

# Synesis

## トレースファイルの保存先変更

---

Rev.A

## 内容

1. はじめに.....	3
1.1. 概要.....	3
2. トレースファイル保存先の変更.....	4
3. トレースファイルを保存先(共有)フォルダをマウント.....	6

文書改訂履歴

改訂年月日	版数	改訂内容	作成
2016/04/12	A	初版	仲村

# 1. はじめに

## 1.1. 概要

---

Synesis では、キャプチャしたパケットデータをトレースファイル(**pcap**)として抽出・保存することができます。そして、このトレースファイルの通常保存先として、データバンク(**Databank**)と呼ばれる領域が、パケットデータ保存(**packetdb**)領域とは別で用意されております。

また、トレースファイルは上記の通常保存先だけでなく、指定した場所へ保存することもできます。さらに、指定する場所にネットワーク上の共有フォルダをマウントしておくことで、ネットワーク上の共有フォルダへ直接トレースファイルを保存することもできます。

本書は、上述のトレースファイルの保存先変更方法について記載しております。

## 2. トレースファイル保存先の変更

1. トレースファイル(pcap)として保存したい期間の記録を選択(チェック)し、「トレースの保存」をクリックします。



2. 「トレースの保存」画面が表示されるので、「詳細設定」にチェックを入れ、「対象ファイルフォルダ」にて「カスタムフォルダ」を選択します。



3. 「対象ファイルフォルダ」に指定したい保存先を記入し、「トレースの保存」をクリックします。



4. トレースファイルが指定の保存先へ保存されます。「ステータス」が「完了」と表示されれば、トレースファイルの保存は完了しています。実際に保存された保存先とファイル名は「ファイルパス」を確認してください。

<input type="checkbox"/>	ステータス	トレースファイルの説明	期間	フィルタ	ファイルパス
<input checked="" type="checkbox"/>	完了		2016/04/13 20:08:17.600 - 2016/0/	なし	/home/toyo/test/mount/1460547694661-3682.pcap

5. トレースファイル保存先の変更はこれで完了です。ネットワーク上の共有フォルダにトレースファイルを直接保存するには、次章の手順を実施します。

### 3. トレースファイルを保存先(共有)フォルダをマウント

1. SSH で Synesis に接続します。

デフォルトのユーザー名、パスワードは下記の通りです。

User : toyo Password : admin

2. “cd” や “mkdir” などのコマンドを使用して、(共有)フォルダをマウントしたいディレクトリを作成・確認します。

3. 下記のコマンドを入力して、fstab ファイルを vi で開きます。パスワードの入力を求められますので、“admin” と入力します

```
$ sudo vi /etc/fstab
```

4. “i”キーを押して「INSERT」モードにしてから、以下の記述を追記してください。

※□は半角スペースを表します



```
//[マウントされる側の IP]/[マウントされるディレクトリ]□[マウントするディレクトリ]□cifs□user=[マ  
ウントされる側のユーザー名], password=[マウントされる側のパスワード]□0□0
```

例 : //172.22.142.10/Public□/home/toyo/test/mount□cifs user=toyo, password=admin□0□0

5. “Esc”キーを押して「INSERT」モードから抜けて、“:wq”を入力し“Enter”キーを押して保存します。

6. 下記コマンドを入力して、Synesis を再起動します。

```
$ sudo shutdown -r now
```

7. 再起動後、再度 SSH で Synesis に接続し(手順 1 参照)、下記コマンドを入力します。

```
$ mount
```

8. 手順 4 の記述が表示されていれば、マウントは正常に完了しています。

9. 2章の手順に従い、(共有)フォルダをマウントしたディレクトリをトレースファイルの保存先に指定することで、ネットワーク上の(共有)フォルダにトレースファイルを直接保存できます。

以上