

IPv6の設計と運用を 具体的に考える

ソフトバンクテレコム株式会社
工藤 真吾

三井情報株式会社
仲西 亮子

はじめに

- 👑 本セッションではIPv6環境を構築中/構築前/設計中の方々に向けたセッションです
- 👑 IPv6環境構築後に運用フェーズを
 - 👑 如何に美しく
 - 👑 未来永劫やる気を持って頑張れる為の具体的な設定例などをご紹介します。
- 👑 ご紹介する設定例は「唯一の正解」ではありません。考え方の一例です。

agenda

1. 美しいLink-local address の世界
2. Filtering technique
3. 無傷にIPv4環境でIPv6ノードを監視する方法

 質疑応答

Chapter-1

美しき

LINK-LOCAL ADDRESSの世界

IPv6アドレスの種類

👑 ユニキャストアドレス (1:1通信に利用)

👑 グローバルユニキャストアドレス

👑 **リンクローカルユニキャストアドレス**

👑 ユニークローカルユニキャストアドレス

今回はココだけ
スコープします

👑 マルチキャストアドレス (1:N通信に利用)

👑 Assignedマルチキャストアドレス

👑 グループを識別するアドレスで複数のノードを識別

👑 エニーキャストアドレス (1:1 or N通信に利用)

👑 サブネットルータエニーキャストアドレス

👑 予約済みサブネットエニーキャストアドレス

👑 複数のノードに指定可能な「機能」に対して設定されるアドレス

Link-local address は何のためにあるのか

👑 プラグアンドプレイ (Plug and Play)

👑 IPv6の特徴である **思想を実現化した賜物**

プラグアンドプレイとは…

つないだら (Plug)、(ユーザが何か特別なことをしなくても) 実行 (Play) できる、という意味で、PCに周辺機器や拡張カード等を接続した際にH/Wとファームウェア、ドライバ、OS、およびアプリケーション間が自動的に協調し、機器の組み込みと設定を自動的に行う仕組みのことである。(出展:wikipedia)

Link-local address が愛されない理由

- 👑 突然発生する(ように見える)
- 👑 グローバルユニキャストアドレスだけで運用させてくれない
 - 👑 Link-local address を disable できない
- 👑 経路表に Link-local address が出てきて運用が複雑になる

どんな時に出現するのか

Routing protocol の ネクストホップ

```
Router#show ipv6 route bgp
B   2001:db8::/32 [20/0]
    via FE80::216:C8FF:FE38:8AE4, GigabitEthernet1/0
```


```
Router#show ipv6 route ospf
OE2 2001:db8:1:1::/64 [110/20]
    via FE80::216:C8FF:FE38:8AE4, GigabitEthernet1/0/15
```

HSRP の Virtual IP address

```
Router#show standby g2/0/2
Virtual IP address is FE80::216:C8FF:FE38:8AE4
```

Link-local address を設定する

 自動設定

 手動設定

メリットとデメリット

自動設定

👑 メリット

- 👑 設定時に何も行わなくても機器が自動設定するので楽

👑 デメリット

- 👑 アドレスから瞬時に機器を特定するには修行が必要
- 👑 アドレスを意識せずネクストホップInterfaceで判断することが必要

⇒機器によって記載方法が変わるので見づらさがある

手動設定

👑 デメリット

- 👑 設定するアドレスを考えるのが面倒
- 👑 設定したアドレスを管理するのが面倒

⇒アドレスポリシー次第で解決

👑 メリット

- 👑 アドレス生成のルール次第では『IPv4のようにIPv6の経路表を読む事が可能』

個人的には全てのinterfaceを手動設定が良いと思う

Link-local address の生成例

👑 1台の機器で1つのアドレスを使う

👑 1台の機器に1つの Link-local address、全てのインターフェースに設定する

⇒全てのインターフェースが全て同じ Link-local address になる

⇒1台の機器は1つの Link-local address しか持たなくなる

👑 IPv4アドレスと Bind する

👑 192.168.1.129/30 ⇒ fe80::192:168:1:129

👑 192.168.1.130/30 ⇒ fe80::192:168:1:130

⇒IPv6アドレスのInterface-ID にIPv4アドレス埋め込む

👑 IPv6のグローバルユニキャストアドレスと bind させる

👑 機器や設置場所などを埋め込む

手動設定が良いワケ

👑 Dynamic routing protocol を動かしている機器の Link/virtual address

👑 Next hop が Link-local address で表示される
⇒ **従って、Link-local address は全てユニークにした方が良い**

👑 IPv4で運用していた脳ミソをIPv6運用に移行できる

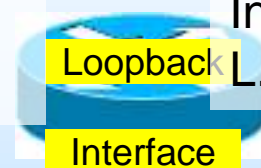
👑 運用移行時に結構重要？！

Link-local address を利用する (1)

👑 ポリシーの例 ~IPv4環境にIPv6を導入する場合~

LB **172.16.0.1**
LB 2001:db8:bb:1::**1/128**
Int1 **192.168.1.129/29**
Int1 2001:db8:**1:128::129/64**
L.L FE80::**192:168:1:129**

LB **172.16.0.2**
LB 2001:db8:bb:1::**2/128**
Int1 **192.168.1.130/29**
Int1 2001:db8:**1:128::130/64**
L.L FE80::**192:168:1:130**



iBGPで接続

OSPFで接続

2001:db8:1:1::/64

LB **172.16.0.3**
LB 2001:db8:bb:1::**3/128**
Int1 **192.168.1.131/29**
Int1 2001:db8:**1:128::131/64**
L.L FE80::**192:168:1:131**



■OSPFの場合

NextHop address
⇒Link-local address

■BGPの場合

Neighbor address
⇒グローバルユニキャストアドレス
とLink-local address
※コマンドによって違いがある

愛せるかしら？

- 👑 Link-local address はしっかり使おう
 - 👑 ルータが勝手に生成するのに任せず、自分が主導権を握る
- 👑 Link-local address はしっかり管理しよう
 - 👑 Link 外のアドレス同士は重複可能だが、トラブルシュートを考えると全てがユニークの方が便利かつ効率的
- 👑 IPv4アドレスが分かればIPv6アドレスが頭で生成できるのが理想的
- 👑 愛す為の努力の秘訣
 - 👑 **忌み嫌わずに積極的に利用する**
 - 👑 **グローバルユニキャストアドレスより優先して利用するくらいの気持ちで**

Chapter-3

無傷にIPV4環境でIPV6ノードを 監視する方法

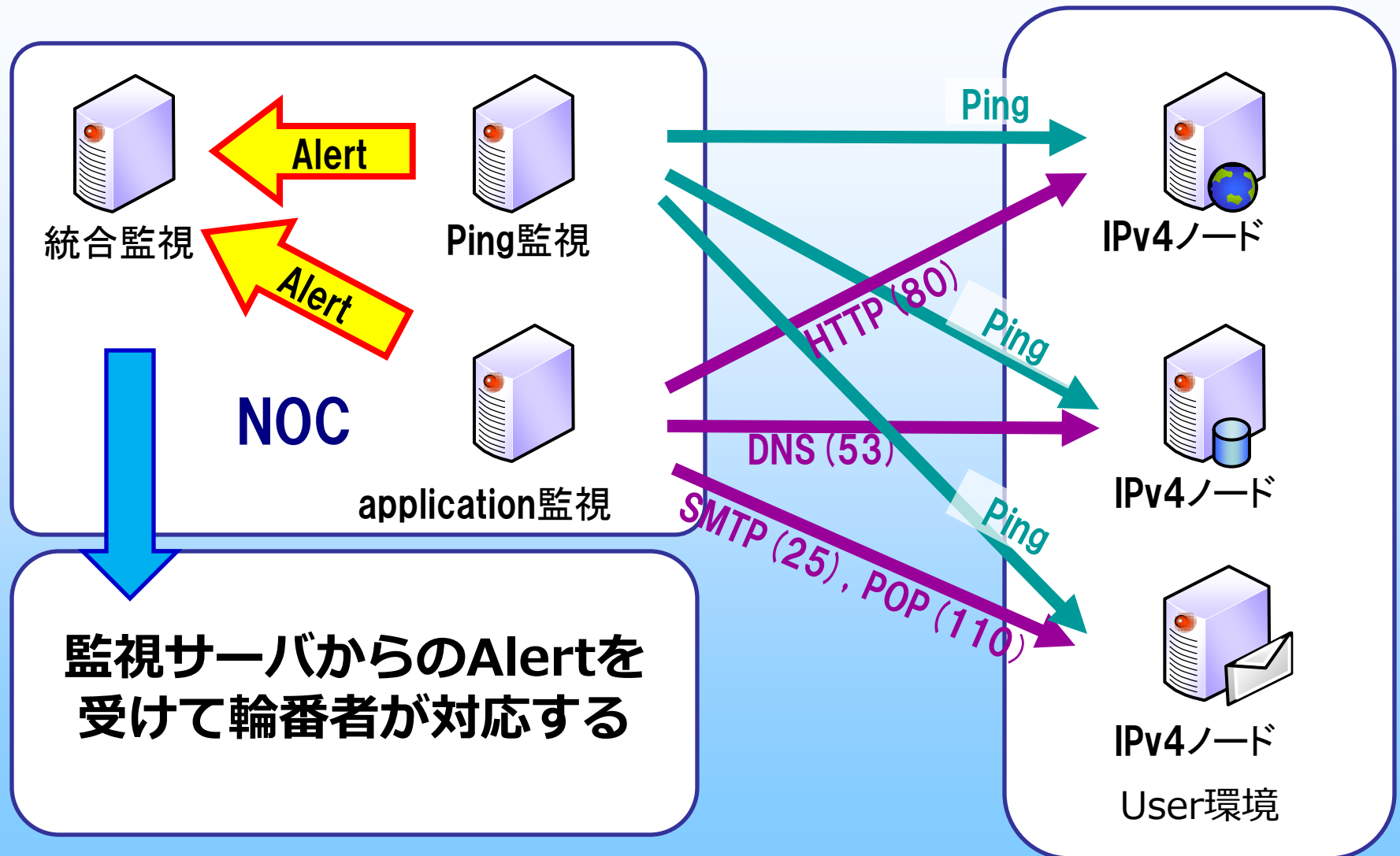
IPv6監視方法

- 👑 新たにIPv6対応のtoolを入れる
- 👑 今あるIPv4 only の監視 tool を利用する
 - 👑 IPv4 だけしか監視できないサーバから IPv6 を監視できる仕組みを作る
 - 👑 トランスレータを導入する
 - 👑 自作する

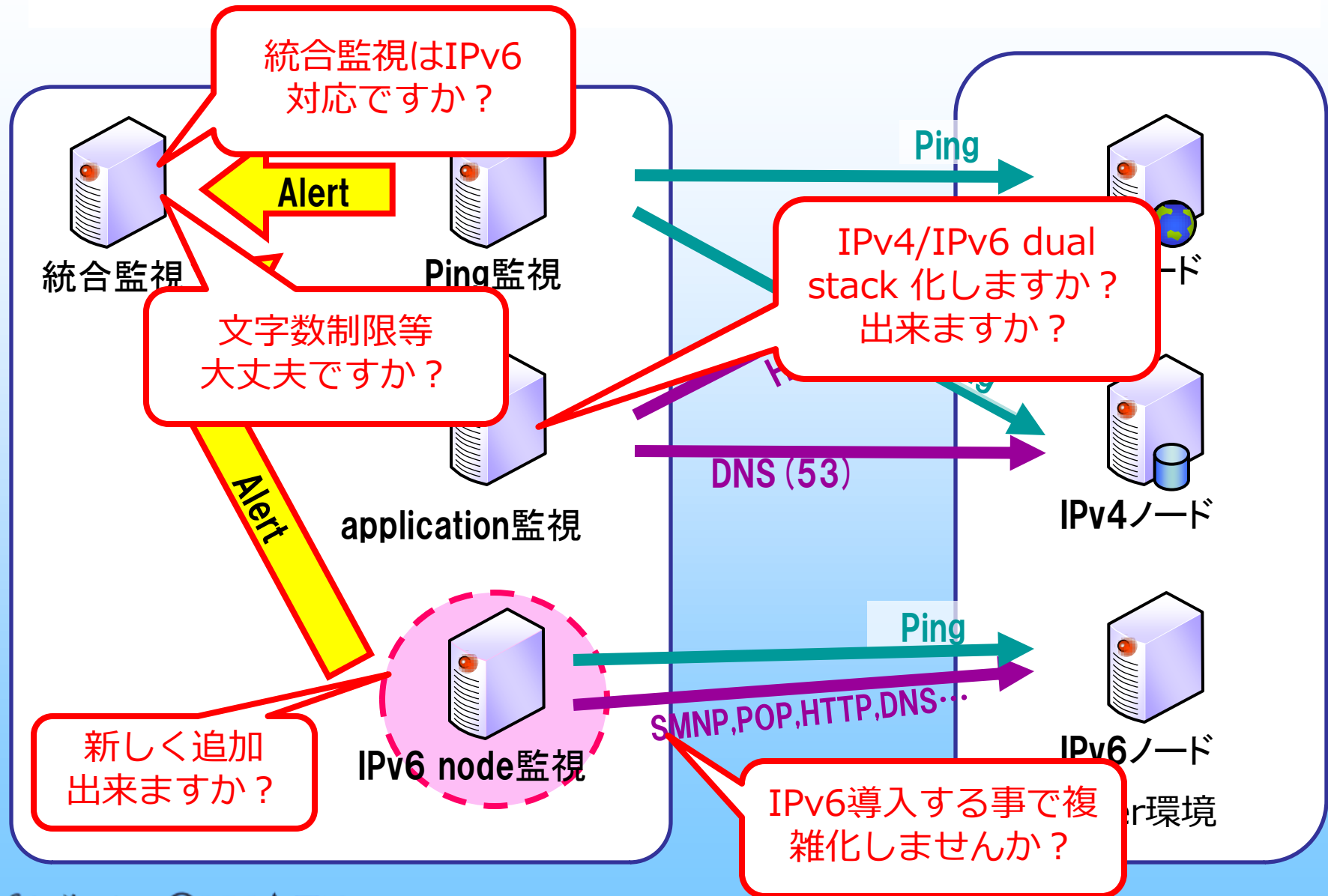
現在の問題点

- 👑 IPv6環境構築後にIPv6ノードを監視する為の tool が少ない
 - 👑 現状利用している監視 tool はIPv4 only だったり…
 - 👑 IPv6監視tool/機材を買おうとしても
 - 👑 予算が通らなかったり…
 - 👑 IPv4の運用がcriticalな為、NOC環境をいじりにくい
 - 👑 IPv6版を現状運用中のNOCに導入するには検証などの理由で時間&工数過多で敷居が高い
- ⇒でも、今すぐIPv6ノードを監視したい！**

おさらい：監視の方法（環境例/IPv4）

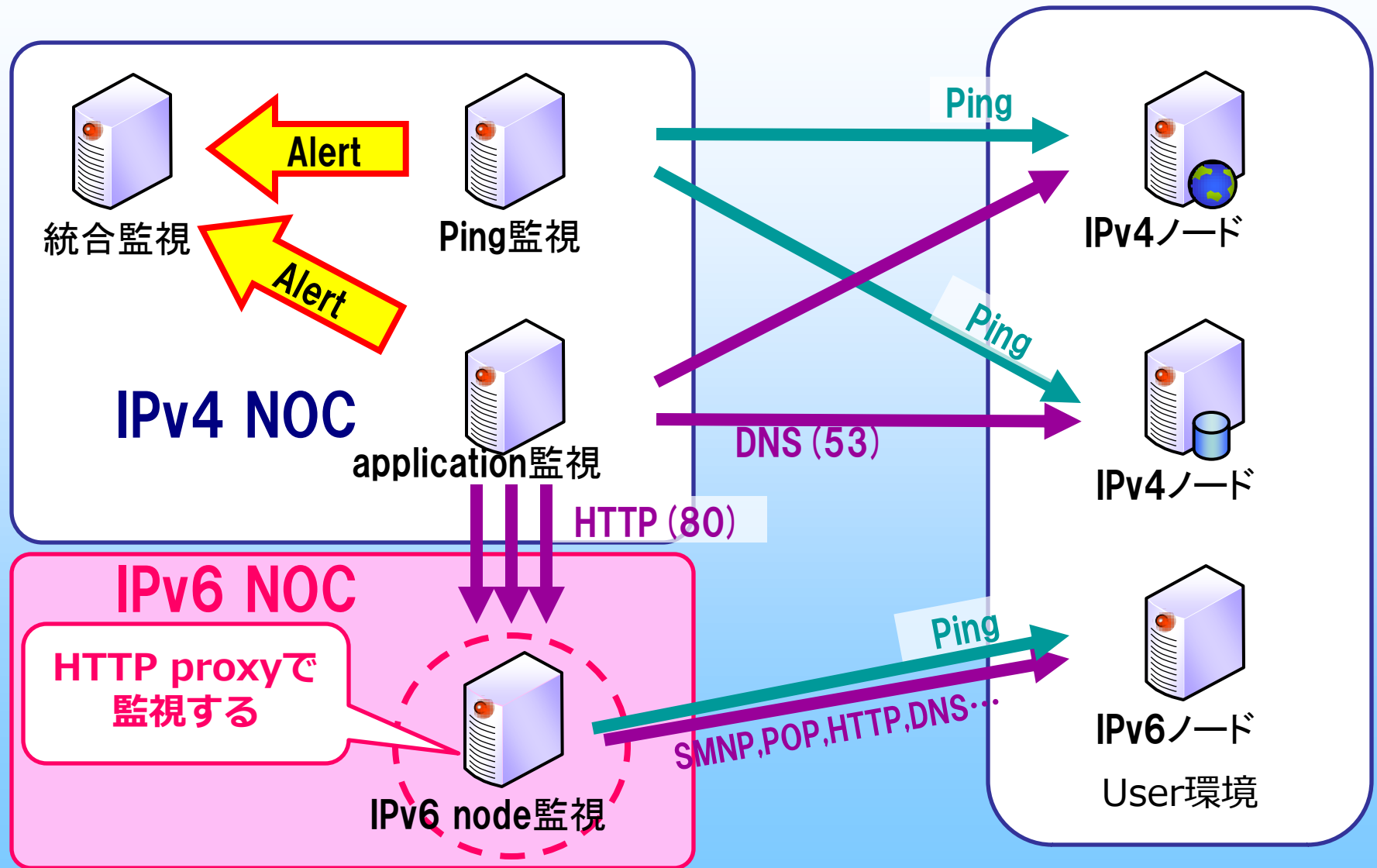


IPv6 node 監視導入の問題点

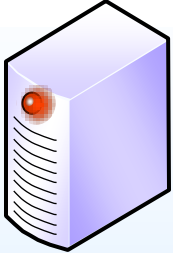


こんなことを
やってみました

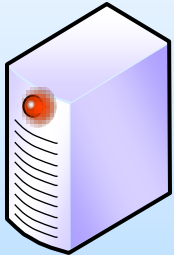
IPv4環境でIPv6nodeを無傷に監視する



概要

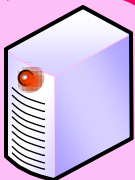


統合監視



application監視

HTTP (80)



IPv6 node監視

①監視サーバからIPv6ノード監視サーバに向けて**URL監視を実行 (IPv4)**

《URLイメージ》

`http://ipv6.poll.serv/protocol/[target:IPv6:Address]/options...`

②IPv6 node監視は指定のプロトコル・対象アドレスへポーリングし、**HTTP応答で結果を通知する。**
正常=200, 異常=5xx etc...

③監視サーバは**HTTP監視の結果**として統合監視へアラートを上げる。

流れ

⑤障害検知



統合監視



Alert

④URL監視エラー検知

application監視



①URL監視

IPv4 NOC

③HTTP status code=5xx

IPv6 NOC

②IPv6 プロトコル監視

IPv6 node監視



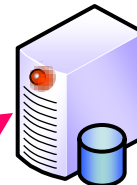
HTTP (80) IPv6

DNS (53) IPv6

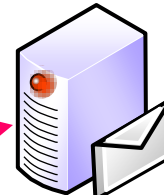
SMTP (25) IPv6



IPv6 web server



IPv6 DNS server



IPv6 mail server

IPv6 環境

結論

👑 暫定の仕組みと割り切って使う

- 👑 現在利用している監視 tool がIPv6対応するまで
- 👑 IPv6対応しているtoolを購入できる日まで
- 👑 IPv6環境は整ったが監視環境が整うまで
- 👑 IPv4環境を作業できるその日まで

👑 但し良いコトもある

- 👑 現在の環境に無影響
 - 👑 IPv4監視サーバからすると「URL監視対象」が増えただけ
- 👑 今すぐ、監視できます！