



Snort+Gigapcap インストールマニュアル

ここでは SNORT (R) 2.4.4 を対象として、Snort をシステムに組み込む方法を説明します。また、GigaPcap 上に Snort を組み込む方法を説明します。

Linux 系の OS 上で Snort を利用するには、パケットキャプチャ用のライブラリである libpcap が必要です。GigaPcap は libpcap の機能が含まれており、Snort のコンパイル時に GigaPcap 用のライブラリを指定することで libpcap を使用します。

1. Snortをシステムに組み込む

1-1. Install PCAP

Snort のインストールの前に libpcap のインストールを行います。
[参考] libpcap の公式サイト : <http://www.tcpdump.org>

- 1.Download libpcap-0.9.4.tar.gz
- 2.tar zxvf libpcap-0.9.4.tar.gz
- 3.cd libpcap-0.9.4
4. ./configure
5. make
6. make install

1-2. Install pcre-6.6.tar.gz

pcre の組み込みを行います。

- 1.Download pcre-6.6.tar.gz
- 2.tar zxvf pcre-6.6.tar.gz
- 3.cd pcre-6.6
4. ./configure
5. make
6. make install

1-3. Install Snort-2.4.4

Snort のインストールを行います。

- 1.Download snort-2.4.4.tar.gz
- 2.tar zxvf snort-2.4.4.tar.gz
- 3.cd snort-2.4.4
4. ./configure --prefix=/opt/snort
5. make
6. make install

1-4. Install Rules for Snort2.4.4

Snort のフィルタールールのインストールを行います。

1. Download snortrules-snapshot-2.4_s.tar
2. tar zxvf snortrules-snapshot-2.4_s.tar

1-5. Configuration for Rule and Log files

最後にフィルタールールとログファイルの設定を行います。

1. /var/log/snort where Snort creates log files by default.
2. /opt/snort/etc. to save configuration files.
3. /opt/snort/rules to save rules files.
4. Copy snort.conf,classification.config and reference.config files from /opt/snort2.4.4/etc to /opt/snort/etc directory .
- 5.Copy all file in Rules (step IV) to /opt/snort/rules.

2. Snort を GigaPcap 上に組み込む

2-1. Install pcre-6.6.tar.gz

前述 “1-2 Install pcre-6.6.tar.gz” と同じです。

2-2. Install Snort-2.4.4

Snort のコンパイル時に GigaPcap 用のライブラリを指定します。

- 1.Download snort-2.4.4.tar.gz
- 2.tar zxvf snort-2.4.4.tar.gz
- 3.cd snort-2.4.4
- 4.以下のオプションを指定して実行します。

```
./configure --with-pcap=/usr/lra
              --without-ucd-snmp
              --with-libpcre-libraries=/usr/local/lib
              --with-libpcre-includes=/usr/include/pcre
              --with-libpcap-includes=/usr/lra/inc
              --with-libpcap-libraries=/usr/lra/lib
```
5. make
6. make install

2-3. How to verify Snort is complied with Gigapcap or not?

GigaPcap上でSnortが動作するかどうかの確認を行います。

#snort -Vコマンドを実行した時に下記のように

```
Welcome to Gigapcap! Copyright (C) 2006 u10 Networks
```

の表示が出ればGigaPcap上でSnortが組み込まれた状態になっています。

```
[root@PE2850 tatenol# snort -V
Welcome to Gigapcap! Copyright (C) 2006 u10 Networks

,,_      -*> Snort! <*-
o"  )~   Version 2.6.0 (Build 59)
""      By Martin Roesch & The Snort Team: http://www.snort.org/team.html
        (C) Copyright 1998-2006 Sourcefire Inc., et al.
```

2-4. Initial Testing

GigaPcap上でSnortが動作しているか確認を行う。GigaPcap上に組み込んでいない場合と比べてほぼ同じメッセージが表示される。

Run

```
/opt/snort/bin/snort -v -i ra:0:0
```

Output

Initializing network Interface ra:0:0

.....

```
07/03-17:11:51.453804 1.2.3.4:4660 -> 10.11.12.13:43981
```

```
UDP TTL:128 TOS:0x0 ID:0 IpLen:20 DgmLen:984
```

```
Len: 956
```

```
=====  
=====
```

```
07/03-17:11:51.453820 1.2.3.4:4660 -> 10.11.12.13:43981
```

```
UDP TTL:128 TOS:0x0 ID:0 IpLen:20 DgmLen:984
```

```
Len: 956
```

```
=====  
=====
```

```
07/03-17:11:51.453836 1.2.3.4:4660 -> 10.11.12.13:43981
```

```
UDP TTL:128 TOS:0x0 ID:0 IpLen:20 DgmLen:984UDP TTL:128 TOS:0x0 ID:0 IpLen:20 DgmLen:984
```

```
=====  
=====
```

Snort received 2021879 packets

Analyzed: 184664(9.133%)

Dropped: 1837215(90.867%)

```
=====  
=====
```

Breakdown by protocol:

TCP: 0 (0.000%)

UDP: 184665 (9.133%)

ICMP: 0 (0.000%)

ARP: 0 (0.000%)

EAPOL: 0 (0.000%)

IPv6: 0 (0.000%)

ETHLOOP: 0 (0.000%)

IPX: 0 (0.000%)

FRAG: 0 (0.000%)

OTHER: 0 (0.000%)

DISCARD: 0 (0.000%)

```
=====  
=====
```

Action Stats:

ALERTS: 0

LOGGED: 0

PASSED: 0

```
=====  
=====
```

Snort exiting

会社名 : ユーテン・ネットワークス株式会社

URL : <http://www.u10networks.com/>

製品お問い合わせ : sales@u10networks.com

※Snort is a registered trademark of Sourcefire, Inc