インターネット標準化
推進委員(ISPC)の
目で見た

IETF101ホットトピック・全体総括報告

2018年4月27日

IETF101報告会

米谷嘉朗
<yoshiro.yoneya@jprs.co.jp>

もくじ

1. TLS Visibility
2. The DNS Camel
3. IASA 2.0
4. The Future of Internet Access
5. 全体総括

1. TLS Visibility (1/4)

- 背景
  - データセンター(DC)内の企業ネットワークでTLS 1.3をどのように運用するかについての議論
    - IETF97@Seoul(2016年11月)のtls WGで議論が始まったもの(cf IETF97報告会、IETF99報告会資料)
  - トラブルシューティングのためDC内の企業ネットワーク管理者がTLS 1.3で暗号化された通信を復号したいというもの

1. TLS Visibility (2/4)

- 現在の提案
  - I-Dはdraft-rhrd-tls-tls13-visibilityとして書き換えられ、クライアントサーバ間のTLSセッションを認定済の第三者がプレインテキストでアクセスできるようにするオプトイン機構(TLS Visibility Extension)を追加しようとしている
  - ネットワーク管理者が事前に生成した鍵ペアの秘密鍵を認定済の第三者に渡しておき、セッション暗号鍵を導き出せるようにするというもの

1. TLS Visibility (3/4)

- 議論のポイント
  - 支持者側
    - 運用者の運用負荷を軽減する
    - ユースケースをDC内の企業ネットワークに限定する
  - 反対者側
    - TLS 1.3の目的を、tls WGチャーターの更新が必要なほど変更するものである
    - 攻撃のリスクを増加させる
- WGでの結論
  - WG I-Dにするかの Hum
    - 賛成：大、反対：大で結論出ず
  - 今後の進め方はチェアと担当ADで相談する
    - ADコメント：ユースケースが非常に重要である

1. TLS Visibility (4/4)

- セキュリティと運用性のギャップ
  - 運用者は暫定的な解と根本的な解のどちら望んでいるか？
    - どのようなソリューションをいつ得られるかに依存
  - ソリューション製品買いで十分か？
    - 適切な価格で得られるか
    - ベンダーが製品をサポート外にしたらどうするか
  - 「普通の」運用者の声をどうやって伝えるか
    - ユースケース、ベストプラクティス、要求条件など

- TLS 1.3の詳細は特集2で！

2. The DNS Camel (1/3)

- DNSはラクダのように何でも運べる？
  - IETFでは車輪の再発明を避けるため、既存の「成功した」プロトコルが使われる傾向にある
    - HTTP、TLS、DNSなど(そのうちQUICも？)
  - ただし、使われるプロトコルは複雑さが増すことが多い
    - 実装、運用の両面において
    - 新規オプション・拡張・プロファイルなどの追加による
    - DNSSECなど
    - IETFはあまりこの点に注意を払ってきていない
  - dnsop WGでの議論

2. The DNS Camel (2/3)

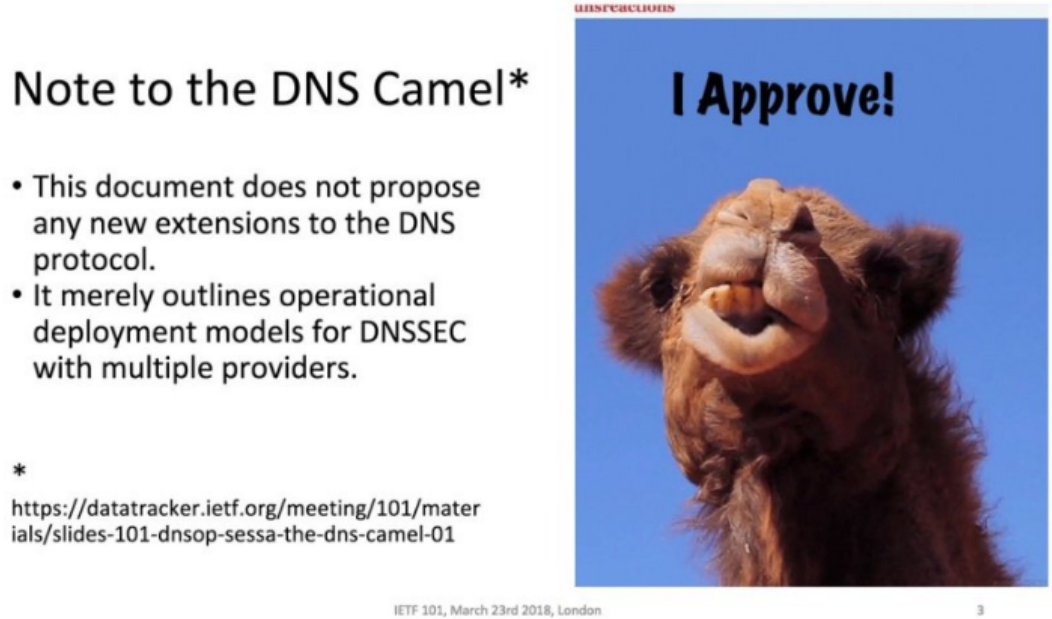
- The DNS Camel：DNS実装者兼DNSプロバイダの叫び
  - DNSに依存するRFCは増加する一方である
  - DNS実装者は「できない」とは言えない
    - プライド、他の実装との競争、新機能への興味
  - 運用者は寡黙に24/7張り付けになる
    - 午前3時でも対応を要求される
    - 標準作成者はその実態を知らない、もしくは運用を過小評価している
  - もっと時間をかけてしっかり議論してほしい
    - 誰にとっての利益になるのか
    - 誰がコストを負担するのか
    - 実装者や運用者の意見は十分に取り込めているか

2. The DNS Camel (3/3)

- dnsop WG参加者の反応
  - 大喝采
  - プロトコルは柔軟な拡張機能を備えるべき
  - 実装すべき最小限の機能をリストアップしよう
  - プロトコルはシンプルに保つべき
  - 運用者の意見をもっと取り込もう
- IETF全体への波及、Plenaryでの意見
  - IETFをもっと運用者が参加できる場にすべき
    - 現状で参加している運用者は“Super Sophisticated”な人たちだ
  - 運用者が管理できるプロトコルを作るべき
  - 何でも暗号化するのは良くない

There was enthusiasm for the idea of going through the "200 DNS RFCs" and deprecating stuff we no longer thought was a good idea. This enthusiasm was more in theory than in practice though as it is known to be soul crushing work.

The concept however of reducing at least the growth in DNS complexity was very well received. And in fact, in subsequent days, there was frequent discussion about the "DNS Camel":



And in fact, a draft has even been written that simplifies DNS by specifying DNS implementations no longer need to probe for EDNS0 support. The name of the draft? draft-spacek-edns-camel-diet-00!

I'm somewhat frightened of the amount of attention my presentation got, but happy to conclude it apparently struck a nerve that needed to be struck.

Next steps

So what are the next steps? There is a lot to ponder.

I've been urged by several very persuasive people to not only rant about the problem but to also contribute to the solution, and I've decided these people are right. So please watch this space!

https://blog.powerdns.com/2018/03/22/the-dns-camel-or-the-rise-in-dns-complexit/

3. IASA 2.0 (1/2)

- IASA 2.0は、IETF Administrative Support Activity (RFC 4071)の改訂活動
  - IETF 101まではBoF
  - 2018/4/20にGENエリアでWG化(iasa2)
- モチベーションは、IETF運営活動をより安定させること
  - 会場選び(mtgvenue)プロセスの実装
  - 運営の人的資源確保(事務局、RFCエディタなど)
  - 運営の費用確保(参加費、スポンサー費、支援金)
  - 運営組織の法人化

  など

3. IASA 2.0 (2/2)

- これからの方向性
  - ISOCとの合弁会社設立
    - ISOCとの関係、税金対応などの理由
  - IETF参加費の値上げ
    - 運営費確保のため
    - リモート参加の増加により参加費の予測精度が下がっている
    - 2019年以降段階的に値上げしていく方針
- Plenaryでの意見
  - ローカル参加者を増やすことを考えるべき
  - スポンサー制度など他の収入源も考えるべき
  - 所得の低い地域からの参加者にとっては、参加費以外の支出(VISA取得費用、宿泊費など)が大きいことも考慮してほしい

4. The Future of Internet Access

- IAB Technical Plenaryのテーマ
  - gaia (Global Access to the Internet for All) RGからのフィードバック
- Wirelessネットワークへの期待
  - インターネットインフラとして
    - 途上国におけるインターネット普及はまだ伸びしろが大きい
  - 小規模な民間サービスとして
    - 先進国においては電波行政変化の遅さ、電波オークション高額化などの問題がある
  - 人口衛星を通信手段として
    - 低軌道衛星であれば広帯域・低遅延で

- 次世代Wireless(5G)の詳細は特集1で

5. 全体総括 (1/2)

- IETFは大きな転換点を迎えている
  - 妥当なコストで実装・運用できるプロトコルが開発できなければIETFの維持はますます難しくなる
  - IABもIESGもその認識をもって「普通の」実装者や運用者の参加を求め始めた
- もっとプロトコル実装者(ソフトウェア・サービス)、運用者視点の声をIETFに届けよう
  - RFCの曖昧さや運用性問題の指摘、具体的なユースケースの提示、経験に基づくプラクティス(成功・失敗いずれも)の提示
  - プロトコル設計者の認知向上が重要

5. 全体総括 (2/2)

- IETF参加の現状
  - ML参加、現地参加、リモート参加
  - 敷居が高い
- 敷居を下げるためにできること
  - 周囲の人・コミュニティへの状況の伝達、および議論
  - 蓄積されたプラクティスの文書化
  - IETFに馴染みがある人への相談
- 近い将来にできそうなこと
  - HotRFCで紹介されたRFC Annotationsの活用

Q&A