東北工業大学新技術創造研究センター紀要 EOS
Vol.24 No.1 p.49 〜 p.56, 2012

〔研究論文〕

# SNMP によるネットワークロギングシステムの構成管理アプリケーションの開発研究

角田　　裕[1)]・太田　耕平[2)]・キニ グレン マンスフィールド[2)]

（2011 年 12 月 27 日受理）

# Development of Configuration Management Application of Network Logging System using SNMP

Hiroshi Tsunoda[1)], Kohei Ohta[2)], Glenn Mansfield Keeni[2)]

Abstract

Logs generated by operating systems and application programs provide important information to a network administrator. Logs are used for various purposes including security management, audit, and forensics of intranet. To use logs for such purposes, management of a logging system itself is an important issue. In this paper, we tackle the configuration management problem of a logging system. A logging system is composed of three elements; originators, collectors, and relays. If there is a mismatch between the configuration of those elements, the path of log collection will be disconnected and logs will be lost in during the transportation. In order to prevent such losses of logs, we propose to collect the configuration information from all hosts in intranet and visualize the path of log collection.

## 1．はじめに

ネットワークが社会基盤としての重要性を増していく中で，ネットワーク自体に非常に高い信頼性が求められ，高度な運用管理･セキュリティ管理技術が必要とされている。ネットワークの運用管理･セキュリティ管理においては，情報の収集と解析がその根幹であり，管理者が情報を確実に収集し解析することができなければ障害やセキュリティインシデントの見逃しや対応の遅れにつながる。ネットワーク管理に必要とされる情報の中でも，各ホストの OS やアプリケーションが出力するログは，誰が・いつ・何をしたのかを表す重要な情報である。従来，ログの主要な用途はサーバの稼働状況の把握や障害管理への利用であった。しかし，現在ではその用途が更に広がり，イントラネットのセキュリティ管理，デジタル・フォレンジック，監査などにも欠かすことのできないものとなっている。その結果，OS やアプリケーションにはより細かな情報までログとして出力することが求めら

1）東北工業大学工学部情報通信工学科
Department of Information Communication Engineering, Faculty of Engineering, Tohoku Institute of Technology
2）株式会社サイバー・ソリューションズ
Cyber Solutions Inc.

れると共に，ログの収集対象も従来のサーバだけでなくクライアントにまで広がっている。また，ネットワーク管理者には，セキュリティ管理や監査に備え，膨大に発生するログを漏らさず確実に収集することが新たな課題として課せられている。

従来から，ロギングシステムで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）は2000年にsyslog WG［2］を組織し，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を行った［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は2010年にその役割を終えたが，ロギングシステム自身の管理についてはまだ多くの課題が残っている。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syslog WGでの筆者らの提案による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。

Syslog-TC-MIBを用いた管理アプリケーションとして，これまでに筆者らはロギングシステムの構成管理を提案している。そして，各ホストのSyslogに関する設定情報を効率的に取得するためのSyslog Configuration MIBの定義および暫定的な実装を行い，構成管理の一環としてログ収集経路の可視化が原理的に可能であることを示している［6］。本稿では，Syslogの設定情報を解析するパーサとネットワーク地図を利用した収集経路の可視化アプリケーションの開発について報告する。

## 2．ロギングシステムの構成管理の課題

### 2.1．Syslogによるロギングの概要

Syslogプロトコルは，出力されたログをUDPパケットとして収集サーバへ送信するという非常にシンプルなプロトコルである。図1にSyslogにより収集したログの一例を示す。個々のログには日付，出力したホスト名，関連するプロセス名などの情報が含まれている。ネットワーク管理者はこれらのログを解析し，ネットワークの運用管理やセキュリティ管理に活用するとともに，ネットワークの運用の健全性を示すものとして保存しておく必要がある。

```
Dec 18 14:17:01 mars CRON[6192]: pam_unix(cron:session): session closed for user root
Dec 18 15:17:01 mars /USR/SBIN/CRON[6256]: (root) CMD ( cd / && run-parts -report
/etc/cron.hourly)
Dec 18 15:17:01 mars CRON[6255]: pam_unix(cron:session): session closed for user
root
```

図1　Syslogにより収集したログのサンプル

OSやアプリケーションがSyslogを用いてログを出力する場合，出力するログはその種別と緊急度によって分類される。Syslogプロトコルで定められている種別と緊急度の一覧を表１と表２にそれぞれ示す。種別は24種類，緊急度は８種類であるため，ログは192種類に分類されることになる。

表１　ログの種別

| | | |
|---|---|---|
| kernel | uucp | local0 |
| user | cron | local1 |
| mail | authpriv | local2 |
| daemons | ftp | local3 |
| auth | ntp | local4 |
| syslog | security | local5 |
| lpr | console | local6 |
| news | cron | local7 |

表２　ログの緊急度

| |
|---|
| emergency |
| alert |
| critical |
| error |
| warning |
| notice |
| information |
| debug |

各ホストにおいて，ログの分類毎の出力先指定などSyslogに関する設定は，図２に示すようなsyslog.confファイルにテキスト形式で記述されている。syslog.confファイルの一列目はログの分類を表し，二列目はそのログの出力先を示す。例えば，図２の下線部の例では，種別に関わらず緊急度がwarningであるログは/usr/adm/syslogファイルに出力され，種別がkernel，緊急度がcriticalであるログは，ホストfinlandiaに送信されることを示している。

```
#ログの分類指定                #出力先
*.=debug                       -/usr/adm/debug
*.warning                      /usr/adm/syslog
*.=crit;kern.none              /var/adm/critical
kern.crit                      @finlandia
kern.crit                      /dev/console
kern.info;kern.!err            /var/adm/kernel-info
mail.=info                     /dev/tty12
mail.*;mail.!=info             -/var/adm/mail
*.=emerg                       *
*.alert                        root,joey
```

図２　Syslog.confファイルの例

ネットワークを通じてログを収集サーバへ集約する場合，Syslogではシステムを構成するホストは以下のいずれかの役割を持つ［１］。

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

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。

## 2.2.　構成管理の必要性と課題

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 すべての syslog の設定が正しくなければならない。

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。そして，その構成管理には以下の３つの要素が課題となる。

１．ロギングシステムを構成する各ホストの syslog 設定の収集
２．syslog 設定内容の解析
３．解析結果に基づくログ収集経路の可視化

次節では構成管理アプリケーションの開発について上記の収集・解析・可視化の３要素に分けて詳述する。

## ３．ロギングシステムの構成管理アプリケーションの開発

### 3.1. Syslog Configuration MIB を用いた設定情報の収集

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 を収集し，複数のホストにおける設定情報を照合して一貫性を検証することが必要である。本研究では，この syslog.conf の収集にインターネットの標準管理プロトコル SNMP を用いる。syslog.conf は通常のテキストファイルであるため，TFTP 等を使用して取得する方法も考えられるが，SNMP を利用する既存のネットワーク管理システムに，提案する構成管理をスムーズに統合するために SNMP を用いて syslog.conf を取得する方針を採用した。

SNMP による syslog.conf の取得には，新たに定義し暫定的に実装した Syslog Configuration MIB（Syslog-C-MIB）を使用する。Syslog-C-MIB の構造を図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 SNMP を利用して順に読み出すことで syslog.conf の内容を取得できる。

### 3.2. syslog.conf 解析用パーサの実装

各ログに対するホストの取り扱いを把握するためには，Syslog-C-MIB を利用してホストから収集した syslog.conf の内容を解析し，ログの分類毎に出力先を調査する必要がある。そこで本研究では syslog.conf の文法を調査し解析用のパーサを実装した。

図４に疑似 BNF 記法で表現した syslog.conf の文法を示す。この文法を元に，Ruby 言語用に開発されたパーサジェネレータである RACC［８］を用いてパーサを実装した。このパーサにより設定内容の解析の過程で文法エラーを検出できるようになるため，パーサ単体でも設定ミスを未然に防ぐことに貢献できる。

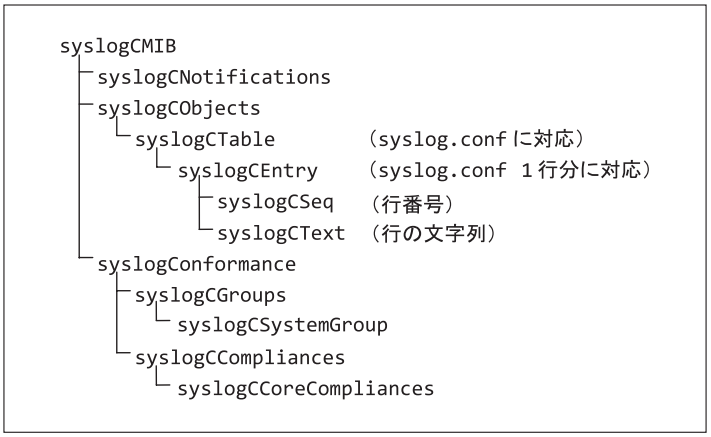


図３　Syslog Configuration MIB の構造

```
 <rule_list> ::= <rule> | <rule_list> <rule>
 <rule> ::= <selectors> <action>
 <selectors> ::= <selector> | <selectors> ';' <selector>
 <selector> ::= <facilities> '.' <severities>
 <facilities> ::= <facility> | <facilities> ',' <facility> | '*'
 <severities> ::= <severity> | '=' <severity> | '!' <severity>
              | '!' '=' <severity> | '>' <severity>
              | '=' '>' <severity> | '>' '=' <severity>
              | '<' <severity> | '<' '=' <severity>
              | '=' '<' <severity> | 'none' | '!' '*' | '*'
<facility> ::= 'mark' | 'kern' | 'user' | 'mail' | 'daemon'
              | 'auth' | 'syslog' | 'lpr' | 'news' | 'uucp'
              | 'cron' | 'authpriv' | 'ftp' | 'local0'
              | 'local1' | 'local2' | 'local3' | 'local4'
              | 'local5' | 'local6' | 'local7' | 'ntp' | 'netinfo'
              | 'remoteauth' | 'install' | 'ras' | 'launchd'
 <severity> ::= 'none' | 'emerg' | 'alert' | 'crit' | 'err'
              | 'error' | 'warn' | 'warning' | 'notice'
              | 'info' | 'debug'
 <action> ::= <remote_host> | <file> | <users> | <process>
 <remote_host> : '@' <host> | '@' <host> ':' <port-number>
 <host>  ::= HOSTNAME | IPV4ADDR | IPV6ADDR
 <port-number> ::= DIGITS
 <users> ::= <user> | <users> ',' <user>
 <user>  ::= '*' | USERNAME
 <file>  ::= FILENAME  | '-' FILENAME  | '|' FILENAME
 <process> ::= '|' PROCESSNAME
```

図４　疑似BNF記法によるSyslog.confファイルの文法表現

### 3.3. ネットワーク地図を利用したロギングシステムの構成可視化

本節では，ロギングシステムの構成管理を行うために開発した特定した収集経路をログの種別毎に可視化するアプリケーションのプロトタイプについて説明する。

Syslog-C-MIB を利用して収集した各ホストの syslog.conf をパーサによって解析することで，各ホストにおいてログの分類毎の出力先が明らかになる。そして，あるホストにおいてログの出力先が他のホストとなっている場合，その送信先のホストにおける設定の調査を再起的に繰り返すことで最終的な collector に至るログの収集経路を特定できる。収集経路をネットワークにおけるホストの接続関係を示したネットワーク地図上に可視化することで，直観的に経路を把握できるプロトタイプとした。ネットワーク地図の作成にはネットワーク地図作成用ライブラリ RomanAPI［9］を用いた。

図５に，開発したプロトタイプにより実際のロギングシステムにおけるログ収集経路を可視化した結果を示す。プロトタイプでは，ログの種別と originator のホストを選択するとそのホストから collector に至るログの収集経路を可視化できる。図５の例では，選択した３つの originator からのログが１つの relay を経由して collector に収集される過程を示している。

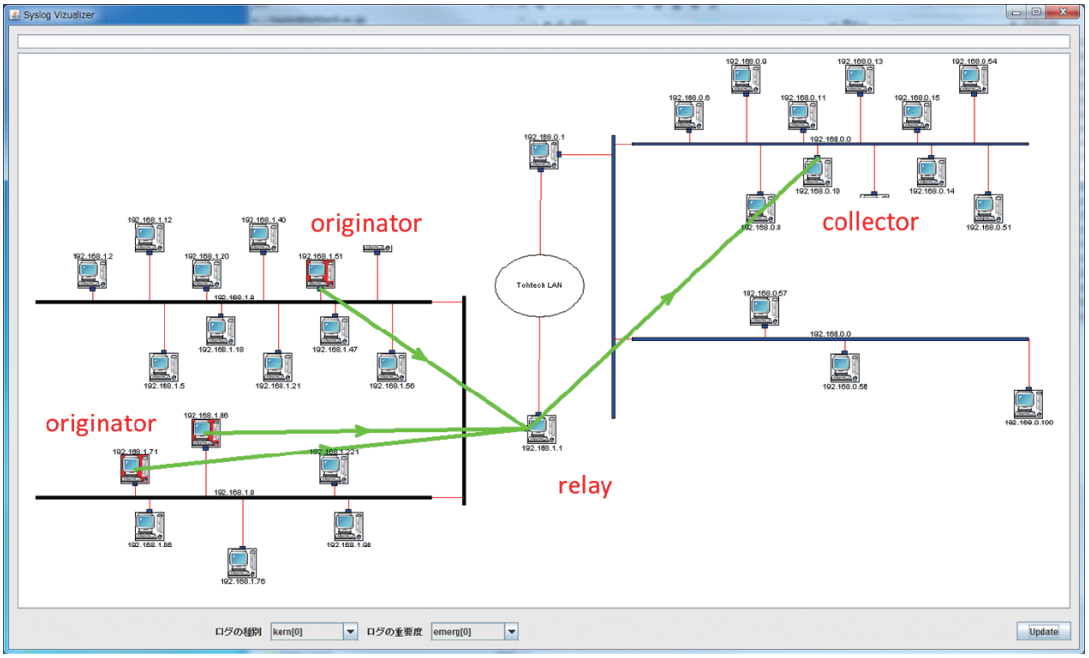


図５　ログ収集経路の可視化結果

図６に収集経路中にループを検出した場合のプロトタイプの出力を示す。前述のとおり，syslog.conf の設定は各ホストで独立しているため，ログの送信先を誤って設定した結果ループの発生が起こり得る。ループの発生はログの収集漏れを生じさせるだけでなく，ネットワークのトラヒックを爆発的に増大させることで，ネットワークの障害を引き起こす恐れがある。開発したプロトタイプを利用することにより収集経路を視覚的に把握できるため管理者がループの存在にいち早く気づくことができる。また，図６に示すようにループを自動的に発見しエラーメッセージを表示する機能を備えている。

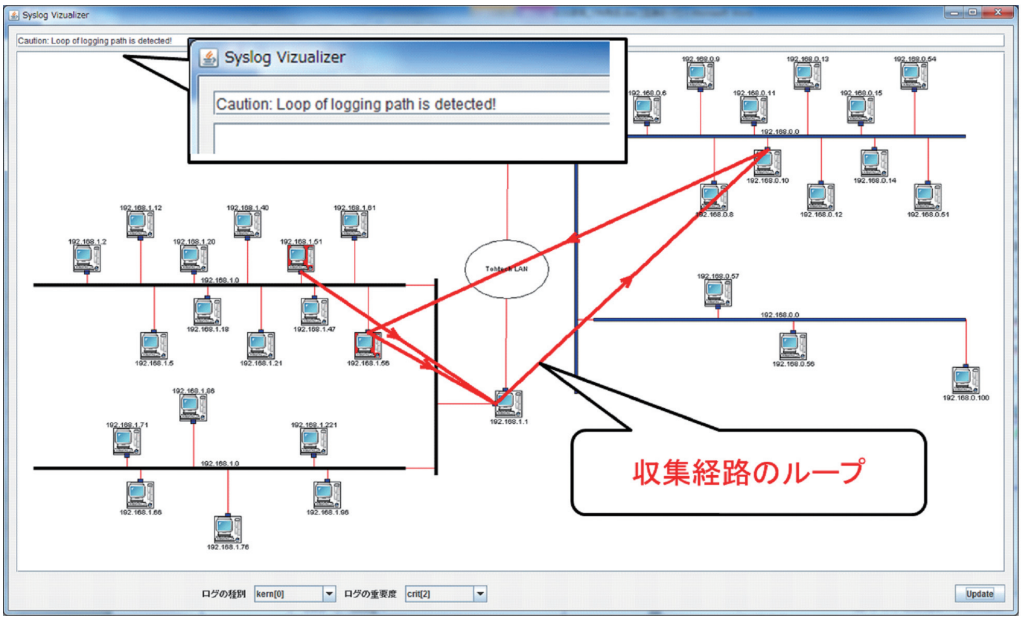


図６　収集経路中にループがある場合

## ４．おわりに

本研究では，ネットワーク管理において欠かせないログ情報を収集するロギングシステムの構成管理の実現を目的とし，ログの収集経路を可視化するアプリケーションのプロトタイプ開発を実施した。現在，ロギングシステムで広く使われている Syslog プロトコルでは，ログの収集経路はロギングシステムを構成する各ホストの設定によって定まる。しかし，複数のホストの設定に関して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おらず，設定の不整合が発生する危険性が存在している。そして，設定の不整合がログの収集漏れや収集経路のループに伴うトラヒック増大によるネットワーク障害を引き起こす可能性がある。本稿では，筆者らによる Syslog Configuration MIB を使用して収集した Syslog の設定情報を解析するパーサおよび解析結果に基づいてネットワーク地図として収集経路を可視化するアプリケーションを提案およびそのプロトタイプ実装結果を示した。本研究の成果によるネットワーク地図上の収集経路可視化は，ネットワーク管理者に対してロギングシステムの全体構成を直観的に提供する手段となる。今後の課題として，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，東北工業大学新技術創造研究センターの地域・産学連携プロジェクト研究費の援助により行われたものである。ここに記して謝意を表する。

## 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］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，“SNMPによるネットワークロギングシステムの構成管理” FIT2009 第８回情報科学技術フォーラム，2009年９月
［７］NET-SNMP, http://www.net-snmp.org/
［８］RACC, http://i.loveruby.net/ja/projects/racc/
［９］インターネットオリエンテーリング可能な地図構成法に関する研究
http://www.cysols.com/research/ipa/ipamaps/index_j.html