L-018

SNMP によるネットワークロギングシステムの構成管理
Configuration Management for Network Logging System Using SNMP

角田 裕† 太田 耕平‡ キニ グレン マンスフィールド‡ 和泉 勇治¶ 根元 義章¶
Hiroshi Tsunoda Kohei Ohta Glenn Mansfield Keeni Yuji Waizumi Yoshiaki Nemoto

1. はじめに

各ホストの OS やアプリケーションが出力するログは、ホスト上で誰が・いつ・何をしたのかを表す重要な情報であり、そのログを収集するロギングシステムはネットワーク管理における重要な役割を担っている。近年では、ログの用途はセキュリティ管理・監査・フォレンジックなどにも広がり、ログ収集の対象が従来のサーバだけでなくクライアントにまで及ぶと共に、監査などの用途にも耐えうる高信頼な収集が求められている。

現在、ロギングシステムには事実上の標準プロトコルとして Syslog プロトコル [1]が広く用いられている。しかし、Syslog はトランスポートに UDP を使用しており収集中に損失したログの回復ができず、なりすましやログの偽造に対する対策を備えていないなど、信頼性・安全性の面で問題点も有している。これらの弱点を補うため、IETF (Internet Engineering Task Force)の syslog WG [2]において、ログ記述の標準フォーマットの策定や、TCP の利用による信頼性の確保、ログの暗号化や署名による安全性の確保など、プロトコルの更新と標準化が進められている[3]。また、ログ収集の信頼性と効率性を両立させる新たなトランスポートについても研究が進められている [4]。

syslog WG においてプロトコルの更新と同様に課題となっているのがロギングシステム自身の管理である。現在、ロギングシステムには、各ホストにおける syslog プロセスの稼働状況やログの送受信量、損失したログの数など、ログ収集の状態を監視しシステム自体を管理する仕組みが備わっていない。その結果、収集中にログの損失に気づくことができないなど、ログ収集の信頼性を確保する上で多くの問題を抱えている。その中で著者らの提案による Syslog の管理専用のデータ型を定義した Syslog-TC (Textual Conventions)-MIB [5]は、国際標準としてロギングシステムに管理性を付与する第一歩となっている。

本研究では、Syslog-TC-MIB を用いた管理アプリケーションとして、ロギングシステムの構成管理を提案する。そして、各ホストの Syslog に関する設定情報を定義した Syslog Configuration MIB を暫定的に実装し、それを用いてログ収集経路の可視化を行うことで、標準のネットワーク管理プロトコルである SNMP によりロギングシステムの構成管理が可能であることを実証する。

2. ロギングシステムの構成管理の必要性

Syslog によるロギングシステムの管理では、

- ログを出力する originator
- ログを収集する collector
- originator と collector の間でログを中継する relay

の 3 種類のホストの接続関係を管理する構成管理が必要である。

Syslog によるロギングシステムでは、originator から送信されたログは、直接、または 1 台以上の relay を経由して collector に受信される。すべての originator が出力するあらゆるログを漏れなく収集するためには、この originator・relay・collector の syslog の設定がすべて正しく行われていなければならない。しかし、originator や relay におけるログの送信先の設定は各ホストで独立しており、ネットワーク全体を通じて一貫性を確認する仕組みは提供されていない。そのため、relay として動作しているホストの syslog 設定が誤って初期化され collector への中継が停止していたり、複数の relay 間でログの中継がループしていたりするなど、設定に不整合が生じていてもそれを検出することは困難である。結果としてそのような設定の不整合は、relay におけるログの停滞や、ログのループによるネットワーク負荷の増大を引き起こし、ログ収集の信頼性を大きく損ねる。

すなわち、信頼性のあるログ収集の実現には、ロギングシステムの構成管理を実施し、システム構成する各ホストが適切なホストへログを送信していることを検証する仕組みが必要である。そこで本研究では、SNMP を利用してロギングシステムの構成管理を行うことを提案する。次節では本研究で新たに定義した構成管理用の MIB について説明する。

3. Syslog Configuration MIB（SyslogCMIB）

ホストの Syslog 設定は syslog.conf ファイルに記載されている。syslog.conf には、ログの種別毎に出力先が記述されている。出力先としては、保存先のファイル名や送信先ホストの IP アドレスやホスト名などがある。ロギングシステムの構成管理には、ネットワーク内のすべてのホストから syslog.conf を取得し、その解析を通じて一貫性を検証することが必要である。

そこで、本研究では、各ホストの syslog.conf に記載された Syslog の設定情報を SNMP によって効率的に取得するために、Syslog Configuration MIB (SyslogCMIB)を新たに定義し暫定的に実装した。

SyslogCMIB の MIB ツリーを図 1に示す。syslog.conf はテーブル形式の syslogCTable オブジェクトに対応し、syslog.conf の 1 行分が syslogCTable のエントリである syslogCEntry オブジェクトに格納されている。管理者は syslogCText オブジェクトの値を順に読み出すことで syslog.conf の内容を取得できる。

4. SyslogCMIB を利用したログ収集経路の可視化

NET-SNMP [6]を活用して SyslogCMIB のプロトタイプを実装し、ロギングシステムの構成管理ログ収集経路の可視化実験を行った。

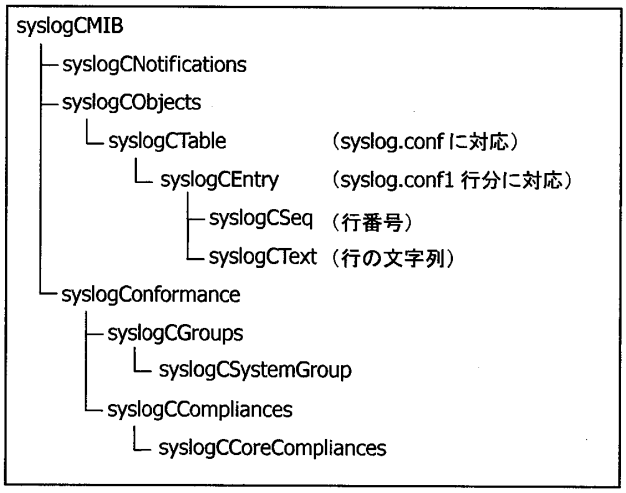

図 1 Syslog Configuration MIB

実験環境は 11 台のホストと 2 台の HUB によって構成されているプライベートネットワークである。各ホストには Ubuntu Linux 8.10 をインストールし、OS 標準の syslog 実装を使用した。実験ではホストのうち 1 台を collector、その他を originator および relay として動作させた。そして、各ホストの syslog の設定に不整合がある場合と無い場合について、ログ収集経路を可視化した。

実験ではすべてのホストに SyslogCMIB のプロトタイプを実装した NET-SNMP をインストールし、Syslog 設定情報を収集した。そして、ある 1 台のホストを始点として設定情報を解析し、ログの送信先となっているホストの設定情報の解析を再帰的に繰り返して収集経路を特定した。

収集経路の一部をオープンソースのグラフ描画ソフト Graphivz [7]を使用して可視化した結果を図 2に示す。

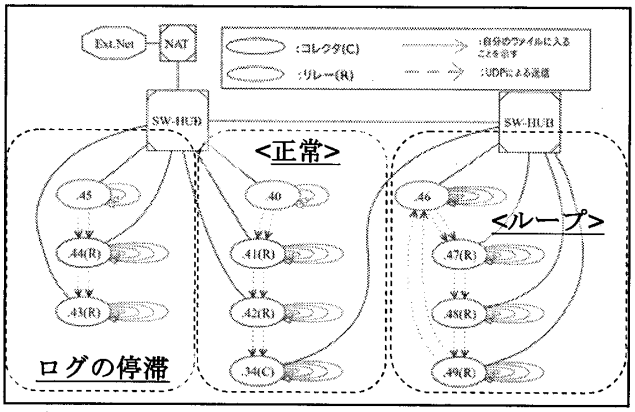

図 2 ログ収集経路の可視化結果

図中の楕円は 1 台のホストに対応しており、楕円内部のラベルはホストの IP アドレスの最下位バイトを示している。ラベルに付加された"C"と"R"は、それぞれそのホストが collector または relay であることを表している。".40"、".45"、".46"の 3 台のホストは originator である。ホストとホストを結ぶ矢印は一方のホストから他方のホストへ向けてログが送信されていることを表す。同じホストに戻る実線の矢印は、そのログがローカルのファイルに保存されるか、ローカルの他のプロセスに入力されることを表している。

この図から、".40"から送信されたログは 2 台の relay によって中継され、collector である".34"に受信されていることがわかる（図 2<正常>）。一方で、".45"から送信されたログは、途中の relay (".43") において syslog 設定の不備があるため、".43"のローカルのファイルに保存され停滞しており、collector に届いていないことがわかる（図 2<ログの停滞>）。同様に、".46"から送信されたログについては、中継のループによって collector に到達していない（図 2<ループ>）。このように、ホストの syslog の設定に不整合があると、originator から送信されたログは collector に到達せずログの収集漏れが生じる。

そして、図 2に示すように syslogCMIB によって収集した情報に基づいて収集経路を可視化することで、設定の不整合を容易に把握できることがわかる。

5. まとめと今後の課題

本研究では、Syslog によるネットワークロギングシステムにおいて、各ホストの Syslog の設定に不整合によりログの収集漏れが生じ、ロギングの信頼性が損なわれることを指摘した。そこで SNMP によるネットワークロギングシステムの構成管理を目的として構成管理用 MIB と SyslogCMIB を策定し、NET-SNMP によるプロトタイプ実装を行い、ホストの syslog 設定情報の SNMP による取得を実現した。策定した MIB とプロトタイプ実装の有効性を実ネットワークに構築したロギングシステムにおけるログ収集経路の可視化実験を通じて検証し、ログの収集経路を可視化することで syslog 設定の不整合を容易に把握できることを示した。

今後の課題として、各ホストの syslog プロセスの稼働状況に構成管理に反映させる必要がある。また、ロギングシステムが稼働しているネットワーク自体の構成管理や、障害管理と連動して構成管理を行う必要がある。

謝辞

本研究は総務省戦略的情報通信研究開発推進制度 (SCOPE-073102001)の援助を受けて実施された。ここに感謝する。

参考文献

[1]R.Gerhards, "The Syslog Protocol", RFC5424, Mar. 2009
[2]IETF Syslog WG, http://www.ietf.org/html.charters/syslog-charter.html
[3]太田耕平、"SYSLOG 技術動向"、情報セキュリティ技術動向調査タスクグループ報告書、IPA セキュリティセンター、2009 年 3 月 http://www.ipa.go.jp/security/fy20/reports/tech1-tg/2_03.html
[4]H. Tsunoda, T. Maruyama, K. Ohta, G. Keeni, Y. Waizumi, and Y. Nemoto, "A Prioritized Retransmission Mechanism for Reliable and Efficient Delivery of Syslog Messages", In Proc. of CNSR2009, May. 2009
[5]G. Keeni, "Textual Conventions for Syslog Management", RFC5427, Mar. 2009
[6]NET-SNMP, http://www.net-snmp.org/
[7]Graphviz, http://www.graphviz.org/

†東北工業大学工学部 Faculty of Engineering, Tohoku Institute of Technology
‡株式会社サイバー・ソリューションズ Cyber Solutions Inc.
¶東北大学大学院情報科学研究科 Graduate School of Information Sciences, Tohoku University