DNS入門基本編

2020年11月26日

Internet Week 2020 DNS DAY

株式会社日本レジストリサービス(JPRS)

池田和樹

1. IPアドレスとドメイン名

IPアドレスとドメイン名

IPアドレス

192.0.2.1
2001:db8::1

対応

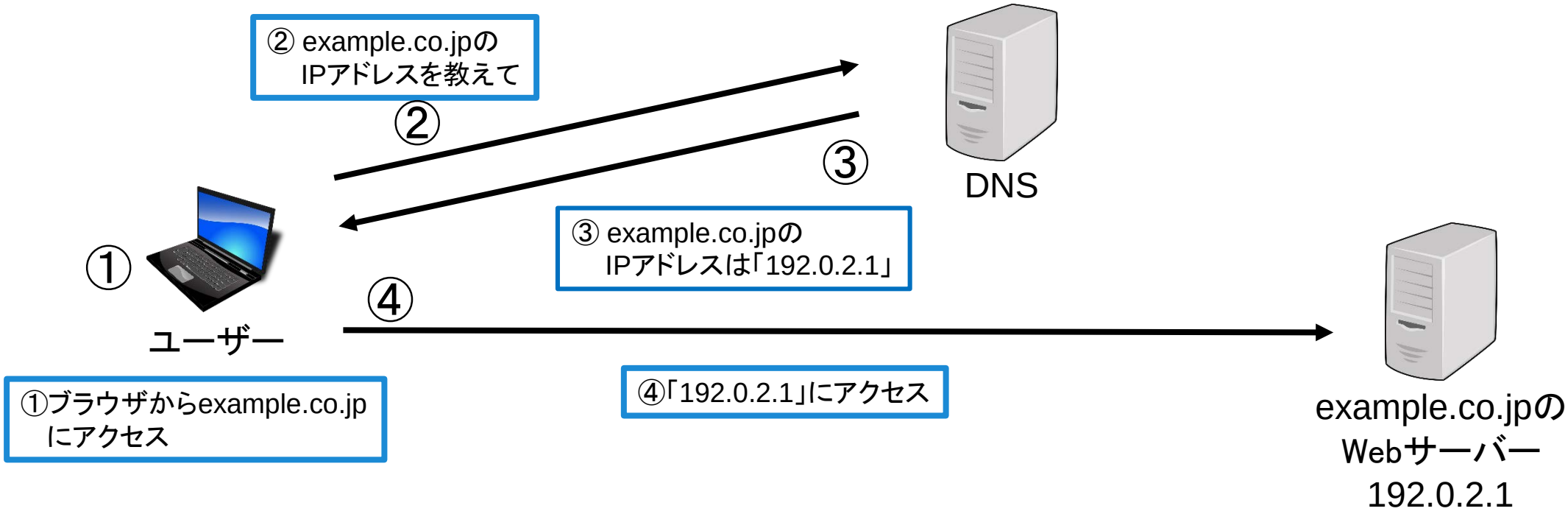
ドメイン名

example.co.jp

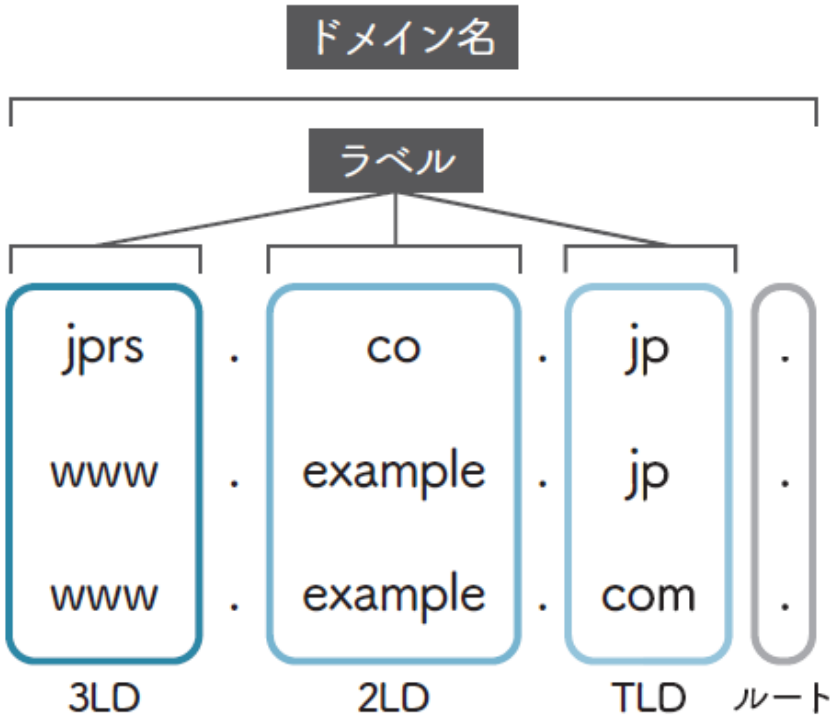
example.co.jp のサーバー

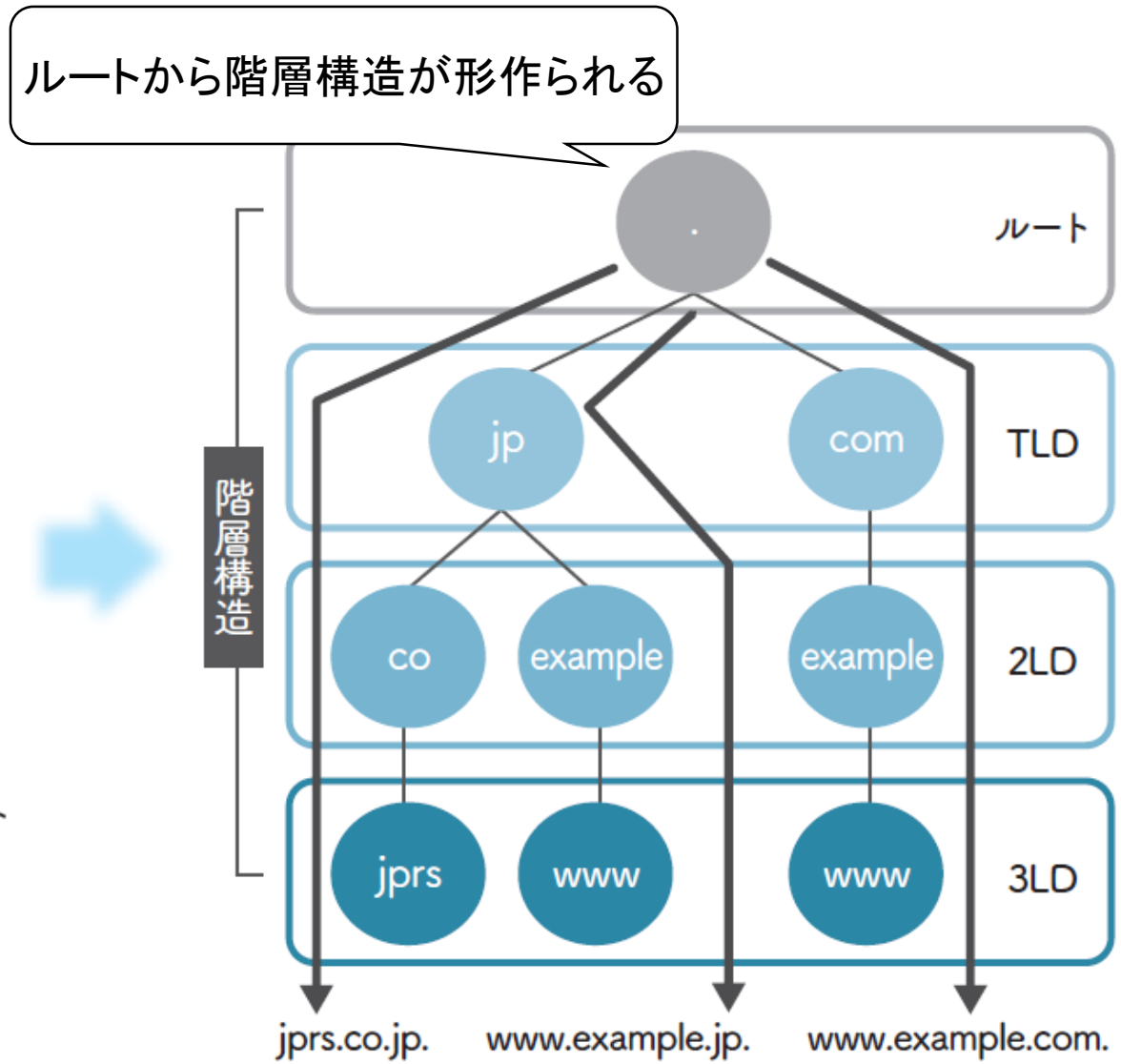
DNS(Domain Name System)

- DNS
  - インターネットに接続されたコンピューターの情報（ドメイン名とIPアドレスの対応など）を得るための仕組み



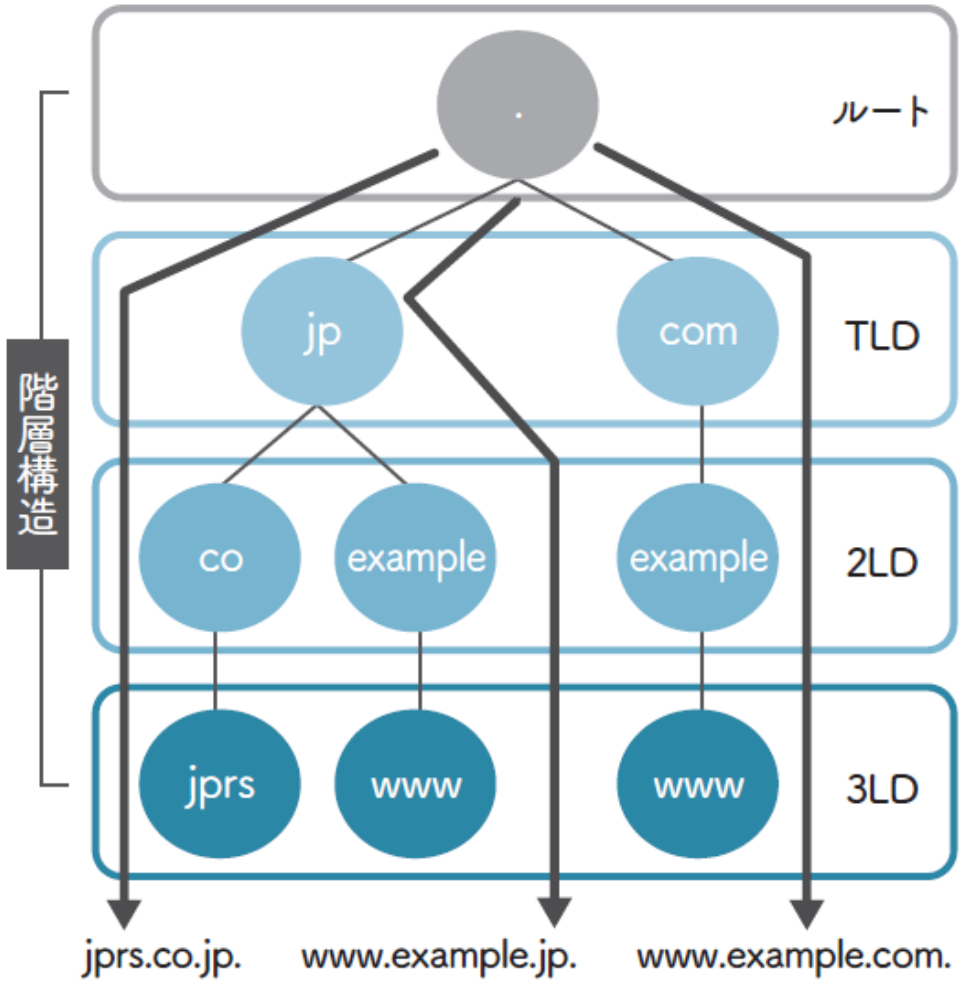
ドメイン名の構成

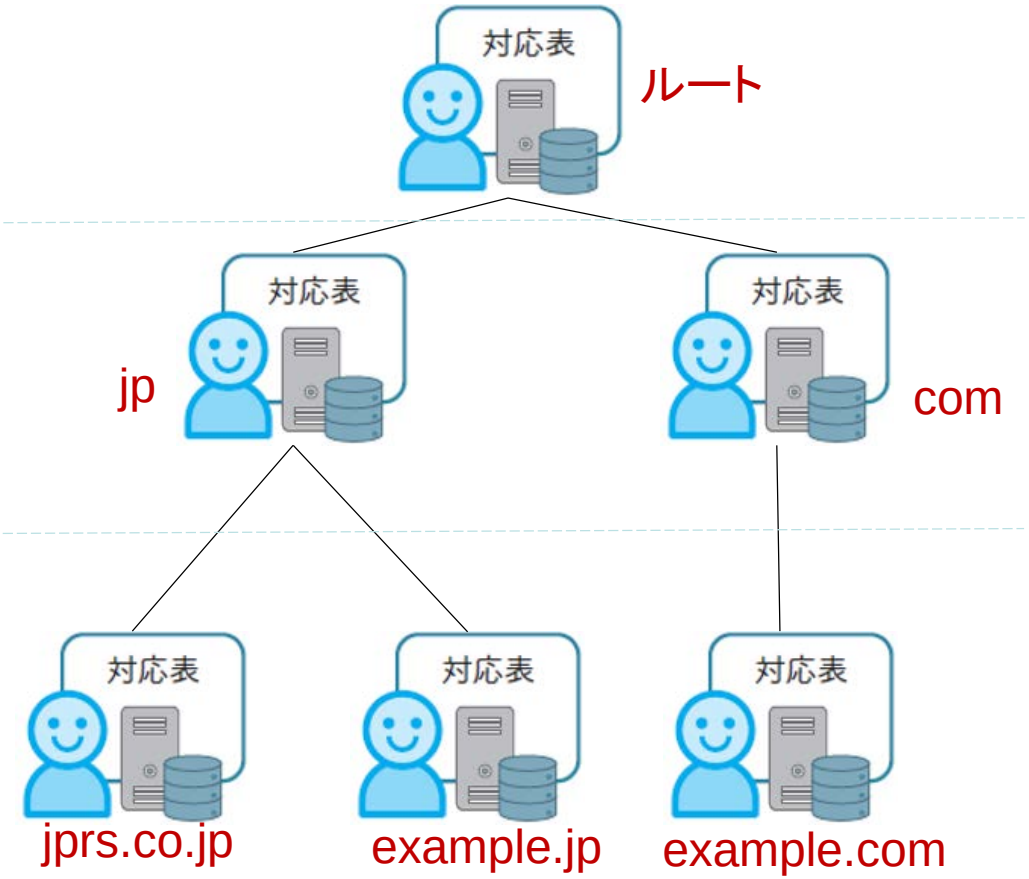




ドメイン名とDNS

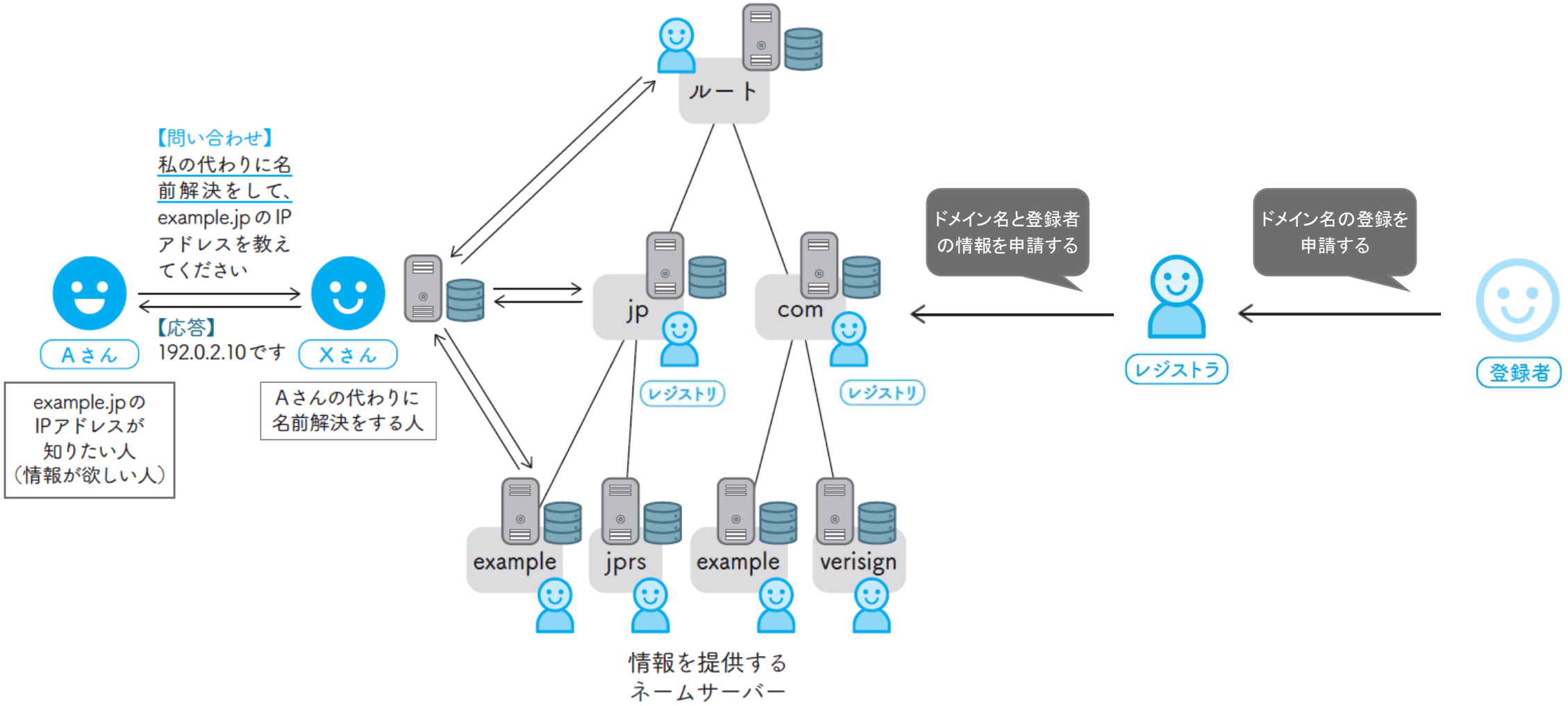
ドメイン名の階層構造が
反映される





2. レジストリとレジストラ

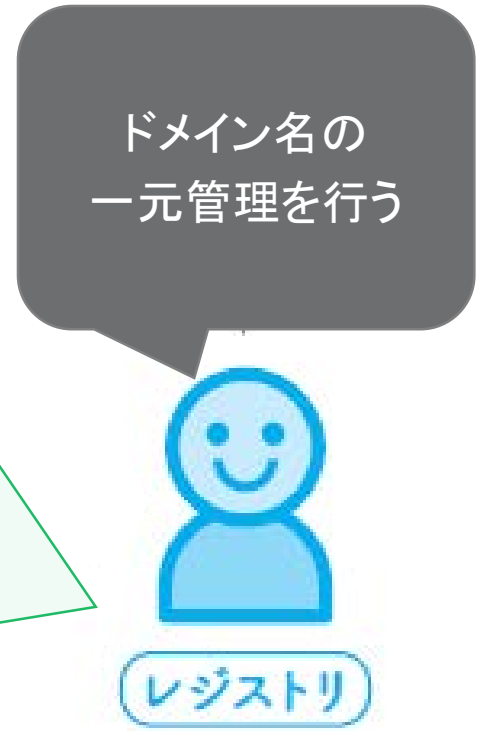
ドメイン名の登録管理とDNSの構成要素の関係



レジストリとレジストラ

レジストリの役割

■レジストリデータベースの運用管理
■ポリシーに基づいた登録規則の策定
■登録申請の受け付け
■Whoisサービスの提供
■ネームサーバーの運用
■情報発信・教育啓発活動



レジストリ（ccTLDとgTLD）

ccTLD: 国や地域ごとに割り当てられる

JPRS JAPAN REGISTRY SERVICES	.jp
CNNIC 中国互联网络信息中心 CHINA INTERNET NETWORK INFORMATION CENTER	.cn
NOMINET	.uk

..etc

2文字

gTLD: 国や地域によらない

VERISIGN	.com .net
neustar	.biz

..etc

3文字以上

一元管理を行う ＝ レジストリは**1TLD1組織**

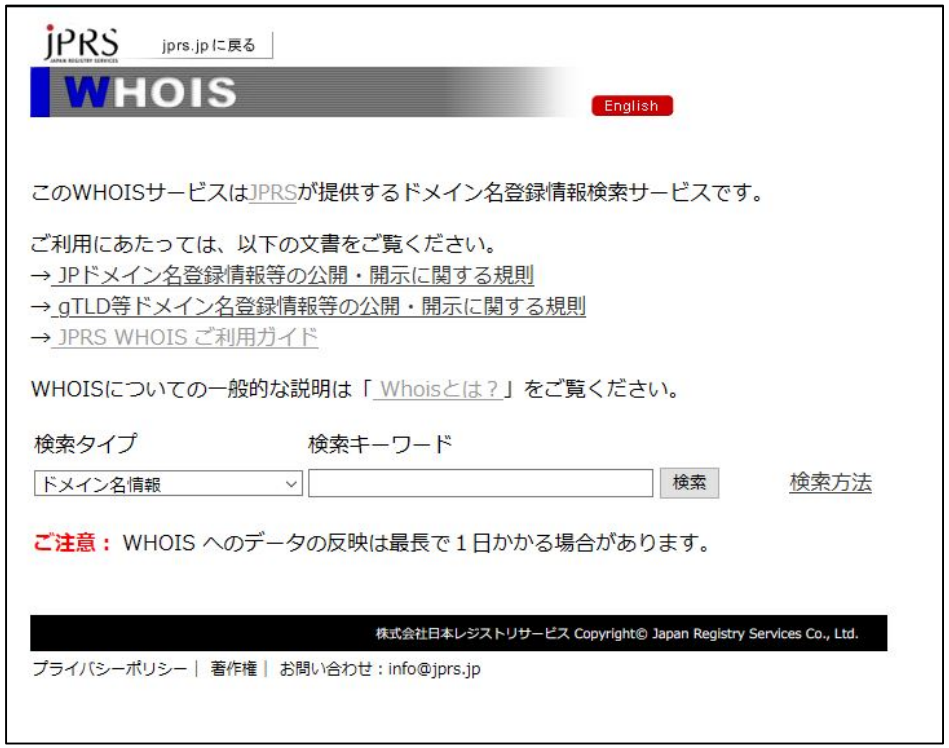
レジストラの役割

- 登録者からの登録申請の受け付け
- レジストリデータベースへの登録依頼
- Whoisサービスの提供
- 登録者情報の管理

レジストラは、1TLDに複数存在可能

Whoisサービス

- ドメイン名やIPアドレスの登録者などに関する情報をインターネットに公開し、利用者が参照できるようにするサービス
  - 目的
    - 技術的な問題が発生した際の、当事者間における連絡先情報の確保
    - ドメイン名の登録状況の確認
    - セキュリティインシデントやドメイン名と商標の関係など、技術的な問題以外のトラブルの解決



JPRS WHOIS | https://whois.jprs.jp

登録者の役割

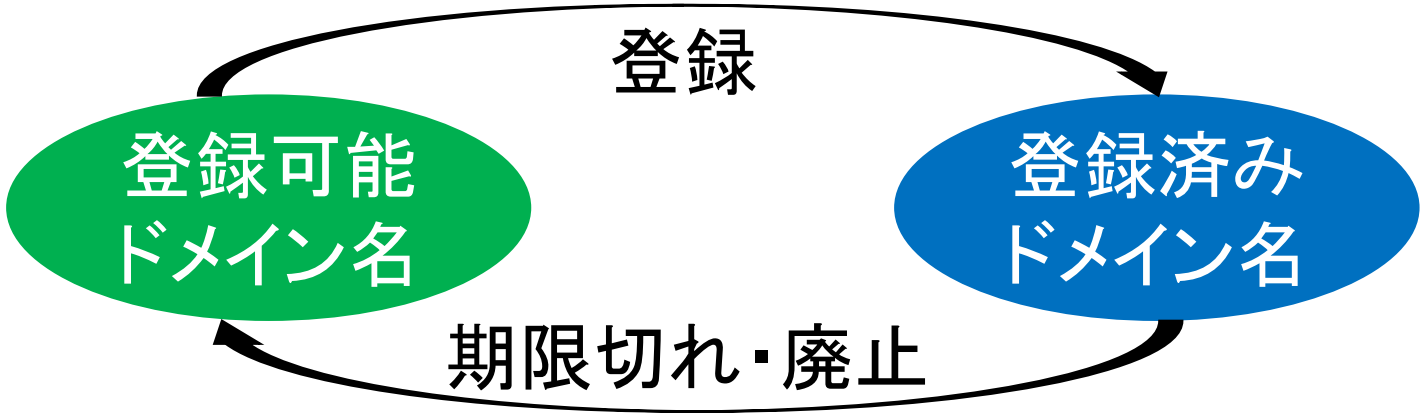
ドメイン名の
登録を
申請する

- 登録するドメイン名の選定
- 申請する事業者の選定
- 登録に必要な情報の提出

3. ドメイン名の管理における注意点

ドメイン名のライフサイクル

- ドメイン名には有効期限がある
- 有効期限が過ぎたドメイン名は一定期間後に廃止され、誰でも登録できるようになる



期限切れ・廃止されたドメイン名の行方

- 廃止されたドメイン名をドロップキャッチされ、再利用されることがある

ドロップキャッチ

期限切れ・廃止したドメイン名を、登録が可能になる瞬間を狙って素早く登録しようとする行為のこと

<u>アクセス数が多いドメイン名だった場合、
SEO的に有利であるため、再利用されることが多い</u>

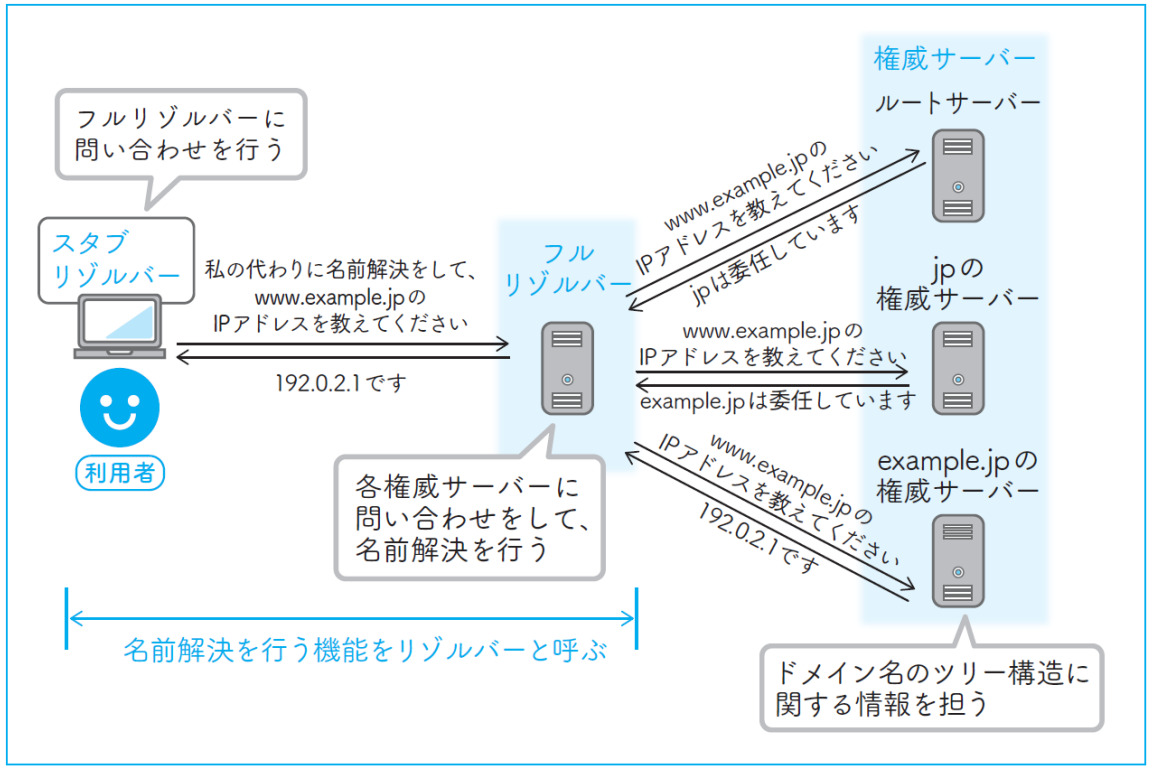
ドメイン名の廃止に関する注意

- 廃止されたドメイン名を第三者が登録しても、商標の侵害等でDRP(ドメイン名紛争処理方針)に該当する事由がない限り、登録・使用を差し止めすることはできない

- 参考：ドメイン名の廃止に関する注意
  - https://jprs.jp/registration/suspended/

4. 権威サーバー入門

DNSの構成要素



スタブリゾルバー

フルリゾルバーに名前解決を依頼する

フルリゾルバー

ルートから順に階層構造をたどり、名前解決を実行する
権威サーバーから得られた情報をしばらく保持する
→キャッシュ

権威サーバー

委任されたゾーンの名前情報（ゾーンデータ）と委任情報を管理する

権威サーバーの役割

- 委任されたゾーン情報の管理
  - 自身が管理している情報（.jpであれば、.jpに関する情報と委任情報）のみを返す
  - あるドメイン名の全ての権威サーバーが止まると、そのドメイン名の名前解決ができなくなる

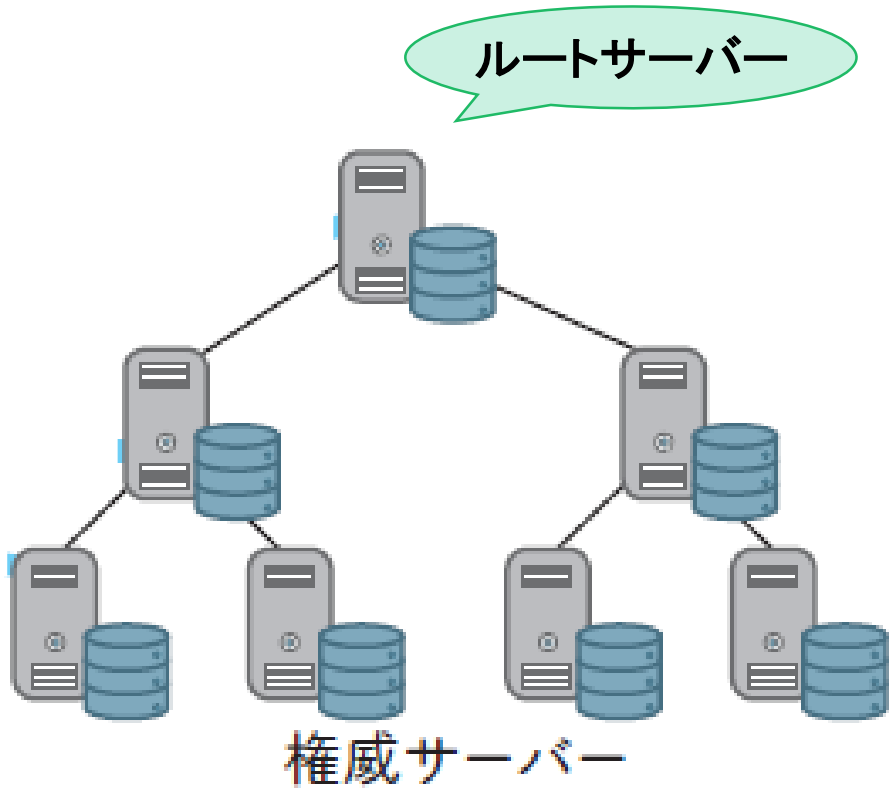
そのドメイン名を使用している全てのインターネットサービスが利用できなくなる

応答する情報・保持する形式

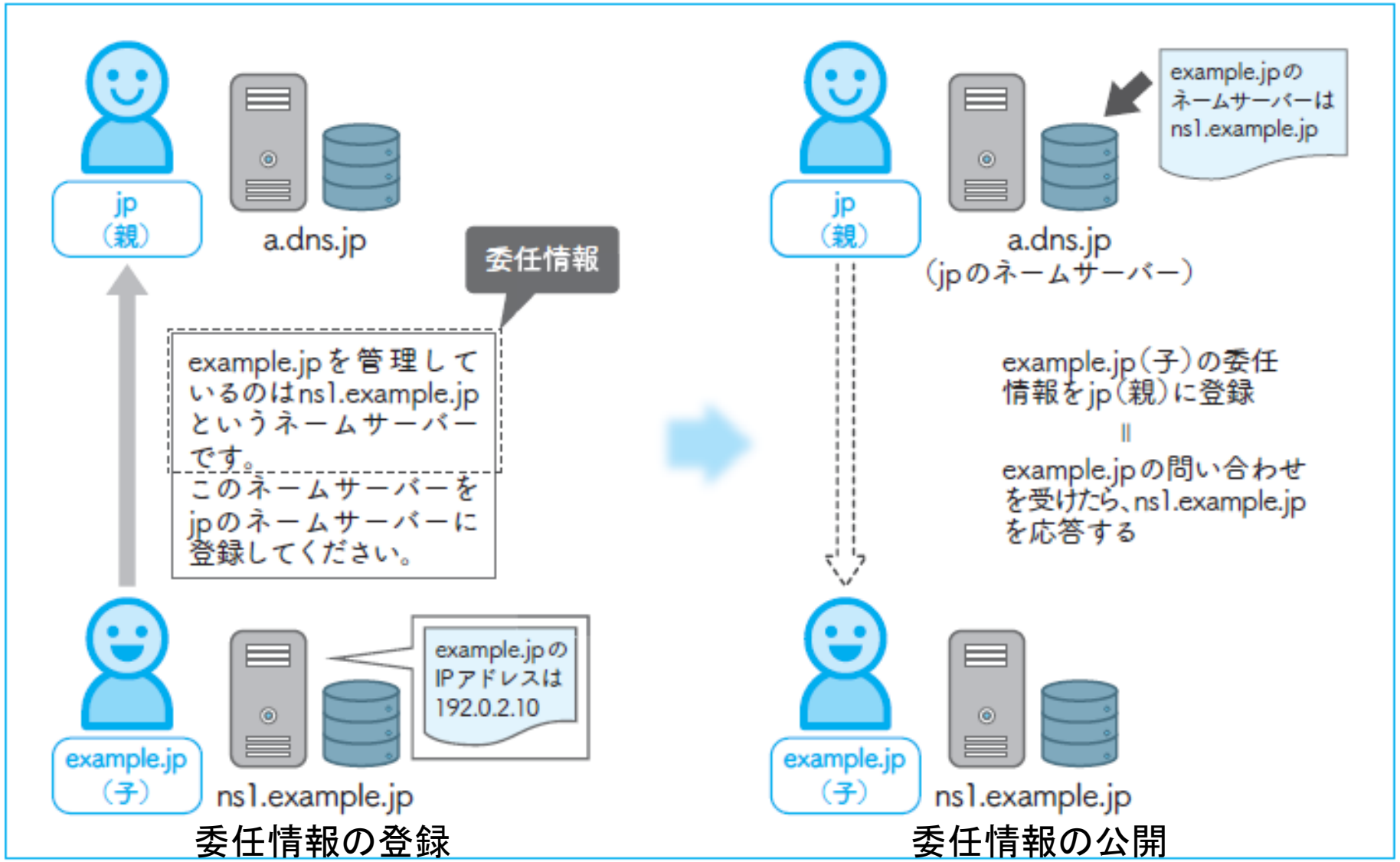
- 応答する情報
  - 自分が管理権限（ゾーンの権威）を持つ情報
  - 委任情報

- 保持する形式
  - 問い合わせ元から指定された「名前（ドメイン名）」と「種類（タイプ）」の情報を元に、目的の情報を探す
  - リソースレコードの形で情報を保持する

- 階層構造の頂点
  - ルートゾーンの権威サーバーを特に、ルートサーバーと呼ぶ

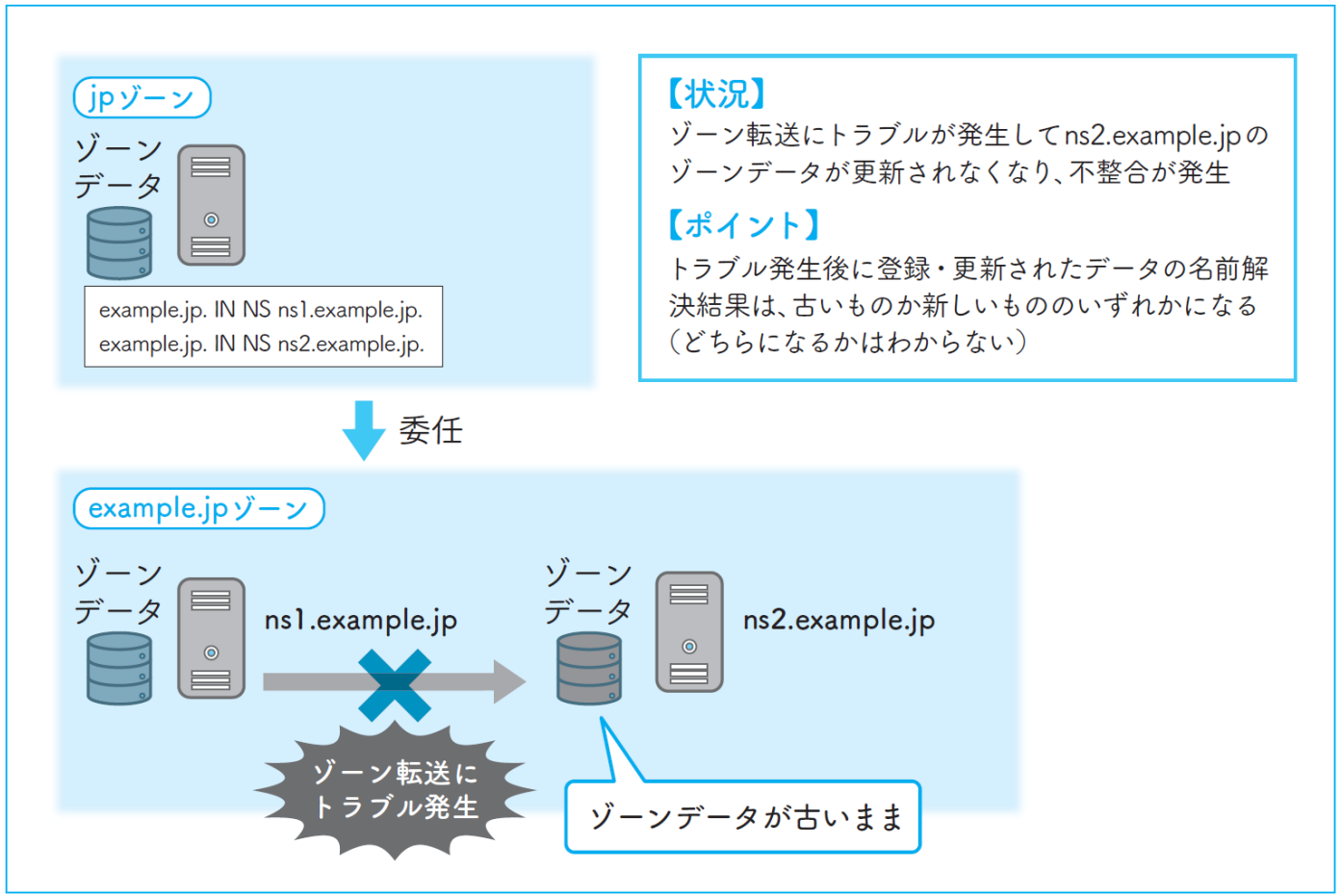


委任情報の内容



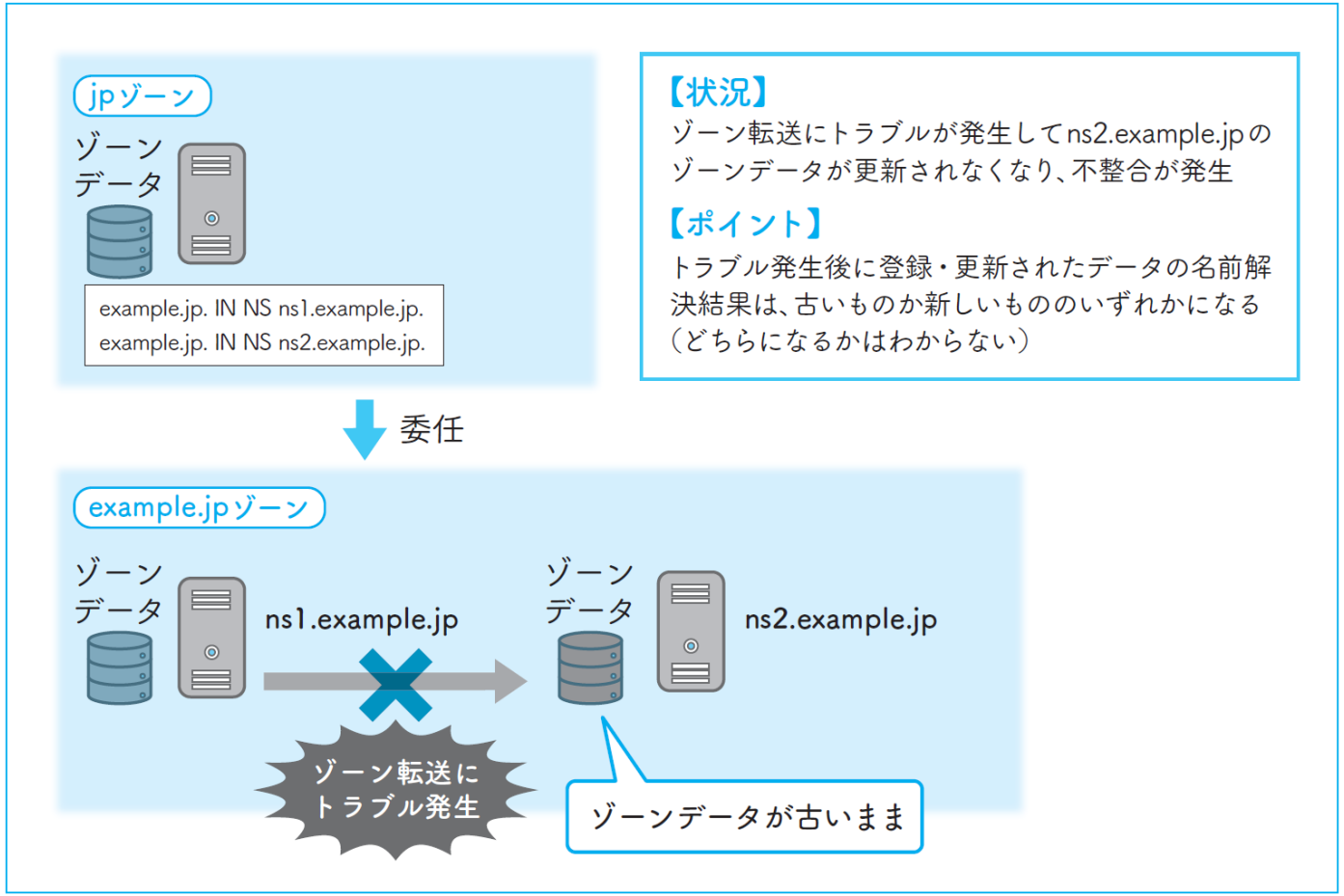
権威サーバー運用のトラブル

- 権威サーバー間のゾーンデータ不整合
  - ゾーン転送のトラブルによって引き起こされる



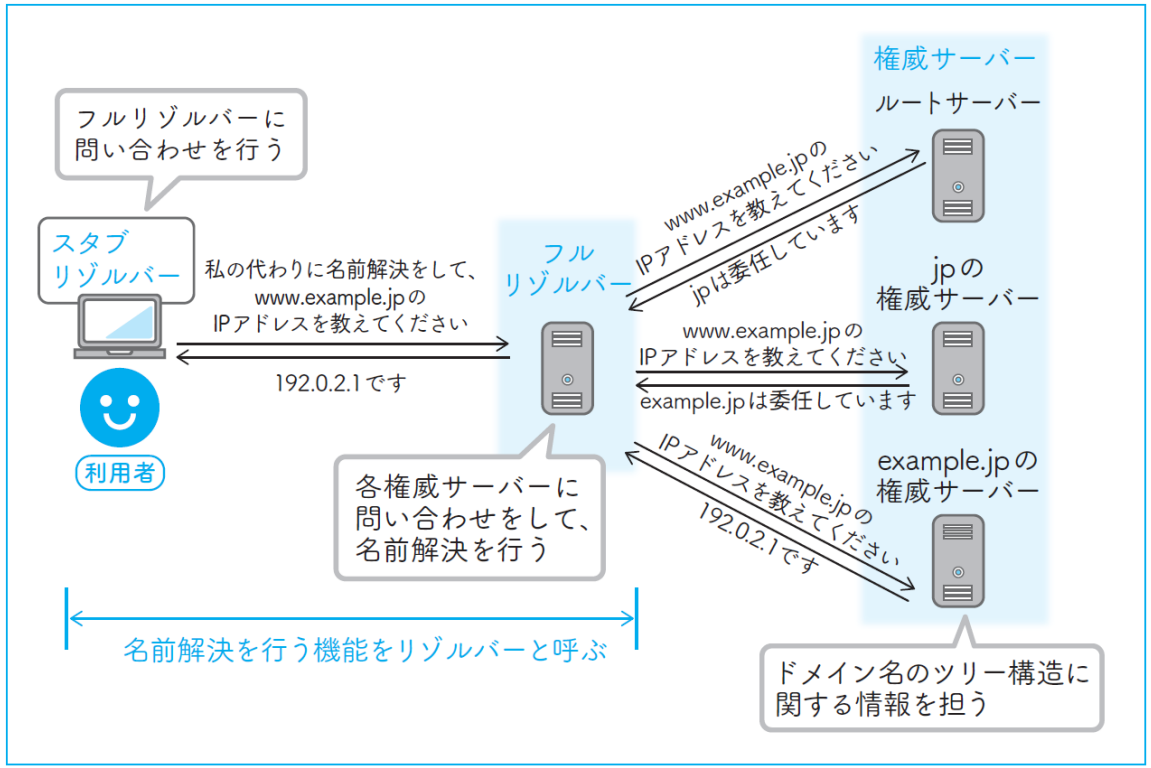
権威サーバー運用のトラブル

- 親子間のNSリソースレコードの不整合
  - 親ゾーンの委任情報の更新を怠ることで引き起こされる



5. フルリゾルバー

DNSの構成要素（再）



スタブリゾルバー

フルリゾルバーに名前解決を依頼する

フルリゾルバー

ルートから順に階層構造をたどり、名前解決を実行する
権威サーバーから得られた情報をしばらく保持する
→キャッシュ

権威サーバー

委任されたゾーンの名前情報（ゾーンデータ）と委任情報を管理する

フルリゾルバーの役割

- 名前解決サービスの提供
  - 利用者と権威サーバーの間で、必要な名前情報を調べる
  - フルリゾルバーが止まると、利用している全ての利用者の名前解決ができなくなる

ドメイン名を使用した全てのインターネットサービスが利用できなくなる

ISPなど、大規模なネットワークのフルリゾルバーに障害が発生した場合、
そのISPの利用者全体に影響が及ぶ

フルリゾルバーの動作（ヒントファイル）

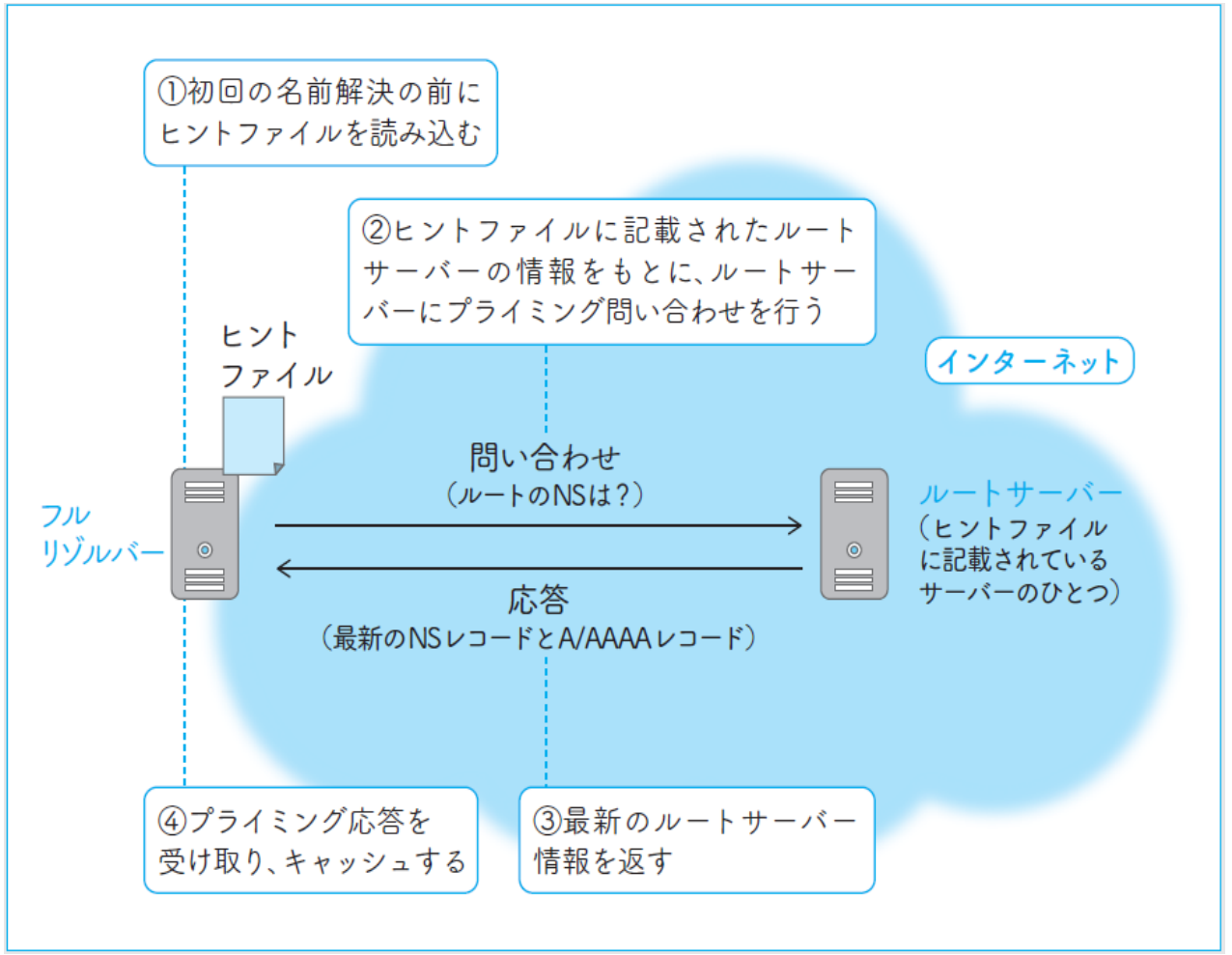
- ルートサーバーのホスト名とIPアドレスが記載されたファイル
  - ルートゾーンのNSリソースレコード
  - ルートサーバーのA/AAAAリソースレコード
- フルリゾルバーに静的に設定され、初回の名前解決時に読み込まれる
  - ルートサーバーが変更された場合、変更を反映する必要がある
- 多くのフルリゾルバーの実装では、ヒントファイルの内容はルートサーバー自身にルートゾーンのNSリソースレコードを問い合わせる際にのみ使われる
  - この動作を「**プライミング**」と呼ぶ

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:     July 09, 2018
;       related version of root zone:     2018070901
;
; FORMERLY NS.INTERNIC.NET
;
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     199.9.14.201
B.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:200::b
（中略：C.ROOT-SERVERS.NET～L.ROOT-SERVERS.NETの情報が記述されている）
;
; OPERATED BY WIDE
;
.                        3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.      3600000      A     202.12.27.33
M.ROOT-SERVERS.NET.      3600000      AAAA  2001:dc3::35
; End of file
```

フルリゾルバーの動作（プライミング）

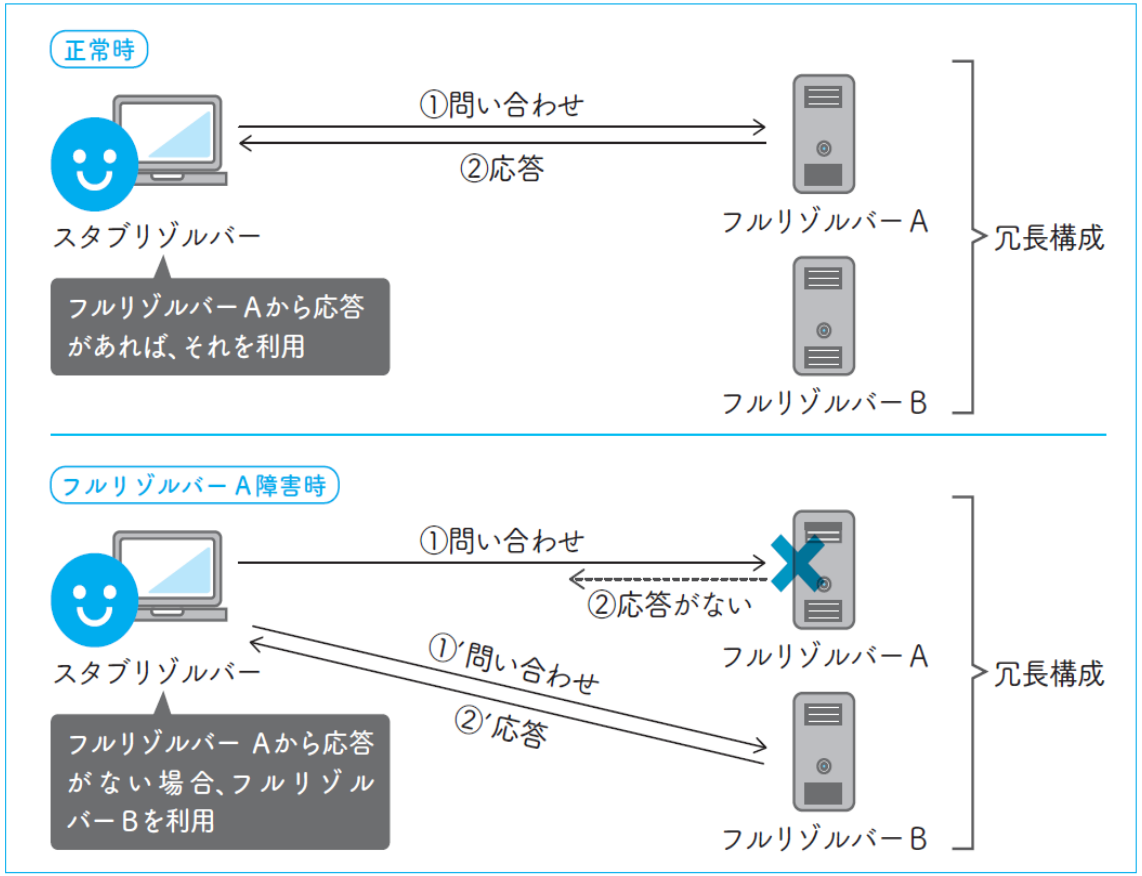
- 最新のルートサーバーの一覧を得るための仕組み
  - ルートサーバーのIPアドレスは、運用上の都合で変更される場合がある
- プライミングの動作
  ① 初回の名前解決の前に、ヒントファイルを読み込む
  ② ヒントファイルの情報をもとに、ルートサーバーにプライミング問い合わせを行う（“.”のNS）
  ③ 応答を受け取る（最新の“.”のNSとルートサーバーのA/AAAA））
  ④ 応答をキャッシュし、以降の名前解決ではその情報を使う

キャッシュが満了した場合、再度プライミングを行う



フルリゾルバーの冗長化

- 複数台のフルリゾルバーを設置・利用することで可用性を向上
  - スタブリゾルバー側で複数のフルリゾルバーを指定可能になっている場合が多い
  - 記載順に問い合わせを送り、問い合わせを送ったフルリゾルバーから応答が得られなかった場合には、次のフルリゾルバーに同じ問い合わせを送るようにすることで1台がダウンしても、名前解決を継続できる



オープンリゾルバーの危険性

- オープンリゾルバーとは
  - アクセス制限が実施されておらず、インターネット上のどのネットワークからでも名前解決サービスを使えるようになっているフルリゾルバー
  - 管理者の意図に反してオープンリゾルバーの状態になってしまっている場合、深刻な危険性を持つ

    → DNSリフレクター攻撃の踏み台にされたり、キャッシュポイズニングをはじめとするDNSを狙ったサイバー攻撃を受けやすくなったりする

パブリックDNSサービス

- さまざまな対策（負荷対策やセキュリティ上の対策など）を実施したうえで、DNSの名前解決を外部サービスとして公開しているものが存在する
  - 外部から見た場合、オープンリゾルバーと同じ状態
- パブリックDNSサービスの例
  - Google Public DNS <https://dns.google.com/>
  - Quad9 DNS <https://www.quad9.net/>
  - 1.1.1.1 <https://1.1.1.1/>
  - IIJ Public DNSサービス <https://public.dns.iij.jp/>
    - 通常のパブリックDNSサービスは提供せず、DNS over TLS / DNS over HTTPSのみを提供
- インターネット上には、さまざまなパブリックDNSサービスが存在
  - それぞれのサービス提供者が定める管理ポリシーのもと、名前解決サービスを提供

6. DNSに関するサイバー攻撃と対策

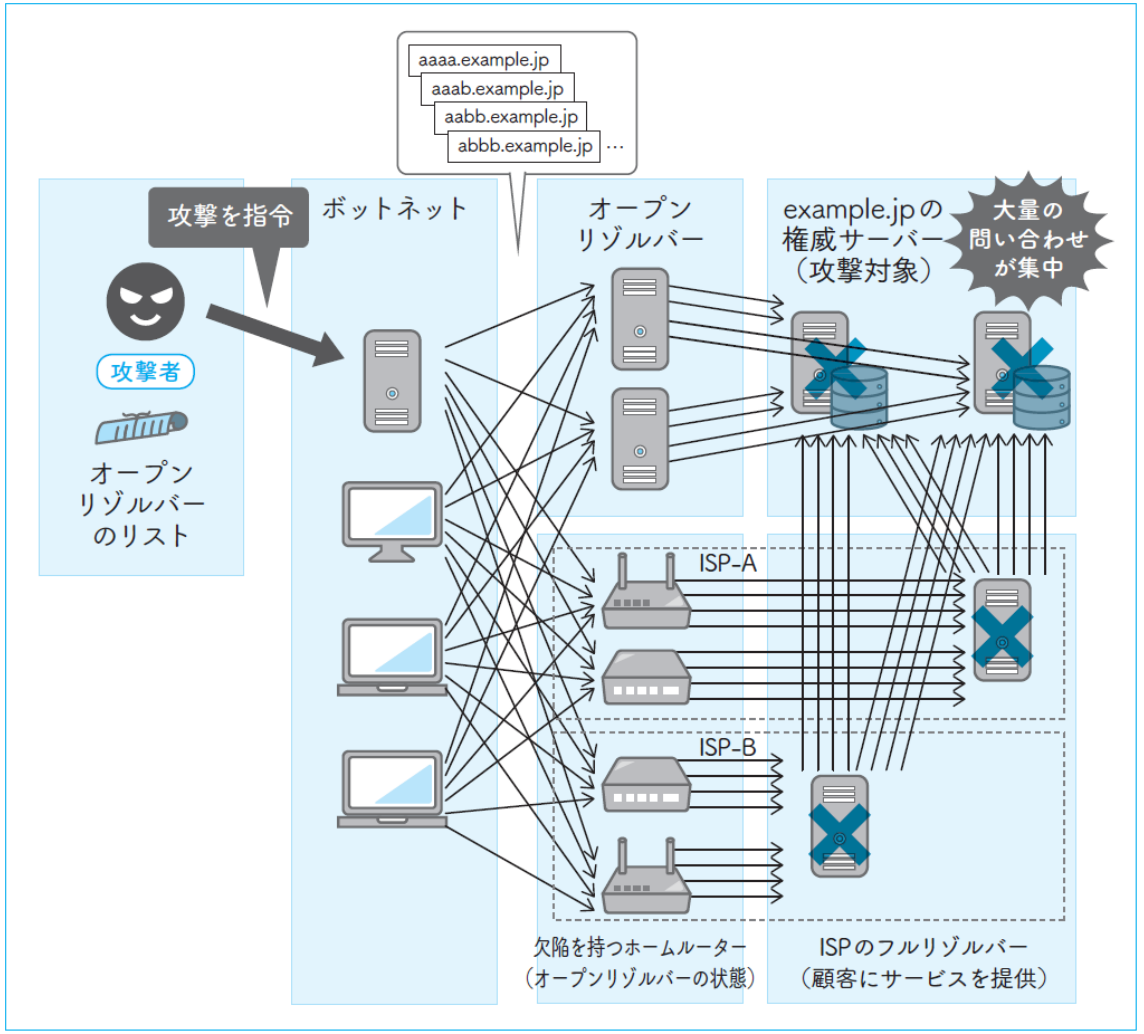
攻撃対象と攻撃手法の分類と例

何が ＼ どういう方法で	（A）帯域や処理容量をあふれさせる	（B）プロトコルの弱点を突く	（C）実装・設定・運用上の問題点を突く
（1）DNSそのもの	1-A	1-B	1-C
（2）他者（DNSを利用）	2-A	2-B	2-C

分類	攻撃手法の例
1-A	権威サーバーやフルリゾルバーへの大量のデータ送信によるDDoS攻撃、**ランダムサブドメイン攻撃**
1-B	権威サーバーやフルリゾルバーへのTCP SYN Flood攻撃、**ランダムサブドメイン攻撃**
1-C	**BINDの脆弱性を突いたDoS攻撃**
2-A	オープンリゾルバーを利用した**DNSリフレクター攻撃**
2-B	**キャッシュポイズニング**による偽サイトへの誘導
2-C	**登録情報の不正書き換えによるドメイン名ハイジャック**、実装のバグを利用した**キャッシュポイズニング**による偽サイトへの誘導、ホームルーターのDNS設定不正変更による偽サイトへの誘導

ランダムサブドメイン攻撃（DNS水責め攻撃）

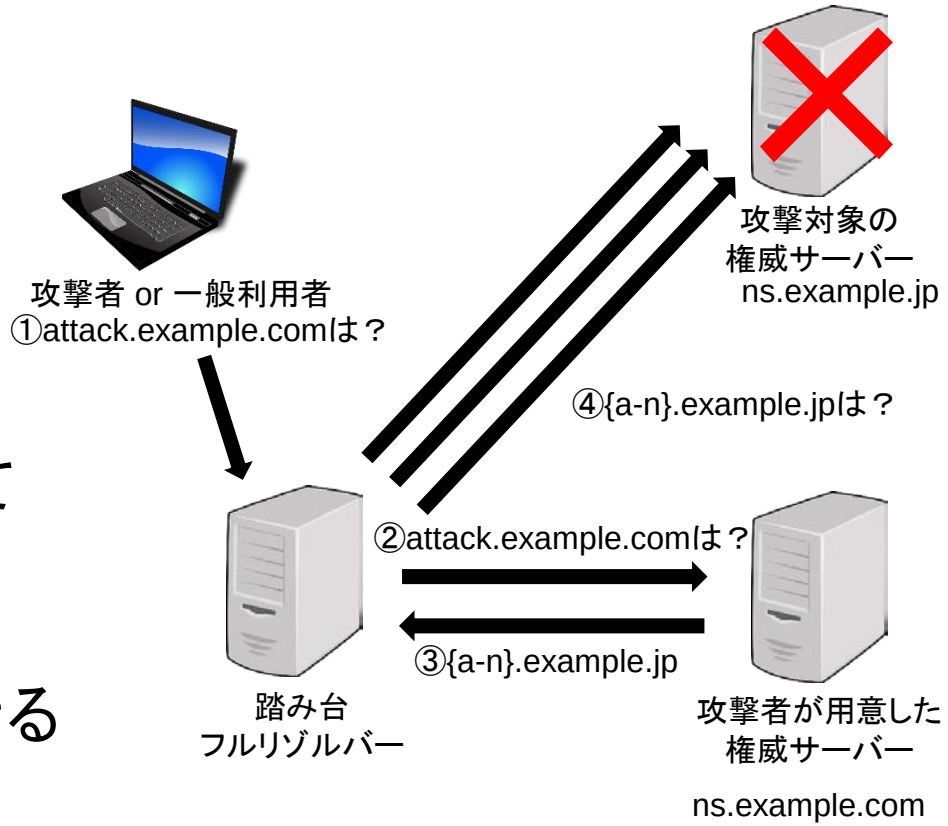
- DNSサーバーに対するDDoS攻撃の1つ
- DNSの問い合わせドメイン名にランダムなサブドメインを付加することで、キャッシュの機能を無効化し、攻撃対象となる権威サーバーやフルリゾルバーをサービス不能状態にする
- 本攻撃では、問い合わせ元のIPアドレスを詐称する必要が無く、攻撃と通常の問い合わせの区別がつかないことから、根本的な対策を実施しづらい



何が ＼ どういう方法で	（A）帯域や処理容量をあふれさせる	（B）プロトコルの弱点を突く	（C）実装・設定・運用上の問題点を突く
（1）DNSそのもの	1-A	1-B	1-C
（2）他者（DNSを利用）	2-A	2-B	2-C

NXNSAttack

- DNSサーバーに対するDDoS攻撃の1つ
- 攻撃者が管理権限を持つドメイン名の委任情報として、攻撃対象のドメイン名に異なるサブドメインを付加したドメイン名を権威サーバーとして指定した多数のNSリソースレコードを登録する（前準備）
- この状況で、攻撃者が準備したドメイン名に対して名前解決を実行させ、フルリゾルバーから攻撃対象の権威サーバーに、権威サーバーホスト名を解決するための問い合わせを集中させる



attack	IN	NS	a.example.jp.
	~~		
	IN	NS	n.example.jp.

何が ＼ どういう方法で	（A）帯域や処理容量をあふれさせる	（B）プロトコルの弱点を突く	（C）実装・設定・運用上の問題点を突く
（1）DNSそのもの	1-A	1-B	1-C
（2）他者（DNSを利用）	2-A	2-B	2-C

BINDの脆弱性を突いたDoS攻撃

- BINDの脆弱性には、リモートから問い合わせを1つ送りつけるだけで権威サーバーやフルリゾルバーのプロセスをダウンさせることが可能なものがある
- こうした脆弱性を外部から突くことで、権威サーバーやフルリゾルバーのサービスを妨害するDoS攻撃が可能
- BINDに限らず、脆弱性はDoS攻撃のターゲットにされる

■（緊急）BIND 9.xの脆弱性（DNSサービスの停止・異常な動作）について
（CVE-2020-8617） - フルリゾルバー（キャッシュDNSサーバー）／
権威DNSサーバーの双方が対象、バージョンアップを強く推奨 -

株式会社日本レジストリサービス（JPRS）
初版作成 2020/05/20（Wed）

▼概要

BIND 9.xにおける実装上の不具合により、namedに対する外部からのサービス不能（DoS）攻撃が可能となる脆弱性が、開発元のISCから発表されました。本脆弱性により、提供者が意図しないサービスの停止や、異常な動作が発生する可能性があります。

該当するBIND 9のパッケージを利用しているユーザーは、各ディストリビューションベンダーからリリースされる情報の収集やバージョンアップなど、適切な対応を速やかに取ることを強く推奨します。

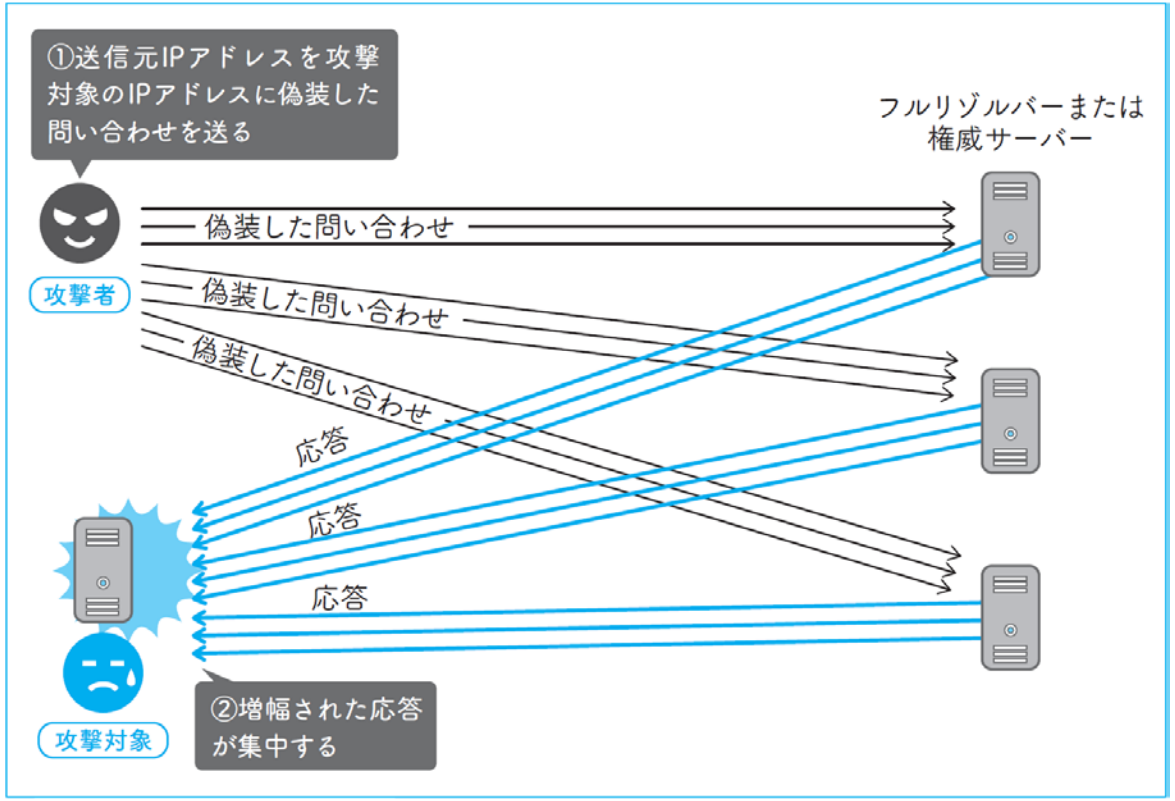
本脆弱性はTSIG（後述）の処理の不具合に由来するものですが、TSIGを明示的に設定していない場合も対象となります。即時の対応を強く推奨します。

https://jprs.jp/tech/ より

どういう方法で / 何が	(A) 帯域や処理容量をあふれさせる	(B) プロトコルの弱点を突く	(C) 実装・設定・運用上の問題点を突く
(1) DNSそのもの	1-A	1-B	1-C
(2) 他者（DNSを利用）	2-A	2-B	2-C

DNSリフレクター攻撃

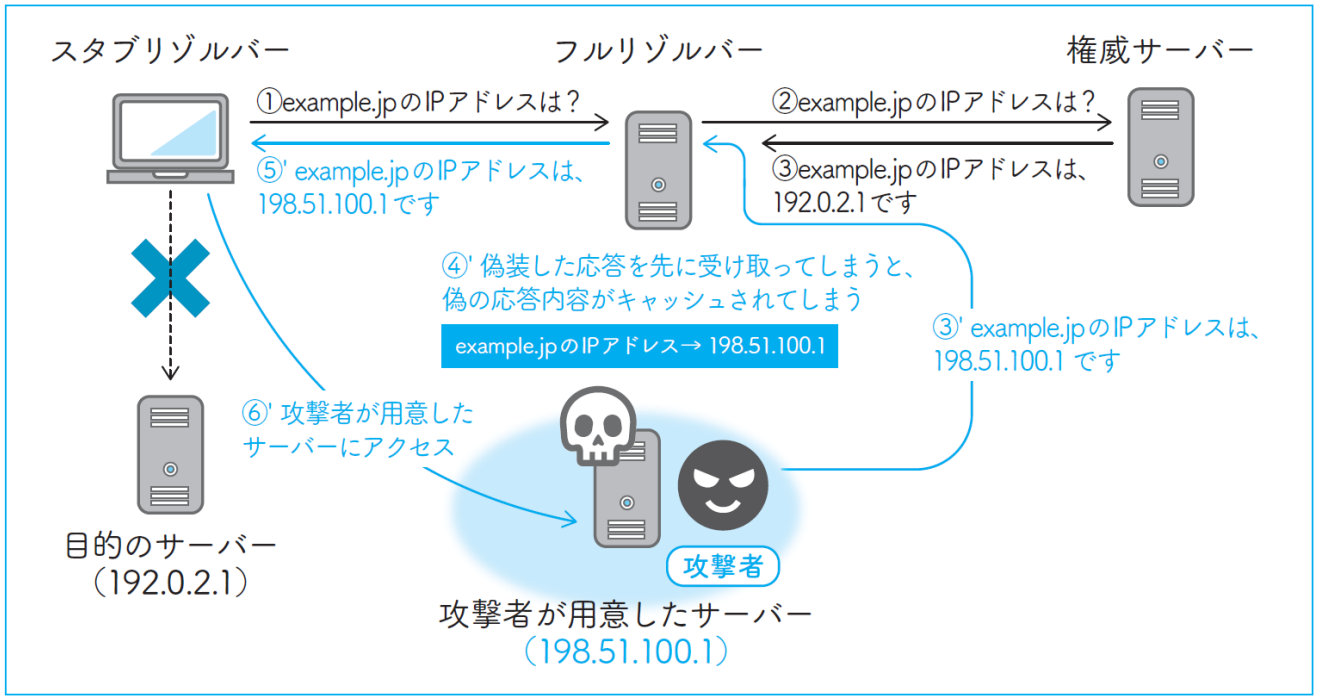
- 送信元IPアドレスを偽った問い合わせをフルリゾルバーや権威サーバーに送ることでそれらのサーバーの応答を攻撃対象に送らせ、サービス不能の状態に陥らせる
- DNSの特性を攻撃に利用
- DNSでは常に、問い合わせよりも応答の方がパケットのサイズが大きくなり、小さな問い合わせパケットで大きな攻撃パケットを生成（攻撃を増幅）できることから「DNSアンプ攻撃（DNS Amplification Attack）」とも呼ばれる



どういう方法で / 何が	（A）帯域や処理容量をあふれさせる	（B）プロトコルの弱点を突く	（C）実装・設定・運用上の問題点を突く
（1）DNSそのもの	1-A	1-B	1-C
（2）他者（DNSを利用）	2-A	2-B	2-C

キャッシュポイズニング

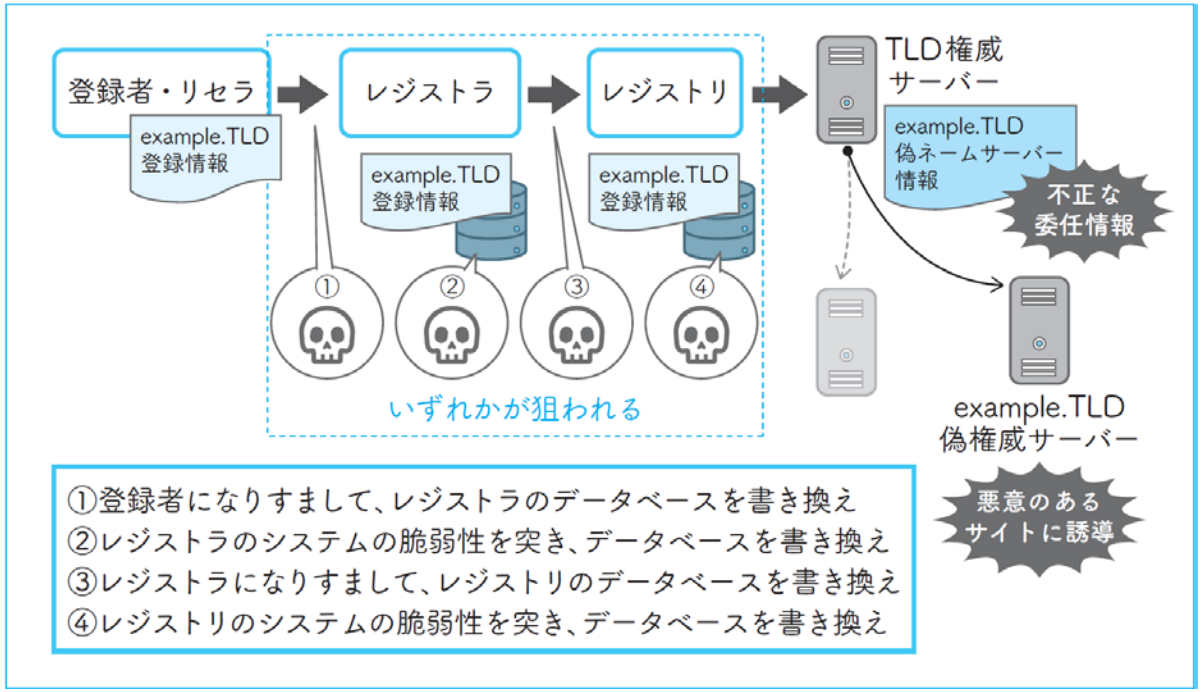
- 偽のDNS応答をフルリゾルバーにキャッシュさせることで、利用者のアクセスを攻撃者が用意したサーバーに誘導し、フィッシングや送信された電子メールの窃盗などを図る攻撃
- カミンスキー型攻撃手法
  - 攻撃対象のドメイン名にランダムなサブドメインを付加した名前を用いることで、連続での攻撃を可能にした
  - ベルンハルト・ミュラー氏がカミンスキー型攻撃手法な攻撃のパターンを発表し、攻撃の危険性が高まった
    - 偽の委任情報を注入



どういう方法で / 何が	(A) 帯域や処理容量をあふれさせる	(B) プロトコルの弱点を突く	(C) 実装・設定・運用上の問題点を突く
(1) DNSそのもの	1-A	1-B	1-C
(2) 他者 (DNSを利用)	2-A	2-B	2-C

ドメイン名ハイジャック

- ドメイン名の管理権限を持たない第三者が不正な手段で、ドメイン名を自身の支配下に置く
- 以下のような攻撃が可能
  - 攻撃者が準備した偽サイトにアクセスを誘導
  - フィッシング、Webサイト閲覧者に対するマルウェアの注入、クッキーの改変、電子メールの盗み身、なりすましメールの発信など
- 代表的な方法
  - レジストリに登録されている情報を書き換える
  - 権威サーバーに不正なデータを登録する



攻撃対象と手法、対策のまとめ

攻撃の対象	攻撃手法の例	対策の例
DNSそのもの 権威サーバーやフルリゾルバーを妨害し、サービスを提供・利用できないようにする	• DNSに対するDDoS攻撃 複数箇所からDNSの構成要素を攻撃	• IP Anycast
	• 脆弱性を突くDoS攻撃 ソフトウェア脆弱性を利用し、サービスを停止	• 最新版のソフトウェアの利用
他者（DNSを利用） DNSを攻撃の手段として使う	• DNSリフレクター攻撃 DNSを使って攻撃の規模を増幅させたりする	• アクセスコントロール • RRL（応答頻度の制限）
	• **ドメイン名ハイジャック** 不正な手段でドメイン名を支配下に置き、偽サイト誘導やメール窃盗をする	• 二要素認証 • クライアント証明書 • **レジストリロック**の利用
	• **キャッシュポイズニング** DNSの名前解決結果を偽情報に差し替えて利用者を偽サイトに誘導する	• DNSクッキーの導入 • DNSSEC

本日のまとめ（1）

- インターネットではIPアドレスとドメイン名がDNSによって対応付けられている
- ドメイン名はルート（. ）から、TLD、2LD、3LD…という階層構造になっている
- TLD毎にドメイン名の登録管理を行うレジストリとドメイン名登録者の申請を取り次ぐレジストラが存在する

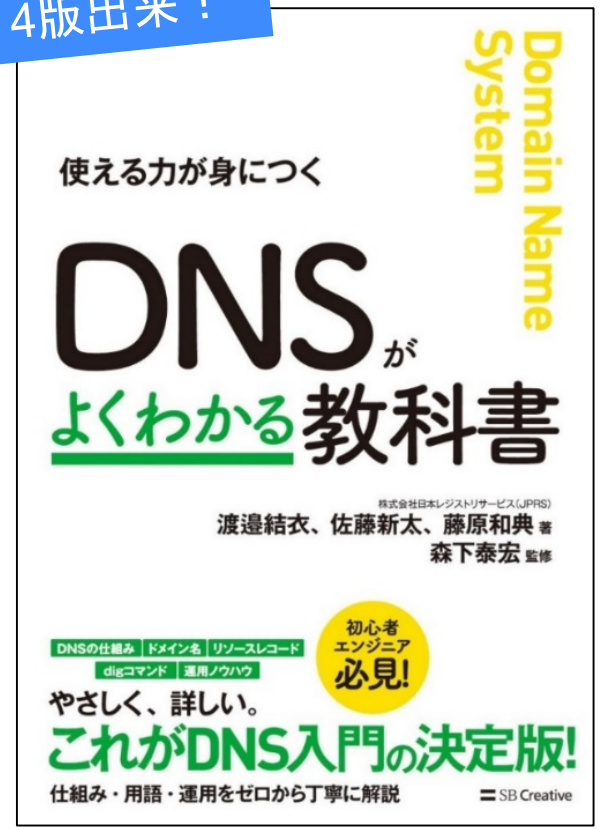
本日のまとめ(2)

- ドメイン名には有効期限があるため、期限が切れないように注意し、廃止も慎重に行う必要がある
- DNSには委任されたゾーン情報を保持する権威サーバーと、名前解決を実行するフルリゾルバーの2種類が存在する
- フルリゾルバーは、どこからでも利用できるオープンリゾルバーにならないように注意する
- DNSに対する攻撃手法は多く存在するが、DNSそのものに対する攻撃なのか、DNSを利用した他者への攻撃なのかを判断し、それぞれに合った対策を練る必要がある

書籍「DNSがよく分かる教科書」

- JPRSの技術者が執筆と監修を担当
  - 著者：渡辺結衣、佐藤新太、藤原和典
  - 監修：森下泰宏
- DNSの仕組みから運用、DNSにまつわるサイバー攻撃と対策、最新のDoTやDoHまでをゼロから体系的に解説

4版出来！



DNSがよくわかる教科書｜SBクリエイティブ
https://www.sbcr.jp/product/4797394481/

※本スライドの図の一部は、本書から引用しています