全学ネットワークログの蓄積・参照システムの実装と評価

近堂 徹[1,a)]　田島 浩一[1]　岸場 清悟[1]　吉田 朋彦[1]　岩田 則和[1]　西村 浩二[1]　相原 玲二[1]

概要：ネットワーク機器で日々発生するログには，ネットワークを管理・維持していくうえで欠かせない重要な情報が多く含まれる。その一方，ネットワーク構成が大規模化・複雑化し，出力されるログも肥大化するなか，その蓄積および抽出プロセスを効率化するためのログ管理基盤が求められている。本論文では，全学ネットワークで提供する複数サービスが出力するログを集約し，クラウドサービスを活用したログ蓄積・参照システムの実装と評価について述べる。広島大学で運用するキャンパスネットワークへの導入を通じて，その効果と課題について考察する。

キーワード：ネットワーク運用，ログ管理，クラウドサービス

Implementation and Evaluation of a Campus Network Log Management System

Tohru Kondo[1,a)]　Koichi Tashima[1]　Seigo Kishiba[1]　Tomohiko Yoshida[1]　Norikazu Iwata[1]
Kouji Nishimura[1]　Reiji Aibara[1]

Abstract: Various logs which are generated from network equipments day-by-day include important information to manage the network. Meanwhile, the growing logs which are generated caused by diversity and complexity of the network have required the efficient log management infrastructure for archiving and processing. To improve this issue, in this paper, we propose the network log monitoring and management system. The proposed system aggregates numerous logs generated from multiple services on the campus network, and accumulates and analyzes using cloud service. We also describe the integration to the Hiroshima university's campus network system, and show the effectiveness and issues of the proposed system through its application.

Keywords: Network Operation, Log Management, Cloud Service

1. はじめに

大学などの高等教育機関におけるキャンパスネットワークは，単にインターネット接続を提供するだけでなく，ICTを活用した授業支援や学外者も含めたBYOD，基幹業務系での利用など，組織の様々な活動を根底から支える重要な情報基盤となった。ネットワークの障害が大きな損失を招きかねないことから、ネットワーク機器やIPアドレス等の各種資源の常時監視といった定常運用時の品質確保が必要となり，運用管理の効率化が求められている。一方，ユーザの利便性を損なわない形でセキュリティを確保することも必要となる。近年，ファイアウォールやIPS/IDS，WAF，認証スイッチ等のセキュリティ機器を導入し，アクセスコントロールや利用者認証によるセキュリティ対策も一般的となり，多くの組織で導入されている。これらのネットワーク機器で発生するログは，ネットワークの常時監視や品質管理といった運用管理目的に利用したり，不正アクセスの予兆検出，インシデント時の利用者追跡といっ

[1] 広島大学情報メディア教育研究センター, Information Media Center, Hiroshima University
[a)] tkondo@hiroshima-u.ac.jp

ⓒ 2016 Information Processing Society of Japan

たセキュリティ目的に利用したりするなど，その用途は多岐にわたる。特にセキュリティ目的では，迅速かつ的確な対応が求められ，内部統制を図るうえでも重要度の高いログの管理が必要不可欠となる。

しかしながらネットワーク構成は複雑化し，取り扱う情報も肥大化する一方であり，運用ログの保管および抽出プロセスを効率的に行うためのログ管理基盤が課題として存在する。広島大学では，2007 年度より全学整備および一元管理によるキャンパスネットワークを構築し，各種ログについて集約化を行ってきた [1][2]．さらには，2014 年度からパブリッククラウドサービスを利用したログ蓄積や分析を行っている。本論文では，キャンパスネットワークにおける全学ネットワークログの蓄積・参照システムについて述べ，これまでの運用における本システムの効果と課題について考察する。

本論文の構成は以下の通りである．まず 2 章では，大学等におけるネットワークログの運用管理や活用に関してまとめる。3 章ではログ蓄積・参照サービスについて提案し，キャンパスネットワーク HINET2014 における実装について述べる。4 章で本システムの性能評価について示し，5 章では導入の効果や課題について考察する。最後に 6 章でまとめを記す。

2. ネットワーク運用におけるログ管理

日々のネットワーク運用で発生するログには，ネットワークを管理・維持していくうえで欠かせない重要な情報が多く含まれる。例えば，ファイアウォールや IPS/IDS ではクライアントからの通信ログが残り，認証スイッチや認証サーバでは利用者や機器の認証ログが残る。また，ネットワークに接続する機器が DHCP でアドレス取得を行えば IP アドレス払出し情報がログに残る。これらのログは通信履歴の把握や利用者追跡を行う上で重要な情報となる。なお，本論文ではキャンパスネットワーク内の設備で発生する各種ログ情報を総称してログと表現する。

これまで，大学におけるログ情報の分析に関する報告は数多く行われている。文献 [3][4][5] では，無線 LAN を対象にした利用動向を調査する目的でログ管理・分析が行われている。無線 LAN には，授業・実習で利用するための持込パソコンだけでなく，構成員が保有するスマートフォンなどのモバイル端末が数多く接続され，かつキャンパス内を移動する。これらの利用動向ログは大学での様々な活動を把握・分析するためのデータとして価値の高いもののひとつとして考えられる。文献 [6] では，無線 LAN に加えて有線 LAN も対象とした学内 LAN 利用ログの分析が行われている。この報告では，学内ネットワークにおける主要なログを 1 カ所に集約し，識別非特定情報に変換 [7] して蓄積するシステムが提案されている。また，利用動向を把握するだけでなく，システム連携による分析アプリケーションの開発も視野に入れられている。

セキュリティの観点からログ分析を行うシステムとして，近年 SIEM(Security Information and Event Management) が注目を集めている。組織内の様々な機器から集めたログ情報に対して相関分析等を行い，セキュリティインシデントの予兆が発見された場合や異常があった場合に通知する仕組みである。SIEM をサービスとして提供する企業も出始めている。筆者らが所属する広島大学でも，これまでネットワーク機器のログ収集および参照サービスの構築と運用を行ってきた [8]。2007 年度より全学整備および一元管理によるキャンパスネットワークを構築し，ネットワークの利用時に研究室を含むすべての利用場所で何らかの利用者認証を要求する。各装置からの出力ログを集約して管理することで，接続機器や通信状況の把握を行っているが，現状では相関分析等の高度な活用までできていない。

ログ保存について考えると，多くの大学で行われているログ収集および管理は学内のログサーバで蓄積されているケースが多い。SYSLOG[9] や fluentd[*1] 等のログ管理ツールでログサーバに集約されたログは，テキストファイルもしくはデータベースに保存され，ネットワーク管理者（以下，管理者）は必要に応じてログファイルを開いて検索をしたり，データベースに接続して SQL 等で検索したりすることになる。そのため，蓄積データ量の上限や検索性能はサーバのハードウェア性能に大きく依存する。また，集約されたログに対して，検索条件の指定により横断的な検索を行う場合，より時間を要する場合もある。

一方で，近年のクラウドコンピューティングの普及により安価に高性能な計算資源を利用できるようになったことで，BI ツールやデータウェアハウスサービスの活用が進んでいる。しかしながら，これらのクラウドサービスをログ解析基盤として活用するには，ログの集約およびクラウド連携をどのように行うかを検討する必要がある。本論文では，ログの収集・蓄積および管理手法に焦点を当て，パブリッククラウドサービスを活用したシステムを提案する。

3. ネットワークログ蓄積・参照システム

2 章ではネットワーク運用におけるログ管理の現状と課題について示した。本章では，提案するネットワークログ蓄積・参照システム（以下，本システム）の構成と動作概要，および本学のキャンパスネットワークへの導入について述べる。

3.1 システム構成と動作概要

システム構成を図 1 に示す。本システムは，ログ収集部，ログ蓄積部，ログ参照部の 3 つの機能ブロックからなる。以下に機能毎に動作概要を述べる。なお，ログ収集部はオ

[*1] http://www.fluentd.org (2016-9-18 参照)

ⓒ 2016 Information Processing Society of Japan

ンプレミス環境，ログ蓄積部はパブリッククラウドサービスを利用して構成することを前提としている。

3.1.1 ログ収集部

ログ収集部は，ログ収集機能とストレージ蓄積機能で構成される。

本システムが対象とするログは，ネットワーク機器やサーバなど，出力元や種類が多岐にわたることを想定しているため，ログの集約化と蓄積のための前処理が必要となる。そこで，ログ収集機能では，特定の機器から送信されるログを SYSLOG 経由で受信し，facility と送信元 IP で分類した後，異なるテキストファイルに出力する。一旦テキストファイルとして出力することで必要な加工を行うとともに，最低限の最新ログをキャッシュとしてローカルストレージに保管しておくことも可能となる。

ストレージ蓄積機能は，ログ受信機能によって出力されたファイルを解析・構造化して，ログストレージにアップロードする機能を提供する。ストレージ蓄積機能は，ログ受信機能とは別のプロセスで動作し，定期的に実行する。なお，現時点では以下に示す一連の処理に要する時間とログの流量から 5 分間隔で本機能を実行している。なお，アップロード失敗などの異常が発生した場合には，次のタイミングでのアップロード処理時にあわせてアップロードが行われる。

まず，実行毎にテキストファイルの追加出力分を処理対象とし，ログ文字列を正規表現で解析して定義するデータ形式に構造化する。その後，ログの集合を，集約キー集合が一致するものごとに集約化する。集約キー集合とは，テーブルごとの特定の項目の集合を指すものである。集約した後は，検索等で必要となる付加情報の補完処理を行う。例えば，送信元 IP アドレスからホスト名への変換は DNS 情報を参照したり，利用者 ID はシステム内の LDAP 情報を参照したりする処理が該当する。これらの前処理を経て，ログストレージにアップロードされる。データの集約処理については 3.3 節で実例を用いて説明し，クラウドサービスへのアップロードについて 3.2 節で詳細に述べる。本機能により，各装置から収集されたログが参照しやすい形で構造化・永続化される。

3.1.2 ログ蓄積部

ログ蓄積部は，アップロードされたログを蓄積し，管理者からの要求（検索，集計，データ削除など）に応じた処理を行う機能を有する。本機能部はクラウドサービスを利用して実現する。これにより，ログ流量や頻度，保存期間といったシステム要件に応じて適切なサービスを選択できることに加え，検索性能についても扱うデータ量に対してクラウド側の計算資源を動的に増減させることで柔軟な性能変更に対応できるというメリットがある。また，蓄積部への制御（データ追加・削除・検索等）は API を利用することで，外部サービスとの境界を明確化することができる。

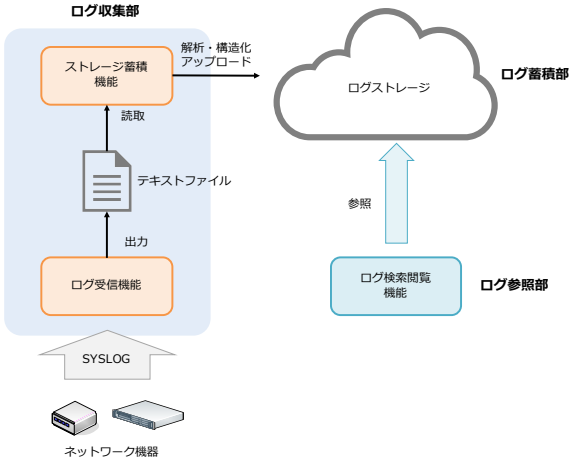

図 1 システム構成概要

クラウドサービスの利用については，3.2 節で述べる。

3.1.3 ログ参照部

ログ参照部は，CUI もしくは GUI で提供されるインタフェースにてログ参照のアクセスを受け付け，ログ蓄積部に対してクエリを発行して結果を表示する機能を有する。この機能により，蓄積したログを属性や期間等でインタラクティブにフィルタリングして検索することができる。ログ蓄積部との通信は定義された API を利用することで，汎用性と拡張性を確保する。

3.2 クラウドサービスの利用

本システムでは，ログ蓄積部はクラウドサービスとして Amazon Web Services が提供する Amazon Redshift（以下，Redshift）[*2] を利用する。Redshift は，列指向データベースを採用し，データ保存量や性能に応じて容量・インスタンスをスケールすることができ，複数インスタンスによるクラスタ構成にも対応するデータウェアハウスサービスである。データアクセスのための API が公開されているほか，通常の PostgreSQL 互換の JDBC/ODBC ドライバで接続することができるため，SQL を基本とした既存アプリケーションとの親和性も高い。

Redshift へのデータは Amazon S3（以下，S3）を介してアップロードする。3.1.1 のストレージ蓄積機能では，データを S3 に対して HTTPS でアップロードし，その後 Redshift の COPY コマンドを実行して S3 から Redshift へデータをロードする。データロードが完了するとアップロードしたファイルは削除するため，S3 のデータ領域は一時的に利用するのみで増加することはない。

なお本システムでは，Redshift 上のデータは一定保存期間を超えた場合か設定する最大容量を超えた場合のいずれかを選択し，古いデータから削除する。したがって，組織のセキュリティポリシーで定めるログの保存期間やログ流

[*2] https://aws.amazon.com/jp/documentation/redshift（2016-9-18 参照）

ⓒ 2016 Information Processing Society of Japan

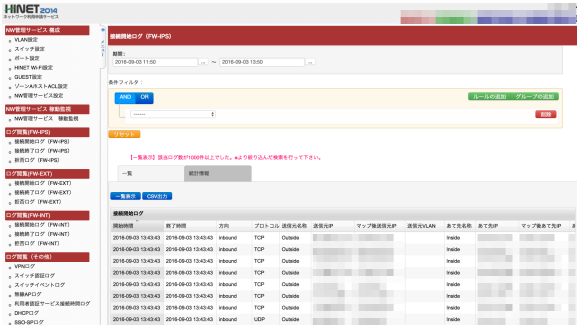

図 4 ネットワーク利用申請サービス (GUI) での検索画面

量に応じて，最大保存期間を柔軟に定義することができる。

3.3 キャンパスネットワーク HINET2014 への実装

広島大学では，2014 年 8 月より運用するキャンパスネットワーク HINET2014 のなかで本システムを実装している。本節では，その実装方法と対象とするログの具体例について示す。

HINET における基幹サーバ構成を図 2 に示し，本システムが対象とするログの種類を表 1 に示す。HINET では，約 2,000 の個別ファイアウォール (NAPT) 機能と DHCP サーバ機能をキャンパスネットワークの機能として全学的に提供し，すべての場所でウェブ認証（シングルサインオン認証を含む）もしくは MAC アドレス認証による利用者認証，全学整備の Wi-Fi では WPA2 エンタープライズによる 802.1X 認証を行っている。したがって，ネットワーク機器やサーバで取得するログによって，学内ネットワークにおけるほぼ全ての利用動向を把握することができる。なお，基幹ネットワークの具体的な構成については文献 [2] にて示しているため，そちらを参照されたい。

一例として，IPS 装置で記録される学内クライアント端末からの接続開始ログのデータ構造を表 2 に示す。なお，可読性を上げるために一部内部処理で利用する属性については表には掲載していない。3.1.1 で示した通り，ログ集約部では，単位時間に [方向，プロトコル，送信元 IP，マップ後送信元 IP，宛先 IP，マップ後宛先 IP，宛先ポート] の組が一致したログについては集約して構造化することで，ログの圧縮を行っている。図 3 にログの集約・構造化の例を示す。

管理者が閲覧する GUI（ウェブインタフェース）画面の様子を図 4 に示す。管理者は障害時や利用者からの問い合わせ時に，本画面でインタラクティブ対象を絞り込みながら動作状況を把握することができる。バックエンドで，Redshift に対して API を用いたアクセスが行われる。このほかにも，シェルスクリプト等の CUI からも SQL を利用してログの検索を行うことも可能である。

4. 性能評価

実際に運用中のシステムを用いてログ検索に要する時間について計測し，性能評価を行う。本論文では，表 1 で示したログ種別の中でも特にログの流量が多い IPS 装置の接続開始ログを対象とした評価について述べる。

4.1 検索性能の比較評価

本システムの検索性能を確認するために，検索条件を指定した際の抽出時間について測定する。参考として，テキストログおよび RDB による従来型の検索手法でのログの抽出時間についても確認した。

測定では，(1) ログ集約部でキャッシュとしてローカルサーバに一時保管しているテキストログ, (2) 集約・構造化されたログを保存した RDB，(3) 運用中の本システムに蓄積されたログ，の 3 つに対して同一条件での検索を行い，結果出力までに要した時間を計測する。検索条件としては「2016 年 8 月 1 日に発生した，宛先 IP アドレスが 182.22.71.250（www.yahoo.co.jp の正引きアドレスのひとつ）に対する新規接続」とした。

各測定における使用機器および実験条件を表 3 に示す。テキストログは 1 日単位で分割されており，検索対象（8 月 1 日分のみ）のファイルサイズは 54GB で，行数は 336,106,250 行であった。RDB については，本システムと同一構造のテーブルを作成し，そこに集約・構造化後したログ（8 月 1 日分のみ）をインポートした。本システムでは 2016 年 1 月 23 日以降のログが全て蓄積された状態となっている。表 3 には実験開始時のログ登録件数を記している。テキストログに対する測定では grep コマンドにて抽出を行い，RDB および本システムでの測定では SQL コマンド（「where (start_datetime between ’2016-08-01 00:00:00’ and ’2016-08-01 23:59:59’) and dst_ip = ’182.22.71.250’」による条件指定）を用いてデータベース接続して抽出を行った。

結果を表 4 に示す。本結果は 5 回測定した平均値・最大値・最小値を示している。なお，本測定においてデータ検索におけるエラーは発生していないことを確認している。この結果から，使用機器および実験条件は異なるものの，本システムによるログ検索がテキストログ，RDB と比較して短時間で処理できていることがわかる。特に，テキストログ，RDB は検索対象が 8 月 1 日分のみであるのに対し，本システムでは 10 億件を超えるログが存在する環境下で最も早く検索が完了する結果となった。

4.2 検索範囲の違いによる所要時間の変化

次に，異なる検索範囲を指定した場合のログ抽出に要する時間を調べる。この測定では，検索対象レコード数の違

ⓒ 2016 Information Processing Society of Japan

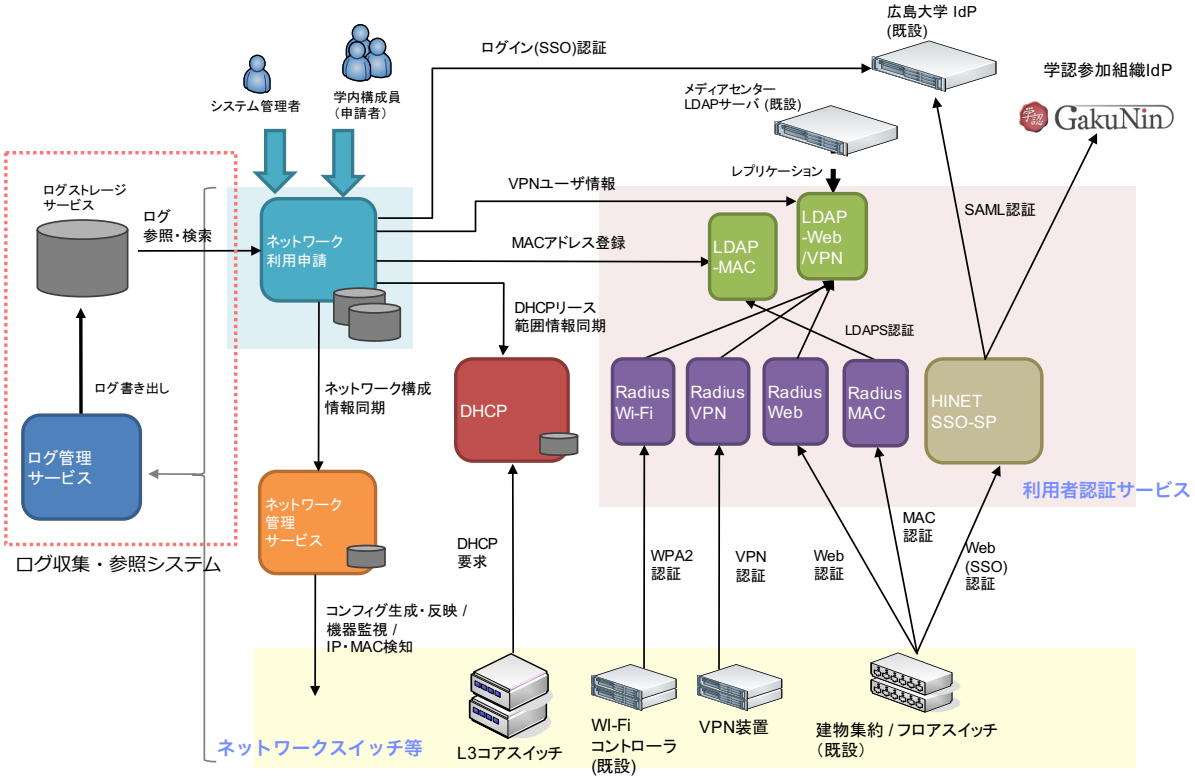

図 2 HINET2014 におけるログ収集対象

表 1 対象とするログ種別

ログ種別	ログ生成元	ネットワーク機器・サーバソフトウェア
IPS ログ	IPS 装置	Cisco ASA5585-X / SSP60
全学 FW ログ	全学ファイアウォール装置	
部局 FW ログ	部局ファイアウォール装置	
DHCP ログ	DHCP サーバ	ISC-DHCP 4.2.5p1 相当
SSO(SSO) 認証ログ	HINET SSO-SP サーバ	NetSoarer L2Gate
Web 認証ログ	Radius Web サーバ	Free Radius 2.1.12-4.el6_3
MAC 認証ログ	Radius MAC サーバ	
WPA2 認証ログ	Radius Wi-Fi サーバ	
LDAP ログ	LDAP-Web/VPN サーバ, LDAP-MAC サーバ	Open LDAP 2.4.33-3.el6
VPN ログ	VPN 装置, Radius VPN サーバ	Cisco ASA5545-X, Free Radius 2.1.12-4.el6_3
無線 AP ログ	無線 LAN 管理装置	Cisco Prime Infrastructure
スイッチログ	キャンパス集約/建物集約/フロアスイッチ	Alaxala AX2530S, AX2430S, AX3830S

表 3 使用機器および実験条件

	(1) テキストログ	(2) RDB	(3) 本システム
CPU	Core i7-2600 3.4GHz (4C/8T)		4vCPU
メモリ	16GB		31GB
HDD	1TB		2TB
ツール	grep	MySQL 5.1.73	Redshift ds2.xlarge
登録件数 (行)	336,106,250	99,110,201	12,513,792,582
条件式	宛先 IP 指定	WHERE 句による時間および宛先 IP 指定	
該当件数 (行)	4,535	1,059	

いによる検索性能を定量的に示すことを目的としている。検索範囲を 1 週間，2 週間，1 ヶ月，2 ヶ月，3 ヶ月に設定し，それぞれで「期間中に発生した，宛先 IP アドレスが 182.22.71.250 に対する新規接続」を検索条件とした場合の抽出に要する時間を計測した。

結果を表 5 に示す。本結果も 5 回測定した平均値・最大値・最小値を示している。なお，表には検索範囲に対応するレコード件数も合わせて記している。この結果から，対象期間の拡大に応じて線形に検索時間を要していることがわかる。検索対象のレコード数が増大することによるものであるが，10 億件以上のログデータが存在する環境下で，1 ヶ月の範囲指定による条件検索であれば 6 分程度で検索できている結果が得られた。

ⓒ 2016 Information Processing Society of Japan

表 2 接続開始ログのテーブル構造

属性	名称	型	出現回数	集約キー	説明
start_datetime	開始時間	日時	1		集約されたログの先頭の日時
end_datetime	終了時間	日時	1		集約されたログの最後の日時
direction	方向	文字列	1	○	通信の向き（”inbound” or ”outbound”）
protocol	プロトコル	文字列	1	○	通信プロトコル (”TCP” or ”UDP”)
src_ip	送信元 IP	文字列	1	○	送信元の IP アドレス
src_mapped_ip	マップ後送信元 IP	文字列	1	○	NAPT 変換後のアドレス（部局 FW 経由時に利用）
src_vlan	送信元 VLAN	文字列	1		送信元の VLAN 情報（抽出可能な場合）
dst_name	宛先名称	文字列	1		宛先の名称（名前が存在する場合）
dst_ip	宛先 IP	文字列	1	○	宛先の IP アドレス
dst_mapped_ip	マップ後宛先 IP	文字列	1	○	NAPT 変換後のアドレス（部局 FW 経由時に利用）
dst_port	宛先ポート	文字列	1	○	宛先のポート情報
dst_vlan	宛先 VLAN	文字列	1		宛先の VLAN 情報（抽出可能な場合）
count	接続回数	4 バイト整数	0..1		集約されたログの件数

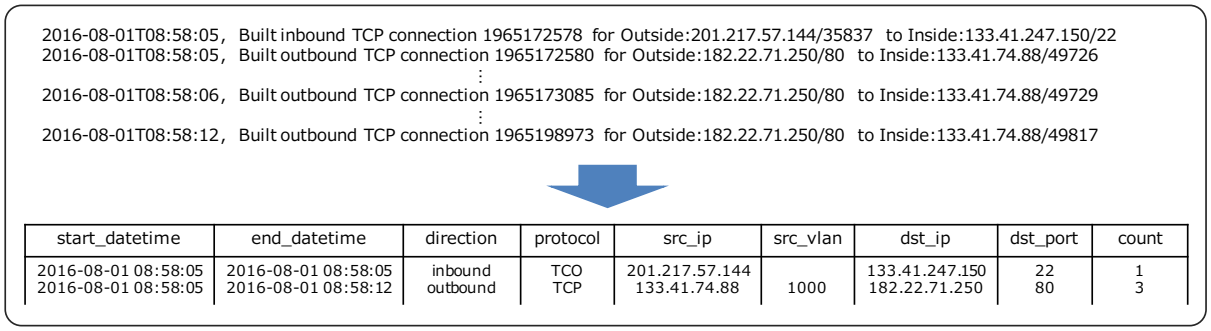

図 3 テキストログからのログ圧縮・構造化の例

表 4 検索時間の比較（単位：秒）

	平均値	最小値	最大値
(1) テキストログ	390.64	389.53	391.55
(2) RDB	93.86	93.45	94.91
(3) 本システム	9.80	9.74	9.88

5. 考察

4 章の評価結果から，ログ検索性能の効果を確認することができた。今回の計測では，比較対象ごとに実験条件が異なるものの，本システムによるログ検索が最も広い対象範囲で高速に検索できている結果となった。Redshift の列指向データベースによる効果に大きく依存していると考えられるが，このようなデータベースシステムをフルマネージド型クラウドサービスで利用できることが本システムの利点のひとつといえる。

一方で，クラウドサービスのコストは考えておく必要がある。Redshift の場合，データ転送料金（S3 とのデータロード，アンロードを含む）は発生しないが，インスタンスに対する月額料金が発生する。しかしながら，定期的なインスタンスアップグレードも行われるため，ハードウェアが陳腐化するなどの問題は発生しない。また，セキュリティについても考慮しておく必要がある。Redshift は，AWS KMS（Key Management Service）もしくは HSM（Hardware Security Module）によるデータベース暗号化を標準でサポートしている。しかしながら，暗号化を有効にすることで，平均して性能が約 20%低下し，ピーク時のオーバーヘッドが 40%となることが示されている。[*3] 他方，Redshift インスタンスに対する接続元 IP アドレス等を利用したアクセス制限も利用（併用）することが可能であり，データへのアクセス対象を制限することもできる。

本稿では IPS 装置が出力する通信ログを例に動作概要と性能評価を述べてきが，本システムでは表 1 に示す各種ログを保存している。したがって，DHCP による IP アドレス払出ログや学内無線 LAN（各アクセスポイント）の利用動向も同様の方法で検索すること可能である。これらのログは，IPS 装置のログ流量と比較すると非常に少なく，同じ範囲を指定した場合でも，より高速に検索できることを確認している。一方，実運用を考えた場合，複数ログの横断的な検索や SIEM で実現されているような相関分析等の高度な処理が行える必要がある。本システムでは表 1 で示す各ログに関連付けて検索可能である。例えば不正な通信を検出した場合，通信先 IP アドレスから利用者を把握するには，IPS およびファイアウォールログでの送信元 IP

[*3] http://awsdocs.s3.amazonaws.com/redshift/latest/redshift-mgmt-ja-jp.pdf (2016-9-16 参照)

ⓒ 2016 Information Processing Society of Japan

表 5 範囲指定の違いによる検索時間（単位：秒）

検索範囲 (期間)	該当件数	平均値	最小値	最大値
1 週間 (8/1-8/7)	571,430,249	101.7	97.8	106.9
2 週間 (8/1-8/14)	1,142,925,994	188.8	185.1	193.5
1 ヶ月 (8/1-8/31)	2,519,020,164	391.6	387.4	397.6
2 ヶ月 (7/1-8/31)	4,712,434,575	736.7	721.2	783.8
3 ヶ月 (6/1-8/31)	6,483,594,034	1016.3	1002.6	1037.7

アドレスを調べ，その結果をキーに認証ログや DHCP ログを検索すればよい。API を利用することで，用途に応じて適切な機能を提供することができるが，具体的な実装については今後の課題である。

6. おわりに

本論文では，ネットワーク運用ログの蓄積と抽出プロセスを効率的に行うためのログ管理基盤として，複数サービスが出力するネットワークログを集約し，クラウドサービスを活用して蓄積および解析を行うログ蓄積・参照システムについて述べた。ネットワーク構成が大規模化・複雑化し，出力されるログは日々肥大化する状況にありながら，ログ管理の負担の軽減と迅速な調査対応が求められる時代になった。今後は，横断的な検索ツールによる利便性の向上に加え，本システムを軸としたログ情報のプロアクティブな活用により，障害検知等の保守・運用管理面での活用を検討していく。

謝辞 本キャンパスネットワークの構築および運用に尽力頂いている情報メディア教育研究センター，ネットワンシステムズ株式会社，株式会社プロキューブの関係者各位に感謝致します.

参考文献

[1] 近堂徹, 田島浩一, 岸場清悟, 大東俊博, 岩田則和, 西村浩二, 相原玲二, ”利用者認証機能を備えた大規模キャンパスネットワークの性能評価”, 情報処理学会 インターネットと運用技術シンポジウム (IOTS)2008 論文集, pp.121-128, 2008.

[2] 近堂徹, 田島浩一, 岸場清悟, 吉田朋彦, 岩田則和, 大東俊博, 西村浩二, 相原玲二, ”クラウドコンピューティング活用のための大規模キャンパスネットワーク”, 情報処理学会 インターネットと運用技術シンポジウム (IOTS)2014 論文集, pp.101-108, 2014.

[3] 鳩野逸生, ”全学無線 LAN 利用ログ情報の解析と応用”, 情報処理学会研究報告インターネットと運用技術（IOT）, 2015-IOT-31(10), pp.1-6, 2015.

[4] 杉木章義, 佐藤聡, 和田 耕一, ”学内無線 LAN システム における利用統計データの分析とその課題”, 情報処理学会研究報告インターネットと運用技術（IOT）, 2013-IOT-23(7), pp.15, 2013.

[5] Blinn, David P. and Henderson, Tristan and Kotz, David, ”Analysis of a Wi-Fi Hotspot Network”, 2005 workshop on Wireless traffic measurements and modeling, pp.1-6, 2005.

[6] 宮下健輔, ”学内 LAN 利用ログの分析と応用”, 情報処理学会研究報告インターネットと運用技術（IOT）, 2014-IOT-27(15), pp.1-5, 2014

[7] 技術検討ワーキンググループ報告書，第 5 回パーソナルデータに関する検討会，首相官邸，2013（2016-11-6 参照）

[8] 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,”ネットワーク機器動作ログ参照サービスの試作”, 情報処理学会研究報告インターネットと運用技術（IOT）, 2013-IOT-20(34), pp.193-196, 2013.

[9] R. Gerhards, Adiscon GmbH, ”The Syslog Protocol”, RFC5424, 2009.

ⓒ 2016 Information Processing Society of Japan