

PSLってどうよ？

2014/04/18 JANOG33.5

石田慶樹

背景

- IANA の TLD のリストでは内部のドメイン名の構造がどのようなになっているかわからない
- レジストリが各TLD の構造を決定する
- ドメイン名や DNS からはどの部分が公的でどの部分が私的是かは判らない



- ドメイン名を何らかの形で利用する立場ではドメイン名の構造を何らかの方法で判別する必要がある
 - Web, Mail, PKI, etc.

PSLとは

- PSL: Public Suffix List
 - <https://publicsuffix.org/>
 - Mozilla がホストしてコミュニティ(ボランティア)が更新
 - Public Suffix とはインターネットユーザがその直下に名前を直に登録もしくは取得できる部分
 - Public Suffix List はすべての既知の Public Suffix のリスト
 - IANA の TLD のリストを補完して構造を追加したもの

PSLとは(続き)

- **PSLの機能**
 - (例)ブラウザでの利用
 - フライバシーにダメージを与える“supercookie”を回避
 - ユーザインタフェースとしてドメイン名の重要部分をハイライト
 - 履歴のソート
- **特徴(Mozillaの説明によると)**
 - Community Driven
 - Universal Acceptance

PSLの利用範囲

- 関係者
 - 一般利用者 $\geq$ Webサービス提供者 >> “インフラオペレータ”
- 利用実績
 - ブラウザ他での利用
 - Firefox, Chrome, Opera
 - QT, WhoisMind
 - 数多くのプログラミング言語のライブラリ
 - 利用はさらに広がる可能性
 - 証明書の発行
 - HTML5
 - DMARC

PSLのフォーマット

<http://publicsuffix.org/list/> にある例

注: 1行に1ルール、本来のリストに行番号は無い

```
1. com
2. *.jp
   // Hosts in .hokkaido.jp can't set cookies below level 4...
3. *.hokkaido.jp
4. *.tokyo.jp
   // ...except hosts in pref.hokkaido.jp, which can set cookies at level 3.
5. !pref.hokkaido.jp
6. !metro.tokyo.jp
```

このルールを解釈 (注: foo, barはホスト名):

1. Cookies may be set for foo.com.
2. Cookies may be set for foo.bar.jp.
Cookies may not be set for bar.jp.
3. Cookies may be set for foo.bar.hokkaido.jp.
Cookies may not be set for bar.hokkaido.jp.
4. Cookies may be set for foo.bar.tokyo.jp.
Cookies may not be set for bar.tokyo.jp.
5. Cookies may be set for pref.hokkaido.jp because the exception overrides the previous rule.
6. Cookies may be set for metro.tokyo.jp, because the exception overrides the previous rule.

PSL(の一部)

```
// This Source Code Form is subject to the terms of the Mozilla Public
// License, v. 2.0. If a copy of the MPL was not distributed with this
// file, You can obtain one at http://mozilla.org/MPL/2.0/.
```

```
// ===BEGIN ICANN DOMAINS===
```

```
// ac : http://en.wikipedia.org/wiki/.ac
```

```
ac
com.ac
edu.ac
gov.ac
net.ac
mil.ac
org.ac
```

```
// ad : http://en.wikipedia.org/wiki/.ad
```

```
ad
nom.ad
```

```
// ae : http://en.wikipedia.org/wiki/.ae
```

```
// see also: "Domain Name Eligibility Policy" at http://www.aeda.ae/eng/aepolicy.php
```

```
ae
co.ae
net.ae
org.ae
sch.ae
ac.ae
gov.ae
mil.ae
```

```
// jp : http://en.wikipedia.org/wiki/.jp
```

```
// http://jprs.co.jp/en/jpdomain.html
```

```
// Submitted by registry <info@jprs.jp> 2014-02-28
```

```
jp
```

```
// jp organizational type names
```

```
ac.jp
ad.jp
co.jp
ed.jp
go.jp
gr.jp
lg.jp
ne.jp
or.jp
```

```
// jp prefecture type names
```

```
aichi.jp
akita.jp
aomori.jp
chiba.jp
ehime.jp
fukui.jp
fukuoka.jp
fukushima.jp
gifu.jp
gunma.jp
hiroshima.jp
hokkaido.jp
hyogo.jp
ibaraki.jp
ishikawa.jp
```

8181行中1756行が.JPドメイン名(2014/04/15現在)

これまでの経緯

2007年 Jo Hermans 氏により作成

2008年6月 IETF dnsop WG ML で協力依頼も非難轟々

2008年7月 DNSOPS.jp の BoF にて力武健次氏が紹介

“「Public Suffix Listとその問題点”

<http://dnsops.jp/bof/20080709/dnsops-jp-20080709.pdf>

2011年6月 新gTLD導入プログラム承認

9月 都道府県型JPドメイン名導入発表に伴う論議

“「欠陥ドメイン名」が世界的に増えそうな件について”

<http://www.geekpage.jp/blog/?id=2011/9/29/1>

2013年10月 新gTLDの委任開始

2014年3月 問題解決に向けての動き

PSLの抱える問題点

- **仕様上の問題**
 - スケーラビリティに欠ける
 - リストの形式が洗練されているか
- **実装上の問題**
 - 静的なリスト形式で動的に更新不可
 - ブラウザではコンパイル時に埋め込み
- **運用上の問題**
 - リストのオーナーシップ
 - レジストリからの自己申告により更新
 - Private Domainも 登録可能

今後発生するであろう問題

- 同じブラウザでもバージョンごとに挙動が異なる
- 一般利用者
 - 例えば”新gTLD”の Web がおかしい(最悪見れない)
- Webサービス提供者
 - 同じ設定をしても TLD によってはまともに動かない
- “インフラオペレータ”
 - 問い合わせがあってもネットワーク／サーバそのものにはおかしいところは見つからない

問題解決に向けて

- **2014年3月**
- **IETF 89(London)にて**
 - **dbound (Domain Boundaries) BOF開催**
 - **PSLに関する議論**
 - **懸念事項の指摘[1]**
 - **保守性の悪さ**
 - **構造の変化への追従性**
 - **新gTLDプログラムへの対応**
 - **結論は出ずに次回に持越し**
- **ICANN 49(Singapore) にて**
 - **SSAC(Security and Stability Advisory Committee) の発表[2]**
 - **今年のAction Item**
 - **検討を開始**

[1] 第89回IETF Meeting報告(前編) <http://jprs.jp/related-info/event/2014/0411IETF.html>

[2] <http://singapore49.icann.org/en/schedule/thu-ssac/presentation-ssac-27mar14-en.pdf>

どうすべきか？

- 解決すべき問題に関してコンセンサスの不在
 - スケーラビリティ
 - 現状：リスト形式
 - 将来：DNSが有力？、他のデータベース？
 - 管理
 - 現状：Mozilla
 - 将来：ICANN？、レジストリ団体？、標準化団体？
 - 配布・同期
 - 現状：ファイル配布
 - 将来：DNS？、新たなプロトコル？
 - 普及
 - 現状：リスト配布＋ブラウザに埋込＋ライブラリの開発
 - 将来：どのように現状のものを置き換えるか

PSLってどうよ？

2014/04/18 JANOG33.5

石田慶樹