パケットキャプチャ取得方法

目次

はじめに

本書では、InterSafeWebFilter(以下 ISWF)及び InterSafe CATS(以下 CATS)の問題切り分けのために、パケットキャプチャについて説明をしています。パケットキャプチャとは、実際のネットワーク上で流れるトラフィックのパケットを採取することです。

パケットキャプチャはネットワーク上で障害が発生した場合に、どこに問題があるのか解析するために実施します。

Windows OS では wireshark というツールを使ってパケットキャプチャの取得を行います。Linux OS、Solaris OS では、コマンドを用いてパケットキャプチャの取得を行います。

wireshark は、Windows OS 上にてパケットキャプチャを取得するためのツールです。

wireshark について、詳しくは下記のサイトやインターネット上のサイトを参考にしてください。

http://www.wireshark.org/

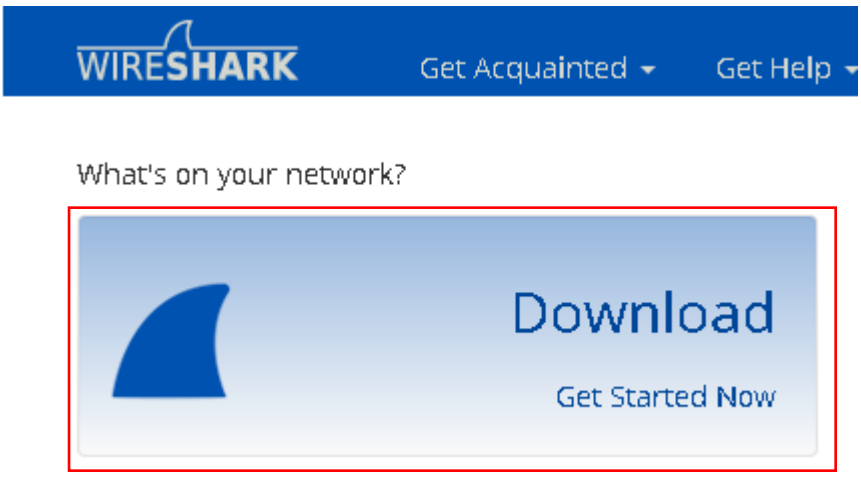
Windows OS 上でのパケット取得方法

Windows OS 上でパケットを取得するために、wireshark というツールを利用します。

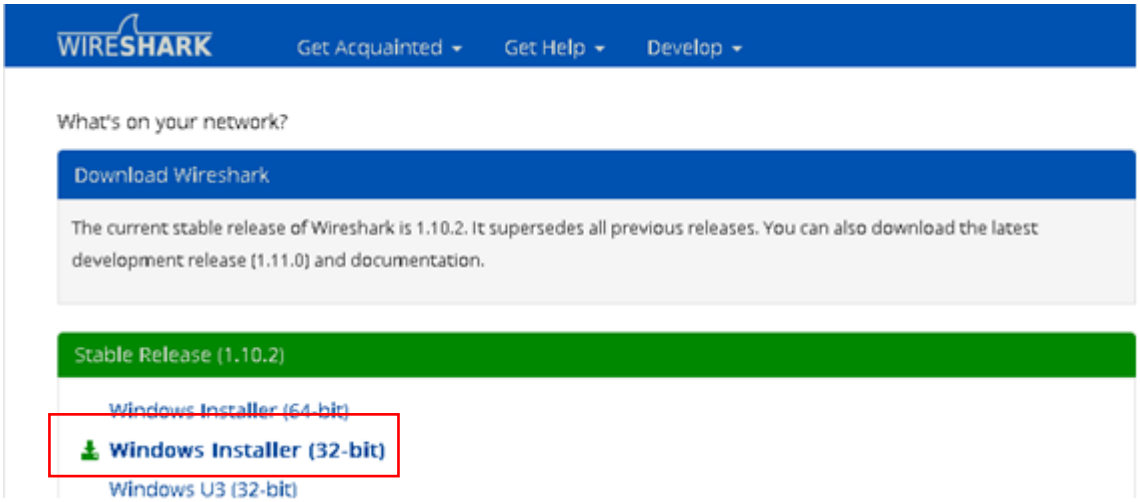
以下の URL から wireshark のダウンロードを行ないます。

http://www.wireshark.org/

1) [http://www.wireshark.org/]にアクセスし、「Download」のリンクをクリックします。



2) のマークがついている Windows Installer をクリックしてインストーラをダウンロードします。

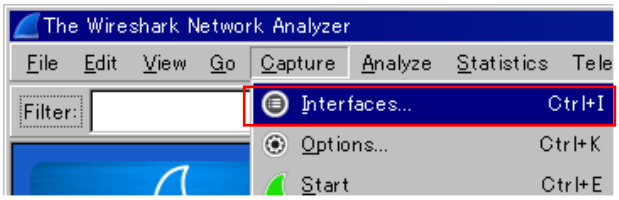


※上記は 2013 年 10 月現在の情報になります。

3) wireshark のダウンロード後、exe ファイルをクリックしインストールをして下さい。

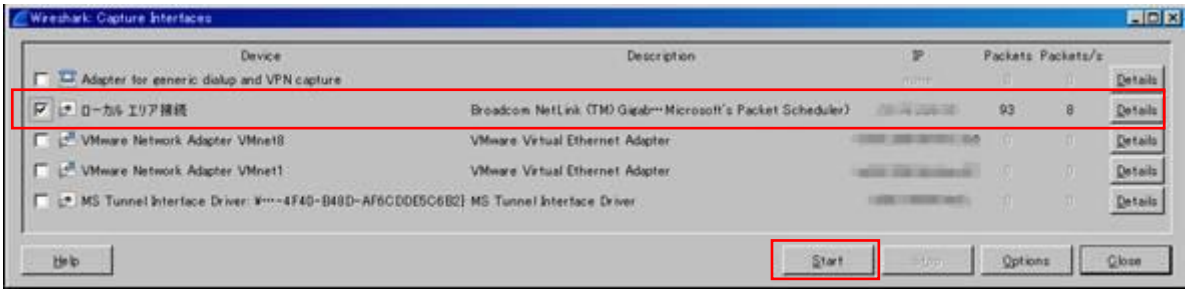
4) インストール完了後、デスクトップにある wireshark のショートカットを起動します。

5) 起動後、ツールバーの Capture > Interfaces を選択します。

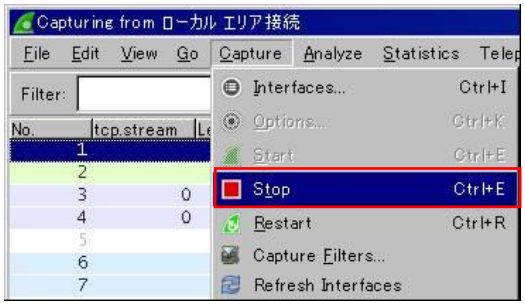


6) 「Packets」列の数字が増加している「Device」にチェックをつけ、「start」をクリックします。

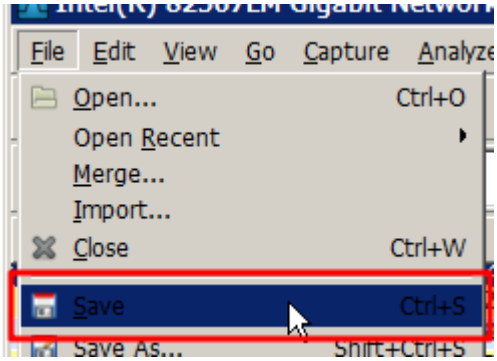
「start」をクリックするとキャプチャが開始されます。



7) ツールバーの Capture > stop を選択して、パケットキャプチャを終了します。

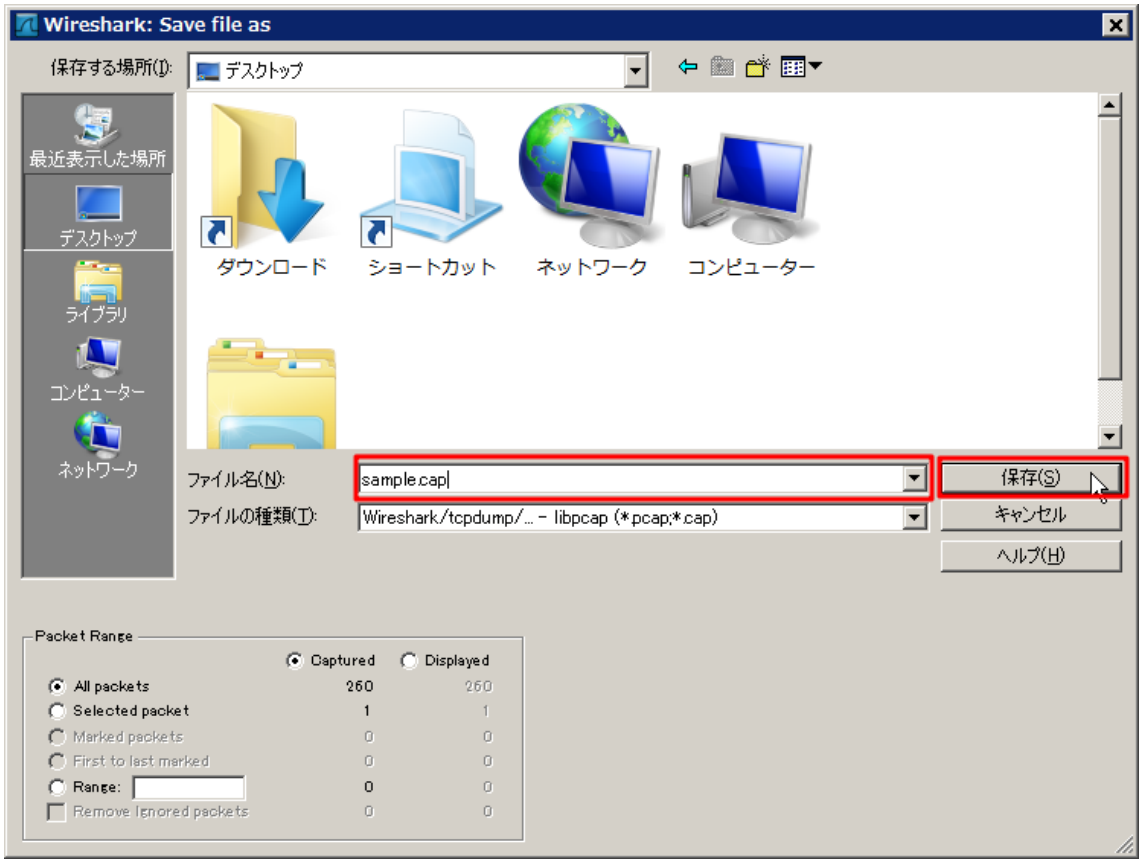


8)　ツールバーの File > Save を選択します。



9)　保存画面が表示されますので、任意の名前を付けて保存してください。

※拡張子は「.cap」で保存してください。



Linux OS 上でのパケット取得方法

OS の tcpdump コマンドを利用します。

例) tcpdump -x -s 3000 -w ファイル名

-x ・・・ 全ての情報を取得

-s ・・・ データ長

-w ・・・ ファイルへ出力

コマンドを実行したディレクトリに「ファイル名」で指定したファイルが作成されます。

Solaris OS 上でのパケット取得方法

OS の snoop コマンドを利用します。

例) snoop –o ファイル名

コマンドを実行したディレクトリに「ファイル名」で指定したファイルが作成されます。

パケットキャプチャ取得方法

2013 年 10 月 第 3 版

作成/発行/企画 アルプスシステムインテグレーション株式会社

〒145-0067　東京都大田区雪谷大塚町 1-7