

“はかる”技術で未来を創る



ロスレス・キャプチャツール

SYNESIS



GARLAND
TECHNOLOGY
See every bit, byte, and packet™

Flowmon
Driving Network Visibility



その時何が起きたのか、SYNESISは知っている

SYNESIS

1G / 10G / 100G SERIES

東陽テクニカが提供する 第3次世代パケットキャプチャ・ソリューション



5Gモバイルバックホール、SD-WANに提案、キャリアグレードの100Gモデル

世界初、100Gロスレス・キャプチャ

MPLS性能モニタリング

金融高速取引/顧客取引の通信バックアップに信頼の実績

600TBの長期保存、ポスト/リアルタイム解析

通信履歴ごとのインデックス検索

エンタープライズ/官公庁の業務運用ネットワーク管理

最小1G 30TB
300万円から

リモートによる一元管理モデルと
ディスプレイ付キャリーハンドモデル

部署ごと、業務アプリケーションごと、
サブネットごとの利用率監視

その他、サービス品質性能監視、開発シーンでも活躍

マルウェア分析

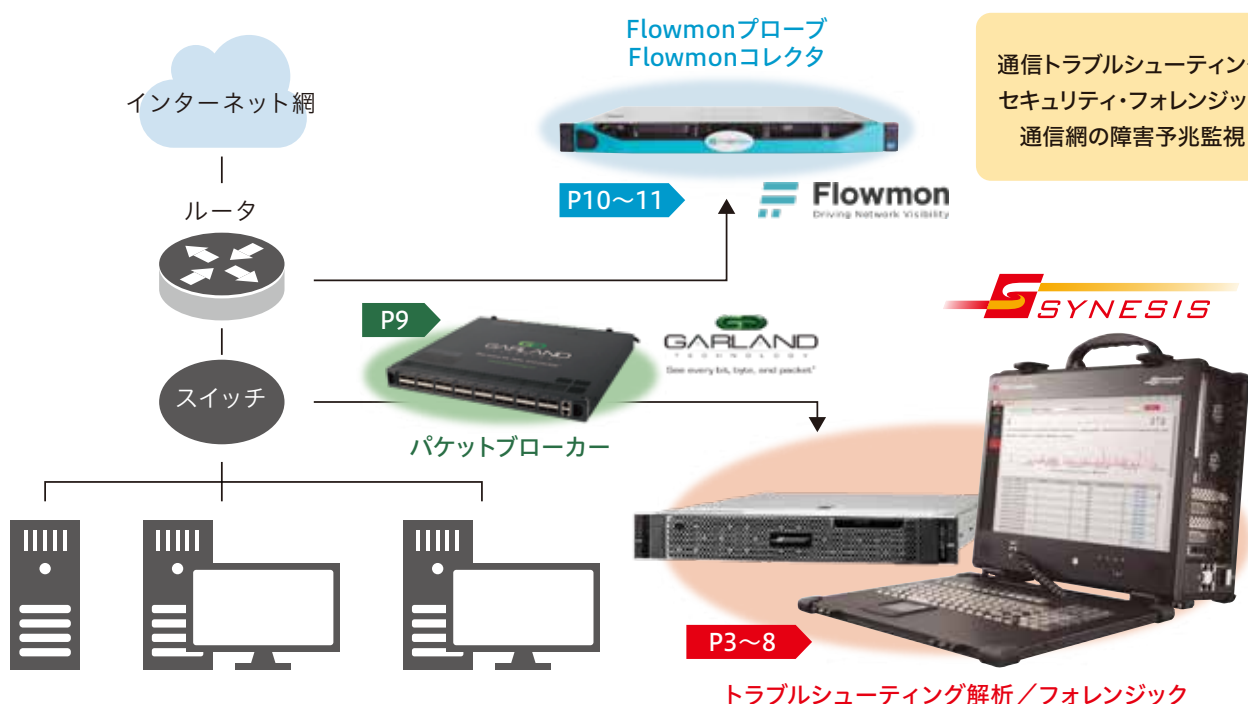
IP電話サービス品質監視

映像サービス品質監視

間欠障害のトラブルシューティング

インターネットサービスの通信分析

マイクロバースト監視



【SYNESIS】概要

SYNESISはネットワークを流れるデータを取りこぼしなくキャプチャし、品質劣化やセキュリティリスクの要因分析に貢献するパケットキャプチャ装置です。



全てのデータをキャプチャ(キャプチャ開始)



No.	開始時刻	終了時刻	ステータス	キャプチャファイル名	容量	備考
1	2017/08/08 11:24:52	2017/08/08 11:24:52	キャプチャ中	キャプチャファイル名	0 B	
2	2017/08/08 11:24:52	2017/08/08 11:24:52	停止	キャプチャファイル名	0 B	完了
3	2017/08/08 11:24:52	2017/08/08 11:24:52	停止	キャプチャファイル名	0 B	完了
4	2017/08/08 11:24:52	2017/08/08 11:24:52	停止	キャプチャファイル名	0 B	完了

キャプチャ開始すると
ステータスがキャプチャ中と表示されます。

キャプチャ停止すると、ステータスが
変わりレコードファイル生成されます

データのキャプチャを行いながら、同時に行うことができます。

問題原因を絞り込む(セッションの特定)

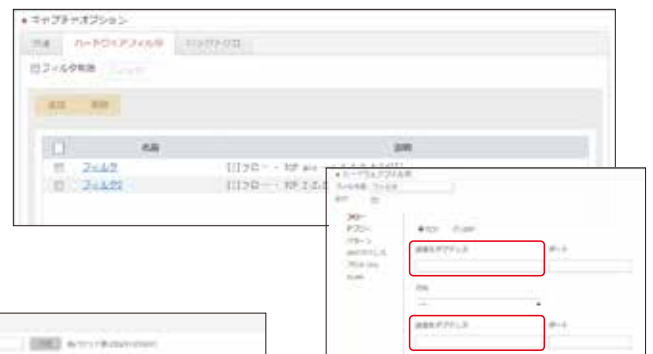


トレンド表示、セッション一覧表示、KPI項目を設定することで、問題原因となるセッションを絞り込みます。

選択可能なKPI項目

- ・APM解析
- ・バイト・パケット・リトライ
- ・NPM解析
- ・総バイト・受信バイト・送信バイト
- ・総パケット・受信パケット・送信パケット
- ・双方向ビットレート・受信ビットレート
- ・送信ビットレート
- ・双方向バーストビットレート
- ・受信ビットレート・送信ビットレート

特定のIPペアのみをキャプチャ(キャプチャフィルタ適用)

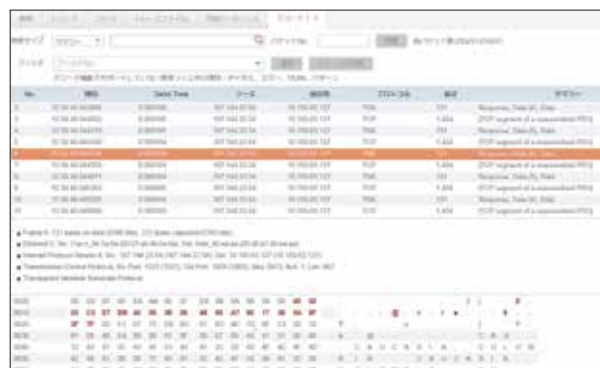


キャプチャフィルタ適用

特定のIPペアをキャプチャフィルタに設定して、キャプチャします。この場合は、設定されたIPペアの情報のみキャプチャされます。

特定のIPペアをキャプチャフィルタに設定して、キャプチャします。この場合は、設定されたIPペアの情報のみキャプチャされます。

解析



No.	開始時刻	終了時刻	ステータス	解析結果	備考
1	2017/08/08 11:24:52	2017/08/08 11:24:52	解析中	解析結果	
2	2017/08/08 11:24:52	2017/08/08 11:24:52	完了	解析結果	
3	2017/08/08 11:24:52	2017/08/08 11:24:52	完了	解析結果	
4	2017/08/08 11:24:52	2017/08/08 11:24:52	完了	解析結果	

WEBブラウザにて解析可能です。また、ローカルPCにトレースファイルを転送し、解析を行うことも可能です。

キャプチャ機能

パケットを連続して取りこぼしなくキャプチャし、蓄積します。

機器でのパケット欠損がないということはトラブルシューティング上、最も重要なことです。

キャプチャ方法

キャプチャする際、SYNESISと通信ネットワークは以下の方法で接続する必要があります。

1. ネットワークTAPを用いた接続 2. スwitchのSPAN(ミラー)ポートへ接続

この方法で接続することにより、SYNESISに障害が発生しても、既存の通信ネットワークには影響を与えません。

TAP接続

全二重回線のトラフィックを上りと下りに分けて、パケットを取り出せます。

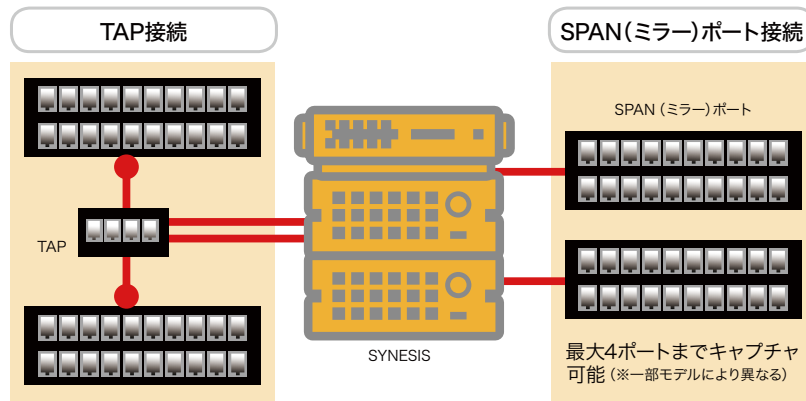
※TAPを挿入する際には、ネットワークを切断する必要があります。

SPAN(ミラー)ポート接続

スイッチ上でSPAN(ミラー)ポートを設定しパケットを取り出します。

通信ネットワークに影響を与えません。

※全二重回線で通信しているネットワークを半二重でパケットを取り出しますので、結果としてパケットロスが起こる可能性があります。



オプションタップ



銅ケーブルTAP



光TAP



アグリゲーションスイッチ

※タップの一例です。用途に応じて各種タップをご提案させていただきます。詳細は Web ▶ <https://www.toyo.co.jp/ict/maker/detail/Garland.html>

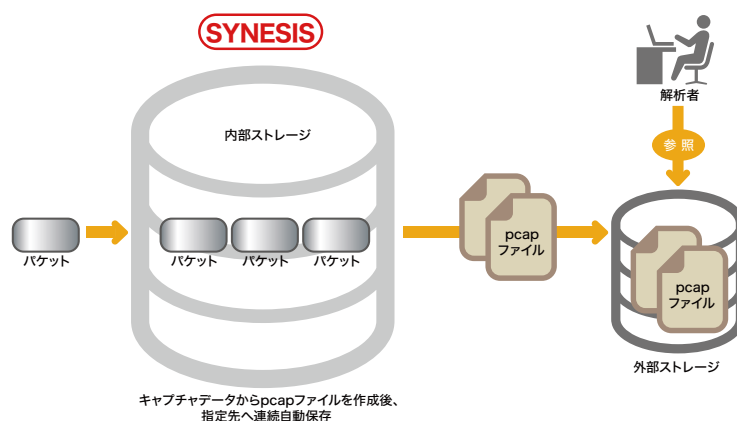
パケットキャプチャ機能

SYNESISは、10M / 100M / 1G / 10G / 40G / 100G / 200Gのネットワークに対応したキャプチャ装置です。ワイヤスピードのトラフィックを取りこぼしなくキャプチャ*できます。

いちいちキャプチャを停止しなくても、パケット解析を行うことが可能です。

また、キャプチャをしながら、自動的にpcapファイルを保存できる自動バックアップ機能をサポートしています。保存先はファイルシステムとして認識できれば、ローカル / リモートどちらも選択が可能です。

※ 特許取得済み「データ書き込み装置及び方法」



フィルタ・スライス機能

SYNESISは、必要なデータ、必要なレイヤのみをキャプチャするフィルタ・スライス機能を搭載しています。(一部のモデルを除く)

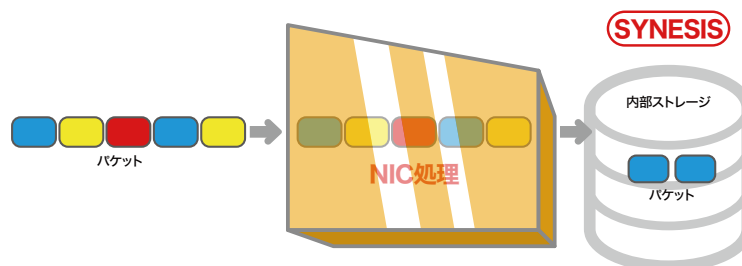
キャプチャ専用カード上で処理をしているため、トラフィックの負荷によらず確実な補足が可能です。

■キャプチャフィルタ

必要なデータだけをキャプチャ

■スライシング

ヘッダの先頭から必要な長さ(バイト)をキャプチャ



ロック機能

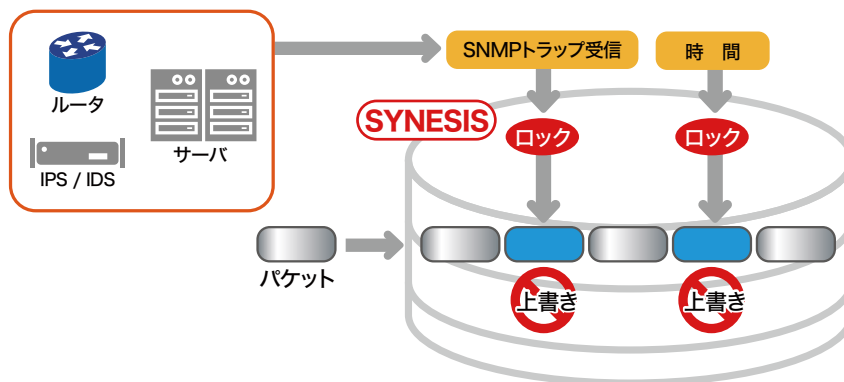
SYNESISは、残しておきたいデータを消さないためにロック機能を使用し、データの上書き禁止領域を指定することができます。ロック設定は、キャプチャ前、キャプチャ後どちらでも可能です。

■キャプチャ前

時刻、SNMPTラップによるロック指定

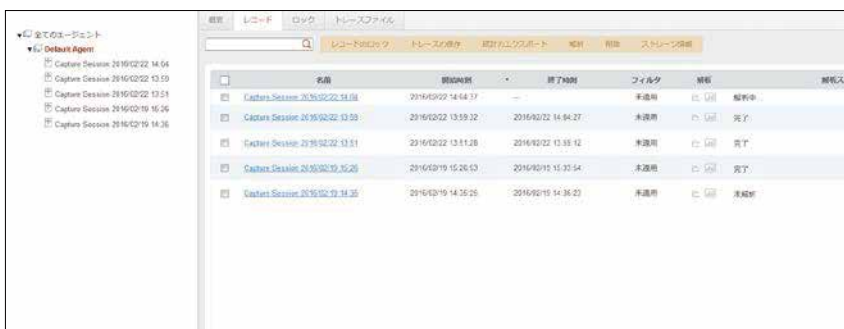
■キャプチャ後

レコード指定によるロック



レコード管理

SYNESISは、キャプチャの開始から停止までを1つのレコードとして管理します。重要なレコードはロック、解析済みのレコードは削除、といった運用管理ができます。レコードリストから、ロック、削除、トレースの保存、統計のエクスポートなどの操作がワンクリックで行えます。



レコード管理画面

インデックス機能

大量なデータの中から、ひとつひとつのパケットを調査して通信トラブルを見つけることは、非常に困難で、時間がかかります。SYNESISは、キャプチャしたデータをインデックス化することにより、大量なデータからネットワークの傾向をつかみ、さらに問題となるコネクションを特定します。

APM/NPM解析

SYNESISでは、通信データ量や応答時間などの各種指標(KPI)^{※1}を送信先や送信元、またはアプリケーションプロトコル別に表示させることができます。送信先/送信元別やプロトコル別にKPIを表示させることで、極端にトラフィック量の多い通信や、応答の遅延が発生している箇所など、問題が発生している箇所を探し出していくことができます。

■APM^{※2}解析

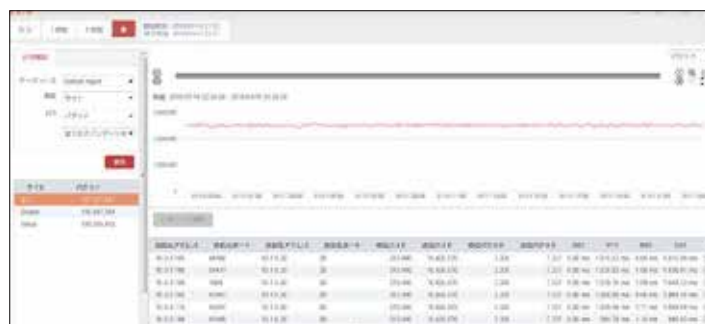
1つの通信の受信側(クライアント)と送信側(サーバ)間の応答の各段階で要している時間を詳細に確認し、遅延や不具合の発生している問題箇所を特定することができます。

■NPM^{※3}解析

各通信のデータ量を送信側と受信側で個別に表示することで、ネットワークの状態を確認することができます。



APM機能からトレース保存



APM機能

※1) Key Performance Indicator

※2) Application Aware Network Performance Method

※3) Network Performance Method

項目ごとにKPI(Key Performance Indicator)を表示

ネットワークの状況から特定のコネクションのみ抽出

解析機能

蓄積された大量なデータから、いかに早く目的の packets や通信を取り出せるかが重要です。
SYNESISは、様々な角度から packets を可視化しますので、目的に応じた解析のアプローチが可能です。

リアルタイムデコード

キャプチャしながらリアルタイムに packets をデコードします。キャプチャしながらネットワークの状況が把握できますので、フィールドでもラボでも重宝する機能です。

リアルタイムデコード画面

リアルタイム統計

キャプチャデータと同時に1秒ごとのトラフィックの統計を保存します。いつ、どのポートで利用率が上がっているかなどの把握が一目でできます。また、それらの統計値を自由にカスタマイズできるダッシュボードが作成できます。ダッシュボードで各項目のトレンドが確認できます。

<トレンド項目>

- L2トラフィック
 - 利用率、バイト/秒、パケット/秒、スループット
- TOP Nアプリケーション
 - およびアプリケーショングループ
 - イン / アウトトラフィック、スループット
- TOP Nホスト
 - イン / アウトトラフィック、スループット



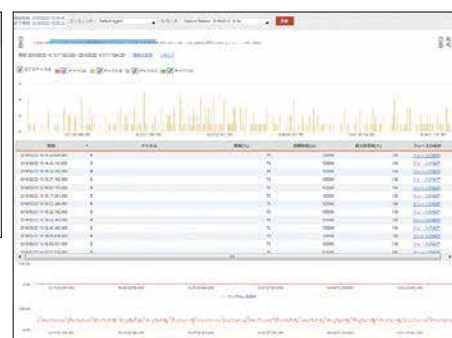
リアルタイム統計画面

マイクロバーストの検出

従来のネットワーク監視装置やパケット解析装置では検出できない、マイクロバーストを検出します。マイクロバーストは、ネットワーク機器の輻輳やパケットロスを引き起こす重大な原因となる事象です。SYNESISは、最小100μsec間隔で閾値を設定し、マイクロバーストがどこで、いつ起こったかの特定およびパケット解析が容易にできます。



(右) マイクロバースト検出画面
(左) マイクロバースト設定画面



アラート機能

SYNESISは、トラフィックの異常を検知してアラートを発することが出来ます。アラートを表示するためには、ユーザが必要な項目ごとに閾値を設定する必要があります。
AANPMアラートは3段階（危険/警告/情報）で閾値設定が可能です。さらに問題となったセッションのみのトレースファイルを保存できます。

■アラート項目

-DLC -NPM -AANPM

■アラートアクション

-E-mail -Syslog -SNMP Trap

AANPMアラート設定画面

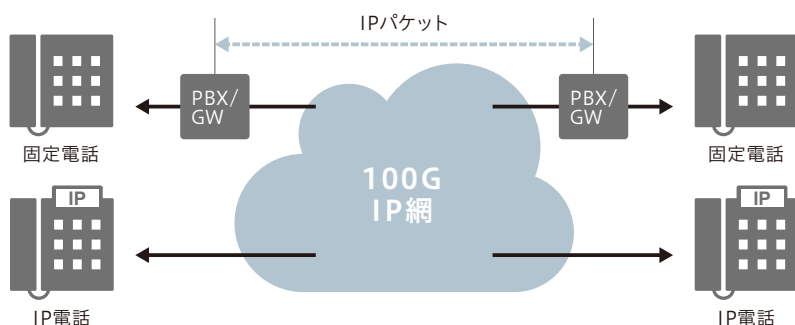
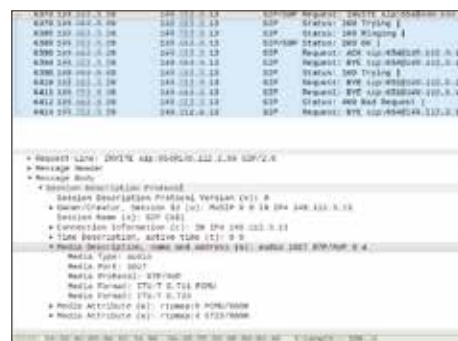
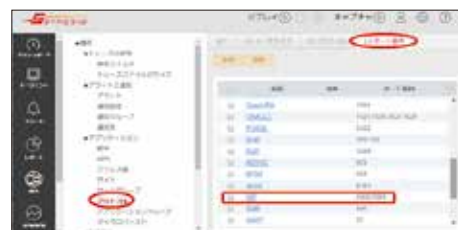
VoIP機能

インターネット回線を利用して音声データをやり取りするVoIPの技術は、現代のコミュニケーションを支える重要な技術です。SYNESISは、長時間連続キャプチャにより、IP相互接続におけるVoIP通信のトラブル調査を円滑にします。

100Gイーサネット回線に集約された大量通話を高速解析

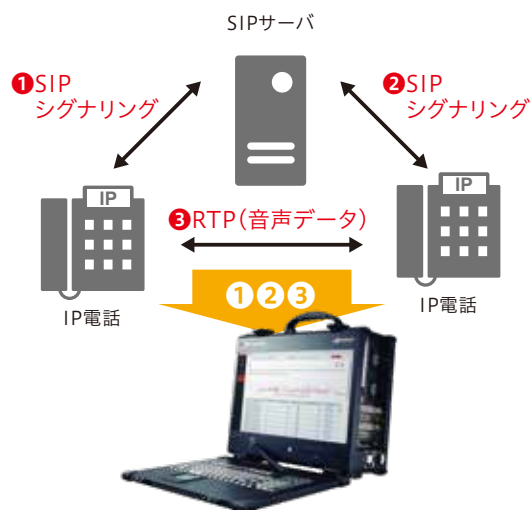
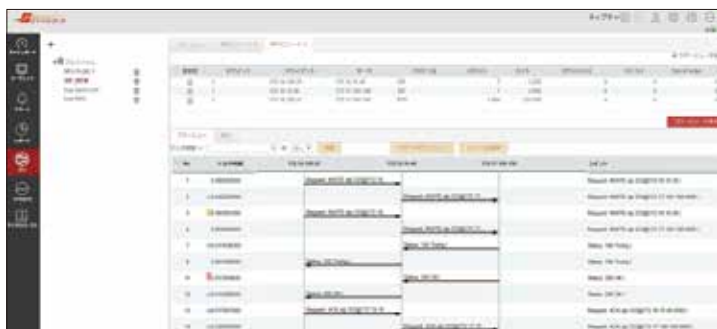


一元監視システム 100Gモデル

可搬型
200G / 100Gモデル

SIP / RTPのマルチフローアナリシス

- SIPの通話シグナリングをわかりやすいマルチフローで表示
- 複数拠点キャプチャファイルをポストアナリシス



コール抽出に要する時間の大幅短縮を実現

電話番号入力による通話抽出

- 発番号および着番号に国番号とユーザ番号(電話番号)による柔軟な検索
 - 32桁までの番号入力が可能
 - 複数の電話番号の指定が可能 (例: "0352687941;0352687990;0352688565")
 - 電話番号の範囲指定が可能
 - 個別の番号と範囲指定を混合して設定が可能
 - 3GPP向けに拡張されたプライベート・ヘッダ(Pヘッダ)に対応
- 「033245...」「+8133245...」など、キャプチャする場所により表現が異なる電話番号でもSIP / RTP / RTCPパケットを漏れなく抽出



SIP / SDP解析とコールの抽出

- SIPのシグナリングのコールステータス
(成功、失敗、ビジー、拒否)
- SIP / SDPにある実際に使われるIPアドレス、
UDPポート、電話番号、Call-ID

[illegible]

RTP / RTCP解析とコールの抽出

- RTP上のパケットロス、シーケンス不正、ジッタ(最大、平均)、コーデック



トラフィックモニタ

- 長期間モニタによるRTP監視
- スレッシュホールドによるアラームトラップ
- 予兆検知時間のトレースデータによる障害解析

VoIP Viewer (有償オプション、2020年4月リリース予定)

- pcapをベースにし、シーケンスをラダー表示・IP電話網の切り分けをより視覚的に行うことができるENUM対応
- シーケンスに含まれる Call-ID を自動検知。特定Call-IDのみの抽出可能
- 各発番号 / 着番号の呼開始時刻、呼終了時刻を容易に把握

その他機能

わかりやすいユーザインタフェース

導入しやすいブラウザアクセスでローカル、リモートから接続可能です。画面はシンプルで操作性に優れており、メッセージは日本語で表示されます。

Restful APIサポート

Restful APIに対応していますので、外部からのアクセスが可能です。自動化ツールによるテスト自動化、インシデント通知によるパケットの保全など、他のシステムとの連携が容易にできます。

時刻同期

せっかく取得したデータも、他のシステムと時刻が同期していなければ、原因の特定が困難になります。SYNESISは、NTP(Network Time Protocol)、GPS(1PPS)、PTP(Precision Time Protocol)、での時刻同期が可能です。

ユーザごとの権限

操作するユーザと閲覧するユーザで、権限を分けてユーザを作成することができます。操作上のヒューマンエラーを未然に防止する運用が可能です。

トレース保存実行管理

過去に実行したトレースファイルの保存条件(期間・フィルタ)はリスト化されます。過去の履歴からどのような条件でトレースファイル化しているか、一目でわかります。

Linuxベースのシステム

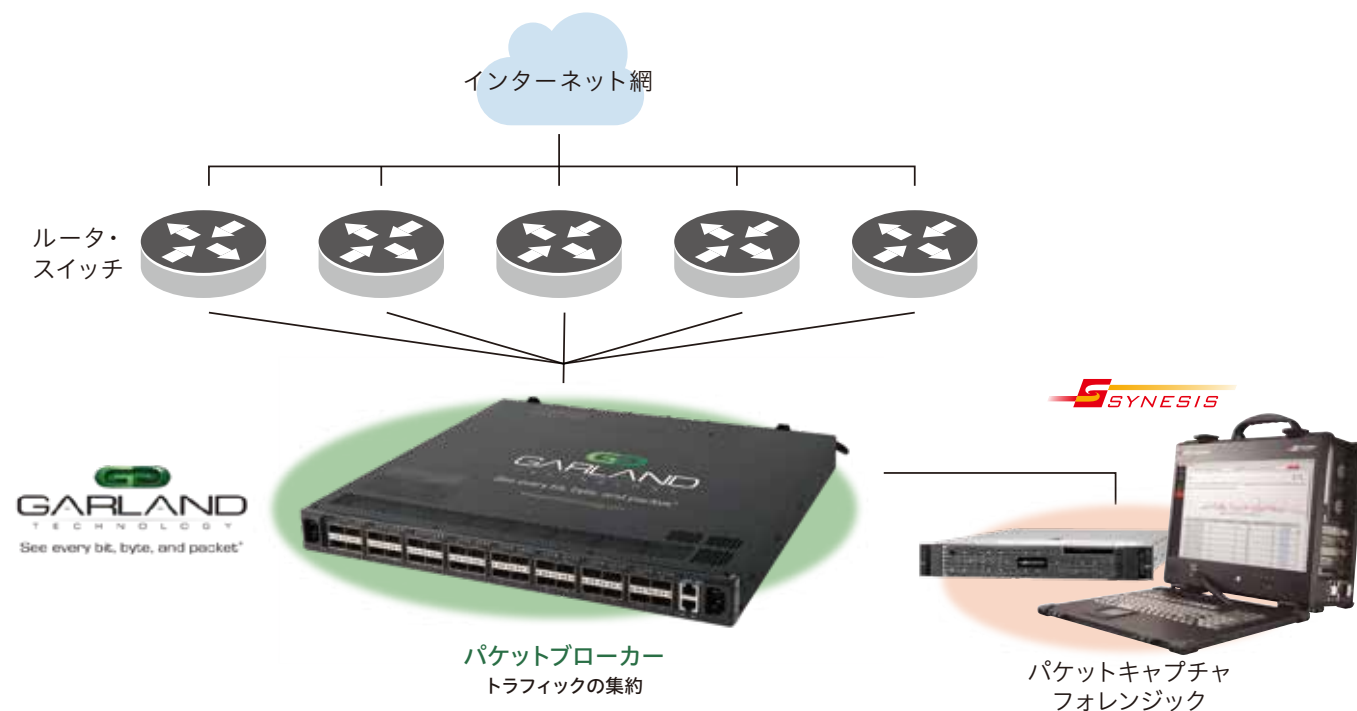
SYNOPSISは、Linuxベースのアプライアンスです。信頼性、可用性、保守性を重視した設計となっています。



【Garland Technology】パケットブローカー

Garland Technology社製ネットワークパケットブローカーは、モニタリング装置、セキュリティ製品にトラフィックを最適化して送信するソリューションです。

アグリゲーション、ロードバランシング機能によりモニタリング装置を効率良く利用することが可能です。

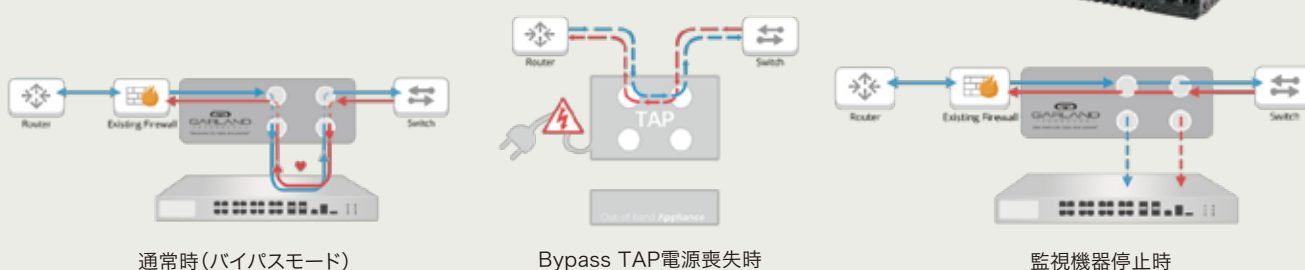


パケットブローカーの主な機能

- アグリゲーション
- リジェネレーション
- フィルタリング (L2-L4; mac address, IPv4, IPv6, TCP, UDP port, offset パターンマッチング)
- ロードバランシング
- VLAN tag, MPLS header ストリッピング, VLAN tag付け
- スライシング
- タイムスタンプ
- パケット重複削除

バイパスタップ

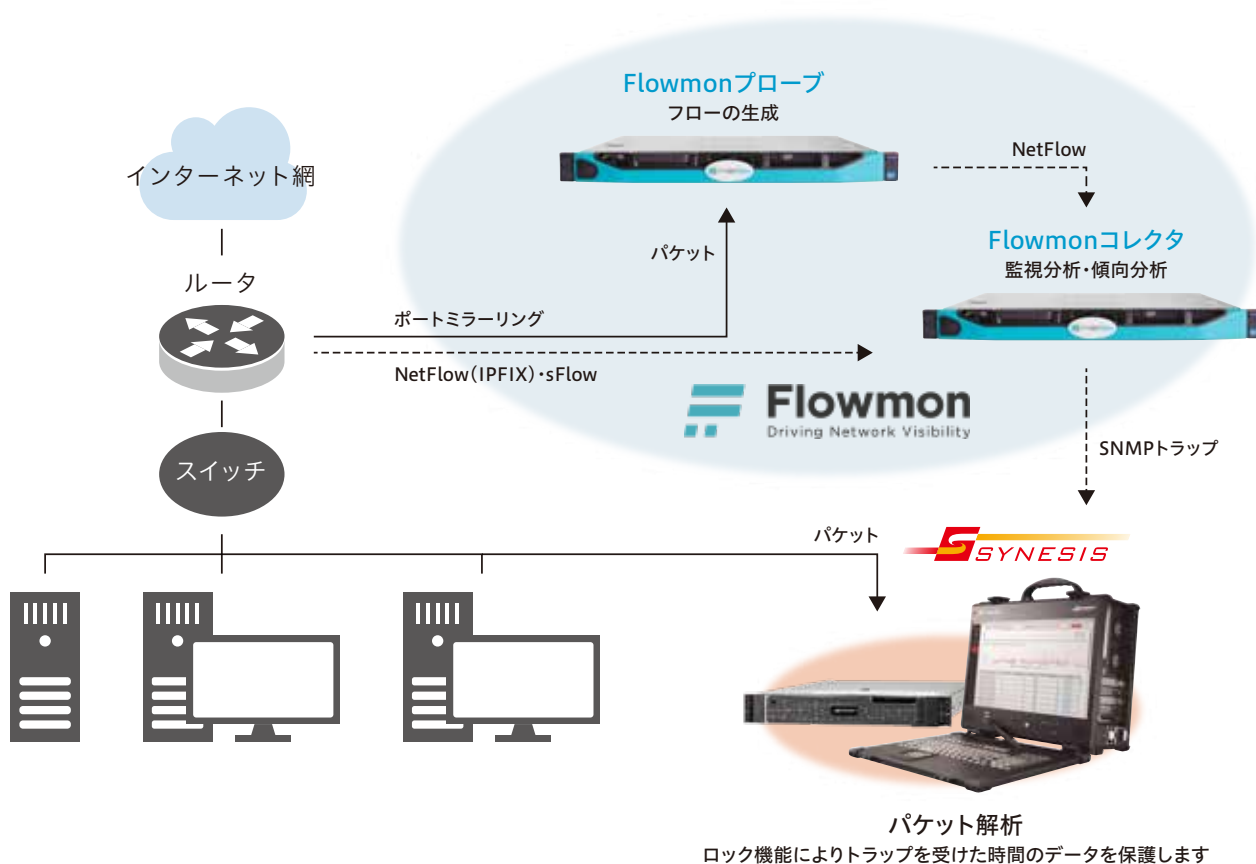
IPSなどのインライン装置を接続し、
インライン装置が不要になった際に自動的に切り離す装置



【Flowmon】Flowmonプローブ・Flowmonコレクタ

Flowmonは、ネットワークフロー技術を活用した革新的なトラフィック監視・分析ソリューションです。フロー情報の取得、監視と分析で「誰が」「いつ」「どこで」「何をしたか」を把握し、ユーザやアプリケーションの利用状況やふるまいを完全に可視化します。

また、目的に応じたプラグインを追加して機能を強化することができ、トータルなセキュリティソリューションの構築を支援します。



Flowmon プローブ

物理アプライアンス

仮想アプライアンス

- 既存のネットワーク機器を買い換えることなく機器のミラーポートやTAPに接続するだけで、取り込んだパケットデータからフロー情報を生成します。
- 10Mbpsより100Gbpsまでの回線に対応し、あらゆる規模のネットワークに適用できます。
- 専用コレクタと同等の分析機能を持つミニコレクタ機能を内蔵しており、プローブ1台から気軽にフロー解析を始められます。

Flowmon コレクタ

物理アプライアンス

仮想アプライアンス

- Flowmon プローブまたは他社ネットワーク機器などからのフロー情報を取得し、ネットワーク上のユーザやアプリケーションの利用状況をGUIで可視化、分析できます。
- 監視カメラのようにトラフィックの詳細を継続的に監視し、通信証跡を管理することでコンプライアンス対策、セキュリティ対策に活用できます。
- 取得したフロー情報の長期保存、蓄積が可能なRAID構成のストレージを内蔵しています。

プラグインオプション



Flowmon ADS

ふるまい検知



Flowmon APM

パフォーマンス監視



Flowmon DDoS
Defender

DDoS対策



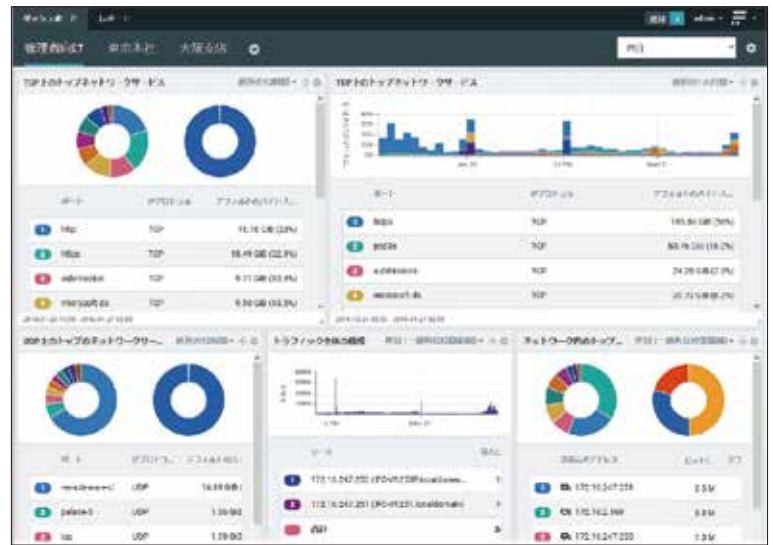
Flowmon Traffic
Recorder

トラフィック記録

Flowmon の運用画面例

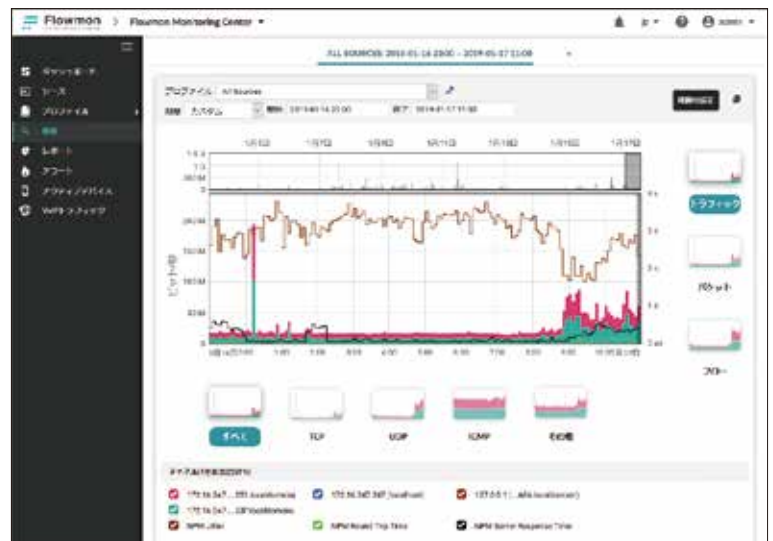
ネットワークの利用状況をわかりやすく表示するダッシュボード画面

- ユーザ (IPアドレスなど)、アプリケーション、トラフィック量、データ量などをグラフで可視化し、ランキング形式で表示
- 管理者向けの一覧画面のほか、拠点や部門ごとの表示項目を設定、切り替えることが可能



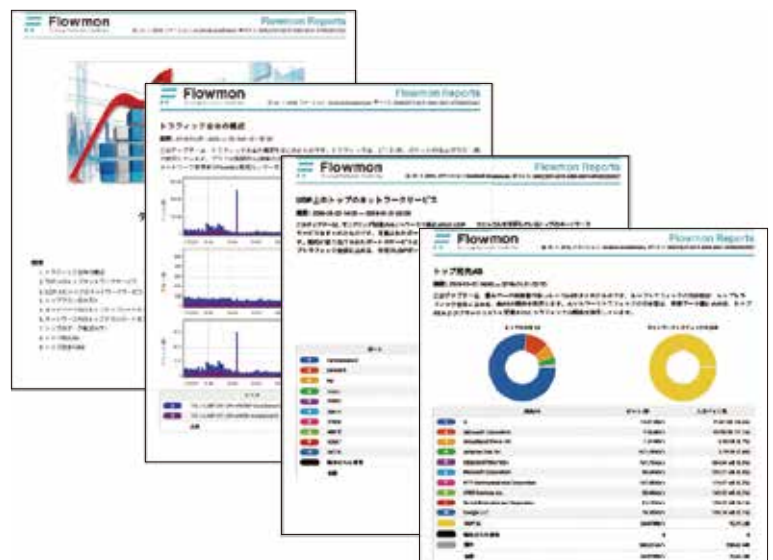
さまざまな視点でネットワークの利用状況を解析

- トラフィック/パケット/フローの各項目と、利用プロトコル、IPアドレスなどを任意に組み合わせで可視化
- 解析対象とする期間の設定も容易
- よく使う組み合わせはプロファイルとして登録可能



PDF形式のレポートを自動的に生成

- トラフィック全体の状況をはじめ、項目ごとにグラフとランキングをまとめたレポートを作成
- 日次/週次/月次でレポートを自動作成して、メール配信や外部ストレージへの保存が可能



SYNESISの7つの特長

1 長時間キャプチャ

トラブルシューティングで重要なことは、事象発生時の生データが残っていること。フォレンジックツールとしても活躍します。

2 ロスレスキャプチャ

ワイヤーレートでもロスしない強力ツール。キャプチャしたデータは外部機器に転送可能です。

3 高精度分解能

ナノ秒単位での高精度タイムスタンプを実現。マイクロバーストの解析や予期せぬトラフィック発生を見逃しません。

4 リアルタイムモニタ

1秒単位のリアルタイムモニタは、特定アプリケーションをグラフィカルに確認できます。

5 10G、40G、100Gサポート

全てのインタフェースでロスレス・長時間キャプチャ・高精度分解能を実現。100G双方向(200Gレート)モデルも世界初リリース予定。

6 国内で設計～製造～サポート

日本生まれの製品開発と製造、最先端の計測器による出荷検査、迅速な国内技術サポートまで一貫して提供しています。

7 安定稼働実績

商用ネットワークにも耐えうる長期間の安定運用。国内海外信頼の実績です。

200Gモデル
堂々リリース



待望の25Gモデル
近日リリース



<https://www.synesis.tech/>



<https://www.toyo.co.jp/ict/maker/detail/Garland.html>



<https://www.toyo.co.jp/ict/products/detail/flowmon.html>

最新・詳細情報は上記URLを確認ください。

株式会社 東陽テクニカ

情報通信システムソリューション部

〒103-8284 東京都中央区八重洲1-1-6

TEL.03-3245-1250 (直通) FAX.03-3246-0645 E-Mail: ict_contact@toyo.co.jp

www.toyo.co.jp/ict/

大阪支店	〒532-0003	大阪府大阪市淀川区宮原1-6-1 (新大阪ブリックビル)	TEL.06-6399-9771	FAX.06-6399-9781
名古屋営業所	〒460-0008	愛知県名古屋市中区栄2-3-1 (名古屋広小路ビルディング)	TEL.052-253-6271	FAX.052-253-6448
宇都宮営業所	〒321-0953	栃木県宇都宮市東宿郷2-4-3 (宇都宮大塚ビル)	TEL.028-678-9117	FAX.028-638-5380
電子技術センター	〒103-8284	東京都中央区八重洲1-1-6	TEL.03-3279-0771	FAX.03-3246-0645
テクノロジーインターフェースセンター	〒103-0021	東京都中央区日本橋本石町1-1-2	TEL.03-3279-0771	FAX.03-3246-0645



JQA-EM4908



JQA-QM8795
技術センター

※本カタログに記載された商品の機能・性能は断りなく変更されることがあります。
※本カタログに記載されている社名・ロゴは各社の商標及び登録商標です。各社の商標及び登録商標はそれぞれの所有者に帰属します。