NetFlowAnalyzerとLG-PROBEを使った解析方法のご紹介

ログイット株式会社
第二事業部
2009.2.6

ログイット株式会社のご紹介

資本金：1億円

設立：１９９９年

所在地：東京都豊島区南大塚

株主：　インフォコム株式会社（１００％）

主な事業内容：

コールセンタ向け音声ロギング装置の販売（NiceLogなど）

情報セキュリティ関連製品の開発・販売　（LSP製品など）

ログイットの情報セキュリティ製品

弊社はネットワークのパケットをキャプチャーして分析する製品を取り扱っています。

- メールアーカイブ
  - ウチノBossメール
  - ウチノBossNEO
- メールアーカイブ＆ウェブログアーカイブ
  - ウチノBossラプター
- フローエクスポータ＆不正PC検知
  - LG-PROBE

3

“ウチノBossメール”の特徴

- メールアーカイブ専用のシンプルでリーズナブルなオールインワン・アプライアンスです。
  - Eメールの保存と監査（検索）に特化したオールインワン・システムです。
  - 小規模サイトから1日平均2万通程度のメールを利用しているサイト向けまで、利用規模に応じた複数のラインアップをご用意。
- **かんたんな導入**
  - パケット・キャプチャ型であるため、既存メールシステムやクライアントPCに手を加える必要がなく、かんたんに導入が可能です。
  - パッシブ接続タイプであるため、障害発生時も他システムに影響を与えません。
- **非常に高いコストパフォーマンス**
  - 最小モデルは、市場最安値クラスです。
  - 他モデルも他社類似製品と比べ、非常に高いコストパフォーマンスを誇ります。
  - ユーザ数や、メール保存数でのライセンスは一切発生しません。

4

製品仕様

製品型式	UBM160-R	UBM250-T	UBM250-R	UBM500-R
アーカイブ規模（平均）※注1	5千通／日（500MB）	1万通／日（1GB）		2万通/日（2Gバイト）
アーカイブ規模（ピーク時）	750Mバイト／日	1．5Gバイト／日		3Gバイト/日
機器仕様				
筐体タイプ	1Uラック（ミニ）	タワー	1Uラック	
ネットワークインターフェース	4Port（管理Port×1,キャプチャPort×1）	2Port（管理Port×1,キャプチャPort×1）	3Port（管理Port×1,キャプチャPort×2）	
ディスク	160G*1	250GBx2（RAID1）		500GBx2（RAID1）
光学ライブ	なし	あり		
電源	シングル			
筐体イメージ				
主な付属品（注2）	ラック金具	キーボード．／ マウス	ラックマウント･レール	
最大消費電力	220W	370W	328W	
OS	Windows XP Pro	Windows Server 2003 SBS	Windows Server 2003 std	
標準価格（税抜き）	￥498．000	￥960．000	（お問い合わせください）	
提供保守サービス	センドバック保守のみ	センドバックおよびオンサイト保守		

デスクトップ（PC)版もございます。(¥498,000円）

※注1：100KB/通のサイズの場合

※注2：キーボード／マウス／ディスプレイが別途必要になります。

価格・仕様は予告なく変更される場合があります．

LG-Probe概要

- 弊社が開発したトラフィック管理／セキュリティプローブです。
- オープンソースをベースとして開発し、高品質／低コストな機器です。
- OEM･ソフトウェアでのご提供も可能です。(設定画面など変更可能)

- **先進のネットワーク･モニタリング機能**
  - **sFlow** / NetFlow エクスポータ
  - Rmon1/2 プローブ

- その他機能
  - ► 充実したセキュリティ機能
    - 不正PC排除機能（MACアドレス検疫）
    - Winny(1,2)通信検知機能
    - 業務外ウェブへのアクセス検知機能
  - ► 侵入検知(IDS)機能（オプション）

今回はNetFlowAnalyzerとLG-PROBEの組み合わせのソリューションに焦点をあててご紹介させていただきます。

LG-Probeの仕様（小型）

- 対応帯域： 100Mbps
  - Flowおよびセキュリティ機能：20－30Mbps
  - Flowのみ：70－80Mbps

  （無線LANモニタは別途）
- ハードウェア仕様
  - CPU:VIA EDEN
  - Memory: 512MB
  - Disk：コンパクトフラッシュ 128MB
  - LAN：10/100Mbps 2ポート
  - FAN、HDDはありません。（超静音）
  - 動作温度：0～60℃ （推奨：5-35）
  - サイズ：W170/H123/D56mm
  - 消費電力：20W
- 基本ソフトウェア
  - Kernel 2.6.20-1
  - BusyBox 1.4
  - NET-SNMP 5.4（v1，v2c、v3暗号化対応）
  - WEBサーバ(Apache 1.33)
  - FTP,TELENET,SYSLOG
  - DHCP／NTPクライアント
  - WEB設定、端末設定機能
- 簡易管理用ソフトウェア付属

パソコン用の液晶モニタ、KBを接続して設定可能です。
また、シリアル端末からも設定が可能です。

※ハードウェアの仕様は予告なく
変更される場合があります。

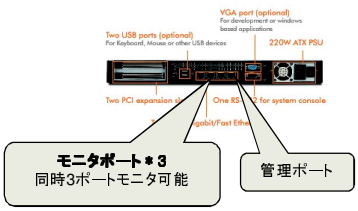
LG-Probeの仕様（中型）

- 対応帯域： 10/100/1000Mbps
  - Flowおよびセキュリティ機能利用時：90Mbps
  - Flowのみ：300Mbps（1モニタ時）

  （無線LANモニタは別途）
- ハードウェア仕様
  - CPU: Intel ペンティアム2.8Ghz
  - Memory: 256MB
  - Disk：コンパクトフラッシュ 128MB
  - LAN：10/100/1000Mbps 4ポート
  - 動作温度：5-40度
  - サイズ：W430/H44/D390mm
  - 電力：220W（最大）
- 基本ソフトウェア等
  - 小型版と同一

▲ Front

▼ Back



※但し、結果は利各ポート
の合計で出力されます。

※ハードウェアの仕様は予告なく
変更される場合があります。

トラフィック情報とFlow情報

- トラフィックの情報ではポートのネットワーク使用率が確認できる

  例：RMON

- Flow情報（NetFlow/sFlow）では通信している端末のIPアドレスやTCP/UDPのポート番号まで確認できる

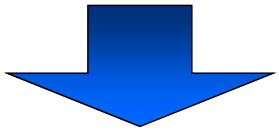
  例：NetFlow、sFlow

9

Flow管理の使用用途

通常の使い方

- ネットワーク回線の使用率を確認
- ネットワーク帯域を占有している端末やアプリケーションを特定

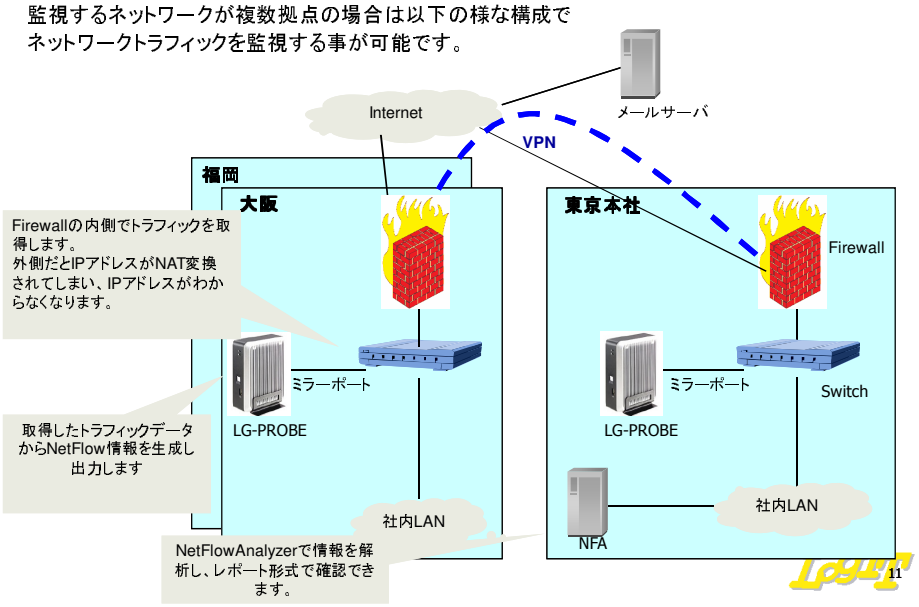


データの見方を変えることによって
もう少し実用的な使い方ができないか？

10

想定したネットワークの接続図

監視するネットワークが複数拠点の場合は以下の様な構成で
ネットワークトラフィックを監視する事が可能です。



11

使用した機器の価格

- ミラーポート付きSwitch
  - HP社　ProCurve Switch 1700-8
  - ¥13,545×3 (拠点数)=¥40,635
- LG-PROBE
  - Logit社　LG-PROBE LGP-10TI（小型機）
  - ¥200,000×3(拠点数)=¥600,000
- Flowコレクタ
  - NetFlowAnalyzer10論理ライセンスパック
  - ¥164,000

合計¥804,635

12

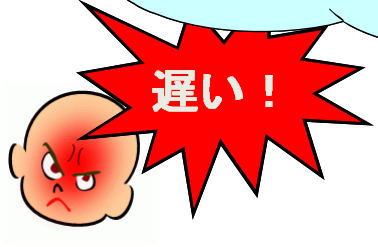
事例1：ネットワーク遅延の調査

13

ネットワーク遅延の調査

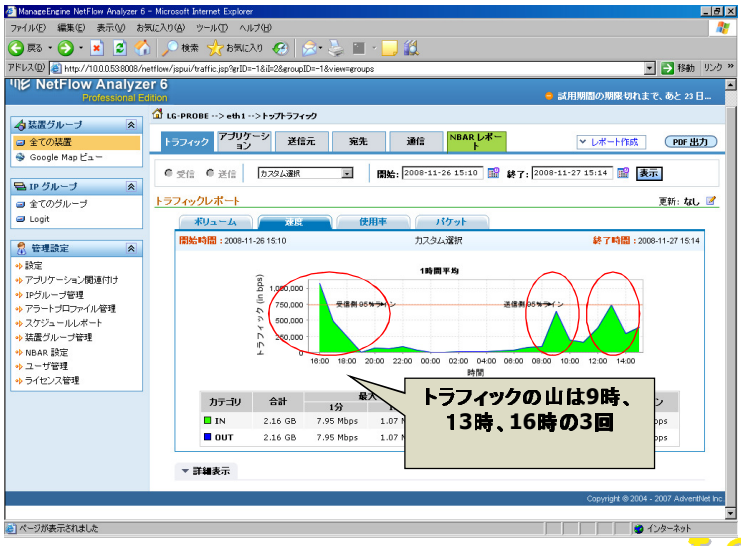
問題：お昼や夕方になるとネットワークが遅くなると苦情が来た
その時間帯のプロトコル分布を見るとHTTPの通信がほとんどだった

- それは業務に必要なトラフィックなのか？
- 必要でないとしたらどのような方策が取れるか？



14

ネットワークの利用状況



15

Webサーバアクセスログの見方

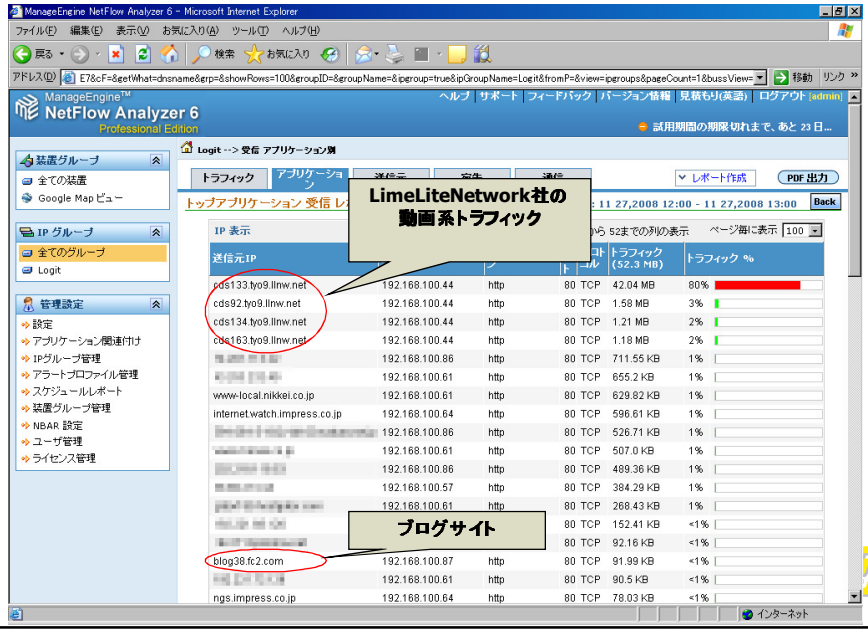
社員のWebサーバのアクセスの履歴を見てみよう！

NetFlowAnalyzerで収集したデータに以下の操作を実行

- トラフィックデータからHTTPの通信（TCP Port80番）を選択
- IPアドレスで通信量の多い順にソート
- DNS解決実行で、IPアドレスからドメイン名に変換

16

Webサーバアクセスログリスト（HTTP）



17

ネットワーク遅延の解決

問題：お昼や夕方になるとネットワークが遅くなると苦情が来た。その時間帯のプロトコル分布を見るとHTTPの通信がほとんどだった

結果：解析してみた結果、動画を扱っているサーバへの通信が大半だった為、あまり好ましくないトラフィックだと判明した

対応：後日、HTTPサーバへのアクセスリストを作成し、社内に公開＆注意喚起したところ、トラフィックは収束した

18

事例2：メール調査

19

メール調査

問題：監査の対象として社外のメールサーバを使用しているか調査する必要がある。アウトソースしているメールサーバ以外の使用を確認したい

- 確認したあとどうする？
- Webメールは使用されているか？

セキュリティ監査が入るから
調査して、対策しておいて！

20

メールサーバアクセスログの見方

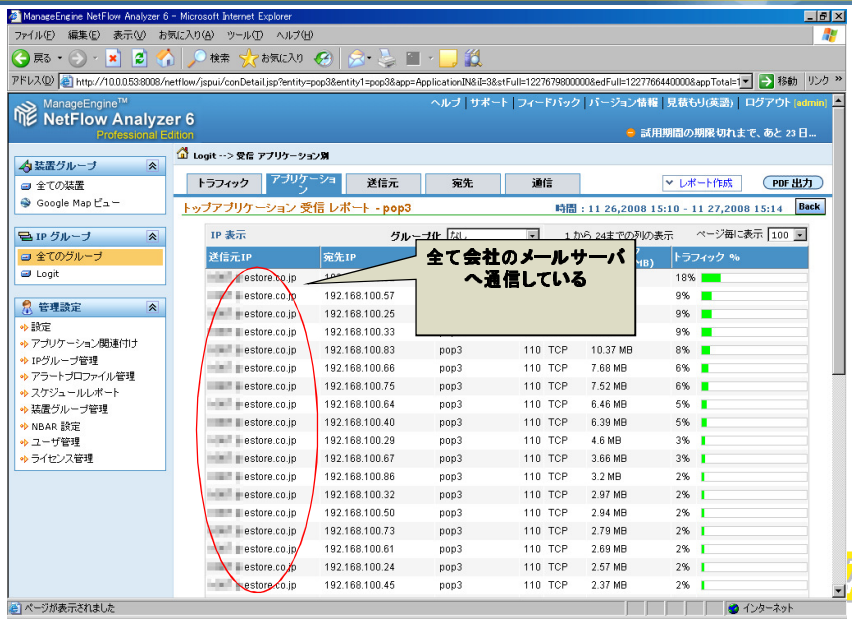
社員のメールアクセスの履歴を見てみよう！

NetFlowAnalyzerで収集したデータに以下の操作を実行

- トラフィックデータからPOP3の通信（TCP Port110番）を選択
  ※POP3Sの通信なら（TCP Port995番）
- IPアドレスで通信量の多い順にソート
- DNS解決実行で、IPアドレスからドメイン名に変換

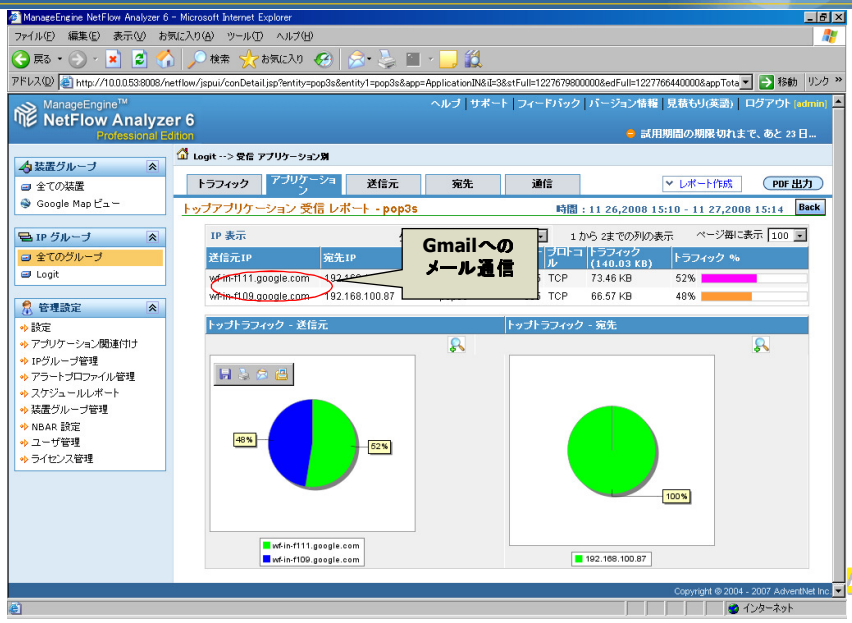
21

メールサーバアクセスログ（POP3）



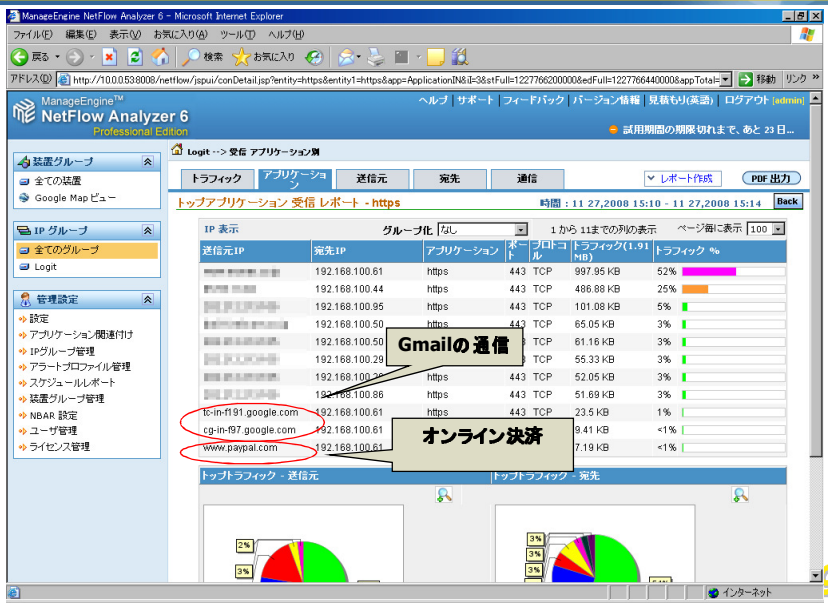
22

メールサーバアクセスログ （POP3s）



23

Webサーバアクセスログ（HTTPS）



24

メール調査　解決編

問題：監査の対象として社外のメールサーバを使用しているか調査する必要がある。
アウトソースしているメールサーバ以外の使用を確認したい

結果：ほとんどの社員は正規のメールサーバとのみ通信していることがわかった。しかし、一部の社員はプライベートなメールサーバを使用している事がわかった。

対応：後日、Firewallにて正規のメールサーバ以外のメール通信（TCP_Port25,110,587,995）を拒否するルールの追加を行った。

またWebメールを使用している社員に対して個別に注意すると共にWebフィルタ装置の導入を検討している。

25

まとめ

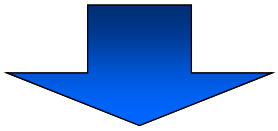
既存のネットワーク環境に1セット導入するとお手軽にネットワークの状況がわかります。

- ネットワークの詳細な使用状況の把握が可能です。
  - ネットワークの使用率
  - 個別サーバ（メールサーバ等）の使用状況
- ネットワーク使用の監査に使用できます。
  - 許可していないメールサーバの監査
  - 適切でないWebサーバの監査
- ピンポイントのトラブル調査に使用できます。

26

更に詳しく調査したい場合は

＜不正予防・事後対策＞
不正が発生した場合に備えて、証拠（証跡）をとっておきたい。
メールから情報が漏洩することを防ぎたい。不正の抑止効果があるためメールのアーカイブを取得したい。
取引先からの指示で、とにかくメールを保存しておく必要がある。ただ、メールサーバは外部にホスティングしている。



ウチノBossシリーズ（メールアーカイブ製品）で
メールの保存、検索で対応

27

おわり

ご清聴ありがとうございました

28