# 親の心子知らず？
# 委任にまつわる諸問題について考える
# ～ランチのおともにDNS～

2012年11月21日

Internet Week 2012 ランチセミナー

株式会社日本レジストリサービス（JPRS）
森下 泰宏・堀 五月

# 講師自己紹介

- 森下 泰宏（もりした やすひろ）
  - 日本レジストリサービス（JPRS）広報宣伝室
  - 主な業務内容：技術広報担当としてドメイン名・DNSに関する技術情報をわかりやすく伝える
  - 最近のキーワード：「重複をお許しください」
- 堀 五月（ほり さつき） イケメン 若者 初陣
  - 日本レジストリサービス（JPRS）システム部
  - 主な業務内容：システム・ネットワークエンジニアとしてJPドメイン名を支える
  - 最近のキーワード：「プレゼンテーション」

# 本日の内容

- 委任の概要と成り立ち
- 委任の特徴とそれに由来する注意点
- 最近のDNS関連トピックス
  - 幽霊ドメイン名脆弱性
  - 共用DNSサービスにおける危険性
  - ドメイン名の強制停止に伴う影響
- 本日のまとめ

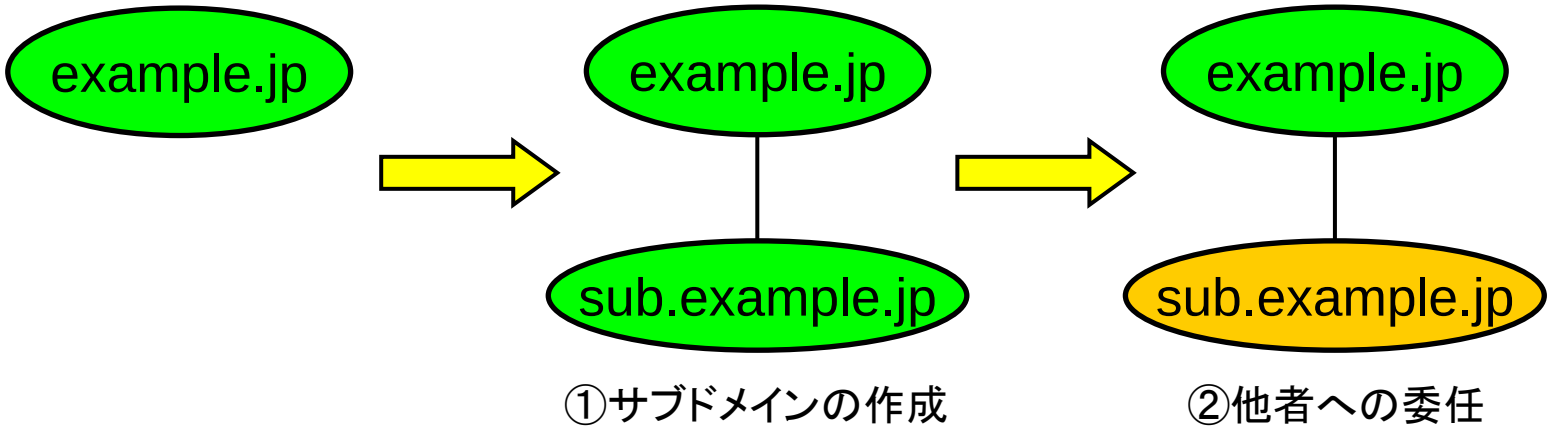
# 委任の概要と成り立ち

# 委任（delegation）とはそもそも何か？

- DNSの根幹部分の一つ
- ドメイン名管理の階層化を実現
- 2つのステップを経由

  ①自分が管理するドメイン名にサブドメインを作成

  ②そのサブドメインの管理権限を他者に委任



# 委任とゾーンの関係

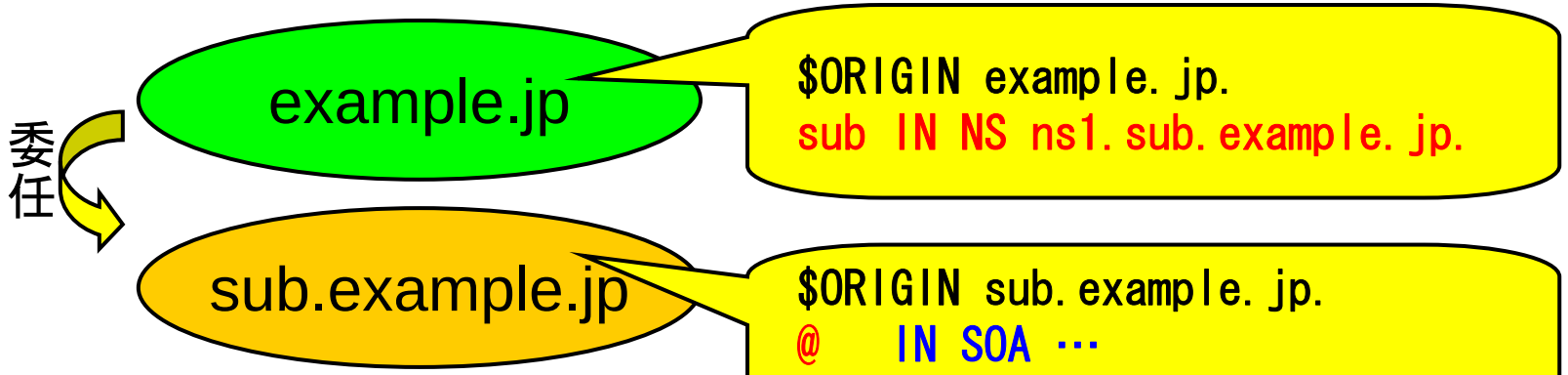
- 委任により、ドメイン名の管理が階層化される
  - 前ページの例では「example.jp」と「sub.example.jp」
- それぞれの管理範囲をゾーン（zone）と呼ぶ
  - example.jpゾーン
  - sub.example.jpゾーン
- つまり、委任はドメイン名を各ゾーンに階層化し、管理範囲を確定するためのしくみ
  - 委任によりゾーンが親と子に階層化される
  - 委任の境界点をゾーンカット（zone cut）と呼ぶ

# トリビア：サブドメインが存在しても必ず委任されているわけではない

- 委任は以下の2ステップにより実現
  ① サブドメインを作成
  ② サブドメインの管理権限を委任
- このため、サブドメインごとに委任が必ず存在しているわけではないことに注意が必要
  - ①は実行されているが、②は実行されていない
- 例：co.jpはjpのサブドメインだが委任されておらず、jpゾーンに属している
  - つまり、example.co.jpはco.jpゾーンからではなく、jpゾーンから委任される

# ゾーンカットに設定される リソースレコード

- ゾーンカットの親側：NSレコードのみ
- ゾーンカットの子側：SOAレコードとNSレコード
- SOAレコード：ゾーンの起点を示し、子側のみで設定
- NSレコード：ネームサーバー情報を示し、双方で設定
- 親と子のNSレコードは役割が異なる（次ページで説明）



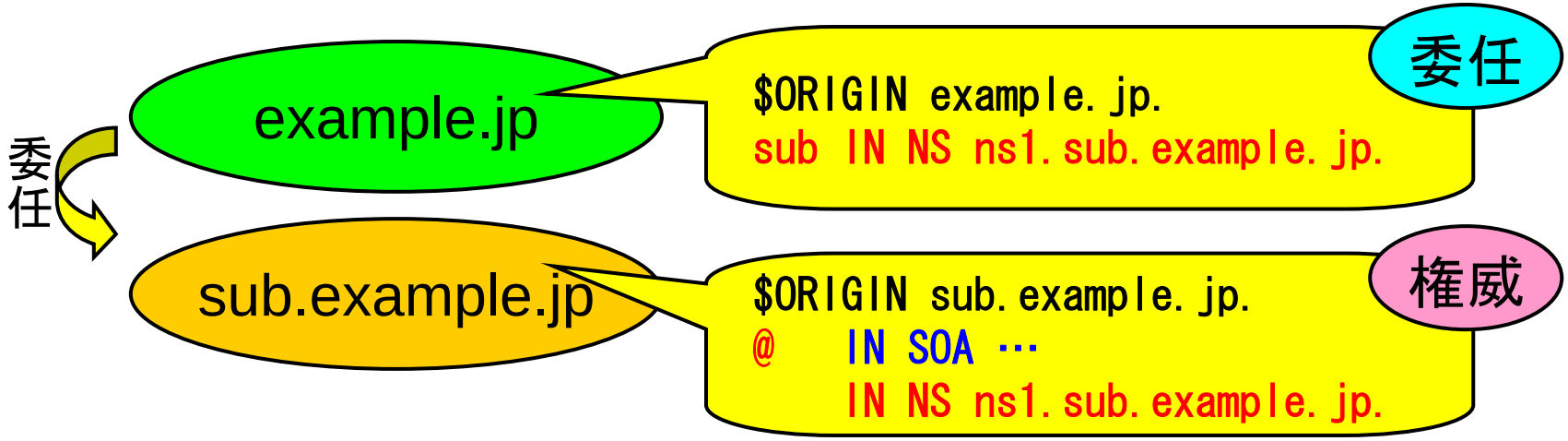

※備考：DNSSECでは親側でのみ設定される**DSレコード**が存在する（今回は解説しません）

# 委任におけるNSレコードの役割

- 親のNSが委任を、子のNSが権威を示す
- 親のNSの意味（委任情報の提示）
  - 「私はそのゾーンをNSで指定した子に委任しています」
- 子のNSの意味（権威情報の表明）
  - 「私はそのゾーンの権威を持っています」
- 委任の成立には上記の双方が必要
- DNSの仕様では子のNSが権威を持つ（親のNSよりも優先）

| レコード | SOA | NS |
|---|---|---|
| 親側 | | 委任の提示 |
| 子側 | 起点の提示 | 権威の表明 |

図：設定されるレコードとその役割



# 委任の特徴と
# それに由来する注意点

# 本日紹介する7つの特徴

- 親の立場からみた特徴（2つ）
  - ① 子の状況にかかわらず一方的に委任できる
  - ② 子の状況が変化しても検知しない
- 子の立場からみた特徴（2つ）
  - ③ 委任の有無に関わらず権威を自称できる
  - ④ どの親からどんな形で委任を受けているかの情報を持たない
- 複雑になってしまった特徴（3つ）
  - ⑤ NSレコードで名前を指定
  - ⑥ 委任情報と権威情報を同種のリソースレコードで指定
  - ⑦ 権威の根拠が権威のない情報に依拠

# …その前に

- 本日紹介する7つの特徴は、DNSの技術的観点（DNSプロトコル）からみたものです
- ここではDNSにおける委任の本質を把握するため、注意点を意図的に強調した形で解説します
- 実際には多くの場面において運用でカバーすることにより、特徴に由来する不具合の発現を抑制しています
- しかし、それにより注意点がなくなるわけではありません
  - 注意点を知ったうえできちんと運用することが重要です

# 特徴①：子の状況にかかわらず一方的に委任できる

- 子の準備ができていなくても委任できる
  - 権威を持つ応答を返さない ⇒ Lame delegation
  - 正しい委任が成立しない
- 子のNSが親のものと異なっていても委任できる
  - 必ずしも違反ではない（引越し途中など）
  - ただし、双方のNSで示されたすべての権威DNSサーバーが権威を持つ同内容の応答を返す必要あり
- 一方的に委任できるということは、一方的に委任を解除・変更できるということでもある
  - 幽霊ドメイン名
  - FBIによるMegaupload.comの強制閉鎖

# 特徴②：子の状況が変化しても検知しない

- 委任成立後に子の状況が変化しても、親はそれを検知しない
  - 子が権威ある応答を返さなくなった
  - 子のゾーン情報が削除された
  - 子のNSが変更された、など
- NSが外部名で指定されている場合、依存関係に伴う別のリスクが存在しうる（特徴⑤で解説）

# 特徴③：委任の有無に関わらず権威を自称できる

- 権威情報（SOA、NS）は子で設定・表明する
- そのため、子は親からの委任の有無に関わらず任意のゾーンに対する権威を自称できる
- 「オレオレ子供」
  - 共用DNSサービスにおける「親子同居問題」（後述）
- ドメイン名パーキング用の権威DNSサーバー
  - 任意のゾーンに対し権威を持つ応答を返す
- この特徴は利点にもなりうる
  - Split DNS
  - その昔の「ネームサーバー3系列」

# 特徴④:どの親からどんな形で委任を受けているかの情報を持たない

- DNSの委任は親からのみの一方向
- 子は自分の親の情報を持たない
  - 「親の心子知らず」?
- 例えば子のゾーンがexample.co.jpである場合、以下のいずれの場合もあり得る(そして、子はどの状況なのかの情報を持たない)
  - ルート、jp、co.jpのうち、いずれか一つから委任されている
  - いずれからも委任されていない

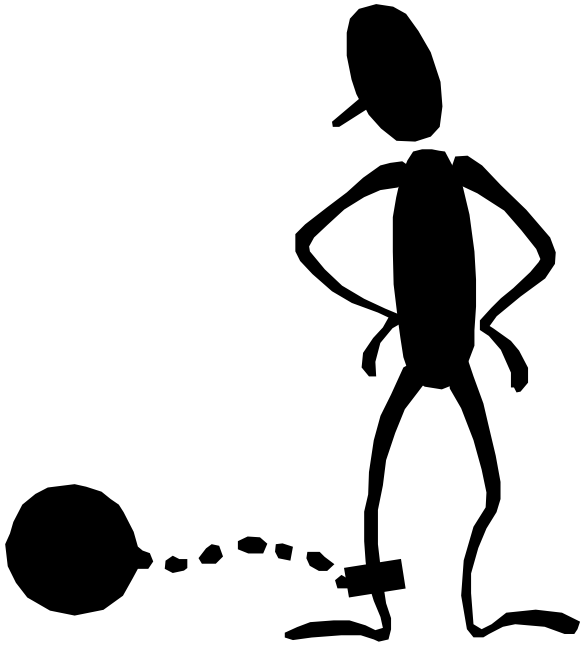
# 特徴④：どの親からどんな形で委任を受けているかの情報を持たない

- この特徴は、逆引きDNSの世界的な整理の際に利用された（ERXプロジェクト）
  - RIR間における（途中の）権威DNSサーバーの整理
  - 末端のPTRレコードに影響を及ぼすことなく実施
- jpにおけるjp⇒{属性,都道府県}.jpの委任解除
  - JPRSでは「ゾーンマージ」と呼称
  - 現在、JPドメイン名はすべてjpから委任されている
    - co.jpやtokyo.jpなどのゾーンは存在・経由しない

つまり、co.jpやtokyo.jpなどのNSレコードは存在しないのが正しい

# ここからの3つ（特徴⑤～⑦）は、、、

- 設計・仕様により複雑になってしまった特徴
- うまく設計すれば避けられたかもしれない
- DNSが生まれながらに背負ってしまった「業」



# 特徴⑤：NSレコードで名前を指定

- 名前の委任先を名前で指定
- これにより委任のしくみが不当に複雑化
  - 内部名：グルーレコード（とそのチェック）が別途必要
  - 外部名：名前の依存関係が親子関係以外にも波及
- トラブルや脆弱性を誘発する弱点となった
  - 他のドメイン名で発生した障害の巻き添え
  - いわゆるVISA.CO.JP問題（ドメイン名ハイジャック）
- キャッシュポイズニングの標的ともなった
  - Kashpureff型、Kaminsky型

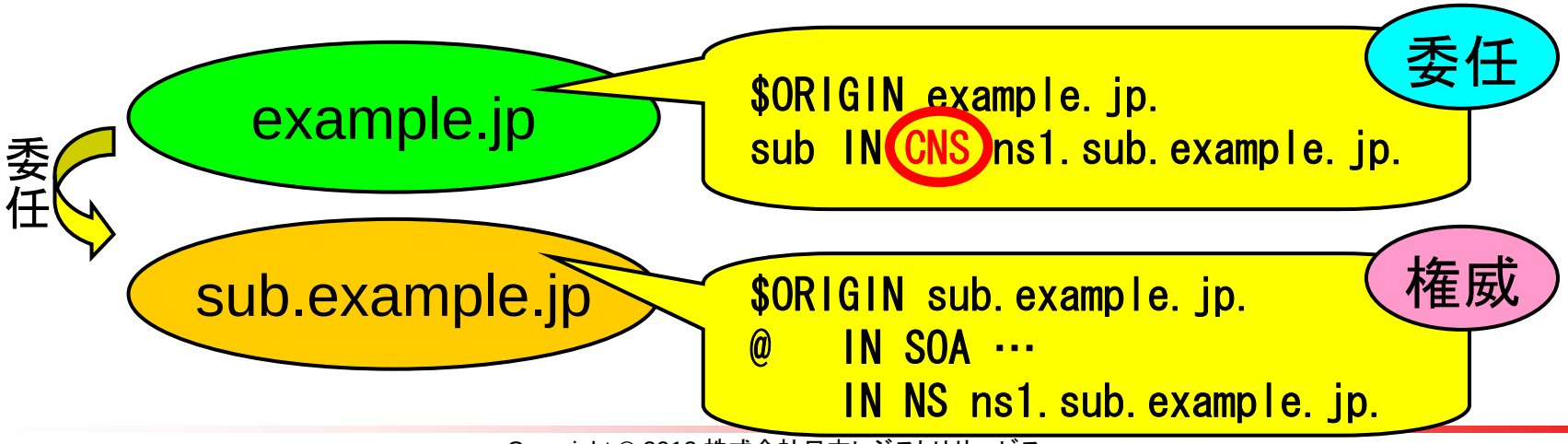
# 特徴⑤：NSレコードで名前を指定

- 名前の委任先を名前で指定するという設計は
  そもそも不自然
  - かつ、外部名も指定可能
- DNS最大の禍根の一つであると言える
  - この設計の採用には理由があった（今回は割愛）
- こんな感じにすればよかったのかもしれない
  - 名前ではなくIPアドレスで指定

```
sub.example.jp.  IN NSIP     192.0.2.1
sub.example.jp.  IN NSIP6    2001:db8::1
```

# 特徴⑥：委任情報と権威情報を同種のリソースレコードで指定

- 役割が異なるものを同種のリソースレコードで指定
  - 親子ともにNSレコードで指定
- 誤解や混乱を招きやすい
  - 浸透問題や幽霊ドメイン名脆弱性につながる弱点
- こんな感じにすればよかったのかもしれない
  - 親のNSを子のNSと別種のリソースレコード（CNS）で指定



# 特徴⑦：権威の根拠が権威のない情報に依拠

- 子のNSが親のNSよりも優先的に取り扱われる
- ただし、これが成立するのは子が子である間だけ
  - 親からの委任がなければ子のNSはそもそも無効
- つまりDNSでは、権威の根拠（子のNS）が権威を持たない情報（親のNS）に依拠していることになる
  - DNSにおける構造上の弱点の一つ
  - 実装ミスを誘発しやすい（例：幽霊ドメイン名）
- DNSSECではDSレコードを新規導入し、親子双方の情報が権威を持つ形で設計
  - ただし副作用も発生（より緊密な親子の絆が必要）

# 最近のDNS関連トピックス

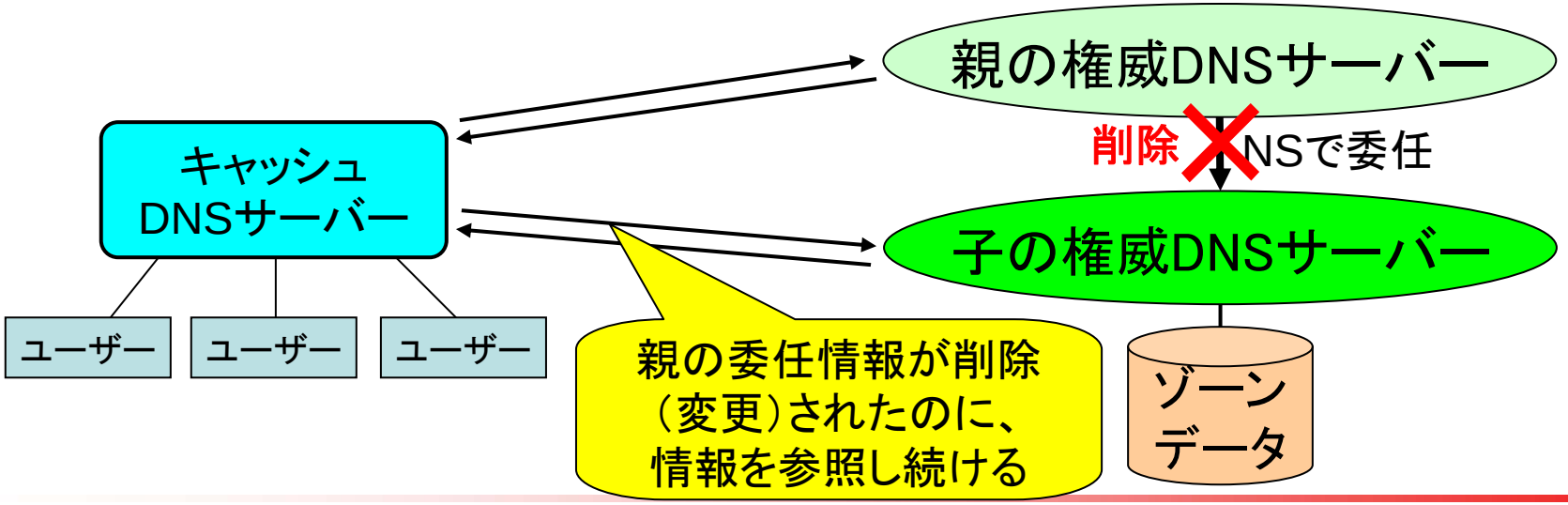
# 最近のDNS関連トピックス

- 2012年に発生した3つのトピックス
  1. 幽霊ドメイン名脆弱性
  2. 共用DNSサービスにおける危険性
  3. ドメイン名の強制停止に伴う影響
- 上記のいずれにも、DNSの委任の特徴と注意点が深く関係している

以降、それぞれの内容について
順を追って紹介します

# 1. 幽霊ドメイン名脆弱性

- 親における委任情報（NSレコード）の削除・変更後も長期にわたり、子ではなくなった子の情報を参照させ続けるように仕向けることができる
- 消える（見えなくなる）はずのものが残り続ける
- 「子のNSが有効なのは親のNSが有効な間だけ」という仕様に関する実装上の不備を突いたもの



# 2. 共用DNSサービスにおける危険性

- サービス事業者が顧客に提供するDNSサービス・システムにおいて、

① 複数の顧客のドメイン名（ゾーン）を、同一の権威DNSサーバーで共用しており、

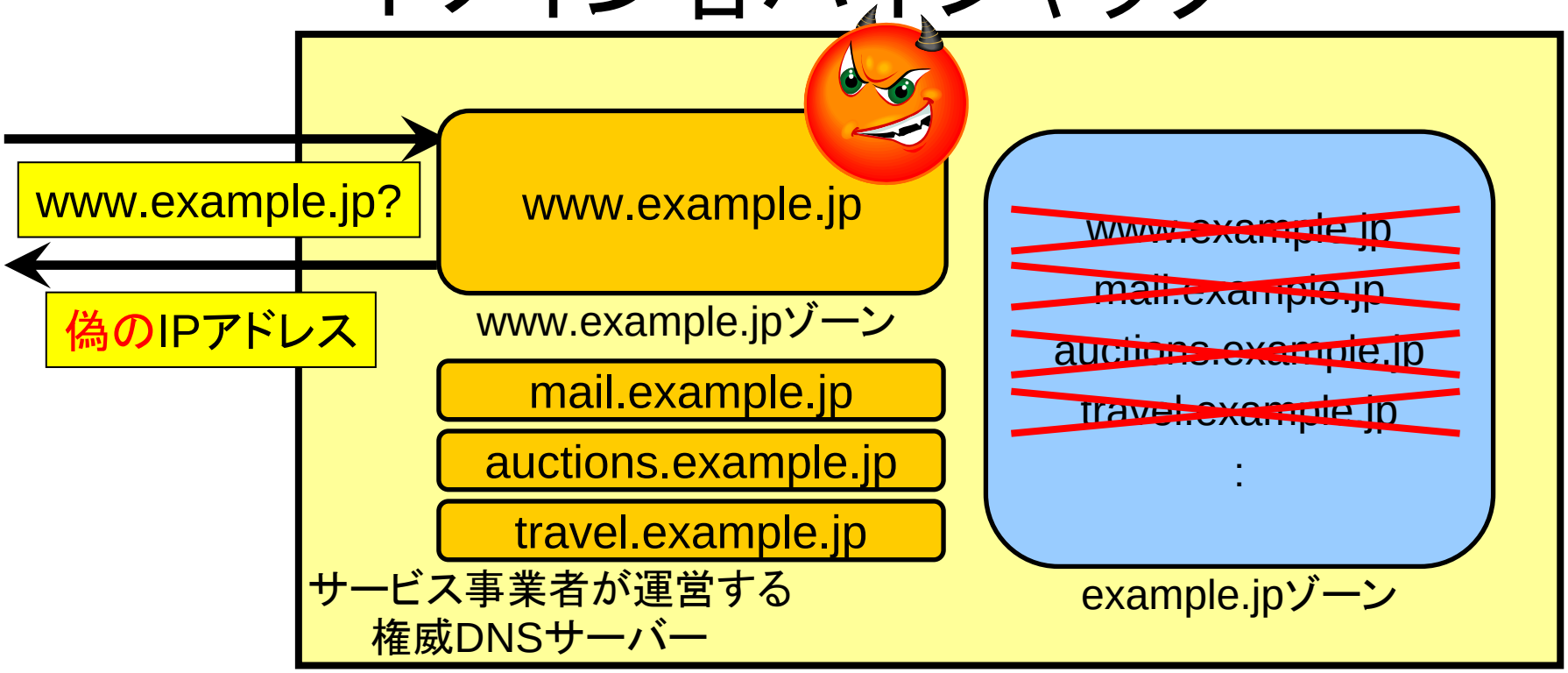
② かつ、顧客によるゾーンの新規作成を許可しており、

③ かつ、サービス事業者のシステムにおいて、顧客が作成するゾーンのチェック・制限が不十分である

…場合に考えうる危険性

ここでは2つの事例を紹介します（他にもあり得ます）

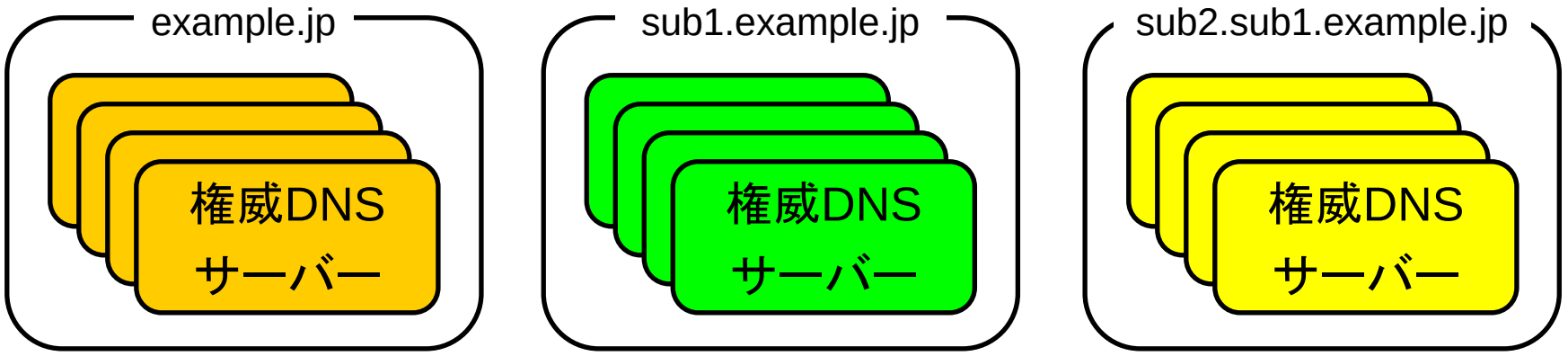
# 事例1:「オレオレ子供」による ドメイン名ハイジャック



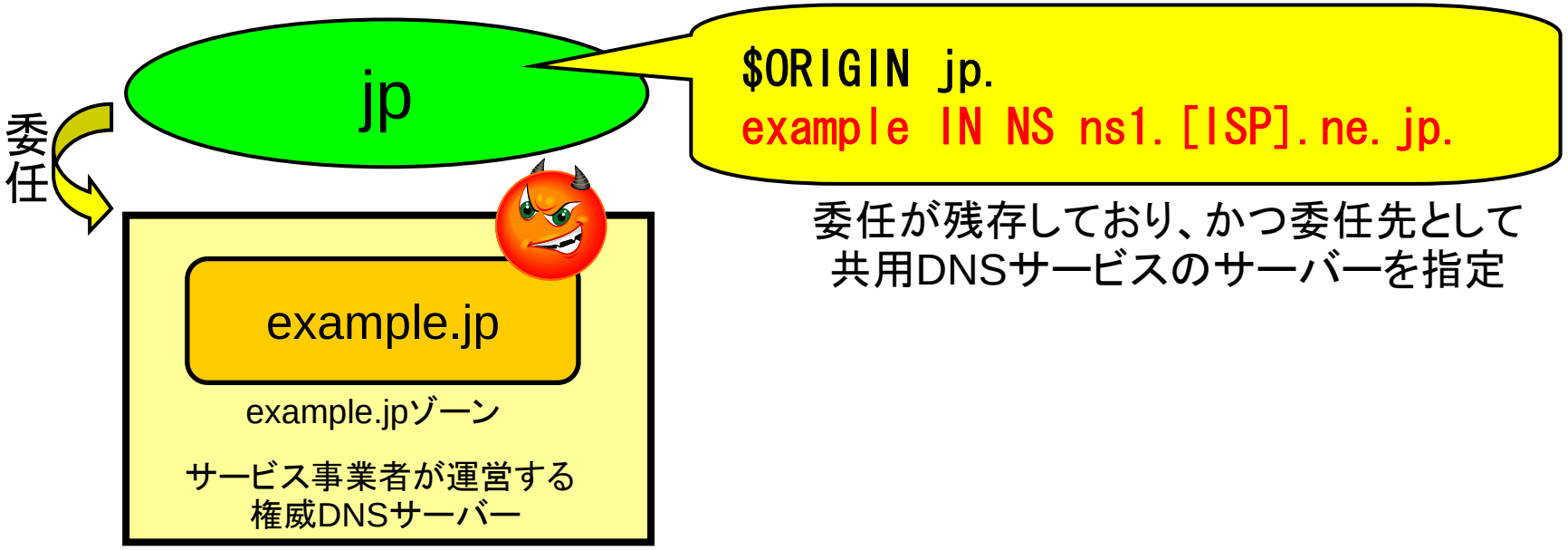

- 運用中のドメイン名のサブドメインを同一サーバー内に作成
- 多くのDNS実装ではより階層の深いゾーンのデータのみを参照
- これにより「*.example.jp」の名前をすべてハイジャック可能
  - ハイジャックするサブドメインの分だけゾーンを作成すればよい

# 参考：ある大手DNSサービスにおける対策

- サブドメイン／スーパードメインの関係にあるゾーンは、別のIPアドレスを持つサーバー上に作成されるように作られている模様
  - 前述の条件①（親子（先祖—子孫）同居）を回避



# 事例2:使用休止ドメイン名の不正使用



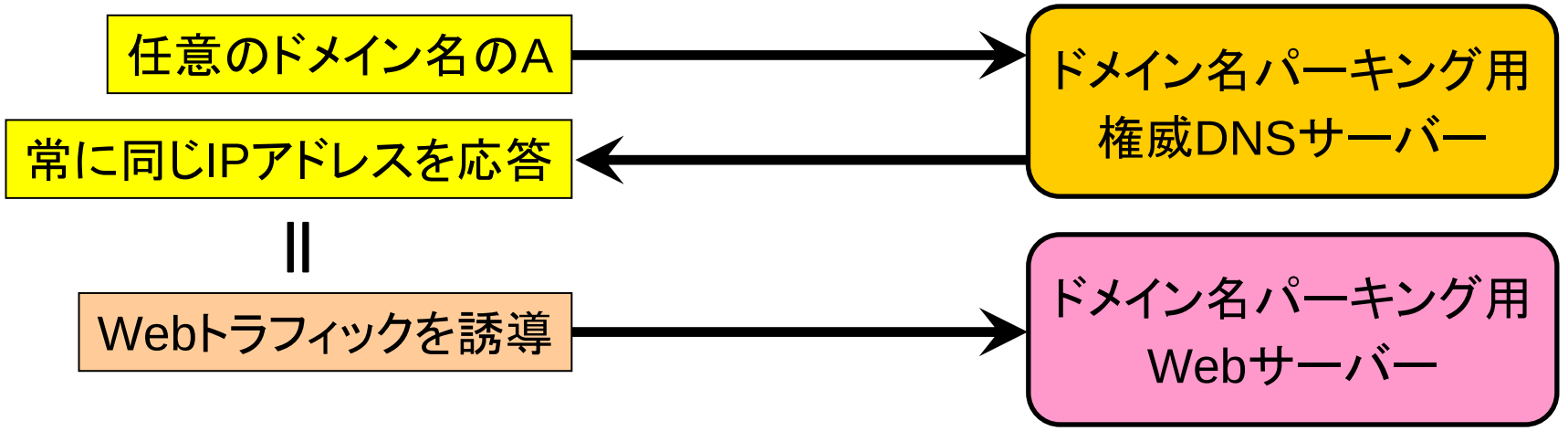

- 前提条件:レジストリの権威DNSサーバー上の委任のみが残存、かつ共用DNSサービスのサーバーを指定している
  - 例:当該ドメイン名のオーナーが他人によるゾーン作成はできないはずと判断、ゾーン情報のみを消去し委任をそのままにしていた場合
- この状態で委任先ゾーンを勝手に作成し、ドメイン名を不正使用

# 3. ドメイン名の強制停止に伴う影響 ～強制停止の概要～

- ドメイン名の強制停止が起こりうる例
  - 司法当局などによる強制執行や差し押え
  - 顧客のサービス約款違反
  - ドメイン名維持料の不払い・滞納、など
- 委任情報の削除ではなく強制変更が主流
  - 委任情報（親のNS）を強制変更、トラフィックを誘導
  - 削除した場合名前解決エラーとなり、Webユーザーへの周知（周知用サイトの表示）ができなくなる
- つまり、技術的にはドメイン名ハイジャックと同等

# ドメイン名の強制停止に伴う影響 ～パーキング用権威DNSサーバー～

- NS変更先として事前準備済の専用サーバーを使用
  - ドメイン名パーキング用の権威DNSサーバーがよく使われる
- 任意のドメイン名のAレコードの問い合わせに対し、常に同一のIPアドレスを権威を持つ応答として返す
- パーキング用Webサーバーにwebトラフィックを誘導



# ドメイン名の強制停止に伴う影響
# ～技術的考察が必要な内容～

## ① 常に同一のIPアドレスを返す権威DNSサーバー

- 大手レジストラを中心に広く使われている
- 権威DNSサーバーの設定変更が必要なくなる
  - 委任情報の強制変更のみで強制停止が可能になる
- こうしたサーバーが他のドメイン名に副作用を及ぼさないか、技術的考察が必要になる

# ドメイン名の強制停止に伴う影響 ～技術的考察が必要な内容～

## ② DNS運用上の問題

- 技術的には強制停止ではなく強制変更であることから、設定内容によっては元の状態への切り戻しに時間を要する可能性がある
  - NS／AレコードのTTL設定値が影響を及ぼす
  - 古いバージョンのBIND 9では、いわゆる浸透問題や幽霊ドメイン名脆弱性が発生しうる
- 他のゾーンのNSで指定されたドメイン名が強制停止の対象となった場合、巻き添えが発生する
  - 外部名をNSに指定する際のリスクの一つ

# 本日のまとめ

# 本日のまとめ（その１）

## ■委任の概要と成り立ち

- 委任はドメイン名を各ゾーンに階層化し、管理範囲を確定するためのしくみ
- 委任によりゾーンが親と子に階層化される
- サブドメインがあっても委任されているとは限らない
- ゾーンの起点はSOAレコードで示される
- NSレコードは親と子で果たす役割が異なっている
- 親のNSが委任を、子のNSが権威を示す

# 本日のまとめ（その2）

## ■委任の特徴とそれに由来する注意点

- 親の立場からみた特徴
  - 子の状況にかかわらず一方的に委任できる
  - 子の状況が変化しても検知しない
- 子の立場からみた特徴
  - 委任の有無に関わらず権威を自称できる
  - どの親からどんな形で委任を受けているかの情報を持たない
- 複雑になってしまった委任
  - NSレコードで名前を指定
  - 委任情報と権威情報を同種のリソースレコードで指定
  - 権威の根拠が権威のない情報に依拠

# 本日のまとめ（その3）

## ■最近のDNS関連トピックス

- 幽霊ドメイン名脆弱性
  - 親子NSの仕様に関する実装上の不備を突いたもの
- 共用DNSサービスにおける危険性
  - 事例1：「オレオレ子供」によるドメイン名ハイジャック
  - 事例2：使用休止ドメイン名の不正使用
- ドメイン名の強制停止に伴う影響
  - 強制停止の概要
  - ドメイン名パーキング用権威DNSサーバー
  - 技術的考察が必要な内容

# Q&A