原子力分野のリスク評価技術の他分野への適用 —情報システムの信頼性評価と管理—

竹澤　伸久，中原　克彦，奥田　裕明

近年，金融機関や通信会社などで，ミッションクリティカルな情報システムが増加している．代表例として証券会社のオンライントレードシステムがあるが，これらは複雑で大規模なシステムである．これらが障害によって停止すると，多大な経済的損失と社会的影響が発生する．その信頼性を定量的に評価し向上させることは，事業リスク管理上重要である．東芝と東芝ソリューションは，原子力分野などで用いられている確率論的リスク評価（PRA）を応用した情報システムの信頼性評価・管理手法を開発している．本稿では，その手法と，金融・証券分野のオンライントレードシステムへの適用について紹介する．

キーワード：信頼性評価，確率論的リスク評価，情報システム，オンライントレードシステム

1．はじめに

近年，金融機関や通信会社などの基幹業務を担っていて停止することが許されないミッションクリティカルな情報システムが増加している．その代表例として証券会社のオンライントレードシステムがあげられる．これらは多数のハードウェアとソフトウェアが複雑に組み合わさった大規模な情報システムである．これらのシステムが障害によって停止すると，金融機関や通信会社などの基幹業務が中断して，多大な経済的損失と社会的影響が発生する．そのため，これらのシステムには，継続して正常に機能し続ける高い信頼性が要求される．このようなシステムの信頼性を定量的に評価して向上させることは，事業リスク管理の面から，企業にとって重要になっている．

一方，リスク評価の実績がある原子力分野では，1970年代に，米国原子力委員会の援助で行われた原子炉安全研究[1]で，確率論的リスク評価（PRA）（例えば文献[1]～[3]）が初めて本格的に用いられて注目されるようになった．それ以来，PRAは海外や国内の原子力プラントなどの大規模で複雑なシステムのリスク（安全性）評価に用いられ，化学プロセス分野や航空宇宙分野でも用いられている．PRAは主にハードウェアからなるシステムに用いられており，筆者らの知る限り，多数のハードウェアとソフトウェアが複雑に組み合わさった大規模な情報システムには適用されてこなかった．しかし，PRAは実績のある手法であり，様々な分野のミッションクリティカルな情報システムにも有効と考えられる．

そこで，東芝と東芝ソリューションは，原子力分野で培ったPRA技術を応用して情報システムの信頼性の評価と管理を行う手法を開発してきた．本稿では，その手法について説明し，他分野への適用例として，金融・証券分野のオンライントレードシステムへの適用について述べる．

以下では，まず，PRAを応用した情報システムの信頼性評価・管理手法について説明する．次に，その手法をオンライントレードシステムに適用するための課題と解決方法を説明する．次に，その手法の有効性を検討するために行ったフィージビリティスタディの結果を示す．最後に，結論を述べる．

2．PRAを応用した情報システムの信頼性評価・管理手法

2.1 PRAの概要

PRAは，イベントツリーとフォルトツリーを用いて，起因事象から事故に至る様々なシナリオと原因を解析して，確率論的にシステムのリスクを評価する手法である．イベントツリーは，起因事象から事故に至

たけざわ　のぶひさ，なかはら　かつひこ
㈱東芝 電力システム社 電力・社会システム技術開発センター
〒235-8523 横浜市磯子区新杉田町8
おくだ　ひろあき
東芝ソリューション㈱ 金融ソリューション事業部
〒103-0015 中央区日本橋箱崎町36-2

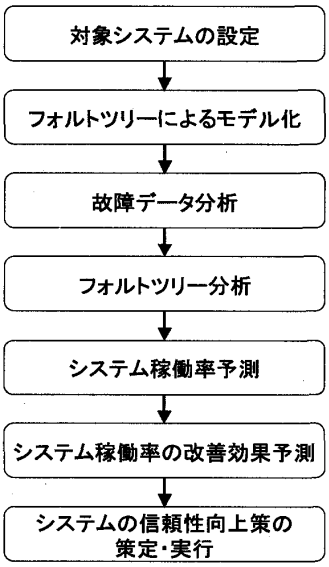

図1　PRAを応用した情報システムの信頼性評価・管理手法

る枝分かれしたシナリオのパスによって事故連鎖を記述し，それぞれの事故連鎖の発生確率を解析するために用いられる．フォルトツリーは，シナリオの好ましくない側の分岐（例えば，安全系の作動失敗）の原因と発生確率を解析するために用いられる．

2.2　PRAを応用した情報システムの信頼性評価・管理手法の手順

図1はPRAを応用した情報システムの信頼性評価・管理手法の手順を示したものである．本手法では，フォルトツリーを用いて，多数の機器で構成されたシステムをモデル化することによって，システムの信頼性を定量的に評価する．その手順の概要は次の通りである．

(1) 対象システムの設定

評価の対象とするシステムとその範囲を設定する．

(2) フォルトツリーによるモデル化

フォルトツリーの頂上事象にシステムで発生することが望ましくない事象を設定する．例えば，重要なサービス機能の停止など，システムが担っているビジネスの継続を困難にするシステム障害を設定する．次に，頂上事象の発生要因を段階的に検討し，それ以上展開できない要因である基本事象を求める．基本事象は，機器や部品などの故障現象や故障状態，ソフトウェアのバグによる停止などである．さらに，基本事象から頂上事象に至る関係を表すフォルトツリーを構築する．

(3) 故障データの分析

既存のシステムの場合には，過去の基本事象の発生間隔データ（故障間隔データ）を確率・統計的に分析することにより，基本事象の発生率（故障率）と平均修復時間を推定する．また，新規のシステムの場合には，過去の分析データや公開データなどから，該当する基本事象の故障率と平均修復時間を取得する．

(4) フォルトツリー分析

フォルトツリーと基本事象の故障率を用いて，頂上事象の発生確率を求め，システムの信頼度を評価する．さらに，各基本事象の発生確率が頂上事象の発生確率にどの程度寄与しているかを示す各基本事象の重要度を定量的に評価し，重要な基本事象を抽出する．

(5) システム稼働率の予測

フォルトツリー，基本事象の故障率，ならびに平均修復時間を用いて，頂上事象の発生確率の時間推移についてモンテカルロシミュレーションを行い，システム稼働率を予測する．

具体的には，時刻t_iにおける基本事象の故障率$r(t_i)$から時間ステップΔt_i間の故障発生確率$r(t_i)\Delta t_i$を導出し，その値と乱数の大小比較によって基本事象の状態を評価する．その上で，フォルトツリーに基づいてシステムの状態を評価する．この際，基本事象が発生した場合は，時間が平均修復時間だけ経過するまで故障状態が継続するとする．これらを評価期間の最初から最後まで時間ステップを進めるごとに繰り返して，システムの状態の時間推移を求める．これにより，その試行におけるシステム機能停止時間がわかるので，システム稼働率を計算できる．この試行をシステム稼働率の統計平均値が収束条件に達するまで多数回繰り返すことにより，システム稼働率の評価結果を得る．さらに，頂上事象の主な発生要因になり，システム稼働率の向上にとって重要な基本事象を評価する．

次に，システム機能停止による損害額や設備の修復費用などのコストを評価する．具体的には，得られたシステム稼働率Aから，式(1)によって，一定の評価期間におけるシステム機能停止による損害額の期待値C_Sを評価する．

$$C_S=(1-A)\cdot T\cdot c \tag{1}$$

ここで，Tは評価期間，cは単位時間当たりのシステム機能停止による損害額である．また，各試行における設備の修復費用を算出して平均値を取ることにより，設備の修復費用の期待値を評価する．

(6) システム稼働率の改善効果予測

基本事象の故障率や平均修復時間あるいはシステムの構成をパラメータとして，システム稼働率の改善効

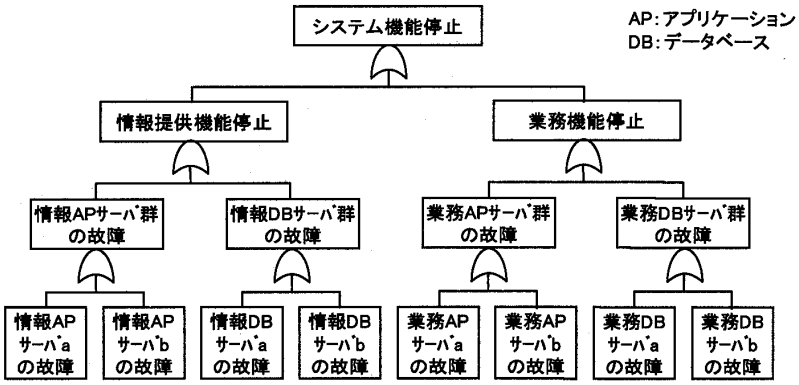

図2　フォルトツリーの展開の例

果を予測し，システム稼働率目標の達成に必要な改善項目を抽出する．さらに，改善のための設備費，システム機能停止による損害額，設備の修復費用などのコストを評価し，投資対効果を最大化する改善方法を検討する．

(7) システムの信頼性向上策の策定・実行

上記(6)で得られた結果を用いて，システムの信頼性向上策を策定し実行する．それによって，システムの信頼性を向上させることができる．さらに，これらの手順を定期的に行うことにより，システムの高い信頼性を維持することが可能となる．

2.3 PRAを応用した情報システムの信頼性評価・管理手法の期待効果

本手法を用いることによる期待効果としては，次のようなことがあげられる．

- 現状のシステムの稼働率を確認することができる．
- 様々なシステム構成をフォルトツリーでモデル化して，その違いが信頼性に及ぼす効果を事前に評価できる．
- 基本事象の重要度を定量的に評価することによって，改善項目の優先順位がわかり，有効な信頼性向上策の策定を支援できる．
- システム機能停止による損害額の期待値がわかるため，システム稼働率の改善策の投資対効果を定量的に把握でき，事業リスク管理の意思決定を支援できる．
- 平均修復時間短縮によるシステム稼働率の改善効果を定量的に評価することにより，システム稼働率の目標達成に必要な修復時間がわかり，その達成のための障害対策を策定できる．

3. オンライントレードシステムへの適用方法

大規模な情報システムでは，多数の多様なハードウェアやソフトウェアで構成されたプラットフォーム上で，独自に構築されたアプリケーションソフトウェアが動作する．ハードウェアは，サーバ等の機器に展開でき，さらにCPU等の部品に展開できる．ソフトウェアは，OSやミドルウェア等に展開でき，さらにこれらを複数の機能に分解したモジュールに展開できる．このように，大規模な情報システムは多数の多様なハードウェアとソフトウェアが物理的・論理的に複雑に組み合わさっているため，前節に示した手法をオンライントレードシステムに実際に適用するのは簡単ではない．そのための課題とその解決方法は以下の通りである．

3.1 フォルトツリーの頂上事象の設定

頂上事象にはビジネス上重要なサービス機能の停止を設定するべきだが，システムが様々なサービス機能を提供しているとその判断は容易ではない．そこで，システムの開発者や運用者へのヒアリングと過去の故障データの分析を行い，そのサービス機能の停止によって実際に利用者に問題が生じたものを重要と判断して頂上事象とした．

3.2 多数の構成要素の取扱い

システムが多数の多様な構成要素からなるので，フォルトツリーが複雑で理解し難くなる．そこで，同様な機能を持つ複数のサーバで構成されるグループにシステムを分割できる点に注目した．まず，機能単位でフォルトツリーを構築し，次に，これをサブ機能単位に展開し，さらに，最小単位である基本事象に順次展開した．これにより，図2の例のようにフォルトツリ

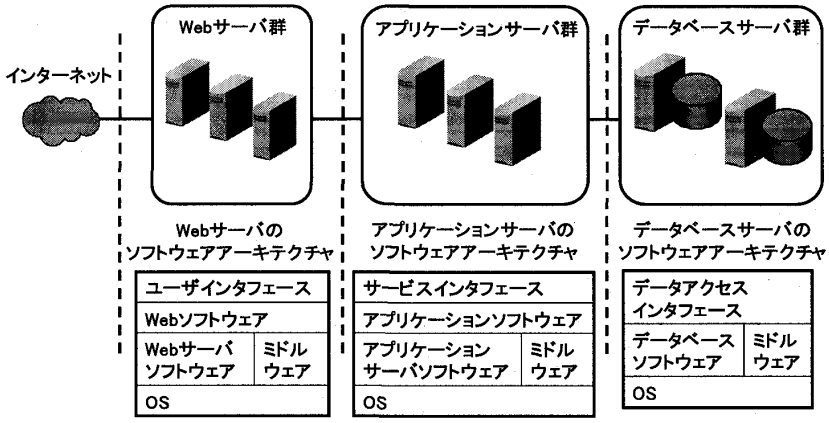

図3　Webシステムのソフトウェアアーキテクチャ

ーを簡潔に表現できる．

3.3　基本事象の展開レベルの設定

大規模な情報システムでは，基本事象として，サブシステム，機器，部品などの様々なレベルの故障が考えられる．基本事象をどのレベルの故障に設定するかは，故障データが取得されているレベルやデータ数等に依存するため，単純にシステム構成のみから設定できない．

そこで，ハードウェアの基本事象を，故障率を推定可能なデータ数の揃うサブシステム，あるいは機器，あるいは部品のレベルの故障で設定する．また，ソフトウェアの基本事象を，図3のようなソフトウェアアーキテクチャを考慮して設定する．このソフトウェア分類をさらにモジュールにも展開できるが，情報システムでは様々なソフトウェアが複雑に関連し合っており，故障の原因をモジュール単位で特定できない場合もある．また，システム運用上，手間をかけてモジュールレベルまでさかのぼって故障の原因を特定していない場合もある．したがって，各分類の詳細にまで立入ってモジュールの故障データを得るのは現実的ではない．そこで，実用的な見地から，OSやミドルウェア等の分類レベルの故障に基本事象を設定する．これにより，図4のように，ソフトウェア間の関係を簡潔に表現できた．

3.4　システムの境界の設定と外部システムの組み込み

大規模な情報システムは，社内の既存システムや社外のシステムなどの外部システムとLANやインターネットを介して接続している．そのため，外部システムの故障に起因してシステムのサービス機能が停止することもある．このような外部システムの影響をどのように取り入れるかが問題となる．そこで，外部システムとの間に境界を定義して，システムの故障の原因となる外部システムの故障をまとめて1つの基本事象とすることにより，システムのフォルトツリーに組み込んだ（図5）．

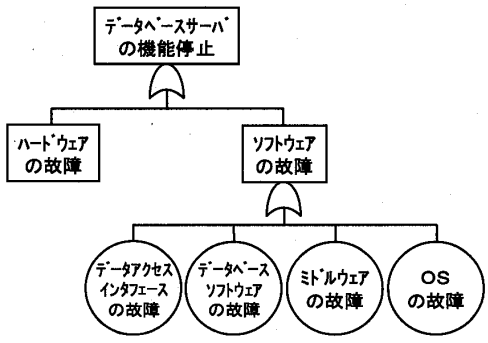

図4　データベースサーバのフォルトツリーの例

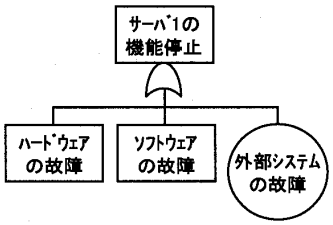

図5　外部システムの故障のフォルトツリーへの組み込みの例

3.5　冗長化構成のモデル化

高い信頼性を要求されるミッションクリティカルな情報システムでは，信頼性向上のため，様々な冗長化構成がとられており，これらの構成をフォルトツリーに組み込む必要がある．

代表的な構成に，クラスタリングとホットスタンバイがある．クラスタリングでは，サーバ2台がサーバ群を構成し，それぞれ処理を行っている．各サーバが相互に監視して，片方のサーバが故障すると，その処理を引き継いでもう片方のサーバが2台分の処理を行

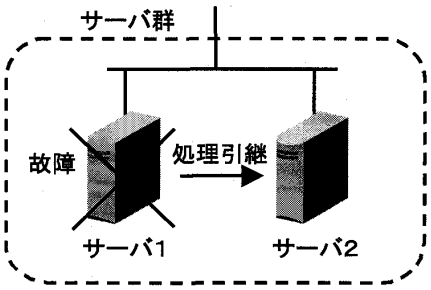

図6　クラスタリングの説明図

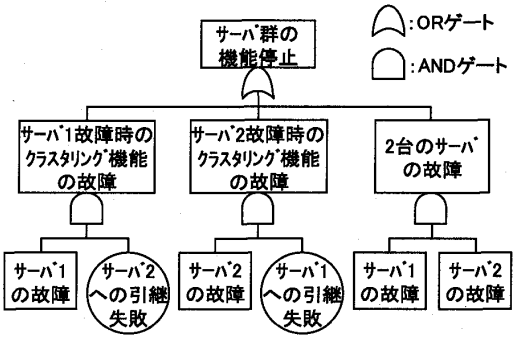

図7　クラスタリングのフォルトツリー

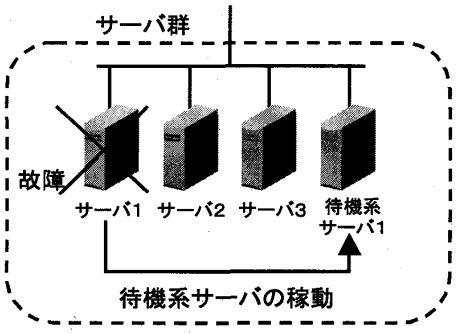

図8　ホットスタンバイの説明図

う（図6）．この場合，サーバ1台の故障時にクラスタリングの機能そのものが故障することも考慮し，サーバ1台が故障したときに処理引き継ぎに失敗するか，サーバが2台共故障した場合にサーバ群全体が機能停止するとしてフォルトツリーを構成した（図7）．ホットスタンバイでは，主系サーバと通常時は利用していない待機系サーバがサーバ群を構成している．待機系サーバは主系サーバを監視し，主系サーバが故障すると，故障したサーバの代わりに稼動する（図8）．この場合，待機系サーバの台数よりも故障したサーバの台数が多ければサーバ群が機能停止するとして，m-out-of-nゲートによってフォルトツリーを構成した（図9）．m-out-of-nゲートは，n個の入力事象の内，m個以上の入力事象が発生したときに出力事象が発生することを表すものである．図9は2-out-of-

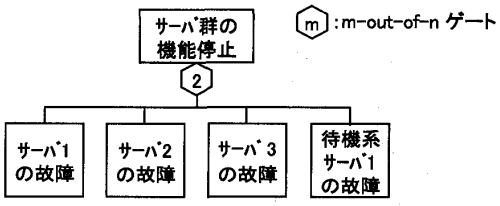

図9　ホットスタンバイのフォルトツリー

4ゲートで表される例である．このようにして，冗長化構成をフォルトツリーに取り込んだ．

(6) ソフトウェアの信頼性の評価方法

ソフトウェアには，運用後もバグの修正，機能追加，修正パッチの適用等の様々な変更が加えられる．そのため，ソフトウェアの故障率の評価にあたっては，ソフトウェアの大幅な変更の時期や故障データの期間等に注意して故障データを整理する必要がある．

4. フィージビリティスタディの結果

本手法の有効性を検討するため，前節の方法を用いて，稼動中のサーバ100台以上で構成されるシステムの主要なサブシステムに関する信頼性評価を行った．評価にあたっては，過去5年間に発生した故障データを用いた．

頂上事象の設定にあたっては，そのサービス機能の停止によって実際に利用者に問題が生じたものを抽出し，そのいずれかの停止を頂上事象と定義した．また，ハードウェアの基本事象を機器レベルの故障，ソフトウェアの基本事象を図3に示したソフトウェア分類のレベルの故障とした．基本事象の故障率の推定にあたっては，まず，故障間隔tの分布関数（非信頼度）$F(t)$として，式(2)で表されるワイブル分布を仮定して最尤法でパラメータを推定した．

$$F(t)=1-\exp\left[-\left(\frac{t}{\eta}\right)^m\right] \tag{2}$$

ここで，mは形状パラメータ，ηは尺度パラメータである．推定されたmとηを用いて，故障率$r(t)$は式(3)によって求められる．

$$r(t)=\frac{m}{\eta}\left(\frac{t}{\eta}\right)^{m-1} \tag{3}$$

次に，現状分析を行い，頂上事象の発生確率（非信頼度）に対する基本事象の重要度を定量的に評価した．基本事象iの重要度としては，式(4)で表されるクリティカリティ重要度（例えば文献[3][4]）を用いた．

$$CI_g(i)=\frac{\partial g}{\partial q_i}\frac{q_i}{g} \tag{4}$$

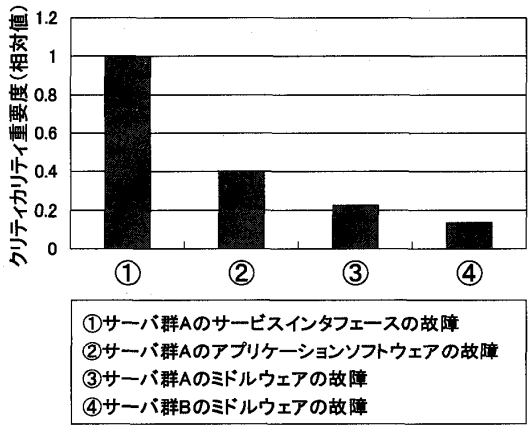

図10　基本事象のクリティカリティ重要度（相対値）

ここで，gは頂上事象の発生確率，q_iは基本事象iの発生確率である．これは基本事象の発生確率の変化に対する頂上事象の発生確率の変化の比であり，この値が高い基本事象の改善ほどシステムの信頼性の改善に寄与することを意味する．図10に上位4つの基本事象の重要度を示す．この結果，これらのソフトウェアの故障が頂上事象の発生の主要因であることがわかった．また，これら4つの要因の発生確率（非信頼度）を1/10にすると，システム非信頼度が約46.6%低減する結果も得られた．

さらに，システム稼働率をモンテカルロシミュレーションによって評価した．評価期間を1年とし，収束条件をシステム稼働率の相対誤差1.0×10^{-5}以下として評価を行った結果，1年間のシステム稼働率は約99.9%となることが明らかとなった．この結果と単位時間当たりのシステム機能停止による損害額から，式(1)を用いて，1年間のシステム機能停止による損害額の期待値を評価できることになる．また，基本事象の平均修復時間をパラメータとしてシステム稼働率を定量的に評価し，システム稼働率の目標を修復時間の短縮によって達成する場合の目安となる平均修復時間を評価できることを確認した．

5. おわりに

PRAを応用した情報システムの信頼性評価・管理手法と，オンライントレードシステムへの適用方法について述べた．さらに，そのフィージビリティスタディにより，この手法がオンライントレードシステムのハードウェアだけでなく，重要な故障要因になるソフトウェアも含めた信頼性の定量的評価と信頼性向上策の評価・検討に適用できることを確認した結果を示した．

この手法は様々な分野のミッションクリティカルな情報システムに適用でき，それらを構築や運用する企業の事業リスク管理を支援することができる．この手法は，証券会社のオンライントレードシステムだけでなく，例えば，銀行のオンラインシステム，クレジットカード会社のオンラインシステム，旅行会社や航空会社のオンライン予約システムなど，様々な分野の情報システムにも適用可能である．

参考文献

[1] USNRC: "Reactor safety study: An assessment of accident risk in U.S. commercial nuclear plants," USNRC, WASH-1400, NUREG-75/014, 1975.

[2] N. J. McCormick: "Reliability and Risk Analysis," San Diego, Academic Press, 1981.

[3] E. J. Henley and H. Kumamoto: "Probabilistic Risk Assessment," IEEE Press, 1992.

[4] 北川賢司:『最新設計審査技術』, テクノシステム, 1987.