# 地震前提から脱却せよ

## 国際規格 ISO/IEC27031 から学ぶ

IT サービス継続対策のポイント

**IT サービスを継続させる仕組みとして IT-BCP という言葉が使われるようになったが、多くは災害対策（ディザスターリカバリー）と同じ意味で使われていることが多い。しかし、過去に地震災害などで実際に IT サービスが止まったケースがどのくらいあるだろう。今求められているのは、災害対策のためだけでなく、ヒューマンエラーを含めたあらゆるリスクから、IT サービスを継続させる視点だ。**

寄稿　深谷純子

## IT サービス継続の国際規格

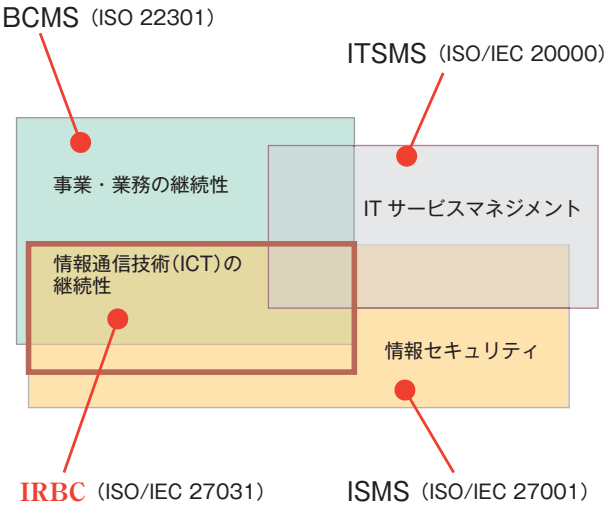
2011 年 3 月に、IT 業務継続計画の実質的な国際規格となる ISO/IEC27031（IT サービス業務継続ガイドライン：IRBC）が公開された（ISO/IEC27031：Guidelines for Information and Communication Technology Readiness for Business Continuity）。

このガイドラインは、情報セキュリティに関する国際標準の一部として策定されているが、IT 担当者には分かりやすく、IT-BCP（※）の策定ポイントが述べられている。

※：ガイドラインでは　IRBC（ICT Readiness for Business Continuity）と記載されているが、本文では IT-BCP と表示する。

IT-BCP を策定する上では、既に公開されている ITSMS（ISO20000 IT サービスマネジメント、いわゆる ITIL：2005 年）と ISMS（ISO27001 情報セキュリティ：2006 年）、そして現在審議中の BCMS（ISO22301 事業・業務の継続性）が関係してくる。これらの標準に一部重複する形で、しかも IT サービスの継続に関して詳細に解説されているのが、当ガイドラインである。

**図 1　関係規格の位置づけ**



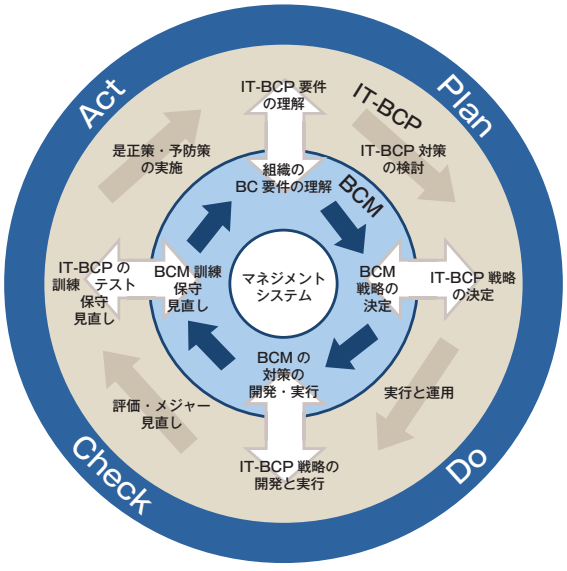

## BCP は、IT-BCP と連動する

業務継続を求められる重要なビジネス機能は、通常 IT に依存しているため、BCP は IT-BCP と連動する。ガイドラインの 1 つ目の特徴は、ビジネスとの連携を強め、BCM の PDCA サイクルに IT-BCP のマネジメントシステムを組み込むことが強調されている点である。ビジネス側に、IT 側の現状のリソース状況、対策に必要なコスト（初期費用と継続費用）と効果、技術的制約等を説明し、IT の回復能力について脆弱点を含めてビジネス側からの承認を求める。IT とビジネスは各々の PDCA サイクルで連携する必要がある（図 2 ⇔の部分を参照）。

## 脅威は自然災害だけではない

2 つ目の特徴は、IT 基盤やシステムに影響があるすべての事象や事件（セキュリティ関係を含む）を想定しており、脅威を地震などの自然災害に特定していない点だ。IT-BCP は全社 BCP と同じではない。実際、地震によってシステムが停止し、それ

**図 2　IRBC と BCMS の統合**



が直接原因で業務が中断したケースは、過去にはほとんどない（ただし、将来的にもないというわけではない）。

IT がビジネスの足を引っ張るという、IT 担当者にとっては最悪のケースでの脅威は、①オペレーションミス、②プログラムエラー、③パフォーマンス低下、④情報漏えい、⑤コンピュータウィルスなどである。従って、訓練に関しても代替システムへの切替やシステム回復作業だけでなく、上記①～⑤が発生した場合の回復訓練が含まれていなくてはいけない。

## 緊急時の初動対応こそ重要

3つ目は、IT-BCP の対応フェーズを、予防、検知、対応、回復、改善と定義している点である。BCP 関連の他ガイドラインと比較すると緊急時の初動対応に重点が置かれている。十分な予防策を講じた上で、障害の早期検知、被害を最小化する迅速な対応が重要だということだ。図3では、経済産業省の事業継続計画策定ガイドライン（2005 年）で定義されているフェーズを左端に記載している。このガイドラインは ISO27031 と同様、情報セキュリティを発端にしているが、結果として回復フェーズが強調された地震用の BCP が意識されている。

## ガイドラインに加えて考慮すべき点

IT サービス業務継続ガイドラインでも触れられていることだが、業務中断を引き起こし、業務に混乱をきたすシステム障害こそ、IT-BCP で取り組むリスクである。それらのリスクを引き起こす真の原因を以下のようにまとめた。

1. 要員に関する問題：担当者のスキル不足、教育や周知不足 、プログラム保守やシステム運用の属人化
2. プログラムに関する問題：改修を重ねた複雑なア

**図 3　BCP で検討するフェーズ**

| 経産省ガイドライン（注） | ISO27031 でのフェーズ | 説　　明 |
|---|---|---|
| | 障害予防<br>Prevention | ICT サービスを、環境的な脅威、ハードウェアの故障、運用エラー、悪意のある攻撃、自然災害などの脅威から守る。組織にとって期待されるレベルのシステム可用性を維持するには欠かせない。 |
| BCP 発動フェーズ | 障害検知<br>Detection | 最も早い機会での障害検知は、サービスに対する影響を最小化し、回復エラーを削減し、サービスの品質を持続する。 |
| | 障害対応<br>Response | 最も適した方法で障害に対応することは、回復が容易になり、ダウンタイムが最短化する。不適切な対応は、ささいな障害をもっと重大なものへとエスカレートする結果になる。 |
| 業務再開フェーズ | 障害回復<br>Recovery | 最適な回復戦略を策定し実行することは、タイムリーなサービスの再開やデータの信頼性維持を確かにする。業務回復優先順位を理解し、最重要サービスを最初に使えるようにする。重要度が下がるサービスは後で回復されるか、状況によっては回復されない場合もある。 |
| 業務回復フェーズ | | |
| 全面復旧フェーズ | | |
| | 改善<br>Improvement | 小規模、大規模の障害から学んだことは、文書化して、分析し、見直すこと。障害の経験から学ぶことで、システム障害に対する予防管理と障害回避の改善につながる。 |

（注）経済産業省「企業における情報セキュリティガバナンスのあり方に関する研究会」報告書（参考資料）事業継続計画策定ガイドライン

プリケーションの使用による問題の分かりづらさ

3. システムリソースに関する問題：リソース不足、想定外の大量アクセスの発生、サポート切れソフトウェアやハードウェアの使用

4. 予算の問題：システム開発・運用の予算削減によるリスク対応力の低下

5. システム要求への問題：無理なシステム機能要求、短期間での対応、頻繁な例外処理の発生

個々の問題は互いに関連性があり、まとめて解決することが望ましい。例えば､プログラムの問題は、スキルや予算が問題になることが多く、リソースの問題は、予算とシステム要求が問題になることも多い。そして、これらのIT サービスが抱える問題のほとんどは､「ビジネス側からの要求を発端としており IT 部門では断りにくいこともある」。

## IT サービス継続対策としてのクラウド

現在注目されているクラウドによって、IT サービスが抱える問題が解決できないだろうか。クラウドには、①システム資源を保有せず、②ネットワーク上のシステムを使用し、③従量制課金によりスケールアウト・スケールインが容易であり、④実績のあるアプリケーションを利用し、⑤標準的なシステム運用がなされている。また､⑥システムの仮想化、⑦分散処理ができることも特長である（クラウドの提供形態によっては、一部の機能しか実現できないものもある)。

通常、BCP の観点でクラウドを検討する場合、災害対策を意識したバックアップ取得オプションを含むシステム運用や、障害時の対応に効果がある仮想化、分散処理によるビジネス拠点との同時被災の回避などが注目されている。上記、クラウドの特長の⑤⑥⑦。

表 1 は、前述した「ガイドラインに加えて考慮すべき点」を解決する視点でクラウドの他の特長も含めて検証してみたものである。もちろん、現行のシステムをすべてクラウド化するのは難しく、業務のやり方を変更する必要もでてくる。しかし、国内や海外でもクラウドを利用する企業が増えてきている

**表 1　IT リスクとクラウドによる解決**

| 業務中断を招く IT リスク | IT リスク発生の原因 | クラウドによる解決の可能性 |
|---|---|---|
| オペレーションミス<br>プログラムエラー<br>パフォーマンス低下<br>情報漏洩<br>コンピュータウィルス<br>ハードウェア障害 | 要員に関する問題<br>・要員不足<br>・スキル不足 | ・センター側で訓練された要員による十分な体制でのサービス提供<br>・セキュリティなど専門性の高い要員によるサービス提供 |
| | プログラムに関する問題 | ・利用実績のあるアプリケーションのため、自社開発に比べて潜在バグが少ない<br>・プログラム開発・保守が不要 |
| | システムリソースに関する問題 | ・システムリソースの拡張が容易<br>・センター側でのバージョンアップ作業による保守性の確保<br>・最新のハードウェアの利用が可能 |
| | 予算の問題 | ・リソース共有化によるコストメリット<br>・将来を見通したリソースの事前調達が不要<br>・開発・運用・保守要員の自社確保が不要 |
| | システム要求に対する問題 | ・標準化されたメニューによる例外処理の排除<br>・標準機能を使用することで、システム要求への早期対応が可能 |

中、クラウドを全く考えないのもリスクではないだろうか。

## 東日本大震災から学ぶ IT 対策のポイント

3 月 11 日に発生した東日本大震災は、広範囲にわたり甚大な被害をもたらした。この貴重な経験を振り返り、現対策の見直しポイントをいくつかまとめてみた。

### ■重要 IT 機器を離す

データセンターが被災地から離れていたため、データセンターの被害はほとんどなかったと思われる。IT 回復作業は、現地のネットワークや PC 端末関係が多かった。このことから、少なくとも重要業務拠点とデータセンター（重要 IT 機器）は、同時被災を回避するためにも離れていた方が有効だと言える。本番センターとバックアップセンターの距離についても、一概に安全な距離は言えないが、例えば電力会社の管轄が分かれるくらいの距離は必要かもしれない。

### ■データは遠隔地保管

データのバックアップは複数保持し、必ず遠隔地保管すること。コストや情報セキュリティの観点でデータの分散保管に課題はあるが、データの重要性と復元の難易度を考えると、必要なデータが有ると無いでは、被災後の復旧スピードが格段に違ってくる。住民基本台帳は県や国でバックアップがあるため回復できたが、その他の重要データの被災は深刻だ。

### ■人の移動は前提としない

バックアップセンターには、なるべく災害発生時に移動することを前提としない方法を検討する。移動する手段がない、キーマンの不在等で移動できる要員がいない場合があるからだ。そのためには、バックアップセンターに常時要員を配置するか、自動化や遠隔操作により移動を最小化する。バックアップセンターに限らず、移動できないことを前提にした業務継続の手段としては、在宅勤務を検討するも有効である。

### ■複数のコミュニケーション手段を準備

今回、被災地は通信回線が途絶し、被災地以外は輻輳や発信制限があり、安否確認システムは十分機能しなかった。対策としては、複数のコミュニケーション手段を準備しておくことと、連絡が取れない場合の対応手順を決めておくことが有効だと思われる。前者に関しては、今回の震災で、チャット（Facebook、Twitter などを含む）や Skype での通話は使えたことから、緊急連絡手段に取り込むことも必要ではないか。後者に関しては、連絡が取れない場合は最悪の事態を想定した手順を始める、指示を待たずにできる範囲を決めておくこと、権限委譲などがある。

## 過去から脱却せよ

IT をレジリエンスにすることで、ビジネス継続を支えたいと思う。それには、今までとは異なる IT-BCP の発想が必要だと思う。P.F. ドラッカーの名言「過去から脱却せよ」を「地震前提の BCP から脱却せよ」と置き換えて終わりにする。

深谷純子（ふかや・すみこ）
深谷レジリエンス研究所代表
レジリエンスに関する研究活動、執筆、講演、コンサルテーションを実施
HP: www.fukayaresilience.com
日本アイ・ビーエム出身