

DNSワイルドカードに関する 技術的特徴と課題

—Site Finderサービスを中心に—

2003年10月8日

第2回ドメイン名ポリシー研究会

株式会社日本レジストリサービス 技術研究部

森下 泰宏 <yasuhiro@jprs.co.jp>

本日の予定

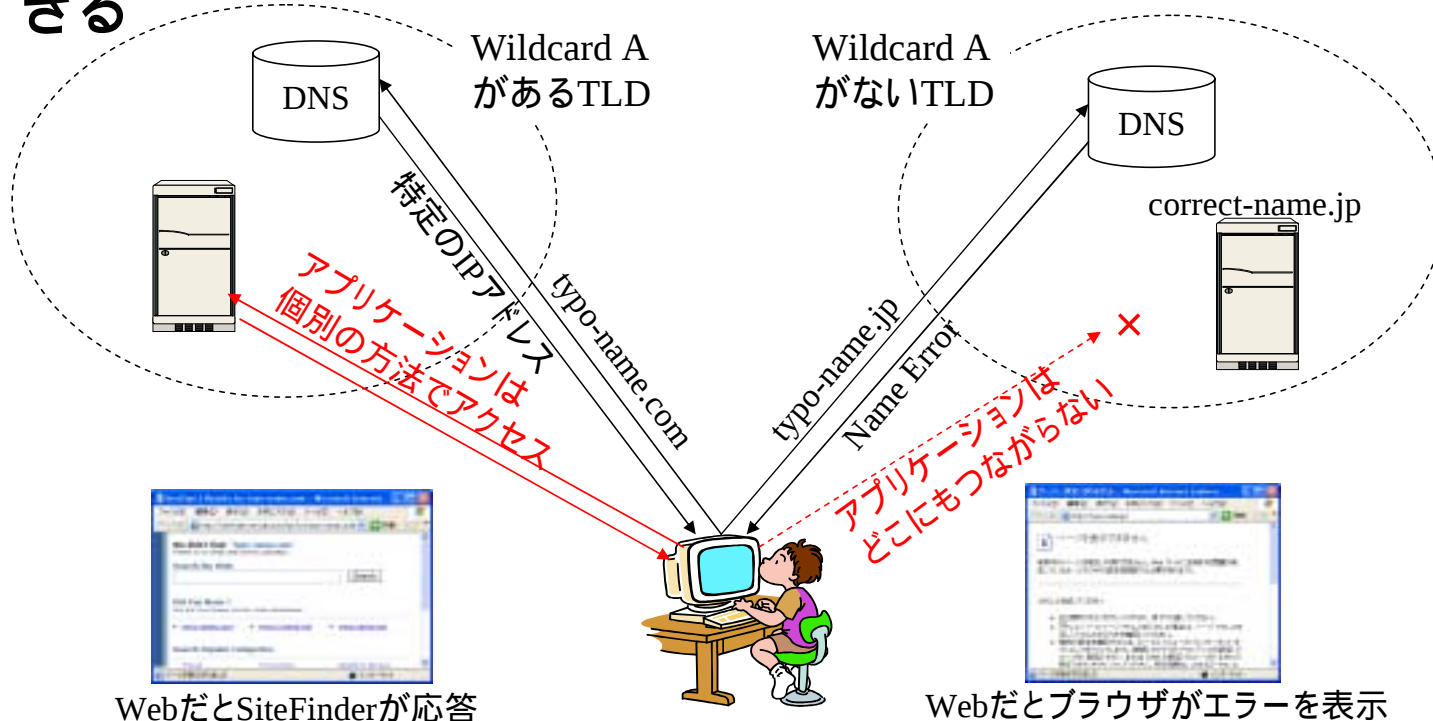
- Site Finderサービスとは
 - Site Finderサービスの特徴
 - Web-based Navigationとの違い
 - Site Finderサービスのしくみ
- DNSのワイルドカードとは
 - 従来からの利用方法
 - 最近出現した利用方法
- ワイルドカード設定時に考慮すべき技術的事項
- Site Finderに関する時系列的な経緯
- 各団体・コミュニティの反応
- 関連URI

Site Finderサービスとは

- 米国VeriSign Inc.(以下VeriSign)が2003年9月15日から2003年10月4日(現地時間)にかけて実施したサービス
- Webブラウザから、「com/netのDNSサーバに登録されていないcom/netドメイン名」が入力された際に、VeriSignが運営するポータルサイト(*)に接続
 - (*) 64.94.110.11 (sitefinder-idn.verisign.com)
- DNSのワイルドカード機能を利用(後述)
 - com/netゾーンに、Wildcard Aを設定

Site Finderサービスの特徴

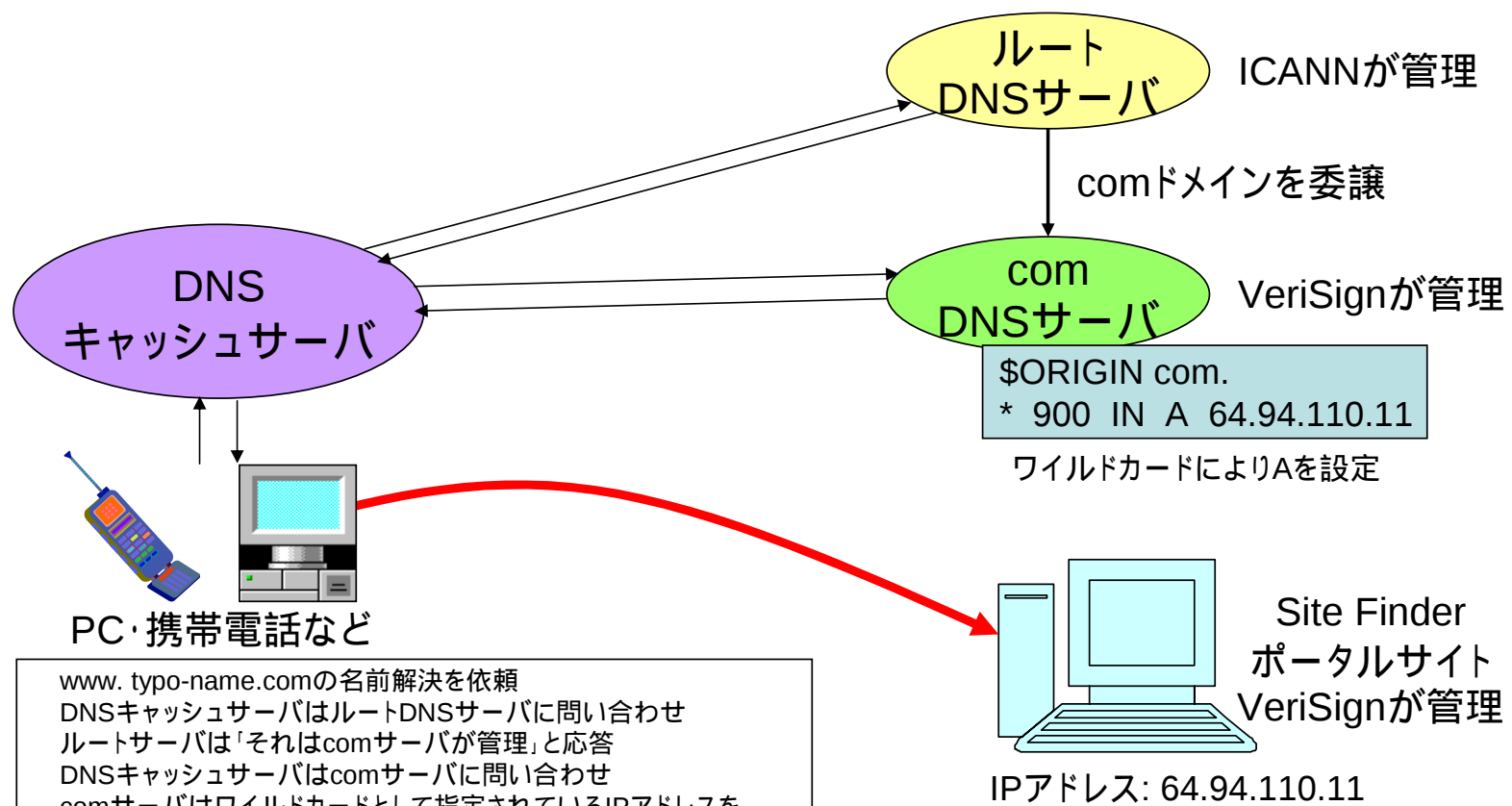
- 利用者が間違った(DNSに設定されていない)ドメイン名を入力した際の挙動を、TLDレジストリが変えることができる



Web-based Navigationとの違い

- Web-based Navigation
 - 登録者が存在する国際化ドメイン名(IDN)が対象
 - 該当するドメイン名の登録者が、自分のドメイン名についてWeb-based Navigationサービスを有効にするかどうかを選択することが(技術的に)可能
- Site Finder
 - 登録者が存在しないすべてのドメイン名が対象
 - 該当するすべてのドメイン名に対し、一律に適用

DNSからみた Site Finderサービスのしくみ



www. typo-name.comの名前解決を依頼
 DNSキャッシュサーバはルートDNSサーバに問い合わせ
 ルートサーバは「それはcomサーバが管理」と応答
 DNSキャッシュサーバはcomサーバに問い合わせ
 comサーバはワイルドカードとして指定されているIPアドレスを、
 www. typo-name.comのIPアドレスとして応答
 DNSキャッシュサーバは問い合わせ元にIPアドレスを応答
 Site Finderポータルサイトへのアクセスが発生

ワイルドカードとは(1)

- DNSの基本機能の一つ
- 特殊なラベル「*」で始まる名前を持つリソースレコード
 - DNSにおいて特別な意味を持つ
- リソースレコードの「合成(synthesizing)」を行うためのものと考えることができる、と記述(RFC1034)
- そのゾーン内に存在しない名前に対してのみ有効

ワイルドカードとは(2)

- ワイルドカードは「そのゾーン内」に対してのみ有効
 - 委譲(delegation)されている名前空間に対しては無効
 - すなわち、あるゾーン上においてNSレコードの登録により、委譲が行われているドメイン名空間については、実在しないドメイン名であっても、ワイルドカードは適用されない
 - 例: 下記の場合、*typo-name.example.TLD*はワイルドカードの影響を受けない

\$ORIGIN	TLD.		
example	IN	NS	ns.example.TLD.
*	IN	A	1.2.3.4

従来からの利用方法

- wildcard MXを主に利用
- インターネットからインターネット以外のシステム(UUCP など)へメールを転送するため等に使うゾーンの生成
 - 以前はよく行われていた
 - JUNET/BITNET等からインターネットへの移行時など
- 外部向け名前空間と内部向け名前空間を分割する
 - メールアドレスはイントラネットとインターネットで同一にしたいが、社内の名前空間の管理構造は隠蔽したい
 - 例: info@sales.example.co.jpというメールアドレスを外部に対して見せるが、外部向けに設定するexample.co.jpのDNSサーバでは、wildcard MXのみを指定する

最近の利用方法

- **Wildcard Aを利用したサービス**
 - Wildcard Aそのものは、DNSプロトコルには違反していない
- **一部のTLDレジストリ**
 - レジストリサービスに利用
 - cc, nuなど (登録可能であることを表示)
 - museum (利用上の便宜&museumドメイン名のプロモーション)
 - レジストリサービス以外のサービスに利用
 - Site Finderサービス
- **日本語ドメインインデックスサービス**
 - jp.ioゾーンに対してwildcard Aを設定
 - IDN非対応のブラウザがそのまま「8ビットDNSクエリ」を投げることを利用

Wildcard Aを設定した場合に考慮すべき 技術的事項(1)

- Web以外のインターネットサービスへの影響(例:メール)
 - 従来「あて先不明」でどこにも接続されずにエラーになっていたメールについて、いったんレジストリが設定したアドレスへの接続(配送処理)が起こることになる
 - これらのメールのコピーやアドレスリストをレジストリ側で保存することも、技術的には可能
- 「そのドメイン名が存在しない」ことを利用したサービスへの影響
 - SPAMメールの検知(From: 等による)に影響が出る
 - SPAMにより惹起されるエラーメールの返信エラー
 - システム管理者が受信するエラーメールの数が急増
- ネットワーク資源の消費
 - 従来発生しなかった、Site Finderサービスを表示するためのネットワークトラフィックが発生
 - 例えば携帯電話でドメイン名を打ち間違えると、その分の「従来発生しなかったパケット通信料金」が発生することになる

Wildcard Aを設定した場合に考慮すべき 技術的事項(2)

- 国際化ドメイン名(IDN)への影響
 - 現在策定中のIDN-adminへの影響
 - idn-adminはvariantsによりドメイン名を予約し、それらのドメイン名についてはDNSが「そのドメイン名は存在しない」と返す(レジストリが「不存在」を保証する)ことにより成立している
 - wildcard Aを設定すると、これに影響が出る可能性がある
- キャッシュ残存による影響
 - シビアなタイミングでサービスを開始したいドメイン名への影響
 - 従来は「存在しない」状態からスタート(negative cache)
 - 今後は「アドレスがある」状態からスタート(通常のcache)
 - TTL値を注意深く設定しないと、キャッシュ残存によるサービスの遅れが出る可能性がある

Wildcard Aを設定した場合に考慮すべき 技術的事項(3)

- Webブラウザに表示されるエラーメッセージ
 - 例えば、ブラウザから得られる言語情報を利用する等により、アクセスした側の母国語によりエラーメッセージを返す、等の配慮が必要となる
- Single Point of Failureの可能性
 - Wildcard Aにより誘導されるIPアドレスでのサービスが停止していた場合、ユーザのWebブラウジングに障害が発生することになる
 - 途中のネットワーク上に経路障害等が発生した場合も同様

時系列での経緯(1)

- 9月15日
 - VeriSign、Site Finderサービスを開始
- 9月16日
 - Vinton Cerf氏、コメント発表
 - “The service could violate long-standing Internet standards.”
 - ISC、Site Finderをキャンセルするパッチを作成中であることを表明
- 9月17日
 - ISC、Site Finderをキャンセルするためのパッチ(BIND 9用)を提供
- 9月18日
 - VeriSign、Site Finderを「修正」と表明
 - 検索エンジンNetsterが独禁法違反でVeriSignを提訴

時系列での経緯(2)

- 9月19日
 - ICANN、最初のAdvisoryを発表
 - VeriSignに、Site Finderを自主的に停止するように要請
 - IABとSECSACにコメントを求める
 - IAB、コメントを発表
 - ゾーン管理者がリスクを熟知し、かつそのゾーンの下で委譲を受けている人々の同意が得られない限り、ワイルドカードを使用しないことを推奨
- 9月21日
 - VeriSign、ICANNに対し返信
- 9月22日
 - Go Daddy、VeriSignを独禁法違反で提訴
 - ICANN SECSACがコメントを発表

時系列での経緯(3)

- 9月23日
 - PIR、VeriSignを非難する声明を発表
 - VeriSign、Site Finderに対する技術委員会を設置
- 9月26日
 - ICANN、Site Finderに関する「まとめサイト」をオープン
 - ISOC、Site Finderへの反対を表明
 - VeriSignに対し「DNSに関する権力濫用」で集団訴訟
- 10月3日
 - ICANN、VeriSignに対し「最後通牒」を通告(以下引用)
 - ICANN has today insisted that VeriSign suspend the SiteFinder service, and restore the .com and .net top-level domains to the way they were operated prior to 15 September 2003. If VeriSign does not comply with this demand by 6:00 PM PDT on 4 October 2003, ICANN will be forced to take the steps necessary to enforce VeriSign's contractual obligations.

時系列での経緯(4)

- 10月3日
 - VeriSign、Site Finderサービスの一時停止に同意
 - VeriSign、IABのコメントに返答
- 10月4日
 - VeriSign、ICANNの命令に従いSite Finderサービス停止
- 10月6日
 - VeriSign、**声明を発表**
 - ZDNet Japanから引用:
 - ...Site Finderがなければ「インフラに投資する予算を創出する機会が制限され」、このサービスを恒久的に中止すればVeriSignの健全性、ひいてはインターネット全体の健全性に悪影響を及ぼすとライス氏は話している。

各団体・コミュニティの反応

- 何らかの態度を表明した団体
 - ICANN, ISOC
 - 反対を表明
 - IAB
 - ゾーン管理者のリスクの熟知と、そのTLD下のコミュニティの同意がない限り、ワイルドカードは使用しないことを推奨
- 何らかの態度を表明したgTLDレジストリ
 - PIR (org)
 - MuseDoma (museum)
- 何らかの態度を表明したccTLDレジストリ
 - AFNIC (fr)
 - JPRS (jp), Nominet UK (uk), auDA (au)

関連URI

- 関連情報のほとんどは、以下のURIからたどることができる
- ICANNの「まとめサイト」
 - Information Page: Verisign's Wildcard Service Deployment
 - <http://www.icann.org/general/wildcard-history.htm>
- VeriSign Inc.のSite Finderのページ
 - <http://www.verisign.com/nds/naming/sitefinder/>
- Domain Name News
 - <http://www.domnam.jp/>