運用管理
から
フロープロトコル解説

丸紅情報システムズ株式会社
ﾌﾟﾗｯﾄﾌｫｰﾑ&ﾈｯﾄﾜｰｸ事業本部
出野 真也
Ideno-Shinya@marubeni-sys.com

アジェンダ

- 運用管理おさらい
  - 構成管理
  - 障害管理
  - 性能管理
- トラフィック・フロー管理～フロープロトコルの解説
  - トラフィック・フロー管理
  - フロープロトコルの解説

    SNMP / RMON2 / ***sFlow*** / sFlow802.11 / Cisco NetFlow / Juniper J-Flow / IPFIX / HP Extended RMON(XRMON) / Riverstone LFAP
- フロー管理ソリューション・プロダクト

運用管理おさらい

- 運用管理の基本機能

(1) 構成管理

ネットワークを構成している各種構成要素を個々に管理し、
また、その各種構成要素の接続の状態をトポロジーマップとして表示

(2) 障害管理

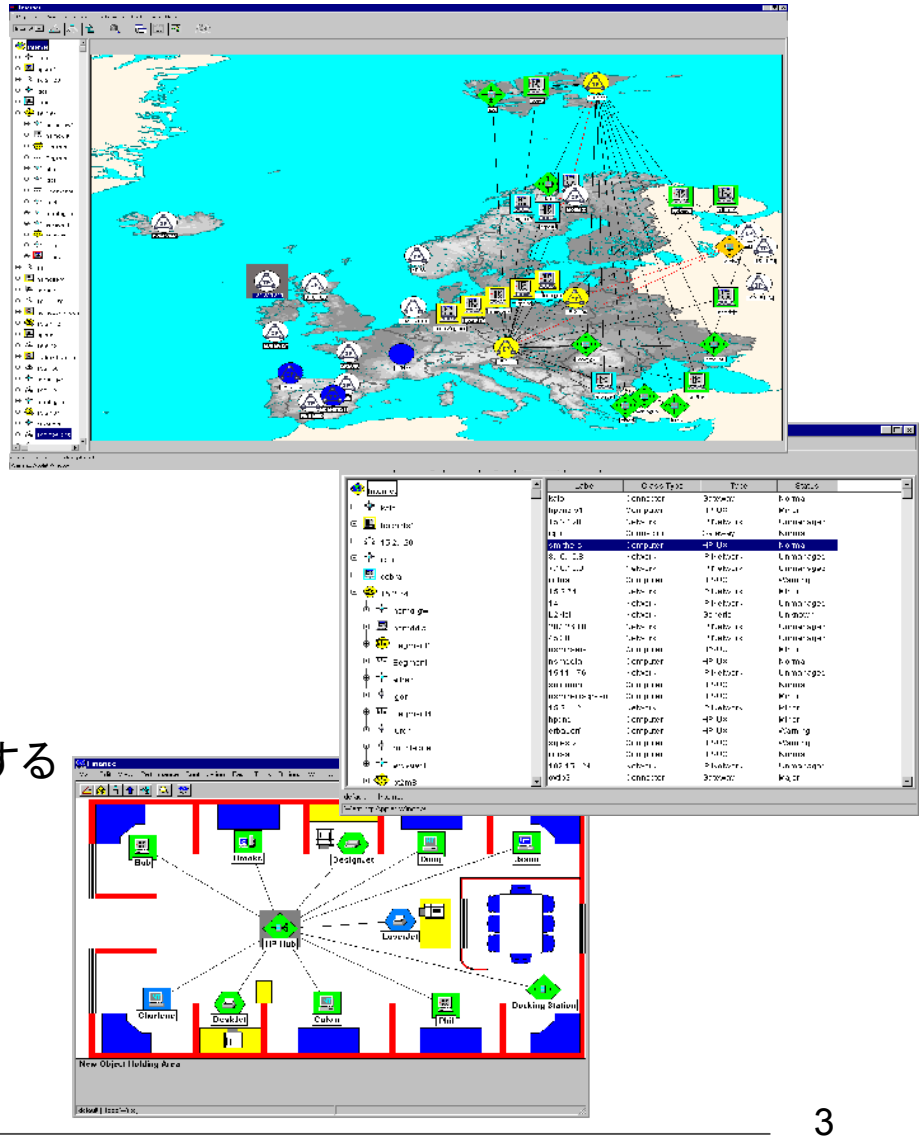
各種構成要素に対しステータス確認を行い障害を検知する、
あるいは、各種構成要素からのイベントを受信することなどによって
障害を検知

(3) 性能管理

ネットワーク・システムの性能・パフォーマンスを定量的に測定

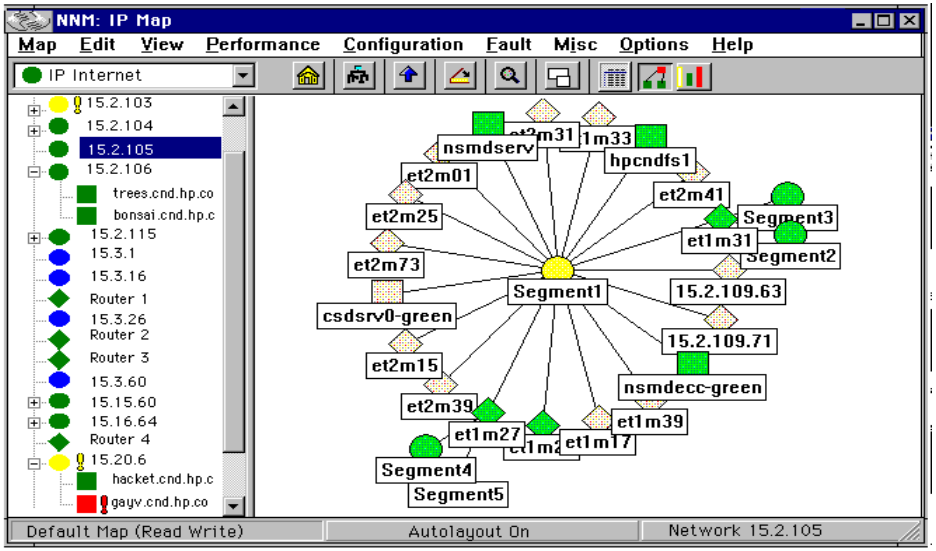
運用管理おさらい

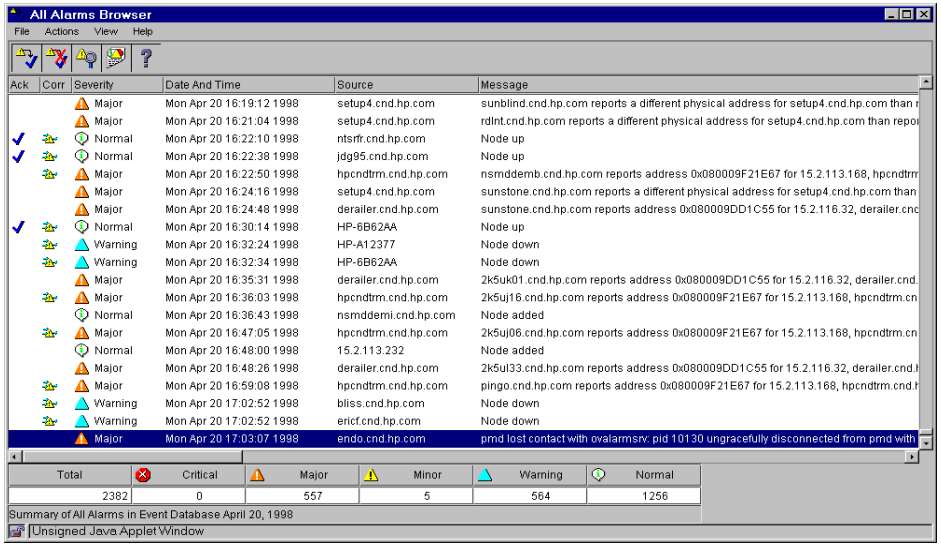
- 構成管理
  - 管理内容
    - 構成機器の種類
    - トポロジー・ノード間接続状態の把握
    - オート・ディスカバリとダイナミック・マップ
    - マップの自動更新
      （ネットワークの変更も自動的に把握）
    - マップのカスタマイズ
    - 管理・非管理の指定
  - 利点
    - 管理者の負担を軽減し、構成管理を容易にする
    - 最新のネットワーク構成の把握
    - 問題の発生箇所の素早い特定



運用管理おさらい

- 障害管理
  - 管理内容
    - ネットワークの状態のモニタリング
    - 監視対象の障害検知
    - イベント通知
    - イベントに対する自動アクション
    - しきい値のユーザ定義
  - 利点
    - 中央で全てのイベントを集中的に管理
    - 問題の発生箇所の素早い特定と自動対応

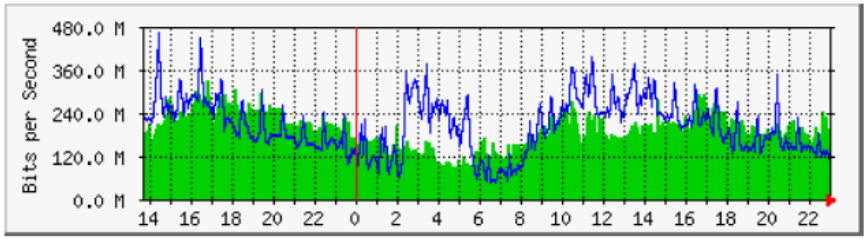




運用管理おさらい

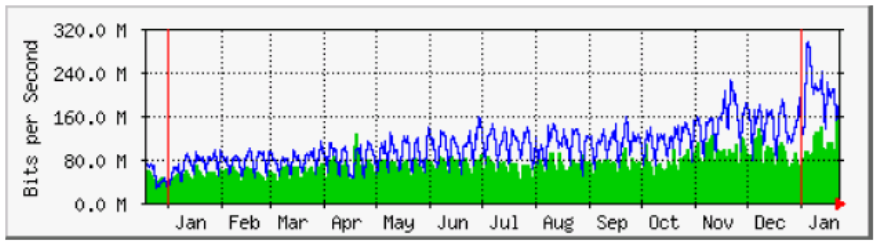
- 性能管理
  - 管理内容
    - SNMP-MIB情報の収集、各種レポート化
    - 測定値（Pingの応答、SNMP-MIB値）の収集
    - 各種レポート化
    - 問題箇所の把握
    - しきい値による性能変動の把握
    - 統計値による分析・障害管理
  - 利点
    - ネットワーク・システムの性能を定量的に把握
    - ネットワーク・システムの性能を一定レベルに維持
    - 使用動向の把握・予測・計画

`Daily' Graph (5 Minute Average)



	Max	Average	Current
In	329.2 Mb/s (7.7%)	192.0 Mb/s (4.5%)	177.4 Mb/s (4.1%)
Out	460.4 Mb/s (10.7%)	200.1 Mb/s (4.7%)	102.9 Mb/s (2.4%)

`Yearly' Graph (1 Day Average)



	Max	Average	Current
In	177.0 Mb/s (4.1%)	70.4 Mb/s (1.6%)	176.0 Mb/s (4.1%)
Out	294.0 Mb/s (6.8%)	106.3 Mb/s (2.5%)	192.1 Mb/s (4.5%)

“性能管理” から “トラフィック・フロー管理” へ

トラフィック・フロー管理

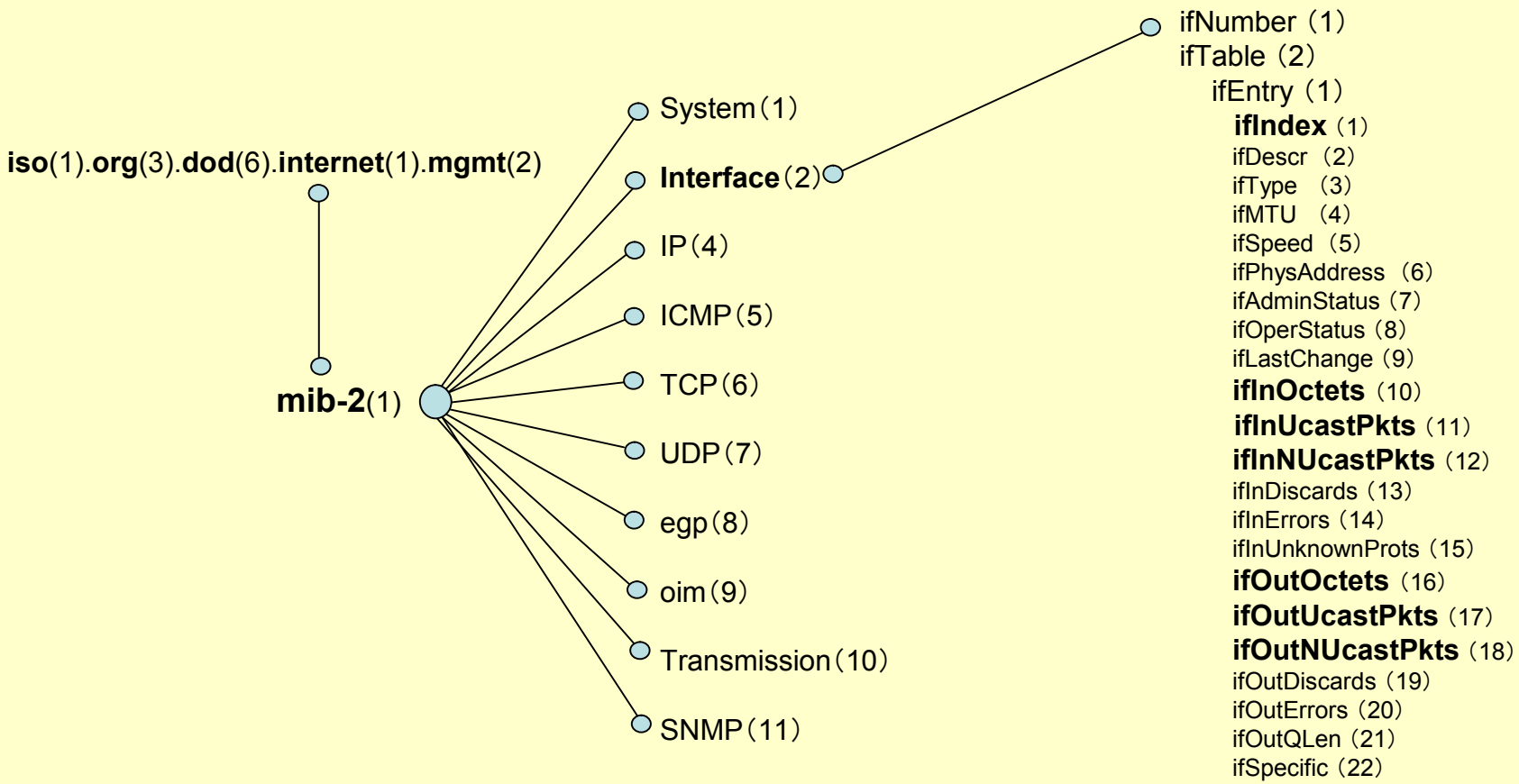
- トラフィック・フロー管理
  - 誰がネットワークを使っているか？誰が何をしているか？
  - 誰と誰、何処と何処が、どのような通信（プロトコル）を、どの程度（バイト数、フレーム数）行なっているか？
- フロープロトコルの解説
  - SNMP
  - RMON/RMON2
  - sFlow / sFlow 802.11
  - Cisco NetFlow
  - Juniper J-Flow
  - IPFIX
  - HP XRMON / RiverStone LFAP
  - sFlow vs NetFlow

SNMP

- SNMP（Simple Network Management Protocol）
  - 1988年の開発以降、インターネットワーク管理のデファクト・スタンダード
  - 管理対象となるネットワーク機器に常駐するSNMPエージェントと、管理する側のSNMPマネージャとのUDP通信により実現
  - SNMPエージェントは監視対象機器の情報を、「MIB（Management Information Base）」と呼ばれる「管理情報ベース」に蓄積
  - SNMPマネージャはSNMPエージェントが取得したMIBの内容から、監視対象機器の状態を統計値として判断
    - フレーム数、バイト数、エラーフレーム数、帯域幅使用率 etc
- 基本はインターフェース/VLAN単位での統計値の収集
  - ➔ MIB Ⅱ (RFC1213) Interface Group / IF-MIB(RFC2233)のHighCounter（64bit）…etc
  - その他の統計値はRFCにて各種拡張・プライベートMIBにて拡張
    - DOT3、DOT5、CPU使用率、温度　など
- トラフィック情報は？誰と誰がどのような通信を行なっていたか？
  - SNMP(MIB2)では、**トラフィックの内容に関する情報・統計値は把握できない**
    - ➔　RMON / RMON2 への拡張

SNMP（MIB OID）

- SNMP MIB Ⅱ インターフェース・グループ



RMON2

- RMON (Remote Network Monitoring)
  - 遠隔地(Remote)にあるLANのトラフィックなどの通信状況をモニタリングする機能。
    SNMPの拡張機能として提供され、統計値はMIBデータベースに蓄積される。
    - RMON（RFC1757） ➔ レイヤー2以下（物理層、データリンク層）を管理
    - **RMON2**（RFC2021） ➔ レイヤー3以上を管理。
      ICMP/IP/UDP/TCPなどが管理可能なので、トラフィック分析が可能
- RMON2の問題点
  - RMON2プローブが必要
    - ハイスピードネットワークでは非常に高価：ギガポートのモニターで一台数百万円
    - 特定の範囲のみの管理 ➔ 全社的な管理は不可能
    - 大量のトラフィックに対しては取りこぼす可能性
  - ネットワークトラフィックに対して不十分な情報
    - 特定のプロトコルのみの分析
    - リアルタイム性がない
  - ネットワークパフォーマンスへの影響
    - RMON2情報の収集の為に、プローブとマネージャー間で大量のトラフィック
  - RMON2実装スイッチ
    - RMON2を動作させるとスイッチのパフォーマンスに多大な影響
  - ハイスピード・ネットワークやスイッチング・ネットワークでは適用しづらい

RMON2 (MIB OID)

- RMON2
  - トラフィック情報はMIB値とてカウントされる

＜ RFC2021のRMON2 (.1.3.6.1.2.1.16) のalMatrix (.1.3.6.1.2.1.16.17)の構成 ＞

MIBダンプによるデータより一部抜粋;

mib-2.16.17.1.1.2.1.0.6.4.192.168.71.90.4.192.168.110.100.14 = 343
mib-2.16.17.1.1.2.1.0.6.4.192.168.71.90.4.192.168.110.100.16 = 2762

mib-2.16.17.1.1.2.1.0.6.4.192.168.71.90.4.192.168.110.100.84 = 2762

SourceIPｱﾄﾞﾚｽ　DestinationIPｱﾄﾞﾚｽ　↓　フレーム数
プロトコル（SNMP）

mib-2.16.17.1.1.2.1.0.6.4.192.168.71.90.4.192.168.110.101.14 = 38
mib-2.16.17.1.1.2.1.0.6.4.192.168.71.90.4.192.168.110.101.16 = 208
mib-2.16.17.1.1.2.1.0.6.4.192.168.71.90.4.192.168.110.101.84 = 208
mib-2.16.17.1.1.2.1.0.6.4.192.168.71.95.4.192.168.110.100.14 = 2
mib-2.16.17.1.1.2.1.0.6.4.192.168.71.95.4.192.168.110.100.16 = 881
mib-2.16.17.1.1.2.1.0.6.4.192.168.71.95.4.192.168.110.100.84 = 881

sFlow：sFlowの誕生

- トラフィック・フロー分析のトラディショナルな解決法
  - SNMPカウンター:
    - インターフェース単位のオクテット数・フレーム数などのカウンター情報
    - トラフィック情報なし
  - RMON2:
    - RMON2プローブが必要（非常に高価）
    - ネットワークトラフィックに対して不十分な情報
    - ネットワークパフォーマンスへの影響　など

部分的な視覚化
少ない情報

↓

勘だよりの
意思決定

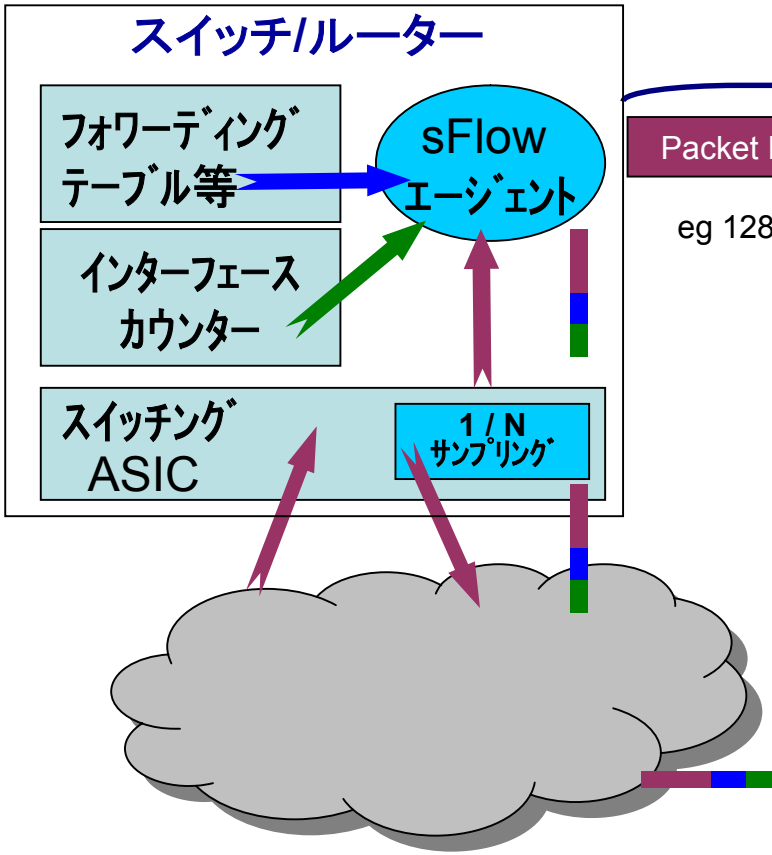
sFlow

トラフィック・フロー分析の次世代の解決法 → *sFlow* の誕生

sFlow：sFlowとは

- **サンプリングベース**のテクノロジー
  - スイッチやネットワークのパフォーマンスへの影響が少ない
  - ハイスピードネットワーク内のトラフィックをモニタリングする事を目的として新たに考案されたテクノロジー
- 米国**InMon**社によって公開： **Open Standard – IETF RFC3176(sFlow V4)**
- ネットワーク機器埋め込み型として設計されたモニタリング・テクノロジー
  - ルータスイッチ内に実装されスイッチのASICにて処理
  - 全てのスイッチ・ポートをモニター
- スイッチの**sFlow**エージェントが**sFlow**を生成し、**sFlow**マネージャーへ即座に送信
  - MIBやキャッシュ上で保持・カウントしない

sFlow：sFlowの動作



sFlow Datagram

Packet Header	Src/Dst i/f	Sampling Perms	Forwarding	user ID	URL	i/f counters
eg 128B		rate pool	src 802.1p/Q dst 802.1p/Q next hop src/dst mask AS path communities localPref MPLS	src/dst Radius TACACS		

InMon Traffic Sentinel
sFlow Collector & Analyser

sFlow：sFlowデータグラム・フォーマット

sFlow Datagram

- **Flow sample**
  - Packet Header：サンプルパケットのパケットヘッダー情報（一部ペイロード含む）
  - Src/Dst i/f：入出力インターフェースのifIndex
  - Sampling Perms：sFlowﾊﾟﾗﾒｰﾀｰ(Sampling Rate,Sampling Pool etc)
  - Forwarding
    - Priority （ Src/Dst 802.1p/TOS)
    - VLAN (Src/Dst 802.1q)
    - Next hop address
    - Source AS, Source Peer AS
    - Destination AS Path
    - Communities, local preference
    - MPLS
  - User ID：Src/Dst RADIUS/TACACS
  - URL
- **Interface statistics sample（SNMPｶｳﾝﾀｰ値）**
  - i/f counters：インターフェース・カウンター・統計値

レイヤー2以上のトラフィックの分析が可能（L2のMACアドレス分析も可能）
sFlow自体はフロー情報ではない ➔ マネジャー側でフロー情報化する必要がある

パケットサンプリングとトラフィック量の計算

- サンプリングされた情報から実際のフレーム数やバイト数を導き出す
- プロトコル別トラフィック量の計算

入力したフレームの総数 = N
総サンプル数 = n
そのクラス(プロトコル)でのサンプル数 = c
そのクラス別のフレーム数は次式により計算 :

$$N_c = \frac{c}{n} \cdot N$$

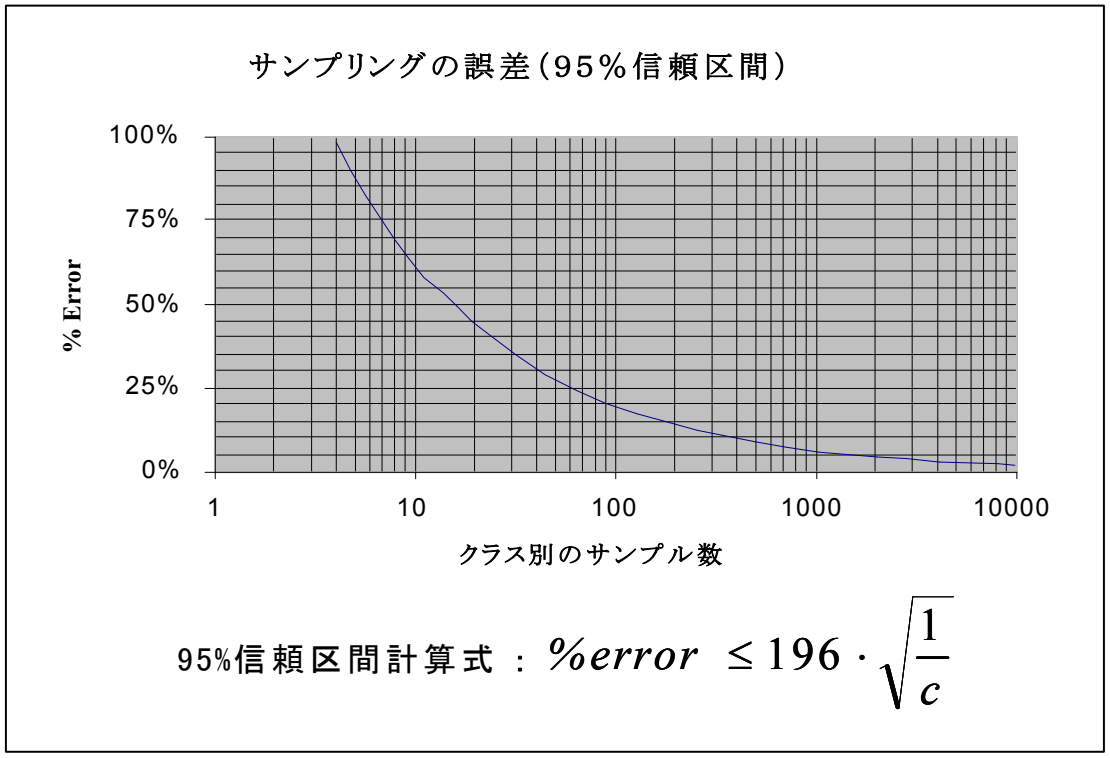
例:
入力したフレームの総数 = 1,000,000
サンプリングレート = 0.25%
総サンプル数 = 2,500
Voiceトラフィックのサンプル数 = 1,000
表示されるVoiceトラフィックのフレーム数は次式により計算:

$$\frac{1{,}000}{2{,}500} \times 1{,}000{,}000 = 400{,}000 \quad \text{フレーム}$$

サンプリングの誤差が発生 ➔ 統計的手法(95%信頼区間分析)により把握

sFlow：サンプリングの誤差（解析制度）

- サンプリングの誤差 ➔ 95%信頼区間によって分析

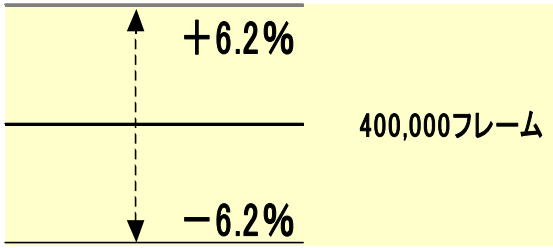


95%信頼区間計算式 ： $\%error \le 196 \cdot \sqrt{\frac{1}{c}}$

例：95%の信頼区間でのエラー率を前ページの例で計算すると、
Voiceトラフィックのサンプル数 = 1,000 なので、

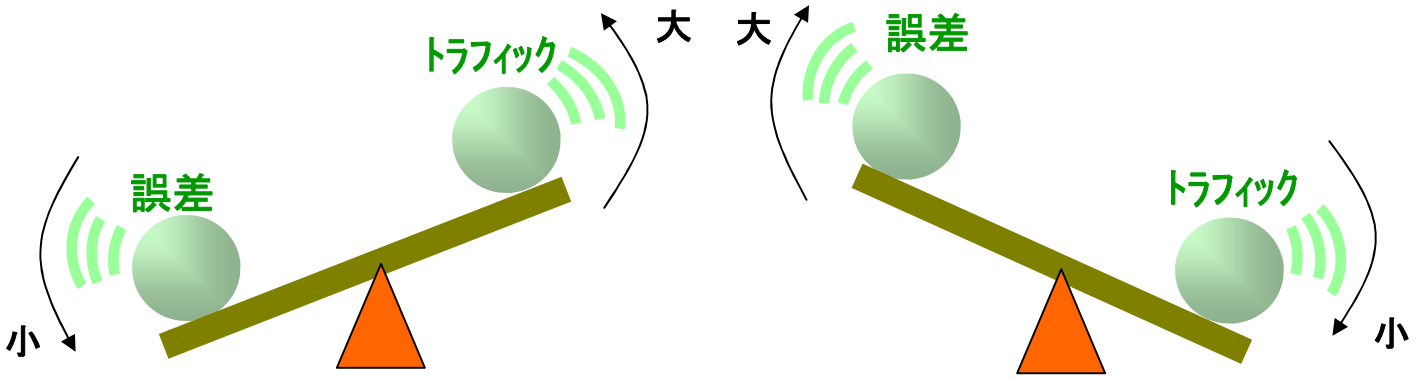
$$\%Error \le 196 \times \sqrt{\frac{1}{1{,}000}} \fallingdotseq \pm 6.2\%$$

表示された“400,000 フレーム”に対し
95%信頼区間では、±6.2%が誤差になるので、
区間は、
375,200フレーム(Lower) ～424,800フレーム(Upper)
となる



sFlow：誤差とトラフィックはトレードオフの関係

- 誤差とトラフィックはトレードオフの関係（トラフィック=分析対象トラフィック）
  - トラフィックが多い　➔　誤差は少ない
  - トラフィックが少ない　➔　誤差は大きい

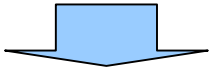


- 誤差を少なくするには？
  - 対象となるフローを増やす
    - サンプリングレートを上げる？
      ➔　サンプリングレートはインターフェース単位に可変であるが、分析の為の頻繁な変更は困難
    - 分析対象期間を延ばす？

sFlow：誤差を少なくする分析

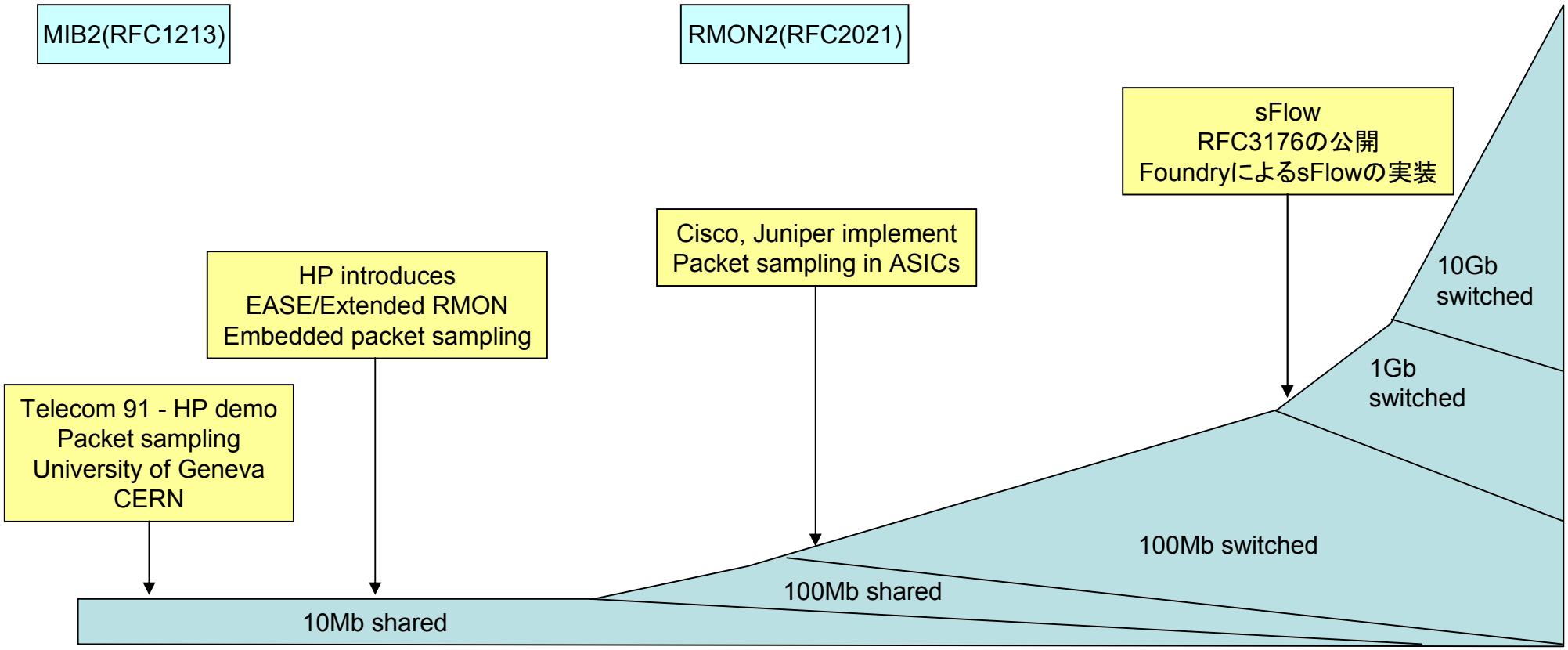
- 誤差を少なくする分析
  - トラフィックが多い場合：通常のサーバーアクセス（HTTP通信など）、DoS攻撃
    - ➔ トラフィックが多いので、**リアルタイム**でも**誤差は少ない**
  - トラフィックが少ない場合：使用頻度・通信量の少ない通信（チャット通信など）
    - ➔ トラフィックが少ないので、リアルタイムでは誤差が大きい
      - ➔ 対象期間を延ばす（“分”から”時間“,”日“,”週“,”月“へ）と対象トラフィックが多くなるので、誤差が少なくなる
  - サンプリング分析のコンセプト
    - メジャーなトラフィックは、誤差が少なく、リアルタイム性も保たれる
    - マイナーなトラフィックは、対象期間を延ばし、誤差を低減
    - スイッチ・パフォーマンス、ネットワーク・パフォーマンスの悪化を防ぐ

- サンプリングベースのテクノロジの為、
  1G/10Gネットワークから更なる広帯域への対応が可能



<u>将来的な100G(ｷﾞｶﾞﾋﾞｯﾄ)、1T（ﾃﾗﾋﾞｯﾄ）、10T、100Tネットワークへの対応</u>

sFlow：パケットサンプリングの歴史



パケットサンプリングは、
ハイスピード＆スイッチング・ネットワークで有効

sFlow：sFlowエージェント実装ベンダー

FOUNDRY NETWORKS
The Power of Performance™

AlaxalA

sFlow ENABLED

hp invent

HITACHI
Inspire the Next

FORCE10

Empowered by Innovation NEC

Allied Telesis

extreme networks

inMon sFlow Probe

Alcatel·Lucent

H3C
IToIP Solutions Expert

※ 各機器でのsFlowの対応状況の詳細は、ハードベンダー様へご確認下さい

- **ワイヤレスネットワーク向けsFlow**
  - sFlowを使用してワイヤレスネットワークをモニタリングする規格(2007年4月)
  - 802.11ワイヤレス・トラフィック上のデータを分析しフロー化
    - WAP(ワイヤレスアクセスポイント)別
    - RADIO別
    - SSID/チャネル別
    - Air Utilization% (802.11gの54Mbpsに対してなど)
    - ワイヤレス・バージョン(802.11a/b/g/n)
    - 暗号方式(TKIP/WEP/CCMP etc)
    - カウンター値
      - Fragments/Multicasts/RTS/Error/Station数/QoS
  - sFlow802.11サポート機器
    - HP ProCurve Wireless Edge Services xl Module / WESM zl module

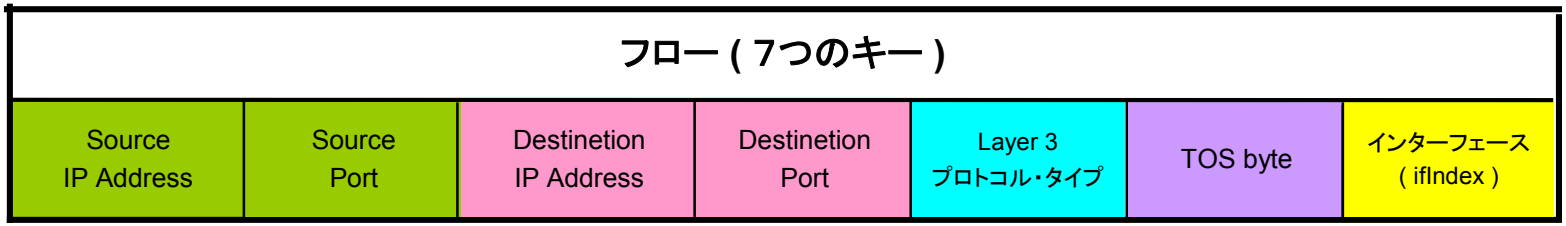
困難だったワイヤレス・トラフィックの可視化が可能に

Cisco NetFlow

- Cisco NetFlow ➔ Ciscoが開発した技術
  - ネットワーク上のIP フローについてネットワーク管理者が情報収集する手段を提供
  - エクスポートされたNetFlow データは、ネットワークの管理やプランニング、課金、攻撃対策、データ マイニングなど、様々な用途に利用可能
  - NetFlow が出力する基本データは、「フロー レコード」と呼ばれる
  - バージョン1,5,7,8,9が存在
  - バージョン9は、RFC3954として公開
  - 一般的には、全てのポートをモニターするのではなく、特定のポートをモニター
- キャッシュ・ベースのテクノロジー（キャッシュ上でフローをカウント）
- L3以上のトラフィックの分析が可能（L2の分析（MACアドレスなど）は不可）
- NetFlowは、フローとして集計された情報として送られる
  ➔ マネジャー側でフロー情報化する必要がない
- パフォーマンス上に問題がある場合は、サンプリング・テクノロジーを使用した“Sampled NetFlow”も用意されている
  - Sampled NetFlow 機能を使用すれば、ルータに転送される「x」個の IP パケットごとに 1 個のパケットをサンプリングできます。サンプリング パケットは、ルータの NetFlow フロー キャッシュに取り込まれます。このサンプリング パケットにより、大多数のパケットに対して NetFlow 用の追加処理が不要となるので、スイッチング処理がより高速に行えるようになり、NetFlow パケットの処理に要する CPU 使用率を大幅に低減できます。（「Ciscoマニュアルより」抜粋）

Cisco NetFlow

- フロー
  - 以下の図の内容を、フローとして、統計値（フレーム数・バイト数）を NetFlowキャッシュ内でカウント
  - NetFlowキャッシュ内で保持・カウントしている情報を、特定のタイミング（条件）でエクスポート



- フローをエクスポートするタイミング
  - インアクティブ・タイマー（デフォルト：15秒）
    - 該当のフローセットのセッションが15秒間インアクティブ（無音）の時、エクスポート
    - コマンド ” ip flow-cache timeout inactive 15 “で設定
  - アクティブ・タイマー（デフォルト：30分）
    - 該当のフローセットのセッションが継続している場合、30分経過時点で、エクスポート
    - コマンド ” ip flow-cache timeout active 30 “で設定
  - TCPコネクションのRSTやFINフラグの検出
  - NetFlowキャッシュがフル

- Cisco NetFlow

Figure 1　Example of a NetFlow Cache

1.NetFlowキャッシュ内での、フローの生成と更新

Srdf	Srd Padd	Dstlf	Dstl Padd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	Next Hop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.023.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.023.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A1	/24	180	00A1	/24	15	10.023.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.023.2	1040	1745	14

2.期限切れ（expiration）

・インアクティブ・タイマーの期限切れ（デフォルト：15秒）
・アクティブタイマーの期限切れ（デフォルト：30分）
・NetFlowキャッシュが、フル
・RST / FIN TCP フラグ

Srdf	Srd Padd	Dstlf	Dstl Padd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	Next Hop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.023.2	1528	1800	4

3.集約（Aggregation）

No

4.エクスポート・バージョン（V5 / 9など）

5.トランスポート・プロトコル
➔パケットのエクスポート

Payload (Flows)

Yes

4.エクスポート・バージョン(V8/9など)

Protocol	Pkts	SrcPort	DstPort	Bytes/Pkt
11	11000	00A2	DstPort	1528

121919

Cisco “NetFlow Services Solutions Guide”より

Juniper J-Flow

- J-Flow ➔ Cisco NetFlow version 5 のOEM
- フローサンプリングを推奨
  - アカウンティング用のフローモニタリングは、モニタリングエンジンと収集エンジンの双方に大きな負荷がかかるため
- 信頼性・誤差
  - sFlow同様、信頼区間の考え方を利用
- 99%信頼区間にて、誤差±3%以内の範囲にて分析することを推奨

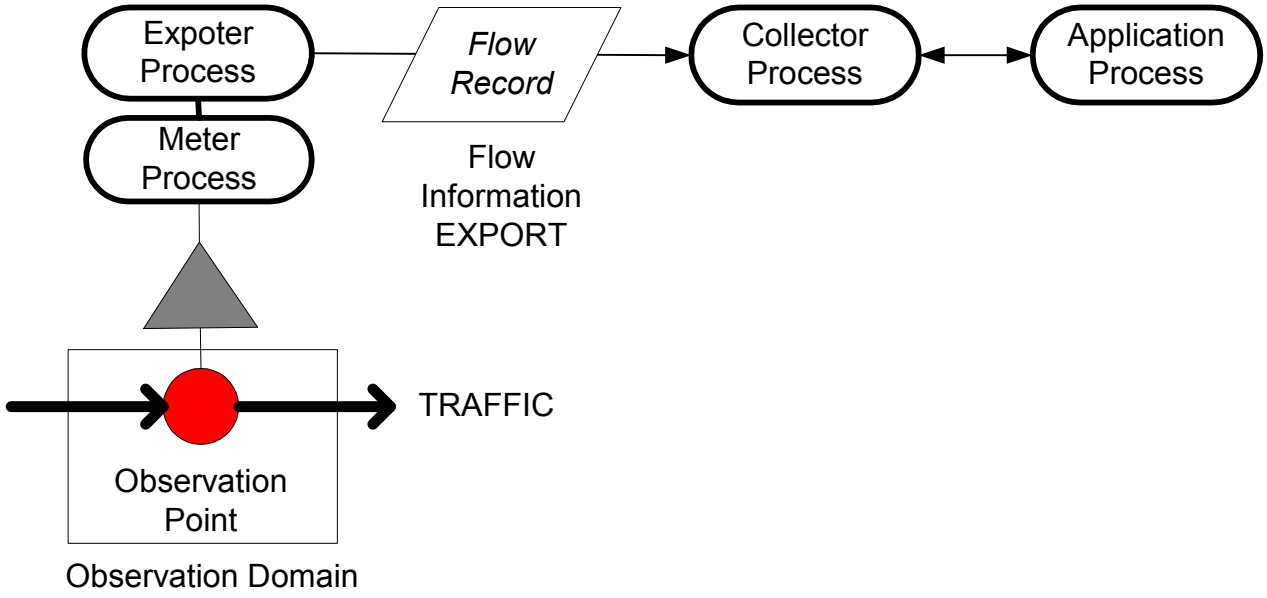
$$\%\,Error \leq 258 \times \sqrt{\frac{1}{\text{該当サンプル数}}}$$

JUNIPER NETWORKS R&E NEWSLETTER「大規模組織のためのトラフィック量追跡管理と使用量割り当て制限」より

IPFIX

- IPFIX
  - IETF IPFIXワーキンググループによる標準化
  - Cisco NetFlow V9をベースに開発
  - RFC5101として仕様化（2008年1月）
  - マルチベンダー：Cisco / Nortel Networks/ NEC / HP etc
  - フロー送信プロトコル：SCTP（Stream Control Transmission Protocol ）を使用
    (UDP/TCP もオプションで使用可能)

- プロセスの定義:
  - Observation Point：観測するネットワーク上のポイント（Interafaceなど）
  - Observation Domain：Observation PointのSet（Router/Switchなど）
  - Meter Process：サンプリング・フィルタリング。フローの解析
  - Exporter Process：テンプレートにあわせてフローレコードとしてエクスポート
  - Collector Process：Exporterから送られた情報をコレクション
  - Application Process：コレクションされた情報を視覚化・分析



IPFIX

- IPFIXの今後
  - 2008年1月に正式RFC化 → ベンダ実装は今後
    - RFC5101：IPFIXプロトコル仕様
      - Export Process から Collector Processへの送出方法
    - RFC5102：Information Model/Elementの定義(Meter/Export Process)
      - 自由度が高い
    - RFC5103：双方向フローのエクスポート
  - NetFlowからの移行
  - 留意点
    - 実装方法　→　簡略化
    - サンプリングへの対応
      - 誤差の把握：マネジャー(Application Process)側での対応
      - IETF PSAMP WGとの連携
- Nortel Networks
  - 対応機器
    - Ethernet Routing Switch 5500/8600 シリーズ

HP XRMON / Riverstone LFAP

- HP Extended RMON(XRMON)
  - 1993年 HP社によって策定
  - HP ProCurveスイッチによって実装

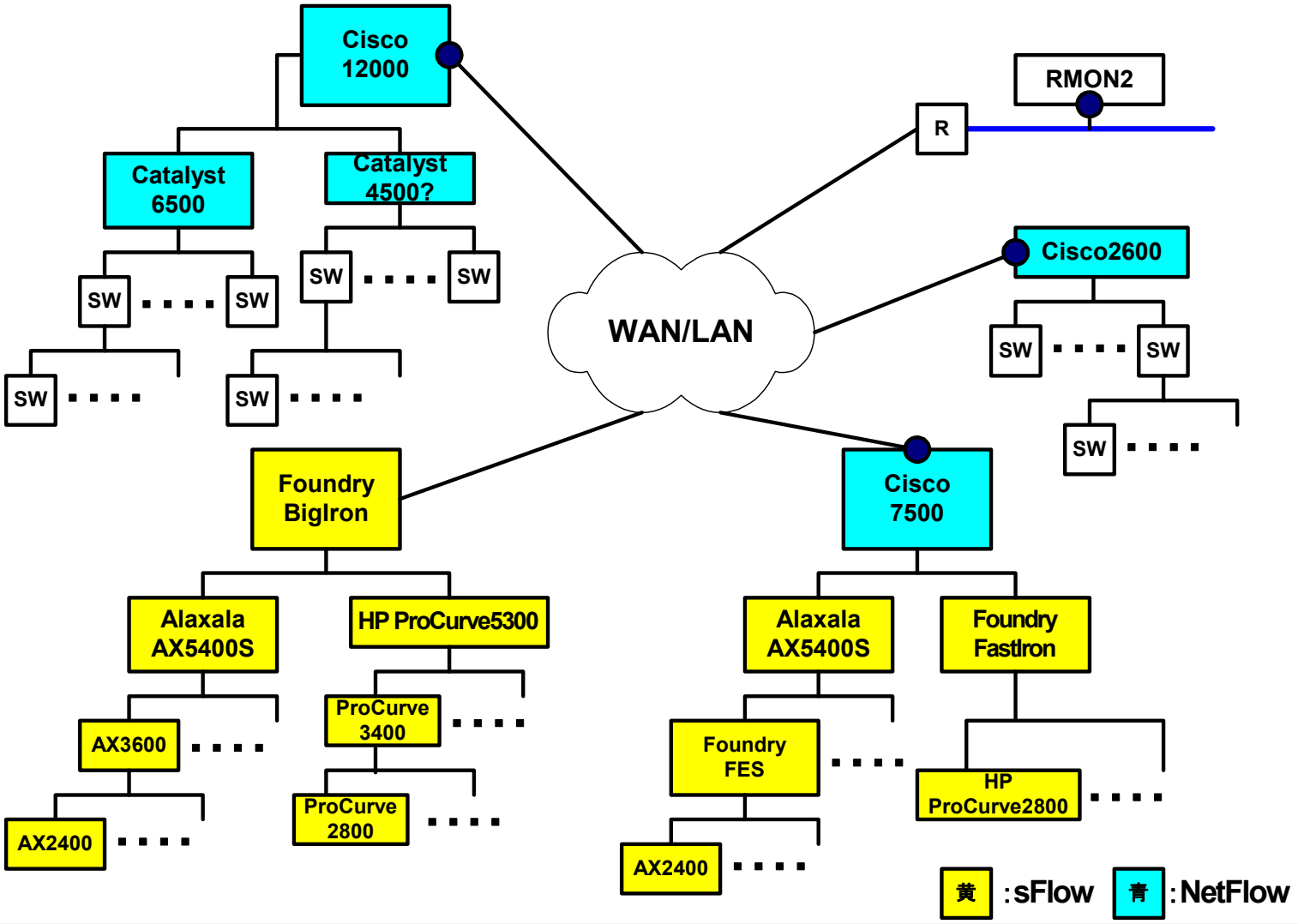
- Riverstone LFAP(Light-weight Flow Accounting Protocol)
  - 2001年 RiverStone社によって策定
  - 2006年 ルーセントが買収（現ルーセント・アルカテル）

sFlow vs NetFlow

- sFlow
  - RFC3176として公開（機器ベンダ非依存のオープンな規格）
  - サンプリングベース
  - 対象レイヤー：L2-L7+Payload
  - 高速スイッチングネットワークの測定を目的に開発
    → WANのモニタリング（BGP AS path 分析）
  - 全インターフェースをモニター
  - AS分析(OriginAS/SourcePeerAS/DestPeerAS/DestinationAS Path)
- NetFlow
  - RFC3954として公開（Cisco色が強い）
  - キャッシュベース
  - 対象レイヤー：L3-L4
  - WANリンクの測定が主たる目的としてリリース
    → LANのモニタリング（CatalystへのNetFlowの実装）
  - 特定のインターフォース(VLAN)をモニター
  - AS分析（SourcePeerAS/DestPeerAS）

sFlow vs NetFlow

- ロケーションの違い：sFlow=全体／NetFlow=Core or WAN



フロー管理ソリューション・プロダクト

- sFlowTrend
  - フリー（無償）版
  - sFlow対応
    - 単一デバイスのモニタリング
    - 収集データはメモリ上で展開（データの保存不可）
- sFlowTrend-Pro
  - sFlow対応
    - 複数デバイスのモニタリング可能
    - 収集データの保存
    - sFlowTrendの商用版。InMon TrafficSentinelの廉価版。
- InMon TrafficSentinel
  - sFlow / NetFlow v1,5,7,9 / J-Flow / IPFIX / XRMON / LFAP / SNMP対応
  - 商用版フロー＆ネットワーク管理システム