DNSの弱点を振り返り、今後の針路について考える

～ランチのおともにDNS～

2022年11月29日

Internet Week 2022 ランチタイムセミナー

株式会社日本レジストリサービス（JPRS）

森下 泰宏・月東 健人

3年ぶりの現地開催！

- 今年のInternet Weekは、**オンラインWeekとハイブリッドWeekの2本立て**で開催されています
- 今年のランチタイムセミナーはハイブリッドWeekのプログラムの一つとして、**3年ぶりの現地開催**となりました！
  - 現地でご参加のみなさまには、**ランチ**をお出ししております！

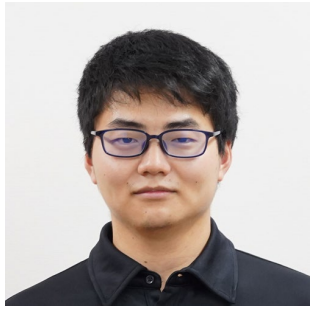
現地でご参加のみなさまへ

- 内容が面白くても、**声を出して笑わないでください！**
  - マスクを外している状態ですので、発声には特にご注意ください
  - 内容がつまらなくて、ブーイングしたくなった場合も同様です

講師自己紹介

- 森下 泰宏（もりした やすひろ）
  - 所属：JPRS 技術広報担当・技術研修センター
  - 主な業務内容：技術広報活動全般・社内外の人材育成
  - 一言：**4年ぶりに壇上に立ててうれしいです！**

- 月東 健人（がっとう けんと）
  - 所属：JPRS システム部
  - 主な業務内容： BGPのメンテナンス・JP DNSの運用
  - 一言：**お昼ご飯をパワーに変えて頑張ります！**



本日の内容

1. 今回取り上げるDNSの弱点（話者：月東）
2. メッセージ圧縮機能の概要とその状況（話者：森下）
3. 状況を踏まえた対応と今後の針路（話者：森下）

1. 今回取り上げるDNSの弱点

弱点とは？

①不十分なところ。欠点。短所。「守備の―」

②よわみ。うしろぐらいところ。「―につけ込む」
「―を握る」

出典：広辞苑 第七版

弱みとして付け込まれやすい
不十分なところ・欠点・短所

今回取り上げるDNSの弱点

- これを踏まえ、今回のランチタイムセミナーで取り上げるDNSの弱点を、以下のように定義する

DNSの実装・運用において弱みとして付け込まれやすい
設計上の不十分なところ・欠点・短所

DNSに関する脆弱性（2020年以降、主なもの）

- NXNSAttack：2020年5月
- SIGRed：2020年7月
- SAD DNS：2020年11月
- DNSpooq：2021年1月
- NAME:WRECK：2021年4月
- tsuNAME：2021年5月
- Phoenix Domain：2023年2月（予定）

近年、DNSの実装に関するさまざまな脆弱性が報告されている

脆弱性の原因

- NXNSAttack：**委任情報の取り扱いの不備**
- SIGRed：**メッセージ圧縮機能の実装の不具合**
- SAD DNS：サイドチャネル攻撃でポート番号を推測可能
- DNSpooq：内部処理・DNSSEC検証の実装の不具合
- NAME:WRECK：**メッセージ圧縮機能の実装の不具合**
- tsuNAME：**委任情報の取り扱いの不備**
- Phoenix Domain：**委任情報の取り扱いの不備**

「委任情報の取り扱いの不備」「メッセージ圧縮機能の実装の不具合」

委任情報の取り扱いとメッセージ圧縮機能

- **委任情報の取り扱い**と**メッセージ圧縮機能**はいずれも、**DNSの仕様（設計）における代表的な弱点**の一つ
  - **実装の不備・不具合、運用ミス**などが発生しやすく、さまざまな**トラブル・脆弱性の原因**になっている

委任情報の取り扱い

- 以下のトラブル・攻撃手法・脆弱性に関係している
  - DNS運用者の変更（DNSの引っ越し）におけるトラブル
  - 登録情報の不正書き換えによるドメイン名ハイジャック
  - Lame delegationを利用したドメイン名乗っ取り
  - カミンスキー型攻撃手法
  - 幽霊ドメイン名脆弱性
  - 第一フラグメント便乗攻撃
  - NXNSAttack
  - tsuNAME
  - Phoenix Domain

今回の題材は「メッセージ圧縮機能」

- 委任情報の取り扱いについては、過去のInternet Weekランチセミナーで取り上げている
  - DNS浸透の都市伝説を斬る（IW2011）
  - 親の心子知らず？委任にまつわる諸問題について考える（IW2012）
  - DNSのメッセージサイズについて考える（IW2013）
  - 未熟なDNSと今後どう付き合うべきか―委任／移転通知インジェクションとDNS水責め攻撃を題材として考える（IW2014）

今回のランチタイムセミナーではこれまで取り上げていなかった
メッセージ圧縮機能を、弱点を振り返る題材として取り上げる

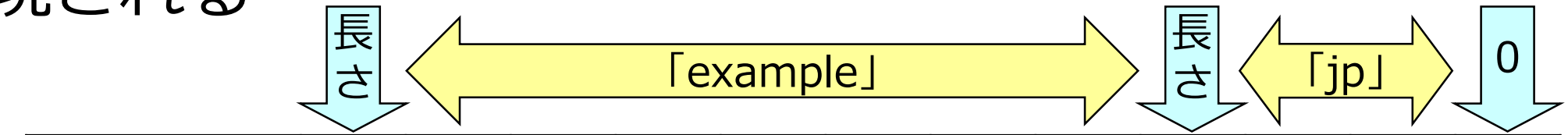
2. メッセージ圧縮機能の概要とその状況

メッセージ圧縮機能とは

- DNSの応答サイズを小さくして、**効率を上げる**機能
- DNSに**もともと備わっている**
  - RFC 1035で定義（4.1.4. Message compression）
- 送信側でメッセージを圧縮、受信側でメッセージを展開
  - フルリゾルバー⇔権威DNSサーバー間の場合、**権威DNSサーバーで圧縮**され、**フルリゾルバーで展開**される

おさらい：DNSメッセージにおける ドメイン名の表現形式

- DNSメッセージにおいて、ドメイン名は**<ラベルの長さ> <ラベル>…<ラベルの長さ> <ラベル> <0>**のように表現される



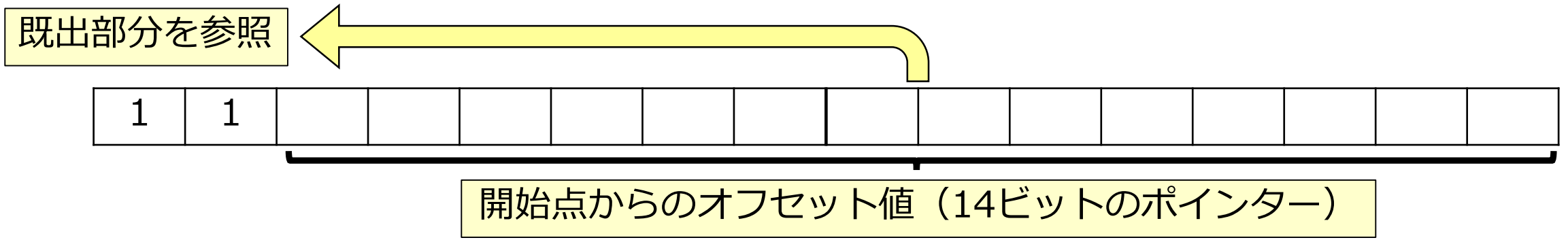
値（16進）	07	65	77	61	6D	70	6C	65	02	6A	70	00
文字	(7)	e	x	a	m	p	l	e	(2)	j	p	(0)

ドメイン名「example.jp」のDNSメッセージにおける表現

- ラベルの長さは63文字までなので、**6ビット**で表せる
  - 上位2ビット分空いている（長さの上位2ビットは常に00）

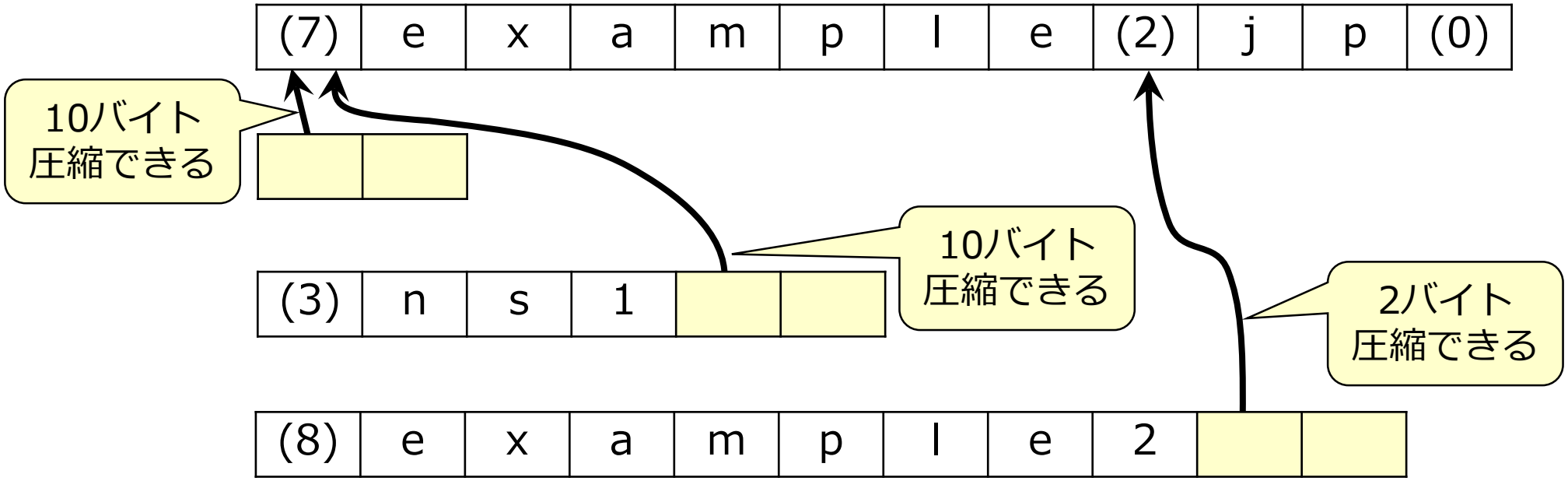
メッセージ圧縮機能：実現方法

- この空きを利用し、ドメイン名の**既出部分**を**初出部分へのポインターで指し示す**ことで、メッセージを圧縮・展開する
  - 上位2ビットを「11」とし、**残りの6ビットと次の1バイト**にDNSメッセージの**開始点からのオフセット値**を設定する
    - 「01」と「10」は、将来の利用のために予約されている



メッセージ圧縮機能：具体例

- 「example.jp」が既出であった場合、
  - 「example.jp」は「＜既出＞」
  - 「ns1.example.jp」は「ns1.＜既出＞」
  - 「example2.jp」は「example2.＜既出＞」のように表せる



メッセージ圧縮機能：ユースケース

- ネームサーバーホスト名を「**そろえる**」理由の一つ
  - ルートサーバーの**root-servers.net**やJP DNSの**dns.jp**など
  - ホスト名をそろえることで、応答サイズを小さくできる

- **同じドメイン名を数多く含む**応答ほど、圧縮効率が高くなる
  - そうでない応答の圧縮効率は、**それほど高くならない**

まとめ：メッセージ圧縮機能の概要

- DNSの**応答サイズを小さくして、効率を上げる**機能
- DNSに**もともと備わっている**
- **ポインター参照**を使い、**ドメイン名を圧縮・展開**する
- **同じドメイン名を数多く含む応答**ほど、圧縮効率が高くなる
  - そうでない応答の圧縮効率は、**それほど高くならない**
- ネームサーバーホスト名を**そろえる理由**の一つ

メッセージ圧縮機能に対する指摘

- メッセージ圧縮機能は**実装に手間が掛かり**、実装の不備が**さまざまな脆弱性の原因になっている**ことが指摘されている
  - **生成・解析に手間が掛かり**、かつ**効率も低い**[*1]
  - **20年にわたり**、サーバー・デバイス・TCP/IPプロトコルスタックなど、**さまざまな製品の脆弱性の原因**となっている[*2]

[*1] Notes on the Domain Name System <https://cr.yp.to/djbdns/notes.html>

[*2] NAME:WRECK - Breaking and fixing DNS implementations <https://www.forescout.com/resources/namewreck-breaking-and-fixing-dns-implementations/>

RFC 9267

- 2022年7月に発行された、**DNSのレコード処理に関する**
  アンチパターンを記述した、Informational RFC
  - アンチパターン：処理・動作・構造などにおける、不適切な例
- 2021年4月にNAME:WRECK脆弱性[*1]を公開した研究者が、分析で得られた結果をまとめたもの
  - **メッセージ圧縮機能**や応答の長さの確認などの処理において見受けられる、**複数のアンチパターン**が紹介されている

[*1] NAME:WRECK - Forescout <https://www.forescout.com/research-labs/namewreck/>

紹介されているアンチパターン（抜粋）

① ポインターがDNSメッセージの外部を指している
② ポインターが自身を指している
③ ポインターがループしている
④ ポインターの展開結果が上限（255）を超えている
⑤ ポインターがネストしている（参照先でポインターが再び現れる）

展開処理の際にはこれらのアンチパターンのチェックを含む、**細心の注意**が必要

新たに標準化されるレコードのデータ部分の圧縮・展開は禁止

- 実装の複雑さや相互運用性の観点から、**DNSで新たに標準化されるレコードのデータ部分の圧縮・展開は禁止**されている
  - RFC 1123（1989年10月発行）で言及され、
    RFC 3597（2003年9月発行）で明示的に禁止された
- そのため、データ部分が圧縮・展開の対象になるレコードは現在は**CNAME・MX・NS・PTR・SOA**のみ
  - RFC 1035で定義され、データにドメイン名を含むもの

```
jprs.jp. 86400 IN NS ns1.jprs.jp.
```

データ部分の圧縮・展開対象はCNAME・MX・NS・PTR・SOAのみ

DNS以外のプロトコルへの影響

- メッセージ圧縮機能は**DNS以外のプロトコル**でも使われており、脆弱性の原因となっている
  - NAME:WRECK脆弱性のレポート[*1]に、以下の記述がある

> This type of encoding is used not only in DNS resolvers but also in multicast DNS (mDNS), **DHCP clients as specified in RFC 3397** (“Dynamic Host Configuration Protocol (DHCP) Domain Search Option”) and **IPv6 router advertisements as specified in RFC 8106** (“IPv6 Router Advertisement Options for DNS Configuration”).

DHCPやIPv6 RAでも使われている？

[*1] NAME:WRECK - Breaking and fixing DNS implementations <https://www.forescout.com/resources/namewreck-breaking-and-fixing-dns-implementations/>

RFC 3397（DHCPのDomain Search）

- DHCPのDomain Searchオプションに、メッセージ圧縮が使われている

> To enable the searchlist to be encoded compactly, searchstrings in the searchlist MUST be concatenated and **encoded using the technique described in section 4.1.4 of "Domain Names - Implementation And Specification" [RFC1035].**

4.1.4. Message compression

- FreeBSDのdhclientはこの部分の実装に不備があり、NAME:WRECK脆弱性の原因となった（CVE-2020-7461）

RFC 8106（IPv6 RAのDNS Configration）・RFC 8415（DHCPv6）

- IPv6 RAのDNS Configurationオプションではエンコーディングをシンプルにするため、メッセージ圧縮は**禁止されている**

> Note that for the simple decoding, **the domain names MUST NOT be encoded in the compressed form described in Section 4.1.4 of [RFC1035].**

- DHCPv6も確認したところ、こちらも**禁止されている**

> A domain name, or list of domain names, in DHCP **MUST NOT be stored in compressed form as described in Section 4.1.4 of [RFC1035].**

ただし、禁止されているのは「**圧縮されたメッセージを送り付けること**」で、**圧縮されたメッセージを受け取った場合の動作**は記述されていない

プロトコルで禁止されている応答の取り扱い

- プロトコルでメッセージ圧縮が禁止されていても、送り付けられた**圧縮済みメッセージを受け入れて展開してしまう実装**が存在し、**脆弱性の原因**となっている
  - NAME:WRECK脆弱性のレポートより：
    - 公式にメッセージ圧縮・展開がサポートされていない場合も、**コードの再利用**や**仕様の解釈**により、**多くの実装でサポートされ続けている**
  - SIGRed脆弱性のレポート[*1]より：
    - 脆弱性の原因であるSIGレコード（DNSSEC旧仕様）のメッセージ展開処理と**同じ関数**が、**RRSIGレコード（現仕様）の処理にも使われている**

[*1] SIGRed - Resolving Your Way into Domain Admin: Exploiting a 17 Year-old Bug in Windows DNS Servers <https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/>

まとめ：メッセージ圧縮機能の状況

- **実装に手間が掛かり**、**不具合や脆弱性の原因**になりやすい
  - メッセージの展開処理において、**細心の注意**が必要になる
  - 実装の複雑さや相互運用性の観点から、**DNSで新たに標準化される**
    レコードのデータ部分の圧縮・展開は禁止されている
- プロトコルで禁止されても、受け取った圧縮済みメッセージを**受け入れて展開してしまう実装**が存在し、脆弱性の原因となる場合がある
- **DNS以外のプロトコル**で使われ、脆弱性の原因となる場合がある

3. 状況を踏まえた対応と今後の針路

振り返り：メッセージ圧縮機能が弱点になってしまった原因

① 悪意の存在を想定していなかった

- 悪意を持つ応答への対応が不十分であった
  - 作られた時期を考えれば、やむを得ないとも言える

② 不正な入力に柔軟に対応し過ぎる実装が存在する

- 未定義・プロトコル違反の応答を受け入れてしまう実装が存在する
  - ネストされているポインター、禁止されている圧縮済みメッセージなど

③ 使われる範囲が広い

- DNS以外のプロトコルで使われている場合がある

弱点を踏まえた対応

- 再掲：前ページで指摘した三つの項目
  - **① 悪意の存在を想定していなかった**
  - **② 不正な入力に柔軟に対応し過ぎる実装が存在する**
  - **③ 使われる範囲が広い**
- このパートではこれらの項目に対応するために、IAB[*1]とIESG[*2]で進められている、IETFの二つの活動を紹介する
  - **edmプログラム**
  - **DNS Directorate**

[*1] IAB：IETFの活動方針と標準化プロセスを監督するグループ。
[*2] IESG：IETFの活動と標準化プロセスの技術的な責任を担うグループ。

edmプログラム

- IABが2020年8月に開始したプログラム
  - 「Evolvability, Deployability, & Maintainability」に由来
  - IETFが標準化するプロトコルの進化・普及・保守の戦略を策定・分析する文書の作成が目的
- 現在、インターネットにおいて長年重要視されてきた、**ポステルの法則を見直す文書**の作成を進めている
  - draft-iab-protocol-maintenance

[*1] Evolvability, Deployability, & Maintainability (edm)
<https://datatracker.ietf.org/program/edm/about/>

ポステルの法則とは？

- **ロバストネス原則**（The robustness principle）
  - 「送信では厳密に・受信では寛容に」
    - “be conservative in what you send, and liberal in what you accept”
- インターネットにおける**プロトコルの設計指針**として、長年にわたり重要視されてきた
  - RFC 761（TCPの初期仕様、1980年1月発行）

> TCP implementations should follow a general principle of robustness: **be conservative in what you do, be liberal in what you accept** from others.

draft-iab-protocol-maintenance

- 2015年3月に、MozillaのMartin Thomson氏が初版を公開[*1]
- 2018年11月から、IABのインターネットドラフトに[*2]
  - 2022年10月時点の最新版：draft-iab-protocol-maintenance-09
- ロバストネス原則の**過剰な適用を見直し、より健全なエコシステムを作ること**が目的
  - ロバストネス原則を**否定するものではない**

[*1] The Harmful Consequences of Postel's Maxim
<https://datatracker.ietf.org/doc/draft-thomson-postel-was-wrong/00/>

[*2] Maintaining Robust Protocols
<https://datatracker.ietf.org/doc/draft-iab-protocol-maintenance/>

指摘されている内容

- ロバストネス原則に、**ソフトウェアの欠陥・サイバー攻撃・予期しない入力に対する耐性**が含まれることを明記
- その上で**「受信では寛容に」の過剰な適用**を問題視

> However, an interpretation that **advocates for tolerating unexpected inputs** is no longer considered best practice in all scenarios.
>
> （参考訳）しかし、**予期しない入力の許容を擁護する**解釈は、もはやすべてのシナリオにおいてベストプラクティスであるとは言えない。

ロバストネス原則の範囲を明確化して**悪意の存在を想定**し、予期しない入力に対し**「受信では寛容に」を過剰に適用することを問題視**

前述した三つの項目の**①と②に対応**

DNS Directorate

- 2022年7月に開催されたIETF 114で設立が提案され、活動を開始[*1]
- IETFには各分野の専門家の立場から提案をレビューする、Directorateという仕組みがあり[*2]、**DNS Directorate**はその一つとして設立

[*1] DNS Directorate (dnsdir)
<https://datatracker.ietf.org/group/dnsdir/about/>

[*2] IETF | IETF Directorates
<https://www.ietf.org/about/groups/directorates/>

設立目的と活動内容

- DNS関連以外のWGの提案にもDNS関連の内容が含まれる場合があるため、それらの内容を**早い段階でレビューすることで、標準化活動をより円滑にする**ことが目的

前述した三つの項目の**③に対応**

- DNSの専門家の立場で、IETFで作成される提案をレビュー
  - WGチェア・エリアディレクターがレビューを依頼
  - レビューを通じ、提案者・WGチェア・エリアディレクターを支援

edmプログラム・DNS Directorateの位置づけ

- いずれも重要な活動であり、その成否は**DNS・インターネットの今後**につながっている
  - そして、**Internet Week 2022全体のテーマ**ともつながっている

> **今年のテーマに込めた想い**
>
> 今年のテーマは、「インターネットの羅針盤～針路を未来に」です。まさに先ほど述べたような、Internet Weekがインターネットに関わる方々の羅針盤でありたい、という想いを込めました。ますます巧妙化するサイバー攻撃、**「インターネットの精神」を改めて見つめ直し**、考えさせられる社会問題など、私たちが考え、議論すべきことは多くあります。このような航海に**細心の注意を払うべき局面で、どちらの方に進むべきかを指し示す**、あるいはどちらの方に進むべきか、議論できる場にしたいと考えています。

⇒ edmプログラムは**前者**、DNS Directorateは**後者**に対応

おわりに：DNS・インターネットの、そしてわれわれの針路は（1/2）

- いずれも今後の針路を定めるべき、**大事な局面**を迎えている
  - 今回ご紹介したedmプログラムやDNS Directorateをはじめ、.ru/.suの取り消し要請や権利侵害を理由としたDNSブロッキング要請にまつわる動向など、**今後の針路を左右する大きな動き**が相次いでいる

IWショーケース徳島の発表資料（前村昌紀氏）

2022年11月10日のGIGAZINEの記事
引用元：<https://gigazine.net/news/20221110-public-dns-1111-blocking-order/>

おわりに：DNS・インターネットの、そしてわれわれの針路は（2/2）

- DNSはインターネットを支える基盤技術であり、その針路は**インターネットのみに留まらず、それを取り巻くさまざまなもの**にも影響する

そのため、DNSの針路はDNSだけでは決まらないし、決められない

- DNSの運用者はDNS以外の技術・ポリシー・社会情勢などについても**幅広く理解し、適切に判断する**ことが必要になる

激動する状況の中、周囲の動向や変化にも気を配りつつ、
よりよい針路を見出せるように力をつけ、みんなで頑張っていきましょう

おまけ

BIND 9.19.7

- BIND 9.19の最新版として、**2022年11月16日**にリリース
  - BIND 9.19は**開発版ブランチ**であり、**次の安定版であるBIND 9.20に組み込まれる機能が開発・追加**されている
- リリースノートに、**こんなことが書かれている**

> The DNS name compression algorithm used in BIND 9 has been revised: it now compresses more thoroughly than before, so responses containing names with many labels might have a smaller encoding than before. [GL #3661]
>
> （参考訳）BIND 9で使われる**DNS名前圧縮アルゴリズムが改訂された**：**以前よりもまんべんなく圧縮されるようになった**ので、 **多くのラベルを持つ名前を含む応答は以前よりも小さなエンコーディングになるかもしれない**。[GL #3661]

[*1] Release Notes — BIND 9 9.19.7 documentation
<https://downloads.isc.org/isc/bind9/9.19.7/doc/arm/html/notes.html#feature-changes>

大丈夫でしょうか・・・

関係者の皆様・腕に覚えのあるみなさまへ

- 9.19のうちに、**まんべんないバグ出し**をお願いします！
- 寝る時に、**枕を少しだけ高くできます！**
  - なお今回の改訂対象は圧縮部分で、**展開部分は改訂されていない模様**です

最後までご清聴・ご視聴いただき ありがとうございました！

<https://jprs.jp/tech/>

@JPRS_official　JPRSofficial　JPRSpress