

BCM Newsletter

～BCM(事業継続マネジメント)ニュースレター～

英国における BCM 構築事例

Newton Information Technology Ltd.

シニアコンサルタント(公認情報システム監査人)

須藤亜紀

ターンブルガイドランスが前提とする、英国におけるコーポレートガバナンスでは、内部統制の責任は取締役会と経営陣の双方が負うこととなります。本ガイドランスはまた、内部統制システムの構築を推進するにあたっての実務的ガイドとしても利用され、その中では、ロンドン証券取引所の上場企業全てにおいて、事業継続性を確保することについても触れられています。英国 FSA(Financial Services Authority:金融庁)もまた、管轄企業に対して、事業継続性を確保するための計画の策定、及び、その有効性のテストを義務付けています。

本稿では、外国の銀行が英国において銀行業に新規参入するに際し、英国 FSA からの認可を得るための準備として筆者が携わったプロジェクトについて、ご紹介をいたします。

1. 英国 FSA 要求事項

銀行業に新規参入するには、英国 FSA からの様々な要求事項を満たしていることを証明しなければなりません。「証明」とは、認可の申請者(当該銀行)による証明だけでなく、外部スペシャリストによる「意見書」の提出も必要となります。

IT に関するコントロール要求事項は、主に以下の9つのエリアに分類されますが、事業継続に関する要求事項については、「情報システムの可用性」(表 1)及び「情報システムの復旧手順」(表 2)の項に含まれています。

- ・ IT ガバナンス
- ・ プロジェクト管理
- ・ オンライン・ビジネス・システム管理
- ・ 情報セキュリティ
- ・ 情報システムの可用性
- ・ 情報システムの復旧手順
- ・ 変更管理手順
- ・ 情報システム関連文書管理
- ・ その他(外部委託など)

表 1 情報システムの可用性について(一部抜粋)

課題	回答例
<ul style="list-style-type: none"> ● ビジネス活動を支える情報システムの可用性に関する目標時間(例:情報システムの稼働率(%)) 	<ul style="list-style-type: none"> ● 営業時間中は、業界標準の 98.7%を情報システム稼働率の目標値とします。
<ul style="list-style-type: none"> ● 情報システムの最大許容停止時間、及び、情報システムの停止中に顧客を損失から保護するための手順 	<ul style="list-style-type: none"> ● ビジネス・インパクト分析の結果、当行における重要ビジネス(例:トレーディング)に関連する情報システムの最大許容停止時間は4時間となりました。4 時間を越えて情報システムが停止する場合には、事業継続計画書を発動します。 ● 情報システムの停止中には、情報システムを使用せず手作業にて顧客対応するための手順があります。
<ul style="list-style-type: none"> ● 情報システム基盤が利用不可能になった際の‘弾力性・回復力’、‘冗長性’について 	<ul style="list-style-type: none"> ● 重要ビジネスに関連する情報システムについては、オフィス内でのホットスタンバイサーバ設置及び、DR サイトにおけるウォームスタンバイサーバ設置・リアルタイムデータ複製を行っています。 ● その他のサーバ(ファイルサーバ、メールサーバなど)に関しても、DR サイトにおいてリアルタイムでのデータ複製を行っています。

表 2 情報システムの復旧手順について(一部抜粋)

課題	回答例
<ul style="list-style-type: none"> ● 事業継続計画(及び災害復旧計画)は、業界ベストプラクティスに基づいて策定されているか 	<ul style="list-style-type: none"> ● 事業継続マネジメントに関するベストプラクティス(BS25999)及び英国 FSA より発行されている‘事業継続マネジメント実践ガイド’に基づき、事業継続計画は策定されています。
<ul style="list-style-type: none"> ● 事業継続計画(及び災害復旧計画)に含まれる主な構成 	<ul style="list-style-type: none"> ● BS25999 及び英国 FSA より発行されている‘事業継続マネジメント実践ガイド⁽¹⁾’を基に構成します(詳細は次項を参照のこと)。
<ul style="list-style-type: none"> ● DR サイトに含まれるサービス 	<ul style="list-style-type: none"> ● DR サイトにて提供される主なサービスは以下の通りです。 <ul style="list-style-type: none"> － フロントオフィス用デスク:4つ － システム管理者及びオペレーション用デスク:8つ － ミーティングルーム
<ul style="list-style-type: none"> ● 事業継続計画(及び災害復旧計画)のテスト頻度及び、改訂の頻度 	<ul style="list-style-type: none"> ● 事業継続計画(及び災害復旧計画)のテスト及び定期レビューは、年 2 回(9 月・3 月)実施します。 ● また、当行でのビジネスや情報システム基盤、あるいは、組織内に変更がある際には、事業継続計画(及び災害復旧計画)を見直し、必要に応じて改訂します。
<ul style="list-style-type: none"> ● 事業継続計画(及び災害復旧計画)書はオフサイトにも保管されているか 	<ul style="list-style-type: none"> ● 事業継続計画(及び災害復旧計画)書は CD に保存し、DR サイト及び BCM チームメンバーの自宅にて保管されています。

⁽¹⁾ 英国 FSA・イングランド銀行及び英国財務省が、2005 年に金融サービス業を対象に行った‘災害時における企業の弾力性・回復力に関する調査’の結果を基に策定したガイドライン。金融サービス業が事業継続計画を考える際の参考となる実践例が提供されている。

2. ベストプラクティスに基づく BCM 構築

上述の通り、英国 FSA は業界ベストプラクティスに基づいた事業継続計画（及び災害復旧計画）の策定を推進しています。英国では PAS56 をベースとした事業継続マネジメントの構築を行っている企業が多くありますが、本プロジェクトでは BS25999 のフレームワークを利用することにしました。

また、具体的な計画書の作成に際しては、英国 FSA より発行されている‘事業継続マネジメント実践ガイド’を参照しています。本実践ガイドでは、以下の項目について‘調査対象企業のほぼ全てが導入している一般的な管理策’及び‘調査対象企業の中で一部のみが導入している、より強度な管理策’を提供しています。

- ・ 企業全体の事業継続に関する対策
- ・ クライシス・マネジメントに関する対策
- ・ 情報システム及び通信に関する障害対策
- ・ 設備に関する対策
- ・ 人に関する対策

BCM 構築にあたって行った、主な作業は以下の通りです。

- ① 主要なビジネスプロセスの洗い出し
- ② ステークホルダー（利害関係者）の特定と要求事項、及び、法令（例：データ保護法）により課せられる義務の特定
- ③ 主要なビジネスプロセスをサポートするためのリソースの特定
- ④ 上述①～③の相互依存関係の分析
- ⑤ 主要なビジネスプロセス、及び、それをサポートする重要なリソースを中断または混乱させる可能性があるとして認識された脅威の特定。尚、脅威の特定にあたっては以下のガイドラインも併せて参照しました。
 - ・ ISO/IEC 27001:2005 - Information Security Management Systems - Requirements
 - ・ BS 7799-3:2006 - Information Security Management Systems - Guidelines for information security risk management
 - ・ ISO/IEC TR 13335-3:1998 - Guidelines for the Management of IT Security - Techniques for the Management of IT Security.
- ⑥ 主要なビジネスプロセス、及び、それをサポートする重要なリソースの中断または混乱による影響の分析
- ⑦ リスク評価

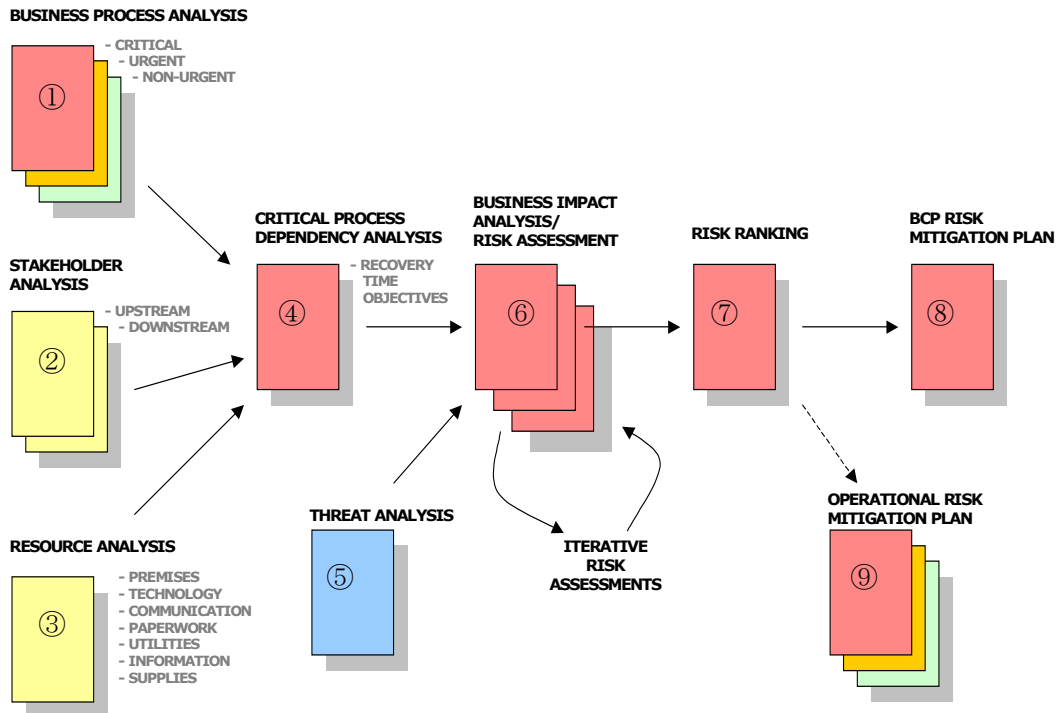


図 1 本事例における BCM 構築プロセス

- ⑧ 事業継続に係るリスクシナリオの特定と、対応計画の策定
- ⑨ 重要なオペレーショナルリスクシナリオの特定 (例: オフィスビルへのアクセス不能、電源の利用不能、オフィスのある地域一帯へのアクセス不能) と、対応計画の策定

3. BCM への取組みに関する訓練及びレビュー

事業継続計画は、「発生の可能性は低いが、発生した際には組織の主要ビジネスの継続に深刻な影響を与えらるリスクシナリオ」について策定されます。そのため、定期的な訓練及びレビューを行わないと、容易に形骸化してしまう危険性があります。

英国 FSA は、策定した事業継続計画の定期的なテスト及び改訂を要求していますが、頻度については特に触れていません。本プロジェクトでは、年 2 回の定期テストを実施することで合意しています。第一回目のテストでは、シナリオとして「オフィスのある地域一帯へのアクセス不能」を想定しています。全社員を合わせても 30 人程度であることと、事前インタビューの結果、BCM チームリーダーを除くほぼ全員が、事業継続計画に関する認識が浅い

ことが判明したため、一部の人のみを対象としたテストではなく、全社員を対象にした訓練を実施することにしました。DR サイトへ移動しての業務継続、監督庁への電話連絡 (実際は弊社スタッフへの電話連絡) など、出来る限りリアルにシナリオを再現してのテストを行いました。筆者及び弊社スタッフは、オブザーバーとしてテストに参加し、BCM チームの対応・管理能力と、各社員がそれぞれ自分に割り振られた役割を適切に果たしているかを確認しました。

4. おわりに

英国においては、情報セキュリティマネジメントへの対応と並び、事業継続マネジメントへの対応レベルが取引先選定時に重要視されます。加えて、英国 FSA が業界ベストプラクティスに基づいた事業継続マネジメントの構築を要求していることを鑑みると、従来の PAS56 に代わり、今後は更に BS25999 のフレームワークを利用した BCM 構築が盛んになってくると思われます。これを受け、日本においても同様の動きがあることが予想されるのではないのでしょうか。

【著者】

Newton Information Technology Ltd.

須藤 亜紀

シニアコンサルタント (公認情報システム監査人)

【本稿に関するお問い合わせ (著者)】

E-mail: A.Sudo@newtonit.co.uk

【株式会社 Newton IT について】

英国、日本にオフィスがあり BS25999 をベースとした BCM の構築、実装支援を行っている。また、J-SOX 対応 (内部統制の構築) や ISO 認証取得支援の実績も豊富。

編集者より

今回は、Newton IT の英国オフィスに勤務されている須藤氏から、英国において BS25999 を活用した事例について、寄稿していただきました。

かつて情報セキュリティマネジメント規格である BS7799 が制定されたとき、最も早い時期からこれに取り組んだのは英国の金融業界であり、ここから波及して、金融業界と取引のある企業や、海外の金融業界に広がっていきまし

た。このような経緯を考えると、今回のように BS25999 が制定されてから比較的早い時期に、金融機関での活用事例が紹介されるのは、象徴的であると言えます。

ところで、今回の事例では、規格による認証取得は求められていません。それにもかかわらず、BS25999 という規格に基づいて BCM 構築を進めています。これはなぜでしょうか？

それは、BCM の導入のしかたや、導入後のマネジメントシステムに関するフレームワークが、規格によって提供されているからです。これらを最初から自力で考えるよりも、既存のフレームワークを利用した方が、必要な要素を漏れなく効率的に導入していくことができ、導入時の試行錯誤を減らすことができると考えられます。

また、リスクアセスメントの際に検討すべき脅威や、対応策として検討すべき項目が、規格の中で網羅的にリストアップされているため、規格を参照しながら導入を進めることによって、検討漏れを防ぐことができます。

もともと、唯一絶対的に正しいフレームワークや、完璧なチェックリストなどは存在しません。しかし今回の事例で活用されている BS7799、同 25999、ISO27001、同 13335 は、いずれも多くの専門家の知見に基づいたガイ

ドラインとして、広く認知されていますので、これらに基づいて進めていけば、導入や運用のしかたについては、概ね妥当であろうと期待できます。また、これらのガイドラインに準拠しているということで、社外に対して取り組み状況を説明しやすくなるというメリットもあります。

このように、規格の使いみちは認証取得だけではありません。当面は認証取得の必要が無いという企業であっても、BCM を効果的に導入・運用するために、関連する規格やガイドラインの活用を検討されてはいかがでしょうか。

(株式会社インターリスク総研 田代 邦幸)

BCM Newsletter 発行事務局
株式会社インターリスク総研
コンサルティング第二部 BCM チーム

東京都千代田区神田駿河台 3-9
TEL 03(3259)3614
FAX 03(3292)6116

BCI ジャパンアライアンス とは

<http://www.bcijapan.jp/>



BCI ジャパンアライアンスは、BCI(The Business Continuity Institute) (下記参照)の活動に賛同する企業・機関が集まって、BCI とともに設立したものです。日本国内において事業継続マネジメント(BCM: Business Continuity Management)の普及・啓発、BCM に関する企業・官公庁・大学など研究機関への情報提供及び規格化・標準化の働きかけ、BCMに関する調査・研究、日本企業に即した BCM 技術の開発を実施してまいります。

BCM Newsletter では、こうした BCI ジャパンアライアンスの活動の一環として、BCM に関する最新情報や実践的な情報を提供してまいります。

BCI について

BCI は、BCM に携わる専門家の支援とガイドラインの提供を目的として、英国に 1994 年に設立された団体です。現在世界 85 カ国に 4,000 名以上の会員を有する世界最大の会員制組織です。

会員機関(50 音順)

- ◇ アイピーシー・インフォメーション・システムズ・ジャパン株式会社
- ◇ 株式会社 IT プロフェッショナル・グループ(ITPG)
- ◇ 株式会社アズジェント
- ◇ 伊藤忠テクノソリューションズ株式会社
- ◇ 株式会社インターリスク総研
- ◇ 三機工業株式会社
- ◇ 長岡技術科学大学経営情報系リスクマネジメント研究室
- ◇ 西日本電信電話株式会社(NTT 西日本)
- ◇ 日本ヒューレット・パッカード株式会社
- ◇ 特定非営利活動法人日本サブライマネジメント協会™
- ◇ 日本マネジメント総合研究所
- ◇ 株式会社 NEWTON IT
- ◇ BSI ジャパン株式会社
- ◇ BTジャパン株式会社
- ◇ ペリージョンソンレジストラー株式会社
- ◇ ストロール社(米国の BCM ソフトウェア開発会社)
- ◇ セバーン社(英国のリスクマネジメント会社)