トラフィック監視・分析ソフトウェア PureFlow Profiler の開発

佐藤敬幸　Takayuki Sato，安齋賢二　Kenji Anzai，脇田智大　Tomohiro Wakita，明戸正人　Masato Aketo

［要　旨］　近年，クラウドサービスの利用拡大やテレワークの普及により，ネットワークのトラフィックが急増している。また，ネットワーク環境は複雑化し，障害発生時の切り分けが困難となっている。ひとたびネットワークに障害が発生すると，業務の生産性を著しく低下させるため，いかにして通信品質を維持するかが企業の課題である。この課題を解決するため，トラフィック状況を可視化し，障害の早期発見と復旧をサポートするソフトウェア「PureFlow Profiler」を開発した。本稿では，PureFlow Profiler の機能と特長を紹介する。

1　まえがき

企業の基幹システムは，従来のオンプレミスからクラウドへの移行に伴い，オンプレミスとクラウドのサーバが混在するようになり，システム構成は複雑化してきている。また，テレワークやオンライン会議などの普及に伴い，ネットワークに依存する業務が増加しているため，ネットワークがつながらない，サーバが遅くなったなどの障害が発生すると，業務に多大な影響を及ぼす。これらの障害の原因はさまざまであるが，代表的な要因を以下に示す。

（1）　回線輻輳による障害

大量のトラフィックがネットワーク上の一部に集中すると，通信回線で輻輳が発生する。このとき，通信は不安定になり，クライアントとサーバ間の遅延やパケットロス・再送の要因となる。また，トラフィックの集中が一時的に発生したものであれば，時間の経過とともに元の状態に戻るため，障害発生時の原因を特定することは極めて困難である。

（2）　機器の故障や老朽化による障害

スイッチやルータなどのネットワーク機器や，サーバが故障すると通信が切断され，ネットワークサービスの停止につながる。また，機器の故障まで至らなくても老朽化により，通信が不安定になることがある。

このような障害原因や障害箇所を特定するためには，ネットワークの通信状況を可視化する必要がある。24 時間 365 日稼働しているシステムを効率的に監視・分析し，障害発生時には迅速に対応することで，被害を最小限に抑えることが求められている。

こうした背景のもと，ネットワークのトラフィックを監視・分析するためのソフトウェア PureFlow Profiler（以下 PFP）を開発した。

2　開発方針

PFP は，サーバソフトウェアとクライアントソフトウェアで構成する（**図 1**）。サーバソフトウェアは，ネットワーク内に設置される帯域制御装置（以下 PureFlow ノード）から統計情報を収集し，最大 255 ノード分をデータベースに一元管理する。クライアントソフトウェアはサーバソフトウェアに接続し，データベースの情報を可視化する。

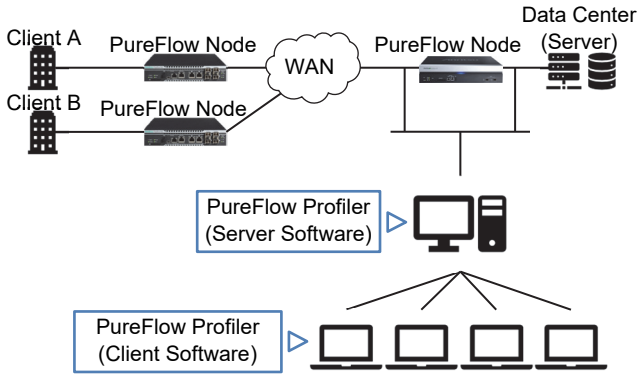

図 1　システム構成

PFP を用いることで，複数のクライアントやサーバを個別に監視するよりも，ネットワーク内の複数 PureFlow ノードを同時に監視することで，システム全体のトラフィック状況を効率的に監視・分析できる。PFP は，障害検知から障害箇所の特定による早期復旧までをサポートすることを目的に設計しており，以下の点に留意した。

2.1　リアルタイムデータの可視化・分析

障害が発生した際，システム管理者が早急に障害原因や障害箇所を特定するため，PFP は PureFlow ノードの統計情報をリアルタイムに収集する。ネットワークの通信状況を的確に把握するために，トラフィック量だけでなく，遅延やパケットロス等の変化もリアルタイムに可視化・分析できるよう留意した。

2.2　長期間蓄積した過去データの可視化・分析

障害が発生した際，正常時と異常時のトラフィック状況を比較す

るため，長期間の統計情報を蓄積できるよう留意した。時系列データを長期間蓄積することで，日／週／月／年単位のトラフィック状況の変化を可視化・分析可能とした。

2.3　容易なグラフ表示操作

過去と現在のトラフィック状況を比較する際，グラフの表示範囲を容易に指定できるよう留意した。具体的には，昨日（前日 0:00 から 23:59 まで）と今日（当日 0:00 から現在時刻まで）など，障害分析に有効な範囲をワンクリックでグラフ表示可能とした。

2.4　迅速な障害通知

常時監視・分析することにより，障害を検知した場合，システム管理者に対して速やかに通知できるよう留意した。通知には，発生時刻，発生箇所，障害状況などの情報を含め，ネットワーク管理プロトコルとして一般的な SNMP(Simple Network Management Protocol)と SYSLOG(System Logging Protocol)の 2 種類をサポートした。

3　基本機能

PFP は，トラフィック量やフロー（PureFlow ノードで識別できるトラフィックの最小単位）数に加え，RTT(Round Trip Time)やパケットロス率など，通信品質を表す測定項目を長期間に渡って収集する。通信品質の変化を分析することで回線帯域や帯域制御ポリシーの見直しだけでなく，障害の早期発見や予兆検知などにも利用可能とするため，以下の基本機能を備える。PFP の主要諸元は**表 5** に示す。

3.1　トラフィック監視

（1）　トラフィック量の可視化

PFP では，ネットワーク上の平均送信トラフィック量(**図 2**)とピークレート(**図 3**)を可視化することで，回線帯域に対する通信量の大きさを監視・分析できる。平均送信トラフィック量は，トラフィック種別ごとにトラフィック量を色分けし，積み上げることによって特定のトラフィック種別が占める割合と総トラフィックの変化を視覚的に分かるように表示している。ピークレートは，1 秒間隔で送信トラフィック量を測定した際の 1 分間（60 回分）での最大値を表示している。平均送信トラフィック量と比較したときに，この差分が大きければ，ネットワークリソースに余裕があり，逆に差分がほとんどない場合は，ネットワークに逼迫するようなトラフィックが流れ続けていると分析できる。

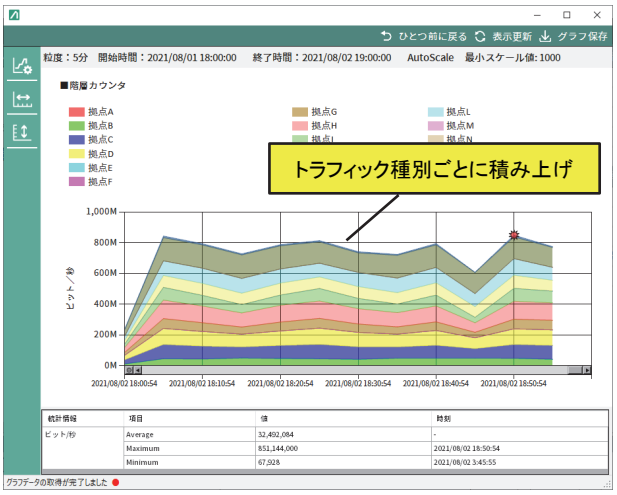

図 2　平均送信トラフィック量グラフ

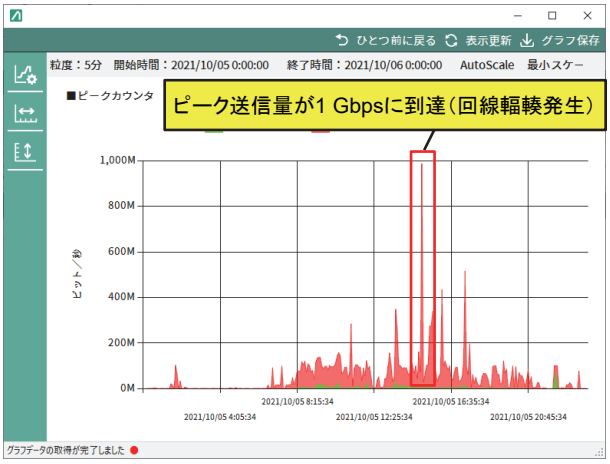

図 3　ピークレートグラフ

また，フロー数グラフにより，ユーザ通信数が集中している時間帯を把握し，性能限界の予測や設備更新の必要性確認に活用できる(**図 4**)。さらに，グラフ表示範囲内の最大値／最小値の日時を簡単に把握できるよう，統計情報を表示し，グラフ上にもマーキングするようにした。

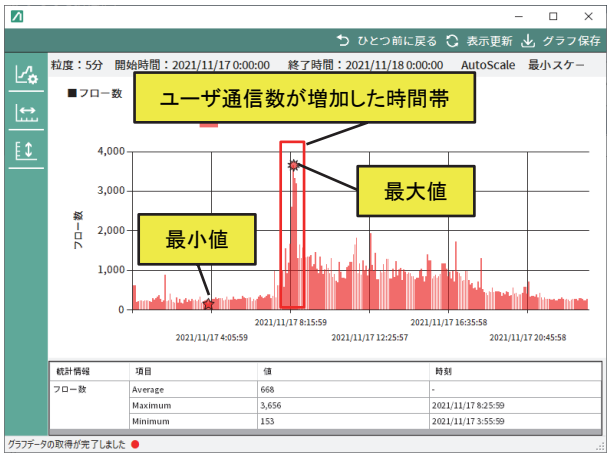

図 4　フロー数グラフ

(2)　トラフィック量上位ユーザの可視化

ネットワークでは，極めて少数のユーザがネットワークリソースを占有し，他の多くのユーザへのサービス品質を低下させる場合がある。このような問題を引き起こす可能性がある通信を特定できるよう，PFP はトラフィック量が多い順に，上位のユーザを可視化できる。PureFlow ノードを通過する全トラフィックの中から，IP アドレスやアプリケーションポート番号ごとに送信トラフィック量が多い上位 25 位までの情報をトップ情報と呼ぶ。PFP ではトップ情報を可視化することで，トラフィックの利用状況を把握できる。**図 5** に示すように上位 2 ユーザが通信回線の約 73%を占有している場合，帯域制御により通信量の制限を設けてネットワークを最適化する必要がある。

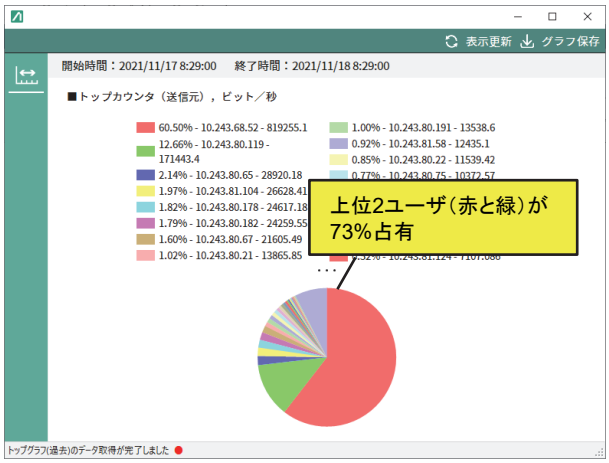

図 5　トップグラフ

3.2　トラフィック分析

PFP には，PureFlow ノードが測定した遅延やパケットロス・再送の情報（**図 6**）を収集し，ネットワークやサーバのパフォーマンス状況を把握するためのトラフィック分析情報を可視化する機能を実装した。

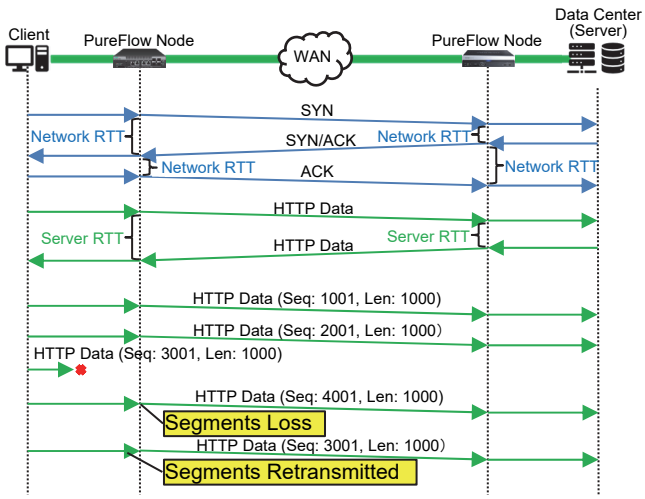

図 6　トラフィック分析の測定ポイント

(1)　TCP 遅延の可視化

障害原因がネットワークとサーバのどちらにあるのかを切り分けるため，ネットワーク遅延（以下 Network RTT）とサーバ遅延（以下 Server RTT）の 2 種類を可視化する。Network RTT はアプリケーションを介さないネットワーク自体の往復遅延を示し，Server RTT はアプリケーションの起動時間を示す。Network RTT は，クライアントが送信した TCP の接続要求パケット（SYN パケット）を転送してから，対向側のサーバが送信した応答パケット（ACK パケットまたは RST パケット）を転送するまでの時間である。一方，Server RTT は，クライアントが送信した最初のデータパケットを転送してから，対向側のサーバが送信したデータパケットを転送するまでの時間である。

PFP では，この Network RTT と Server RTT のグラフや分布図（ヒストグラム）を表示し，特異な RTT の存在やバラツキの傾向を把握できる。

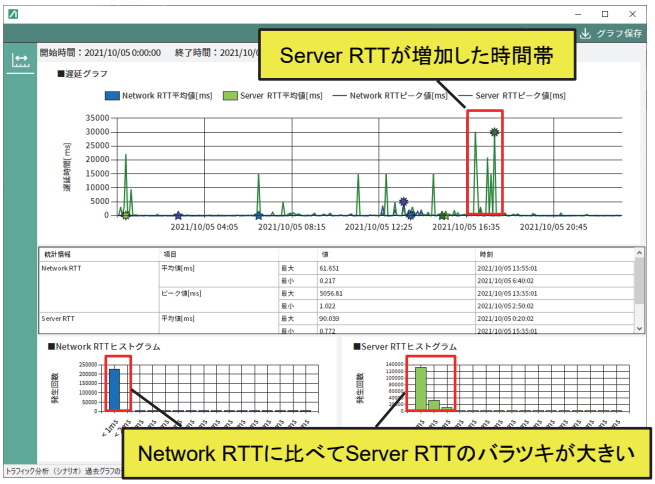

図 7　遅延グラフ

この遅延グラフより，通信品質の劣化の原因がネットワークにあるのか，サーバにあるのかを判別し，通信回線やサーバ機器の見直しなど，原因にあわせた対策が可能となる。また，ヒストグラムを分析することでネットワークやサーバのいつもと違う挙動を把握し，障害発生の予兆を確認できる。

(2)　TCP パケットロス・再送の可視化

通信品質状況を確認可能とするため，TCP プロトコルのシーケンス番号をパケットごとに参照し，パケットロスと再送のバイト数と発生回数を可視化する。TCP ヘッダのシーケンス番号が次に受信すべきシーケンス番号よりも大きいときにパケットロスと判定し，シーケンス番号よりも小さいときに再送と判定する。

PFP では，このパケットロスと再送の情報から，パケットロス率と再送率を算出し，グラフを表示する。

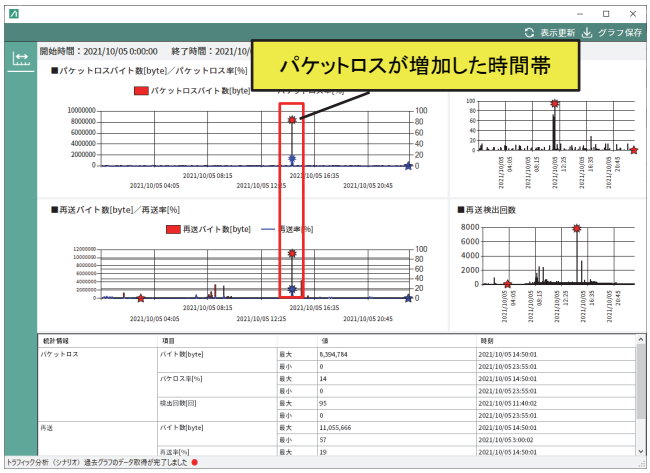

図 8　パケットロス・再送グラフ

このパケットロス・再送グラフより，通信品質の劣化している時間帯を把握できる。また，パケットロス率や再送率を PureFlow ノードごとに比較することで，どの区間でパケットロスや再送が多発しているのか特定できる。

3.3　アラーム通知

常時監視・分析することにより，あらかじめ設定した閾値（上限値・下限値）と連続検知回数を上回った，あるいは下回った際に閾値超え検知イベントとして通知できる。通知できるイベントとして「SNMP Trap 送信」，「Syslog 送信」の 2 種類を実装した。PFP で閾値設定可能な情報を**表 1** に示す。

表 1　閾値設定

閾値設定	上限値	下限値	連続検知回数
送信トラフィック量[bps]	○	○	○
フロー数[flows]	○	○	○
ネットワーク遅延[ms]	○	—	○
サーバ遅延[ms]	○	—	○
パケットロス率[%]	○	—	○

このアラーム通知機能により，送信トラフィック量やフロー数などの過多／過少を PFP で検知し，「ネットワーク異常」を瞬時に把握できる。

4　特長

4.1　総合的な情報の可視化

個別のグラフ表示だけでは，障害原因を分析するのに手間がかかる。システム管理者がネットワークやサーバの動作状況を総合的に分析可能とするため，同一時間帯の各種情報の相互関係を容易に把握できるよう，一括でグラフ表示・レポート出力可能とした（**図 9**）。

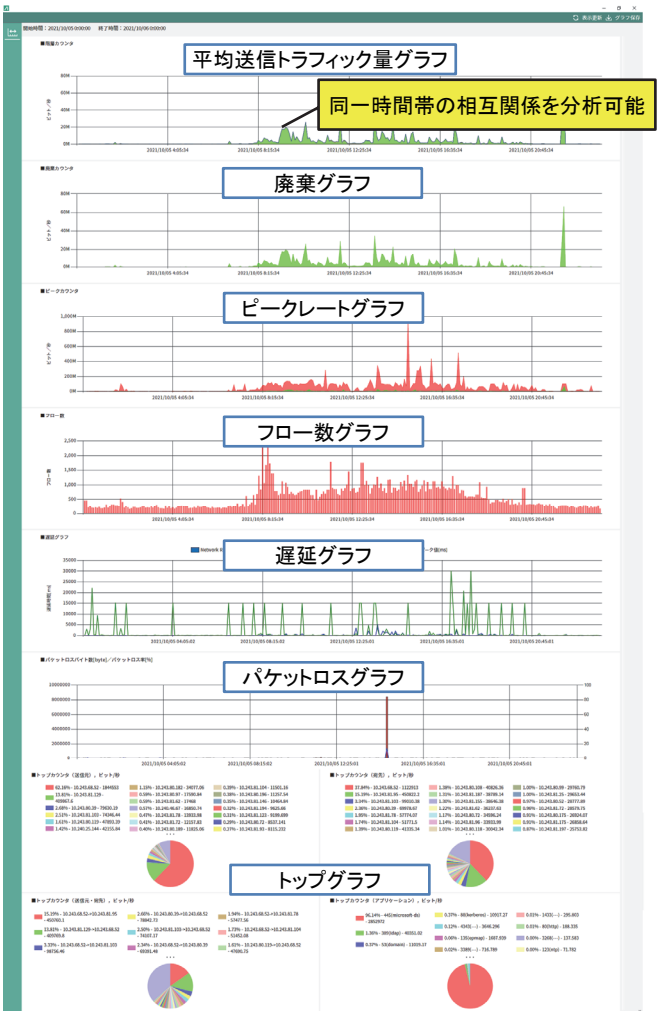

図 9　総合情報グラフ

総合情報グラフの種別を**表 2** に示す。

表 2　総合情報グラフの種別

情報種別	グラフ種別
モニタ情報	平均送信トラフィック量グラフ，廃棄グラフ，ピークレートグラフ，フロー数グラフ
トップ情報	トップグラフ
トラフィック分析情報	遅延グラフ，パケットロスグラフ

総合情報グラフを分析することで，回線輻輳状況，ユーザ利用状況による遅延やパケットロス発生などの相関関係を判別し，通信品質の劣化に関する障害原因を判断できる。例えば，通信速度が遅い時間帯やサーバ接続できない時間帯で，モニタ情報とトラフィック分析情報を比較する。このとき，パケットロスや再送が多く発生している時間帯に回線帯域が占有されていないかなどの障害原因となり得る情報を追究し，その原因に対する適切な対策の意思決定をサポートする。さらに，トップ情報を合わせて確認することで，回線帯域を占有しているユーザを把握でき，帯域制御ポリシーの見直しなどの対策につなげることもできる。

4.2　区間 RTT によるボトルネックの可視化

障害箇所を特定するためには，システム全体のボトルネック箇所を把握する必要がある。各 PureFlow ノードが測定した情報は，各測定ポイントでの分析は可能だが，システム全体でどの区間がボトルネックかを分析することができない。そのため，PFP では，各測定ポイントの RTT のうち，同一フロー（上りフローと下りフロー）の情報をデータベース内から抽出し，隣接する PureFlow ノードから収集した RTT の差分を区間 RTT として算出することでラダー図表示を実現した（**図 10**）。各区間 RTT の最大値を赤字で表示することで，どの区間で大きな遅延が発生しているのかを直感的に判別できる。

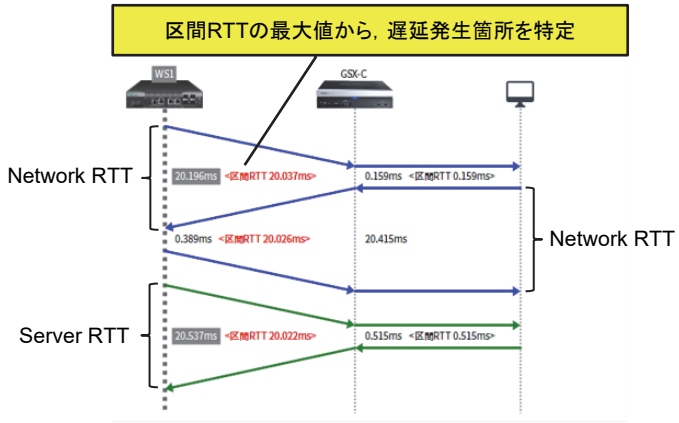

図 10　ラダー図

4.3　アクティブ測定

ネットワーク測定の手法は，パッシブ測定とアクティブ測定に大別される。パッシブ測定は，クライアントとサーバ間でネットワーク上を通過しているパケットを測定する手法である。一方，アクティブ測定は測定対象の機器に対して，自発的にパケットを送出して測定する手法である。

クライアントからサーバへの通信要求が発生しない場合でも，システムを定常監視・分析するためには，アクティブ測定が必要となるため，PureFlow ノードから任意のサーバに対して周期的に RTT やパケットロス・再送を測定するためのパケットを送信可能とした。アクティブ測定は，任意のサーバに対し，1 分周期に HTTPS (Hypertext Transfer Protocol Secure)または ICMP(Internet Control Message Protocol)トラフィックを生成し，トラフィック分析の測定対象とする。ICMP トラフィックを生成する例を**図 11** に示す。ICMP トラフィックでは，ICMP Echo Request を送信してから，対向側の端末が送信した ICMP Echo Reply を受信するまでの時間を Network RTT として可視化する。

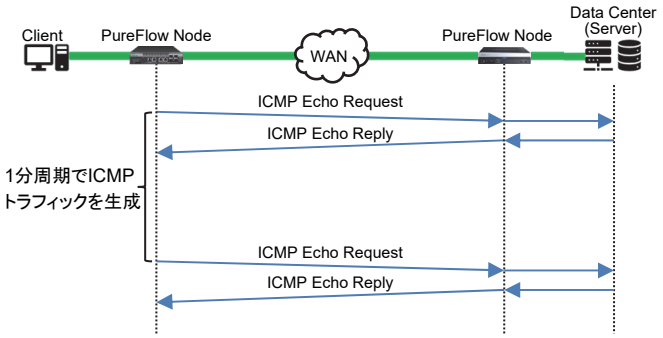

図 11　アクティブ測定（ICMP トラフィック）

4.4　グラフ表示の高速化

ネットワークやサーバの動作状況を確認する際，短期間でのリアルタイム分析から，長期間での過去分析が可能であるが，年単位などの長期間のグラフを表示する際，グラフ表示範囲内のデータをすべて抽出するとグラフの描写に時間がかかる。そのため，グラフの表示範囲に応じて，利用するデータの粒度を選択することでグラフを表示するまでの処理時間を高速化した（**表 3**）。

PFP は PureFlow ノードから収集データを「収集周期によるリアルタイムデータ」として収集するが，収集したデータから 5 分，1 時間，3 時間，1 日の異なる粒度にサンプリングすることで，最適な粒度でデータベースを作成するようにした。当該期間のデータベースをすべて抽出し，モニタ情報の送信トラフィック量では平均値，フロー数では最大値，トップ情報では IP アドレスやアプリケーションポート番号ごとの合算値から上位 25 位を算出して，各粒度のデータを蓄積する。

表 3　グラフ表示範囲と利用データ

グラフ表示範囲	利用データ
24 時間未満	リアルタイムデータ
24 時間以上，7 日未満	5 分粒度データ
7 日以上，1 か月未満	1 時間粒度データ
1 か月以上，1 年未満	3 時間粒度データ
1 年以上	1 日粒度データ

4.5　データベースの最適化

長期間分析の要求を満足するため，データ蓄積するデータベース容量を最適化する。サーバのストレージ容量には限界があり，容量枯渇を回避するために，各粒度データに個別の保存期間を設定可能とし，保存期間を超えたデータはロールアップさせることで，データ蓄積を制限する機能を実装した。

表 4　データベース保存期間

モニタ情報	保存期間	初期値
リアルタイムデータ	1 日～60 日間	1 日間
5 分粒度データ	1 週～300 週間	4 週間
1 時間粒度データ	1 か月～24 か月間	1 か月間
3 時間粒度データ	1 年～5 年間	1 年間
1 日粒度データ	3 年間, 6 年間, 9 年間	3 年間

5　サイレント障害検出への応用

ネットワーク機器やサーバのデバイスの故障，ソフトウェアバグなどで，ネットワーク内の一部の通信だけが不通となる状態が発生するケースがある。この場合，機器自身が障害を認識しないことが多く，通常の監視システムでも検出することはできない。このような障害をサイレント障害と呼ぶ。サイレント障害はユーザから「つながらない」などのクレームにより障害が発覚することが多い。サイレント障害の検出には，ネットワークの経路ごとに通信を監視することが有効である。

この無通信状態は，PFP のアラーム通知機能を応用することで検出可能である。PureFlow ノートが任意のサーバに対してアクティブ測定を実施し，その結果を PFP で監視することで，経路ごとの無通信状態を検出できる。**図 12** に，無通信状態が生じた際のフロー数グラフを示す。

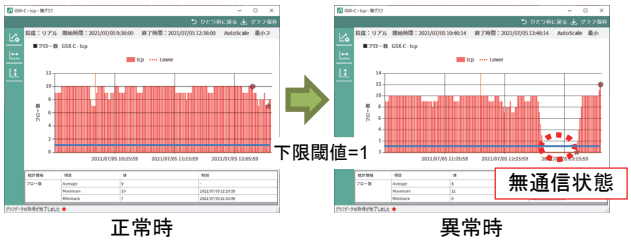

図 12　フロー数グラフ

フロー数の下限閾値を 1 に設定することで，フロー数が 0(=無通信状態)を検出し，アラーム通知する。各サーバに対する経路ごとにアクティブ監視することで，部分的な障害まで把握できる。

6　むすび

本稿では PFP の機能および特徴について述べた。PFP は，TCP 通信の遅延やパケットロスに着目し，それらを監視・分析することで，障害の早期発見につなげるソリューションである。今後，5G ネットワークの導入が加速し，新たなアプリケーションやサービスが増えることで，5G 通信品質の監視・分析が課題になると想定している。今後も映像アプリケーションなどに使用される RTP(Real-time Transport Protocol)の分析や，障害の予兆検出の自動化など改善を図り，ネットワークシステムのさらなる品質向上に貢献していきたい。

参考文献

1)　令和 3 年版　情報通信白書　総務省

執筆者


佐藤敬幸
環境計測カンパニー
インフラレジリエンス事業部
ソリューション開発部


安齋賢二
環境計測カンパニー
インフラレジリエンス事業部
ソリューション開発部


脇田智大
環境計測カンパニー
インフラレジリエンス事業部
ソリューション開発部


明戸正人
環境計測カンパニー
インフラレジリエンス事業部
ソリューション開発部

表 5　諸元表

	項目				PureFlow Profiler	備考
1	ノード管理				○	最大 255 ノード
2	モニタ情報	Network ポートカウンタ			○	―
		シナリオカウンタ(階層, 廃棄)			○	―
		ピークレート値			○	1 分間のピーク
		フロー数			○	ユーザ通信数
3	トップ情報	トップカウンタ	送信元, 宛先, 送信元・宛先, アプリケーション		○	Top25 まで
4	トラフィック分析情報	シナリオ分析 (シナリオ単位のプロトコル集計)	TCP	ネットワーク遅延	○	平均/最大/最小/分布
				サーバ遅延	○	平均/最大/最小/分布
				パケットロス	○	パケットロス率/バイト/回数
				再送	○	再送率/バイト/回数
		フロー分析 (フロー単位のトップ集計)	TCP トップ	遅延が大きい TCP フロー	○	Top100 まで
			ICMP トップ	遅延が大きい ICMP フロー	○	Top100 まで
			区間遅延(区間 RTT)		○	ラダー図表示
5	グラフ	リアルグラフ			○	―
		過去グラフ			○	―
		総合情報グラフ			○	情報一括表示
6	レポート	定期レポート(CSV/HTML)			○	―
		手動レポート(CSV/HTML)			○	―
7	グラフ/レポート種別	積み上げ, 折れ線, 円, 棒, 表			○	―
		折れ線/棒/ヒストグラフ			○	ネットワーク遅延/ サーバ遅延グラフ
		フロー一覧/ラダー図			○	区間分析
8	アラーム通知 (Syslog 通信/ SNMP Trap 送信/ コンソール表示)	トラフィックレート			○	上限値/下限値
		フロー数			○	上限値/下限値
		シナリオ分析 TCP	ネットワーク遅延/サーバ遅延[ms]		○	上限値
			パケットロス[%]		○	上限値
9	データベース保存期間	モニタ情報			○	最大 9 年間
		トップ情報			○	最大 1 年間
		トラフィック分析情報			○	最大 1 年間
10	バックアップ	オンラインバックアップ・リストア			○	―
11	シナリオコメント	インポート・エクスポート			○	一括操作可能
12	Radius 認証機能	ローカル認証と Radius 認証を選択可			○	―
13	接続対象モデル	NF7101C PureFlow GSX			○	―
		NF7501A PureFlow WS1			○	―

公知