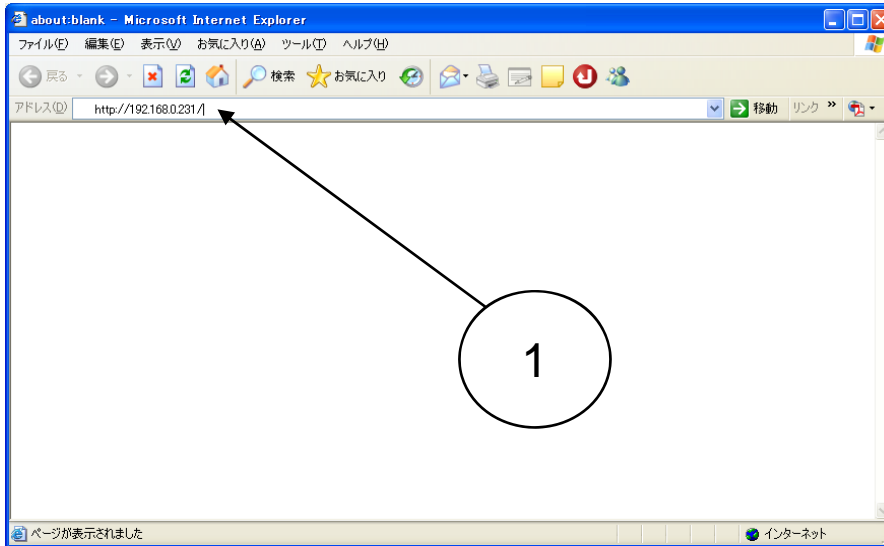


TwProbe基本設定マニュアル

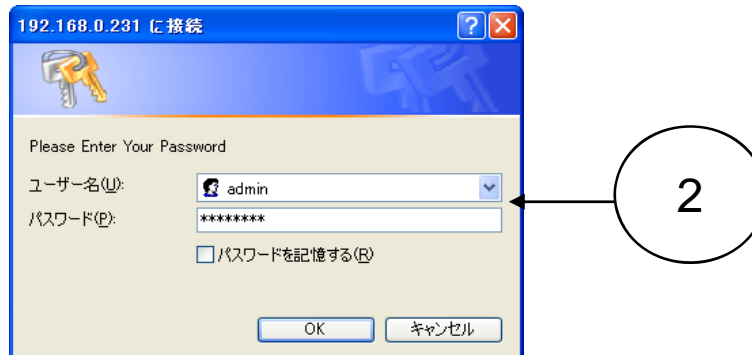
Twise Labo., Inc.

(2) WEB画面



■ログイン■

- ① WEBブラウザで機器のIPアドレスを指定します。
- ② WEB用に設定したユーザー名・パスワードを入力して<OK>をクリックします。INFO画面に遷移します。



(2)WEB画面

■INFO画面■

INFO画面では現在の設定値が表示されます。



■メニューボタンの説明■

画面左側の各メニューをクリックすると、該当画面を表示します。

<INFO>	初期画面です。 基本的な登録情報を一覧表示します。
<SYSTEM>	ユーザ情報、ライセンス管理、時刻管理、シャットダウンや再起動の制御を行います。
<NETWORK>	IPアドレス、Syslog、SNMPなどの情報を設定します。
<MONITOR>	モニタ画面を表示します。 機器状態のモニタリング、設定などができます。
<LOG>	ログ情報を表示します。(別ウィンドウ)
<HELP>	このマニュアルを表示します。(別ウィンドウ)

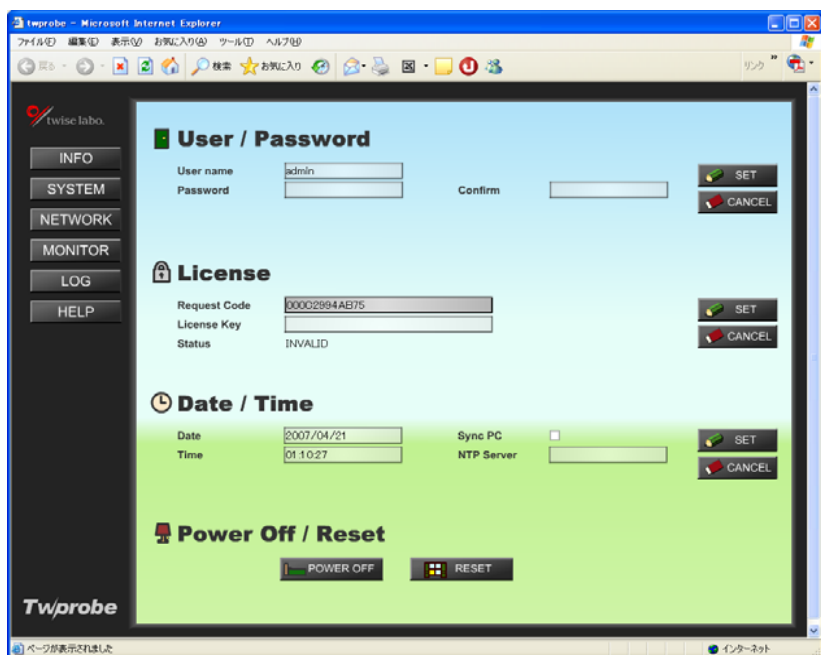
(2) WEB画面

■ SYSTEM画面 ■

ユーザ情報、ライセンス管理、時刻管理、シャットダウンや再起動の制御を行います。

必要な情報を入力して<SET>をクリックすると登録情報を変更します。

<CANCEL>で、入力内容を元に戻します。



■ User / Password

User Name	WEBにアクセスするためのユーザ名です。
Password	WEBにアクセスするためのパスワードです。 [Confirm]に確認のため再入力して下さい。

■ License

Request Code	ライセンスキーを得るためのリクエストコードです。 欄内の文字列をドラッグして選択し、右クリックメニューから「コピー」を選択すると、文字列をコピーできます。
License Key	弊社より送付されたライセンスキーを入力します。
Status	ライセンスの状況を示します。

■ Date / Time

Date	現在のシステムの日付です。
Time	現在のシステムの時刻です。
Sync PC	チェックをつけると、PCの時刻に同期します。
NTP Server	NTPサーバの時刻に同期させる場合に、NTPサーバのIPアドレスを入力します。

■ Power Off / Reset

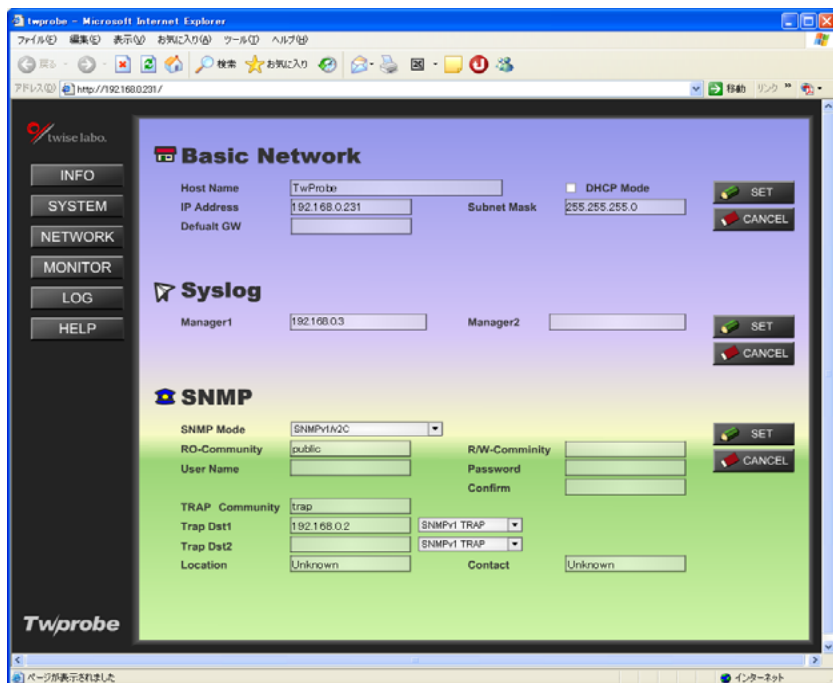
<POWER OFF>	システムをシャットダウンします。
<RESET>	システムを再起動します。

(2)WEB画面

■NETWORK画面■

IPアドレスなどの基本情報、Syslogの送付先、SNMP情報を設定します。

必要な情報を入力して<SET>をクリックすると登録情報を変更します。
<CANCEL>で、入力内容を元に戻します。



■Basic Network

Host Name	機器のホスト名です。
DHCP Mode	チェックするとIPアドレス、サブネットマスク、デフォルトゲートウェイの情報は無効になります。
IP Address	機器のIPアドレスです。
Subnet Mask	サブネットマスクを指定します。
Default GW	デフォルトゲートウェイを指定します。

■Syslog

Manager1,2	Syslogの送付先を指定します。 入力形式「IPアドレス:ポート番号」 (ポート番号は省略可能)
------------	---

■SNMP

SNMP Mode	SNMPのバージョンを指定します。
RO-Community	SNMPによるポーリング実施時の読込Community名です。
RW-Community	読み書きCommunity名です。
User Name	SNMPv3を使用する場合のユーザ名です。
Password	SNMPv3を使用する場合のパスワードです。
TRAP Community	TRAPに付加されたCommunity名を指定します。
TRAP Dst 1,2	TRAPの送信先とバージョンを指定します。
Location	機器が設置されている場所です。(sysLocation)
Contact	機器の管理者を指定します。(sysContact)

(2) WEB画面

■ MONITOR画面 ■

機器の状態をグラフィカルに表示します。

各種設定を行うと、画面右上の、時計下の欄に、設定結果が表示されます。



■ モニタ表示

Monitor	モニタポートのON/OFF状態を、緑/グレー表示します。
Control	管理ポートのON/OFF状態を、緑/グレー表示します。
xFlow Collector	xFlowの送信先を指定します。 入力形式「IPアドレス:ポート番号」 (ポート番号は省略可能) 「0.0.0.0」を入力すると、クリアされます。

■ IDS

<ON><OFF>	IDS機能のON/OFFを切り替えます。
Send IDS Alert Trap	閾値を超えた時にTRAPを送信するかどうかを指定します。
IDS Alert Count Pri.	TRAPを送信する閾値のレベルを指定します。
Alert Threshold	攻撃情報の閾値を指定します。
Alert Count	攻撃情報の統計を5分、1時間、24時間ごとに表示します。
Last 5Min.Alert Status	5分間の攻撃状態を、LED表示します。
<MUTE>	5分間の攻撃が重度の閾値を超えている場合、音声ファイルを再生します。OFF(ボタングレー)の場合は再生しません。

(2) WEB画面

■ MONITOR画面 ■

機器の状態をグラフィカルに表示します。

各種設定を行うと、画面右上の、時計下の欄に、設定結果が表示されます。



■ TRAFFIC

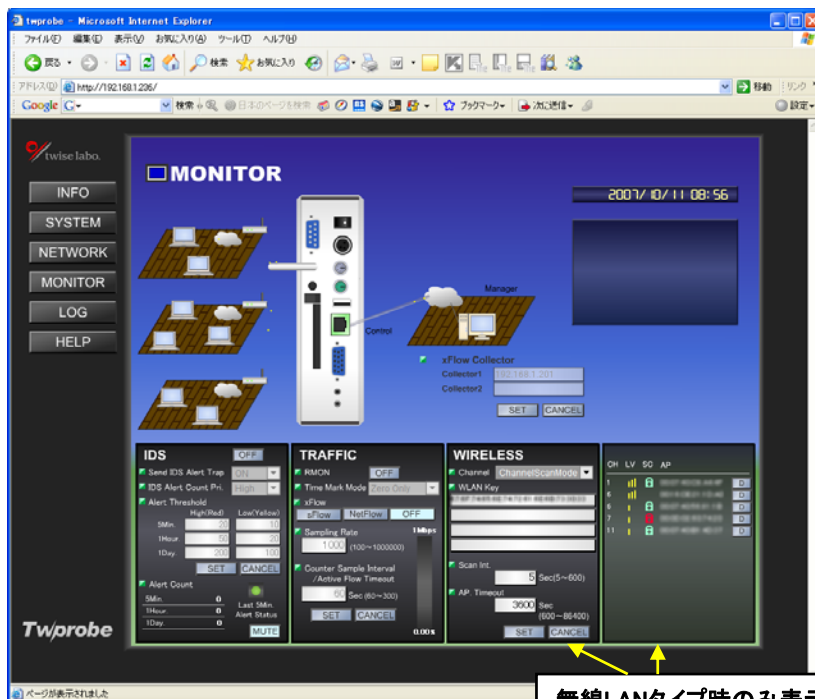
RMON	RMON機能の使用を<ON><OFF>ボタンで切り替えます。
xFlow	xFlow機能の使用を<sFlow><NetFlow><OFF>で切り替えます。 -NS版は、sFlowとNetFlowを同時に設定することができます。
Sampling Rate	パケットをサンプリングにおいて間引き割合を指定します。 指定した数値分のパケットを受信した場合に、1パケットTFWMONIにパケットサンプルを送信します。 トラフィックが少ない場合には小さな値、多い場合は大きな値を設定してください。 (sFlowのみ)
Counter Sample Interval	トラフィックの統計情報を記録したカウンタサンプルをTFWMONIに送信する間隔を秒単位で指定します。 (sFlowのみ)
Active Flow Timeout	NetFlowのアクティブタイマーのタイムアウト値です。アイドルタイマーのタイムアウトは、この値の1/10が設定されます。
トラフィックメータ	現在のトラフィック量を%で表示します。

(2) WEB画面

■ MONITOR画面 ■

機器の状態をグラフィカルに表示します。

各種設定を行うと、画面右上の、時計下の欄に、設定結果が表示されます。



無線LANタイプ時のみ表示。
ChannelScanModeの表示例です。

■ WIRELESS

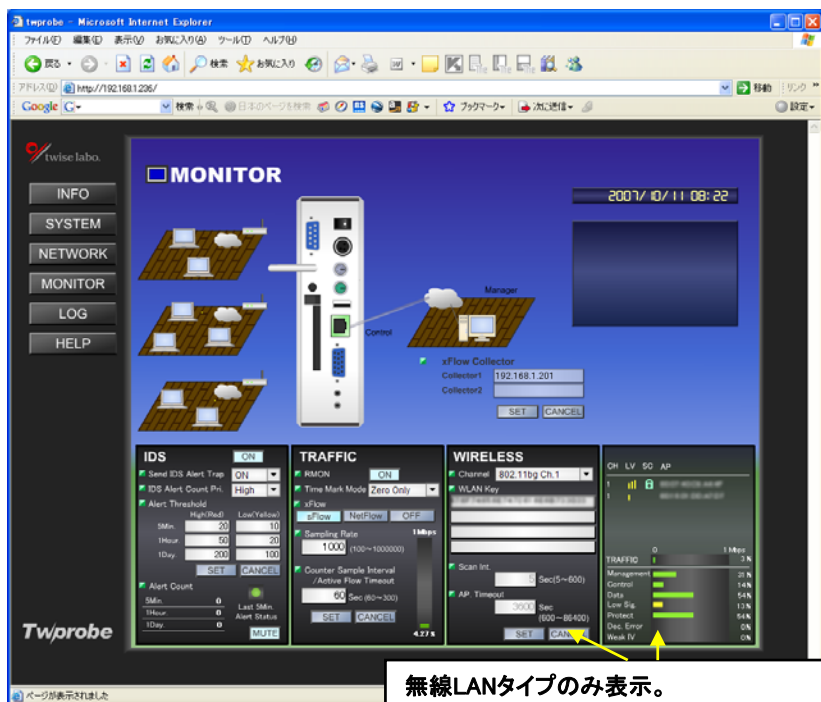
Channel	モニタする無線LANのチャンネルを指定します。 ChannelScanModeは、対応している無線LANの全チャンネルをスキャンしてアクセスポイント(AP)を検索します。 このとき、IDSおよびTRAFFIC機能は、自動的にOFFになります。
WLAN Key	無線LANの暗号キーを設定します。 設定可能なキーは、以下のとおりです。 01:02:03:04:05 (40/64-bit WEP) 01:02:03:04:05:06:07:08:09:10:11:12:13: (104/128-bit WEP) wpa-pwd:MyPassword:MyAP (WPA + plaintext password + SSID) SSIDは、必須です。 wpa-psk:0102030405...6061626364 (WPA + 256-bit key)
Scan Int.	アクセスポイント(AP)を検索する間隔を秒単位で指定します。(ChannelScanModeのみ)
AP. Timeout	発見したアクセスポイントを無効にするまでのタイムアウトを秒単位で指定します。(ChannelScanModeのみ) この時間内に再度発見した場合は、タイムアウトは、その時点からカウントします。

(2) WEB画面

■ MONITOR画面 ■

機器の状態をグラフィカルに表示します。

各種設定を行うと、画面右上の、時計下の欄に、設定結果が表示されます。



無線LANタイプのみ表示。
チャンネル番号を指定した場合の表示例です。

■ Channel List

CH	チャンネル番号です。
LV	電波レベルを3段階で表示します。
SC	暗号化のレベルを表示します。 ・青 低レベル暗号 (WEP) ・赤 強力暗号
AP	アクセスポイントのMACアドレスを表示します。
<D>	詳細情報を別ウィンドウにて表示します。 (ChannelScanModeのみ)

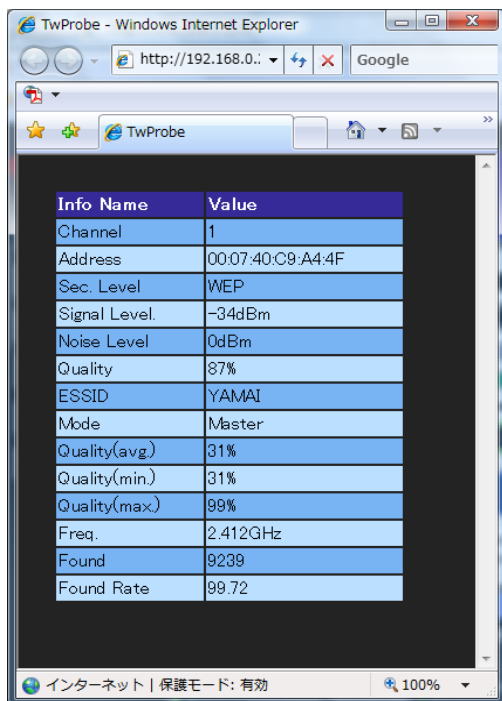
■ Traffic Graph

TRAFFIC	トラフィック量をグラフ表示します。左上に最大値が表示されます。
Management	管理フレームの割合です。
Control	制御フレームの割合です。
Data	データフレームの割合です。
Low Sig.	信号レベルが低いフレームの割合です。遠くにあるノードからのフレームが多い場合に、大きくなります。
Protect	暗号化されたフレームの割合です。一般的に暗号化設定された無線LANネットワークでは、データフレームの割合と一致します。
Dec. Error	復号エラーが発生したフレームの割合です。キーが正しく設定されている場合、暗号化されたフレームの割合と一致します。キーが正しく設定されていない場合、大きくなります。
Weak IV	暗号キーを解読されやすいIVを設定したフレームの割合です。この値が大きい場合、注意が必要です。

(2) WEB画面

■ 詳細画面 ■

WIRELESS表示のとき、Channel Listの<D>ボタンをクリックすると表示されます。アクセスポイントの詳細情報を表示します。



The screenshot shows a web browser window titled 'TwProbe - Windows Internet Explorer'. The address bar contains 'http://192.168.0.:'. The main content area displays a table with the following data:

Info Name	Value
Channel	1
Address	00:07:40:C9:A4:4F
Sec. Level	WEP
Signal Level	-34dBm
Noise Level	0dBm
Quality	87%
ESSID	YAMAI
Mode	Master
Quality(avg.)	31%
Quality(min.)	31%
Quality(max.)	99%
Freq.	2.412GHz
Found	9239
Found Rate	99.72

Channel	チャンネル番号です。
Address	アクセスポイントのMACアドレスです。
Sec. Level	暗号化のレベルです。
Signal Level	電波の信号レベルです。
Noise Level	電波のノイズレベルです。
Quality	通信品質を示します。
ESSID	ESSIDを示します。
Mode	アクセスポイントの動作モードを示します。
Quality (avg.)	通信品質の平均値です。
Quality (min.)	通信品質の最小値です。
Quality (max.)	通信品質の最大値です。
Freq.	周波数です。
Found	このAPを検出した回数です。
Found Rate	検索を実施した回数に対して、このAPを検出した割合です。

(2) WEB画面

■ LOG表示 ■

対象機器のLOGを表示します。



The screenshot shows a Microsoft Internet Explorer browser window displaying the Twprobe web interface. The address bar shows the URL `http://192.168.0.231/LOG_frame.html`. The page features the Twprobe logo on the left and the Twise Labo logo on the right. A "ログ表示" (Log Display) button is visible. The main content area displays a log titled "syslog" with the following entries:

```
Apr 19 15:13:56 TwProbe syslog.info syslogd started: BusyBox v1.4.1
Apr 19 15:13:56 TwProbe user.info twtppcd Start
Apr 19 15:13:58 snort: OpenPcap0 device eth1 network lookup: "eth1: no IPv4 address assigned
Apr 19 15:13:58 snort[1059]: Initializing daemon mode
Apr 19 15:13:58 snort[1062]: PID path stat checked out ok. PID path set to /var/run/
Apr 19 15:13:58 snort[1062]: Writing PID "1062" to file "/var/run//snort_eth1.pid"
Apr 19 15:13:58 snort[1062]: Parsing Rules file /etc/snort/snort.conf
Apr 19 06:13:58 TwProbe daemon.info init: Starting pid 1065, console /dev/tty1: '/sbin/getty'
Apr 19 06:13:58 TwProbe daemon.info init: Starting pid 1066, console /dev/tty1: '/sbin/getty'
Apr 19 15:13:58 snort[1062]: -----[Flow Config]-----
Apr 19 15:13:58 snort[1062]: |Stats Interval: 0
Apr 19 15:13:58 snort[1062]: |Hash Method: 2
Apr 19 15:13:58 snort[1062]: |Memcap: 10485760
Apr 19 15:13:58 snort[1062]: |Rows: 4099
Apr 19 15:13:58 snort[1062]: |Overhead Bytes: 16400(0.16)
Apr 19 15:13:58 snort[1062]: -----
Apr 19 15:13:58 snort[1062]: Frag0 global config
Apr 19 15:13:58 snort[1062]: Max frags: 65536
Apr 19 15:13:58 snort[1062]: Fragment memory cap: 4194304 bytes
```