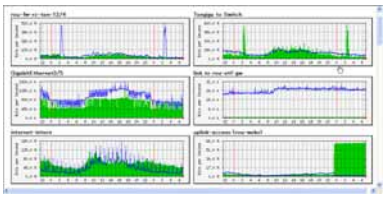
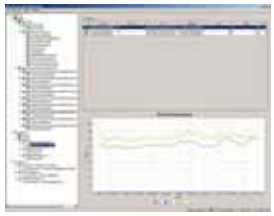
T25:フローベースのトラフィック計測と解析
Part Ⅰ フロー技術とプロトコル

進藤　資訓
ファイブ・フロント(株)
Chief Technology Officer
mshindo@fivefront.com

従来のネットワーク管理

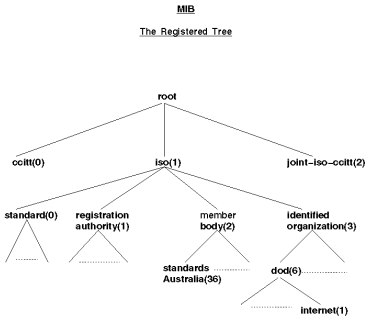
- SNMPベース
  - MRTG
  - HP/OV
  - …
- RMONベース





SNMPが提供するトラフィック情報

- (論理) インターフェースを通過したパケット数やバイト数
  - IfInUcastPkts, IfOutUcastPkts
  - IfInOctets, IfOutOctets
  - …
- “インターフェースベース”のネットワーク管理



SNMPが提供してくれないもの

- 誰がトラフィックを流しているのか？
  - End to End トラフィックの把握
- どのようなトラフィックを流しているのか？
  - アプリケーションの把握
- ネットワーク型攻撃のすばやい検知

新しいネットワーク管理手法

- “フローベース”のネットワーク管理！
  - End to End の情報
  - アプリケーション
  - AS の情報
  - …
- 今まで見えていなかったネットワークの真の姿が見えてくる！！

フロー技術

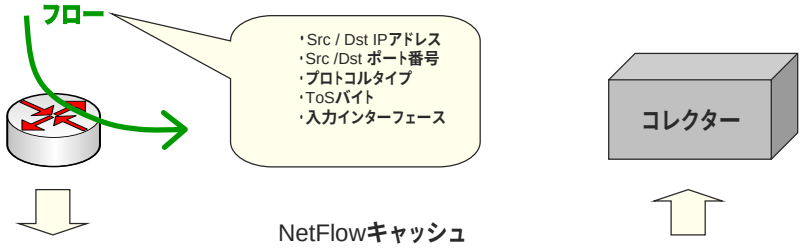
- NetFlow
  - Ciscoが開発した技術
  - Cisco, Juniper, AlaxalA, etc.
- sFlow
  - InMonが中心となって開発した技術
  - Foundry, Extreme, AlaxalA, Force10, HP, etc.
- IPFIX
  - IETFによる標準プロトコル
  - マルチベンダー
  - NetFlow V9がベース

適用分野

- サービス・プロバイダ
  - アプリケーションの把握
  - ピアリングの最適化
  - セキュリティー
  - QoS
  - 将来予測
  - 課金
  - …
- エンタープライズ
  - アプリケーションの把握
  - ユーザー挙動の把握
  - 攻撃の検知
  - 課金
  - …

NetFlowキャッシュ

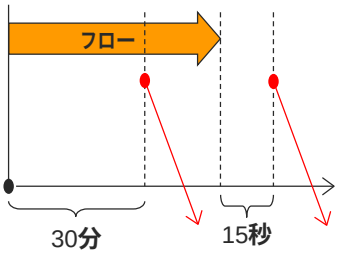
- NetFlowはキャッシュ・ベースのテクノロジー



Src IF	Src IP	Dst IF	Dst IP	Proto	Bytes	…	Active	Idle
10	a.a.a.a	24	x.x.x.x	6	1234		327	4
15	b.b.b.b	24	y.y.y.y	17	23456		1920	25
24	c.c.c.c	3	z.z.z.z	6	5678		54	10

キャッシュなので・・・

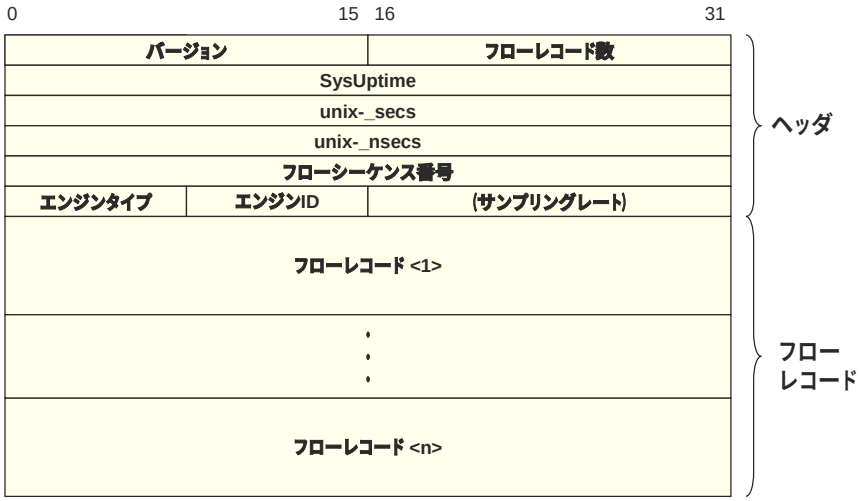
- **いつかはフラッシュする必要がある**
  - Inactive Timer（default = 15**秒**）
  - Active Timer（default = 30**分**）
  - TCP FIN or RST
  - **キャッシュが一杯になった時**
- **実装依存**



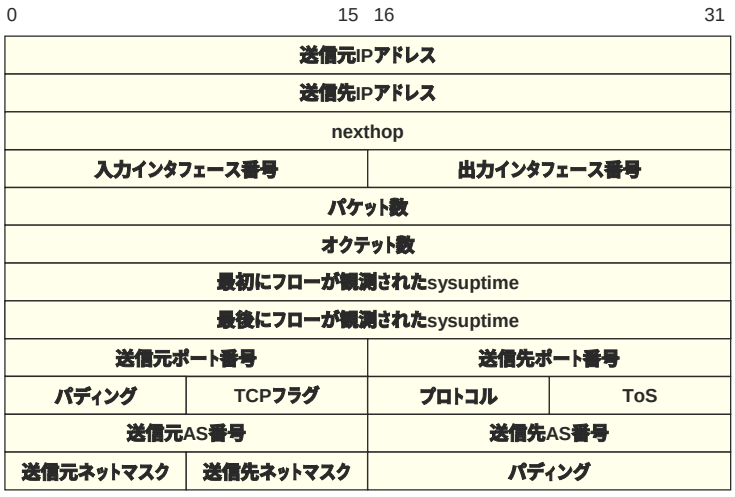
NetFlow**バージョン**

バージョン	特　　徴
1	最初のバージョン。現在ではほとんど使われていない。
5	最も多く使われているバージョン（と思われる）。BGP ASとフローシーケンスをサポート。
7	Catalyst Switchシリーズのための拡張。
8	アグリゲーションをサポート。
9	テンプレートベース。IPFIXのベース。

NetFlow V5 PDU



NetFlow V5 フローレコード



NetFlow V9

- テンプレート・ベース
- RFC 3954（Informational）
- IPFIX のベースになった
  - 詳しくはのちほど IPFIX のところで説明

NetFlowパフォーマンス

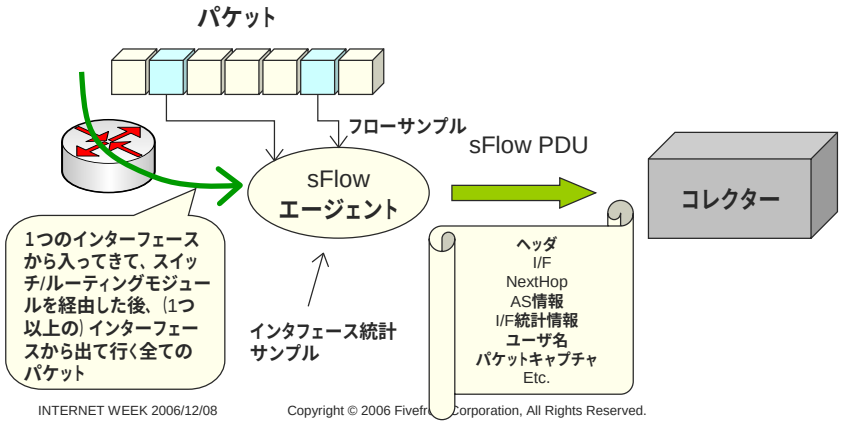
- オーバーヘッド
  - パケットの分類
  - エクスポート処理
    - 多くのCiscoハードウェアはパケットの分類をハードウェアで処理することができる
- バージョン（V5, V8, V9）にはほぼ非依存
- サンプリングは有効！
- 例）
  - Cisco 12000、100:1サンプリングの場合、7〜15%程度のCPU負荷増

sFlow

- NetFlow（Cisco流）への反発??
- RFC 3176 [sFlow V4]（Informational）

サンプリング

- sFlowは“サンプルベース”のテクノロジー
  - NetFlowのようなフローキャッシュは持たない



sFlowの特徴（vs NetFlow V5）

- レイヤ2の情報を取得できる
- IPv6を扱える
- IP以外のプロトコル（IPX、AppleTalk、等）を扱える
- パケットキャプチャができる
- BGP関連機能のサポート
  - BGP Next Hop
  - Community
  - AS PATH
  - Local Preference
- カウンタのサポート
- 軽い Agent（エクスポータ）実装

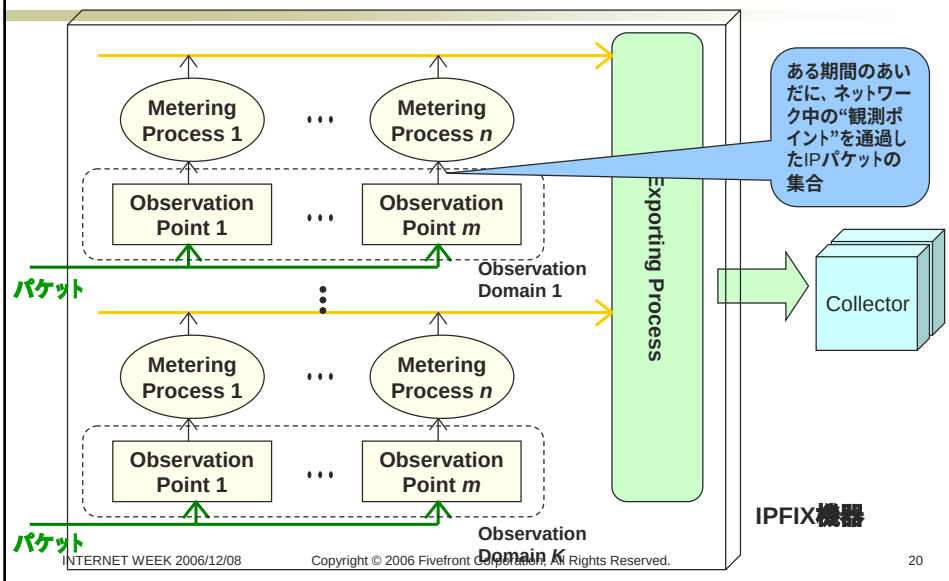
sFlowのバージョン

バージョン	特　　徴
2	最初のバージョン
4	BGP community の追加（RFC 3176）
5	CPU/メモリ使用率、BGP nexthop、MPLS、NATサポート追加。Vendor-specific レコードで拡張可能。

IPFIX

- IP Flow Information eXport
  - draft-ietf-ipfix-architecture-12.txt
  - draft-ietf-ipfix-protocol-23.txt
  - draft-ietf-ipfix-info-14.txt
- **歴史**
  - 49th IETF Dec. 2000, (rtfm2 – realtime traffic flow measurement 2 BOF)
  - 51st IETF August 2001 (ipfx BOF)
  - **候補**
    - sFlow, NetFlow, LFAP, etc.
- **関連WG**
  - PSAMP（Packet Sampling）WG
    - 54th IETF July 2002

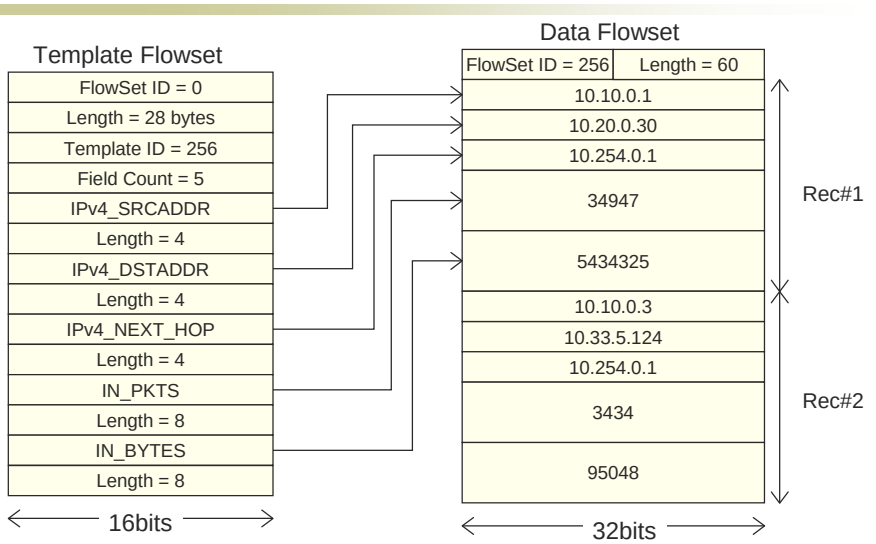
IPFIX アーキテクチャ



テンプレート

- テンプレート・セット
  - データセットの“設計書”のようなもの
  - 拡張性を持たせる手段
    - TLV でも実現できたが、オーバーヘッドが問題
- オプション・テンプレート・セット
  - フローには直接関係ないメタな情報を伝える

Template Flowset & Data Flowset の例



IPFIX の新機能（NetFlow V9と比較して）

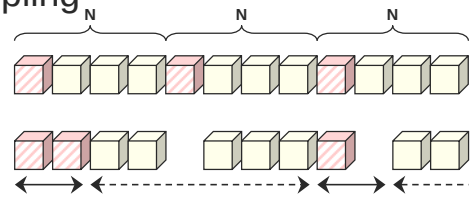
- SCTP/PR-SCTPが必須のトランスポートになり、UDP・TCPがオプションに
- フィールド指定フォーマットの導入
  - ベンダー拡張が可能
- 可変長IEのサポート
- テンプレートを明示的に消去するTemplate Withdraw Messageの導入
- セキュリティー
  - IPsec or TLS（オプション）

サンプリング

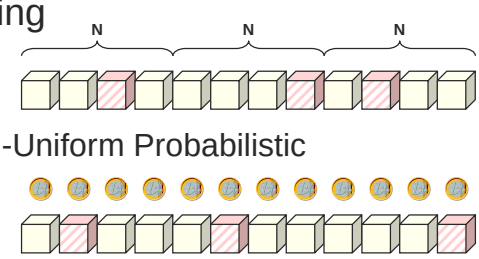
- 目的
  - エクスポータのCPUやメモリの節約
  - ネットワーク帯域の節約
  - コレクターの性能の節約

サンプリング方式

- Systematic Sampling
  - Count-based
  - Time-based



- Random Sampling
  - n-out-of-N
  - Uniform or Non-Uniform Probabilistic



サンプリング

- **最適なサンプリング値は？？**
  - **フローの使用目的によって異なる**
  - **ハードウェア･アシストの有無**
  - **典型的なのは**100～**数**1,000
- **当然失われるものもある**
  - **フロー数 (攻撃)**
  - **スキャン等の振る舞い**
  - **・・・**

商用コレクター製品（アルファベット順）

- AdventNet – NetFlow Analyzer (N)
- ARBOR Networks – peakflow (N, S)
- Foundry Networks – IronView (S)
- GenieNRM – GenieATM (N, S)
- InMon – InMon Traffic Sentinel (S, N)

フリーコレクター製品（アルファベット順）

- CAIDA – cflowd (N)
- flow-tools & FlowScan(N)
- InMon – sflowtools (S), sFlowTrend (S)
- NFDUMP & NfSen (N)
- ntop – ntop (N, S, I)
- Many More!!!

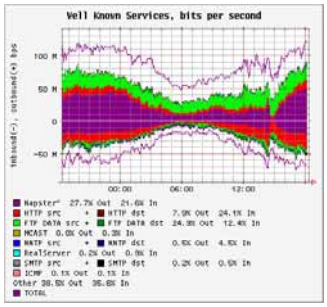
flow-tools

- **ツールの集合**
  - flow-{capture, cat, dscan, expire, export, fanout, filter, gen, header, import, log2rrd, mask, merge, nfilter, print, receive, report, rpt2rrd, rptfmt, send, split, stat, tag, xlate}
- NetFlow V1, V5, (V6), V7, V8
- **例)**

```
% ./flow-receive 0/0/9990 | ./flow-print | head -10
Sif SrcIPaddress     Dif DstIPaddress     Pr SrcP DstP Pkts     Octets
60  206.204.84.9     00  10.0.135.63      06 15   5f0  2        88
00  10.0.135.63      60  206.204.84.9     06 5f0  15   16       787
60  206.204.84.9     00  10.0.135.63      06 15   5f0  13       1742
00  10.0.155.25      60  204.62.245.167   06 50   bae5 15       948
```


FlowScan

- cflowd / flow-tools / argus / lfapd (collector) + RRD (D/B) + RDDTools (visualization)
- Platform : UNIX



http://www.caida.org/tools/utilities/flowscan/index.xmlより引用

GenieATM 6000

- NetFlow V1, V5, V7, V9
- sFlow V4, V5
- NetStream
- **アプライアンス**

http://www.fivefront.com/products/genie/atm6000/function.html**より引用**

ARBOR peakflow

- NetFlow V5, V7, V9
- sFlow V2, V4, V5
- **アプライアンス**

http://www.arbornetworks.com/products_x.php**より引用**

InMon Traffic Sentinel

- sFlow
- NetFlow V1, V5, V7, V9
- **ソフトウェア**

http://www.msol.co.jp/it/Inmon/i-tokucho.html**より引用**

参考資料

- NetFlow **関連情報**
  - http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html
- NetFlow V9 RFC **日本語訳**
  - http://www.fivefront.com/technology/flow/rfc3954-jp.html
- sFlow **関連情報**
  - http://www.sflow.org/
- IPFIX
  - http://www.ietf.org/html.charters/ipfix-charter.html
- **各種ツール**
  - http://www.switch.ch/tf-tant/floma/software.html