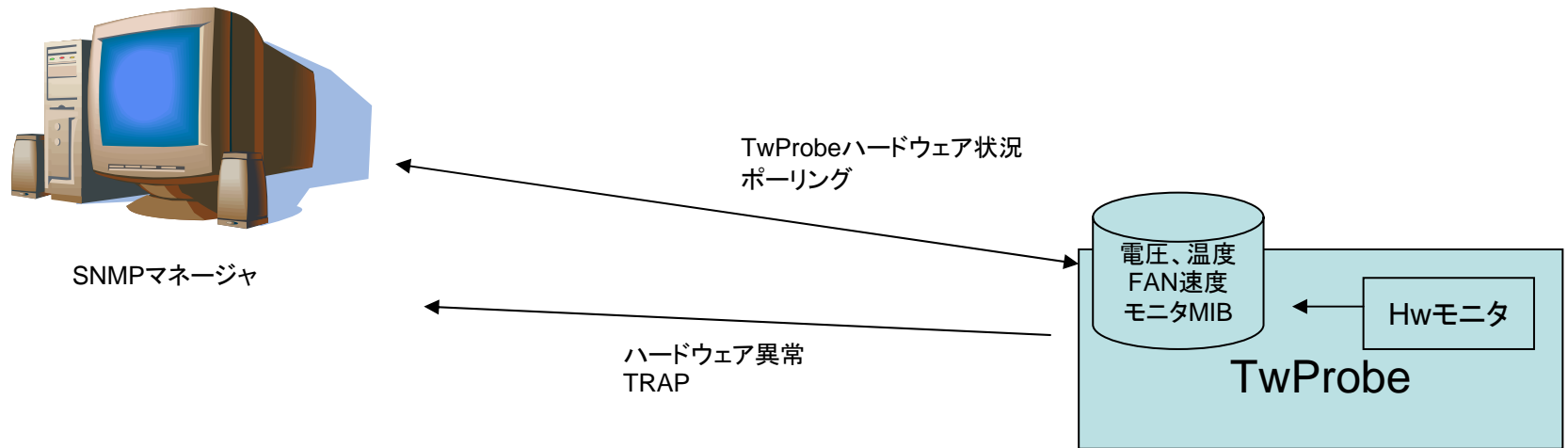


# TwProbe拡張MIB概要

Twise Labo Inc.

2007.10.31

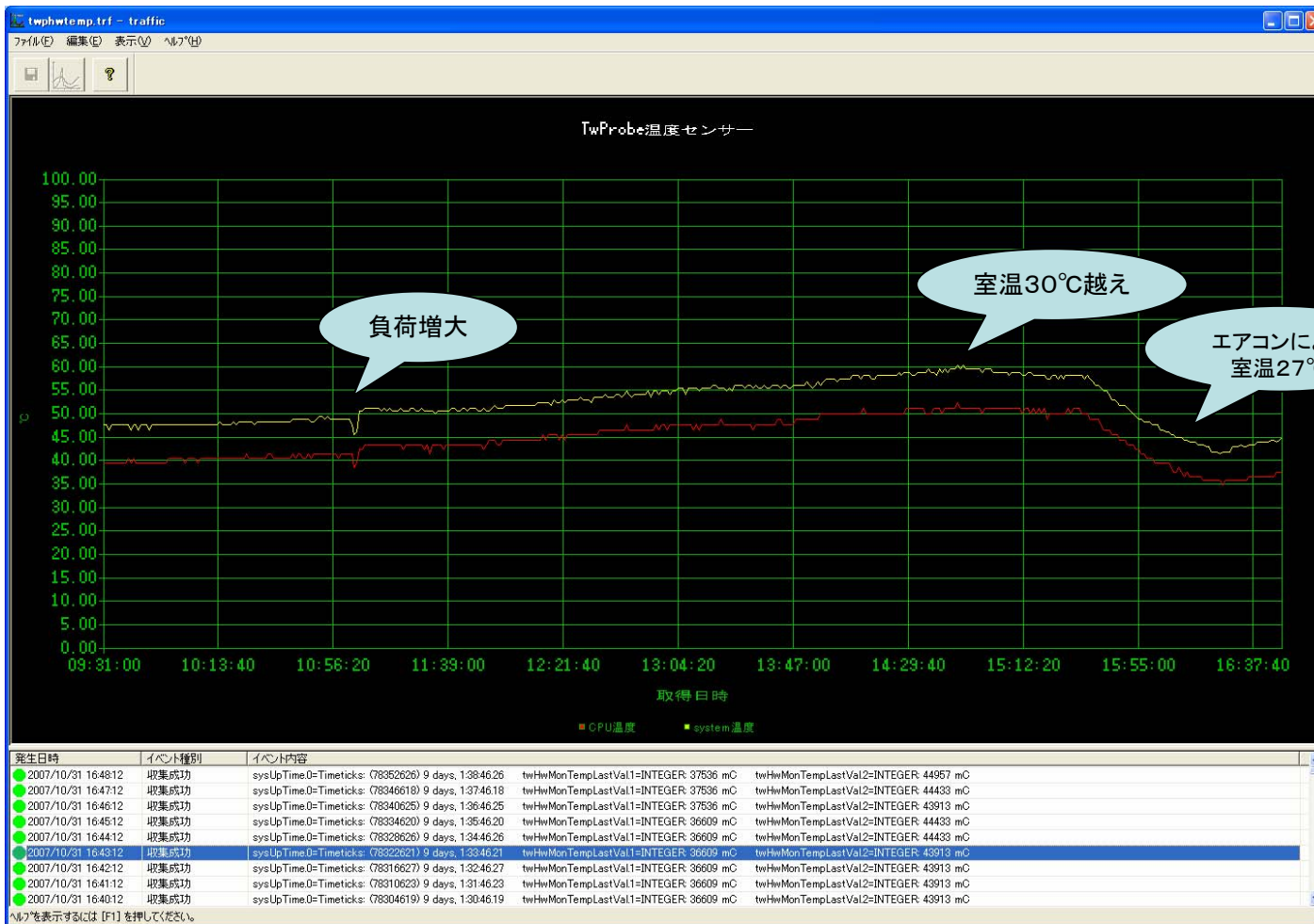
# TwProbeハードウェアモニタMIB



TwProbe自体の動作環境をモニタするためのMIBです。  
内部温度、CPU温度、電圧、FAN速度(FANがあれば)を測定可能です。

このエージェントは、TwProbe以外でも、スパーI/Oのセンサー機能を搭載したPC(PCサーバ)で動作させることができます。  
部分販売も可能ですので、詳細は、弊社までお問い合わせ下さい。

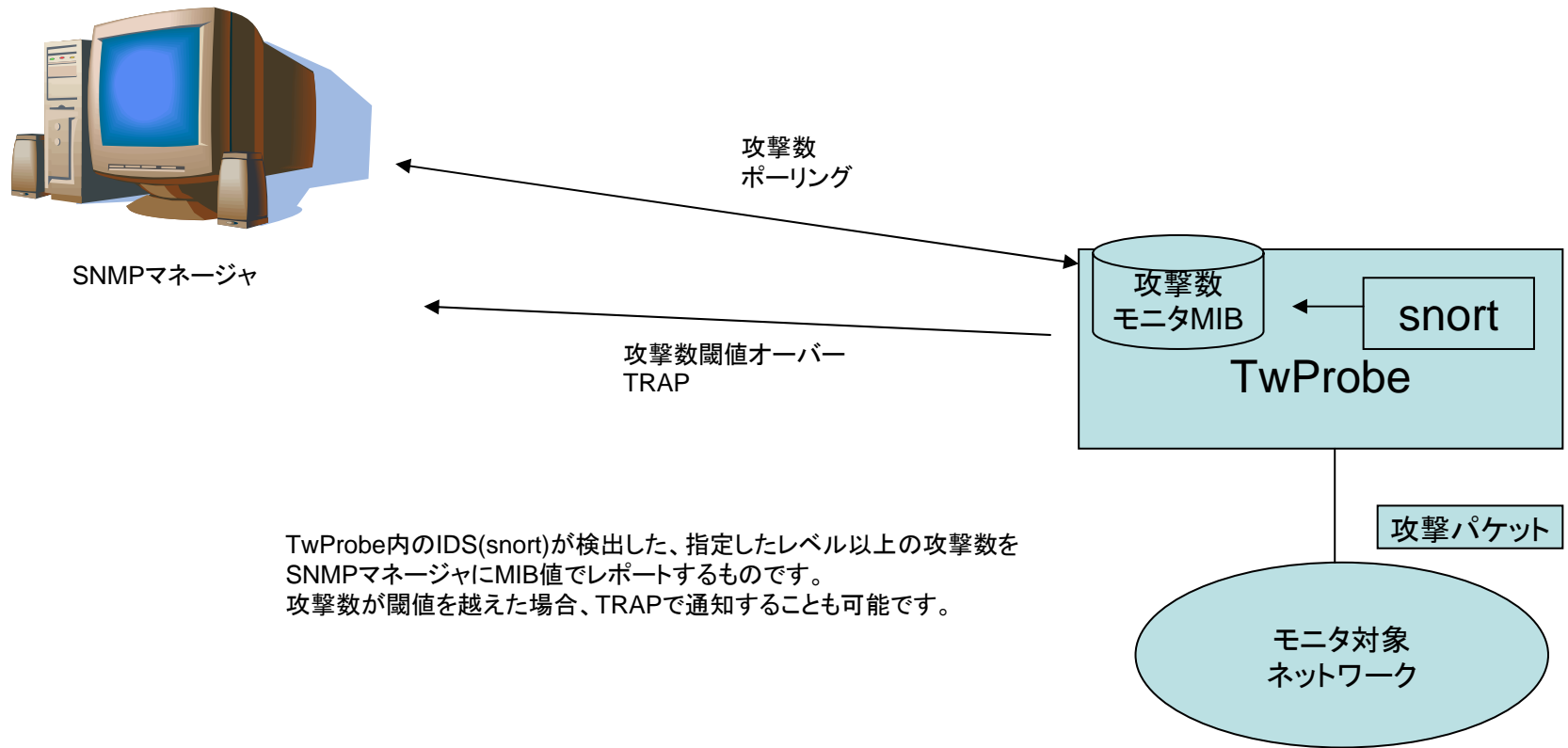
# TwProbe温度モニタの例



TWSNMPマネージャの  
グラフ機能で取得した例  
Twphwtemp.trfで測定

センサーの精度は高くありませんが  
動作環境の温度と、  
TwProbeの負荷に比例して、  
温度測定が可能です。

# IDS(snort) 管理MIB



TwProbe内のIDS(snort)が検出した、指定したレベル以上の攻撃数をSNMPマネージャにMIB値でレポートするものです。  
攻撃数が閾値を越えた場合、TRAPで通知することも可能です。

# IDS管理MIBの例

The screenshot shows the twprobe web interface. The browser window title is "twprobe - Microsoft Internet Explorer" and the address bar shows "http://192.168.1.236/". The interface has a sidebar with navigation buttons: INFO, SYSTEM, NETWORK, MONITOR (selected), LOG, and HELP. The main content area is titled "MONITOR" and features a central illustration of a device with a "Control" button and a "Manager" cloud icon. Below this are three panels: "IDS", "TRAFFIC", and "WIRELESS".

**IDS Configuration:**

- Send IDS Alert Trap: ON
- IDS Alert Count Pri.: High
- Alert Threshold:
  - 5Min. High(Red): 20, Low(Yellow): 10
  - 1Hour: 50, 20
  - 1Day: 200, 100
- Alert Count:
  - 5Min.: 0, Last 5Min.: 0
  - 1Hour: 0, Alert Status: 0
  - 1Day: 0

**TRAFFIC Configuration:**

- RMON: ON
- Time Mark Mode: Zero Only
- xFlow: sFlow NetFlow OFF
- Sampling Rate: 1000 (100~1000000)
- Counter Sample Interval / Active Flow Timeout: 60 Sec (60~300)

**WIRELESS Configuration:**

- Channel: 802.11bg Ch.1
- WLAN Key: [Empty]
- Scan Int.: 5 Sec(5~600)
- AP. Timeout: 3600 Sec (600~86400)

**TRAFFIC Status:**

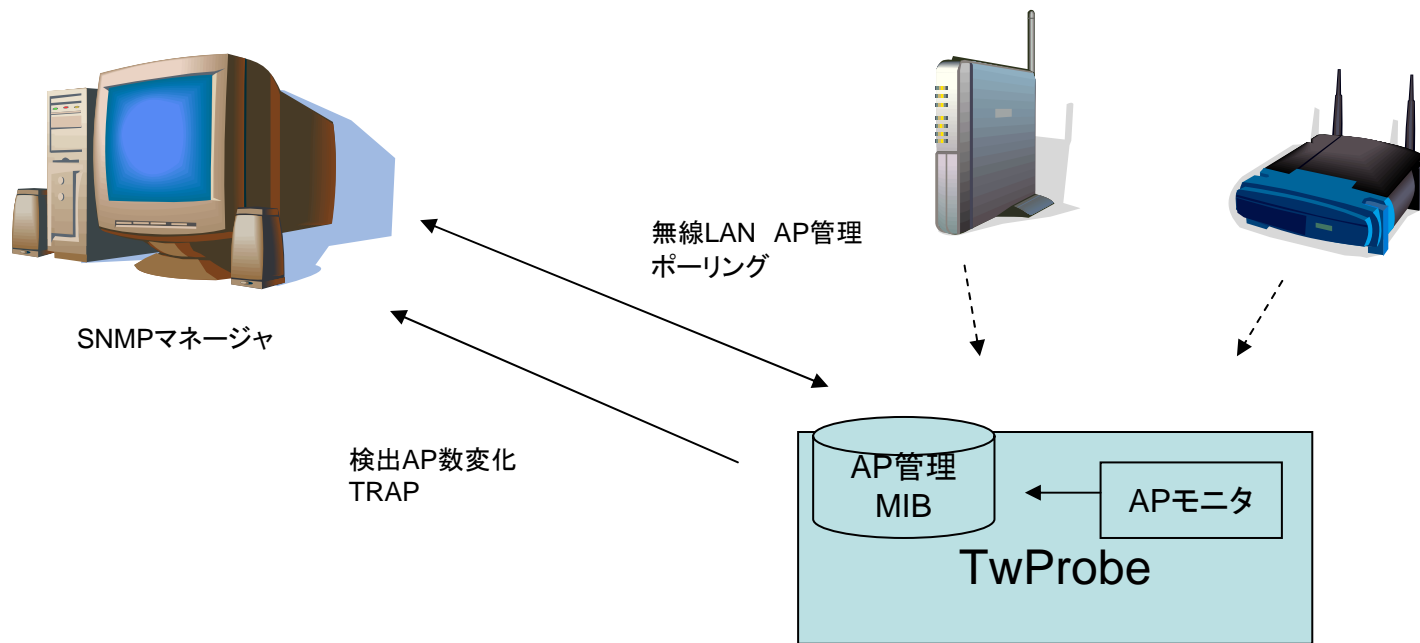
CH	LV	SC	AP
1		🔒	802.11bg Ch.1
1			802.11bg Ch.1

TRAFFIC	0	1 Mbps
Management	31%	
Control	14%	
Data	54%	
Low Sig.	13%	
Protect	54%	
Dec. Error	0%	
Weak IV	0%	

この部分の表示内容を、  
SNMPからアクセス可能にする  
ためのMIB定義です。  
TRAPの送信制御も可能です。

# 無線LAN管理MIB チャンネルスキャンモード



TwProbeが設置された範囲で、  
受信した無線LANの電波からAPポイントのリストを作成します。  
APの以下の情報をMIBとして、SNMPマネージャからアクセス可能です。  
APのアドレス、ESSID、使用チャンネル、電波レベル、セキュリティレベル



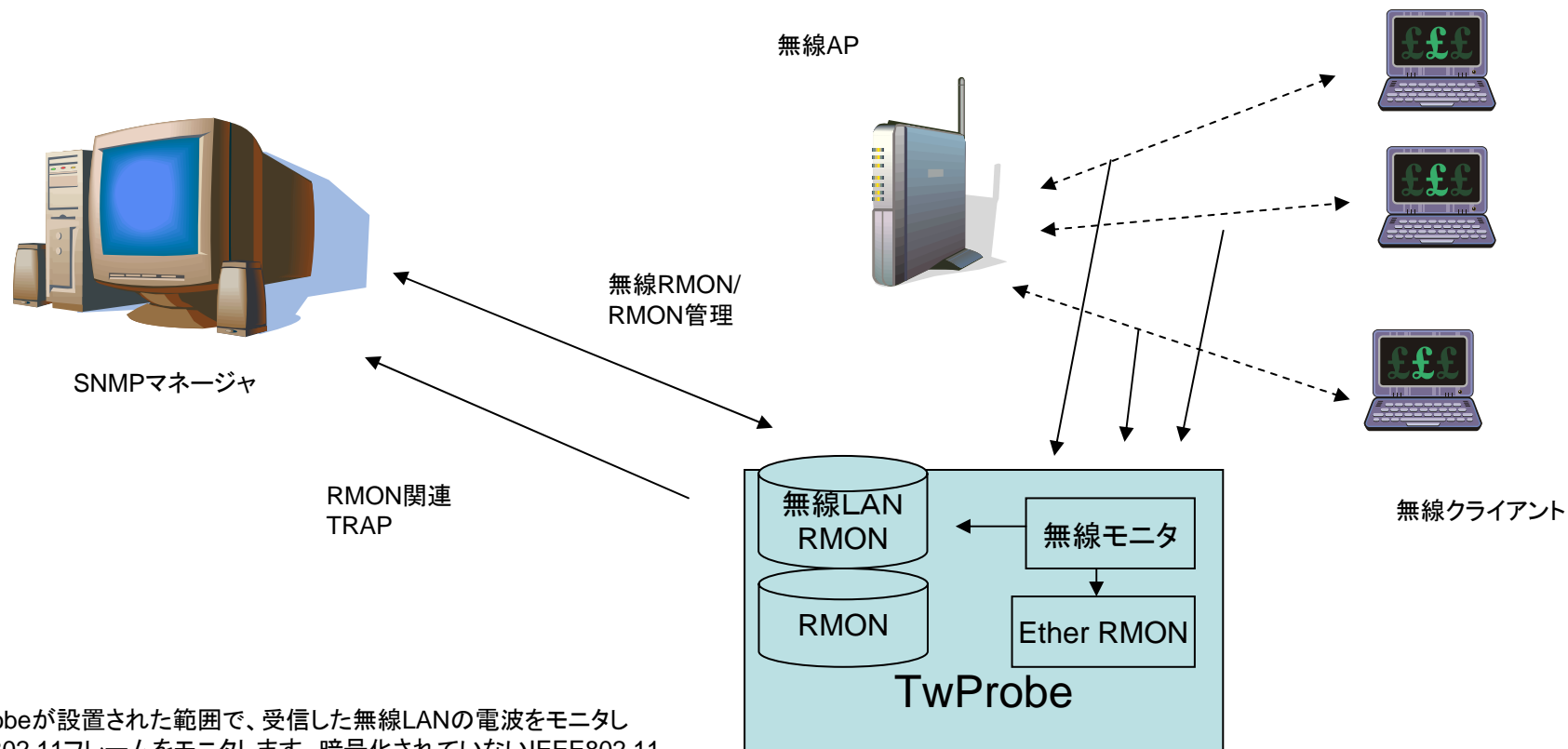
# 無線LAN管理の例

The screenshot shows the Twprobe web interface in Microsoft Internet Explorer. The browser address bar displays <http://192.168.1.236/>. The interface features a navigation menu on the left with buttons for INFO, SYSTEM, NETWORK, MONITOR, LOG, and HELP. The main content area is titled "MONITOR" and includes a central diagram of a wireless LAN setup with a central "Manager" unit and several "Control" units connected to laptops. A status bar at the top right shows the date and time: 2007/10/11 08:56. Below the diagram, there are configuration sections for "xFlow Collector" (Collector1: 192.168.1.201), "IDS" (Alert Threshold: High, Alert Count: 0), "TRAFFIC" (Sampling Rate: 1000, Counter Sample Interval: 60), and "WIRELESS" (Channel Scan Mode, Scan Int.: 5, AP Timeout: 3600). A table on the right displays wireless LAN information:

CH	LV	SC	AP
1		🔒	D
6		🔒	D
6		🔒	D
7		🔒	D
7		🔒	D
11		🔒	D

この部分に表示される無線LANのAP情報に関して、詳細を、SNMPのMIBとして管理できます。チャンネル、電波レベル、セキュリティレベル、アドレスなどがあります。

# 無線LAN管理MIB チャンネルモニタモード



TwProbeが設置された範囲で、受信した無線LANの電波をモニタしIEEE802.11フレームをモニタします。暗号化されていないIEEE802.11ヘッダ部分から、フレーム種別統計、ステーション別、ステーション間マトリックスのWRMON情報をMIBとして提供します。同じチャンネルを使用するAPの検出も可能です。正しい暗号キーを設定し、フレーム復号できる場合は、EtherNetフレームに変換し、EtherNetのRMON1/2の管理MIBを提供します。

# 無線LAN RMON管理MIBの例

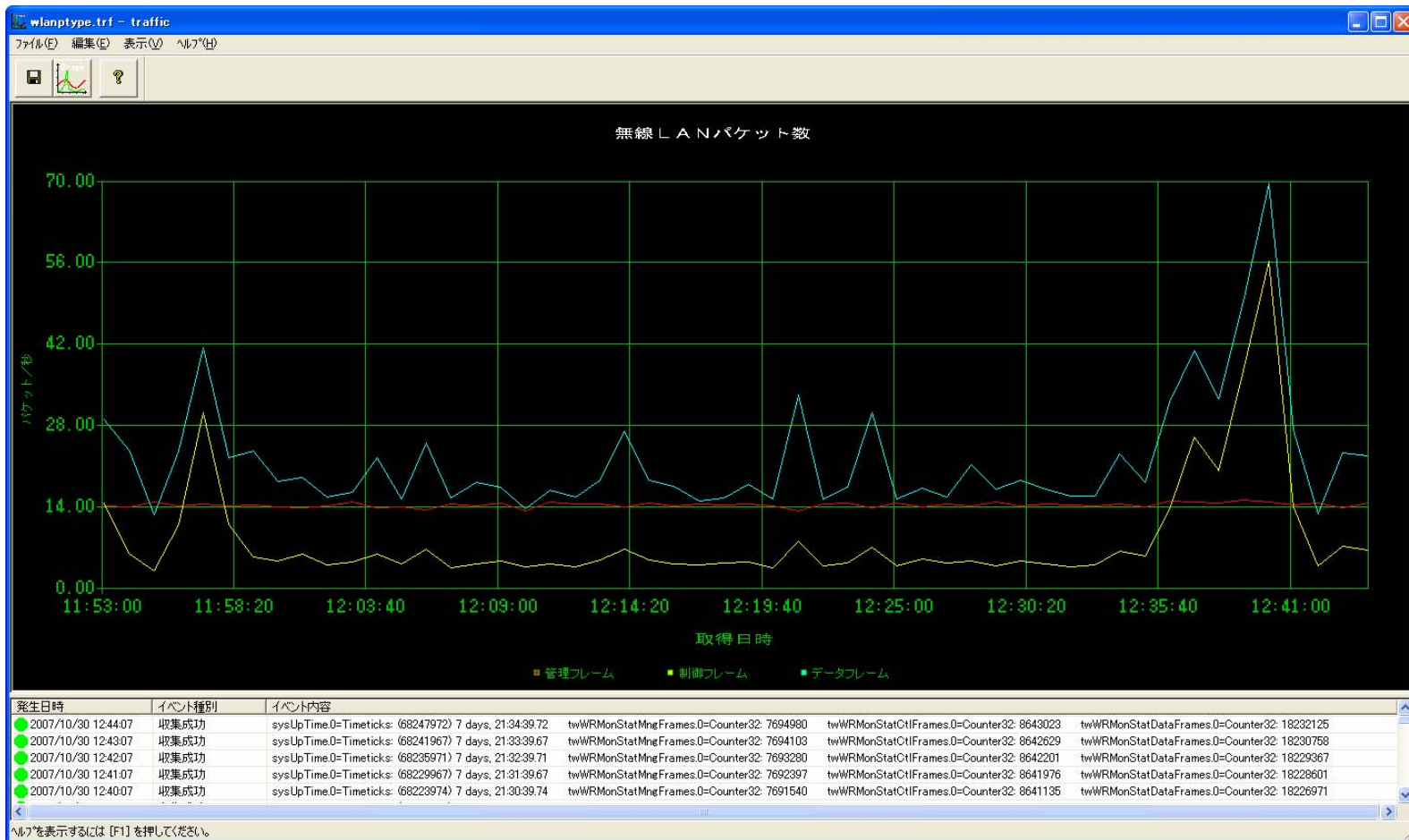
The screenshot shows the TwiProbe web interface in Microsoft Internet Explorer. The browser address bar shows `http://192.168.1.236/`. The interface has a navigation menu on the left with buttons for INFO, SYSTEM, NETWORK, MONITOR, LOG, and HELP. The main content area is titled "MONITOR" and features a central graphic of a router connected to three laptops. Below this are several configuration panels:

- IDS:** Includes options for "Send IDS Alert Trap" (ON), "IDS Alert Count Pri." (High), and "Alert Threshold" (High/Low) with numerical inputs (20, 10, 60, 20, 200, 100).
- TRAFFIC:** Includes "RMON" (ON), "Time Mark Mode" (Zero Only), "xFlow" (ON), "sFlow" (OFF), "NetFlow" (OFF), "Sampling Rate" (1000), and "Counter Sample Interval / Active Flow Timeout" (60 Sec).
- WIRELESS:** Includes "Channel" (802.11bg Ch.1), "WLAN Key", "Scan Int." (5 Sec), and "AP. Timeout" (3600 Sec).

A "xFlow Collector" section is visible with "Collector1" set to "192.168.1.201" and "Collector2" empty. A speech bubble points to this section, containing the following text:

この部分の表示内容を、SNMPからアクセス可能にするためのMIB定義です。同じチャンネルを使用するAPのリストや、フレーム種別毎の統計も表示できます。信号レベルの低いフレーム数や、脆弱性のあるフレームの数も測定できます。

# 無線LAN RMON管理の例



無線LANのフレーム種別による、通信量のグラフです。TWSNMPを使用して表示しています。  
データ通信を行っていない状態でも、定常的に、管理フレームなどが流れている様子が分かります。  
(この情報は、暗号キーを設定しない状態でも取得可能です。)