

# BCMS 実証運用 中間報告

平成 21 年 9 月



財団法人 日本情報処理開発協会

## BCMS 実証運用 中間報告

1.	はじめに.....	1
2.	BCMS 実証運用の概要.....	1
3.	BCMS 実証運用 中間報告.....	2
	1) .BCMS 認証機関の評価について.....	3
	2) .BCMS 適合性評価制度の評価について.....	5
	3) .BCMS 実証運用に対する総合評価.....	6
4.	参考資料.....	8

## 1. はじめに

企業・組織において事業継続を図る上で影響を及ぼす様々なリスクに対して、どのように対応を図っていくかは、大きな課題である。企業・組織にとって、そのような不測の事態においても事業そのものを中断することなく、継続・維持するための方針や手続きをまとめたものが BCP (Business Continuity Plan : 事業継続計画) である。また BCP の作成も含め、事業継続の戦略的な運営管理の手法が BCM (Business Continuity Management : 事業継続マネジメント) である。

また、ネットワーク型社会においては、個別組織が単独で取り組むだけではレジリエンスの確保が難しいので、サプライチェーンなどの外部組織との相互依存性や地域コミュニティなどの社会的な階層性を考慮する必要がある。

しかしながら、組織自らの企業価値の向上や社会的責任を果たすべき取組みとして、BCP/BCM を考えるならば、まずは個別組織のステークホルダーのニーズに応えることが前提となる。こうした現状の中で、個別組織を取り巻くステークホルダーを認識しながら、自然災害や IT 事故など様々な脅威を前提として事業継続に取り組むこととなる。

とりわけ、昨今は事業の IT への依存度が高まっており、事業継続を考える際にも多くの場合、直接・間接のいずれにせよ、IT システムを除外して考えることは不可能である。また、事業継続性の確保の観点から、これら IT システムに対する脅威は、企業・組織全体に対する事業に影響を及ぼすものであることを認識した上で BCP/BCM を策定することが重要であり、そうした方法論に対するニーズが高くなってきている。そして、BCM ライフサイクルが効果的に運用管理され、改善されることを確実にするマネジメントシステムが BCMS (Business Continuity Management System : 事業継続マネジメントシステム) であり、これに対応する規格として BS 25999-2 がある。

このような状況を踏まえ、JIPDEC としては、わが国の産業の健全な発展を図るため、BCMS 認証基準 (BS 25999-2) を用いた枠組みによる BCMS の普及・定着を、国際整合性への意識をしつつ図っていくこととする。

## 2. BCMS 実証運用の概要

BCMS 適合性評価制度の正式運用を実施するための準備として、平成 20 年度及び平成 21 年度の実施を BCMS 実証運用と位置付け、BCMS 実証運用の評価結果により認定・認証制度を確立することを目的とする。

BCMS 実証運用時に適用する認証のための基準は BCMS 認証基準 (BS 25999-2) とし、実証運用を通じて正式運用時の BCMS 認証基準の内容を検討する。また、認定のための基準は BCMS 認証機関認定基準及び指針 (JIP-BCAC100-0.8) とし、実証運用を通じて内容を検討する。

BCMS 実証運用期間中では、JIPDEC は申請した認証機関に対して評価を行い、認証機関は組織への BCMS 認証審査を行う。また、BCMS 認証審査は可能な限り JIPDEC が立ち会い、認証機関の BCMS 認証審査等を評価する。

なお、BCMS 実証運用では「仮認定」、「仮認証」とし、BCMS 実証運用期間終了後、差分審査等を経て正式な「認定」、「認証」に移行する。

BCMS 実証運用における運営体制は、次のとおりである。

#### **【BCMS 準備運営委員会】**

BCMS 実証運用の円滑かつ公平な実施のため、BCMS 準備運営委員会を JIPDEC 内に設置し、認証機関の認定に必要な基準や審査員資格基準などについて検討し、かつ諮問的な役割を担う。また、正式運用への移行を検討・評価する役割も担う。

#### **【BCMS 技術専門部会】**

BCMS に関連するガイド等を作成し、かつ利害関係者との協議を行うための場として、BCMS 技術専門部会及び作業部会を設置する。

#### **【事務局】**

BCMS 実証運用を円滑に推進するため、JIPDEC 内に事務局を設置する。

### **3. BCMS 実証運用 中間報告**

BCMS 実証運用は、平成 20 年 7 月 30 日に開始し、BCMS 実証運用実施要領を Web で公表した。また、BCMS 適合性評価制度の検討について財団法人日本適合性認定協会と協力していく旨の内容を公表した。

平成 20 年 9 月 29 日には認証機関向けの BCMS 実証運用説明会を実施し、JIPDEC で認定している ISMS/ITSMS 認証機関のほぼ全機関（参加者数 54 名）の出席があった。また、平成 20 年 10 月 30 日には BCMS の導入を検討している事業者向けの BCMS 実証運用説明会を実施し、108 名の申込みがあり、97 名の参加者があった。

平成 21 年 7 月現在、BCMS 実証運用に申請した認証機関は全 5 機関で、認証機関名は次のとおりである。仮認定を発行した認証機関は、3 機関である。

#### **[BCMS 実証運用 申請機関]**

申請 5 機関

- ・ [BCR004P] BSI マネジメントシステム ジャパン株式会社
- ・ [BCR018P] ビューローベリタスジャパン株式会社 システム認証事業本部
- ・ [BCR021P] SGS ジャパン株式会社 認証サービス事業部
- ・ [審査中] 日本検査キューエイ株式会社
- ・ [審査中] 財団法人 日本品質保証機構 マネジメントシステム部門

BCMS 実証運用の評価基準は、BCMS 認証機関認定基準及び指針 (JIP-BCAC100-0.8) 及び BCMS 審査員の資格基準に関する指針 (JIP-BCAC401-0.8) に基づいて実施した。現時点における BCMS 実証運用の評価結果は、次のとおりである。

## 1) BCMS 認証機関の評価について

### (1) 認証機関の組織体制 (JIP-BCAC100-0.8 6 組織運営機構に対する要求事項及び9 プロセス要求事項)

BCMS 認証業務における組織体制の準備状態については、各認証機関は JIS Q 17021 への対応済みであり、ISMS、QMS 等の他マネジメントシステム規格と同様の組織体制となっていた。

また、認証業務手順については、他マネジメントシステム規格の手順と統合されており、BCMS に関する差分 (審査工数、審査員の力量の定義等) を追加するかたちで行われていた。

これらのことから、認証機関における組織体制及び手順の準備状態は十分と考えられる。

### (2) 審査員に対する教育及び力量評価の仕組み (JIP-BCAC100-0.8 7 資源に対する要求事項)

BCMS 実証運用の実施要領にある BCMS 審査員の資格基準に関する指針 (JIP-BCAC401-0.8) における資格基準である「CBCI<sup>(1)</sup>又は同等の資格」を有しており、力量的にも問題ないものであった。また、すでに資格を取得し、審査実績がある審査員を中心に BCMS 審査員の増員を計画していた。

注<sup>(1)</sup> CBCI : Certificate Business Continuity Institute

### (3) 要員 (審査員以外) に対する教育及び力量評価の仕組み (JIP-BCAC100-0.8 7 資源に対する要求事項)

要員 (審査員以外) については、BCMS 認証審査へのオブザーバ参加を実施したり、また、BCMS に関する資格保有者が見積、契約など最初の部分を担当したりと、機関全体の力量向上を図っており、BCMS 認証業務に対して積極的に力量の向上を目指していた。

### (4) 審査員の力量 (JIP-BCAC100-0.8 7 資源に対する要求事項)

#### (4)-1 審査員の力量・知識

審査員の知識については、CBCI 資格を取得するなどして、全ての認証機関が審査員の力量を担保することを実施していた。審査員の力量・知識については、問題ないと考えられる。

#### (4)-2 審査スキル

#### [適用範囲の適正]

適用範囲の確認については、経営者インタビューを通じて「事業継続の要求事項」、「組織の目的及び義務」の観点から十分な審査が実施されていた。

#### [組織文化に BCM を組み込む]

審査では、従業員に対する教育記録・評価内容を確認することで対応していた。さらに、BS 25999-2 の特徴でもある「組織文化に BCMS を組み込む」の「文化」について、十分な時間をかけて審査が実施されていた。

#### [BIA・リスクアセスメント・事業継続戦略の決定]

BIA、リスクアセスメントについては、それぞれの結果を確認し、手順及び記録の面から規格要求事項への適合性について確認しており、十分な審査スキルが確保されていた。

#### [BCP・IMP]

BCP、IMP の文書を確認し、実際の場面（インシデント発生の時間帯等）を想定した確認がなされており、組織に対して適切な指摘がなされていた。審査スキルも十分に確保されていると考える。

#### [演習、維持及びレビュー]

演習計画、結果等について内容を確認し、認証基準の要求事項への適合性について十分な審査が実施されていた。演習についても BCP、IMP と同様に様々な場면을想定した確認がなされており、審査スキルも十分に確保されていると考える。

#### (5) 登録証の記載内容 (JIP-BCAC100-0.8 8 情報に関する要求事項)

登録証に記載する内容については、QMS と同様であり、認証範囲（製品、サービスなどを含んだ）、サイト、対象組織が記載され、特に問題はなかった。

## 2) BCMS 適合性評価制度の評価について

現時点における、BCMS 認証機関認定基準及び指針（JIP-BCAC100-0.8）及び BCMS 審査員の資格基準に関する指針（JIP-BCAC100401-0.8）に関する要求事項としてさらに継続検討が必要な事項は、次のとおりである。

### (1) 登録証における適用範囲の記載内容

BCMS 認証を取得し、社会に対して提示する場合に登録証に記載した方が良い項目（認定基準で要求されている項目にさらに加えた方が良い項目）。

項目	区分	評価
想定した脅威（リスク）	継続検討	BCMS というマネジメントシステムに対する認証であるため、想定した脅威（地震、火事、パンデミック等）だけを記載することについては、誤解を生じる可能性があるため慎重に検討する必要がある。この点については、継続検討とした。

※登録証に記載する項目とは別に、日本における BCMS 適合性評価制度として、認証に関する情報を社会に対してどこまで公開すべきかを議論していく必要がある。

### (2) 審査工数

BCMS 認証審査を行う上で必要する審査工数を決定するために加味した方がよい項目。

項目	区分	評価
従業員数	要	ISMS、QMS 等と同様、従業員数は審査工数に加味すべき要因であると考ええる。
サイト数	要	〃
重要な製品	要	従業員数、サイト数だけでなく、重要な製品/サービスごとに BCP を策定する場合があるので、現時点では審査工数に加味した方が良いと考える。
業種	継続検討	現時点では、情報・通信に関する企業が多かったが、業種が審査工数に影響する点は見受けられなかった。この点については、継続検討とした。

### (3) 業種の専門性

BCMS 認証審査を行う上で業種区分の必要性。

項目	区分	評価
業種区分	継続検討	現時点では、立会審査3件、また事務所審査で5件の審査記録を確認したが、情報・通信に関する企業が多かった。そのため、業種区分の必要性について結論を出すためには、今後の立会審査または事務所審査での審査記録で確認件数を積み上げ、全体的な比較検討を行うことが必要であり、継続して検討を行う。

### 3) BCMS 実証運用に対する総合評価

「1) BCMS 認証機関の評価について」は、各認証機関とも規格要求事項（BS 25999-2）に沿って、適切な審査が実施され、特に大きな問題はなかった。BCMS はトップダウンの要素が強いため、BCM の方針、適用範囲の決定から BIA、リスクアセスメント、さらには BCP 策定までの流れが重要であると考えられる。この関係についてもう一段深く審査することにより、受審側にとってさらに価値ある審査になると考えられる。

「2) BCMS 適合性評価制度の評価について」で継続検討となったところは、登録証への記載事項、審査工数及び業種の専門性についてである。

登録証への記載事項については、サイト、製品/サービス以外に、BCP で対象としたリスク（地震、パンデミック等）を記載した方が良いのではないかという意見もあったが、BCMS というマネジメントシステムに対する認証であるため、想定した脅威（地震、火事、パンデミック等）を記載することについては、慎重に検討すべきであるという意見もあった。この点については、継続検討とした。

業種の専門性については、現時点では情報・通信に関する企業が多かったため、(2) 審査工数の「業種」、(3) 業種の専門性については、さらなる判断必要である。この点については、継続検討とした。

最後に、BCMS 認証基準（BS 25999-2）及び BCMS 認定基準についてである。

BCMS 認証基準については、事業継続マネジメントシステム要求事項の規格が現時点では BS 25999-2 だけである。その内容については、ISMS、QMS 等の他のマネジメントシステムとの整合性もよく、問題ないと考えている（4. 参考資料を参照）。ただし、BCMS 認証基準に関しては国際整合性を確保するため、今後発行予定である ISO/IEC 22301 の動向を注視していく必要がある。

次に、BCMS 認証機関認定基準及び指針（JIP-BCAC100-0.8）については、BCMS

実証運用を通じて得られた結果から、BCMS 固有の審査員の力量に関する定義、審査工数等について、今後、さらなる検討が必要であると判断した。

現在の BCMS 認証組織数に対する審査員の人数としては、問題ないとする。また、全ての認証機関で BCMS 審査員の増員（2～3名の増員、多いところでは8名の増員）を計画しているため、今後 BCMS 認証組織数の増加に対応できると考えられる。今後の市場の大きさについては予想しにくいですが、仮に認証組織数を 300 件とした場合、実証運用 5 認証機関（計 15 名）、正式運用後 10 認証機関（計 30 名＋増員計画分）であれば、審査員の数として十分な現状であるとする。

以上の結果から、次の継続検討項目が残っている状況である。今後、正式運用に向け、これらの項目について、より明確にするために、BCMS 実証運用を延長していくこととする。

- ① 登録証における適用範囲として、想定した脅威（リスク）を記載すること。
- ② 審査工数を決定する要因として業種を加味すること。
- ③ BCMS 認証審査を行う上で業種区分を加味すること。
- ④ BCMS 認証機関認定基準及び指針について、改訂すること。

#### 4. 参考資料

BS-25999-2 と他のマネジメント規格との対応表

BS 25999-2:2007	ISO/IEC 27001:2005	ISO 9001:2000
0 序文 (まえがき)	0 序文 0.1 一般 0.2 プロセスアプローチ 0.3 他のマネジメントシステムとの両立性	0 序文 0.1 一般 0.2 プロセスアプローチ 0.3 ISO 9004 との関係 0.4 他のマネジメントシステムとの両立性
1 適用範囲	1 適用範囲 1.1 一般 1.2 適用	1 適用範囲 1.1 一般 1.2 適用
	2 引用規格	2 引用規格
2 用語及び定義	3 用語及び定義	3 用語及び定義
3 BCMS の計画 3.1 概要 3.2 BCMS の確立及び管理	4 ISMS 要求事項 4.1 一般要求事項 4.2 ISMS の確立及び運営管理 4.2.1 ISMS の確立 4.2.2 ISMS の導入及び運用	4 QMS 要求事項 4.1 一般要求事項
4 BCMS の導入及び運用 4.1 組織の理解 4.2 事業継続戦略の決定 4.3 BCM 対応の開発及び導入 4.4 BCM の取組みの演習、維持及びレビュー	4.2.4 ISMS の維持及び改善	
3.4 BCMS の文書及び記録 3.4.1 概要 3.4.3 BCMS 文書の管理 3.4.2 BCMS 記録の管理	4.3 文書化に関する要求事項 4.3.1 一般 4.3.2 文書管理 4.3.3 記録の管理	4.2 文書化に関する要求事項 4.2.1 一般 4.2.2 品質マニュアル 4.2.3 文書管理 4.2.4 記録の管理

<p>5 BCMS の監視及びレビュー</p> <p>5.2 BCMS のマネジメントレビュー</p> <p>5.2.1 概要</p> <p>5.2.2 レビューへのインプット</p> <p>5.2.3 レビューからのアウトプット</p> <p>5.1 内部監査</p>	<p>7 ISMS のマネジメントレビュー</p> <p>7.1 一般</p> <p>7.2 レビューへのインプット</p> <p>7.3 レビューからのアウトプット</p> <p>6 ISMS 内部監査</p>	<p>5.6 マネジメントレビュー</p> <p>5.6.1 一般</p> <p>5.6.2 マネジメントレビューへのインプット</p> <p>5.6.3 マネジメントレビューからのアウトプット</p> <p>8.2.2 ISMS 内部監査</p>
<p>6 BCMS の維持及び改善</p> <p>6.1 予防処置及び是正処置</p> <p>6.2 継続的改善</p> <p>6.1.3 是正処置</p> <p>6.1.2 予防処置</p>	<p>8 ISMS の改善</p> <p>8.1 継続的改善</p> <p>8.2 是正処置</p> <p>8.3 予防処置</p>	<p>8 改善</p> <p>8.5.1 継続的改善</p> <p>8.5.2 是正処置</p> <p>8.5.3 予防処置</p>

以上