

「不正アクセスの高感度検出及び
グローバル警戒機構に関する研究」
報告書

第 編 インストールマニュアル

平成13年2月

情報処理振興事業協会
セキュリティセンター

目次

<u>1. IDWS - インストール・マニュアル</u>	1
<u>1.1. パッケージについて</u>	1
<u>1.2. 1.2 事前に必要とされる環境設定</u>	1
<u>1.3. 1.3 パッケージのインストール</u>	1
<u>1.4. アプレットのパーミッション設定</u>	2
<u>1.5. Configuration の設定</u>	2
<u>1.5.1. Manager Configuration ファイル</u>	3
<u>1.6. Plugin に関する配置とインストール</u>	4
<u>1.6.1. ID MIB インストールガイド</u>	4
<u>1.6.2. Snort Output Plugin インストールガイド</u>	5
<u>1.6.3. SML-XML Plugin インストールガイド</u>	9
<u>1.6.4. 統計 MIB Plugin インストールガイド</u>	11
<u>1.6.5. XML-SMI Plugin インストールガイド</u>	13
<u>1.7. IDWS パッケージを走らせる</u>	14

1. IDWS - インストール・マニュアル

1.1. パッケージについて

パッケージは `idws.tar.gz` のファイル名で表示される。

1.2. 事前に必要とされる環境設定

- JDK のバージョン 1.2 がフルインストールされていること
- Perl の 5.0 もしくはそれ以上に新しいバージョンがフルインストールされていること

1.3. パッケージのインストール

ユーザのホームディレクトリに `idws.tar.gz` のファイル (パッケージ) をコピーする。このファイルを展開するために、次のような操作を行う。

```
% zcat idws.tar.gz | tar xvf-  
or  
% gunzip idws.tar.gz  
% tar -xvf idws.tar
```

`public_html` というディレクトリが作成される。

```
% <~user>/public_html
```

`public_html` 以下は次のように構成される。

a. ディレクトリ

```
idws2  
roman  
lib
```

b. シェル・スクリプト

```
startIDWS      - IDWS パッケージ起動スクリプト  
startINMI     - INMI パッケージ起動スクリプト
```

ディレクトリ `idws` 以下の構成は次のようになっている。

- a. ディレクトリ
 - data
 - manager
- b. アーカイブ・ファイル
 - Smi2Xml.tar.gz - SMI to XML プラグイン
 - StatisticsMIBRequiredFiles.tar.gz - Statistics MIB プラグイン
 - Xml2Smi.tar.gz - XML to SMI プラグイン
 - idsMIBAgentRequiredFiles.tar.gz - ID MIB プラグイン
 - snifferRequiredFiles.tar.gz - Snort Output プラグイン
- c. その他
 - romanapplet.html
 - getPacket
- d. README ファイル
 - README - IDWS インストール Readme
 - README.IDMIB - ID MIB インストール Readme
 - README.PLUGIN -Snort 出力 Plugin インストール Readme
 - README.SMI2XML - SMI to XML Plugin インストール Readme
 - README.STATSMIB- Statistics MIB Plugin インストール Readme
 - README.XML2SMI - XML to SMI Plugin インストール Readme

1.4. アプレットのパーミッション設定

アプレットのパーミッション設定を行うファイルは PC 使用の場合は WINDOWS ディレクトリに、UNIX 使用の場合にはユーザのホームディレクトリにある。

JDK1.2 に付属されている `policytool` はパーミッションのポリシへのアクセスを設定するために使用される。このプログラムを走らせるには、以下のようにコマンドプロンプトで `policytool` というコマンドを打ち込めばよい。

```
% policytool
```

なお、アプレットには全てのパーミッションが与えられるのが望ましい。

1.5. Configuration の設定

パッケージを走らせる前に、ユーザ環境に合うように Configuration ファイルが配置・保存される必要がある。

1.5.1. Manager Configuration ファイル

1.5.1.1. snmp.conf

このファイルが格納される位置は、以下のように ~user/idwsConfig/CysolIDS /tmp/CysolIDS.conf ファイルの中で明示される。

```
IDSSNMPCONFFILE. /tmp/Snmp.conf
```

このファイルは以下のような Configuration に関する変数 (パラメータ) を保持している。

- a. snmptrapd コマンドについてはマネージャがインストールされているマシン上で snmp デーモンが走っているかを明示する必要がある。以下のように明示される。
snmptrapdCommand = snmptrapd -p 5772 -P -On
- b. snmpinform command header は以下のように明示される必要がある。
snmpinformheader = snmpinform -v2c -p 5772
- c. 時間ベースの相関分析のためのタイムアウト設定の必要性。以下のように秒単位で明示される。
CorrelationTimeout = 25
- d. Scan ベースの相関分析のためのタイムアウト設定の必要性。上と同様に、秒単位で明示される必要がある。
ScanCorrelationTimeout = 30,000

このファイルのコピーは public_html/idws2/manager/conf ディレクトリの下にある。

1.5.1.2. Agentslist.cf

このファイルが格納場所は ~user/idwsConfig/CysolIDS ファイルの中で以下のように明示される。

```
AGENTCONFFILE. /tmp/AgentsList.cf
```

これは、パターン相関分析のための SNMP query を受けとる agent のリストを保持しているファイルである。以下のように明示される。

```
Agent1 = 192.0.0.30  
Agent2 = 192.0.0.40
```

このファイルのコピーは public_html/idws2/manager/conf ディレクトリの下にある。

1.5.1.3. CySolIDS.conf

このファイルは、`~user/idwsConfig`にある。IDWS が使用する全てのファイルのパスはここに記述される。

このファイルのコピーは `public_html/idws2/manager/conf` ディレクトリの下にある。

1.6. Plugin に関する配置とインストール

1.6.1. ID MIB インストールガイド

1.6.1.1. パッケージ

このパッケージは `idsMIBAgentRequiredFiles.tar.gz` という名前のアーカイブ・ファイルである。これは IDS Notification MIB を追加のために、`ucd-snmp-4.1.2agent` が拡張されたものである。

1.6.1.2. 事前に必要とされる環境設定

システム中に `ucd-snmp-4.1.2` がインストールされていることが必要である。

1.6.1.3. パッケージのインストール

1. 1.6.1.2の環境設定がなされていないならば `ucd-snmp-4.1.2`をインストールする。
2. 以下のようにして `ucd-snmp-4.1.2`ディレクトリに移動。
`% cd ucd-snmp-4.1.2`
3. 以下のようにしてアーカイブ・ファイルをコピー。
`% cp idsMIBAgentRequiredFiles.tar.gz`
4. 以下のコマンドを使用してアーカイブ・ファイルを展開。
`% zcat idsMIBAgentRequiredFiles.tar.gz | tar xvf -`

この展開により、以下のようなファイル群が作られる。

```
agent/mibgroup/mIdMIB.c
agent/mibgroup/mIdMIB.h
config/outdata.conf
idsMibs/IDS_MIB.txt
```

5. 以下のコマンドでパッケージの配置 (コンフィギュア) を行う。

```
% ./configure --prefix=<install Path for snmpd and snmptrapd >
--with-mib-modules="mIIdMIB" --with-
mibdirs="/usr/local/share/snmp/mibs:
<absolute path of ucd-snmp-4.1.2 directory>/idsMibs"
```

注意：特別な設定を行わない場合、snmpd のパスは /usr/local/sbin のようになっている。
--prefix というオプションを configure のコマンドに付けることで異なるパスに snmpd をインストール出来る。

6. パッケージを build するために以下のコマンドを用いる。

```
% make
```

7. パッケージのインストールを以下のように行う。

```
% make install
```

1.6.1.4. Configuration の設定

config/outdata.conf

これは作成されるデータベースのファイル名とパスの設定に使用される。ここに snort によって書かれ作成される the incident.idb への絶対パスを与える。

String の = の左側には incidentDBPath があることに注意されたい。

1. snmpd を以下のように起動。

```
% sbin/snmpd -p 5555
```

2. 警告を受けた後、以下のようにしてテーブルを見ることが出来る。

```
% snmpwalk -p 5555 <host> <community> mIIdMib
```

または

```
% snmpwalk -p 5555 <host> <community> 47733
```

1.6.2. Snort Output Plugin インストールガイド

1.6.2.1. パッケージ

2つのアーカイブ・ファイルからパッケージは構成されている。

1. cysol-snort.tar.gz
2. snifferRequiredFiles.tar

1.6.2.2. パッケージのインストール

1. snort をインストールするディレクトリに移動。システムに snort をコンパイルするのに必要なライブラリがインストールされていることを確認する。
2. `cp cysol-snort.tar.gz .`
3. `zcat cysol-snort.tar.gz | tar xvf -`
4. `cd sniffer`
5. `cp snifferRequiredFiles.tar.gz .`
6. `zcat snifferRequiredFiles.tar.gz | tar xvf -`
7. `cd snort`
8. `./configure --prefix=<Absolute path of snort>`
9. 以下のように Makefile 中 LIBS パスをアップデートする。
`LIBS = -lpcap -lsocket -lssl -lcrypto`
10. `make clean`
11. `make`
12. `make install`

1.6.2.3. パッケージのインストール (詳細)

snort をインストールするディレクトリに移動。

1. `cysol-snort.tar.gz` をコピーする。
`% cp cysol-snort.tar.gz .`
2. 以下のコマンドを用いてアーカイブ・ファイルを展開。
`% zcat cysol-snort.tar.gz | tar xvf -`
この操作により `sniffer/snort` ディレクトリが作成され、全ての snort のファイルがそこに保持される。
3. `sniffer` ディレクトリに移動。
`% cd sniffer`
4. `snifferRequiredFiles.tar.gz` file. をコピー。
`% cp snifferRequiredFiles.tar.gz .`
5. 次のようなコマンドを用い、アーカイブを展開。
`zcat snifferRequiredFiles.tar.gz | tar xvf -`
この操作により以下のファイルとディレクトリが複製される。
`./snort/idwsControl.c`
`./snort/idwsControl.h`

```
./snort/spo_snortnet.c
./smort/spo_snortnet.h
./config/SnortPlugin.conf
./config/CysolIDS.conf
./snortlog/
./startsnort
./rules.txt
./data/
```

6. snort ディレクトリに移動。

```
% cd snort
```

7. 以下のコマンドで

```
% ./configure --prefix=<Absolute path of snort>
```

8. 以下のように Makefile 中 LIBS パスをアップデートする。

```
LIBS = -lpcap -lsnmp -lkstat -lsocket -lnsl -L/usr/local/ssl/lib -lcrypto
```

9. make clean を行う。

```
% make clean
```

10. パッケージを build する。

```
% make
```

11. パッケージをインストールする。

```
% make install
```

1.6.2.4. Configuration の設定

1. CysolIDS.conf

場所: ~user/idwsConfig

CysolIDS.conf はディレクトリ sniffer/config からディレクトリ/tmp にコピーされる。CysolIDS.conf ファイルの中でファイル中のパスを明示する。

2. SnortPlugin.conf

場所: ~user/idwsConfig

SnortPlugin.conf は sniffer/config から CysolIDS.conf configuration ファイルに記述されているパスにコピーされる。Configuration ファイルの中は以下の通り。

```
footprintDBPath = /opt/home/idws/sniffer/data/footprint.idb;
incidentDBPath  = /opt/home/idws/sniffer/data/incident.idb;
manager         = megahira public 5772;
engineID        = 80 00 07 E5 01 C0 00 00 1E;
```

```
SENSORID      = MySensorID 12345
SENSORVERSION = My SensorVersion Alpha 1.1
ALERTVERSION  = My Alert Version 1.0
SENSORLOCALADDRESS = 192.168.0.31
```

1行目は footprint.idb ファイルのパスを明示しており、2行目は incident.idb file のパスを、3行目は snmp inform が送られるマネージャを、4行目は snort が走っているホストマシンのエンジン ID を明示している。エンジン ID はホストマシン上の snmpwalk により得られる。

String の = の左側には incidentDBPath、footprintDBpath、manager、engineID、SENSORID、SENSORVERSION、ALERTVERSION、SENSORLOCALADDRESS があることに注意されたい。

1.6.2.5. パッケージのインストール

1. snort ディレクトリ中の親ディレクトリに移動。
2. snifferRequiredFiles.tar.gz を以下のようにコピー。
`% cp snifferRequiredFiles.tar.gz .`
3. 以下のコマンドを用いて tar 型を展開する。

```
zcat snifferRequiredFiles.tar.gz | tar xvf -
```

この操作により以下のファイルとディレクトリが複製される。

```
/snort/idwsControl.c
./snort/idwsControl.h
./snort/spo_snortnet.c
./smort/spo_snortnet.h
./config/SnortPlugin.conf
./config/CysolIDS.conf
./snortlog/
./startsnort
./rules.txt
./data/
```

4. snort ディレクトリへ移動。
`% cd snort`
5. Makefile.am の内容を変更。
idwsControl.c と idwsControl.h を snort_SOURCES に加える。

そして snort_SOURCES から spo_log_database.c と spo_log_database.h を取り除くことが必要。なぜならいくつかの変数が ucd-snmp 中の変数とクラッシュを起こす可能性があるからである。

6. plugbase.h から次に示される行を消去。
`#include "spo_log_database.h"`
7. plugbase.c から次に示される行を消去。
`SetupLogDatabase();`
8. 以下のように automake を行う。
`automake Makefile`
9. 以下のように configure を行う。
`% ./configure --prefix=<Absolute path of snort>`
10. Makefile 中の LIBS path を以下のようにアップデートする。
`LIBS = -lpcap -lsnmp -lkstat -lsocket -lnsl -L/usr/local/ssl/lib -lcrypto`
11. make clean を行う。
`% make clean`
12. make を行う。
`% make`
13. make install を以下のように行う。
`% make install`

1.6.2.6. パッケージを走らせる

1. sniffer ディレクトリへ移動。
2. super ユーザになる。
3. 以下のように startsnor のスクリプトを走らせる。t
`startsnort`

もし前の snort のログを消去したいときは、snortlog/alert ファイルの Delete に yes を選択する。

1.6.3. SML-XML Plugin インストールガイド

1.6.3.1. パッケージ

Smi2Xml.tar.gz というアーカイブ・ファイルがパッケージである。

1.6.3.2. パッケージのインストール

1. Plugin をインストールしたいディレクトリに移動する。
2. `cp Smi2Xml.tar.gz .`
3. `zcat Smi2Xml.tar.gz | tar xvf -`
4. `gcc -o Smi2Xml Smi2Xml.c`
5. XMLDests という configuration ファイルに向けて XML が送られる電子メールアドレスを追加する。
6. `snmptrapd.conf` に次の 1 行を追加する。

```
traphandle .1.3.6.4.1.282.17.5.1 ~user/SmiXml/Smi2Xml
-c ~user/idwsConfig/CysolsIDS.conf
```

1.6.3.3. パッケージのインストール

1. Plugin をインストールしたいディレクトリに移動する。
2. 以下のようにして `Smi2Xml.tar.gz` ファイルをコピー。

```
% cp Smi2Xml.tar.gz .
```
3. アーカイブ・ファイルを以下のコマンドで展開。

```
% zcat Smi2Xml.tar.gz | tar xvf -
```

この操作により以下のファイルが複製される。

```
SmiXml/Smi2Xml.c
SmiXml/Smi2Xml.h
SmiXml/SMIXMLtab
SmiXml/XMLDests
```
4. `SmiXml` ディレクトリに移動し、下記のようにプログラムをコンパイルする。

```
% gcc -o Smi2Xml Smi2Xml.c
```

1.6.3.4. Configuration の設定 (セットアップ)

XML Dests

XML ファイルがメールで送信される相手を配置するために存在するのが `XMLDests` ファイルである。

格納場所 : 以下で明示される `/tmp/CysolIDS.conf` configuration ファイル中の行

```
XMLDESTSFILE /tmp/XMLDests
```

この config ファイルは以下のフォーマットを有する。

idws@megahira

root@hakuba

SMIXMLtab

SMIXMLtab configuration ファイルは SMI もしくは XML 変換に用いられる。

格納場所：~user/idwsConfig/CysolIDS.conf ファイル中の以下の行

```
SMIXMLTABFILE /tmp/SMIXMLtab.
```

smnptrapd.conf

格納場所：次のような共有ディレクトリ以下の snmp ディレクトリ

usr/local/share/snmp

以下の行は smnptrapd プログラムが smnp inform を受信したときはいつでも SMI2XML を実行するために加えられなくてはならない。

```
traphandle .1.3.6.4.1.282.17.5.1 ~user/SmiXml/Smi2Xml -c ~user/idwsConfig/CysolsIDS.conf
```

1.6.3.5. パッケージを走らせる

マネージャが起動するとき、traphandler を呼ぶ smnptrapd が起動される。

1.6.4. 統計 MIB Plugin インストールガイド

1.6.4.1. パッケージ

このパッケージは StatisticsMIBRequiredFiles.tar.gz というアーカイブファイルで与えられる。

1.6.4.2. 事前に必要とされる環境設定

システム中に ucd-snmp-4.1.2 がインストールされていること。

1.6.4.3. パッケージのインストール

1. もし環境設定がなされていないならば、ucd-snmp-4.1.2 をインストールする。

2. 以下のようにファイルをコピーし、tar 型の展開を行う。

```
% cd ucd-snmp-4.1.2
% cp StatisticsMIBRequiredFiles.tar.gz
% zcat StatisticsMIBRequiredFiles.tar.gz |tar xvf -
```

この操作により以下のようなファイルを作成する。

```
agent/mibgroup/idTrStatsMIB.c
agent/mibgroup/idTrStatsMIB.h
config/TrafficData.conf
idsMibs/STATISTICS_MIB.txt
```

3. ucd-snmp-4.1.2 ディレクトリへ移動。

```
% cd ucd-snmp-4.1.2
```

4. 以下のようにパッケージの configure を行う。

```
%. /configure --prefix=<install Path for snmpd and snmptrapd >
--with-mib-modules="idTrStatsMIB"--with-mibdirs= "/usr/local/share/snmp/mibs:
<absolute path of ucd-snmp-4.1.2 directory>/idsMibs"
```

例としてユーザ idws の場合、以下のように configure される。

```
%. /configure --prefix="." --with-mib-modules="idTrStatsMIB"
--with-mibdirs= "/usr/local/share/snmp/mibs:
/export/zaohome/nandita/ucd-snmp-4.1.2/idsMibs"
```

注意：snmp の特に設定をしない場合のインストール・パスは `is /usr/local/sbin` である。Configure コマンドに `--prefix` コマンドをつけてやることで、snmp に異なるパスをインストールすることが出来る。

5. 次のコマンドによりパッケージを build する。

```
% make
```

6. 以下によりパッケージをインストールする。

```
% make install
```

1.6.4.4. Configuration の設定 (セットアップ)

config/TrafficData.conf

Traffic Statistic データファイルの名前とパスを configure するために用いられるのが TrafficData.conf ファイルである。ここで RMONagent によって書き込まれ、作られる Traffic_Stat_table.txt ファイルに絶対パスを与える。

1. snmpd 起動。

```
% sbin/snmpd -p 6666
```

2. Traffic-Stat-Table というデータファイルに Traffic の統計結果が書き込まれた後は以下のようにしてそれを見ることが出来る。

```
% snmpwalk -p 6666 <host> <community> idTrStatsMIB
```

or

```
% snmpwalk -p 6666 <host> <community> 47734
```

注意: 入力データファイル名は Traffic-Stat-Table.txt. このファイル名を固定させなくてはならないことはないが、しかしこのファイルの格納される場所は TrafficData.conf ファイルの中で言及されている必要がある。

1.6.5. XML-SMI Plugin インストールガイド

1.6.5.1. パッケージ

このパッケージは Xml2Smi.tar.gz というアーカイブ・ファイルである。

1.6.5.2. パッケージのインストール

1. Plugin をインストールしたいディレクトリに移動する。
2. `cp Xml2Smi.tar.gz .`
3. `zcat Xml2Smi.tar.gz | tar xvf -`
4. JAVA XML パーサをインストールし、次のようにコンパイルする。
`javac XMLAlertParser.java`
5. 以下の行を forward ファイルに書き込む。
`"|usr/bin/perl /tmp/extXml.pl"`

1.6.5.3. パッケージのインストール

1. Plugin をインストールしたいディレクトリに移動する。
2. 以下のようにして Xml2Smi.tar.gz ファイルをコピー。
`% cp Xml2Smi.tar.gz .`
3. 以下のようにしてアーカイブ・ファイルを展開。
`% zcat Xml2Smi.tar.gz | tar xvf -`

この操作により以下のファイルが複製される。

```
XmlSmi/XMLAlertParser.java
```

```
XmlSmi/AlertData.css
```

```
XmlSmi/SMIXMLtab
XmlSmi/extXml.pl
XmlSmi/idmef-message.dtd
```

4. 下のようにしてプログラムのコンパイルを行う。

XMLAlertParser.java をコンパイルするためには Java XML parser が必要となる。以下のサイトからダウンロード可能 site www.java.sun.com/xml/download.html

```
% javac XMLAlertParser.java
```

1.6.5.4. Configuration の設定 (セットアップ)

```
.forward
```

格納されている場所：ユーザのホームディレクトリ

以下の行を.forward ファイルに追加。

```
"|/usr/bin/perl /tmp/extXml.pl"
```

1.6.5.5. パッケージを走らせる

メールがこのアカウントにやってくる時はいつでも、XMLAlertParser プログラムは XML ファイルを調べ SMI ファイルに書き込む。

1.7. IDWS パッケージを走らせる

1. public_html ディレクトリに移動。

```
% cd ~<user>/public_html
```
2. IDWS マネージャを起動。

```
% startIDWS
```
3. 他のコンソールから INMI を起動。

```
% cd ~<user>/public_html
% startINMI
```

もし INMI を離れた場所から走らせたいときは、以下のように起動する。

```
% appletviewer http://<manager IP address>/<~username>/romanapplet.html
```

4. snort plugin を起動する。詳細についてはこのパンフレットの Snort についての部分を参照のこと。

5. 攻撃の可視化について

適切なルールが rules.txt に書き込まれれば、そのルールにあう（反する？）不法なパケットは検知され、警告が表示されマップ上に可視化される。

可視化のためには INMI ウィンドウ上にネットワーク・マップが表示されなくてはならない。

見るためには、ユーザ・インターフェースにある view メニューの下の Show Alerts List というアイテムを HTML 上でクリックすればよい。