



ドメイン名を中心としたインターネットポリシーレポート 2013年9月号

## ドットなしドメイン名(Dotless Domain Names)について

### 1. はじめに

新 gTLD プログラムの導入に伴い 1,000 を超える TLD が DNS へ追加されようとしています。これは興味深いことですが、追加される TLD の利用方法によっては混乱が予想されます。例えば“.BRAND”として登録された TLD を利用する上で、セカンドレベル以降のサブドメインを設けず、「<http://brand/>」や「[example@brand](mailto:example@brand)」というように、URL やメールアドレスに“BRAND”とだけ書いたとき、いったい何が起ころのでしょうか？

ICANN のセキュリティと安定性に関する諮問委員会(Security and Stability Advisory Committee; SSAC<sup>1</sup>)は「.」で区切らずに TLD のみで構成されたドメイン名を「ドットなしドメイン名(dotless domain)」と名付け、上記のようなドメイン名について、ほかのドメイン名と同じように利用できるかどうか調査を行い、その調査結果を SAC053 として報告しました。

本ポリシーレポートでは、SAC053 および次項に引用する ICANN における決議の際に判断の参考に用いられた文書を元に、ドットなしドメイン名とその問題点について解説します。

### 2. 背景

これまでのドメイン名の利用環境においては、セカンドレベル以降に任意の文字列を申請者が選択して利用することができましたが、トップレベルのドメイン名の文字列をユーザーが任意に選ぶことはできませんでした。しかし、新 gTLD の導入により、新 gTLD の申請者は、「新 gTLD 申請者ガイドブック」に基づき、TLD のレベルで文字列を選ぶことが可能となりました。

このような状況変化の中で、今回新 gTLD を申請した一部の申請者は、「ドットなしドメイン名」と呼ばれる「<http://brand/>」や「[mail@brand](mailto:mail@brand)」のような、「.」を仕様せずに英数字、数字、ハイフンおよび IDN として認められている文字列によるラベル<sup>2</sup>のみで構成されるドメイン名の利用を想定しました。

しかし、このような利用については、SSAC による報告書 SAC053 や Internet Architecture Board (IAB) による声明において、技術的な影響に対する懸念も確認されています。これを踏まえて、ICANN の新 gTLD プログラム委員会(New gTLD Program Committee; NGPC)<sup>3</sup> は、ドットなしドメイン名に対するパブリックコメントを実施しました。さらに、ICANN 自身も Carve Systems 社に対して調査委託し、その結果も公開しています。

- ICANN のセキュリティと安定性に関する諮問委員会(ICANN Security and Stability Advisory Committee; SSAC)によるレポート  
“SAC053: SSAC Report on Dotless Domains”

<sup>1</sup> <http://www.icann.org/en/groups/ssac>

<sup>2</sup> 「ドメイン名の仕組み」 ページ「ドメイン名の構造」項目：<https://www.nic.ad.jp/ja/dom/system.html>

<sup>3</sup> <http://www.icann.org/en/groups/board/new-gtld>

<http://www.icann.org/en/groups/ssac/documents/sac-053-en.pdf>

- Internet Architecture Board (IAB)による TLD でのドットなしドメイン名に反対する声明  
“IAB Statement: Dotless Domains Considered Harmful”  
<http://www.iab.org/documents/correspondence-reports-documents/2013-2/iab-statement-dotless-domains-considered-harmful/>
- ICANN の委託による Carve Systems 社によるドットなしドメイン名に関する報告  
<http://www.icann.org/en/groups/ssac/documents/dotless-domain-study-29jul13-en.pdf>

上記の情報に基づき、2013年8月30日、ICANNのNGPCは、ドットなしドメイン名を利用可能とした場合、そのリスク軽減の実現性が乏しいとの判断の下、ドットなしドメイン名(dotless domain names)の利用を禁止することを決議し、採択しました。

<http://www.icann.org/en/news/announcements/announcement-30aug13-en.htm>

次項より、ドットなしドメイン名の利用における問題点を事例とともにご紹介します。

### 3. 各種アプリケーションでのドットなしドメイン名の取り扱い

ドメイン名の完全に一意な形式を、Fully Qualified Domain Name(FQDN:「絶対ドメイン名」または「完全に指定されたドメイン名」と呼びます。FQDNは、ラベルを「ドット」(ピリオド)でつなげ、最後にドットで終わるものです。例えば“www.nic.ad.jp.”はFQDNであり、四つのラベルがドットで結ばれ、それぞれDNSの階層を表しています。末尾の“.”は階層の終端を意味しており、DNSのルート(root)を示しています。FQDNは、ドメイン名を特定するのに必要な情報をすべて含んでおり、あいまいさはありません。

しかし、普段ユーザーがドメイン名を利用するときは、一般的にFQDNを省略し、「完全に限定」されない状態で使用されます。例えば“www.nic.ad.jp”というドメイン名は末尾の“.”がないため、FQDNではありません。また、<http://www/> といった省略表記もFQDNではありません。

すべてのアプリケーションが取り扱うドメイン名が、FQDNのみの利用を強制しているのであれば、ドメイン名には常にあいまいさがなくなり、どのようなアプリケーションであっても、予測不可能な動作をすることはほとんどなくなります。

しかし、現在のアプリケーションは、そのような仕様になっていません。よく使われるほとんどのアプリケーションは、多くのユーザーの利用傾向を踏まえ、簡潔な表現や省略表記、あるいは独自の表記をドメイン名として受け付けます。

それぞれ違うアプリケーションがそれぞれ違う方法で、短く省略されたドメイン名をFQDNに補完しようとするため、ドットなしドメイン名は予想もつかない結果になること

が起り得ます。

以下では、ドットなしドメイン名を使用した場合に起り得るアプリケーションのあいまいな挙動について、四つの代表的なケースをご紹介します。

### 3.1. Web ブラウザによる挙動

ユーザーがアドレス欄に文字を入力したとき、Web ブラウザはそれがドメイン名かどうかチェックします。簡単な方法としては、それがドットで区切られたラベルが二つ以上あるかどうかチェックするというものがあり、一部の Web ブラウザはこの方法を適用しています。この場合、ドットなしドメイン名は、ドットがなくラベル一つのみなので、Web ブラウザからはドメイン名として認識されません。

Web ブラウザは、ドットなしドメイン名の入力に対してユーザーの意図を推測し、以下のような挙動をすることが予想されます。

- a. URL(Uniform Resource Locator)内のドメイン名に対して、先頭に“www”といったラベルを付けたり、末尾に“com”や“jp”といったラベルを付け加えたりして DNS に問い合わせる。例えば“example”という入力に対しては [www.example.com](http://www.example.com) や [www.example.jp](http://www.example.jp) といったドメイン名を用いて問い合わせを行う。
- b. 検索パス(\*4.3)が設定されている場合、ドットなしドメイン名にその検索パスを付け加えてドメイン名を検索する。
- c. ドットなしドメイン名の文字列をそのまま検索エンジンに渡す。
- d. 直接変更なしに DNS に問い合わせる。

OS や Web ブラウザ、ユーザーの設定によりますが、上記のいずれか、あるいは複数の挙動が起り得ます。上記の d. のケース以外では、ユーザーがドットなしドメイン名を入力したときに、そのサイトにアクセスできるかどうかは保証されません。

### 3.2. ローカルエリアネットワークの設定による挙動

インターネットでは TCP/IP プロトコルが用いられますが、コンピュータやその他のデバイスが直接接続されるローカルエリアネットワーク(LAN)では、TCP/IP 以外のプロトコルが用いられることがあります。サービスの検索やファイル共有、プリンタの検索などに SMB、CIFS、NetBIOS、NFS、AFP といったプロトコルが利用されます。これらのプロトコルでは、WINS のような DNS 以外の名前空間および名前解決サービスが用いられることがあります。また、名前解決サービスの例として、DNS を用いるものの、トップレベルドメインに “.local” を付け加えて名前解決を行う Bonjour<sup>4</sup> のようなプロトコルもあります。

ドットなしドメイン名は、その本質から一つのラベル、つまり文字の並びでできています。FQDN 形式ではない場合、LAN に接続されたデバイスが最初に DNS へ問い合わせを行うことはなく、別のメカニズムが使用される可能性が高くなります。さらに、“BRAND” といった文字列は LAN 内で別の用途で用いられ、インターネット上のサービスに接続するため

<sup>4</sup> [http://support.apple.com/kb/HT3473?viewlocale=ja\\_JP&locale=ja\\_JP](http://support.apple.com/kb/HT3473?viewlocale=ja_JP&locale=ja_JP)

に用いられない可能性も考えられます。このようなケースでは、ドットなしドメイン名は本来意図した名前解決はされません。

OSがどのような方法で名前を解決するかどうかの標準はないため、ユーザーはときによって違った結果を受けることになります。

### 3.3. DNS スタブリゾルバによる挙動

エンドユーザーのアプリケーションがドメイン名を書き換えなかったとしても、DNS スタブリゾルバ<sup>5</sup>が同じ結果を返すとは限りません。これは「検索パス(search path)」と呼ばれる機能によるものです。

検索パスが設定された DNS スタブリゾルバは、ドットなしドメイン名の問い合わせに対して、検索パスを付け加えてドメイン名を検索し、それに失敗すると検索パスを付けないドメイン名で再度問い合わせを行います。例えば、検索パスに“example.com”が設定されている DNS スタブリゾルバにドットなしドメイン名“dotless”を問い合わせると、まずはじめにリゾルバは“dotless.example.com”を検索します。もし、その結果がドメイン不在応答(non-existent domain, NXDOMAIN)となった場合に、リゾルバは“dotless”を検索します。このような動作はスタブリゾルバの設定により変わり、振る舞いはさまざまなものになります。

今日では、検索パスを設定することは一般的に行われることです。特に企業などの環境では、検索パスが設定されていることを前提とした文書が作成されます。

例えば、イントラネットに置かれたメールサーバで利用される Web インタフェースの URL は、<http://email.example.com/>ではなく <http://email/>と書かれることがよくあります。

これらの事象は、ドットなしドメイン名が一意のアドレス、もしくはサービスを特定できないことを表しています。<http://brand/>という URL は、ドットなしドメイン名の brand にアクセスされず、検索パスに設定されたドメイン「example.com」を加えた、<http://brand.example.com/>にアクセスされる可能性があるということです。

## 4. ドットなしドメイン名とセキュリティ

また、ドットなしドメイン名がサービスコンテンツを持った場合、セキュリティ上の懸念も発生します。「ドットのないホスト名は、組織内の信頼できるネットワーク内に存在するものである」という前提で運用が行われていたケースでは、その前提が覆されます。例えば Windows OS では、ドットのないホスト名はイントラネット内のコンピュータであると認識され、組織内と同様のセキュリティ権限を与えられるかもしれません。ユーザーの設定次第では、コードの実行が許可されることにもなり得ます。

他に注意すべき点としては、「認証」についても同様の懸念が発生することです。

例えば、現在、複数の認証局がドットのないホスト名に対し、(そのホストがグローバルに到達性がないという仮定の下で) 検証することなしにサーバ証明書を発行しています。も

<sup>5</sup>自身で名前解決機能を持たず、他の DNS への問い合わせと結果の出力のみを行う DNS リゾルバ

し、**TLD** をドットなしドメイン名として利用することが許可された場合、プライバシーや完全性といった **SSL** 通信のセキュリティに著しい影響を与えることになります。

そして、最後に重要なこととして、**Web** ブラウザで利用するプロキシサーバを設定するために、多数の組織において自動プロキシ設定スクリプトに、次のような行が含まれていると想定されることが挙げられます。

```
if (isPlainHostName(host)) return "DIRECT";
```

これは、イントラネット内のリクエストがプロキシサーバに送られないことを意味しています。つまり、ドットなしドメイン名への接続は、ユーザーの自動プロキシ設定スクリプトによってプロキシ接続が必要ないと判定され、アクセス先へとリクエストを直接送られることとなります。しかし、プロキシサーバを通らないインターネット向けの接続は組織のファイアウォールによって拒否され、その結果、接続に失敗することになるでしょう。もしドットなしドメイン名でサービスが公開されたとしても、自動プロキシ設定スクリプトによるトラフィック制御機能によって、そのサービスにアクセスできないユーザーが多数出る可能性があるのです。

## 5. 最後に

ここまで述べてきたように、ドットなしドメイン名の利用にはさまざまな懸念点が存在します。**SSAC** は、ドットなしドメイン名はインターネット上での普遍的な到達性が確保されないとして、その利用に対して強く反対しています。そのため、**TLD** レジストリに対しては、いかなる場合においても、**A**、**AAAA**、**MX** などのリソースレコードへのドットなしドメイン名の登録を、契約上で禁止することを求めました。

さらに、「2. 背景」でもご紹介した通り、**Internet Architecture Board (IAB)**からも、**TLD** でのドットなしドメイン名に反対する声明が発表されており、ドットなしドメインの利用には技術的な懸念があることが確認されています。

ドットなしドメインの利用における懸念をもう一度整理すると以下の通りとなります。

- ドットなしドメイン名は、**Web** ブラウザの仕様や **DNS** スタブリゾルバ設定に応じて、ユーザーが本来参照したいサーバのドメイン名として認識されない場合が多く、ユーザーが参照したい **Web** ページを参照できない、またはそれらの挙動により補完されたドメインを利用したほかの **Web** サイトに到達する可能性がある
- 組織内のネットワークに閉じて利用している名前として認識され、本来インターネット上に流されるべきではないデータが流される可能性がある、または反対にドットなしドメイン名を利用したサイトへの接続が困難になる恐れがある。

このような状況を鑑み、冒頭で述べた通り、**ICANN** の **NGPC** は **SSAC** の勧告を元にドットなしドメイン名の使用を禁ずる決議を採択しました。

この決議は、一部の申請者にとっては想定していた用途でドメイン名の利用ができないことにはつながりますが、**ICANN** としてはドットなしドメイン名の利用による影響を考慮した上で、その利用を認めた場合の方が、懸念が大きいと判断したと言えます。