

Version 11/17

# DMM.com Labo

Internet Week 2016 D3 DNS DAY

## コンテンツプロバイダから見た 権威DNSサーバ

2016年12月1日

株式会社DMM.comラボ

高嶋隆一

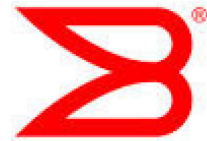
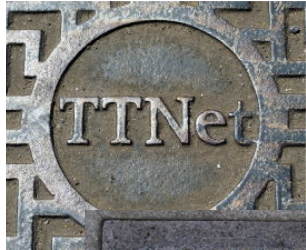
# 本セッションの目的

権威DNSサーバの運用における

- ✓ 想定されるユースケース
- ✓ ユースケース毎に用いられる実装
- ✓ ユースケース毎の注意点

を、コンテンツプロバイダの視点から説明し、議論する事!

# 自己紹介



BROCADE



midokura

イマココ →

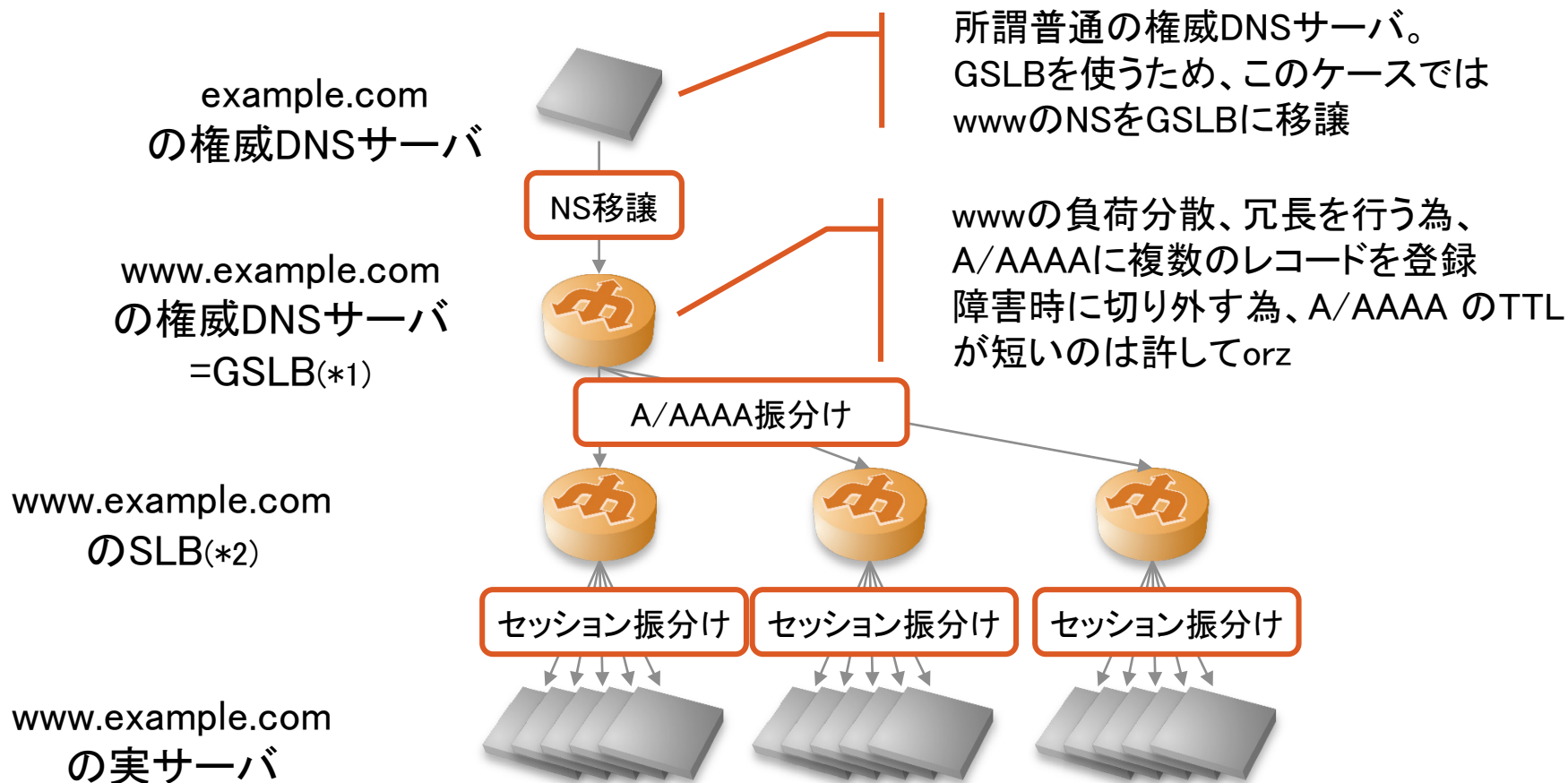
**DMM.com** Labo

2

# サービス提供用ドメイン名 の利用のされ方から考えてみる



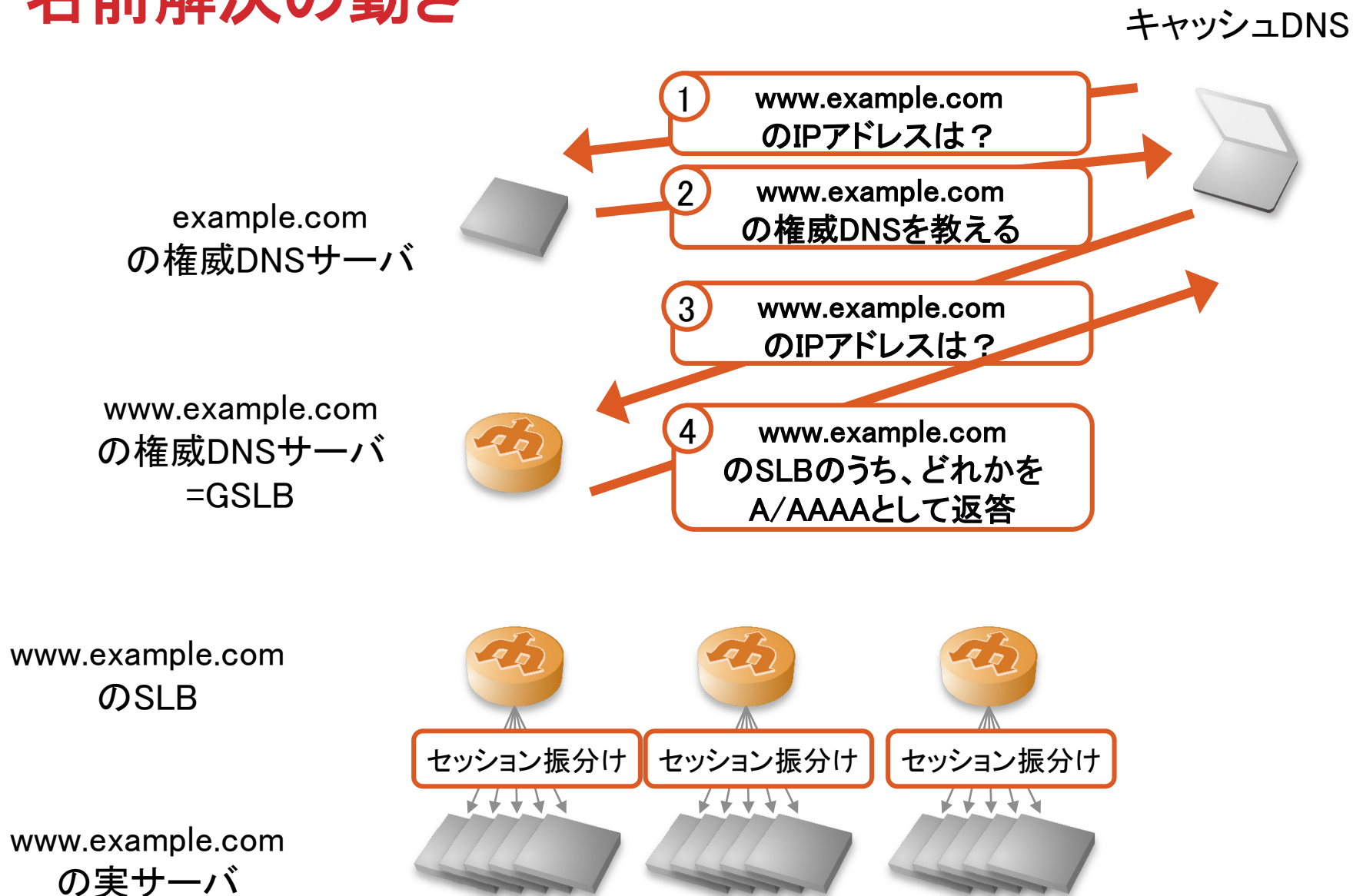
# よくあるwebサービスのアーキテクチャ



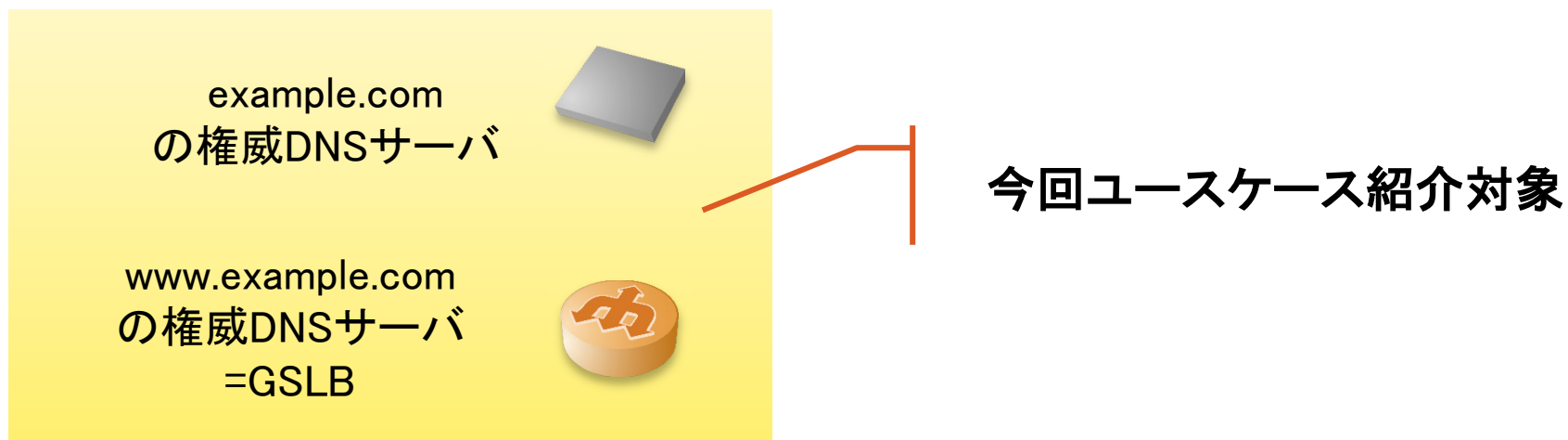
(\*1)GSLB=Global Server Load Balancing: クライアントによって返すA/AAAAの内容を変える事により、複数の実サーバを持たせる負荷分散、冗長化の仕組み

(\*2)SLB=Server Load Balancing: UDP/TCP等のセッションを複数の実サーバに振分ける負荷分散、冗長化の仕組み

# 名前解決の動き

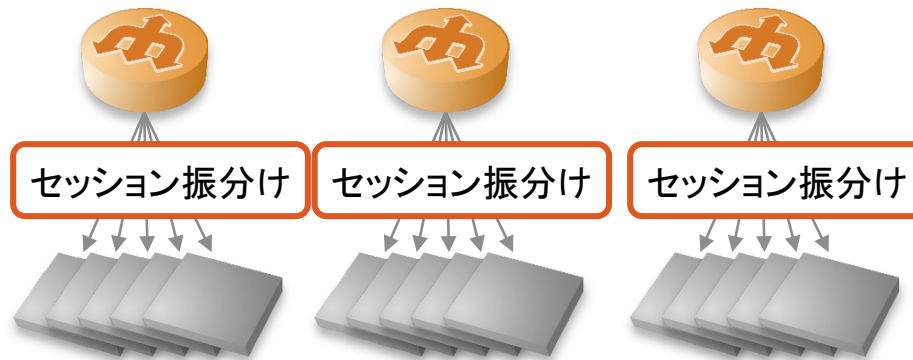


# よくあるwebサービスのアーキテクチャ



www.example.com  
のSLB

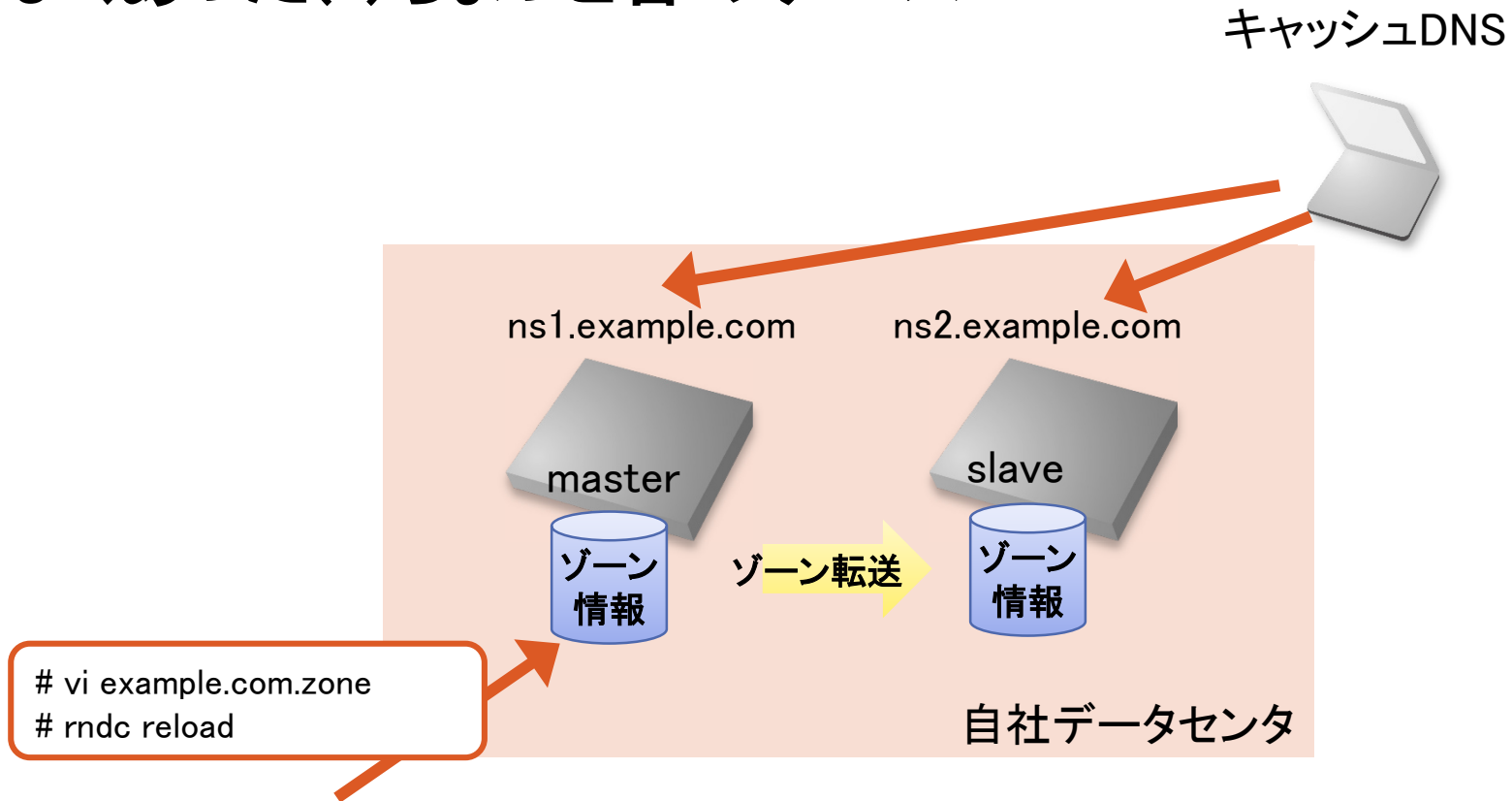
www.example.com  
の実サーバ



# ユースケースその1: example.com の権威DNSサーバ

# example.comの権威DNSサーバ

## よくあった(?)ちょっと昔のケース



admin



# example.comの権威DNSサーバ

SLB等の冗長化を未使用の  
為、1台のNSのメンテ、障害  
がクライアント待ち時間増加  
に繋がる

キャッシュDNS



オリジナルデータを持つ  
サーバが直接クエリにも答  
える為メンテしづらい

ns1.example.com

ns2.example.com

master

slave

ゾーン  
情報

ゾーン転送

ゾーン  
情報

オンプレだと  
DoS/DDoSが怖  
い

```
# vi example.com.zone  
# rndc reload
```

自社データセンタ

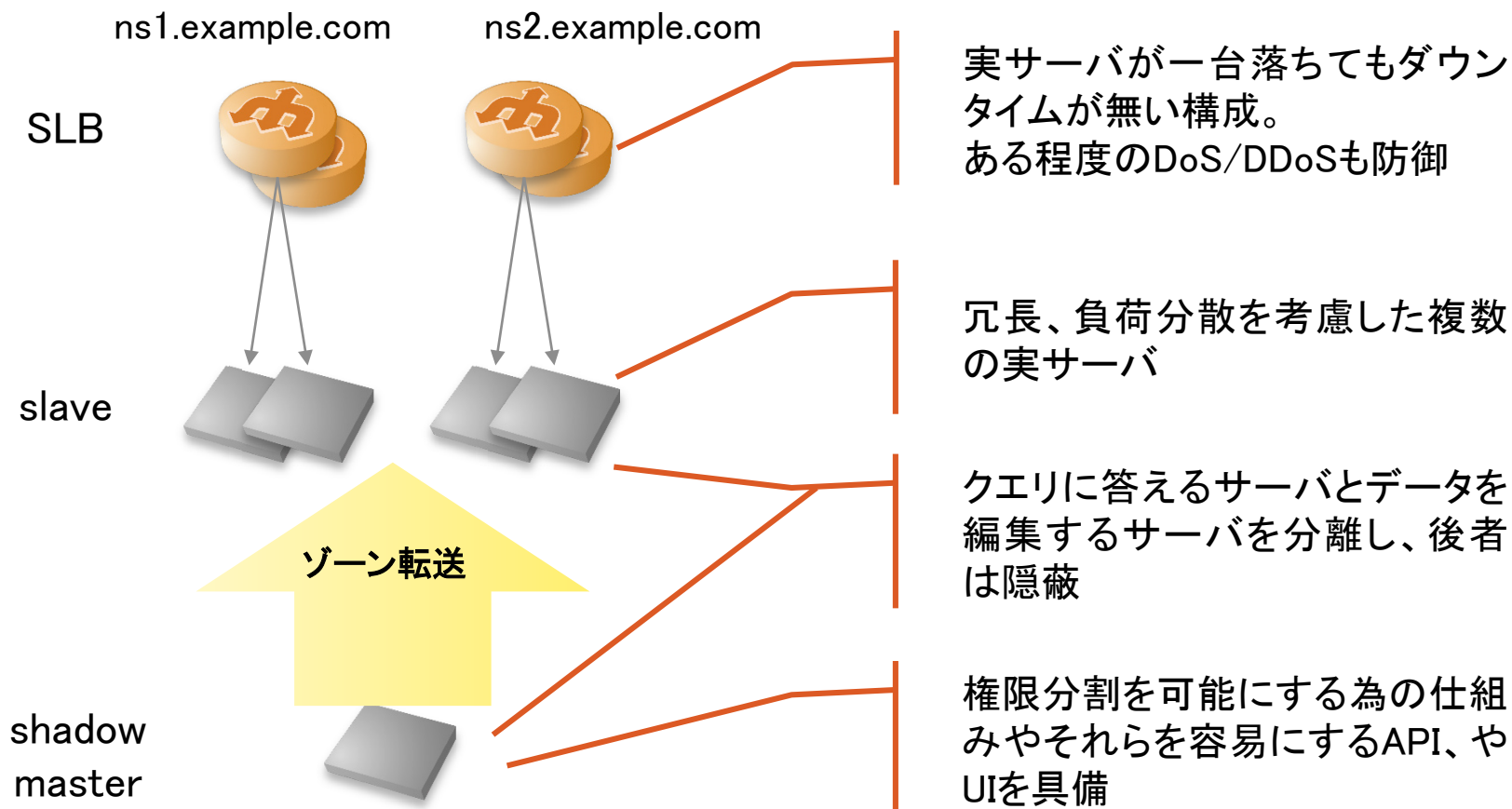
admin



基本的には admin(root) がゾーン情報  
を編集する事になり、権限分割するに  
はサブドメインを切るしかない

# example.comの権威DNSサーバ

## 解決しようとするこんな感じ



# example.comの権威DNSサーバ

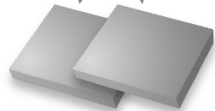
## 実装

SLB



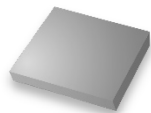
今時のハードウェアアプライアンスならどれもよいが、Source IPアドレス毎のTCP/UDPのレートリミットができるとなおよい

slave



複数の実装(例:BIND9+NSD)にしておく。負荷に応じてスケールアウトできる様な構成にしておくとなおよい

shadow  
master



権限分離、API、UIが必要な為、選択肢としては  
✓ PowerDNS等の作り込みを自作でがんばる  
✓ 売り物のアプライアンスを買う  
の2択。後者はこの用途であればVM版でもよいのでコストはある程度抑えられる。



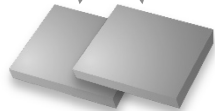
# example.comの権威DNSサーバ

## 今時の(?)実装

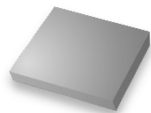
SLB



slave



shadow  
master



権威DNSサーバの機能まるごとをRoute53、AzureDNS、Akamai Fast DNS等のサービスを買ってしまうのも手。

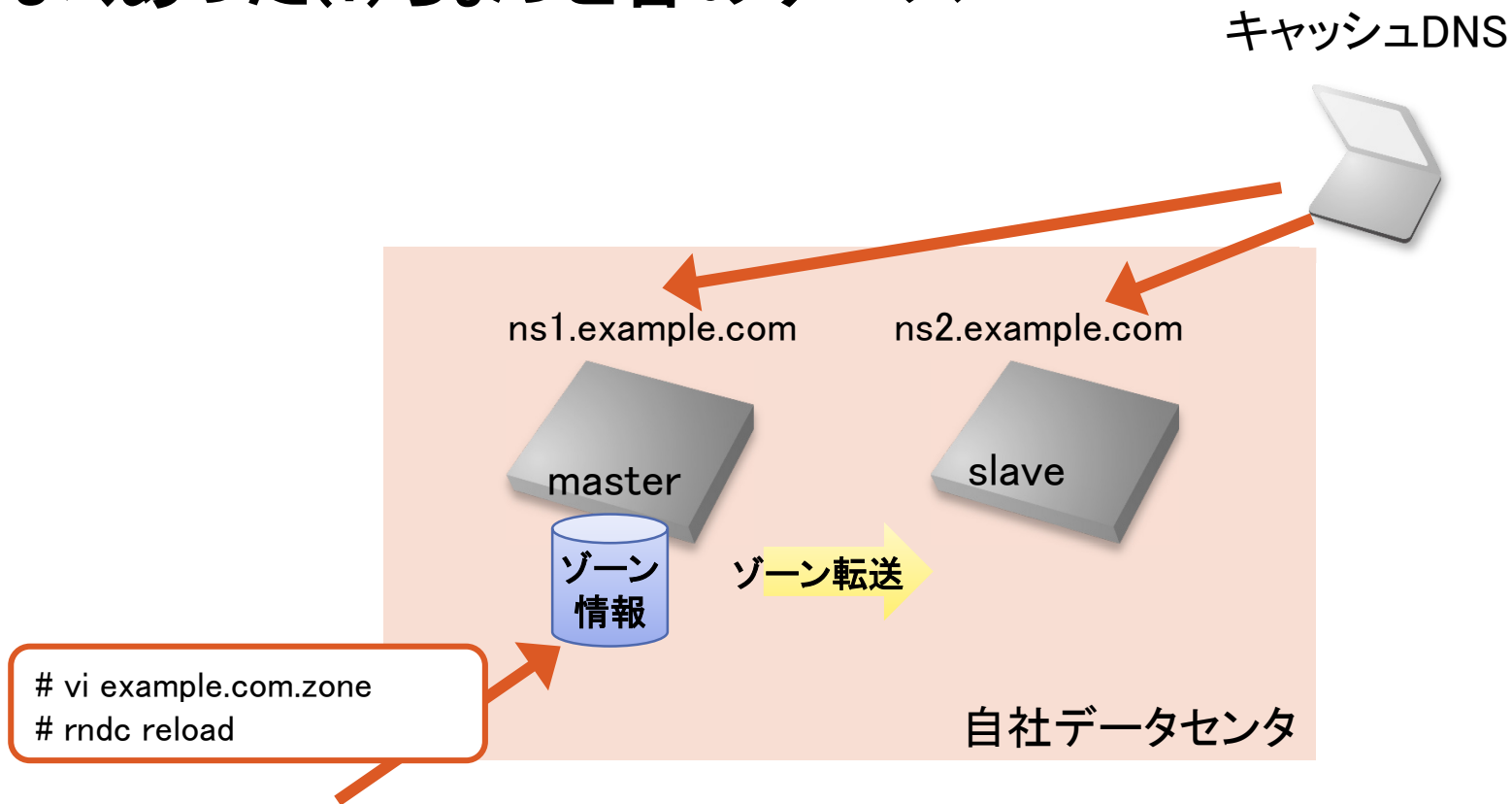
自然とDDoS対策も入ってくる。

ただ、クラウドDNSサービスやクラウドそのものがDDoS/不具合等で落ちる事例もあるので、NS毎にバラす等の考慮も必要

ゾーン編集機能も、権限分離、API、UI等豊富に提供されている。

# example.comの権威DNSサーバ

## よくあった(?)ちょっと昔のケース



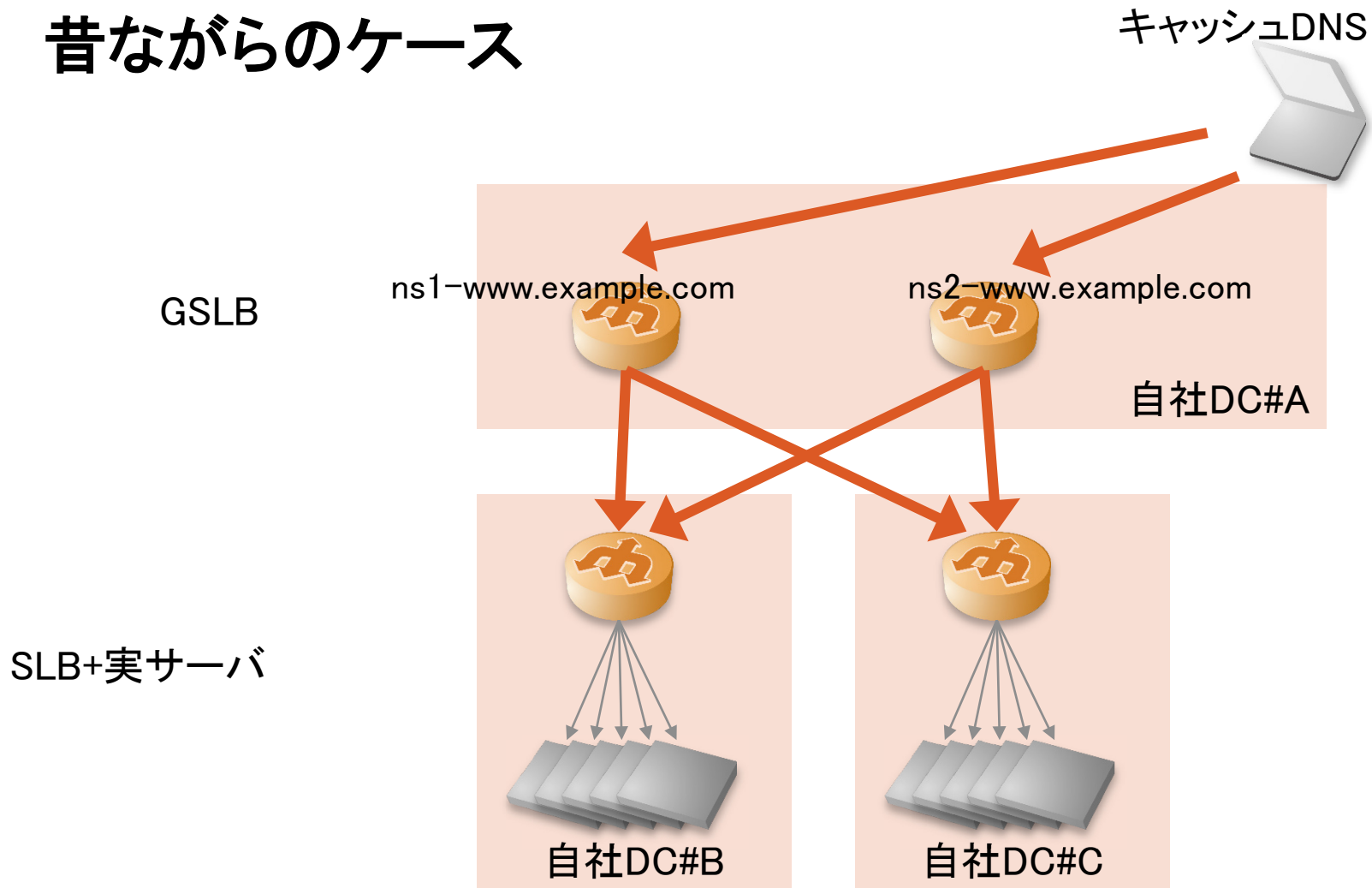
admin



ユースケースその2:  
www.example.com の  
権威DNSサーバ=GSLB

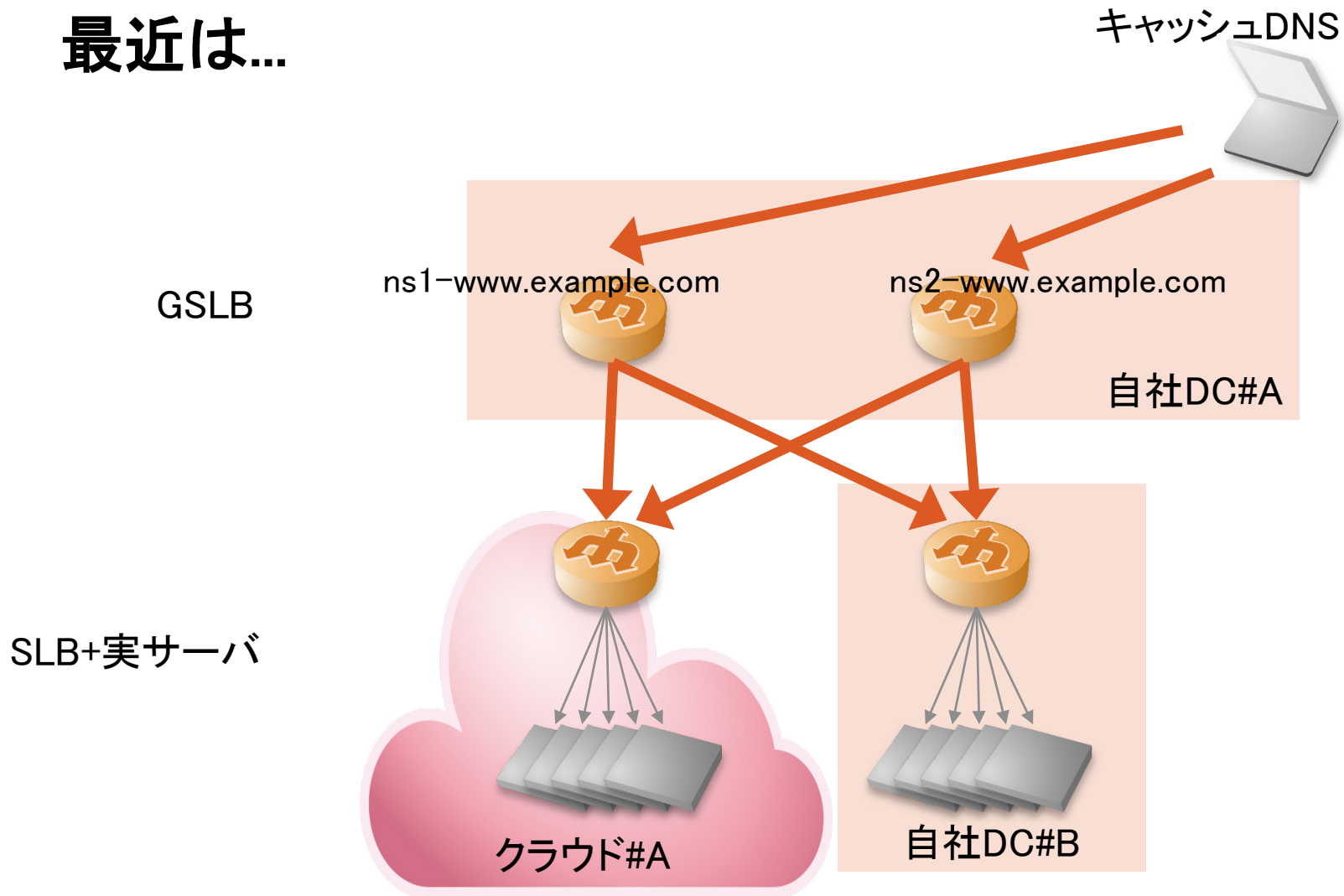
# GSLB

## 昔ながらのケース



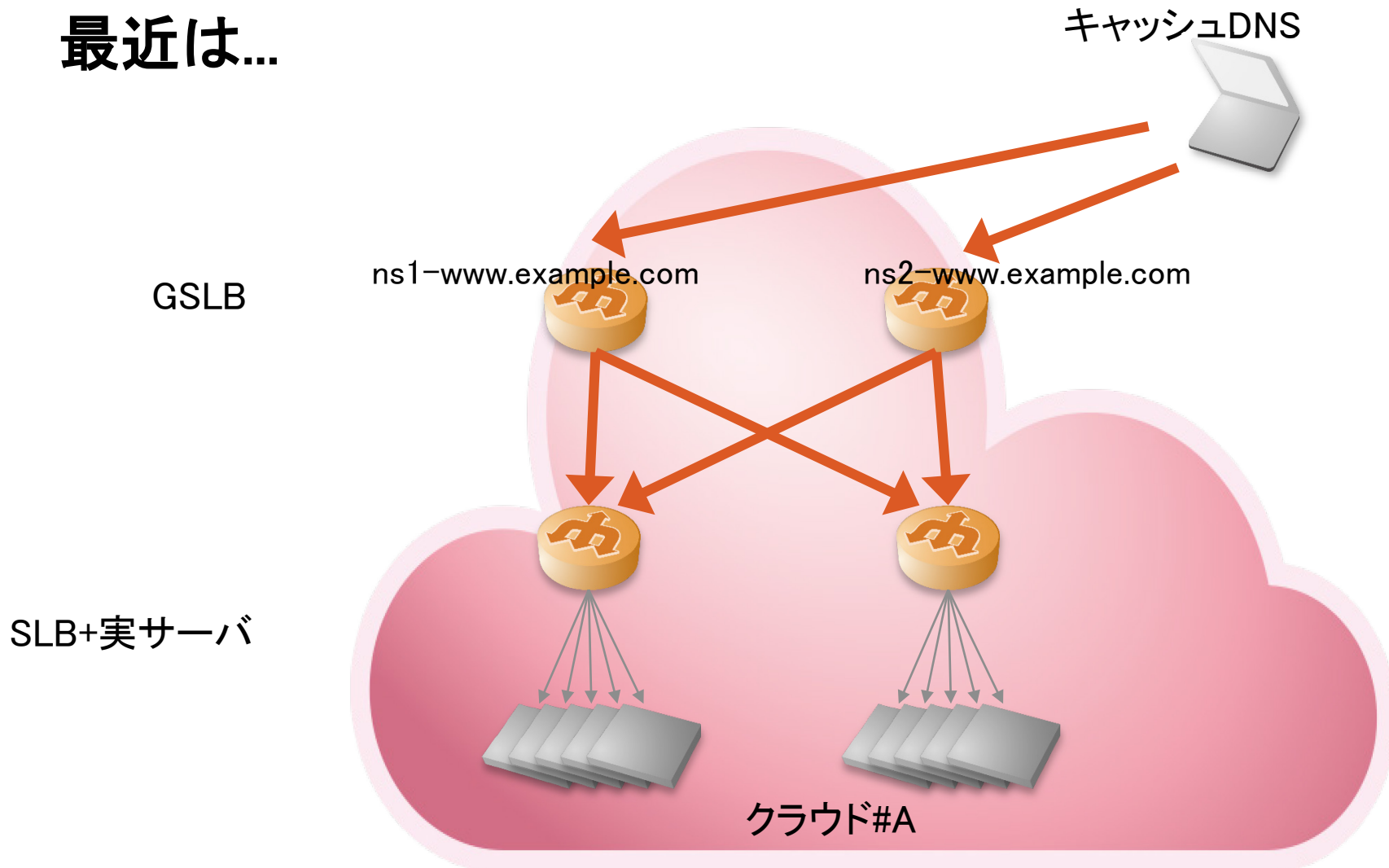
# GSLB

最近は...



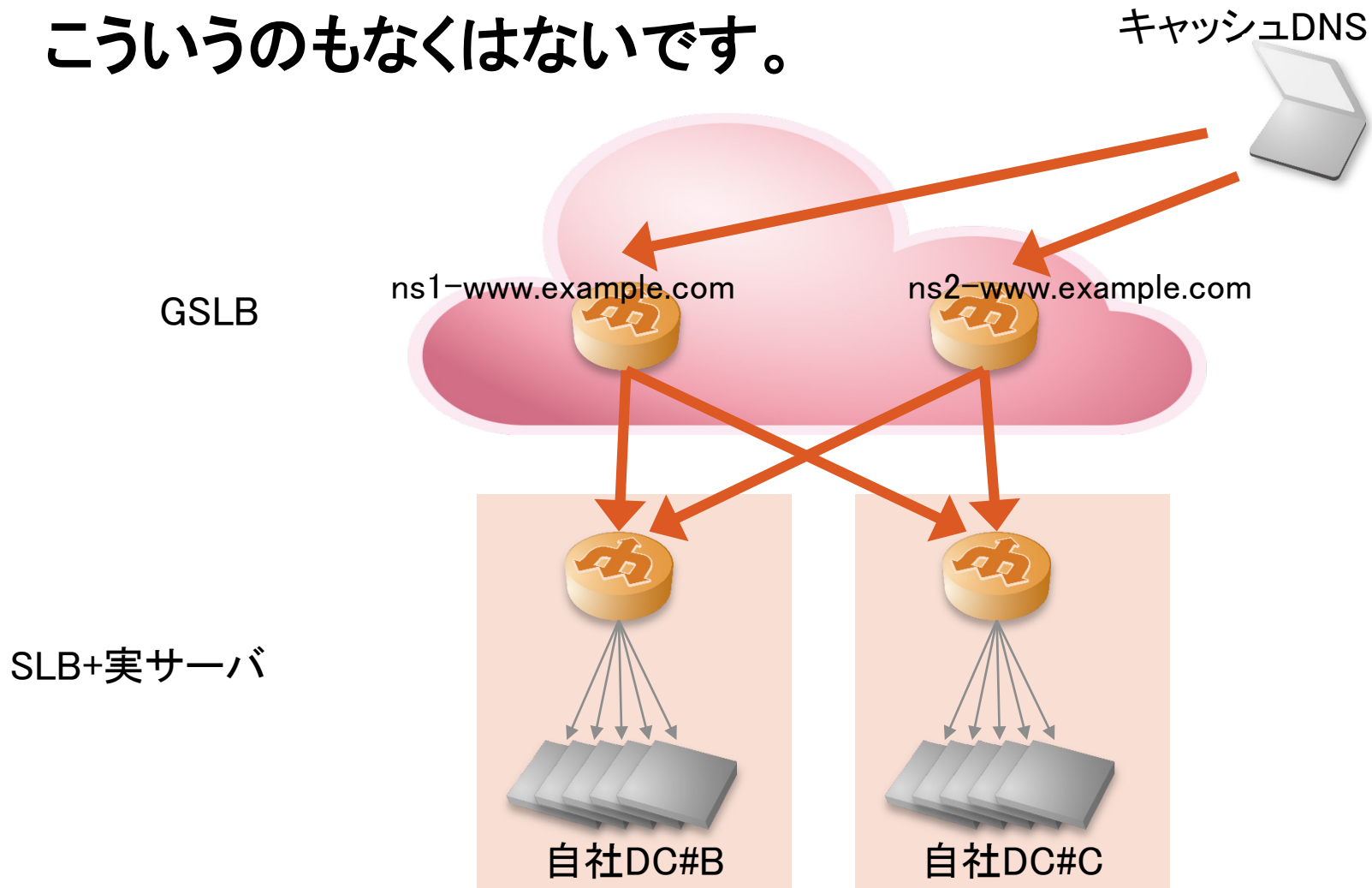
# GSLB

最近は...



# GSLB

こういうのもなくはないです。



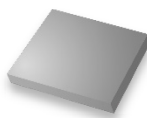
# GSLB実装

## 実装



LBアプライアンス

昔ながらのハードウェアアプライアンスLBを利用した形。最近ではベアメタル版やVM版もある為、スペックが絞ればリーズナブルにもなる。



オープンソース

gdnssdはDNS負荷分散、ヘルスチェックを含めた実装として最近hot。  
一般的な権威DNSサーバとヘルスチェックを自己実装して連携してできなくもない。



クラウドサービス

Amazon Route53、Akamai Global Traffic Management、Azure Traffic Manager等、各社出揃ってきている。  
WebフロントをクラウドやCDNで使う場合には連携が強力でステキ。



Thank you!