＜研究論文＞

情報セキュリティの可用性に関する考察

A Study on the Availability of Information Security

黒川　信弘　Nobuhiro Kurokawa　情報セキュリティ研究プロジェクト
植野　俊雄　Toshio Ueno　情報セキュリティ専門監査人
齋藤　敏雄　Toshio Saito　ISU　日本大学

概要

最初に東日本大震災による企業[1]の事業被害状況を示し、震災で明確になった事業継続管理の取組みの現状と課題を示す。次にISMS[2]における事業継続管理のポイントをまとめ、情報セキュリティにおける可用性の観点から現状の企業のISMSへの取組みの問題点を明らかにし、さらにISMSにおける事業継続管理の位置づけと可用性の関係および、事業継続管理を中心とした可用性の考え方を示す。最後に、企業の情報セキュリティにおける可用性の位置づけと特徴を明らかにし、可用性を実現するための考え方と具体的な方策を提言する。

キーワード：情報セキュリティ、可用性、事業継続管理、ISMS

はじめに

2011年に発生した東日本大震災は、我々日本人に未曽有の被害と多くの教訓を残した。東北日本地域に存在する企業の被害は甚大なものとなったが、一方で我々は災害や事故時の事業継続能力が企業存続のための重要な要素となることを再認識した。情報セキュリティ面からも、多くのサーバやデータが流され使用不能となった惨状を目の当たりにして、事業継続管理の意味合い、在り方が問われるものとなり、その結果、情報セキュリティを構成する要素としての可用性に対する考え方の再検討を要求される事態となった。つまりこの大災害は、組織にとっての可用性とは何であるか、その維持のために何をすればいいか、改めて考えさせられる機会となった。

本論文では、今まで機密性の後ろに隠れていた“可用性”にスポットを当て、企業にとっての情報セキュリティにおける可用性の真の意味合いとは何かを事業継続との関連で明らかにする。特に、事業継続管理と可用性の関係を考察するとともに、情報セキュリティにおける可用性の位置づけと特徴を明らかにし、可用性を実現するための考え方と具体的な方策を提言する。

第一章　東日本大震災における事業継続管理

1-1. 東日本大震災における企業の被害状況

2011年3月11日14時46分頃、東日本大震災が発生した。人類史上最大級のこの震災はマグニチュード9.0の地震による揺れに引き続いて発生した広範囲にわたる大規模な津波で東北日本太平洋沿岸部に壊滅的な被害をもたらした。さらには原子力発電所からの放射性物質の漏えいを伴う重大な原子力事故という二次災害に発展した。これら被害の状況は、人的、物的、経済的に阪神淡路大震災をもはるかに凌駕するものであり筆舌に尽くしがたいものがある。

それら甚大な被害に関して、企業へのアンケート[1]結果によれば、今回の震災で26％の企業が「重要な業務が停止した」と答えている。このうち21％はその停止期間が1カ月以上に及んだという。さらに「一部業務が停止した」（29％）を含

2012/9/11 受付、2013/3/21 受理

めると55%の企業で何らかの業務停止が発生したことになる。重要な業務が停止した理由として、「停電のため」(62%)、「業務に必要な生産拠点が利用できなかった」(45%)、「取引先の業務停止などにより必要な調達・供給が行えなかったため」(44%)を挙げている。

㈱NTTデータ経営研究所の意識調査[2]によれば、これら震災による被害の影響は、大規模・多拠点の企業ほど重要な業務が停止した割合が高くなり、1000人以上の企業は78.6%、5000人以上では8割を超えている。

このように今回の大震災による企業における被害は日本がかつて経験しなかったほど甚大なものである。

1-2. 特筆すべき具体的な被災状況

今回の震災で企業活動に関係する面から特筆すべき事象を二つ取りあげる。一つ目は、情報システムの被災である。建物自体が津波に飲み込まれ、コンピュータはじめ多くの機材・設備が流され、あるいは浸水され、壊滅的な損害を受けた事例が多い。それ以外でもサーバラックが倒れた、プリンタが落下したなどの地震の揺れによる機材の物理的な破損も多く見られた。情報システム全体を立ち上げるためには、システム要員をはじめベンダ技術者、あるいはマニュアルなどが必要になるため、人的損害および交通インフラ等の正常化も含めてソフト面での可用性喪失も大きな問題となった。

二つ目は、通信ネットワークの可用性喪失である。基地局やケーブルの流出・破損とともに派生的に行われた通信規制などによりネットワークは壊滅的な状況となり、固定電話、携帯電話の音声通話・メールおよびインターネットがほぼ利用できなくなった。ただ、ツイッターなどインターネットSNS系サービスはレスポンスが落ちたにしても割合に利用できたという声もあった。

1-3. 事業継続の観点から参考となる企業の事例

その他に今回の震災で事業継続に係るものとして2、3の事例を取りあげる。

ICT企業やNPO・ボランティア団体は震災後早期にミラーサイトを立ち上げて、被災自治体ホームページのバックアップや被災者の所在探しを支援した。その他にも、日本マイクロソフト、日本IBM、ヤフー、ウェザーニュースなどの復興支援サイトでも関連情報提供が早期に行われ、さらには被災自治体や被災者支援を行うNPO団体に対して無償でクラウドサービスを提供した事業者も多い。緊急時に即座に情報システムを立ち上げることが可能であるクラウドサービスのBCP[3]機能をアピールすることにもつながった。

富士通では、福島県工場が被災したことで、デスクトップパソコンの製造中止を余儀なくされたが、震災の二日後には島根県のノートPC工場での代替製造を開始し、12日目には出荷を開始できた。これは2年間に及ぶ40回以上のBCP訓練、机上シミュレーションなどが功を奏した結果と言える。

また日本ガス協会によれば[4]、阪神淡路大震災など度重なる災害からの教訓と危機管理計画の策定によって大幅な事業復旧の成果を挙げた。具体的には耐震設計手法の導入による設備被害の低下(十分の一へ[4])、大幅なシステム変更による震災発生後のガス供給停止時間の短縮(16時間から50分へ)、業務面の仕組みの整備による震災発生から復旧までの日数の大幅な短縮(94日から54日へ)などの事業復旧の迅速化につながったと報告している。

1-4. 事業継続に対する企業の認識と課題

企業の事業継続管理についての認識は次の通りである。アンケート[1]によればBCP策定済み企業は49%、策定中17%であり3分の2はおおむね準備を終えつつあったと言っている。その一方、今回の震災でBCPが機能したかどうかについては「十分機能した」は7%に留まっており、「ほとんど機能しなかった」が15%あるなど9割がたの企業はその効果を疑問視している結果となった。

そのような自己評価を下した企業の考えるBCPの課題としては、「サプライチェーンの再構築」(42%)、「社員の安否確認システムの導入」(38%)、「情報システムに関する防災対策」(38%)が多く挙げられている。また今回の震災を経験して6割を超える企業がBCPを見直す考えを持っていた。

本論文では、東日本大震災を契機として浮き彫りになった事業継続管理の問題を、情報セキュリティにおける可用性の観点から考察する。

第二章　ISMS における事業継続管理

2-1. ISMS における事業継続管理とは何か

事業継続マネジメント（BCM）実践ガイドライン [6] では、事業継続実践アプローチを 6 段階（「図 2-1. 事業継続実践アプローチの 6 段階」）で示している。これを参考にしながら ISMS の管理策「A.14 事業継続管理」の狙いを管理策ごとに示す。

ISMS の管理策「14.1 事業継続管理における情報セキュリティの側面」は、情報システムの故障や災害の影響からの事業活動の中断に対処するとともに、情報システムが支える重要な業務プロセスやそれによって営まれている事業を保護し、時機を失しない再開を確実にすることを目的としている。

「14.1.1 事業継続管理手続への情報セキュリティの組込み」は、組織の事業継続に必要な情報セキュリティの要求事項を取り扱う管理された手続きを策定し特定することが目的で、図 2-1. の "段階 1" に対応し、6 段階からなる事業継続実践アプローチを情報システムの中断に対する事業継続管理に適用することを示している。

「14.1.2 事業継続及びリスクアセスメント」は、図 2-1. の "段階 2" 及び "段階 3" に対応し、業務プロセスの中断を引き起こす事象の特定、その発生確率及び影響の検討、リスクの特定、定量化、および優先順位付け、それらを事業継続戦略として策定し、経営陣の承認を得ることなどを狙いとする。

「14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施」は、図 2-1. の "段階 4" に対応し、インシデント対応判断の基準、手順、体制の決定、事業継続計画発動の手順と事業継続計画の手順の策定、復旧活動に関連する各々の事業や部門の対応計画の策定、手順及び手続の文書化、教育や計画の試験及び更新などを狙いとする。

「14.1.4 事業継続計画策定の枠組み」は、上記管理策 14.1.3 の計画を整合性の取れたものにするための枠組みの整備を目的としている。具体的には、事業継続の各計画の各要素の実行責任者、段階的計画及びその発動条件など、事業継続の取組み方を記述し、変更管理方法を明確にし、それぞれの管理者を置く、などを狙いとする。

「14.1.5 事業継続計画の試験、維持及び再評価」は、図 2-1. の "段階 5" 及び "段階 6" に対応し、最新で効果的な事業継続計画を確実にするために、計画の各要素の各種テスト・更新を実施することを狙いとする。

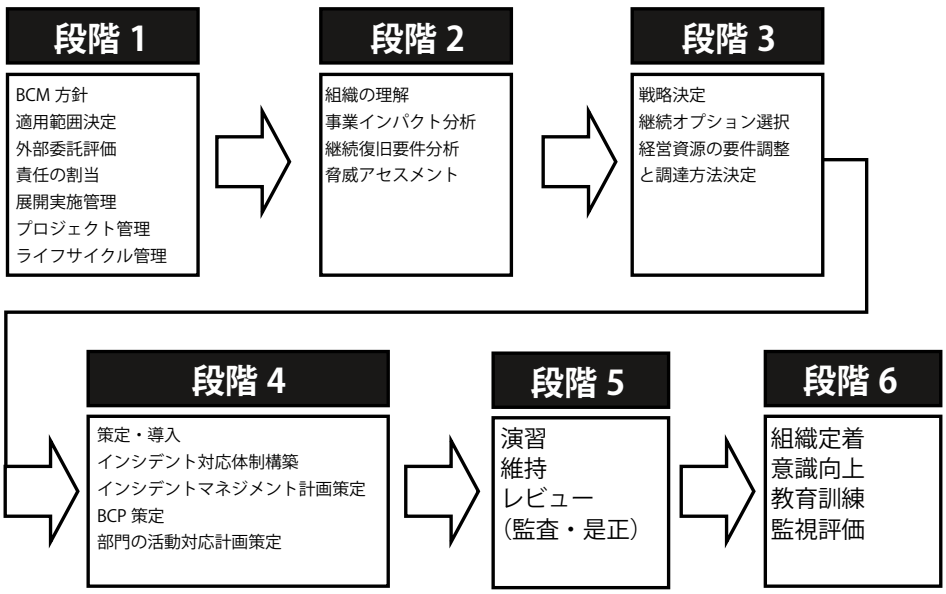

図 2-1. 事業継続実践アプローチの 6 段階

2-2. ISMS の具体的な事業継続管理策例

情報システムに関して、ISMS 認証取得をした組織に見られる具体的な管理策例を「表 2-1. 企業における具体的な ISMS の管理策例」に示す。ここでは参考として経理・人事・総務などの本社機能の基幹業務、非 24 時間対応ヘルプデスク業務、24 時間対応の IT サービス提供業務の 3 つの事例をあげる。ISMS における事業継続管理の実際の具体策として参考になる。

2-3. ISMS 事業継続管理における企業の現状

事業継続管理に関して ISMS で要求されている具体的な内容と実際の企業事例を紹介してきたが、現実にはその取り組みはなかなかうまくいっていない例が多い。その現状と原因は以下にあると言える。

(1) ISMS 事業継続管理の現状

ISMS 認証取得をした組織の事業継続管理には以下のような事例が散見され、現実の企業では必ずしも実効的かつ有効な事業継続管理になっていない。

①特定の原因事象にだけ対応

地震を中心とした災害対策の指針に沿って、震災だけに対応した事業継続管理を行っているケースである。これら指針は大地震発生時の影響による業務の中断をモデルとしているので、組織が業務中断の原因を想定するときに、地震に重きを置いてそれ以外の中断原因の想定がおろそかになってしまう恐れがある。これは、今回の大震災で露見したように、地震は考慮されていたが津波は考慮されていなかったなどの不備につながる。

②復旧に必要なリソースの使用可能性を未考慮

業務中断を引き起した事象によって、業務継続のための一連の復旧活動に必要なリソースまでも使用できなくなり、事業継続計画が手順どおりに実行できないケースである。今回の大震災では、通信手段がすべて使用不可になり被害状況さえ正確に把握できない、人的資源そのものが確保できない、生存のための物資さえ確保が困難、移動・運搬手段がなく活動拠点に行けない、情報システムだけでなく文書・データも全て喪失した等の例が発生した。

表 2-1　企業における具体的な ISMS の管理策例

適用業務	本社基幹業務	ヘルプデスク業務	ＩＴサービス提供業務
A.14.1.1 事業継続管理の組込み	経理 , 人事 , 総務などの本社の基幹業務	非 24 時間対応ヘルプデスク業務	24 時間対応ＩＴサービス提供業務
A.14.1.2 事業継続及びリスクアセスメント	基幹システムサーバとクライアントで基幹業務を遂行 ①サーバ一時障害→修理後再立ち上げ ②恒久障害→代替サーバで再立ち上げ ③本社一時的使用 / 出勤不可→回復待ち ④長時間使用 / 出勤不可→別拠点で復旧し , 業務開始	電話 ,FAX, e メール ,CTI でインシデント /FAQ 知識データベース , 製品マニュアルを使用して問合せ対応 ①個々の連絡手段の不通→代替手段 ② CTI, DB が使用不可→人手対応 ③拠点使用不可→別拠点へ片寄せ ④要員出勤不可→別拠点へ片寄せ	SLA を提示した SaaS サービスの提供 ①サーバユティリティ→ iDC に設置 ②免振建物 , 電源 / ネットワーク多系 , 自家発電 , など可用性の高い iDC を選択 ③システムを多重化し切り替え可 ④　同左③　⑤　同左④
A.14.1.3 事業継続計画の策定及び実施	①一時的中断か恒久障害中断かを判断 ②猶予できない業務の暫定対応手順 ③サーバ障害時バックアップから復旧 ④本社使用不可時は , 別拠点で基幹システムを復旧 ⑤本社使用 / 出勤不可時は別拠点で代替	①連絡手段の代替確保手順 ②使用不可情報の手作業対応手順 ③平常時 2 拠点で縦割り並行運用 ④別拠点切り替え手順 ⑤両拠点不可時の電話と人手の対応手順	①ネットワーク ,iDC 稼動状況 , 運用オフィス / 機器使用可否を判断して対応決定 ②同左①　③同左②　④同左④ ⑤同左⑤ ⑥利用者への情報伝達手順
A.14.1.4 事業継続計画策定の枠組み	①基幹サーバを日次バックアップ ②バックアップ内容を日次別拠点に転送 ③本社・別拠点に予備サーバ /PC 確保 ④猶予できない業務の暫定対応時基準 ⑤安否確認システム ⑥飲食料等備蓄 ⑦バックアップから復旧できない場合の対応策	①固定電話以外に携帯電話番号を通知 ②毎日終了時仕掛案件をリスト出力 ③別拠点と DB 同期化 ④バックアップからの DB 復元 ⑤同左⑤	①同左① ②利用者へ定期的なデータアーカイブ推奨 ③免責条項　iDC の主要機能停止 / 広域ネットワーク障害 ④同左④　　⑤同左⑤ ⑥事業が継続できない場合の対応策
A.14.1.5 事業継続計画の試験 , 維持及び再評価	①安否確認テスト ②避難訓練 , 飲食料等試用テスト ③バックアップからの復元テスト ④別拠点でのシステム復元テスト ⑤別拠点への出勤テスト	①同左①　②同左②　③同左③ ④人手対応テスト ⑤別拠点への切り替えテスト	①同左①　②同左②　③同左③ ④同左④　⑤同左⑤ ⑥利用者へ情報伝達テスト ⑦営業所へ運用チーム移動・出勤テスト ⑧利用者アーカイブからのデータ再登録

③形ばかりの事業継続管理

情報システムに関する事業継続計画としては、システム停止時の対応手順、バックアップからの復旧、災害時の避難訓練だけの事業継続計画を構築し、他方事業継続計画の試験としては避難訓練だけしか実施されていないというケースである。このため今回の大震災では、階下へ避難したことによる津波被害への遭遇、地下室や1階に設置の防災対策品の浸水や流失、サーバと同じオフィスに保管していたバックアップの両方が喪失などの事例が発生した。

④複数規定の並存

緊急事態管理規定、防災管理規定、パンデミック管理規定など様々な計画、規定が個別に策定されており、それに加えISMS構築に際してシステム停止時の対応手順とバックアップからの復旧手順を事業継続管理として策定しており、組織の事業継続計画としては整合性のない複数の規定が並存するケースである。縦割組織の弊害とも言えるが、この場合、全社員への周知、訓練、変更の反映などがばらばらに独立して行われ、マネジメントシステムの維持と非常事態時の活動の実効性と有効性に問題が出る可能性が高い。

(2) 有効でない事業継続管理が構築される原因

原因として以下のことが考えられる。

①「情報システムに関する事業継続管理」だけの構築

ISMS管理策「14.1.1 事業継続管理手続への情報セキュリティの組込み」の意味するところは、「情報システムに関する事業継続管理」だけを構築することではない。つまり「組織の事業継続管理」へ“情報セキュリティ”を組み込むことを意図しているのである。

② ISMS管理策14.1.1 〜 14.1.5だけに沿って事業継続管理を構築することの難しさ

ISMSに沿って忠実に検討した場合でも、各々の管理策について以下の課題・問題点が出ると想定される。これらに対して適切な対応ができるノウハウをほとんどの組織が未だ有していない。

・事業継続の対象とする情報システムの選定
・洗い出しの範囲（業務プロセス、資産・資源、業務中断要因、発生確率、影響先等）
・インシデントの報告ルート、判断する手順、体制などの構築方法
・テストの実施の程度（程度、範囲、参加者、頻度等）

③事業継続管理に精通した知識・経験を持つ人材の少なさ [7]

国内のISMS認証登録事業者が4209組織に対してBCMS認証登録事業者が39組織しかなく、またJRCA[5]のISMS審査員登録者が約2000人に対してIRCA のBCMS審査員登録者は39人である。事業継続管理に精通した知識・経験を持つ専門家は非常に少なく、ISMS構築事業者が事業継続管理について知識・経験が豊かな者の支援を受けることが難しい現状といえる。(いずれも2013年2月時点)

第三章　情報セキュリティの観点からの可用性と事業継続管理に関する考察

3-1. ISMSにおける可用性と事業継続管理の関係

はじめにISMSで示されている133の管理策のうち、可用性実現に関連するものを抽出してみた。まず最も多いのがリスクを下げる予防的な対策である。「A5方針」から「A12情報システム」まで全般にちらばっている。次にインシデントを発見する管理策と発生したインシデントの影響を極小化する管理策である。「A13 インシデント」を中心に「A6組織」、「A9物理/環境」に存在する。「A14事業継続管理」は、情報システムの可用性を維持するための予防が期待通りにできなかった場合の復旧計画であり、事後対処の対策である。可用性に関係するISMSの詳細管理策を概念的に表すと「図3-1.ISMS詳細管理策における事業継続管理と可用性の関係」のようになる。

ISMSは本質的にはリスクアセスメントによる予防活動が主体である。仮に予防できなかった場合には早期の事後処置や影響の局所化などの対策も、セキュリティ喪失の影響を低減させるための重要な管理策となる。

例えば、「機密性」では紛失・盗難が防止できなくても、暗号化でデータが参照されないようにする、携帯電話のデータをリモートで消去する、紛失した通門カードのIDで入門できないように設定変更するなどの管理策がある。「完全性」ではデータ誤りを防止できなくても、表の縦と横の合計のチェックによる計算誤りの検出、データ入力についてベリファイ入力での検証、チェックSUMによるデータ脱落や改ざんの検出などの管理策がある。「可用性」では機器の停止を防止で

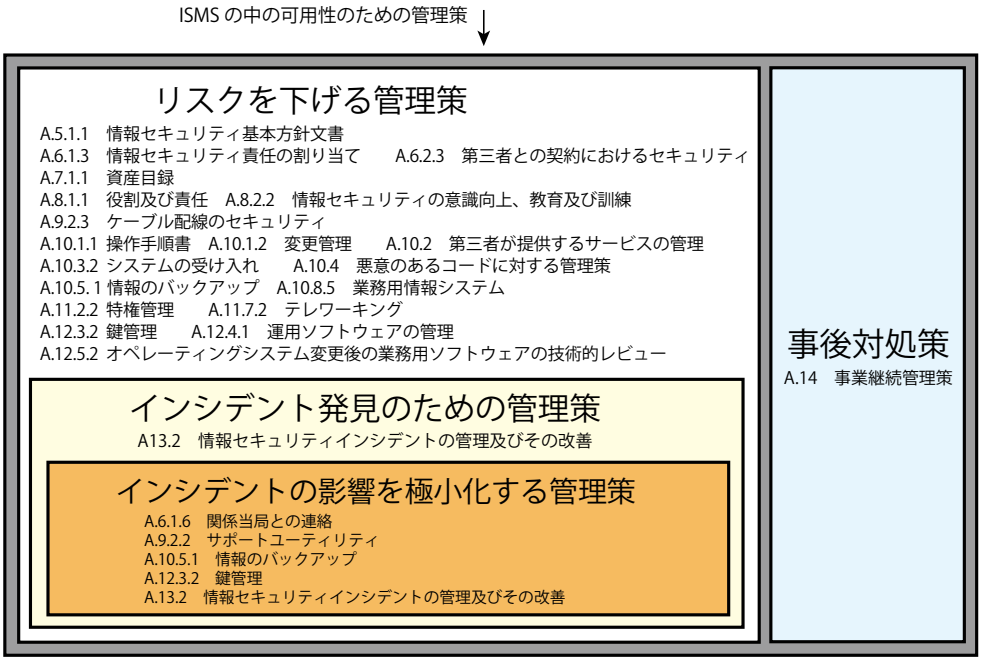

図 3-1　ISMS 詳細管理策における事業継続管理と可用性の関係

きなくても、迅速な修復や切り替えによる停止の時間短縮、バックアップ設備あるいは代替処置で業務への影響低減、一定期間での修理や復旧で業務再開することによる混乱拡大防止などがある。

この「可用性」に対する“一定期間での修理や復旧で業務再開することによる混乱拡大防止”という対策について、検討し、計画し、導入し、試験し、継続的な改善を行うことが、情報セキュリティにおける事業継続管理なのである。

3-2. 可用性と事業継続管理が重視されない理由

2-3 節で ISMS 事業継続管理における企業の現状と原因を述べた。そこで明らかにしたように、現状では情報セキュリティの可用性と事業継続管理の重要性が十分に認識されているとは言い難い。その理由として次の 3 点が考えられる。

(1) 可用性と事業継続に対する危機意識の欠如

①日本の安全神話文化

欧米文化では、戦争、テロ、暴動、銃犯罪、強奪、企業買収、役員や技術者の引き抜き、ストライキなどの多種多様なリスクが想定され、それらのリスクを前提としたトップマネジメントによるリスクマネジメントが当たり前に行われている。それに比べると、日本では、多くの組織が想定するのは大地震と火災という非常に限られたリスクである。そのため、事業中断に対する事業継続の計画も、単に地震や火災時の避難訓練程度で終わっているケースが多くみられる。

②高信頼システム利用による安心感の蔓延

日本の銀行 ATM システム、鉄道運行システムを始めとして、我が国の経済社会を支える基盤としての情報システムは高度化・高信頼化され、システム停止もほとんど発生しない。そのため、サービスというのは何時でもすぐに期待通りに利用できるという感覚が利用者の間に蔓延している。

③サプライチェーン高度化の落とし穴に対する認識不足

企業においては経営の効率化を目指し、在庫を持たない、外注化、コスト低減のための調達先絞込みなどの施策が高度に進んできた。その結果、一つの企業の生産・サービスが停止した場合、連鎖的に多くの企業にその影響が伝播することになった。今回の大震災でペットボトルのふたの生産が止まり、日本中のペットボトル飲料の出荷が滞ったことは典型的な事例である。

(2) 情報セキュリティ推進における機密性重視の傾向 [8]

①一般的理解

国語辞書で「情報セキュリティ」の意味をみると“情報”の“安全”とある。2005 年 4 月に施行された「個人情報の保護に関する法律」からの要求及びそれらの発端になった個人情報漏えいの事件・事故の影響が強いせいか、我が国においては情報セキュリティとは情報の「機密性」を維持することと理解する人が多いと考えられる。

②企業の情報セキュリティ方針

昨今、営業秘密の侵害、産業スパイ、個人情報漏えいによる損害賠償など、企業の機密情報漏えいによる被害が顕著である。そこで多くの組織は情報セキュリティ基本方針の中で、情報の漏えいを起こさないための予防策に真剣に取り組んでいることを謳っている。実際、多くの組織の基本方針を参照してみると機密性を重視していることがわかる。以下の順に多かった。

・情報セキュリティ全般（または機密性、完全性、可用性のすべて）としているもの
・不正アクセスや漏えい、改ざんの防止を特に挙げているもの
・事業継続を特に挙げているもの

(3) ISMS では事業継続管理はわき道的存在

ISMS 規格上からは妥当な理由があれば該当する管理策の適用を除外してもよいことになっている。ISMS 管理策 14.1.1 〜 14.1.5 の事業継続管理については適用を除外しても組織の社会的責任を果せるのであれば、JIS Q 27001 規格に適合していることになる。また、事業継続管理は情報システムの可用性を維持するための予防が期待通りにできなかった場合の後始末的な対策という位置づけである。事業継続に対応するリスクは“受容”し、リスクが現実なものになったときに危機管理の事案として対応すればよいとして、情報セキュリティの取り組みの外に追いやることもありうる。

3-3. 事業継続管理（BCM）と可用性評価

機密性の後ろに隠れあまり注目されなかった可用性ではあるが、本節では可用性と BCM について考察する。特に BCM を考える場合の資産の可用性評価の考え方と評価する資産の範囲を示す。本節で使用する資産は ISMS ユーザーズガイド [18] による定義に従うもので、情報に関連するハード、ネットワーク、ソフト、そして人を含む広義の意味で使用する。

(1) 事業継続のための資産の可用性評価の考え方

着眼点をどこに置くかによって、次の 3 つの考え方がある。一つ目は個々の資産に着目するもので、個々の資産の可用性を脅かす脅威に対してぜい弱性が存在するかどうかを評価し、この資産の可用性が喪失した場合の影響を想定してリスクを算出する。この評価は一般にコンポーネント [7] の可用性を評価する方法で行う。資産の可用性喪失時の影響の想定にあたっては、この資産の停止時の他のコンポーネントおよび業務システムへの影響を考える。業務への影響を考慮して、当該資産の可用性喪失の低減のための対策として、予防保守、冗長化、迅速な修復などのリスク低減策を講じる。この考え方では、影響があると判断されれば、どの資産も一律に重要と評価されがちである。

二つ目は、資産が提供するサービスの視点から評価するもので、このサービスが停止・喪失した場合の顧客・利害関係者への影響を想定してリスクを算出する。この考え方では、サービスを受ける末端の顧客までたどるので、優先順位が高い重要な事業を支えるプロセスへの影響を評価することができる。

三つ目が本研究の主題の一つである事業継続という視点で評価する考え方である。事業継続の観点から、事業を支える情報システムを構築する資産の可用性を評価する場合、資産台帳に登録された全ての資産を同列に評価することはしない。まず、重要な事業を特定し、その事業の重要なプロセスを支える情報システムを洗い出す。そして、その情報システムを構成する資産を特定して、その資産毎に可用性を喪失する恐れがある装置の故障、人による誤り、盗難、火災、自然災害、テロ行為などの脅威とそれに対するぜい弱性を評価する。このぜい弱性を低減できる対策があれば採用する。その上で重要な事業を支える情報システムの可用性を喪失してしまうことの発生確率及び影響を検討する。重要な事業を支える情報システムの可用性の喪失に対しては、復旧のシナリオを検討し、復旧方法を決定し、事業継続計画を策定する。

(2) 事業継続のために評価する資産の範囲

事業継続のために可用性を評価する資産の範囲としては、重要な事業の重要なプロセスを支える情報システムを構成する資産だけでなく、事業継続計画の緊急対策や復旧の活動に使用する資産も含まれる。特に、後者については情報システムに

関する資産に限らないことに注意が必要である。

稼働中の情報システムの可用性の評価対象は、情報システムを構成するハード・ソフト、稼動を支える電源等のユーティリティ、および運用を支える人員などである。しかし、一度これらが被災などで使用できなくなった場合、代替機器のベンダからの調達、代替拠点への機器の搬入と必要な人員の移動など情報システムの構成要素以外の資産（人やサービスなどの資源）が必要になる。事業継続計画の緊急対策や復旧の活動が計画通りに実行できるためには、これらの資産についても、可用性を維持するためのリスク低減策の検討、可用性を喪失した場合の代替策の検討をしておく必要がある。

第四章　情報セキュリティにおける可用性実現のための方策

4-1. 情報セキュリティにおける可用性の位置づけと特徴

JIS（JIS Q27002:2006）では、“情報セキュリティとは情報の機密性、完全性及び可用性を維持すること”とある。しかし、今までのところ現実の企業活動の中では、特に機密性を中心に情報資産を守ってきた例が多い。例えば、ある企業の現実の情報セキュリティ対策のうち可用性に関する管理策の割合は全体の凡そ 1 割である。その実態は、ISMS に 133 個ある管理策のうち可用性に係るものは 22 個（17%）だけであることが大きく起因しているとも思われる。

ここで情報セキュリティにおける可用性の位置づけについて再確認をしたい。可用性を考える場合、情報資産そのものだけでなく、情報資産の存在する建物、利用する人や組織、情報システムなど周りの資産・コンポーネントの可用性を維持しなければならない。そうなると個々の情報資産の可用性の維持という切り口に加え、総務部門、人事部門、購買部門、法務部門、情報システム部門など企業内の全部門における企業活動を視野に入れて広範囲にわたる多面的、重層的な取り組みが必要になる（「表 4-1. 組織と可用性の関係」）。情報セキュリティ面から見ると可用性の管理策は数少ないが、企業全体で見れば可用性に関して実施されている管理策はかなりの数に上る。

JIS（JIS Q 13335-1:2006）では、可用性とは「認可されたエンティティが要求した時に、アクセス及び使用が可能である特性」とある。要求される情報資産の具体例には、事業・業務に関する計画データ、日々の生産・販売のためのデータなど現場の日常業務に直結するものが多く、これらは企業内部の特性の異なる複数の業務部門にまたがって広範囲に分布している。また取引先である原料や部品の供給会社および販売会社などの顧客によって保有されるデータもあり、これらも数多くの企業に広範囲に分布している。他方、情報資産を要求する側もまた、広範囲に分布する複数の業務部門であり外部企業である。このように今日の経済社会では、特性の異なる数多くの部門と企業が情報資産を要求する側と要求される側となり、これらが網の目状に連結し合って複雑なシステムを構成していることが、可用性の実現と維持を困難にしている本質的な理由である。この問題を解決するための一つの方策として、情報通信技術を駆使した情報システムの構築・運用がある。

可用性の実現・維持のためには、例えば情報システム面では、二重化、フェイルセーフ、フェイ

表 4-1　組織と可用性の関係

部署	切り口	可用性の検討要素
人事部門	人	人の稼働性、供給 （帰宅困難、出社困難、在宅勤務、グローバル性、時差対応）
総務部門	建物、設備	建物の利用、機器設備の利用
法務部門	契約	他社との取引契約のＳＬＡ等
購買部門	ＳＣＭ	取引先からの部品供給など
情報システム部門	情報システム	情報システムの可用性
全部門	情報資産	資産・コンポーネントの可用性
全社	事業・サービス	事業・業務・サービスなどの提供

ルソフトなどの冗長化手法に関する考え方と多様な技術を導入する必要がある。組織の面でも、BCM、教育訓練、代替手段の準備など多方面の対策が必要になる。

今日の経済社会では可用性の実現・維持のために考慮しなければならない対象は複雑なシステムであるため、情報や人・モノの流れの全体像が捉えにくいという意味で、機密性と完全性に比べて抽象的かつ複雑な概念であり、直感的にわかりづらいものである。(「表 4-2. 情報セキュリティの中の可用性の位置づけ」)

以上のように可用性については IT 面も含め多面的、重層的かつ広域性の対応をしていかねばならないことがわかる。IT 面での対処方法も様々にあり、企業の中では情報セキュリティというよりは情報システムの可用性確保として実践されることが多い。それら可用性の特徴についてまとめると以下のようになる。

①抽象性

上記のように、可用性の概念は機密性、完全性に比べて抽象的であり一般の人にはわかりづらい。

②広範囲性（物理的な多様性）

可用性を実現するためには、地理的、物理的、時間的に広範囲な視点と取り組みが必要となる。

例：建物全体、敷地全体、地域分散、
　　広域対応

③人と組織の多様性（論理的な多様性）

可用性実現のためには情報セキュリティの取り組みにとどまらず、組織内の特性の異なる多くの部門間および組織外部とのあらゆる活動との接点に焦点を合わせた取り組みが必要になる。

例：事業サービス、事業継続管理、拠点展開
　人の面：人事部門
　建物・施設面：総務部門
　契約の面：法務部門
　情報システム：情報システム部門
　取引先・関係先：購買部門
　市場・顧客面：営業部門

④対象の多面性

情報資産の可用性のみに限らず、情報資産を取り巻く情報システム、建物などの多くのシ

表 4-2　情報セキュリティの中の可用性の位置づけ

評価項目	可用性	機密性	完全性
性質の説明	使いたいときに使える ［**抽象的**］	秘密管理 ［**わかりやすい**］	正確で完全 ［**シンプル**］
直接的な脅威	・紛失、破壊、改ざん ・環境等が使えない、使える人がいない	・漏えい、紛失、搾取 ・故意、ミス	・破壊、改ざん ・故意、ミス、故障
実現に向けての考え方	①事業、業務、人、職場、組織、情報システム、建物等環境（地理的、気象的、物理的）など広範囲に多面的、重層的に検討する ②二重化、フェイルセーフ、フェイルソフトなどの手法を導入 ③信頼性、保守性と合わせてシステム全体の信頼性を総合的に評価する（RAS）基準となる。即ち、MTBF、MTTR から稼働率として評価する。 ［**広域性・多面的・重層的で複雑**］	①情報資産への適切なアクセス管理を実施 ②組織全体の統一的な統制で実現 ［**統一的**］	①改ざん検出、改ざん防止の（技術）手法の検討導入 ②情報資産ごとに対処を実施 ［**局所的**］
具体的な情報資産例	事業計画、危機管理マニュアル、工場の生産計画データ、作業マシン動作データ、日々の取引データ、顧客サービスデータ　など ［**企業の日々の活動に密接**］	営業秘密、顧客情報、企業戦略・事業計画、技術開発情報など ［**企業価値の源泉**］	財産情報、経営情報、金銭情報、個人情報など ［**財産的**］
実現のための具体的な手法	①二重化（施設、設備、情報システム、ネットワーク、ユーティリティ）、要員訓練・シミュレーション、事業継続管理、代替手段の準備、危機管理 ② IT 面の可用性確保の具体的手法 ③サプライチェーン・マネジメントの見直し ［**事後的対策が主体**］	①アクセス制御（個人認証、機器認証） ②暗号化	①電子署名 ②バックアップ ③改ざんシール ④チェック SUM ⑤ WRITE ONCE

ステムを対象として多面的な取り組みが必要となる。

例：情報資産＜情報システム＜建物＜環境・設備

4-2. 情報セキュリティの可用性を実現するための方策

どのようにすればこのような特徴を持つ可用性を実現することができるのか。第一は、マネジメントの観点からの方策がある。以前から企業内に情報セキュリティを担当する人材が不足しているということがよく言われている。本論文の第二章でも“事業継続管理に精通した知識・経験を持つ人材の少なさ”という内容を指摘した。そのことは、言い換えれば、幅広い範囲のことを一人でできるスーパーマンを無いものねだりしているに等しい。事業方針、災害対応、拠点展開、施設･設備、業務サービス、顧客・市場などを一人で幅広く担当できる人材などもともと存在しない。加えて情報システムなどIT技術にも長けた人材など探してもいるはずがない。情報セキュリティ人材とはどうあるべきか。その回答はこれら幅広い分野を個々に任せられる人材群あるいは部門をコントロールするということである。情報セキュリティの可用性を実現するために大事なことは、現場中心のセキュリティ活動に加えて、企業全体を俯瞰する立場の人が広い視野で個々の分野をコントロールすることである。経営・管理層のキーマンが現場における可用性の個々の要素の専門家をコントロールすることが基本である。

第二に、事業継続管理という観点からの方策である。ISMSでは情報資産の機密性、完全性、可用性を維持するために多様な管理策を要求している。その中で可用性の管理策に着目すれば、事業継続管理を中心としたものがほとんどである。企業の最大の使命は事業の継続ということであると考えれば、組織全体の事業継続管理の枠組みの中に情報資産の可用性維持の取り組みを位置づけるのも納得できる。情報セキュリティの可用性とはそのまま事業継続管理の枠組みの中に取り込まれる性格のものであろう。ここで特に重要なことは、「情報資産そのものの可用性」とそれを「利用す

表4-3　可用性を取り扱う枠組みの比較

◎：主目的　　○：補足的目的　　△：参考的

枠組み	ISMS（ISO27001）	システム監査（システム管理基準）	ITSMS（ISO20000）	BCMS（BS25999）	COBIT
目的	情報資産の防御	情報システムの健全性確保	ITサービスの継続性維持	事業継続管理	ITガバナンス
機密性	◎	△	△ （情報セキュリティ管理など）	－	○
完全性	○	◎	△	－	○
可用性	○ ①そのほとんどは事業継続管理としての可用性 ②情報セキュリティの側面からの事業継続管理の取り組み ③可用性該当部分 詳細管理策 14.1 事業継続管理における情報セキュリティの側面 他	○ （RASIS面から） ①運用業務を中心にシステムの可用性に着目 ②可用性該当部分 Ⅰ. 情報戦略 5. 事業継続計画 Ⅳ. 運用業務 2. 運用管理 4. データ管理 6. ソフトウェア管理 7. ハードウェア管理 8. ネットワーク管理 9. 構成管理 10. 建物・関連設備管理 Ⅴ. 保守業務 Ⅵ. 共通業務 7. 災害対策	◎ （サービス継続性及び可用性管理など） ①意味合い ITサービスの運用管理の枠組み （全体がITサービスの可用性に関するもの） ②可用性該当部分 IT-BCMとしての事業継続管理	◎ 事業継続そのものの枠組み ①可用性該当部分 ・危機管理 ・防災管理	○ （ビジネス要件として） ①ビジネス要件としての可用性を扱っている （サービス提供とサポートなど）

るための環境の可用性」の二つの観点である。

第三は、可用性の維持に取り組むための既存の枠組みの利用である。市場には様々な取り組みのための枠組みが存在する。システム監査では、システム管理基準で情報システムの情報戦略として事業継続計画を取り上げている。また運用業務を中心に可用性維持の評価視点を有している。IT-BCP[8] としての ITSMS[9] は、そのもの自身が IT サービスの可用性維持の取り組みである。BCMS は IT に限らず企業の活動における事業継続の取り組みを広く取り扱っている。COBIT はビジネス上のサービス提供とサポートに関しての可用性などを扱っている。どちらかといえば機密性に重心がある ISMS で可用性の施策を実践するか、あるいは可用性そのものを中心におく枠組みに沿って取り組むかは、企業の事業内容や構造、業務の特性に依存するところが大きい。(「表 4-3. 可用性を取り扱う枠組みの比較」)

4-3. 結論

本論文で取り上げた「2-3. 有効でない事業継続管理が構築される原因」に対する対処も含めて企業における可用性への取り組みのポイントをまとめると次のようになる。(1) は 2-3 ①と 2-3 ③に、(2) は全てに、(3) は 2-3 ②に対応するものである。

(1) 可用性を維持する取り組みは、企業全体を俯瞰できる立場の人材による取りまとめが必要

全社的事業継続管理の枠組みとリンクして情報セキュリティ面の事業継続管理を位置づける。可用性の維持は、全体を統括する人のコントロール下で、組織ごとに分担して推進する。建物管理、情報システム、全社的な統制や就業規則などそれぞれ担当専門部署との連携が重要である。

(2) 可用性に対する取り組みは、組織の統制の下、長期的な目標に沿って進めることが肝要

可用性実現のためには、バックアップ設備や施設、他社とのアライアンスやサプライチェーン・マネジメントの見直し、要員の訓練・シミュレーションなども必要になり、一企業内に留まらない場合が多い。時間的、コスト的にも一挙に実現というわけにもいかない面がある。お金も時間も人手もかかるため長期的な目標を持って、地道に積み上げていく努力が大切である。

(3) 情報システム面に関わる要素が大きいので、システム監査的な見方も重要

情報システムの有効性、効率性などとも合わせて全体統括的な施策を検討することが必要である。情報セキュリティ監査が情報システム及び情報資産を対象とする一方、システム監査は情報システムを対象として広くその健全性の確保を目的とするものである。こういったシステム監査的な見方で可用性を見直すことも有効である。

おわりに

本論文では、東日本大震災によってその重要性が再認識された事業継続の視点から、組織における情報セキュリティの可用性の問題を取り上げ、事業継続管理と可用性の関係を考察するとともに、情報セキュリティにおける可用性の位置づけと特徴を明らかにし、可用性を実現するための考え方と具体的な方策を提言した。

情報セキュリティの可用性に関して個別具体的には、バックアップやリスクアセスメントの問題など、今後引き続き議論し解決すべき問題が残されている。

今後も引き続き企業や社会に役立つ情報セキュリティの深耕に努めていきたい。

参考文献

[1] 株式会社野村総合研究所「東日本大震災の影響と BCP（事業継続計画）に関するアンケート調査結果」2011 年 6 月 30 日

[2] ㈱ NTT データ経営研究所「東日本大震災を受けた企業の事業継続にかかる意識調査」2011 年 7 月 19 日

[3] 経済産業省「東日本大震災後の産業実態緊急調査②」2011 年 8 月

[4] 池島 賢治 一般社団法人日本ガス協会常務理事「東日本大震災を教訓として『エネルギー』考える 」平成 23 年 12 月 21 日公益財団法人 JR 西日本あんしん社会財団主催「安全セミナー」発表資料

[5] BS 25999-2:2007 規格「事業継続マネジメント － 第 2 部：仕様」(Business continuity management Part 2: Specification)

[6] BCI Japan Alliance「事業継続マネジメント (BCM) 実践ガイドライン」2008.11

[7] 一般財団法人日本情報経済社会推進協会

（JIPDEC）2012.8.9
http://www.isms.jipdec.or.jp/isms.html 、http://www.isms.jipdec.or.jp/bcms.html
[8] 頼永忍、原田要之助「組織の事業継続性向上に資する情報セキュリティマネジメント手法の提案」、日本セキュリティマネジメント学会第 26 回全国大会、2012.6.23
[9]「JIS Q 27001:2006 情報セキュリティマネジメントシステム　要求事項」（日本規格協会）2006.5.20
[10] 中尾康二、中野初美、平野芳行、吉田健一郎「ISO/IEC17799:2005 情報セキュリティマネジメントシステム　実践のための規範（日本規格協会）2007.3.8
[11]「情報技術－セキュリティ技術－事業継続のための情報通信技術の準備態勢に関する指針 ISO/IEC 27031:2011」2011.3.1
[12] 内閣府防災担当「事業継続ガイドライン第二版」平成 21 年 11 月
[13] 経済産業省商務情報政策局「事業継続計画策定ガイドライン」2005 年 6 月
[14] 経済産業省「IT サービス継続ガイドライン」平成 20 年 9 月
[15] レジリエンス協議会「IT サービス業務継続ガイドライン」2011.3.18
[16] 田川義博「東日本大震災にみる情報セキュリティと企業行動」、原田要之助「東日本大震災に学ぶ事業継続計画と IT の在り方」（情報セキュリティ大学院大学情報セキュリティ総合科学第 3 号）2011 年 11 月
[17] 日本情報経済社会推進協会「BCMS ユーザーズガイド」-BS25999-2:2007 対応 2008.7.28
[18] 財団法人　日本情報処理開発協会「ISMS ユーザーズガイド –JIS Q 27001:2006（ISO/IEC27001:2005）対応 -」平成 20 年 1 月 31 日（第 2 刷）

脚　注

1：本論文にて“企業”とした個所は、様々な事業体や組織体を意味する
2：情報セキュリティマネジメントシステム（第三者認証のための規格は JIS Q 27001）
3：Business Continuity Plan: 事業継続計画
4：いずれも阪神淡路震災との比較
5：日本規格協会 マネジメントシステム審査員評価登録センター
6：The International Register of Certificated Auditors - 国際審査員登録機構
7：IT サービスにおけるサービスの構成要素を言う。サーバ、ソフトウェア、メモリ、運用手順書など。
8：IT 面からの事業継続計画の策定
9：IT Service Management System：サービス提供者が提供する IT サービスのマネジメントを効率的、効果的に運営管理するための仕組みのこと（第三者認証のための規格は、ISO20000）
10：Business Continuity Management System：組織の“事業継続能力”を“継続的に維持・改善するための経営手法”のこと（第三者認証のための規格は BS25999）
11：Control Objectives for Information and related Technology：米 ISACA（情報システムコントロール協会）が提唱している IT ガバナンスの成熟度を測るツール