O-001

情報システムにおける災害対策評価
Countermeasures-against-calamities Evaluation in IT Systems

山田 耕一†　　砂田英之†
Kouichi Yamada　　Hideyuki Sunada

1. まえがき

事業活動が情報システムに依存するようになり、企業における情報システムの災害対策が必要とされている。災害を想定した事業継続計画については、経済産業省より、「事業継続計画策定ガイドライン」が提示されており、BCM(Business Continuity Management)のフローが示されている。また、東日本大震災を契機に、既存の事業継続計画(BCP = Business Continuity Plan)を見直す動きもある。

しかし、従来の方式では、BCP 策定におけるリスク評価のためのシステムの定義や災害の定義に関する方法が示されておらず、個別の災害についてのリスク分析はできるものの、複数の災害について発生頻度も考慮したリスク分析を自動的に実施するといったことができていなかった。

本論文では、これらの課題に対し、リスク評価のためのシステムおよび災害の定義方法および評価方式を提案する。

2. 従来の BCP 策定

2.1 従来方式

事業継続計画(BCP)に関しては、経済産業省が策定ガイドラインを公開している**[1]**。

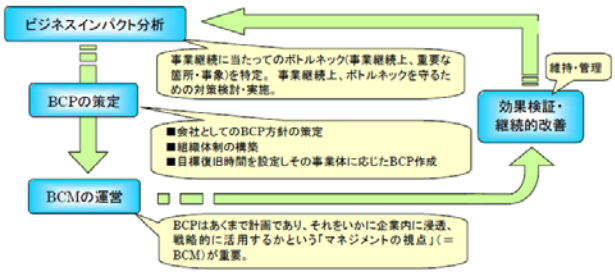

図 1. BCM のフロー（出展：経済産業省「事業継続計画策定ガイドライン」）

このガイドラインでは、ビジネスインパクト分析から BCP 策定までの流れとして、以下の通り規定している。

(1)ビジネスインパクト分析（優先順位付け、ボトルネック特定、目標復旧時間設定）
(2)リスク分析
(3)発動基準の明確化
(4)BCP 策定

また、内閣府の企業防災のページにて、事業継続ガイドラインが公開されている**[2]**。これでは、次の様にして BCP を策定する。

(1) 検討対象とする災害の特定
(2) 影響度の評価
(3) 重要業務が受ける被害の想定
(4) 重要な要素の抽出
(5) 事業継続計画の策定

リスク分析の技術に関しては、設備の耐震グレードをパラメータとして地震による施設の被害を算出する仕組みがある。このとき使用する指標は、地震 PML(地震による予想最大損失額：PML = Probable Maximum Loss)等がよく知られている。

2.2 問題点

従来の方式には、以下の問題がある。

・社会インフラの被害想定
内閣府のガイドラインでは、社会インフラの被害については、想定自体が容易ではないため、妥当と思われる前提を決めることとなっている。そのため、社会インフラ復旧率を最悪ケースで想定したり、逆に甘い見通しとなることがある。

・複数の災害
一般的な BCP 策定では、リスク評価のためのシステムの定義や災害の定義に関する方法が開示されておらず、個別の災害についてのリスク分析はできるものの、複数の災害について発生頻度も考慮したリスク分析を自動的に実施するといったことができていない。たとえば、本社に認証サーバ、営業所に業務サーバがある構成では、両方のサーバが動作しないと業務が出来ない。従来方式では、本社と営業所の個々の災害について分析は出来るが、両方を含んだリスク分析は出来ない。

・物理構成と論理業務の関係
物理的な構成と、論理的な業務とを結びつけて評価する方式がない。そのため、稼働率が最も低くなる物理リソースをボトルネックとして、業務の稼働率評価を行っている。しかし、各要素の依存関係を反映していないため、実態と合わない。

以上より、対策が有効なのか／適切なコストなのかを判断することが困難となり、無効な対策を取っていたり、必要以上に BCP への投資をすることがあった。

3. 災害対策評価方式

前述の問題を解決するため、インフラや物理的な機器構成の関係を示す「リソース定義」と、物理的な構成(災害から直接被害を受ける物)と、論理的な業務(停止することで損失が発生する物)の関連を示す「業務定義」を定義する。

†三菱電機株式会社 情報技術総合研究所
Information Technology R&D Center, Mitsubishi Electric Corporation

3.1 リソース定義

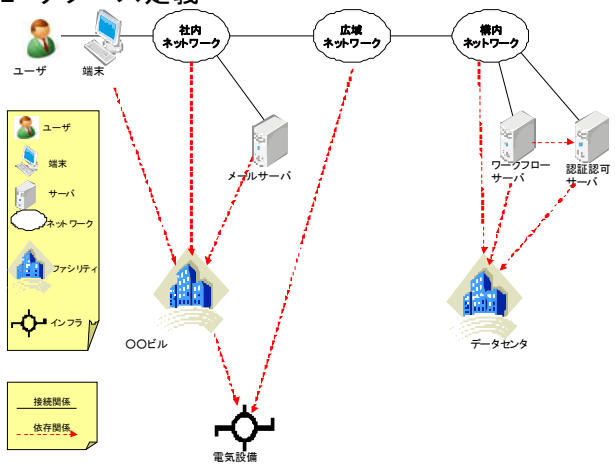

図 2　リソース定義例（データセンター活用型）

リソース定義では、情報システムを構成する要素を、ユーザ／端末／サーバ／ネットワーク／ファシリティ／インフラに分類したリソースを用いて、接続および依存関係を定義する。ユーザ／端末については、接続関係が変わらなければ、具体的なインスタンスの定義は実施せずに、1 つのまとまりとして定義する。その他のサーバ／ネットワーク／ファシリティ／インフラに関しては具体的な（グループ化したものでも可能）インスタンスを定義し、それぞれのリソースの接続関係および依存関係を定義する。

図 2はデータセンター活用型の社内情報システムをモデルとして定義した例である。本例における端末は社内のネットワークに接続するとともに、ユーザからの操作を受け付ける（接続として定義）。また、電気の供給など、ファシリティ（○○ビル）がないと動作不能であることから、依存関係としてファシリティとの関係を定義する。この例では、ワークフローサーバは、端末から広域ネットワークを介して接続する。ワークフローサーバ上のサービスが動作するには、認証認可サーバによる認証認可の結果がないと動作できないため、依存関係として認証認可サーバとの関係を定義する。データセンタのファシリティが自家発電装置を有している場合には、社会インフラの電力設備が稼働不能な状態に陥っても動作可能であるため、インフラとの依存関係は結ばない。なお、図には表現していないが、それぞれのリソースの属性として所在値の情報を設定する。また、データセンタのファシリティが免震構造になっている場合には、属性として免震構造の有無および地震の抑制率を定義する。

現状構成の他に評価したい災害対策の構成があれば、同様にリソース定義を行う。この例ではデータセンターを使ったリソース定義をしたが、データセンターを使わない構成や、センターを二拠点化した構成、ネットワークを二重化した構成などを評価する場合は、それぞれのリソース定義を行う。

3.2 業務定義

業務定義は、情報システムの提供する機能によって、どのような業務が成り立っているかを示す物である。

業務内容を情報システムの提供するサービスの視点で整理し、サービスの利用者（サービスの始点）およびサービスの提供側（サービスの終点）によって定義し、そのサービスを利用した業務による売り上げを定義する。サービスの始点となるユーザは、複数の業務を担当する場合があるため、物理的なユーザから、論理的なユーザへの関連を示して定義を行う。表 1にユーザの業務内容例を示す。

表 1　ユーザの業務内容

ユーザ(物理)	ユーザ(論理)	実施業務	売り上げ
佐藤一郎	ユーザ①	業務①	20 万円／日
高梨真莉	ユーザ①	業務①	10 万円／日
	ユーザ②	業務②	15 万円／日
田中太郎	ユーザ②	業務②	15 万円／日
橘里依	ユーザ①	業務①	10 万円／日
	ユーザ②	業務②	15 万円／日
吉沢志保	ユーザ②	業務②	30 万円／日
佐藤華子	ユーザ②	業務②	25 万円／日

表 1の例では、物理ユーザの高梨真莉さんは 1 日に 2 つの業務を実行する、2 つの論理ユーザに展開される。具体的には、業務①を実施し 10 万円／日を売り上げる論理ユーザ①と、業務②を実施し 15 万円／日を売り上げる論理ユーザ②とに展開できる。

一方、業務については始点と終点を定義する。始点はサービスを利用するユーザ、終点はサービスを提供するリソースである。たとえば業務①はワークフローを用いる業務、業務②はメールを利用する業務だとする。ワークフロー業務など、サービス停止時に紙による代替運用の方法がある場合には、代替方法の有無として有を定義し、その場合の業務効率のロス分（サービス稼働時に比べ 50%に低下など）を定義する。複数のサーバがあり、いずれかのサーバ上で動作するサービスが利用できれば業務が実行可能な場合には、終点として複数のリソースを定義する。

以上の結果から、業務定義の例を表 2に示す。

表 2　業務定義例

業務	始点	終点	売り上げ	代替の有無(効率低下率)
業務①	ユーザ①	ワークフローサーバ	40 万円/日	有(50%)
業務②	ユーザ②	メールサーバ	100 万円/日	無(−)

3.3 災害対策評価方式の概要

前記のように定義した、リソース定義と業務定義を用いた、具体的な評価方法について述べる。

本方式では、インパクト定義(後述)を使って個別の災害での被害を求め、リソース定義と業務定義によるリソースと業務の関係を使って複数の地点にまたがるシステムを用いた業務の稼働率を求める。これにより、他地点にまたがるシステムの被害の算出や、物理的な構成と、論理的な業務とを結びつけた評価を行うことが出来る。

リスク評価のためのシステムおよび災害の定義方法および評価方式の概要を図 3に示す。

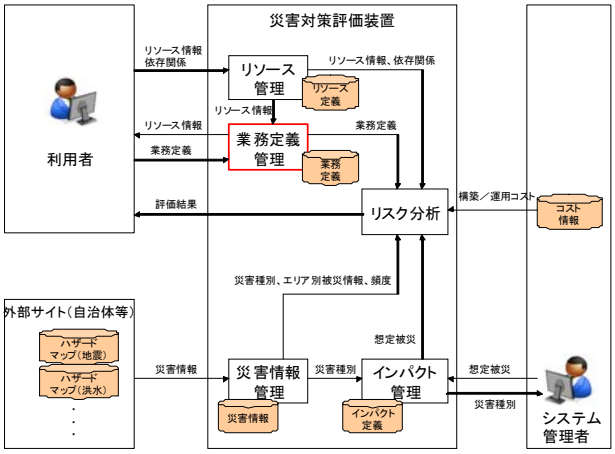

図 3　災害対策評価方式のブロック図

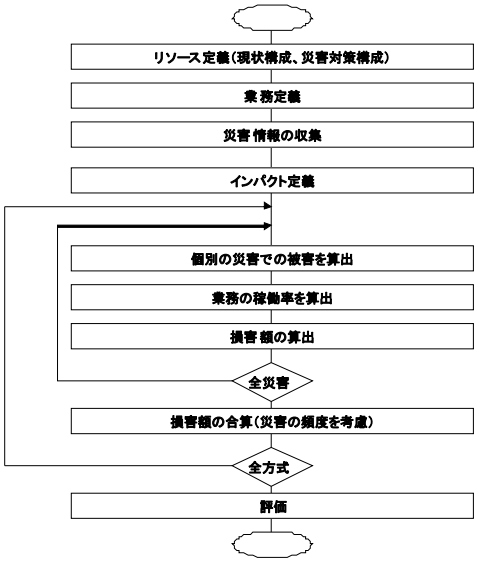

図 4. 災害対策評価の流れ

リソース管理は、情報システムをモデル定義する設定画面の提供や、ファイルの入力により、評価対象となる情報システムに関するリソース（ユーザ、サーバ、ネットワーク、ファシリティ、インフラ設備等）構成および依存関係を管理し、他の装置に対して提供する。

業務定義管理は、リソース管理から評価対象の情報システムを構成するリソース情報を取得し、利用者にリソース情報を開示する。（予めリソース情報が利用者にわかっている場合には、この手順は省略しても構わない）

提示されたリソース情報を用いて利用者が業務定義管理の提供する設定画面やファイルの入力により業務定義を行い、業務の実行に必要な業務の始点／終点のリソースおよび業務を実行した場合の売り上げ等の情報を管理し、他の装置に対して提供する。

災害情報管理は、自治体等で公開されるハザードマップの情報を収集・変換。または、変換後の情報のファイルによる入力によって災害情報を取得し、他の装置に対して提供する。

インパクト定義は、災害情報管理の管理する災害情報の種別（地震、津波など）および強度（震度５，震度６など）の一覧を取得し、災害の種別、強度が発生した場合のリソース種別に対する想定被害（稼働率）を統計情報などを参照に管理者が入力し、管理する。管理した情報は他装置に対して提供する。

リスク分析は、リソース定義、災害情報、インパクト定義から個々の災害が発生した場合の個別のリソースの非稼働率を算出し、業務定義の始点～終点の経路に対して評価を行い、業務停止率および被害額を算出する。

また、上記の被害額に対して災害の発生頻度を考慮したリスクを算出し、利用者に対して通知する。

3.4 災害対策評価方式の処理の流れ

処理の流れを図 4に示す。

災害対策の評価にあたり、ユーザがリソース管理の提供する設定機能を通じて、またはリソース定義ファイルの入力によって、現状の情報システムの構成を定義する。

3.4.1 災害情報の収集

評価対象とする災害の種類および設定方法を表 3のように予め決定しておき、ハザードマップなどの情報を収集する。

表 3　災害情報の収集定義

自然災害種類		対象	自動収集	公開サイト
地震		○	○	地震調査研究推進本部
津波		○	○	
気象災害	風水害	○	○	各自治体
	土砂災害	○	×	
	雪害	○	×	
	落雷	○	×	
噴火		○	×	
隕石		×		

※自動収集＝×の箇所は、管理者により直接、定義ファイルを編集するなどの方法で設定する。

例えば、地震調査研究推進本部では、「海溝型地震の長期評価」「活断層型地震の長期評価」が公開されており、地震の発生頻度や各地での災害の階級（震度）などの情報を取得することができる。

公開サイトから収集または管理者の定義した災害情報を、リソース定義で設定した所在値情報に対応した階級の情報に変換し、本システムに設定する(図 5)。

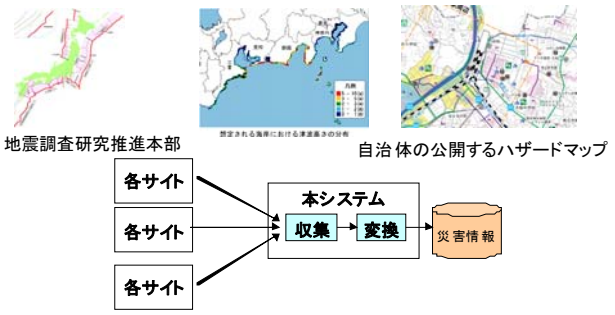

図 5. 災害情報収集

変換する場合には、所在値（例えば市町村の単位や、緯度経度のメッシュ分割などで定義）の領域に該当する災害階級の平均値、または最大値を設定するなどの方法がある。地震の場合の、変換後の災害情報の例を表 4に示す。

表 4　変換後の災害情報（所在値を都道府県単位とした場合）

地震名	発生確率 30 年以内	階級（震度）				
		東京	神奈川	千葉	埼玉	・・・
根室沖	40%	－	－	－	－	
三陸沖北部	90%	－	－	－	－	
宮城県沖	99%	－	－	－	－	
首都直下型	70%	6 弱	5	5	5	
東海地震	87%	3	4	3	3	
・　・　・						
△△地震	50%	7	6 強	5	5	

同様に他の災害についても、災害情報の収集および変換を実施する。災害情報を公開しているサイトがない場合には、管理者による直接の定義ファイルの編集などによって設定する。

3.4.2 インパクト定義

対象とした災害の種別、階級からリソース種類ごとに災害による停止割合および時間を設定する。地震災害の場合の例を表 5に示す。

表 5　地震災害時のインパクト定義例

リソース	震度 7		震度 6強		震度 6弱		・・・
	停止割合	停止時間	停止割合	停止時間	停止割合	停止時間	
ユーザ	60%	2 日	30%	2 日	15%	2 日	
端末	60%	1 日	30%	1 日	15%	1 日	
サーバ	30%	1 日	15%	1 日	7%	1 日	
ネットワーク	5%	1 日	3%	1 日	1%	1 日	
ファシリティ	2%	2 日	1%	2 日	0.5%	2 日	
インフラ	100%	1 日	50%	1 日	25%	1 日	

インパクト定義では、例えば、震度 7 の地震が発生すると「ユーザの 60%は怪我等により 2 日間の業務ができない状態となる」ということを定義する。停止割合や停止時間の値は過去の統計や、災害予測などを参考に設定する。機器に関しては、ベンダの公開する情報があれば、そちらを参考に設定する。対象とする災害の全てに対して、上記と同様の定義を実施する。

3.4.3 被害の算出

それぞれの定義が完了したら、リスク分析装置において個別の災害が発生した場合の被害（停止率）を算出し、停止率から被害額を算出する。

まず、データセンタ活用構成の評価（△△地震が発生した場合）のリソースの所在値および災害情報から、発生する階級を求める。次に免震構造の属性を考慮する。たとえば、データセンタに「免震構造＝有」の属性があることとし、「階級を 1 ランク下げて評価」の設定とする。

リソース定義(図 2)によると、データセンタに依存関係のあるリソースは

ワークフローサーバ
認証認可サーバ
構内ネットワーク

の 3 つである。データセンタそのものを含め、4 つのリソースに対して免震構造の属性を考慮し、階級を 1 ランク下げる。

表 6　△△地震発生時に各リソースが被る階級（免震属性考慮後）

リソース			階級
インスタンス	種別	所在値	
ユーザ	ユーザ	神奈川	6 強
端末	端末	神奈川	6 強
ワークフローサーバ	**サーバ**	**東京**	**6 強**
メールサーバ	サーバ	神奈川	6 強
認証認可サーバ	**サーバ**	**東京**	**6 強**
社内ネットワーク	ネットワーク	神奈川	6 強
広域ネットワーク	ネットワーク	神奈川	6 強
	ネットワーク	東京	7
構内ネットワーク	**ネットワーク**	**東京**	**6 強**
○○ビル	ファシリティ	神奈川	6 強
データセンタ	**ファシリティ**	**東京**	**6 強**
電気設備	インフラ	神奈川	6 強

元の災害情報の例では、△△地震に対し東京は階級 7 であったが、免震構造属性の適用により、データセンターと、

データセンターに依存関係があるリソースの階級は 6 強に下がっている。

次に、リソース種別、階級とインパクト定義の情報から単位時間あたりの停止率を算出する。例えば、ワークフローサーバは、「階級＝6 強」、「リソース＝サーバ」のため、それから求められる停止率はインパクト定義から「停止割合＝15%、停止時間＝1 日」となる。なお、停止率を求める期間は、インパクト定義で設定した最大停止時間が必要となる。

さらに、依存関係を考慮して、実質、利用可能な状態にあるのかを考慮した停止率を求める。例えばメールサーバの場合、依存関係にあるリソースの 1 日目の停止率は、インパクト定義(表 5)より

メールサーバ　15%（稼働率＝85%）
○○ビル　1%（稼働率＝99%)
電気設備　50%（稼働率＝50%）

となり、実質のメールサーバの停止率は

1 - 0.85×0.99×0.5 ＝ 0.58　(58%)

と算出できる。依存関係を反映した、実質の停止率の例を表 7に示す。

表 7　△△地震発生時の各リソースの停止率

リソース			停止率		
インスタンス	種別	階級	1 日目	2 日目	・・・
ユーザ	ユーザ	6 強	30%	30%	
端末	端末	6 強	65%	31%	
ワークフローサーバ	サーバ	**6 強**	28%	1%	
メールサーバ	サーバ	6 強	58%	1%	
認証認可サーバ	サーバ	**6 強**	16%	1%	
社内ネットワーク	ネットワーク	6 強	52%	1%	
広域ネットワーク	ネットワーク	6 強	52%	0%	
	ネットワーク	7	53%	0%	
構内ネットワーク	ネットワーク	**6 強**	4%	1%	
○○ビル	ファシリティ	6 強	51%	1%	
データセンタ	ファシリティ	**6 強**	1%	1%	
電気設備	インフラ	6 強	50%	0%	

次に業務を実行するためのパスを抽出し、業務の停止率の評価を行う。例えば業務①は、始点＝ユーザ、終点＝ワークフローサーバで、この間のパスを図 2のリソース定義の接続関係から求めると、

ユーザ→端末→社内ネットワーク→広域ネットワーク→構内ネットワーク→ワークフローサーバ

と接続していることが求められる。パス上の全てのリソースが稼働して業務が成り立つため、△△地震発生時の業務の停止率は個々のリソースの停止率から業務①の停止率は、

1 日目　98%
2 日目　53%
3 日目　0%

と求めることができる。

パスを抽出する際には、代替のルートがないかも考慮し、代替のルートを含めて稼働率を算出する。同様に全ての業務についての停止率を求め、売り上げ情報から表 8のように被害額を算出する。

表 8　△△地震が発生した場合の損失

業務	損失		
	1 日目	2 日目	・・・
業務①	39.2 万円	21.2 万円	
業務②	95 万円	53 万円	

業務①については、「代替手段＝有」と設定されているので、低下率を考慮して表 9のように求めることができる。

表 9　△△地震が発生した場合の損失（代替手段を考慮した場合）

業務	損失		
	1 日目	2 日目	・・・
業務①	19.6 万円	10.6 万円	
業務②	95 万円	53 万円	

以上より△△地震が発生した場合の損失額は、上記の損失を合計した 178.2 万円と求めることができる。同様に他の災害についての被害を算出する。

3.2.6 リスク評価

対象とする全ての災害に関する被害額が算出できたら、損失額と災害の発生頻度からリスクを算出し、表 10のようにまとめる。

表 10　データセンタ活用型のリスク

災害		発生確率[%] (年間に換算)	発生時損失 [万円]	リスク [万円／年]
地震	根室沖	1	XXX	XXX
	三陸沖北部	3	XXX	XXX
	宮城県沖	3	XXX	XXX
	首都直下型	2	XXX	XXX
	東海地震	3	XXX	XXX
	・・・			
	△△地震	2	178.2	3.6
津波		1	XXX	XXX
気象災害	風水害	3	XXX	XXX
	土砂災害	1	XXX	XXX
	雪害	3	XXX	XXX

	落雷	1	XXX	XXX
噴火	□□山	1	XXX	XXX
			合計	3900

表 10では省略して記載しているが、落雷など局所的な災害については、所在値ごとに発生頻度、発生時損失を算出し、リスクとして計算を行う。データセンタ活用型の評価に関しては以上であるが、同様に他の方式（例えばオンプレミス型）の評価を実施する。

全ての方式についてのリスク評価が完了したら、方式ごとの評価結果から

・発生時の最大損失
・各方式のリスク
・最大復旧時間
・構築、運用、リスクの費用合算

などをまとめる。なお、費用合算を求める場合には、構築、運用コストを別途、指定する。また、構築費用は償却費用などの単位期間あたりの支出として換算する。

表 11　方式比較

方式	発生時最大損失 [万円]	最大復旧時間 [日]	リスク [万円／年]	費用合算 [万円／年]
オンプレミス型	4000	30	4000	50000
データセンタ活用	3500	30	3900	49000

表 11の結果から、利用者が評価した方式のなから最適なものを選択する指標を得ることができる。

4. 評価

BCP 策定における、従来のリスク評価方式では、個別の災害について、個々のリソース(建屋など)の被害想定しか行えなかった。本方式では、インパクト定義を使って個別の災害での被害を求め、リソース定義と業務定義によるリソースと業務の関係を使って複数の地点にまたがるシステムを用いた業務の稼働率を求めることが出来る。それにより、想定被害額を適切に求めることが出来た。

また、本方式の課題に対し、以下の様に解決することが出来た。

・社会インフラの被害想定
　社会インフラの復旧率については、被害の階級に応じて設定出来る。また、災害毎に階級の設定を行うため、想定される災害に対し、適切な復旧率を設定出来る。
・複数の災害
　対象とする複数の災害に対して、損失額と頻度からリスクを算出することが出来る。複数の地域をまたがったシステム構成の場合でも、リソース定義により、サーバ等のリソースの依存関係を示すことが出来るため、被災した地域が 1 カ所に限らない場合でも、リスク評価を行うことが出来る。
・物理構成と論理業務の関係
　業務定義により、サービスの始点から終点までの関係を定義出来るため、物理的な構成要素と論理的な業務の関係を適切に定義出来る。

5. 今後の課題

本論文にて、リスク評価のためのシステムおよび災害の定義方法および評価方式を提案した。

しかし、災害によって発生する費用以外にも、バックアップや二重化などの対策により生じる費用がある。また、対策を行うことにより、災害時の稼働率も変わるため、損失も変動する。

今後は、目標復旧時間(RTO)や目標復旧地点(RPO)の設定と、それによって発生する金額的要件、業務の代替手段を取った場合に余分にかかる費用、災害時の稼働率変動を取り入れた、評価方式の検討を進めていく。

また、今回は検討を行ったのみであるため、本方式の実装を行いたい。また、公開されている災害情報の収集と、その情報を本システムに取り込むための変換方式の検討を行う予定である。

参考文献

[1] 経済産業省「事業継続計画策定ガイドライン」 http://www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide.pdf
[2] 内閣府 企業防災のページ 「事業継続ガイドライン 第二版」 http://www.bousai.go.jp/MinkanToShijyou/guideline02.pdf

以上