情報システムの継続的運用計画支援システムの拡張

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 事業の中断・阻害が発生した場合であっても，一定のレベル以上の製品又はサービスを提供し続ける組織の能力を確保するための管理手法として，事業継続マネジメントを実施する組織が増加している．しかし，事業継続マネジメントシステムでは不確実性の問題に対応する必要があるため，適切に実施するのは容易ではなかった．そこで著者らは，事業継続マネジメントにおける情報システムのリスクマネジメントを支援するためイベントツリー分析と PERT 手法を組み合わせる方式を開発してきた．今回は以前提案した手法を復旧所要時間の累積度数分布を計算できるようにすると共に，結果をわかりやすく表示する方式を追加した．

An Extended Result on 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 The number of organizations to implement BCM (Business Continuity Management) has a tendency to increase, because the organization is in need of capability to continue delivery of products or services at acceptable predefined levels following disruptive incident. However the BCM is not easy, because BCM must solve the issues caused by uncertainty of the incident sequence. To solve the issue, we proposed method combined with the Event Tree Analysis and PERT to support risk management of Information system in BCM system. In this paper, we propose the extended method which calculates and illustrates the cumulative frequencies distribution on restoration time.

1 はじめに

インシデントによって事業の中断・阻害が発生した場合であっても，一定のレベル以上の製品又はサービスを提供し続ける組織の能力を確保するための管理手法として，事業継続マネジメント（以降 BCM）を実施する組織が増加している．現状では BCM を実施していない組織であっても，今後の JIS 化の動きが加速されるとなれば，早晩，重要な取引先から要求される可能性は高いといえる[1]．このことから，BCM のニーズは今後も高まっていくと考えられる．しかし，事業継続マネジメントシステム（以降 BCMS）では多くの要求事項がなされてお

り[2], 適切に実施するのは容易でなかった. これを緩和するため, 様々な分野において事業継続の研究が行われている. 特に, 土木工学の分野において盛んであり, PERT 手法を用いた効果的な対策案の選定に関する提案などが行われている[3]. また, 情報技術の分野においては, 事業継続性を高めるための ISMS フレームワークの改善案などが提案されている[4]. しかし, 情報技術の効果的な対策案の選定に関する研究は確認することができなかった. そこで, 著者らは BCMS における情報システムのリスクマネジメントを支援する方式を提案する. 以前提案した手法[5]では, イベントツリー分析と PERT 手法を組み合わせることによって, 事業継続リスクの特徴である被害発生確率と復旧所要時間の両方の変化に対応したリスク分析手法の提案を行い, 更に「組織として復旧しなければならない業務再開の目標の期間」(以降 RTO)を達成するために必要な対策案の算出を行った. しかし, 実行する必要のない作業の処理を行う段階において作業間の先行後続の関係が崩れることで正しく復旧時間の算出が行われない問題や, 分析結果の分布を考慮することが出来ないといった問題があった. 本稿では, これらの問題を解決した手法の報告を行うと共に, 分析結果の出力方法について新たに検討を行った.

2 前回の報告からの更新点

機材が故障しないことや対策が効果を発揮することによって, 実行する必要のない不要な作業が生まれる. 従来は不要な作業を作業リストから取り除いて PERT 計算を行っていた. この処理を行う際に先行後続の関係が崩れないように, 作業の先行作業や対策の効果は該当する全ての作業を指定する必要があった. これが数値決定の難解さを増長させる原因になっていた. そこで, 実行する必要のない不要な作業は所要時間を0として計算することにした. これによって, 作業の先行後続の関係が崩れることがなくなった. また, 対策案の効果設定も, 影響のある作業地点を一点指定するだけで十分になり, 数値決定が行いやすくなった.

また, 分析結果の出力についても, 対応を必要とするリスクの特定を行う際には, 復旧時間の期待値は判断の指標として適しているが, 対応を必要とするリスクの対応策を考える際には, 復旧時間の分布についても考慮する必要がある. これを解決するため, 新たな分析結果の出力方法を検討した.

上記の他に, 適用手順, ヘッディング項目の決定基準, 対策の実行条件についても更新を行った.

3 適用手順

ISO31000:2010 で規定されているリスクアセスメントプロセスに則って適用を行う[6]. リスクアセスメントの各プロセスにおいて実施される内容を 3.1～3.5 に示す. また, リスクマネジメントプロセスの関係図を基にした適用手順のフロー図と, 提案手法の対象範囲を図1に示す.

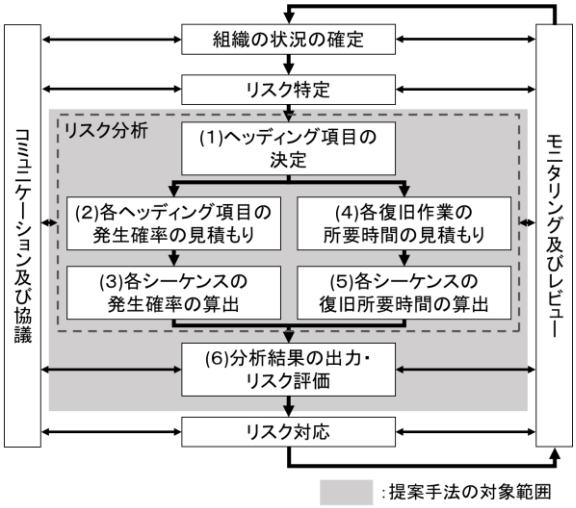

図 1 適用手順フロー図

3.1 組織の状況の確定

事業影響度分析(以降 BIA)[2]を実施し, 優先復旧目標となる重要システム, RTO, システムの最小稼働構成などの確定を行う.

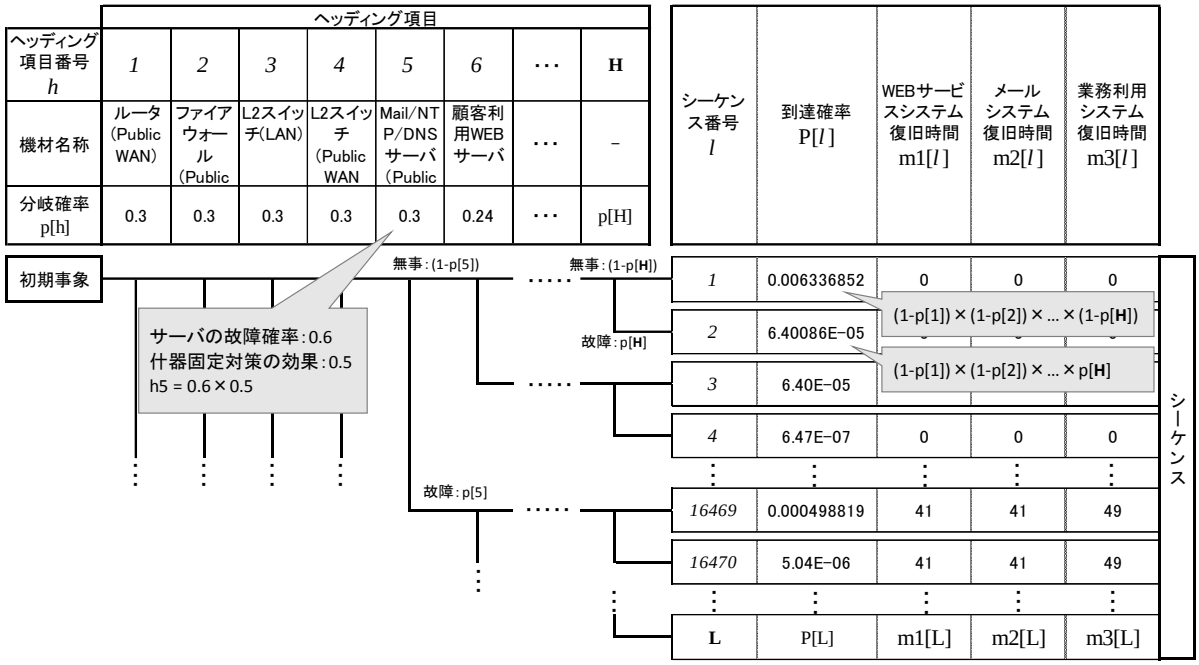

図 2 イベントツリー

3.2 リスク特定

重要システムへの影響があるリスクの洗い出しを行う. 地震や津波といった天災だけでなく, 機器の故障や断線といった事象もリスクとなりえる. ここで洗い出されたリスクを初期事象として適用を行う.

3.3 リスク分析

特定されたリスクが顕在化してインシデントが発生する可能性と, 発生した場合の被害の想定を分析する. 提案手法の(1)～(5)フェーズ(図1参照)がこのプロセスに該当する.

3.4 リスク評価

リスクの影響が受容可能か又は許容可能かを決定するために, リスク分析(3.2 項)の結果をリスク基準の RTO と比較する. 提案手法の(6)フェーズ(図1参照)がこのプロセスに該当する.

3.5 リスク対応

BIA で設定した RTO を達成するために, 分析したリスクのうちどのリスクに対策を講じる必要があるのかを選択して対応する.

提案手法のリスク分析結果を利用することによって, 円滑に判断を行うことが可能になる.

4 提案手法

4.1 提案手法の概要

被害発生確率と復旧所要時間の両方の変化に対応するために, 安全性工学で用いられるイベントツリー分析[7]とプロジェクトの工程管理に用いられる PERT 手法[8]を組み合わせてリスク分析を行う.

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. そして各被害状況から必要な復旧作業を推定し, PERT 手法に基づいて計算を行うことによっ

て，各シーケンスの所要時間を自動的に求めることができる．これらの処理によって，初期事象から発生しうる全ての被害状況を網羅した分析をすることができる．

次項から提案手法の処理について，図1に示したフェーズに沿って説明する．

4.2 ヘッディング項目の決定

イベントツリーでは，各ヘッディング事象の発生の有無によりシーケンスが分岐していく（図2参照）．事業継続リスクにおいて，各シーケンスの分岐が発生する要因は機材の故障であると考える．提案手法において，機材は2種類に分類される．システムを構成する機材と対策の実行に必要な機材である．よって，これら2種類の機材の故障に関する事象をヘッディング項目とする．

4.3 各ヘッディング項目の発生確率の見積もり

各機材の故障確率を決定する．初期事象としたリスクによって，各機材がどの程度の確率で破損するのかを見積もる．また，発生確率に効果のある対策を実行することによって，ヘッディング項目の分岐確率は変化する．

以下に計算式を示すが，各シーケンスの発生確率の算出との関連性が強いため，4.4 項と合わせて参照してほしい．

$$p[h] = p'[h] \times \mathrm{xp}[h] \qquad (1)$$

h ：h 番目のヘッディング項目
$p[\,h\,]$ ：h の分岐確率
$p'[\,h\,]$ ：h の故障確率
$\mathrm{xp}[\,h\,]$ ： h に効果を発揮する対策の効果

4.4 各シーケンスの発生確率の算出

イベントツリー分析に則って，各シーケンスの発生確率を算出する．計算式は以下のようになる．

$$\mathbf{P}[l] = \prod_{h=1}^{\mathbf{H}} \mathbf{P}'[h] \qquad (2)$$

$$\mathbf{P}'[h] = ((1 - p[h])(1 - y[h]) + p[h] * y[h]) \qquad (3)$$

$$y[i] = \begin{cases} 1: \text{ヘッディング項目}i\text{が下に展開} \\ 0: \text{ヘッディング項目}i\text{が横に展開} \end{cases} \qquad (4)$$

l ： l 番目のシーケンス
$\mathbf{P}[\,l\,]$ ：l の到達確率
$\mathbf{H}$ ：ヘッディング項目数
h ：h 番目のヘッディング項目
$p[\,h\,]$:h の分岐確率

4.5 基礎復旧作業群の洗い出し

基礎復旧作業群とは，全ての対策が失敗したとしても実行することのできる作業群である．全ての機材が破損した状況からの復旧を想定して，必要な作業を洗い出すことで決定する．

また，それぞれの復旧作業の所要時間についても見積もりを行う．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，見積もることが可能である．また，訓練の実施結果を反映することで，より精度の高い所要時間の見積もりを出すことができる．

4.6 各シーケンスの復旧所要時間の算出

各シーケンスの復旧所要時間は，PERT 手法を用いて算出する（図3参照）．PERT 手法は，各作業所要時間と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． しかし，本手法では以下の要素も考慮する必要がある．

① 複数のシステムが混在するため，終点が1つではない

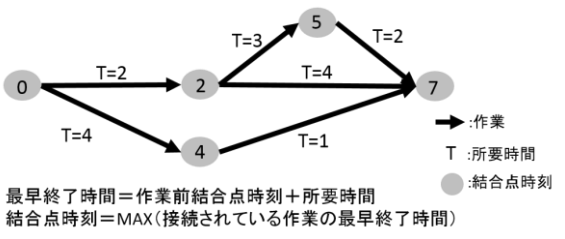

図 3 PERT

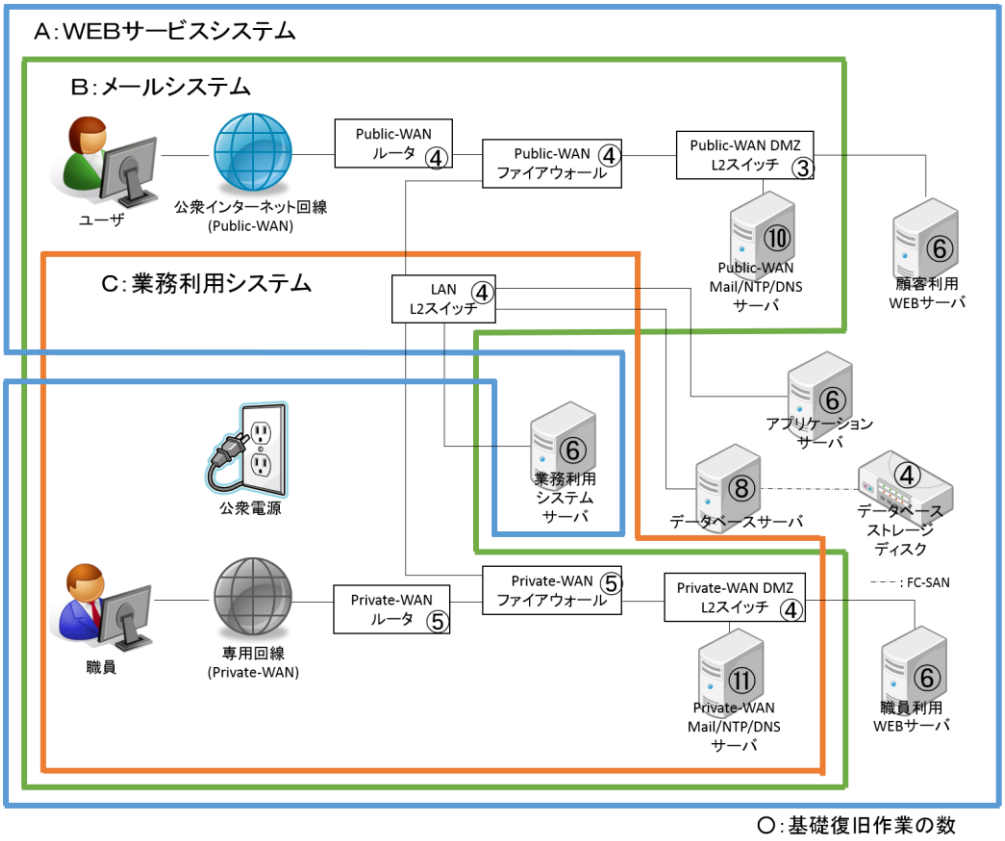

図 4 適用対象モデルの構成図

② 機材が故障しなかった場合，不要となる作業がある

③ 対策によって所要時間が短縮されることにより，不要となる作業がある

④ 対策には作業の所要時間に効果を発揮する対策と最早終了時間を置き換える対策があり，それぞれ処理が異なる

⑤ 対策を実行するために必要な機材が故障している場合，対策は実行されない

⑥ 対策を実行しない方が，所要時間が短くなる場合がある

これらの要素を踏まえながら，所要時間の算出を行う計算式を以下に示す．

システム毎に復旧終了地点となる作業を設定し，全ての復旧終了地点の終了時刻が算出されるまで試行を繰り返す． ･･･①

機材が故障しなければ，その作業の最早終了時間は 0 とする． ･･･②

$$EF[a] = ef[a] \times B(a) \quad (5)$$

a： 基礎復旧作業

EF[a]：a の所要時間

$$B(a) = \begin{cases} 1: a \text{ の対象が故障している} \\ 0: a \text{ の対象が故障していない} \end{cases} \quad (6)$$

最早終了時間を置き換える対策と最早終了時間の比較を行い，時間が短くなる方を選択する． ･･･③④⑥

$$ef[a] = MIN\{xe[a] \times C(xe[a]),\ ef'[a]\} \quad (7)$$

xe[a] ： a の最早終了時間を置き換える対策

$$C(xe[a]) = \begin{cases} 1: xe[a]\text{が実行できる} \\ \infty: xe[a]\text{が実行できない} \end{cases} \quad (8)$$

･･･⑤

最早終了時間を求める．

$$ef'[a] = ES[a] + T[a] \quad (9)$$

最早開始時間を求める.

$$ES[w] = MAX\{Pre[a]\} \quad (10)$$

Pre[a] ： a の先行作業群

所要時間に効果を発揮する対策と，所要時間の比較を行い，時間が短くなる方を選択する．･･･③④⑥

$$T[a] = MIN\{xt[a] \times C(xt[a]),\ t[a]\} \quad (11)$$

t[a] ： a の所要時間

xt[a] ： a の所要時間に効果を発揮する対策

$$C(xt[a]) = \begin{cases} 1: xt[a]\text{が実行できる} \\ \infty: xt[a]\text{が実行できない} \end{cases} \quad (11)$$

･･･⑤

4.7　分析結果の出力･リスク評価

リスク特定プロセスで洗いだしたリスクの中から対応を必要とするリスクの特定を行う際には，復旧時間の期待値を判断の指標とすることができる．期待値の計算式を以下に示す．

$$\mathbf{R} = \sum_{l=1}^{\mathbf{N}} \mathbf{P}[l] * m[l] \quad (12)$$

R ：リスク値（停止時間の期待値）

N ：全シーケンス数

l ：l 番目のシーケンス

P[l] : l の発生確率

m[l] : l の復旧所要時間

対応を必要とするリスクの対応策を考える際には，「対策を採らなかった場合の復旧時間」から，「対策をとった場合の復旧時間」の差分を求めることで，対策の効果を数値化することができる．復旧時間の期待値の差分を出すことは容易であるが，復旧時間のばらつきに関しては考慮することができない．そこで，シーケンス毎に差分を求めることでこれを達成しようと考えたが，対策の採用可否によってシーケンスの到達確率が異なるため，正しく差分を求めるのは容易ではなかった．

最終的に，復旧時間を昇順にソートし，各シーケンスの発生確率の累積とのグラフを作成することで，復旧にかかる所要時間の累積度数分布を表現することができた（図5参照）．このように見える化することによりどの対策案がよいか直感的に判断できるようになると考えられる．

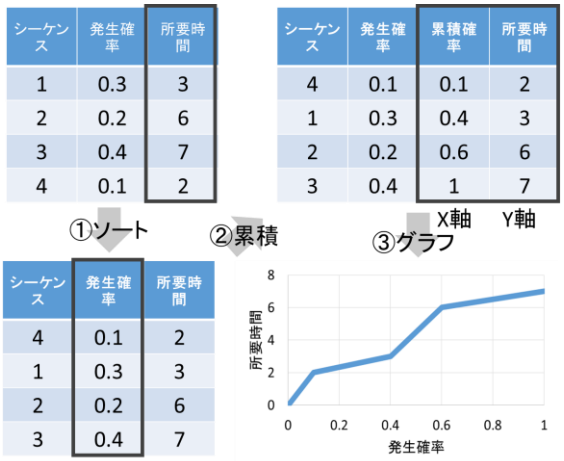

図 5 分析結果出力過程

5　適用実験

新たに導入した分析結果出力方法が，対応を必要とするリスクの対応策を決定するプロセスにおいて有用であるか検討する．実験1では対象システム全ての出力結果を生成する．実験2では対策を採用した際の出力結果を生成する．

5.1　適用モデル

適用モデルの各種設定について述べる．対象とするシステム一覧を表1に示し，適用モデルの構成図を図4に示す．図中の各機材に，基礎復旧作業との関係数も示した．また，初期事象は震度6強程度の地震を想定し，各種数値の設定を行った．各復旧作業の所要時間の設定指標を表2に，各機材の故障確率の設定指標を表3に，採用済みの対策案を表4に示す．

表 1　対象システム一覧

	名称	RTO (h)
A	WEB サービスシステム	30
B	メールシステム	100
C	業務利用システム	100

表 2 復旧所要時間の設定指標

名称	時間(h)
一般的に入手がし易い機材の調達	24
専門性がある機材の調達	92
単一性がある機材の調達	2160
各種インストール	2
各種設定	4
リストア	6
動作確認	1

表 3 故障確率の設定指標

名称	故障確率
構成機材	0.6
クラスタリング・負荷分散対策	0.8
什器固定対策	0.5

表 4 採用済みの対策案

対策案内容	所要時間	機材故障確率
各種データ関連のバックアップ保管	1	0.01
ネットワーク経由でのミドルウェア入手	14	-
ネットワーク機器の設定資料保管	1	0.01

5.2 実験結果1

実験1では，現状の重要システムの復旧所要時間を確認するために，各システムの分析を行う．出力結果を図6～8に示す．

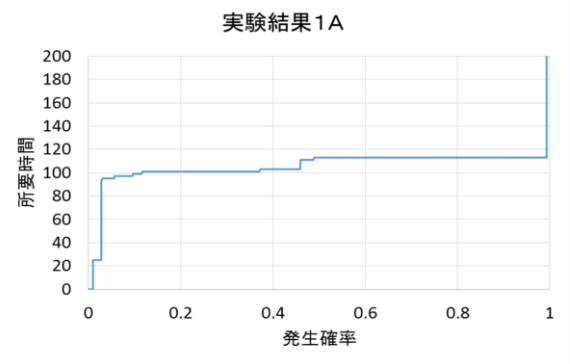

図 6 実験結果1A

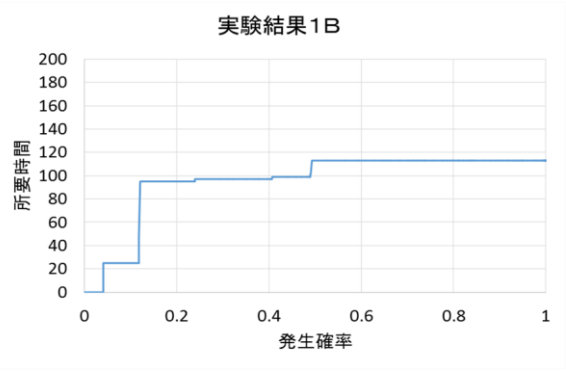

図 7 実験結果1B

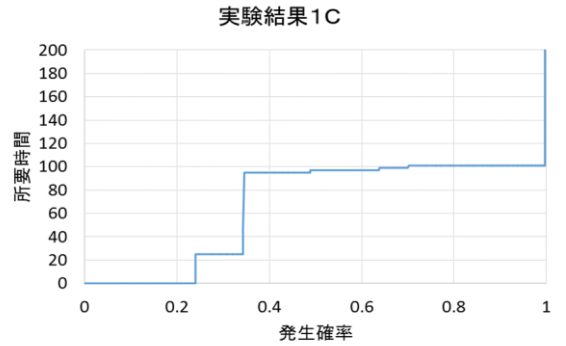

図 8 実験結果1C

5.3 実験結果2

RTO を達成するためには手段を選ばずに対策を採用したいところであるが，効果の高い対策はコスト(金額)も相応に高い．そのため，組織の資金状況に照らし合わせて対策を考えなければならないという状況は珍しくない．実験2では現状の組織の資金状況に適応する対策が X1 と X2 であり(表5参照)，そのどちらを採用するか選択を迫られている状況を想定して実験を行う．X1 は遠隔地に主だった機材を予め準備しておく対策である．また，X2 は機材の故障に備えて，代替用の機材を保管しておく対策である．対策案をそれぞれ採用した際の出力結果を図9に示す．

表 5 対策案

ID	対策案内容	所要時間	機材故障確率
X1	遠隔地の復旧拠点を用意する	48	0.01
X2	各種機材の予備を保管しておく	1	0.01

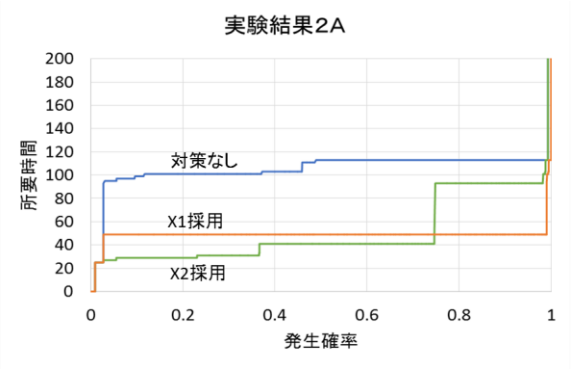

図 9 実験結果2A

5.4 考察

実験結果1には，構成機材の数が少ないほどシステムの故障確率が低いという特徴が反映されている．また，実験結果1A と1B のグラフの発生確率 0.5 付近で同様の変化が見られることから，WEB サービスシステムとメールシステムで共通している機材が所要時間のボトルネックになっているであろうことが推測できる．

実験結果2には，対策の効果が面積として現れており，X1 と X2 の効果に大きな差は無いことが見て取れる．採用する対策は，RTO が 50h を超える場合（図10，RTO：80h 参照）は，99%に近い確率で RTO を達成することのできる X1 を採用することが望ましい．今回の適用モデルの場合，WEB サービスシステムの RTO は 30h であるため，対策は X2 を採用することが望ましい．X2 を採用することによって RTO を達成することのできる確率が約 20%向上する（図10，RTO：30h 参照）．

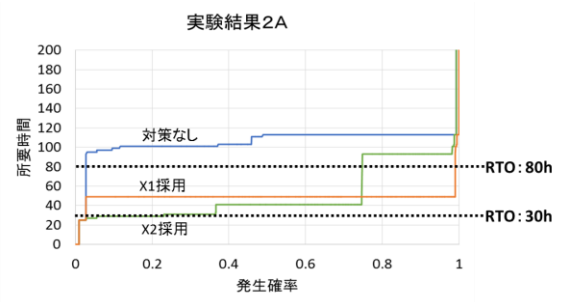

図 10 実験結果2A 考察

6 おわりに

本稿では，作業間の先行後続の関係が崩れてしまう問題の解決と，対応を必要とするリスクの対応策を決定するプロセスを支援する分析結果出力方法の導入を行った．新しく導入した分析結果出力方法は，対策案の効果がグラフ上で面積として現れることで，直感的にどの対策が有効なのか判断することができる．検討を進めることで，対策案の組み合わせに関する判断も支援することができるようになると考える．

今後は，職員の参集状況や計画停電といった，リソースの動的な変化への対応も行っていく．

参考文献

[1] 中島 一郎（編著）：ISO22301:2012 事業継続マネジメントシステム要求事項の解説，一般社団法人 日本規格協会(2013).

[2]ISO22301:2012 Societal security – Business continuity management systems – Requirements

[3] 副島 紀代，目黒 公郎：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，vol. 56， pp. 145-150，2011/03/01.

[4]頼永 忍，原田 要之助：情報セキュリティマネジメントにおける事業継続性向上に資する改善策の提案，コンピュータセキュリティシンポジウム 2013，2013/10/21.

[5]松永一朗，佐々木良一：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，コンピュータセキュリティシンポジウム 2013，2013/10/21.

[6]JIS Q 31000:2010 リスクマネジメント-原則及び指針

[7]松岡 猛，三友 信夫 and 松倉 洋史：確率論的安全評価法とその海洋分野への応用-タイタニック号事故を例にして-，International Conference on Probabilistic Safety Assessment and Management，2000/12/1.

[8]関根 智明：OR ライブラリー11 PERT・CPM，日科技連出版社(1965)