DNSSEC実証実験に参加して

2023年5月19日

株式会社グローバルネットコア

佐藤 宏邦

GLOBAL NET CORE

https://www.global-netcore.jp/

自己紹介

佐藤 宏邦

所属会社：株式会社グローバルネットコア

所属部署：インフラサービス部サービス運用課

趣味：温泉旅行

最近のタスク：業務自動化

DNSSECとは

DNSSECは、DNS応答に添付された署名を受信側で検証することにより、正しい相手から届いた正しいデータであることを確認できるようにするための技術です。

現在少しづつ普及が進んでいます。

・全世界での普及率：約30％

・日本での普及率：約14％

DNSSECの仕組み

公開鍵暗号方式と電子署名の仕組みを応用し、DNSの権限移譲の構造に合わせた形で信頼の連鎖を構築することで実現

DNSSECの仕組み（電子署名）

(1)ゾーンの管理者が秘密鍵と公開鍵の鍵ペアを作成。

(2) 管理者がゾーン内のRRを秘密鍵で署名し、電子署名を作成。また、対応する公開鍵を公開し参照できるようにする。

(3) ゾーンに対して問い合わせがあった場合、権威サーバは電子署名付きの応答を返す。

(4)この電子署名付きの応答を公開鍵で復号できた場合には、その応答は確かに該当ゾーンの管理者が作成したもので、かつ改ざんもされていないと判断される。

DNSSECの仕組み（信頼の連鎖）

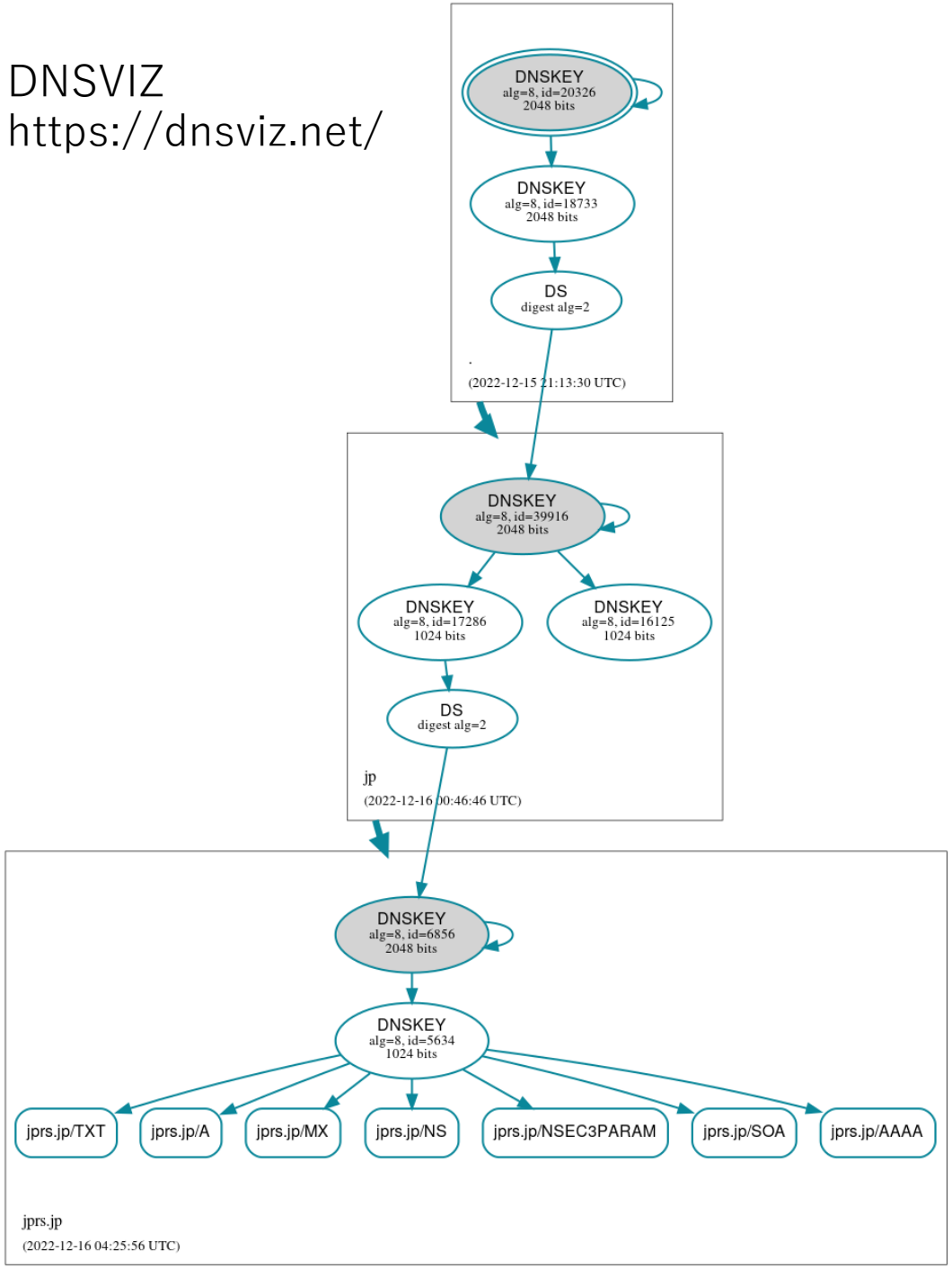
(1)ゾーンの管理者は、親ゾーンの管理者に公開鍵のハッシュ値(DS：Delegation Signer)を渡す。

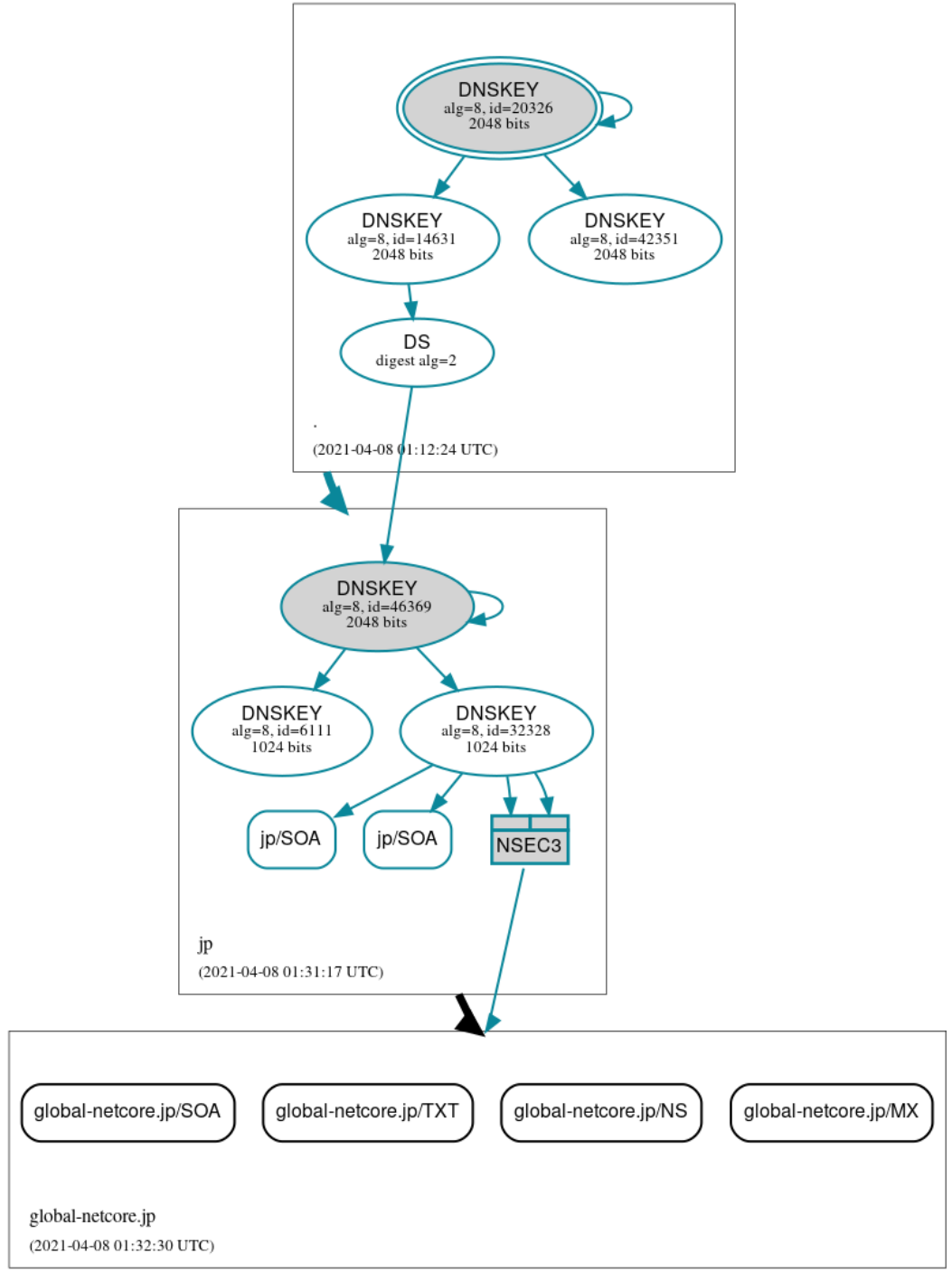
(2)親ゾーンの管理者は、渡されたDSが正しいことを確認し、親ゾーンの秘密鍵で署名をして公開。

(3)その親ゾーンも同様に、さらにその親のゾーンにDSを登録することで、信頼の連鎖(chain of trust)ができます。

これがDNSキャッシュサーバ管理者の信頼するゾーンまで行われれば、所定のゾーンに対して連鎖的に検証を行うことができるようになります

DNSVIZ
https://dnsviz.net/





DNSSECで利用されるRR

- DNSKEY：ゾーンを署名する秘密鍵に対応する公開鍵です。
- RRSIG：リソースレコードの電子署名です。
- DS：DNSKEYのハッシュ値です。
- NSEC：不存在との旨の回答に署名するためのリソースレコード
- NSEC3：NSECのように次のゾーン名を直接示すのでなく、そのゾーン名がわからないようにハッシュ関数で計算されたハッシュ値により、ゾーンを示します

DNSSECで利用される鍵

DNSSECでは署名に用いる鍵が2種類あります。

〇ゾーンに署名するゾーン署名鍵ZSK (Zone Signing Key)

〇ZSKに署名する鍵署名鍵KSK (Key SigningKey)

- ゾーン署名鍵ZSKは、各ゾーンに署名するものです。
- 鍵署名鍵KSKは、ゾーン署名鍵ZSKを署名するものです。
- 鍵署名鍵KSKについて公開鍵のハッシュ値を求め、その値をDSとします。
- 親ゾーンには、鍵署名鍵KSKのDSを登録することになります。

DNS実証実験

- 実験環境

用意された環境(BIND)で実際に設定を行い確認する

ドメインがジャックされた際の応答の変化を確認する

(実験環境は経路変更で疑似的にジャック状態にできる)

- 自社環境

自社の環境(PowerDNS)で設定の確認（ローカル環境）

BINDで行っていた設定がどういった設定に当たるか確認

実験環境での実証試験1

- 鍵ペアの作成はコマンド1行なので容易。但し、作成されたファイル名は自動命名でゾーン名＋ID.{key|private}となっているためzsk/kskそれぞれのIDを記録しておく必要がある

```
zsk
dnssec-keygen -a RSASHA256 -b 2048 -n ZONE {zone_name}
ksk
dnssec-keygen -f KSK -a RSASHA256 -b 4096 -n ZONE {zone_name}
```

- ゾーンへの公開鍵登録は出力されたファイル(～.key)をincludeするだけで済むので難しくはない。ID管理してないと間違いそう。

実験環境での実証試験2

- 秘密鍵による署名は、作業としてはコマンド1行。ただ、ゾーン編集時に都度署名が必要になるので手間ではある。尚、署名されたファイルが新規で作成されるので初回はconfファイルの修正が必要。

```
dnssec-signzone –k {ksk_file} {zone_file} {zsk_file}
```

- DSの作成は簡単なコマンド1行なので容易。

```
dnssec-dsfromkey {ksk_file} > {output_file}
```

- DSの登録をするまでは基本的には名前解決に影響はない。（内部的にはステータスは違うようですが。。。）

DNSSECによるセキュリティステータス

- Secure
  状況：親ゾーンにDSレコードがあり、RRsetの署名検証に成功
  応答：ADフラグありの応答
- Insecure
  状況：親ゾーンにDSレコードなし、RRsetに署名あり
  応答：ADフラグなしの応答
- Indeterminate
  状況：親ゾーンにDSレコードなし、RRsetに署名なし
  応答：ADフラグなしの応答
- Bogus
  状況：親ゾーンにDSレコードがあり、RRsetの署名検証に失敗
  応答：SERVFAILエラー応答

自社環境での実証試験1

- 鍵を登録するのは容易だが2種類の方法がある。一つはzsk/kskを統合したcsk形式で作成する方法で、アルゴリズムがECDSAP256SHA256に限られる。もう一つはBINDと同様にzsk/kskを利用する方法でこちらは複数のアルゴリズムを選択できる。WebUIのPowerAdminを利用した場合は前者の方法で鍵が作成される。

```
csk
pdnsutil secure-zone {zone_name} ; pdnsutil rectify-zone {zone_name}
zsk
pdnsutil add-zone-key {zone_name} zsk 1024 active rsasha512
ksk
pdnsutil add-zone-key {zone_name} ksk 2048 active rsasha512
```

自社環境での実証試験2

- 秘密鍵はDBの専用のテーブルに登録されるのが確認できたが公開鍵の保存場所が不明。DBの一般レコードのテーブルにも存在しないが問い合わせた際にデータは返ってくる。
- ゾーンへの登録は上記の通り自動で行われている。
- 署名は鍵作成時に自動で行われる。ゾーン編集時の署名都度署名する必要があるがPowerAdminを利用している場合は編集時のプログラムで自動的に署名されるため意識することはない。

```
pdnsutil rectify-zone {zone_name}
```

自社環境での実証試験3

- 署名の期限は実施日から直近過去の木曜日を基点とし、1週間前から2週間後まで。期限が残り1週間になると自動で更新が実施される（実質毎週更新）
- 鍵にはactive/inactiveのステータスがあるがDNSKEYレコードはステータスがどうであれ全て表示される。署名は全てのactiveな鍵によって実施される。
- DNSSEC登録時にsecure-zoneを実施したゾーンではadd-zone-keyで鍵タイプをどう選んでもcskタイプになる。

自社環境での実証試験4

- PowerDNSではDNSSEC関連の処理が自動で実施されるがSOAレコードが更新されない。PowerDNS同士では同期されるらしいが別ソフトを利用している場合はメタデータに個別の設定が必要。但し、その場合も毎週木曜日の更新のためそれまで同期されない。。。（鍵の新規追加とか）

DNSSECで障害が発生する状況

- 運用の中で障害になり得るのは以下の場合と推定される
  - DSの登録ミス（初回、ロールオーバー時）
    - 上位ドメイン管理者側のミス
    - 渡すレコードの間違い
  - 署名時の鍵間違い
  - 署名の期限切れ

DNSSECで障害が発生した場合の対応

DSの登録ミス

上位ドメイン管理者側のミス

→　上位ドメイン管理者に対応を依頼

渡すレコードの間違い

→　正しいレコードで修正依頼

署名時の鍵間違い　→　再署名

署名の期限切れ　→　再署名

DNSSECでの障害検知

・DSの登録ミス

　常時監視が必要

・署名時の鍵間違い

　設定時の確認で気づける

・署名の期限切れ

　常時監視が必要

監視方法：自作のスクリプトしかない？

DNSSECで障害が発生した例

2010年：arpa　署名有効期限切れ

2010年：.be　署名有効期限切れ

2011年：.uk　予備系の鍵同期漏れ

2011年：mozilla.org　勇み足でDS登録

2011年：.fr　bindバグ

2011年：.kg　サーバーの内部時計がローカルで署名が未来だった

2021年：slack.com　DSのキャッシュがあるうちに署名解除

DNSSECのメリット・デメリットを考える

・メリット

データの正当性を確保できる

・デメリット

第三者による設定が必要となる

想定外の通信断の発生

DNS関連作業における作業負荷の増加

まとめ

・設定自体はさほど面倒ではない。
　但し細かい作業は増える。
・有効期限の管理や鍵の管理は面倒かも？
　→この辺は自動化できると楽でよい
・メリットよりデメリット(リスク)のほうが大きそう
　→金融機関のような厳格な運用が求められるところならありかも