

NTPサーバ設定事例



もっともらしい Stratum2サイトを目指して

新潟インターネット研究会 井上幹生

設定に関わるファイル

- **/etc/ntp.conf**
 - 参照するサーバ、参照するモード
 - 認証・アクセス制限、関連ファイル名等々
- **/etc/ntp.drift**
 - 内部時計と実時間の偏差を記録
 - 自動的に生成される。
- **/etc/ntp.keys**
 - 認証用のキーファイル

安易な設定

- **/etc/ntp.confに2行だけ**
 - 上位のサーバをひとつ指定するだけ
 - driftfileの行は無くても動く
 - これで立派な stratum 2サーバ!!

```
server clock.tl.fukuoka-u.ac.jp
driftfile /etc/ntp.drift
```

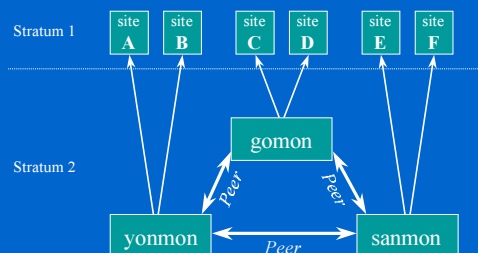
何がまずいか

- **ホストの内部時計はいいかげん**
 - 毎日数秒から数十秒はずれる
 - driftファイルだけでは不安?
- **上位のサーバとの接続状況の影響**
 - 接続できない場合や遅い場合
 - 参照する時間が当てにできない状況
- **サイトの時間基準としては不十分?**
 - 多くのホストの基準時間

もっともらしい目標

- **自サイトでは3台のホストでピアリングする。**
 - サイト内での基準時間の自律性を向上させる
- **各ホストは2台の上位サーバに接続する。**
 - 上位との接続性の向上
- **ログを残す。**
- **他サイトからの接続を制限をする。**

こんなことをやりたい



実験に使用したサーバ

記号	実際のサーバ	参照ホスト
A	eagle.center.osakafu-u.ac.jp (157.16.213.52)	yonmon
B	ntp.sut.ac.jp (133.31.180.6)	
C	clock.tl.fukuoka-u.ac.jp (133.100.11.8)	gomon
D	ntp.tut.ac.jp (133.15.64.8)	
E	cesium.mtk.nao.ac.jp (133.40.40.133)	sanmon
F	clock.nc.fukuoka-u.ac.jp (133.100.9.2)	

sanmonの設定

・参照するサーバの指定

—preferオプションで優先的に同期するホストを指定

・ピアリングするサーバの指定

```
# Stratum 1 servers
server 133.40.40.133 prefer # cesium.mtk.nao.ac.jp
server 133.100.9.2         # clock.nc.fukuoka-u.ac.jp
#
# Peer servers
peer 210.154.137.98        # yonmon.nisoc.or.jp
peer 210.154.137.99        # gomon.nisoc.or.jp
#
# Files
driftdir /etc/ntp.drift
```

yonmonの設定

・sanmonと同じ

```
# Stratum 1 servers
server 157.16.213.52      # eagle.center.osakafu-u.ac.jp
server 133.31.180.6 prefer # ntp.sut.ac.jp
#
# Peer servers
peer 210.154.137.99      # gomon.nisoc.or.jp
peer 210.154.137.97      # sanmon.nisoc.or.jp
#
# Files
driftdir /etc/ntp.drift
```

gomonの設定 (1)

・基本はsanmon、yonmonと同じ

```
# Stratum 1 servers
server 133.100.11.8      # clock.tl.fukuoka-u.ac.jp
server 133.15.64.8 prefer # ntp.tut.ac.jp
#
# Peer servers
peer 210.154.137.97      # sanmon.nisoc.or.jp
peer 210.154.137.98      # yonmon.nisoc.or.jp
```

gomonの設定 (2)

・アクセス制御を追加する

—デフォルトで全てのホストとの接続を無視

—接続する必要があるホストを許可する

•localhostを許可しないと大変

•参照するホストも忘れずに

```
#
# Access Control Options
restrict default ignore # ignore most of host
restrict 127.0.0.1       # free access from localhost
restrict 210.154.137.97  # sanmon.nisoc.or.jp
restrict 210.154.137.98  # yonmon.nisoc.or.jp
restrict 210.154.137.99  # gomon.nisoc.or.jp
restrict 133.100.11.8    # free from clock.tl.fukuoka-u.ac.jp
restrict 133.15.64.8     # free from ntp.tut.ac.jp
```

gomonの設定 (4)

・せっかくだからログもとみましょう

```
#
# Monitoring Options
statsdir /var/log/ntp/ # directory for statistics files
filegen peerstats file peerstats type day enable
filegen loopstats file loopstats type day enable
filegen clockstats file clockstats type day enable
#
# Files
driftdir /etc/ntp.drift
```

動いているか調べてみよう

- ntpqコマンドでサーバに問い合わせる

```
% ntpq -p yammon.nisoc.or.jp
remote      refid      st t when poll reach  delay  offset  disp
-----
cesium.nsk.nao.  2 u 195a 1024  0    85.33  -8.818 16000.0
+clock.nc.fukuok 1 u 193 256 377 121.40  -53.084 558.07
+yammon      subntp.sub.ac.jp 2 u 17 64 353  -36.60  72.022  28.76
+gomon      higu.tut.ac.jp 2 u 108 256 337  -36.45  -46.789  12.83

% ntpq -p yammon.nisoc.or.jp
remote      refid      st t when poll reach  delay  offset  disp
-----
+esjiccenter.es 1 u 62 64 372 2325.28  -1168.6  957.87
+subntp.sub.ac.jp 1 u 16 64 125 6264.80  -3198.7  774.41
+yammon      clock.nc.fukuok 2 u 33 64 377  3.10  -163.68  23.54
+gomon      higu.tut.ac.jp 2 u 15 64 377  3.33  -147.68  6.94
```

その他

- ntpdateコマンドを忘れずに
 - 特に初めてxntpdを動かすときは、直前に実行しましょう
- なかなか動かない
 - xntpdは、起動してもすぐに同期をとりません
 - 30分から1時間は、他の事をしながら待ちましょう
- ピアリングは結構重い

まとめ

- 動かすだけなら簡単
 - ピアリングは簡単
 - 複数の上流の参照も簡単
- まじめにやるとそれなりに苦労
 - アクセス制限はめんどくさい
 - 安心して使える上流は少ない
- やっぱりサイト単位に stratum 1 !