RCSS ディスカッションペーパーシリーズ ISSN-1347-636X
第 57 号　2007 年 11 月
Discussion Paper Series
No.57 November, 2007

企業価値を高める事業継続計画の提案
－システムリスクを中心とした議論－

竹村 敏彦・長岡 壽男

RCSS

文部科学省私立大学学術フロンティア推進拠点
関西大学ソシオネットワーク戦略研究センター

Research Center of Socionetwork Strategies,
The Institute of Economic and Political Studies,
Kansai University
Suita, Osaka, 564-8680 Japan
URL: http://www.rcss.kansai-u.ac.jp
http://www.socionetwork.jp
e-mail: keiseiken@jm.kansai-u.ac.jp
tel: 06-6368-1228
fax. 06-6330-3304

企業価値を高める事業継続計画の提案
－システムリスクを中心とした議論－

竹村 敏彦*
関西大学ソシオネットワーク戦略研究センター†

長岡 壽男‡
関西大学ソシオネットワーク戦略研究センター

2007 年 11 月

概 要

本研究の目的は、企業の直面する多様なリスクに対して有効となる事業継続計画（BCP）の立案に対する提案をおこなうことにある。まず、企業の直面している多様なリスク（企業の信用リスク、自然災害被災のリスク、テロによるリスク、情報システムリスク、不祥事のリスクなど）を経営課題の側面から整理する。次に、リスクを最小限にすることを目的とする形式的な BCP の立案に終始することではなく、それを戦略的にとらえ、企業価値を向上に資するビジネスモデルを提案する。最後に、これらを踏まえて、有効な BCP の立案につながるアイデアを具体的に提示する。

KEYWORD: 事業継続計画（BCP）、事業継続マネジメント（BCM）、情報セキュリティ、企業価値、信頼資産

*関西大学ポストドクトラル・フェロー・E-mail: takemura@rcss.kansai-u.ac.jp
†〒 564-8680 大阪府吹田市山手町 3-3-35 関西大学経済・政治研究所ソシオネットワーク戦略研究センター
‡関西大学 RCSS 委嘱研究員・E-mail: nagaoka@rcss.kansai-u.ac.jp

Suggesting a Business Continuity Plan to Heighten Enterprise Value

Toshihiko Takemura
E-mail: takemura@rcss.kansai-u.ac.jp
Research Center of Socionetwork Strategies, Kansai University,
3-3-35 Yamate, Suita, Osaka, 564-8680, JAPAN,

Hisao Nagaoka
E-mail: nagaoka@rcss.kansai-u.ac.jp
Research Center of Socionetwork Strategies, Kansai University,
3-3-35 Yamate, Suita, Osaka, 564-8680, JAPAN.

June, 2007

Abstract

The purpose of this paper is to suggest what business contingency plan (BCP) becomes effective against various risks the enterprises face. First of all, we arrange the countermeasures against risks from the aspect of the business the enterprise has faced. The risks are credit risk of the enterprise, risk of a natural disaster, risk by terrorism, information system risk, and the scandal, etc. Next, we propose the BCP business model contributes to the improve their enterprise values, not just making the formal BCP which minimizes risks. The BCP should be strategic. Finally, we concretely present effective BCP.

Keyword: Business Continuity Plan, Business Continuity Management, Information Security, Enterprise Value, Reliance Asset

1　はじめに

毎年、台風や地震、集中豪雨などの自然災害が日本各地において発生している。それに加えて、インターネットがビジネスプラットフォームとなった現在では日々新たな脅威が出現し、各企業は多種多様なリスクと背中合わせの状態にある。従来は緊急時対応計画（コンティンジェンシープラン）を作成して（一時避難的な）対策がなされていたものの、上述したようにインターネットへ強く依存している企業にとっては、継続的な計画を作成しておく必要がある。それは事業継続計画（BCP; Business Continuity Plan）と呼ばれるものである。

ここで、従来からあるコンティンジェンシープランはと BCP の違いについて簡単に触れることにする。前者と後者の大きな違いは、後者は人命に加えて、ビジネスの早急な再開にも重きをおいているものとなっている。特に、本研究のトピックとして取り上げる情報システムとは、ほぼビジネスという言葉と同値と言っても過言ではない。これは言い換えると、情報システムを止めることはビジネスを止めることを意味する。そして、それは 1 つの企業のみが損害を被るのではなく、それに関連する多くの企業がその被害を被ることになり、一時避難的な対策では不十分となるのである。

これらの状況および近年の国外の動向を踏まえて、日本の各省庁はそれぞれ BCP に関するガイドラインなどを策定している。

経済産業省 (2007) によれば、日本の上場企業における BCP 策定率は 9.8%程度に留まっており、海外企業の 47%と比べて遅れをとっている。注目すべきことは、海外での BCP を策定する理由として既存・見込み顧客からの要請が中心となっている。海外の動向を踏まえると、各企業の BCP 整備は、グローバルサプライチェーンに入るための必須条件となりつつある。

このような状況を鑑みて、本研究では、各企業における BCP 策定および事業継続マネジメント（BCM; Business Continuity Management）の必要性および BCP 策定と企業価値の関係について議論し、有効となる BCP 策定において必要とされるいくつかのアイデアを提示する。なお、本研究では BCP における重要な項目の 1 つである情報セキュリティ対策を取り上げている[1)]。

本研究の構成は次の通りである。次節で企業の直面している様々なリスクなどについて経営課題の側面から整理する。第 3 節では企業価値を高める情報セキュリティ対策・投資を BCP の観点から議論する。第 4 節では有効な BCP の策定につながるアイデアをいくつか提示する。そして、最後の節にて本研究のまとめと今後の課題を与える。

2　企業を取巻くリスクと BCP

本節では、BCP に関するリスクなどについて簡単に説明する。なお、網羅的に企業のリスクマネジメントを議論しているものとして吉川 (2006) などがあるので参照されたい。

企業が直面する可能性があるものとして、地震などの自然災害、爆発・テロなどの人為的災害、情報システム障害・インターネットの脅威などの情報通信技術（ICT; Information and Communication Technology）に関する事故やトラブル、不祥事など多数存在する。これらに直面すると、事業所・工場の閉鎖、情報システムの被災・停止、営業停止、重要情報やデータの損失、情報流出・漏洩およびそれによる企業のイメージの低下など、企業にとって存亡にかかわる状態に陥ることになる。特に、ICT に関する事故やトラブルは次節で見るように、もっとも遭遇しやすいリスクであるといえる。このような状態に陥らないようにするための計画およびマネジメントが必須なものとなっ

[1)] 一般的に、BCP 策定にあたって、個々のリスクの対応策を個別かつ網羅的に進めることは得策ではなく、企業存続に重大な影響を与えるものを選んで共通する部分を活用することが推奨されている。

ている。つまり、各企業は、組織を脅かす潜在的なインパクトを認識し、利害関係者の利益、名声、ブランドおよび価値創造活動を守るために、復旧力および対応力の構築する有効な計画である BCP およびそれを実行するためのフレームワークである BCM が必要とされる[2)]。また、近年 BCP の ISO 標準化対応が経済産業省を中心に進められ、また海外でも国際標準化の動きが見られている。今後経営において重要な役割を果たすものとなることが予想される。BCP および BCM の国際的な動向については財団法人日本情報処理開発協会 (2007) などを参照されたい。

3　企業価値を高める BCP

経済学や経営学の分野において、インターネットなどの ICT 投資が企業の生産性や効率性、企業価値の向上に大きく貢献していることが様々な実証研究の結果から明らかにされている[3)]。

総務省 (2006) によれば、企業のインターネット普及率は 2005 年度末には 99.1%にまで達しており、インターネットは企業活動にとって必要不可欠なビジネスプラットフォームとなったといえる。このようなビジネス環境において、企業は急速に ICT への依存度を強めており、このことは今後さらに進むと予想される。それゆえに、企業にとって「情報システムを止めないこと」と「ビジネスを止めないこと」が同値となりつつあるといえる。しかしながら、一方でインターネットには様々な脅威（マルウェア、フィッシングや DoS（Denial of Service）攻撃、ゼロディアタックやボットネットなど）が存在しており、これらの情報インシデントに関する問い合わせ件数は情報処理推進機構（IPA）などによれば年々増加傾向にある[4)]。つまり、各企業はこれらの脅威の被害者になる（時として知らないうちに加害者もなっている）可能性が高くなる。また、近年では個人情報漏洩などに関して本来非難されるべき加害者よりも被害者を非難する風潮もある。それゆえに、これらの脅威から情報資産および各種資産を防護するための情報セキュリティ対策が必要とされる。今までの情報セキュリティ対策はコンプライアンス（法令順守）、取引先との契約のためといった保守的な動機による形式的なものが多かった。これらの形式的な対策・投資は、本質的な問題として必ずしも社会的責任を果たしているとはいえない。また、もし本格的に対策をおこなうとすれば膨大な費用および時間が必要とされるために、費用便益の観点から企業では必ずしも優先されずに、リスクコントロールをうまくできているとはいいがたい。それゆえに、本研究では、形式的な情報セキュリティ対策・投資ではなく、戦略的な情報セキュリティ対策・投資が必要であることを主張する。この戦略的情報セキュリティ対策は、BCP の策定や BCM において必須な項目であるといえる[5)]。

本研究における戦略的情報セキュリティ対策・投資とは、単に直面している情報資産および各種資産を防護する（直面しているリスクを回避する）ことを目的としているだけではなく、様々なリスクなどに対して適切な対応ができる、またセキュリティ文化（Culture of Security）をもつ企業として社会や市場から評価されるために実施するための対策・投資である。社会や市場から評価されることによって、企業価値を高められるということが本質的な考え方である。そのためには、企業内で単にその対策を実施するだけでなく、社会や市場に対してその状況（対策の内容・評価）を

---

2) BCP は、コンティンジェンシープランよりもある意味広い概念であり、いくつか異なる点を有することに注意されたい。

3) Ukai *et al.* (2005) や江良・竹村 (2005) は日米における包括的な ICT 投資の経済分析に関するサーベイを与えているので参照されたい。

4) http://www.ipa.or.jp/を参照されたい。

5) （情報）セキュリティの機能（抑制・予防・検知・回復）は BCP 策定に必須とされる項目である。
戦略的情報セキュリティ対策・投資は、企業の社会的責任（CSR; Corporate Social Responsibility）、コーポレートガバナンス、コンプライアンス体制、内部統制システムにおいても基礎となる必須項目である。

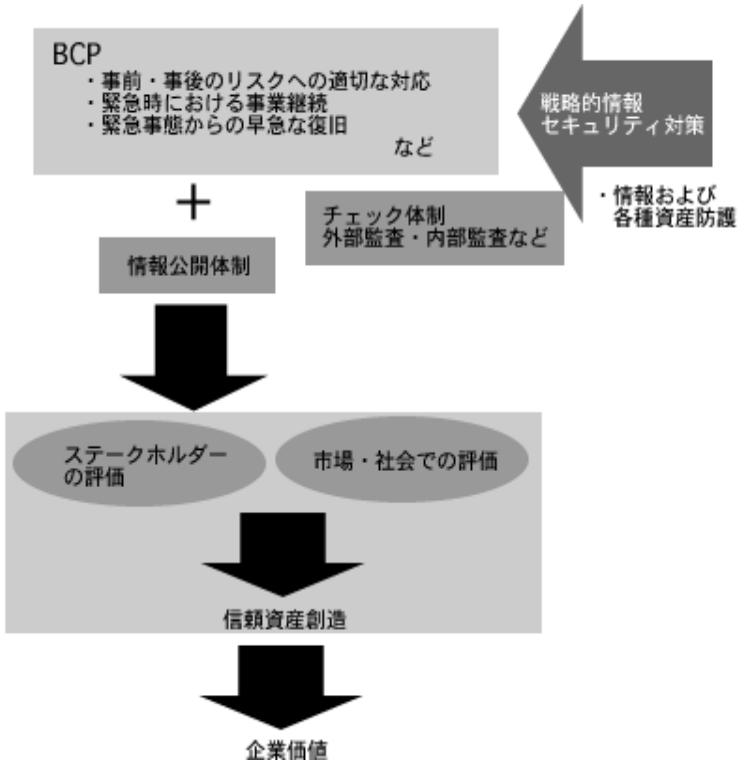

図 1: 戦略的情報セキュリティ対策が企業価値を創造するプロセス

公開することも重要であると考えられる[6)]。

戦略的情報セキュリティ対策が企業価値を創造するプロセスを図示したものが図 1 である。

田中・松浦 (2005) や竹村 (2007) で指摘されているように、情報セキュリティ対策の中でも、情報セキュリティ教育（人材育成）の徹底や情報セキュリティインシデントへの対応体制の明確化、PDCA サイクルの確立などは企業の目に見えない信頼資産（intangible trust asset）を創造する上で重要である[7)]。この信頼資産が新たな企業価値向上に寄与するものである。各企業は戦略的に情報セキュリティ対策・投資をすることで、この信頼資産を創造することができる。これは、従来考えられていた情報セキュリティ対策・投資のイメージとは異なるものであり、積極的に対策・投資をするインセンティブとなりうる。

4 有効な BCP の策定

経済産業省 (2005) によると一般的な BCP 策定において、1) 事業継続に重大な影響を与える問題の分析、2) 事故や災害の発生に対して、体制・組織の構築や対応計画の策定、3) 計画の戦略的活用と運営などを経て、改善箇所を PDCA サイクルの中で継続的に修正、といったプロセスを踏むことが望まれている。基本的には、これらの各省庁から出されている BCP 策定マニュアルを参考にして、各企業の特性に適ったものを策定すればよい。しかしながら、一部の企業で「具体的な対応がわからない」、また「金融商品取引法（J-SOX 法）における IT への対応（IT 統制）などと

6) 情報セキュリティ報告書などにおける公開内容については様々な議論がされている。
7) PDCA サイクルとは、

の関連から混乱が生じている」、「策定するだけで実現可能であるかは不明である」、といったことなども指摘されている。そのために、本節では、いくつかの BCP に盛り込まれるべき実行可能かつ、必要最低限であると著者たちが考える項目についてまとめる。表 2 には、有効であろう BCP 策定に関するアイデアをまとめている。

表 1: 有効な BCP 策定に必要とされる項目

項目	内容
業務	優先業務の特定化 迅速な復旧活動
事務	生産設備・仕入調達などの代替策 提供できるサービスレベルの協議 人員確保
情報システム	バックアップシステム・リカバリーシステムの確立 ネットワークの切り分け 情報システムセキュリティ対策
組織マネジメント	トップマネジメントのリーダーシップと責任の明確化 教育・訓練体制の確立 現場とのコミュニケーション 連絡体制・組織の整備
チェック体制	内部監査 外部監査
広報・情報公開	社会およびステークホルダーへの連絡体制の確立・説明責任

このアイデアの特徴を簡単にまとめてこの節を終わることにする。もっとも緊急事態のときに主要な事業を継続・復旧することが企業にとって最優先されることであるが、その次に重要なことが関連機関との連絡体制である。つまり、(一時的であれ) 事業を縮小したり、取引先や顧客に対しても影響を与えたりする。それらの影響を最小にすることも考慮しなければならない。また、2 次被害が予想されるような情報システムに関する事故においては、それが生じないように、管轄官庁、取引先や顧客に対して適切に連絡体制を確立することや、マスコミを利用してその 2 次被害拡大を防止するための対策および経緯などの説明責任を果たすことが重要とされる。

この他にも、事前および事後対策として、外部や内部の様々な監査体制の導入も有効である。もちろん、リーダーシップを発揮し、また遭遇した状況について説明責任を果たすトップマネジメント・組織のあり方についても考える必要がある。

5 まとめ

本研究では、簡単ではあるが企業の直面しているリスクを整理すると同時に、BCP 策定および BCM の必要性について言及した。また、情報セキュリティ対策を取り上げて、BCP 策定が企業価値を高めうることについても議論してきた。そして、いくつかの BCP 策定において有効となるアイデアを提示してきた。

企業価値を高めることについて、業績を上げることだけでなく、企業がいかに直面している問題に対して適切な対応ができるかというマネジメントについてもステークホルダーは評価している。その表れが、近年注目されている CSR、コーポレートガバナンス、コンプライアンス、内部統制などである。これらはそれぞれが独立したものではなく、相互に深く関連している。また、BCP もこれらの基礎を構成しており、深く関連するものである。それゆえに、これらのマネジメントを考えるときは、独立してこれらへの対応を図るのではなく、これらの内容を整理・調整して効率的なマネジメントをおこなうべきである。その役目を BCP や BCM は担うものであると考える。

第 1 節でも触れたように、海外において事業展開する場合、BCP の策定が必要条件となりつつある。また、経済産業省 (2007) で指摘されているように、近年では国際標準化の流れが進んでおり、各企業にとって積極的に BCP を策定することが将来必要となると予想される。このような国内外の動向を踏まえると、経営戦略として BCP の策定が今後の企業のカギとなることを示唆できる。

最後に、本研究では一般的な企業を対象に議論してきた。しかしながら、経済・社会全体への影響・責任が大きいとされる重要インフラについてはより高いレベルの BCP 策定が望まれる。これらについての議論は今後の課題としたい[8)]。

追記

本研究は、竹村が文部科学省の科学研究費補助金交付課題「情報インフラにおけるセキュリティ投資の経済分析」（課題番号 18730202・若手研究 (B)・研究代表者 竹村敏彦）、長岡が文部科学省の科学研究費補助金交付課題「金融パニックシミュレーション実験－妥当なミクロ金融政策の構築－」（課題番号 19653027・萌芽研究・研究代表者 鵜飼康東）から助成を受けておこなった研究成果である。

また、本稿は 2007 年 11 月 4 日の愛知学院大学に於ける第 55 回日本情報経営学会全国大会で発表した「企業価値を高める事業継続計画」を加筆修正したものである。討論者である水尾順一氏（駿河台大学経済学部・教授）とセッションの司会である高橋敏朗氏（大阪市役所・監査委員）から有益な助言をいただいた。また、鵜飼康東氏（関西大学ソシオネットワーク戦略研究センター・センター長）からも貴重なコメントを頂いた。ここに記して謝意を表したい。もちろん残る誤りは、全て筆者の責に帰すものである。

参考文献

[1] Ukai, Y., S. Wanatabe, H. Nagaoka and T. Takemura (2005) *Economic Analysis of Information System Investment in Banking Industry*, Springer, Tokyo.

[2] 江良亮・竹村敏彦 (2005)『電気通信インフラ整備と政策評価（平成 16 年度自主研究報告書)』国際通信経済研究所（RITE）, RITE04-J04, pp.1-41.

[3] 経済産業省 (2005)「事業継続計画（BCP）策定ガイドラインの概要」経済産業省商務情報政策局情報セキュリティ政策室.

[4] 経済産業省 (2007)「経済産業省の情報セキュリティ政策と動向」経済産業省商務情報政策局情報セキュリティ政策室.

[8)] 例えば、銀行業における BCP 策定に関しては日本銀行 (2005) などを参照されたい。

[5] 財団法人日本情報処理開発協会 (2007)「事業継続管理（BCM）に関する調査報告書－ BCM（BS25999）と関連領域の整理」財団法人日本情報処理開発協会.

[6] 総務省 (2006)『情報通信白書』ぎょうせい.

[7] 竹村敏彦 (2007) 「情報セキュリティ投資の経済分析」RCSS Disucussion Paper Series (関西大学), No.49.

[8] 田中秀幸・松浦幹太 (2006)「情報セキュリティ投資の経済的動機付けに関する企業レベルの実証研究」, 研究調査報告書（財団法人電気通信普及財団）, 第 21 号, pp.9-16.

[9] 長岡壽男・竹村敏彦 (2007)「企業価値を高める事業継続計画」『情報経営（第 55 回全国大会予稿集）』, pp.149-152.

[10] 日本銀行 (2003)「金融機関における業務継続体制の整備について」日本銀行.

[11] 吉川吉衛 (2006)『企業リスクマネジメント』中央経済社.