2006 年 5 月 15 日

NIST SP800 シリーズに見る情報セキュリティと事業継続計画

IPA セキュリティセンター　菅野泰子

1. はじめに

2004 年、2005 年は、世界的に大規模な自然災害が相次いだ年であった。日本は世界有数の地震国であり、かつ火山の噴火、相次ぐ大型台風、大雪による被害等、災害の爪あとが消える間もなく次々と大規模災害に見舞われている。このような社会情勢を受けてか、2005 年 3 月に、経済産業省より「事業継続策定ガイドライン」が発表され、2005 年 8 月に内閣府中央防災会議より「事業継続ガイドライン第一版」が発表されると、事業継続管理・事業継続計画に対して大きな関心が寄せられるようになった。なお、2005 年 10 月には、内閣府の「事業継続ガイドライン」の理解を助ける補足資料として「事業継続計画の文書構成モデル例 第一版」が発表され、2006 年 2 月には、中小企業庁より「中小企業 BCP[1]策定運用指針」が入門診断、BCP 策定のための様々なテンプレート、実際の策定例とともに発表されている。これらのガイドラインに共通するのは、事業継続計画への取組みをできるところからスタートさせることが重要であると呼びかけ、そのための枠組みや具体例を提示している点である。とりわけ、中小企業庁の指針や文書類は、中小企業が投入できる時間と労力に応じ、その企業なりの BCP が策定できるように細やかな配慮がなされている。

さて、経済産業省と内閣府から時期をほぼ同じくして出された事業継続策定ガイドラインは、BCP の基本的考え方や事業継続計画策定の枠組み設定に大きな違いは無い。また、両者ともその基本部分は、BCP の国際標準策定の動きを睨みながら、欧米の主要な BCP/BCM[2]ガイドラインの考え方を取り入れたものになっている。しかし、ケーススタディでは、経済産業省のガイドラインは、IT 事故を取り上げ、内閣府のガイドラインは（自然災害全般を視野に入れてはいるものの）地震を想定リスクとして BCP の取組みをスタートさせることを推奨している。

内閣府の取組みの核は防災である。そして、防災対策の歴史は古い。内閣府のパンフレット「わが国の災害対策(Disaster Management in Japan)」のなかの「災害対策の歩み」を見ると、防災法制度・体制整備への取組みの年表は、明治 13 年(1880 年)から始まっており、この年に、日本地震学会が発足している。また、災害対策の沿革（戦後）は、昭和 21 年(1946 年)の南海地震から始まり、総合的な防災体制整備の機運は、昭和 34 年(1959 年)の伊勢湾台風を契機として高まったとしている。一方、情報セキュリティ分野の事業継続の取組みは、防災ほどの歴史はないが、IT の始まりとともに芽生え、企業や社会への IT の浸透とともに、その取組みは進化している。

---

[1] BCP：Business Continuity Planning（事業継続計画）

[2] BCM：Business Continuity Management（事業継続管理=事業継続計画策定から導入、運用、見直し、継続的改善を含む事業継続のためのマネジメントを言う）

2. ISO/IEC17799 と NIST SP800 シリーズに見る情報セキュリティと事業継続計画

情報セキュリティにおける事業継続の取組みは、Contingency Plan（緊急時対応計画）や Computer Security Incident Handling（コンピュータセキュリティインシデント対応）として良く知られている。米国国立標準技術研究所（以下 NIST[3]と言う）は、情報セキュリティに関する様々な規格やガイドラインを策定し、発表しているが、1995 年に発表された SP[4]800-12 An Introduction to Computer Security: The NIST Handbook（NIST コンピュータセキュリティハンドブック）の第 11 章は「緊急事態や災害への備え」（PREPARING FOR CONTINGENCIES AND DISASTERS）であり、第 12 章は、「コンピュータセキュリティインシデント対応」（COMPUTER SECURITY INCIDENT HANDLING）を取り上げている。これらは、後年、一冊のまとまったガイドラインとなり、2002 年 6 月には SP800-34 Contingency Planning Guide for Information Technology Systems（IT システムのための緊急時対応計画ガイド）が、2004 年 1 月には SP800-61 Computer Security Incident Handling Guide（コンピュータインシデント対応ガイド）が、2005 年 11 月には、SP800-83 Guide to Malware Incident Prevention and Handling（不正プログラムインシデント防止・対応ガイド）が発表されている。

なお、情報セキュリティにおいて、事業継続という言葉が使われている代表例としては、情報セキュリティマネジメントの国際標準 ISO/IEC17799 が挙げられる。

ISO/IEC 17799:2000 →JIS X 5080

（ISO/IEC 17799:2000 がJIS化されたものがJIS X 5080である）

Security policy セキュリティ基本方針	(2)
Security organization 組織のセキュリティ	(10)
Asset classification & control 資産の分類及び管理	(3)
Personnel security 人的セキュリティ	(10)
Physical & environmental security 物理的及び環境的セキュリティ	(13)
Communications & operations management 通信及び運用の管理	(24)
Access control アクセス制御	(31)
Systems development & maintenance システムの開発及び保守	(18)
Business continuity management 事業継続管理	(5)
Compliance 適合性	(11)

括弧内の数字は、管理策の数を示す。

ISO/IEC 17799:2005 →JIS Q 27002

（ISO/IEC 17799:2005 はJIS化されてJIS Q 27002となる）

Security policy セキュリティ基本方針	(2)
Organizing information security 情報セキュリティのための組織	(11)
Asset management 資産の管理	(5)
Human resources security 人的資源のセキュリティ	(9)
Physical & environmental security 物理的及び環境的セキュリティ	(13)
Communications & operations management 通信及び運用管理	(32)
Access control アクセス制御	(25)
Information systems acquisition, development and maintenance システムの取得、開発及び保守	(16)
Information security incident management 情報セキュリティインシデントの管理	(5)
Business continuity management 事業継続管理	(5)
Compliance 順守	(10)

※17799:2005の日本語表現は暫定的な仮訳

図１　ISO/IEC17799:2000 と ISO/IEC17799:2005 の管理ドメイン

[3] NIST：National Institute of Standards and Technology

[4] SP: Special Publications　NIST が発行する情報セキュリティに関するセキュリティ文書シリーズ。セキュリティ技術、セキュリティマネジメント等、幅広く網羅している。

ISO/IEC17799:2000(2000 年発行)には 10 の管理ドメインがあり、9 番目のドメインが事業継続管理（Business Continuity Management）であり、ISO/IEC17799:2005(2005 年発行)では情報セキュリティインシデントの管理(Information Security Incident Management)という管理ドメインが１つ増えて管理ドメインが 11 になり、10 番目の管理ドメインが事業継続管理（Business Continuity Management）である。2000 年版と 2005 年版の管理ドメインの名称は事業継続管理と変わらないが、その目的を見ると、微妙な（だが情報セキュリティと事業継続の関係からから考えると大きな）違いが見られる。以下に、2000 年版と 2005 年版より、事業継続管理のカテゴリ名及び目的に関する部分を引用する。

ISO/IEC17799:2000（JIS X 5080）より

11. 事業継続管理 11.1 事業継続管理の種々の面（Aspects of business continuity management） 目的：事業活動の中断に対処するとともに，重大な障害又は災害の影響から重要な業務手続を保護するため。 災害及びセキュリティ障害（例えば，自然災害，事故，装置の故障及び悪意による行為の結果）による中断を，予防管理策と回復管理策との組合せによって許容可能なレベルにまで抑えるために，事業継続管理手続を実施することが望ましい。（以下省略）

ISO/IEC17799:2005 より（日本語暫定訳）

14 事業継続管理 14.1 事業継続管理における情報セキュリティの側面 （Information security aspects of business continuity management） 目的：情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに，それらから重要な業務プロセスを保護し，また，事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。 組織への影響を最小に抑えるため，及び予防的管理策と回復のための管理策との組合せによって，情報及び情報処理施設に関連する資産の損失（例えば，自然災害，事故，装置の故障及び悪意による行為の結果の場合がある。）を受容可能なレベルにまで回復するために，事業継続管理手続を実施することが望ましい。この手続では，重要な業務プロセスを識別すること，並びに運用，要員配置，資材，配送及び設備といった点で関連する，情報セキュリティ管理面以外の事業継続の要求事項と情報セキュリティ管理面の事業継続の要求事項とを統合することが望ましい。（以下省略）

2000 年版の事業継続管理にかかわる管理カテゴリは、Aspects of business continuity management（事業継続管理の種々の面）であり、2005 年版のそれは、Information security aspects of business continuity management（事業継続管理における情報セキュリティの側面）である。つまり、2005 年版では情報セキュリティ関連であることが明示されているのに対し、

2000 年版ではそうは書かれていない。また、「目的」を比べると 2005 年版では、「情報システムの重大な故障又は災害の影響からの～」と始まり、情報システムにかかわる事業継続管理であることが強調されている。さらには、2000 年版（JIS X 5080）「11.1.2 事業継続及び影響分析」では、「業務手続の中断を引き起こし得る事象の特定と、リスクアセスメントには, 事業資源及び手続の管理者が全面的に関与することが望ましい。このアセスメントは，すべての業務手続を検討するものであり，情報処理施設に限定しない。」とあるのに対し、2005 年版では、同じ、事業継続管理の第 2 番目の管理策「14.1.2　事業継続及びリスクアセスメント」で、「事業継続に関するリスクアセスメントは，事業資源及び業務プロセスの管理者の全面的な関与のもとで実施することが望ましい。このアセスメントは，すべての業務プロセスを検討し，情報処理施設に限定しないことが望ましいが, 情報セキュリティ特有の結果を含むことが望ましい。」（下線筆者）とある。2000 年版では、組織の全てのビジネスプロセスを対象とした事業継続管理であるのに対し、2005 年版では、事業継続における情報セキュリティの側面を強調しようとする意図が感じられる。

3. BCP と Contingency Plan[5]（緊急時対応計画）の違い

平成 17 年 3 月付けの INTAP の報告書「平成 16 年度ビジネス継続性技術調査報告書」には、次の記載がある。「現在利用可能なビジネス継続マネジメントのベストプラクティスにはいくつかの方法が存在するが、多くの組織が依然として狭義の対応を行う情報技術の災害復旧（ITDR[6]）とビジネスの復旧、回復、及び計画に必要な情報を提供するだけの官僚的なアプローチのみにフォーカスし続けている。これは、対処的で予防的、更に組織、場合によっては業界全体がリードする包括的かつ統合された広義のビジネス継続マネジメントのプロセスとは対照的である。ビジネス継続マネジメントをビジネスの原動力となるプロセスとして捉えた場合、ITDR 及び復旧計画は、効果的で目的に合ったビジネス継続マネジメントの適合性と実効性を通して組織・業界の耐障害性（レジリエンシー）を推進及び提供するプロセス上の重要な要素として位置づけられる。」

情報セキュリティ(または IT)の世界で推進されてきた事業継続の取り組みは、ITDR（IT 災害復旧計画）であり、IT 緊急時対応計画（IT コンティンジェンシープラン）である。本来、事業継続の取り組みは、すべての業務プロセスを検討し全社的に行ってこそ意味があるものであり、IT に該当する部分でだけ行うものではない。ただ、BCP に関する取り組みが注目されてきたのは、ここ数年のことなので、それまでは、防災は防災のガイドライン、IT は IT 事故対応のガイドラインを策定してきたのも無理からぬことではある。

経済産業省の「事業継続策定ガイドライン」は、INTAP の報告書と時を同じくして発表されているのだが、それは、ケーススタディこそ IT 障害を取り上げているが、その内容は、広範なビジネスを対象とした「事業継続計画」そのものである。この報告書から 1 年たった 2006 年 3 月現在では、「多くの組織が依然として狭義の対応を行う情報技術の災害復旧（ITDR）とビジネスの復旧、回復、及び計画に必要な情報を提供するだけの官僚的なアプローチのみにフォーカスし続けている。」という状況は、もはや鳴りを潜めている。むしろ、「コンティンジェンシープラ

[5] Contingency Plan: 緊急時対応計画、コンティンジェンシープラン
[6] ITDR: IT Disaster Recovery　IT 災害復旧

ン」などと言おうものなら、「それは、（事業継続ではない）単なる緊急時対応計画ですね」と言われかねない局面さえある。

だが、事業継続計画と緊急時対応計画はどのように違うのだろうか？そしてまた、情報技術の災害復旧（IT Disaster Recovery）と緊急時対応（IT Contingency Planning）はどのように違うのだろうか？事業継続計画に関連する計画は数多く存在する。「事業継続計画（BCP）」「緊急時対応計画（Contingency Plan）」「災害復旧計画（Disasters Recovery Plan）」「インシデント対応計画(Incident Response Plan)」などは、馴染みのある言葉である。ところが、これらの計画の共通点は何で、異なる点は何で、どのように相互に関連しているか、となると、明確に分類、整理しているものが少ないように思う。経済産業省の「事業継続策定ガイドライン」では、BCP と Contingency Plan の違いを次のように説明している。以下に該当する部分を引用する。

「BCP と CP（コンティンジェンシープラン）との違いは、想定できるインシデントに対して、発生した場合の対応計画をあらかじめ策定しておくことは同様であるものの、BCP は事業の継続性の観点から事項、手順、体制、資源等の計画を具体化したものであると言える。また、CP は緊急事態発生直後の行動を中心とした計画であるのに対し、BCP は事前にビジネスプロセスの脆弱性を分析（ビジネスインパクト分析）した上で、それに基づいた計画を実施することに特徴がある。」

つまり、BCP は、ビジネスインパクト分析をした上で、コアとなる事業をいかに継続させるかという事業継続により焦点があてられているのに対し、コンティンジェンシープラン（緊急時対応計画）は、緊急事態発生直後の行動を中心とした計画であるという説明である。しかし、NIST SP800-34 の「IT 緊急時対応計画」[7]を見ると、計画を立てる際には、ビジネスインパクト分析から始まり、その手順は、BCP における手順と大きな違いは無い。強いて言えば、それは呼び名の違いであるとさえ思えてくる（もちろん、ビジネス全体に焦点をあてる BCP と IT に焦点をあてる IT 緊急時対応計画には明確な違いがある。それについては後述する。）

同じ経済産業省のガイドラインでは、＜2001 年 9 月 11 日 同時多発テロの対応＞として、以下の事例が紹介されているので引用する。

「世界貿易センター地域に所在していた金融系会社が、最重要拠点を失ったにもかかわらず危機的状態を見事なまでにくぐり抜け、9,000 人以上の従業員を無事に避難させたばかりか、その翌日からその拠点にあった事業の一部を他の場所で再開した。この会社は、自社の業務状況･リスク状況を分析（ビジネスプロセスの脆弱性分析）に沿って BCP を策定し、BCP のトレーニングを効果的に実施してきた。この BCM の過程では、あらかじめ、どの業務を国内外のどこの拠点に移すことができるか、さらにどの従業員をどの拠点に移すかについて検討をしていた。また、経営層の BCM に対する理解が会社内での BCM 推進に大きな役割を果たしたことは言うまでもない。」

これと同じ事例と思われるものが、「企業経営における IT 事故対応に関する調査研究報告書」(2004 年 3 月 ㈱インターリスク総研（経済産業省委託調査）の中で、「第 4 章、4.3 メリルリンチ社」の事業継続の取り組み事例として紹介されている。（http://www.bcijapan.jp/documents/BCM_survey.pdf） こ

[7] 正式名称は、NIST SP800-34 Contingency Planning Guide for Information Technology Systems (IT システムのための緊急時対応計画ガイド)。本稿では、以下「SP800-34 IT 緊急時対応計画」又は、SP800-34 と称す。

の報告で使われている名称は、事業継続の責任者は「グローバル災害計画担当役員」であり、事故が起こった時に動くのは、「全社緊急時対応チーム」であり、災害復旧に威力を発揮した強力なデータベースの名称は、「災害復旧計画システム」である。ここで何を言いたいかと言うと、名称に惑わされてはならないということである。同じ事業継続計画と言っても、それは、内容を確認してみると、IT 事故を対象とした IT 緊急時対応計画の性格をもつものかもしれないし、全社を対象とした事業継続計画であるかもしれない。そして、その反対のケースもあるのである。

視点を変えてみよう。では、ISO/IEC17799 では、管理ドメインの名称をなぜ「事業継続管理」とし、「緊急時対応計画」としなかったのか？情報セキュリティの三要素は機密性、完全性、可用性であるが、「事業継続」は可用性にあたる。そして、管理ドメインの名称を「事業継続管理」としたのは、「可用性」という言葉の背後にある「何のための可用性か？」という目的を強く意識しているためと考えられる。情報システムをいつでも「用いること可」の状態にしておくのは、まさに、ビジネス存続のために必要だからである。また、その名称を「事業継続管理」として「事業継続計画」としなかったのは、BCP を策定し、導入し、運用し、見直すというマネジメントサイクルで考えているからである。IT が社会・経済・政治に深く浸透している現在、IT の関与しないビジネスプロセスは、むしろ少なくなっており、事業継続計画に IT が関与する範囲が拡大しているという事情もある。また、相次ぐ天災により、事業継続が求められるという社会背景がある。例えば、日本では、2004 年 10 月 新潟県中越地震の際に、被災地に製造拠点を置く取引先や子会社などが被災し、サプライチェーンが途絶えたことで親会社や取引先の事業継続に影響が出たケースがあり、CSR の観点からも事業継続管理が求められるようになった。しかも、IT システムの中断がビジネスの中断に直結するという局面も少なくないので、「情報システムの重大な故障又は災害の影響からの事業活動の中断に対処する」一連の活動を「（情報セキュリティにおける）事業継続管理」と言うのは、時代の趨勢を捉えている。

一方、NIST の様々なガイドラインを読むと、組織のミッションを遂行するために、IT や情報セキュリティがあるという目的意識は明確である。それなのに、NIST SP800-34 IT 緊急時対応計画では、なぜその名称を「IT 緊急時対応計画」とし、「事業継続管理」としなかったのか？ NIST SP800-34「2.2 計画の種類」には、次の記載がある。「一般には、IT 緊急時対応計画とその関連計画領域の定義として、普遍的に受け入れられているものは存在しない。このような定義が存在しないことで、各種の計画の実際の範囲と目的を考える際に、混乱が生じることがある。本項では、IT 緊急時計画に関する共通理解の基盤を提供するため、その他の種類の計画をいくつか特定し、IT 緊急時対応計画と比較してその目的と範囲について説明する」。SP800-34 では、計画の種類として、以下の 8 つの計画を挙げ、定義し、その相互の関連について言及している。

- 事業継続計画（BCP: Business Continuity Plan）
- 事業復旧（再開）計画（BRP: Business Recovery (or Resumption) Plan ）
- 運用継続計画（COOP: Continuity of Operations Plan）
- サポート継続計画/IT 緊急時対応計画(Continuity of Support Plan/IT Contingency Plan)
- 緊急時コミュニケーション計画(Crisis Communications Plan)
- サイバーインシデント対応計画(Cyber Incident Response Plan)

・ 災害復旧計画（DRP: Disaster Recovery Plan）
・ 人員緊急時計画（OEP: Occupant Emergency Plan）

ここでは、「事業継続計画」の対象範囲は「ビジネスプロセス」と定義され、IT が事業継続計画の対象範囲となるのは、ビジネスプロセスのサポートに IT が関与する場合としている。また、IT 緊急時対応計画は、IT システムの中断を対象とし、ビジネスプロセスに焦点をあてているわけではない（not business process focused）、とある。NIST がその文書の名称を「IT 緊急時対応計画」とし、「事業継続管理」としなかったのは、それは、この定義に照らし、SP800-34 が IT 緊急時対応計画を扱ったものであり、事業継続計画を扱ったものではないからである。ここで誤解を避けるために言うと、not business process focused というのは、責任範囲を明確にしているだけなのであり、ビジネスプロセスを重視していないわけでは無い。「情報システムは通常、ビジネスプロセスをサポートする。しかし、ビジネスプロセスは情報システムに関係しない、他の多様なリソースおよび機能にも依存する」（SP800-34 より）ため、IT 以外の他の多様なリソースおよび機能に関しては（業務分掌外または権限が無いため）立ち入らないのである。後述するが、IT 緊急時対応計画の策定では、最初の段階でビジネスインパクト分析を行い、まず、重要なビジネスプロセスを特定し、そのプロセスを動かしている重要な IT リソースと関連づけ、その IT リソースが中断した時の影響と停止許容時間を判定した上で、復旧優先度を決定していく。IT はミッション遂行のためにあるのであり、そのために、IT のかかわるビジネスの優先度決定が重要になるのである。もうひとつ大事なことは、SP800-34 では、緊急時対応に関する諸計画策定、更新の際には、各計画間の連携を取ることが重要であるとも述べられている点である。つまり、IT 緊急時対応計画は、事業継続管理の中の重要な要素として位置づけられており、また、それゆえ、各計画間の整合性を取ることが必要になるのである。このスタンスは、昨年 12 月に内閣官房情報セキュリティセンターより公表された、「政府機関の情報セキュリティ対策のための統一基準」の「6.3.2 事業継続計画（BCP）との整合的運用の確保」の各項の記載と近い（http://www.bits.go.jp/active/general/pdf/k303-052.pdf）。

4. 参照モデルとしての緊急時対応に関する諸計画の相互関係図

NIST SP800-34 では、上の項で述べた、8 つの緊急時対応関連の諸計画の相互関係を図示している（図 2 参照）。この図は、計画の相互関係のみならず、どの計画がビジネスプロセスに関与し、どれが IT 関連の計画であるか、そして、特に重要な計画が何かも示している。なお、この図を見て、これら全ての計画を策定しなければならないと読んではならない。この図は、優れた分類・整理学を提供しており、各計画が互いの位置づけを理解するための参照モデル（Reference Model）として使える。例えば、ここにあるガイドラインがあるとする。そのネーミングがどうであれ、内容がこの図のどの計画にあたるかを見ていくことで、その計画なりガイドラインの性格が浮き彫りにされる。また、自社の事業継続関連の計画を作る時にも、自分の会社がどの計画をつくろうとしているかの理解を助けてくれる。自社の規模、ビジネスプロセス、想定する事故や災害に応じて、策定すべき緊急時対応関連の計画はそれぞれに違うであろう。自社にとって、どのような種類の計画を策定するのが妥当であるかを考える時、この図は、自社の計画の位置を知るのに役立つ。

なお、NIST SP800-34　2.2 計画の種類には、「最終的には、組織は一連の計画を使用して、組織の IT システム、ビジネスプロセス、施設に影響を及ぼす中断に対して対応、復旧、継続の準備をする。」との記載があるが、これは、全ての計画が必要と言っているのではない。この部分の英語の原文は、”Ultimately, an organization **would** use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and the facility.”（下線筆者）である。下線の部分が shall でも should でもなく would なのは、そういう意味である。ちなみに、最近、SP800-34 の著者の一人である NIST の専門家と話す機会を持ったが、この図を参照モデルとして使うことが可能であること、また、NIST の推奨するセキュリティ管理策においては、事業継続に関する計画として、IT 緊急時対応計画を必須としているのであり、あとの計画はケースバイケースであるとのことであった。

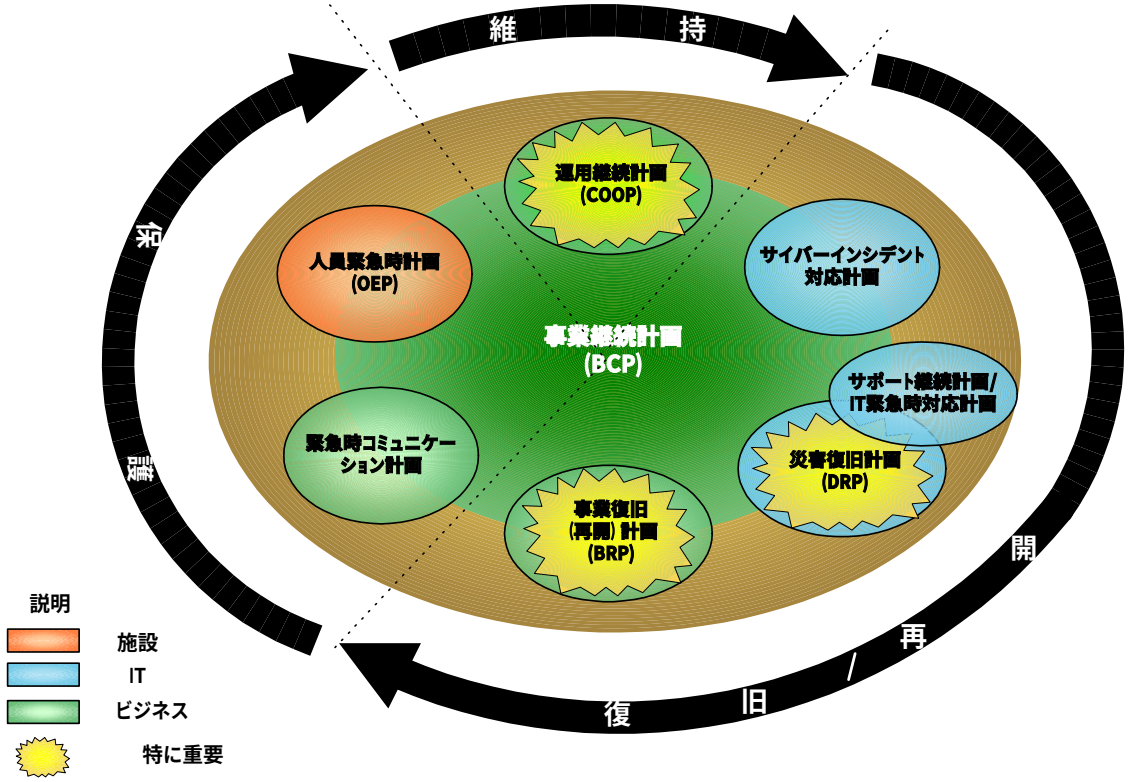


図2 緊急時対応に関する諸計画の相互関係図

この図で、事業継続計画が中央に配置され、各種計画と重複する部分がある点に注目したい。この図から、事業継続計画は各計画の中心にあり、各計画は、事業継続計画をサポートしていると見て取れる。この図を参照モデルとして使用する時、例えば、経済産業省の「事業継続策定ガイドライン」は、事業継続計画の枠組みと手順を示しており、リスクコミュニケーションに言及し、かつ IT 事故とインシデント対応、広域災害をケーススタディとして取り上げていることから、事業継続計画と IT 緊急時対応計画、サイバーインシデント対応計画、災害復旧計画、緊急時コミュニケーション計画を含むと考えられる。ま

た、内閣府中央防災会議の「事業継続ガイドライン第一版」は、事業継続計画の枠組みと手順を示しており、リスクコミュニケーションに関し言及し、対応するリスクとして「わが国の重大な災害リスクで海外からも懸念の強い「地震」を取り上げていることから、事業継続計画、災害復旧計画、緊急時コミュニケーション計画を含むと考えられる。なお、NIST の定義で、災害復旧計画が対象とするのは、「ほぼ、IT に特化している。影響が長期にわたる大規模災害に限定される。」となっている。

さて、世界各国で策定されているBCP/BCMのガイドラインはこの図にあてはめるとどのあたりに位置するのであろうか？ここでは、国際標準化（ISO化）を目指している2つのガイドラインを取り上げてみる。英国では、BCI[8]の「Good Practice Guidelines」をもとに英国規格協会（BSI）が策定したPAS[9]56 Guide to Business Continuity Managementがある。もうひとつは、米国のNFPA[10]が策定したNFPA1600「Standard on Disaster/Emergency Management and Business Continuity Programs」（2004年版）がある。2つとも、枠組みや手順を示し、リスクを特定していないことから、この図では、中央の事業継続計画にあたると考えられる。ちなみに、リスクを特定していないというのは、リスクについて言及が無いということではなく、原因であるリスクを問うよりも「結果事象」を重要視しているということであり、結果として様々なリスクに対応できることになる。国際標準化を目指すには、万人向け（または森羅万象向け）である必要があるということなのだろう。例えば、NFPA1600の付録A（Annex A Explanatory Material A.5.3.2）には、”The hazard identification should include, but is not limited to, following types of potential hazards:”(リスクは以下を含みかつこれらに限らない)として、地震、津波、火山の噴火、雪害、雪崩、台風、ハリケーン、竜巻、洪水、旱魃、飢饉、疫病、伝染病（SARS、鳥インフルエンザ）、火事、交通事故、ガス爆発、水や空気の汚染、停電、通信障害、テロ、戦争、暴動、ストライキ、誤情報、犯罪、放火、電磁波などなど、およそ考えつくありとあらゆるリスクを掲載している。

5. 誰が事業継続計画を策定するのか？

さて、事業継続計画というのは、経営判断により整備する性質のものだが、では、誰にこのように広範な事故･災害･リスクに対応する事業継続計画策定を任せることができるのであろうか？米国のDRII[11]は、事業継続及び災害対策関連の計画策定を担当する管理者に対する認定制度である「ビジネス継続プロフェッショナル」などを提供しており、BCIでは、事業継続の専門家として必要な能力を、以下の10項目に分類し公表している。

1 イニシエーションと管理
2 ビジネスインパクト分析
3 リスク評価とコントロール
4 事業継続管理戦略を作る

[8] BCI: The Business Continuity Institute
[9] PAS: Publicly Available Specification :一般仕様書。PAS56 は、英国標準ガイドラインである。
[10] NPA: National Fire Protection Association: 米国防火協会
[11] DRII: Disaster Recovery Institute International　災害危機管理の教育・指導・資格認定を行う非営利団体で、1988 年に米国で設立

5 緊急時対応とオペレーション
6 事業継続およびクライシス・マネジメント計画の開発と導入
7 アウェアネスと訓練プログラム
8 事業継続とクライシス・マネジメント計画の維持と実践
9 クライシスコミュニケーション
10 外部エージェンシーとの調整（Co-ordination with External Agencies）

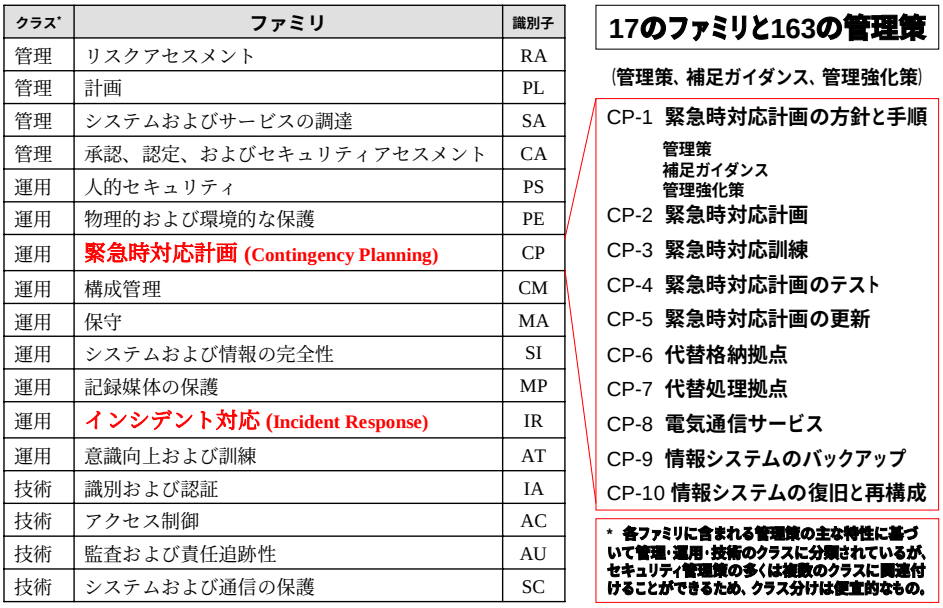
ここで注目したいのは、「外部エージェンシーとの調整」能力である。これだけカバーする範囲が広いと、事業継続の専門家が全てをカバーできるとは考えにくい。よって、例えば情報セキュリティ事故の場合は、情報セキュリティの専門家の協力が、鳥インフルエンザのような疫病の場合は、防疫の専門家の協力が、大規模災害の時には防災の専門家や災害支援のための団体、警察、消防、自治体などの協力が不可欠となり、外部組織との調整能力が重要になるのである。つまり、BCPの専門家には、経営的視点、調整能力、コミュニケーション能力、緊急事態に即した判断能力など、ジェネラリストとしての総合力、指導力が求められることになる。また、全社的な事業継続計画の策定にあたっては全ての関係者を集めた全社横断的な委員会を組織して策定する場合もあるだろう。但し、これもケースバイケースで、中小企業の場合などは、大掛かりな委員会ではなく、少数の幹部や担当者の合議検討で済む場合もあるだろうし、経営陣より策定を任されたBCP担当が作成したドラフトを経営者が承認するというストーリーがあるかもしれない。さらには、コアビジネスは誰が見ても明らかにWeb販売であれば、ビジネスインパクト分析を行うまでもなく、Webサイトの中断が想定する最大のリスクとなり、Webサイトの安全のための脆弱性管理も必要となり、情報セキュリティの専門家が関与する余地が大きくなる。

情報セキュリティと事業継続計画の関係について言えば、情報セキュリティは、事業継続計画における重要な部分であり、ITへの依存度が高ければ高いほど、ITの専門家や情報セキュリティの関係者が事業継続計画の策定および事業継続管理に関与する部分は大きくなる。また、すでにIT緊急時対応計画があり、新たに全社的事業継続計画策定の動きがある時には、お互いに連携を取り、二つの計画に矛盾の無いよう、二重に処理を実施することの無いよう、整合性を取るために積極的に協力すべきであろう。

6. ISO/IEC17799 と SP800-53

いままで、SP800-34 について述べてきたが、NIST の SP シリーズ文書で、ISO/IEC17799 と並び称されるのは、SP800-53 Recommended Security Controls for Federal Information Systems（連邦政府情報システムにおける推奨セキュリティ管理策）という文書である。ISO/IEC17799 は情報セキュリティ対策におけるベストプラクティスを集めた管理策集であり、SP800-53 は、そのタイトルが示す通り、米国連邦政府が情報セキュリティ対策を行なう際に推奨される管理策を集めたものである。ISO/IEC17799:2005 には、11 の管理領域と 133 の管理策がある、一方、SP800-53 には、17 の管理策ファミリ（管理領域と同様の意味）と 160 を超える管理策がある。ISO/IEC17799:2005 では、事業継続管理に関しては、ひとつの目的と 5 つの管理策があり、SP800-53 の IT 緊急時対応計画に関しては、9 つの管理策が記載されている。

なお、NIST SP 800-53 に示す管理策ファミリは、管理、運用、技術の 3 つの管理策クラスのいずれか 1 つと関連付けられている。しかし、セキュリティ管理策の多くは複数のクラスに関連付けることができるため、クラス分けは便宜的なものであることに留意されたい。たとえば、緊急時対応計画（CP）は運用に分類されているが「CP-1 緊急時対応計画の方針と手順」は運用及び管理両方の特性を持つ。



クラス*	ファミリ	識別子
管理	リスクアセスメント	RA
管理	計画	PL
管理	システムおよびサービスの調達	SA
管理	承認、認定、およびセキュリティアセスメント	CA
運用	人的セキュリティ	PS
運用	物理的および環境的な保護	PE
運用	緊急時対応計画 (Contingency Planning)	CP
運用	構成管理	CM
運用	保守	MA
運用	システムおよび情報の完全性	SI
運用	記録媒体の保護	MP
運用	インシデント対応 (Incident Response)	IR
運用	意識向上および訓練	AT
技術	識別および認証	IA
技術	アクセス制御	AC
技術	監査および責任追跡性	AU
技術	システムおよび通信の保護	SC

図3. SP800-53の管理策－ファミリ、クラス、識別子 (CP関連)

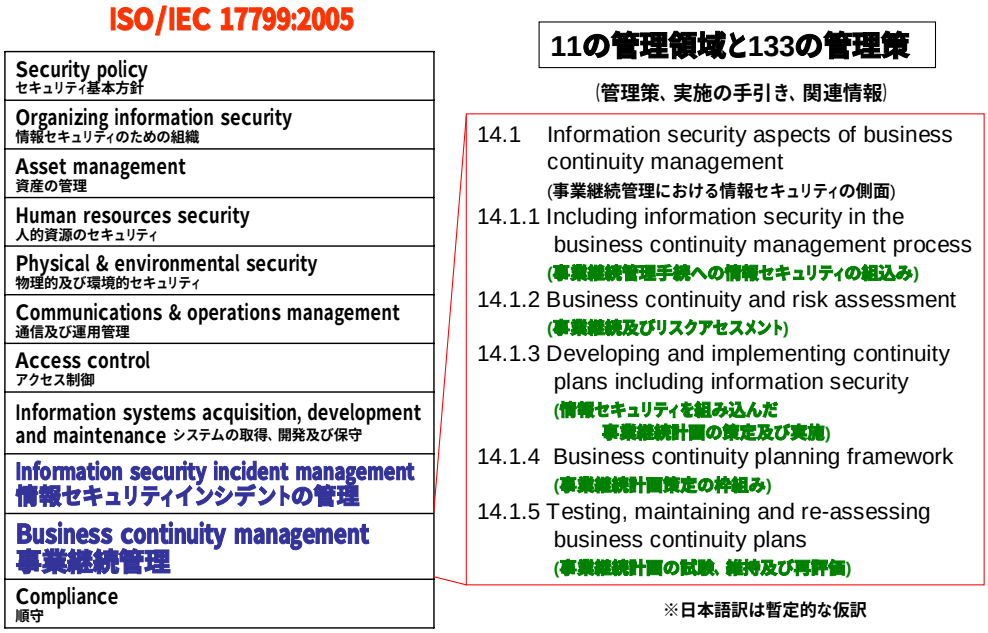


図4. ISO/IEC17799:2005の管理策(BCP関連)

SP シリーズ文書は立体的な構成になっている。管理策集として SP800-53 があり、そのそれぞれの管理策を実行に移すために、より詳細なガイドラインが用意されている。例えば、SP800-53 にはリスクアセスメントの管理策があり、それを実行に移すための詳細なガイドラインには、SP800-30 Risk Management Guide for Information Technology Systems (IT システムのためのリスクマネジメントガイド)があり、同様に、CP(緊急時対応計画）の管理策を実行に移すための詳細なガイドラインは、SP800-34 Contingency Planning Guide for Information Technology Systems（IT システムのための緊急時対応計画ガイド）が提供し、IR（インシデント対応）の管理策を実行に移すための詳細なガイドラインには、SP800-61 Computer Security Incident Handling Guide （コンピュータインシデント対応ガイド）と SP800-83 Guide to Malware Incident Prevention and Handling (不正プログラムインシデント防止・対応ガイド）がある。

なお、IPA では、海外の情報セキュリティ関連文書等の翻訳・調査研究を NRI セキュアテクノロジーズ(株)と共同で行い、その成果を一般に公開している。2006 年 3 月現在、12 文書の翻訳を公開しているが、SP800-53、SP800-34、SP800-61 の日本語翻訳は双方の Web ページより無償でダウンロード可能であり、SP800-83 も将来翻訳公開する予定である。

6. SP800-34　IT 緊急時対応計画

SP800-34 は、IT 緊急時対応計画を策定するための、体系的で費用対効果の高いソリューションを提供しており、時間とコストをかけずに、計画策定と運用ができるように、計画管理ツールとしても利用できる図表やテンプレートを含み、巻末付録には、「IT 緊急時対応計画のフォーマット例」や、「ビジネスインパクト分析の例とビジネスインパクト分析テンプレート」も掲載されている。以下に SP800-34 の特徴を示す。

1. 目的、範囲、対象とする読者が明確（誰が何のためにどのように利用するか明確）
2. 緊急時対応に関する諸計画の相互関係を示し、定義している。
3. 緊急時対応計画とリスクマネジメントプロセスを示している。
4. 緊急時対応計画とシステム開発ライフサイクルを示している。
5. 緊急時対応計画策定プロセスを以下の 7 つのステップにわたり解説している。
6. 豊富なテンプレートと付録が添付され、計画管理ツールとしても利用可能である。
7. 技術的考慮事項と人的考慮事項についても述べている。

6.1 IT 緊急時対応計画とインシデント対応の想定する脅威

IT システムに対する脅威としては、一般的に以下の脅威が挙げられる。

自然の脅威 ― 台風（ハリケーン)、竜巻、洪水、火災など
人的脅威　 ― 操作ミス、妨害行為、悪意のあるコードの埋め込み、テロ攻撃等
環境的脅威 ― 機器故障、ソフトウェアエラー、通信ネットワークの切断、停電等

しかし、SP800-34 IT 緊急時対応計画には「サイバー攻撃（サービス拒否、ウイルスなど）への対応については取り上げない。これらのインシデントへの対応には、IT 緊急時対応計画の対象範囲外の内容が含まれている。同様に、本ドキュメントでは、不法侵入、サービス拒否攻撃、悪

意のあるロジックの注入などのサイバー犯罪に対するコンピュータフォレンジック分析による証拠保存に関連する、インシデント対応についても記述していない。」との注記がある。そして、SP800-34 で取り上げられなかった、サイバー攻撃やサイバー犯罪に対する対応については、先に紹介した「コンピュータインシデント対応ガイド」や「不正プログラムインシデント防止・対応ガイド」で取り上げられている。但し、これらのガイドラインでは、インシデント対応における方針、手順、訓練、テストを用意することを求めているのであり、インシデント対応計画の策定を求めているわけではない。計画策定が求められるのは、あくまでも IT 緊急時対応計画である。しかし、人的脅威のうちでもサイバー攻撃やサイバー犯罪などの悪意のある攻撃に関しては、予防措置や検知、回復措置にしても、フォレンジック分析や証拠保存にしても、技術的に高度な専門性が求められるため、IT 緊急時対応とは別に詳細なガイドラインを設けているのである。

ちなみに、ISO/IEC17799:2005 では、「情報セキュリティインシデントの管理」と「事業継続管理」の別の管理領域を設けていながら、例えば、「10.4.1　悪意のあるコードに対する管理策」の実施の手引きの中で、「悪意のあるコード感染からの回復のための適切な事業継続計画の策定」を求めている。これは、上の考え方に少し似ている。

6.2　緊急時対応計画とシステム開発ライフサイクル

SP800-34「2.3 緊急時対応計画とシステム開発ライフサイクル」では、緊急時対応計画とシステム開発ライフサイクルの関係についての記載がある。以下にシステム開発ライフサイクル（SDLC: System Development Life Cycle）のそれぞれのフェーズにおける主な活動を挙げる。

開始フェーズ：　　新 IT システムの企画に際し、緊急時対応計画の要件を考慮する

開発/調達フェーズ：緊急時対応策は、運用要件を反映する

導入フェーズ：　　緊急時対応策を検証、テストする

運用/保守フェーズ：

・緊急時対応計画手順を包含する訓練と意識向上プログラムを整備する

・定期的にバックアップを実施して、オフサイトに保存する

・必要に応じた緊急時対応計画の保守・更新をする

廃棄フェーズ：

既存システムを撤去し、別のシステムに交換する場合も、緊急事態について考慮する

ここで、「緊急時対策をシステム開発ライフサイクル（SDLC: System Development Life Cycle）のすべての段階で考慮することで、コスト削減や運用負荷軽減に寄与できるが、緊急時対応計画は主に運用/保守段階フェーズの活動に関連する」（要旨）と述べている点は注目に値する。「運用/保守段階フェーズ」の主要な活動として、教育や訓練、バックアップ、計画の保守更新が挙げられている。つまり、緊急時対応計画は、緊急事態発生時に活用できてこそ意味があるのであり、そのためにしっかりした、運用と保守が求められるのである。

6.3　ビジネスインパクト分析の実施

ビジネスインパクト分析は、緊急時対応計画プロセスにおける主要なステップである。ビジネス

インパクト分析は、重要なビジネスプロセスを特定し、そのプロセスを動かしている重要な IT リソースと関連づけ、その IT リソースが中断した時の影響と停止許容時間を判定した上で、復旧優先度を決定していく。そして、この分析結果は、他の緊急時対応関連計画の策定時にも利用できるとしている。

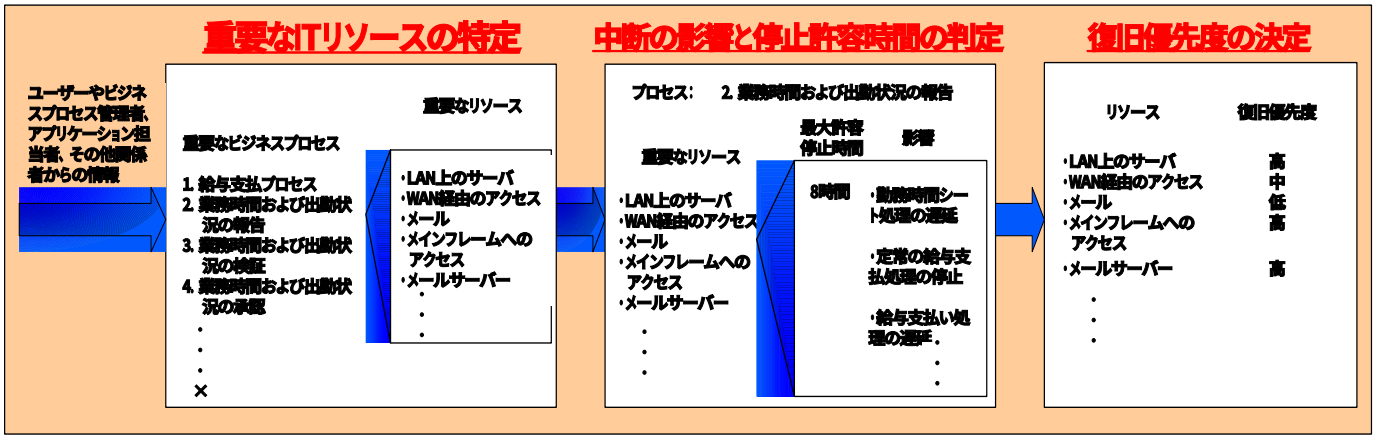


図4　ビジネスインパクト分析

6.4　IT 緊急時対応計画の策定

SP800-34 では、緊急時対応計画策定プロセスを以下の 7 つのステップにわたり解説している。

(1)緊急時対応計画ポリシーステートメントの策定　(2)ビジネスインパクト分析の実施
(3)予防対策の特定　(4)復旧戦略の策定　(5)IT 緊急時対応計画の策定
(6)テスト、訓練、演習の計画　(7)計画の保守

ビジネスインパクト分析が終わり、予防対策、復旧戦略を策定した後、IT 緊急時対応計画を策定する。IT 緊急時対応計画の構成については、以下の図 6 を参照されたい。

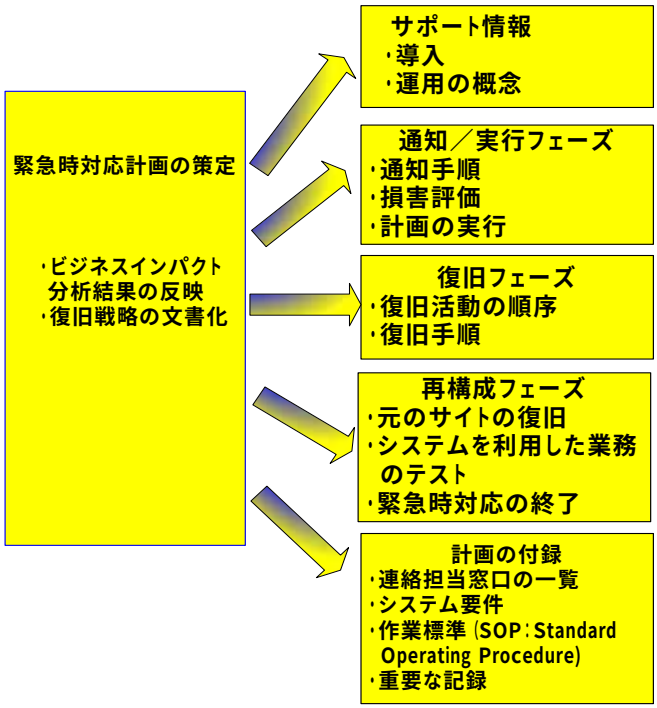


図6　IT緊急時対応計画の構成

7. おわりに

SP800-34の巻末付録Dには、緊急時対応計画における人的考慮事項が記載されている。そこでは、IT緊急時対応計画は、人員緊急時計画、事業継続計画、緊急時コミュニケーション計画などの各計画と整合性をとる必要があると述べられ、特に壊滅的なイベントを想定する場合には、以下の点を十分に考慮することとしている。

・人員緊急時計画：人員の安全性と撤退計画、退去手順、安否確認手順・方法、定期的な避難訓練、退避の際の人員確認の手順、災害後に人員の人数を数えるための手順と何通りかの連絡方法

・地域の消防署、警察署、レスキュー組織との連携し、事前に良好な関係を構築すること。

・コミュニケーション計画: 組織内での内部伝達と外部関係者への伝達窓口や手順

・人員の福利厚生：避難所、就業場所、人材調達、災害後の悲嘆へのカウンセリング

ここで銘記すべきは、深刻な状況下では、人的問題への対処が、事業継続や事業再開よりも優先するということであり、生命の安全等の「人的考慮事項」は最重要課題であるということである。そして、このことは、教育訓練の際にも、緊急事態に遭遇し、判断に迷うことの無いよう（自分の命と事業継続を天秤にかけることの無いよう）きちんと話しておくべきであろう。

参考資料

事業継続策定ガイドライン（経済産業省）

http://www.meti.go.jp/report/downloadfiles/g50331d06j.pdf

企業における情報セキュリティガバナンスのあり方に関する研究会報告書

http://www.meti.go.jp/report/data/g50331dj.html

事業継続ガイドライン 第一版　（内閣府　中央防災会議）

http://www.bcijapan.jp/documents/guideline01.pdf

事業継続計画の文書構成モデル例 第一版（内閣府　中央防災会議）

http://www.bousai.go.jp/MinkanToShijyou/shiryou4.pdf

わが国の災害対策(Disaster Management in Japan)

http://www.bousai.go.jp/panf/saigaipanf.pdf

企業経営における IT 事故対応に関する調査研究報告書　（㈱インターリスク総研）

http://www.bcijapan.jp/documents/BCM_survey.pdf

INTAP「平成 16 年度ビジネス継続性技術調査報告書」(平成 17 年 3 月)

http://www.net.intap.or.jp/INTAP/information/report/16-business-report.pdf

災害発生時における日本銀行の業務継続体制の整備状況について

http://www.boj.or.jp/about/03/data/sai0307a.pdf

金融機関における業務継続体制の整備について（2003 年 7 月日本銀行）

http://www.boj.or.jp/set/03/data/fsk0307a.pdf

当取引所の BCP(緊急時事業継続計画）について(2004 年 6 月 23 日 東京証券取引所)

http://www.tse.or.jp/guide/bcp/bcp2004.pdf

Business Continuity Management Good Practice Guidelines (2005)

http://www.thebci.org/goodpracticeguidetoBCM.pdf

NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2004 Edition http://www.state.nj.us/njoem/pdf/nfpa1600.pdf

NIST SP800 シリーズ文書

http://csrc.nist.gov/ http://www.ipa.go.jp/security/publications/nist/

SP800-12 An Introduction to Computer Security: The NIST Handbook
（コンピュータセキュリティハンドブック）(October 1995)

SP800-34 Contingency Planning Guide for Information Technology Systems
（IT システムのための緊急時対応計画ガイド） (June 2002)

SP800-61 Computer Security Incident Handling Guide (January 2004)
（コンピュータインシデント対応ガイド）

SP800-83 Guide to Malware Incident Prevention and Handling (November 2005)
（不正プログラムインシデント防止・対応ガイド）

SP800-53 Recommended Security Controls for Federal Information Systems (February 2005)

連邦政府情報システムにおける推奨セキュリティ管理策

ISO/IEC17799 関連

JIS X 5080、 ISO/IEC 17799:2000、 ISO/IEC 17799:2005

政府統一基準関連

政府機関の情報セキュリティ対策のための統一基準

http://www.bits.go.jp/active/general/pdf/k303-052.pdf

「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版［全体版初版］）」解説書

http://www.bits.go.jp/active/general/pdf/k303-052c.pdf

政府機関統一基準と ISO/IEC17799：2005 等との対応について

http://www.bits.go.jp/active/general/pdf/rel2005_iso.pdf