# 10'00"00 インターネット10分講座

MIN SEC 1/100S INTERNET

# TLDにおける名前衝突 (Name Collision)問題

今回のインターネット10分講座では、新gTLDの大量導入に伴う新たなセキュリティリスクとして懸念されている、「名前衝突(Name Collision)」と呼ばれる問題について、その概要と対策を解説します。

## ◆ 内部向けのドメイン名と新gTLDが重複する「名前衝突」という問題

2013年後半から、「.com」「.net」など従来のgTLD(generic Top Level Domain; 分野別トップレベルドメイン)に加えて、新たにgTLDが多数追加されることになりました。それらの中には、例えば「.engineer」「.software」「.host」など、よく使われる文字列を中心にさまざまな文字列が含まれ、今後gTLDとして登録されようとしています。

その一方で、企業内のプライベートネットワークや家庭内のLANなどで、内部向けに今までgTLDに存在していない名前、例えば「.corp」や「.home」などのドメイン名を、TLDとして利用するケースがあります。これまで、gTLDの数はそれほど多くなく限定的であり、存在しない文字列を選択し利用することができました。しかし、今後gTLDが追加されその数が増加することから、そうした内部向けに利用していたTLDが、パブリックなDNSに登録されるgTLDと、文字列が重複する可能性が高くなってきています。実際に重複した場合、DNSの動作が期待するものとは違った動作となることが懸念されます。この問題を「名前衝突(Name Collision)」と呼びます。

名前衝突は今回初めて発生する事象では無く、これまでも「cs(旧チェコスロバキアのccTLD、現在は登録廃止)」や「edu.com」などのドメイン名が登録された際にも発生したことがありました。

例えば「.cs」が登録された時には、「computer science」の意味合いで「cs」というドメイン名を利用している大学などで不具合が発生しました。[※1][※2] また、「edu.com」が登録された時は、名前解決できるまで自身のドメイン名を短縮しつつホスト名の末尾に繰り返し付加するという、古いDNSの実装上の挙動によって、例えば「example.com」のユーザーが「university.edu」と通信しようとした時に「university.edu.com」にアクセスしようとするという問題が発生しました。[※3]

今回の新gTLD追加は大量に行われるため、衝突の可能性や影響範囲は、より大きなものになると考えられています。[※4]

## ◆ 1,300を超える新しいgTLDの大量導入

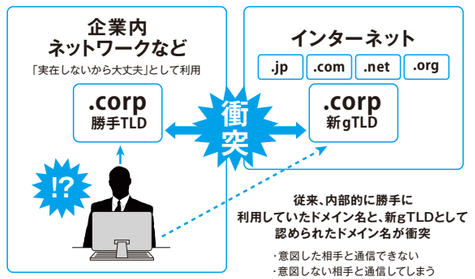
gTLDには従来からあった、世界の誰もが登録できる.com、.net、.orgや、登録者が限定される.edu、.govなどのドメイン名に加えて、2000年以降.biz、.info、.asiaなどのgTLDが順次追加されてきました。とはいえ、その数は15程度で、増加する量も限定的でした。

しかし、ドメイン名をはじめとした各種インターネット資源のグローバルな管理を調整するICANNでは、2012年より「新gTLDプログラム」と題した新たな枠組みに基づいて、募集が行われています。このプログラムでは、あらかじめ決められた募集要項の要件を満たした申請であれば、基本的には誰でもgTLDの登録ができるといった方式へと変更されました。また、登録数の最大数も特に制限されなかったため、2012年の募集に対しては1,930件の応募があり、申請文字列の重複や申請者による取り下げなどを除いても、そのうち1,300件以上のgTLDが追加される見込みです。2014年7月現在、gTLDとして約330のドメイン名がルートゾーンに追加されています[※5][※6]。また、新gTLDの募集は今後も継続して行われる予定で、将来にわたって新gTLDが増えていくと考えられています。

## ◆ 名前衝突の具体例

名前衝突問題で具体的に問題となるのは、例えばインターネット上のドメイン名を検索するつもりが、ローカルネットワークで独自に付けたTLDに対して名前解決を行ってしまう、またその反対に、ローカルネットワークのドメイン名を検索するつもりがインターネット上のTLDに対して名前解決してしまう、などの動作が行われるケースです(図1)。

**図1:名前衝突の例**




また、TLDとして重複しなくても、サーチリストと呼ばれるDNSでのドメイン名の補完機能によっても、名前衝突の問題が発生する可能性があります。例えば「www.corp」といったドメイン名が、サーチリスト機能を用いて「www.corp.example.co.jp」のように補完されることを期待して動作するシステムの場合、TLDとして「.corp」が登録されると、名前衝突が発生することがあります。(図2-1、図2-2)

**図2-1:サーチリストを利用しているケース(新gTLDの登録前)**

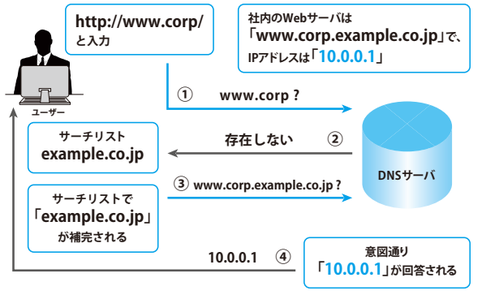
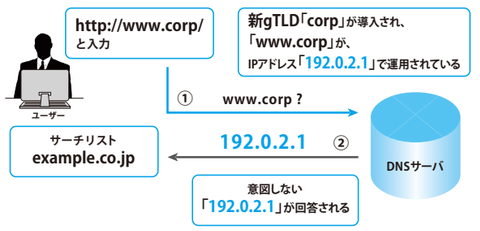
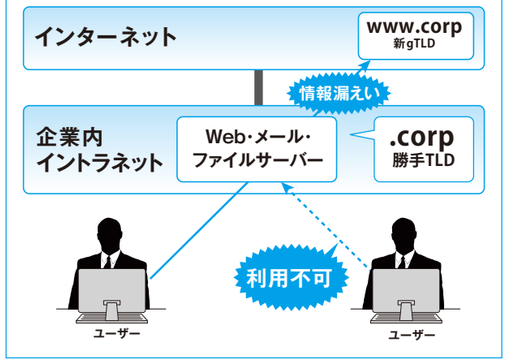



**図2-2:サーチリストを利用しているケース(新gTLDの登録後)**




こうした名前衝突が発生すると、さまざまな問題が起きる可能性が出てきます。例えば、次のような問題が想定されます(図3)。

**図3:名前衝突により想定される問題**




○ サービスが利用できない

- 企業のイントラネット上のサーバにアクセスできなくなる、メールの送受信ができなくなる。
- 内部的に勝手に利用していたTLDや短縮名を利用したサービスの挙動が変わり、ユーザーに提供しているサービスが正しく動作しなくなる。
- 勝手に利用していたTLDを含むドメイン名の証明書の新規発行や、発行済み証明書の利用ができなくなる。
- サーバ内部の設定でサーチリストによる短縮名使用時に、他サーバへの通信ができなくなる。
- イントラネット内部のエンドユーザーが、名前衝突する新gTLDにアクセスできなくなる。

○ 情報が漏えいする

- 組織内部のサーバのつもりが組織外部のサーバにアクセスし、情報漏えいを起こしてしまう。
- 社内で利用しているホスト名が外部に漏えいする。

## ◆ ICANNの対応

新gTLDを募集し、実際に追加を行うICANNは、この名前衝突の問題を重要視しており、新たなgTLDの追加を進めるにあたって、名前衝突への対策を行うことを決定しています。例えば、IT技術者向けの名前衝突の確認と回避策に関するガイドラインの作成や、名前衝突に関する情報の提供など、周知活動を行っています。[※7]

また、ICANNでは、次のような対策が採られています。

- .home、.corpについては、特に名前衝突の影響が大きいことが考えられるため、無期限に新gTLDとしての追加を保留
- 申請されたgTLDごとに、名前衝突の恐れがあるTLD名の調査を行い、リストの提示および対策の提案を実施
- 名前衝突のリスク評価と対応のフレームワークを構築し、新gTLD導入のプログラムにおいて適用

さらに、名前衝突の問題への対策として、次のような事項についても検討されています。

・.mail について新 gTLD への追加保留の検討
・IP アドレスにおけるプライベートアドレスのように、インターネットでは使われずに、組織内で自由に使うことができるプライベートドメイン名の検討

## ◆ 名前衝突への根本的対策

名前衝突の問題への根本的な対策は、TLD の重複を避けることです。つまり、原因となっている、内部向けの TLD やサーチリストの使用を止めることです。例えば、内部利用向けの TLD に関しては、インターネットで利用できるグローバルなドメイン名を使用することであり、サーチリストに関しては、その使用を止め、完全なドメイン名（FQDN）[※8] を用いることが対応策となります。

しかし、対策にはすでに稼働中のシステムを改修したり、サービス変更によるユーザーへの影響などが発生したりするため、対応の際には十分な検討や準備が必要です。

以降のセクションでは、対象者のケース別に発生する可能性のある問題と、その対応策について解説します。

## ◆ 対象者別に想定される問題と対応策

### 企業ネットワーク管理者

企業内と社外のネットワークを区別し明示するために、社内向けに内部目的の TLD を使っている場合や、短縮したドメイン名に対してサーチリスト機能でドメイン名を補完している場合に、次のような名前衝突の問題が発生する可能性があります。

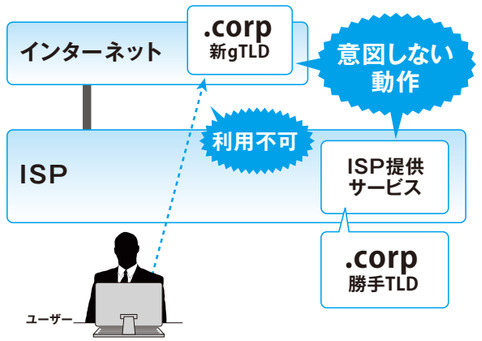
（1）企業内ネットワークの利用者が、名前衝突する新 gTLD にアクセスできなくなる
（2）内部目的の TLD や短縮名での利用を前提に構築されたシステムにおいて、誤動作やセキュリティ被害が発生する

いずれの問題も、ファイアウォール等を利用してインターネットと遮断し、ネットワークを分離することで回避できますが、将来の拡張性やインターネットとの接続性を考慮した場合、内部利用目的の TLD を利用せず、インターネットの DNS に登録されたパブリックなドメイン名を利用するように修正することが、望ましいと考えられます。

### ISP 運用者

ISP において内部目的の TLD を使っている場合、次のような問題が起きる可能性があります（図 4）。

**図4：ISP提供サービスと新gTLDの衝突**




（1）エンドユーザーが、名前衝突する新 gTLD にアクセスできなくなる

エンドユーザーのプライベートネットワークなどで、ネットワーク機器の設定用 URL などに、内部利用目的の TLD を用いた名前空間が使われていることがあります。その TLD で名前衝突が起きた場合、ユーザーは新 gTLD のサービスにアクセスできなくなります。こうした問題は ISP の問題ではなく、ユーザーのプライベートネットワークの問題であるため、ISP 運用者はユーザーサポートなどで問題の切り分け、解決策の誘導などが必要になる可能性があります。

（2）エンドユーザー向けサービスの挙動の変化

ISP が、自社ユーザー向けのサービスをプライベートな TLD を使ったドメイン名、例えば「www.service.isp」といったドメイン名で提供しているケースがあります。その TLD「.isp」と同じ文字列が、新 gTLD「.isp」として登録された場合、その ISP のキャッシュ DNS サーバは、「.isp」の名前を ISP 内部で解決するため、ISP のエンドユーザーは、新 gTLD「.isp」を使ったドメインにアクセスできないという問題が生じます。この問題への対策は、サービスに用いる TLD を、パブリックなドメイン名に変更することになります。

（3）ISP の内部ネットワークでの名前衝突

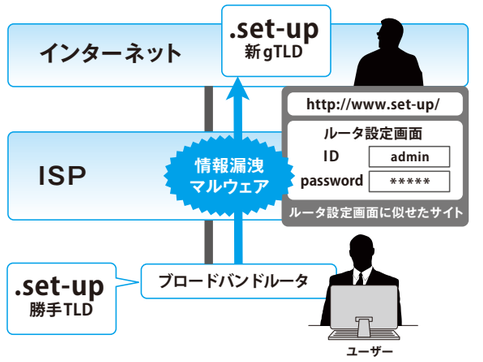
自社ユーザー向けではなく ISP の内部利用目的でプライベートな TLD を利用しているケースで、自社ユーザーの利用するキャッシュ DNS サーバが内部利用目的の TLD に対して名前解決を行うようになっている場合、名前衝突の問題が発生し、エンドユーザーはインターネット上の新 gTLD のサービスが利用できなくなります。この問題についても対応策としては、内部で勝手な TLD を利用せず、パブリックなドメイン名を利用するように変更することです。

### ネットワーク製品や情報家電等のベンダー

ルータなどのネットワーク製品や情報家電・ソフトウェアなど、ネットワークに接続される製品で内部利用目的のドメイン名を使っている場合、新 gTLD の追加と使用開始に伴い、これまで問題なく使えていた機能が突然使えなくなる可能性があります。

例えば、ルータ等の設定で「http://www.set-up/」のような URL にアクセスするような機器の場合、「.set-up」が新 gTLD として登録されると名前衝突の問題が起きることになり、ユーザーは新 gTLD のドメインにアクセスできなくなります。また、設定用 URL に用いられる TLD が実際に新 gTLD として登録され、悪意のあるサイトが構築された場合、上記の製品ユーザーはアクセスできないとしても、その他のユーザーはアクセスできるため、設定画面と誤認し、セキュリティ上のリスクが発生する恐れがあります（図 5）。

**図5：設定画面を装った外部Webに誘導されるケース**

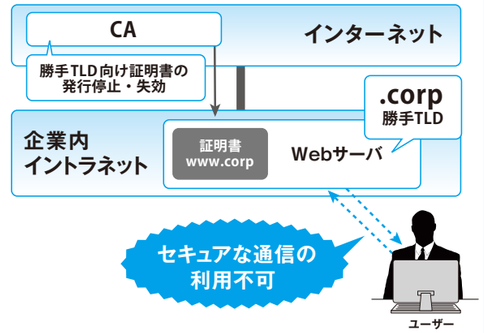



こうした問題に対策するためには、ドメイン名でのアクセス誘導ではなく IP アドレスで行う、もしくは設定用アプリケーションを配布し、このアプリケーションでネットワーク内の機器を検出し設定を行うなどの方法をとる必要があります。

### 証明書を利用している組織

これまではパブリックな DNS で名前解決できないドメイン名や、プライベート IP アドレスが記載されたサーバ証明書であっても、発行を受けることができました。しかし、今後は名前衝突の問題が発生する可能性があるため、各認証局ではそういった内部利用目的の証明書は発行せず、既存の内部利用目的の証明書も 2016 年 10 月までに失効されることになりました。さらに、ICANN から承認された新 gTLD を含む証明書については、ICANN とレジストリとの契約公開から 30 日以内に発行（再発行および更新も含む）が停止されることになっています。また 120 日以内に、同新 gTLD を使用したすべての証明書が失効されます。（図 6）

**図6：内部向け証明書の失効**




もし、そのような証明書を利用していて、自組織の証明書が失効した場合は、社内システムの改修や業務フローの変更など対応が必要になる可能性がありますので、確認が必要です。

内部利用目的のドメイン名を対象とする証明書をパブリック認証局から入手している組織は、パブリックな名前空間のドメイン名へ移行することが推奨されます。CA/Browser Forum[※9] の規定した証明書の発行基準である Baseline Requirements によると、以下の日程で対応が行われるとされています。

（1）2012 年 7 月 1 日以降発行された内部利用目的のドメイン名を対象とする証明書は、有効期限が 2015 年 11 月 1 日以降にならないようにする

（2）内部利用目的のドメイン名を対象とするすべての証明書は 2016 年 10 月までに失効する

### システムインテグレーター、ネットワークインテグレーター

システムインテグレーター、ネットワークインテグレーターに関しては、納入・運用するシステムの性質によって、ここまで説明してきた各問題いずれもが発生する可能性があります。それぞれの問題について切り分け、対応が必要になります。

## ◆ 日本国内での名前衝突に関する検討

この名前衝突の問題は、前述の通り新 gTLD の申請受付および登録を行っている ICANN でも、検討と対策が実施されています。しかし、問題の所在や情報の周知は、日本国内では十分なものではありませんでした。そのため JPNIC では、国内での本問題の検討および対策方法の周知を目的として、「新 gTLD 大量導入に伴うリスク検討・対策提言専門家チーム」を設立し、それらの問題に対応すべく活動を行いました。この専門

家チームは、DNSの運用やISP運用者、認証局業務などへの高い知見を持ったメンバーを中心に構成され、名前衝突問題の影響と対策を検討し、報告書として取りまとめました。

### 新gTLD大量導入に伴うリスク検討・対策提言 専門家チームメンバー 一覧

| 役割 | 所属 | 氏名 |
|---|---|---|
| 共同チェア | NTTコミュニケーションズ株式会社 | 外山 勝保 |
| | 株式会社インターネットイニシアティブ/<br>日本DNSオペレーターズグループ(DNSOPS.JP) | 山本 功司 |
| 検討メンバー | NTTコミュニケーションズ株式会社 | 近藤 和弘 |
| | 株式会社日本レジストリサービス | 佐藤 新太 |
| | 株式会社日本レジストリサービス | 松浦 孝康 |
| | 株式会社インターネットイニシアティブ/<br>日本ネットワーク・オペレーターズ・グループ(JANOG) | 松崎 吉伸 |
| | NTTコム ソリューション＆エンジニアリング株式会社 | 保多 洋 |
| | 株式会社インターネットイニシアティブ | 山口 崇徳 |
| 特定課題検討メンバー | クロストラスト株式会社 | 秋山 卓司 |
| | セコム株式会社IS研究所 | 島岡 政基 |

「新gTLD大量導入に伴う名前衝突(Name Collision)問題とその対策について」
https://www.nic.ad.jp/ja/dom/new-gtld/name-collision/name-collision-report.pdf

また、報告書の公開に合わせて内容を短くまとめた「概要編」、および名前衝突の問題について紹介するWebページも作成しました。対象者別に影響と対策をわかりやすくまとめておりますので、皆さまもぜひご一読ください。これらの資料を元に、JPNICでは周知活動を行っています。

「新gTLD大量導入に伴う名前衝突(Name Collision)問題とその対策について」概要編
https://www.nic.ad.jp/ja/dom/new-gtld/name-collision/summary.pdf

名前衝突に関するWebサイト
https://www.nic.ad.jp/ja/dom/new-gtld/name-collision/

## ◆ 最後に

名前衝突の問題は、内部利用目的のドメイン名とパブリックなDNSでのドメイン名が重複することであり、そうした状況が起こる可能性や問題の影響範囲は未知数です。また、その影響は新gTLDの申請者にとどまらず、それ以外の一般的なユーザーにまで広がる可能性が懸念されます。そのため、関係者の皆様におかれましては、自社やご自宅、あるいは周辺のシステムでパブリックなドメイン名を使用していないサービスがあるかどうかご確認いただき、もしあれば報告書やWebページをご参考に対処いただければと思います。また、名前衝突問題の存在をご存じない方もいらっしゃるかと思いますので、情報の周知にご協力いただければ幸いです。本問題に関して何かお困りの点がありましたら、また、JPNICがご協力できることがありましたら、下記お問い合わせまでお気軽にご連絡ください。

**問い合わせ先**
domain-query@nic.ad.jp

(JPNIC技術部 小山祐司)

※1 The Good Old Days：Networking in UK Academia ～ 25 Years Ago
http://www.uknof.com/uknof7/Reid-History.pdf

※2 IAB comment on stability of ISO 3166 and other infrastructure standards, 24 September 2003
http://www.iab.org/documents/correspondence-reports-documents/docs2003/2003-09-25-iso-cs-code/

※3 A Security Problem and Proposed Correction With Widely Deployed DNS Software
http://www.ietf.org/rfc/rfc1535.txt

※4 SAC 045 "Invalid Top Level Domain Queries at the Root Level of the Domain Name System"
https://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf

※5 申請された新gTLDの一覧
New gTLD Current Application Statusa
https://gtldresult.icann.org/application-result/applicationstatus

※6 委任済み新gTLDの一覧
Delegated Strings
http://newgtlds.icann.org/en/program-status/delegated-strings

※7 Name Collision Resources & Information
http://www.icann.org/en/help/name-collision

※8 FQDN(Fully Qualified Domain Name)
DNSの階層構造において、あるノードからルートまでのすべてのラベルを並べて表記したもので、日本語では「完全に指定された(限定された)ドメイン名」や「絶対ドメイン名」などと呼ばれる。

※9 CA/Browser Forum
電子証明書を使った通信の安全性や、その利便性を向上させるためのガイドラインを策定している、会員制の任意団体。
https://cabforum.org