オンライン取引システムの信頼性評価

Reliability Analysis of Online Trading Systems

竹澤　伸久　　奥田　裕明　　佐久間　晃

■TAKEZAWA Nobuhisa　■OKUDA Hiroaki　■SAKUMA Akira

証券会社のオンライン取引システムは，大規模かつ複雑な情報システムである。障害が起これば多大な経済的損失を生じるため，高い信頼性が要求される。企業にとって，システムの信頼性を評価し向上を図ることは，事業リスク管理の観点から重要である。

東芝は東芝ソリューション（株）と共同で，原子力プラントで実績のある確率論的安全評価手法を応用した情報システムの信頼性の評価と管理のための手法（以下，信頼性評価・管理手法と略記）を開発している。今回，オンライン取引システムへ適用し，ハードウェアとソフトウェアを含む信頼性の定量的評価ができること，及び信頼性向上策の評価・検討に有効なことを確認した。

The online trading system of a securities company is a complicated large-scale information system. Since the failure of such a system will cause serious economic loss, high reliability must be maintained. Hence, from the standpoint of enterprise risk management, it is important for enterprises in this business field to evaluate and improve the reliability of their online trading systems.

Toshiba Corp. and Toshiba Solutions Corp. are developing a reliability assessment and management method for information systems applying probabilistic safety assessment (PSA) techniques used in nuclear power plants. This method is capable of quantitatively evaluating the reliability of an online trading system in terms of both hardware and software. It is therefore effective for the examination and evaluation of reliability improvement measures.

1　まえがき

近年，金融機関や通信会社などで，ミッション クリティカルなオープンシステムが増加している。証券会社のオンライン取引システムはその代表例である。これらは，大規模で多数のハードウェアやソフトウェアが複雑に組み合わさった情報システムであることが多く，障害が発生して停止すると，企業は業務の中断によって多大な経済的損失を受けるため，絶え間なく正常に機能し続ける高い信頼性が要求される。システムの信頼性を定量的に把握して向上を図ることは，事業リスク管理の面から，企業にとっていっそう重要になっている。

これまでに，東芝は東芝ソリューション（株）と共同で，原子力分野で広く用いられる確率論的安全評価（PSA）手法[(1)]を応用した災害・障害リスク管理ソリューション[(2)]を開発してきた。これは，地震などの災害による情報システムのリスクを定量的に評価し，投資対効果を考慮した最適な災害対策の意思決定を支援するものである。その経験に基づき，現在，日常起こる情報システムの故障や障害に対するソリューションとして，PSA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。ここでは，その手法の概要と，オンライン取引システムへの適用について述べる。

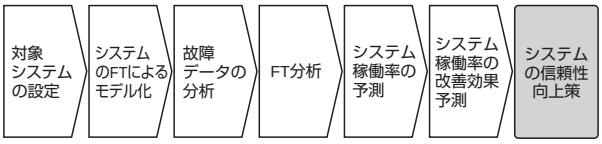

図1．PSAを応用した情報システムの信頼性評価・管理手法の手順 ―一連の手順により，システム稼働率目標の達成に必要な改善項目や投資対効果を最大化する改善方法がわかる。それにより，システムの信頼性向上策の策定とシステムの信頼性向上が図れる。

Procedure of reliability assessment and management method for information systems applying PSA techniques

2　PSAを応用した信頼性評価・管理手法の概要

PSAは，海外や国内の原子力プラントの安全性評価に用いられるもので，当社でも実績がある。それは確率論を用いてシステムの安全性を評価する手法であり，多数の機器で構成されたシステムをフォルトツリー（FT）でモデル化することにより，システムの信頼性を定量的に評価できる。

図1は，PSA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，概要は次のとおりである。

⑴　対象システムの設定　　評価の対象とするシステムの範囲を設定する。

⑵　システムのFTによるモデル化　　FTの頂上事象（シ

ステムで発生することが望ましくない事象)を設定し，次に，頂上事象を発生させる要因となる基本事象(機器や部品などの故障現象や故障状態)を設定する。それに基づき，FTを構築する。

⑶ 故障データの分析　既存システムの場合，過去の基本事象の故障間隔データを確率・統計的に分析することにより，故障率と平均修復時間(MTTR)を推定する。新規システムの場合，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MTTRを取得する。

⑷ FT分析　FT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。更に，頂上事象の発生に対する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。

⑸ システム稼働率の予測　FT，基本事象の故障率，及びMTTR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。更に，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。

⑹ システム稼働率の改善効果予測　基本事象の故障率やMTTR又はシステム構成をパラメータとして，システム稼働率の改善効果を予測し，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。更に，改善のための設備費やシステム機能停止による損害額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。

このようにして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ことにより，システムの信頼性を向上させることができ，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できる。

3 オンライン取引システムへの適用方法

オンライン取引システムは，多種多様なハードウェア(サーバ，ネットワーク機器など)やソフトウェア(基本ソフトウェア(OS)やミドルウェアなど)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，大規模で複雑なオープンシステムである。

ハードウェアは，まずサーバやネットワーク機器などの機器に展開でき，更に，CPUや内蔵HDD(ハードディスク装置)などの部品に展開できる。ソフトウェアもこれと同様に，OS，ミドルウェア，アプリケーションソフトウェアなどに展開でき，更に，機能単位に分解したモジュールに展開できる。オンライン取引システムは，これらの多数の多様なハードウェアとソフトウェアを物理的，論理的に複雑に組み合わせたものである。そのため，前章の手法を適用するためには様々な課題を解決する必要があり，それらの課題と解決方法をまとめると，次のとおりである。

3.1 頂上事象の設定

システムのFTの頂上事象には，ビジネス上重要なサービス機能の停止を設定する必要がある。しかし，それはシステムの構成情報だけではわからないので，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利用者に実際に問題が生じたものを抽出する。抽出されたサービス機能の停止を重要と判断し，頂上事象とする。

3.2 多数の構成要素の取扱い

大規模なオープンシステムは，多数の多様な構成要素から成るので，FTが複雑で理解しにくくなる可能性がある。そこで，オープンシステムが，同様の機能を持つ複数のサーバで構成されるグループに分割できる点に注目する。この特徴を利用して，まず機能単位でFTを構築し，これをサブ機能単位，更に最小単位である基本事象に展開していく。これにより，FTを簡潔に表現することができる。

3.3 基本事象の展開レベルの設定

大規模なオープンシステムでは，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が考えられる。この展開レベルは，故障データの得られるレベルや故障データ数などに依存するため，単純にシステム構成だけから設定できない。

そこで，ハードウェアに関しては，有意な故障率の推定ができるデータ数のそろうレベルで基本事象を設定する。ソフトウェアに関しては，ソフトウェア アーキテクチャを考慮する。一般的にウェブシステムのソフトウェア アーキテクチャは**図2**のようになっており，このソフトウェア分類を更にモジュールに展開できる。しかし，オープンシステムでは様々なメーカーのソフトウェアが用いられるため，各分類の詳細にまで立ち入ってモジュールの故障データを得るのは現実的には困難である。このため，展開レベルをソフトウェア分

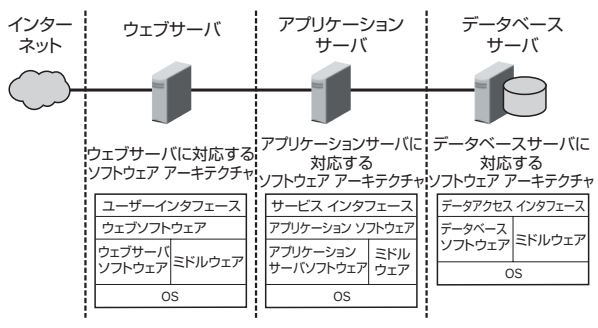

図2．ウェブシステムのソフトウェアアーキテクチャ ― これらのソフトウェアの各分類レベルで基本事象を設定することにより，ソフトウェア間の関係を簡潔に表現できる。

Software architecture of Web systems

類までにして，OSやミドルウェアなどの各分類レベルで基本事象を設定する。それにより，ソフトウェア間の関係を簡潔に表現できる。

3.4　システムの境界の設定と外部システムの組込み

オープンシステムは，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やインターネットなどを介して接続しており，これらの外部システムとの境界が明確ではない。そこで、その境界を適切に定義したうえで，これらの外部システムの故障をひとまとめにして一つの基本事象とすることにより，対象システムのFTに組み込む。

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 クリティカルなオープンシステムでは，信頼性向上のために，様々な冗長化構成がとられており，FTにはこの構成を組み込む必要がある。

代表的な構成には，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。片方が故障した場合，もう片方が2台分の処理を行う。この場合，クラスタリング自体の失敗も考慮し，サーバ1台が故障したときにクラスタリングが失敗するか，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FTを構成する(**図3**)。ホットスタンバイでは，主系サーバと待機系サーバがサーバ群を構成し，主系サーバが故障した場合，待機系サーバに処理を引き継ぐ。この場合，待機系サーバの台数よりも主系サーバの故障する台数が多ければサーバ群全体が機能停止するとして，m-out-of-nゲート(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)でFTを構成する。**図4**は主系サーバ3台と待機系サーバ1台の例だが，このようにして，冗長化構成をFTに整合的に取り込むことができる。

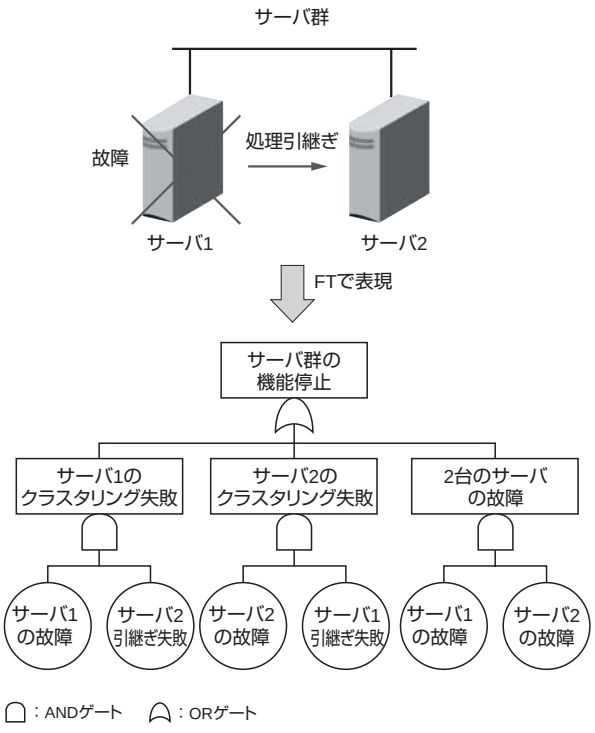

図3．クラスタリングのFT表現 ― サーバ1台が故障したときにクラスタリングが失敗するか，サーバが2台共故障した場合にサーバ群全体が機能停止するとして，FTを構成する。

Fault tree representation of clustering

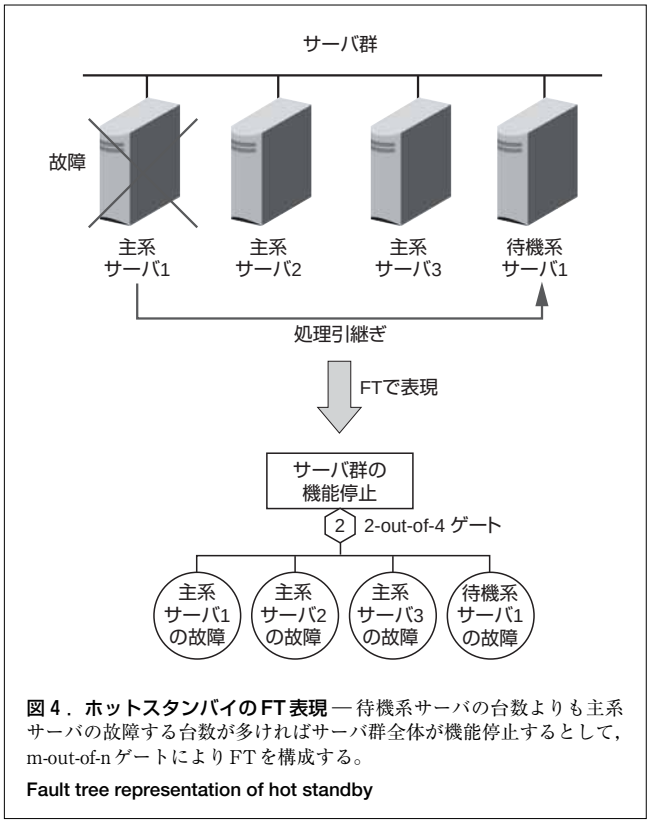

図4．ホットスタンバイのFT表現 ― 待機系サーバの台数よりも主系サーバの故障する台数が多ければサーバ群全体が機能停止するとして，m-out-of-nゲートによりFTを構成する。

Fault tree representation of hot standby

3.6　ソフトウェアの信頼性の評価方法

ソフトウェアの故障データ分析では，ハードウェアとの違いを考慮する必要がある。ソフトウェアには，運用後もバグの修正，機能の追加，修正パッチの適用など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，これらの変更の時期や故障間隔データの期間などに注意する必要がある。

4　オンライン取引システムへの適用性の評価結果

この手法の適用性を評価するため，稼働中のシステムの主要部分の信頼性評価を行った。評価には，過去5年間の故障データを用いた。

頂上事象の設定にあたっては，対象システムが提供するサービス機能の中から，実際にその停止によって利用者に

問題が生じたものを抽出し，そのいずれかのサービス機能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はサーバなどの機器レベル，ソフトウェアの基本事象は図2のソフトウェア分類のレベルとした。各基本事象の故障率は，ワイブル分布を仮定した最尤（さいゆう）法によって推定した。

この故障率と前章の方法で構築したFTを用いて現状分析を行い，頂上事象の発生に対する基本事象の重要度を定量的に評価した。**図5**は，上位四つの基本事象の重要度を示したものである。この結果，これらのソフトウェアの故障が頂上事象の主な発生要因になることがわかった。また，これら四つの基本事象の発生する確率（非信頼度）を1/10にすると，システムの非信頼度が約46.6％低減する結果も得られた。

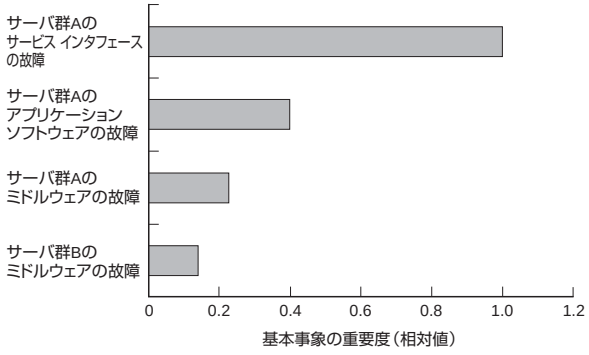

図5．基本事象の重要度 ― 頂上事象の発生要因になる上位四つの基本事象の重要度を示している。この結果から，これらの要因に対する対策がシステムの信頼性の向上に有効であることがわかる。

Importance of basic events

システム稼働率をモンテカルロシミュレーションで評価した結果，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。オンライン取引システムのシステム停止による損害額を7億円/時間[3]とすると，損害額の期待値は約61億円/年となる。このように損害額の期待値がわかると，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るようになり，事業リスク管理に関する意思決定に有効な情報を提供できる。また，基本事象のMTTRをパラメータとして，MTTRとシステム稼働率との関係を定量的に評価し，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MTTRを把握することができた。

以上から，この手法がオンライン取引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まで含めた信頼性の定量的評価に適用できることがわかった。これにより，様々な構成のシステムをFTでモデル化することで，システム構成の違いがシステム信頼性に及ぼす効果を事前に評価できるようになった。また，頂上事象の発生に対する各基本事象の重要度を定量的に評価できるため，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する情報が得られた。更に，基本事象のMTTR短縮によるシステム稼働率の改善効果を定量的に評価できるため，システム稼働率の目標達成に必要なMTTRがわかり，それを保証するためのシステム障害対策の策定が可能となった。

5 あとがき

PSAを応用した情報システムの信頼性評価・管理手法の概要と，オンライン取引システムへの適用方法を述べた。更に，その適用性評価により，この手法がオンライン取引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・検討に有効なことを確認した。

こうした手法は，情報システムを運用する様々な業界の企業の事業リスク管理にも適用できるものである。今後は，証券のオンライン取引システムだけでなく，銀行のオンラインシステム，クレジットカードのオンラインシステム，旅行や航空券のオンライン予約システムなど，様々な業界の情報システムに適用先を拡大して行く。

文　献

(1) McCormick, N. J. Reliability and Risk Analysis. San Diego, Academic Press, 1981, 458p.
(2) 災害･障害リスク管理ソリューション．東芝レビュー．**59**, 3, 2004, p.85.
(3) Kembel, R. Fibre Channel: A Comprehensive Introduction. Tucson, Northwest Learning Associates, 2000, 630p.

竹澤　伸久　TAKEZAWA Nobuhisa, D.Sc.

電力・社会システム社 電力・社会システム技術開発センター システム解析技術開発部主務，理博。リスク評価応用技術の研究・開発に従事。日本物理学会，日本原子力学会，日本金融・証券計量・工学学会会員。

Power and Industrial Systems Research and Development Center

奥田　裕明　OKUDA Hiroaki

東芝ソリューション（株）ソリューション第二事業部 証券ソリューション部主幹。金融システムの開発に従事。

Toshiba Solutions Corp.

佐久間　晃　SAKUMA Akira

電力・社会システム社 情報制御事業推進室参事。リスク評価と安全規格への適合を支援する業務に従事。

Information & Control Solution Dept.