ネットワーク見える化ソリューションの決定版

アプリケーションとトラフィックをリアルタイムに高速分析

ntopng

ntopng は、SNMP,DPI,NetFlow 全ての長所を
あわせもった特別なネットワークトラフィック分析製品です。

単一ホストの行動をどこまでも追える!
それが最強トラフィック分析ツール ntopng!

さらに

PATLITE®

連携で
素早い対応が
可能になります

ntopng： パトライト社製ネットワーク監視表示灯との連携利用

この資料では、ntop 社の ntopng とパトライト社製 MP3 再生ネットワーク監視表示灯「NH-FV シリーズ」の連携利用 「ntopng でアラートを検出したら、音声出力、パトライト監視表示灯を点灯させる方法」について説明します。

パトライト社製ネットワーク監視表示灯

パトライト社製ネットワーク監視表示灯「NH-FV シリーズ」は、SNMP TRAP を受信して障害の発生を光と音でいち早く管理者に知らせることができます。また、RSH コマンド、SOCKET 通信（PHN 互換コマンド、PNS コマンド）、HTTP コマンドで光、音声を制御することができます。

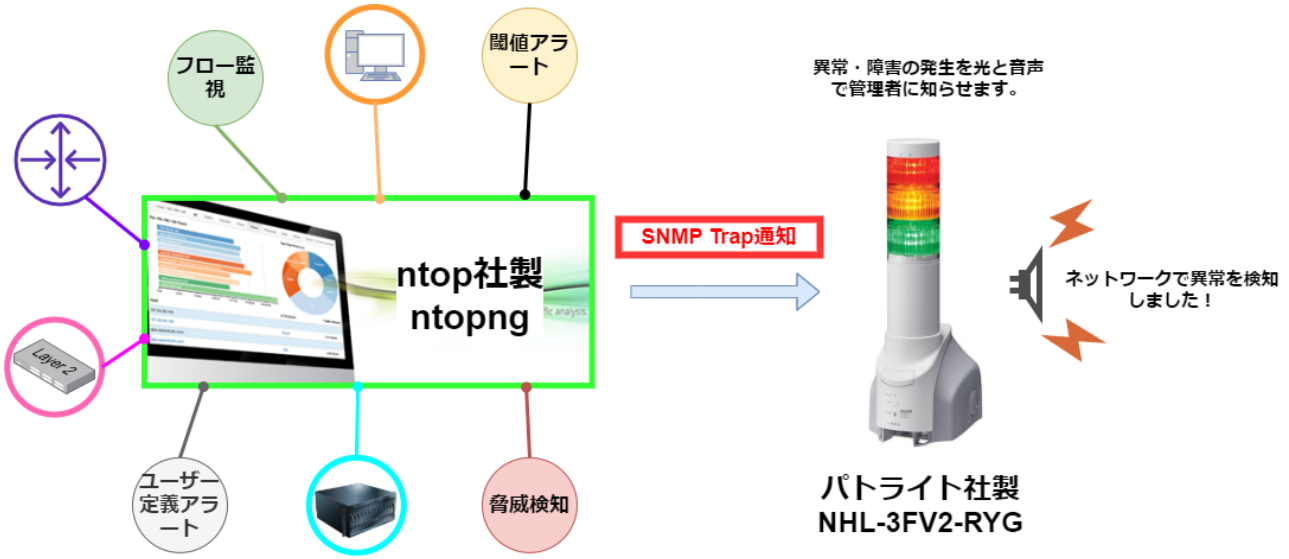
詳しくは、パトライト社 HP をご確認ください：
NH-FV シリーズ： https://www.patlite.jp/nh_fv/nh_fv01.html

この資料の説明には「NHP-3FV2-RYG」を使用しています。
ご利用のモデルまたはバージョンにより、設定画面が異なる可能性があります。

ntop 社製リアルタイム高速トラフィック分析 ntopng

ntopng はトラフィックをリアルタイムで監視し、ユーザースクリプトと呼ばれるプログラムに設定した条件や閾値に接触したフローを発見した場合、メール送信や外部サービスにアラートを発報することができます。このユーザースクリプトプログラムに SNMP TRAP 送信処理を追加することにより、パトライト社製のネットワーク監視表示灯を制御することができます。

この資料では、障害検出時に SNMP TRAP をパトライト監視表示灯に送信して表示灯を点灯する手順を紹介します。

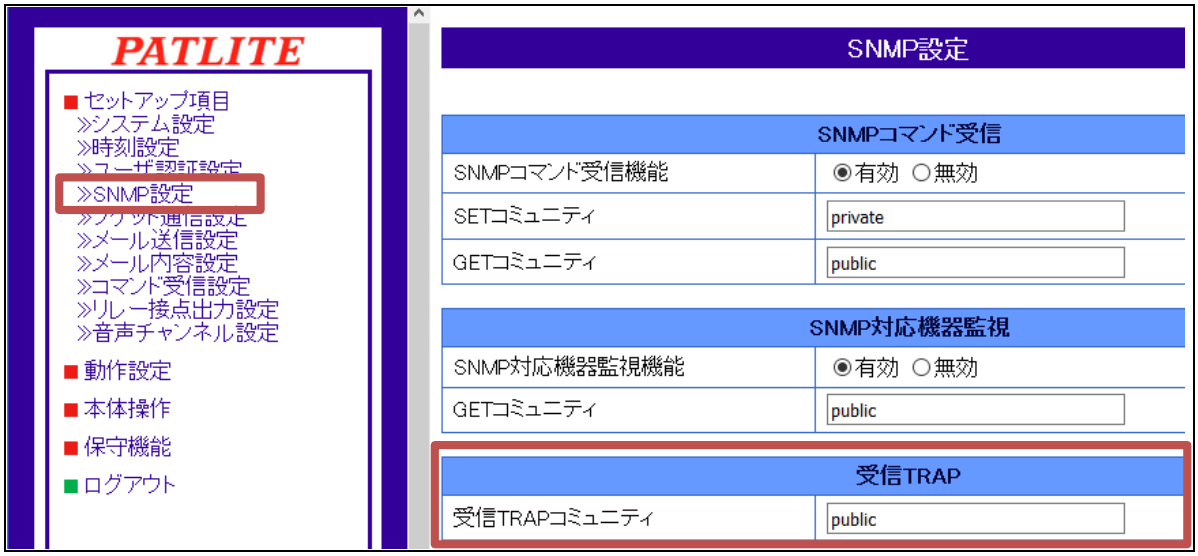


前提条件

- 表示灯のシステム設定で IP アドレスの設定が完了していること。

  「セットアップ項目 >> システム設定」で設定します。

- 表示灯の SNMP 設定が完了していること。
  SNMP TRAP を受信して表示灯を制御する場合は、**「セットアップ項目 >> SNMP 設定」→「受信 TRAP コミュニティ」**に通信時に使用するコミュニティ名を設定してください。(この資料では、デフォルトの `public` を使用します。



- ntopng のインストールおよび初期設定、監視登録が完了していること。

  本ドキュメントの例では ntopng の IP アドレスとして、192.168.91.46 を設定しています。

SNMP TRAP 送信での連携

ここでは、弊社作成の営業時間外にリモートアクセスした場合にアラートを発報するユーザースクリプト（名前: **時間外のリモートアクセス**[1]）を有効にし、ネットワーク監視表示灯の赤・黄・緑の色灯を点滅、音声で「ネットワークで異常を検知しました」とアナウンスするように設定します。

ntopng のユーザースクリプトを使えば、例えば以下のようなアラートを生成し、ネットワーク監視表示灯と連携することができます。

ユーザースクリプト名	説明
SYN スキャン攻撃者アラート	送信された SYN の数/分（応答なし）がしきい値を超えたときにアラートをトリガーします
SYN スキャン被害者アラート	受信した SYN の数/分（応答なし）がしきい値を超えたときにアラートをトリガーします
スループットアラート	平均スループット（送信+受信）がしきい値を超えたときにアラートをトリガーします
活動時間差分アラート	アクティビティ時間の差分がしきい値を超えたときにアラートをトリガーします

メモ: ユーザースクリプト/ホストの一部のアラートを記載しております。

表示灯の SNMP TRAP 受信設定で使用する ntopng の OID は以下の通りです:

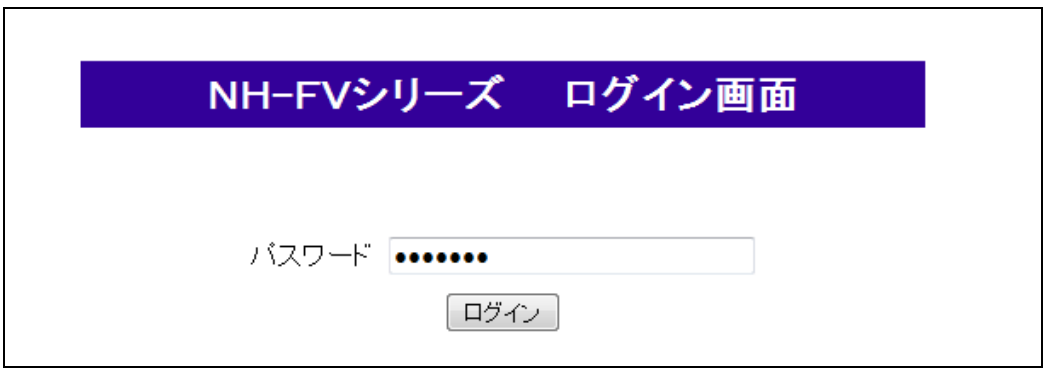
本例の TRAP 番号	説明
`.1.3.6.1.2.1.16.0.1`	risingAlarm を利用

メモ: ntopng の TRAP 通知は SNMP TRAP V2 形式を使用します。

表示灯側（NH-FV シリーズ）の設定

まず、表示灯側で SNMP TRAP を受信したときの動作を設定します。

Step 1. 表示灯の管理画面にログインします。



[1] **時間外のリモートアクセス**は弊社作成のプログラムであり、ntopng デフォルトではインストールされておりません。

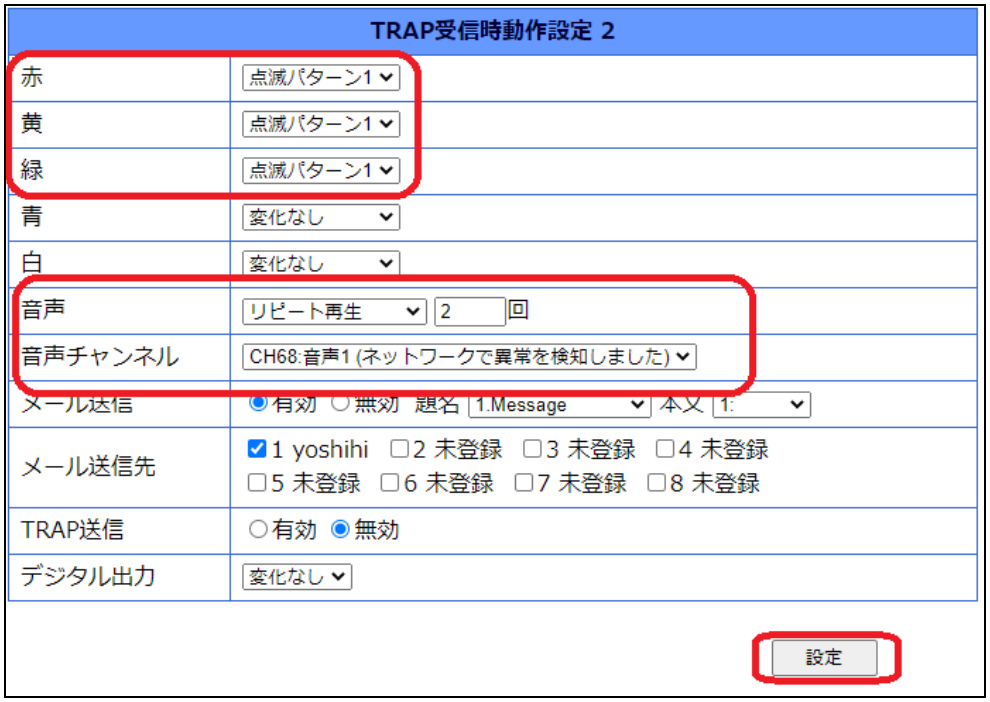
Step 2.　画面左のメニューから**「動作設定 >>TRAP 受信設定」**を選択します。

Step 3.　TRAP 受信設定を入力します。

「受信 TRAP グループ設定 2」で以下の情報を入力します

項目	説明
グループ名称	TRAP 通知の内容についてわかりやすい名前をつけて下さい
TRAP 送信元アドレス	TRAP 送信元のアドレス（例： ntopng の IP アドレス）
TRAP 番号	1.3.6.1.2.1.16.0.1

画面下部の「**TRAP 受信時動作設定 2**」で赤・黄・緑の色灯点滅と音声チャンネル再生を設定します。



最後に画面一番下の「設定」ボタンを押します。→「設定完了しました。」と表示されます。

これで表示灯側の設定は終了です。

ntopng 側の設定

ntopng 側で、ユーザースクリプト、**時間外のリモートアクセス**を設定します。

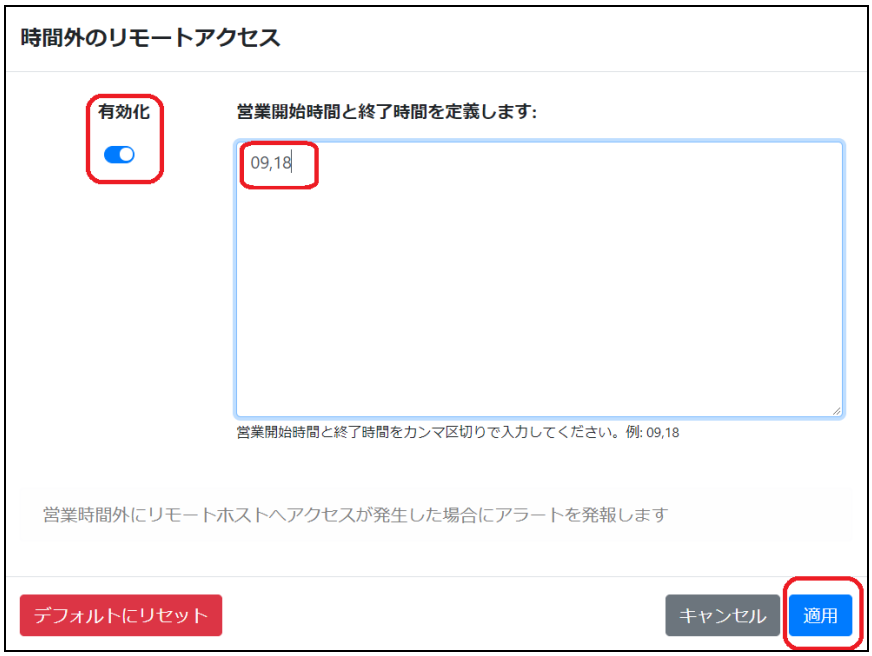
Step 1. ntopng Web インターフェースにログインします。

Step 2. 画面左メニュー「**設定**」-「**ユーザースクリプト**」から「**フロー**」タブをクリック、アクション列の編集ボタンをクリックしてください。

Step 3.　次に無効化タブをクリックしてください。

Step 4.　**時間外のリモートアクセス**のアクション列、編集ボタンをクリックしてください。

Step 5.　有効化スイッチを押し、営業開始と終了時間を「,」区切りで設定後、適用ボダンをクリックしてください。



これで ntopng 側の設定は終了です。

動作について

設定したユーザースクリプトの条件に一致すると、SNMP TRAP が表示灯に送信されます。赤・黄・緑色の表示灯が点滅し、同時に音声アナウンスが3回再生されます。

以上

お問い合わせ

弊社では、ntopng に関するご意見、フィードバックをお待ちしております。

ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

住所：　〒183-0023 東京都府中市宮町 2-15-13 第 15 三ツ木ビル 8F
URL：　http://www.jtc-i.co.jp/
電話番号：　042-358-1250
FAX 番号：　042-360-6221
ご購入のお問い合わせ：
　お問い合わせフォーム　https://www.jtc-i.co.jp/contact/scontact.php
　メール　sales@jtc-i.co.jp
製品サポートのお問い合わせ：
　カスタマーポータル　https://www.jtc-i.co.jp/support/customerportal/

※ PATLITE、パトライト、シグナル・タワーは、株式会社パトライトの登録商標です。
※ ntopng は ntop 社の登録商標です。