自律型エージェントによる運用監視システム

佐藤 祐[†]　伊藤 雅博[†]　高橋 修[‡]

日本ヒューレット・パッカード株式会社[†]　公立はこだて未来大学[‡]

1. はじめに

運用監視システムにおいて，監視対象機器ごとに最適な監視しきい値を設計することは非常に重要である．しかし昨今における IT システムの大規模化・複雑化が進む中で，システム運用管理者が個々の監視対象機器の特性を踏まえた上で，それぞれに対して最適なしきい値を設計することは困難である．

不適切なしきい値が設定されている場合，不要な通知メッセージ等への対処により運用コストが増大するだけでなく，監視システム自体の信頼性を低下させる．また，度重なるしきい値の見直し作業は日常の運用効率を低下させ，システム運用管理者がより付加価値の高い業務を行う機会を減らしかねないという問題をはらんでいる．

そこで，本研究においては以上のような問題を鑑み，以下の方式を使った自律型監視エージェントについて検討する．

・自動閾値決定方式
・エージェント間監視方式

監視対象機器のしきい値を，システム運用管理者が機器ごとに設計するのではなく，監視対象機器に導入された監視エージェントが自動的に最適なしきい値を設定し異常値を検出する．また，自律型の監視エージェントが導入された監視対象機器が，相互に監視し合い，監視システムの信頼性を向上させる方法についても検討する．これにより，監視運用に関するコストや効率を改善することが出来ると考える．

2. 既存の監視運用と問題点

一般的に，システム運用管理者は監視システム(図 1)において，日常の運用によって蓄積されたデータを定期的に収集解析し，さらに個々の監視対象機器の特性を踏まえたうえで，それぞれに対する最適なしきい値を再設計する．

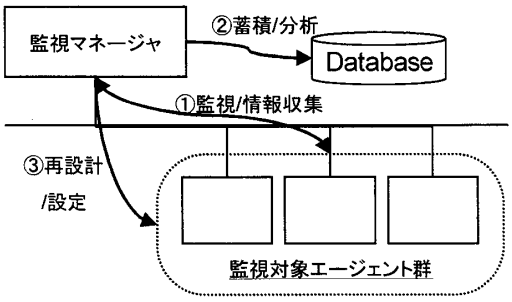

図 1 運用監視システム概要図

しかし，そのようなリアクティブなシステム運用では，常に妥当性のある最適な監視しきい値を保つことは難しい．一度設定した静的な監視しきい値は，定期的にシステム管理者によって見直されるか，多くの場合はなんらかのアラーム，エラーなどの発生といった具体的事象となって問題が発生するまで放置され，不適切な監視しきい値となってからもそのまま運用（又はアラームが発生してもそれ自体を無視）されるために，監視システムの役割の一つである障害の予見を果たせないことが多い．

また，経験の浅いシステム運用管理者にとっては，個々の監視対象機器において何をどのように監視すれば良いかの判断がつかない場合が多く，運用仕様がバラバラになるといった問題が発生し，それに起因して運用効率・信頼性の低下が発生していた．

3. 自律型エージェントの提案

3.1 自動しきい値決定方式

監視対象となるサーバ機器において，自動的にしきい値を計算するには，ある程度の蓄積された情報が必要となる．一定期間のテスト運用を経て蓄積されたデータ（正規母集団）を元に，監視対象機器に導入された監視エージェントは，その都度リソース情報について異常である数値は何かを判断する必要がある．この異常値を検出する方法として，「グラブススミルノフの棄却検定法[1]」を応用する．

グラブススミルノフの棄却検定法は，元々は正規母集団からから外れ値を除くための手法ではあるが，この外れ値と認定した数値を「閾値を

A management system by the autonomy type agent.

Yu Sato[†], Masahiro Ito[†], Osamu Takahashi[‡]
Hewlett-Packard Japan, Ltd. [†] Future University - Hakodate[‡]

超えた異常な値」として運用監視システムに適用することができる.

監視エージェントはあらかじめ設定された監視周期ごとに，機器のリソースを収集しデータベース化する．収集されたリソースはその都度「グラブススミルノフの棄却検定法」にかけられ，今までの収集されたデータの統計と比較して，異常に離れた値か否か検定される．その値が検定式により異常であると判断された場合，監視エージェントはしきい値を超えたと判断して監視マネージャに対して障害を通知する（この異常値は監視エージェントの統計データベースには蓄積されない）．

監視エージェントが，毎回チェックするリソースが異常値でないと判断された場合は統計データに取り込まれ次回からの計算に適用される.

この方法により，ある程度の運用期間を経ることによって統計データ量が増し，異常値を検出する検定方式の精度の向上も可能となる.

以下に動作例を示す.

監視エージェントが定期的に CPU 使用率を収集したデータベースを表 1 とした場合，最後に収集した値「80」が異常値であるかどうかを有意水準 5%で検定する.

表 1 監視エージェントが収集した CPU 使用率(%)

回	1	2	3	4	5	6	7	8	9	10
値	30	40	35	41	41	40	43	35	37	38
回	11	12	13	14	15	16	17	18	19	20
値	34	33	33	35	32	39	35	38	40	80

・標本平均 38.95%

・標本分散 105.5236842

標本平均を $\overline{X}$，標本分散を μ としたときに，最大の測定値 X_i について次式による T_i を求める.

$$T_i = \frac{X_i - \overline{X}}{\sqrt{\mu}}$$

表 1 を適用すると以下のとおりとなる.

$$T_{20} = \frac{80 - 38.95}{\sqrt{105.52}} = 3.99$$

標本の大きさ 20，有意水準 5%としたときの有意点 t を 2.557 とする.

T_i ＜ t のとき，X_i は異常値ではない.

T_i ≧ t のとき，X_i は異常値とする.

よって，3.99 ≧ 2.557 のため 80 は異常値であると判断できる.

3.2 エージェント間監視方式

監視システム全体の信頼性を向上させる方法の一つとして，監視エージェント同士でのチェック機能が必要となる．監視エージェントがお互いを死活監視することで，一つのネットワーク経路だけでなく複数の経路を使用して監視マネージャとの経路を確保することができ，ネットワーク障害による通信不可の状態を軽減することができる(図 2).

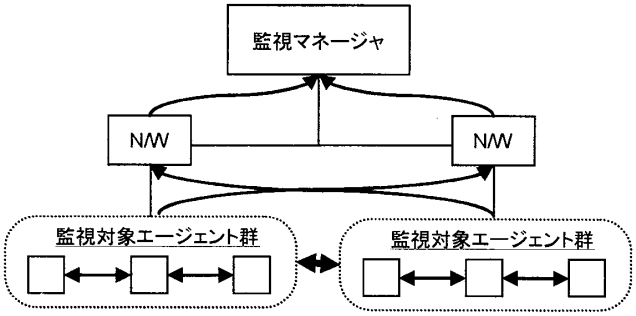

図 2 エージェント間監視方式概要図

監視エージェントは，ネットワークプロトコルのスパニングツリーに似た仕組みを用い，同一セグメントに存在する被監視対象エージェントがそれぞれに被監視対象エージェントと情報を交換し，ルートとなるサーバを決定する.

また，監視マネージャまでの経路に障害がある場合はその情報も交換し，最適な経路で通知できるような仕組みを持つ.

相互監視の機能を持つ監視エージェントは，新しい機器が追加された場合や，既存の機器が削除された場合に再計算を行い，新たなルートと優先度を決定する.

4. まとめ

システム運用監視の効率化とコスト削減の為に，自律型の監視エージェントが果たす役割は非常に重要である．本稿のテーマ以外にも自律型の監視エージェントとしての可能性は多岐にわたり，今後は SNMP [2]のセキュリティを応用した監視等も重要となってくる.

参考文献

[1]佐藤敏雄・松村宰「やさしい医療系の統計学」医歯薬出版(2002 年)

[2]SNMP(http://www.snmp.org/)