わたしたちの DNSViz

アカマイ・テクノロジーズ合同会社
シニア・ソリューションズ・エンジニア
松本 陽一

このプレゼンテーションにおいてなされる記述は作成者個人の見解を示すものであり、アカマイ・テクノロジーズの見解を示すものではありません。提供される情報は作成時点において正確なものであると考えておりますが、当該情報についてなんら表明又は保証を行いません。

あれ？そのとき

地震！　→ 各種地震情報サイト

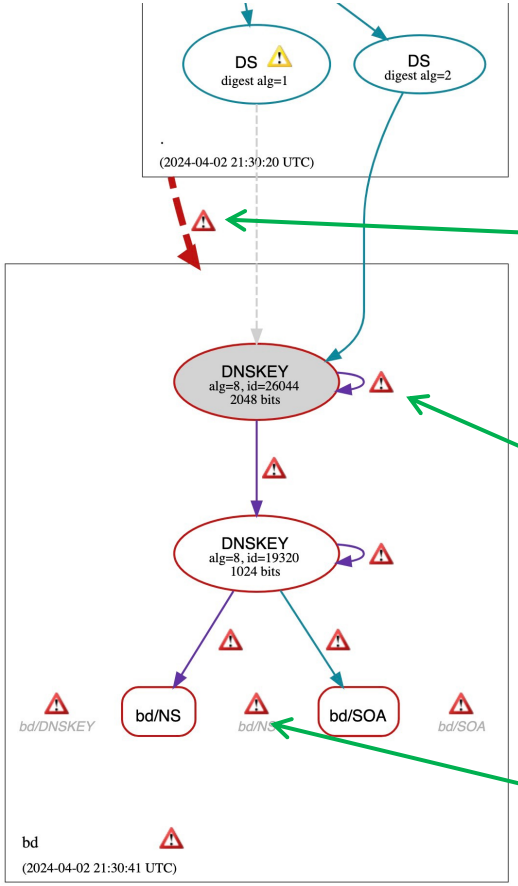
ある名前が引けない！　→ DNSViz

多くの情報が図や表でわかりやすく視覚化されている
過去のデータも公開

例: bd. (バングラディシュの ccTLD)

2024-04-02 21:30:41 UTC

https://dnsviz.net/d/bd/Zgx5AQ/dnssec/



マウスオーバーによりエラーの詳細をツールチップで表示

Description: Delegation from . to bd.
Status: BOGUS
Errors: No valid RRSIGs made by a key corresponding to a DS RR were found covering the DNSKEY RRset, resulting in no secure entry point (SEP) into the zone. (204.[redacted], 2001:[redacted], UDP_-_EDNS0_4096_D_KN)

委任の問題「DS に対応した DNSKEY に有効な RRSIG がない」

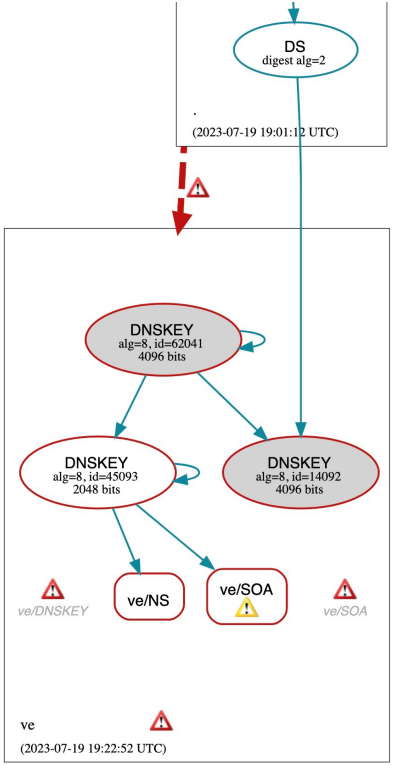
Id: bd./8/26044
Description: RRSIG covering bd/DNSKEY
Signer: bd.
Algorithm: 8 (RSA/SHA-256)
Key tag: 26044
Original TTL: 86400 (1 day)
Labels: 1 (no wildcard)
Inception: 2024-03-03 20:39:35 UTC (30 days in the past)
Expiration: 2024-04-02 21:22:07 UTC (8 minutes in the past)
TTL: 86400 (1 day)
Status: EXPIRED
Servers: 204.[redacted], 2001:[redacted]
NS names: bd-ns.anycast.pch.net.
NSID values: 1.sfo.pch
Query options: UDP_-_EDNS0_4096_D_KN
Errors: The Signature Expiration field of the RRSIG RR (2024-04-02 21:22:07+00:00) is 8 minutes in the past.

RRSIG の問題「署名が 8 分前に期限切れ」

Description: Response errors for bd/NS
Errors: The response had an invalid RCODE (SERVFAIL). (123.[redacted], 203.[redacted], 203.[redacted], 2407:[redacted], 2407:[redacted], 2407:[redacted], UDP_-_NOEDNS_)
Status: ERROR

レスポンスの問題「NS レコードを問い合わせるクエリーに対して一部の権威ネームサーバーが SERVFAIL を返している」

DNSSEC 運用上の事故の多様性 – 他の例

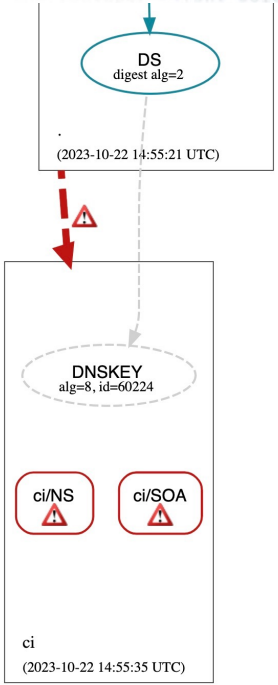


← ve. (ベネズエラの ccTLD)

2023-07-19 19:22:52 UTC

KSK ロールオーバーの失敗と見られる
新鍵に対応した DS をルートゾーンに登録していないのに旧鍵による署名をやめてしまった？

https://dnsviz.net/d/ve/ZLg4DA/dnssec/



ci. (コートジボワールの ccTLD) →

2023-10-22 14:55:35 UTC

DS がルートゾーンに登録されたまま公開鍵(DNSKEY)も署名(RRSIG)も消してしまった？
権威ネームサーバの IP アドレスは変わっておらず、シリアル(SOA)も自然に増えている

https://dnsviz.net/d/ci/ZTU35w/dnssec/

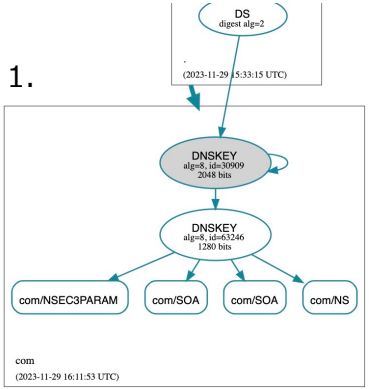
主要 gTLD のアルゴリズムロールオーバー

2023 年に順次 RSASHA256 (8) → ECDSAP256SHA256 (13)

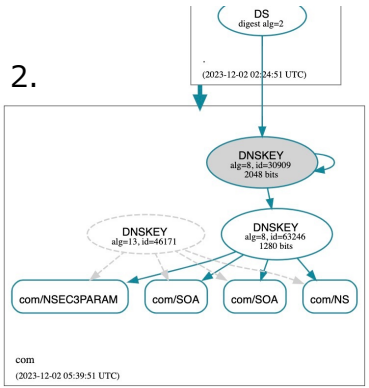
Zone	Start	Rollover	End
EDU	Sept 6	Sept 12-15	Sept 22
NET	Oct 25	Oct 31-Nov 3	Nov 10
COM	Nov 29	Dec 5-8	Dec 15

https://indico.dns-oarc.net/event/47/contributions/1012/attachments/973/1821/verisign-tld-updates.pdf

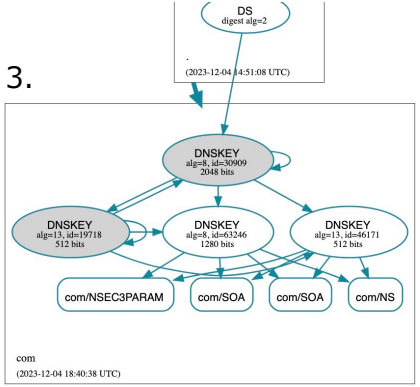
1.



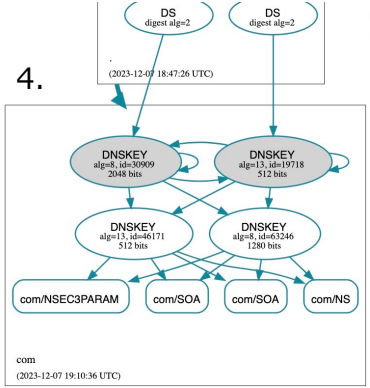
2.



3.

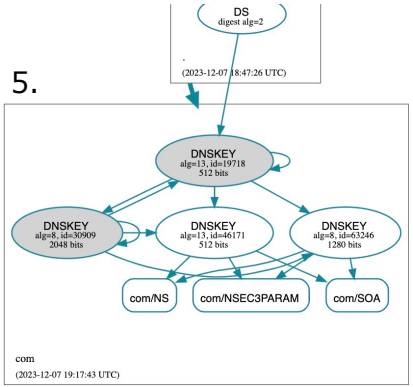


4.

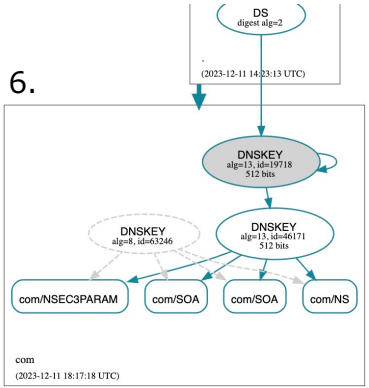


1. alg=8 のみ
2. alg=13 の ZSK による署名
3. alg=13 の ZSK/KSK の DNSKEY 登場
4. alg=13 KSK の DS 追加
5. alg=8 KSK の DS 削除
6. alg=8 の DNSKEY 削除
7. alg=8 の ZSK による署名削除

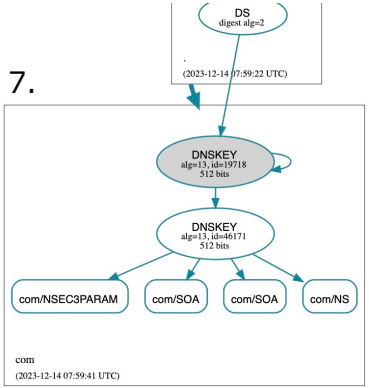
5.



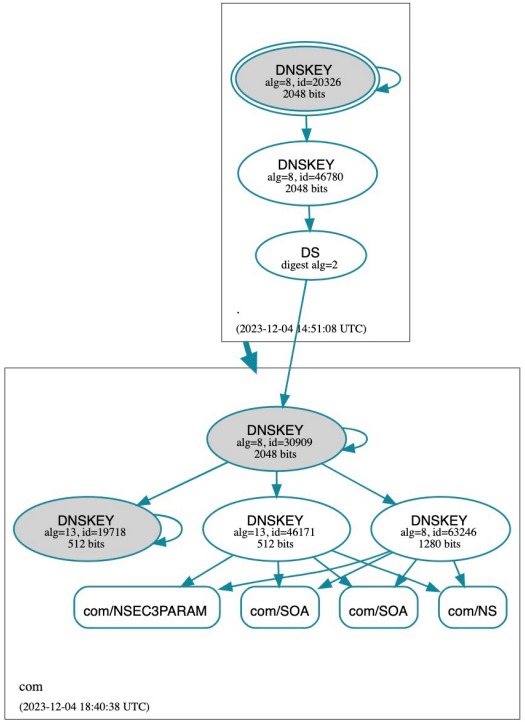
6.



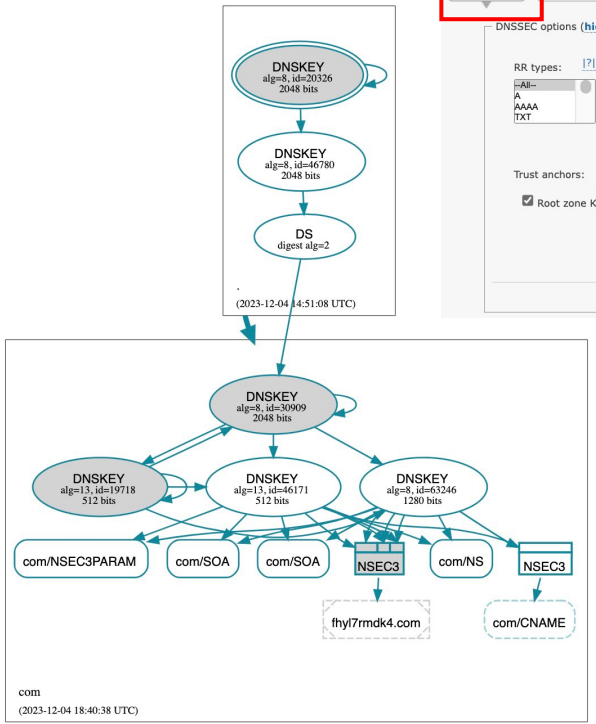
7.



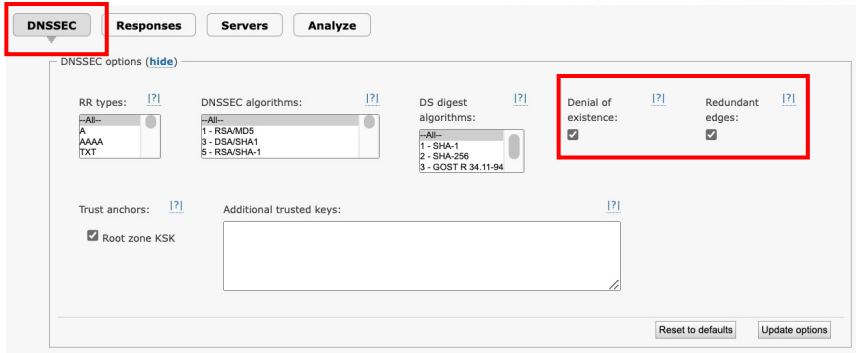
DNSSEC options (描画時のオプション)



デフォルト (いずれもオフ)



Deneial of exisitence と Redundant edges をチェック

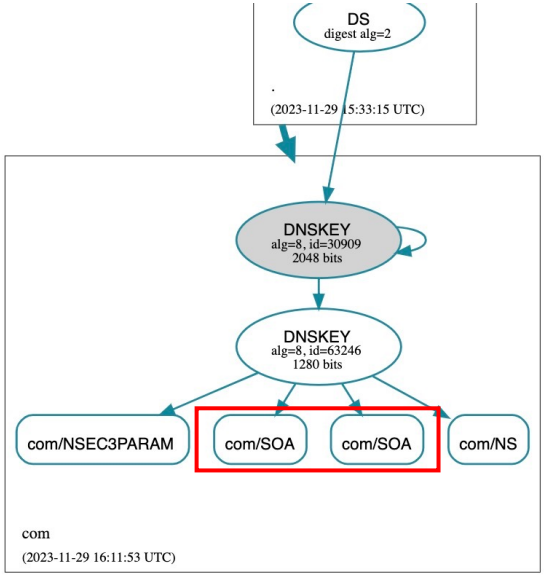


Denial of existence: 不存在の証明
(ランダムなサブドメインの情報も表示)
不存在証明に問題があると署名されていない
サブドメインが BOGUS となるので重要

Redundant Edges:
(デフォルトでは表示されない)本来不要な署名の情報も表示。全ページの図ではオン

描画のオプションであり、過去のデータでも描画時に適用可能

Responses
レスポンスの詳細を表示



com/SOA が二つあった

→ 複数の権威ネームサーバー間で
シリアル値の異なる SOA

DNSSEC | Responses | Servers | Analyze

DNS Server Responses

Responses for com/SOA

Name	TTL	Type	Data	Status	a.gtld-servers.net. (192.5.6.30)	a.gtld-servers.net. (2001:503:a83e::2:30)	b.gtld-servers.net. (192.33.14.30)	b.gtld-servers.net. (2001:503:231d::2:30)	c.gtld-servers.net. (192.26.92.30)	c.gtld-servers.net. (2001:503:83eb::30)	d.gtld-servers.net. (192.31.80.30)	d.gtld-servers.net. (2001:500:856e::30)
com	900	SOA	a.gtld-servers.net. nstld.verisign-grs.COM 1701274289 1800 900 604800 86400	OK	Y	Y			Y	Y	Y	Y
	900	RRSIG	SOA 8 1 900 20231206161129 20231129150129 63246 com. vD4FjRgrXQXlAJKzj9TgSPGlypqVrTOy	VALID	Y	Y			Y	Y	Y	Y
com	900	SOA	a.gtld-servers.net. nstld.verisign-grs.COM 1701274119 1800 900 604800 86400	OK			Y	Y				
	900	RRSIG	SOA 8 1 900 20231206160839 20231129145839 63246 com.	VALID			Y	Y				

Servers

DNSSEC | Responses | Servers | Analyze

DNS Server Status

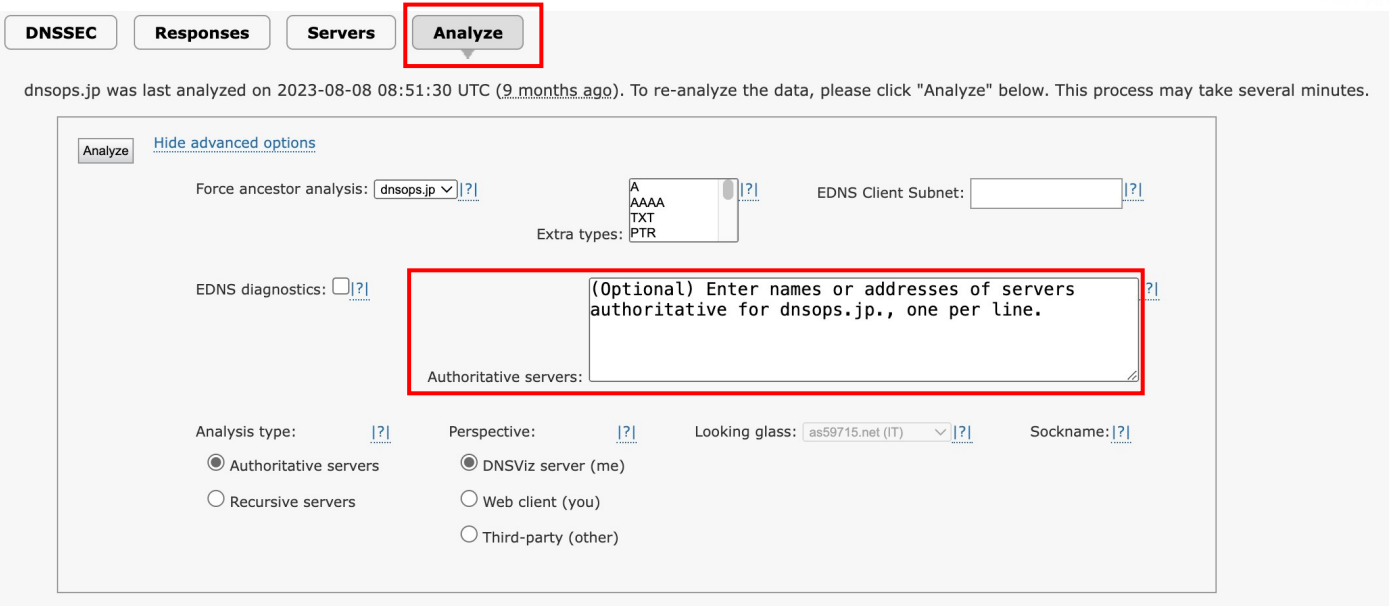
Delegation Information

Name	Parent zone			Child zone		
	Exists?	Glue/additional records		Exists?	Authoritative IPs	
ns1.dnsops.jp	yes	A	210.	yes	A	210.
		AAAA	2400:		AAAA	2400:
ns2.dnsops.jp	yes	A	160.	yes	A	160.
		AAAA	2001:		AAAA	2001:

- 委任 (リファーラル) の NS、Additional Section の A/AAAA (グルー)
- 権威ネームサーバーの応答する NS とその名前に対する A/AAAA

ずれがあった場合、図でも Warning が表示される

Analyze (新規の調査とそのオプション)



- Analyze -> Advansed Option の中では権威ネームサーバーの選択ができる。実際に上位ゾーンから委任の設定をしてもらう前に確認できる
- [Analyze] ボタンで調査開始

あらためて DNSViz

主に権威ネームサーバーに様々なクエリーを行い、分析してゾーンの状態を可視化するツール

- プロトコル上の正常性
- 委任の状態
- DNSSEC の鍵や署名

など

問題の発見や分析だけでなく、DNS や DNSSEC の勉強になる！

2 つの利用方法

- WEB サービス https://dnsviz.net/ - これまで見てきたもの。以下 dnsviz.net
- コマンドラインツール dnsviz - ここから説明 (https://github.com/dnsviz/dnsviz)

コマンド版 dnsviz を使う理由

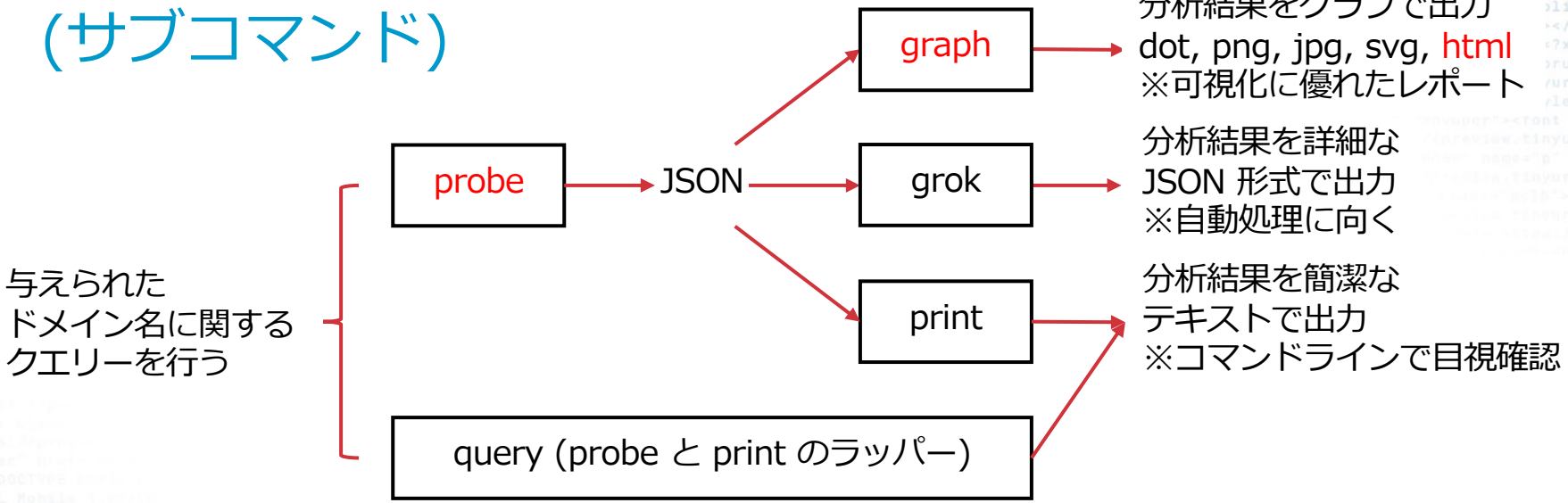
- dnsviz.net は原則として履歴が残り公開される
  恥ずかしい失敗が将来に渡って晒される
- dnsviz.net はしばしば調子が悪いことが…
  IPv6 の疎通が悪いことがあったり、一部の機能が使えなかったり
  過去のデータが飛んでしまったことも
- グラフだけでなく、JSON 形式でもアウトプットできる → チェックの自動化
- プライベート網内のサーバーの調査にも使える

など

コマンド版 dnsviz のインストール

- GitHub の README に丁寧に解説されている https://github.com/dnsviz/dnsviz
- dnsviz 自体は Python で書かれているが、多くのモジュールやライブラリに依存する。一部機能には BIND も必要。必要なものが欠けているとインストール時や実行時にエラー等
- どこまでどのパッケージシステムを使うか、VirtualEnv の使用、各パッケージのオプションなど多くの選択肢
- Docker コンテナも提供されている
- UNIX ライクな OS 向けに書かれており、Windows では何らかの仮想化技術を使う必要がある

dnsviz コマンドの使い方 (サブコマンド)



(dnsviz.net で表示されるような) HTML 形式のレポートを出力するには
"dnsviz prove" で 出力した JSON を入力として "dnsviz graph" を実行

HTML 形式の場合、ブラウザで表示すると dnsviz.net 同様にマウスオーバーしたときのツールチップ表示もされるので HTML 形式が最も有益

dnsviz コマンドの使い方 (例)

```
% dnsviz probe -A -a . example.com > example.com.json
Analyzing .
Analyzing com
Analyzing example.com
% dnsviz graph -T html -O < example.com.json
% ls
example.com.html        example.com.json
%
```

dnsviz probe

-A: リゾルバーではなく権威ネームサーバーにクエリー

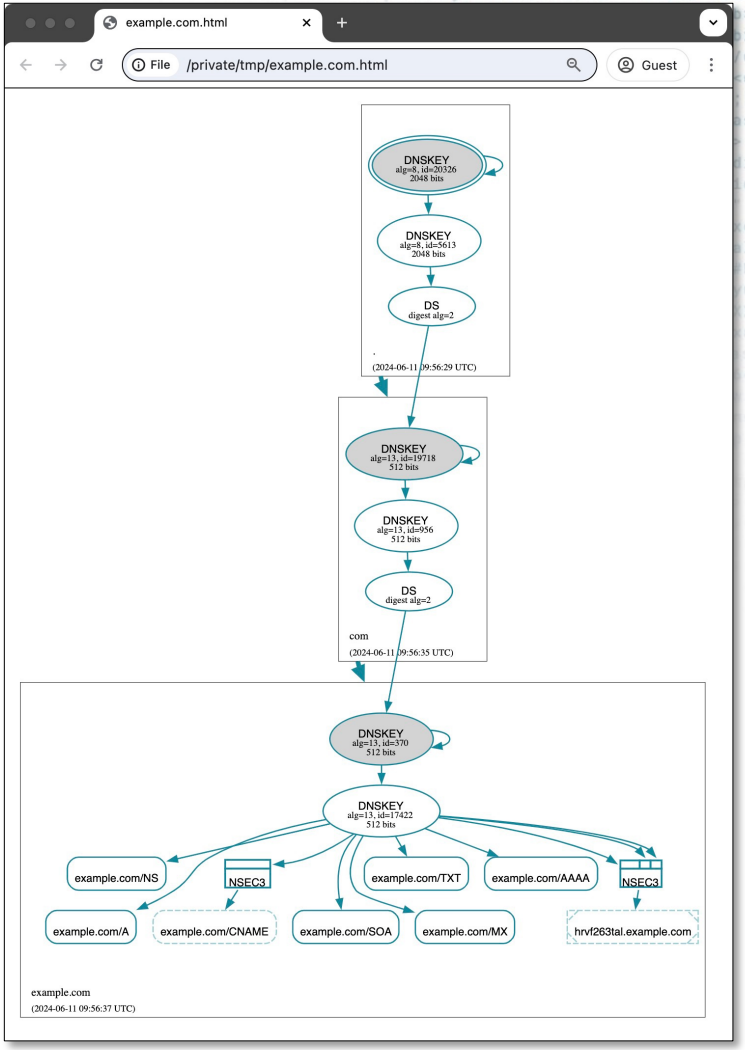
-a <ancestor>: 開始する上位ドメイン
ここではルート (.) を指定

dnsviz graph

-T: 出力フォーマット

-O: ドメイン名とタイプから出力ファイル名を決定

出力された HTML には図はインライン SVG として埋め込まれているが、「file:」型 URI で示された CSS と Javascript は必要



dnsviz コマンドをエイリアスにしておく

bash / zsh の例

```
% alias dviz='function _dviz(){ date=`date +%Y%m%d%H%M%S`;dnsviz probe -A -a . $1
|tee $1-$date.json|dnsviz graph -T html -o $1-$date.html;};_dviz'
% dviz example.com
Analyzing .
Analyzing com
Analyzing example.com
% ls
example.com-20240612151348.html   example.com-20240612151348.json
%
```

- 何回も実行し、履歴を確認したくなるので
  ファイル名に日付をいれて保存
- 中間の json 形式で保存しておくと将来別の形式で出力したり、
  バージョンが変わった時に便利

ちょっと抜き打ち調査

TOPIX 企業のドメイン名 2168 (DNSOPS.JP「統計」ページより) のうち 100 件を無作為抽出

Error があったもの: 5 ドメイン / Warning があったもの: 12 ドメイン

いずれかがあったもの: 15 ドメイン (両方あったものが 2)

Error の例

- ワイルドカードに設定されているとみられる CNAME の他社ドメインにおいて FQDN の上位ドメインが NXDOMAIN 応答 (RFC 8020 非準拠)
- 複数あるネームサーバーのうち 1 つが応答しない、UDP では応答があるが TCP では応答がない

Warning の例

- リファーラル / グルーと権威ネームサーバーの返す NS やそれに対応した A / AAAA が異なる (利用している権威 DNS サービスやレジストリ側の事情も？)
- 一部の応答に AA フラグが立っていない

DNSViz - まとめ

- DNSSEC 関連だけでなく権威ネームサーバのあらゆる問題や委任の問題も細かく調査して可視化してくれて、非常に有益
- コマンドラインでローカルで実行できる
    - インストールがちょっと面倒
    - コマンドラインがちょっと複雑

    → 苦労する価値はあるはず
- DNS / DNSSEC について勉強する際、人に説明する際にも便利


Akamai