ネットワーク管理情報の収集・分析支援システム

– magP の現状と今後の課題 –

中嶋 良彰[*]　　大野 浩之[†]
(東京工業大学大学院情報理工学研究科)　　(東京工業大学 Titanet 運用センター)

1　はじめに

計算機やネットワークの管理作業は、管理者の知識や経験に依存し、負担の大きい作業である。また、計算機が普及、ネットワークが大規模化によって、発生する問題も多様化してきている。例えば、次のような問題が考えられる。

- 多種多様なアプリケーションやコマンドに関する知識が必要なことに起因する問題
- 管理者の不足に起因する問題
- 管理対象を常に監視していることは難しいことに起因する問題

管理作業では「情報の調査」と「分析作業」が重要な役割を占める。著者らはこの作業を支援するために、magP [1] の開発を進めている。magP は自動的に管理対象の情報を収集・分析し、障害の発生やその原因を管理者に知らせるエージェントシステムである。分析結果は電子メール、ページャなどの方法で管理者へ報告されるため、管理者は障害に迅速に対応することができる。また、熟練していない管理者の作業を支援することもできる。本講演では、この magP の現状と今後の課題について報告する。

2　管理対象の情報の取得と分析

magP には、情報オブジェクトと分析オブジェクトという概念があり、この 2 つのオブジェクトのインスタンスを生成しながら動作する。

2.1　分析オブジェクト

分析オブジェクトは、分析に必要な情報を情報オブジェクトから取得し、条件が満たされ次第、対応するアクションを実行する。そのために、分析オブジェクトは、必要な情報オブジェクトのインスタンスを生成し、それと通信を行ないながら分析を行なう。また、必要な情報オブジェクトが十分に揃っていると仮定すれば、ユーザ (管理者) は情報の調査方法に関する知識を要求されることなく、情報を中心とした分析ルールの記述を行なうことができる。

2.2　情報オブジェクト

情報オブジェクトは、分析オブジェクトに分析に必要な情報を提供する。分析オブジェクトに対して共通のインタフェース (プロトコル) を提供し、具体的な情報の取得方法は隠蔽する。これによって、情報種類に応じて調査方法が異なる (利用するアプリケーションやコマンドが異なる) ことが引き起こす問題を解決し、管理に必要なアプリケーション (コマンド) に関する知識を軽減する。

また、いくつかの特別な情報オブジェクトが用意されている。

syslog object UNIX の syslogd というデーモンプログラムに集まるシステムメッセージを全てフィルタリングし、必要なものを分析オブジェクトに提供する。

SNMP object SNMP によってシステムの情報を取得し、分析オブジェクトに提供する。

通常、情報オブジェクトは必要時に生成されるが、この 2 つのオブジェクトは常時存在し、分析オブジェクトに情報を送信しつづけ、受動的な情報調査に利用される。

---

magP: A Support System for Collecting and Analyzing Network Management Information

Yoshiaki NAKAJIMA. (Graduate School of Information Science and Engineering, Tokyo Institute of Technology)

*Hiroyuki OHNO (Network Operation Center, Tokyo Institute of Technology)

2.3 インスタンス生成と実行の流れ

magP は、分析オブジェクトと情報オブジェクトのインスタンスが相互に通信を行ないながら動作する。その過程 (図 1) について、おおまかに述べる。

1. 分析オブジェクトと必要な情報オブジェクトのインスタンスが生成される。
2. 情報オブジェクトは分析オブジェクトの要求に応じて情報を送信する。
3. 分析オブジェクトでは条件が満たされ次第、アクション (ユーザーへの報告、分析オブジェクトの生成・追加、他エージェントへの転送など) を実行する。

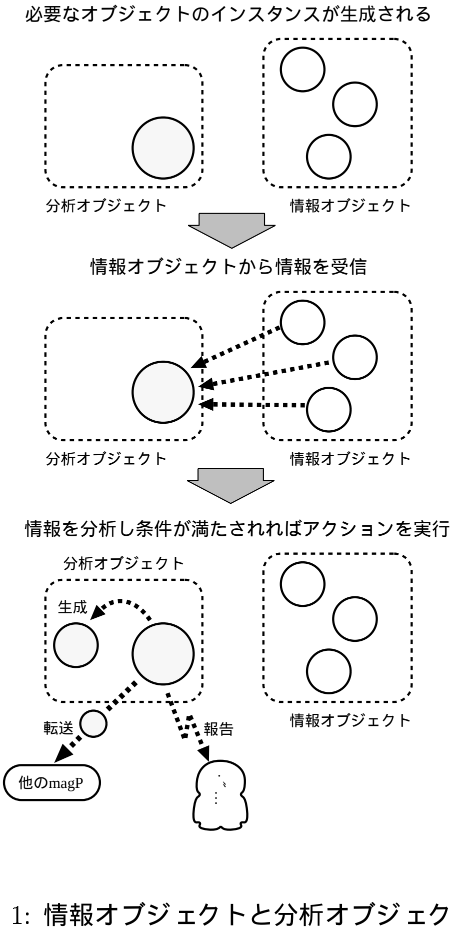

図 1: 情報オブジェクトと分析オブジェクト

3 magP

現在の magP は、`magpd` と `magpc` の 2 つのプログラムから構成される。`magpd` は、分析オブジェクトと情報オブジェクトの管理、ユーザ (管理者) の操作受け付け、他の `magpd` との通信などを行ない、各計算機に 1 つだけ常駐する。`magpc` は、`magpd` に対する分析オブジェクトのインスタンス生成命令の発行やインスタンス生成スケジュールの操作などを行なう。

magP は、「利用する道具に関する知識が減少する」「管理対象を常に監視する必要がなくなる」など、1で述べた問題に有効である。また、その他にも次のようなことが可能である。

- syslog オブジェクトや SNMP オブジェクトを利用すれば、受動的な情報獲得が可能。
- 分析オブジェクトの追加によって自動的に知識を追加することが可能。
- 分析オブジェクトの転送によって不正侵入などの知識を自動的に伝搬させることが可能。
- 分析不能な事態に陥った場合でも、自動的に管理者や他のエージェントに報告を行なうため、ポーリング以外の手段で障害を検知することが可能。
- 分析オブジェクトを充実させることによって単純な作業はエージェントに任せ、管理者は重要な作業に専念することが可能。

4 今後の予定

今後は、特に次のような点を中心に開発を進めていく予定である。

- オブジェクト定義記述支援のための GUI の実装。
- エージェントの動作監視 GUI の実装。
- 認証機構、アクセス制御機構の実装。
- 電子メール・電話などによる遠隔操作機能の追加。

謝辞

さまざまな助言を頂いた東京工業大学大学院数理・計算科学専攻の木村泉教授、木村・大野研究室の皆さんに感謝致します。

参考文献

[1] 中嶋良彰, 大野浩之. 管理情報を自動的に収集・分析するネットワーク管理支援系の設計と実装. 分散システム運用技術研究グループ資料. 情報処理学会, May 1995. 資料番号 DSM-9505035.