SAC070

静的 TLD/Suffix List の使用に関する SSAC の報告書

本文書は、JPNIC/JPRS（JPNIC-JPRS-ICANNの覚書）の支援の下でICANNによって翻訳されています。元の文書は以下から参照いただけます。
www.icann.org/en/system/files/files/sac-070-en.pdf

ICANN セキュリティと安定性に関する諮問委員会（SSAC）の報告書
2015 年 5 月 28 日

序文

本書は、ICANN 理事会、ICANN コミュニティおよびより広範なインターネットコミュニティ向けに 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）が作成した、**アプリケーションにおける静的 TLD/Suffix List の使用**に関する報告書です。

SSAC は、インターネットのドメイン名とアドレス管理の仕組みの安全性と完全性に関連する問題に焦点を当てて活動しています。検討の対象には、運用上の事項（例：正確で信頼性の高いルートゾーン公開システムに関する事項）、管理上の事項（例：アドレス割り振りおよびインターネット番号割り当てに関する事項）および登録に関する事項（例：レジストリおよびレジストラサービスに関する事項）が含まれます。SSAC ではドメイン名とアドレス管理のサービスに対する脅威の評価およびリスクの分析に継続的に取り組んでおり、安定性と安全性に対する最大の脅威がどこに存在するかを判定して ICANN コミュニティに助言しています。SSAC には、規制、執行、または裁定を行う権限はありません。そのような権能は他の団体に属するものであり、ここで行う勧告はそれ自体の是非によって評価されるべきものです。

この報告書への寄稿者の一覧、SSAC メンバーの経歴と利益相反申告、およびこの報告書における結論と提案に対する SSAC メンバーの議論忌避および異議については、本書の最後をご参照ください。

目次

要旨

Public Suffix とは何かについて、コンセンサスによって統一された定義はありません。この報告書では、Public Suffix を「Public Suffix ドメインの所有者と関連のない複数の団体がその下位にサブドメインを登録できるドメイン」と定義します。[1] Public Suffix ドメインの例として、「org」、「co.uk」、「k12.wa.us」および「uk.com」などが挙げられます。

ドメインネームシステム（DNS）ラベルが特定の Public Suffix から監督権限を変更する際にその境界を決定するプログラム的な方法はありませんが、境界の正確な追跡は、Web ブラウザを含む最新の多くのシステムやアプリケーションにおけるセキュリティ、プライバシー、有用性にとって極めて重要となっています。この境界を決定する方法の 1 つは、Public Suffix List（PSL）を使用することです。PSL は、既知の Public Suffix を一覧化した静的なファイルです。

本報告書では、インターネットでの利用が増加している PSL に関して、そのセキュリティと安定性のニーズを詳細に調査しています。SSAC（セキュリティと安定性に関する諮問委員会）は本報告書で、Mozilla の PSL を典型例として現状を調査しています。SSAC では Mozilla のリストがさまざまな目的で利用されていることを把握しました。そして、今回のケーススタディを通じ、PSL の内容全般および PSL の使用と維持を取り巻く運用および管理上の懸念という 2 つの一般的領域においてさまざまな困難が潜在していることがわかりました。

本報告書は、Mozilla およびその他の PSL プロバイダーを批判するものではありません。Mozilla のボランティアは、そうすることを強制される正式な責任を負っていないにも関わらず、インターネットコミュニティに対して重要なサービスを成功裏に提供しています。このことは賞賛されてしかるべきです。

セキュリティコントロールを含む多くのインターネットのユーザー体験および機能でクリティカルパスになっているにもかかわらず、PSL には広範囲にわたって一貫した適用、説明責任および実装はありません。この事実が、現状の PSL の利用慣行におけるセキュリティと安定性に影響を及ぼしています。

SSAC は今回、特に以下の点を見出しました。

- PSL は、利便性と内容の正確性との妥協であるという性質を持っています。
- 「Public Suffix」とその関連用語にはコンセンサスによる定義がなく、

[1] https://tools.ietf.org/html/draft-pettersen-subtld-structure-10

実際、PSL は DNS 内の管理境界に関連した複数の目的のために使用されています。

- 問題に遭遇するかもしれない個人や組織が頼りにできるような、一貫した公正、公平な方法で PSL が生成されることを保証する説明責任の仕組みがありません。

- Mozilla PSL とその他の PSL に対して行う変更と追加におけるプロセスおよび責任に関して、レジストリと Public Suffix List の維持者との間にナレッジギャップがあります。

- PSL の使用に関して、あらゆる状況に対応するライブラリ、フレームワーク、ツールおよび仕組みが存在しません。さらに、実装者は、PSL エントリをソフトウェアまたはその他のサービスで一貫性のある方法で使用していません。レジストリは、サフィックスに関して全てのデバイスおよびアプリケーションにわたって同様の挙動を期待できません。このような挙動によって、ユーザー体験が不安定になっています。

- PSL の変更をソフトウェアアプリケーションおよびインターネットサービスに実装する際にさまざまなレイテンシがあります。PSL のエントリを変更するために更新および配布を行うサイクルは、新トップレベルドメイン（TLD）および/または TLD ポリシーの有用性と受け入れやすさに影響します。

- PSL の内容および維持者からユーザーへの PSL の伝送に関して、認証およびその他の標準的なセキュリティコントロールは通常ありません。

- PSL の使用例が多岐にわたっているため、全てのアプリケーションと使用方法を網羅でき、全ての対象者に適用可能な万能型の PSL を作成することは困難かもしれません。

- 新分野別トップレベルドメイン（gTLD）が既存の gTLD と類似した Public Suffix を使用する場合、TLD 全体が「パブリック」であることから通常 Public Suffix は 1 つとなるため、1 つの PSL のサイズに及ぼす影響は限定的なものとなります。しかし、新 gTLD が複数のパブリックサブドメインを含むこともある一部の国コード TLD（ccTLD）のように Public Suffix を使用する場合、PSL への影響はかなり大きくなる可能性があります。

SSAC は、この報告書において以下を勧告します。

第一に、SSAC は Internet Engineering Task Force（IETF）およびアプリケー

ションのコミュニティに対し、代替となるソリューションを設計、標準化および採用することにより、この基本的な設計上の問題に直接対処するよう求めます（勧告 1）。第二に、PSL が現在普及していること、そして IETF が代替ソリューションを標準化しコミュニティがそれを導入するまでには時間を要することに鑑み、現状における PSL の維持と使用に関する優先度の高いリスクを緩和するべく、短期的な方策を講ずるよう勧告します（勧告 2〜6）。

1. PSL の代替ソリューションが議論されていることから（付録 A）、SSAC は IETF およびアプリケーションコミュニティに対し、IETF のプロセスを介して詳細な仕様の策定と標準化に向け検討を進めるよう勧告します。

2. IETF は、「Public Suffix」およびその他の関連する用語（例：「Private Suffix」）の定義についてコンセンサスを形成するべきです。

3. レジストリ運用者と一般的な PSL 維持者とのナレッジギャップを解消するため、ICANN と Mozilla Foundation は、TLD レジストリ運用者に Mozilla PSL の情報を提供するための資料を共同で作成するべきです。

4. インターネットコミュニティは、PSL に対する現在のアプローチを標準化するべきです。特に以下に示す対策が必要となります。

    a. ICANN は、ユニバーサル・アクセプタンスを目指す取り組みの一環として、PSL の堅牢な（すなわち認証、適時性、安全性、責任の所在が明確な）配布の仕組みを実装しつつプログラミングおよびオペレーティングシステムライブラリを開発して配布するよう、ソフトウェア開発コミュニティ（オープンソースコミュニティを含む）に促すべきです。

    b. アプリケーション開発者は、この作業の仕様として、標準的なファイル形式と最新の認証プロトコルを使用するべきです。

    c. アプリケーション開発者は、独自の PSL を Mozilla PSL や Internet Assigned Numbers Authority（IANA）の PSL 案のように広く認知され受け入れられている PSL 実装（勧告 5）に置き換えるべきです。

5. IANA は、IANA が直接やりとりするレジストリ内のドメインについての情報を含んだ PSL をホストするべきです。このような PSL では少なくとも IANA ルートゾーンの全 TLD を含まなければならず、それによって当該ドメインについて権威を持つものとなります。

6. ICANN は、PSL に関連した使用とアクションをドメイン名のユニバーサル・アクセプタンスに関する作業に明示的に含める必要があります。[2]

[2] https://www.icann.org/resources/pages/universal-acceptance-2012-02-25-en

1　はじめに

ドメインネームシステム（DNS）は、インターネットプロトコル（IP）アドレスなどのインターネット資源に名前を階層的に割り当てるための分散型システムであり、数値のアドレスではなく人間が判別可能な名前を使用して、これらの資源にアクセスできるようにします。Public Suffix List（PSL）は、そのサブネームスペースの管理が登録を実施する組織や団体に委任されているようなパブリックネームスペースを示す DNS 名を識別しようとする努力の結果です。このようなリストの維持によって、Web のセキュリティ、プライバシーおよびポリシーを支えることができ、その他のアプリケーションやサービスにおける多くのプロセスとツールの利便性を向上させることもできます。最もよく知られている PSL は、Mozilla Foundation の協力のもと、ボランティアによって運営されています。

本報告書は、Mozilla およびその他の PSL プロバイダーを批判するためのものではありません。Mozilla のボランティアは、そうすることを強制される正式な責任を負っていないにも関わらず、インターネットコミュニティに対して重要なサービスを成功裏に提供しています。このことは賞賛されてしかるべきです。

静的なトップレベルドメイン（TLD）のリストまたは Mozilla PSL の使用における有効性や拡張性はこれまでも疑問視されてきましたが、新たな gTLD の創設頻度が高くなっている現在、そのような状況がとりわけ顕著になっています。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）が作成したこの報告書では、PSL の既知の使用事例について概説し、現在の Mozilla PSL システムの拡張性について調べています。また、潜在的なセキュリティ、安定性、有用性に関する懸念についても説明します。そして、サービスを向上するための勧告を Internet Corporation for Assigned Names and Numbers（ICANN）とインターネットコミュニティに対して行います。

本報告書では、インターネットコミュニティが Public Suffix List を維持し普及させる取り組みの例として、Mozilla Foundation が維持する PSL を取り上げます。プライベートに運用されている派生的なもしくは同じような静的な Suffix List は多く存在します。この報告書は、このような Public Suffix List の運用主体に対して情報を提供することを目的としており、Mozilla PSL 以外のプライベートに維持される Suffix List に関する重要で潜在的価値の高い考慮事項が含まれているかもしれません。

本報告書は、以下の読者への情報提供を目的としています。

- PSL の定義と実装に関する問題とその影響について把握していない ICANN コミュニティのメンバー（TLD のレジストリおよび TLD のドメインの所有者がその代表的な例です）。本報告書は、このコミュニティに教育的なコ

ンテンツを提供することも目的としています。

- 本報告書で概説する問題に起因する不整合と混乱の解決に取り組んでいる標準化・調整団体（IETF、World Wide Web Consortium（W3C）、 ICANN 等）の技術者およびポリシー策定者。本報告書は IETF の「プロブレムステートメント」に似ていますが、PSL のポリシーに関する側面も含まれます。例えば IETF は通常、PSL に含まれる情報の決定者およびそうした決定について説明責任を持つ持続的可能なプロセスに関しては取り組みを行っていません。
- ソフトウェアやサービスの一部としてさまざまな Public Suffix と静的 TLD のリストを使用している可能性のあるソフトウェアベンダーとサービスベンダー。本報告書は、これらの使用法に関する課題の特定も目的としています。
- 特定の状況、ソフトウェア、オペレーティングシステムまたは使用するサービスによって、同じ文字列であっても回答、表示、効果およびその他の応答が異なることに混乱している一般のインターネットユーザー。

2 背景と用語

PSL の使用は、その他のインターネット技術と密接に関連しています。以下で関連するインターネット技術を紹介します。

2.1 DNS

DNS *名*は、ドットで区切られる一連のラベルから構成され、その名前の DNS における系統を示しています[3]（厳密に言えば、名前空間ツリー内のノードの連結です）。例えば foo.bar.baz の場合、foo.bar.baz、bar.baz、baz（トップレベルドメインまたは TLD）という順番でレベルが上がり、最後には（暗黙的な）*ルート*ドメインになります。ルートドメインから始まるサブドメイン空間のトップダウンの委任は、分散型の権威やグローバルな名前の一意性など DNS を区別するために必要な世界的システムプロパティを有効にするための処置です。*ゾーン*とは、DNS 内の名前空間において自律的に管理される部分です。ドメイン名空間が子ゾーンに委任される場合、子ゾーンの管理者によって他のゾーンにさらに委任されたことが明示されない限り、全てのサブドメインの名前空間がこの子ゾーンに属します。

2.2 Public Suffix と Public Suffix List

Public Suffix とは何かについて、コンセンサスによって統一された定義はありません。この報告書では、Public Suffix を「Public Suffix ドメインの所有者と関連のな

[3] 技術的には、DNS 名前空間はツリー構造になっており、RFC 1034 セクション 3.1 によると「あるノードのドメイン名は、ツリーにおいてそのノードからルートへのパス上にあるラベルがリストになったもの」です。ドットは表示規則の 1 つです。

い複数の団体がその下位にサブドメインを登録できるドメイン」と定義します。Public Suffix ドメインの例として、「org」、「co.uk」、「k12.wa.us」および「uk.com」などが挙げられます。

一般的に、TLD（例：com）はドメイン（例：example.com）を登録する団体にサブドメイン空間を委任するためだけに使用されることがほとんどであり、そのゾーンに直接ホスト名を含むことは一般的にありません。したがって、これらの TLD は定義上、Public Suffix です。

多くの国コード TLD（ccTLD）（例：uk）および一部の gTLD では、特定の第 2 レベル（例：gov.uk）または第 3 レベルのドメイン（例：k12.pa.us）でも委任を可能としており、下にあるホスト名を別の団体に登録して管理を委任することができます。したがって、2 文字の ccTLD または gTLD 名の下に「実質的な TLD」を作成することも可能です。これらの第 2 または第 3 レベルのドメインも Public Suffix となります。

PSL は、既知の Public Suffix の全て（またはサブセット）を表示する静的なテキストファイルです。Mozilla Foundation が最もよく知られた PSL を維持しています。各種のアプリケーション向けに調整されたさまざまな TLD/PSL リスト同様、IANA の TLD リストも、この定義では PSL と見なすことができます。これらの PSL リストのいくつかは一般に公開されていますが、多くはコードまたはソフトウェア構成に埋め込まれており、ユーザーには表示されず操作もできません。

Public Suffix List が存在し定期的に更新されているのは、以下の理由からです。

- 複数レベルで構成される登録ドメインから 2 つ以上のラベルを持つ DNS エントリの Public Suffix を決定するプログラム的な方法が現在ないため。しかし、Public Suffix の定義を追跡し的確に利用することは、現代における多くのシステムおよびアプリケーションにおけるセキュリティ、プライバシーおよび有用性にとって非常に重要となっています。
- 時間の経過と共に新たな TLD がルートゾーンに追加されてきており、新たなサフィックスが既存 TLD に追加（および既存 TLD から削除）されているため。
- TLD 内で管理境界を決定するルールが時間と共に変化する場合があるため。例えば英国では、.uk の直下にドメイン名を登録するポリシーが変更されました。新 gTLD のビジネスモデルが進化するにしたがって、このような状況は数多く発生すると思われます。
- TLD で徐々に国際化ドメイン名（internationalized domain names, IDN）が導入されてきているため。IDN で許可される文字の拡張リストを活用した新たな Public Suffix が登場する可能性があります。

3 Public Suffix List の使用例

このセクションでは、Mozilla の Suffix List を典型として、Public Suffix List のいくつかの一般的な使用例を列挙して説明します。

3.1 Cookie の設定

有効な TLD を信頼性の高い方法で特定できるかどうかは、Hypertext Transfer Protocol（HTTP）の cookie のプライバシーとセキュリティに影響します。Cookie に過剰な権限が付与されることがその代表的な例です。その場合、foo.bar.example にある Web サーバーが、たまたま Public Suffix である bar.example というドメイン値で cookie を送信します。Public Suffix List がなければブラウザは bar.example が Public Suffix であることを認識できず、foo.bar.example ドメイン内の他のホストだけではなく bar.example にある他のホストに対しても、後続の要求で cookie を送信してしまいます。ブラウザは通常、明示的なユーザーの同意や操作がなくてもこれらの cookie を送信するため、閲覧履歴やログインセッションを含む機密のステータス情報が別の団体に漏えいする場合があります。過剰な権限が付与された cookie に含まれる機密情報は、ほぼ確実にユーザーの許可を得ていないサーバーに送信され、情報が閲覧されます。これはセキュリティおよびプライバシーに関する重大なリスクとなります。

Public Suffix List は、過剰な権限が付与された cookie が不注意で（または故意に）Web サーバーに設定されてしまうリスクを最小化します。このセキュリティ上の目的は、cookie ポリシーに使用される Public Suffix List の開発を目指すブラウザ横断的な取り組みを 2006 年に開始した Mozilla Firefox の開発者にとって、主要な推進力でした。[4] 現在、Firefox、Chromium/Chrome、Safari および Opera が Mozilla PSL を使用して cookie の設定を判別しています。Internet Explorer は、Windows 10 から Mozilla PSL を使用する予定です。[5]

3.2 ドメインの強調表示/ブラウザ履歴のソート

ある Uniform Resource Locator（URL）におけるホスト名のうちプライベートで登録された（階層的に）最上位のラベルを判別し、ブラウザのアドレスバーで強調表示するために、一部のブラウザは Mozilla PSL を使用しています。このように強調表示するのは、ソーシャルエンジニアリングの有効性を低下させるためです。扱いにくい事例として www.victimlabel.adhggj.fsddsaf.adfd.attacker.example を挙げますが、ここでユーザーは関連するラベルが「www.victim-label」だと考えてしまうかもしれません。しかし、実際に関連するラベルは「attacker.example」です。

---

[4] 有効な TLD の最初のリストを作成するまでに交わされた多くの議論は、Mozilla の 2006 年 Bugzilla バグレポートからコメントとして文書化されています。

[5] http://blogs.msdn.com/b/ie/archive/2014/10/06/interoperable-top-level-domain-name-parsing-comes-to-ie.aspx

3.3 ナビゲーションショートカットの使用

Google Chrome と Safari は、Mozilla PSL を使用して、ブラウザのアドレスバーに入力されたテキストがホスト名なのか検索語なのかを判別しています。例えば「com」という用語は、「com」という語句の検索として扱われます。これは、この用語が（Public Suffix であることから）登録ドメインに名前解決されないためです。しかし、「foo.com」という用語は、登録ドメイン（「foo.com」）を含んでいるため、ナビゲーションとして扱われます。

3.4 ワイルドカード証明書発行の制限

CA ブラウザーフォーラムのベースライン要件（11.1.3）では、ワイルドカード証明書を発行する前に、その証明書が Mozilla PSL にあるエントリ（例：*.co.uk）のために発行されていないこと、またはその団体が実際に Public Suffix 全体を所有していることを確認するよう認証局に求めています。

3.5 トップレベルドメインの検証

多くのプログラミング言語と Web アプリケーションは、例えばユーザーが指定した URL または電子メールアドレスにおいて、PSL または静的 TLD リストを使用してフォーム入力または TLD の有効性を判別するロジックを検証しています。

3.6 スパム対策

処理時間を短縮する目的で、多くのメールゲートウェイおよび/またはスパムフィルターは最初の合否判定として PSL での一致を用いた基本的チェックを行い、送信元/返信先アドレスの最も右のラベルの妥当性を検証します。

Domain Based Message Authentication, Reporting and Conformance（DMARC）の Request For Comments（RFC）草案では、Mozilla PSL を使用して「組織ドメイン」を判別しています。これが、DMARC アルゴリズムが DMARC に関して DNS レコードを検索する場所です。DMARC は、組織の境界を決めるプログラム的なまたはプロトコルベースの方法を見出す IETF の取り組みにおいて、その推進力となっている使用事例の 1 つです。

以下の表で、各種の PSL 使用事例を概説します。

表 1：PSL の使用事例

（https://wiki.mozilla.org/Public_Suffix_List/Use_Cases を元に作成）

使用事例	説明	質問	アプリケーションの例
Cookie の設定	指定されたドメインのサフィックスにCookieを設定することを許可するかどうか決定します	ドメインとそのサフィックスは同じ団体によって管理されますか？	Mozilla Firefox、Google Chrome、Safari、Opera
「責任のあるドメイン」の強調表示/ブラウザ履歴ソーティング	UIで強調表示またはソートするドメインの部分を決定します - 「Public Suffix+1」	ドメインとそのサフィックスは同じ団体によって管理されますか？	Mozilla Firefox
ナビゲーション可能性	ブラウザがDNSに問い合わせることなく指定URLへの移動処理に入るべきかどうかを決定します	このドメインにはAレコードがあります（ありそうです）か？	Google Chrome
Secure Sockets Layer（SSL）ワイルドカード	*.public.suffix の SSL ワイルドカード証明書を発行するか、または受け入れるかを決定します	このドメインのサーバーとそのサフィックスは同じ団体によって運用されますか？	認証局
TLD検証	多くのプログラミング言語は、フォーム入力の検証のために、またはさまざまな方法で生成されるドメイン名の中のTLDが有効かどうか判別するロジックの中でPSLを使用しています	ユーザーが生成して送信したURLには有効なTLDが関連付けられますか？	Webフォーム、プログラミング言語ライブラリ
スパム対策	処理時間短縮のため、PSLでの一致を用いた基本的チェックによる最初の合否判定として、ドメインのTLDを確認して送信元/返信先アドレスの妥当性を検証します	.exampleがTLDのリストにない場合、<perp@scam.example>からのメールをすぐに落とすべきですか？	スパム対策ソフトウェア

4 PSL の生成と維持に関する課題

以下のセクションでは、SSAC が懸念している事項のうち、PSL の中身の生成と維持に特有のものについて説明します。これらは PSL の使用目的とは無関係の一般的な懸念です。

4.1 「Public Suffix」の定義に対するコンセンサスの欠如

「Public Suffix」の定義についてはさまざまな意見があり、多くの関係者がそれぞれの詳細なニーズやソリューションを基準に定義を行っています。適切な定義について権威ある立場を強く表明しているケースも多くありますが、その定義はさまざまで整合していません。

Mozilla の Public Suffix List で明確に説明されているのは、リストの範囲をパブリック/ICANN およびプライベートという 2 つに分けるという点です。Mozilla では以下のように定義しています。

- パブリック/ICANN セクションには、インターネット調整ポリシー（Internet Coordination Policy, ICP-3）[6]に準じた gTLD と ccTLD のサフィックスエントリが含まれ、それらは IANA によって直接委任されるか、関連付けられます。
- *プライベート*セクションには、CentralNic（eu.com および us.org などの所有者）のような多くのサブドメイン登録サービス [7]と、DynDNS、Amazon、Google、GitHub、Heroku[8]、Microsoft および Red Hat のような DNS 解決およびクラウドサービスを提供する企業のエントリが含まれます。登録ドメインの所有者がそれぞれ関係のない別の団体にサブドメインを委任する場合があるため、このセクションが存在します。

こうした分類は必要で意思決定を向上するために有用かもしれませんが、Mozilla PSL を維持するボランティアのコミュニティとその利用者の両方に対して、次のような問題を発生させる場合があります。

---

[6] https://www.icann.org/resources/pages/unique-authoritative-root-2012-02-25-en

[7] Anti-Phishing Working Group で定義されているように、サブドメイン登録サービスは、所有するドメイン名の下位にあるサブドメインの「ホスティングアカウント」を顧客に提供するプロバイダーを指します。http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf

[8] Hiroku Website セキュリティノート：https://devcenter.heroku.com/articles/cookies-and-herokuapp-com

- *レジストリステータスの混乱*。Mozilla PSL でのパブリック/プライベートの境界は明確でなく、注釈がないと第三者がその違いに混乱する場合があります。「プライベート」としてマークされている場合でも Mozilla PSL にサフィックスが存在すると、IANA から直接委任されたレジストリに相当するステータスを持っている、または IANA およびその TLD の管理権限の明確な移管が行われているという意味を含む場合があります。

- *信頼関係が一般ユーザーに誤解される恐れ。*DNS 自体の構造を基準に信頼性が推測される場合があります。Mozilla PSL の ICANN ドメインセクションでこのような信頼がある程度有効であると主張できるかもしれません。というのも、多くの場合、TLD のポリシー設定に責任を持つ運用者が PSL の第 2 レベルドメイン（SLD）のポリシーも設定することになり、少なくともある程度の一貫性が期待できるためです（例：com.au と.au、gov.cn と.cn）。しかし、プライベートドメインのセクションでは、TLD のレジストリによって運用されていない、あるいはレジストリと関係がないため、このような信頼性が失われる場合があります。例えば.de（ドイツの ccTLD）は DENIC によって運用されていますが、com.de は DENIC と関係のない CentralNic という団体によって運用されています。Mozilla PSL では 1 つのファイルにこれらの両方が含まれているため、この区別が明確でない可能性があります。他方、団体が信頼関係の基盤として IANA の TLD リストを使用している場合には、逆の状況が発生する可能性もあります。これは、多くのレジストリ、とりわけ ccTLD は、ゾーンを細分化して登録ドメインの正規の Public Suffix 部分としてトップレベルを全く使用していないためです。例えば、IANA の TLD リストにある.au（オーストラリア）の下にはドメインが全く登録されていませんが、com.au、net.au、org.au などの下でドメインが登録されています。これは、管理上の関係を完全に説明するものとして「プライベート」または「パブリック」を用いるという Mozilla の概念の限界が露呈しているポイントです。

- *Public Suffix と Private Suffix の混乱。*ほとんどのアプリケーションが、ICANN ドメインとプライベートドメインの両方を区別せずに使用しています。しかし、時々これらの 2 つを区別する必要が出てきますので、これらの 2 つのセクションが 1 つのファイルに表示されることが区別を困難にします。例えば DMARC の仕様[9]では、Mozilla PSL を使用して「組織ドメイン」を決定しています。ここで、DMARC アルゴリズムが DMARC ポリシーに関する DNS レコードを検索することになります。この使用では Mozilla PSL のプライベートエントリをおそらく排除すべきですが、現在の DMARC の仕様では排除すべきとは明示していません。これら 2 つのセクションを一緒に使用するためには、実装者が判断できるだけの Mozilla PSL に関する知識が必要となりますが、実装者にはその知識がない場合もあります。

[9] https://www.rfc-editor.org/rfc/rfc7489.txt

業界全体として「Public Suffix」について一貫した定義がないために、このような混乱が生じています。Public Suffix または Private Suffix とは何か、両者の相違、各タイプを更新する権限があるのは誰かを多くの人が理解していません。いくつかの使用例では、「Public」と「Private」という単純な区分けよりも、管理上の境界についてさらに詳細な区別が必要となるといったことも全くあり得ます。

4.2 PSL 運営者の説明責任の欠如

PSL については広く同意されている定義が存在せず、正式な標準がなく、加えて PSL の公開について正式な地位にある団体もありません。そのため、何らかの問題に遭遇するかもしれない個人や組織が頼りにできるような、一貫性があり公正で偏見のない方法によって PSL が作成されることを保証する説明責任の仕組みが存在していません。こうしたことの明らかな例外の 1 つは、非常に限定的な PSL リストを提供している IANA です。Mozilla PSL については、その公共性とかなり透明性の高いプロセスから、ある程度説明責任を果たせているとみなすことができます。

その他の PSL の維持者は通常、自社独自のソフトウェア、サービスまたはシステムをサポートしている民間企業です。市場の圧力により、自社製品において正確な PSL 情報を維持しなければならないという説明責任と動機がある程度は存在しています。しかし、プライベートな PSL の変更を誘導するために多数の苦情や主要な相互運用性の問題に頼ることには、多くのリスクがあります。また、これでは Public Suffix の申請者のコミュニティを全てサポートすることになりません。そうした申請者は PSL 提供者が費用を被ってまで変更するだけの十分な利用または説得力のある事例を示すことができません。したがって、TLD のユニバーサル・アクセプタンスのような目標をこれほど多様な環境で実現することは困難です。

ボランティアが維持する Mozilla PSL を例にとると、セキュリティ、公正さまたはプロセスに関する深刻な問題は発生していないため、正式な説明責任のプロセスがないにも関わらず、公開で維持されている PSL として最も幅広く採用されるようになっています。しかし、こうして成功を収めた実績に関わらず、監視、説明責任およびポリシーに関するプロセスが組織の性質上不十分であることから、リスクは依然として残っています。そのリスクには以下が含まれます。

- *企業や政府団体による実効支配。*正式なまたは有限のメンバーシップ/リーダーシップを持たないボランティア組織は、確固たる意思を持って取り組んでくる団体に牛耳られる場合があります。このような団体は、インターネット利害関係者全体としての利益ではなく自らの既得権を強化するために、サフィックスの追加または削除の決定を行う可能性があります。このような自社の利益に根ざした決定には、競合企業のサフィックスの追加を許可しない、または自らの信条に反するサフィックスを検閲するといった判断が含まれる場合があります。乗っ取りやリストのポリシーについての懸念があると、

人々はより信頼でき自分たちのニーズに合った方法を確立するために現在のオープンソースプロジェクトの利用を見送るかもしれません。このようにして Mozilla PSL を断念する際に必要となる運用とプログラミングの費用または教育に要する労力は検討しきれていませんが、ささいなものではないと想定されます。したがって、代替策を比較検討するときに考慮するべき「切り替えコスト」が出てきます。

- *継続性。*ボランティアの多くがこの作業から離れてしまうと、後継者を確保する強力な計画がない限り、運用自体が継続できなくなる恐れがあります。
- *エラーまたは悪意あるエントリ。*現在までのところ問題になっていませんが、全体的な説明責任の枠組みや監視体制の欠如により、エラーを解決したりセキュリティ/レビューのプロセスを確立することによって、確固たる意思を持つ敵対者が悪意ある変更を挿入できないようにしたりするベストプラクティスの執行が、いっそう困難になります。
- *企業や組織がリスト/プロセスを信頼できるようにする法的地位。*正式な提携組織、公開によるレビューと異議申立のプロセスおよび利害関係者の関与がない場合、企業や組織のリスク管理チームは Mozilla PSL チームのようなボランティア集団が提供する PSL の利用を認めない可能性があります。自社で独自の PSL を維持すると決定した企業もあり、上記のことがそのような決定に至った主な要因になっているかもしれません。これが、このエコシステム全体で PSL エントリの統一性が図られない原因になっています。

4.3 PSL へのエントリ追加に関するナレッジギャップ

エントリの追加に関するプロセスと責任について、レジストリと PSL 維持者との間にナレッジギャップが存在することが多くあります。有名な Mozilla PSL についてもこのギャップが存在しており、特に民間企業などの他の PSL ではこのギャップはさらに大きくなっています。

PSL は、PSL 維持者にエントリを提出する要求者に依存しています。また、PSL 維持者は、新たな TLD または新たな TLD レジストリポリシーを基準として PSL エントリを新規に追加するべきかどうかを判断し、判断にあたって要求者に依存しています。レジストリが PSL エントリへの更新を要求しない場合、PSL 維持者が特に勤勉でない限り、その TLD またはエントリはタイムリーに追加されないか、または全く追加されなくなります。PSL に依存するブラウザやその他のアプリケーションは、追加されていない Public Suffix または TLD を認識しません。しかし、レジストリ管理者は、Mozilla PSL の場合であっても、要求をどこに申請するのかを知らないことがしばしばあります。さまざまな組織や個人によって多くの PSL のバージョンが管理されている場合に、この状況はさらに悪化します。

レジストリ管理者のほかに、個々のドメインの所有者とソフトウェアのレポーターもいくつかの PSL にエントリを提出する場合があります。こうしたケースでは、

PSL 維持者は関連する Public Suffix に責任を負う団体や組織と共にその申請を確認する必要があります。しかし、PSL 維持者がこれらの団体と関係を構築していないことがよくあります。このような関係を構築して信頼関係を維持するには時間がかかります。レジストリ（または団体）が要求に関する検証の質問に回答しない場合、さらに遅延することがあります。

例えば以下のような事例から、これらのギャップが確かに存在していることが示唆されています。

- .post という gTLD は DNS ルートに 2012 年 8 月に追加され、その最初の第 2 レベルドメイン名が使用可能になったのは 2012 年 10 月でした。しかし、.post は Mozilla PSL に 2013 年 4 月まで追加されませんでした。レジストリ管理者が要求を出していなかったため、この遅延が発生しました。

- ccTLD の.sx（シント・マールテン）と.cw（キュラソー）は、2011 年 10 月に委任されました。この 2 つの TLD の第 2 レベルドメインは、少なくとも 2012 年 7 月から実際に使用されています。しかし、これらの TLD は 2013 年 2 月まで Mozilla PSL に追加されませんでした。レジストリ管理者が要求を出していなかったため、この遅延が発生しました。

- Mozilla のボランティアによると、2010 年と 2011 年に Mozilla の PSL に追加されなかった TLD については、一部の ccTLD 運用者が Mozilla からの確認要求に返答しなかったことが、追加されない重大な要因となりました。

4.4 PSL にエントリを追加する際のレイテンシ

セクション 4.3 で概説したように、PSL の存在に対する理解およびエントリを追加または編集するにあたってのポリシーに対する理解といった要求者側の教育の問題を克服したとしても、PSL エントリの更新を遅らせるプロセスが PSL 維持者側にある可能性があります。例えば、Mozilla PSL はボランティアが費やすことのできる時間に依存しています。他の PSL は、PSL を静的ファイルとして展開する場合に維持するソフトウェアまたはソフトウェアライブラリのリリーススケジュールに依存します。その他の PSL 運用者はオンラインでのアップデートを提供できる場合もありますが、そのようなリソースの更新を遅らせる別の優先事項を持っているかもしれません。

SSAC の分析によると、2008 年 1 月から 2014 年までに Mozilla PSL を更新する要求が 172 件確認され、解決されています。[10] 要求を解決するまでにかかった時間

[10] 2012 年以前は、同じチケットプロファイル内で IDN ホワイトリスト追加要求が存在していました。そのため、同型異義ドメインの削減を目的として、レジストリの公開するコードポイントに対する広範なレビューも行われていました。SSAC のアナリストは、データ比較の一貫性を維持するために、PSL の要求

の中央値は 23.9 日であり、要求の 75 パーセントは 77.6 日間以内に解決され、90 パーセントが 5 ヶ月以内に解決されています。表 3 は詳細な統計を示しています。

表 3：PSL の処理速度に関する統計（日数）

	要求を解決するまでの時間（日数）
平均値	65.9
中央値	23.9
最小	0.0
最大	885.9
25%パーセンタイル	3.4
50%	23.9
75%	77.6
90%	155.7

次の要因が重なる場合に遅延が生じることがあります。

- セクション 4.3 で説明した PSL へのエントリの追加に関するナレッジギャップ
- Mozilla PSL のボランティアに要求を処理する時間がないこと

同じような問題は各種の PSL に依存するその他のソフトウェアでも見られますが、そのような PSL はほとんどが非公開であるため、遅延に関するデータを入手することが困難になっています。

4.5 PSL エントリとファイルの形式

PSL がどのように見えるべきか、そして PSL がどのように保管または分配されるべきかについて、標準化組織によるガイドライン、RFC および業界標準はありません。配布に関する問題については、後のセクションで説明します。可能なリストの種類としては、静的ファイル、動的なデータベース、中央リポジトリまたは分散システムソリューションなどいくつかあります。PSL への実際のエントリについては興味深い課題もあります。各種のポリシーは DNS の「ツリー」のレベルごとまたは特定のゾーンごとに異なっているため、一貫性を確保することが困難になっているのです。ツリーのあるレベルにおいて考えられる全ての兄弟および親のポリシーが同じであれば、各サフィックスの単一のエントリは単純になり、うまくいくでしょう。しかし実際はそうはならず、「例外」と相違を示す必要が出てきます。

標準に最も近いのは、恐らく Mozilla PSL でしょう。Mozilla PSL はインターネット経由でアクセスできる静的なファイルです。Mozilla PSL の現在の形式は、単純なエントリ（例：bar.example）、ワイルドカードエントリ（例：*.bar.example）

から IDN ホワイトリストの要求を手動で分割しています。

およびワイルドカードへの例外（例：!brown.bar.example）をサポートしています。IDN はそうしたエントリの 1 つであり、ファイルの中で UTF-8[11]（U-LABEL）としてエンコードされます。[11]この形式はこれまで問題なく使用されていますが、形式をさらに専門化、最適化することで、Mozilla PSL が利点を享受できるようになるかもしれません。

形式以外にも、メタデータが各種の使用例で便利に利用できます。例えば、タイムスタンプ、生存時間（TTL）、または PSL の各エントリの起源に関するその他のインジケーターは、キャッシュやバージョンコントロールなどのアプリケーションで有用となるでしょう。認証や整合性の検証も同じように、セキュリティアプリケーションで有用になる場合があります。Mozilla PSL の生成プロセスにはバージョンコントロールシステムがありますが、ファイル自体に人間またはマシンが明確に確認できるバージョンや生成日を示す仕組みがないため、手元のデータの新しさを把握することは難しくなっています。

4.6 PSL へのプライベートネームスペースの追加

リスト維持者のポリシーによっては、パブリックでない名前空間または代替ルートの TLD のサフィックスが追加されている場合があるため、Public Suffix List に入っているサフィックスを綿密に調査する必要があります。[12]ベストプラクティスとして、広範に展開される PSL は、インターネットエコシステムの長期的なセキュリティと安定性をサポートし、あいまいさや混乱を引き起こすことが無いようにする必要があります。有用なガイドラインである ICP-3 は、一意で権威あるルートを持つインターネット識別子構造を忠実に守ることの重要性を述べています。[13]例えば、Mozilla PSL は ICP-3 を順守しており、したがってインターネットの安定性を支えています。[14]

PSL が ICP-3 を無視すると、どのサフィックスがパブリックでどのサフィックスがパブリックでないかを決定するにあたって矛盾が生じたり相互排他的になったりする可能性があります。この状況は、アプリケーション内や異なる PSL を使用する同じマシンのアプリケーション間で不確定な動作を発生させる恐れがあります。とくに、独自のプライベートな名前空間を持つネットワークに実装している場合にこの問題が発生する場合があります。

---

[11] Universal Coded Character Set の U + Transformation Format - 8 ビット。http://en.wikipedia.org/wiki/UTF-8

[12] 例えば、プライベート/企業のドメイン空間は、企業ネットワークのネームサーバーのみで把握されます。

[13] ICANN。DNS の一意で権限のあるルート。ICP-3。2001 年 7 月。
https://www.icann.org/resources/pages/unique-authoritative-root-2012-02-25-en

[14] 詳細：wiki.mozilla.org/Public_Suffix_List。実際のリスト：
http://publicsuffix.org/list/effective_tld_names.dat.

PSL の内容はまた、コンセンサスによって形成された「Public Suffix」の定義を考慮する必要があります。この懸念事項については、セクション 4.1 で詳細に説明しています。当然ながら、この定義は PSL の中身に情報を与えるものでなければなりません。

5 PSL の使用に関する問題

PSL の技術的な使用には次の懸念があります。SSAC は、最新の PSL の実装、レイテンシ、コンテンツ、および使用例の変わりやすさにおいて問題を見つけています。

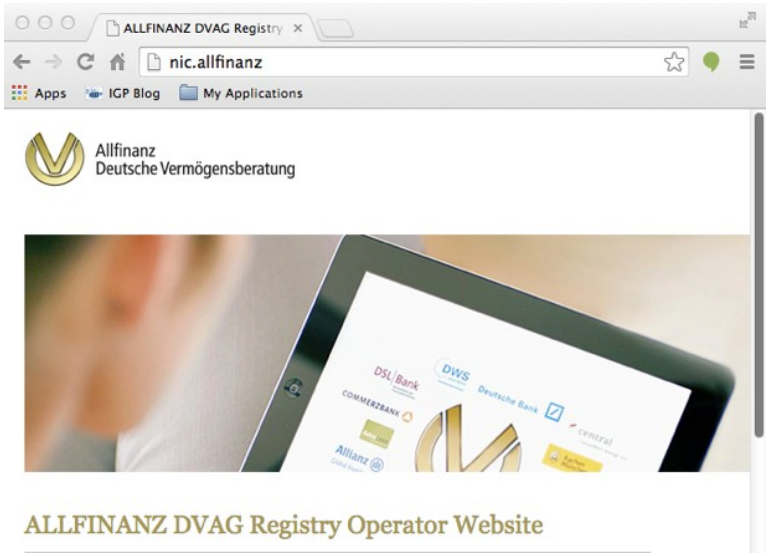
5.1 Suffix List の使用や処理の不整合

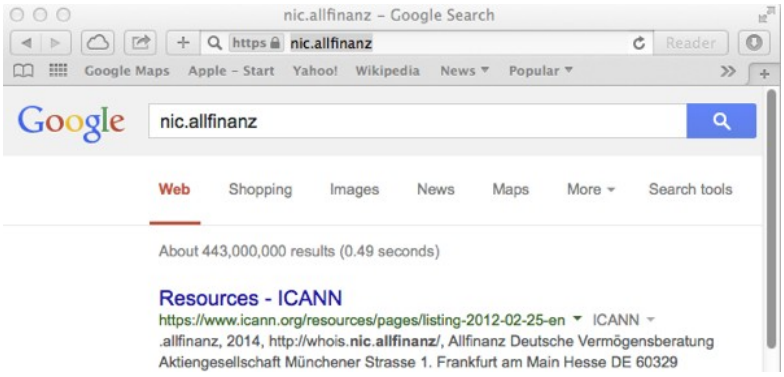
アプリケーションが統一的なライブラリ、標準、ファイル構造およびサフィックスの決定の仕組みを使用していないため、同じコンピューターにある異なるアプリケーションで、異なる結果がユーザーに返される場合があります。これは、信頼性のあるインターネットの機能に必要となるその他のいくつかの機能でも提起されてきた根本的な問題の 1 つです。PSL 以外のこれら事例では通常、インターネット標準が作成され継続的に更新されています。しかしこれらの取り組みは PSL では成文化されておらず、ソフトウェア開発者、Web サービスおよびその他の団体は、PSL の作成、維持、更新および使用の方法を決定しなければなりません。

多くのアプリケーションが Mozilla PSL を採用していますが、同じ方法で使用しているわけではありません。また、あるコンピューターにおけるさまざまなソフトウェアパッケージで完全に異なる PSL が使用される可能性があり、ソフトウェアの相互運用性の確保やデバッグが難しくなります。例えば、Microsoft は Windows 10 の IE 11 から Mozilla PSL の使用へと移行する旨を発表しました。しかし、それよりも古いバージョンでは現在の Microsoft のプライベートな PSL と PSL 形式を引き続き使用することになります。この移行は建設的な進展ですが、全ての IE 10 とそれ以前の導入環境がアップグレードされるまでは、変動するリスト内容、更新および構造に関する全ての問題が移行期間にわたって存在することになります。

時が経てば IETF DBound Working Group（付録 A 参照）がこの状況を改善できる可能性がありますが、迅速に解決される見込みはありません。

次のスクリーンショットは、Google Chrome（バージョン 37.0.2062.124）と Safari（version 7.0.6 9537.78.2）における新 gTLD ドメイン名（nic.allfinanz）の表示の違いを示しています。





PSL の処理におけるこのような不一致によって、ユーザーが混乱したり、新 gTLD、IDN、Private Suffix 空間または PSL に依存するその他あらゆるものの有用性が低下したりする恐れがあります。

5.2 PSL の変更をソフトウェアアプリケーションおよびインターネットサービスに実装するまでのレイテンシ

PSL を使用するソフトウェアアプリケーション、Web サービスおよびその他のツールにおける PSL 変更のレイテンシの問題を示す例として、Mozilla PSL を取り上げます。Mozilla PSL は現在、バグ報告システムを使って Web のアドホックな公開スケジュールと組み合わせて更新要求を処理しているため、少なくとも 3 種類の遅延が発生します。これらの課題は、テキストベースの手動の PSL が直面する代表的なものです。第一のタイプは、バグ報告からコードコミットまでの伝播であり、PSL 作成時に固有の遅延としてセクション 4.2 で説明しています。PSL の内容の更新に加え、遅延を生じさせる以下の 2 つの要素が潜在しています。

- *PSL の更新をソフトウェアが独立して行う場合における、Web 公開からソフトウェアアプリケーションにおける新たな Mozilla PSL の採用までの伝播。*

Mozilla PSL に更新を取り入れるために設定を更新する方法は、ソフトウェアによって異なります。ソフトウェアは通常、全てのクライアントに更新をプッシュする仕組みを持たないため、PSL のようなリソースの更新済み設定を求めてポーリングします。どれだけ遅延するかは、ソフトウェアに組み込まれている更新のポーリング間隔とインターネットや PSL のソースリポジトリへのアクセスなどの要素によって決まります。アクセスは、ローカルポリシー（例：ファイアウォールのルール）やインターネットへの接続性の不十分さ（例：モバイル機器のローミング）によって制限される場合があります。

- *Web 公開から末端側ソフトウェアに向かっての伝播。*例えば、Web ブラウザなどの正確な PSL に大きく依存しているものの展開されるソフトウェアに組み込む形でポーリングの仕組みを提供していないソフトウェア製品やサービスでは、頻繁な更新周期が一般的に適用されます。これらのケースでは、更新には承認された認証局や PSL などの項目の設定変更が含まれます。例えば、Google Chrome や Mozilla は少なくとも 6 週間ごとに更新版を定期的にリリースしています。Safari を含むその他のブラウザでは、PSL の変更が設定に反映されるまでにより長い時間がかかる場合があります。多くのブラウザが非常に多くのセキュリティアップデートを公開しているため、PSL の更新サイクルは短くなる場合があります。重要なマイナス要素は、エンドユーザーが自動更新機能を有効にするか、または手動でソフトウェアを更新しない限りそうした更新が伝播しないという点です。

多くのサードパーティによる PSL ベースのソフトウェアライブラリには、ブラウザのような動的アップデート機能も頻繁な更新サイクルもなく、Mozilla PSL（または組み込まれたいずれかの PSL）の古いコピーをそのまま使用している可能性があります。手動アップデートがこれらのソフトウェア製品で実行されない限り、古いコピーが無期限に使用されることになります。このアップグレードパスの欠如は、PSL の更新において特定されている最大の問題です。ほとんどのアプリケーション開発者は、Mozilla PSL を利用している場合を含め、使用している PSL の更新だけに基づいてアプリケーションの更新をリリースすることはありません。したがって、Mozilla PSL のような公開の PSL ソースに問い合わせることによってユーザー設定がインストールされる状況においては、そのアプリケーションがユーザー設定を自動的に更新しない限り、アプリケーションで使用される PSL の更新は、バグ修正やアップグレードを含むソフトウェア自体の更新サイクルに依存することになります。多くのユーザーにとってこれが意味するのは、アプリケーションで使用されている PSL への更新を受け取れるとしてもそのようなことはめったに起こらない、ということです。特に、定期的な更新をしない場合やソフトウェアの新バージョン適用のために長い承認プロセスを経なければならない場合には、こうした傾向は顕著になります。

このような遅さが歴史的に許容されてきたのは、TLD がまれにしか変更されなかったためです。しかし、複数の要因から最近ではより頻繁に変更が行われるようになっています。ICANN の新 gTLD プログラム、IDN の追加、ccTLD のさらなる細

分化および種々のベンダーが維持しているものを含むプライベートな名前空間での実質的な TLD の利用が継続的に増えていることが、その要因として挙げられます。この変更頻度の高さは Mozilla のボランティアおよびソフトウェアの開発者に困難をもたらしており、最終的には新 TLD および/または既存 TLD におけるポリシー変更の使いやすさと受け入れに影響を及ぼします。

現時点で、Mozilla PSL は毎日約 100 万回ダウンロードされています。このデータからは、同じ団体がこのファイルにどのぐらいの頻度でアクセスしているのかが直接的に明示されないため、今後の使用を予測することは難しくなっています。

パブリックなトップレベルの名前空間の変更に Mozilla PSL を使用しているアプリケーションの問題以外に、別の課題があります。「独自の」PSL を使用するアプリケーションのユーザーは、どの子ドメインが Public Suffix とみなされるべきかに関する全レジストリのポリシーに合わせて TLD の最新リストを維持できるかは、ソフトウェア開発者に完全に依存しています。大手の開発者（例：Internet Explorer[15]を更新する Microsoft）にとってもこれは難しい問題ですが、そうした開発者は広範なユーザー層を満足させる上での必要性に鑑み、あくまでやり通しています。その他のアプリケーションの場合、これは乗り越えられない難題をもたらすかもしれません。

5.3 PSL の内容の認証

インターネット全体にわたって普及しているデータについては全て言えることですが、ユーザーが可読でタイムリーな PSL を持つだけでは不十分です。ユーザーは正確かつ真正な PSL を持っていなければなりません。PSL はしばしばセキュリティに関連する意思決定で使用されるため、使用する前にファイルやエントリを認証することが重要です。そうしないと、改変の標的になる場合があります。いくつかの PSL は、Transport Layer Security（TLS）などの標準技術を使用して安全に配布しており、PSL のプロバイダーから直接送信する場合にはうまく機能しています。また、置かれているだけの状態にありかつ PSL プロバイダーから直接配布するものではない時に PSL の中身を保護する認証手段を検討する必要があります。というのも、データがインターネットをうまく通り抜けていく上で、それらが一般的なセキュリティ上のリスクとなるためです。そのデータの破壊が当該 PSL の全ユーザーに迅速に広がることから、これは特に分配者に関連性の高い問題です。デジタル証明書などの情報認証における一般的なベストプラクティスを適切に統合できればそれで十分でしょう。セクション 4.5 で考察したように、PSL の形式や処理方法に関する合意がないことよって、認証の問題が深刻になっています。ある認証ソリューションを他のソリューションに統合するのが理想的です。

[15] http://blogs.msdn.com/b/ie/archive/2014/10/06/interoperable-top-level-domain-name-parsing-comes-to-ie.aspx

5.4 PSL のさまざまな使用事例

PSL の作成者は通常、何が Public Suffix で何が Public Suffix でないかを知ることが重要であるという認識のもと、特定の問題を解決するために PSL を作成します。そうした PSL は、ひとたび作成されれば他の問題を解決するために使用されるかもしれません。例えば、Mozilla PSL の最初の目的はブラウザの cookie の問題を解決することでしたが、現在は多くの組織や団体がさまざまな問題を解決するために使用しています。それぞれの使用例では、Mozilla PSL のどの部分を使用するかについて異なる要件が存在します。セクション 3 に一般的な使用例を掲載します。多くの使用例では問題なく稼働していますが、求められる PSL の記載事項は脅威モデルによって異なる場合があります。

- Cookie と CA については、敵対者のドメインが、本当はターゲットとなるドメインとは異なる管理の下にありながら、同一の管理下にあるかのように偽装される脅威があります。単純な例として、foo.example が*.example または.example の証明書または cookie を要求する場合があります（CA は *.TLD の証明書の付与を禁止されていますが、悪意があれば付与できますので、これは単純化した例です）。

- 電子メールでの脅威として、敵対者のドメインが本当は同じ管理下にあるものの、異なると主張される場合があります。例えば、abc.xyz.bigbank.example から送信されたように装うスパムでその DMARC レコードが bigbank.example になっている場合があります。

脅威モデルに応じて、PSL の検索が失敗した時のスキームとして failed open（アクセスをそのまま許可）または failed closed（アクセスをブロック）のいずれを採用するかが異なります。意図する使用例によるこうした選択の違いにより、幅広い対象者、アプリケーションまたは用途のための万能型の PSL プロセスを統一して使用することが困難になるかもしれません。

複雑な問題の 1 つは、さまざまなプロトコルにさまざまな管理境界が存在しているために、PSL の内容をプロトコル固有にする必要があるかもしれないということです。現在の PSL は、そうした使用方法の多様性に対応できない可能性があります。例えば、.name は、*firstname.lastname.name* のようにドメインとして登録できる一方、電子メールとしては *firstname@lastname.name* のような形で使用されるため、電子メールで使われる名前空間と Web およびその他のアプリケーションで使われる名前空間でポリシーの管理が異なっています。このような不一致は、例えば DMARC 標準との間で問題を発生させます。

6 アーキテクチャに関する注意事項

PSL はソフトウェアエンジニアにとって便利なものです。PSL は、他では簡単に

入手できない情報の総括表、すなわち DNS の Public Suffix およびそれに関連した DNS のラベル階層内にある組織境界の意味の一覧を、1 つのリソースの中にまとめて格納しています。しかし、このような総括表情報への依存は、一定のリスクを伴います。

このアプローチは、避けられない欠点の原因となっています。第三者がこれらのリストを維持するときには、リストが正確かつ完全であり信頼できることを保証するように求められます。セクション 4 で説明したように、これらの欠点には、「Public Suffix」に対する共通で正確な意味論的定義がないこと、リストの作成に関する説明責任がないこと、リストの不完全性、形式の相違および特定のケースにおいてリストにプライベートな名前空間が侵入してしまうことなどが含まれます。

また、これらのリストは、そこに列挙される名前のポリシー決定に責任を持つ団体が維持するものではありません。リストは、DNS の中身に関する第三者による多数の解釈を示したものです。DNS からの包括的なポリシー情報を収集しようとする場合、第三者によるそのような試みは、本質的に避けられない弱点を抱えることになります。

さらに、DNS 自体の Public Suffix 空間の性質が変化することも注意すべき事項です。Public Suffix の数がゆっくりと増大し、Public Suffix の既存ポリシーの変更が頻繁でない場合、Public Suffix List の漸進的な維持はリストの正確性および完全性を向上させます。リストの完全性と正確性確保は、元来は静的なターゲットでした。

この環境は今や決定的に変化しました。TLD リストの拡大および顧客のニーズに対応する目的で行うドメインのポリシー変更は、Public Suffix セットがもはや少しも静的でなくなっていることを意味しています。PSL で内在する Public Suffix セットを追跡する際に起こる継続的な遅延は、最新の Public Suffix に対するユニバーサル・アクセプタンスの問題、この不一致の結果生じる cookie の意図しない利用またはドメイン名証明書の意図しない範囲に関連した当然の疑問を提起しています。

リストにこうした本来的な欠点がある状態では、正確性、完全性、適時性および信頼性という肝心の目的を達成できるのかという疑問が生じます。この情報の定義と作成のあり方を大幅に変えない限り、これらの目的を達成する方法を見出すのは困難です。設計要件が変更されやすいため、これらの問題が解決できたとしても、1 つのソースにこの情報を利便性の高い方法で維持することはできないかもしれません。

手動の PSL が必然的にこのような欠陥の影響を受け、せいぜい DNS の部分的側面しか見せることができないなら、PSL はその使用における必要な目的を達成できないかもしれません。特に、インターネットコミュニティが PSL の限界を知りながらセキュリティ機能としての PSL に依存するべきなのかは不明なところです。

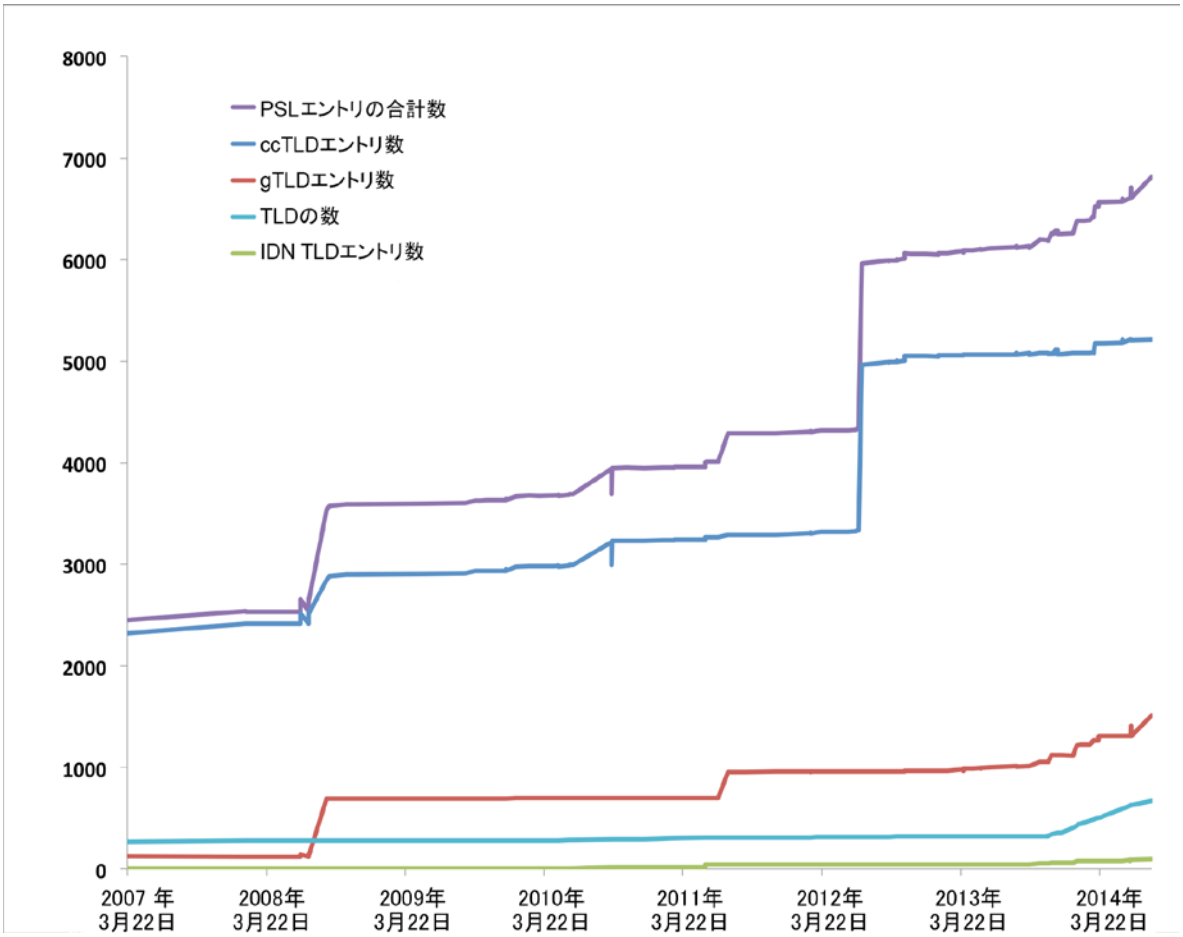
はっきりと異なる 2 つの概念を融合することは、通常は賢明ではありません。PSL

の概念は、プライベートな名前空間に対するパブリックな名前空間の境界点と、パブリックな DNS サフィックスの列挙とを融合して単一の総括表にすることができます。表 1 で示すように、DNS 階層における組織境界の不正確な仮定が情報の漏えいにつながる場合があり、第三者が DNS 内の境界の位置について何らか仮定するよう強いられることになります。DNS 内の組織境界のような情報が、ゾーンに責任を負う団体によって維持および公開されるようにすることがより慎重な方法なのかもしれません。この戦略により第三者の誤り、負担および遅延が解消されますが、そのためのコストがかかることになります。

7 新 gTLD の拡張性の問題

2014 年 8 月 11 日時点で、Mozilla PSL は 6,763 件のエントリを含むテキストファイルになっています。時間の経過と共に gTLD のエントリは増加しており、わずか 100 件強から 2014 年には約 1,000 件にまで達しています。しかし、Mozilla PSL に含まれる gTLD（457）のほとんどには、TLD 自身を示す 1 件のエントリしかありません。現在における gTLD のエントリ数の中央値は 1 であり、異常値があるため平均値は 43 ですが、PSL エントリの 75 番目のパーセンタイルは、8.5 です。PSL の総合的な gTLD エントリ数は直線的に増加する傾向にあり、gTLD エントリは、以下の図 1 に示すように PSL エントリ数のわずか 5 分の 1 となっています。

図 1：カテゴリ別の Mozilla PSL エントリ数の推移



この過去の統計から結論付けることができるのは、gTLD が最初はフラットで恐らく第 2 レベル登録のみを提供しているため、PSL の中身に関して言うと gTLD の追加が Mozilla PSL にもたらすオーバーヘッドは限定的だということです。しかし、この比率を大きく変更させる可能性がある複数のレジストリサービス評価申請が、現在保留されています。最も顕著な例は Atgron, Inc,（新 gTLD である.wed のレジストリ運用者）のものです。同社は、第 3 レベルのドメイン名登録提供を ICANN に要求しています [16]。このスキームによると、レジストリは 11,000 件の第 2 レベルドメインを予約し、第 3 レベルの登録を提供することになります。他のレジストリも同じような要望を出しています。実際、新 gTLD プログラムにおける多くの申請者は、ccTLD とより整合した、特に特定の地理に焦点を当てた形でレジストリを運用する意思を表明しています。一部の ccTLD には一般が利用可能な多数の委任をそのプライマリ TLD に追加する傾向がありますので、gTLD の拡張における過去の傾向は今後参考にならない可能性がります。

[16] Atgron.Inc.による ICANN レジストリサービス申請サービスの申請書：
https://www.icann.org/en/system/files/files/atgron-wed-request-08oct13-en.pdf

既存の.name レジストリは、非常に多数ある姓の第 2 レベルの下で多数の第 3 レベル登録を提供しています。しかし、同レジストリはそれらを Mozilla PSL に追加するよう求める申請は出していません。そのような膨大な変更によって PSL が著しく長大になる可能性があります。

これらを基に言えるのは、こうした傾向によって PSL が現在のサイズよりも 10 倍以上大きくなる可能性があるということです。このように大規模な静的ファイルは、依拠している PSL との迅速かつオーバーヘッドの少ないトランザクションを必要としているソフトウェアに、パフォーマンスの問題を発生させる場合があります。現在の状況は、インターネットの草創期に似ています。当時、全てのドメインエントリはオペレーティングシステムにある「hosts.txt」ファイルに置かれていました。DNS はこの問題を解決するために開発され、システムを分散し、クライアントのコンピューターが全てのドメインや TLD を保存することを不要にしました。予測される PSL のサイズは、全てのクライアントにロードされる固定のテキストファイル内で実装可能なものよりも大きくなるかもしれません。

8　結論

結論 1：PSL は利便性と内容の正確性との設計上の妥協です。

セクション 6 で詳細に説明したように、PSL は DNS におけるポリシーと組織境界に関する便利な総括表となることを目的としていますが、第三者が行うこれらリストの維持および管理の性質により、セキュリティが優先されるシステムで基本的な役割を果たすのに適したレベルの信頼性と適時性を確保することが事実上不可能です。

利便性とコンテンツの正確性との間にあるこの設計上の妥協の根底にあるのは、運用システムにセキュリティを実際に適用するときの共通のテーマです。利便性と効率性に対する要求およびオリジナルのソースからの権威ある命令に等しいものとして第三者の証明を受け入れる際の適切な用心の間には、常にトレードオフが存在します。

結論 2：「Public Suffix」およびその関連用語の定義についてコンセンサスはなく、実際のところ PSL は DNS 内の管理境界に関連する複数の目的のために使用されています。

セクション 4.1 の通り、「Public Suffix」の定義については意見の相違があり、定義を自分たちの明確なニーズまたはソリューションに基づいて行っている利害関係者の間でばらつきがあります。「Private Suffix」名を多くの PSL アプリケーションに追加することでこの状況は悪化します。これは、そのようなサフィックスに対して同一のニーズと利用例が数多くあるためです。「Public Suffix」と関連する用語について業界を広く網羅する一貫した定義がないため、このような混乱が生じて

います。また、その後露見した問題が示すように、この欠如は PSL の作成および使用の観点で、この報告書が説明した課題の多くにおいて中核をなしています。

結論 3：**問題に遭遇するかもしれない個人や組織が頼りにできるような、一貫した公正、公平な方法で PSL が生成されることを保証する説明責任の仕組みがありません。**

セクション 4.2 の通り、Mozilla PSL は、その公共性とかなり透明なプロセスがあることである程度説明責任を果たしているとみなすことができます。しかし、説明責任についてはギャップが存在します。一般的に、PSL の内容を決定する正式な権限または説明責任を有する組織や団体が今のところ存在しません。

結論 4：**Mozilla PSL とその他の PSL に対する変更および追加におけるプロセスと責任に関してレジストリと Public Suffix List 維持者との間にナレッジギャップがあります。**

結論 5：**PSL の使用に関する普遍的で共通したライブラリ、フレームワーク、ツールなどが存在しません。また、実装者がソフトウェアまたはその他のサービスにおいて PSL エントリを一貫性のある方法で使用していません。レジストリは自分たちのサフィックスについて全てのデバイスやアプリケーションで同じような動作を期待することができません。このような挙動によりユーザー体験が不安定になっています。**

結論 6：**PSL の変更をソフトウェアアプリケーションおよびインターネットサービスで実装する際のレイテンシはとても多種多様です。PSL のエントリ変更を更新および配布するサイクルは、新 TLD および/または TLD のポリシーの有用性と受け入れに影響します。**

セクション 5.2 の通り、最良のシナリオでもレイテンシは 12 週間程度になる可能性があります。通常はこれ以上のレイテンシが生じることが多く、全く更新されない PSL も中には存在します。

結論 7：**PSL の内容と維持者からユーザーへの PSL への伝送について認証およびその他の標準的なセキュリティコントロールが一般的に欠如しています。**

結論 8：**PSL の使用事例が多様であるため、全ての応用や使用方法を網羅でき、全ての対象者に適用される万能型の PSL を作成するのは困難かもしれません。**

結論 9：**新 gTLD が既存 gTLD と似た Public Suffix を使用する場合、その TLD 全体が「パブリック」であるため、存在する Public Suffix は 1 つになることが多い状況です。そしてこの場合、PSL のサイズへの影響は限定的です。しかし、新 gTLD が 2 つ以上のパブリックサブドメインを含む一部の ccTLD のように Public Suffix を使用する場合、PSL への影響が大きくなる可能性があります。**

9　勧告

第一に、SSAC は IETF とアプリケーションコミュニティに対し、代替となるソリューション（勧告 1 参照）を設計、標準化および適用することにより、この基本的な設計上の妥協に直接対応するように求めます。第二に、PSL が広く利用されていること、そして IETF が代替のソリューションを標準化しコミュニティがそれを展開するまでに時間を要することから、PSL の現在の維持管理と使用に関するいくつかの優先度の高いリスクを緩和する短期的な方策を講ずることを勧告します（勧告 2〜6）。

勧告 1：PSL の代替ソリューションが議論されていることから（付録 A 参照）、SSAC は IETF およびアプリケーションコミュニティに対し、IETF のプロセスを介して詳細な仕様を策定しできる限り標準化していく方向で検討するよう勧告します。

その取り組みにおいては、新たな標準とソリューションによって対応すべきプロブレムステートメントを検討する際のインプットとして、本報告書で提起された課題を考慮しなければなりません。

「各種のインターネットプロトコルとアプリケーションには、2 つのドメイン名が関連しているかどうかを決定する仕組みが必要である」という所見から提起された課題を検討する目的で 2015 年 4 月に設置を認められた DBOUND ワーキンググループは、他の種類の管理境界に関連づけつつ、この問題のもっと一般化したバージョンについて検討しています。しかし、「Public Suffix の指定」の問題について関心がある技術者は、そこに参加することを検討すべきです。

勧告 2：IETF は、「Public Suffix」と関連する用語（例：「Private Suffix」）の定義についてコンセンサスを形成するべきです。

DBOUND のチャーターおよびプロブレムステートメント案では、追加するべき有用な区別がいくつか提案されています。

勧告 3：レジストリと一般的な PSL 維持者の間にあるナレッジギャップを解消するため、ICANN と Mozilla Foundation は、TLD レジストリ運用者に提供できる Mozilla PSL 関連の資料を協力して作成するべきです。

勧告 4：インターネットコミュニティは、PSL に対する現在のアプローチを標準化するべきです。特に以下に示す対策が必要となります。

勧告 4a：ユニバーサル・アクセプタンスに関する取り組みの一環として、ICANN はソフトウェア開発コミュニティ（オープンソースコミュニティを含む）に対し、PSL の堅牢な（認証され、適時性があり、安全で、説明責任のある）配布の仕組みを実装しながらプログラミングおよびオペレーティングシステムのライブラリを開発および配布するよう、奨励していかなければなりません。これらのライブラリ

は、あらゆるプラットフォームで PSL の一貫した標準的な解釈ができることを保証すべく、全ての共通したプラットフォームおよびオペレーティングシステムを横断するように記述されるべきです。

勧告 4b：アプリケーション開発者は、この作業の仕様として、標準的なファイル形式と最新の認証プロトコルを使用するべきです。

勧告 4c：アプリケーション開発者は独自の PSL を、Mozilla PSL や提案されている IANA PSL（勧告 5）のようによく知られ広く受け入れられている PSL 実装に置き換えるべきです。

勧告 5：IANA は、IANA が直接やりとりしているレジストリ内のドメインに関する情報を含む PSL をホストするべきです。このような PSL は、当該ドメインについて権威あるものとなります。

そのリストは少なくとも、IANA ルートゾーンにある全ての TLD を含んでいるべきです。

勧告 6：ICANN は、PSL に関連した使用とアクションをユニバーサル・アクセプタンスに関する作業に明示的に含めるべきです。

10 謝辞、利害関係の開示、反対意見および議論の忌避

透明性を確保するため、以下に続くセクションでは読者に対し SSAC プロセスにおける 4 つの観点についての情報を提供します。謝辞のセクションでは SSAC メンバー、外部専門家および本書に直接貢献した ICANN スタッフの一覧を掲載します。利害関係開示のセクションでは、全 SSAC メンバーの経歴を紹介し、あるメンバーが本報告書の作成に参加することで実際の利益相反を生じる、または生じるように見える、あるいは潜在的に利益相反を生じるかもしれない利害関係を開示しています。反対意見のセクションは、個々のメンバーが、本書の内容または作成プロセスに関して反対意見を持っている場合にそれを説明する場として設けています。議論の忌避のセクションでは、本報告書が扱う話題の議論を忌避した個々のメンバーを特定します。反対意見および議論の忌避のセクションに掲載するメンバーを除き、本書は SSAC の全メンバーの総意により承認されています。

10.1 謝辞

以下のメンバーおよび外部専門家が本報告書の作成にあたり時間、労力および意見を提供してくれたことについて、SSAC として感謝の意を表します。

SSAC メンバー

Jaap Akkerhuis
Patrik Fältström
Geoff Huston
Warren Kumari
Danny McPherson
Ram Mohan
Rod Rasmussen
Suzanne Woolf

招待されたゲスト参加者：
Casey Deccio[17]
Jothan Frakes

ICANN スタッフ

Patrick Jones
Julie Hedlund
Kathy Schnitt
Steve Sheng（編者）
Jonathan Spring

10.2 利害関係の開示

SSAC メンバーの経歴情報および利害関係の開示情報は、以下より入手できます。
https://www.icann.org/resources/pages/biographies-2014-10-08-en

10.3 反対意見

反対意見はありませんでした。

10.4 議論の忌避

忌避したメンバーはいませんでした。

[17] 本件について彼が行った ICANN 主任研究員としての貢献について。

付録 A：Public Suffix List の代替案

SSAC では、Mozilla PSL に代わる次の手段があることを認識しており、インターネットコミュニティがこれらの仕様化と適用を検討すべきであると考えています。

Public Suffix 構造化ファイル形式

新たな PSL の設計が、ファイル形式と取得方法を標準化するために提案されています。[18] Extended markup language（XML）が、この設計で提案されているリストの形式です（実際には JavaScript Object Notation（JSON）またはその他の構造化言語も使用できます）。取得の方法としては Hypertext Transfer Protocol（HTTP）が提案されています。この形式では、トップレベルドメイン（TLD）、また必要な場合にはトップより下の複数レベルで、Public Suffix を柔軟に定義できます。取得は Secure Sockets Layer（SSL）などの方法で安全に行うことが可能です。

標準的な Public Suffix の配布方法

この提案は、構造化ファイル形式に依存しています。ファイル形式が標準化されれば、リストの維持と配布も標準化できます。このシステムを現在の Mozilla PSL と比較したときの利点は、TLD レジストリに維持が分散されるため単一の団体がリスト全体の更新について責任を負う必要がなくなることです。その代わりに、各 TLD が自らのツリーを維持する責任を追うことになります。しかし、下位の団体が独自の Public Suffix を再帰的に維持できるような委任プロセスは定義されていません。複雑な Public Suffix のシナリオでは、これは受け入れられない場合があります。

ドメインネームシステム（DNS）を用いたドメインの検証の強化

別の提案では、DNS 名が Public Suffix かどうかを判別するために DNS および HTTP を使用することが提案されています。[19] この提案では、ブラウザが当該サフィックスについてタイプ「A」（アドレス）の DNS ルックアップを実行し、その応答はサフィックスがパブリックであるかどうかを決定するために使用されます。つまり、通常は Public Suffix に関連付けられたアドレスがあるとは想定されない、ということです。クライアントがこのような DNS ルックアップを実行できない場合には、代わりにサフィックスに HTTP HEAD 要求を実行できます。そこで成功の応答が得られれば、当該ドメインが Public Suffix ではないということになります。

単純さがこの提案の長所です。しかし、単純さは短所にもなります。

Internet Engineering Task Force（IETF）における関連作業

DBOUND（*D*omain *Bound*aries）は IETF で新たに設置が認められたワーキンググループで、2 つのドメイン名が関連しているかどうかを決定するソリューションの

[18] https://tools.ietf.org/html/draft-pettersen-subtld-structure-10

[19] https://tools.ietf.org/html/draft-pettersen-dns-cookie-validate-05

策定を目的としています。[20] DBOUND の 2015 年 1 月版プロブレムステートメント案（http://datatracker.ietf.org/doc/draft-sullivan-dbound-problem-statement/）はまだ完全ではないものの、「ポリシー領域」を定義することがドメインの関係の有無を決定する一つの仕組みになると述べています。しかし、ポリシー領域を決定する現在の方法、つまり Mozilla PSL は、不十分であると考えられています。「ポリシー領域」とは、概して言えば、1 人の管理者のコントロール下にあるドメインの一群です。[21] DBOUND ワーキンググループからは DNS ポリシー領域の境界を主張する提案と組織境界を公開する提案という 2 つの違ったソリューションが出ていますが、まだ議論の初期段階にあります。

DNS ポリシー領域境界の主張 [22]

同じ DNS サブツリー内のどのドメインが関連しているかを定義するソリューション案の 1 つは、DNS で「start of policy authority」（SOPA）レコードを作成することです。提案されているこの SOPA レコードによって、ドメイン管理者は対象のドメインがドメインのポリシー領域に含まれているかどうかを明確に示すことができます。ただ、この提案の作者は、DNS セキュリティ拡張（DNSSEC）を使用しなければなりすましやキャッシュポイズニングといったお決まりの問題が発生するということを認めています。このソリューションは対象のドメインがオーナー名の祖先、子孫、または兄弟である場合にのみ有効であり、DNS サブツリー全体を横断的にリンクする場合には賢明な策ではありません。

DNS での組織境界の公開 [23]

どのドメインが同じ組織の管理下にあるかを定義する 1 つのソリューションとして、新しいサブドメイン「_ob」を作成し、このドメインを TXT レコードに挿入して組織の境界をマークする、という方法が提案されています。この提案には、複数の組織境界の移行を処理する方法も含まれます。_ob ドメインへのクエリに対して NXDOMAIN または NSEC の結果が返されるまで、ルックアップごとに 2 回または 3 回の DNS クエリが必要となります。このソリューションは DNSSEC がない時に通常起こる問題を抱えており、加えて、DNS サブツリー全体で関連ドメインを横断的にリンクすることはできません。

[20] https://datatracker.ietf.org/wg/dbound/charter/

[21] https://datatracker.ietf.org/doc/draft-sullivan-dbound-problem-statement/?include_text=1

[22] http://tools.ietf.org/html/draft-sullivan-domain-policy-authority-01

[23] https://tools.ietf.org/html/draft-levine-orgboundary-02

付録 B：Mozilla の Public Suffix List

Mozilla PSL のエントリ

2014 年 8 月 11 日時点で Mozilla PSL は 6,763 件のエントリを含むテキストファイルになっており、次の 2 つのセクションに整理されます。

- *ICANN* ドメインセクションには、6,333 件の gTLD および ccTLD のサフィックスエントリが含まれます。このセクションは、ICP-3[24]に準拠するサフィックスを含むようになっており、IANA から直接委任されるか、IANA に関連付けられます。
- *プライベート*ドメインセクションには、 CentralNic（eu.com や us.org などの所有者）のような多数のサブドメイン登録サービスおよび DynDNS、Amazon、Google、GitHub、Heroku のような企業に加え、ドメインネームシステム（DNS）とクラウドサービスを提供する Microsoft と Red Hat といった企業からのエントリがあり、合計で 430 件が含まれています。[25]一部の登録ドメイン所有者は互いに信頼関係のない複数の団体にサブドメインを委任する場合があり、そのためにこのセクションが存在します。

ICANN ドメインセクションとプライベートドメインセクションの PSL エントリにおけるラベルの分布を分析すると、PSL がどのように使用されているかについて定量化可能な統計情報を得ることができます。この分布は、ラベル数、セクション（ICANN またはプライベート）および TLD の種類という 3 つの変数に応じて示されます。

表 3：PSL におけるエントリのラベル分布 - エントリの種類別

	gTLD	ccTLD	IDN 小計	合計
1 ラベル-ICANN	457	225	87	769
2 ラベル-ICANN	651	2,986	6	3,643
3 ラベル-ICANN	0	1,918	0	1,918
4 ラベル-ICANN	0	3	0	3
1 ラベル-プライベート	0	0	0	0
2 ラベル-プライベート	308	70	0	378
3 ラベル-プライベート	27	9	0	36
4 ラベル-プライベート	15	1	0	16
総計	1,458	5,212	93	6,763

1 ラベルのエントリ（すなわち TLD）は定義上、Public Suffix です。ccTLD 下の 2 および 3 レベルのエントリは、PSL エントリの 72.5%を占めています。これらの

[24] https://www.icann.org/resources/pages/unique-authoritative-root-2012-02-25-en

[25] Hiroku Website セキュリティノート：https://devcenter.heroku.com/articles/cookies-and-herokuapp-com

エントリの大部分は ccTLD が示す国内の地理的な地域に対応しており、[26] 少数の TLD がリストの大部分に寄与しています。

表 4：PSL の ICANN ドメインセクションにある 50 エントリ以上の TLD

TLD	PSL エントリ数
JP	1748
NO	754
MUSEUM	549
IT	369
US[27]	225
PL	180
RU	133
AERO	90
UA	79
BR	71

Mozilla PSL の成功要因

Mozilla PSL プロジェクトは検討事項を限定した形で開始し、ブラウザのセキュリティとユーザーのプライバシーを向上することのみを目的にしていました。以降、このプロジェクトは成功を収めています。Mozilla PSL は大多数のブラウザで使用されており、したがって派生的利用も数多くあります。この広範な適用は、このような「サフィックス」リストに対するニーズを物語っています。他の似たような取り組みも存在していますが、ほとんどは本格化しなかったり頓挫したりしており、代わりに Mozilla PSL が使用されているようになっています。というのも、Mozilla PSL がニーズを満たしているためです。Mozilla Firefox、派生的ユーザー、インテグレーター、開発者およびプロジェクトで、Mozilla PSL が成功を収めることになったいくつかの要因があります。

- １つの団体がリストを管理しています。変更についての連絡先が 1 つであり、変更を承認するプロセスが 1 つです。
- 維持者が信頼のおける組織であり、HTTP の使用、プライバシーおよびセキュリティについて十分な知識を有しています。
- PSL が使用されるシステムと緊密に統合できるよう、バグ追跡システムによるバージョンコントロールがあり、リリースサイクルに従っています。
- エントリのデータベースをアプリケーションに埋め込むことができます。これにより、ルックアップの頻度が高い場合でもレイテンシを軽減でき、

[26] .us の場合多くのレガシーエントリは RFC 1480 に従っており、米国の各州が、例えばアイダホ州なら「id.us」といった形式で表現されています。
[27] 通常、.US の下にある 3ld+より下のエントリは、RFC 1318 または RFC 1480 のレガシーエントリです。

レコードレベルのルックアップが迅速かつ効率的になります。

- 合理的な「TLD」の論理への幅広いニーズに対応した既存ソリューションであるため、開発者は開発に専念できます。