Vol.2013-IOT-20 No.34
2013/3/15

ネットワーク機器動作ログ参照サービスの試作

田島 浩一　西村 浩二　近堂 徹　岸場 清悟
大東 俊博　岩田 則和　相原 玲二

ファイアウォールや IDS，認証ネットワークの利用などネットワーク機器の利用状況や動作についての確認方法は，最新の状態は SNMP 等の管理用プロトコルの利用により可能であるが，過去の動作は基本的に動作ログとして外部出力されるものを利用する事になる．過去の動作ログの利用として，たとえば IDS やファイアウォールの動作ログについて，警告の様なログの累積が一定数を超えた利用についてその確認を行うといった調査が可能である．本研究ではネットワーク機器の動作ログを参照するサービスとその試作，および，学内で運用している IDS やファイアウォールの動作ログを対象として処理した際の評価について報告する．

A Trial of Event Log Reference Service for Networking Devices

Koichi TASHIMA　Kouji NISHIMURA　Tohru KONDO　Seigo KISHIBA
Toshihiro OHIGASHI　Norikazu IWATA　Reiji AIBARA †

The way of current confirmation of such as usage or behavior of these devices (firewall, IDS, network switch authentication) are managed by the management protocol such as SNMP protocol. On the other hand, the way of confirmation of behavior in the past is managed by access of the external output operation log. As an example of the use of the log of past behavior, it can use to examine the reason why the cumulative warning log has exceeded the limits.
In this paper, we describe about a trial of implementation of event log reference service for networking devices. And report on the evaluation of these devices (firewall and IDS) operating in campus network.

1. はじめに

ネットワークのセキュリティ対策等で用いられているファイアウォールや IDS，管理機能を持つネットワークスイッチやルータ等では，装置の動作を外部にログとして出力する機能を持つものが多く，通常はログを記録する様に設定し運用される．これらの機器で現在の設定や動作状況の確認は，これらの機器管理を目的とした SNMP 等管理用のプロトコルが利用可能であるが，装置内の記憶容量を超える過去の動作については，出力され保存される動作ログのみで参照可能である．

IDS による監視およびインシデント発生時の追跡に関して，中村らの報告[1]では，追跡および記録の抽出を自動化し管理者の運用コストを削減する方法が提案されている．本手法では後述する IDS の動作ログ集計において IDS の追跡記録を行う目的は同じであるが，対象の通信以外にその前後の通信を検索対象として利用する点が異なる．

広島大学では，2008 年度より新キャンパスネットワークの HINET2007 [2]の運用開始にあわせて，新キャンパスネットワークの利用においては，ユーザ端末は原則として認証利用し利用記録を残すとともに，ファイアウォール，IDS およびそれら管理用としてログサーバを設置し不正アクセスおよびインシデント発生時の追跡のため記録保存をする構成とした．

本報告では，これらネットワーク機器の動作ログを参照可能なサービスとして構成し，利用クライアント例として IDS が検出する不正アクセスの一部についてその集計に利用する実装を行いその評価を行った．

2. システム要件および必要機能

実装へのシステム要件および必要機能，動作概要について機能毎に以下に示す．

2.1 動作ログ参照サービス

本サービスの対象である，動作をログとして出力可能なネットワーク機器は多岐にわたり，機器の種類等により多様であり，表記方法が統一規格化されていない．同一の製造元であっても製品やその世代等でも出力が異なる場合がある．しかしながら，ファイアウォールの動作ログの例では，ログのメッセージは異なっていても，動作としては，

† 広島大学 情報メディア教育研究センター
Information Media Center, Hiroshima University

ⓒ 2013 Information Processing Society of Japan

通過/遮断の区別，通信の送信元/送信先アドレスおよびポート番号など一般的に共通した動作が多く記録される事が想定される．これらファイアウォールのログについてはIPアドレスや時刻等を検索キーとし，該当するレコードを提供する事が求められる．

他方，認証ログについては認証に RADIUS プロトコル[3]が用いられる場合が多く，その場合はメッセージ表記の多くがプロトコル対応により標準化されたものが使用されている．これら認証ログについては，現在のネットワーク構築時に認証ログを管理者権限による WEB アクセスで閲覧および検索できる機能を用意しているが，権限に応じた検索や取得範囲の設定機能を用意していなかった事（現状では管理者権限で全ての機能を利用可能）と，自動実行により機械アクセスを繰り返す参照元のプログラムに管理者権限相当の ID を設定する必要がある．そのため，実装では，本サービスをどの権限どれだけの回数が参照されたかなどを管理するため,検索の範囲や取得する対象の指定等,検索のパターンに応じたアクセスキーおよびそのパスワードを発行し利用する方法とした．

2.2 IDS ログ集計システム

IDS の動作は，広く知られる通り通信の監視を行い，侵入を試みようとする通信などを検出する.その方法として，事前に設定および定義した特定のパターンと照合して一致した通信が見つかった場合に警告を出力するが，正常な通信の一部が意図せずにパターンに適合すると誤って警告対象となる false positive が発生する．

IDS で検出される警告は，警告対象の通信を行っている利用者へ通知し改善を求める事で不正アクセスやその未然対策が期待されるため，学内のポリシーに違反する通信より，まず数種類に限定して利用者へ通知し確認または改善を求める為の集計システムとして構築した．なお，集計結果は利用者への通知する際に，一定量の false positive を考慮して警告数に対する通知の閾値設定や，警告対象となった通信やその通信先，および，対象の通信についてその前後の通信についてのファイアウォールログ等での確認等を目的とする．実際の運用例では，通知の結果 false positive と確認された際にその原因調査および検出方法の設定変更等に利用する．

3. システム構成

本稿で構築したシステム構成例を示す．

3.1 サーバ構成

図 1 に試作を行ったサーバ等システム構成を示す．既設のネットワークおよびサーバ構成は運用中であるため構成等を変更せず，また，構築するログ参照サービスで性能の評価も行うため，既設の構成にログ参照用としてサーバを新設する構成とした．

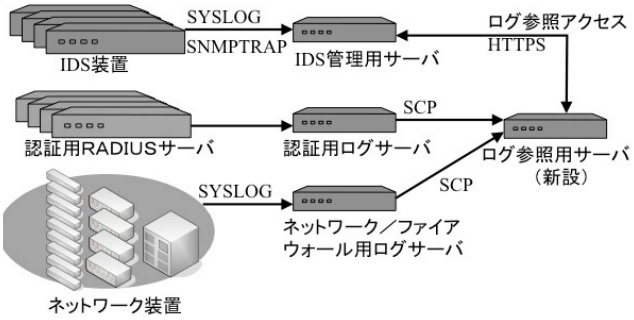

図 1　システム構成図
Figure 1　System configuration.

ログ参照用サーバには，2.1 節の必要機能の通り認証ログおよびファイアウォール等のネットワークログをそれぞれ保存されている既設サーバから転送され，ログ参照用サーバ内のデータベースへ登録される．

認証ログ　ネットワーク装置で提供されている WEB 認証および MAC 認証の動作ログを保存する．対象機種は，本キャンパスで用いられている認証スイッチの，アラクサラネットワークス社製 AX1230 / AX2430/ AX2530 / AX6300 の 4 機種に対応させた．

ファイアウォールログ　対象機種は，同じく本キャンパスで用いられている CISCO 社製 Catalyst6500 用ファイアウォールサービスモジュールに対応させた．

3.2 参照アクセス及びアクセスクエリーの構成

ログ参照を行うアクセスは，通信プロトコルに HTTPS を，クエリーの記述を XML 形式，返答の記述を XML および CSV 形式とした．

リクエストに記述するクエリーには，指定する項目名と値を用いるキーバリュー型とし，キーに相当する部分は，

表 1　認証ログの項目名
Table 1　Attribute of authentication log.

項目名	RADIUS Attribute
IP アドレス	Framed-IP-Address
MAC アドレス	Calling-Station-Id
WEB 認証時のログイン ID	User-Name
ログイン先認証スイッチ IP アドレス	NAS-IP-Address
ログイン先認証スイッチ ポート番号	NAS-Port
ログイン先ポートの VLAN-ID	NAS-Identifier
UNIX-time 表記での時刻	Timestamp
ログインとログアウトの識別	Acct-Status-Type
MAC アドレス	Calling-Station-Id

ⓒ 2013 Information Processing Society of Japan

認証ログの多くが既に対応していた RADIUS および RADIUS アカウンティング（RFC2865 等）を基本的に用い，ファイアウォールのログについては類似する文字列をキーとして定義した．クエリーに用いた項目名を，表 1 および表 2 に示す．

表 2　ファイアウォールログの項目名
Table 2　Attribute of firewall log.

項目名	Attribute
IP アドレス　および ポート番号	Source-/Destination-/Wan-IP-Address / Port
プロトコル種別	Protocol-Code
処理内:Drop/Droped /Deny/Denied/ Teardown/Built-inbound/-outbound . . .	Message-Code
セッション ID	Session-ID
イベント ID	Event-ID
UNIX-time 表記時刻	Timestamp
FW 装置名	Device-Identifier
付加メッセージ	Message

4. 実装および性能評価

３節のログ参照サービスについて以下の通り実装評価を行った．

4.1 実装環境

本稿で用いたサーバ構成を 3 に示す．

表 3 サーバスペック
Table 3 Server specifications.

サーバ	スペック
IDS 管理用	CPU: Xeon E5645 @2.40GHz(6core) / Memory 16GB / Gb-Ether / CentOS6.0
ログ参照 サービス用	CPU: Core i7-2600 @3.40GHz(4core) / Memory 16GB / Gb-Ether / CentOS6.2

これら 2 台のサーバは同一のサブネット内に設置され，ICMP による RTT 測定では 0.3[ms]でありホスト間の通信には遅延はほぼ無い構成である．

ログ参照サービス用として HTTPS には Apache 2.2.15 を，データベースソフトには，mysql [5] Ver 14.14 Distrib 5.1.61 をそれぞれ用い登録および参照に用いるプログラムは perl および perl 用 SQL データベースのモジュールを用いて実装した．

4.2 評価環境および測定結果

ログ参照サービス用サーバで処理されるログの量を図 2

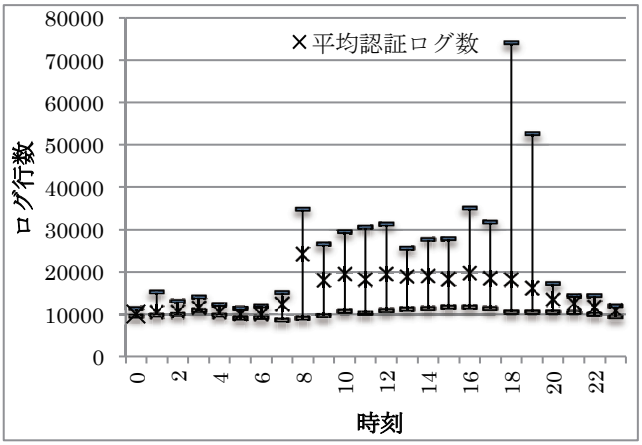

図 2 認証ログ数（2013 年 1 月 4 日～1 月 31 日）
Figure 2　Number of authentication log (2013/01/04-2013/01/31)．

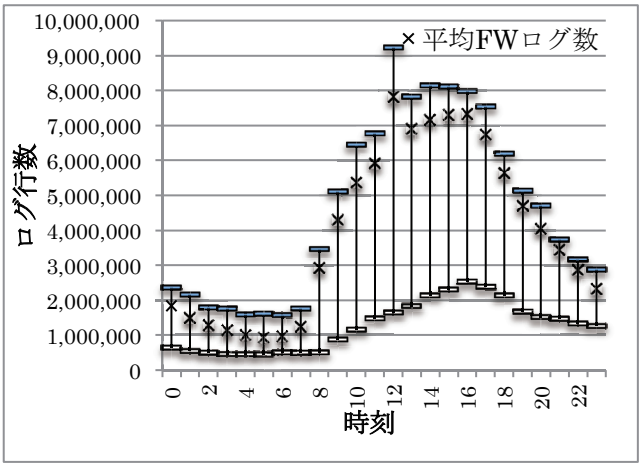

図 3 ファイアウォールログ数(2013 年 1 月 4 日～1 月 31 日)
Figure 3　Number of firewall log (2013/01/04-2013/01/31).

および図 3 に示す．図 2 の認証ログの処理対象は 3.2 節の認証ログの仕様の通りログ仕様が標準化されているため登録に要する時間は，毎回の処理でファイアウォールログの登録時間の約 20 分の 1 以下の処理時間であった．

1 時間分のファイアウォールログの登録に要する時間は，評価期間の 2013 年 1 月 4 日～1 月 31 日では，最大で約 922 万エントリの登録時の 27 分 02 秒が最大であったが，処理時間は処理ログ数に比例する結果となり，毎秒の平均処理可能エントリ数は約 6400（期間の最大 6612，最小 6157）であった．

参照元となる IDS 管理用サーバでは 1 時間毎に過去の 1 時間分の集計を行い管理者用 WEB ページへ更新掲載している．このタイミングに合わせて，ログ参照サービスサーバへのログの取り込みは，既設のログサーバより SCP コマンドにより 1 時間毎に転送を行いログ参照サービス内デ

ⓒ 2013 Information Processing Society of Japan

ータベースへ登録を行う．そのため 1 時間分の処理に 1 時間以上を要しない事が求められるが現在の構成では処理が可能という結果であった．

5. おわりに

本報告では，ログ参照サービスの試作，および，サービス利用例として IDS 管理サーバにインシデント集計システムをそれぞれ実装した．試作したログ参照サービスは，IDS 管理サーバで行われていたスケジュールを変更する事なく予定されていた処理時間が実現可能であった．

実際に運用中のシステムで利用していると，数秒程度のログ時刻のずれが発生する事があり，それらを考慮し対象とする時間の前後の範囲を指定して検索する機能が必要となる．そのためデータベースには範囲検索に有効と考えられる SQL 型を用いたが，保存するデータの特性や条件次第では，でより効率がよいとされる非 SQL 系のデータベースでの実装比較を今後予定している．

謝辞　HINET2007 の構築および運用に尽力して頂いている広島大学総務室情報化推進グループおよび情報メディア教育研究センターの関係者に感謝します．また，本研究の一部は日本学術振興会科学研究費補助金　課題番号（23500089，24300025）の支援を受けて実施しています．ここに記して謝意を表します．

参考文献

1) 中村，戸田，井上，福田：侵入検知とモニタリングシステムを組み合わせた異常トラヒックの自動保存, 情報処理学会研究報告, IOT-12(38)，pp. 1-6, (2011).
2) 広島大学情報メディア教育研究センター: HINET 2007 情報, http://home.hiroshima-u.ac.jp/infra/hinet2007info
3) RADIUS protocol，RFC 2865, http://www.ietf.org/rfc/rfc2865.txt
4) 田島，近堂，岸場，大東，岩田，西村，相原：大規模キャンパスネットワークにおける MAC アドレス認証端末の移動管理，学術情報処理研究，no.15, pp.53-60, (2011).
5) Mysql website: http://www.oracle.com/jp/products/mysql/index.html

ⓒ 2013 Information Processing Society of Japan