IT 専門家のための名前衝突の確認および抑止方法ガイド

2013年12月5日　バージョン1.0

本文書は ICANN が発行している以下の文書を JPRS が翻訳したものです。

Guide to Name Collision Identification and Mitigation for IT Professionals

https://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-05dec13-en.pdf

株式会社日本レジストリサービス

http://jprs.co.jp/

2014 年 6 月 9 日　Ver. 1.0 (初版)

目次

1. はじめに

新しいトップレベルドメイン名がグローバルDNSルートに入ると、組織は自分のネットワーク固有の「内部利用名」を解決するためのクエリが異なる内容の応答を受ける可能性があり、ユーザーやプログラムに異なる結果をもたらすことがあり得ます。これには、基本的に2つの問題点が存在します。すなわち、グローバルインターネットに漏れ出す「内部利用名」と、グローバルDNSの名前空間と衝突する形で定義されたプライベートな名前空間です。

異なる結果が出る原因は、ネットワーク管理者が内部利用の名前空間を使ってローカルに解決していたDNSクエリが、グローバルDNSの新しいトップレベルドメインのデータを使って解決されるようになるからです。こうした理由から、内部ネットワークを出ることは決してないと見込んでいたクエリが、グローバルDNSから結果を受け取り、それらの結果が異なるという事態になります。小さな例としては、漏れた名前が異なる結果を出すことでユーザーにとって厄介な症状が起きます（たとえば、ウェブページへのアクセスが遅延する可能性があります）。また、これらはセキュリティの問題を引き起こすかもしれません（電子メールが間違った受取人に配信されるなど）。

本書は、組織がプライベートな名前空間を使っているよくあるケースについて、回避策と防止策を取り扱います。本書は、内部利用名がグローバルDNSに漏れたときに組織がどのようなことに遭遇するかを記述し、推奨される抑止方法を記述します。ここで提示されている内容や助言は、DNSがどのように動作するのか、自分の内部利用名システムがどのように動作するのかについて十分に理解しているIT専門家（ネットワーク管理者、システム管理者、およびIT部門のスタッフ）に向けたものです。背景についてもっとよく知りたい読者は、付録Aの文書を参照してください。セキュリティに興味がある読者は、特にICANNのセキュリティと安定性に関する諮問委員会（SSAC）が出しているレポートを参照してください。

ICANNは、グローバルDNSルートの内容を管理する組織であり、プライベートな名前空間がグローバルDNSルートと衝突するような組織を支援するため、名前空間問題の専門家と協議しながら本書を作成しました。他にもICANNは、グローバルDNSがどのように構成されるか、新しい名前がどのようにDNSルートに追加されるか等を記述した文書も発行しています。本書の付録Aには、さらに詳しく調べる人のために、多くのテーマに関する参考文献がリストアップされています。

本書は、名前衝突の抑止策を取り扱ってはいますが、組織が名前解決時に遭遇する可能性のある問題だけを論じている点に注意してください。本書は、グローバルDNS自体の運用に関連したその他の問題については取り扱っていません。たとえば、グローバルDNSのルートネームサーバーは、グローバルDNSで処理されることを意図していなかったクエリで常にあふれていますが（付録AのSAC 045を参照のこと）、このような余分なクリエにも回答できるようにルートネームサーバーは常に十分な余裕を持たせてあります。ルートネームサーバーに関する類似の問題は、本書では取り扱いません。本書では意図せずに公のDNSルートネームサーバーに誤送信されたクエリのことだけを取り扱っています。

ICANNは、名前衝突に関する参考資料を提供するためのウェブページを作成しており、http://www.icann.org/en/help/name-collisionで見ることができます。また、このページは、新しいジェネリックトップレベルドメイン（gTLD）によって引き起こされた名前衝突の結果として、明らかに深刻な悪影響があったことを報告するためのプロセスも記載しています。

1.1 名前衝突

グローバルDNSは階層的な名前空間であり、DNSの名前は、フルネームを作り出すための1つ以上のラベルから構成されています。階層の最上部には、com、ru、asiaなどの名前の集合を含んだDNSルートゾーンがあります。これらはグローバルTLD（トップレベルドメイン）で、一般的には単にTLDと呼ばれます。フルドメイン名（「完全修飾ドメイン名」（FQDN）と主に呼ばれます）は、たとえばwww.ourcompany.comのようなものです。

ほとんど全てのプライベートな名前空間も階層的です。プライベートな名前空間は主に以下の3種類があります。

- **グローバル DNS から分岐した名前空間**

  グローバル DNS から分岐したプライベートな名前空間は、グローバル DNS で解決可能な名前をルートとしていますが、その名前に基づいた全体的なディレクトリ構造はローカルに管理されており、IT 管理者としてはグローバル DNS への公開を前提としていないものです。たとえば、winserve.ourcompany.com をルートとしたプライベートな名前空間を考えてみましょう。そのプライベートな名前空間の名前（winserve）はプライベートなネームサーバーによって管理され、グローバル DNS からは見えません。

- **プライベート TLD を持つ独自のルートを使った名前空間**

  このプライベートな名前空間のルートは、グローバルTLDではない単独のラベルです。プライベートTLDも含めた全体のディレクトリ構造は、グローバルDNSからは見えないプライベートなネームサーバーによって管理されています。たとえば、プライベートな名前空間のルートがourcompanyであれば、プライベートなネームサーバーはwww.ourcompanyやregion1.ourcompanyやwww.region1.ourcompanyなども管理しています。プライベートTLDを持つ独自のルートを使った名前空間は、様々なタイプのものが存在します。その例としては、マイクロソフト社のアクティブディレクトリ（一部の構成において）、マルチキャストDNS（RFC 6762）および、まだ一部のインターネットで使用されている旧式のLANディレクトリサービスがあります。

- **サーチリストを使用して作成された名前空間**

  サーチリストはローカル名用リゾルバの一機能です（プライベートな名前空間とグローバルDNSのいずれの再帰的リゾルバにも使えます）。サーチリストを使うことで、ユーザーは、利便性のために短い名前を入力することができます。解決を行う際に、ネームサーバーは、クエリの名前の右に、設定された名前を追加します（これらの設定された名前のことを「サフィックス」と呼んでいます）。

グローバル DNS から分岐した名前空間は、サーチリストと組み合わせたときにだけ、名前衝突を引き起こします。グローバル DNS から来た FQDN を持つクエリは、定義上、グローバル DNS の別の名前と名前衝突を起こすことはありません。そのようなクエリが名前衝突を起こす可能性があるのは、サーチリストを使って不注意に作成されたときだけです。

「プライベートな名前空間」の概念は、典型的なインターネットの利用方法によく慣れている多くの人々を混乱させます。すなわち、グローバルDNSのネーミングだけに慣れている人々は、一部の名前解決のクエリがグローバルDNSへのクエリにならず、なってはいけないことを知れば驚くかもしれません。一部の名前のクエリは、プライベートな名前空間で意図的に開始されるようになっていますが、最終的にグローバルDNSまで行くことを知ったら、彼らはもっと驚くでしょう。名前衝突が起きる理由の一つは、プライベートな名前空間のネームサーバー向けに意図されたクエリが、誤ってグローバルDNSで開始されることにあります。

1.2 プライベート TLD による名前衝突

名前衝突は、2つのイベントの結果として発生します。まず、プライベートTLDをルートにした完全修飾ドメイン名のクエリが、プライベートネットワークからグローバルDNSに誤送信されま

す。次に、そのクエリがプライベートTLDに基づいたプライベートネットワーク上に存在する名前と全く同じ名前について、グローバルDNSで該当する場所を指し示します。

そのような名前衝突のよくある原因の一つは、マイクロソフト社のアクティブディレクトリのようなシステムで、システムを設定するときにはグローバルDNSのTLDではない名前を利用したが、後にグローバルDNSに追加されることにより発生します。このような種類の名前衝突は、すでに以前から何度も発生しており、グローバルDNSに新しいTLDが導入されるにつれて今後も続くと予想されています（付録Aの「新gTLDプログラム案内書」を参照のこと）。

1.3　サーチリストによる名前衝突

名前衝突のもう1つの原因は、サーチリスト処理です。クエリがFQDNでない場合、それは非修飾ショートネームです。サーチリストは、1つ以上のサフィックスを含んでいます。これらは、クエリの右側に反復的に付加されます。リゾルバが非修飾短縮名を解決できない場合、名前を解決しようとしてリストからサフィックスが付加され、マッチした名前が見つかるまでこれが続きます。サーチリストは便利な機能ですが、サーチリスト処理はFQDNでない非修飾短縮名を使うため、誤ってグローバルDNSのルートではない名前空間を作り出します。そのような場合、名前衝突は、ユーザーが非修飾短縮名として使おうとした文字列がサーチリストによって補完され、FQDNとして解決される場合に生じます。

たとえば、ourcompany.comおよびmarketing.ourcompany.comというサフィックスから構成されたサーチリストを、ネームリゾルバが持っていたと仮定しましょう。さらに、ユーザーが、そのリゾルバを使っているプログラムにwwwを入力したと仮定します。そうすると、リゾルバは最初にwwwを検索し、それで結果が返送されなかったら、ourcompany.comおよびmarketing.ourcompany.comを検索するかもしれません。

この例の記述に「かもしれません」という言葉を使ったことに注意してください。名前解決を行うときにサーチリストがどのように適用されるかというルールは、OSやアプリケーションによってまちまちです。一部のシステムは、サーチリストを適用する前に、常にプライベートな名前空間またはグローバルDNSのどちらかで名前を解決しようとします。しかし、別のシステムは、サーチする文字列が“.”文字を含んでいなければ、最初にサーチリストを使います。さらに他のシステムでは、サーチする文字列が“.”文字で終わっていれば、サーチリストを使います。一部のOSおよびアプリケーション（ウェブブラウザなど）は、自分のサーチリストのルールを何度も変更してきました。したがって、サーチリストがいつ使われ、いつ使われないか、どれが非修飾短縮名で、どれがそうでないか、非修飾短縮名がグローバルDNSに漏れる可能性が高

いかどうかを予測することは困難です。サーチリスト処理の詳細な多様性については、付録Aの「新gTLDの問題点：ドットレス名と名前衝突」を参照してください。

このようなサーチリストの説明は、一部の読者を驚かせるかもしれません。なぜなら、その機能は一見して「プライベートな名前空間」を作成しているとは思えないからです。サーチリスト内の全てのサフィックスは、名前解決中に調べることのできる別の名前空間を定義します。これにより、クライアントがその名前空間の特定リゾルバにクエリを出した時だけ確実に動作するプライベートな名前空間が作成されます。サーチリストの実装によっては、一部のネームリゾルバは、サーチリストの名前のどれかを付加する前に、ユーザーが入力あるいはソフトウェアで設定された非修飾短縮名の名前解決を試行するかもしれません。たとえば、インターネット上のある場所でwww.hrをタイプすると、DNSリゾルバからある1つの結果が得られ、異なる場所で同じものをタイプすると別の結果が出てくるかもしれません。これらが発生する場合、その名前空間の1つは他方とは相対的にプライベートな空間となります。

グローバルDNS経由でFQDNの解決をせずにサーチリストを使うと、名前解決における不確実性の一因となります。サーチリストによって発生する名前衝突は、サーチリストが非常によく使われているため、予測が困難です。これらは、多くのOS、ネットワーク機器、サーバーなどで名前解決のソフトウェアの一部となっています。名前解決のソフトウェアは、システムによって異なる動きをし、同じOSでもバージョンによって異なります。また、クエリがネットワーク上のどこから来たか、OSの機能やアプリケーションの視点での解釈によっても異なります。グローバルDNSだけを使って名前解決を行うサービスを適用することは、このような結果の予測不能性や不確実性を避ける最も確実な方法です。

2　名前衝突によって引き起こされる問題

プライベートネットワークからグローバルDNSに誤送信されたクエリに基づく名前衝突は、多くの思いがけない結果を生み出す可能性があります。クエリが、予想したプライベートな名前空間ではなくグローバルDNSから肯定的な応答を受け取った場合、そのクエリを出したアプリケーションは、プライベートネットワークの一部ではないシステムに接続しようとし、それに成功するかもしれません。このような接続は（名前解決中の遅延を引き起こすので）厄介なことになりかねません。また、セキュリティの問題が生じる可能性があります。すなわち、そのアプリケーションが接続後に何か行うことを当てにして、悪意の目的で不当に利用されかねない脆弱性を作り出します。

2.1　予期しないウェブサイトへの接続

ユーザーが、プライベートネットワークにいるとき、自分のウェブブラウザにhttps://finance.ourcompanyと入力し、ネットワークがourcompanyというプライベートTLDの名前空間を持っていたと仮定しましょう。finance.ourcompanyに対するブラウザのクエリが期待された通りに解決されると、ブラウザはファイナンス部門の内部ウェブサーバーのIPアドレスを受け取ります。しかし、TLD ourcompanyもグローバルDNSの一部であり、そのTLDがセカンドレベルドメイン（SLD）名financeを持っていたとします。クエリが誤送信されると、クエリがプライベートな名前空間で解決された時とは別のIPアドレスに解決されます。ここで、この異なるIPアドレスがウェブサーバーのホストであったとすると、ブラウザは、プライベートネットワーク上ではなく公なインターネット上のウェブサーバーに接続しようとするでしょう。

前述の通り、プライベートTLDは持っていないがサーチリストを使っているネットワークで、同じ問題が起きる可能性があります。名前ourcompany.comを持つサーチリストをユーザーが使っているような一般的なネットワーク上で、ホストwww.finance.ourcompany.comに行くためにユーザーが名前www.financeをブラウザに入力したとしましょう。ここでは喫茶店にいる従業員がモバイル機器からブラウザを使っていたと仮定します。このクエリがインターネットに誤送信されて、financeという名前のTLDが存在していた場合、異なるIPアドレス、たとえばグローバルDNSでの名前がwww.financeであるような全く異なるホストにクエリが解決される可能性があります。そのクエリにより、ブラウザは、クエリがプライベートネットワーク上のリゾルバに向かった場合とは全く異なるパブリックネットワークの一部にあるウェブサーバーに接続しようと試みるでしょう。

このシナリオに対するユーザーの一般的反応は、そのユーザーはこれが間違ったウェブサイトであることに気が付き、すぐにそこから離れるだろうというものでしょう。しかし、ウェブサーバーは以前にブラウザが訪問したのと同じドメイン名を持っているため、ブラウザがウェブサーバーを「信用」し、ブラウザはウェブサーバーへ大量の情報をさらしてしまいます。ブラウザは、自動的にログインやその他の機密データを入力し、それによってその情報が組織外部で収集や分析されてしまいます。他の状況では（たとえば、入念に仕組まれた組織への攻撃など）、ブラウザは、コンピュータ上に危険なプログラムをインストールする悪意のあるコードをホストしているサイトに接続するかもしれません。

TLSおよびデジタル証明書を使っても、名前衝突による損害を防止するのに役立たない可能性があることに注意してください。実際に、これがユーザーに誤った安心感を与えるため、事態をもっと悪くするかもしれません。グローバルDNSの名前への証明書を発行する認証局

（CA）の多くは、プライベートなアドレス空間で非修飾ショートネームの証明書も発行しているので、常に有効な証明書にみえるサイトにユーザーを導くことも可能です。プライベートな名前空間からの名前を持つ証明書についての詳細は、付録AのSAC 057を参照してください。

2.2　間違った受取人へのメール配信

名前衝突から生じうる結果は、ウェブブラウザだけに限りません。ある受取人宛の電子メールは、受取人のアドレスのホスト名が一緒であれば、別の受取人に送信される可能性があります。たとえば、chris@support.ourcompany宛の電子メールは、ourcompanyがグローバルDNSのTLDになれば、全く異なるユーザーアカウントに配信されるかもしれません。メッセージが特定の電子メールユーザーに配信されなかった場合でも、送信しようとする試行があれば、そのような試行によって電子メールの内容が組織外部で収集または分析される恐れがあります。

ファイアウォールやルーター、さらにはプリンタのようなネットワーク機器の多くが、電子メールで通知またはログデータを送信するように設定されている可能性があります。後で電子メール通知用に入力された受取人の名前が、グローバルDNSで名前衝突を起こすと、通知はまったく意図しない受取人へ配信されてしまうかもしれません。ネットワーク設定やホスト動作を記されたメッセージ本体のイベントまたはログデータが、思いがけない受取人に誤送信されてしまう可能性があります。ITスタッフが定常的に行うネットワークパフォーマンスやトラフィック分析において、そのようなデータの正式な受取人がログデータを受信しなければ、分析が中断してしまうことになります。または、通知のトリガーとなるイベントの調査や対策が行われない可能性があります。

2.3　セキュリティの低下

対策が行われないままになった名前衝突のイベントは、プライベートネットワークのシステムでの予期しない動作または損失を引き起こしかねません。名前解決が正しく動くことに依存しているシステムやセキュリティ機能を担うシステムは、FQDNを使いグローバルDNSから名前解決する場合に高い信頼性で動作ができます。

たとえばファイアウォールでは、セキュリティルールは、パケットフローの発信元または送信先をベースにしています。パケットの発信元および送信先はIPv4またはIPv6ですが、多くのファイアウォールはドメイン名も入力できるようにしています。非修飾短縮名が使われ、名前解決が期待された通りに実施されなかった場合、管理者が意図した通りにトラフィックの遮断や許可がルール通りに適用されない可能性があります。同様に、ファイアウォールのログはドメイ

ン名を使うことが多く、予測不可能な方法で解決される非修飾短縮名を使うと、イベント監視、分析または対応を阻害することがあります。ログをレビューするITスタッフは、たとえば、ログが作成された場所に応じてログの非修飾短縮名が異なるホストを識別するため、イベントの深刻度を誤解するかもしれません（すなわち、ログでは、同じ非修飾短縮名が複数の異なるIPアドレスに対応して現れる可能性があります）。この問題は、ほとんどのファイアウォールが自身のDNSリゾルバを動作せることができ、または管理者がサーチリストを利用または設定できるため、さらに悪化する恐れがあります。

2.4 名前衝突で影響を受けるシステム

ネットワークに接続された全てのシステムは、プライベートTLDをルートにしたホスト名を使っているか、またはサーチリストをベースにしたホスト名を使っているかについて、チェックすべきです。これらを使っている事例については、すべて、グローバルDNSからのFQDNを使うように更新する必要があります。チェックすべきシステムまたはアプリケーションを以下に列挙しますが、これで全てではありません。

- ブラウザ

  ウェブブラウザではユーザーがHTTPプロキシの場所を指定でき、そのHTTPプロキシはほとんどの場合プライベートネットワーク上にあります。ユーザーまたはITスタッフによって作られたカスタムのホームページ、ブックマークまたはサーチエンジンがあるかどうかをチェックしなければいけません。これらは、プライベートネットワーク上のサーバーへのリンクを持っているかもしれません。また、一部のブラウザは、プライベートネットワーク上のホスト名を指したSSL/TLS証明書に関して、失効情報をどこで取得するかを設定するオプションも持っています。

- ウェブサーバー

  ウェブサーバーは、ホスト名が埋め込まれたメタデータおよびリンクを持つHTMLコンテンツを提供します。プライベートネットワーク上のウェブサーバーが非修飾短縮名を使ったコンテンツを持っているかどうかをチェックしてください。ウェブサーバーの設定ファイルが、プライベートネットワーク上の他のホストの非修飾短縮名を使っているかどうかをチェックしてください。

- 電子メールユーザーエージェント

「Outlook」や「Thunderbird」のような電子メールクライアントは全て、POPまたはIMAPプロトコルを使ってどこで電子メールを受け取るか、SUBMITプロトコルを使ってどこで電子メールを送信するかについての設定オプションを持っています。これらは全、プライベートネットワークのホスト名を使っているかもしれません。これらのアプリケーションが、非修飾短縮名を割り当てたホストからSSL/TLSに関する失効修復情報を取得するように設定されているかどうかをチェックしてください。 (訳注: 原文のまま。証明書関連の内容は記載場所の間違いか?)

● 電子メールサーバー

電子メールサーバーが、バックアップの電子メールゲートウェイ、オフラインのストレージサーバーなど、他のローカルホストの非修飾短縮名をリストした構成を持っているかどうかをチェックしてください。

● 証明書

音声通話およびインスタントメッセージングプログラムなど、X.509証明書を使ったアプリケーションが、SSL/TLS証明書の失効情報をどこで取得するかを示す非修飾短縮名を使った設定情報を持っているかどうかをチェックしてください。

● その他のアプリケーション

カスタムアプリケーションは、ホスト名が格納できる設定パラメータをたくさん持っている可能性があります。最も明確な場所は設定ファイルですが、多くの種類のアプリケーション情報、ソーシャルメディアまたはウィキサイトのリンク、またはソースコード内のハードコードにおいてもホスト名が現れる可能性があります。これらの設定情報において非修飾短縮名をチェックしてください。

● ネットワーク機器

ファイアウォール、セキュリティ情報およびイベント管理（SIEM）システム、ルーター、スイッチ、ネットワーク監視装置、侵入検知または防止システム、VPNサーバー、DNSサーバー、DHCPサーバー、ログサーバーのネットワーク基盤機器をチェックし、これらがプライベートネットワーク上の他の機器の非修飾短縮名を使って設定されているかどうかを確認してください。

● クライアント管理

組織のワークステーションやネットワーク機器を設定する集中クライアント管理ツールが、システムを制御したりリセットする設定に非修飾短縮名（特にサーチリスト）を持っているかどうかをチェックしてください。

- モバイル機器

電話やタブレットなどのコンシューマ機器は、上記のアプリケーションの一部と同じ設定オプションを持ち、これによってローカルネットワークから非修飾短縮名を含んだ設定を選択している可能性があります。

これらのシステムの全ては、非修飾短縮名を持つ設定データがないかどうかをチェックし、プライベートな名前空間のルートが変更されたとき、またはサーチリストが使われなくなったとき、そのような名前を変更できるようにすべきです。

3 名前衝突の抑止を実施する時期

国の名前が変更されたときやICANNが新しいTLDを委任したときなどに、グローバルDNSルートゾーンにTLDが追加されます。両種のTLDとも、この20年以上の間、ほぼ毎年のように追加がされてきました。今年（2013年）は新しいTLDが追加され、2014年以後もさらに追加が予定されています。

過去にTLDがDNSへ追加されたとき、いくつかの名前衝突が起きていることが判明しています。また過去には、プライベートの名前空間から長年にわたって名前が漏れており、一部のケースでは非常に高い頻度であったことが示されています。詳細については付録AのSAC045を参照してください。これまでの歴史では、プライベートネットワーク用の名前空間と名前解決が、管理者が考えているほどには十分に隔離されておらず、管理者が内部のネームサーバーで解決するように意図したクエリが代わりにグローバルDNSのリゾルバにたびたび送信されていたことが明らかになっています。

ネットワーク管理者は、グローバルDNSのルートにある名前のリストが不変であるという前提に基づいて名前を選択することが多いようですが、実際には時と共にリストは変化します。たとえば、csのTLDが約25年前にチェコスロバキア国として追加されたとき、多くの大学はサーチリスストを用い、コンピューター科学(Computer Science)部においてユーザーがcsで終わる名前を入力しても大学のドメイン名で完全修飾されるようにしていました。そうした状況でcsで終わる名前がグローバルDNSにおけるFQDNとなりました。これは新しいTLDをルートゾー

ンに加えることが名前解決の不確実性を生み出す結果となる例です。現在のグローバルDNSのTLD名がプライベートの名前空間（プライベートTLDまたはサーチリスト）にある名前とほとんど重複してこなかったことから、ネットワーク管理者は、どの名前がグローバルDNSのルートにあるかについて最新の情報を知ることを忘れがちです。

IT部門は、できるだけ速やかに抑止対策を始めることが望まれます。「我々は自分のファイアウォールの改善だけをする」という姿勢を取ると、ある程度の衝突を減らすことはできても、全てを根絶することは絶対にできません。同様に、「我々はユーザーが確実に我々のネームサーバーを使うようにする」とか「遠隔地の利用者がVPNを使うようにする」というのも、一部の衝突を減らし得ますが、残りの衝突の診断を難しくさせる可能性があります。

名前衝突は、名前に使われる文字種とは無関係に発生しえますが、プライベートTLDに「ä」や「中」や「ŭ」などの非ASCII文字を使うと、衝突の分析が複雑になります。リゾルバは、予測しがたい、インターネットの標準に一致しないようなやり方でこれらのクエリを送出するかもしれないため、いつ名前衝突が起きるかを見つけるのがいっそう難しくなります。

グローバルDNSのルートは以前よりずっと拡大するでしょうが、ルートにTLDを加えることはそれほど珍しいことではありません。新しいTLDが加えられるたびに、ほとんどの場合気づかれることなくインターネットに漏れているプライベートの名前空間との名前衝突が発生する可能性があります。長年にわたってこのような名前を使ってきた多くの組織は、衝突のリスクを負ってきました。

グローバルDNSのFQDNをすでに自分のネットワークに使っている組織にとっては、新しい名前がDNSルートに加えられても問題ではなく、今後も問題になることは絶対にない点に留意してください。これらの組織は名前衝突がないため、自分たちがDNS名を使うことに何の影響もありません。問題があるのは、プライベートTLDを使っている組織、または短くした名前がグローバルDNSの有効な名前でもあるような非修飾短縮名を入力できるようにしたサーチリストを使っている組織です。

3.1　衝突の可能性の確認

組織のプライベートの名前空間との名前衝突があるかどうかを確認するためには、組織が使っているプライベートの名前空間とDNSサーチリストの全てを特定し、リストにして、これらのソースでトップレベル名のリストを作成する必要があります。ほとんどの組織では、1つプライベートTLDによる名前空間を1つ使っているのが典型的ですが、特にプライベートの名前空間

を使っている他の組織と組み合わせられた組織（たとえば、事業統合または買収の結果）では、複数のプライベートTLDを持つことがあります。

次に、グローバルDNSゾーンの現在のコンテンツおよび予想されるコンテンツの両方を確認する必要があります。グローバルDNSの現在のルートゾーンにある名前は、http://data.iana.org/TLD/tlds-alpha-by-domain.txtで見つけることができます。プライベート名空間の名前が、2013年に活動している新gTLDプログラムで割り当てが検討されているかどうかを確認するには以下の手順を実行してください。

1. https://gtldresult.icann.org/application-result/applicationstatusへ行く。
2. "String"カラムの矢印をクリックする。
3. 自分のプライベートの名前空間の名前を持つレンジが出てくるまで、ページをスクロールする。

作成したプライベートTLDのリストとDNSゾーンの名前のリストの間に重複があった場合、名前衝突の可能性があるため、抑止対策が必要となります。

現行ラウンドの新TLDがルートゾーンに入れられた後でもさらに多くのものが提案されるため、新TLDのリストが変化し、プライベートの名前空間と今後の新TLDとの間で名前衝突が起きる可能性があります。また、2文字から成るプライベートTLD（たとえばab）を持つ組織は、2文字のトップレベルドメイン名は国コードに使用するために予約されており、全く異なる手続きを介してルートゾーンに加えられることを知っておくべきです。

4 プライベート TLD に関連した問題を抑止する手順

数十年にわたって、プライベートTLDを使うことはベストプラクティスとして推奨されてきませんでした。事実、マイクロソフト社のアクティブディレクトリやサーバー製品に添付されている説明書では、長年にわたってプライベートTLDを使わないことを明示的に推奨してきました。プライベートTLDで終わる名前がグローバルDNSへ漏れることによる名前衝突に最も効果的な抑止策は、プライベートTLDを使うのを止めてグローバルDNSをルートとしたものに変えることです。このセクションの手順は、内部的な理由によってグローバルDNSの名前空間をルートにしてFQDNの解決のためにグローバルDNSにクエリを出すことをせず、代わりにプライベートTLDをルートとして使い、サーチリストを使って非修飾短縮名を解決しているどんなネットワークにも当てはまります。

本セクションの内容は、すでに名前解決のクエリがグローバルインターネットに誤送信されている組織だけでなく、プライベートTLDを使用しているあらゆる組織に当てはまります。自分の組織が「安全」と考えているプライベートTLDを使っている場合、すなわち、グローバルDNSルートへの申請や承認がされているわけではないような名前を使っている場合であっても、グローバルDNSをルートとする名前へ変更することを真剣に検討すべきです。複数のプライベートTLDを持つ大組織で働いている人は（たとえば、別の会社と合併になったが内部の2つの名前空間を統合していない会社など）、本セクションの手順をそれぞれのプライベートTLDについて実行しなければいけません。

組織がプライベートTLDを使うことにした場合、おそらく特定の命名規則を念頭に置いてそれを行ったでしょう。本セクションの手順は、そのような独自のやり方と対立する可能性があります。プライベートTLDを原因とした名前衝突に関連する問題を十分に抑止するためには、ユーザーとシステムの両方ともがドメイン名の使い方を変更する必要があり、ローカルのネームサーバーは、一部のユーザーが不便と感じるかもしれないようなやり方で再設定する必要があります。組織に影響を与えかねない、予期せぬ、望ましくない結果についての説明をすることで、利用者の認知度を上げて受容を促進すべきです。

重要な注：

本セクションの手順を実行するのと同時に、サーチリストが原因となる名前衝突を抑止する必要があるかもしれません。それに関しては、セクション 5 で記述しています。そのセクションにある多くの手順は本手順と同様であり、同時に実行することができます。

4.1　権威 DNS サーバーに入るクエリを監視する

プライベートTLDの問題を抑止するためには、コンピュータ、ネットワーク機器、および現行のプライベートTLDをリクエストに使っているその他のシステムを全てリストアップしなければいけません。使用中の名前を変更する場合、古いプライベート名を自動的に使っている全ての機器を更新する必要があります。

このようなシステムのモニタリングおよび列挙を行う方法としては、以下に示す3つの一般的な方法があります：

- 権威DNSサーバー（たとえばアクティブディレクトリ）は、ロギング機能を持っている場合があります。プライベート名の全クエリの詳細を収集するために、ロギング機能をオンにしてください。

- 多くの新しいファイアウォールは、プライベート名のクエリを検出し記録するように設定できます。これは、ネットワークのトポロジーによっては、名前解決のシステム自体で行うロギングほど効果的でないかもしれません。たとえばクエリがファイアウォールに到達しなければ、ファイアウォールはクエリを見ることができずに見逃すでしょう。

- 上記のどちらも使えない場合、Wiresharkのようなパケット取得プログラムを使って、権威ネームサーバーとの間で送受信されたトラフィックを監視し収集してください。しかし、この方法はプライベート名のクエリだけを見つけるためには、取得したデータをプログラムで処理する必要があります。

一部の組織では、全てのクエリを見つける可能性を増やすため、上記の2つ以上を選ぼうとする（そして選ぶべき）でしょう。この手順は、混乱しやすい結果を招くかもしれないことに注意してください。コンピュータや電話のような機器は、ユーザーが名前を入力するようなアプリケーションを持っています。これらの機器は、古いプライベート名が何処にも保存されていない場合であっても、調査の際に姿を現します。この手順では、アプリケーションで古いプライベート名が保存され使用されているネットワーク上の場所を全て知ることが目的となります。

4.2 プライベート TLD を使う各システムのインベントリ情報を自動化されたやり方で作成する

前述の手順で取得したログデータのサマリーが必要となります。そのサマリーは、クエリを出す機器の全要素ではなく、クエリを出した全ての機器およびその出した名前のリストとすべきです。クエリされた全ての名前が必要なのは、一部の機器は解決する必要のあるアプリケーションを複数持っていることがあるためです。したがって、サマリーは、全てのシステムと、プライベートTLDを使っている各システム上の全アプリケーションの両方を含んでいなければなりません。このサマリーは、変更を必要とする機器のインベントリ情報となります。

4.3 グローバル DNS 名がどのように管理されているか確認する

おそらく読者は、すでに組織のグローバルDNS名を持ち、プライベートな名前空間のルートにそのドメイン名を使えるようになっているでしょう。読者は、DNS名を担当しているのが誰か、DNSの名前を登録し更新するのにどのようなプロセスを使っているかを確認する必要があります。これは、IT部門内で実施されているかもしれませんし、サービスプロバイダ（多くの場合、自分のインターネット接続を提供してもらっている会社と同じである）を介して実施されているかもしれません。

4.4 プライベートの名前空間のルートをグローバル DNS の名前を使うように変更する

グローバルDNSをプライベートの名前空間のルートとして使うための一般的方法は、グローバルDNSから委任された公にアクセス可能な名前を用い、既存の権威DNSサーバーを使ってその配下にある全ての名前を管理することです。たとえば、ourcompany.comというグローバルなドメイン名を持つ会社の場合、ルート名としてad1.ourcompany.comを選んでもよいでしょう。

組織がグローバルDNSに複数のドメイン名を持っている場合、組織内のITスタッフが最も簡単に制御できるものの配下にある名前をルートにすべきです。一部のケースでは、追加の名前が、たとえばマーケティング部門のような別の部門で制御されている場合があります。可能であれば、すでにIT部門の制御下にある名前の配下で、自分の名前のルートにするのがベストです。

この変更を行うための手順は、持っているプライベートネームサーバーのソフトウェア、そのソフトウェアの特定バージョン、プライベートネットワーク上にあるネームサーバーのトポロジー、ネームサーバーの既存設定に依存します。これらの詳細は、本書の範囲を超えており、現行システムのベンダーが出している説明書で記載されるべきです。また、多くの組織では、特にグローバルDNS名の管理とプライベートの名前空間の管理とが分かれている場合、このような変更を行う前に一定レベルの管理職から許可をもらう必要があります。

本手順の一部として、プライベートの名前空間の名前を使っているホストの証明書を持っている場合、新しい（完全修飾の）名前を使うこれらのホストの証明書を作成する必要があります。これらの証明書を入手するための手順は、自身のCAに依存しており、したがって本書の範囲ではありません。

4.5 必要に応じ、ホストに新しい IP アドレスを割り当てる

古いプライベートTLDの名前に基づいたTLS証明書を持っている場合、新しい名前のための証明書を新たに取得する必要があります。ウェブサーバーが、同じIPアドレスのTLSにおいて複数のドメイン名が使えるよう、TLSのサーバー名表示（Server Name Indication、SNI）拡張機能をサポートしていない場合、元のIPアドレス上の古いプライベート名および新しいIPアドレス上の新しい名前をホストがサポートできるようにするため、IPアドレスをホストに追加する

必要があります。または、ウェブサーバーソフトウェアを、SNI拡張機能が正しく取り扱えるバージョンに更新することもできます。

4.6 新旧のプライベート名が同値であることを監視するためのシステムを作成する

新しいルートを使うために全てのプライベート名を変更した場合、インベントリ情報に入っておらずDNSをルートとした名前に更新されていないシステムを確認するため、古いプライベート名に対するアドレスの提供を続け、クエリを記録し続けます。これには、古いプライベート名と新しいプライベート名が同じIPアドレスの値を持っていることを確認する必要があります。

一部のプライベートな名前空間向けのソフトウェアは2つのツリーを平行して保持することが可能ですが、古いソフトウェアまたは複数の権威DNSサーバーを持っている場合、カスタムツールを使って同値であることをモニターしなければならない可能性が高くなります。これらのカスタムツールは、新旧の両方の名前空間で全ての名前に頻繁にクエリを出し、不一致があれば警告を出すことで、他方のシステムと平行した形で変更されなかったシステムを突き止めるようにする必要があります。

前の手順において、SSL/TLS証明書を持ことによりIPアドレスを追加する必要があった場合、同値監視ソフトウェアでは不一致を許容する必要があります。

4.7 新しい名前を使えるようにユーザーおよびシステム管理者を訓練する

設定に名前を入力するようなシステムを変更することに加えて、ユーザーが古いプライベート名を新しいものに切換えできるようにするため、ユーザーの考え方を変える必要があります。このようなトレーニングは、ユーザーが新しい名前に慣れる機会を作るため、以下の手順を実施する前に行うべきであり、トレーニングでは、変更が実施されつつあり、すぐに新しい名前の考え方を取り入れるようにすべきであることを明確にする必要があります。また、これは、FQDNの使い方をユーザーに訓練する良い機会でもあります。組織に影響を与えかねない予期せぬ望ましくない結果についての説明をすることで認知度を上げて受容を促進すべきです。

4.8　関連システムを全て新しい名前に変更する

この時点において、古いプライベート名から新しい名前への移行がネットワーク上の全てのシステム（PC、ネットワーク機器、プリンタなど）に実施されます。プライベート名は、システム単位で新しいDNS名に置き換えられます。システム上の全てのソフトウェアにあるプライベート名の全ての要素は、新しいDNS名と置き換えられます。同時に、サーチリストによる非修飾短縮名の利用は廃止すべきです。

上記までに開始された監視は、本手順にとってきわめて重要です。あなたが古いプライベート名を埋め込んだ全てのシステムの全てのアプリケーションを確認できる可能性は高くありません。その代わり、各システムを変更した後にシステムがまだ古いプライベート名のクエリを出すかどうかを監視システムで調べる必要があります。

多くのシステムは、最初に実行される時、いくつかの初期化アプリケーションを実行します。これらのアプリケーションは、内部にシステム名を埋め込んでいる可能性があり、それらを全て見つけだすのは困難になりかねません。システムの全ての名前を古いプライベート名から新しいDNS名へ変更した後、システムをリブートし、監視ソフトウェアを使って名前解決を監視してください。システムが何らかの古いプライベート名の名前解決をしている場合、どのソフトウェアがそのクエリを出しているかを突き止め、新しい名前を使うようにそれを変更する必要があります。このプロセスは、システムを全て正しく設定するために、何度がリブートを行うことになるかもしれません。

4.9　ネームサーバーで古いプライベート名の利用の監視を開始する

古いプライベート名に関する全てのクエリの監視を開始するよう、権威ネームサーバーを設定します。ユーザーはこれらの名前を使わなくなっているはずであり、この監視によって作成されるログはそれほど大きくならないでしょう。もし大きくなるようであれば、ネットワーク上の特定システムについて、上記の手順のいくつかを繰り返す必要があるかもしれません。

4.10　古いプライベート名を監視するために周辺での長期的監視を行う

これまでの手順によって、古いプライベート名の利用の大部分を見つけだしたはずですが、いくつかの（おそらく主要な）システムは、ごくたまにではありますが、古いプライベート名をまだ使っている可能性があります。これらの名前解決のクエリを検出する方法の1つは、ネットワークの外部接続点にある全てのファイアウォールにルールを追加し、誤送信されているリクエストを探し出すことです。このようなルールは、高いプライオリティを付けておくべきであり、IT

スタッフに迅速に警告を出せるように、イベント通知が生成できる設定にすべきです。別の方法として、これらのイベントをファイアウォールのログで見つけることも可能ですが、それをやると失敗の確率が高くなります。リクエスト発生時をトリガーとした警告により、スタッフはおそらく極めてまれとなったイベントを検出することができます。一部のファイアウォールは、追加費用で機能を付加しないと、このタイプのルールをサポートしません。自分のファイアウォールがそうであれば、迷子になったリクエストを見つけることの利益が追加費用に値するかどうかを評価する必要があります。

4.11 全ての古いプライベート名を機能しないアドレスを指すように変更する

ユーザーを訓練した後、古いプライベート名を除去する前に彼らが古いプライベート名を使わなくするための最も効果的な方法は、全ての古いプライベート名をどのような種類のサービス要求にも反応しないように設定したサーバーを指すようにすることです。これは、まだ古い名前空間を使っているが、これまでの手順で検出されなかったシステムを一掃するのにも役立ちます。

指し示すアドレスは、どんなサービスも実行していないことが保証されたサーバーとすべきです。これを行うことで、古いプライベート名を使っているシステムが誤った情報を受け取る可能性がなくなり、アプリケーションが簡単に検出できるエラーを報告するか、ユーザーが理解できるようになります。認知度向上のトレーニング中に、ユーザーにこの種のエラーを全てITスタッフに報告するように推奨できます。この手順が実施されるとき、新旧の名前の同値をチェックするモニタリングシステム（上述）は、変更について最新の情報を維持する必要があります。

名前の変更は一度に1つずつとし、毎回の変更または変更のバッチの間隔を少なくとも数時間にはすべきです。この手順はIT部門へ電話が入る可能性が高いですが、このように変更を段階的にすることで、まだ使用されていた名前の機能停止が順番になり、電話の負荷を分散できるようになります。

4.12 古いプライベート名でホストに証明書が出されている場合、それらを無効にする

組織が、古いプライベート名を使っているネットワーク上のサーバーにSSL/TLS証明書を持っていた場合、それらの証明書を無効にすべきです。組織が自分でCAとして活動しているなら、これをやるのはとても簡単です。商業CAを使ってプライベートの名前空間に証明書を発行してもらった場合、そのCAの失効要求プロセスを確認する必要があります。CAによって、そのような要求に対する要件が異なっている可能性があります。

4.13 新しい名前を使った長期運用

古いプライベート名およびその配下にあるドメインは、まだ提供されており、ネームサーバーを動かしているかぎり今後も提供され続けることに注意してください。これらを除去する理由はなく、アクティブディレクトリなどの多くのシステムにおいて、システムに設定された最初の名前を除去するのは困難である可能性があります。

実際に、名前をそこに残しておくだけの十分な理由があります。すなわち、これにより、ネットワーク上のシステムにある古いプライベート名の残留痕跡があるかどうかを確認することができます。そのプライベートTLD配下の全ての名前に対応した全てのアドレスがサービスを実行していないホストを指し示しているかぎり、ネームサーバーの両方のログ（およびそのサーバーへの全てのトラフィックを記録するシステムを使うことでさらに）を使うことで、古いプライベート名を十分に除去できたかを確認することができます。

5 サーチリストに関連した名前衝突を抑止する手順

サーチリストが原因の名前衝突に関する問題を高い信頼性で抑止するためは、ユーザーおよびシステムはドメイン名の使い方を変更する必要があります。変更通知、認知度プログラム、およびトレーニングを使って、前もってユーザーに準備させることが役に立つかもしれません。

すでに集中管理を行っている場合、これらの処置は、おそらく読者が想像するほど難しくはありません。サーチリストを通常使っている多くの人は、必要であれば（組織のプライベートネットワークの外部からサーバーへアクセスする場合など）フルネームを入力できることを知っており、非修飾短縮名しか理解していない人よりもトレーニングは少なくてすむでしょう。

5.1　ネームサーバーに入ってくるクエリを監視する

サーチリストによって生じる問題を抑止するためには、全てのコンピュータ、ネットワーク機器、および何らかのリクエストでサーチリストを使っているその他のシステムを全て知る必要があります。自動化されたやり方でサーチリストを使っている全ての装置は、更新する必要があるでしょう。

このようなシステムの監視およびリスト作成を実施する方法としては、以下の3つが一般的です。

- キャッシュDNSサーバー（たとえばアクティブディレクトリ）はロギング機能を持っている場合があり、非修飾短縮名を用いる全クエリの詳細を収集するために、ロギング機能をオンにすることができます。
- 多くの新しいファイアウォールは、プライベート名のクエリを検出し記録するように設定できます。これは、ネットワークのトポロジーによっては、名前解決のシステム自体からのロギングほど効果的でないかもしれません。たとえば、クエリがファイアウォールに到達しない場合、ファイアウォールはクエリを見ることができずに見逃すでしょう。
- 上記のどちらも使えない場合、Wiresharkのようなパケット取得プログラムを使って、ネームサーバーを監視し収集できます。しかし、この方法は、非修飾短縮名のクエリだけを見つけるためには、取得したデータをプログラムで処理する必要があります。

この手順は、混乱しやすい結果を招くかもしれないことに注意してください。コンピュータや電話のような機器は、ユーザーが名前を入力するようなアプリケーションを持っています。これらの機器は、非修飾短縮名が何処にも保存されていない場合であっても、調査の際に姿を現します。この手順では、アプリケーションで非修飾短縮名が保存され使用されている、ネットワーク上の場所を全て知ることが目的となります。

5.2　非修飾短縮名を使っている各システムのインベントリ情報を自動化されたやり方で作成する

読者は、前の手順で取得したログのサマリーが必要となります。そのサマリーは、クエリを出す機器の全要素ではなく、クエリを出した全ての機器およびその出した非修飾短縮名のリストとすべきです。クエリを出した全ての名前が必要な理由は、一部の機器は解決する必要のあ

るアプリケーションを複数持っていることがあるためです。このサマリーは、変更を必要とする機器のインベントリ情報となります。

5.3　FQDN を使うようにユーザーおよびシステム管理者を訓練する

何らかの設定（システム全体の設定または個別アプリケーションの設定）で非修飾短縮名が入力されているようなシステムを変更することに加えて、ユーザーが短い名前をFQDNに切換えできるようにするため、ユーザーの考え方を変える必要があります。組織に影響を与えかねない予期せぬ望ましくない結果についての説明をすることで、認知度を上げて受容を促進すべきです。

5.4　影響を受ける全システムを FQDN 利用に切り替える

非修飾短縮名を、それと同等のFQDNに、システム単位で置き換えてください。システム上の全ソフトウェアにある非修飾短縮名の全ての要素を、FQDNに置き換える必要があります。

上記までに開始された監視は、本手順にとってきわめて重要です。あなたは、非修飾短縮名を埋め込んだ全てのシステムの全てのアプリケーションを確認できる可能性は高くありません。その代わり、各システムを変更した後にシステムがまだ非修飾短縮名のクエリを出すかどうかを監視システムで調べる必要があります。

多くのシステムは、最初に実行される時、いくつかの初期化アプリケーションを実行します。これらのアプリケーションは、サーチリストに依存するシステム名を埋め込んでいる可能性があり、それらを全て見つけだすのは困難になりかねません。システムの全ての名前がFQDNを使うように変更した後、システムをリブートし、監視ソフトウェアを使って名前の解決を監視してください。システムが何らかの非修飾短縮名の名前解決をしている場合、どのソフトウェアがそのクエリを出しているかを突き止め、FQDNを使うようにそれを変更する必要があります。このプロセスは、システムを全て正しく設定するために、何度がリブートを行うことになるかもしれません。

5.5　共有のネームリゾルバでサーチリストをオフにする

この時点において、非修飾短縮名からの移行がネットワーク上の全てのシステム（PC、ネットワーク機器、プリンタなど）に実施されます。サーチリストは、名前解決を行うシステムや、DHCPサーバーのように他のシステムへの設定に関与するシステムにおいて存在している可能性があります。これらのシステムはスタンドアロンのネームサーバーであることが多いです

が、ファイアウォールまたはその他のシステム機器の場合もあります。システムの種別とは無関係に、ある名前空間内でユーザーが非修飾短縮名を使うのを防止するために、サーチリストはそれぞれのシステムオフにする必要があります。

5.6　ネームサーバーで非修飾短縮名の利用の監視を開始する

サーチリストを使う必要のある名前に関する全てのクエリの監視を開始するよう、自分のネームサーバーを設定します。事前の通知とトレーニングが実施されている場合、ユーザーはこれらの名前を使っていないはずであり、この監視によって作成されるログはそれほど大きくはならないでしょう。もし大きくなるようであれば、ネットワーク上の特定システムについて、上記の手順のいくつかを繰り返す必要があるかもしれません。

5.7　非修飾短縮名を監視するために周辺で長期的監視を行う

これまでの手順によって、非修飾短縮名の利用の大部分を見つけだしたはずですが、いくつかの（おそらく主要な）システムは、ごくたまにではありますが、非修飾短縮名をまだ使っている可能性があります。これらの名前解決のクエリを検出する最も有効な方法は、ネットワークの外部接続点にある全てのファイアウォールにルールを追加し、誤送信されているリクエストを探し出すことです。このようなルールは、高いプライオリティを付けておくべきであり、ITスタッフに迅速に警告を出せるように、イベント通知が生成できる設定にすべきです。別の方法として、これらのイベントをファイアウォールのログで見つけることも可能ですが、それをやると失敗の確率が高くなります。リクエスト発生時をトリガーとした警告により、スタッフはおそらく極めてまれとなったイベントを検出することができます。一部のファイアウォールは、追加費用で機能を付加しないと、このタイプのルールをサポートしません。自分のファイアウォールがそうであれば、迷子になったリクエストを見つけることの利益が追加費用に値するかどうかを評価する必要があります。

6　まとめ

名前衝突は、プライベートの名前空間を使っている組織に、思いがけない結果を生じさせる可能性があります。本書は、そのような潜在的結果の一部をリストし、組織内でのプライベートな名前空間の使い方を変更するためのベストプラクティスを提供します。

グローバルDNSでTLDとなる（または、すでになっている）プライベートTLDを使っている名前空間は、その名前空間を、グローバルDNSをルートとした名前空間へ移行させることが最上の抑止策となります。サーチリストを使って名前を簡略化していた名前空間の場合、サーチリ

ストの利用を排除することでしか抑止ができません。これらの抑止策を実施するための手順には、衝突の原因となりうる名前の全要素が使われなくなっていることを確認するための、プライベートネットワークにおける長期的な監視も含まれています。

名前衝突問題の包括的な抑止策は、ドメイン名が使われている全ての場所でFQDNを使うことです。すでにグローバルDNSを使っているネットワークにおいて、これはサーチリストを使わないことを意味します。プライベートな名前空間を使っているネットワークにおいて、これはプライベートな名前空間がグローバルDNSをルートにし、サーチリストを使わないことを意味します。

付録 A: 参考資料

以下の文書は、ICANN内部の様々な組織が作成したものです。他の組織でも同様に役に立つ文書を提供しています。特に、ネームサーバーのソフトウェアやハードウェアのベンダーが、彼らのテクニカルサポート用ウェブサイト上で有用な情報を載せているかもしれません。

A.1 新 gTLD プログラム案内

このページは、数百の新しいgTLDをグローバルDNSに追加するプログラムについて、その歴史、実装、および進捗を記述しています。

http://newgtlds.icann.org/en/about/program

A.2 DNS における名前衝突

ICANNは、潜在的な名前衝突に関して深く調査した報告書の作成をInterisle Consulting Group, LLCに委託しました。この報告書は、名前衝突の概要を示し、ルートサーバーで現在でもクエリが出されているが実際には存在しないTLDに関するデータを紹介し、名前衝突が提示する問題点について背景を広範囲に論じています。

http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf

A.3 新 gTLD 衝突発生管理プラン

これは、新gTLDとプライベートの名前空間の間で発生する名前衝突をいかに管理するかについて、ICANNが採用したプランです。また、これはルートゾーンにおける名前衝突に関連した以前の提案書についてICANNが受領したコメントへのポインタを多く含んでいます。

http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-07oct13-en.pdf

A.4 新 gTLD の課題:ドットレス名および名前衝突

異なるシステム上のサーチリストは、クエリをされた非修飾短縮名が何であるかに応じて、大きく異なる結果に行き着く可能性があります。この記事はドットレスのドメイン(TLD名そのものにアドレスレコードを持つTLD)用のサーチリストに焦点を当てていますが、サーチリスト処理の記述は他の多くのコンテキストにおいて有益です。

https://labs.ripe.net/Members/gih/dotless-names

A.5 SAC 045:ドメイン名システムのルートレベルにおける無効なトップレベルドメインのクエリ

このICANNのSSAC報告は、作成時にルートサーバーで観測されたTLDのクエリの種別を記述しています。

http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf

A.6 SAC 057:内部利用名証明書に関する SSAC 勧告

このICANNのSSAC勧告は、プライベート(内部)名を持つ証明書が持つセキュリティおよび安定性に関する意味について記述しています。このレポートは、攻撃者が利用する可能性があり、安全なインターネット通信におけるプライバシーや完全性に重大なリスクを与える恐れのあったCAの実務を特定しています。

http://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf