MITSUBISHI ELECTRIC
Changes for the Better

ITソリューションで、エコチェンジ。 eco Changes

BINDからの卒業やってみよう ～注意すべきポイント～

オープンソースカンファレンス 2018.Tokyo/Spring

2018年02月23日

三菱電機インフォメーションシステムズ株式会社

MDIS

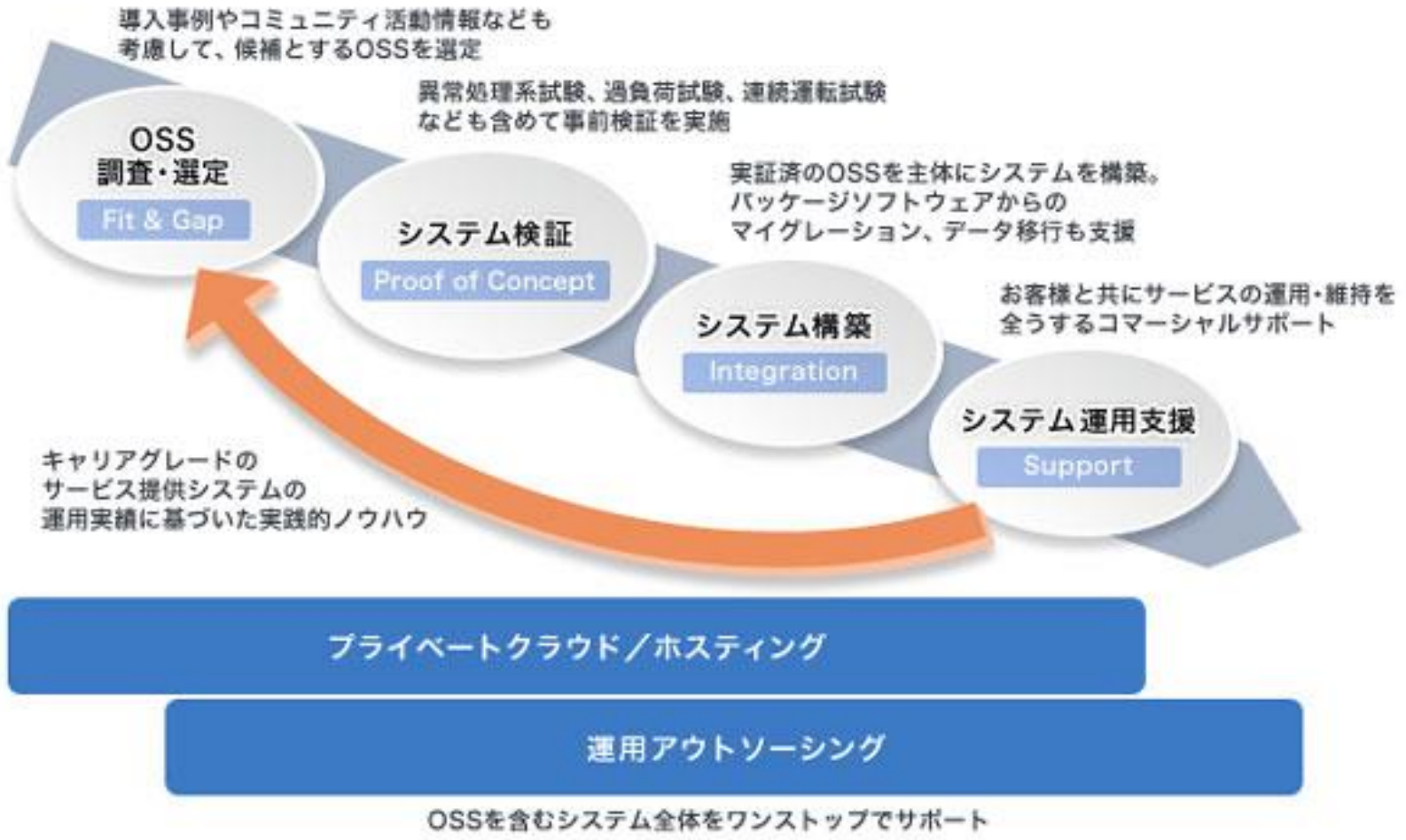
MITSUBISHI ELECTRIC
Changes for the Better

目次

自己紹介

- 名前：奥田正洋
  佐藤　匠
- 所属：三菱電機インフォメーションシステムズ株式会社
  （略称：MDIS）
- 所属部署は、通信キャリア向けのインターネットインフラサービスの開発、保守を行うSIer
- 2009年よりDNS関連業務に従事

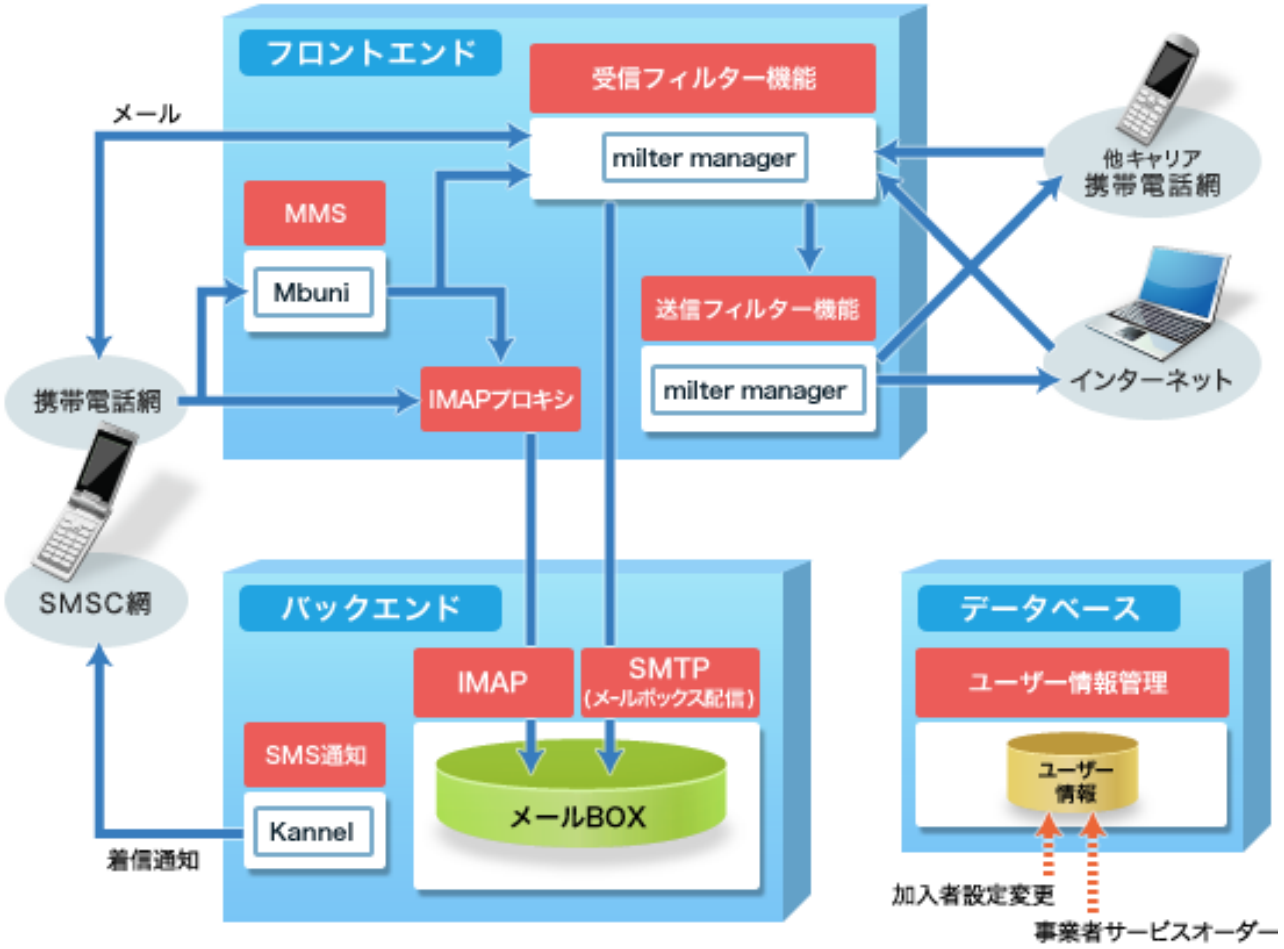
三菱電機のOSSへの取り組み（通信キャリア向け）



■ ライセンスフリーのOSSでキャリアグレードのサービス提供システムを構成
■ 試行検証と実践に基づくシステムコンサルテーション

三菱電機のOSSへの取り組み（通信キャリア向け）

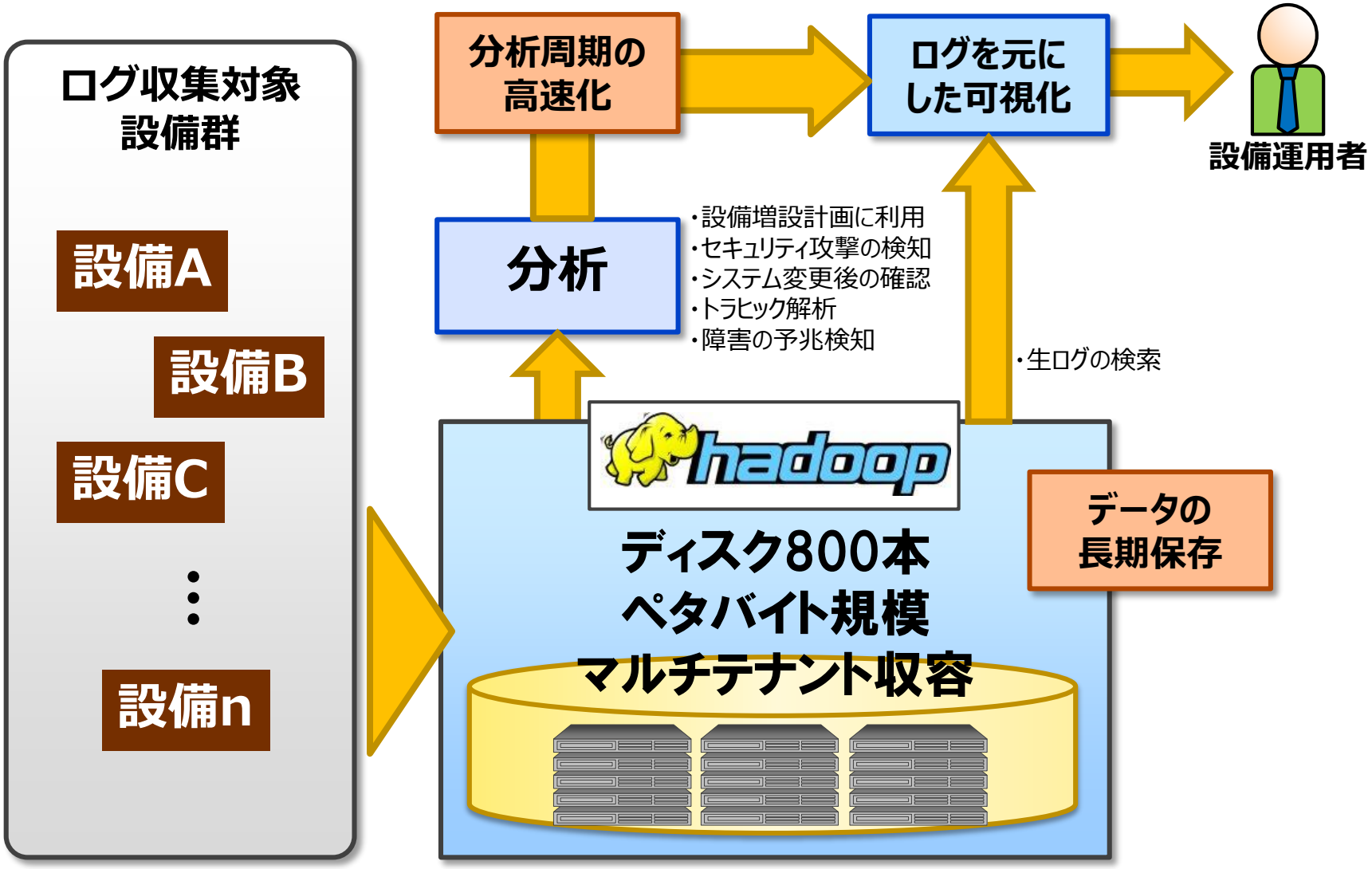
事例１）携帯電話・スマートフォン向けのメールサーバを、オールOSSで構築



■Mbuni ・・・MMSC機能を持つOSS　最新MMS規約に準拠
■Kannel ・・・SMS機能を持つOSS　SMPPv3.4対応
■milter manager ・・・フィルター処理を実装するmilterプログラムの制御・管理

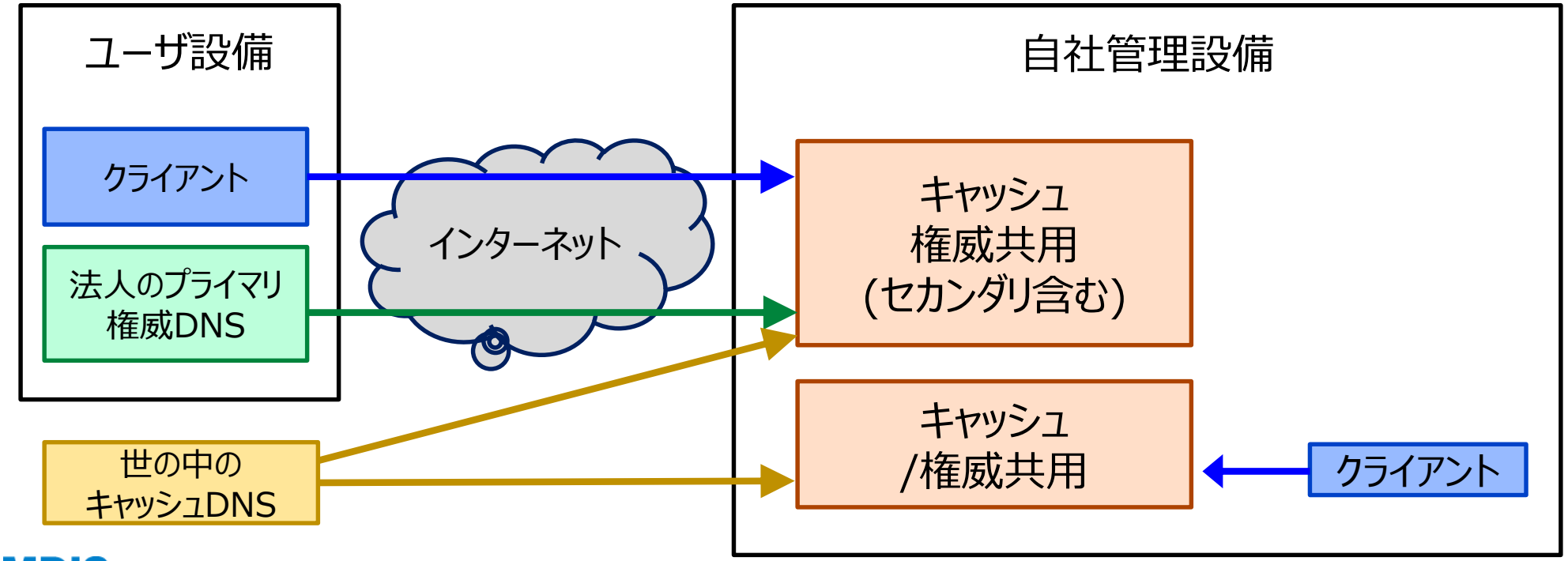
三菱電機のOSSへの取り組み（通信キャリア向け）

事例２）サービス提供設備の動作ログを集積して分析するシステムにHadoopを適用



1－1．講演の範囲

- BINDで建てたDNSを別ソフトウェアに切り替える検討をしたので、その成果と注意点のご紹介
- 主にDNSソフトウェアの切替とDNSサーバの切替手法の話



1－2．講演の範囲

BINDから別ソフトウェアへの切替を検討した背景

- 多発するBINDの脆弱性
  - BINDの脆弱性が毎年多数報告（2017年1月～で10件以上）
  - 発表から1週間もすると脆弱性を突いた攻撃
  - 脆弱性によってはワンパケットでプロセスダウン（通称：BINDコロリ）

- 高まるDNSの重要性(ユーザの意識向上)
  - DNSが停止するとサービスが停止
  - 設備のBCP切替はDNSのレコード変更で対応（災害時も無停止が必須）
  - 脆弱性発表の当日にユーザ様から影響確認・対応スケジュールの問い合わせ
  - 発表の翌日にはバージョンアップ作業

2．代表的なOSS DNSソフトウェア

- BINDの特徴
  - DNSソフトウェアとして広く使われている
  - キャッシュ機能
  - 権威機能
  - キャッシュ機能と権威機能を同時に提供可能

- 開発元
  - Internet Systems Consortium
  - 米国の非営利団体

2．代表的なOSS　DNSソフトウェア

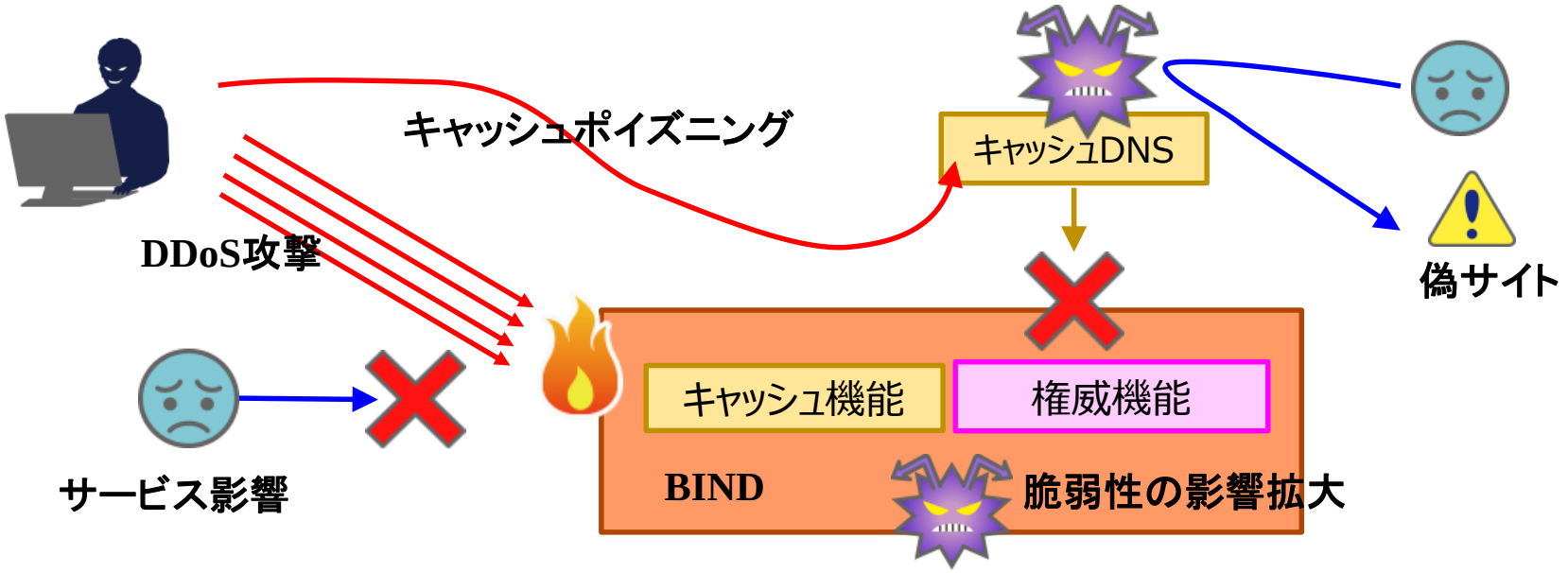
代表的なOSSのDNSソフトウェアの分類

分類	DNSソフトウェア
キャッシュDNS	BIND
	Unbound
	PowerDNS Recursor
権威DNS	BIND
	NSD
	PowerDNS Authoritative
キャッシュ権威共用	BIND

2．代表的なOSS　DNSソフトウェア

DNSソフトウェア開発の流れは、以下のようなデメリットがあるためキャッシュと権威を分離する方向で進んでいる

- キャッシュ権威を共有した場合のデメリット
  - 脆弱性が発表された場合の影響範囲が広がる
  - キャッシュ機能へのDDoSにより、同居する権威DNSのサービスにも影響する
  - キャッシュへのDDoSに引きずられて権威が応答出来なくなることにより、結果的に収容ドメインのキャッシュポイズニングのリスクが高まる



3 – 1．BINDから切り替えることの難しさ

権威機能のみ/キャッシュ機能のみであれば対応するOSSソフトウェアがあるが、切替は単純ではない

一例：権威DNSのゾーン転送処理の違いをご紹介

分類	DNSソフトウェア
キャッシュDNS	BIND
	Unbound
	PowerDNS Recursor
権威DNS	BIND
	NSD
	PowerDNS Authoritative
キャッシュ権威共用	BIND

3 – 2．BINDから切り替えることの難しさ

DNSソフトウェア切替に伴う確認

- 新DNSソフトウェアの単体機能の確認
- dumpファイルを利用したオンメモリレコードの比較
- 新旧DNSソフトウェアのdigによる全レコードANSWER応答比較

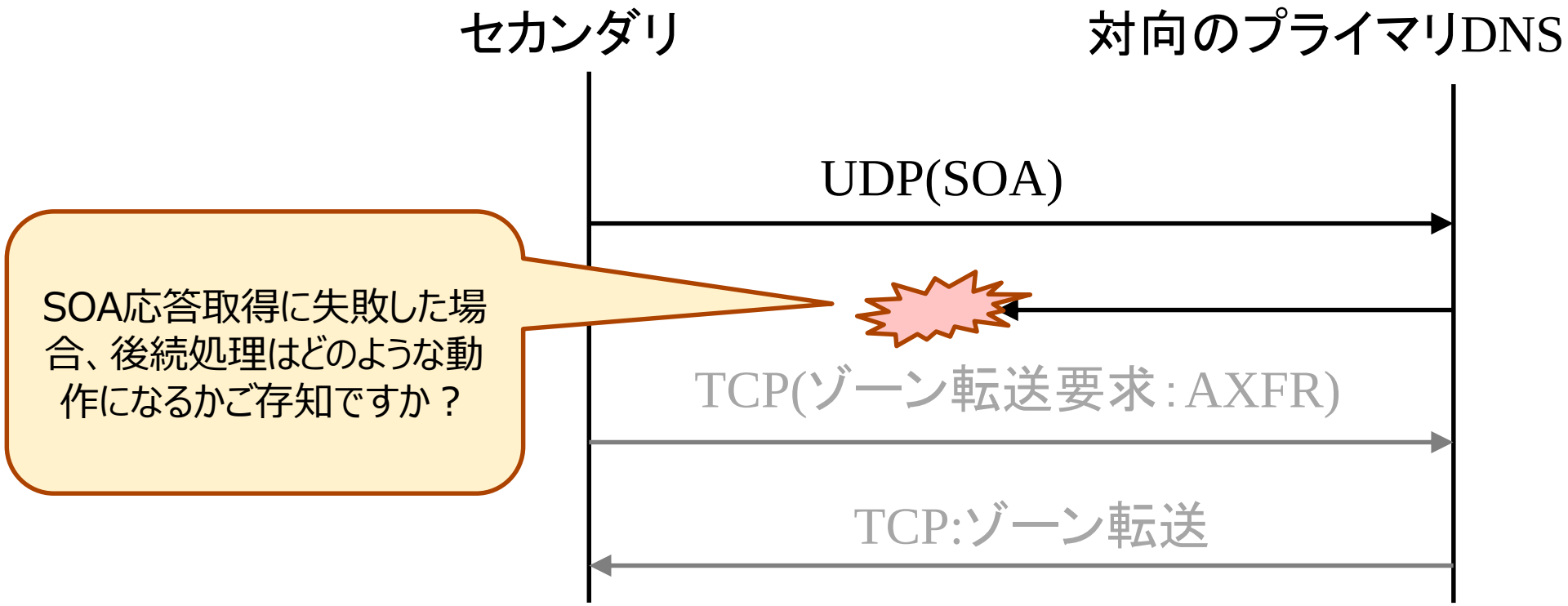
```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54334
 ;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
 ;; WARNING: recursion requested but not available

 ;; QUESTION SECTION:
 ;www.example.co.jp.        IN        A

 ;; ANSWER SECTION:
 www.example.co.jp.        300       IN        A         203.0.113.1
```

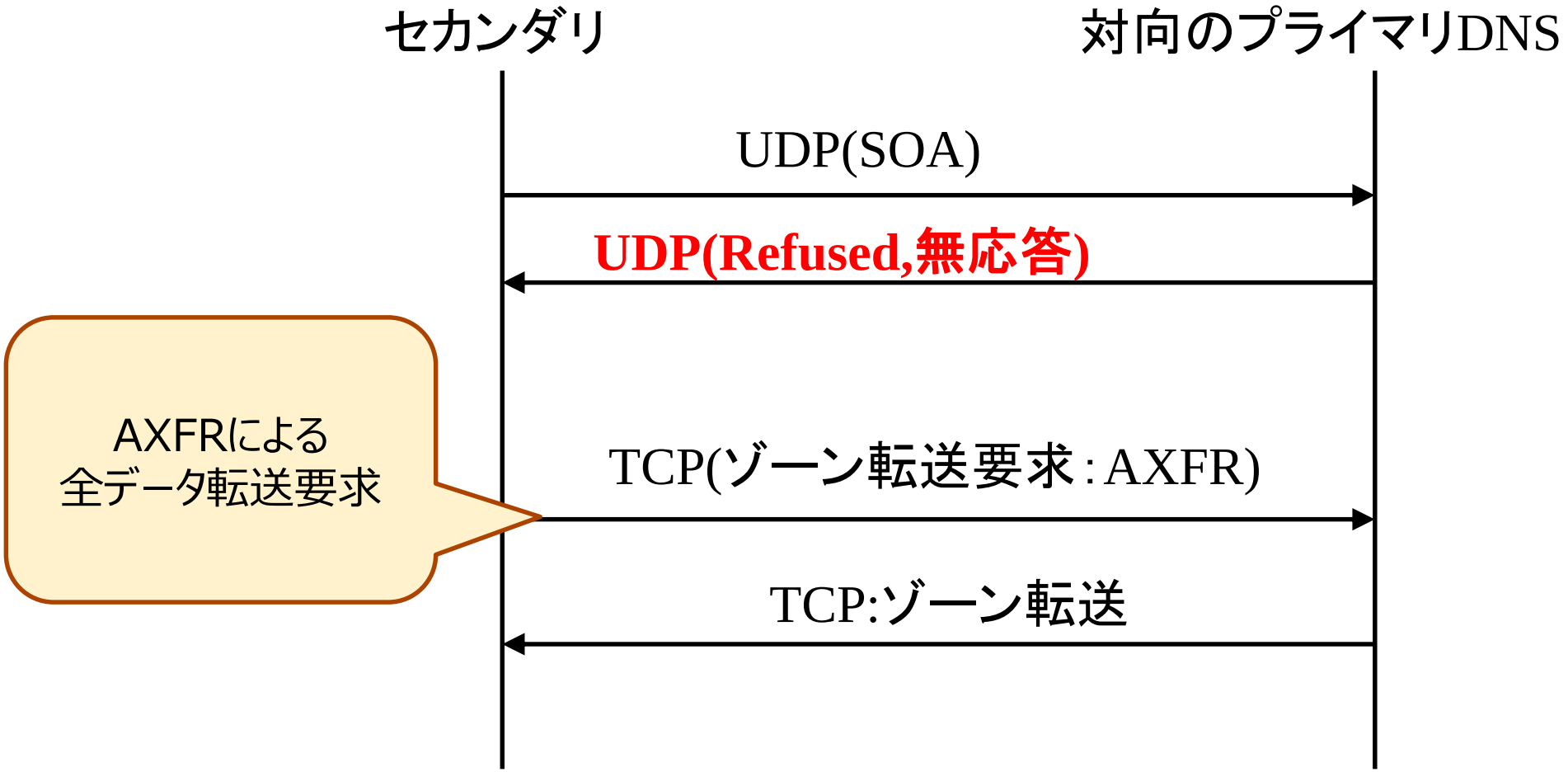
3 – 3．BINDから切り替えることの難しさ

ゾーン転送シーケンス
SOAクエリの応答が失敗した場合の動作は、RFCには定義されていない



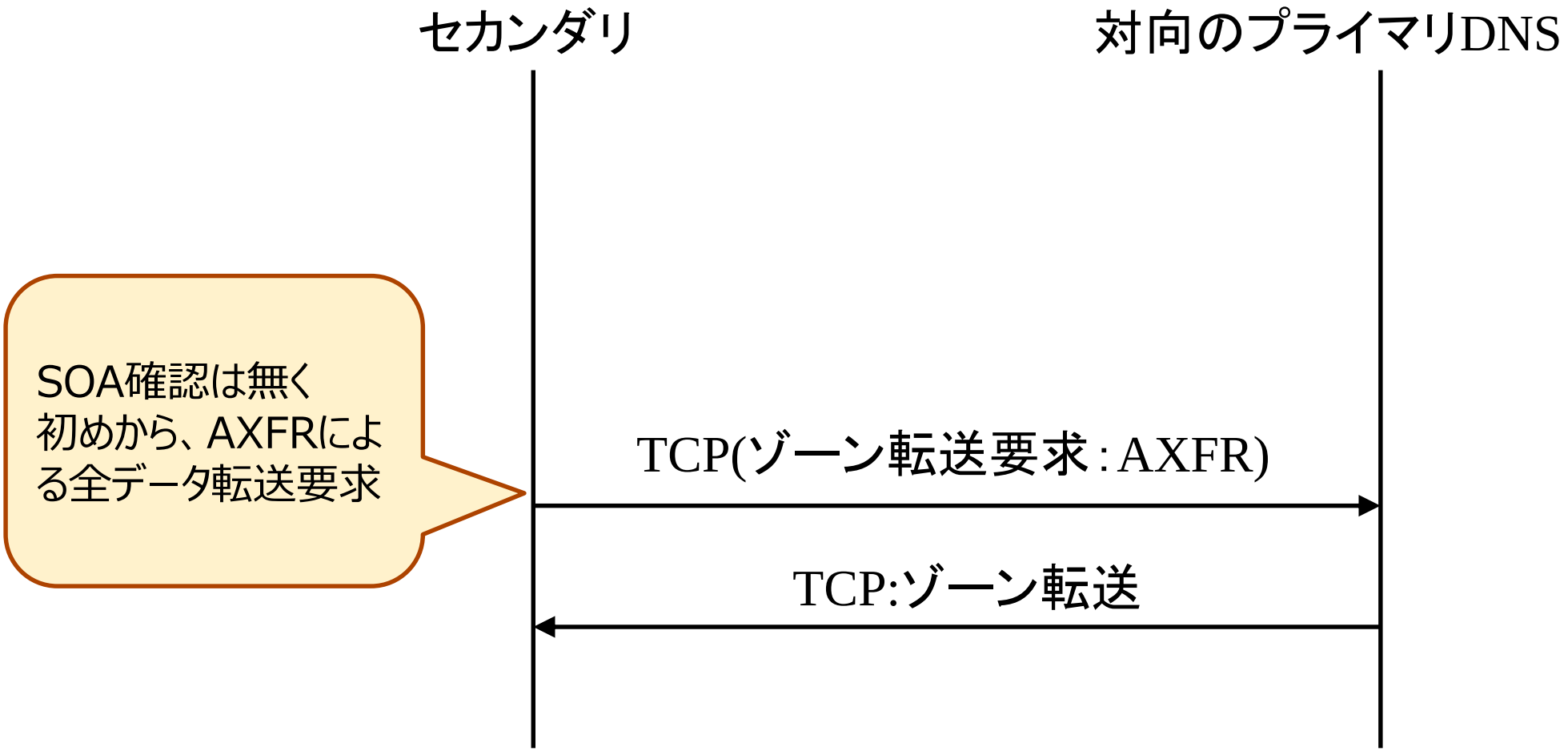
3－4．BINDから切り替えることの難しさ

- BINDのゾーン転送シーケンス



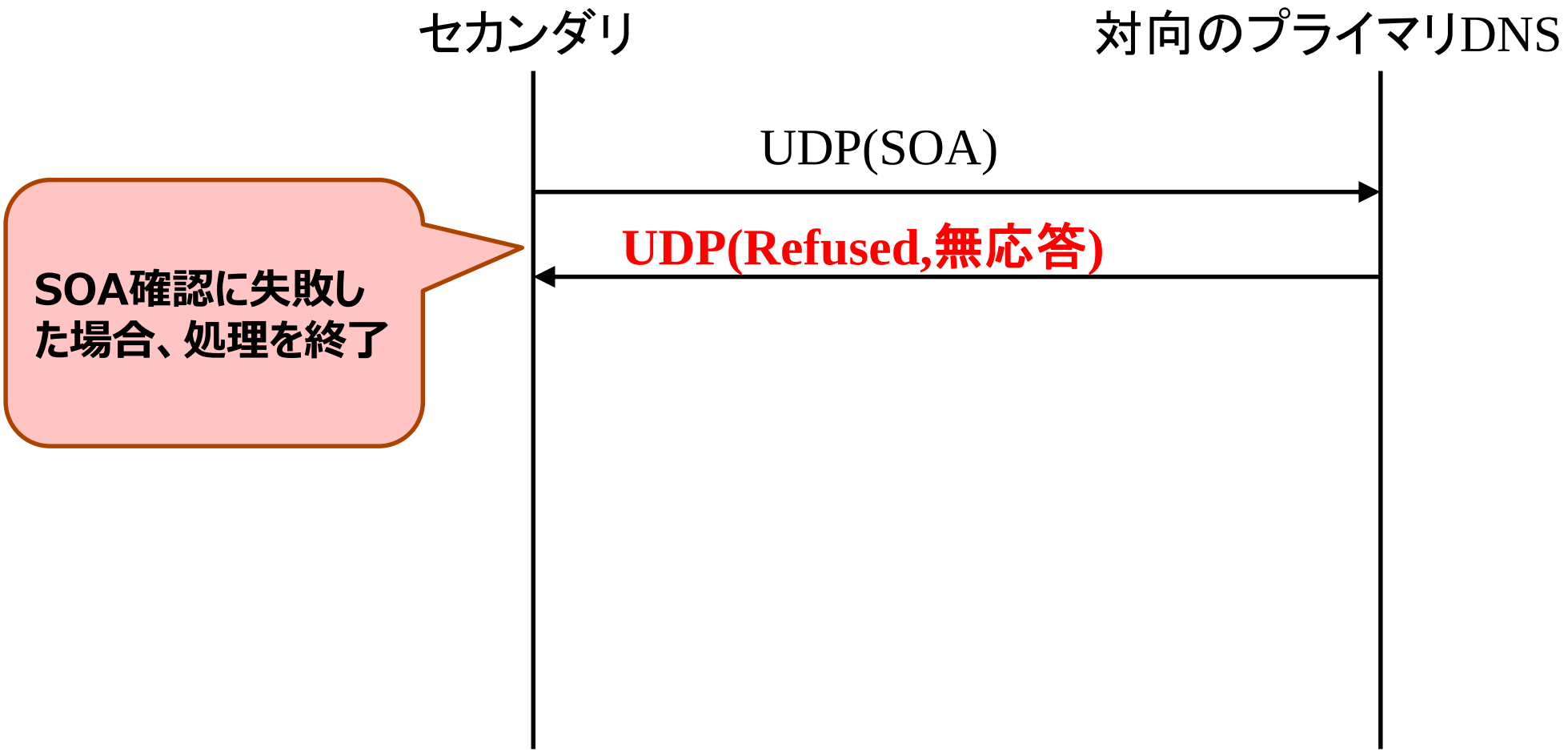
3 – 5．BINDから切り替えることの難しさ

- NSDのゾーン転送シーケンス



3－6．BINDから切り替えることの難しさ

- PowerDNSのゾーン転送シーケンス



3 – 7．BINDから切り替えることの難しさ

DNS毎の実装を知らずに切り替えると以下のような事象に陥る

- BINDからNSDへの切替
  - 常にAXFRになるためDNSサーバの負荷が高くなる
- BINDからPowerDNSへの切替
  - SOAの失敗時にAXFRに遷移しないため、ゾーン転送に失敗するゾーンが存在する

3 – 8．BINDから切り替えることの難しさ

今回のご紹介は一例にすぎない

我々が検証した中で、BINDからの切替の難しさを感じるところ

- RFCの記述に曖昧なところがあり、DNS毎に挙動が異なる箇所がある
- BIND独自処理を事前に把握することが難しく、切替作業の難易度を高める

４．キャッシュ権威共用の切替

そもそも、キャッシュ権威共用には代替のDNSソフトウェアが無い。
キャッシュ権威共用が理由でBINDを使用するケースも多い？

分類	DNSソフトウェア
キャッシュDNS	BIND
	Unbound
	PowerDNS Recursor
権威DNS	BIND
	NSD
	PowerDNS Authoritative
キャッシュ権威共用	BIND

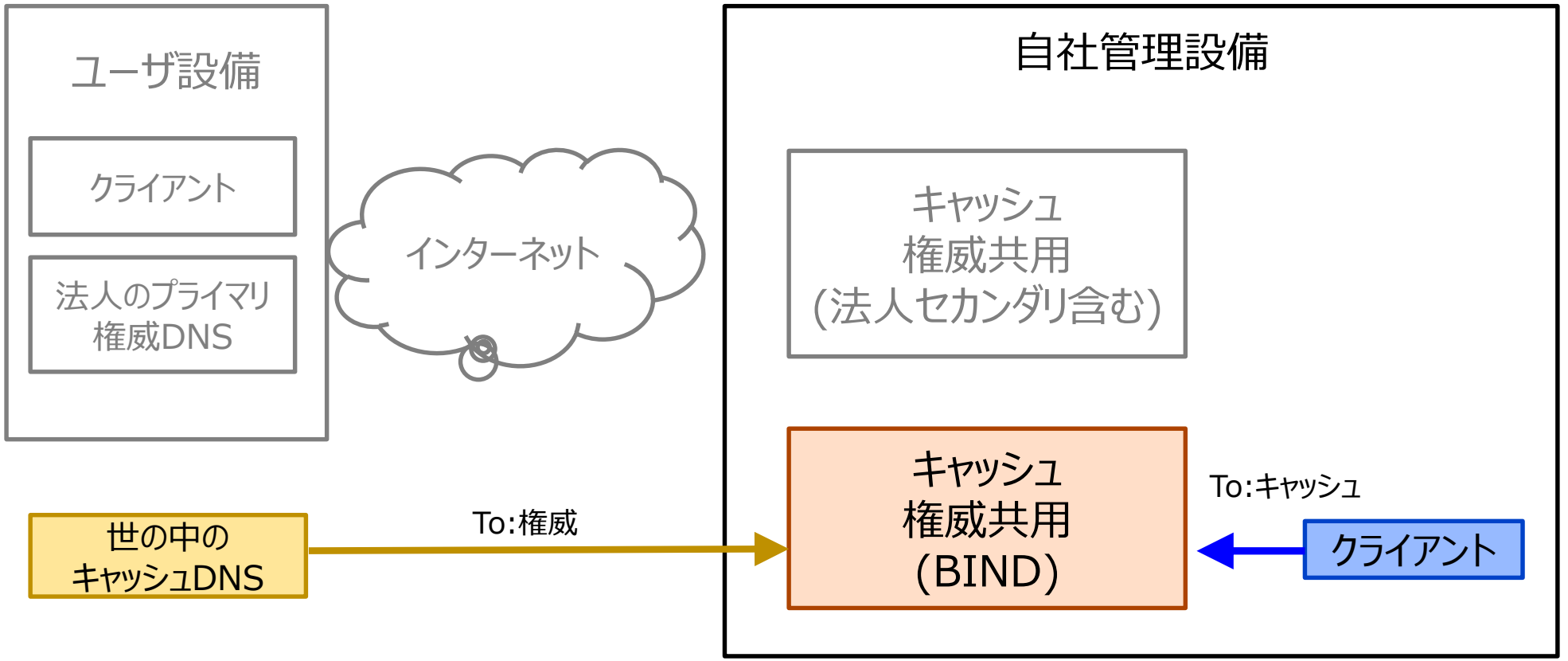
４．キャッシュ権威共用の切替

自社でプライマリDNSを管理している場合、BINDから切替が可能

- 新設した権威DNSに１ドメインずつ移管する方法
- 新設した権威DNSに一括して移管する（NSのAレコード変更）

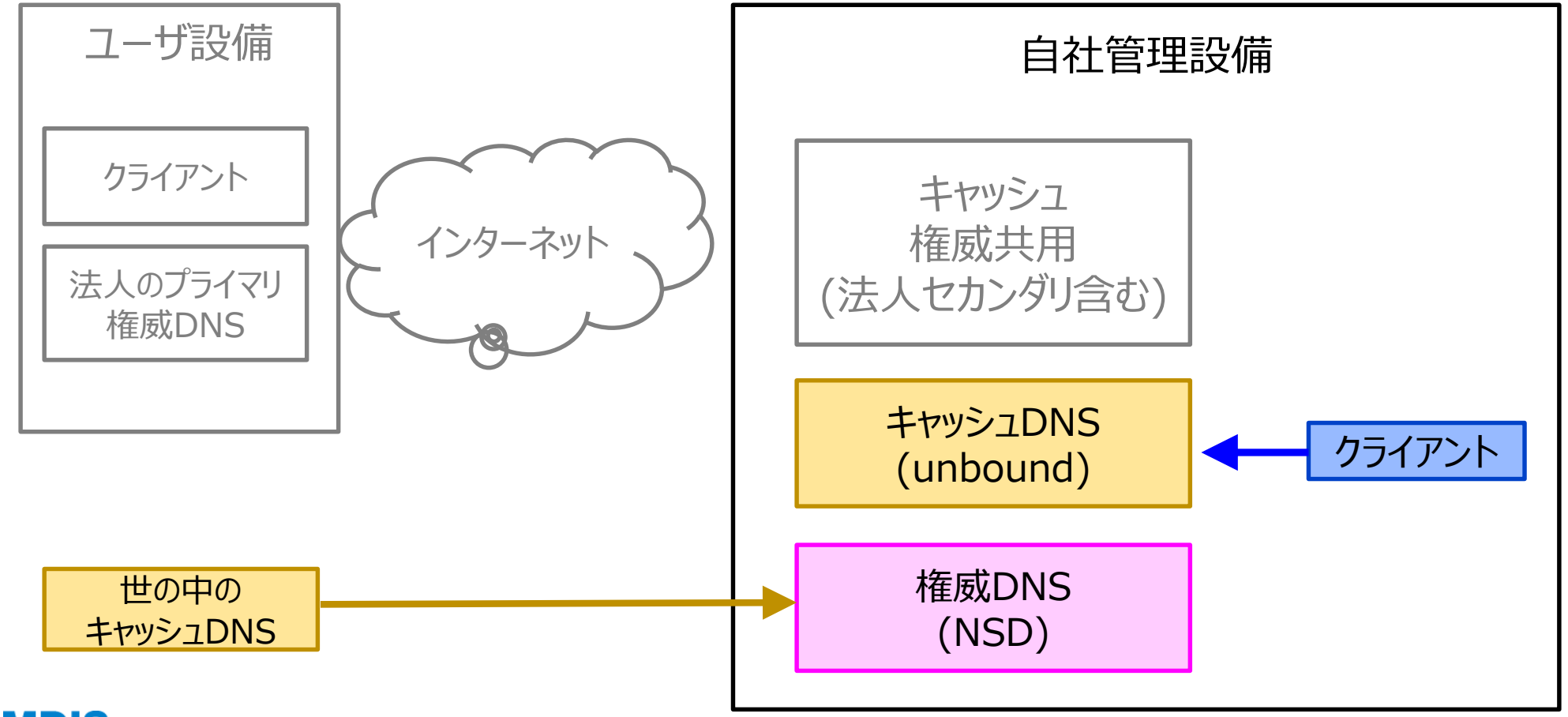
４－１－１．ドメイン単位の切替方法

- 現状キャッシュ権威共用のDNS



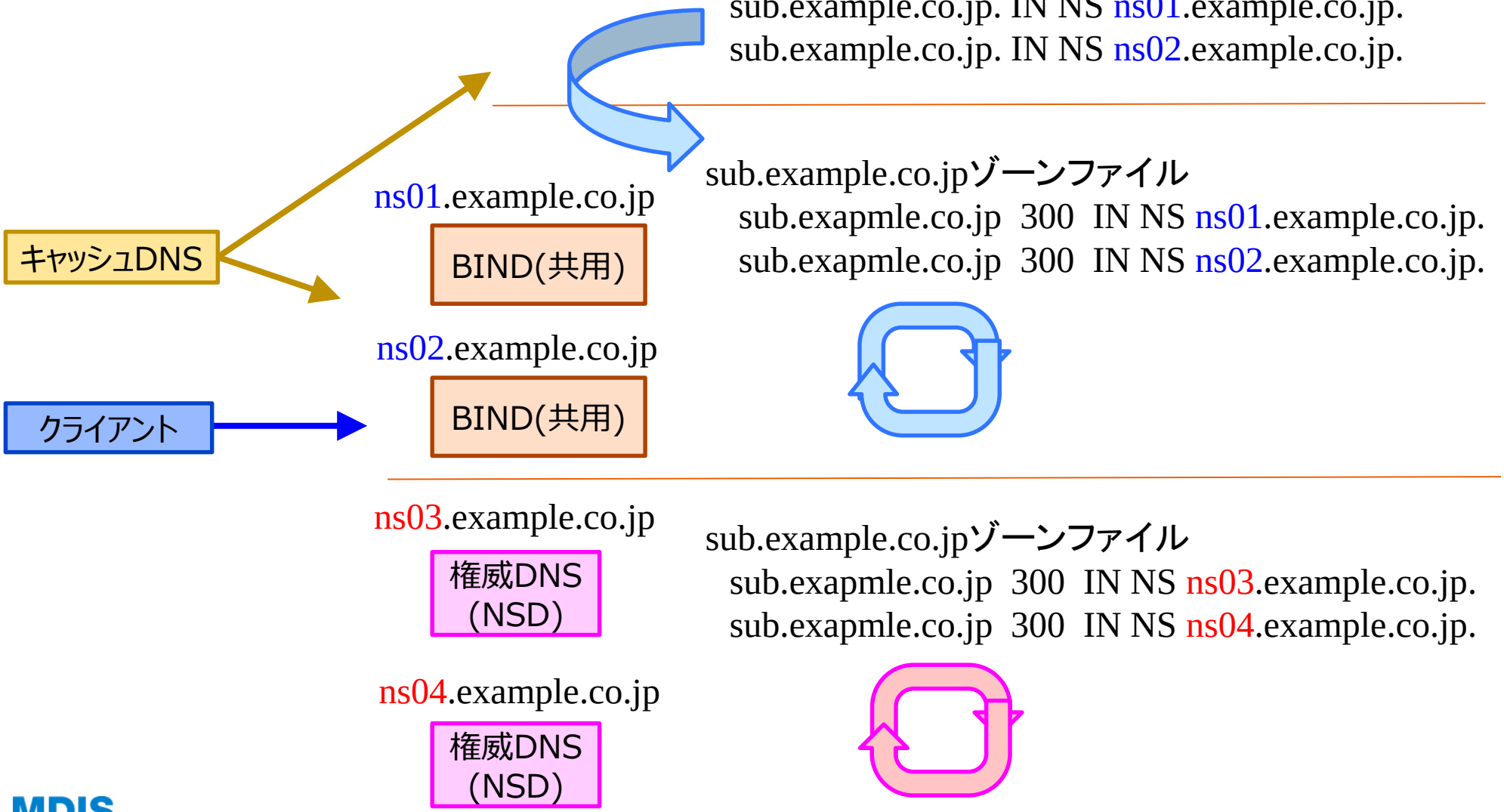
4－1－2．ドメイン単位の切替方法

- 新設したDNSにドメインを移管する方法



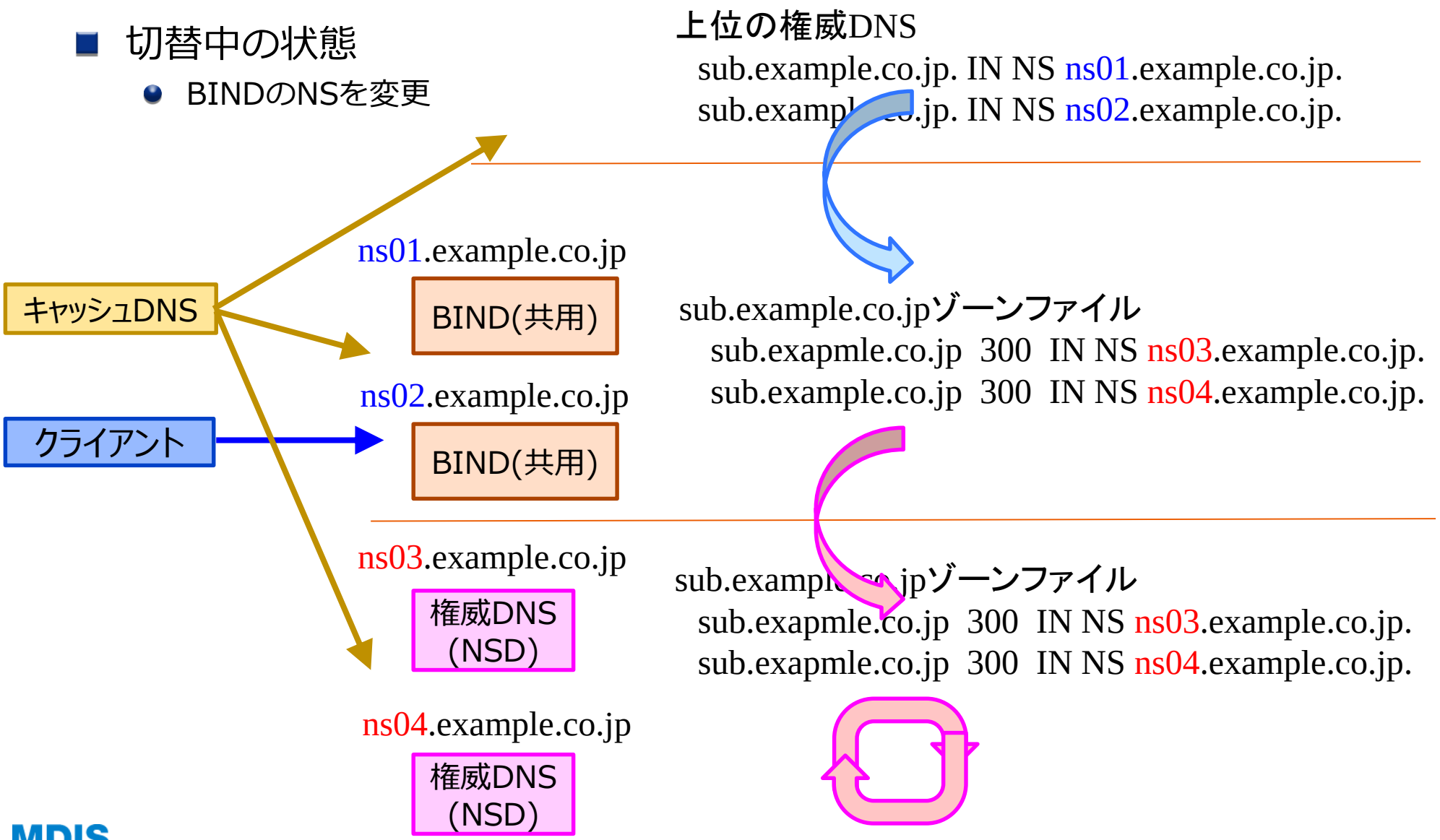
４－１－３．ドメイン単位の切替方法

- 切替前の状態



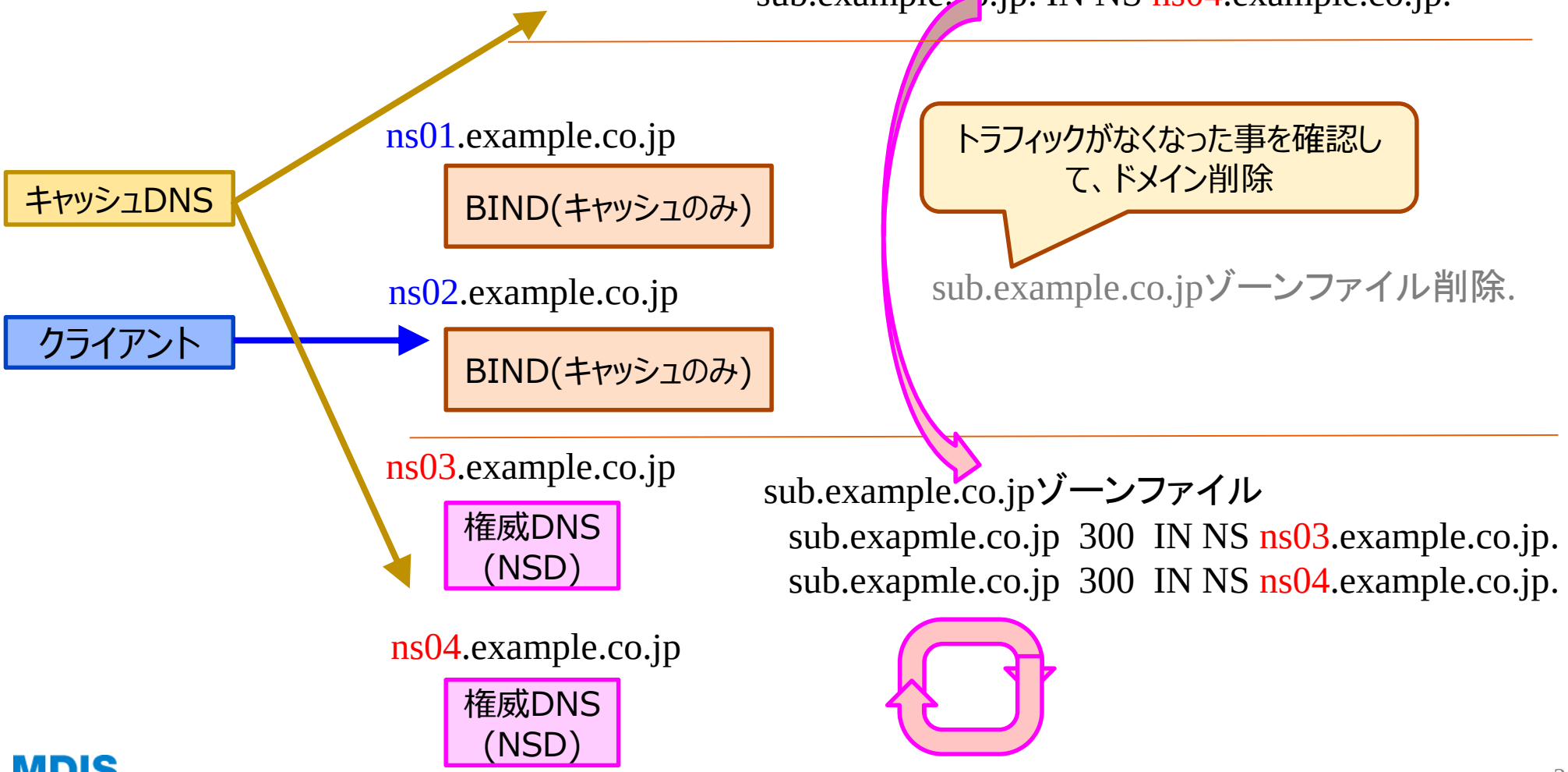
４－１－４．ドメイン単位の切替方法

- 切替中の状態
  - BINDのNSを変更



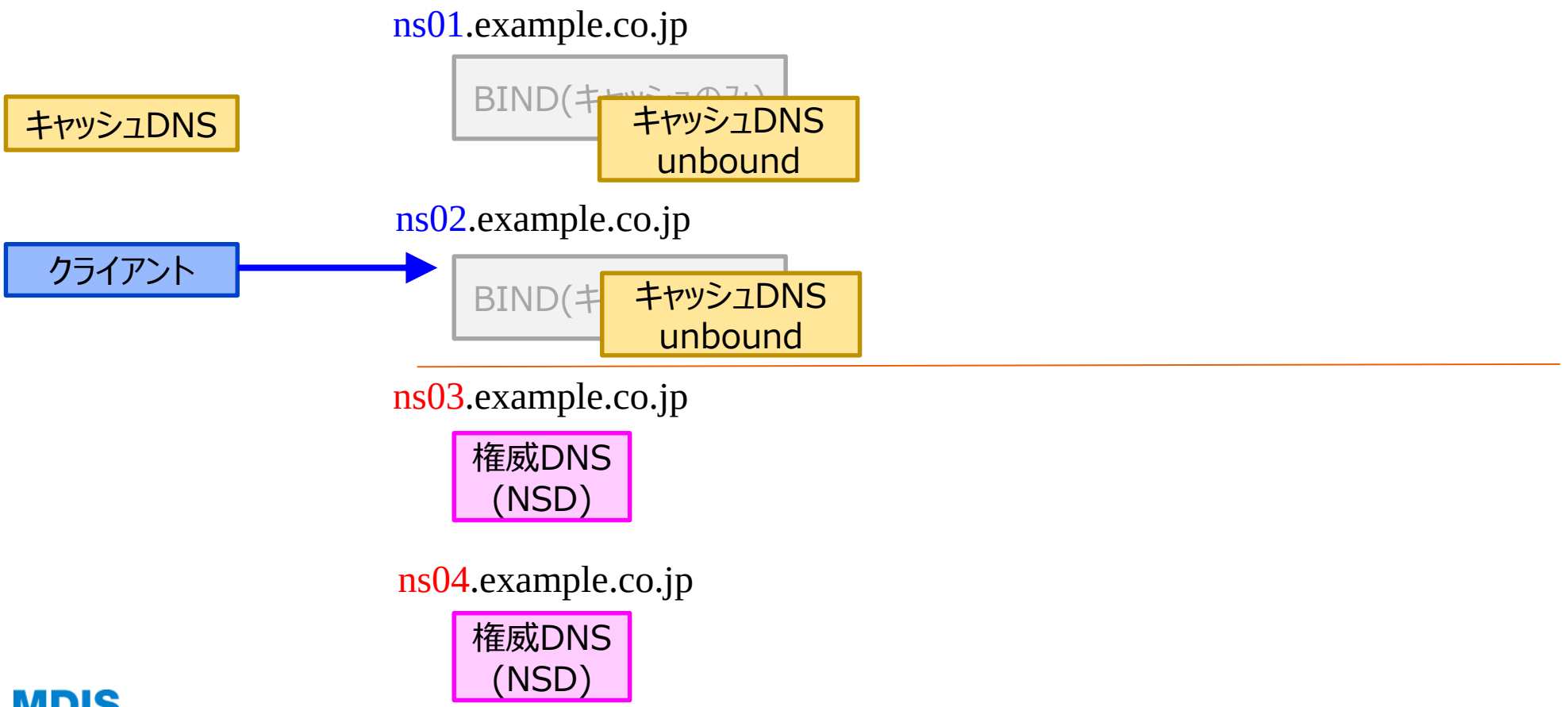
４－１－５．ドメイン単位の切替方法

- ドメインの移管完了
  - 上位権威DNSのNSを変更



４－１－６．ドメイン単位の切替方法

- BINDの置換
  - キャッシュ機能のみとなったBINDを別のソフトウェアに置き換える



４－１－７．ドメイン単位の切替方法

ドメイン毎の移管による切替方式

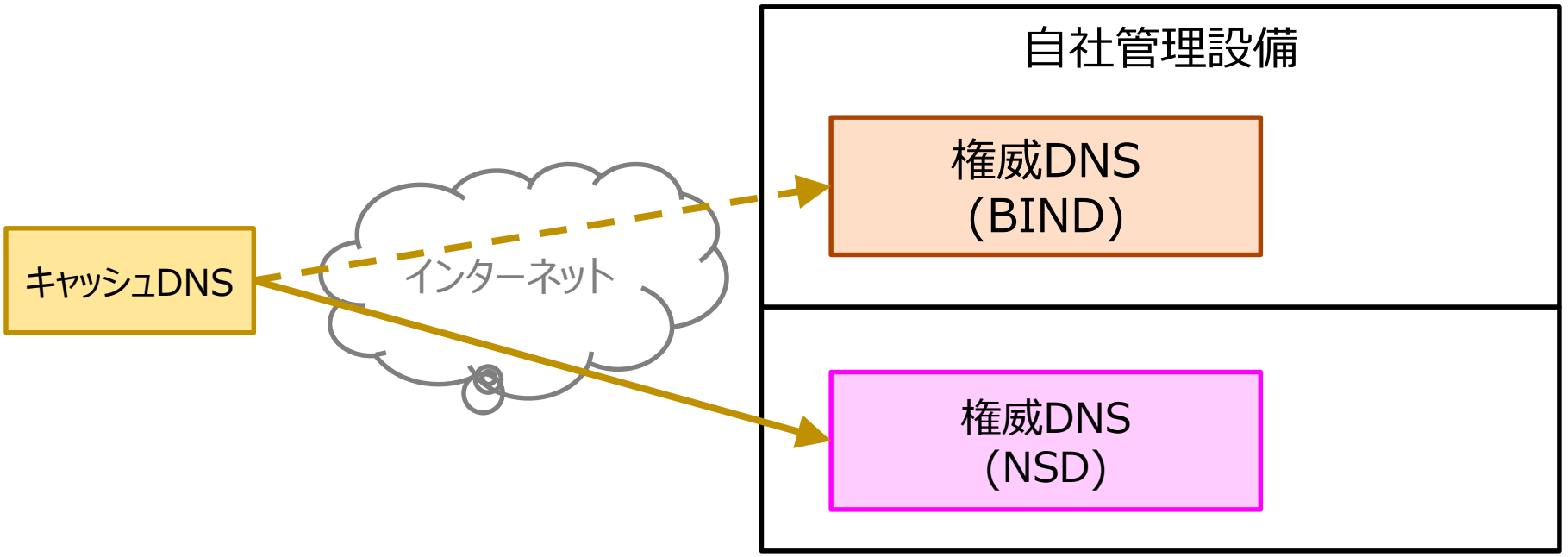
- １ドメイン毎に行うため確実に移管できる
- ドメイン数が多いと手間がかかる

一括移管方法も紹介します！

4－2－1．一括切替方法

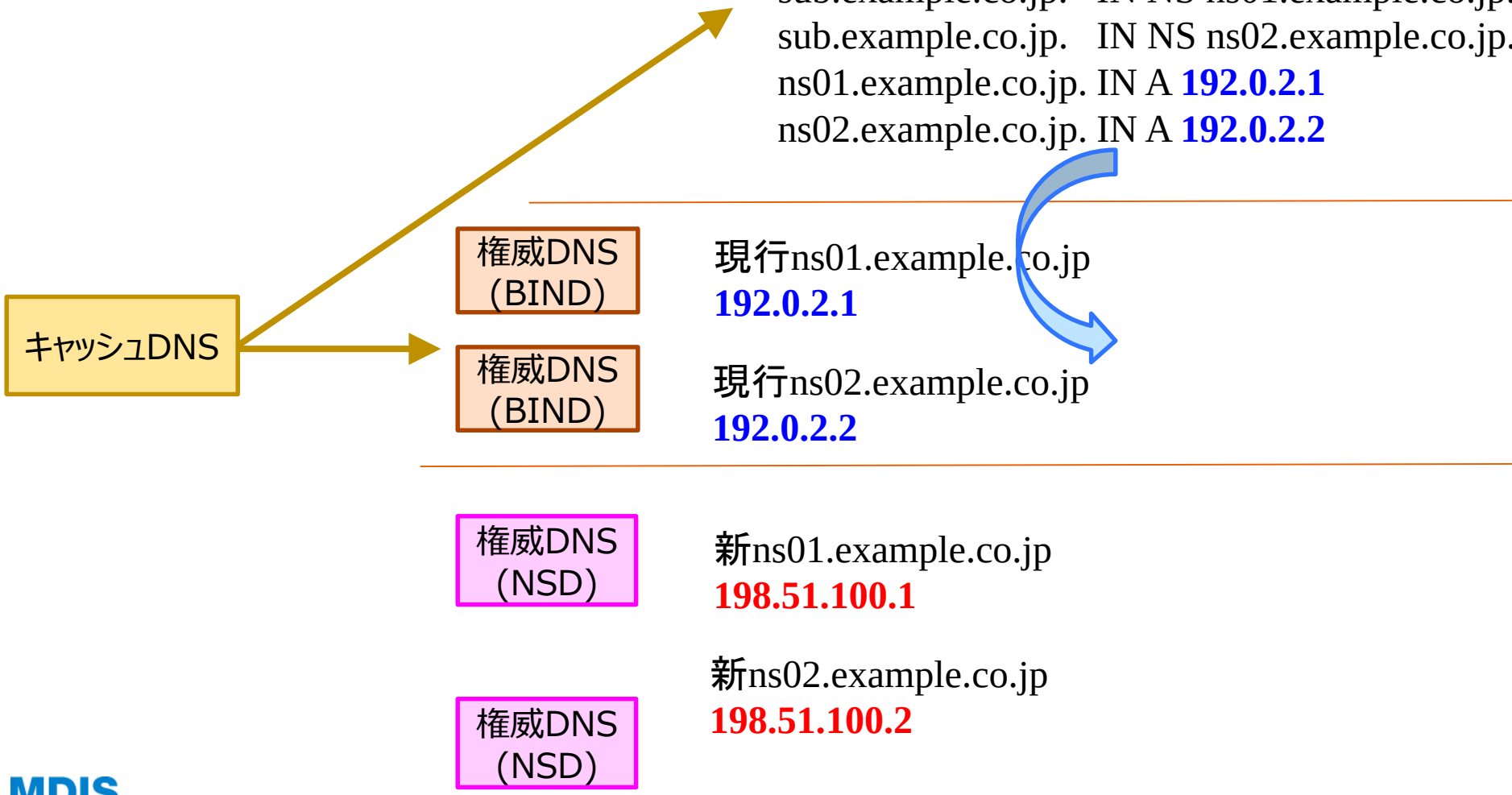
ネームサーバのIPアドレスを変更して、上位DNSからの委任先を変更する

- 権威機能のみであること
- ネームサーバのAレコードを保持する権威DNSと切替を行うDNSサーバが別であること
- 切替を行うDNSサーバのNSレコードが全て切替対象のDNSであること
- IPアドレスの変更が許容される



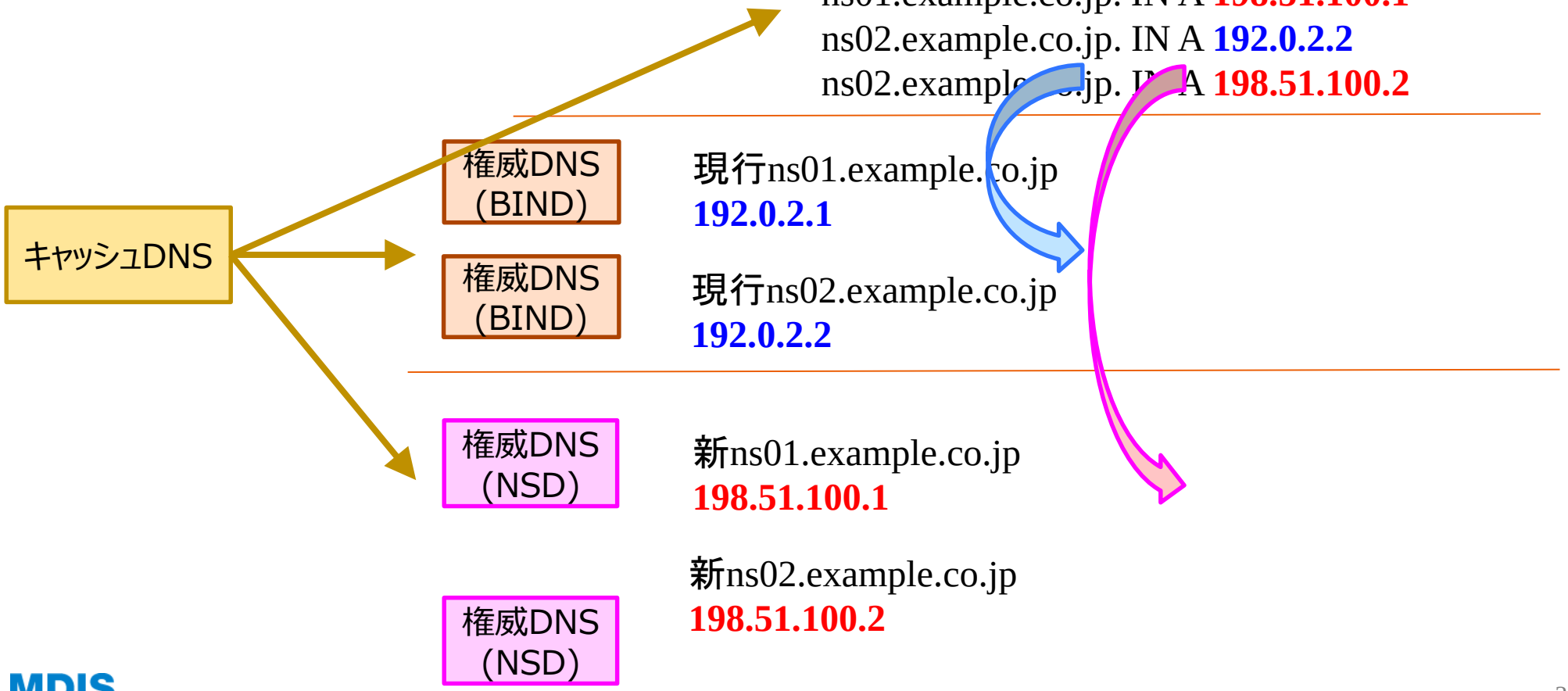
4－2－2．一括切替方法

- 切替前の状態



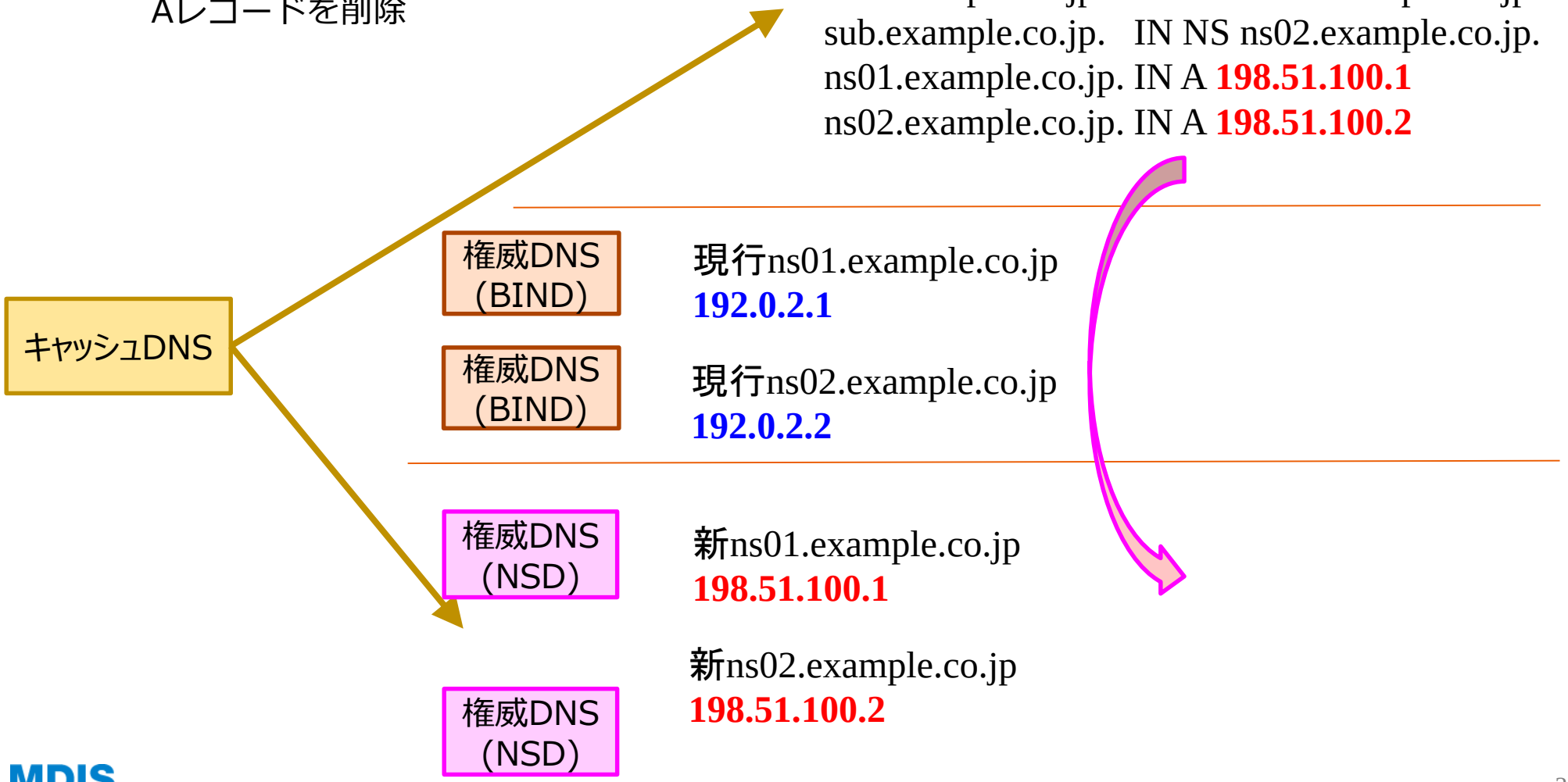
4－2－3．一括切替方法

- 切替中
  - 上位権威DNSにAレコードを追加
  - キャッシュからの再起問い合わせが分散



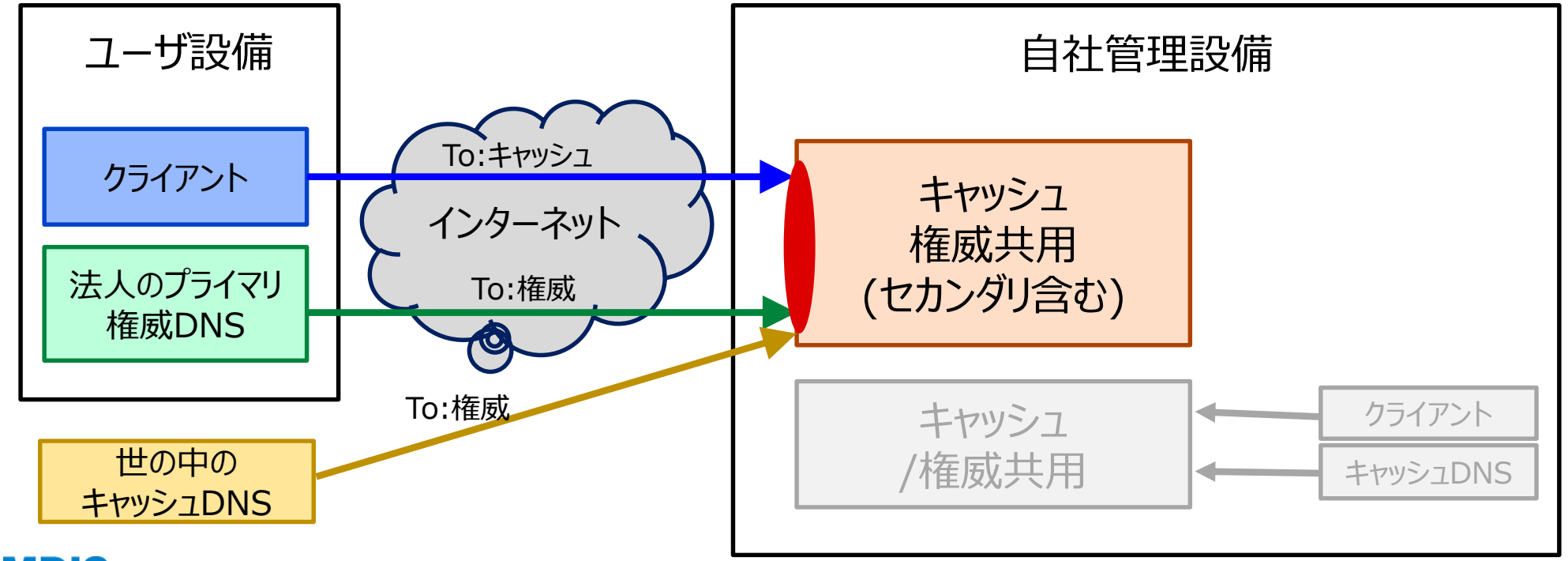
4－2－3．一括切替方法

- 完了時
  - 上位権威DNSから現行のNSのAレコードを削除



5．課題となる構成

- 単純にDNSを置き換えられないケースの紹介
  - IPアドレスを社外に共有しているため、権威機能とキャッシュ機能の分離ができない。
  - キャッシュ機能と権威機能を同時に提供できるOSSは、BIND以外は無い



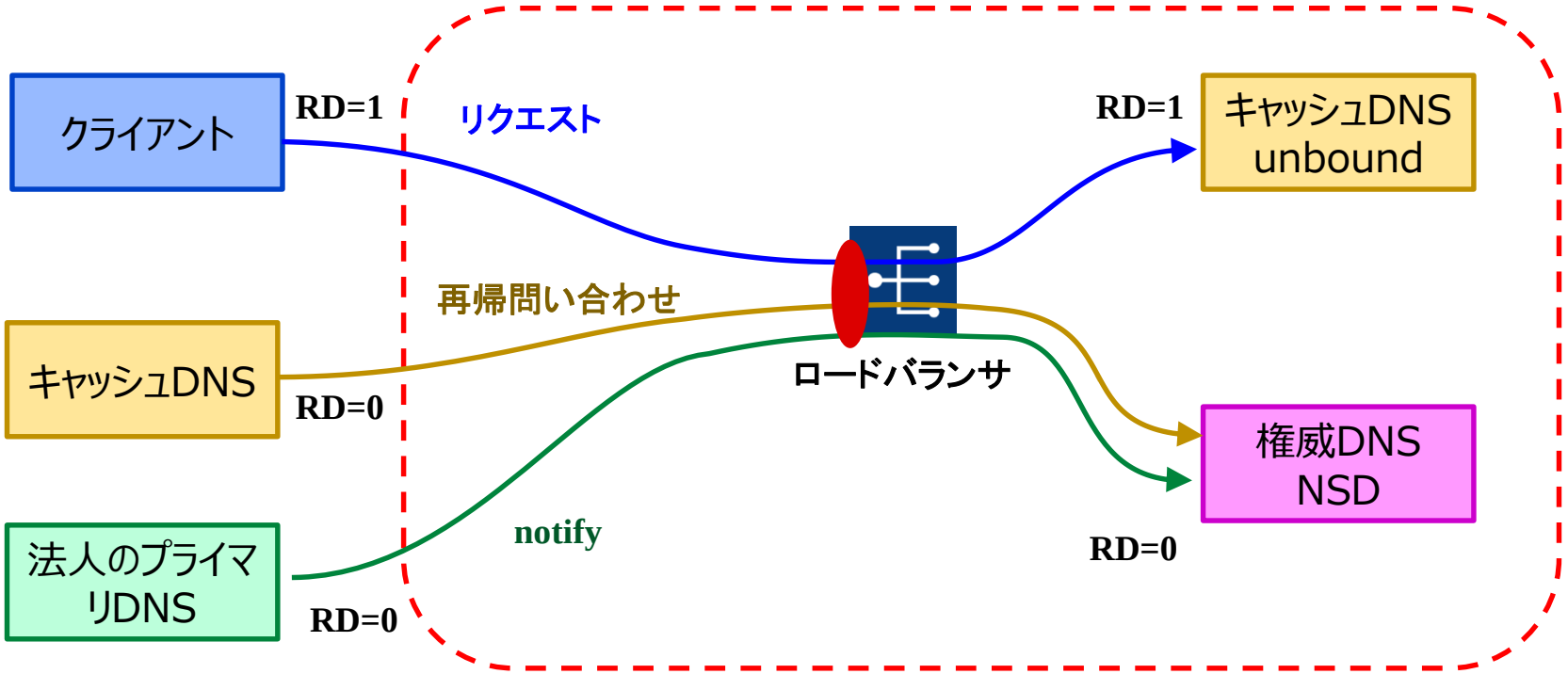
5－1－1．回避方法（RDフラグによる振り分け）

BIND以外のOSSを利用したキャッシュ権威を同一IPアドレスで提供する案

- ロードバランサにて、RDフラグを分岐条件とし振り分け先を決定

RD(Recursion Desired)フラグとは、

- 再起問い合わせを希望する場合：1
- 希望しない場合：0



5 – 1 – 2．回避方法（RDフラグによる振り分け）

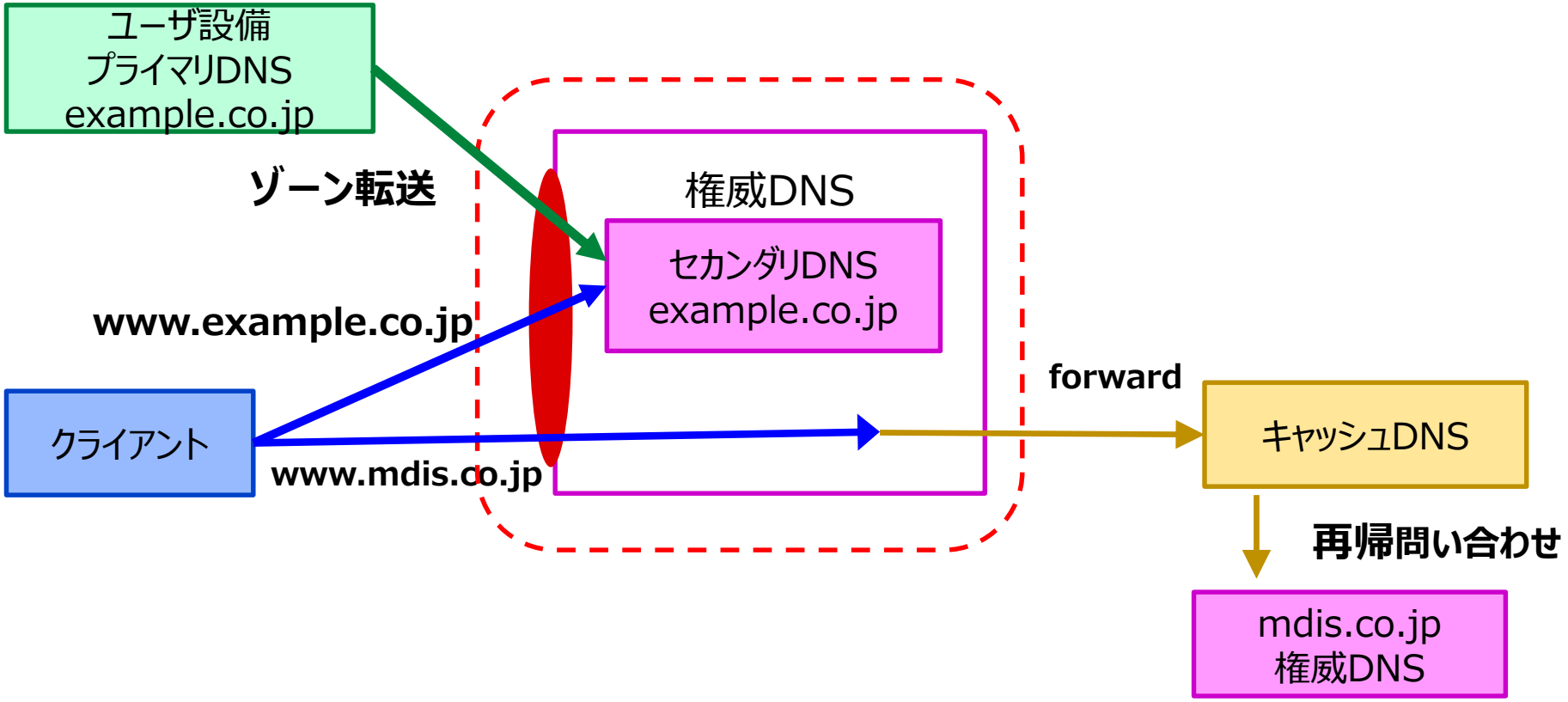
- RDフラグによる振り分けのリスク
  - クライアント、キャッシュDNS、法人プライマリDNSが期待する「RDフラグ」の設定が必須

- RDフラグによる振り分けは、**対向設備の実装に依存**する所が大きく、自システムだけではコントロール出来ないため、**検討段階で断念した**

5 – 2 – 1．回避方法（DNS機能による実現）

BIND(キャッシュ権威共用)と同じように振舞うためには・・・

- 自身で保持しているドメインは権威応答
- ドメインを**保持していなければ**、**forwardしてキャッシュDNSに成りすます**



5 – 2 – 2．回避方法（DNS機能による実現）

- この構成が取れるDNSソフトウェアは、(弊社の知る限り)OSSでは存在しない
- BINDと類似動作のため、置換えが可能
  - 有償DNSソフトウェアの利用が必要

6．まとめ

- キャッシュ権威共用のリスクを認識
  - 脆弱性の影響範囲が広がる
  - キャッシュ機能へのDDoSにより、同居する権威DNSのサービスにも影響する
  - 権威が応答できないことによりキャッシュポイズニングのリスクが高まる

- キャッシュ権威共用を分離
  - 1ドメインずつ移管することで、キャッシュ機能と権威機能を分離

キャッシュ権威を分離することで、DNSサーバのリスクは軽減される
BINDの脆弱性リスクは残る

6．まとめ

さらにBINDの脆弱性対処から開放されたい方は、DNSソフトウェアの切替も検討が必要

- BINDの独自処理があることを認識
  - 単純な機能確認だけでは不足
  - BINDの独自処理が動作しているケースがある。自社の使い方をよく確認
- BINDから切替可能な用途と単純置き換え出来ないケースを認識

用途	OSS　DNSソフトウェアでの切替
キャッシュDNS	可能
権威DNS	可能
キャッシュ権威共用	可能 ドメインを別の権威DNSに移管する作業が必要
キャッシュ＆ユーザ設備セカンダリ	不可 （有償DNSソフトウェアであれば実現できるものもある）

6．まとめ

本講演が皆様の安全なDNSサーバ運用の手助けになれば幸いです

ご注意

・本書の内容の一部又は全部を当社に断りなく、いかなる形でも
転載又は複製することは、固くお断りします。
・本文記載の社名、製品名、ロゴは各社の商標または登録商標です。