Vol.2010-IS-111 No.16
2010/3/18

事業継続計画作成・検証支援システムの提案

鶴 薫†

社会全体が高度化する現代において，企業や官公庁などの組織が，自然災害や新型インフルエンザなどが発生した際にもその主要業務の継続を可能とするために事業継続性という考え方が登場した．しかし，様々なリスクに対応する為に事業継続性管理の PDCA サイクルを回し続けるのは組織の負担ともなる．本稿では，組織の業務，および，経営資源をモデル化し，個々の経営資源の時間経過における状態遷移をシミュレーションすることにより，事業継続計画における具体的な対応策立案作業，立案された計画の検証作業，及び，有事の際の対応作業を支援可能なシミュレータを提案する．

A Proposal of a Support System for Business Continuity Plan Making and Verification

Kaoru Tsuru†

In this highly complicated society, the idea of "Business Continuity" has appeared. This idea makes the organizations such as enterprises, governments and municipal offices enable to continue their main business when the incident such as natural disaster, expansion of infectious disease, etc. occurred. However the load on the PDCA-cycle of "Business Continuity Management" to correspond to various risks is getting heavy in the organizations. In this paper, I propose the simulator that can support the several works such as planning, verifying concrete action plans in the "Business Continuity Plan". The simulator is based on modeling the activity of the organizations and is simulating the state transition with the time passage of resources on business in the organizations.

1. はじめに

2001 年の米国同時多発テロを契機として，大規模地震，世界的な新型インフルエンザの流行などの事件が起こるに従い，企業や官公庁といった組織が，事業継続(BC: Business Continuity)／事業継続計画(BCP: Business Continuity Plan)／事業継続性管理(BCM: Business Continuity Management)に対して取り組み始めた．現時点では，一般の企業全般に浸透しているとは言い難いが，電気・ガス・水道・交通・金融といった社会インフラを担う企業や，自治体などの公共セクターでの取り組みが進んでいる．一方，ISO 規格化の動きや，事業継続性管理システムの認証規格として作成された英国規格である BS25999-2 に対応した認証取得が国内でも可能となり，盛んに喧伝されるなど，事業継続への取り組みが一般企業にも浸透する素地が出来つつある．

しかし，事業継続計画の立案作業，及び，立案した計画を PDCA サイクルにより更新する作業は，対応リスクが増えるに従い，増大することになるが，IT を利用して支援を行うツール類が十分ではない．本稿では，事業継続計画の立案対象となる組織の活動をモデル化し，モデル化された個々の経営資源の時間経過における状態遷移をシミュレーションすることにより，事業継続計画における具体的な対応策立案作業，立案された計画の検証作業，及び，有事の際の対応作業を支援可能なシミュレータを提案する．

2. 背景と課題

2.1 事業継続計画

事業継続計画の本来の考え方では，想定外のリスクが発生しても事業が継続可能なような対策を策定するというものだが，現実的には，まず，対応すべきリスクを定義して，そのリスク発生時にも事業を継続させようというアプローチが取られている．先進的な取り組みを行っている組織においては，当初，地震という日本で特に意識される災害に特化した形で事業継続計画の策定を行っている．近年注目を集めている新型インフルエンザのパンデミック対応では，地震対応の事業継続計画をベースとしてパンデミックにも対応可能なように計画を見直す，または，全く別個の事業継続計画を立案する，という 2 通りのアプローチが見受けられる．

事業継続計画の考え方は，従来のリスク管理で被害規模は大きいが発生確率が低い為に対策がなされないようなリスクにこそ対応しなくてはならいないというものである．例えば，情報システムで馴染みの深い ISMS(Information Security Management System)の考え方は，組織の情報資産に対するリスクを資産価値，影響度，蓋然性を基準として評価し，リスクが許容限度以上のものについて，機密性，完全性，可用性の

† 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

観点から対策を実施する，というものであり，事業継続の考え方も入っているが，実際の運用に際しては，影響度は大きいが発生確率が低い大規模災害がその対策コストの大きさもあり，十分な対応がなされないことが往々にして起きており，ISMS に対応済みの組織も事業継続計画への取り組みが必要になってくる．

事業継続性管理では，従来のマネージメントシステムと同様に図 1([1]より)に示すような管理サイクルを回すことにより，事業継続計画の有効性を担保しようとしている．これは，PDCA サイクルを形成しており，図 1 の「方針」「計画」が Plan,「実施および運用」「教育・訓練の実施」が Do,「点検および是正処置」が Check,「経営層による見直し」が Action に相当する．こうしたマネージメントシステムを認証する規格としては，英国規格 BS25999-2 があり，国内でも取得可能となっている．また，ISO における規格化も進められており，将来的には多くの組織が取得するような動きになることが予想され，この分野における情報技術の進展が望まれている．

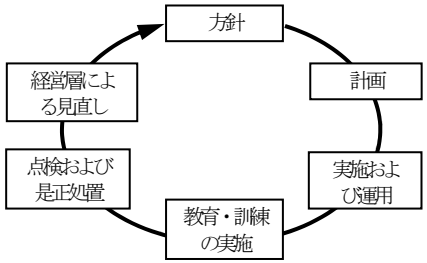


図 1　BC のマネジメントサイクル

2.2 情報技術による事業継続の支援

事業継続への取り組みが，今後，一般化することが想定される中で，事業継続を支援する情報技術の分野は,図 2 に示すように平常時における図 1 の管理サイクルの各フェーズに対応した技術と有事,即ち災害発生時に必要とされる技術から構成される．この分野の情報技術は，[2]によれば，当初，主に IT の災害対策システム構築に関する技術・製品がほとんどであったが，現在では，[3]のような災害発生時の初動対応に必要な通信・安全確認に関する技術・製品や，[4]，[5]のような復旧管理支援に関する技術・製品，又，[6]，[7]のような平常時の事業継続性管理の PDCA サイクルの各フェーズの管理を支援するようなマネージメントシステム用の技術・製品も登場してきている．また，[8]のような教育・訓練支援を行うような研究や，[9]のような防災計画・防災マニュアルの作成・評価支援を行うような研究もあるが，まだ十分ではない．本研究では，図 2 で示された技術の中で，事業継続性管理の PDCA サイクルの各フェーズにおける作業負荷を低減させるための技術開発を主な目的としている．

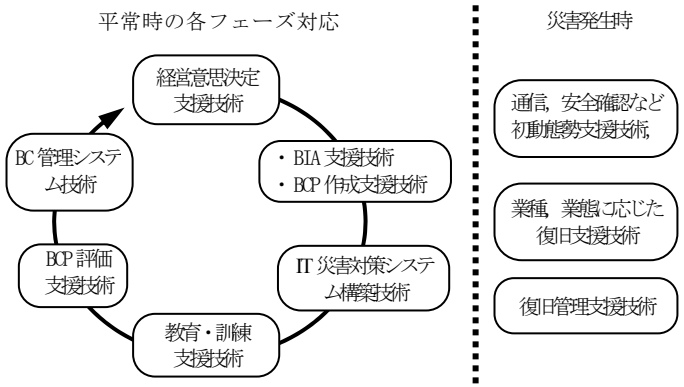


図 2　BC を支援する情報技術

2.3 課題

特に我が国の組織において，事業継続性管理における PDCA サイクルの各フェーズを実施するには以下の問題があると考える．

①. 方針と計画を明快に区分出来ない為，作業負荷増大
事業継続計画策定の順序としては，経営層による方針・戦略の決定を経て，その戦略に沿った事業継続計画策定を行うというのが教科書的な流れがあるが，現実には，取り得る戦略は，実現可能な技術と負担可能なコストにより制限される．この為，方針が定まる前に，具体案を考えて，技術的な裏付け，コスト計算を行い，経営層に報告するというステップを何度も繰り返す必要がある．

②. 部門の壁の為，調整にようする作業負荷増大
前項での具体案の検討が個別部門単位に行われ，通常，事業継続計画作成担当者が整合性を調整するのだが，各部門から提出された具体案をオプションとして組合せを検討するのに多大な労力を要する．

③. 個別リスク対応での事業継続計画の策定による負荷増大・コストアップ
対象リスクが増えると個別に事業継続計画を策定する傾向があり，各フェーズの運用負荷，及び，コストが増大する．特に対象リスクにより，主として対応する部門が異なると，別々に立案してしまう傾向が強い．このため，往々にして個別最適がなされて，全体最適にはならず，組織全体として見ると負荷が増大し，対策コスト，及び，管理コストアップにつながる．

④. 事業継続計画の評価が困難
策定された事業継続計画に従った総合訓練がなかなか行えない．部門単位での訓

練は比較的行いやすいが，その結果を事業継続計画に簡単に反映して評価する仕組みがない．

⑤. 事業継続計画運用の柔軟性が低い
現状，対象リスクごとに一つの被害想定で事業継続計画を策定する傾向がある為，異なる被害想定で事業継続計画が利用可能かを評価するのが難しい．同様に，有事の際に計画時と異なる被害規模の場合，事業継続計画を柔軟に運用するのが難しい．

3. シミュレータの提案

3.1 概要

上記で述べた課題を解決する手段として，継続対象とする事業内の業務プロセス，及び，業務プロセスが依存する経営資源（以下，リソース），及び，事業継続計画での実行プロセスをモデル化し，時間経過における各リソースの状態遷移を予め想定したシナリオに基づきシミュレーションすることにより，分析・評価可能なシミュレータを提案する．具体的には以下のような機能とそれによる効果が期待できる．

(1) 部門別に複数の被害想定，複数の対応策の検討を行い，それらをシミュレータで集約し全体を俯瞰する機能．⇒ 課題①②に対応

(2) 複数の対応策をオプションとして，どのオプションを選択するのが最も良いか，経過時間による事業の操業度（業務レベル），対応策の合計コストにより評価を可能とする機能． ⇒ 課題②③に対応

(3) 部門個別に実施した訓練結果に基づく想定の見直し（主に個別の対応策の必要時間に関して）をシミュレータで集約し，全体への影響を見ることにより，全体を評価する機能．⇒ 課題④に対応

(4) 被害想定担当者以外が，個別リソースの被害想定を変更して全体を検証・評価することができ，又，有事の際に実際の被害に変更して事業継続計画の効果を簡易に評価できる機能． ⇒ 課題⑤に対応

3.2 モデル化の考え方

前節に挙げた機能を実現する為にシミュレーション対象モデルを検討した．情報システムにおいて，構成要素であるコンポーネントに障害が発生した際にどのような影響が及ぶかを分析する手法として[10]にある CFIA (Component Failure Impact Analysis) や，ITIL(Information Technology Infrastructure Library) で定義された CMDB (Configuration Management Database) ([11])を用いた手法がある． 筆者はこれらに着想を得て，事業を業務プロセスに分解し，業務プロセスから業務プロセスを構成する要素，即ち，業務プロセスが依存するリソース（他のサービス，情報システム，人員，設備，社会インフラなど）に分解し，その依存関係から，あるリソースが被害を受けた際の影響範囲を簡易に特定できる図 3 に示すようなモデルをまず想定した．

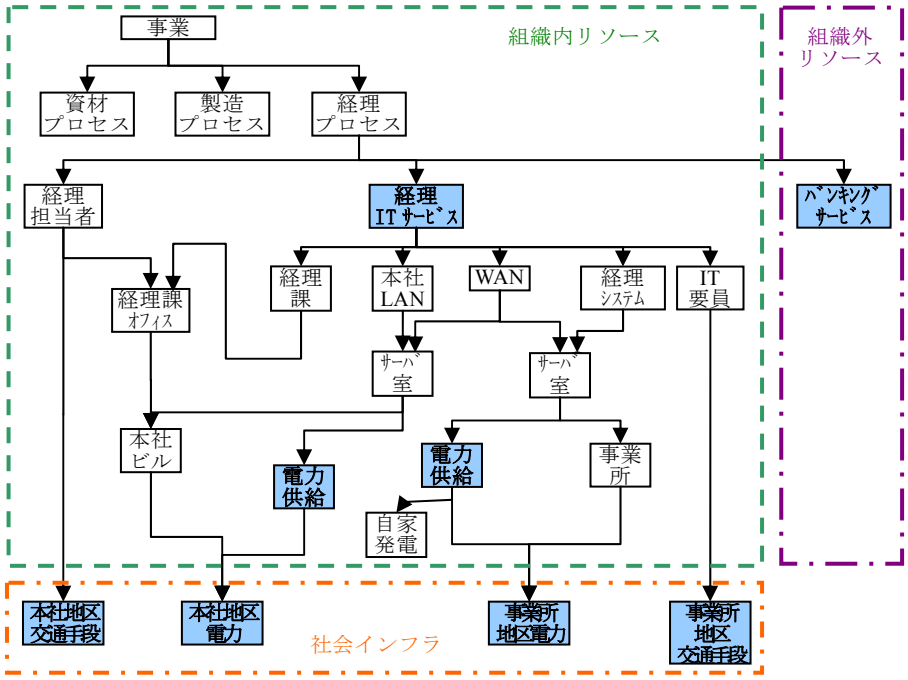


図 3 業務プロセスとリソースの依存関係

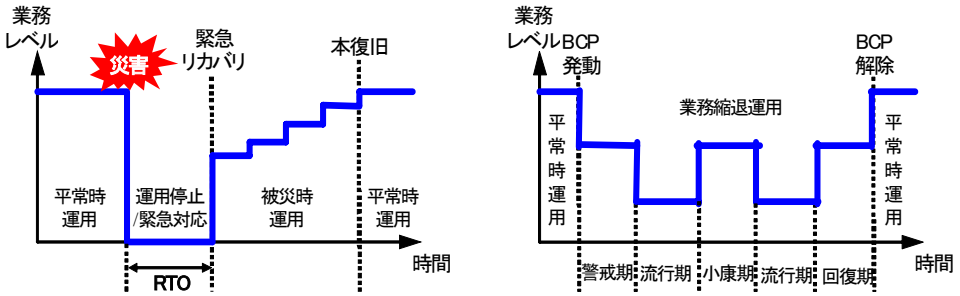
このようなリソースの依存関係で影響分析を行う手法自体は，影響分析ダイヤグラムとして[12]でも触れられているが，本提案でのモデル化の特長としては以下である．

・ ある部門で被害想定できないような他者に依存している部分をその部門から見てブラックボックス化する．
図 3 において，網掛けをしている部分は，他者が提供するサービスと捉える．例えば，経理部門で経理プロセスをモデル化しようとすると，自部門で判るのは，経理担当者がいて経理 IT サービスとバンキングサービスを利用して業務を遂行しているというレベルである．経理 IT サービスが具体的にどのようなリソースに依存しているかは経理部門が知る必要はなく，経理 IT サービスのモデル化は情報システム部門が行えば良い．また，情報システム部門が経理 IT サービ

スをモデル化しようとすると，電力供給に関してどのようなリソースに依存しているかを知る必要はなく，電力供給のモデル化は，設備保守部門が行えば良い．なお，同様に被災想定も各部門がモデル化した範囲で実施する．

・ 時間と状態遷移の概念を導入し，単純な被災/復旧という概念以外にも対応可能とする．

図 4の(a)に示すような自然災害によって被災してから単純に時間経過と共に復旧へ向うという状態変化だけではなく，(b)に示すようなパンデミックによって時間経過と共に業務レベルが上下することへの対応を考慮し，図 5 に示すように扱うリソースに対して遷移状態を定義し，業務レベルの上下を表せるようにする．ここでは，"Available"をリソースの利用可能レベル 100%とし，"Stop"，"Unavailable"らを利用可能レベル 0%とし，"Restricted"において利用レベル 1～99%を表せるようにする．



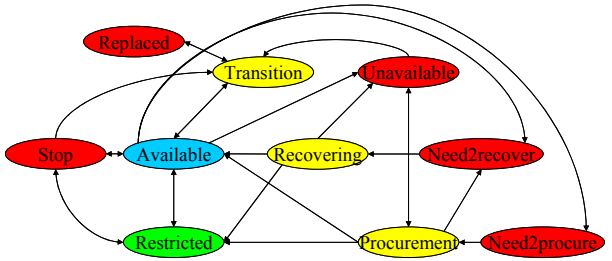
(a) 地震の例　　(b) パンデミックの例

※ RTO: Recovery Time Objective

図 4　被災時の時間経過における業務レベル

・ 復旧だけではなく代替も可能なようにリソースの代替をモデル化する．

図 6 で示されるような×印で示される"Unavailable"となったリソースの代替リソースを代替オプションのモデルとして記述できるようにする．この代替オプションへの切替えを表わす為に，遷移状態として"Replaced"を定義する．代替や，復旧の実行プロセス自体は明示的に扱うのではなく，代替リソースへの切り替えを"Transition"という状態で扱い，"Transition"への遷移を"条件付き状態遷移"で扱う．"条件付き状態遷移"とは，リソースが別の状態に遷移する際の条件を指定できるもので，例えば，「リソース A が"Available"且つリソース B が"Available"となったら，リソース C は"Transition"に遷移する」という条件を指定可能としている．



Available	正常に機能
Restricted	制限付きながら機能（レベル1～99%）
Transition	代替切替中
Replaced	代替済み
Recovering	復旧中
Procurement	調達中
Unavailable	機能停止（異常停止）
Need2recover	機能停止(復旧が必要)
Need2procure	機能停止(調達が必要)
Stop	停止中（正常停止）

図 5　リソースの遷移状態

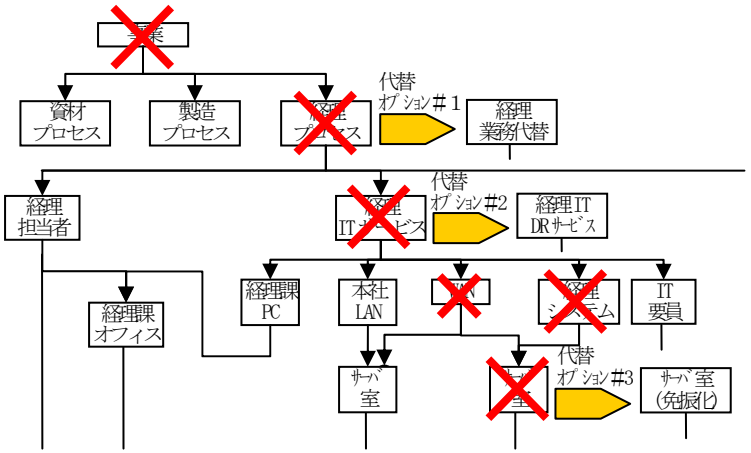


図 6　代替オプション

3.3 シミュレータ内容

以下，シミュレータの内容を図 7 のシミュレータを利用した作業フローに合わせて示す．

①. モデル入力

各部門が自部門の担当する範囲でリソース，及び，リソース間の依存関係を記述・入力する．例えば，業務部門は，自部門の業務プロセス，及び，業務プロセスが依存する各種リソースを記述する．

②. リスクシナリオ入力

BCP 作成担当が提示した複数のリスクのシナリオに従い，自部門の各リソースの時間経過における状態遷移を表 1 の例に示すように記述・入力する．その際に，他部門のリソースに依存して状態遷移が発生する時刻が決まるものは，条件付き状態遷移として，遷移時刻は変数で記述・入力する．

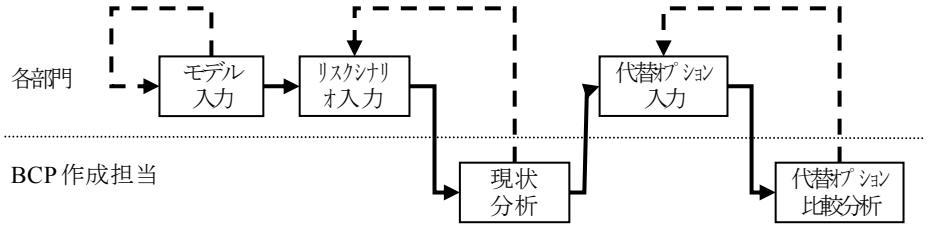


図 7　シミュレータを利用した作業フロー

③. 現状分析

BCP 作成担当が，入力されたモデル，及び，リソースの状態遷移を元に，業務プロセス，及び，事業の経過時間における状態遷移をシミュレーションする．例えば，図 8 のように，ある業務プロセスに着目した状態遷移を表示させる．こうした現状分析に基づき，経営層と大まかな目標値を設定し，各部門に対して，対応策の検討を依頼する．

表 1 リソースの状態遷移記述例

ﾘｿｰｽ名称	遷移時刻	遷移状態	ﾘｿｰｽﾚﾍﾞﾙ	条件
経理ｼｽﾃﾑ	00:00	Unavailable	0%	なし
経理ｼｽﾃﾑ	X	Recovery	0%	IT 要員=Available && サーバ室=Available
経理ｼｽﾃﾑ	X+06:00	Restricted	30%	なし
経理ｼｽﾃﾑ	X+Y	Restricted	80%	○○ｼｽﾃﾑ=Available
経理ｼｽﾃﾑ	X+Y+02:00	Available	100%	なし

④. 代替オプション入力

各部門が検討した対応策を代替オプションとして，記述・入力すると共に，状態遷移も記述・入力する．基本的にモデル入力，リスクシナリオ入力と同様の手順で行うが，代替オプションの実行に伴うコストも入力する点が異なる．

⑤. 代替オプション比較分析

BCP 作成担当が，代替オプションの組合せを BCP オプションとして設定し，その BCP オプション毎に例えば，図 9 に示すように複数リスクでの経過時間における業務レベル推移，導入コストなどの指標で比較評価する．

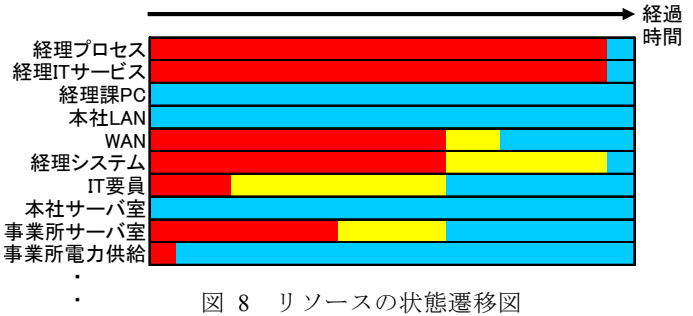


図 8　リソースの状態遷移図

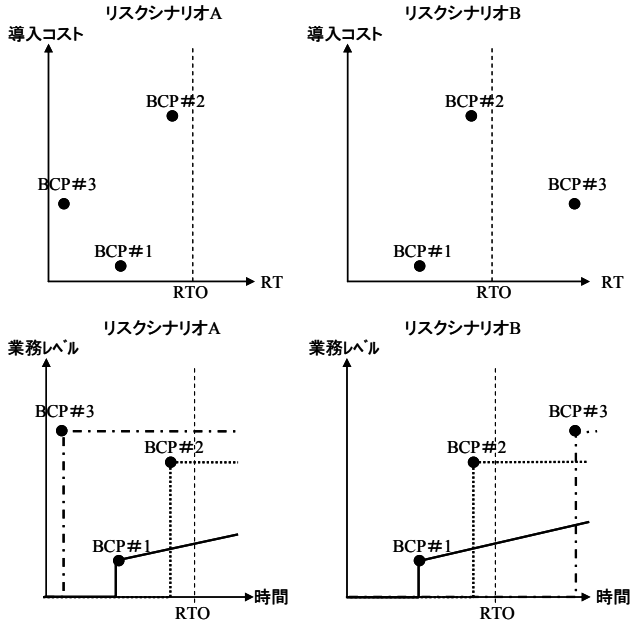


図 9　BCP オプションの比較例

Vol.2010-IS-111 No.16
2010/3/18

4. シミュレータの実装

4.1 試作

試作では，某社の情報システム部門，および，総務部門に協力を依頼し，情報システム部門が内部統制報告書を作成する為に行った営業，資材，経理業務と情報システムの関係を分析した結果を元にして，業務プロセスと業務プロセスが依存するリソース（情報システム，人員，設備，社会インフラ）のモデル化を実施した．対象リスクとしては，首都直下型地震を想定してリスクシナリオを作成した．リスクシナリオにおける被害想定では，内閣府中央防災会議の被害想定を元に経過時間における状態遷移の設定を行った．また，情報システムに関しては，障害復旧計画書での人員計画，作業想定時間を元に状態遷移の設定を行った．

なお，試作システムで実装した機能は，作業フローにおける現状分析の機能までである．シミュレータは，WindowsXP 上で，図 10 に示すように，データベースに MS Access2003，シミュレータ用 GUI に Internet Explore，シミュレーションエンジン部分に Apache+PHP，状態表示画面に MS Visio2007 を用いて作成した．図 11 に試作したシミュレータ画面の一部を示す．

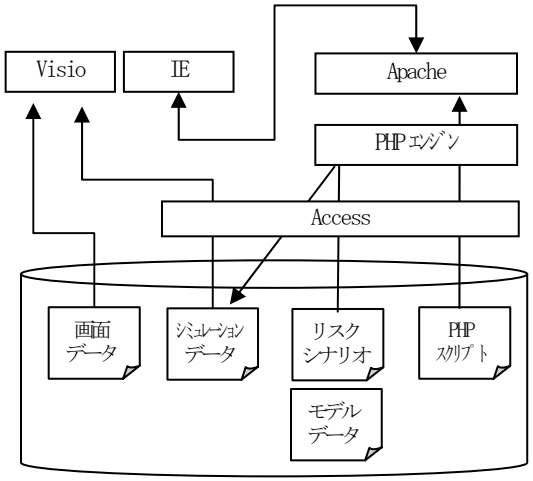
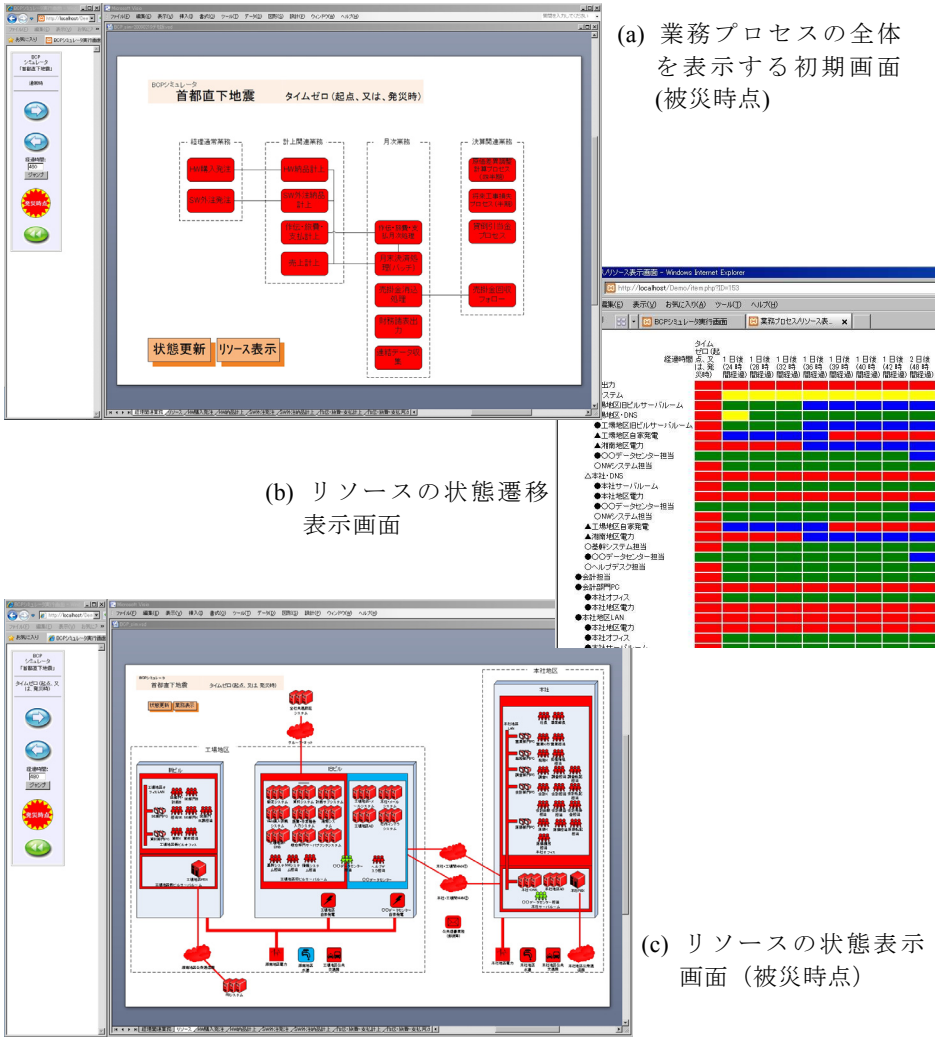


図 10　試作したシミュレータの構成



(a) 業務プロセスの全体を表示する初期画面(被災時点)

(b) リソースの状態遷移表示画面

(c) リソースの状態表示画面（被災時点）

図 11　試作したシミュレータの画面例

4.2 評価

本提案の試作においては，一部の機能の実装にとどまったが，2.3 節に示した課題①～⑤の解決に以下のように有効だとの結論を得た．

課題①に関しては，経営層に全体像を俯瞰いただき説明する為のツールとしては有効だろうとの意見をいただいたので，方針と計画の間で繰り返される手順の負荷低減になると考えられる．課題②に関しては，入力の容易性など使い勝手が上がれば，各部門で入力して貰えるとの感触を得たので，BCP 作成担当者の負荷低減になると考えられる．課題③④に関しては，今回の試作では全ての機能を実装できなかったが，机上で検討した機能自体は経営層，及び，現場担当者から評価いただけたので，管理負荷低減，対策コスト・管理コストの低減が可能だと考えられる．課題⑤に関しては，手軽に被害想定を変えて状況の推移を確認できるので，有効だとの現場の評価をいただいたので，様々な条件下での計画の検証負荷低減，実際の被災時の柔軟な計画運用性向上に有効だと考えられる．

4.3 今後の課題

本提案のシミュレータに用いるモデルでは，各要素・リソースの粒度を自在に調整可能な余地を持たせている．従って，情報システムの各コンポーネント単位，人員の人一人単位まで，詳細なモデル化を行うことも可能であるが，モデルの更新負荷を考慮すると，ある程度の抽象化が不可欠である．今後，実適用を行う為には，導入に際してどの程度の粒度とするかのガイドラインを設定する必要がある．

4.4 将来構想

今回の実装では，データ構造を独自に設計したが，将来的には[13]で定義されている共通情報モデル(CIM)を適用すべく，現在検討中である．CIM のモデル化対象は情報システムを対象としているが，コアモデル定義，共通モデル定義，以外にベンダー拡張モデルの定義が可能となっており，情報システムではない部分のモデル化をベンダー拡張により可能だと考えている．CIM を用いてモデル化することにより，CIM に基づく運用監視システムと本提案のシミュレータを接続し，ある情報システムコンポーネントに障害が発生した際の業務への影響範囲も見ることができるようになるなどの効果が期待できる．なお，CIM では，時間の概念がないため，この点に関しては実装で対応する．

5. おわりに

対象とすべきリスクが増加する状況にあって，定期的な更新を欠かさずに実効性のある事業継続計画を持ち続けるには，計画立案・検証・見直しなどの作業負荷が大きく，従来のように部門別の縦割りで対策立案を行うと管理コストが増大する上に対策コストが増大するというような課題があった．こうした課題を解決する為，事業継続計画の作成・検証を支援するシステムとして，部門別に業務プロセスとリソースの依存関係を定義したモデルを作成し，リスク発生時における各リソースの状態遷移などを記述することにより，これらを集約して，事業として経過時間に対してどのように状態遷移するかを検証可能なシミュレータを提案した．BCP 作成担当者の作業負荷低減，事業継続性管理における管理コスト，対策コストの低減に提案したシミュレータが有効な手段であるとの目途を得た. 今後は, 実適用に向けた評価を行う予定である．

参考文献

1) 内閣府防災担当，ほか：事業継続ガイドライン第一版 -わが国企業の減災と災害対応の向上のために-, http://www.bousai.go.jp/MinkanToShijyou/guideline01.pdf , (2005).
2) 鶴薫：事業継続性を支援する IT 技術に関する一考察, 情報処理学会研究報告 2006-IS-95, pp.39-45(2006)
3) 後藤啓一:災害時に威力を発揮する双方向通信型の「減災コミュニケーションシステム」, NTT 技術ジャ-ナル 20(9), (234) pp.26-30 (2008)
4) 福田路子，ほか：緊急時指揮支援システム「NoKeos」の紹介, NTT 技術ジャ-ナル 17(9), (198) pp.30-34 (2005)
5) 伊藤良浩:BCP の初動対応を支援する危機管理業務支援システム， NTT 技術ジャ-ナル 20(9), (234) pp.36-39 (2008)
6) SunGard Availability Services：Business Continuity Management Software, http://www.availability.sungard.com/ITSolutions/software/Pages/software.aspx
7) Andrzej Zalewski，ほか：Modeling and Analyzing Disaster Recovery Plans as Business Processes, Lecture Notes in Computer Science, Vol. 5219, pp.113-125 (2008).
8) 源栄正人，ほか：緊急地震速報と連動した学校向け防災教育・訓練支援システムの実証試験と今後の展開，東北地域災害科学研究 43, pp.67-72 (2007)
9) 川村誠吾，ほか：想定外事象の自動生成機能を持つ災害時事業継続支援システム．第 71 回情報処理学会全国大会, pp.4-533～4-534(2009).
10) N.Joshi, ほか: "Integration of domain-specific IT processes and tools in IBM Service Management", IBM Systems Journal vol.15, No.3 (2007).
11) Great Britain. Office of Government Commerce："Software asset management" (2003).
12) 伊藤毅，ほか：富士通における BCP(事業継続計画)策定, Fujitsu 57(5) (336) pp.474-481(2006).
13) DMTF：Common Information Model(CIM) Specification Version 2.2 (1999).