

*2 接続障害の場合は、ネットワーク接続が失われた後に申告が

ような状況において、過去にどのような機器がどこに接続されていたかに関する情報が必須である。また、ネットワークの更新などを実施する場合は、利用者からの要望の査定には、実際の利用状況の把握が必要となることが想定される。

このような状況に対応するため、KHAN2017 には単なる syslog 情報の集積や商用のネットワーク管理システムを利用だけでなく、必要な情報を収集するためのプログラムの開発を行っている。以下に、KHAN2017 で実施している情報収集および監視機能の概要について述べる。

3 Network Management System(NMS) による監視

3.1 有線ネットワーク

KHAN2017 を構成するネットワーク機器の管理を行うために、商用の NMS を導入している (Zoho 社製 OpManager)[2]。ネットワーク機器の中で、各建物のフロアに設置されたスイッチ (エッジスイッチ) を除くすべての機器に、NMS を snmp(Simple Network Management Protocol) サーバとして登録して機器の死活・性能管理を実施している*3。機器のダウン、重大な Trap の発生、トラフィック情報の大幅な変化に対して、Alert が発生するように設定している。機器の停止など重大な Alert に関しては、事務室内のパトライトを点灯させるとともに、メールを発信して管理者に通知している。

また、エッジスイッチにおいて、ループが発生した場合、該当ポートの遮断とともに Trap が発生するように設定しているが、ループの Trap は、パトライト機器へ直接送信するようにしている。

3.2 無線ネットワーク

KHAN2017 において、全学無線 LAN サービス実現のために HPE/Aruba 社製の製品を導入しているが、AP およびユーザの接続状況を監視するために、同社製の AirWave を導入している [3]。AirWave においては、無線コントローラおよびアクセスポイント (以下 AP) の死活管理、利用電波帯域の状況、セッション情報を含むユーザの利用状況の監視を行っている。特に、ユーザのセッション情報 (接続情報) に関しては、一日に一度前日の情報を収集して保存している*4。

行われる場合が多い。

*3 すべての機器を登録するためのライセンスを取得していないため、管理対象の末端の L2 スイッチは登録していない。

*4 AirWave で利用可能なリソースの関係で詳細情報は数カ月分しか保存されないためである。

4 Syslog 情報収集

KHAN2017 では、ネットワーク機器が発生するログ情報を集約するためのサーバを導入している。すべてのネットワーク機器に対して、syslog サーバをログ収集サーバに設定している。ログ収集サーバにおいては、rsyslog[5] を利用して、年、月、日毎にフォルダを作成してログ情報を蓄積している。

収集されたログ情報は、ログ収集サーバにログインすることにより参照することができるが、技術者でない職員でも容易に参照できることを目的とし、Web ブラウザからログ情報を参照するためのインタフェースを実装している。

5 通信状況の収集

5.1 Firewall における通信情報取得

KHAN2017 においては、学内と学外、およびプライベートアドレスとグローバルアドレスのネットワークの境界に、次世代 Firewall 装置 (Paloalto 社)[6] を導入しており、Traffic ログおよび URL ログを収集している。収集された情報は、syslog によりログ収集サーバに送信するとともに、夜間バッチ処理によって、前日分のログをログ収集サーバに送信している。

ログ収集サーバに蓄積された情報は、莫大な容量になるため、夜間のバッチ処理により、IP アドレス毎にトラフィック情報、アプリケーション情報、URL 情報などを集約し、Web ブラウザから参照するためのインタフェースを実装している。表示画面例を図 2 に示す。図 2(a) における集計条件設定画面では、集計範囲、対象セグメント、表示情報の選択が可能である。

5.2 sFlow を用いた学内通信状況取得

前述の Firewall における通信情報取得において、Firewall 装置を通過する通信に関する情報は取得できるが、プライベートネットワーク内の通信など Firewall 装置を通過しないものに関しての情報を取得することはできない。KHAN2017 においては、基幹ルータおよび基幹ルータに直結しているネットワーク機器のインタフェースにおいて、sFlow を用いた通信のサンプリング情報を収集し、商用の sFlow コレクタである NetFlowAnalyzer で収集している [4]。これにより、Firewall 装置を通過しない通信に関する情報もある程度取得できる*5。

*5 KHAN2017 は、L2 構成のネットワークであるため、セグメント間通信であれば必ず基幹ルータを経由する。

表示日範囲指定

2019/09/17 ▼ 2019/09/17 ▼
長期間を指定すると処理時間がかかります。

表示対象アドレス指定

対象セグメントを指定してください。

- ☐ グローバルアドレス
- ☒ 事務系アドレス
- ☐ プライベートアドレス(教育研究用)
- ☐ プライベートアドレス(WiFi用)
- ☐ プライベートアドレス(VPN用)
- ☐ NAT割付グローバルアドレス

正規表現パターン: : パターンを入力した場合は上の指定は無効になります。

表示対象情報指定

- ☒ 1日総トラフィック
- ☐ トラフィック(H毎)
- ☒ 観測アプリケーション
- ☒ 観測OS
- ☐ 観測ブラウザ
- ☐ その他観測エージェント

パターン検索の場合の文字列: (アプリケーション用)

パターン検索の場合の文字列: (OS用)

パターン検索の場合の文字列: (ブラウザ用)

パターン検索の場合の文字列: (その他Agent用)

パターン検索を指定した場合はマッチする項目のみ表示されます。実行

(a) 集計条件設定画面

トラフィック

ipcategory = ["jimu", "privateER", "privateWifi", "privateVPN", "NAT"]

IPアドレス	受信量	送信量	2ch-base	360-safeguard-update	adobe-cloud	adobe-creative-cloud-base	adobe-echoign	adobe-flash-socketpolicy-server	adobe-media-player	adobe-update	airdro
10.10.10.1	3404497346	169761747	0	0	0	0	0	0	0	0	0
10.10.10.2	24594	76196	0	0	0	0	0	0	0	0	0
10.10.10.3	25314	1087277	0	0	0	0	0	0	0	0	0
10.10.10.4	7708	7708	0	0	0	0	0	0	0	0	0
10.10.10.5	5133	4040	0	0	0	0	0	0	0	0	0
10.10.10.6	376	376	0	0	0	0	0	0	0	0	0
10.10.10.7	117050610	20455026	0	0	0	0	0	0	0	0	0
10.10.10.8	32466	15247	0	0	0	0	0	0	0	0	0
10.10.10.9	5133	4040	0	0	0	0	0	0	0	0	0
10.10.10.10	54078	4534	0	0	0	0	0	0	0	0	0
10.10.10.11	336364	25507	0	0	0	0	0	0	0	0	0
10.10.10.12	354547	26761	0	0	0	0	0	0	0	0	0
10.10.10.13	235629	18377	0	0	0	0	0	0	0	0	0
10.10.10.14	5133	4040	0	0	0	0	0	0	0	0	0
10.10.10.15	370841388	26923064	0	0	0	4	0	0	0	0	0
10.10.10.16	0	18048	0	0	0	0	0	0	0	0	0
10.10.10.17	7614	7614	0	0	0	0	0	0	0	0	0
10.10.10.18	0	18048	0	0	0	0	0	0	0	0	0

(b) 集計結果表示例

2019年09月16日のトラフィック

Global: 4213, NAT: 114, Private: 3672, Jimu: 249, Wifi: 1725, VPN: 307

IP Address	送信パケット数	受信パケット数	送信バイト数	受信バイト数	検出アプリケーション
10.10.10.1	0	0	145	0	not-applicable
10.10.10.2	66	0	4396	0	not-applicable
10.10.10.3	228	0	14744	0	not-applicable
10.10.10.4	56	0	5264	0	not-applicable
10.10.10.5	316	0	29704	0	not-applicable
10.10.10.6	315422	315860	184891549	332978686	ssl,dns,google-base,web-browsing,ping,traceroute,ms-update,incomplete,ocsp,facebook-base,twitter-base,yahoo-mail-base,google-analytics,soap,adobe-cloud,google-cald-base,ms-teams,windows-azure-base,adobe-creative-cloud-base,not-applicable,ms-store,yahoo-web-analytics,ms-office365-base,ms-product-activation,windows-push-notifications,xbox-live
10.10.10.7	529664	622687	67595803	804507527	ssl,dns,web-browsing,incomplete,google-base,yahoo-web-analytics,facebook-base,youtube-base,twitter-base,ocsp,analytics,linkedin-base,itunes-base,ms-update,bing-maps-base,naver-line,ms-office365-base,windows-azure-base,not-applicable,soap,insufficient-data,flash
10.10.10.8	820	76	76196	17650	not-applicable,dns,incomplete
10.10.10.9	13781	81	1087183	18370	not-applicable,dns,incomplete
10.10.10.10	82	7708	7708	7708	ntp
10.10.10.11	14	12	4040	5133	ssl,dns
10.10.10.12	14	12	4041	5133	ssl,dns
10.10.10.13	4	4	376	376	ntp
10.10.10.14	190	190	17044	29176	not-applicable

(c) IP 毎詳細画面

図2 Firewallにおける通信情報集計表示

6 その他ネットワーク利用状況収集

その他ネットワークの運用およびセキュリティインシデント対応に必要な、IP の利用状況、ネットワーク機器設定情報およびネットワーク機器へのネットワーク機器の接続情報を、ネットワーク機器が提供する REST API(Restfull API) 機能または snmp による取得プログラムを開発し一定間隔で実行している。

6.1 IP アドレスの利用状況

1 時間毎に、基幹ルータ機器上の ARP テーブルを取得することにより、学内に存在するセグメントの IP の利用状況を記録している。

・ IPアドレス, Macアドレスは全体マッチ, ベンダー名は部分マッチで検索されます。

IPアドレス, Macアドレス, ベンダー名による検索

アドレス/ベンダー名: 検索対象: 検索範囲 From: 2019/09/19 ▼ To: 2019/09/19 ▼ 実行

キャンパス: 記科

2019/09/19 2019/08 2019/07 2019/06 2019/05 2019/04 2019/03 2019/02 2019/01 2018/12 2018/11 2018/10 2018/09 2018/08 2018/07 2018/06 2018/05 2018/04 2018/03 2018/02 2018/01 2017/12 2017/11 2017/10 2017/09 2017/08 2017/07 2017/06 2017/05 2017/04 2017/03 2017/02 2017/01 2016/12 2016/11 2016/10 2016/09 2016/08 2016/07 2016/06 2016/05 2016/04 2016/03 2016/02 2016/01 2015/12 2015/11 2015/10 2015/09 2015/08 2015/07 2015/06 2015/05 2015/04 2015/03 2015/02 2015/01 2014/12 2014/11 2014/10 2014/09 2014/08 2014/07 2014/06 2014/05 2014/04 2014/03 2014/02 2014/01 2013/12 2013/11 2013/10 2013/09 2013/08 2013/07 2013/06 2013/05 2013/04 2013/03 2013/02 2013/01 2012/12 2012/11 2012/10 2012/09 2012/08 2012/07 2012/06 2012/05 2012/04 2012/03 2012/02 2012/01 2011/12 2011/11 2011/10 2011/09 2011/08 2011/07 2011/06 2011/05 2011/04 2011/03 2011/02 2011/01 2010/12 2010/11 2010/10 2010/09 2010/08 2010/07 2010/06 2010/05 2010/04 2010/03 2010/02 2010/01 2009/12 2009/11 2009/10 2009/09 2009/08 2009/07 2009/06 2009/05 2009/04 2009/03 2009/02 2009/01 2008/12 2008/11 2008/10 2008/09 2008/08 2008/07 2008/06 2008/05 2008/04 2008/03 2008/02 2008/01 2007/12 2007/11 2007/10 2007/09 2007/08 2007/07 2007/06 2007/05 2007/04 2007/03 2007/02 2007/01 2006/12 2006/11 2006/10 2006/09 2006/08 2006/07 2006/06 2006/05 2006/04 2006/03 2006/02 2006/01 2005/12 2005/11 2005/10 2005/09 2005/08 2005/07 2005/06 2005/05 2005/04 2005/03 2005/02 2005/01 2004/12 2004/11 2004/10 2004/09 2004/08 2004/07 2004/06 2004/05 2004/04 2004/03 2004/02 2004/01 2003/12 2003/11 2003/10 2003/09 2003/08 2003/07 2003/06 2003/05 2003/04 2003/03 2003/02 2003/01 2002/12 2002/11 2002/10 2002/09 2002/08 2002/07 2002/06 2002/05 2002/04 2002/03 2002/02 2002/01 2001/12 2001/11 2001/10 2001/09 2001/08 2001/07 2001/06 2001/05 2001/04 2001/03 2001/02 2001/01 2000/12 2000/11 2000/10 2000/09 2000/08 2000/07 2000/06 2000/05 2000/04 2000/03 2000/02 2000/01 1999/12 1999/11 1999/10 1999/09 1999/08 1999/07 1999/06 1999/05 1999/04 1999/03 1999/02 1999/01 1998/12 1998/11 1998/10 1998/09 1998/08 1998/07 1998/06 1998/05 1998/04 1998/03 1998/02 1998/01 1997/12 1997/11 1997/10 1997/09 1997/08 1997/07 1997/06 1997/05 1997/04 1997/03 1997/02 1997/01 1996/12 1996/11 1996/10 1996/09 1996/08 1996/07 1996/06 1996/05 1996/04 1996/03 1996/02 1996/01 1995/12 1995/11 1995/10 1995/09 1995/08 1995/07 1995/06 1995/05 1995/04 1995/03 1995/02 1995/01 1994/12 1994/11 1994/10 1994/09 1994/08 1994/07 1994/06 1994/05 1994/04 1994/03 1994/02 1994/01 1993/12 1993/11 1993/10 1993/09 1993/08 1993/07 1993/06 1993/05 1993/04 1993/03 1993/02 1993/01 1992/12 1992/11 1992/10 1992/09 1992/08 1992/07 1992/06 1992/05 1992/04 1992/03 1992/02 1992/01 1991/12 1991/11 1991/10 1991/09 1991/08 1991/07 1991/06 1991/05 1991/04 1991/03 1991/02 1991/01 1990/12 1990/11 1990/10 1990/09 1990/08 1990/07 1990/06 1990/05 1990/04 1990/03 1990/02 1990/01 1989/12 1989/11 1989/10 1989/09 1989/08 1989/07 1989/06 1989/05 1989/04 1989/03 1989/02 1989/01 1988/12 1988/11 1988/10 1988/09 1988/08 1988/07 1988/06 1988/05 1988/04 1988/03 1988/02 1988/01 1987/12 1987/11 1987/10 1987/09 1987/08 1987/07 1987/06 1987/05 1987/04 1987/03 1987/02 1987/01 1986/12 1986/11 1986/10 1986/09 1986/08 1986/07 1986/06 1986/05 1986/04 1986/03 1986/02 1986/01 1985/12 1985/11 1985/10 1985/09 1985/08 1985/07 1985/06 1985/05 1985/04 1985/03 1985/02 1985/01 1984/12 1984/11 1984/10 1984/09 1984/08 1984/07 1984/06 1984/05 1984/04 1984/03 1984/02 1984/01 1983/12 1983/11 1983/10 1983/09 1983/08 1983/07 1983/06 1983/05 1983/04 1983/03 1983/02 1983/01 1982/12 1982/11 1982/10 1982/09 1982/08 1982/07 1982/06 1982/05 1982/04 1982/03 1982/02 1982/01 1981/12 1981/11 1981/10 1981/09 1981/08 1981/07 1981/06 1981/05 1981/04 1981/03 1981/02 1981/01 1980/12 1980/11 1980/10 1980/09 1980/08 1980/07 1980/06 1980/05 1980/04 1980/03 1980/02 1980/01 1979/12 1979/11 1979/10 1979/09 1979/08 1979/07 1979/06 1979/05 1979/04 1979/03 1979/02 1979/01 1978/12 1978/11 1978/10 1978/09 1978/08 1978/07 1978/06 1978/05 1978/04 1978/03 1978/02 1978/01 1977/12 1977/11 1977/10 1977/09 1977/08 1977/07 1977/06 1977/05 1977/04 1977/03 1977/02 1977/01 1976/12 1976/11 1976/10 1976/09 1976/08 1976/07 1976/06 1976/05 1976/04 1976/03 1976/02 1976/01 1975/12 1975/11 1975/10 1975/09 1975/08 1975/07 1975/06 1975/05 1975/04 1975/03 1975/02 1975/01 1974/12 1974/11 1974/10 1974/09 1974/08 1974/07 1974/06 1974/05 1974/04 1974/03 1974/02 1974/01 1973/12 1973/11 1973/10 1973/09 1973/08 1973/07 1973/06 1973/05 1973/04 1973/03 1973/02 1973/01 1972/12 1972/11 1972/10 1972/09 1972/08 1972/07 1972/06 1972/05 1972/04 1972/03 1972/02 1972/01 1971/12 1971/11 1971/10 1971/09 1971/08 1971/07 1971/06 1971/05 1971/04 1971/03 1971/02 1971/01 1970/12 1970/11 1970/10 1970/09 1970/08 1970/07 1970/06 1970/05 1970/04 1970/03 1970/02 1970/01 1969/12 1969/11 1969/10 1969/09 1969/08 1969/07 1969/06 1969/05 1969/04 1969/03 1969/02 1969/01 1968/12 1968/11 1968/10 1968/09 1968/08 1968/07 1968/06 1968/05 1968/04 1968/03 1968/02 1968/01 1967/12 1967/11 1967/10 1967/09 1967/08 1967/07 1967/06 1967/05 1967/04 1967/03 1967/02 1967/01 1966/12 1966/11 1966/10 1966/09 1966/08 1966/07 1966/06 1966/05 1966/04 1966/03 1966/02 1966/01 1965/12 1965/11 1965/10 1965/09 1965/08 1965/07 1965/06 1965/05 1965/04 1965/03 1965/02 1965/01 1964/12 1964/11 1964/10 1964/09 1964/08 1964/07 1964/06 1964/05 1964/04 1964/03 1964/02 1964/01 1963/12 1963/11 1963/10 1963/09 1963/08 1963/07 1963/06 1963/05 1963/04 1963/03 1963/02 1963/01 1962/12 1962/11 1962/10 1962/09 1962/08 1962/07 1962/06 1962/05 1962/04 1962/03 1962/02 1962/01 1961/12 1961/11 1961/10 1961/09 1961/08 1961/07 1961/06 1961/05 1961/04 1961/03 1961/02 1961/01 1960/12 1960/11 1960/10 1960/09 1960/08 1960/07 1960/06 1960/05 1960/04 1960/03 1960/02 1960/01 1959/12 1959/11 1959/10 1959/09 1959/08 1959/07 1959/06 1959/05 1959/04 1959/03 1959/02 1959/01 1958/12 1958/11 1958/10 1958/09 1958/08 1958/07 1958/06 1958/05 1958/04 1958/03 1958/02 1958/01 1957/12 1957/11 1957/10 1957/09 1957/08 1957/07 1957/06 1957/05 1957/04 1957/03 1957/02 1957/01 1956/12 1956/11 1956/10 1956/09 1956/08 1956/07 1956/06 1956/05 1956/04 1956/03 1956/02 1956/01 1955/12 1955/11 1955/10 1955/09 1955/08 1955/07 1955/06 1955/05 1955/04 1955/03 1955/02 1955/01 1954/12 1954/11 1954/10 1954/09 1954/08 1954/07 1954/06 1954/05 1954/04 1954/03 1954/02 1954/01 1953/12 1953/11 1953/10 1953/09 1953/08 1953/07 1953/06 1953/05 1953/04 1953/03 1953/02 1953/01 1952/12 1952/11 1952/10 1952/09 1952/08 1952/07 1952/06 1952/05 1952/04 1952/03 1952/02 1952/01 1951/12 1951/11 1951/10 1951/09 1951/08 1951/07 1951/06 1951/05 1951/04 1951/03 1951/02 1951/01 1950/12 1950/11 1950/10 1950/09 1950/08 1950/07 1950/06 1950/05 1950/04 1950/03 1950/02 1950/01 1949/12 1949/11 1949/10 1949/09 1949/08 1949/07 1949/06 1949/05 1949/04 1949/03 1949/02 1949/01 1948/12 1948/11 1948/10 1948/09 1948/08 1948/07 1948/06 1948/05 1948/04 1948/03 1948/02 1948/01 1947/12 1947/11 1947/10 1947/09 1947/08 1947/07 1947/06 1947/05 1947/04 1947/03 1947/02 1947/01 1946/12 1946/11 1946/10 1946/09 1946/08 1946/07 1946/06 1946/05 1946/04 1946/03 1946/02 1946/01 1945/12 1945/11 1945/10 1945/09 1945/08 1945/07 1945/06 1945/05 1945/04 1945/03 1945/02 1945/01 1944/12 1944/11 1944/10 1944/09 1944/08 1944/07 1944/06 1944/05 1944/04 1944/03 1944/02 1944/01 1943/12 1943/11 1943/10 1943/09 1943/08 1943/07 1943/06 1943/05 1943/04 1943/03 1943/02 1943/01 1942/12 1942/11 1942/10 1942/09 1942/08 1942/07 1942/06 1942/05 1942/04 1942/03 1942/02 1942/01 1941/12 1941/11 1941/10 1941/09 1941/08 1941/07 1941/06 1941/05 1941/04 1941/03 1941/02 1941/01 1940/12 1940/11 1940/10 1940/09 1940/08 1940/07 1940/06 1940/05 1940/04 1940/03 1940/02 1940/01 1939/12 1939/11 1939/10 1939/09 1939/08 1939/07 1939/06 1939/05 1939/04 1939/03 1939/02 1939/01 1938/12 1938/11 1938/10 1938/09 1938/08 1938/07 1938/06 1938/05 1938/04 1938/03 1938/02 1938/01 1937/12 1937/11 1937/10 1937/09 1937/08 1937/07 1937/06 1937/05 1937/04 1937/03 1937/02 1937/01 1936/12 1936/11 1936/10 1936/09 1936/08 1936/07 1936/06 1936/05 1936/04 1936/03 1936/02 1936/01 1935/12 1935/11 1935/10 1935/09 1935/08 1935/07 1935/06 1935/05 1935/04 1935/03 1935/02 1935/01 1934/12

Port	Type	Stat	VLAN Label(Config)	VLAN Label(Exec)	VLAN ID(Config)	TAG No	Port Name	備考
1	ACCESS	-	P_AGR_20	P_AGR_10	1	KH-D202-1	2F D20	HD2
2	ACCESS	-	P_AGR_20	P_AGR_10	1	KH-D202-1	2F D20	HD2
3	ACCESS	-	P_AGR_20	P_AGR_10	1	KH-D103-1	1F D10	DLAN SA 0208C 2番車 (D104 D10)
4	ACCESS	-	P_AGR_20	P_AGR_10	1	KH-B101-1	1F B10	HD2
5	ACCESS	-	P_AGR_20	P_AGR_10	1	KH-C101-1	1F C10	HD2
6	ACCESS	-	P_AGR_20	P_AGR_10	1	KH-D201-1	2F D20	新増 HI

(a) エッジスイッチポート設定確認/変更画面

Label	VLAN ID	エッジスイッチポートへの割当(Config)
1C	24	2
		-03+(1/0/10(t))
		-02-prvp (52(t))
		-03+(1/0/10(t))
		-01 (28(t))
		-02 g (48; 52(t))
1C	24	3
		-03+(1/0/10(t); 1/0/7)
		-03+(1/0/10(t); 1/0/7)
		-01 (21; 28(t))
		-02 g (45; 52(t))
1C	24	4
1C	27	5
1C	/27	6
1C	26	7
1C	8/25	8
1C	24	9
13	/26	14
		-02 g (52(t))
		(21; 28(t))
		(45; 52(t))
		(28(t))
		(28(t))
		(21; 28(t))

(b) セグメント/VLAN のエッジスイッチポート割付状況表示画面

図4 エッジスイッチ設定状況確認及び設定変更画面

7 ネットワーク機器設定情報の取得

1週間に一度の周期で、すべてのネットワーク機器の設定情報 (config) を取得し、保存している。収集した設定情報を用いることにより、エッジスイッチのポート毎のセグメント割り付け情報、および各セグメントがどのエッジスイッチのポートに設定されているかを参照することができる。現在、Web インタフェースからエッジスイッチのセグメント割り当ての変更機能の開発を行っている。図4にエッジスイッチポート設定確認/変更画面およびセグメントの割り付け状況確認画面例を示す。

8 収集情報機能の実装における問題点

ネットワーク機器から情報を収集するにあたって、(1) REST-API, (2) snmp, (3) CLI(Comman Line Interface) を利用しているが、実装に当たっては、以下の様な問題点がある。

- 古いネットワーク機器は、REST-API を実装していない場合があり、この場合は snmp を利用する必要がある。snmp を利用する場合も、標準 MIB で対応していない場合は、ネットワーク機器ベンダーや Firmware のバージョンによって動作が異なる場合がある。
- REST API の利用に際し、十分なマニュアル情報が得られない場合がある。
- REST API および snmp でも収集できない情報がある場合は、CLI を利用する必要があるが、出

力情報の解釈が困難な場合がある。

KHAN2017 においては、ベンダーから十分な情報が得られたため実装可能であったが、今後のプログラムのメンテナンスに関しては十分に注意する必要がある。Firmware のアップデートによる動作が変わる可能性があるためである*6。

9 終わりに

2018 年 2 月の KHAN2017 稼働開始以来、現在に至るまで本稿における情報収集機能は稼働中である。収集された情報は、開発の意図通り障害時の状況把握、ユーザサポート、情報セキュリティインシデント発生時の調査に利用されている。

今後は、前ネットワークにおいても収集した同種の情報と現在の収集情報を照合することにより、ネットワークに利用状況がどのような変化したか、KHAN2017 で導入したプライベートネットワークが意図通り利用されているかの検証に用いる予定である。

参考文献

- [1] 鳩野, 伴, 伊達, 北内: 神戸大学におけるキャンパスネットワークの更新および全学無線 LAN サービスと統合した研究室向けプライベートネットワークの導入, 情報処理学会研究報告, 2018-IOT-43, 2018.
- [2] Zoho 社: ManageEngine OpManager: <https://www.manageengine.jp/products/OpManager/> (2019 年 9 月現在)
- [3] HPE 社: Aruba AirWave ネットワーク管理: <https://www.arubanetworks.com/ja/products/networking/management/airwave/> (2019 年 9 月現在)
- [4] Zoho 社: NetFlow/sFlow 対応: フローコレクタ, https://www.manageengine.jp/products/NetFlow_Analyzer/ (2019 年 9 月現在)
- [5] rsyslog: The rocket-fast Syslog Server - rsyslog, <https://rsyslog.com/> (2019 年 9 月現在)
- [6] Paloalto Networks: PA-5200 Series, <https://www.paloaltonetworks.jp/products/secure-the-network/next-generation-firewall/pa-5200-series> (2019 年 9 月現在)

*6 情報収集プログラム開発中に Firmware のマイナーバージョンが異なった同一ベンダーの機器で、REST API または snmp の動作が異なる場合があることに複数回遭遇した。