平成 22 年度
内閣官房情報セキュリティセンター委託調査

平成 22 年度
「サイバー攻撃動向等の環境変化を踏まえた重要インフラのシステムの堅ろう化に関する調査」

報告書

平成 23 年 3 月

株式会社 日立製作所

目次

1. 調査要領 2
2. 事例に基づく重要インフラのシステムの堅ろう性に関する調査・分析 3
2.1 堅ろう性等の定義・概念の比較 3
2.1.1 日本における定義 4
2.1.2 米国における定義又は概念 6
2.1.3 EU における定義又は概念 11
2.1.4 英国における定義又は概念 14
2.1.5 海外と日本における定義又は概念の比較 18
2.2 海外のサイバー攻撃事例の整理 18
2.2.1 海外のサイバー攻撃事例 18
2.2.2 海外のサイバー攻撃事例の整理 24
2.3 事例に基づく我が国の重要システムの堅ろう性に関する調査・分析 31
2.3.1 整理・分析の観点 31
2.3.2 重要システムの堅ろう性に関する整理・分析 31
2.4 堅ろう性に関する課題の抽出・提言 33
2.4.1 重要システムの堅ろう化のためのポイント 33
2.4.2 堅ろう性に関する課題の抽出・提言 35
3. 重要インフラの事業継続計画（BCP）の在り方に関する調査 37
3.1 日本国内の BCP 動向 37
3.1.1 BCP 普及状況 37
3.1.2 金融業界の動向 43
3.1.3 日本の BCP に関するガイドライン等 49
3.1.4 日本の BCP で求められている要件等 54
3.1.5 日本の BCP 事例 61
3.2 海外の BCP に関する調査 68
3.2.1 英国における BCP 動向 68
3.2.2 米国における BCP 動向 77
3.2.3 シンガポールの BCP に関する動向 85
3.2.4 国際規格化された BCP に関するガイドライン等 86
3.2.5 海外の BCP で求められている要件等 88
3.2.6 海外の BCP 事例 100
3.3 演習に関する調査 105
3.3.1 国内の BCP 演習事例 105
3.3.2 海外の BCP 演習訓練事例 111
3.4 BCP に関する課題の抽出・提言 116
3.4.1 BCP に関する調査の整理・分析 116
3.4.2 BCP に関する課題の抽出・提言 118
別紙 1. 第 2 次行動計画で示されている重要インフラ分野 123
別紙 2. IPA テクニカルウォッチ:『新しいタイプの攻撃』に関するレポート 124
1. 昨今のサイバー攻撃の実態と傾向 124
2. 『新しいタイプの攻撃』の実態 124

1. 調査要領

(1) 件名

サイバー攻撃動向等の環境変化を踏まえた重要インフラのシステムの堅ろう化に関する調査

(2) 目的

本調査は、重要インフラを取り巻く環境の変化のうち、主に「サイバー攻撃に対する重要インフラシステムの堅ろう性確保」との視点で、内閣官房情報セキュリティセンター（以下、NISC という。）として取組むべき政策課題の検討に必要な基礎的な情報収集及び分析を行うことを目的とする。

平成 22 年 5 月、情報セキュリティ政策会議において「国民を守る情報セキュリティ戦略」が決定され、重要インフラにおける具体的な取組の一つとして「重要インフラ防護対策の向上」が掲げられた。同取組では、重要インフラに被害があった場合でもサービス提供が維持できるよう、システムの堅ろう化等について検討することが求められている。

一方、最近のサイバー攻撃の動向に目を向けると、平成 21 年 7 月に米韓において大規模サイバー攻撃が発生したほか、国内においてもガンブラー型攻撃が多発している等、情報システムに対する脅威が高まっており、重要インフラにおいてもこのようなサイバー攻撃の動向を踏まえて的確に対応する必要性に迫られている。

加えて、システムの堅ろう性は、事業継続計画（BCP）に基づく情報システムの安定的な運用ができるかどうかによっても大きく影響されることから、情報システムの安定運用の視点から見た BCP の課題についても基礎的な情報収集及び分析を行う必要がある。

本調査の成果は、NISC における今後の情報セキュリティ政策の企画立案に活用し、サイバー攻撃に対する重要インフラの情報セキュリティ対策の向上に資するものとする。

なお、「重要インフラ」とは、平成 21 年 2 月 3 日に情報セキュリティ政策会議が決定した「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」において、「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものである。」と定義されており、同計画において、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む。）」、「医療」、「水道」及び「物流」の 10 分野（別紙 1 参照）の重要インフラを防護対象としている。

(3) 調査期間

平成 22 年 10 月 19 日（火）～平成 23 年 3 月 25 日（金）

(4) 調査の実施方針

調査にあたっては、国内における調査は基本的には重要インフラ事業者及び有識者へのヒアリングにより情報を収集し、海外の調査については国内有識者へのヒアリング及びインターネット上での公開情報、書籍等により収集した。ヒアリングを行った重要インフラ事業者及び有識者を表 1 に示す。

表 1. ヒアリング対応者一覧

#	分類	組織または有識者数
1	重要インフラ事業者	8 社
2	研究機関有識者	3 名
3	ベンダ有識者	3 名

2. 事例に基づく重要インフラのシステムの堅ろう性に関する調査・分析

1.(2)にて、「国民を守る情報セキュリティ戦略」の重要インフラにおける具体的な取組の一つとして「重要インフラ防護対策の向上」が掲げられ、同取組では、重要インフラに被害があった場合でもサービス提供が維持できるよう、システムの堅ろう化等について検討していると記したが、本章では、現在の我が国の重要インフラのシステムが堅ろうであるかについて調査を行った結果を示す。なお、システムの信頼性等の視点で見た堅ろう性については、既に経済産業省や情報処理推進機構等の各種調査※により検討されているため、本調査ではサイバー攻撃に焦点を当て、調査を行った。

調査の方法として、まず、「堅ろう性」の我が国の考え方を調査し、海外との差異を比較した。その結果を 2.1 に示す。続いて、サイバー攻撃の動向を把握する為、大規模なサイバー攻撃を受けた実績のある海外に焦点を当て、そのサイバー攻撃事例の収集を行った。その結果を 2.2 に示す。2.2 で示した海外事例をもとに、我が国の重要インフラ事業者へ、同様のサイバー攻撃を受けた場合の、システムの堅ろう性、重要インフラサービスへの影響についてヒアリングを実施した結果、及びヒアリング内容をもとに、システムの堅ろう性について整理・分析した結果を2.3 に示す。2.3 の結果及び有識者へのヒアリング結果(2.4.1 参照)をもとに、我が国の堅ろう性に関する課題をまとめたものを 2.4.2 に示す。

※(参考)システムの信頼性等の視点で見た堅ろう性に関する文献
≪経済産業省 発行文献≫
・情報システム・ソフトウェアの信頼性及びセキュリティの取り組み強化に向けて～中間報告書～（平成 21 年 5 月）
http://www.meti.go.jp/press/20090528001/20090528001.html
・情報システムの信頼性向上に関するガイドライン第 2 版 （平成 21 年 3 月）
http://www.meti.go.jp/press/20090324004/20090324004.html
・情報システムの信頼性向上のための緊急点検結果と今後の対応について （平成 19 年 8 月）
http://www.meti.go.jp/press/20070808007/20070808007.html

≪情報処理推進機構 発行文書≫
・重要インフラ情報システムの信頼性向上の取組みガイドブック （策定中）
・重要インフラ情報システム信頼性研究会[平成 21 年度報告書]（平成 22 年 3 月）
http://sec.ipa.go.jp/reports/20100427.html
・重要インフラ情報システム信頼性研究会[平成 20 年度報告書]（平成 21 年 4 月）
http://sec.ipa.go.jp/reports/20090409.html

2.1 堅ろう性等の定義・概念の比較

米国、EU 及び英国の海外の 3 つの国・地域における「サイバー攻撃」、「重要システム」及び「システムの堅ろう性」の定義又は概念について文献等により調査し、本調査において調査した日本における定義(暫定を含む)との比較を行った。日本における定義を 2.1.1 に、米国、EU、英国における

定義又は概念を 2.1.2～2.1.4 に示す。なお海外の定義については、複数文献で記されている概念を元に、複合してまとめた。

2.1.1 日本における定義

本調査において調査した日本における「サイバー攻撃」「重要システム」「システムの堅ろう性」の定義を表 2 に示す。

表 2.日本における定義(暫定を含む)

用語	日本における定義(暫定を含む)
サイバー攻撃※	DDoS・DoS 攻撃、不正侵入、重要情報の詐取、データ改ざん・破壊、不正コマンド実行等、情報通信ネットワークや情報システムを利用した電子的攻撃。
重要システム	重要インフラサービスを提供するために必要な情報システムのうち、重要インフラサービスに与える影響の度合いを考慮して、重要インフラ事業者毎に定めるものである。
システムの堅ろう性※	システムをサイバー攻撃から守り、サービスを安定的に提供できることとし、以下のようなシステムを「堅ろう性が高い」とみなす。 ・サイバー攻撃を受けにくいシステム ・サイバー攻撃を受けてもサービスを停止させないシステム ・サイバー攻撃によりサービスの一部が停止してもそれ以上拡大させないシステム ・サイバー攻撃によりサービスが停止しても早期に復旧できるシステム

※「サイバー攻撃」「システムの堅ろう性」については、本調査において暫定的に定義したもの。

日本においては、国民生活や経済活動の円滑な営みのために、情報セキュリティ対策における官民における統一的、横断的な推進組織が政府により設置されている。情報セキュリティ政策の基本戦略を決定する組織として「情報セキュリティ政策会議」があり、その施策遂行機関として「内閣官房情報セキュリティセンター」を平成 17 年に設置している。

表 2 に示した、日本における「サイバー攻撃」「重要システム」「システムの堅ろう性」の定義のおおもとは、「情報セキュリティ政策会議」及び「内閣官房情報セキュリティセンター」が示す定義又は概念が参考にされている。主な文献・ガイドラインについて、以下に示す。

(1) サイバー攻撃

文献名	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針(第 3 版)
発行日	平成 22 年 5 月 11 日
発行元	情報セキュリティ政策会議
URL	http://www.nisc.go.jp/active/infra/pdf/infra_pl09.pdf
文献採用理由	政府が策定した指針であり、サイバー攻撃の攻撃名称が列挙されていることから採用した。
示されている	(1)サイバー攻撃をはじめとする意図的要因

定義又は概念	不正侵入、データ改ざん・破壊、不正コマンド実行、ウイルス攻撃、サービス不能(DoS: Denial of Service)攻撃、情報漏えい、重要情報の搾取、内部不正等

文献名	国民を守る情報セキュリティ戦略　用語集
発行日	平成 22 年 5 月 11 日
発行元	情報セキュリティ政策会議
URL	http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf
文献採用理由	政府が策定した戦略であり、用語「サイバー攻撃」は定義されていないが、「サイバー犯罪」が定義されており、サイバーの概念を得る事を目的とし、採用した。
示されている定義又は概念	サイバー犯罪 インターネット等の高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪

文献名	重要インフラのサイバーテロ対策に係る特別行動計画
発行日	平成 12 年 12 月 15 日
発行元	情報セキュリティ対策推進会議
URL	http://www.nisc.go.jp/conference/seisaku/ciip/dai1/pdf/1sankosiryou2.pdf
文献採用理由	政府が策定した計画であり、用語「サイバー攻撃」を定義している文献であることから採用した。ただし、本計画は既に「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」に置き換えられている。
示されている定義又は概念	重要インフラの基幹をなす重要な情報システムに対して、情報通信ネットワークや情報システムを利用した電子的な攻撃。

(2) 重要システム

文献名	重要インフラの情報セキュリティ対策に係る第 2 次行動計画
発行日	平成 21 年 2 月 3 日
発行元	情報セキュリティ政策会議
URL	http://www.nisc.go.jp/active/infra/pdf/infra_rt2.pdf
文献採用理由	政府が策定した計画であり、用語「重要システム」を定義している文献であることから採用した。
示されている定義又は概念	「重要システム」とは、重要インフラサービスを提供するために必要な情報システムのうち、重要インフラサービスに与える影響の度合いを考慮して、重要インフラ事業者毎に定めるものである。

(3) システムの堅ろう性

文献名	重要インフラのサイバーテロ対策に係る特別行動計画
発行日	平成 12 年 12 月 15 日
発行元	情報セキュリティ対策推進会議

URL	http://www.nisc.go.jp/conference/seisaku/ciip/dai1/pdf/1sankosiryou2.pdf
文献採用理由	政府が策定した計画であり、システムの堅ろう性についての概念が示されていることから採用した。ただし、本計画は既に「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」に置き換えられている。
示されている定義又は概念	政府及び民間重要インフラ事業者等は、いわゆるサイバーテロの脅威に対して強固な基盤を構築するために必要な技術開発、脅威の分析、対策・技術に関する調査研究等を、官民の協力・連携を図りながら推進する。

文献名	情報セキュリティ 2010
発行日	平成 22 年 7 月 22 日
発行元	情報セキュリティ政策会議
URL	http://www.nisc.go.jp/conference/seisaku/ciip/dai1/pdf/1sankosiryou2.pdf
文献採用理由	政府が策定した計画であり、システムの堅ろう性についての概念が示されていることから採用した。
示されている定義又は概念	重要インフラ各分野における脅威の分析や分野横断的演習の継続的な実施を通じて、重要インフラ事業者等の情報セキュリティ対策を向上させ、重大な IT 障害等が発生した場合においても、その被害が局所化・最小化されるよう促す。また、被害があった場合でもサービス提供が維持できるよう、制御システムを含め、システムの堅ろう化等について検討する。

文献名	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第 3 版）
発行日	平成 22 年 5 月 11 日
発行元	情報セキュリティ政策会議
URL	http://www.nisc.go.jp/active/infra/pdf/infra_pl09.pdf
文献採用理由	政府が策定した指針であり、システムの堅ろう性についての概念が示されていることから採用した。
示されている定義又は概念	各重要インフラ事業者等においては、（途中省略）こと情報セキュリティに関しては、対策の効果が目に見えにくいことから、当該対策が十分であるか、事業者自らが十分な対策をなしているのか、を自己検証しつつ、国民生活や社会経済活動に重大な影響を及ぼさないよう IT 障害から重要インフラを防護する対策を進めることが重要である。その際、未然防止のための対策と、IT 障害発生後の拡大防止・早期復旧に向けた対応のバランスを取ることが望ましい。

2.1.2 米国における定義又は概念

米国では、1996 年に「大統領令 13010[1]」が発表され、それ以降、情報セキュリティ関連の政策が活発に打ち出されるようになった。2000 年の「情報システム保護のための国家計画[2]（National Plan for

1 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1996_register&docid=fr17jy96-92.pdf

2 http://clinton4.nara.gov/media/pdf/npisp-fullreport-000112.pdf

Information Systems Protection)」で重要インフラ等へのサイバー攻撃からの防御に重点を置き、2001 年の同時多発テロを経て、重要インフラ保護に係る取組を強化。その後、2002 年 11 月にテロと自然災害から国土の安全を守るために、政府組織の 1 つに DHS(U.S.Department of Homeland Security:米国国土安全保障省)を設立している。2006 年に NIPP(National Infrastructure Protection Plan:総合的にインフラを守る計画)策定、2009 年に改定される等、更なる強化を図っている。

DHS 内には NIAC(NATIONAL INFRASTRUCTURE ADVISORY COUNCIL:国家インフラ諮問委員会)を設け、重要インフラ分野とその情報システムのセキュリティに関するアドバイスの提供を行っている。本調査では、信頼性確保のため、連邦議会制定法に加え、DHS、NIAC が示す定義又は概念を参考に調査を行い、その結果を表 3 に示す。

表 3. 米国における定義又は概念

用語	米国における定義又は概念
サイバー攻撃	システムに対して、インターネットを介して、攻撃すること。具体的には以下の行為を指す。 ・Probe(探索) ・Scans(調査) ・Account(アカウントの奪取) ・sniffer(盗聴) ・Denial of Service(サービス拒否) ・Exploitation of Trust(なりすまし) ・Malicious Code(悪意のコード(マルウエア) ・Internet Infrastructure Attacks(インターネット施設への攻撃)
重要システム	国を支える必要不可欠なサービスは重要インフラと重要なリソースの双方が提供している。重要なリソースとは、官及び民間で管理される、経済及び行政の運用における最小限不可欠なリソースを指す。
システムの堅ろう性	以下の様な特徴を持つもの。 ・Robustness(丈夫さ): 危機に直面した際の、重要な操作と機能を維持する能力。 ・Resourcefulness(臨機さ): 熟練した技術を使い、危機や混乱に対応・管理する。 ・Rapid recovery(迅速なリカバリ): 能力が中断後可能な限り迅速かつ効率的に、再構成、通常の操作に復帰する。

≪参考文献≫

米国の「サイバー攻撃」「重要システム」「システムの堅ろう性」の定義又は概念について調査するにあたり、参考にした文献を以下に示す。

(1) サイバー攻撃

文献名	プレスリリース Protecting Our Federal Networks Against Cyber Attacks (2008 年 4 月)
発行元	DHS
URL	http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm

文献採用理由	サイバー攻撃に対する政府としての方針をまとめた発表資料であることから採用した。
示されている定義又は概念	情報技術は、政府と民間両方に対して、世界中の必要不可欠なサービスを効率良く、タイムリーに提供する手段として成長してきた。その結果、これらの重要システムは、インターネット経由での攻撃を受ける潜在的なリスクにさらされたままである。米国の公序良俗、経済、行政サービス、国家安全保障を守るために、私たちの重要な情報インフラの中断を最小限に抑えることは米国の政策である。 【以下原文】 Information technology has grown to provide both government and the private sector with an efficient and timely means of delivering essential services around the world. As a result, these critical systems remain at risk from potential attacks via the Internet. It is the policy of the United States to prevent or minimize disruptions to our critical information infrastructure in order to protect the public, the economy, government services, and the national security of the United States.

文献名	PRIORITIZING CYBER VULNERABILITIES FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL October 12, 2004
発行元	DHS-NATIONAL INFRASTRUCTURE ADVISORY COUNCIL(NIAC)
URL	http://www.dhs.gov/xlibrary/assets/niac/NIAC_CyberVulnerabilitiesPaper_Feb05.pdf
文献採用理由	政府が発行している資料で、サイバーに特化した攻撃方法をまとめており、キーワードの裏付けになるため採用した。
示されている定義又は概念	サイバー攻撃の詳細は、Probe（探索）、Scans（調査）、Account（アカウントの奪取）、sniffer（盗聴）、Denial of Service(サービス拒否)、Exploitation of Trust（なりすまし）、Malicious Code（悪意のコード（マルウエア）、Internet Infrastructure Attacks（インターネットインフラへの攻撃） 【以下原文】 Appendix A: Summary of Types of Cyber Attacks Probe、Scans、Account、sniffer、Denial of Service、Exploitation of Trust、Malicious Code、Internet Infrastructure Attacks

(2) 重要システム

文献名	Homeland Security Presidential Directive 7 （国土安全保障大統領指令 7）
発行元	DHS
URL	http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm
文献採用理由	政府発行指令の中で重要インフラを定義しているため、採用した。
示されている定義又は概念	アメリカのオープンで技術的な複雑社会は多用な重要インフラと主要なリソースを含んでおり、潜在的なテロのターゲットである。

	重要インフラと重要リソースは、アメリカ社会を支えるに必要不可欠なサービスを提供している。 (※重要インフラの定義は「USA patriot Act of 2001」、重要リソースの定義は「Homeland Security Act of 2002」参照となっている。) 【以下原文】 America's open and technologically complex society includes a wide array of critical infrastructure and key resources that are potential terrorist targets. Critical infrastructure and key resources provide the essential services that underpin American society.

文献名	USA patriot Act of 2001
発行元	連邦議会制定法
URL	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf
文献採用理由	重要インフラの損害が日本と異なり、安全保障問題として表現している点に着目した法であることから採用した。
示されている 定義又は概念	このセクションでは、「重要なインフラストラクチャ」という語は、システムや資産(有用な人・資源・利点)を意味している。それが物理的なものか仮想的なものかにかかわらず、アメリカにとってはとても重要であり、それの停止や破壊は安全性、国民経済の安定、国民の健康と安全やそれらを組みあわせた事柄を弱体化させる。 【以下原文】 In this section, the term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

文献名	Homeland Security Act of 2002
発行元	DHS
URL	http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf
文献採用理由	法の中で重要インフラの定義をしていることから採用した。
示されている 定義又は概念	重要リソースとは、官及び民間で管理される、経済及び行政の運用における最小限不可欠なリソースを意味する。 【以下原文】 (9) The term ''key resources'' means publicly or privately controlled resources essential to the minimal operations of the economy and government.

(3) システムの堅ろう性

文献名	CRITICAL INFRASTRUCTURE RESILIENCEFINAL REPORT AND

	RECOMMENDATIONS
発行元	DHS-NIAC
URL	http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf
文献採用理由	政府として堅ろう性の言葉を定義している文献のため採用した。
示されている 定義又は概念	重要インフラの resilience は 3 つの重要な特色によって特徴付けられる。 ・Robustness（丈夫さ）: 危機に直面した際の、重要な操作と機能を維持する能力。 物理的な建物やインフラデザイン(オフィスビルと発電と流通機構、橋、ダム、堤防)か、システム冗長と代替手段(輸送、送電網、通信網)に適用される。 ・Resourcefulness（臨機さ）: 熟練した技術を使い、危機や混乱に対応・管理する能力。 これにより、損害を制御し、緩和するための優先順位を効果的に決定する。ビジネス継続計画、トレーニング、サプライチェーン・マネジメントが含まれる。 ・Rapid recovery（迅速なリカバリ）: 中断後 可能な限り迅速かつ効率的に、再構成、通常の操作に復帰する能力。コンティンジェンシープランや緊急時の手順書に含まれ、適切な場所に適切な人材と資源を配置することを意味する。 【以下原文】 For the purpose of this study, critical infrastructure resilience is characterized by three key features: ・ Robustness: the ability to maintain critical operations and functions in the face of crisis. This can be reflected in physical building and infrastructure design (office buildings, power generation and distribution structures, bridges, dams, levees), or in system redundancy and substitution (transportation, power grid, communications networks). ・ Resourcefulness: the ability to skillfully prepare for, respond to and manage a crisis or disruption as it unfolds. This includes identifying courses of action, business continuity planning, training, supply chain management, prioritizing actions to control and mitigate damage, and effectively communicating decisions. ・Rapid recovery: the ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption. Components include carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right place.

文献名	National Infrastructure Protection Plan （NIPP:国家インフラ保護計画）
発行元	DHS
URL	http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
文献採用理由	政府として堅ろう性の言葉を定義している文献のため採用した。

示されている 定義又は概念	Resilience（回復力）: 変更発生時や災害発生時に回復するか、正常に対応できる能力。 【以下原文】 Resilience. The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

2.1.3 EU における定義又は概念

EU では、2009 年にセキュリティ政策「Critical Information Infrastructure Protection（CIIP）」が採択され、EU 加盟国の大規模なサイバー攻撃等発生時における対応能力の強化を大きな目的に挙げている。CIIP には、EU 加盟国に国レベルでサイバーセキュリティ訓練を行うように呼びかける計画等が盛り込まれる等サイバーセキュリティに対する取組みが活発になってきている。

本調査では、信頼性確保のため EU の法の制定権限を有する欧州議会（メンバは民主的に選ばれる）、欧州連合理事会（THE COUNCIL OF THE EUROPEAN UNION、メンバーは加盟国を代表する閣僚によって構成される）が示す定義又は概念、及び欧州連合の機関の一つである ENISA（European Network and Information Security Agency：欧州ネットワーク情報セキュリティ庁）が示す定義又は概念を参考に調査を行った。その結果を表 4 に示す。

なお、ENISA は、ネットワークセキュリティ及び情報セキュリティに関する予防・対応能力を促進することを任務とし、2004 年に設立された機関である。

表 4. EU における定義又は概念

用語	EU における定義又は概念
サイバー攻撃	情報システムに対し、不法なシステム干渉、及び不法なデータ干渉等の不正アクセスを行うこと。
重要システム	システムのうち、混乱や破壊、特定のインフラストラクチャの影響の重大度が高いものが重要インフラ（ECIs）になりうる。ECIsは、EU を横断する以下の評価基準により決定するが、その評価基準に該当するかどうかの詳細基準は当該加盟国によってケースバイケースに基づいて決定する。 ・死傷者評価基準 ・経済効果評価基準 ・公開の効果基準
システムの堅ろう性	堅ろうなシステムとは、以下をみなす。 通常の動作に影響を与える障害（意図的又は自然に引き起こされたもの）に直面した際、欧州委員会が定める許容レベルのサービスを提供し、維持する能力をもつもの。

≪参考文献≫

EU の「サイバー攻撃」「重要システム」「システムの堅ろう性」の定義又は概念について調査するにあたり、参考にした文献を以下に示す。

（1） サイバー攻撃

文献名	Council Framework Decision 2005/222/JHA
発行元	THE COUNCIL OF THE EUROPEAN UNION,
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML
文献採用理由	重要システムへの防御の観点で攻撃の定義が記載されている文献のため採用した。
示されている定義又は概念	情報システムへの不法なアクセスやシステムへの干渉、データへの干渉といった一般的な攻撃による犯罪行為に対して、一般的な対策を行う必要がある。 【以下原文】 There is a need to achieve a common approach to the constituent elements of criminal offences by providing for common offences of illegal access to an information system, illegal system interference and illegal data interference.

(2) 重要システム

文献名	COUNCIL DIRECTIVE 2008/114/EC
発行元	EU 議会指令
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF
文献採用理由	定量的な評価を行う為の基準案があることから採用した。
示されている定義又は概念	EU の重要インフラ「ECIs(European critical Infrastructures)」になりうる、EU における評価基準は以下を包括するものとし、混乱や破壊、特定のインフラへの影響の重大度に基づいて決定する。基準に該当する特定の重要なインフラか否かを判断する正確なしきい値は、当該加盟国によって個別に決定する。 ・死傷者評価基準(死者・負傷の潜在的数で評価) ・経済効果評価基準(経済的損失。製品やサービスの劣化で評価。潜在的環境効果を含む) ・公開の効果基準(国民の信頼、身体的な苦痛や日常生活の破壊への影響の観点から評価。必要不可欠なサービスの損失を含む)。 【以下原文】 Article 3 Identification of ECIs 1. Pursuant to the procedure provided in Annex III, each Member State shall identify potential ECIs which both satisfy the cross-cutting and sectoral criteria and meet the definitions set out in Article 2(a) and (b). The Commission may assist Member States at their request to identify potential ECIs. The Commission may draw the attention of the relevant Member States to the existence of potential critical infrastructures which may be deemed to satisfy the requirements for designation as an ECI. Each Member State and the Commission shall continue on an ongoing basis the process of identifying potential ECIs. 2. The cross-cutting criteria referred to in paragraph 1 shall comprise the

	following: (a) casualties criterion (assessed in terms of the potential number of fatalities or injuries); (b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects); (c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services). The cross-cutting criteria thresholds shall be based on the severity of the impact of the disruption or destruction of a particular infrastructure. The precise thresholds applicable to the cross-cutting criteria shall be determined on a case-by-case basis by the Member States concerned by a particular critical infrastructure. Each Member State shall inform the Commission on an annual basis of the number of infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds. The sectoral criteria shall take into account the characteristics of individual ECI sectors. The Commission together with the Member States shall develop guidelines for the application of the cross-cutting and sectoral criteria and approximate thresholds to be used to identify ECIs. The criteria shall be classified. The use of such guidelines shall be optional for the Member States. 3. The sectors to be used for the purposes of implementing this Directive shall be the energy and transport sectors. The subsectors are identified in Annex I. If deemed appropriate and in conjunction with the review of this Directive as laid down in Article 11, subsequent sectors to be used for the purpose of implementing this Directive may be identified. Priority shall be given to the ICT sector.

(3) システムの堅ろう性

文献名	ENISA HP glossary
発行元	ENISA
URL	http://www.enisa.europa.eu/act/res/files/glossary
文献採用理由	堅ろう性について ENISA の HP 上で定義されているため採用した。
示されている 定義又は概念	通常の動作に影響を与える障害（意図的又は自然に引き起こされたもの）に直面した際、システムが欧州委員会の定める許容レベルのサービスを提供し、維持する能力。 【以下原文】 The ability of a system to provide & maintain an acceptable level of service, in face of faults (unintentional, intentional, or naturally caused) affecting normal operation

2.1.4 英国における定義又は概念

英国では、1999 年に「国家情報セキュリティ調整センター（National Infrastructure Security Cordination Center（NISCC））」を設立。同年に「重要インフラ防護プログラム（Critical National Infrastructure Protection Program）」を策定している。その後 2007 年に NISCC と英国セキュリティサービス（MI5）の一部、国家セキュリティアドバイスセンターが合併して、「国家インフラ防護センター（Centre for the Protection of National Infrastructure（CPNI））」を設立する等の強化を図っている。

さらに、英国では、内閣府（Cabinet Office）が民間組織向けに事業継続に関するサイトを設けており、その中で、事業継続に関する考え方やフレームワークや政策等ついて情報を提供している。本調査では、信頼性確保のため、英国内閣府が示す定義又は概念を参考に調査を行い、その結果を表 5 に示す。

表 5. 英国における定義又は概念

用語	英国における定義又は概念
サイバー攻撃	インターネット、広い通信ネットワーク、及びコンピュータシステムへの攻撃
重要システム	重要インフラの定義は、英国内での日常生活に必要不可欠であり、国家として社会的・経済的に継続するために必要な施設、システム、拠点、ネットワークとする。 重要インフラになりうるシステムの選定基準は、そのインフラが停止した場合に、生命、経済、重要サービスについて、影響が生じた際の影響度を分析し、判断する。どれか一つにでも生じる影響の大きさがカテゴリ 3 以上の影響が生じたものを重要インフラとする。カテゴリ 3 とは、実質的な重要性と必要不可欠なサービスの配信のインフラストラクチャで、損失が広範囲な地域や数十万の人々に影響を与える可能性のもの。
システムの堅ろう性	堅ろうなインフラストラクチャ（robust infrastructure）は、以下をみなす。 ・従来の、又は非従来の破壊的な活動が、市民荒廃や広範な緊急事態を招いた際、効果的に、柔軟に、かつ急速に対処することができる。

≪参考文献≫

英国の「サイバー攻撃」「重要システム」「システムの堅ろう性」の定義又は概念について調査するにあたり、参考にした文献を以下に示す。

（1）サイバー攻撃

文献名	UK Resilience HP
発行元	Cabinet Office
URL	http://www.cabinetoffice.gov.uk/intelligence-security-resilience/national-security/cyber-information-security.aspx
文献採用理由	システムへの攻撃について英国内閣府 HP 上で定義されているため採用し

	た。
示されている 定義又は概念	サイバースペース(インターネット、広域通信ネットワーク、及びコンピュータシステムを含む)からのリスクは、優先度の高いリスクとして政府が特定。 【以下原文】 The risks from cyberspace (including the internet, wider telecommunications networks and computer systems) have been identified by the Government as a high priority risk.

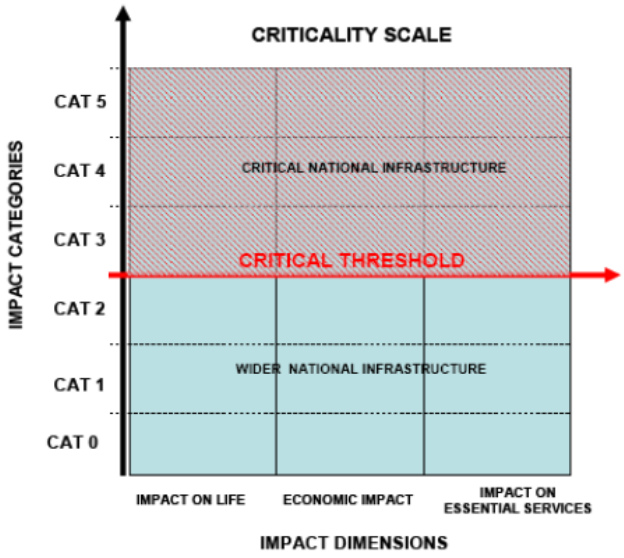
(2) 重要システム

文献名	Strategic Framework and Policy Statement
発行元	Cabinet Office
URL	http://www.cabinetoffice.gov.uk/media/349103/strategic-framework.pdf
文献採用理由	重要システムについて英国内閣府 HP 上で定義されているため採用した。
示されている 定義又は概念	A1.3 国家インフラの全てが"重要"な状況にあるわけではない。"重要"な特定の要素を含んでいるインフラにおいては、必要不可欠なサービスの可用性や完全性に悪影響を与え兼ねない損失や侵害は、厳しい経済状況や社会的重大性、人命の損失につながりかねない。これらの"重要"な資産は、国家の重要インフラ(CNI)を構成し、インフラ資産と個別に呼ばれている。インフラ資産は、物理的(敷地・設備・機器部品)もしくは論理的(情報ネットワーク・システム)なものでありうる。 A1.4 重要度の尺度には三つの要素がある。国の必要不可欠なサービスの提供への影響、(必要不可欠なサービスの損失に起因する)経済的影響、及び(必要不可欠なサービスの損失に起因する)生活への影響である。これらは図A1 に図解されている。インフラは、これらの影響を与えるいずれかの要素を使って分類することが出来る。指定は各影響要素においてもっとも重要度の高いカテゴリを反映すべきである。 (図より) カテゴリ 3 その喪失が地理的に広大な地域もしくは非常に多数の人々に影響を与え得る、必要不可欠なサービス部門及びその送達にとって非常に重要なインフラ。 (途中略) A1.6 基準にはクリティカルな閾値が設定されており、それは、その値以上の場合、これらのカテゴリーに分類されるインフラが重要な国家インフラの一角を形成するとみなされるべきである程、喪失の衝撃が深刻とみなされるレベルである。閾値は現在 CAT3(カテゴリー3)に設定されている。 2.6 イギリスの国家インフラは、政府により次のように定義されている。「国家の機能、及び、イギリス内の日常生活がそれに依拠している必要不可欠なサービスの送達に必要な設備、制度、用地、及びネットワーク。」 【以下原文】 A1.3 Not everything within a national infrastructure sector is “critical”. Within the sectors there are certain “critical” elements of infrastructure, the loss or compromise of which would have a major detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life. These “critical” assets make up the nation s Critical National Infrastructure (CNI) and are referred to individually

as “infrastructure assets”. Infrastructure assets may be physical (e.g. sites, installations, pieces of equipment) or logical (e.g. information networks, systems).

A1.4 The Criticality Scale includes three impact dimensions: impact on delivery of the nation s essential services; economic impact (arising from loss of essential service) and impact on life (arising from loss of essential service). These are illustrated in figure A1. Infrastructure may be classified using any one of these factors of impact. The designation should reflect the highest criticality category reached in either of the impact dimensions.

Criticality Scale	Description
CAT 5	This is infrastructure the loss of which would have a catastrophic impact on the UK. These assets will be of unique national importance whose loss would have national long-term effects and may impact across a number of sectors. Relatively few are expected to meet the Cat 5 criteria
CAT 4	Infrastructure of the highest importance to the sectors should fall within this category. The impact of loss of these assets on essential services would be severe and may impact provision of essential services across the UK or to millions of citizens
CAT 3	Infrastructure of substantial importance to the sectors and the delivery of essential services, the loss of which could affect a large geographic region or many hundreds of thousands of people
CAT 2	Infrastructure whose loss would have a significant impact on the delivery of essential services leading to loss, or disruption, of service to tens of thousands of people or affecting whole counties or equivalents
CAT 1	Infrastructure whose loss could cause moderate disruption to service delivery, most likely on a localised basis and affecting thousands of citizens
CAT 0	Infrastructure the impact of the loss of which would be minor (on national scale).

	 （途中略） A1.6 A critical threshold has been set on the scale and is the level above which the impacts of loss are considered so severe that infrastructure falling into these categories should be considered to form part of the Critical National Infrastructure. The threshold is currently set at CAT 3. 2.6 The UK's national infrastructure is defined by the Government as: ″those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends″.

（3）システムの堅ろう性

文献名	UK Resilience HP
発行元	Cabinet Office
URL	http://www.cabinetoffice.gov.uk/ukresilience/response/recovery_guidance/glossary.aspx
文献採用理由	堅ろう性に対する言葉の定義が英国内閣府 HP 上で示されているため採用した。
示されている定義又は概念	組織、サービス又はインフラがインシデントに対応できる能力。 【以下原文】 The ability of the community, services or infrastructure to withstand the consequences of an incident.

文献名	UK Resilience HP
発行元	Cabinet Office

URL	http://www.cabinetoffice.gov.uk/ukresilience/response/recovery_guidance/glossary.aspx
文献採用理由	堅ろう性に対する言葉の定義が英国内閣府 HP 上で示されているため採用した。
示されている定義又は概念	政府は、コアのフレームワークを通じて、英国のすべての部分にわたってResilience(回復力)を構築しようとしている。 Capability Programme の目的は、従来の、又は非従来の破壊的な活動が、市民荒廃や広範な緊急事態を招いた際、堅ろうなインフラの対応が、効果的に、柔軟に、かつ急速に対処するために設けられることを確実にすることである。 【以下原文】 Capability Programme The core framework through which the Government is seeking to build Resilience across all parts of the UK. The aim of the Capabilities Programme is to ensure that a robust infrastructure of response is in place to deal rapidly, effectively and flexibly with the consequences of civil devastation and widespread emergencies inflicted as a result of conventional or non-conventional disruptive activity.

2.1.5 海外と日本における定義又は概念の比較

海外の定義又は概念と、日本の定義を比較すると、国・地域によって詳細度は異なるものの、基本的な考え方に大きな差異はないことが分かった。

「重要システム」の定義については、英国では国として細かく定めているが、それには2つの背景があると考えられる。一つには、英国はEUの加盟国であり、EUでは「重要インフラ」の特定基準は加盟国によって決定することとしているためである。二つ目には、英国では、過去に大洪水、テロにより重要インフラの大規模な被害※を経験していることから、より具体的に守るべき重要インフラが選定できるよう、配慮されているものと考えられる。

米国における各定義等は、同時多発テロを受けた後に、急速に整備が進められているが、その内容は、日本の定義と近い表現である。

これらのことより、日本における「サイバー攻撃」「重要システム」「システムの堅ろう性」の定義は、海外と比較し、同等だと言え、以降の調査は 2.1.1 に示す定義をもって進めることとする。

なお、「サイバー攻撃」は不確定要素が多いため、5 年程度経過したのちに再度検証が必要である。また、「重要システム」「システムの堅ろう性」の双方は更なる検討の中で、レベル分けを行うことによって、別に述べる日本国における事業継続計画の策定と運用が明確になると考える。

※英国では、2005 年にロンドン同時爆破テロ(ロンドン地下鉄の 3 つの列車がほぼ同時に爆破され、その約 1 時間後にロンドン市内を走る 2 階建てバスが爆破された)、2007 年にイングランドでの豪雨及びそれに伴う大洪水により、広域の停電や 1 週間以上の断水に見舞われる等の被害を経験している。

2.2 海外のサイバー攻撃事例の整理

2.2.1 海外のサイバー攻撃事例

海外(主に米国及び欧州)における政府機関、重要インフラ、主要企業がサイバー攻撃を受けた事例について、文献等により収集した結果を表 6 に示す。

表 6. 海外サイバー攻撃事例

項番	攻撃の種類	時期	業種（国）	攻撃概要	影響
1	不正侵入	2000 年 3 月	水道（オーストラリア）	クイーンズランド州マルーチー(Maroochy)市の上下水処理場において、元請負業者の技術者が、汚水処理管理システムをハッキングした。元請負業者の技術者との契約を切った後も当該システムのリモートアクセス用ID・パスワードを変更していなかった。元請負業者の技術者は正社員雇用の依頼を断られたことを逆恨みし、不正なリモートログインを続け、ポンプ場の下水処理システムを誤動作させ、上水処理システムのバルブを不正に閉じる等の操作をおこなった。[3]	不正に汚水が開放された。数百万リットルの汚水が公園や川に流れ出し、悪臭を放った。
2		2006 年 8 月	交通（米国）	ロサンゼルス市内の交通監視センターにおいて、信号を自動制御するシステムを元職員がハッキングした。監視センターの元職員が解雇されたのを逆恨みし、解雇後も当該システムのリモートアクセス用 ID・パスワードが変更されていなかったことを利用し、不正ログインができてしまった。[4]	4 か所の重要ポイントで交通信号をシャットダウンさせ、壊滅的な交通遅延を発生させた。システムの正常化までに 4 日を要した。
3		2006 年 10 月	水道（米国）	ペンシルバニア州ハリスバーグの上水ろ過工場において、ハッカーがリモートアクセスにより SCADA システムをハッキングした。 ハッカーは認証情報を奪取するプログラムを仕込んだスパムメールを、上水ろ過工場をターゲットとして送付。メールを開いた従業員のノートパソコンがウイルスに感染。従業員が当該パソコンで SCADA ネットワークにリモートアクセスでログインした際に、インターネット経由で認証情報がハッカーの手に渡り、インターネット経由で SCADA を操作された。[5]	実害はなかった。
4		2008 年 1 月	鉄道（ポーランド）	列車の制御システムを 14 歳の少年がテレビのリモコンを改造したものでハッキングした。 列車のポイントを実際に切り替える装	列車 4 台が脱線、12 名負傷した。

[3] http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/
[4] http://www.gao.gov/new.items/d071036.pdf
[5] http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra.html

項番	攻撃の種類	時期	業種（国）	攻撃概要	影響
				置（リモートコントロール可能なもので列車無線を使ってポイントの切り替えを行うもの）に対して、テレビのリモコンを改造し、ポイントを操作した。結果、電車を脱線させた。[6]	
5		2010 年 7 月	金融（米国）	米国内 2 種の ATM 端末がハッキング可能であるとセキュリティカンファレンスで発表された。 インターネットで販売されている ATM の保守用の鍵を入手し、物理的に扉を開け、銀行等が ATM 専用の制御ソフトウェアの脆弱性を利用してシステムに侵入し、スタンドアロン並びにローカル LAN 経由で操作が可能であるとした。[7]	パスワードの入手、預金の引き出し、送金が可能であるとし、ATM メーカーが改善を行った。
6	不正侵入、データ破壊	2005 年 11 月	医療（米国）	テキサス州の LifeGift 臓器提供センターにおいて、元職員が患者と合致する臓器の照合に利用されるデーターベースをハッキングした。 当該データーベースはインターネット経由でリモートアクセスにより参照できるシステムであるが、元職員が退職後も当該システムのリモートアクセス用 ID・パスワードを変更していなかったため、不正ログインができてしまった。[8]	データーベースを削除されたが、治療に影響が出るような深刻な被害はなかった。
7	不正侵入、重要情報の搾取	2010 年 1 月	金融（米国）	ニューヨーク州ロングアイランドの銀行、Suffolk County National Bank (SCNB)において、ハッカーがオンラインバンキングシステムをハッキングした。 ID・パスワードファイルが SQL インジェクションで抜き取られ、不正侵入された。[9]	8300 人分のオンラインバンキング用ログイン ID 及びパスワードが盗まれた。6 日間にわたり侵入されていたが、その後乗っ取られたサーバをすぐに再構築したため、盗まれたアカウントでの不正アクセスの形跡はあったものの損失はなかっ

[6] http://www.theregister.co.uk/2008/01/11/tram_hack/
[7] BlackHat2010 資料より
[8] http://houston.fbi.gov/dojpressrel/pressrel08/ho06242008.htm
[9] http://www.theregister.co.uk/2010/01/12/bank_server_breached/

項番	攻撃の種類	時期	業種（国）	攻撃概要	影響
					た
8		2010 年 2 月	政府機関（ラトビア）	ラトビア国税庁において、電子納税システムがハッキングされた。 ID・パスワードが SQL インジェクションで抜き取られ、不正侵入された。[10]	個人/企業情報や納税情報が漏えいした。
9		2010 年 4 月	企業（米国）	テキサス州の大手電力会社 Lower Colorado River Authority のコンピュータシステムに海外のある単一の IP アドレスから 4800 回の総当たり攻撃を受けた。実際にはログインされなかった。[11]	実害はなかった。
10		2010 年 7 月	金融（米国）	インディアナ州において、クレジットカードの中央処理システムがハッキングされた。 ID・パスワードが、SQL インジェクションで抜き取られ、不正侵入された。[12]	カード情報が漏えいし、全米のレストラン顧客が影響を受け、被害額は 10 万ドル以上となった。
11		2010 年 12 月	企業（米国）	Google 社、金融機関、政府機関、IT、金融、メディア、化学等、米国の 30 社以上において、Internet Explorer（IE）の脆弱性を狙った情報搾取用のプログラムを仕組まれるゼロディ攻撃をうけ、不正アクセスされた。[13]	ソースコードが狙われ、盗まれた。知的財産を狙ったものだった。
12	不正コマンド実行	2003 年 8 月	鉄道（米国）	鉄道会社 CSX 社において、信号管理システムのネットワークからインターネット接続を行い、32/Blaster ワームに感染した。 ワームの感染拡大活動によりシステ	ワシントン周辺の 3 路線で列車の停止や代やの乱れが発生し、午前中の通勤客等へ支障がでた。

10 http://www.monstersandcritics.com/news/europe/news/article_1533738.php/Massive-security-breach-suspected-at-Latvian-tax-office

11 http://www.click2houston.com/news/23046216/detail.html

12 http://www.scmagazineuk.com/indiana-restaurant-chain-in-the-us-hit-by-credit-card-breach-after-hack-of-central-processing-system/article/173951/

13 http://www.wired.com/threatlevel/2010/03/source-code-hacks/

項番	攻撃の種類	時期	業種（国）	攻撃概要	影響
				ム全体に負荷がかかり、信号システムが使用できかくなってしまった。[14]	
13		2003 年 8 月	電力（米国）	オハイオ州の原子力発電所で Microsoft 社の SQL サーバを狙った Slammer ワームに感染した。 発電所のコンサルタント会社が Slammer ワームに感染した端末にてリモートアクセスをし、ワームを蔓延させてしまった。[15]	原子力発電所の安全監視システム等が約 5 時間停止したが、電力の供給には影響なかった。
14		2005 年 8 月	企業（米国）	ダイムラー・クライスラー（現ダイムラー）において、インターネット経由で LAN 上にある PC,制御用装置（Windows2000 搭載）が Zotob ワームに感染した。結果として、通信障害を引き起こした[16]	13 の自動車工場で組立ラインが 50 分程度操業停止となり、50,000 人以上の労働者が作業中断を余儀なくされた。
15		2010 年 3 月	政府機関（米国）	米国の運輸保安局（TSA）のテロリストデータを管理している同局のサーバに対し、元職員が使用禁止しているソフトウェアを持ち込みインストールした。 ソフトウェア等の資産管理が行われていなかった。[17]	実害はなかった。
16		2010 年 8 月	電力（イラン）	Windows の脆弱性を利用したワーム Stuxnet を入れ込んだ USB ストレージを、不正に原子力発電所内に持ち込み、SCADA（Supervisory Control and Data Acquisition）システムとネットワーク上接続されている PC に接続してしまったことから感染してしまった。[18] さらに感染後、Windows 上で動作する独シーメンス社製ソフトウェアの脆弱性を利用してプラントを制御する PLC（プログラマブルロジックコントロ	原子力発電所の産業関連コンピュータ約 3 万台が Stuxnet ワームに感染した。原発システムに深刻な影響を及ぼす状況ではなかった。

14 http://jacksonville.com/tu-online/stories/082103/bus_13328014.shtml
15 http://www.securityfocus.com/news/6767
16 http://www.eweek.com/c/a/Security/Zotob-PnP-Worms-Slam-13-DaimlerChrysler-Plants/
17 http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=223500107
18 http://www.physorg.com/news204701147.html 、http://www.energyjl.com/2010_folder/October/10new1019_2.html

項番	攻撃の種類	時期	業種（国）	攻撃概要	影響
				ーラ）に悪質なコードを書き込んだ。	
17	DDoS 攻撃	2007 年 4 月	政府（エストニア）	エストニア政府・金融機関の Web サイトが DDoS 攻撃をうけた。 攻撃元はロシアだと言われており、重要インフラを使用不能にすることを目的とした攻撃であった。[19]	エストニア政府・金融機関の Web サイトがアクセス不能になり、業務停止に陥った。
18		2008 年 8 月	政府（グルジア）	グルジア政府 Web サイトが DDoS 攻撃をうけた。 ロシア軍がグルジア攻撃中の出来事であり、情報システムを使用不能することを目的とした攻撃であった。[20]	グルジア政府 Web サイトがアクセス不能に陥った。
19		2009 年 7 月	政府（韓国）	韓国政府 Web サイトが DDoS 攻撃をうけた。 韓国国内で、一般の個人がパソコンでインターネットにアクセスした際に不正プログラムに感染、利用者が意図しないウェブアクセスが一斉に実行させるという手法で、韓国政府の Web サイトにアクセスが集中した。攻撃のプロセスが珍しい事案であるが、攻撃の目的は不明。[21]	韓国政府 Web サイトがアクセス不能に陥った。
20		2009 年 12 月	企業（米国）	DNS プロバイダーNeuStar 社の UltraDNS サービス botnet により DDoS 攻撃を受けた。 UltraDNS サービスは可用性が高いということを売りにしているサービスであったが、可用性を損なうことが証明された。さらにそのサービスを利用する企業が提供している web サービスが引きずられて利用不能に陥った。[22]	Amazon やウォルマートや Expedia 等の大手オンラインショッピングサイトがクリスマスの繁忙期に約 1 時間アクセス不能になった

[19] http://www.securityfocus.com/news/11503
[20] http://www.afpbb.com/article/environment-science-it/it/2506265/3215193
[21] http://www.afpbb.com/article/environment-science-it/it/2734844/5863452
[22] http://www.theregister.co.uk/2009/12/24/ddos_attack_ultradns_december_09/

2.2.2 海外のサイバー攻撃事例の整理

2.2.1 の事例より、システムがサイバー攻撃を被った要因として、我が国の重要システムの堅ろう化の視点で特に注意すべき代表的な次の 6 つの要因を抽出した。

① 「重要システム」と外部との接続経路の問題
  (a) 「重要システム」と「インターネットへ接続したシステム（情報系システム等）」とがネットワークで接続されており、この経路で攻撃を受けた。
  (b) 「重要システム」と「インターネットへ接続したシステム（情報系システム等）」とは分離されていたが、それ以外の経路（USB ストレージ等の媒体によるデータの授受、インターネットと接続された監視用 PC によるリモートログイン等）が存在し、そこが攻撃に利用された。

② 「重要システム」へのアクセス者に対する認証管理の問題
  (a) 元職員や元請負業者等の認証情報（ID、パスワード等）が登録されたままとなっており、それを使って攻撃を受けた。
  (b) 従業員のノート PC がウイルス感染したことにより、インターネット経由でリモートログインした際に認証情報が搾取されてしまった。

③ 「重要システム」を構成する機器の物理的な防御対策（鍵付筐体による内部機器の防御等）の問題
  ・すべての同一筐体に対して同一の対策を採っていたため強固な物理的対策とはなっていなかった。具体的には、同一の鍵を用いていたため、ひとつの鍵の入手で全筐体への攻撃が可能であった。

④ 独自システムとオープンシステムの脆弱性の問題
  ・オープンシステム（Windows PC 等）に対しその脆弱性をついて侵入。侵入したオープンシステムと接続されている独自システムの脆弱性をついて攻撃が実施された。

⑤ 人的側面の管理の問題
  ・従業員の不適切な行動（不正な持ち込み、不正な持ち出し等）が起点となり攻撃を受けた。

⑥ 新たな攻撃手法への対策の問題
  ・複数の攻撃手法を組合わせた「新しいタイプの攻撃※」が想定されてなく、攻撃を受けてしまった。

※IPA では、脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しく執拗な攻撃の中でも、システムへの潜入等の「共通攻撃手法」と情報窃取等の目標に応じた「個別攻撃手法」から構成される攻撃を「新しいタイプの攻撃[23]」と呼んでいる。（一部抜粋版を別紙 2 に示す）

重要インフラに対するサイバー攻撃としては、上記の他に DDoS 攻撃や SQL インジェクション等も起きているが、これらは重要システムの維持に影響するものではなく、インターネット上で提供するサービスの一般的な問題であるため、以降では分析の対象から除くこととする

これら 6 つの要因と、2.2.1 で示した事例との対応を表 7 に示す。

表 7. 6 つの要因と 2.2.1 の事例との対応

要因			対応する事例（表 6）の項番
①	「重要システム」と外部との接続経路の問題	(a)	項 14
		(b)	項 3、項 12、項 13、項 16
②	「重要システム」へのアクセス者に対する認	(a)	項 1、項 2、項 6、項 15

[23] http://www.ipa.go.jp/about/technicalwatch/pdf/101217report.pdf

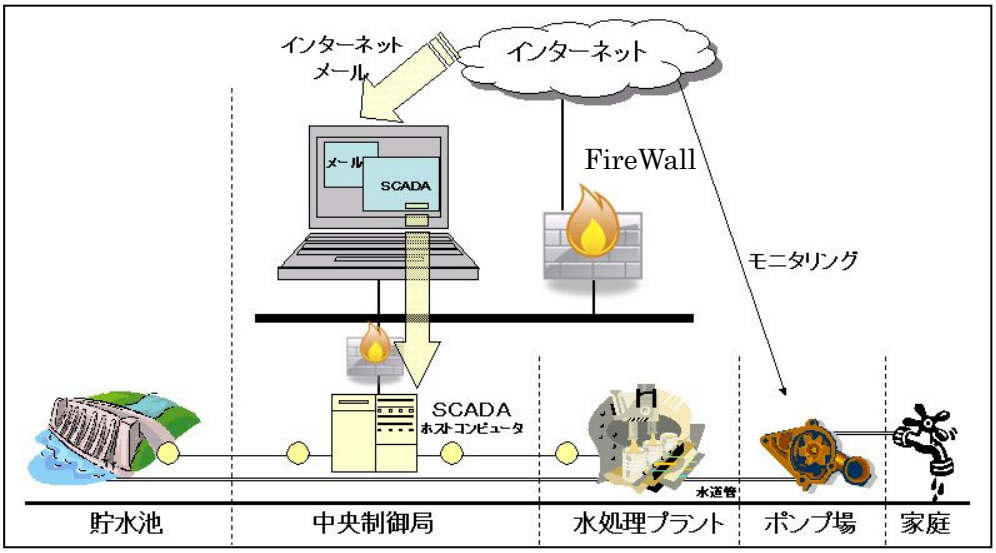
要因			対応する事例(表 6)の項番
	証管理の問題	(b)	項 3
③	「重要システム」を構成する機器の物理的な防御対策(鍵付筐体による内部機器の防御等)の問題		項 5
④	独自システムとオープンシステムの脆弱性の問題		項 4、項 5、項 16
⑤	人的側面の管理の問題		項 5、項 16
⑥	新たな攻撃手法への対策の問題		項 16
その他	インターネットに接続したシステム上でサービスを提供することによる問題		項 7、項 8、項 9、項 10、項 11、項 17、項 18、項 19、項 20

表 7から分かるように、表6の【項3】は上記6つの要因の中の①②を、【項5】は③④⑤を、【項16】は①④⑤⑥を含んでおり複数の要因を含んだ事例である。また、これら 3 つの事例に上記①から⑥の要因がすべて含まれており、これら 3 つの事例は 2.2.1 で抽出した表 6 の 20 の事例の中で代表的な事例と捉えることができる。

そこで、重要インフラ事業者及び有識者へのヒアリングに資することを目的として、これら 3 つの事例を取り上げてより詳細な整理を実施した。これら事例を整理した結果について、次の 2.2.2.1～2.2.2.3 に示す。

2.2.2.1 上水ろ過処理管理システムへの不正アクセス

本事案は、2.2.1 の項番 3 の事例であり、2.2.2 の①②が該当する事案である。重要システムを含めた情報システムの堅ろう性は認証管理によって維持管理されている。本事案は認証管理情報が標的型攻撃によって奪取された事案である。インターネットへ接続したシステムと重要システムが適切に分離されずに「インターネット側から認証管理のみで接続できるシステム」、「インターネットへ接続したシステムと重要システム間でのデータ授受において媒体をもちいるシステム」等で、我が国においても同様の事案が発生することが考えられる。

事案名	上水ろ過処理管理システムへの不正アクセス
発生年月	2006 年 10 月
国	米国
被害を受けたシステムの構成	・中央制御局の PC では、ウィンドウを切り替えて情報系システムと制御システムの情報を表示していた（PC 内で論理的に切り分けており、情報系システムと制御システム（SCADA システム）は、直接接続されていなかった）。 ・PC を情報系システムに切り替えた際には、従業員のメールの授受等に使用していた。 ・PC を制御システムに切り替えている際には、PC からインターネットを経由して、ポンプ場の機器を監視・制御する構成をとっていた。インターネット経由の操作の際には、アクセス者に対する認証管理を行っていた。  制御システム構成
攻撃手法	ハッカーは認証情報を奪取するプログラムを仕込んだスパムメールを、上水ろ過工場をターゲットとして送付。従業員が PC を情報系システムに切り替え、メールを開いた際、PC がウイルスに感染。従業員が当該ホストコンピュータを制御システムに切り替えた際に、ウイルスにより制御システムの認証情報が収集されてしまった。PC を再度情報系システムに切り替えた際、収集した認証情報がインターネット経由でハッカーの手に渡り、略奪された認証情報によりインターネット経由で SCADA を操作された。

事案名	上水ろ過処理管理システムへの不正アクセス
攻撃を受けた背景	インターネット経由で上水施設の SCADA への侵入を試みたものであった。侵入後に何をするつもりだったのかは不明。
サイバー攻撃対策への取組状況	システムへのリモートアクセスについて、ログインパスワードの定期的な変更の仕組みはあったものの、従業員が更新を怠っていた。
重要インフラサービスへの影響度合い	実害はなかった。
重要インフラ事業者の対処策	システムのすべてのパスワードを変更し、システムへのアクセスを排除した。

2.2.2.2 ATM 端末への不正アクセスの可能性

本事案は、2.2.1 の項番 5 の事例であり、2.2.2 の③④⑤が該当する事案である。本事案では 2 層のセキュリティ対策によって守られている。しかし、1層目の物理的防御策に対してはインターネットで販売されている物理鍵を入手することにより、2 層目の論理的防御策に対してはソフトウェアの脆弱性を用いることにより破ることができ、現金が奪取できてしまう。

「1層目のセキュリティに頼った、2 層目の安全管理の不備」、「1層目の鍵をインターネットで売買する関係者のモラル低下（人的側面の管理の不備）」、「2 層目のオープンシステム（ここでは汎用的なOS）の脆弱性」、「2 層目への脆弱性へ容易にアクセスできるハードウエアコネクタの存在」等の脆弱性を利用した攻撃は、我が国においても同様の事案が発生する可能性があると考えられる。

なお、「1層目のセキュリティに頼った、2 層目の安全管理の不備」について、本事案では 1 層目の物理鍵が破られ、2 層目のソフトウェアの脆弱性が突かれて破られたパターンだが、これに限らず、例えば 1 層目は「施錠された部屋」で防御していることに頼り、2 層目は「システムのコンソール端末が共通パスワードで操作可能（共通パスワードを利用している点が脆弱）」という場合等、複数のパターンが考えられる。

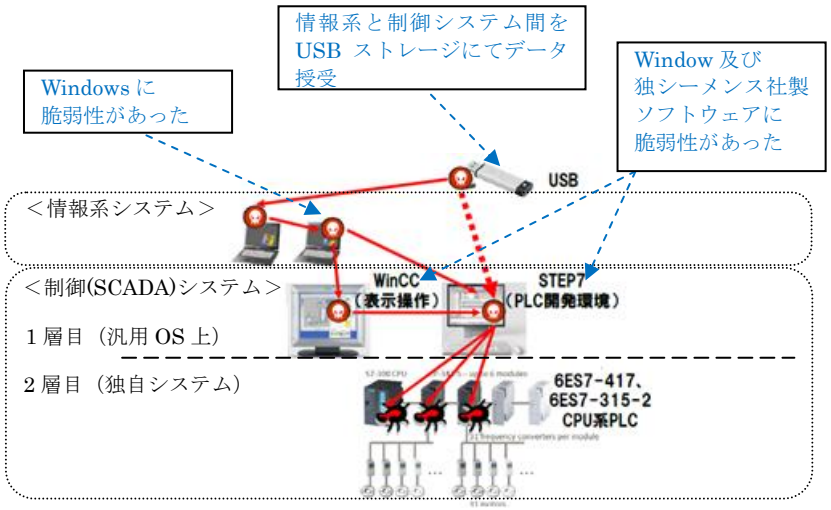
事案名	ATM 装置への不正アクセスの可能性
発生年月	2010 年 7 月
国	米国
被害を受けたシステムの構成	以下の ATM 装置メンテナンスパネルを物理的に開け、その後不正プログラムを侵入させる攻撃であるため、システム構成はないが、ATM 装置の構成を以下に示す。 ・1 層目として、ATM 装置のメンテナンスパネルを施錠管理していた。 ・メンテナンスパネルの鍵は同種筐体で1種類であった。 ・ハードウェアの回路基板にはメンテナンスにも利用できる、拡張コネクタが設けてあった。 ・2 層目として、ATM 装置の OS にオープンシステムの Windows CE を使用していたが、Windows CE を対象とした ATM 専用の制御言語を用いることで独自構成をとっていた。 ・Windows CE の脆弱性対策は行っていなかった。

事案名	ATM 装置への不正アクセスの可能性
	
攻撃手法	米国内 2 種の ATM 装置がハッキング可能であるとセキュリティカンファレンスで発表された。 2 通りの攻撃内容が発表され、一つはスタンドアロン型 ATM 装置の扉を物理的に開け、不正プログラムをインストールする方法である。 ATM 装置メーカー保守業者が取り扱う ATM メンテナンスパネルの鍵がインターネットサイトで販売されている。この鍵は、筐体が同種であれば鍵も同じであり、入手できてしまえばどの装置もあけることが可能である。鍵を開け、Windows CE を対象とした ATM 専用の制御言語の脆弱性をついた侵害プログラムを、回路基板上の拡張コネクタを利用してインストールすることで、プログラムで指定された枚数の札を出力できるとした。 注:現金は別鍵で管理されているボックス内にあり、鍵は流通していない。 もう一つは、ATM が接続されているネットワーク機器の空き LAN ポートを利用し、USB ストレージでプログラムをブロードキャスト配信し、プログラムで指定された枚数の札を出力できるとした。 物理と論理の両方の脆弱性を利用した事例。
攻撃を受けた背景	ー(実害が出る前に対策したため、攻撃受けず)
サイバー攻撃対策への取組状況	「重要システム」は「インターネットへ接続したシステム」とは分離しており、ネットワークからの侵害が無いとの前提で、物理的な侵害を受けないための対策を行っていた。(この事例の場合、物理的な侵害を受けないための対策であったATM装置のメンテナンスパネル鍵がインターネットサイトで販売されていた点、その鍵が同種筐体であれば共通の鍵が使用されていた点、ならびに、回路基板上に拡張コネクタが残されており、プログラムの投入を容易にしていた点が脆弱であった)
重要インフラサービスへの影響度合い	ATM内の現金を引き出すことが可能であるとした。
重要インフラ事業者の対処策	セキュリティカンファレンスで発表する前に、ATM 装置のメーカーへ忠告し、改善対応を行った。

2.2.2.3 産業関連コンピュータの不正プログラム(Stuxnet)感染

本事案は、2.2.1 の項番 16 の事例であり、2.2.2 の①④⑤⑥が該当する事案である。重要システムの中でも、制御系と呼ばれるシステムは独自の OS や装置によって構成されている独自システムであり、実質サイバー攻撃が受けにくいとされてきた。本事案では、組織内の情報系システムでワームに感染した USB ストレージを起点※とし、制御システムの 1 層目であるオープンシステム(汎用的な OS や装置)へ侵入。侵入したオープンシステムを足がかりとして 2 層目の独自システムへ侵入された事案であり、独自システムであっても攻撃が可能であることを示した事案である。本事案は、「多層に渡る攻撃である」という点を除けば、2.2.2.1、2.2.2.2 で述べた攻撃手法を組み合わせた事例であり、我が国においても同様の事案が発生することが考えられる。

※感染経路は、組織内の情報系システム＋USB ストレージ経由、不正持ち込みの USB ストレージ経由、ネット経由と諸説あるが、本調査では組織内の情報系システム＋USB ストレージ経由で感染した説を示す。

事案名	産業関連コンピュータの不正プログラム(Stuxnet)感染
発生年月	2010 年 8 月
国	イラン
被害を受けたシステムの構成	・制御システムは情報系システムと直接接続されていなかった。また、インターネットにも接続されていなかった。 ・制御システムの監視や PLC の開発は、Windows 上で動作する、制御系独自の独シーメンス社製ソフトウェアを使用していた。 
攻撃手法	情報系システムPC上の Windows の脆弱性を利用したワーム Stuxnet が、USB ストレージに感染。未知ワームであった Stuxnet は検知されずに、USB ストレージが原子力発電所内に持ち込まれた。Windows で動作する SCADA(Supervisory Control and Data Acquisition)システムへ USB ストレージを接続してしまったことから制御システムに感染してしまった。Stuxnet は、Windows 上で動作する独シーメンス社製ソフトウェアの脆弱性を利用して感染を拡大し、制御ネットワーク上の独自システムへ侵入しプラントを制御する PLC(プログラマブルロジックコントローラ)に悪質なコードを書き込んだ。

事案名	産業関連コンピュータの不正プログラム（Stuxnet）感染
攻撃を受けた背景	Stuxnet は SCADA（Supervisory Control and Data Acquisition）システムをターゲットに設計されていたことから、イランのブシュエール（Bushehr）原発を標的にしたものと推測されている。
サイバー攻撃対策への取組状況	「重要システム（SCADA システム）」は「インターネットへ接続したシステム（情報系システム）」とは分離しており、ネットワークからの侵害が無いとの前提で、物理的な侵害を受けないための対策を行っていた。
重要インフラサービスへの影響度合い	イランの産業関連コンピュータ約 3 万台が Stuxnet ワームに感染した。原発職員のコンピュータも感染する等周辺システムは感染したが、原発システムに深刻な影響を及ぼす状況ではなかった。
重要インフラ事業者の対処策	イランのヘイダル・モスレヒ情報相が声明を発表し、サイバースペース上の破壊活動を発見したので、対決法を設計のうえ実行に移し、破壊活動を全て阻止したとしている。

2.3 事例に基づく我が国の重要システムの堅ろう性に関する調査・分析

2.2.2.1～2.2.2.3 に示した海外事例の詳細をもとに、我が国の重要インフラ事業者へ、同様のサイバー攻撃を受けた場合の、システムの堅ろう性、重要インフラサービスへの影響についてヒアリングを実施した。このヒアリング内容をもとに、システムの堅ろう性について整理・分析した結果を以下に示す。

2.3.1 整理・分析の観点

2.1 で整理したように、システムの堅ろう性は、「サイバー攻撃を受けにくい」、「サイバー攻撃を受けてもサービスを停止させない」、「サイバー攻撃によりサービスの一部が停止してもそれ以上拡大させない」、「サイバー攻撃によりサービスが停止しても早急に復旧できる」、という4つの項目で特徴付けられ、これら 4 項目を満足するシステムが堅ろう性の高いシステムであると定義される。ここでの分析においても、この定義に基づき、次の 4 つの観点からヒアリング結果を整理・分析することとした。

- ・サイバー攻撃を受けにくいシステムという観点
- ・サイバー攻撃を受けてもサービスを停止させないシステムという観点
- ・サイバー攻撃によりサービスの一部が停止してもそれ以上拡大させないシステムという観点
- ・サイバー攻撃によりサービスが停止しても早期に復旧できるシステムという観点

2.3.2 重要システムの堅ろう性に関する整理・分析

2.2.2 では、海外のサイバー攻撃事例を整理した結果で、サイバー攻撃を被る要因として 6 つの要因(2.2.2①～⑥)を抽出した。逆に考えると、これら 6 つの要因に対する対策がなされていれば、堅ろう性を高めるための対策がされていると言える。したがって、ここでは、6 つの要因に対するヒアリングから得られた各事業者の多様な対策状況について整理した。整理した結果を以下に示す。

(1)サイバー攻撃を受けにくいシステムという観点

サイバー攻撃を受けにくくするために、次のような対策が取られている。

①重要システムと外部との接続経路への対策

- ・インターネットへ接続したシステムと重要システムを分離することで攻撃経路を絶っている。
- ・外部記録媒体接続ポートを物理的に閉鎖することで、攻撃経路を絶っている。

②重要システムへのアクセス者に対する認証管理

- ・技術的なアクセスコントロールにおいて攻撃経路を絶っている。

③重要システムを構成する機器の物理的な防御対策

- ・入退室管理の徹底や、建物の構造等で物理的な攻撃経路を絶っている。

④オープンシステムの脆弱性の管理

- ・重要システムには独自システム構成をとっている。
- ・2 種類のウイルスチェックソフトを使ってウイルスチェックを行っている。外部記録媒体を使用する前にはウイルスチェック専用端末にてウイルスチェックを行ってから使用している。

⑤人的側面の管理

- ・組織に関連する人員(従業員、委託先作業員等)へのサイバー攻撃を含む情報セキュリティ教育を定期的に実施し、組織内の規定や法・条例等を遵守させている。また、適性を見ながら適正配置している。
- ・重要システムの操作には勤続年数の長い信頼のできる役職付の人員を配置している。

⑥新たな攻撃への対応

- ・組織内の専門部署や、情報管理施策計画の中で、常に新しいリスクについて検討している。
- ・組織内外での事故事例を収集し、自組織における対策状況を随時確認している。

(2)サイバー攻撃を受けてもサービスを停止させないシステムという観点

サイバー攻撃を受けてもサービスを停止させないために、次のような対策が取られている。

①重要システムと外部との接続経路への対策

・他との接続点について、サイバー攻撃を防御・検知する仕組みを導入している。

②重要システムへのアクセス者に対する認証管理

・技術的なアクセスコントロールを強化している(同時にアクセスできるアカウント数の制限等)。

③重要システムを構成する機器の物理的な防御対策

・システムやオフィスを二重化し、バックアップを持つ構成(アクティブ/スタンバイ)、又は両系とも現用として運用する構成(アクティブ/アクティブ)をとっている。

④オープンシステムの脆弱性の管理

・オープンなシステムと独自の構成を組み合わせることで、攻撃を受けた場合でも影響が広がらない構成にしている。

・オープンシステムに対しては、セキュリティ対策ソフトを導入している。また、セキュリティパッチについては適用時の影響を検討し問題ないことが確認できた上で適用している。

⑥新たな攻撃への対応

・組織外での事故事例をもとに、自組織において対策を講じている。

(3)サイバー攻撃によりサービスの一部が停止してもそれ以上拡大させないシステムという観点

サイバー攻撃によりサービスの一部が停止してもそれ以上拡大させないために、次のような対策が取られている。なお、緊急時に人員が的確に行動できるようとられている対策であることから、「⑤人的側面の管理」に分類できると考えられる。

⑤人的側面の管理

・攻撃を受けて重要システムが停止した場合や、重要システムが攻撃を受けているために重要サービスの維持へ影響を与えかねない場合には、被害を拡大させない様に当該システムを切断し、手動で重要サービスを維持できる体制をとっている。また、対応に必要な人員を確保している。

・上記の様な対策を、重要サービスの維持に関する緊急時の対応手順書、BCP 等で明文化している。

・緊急時の対応手順書、BCP に則り、組織の人員や委託先作業員を含めた演習を実施している。

(4)サイバー攻撃によりサービスが停止しても早期に復旧できるシステムという観点

サイバー攻撃によりサービスが停止しても早期に復旧できるために、次のような対策が取られている。なお、緊急時に人員が的確に行動できるようとられている対策であることから、「⑤人的側面の管理」に分類できると考えられる。

⑤人的側面の管理

・通信の断絶で中央制御室から制御システムのコントロールが不可となったことにより、サービスが停止してしまった場合には、各拠点へ人員を出動させ、拠点間で連絡を取り合ってコントロールすることでサービスを復旧できる体制をとっている。また、対応に必要な人員を確保している。

・上記の様な対策を、重要サービスの復旧手順書、BCP 等で明文化している。

・復旧手順書、BCP に則り、組織の人員や委託先作業員を含めた演習を実施している。

以上示した(1)～(4)の結果から、ヒアリングした重要インフラ事業者の重要システムでは、

・サイバー攻撃を受けにくいための対策、

・サイバー攻撃を受けてもサービスを停止させないための対策、

・サイバー攻撃によりサービスの一部が停止してもそれ以上拡大させないための対策、

・サイバー攻撃によりサービスが停止しても早急に復旧できるための対策、

のそれぞれが取られていると言うことが出来る。すなわち、堅ろう化の定義の「サイバー攻撃を受けにくい」ための対策だけでなく、「サイバー攻撃を受けてもサービスを停止させない」以降の対策の重要性が認識されつつあるということが出来る。

2.4 堅ろう性に関する課題の抽出・提言

2.4.1 重要システムの堅ろう化のためのポイント

堅ろう性に関する課題の抽出、及び提言をまとめるにあたり、2.3 の調査結果を踏まえ、重要システムの堅ろう化のためのポイントを整理する。なお、表 1 に示す有識者へのヒアリングにおいていただいた下記ご意見も取り込んで整理する。

- ・研究機関のある組織では、研究目的で重要システムのデータを取扱う可能性がある。その場合の PC や USB ストレージ等の外部記録媒体の持込み・持ち出し管理が行われていない場合がある。研究目的等の場合であっても例外とせず、外部記録媒体の持込み・持出し管理を、厳格に行う必要がある。
- ・危険な問題（脅威）として認識しているが、事情により対応できていない問題（ユーザが少ない為対応の優先度を低く位置づけられている、複雑なシステムの組み合わせをしている為に解決できないセキュリティ問題を抱えている　等）について、対応を放置していると、重大な事故につながる可能性がある。中長期計画の中で対応を検討するか、他の対策で補う等の検討をすることが必要である。
- ・ヒヤリハットを放置すると重大な事故につながる可能性がある。ヒヤリハットを分析し、現場に対策等をフィードバックすることが重要である。
- ・委託や孫請け会社（再委託）、保安員、シンクタンク等への情報セキュリティの責任の適正な管理（サプライチェーン・マネジメント※）を行うことが重要である。
- ・外部人員（外注、派遣、研修生、留学生等の海外関係者等）の管理や内部犯行への対策を検討することが重要である。
- ・「セキュリティリスク（機密性維持の観点から見たリスク）」と「装置を操作できなくなるというリスク（可用性維持の観点から見たリスク）」は相反するものであるが、リスク同士を対立させるべきではない。多重リスクだと捉え、バランスよく、複数の対策を講じるべきである。
- ・重要インフラ事業者同士の海外と日本間での情報交換が活発ではない。このことについて、日本と海外とではシステムや組織の構成が違い、また閉域ネットワーク・独自システムの構成をとっているから安心であると思っている可能性がある。
- ・昔はダイアルアップを使ってインターネットへ接続しており、LAN と WAN で分けられていたが、現在では LAN と WAN の境目がなくなった。ダイアルアップの頃の「攻撃を受ける事が特別」だった時代とは環境が変わっている。また攻撃手法も昔に比べると多様化している。現在は「攻撃は受けるのが当たり前」という意識をもち、新しい攻撃に備える為にも対策は必須であるという認識を持つべきである。
- ・ IT 依存をしている箇所について把握しているつもりであっても、ネットワーク構成とノードに対する基本設計に関する指針がないために正確なインベントリができていないのではないか。思わぬ IT 依存があることを見落としている可能性がある。重要システムが堅ろうであることを計るメジャーとして、行うべき基本対策の明示が必要である。

※サプライチェーン・マネジメント（supply chain management（SCM）：供給連鎖管理）とは、従来は物流等において使われていた用語だが、情報セキュリティの世界では、会社・組織の壁を超えて情報セキュリティの責任が〝連鎖（連携）〟することを意味する。たとえば作業委託等で委託元が規定する責任が委託先にも連鎖する様に適正管理する事を言う。

上記の各ご意見について対策の観点で重要な項目を整理すると、以下の 7 つが重要対策項目だと言える。

(ア)サイバー攻撃に対するネットワーク以外の経路の管理:
サイバー攻撃に使われる可能性がある外部記録媒体をより厳重に管理する必要がある。
(イ)サイバー攻撃に対する定期的な脅威管理:
論理的攻撃に対する脅威危険な問題(脅威)として認識しているが事情により対応できていない問題やヒヤリハットへの対策を疎かにせず、取り組むことが重要である。
(ウ)重要システム維持と情報セキュリティ対策の為の組織外要員を含めた人員の適正な管理と組織間の役割の明確化:
組織と組織間でのサプライチェーン・マネジメント、組織と関わる内外部の人員の適正な管理が重要である。
(エ)サイバー攻撃に対するシステムの階層設計:
複数のリスクに対し、バランスよく、複数の対策を階層的に講じるような設計をすることが必要である。
(オ)サイバー攻撃に対する専用システムの抗性設計:
閉域ネットワークや独自システムの構成をとっているから安心であるという意識を払しょくする必要がある。
(カ)サイバー攻撃等に対する情報収集と PDCA 管理へのフィードバック:
現在は「攻撃は受けるのが当たり前」という意識をもち、新しい攻撃に備える為にも対策は必須であるという認識を持つべきである。
(キ)重要システム維持と情報セキュリティ対策の PDCA 評価の為のメジャーメント:
重要システムが堅ろうであることを計るメジャーがないため、行うべき基本対策の明示が必要である。

2.2.2 で示した、サイバー攻撃を被る 6 つの要因(2.2.2①～⑥)と、上記重要システムの堅ろう化のための重要な 7 つの対策項目(上記(ア)～(キ))を対応づけると以下の様になる。

①	「重要システム」と外部との接続経路の問題	(ア)	(イ)				(カ)	(キ)
②	「重要システム」へのアクセス者に対する認証管理の問題			(ウ)				
③	「重要システム」を構成する機器の物理的な防御対策(鍵付筐体による内部機器の防御等)の問題	(ア)				(オ)		
④	独自システムとオープンシステムの脆弱性の問題		(イ)					
⑤	人的側面の管理の問題			(ウ)				
⑥	新たな攻撃手法への対策の問題				(エ)	(オ)		

図 1.サイバー攻撃を破る要因と重要システムの堅ろう化のための対策項目 相関図

図 1 より、サイバー攻撃を破る要因の一つに対して一つの対策を施すのみでは、重要システムを堅ろうに保つことは難しく、多層に渡って防御(多層防御)する考え方が必要だと言える。また、有識

者ヒアリングより、重要システムに関わる雇用の体系が変化してきており、人的管理も多層防御の一つの層と捉えて考える必要がある。そして、全体の共通事項として、堅ろう性維持のための PDCA 管理において管理状況・対策状況が有効であることを計る為のメジャーが必要だと言える。これらのことについて、2.4.2 に課題としてまとめ、提言を示す。

2.4.2 堅ろう性に関する課題の抽出・提言

本項では、堅ろう性に関する課題の抽出・提言を示すが、課題の抽出を行うにあたり、まず 2 章における調査のまとめを以下に示す。

2.1 では、「堅ろう性」の我が国の考え方を調査し、海外の定義又は概念と比較した。その結果、国・地域によって詳細度は異なるものの、基本的な考え方に大きな差異はないことが分かった。

続いて、2.2 において、サイバー攻撃の動向を把握する為、大規模なサイバー攻撃を受けた実績のある海外に焦点を当て、そのサイバー攻撃事例の収集を行った。そして、収集した事例より、サイバー攻撃の被害を被った要因として、我が国の重要システムの堅ろう化の視点で特に注意すべき代表的な 6 つの要因を抽出した。

2.3 では、2.2 で示した海外事例をもとに、我が国の重要インフラ事業者へ、同様のサイバー攻撃を受けた場合の、システムの堅ろう性、重要インフラサービスへの影響についてヒアリングした結果を分析した。重要インフラ事業者ヒアリングでは、2.2 で示した重要システムの堅ろう化の視点で特に注意すべき代表的な 6 つの要因を排除するべく、サイバー攻撃を受けにくくする対策を実施しており、それに加えて、サイバー攻撃を受けてもサービスを停止させない対策や早期復旧のための対策が重視されつつあるという傾向が分かった。また、サイバー攻撃を受けてもサービスを停止させない対策や早期復旧のための対策としては、人的側面での対策が取られていることが分かった。

さらに 2.4.1 にて有識者ヒアリング等により重要システムの堅ろう化のための具体的な対策のポイントを調査したところ、7 つの対策項目が明らかになり、また、サイバー攻撃を受けない為には一つの対策だけでは不十分であり重要システムの堅ろう性が保てないことが分かった。

重要システムは、停止してしまうと少なからず重要サービスにも影響がでてしまう。逆に言えば、重要サービスを停止させない為にも重要システムを堅ろうに保つ必要がある。2.3 で得られた傾向、2.4.1 で得られた対策項目から、表 2、2.3.1 で示される堅ろう性の 4 つの観点をより実戦的に高めるため多層防御が必要である。そのため、情報セキュリティを構成する要素を「システム構成の層」と「人的構成の層」からなるものと捉え、各々のバランスに配慮して運用管理することで多層防御を実現する。

[1]システム構成の層

重要システムは、サイバー攻撃を受けにくい構成とするために、階層的なシステムの防御設計を行う。結果として、サイバー攻撃を受けてもサービスを停止させない状態を維持するシステムとなる。

[2]人的構成の層

人的セキュリティコントロールの観点で、重要システムを取り扱う人員に対し階層的に指揮命令や教育、演習を行き届かせることにより、人的側面が起点となるサイバー攻撃を受けにくいシステムとする。また、サイバー攻撃を受けた場合の緊急時対応/復旧をこのような人員を確保し実施することにより、最終的には手動で対応することで、緊急待避的なサービスの維持を可能とする。

多層防御を行う際の具体的課題としては、2.4.1 でのポイントを踏まえ、次にあげる事項への対応が挙げられる。

[1] システム構成の層に関する課題

サイバー攻撃を受けにくい構成の多くは、独自システムによる構成の維持、「インターネットへ接続したシステム」とは分離した環境に置くことであった。しかしながら今後重要システム及びそれに

付随する周辺装置において、オープンシステム化が進むことは避けられないと考えられる。歴史的に独自システムだったシステムも、それ自体がオープンシステム上やインターネット接続が前提で設計される状況となり、”独自“を維持することは困難になると考えられる。

また、USB ストレージを利用したサイバー攻撃に見られるように、サイバー攻撃の経路の多様化により「インターネットへ接続したシステム」と分離した環境に置くことのみでは重要システムを守る事は困難になると考えられる。

重要であるのは、システム構成上、独自システムであったり、インターネットと分離した環境に置いているために、サイバー攻撃を受ける可能性はないと考える事の妥当性は無いということである。つまり、どの様な構成であっても攻撃を受ける可能性は常にあることを認識することである。組織に見合った対策を常に検討する様な体制を持ち、2.2.2(6)で示した「新しいタイプの攻撃」に備えるべく、物理的・システム技術的・運用技術的の様々な角度から防御をし、管理徹底することで、攻撃を受けても重要インフラサービスを継続させる環境を備えることが必要である。

[2] 人的構成の層に関する課題

人員の管理について、2.4.1 の有識者ヒアリングでも指摘されているように、今後、要員モラルの低下や、教育の行き届いていない委託先に重要操作を依頼する等により、堅ろう性が保てなくなるといった課題が考えられる。

人的階層管理の範囲を正規社員の管理に加え、サプライチェーンを構成する委託・再委託先人員、研究員(留学生、インターンシップ生)人員についても、適正配置、教育、演習を実施し、技術やモラルを維持向上させることが、重要インフラサービス維持の為の重要の鍵になると言える。また、重要サービスが完全に停止してしまうという危機的状況を回避するために、手動操作を担う人員の確保も重要であると言える。

これら課題解決後に各重要インフラ事業者が運用フェーズに入る前に、多層防御の管理状況・対策状況が有効であることを計る為のメジャーのあり方について検討する必要がある。

3. 重要インフラの事業継続計画（BCP）の在り方に関する調査

本調査の目的（1.（2）参照）より、システムの堅ろう性は、事業継続計画（Business Continuity Plan：BCP）※に基づく情報システムの安定的な運用ができるかどうかによっても大きく影響されると考えており、本章では、情報システムの安定運用の視点から見た BCP の課題についても基礎的な情報収集及び分析を行った結果を示す。

なお、日本国内における、BCP の動向、ガイドライン等、BCP で求められている要件、実際に策定・運用されている BCP 事例を調査した結果を 3.1 に、比較の対象として海外における、BCP の動向、ガイドライン等、BCP で求められている要件、実際に策定・運用されている BCP 事例を調査した結果を 3.2 に示す。また、BCP の実効性の検証を目的として行われている国内外の BCP 演習について調査した結果を 3.3 に示す。3.1～3.3 の結果をもとに、我が国の BCP に関する課題をまとめたものを 3.4 に示す。

※事業継続計画（Business Continuity Plan：BCP）とは、企業が自然災害、大火災、テロ攻撃等の緊急事態に遭遇した場合において、事業資産の損害を最小限にとどめつつ、中核となる事業の継続あるいは早期復旧を可能とするために、平常時に行うべき活動や緊急時における事業継続のための方法、手段等を取り決めておく計画のこと。[24]

3.1 日本国内の BCP 動向

3.1.1 BCP 普及状況

本節では内閣府により平成 21 年度に実施された「企業の事業継続及び防災の取組に関する実態調査[25]」の結果に基づき、国内事業者の BCP 策定状況について概観する。

（1）BCP 策定率

大企業では、28%が「策定済み」であり、「策定中」(31%)を加えると 58%となる。中堅企業では、「策定済み」が 13%であり、「策定中」(15%)を加えると、3 割程度の水準にとどまっている。さらに「策定予定なし」が 10%、「BCP を知らない」が 45%にも及んでいる。

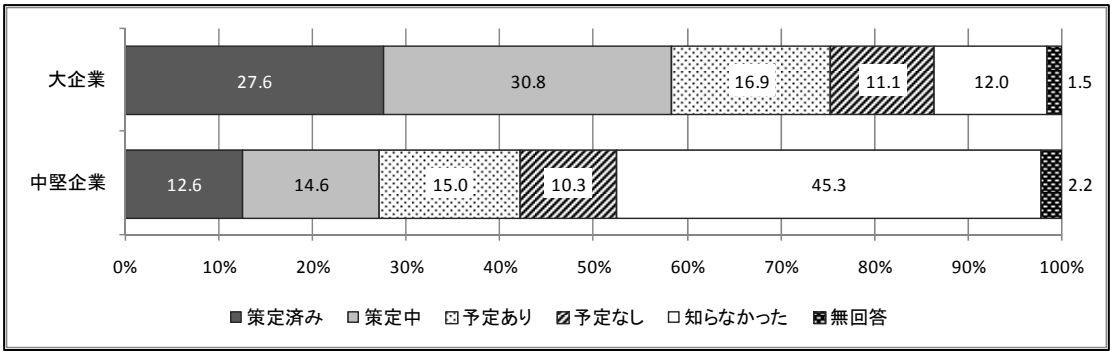
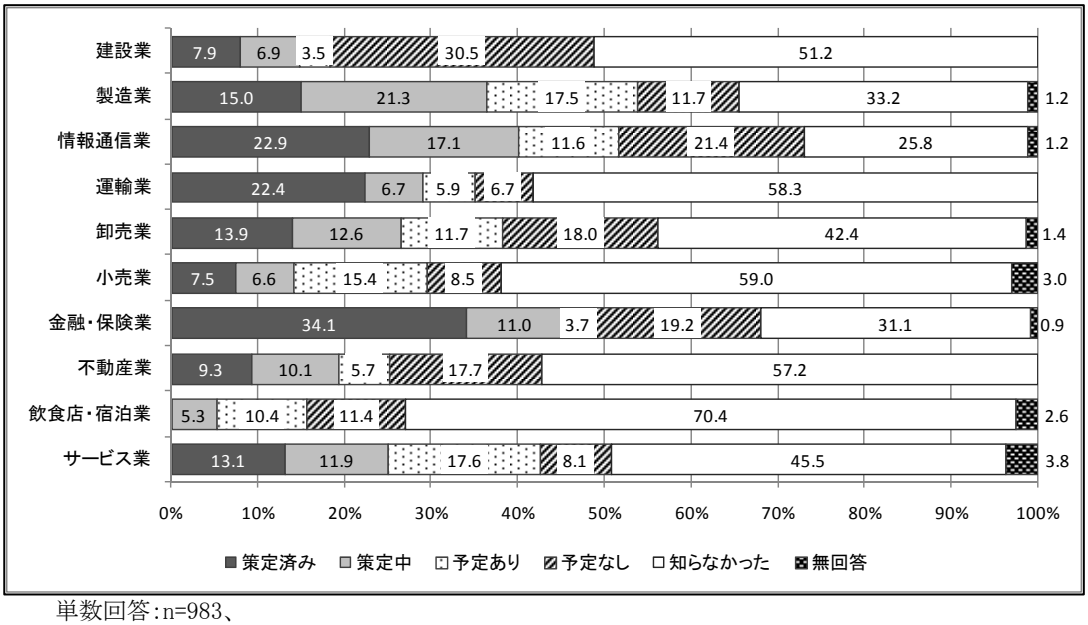


図 2.BCP の策定状況

[24] http://www.chusho.meti.go.jp/bcp/contents/level_a/bcpgl_01_1.html
[25] http://www.bousai.go.jp/kigyoubousai/topics/100330-2.pdf

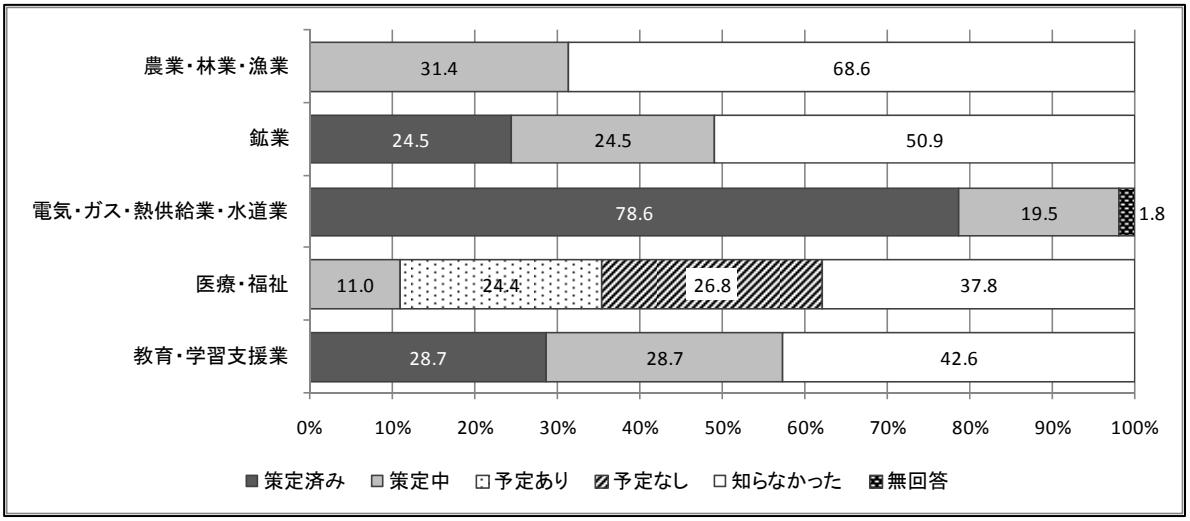
(2) 業種別 BCP の策定率

業種別では金融・保険業が BCP の策定が最も進んでいる。これは監督官庁からの指導による影響が大きいものと考えられる。その他、情報通信業、運輸業等で策定が進んでいる。なお、回答数が少なかったため参考値との位置づけではあるが、電気・ガス・熱供給・水道業等の社会インフラ事業者においても BCP の策定が進んでいる状況がうかがえる。



単数回答:n=983、
対　　象:建設業、製造業、情報通信業、運輸業、卸売業、小売業、金融・保険業、不動産業、飲食店・宿泊業、サービス業に該当する企業

図 3.業種別 BCP の策定状況



単数回答:n=983、
対　　象:建設業、製造業、情報通信業、運輸業、卸売業、小売業、金融・保険業、不動産業、飲食店・宿泊業、サービス業に該当する企業

図 4. 業種別 BCP の策定状況(参考値)

(3) BCP 策定時の問題点・課題

BCP の実効性向上のための阻害要因として、現場の意識の低さ、部署間・サプライチェーン企業との連携の困難さ、策定のためのリソース確保の困難さ、ノウハウ・スキル獲得の困難さ、等があがっている。

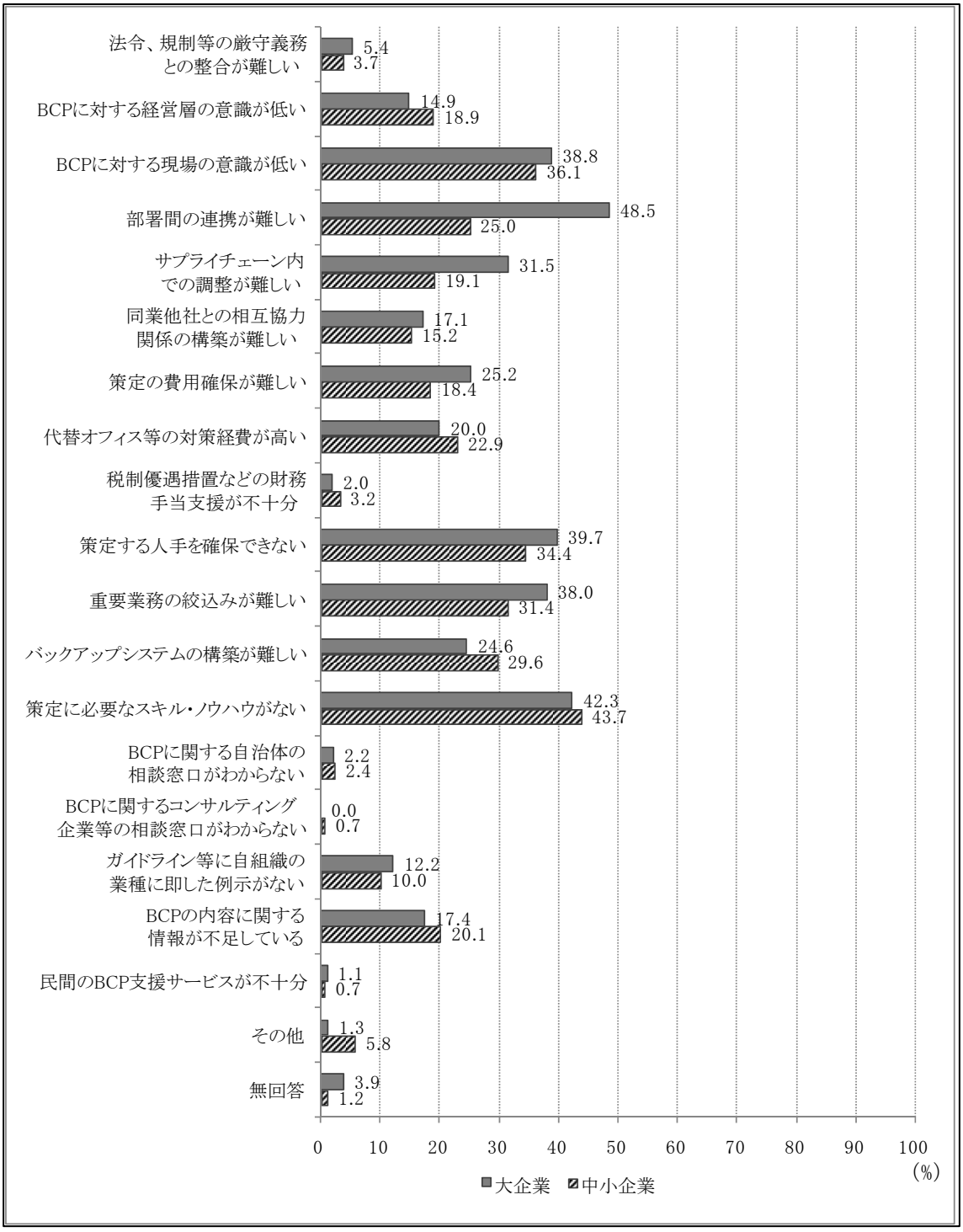


図 5. BCP 策定時の問題点・課題

(4) BCP の未策定理由

BCP 未策定の理由として、法令・規制がないこと、策定のためのリソースやノウハウ・スキルの獲得が困難であること等が挙げられている。

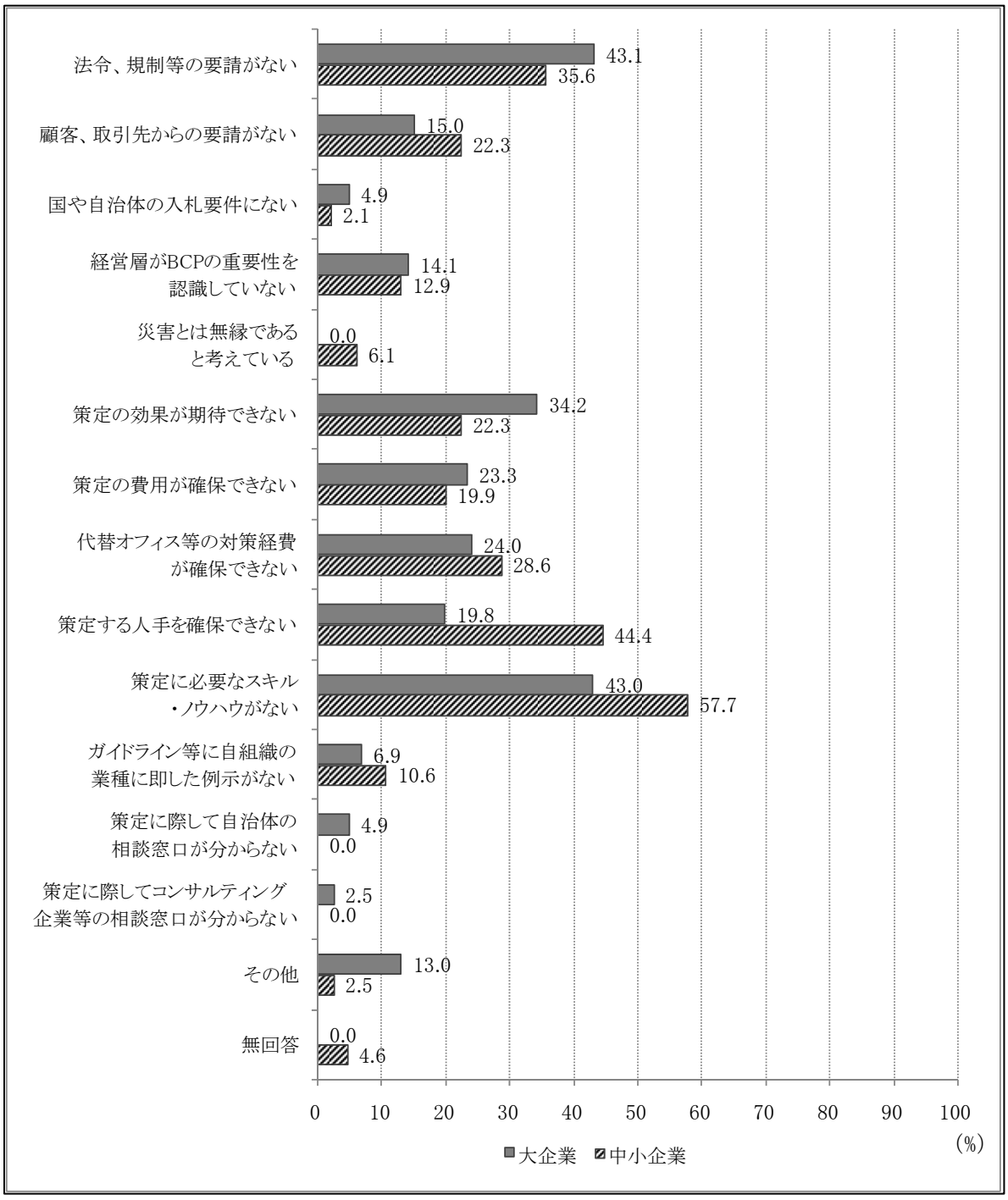


図 6. BCP の未策定理由

(5) 災害発生時の製品・サービスの供給確保実施状況

大規模災害等を想定した場合、事業の継続にはサプライチェーンの取引先や同業他社との協調が欠かせないが、外部組織との連携についてほとんど対策が講じられていない状況がうかがえる。

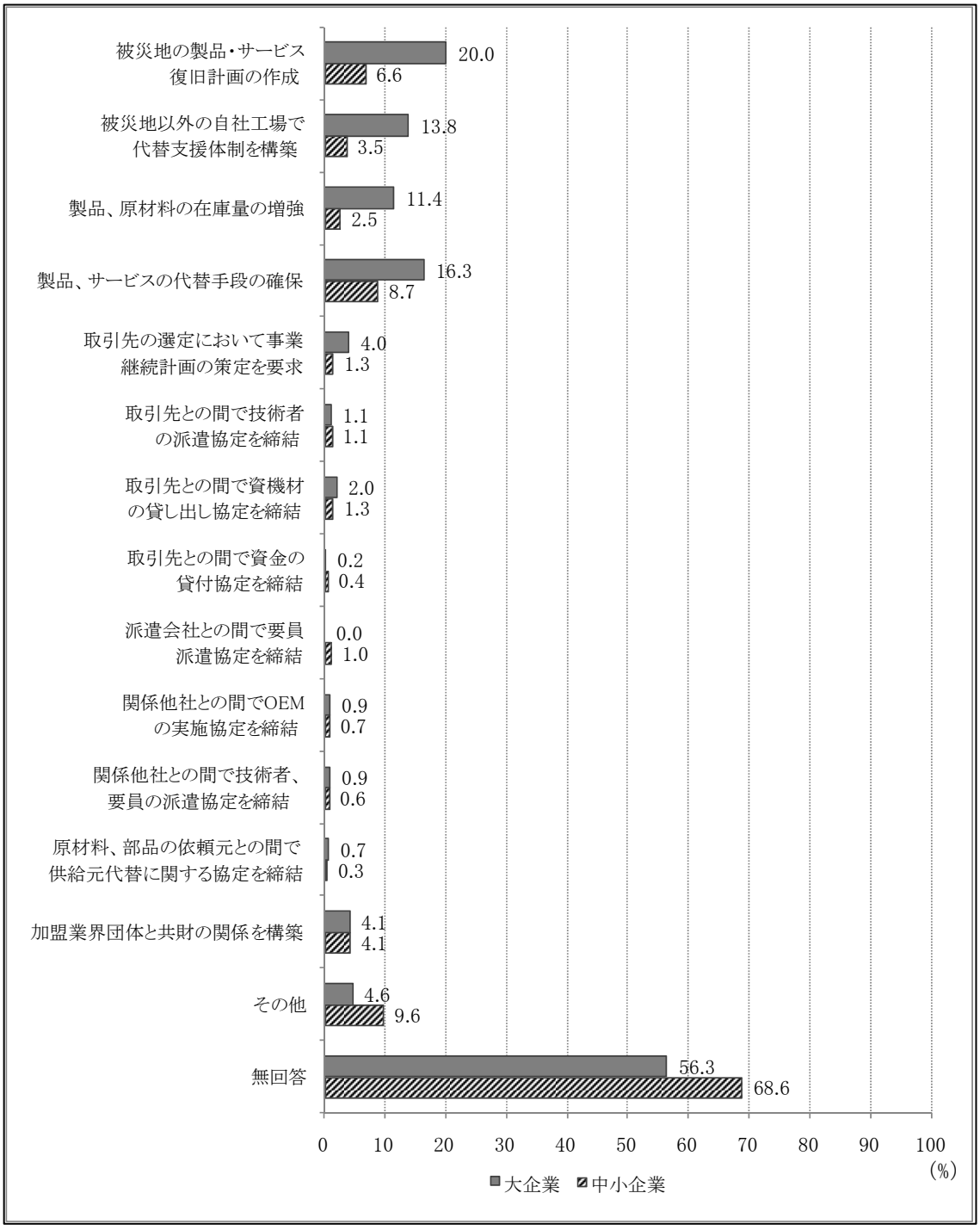


図 7. 災害発生時の製品・サービスの供給確保実施状況

(6) BCP の対象リスク

対象リスクとして、新型インフルエンザ、地震、火災等を想定した BCP を策定している企業が多い。しかしながらいずれも策定率は 50%未満である。また、システム障害、交通の遮断、テロ、停電、要員の喪失、水害、風評等多くの欧米企業が対象としているリスクに対して、日本企業では対策が進んでいない可能性がある。

表 8. BCP の対象リスク

	地震				
	策定済みである	策定中である	予定がある	予定はない	無回答
大企業	35.8	32.6	27.5	2.3	1.8
中堅企業	28.4	22.8	36.6	6.8	5.4
全体	33.0	24.0	32.6	5.9	4.5
その他企業	34.7	19.3	32.8	7.6	5.6

	水害				
	策定済みである	策定中である	予定がある	予定はない	無回答
大企業	14.4	11.0	18.2	44.4	12.0
中堅企業	10.2	5.5	24.4	36.7	23.2
全体	12.7	7.5	19.3	38.0	22.6
その他企業	13.5	6.7	16.2	34.8	28.8

	風害				
	策定済みである	策定中である	予定がある	予定はない	無回答
大企業	11.8	9.2	11.0	51.7	16.3
中堅企業	6.3	4.9	15.3	45.6	27.8
全体	10.0	8.2	11.6	44.2	25.9
その他企業	11.5	10.1	9.4	38.4	30.6

	雪害				
	策定済みである	策定中である	予定がある	予定はない	無回答
大企業	7.7	5.0	6.7	60.9	19.6
中堅企業	4.2	2.7	11.0	51.3	30.8
全体	6.0	4.9	8.0	54.1	27.0
その他企業	6.2	6.4	6.6	51.9	28.9

	火災				
	策定済みである	策定中である	予定がある	予定はない	無回答
大企業	24.3	18.3	26.7	24.4	6.3
中堅企業	26.5	11.3	29.1	16.9	16.1
全体	26.8	15.4	27.9	17.6	12.4
その他企業	28.5	16.5	27.7	13.7	13.5

	新型インフルエンザ				
	策定済みである	策定中である	予定がある	予定はない	無回答
大企業	45.6	30.9	18.7	3.5	1.3
中堅企業	42.4	29.8	22.0	2.6	3.2
全体	45.4	25.5	20.6	4.0	4.5
その他企業	47.5	19.0	20.9	5.3	7.4

3.1.2 金融業界の動向

3.1.2.1 日本銀行・金融庁の取組状況

金融業界では日本銀行、金融庁を中心として、被災地等における住民生活及び経済活動の維持を目的に、BCP の普及促進が他業種に先駆けて進められている。本節では日本銀行及び金融庁の取組状況を中心に、金融業界の動向をまとめる。

下表に記載の通り日本銀行からは、2002 年頃から BCP に関する情報発信が始まり、2003 年 7 月には「金融機関における業務継続体制の整備について」という指針的な文書が公表された。この中で、日本の金融機関は既に何らかの業務継続体制を構築しているものの、その実態は個別の業務システムや拠点単位の被災に焦点を当てたものにとどまっていると指摘されており、「被災地等における住民の生活や経済活動の維持」「経済面での混乱拡大の抑制」「金融機関経営におけるリスクの軽減」の3つが BCP 整備の意義として掲げられている。

また 2008 年 5 月には「業務継続体制の実効性確保に向けた確認項目と具体的な取組事例―先進事例を中心に」という金融機関における先進的な具体事例を集めた文書(その後 2010 年に増補改定)が公表された。金融機関では当該文書の記載項目が日銀考査での事実上の確認項目として認識され、取組が進められた。

さらに、2009 年 2 月には、日銀主催の金融高度化セミナー「新たな業務継続計画 新型インフルエンザ対策」が開催され、金融機関各社のみならず現金輸送業者等の関連事業者も参集し、BCP の観点から新型インフルエンザ対策の課題が議論された。

表 9. 日本銀行が公表した金融機関の業務継続体制に関係する資料一覧[26]

発行日	タイトル
2002年3月	金融機関の拠点被災を想定した業務継続計画のあり方
2003年2月	緊急時における業務継続・復旧体制に関するアンケート調査結果について
2003年7月	金融機関における業務継続体制の整備について
2006年9月	金融高度化セミナー「金融機関における業務継続体制の高度化に向けて」
2007年3月	業務継続体制の整備状況に関するアンケート(2006 年12 月)調査結果
2008年3月	金融機関における新型インフルエンザ対策の整備について ―内外金融機関の取組事例の紹介
2008年5月	業務継続体制の実効性確保に向けた確認項目と具体的な取組事例 ―先進事例を中心に
2008年6月	業務継続体制整備の具体的な手法 ―「業務継続体制整備に関する情報交換会」における議論の内容と工夫事例
2009年2月	業務継続体制の整備状況に関するアンケート(2008 年11 月)調査結果
2009年4月	金融高度化セミナー「新たな業務継続計画 新型インフルエンザ対策」(2009年2月実施)
2010年3月	バックアップ・コンピュータセンターの実効性確保にかかる課題と対応策
2010年3月	海外における「ストリートワイド訓練」の概要 ―業務継続計画の実効性確認手段としての業界横断的訓練
2010年3月	業務継続体制の実効性確保に向けた確認項目と具体的な取組事例 (増補改訂版)

[26]日本銀行ホームページを基に作成
http://www.boj.or.jp/research/brp/ron_2010/index.htm/

2010年3月に公表された日銀の考査実施方針では、BCPの十分性、整合性を含めた実効性について検証を行うとともに、BCPを策定するのみならずPDCAサイクルが機能的に行われているかについて、詳細な確認がなされることが記載されている。また、病原性の高い新型インフルエンザ流行に備えた対策内容が、確認項目として挙げられている。

◆日本銀行「2010年度の考査の実施方針等について(一部抜粋)」[27](2010年3月)

(業務継続体制の整備)
業務継続体制の整備は、各金融機関の業務上の課題としてのみならず、わが国決済システムの円滑な運行という観点からも重要である。考査では、金融機関に対して、業務継続体制の整備と実効性確保をさらに促していく。特に、決済面におけるプレゼンスが大きい先については、業務継続計画の内容の十分性や整合性、経営資源の確保を含めた実効性について検証を行うとともに、業務継続体制整備に関するPDCAサイクルの機能度を確認する。その他の金融機関についても、業務内容や地域におけるプレゼンス等を踏まえた検証を行い、必要な助言を行う。また、病原性の高い新型インフルエンザ流行に備えた体制整備について、重要業務の絞込みや要員面を中心に点検する。

金融庁の監督方針においても、新型インフルエンザや地震等に備えた業務継続態勢の構築が求められている。

◆金融庁「平成22事務年度 主要行等向け監督方針(一部抜粋)」[28](平成22年8月)

4. 顧客保護と利用者利便の向上
(5)業務の継続性の確保
金融機関のシステムは業務運営の根幹をなすインフラであり、システムの高度化・複雑化に伴い、システム障害の発生による顧客取引への影響は益々大きなものとなっている。主要行等が金融システムにおける中核的な役割を担っていることを踏まえ、各行におけるシステムの継続性について、経営陣による主導性とコミットメントの下で、適切なリスク管理が図られているか確認する。また、新型インフルエンザの流行や地震等に備えた業務継続態勢が構築されているかについても確認する。

金融業界では、地震・水害等の大規模災害が発生した際には、金融当局から出される通達に従い業務を継続する必要がある。以下に、平成 20 年に発生した岩手・宮城内陸地震の際に、金融当局から被災地の金融機関向けに出された通達を掲載する。金融機関では被災地における必要最低限の金融サービスの提供のために、通帳や印鑑の紛失等災害発生時に想定される様々な事象への対応のための準備が、監督官庁からの要請を受けてなされていることが分かる。また、情報システムに頼らない手作業での業務の継続手段も確保されている。

◆「平成20年岩手・宮城内陸地震」にかかる災害に対する金融上の措置について[29](宮城県)

27 http://www.boj.or.jp/finsys/exam_monit/exampolicy/kpolicy10.pdf
28 http://www.fsa.go.jp/news/22/20100827-2/02.pdf
29 http://www.boj.or.jp/announcements/release_2008/fso0806b.htm/

◆金融機関(銀行、信用金庫、信用組合等)への要請
(1)預金証書、通帳を紛失した場合でも預金者であることを確認して払戻しに応ずること。
(2)届出の印鑑のない場合には、拇印にて応ずること。
(3)事情によっては、定期預金、定期積金等の期限前払戻しに応ずること。また、これを担保とする貸付にも応ずること。
(4)今回の災害による障害のため、支払期日が経過した手形については関係金融機関と適宜話し合いのうえ取立ができることとすること。
(5)災害時における手形の不渡処分について配慮すること。
(6)汚れた紙幣の引換えに応ずること。
(7)国債を紛失した場合の相談に応ずること。
(8)災害の状況、応急資金の需要等を勘案して融資相談所の開設、審査手続きの簡便化、貸出の迅速化、貸出金の返済猶予等災害被災者の便宜を考慮した適時的確な措置を講ずること。
(9)休日営業又は平常時間外の営業について適宜配慮すること。また、窓口における営業が出来ない場合であっても、顧客及び従業員の安全に十分配慮した上で現金自動預払機等において預金の払戻しを行う等災害被災者の便宜を考慮した措置を講ずること。
(1)～(9)にかかる措置について実施店舗にて店頭掲示を行うこと。
営業停止等の措置を講じた営業店舗名等、及び継続して現金自動預払機等を稼動させる営業店舗名等を、速やかにポスターの店頭掲示等の手段を用いて告示するとともに、その旨を新聞やインターネットのホームページに掲載し、取引者に周知徹底すること。

3.1.2.2 金融機関の BCP 普及状況

本節では、日本銀行により金融機関に対して2008年11月に実施された「業務継続体制の整備状況に関するアンケート[30]」の結果に基づき、前節までに述べた日本銀行、金融庁の活動により取組が進んだ金融業界の BCP の普及状況ついて示す。

表 10. アンケート調査対象

	2008 年調査（第 4 回）		2006 年調査（第 3 回）		2004 年調査（第 2 回）		2002 年調査（第 1 回）	
回収期間	2008 年 10～11 月		2006 年 12 月～2007 年 2 月		2004 年 9～11 月		2002 年 8～10 月	
回収率	100%		100%		100%		100%	
	先数	構成比(%)	先数	構成比(%)	先数	構成比(%)	先数	構成比(%)
大手銀行	12	14.3	12	14.3	12	16.3	14	20.6
地域金融機関	17	20.2	16	19.0	16	18.6	10	14.7
国内証券	10	11.9	10	11.9	13	15.1	13	19.1
外国銀行・外国証券	29	34.5	32	38.1	26	30.2	16	23.5
その他(注)	16	19.0	14	16.7	17	19.8	15	22.1
合計	84	100.0	84	100.0	86	100.0	68	100.0

(注)系統金融機関、短資、証券系信託銀行、資産管理系信託銀行等

[30] http://www.boj.or.jp/research/brp/ron_2009/data/ron0902a.pdf

(1) BCP 策定率

大手金融機関を中心に84社を対象とした本調査では、86%の企業がBCPの整備を完了し、定期的な見直しも行っているとの結果であった。また日本銀行、金融庁からの働きかけにより年々BCPの普及が進んでいる状況が伺える。

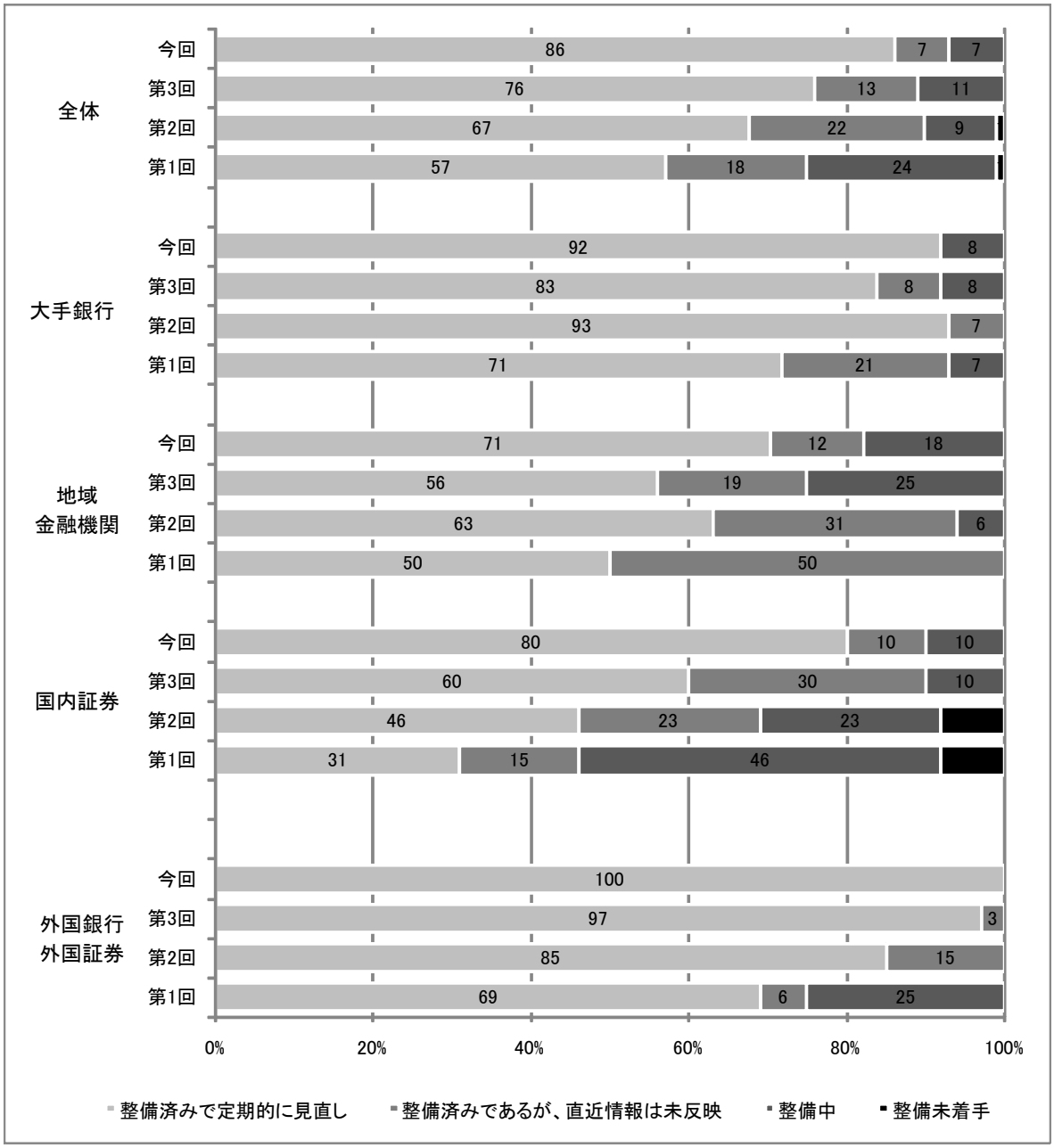


図 8. 全社的な業務継続体制の整備状況

(2) 実効性の確保状況

BCPの策定率が高い水準に達している一方で、想定するリスクが顕在化した場合に実際にBCPが機能するかという観点から、「BCP のフィージビリティが確保されている」と回答した先は、全体の 38%にとどまっている。ただし、2年前の前回調査よりは、その数は全ての業態において上回っており、日

本銀行ではその要因として、バックアップ用オフィスの整備、マニュアルの習熟、訓練とその結果を踏まえた見直し等が進んだことをあげている。

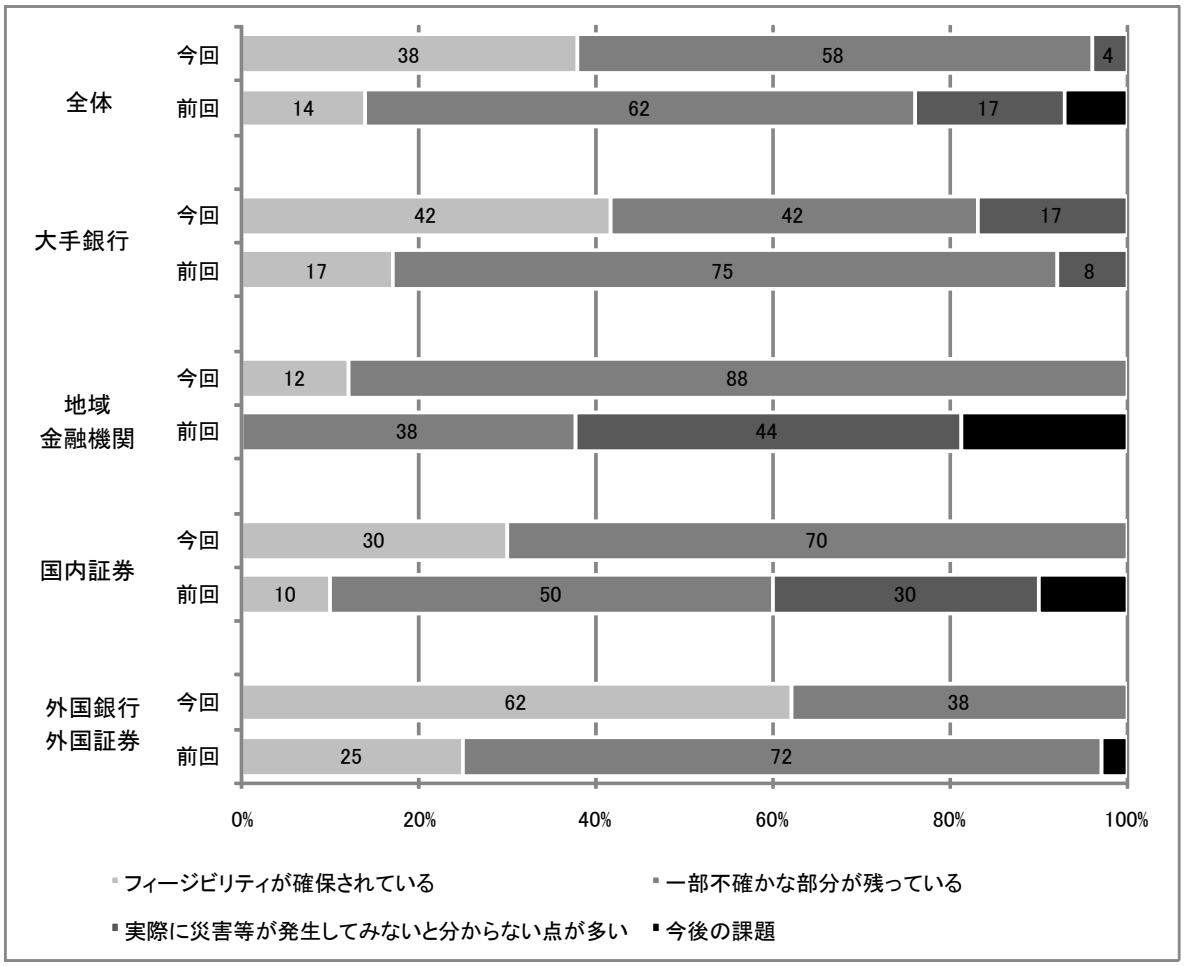


図 9. 業務継続の実効性確保状況

(3) 想定するリスク要因

BCP で想定するリスク事象として、地震、自社システムの大規模障害、火災・漏水等、風水害、感染症等を挙げる企業が多かった。サイバーテロを対象リスクとしている企業は 65%であった。

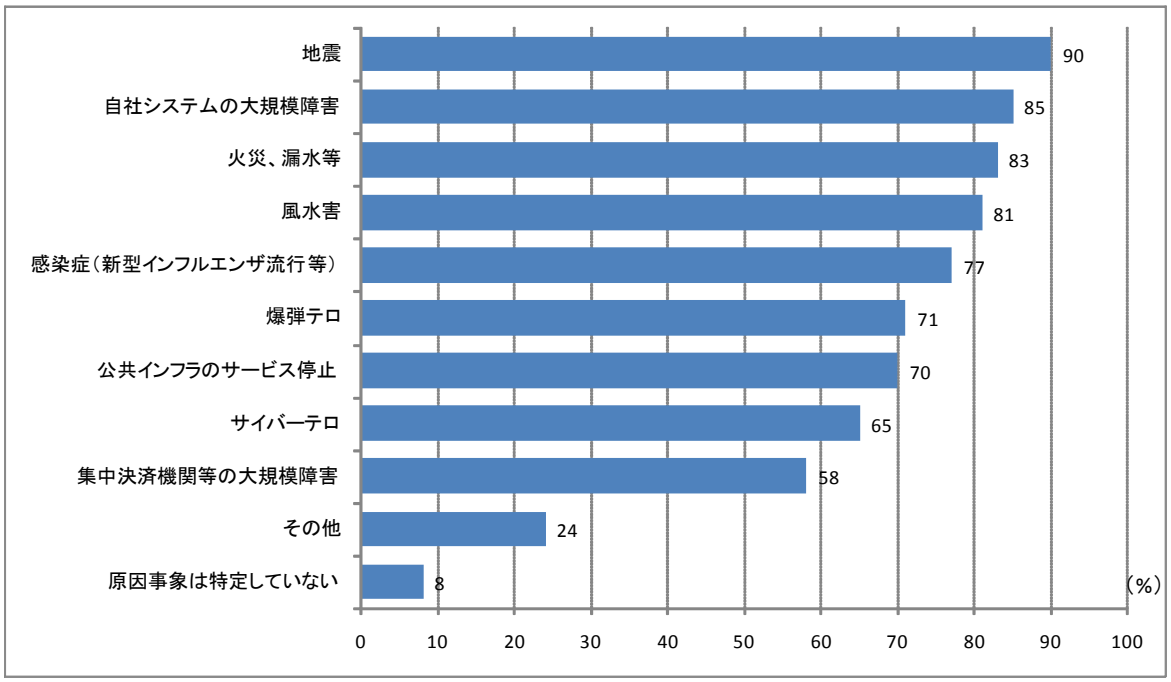


図 10. 被災シナリオの原因事象(複数回答)

(4) 訓練内容

実施されている訓練の内容をみると、ほとんどの企業が「システム部門におけるバックアップ・センター切替訓練」を実施している。このほかにも各種の参集訓練や手作業訓練、社内横断的な訓練がそれぞれ半数程度の企業で実施されていた。なお、グループ内企業による共同訓練を実施している企業は 39% にとどまった。

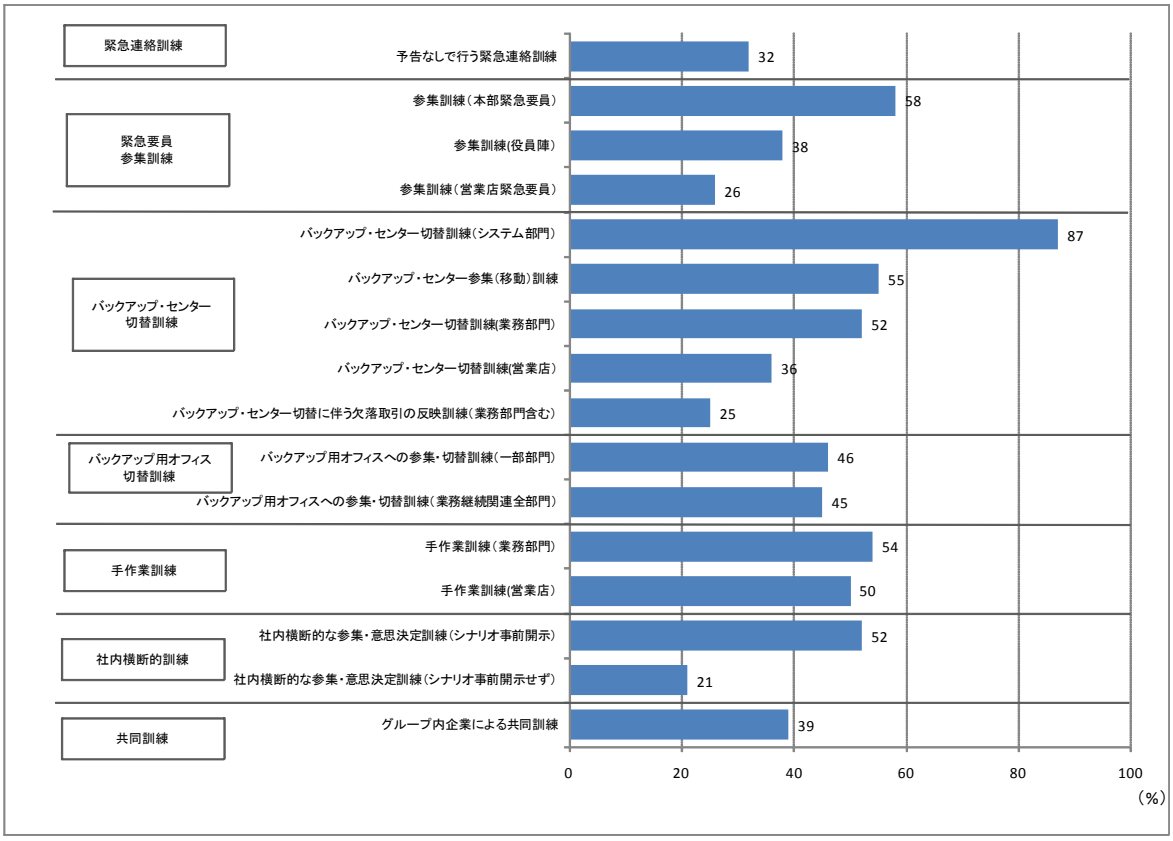


図 11. 実施したことのある訓練

3.1.3 日本の BCP に関するガイドライン等

日本の BCP に関する政策やガイドライン等について、インターネット上で公開されている情報、書籍等を対象に、重要インフラ事業者が参考とすべき政策やガイドライン等のうち、特に官公庁が発行したものを調査した。その結果を表 11 に示す。

表 11. 日本の BCP に関するガイドライン等

項番	文書名	発行機関	発行月	対象組織	想定している脅威(概要)		
					災害	疾病	IT脅威
1	事業継続計画(BCP)策定ガイドライン[31]	企業における情報セキュリティガバナ	平成 17 年 3 月	企業一般	―	―	○

[31] http://www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide.pdf

項番	文書名	発行機関	発行月	対象組織	想定している脅威(概要)		
					災害	疾病	IT脅威
		ンスのあり方に関する研究会 経済産業省					
2	先進企業から学ぶ事業リスクマネジメント実践テキスト[32]	経済産業省	平成17年3月	リスクマネジメントに着手しようとしている企業一般	○	○	○
3	事業継続ガイドライン第二版 －わが国企業の減災と災害対応の向上のために－[33]	事業継続計画策定促進方策に関する検討会 内閣府 防災担当	平成21年11月 (初版は平成17年8月)	企業一般	○	－	－
4	中小企業BCP策定運用指針 第1版 －どんな緊急事態に遭っても企業が生き抜くための準備－[34]	経済産業省中小企業庁	平成18年2月	中小企業	○	－	－
5	中央省庁業務継続ガイドライン 第1版 ～首都直下地震への対応を中心として～[35]	内閣府 防災担当	平成19年6月	中央省庁	○	－	－
6	地方公共団体におけるICT部門の業務継続計画(BCP)策定に関するガイドライン[36]	総務省	平成20年8月	地方公共団体のICT部門	○	－	○
7	IT サービス継続ガイドライン[37]	経済産業省	平成20年9月	企業一般のITサービス	－	－	○
8	中小企業 BCP 策定運用指針を用いた新型インフルエンザ対策	経済産業省中小企業庁	平成21年3月	中小企業	－	○	－

32 http://www.meti.go.jp/policy/economic_industrial/report/downloadfiles/g50331i00j.pdf
33 http://www.bousai.go.jp/MinkanToShijyou/guideline02.pdf
34 http://www.chusho.meti.go.jp/bcp/download/bcppdf/bcpguide.pdf
35 http://www.bousai.go.jp/jishin/gyomukeizoku/pdf/gyoumu_guide_honbun070621.pdf
36 http://www.soumu.go.jp/menu_news/s-news/2008/pdf/080821_3_bt1.pdf
37 http://www.meti.go.jp/press/20080903001/02_it_gl.pdf

項番	文書名	発行機関	発行月	対象組織	想定している脅威(概要)		
					災害	疾病	IT脅威
	のための中小企業BCP(事業継続計画)策定指針[38]						
9	新型インフルエンザ対応 中央省庁業務継続ガイドライン[39]	新型インフルエンザ及び鳥インフルエンザ等に関する関係省庁対策会議	平成21年8月	中央省庁	ー	○	ー

表 11 に示すガイドライン等の概要については、以下の通りである。

(1) 事業継続計画(BCP)策定ガイドライン(表 11 の項番1)

[発行機関: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、経済産業省]

- BCP の構築を検討する企業にとって、考え方の理解を促すガイドラインという位置付けであり、また IT 依存度が高まっていることを受け、IT 事故を主に想定したものである。基本的考え方、総論、策定にあたっての検討項目、個別計画の4つの章と、参考資料から構成され、具体的な計画の構築手順を説明している。
- 3.2.4 で述べる、ISO/PAS 22399 策定プロセスの、国際規格原案作成にあたり、日本からインプットする情報作成時に国内において参照された文書。

(2) 先進企業から学ぶ事業リスクマネジメント実践テキスト (表 11 の項番 2)

[発行機関:経済産業省]

- 近年企業経営の重要な課題となっている「リスクマネジメント」について、各企業の取組を促進するため、先進的な取組みを行っている企業17社の事例を踏まえたテキストであり、これからリスクマネジメントに着手しようとしている企業を対象とし、これらの企業がリスクマネジメントに組織的に取組んでいく際に必要となる知識の提供を目指したものである。
- 危機的な事態が生じるのは地震や台風等の自然災害による場合もあれば、火災や情報システムダウン等の事故による場合もあり、更には業務上のミスや不祥事による場合もあるとしている。BCP の先進企業例では、今日の事業活動における IT システムへの依存度が飛躍的に高まっており、システム面から見た事業継続計画が不可欠になっていることから、IT システムにおける BCP を取り上げている。

(3) 事業継続ガイドライン第二版 ーわが国企業の減災と災害対応の向上のために(表 11 の項番 3)

[発行機関:事業継続計画策定促進方策に関する検討会、内閣府 防災担当]

- 日本企業に対して事業継続の取組みの概要及び効果を示し、防災のための社会的な意義や取引における重要性の増大、自社の受けるメリット等を踏まえて企業が自主的に判断するのを促すものとして策定された。ガイドラインの構成は「ポイント、事業継続の必要性と基本的考え方、事業継続計画及び取組みの内容、経営者及び経済社会への提言」から成

[38] http://www.chusho.meti.go.jp/bcp/influenza/download/bcpshingatainful_all.pdf
[39] http://www.cas.go.jp/jp/seisaku/ful/dai23/siryou2_2.pdf

る。

- 事業継続の取組みが有効なビジネスリスクには、大きく分けて、突発的に被害が発生するもの（地震、水害、テロ等）と段階的かつ長期間に渡り被害が継続するもの（新型インフルエンザを含む感染症、水不足、電力不足等）があるが、このガイドラインでは、主として突発的に被害が発生するリスクのうち特に自然災害を想定した記述をしている。さらに、想定される災害リスクとして、日本企業にとって想像がつきやすく、対峙すべき最も大きな自然災害リスクである地震を想定リスクとして、社内の取組みをスタートさせることを推奨している。
- 3.2.4 で述べる、ISO/PAS 22399 策定プロセスの、国際規格原案作成にあたり、日本からインプットする情報作成時に国内において参照された文書。

(4) 中小企業BCP策定運用指針 第1版 －どんな緊急事態に遭っても企業が生き抜くための準備－（表 11 の項番 4）

[発行機関:経済産業省中小企業庁]

- 日本では地震、台風、集中豪雨等の自然災害が毎年多発し、多くの中小企業が直接間接の被害を被っており、被災による中小企業の事業中断は、そのまま廃業や倒産に直結しかねない深刻な事態である。また被災地の地域経済にも大きな打撃を与えている。
- 経済産業省中小企業庁は、災害に対する有効な事前対策として、中小企業へのBCPの普及浸透が必要であると考えている。中小企業の経営者自身が、緊急時に会社がどういう状況になり、どう行動すべきか、イメージを筋道立てて検討し、事前に対策を整理しておくことで、企業が緊急時に生き抜くための手助けをしようと策定されたもの。
- 国内企業数の 99%を占め国家経済の根幹をなす中小企業に BCP を普及浸透することによって、不測の緊急事態にあっても活動を止めない強靭な経済社会基盤の構築を目指している。
- この指針は、中小企業が投入できる時間と労力に応じて、「平常時における BCP の策定と運用」、「財務診断モデル」は、基本・中級・上級コースの 3 コースに分けて策定されている。また、共通項目として、「緊急時における BCP の発動」「事前対策メニュー一覧」「BCP 様式類」が用意されている。

(5) 中央省庁業務継続ガイドライン 第1版 ～首都直下地震への対応を中心として～（表 11 の項番 5）

[発行機関:内閣府 防災担当]

- 首都直下地震が発生した場合、発災地が首都地域であることから中央省庁も被災することが予想されるが、中央省庁は、平常時から国家機能、国民生活及び経済活動等に係る重要な業務を担っている組織でもあることから、被災した場合でも、一定範囲の通常業務はその継続が強く求められる。
- そのため、中央省庁には、応急業務及び継続の必要性の高い通常業務（このガイドラインでは、「非常時優先業務」といっている）について、業務継続（継続又は早期の再開若しくは実施）のために必要な資源が、共に適切に確保されていることが求められる。
- 内閣府防災担当発行の「首都直下地震対策大綱」及び「首都直下地震応急対策活動要領」において、BCP の策定が施策として位置付けられたこともあり、このガイドラインは、このような既往の決定や中央省庁の業務継続への社会的要請を踏まえ、各省庁が業務継続力の向上を図るための計画（業務継続計画）を作成する際の作業を支援することを目的とし、その計画に盛り込む内容や計画策定手法等についてまとめたものである。基本的な対象事象は首都直下地震としている。

(6) 地方公共団体におけるICT部門の業務継続計画(BCP)策定に関するガイドライン(表 11 の項番 6)

[発行機関:総務省]

- 地方公共団体は、災害時において、地域住民の生命、身体の安全確保、被災者支援、企業活動復旧のために、災害応急業務、復旧業務及び平常時から継続しなければならない重要な業務を実施していく責務を負っている。
- 昨今においてはこれらの業務の継続を確保するためには、情報システムがまさに必要不可欠であり、災害時に情報システムが稼働していることは極めて重要である。そのため、役所の業務全体において業務継続計画を策定する動きが未だなくても、率先して「情報システムに関する業務継続計画」を策定し、業務の継続力を高めていかなくてはならない。
- 情報システムは、平常時からの業務継続の備えがないと、被害を受けてからの事後的な復旧に多くの時間を要してしまう特性が強い。また、住民情報等を失い、その回復に多くの時間を要してしまえば、甚大で回復困難な影響を住民・企業に生じさせてしまう。かかる観点からも、業務継続計画の策定の必要性が高い典型的な部門であり、先行して業務継続力をつけることの価値は大きい。
- 以上のような問題意識を踏まえ、情報システムを所管するICT 部門のBCP策定に向けた地方公共団体の取組を支援するため策定されたものである。
- なお、このガイドラインは、対象を基本的には地方公共団体の情報システム・ネットワーク等に関する企画や統括管理をする部門(ICT 部門)とし、主たる対象事象を大地震をとしている。(大地震を前提とした場合、火災等の二次災害及び電力途絶等事態も想定して対処することが求められることや、施設・設備の損壊がテロ等の他の原因であっても対応が類似しており、応用が容易なためとされている)

(7) IT サービス継続ガイドライン(表 11 の項番 7)

[発行機関:経済産業省]

- 上記(1)の「事業継続計画(BCP)策定ガイドライン」では、事業継続計画の基本的な考え方から具体的な計画の構築手順までを解説したものであり、「情報セキュリティに絶対はなく、事故は起こりうるもの」との前提に立った上で、事業継続は企業の社会的責任にも関係する問題であるとの考えから策定したものである。
- しかし、「事業継続計画(BCP)策定ガイドライン」は、計画策定といったいわば高次の内容に焦点を絞っていることから、現場の立場から見た場合、同ガイドラインを使用することで高度な事業継続のための対策を直ちに策定できるとは限らないという一面があった。
- また、BCP を策定する企業の数は増加してはいるものの、未だその割合は十分とはいえない状況にある他、IT への依存性の増大もあり、事業継続の阻害要因として IT 関連のトラブルを挙げる企業の数は非常に多い。
- そこで、「事業継続計画(BCP)策定ガイドライン」の IT にかかる部分について、企業をはじめとするユーザ組織を念頭に実施策等を具体化するものとして策定に至ったものである。
- このガイドラインは、組織における IT サービスの企画、開発、調達、導入、運用、保守等に携わる部門や担当者が、事業継続マネジメント(BCM)に必要な IT サービス継続を確実にするための枠組みと具体的な実施策を示し、取組の実効性の向上を支援することを目的としている。

(8) 中小企業 BCP 策定運用指針を用いた新型インフルエンザ対策のための中小企業 BCP(事業継続計画)策定指針(表 11 の項番 8)

[発行機関:経済産業省中小企業庁]

・ 新型インフルエンザの大流行に対応した BCP を策定する際に、参考とすべき事項が記載されており、特に中小規模の企業が効率的に BCP を策定するためのガイド的内容となっている。上記(4)の基本コースの内容に添って解説されている。

(9) 新型インフルエンザ対応 中央省庁業務継続ガイドライン(表 11 の項番 9)
[発行機関:新型インフルエンザ及び鳥インフルエンザ等に関する関係省庁対策会議]

・ 政府の各部門においては、新型インフルエンザ発生時においても、当該対策を行うと共に通常業務を継続、維持することが求められる。具体的には、国としての意思決定機能を維持し、最低限の国民生活の維持、治安の維持、経済活動の調整・支援等に必要な業務を円滑に継続すると共に、関係機関や自治体、国民への情報提供や支援を混乱することなく適切に行うこと必要である。
・ 本ガイドラインは、上記ミッションを踏まえ、中央省庁がその機能を維持し必要な業務継続を行うために、新型インフルエンザ発生時に想定される社会・経済の状況やこれを踏まえた講ずべき措置を示し、各府省における適切な業務継続計画の策定を支援することを目的とし、策定されたものである。
・ なお、このガイドライン及びこれに基づく業務継続計画は、他の大規模感染症や広域の毒物被害等においても有用となるものとしている。また、テロや大事故の場合には、上記(5)を参考にした首都直下地震 BCP と、本ガイドラインに基づく新型インフルエンザ BCP の双方を参考にすることが望ましいとしている。

3.1.4 日本の BCP で求められている要件等

日本では地震や台風被害の発生率が高いことから、3.1.3 に示したように、事業継続ガイドライン等においては、地震や天災等に対する「災害対策」が主眼とされており、本調査の目的である「サイバー攻撃」をリスクとしてフォーカスしているガイドラインは殆ど見当たらなかった。ただし、昨今では業務の運用維持には必要不可欠ともいえる「IT サービス」の事業継続に関するガイドラインは、災害対策ガイドラインと対になる形で発行されている。

日本における事業継続マネジメントに対する第三者認証制度は、一般財団法人日本情報経済社会推進協会(JIPDEC)が BCMS 適合性評価制度を 2010 年 4 月より開始しており、認証基準は英国の「BS25999-2:2007」を採用している。

国際的な基準の動向については、3.2 章にて示すが、国際規格化に先立った公開仕様書として 2007 年に発行された「ISO/PAS22399」では、日本の国内規格「事業継続計画策定ガイドライン(経済産業省、2005 年発行)」、「事業継続ガイドライン一版(内閣府中央防災会議専門調査会、2005 年発行)」が参考規格として参照されている。

3.1.3 の調査結果を元に、重要インフラサービスの維持・継続に関わる重要システムの安定運用の視点で、必要だと考えられる取組を以下に示す。なお、主な対象ドキュメントとしては、以下は国際規格化への日本からのインプット作成時に参照された表 11 の項番 1「事業継続計画策定ガイドライン(経済産業省)」、及び表 11 の項番 3 の「事業継続ガイドライン二版(内閣府)」を主なガイドラインとして引用し、これら 2 つのガイドラインには無い有益と考えられる内容が他のガイドラインに含まれる場合にはそれらのガイドラインも引用する。

3.1.4.1 事業継続計画の推進体制

事業継続計画の推進体制を検討する際、策定、演習、計画の見直し(事業継続マネジメントシステ

ム）の繰り返しによる継続的改善を維持できること、実際の発動時に計画通りに対処できることの双方を考慮しなくてはならない。

(1) 推進組織

主なガイドラインでは次のように記されている。

≪事業継続計画策定ガイドライン（経済産業省）≫

BCP では、事業継続に係る組織内の様々な問題を取り扱うことから、原則すべての部署等の関係者がこれに関わることが必要となる。したがって、全社的横断組織（タスクフォース）を設けて対応することが有効である。中心的な構成メンバーとしては、人事・給与、総務（総務・施設関連）、財務・調達、経営、広報、法務、営業・マーケティング、製造、情報システム等の関係者を含むことが考えられる。

≪事業継続ガイドライン二版（内閣府）≫

対策は決して経営企画部門や総務部門といった一部の部門の対策に限られるものではなく、非日常的な様々な業務が発生するため、全社の各部門に、災害対策の横断組織を作ってもよい。

推進にあたっては、組織全体にかかる横断的組織を推進組織として立ち上げ、対応すべきであると記されている。また、重要インフラサービスの維持・継続にかかわる重要システムの安全運用の観点から、情報システム部門の関与が必須だと記されている。

(2) 経営陣

主なガイドラインでは次のように記されている。

≪事業継続計画策定ガイドライン（経済産業省）≫

組織として最終的な責任の所在を明確化するために、組織の経営陣の役割・責務を明記することが望まれる

なお、BCP 策定には、経営陣の関与・承認は必須であるので、タスクフォースのメンバーの中に経営陣を含めることもできるが、上位組織として経営陣等で構成する組織（例えば、リスク管理委員会、BCP 委員会等）を設ける場合もある。これにより、組織全体による支援が約束されることとなる。

≪事業継続ガイドライン二版（内閣府）≫

事業継続の取組みの推進や災害発生時の対応には、事業継続の組織体制の構築とその役割および指揮命令系統を明確にしておく必要がある。また、これら事業継続対応組織の責任者は、経営層の中から任命される必要がある

事業継続計画の推進や発動においては、経営陣の関与が必須だと記されている。

(3) 事業継続計画責任者

事業継続ガイドライン二版（内閣府）では追求されていないが、事業継続計画策定ガイドライン（経済産業省）では、推進組織と経営陣の間に次のような組織も設置すべきと記されている。

≪事業継続計画策定ガイドライン(経済産業省)≫

BCP責任者(BCマネージャー)の任命
BCP 策定には、多数の組織や要員が関与するが、最終的にはBCP 責任者がその取りまとめについて責任を負う必要がある。BCP 責任者はBC マネージャーとも呼ばれ、次のような役割を担う。また、組織として最終的な責任の所在を明確化するために、組織の経営陣の役割・責務を明記することが望まれる

＜BCP 責任者の役割＞
○BCP プロジェクトの調整、組織管理
○経営陣からの支援の取り付け
○プロジェクト計画の策定と予算管理
○教育・テスト計画の策定と指導
○定期的なBCP の見直し

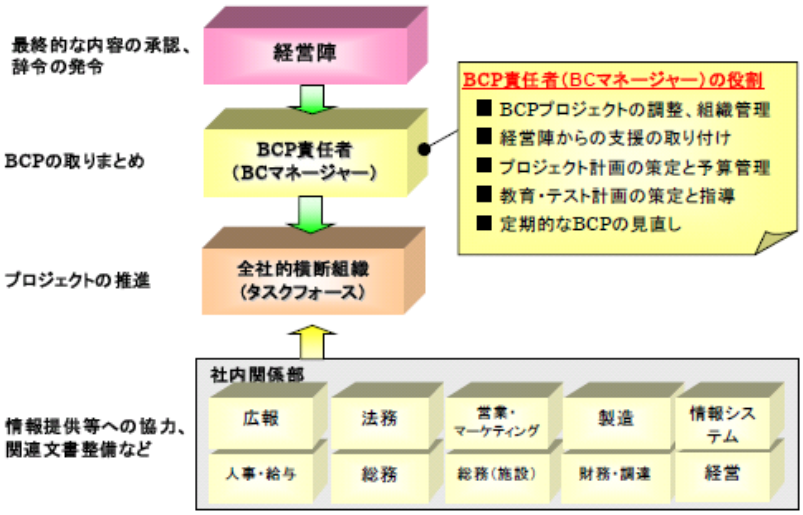


図 12. 事業継続計画策定ガイドライン「事業継続計画プロジェクト組織体制の例」

(4) その他

「事業継続ガイドライン二版(内閣府)」では、確立した体制が機能しなかった場合の権限委譲や代行順位についても事業継続計画の検討において考慮しておくべきだと記されている。

≪事業継続ガイドライン二版(内閣府)≫

■ 災害対策本部長に連絡が付かなかった場合や不在の場合の権限委譲や代行順位をあらかじめ決定しておく必要がある。
■ 各部門の対策実施本部長も権限委譲や代行順位を決定する必要がある。

同じく「事業継続ガイドライン二版(内閣府)」では、組織外との連携についても事業継続を検討する際に十分に考慮すべきだと記されている。

対外的な情報発信および情報共有
災害発生後は、取引先、消費者、従業員、株主、市民、自治体などと情報を共有することが重要で

ある。企業活動が関係者から見えなくなる、何をしているのか全然わからないといった、いわゆるブラックアウトを防ぐための対策を講じる必要がある。そのためにも、関係者との事前の協議が重要となる。
中堅中小企業でも取引先企業やサプライチェーンの発注者への情報提供が必要である。対外的な情報発信および情報共有に関し、事業継続計画を検討する際に十分に考慮すべき点を例示する。
■ 情報収集・伝達、広報体制の確立
■ 関係当局、周辺住民、サプライチェーン等の関係者との連絡体制の構築
■ 通信・情報連絡手段の確保

また、「中小企業BCP策定運用指針第1版」（経済産業省中小企業庁）では、組織全体への周知も有効であると記されている。

≪「中小企業BCP策定運用指針第1版」（経済産業省中小企業庁）≫

●BCP の策定・運用推進に取り組んでいることを全ての従業員に周知する
BCP の運用は全ての従業員が対象になりますし、実際の緊急時には従業員の行動が計画の成否を左右します。BCP の運用に対して従業員の参加意識を高める必要があります。

3.1.4.2 事業継続計画が備えるべき要件

「事業継続計画策定ガイドライン（経済産業省）」では、事業継続計画が備えるべき要件として、「BCP 策定までの流れ」として次のように記している。

≪「事業継続計画策定ガイドライン（経済産業省）」

ステップ1:ビジネスインパクト分析
①事業継続、復旧の優先順位付け
②ボトルネックの特定
③目標復旧時間の設定
ステップ2:リスク分析
ステップ3:発動基準の明確化
ステップ4:BCP 策定

「事業継続ガイドライン二版（内閣府）」では、事業継続計画が備えるべき要件として、次のように記している。

≪事業継続ガイドライン二版（内閣府）≫

事業継続の取組みの特徴
(1) 事業に著しいダメージを与えかねない重大被害を想定して計画を作成する。
(2) 災害後に活用できる資源に制限があると認識し、継続すべき重要業務を絞り込む。
(3) 各重要業務の担当ごとに、どのような被害が生じるとその重要業務の継続が危うくなるかを抽出して検討を進める。結果としてあらゆる災害が想定される。
(4) 重要業務の継続に不可欠で、再調達や復旧に時間や手間がかかり、復旧の制約となりかねない重要な要素（ボトルネック）を洗い出し、重点的に対処する。
(5) 重要業務の目標復旧時間を設定し、その達成に向け知恵を結集し事前準備をする。
(6) 緊急時の経営や意思決定、管理等のマネジメント手法の1つに位置づけられ、指揮命令系統

の維持、情報の発信・共有、災害時の経営判断の重要性等、危機管理や緊急時対応の要素を含んでいる。

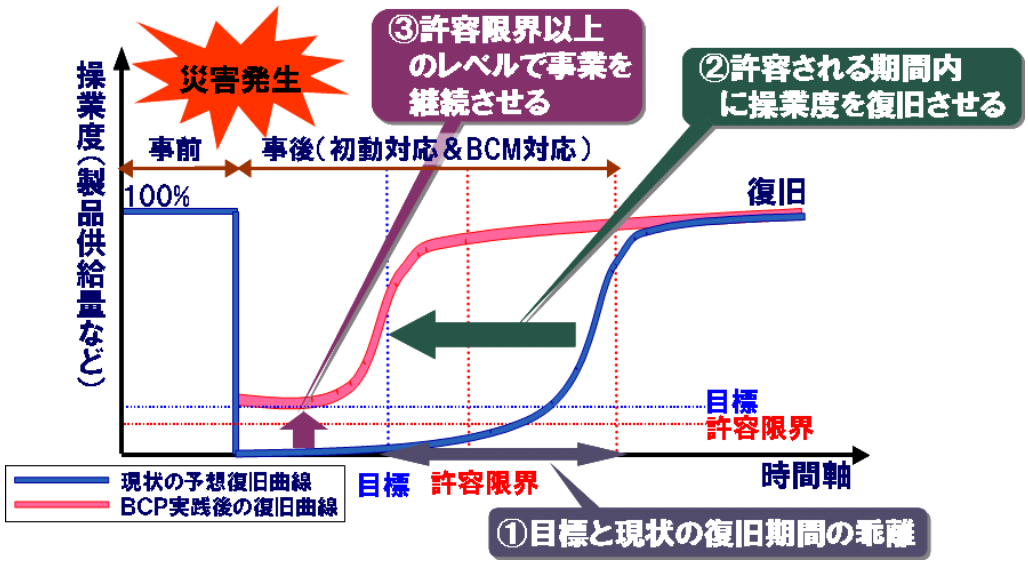


図 13. 事業継続ガイドライン二版「事業継続計画（BCP）の概念

「IT サービス継続ガイドライン」では、緊急時における情報セキュリティ対策の不実施による情報セキュリティ水準の低下に加え、想定外の事態において IT サービス継続を優先するために、必要な情報セキュリティ水準の低下についても検証しておくことが重要であると記している。

≪IT サービス継続ガイドライン（METI）≫

4.3.3 緊急時におけるセキュリティ水準の低下
組織において求められる情報セキュリティ水準は、情報セキュリティに関係するリスク分析に基づいて、その組織が受容できないと判断するリスクに対して、そのリスクを軽減・分散・転嫁等するための管理策として決定される。
そのため、リスク分析では、組織として平常時における一定の水準を定めることになるが、緊急時においては平常時と異なる水準を認めざるを得ない場合も考えられる。言い換えると、平常時では受容できないとしていたリスクの一部を、緊急時にのみ受容する場合があるということである。具体的には、情報セキュリティ水準のうち、可用性の水準を維持するために、機密性及び完全性に関する水準の低下を認める場合がある。ここでいう緊急時とは、IT サービスの継続が困難となる事態であるが、あらかじめ分析して定めたリスク管理策の維持と IT サービス継続が相反する場合に、そこで改めて IT サービス継続が中断するリスクを加味した上で、可用性以外の情報セキュリティ水準を決定する必要がある。
ISO/IEC 18044:Information Security Incident Management では、「計画準備段階として事前計画に基づく対応手順を充実させて、実際のインシデント発生時に、手順にしたがって対応することを基本としている。しかし、その一方で、計画準備段階に用意した手順がインシデントの実情に沿わないときには、手順以外の方法による対応をするための手続きも必要であること」を指摘している。なぜなら、インシデント発生時においては、事前予測の想定範囲外の状況となることもあり、その場合には、事後対応を事前計画で想定した範囲内だけで実施することは、むしろ想定外の状況に柔軟に対応できなくなる場合があるためである。そのため、想定外の状況に遭遇した場合に、実際の

担当者が事前に定められた処置よりも適切であると判断する処置を、例外処置として実施するための手続きを事前に検討しておくことも必要である。ISMS ユーザーガイド第 2 版[JIPDEC.1]では、そのような例外処置についても管理するような管理策を講じることについて述べている。このことから、緊急時における情報セキュリティ対策の不実施による情報セキュリティ水準の低下に加え、想定外の事態において IT サービス継続を優先するために、実際の担当者に判断を委ねることによる情報セキュリティ水準の低下についても検証しておくことが重要である。

また、組織が災害時に考慮すべき重要事項は事業継続の他に、少なくとも次にあげる 3 点があると記している。

≪事業継続ガイドライン二版（内閣府）≫

○ 生命の安全確保
顧客が来店したり、施設内に留まったりすることが想定されている業種においては、まず顧客の生命の安全確保が求められる。
企業の役員、従業員、関連会社、派遣社員、協力会社など、業務に携わる人々の生命の安全を確保することがその次に重要なのは言うまでもない。
○ 二次災害の防止
例えば地震や水害などの場合、火災の防止、建築物・構築物の周辺への倒壊阻止、薬液の漏洩防止など、周辺地域の安全確保の観点から二次災害防止のための取組みが必要である。
○ 地域貢献・地域との共生
災害が発生した際には、市民、行政、取引先企業などと連携し、地域の一日も早い復旧を目指したい。地域貢献には、援助金、敷地の提供、物資の提供などが一般的であるが、このほかにも技術者の派遣、ボランティア活動など企業の特色を活かしたサポートが望まれる。平常時からこれら主体との連携を密にしておくことも望まれる。

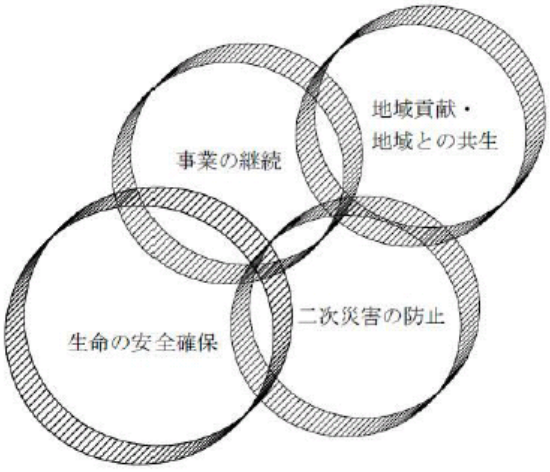


図 14. 事業継続ガイドライン二版「事業継続と共に求められるもの」

＜考察＞
事業継続計画を検討する際、重要インフラサービスの維持・継続にかかわる重要システムの安定運用の観点では、主なガイドライン等で記されている要件等に加え、次に挙げる事項を考慮することが必要だと考える。

- 脅威を検討する際、従来から考慮されている対災害以外に、昨今ではサイバー攻撃や新型インフルエンザパンデミック等、新しい脅威も考慮し、検討する

・ 継続すべき重要業務、重要システムを絞込む際、最終的にはシステムに頼らない、人によるサービス継続が可能であるかということも考慮し、検討する

脅威によっては、事業継続の考え方が変わってくることも注意しておかなくてはならない。いずれの脅威に対しても、限られた資源の中から事業を継続していく必要があるのだが、たとえば、物理的損害が多く見られる災害やサイバー攻撃に対しては、確保できた人員を重要業務・重要システムに充て、早期に復旧させることが重要となるが、人的損害が多く見られるパンデミックに対しては、重要ではない業務から停止・縮退し、最低限の人員でシステムを活用しながら運営していくことでサービスの維持・継続が確保できると考える。

3.1.4.3 直面している課題

「事業継続ガイドライン二版(内閣府)」にて次に記す課題があげられている。発行から約 1 年 4 ヶ月が経過するが現在も継続した課題だと考える。

≪事業継続ガイドライン二版(内閣府)≫

わが国企業は、地震等の自然災害の経験を踏まえ、事業所の耐震化、予想被害からの復旧計画策定などの対策を政府の諸制度や事業とも連動して進めてきており、防災対策は諸外国に比べて先進的と評価されている。しかし、どのような災害・事故に遭遇しても重要業務を中断させないという経営戦略である事業継続の面では遅れていると言わざるを得ない。事業継続の取組みを進めれば、その企業自身のメリットのほか、取引による連鎖的な影響も少なくなり、災害の間接的被害額を減らすことができる。それが本ガイドライン策定の動機である。
事業所ごとに懸念の大きい災害に備えて被害軽減策を講ずるこれまでの防災対策は今後とも極めて重要であるが、その発想とアプローチにおいて事業継続の取組みとは異なるところが多い。対策内容には双方に重なる部分もあり、「双方ともに推進すべき」と考えると分かりやすい。(政府・地方公共団体としても、前者の防災対策のため、懸念の大きい災害の被害想定やインフラ回復見込み等を推定・公表、防災事業への投資等の努力を引き続き行っていく。)
この事業継続の取組みを促進するうえで、本ガイドラインの検討過程において論点となった幾つかの点について、あらかじめ考え方を整理し、以下に示しておく。

第一に、企業が自らの事業継続を重要な目標として追求することを奨励するとはいえ、まず災害時には生命の安全確保を考えることが大切であると繰り返しておきたい。

第二に、事業継続計画において、想定されるリスクとしてテロなどの人為的なものを重要視している欧米に比べ、わが国は自然災害を中心としている。自然災害は人為的なリスクよりも一般に被害が広域的で、未然防止も難しく、有効な対策が少なからず異なると考えられる。そこで、わが国企業は、欧米の事業継続計画をそのまま模倣するのではなく、わが国の事情に合ったものを策定すればよい。一方で、国際的に見てわが国企業による事業継続の取組みが高いレベルにあると認識されるよう、共通の骨格を維持した計画を目指すべきであろう。

第三に、本ガイドラインは民間企業を主な対象とし、サプライチェーンを意識しつつ企業が協調して取り組む必要性・有効性を強調しているが、事業継続計画が実効性あるものとするためには、行政側の理解と適切な対応も求められる。例えば、企業の業務再開に必要な設備補修等に行政の許認可が必要な場合において、各行政主体が災害被害軽減における企業の事業継続の重要性をよく認識した上で対処することが望まれる。

＜考察＞

上記にもあるように、サプライチェーンの関与は忘れてはならない。重要インフラサービスは、その社会的必要性の高さから、サプライチェーンの断絶により受ける影響、又は与える影響が大きいと考

えられる。事業継続計画に実効性を持たせるためにも、平常時より、重要インフラサービスを提供する事業者と支えるサプライチェーンの双方で事業継続計画の内容について確認し、演習を行っておくことで、サプライチェーンがボトルネックとなる事業停止を回避できると考える。

3.1.5 日本の BCP 事例

日本において実際に策定・運用されている BCP について、重要インフラ事業者へヒアリングを行い調査した。しかしながら詳細な BCP については、組織の弱点となる記述が含まれるため、ヒアリング対象のすべての重要インフラ事業者において非公開文書として位置づけられていたため、ヒアリングにて得られた BCP の特徴について以下にまとめる。

まず、BCP の主な想定リスクは、ほぼ災害であった。続いて近年の新型インフルエンザパンデミックを受け、これまでの災害版 BCP に加え、新型インフルエンザ版 BCP を追加策定したという重要インフラ事業者が多くみられた。事業や業務が絶たれるリスクとして IT 障害等の技術的リスクがあることは認識されていたが、BCP には含まれず、個別に緊急時対応マニュアルとして備えている場合や、災害・新型インフルエンザパンデミックの BCP で技術的リスクもカバーできるとしている組織がほとんどであった。また、事業や業務を停止させる事象を招く発生原因には焦点をあてず、発生する事象の観点で「重要サービスが停止した場合」という想定の元に、全体的な BCP を策定されている重要インフラ事業者もあった。

BCP の見直しについては、ほとんどのヒアリング対象重要インフラ事業者にて、年に 1 回実施されていた。また、定期的な見直しに加え、他組織で起きた事業の継続が危ぶまれた事故事例や、演習で確認された問題点等を適宜 BCP に反映している組織がほとんどであった。

重要業務の継続に不可欠なシステムの見直しについては、年に 1 回、情報資産の棚卸や年度の切り替わり時期に実施している重要インフラ事業者がほとんどであったが、重要システムに該当するか否かの判断基準の見直しはほぼ行われていなかった。中には、サービスの体系が不変なため、重要システムの判断基準及び重要システムの位置づけも不変であるとし、サービス体系の変更を見直しの契機としている事業者もあった。

ヒアリングでは文書化された BCP を入手できなかったため、公開されている BCP を調査し、3.1.5.1～3.1.5.4 にまとめる。

3.1.5.1 東京証券取引所における BCP 取組事例

東京証券取引所の BCP 取組事例を以下に示す。

組織名	東京証券取引所
文書名	緊急時事業継続計画[40]
主なリスク	以下の原因事象と結果事象の組合せで考えている。 （原因事象） ・地震、風水害等の自然災害 ・システム障害 ・電力、通信等の社会インフラの停止 ・物理的破壊行為 ・サイバーテロ等のテロ行為 ・新型インフルエンザの流行　等 （結果事象） ・建物の利用不可

[40] http://www.tse.or.jp/about/bcp/b7gje60000004lrh-att/bcp.pdf

組織名	東京証券取引所
	・システムの利用不能 ・人員の不足 ・外部機関の停止　等
記載内容	1. 基本的な考え方 2. 再開目標 3. 対象とする範囲 4. 結果事象ごとの対応方針 (1)プライマリーセンターの利用継続を前提とした対応 (2)セカンダリセンターへの切り替えを前提とした対応 (3)システム障害時の対応 5. 対応のための体制整備 6. 今後の課題
体制	「5. 対応のための体制整備」に以下の記載あり。 ・リスクが顕在化した際にはBCP対策本部を設置する。 ・対応のために以下の体制、インフラ整備を行っている。 －人員の確保 －通信手段の確保 －代替オフィス －データセンター －テスト・教育研修 －安否確認システムの導入
BCP 見直し頻度	年 2 回以上
その他特徴的な取組	2002 年 4 月に東京証券取引所への爆破テロ未遂があり、BCP 発動時に以下等の問題点が発覚し、それを受けて BCP を改訂。 ・業務時間外でのテロを想定していなかった(代替オフィスに手ぶらで向かうことになり、必要書類、PCが不足) ・代替オフィスで業務を継続する社員を事前に決めていなかった(代替オフィスのスペース以上の人数が集まり混乱) ・避難解除を通知する為の連絡網が未整備だった ・業務再開のチェック体制がなかった(どの部門が再開できたのかすぐに確認できなかった) ・当初は想定リスク毎にBCPを策定していたが、BCP毎に連絡ルートが異なっていた ・BCP に記載してあった電話番号が間違っていた 2004 年 6 月に見直しが完了し、2004 年 10 月に訓練を実施。その後、証券会社の関係者等で構成する BCP フォーラムが策定した「取引所取引専門部会の報告書」に再開・復旧目標の提示等の課題が上がったことを踏まえて、2007 年 3 月に改訂。これまで明記していなかった復旧時間を 24 時間以内に復旧する目標をたて、再開・復旧目標、バックアップ体制

組織名	東京証券取引所
	の強化、コンティンジェンシープランの見直し結果を盛り込んだ。

3.1.5.2 横浜市における BCP 取組事例

横浜市の BCP 取組事例を以下に示す。

組織名	横浜市
文書名	・横浜市業務継続計画【新型インフルエンザ編】[41] ・横浜市業務継続計画【地震編】(中間案)[42] (※地震編は作成途中のため、以下新型インフルエンザ編の内容を記す)
主なリスク	【新型インフルエンザ編】 新型インフルエンザ
記載内容	【新型インフルエンザ編】 1 はじめに 2 基本的な考え方 3 想定事態 4 感染防止策 5 優先的に継続する業務及び縮小・休止する業務 6 業務の継続、縮小及び休止の実施等 7 業務を継続する体制 8 感染防止策等の周知 9 研修・訓練の実施 10 計画の点検・見直し
体制	【新型インフルエンザ編】 ・対応のために以下の体制、インフラ整備を行っている。 －情報収集・連絡体制の整備 －代替意思決定者の指定 －職員の応援 －必要な人員等の検証 －関係部署等との協力・連携体制の構築
BCP 見直し頻度	見直し頻度の詳細記載なし。 (継続的に見直しを実施する。また新型インフルエンザに関する新たな知見の入手、本市対策の充実・強化、訓練等の課題を踏まえた見直しを実施するとの記載あり)
その他特徴的な取組	2010 年日本APEC横浜開催に向け同時多発テロに対応する図上訓練を実施。

41 http://www.city.yokohama.jp/me/shobo/kikikanri/bcp/influ-bcp2009.pdf
42 http://www.city.yokohama.jp/me/shobo/kikikanri/bcp/chukanan.pdf

3.1.5.3 愛知県における BCP 取組事例

愛知県の BCP 取組事例を以下に示す。

組織名	愛知県
文書名	・愛知県庁業務継続計画（愛知県庁BCP)【東海・東南海地震連動編】[43] ・愛知県庁業務継続計画（愛知県庁 BCP)【新型インフルエンザ対応編】[44]
主なリスク	【想定東海・東南海地震連動編】 ・東海・東南海地震 【新型インフルエンザ対応編】 ・強毒性新型インフルエンザ（H5N1 型等）
記載内容	【想定東海・東南海地震連動編】 第1章　愛知県庁業務継続計画の基本的な考え方 第2章　計画の前提となる被害想定 第3章　非常時優先業務の選定 第4章　業務継続における課題と対応 第5章　今後の取組み 【新型インフルエンザ対応編】 第1章　はじめに 第2章　業務継続計画の基本的な考え方 第3章　業務の仕分け 第4章　必要な人員、物資及びサービスの確保 第5章　職員等の健康管理 第6章　感染防止策の徹底 第7章　業務継続計画の実施 第8章　今後の取組み
体制	【想定東海・東南海地震連動編】 「第2章 2 県の業務継続に与える影響」に以下の記載あり。 ・特別チーム（大規模災害時業務継続対策特別チーム） ・非常配備体制 【新型インフルエンザ対応編】 「第1章 4 実施体制」に以下の記載あり。 ・平常時の体制 ・新型インフルエンザ発生時の体制

43 http://www.pref.aichi.jp/0000028478.html
44 http://www.pref.aichi.jp/0000036171.html

組織名	愛知県
	≪県の新型インフルエンザ推進体制≫ −愛知県新型インフルエンザ対策本部（本部長、構成員の記述あり） −愛知県新型インフルエンザ対策本部幹事会 −事務局
BCP 見直し頻度	見直し頻度の詳細記載なし。 （業務継続計画のより適切な運用等を図るため、研修・訓練等の実施・検証を通じ、また、国の動向を踏まえ、必要に応じて業務継続計画の見直しを行うとの記載あり）
その他特徴的な取組	・非常時優先業務を特定するため、全3,799業務の洗い出しを行い、約2割に当たる691業務を選定した。 ・非常時優先業務については、被災者の観点から考えて、発災から2週間にかけての実施時期や復旧目標を設定した。 ・中小企業向けBCP策定ガイドライン「あいちBCP」を策定。業種分類や企業規模、防災やBCPに対する取組具合に応じて企業が取組やすいよう、例示を含めて記されている。

3.1.5.4 農林水産省における BCP 取組事例

農林水産省の BCP 取組事例を以下に示す

組織名	農林水産省
文書名	農林水産省業務継続計画[45]
主なリスク	首都直下地震
記載内容	第1章　本計画の目的と構成 第2章　非常時の業務継続への影響と業務継続性確保の基本方針 第3章　非常時に継続すべき優先業務 第4章　非常時の業務継続力向上のための措置
体制	「第4章　非常時の業務継続力向上のための措置」に以下の記載あり。 ・非常参集要員の指定 ・事故時等の指揮命令系統の明確化 ・安否確認連絡体制の整備 ・食品、飲料水等の備蓄 ・庁舎の耐震化、代替施設の設備機器の整備 ・自家電気設備の増設 ・災害時優先電話等の利用

[45] http://www.maff.go.jp/j/saigai/keikaku/pdf/h2003_plan.pdf

組織名	農林水産省
	・情報システムの可用性の向上
BCP 見直し頻度	毎年度点検し、必要に応じ計画を見直す。

3.1.5.5 東京ガスにおける BCP 取組事例

東京ガスの BCP 取組事例を以下に示す

組織名	東京ガス
文書名	・防災業務計画[46] ・新型インフルエンザ対策行動計画[47] ・国民保護業務計画[48]
主なリスク	【防災業務計画】 一般防災、大規模地震防災 【新型インフルエンザ対策行動計画】 新型インフルエンザ 【国民保護業務計画】 武力攻撃事態
記載内容	【防災業務計画】 第1編　総則 　第1章　総則 第2編　一般防災業務計画 　第1章　防災体制の確立 　第2章　災害予防に関する事項 　第3章　災害応急対策に関する事項 　第4章　災害復旧に関する事項 第3編　大規模地震防災強化計画 　第1章　大規模地震防災体制の確立 　第2章　災害予防に関する事項 　第3章　災害防災応急対策に係る措置に関する事項 【新型インフルエンザ対策行動計画】 1. 総則 　1-1 目的

46 http://www.tokyo-gas.co.jp/safety/bousai.pdf
47 http://www.tokyo-gas.co.jp/safety/shingata.pdf
48 http://www.tokyo-gas.co.jp/safety/kokumin.pdf

組織名	東京ガス
	1-2 定義 1-3 危機管理体制 2. 非常体制移行前の対応 2-1 情報収集及び周知 2-2 新型インフルエンザ流行時に事業運営体制の検討 2-3 従業員等への感染の予防のための措置 3. 第一次非常体制における対応 3-1 情報収集及び周知 3-2 感染拡大時の事業運営体制 3-3 感染拡大予防のための措置 4. 第二次非常体制における体制 4-1 情報収集及び周知 4-2 感染拡大時の事業運営体制 4-3 感染拡大予防のための措置 【国民保護業務計画】 第1編 総則 第1章 総則 第2編 平素からの備え 第1章 組織・体制の整備 第2章 計画実行のための準備 第3編 武力攻撃災害への対処に関する措置 第1章 情報の収集及び報告 第2章 災害時における広報 第3章 防災要員の確保 第4章 災害時における復旧用資機材の確保 第5章 生活関連等施設の安全確保 第6章 応急の復旧 第4編 武力攻撃災害の復旧に関する措置 第5編 災害対処自体への対処
体制	【防災業務計画】 「第2編 第1章 防災体制の確立」に以下の記載あり。 ・防災体制 ・対策組織の運営 ・外部関係機関との協調 【新型インフルエンザ対策行動計画】

組織名	東京ガス
	「1. 総則」に以下の記載あり。 ・危機管理体制 「2. 非常体制移行前の対応」に以下の記載あり。 ・新型インフルエンザ流行時の事業運営体制の検討 「3. 第一次非常体制における対応」「4. 第二次非常体制における対応」に以下の記載あり。 ・感染拡大時の事業運営体制 【国民保護業務計画】 「第 2 編　第 1 章　組織・体制の整備」に以下の記載あり。 ・国民保護体制の組織及び分担業務 ・社外機関との協調
BCP 見直し頻度	毎年見直しを実施。その他訓練結果等に基づき適宜行っている。
その他特徴的な取組	・新型インフルエンザ対策行動計画は、策定当初の平成 19 年時点では強毒性を想定したものであったが、平成 21 年に弱毒性も想定した内容に改訂している。(改訂版は公開されていない) ・地震は経営上のリスクととらえ、地震を想定した訓練は、全社単位で年に 1 回、その他工場では週に 2 回ガスを止める訓練を行っている。

3.2 海外の BCP に関する調査

3.2.1 英国における BCP 動向[49]

3.2.1.1　政府施策

本節では英国政府による BCP 普及のための主な施策について整理する。

(1) 2004 年民間緊急事態法

発行者	英国議会
名称	2004 年民間緊急事態法 (Civil Contingencies Act 2004、以下 CCA2004)
発効日/開始日	2004 年 11 月 18 日成立

民間保護の法的枠組みに関する後述の問題を議論するため、2001 年 8 月に英国政府から討議文書「イングランド及びウェールズにおける危機管理の未来 」が発表され、討議が行われた。この討議の中で明らかになった、2001 年以前の法制度の主な問題点は以下の通りであった。

- 民間防衛の取組が、中央政府と地方自治体の縦割りになってしまい、地方自治体間や民間企業、非営利組織等との連携が促進されていないこと。
- 2000 年以降の燃料危機や洪水の多発、また 2001 年の英国内口蹄疫や米国同時多発テロの発生等、従来の法律が緊急事態として定義していた国際戦争やストライキ以外の新しい脅威への対応が不十分であること。

[49]東京海上日動リスクコンサルティング資料等より作成
http://www.meti.go.jp/meti_lib/report/2010fy01/E000900.pdf

- 緊急事態宣言が全国レベルでしか出せず、現代イギリスの分権事情が反映されていないこと。
- 1998 年人権法や、欧州人権条約等、緊急事態下における人権の扱いに関する考慮が必要となったこと。
- 1990 年代に英国ビショップスゲイトやマンチェスターで爆弾テロが発生した際に、事業継続対策を行っていた組織の対応が優れていた。そのため、政府や地方自治体が率先して事業継続マネジメントの普及活動を行うことが求められるようになった。

討議の結果、1948 年民間防衛法と1920 年国家緊急権法は廃止し、新たな法律が作成されることとなった。

2003 年 6 月、内閣府大臣により民間緊急事態法案の草案が公表され、議会委員会による議論、パブリックコメント受付、修正を経て 2004 年 11 月 18 日に成立した。なお、本法律に基づく施策推進は英国内閣府民間緊急事態事務局により行われている(図 14 の網掛け部分が主な CCA2004 推進組織)。

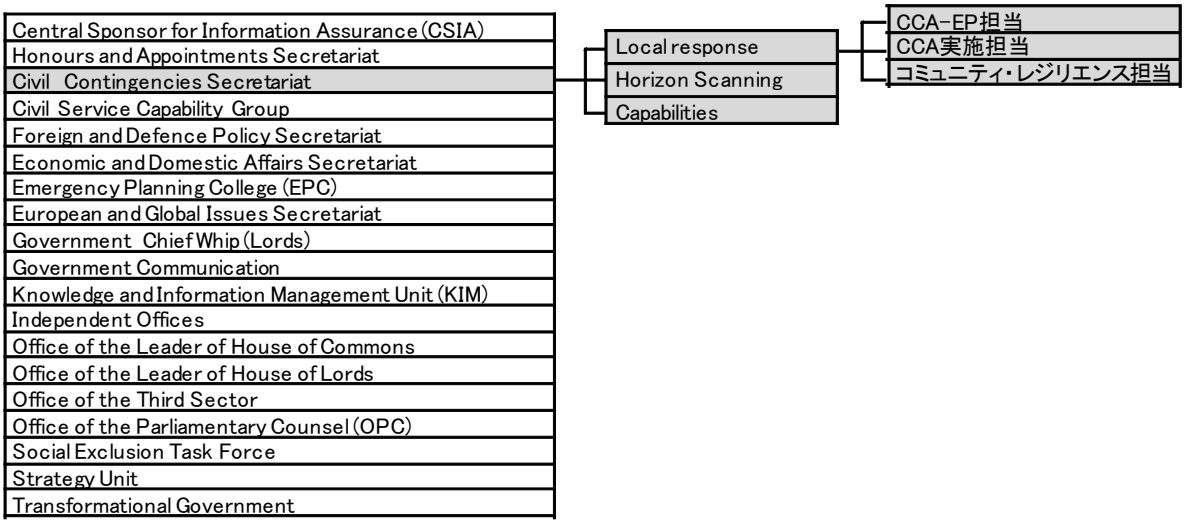


図 15. 英国内閣府組織図

CCA2004は、テロリズム、自然災害、伝染病、ライフラインや社会インフラの停止等の幅広い緊急事態から市民を保護するための法的枠組みである。具体的には、地方自治体等による市民保護活動とその事前計画の義務化と、緊急事態発生時における中央政府の緊急権の強化の二つの柱によって、市民保護を包括的、迅速かつ強力に実施することを目的としている。

(2) 緊急事態計画カレッジ

運営者	英国内閣府
名称	緊急事態計画カレッジ (Emergency Planning College、以下 EPC)
発効日/開始日	1989 年創立

緊急事態対応カレッジの運営目的は、CCA2004 に係わる分野の学習機会を提供することで、英国のレジリエンシーの向上を図ることである。また、全国自治体の担当者が同カレッジのコースを受講することで、災害対応及び事業継続の水準の向上及び均一化がなされている。同カレッジが実施するコースやイベントは、参加者の緊急事態対応及び管理能力の向上に資するよう計画されている。

緊急事態対応カレッジは、政府関係者、自治体関係者、民間企業従業員等を対象に、危機管理及び緊急事態計画分野の短期講義やセミナー、ワークショップ等を開催している。1 年間の参加者は、約 6,500 人程度である。以前は CCA2004 で対応者として指定されている組織の者がコースを受講できたが、2010 年より、第 2 レベル対応者以外の民間組織所属者もコースが受講できるようになった。

通常コースは 1 日～4 日間で完了する短期コースであり、イギリス中東部のヨーク市近郊の同カレッジ校舎で実施される。緊急事態計画関連の約 40 コースが提供されており、1 コースにつき 1 年で 2 回～20 回程度実施される。各コースは有料で、参加者の所属により料金が異なる。短期コースの主なテーマ項目は以下の通り（各項目につき 3～10 のコースが提供されている）[50]

- 緊急対応の基礎
- リスクマネジメント
- 計画策定
- 緊急事態マネジメント
- 事業継続マネジメント
- 公衆安全
- CBRNテロ（化学、生物、放射性物質、核兵器を用いるテロ）対応マネジメント
- 専門研究
- 緊急時医療サービス
- 中央政府
- 戦略的トレーニング

上記コースについては、内閣府緊急事態事務局と検討の上決定している。従って、国の想定するリスクや、対策計画が変更された場合は、コースのテーマや内容も柔軟に変更される。なお、講師の経歴は、内閣府緊急事態対応事務局からの派遣や、軍出身者が多い。

3.2.1.2 BCP 普及状況

本節では、英国内閣府によるBCPに関するアンケート結果[51]に基づき、英国におけるBCPの普及状況を概観する。

（1）BCP 策定率の推移

下図より英国における BCP 策定率はこの 8 年の間、ほぼ横ばいであることが分かる。英国では BCP の普及を目指し 2004 年に Civil Contingency Act が制定されたが、BCP の取組みの高度化を支援する内容が主であり、BCP の策定が義務付けられている訳ではないため、策定率の向上に

[50] 全コース科目については、同カレッジのウェブサイト参照
http://www.cabinetoffice.gov.uk/epcollege/training/courses.aspx

[51] A Decade of Living Dangerously :The Business Continuity Management Report 2009
https://www.managers.org.uk/sites/default/files/user35/CMI_-_BCM_March_2009_-_Full_Report.pdf

はあまり寄与していない状況が伺える。

図 16. BCP 策定率の推移

(2) 従業員規模別の BCP 策定状況
規模の小さい組織ほど BCP 策定率が低い傾向が見られる。

表 12. 規模別 BCP 策定状況

組織規模(従業員数)	策定率
大規模(251 人以上)	64%
中規模(51-250 人)	49%
小規模(50 人以下)	25%
平均	52%

(3) サプライヤー・外注先への BCM 適用率
「重要なサプライヤーのみに BCM を適用している」と回答した組織が 29%であり、「全サプライヤーに適用している」と回答した組織は 10%であった。すなわち、70%以上の組織が重要なサプライヤーにすら BCM を適用していない実態が分かる。

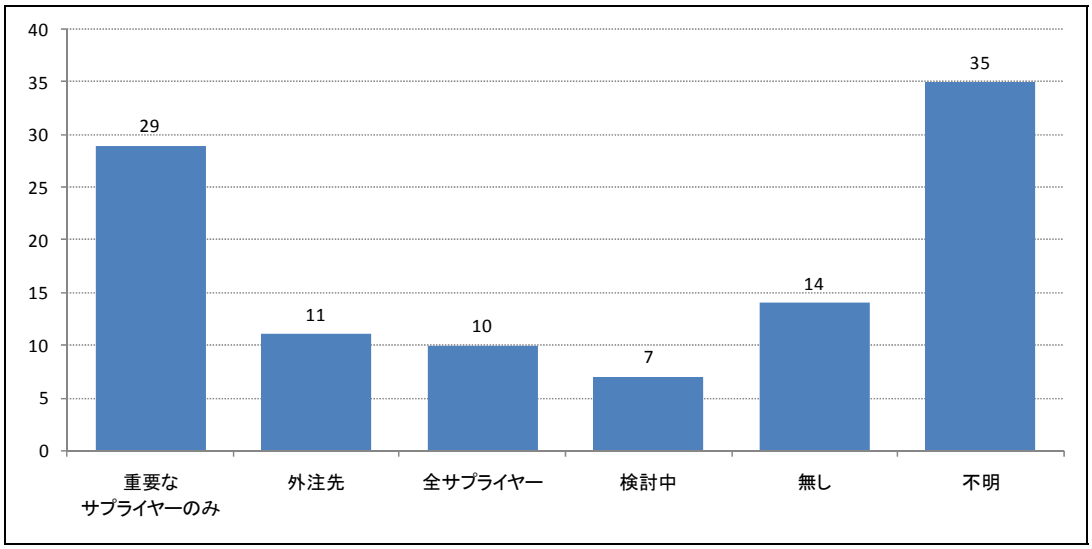


図 17. サプライヤーや外注先への BCM 適用率

(4) BCP 発動状況

過去 1 年間において、業務停止の要因となったインシデントの発生割合及び当該インシデントが BCM での対象リスクとなっていた割合についての調査結果を以下に示す。

英国では情報システム関連障害への対応が BCM の主な対象事象であることが分かる。また、異常気象(洪水、強風等)、要員の喪失、交通の遮断等も主な BCM の対象リスクとして含まれていることが分かる。

日本国内に比べ、事業継続を脅かすインシデントの発生頻度が高いため、英国では BCM 構築の必要性も、経営課題としてより強く認識される環境であると考えられる。

表 13. 過去 1 年間に発生したインシデント

回答数: 1012 件	2002 年	2003 年	2004 年	2005 年	2006 年	2007 年	2008 年	2009 年	BCM 対象率 (%)
情報システム障害	19	24	25	41	38	39	43	40	42
異常気象(洪水、強風等)	18	15	10	18	9	28	29	25	30
要員の喪失	–	26	20	28	29	32	35	24	30
通信障害	–	–	23	28	24	25	30	23	37
ユーティリティー障害 (電気、ガス、上下水道等)	–	–	–	28	19	21	14	21	26
従業員の疾病や事故	13	9	8	19	13	17	17	16	26
重要技能の喪失	33	16	14	20	19	20	21	14	26
否定的な記事や風評	24	17	16	17	16	19	18	14	16
交通の遮断	5	5	6	11	13	13	16	13	39
企業ブランド、評価、イメージの悪化	15	7	8	11	8	11	10	11	19
サプライチェーンの途絶	19	11	12	10	10	13	12	9	19
圧力団体の抗議	10	7	7	6	7	7	6	7	12
ストライキ	–	–	–	5	6	7	7	7	16
火災	6	5	5	5	5	6	5	5	33
環境事故	9	5	4	7	5	6	7	7	28
顧客の健康被害や製品安全上の問題	11	6	4	6	6	6	7	4	17
テロリストによる攻撃	2	1	1	2	3	3	3	2	27

(5) BCM の取組みへの動機

著しい脅威と認識されているリスク事象についての調査結果を以下に示す。

サイバー攻撃、疫病、インフルエンザパンデミックに続いて、異常気象や洪水等の自然災害も著しい脅威として強く認識されていることが伺える。また、テロの脅威に対する認識も非常に高いことが分かる。

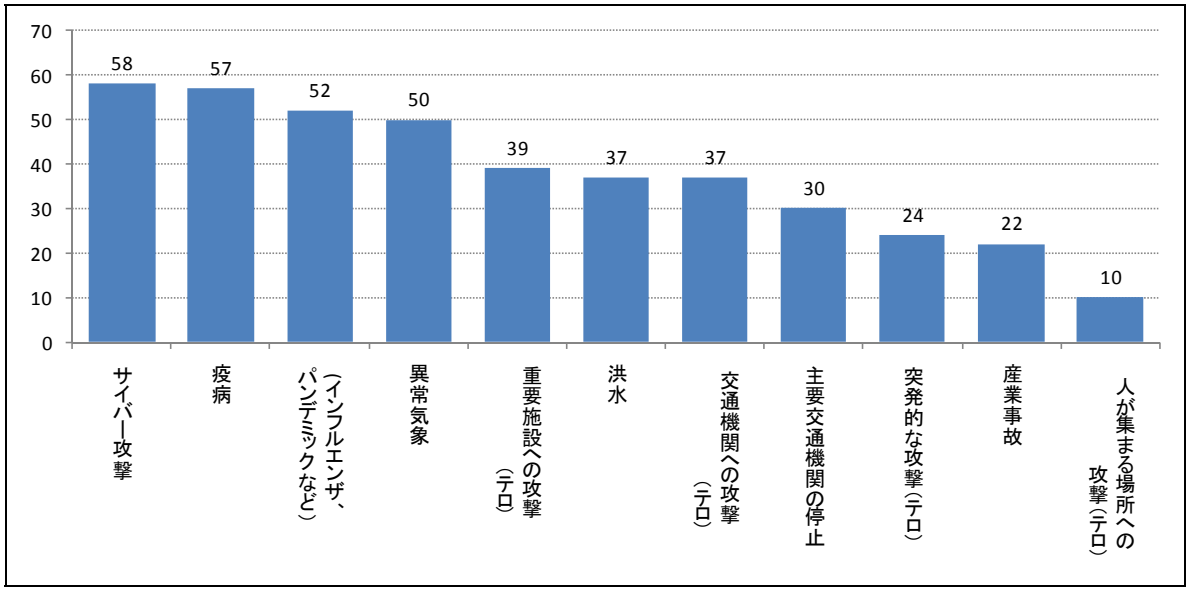


図 18. 著しい脅威と認識されているリスク

(6) 業種毎の BCP 策定率及び主な BCP 策定の動機付け要因

政府・自治体、金融機関、医療・介護、情報システム、インフラ等の業種では、BCP の策定がとりわけ進んでいることが分かる。また医療・介護等一部業種では BCP 関連規制により BCP 策定が進んでいる状況が伺える。なお、太枠内は英国における主な重要インフラ事業者が属する業種。太枠外の業種では「情報システム」の通信キャリア事業者、「製造業」の食品加工事業者などが重要インフラ事業者として指定されている。

表 14. 業種毎の BCP 策定率と主要な策定契機

業種	BCP 策定率	主要な策定契機	解説・提言
中央政府機関	90%	・中央政府 ・ガバナンス ・公共入札	公的サービスを継続するために、中央政府機関は実効性のあるBCMを構築する必要がある。同分野のBCMが進むことで、BCMの普及が進み、ひいては英国企業のインシデント対応力を高めることとなる。また、重要サプライヤーのBCMについても確認しておくことが重要である(BCM評価にはBS25999を使用することが可能である)。
金融機関	86%	・ガバナンス ・法規制 ・監査や認証	既に一部の国内法規制は、金融機関にBCMを要求している。また、近い将来整備が想定される国際法規制においても、BCMが要求要素となると考えられる。BCMが情報システムリスクだけでなく、全てのリスクをカバーしていることが必要となる。また、全ての金融取引先が有効なBCMを構築していることが求められる。
地方自治体	79%	・中央政府 ・ガバナンス ・法規制	民間緊急事態法2004の制定によってBCM構築が広がっている。同法律により、地方自治体は所轄地域内の企業及び慈善団体に対してBCM普及を進める役割を負うことが定められている。英国経済は小規模組織によって基礎が支えられているが、そのような組織はインシデントに対する脆弱性が高い。地方自治体は、そのような小規模組織に対して適切な指導を実施する責任がある。また、地方自治体への納入業者や協力組織に対しても、契約の際にBCMを確認する必要がある。
インフラ(電気・ガス・上下水道)	62%	・法規制 ・ガバナンス	インフラ企業は有効なBCMを構築している必要がある。2007年の洪水に関する内閣府調査では、インフラ企業がBCMを構築することが必須であり、またそのためにBS25999を使用することが望ましいと述べられている。インフラサービスは複雑なサプライチェーンを有しており、従って重要サプライヤーが自社BCM上の要求を満しているか確認する必要がある。
医療・介護	62%	・ガバナンス ・中央政府 ・法規制 ・既存顧客	英国保健省が推進している「リスク対応力増進プロジェクト」の結果か、本業界ではBCMに対する認識が高かった。特にBS25999及びNHSのBCPガイドラインの普及が進んでいる。医療サービスの供給に欠かせないサプライヤー、関係先、提携先等が、実効性の高いBCMを構築していることを確認しておく必要がある。NHSの機構改革が進んでいるが、BCMの構築・推進が必要なことに変わりは無い。
情報システム(※)	50%	・ガバナンス ・潜在顧客	情報システムサービスは、依然として組織の最も重要なリソースである。また、外部会社に外注することが多いことも特徴である。どのような契約形態であれ、BCMが重要である。有効なBCMが構築されていることは、既存顧客・潜在顧客両方にとって大きなアピールとなる。ITソリューションの提供に際しては、多数の製品やサービスを利用する必要がある。取引先や提携先の全てが、有効なBCM体制を整備している必要がある。なお、BCM評価にはBS25999を使用することが可能である。
教育	44%	・ガバナンス ・中央政府 ・監査や認証	教育機関が閉鎖された場合、親への負担が増大し、結果的に他分野に大きな影響を及ぼすと考えられる。従って、教育機関がBCMを構築することは、社会全体の対応力を底上げすることになる。高等教育機関では学生の満足度向上が重要な要素であるが、そのためには講義を継続的に実施することが欠かせない。BCMを構築する際には、この点についても認識が必要である。また、研究活動も収益上は重要な要素であるが、一部の研究資金提供機関がBCMを要求するようになってきていることに注意が必要である。
製造業	39%	・既存顧客 ・保険会社 ・ガバナンス	製造業は、複雑かつ広大なサプライチェーンネットワークに支えられている。経済不況の時期には、サプライチェーン上の組織に発生するインシデントを監視し、どのような事態でも顧客の要求に応じられるようにする必要がある。重要サプライヤーが有効なBCMを構築していることを確認しておくことが重要である。なお、BCM評価にはBS25999を使用することが可能であり、既に世界中で使用されている。重要サプライヤーのインシデント対応能力が確証できない場合は、製品供給を止めないための代替策を準備しておくことが必要である。
建築・土木	37%	・既存顧客 ・ガバナンス ・保険会社	建築・土木業界は、現在経済不況の影響を大きく受けている。インシデント関連のリスクを最小化するためには、業界及び個別プロジェクトごとのBCMが機能する必要がある。本業界では、取引や外注、下請け等のサプライチェーンが複雑であるが、その全てがBCMを構築している必要がある。BCMを構築していることが、主要な案件については入札要件となる可能性も高い。また、保険会社に自組織のBCMを説明しておく必要がある。
ビジネスサービス	31%	・既存顧客 ・潜在顧客 ・保険会社 ・公共入札	本業界は、経済不況の影響を大きく受ける傾向がある。インシデントが発生した場合、顧客は容易に競合他社に乗り換えることが可能であり、結果としてキャッシュフローの悪化や財務危機に陥る可能性がある。BCMを適切に構築することで、インシデントの影響を最小化し、また顧客の信頼を高めることが可能である。そのためには、顧客や保険会社に自組織のBCMを説明しておく必要がある。また、重要サプライヤーのBCMについても確認しておくことが重要である(BCM評価にはBS25999を使用することが可能である)。

※主にシステムソリューションサービスを提供する企業だが通信キャリアも含まれる

3.2.1.3 英国の BCP に関するガイドライン等

英国での主な BCP に関するガイドライン等を表 15 に示す。

英国は、2002 年に世界で初めて事業継続管理に関するガイドライン「Good Practice Guideline」を発行し、事業継続管理に関する取組が早くから行われてきた。その取組は、2005 年のロンドン連続バス・地下鉄テロ等を機に、さらに危機管理に対する意識の高まりを見せ、あらゆる脅威を想定した事業継続に関するガイドラインの国家規格化、国際規格への標準化に力を注いでいる。BS25999 は英国内のみならず、世界的に参考とされている。

表 15. 英国の BCP に関するガイドライン等

項番	文書名	発行機関	発行年月	対象組織	想定脅威		
					災害	疾病	IT 脅威
1	GPG2010[52] (Good Practice Guideline 2010)	BCI (事業継続協会)	2010 年 3 月 (初版は 2002 年)	全般	○	○	○
2	BS25999-1:2006[53] (事業継続マネジメントに関する実践規範)	BSI (英国規格協会)	2006 年 11 月	全般	○	○	○
3	BS25999-2:2007[54] (事業継続マネジメントに関する仕様)	BSI (英国規格協会)	2007 年 11 月	全般	○	○	○
4	BS25777-1:2008[55] Information and communications technology continuity management – Code of practice (情報通信技術の継続性マネジメントに関する実践規範)	BSI (英国規格協会)	2008 年 12 月	全般の ICT	○	○	○

表 15 に示すガイドライン等の概要を以下に示す。

(1) GPG2010(Good Practice Guideline 2010)(表 15 の項番1)

[発行機関:BCI]

- GPG2010 は、BCI(The Business Continuity Institute:事業継続協会)が 、あらゆる規模、部門、所在地を問わず適用できるとして、2002 年に世界で初めて BCM に関する包括的な概念・考え方を示し、発行したガイドラインである。改訂を繰り返し、2010 年に最新版を発行している。この改訂はインフルエンザによる世界的なパンデミック、経済危機、サイバー犯罪、気候変動等、新しいグローバルな脅威が考えられる昨今の背景があり、改訂のタイミングに至った。
- BCI は、1994 年に設立された、非営利専門機関。事業継続の教育、認証、専門性の開発

52 http://www.thebci.org/gpg.htm
53 http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030157563
54 http://shop.bsigroup.com/ProductDetail/?pid=000000000030169700
55 http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030166966

等を行っている。なお、本ガイドラインは、対象組織を問わないとしているが、BCI は、BT(英国最大の通信会社)、Continuity Shop(BCI の書籍等の販売会社)、Milton Keynes Council(英国の地方自治体)の 3 組織が出資している団体であることから、地方自治体をサポートする目的も含んでいると考えられる。

(2) BS25999-1:2006(事業継続マネジメントに関する実践規範)(表 15 の項番 2)

[発行機関:BSI]

- BS25999-1:2006 は、BSI(British Standards Institution:英国規格協会)によって、対象となる組織やリスクを問わない規格として 2006 年に発行された。組織が事業中断による影響を最小限に抑え、事業継続上の脅威に対処する能力を明示するための指針であり、事業継続を可能にすることを目的として策定された。プロセス、原則、用語の規定に加え、BCM を構築するうえでのベストプラクティスが規定されている。BSI が発行した「PAS56(Business Continuity Management System)」の後継にあたるガイドラインである。
- BSI は、前身が工学標準化委員会(Engineering Stanards Committee)であり、1929 年に英国王室から認可(Royal Charter)を受けている。国家規格を発行する英国唯一の機関として 英国政府から認可を受けている組織である。

(3) BS25999-2:2007(事業継続マネジメントに関する仕様)(表 15 の項番 3)

[発行機関:BSI]

- BS25999-2 は、BS25999-1 では BCM のためのガイドラインを示していたのに対し、BCM のための仕様として 2007 年に BSI が発行したものであり、BCM の要求事項について詳しく述べられている。これを参照することで、組織はパートナー企業やサプライヤーとの適切な BCM の手順を確実にできるとしており、BCMS の第三者認証規格になっている。

(4) BS25777-1:2008Information and communications technology continuity management - Code of practice(情報通信技術の継続性マネジメントに関する実践規範)(表 15 の項番 4)

[発行機関:BSI]

- BS25777-1 は、BS25999 において情報システムのレジリエンスを向上させるための具体的な記述が少ないのを補完する位置づけのガイドラインとして、2008 年に BSI が発行したものである。BSI が発行した「PAS77(IT Service Continuity Management)」の後継にあたるガイドラインである。第三者認証規格「BS25777-2」の公開準備も進められている。

3.2.2 米国における BCP 動向[56]

3.2.2.1 政府施策動向

(1) 民間組織におけるインシデント対応の審査及び認証プログラム(PS-Prep)

主管	米国国家安全保障省
名称	民間組織におけるインシデント対応の審査及び認証プログラム (PS-Prep:Voluntary Private Sector Preparedness Accreditation and Certification Program)
発効日/開始日	2007 年 8 月

米国のインフラ企業(交通、金融、ガス、電力、水道等)の 85%が民間企業となっている。そのため米国内では、インフラ企業が災害や事故等で業務が停止した場合の影響について懸念が強まっていた。このようなインフラ企業の多くが、災害対策計画や緊急対応計画、事業継続計画を策定しているが、その実効性について担保する仕組みは存在しない。また、中小規模の企業について、災害対策や緊急事態対策が進んでいないことも問題として認識されていた。

2001 年米国同時多発テロや、2005 年のハリケーンカトリーナ被災の際には、民間企業にも大きな被害が発生し、市民生活への影響が拡大した。また、事前に緊急事態対応計画類を準備していた企業は比較的被害が少なかったとも報告されている[57]。この背景をもとに 2007 年 8 月に議会によって承認された「9 月 11 日委員会勧告実施法(“Implementing Recommendations of the 9/11 Commission Act of 2007”、PUBLIC LAW 110-53)第 9 条 民間組織のインシデント対応」(以後「同法」)は、民間企業の事業継続を一定のレベルで確保するための仕組みづくりを目的としている。

56 東京海上日動リスクコンサルティング資料ほかより作成
http://www.meti.go.jp/meti_lib/report/2010fy01/E000900.pdf
57 指田朝久「カトリーナ災害と事業継続」(地域安全学会論文)

(2) PS-Prep 推進体制

同法の主管官庁は国家安全保障省(DHS: Department of Homeland Security)であり、その組織図及び主な推進部門は以下の通り。(太枠内の組織が Ps-Prep の主な推進担当組織)

FEMA が全体の取り組みを主導し、National Protection & Program 部門内にある Infrastructure Protection グループが、重要インフラ分野での対策推進に注力している。ここでは、PS-PREP 認証制度の立上げに合わせて、重要インフラ分野の事業者に求められる BCP の取り組み水準を示すガイドラインの整備が、既存の BCP 関連ガイドラインとの整合を踏まえつつ、分野毎に行われている。

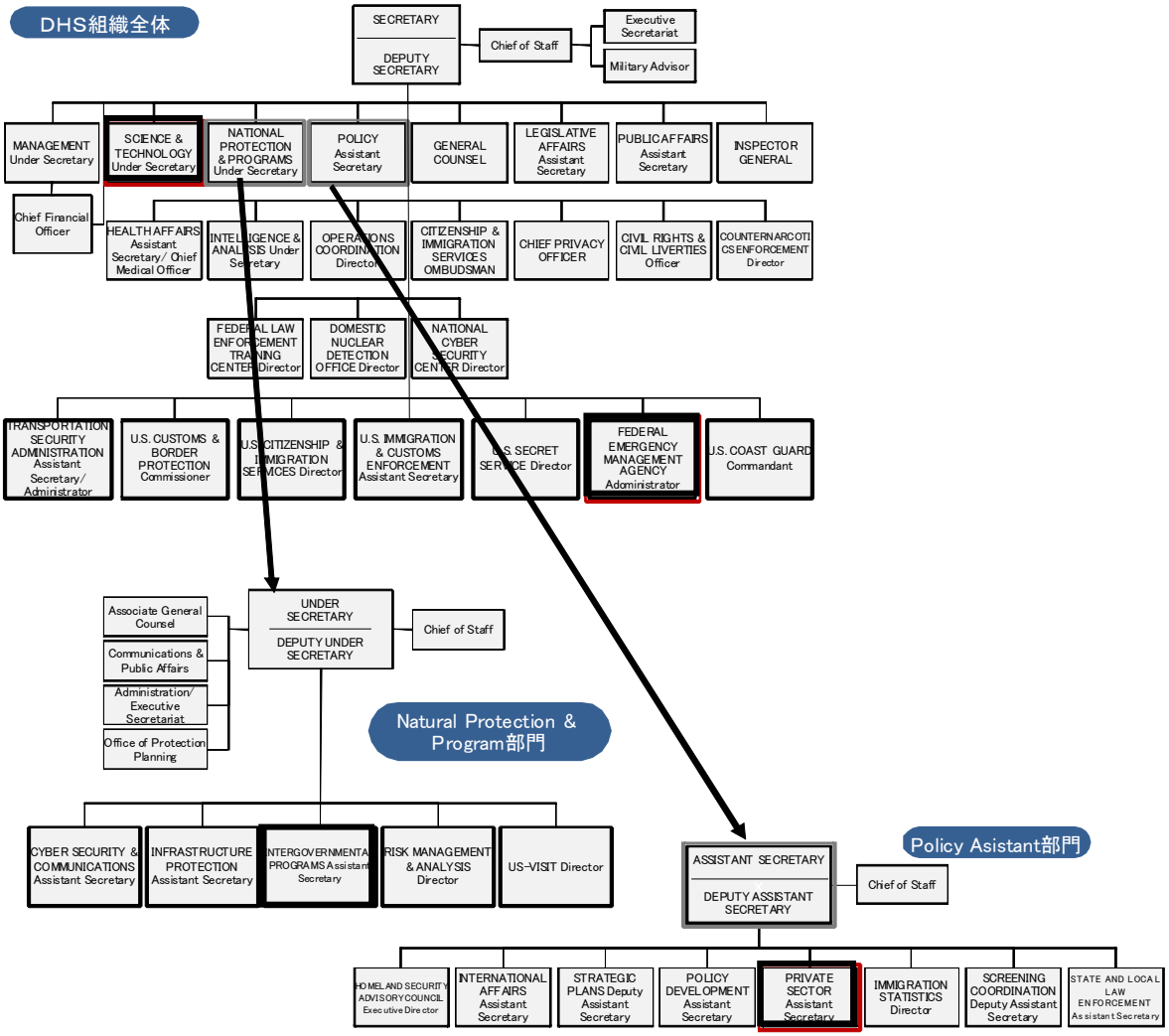


図 19. 米国国土安全保障省 組織図

(3) 緊急事態管理研修所(EMI: Emergency Management Institute)

EMI は FEMA の管轄する組織であり、メリーランド州エミツバーグにある国家緊急事態訓練センター(National Emergency Training Center 、NETC)の敷地内に所在している[58]。創設は 1980 年であり、それ以降政府及び地方自治体の職員や民間組織、自主防災活動組織、重要インフラ関連企業の

職員を対象とした災害対応及び緊急事態対応に関する教育を実施している。なお、参加費は無料である。

研修の形態としては、EMI 本部で実施する研修(レジデントコース)、地方政府拠点において EMI が支援して行う研修(ノンレジデントコース)、及びインターネット回線を利用した遠隔教育の三種類がある。各研修への年間参加者数は、レジデントコースが約 5，500 人、ノンレジデントコースが約 100,000 人、遠隔教育が数万人である。

研修は、災害被害の軽減、準備(計画)、対応、復旧の四分野についてそれぞれ提供されている。研修の内容は、大まかに分類して以下の通りである[59]。

・自然災害(地震、ハリケーン、洪水、ダム)
・人為災害(危険物質、テロ、放射能事故、化学物質関連事故)
・専門スキル
・リーダーシップ
・教育手法
・訓練の計画と評価
・情報技術
・広報
・総合緊急事態対応
・指導者育成

将来的に PS-Prep が開始された際には、その実施に関係する研修も実施することが検討されている。

3.2.2.2 BCP 普及状況

本節では、米国における BCP 普及状況について、KPMG 社によるアンケート調査結果をもとに記載する(※本調査は、BCM 関連のコンサルティング事業を行なう KPMG 社が発行する情報誌の読者が調査対象となっていることに留意する必要がある)。

(1) KPMG アンケートの実施概要

表 16. アンケート調査実施概要

調査対象	KPMG が発行する BCM 関連情報誌(”Continuity Insights”)の読者からサンプル対象者を募集
調査地域	全米
調査手法	ウェブサイト上でのアンケート
調査時期	2008 年 1 月
有効回答数	872 件

[59] http://training.fema.gov/aboutEMI.asp

表 17. アンケート回答組織の形態別回答割合

組織形態	KPMG 調査 (回答割合)
民間企業(株式上場企業)	43.74%
民間企業(株式非公開企業)	26.98%
政府・地方政府等	17.80%
非営利組織	11.48%

(2) BCM の実施状況

BCM の管理体制を構築済みとの回答が 58.19%、何らかの取組みを開始しているとの回答を含めた場合、95.53%の企業等が、2008 年 1 月の調査時点で BCM の取組みを既に実施していたことが分かる。

表 18. BCM の実施状況

Q.貴社の BCM プログラムの状況は以下のどれに最も近いですか？

実施状況	KPMG 調査 (回答割合)
BCM は実施していない	4.47%
現在BCMを構築中である (プログラムの範囲、目的、体制、予算、文書体系等を検討中)	11.23%
リスク分析や事業影響度分析を実施中である(初回)	6.53%
BCPや危機管理計画、災害復旧計画等の文書類を策定中である	19.59%
BCM の管理体制が整い、方針、各種文書、文書更新体制、訓練体制が整備されている	58.19%
	100.00%

(3) BCM の対象範囲

IT 事業者等の外部のサービス事業者を BCM の対象範囲に含めているとの回答は 50.75%、サプライチェーンを構成する企業等を対象範囲に含めているとの回答は 36.88%であった。

表 19. BCM の対象範囲(外部サービス事業者(IT 事業者等)への対応状況)

対応状況	KPMG 調査 (回答割合)
対象範囲に入れていない	25.32%
現在対象範囲を広げるべく作業中である	23.94%
重要な取引先について、全てではないが対象範囲としている	35.40%
全ての重要な取引先について、対象範囲としている	12.49%
全ての取引先について、対象範囲としている	2.86%
	100.00%

表 20. BCM の対象範囲(サプライチェーンへの対応状況)

対応状況	KPMG 調査 (回答割合)
対象範囲に入れていない	34.02%
現在対象範囲を広げるべく作業中である	29.10%
幾つかのサプライチェーン関係者を対象範囲に入れている	32.99%
全てのサプライチェーン関係者を対象範囲に入れている	3.89%

(4) BCP 発動状況

過去1年間の BCP 発動有無、及び過去1年間に使用した復旧手順書に関する調査結果を以下に示す。約半数の企業等が過去1年間に BCP を発動するような事態を経験していることが分かる。また、下図から過去1年間に使用した復旧手順書はほとんどが情報システム関連の障害からの復旧手順書であることが分かる。

これより、米国における BCP とは地震のような大規模災害を前提としたものだけではなく、情報システムの障害のような比較的対応が容易なリスク事象も、BCP の対象として捕らえている様子が伺える。

表 21. 過去 1 年間の BCP 等の発動有無

Q. 過去 1 年間に BCP、危機管理計画、災害復旧計画を発動したことがありますか?

過去 1 年間の BCP 等の発動	KPMG 調査
発動あり	49.71%
発動なし	50.29%

表 22. 過去1年間に使用した復旧手順書

復旧手順	KPMG 調査(回答割合)
ソフトウェア障害復旧計画	28.78%
データセンター復旧計画	15.02%
データ・ストレージ復旧計画	18.35%
電子メール復旧計画	19.15%
チャット機能復旧計画	8.14%
ネットワーク復旧計画	25.11%
電話通信復旧計画	19.50%
職務エリア復旧計画	27.75%
無し	40.60%

(5) 事業停止による損失額の定量化

事業停止による「1時間」の事業停止による損失額についての調査結果を以下に示す。多くの企業が自社の事業が停止した場合の影響度合いについて、金額換算で定量的に把握しており、リスクの度合いに応じて戦略的に BCM の構築を進めている状況が伺える。

表 23.「1時間」の事業停止による推定損失額

推定損失額	KPMG 調査 (回答割合)
5万ドル未満	19.82%
5万ドル以上　10万ドル未満	13.86%
10万ドル以上　25万ドル未満	10.88%
25万ドル以上　50万ドル未満	7.67%
50万ドル以上　100万ドル未満	6.19%
100万ドル以上　500万ドル未満	6.41%
500万ドル以上	3.21%
不明	31.96%
	100.00%

(6) BCM 実効性の確認方法

BCM プログラムを構築した企業等がその実効性をどのように確認しているかについての調査結果を以下に示す。訓練や監査による確認のほか、同業他社との比較、測定モデルとの比較、評価測定の実施等の回答が多かった。

表 24. BCM 実効性の確認方法

測定方法	KPMG 調査 (回答割合)
監査の実施	51.78%
同業他社との比較	31.84%
成熟モデルとの比較	15.81%
測定モデルとの比較	30.58%
評価測定の実施	22.68%
BCP訓練の実施	71.71%
サービスレベル評価	13.75%
規格類との比較	8.71%
復旧テストの実施	16.61%
測定は実施していない	13.97%
	100.00%

3.2.2.3 米国の BCP に関するガイドライン等

米国での主な BCP に関するガイドライン等を表 25 に示す。

米国は、テロや自然災害が多い土地であることから事業継続に関する意識が高い。2001 年に設立された DHS は、テロや自然災害等の緊急事態発生時の速やかな復旧のために、政府認定の民間認証機関による事業継続性認証プログラム PS-Prep(Voluntary Private Sector Accreditation and Certification Preparedness Program:緊急事態準備に関する適合性評価制度)の導入を決定した。PS-Prep には表 25 のガイドライン等に加え、表 15 に示した英国の BS25999 も採用している。

表 25. 米国の BCP に関するガイドライン等

項番	文書名	発行機関	発行月	対象組織	想定脅威		
					災害	疾病	IT 脅威
1	ANSI NFPA1600[60] (Standard on Disaster/Emergency Management and Business Continuity Programs -災害・緊急時の管理・事業継続プログラム)	NFPA(米国防火協会)	2010(初版は 2004 年 1 月)	全般(政府、NGO、企業、市民等)	○	ー	ー
2	ANSI/ASIS SPC.1[61] (Organizational Resilience - Security,Preparedness and Continuity Management Systems-Requirements with Guidance foe Use -組織レジエンス:セキュリティ、緊急事態準備、継続マネジメントシステム-要求事項及び利用の手引)	ASIS(ASIS インターナショナル)	2009 年 3 月	全般	○	○	○

表 25 に示すガイドライン等の概要を以下に示す。

(1) ANSI NFPA1600(災害・緊急時の管理・事業継続プログラム)(表 25 の項番 1)

[発行機関:NFPAI]

- NFPA1600 は、すべての災害・緊急時を対象とした管理・事業継続プログラムであり、政府、非政府組織(NGO)、民間団体、市民等地域や国を問わず適応できる規格として、NFPA(National Fire Protection Association:米国防火協会)と ANSI(American National Standards Institute:米国規格協会)によって策定されたものである。
- この規格では、防止、軽減、準備、対応、継続性、及び回復するために必要な、開発、実装、評価、事業継続プログラムの基本的な基準を提供している。

60 http://www.nfpa.org/assets/files/PDF/NFPA16002010.pdf

61 http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf

- 1995 年に災害管理の規格として初版が発行され、DHS、IAEM（International Association of Emergency Managers）、NEMA（National Emergency Management Association） が規格の開発に協力し、改訂を繰り返している。2010 年版では大きな改訂を行っており、章立てを一般的な PDCA（Plan、Do、Check、Act：計画、実行、評価、改善）の継続的手順と一致させ、また、リーダーシップ・コミットメントの重要性、記録管理に関する項目が新しく追加されている。2009 年には、安全法に基づいたテロ対策技術として DHS に認定されている。DHS が推進する PS-Prep の適用基準の一つ。
- 米国の NFPA（National Fire Protection Association：米国防火協会）は 1896 年に設立された、国際的な非営利団体であり、火災やその他の危険から生活を守るための規格の策定や研究、教育等を提供している。NFPA は、政府関連組織として、設立当時から NIST(当時は National Bureau of Standards)と関連が深く、また DHS とも関連が深く、ガイドライン策定においても影響を受けていると考えられる。

(2) ANSI/ASIS SPC.1(Organizational Resilience - Security,Preparedness and Continuity Management Systems-Requirements with Guidance foe Use -組織レジエンス：セキュリティ、緊急事態準備、継続マネジメントシステム-要求事項及び利用の手引（表 25 の項番 2）

[発行機関：ASIS インターナショナル]

- SPC.1 は、組織のセキュリティ、緊急事態準備、継続マネジメントシステムを構築する際の手引であり、あらゆる形態の組織に適応できるとしている。ASIS インターナショナル（Advancing Security Worldwide International）が策定したものである。2009 年に初版が発行され、同年に ANSI によって米国規格として承認を受けている。
- テロや自然災害等の不足の事態に対して、発生前から準備し、発生後には事業中断を最小限にとどめ、早期に通常状態に復旧するしくみを構築する手引きである。安全法に基づいたテロ対策技術として認定されている。DHS が推進する PS-Prep の適用基準の一つ。
- ASIS インターナショナル（Advancing Security Worldwide International）は、1955 年に設立された、国際的な一般社団法人であり、セキュリティの情報提供や共有、教育、出版、展示会等を行っている。ASIS は米国の内国歳入法典第 501 条C項 3 号（501（c）（3））の規定に基づき、連邦法人所得税免税や寄付税制上の優遇措置等の対象となる免税(Exempted)非営利公益法人の一つ。

3.2.3 シンガポールの BCP に関する動向

シンガポールについては、具体的な取組に関する公的情報が見当たらず、ここでは主な BCP に関するガイドラインを示すことで動向とした。

表 26. シンガポールの BCP に関するガイドライン等

項番	文書名	発行機関	発行月	対象組織	想定脅威		
					災害	疾病	IT 脅威
1	SS540:2008[62] 事業継続管理のためのテクニカル・レファレンス	SPRING (Standards,Productivity and Innovation Board) Singapore	2008 年	シンガポールの企業全般	特定されていない		

表 26 に示すガイドライン等の概要を以下に示す。

(1) SS540:2008 事業継続管理のためのテクニカル・レファレンス (表 26 の項番 1)

[発行機関:SPRING]

- SS540:2008 は、事業継続管理のための技術規格書であり、その対象は、規模の大小を問わずすべての組織に適用できるとしており、また、組織の機能を停止させるような脅威(意図的/非意図的、予期していた/予期していない危機、災害)すべてに対して対応するものとしている。
- シンガポール政府の外郭団体であり、企業をサポートする国内規格団体でもある SPRING によって、2005 年に TR19 として一時的な規格として発表され、2 年間の試行期間を経て、2008 年にシンガポールの標準規格 SS540 として策定された。
- なお、本ガイドラインは、対象組織を問わないとしているが、SPRING は、シンガポールの経済産業省にあたる Ministry of Trade and Industry が監督官庁としてかかわっている団体であることからも、民間企業をサポートする目的で策定された規格であると考えられる。
- この規格は、 重要な資産、人物、環境、無形資産、物理資産の堅ろう性と保護を強調しており、ICT 分野のBCMとして、3.2.4 に示す国際規格「ISO/IEC 27031(事業継続性のための情報通信技術準備ガイドライン)」で参照されている規格である。

62 http://www.singaporestandardseshop.sg/product/productView.aspx?id=235b31c7-7d39-4282-9205-6e4a5a3f7805

3.2.4 国際規格化されたBCPに関するガイドライン等

これまでの各国の取組とは別に、ISOで国際規格化されたBCPに関する状況を、ガイドライン等を代表例として以下に示す。

表 27. 国際規格化されたBCPに関するガイドライン等

項番	文書名	発行機関	発行月	対象組織	想定脅威		
					災害	疾病	IT脅威
1	ISO/PAS 22399:2007[63] 社会セキュリティー緊急事態準備と業務継続マネジメントガイドライン	ISO	2007年11月	全般	○	○	○
2	ISO/DIS 22301[64] 社会セキュリティ-緊急事態準備と業務継続マネジメント要求事項	ISO	2010年11月	全般	○	○	○
3	ISO/IEC 27031[65] 事業継続性のための情報通信技術準備ガイドライン	ISO	2011年3月	全般	○	○	○

表 27 に示すガイドライン等の概要を以下に示す。

(1) ISO/PAS 22399:2007 社会セキュリティー緊急事態準備と業務継続マネジメントガイドライン (表 27 の項番 1)

[発行機関:ISO]

- ISO/PAS 22399は、ISO(International Organization for Standardization:国際標準化機構)のTC 223(社会セキュリティに関するISOの専門委員会)が、組織における緊急事態への準備と業務の継続に関する一般的な原則及び要素を提供する指針として検討を進めており、2007年にPAS (Publicly Available Specification:公開仕様書)として発行されている。
- 検討には50カ国以上の国が参加し、主要な取組を行ってきた日本、米国、英国、イスラエル及びオーストラリアの5カ国の国内規格又は政府の指示文書等を組み合わせたものである。
- 日本からのインプット情報作成時に国内規格「事業継続計画策定ガイドライン(経済産業省、2005年発行)」、「事業継続ガイドライン一版(内閣府中央防災会議専門調査会、2005 年発行)」が参照されている。次の(2)に示す「ISO/DIS 22301」のベストプラクティスを纏めたものにあたる。

(2) ISO/DIS 22301(社会セキュリティ-緊急事態準備と業務継続マネジメント要求事項ドライン)

63 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50295

64 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50038

65 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44374

（表 27 の項番 2）

［発行機関：ISO］

- ISO/DIS 22301は、ISOのTC223が、組織における緊急事態への準備と業務の継続に関するマネジメントシステムの要求事項として検討を進めており、2010年にDIS（Draft International Standard：国際規格原案）として発行されている。すべての組織に適応できるとしているが、基準に基づく画一的なシステム、体制を求めるものではない。組織のBCMSの要求事項を規定している。

(3) ISO/IEC 27031（事業継続性のための情報通信技術準備ガイドライン）（表 27の項番3）

［発行機関：ISO］

- ISO/IEC 27031は、ISOとIEC（International Electrotechnical Commission：国際電気標準会議）のJTC1（Joint Technical Committee 1：第1合同技術委員会）におけるSC27（情報セキュリティに関する標準化を担当する専門委員会）が、事業継続の活動において、特に事業継続性のためのICT（Information and Communication Technology：情報通信技術）準備（IRBC（RBC： Readiness for Business Continuity））に対して焦点をあて、2010年にFDIS（Final Draft International Standard：最終国際規格原案）が発行され、2011年3月1日に正式版として発行されている。
- IRBCとして組織が構築すべきフレームワークやプロセスを記述したガイドラインであり、情報セキュリティマネジメントシステム(ISMS)及び／又は事業継続マネジメントシステム(BCMS)が構築されている組織において、IRBCがどのように実装，運用されるかについても言及している。

3.2.5 海外の BCP で求められている要件等

海外の BCP に関する政策やガイドライン等について文献等（インターネット上での公開情報、書籍等）により調査した、海外におけるBCPの推進体制、BCPが備えるべき要件、直面している課題等について、重要インフラサービスの維持・継続に関わる重要システムの安定運用の視点で整理した結果を以下に示す。

3.2.5.1 事業継続計画の推進体制

海外（英国、米国、シンガポール）及び国際規格で求められている推進体制について調査した結果、どの規格においても推進組織の確立、経営陣の関与が必要だと記しており、記述の詳細さは異なるが、日本のガイドライン等が示す推進体制と大きな差異はないと考える。

以下に海外（英国、米国、シンガポール）及び国際規格で求められている推進体制について調査した結果を(1)～(4)に示す。

(1) 英国

GPG2010、BS25999-1:2006 及び BS25999-2:2007、BS25777-1:2008 のそれぞれにおける推進体制に関する記述を以下に示す。

≪GPG2010≫

【推進組織について】

BCMプログラム推進のため、以下のような役割を持つグループを設置する場合もある。
·BCM プログラム委員会または運営委員会
 -助言、指導、管理監督を与えるための管理グループ

·ビジネスの継続性チーム
- インシデントに対応し、誰が BCP 作成に大きな役割を担うべきかを判断するための戦術戦略的運用チーム

·インシデントレスポンスフォーラム
- 調整の問題を解決するため、インシデントレスポンスに関与するすべてのチームの代表者を含むフォーラム。このグループは、訓練や実施に必要な要件を選定するために有効である。

【以下原文】

Additional groups may be formed to assist in the development of the BCM programme. These include:
· BCM Programme Board or Steering Committee
 - a management group to give advice, guidance and management oversight

· Business Continuity Teams
- the strategic, tactical and operational teams that would respond in an incident, and who should contribute significantly to the writing of the Business Continuity Plans

· Incident Response Forum
- a forum comprising representatives of all teams involved in incident response to resolve coordination issues. This group may be a useful focus for identifying training and exercising requirements

【経営陣について】

トップマネジメントのメンバーは、組織の BCM 能力とその有効性の全体的な責任を与えられるべきである。これは、BCM のプログラムに対して、組織内の重要性を適切なレベルで効果的な実装を行う大きなチャンスを与えられていることを保証する。

【以下原文】

A member of Top Management should be given overall accountability for the organization's BCM capability and its effectiveness. This ensures that the BCM programme is given the correct level of importance within the organization and a greater chance of effective implementation.

【BCM マネージャーについて】

BCM プログラムを管理するため、ほとんどの組織では、Business Continuity Manager と呼ばれる個人を指名する。この役職は、組織の規模に応じてフルタイムもしくはパートタイムの役割となる。

大規模な組織では、以下の活動を支援するため、BCM マネージャーを補助する人員を追加する場合もある。

·訓練の運営
·情報収集
·既存ドキュメントの改訂
·BCM 実装の補助
·限定的な分野での BCM 取り纏め

【以下原文】

An individual should be appointed to manage the BCM programme and (in most organizations) will be known as the Business Continuity Manager. Depending on the size of the organization, this may be a full or part time role.

For larger organizations, additional staff may be nominated to work with the BCM Manager to assist with the following activities:

· Conduct exercises
· Information collection
· Undertake documentation revisions
· Assist in BCM implementation
· Act as BCM coordinator in their areas

≪BS25999-1:2006、BS25999-2:2007≫

【推進組織について】

BS25999-1:2006 5.2.1 注釈

事業継続計画の実装と維持を担当する者は、組織の大きさ、規模及び複雑さに応じて、組織の多くの領域に所属する場合がある。

但し、適切な権限を持つ者（例えば所有者、取締役又は選出された代表者）が、BCM の全体的な責任を持ち、この機能の継続的な成功を確保するために直接説明義務を負うことが不可欠である。

【以下原文】
COMMENTARY ON 5.2.1
Individuals tasked with implementing and maintaining the business continuity programme may reside in many areas of an organization depending on its size, scale and complexity. It is essential, however, that a person with appropriate authority (e.g. owner, board director or elected representative) has overall responsibility for BCM and is directly accountable for ensuring the continued success of this capability.

【経営陣について】
BS25999-1:2006 5.2.1
BS25999-2:2007 3.2.3.3
経営トップは、以下のことを実施しなければならない。
a)BCM のポリシーや実装の説明責任を負うため、適切な上位性と権威を持つ人を指名もしくは推薦する。
b)他の責務と無関係に BCMS を導入、維持するべき人を 1 名以上指名する。

【以下原文】
Top management shall:
a) appoint or nominate a person with appropriate seniority and authority to be accountable for BCM policy and implementation;
and
b) appoint one or more persons, who, irrespective of other responsibilities, shall implement and maintain the BCMS.

≪BS25777-1:2008≫
BS25999-1:2006 で不足していた情報システムのレジリエンスを向上させるためのガイドラインとして発行されたため、体制についての記述なし。

(2) 米国
ANSI NFPA1600、ANSI/ASIS SPC.1のそれぞれにおける推進体制に関する記述を以下に示す。

≪ANSI NFPA1600≫
【推進組織について】
4.3 * プログラム委員会。
4.3.1 * プログラム委員会は、そのポリシーに基づいた実体によって確立すること。
4.3.2 プログラム委員会は、そのプログラムの準備、開発、実施、評価、及びプログラムのメンテナンスの調整、支援を提供すること。
4.3.3 * プログラム委員会は、専門的技術、実体に関する知識、及び実体の中ですべての主要な機能的領域からのリソースを特定する能力を持っているプログラムコーディネータと他のものを入れ、適切な外部の意見を求めること。

【以下原文】
4.3* Program Committee.
4.3.1* A program committee shall be established by the entity in accordance with its policy.

4.3.2 The program committee shall provide input for, and/or assist in, the coordination of the preparation, development,implementation, evaluation, and maintenance of the program.
4.3.3* The program committee shall include the program coordinator and others who have the expertise, the knowledge of the entity, and the capability to identify resources from all key functional areas within the entity and shall solicit applicable external representation.

【経営陣について】

4.1 *リーダーシップとコミットメント
4.1.1 指導部は、インシデントの予防、重大な問題とならないような緩和策、準備、対応、対応中の継続性維持のため、プログラムへのコミットメントを明確に示さなければならない。
4.1.2 指導部のコミットメントは、以下を含まなければならない。
(1)プログラムのポリシー、計画、及び開発、実装、保守手順
(2)プログラムサポートのためのリソース
(3)プログラムの有効性を確保するためのレビューや評価
(4)不足しているものの補充
4.1.3 実体は、ポリシー、実施計画に準拠し、プログラムをサポートするために開発されて手順に従わなければならない。

【以下原文】

4.1* Leadership and Commitment.
4.1.1 The entity leadership shall demonstrate commitment to the program to prevent, mitigate the consequences of, prepare for, respond to, maintain continuity during, and recover from incidents.
4.1.2 The leadership commitment shall include the following:
(1) Policies, plans, and procedures to develop, implement,and maintain the program
(2) Resources to support the program
(3) Reviews and evaluations to ensure program effectiveness
(4) Correction of deficiencies
4.1.3 The entity shall adhere to policies, execute plans, and follow procedures developed to support the program.

【プログラムコーディネータについて】

4.2 *プログラムコーディネータ
プログラムコーディネータは、エンティティが任命するものとし、プログラムの開発、実装、管理、評価、及び維持する権限を持つ。

【以下原文】

4.2* Program Coordinator.
The program coordinator shall be appointed by the entity and authorized to develop, implement,administer, evaluate, and maintain the program.

≪ANSI/ASIS SPC.1≫
【推進組織について】

【以下翻訳版より】
破壊的なインシデントの最中に危機管理を効果的に担うために、適切な管理組織が置かれることが必要である。管理組織、決定権限、及び実施責任について明確な定義が存在しなければならない。組織はインシデント/事象への対応を指導するための危機管理チームを持つことが望ましい。このチームは、上級経営者又はその代表者の明確な指示に基づき、経営資源人事、情報システム、設備、保安・警備、法務、広報、製造、倉庫管理、及びその他の事業上重要な支援機能を果たす職務者で構成されることが望ましい。

危機管理チームは、組織の規模及びタイプ、従業員の数、場所等といったような構成要素を考慮して、適切だと思われる多くの対応チームによる支援を受けることができる。

【経営陣について】

【以下翻訳版より】
このコミットメントの一部として、トップマネジメントは、マネジメントシステムを実施するために定義された責任及び権限をもった、特定の管理代表者を指名することが望ましい。大規模又は複雑な組織では、指名された代表者が複数いてもよい。小規模又は中規模の企業では、これらの責任を一人の個人が引き受けても差し支えない。

(3) シンガポール

SS540:2008 における推進体制に関する記述を以下に示す。

≪SS540:2008≫
【推進組織について】

3.3BCM の運営委員会
組織の戦略的な回復・継続計画を決定する使命をもつ、事業所有者、技術専門家や事業継続の専門家等の意思決定者から成る委員会。(この委員会には、任命経営幹部の一人または複数のメンバーを含む)
プロジェクトの完了時に解散される通常のプロジェクト管理委員会とは異なり、この委員会は永続的なもの。

【以下原文】
3.3BCM steering committee
A committee of decision makers (including one or more members of executive management appointed to this committee), business owners, technology experts and business continuity professionals, tasked with making strategic recovery and continuity planning decisions for the organisation.
Unlike usual project management committee that is disbanded on completion of the project, this commitee is permanent.

【経営陣について】

3.20 エグゼクティブ管理
組織内の最高意思決定レベルの者を置く。

【以下原文】
3.20 exective management
the highest decision making level in the organisation

(4) 国際規格

ISO/PAS 22399:2007、ISO/DIS 22301、ISO/IEC FDIS 27301 のそれぞれにおける推進体制に関する記述を以下に示す。

≪ISO/PAS 22399:2007≫

【推進組織について】

実装のための組織体制
ポリシーやプログラム戦略はプロジェクトチームによって計画、実施される。
以下を備える公式または非公式のプロジェクト管理体制が必要である。
- トップマネジメントの可視性と関与を継続するための要件
- スキル要件
- プロジェクトのリソース、予算、資金調達の要件
- 組織の専門知識
- プロジェクトに関わっている組織分野

(途中略)
部門横断的に IPOCM(Incident Preparedness and Operational Continuity Management:緊急事態準備と業務継続マネジメント)プログラム委員会を形成する場合もある。
そのメンバーは、様々な組織全体の問題を解決するために有効な、IPOCM プログラムに関連する主要な機能に関与する部門で構成されなければならない。

【以下原文】

Organizational structure for implementation
Policy and strategy for the program is developed and implemented by the Project team. Determine the need for formal or informal project management structures based on:

– requirements for continuing top management visibility and involvement;
– skills requirements;
– resource, budget, and financing requirements for the project;
– specialist knowledge of the organization;
– areas of organization involved in the project.

(途中略)
A cross-functional IPOCM program committee may be formed. Its members should be composed of those involved in the major A cross-functional IPOCM program committee may be formed. Its members should be composed of those involved in the major functions relating to the IPOCM program in order to enable it to address various organization-wide issues.

【経営陣について】

経営トップの責任と権限は、その組織の最終的な責任はどこにあるかを明確にするために定義する必要がある。

【以下原文】
Responsibility and authority of top management should be defined in order to make it clear where ultimate responsibility lies in the organization.

【プログラムコーディネータについて】
組織は、IPOCM プログラム設立の責任を持つべき IPOCM プログラムコーディネータを指名できる。

IPOCM プログラムコーディネータは、インシデントへの準備と業務継続のプロジェクトの調整、経営トップからの支持の獲得、計画と導入、IPOCM プログラムのトレーニングの実施、定期的な緊急事態への準備と業務継続性の確認を行う責任を負わなければならない。

【以下原文】
An organization may appoint an IPOCM program coordinator who should have responsibility for establishing the IPOCM program.

The IPOCM program coordinator should be responsible for coordinating incident preparedness and operational continuity projects, managing incident preparedness and operational continuity organizational structure, obtaining support from top management, developing and implementing the IPOCM program, providing training, and regularly reviewing the incident preparedness and operational continuity program among others.

≪ISO/DIS 22301≫
【推進組織について】
記述なし。

【経営陣について】、【事業継続計画責任者について】
トップマネジメントは、BCM に関してリーダーシップを発揮しなければならない:
–目に見える形で全体的な方向性とオペレーションを指示及びコントロールする
– BCMS が組織の事業継続性のパフォーマンスに寄与することを確実にするよう、各人の動機付けを行う。
注
リーダーシップの発揮は、経営トップのみに限定されない。

【以下原文】
5.1
General
Top management shall demonstrate leadership with respect to the BCMS by:
–visibly directing and controlling its overall direction and operation;
–motivating persons to ensure the BCMS supports the business continuity performance of the organization.
NOTE
Leadership is not restricted to just top management.

≪ISO/IEC 27031≫

【推進組織について】

IRBC プログラムのサポートや管理のために、多くの専門的な IRBC 実践者や、その他の管理分野や部門のスタッフが必要となる場合がある。

【以下原文】

A number of professional IRBC practitioners and staff from other management disciplines and departments may be required to support and manage the IRBC program.

【経営陣について】

5.7.1 管理のリーダーシップとコミットメント

IRBC プログラムを効果的なものにするためには、十分に組織へ統合したプロセスであり、組織の管理活動、組織のトップによる働きかけ、経営トップにより支持され推進されるものであることが必要である。

【以下原文】

5.7.1 Management leadership and commitment

To be effective an IRBC program should be a process fully integrated with the organization's management activities, driven from the top of the organization, endorsed and promoted by top management.

3.2.5.2 事業継続計画が備えるべき要件

海外（英国、米国、シンガポール）及び国際規格で求められている「備えるべき要件」について調査した結果、基本的な要件については、日本のガイドライン等が示す要件と大きな差異はないが、重要システムの安定運用の視点では異なる点が見られた。

以下に海外（英国、米国、シンガポール）及び国際規格が示す「備えるべき要件」について調査した結果を(1)～(4)に示す。

(1) 英国

GPG2010、BS25999-1:2006、BS25999-2:2007 では日本と同等に基本的な BCP の要件が記されている。なお、日本のガイドライン等と異なる視点として次のような記載がなされている。

・BS25777-1:2008 は BC25999 で不足していた情報システムのレジリエンス向上を目指し、策定されたガイドラインであり、BCP の検討の中で情報通信技術（ICT）継続の検討も考慮することという要件が記されている。また、事業継続のための ICT の要件を理解する必要があるとし、ICT サービスの維持には、事業継続性の要件に加えて、リスクや追加のレジリエンス、回復リソースのための、資金や予算分配が必要になることを理解する必要があると記されている。

≪BS25777-1:2008≫

組織は、ICT の継続性管理の範囲を定義する必要がある。ICT の目標を設定するには以下を考慮する必要がある

a)ICT の継続のための要件;

b)事業継続性の範囲、目的と義務、規制法令及び契約上の義務

c)リスクと ICT リスクの許容レベル。

d)事業継続性の要件
e)その主要なステークホルダーの利益。

組織は、事業とICTの継続の範囲内でのICTシステムを識別する必要がある。
【以下原文】3.2.1
General
The organization should define the scope of ICT continuity management and set ICT objectives, with due regard to the:
a)requirements for ICT continuity;
b)business continuity scope, objectives and obligations, including statutory, regulatory and contractual duties;
c)acceptable level of risk and ICT risks;
d)business continuity requirements; and
e)interests of its key stakeholders.
The organization should identify the ICT systems within the scope of business and ICT continuity.

≪BS25777-1:2008≫

4.1　事業継続性の要件を満たすためにICTの継続性の要件を定義する
(途中略)
4.2 重要なICTサービスを理解する
(途中略)
4.3 事業継続性の要件と重要なICTの継続能力との間の特定のギャップを理解する
(途中略)
4.3.2 トップマネジメントは、重要なICTサービスの継続能力と事業継続性の要件の間にあるギャップを知らされなければならない。
このようなギャップは、以下のようなリスク、追加のレジリエンス、及び回復リソースが必要である場合がある。
a)スタッフ。人数、スキルや知識を含む。
b)ICTの施設。例えば収容するために使用される施設コンピュータルーム。
c)サポート技術。プラント、機器及びネットワーク(技術)。
d)情報のアプリケーションやデーターベース
e)外部サービスとサプライヤー(供給)。
このような追加のレジリエンスと回復リソースには、さらに資金や予算配分が必要な場合がある。

【以下原文】
4.1Defining ICT continuity requirements to meet business continuity requirements
(途中略)
4.2Understanding critical ICT services
(途中略)
4.3Identifying gaps between critical ICT continuity capability and business continuity requirements
(途中略)
4.3.2
Top management should be informed of any gaps between critical ICT services continuity capability and business continuity requirements.
Such gaps might indicate risks and the need for additional resilience and recovery resources, such as:
a) staff, including numbers, skills and knowledge;

b) premises used to house ICT facilities, e.g. computer room;
c) supporting technology, plant, equipment and networks (technology);
d) information applications and databases; and
e) external services and suppliers (supplies).
Such additional resilience and recovery resources might require further finance or budget allocation.

(2) 米国

ANSI NFPA1600 では日本と同等に基本的な BCP の要件が記されている。なお、日本のガイドライン等と異なる視点として次のような記載がなされている。
・システムに係る要件としては、ANSI/ASIS SPC.1 にて、計画策定時のリスクアセスメント及び影響度分析の際に、システムの維持にかかる内容として、データ及び通信の完全性並びにサイバーセキュリティを考慮するよう記されている。

≪ANSI/ASIS SPC.1≫

【以下翻訳版より】
A.3 計画
A.3.1 リスクアセスメント及び影響度分析
（途中略）
リスクアセスメント及び影響度分析は、下記であることが望ましい
a）組織の活動、機能、製品、及びサービスに関係したリスク、並びにそれらの危機状態に、そして組織の業務、人間、財産、資産、報酬の支払い能力、イメージ及び評判、利益、信用、並びに/又は環境に対する直接的、若しくは間接的な影響を与えるそれらの潜在力に、検討を加えること
b）特定された潜在的リスク及びそれらが現実になった場合のそれらの影響の重大性に関する可能性又は確率を見積もるため、文書化された定量的又は定性的方法論を利用すること
c）その業務に対し認められるすべての潜在的リスクを十分に考慮することにより、合理的な基準を基礎とすること
d）重要なインフラストラクチャ及びサプライチェーン依存状態並びに責務を含む、他者へのその依存状態及び組織への他者の依存状態を検討すること
e）データ及び通信の完全性並びにサイバーセキュリティを検討すること
f）組織の活動を統制する法的及びその他の義務の結果を評価すること
g）ステークホルダー、下請け業者、サプライヤー及びその他の影響を受ける関係者と関連したリスクを検討すること
h）リスクに関する情報を分析し、重大な結果を引き起こすかもしれないリスク及び/又は、その結果が重大性に関して決定され難いリスクを選択すること
i）想定される各々のハザード又は脅威にあるレジリエンスのレベル並びに、重要で欠くことのできない危機的な各資産を分析し評価すること
j）管理及び影響を与えることができるリスク及び影響力を評価すること。（しかし、どんな状況でも、リスクの需要、回避、管理、最小化、許容度の変化及び/又は処理のため、管理の程度及びその戦略を決定するのは組織である。）

(3) シンガポール

基本的な BCP の要件、システムに係る要件どちらも、日本と同等の記述である。なお、日本のガイドライン等と異なる視点として次のような記載がなされている。
・システムに関しては、重要な機能/重要なビジネス機能をサポートするために必要となる情報システムを特定しなければならないと記されている。

≪SS540:2008≫

8.2.8
情報及び情報システムの要件

回復中に CBFs(Critical functions/critical business functions:重要な機能/重要なビジネス機能)をサポートするために必要な情報及び情報システムが特定されなければならない。
以下のような要件を定めたポリシーが含まなければならない
a) 重要な記録。例えば顧客の注文及びフォームのドキュメント。
b) 電子バックアップ及びストレージ。例えば前日の取引
c) マニュアルの手順
d) IT システムやアプリケーションプログラム。

【以下原文】
8.2.8
Information and information system requirements

The information and information system required to support CBFs during recovery shall be identified.
Policies stipulating such requirements shall include:
a) Vital records, e.g.documentation of customer orders and forms;
b) Electnoic backup and storage, e.g. previous day's transactions;
c) Manual procedures;and
d) IT systems and application programs.

(4) 国際規格

ISO/PAS 22399:2007 ISO/DIS 22301 では日本と同様に基本的な BCP の要件が記されている。なお、日本のガイドライン等と異なる視点として次のような記載がなされている。
・システムに係る要件としては、ISO/IEC 27031 にて、重要な ICT サービスを理解すること、事業継続の要件と ICT 継続の要件にはギャップが生じることを認識し、それを考慮した計画の策定が必要だと記されている。

≪ISO/IEC 27031≫

6.3.2 重要な ICT サービスの理解
(途中略)
それぞれの重要な情報通信サービスについて、現在の継続能力を、例えば、単一点障害の様なサービスの中断や劣化のリスクを評価するために予防の観点から検討する必要がある。(全体的な BCM リスクアセスメント活動の一環としてみなすことができる)。ICT サービスのレジリエンスを向上し、それによりサービス中断の可能性、サービス中断の影響を低下させるための機会が求められるべきである。また、ICT サービス中断の早期発見及び対応を可能とする機会を強調することがある。組織がサービスのレジリエンスを改善するために特定の機会に投資するビジネスケースがあるかどうかを判断することができる。このサービスのリスク評価は (組織、組織のリスク管理フレームワークの一部を形成するこ

とがある)、ICT サービスの回復能力を強化するためのビジネスケースを助言するかもしれない。

6.3.3 ICT の準備機能及び事業継続性の要件間の特定ギャップ
それぞれの重要な情報通信サービスについて、現在の ICT の準備手配(予防、監視、検出、対応、復興など) に対し、事業の継続のために必要な ICT の要件と比較して、必要なすべてのギャップ(乖離)を文書化しなければならない。

【以下原文】
6.3.2 Understanding critical ICT services
(途中略)
For each critical ICT service the current continuity capability should be reviewed from a prevention perspective to assess risks of service interruption or degradation (which can be taken as part of the overall BCM risk assessment exercise), e.g. single points of failure. Opportunities should also be sought to improve ICT service resilience and thereby lower the likelihood and/or impact of service disruption. It may also highlight opportunities to enable early detection and reaction to ICT service disruption. The organization can decide if there is a business case to invest in identified opportunities to improve service resilience. This service risk assessment (which may form part of the organization's overall risk management framework) may also advise the business case for enhancing ICT service recovery capability.

6.3.3 Identifying gaps between ICT Readiness capabilities and business continuity requirements
For each critical ICT service the current ICT Readiness arrangements – such as prevention, monitoring, detection, response and recovery – should be compared with business continuity requirements and any gaps should be documented.

3.2.6 海外の BCP 事例

3.2.6.1 米国における事業者の取組事例(大手 IT 機器製造事業者)[66]

米国大手 IT 機器製造時業者の BCP 取組事例を以下に示す。本企業は、事業のグローバル化が進んでおり海外拠点も含めて過去に様々なリスク事象を経験しているため BCP に対する意識も高く、2005 年頃に外部からリスクマネジメントの専門家を招き、2010 年 2 月時点で 4 名の担当者からなるリスク管理部門及び各拠点のリスクマネージャーを中心として高度な取組を行っている。独自に開発したレジリエンシー指標やオンライン上の特別サイトを用いたサプライチェーン企業の効果的な管理は、国内の重要インフラ事業者にとっても参考になるものと考えられる。

表 28 米国大手 IT 機器製造業者の BCP 取組事例

	米国大手通信機器製造業者
体制	本社リスク管理部門には、4 名の職員が勤務している。また、各拠点に 1 名、リスクマネージャーが勤務している。全社的に合計すると、リスクマネジメントを担当している職員は 40 名程度である。 2005 年頃に当社にリスクマネージャーとして採用された。
過去の被災体験	世界中に拠点があるため、災害や事故に遭う可能性が非常に高い。近年経験した事例は以下の通りである。 2005 年 ハリケーンカトリーナによる物流の混乱 2006 年 台湾地震におけるアジア地域のインターネット回線の混乱 2007 年 A 社のホームページ停止 2008 年 四川大地震によるサプライチェーンの混乱 2008 年 ヨーロッパの支社における強盗事件 2008 年 ムンバイのホテルにおけるテロ事件 2009 年 H1N1 新型インフルエンザ 四川大地震では、サプライヤーの 6 社が被災した。その際には、サプライチェーン・リスクマネジメント部門が迅速に影響を把握し、代替調達の実施などで影響を最小限にとどめた。
取組みへの主な動機要因	現在の仕組みができた経緯は、以下の通りである。 2004 年 経営陣の主導により事業継続プログラムが開始される。この背景としては、 会社が大きくなり、リスクマネジメント体制を統合する必要が生じたためである 。 非常に数多くの取引先から、事業継続体制について質問が来ており、市場の圧力を認識している。過去 6 ヶ月間に BCM 関連の質問を寄せてきた取引先(主に販売店)との取引合計額が、10 億ドルに上ることが明らかになった。
主なリスク	上述の被災経験のあるリスクに加え、サンノゼ市における大地震や、9.11 テロレベルの事件が将来発生することを見込んでリスクマネジメントを実施している。 本社の所在するカリフォルニア州は、地震が多い地域である。そのため、本社では大地震を想定した訓練を毎年実施し、事業継続計画に反映している。

[66]東京海上日動リスクコンサルティング資料ほかより作成
http://www.meti.go.jp/meti_lib/report/2010fy01/E000900.pdf

	米国大手通信機器製造業者
取引先への確認方法	サプライヤー・リスクマネジメントの運用には、以下の要素が含まれる: 取引先の場所と連絡先の把握 取引先の事業と拠点に関する評価の実施 重要なパーツがどこで製造されているかの追跡調査 各サプライヤーの復旧時間(TTR: Time to Recover)の設定 各サプライヤーの BCP の監査及び試験 上記「取引先の事業と拠点に関する評価の実施」においては、50 程度の質問に回答させ、その結果から評価を行う。 上記「重要なパーツがどこで製造されているかの追跡調査」においては、サプライヤーの取引先(外注先)拠点まで確認している。 また、世界中の災害や事件(1 日に 10 から 50 件程度発生している)の分析を行い、A 社のサプライヤーに影響が及ぶ場合は迅速に把握できるシステムを構築している。 各サプライヤーについて、どのようなリスクが最も影響が大きくなりそうか把握している。そのようなリスクには、地震も含まれる。地震のような大規模災害が想定される場合は、代替サプライヤーの準備が基本的な対策である。
取引先への要求	上記各プロセスを効率的に実施するための、オンライン上の特別サイトを設置・運用している。そのサイトで収集された情報は、サプライチェーン・データベースに入力され、サプライヤー戦略等に利用されている。
認証制度へのスタンス	事業継続マネジメントの構築にあたっては、BS25999 などの各種ガイドラインを参考としている。ただし、全社的に特定単一の規格等の認証を受けているわけではない。これは、一つの規格のみに準拠した場合、抜けや漏れが発生する可能性があるからである。ただし、一部の支社では、緊急対応に関する規格の認定を受けていることもある。 明確にひとつの規格に準拠するのではなく、各規格を検討し、その中からよい部分を参考にすることにしている。 PS-Prep については任意プログラムであるので、当面は参加しない予定である。ただし、将来市場の状況によっては参加を検討する。
その他特徴的な取組み	ビジネス・レジリエンシー・マネジメントにおける優先順位は、以下の通りである: 従業員の保護 業務能力の回復 顧客や取引先の支援 コミュニティーの支援(多くの拠点で、コミュニティーとの協働プログラムを実施している) 株主利益の保護 独自に開発したレジリエンシー指標を用いて、部門ごとのレジリエンシーを数値化している。 指標に用いるのは、「①製品のレジリエンシー(全体の 30%に寄与)」、「②サプライヤーのレジリエンシー(全体の 20%に寄与)」、「③製造拠点のレジリエンシー(全体の 30%に寄与)」、「④試験機のレジリエンシー(全体の 20%に寄与)」の 4 つの要素から算出している。 レジリエンシー指標は、現状の評価と、改善策の特定のために使用している。このような定量的な指標を使用することで、他部門に改善依頼をすることが容易となっている。

3.2.6.2 英国における事業者の取組事例(大手電力事業者)[67]

英国大手電力事業者の BCP の取組について以下に示す。英国では、1990 年代後半に電力事業の自由化が行われて以来、電力供給サービス事業の競争が激化した。そこで本事業者は経営方針として、BCP の高度化によりサービスの信頼性を高め、他の事業者との差別化を図ろうとしている点が国内電力事業者との前提の違いとして挙げられる。しかしながら、過去の事故データから業務が一定時間停止した場合の被害金額を定量化することにより、BCP 対策のための予算を継続的に確保し BCP を高度化させている点、及び大学院で専門教育を受けた BCM マネージャーが第三者認証制度等の仕組みを効果的に活用し、取引先の BCP について実効性の確認を行っている点は、国内の重要インフラ事業者の BCP 高度化において参考になるものと考えられる。

表 29 英国大手電力事業者の BCP 取組事例

	英国大手電力事業者
体制	フルタイムで BCM 活動に携わる BCM 管理者が4名在籍。その活動の対象範囲には、セキュリティ管理、オペレーションリスク管理、など全てのビジネスの阻害要因となるリスクが含まれている。 さらにその下には、BCM 活動の実効責任を負う、計画管理者が配置されており、計画の推進や訓練実施の責任を負っている。 上記の体制は、5, 6 年前から取られており、品質監査の仕組みとも整合が取られている。 BCM マネージャーとして社外のコンサルタントを採用。当該 BCM マネージャーは過去に、Glasgow Caledonian University にて経営学を修了した際にリスクマネジメントを専攻し事業継続についての研究を行った。
過去の被災体験	数年前、確か日曜の朝だったと記憶しているが、大規模なブラックアウトが発生したことがある。その後の6週間は事業継続チームによるマネジメントへと切替えられた。当社の見積によれば、BCM 体制がなかった場合と比較して2300万ポンドの損失を回避することが出来た計算となる。 過去のリスク事象について、外部組織とデータの共有等は行っていない。自社内で発生事象と損失額に関する統計データを蓄積している。
取組みへの主な動機要因	1998 年頃に電力事業の自由化が行われ、施設の保有運用と供給サービスの事業が分離された。その後、電力供給サービス事業の競争が活発化している。 当社でも顧客対応力の強化のため緊急事態対応についての議論が行われるようになった。 自由化前には競争がなく危機管理の意識も低かったが、現在では電力サービスを提供する会社の対応に不満があれば、消費者はいつでも他の業者に乗り換えられるため、サービスの信頼性が最大の差別化要因となっている。
主なリスク	当社では危機管理から重大事故まであらゆるレベルのリスクを BCM の対象としている。 事業環境における主なリスクは下記、 パンデミック 大規模停電 海外の委託サービスの停止 統合予定のスペイン企業とのシステム統合 電力取引の停止(取引先の停止等) 情報システムの停止、データ消失 テロリズム

[67]東京海上日動リスクコンサルティング資料ほかより作成
http://www.meti.go.jp/meti_lib/report/2010fy01/E000900.pdf

	英国大手電力事業者
取引先への確認方法	取引先への確認はまずはアンケートを行い、その回答結果等を踏まえて詳細な調査を行う部分を決める。監査等も行う。 その後、計画文書、実施プロセス・エビデンス、ガバナンス体制、調達プロセスなどの確認を行う。また、サプライチェーンの確認状況に関するエビデンスも見る。 当社も取引先に対しては、BCM 実施の証拠となる文書の提示を求めている エビデンスがない場合は、打合せを行い正しく管理できているかを確認する。 取引先企業間の代替のきかないリソース、重要なリソースの関係性の分析を主に実施する。インドや南アフリカにも一部業務を委託しているが、現地での確認も行う。
取引先への要求内容	当社からの要求水準(RTO、RLO)は SLA の契約の中で明示されており、それを守れるか否かによって取引先を選定するにあたっての要素となる。 取引先が契約内容を守れずに当社に損失が発生した場合には、全ての損失を補償する義務がある。取引先への委託費用は多額であり、契約を守るための対策を行う義務がある。 例えば、取引先から提示された大災害発生時の RTO が 24 週間であった場合に、14 週間での復旧を目指して交渉する場合もある。 このような取引先への確認は、ユーティリティ関係の企業では一般的になりつつあるのではないか。
認証制度へのスタンス	BS25999 の仕組みにより取引先への確認は容易に行えるようになりつつある。BS25999 を活用した取引先の BCM 成熟度の向上も期待される。 BCM の要請を受ける立場で考えた場合、全ての取引先からの要請に個別に対応していたのでは負担が大きいため、BS 認証により自社のマネジメントシステムの有効性を証明できることは有益である。
その他特徴的な取組み	損失額の計算は、あるリスクが顕在化した場合に、最も発生する可能性の高いシナリオを想定し行う。そのうえで、軽減される被害額に見合うコストでの対策を検討する。被害額を計算する際の主なものは電力供給停止による収益の減少であるが、中には他社の事業停止により当社が負担する賠償金も含まれる。例えば、銀行の決済システムが停止した場合は、停止期間中の負債の金利負担なども発生する。 大きな収益を得ている優良顧客へのサービスを優先し対応を行うこととなる。 リスクマネジメントは下手に取組めばコスト要因になるだけであるが、上手に取組めば収益を上げることができる。戦略的なリスクマネジメントの中の1つの要素として BCM を捉えている。

3.2.6.3 Reserve Bank of New Zealand(ニュージーランド中央銀行)の取組事例

文書名	BCP Pandemic Plan (BCP パンデミック計画)[68]
体制	記載なし
主なリスク	パンデミック
記載内容	1.0 背景 1.1 政府の指令 1.2 パンデミックアウトブレイクシナリオ 1.3 基本的なサービスの提供 1.4 スタッフの健康 1.5 既存の BCP との統合 2.0 執行決定のマトリクス:パンデミックシナリオ 3.0 ステータス赤:クリティカルシステムと活動

[68] http://www.rbnz.govt.nz/crisismgmt/2198851.pdf

	3.1 機能を維持する要件 3.2 移行プロセス 　通貨 　建物サービス 　金融サービス 　コミュニケーション 　人事 3.3 プレポジショニング

3.2.6.4 Basingstoke & Deane(イギリスの地方自治体)の取組事例

文書名	Business Continuity Management Policy[69]
体制	シニアマネジメントチーム(SMT) BCP プロジェクト管理委員会 地域プロテクション長 サービス長 BCM コーディネーター
主なリスク	リスクの想定はないが、以下の事象を想定 ・オフィス施設が影響を受ける ・オフィス施設及び周辺地域が影響を受ける ・サポートリソースが影響を受ける
記載内容	1.0 はじめに 2.0 対象範囲と起動のシナリオ 3.0 政策声明 4.0 実施方針 5.0 役割と責任 6.0 回復のための戦略 7.0 コミュニケーションと啓発方針 8.0 トレーニングのテストとメンテナンス方針 9.0 レビュープロセス 10.0 監査とガバナンス

3.2.6.5 メリルリンチの取組事例

文書名	メリルリンチ社 Web ページより (Business Continuity Statement)[70]
体制	記述なし
主なリスク	具体的な明記なし (事業を中断させるイベント)
記載内容	・影響を受ける事業の移動について ・冗長構成について ・重要なビジネス機能を復旧するためのプロセスについて ・アクティブ化とリカバリのプロセスを管理するビジネスチーム及び技術チームについて

69
http://www.basingstoke.gov.uk/NR/rdonlyres/AF9AF9E7-CB74-4BFF-BD04-96E7953B8007/0/BDBCBCMPolicyapprovedversion11dated280109.pdf

70 http://www.ml.com/?id=7695_17469_14179

	・従業員の緊急時の連絡について ・定期的な手順のリハーサル、テストについて

3.3 演習に関する調査

3.3.1 国内の BCP 演習事例

日本において BCP の実効性を確認している演習の内容について、重要インフラ事業者へヒアリングを行い調査した。ヒアリング対象のすべての重要インフラ事業者において演習の詳細シナリオは非公開文書として位置づけられていたため、ヒアリングにて得られた BCP 演習の特徴について以下にまとめる。

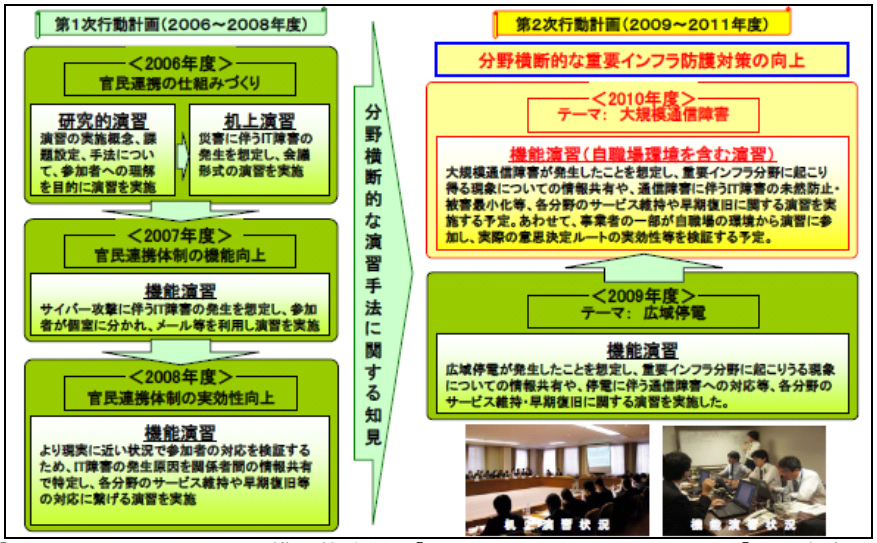
ヒアリング対象の重要インフラ事業者では、BCP 自体が災害を対象としているものが多い為、災害対応演習と併せて実施しているパターンがほとんどであった。その内容は、発生原因を決定してシナリオを作成し、正しく復旧できることを確認する、以下のような演習であることがほとんどであった。

・BCP は災害をリスクとして想定していた(他のリスクも災害 BCP で網羅していたパターンもあり)
・BCP の実効性を検証するための演習ではなく、ほとんどが災害対応訓練として実施していた
・情報システムについては別途障害対応の詳細手順書を持ち、障害対応訓練として実施していた

ヒアリングでは文書化された BCP 訓練シナリオを入手できなかったため、公開されている BCP 訓練事例を調査し、3.3.1.1～3.3.1.5 にまとめる。

3.3.1.1 NISC の取組

内閣官房情報セキュリティセンター(以下 NISC)では、重要インフラ事業者が参加する BCP の観点も含めた分野横断的演習を 2006 年以降 5 回開催した。その内容は研究的演習から始まり、机上演習、実機を使った機能演習と年々高度化され、参加者の対応力レベルの向上に応じた訓練が行われている(下図参照)。



資料:NISC「重要インフラにおける分野横断的演習～【CIIREX 2010(シーレックス2010)】～の実施について」[71]

図 20.NISC 分野横断的演習の目標と概要

以下に 2009 年度に実施された演習の実施概要及び成果・課題を示す。本演習では、重要イン

[71] http://www.nisc.go.jp/press/pdf/ciirex2010_press.pdf

フラ事業者における BCP 策定・改訂に向けた課題抽出が検証項目として掲げられ、その結果「共有リソース(アウトソース先ベンダや燃料供給等)の輻輳」及び「よりクリティカルな状況への対応力(期間や規模等)」が今後の課題として認識された。

表 30. NISC 2009 年度演習の実施概要

実施日	2009 年 11 月 27 日
対象リスク	広域停電
形式	実機を用いた機能演習
参加者	【重要インフラ事業者】:情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流の10分野 【セプター】:10分野の14セプター 【有識者】:慶応大学 大林教授(座長)他 【政府】:内閣官房情報セキュリティセンター、重要インフラ所管省庁
概要	我が国において広域的な停電が発生し、通信・水道のサービス提供の一部に影響が波及。その結果、各重要インフラ分野においては、IT 障害の未然防止・被害最小化のために対応を迫られた。

資料:NISC 資料より作成

1. 分野横断的演習を通じ、各重要インフラ事業者等において停電時の情報システムの稼動継続にかかわる BCP の策定・改訂に向けた気づきを得ることができた
2. 分野横断的演習に対しては、多数の参加者が必要性を感じており、今後も重要インフラ防護の視点からシナリオや手法に関して関係者との検討を重ねつつ、継続して実施する意義が再認識された
3. 過去3年間で構築されてきた官民の情報共有体制を通じて IT 障害発生時に円滑な情報共有がなされることが再確認できた

- 分野横断的演習の意義を増すためには、共有リソース(ベンダや燃料等)の輻輳を想定したシナリオも検討する必要がある
- BCP を始めとする重要インフラ防護対策の検証のためには、よりクリティカルな状況(期間や規模等)についても想定する必要がある

資料:NISC

図 21.NISC 2009 年度演習の成果・課題

3.3.1.2 金融業界の訓練実施動向

① 金融機関の具体的な取組事例

日本銀行から国内で営業活動を行う金融機関の BCP 訓練事例を集めたガイドラインが公表されている[72]。その中には、営業店や業務委託先、グループ関連会社等も含めた組織横断的な総合訓練を実施している事例も見られる。

72 「業務継続体制の実効性確保に向けた確認項目と具体的な取組事例 (増補改訂版、2010 年 3 月)」 http://www.boj.or.jp/research/brp/ron_2010/data/ron1003d.pdf

表 31.金融機関の具体的な取組事例

整備が必要な項目		具体的な取組事例
訓練計画	統括部署及び統括責任者が、自社の業務継続体制の整備状況を踏まえて、効果的な訓練計画を策定していること	• 業務継続計画の実効性確認や業務継続要因の習熟度向上の観点から、全社的な重点課題を定めたうえで、それに即した訓練計画を策定している • 訓練内容として、意思決定・連絡訓練、避難訓練、参集訓練、バックアップ機器立ち上げ訓練、バックアップセンター切替訓練、業務手作業訓練、日回し訓練（業務手順を通しで確認する訓練）等を、現実的なシナリオを用いて実施している • 訓練対象として、「重要業務」に関連する部署が網羅されている
	訓練の目的や業務継続要因の習熟度に応じた訓練内容のバリエーション	• 訓練内容が徐々に高度化するように、訓練内容や役割分担を変化させている • 訓練内容によっては、「抜打ち訓練」や「シナリオ・ブラインド訓練」等を有効活用している
訓練の実施	「重要業務」に関する訓練を行っていること	◎「重要業務」についての訓練を、その重要性に応じて頻度にメリハリをつけつつ行っている • 重要性の高い業務については、シナリオや訓練方法にバリエーションを持たせる工夫を講じつつ、計画的かつ定期的な訓練を実施している
	全社ベースでの総合訓練を行っていること	• 全社横断的な訓練を、定期的に（年1回以上等）実施している • 全社ベースの総合訓練に、業務継続に係る関係部署が広く参加している（営業店、委託先、グループ関連企業等） • 決済システム運営主体等との連携体制についても確認している • 決済システム運営主体の業務継続訓練には欠かさず参加することとしている
	訓練実施にあたり「重要業務」継続に必要な手順を実際に行っていること	具体的な取り組み事例の記載なし
	連絡体制の確認	◎緊急連絡先一覧を用いた安否確認、対策本部への情報集約的訓練を実施している • 緊急連絡手段の接続確認を定期的に（半年毎等）行っている
	対策本部立上げと業務継続計画発動の意思決定	• 対策本部のメンバーを招集の上、業務継続計画発動に係る重要判断（継続業務決定、バックアップオフィス立上げ、バックアップシステム切替）を含む意思決定の訓練を行っている • 代替要員による訓練も実施している
	バックアップオフィスへの参集・立上げ	• 業務継続要因が実際にバックアップオフィスに参集し、通信機器、端末、帳票類、マニュアル等を使用した訓練を、定期的に（年 2 回等）実施している
	オフサイト・バックアップシステムへの切替	• オフサイド・バックアップシステムへの切替に要する一連の作業（要員参集、システム立上げ、バックアップデータ読込、データ補正等）を、ユーザ部署も参加して「通し」で行っている • 可能な限り実機（本番系システム、それが難しい場合は、待機系システムや開発系システム）を利用した訓練を行っている

整備が必要な項目		具体的な取組事例
		• 切替訓練では、隔地保管しているバックアップデータの伝搬送・読込やそれを用いた稼働確認まで実施している • データ補正の訓練では、バックアップデータ取得後の取引やデータ伝送途中での被災等バックアップシステムに自動的に反映されない欠落データの特定・反映や手作業取引分の後追い入力・反映も含めている
訓練結果の分析・報告	訓練結果を分析して、業務継続計画のフィージビリティやマニュアルの有効性を確認していること	• 「重要業務」の復旧目標時間が達成できるかを検証している • 被災時には経営資源（機器能力、要員等）が制約される可能性も踏まえつつ、訓練を実施し、「実際に復旧に要する時間」を測定している • 訓練の結果、復旧目標時間を達成できないことが判明した部分については、その阻害要因を分析している • バックアップオフィスやバックアップセンター等に設置してある設備・機器類の十分性についても検証している • マニュアルについて、記述されているとおりの作業手順により業務継続が実行できることを検証している
	訓練結果及びその分析結果を経営陣に報告していること	• 全社ベース訓練を実施する都度、統括部署が結果を検証・分析のうえ、役員会等に報告している • 統括部署は、部署毎の訓練実施状況や訓練結果の概要についても、把握している • 役員会等において業務継続計画の有効性評価に係る議論が行われ、改善に向けた意思決定が経営レベルで行われている
業務継続計画の見直し	訓練結果及びその分析結果を、業務継続計画やマニュアルの見直しに結び付けていること	• 訓練結果及びその分析結果に基づき、業務継続計画やマニュアルを見直している（PDCA の実施）注） 注）業務継続体制整備の PDCA とは、以下のようなサイクルの継続的実施を指す Plan　：業務継続に関する基本方針や体制整備計画の策定 Do　：業務継続計画の策定及び訓練による習熟 Check:体制整備状況の点検や訓練結果等による実効性の検証 Action：点検・検証の結果等に基づく体制・計画の見直し • 復旧目標時間の達成が難しい場合、バックアップシステムやバックアップ方法の見直し・検討に結びつける体制としている

◎：とりわけ多くの金融機関において取り組まれている基本的な事例
資料：日本銀行「業務継続体制の実効性確保に向けた確認項目と具体的な取組事例」より作成

② 日本銀行のステージワイド訓練

新型インフルエンザ対策の必要性認識の高まりを受けて、2009 年 2 月に日本銀行が主催したステージワイド訓練の概要を以下に示す。本訓練では、BCP 有識者であるモデレータの進行のもと、国内における新型インフルエンザの発生シナリオが紹介され、各銀行の BCP 担当者及び銀行業務のアウトソーサーである現金輸送業者を含めて、各社の対応における課題について議論がなされた。

表 32.日本銀行ステージワイド訓練の実施概要

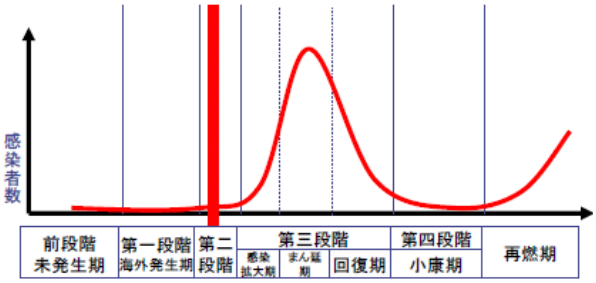
主催	日本銀行
実施日	2009 年 2 月
テーマ	新型インフルエンザ発生時の対応
形式	モデレータと 6 名のパネリスト(都銀、信託銀行、地銀、現金輸送業者、日銀)による公開討論
オブザーブ企業	全国の金融機関から約 540 名が参加

20××年 11 月 27 日	B 氏(成田在住)の検体から H5N1 が確認。B 氏の濃厚接触者の健康監視開始。都道府県より各指定医療機関へ発熱外来の設置要請。※第二段階:国内発見早期
20××年 12 月 3 日	×国周辺をはじめ感染者は、13 カ国に拡大。発生国を中心に物流や経済活動の停滞が顕在化。世界的な物流不足、物価上昇が懸念される。※WHO Level6 宣言

【世の中】
・学校閉鎖にともない欠勤する従事者が増加、事務所での健康管理が強化される
・インターネット・電話の使用が増える

【政府など】
・千葉県をはじめ、関東首都圏の学校閉鎖開始
・各保健所で発熱相談センターが開設

【金融】
・現金を引き出す市民が一段と増加(ATM 利用も一段と増加)



資料:日本銀行「ステージワイド訓練　新型インフルエンザ発生シナリオ」より

図 22.日本銀行ステージワイド訓練のシナリオ例[73](一部抜粋)

3.3.1.3　静岡県の取組:緊急防災支援室(スペクト)

静岡県では、県、市及び民間の重要インフラ事業者(通信、鉄道、電気、ガス等)から幅広く要員を集め、平成 8 年に緊急防災支援室(スペクト)を立ち上げた。本組織において平時から、対策マニュアルの整備や図上訓練が行われている。本事例は地域における重要インフラ事業者の業種横断的な取組として先進的な活動事例である。

[73] http://www.boj.or.jp/announcements/release_2009/data/fsc0902a7.pdf

表 33.静岡県緊急防災支援室の体制[74]

所属	職種	派遣元	派遣人数		
県	行政(事務、土木、建築、無線)		9	14	27
	医療(看護師)		1		
	教育(小学校教員)		1		
	警察(警察官)		3		
市	行政	下田市、三島市、富士市、島田市、静岡市	5	6	
	消防	浜松市	1		
民間	電話	NTT 西日本	1	7	
	鉄道	JR 東海	1		
	電気	中部電力、東京電力	2		
	都市ガス	静岡ガス、中部ガス	2		
	プロパンガス	県プロパンガス協会(鈴与商事)	1		

3.3.1.4 岡山市水道局の取組

岡山市は、東南海、南海地震防災対策推進地域に指定されているという背景があり、岡山市水道局では対災害訓練を実施している。また、岡山県地域防災計画、岡山市地域防災計画等に基づき、岡山県主催の合同訓練にも参加している。

以下に訓練概要を記す。以下の訓練は定期的に実施されているものが主だが、参集訓練(交通機関が使えないことを想定し、自宅近くの拠点に出勤し、対応する訓練)は抜き打ちで不定期に実施している。

・訓練の種類[75]…防災訓練、参集訓練　等
・主催…岡山市水道局、岡山県防災会議、日本水道協会岡山県支部　等
・シナリオ…地震や津波を想定し、地域やその他事業者と連携して以下の様な訓練を実施。
　　-水道の他、電力、通信、ガス等の事業者と連携しライフラインの応急復旧訓練
　　-応急給水、配水管復旧訓練
　　-応援隊の派遣・受入訓練
　　-宿泊訓練　　等

訓練を通じて確認された課題に対しては、対処を実施している。

課題 1:給水や止水等の技術を要する訓練の際には、その担当技術者が対応していたが、災害で技術者の派遣が難しい状況に陥ることも考えられる。
対処　:平成 21 年より、事務担当者も止水等の復旧訓練に参加している。

課題 2:実際の災害時の混乱を経験したことのある、経験者の不足。
対処　:岡山市水道局の退職者が有する水道に関する知識、技能及び経験を生かし、水道局の行う被害情報の収集及び応急給水活動を支援するボランティア団体として、「岡山市水道局退職者災害時支援協力隊」を平成 20 年に発足。上記訓練にも参加している。

情報システムの安定運用の観点での訓練情報は公開されていないが、岡山県インターネットセキュリティ対策連絡協議会[76]の賛助会員であることから、情報システムの安定運用に必要なセキュリティ対策情報を収集し、活用していると考えられる。

74 http://www.bousai.go.jp/oshirase/h15/0902nagoya/sizuoka.pdf
75 http://www.water.okayama.okayama.jp/guest/bousai3.htm
76 http://www.oisec.jp/top.htm

3.3.1.5　東京証券取引所の取組

東京証券取引所では、BCP を、東京証券取引所爆破テロ予告を機に見直しを実施。全 15 部門すべての BCP が 2004 年 6 月に完成した。2004 年 10 月に訓練を実施した。

演習の種類	災害訓練
主催	東京証券取引所
シナリオ	全館避難命令が発令され、A ランクの業務を代替オフィスで継続する
演習を通じて確認された課題	「代替オフィスでは携帯電話を使って各部門と連絡を取り合う手はずが、電波状態が悪いところがあり、連絡ができなかった」等、BCP の不備を約 70 項目が発覚。
対処	訓練後半年をかけて BCP を見直し、以下の対策を追加した。 ・携帯電話の代わりの連絡手段として、構内 PHS を整備。 ・代替オフィスを約 1 年間で 3 倍の規模（収容員数を 30 人から100人へ。常時するパソコンを 5 台から 50 台へ）にする計画を立てた。 ・代替オフィスでは、取引業務の継続を中心としていたが、マスコミを通じた広報業務等も代替オフィスで継続できるようにする計画を立てた。

3.3.2 海外の BCP 演習訓練事例

海外では、ストリートワイド訓練と呼ばれる同一業種内での企業横断的な訓練が、金融業界を中心に実施されている。また、地域横断という観点では、英国において地域レジリエンス・フォーラムと呼ばれる業種横断的な活動がなされている。本節ではこれらの 2 つの活動についてまとめる。

3.3.2.1　金融業界のストリートワイド訓練[77]

海外とりわけ英国、米国、シンガポール等においては、ストリートワイド訓練と呼ばれる企業横断的な訓練が行われている。このような訓練の有効性として、他社の業務継続計画との相互依存関係を踏まえ、以下のような項目が確認できる点が挙げられる。

・自社計画と被災時の社会状況との整合性
・自社計画と関係先の業務継続計画との整合性
・業界内の連絡体制構築

なお、金融業界の特徴として、一部の金融機関において被災時の対応が遅れ決済処理が滞ることにより、業界全体の決済機能が麻痺する可能性があり、他の業種に比べてこのような業界を挙げての取組が進んでいる。

表 34.海外におけるストリートワイド訓練の実施事例

	時期	被災想定	期間	参加社数	準備期間	実施主体
英国	03 年秋	テロ	半日	16 社	4 ヶ月	民間金融機関 関係当局 （金融ｻｰﾋﾞｽ機構）
	04 年秋	テロ	半日	32 社	5 ヶ月	関係当局 （金融ｻｰﾋﾞｽ機構、財務省、英国中銀）
	05 年秋	テロ	半日	約 70 社	6 ヶ月	
	06 年秋	新型ｲﾝﾌﾙｴﾝｻﾞ	6 週間	約 70 社	6 ヶ月	
	09 年秋	暴風雨（洪水）	半日を 2 回	76 社	6 ヶ月	

77日本銀行「海外における「ストリートワイド訓練」の概要 ―業務継続計画の実効性確認手段としての業界横断的訓練―」などを基に記載
http://www.boj.or.jp/research/brp/ron_2010/data/ron1003c.pdf

	時期	被災想定	期間	参加社数	準備期間	実施主体
ｼﾝｶﾞﾎﾟｰﾙ	05 年春	テロ	半日	12 社	1 ヶ月	銀行協会 関係当局 (ｼﾝｶﾞﾎﾟｰﾙ通貨庁等)
	06 年春	テロ	半日	約 100 社	6 ヶ月	
	08 年秋	新型ｲﾝﾌﾙｴﾝｻﾞ	2 週間	約 140 社	9 ヶ月	
米国	07 年秋	新型ｲﾝﾌﾙｴﾝｻﾞ	3 週間	2,775 社	4 ヶ月半	各種業界団体 関係当局 (財務省、通貨監督局、米国証券取引委員会、連邦準備制度理事会等)
	09 年秋	サイバーテロ	5 日間	48 社	6 ヶ月	
豪州	08 年春	新型ｲﾝﾌﾙｴﾝｻﾞ	5 週間	33 社	12 ヶ月	業界有識者会議
仏	08 年秋	テロ(停電)	半日	15 社	6 ヶ月	市場振興団体 関係当局(フランス中級)
蘭	09 年夏	サイバーテロ	1 日	16 社	6 ヶ月	関係当局(オランダ中級)

資料:日本銀行

以下に各国のストリートワイド訓練への非金融事業者の関与有無をまとめた資料を示す。電気、ガス、水道、鉄道、通信等のインフラ事業者に加えて、業務の外部委託先である現金輸送業、ATM 管理業者等も訓練に関与していることが分かる。

表 35.シナリオ策定に協力した非金融セクター(外部主体への依存部分)

国名	実施内容	電力	ガス	水道	鉄道	航空	データ通信	電話	携帯電話	警察	消防	現金輸送	ATM管理	その他
英	03 年テロ	○	×	×	○	×	×	○	×	○	×	×	×	地方自治体
	04 年テロ	○	○	○	○	×	×	○	×	○	×	×	×	地方自治体
	05 年テロ	○	○	○	○	×	×	○	○	○	○	○	×	地方自治体
	06 年ｲﾝﾌﾙ	○	×	×	○	×	×	○	○	○	×	○	×	地方自治体 バックアップ施設業者
	09 年暴風雨	○	×	○	○	○	○	○	○	○	○	○	○	地方自治体 バックアップ施設業者
ｼﾝｶﾞﾎﾟｰﾙ	05 年テロ	×	×	×	×	×	×	×	×	△	△	×	×	通信開発庁
	06 年テロ	×	×	×	△	×	×	×	×	○	○	○	○	バックアップ施設業者
	08 年ｲﾝﾌﾙ	○	○	○	○	○	○	○	○	○	○	○	○	
米	07 年ｲﾝﾌﾙ	○	○	×	×	○	○	○	○	×	×	○	○	医療
	09 年ｻｲﾊﾞｰ	×	×	×	×	×	×	×	×	×	×	×	×	政府機関(FBI、CIA等)
豪	08 年ｲﾝﾌﾙ	○	○	○	○	×	○	○	○	○	○	○	×	
仏	08 年テロ	○	○	○	○	×	○	○	○	○	○	○	×	

国名	実施内容	電力	ガス	水道	鉄道	航空	データ通信	電話	携帯電話	警察	消防	現金輸送	ATM管理	その他
蘭	09年ｻｲﾊﾞｰ	×	×	×	×	×	○	×	×	×	×	×	×	政府機関(ﾊｲﾃｸ犯罪等)

注:△印は、シナリオ策定に関与しないが、訓練当日に参加
資料:日本銀行

また、米国、英国における訓練の被災シナリオの例を、次に示す。

表 36.米国 2007 年訓練の被災シナリオ(新型インフルエンザ)

訓練期間(想定期間)		1週目(9/24-10/7)	2週目(10/8-11/4)	3週目(11/5-12/3)
感染拡大状況		米防災センター(CDC)が世界的流行発生を宣言	米国における感染拡大のピーク	米国における感染拡大が収束
	WHOフェーズ	フェーズ6	フェーズ6	フェーズ6
	米国基準	ステージ5	ステージ5	ステージ6
欠勤率	全米	25%	49%	35%
	ラ米、東欧等	15%	30%	45%
	欧州、中東等	25%	高水準	20%
	アジア、豪州等	10%	25%	40%
医療		集中治療室(ICU)の95%が満室	医療機関不足、診察待ち患者が増加	医療機関不足、診療待ち患者は減少
小売		生活必需品供給15%減、配達遅延	生活必需品供給50%減、配達期間2週間	生活必需品供給は依然として低水準
金融	市場	米経済原則 米株5%下落 米債利回り25bps定価 商品価格10%下落	米実質GDP3/4%減 米株12.5%下落 米債利回り50bps低下 商品価格20%下落 流動性30%低下	米実質GDP1.5%減 米株5%上昇 取引量・流動性回復
	事務	ｵﾝﾗｲﾝｻｰﾋﾞｽ35%増 ｺｰﾙｾﾝﾀｰ事務20%増 ATM引出し15%増 ATM稼働率85%	銀行支店50%閉鎖 ｵﾝﾗｲﾝｻｰﾋﾞｽ60%増 ｺｰﾙｾﾝﾀｰ待ち時間倍増 ATM稼働率60%	市場データ15分遅延 消費者ローン支払20%増 ATM稼働率70%
学校		80～90%閉鎖	前項閉鎖	2～3週間後に再開
公益事業		通常時の80%操業	毎日2時間停電	電力供給安定
電話/インターネット		新規サービス開始や修繕に対する対応50%減	一般家庭用インターネット回線50%減	インターネット回線50%減
郵便		通常日2日遅延	通常比7-10日遅延	通常比3-5日遅延
交通機関		陸・空の運輸40%減	交通機関50%停止	徐々に増便
燃料		供給減、価格上昇	ガソリン供給10%減 自家発燃料供給20%減	徐々に供給回復
施設		清掃遅延	清掃ほぼ停止	―
社会活動		多くのイベント中止・延期 犯罪発生率上昇	殆どのイベント中止・延期 夜間外出禁止令	殆どのイベント中止・延期 夜間外出禁止令継続

資料:日本銀行

表 37.英国 2009 年訓練の被災シナリオ（暴風雨）

	訓練 1 日目	訓練 2 日目
天候	長雨続きに暴風雨が縦断し、建物や樹木が損壊（風速 30m、時間雨量 40 ㎜、局地的に激しい集中豪雨）	暴風雨は勢力が弱まり、徐々に沈静化
交通機関	バス、鉄道、地下鉄、フェリー等、大半の交通機関が停止	復旧作業は行われているが、なお 30％の交通機関が停止
電力、水道等	多くの地域で供給停止	供給停止が続く地域が多い
情報通信	電話、データ通信とも不通。 市況情報伝達手段も停止	一部地域での不通が続く
決済インフラ	SWIFT（電信手段）、RTGS（大口決済）に障害発生	特に支障なし
欠勤率	交通途絶に加え、自宅浸水等もあって、欠勤多発 ・自宅住所の郵便番号と本人氏名の冒頭アルファベット等により、欠勤者を指定（地域により欠勤率 25～70％）	
本部機能	運河に囲まれた金融集積地区 Canary Wharf への立ち入り制限、バックアップ施設への切替多発	バックアップ施設で業務を続ける先が多い
営業店舗	多くの店舗が閉鎖	営業再開できない店舗が少なくない
社会情勢	営業再開できない銀行に対し、流動性危機との噂が流れ、コールセンターへの問い合わせが殺到	
外部関連業者	バックアップ施設提供業者も含め、サービス水準が低下	

資料：日本銀行

3.3.2.2 英国地域レジリエンス・フォーラム[78]

英国では2004年民間緊急事態法において、緊急対応組織（消防署等）や地方自治体は「第一レベル対応者（※第一レベル対応者には、地方自治体、警察、消防隊、救急隊、医療機関、内相等であり、緊急事態に直接対応する義務を負う）」として定義され、具体的には以下の項目が義務付けられている。

- ・緊急事態対応業務の実施及び、重要な通常業務の継続実施を目的とした計画及び手順書を策定し、毎年見直すこと。
- ・上記計画にのっとった訓練を実施すること。
- ・対応業務に係わるサプライチェーン継続対策を実施すること。
- ・管轄地域で発生が予想される災害や事件を想定し、その発生確率と想定被害をまとめたリスク登録簿（中央政府の場合は全国のリスクを対象とし、地方自治体は管轄地域のリスクを対象とする）を作成し、適切なリスク管理を実施すること[79]。
- ・市民保護に関する情報を周知すること。
- ・緊急事態対応者間での情報交換を実施すること。

また地方自治体には、上記に加えて以下の対応を取ることが義務付けられた。

- ・管轄地域の緊急事態対応者の役割と責任を明確に定めること。

78 東京海上日動リスクコンサルティング資料等より

79 全国リスク登録簿
http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx

・管轄地域の企業や非営利組織に対して、事業継続マネジメントに関するアドバイスや補助を実施すること。
・コミュニティー全体に対して、事業継続マネジメントの普及活動を行うこと。
・必要に応じて、個別組織のリスク評価、計画策定、訓練等について支援すること。支援については有償で実施してもよい。

また、2004年民間緊急事態法では、ライフラインや社会インフラを支える事業者等は「第二レベル対応者（※第二レベル対応者には、水道、ガス、電気、通信等にかかわる公益事業者や、鉄道、航空、港湾の運輸関係者等が含まれている）」として定義されている。第二レベル対応者は緊急事態において第一レベル対応者を補助する責務を追っており、法的な義務として「緊急事態対応者間の協力及び情報交換の実施」が課せられている。

このような状況下で、各地方自治体（都道府県、市町村レベル）では、「地方レジリエンス・フォーラム（LRF: Local Resilience Forum）」を定期的に開催し、地域の市民団体や事業者と、緊急事態対応に関する情報交換を実施している。また、ほぼ全ての広域自治体（※日本の都道府県にあたり総計119の自治体数となる）が「（地名）レジリエンス」又は「（地名）緊急対応計画」との名称のウェブサイトを運営している。これらのウェブサイトの典型的な内容は、以下の通りである。

・緊急対応計画とは
・現在のリスク状況（新型インフルエンザの解説等）
・緊急対応計画の作り方
・事業継続計画の作り方
・××地方のリスク（リスク登録）
・緊急連絡先
・緊急時訓練、教育、セミナーのお知らせ
・児童向け学習ページ
・緊急対応の関連組織

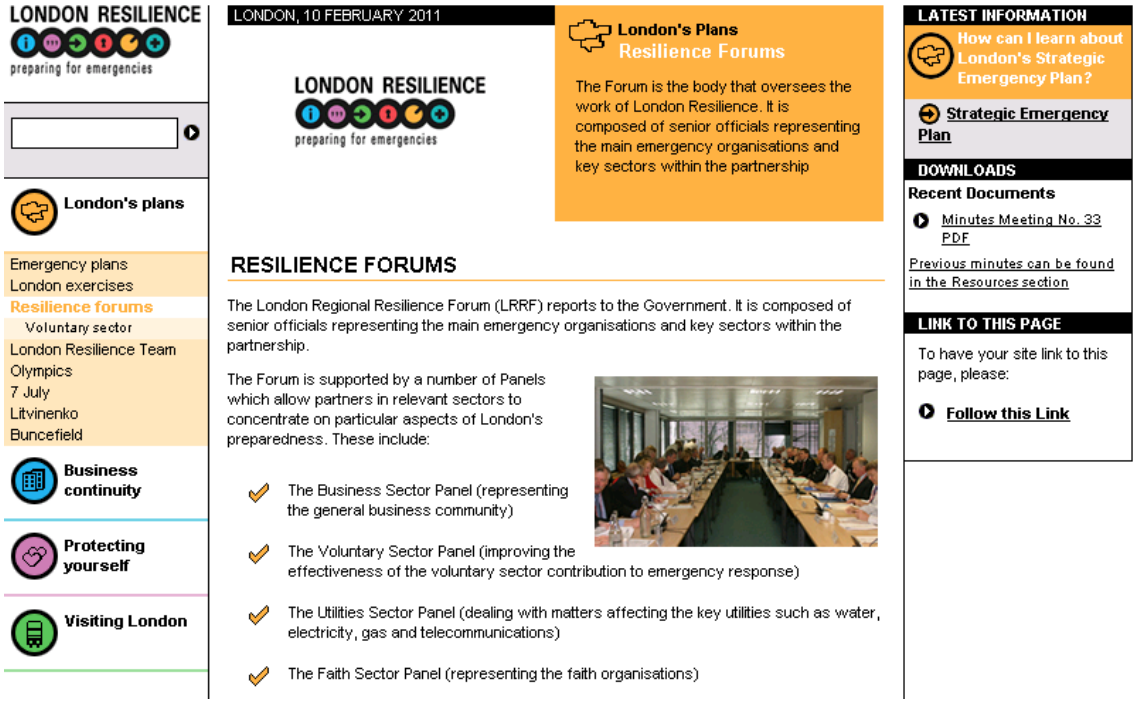


図 23.ロンドン地域レジリエンス・フォーラムの Web サイト（参考）

3.4 BCP に関する課題の抽出・提言

3.4.1 BCP に関する調査の整理・分析

3.4.1.1 BCP ガイドライン等に関する整理・分析

3.1 と 3.2 で調査した、国内外の BCP で求められている要件等及び実際に策定・運用されている国内外の BCP についての要点を以下(1)～(3)に整理して示す

(1)海外ガイドラインと国内ガイドラインとの比較

3.2.5.2 より、BCP のガイドライン等において求められている推進体制、備えるべき要件について、我が国と海外で比較したところ、大項目レベルでは大きな差異は見られなかったが、システムに求められている要件の詳細記述においては、備えるべき要件について、日本のガイドライン等にはない記述が海外のガイドライン等で見られた。

3.2.5.2(1)より、英国では、「BCP の検討の中で ICT 継続の検討も考慮すること」という要件が記されている。また「事業継続のための ICT の要件を理解する必要がある」と記されており、BCP における情報システムの関与が明示されている。

3.2.5.2(2)より、米国では、BCP 策定の過程で行うリスクアセスメント等の際にシステムの維持に係る内容として、データ及び通信の完全性並びにサイバーセキュリティを考慮するようにと、より具体的に技術的な考慮すべき点が例示されていた。

3.2.5.2(3)より、シンガポールでは、重要な機能や重要なビジネス機能をサポートするために必要となる情報システムを特定しなければならないと記しており、英国同様に情報システムの事業継続への関与を明示している。

3.2.5.2(4)より、国際規格 ISO/IEC 27031(事業継続性のための情報通信技術準備ガイドライン)では、重要な ICT サービスを理解するべきであり、さらに事業の継続のために必要な ICT 要件と、既存で備えている ICT 継続の要件にはギャップが生じることを認識し、それらを考慮した事業継続計画の策定が必要だと記されている。

(2)BCP で想定するリスク

3.1.3 より、日本では、地震や台風等の自然災害が多発しているという背景から、BCP 策定のスタート時の想定リスクは、自然災害、中でも地震とすることを推奨しているガイドラインが多く、IT サービスを継続するための BCP ガイドラインにおいてもその想定リスクは自然災害としている。そして、段階的に想定を広げていくよう記されている。

3.1.5 より、前述の災害を想定した BCP に加え、近年の新型インフルエンザパンデミックを受け、これまでの災害版 BCP に加え、新型インフルエンザをリスクとして想定した BCP を追加策定したという状況であった。

災害を対象リスクとしている BCP は、被害を受けた業務を早期に再開することを目的とした業務復旧型、新型インフルエンザパンデミックを対象リスクとしている BCP は、必要最低限の業務に絞り込み、その継続を目的とした業務縮退型と言え、この双方のパターンを持ち合わせることで、より柔軟で効果的な事業継続の対応ができると考えられる。例えば、大規模な災害や障害を対象リスクとする BCP についても、業務縮退型の対応が有効である場合があることから、新型インフルエンザパンデミックの BCP を参考として、段階的に業務縮退型の対応を取り込んでいくことが考えられる。

また、3.1.5 より日本においては、 災害版 BCP が想定している以外の IT 障害等の技術的リスクについては、BCP とは別の IT 緊急時対応マニュアルとして備えている場合や、他のリスクを想定した BCP で技術的リスクもカバーできるとしていた重要インフラ事業者もあった。

なお、英国においては、サイバー攻撃が最も著しい脅威として認識されており、続いて疾病、インフルエンザパンデミック、異常気象となっている(3.2.1.2 図 18)。

米国においては、過去1年間に使用した復旧手順書はほとんどが情報システム関連の障害からの復旧手順書であり、米国における BCP とは地震のような大規模災害を前提としたものだけではなく、情報システムの障害のような比較的対応が容易なリスク事象も、BCP の対象として捉えている(3.2.2.2 表 22)。

(3)BCP と情報セキュリティの関係性

3.1.4.2 で示したように、BCP の策定において、IT サービス継続を優先するために必要となる情報セキュリティ水準の低下について検討することの必要性がガイドラインにより示されている。これに関して、情報処理推進機構が公開している文書では次のように記されている。

<<情報セキュリティ事業継続計画(BCP)とは>>[80]。

企業における情報技術(IT)の本格的な活用が進み、事業基盤としての情報システムの重要性や企業が保有する情報資産の価値は増大していますが、その一方で、それらに関連するトラブルが増え、企業の継続的な事業・サービス提供を脅かすリスクも増大しています。(途中略)
我が国では、防災対策を中心とする危機管理には長い歴史があります。一方、情報セキュリティ分野の事業継続の取組みは、防災ほどの歴史はありませんが、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、進化しています。情報セキュリティの観点から、事業継続計画を考える、または IT 緊急時対応計画を検討する場合には、既存の BCP 関連計画の有無を確認した上で、各部署と連携を取りながら、全社的に整合性のある BCP を策定する必要があります。

図2緊急時対応に関する諸計画の相互関係図

<<NIST SP800 シリーズに見る情報セキュリティと事業継続計画>>[81]

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

80 http://www.ipa.go.jp/security/manager/protect/bcp/index.html
81 http://www.ipa.go.jp/security/publications/nist/documents/2006BCP.pdf

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。

3.4.1.2 BCP 演習に関する整理・分析

3.3 で調査した、国内外の BCP の実効性を目的として行われている演習事例について要点を示す。

我が国での BCP 演習は、BCP 自体が災害を対象としているものが多い為、災害対応訓練と併せて実施しているパターンが見受けられた。その内容は、発生原因を決定してシナリオを作成し、シナリオ通りに正しく復旧できることを確認する訓練であることがほとんどであった。また、情報システムについては別途障害対応の詳細手順書を持ち、障害対応訓練として実施していた。

備えるべき BCP 及び BCP 訓練の内容としては問題がなさそうに見えるが、サイバーテロ予告といった、実際に情報システムが停止しないような事象が発生した場合に BCP が発動できるのかというところに懸念が残る。

3.4.2 BCP に関する課題の抽出・提言

3.4.2.1 重要インフラの BCP の在り方に関するポイント

BCP に関する課題の抽出、及び提言をまとめるにあたり、3.1～3.3 の調査結果、3.4.1 の整理・分結果から、重要インフラのBCPの在り方に関するポイントを以下に整理する。なお、表 1に示す有識者へヒアリングを実施し、いただいたご意見を取り込んだ。

(1)BCP の普及について

- 日本における BCP の普及率は高まりつつあるが、分野や規模に分類するとその格差が見える。その差については、監督官庁からの BCP 策定の指示が出ているか否か、又は重要システムの停止が重要インフラサービスに与える影響の度合いが関係しているものと考えられる。

(2) 地域別 BCP レベルの指針(メジャー)の必要性について

- 事業者が個々に BCP を策定するのでは、事業継続のレベルは経営の判断となってしまうため、国民の生活を守ることを目的とした BCP ではなくなってしまう可能性がある。事業者は、利用者からみた許容影響期間、許容影響範囲を設定・明示する必要がある。(すでに、「中央省庁業務継続ガイドライン」においては、一部の重要インフラの施設被害について、復旧する目標日数が定められいる(電力:6 日、上水道:55 日、ガス:55 日、通信:14 日)が、他の重要インフラについては、水準が明示されていない。また、実効的な BCP とするために必要な演習のレベルについても明示されたものがない。)
- 都道府県レベルで許容影響期間、許容影響範囲を示し、続いて地域や事業者はその指し示している方向に合わせる形で検討していくとBCPの策定が行いやすいのではないか(都道府県が明示することで、地域、事業者は復旧時間の目安等が立てやすくなり、事業者でのBCP 策定も進めやすくなるのではないか)。
- 県もしくは、外郭団体等が主導となり、地域のレベルに見合った BCP を策定し、演習を行うという運用が重要なのではないか。
- 上記を行うにあたり、国として、利用者からみた場合に分野横断的に何を維持すべきなのか、具体的な指針を提示することが重要なのではないか。

(3)リスク分析・業務重要度分析について

- 食品偽装や口蹄疫等の事故や障害も事業の継続が絶たれる要因であることを認識することが重要である(特定県(特定品、日本で一番の生産高である品)では、影響が大きいはずである)。

・BCP の第一歩は、停止してよいものを把握することである。
・安否が確認できれば、それに伴い人員配置、復旧計画が立てられるはずである。安否確認は重要である。
・パニックに陥らないためにも、鉄道が動かなくても他の手段で物流が機能すればよく、正確な情報を得るために通信や放送は重要であると考えられる。
・国は何を維持するべきなのかのメジャーを示すべきである。たとえば安否情報等、人命に係わらないが迅速に提供することで安心感を与えられる等の時系列的に待てないものがあるはずである。
・「重要システム」について、重要インフラ分野毎に第 2 次行動計画（別紙 1）で示されているが、実態は「重要システム」と BCP で重要業務の継続に不可欠なシステムとは必ずしもすべてが一致していないのではないか。

(4) 個別対策について
・拠点が海外にわたる事業者においては、エリア（国別）の BCP を検討する必要がある可能性がある。

(5) 非常時における規則の緩和について
・日本における BCP は、機密性を重んじており、可用性を抑えている傾向がある。その為、状況に応じて機密性や可用性の重きを可変させるといった対応が出来ない、つまりBCPが使いこなせない可能性がある。また、日本では、情報セキュリティの運用においても、機密性・完全性・可用性の、状況に応じた可変的な扱い（臨機応変な対応）に慣れていない。（例えば、個人情報保護法が制定され、機密性を重んじるばかりに、いざという時に、必要な個人情報が開示出来なかった 等）

(6) 演習について
・米国政府ではBCPを実効性あるものにするために、重要インフラ事業者に対して演習を求め、その演習結果を評価しアドバイザリを発行している。
・BCP を策定済みの事業者は、策定の過程で演習を実施しているはずだが、その演習で事業継続上重要な項目を確認しているのかということについては課題が残っていると考えられる。
・日本における BCP の演習は、対応可能なシナリオを設定してしまい、問題点が発見されにくい方法をとっている事業者が多いのではないか。
・日本における BCP の演習は、発生事象ではなく、発生原因を意識したものが多く、問題なく対応できることを確認するための演習内容になっているため、BCP の問題点を洗い出すことができていない可能性がある。
・上記（2）に示した地域の単位で分野横断的な BCP 演習を実施するのが望ましい。分野によってはすでに横断的に実施しているところもあるが、事案発生時の許容される復旧時間は、国ごとに異なるように、都道府県ごと、市区町村ごと等地域で事業者の特性や住民の特性が異なるため、備えるべき BCP のレベルも変わってくると考えられる。（3.1.5.3 で示した愛知県の取組は、まさに愛知県の地域の特性を考慮した具体的な BCP モデルを事業者に対して指し示している。愛知県では東海地震・東南海地震の発生が懸念される地域であるため、その想定リスクを地震に絞って例示している。BCP 策定時に戸惑いやすい、復旧目標の設定やサプライチェーン間の連携方法については実際の愛知県内の事業者 BCP 事例をもとに例示されている。）

3.4.2.2 実効性のある BCP とするための提言

今回の BCP 調査より、内閣府策定の BCP を NISC として情報セキュリティの観点を踏まえ、より実効性のある BCP にするためには、次の項目の実施が必要だと考える。

（1）BCP ガイドライン内容の拡充
・3.2.5.2（2）の米国のガイドラインにて、考慮すべきリスクが具体的に例示されていた（データ及

び通信の完全性並びにサイバーセキュリティを考慮する）ように、システムを維持するのに考慮すべきリスクを、我が国のガイドライン等においても具体的に例示することが必要である。
・複数のリスクをカバーする BCP を策定するのであれば、その想定しているリスクに全て対応できるか、検討及び演習を行うべきである旨を指し示すことが必要である。
・IT システムの緊急時の対応も BCP に関連付ける必要があること、そして 3.1.4.2 で示した「緊急時におけるセキュリティ水準の低下」（IT サービス継続ガイドライン）についても BCP 検討の際に盛り込む必要があることを、強調することが必要である。

我が国の重要インフラの BCP に盛り込むべき項目（例）を表 38 に列挙する。なお、表 38 に記載した事項は一例であり、組織に応じた内容を検討する必要がある。

表 38 BCP に盛り込むべき項目（例）

BCP に盛り込むべき項目（例）		備考
想定リスク		・地震、火災、洪水、津波、テロ、情報システム障害、サイバーテロ、パンデミック、資源不足、交通機関不通等があげられる。 ・複数のリスクをカバーする場合にはその旨も明記するとよい。
適用範囲		BCP を適用する組織、建屋、人員、システム等があげられる。
重要業務・重要システムの特定		ビジネスインパクト分析、ビジネスリスク分析等により、早期に復旧させる、または縮退時も稼働させる業務やシステムの特定等があげられる。
対応内容		BCP 発動基準、重要業務の目標復旧時間、復旧順位・縮退順位、人員の確保、通信手段の確保、代替手段、二次被害防止策、業務時間外の場合の対応等があげられる。
組織内での連携		権限委譲・代行順位、広報体制、連絡体制、安否確認方法等があげられる。
組織外との連携		近隣の都道府県・市町村、国民、利害関係者、サプライチェーン等との情報収集・伝達体制、協力体制等があげられる。
例外措置		緊急時におけるセキュリティ水準の低下等への考え方を明示する等があげられる。
BCP の解除		BCP 解除の判断基準、解除の連絡方法等があげられる。
通常時からの備え		
	推進体制	経営陣の役割・責務、BCP 責任者・BCP 推進組織（組織全体にかかる横断的組織）の役割・責務、BCP 発動時の体制等があげられる。
	演習	演習の実施頻度、実施体制（組織単体・関連組織との連携）、演習からのフィードバック等があげられる。なお、事業の継続を意識した、BCP 演習の内容とするとよい。
	BCP の点検・見直し	点検・見直し方法、点検・見直し頻度等があげられる。見直しでは、BCP の想定リスクの再検討等も内容に入れるとよい。

BCP に盛り込むべき項目（例）		備考
	サプライチェーンへの BCP の要求	自組織の事業継続に必要なサプライチェーンにも BCP の作成を依頼する等があげられる。

(2) 分野毎のガイドラインの作成

・金融事業者では先進的な取り組み事例をまとめていたように（3.1.2.1 参照）、重要インフラ分野毎に個別のガイドラインを作成することが有効である。

(3) 重要業務の継続に不可欠なシステムの抽出

・第 2 次行動計画（別紙 1）で示されている重要システムと、重要インフラ事業者が想定する BCP で重要業務の継続に不可欠なシステムとは必ずしもすべてが一致しているわけではなかった。災害や障害のレベルによって、復旧目標が変化するため、それに伴い重要業務の継続に不可欠なシステムも、変化するものであるという認識を持つ必要がある。重要業務の継続には、災害や障害のレベルによって、不可欠な対応・システムを整理しておくことが重要である。

(4) 実効性のある演習と評価の実施

・真に実効性のある BCP とするためには、BCP を PDCA サイクル（Plan（計画）→ Do（実行）→ Check（評価）→ Act（改善））に則り運用していく中での、演習と評価が重要である。評価には、内部での監査を充実させる他、米国で推進されている第三者認証制度（3.2.2 参照）について、我が国においても活用を促すことが有効だと考える。演習については 3.4.2.3 にて提言を述べる。

3.4.2.3 実効性のある BCP 演習とするための提言

今回の BCP 調査より、NISC として情報セキュリティの観点を踏まえ、より実効性のある BCP 演習にするためには、次の項目の実施が必要だと考える。

(1) BCP 演習内容の拡充

・発生原因から成るシナリオ型演習が多く見られたが、不測の事態に真に備える為には、発生原因には注目せず、「IT 不通になった場合」等の発生事象から考え、復旧させる演習にすべきである。

・容易に復旧できる内容ではなく、復旧が困難な演習シナリオとすることで、BCP の問題点を洗い出す演習内容にすべきである。

・サプライチェーン・マネジメントを考慮した演習を実施するべきである。

我が国の重要インフラの BCP 演習に盛り込むべき項目（例）を表 39 に列挙する。なお、表 39 に記載した事項は一例であり、組織に応じた内容を検討する必要がある。

表 39 BCP 演習に盛り込むべき項目（例）

BCP 演習に盛り込むべき項目（例）	備考
実施概要	発生原因ではなく発生事象からの内容にするとよい。
実施詳細内容	シナリオ型、シミュレーション型、机上型等の実施方法があげられる。 事業の継続を意識した内容とするとよい。
体制	主催、参加メンバー、連携組織、オブザーバー等があげられる。

スケジュール	実施する期間、タイムスケジュール等があげられる。
その他	演習で確認された問題点の取り扱い等について明記しておくとよい。

(2)事業継続と情報システムの関わりを考慮した演習の実施

3.3.1 より、BCP 演習の多くは災害対応訓練という位置づけであり、情報システムの復旧演習はBCP 演習とは別物という位置づけであった。しかし、次に示すように、情報システムの復旧演習は、重要インフラの各分野の特徴に応じて、BCP 演習の一環として実施すべきである。

重要インフラ分野は、水道分野・ガス分野・電力分野のライフライン系、鉄道分野等の交通インフラ系、情報通信分野・金融分野の情報インフラ系に分類できると言う意見がある[82]。このライフライン系、交通インフラ系、情報インフラ系では、次に示すように事業継続のための情報システムへの依存度が異なるため、BCP におけるサービスの維持・継続に関わる情報システムの安定運用の視点も異なる。

ライフライン系・交通インフラ系においては、制御等の作業において、人手の代わりとして情報システムを活用している場合が多い。このため情報システムが停止してしまった場合でも、人員さえ確保できれば、通常状態の運用は難しくとも、緊急待避的な最低限の事業継続が可能であると言える。

一方、情報インフラ系においては、情報システムは人手の代わりとしてではなく、サービス維持の要であるため、情報システムの回復が事業継続に大きな影響を及ぼす。よって、情報インフラ系では、情報システムの事業継続への関与を強く意識し、充実させる必要があると考えられる。

情報システムの復旧演習は、システム障害からの復旧だけを目的とするのではなく、BCP 演習の一環としてとらえ、重要インフラの各分野の特徴に応じて実施することが必要である。

(3)分野合同演習

国として、地域ごとにライフライン系、交通インフラ系、情報インフラ系それぞれの BCP の策定レベル、演習レベル(以下、策定レベル等という。)を指し示すべきである。

ただちに国として策定レベル等を示すことは難しいと考えられるため、例えば、セプターカウンシル等との連携の中で、重要インフラ分野間で現実的(実効的)な策定レベル等を見極めていくことも重要だと考えられる。検討された策定レベル等を基に、分野合同演習を実施できるような環境を整えていくことも必要と考える。

その際、演習の実施方法として、国は評価者として演習に参加し、相互依存性に配慮した全体の方針決定と、演習結果報告を受けることで、重要インフラ分野間でのより実効的な意見交換が期待でき、また、国が評価者となることで、BCP の PDCA をまわす上での Check フェーズ機能が高まると考える。その為にも国として標準的な評価基準の策定が重要だと言える。

以上

[82]中央防災会議発行「首都直下地震対策専門調査会報告」より
http://www.bousai.go.jp/jishin/chubou/shutochokka/houkoku.pdf

別紙1. 第 2 次行動計画で示されている重要インフラ分野

重要インフラ分野	IT障害やその影響の例	対象となる重要システム例
情報通信	・電気通信サービスの停止 ・電気通信サービスの安全・安定供給に対する支障等 ・放送サービスの停止	・ネットワークシステム ・オペレーションサポートシステム ・ニュース・番組制作システム ・編成・運行システム
金融 銀行 生命保険 損害保険 証券会社 金融商品取引所	・預金の払い出し、振込等資金移動、融資業務の停止 ・保険金の支払い停止 ・有価証券売買の停止 等	・勘定系システム ・資金証券系システム ・国際系システム ・対外接続系システム （オープンネットワークを利用したサービスを含む。）
航空	・運航の遅延、欠航 ・航空機の安全運航に対する支障等	・運航システム ・予約・搭乗システム ・整備システム
鉄道	・列車運行の遅延、運休 ・列車の安全安定輸送に対する支障等	・列車運行管理システム ・電力管理システム ・座席予約システム
電力	・電力供給の停止 ・電力プラントの安全運用に対する支障等	・制御システム ・運転監視システム
ガス	・ガスの供給の停止 ・ガスプラントの安全運用に対する支障等	・プラント制御システム ・遠隔監視・制御システム
政府・行政サービス（地方公共団体を含む）	・政府・行政サービスに対する支障 ・個人情報の漏洩、盗聴、改ざん	・各府省庁及び地方公共団体の情報システム（電子政府・電子自治体への対応）
医療	・診療支援部門における業務への支障等	・診療録等の管理システム
水道	・水道による水の供給の停止 ・不適当な水質の水の供給　等	・水道施設や水道水の監視システム ・水道施設の制御システム等
物流	・貨物の遅延・停止 ・貨物の所在追跡困難	・集配管理システム ・貨物追跡システム ・倉庫管理システム

情報セキュリティ政策会議決定「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」より引用

別紙2. IPA テクニカルウォッチ:『新しいタイプの攻撃』に関するレポート
～Stuxnet（スタックスネット）等の新しいサイバー攻撃手法の出現 ～（抜粋）

IPA（独立行政法人 情報処理推進機構）セキュリティセンターから 2010 年 12 月 17 日 に発行された、「IPA テクニカルウォッチ:『新しいタイプの攻撃』に関するレポート ～Stuxnet（スタックスネット）等の新しいサイバー攻撃手法の出現～」より、『新しいタイプの攻撃』に関する概要をまとめた部分を以下に抜粋する。

以下「IPA テクニカルウォッチ:『新しいタイプの攻撃』に関するレポート ～Stuxnet（スタックスネット）等の新しいサイバー攻撃手法の出現～」より一部抜粋

1. 昨今のサイバー攻撃の実態と傾向

1. 1. 新しいサイバー攻撃手法の出現

脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しく執拗な攻撃が出現してきている。この新しいサイバー攻撃は 2010 年の春頃から海外では APT(Advanced Persistent Threats)と呼ばれている。
IPA では、システムへの潜入等の「共通攻撃手法」と情報窃取等の目標に応じた「個別攻撃手法」から構成される攻撃であると分析した。このように「共通攻撃手法」と「個別攻撃手法」を持った攻撃を IPA では、『新しいタイプの攻撃』と呼ぶ。
この攻撃を使った最近の事例としては世界的に話題となった Stuxnet と呼ばれるコンピュータウイルスが挙げられる。Stuxnet は、原子力発電所の制御システムに影響を及ぼしたのではと報道されている。なお、日本国内でも数件の検出事例が報告されているが、被害事例は報告されていない。

1. 2. 社会インフラへの攻撃の広がり

従来の攻撃対象は、情報システムであり、そのシステム上にある資産や情報等を狙ったものであった。電力や鉄道等のような社会インフラは、制御システムを組み込んで、実現されている。そのため制御システムを攻撃されると社会インフラが影響を受け、社会全体が影響を受ける可能性がある。このように、社会インフラが攻撃者のターゲットになったことに合わせて、防御側が守るべきシステム範囲も広がり、制御システムの関係者を巻き込んだ体制も必要となってきている。

2.『新しいタイプの攻撃』の実態

IPA では、システムへの潜入等の「共通攻撃手法」と情報窃取等の目標に応じた「個別攻撃手法」から構成される攻撃であると分析した。

2. 1. 脅威・問題点分析について

脅威は、システム構成や業務等で異なる。「個別攻撃手法」の対象を、情報システムや制御システムにすることにより、幅広い各種システムが攻撃対象となり、個別の防御対策は困難である。
例えば日本において、前述の制御システムは、一般に米国等と比較して、制御ネットワークが独立・分離されている事に加え、制御システムも今回悪用された制御システムの製品ベンダとは異なる事から、直ちに、海外と同様の脅威が発生するとは限らない。日本における適切な対策を進めるためには、単に技術的な情報を海外から得るだけでは無く、日本の実情に応じた分析と対策を行う必要がある。
そのためには、「共通攻撃手法」に対する対策を、日本の実情に応じた影響(ビジネスインパクト)をシステム設計の中で検討し、対策を実施することが重要である。
また、攻撃者は Windows や Linux に熟知しているだけでなく、制御システムについての知識も十分持っていると推測される。このような攻撃者に対応するためには、防御側でも制御システムを含む幅広い技術者の連携で対応する必要があるということも言える。

2. 2. 『新しいタイプの攻撃』の流れ

標的型メール攻撃や USB ストレージを悪用したウイルス等による組織の情報搾取を目的とした情報システムへの攻撃においても同様な共通的攻撃手法が用いられる。
セキュリティベンダー等の各機関が出しているレポートや IPA での解析結果を踏まえると、『新しいタイプの攻撃』は概ね下記のようなステップで攻撃が行われる。
＜「共通攻撃手法」と「個別攻撃手法」の流れ＞
(「共通攻撃手法」)
① インターネットや USB ストレージを通じた情報システムへのウイルス感染
② システムの脆弱性を利用することによる情報システム環境内部でウイルスの拡散
③ バックドアを作成し、外部の指令サーバ(C&C サーバ)と通信することにより、ウイルスの増強や新たなウイルスのダウンロードの実行
※ウイルスの増強やダウンロードは以降④⑤の手順でも実行される可能性あり。
(「個別攻撃手法」:Stuxnet の場合)
④ 原子力システム等を制御する装置が配備してある、制御システムへの侵入
⑤ 制御システム上にある装置に対する攻撃の実行

以上