Vol.2010-IOT-8 No.15
2010/3/1

ネットワークサービスの可視化を主眼に置いた戦略的監視手法の提案

川崎敏行† 和﨑克己††

近年，インターネットの普及によって，多くの企業および学校，官公庁でインターネットを利用したミッションクリティカルなシステムが増加してきている．そのため，今まで以上にシステムの高可用性が必要とされるようになってきた．しかし，一方でシステムの大規模化，複雑化が進み，限られたシステム運用者リソースで全てのイベントに対応することが困難になってきている．本研究では，この問題に対応するため，ネットワークサービスの可視化という概念を取り入れ，システム運用者の監視業務を支援するシステム改善方法を提案する．これによって，限られたシステム運用者リソースで大規模複雑化したシステムを管理することが可能となり，システムの可用性を重視した運用方針の戦略を立てることが可能となる．

Proposal for Strategic Monitoring Methodology with an Emphasis on the Visibility of Network Services

Toshiyuki Kawasaki† and Katsumi Wasaki††

With th e sp read of Int ernet in re cent years, t here a re in creasing nu mbers of Internet-based m ission-critical systems at companies, s chools, and gover nmental agencies which makes th e high availability of s ystems more important th an eve r. However, as systems grow in scale and complexity, it beco mes difficult to handle all of the possible event s that can ar ise using only limited syst em a dministrator resou rces. In this stud y, to d eal with th is issu e, we p ropose a method of i mproving s ystems fo r supporting monitoring tasks and operations of system administrators by incorporating the concept of visibility of n etwork s ervices. T his method makes it pos sible for s ystem administrators to manage l arge and co mplicated s ystems using li mited system administrator r esources thus allo wing them to de velop ope ration strategies w ith a n emphasis on system availability.

1. はじめに

近年，インターネットの普及によってさまざまなネットワークサービスが提供されるようになった．例えば，オンライントレード，オンラインバンキング，オンラインショッピング，各種行政申請等その種類は多岐に渡る．一方，ネットワークサービスを構成するネットワーク機器やサーバ機器（以下，機器）は，冗長化構成，分散化構成の採用により，大規模複雑化が進んでいる状況である．

ネットワークサービスの普及に伴い，システム運用の方式も変化してきている．例えば，現在はシステム運用コストの削減，各種ASP（Application Serv ice Provider）サービスの効率的な利用を目的に，外部のシステムアウトソーシング業者に業務を委託する事例が増えてきている[1].

多くのネットワークサービスは，高い利便性とシステム可用性が求められる状況[2]であるが，障害イベント（以下，イベント）発生時のサービス影響範囲の特定は困難を要する作業である．これまでも，システム運用者（以下，運用者）のスキルレベルや熟練度に大きく左右される状況であったが，外部のシステムアウトソーシング業者の参入に伴い，運用者の対応品質を高品質に均一化することがさらに困難になってきている．また，システムの大規模複雑化により，高いスキルレベルや経験を有する運用者であっても，システム同士の依存関係を完璧に把握することは大変困難な状況であると考えられる．

本研究報告では，システムの依存関係をブール代数で表現し，各種システム監視項目（以下，監視項目）を当てはめることで，速やかにネットワークサービスの正常性を判断し，システムの高可用性を維持する手法を提案する．以下，2 章では，関連した研究の紹介をし，3 章では従来のシステム監視手法の問題点を整理する．さらに 4 章ではブール代数を用いた改善方法について述べ，5 章で本研究の考察を行う．最後に 6 章では，今後の検討課題についてまとめる．

2. 関連研究

2.1 商用監視ツール

既存の商用監視ツールにはさまざまなものが存在する．特に，株式会社日立製作所，富士通株式会社，日本電気株式会社のソフトウェアは業界で大きなシェアを占めている[3]．多くの商用監視ツールは，ネットワークサービスという大きな括りでネットワークサービスの正常性を分析するものは少なく，アプリケーションプロセスの閾値監

†信州大学大学院総合工学系研究科システム開発工学専攻
Graduate School of Science and Technology Shinshu University
†† 信州大学大学院工学系研究科情報工学専攻
Graduate School of Science and Technology Shinshu University

視の結果に異常があった場合，その内容を運用者へ通知するといったものが多い．また，商用監視ツールは，製造元によって独自のデータの持ち方を採用している場合が多く，複数の製造元のツールを採用している場合，汎用的にデータを交換できる可能性が低い．

2.2 フリー監視ツール

伝統的なSNMP（Simple Network Management Protocol）[4]を用いた方法，商用監視ツールに近い機能を実現させるOSS（Open Source Software）を用いた方法がある．特にHinemos[5]は独立行政法人情報処理推進機構（IPA）が推進する平成 16 年度オープンソースソフトウェア活用基盤整備事業から生まれたフリー監視ツールである．フリー監視ツールは導入コストを抑えることができ，システム運用組織が自由にカスタマイズできるという利点がある．しかし，ネットワークサービスという大きな括りでネットワークサービスの正常性を自動で判断することが難しいため，最終的に運用者のスキルレベルや熟練度に大きく左右される状況を招くことが予想される．

2.3 リレーショナルデータベースを用いた方式

文献[6][7][8][9][10]では，システム運用管理を目的としたOSS，独自のアプリケーションを用いてシステム構成情報を取得し，リレーショナルデータベースに情報を持たせることでシステム構成管理を実現している．この研究では，システム構成情報や依存関係をリレーショナルデータベースに定義することで，イベント発生時の調査を容易にしている．しかし，ネットワークサービスという大きな括りでネットワークサービスの正常性を自動で判断することが難しいため，最終的に運用者のスキルレベルや熟練度に大きく左右される状況を招くことが予想される．

3. 問題点の整理

3.1 監視項目の分類

監視項目は，対象となるシステム要件やネットワークサービスの構成に合わせて定義する必要がある．表 1 は監視項目の例を示したものである．

定義する監視項目は，ネットワークサービスの停止の予防を目的としたプロアクティブなもの（以下，プロアクティブ監視項目），ネットワークサービスの復旧を目的としたリアクティブなもの（以下，リアクティブ監視項目）[11][12]に分類することができる．表 2 は，Ping疎通を例にプロアクティブ監視とリアクティブ監視の違いを示したものである．リアクティブ監視項目は，プロアクティブ監視項目に比べてネットワークサービスへの影響が明確である．

さらに，プロアクティブ監視項目とリアクティブ監視項目は，正常または異常の判断が明確にできるもの（以下，ステータス監視項目），各種ログファイルの文字列監視を行うもの（以下，ログ監視項目）に分類することができる．表 3 はアプリケーションプロセス監視を例にステータス監視項目とログ監視項目の違いを示したものである．ログ監視項目は，ステータス監視項目に比べて運用者による判断が必要となる可能性が高い．

表 4 は各監視項目の分類を整理したものである．大分類では，イベント発生時の対応方法の違いを明確にしており，小分類ではイベント発生時の判断方法の違いを明確にしている．リアクティブ監視項目に属する，ステータス監視項目（B-1）のイベントを検知した際は，ネットワークサービスの復旧を目的とした早急な障害対応が求められる．

表 1　監視項目の例

	監視項目
1	Ping 死活監視
2	WEB サーバアプリケーションプロセスの個数に対する閾値監視
3	WEB サーバアプリケーション使用ポートに対する PORT ALIVE 監視
4	WEB コンテンツに対する GET リクエスト監視

表 2　プロアクティブ監視項目とリアクティブ監視項目

種類	ネットワーク サービスの影響	検知内容
プロアクティブ監視項目	要調査	Ping 疎通が 20%ロスした
リアクティブ監視項目	あり	Ping 応答が無かった

表 3　ステータス監視項目とログ監視項目

種類	正常・異常 の判断	検知内容
ステータス監視項目	明確	アプリケーションのプロセスが存在しなくなった
ログ監視項目	運用者による判断が必要	アプリケーションのログに「エラー」の文字列が出力された

表 4　監視項目の分類

大分類		小分類	
A	プロアクティブ監視項目	A-1	ステータス監視項目
		A-2	ログ監視項目
B	リアクティブ監視項目	B-1	ステータス監視項目
		B-2	ログ監視項目

3.2 監視項目管理の問題点

運用者は，ネットワークサービスと各監視項目の関係を明確に把握している必要がある．特にリアクティブ監視項目のイベントを検知した際は，関係するネットワークサービスの影響範囲を特定することが必須である．

しかしながら，現在はシステムの大規模複雑化が進んでおり，複数の機器に機能を分散させてネットワークサービスを提供する場合が多い．また，複数の機器で構成される 1 つのシステム環境内で複数の異なるネットワークサービスが提供されるケースも珍しくない．

図 1 は，1 つのシステム環境内で複数の異なるネットワークサービスが提供される例を示したものである．この環境では，Service1～Service3 という名称の 3 つのネットワークサービスが提供されている．図 1 の環境において，データベースサーバ(DB01)のデータベースアプリケーションプロセスのダウンを検知した際，即座に Service3 に影響が出ていると判断できるであろうか．

明確な判断をするには，Service3 を構成する機器の依存関係，各監視項目の依存関係を熟知している必要がある．既存の監視システムでは，運用者へデータベースアプリケーションプロセスのダウンは通知されるが，当該障害が及ぼすネットワークサービスの影響までは通知されない．

つまり，現在運用されている多くのシステムは，ネットワークサービスと各監視項目との関係を明確に把握することが困難であり，多くの場合，運用者のスキルレベル，熟練度によってシステムの可用性が左右される状況にある．このような状況下においては，運用者の人員交代等によって障害対応時間に大きな差が生じる可能性が高く，同時にシステムの可用性低下を招いてしまう可能性が高い．

そのため，提供しているネットワークサービスの種類を明確に定義し，リアクティブ監視項目のイベント発生時には，全てのネットワークサービスの影響範囲を的確に把握することのできる手法を検討する必要がある．

4. 提案方式

4.1 本提案で取扱う課題の範囲

本研究では，イベント発生時にネットワークサービスへの影響が明確なリアクティブ監視項目について取扱うこととし，プロアクティブ監視項目については改善範囲に含めない．

ステータス監視項目による監視は，正常または異常の判断が明確に行うことができる．一方，ログ監視項目は検知したメッセージ内容について運用者による調査，判断が必要になる場合が多い．そのため，ログ監視項目にて検知した内容を機械的に処理することは難しい．

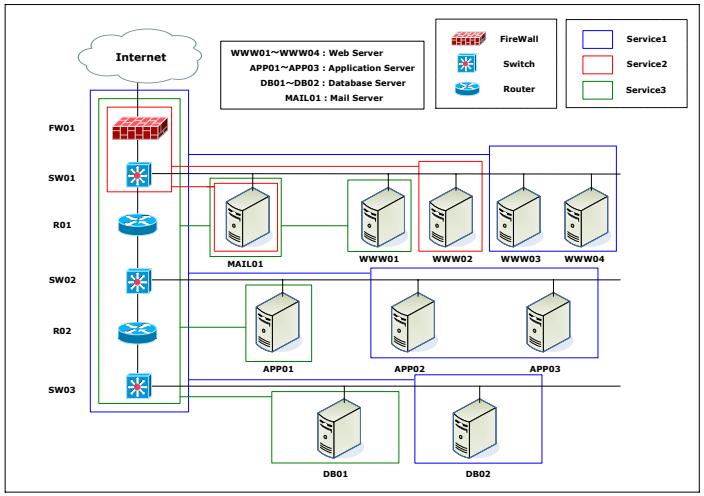

図 1　複数のサービスが混在した複雑なシステムの構成例

しかし，システムのリアルタイムな状態や動作に関する内容であれば，ログ監視項目はステータス監視項目に置換えて表現できる場合が多い．例えば，ログ監視項目にて「NFS se rver ホスト名 no t responding」という文字列を含むメッセージを検知した際は，NFS サーバへのアクセスが正常に行えていないことを意味する．このログ監視項目は NFS サーバへの読込み・書込み結果を判断するプログラムで代替可能であり，ステータス監視項目で表現することができる．

即ち，システムの正しい状態を定義することができれば，あらゆる監視項目はステータス監視項目として扱うことができる．そのため，本研究では，正常・異常の判断が明確にできるステータス監視項目のみを取扱うこととし，ログ監視項目に関しては改善範囲に含めない．以降，本研究で取扱うリアクティブ監視項目に属するステータス監視項目を主監視項目と呼ぶこととする．

4.2 ブール演算式を用いたシステムの依存関係表現

4.2.1 主監視項目のグループ化

システム運用の現場では，さまざまな目的の監視項目が存在する．ここでは，さまざまな目的の監視項目の中から，ネットワークサービスに特化した主監視項目のグループ化を行う．図 2 は，主監視項目の分類例を示したものである．例えば，監視対象の機器名を Node，Node で定義されている全ての監視項目を Node_ALL (M01-M12)，Service1 に直接関係する全ての主監視項目を Node_A1，Service2 に直接関係する全て

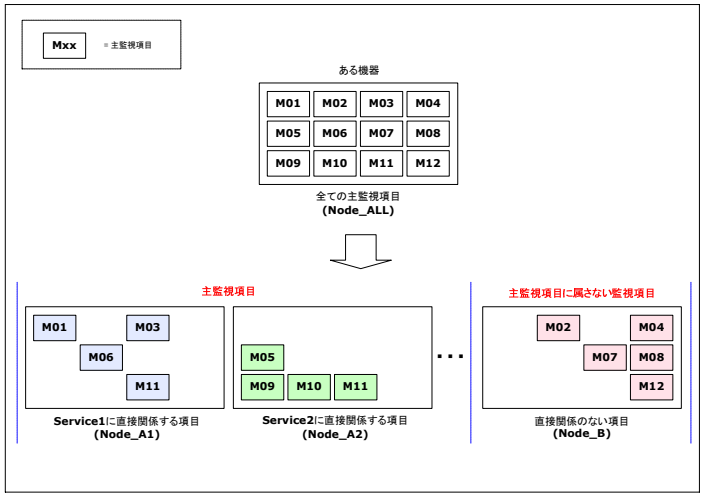

図 2　主監視項目の分類例

表 5　主監視項目の整理例

グループ	監視項目
Node_A1	M01，M03，M06，M11
Node_A2	M05，M09，M10，M11
Node_B	M02，M04，M07，M08，M12

の主監視項目を Node_A2，主監視項目に属さない全ての監視項目を Node_B とした場合，表 5 のように整理することができる．

主監視項目のグループ化が完了次第，グループの関連性を分かりやすく表現するためブール演算式を用いて表す．例えば，Node_A1 が正常になるためには，Node_A1 に属する全ての主監視項目が正常である必要がある場合，次の式で表すことができる．

$$\text{Node\_A1} = \text{M01 AND M03 AND M06 AND M11} \quad (1)$$

具体的に，主監視項目 M06 が正常でなくなった場合，ブール値を True（主監視項目正常時）および False（主監視項目異常時）で表し演算すると次のようになる．

$$\begin{aligned}\text{Node\_A1} &= \text{True AND True AND False AND True} \\ &= \text{False}\end{aligned} \quad (2)$$

また，Node_A2 に関して，主監視項目 M10 または M11 のどちらか一方が正常であれば良く，それ以外は全て正常である必要がある場合，次の式で表すことができる．

$$\text{Node\_A2} = \text{M05 AND M09 AND (M10 OR M11)} \quad (3)$$

具体的に，主監視項目 M10 が正常でなくなった場合，ブール値を True（主監視項目正常時）および False（主監視項目異常時）で表し演算すると次のようになる．

$$\begin{aligned}\text{Node\_A2} &= \text{True AND True AND (False OR True)} \\ &= \text{True}\end{aligned} \quad (4)$$

このように，主監視項目のグループをブール演算式で表現することで，発生イベントに対応する主監視項目と影響するネットワークサービスを運用者へ通知することが可能となる．

4.2.2 機器のグループ化

1 台の機器を用いて各種ネットワークサービスが提供される場合は，前節で述べた主監視項目のグループ化によってイベント検知時の影響範囲を特定することが可能となる．しかし，現在は複数の機器を用いて各種ネットワークサービスを提供している場合が多いため，機器のグループ化が必要である．機器のグループ化は，対象とするネットワークサービスに関係する機器をグループにまとめる．例えば，図 1 の各種ネットワークサービスに関して機器をグループ化すると表 6 のようになる．

機器のグループ化が完了次第，主監視項目のグループ化の時と同様にグループの関連性を分かりやすく表現するため，ブール演算式を用いて表す．例えば，図 1 および表 6 より，Service1 は次のブール演算式で表すことができる．

$$\begin{aligned}\text{Service1} = {} & \text{(WWW03 OR WWW04) AND (APP02 OR APP03)} \\ & \text{AND DB02 AND FW01 AND SW01 AND R01} \\ & \text{AND SW02 AND R02 AND SW03}\end{aligned} \quad (5)$$

具体的に，機器 MAIL01 でハードウェア障害が発生した場合，ブール値を True（主監視項目正常時）および False（主監視項目異常時）で表し演算すると次のようになり，Service1 に影響を及ぼさないことが分かる．

$$\begin{aligned}\text{Service1} = {} & \text{(True OR True) AND (True OR True)} \\ & \text{AND True AND True AND True AND True} \\ & \text{AND True AND True AND True} \\ = {} & \text{True}\end{aligned} \quad (6)$$

このように，機器のグループをブール演算式で表現することで，運用者は各機器と各種ネットワークサービスの関係を把握することが可能となる．

表 6　各種ネットワークサービスに関する機器のグループ例

機器	Service1	Service2	Service3
MAIL01		○	○
WWW01			○
WWW02		○	
WWW03	○		
WWW04	○		
APP01			○
APP02	○		
APP03	○		
DB01			○
DB02	○		
FW01	○	○	○
SW01	○	○	○
SW02	○		○
SW03	○		○
R01	○		○
R02	○		○

表 7　各種ネットワークサービスに関係する主監視項目と機器の整理例

機器	Service1	Service2	Service3
MAIL01		MAIL01_A2	MAIL01_A3
WWW01			WWW01_A3
WWW02		WWW02_A2	
WWW03	WWW03_A1		
WWW04	WWW04_A1		
APP01			APP01_A3
APP02	APP02_A1		
APP03	APP03_A1		
DB01			DB01_A3
DB02	DB02_A1		
FW01	FW01_A1	FW01_A2	FW01_A3
SW01	SW01_A1	SW01_A2	SW01_A3
SW02	SW02_A1		SW02_A3
SW03	SW03_A1		SW03_A3
R01	R01_A1		R01_A3
R02	R02_A1		R02_A3

4.2.3 主監視項目および機器のグループ化情報の結合

主監視項目のグループ化は，イベントとして検知した主監視項目より各種ネットワークサービスの影響度を特定することができるが，ネットワークサービスを提供する上で必要な機器の依存関係に関しては特定できない．

機器のグループ化は，ハードウェア障害等のイベントが発生した際，対象機器が各種ネットワークサービスとどのような関係にあるかを特定できるが，主監視項目との依存関係に関しては特定できない．

そのため，主監視項目および機器のグループ化情報を結合すれば，システムが複数の機器で構成される場合であっても，イベント検知時に各種ネットワークサービスの影響範囲を特定することが可能となる．表 7 は，図 1 の各種ネットワークサービスに関係する主監視項目と機器の関係を整理した例である．表 7 の内容を基に，Service1 についての関係をブール演算式で表すと次のようになる．

$$\begin{aligned}\text{Service1} = {} & (\text{WWW03\_A1 OR WWW04\_A1}) \text{ AND } (\text{APP02\_A1 OR APP03\_A1}) \\ & \text{AND DB02\_A1 AND FW01\_A1 AND SW01\_A1 AND R01\_A1} \\ & \text{AND SW02\_A1 AND R02\_A1 AND SW03\_A1}\end{aligned} \quad (7)$$

例えば，WWW03_A1 に属するある主監視項目の 1 つが障害になり，その他の主監視項目が正常であった場合，Service1 についてのブール演算式の演算結果は次の通りとなり，完全ネットワークサービスが停止していないという事が確認できる．

$$\begin{aligned}\text{Service1} = {} & (\text{False OR True}) \text{ AND } (\text{True OR True}) \\ & \text{AND True AND True AND True AND True} \\ & \text{AND True AND True AND True} \\ = {} & \text{True}\end{aligned} \quad (8)$$

5. 研究の考察

従来の監視手法を用いた場合，イベントを検知した際に監視項目の大分類（プロアクティブ監視項目またはリアクティブ監視項目）を判別しなくてはならなかった．もしも，検知したイベントがリアクティブ監視項目に属するものであれば，各種ネットワークサービスとの依存関係を調査した上で早急に影響範囲を特定し，ネットワークサービスへの影響度を評価する必要があった．しかし，各種監視項目とネットワークサービスの依存関係を把握するには多くの時間を要する可能性が高い．例えば，N 個

の監視項目の中で，1 個，2 個，3 個... の監視項目を使用する組合せが，それぞれ 1 個ずつ出現する時の組合せ総数 Monitor_total は次の通り表現できる．

$$\text{Monitor\_total} = {}_nC_1+{}_nC_2+...+{}_nC_{n-1}+{}_nC \quad (9)$$

一方，二項定理より

$$(x+y)^n = \sum_{k=0}^{n} {}_nC_k x^k y^{n-k} \quad (10)$$

ここで，$x=y=1$ とすると

$$2^n - 1 = {}_nC_1+{}_nC_2+...+{}_nC_{n-1}+{}_nC_n \quad (11)$$

を得る．(9)式の右辺＝(11)式の右辺となることから

$$\text{Monitor\_total} = 2^n - 1 \quad (12)$$

となる．実際には，${}_nC_m$ が複数個存在することが予想され，(12)式よりも大きな組合せ総数を扱わなくてはならないことになる．当然，イベントに対応する運用者のスキルレベルや熟練度を加味すると対応の状況は変わるが，各種監視項目の絶対数から比べればその有効性は不確実と考えられる．また，いくらスキルレベルが高く，熟練度の高い運用者であっても，(12)式で表されるような膨大な各種監視項目の組合せを基に，常に正しい依存関係を特定できるとは限らない．たとえ，ネットワークサービスの正しい組合せを特定できたとしても，冗長構成環境やディザスタリカバリ環境では，検知された監視項目の組合せによっては，与えられた時間内にネットワークサービスの影響度を正しく評価しきれない可能性も大きくなる．

本研究では，主監視項目とネットワークサービス，機器とネットワークサービス，主監視項目と機器に関する依存関係を明確にし，運用者のスキルレベルや熟練度によらず，主監視項目の総組合せからネットワークサービスの正しい組合せを特定する手法を提案した．加えて，提供サービスの正しい組合せをブール演算式で表すことで，冗長構成やディザスタリカバリ環境といった複雑な環境においても，正しくネットワークサービスの影響度を評価できることを示した．これらの結果より，本研究概念の導入によって，各種ネットワークサービスの正常性を効率的に把握することが可能となった．さらに，主監視項目に属するイベントの検知時に行っていたドキュメント調査，リバースエンジニアリングの実施といった運用者の知識やスキルレベルに依存する作業を大きく減少させ，結果的に運用者の対応品質を高均質に均一化する事も可能となる．

6. 今後の検討

本研究概念は，誤った情報で主監視項目のグループ化定義，機器のグループ化定義，主監視項目と機器のグループ化情報の結合定義を行ってしまうと，各種ネットワークサービスの正常性判断を正しく行うことができず，さらに状況を悪化させてしまう可能性がある．また，本研究概念の導入方法は，さまざまな方法が考えられる[13]．具体的な導入方法に関しては，既存のシステム監視環境を考慮の上，柔軟に検討していくべきである．しかし，導入方法によってはシステム監視情報等の 2 重管理を発生させてしまう可能性も高い．これらの問題は運用開始前の厳密なチェック，運用開始後の動作傾向チェックで十分に回避可能であるが，さらに利便性の高い厳密なチェック方法に関して引続き検討していきたいと考えている．

参考文献

1) 赤津雅晴: 成功するアウトソーシングの勘所，情報処理学会会誌，Vol.46，No.5，pp.534-539
2) 金子勲，高野勉: 大規模ネットワークシステムにおけるシステム管理／ネットワーク管理の現状，UNISYS TECHNOLOGY REVIEW，http://www.unisys.co.jp/tec_info/tr70/7002.pdf，第 70 号，pp.21-38 (2001)
3) 第 3 回：徹底比較！商用の監視ソフトウエア，http://thinkit.jp/article/751/3/
4) Net-SNMP，http://www.net-snmp.org/
5) Hinemos：コンピュータ、システム、ネットワークの運用管理を実現するオープンソースソフトウェア(OSS)，http://www.hinemos.info/
6) 大平栄二，大谷俊雄，宮脇当為，小川祐紀雄，右馬伸一: 大規模 IP ネットワークの情報管理システムの検討，電子情報通信学会論文誌，Vol.J86-B，No.7，pp.1278-1286 (2003)
7) 小川祐紀雄，中谷彰宏，大平栄二，長谷川聡，石井直輝: ネットワーク統合管理データベースと大規模 IP ネットワーク性能診断システムの開発，電子情報通信学会論文誌，Vol.J86-B，No.7，pp.1278-1286 (2003)
8) 森一，敷田幹文: サーバ依存関係を考慮したシステム構成管理の支援法，情報処理学会論文誌，Vol.41，No.12，pp.940-948 (2005)
9) 後藤宏志，敷田幹文: サーバの依存関係を考慮したログ情報による障害監視支援の提案，情報処理学会研究報告 マルチメディア通信と分散処理，No.121，pp.37-42 (2006)
10) 長田智和，谷口祐治，玉城史朗: 大規模分散ネットワーク運用管理システムの提案，情報処理学会研究報告 分散システム/インターネット運用技術，No.113，pp.31-36 (2000)
11) Office of Government Commerce: サービスサポート，TSO 出版 (2003)
12) Office of Government Commerce: サービスデリバリ，TSO 出版 (2003)
13) 川崎敏行: ネットワークサービスの可視化を主眼に置いたシステム運用者支援方法の提案，情報システム学会論文誌 (JIS SJ)，第 4 巻 1 号，pp.1-16 (2008)