これから始める
IPv6対応監視システム

JANOG（日本ネットワーク・
オペレーターズ・グループ）

大久保 修一、高橋 真

Japan Network Operators' Group

プロバイダ(ISP)や通信事業者のコミュニティ

ML、年2回のイベント(無料)

次回JANOG28は日本橋(2011年7月14日～15日)

JANOG27@金沢
2011年1月

自己紹介

- 大久保 修一
- さくらインターネット（株）研究所　所属
  - http://research.sakura.ad.jp/
- 数年後のビジネスのネタになりそうな技術の目利きなど。
- キーワード：クラウドコンピューティング、IPv4アドレス枯渇対策、その他
- 2010/6までは、弊社ネットワークの運用を担当していました。
- Twitter: @jq6xze_1

自己紹介

髙橋　真（たかはし　まこと）

出身：　秋田県の雪が3mぐらい積ってるところ
　　祖父はマタギ（熊撃ち）
所属：　某キャリア/ISP
本職：　自社ネットワークオペレーションの
　　自動化、システム化
好きなもの：最広義でのインターネット
　　アルコール一般

Twitter: makotaka

Agenda

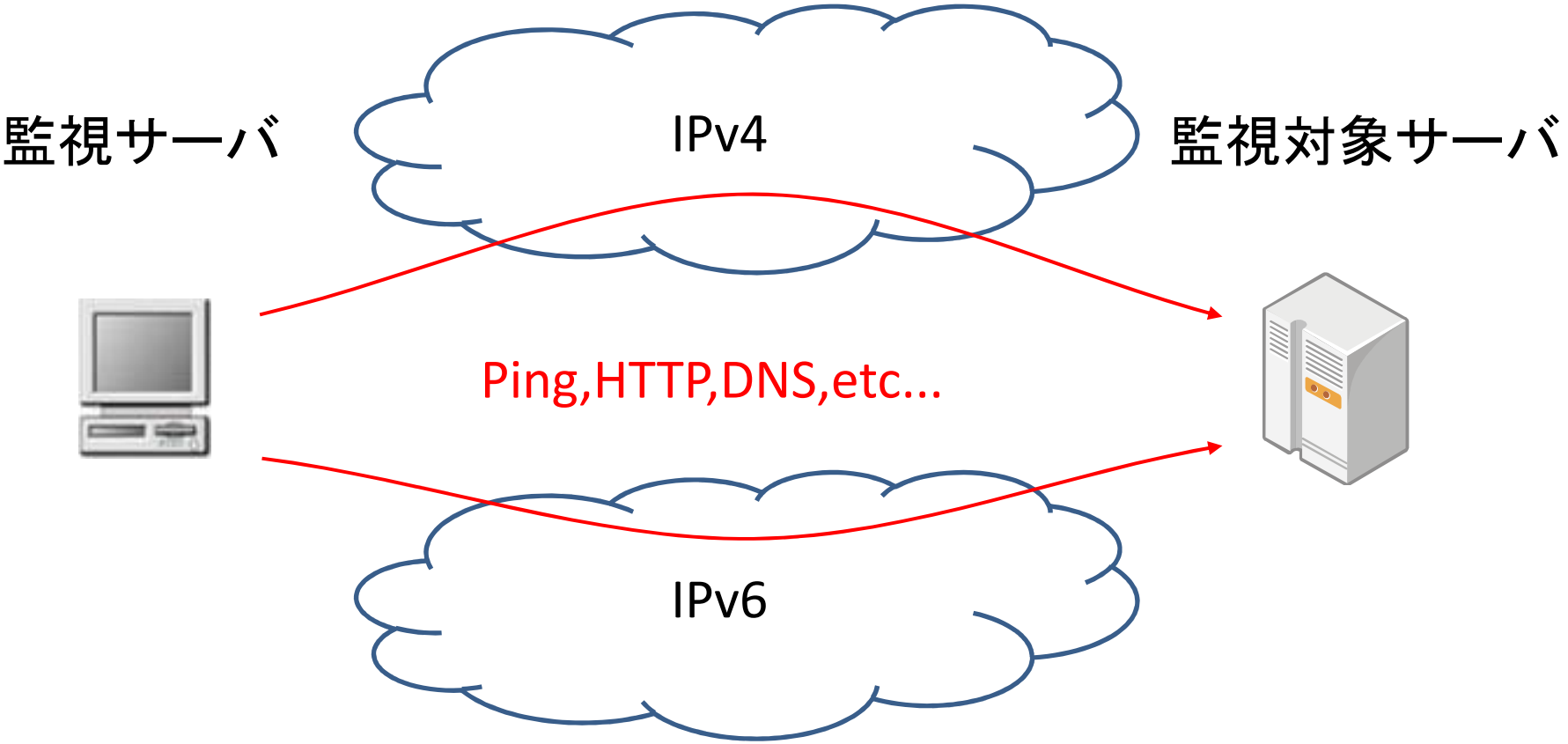
- 監視のIPv6対応について
  - IPv6に対応した監視ソフト
  - 監視サーバのDualStack化
  - SNMPのIPv6監視
  - IPv6アドレスの種別
  - IPv6アドレスの表記
- NagiosとZabbixの用途の違い
- NagiosによるIPv6監視について
- ZabbixによるIPv6監視について
- おわりに
- 質疑応答

IPv6に対応した監視ソフト

監視ソフト名	URL等	種別
Nagios	http://www.nagios.org/	統合監視
Zabbix	http://www.zabbix.com/jp/	
Pandora FMS	http://pandorafms.org/	
Cacti	http://www.cacti.net/	リソースモニタ
MRTG	http://oss.oetiker.ch/mrtg/	
SmokePing	http://oss.oetiker.ch/smokeping/	品質監視
Net-SNMP	http://www.net-snmp.org/	ツール
fping	http://fping.sourceforge.net/	

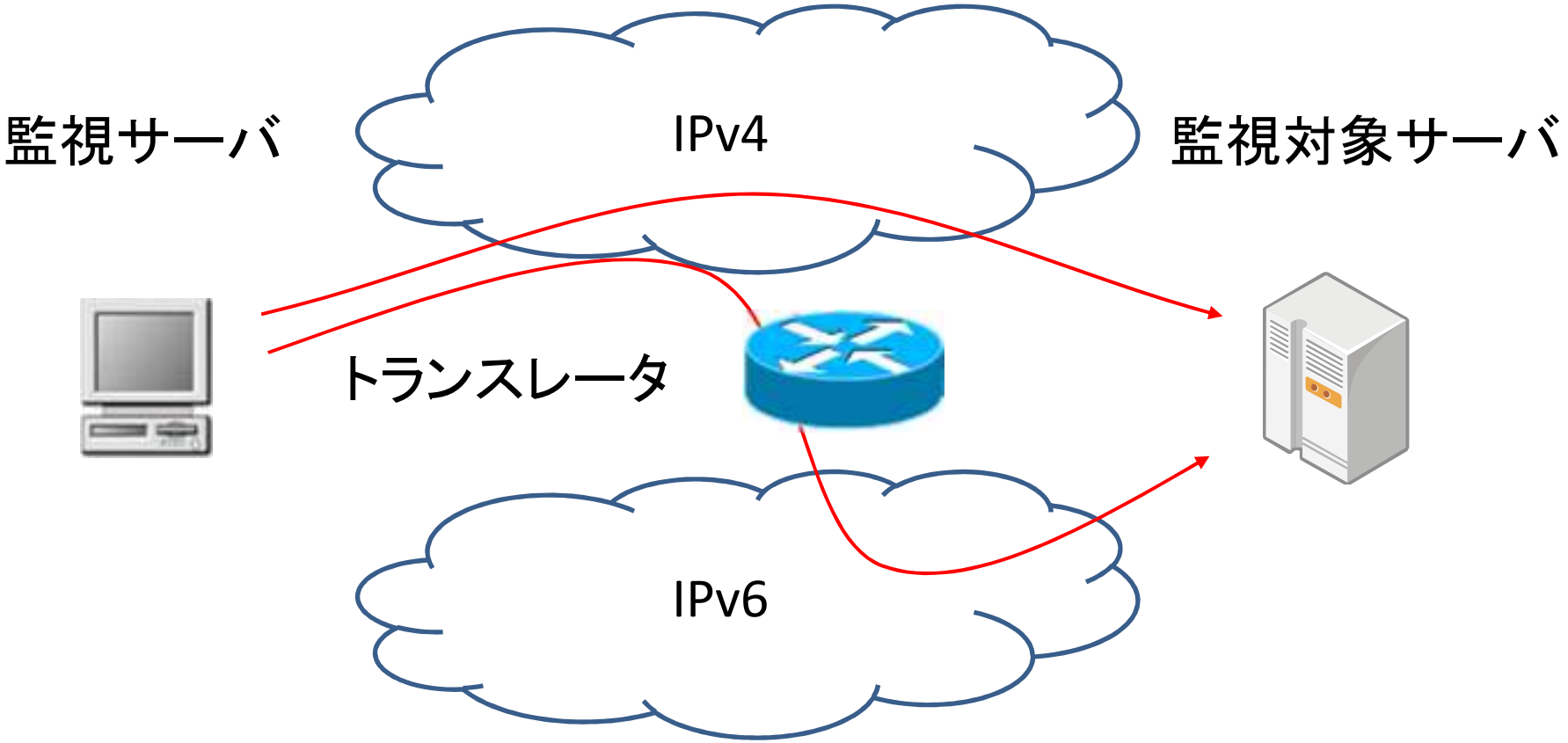
Dual Stackホストの監視

必ず両方のプロトコルで監視しましょう！



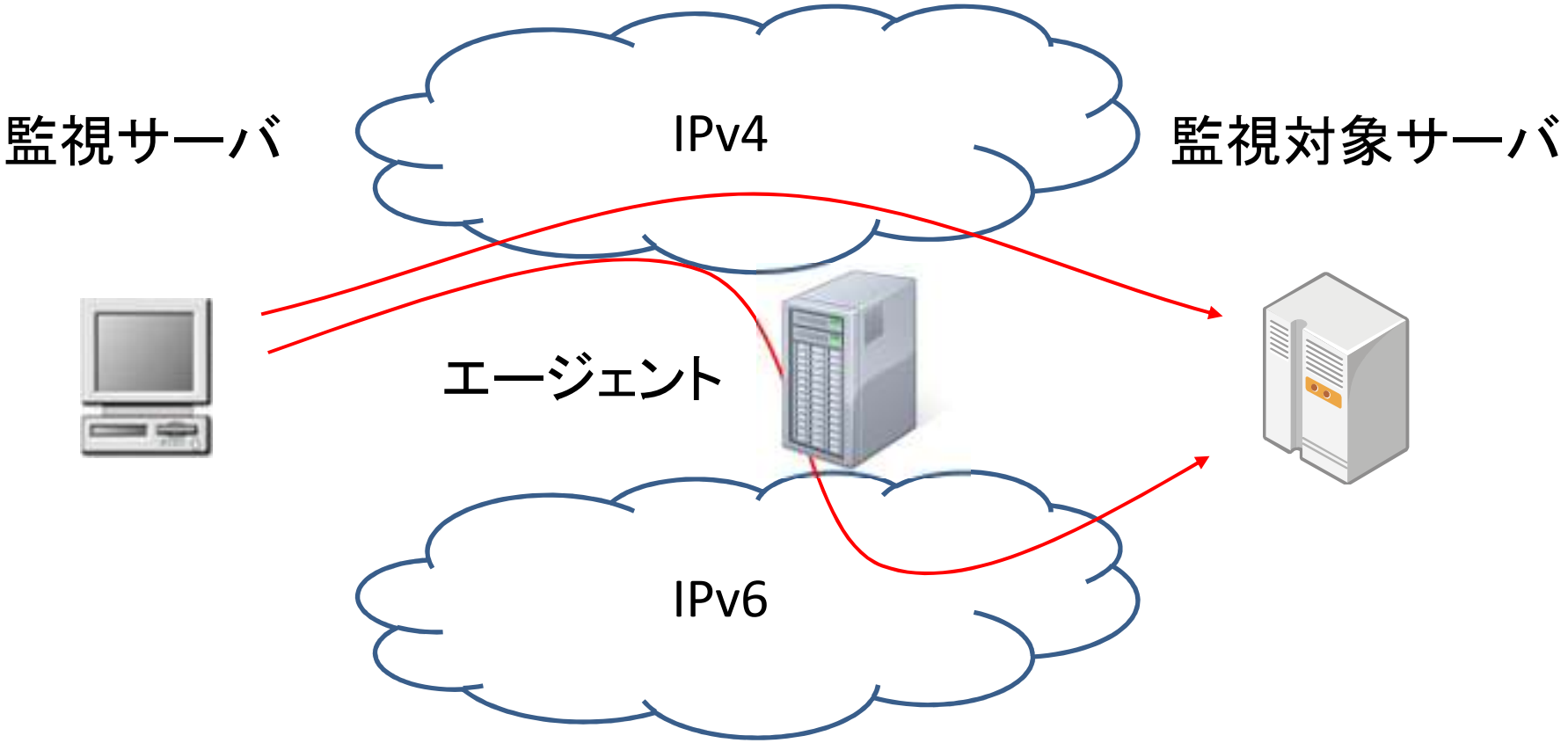
監視サーバがIPv6に対応していない場合

プロトコルトランスレータを使った方法もあります



監視サーバをIPv6に接続できない場合

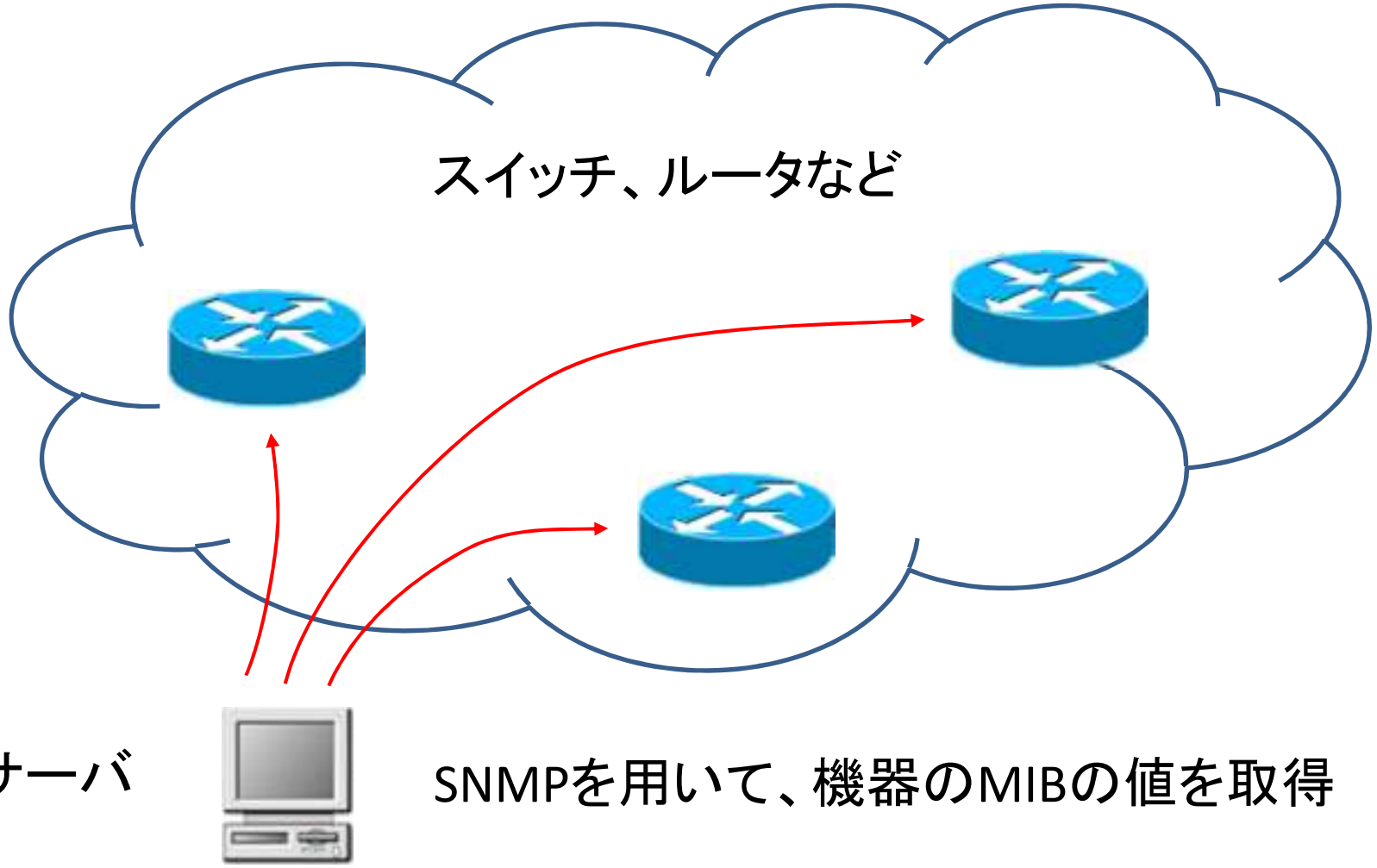
エージェント経由で監視する方法もあります



SNMPによる監視

- 主にネットワーク機器の
  - CPU負荷
  - Memory使用率
  - インターフェイス状態
  - インターフェイスエラー
  - トラフィック流量
  - 経路数
- などをリモートから監視するために使用されます。

SNMPによる監視



SNMPのIPv6について

- ネットワーク機器の中には、SNMPエージェントがIPv6に対応していないものもある。
- SNMPはIPv6トランスポートでなく、IPv4で監視しても問題ない。

IPv6を使ってSNMP監視する場合

- NetSNMPはIPv6に対応している

```
# snmpget -v2c -c himitsu udp6:2001:db8:100:200::1 ¥
  SNMPv2-MIB::sysName.0
SNMPv2-MIB::sysName.0 = STRING: router.example.jp
```

- アクセス制御を忘れずに！
- IPv4では制限がかかっているものの、IPv6では制限がかかっていない、ということも。

IPv6を使ってSNMP監視する場合

- ×悪い例（IPv6では筒抜けになっている）

```
ip access-list standard remote-snmp
 permit 192.168.0.0 0.0.0.255

snmp-server community himitsu RO remote-snmp
```

Cisco IOSの例

- ○正しい例

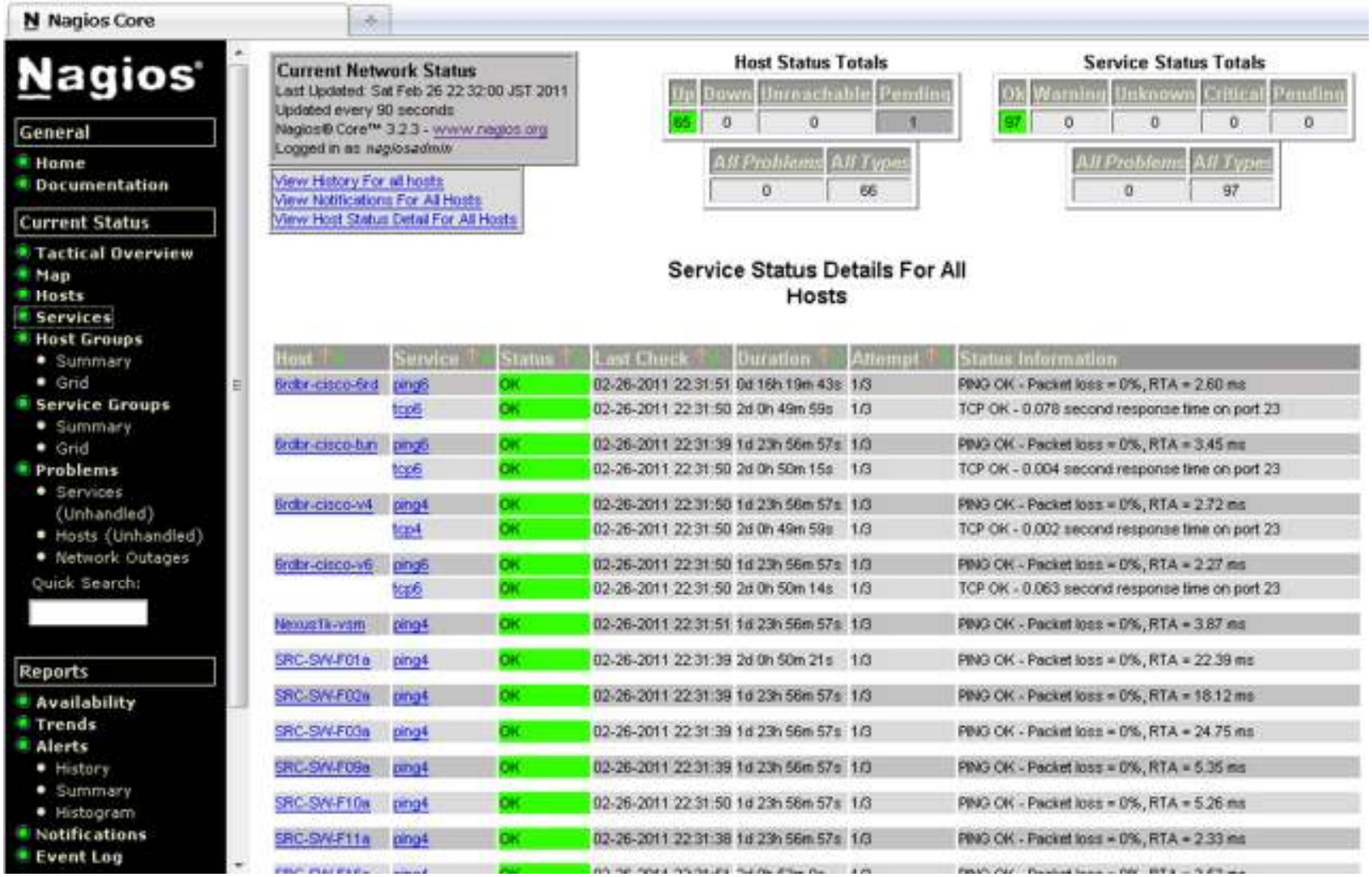
```
ip access-list standard remote-snmp-ipv4
 permit 192.168.0.0 0.0.0.255

ipv6 access-list remote-snmp-ipv6
 permit ipv6 2001:db8:100:200::/64 any

snmp-server community himitsu RO ipv6 remote-snmp-ipv6 remote-
snmp-ipv4
```

Cisco IOSの例

NagiosによるIPv6監視

- 無料で使えるオープンソースの監視ソフト
- Webサイト: http://www.nagios.org/
- 現在の最新バージョン: Nagios Core 3.2.3
- プラグイン（監視コマンド）も充実。ほとんどはIPv6に対応。簡単に自作することもできる。
- 監視設定はサーバ上のファイルに記述。
- 監視状況の確認はWebインターフェイス。

Nagiosスクリーンショット例



Nagiosのインストール手順

- OSのインストール（今回はCentOS5.5で説明）
- IPアドレス等初期設定
- sendmailの設定
- RPM Forgeインストール
- Nagiosインストール、初期設定
- 監視設定の追加

IPアドレスを設定

- /etc/sysconfig/network

```
HOSTNAME=centos55-2
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6_AUTOCONF=no
```

- /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
IPADDR=192.168.0.2
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
IPV6INIT=yes
IPV6ADDR=2001:db8:100:200::300
IPV6_DEFAULTGW=2001:db8:100:200::1
```

初期設定

- SELinuxとiptablesはとりあえずdisableにしておく。

```
% vi /etc/selinux/config
SELINUX=disabled

% chkconfig iptables off
% chkconfig ip6tables off
```

メール設定

- Nagiosは負荷（Load Avarage）が高くなるので、閾値を上げておく。

```
% yum install sendmail-cf
% cd /etc/mail/
% vi sendmail.mc
define(`confQUEUE_LA', `100')dnl
define(`confREFUSE_LA', `100')dnl

% make
% service sendmail restart
```

RPM Forgeインストール

- 標準のレポジトリには存在しない。
- RPM ForgeのレポジトリからNagiosをインストールする。
- 64bit版の場合

```
% cd /tmp
% wget http://packages.sw.be/rpmforge-
  release/rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm
% rpm -Uvh rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm
```

- 32bit版の場合

```
% cd /tmp
% wget http://packages.sw.be/rpmforge-
  release/rpmforge-release-0.5.2-2.el5.rf.i386.rpm
% rpm -Uvh rpmforge-release-0.5.2-2.el5.rf.i386.rpm
```

Nagiosのインストール

- yumを使ってインストール。

```
% yum install nagios
% yum install nagios-plugins
```

- Apache等も一緒にインストールされる。
- Nagios Core 3.2.3がインストールされる。
  （2011年3月現在）

Nagiosの初期設定

- /etc/nagios/objects/contacts.cfg

```
define contact{
        contact_name  nagiosadmin             ; Short name of user
        email         jibun@example.jp        ; <<***** CHANGE
THIS TO YOUR EMAIL ADDRESS ******
        }
```

メールアドレスを記入

- Webインターフェイスパスワード設定

```
% htpasswd -c /etc/nagios/htpasswd.users nagiosadmin
```

デーモンの起動

- 自動起動の設定も行う。

```
% /etc/init.d/httpd start
% /etc/init.d/nagios start

% chkconfig httpd on
% chkconfig nagios on
```

- Webアクセスの確認
  - http://192.168.0.2/nagios/
- デフォルトでサーバ自身の監視が行われる。

ローカルホストの監視解除

- /etc/nagios/nagios.cfg

```
#cfg_file=/etc/nagios/objects/localhost.cfg
cfg_file=/etc/nagios/objects/servers.cfg
```

新規に作成する設定ファイル名を指定

IPv4 PING監視

- /etc/nagios/objects/servers.cfg に追加

```
define host {
        use                     generic-host
        host_name               rs02
        address                 192.168.100.100
        check_command           check-host-alive
        max_check_attempts      3
        check_interval          0
        retry_interval          1
        contact_groups          admins
}

define service {
        use                     generic-service
        service_description     ping
        host_name               rs02
        check_command           check_ping!100,40%!300,100%
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}
```

IPv6 PING監視

- /etc/nagios/objects/servers.cfg に追加

```
define host {
        use                     generic-host
        host_name               rs02-v6
        address                 2001:db8:100:200::500
        check_command           check-host-alive
        max_check_attempts      3
        check_interval          0
        retry_interval          1
        contact_groups          admins
}

define service {
        use                     generic-service
        service_description     ping
        host_name               rs02-v6
        check_command           check_ping!100,40%!300,100%
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}
```

HTTPの監視

- /etc/nagios/objects/servers.cfg に追加

```
define service {
        use                     generic-service
        service_description     http
        host_name               rs02
        check_command           check_http!-H www.example.jp
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}

define service {
        use                     generic-service
        service_description     http
        host_name               rs02-v6
        check_command           check_http!-H www.example.jp
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}
```

DNSの監視

- /etc/nagios/objects/commands.cfg に追加

```
define command{
        command_name    check_dig
        command_line    $USER1$/check_dig -l $ARG1$ -H $HOSTADDRESS$
}
```

DNSの監視

- /etc/nagios/objects/servers.cfg に追加

```
define service {
        use                     generic-service
        service_description     dns
        host_name               rs02
        check_command           check_dig!www.example.jp
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}

define service {
        use                     generic-service
        service_description     dns
        host_name               rs02-v6
        check_command           check_dig!www.example.jp
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}
```

TCPポート監視設定

- /etc/nagios/objects/servers.cfg に追加

```
define service {
        use                     generic-service
        service_description     tcp25
        host_name               rs02
        check_command           check_tcp!25
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}

define service {
        use                     generic-service
        service_description     tcp25
        host_name               rs02-v6
        check_command           check_tcp!25
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}
```

SMTP監視

- /etc/nagios/objects/servers.cfg に追加

```
define service {
        use                     generic-service
        service_description     smtp
        host_name               rs02
        check_command           check_smtp
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}

define service {
        use                     generic-service
        service_description     smtp
        host_name               rs02-v6
        check_command           check_smtp
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}
```

SNMP監視

- SNMPクライアントをインストール

```
% yum install net-snmp
% yum install net-snmp-utils
```

- ルータやスイッチにアクセスできることを確認

```
% snmpwalk -v2c -c himitsu 192.168.100.100
% snmpwalk -v2c -c himitsu udp6:2001:db8:100:200::600
```

SNMP監視

- /etc/nagios/objects/servers.cfg に追加

```
define service {
        use                     generic-service
        service_description     ifoper1
        host_name               cisco
        check_command           check_snmp!-C himitsu -o IF-MIB::ifOperStatus.1 -c 1:1
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}

define service {
        use                     generic-service
        service_description     ifoper2
        host_name               cisco-v6
        check_command           check_snmp!-H udp6:2001:db8:100:200::600 -C himitsu -o
IF-MIB::ifOperStatus.2 -c 1:1
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}
```

IPv4でSNMPアクセスできるのであれば、IPv4で取得するのが無難。

IPv6で監視する場合、IPv6アドレスがそのまま渡されてエラーになるので、-H オプションでudp6:を指定する。

設定のリロード

- 設定を変更したら、リロードする。

```
# service nagios reload
nagios (pid 15933 15930 15927 15924 15918 15913 15906 15903 15900 15897 15894 15890
15886 15883 15880 15876 15872 3138) を実行中...
nagios を再読み込み中:                                          [  OK  ]
```

設定のこつ

- SNMPはIPv4で取得するのが無難。
- ホスト指定は、IPアドレスを直接書くのが無難。
- もし、IPv4アドレス（Aレコード）とIPv6アドレス（AAAAレコード）両方を登録したDNS名をホスト指定する場合、結構大変。
  - 標準のチェックコマンドの設定では、どちらのプロトコルでモニタするか指定できない。
  - IPv4用とIPv6用でチェックコマンドを別に作成するのがよい。
  - 明示的にプロトコルを指定して監視する。

チェックコマンドを明示的に分ける

- /etc/nagios/objects/commands.cfg に追加

```
define command{
        command_name    check_ping4
        command_line    $USER1$/check_ping -4 -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -p 5
        }

define command{
        command_name    check_ping6
        command_line    $USER1$/check_ping -6 -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -p 5
        }
```

チェックコマンドを明示的に分ける

- /etc/nagios/objects/servers.cfg

```
define host {
        use                     generic-host
        host_name               rs02
        address                 rs02.src.sakura.ad.jp
        check_command           check-host-alive
        max_check_attempts      3
        check_interval          0
        retry_interval          1
        contact_groups          admins
}
```

チェックコマンドを明示的に分ける

- /etc/nagios/objects/servers.cfg

```
define service {
        use                     generic-service
        service_description     ping6
        host_name               rs02
        check_command           check_ping6!100,40%!300,100%
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}

define service {
        use                     generic-service
        service_description     ping4
        host_name               rs02
        check_command           check_ping4!100,40%!300,100%
        normal_check_interval   1
        retry_check_interval    1
        max_check_attempts      3
}
```

おまけ

- Nagiosの監視設定は膨大になる。
- CSV形式等のファイルから自動生成するのがおすすめ。
- 当方で使っているCSVファイルの例

```
#=============================================
[service network]
#=============================================

# service global network (61.211.***.**/27)
gateway1a       61.211.***.**                   ping4
gateway1b       61.211.***.**                   ping4
rs01-v4         61.211.***.**                   ping4 dig4|rs01.src.sakura.ad.jp
rs01-v6         2001:e40:***:***::**            ping6 dig6|rs01.src.sakura.ad.jp
rs02            rs02.src.sakura.ad.jp           ping4 ping6 http4|-H__research.s
akura.ad.jp http6|-H__research.sakura.ad.jp
rs03            rs03.src.sakura.ad.jp           ping4 ping6
doujin          61.211.***.**                   ping4 http4|-H__douj.in
vmware6         61.211.***.**                   ping4

# translator
www-v6:NC       2001:e40:***:***::****:****     http6|-H__www.sakura.ad.jp
```