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
Japan Network Information Center

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 7 月号

新 gTLD の導入に伴う「内部利用目的での証明書への影響」に関する SSAC による勧告について

1. はじめに

新 gTLD プログラムの開始により、今後 1,000 を超える gTLD が追加されることが見込まれている一方、企業などの内部ネットワークで利用しているローカルなドメイン名やホスト名（以下、内部利用名)が新 g TLD の文字列と衝突する可能性があります。
これに伴うセキュリティ上の問題として、新 gTLD と文字列が衝突する内部利用名に対してサーバ証明書を発行し、Web サーバの認証に利用できることが確認されています。

ICANN のセキュリティと安定性に関する諮問委員会(Security and Stability Advisory Committee; SSAC) [1]では、この問題に伴うセキュリティ上の脅威を指摘する SSAC 勧告、「SAC057 : SSAC Advisory on Internal Name Certificates[2]」を 2013 年 3 月に出しています。本ポリシーレポートでは、この SAC057 についてご紹介します。

2. 内部利用名に対するサーバ証明書発行

インターネットユーザーが、SSL を利用して Web サイトを参照する際、ユーザーの Web ブラウザは、サーバ証明書を持つ Web サイトのみを、信頼できる Web サイトとして認識します。

上記のような Web サイトの信頼性を確認する上で、サーバの認証に用いられる「サーバ証明書」は、通常、認証局(Certificate Authority; CA)と呼ばれる組織により、申請者がその Web サイトで利用しているドメイン名の登録者であることを確認した上で発行されています。

証明書は、その信頼性が重要です。そのため、基本的に CA ではサーバ証明書発行申請を受けると、申請者がドメイン名の正当な利用者であることを確認する手段の一つとして、サーバ証明書で申請されているドメイン名の利用者を、TLD レジストリに登録されている情報などから調べ、サーバ証明書の申請者がそのドメイン名の登録者であることの確認を取った上で、証明書を発行していることが一般的です。

しかし企業内など、インターネットに接続されない内部ネットワークにおいても、サーバ証明書を取得したいという需要は少なくありません。この場合、サーバなどに利用される「www.company.local」、「server1.company.corp.」等のドメイン名や、NetBIOS で使われている「Web1」、「ExchCAS1」、「Frodo」等のホスト名などが、内部利用名によるサーバ証明書の取得において利用される文字列の例として挙げられます。

これらの内部利用名は、TLD レジストリのデータベース上に登録されているものではなく、申請者がドメイン名の登録者であることの検証ができないため、多くの CA では、既存の

[1] http://www.icann.org/en/groups/ssac
[2] http://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf

TLD との重複が確認されなければ、そのまま証明書の発行を行っているのが実情です。

3. 新 gTLD の導入に伴い確認されている問題

内部利用名のサーバに対して既に発行されたサーバ証明書の中には、証明書に含まれる内部利用名が、申請中の新 gTLD と同一での文字列であるということが起こり得ます。

また、新 gTLD として申請中の文字列は、ICANN からの TLD の委任が完了していないため、本稿執筆時点で内部利用名に対するサーバ証明書の発行申請を受けた場合、多くの CA では既存の TLD のように、レジストリの登録情報を確認する術がなく、内部利用を目的とした申請として、証明書の発行を進めています。

すなわち、新 gTLD の運用開始後、内部利用名と新 gTLD が衝突してしまった場合、内部利用を目的とした証明書の発行を受けた組織は、その証明書を Web サーバ向けの証明書として流用してインターネット上に Web サイトを立ち上げれば、内部利用名と同じ名前をインターネット上で正式に持つサーバに成りすまし、証明付きの信頼できるものとして見せることが可能となるため、顕著なセキュリティ上の脅威となるのです。

SAC057 勧告では、SSAC のメンバーが行った、申請中の gTLD を含む内部利用名によるサーバ証明書を CA から取得して、Web サイトを立ち上げるまでの実験についても記述してあります。

それによると、SSAC メンバーが申請中の新 gTLD の一つである".site"を含むホスト名「www.site」へのサーバ証明書を、内部用途として申請したところ、1 年間の有効期限を持つ証明書が発行されました。さらに、ローカルで構築した偽のルート DNS サーバ上で、www.site の委任設定を行った上で、www.site を証明書付で運用したところ、複数の主要な Web ブラウザが、内部利用目的での証明書を正しいものと認識する、すなわち、インターネット上で正しく委任されたホスト名の場合と同様に、偽の Web サイトを、正当なものと見なしていることも確認されました。

さらなる詳細については、本勧告 SAC057 の「2.2 Case Study」項目にて、実験で実施した一連の手続きが、証明書や Web ブラウザのスクリーンショット等も含めて紹介されていますのでご確認ください。

4. 内部利用を目的とした証明書の発行状況

ここまでに示した通り、内部利用名と新 gTLD が衝突する場合、内部利用を目的とした証明書の発行を受けた組織は、その証明書を Web サーバ向けの証明書として流用して、インターネット上の Web サイトを立ち上げ、内部利用名と同じ名前をインターネット上で正式に持つサーバに成りすまし、証明付きの信頼できるものとして見せることが潜在的には可能となります。SAC057 勧告で引用されている SSL Observatory[3]の調査によると、157 の CA が内部利用名を含む証明書を発行したことが確認されており、発行された証明書数は 37,244 件となります。このうち、サーバ名に申請されている新 gTLD の文字列と同じ TLD を用いている証明書が 1,053 件、うち現在も有効期限内の証明書は 210 件あるそうです。これらは 2010 年時点での調査結果であり、また、インターネット上で確認できているもの

[3] https://www.eff.org/observatory/

に限った数であるため、内部ネットワークに閉じて利用されているものも含めると、実際の発行数はさらに多いと SSAC の勧告では推定しています。

5. SSAC および ICANN セキュリティチームによる対応

この問題は、SSAC による勧告が策定される以前に、認証局とブラウザベンダーが集まるフォーラムである CA/Browser Forum[4]（以下 CA/B Forum）でも認識されており、2016 年[5]までに対策を採ることが 2012 年 7 月の総会で決議されていました。しかし、それでは 2013 年の新 gTLD の導入開始から約 3 年間、脆弱性のある状態での運用が続けられることになります。

SSAC では、この問題は迅速な対応を必要とするセキュリティ上の脅威であり、かつ、対策が採られるまでは状況を広く公開するべきではないと判断し、2012 年 11 月に SSAC メンバーにより問題提起が行われた後、2013 年 1 月に勧告文書を完成させ、まずは ICANN のセキュリティチームに個別に報告を行いました。そして、一定の対策が採られたことを確認した上で、2013 年 3 月に本勧告を公開しています。

6. ICANN への勧告

SSAC から ICANN に対して行った勧告は以下の通りです。

- 申請中の新 gTLD を委任済みの TLD と同様に扱うようにとの、CA/B Forum および CA への呼びかけの実施、また、より幅広い影響と回避策の検討
- 回避策が適用される前に情報を公開することにより、ユーザーへの被害が広がる可能性を踏まえ、極秘に関係者とのやり取りを進める必要があることから、CA/B Forum と CA との信頼関係の構築
- 脆弱性が公開された時点で悪用が容易となることを考慮した上での、脆弱性に関する情報公開ポリシー(Disclosure Policy)の適用
- 情報公開ポリシーに基づき、影響を受ける関係者に対するコミュニケーションプランの策定
- 脆弱性が不適切に早い段階で漏洩した場合に備えた緊急時の対応策、および積極的な脆弱性の公開計画策定

7. 現在の状況

ICANN のセキュリティチームからの連絡に基づき、CA/B Forum は 2012 年 2 月の年次総会で、メンバーに対して以下の対策を求めることを決議しました。

・新 gTLD 向けの契約締結後、30 日以内に新規証明書の発行を停止
・新 gTLD 向けの契約締結後、120 日以内に発行済みの証明書を失効(revoke)

従って、当初の予定であった 2016 年まで対応を待たず、上記に示す新 gTLD の委任開始直

[4] https://www.cabforum.org
[5] ICANN ダーバン会議でのセキュリティ、安定性、回復性(SSR)セッションでの CA/B Forum の代表者からの発表では 2015 年となっていました（スライド 11）。
http://durban47.icann.org/meetings/durban2013/presentation-certificates-revocation-17jul13-en.pdf

後の時期に、証明書の発行停止および失効が行われることになりました。

ただし、上記の措置は CA/B Forum のメンバーである主要な CA に対しては適用されますが、その他の CA に対して適用されるものではない状況です。従って、引き続きこれらの CA においても、脅威の軽減に向けた対応は必要となります。

なお、Firefox などを提供している Mozilla 財団は、この脅威に対応するために、 同財団の提供する Web ブラウザのルート証明書ストア(Trust Store)に自社の証明書が登録された状態を維持するためには、2013 年 7 月 31 日までに上記の CA/B Forum の決議に対応することを、現在登録されているすべての CA に求めています。

8. 発行済みの内部利用を目的とした証明書への対応

第 47 回 ICANN ダーバン会議[6]での“Security, Stability & Resiliency (SSR) Update”セッション[7]では、CA/B Forum の代表者から CA/B Forum では、新 gTLD の文字列と一致する内部利用を目的とした証明書の発行を受けている組織に対して、個別に連絡を取る措置を進めているとの発言が確認されています。

また、同セッションでは CA/B Forum の代表者から ICANN に対して「内部利用を目的とした証明書において、DigiCert や PayPal で最もよく利用されている文字列を含む gTLD の申請は、申請自体の承認は行っても、委任を 2015 年まで遅らせる」ことを求める助言(Recommendation)が発表されました。なお、DigiCert は.corp の委任に懸念を示した書簡[8](2013 年 3 月 7 日)を、PayPal も新 gTLD との重複が懸念される名前の一覧を示した書簡[9](2013 年 3 月 15 日)を、それぞれ ICANN に提出しています。

これらの文字列は、多くの組織の内部ネットワークで利用されているために、現時点で内部利用を目的とした証明書を失効すると影響が大きいと考えられています。現在発行されているすべての証明書の期限が 2015 年には切れるため、上記の助言(Recommendation)に至ったということです。

現在、DigiCert の Web サイトでは、内部利用を目的とした証明書に関して、Microsoft Exchange のためのセキュリティ対策となる設定の方法を案内しています。詳細については、以下の Web サイトをご確認ください。

DigiCert Internal Name Tool for Microsoft Exchange
http://www.digicert.com/internal-domain-name-tool.htm

9. 内部利用名に関するその他の課題

ここまでに述べたサーバ証明書の問題以外に、新 gTLD で申請されている文字列と、内部利用名が衝突した場合の影響に関する調査の結果が前述の SSR セッションで発表され、具体的な影響に関するさらなる調査の必要性が確認されています。この調査によると、DNS ルートサーバにおける検索数が多い TLD として、.home が 5 位、.corp が 15 位に挙げられ

6 http://meetings.icann.org/ICANN47
7 http://durban47.icann.org/node/39759
8 http://www.icann.org/en/news/correspondence/wilson-to-chehade-crocker-07mar13-en
9 http://www.icann.org/en/news/correspondence/hill-smith-to-chehade-crocker-15mar13-en.pdf

ています。一方、この調査に対して、「単純に検索数が多いから問題が大きいとは限らず、これらの名前が、組織の内部ネットワークでどのように利用されているのかによって、影響の度合いを検証する必要がある」との意見が、ICANN ダーバン会議の当該セッションでは表明されていました。

詳細については、SSR セッションの発表資料 [10]をご確認ください。セッションでの議論の発言録(トランスクリプト)も、追って公開される予定です。

10. 終わりに

本稿で紹介したように、SSAC は新 gTLD の導入に伴い対応が必要となるセキュリティ上の課題について、適宜勧告を出しています。また、SAC057 勧告は、SSAC が勧告の発表前に ICANN に必要な対応を促し、取るべきセキュリティ対策につなげたという興味深い事例です。

本勧告に伴う継続課題への対応は、現在も ICANN コミュニティで議論と検討を続けており、新 gTLD の委任までのプロセスをできるだけ遅らせることなく円滑に進めていきたいという新 gTLD 申請者の要請と、セキュリティ上の懸念への対応とのバランスを ICANN がどう取っていくのか、引き続き動向を注視していく必要がありそうです。第 47 回 ICANN ダーバン会議における GAC 勧告では、ICANN 理事会に対して、問題の分析を直ちに行うことが求められています。

また、これらのセキュリティの脅威について、ICANN 会議などには参加しておらず、実際に影響を受けるユーザーへの周知をどうしていくのかについても、今後の課題として挙げられます。

なお、SSAC では新 gTLD に関する報告・勧告以外にも、DNS を利用したコンテンツのブロッキングや WHOIS 登録情報の認証など、その他 ICANN の活動に関連する勧告を発行しています。興味のある方は、以下の URL からこれまでの SSAC の報告・勧告をご確認ください。

http://www.icann.org/en/groups/ssac/documents

11. 謝辞

本稿の執筆にあたり、SSAC メンバーである株式会社日本レジストリサービスの佐藤新太氏に貴重なアドバイスをいただきました。ここに感謝の意を表します。

[10] http://durban47.icann.org/node/39759