Vol.2015-IOT-28 No.28
2015/3/6

SNMP を利用したバーストトラフィック検知方式の検知精度評価の報告

村井秀聡[†1]　砂田英之[†1]　牧和宏[†2]

ネットワークの監視では，通常の平均トラフィック監視では検知できず，障害の原因が不明となる事例が存在しており，この要因の一つとして，瞬間的にトラフィックが増大するバーストトラフィックが挙げられる．我々は，このような障害への対応として，「SNMP を利用したバーストトラフィック検知方式」を提案しており，今回，データセンターでの検知を目的とした提案方式の検知精度評価を実施した．本稿では，その評価結果について報告する．

Report of the accuracy evaluation of SNMP-based Burst Traffic detection method

SHUTO MURAI[†1]　HIDEYUKI SUNADA[†1]
KAZUHIRO MAKI[†2]

In the monitoring of the network, there are cases in which the general average traffic monitoring can not be detected and cause of the failure is unknown. One of the factors that cause them, include the Burst Traffic. As a solution of these failures, we have proposed "SNMP-based Burst Traffic detection method". This time, for the purpose of detection of the Data Center, was carried out the detection accuracy evaluation of the proposed method. In this paper, we will report on the results of the evaluation.

1. はじめに

東日本大震災を機に，事業継続性の観点からデータセンターやクラウドサービスの利用が増加している[1]．利用者の増加に伴い，データセンター内のネットワークやクラウドサービスを提供するネットワークにおいて，パケットロスや遅延などの通信障害が生じている．この原因の 1 つとして，クライアントからのアクセス集中などによって，瞬間的にトラフィック量が増大するバーストトラフィックが考えられている．

現状，バーストトラフィックの検知方法には，ミリ秒単位の集計による通信負荷増加や検知機器の導入によるコスト増加などの課題が存在しており，データセンター事業者や監視をサービスとして提供する事業者にとって，導入時の壁となっている．そのため，これらの課題を解決可能なバーストトラフィック検知方法が求められている．

上記課題に対して，我々は，SNMP（Sinmple Netowork Management Protocol）[2]を利用したトラップとポーリングの組合せによるバーストトラフィック検知方式を提案している[3]．提案方式は，従来の監視方法と項目を組合わせた検知方式であるため，特別な装置を導入する必要はなく，また通信負荷についても問題がないことを実機にて確認した．本稿では，提案方式のバーストトラフィックの検知精度を評価するために実施した実機検証について報告する．

†1 三菱電機株式会社 情報技術総合研究所
Information Technology R&D Center, Mitsubishi Electric Corp.
†2 三菱電機インフォメーションネットワーク株式会社
Mitsubishi Electric Information Network Corp.

2. バーストトラフィックの定義

今回，本稿で取り扱うバーストトラフィックの定義について記述する．

バーストトラフィックは，瞬間的（100ms 以上 10000ms 以下）にネットワークトラフィックが急激に増大（ネットワーク使用率の 80%以上）する現象とする．

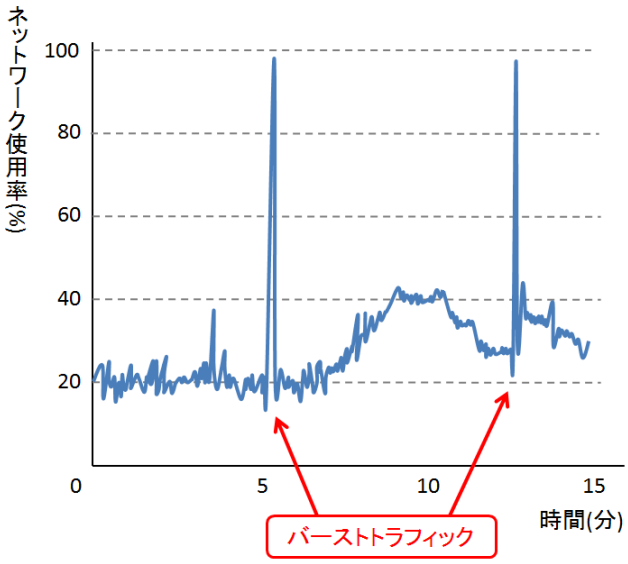

図 1　バーストトラフィック例

3. 提案のバーストトラフィック検知方式

3.1 ネットワーク監視の現状

通常，ネットワークを監視する場合，ネットワーク機器

ⓒ 2015 Information Processing Society of Japan

のカウンタや平均流量（bit/Sec）などの MIB（Management Information Base）情報から平均的なトラフィックを監視することなどが一般的である[4]．また，通常のトラフィック監視は，通信負荷を考慮して数分間隔での収集を実施している．しかし，上記の監視方法においては異常がないものの，以下のような障害情報としてユーザから報告される場合が存在する．

- TCP コネクションの失敗
- 応答時間の不安定化
- 映像・音声の途切れ

これらの現象を引き起こす要因の一つとして，バーストトラフィックが考えられている．これは，通常のトラフィック監視の場合，取得するトラフィック量が取得間隔で平準化されるため，瞬間的にトラフィックが増大するバーストトラフィックを検知できないことに起因する．

3.2 現状のバーストトラフィック検知方法とその課題

バーストトラフィックを検知するためには，計測するデータの集計をミリ秒単位で行う方法がある．しかし，ミリ秒単位の集計は，パケット収集回数が増加するため，ネットワークの通信負荷を増大する可能性が高く，現実的な方法とは言えない．

また，ネットワークの通信負荷を考慮し，ミリ秒単位での収集によるバーストトラフィック検知製品（Network Time Machine : FLUKE networks 社など）が存在する[5]．しかし，ネットワークの規模に応じて導入する検知機器の台数や機器の接続数が膨大となるため，導入にかかるコストが増加するといった課題が存在する．

3.3 提案のバーストトラフィック検知方式について

我々は，前節に記載される課題を解決するために，現行の監視方法の枠組みでバーストトラフィックを検知する方式を提案している．

提案する検知方式は，通信負荷を考慮し，SNMP による監視サーバへの通知／収集を併用して得られる以下の情報から判定する方式である．

- 1 秒平均の通信量使用率（閾値を跨ぐ場合のみ通知．表 1 の 1，2 を指す．）
- 転送可能量を超過して受信したために破棄したパケット数（一定間隔で収集．表 1 の 3 を指す．）

表 1　提案のバーストトラフィック検知方式

番号	監視方法	監視項目
1	トラップ	インタフェースで受信した総オクテット数
2		インタフェースで送信した総オクテット数
3	ポーリング	パケットロス数

ただし，我々の提案する検知方式には，以下の制約が存在する．

- ネットワーク機器で，トラップを投げるための RMON（Remote Network Monitoring）が利用可能である
- 提案する検知方式の監視項目 3 つが取得可能である
- ネットワークが自動で帯域制限などを実施しない

3.4 提案検知方式による効果

本節では，提案方式を用いることによって得られる効果の例を記述する．

仮に，現状の監視方法が 5 分間隔のポーリングによる監視方法とした場合，図 2 に示すバーストトラフィックによる通信障害を全て検知することができない．これは，3.1 節で記述した通り，取得するトラフィック量が取得間隔（この場合では 5 分）で平準化されるためである．

一方で，提案方式では，トラップによる監視方法とポーリングによる監視方法を併用した方式である．トラップでは，1 秒平均の通信量使用率が 80%以上を超えた場合に監視サーバに通知され，検知できる．ポーリングでは，現状の監視方法と同様に 5 分間隔で行い，パケットロス数を収集することで判断が可能となり，検知できる．仮に，トラップによる監視方法で，判定間隔の 1 秒間で平準化されることで検知できなかった場合においても，併用するポーリングで収集したパケットロス数によって検知することが可能である．また，逆に，ポーリングによる監視方法で，バーストトラフィックが発生しても閾値を超えず検知できなかった場合においても，併用するトラップで判定した通信量使用率によって検知することが可能である．

よって，提案方式では，各判定方法の判定結果の論理和を行うことで，図 2 に示すバーストトラフィックによる通信障害を全て検知することが可能となる（図 3 参照）．

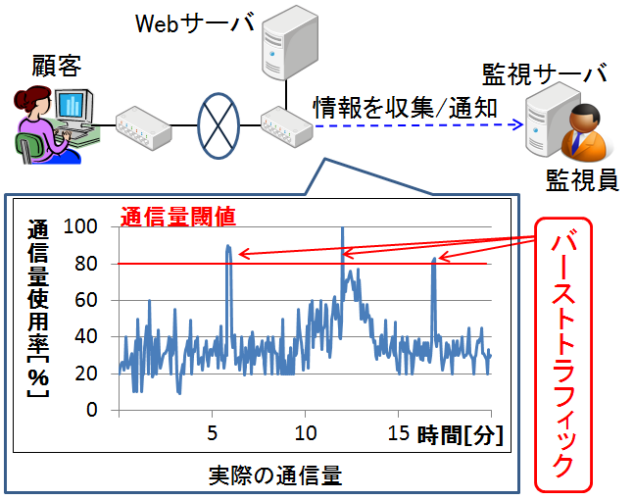

図 2　実際の通信量の例

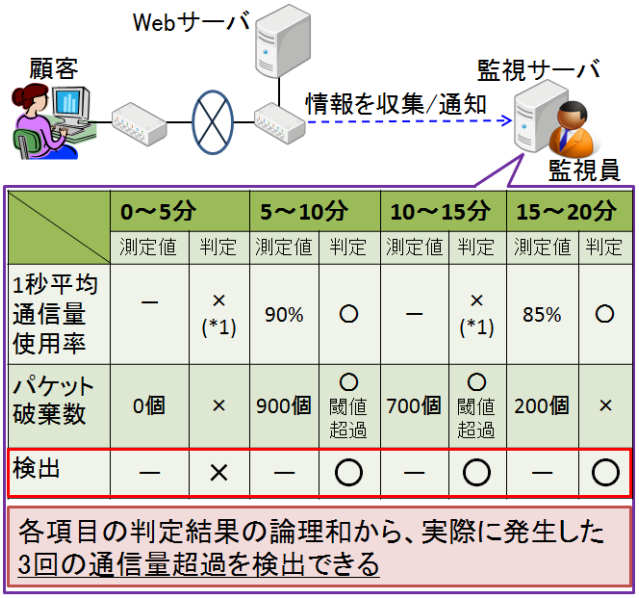

図 3　提案方式によるバーストトラフィック検知の例

4. 提案方式の検知精度の評価

提案するバーストトラフィック検知方式によって，どの程度のバーストトラフィックまでを検知することが可能であるか，また提案方式の適用による通信負荷に問題がないかを評価するため，以下について検討した．

- 評価環境（4.1 節参照）
  - 評価対象（4.1.1 項参照）
  - 評価モデル（4.1.2 項参照）
- 評価項目（4.2 節参照）

これらについては，次節以降に詳細を記述する．

4.1 評価環境

本節では，評価環境を構築するにあたって実施した，評価対象の選定，評価モデルの定義について記述する．

4.1.1 評価対象

提案するバーストトラフィック検知方式の適用先として，データセンター事業者や監視をサービスとして提供する事業者を想定している．そのため，サービス事業者の一般的なネットワーク構成をもとに評価モデルを定義する（図 4 参照）．

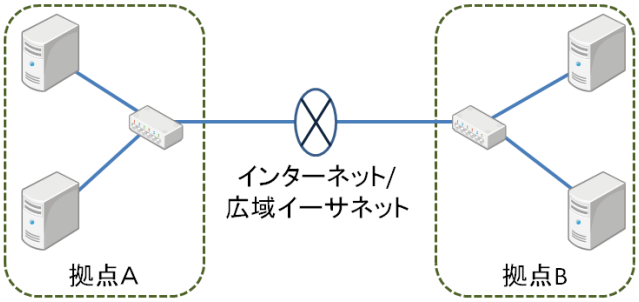

図 4　サービス事業者の一般的なネットワーク構成

4.1.2 評価モデル

定義した評価モデルは，以下の 2 つである．

- 拠点内通信（図 5 参照）
  - 拠点内で閉じたネットワークに対して，バーストトラフィックが検知可能かを評価する
  - 検証では，Cisco 社製の Catalyst シリーズのスイッチを使用する
- 拠点間通信（図 6 参照）
  - 拠点と別の拠点間のネットワークに対して，バーストトラフィックが検知可能かを評価する
  - 検証では，Cisco 社製の Cisco 892J を使用する

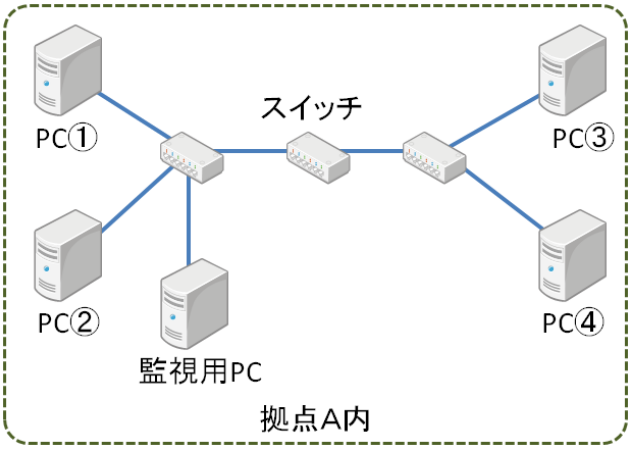

図 5　拠点内通信のネットワーク構成モデル

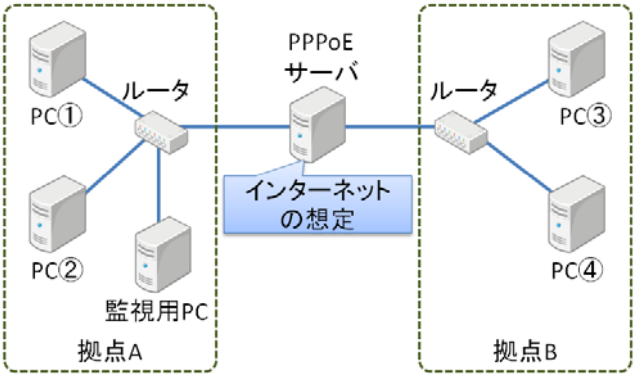

図 6　拠点間通信のネットワーク構成モデル

4.2 評価項目

各評価モデルにて，以下の項目を検証する．

(1) バーストトラフィック検知率
  - どの程度のバーストトラフィックを検知することが可能であるかを確認する

(2) トラフィック量
  - 提案方式の適用によって通信負荷に問題が無いかを確認する
  - 尚，本項目については，トラップによる通信負荷に焦点を当てて，評価を実施する

ⓒ 2015 Information Processing Society of Japan

4.3 拠点内通信における検証

本節では，拠点内通信のネットワーク構成モデルの検証方法，検証パターン，検証結果を記述する．

4.3.1 検証方法

各 PC から別の PC へデータ（定常データ，またはバーストするデータ）を送信し，監視用 PC がトラップの受信，および各ネットワーク機器からのパケットロス数を取得する（図 7 参照）．バースト検知判定基準を以下に示す．

- トラップを受信する
- パケットロス値が 100 以上

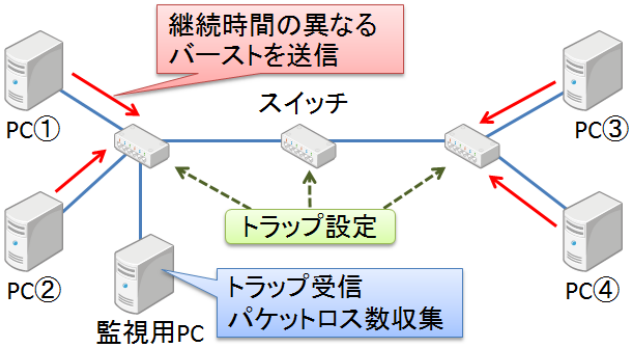

図 7　拠点内通信モデルの検証方法の説明図

4.3.2 検証パターン

検証パターンは，以下の組合せ（通信経路，通信負荷，帯域構成）で実施した．総検証パターン数は，108 パターンである（＝通信経路：6 通り＊通信負荷：6 通り＊帯域構成：3 通り）．これらの各検証パターンで，検知可能なバースト継続時間の計測を行った．

① 通信経路（表 2 参照）

重複を除外し，有効なパターンとして以下の 6 通りを対象とする．

② 通信負荷（表 3 参照）

重複を除外し，有効なパターンとして以下の 6 通りを対象とする．

③ 帯域構成（表 4 参照）

スイッチ間の帯域の組合せとして以下の 3 通りを対象とする．

表 2　拠点内通信モデルの通信経路のパターン表

パターン番号	送信先			
	PC①	PC②	PC③	PC④
1	PC②	PC①	PC④	PC③
2	PC③	PC④	PC①	PC②
3	PC②	PC④	PC④	PC②
4	PC④	PC④	PC②	PC②
5	PC④	PC④	PC④	PC②
6	PC②	PC④	PC②	PC②

表 3　拠点内通信モデルの通信負荷のパターン表

パターン番号	送信するデータ量（ネットワーク帯域使用率）				備考
	PC①	PC②	PC③	PC④	
1	20%	20%	20%	20%	定常
2	0%	0%	0%	100%	バースト
3	0%	0%	100%	100%	
4	0%	100%	0%	100%	
5	0%	100%	100%	100%	
6	100%	100%	100%	100%	

表 4　拠点内通信モデルの帯域構成のパターン表

パターン番号	帯域（アルファベットは図 8 を参照）			
	A	B	C	D
1	1Gbps	100Mbps	100Mbps	100Mbps
2	100Mbps	100Mbps	100Mbps	100Mbps
3	1Gbps	10Mbps	100Mbps	100Mbps

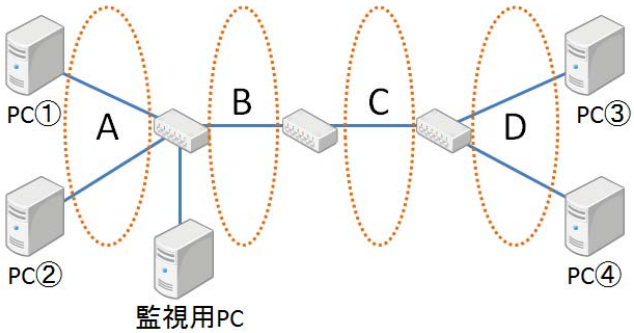

図 8　拠点内通信モデルの帯域構成の説明図

4.3.3 検証結果

拠点内通信モデルにおけるバースト検知率の結果を表 5 に示す．バーストとなるデータを送信する PC から送り先の PC までの経路上の回線のどこかで検知できたものを成功としている．

バーストとなるデータの送信継続時間が 3900ms の場合，全パターンでバーストを検知できていることが分かる．

表 5　拠点内通信モデルにおけるバースト検知率

バースト継続時間	全体	帯域パターン 1	帯域パターン 2	帯域パターン 3
100ms	49%	74%	0%	74%
300ms	53%	74%	10%	74%
500ms	68%	74%	55%	74%
700ms	74%	74%	75%	74%
900ms	78%	80%	75%	80%
3000ms	94%	93%	95%	93%
3500ms	95%	95%	95%	95%
3900ms	100%	100%	100%	100%

ⓒ 2015 Information Processing Society of Japan

4.4 拠点間通信における検証

本節では，拠点間通信のネットワーク構成モデルの検証方法，検証パターン，検証結果を記述する．

4.4.1 検証方法

各 PC から別の PC へデータ（定常データ，またはバーストするデータ）を送信し，監視用 PC がトラップの受信，および各ネットワーク機器からのパケットロス数を取得する（図 9 参照）．バースト検知判定基準を以下に示す．

- トラップを受信する
- パケットロス値が 100 以上

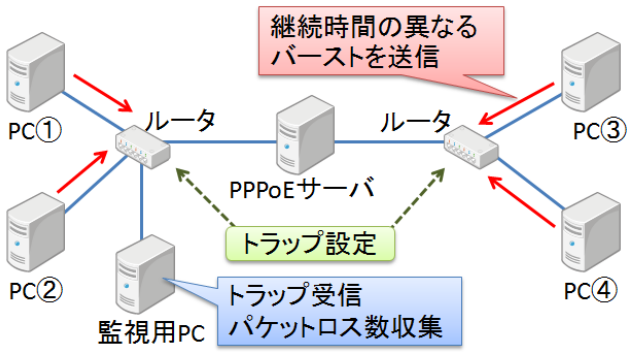

図 9　拠点間通信モデルの検証方法の説明図

4.4.2 検証パターン

検証パターンは，以下の組合せ（通信経路，通信負荷，帯域構成）で実施した．総検証パターン数は，36 パターンである（＝通信経路：2 通り＊通信負荷：6 通り＊帯域構成：3 通り）．これらの各検証パターンで，検知可能なバースト継続時間の計測を行った．

① 通信経路（表 6 参照）

重複およびインターネットを経由しないパターンを除外し，有効なパターンとして以下の 2 通りを対象とする．

② 通信負荷（表 7 参照）

重複を除外し，有効なパターンとして以下の 6 通りを対象とする．

帯域構成（

③ 表 8 参照）

ルータ間の帯域の組合せとして以下の 3 通りを対象とする．

表 6　拠点間通信モデルの通信経路のパターン表

パターン番号	送信先			
	PC①	PC②	PC③	PC④
1	PC③	PC④	PC①	PC②
2	PC④	PC④	PC②	PC②

表 7　拠点間通信モデルの通信負荷のパターン表

パター	送信するデータ量				備考
ン番号	（ネットワーク帯域使用率）				
	PC①	PC②	PC③	PC④	
1	20%	20%	20%	20%	定常
2	0%	0%	0%	100%	バースト
3	0%	0%	100%	100%	
4	0%	100%	0%	100%	
5	0%	100%	100%	100%	
6	100%	100%	100%	100%	

表 8　拠点間通信モデルの帯域構成のパターン表

パターン番号	帯域（アルファベットは図 10 を参照）			
	A	B	C	D
1	1Gbps	100Mbps	100Mbps	100Mbps
2	100Mbps	100Mbps	100Mbps	100Mbps
3	1Gbps	10Mbps	100Mbps	100Mbps

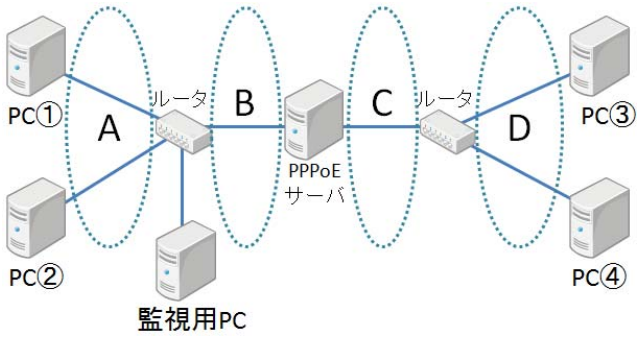

図 10　拠点間通信モデルの帯域構成の説明図

4.4.3 検証結果

拠点間通信モデルにおけるバースト検知率の結果を表 9 に示す．バーストとなるデータを送信する PC から送り先の PC までの経路上の回線のどこかで検知できたものを成功としている．

バーストとなるデータの送信継続時間が 3500ms と 3900ms の場合，全パターンでバーストを検知できていることが分かる．

表 9　拠点間通信モデルにおけるバースト検知率

バースト継続時間	全体	帯域パターン 1	帯域パターン 2	帯域パターン 3
100ms	67%	100%	0%	100%
300ms	67%	100%	0%	100%
500ms	67%	100%	0%	100%
700ms	67%	100%	0%	100%
900ms	67%	100%	0%	100%
3000ms	77%	100%	33%	100%
3500ms	100%	100%	100%	100%
3900ms	100%	100%	100%	100%

ⓒ 2015 Information Processing Society of Japan

4.5 総合評価

本節にて，検証結果の総評について記述する．

(1) バーストトラフィック検知率

- 拠点内通信モデル，拠点間通信モデルともに，約 4 秒程度継続するバーストトラフィックは，100%の検知が可能である
- 機器毎にトラップのバースト判定時間が異なるため，機器によって検知できるものとできないものが存在するため，本方式適用時にトラップの判定時間の設定を検討する必要がある

(2) トラフィック量

- 監視サーバが受信したトラップ数は，平均 6.1 個であり，1 つ当たりのトラップのデータ量は約 187byte であり，回線上を流れたトラップの総データ量は平均 1140byte となる
- 想定する適用対象帯域は 10Mbps～1Gbps であるため，上記データ量は十分小さい値となる
- また，トラップは UDP パケットのため，ロスしても再送制御がなく，通信データ量が増加することはない
- 以上を踏まえ，従来の回線で本検知方式を使用することは問題ないと判断する

よって，本検知方式は，従来の監視方法では検知できないバーストトラフィックに対し，本稿で定義した 10 秒以内バーストトラフィック（2 章参照）の定義内に十分収まる約 4 秒程度のバーストトラフィックが検知可能であるため，バーストトラフィックの検知方式として有効であると判断できる．また，通信負荷についても従来の回線での使用に問題がないため，提案方式が適用可能であると判断できる．

5. おわりに

我々は，バーストトラフィック検知方法の課題である通信負荷増加や検知機器導入によるコスト増加等の課題に対して，SNMP を利用したトラップとポーリングの組合せによるバーストトラフィック検知方式を提案し，提案の検知方式における検知精度の評価を実施した．

評価の結果，拠点内および拠点間のネットワーク構成をモデル化した環境において，現状の監視では検知できないバーストトラフィックの検知が可能であることを確認できたため，提案方式はバーストトラフィック検知方式として有効なものと言える．また，通信負荷についても従来の回線での使用に問題がないことが確認できたため，適用についても問題がないと言える．

今後は，提案方式を無線接続に対して適用ができないかを検討していくとともに，提案方式の本番環境への適用について検討（トラップ判定の設定基準など）を行っていく予定である．

参考文献

1) 富士キメラ総研：データセンタービジネス市場調査総覧 2014 年版（上巻，下巻），2014-02-21
2) 斗光佳輝：Windows ネットワークスキルアップテキスト―ネットワーク構築と管理の基礎を学ぶ (NE サポートシリーズ)，CQ 出版，2003-09-01
3) 村井秀聡 他：SNMP を利用したバーストトラフィック検知方式の提案，FIT2014 第 13 回情報科学技術フォーラム，運用管理とセキュリティ
4) 水越一貴 他：通信トラフィック監視システムの試作とバーストトラフィックの検出，情報処理学会研究報告．DSM，[分散システム/インターネット運用技術] 2004(77)，31-36，2004-07-30
5) Network Time Machine，FLUKE networks，http://jp.flukenetworks.com/enterprise-network/network-monitoring/Network-Time-Machine

ⓒ 2015 Information Processing Society of Japan