を残す。
- 被害をうけた機器と受けていないものを分ける。
- その他の具体的な機器に対する指示を示す。

(4) 南北カロライナ州：緊急時対応計画委員会 Contingency Planning Association of the Carolinas (CPAC)

南北カロライナ州緊急時対応計画委員会（Contingency Planning Association of the Carolinas =CPAC）は、サウス・カロライナ州及びノース・カロライナ州で緊急時対応計画に関する情報、資産を共有し、両州に災害復旧計画や継続計画との必要性を広めようとしているグループである。メンバーシップは、このグループに貢献できる、もしくは、このグループから得るものがあると考える個人、組織に広くオープンとなっている。

CPAC は、組織運営に影響を及ぼす計画外の中断発生後の業務再開に向け、先を見越した準備を行うことを支援するため、業務継続計画や災害復旧の分野で、意見、情報交換を必要とする地方、州、連邦政府、ビジネス・コミュニティ、個人が参加できるフォーラムを運営している。CPAC に参加するメンバーは、政府職員のほか、大学の専門家、電気・ガスなどの公共サービス、金融、保険、製造、小売、医療、電気通信などの業界関係者及び、DR サービス・ベンダ関係者などとなっている。これにより災害復旧時に政府機関と民間ビジネス間の効果的なコミュニケーションの改善が期待できる。また、CPAC は、ビジネス、政府、個人に共通の問題を認識させ、決議を提案し、過去の経験から学んだ教訓を共有することにより緊急時対応計画のもつ価値を認識させようとしている。CPAC はまた、効果的な緊急時対応計画と災害復旧をより容易にするベンダー紹介もしている。

CPAC は年次総会以外にも、年数回会議を主催している。ここ 3 年間の総会のテーマは

- 危機、脅威、戦術、メディアの管理　（Managing the Crisis: Threats, Media, and Tactics）
- 業務再開　（Getting back in Business）
- 職場での脅威と業務継続　（Workforce Threats & Business Continuity）
- 机上 SARS 大発生演習　（Mock Tabletop Exercise Dealing with a Major SARS Outbreak）

であった。また、CPAC メンバーは、基本的にはノース・カロライナ州政府とサウス・カロライナ州政府が提供している無料の緊急事態管理訓練クラスに参加できる。以下のようなクラスが提供されている。

- テロの認識
- 緊急事態対応者用 米国危機管理システム（National Incident Management System : NIMS）・災害事故指令システム（Incident Command System : ICS）

- 災害援助ワークショップ
- 捜索と救助の基礎
- 災害からの復旧

3. 重要インフラに関連した民間の取り組み

(1) 証券業界

① 証券会社における BCP/DR

米国証券業協会（National Association of Securities Dealers=NASD）は、2002 年 8 月 7 日に米国証券取引委員会（Securities Exchange Commission=SEC）に対して、すべての証券会社に BCP の作成・実施を求める Rule 3510 を提出した。同年 8 月 30 日には、ニューヨーク証券取引所（New York Stock Exchange=NYSE）も、NASD とほぼ同じ内容の Rule 446 を SEC に提出した。SEC はこれらを 2004 年 4 月 7 日に承認している。

NASD Rule 3510 と NYSE Rule 446 は、証券会社が、大きな業務上の混乱が発生した場合にも、顧客に対する義務を全うできるよう、無理のない業務継続計画作成を要請している。ここでの義務とは、大事が発生した際でも、顧客が所有するファンドや証券にアクセスできるようにすることを指しており、必ずしも取引活動の再開を意味するものではない。Rule 3510 と Rule 446 は、業務継続計画が以下の 10 の主要要素を含むことを義務づけている。

BCP に含まれるべき主要要素

要素	備考
① データ・バックアップと復旧（ハード・コピーと電子版）	SEC や NASD の規則や、具体的に記録の保持義務に関して記述している資料にそって、証券会社がどの記録を保持しなければならないかを判断する。
② ミッション・クリティカル・システム	注文受付、注文入力、実行、比較、配分、手じまい、証券取引の決済、顧客アカウントのメンテナンス、顧客アカウントへのアクセス、ファンドと証券の引き渡しなどを含んだ、証券取引の迅速で、正確な処理を保証するのに必要なシステムをミッション・クリティカル・システ

	ムという。
③　財務と運営査定	証券会社は、その運営、財務、信用リスク・エクスポージャーに変化があったことを確認するための文書化された手順を準備しなければならない。
④　顧客と証券会社間の代替コミュニケーション	ー
⑤　証券会社とその従業員間の代替コミュニケーション	ー
⑥　従業員の物理的な代替所在場所	ー
⑦　重要な組織、銀行、関係グループへの影響	大きな業務上の混乱が重要な業務関係のある組織、銀行、関係するブローカー、ディーラー、企業顧客などに及ぼす影響を確認する手順を持たなければならない
⑧　規制に対する報告	ー
⑨　規制機関とのコミュニケーション	ー
⑩　顧客のファンドや証券へのアクセス	ー

NASD と NYSE が、各証券会社について、上記の 10 要素が遵守されているかを確認する。証券会社が、上記 10 要素のうち自社に該当しない要素だと判断する場合は、それを除く理由の審査を NASD、NYSE から受けなければならない。さらに、各社の BCP は、証券会社の経営幹部メンバーにより承認されなければならず、毎年、更新されなければならないとされている。

また、Rule 3510 と Rule 446 では、clearing firm と呼ばれる受託先証券会社に、ミッション・クリティカルなシステムの面で依存している場合についても規定している。introducing firm と呼ばれる委託元の証券会社が、受託先証券会社に対して、このようなシステムを依存しているということは、これらの Rule で遵守を求められている特定の要素について、そのコンプライアンスを他社に依存する形になる。そのため、Rule 3510 と Rule 446 は、委託元会社と受託会社間の規定遵守に関する責任切り分けなど、両社の関係を示す説明を文書によって行うことを求めている。ただし、外部に委託する証券会社は、ミッション・クリティカル・システムを受託する証券会社に依存しているからといって、規定遵守の目的で受託契約を変更する必要はないとされている。

NASD Rule 3510 と NYSE 446 では、こうした各社の BCP だけではなく、証券業界として、連携して緊急事態に対応できるよう、証券会社各社に、重大な業務混乱が発生した際に、NASD や NYSE が連絡できる緊急時連絡係を指名することを要請している。NASD Rule は 2 人の指名を要請しており、NYSE は 1 人としている。連絡係、連絡先などが変更になった場合、随時 NASD と NYSE に知らせなければならないとしている。

NYSE メンバーである証券会社は、2004 年 8 月 5 日までに BCP を作成し、連絡係を NYSE に通知することとされた。一方、NASD は、受託する証券会社には計画を 2004 年 8 月 11 日までに作成するように要請し、委託する証券会社には、2004 年 9 月 10 日を期日と設定した。また、受託、委託どちらの証券会社も、2004 年 6 月 14 日までに連絡係を NASD に登録しなければならないと定められている。

② 証券取引所における BCP/DR

証券会社に対する緊急事態対応計画だけではなく、証券取引所自らの対応計画も進められている。2003 年 9 月に、SEC は、NYSE、Nasdaq 株式市場、地方株式取引所、オプション取引所、電子コミュニケーション・ネットワークを含む証券取引を行う組織が遵守しなければならない業務継続原則を発表した。この原則は、

- 大規模混乱後、遅くとも翌日には、取引を再開すると想定した業務継続計画を作成する
- 一次サイトとバックアップ・サイトを地理的相違点の多い場所に置く
- 市場データ収集や、開示システム（dissemination systems）のような重要共有情報システムの完全な回復を保証する
- 大規模混乱からの復旧の際のバックアップ有効性をテストする

という内容を含んでいる。この原則にある業務継続計画を遅くとも 2004 年末には準備し終えていなければならないとしている。

こうした復旧目標を決めるとともに、SEC は、大災害が発生した後、取引のために十分な場所が確保できるよう追加アクションを取った。SEC 担当者は、NYSE と NASDAQ の 1 取引フロアが使用できなくなったら、他フロアで取引ができるように準備するよう要請した。どちらの市場関係者も、他市場の証券を取り扱えるよう、システムを変更し、証券会社の能力をテストしたとしている。また万一、NYSE と NASDAQ どちらもが取引を再開できなかったら、電子コミュニケーション・ネットワークと地方取引所が通常これらの市場で取り扱われている株の取引を続行できなければならないとしている。SEC は、電子コミュニケーション・ネ

ットワーク関係者との議論と、調査の結果から、電子コミュニケーション・ネットワークと地方取引所は、相当量の追加取引を行うことができると判断している。

しかしながら、2004 年に金融市場の緊急事態に備えての準備度を調査した GAO は、SEC は、証券市場での取引が、大規模災害後の迅速な再開を保証するような、総合的な査定をしきれていないと批判している。また SEC が、大災害後にどれくらいの証券会社が業務を再開できるのかの調査をしていないことについても、疑問を呈しているとした。尚、GAO によれば、連邦金融行政官は、市場に通常取引と受託取引を 1 営業日以内に再開することを期待しており、財務省の重要インフラストラクチャ保護プログラム担当者は、市場が長期に亘って閉じることはないと保証することは、大災害に伴う不安定な時期に投資家の信頼を得るために大切であるとしている。

(2) 医療業界

医療業界は、「医療保険の携行性と責任に関する法律（Health Insurance Portability and Accountability Act=HIPAA）」の制定により、BCP と DR をすべての医療機関で準備することが義務付けられている。

HIPAA は、1986 年の Internal Revenue Service Code を修正したもので、1996 年 8 月 21 日に制定され、Kennedy-Kassebaum 法とも呼ばれている。この法律は、医療組織における管理の簡素化（Administrative Simplification）を謳っており、

- 標準電子データ相互交換により、健康管理の能率を改善する
- 標準を設け、守らせることにより、健康状態データのセキュリティと安全を守る

ことを要請している。より具体的には、HIPAA は、米国保険福祉省（Department of Health and Human Services=HHS）に以下を保証する規則を作成するよう求めた。

- 患者の健康状態、事務、会計などに関する電子データの標準化
- 個人、職員、健康計画、健康ケア提供者それぞれに対する健康 ID 付与
- 過去、現在、未来の個人特定可能な健康状態情報の機密と完全性を守るセキュリティ標準

HIPAA は大きく分けて、①電子トランザクションの標準、②ユニーク ID 標準、③セキュリティ規則、④プライバシー規則の 4 パートからなり、それぞれについて、HHS が公布した詳細な規則がある。BCP/DR に関連するのは、このうち③セキュリティ規則である。同規則は、電子的に保管されていたり、送られたりする

個人に関する全ての健康状態情報に、均一なセキュリティ保護を提供するものと位置づけられている。

HIPAA セキュリティ規則は、関連医療機関が作成、受信、維持、伝達する電子保護健康状態情報（ePHI）のセキュリティ、完全性、可用性（availability）を保証することを要請している。また医療機関にある程度予測可能な脅威や危険から、ePHI のセキュリティと完全性を守ること、プライバシー規則で許可されていない、もしくは必要がないとされている情報を予測可能な利用や開示から守ること、職員による法遵守の保証を要請している。防御には、適切な方針と手順の適用、ePHI への物理的アクセスの保護、ネットワーク、コンピュータ、その他の電子機器への技術的セキュリティ対策の適用が含まれる。セキュリティ標準には、拡張性が持たせてあり、特定のテクノロジーの使用を義務づけていない。医療機関は、完全なセキュリティ査定とリスク分析の結果選ばれたソリューションであれば、医療機関の運営にふさわしいものを選択することができるとしている。

同キュリティ規則は、1998 年 8 月のドラフト版以来、4 年以上をかけて作られた。最終標準は、2003 年 2 月 20 日に公布され、2003 年 4 月 21 日に施行となった。関係医療機関は、2005 年 4 月 21 日までの 2 年間で同標準に従うことが求められた。

緊急時対応計画作成に関する標準は、セキュリティ規則の管理保証規約に含まれている。それは、医療機関に対して、ePHI を保持するシステムに損害を与える緊急事態（火事、破壊行為、システム障害、自然災害）に対応するための方針と手順を確立することを要請している。主な項目は以下の通り。

① データ・バックアップ計画（必須） - ePHI の完全コピーを作成、維持する手順を確立し、運用する。
② 災害復旧計画（必須） - データの欠損を修復する手順を確立し、必要に応じて実行に移す。
③ 緊急時モード運営計画（必須） - 緊急時モードで運営しながらも ePHI のセキュリティを守るための重要業務プロセスを継続する手順を確立し、必要に応じて実行に移す。
④ テストと更新手順（推奨） - 定期的なテストと緊急時対応計画の更新の手順を運用する。
⑤ アプリケーションとデータの重要度分析（推奨） - 他の緊急時対応計画構成要素と比較して特定のアプリケーションとデータの相対的重要度を分析する。

(3)　防火業界

米国防火協会（National Fire Protection Association=NFPA）は、1896 年に設立された国際非営利会員制組織で、現在、100 ヶ国と 320 企業の社員を含む 75,000 人を会員に持つ。NFPA は世界をリードする防火の代弁人で、公衆の安全の権威である。NFPA が作成した 300 の規約と標準は、米国内のすべての建物、プロセス、サービス、設計、設置に影響を与えている。6,000 人以上の様々な専門バックグラウンドのボランティアが、230 の技術規約作成委員会や、標準作成委員会に所属し、規約作成に取り組んでいる。NFPA のミッションは、規約、標準、研究、訓練、教育を供給、擁護することにより、火事やその他の危険が原因の負担を減少させることである。

NFPA が作成した BCP ガイドライン NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs は、FEMA、the National Emergency Management Association、the International Association for Emergency Managers などによって承認されている。同ガイドラインの目的は、災害や緊急事態管理と業務継続計画の責任者が、現行の計画を査定し、その結果から、さらに災害や緊急事態の影響を減らし、事態が発生した場合は、そこから速やかに復旧できるような計画を作成、運用、維持するための基準を提供することにある。同ガイドラインは、公的機関だけではなく、民間企業・団体などにも適用可能となっている。

ガイドラインの目的の記述や、用語説明を除くと、実際の内容は第 4 章「計画管理」と第 5 章「計画要素」に書かれており、以下のような構成となっている。

NFPA 1600 の章立て

第 1 章　基本方針　（Administration）	
第 2 章　参照文献　（Referenced Publications）	
第 3 章　用語定義　（Definitions）	
第 4 章　計画管理　（Program Management）	
	・計画基本方針　（Program Administration） ・計画調整者　（Program Coordinator） ・顧問委員会　（Advisory Committee） ・計画評価　（Program Evaluation）
第 5 章　計画要素　（Program Elements）	
	・序説　（General） ・法と権威　（Law and Authorities） ・危険確認、リスク査定、影響分析　（Hazard Identification, Risk Assessment, and Impact Analysis）

- 危険抑制　（Hazard Mitigation）
- 資源管理　（Resource Management）
- 相互扶助　（Mutual Aid）
- 計画作成　（Planning）
- 指揮、管理、調整　（Direction, Control, and Coordination）
- 通信、警告　（Communication and Warning）
- 運用、手順　（Operations and Procedures）
- 物流、施設　（Logistics and Facilities）
- 訓練　（Training）
- 演習、評価、修正　（Exercises, Evaluations, and Corrective Actions）
- 危機通信、大衆向け情報　（Crisis Communication and Public Information）
- 財政、事務　（Finance and Adminisration）

NFPA では、NFPA 1600 に関するワークショップやセミナーも開催している。

NFPA のワークショップ/セミナー

ワークショップ/セミナー	内容
Business Continuity Planning 1-day Seminar	米国議会、American National Standards Institute (ANSI)、the 9-11 Commission、HHS に承認を受けた NFPA 1600 を紹介する。
Executive Forum (NFPA 1600) 1-day Seminar	BCP を作成、改善するために NFPA 1600 の主要要素を説明。
Auditing and Assessment (NFPA 1600) 1-day Seminar	BCP の監査、査定方法に焦点をあてる。
NFPA 1600 2-day Workshop	上記 2 セミナーを 1 ワークショップとしたもの。

（参考資料）

http://www.fas.org/irp/offdocs/pdd/fpc-65.htm
http://www.orau.gov/emi/events/2005%20Meeting/presentations/Session%203Akiell-Handout7.pdf
http://www.gao.gov/new.items/d05577.pdf
http://www.fema.gov/txt/government/coop/fpc65_0604.txt
http://www.senate.gov/~gov_affairs/index.cfm?Fuseaction=Hearings.Detail&HearingID=330
http://hsgac.senate.gov/_files/030806Walker.pdf
http://www.ready.gov/business/index.html
http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=8203&channelPage=%2Fep%2Fchannel%2FgsaOverview.jsp&channelId=-13228
http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/citizens1_R2-fG1-e_0Z5RDZ-i34K-pR.pdf
http://www.nascio.org/
http://www.nascio.org/awards/2002awards/security.cfm
http://www.nascio.org/awards/2003awards/security.cfm
http://dcema.dc.gov/dcema/site/default.asp?dcemaNav=|31806|
http://dcema.dc.gov/dcema/cwp/view,a,1226,q,568249.asp
http://dcema.dc.gov/dcema/cwp/view,A,1226,Q,621456.asp
http://www.dir.state.tx.us/index.htm
http://www.dir.state.tx.us/IRAPC/bcpg/bcpg.pdf
http://www.dir.state.tx.us/IRAPC/practices/pdf/practices-pt1.pdf
http://www.icma.org/upload/library/2005-08/{57AB309E-4102-40F2-9DF5-E76F8D2192C2}.pdf
http://www.cpaccarolinas.org/
http://www.omm.com/webdata/content/publications/client_alert_financial_services_2004_05_06.htm
http://www.house.gov/commerce_democrats/press/d04984.pdf
http://www.hipaadvisory.com/regs/HIPAAprimer.htm
http://www.hipaadvisory.com/regs/finalsecurity/summaryanalysis.htm
http://www.hipaadvisory.com/regs/finalsecurity/regulationtext.htm#appendix
http://www.nfpa.org/
http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf

このレポートに対するご質問、ご意見、ご要望がありましたら、
hiroyoshi_watanabe@jetro.go.jpまでお願いします。