ネットワークインシデント情報を確実に捕捉！ NTMによるネットワークフォレンジック ソリューション

東陽テクニカ
情報通信システム営業部
協栄エレクトロニクス

2013年1月

個人情報漏えいインシデント現状

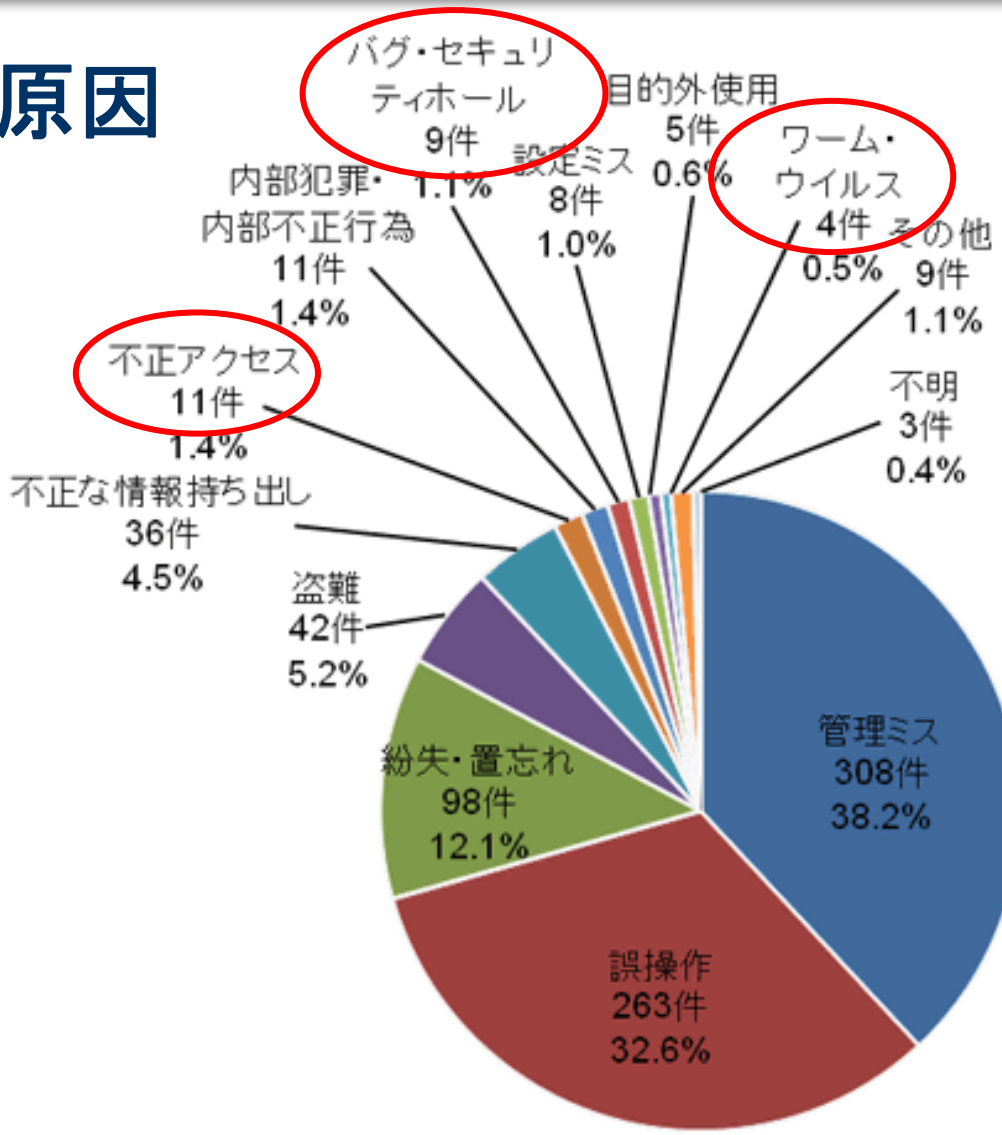
表 1：2011 年上半期 個人情報漏えいインシデント 概要データ【速報】

漏えい人数	208 万 5566 人
インシデント件数	807 件
想定損害賠償総額	573 億 1642 万円
一件当たりの平均漏えい人数(※1)	2667 人
一件当たり平均損害賠償額(※1)	7329 万円
一人当たり平均損害賠償額(※2)	4 万 1192 円

出展：JNSA セキュリティ被害調査ワーキンググループ
2011年 情報セキュリティインシデントに関する調査報告書【上半期 速報版】

東陽テクニカ

情報漏えい原因



出展：JNSA セキュリティ被害調査ワーキンググループ
2011年 情報セキュリティインシデントに関する調査報告書【上半期 速報版】

図 1：原因別の漏えい件数

東陽テクニカ

無視できないネットワーク経由の情報漏えい

表 2：2011 年上半期 個人情報漏えいインシデント トップ 10

No.	漏えい人数	業種	原因
1	100 万7052 人	生活関連サービス業，娯楽業	不正アクセス
2	12 万8307 人	金融業，保険業	管理ミス
3	7 万3000 人	卸売業，小売業	ワーム・ウイルス
4	6 万4728 人	複合サービス事業	管理ミス
5	6 万4728 人	複合サービス事業	管理ミス
6	6 万4728 人	複合サービス事業	管理ミス
7	6 万4728 人	複合サービス事業	管理ミス
8	5 万人	公務(他に分類されるものを除く)	内部犯罪・内部不正行為
9	3 万6504 人	卸売業，小売業	ワーム・ウイルス
10	3 万人	サービス業(他に分類されないもの)	バグ・セキュリティホール

No.4～7 の 4 件のインシデントは、漏えい人数がまとめて公表されたため、インシデント数(4 件)で除算した値を漏えい人数に採用しています。

出展：JNSA セキュリティ被害調査ワーキンググループ
2011年 情報セキュリティインシデントに関する調査報告書【上半期 速報版】

ネットワークフォレンジックとは

- 不正アクセスや情報漏えいに備え、通信の履歴や、やり取りしたデータそのものを記録し残すこと
- 通信回線上のパケットを、一定期間にわたり保存することにより、インシデント(情報セキュリティ上の脅威となりうる出来事)発生事後に調査・分析を行うことができる
- 犯人や被害範囲の特定に加え、自己防衛や犯罪の抑止効果もつ
- 法制により企業における情報セキュリティの確保が求められている

法律による規制

- 個人情報保護法(2005年4月全面施行)
  - *各種ガイドラインにて個人情報へのアクセスや入退室の履歴などを記録し保存しておくことが望ましいと規定*
- 不正アクセス禁止法(2000年2月施行)
  - *不正アクセスがあったことを検知したり痕跡をたどるために通信ログや操作履歴が必要*
- 不正競争防止法(2005年11月施行)
  - *営業秘密を違法な手段で取得・使用したり他人に売却したりしていないことを証明する必要がある*
- 日本版SOX法(2007年9月施行)
  - *財務報告に関係する業務プロセスがルールどおりに運用されていることを証明する必要がある*

司法の場で、記録の保存がもとめられている

情報漏洩対策はもはや避けては通れない！

ネットワークフォレンジックツールに求められる機能

- Gigabitイーサネット回線の高負荷環境においても、パケットを逃さず確実に記録できること
- テラバイトクラスのストレージを備え、長期間にわたりパケットのキャプチャを継続できること
- キャプチャした膨大なパケットの中から目的の情報を迅速に見つけ出し効果的に解析が行えること
- インシデント発生前後のパケットデータをエビデンスとして確実に保全できること

Network Time Machineによる対策

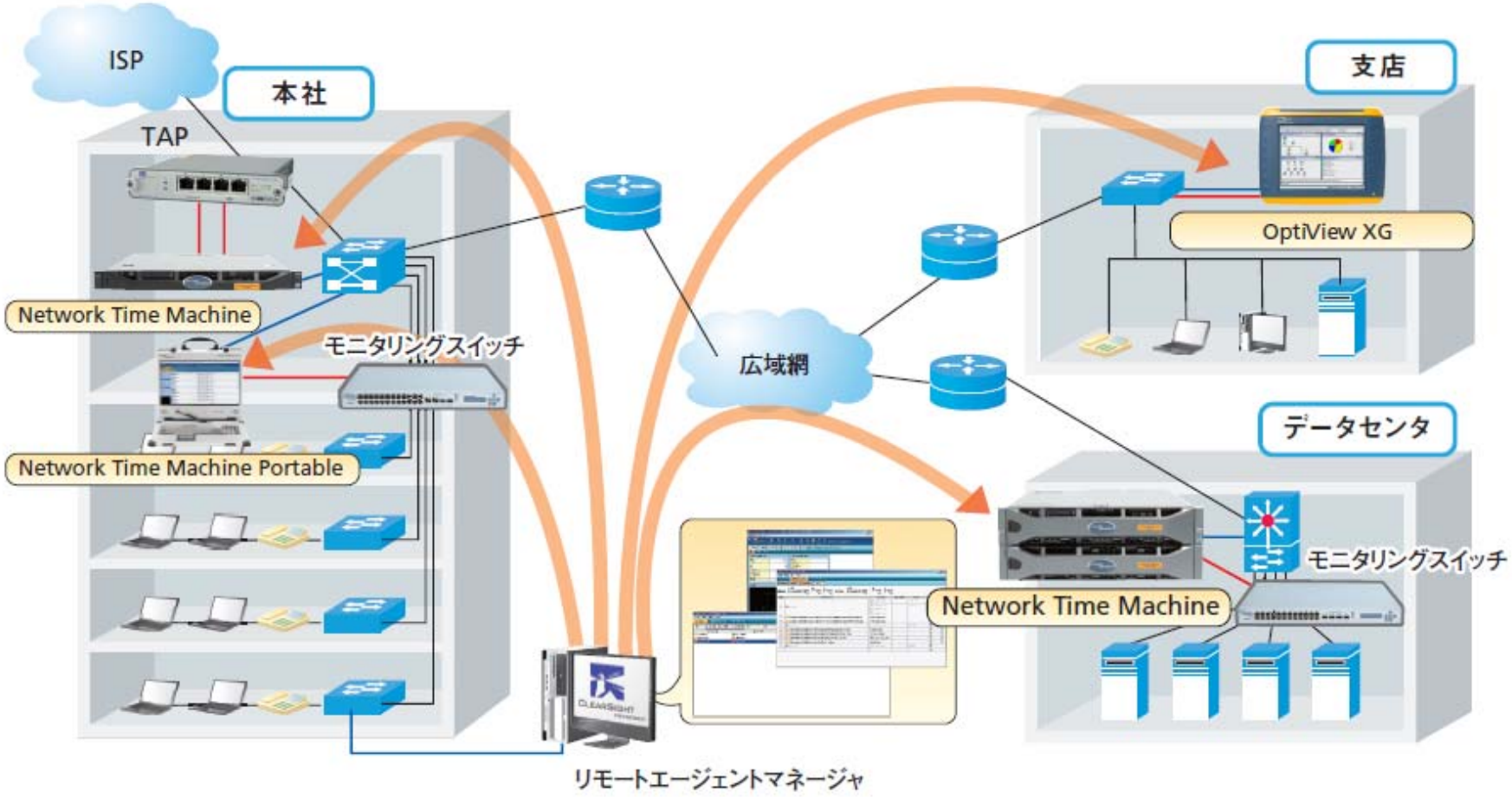
ネットワークタイムマシーン特長

- 業界標準ClearSightアナライザをベースとした大容量のLANアナライザ
- テラバイトクラスのHDDに長時間の連続キャプチャが可能
- ギガビットネットワークをワイヤレートで取りこぼすことなくキャプチャ可能
- 直感的なGUIと抜群のデータ解析能力
- ネットワークをまたがる通信の解析を可能にするマルチセグメント機能
- 大量のキャプチャデータの効率的な解析を可能にするアトラス・インデックス機能
  - *ネットワーク統計情報のデータ収集とトレンド表示*
  - *ネットワーク/サーバ/クライアントのパフォーマンスボトルネック解析*
  - *マイクロバーストの発生検知及び解析機能*

機器のモデル

ポータブルタイプ 持ち運びに便利	ラックマントタイプ 据え置き型
	
キーボード、ディスプレイを備えた可搬型フィールド用モデル	長時間の連続キャプチャに対応する大容量、ハイパフォーマンスモデル

監視イメージ


ISP
本社
TAP
Network Time Machine
モニタリングスイッチ
Network Time Machine Portable
広域網
支店
OptiView XG
データセンタ
モニタリングスイッチ
Network Time Machine
リモートエージェントマネージャ

NTM利用シーン

1. ネットワークトラブルシューティング

   長時間連続でキャプチャできるため、不定期に起こる間欠障害の原因を記録可能。

   さらに、通信シーケンスが自動でラダー表示されるため、遅延の原因を効率よく発見できる。

2. ネットワーク調査

   サーバやSWなどのネットワーク機器にどのようなパケットが流れているかを長時間保存し、トラフィックの傾向を解析することが可能。

   サーバの置換えや増設の際に機器に流れるトラフィックの解析をする際に利用できる。

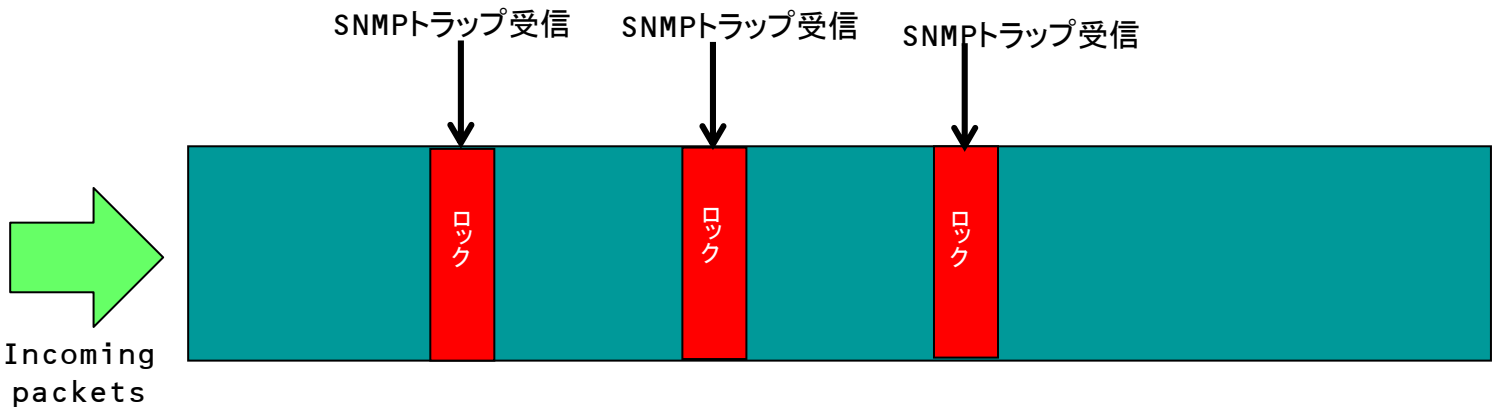
3. ネットワークフォレンジック

   情報漏洩、不正アクセスパケットの捕捉

東陽テクニカ

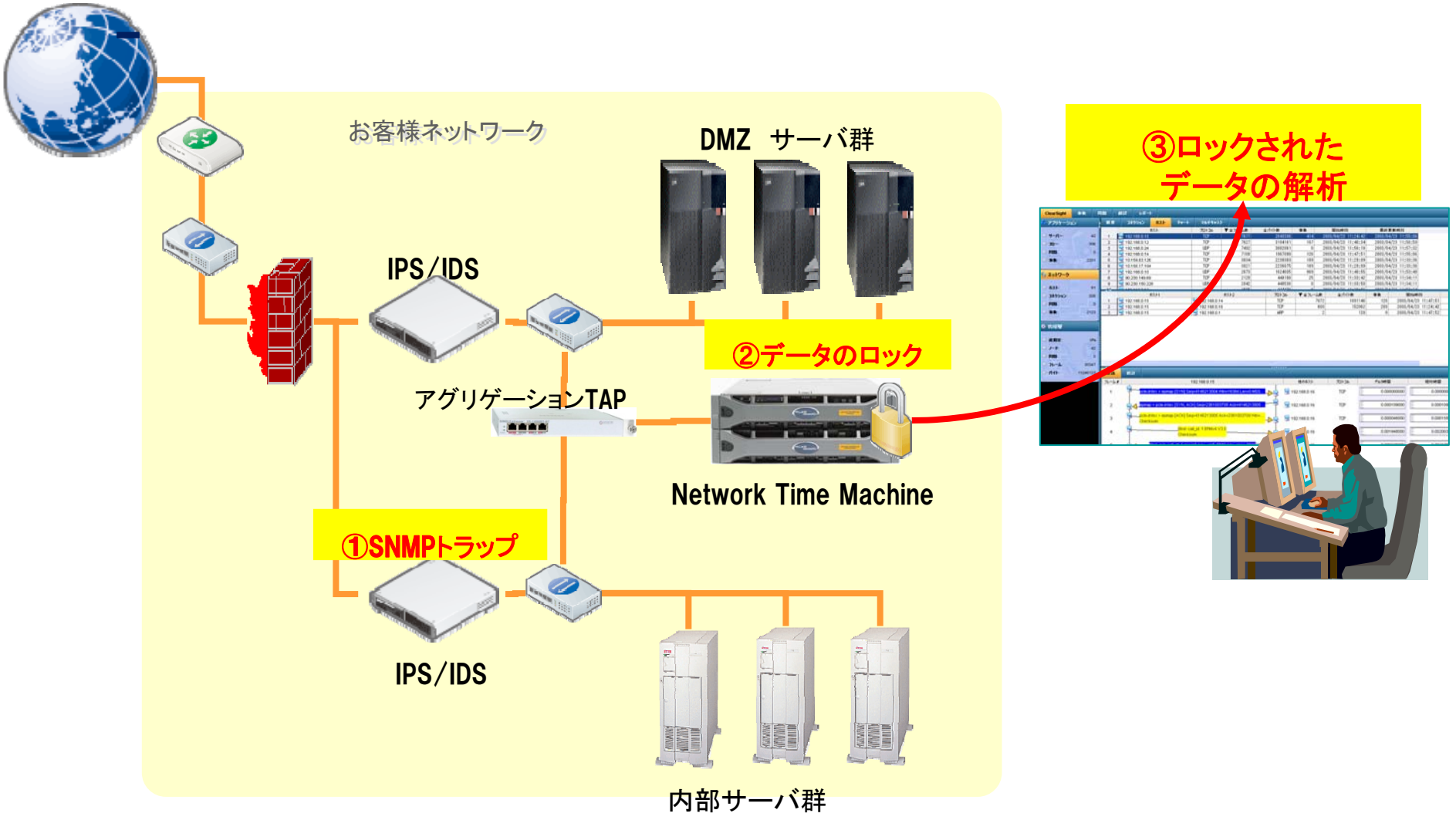
Network Time Machineによる
確実なデータの保全

インシデント発生時のデータロック



- 外部デバイスからのSNMPトラップパケット前後数分間のデータをロックし上書きから保護
- Network Time Machineリアルタイムアラートによるデータロックも可能
- ネットワークインシデントや障害発生時のデータを確実に記録し、後から詳細に解析したりエビデンスとして使用することが可能

外部セキュリティデバイスとの連携　構成例　– データの保護



SNMPによるデータロック機能

Network Time MachineがIDS/IPSやその他のネットワーク機器からのSNMPトラップを受信することにより、その前後数分間のデータを上書きされないように保護し、インシデント発生時のパケットを確実に捕捉することが可能。

ロックすることで、データの上書きの可能性を排除し、実際の攻撃パケットや流出データを“確保”、現実に起こったリスクを可視化することが可能。
そのため、緊急事態に際して行われるインシデントレスポンスやフォレンジックスフェーズでの影響度把握がすばやく行え、対策検討の意思決定を支援可能になります。

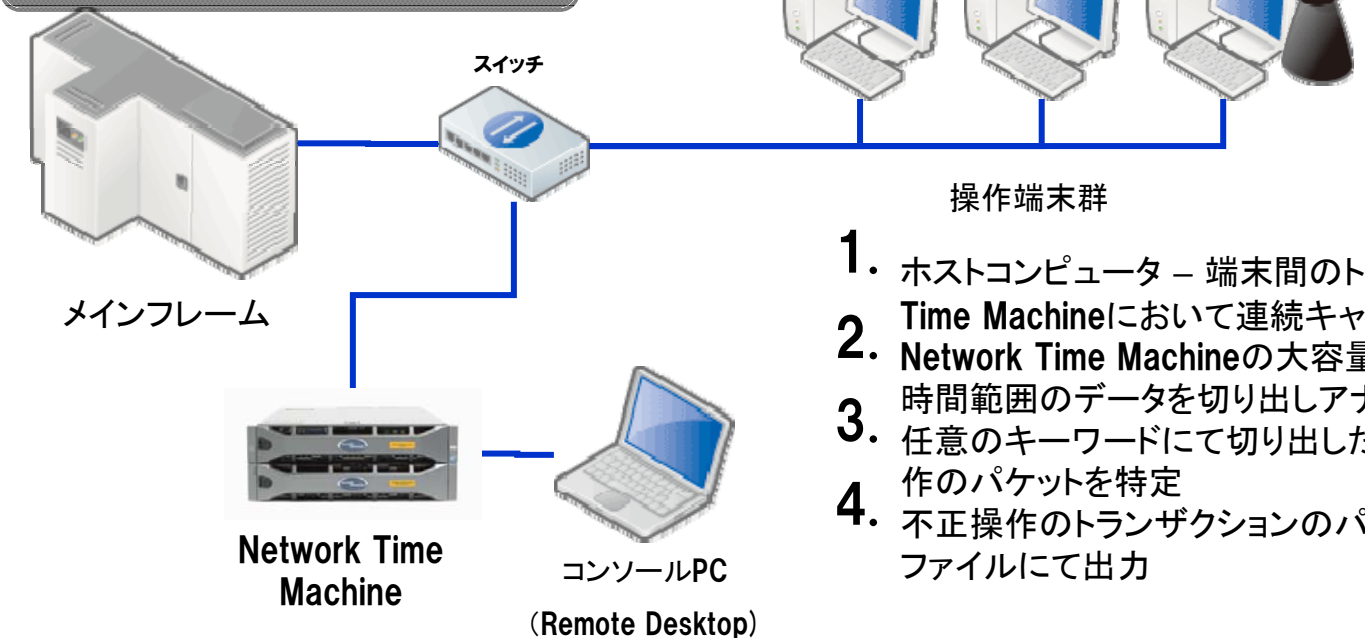
情報漏洩対策事例

情報漏洩対策　事例　－ 内部からの情報漏洩対

目的

- ホストコンピュータに対する端末からの操作のパケットを記録/検索、不正操作を行ったユーザの特定
- 内部からの情報漏洩対策

システム構成/解析手順

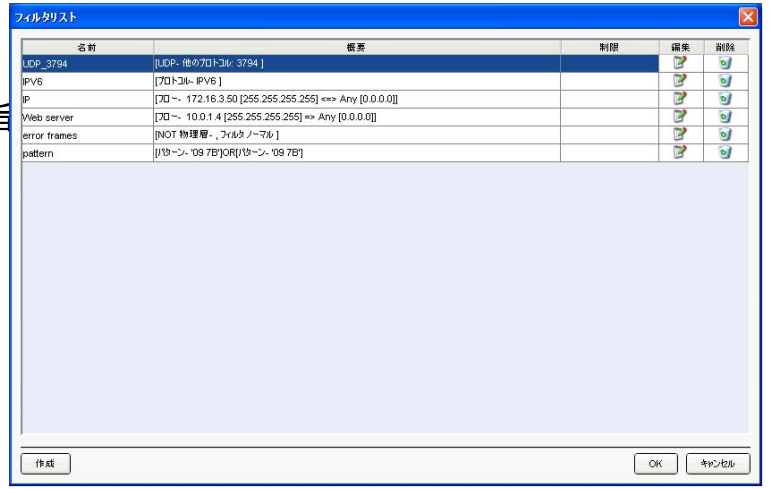


1. ホストコンピュータ – 端末間のトラフィックをNetwork Time Machineにおいて連続キャプチャ
2. Network Time Machineの大容量ストレージから目的の時間範囲のデータを切り出しアナライザに読み込み
3. 任意のキーワードにて切り出したデータを検索し不正操作のパケットを特定
4. 不正操作のトランザクションのパケットデコードをテキストファイルにて出力

東陽テクニカ

情報漏洩対策　事例　－ 解析運用方法/手順 －

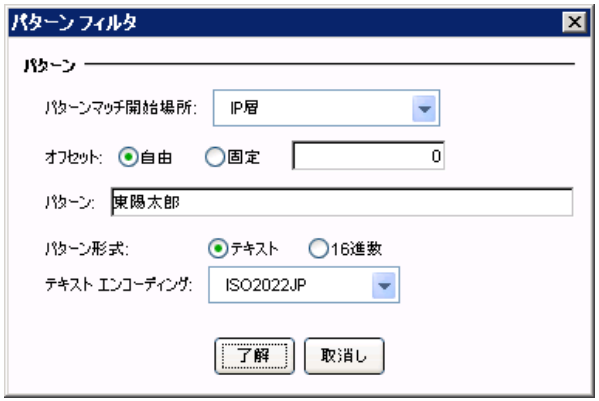
パターン: マッチさせたいパターンを指定



パターン形式がテキストの場合は、最大256文字のテキストまで指定できます。
パターン形式が16進数の場合は、パターンバイト列を、
ひとつのスペースで区切られた16進数で指定します。
その場合は最大256バイトまで指定できます。

パターン形式: [テキスト | 16進数]

テキストエンコーディング: [ASCII | ISO2022JP | SJIS]。
指定したテキストパターンのエンコーディングを選択します。この設定はパターン形式でテキストを選択した場合にのみ有効になります。
テキストパターンに半角カタカナを指定した場合の符号化は、ISO2022JPを選択するとJIS7（16進数で21から5Fの文字コードを使用）、SJISを選択するとJIS8（16進数でA1からDFの文字コードを使用）で行われます。

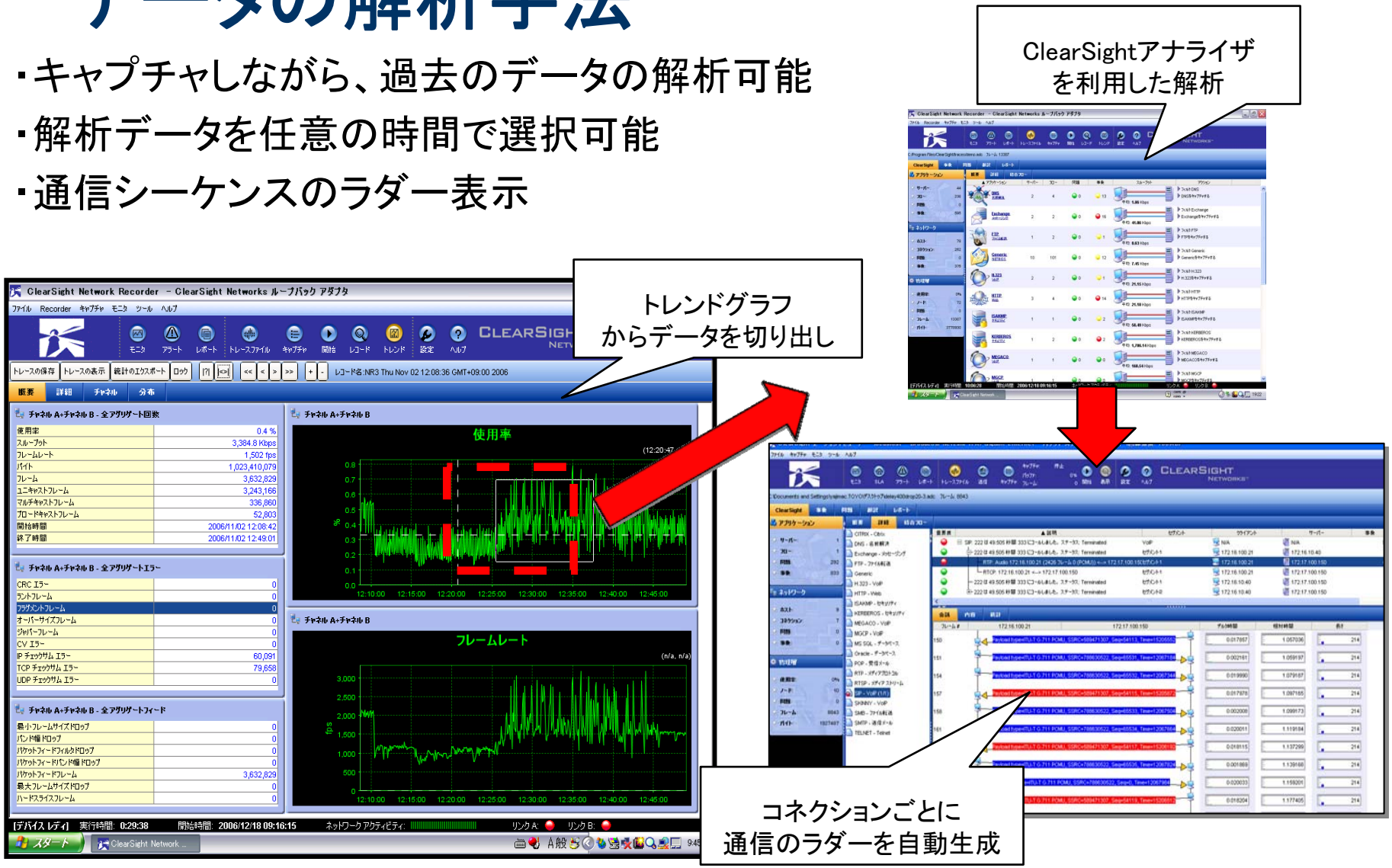


東陽テクニカ

Network Time Machineの解析機能

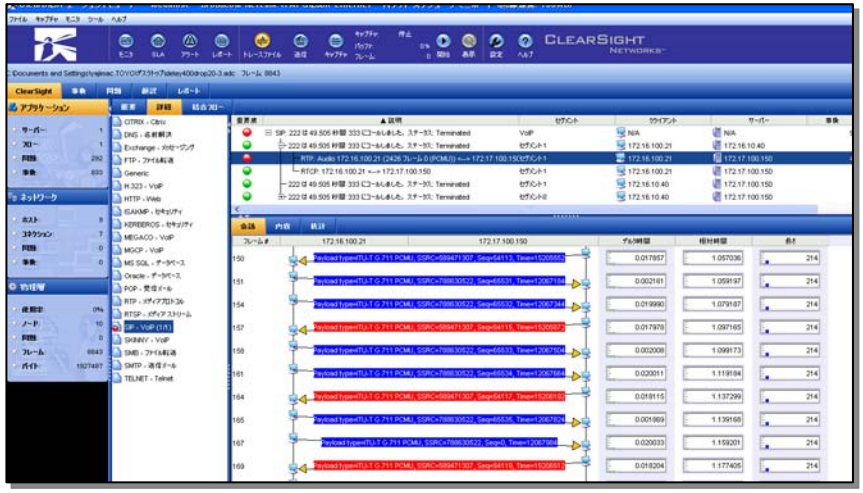
データの解析手法

- キャプチャしながら、過去のデータの解析可能
- 解析データを任意の時間で選択可能
- 通信シーケンスのラダー表示



プレイバック機能

キャプチャデータからHTTP、電子メール、データベース、
動画や音声通話などの再生が可能。

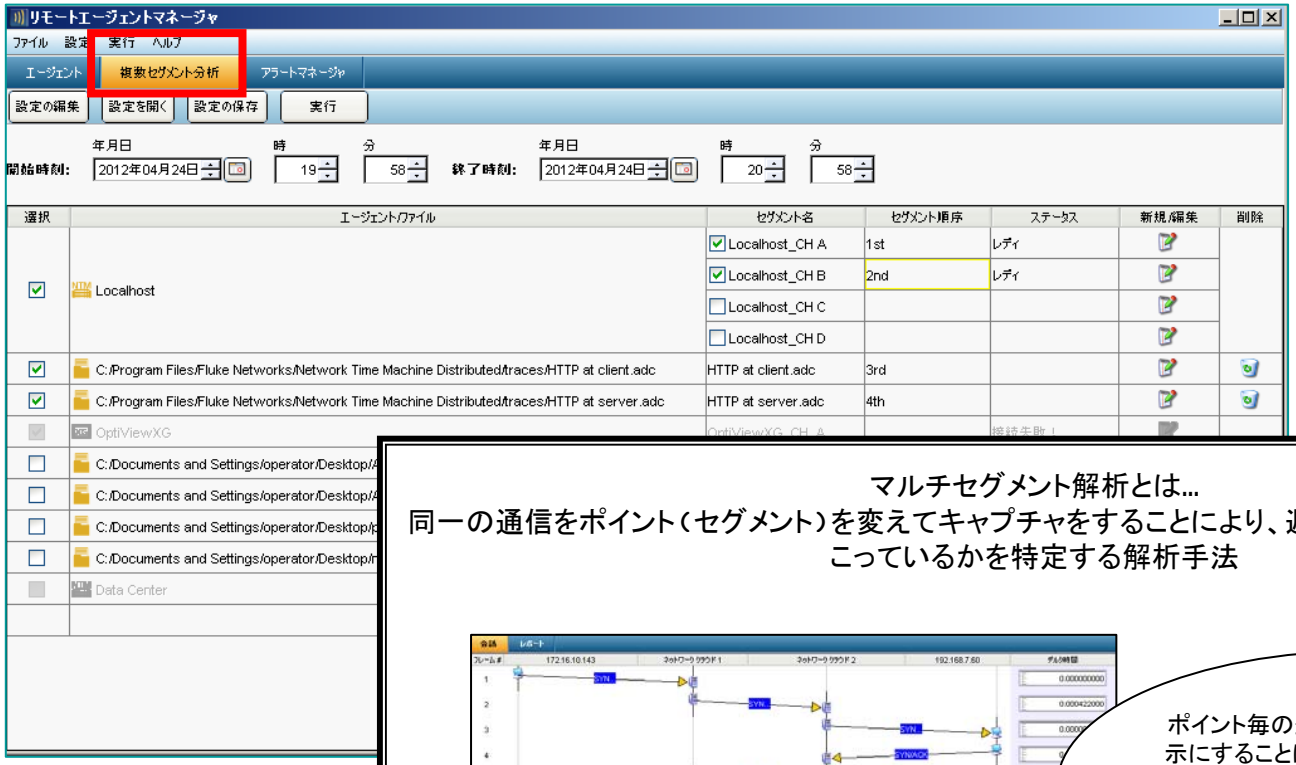


【サポートCODEC】

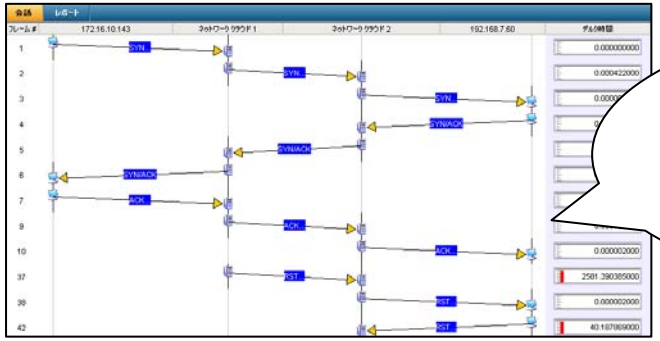
- Audio CODECs include G711(U-law, A-law), G.722, G.723, G.726, G.729, GSM Mono, MPEG1 and MPEG2
- Video CODECs include JPEG (411, 422, 111), H.261, H.263 (Mode A, Mode B), H.264 (Baseline, Main, Extend), MPEG2-TS (type: 14), MPEG2 layer II (type: 33), MPEG4 and iLBC

複数セグメント解析

他のNTMエージェントやトレースファイルとのマルチセグメント解析が可能

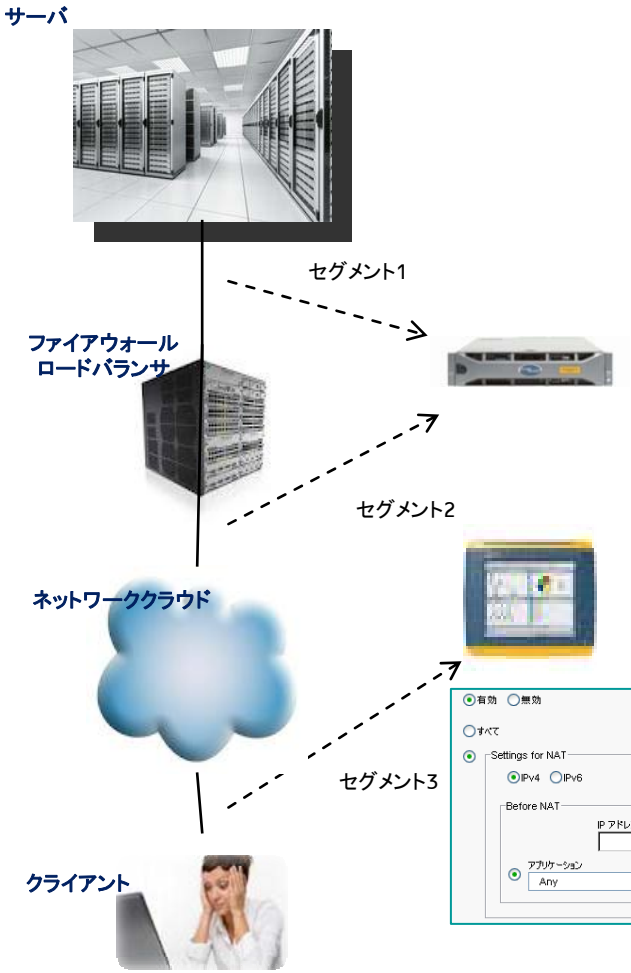


マルチセグメント解析とは...
同一の通信をポイント(セグメント)を変えてキャプチャをすることにより、遅延やロスがどのポイントで起こっているかを特定する解析手法



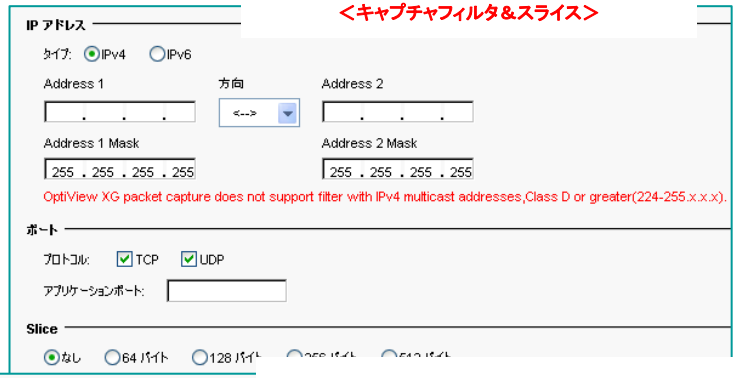
ポイント毎の通信をひとつのラダーで表示にすることにより通信の可視化を実現

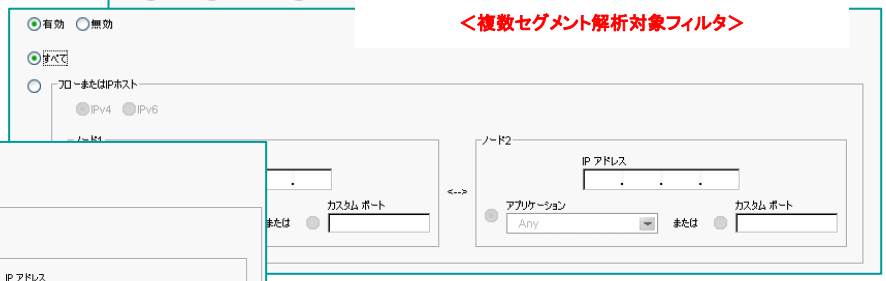
複数セグメント解析手順

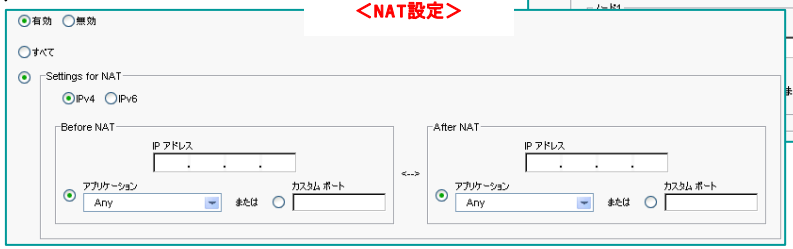


①RAM上でエージェントやファイルを特定
- Network Time Machine
- OptiView XG
- トレースファイル

②解析対象の事前設定
- フィルタ&スライス
- 複数セグメント
- 複数ティア
- NAT



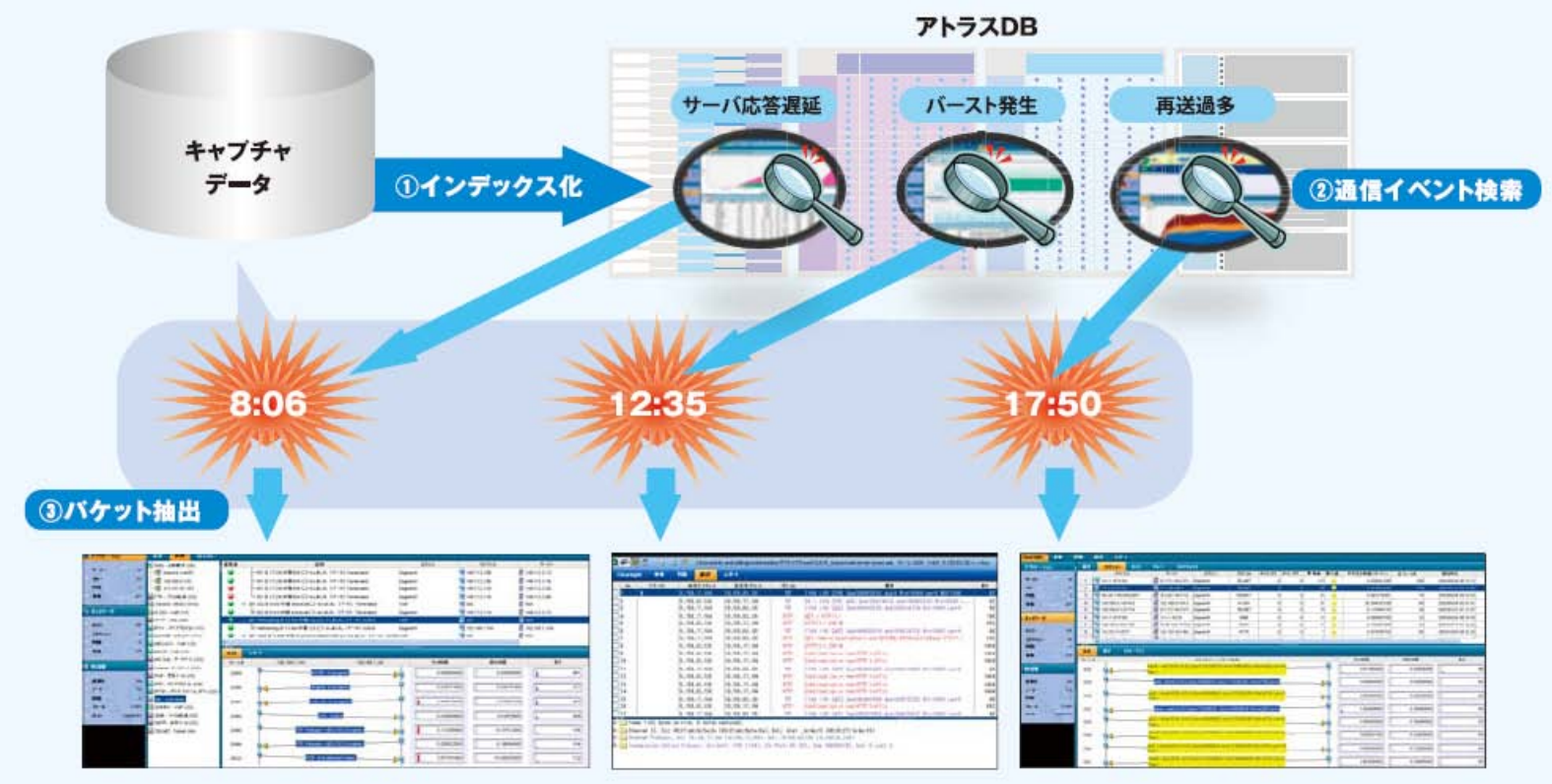




③キャプチャ開始、停止時刻を設定し、実行

アトラス機能

アトラス機能とは、キャプチャした大量のデータをインデックス化し、目的の情報を簡単に検索する機能

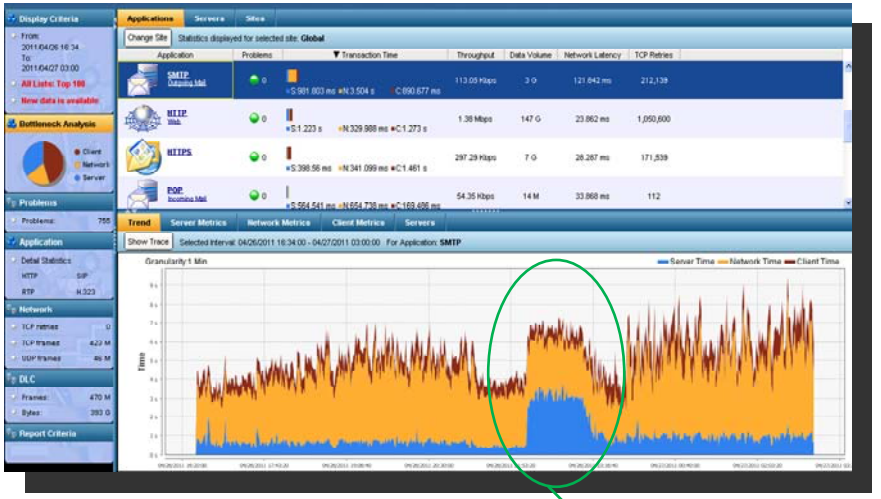


不審な挙動をしているPCや、特定のサーバのIPアドレスやホスト名からそれらの通信履歴を抽出し操作データを追跡することが可能

東陽テクニカ

パフォーマンスボトルネック解析（PBA）

- キャプチャする箇所について
  - クライアント側またはサーバ側のいずれか１箇所でキャプチャしたデータから分析
  - 従来のようにサーバ側とクライアント側の2箇所で同時にキャプチャする必要はなし
- 解析対象
  - TCPトラフィック
- パフォーマンスは下記の項目毎に確認可能
  - 各アプリケーション毎
  - 各サーバ毎
  - 各サイト毎（クライアント毎）
- パフォーマンス要因を3つに分解
  - サーバ時間
  - ネットワーク時間
  - クライアント時間



期間を選択して、
詳細をトレース解析

**サーバやネットワークのパフォーマンスに影響するような
インシデントを検知することが可能**

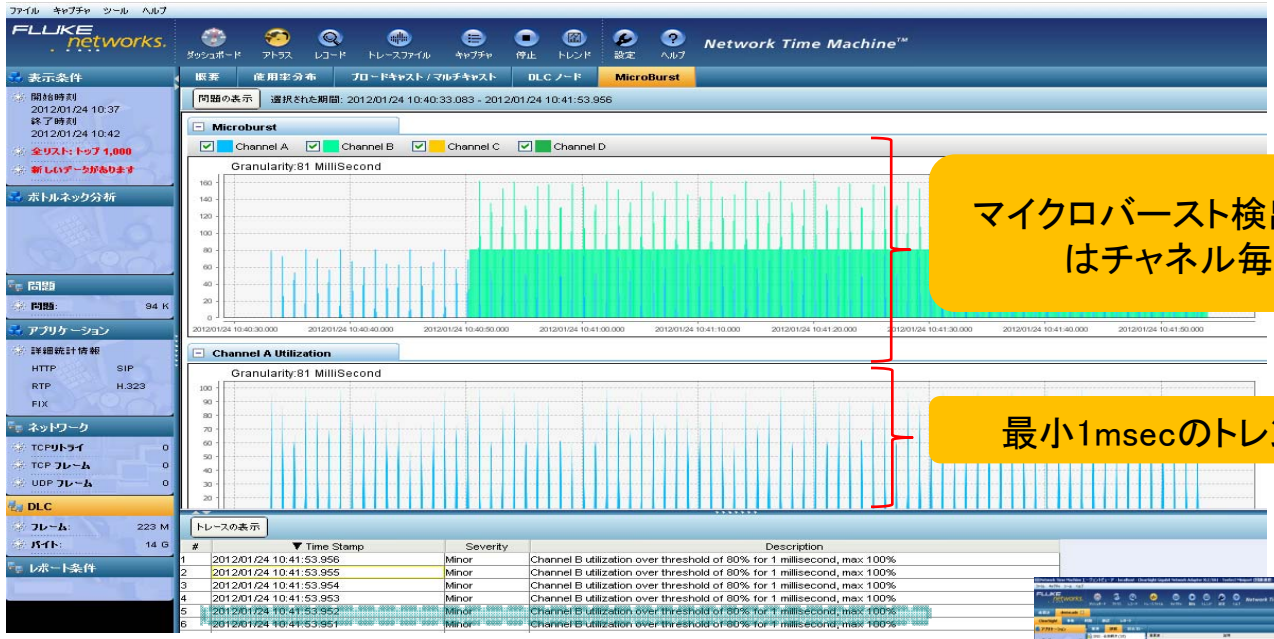
東陽テクニカ

マイクロバーストとは..

- 一般的なモニタやアナライザでは測定できない瞬間的なバーストトラフィック
- 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引き起こす
- マイクロバーストに起因する障害調査にはバーストに関わったトラフィックの分析が必要
- 安定したネットワークの構築のためにはバーストトラフィックの発生状況の把握が重要

マイクロバースト解析

最小1msec分解能でトラフィックトレンドの表示をすることで、
従来のアナライザでは検出できなかった瞬間的なバーストの発生を
検知・解析する機能です。



マイクロバースト検出
はチャネル毎

最小1msecのトレンド表示

“トレースの表示”より
トレース解析が可能

東陽テクニカ

まとめ

- 業界標準ClearSightアナライザをベースとした大容量のLANアナライザ
- テラバイトクラスのHDDに長時間の連続キャプチャが可能
- インシデント発生時のパケットを確実に保全するレコードロック機能
- 大量のデータの中から目的のパケットを効率的に見つけ出すフィルタ/検索機能
- 直感的な日本語GUIとラダー表示による迅速な障害原因の解析
- アトラス解析機能により、不正な通信の特定と抽出を効率化
- マイクロバースト解析による急激なトラフィック増加の検知

いつ発生するかわからないインシデントのパケットログを確実に記録し、迅速に問題解析を行うことが可能！！

東陽テクニカ

NTMに関するお問い合わせ先

- 九州地区代理店
  - 株式会社協栄エレクトロニクス
  - TEL：092(761)6657
  - http://www.kyoei-ele.com/

- 国内総代理店
  - 株式会社東陽テクニカ
  - TEL：06(6399)9771