情報システムの継続的運用計画支援システムの開発と適用

松永 一朗† 佐々木 良一‡

†東京電機大学
120-8551 東京都足立区千住旭町 5 番
matsunaga@isl.im.dendai.ac.jp, sasaki@im.dendai.ac.jp

あらまし 情報技術が様々な組織の根幹を支える様になり，情報システムが停止した場合の影響が非常に大きいものとなっている．そのため，情報システムの運用継続性の確保が重要な課題に挙がっている．しかし，情報システムの継続性には関与者も多く，考慮するべき内容が複数あり，またその内容は複雑に絡み合っているため，適切な対策の組み合わせを求めるのが困難であった．著者らは，信頼性工学で用いられるイベントツリー分析法とプロジェクトの工程管理に用いられる PERT 手法を組み合わせるリスク分析方法と支援システムを開発するとともに，その適用を地方自治体の情報システムに対して行い，必要な対策案の組み合わせを明確にしたので報告する．

Development and application of continuity operation plan support system for Information Technology

Ichiro Matsunaga† Ryoichi Sasaki‡

†Tokyo Denki University.
5 Asahi-cho, Senju, Adachi, Tokyo 120-8551, JAPAN
matsunaga@isl.im.dendai.ac.jp, sasaki@im.dendai.ac.jp

Abstract Because information technology (IT) became the basis of various organizations, the impact of information system's stop became big extremely. Therefore continuous operation of IT is an important problem. However, to keep continuous operation of IT is difficult, because there are many people concerned, multiple contents which they should consider more, and contents which are connected with each other complicatedly. To solve the problem, we report the developed method by combining the event tree analysis used in reliability engineering and the PERT technique used in process management. In addition, we report also the support system of the method and its application result.

1 はじめに

金融，航空，鉄道，電力，ガス，政府・行政サービス，医療，水道，物流などの社会の重要インフラを含め，社会の多くの仕組みが IT（Information Technology）システムに依存するようになった．このような IT システムの安全を確保するためには，従来の「情報セキュリティ」の概念だけで扱うのは無理な時代になっている．IT システムの安全性は，意図的な不正だけでなく，天災やハードウェアの故障，ソフトウェアのバグ，ヒューマンエラーによっても脅かされるが，従来の情報セキュリティではこれらの意図的でない脅威はほとんど取り扱ってこなかった．このような，

IT システムにおいて広い意味での安全が失われる可能性を「IT リスク」と呼ぶ[1]. 本稿では, IT リスクのうち, Availability を脅かすリスクである天災や故障といった災害に注目を行い, IT システムの運用継続性という面から定量的なリスク分析を行った.

ここでは事故後の様々なシーケンスを想定できるようするために必要となるリスク分析手法としてイベントツリー分析法[2]を利用し, さらに各シーケンスにおける被害の大きさを算出する際の業務停止時間を推定するために, プロジェクト管理手法である PERT 手法[3]を用いている.

イベントツリー分析法は様々なリスク分析において利用されており, 特に原子力工学の分野で実績がある. 情報技術の分野においても, 公開鍵暗号危殆化に関するリスク分析などが行われている[4]. また PERT 手法は製品開発などの日程計画を立てる際に有効なプロジェクト管理手法である. PERT 手法を用いたリスク分析として, 土木工学の分野において業務継続計画における効果的な対策案の選定に関する提案が行われている[5]. しかし, 本研究以外に PERT 手法を用いたリスク分析の適用例は見受けることができなかった. またイベントツリー分析法と PERT 手法を組み合わせたリスク分析方式は, 従来なかったと考えている.

この方式によって, リスク分析に必要な労力を軽減することができるため, 適用対象の規模が大きくなった場合にも対応することができるようになった.

2　対策案の選定手順

当手法の概略図を図1に示す. また当手法を用いた対策案の選定手順を以下に示す（図2参照）.

(1) 重要システムの特定
適用の対象とするシステムを特定する.

(2) 目標復旧時間の設定
(1)で特定したシステムの, 目標とする復旧時間を設定する.

(3) リスクの提起
初期事象となるリスクを決定する.

(4) ヘッディング項目の決定
初期事象による影響を分析し, イベントツリーのヘッディング項目を決定する. イベントツリーについては, 後ほど説明する.

(5) 各ヘッディング項目の発生確率の見積もり
各ヘッディング項目の故障確率, 失敗確率を見積もる.

(6) 各シーケンスの発生確率の算出
イベントツリー分析法を用いて, 各シーケンスの発生確率を算出する.

(7) 各復旧作業の作業時間見積もり
インシデント発生後の状況下における各復旧作業の所要時間を見積もる.

(8) 各シーケンスの停止時間の算出
PERT 手法を用いて, 各シーケンスの停止時間を算出する. PERT 手法については, 後ほど説明する.

(9) 停止時間の期待値の推定
(6)と(8)の結果から, リスク値として停止時間の期待値を推定する.

(10) 現状のリスク評価
(2)で求めた目標復旧時間を, リスク値が達成しているか確認する.

(11) 対策案の選定
目標復旧時間を達成するために必要な対策案を検討し, 適用に加える.

さらに詳細なリスク分析を行う必要がある場合には, (3)において複数のリスクを提起することが望ましい.

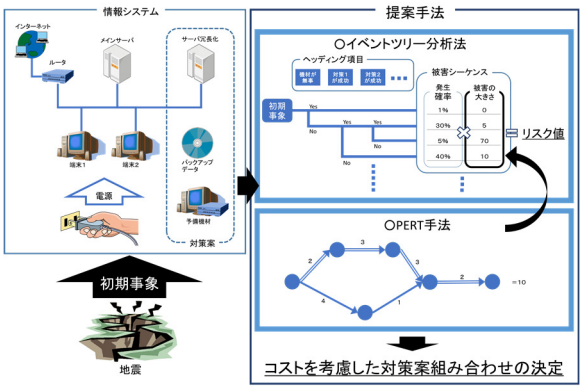

図 1　提案手法概略図

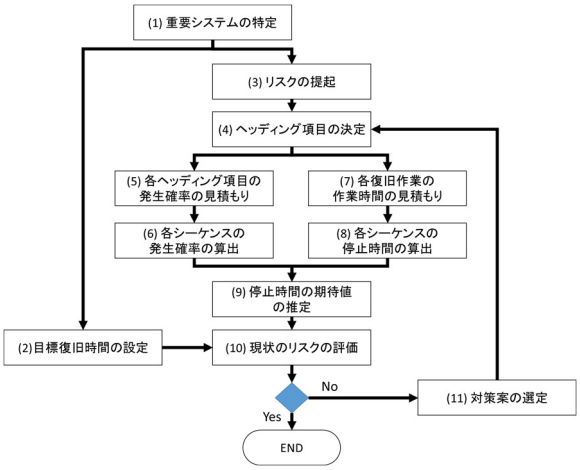

図 2　対策案の選定手順

3　イベントツリー分析法と PERT 手法を用いたリスク分析方式

3.1　提案方式の概要

IT システムの運用継続性を脅かすリスクには，以下の2つの特徴がある．

1. 複数の初期事象が想定され，さらに1つの初期事象から発生する被害のシーケンスは複数存在する
2. 被害の大きさがシステムの停止時間に依存している

1のような複数の被害のシーケンスが想定される問題の分析には，従来からイベントツリー分析法がよく用いられている．イベントツリー分析法を用いることによって，無数にあるシーケンスを網羅することができる．さらにヘッディング項目の発生確率を決定することで，各シーケンスの発生確率を容易に算出することができる．

イベントツリー分析法は幅広いリスクに対して有効な分析手法であるが，各シーケンスの被害の大きさについてはそれぞれ見積もりを行っていく必要があるため，ヘッディング項目数が非常に多くなった場合，被害の大きさを見積もることが困難になってしまう．しかし IT システムの運用継続性を脅かすリスクにおいては，この問題を解決することができる．

解決には IT システムの運用継続性を脅かすリスクの2つ目の特徴である，被害の大きさがシステムの停止時間に依存しているという点を利用する．

一般的に，システムが停止している時間は復旧作業を行っており，復旧作業が終わった段階でシステムが稼働する．つまりシステムの復旧に必要な作業と，その作業の所要時間を把握することができれば，システムの停止時間を算出することができる（図3参照）．またシステムの復旧に必要な作業は，各シーケンスにおける機材と対策の状態から推定することが可能であり，各復旧作業にかかる所要時間は既往の被害予測結果を利用し，ある程度見積もることが可能である．ここで復旧工程全体の所要時間を算出する際に PERT 手法を用いる．

各シーケンスにおける被害の大きさを計算で求めることによって，従来の方式に比べて，リスク分析を行う際に必要な負担を軽減することができるため，適用対象の規模が大きくなった場合にも対応することができる．

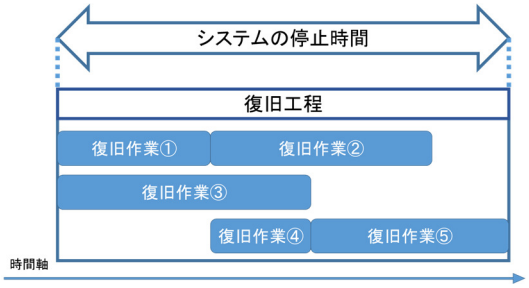

図 3　システムの停止時間

3.2　イベントツリー分析法を用いた分析

イベントツリー分析法は，横軸にヘッディング項目を配置し，初期事象からツリー状にシーケンスを分岐させていくことによって，最終的な進展事象を論理的に表す事ができる．ヘッディング項目とは，初期事象から始まり事故に至るまでにおける事象のことであり，当手法でのヘッディング項目は，1）構成機材・環境基盤が破損・停止しているか否か，2）対策案が効果を発揮するか

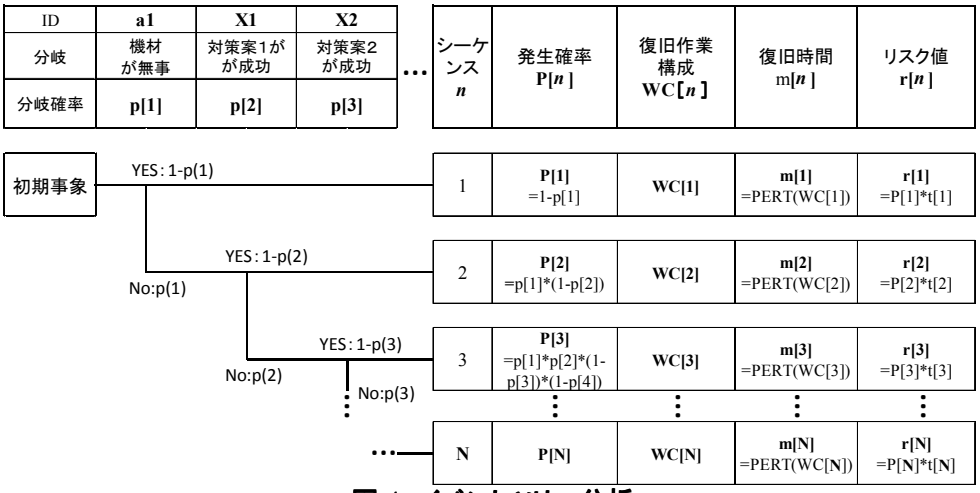

図 4 イベントツリー分析

否か，の2点となる．

また，イベントツリー分析法は定量的な取り扱いを行うことが可能であり，各ヘッディング項目の発生確率を入力することで，各事象への進展確率を求めることができる．

本稿ではイベントツリー分析法を用いて，各シーケンスの発生確率と復旧に必要な作業の構成を推定する（図4参照）．各シーケンスの発生確率を算出する式を以下に示す．

$$\mathbf{P}[n] = \prod_{i=1}^{H} \mathbf{P}'[i]$$

$$\mathbf{P}'[i] = ((1 - p'[i])(1 - y[i]) + p'[i] * y[i])$$

$$y[i] = \begin{cases} 1: \text{ヘッディング項目}i\text{が下に展開} \\ 0: \text{ヘッディング項目}i\text{が横に展開} \end{cases}$$

$$p[\mathrm{i}] = p'[i] * x[i] + (1 - x[i])$$

$$x[i] = \begin{cases} 1: i\text{番目の対策を講じる} \\ 0: i\text{番目の対策を講じない} \end{cases}$$

n ：n 番目のシーケンス

$\mathbf{P}[n]$ ：n の発生確率

H ：ヘッディング項目数

i ：i 番目のヘッディング項目

$p[i]$:i の分岐確率

$p'[i]$:i の破損確率・失敗確率

$x[i]$:i の対策案の採用状態

対策を講じなかった場合，そのヘッディング項目は必ず失敗するものとして計算を行う．

次に各シーケンスにおける復旧に必要な作業構成の推定を行う．図4における WC[n]は n 番目のシーケンスにおける要実施項目である．

まず推定を行っていく際の基準となる作業構成として，全ての機材が破損，全ての対策が失敗した状況のシーケンス WC[**N**]を考える．例として，地震や落雷によって機材が破損した場合の復旧作業の流れを図５に示す．この場合，WC[**N**]は，{A1, A2, A3, A4, E, F}となる．

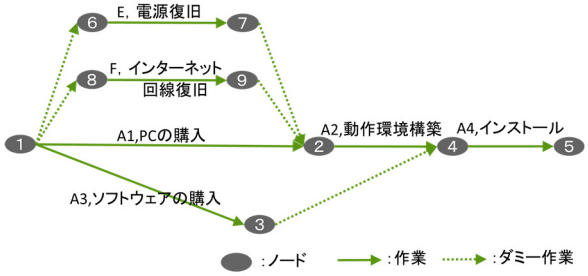

図 5 WC[N]の復旧作業工程

WC[**N**]を基にして各シーケンスにおける復旧作業構成を推定する．必要なソフトウェアがインストール済みである PC を購入することができる対策があるとする（対策案 X1）．対策案 X1 が成功した場合，図4におけるシーケンスは n=2 である．対策案 X1 が成功したことによって，復旧の流れは図6のように変化し，n=2 の復旧に必要な作業構成 WC[2]は{X1, E, F}となる．このことか

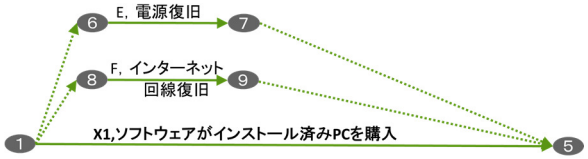

図 6 WC[2]の復旧作業工程

ら，対策 X1 が効果を発揮した場合の効果対象は{A1，A2，A3，A4}であることが分かる．このようにして各機材・対策の効果対象を求めることで，各シーケンスの復旧作業構成を推定することができる．

3.3 PERT 手法を用いた分析

PERT 手法は作業時間と作業の先行後続の関係が分かっていれば，そのプロジェクトの所要時間を算出することができる手法である．前項で各シーケンスにおける復旧作業構成を推定したので，そこから復旧作業の所要時間を求める．

本稿では PERT 手法を用いて，各シーケンスにおける被害の大きさであるシステムの停止時間を算出する．前項で取り上げた作業構成 WC[**N**]の所要時間(m[**N**])の算出過程を表1に示し，WC[2]の所要時間(m[2])の算出過程を表2に示す．

各シーケンスにおけるシステムの停止時間を算出する式を以下に示す．

$$et[\,l\,] = \mathrm{MAX}(\,st[\,pre[\,l\,]\,]\,) + t[\,l\,])$$

$$m[n] = \mathrm{MAX}(\mathbf{ET})$$

l :構成作業の作業 ID
st[l] : l の最早開始時間
pre[l] : l の先行作業・必須環境(predecessor)
t[l] : l の所要時間
et[l] : l の最早完了時間
ET :全ての最早完了時間
n : n 番目のシーケンス
m[n] :停止時間

表 1 m[N]の復旧時間算出過程

ID	作業名	所要時間	先行作業	必須環境	最早開始 st[/]	最早完了 et[/]
A1	PCの購入	t[A1]	-	-	st[A1] =MAX(0)	et[A1] =st[A1]+t[A1]
A2	動作環境構築	t[A2]	A1	E,F	st[A2] =MAX(et[A1],et[E],et[F])	et[A2] =st[A2]+t[A2]
A3	ソフトウェアの購入	t[A3]	-	-	st[A3] =MAX(0)	et[A3] =st[A3]+t[A3]
A4	インストール	t[A4]	A3	E	st[A4] =MAX(et[A3],et[E])	et[A4] =st[A4]+t[A4]
E	電源復旧	t[E]	-	-	st[E] =MAX(0)	et[E] =st[E]+t[E]
F	インターネット回線復旧	t[F]	-	-	st[F] =MAX(0)	et[F] =st[F]+t[F]

表 2 m[2]の復旧時間算出過程

ID	作業名	所要時間	先行作業	必須環境	最早開始 st[/]	最早完了 et[/]
X1	PCの購入	t[X1]	-	-	st[X1] =MAX(0)	et[X1] =st[A1]+t[A1]
E	電源復旧	t[E]	-	-	st[E] =MAX(0)	et[E] =st[E]+t[E]
F	インターネット回線復旧	t[F]	-	-	st[F] =MAX(0)	et[F] =st[F]+t[F]

3.4 リスク値の算出

各被害状況の停止時間と発生確率から，リスク値である「停止時間の期待値」を算出する．計算式は以下のようになる．

$$\mathbf{R} = \sum_{n=1}^{\mathrm{N}} \mathbf{P}[n] * m[n]$$

R :リスク値（停止時間の期待値）
N :全シーケンス数
n : n 番目のシーケンス
P[n] :発生確率
m[n] :停止時間

4 適用対象のモデル

4.1 適用対象のモデルの決定

本稿では総務省発行の「地方公共団体における ICT 部門の業務継続計画策定に関するガイドライン 策定例」（以降，策定例）[6]と「地方公共団体における ICT 部門の業務継続計画（ICT-BCP）初動版サンプル」（以降，初動版サンプル）[7]を基に適用対象のモデルを作成した．適用対象の属性を表3に示す．

また今回の適用では，策定例において詳細な事業影響度分析がなされていた4種のシステムを取り扱うこととする．各システムの詳細と目標復旧時間を表4に示す．

表 3 適用対象の属性

組織形態	地方公共団体
地域	都市部
人口	約40万人
ICT 部門の職員数	約30名
想定リスク	震度6強の地震

表 4 各システムの管理部門と目標復旧時間

システム名	主管管理部門	目標復旧時間
国民保険システム	保険年金課	3 日
年金システム	保険年金課	7 日
介護保険システム	保険年金課	7 日
住民記録システム	市民窓口センター	24 時間

4.2 メインタスクとサブタスクの設定

複数のシステムで必要とされる機材やメインタスクの要所で関連してくる機材を，サブタスクとしてまとめることにした（表5参照）．A, B, C, D がメインタスクであり，その他はサブタスクとなる．また以降使用される各 ID の頭文字は，この対応に準じたものが付けられている．

表 5 タスクと対応機材

タスク名	対応機材
A	国民保険システム
B	年金システム
C	介護保険システム
D	代替住民記録システム
E	電力インフラ関連
F	インターネットインフラ
G	構内ネットワーク関連
H	VPN 関連
I	住民記録端末
J	年金端末
K	介護保険端末

4.3 構成機材の抽出

各システムを構成している機材を抽出する．策定例，初動版サンプル共に詳細な機材構成については言及されていなかった．そこで一般的なシステム構成を基にして，策定例・初動版サンプルで述べられている内容からシステム構成を推察した．

また，「住民記録システム」に関しては，策定例での最低復旧目標レベルが代替作業の開始であったため，それに準じた構成とした．その他のシステムの構成は同一の構成と想定した．表6に構成機材を示す．

表 6 機材構成

機材ID	機材名	破損確率	破損した際の復旧作業
a1,b1,c1	サーバPC	0.8	A1,A2,A3,A4,A5,A6,A7,A8
a2,b2,c2	ソフトウェアデータ	0.05	A3
a3,b3,c3	バックアップデータ	0.05	A5
d1	端末用PC	0.8	D1,D2,D3,D4,D5
d2	代替作業用データ	0.05	D3
d3	プリンター	0.6	D6
e1	電力インフラ	0.99	E1
f1	インターネット回線	0.99	F2
g1	L3スイッチ	0.3	G1,G2
g2	L2スイッチ	0.3	G3,G4
g3	構内LANケーブル	0.5	G5,G6
h1	VPNルータ	0.4	H1,H2
i1,j1,k1	端末用PC	0.8	I1,I2,I3,I4,I5
i2,j2,k2	端末用ソフトウェア	0.05	I3

4.4 復旧作業の検討

機材構成を参照しながら，各システムの復旧に必要な作業の洗い出しを行う．表7に復旧作業を示す．

表 7 復旧作業

作業ID	作業名	所要時間	先行作業	必須環境
A1,B1,C1	サーバ用PC調達	96	–	–
A2,B2,C2	動作環境構築	2	A1	E,F
A3,B3,C3	サーバソフトウェア作成	8760	–	–
A4,B4,C4	サーバソフトウェア調達	0.5	A3	–
A5,B5,C5	バックアップデータ作成	8760	–	–
A6,B6,C6	バックアップデータ調達	0.5	A5	–
A7,B7,C7	ソフトウェアインストール	3	A2,A4	E
A8,B8,C8	バックアップデータ復元	8	A6,A7	E
A9,B9,C9	システム動作確認	5	A8	E,F,G,H,I
D1	端末用PC調達	48	–	–
D2	端末動作環境構築	0.5	D1	–
D3	代替作業用データサルベージ	8760	–	–
D4	代替作業用データ調達	0.5	D3	–
D5	代替作業用データインストール	1	D2,D4	–
D6	プリンター調達	48	–	–
D7	代替作業資料印刷	0.5	D5,D6	E
E1	電力インフラ復旧	72	–	–
F1	回線復旧	72	–	–
F2	通信状態確認	0.1	F1	–
G1	L3スイッチ調達	96	–	–
G2	L3スイッチ設置	1	G1	–
G3	L2スイッチ調達	24	–	–
G4	L2スイッチ設置	1	G3	–
G5	LANケーブル調達	24	–	–
G6	配線	2	G5	–
G7	構内ネットワーク動作確認	1	G1,G3,G5	E
H1	VPNルータ調達	96	–	–
H2	VPNルータ設定	4	H1	E
H3	VPN動作確認	2	H2	E,F
I1,J1,K1	端末用PC調達	48	–	–
I2,J2,K2	端末動作環境構築	2	I1	E,F
I3,J3,K3	端末用ソフトウェア作成	8760	–	–
I4,J4,K4	端末用ソフトウェア調達	0.5	I3	–
I5,J5,K5	端末用ソフトウェアインストール	2	I2,I4	E,F

4.5　対策案の考案

対策案は策定例と初動版サンプルにおいて講じられている対策を初期状態とし，さらに一般的に行われている対策（冗長化や予備機材の保管）を考案することとした．表8に対策案の一覧を示す．

表 8　対策案一覧

対策ID	対策名	作業時間	必須環境	効果対象	失敗確率
XA1,XB1,XC1	サーバ環境のイメージバックアップ化	10	E	A2,A3,A4,A7,A8	0
XA2,XB2,XC2	C庁舎にソフトウェアデータ保管	2	–	A3	0.01
XA3,XB3,XC3	C庁舎にバックアップデータ保管	2	–	A5	0.01
XA4,XB4,XC4	サーバ用PCの冗長化	0	E,F,G,H,I	A1,A2,A3,A4,A5,A6,A7,A8	0.8
XA5,XB5,XC5	サーバ用PCの予備保管	2	–	A1	0.05
XA6,XB6,XC6	バックアップサイトの構築	8	–	A1,A2,A3,A4,A5,A6,A7,A8	0.02
XD1	予備端末保管	2	–	D1	0.05
XD2	代替作業用データ保管	2	–	D3	0.01
XD3	予備プリンター保管	0	–	D6	0.03
XE1	非常時発電設備	−9.5	–	–	0.15
XE2	追加燃料の保管	−24	–	–	0.15
XE3	追加燃料安定供給契約	−8760	–	–	0.15
XF1	回線冗長化	0	–	F1	0.1
XG1	L3スイッチのバックアップ構成	0	–	G1,G2	0.3
XG2	予備ネットワーク機材をC庁舎に保管	2	–	G1,G3,G5	0.02
XH1	VPNルータのバックアップ構成	0	–	H1,H2	0.3
XH2	VPNルータの予備機材をC庁舎に保管	2	–	H1	0.02
XI1,XJ1,XK1	端末環境のイメージバックアップ化	2	E	I2,I5	0
XI2,XJ2,XK2	予備端末保管	2	–	I1	0.05
XI3,XJ3,XK3	端末用ソフトウェア保管	2	–	I3	0.01

4.6　災害による被害の見積もり

各ヘッディング項目の発生確率，復旧作業と対策案の所要時間の見積もりを行う．被害の想定各や数値の決定は策定例と初動版サンプルを参考に行った．各数値は表6～8に示す．

5　適用結果

適用を行うにあたって、計算処理の自動化を図るために，評価システムを Excel2013，VBA で開発し，これを用いて分析を行った．

5.1　現状のリスク

現状のリスク分析として，策定例での最終的な対策状態のリスク値を算出した．採用されている対策案は，表8における(XA2，XA3，VB2，XB3，XC2，XC3，XD2，XE1，XG2，XI3，XJ3，XK3)である．表9に分析結果を示す．

年金システムと介護保険システムについては目標復旧時間を達成することができているが，国民保険システムと住民記録システムは目標復旧時間を達成することができていない．つまり策定例での対策採用状況では，震度6強の地震に対して不十分であるといえる．この2つのシステムに関しては，さらに対策を講じる必要がある．

次項では，目標復旧時間を達成するために必要な対策案組み合わせの検討を行う．

表 9　現状のリスク

システム名	目標復旧時間	停止時間期待値
国民保険システム	72 時間	116.09 時間
年金システム	168 時間	116.09 時間
介護保険システム	168 時間	116.09 時間
住民記録システム	24 時間	67.27 時間

5.2　対策案の追加採用

まずは，より重要なシステムである住民記録システムの目標復旧時間を達成するための対策案組み合わせを求めたところ，現状の対策案に（XD1，XD3，XE2，XE3）を追加した対策案組み合わせのみが目標復旧時間を達成することができた．

次に（XD1，XD3，XE2，XE3）を追加採用した状態で，国民保険システムの目標復旧時間を達成するための対策案組み合わせを求める．目標復旧時間を達成することができた追加対策案の組み合わせのうち，コストが低いものを表10に示す．国民保険システムの目標復旧時間を達成するためには，最低でも対策案 XF1「インターネット回線の冗長化」を行う必要があり，さらに対策

案 XA5「サーバ用 PC の予備機材の保管」もしくは，XA6「バックアップサイトの構築」のどちらかを採用することが分かった．また目標復旧時間を達成するための最も適した追加対策案の組み合わせは（XA5，XD1，XD3，XE2，XE3，XF1）であることが分かった．

今回の適用結果から高い運用継続性を得るためには，電源や通信といった環境基盤の対策充実が必要であることが分かった．しかし目標の復旧時間を達成するためには，予備の機材を保管しておくといった各機材に対する対策も必要であり，全体のバランスがとれた対策を採用することが重要である．当手法は複数のシステムのリスク値を同時に算出することが可能であるため，対策のバランスを考える際に有用である．

表 10 目標復旧時間を達成した組み合わせ

組み合わせ	国民保険システム	住民記録システム	コスト
XA5，XD1，XD3，XE2，XE3，XF1	65.87 時間	21.96 時間	5780000 円
XA1，XA5，XD1，XD3，XE2，XE3，XF1，	62.27 時間	21.96 時間	5830000 円
XA1，XD1，XD3，XE2，XE3，XF1，XH2	56.65 時間	21.96 時間	5875000 円
XA6，XD1，XD3，XE2，XE3，XF1	57.55 時間	21.96 時間	6170000 円

6 おわりに

本稿では IT システムの運用継続性を脅かすリスクの分析手法の提案を行った．あわせて策定済みの業務継続計画を基にしたモデルに適用を行い，その問題点の指摘を行った．

今回は策定済みの資料を基に適用を行ったため想定した初期事象は一つであったが，災害の強度や別の初期事象を想定した際に，様々な変化があると考えられる．今後は複数の初期事象を想定したリスク分析を行っていく予定である．

参考文献

[1] 佐々木良一・氏田博士・小松文子・瀬戸洋一・千葉寛之・名内泰蔵・林紘一郎・原田要之助・福沢寧子・村瀬一郎・渡辺健司 (2013)『IT リスク学―「情報セキュリティ」を超えて―』共立出版.

[2] 科学技術振興機構 (2013/8/18)「Web ラーニングプラザ リスク解析技術 イベントツリー分析」 http://weblearningplaza.jst.go.jp/cgi-bin/user/lesson_start.pl?course_code=543&lesson_code=4694&now_course=543&type=force

[3] D. G. Malcolm, J. H. Roseboom, C. E. Clark, W. Fazar (1959) Application of a Technique for Research and Development Program Evaluation, *Operations Research*, Vol.7, No.5, pp.646-669.

[4] 藤本肇・上田 祐輔・佐々木良一 (2008)「デジタル署名付き文書への公開鍵暗号危殆化対策の組合せ最適化法の提案と一適用」情報処理学会論文誌, 49(3), 1105-1118.

[5] 副島 紀代 (2011)「事業継続に向けた効果的な事前／事後対策の選定手法」, オペレーションズ・リサーチ：経営の科学, 56(3), 145-150.

[6] 総務省 (2008/08/21)「地方公共団体における ICT 部門の業務継続計画策定に関するガイドライン 策定例」 http://warp.ndl.go.jp/info:ndljp/pid/283520/www.soumu.go.jp/s-news/2008/pdf/080821_3_bt6.pdf

[7] 総務省 (2013/05/08)「地方公共団体における ICT 部門の業務継続計画（ICT-BCP）初動版サンプル」 http://www.soumu.go.jp/main_content/000222226.pdf