“はかる”技術で未来を創る

東陽テクニカ

SYNESIS

100GbE S2D フルレートパケットキャプチャ/解析装置

Synesis

高性能・高信頼性・高可用性の追究から誕生!

概 要

約30年前、東陽テクニカは、後に業界標準となるTCP/IPプロトコルを7層翻訳できるアナライザを販売開始して以来、最新の通信規格に対応したパケット解析装置の販売および保守を提供してまいりました。
Synesisは、お客様のご要望、先進的な技術、解析・測定ノウハウを取り込みながら既存のパケット解析装置にはない可用性、コストパフォーマンスに優れた製品開発を目標に取り組んでいます。

特長 1

高性能、高品質

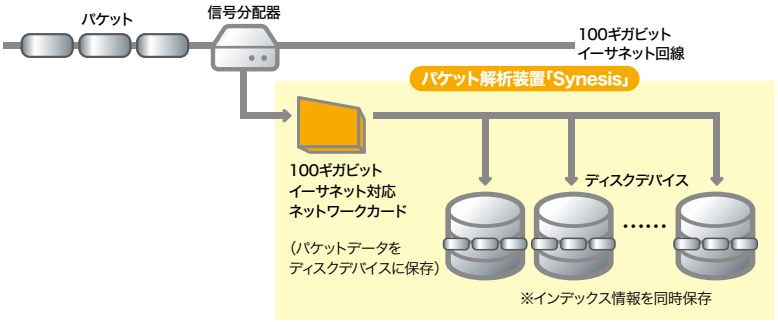
- 東陽テクニカが開発したアプリケーションは、100Gbpsラインレートのような大容量トラフィックであっても、パケットロスなく高速でディスクデバイスにストリーミングし、直接保存できます。これにより、100Gbpsキャプチャシステムだけでなく、既存のパケット解析装置では実現できなかった40Gbpsキャプチャポータブルなど、Synesisでは幾つもの革新的なモデルを提供しています。

- Synesisは、ショートパケットからロングパケットまでパケットサイズによらず、キャプチャ性能を保証します。また、ディスクデバイスの最適化を実現し、既存のパケット解析装置よりも高速なキャプチャ性能を、コンパクトなパッケージで提供することで、多くのお客様が望まれていたパケット解析装置の大幅なコストダウンを達成しています。

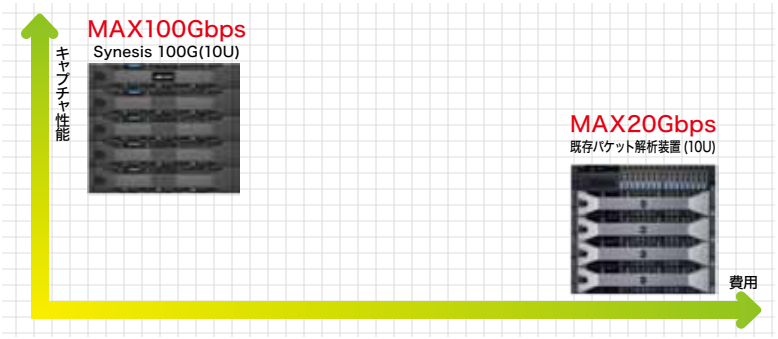
■一般的なパケット解析装置
- 64バイト（ショートパケット）によるキャプチャ性能

■Synesis Distributed / Portable
- 64～1518バイトによるキャプチャ性能

■開発アプリケーションの動作概念



■既存パケット解析装置との比較



特長 2

マイクロバーストトラフィックの検出

- Synesisは、最小100μsec間隔でトラフィック量、継続時間のしきい値を設定するだけで、大量のパケットデータの中から、マイクロバーストの有無を検出します。ユーザは、任意のマイクロバーストトラフィックをトレースファイルとして保存でき、より詳細な解析を行うことが可能です。

■マイクロバースト検出画面

特長 3

トレースファイルの抽出時間を大幅に短縮（APM解析）

- Synesisは、パケットをキャプチャする際に、既存のパケット解析装置よりも多くの情報、例えばIPアドレスやポートなどのインデックス情報を同時に保存することで、目的のパケットを検索、抽出する時間を大幅に短縮できるApplication Aware Network Performance Method（APM）を搭載しています。

■パケット解析・性能の検証結果

APMで トレース ファイル化	01:38.03(s)	● パケットが書き込まれている期間を検索 ● 通信量の多いコネクションのみをトレースファイルとしてダウンロード
保存フィルタで トレース ファイル化	3:47:01.89(s)	● APMを用いた際と同じ条件を保存ファイルに適用し、パケットが書き込まれている期間を検索 ● 保存フィルタに適用した条件はIPアドレス

※検証条件:66TBのパケットデータから任意のコネクションを抽出（社内比）

■ Synesis の充実した製品ラインナップ例

Model	Portable 4G	Portable 40G	Portable 100G	Distributed 4G	Distributed 40G	Distributed 100G
キャプチャポート	4 x 1GbE	4 x 10GbE/1GbE	2 x 100GbE	4 x 1GbE	4 x 10GbE/1GbE	2 x 100GbE
キャプチャパフォーマンス	4Gbps	40Gbps	100Gbps	4Gbps	40Gbps	100Gbps

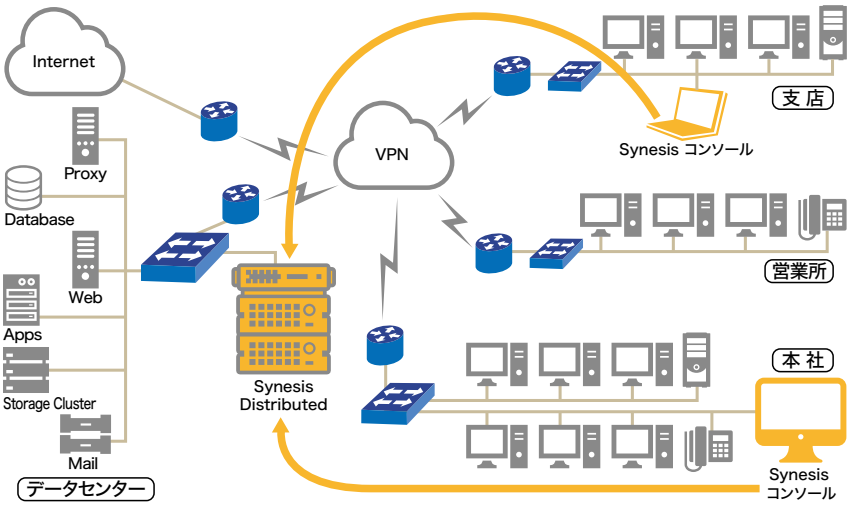
使用例（活用例）

使用例 1 ▶拡張インデックスの実装により、パケット解析能力の向上、解析時間の大幅な短縮を実現

拡張インデックスを用いて、トレースの抽出時間を大幅に短縮

- さまざまなアプリケーションが利用され、かつ数多くの事業所が繋がる今日の企業情報システムにおいて、通信品質の低下やセキュリティ上の問題が発生した場合、システム管理者は、従来のパケット解析装置で時間情報のみのインデックスを利用して、キャプチャした膨大なパケットデータの中から問題を引き起こす原因を特定しなければなりませんでした。時には10時間以上の時間を必要とする作業でした。
- システム管理者は、Synesisを導入することで、時間情報の他に、任意のサイト、任意のアプリケーション、任意のサーバ情報など拡張したインデックスを利用し、障害の原因となるパケットデータを容易に見つけ出すことが可能になります。

■ Synesis Distributed 導入イメージ1

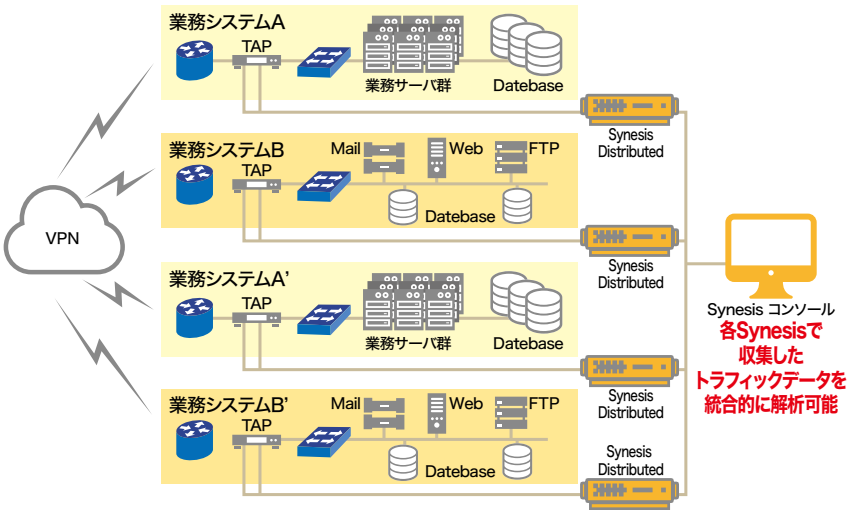


使用例 2 ▶統合ネットワーク監視ツール ～複数エージェント、複数回線の通信内容を統合的に解析～

複数のSynesis Distributed監視データを統合解析

- システム管理者は、複数のSynesis Distributedが収集したトラフィックを統合的に解析することが可能です。任意の期間に、どのサイトから、どのアプリケーションがもっとも利用されているのかリストアップし、任意のコネクションについてパケットレベルの詳細解析を行うことが可能になります。
- Synesisは、任意のサイトやサーバに対して、再送多発や低レスポンスを監視するために、3段階のしきい値を設定することが可能です。システム管理者は、ユーザからクレームを受ける前にSynesisのアラームにより異常を把握し、アラームに関連したパケットデータからトラブルシューティングを始めることもできます。

■ Synesis Distributed 導入イメージ 2

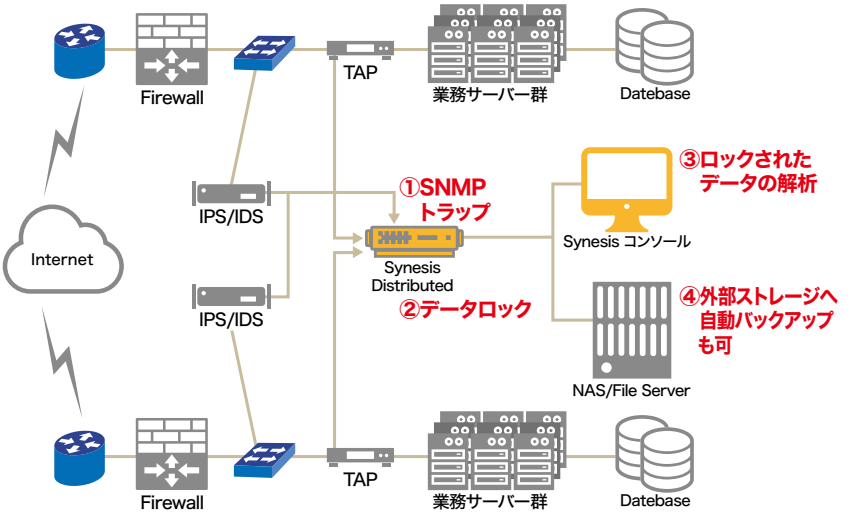


使用例 3 ▶外部セキュリティデバイスとの連携　～キャプチャデータの保護～

SNMPトラップをトリガーにしたパケットデータロック機能

- Synesisは、IDS/IPSやその他のネットワーク機器からSNMPトラップを受信することにより、その前後数分間のパケットデータを上書きされないようにロックすることが可能です。これにより、システム管理者は、実際の攻撃パケットや流出データを確保し、現実に起こったリスクを可視化することが可能になります。
- システム管理者は、Synesisでキャプチャしたパケットデータを NASなどの外部ストレージへ任意のスケジュールで自動バックアップすることもできます。

■ Synesis Distributed 導入イメージ3

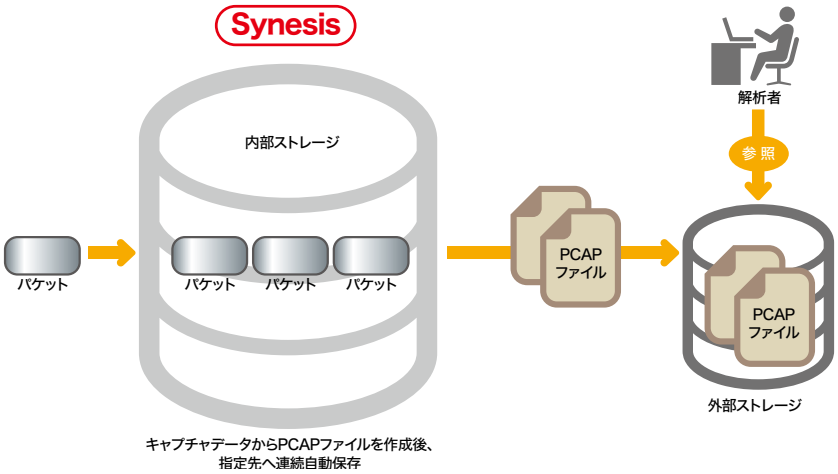


キャプチャ機能

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もっとも重要なことです。

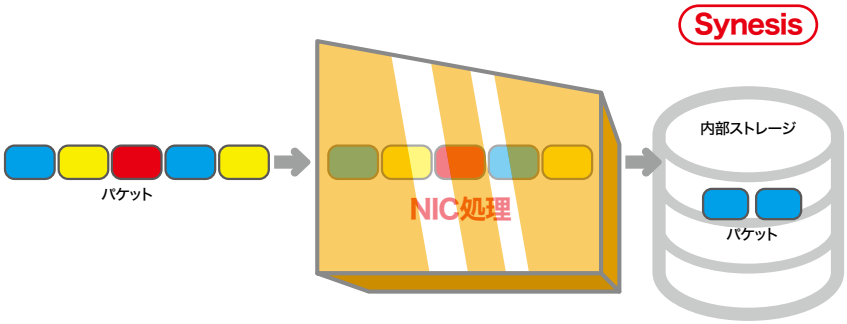
パケットキャプチャ機能

Synesisは、10M/100M/1G/10G/100G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オート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。



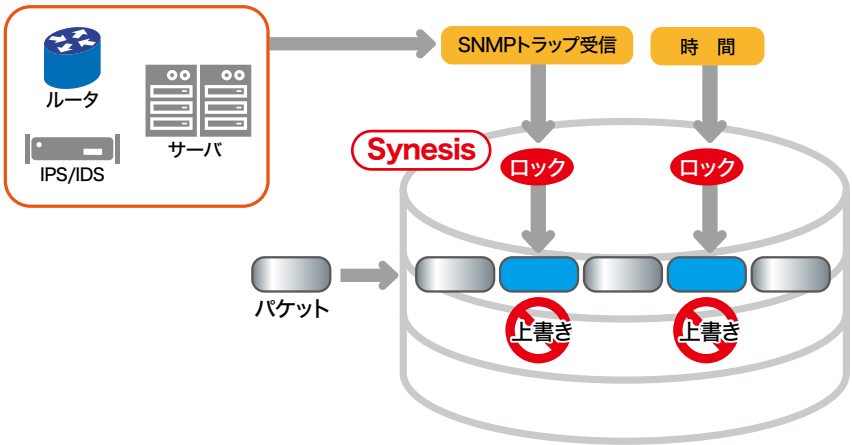
フィルタ・スライス機能

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



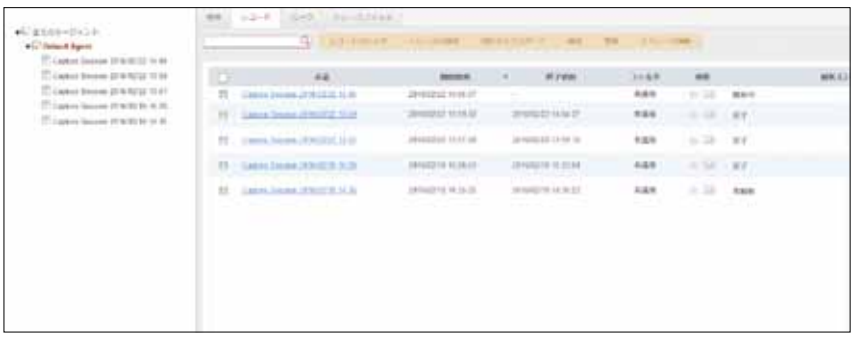
ロック機能

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、SNMPト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ひと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。

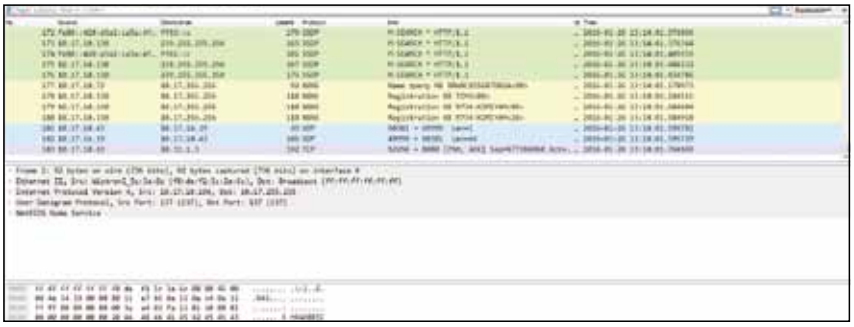

レコード管理画面

解析機能

蓄積された大量なデータから、いかに早く目的のパケットや通信を取り出せるかが重要です。
Synesisは、さまざまな角度からパケット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パケットをデコードします。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、どのポートで使用率が上がっているかなどの把握がひとめでできます。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
  -使用率、バイト/秒、パケット/秒、スループット
- TOP Nアプリケーション及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間隔でしきい値を設定し、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できます。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しきい値を設定する必要があります。
AANPMアラートは3段階(深刻/重要/ノーマル)でしきい値設定が可能です。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

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

キャプチャインデックス機能をもちいて、KPI（Key Performance Indicator）でネットワークの状況をトレンドベースで把握します。

APM機能からトレース保存

APM機能

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

■解析する項目

- **サイト**：サイト（サブネット）ごとの表示
- **アプリケーション**：アプリケーションごとの表示
- **サーバグループ**：サーバグループ（IP組み合わせ）ごとの表示
- **サーバ**：サーバごとの表示

■KPI

- **パケット**…通信パケット数
- **バイト**…通信バイト数
- **ART (Application Response Time)** サーバアプリケーションがクライアントリクエストに応答するのにかかる時間
- **CRT (Client Response Time)** ……クライアントがリクエストを開始するのにかかる時間
- **NRT (Network Round-trip Time)** …ネットワークをパケットが往復するのにかかる平均のラウンドトリップ時間
- **PTT (Payload Transfer Time)** ……サーバがクライアントリクエストへのレスポンスを送るのに要した時間
- **SRT (Server Response Time)** ……サーバがクライアントリクエストに応答し、レスポンスを完了させるのに要した時間
- **レイテンシ** ……片方向のネットワークを通過するパケットの平均時間
- **リトライ** ……TCPの再送パケットのシーケンス数
- **スループット** ……[受信バイト＋送信バイト]/サンプル時間[Kbit/sec]で計算される値
- **バーストスループット** ……時間周期中の最大スループット。周期が10分の場合は10スループットの値が存在しますが、その中で最大のものをバーストスループットとします。

オプション機能

パケットリプレイヤ

pcapファイルをキャプチャ時と同じリンクスピードで送信します。（10GbE／1GbEサポート）
リプレイ回数をオプションで指定することが可能です。
また、pcapファイル内のパケットヘッダのうち、以下の項目を置換します。

-MACアドレス
-VLAN ID
-IPアドレス(v4/v6)

■使用例

1）Synesisポータブルで連続キャプチャして、障害発生時にトレースファイルを保存します。
2）調査用にトレースファイルのヘッダを書き換えます。
3）再現環境上でファイルを再生し、障害の原因調査を行います。

■パケットリプレイヤの図

ユーザビリティ

箱から出したらすぐに使用できるように設計された製品です。簡単な操作画面、他のシステムとの連携など細かい点までこだわった設計となっています。

■わかりやすいユーザインターフェース
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。

■Open APIサポート
Open 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、GPS（Global Positioning System）、NTP（Network 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、権限をわ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、ひとめでわかります。

■Linuxベースのシステム
Synesis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おります。

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.スイッチの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。

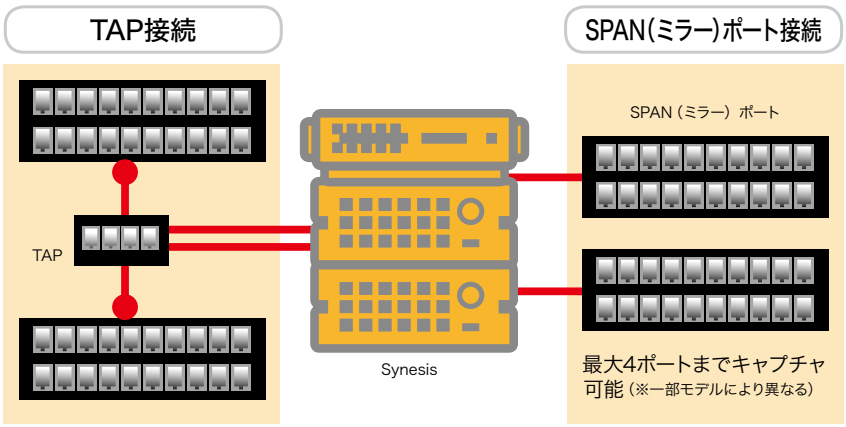
■TAP接続
ネットワークにTAPを挿入してパケットを取り出します。
<メリット>
- 全二重回線のトラフィックを上りと下りにわけて、パケットを取り出せます。

<デメリット>
- 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。
<メリット>
- 通信ネットワークに影響を与えません。

<デメリット>
- 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。

■接続図



オプションタップ ※以下はタップの一例です。用途に応じて各種タップをご提案させていただきます。

カッパーTAP

光TAP


アグリゲーションスイッチ

パケット解析装置の実績

1986
米国Network General社が
Snifferをリリース

1987
東陽テクニカが米国Network General社の
代理店権を獲得、国内で販売開始

1989
東陽テクニカが日本語化に取り組んだ
Snifferラップトップモデルを販売開始

1996
米国Network General社の
有償トレーニング「Sniffer University」を
開始

1997
米国McAfee社が
米国Network General社を買収

2003
米国ベンチャーを買収し、100%子会社である
米国ClearSight Networks社を立ち上げる。
同年10月ClearSightアナライザを販売開始

2006
他社に先駆けて、後に業界標準となる
Stream to Disk型キャプチャ装置である
ClearSight Network Time Machineの
販売開始

2007
他社に先駆けて、10GbE対応
ClearSightアナライザを販売開始。
ClearSight Network Time Machine
Portableの販売開始

2009
米国Fluke Networks社がClearSight
Networks社を買収。
東陽テクニカはFluke Networks社の
国内総代理店として販売、開発支援を継続

2012
Network Time Machine Portableが
INTEROP Tokyoで
Best of Show Awardを受賞

2014
Network Time Machineの
国内販売台数が700台を突破

2014
米国NetScout社がFlukeNetworks社
を買収。東陽テクニカは総代理店として
販売を継続

東陽テクニカ社製パケット解析装置Synesis 100Gの販売を開始!!

株式会社東陽テクニカが提供する各種ネットワーク・ソリューション製品、サービス及びセミナーの最新情報はこちらへ

★Synesisホームページ　http://www.toyo.co.jp/ict/synesis/

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　FAX.03-3246-0645
E-Mail : synesis-sales@toyo.co.jp
大 阪 支 店 TEL.06-6399-9771 FAX.06-6399-9781
名古屋営業所 TEL.052-772-2971 FAX.052-776-2559
www.toyo.co.jp/ict/synesis/

JQA-EM4908 JQA-QM8795
電子技術センター

SSS-4727-00-1603000-067-5.0-F19-CA