L-019

SNMP を利用したバーストトラフィック検知方式の提案

A proposal of SNMP based Burst Traffic detection method

村井 秀聡† 砂田 英之† 牧 和宏‡
Shuto Murai Hideyuki Sunada Kazuhiro Maki

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，クライアントからのアクセスが集中することで，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発生し，パケットロスや遅延などの通信障害に似た現象が引き起こすといった問題が生じている．そのため，バーストトラフィックを検知することが可能な監視を実施する必要がある．

バーストトラフィックは，一定周期の収集による平均的なトラフィック監視では検知できず，トラフィックをミリ秒単位等の細かい集計によって検知することが可能である．しかし，細かい集計は通信負荷の増加を引き起こすため，現実的な方法とは言えない．また，通信負荷を考慮したミリ秒単位でトラフィックを収集する製品も存在するが，大規模なネットワークでは導入すべき機器数が増加し，コストが高くなるといった課題が存在する．

そこで，我々はこれらの課題を解決すべく，「現行の監視の枠組みでバーストトラフィックを検知する方式」を提案する．本稿では， SNMP を利用したバーストトラフィック検知方式及び実機評価について報告する．

2. 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，ネットワーク機器のカウンタや平均流量(bit/Sec)などの MIB を参照した平均的なトラフィックを監視することが一般的である[1]．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. バーストトラフィックについて

3.1. 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載する．

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．

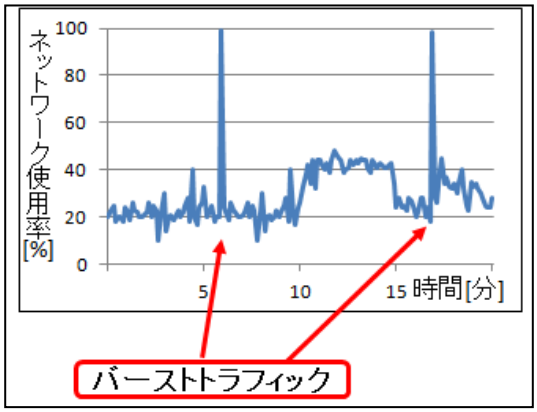

図 1 バーストトラフィック例

3.2. バーストトラフィックの検知方法と課題

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)等が存在する[3]．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接続数が膨大となり，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．

4. 検知方式の提案

本稿では，上記課題解決のため，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する．

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 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

† 三菱電機株式会社 情報技術総合研究所
‡ 三菱電機情報ネットワーク株式会社

5. 提案方式の導出過程

4章で提案したバーストトラフィック検知方式は，以下の手順を実施し，導出した．

- 現行の監視方法と監視項目を調査し，バーストトラフィックを検知可能と思われる監視方法と監視項目の組合せを抽出(6章)
- 抽出した組合せを実機検証し，検知方式を導出(7章)

6. 監視方法／項目の組合せ候補の抽出

表 2は，バーストトラフィックを検知可能と思われる監視方法と監視項目の組合せ候補の一覧である．これらは，以下の事象が起こることを想定して抽出した．

- 大量のトラフィック量が流れる(表 2の番号 1，2)
- トラフィックを処理しきれず，パケットがロスされる，または滞留する(表 2の番号 3，6，7)
- 大量のトラフィックを処理するためにリソースを消費する(表 2の番号 4，5)

監視方法については，SNMP(Simple Network Management Protocol)[4]におけるポーリングによる状態収集とトラップによる状態収集を対象とした．また監視項目については，標準 MIB (Management Information Base)の MIB-2 と拡張 MIB(今回は，Cisco の Catalyst スイッチでサポートされる MIB グループ)を対象とした．

表 2 監視方法・項目の組合せ候補

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		出力キューに滞留する送信待ちパケット数
4		CPU 使用率
5		メモリ使用率
6	ポーリング	パケットロス数
7		エラーのために廃棄されたパケット数

7. 実機検証

抽出した組合せ候補に対して，以下の項目を実機にて検証し，バーストトラフィック検知方式を導出する．

- 監視項目の挙動確認(7.2章)
- 監視方法の利用確認(7.3章)
- 負荷確認(7.4章)

尚，以下のスイッチとルータを用いて検証を行った．

- スイッチ：Catalyst 2960，3550，3750(Cisco)の 3 台
- ルータ：Cisco 892J(Cisco)，RTX810(YAMAHA)の 2 台

7.1. 検証環境

データを送信する PC と受信する PC 間にネットワーク機器を接続し，ネットワーク機器を監視する PC を配備した環境を構築した(図 2参照).

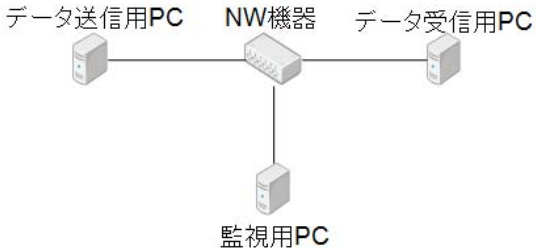

図 2 検証環境

7.2. 監視項目の挙動確認

表 2に示す監視項目がバーストトラフィック発生時に，値が変化することを確認し，監視項目の妥当性を検証する．また，値が変化する場合の更新頻度も確認する．

7.2.1. 検証項目

監視項目の挙動確認における検証項目を以下に示す．

- バーストトラフィックと監視項目候補の相関
- 監視項目の更新頻度

7.2.2. 検証方法

図 2に示すデータ送信用 PC からデータ受信用 PC にデータを送信し，監視用 PC が NW 機器から監視項目の値を取得する．送信するデータは，以下の 4 パターンを実施し，監視項目の値を取得する．また，監視用 PC がネットワーク機器から値を取得する頻度は 1 秒間隔とする．

≪送信するデータのパターン≫

- バーストトラフィックが発生しないデータ量
- バーストトラフィックが 100ms 継続するデータ量
- バーストトラフィックが 500ms 継続するデータ量
- バーストトラフィックが 900ms 継続するデータ量

7.2.3. 検証結果

バーストトラフィックと監視項目候補の相関，監視項目の更新頻度の結果をそれぞれ表 3，表 4に示す．

表 3から，全ての対象機器において，インタフェースで受信した総オクテット数，インタフェースで送信した総オクテット数，パケットロス数がバーストトラフィックと相関があり，検知に利用可能であると判断する．

監視項目の更新頻度間隔については，スイッチやルータ毎に異なるため，トラップ設定を行う場合は，機器毎に設定値を変更する必要があることが確認できた．

表 3 監視項目の相関確認結果

表 2 番号	挙動結果		
	スイッチ	Cisco ルータ	YAMAHA ルータ
1	○	○	○(LAN と WAN ポート間)
2	○	○	○
3	×	×	×
4	×	×	×
5	×	×	×
6	○	○(WAN ポート)	○
7	×	×	×

表 4　監視項目値の更新頻度結果

機器	更新頻度結果
スイッチ	1 秒更新
Cisco ルータ	LAN ポート：10 秒更新 WAN ポート：5 秒更新
YAMAHA ルータ	10 秒更新

7.3. 監視方法の利用確認

抽出した監視項目に対するトラップが可能であるか，及びトラップの判定間隔を確認し，トラップによるバーストトラフィック検知方式の妥当性を検証する．

ポーリングについては，一般的に使用される監視方法であるため，検証対象外とする．

7.3.1. 検証項目

監視方法の利用確認における検証項目を以下に示す．

- トラップの利用可否
- トラップの判定間隔

7.3.2. 検証方法

ネットワーク機器にトラップ設定(閾値と送信先の設定)を行い，閾値を越える通信量となるバーストトラフィックを送信する．その際，ネットワーク機器から監視用 PC にトラップが送信されるかを確認する．

7.3.3. 検証結果

各機器ごとのトラップの利用可否とトラップの判定間隔の検証結果を表 5に示す．

スイッチの Catalyst 2960，Catalyst 3550 では 1 秒間隔でトラップ判定が行われるため，トラップ設定の閾値は 1 秒間の最大通信量を考慮して設定する必要があることが分かった．また同様に，Catalyst 3750，Cisco ルータの WAN ポートでは 5 秒，Cisco ルータの LAN ポート，YAMAHA ルータでは 10 秒間の最大通信量を考慮して設定する必要がある．

また，YAMAHA ルータでは，RMON が利用不可であり，YAMAHA ルータの拡張 MIB を利用してトラップを送信する必要があることが分かった．これらの拡張 MIB は，PP インタフェースの回線使用率となっており，PPPoE 接続を行う通信のみバースト判定が可能という制限がつく．

表 5　監視方法の利用確認結果

機器	スイッチ	Cisco ルータ	YAMAHA ルータ
トラップ利用可否	○	○	○
トラップ判定間隔	1 秒 または 5 秒	5 秒(WAN ポート), 10 秒(LAN ポート)	10 秒
備考	RMON	RMON	拡張 MIB

7.4. 負荷確認

トラップを利用した監視方法を用いた場合の通信負荷に問題がないかを検証する．一方のポーリングを利用した監視方法は一般的に使用される 5 分間隔で行うため，通信負荷に問題はないとし，検証対象外とする．

7.4.1. 検証項目

負荷確認における検証項目を以下に示す．各項目において，トラップ未設定時とトラップ設定時の値を比較することで検証する．

- トラップを利用した監視によるネットワーク機器への影響，通信への影響
  - CPU 使用率
  - パケットロス
  - 遅延

7.4.2. 検証方法

データ送信用 PC からデータ受信用 PC にデータを送信し，データ送信用 PC でデータ送信時間とデータ送信量，データ受信用 PC でデータ受信時間とデータ受信量を記録する．記録からパケットロス数や到達に掛かる時間を計測する．また，監視用 PC からネットワーク機器の CPU 使用率を取得する．

送信するデータは，以下の 3 パターンを実施する．各パターンごとに，NW 機器への設定を「トラップ設定あり」と「トラップ設定なし」の 2 パターンに設定し，検証する．

≪送信するデータ≫

- バーストトラフィックが発生しないデータ量
- バーストトラフィックが 100ms 継続するデータ量
- バーストトラフィックが 900ms 継続するデータ量

7.4.3. 検証結果

CPU 使用率，パケットロス，遅延に対する検証結果をそれぞれ表 6，表 7，表 8に示す．パケットロスは，ロスしたパケット数の平均値で比較し，遅延についてはパケット到達時間で比較する．

トラップ設定時の CPU 使用率は，未設定時と比較した結果，最大 1%増加となっているため，トラップ設定を行っても問題ないことが確認できた．

パケットロス数は，全てのパターンでトラップ設定による大きな差はなく，トラップ設定を行っても問題ないことが確認できた．

パケット到達時間(遅延)は，未設定時と比較した結果，未設定時の値に対し 3ms 増加，2ms 減少となっているため，トラップ設定を行っても問題ないことが確認できた．

以上から，トラップ設定を行った場合において，ネットワーク機器や通信に与える影響は実用に耐えうると判断した．

表 6　CPU 使用率の計測結果(単位：%)

パターン	定常通信		バースト 100ms		バースト 900ms	
設定の有無	無	有	無	有	無	有
Catalyst 2960	4	4	4	4	4	4
Catalyst 3550	0	0	0	0	0	0
Catalyst 3750	6	7	6	7	6	6
Cisco 892J	4	4	4	3	9	9
RTX810	14	15	14	14	16	16

表 7　パケットロス数の計測結果(単位：個数)

パターン	定常通信		バースト100ms		バースト900ms	
設定の有無	無	有	無	有	無	有
Catalyst 2960	0	0	4	1	438	455
Catalyst 3550	0	0	27	21	441	476
Catalyst 3750	0	0	7	7	441	409
Cisco 892J	0	0	1	1	532	574
RTX810	0	0	50	51	648	650

表 8　パケット到達時間の計測結果(単位：ms)

パターン	定常通信		バースト100ms		バースト900ms	
設定の有無	無	有	無	有	無	有
Catalyst 2960	10	10	8	8	5	5
Catalyst 3550	10	13	10	9	4	2
Catalyst 3750	9	10	10	13	12	14
Cisco 892J	7	7	11	9	8	8
RTX810	14	16	9	9	6	6

7.5. 総合結果

以上の結果から，4章に示す検知方式が通信負荷を考慮し，バーストトラフィックを検知可能であることを確認した．

ただし，提案方式には以下の制約が存在する．

- トラップを投げるための RMON が利用可能である
- 受信オクテット数，送信オクテット数，パケットロス数の情報が取得可能である
- 帯域が確定する有線接続に対して有効である

8. 提案方式による効果の例

本章では，提案方式による効果について説明する．

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 3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，2章で記載した通り，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．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 3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 4参照)．

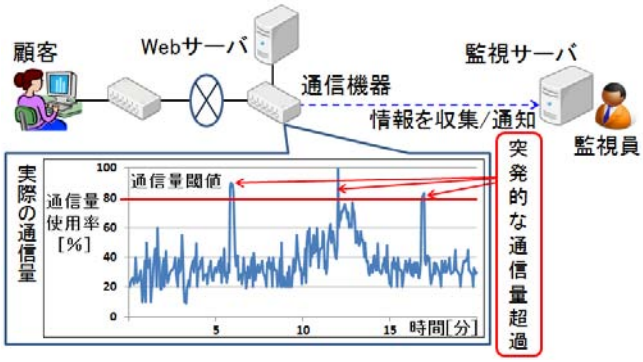

図 3　実際の通信量の例

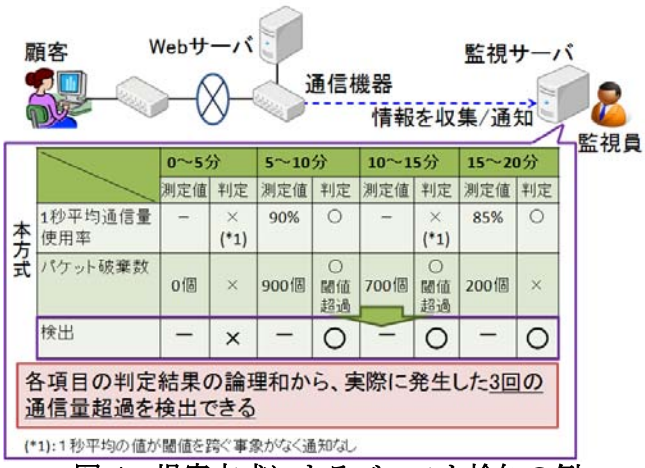

図 4　提案方式によるバースト検知の例

9.　結論

今回，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た．

本方式は，従来の監視方法と項目を組合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い．また，実機検証にて通信やネットワークへの影響が現状とほぼ変わらないことを確認しており，本方式適用における通信負荷は問題ないと考える．

今後は，本方式を実システムへの適用に向けて，実システム環境におけるバーストトラフィックの検知率の評価等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] 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

[3] Network Time Machine ， FLUKE networks ， http://jp.flukenetworks.com/enterprise-network/network-monitoring/Network-Time-Machine

[4] 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