巡回監視による監視対象トラフィックデータの削減とその影響に関する評価

長谷川 皓一[1]　山口 由紀子[2]　嶋田 創[2]　高倉 弘喜[3]

概要：一般的な攻撃検知手法の一つとして，IDS 等を用いたネットワークトラフィックの監視が行われている．しかし，監視対象のトラフィック量の増加に伴い，監視を行う機器等のコストも膨大となっていく．それに対し我々は，監視を行う対象を切り分け，その対象を巡回的に切り替えることで，同時に監視する必要のあるトラフィック量を削減するネットワーク巡回監視を提案してきた．本稿では，複数のセグメントから構成される小規模な組織ネットワークに対してネットワーク巡回監視を適用することを想定し，削減可能な監視対象トラフィック量およびその影響について，机上検討および実機を用いた検証実験による評価を行う．

キーワード：ネットワーク監視，巡回監視，パケットキャプチャ

An Evaluation on Reduction of Traffic Amount and Influence by Network Patrol Monitoring

Hirokazu Hasegawa[1]　Yukiko Yamaguchi[2]　Hajime Shimada[2]　Hiroki Takakura[3]

Abstract: Monitoring network traffic data by using appliances like IDS is one of the general attack detection methods. However, with the increase in the amount of traffic to be monitored, the cost of monitoring equipment is also becoming enormous. As a solution for this problem, we proposed network patrol monitoring. It can reduce the amount of traffic that needs to be monitored at the same time by dividing monitoring target to several segments and switching those separated segments periodically. This paper evaluates the amount of monitored traffic that can be reduced by the network patrol monitoring and its impact based on desk study and verification experiments that models a small organization network composed of multiple segments.

Keywords: Network Monitoring, Patrol Monitoring, Packet Capturing

1. はじめに

サイバー攻撃の検知手法の一つとして，ネットワークトラフィックの監視が一般的に行われている．これは，インターネットと組織内部ネットワークの境界部に設置したIDS 等により，不審な通信を監視するものである．しかし，監視対象のトラフィック量の増加に伴い，監視を行う機器等のコストも膨大となっていく．規模の大きな組織においては，このようなネットワークの境界部に設置する機材に対して非常に高額なコストが必要となる．

それに加え，標的型攻撃などの昨今の巧妙化するサイバー攻撃への対策の一つとして，ネットワークの境界部のみならず，ネットワーク内部でマルウェアが行う通信を検知に用いる手法もある．例えば，我々はこれまでに，組織内部のネットワークの適切なセグメンテーションおよびアクセス制御を行うネットワーク内部分離設計に着目してきた [1]．ネットワーク内部分離設計では，異なる部署間の端末同士の直接通信といった不必要な通信区間を予め

[1] 名古屋大学 情報戦略室
Information Strategy Office, Nagoya University
[2] 名古屋大学 情報基盤センター
Information Technology Center, Nagoya University
[3] 国立情報学研究所
National Institute of Informatics

遮断しておくことにより，マルウェアが偵察活動等のために通信を試みようとする活動の形跡を検知することが可能である．独立行政法人情報処理推進機構の「高度標的型攻撃」対策に向けたシステム設計ガイド [2] においても，ActiveDirectory への不審なアクセスや，サーバへの不正ログインなど，ネットワーク内部のマルウェアの活動に対して対策を強化することが推奨されている．標的型攻撃で用いられる巧妙なマルウェアの場合，ネットワークの境界部における対策をすり抜けてしまう場合も多いため，このような内部通信の監視，およびそれを用いた検知は今後より一層重要になると考えられる．

また，昨今では，Software Defined Network(SDN) と呼ばれる技術を用いてトラフィックの収集が可能であったり [3]，トラフィックのミラーリングを行うことが可能な安価なネットワークスイッチも存在するため，比較的容易に既存のネットワークに対して通信監視の基盤を導入することも可能である．

しかしながら，組織内ネットワークの全内部通信の監視は，ネットワークの境界部の監視に比べて通信量が多いため，さらにコストが必要となる．

それに対し我々は，監視を行う対象を切り分け，その対象を巡回的に切り替えることで，同時に監視する必要のあるトラフィック量を削減するネットワーク巡回監視を提案してきた [4]．このネットワーク巡回監視は市販の監視機器性能に対して監視対象トラフィックが膨大過ぎる場合にも有効であり，例えば，国立情報学研究所が主催する「大学間連携に基づく情報セキュリティ体制の基盤構築」においても採用されている [5]．ネットワーク巡回監視は，監視対象トラフィック量の削減により監視コストの低減が期待できるが，常時全パケットを監視する一般的な監視方法と異なり，監視対象外の時間帯にマルウェアが行う通信を見逃してしまう欠点がある．

本稿では，企業内部ネットワークに対してネットワーク巡回監視を適用した場合を想定し，ネットワーク巡回監視により削減可能なトラフィック量，およびその影響に関して，机上検討および実組織のネットワークを模して作成した複数のサーバ/クライアントを含む実機検証環境を用いた評価を行う．

2. 想定する実組織のネットワーク環境

本稿では，図 1 に示す比較的小規模な企業内部ネットワークに対して，ネットワーク巡回監視を適用する場合を想定する．想定環境では，ネットワーク内に総務部，経理部，営業部，運営管理部，開発部の 5 部署それぞれのセグメントに加え，サーバセグメントと DMZ セグメントが存在する．各セグメント間のアクセスコントロールは行われておらず，自由にセグメント間の通信が行える状態である．

ネットワークに接続される端末数は，サーバセグメント

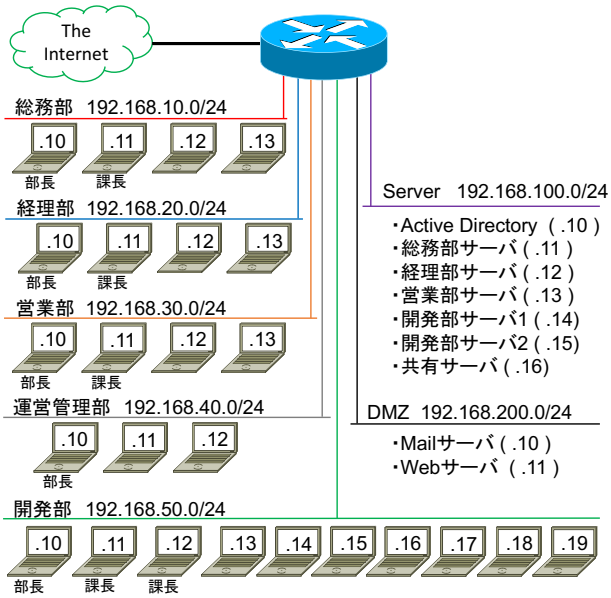


図 1 想定する実組織ネットワーク

Fig. 1 Assumed an Actual Organization Network

の Windows サーバが 7 台，DMZ セグメントの Linux サーバが 2 台，各部署の Windows クライアントが 25 台となっている．ネットワーク巡回監視はセグメント単位で実施するが，ネットワーク内部通信の監視を目的として行うため，DMZ セグメントを出入りする通信についてはネットワーク境界部において別途常時監視が行われるものとし，監視の対象としない．そのため，ネットワーク巡回監視の対象となるセグメント数は 6 となる．

3. 机上検討

想定環境においてネットワーク巡回監視を適用した場合の削減可能な監視対象トラフィック量および，ネットワーク巡回監視による影響について，まずはじめに机上検討を行う．机上検討においては，全てのセグメントにおいて単位時間あたりの通信の流量が同じであると仮定する．

3.1 監視対象トラフィック量の削減

想定環境において，ネットワーク巡回監視を適用することにより削減可能なネットワークトラフィック量を検討する．まず，ネットワーク巡回監視を適用せず，想定環境における全てのセグメントを常時監視する場合の監視対象トラフィック量を比較基準とし，1 とする．ここで，ネットワーク巡回監視を用いて監視を行う際に，一度に並列で監視を行うセグメントの数を並列監視数 $n(1 \leq n \leq 6)$ とする．並列監視数 n が最大値（この場合 6）を取る場合，全てのセグメントを並列に監視できる．従って，$n = 6$ の場合の監視対象トラフィック量は，ネットワーク巡回監視を導入しない場合における監視対象トラフィック量と同等の 1 となる．それに対し，n の値を 1 から 5 とする場合，n の

値が小さいほど一度に監視するセグメントの数は少なくなり，監視対象トラフィック量の削減が可能である．つまり，ネットワーク巡回監視を用いることで監視対象トラフィック量は $n/6$ となる．

3.2 ネットワーク巡回監視による影響

次に，ネットワーク巡回監視を適用した場合に生じる影響について検討する．ネットワーク巡回監視を行う場合，ある時間帯において監視対象となっていないセグメントで発生したマルウェアによる悪性通信（マルウェアの活動を中心とする，サイバー攻撃に関連する通信）を見逃してしまう．そこで，ある時間にある端末がマルウェアに感染したことを想定し，そのマルウェアが発する悪性通信をキャプチャできるまでに要する時間の差異を検討する．標的型攻撃において用いられるマルウェアは標的に合わせて専用に設計される場合も多いため，C&C サーバとの通信間隔なども様々なパターンが存在する [6]．また，標的型攻撃は長期間に渡り潜伏しながら密かに活動するものであると考えられてきたが，トレンドマイクロの分析 [7] によれば，数時間から 1 日の間に情報を持ち出すといった短期間で行われる攻撃も使い分けられるように存在しており，攻撃によっても通信頻度，パターンなどは異なるものであると考えられる．今回の検討では，インシデントの発生モデルとして，マルウェア感染の初期段階である以下の条件を想定する．

- 営業部セグメントの 1 台の端末（192.168.30.11）がマルウェアに感染した．
- マルウェアは，60 分間に 1 度，ランダム時刻に C&C サーバと通信を行う．

1 回のネットワーク巡回監視における各セグメントの監視時間は 10 分間とし，常に同じ順に監視対象セグメントを切り替えると想定する．

このモデルにおいて，ネットワーク巡回監視を適用しない場合には，全てのセグメントを常時監視しており，マルウェアが発する悪性通信を全てキャプチャすることが可能である．つまり，ネットワーク巡回監視を適用しない場合，マルウェアが発した悪性通信を最初にキャプチャ可能な時刻は最初にマルウェアが通信を行った時刻となる．

これに対し，ネットワーク巡回監視を用いる場合にマルウェアの通信をキャプチャ可能な時刻の遅延を期待値の形で評価する．ネットワーク巡回監視では，並列監視数 n を最大（$n = 6$）として常時全てのセグメントの監視を行う場合，最初にマルウェアが悪性通信を行った時刻にキャプチャが可能であり，ネットワーク巡回監視を用いない場合と同等である．しかしながら，並列監視数 n が 1 から 5 で巡回監視を行う際には，感染端末が発生した営業部セグメントの監視を行っていない時間帯にマルウェアが発した悪性通信のキャプチャが行えず，何回か見逃す可能性がある．見逃しが発生する場合には，マルウェアが発する何回目かの悪性通信をキャプチャできるまでの時間が，マルウェア通信のキャプチャ時刻の遅延となる．そこで，マルウェアの発した悪性通信をキャプチャするまでに要する時間の期待値を分単位で求める．マルウェアは 60 分間に 1 度の頻度で通信を行うため，60 分単位で検知できる確率を離散的に求めることにより，検知するまでの所要時間（分）の期待値が求まる．

まず，並列監視数 n に応じて，60 分間のうちで一つのセグメントを監視できる時間 $Time(n)$ を求める．

$$Time(n) = \left(\frac{60}{\text{セグメント数}}\right) n \tag{1}$$

想定する実組織ネットワークでは監視を行うセグメント数は 6 であるため，$Time(n) = 10n$ となる．$Time(n)$ を用いて，以下の式によりマルウェア通信をキャプチャするまでに要する時間の期待値を求めた．

$$\text{期待値 } E(n) = \sum_{h=0}^{\infty} 60h \left(\frac{Time(n)}{60}\right) \left(1 - \frac{Time(n)}{60}\right)^{h} \tag{2}$$

表 1 に，想定する実組織ネットワーク環境における並列監視数 n とマルウェア通信をキャプチャするまでに要する時間の期待値を示す．

表 1 並列監視数 n とキャプチャに要する時間の期待値
Table 1 Parallel Monitoring Number n and Expected Value of Time Required for Capture.

n	キャプチャに要する時間期待値
1	300 分
2	120 分
3	60 分
4	30 分
5	12 分
6	0 分

並列監視数 n が小さいほど同時に監視するトラフィック量が少ない．そのため，並列監視数 n が小さいほどマルウェア通信をキャプチャできる可能性も小さくなり，キャプチャするまでに要する時間の期待値も増えている．

4. 模擬実組織ネットワーク環境における実機検証

本節では，想定する実組織のネットワーク環境を実機により構築する方法および，実際にトラフィックのキャプチャを行う検証実験の方法およびその結果を示す．

4.1 実験環境

4.1.1 想定環境の構築

図 1 に示した想定環境を実際に構築した．総務部，経理部，営業部，運営管理部，開発部に属するクライアント端末として，25 台の Microsoft Windows 10 端末を配置した．これらのクライアント端末は，通常通信を模倣するものとして，5 分間に 1 度ランダム時刻に Web ブラウザを起動し，インターネット上の Web サーバに対して http アクセスを行う．また，10 分間に 1 度，ランダム時刻に，サーバセグメント内の各サーバに用意された，端末の使用者がアクセス可能なディレクトリに対してテキストファイルを書き込むアクセスを行う．さらに，各クライアント端末上ではメールクライアントソフトウェアが常時起動しており，1 分間に 1 度，DMZ セグメント内の Mail サーバに対して受信メールの確認を行う設定となっている．

サーバセグメントに属するサーバ端末として，7 台の Microsoft Windows Server 2012 R2 を配置した．この内，1 台のサーバ端末が Active Directory の機能および DNS の機能を有し，ネットワーク内の全クライアント端末が使用するユーザアカウントの管理，サーバセグメント内に配置された各サーバ端末内のディレクトリに対するアクセス制御，および DNS サービスを行っている．また，DMZ セグメントに属するサーバ端末として，2 台の Ubuntu Server を配置した．この内 1 台は Mail サーバとして機能し，postfix および dovecot によりネットワーク内の全ユーザに対してメール機能を提供している．もう 1 台のサーバ端末は組織外部への Web サービスを提供するための Web サーバとして apache が稼働している．

この環境は，VirtualBox[*1]による仮想マシンを用いて実現している．物理的な構成を図 2 に示す．16 台の PC 端末を利用し，各端末のスペックに応じて 1 台から 4 台の仮想マシンを割り当てている．これに加え，1 台の PC 端末がルータソフトウェアの VyOS[*2]を用いた PC ルータとして稼働している．

4.1.2 ネットワーク巡回監視の実装

ネットワーク巡回監視のためには，一定時間ごとに通信をミラーするセグメントを変更する必要があるが，この実装にはいくつかの方法が考えられる．1 つ目の方法として，OpenFlow のような SDN を用いた実装が考えられる．しかしながら，OpenFlow 対応のネットワークスイッチはまだまだ高価であること，このような比較的単純な用途ではオーバースペックという点から費用対効果が低い．2 つ目の方法としては，一定時間ごとにミラー設定を変更する設定が可能なネットワークスイッチを用いた実装が考えられる．例えば，Juniper 社のネットワークスイッチでは設定の操作に Python 言語と専用の API を利用できる Junos PyEZ というフレームワークがあり [8]，time.sleep と設定変更 API を組み合わせることで実装可能である．

今回の実験では，ネットワーク巡回監視コストのさらなる削減を目的として，GUI による設定変更にのみ対応した安価なネットワークスイッチに対して，GUI スクリプトを用いてミラー設定を一定時間ごとに変更する，低コストでネットワーク巡回監視を実現する手法を用いた [9]．図 2 に示したように，実験ネットワークに NETGEAR 製の GS108E スイッチを 3 台（GS108E_1，GS108E_2，GS108E_3）配置している．GS108E はポートミラーリング機能を有しており，ミラー対象を Web インターフェイスから選択可能である．

GS108E_1 には，1 番ポートから 5 番ポートまでの 5 つのポートに対して，それぞれ総務部セグメント，経理部セグメント，営業部セグメント，運営管理部セグメント，開発部セグメントが接続されており，これらのポートの通信をミラーリングし，GS108E_3 へと送出する．ミラーリング対象のポートは，接続された制御用 PC（Controller）が Web インターフェイスから自動的に設定変更を行い決定する．GS108E_2 も同様に，1 番ポートに接続されたサーバセグメントの通信をミラーリングし，GS108E_3 へと送出する．GS108E_3 に対して，GS108E_1 と同様に制御用 PC により表 2 に示す例のような監視スケジュールで適切な設定を行うことにより，ネットワーク巡回監視によるミラートラフィックをトラフィック収集用 PC（Capture）に送出する．

表 2　1 並列巡回監視の監視設定例
Table 2　Example of Configuration about 1 Parallel Patrol Monitoring.

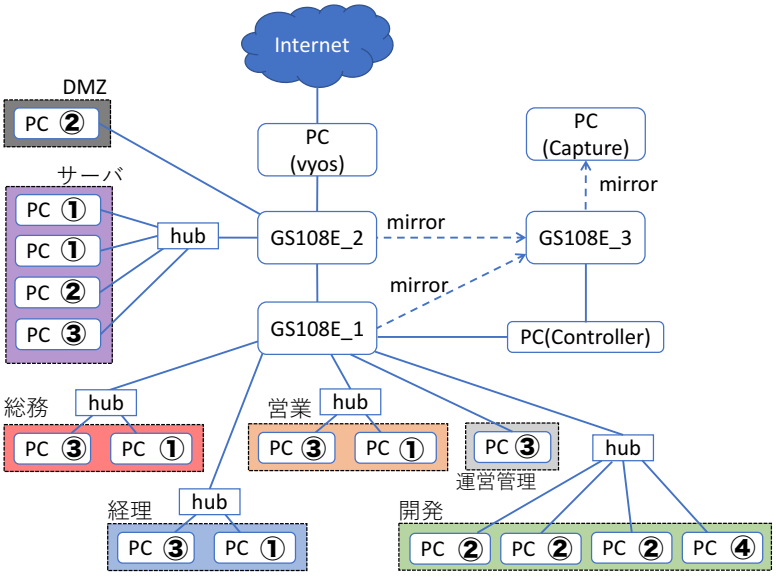
時刻	GS108E_1 監視対象	GS108E_3 監視対象
0:00〜0:10	総務部	GS108E_1(総務部)
0:10〜0:20	経理部	GS108E_1(経理部)
0:20〜0:30	営業部	GS108E_1(営業部)
0:30〜0:40	運営管理部	GS108E_1(運営管理部)
0:40〜0:50	開発部	GS108E_1(開発部)
0:50〜1:00	総務部（監視対象外）	GS108E_2(サーバ)
1:00〜1:10	総務部	GS108E_1(総務部)
⋮	⋮	⋮

4.2 収集トラフィック量の検証

構築した環境下において，実際にネットワークトラフィックを収集し，削減可能な監視対象トラフィック量の検証を行った．この際，トラフィック収集を行う時間は 60 分間とし，ネットワーク巡回監視を適用する場合には一度に監視を行う監視時間は 10 分間とした．その上で，以下のパターンの監視方法でトラフィックのキャプチャを行った．

(1) 非巡回監視

[*1] https://www.virtualbox.org/
[*2] https://vyos.io/



＊丸数字はPC上で稼働する仮想端末の数

図 2 実験環境の物理構成
Fig. 2 Physical Constitution of Experiment Environment

全てのセグメントのトラフィックを常時監視する．

(2) 1 並列巡回監視
1 セグメントずつ巡回して監視する．

(3) 2 並列巡回監視
2 セグメントずつ巡回して監視する．

(4) サーバセグメント+1 並列巡回監視
サーバセグメントのトラフィックを常時監視した上で，その他のセグメントを 1 セグメントずつ巡回して監視する．

これらのパターンのトラフィックキャプチャを各 3 回ずつ行った．表 3 に，観測されたトラフィック量の平均値を示す．

表 3 観測されたトラフィック量（60 分間）
Table 3 Amount of Captured Network Traffic (60 min).

監視方法	平均監視トラフィック量
非巡回	169.93MB
1 並列巡回	23.63MB
2 並列巡回	40.80MB
サーバ seg+1 並列巡回	32.13MB

4.3 マルウェア通信見逃しの検証

次に，ネットワーク巡回監視を適用することによるマルウェア通信の見逃しを検証する．実験環境内において，標的型攻撃の侵攻段階の異なる 2 パターンのインシデント発生モデルを想定し，実際にトラフィックのキャプチャを行った．この際，ネットワーク巡回監視の方法は 4.2 節と同様とし，監視時間は 10 分間，監視方法は 1 並列巡回，2 並列巡回，サーバセグメント常時監視+1 並列巡回の 3 パターンとした．トラフィックのキャプチャ時間は，表 1 で示した並列監視数 n に応じたキャプチャに要する時間の期待値を用い，1 並列巡回は 300 分，その他は 120 分とした．これにより，表 1 の期待値時間内でマルウェア通信のキャプチャが可能か検証する．このようなトラフィックのキャプチャをそれぞれの監視方法につき 3 回ずつ行った．なお，ネットワーク巡回監視を適用しない場合については，マルウェアの通信を全てキャプチャ可能であることが自明であるため，今回は実験の対象としていない．

4.3.1 感染初期段階におけるマルウェア通信

3.2 節と同様の，以下のインシデント発生モデルを想定する．

- 営業部セグメントの 1 台の端末（192.168.30.11）がマルウェアに感染した．
- マルウェアは 60 分間に 1 回，ランダム時刻に C&C サーバと通信を行う．

マルウェア通信の模擬として，192.168.30.11 の端末から，60 分間に 1 度ランダム時刻に，インターネット上に設置された Web サーバに対して http アクセスを行う．このような状況においてトラフィックのキャプチャを行い，キャプチャしたトラフィック中に模擬したマルウェア通信が含まれているか確認した．表 4 にマルウェアの通信のキャプチャに成功した件数および，キャプチャ成功率の平均値を示す．

実験の結果，机上検討で求めた期待値時間の監視を行っても，マルウェア通信のキャプチャに成功した件数が 0 で

表 4　感染初期段階におけるマルウェア通信キャプチャ結果
Table 4　Trial Result of Malware Communication Capturing in Initial Stage of Infection.

監視方法	キャプチャに成功した件数 / 全通信件数			平均キャプチャ成功率
	試行 1 回目	試行 2 回目	試行 3 回目	
1 並列巡回	1/5 件	0/5 件	3/5 件	27%
2 並列巡回	0/2 件	1/2 件	2/2 件	50%
サーバセグメント +1 並列巡回	0/2 件	1/2 件	0/2 件	17%

あり，見逃してしまう場合も多く発生した．

4.3.2　基盤構築段階におけるマルウェア通信

次に，攻撃の段階が進み，基盤構築を行っている段階を考慮し，マルウェアによる通信頻度を増やした以下のモデルを想定し，感染初期段階におけるマルウェア通信の実験の際と同様にトラフィックのキャプチャを行った．ただし，この実験については，すべての監視方法の場合においてキャプチャを行う時間を 120 分間とした．

- 営業部セグメントの 1 台の端末（192.168.30.11）がマルウェアに感染した．
- 営業部セグメント内で別の 1 台の端末（192.168.30.10）にマルウェア感染が拡大している．
- それぞれのマルウェアは 60 分間に 1 度，ランダム時刻に C&C サーバと通信を行う．

このような状況が既に一定期間継続しているという条件のもと，キャプチャを行う際に以下の活動が行われるものとする．

- 営業部セグメント内の 2 台の感染端末は運営管理部の部長の端末（192.168.40.10），開発部の部長の端末（192.168.50.10），課長の端末（192.168.50.11，192.168.50.12）に対してそれぞれ 60 分間に 1 度，ランダム時刻に感染拡大のために通信を試みる．
- さらに，キャプチャ開始から 1 時間後以降から 2 時間後までの間のランダム時刻に 1 度，感染が拡大した運営管理部の端末（192.168.40.10）から ActiveDirectory サーバ（192.168.100.10）に対して通信が発生する．

つまり，マルウェアが発する悪性通信は，120 分間中に，C&C サーバに対する通信が計 4 件，感染拡大のためにセグメントをまたいで行われる通信が計 16 件，サーバに対する通信が計 1 件である．以上の想定においてキャプチャを 3 回試行した結果，マルウェアが発する上記の 3 種類の通信のそれぞれについてキャプチャに成功した件数の平均値およびキャプチャ成功率を表 5 に示す．

外部の C&C サーバに対する通信に関しては，感染初期段階におけるマルウェア通信と同様に見逃してしまう場合も多く見受けられ，全 9 回のキャプチャ（監視方法 3 種類，キャプチャ施行回数 3 回）の内，4 回のキャプチャにおいては全ての C&C 通信を見逃すという結果になった．一方で，感染拡大のための内部通信および感染端末から ActiveDirectory に対する通信に関しては，外部通信と比べてキャプチャに成功する場合が多く，また全ての通信を見逃すというケースは存在しなかった．

5.　考察

監視対象トラフィック量に関しては，机上検討の段階では各セングメントの通信流量が一定であるという想定のもとに算出し，並列に監視を行うセグメント数である並列監視数 n に応じた $n/6$ であるとした．実際には，セグメント内の端末数や，各端末の通信量に依存するため，一概に $n/6$ の通信量になることは少ない．しかしながら，実機検証における収集トラフィック量の検証結果から，ネットワーク巡回監視を適用することにより，並列監視数 $n = 1$ の場合の巡回監視時にはキャプチャしたトラフィック量が約 1/7 になり，並列監視数 $n = 2$ の場合の巡回監視においても，監視対象の決定方法により異なるが，キャプチャしたトラフィック量は 1/4 から 1/5 となっていた．これらの値は，それぞれ机上検討で示した値の $1/6(n = 1$ の場合$)$，$2/6(n = 2$ の場合$)$ よりも多くのトラフィック量の削減に成功している．以上より，概ね机上検討で示した値に近いトラフィック量の削減が可能であることが示された．

今回の検証では，比較的小規模な実験環境において，各クライアントがわずかな通信しか発生させておらず，常時監視した場合でも単位時間あたりのトラフィック量は 130MB 程度と非常に少ない数字であった．しかし実際には，使用環境にもよるが，各クライアントがより大量な通信を発生させる上，規模が大きなネットワークではその台数も大きくなるため，トラフィック総量は大幅に大きくなる．そのため，ネットワーク巡回監視によるトラフィック量の削減は大きなコストダウンに繋がる有用なものであると考えられる．

マルウェア通信の見逃しについては，感染端末が組織ネットワーク内に 1 台のみ存在し外部の C&C サーバとの通信回数も少ない，攻撃の段階が最初期の場合においては，ネットワーク巡回監視による見逃しが多く発生してしまうことがわかった．机上検討においては，ネットワーク巡回

表 5　基盤構築段階におけるマルウェア通信キャプチャ結果 (試行 3 回の平均値)
Table 5　Trial Result of Malware Communication Capturing in Attacking Infrastructure Building Stage (Average of 3 Trial).

監視方法	キャプチャに成功した件数 / 全通信件数			キャプチャ成功率		
	外部通信	内部通信	サーバへの通信	外部通信	内部通信	サーバへの通信
1 並列巡回	0.3/4 件	5.0/16 件	0.3/1 件	8%	31%	33%
2 並列巡回	1.0/4 件	9.3/16 件	1.0/1 件	25%	31%	100%
サーバセグメント +1 並列巡回	0.3/4 件	4.0/16 件	1.0/1 件	8%	25%	100%

監視を適用した場合に，並列監視を行うセグメント数に応じたマルウェア通信のキャプチャに要する時間の期待値を示した．実機検証を行なった結果，机上検討で求めた期待値時間の監視を行なってもキャプチャに失敗する場合も多く，キャプチャの成功率が最も悪い場合には 17%程度と，監視方法によっては約 8 割の通信を見逃してしまうケースもあった．しかしながら，ネットワーク巡回監視による内部ネットワークの監視は，従来から行われているネットワークの境界部における監視を補完する位置付けである．ネットワーク境界部における監視では，今回の実験で見逃してしまうようなマルウェアによるインターネットに対する通信を観測することが可能である．そのため，ネットワーク巡回監視は従来から行われているネットワーク境界部における監視と並列して行うことが必須であると考えられる．

次に，攻撃の段階が進行し，マルウェアが基盤構築を行なっている場合の通信のキャプチャについて議論する．基盤構築段階を想定した実機検証において，マルウェアが発する外部の C&C サーバに対する通信に関しては，感染初期段階を想定した実験の結果よりキャプチャの成功率は低く，8%から 25%程度であり，マルウェア通信の見逃し率が高いことがわかる．

一方で，感染拡大のためのセグメントをまたいだ内部通信や，ActiveDirectory サーバ対する通信については，多くのキャプチャに成功しており，キャプチャ成功率は内部通信は 25%から 31%，サーバへの通信は 33%から 100%という結果になった．これは，マルウェアによる通信が発生した際に，送信元 IP アドレスのセグメント，もしくは送信先 IP アドレスのセグメントのいずれかが，ネットワーク巡回監視による監視対象となっていればキャプチャが行えるため，キャプチャできる可能性が高まるためであると考えられる．また，基盤構築段階を想定した実験の全てのキャプチャにおいて，2 件以上の内部通信をキャプチャ出来ており，マルウェアの活動のなんらかの兆候をキャプチャ可能であるものと考えられる．この結果は，ネットワーク内部の通信を観測するという本来の目的を達成できているということである．

今回行った実機検証においては，2 つのセグメントを並列して監視する巡回方法として，2 セグメントずつ切り替えを行う場合と，サーバセグメント常時監視を行った上での 1 セグメントの巡回切り替えを行う場合の，2 種類の監視方法を選択した．その結果，サーバセグメントの常時監視を行った場合は，マルウェアが発する組織内サーバに対する通信は全てキャプチャ可能な一方で，C&C サーバに対する通信やネットワーク内部の通信のキャプチャ成功率は 2 セグメントずつ監視対象を切り替えた場合に比べて低いものであった．この結果から，2 並列の巡回を行う場合でも監視対象の選択方法によって，キャプチャできる可能性が高いマルウェア通信の種類が異なることがわかる．つまり，C&C 通信等の攻撃の兆候を見つけたい，重要サーバへの通信を監視したいなどといった，内部通信の監視目的や検知したいマルウェア通信の種類といった利用者のニーズに合わせて適切な監視方法を選択することにより，ネットワーク巡回監視によるマルウェア通信の見逃しという影響を低減できる可能性があると考えられる．

以上より，ネットワーク巡回監視は，監視対象トラフィックの削減によるコスト減を実現しつつ，マルウェアによる内部ネットワークの通信を観測可能な有用な手法であると考えられる．

6. おわりに

本稿では，組織内部のネットワークトラフィック監視を行う手法であるネットワーク巡回監視について，監視対象トラフィック量の削減および，手法を適用することによるマルウェア通信の見逃しという影響について，机上検討および実機による検証を行った．結果，監視対象トラフィック量は並列に監視を行う対象の数に応じて異なるが，概ね机上検討のとおり削減できることが確認できた．また，机上検討で得られたマルウェア通信のキャプチャに要する時間の期待値の観測を行なっても，キャプチャできない場合があった．しかしながら，マルウェア活動のいずれかの通信が観測できる可能性が高く，この手法による影響は小さいものであると結論づけた．以上より，ネットワーク巡回監視の有効性を示した．

今後の課題として，今回の実験で想定した以外の様々なインシデントの状況を想定した実験を行い，攻撃の侵攻度合いや初期感染端末の台数等に応じたマルウェア通信キャプチャの成功率の変化を求めることにより，ネットワーク

巡回監視を適用した場合に見逃す可能性が高い攻撃段階や状況を明らかにする必要がある．

謝辞　本稿の執筆にあたり多くの助言を頂いた名古屋大学情報基盤センター村瀬勉教授に感謝する．

参考文献

[1] 長谷川皓一，山口由紀子，　嶋田創，高倉弘喜：ディレクトリサービス情報とトラフィックデータによる ACL 自動生成システム，電子情報通信学会論文誌 D，Vol.J100-D，No.3，pp. 353–364 (2017).
[2] 独立行政法人情報処理推進機構：「新しいタイプの攻撃」の対策に向けた設計・運用ガイド改定第 2 版，（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000017308.pdf⟩.
[3] 堤　啓彰，谷口義明，井口信和，渡辺健次：OpenFlow ネットワークモニタリングシステムの開発，インターネットと運用技術シンポジウム 2014 論文集，pp. 23–30 (2014).
[4] Hasegawa, H., Yamaguchi, Y., Shimada, H. and Takakura, H.: Proposal of a Network Control System to Detect, Analyze and Mitigate Targeted Cyber Attacks, 電子情報通信学会技術報告，Vol.113，No.240，IA2013-26，pp. 1–6 (2013).
[5] 国立情報学研究所：平成 28 年度 SINET・学術情報基盤サービス説明会資料，（オンライン），入手先 ⟨http://www.nii.ac.jp/userdata/openforum/PDF/2016/8_setsumeikai2016_security_20161119.pdf⟩.
[6] 田辺瑠偉，　鉄穎，　水戸慎，牧田大佑，神薗雅紀，星澤裕二，吉岡克成，　松本勉：長期動的解析によるマルウェアの特徴的な DNS 通信の抽出，コンピュータセキュリティシンポジウム 2012 論文集，Vol. 2012, No. 3, pp. 712–719 (2012).
[7] トレンドマイクロ：国内標的型サイバー攻撃分析レポート 2016 年版，（オンライン），入手先 ⟨https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=194⟩.
[8] TechLibrary, J. N.: Junos PyEZ, (online), available from ⟨https://www.juniper.net/documentation/en_US/release-independent/junos-pyez/information-products/pathway-pages/index.html⟩.
[9] 長谷川皓一，山口由紀子，　嶋田創，高倉弘喜：ネットワークトラフィック巡回監視の実装に関する一検討，平成２９年度電気・電子・情報関係学会 東海支部連合大会論文集，C4-7 (2017).