組織内ネットワークでの攻撃伝搬に対する既存のネットワーク機器を活用した監視手法の検討

鳥居 大輔[1] 石原 真太郎[1] 秋山 豊和[1] 小林 和真[1]

概要：
標的型攻撃等の組織内のネットワークで伝搬する攻撃の増加が報告されており，これらの攻撃では，組織内の感染ノードから，他の組織内ノードへの攻撃が行われ，感染が拡大していく．最初の組織内ノードへの感染はゼロデイ攻撃が使用されるため，感染拡大の検知には外部から内部への通信の監視だけでは足りず，組織内ネットワークでの通信を監視をする必要がある．本研究では，コストを抑えるために，既存のスイッチなどのネットワーク機器を更新せず組織内ネットワークを監視する手法として，中継するスイッチの機能を用いてスイッチを流れるトラフィックを中央の監視サーバに転送する手法（低コスト集中監視方式）を検討する．すべての組織内ネットワークに流れるパケットの情報を取得しようとした場合，ファイルサーバへのアクセスなど，通常は組織内ネットワークに閉じたトラフィックがすべてコアネットワークの監視装置に流れ込むため，監視装置を更新せずに定常的に監視するためには，トラフィックの削減が求められる可能性がある．本研究では低コスト集中監視方式において課題となるスイッチのトラフィックプローブ機能について調査し，その課題について整理した．また，キャンパスネットワークを対象として，想定する監視で発生するトラフィック量を調査した．さらに，組織内ネットワーク攻撃に悪用されるプロトコルなどに監視対象を限定することで，両手法で監視可能な分量への監視トラフィックの削減可否を調査した．

A Study on Monitoring Method for Inside Network Attack Propagation Exploiting Existing Network Equipment

DAISUKE TORII[1] SHINTARO ISHIHARA[1] TOYOKAZU AKIYAMA[1] KAZUMASA KOBAYASHI[1]

1. はじめに

標的型攻撃等の組織内のネットワークで伝搬する攻撃の増加が報告されており，これらの攻撃では，組織内の感染ノードから，他の組織内ノードへの攻撃が行われ，感染が拡大していく．最初の組織内ノードへの感染は，ゼロデイ攻撃が使用されるため，感染拡大の検知には外部から内部への通信の監視だけでは足りず，組織内ネットワークでの通信を監視をする必要がある [1]．その手法として各ネットワークスイッチに侵入検知システム（IDS）を設置してモニタリングする手法が考えられるが，コスト面から実現が困難な場合が多い．そこで本研究では，コストを抑えるために，既存のスイッチ等を更新せず組織内ネットワークを監視する低コスト集中監視方式を提案する．提案方式の実現アプローチとして，(1) 中継するスイッチのミラーリング機能を用いてスイッチを流れるトラフィックを中央の監視サーバに転送する手法 (ミラーリング方式) と，(2) 中継するスイッチを流れるトラフィックの統計情報とログ出力を用いる手法（サマリ方式）が考えられる．特にミラーリング方式のように，すべての組織内ネットワークに流れるパケットの情報を取得しようとした場合，ファイルサーバへのアクセスなど，通常は組織内ネットワークに閉じたトラフィックの情報がすべてコアネットワークの監視装置に流れ込むため，監視装置を高性能なものに更新せずに定常的に監視するためには，トラフィックの削減が求められる可能性がある．本研究では低コスト集中管理方式の活用可否

[1] 京都産業大学
Kyoto Sangyo University

を調査するため，まず (1) 機器によって異なるトラフィックのプローブ方式について調査し，課題を整理する．また，(2) キャンパスネットワークをモデルとして，想定する監視に必要なトラフィック量を調査する．さらに，(3) 組織内ネットワーク攻撃に悪用されるプロトコル [2]（以下攻撃プロトコル）などに監視対象を限定することで，監視可能な分量への監視トラフィック量の削減可否を調査する．

(1) の課題では，VLAN を用いたリモートポートミラーリング (RSPAN) や，ミラーリングしたパケットを GRE でカプセル化する ERSPAN，トラフィックをサンプリングする sFlow やトラフィックの特定の情報を出力する NetFlow などのサポート状況や機能面での課題を調査する．(2) の課題では，(1) で調査したプロトコルを用いた場合のトラフィック量について，公開されているキャンパスネットワークの情報をベースに検討を行う．(3) の課題では，攻撃プロトコルの一般的なネットワークでのトラフィック量を明らかにするため，一例として学内ネットワークでのトラフィックを調査する．また，脆弱性の情報 (CVE) ならびに脆弱性の危険度を示す指標 (CVSS) を用いて，それぞれの攻撃プロトコルの危険性などについて調査する．さらに，調査結果に基づいて，両手法での監視トラフィック低減への適用可否について考察する．

以下， 既存の機器を活用した監視方法の提案を 2 節で，関連研究については 3 節で，(1), (2), (3) の課題に関してそれぞれ 4, 5, 6 節で述べ，7 節で本稿のまとめと今後の課題について述べる．

2. 提案するトラフィック監視手法

標的型攻撃は [1][2] によると，まず対象の組織に対して，ある踏み台ホストに侵入し，踏み台デバイスに，Remote Access Trojan(以下 RAT) に感染さる．そこから，例えば Windows 端末の場合，Pass-the-hash 攻撃ツールなどを用いて取得したパスワードハッシュ値を用いて，さらに他の端末に対して，Remote Desktop Protocol (RDP) や Server Message Block (SMB) のなどのプロトコルを悪用してマルウェアを感染させ，感染範囲を徐々に広げていき，最終的には目的の情報の窃取や改ざん等を行う．このような攻撃の全容を知るためには，外部から組織内ネットワークへの通信だけを見るファイアウォールや IPS/IDS 等のログだけでは足りず，組織内ネットワークの通信も監視する必要がある．

図 1 に，想定する組織内ネットワークでの感染拡大と本稿で提案するトラフィック監視手法の概要を示す．一般的なネットワークでは，外部接続部分にファイアウォールが置かれているため，組織内ネットワークでの攻撃伝搬の検知は難しい．一方で，全てのスイッチにファイアウォール等を設置をすることはコスト面から厳しい．そのため，本研究ではスイッチや監視機器を追加，更新せずに，組織内

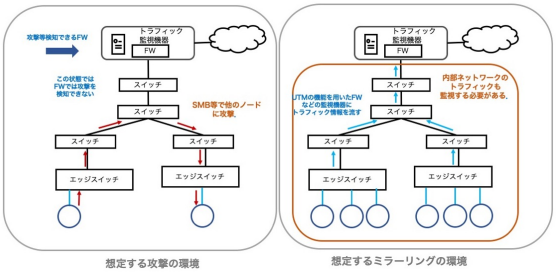

図 1 提案するトラフィック監視手法

ネットワークのスイッチの機能を用いてトラフィックの情報をプローブし，ファイアウォールや SIEM など，攻撃検知が可能な監視装置に転送することで組織内での攻撃伝搬の検知を目指す．一方で，すべての組織内ネットワークの機器からトラフィックの情報を監視機器に転送する場合，監視機器の性能向上を伴わずに定常的に監視するためには，トラフィックの削減を求められる可能性があり，本研究では，感染拡大時に悪用される RDP や SMB 等のプロトコルに限って監視を行うことによるトラフィック低減可否について調査する．

組織内ネットワークの攻撃伝搬を検知するために必要な，監視属性について，その理由とともに表 1 に示す．また，表 1 の監視属性を監視装置に伝送する際に，スイッチに求められる要件について表 2 に示す．

表 1 の IP, MAC, ポート番号については，文献 [1] より，組織内ネットワークの攻撃伝搬を検知には，IP,MAC, ポート番号が必要となるからである．一方で本研究の想定環境では，直接スイッチから情報を得るのではなく，遠隔にあるスイッチから情報を収集するために監視が必要であると考えられる．

なお，トラフィックを削減する手法のうち，フィルタリング手法とは異なる手法として，サンプリング方式が挙げられる．DDoS 攻撃等の大量の同じ攻撃パケットの場合サンプリング方式でも検知できるが，本稿では，文献 [1] の攻撃伝搬に注目しており，この攻撃では，大量の攻撃パケットが出力されないため，本稿においては，サンプリング方式は利用できないと考えられる．

既存のスイッチに実装された監視手法におけるプローブに活用可能な機能について，表 1 の監視属性および表 2 の要件をどの程度満たすかについて調査した結果を 4 節で示す．

3. 関連研究

組織内のネットワークを監視をするものとして文献 [3] が挙げられる．また，監視機器のトラフィック削減を行う目的は同じであるが，監視対象が異なる研究として，文

献 [4] が挙げられる．

文献 [3] では，エッジスイッチの上流ポートでミラーリングしているが，トラフィックの削減が考えられていない．

文献 [4] では，ファイアウォールや UTM の装置の負担軽減のため，NetFlow を使用した攻撃検知の検討が行われているが，この研究で対象としている攻撃は DDoS であり，本研究では文献 [1] のように，感染した端末からの攻撃伝搬に注目する．

4. 既存のスイッチを用いたトラフィック収集方式

既存のスイッチの機能を用いて監視装置にトラフィックを転送する手法として，本節では，ログ収集方式としての syslog，遠隔ミラーリングを行う RSPAN および ERSPAN，フロー情報を収集する sFlow や NetFlow 用いた場合に，表 1 の監視属性，表 2 の要件をどの程度満たすことができるかについて調査する．

4.1 Syslog を用いたトラフィック収集方式

ログメッセージをネットワーク経由で転送する標準規格として syslog プロトコルがある．一般的なネットワーク機器ではこの機能をサポートしており，これを活用することでトラフィックを監視する手法について述べる．具体的にはアクセスコントロールリスト (ACL) で監視したいパケットを指定し，パケットを破棄せずにログを残す方法であり，出力されたログを syslog で遠隔の監視サーバに送信して監視する手法である．

この手法では，スイッチの要件が満たせない可能性がある．まず，1 つ目はスイッチはパケット転送を主機能として設計されており，ログ出力性能は低いため，監視できるトラフィック数が少なく，監視に利用できない可能性がある点が挙げられる．今回スイッチによるログ出力性能を評価するため，Catalyst2960 Plus に着目し，アクセス制御機能により，対象のトラフィックを検知した際に出力されるログの出力性能を計測した．環境は図 2 で行い，結果は図 3 の通りとなった．図 3 より，ログの出力性能が最大で 1 秒間に 2,700 パケット程度しか出力できないことがわかった．

表 1　組織内ネットワークでの攻撃伝搬の検知に必要な監視属性

属性名	理由
VLAN 情報	攻撃発生時に，どのネットワークの端末が原因なのか，どのネットワークに影響が発生したのかを知る必要があるため．タグ VLAN が用いられているネットワークの識別に必要．
インタフェース情報	VLAN 情報と同様にどのネットワークが関連しているかを確認するため．ポート VLAN で構成されるネットワークの識別に必要．
デバイス情報	ネットワーク内のどの範囲に影響が生じたのか把握する上で，どのスイッチで観測されたトラフィックかを把握しておくために必要．
監視したパケットの送受信 IP アドレス	送信元の IP は，攻撃通信を検知した場合に，L3 での攻撃元，攻撃先を分析するために必要．
監視したパケットの送受信 MAC アドレス	IP アドレス同様 L2 での攻撃通信の分析に必要．
TCP/UDP ポート番号	IP・MAC アドレスと同様に，L4 での攻撃通信の分析に必要．なお，[1] では，RAT が攻撃伝搬に使用する際の SMB・RDP 及び HTTPS のトラフィックに注目しており，トラフィックの絞り込みに活用できる可能性がある．

表 2　スイッチでの監視属性のプローブ時に求められる要件

項目名	理由
対応している機種が多い	既存のネットワーク機器を変更せずに適用する場合，より多くの既存機器で対応している必要があるため．
フィルタリング	全てのトラフィックは監視できない可能性があるため，攻撃に用いられる可能性の高いトラフィックに絞り込むために必要．

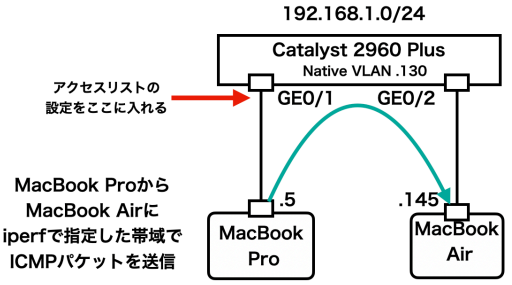

図 2　CISCO のアクセスリストログの出力率の確認方法

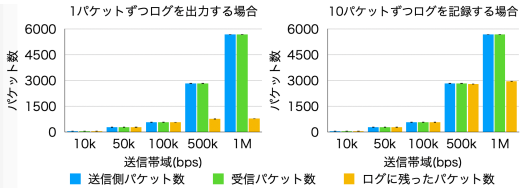

図 3　CISCO のアクセスリストログの出力率のの結果

次に，syslog 方式では，ベンダごとに出力できる情報が異なるため実運用されているスイッチでは監視に必要な情報が得られない可能性がある [5][6]．一部ベンダではブロックしたパケットしかログ出力できないものもあり，その場合，本手法では適用できない [5]．

4.2 RSPAN を用いたトラフィック収集方式

RSPAN は，ポートミラーリングに対して，VLAN を指定することで，遠隔地にミラーリングする手法であり，図 4 にその動作概要を示す [7]．この手法では，すべてのパケットを転送するため，表 1 に示した情報のうち送信/宛先の IP/MAC と，送受信 UDP/TCP ポート番号は収集できる．しかし RSPAN では，ミラーリングされたパケットには，転送に用いる VLAN のタグしかつけられないため，インタフェース情報，デバイス情報，VLAN 情報が得られない．図 5 に示すように，どのスイッチがミラーリングしたものかわかるように，各スイッチごとに RSPAN で使用する VLAN を切り分けることができれば，デバイス情報を得られる．また，ポートごとに RSPAN で用いる VLAN を変更した場合は，どのポートでミラーリングしたものかわかるようになり，攻撃等が発生した際にどの機器が攻撃されているのか分かるようになる．

RSPAN の他の課題としては，中継機器の間に RSPAN に対応していない機器があった場合，該当スイッチに接続されていない MAC アドレスも学習してしまい，Forwarding Table が壊れてしまう点が挙げられる．それを回避するた

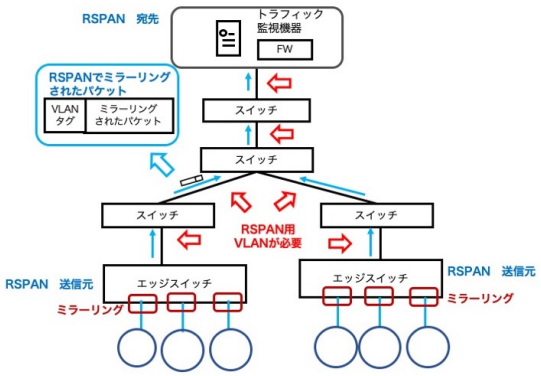

図 4　RSPAN の概要図

めには，VLAN の MAC ラーニング機能をオフにする必要がある．以上から，本手法を適用するには RSPAN か，VLAN の MAC ラーニング機能のオフのどちらかの機能に対応している必要がある．一方で Catalyst 2960 等のフィルタがかけられない機種を用いた環境には，本手法を適用できない．

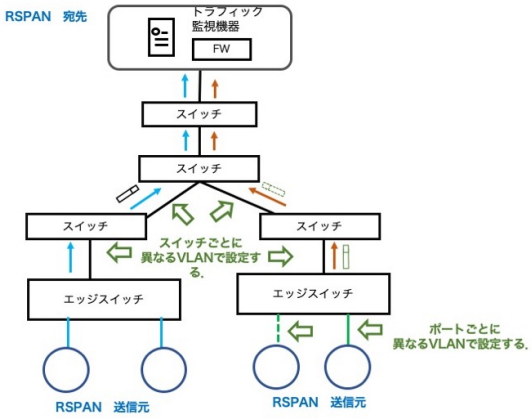

図 5　RSPAN の課題に対する対策

4.3　ERSPAN を用いたトラフィック収集手法

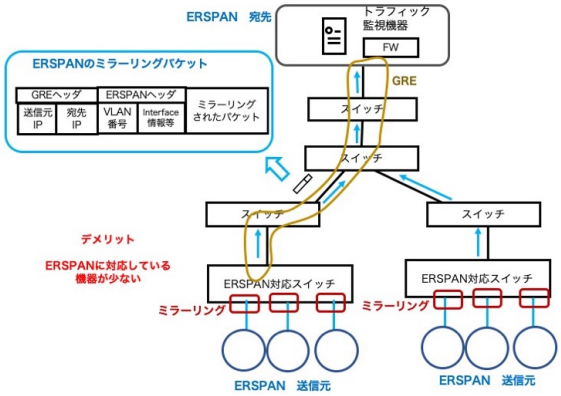

図 6　ERSPAN の概要図

ERSPAN は図 6 に示したように，ミラーリングしたパケットを ERSPAN ヘッダを付け GRE でカプセル化して遠隔地に送信する手法である [8]．この手法で収集できる情報としては，ERSPAN II 及び ERSPAN III において，ERSPAN ヘッダ内にポート番号や VLAN 情報等が載せられるため，攻撃元のノードが接続しているインタフェースを特定することができる．

一方で，本稿で想定している，ネットワーク機器を更新せずに監視するために，必要なスイッチの要件のうち満たせないものとして，対応機種が少ないことが挙げられる．ERSPAN は Open vSwitch などのソフトウェアスイッチでは対応しているものあるが，既存の実機のスイッチでは対応している機種が少なく，この手法においては，ネットワーク機器を更新せずに監視することができない可能性が高い．CISCO においては Catalyst 6500/6000 Series や ASR1000 シリーズと言った高性能なコアスイッチやコアルータしか対応しておらずそれ以外のスイッチでは対応していない [9]．

4.4　sFlow を用いたトラフィック収集方式

sFlow はネットワークに流れるトラフィックの監視をするために，トラフィックをサンプリングし，そのパケットの情報を遠隔の管理サーバに送信するプロトコルである．sFlow で満たせる要件としては，VLAN 情報やポート番号，送信元/宛先，MAC/IP アドレス，受信したインタフェース情報が取得できる．一方で機器によって，サンプリングする設定しかできない場合もある．また，特定のプロトコルに絞るフィルタリングをサポートしておらず，フィルタリングの要件を満たさない．

4.5　NetFlow を用いたトラフィック収集方式

NetFlow は sFlow と同じようにネットワークに流れるトラフィックを監視するための規格である．運用上のスイッチの要件のうち満たしているものとしては，sFlow とは異なり，サンプリングは任意であり，すべてのパケットの情報を収集できる点が挙げられる．また，CISCO の機器では ACL ベースによるフィルタリングも行うことができる．

一方で，v9 以前では MAC アドレスの情報を取得できないため，表 1 の要件を満たさない．v9 以降では要件を満たす [10][11]．

5.　キャンパスネットワークにおける監視トラフィック量の推定

本節では，トラフィックをすべてミラーリングした場合のトラフィック量と，監視するために必要なトラフィックの削減割合を調査するため，文献 [12][13][14] で示されているネットワーク及びトラフィック量を元に想定したキャンパスネットワークを用いて，提案手法を適用した場合のミ

ラーリングトラフィック量を調査する．

文献 [12][13] を元に想定したキャンパスネットワークを図 7 に示す．図 7 では，文献 [12][13] を参考に，建物の規模や棟数，建物間の帯域などを設定した．想定環境は，1 棟 3 階建の建物 20 棟から構成され，各棟内は 1Gbps で接続されており，各コアスイッチと棟スイッチは 2Gbps とした．2 つの線をリンクアグリゲーションしており一本として見ることができると想定し，最大 2Gbps まで流すことができると想定する．また，コアスイッチ 1 とファイアウォール間の帯域は 10Gbps と想定する． また，棟内の構成については，棟スイッチ (S_b)，フロアスイッチ (S_f)，エッジスイッチ (S_e) から構成されると想定する．なお，端末総数は文献 [14] を参考にしたが，本稿では計算を簡素化するために，建物 6 棟に講義室があり，講義室以外のトラフィックは考えない．

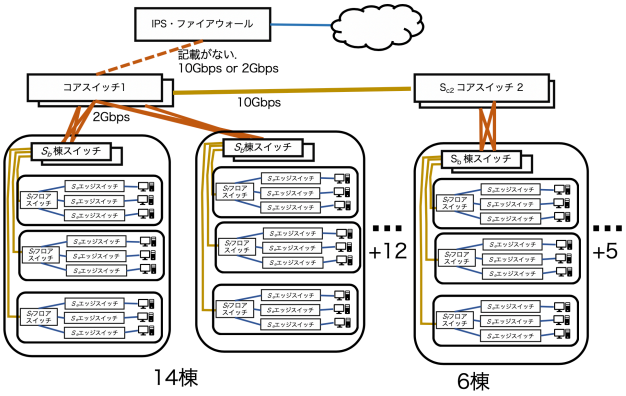

図 7　文献 [12][13] を元に想定したネットワーク図

組織内ネットワーク監視のためのミラーリングは，すべてのスイッチにおいて，下流のポートを流れるトラフィックをミラーリングする．このときトラフィックは，ミラーリングしなくても，外部接続部分を通過するもの（学外トラフィック）とミラーリングしなければ監視できないもの（学内トラフィック）に分類できる．学外トラフィックをミラーリングしてしまうと，重複して監視することになるため，無駄が生じる．また，学内トラフィックにおいて，コアネットワークに配置された学内サーバとエッジスイッチに接続された端末の通信を，エッジスイッチ，フロアスイッチ，棟スイッチ，コアスイッチそれぞれでミラーリングすると，トラフィックの重複が生じる．さらに，ブロードキャストのトラフィックは，同一セグメント内のスイッチにすべてコピーされるため，重複が生じる．これらの重複について，(1) 区別できない場合，(2) 学外/学内のみ区別した場合，(3) 学外/学内サーバ/ブロードキャスト/その他学内の 4 種類に区別した場合について考える．(1) はフィルタ機能がないため区別できない場合，(2) は単純に送受信アドレスによって，学内トラフィックのみに絞り込んだ場合，(3) は学内トラフィックでも，コアネットワークを経由するものは，コアネットワークでのみミラーリングし，ブロードキャストも同一セグメント内での最も上流のスイッチでのみミラーリングする場合をそれぞれ示している．なお，簡単のため各棟のセグメントはコアスイッチで終端されているものとし，ブロードキャストもコアスイッチでミラーリングする．講義室の PC1 台あたりの，学外に向かうトラフィックを $T_{\text{学外}}$，学内サーバに向かうトラフィックを $T_{\text{学内サーバ}}$，ARP 等のブロードキャストトラフィックを T_B とし，エッジスイッチ配下の端末台数を N とする．各スイッチ S から上流に流れるトラフィックを $T_i(S)$，各スイッチでミラーリングして上流に送信するトラフィックを $M_i(S)$ それぞれ図 8 の通りになると考えられる．なお，すべてのスイッチからのミラーリングトラフィックの合計は $T_{all}(i) = \sum_{S\in \text{ キャンパスネットワーク}} M_i(S)$ となる．ただし，図 8 中の計算では，$T(S), M_i(S)$ は物理インタフェースの帯域上限を最大値として計算する．

表 3 にネットブートの PC の起動時，及び授業などで学内サーバに保存されている動画の視聴時に想定される PC1 台あたりのトラフィック量を示す．起動時の $T_{\text{学外}}$, $T_{\text{学内サーバ}}, T_B$ は京都産業大学の情報処理教室で計測した値を用いた．なお，京都産業大学における計測についての詳細は 6 節で説明する．図 8 の式を用いて，各想定トラフィック量から算出した，ミラーリングされるトラフィック量を同じく表 3 に示す．起動時の監視トラフィック量は (1) 及び (2) の場合は，約 78Gbps となり，フィルタリング機能なしで提案方式を適用するのは困難であることが分かる．(3) では，約 12Gbps となり，削減はできている一方で，コアスイッチとファイアウォール間の帯域である 10Gbps を超えてしまっており，さらなる削減が必要となる．一方で，動画視聴をした場合の監視トラフィック量は，(1) 及び (2) では，約 490Mbps になっており，(3) においては，約 110Mbps となり，提案方式を適用するのは可能であると考えられる．情報処理教室の場合は，サーバを経由しない端末間の通信がほとんど発生しないため，このような結果になるが，研究室等のトラフィックについては，別途調査が必要である．

表 3　想定環境とその時のトラフィック量およびミラーリングしたトラフィック量

想定環境	$T_{\text{学内サーバ}}$ (Mbps)	T_{B} (Mbps)	$T_{\text{学外}}$ (Mbps)	$M_1(S_{c1})$ (Mbps)	$M_2(S_{c1})$ (Mbps)	$M_3(S_{c1})$ (Mbps)
起動時	600	0.001	0.7	78000	78000	12000
動画視聴時	0.15	0.001	0	490	490	110

なお，監視トラフィックを転送するのに十分な帯域が確保できる場合は，Gigamon[15] や NTO[16] など，重複解消機能をもったパケット処理装置を活用する方法が考えられるが，本研究では必ずしも十分な帯域が確保できない場合を想定しているため，以降ではさらなるトラフィック削減

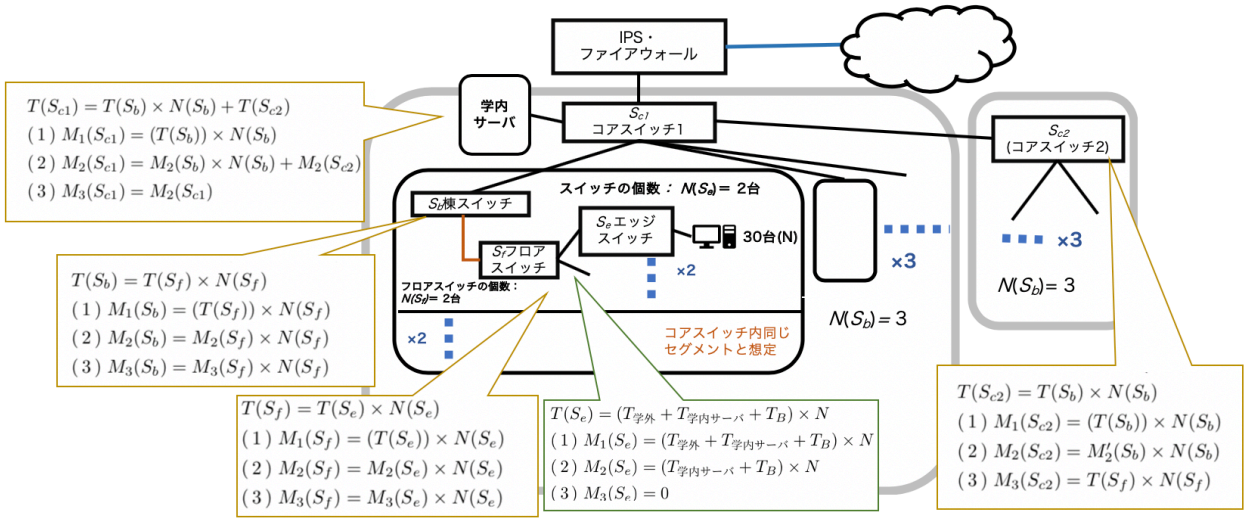

図 8　想定するキャンパスネットワークでのトラフィック量

の可否について検討する．

6. プロトコルの取捨選択によるトラフィック量削減可否の調査

さらなるトラフィック量の削減について，本節では，攻撃に利用される頻度等に基づいて，監視対象プロトコルを取捨選択することによるトラフィック削減可否について調査する．

本節では文献 [17] が対象としているプロトコルをベースとして，平常時のトラフィックにおいて，攻撃に悪用されるプロトコルのトラフィック量を調査する．調査には京都産業大学の情報処理教室の PC を用いて，起動時の 7 分間および起動後 8 分間のトラフィックを計測した．起動時に比べ起動後のトラフィックは少なかったため，以降では起動時についてのみ説明する．起動時の 1 秒あたりのトラフィック量 (bps) の最大値，1 秒あたりのパケット数 (pps) の最大値，関連する脆弱性数，特にリスクが高い脆弱性数を表 4 に示す．表 4 より，リスクの高い脆弱性が多い RDP のトラフィックは，最大でも 2,700 pps 以下であるため，出力性能が制限される syslog を用いたトラフィック収集方式も適用できると考えられる．一方で SMB や HTTPS は，リスクが高い脆弱性が多く，監視する必要があるが，2,700 pps を超えているためこの方式は適用できない．RSPAN，ERSPAN，NetFlow を用いたトラフィック収集方式においてフィルタリングを適用した場合でも，すべての PC が同時に起動してしまった場合，表 4 に載せたプロトコルの 1 台あたりのピークトラフィック量は $T_{学内サーバ} = 16Mbps$ となる．仮に 150 台が同時に起動した場合でも単純計算すると，2.4Gbps 程度となり，監視することができない．一方で，スイッチの処理性能をも上回っているため，全台数同時に起動することを前提に設計はされていない可能性が考えられる．例えば，実際にはあるひとつの教室においてのみ授業開始時に一斉に起動する程度が考えられる．この場合，(1) の方式のミラーリングトラフィックは 2550Mbps,(2) の方式のミラーリングトラフィックは 2445Mbps であり，両法式とも処理性能を超えている可能性があるが，(3) の方式のミラーリングトラフィックは 489Mbps 程度である．しかし，同時に起動した場合は，リアルタイムな監視は難しい．そのため，CVSS の値が 9.0 以上など，フィルタリングの条件をさらに絞るなどの手段で，さらなるトラフィックの削減を検討するか，ピーク時のトラフィックの観測漏れを許容する必要がある．

表 4　プロトコルの最大 bps，pps と関連する脆弱性数

プロトコル名 [17]	起動時の学内トラフィックの最大 bps	起動時の最大 pps	プロトコルに対する脆弱性の数	CVSS(リスク指標) が HIGH 以上の脆弱性の数
SMB	700K	4700	38	26
RDP	0	0	18	12
Kerberos	300K	2900	6	5
RPC	25K	1400	11	5
LDAP	16M	69700	3	3
HTTPS or HTTP	700K (学外トラフィック)	2200	46	25
WinRM(HTTP)	0	0	16	4
WinRM(HTTPS)	0	0	16	4
上記のトラフィックの最大	16.3M			

7. まとめと今後の課題

本稿では低コスト集中監視方式の実現に向けて，syslog, RSPAN, ERSPAN, sFlow NetFlow などのスイッチのプローブ機能のトラフィック監視への適用可能性を調査した．また，フィルタリングによるトラフィック削減可能性について調査した．結果としてトラフィックは削減できたが，提案手法による監視の実現には，更にトラフィック削減が必要であることが分かった．今後の課題として，本稿では論文 [1][2] のみを取り上げたが、他の組織内ネットワー

クで使用される攻撃がどのようなものであるのかの調査が必要である．また，実際に収集したデータを用いてファイアウォール等が攻撃検知可能であるか等の検証をする必要がある．その際，ファイアウォールの分散配置によるコアトラフィックの低減についても検討が必要である．さらに，本稿ではキャンパスネットワークなどの，物理ネットワークを対象としたが，今後は Open vSwitch などのソフトウェアスイッチのミラーリング機能を調査し，クラウドサービスにおける監視手法も考える必要がある．

謝辞

本研究の一部はアラクサラネットワークス株式会社との共同研究として実施されたものであり，研究開発の過程で NICT 総合テストベッドを活用させていただいた．ここに記して謝意を表す．

参考文献

[1] 山田 正弘 他 4 名 “組織内ネットワークにおける標的型攻撃の検知方式”, 研究報告セキュリティ心理学とトラスト (SPT),Vol.2013-SPT-6,No. 53, pp.1-6(2013).

[2] 佐々木 良一, 他 2 名 “標的型攻撃に対するネットワークフォレンジック対策の現状と今後の展望,” コンピュータセキュリティシンポジウム 2013 論文集, vol.2013, No.4, pp.155-162, (2013).

[3] 三島 和宏, 他 3 名 “ ネットワークモニタリングによる高セキュリティリスク端末の自動遮断システムとその運用”, 研究報告インターネットと運用技術 (IOT),Vol.2030-IOT-48,No. 4, pp.1-6(2020).

[4] 鈴木 彦文, 他 4 名 “NetFlow トラフィックデータの取得と解析に関する共同研究”, 学術情報処理研究,2018 年 22 巻 1 号 p. 3-11(2018).

[5] ALAXALA Networks, Corp., “コンフィグレーションガイド Vol.2”, [Online]. 参照先 https://www.alaxala.com/jp/techinfo/archive/manual/AX6000S/html/11_9/CFGUIDE2/0026.HTM （参照日 2020-05-17).

[6] CISCO Inc., “Understanding Access Control List Logging”, [Online]. 参照先 https://tools.cisco.com/security/center/resources/access_control_list_logging (参照日 2020-05-17).

[7] CISCO Inc., “Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド Rel. 12.2(40)SE”, [Online]. 参照先 https://www.cisco.com/c/ja_jp/td/docs/sw/lanswt-access/cat2960swt/cg/005/swcfg/swspan.html (参照日 2020-04-22).

[8] IETF Tools, “Cisco Systems’ Encapsulated Remote Switch Port Analyzer (ERSPAN) ”, [Online]. 参照先 https://tools.ietf.org/html/draft-foschiano-erspan-03 (参照日 2020-04-22).

[9] CISCO Inc., “Catalyst Switched Port Analyzer (SPAN) Configuration Example”, [Online]. 参照先 https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html (参照日 2020-04-22).

[10] CISCO Inc., “NetFlow Export Datagram Format”, [Online]. 参照先 https://www.cisco.com/c/en/us/td/docs/net_mgmt/NetFlow_collection_engine/3-6/user/guide/format.html (参照日 2020-04-22).

[11] CISCO Inc., “NetFlow Version 9 Flow-Record Format ”, [Online]. 参照先 https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html (参照日 2020-04-22).

[12] 松田 勝敬, “キャンパスネットワークにおける WAN 接続環境の変更”, 東北工業大学紀要,No.36,pp.25-31(2016).

[13] 松田 勝敬他 1 名 “キャンパスネットワークにおける WAN 接続広帯域化の効果”, 第 78 回全国大会講演論文集,Vol 2016, No.1,pp.27-28(2016).

[14] 東北工業大学, “情報サービスセンター”, [Online]. 参照先 https://www.tohtech.ac.jp/outline/institution/infocenter/ (参照日 2020-05-18).

[15] マクニカネットワークス社, “Gigamon”, [Online]. 参照先 https://www.macnica.net/gigamon/（参照日 2020-05-18）.

[16] Ixia 社, “NTO”, [Online]. 参照先 https://www.ixiacom.com/ja/resources/ixia-nto-overview（参照日 2020-05-18）.

[17] “インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 (第 2 版)”, 一般社団法人 JPCERT (2017).