セキュリティ確保を目指したネットワークイベント記録の高信頼な収集と管理技術の開発（073102001）

Research and Development for Highly Reliable and Secure Log Management System

研究代表者

根元義章　東北大学大学院情報科学研究科

Yoshiaki Nemoto　Graduate School of Information Sciences, Tohoku University

研究分担者

和泉勇治†　角田裕††　キニ グレン マンスフィールド†††　太田耕平†††

Yuji Waizumi†　Hiroshi Tsunoda††　Glenn Mansfield Keeni†††　Kohei Ohta†††

†東北大学 大学院情報科学研究科　††東北工業大学 工学部　†††株式会社サイバー・ソリューションズ

†Graduate School of Information Sciences, Tohoku University

††Faculty of Engineering, Tohoku Institute of Technology　†††Cyber Solutions, Inc.

研究期間　平成 19 年度～平成 20 年度

概要

本研究開発では、ログ収集プロトコル SYSLOG を更新する新しい標準に、新たに管理性を付与する標準案を提案し、まずはその基盤となる管理情報（MIB）の国際標準を確立した。本 MIB は SYSLOG そのもののみならず SYSLOG に関する情報を扱う他の標準の基盤となるものでインターネット管理全体に対する貢献となる。また、その必要性、重要性を実験およびシミュレーションによって定量的に明らかにするとともに、今日の ICT インフラにふさわしいレベルの信頼性を実現する効率的なトランスポート技術、モバイル端末のログ管理技術、ロギングシステムの構成管理技術を確立した。本研究開発による国際標準技術・ロギングシステムの高信頼化技術は、次世代 ICT インフラを支えるセキュアネットワークの基盤となる技術である。

Abstract

In this project, we have worked on improving the manageability of the updated SYSLOG protocol and have specified a standard Management Information Base (MIB) for basic monitoring of logging systems. This MIB can be utilized by other standards that use information of SYSLOG systems and will contribute to the entire area of network management. Moreover, we have investigated the issues of SYSLOG logging systems through various experiments and simulations, and have proposed efficient transport techniques, log management technology for mobile terminals, and the technology for configuration management of logging systems. These technologies provide reliability that is essential in logging systems that are used in the current ICT infrastructure.

１．まえがき

インターネットの運用・セキュリティ管理は、ネットワークイベント記録（ログ）の収集と解析を基本としており、あらゆる対象から洩れなく確実にログを収集し、ログを運用・セキュリティ管理、さらには監査にも活用することが望まれている。しかし、インターネットでの事実上の標準として現在広く使われているログ収集プロトコル SYSLOG は、その起源の古さ故に信頼性・安全性・拡張性に多くの問題を有し、現在の ICT インフラが要求する水準からは大きく遅れをとっている。本研究開発では、SYSLOG の更新に貢献すると共に、SYSLOG 遠隔管理技術の国際標準化、およびそれを活用した次世代のログ管理技術の確立を目指す。

２．研究内容及び成果

本研究開発では図 1 に示すように、ログ収集プロトコル SYSLOG の管理用 MIB 群の策定とその標準化、実用的な観点からのロギングシステムの問題点の明確化、およびそれらを克服する技術の提案を行った。

SYSLOG への可管理性の導入と標準化

SYSLOG への可管理性の導入を目指し、SYSLOG によるロギングシステムをネットワーク管理の標準プロトコル SNMP から管理できるようにするために、株式会社サイバー・ソリューションズが中心となって以下の 3 種の管理情報ベース(MIB)を策定し、実装した。

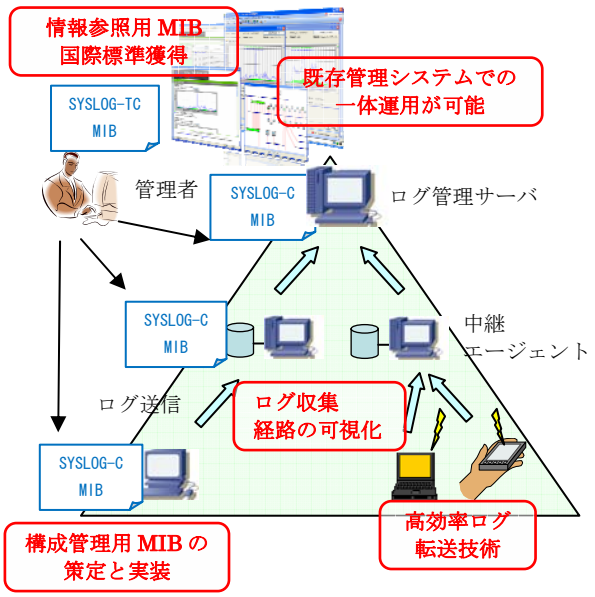

図 1 本研究開発の成果

●SYSLOG 管理用 MIB：SYSLOG-MIB
●SYSLOG 情報の参照用 MIB：
SYSLOG TC (Textual Convention)-MIB
●SYSLOG 構成管理用 MIB：
SYSLOG-C(Configuration)-MIB

これらの MIB を活用することにより、ネットワーク運用の根幹であるにも拘わらず従来はそれ自体の管理が軽視されていたロギングシステムを、他のネットワークシステムと同様にネットワーク管理の標準管理プロトコルによって統一的に管理することが可能となった。

このうち、SYSLOG-MIB と TC-MIB について IETF の SYSLOG WG において標準化活動を展開した結果、TC-MIB が WG からの標準案を経て標準化団体全体に対しての提案となり、最終的には、2009 年 3 月に

標準案（Proposed Standard）RFC5427

として発行された。本 RFC は、今後 SYSLOG に関連する管理標準を作成する際の基礎となる標準であり、他の RFC から参照されるなど、すでに活用が始まっている。

時間の網羅性を実現する分散型のログ保管技術の確立

東北大学が中心となって行った実ネットワークにおけるログ収集の実験から、従来は明らかにされていなかった以下の新たな知見を見いだした。

●発生するログの量は時間的にもネットワーク的にも大きな偏りが存在すること
●ログの損失が日常的に発生していること
●ネットワーク上の通信に問題がなくてもバースト的なログの発生によりログが損失すること

これらの事実はログが監査証跡として活用される上での大きな障害であることから、この問題に対して中継エージェントの階層配置によりログを分散して保管し欠損ログを回復する技術を提案した。提案では、ネットワークトポロジや各ノードからのログ送信量の偏りを考慮し、特定の中継エージェントに過度に中継処理が集中しないような設置場所の選択方式を検討し、シミュレーションによりその有効性を確認した。

さらに、上記技術の開発を通して、階層構造を成す中継エージェントによる分散型のログ保管を実現するためには、中継エージェントを含めたロギングシステムの構成管理が不可欠であることを明らかにした。そして、株式会社サイバー・ソリューションズと協力し SYSLOG 構成管理用の SYSLOG-C-MIB を新たに策定・実装した。そして、それを利用して全研究機関が共同で高信頼性ネットワークロギングシステムのプロトタイプ開発と実証実験を行い、実ネットワークに配備されたロギングシステムの構成を可視化し、ログの収集漏れの原因となる事象を効率的に把握できる技術を確立した。

対象の網羅性を実現する効率的なログ収集/転送技術の確立

東北大学と東北工業大学が中心となって以下の技術を提案した。

●ログの重要度に着目した効率的なログ転送プロトコル
●通信ストリーム数の動的制御機能を備えた適応型トランスポートプロトコル
●無線環境におけるモバイル機器からの効率的なログ収集方式
●高移動度なモバイル機器のための効率的な移動管理方式

これらの技術により、ネットワーク管理上重要な対象となりつつある移動端末をログ収集の対象とすることが可能となる。移動端末からのログ収集は、無線通信の利用が前提であること、端末自身が十分なリソースを有していないケースも多いため効率化が必要であること、の 2 点が課題であった。上記の提案はそれらの課題に対する解決策を与えるものであり、ログ収集対象の網羅性を大きく高めることに繋がった。

３．むすび

国際標準における本研究開発の成果は、SYSLOG だけではなく、SYSLOG 情報を利用するすべての管理標準から利用できるものであり、ネットワーク管理全体への貢献となった。ロギングシステムの運用面では、これまでのシステムでは不十分であった網羅性・信頼性を大幅に向上させ、ICT インフラの運用管理の最前線であると同時に、その健全性を保証するという点では最後の砦となるログ管理に「信頼できる完全な記録」を実現する技術を確立した。

今後は、議論中となっている SYSLOG-MIB、新たに策定した SYSLOG-C-MIB の国際標準化に向けて、引き続き IETF の SYSLOG WG において積極的な標準化活動を行っていく。また、既存の SYSLOG 実装である syslog-ng, rsyslog などに対して本研究開発の成果の活用を働きかけ、高信頼なロギングシステムとして成果の普及を図る。

【国際標準提案リスト】

[1] IETF SYSLOG WG、RFC5427、Textual Conventions for Syslog Management、提案年月日：2007 年 5 月 22 日、修正提案年月日：2007 年 6 月 21 日、7 月 7 日、12 月 3 日、12 月 4 日、2008 年 1 月 21 日、2 月 5 日、4 月 30 日、5 月 23 日、採択年月日：2009 年 3 月

[2] IETF SYSLOG WG 、draft-ietf-syslog-device-mib-17.txt 、Syslog Management Information Base、提案年月日：2001 年 9 月 9 日、修正提案年月日：2007 年 7 月 9 日、2008 年 2 月 12 日

【参加国際標準会議リスト】

[1] Internet Engineering Task Force (IETF)・70th IETF,Vancouver,BC,Canada,December 2-7,2007

[2] Internet Engineering Task Force (IETF)・71st IETF,Philadelphia,PA,USA,March 9-14,2008

[3] Internet Engineering Task Force (IETF)・72nd IETF,Dublin Ireland,July 27-August 1,2008

【誌上発表リスト】

[1] H. Tsunod, T.Maruyama,K.Ohta, Y.Waizumi, G.Mansfield, and Y.Nemoto ,"A Prioritized Retransmission Mechanism for Reliable and Efficient Delivery of Syslog Messages", Proceedings of Communication Networks and Services Research Conference (CNSR 2009), (accepted: will be published in May 2009)

[2] 角田、丸山、阿部、太田、和泉、キニ、根元、“ログの重要度に基づいた適応型送信制御による効率的なログ転送方式の提案”、電子情報通信学会技術研究報告 Vol.107、No.530、CS2007-78、pp.27-32（2008 年 3 月 6 日）

[3] 太田、 “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、 pp.17-20、IPA セキュリティセンター、 2009 年 3 月 23 日

【本研究開発課題を掲載したホームページ】

http://http://www.cysol.co.jp/research/SCOPE-Syslog/index_j.html