

2014年6月9日

各位

一般社団法人日本ネットワークインフォメーションセンター

内部システムで利用しているドメイン名にご注意！

～名前衝突(Name Collision)問題の周知と対策実施のお願い～

今年2014年1月にJPNICからもお伝えした通り(※1)、ドメイン名などのインターネット資源をグローバルに調整するICANN(The Internet Corporation for Assigned Names and Numbers)によって、2013年10月から1,300を超える新たなgTLDの委任が順次開始され(※2)、今後、インターネット上で多くのTLDが使われ始めることとなります。これにより、DNSにおける「名前衝突」と呼ばれるセキュリティリスクが、一般的なユーザーをはじめとする広範囲に発生する可能性が指摘されています。

(※1)名前衝突(Name Collision)問題へのJPNICの取り組みについて

<https://www.nic.ad.jp/ja/topics/2014/20140121-01.html>

(※2)申請が認められ追加されたgTLDの一覧

<http://newgtlds.icann.org/en/program-status/delegated-strings>

名前衝突問題とは、従来「既存のTLDに存在しないから問題ない」として組織内のネットワークなどで利用されていたドメイン名が、新しくgTLDとして追加されたドメイン名と同じ文字列として衝突することで、内部ネットワークに閉じた通信が意図せずにパブリックなDNSに到達したり、またはその逆の通信等が行われてしまったりして、「サービスが利用できない」「情報が漏えいする」といった混乱がインターネット上に起こる状態を指します。今まではTLDとして使われていなかった文字列でも、今回1,300以上もTLDが増え、また今後さらに増加させる計画があるとされていることで、そのリスクが飛躍的に高まりました。

そのためJPNICでは、この問題に対する国内での広範な周知に向け、数多くの業界の専門家とともにこの問題を検討する「新gTLD大量導入に伴うリスク検討・対策提言専門家チーム」(※1)を設立し、活動を続けてまいりました。このたび、この専門家チームの報告書ができあがりましたのでお知らせすると

共に、併せて、各対象者別(の対策等を記した)Web サイト等も準備しましたので、社内等で本件の共有および対策を行っていただきたくお願いいたします。

- ・「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」 報告書 (PDF、2,84MB)
<https://www.nic.ad.jp/ja/dom/new-gtld/name-collision/name-collision-report.pdf>

- ・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 (PDF、113KB)
<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/>
 - 企業ネットワーク管理者向け
 - ISP 運用者向け
 - ネットワーク製品や家電などのベンダー向け
 - パブリック認証局およびその代理店向け
 - Sler、Nler 向け の対策方法が個別に記載されています

gTLD の増加は、一見、ご自身やご自身の管理するネットワークとは何らの関係もないと思われがちですが、社内での設定や、ご自身で提供されているサービスの設定等につきましても、今一度見直していただきたくお願い申し上げます。

■本件に関するお問い合わせ先

お問い合わせと併せ、この方面にもお知らせした方が良いと思われる周知先がありましたら、JPNIC までぜひお知らせください。

- ・一般的なお問い合わせ: domain-query@nic.ad.jp
- ・取材のお申し込み: press@nic.ad.jp

■一般社団法人日本ネットワークインフォメーションセンターについて

一般社団法人日本ネットワークインフォメーションセンター（略称：JPNIC <ジェーピーニック>、理事長：早稲田大学教授 後藤滋樹、<https://www.nic.ad.jp/>)は、インターネットの運営に不可欠な IP アドレスの日本国内における登録管理業務を行う機関です。併せて、インターネットに関する教育・普及啓発活動や各種調査研究活動、インターネットの国際的な広がりに対応するための国際的な調整業務を行っています。

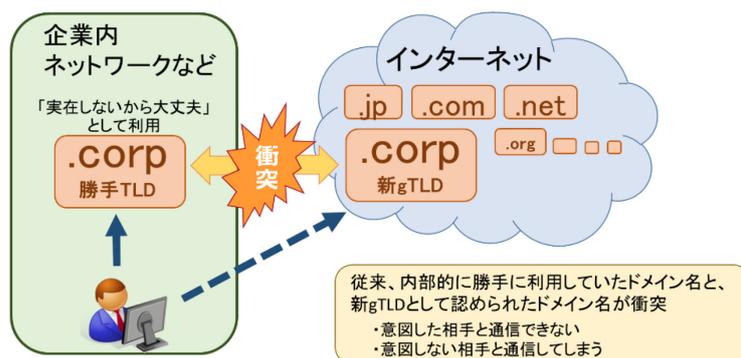
任意団体としてインターネットの急速な普及を底辺から支える活動を 4 年間継続して行ったのち、1997 年、科学技術庁(現文部科学省)、文部省(現文部科学省)、通商産業省(現経済産業省)、郵政省(現総務省)の共管による社団法人となりました。2013 年 4 月からは一般社団法人として活動しています。

以上

新 gTLD の大量導入と、それにより発生する新たな懸念 ～名前衝突の危険性～

名前衝突(Name Collision)とは ～新 gTLD の導入に伴う新たなセキュリティリスク～

現在、ICANN(*1)により新しい gTLD(generic Top Level Domain)の追加が進んでいますが、この影響で「名前衝突(Name Collision)」という問題の発生が懸念されています。詳細は後述しますが、これは従来「既存の gTLD に存在しないから問題無い」として組織内ネットワークなどで利用されていたドメイン名が、新しく gTLD として追加されたドメイン名と衝突してしまうという問題です。この名前衝突が起こると、意図した相手と通信ができなくなってしまったり、意図しない相手と通信をしてしまったりする恐れがあります。



(*1) ICANN : The Internet Corporation for Assigned Names and Numbers - DNS ルートネームサーバシステムを民間主導でグローバルに調整する目的で 1998 年 10 月に米国で設立された民間の非営利法人

ICANN による新 gTLD 大量導入

2012 年から ICANN により実施されている「新 gTLD プログラム」では、追加する gTLD の数に上限を設けなかったことから 1,930 件もの応募があり、そのうち 1,300 程度の gTLD が追加されると見込まれています。2013 年 10 月 23 日には最初の四つが追加され、2014 年 6 月 4 日時点では 304 の gTLD が追加されています。ICANN は、今回だけでなく 2 回目以降の募集も予定していますので、今後、gTLD は不定期に増え続けていく予定です。

今回申請された文字列の一覧：<https://gtldresult.icann.org/application-result/applicationstatus>

申請が認められ追加された gTLD の一覧：<http://newgtlds.icann.org/en/program-status/delegated-strings>

名前衝突問題が発生するケース

名前衝突問題が起こるのは、パブリックな名前空間で使う TLD と異なる TLD を企業のイントラネット等の内部用として利用していて、新 gTLD の追加によってその文字列が重複してしまう場合です。また、TLD として利用してなくても、ドメイン名の省略目的で DNS のサーチリスト機能を利用している場合にも名前衝突が発生します。例えば「www.corp」といったドメイン名がサーチリスト機能によって「www.corp.example.com」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場合があります。

名前衝突によって起こる問題

名前衝突が発生することにより、以下のような問題が発生することが考えられます。

- (1) 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
- (2) 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
- (3) サービスが正しく動作しなくなる
- (4) 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

- (5) 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
- (6) イン트라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
- (7) 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
- (8) 社内で利用しているホスト名が外部に漏えいする

名前衝突の問題の対策

名前衝突の問題は、内部利用目的で使用しているドメイン名がパブリックな名前空間で使用される TLD と重複することであるため、その根本的な解決策は、新 gTLD と重複する恐れのあるドメイン名を利用しないようにすること、また、サーチリスト機能を使用しないようにすることです。

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の留意事項

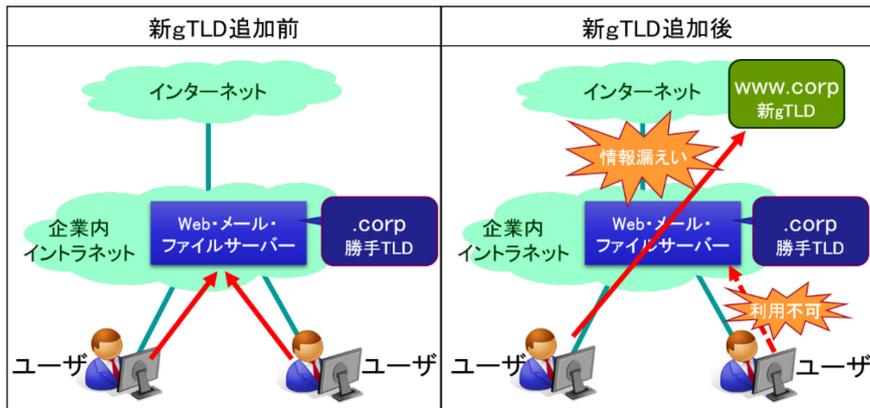
システムインテグレーター、ネットワークインテグレーターに関しては、納入したシステムにおいてこれから説明する各対象者別の問題が発生する可能性があります。システム・機器等の種別によって関連する項目をご参照ください。

企業ネットワーク管理者の留意事項

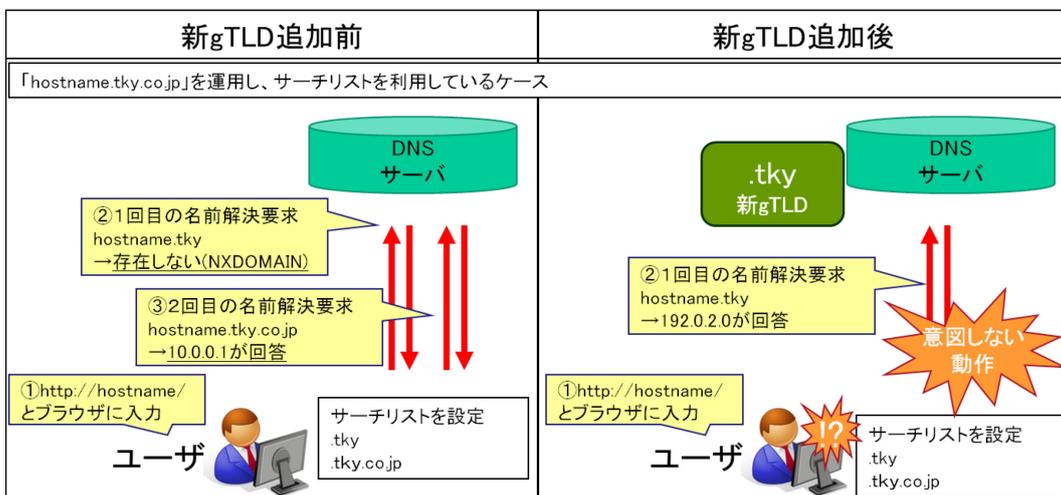
新 gTLD が登録・使用開始され名前衝突が起こった場合、今までアクセスできていた社内のサイトにある日突然アクセスできなくなったり、内部のサーバにアクセスするつもりが外部のサーバに接続してしまう、また、社内ネットワークの利用者が名前衝突する新 gTLD にアクセスできなくなるという事象が起き得ます。

こうした名前衝突の問題を回避するには、内部利用目的のドメイン名を使わずにパブリック名前空間のドメイン名を利用するようネットワークの設定やシステムを修正することが必要です。

- 1) イン트라ネット内で内部利用目的のドメイン名を利用している場合



- 2) サーチリスト（ドメイン名補完）の機能を利用している場合



内部利用目的の証明書を取得している組織の留意事項

従来は内部利用目的(*2)であってもサーバ証明書の発行を受けることができましたが、今後、各認証局では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。

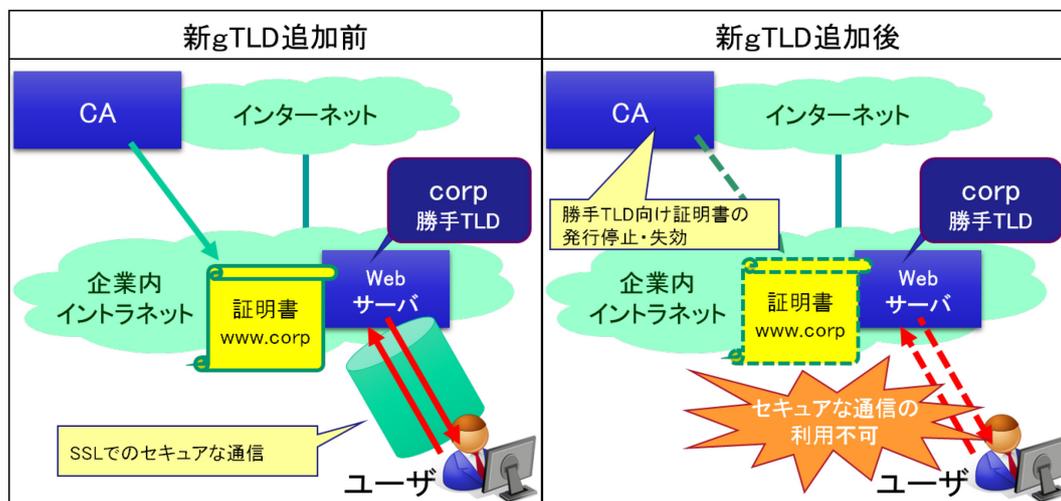
内部利用目的のドメイン名を対象とする証明書をパブリック認証局から入手している組織は、パブリックな名前空間のドメイン名へ移行することが推奨されます。もし、そのような証明書を利用して、自組織の証明書が失効した場合は、社内システムの改修や業務フローの変更など対応が必要になる可能性がありますので、確認が必要です。

CA/Browser Forum 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 日以降発行される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される
- 2) 内部利用目的のドメイン名を対象とする全ての証明書は 2016 年 10 月迄に失効される

なお、現在利用中の内部利用ドメインと重複する新 gTLD が登録された場合には上記の日程よりも前に移行を求められる場合があります。詳細につきましては下記 URL をご参照ください。

Baseline Requirements Documents <https://cabforum.org/baseline-requirements-documents/>



(*2) ここで言う内部利用目的の証明書とは、公開 DNS サーバから名前解決できない FQDN、あるいはプライベート IP アドレスが記載されたサーバ証明書を指します。前者にはインターネット上で利用されていない gTLD を内部利用する場合も含まれます。

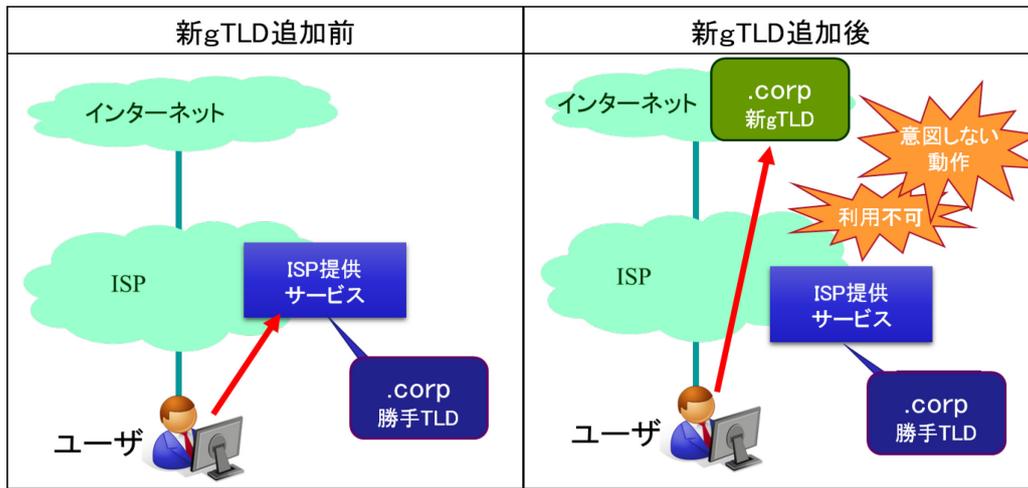
ISP 運用者の留意事項

エンドユーザー宅内のプライベートネットワークで、ネットワーク機器の設定用 URL などに内部利用目的のドメイン名を用いた名前空間が使われていることがあります。

そうした状況で名前衝突が起きた場合、プライベートネットワークで利用している内部利用目的のドメイン名の方が優先されるため、ユーザーは新 gTLD の名前空間にアクセスできないという問題が起きます。

また、"www.service.isp" のようなドメイン名を用いてエンドユーザー向けにサービスを提供している場合でも、"isp" が新 gTLD として登録されると名前衝突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。

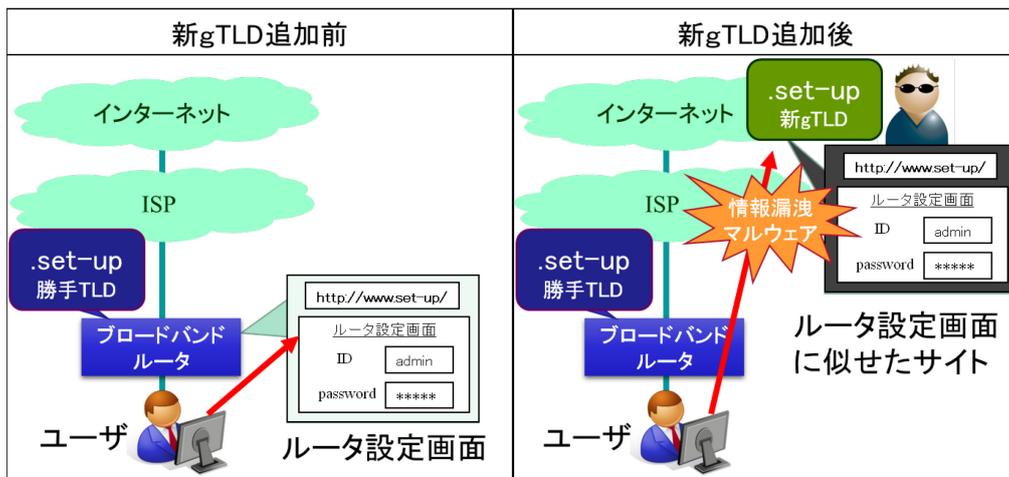
こうした問題に対策するためには、ユーザー向けサービスで利用する名前空間に内部利用目的のドメイン名を使うのを止め、パブリックな名前空間のドメイン名でサービス提供するように改める必要があります。



ネットワーク製品や情報家電等のベンダーの留意事項

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。たと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、ユーザーが意図しない Web サイトに誘導されたり、また、新 gTLD のドメインにアクセスできなくなったりします。

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無く 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、それにより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。



最後に

名前衝突の問題は、IT 関連企業だけではなく、インターネットを利用する一般企業や一般ユーザーにも影響が出る可能性があります。そのため、本問題の存在が広く周知されることは重要です。JPNIC は、関係者の皆様に問題の把握と対処を行っていただくことを目的に、報告書の作成などの周知活動に努めて参ります。皆様におかれましても関係者の方々と情報を共有していただければ幸いです。また、お知らせした方が良いと思われる周知先がありましたら JPNIC までぜひお知らせください。

本問題に関するご意見、ご質問などがありましたら、下記の問い合わせ窓口までお気軽にご連絡ください。

- 問い合わせ窓口 domain-query@nic.ad.jp
- JPNIC Web 「名前衝突(Name Collision)問題」
<https://www.nic.ad.jp/ja/dom/new-gtld/name-collision.html>