DNSとドメイン名に関連した標準化の動向(IETF)

～ extended DNS errors、iotops、danish ～

木村泰司

話者について

名前	木村泰司
所属	日本ネットワークインフォメーションセンター(JPNIC)
業務	セキュリティ/認証局/RPKI 国際動向 → IETF他, レジストリ
活動	• JNSA PKI相互運用技術WG • WIDEプロジェクト moCA WG, ボード • フィッシング対策協議会 技術・制度検討WG • セキュリティ・キャンプ 講師
IETF	• MLは1997年頃より、ミーティングは2002年頃より

内容

- **DNSとドメイン名に「関連した」標準化の動向(IETF)をお届けします。**
  - Extended DNS errors
  - iotops
  - danish

  BOFや議論方面です。

Extended DNS Errors

正確には一年よりちょっと前

Extended DNS Errors (RFC8914) (1/2)

- **DNSの応答における状態を示すコード**：NOERROR(エラーなし)・NXDOMAIN(名前が存在しない)・REFUSED(拒否された)・SERVFAIL(サーバ側の異常)等があった。
- これらを**拡張するとより詳しいエラーの内容、例えばDNSSECのエラーの内容を返すことができる。そのためSERVFAILだけでは失敗の理由が分からなかったものがより分かり易くなる。**

■時系列・議論されている所

2017年2月	2017年10月	2018年6月	2019年7月	2020年10月
• Warren Kumari氏(Google)ら4名のIndividual Draft投稿。当初は lame や TooBusy も。	• dnsop WGのDraftとして投稿。	• 再投稿。現在の形に近い形に。	• エラー内容が整理される(-07)。	• RFC8914

■拡張されたDNSエラーコード (RCODE)
- サポートされていないDNSKEYアルゴリズム
- サポートされていないDSダイジェストタイプ
- 古くて無効な応答内容
- **改ざんされた応答内容**
- **DNSSECの検証結果は「偽」**
- DNSSECの検証結果は「不確定」
- **署名の期限切れ/まだ有効でない**
- 署名鍵が見つからない
- 署名のレコードが見つからない
- NSECが見つからない
- フィルタリングされた
- **ネットワークエラー**　など

■Extended DNS Errorsを使うにあたって考えるべきこと
- 拡張を含めるためにはEDNS0を扱うことができる必要
- エラーそのものを認証することはできない
- 受け取ったクライアントはどうすれば？

三つの立場

Extended DNS Errors (2/2) - IETF勉強会＆座談会より

安心して
使いたい立場

DNSSEC検証する
リカーシブリゾルバー

権威サーバ

エンドユーザ

- 「つながらない」
  その時どうする？(どう案内されてると良い？)

- アプリケーションはどうするか。
  - DoHをDNS,DNSSEC(DMARC)の検証のために使うのがいいのではないか。DANE、SPFの検証も。
  - ユースケース、Webアプリケーションで使えるようにする。

**ネットワーク
サービス提供の立場**

- そもそも検証開始をどう判断する？

- DoHサーバ
  - アプリケーションに署名状況やエラーが分かるようにする。draft-addy-dnsop-error-page
    ↓
    draft-reddy-dnsop-error-page

**オンラインの
サービス提供の立場**

- そもそも署名開始をどう判断する？
- エラーが伝えられるなら変化も？

- 積極的に提供しずらい。
- メリットが理論的には分かるがサービス提供上よりも、何かあったらいやだなという気持ち

iotops

IOT Operations(iotops) WG (1/2)

- **IoTデバイスの利用開始とライフサイクル管理に関する議論を行うWG**
  - Internetか管理ドメインの中でネットワークに接続
  - UIが限定されている、もしくはエンドユーザ向けにはない。
  - 数が多くて手動で設定できない。
- **これまで**
  - 2020年10月ML開始、2021年2月趣意書AD承認
  - IETFミーティング x 3、Interim x 1
- **関連WG**
  - ACE, ANIMA, CBOR, CORE, DRIP, LAKE, LPWAN, LWIG, ROLL, SUIT, TEEP, 6LO, 6TISCH

IOT Operations(iotops) WG (2/2)

- **議論されているI-D**
  - draft-irtf-t2trg-secure-bootstrapping-01
    初期セットアップのプロセスと用語
  - draft-moran-iot-nets-00
    関連セキュリティ技術のサマリ
  - draft-nordmark-iotops-onboarding-00
    “エッジコンピューティング”との対比
  - draft-richardson-iotops-iot-iot-01
    所有者に関する概念の整理
  - draft-richardson-t2trg-idevid-considerations-05
    工場出荷時のトラストアンカーの種類と鍵生成

直接的なリソースレコードの定義には至っていないが、DNSにおける名前とIPアドレスの利用が前提となっている。InterimではNISTによる「IoTデバイス」の分類も。

danish

danish（DANE AutheNtication for Iot Service Hardening）(1/2)

- **名称**
  - DANE Authentication for Network Clients Everywhere (DANCE) WG になる模様。
- **DANEを使った認証の議論**
  - DNSSEC前提
  - IoTデバイスのためのTLSサーバ/クラインと認証
  - SMTPクライアントとしても認証
- **これまで**
  - 2021年1月議論開始、趣意書を議論中
  - IETFミーティング x 2

danish (2/2)

- **議論されているI-D**
  - draft-huque-dane-client-cert-07
    DANE TLSAレコードを使ったクライアント認証
  - draft-huque-tls-dane-clientid-05
    DANEのクライアント識別子のためのTLS拡張
  - RFC 9102 (draft-dukhovni-tls-dnssec-chain)
    TLSにおけるDNSSECチェーンに関する拡張。TLS WGより。

DNSSECの利用を前提とし、TLSAを使ってTLSの相互認証を行おうとしている。前提として、センサーデバイス等、IPでつながるデバイスの名前空間がばらばらになり従ってPKIドメインとしても様々なものができてしまうことによる混乱を避けるため、という意図がある。(IETF111 BOF)

おわり