株式会社ミライコミュニケーションネットワーク

権威DNSサービス調査

～複数のDNSプロバイダでDNSSEC対応してみた～

2023年6月23日

ミライコミュニケーションネットワーク

田中温子

自己紹介

- 名前　田中温子
- 所属　株式会社ミライコミュニケーションネットワーク
  技術部運用チーム所属
- お知らせ
  - ChuNOG2を8/3に長野県松本市で開催します
  - connpassで参加受付中
- 最近の悩み事
  - ペットを飼いたいが家族に反対されている

今日の内容

- これまでにDNSControlを使ってみて、異なるDNSプロバイダ間のゾーンの移行や、管理に十分使えるツールだと感じた
  →DNSSEC署名ありの場合にも使えるのか
  →そもそも複数のDNSプロバイダでDNSSEC対応をやったことがない

DNSControlとは

- なにができる？
  - 複数のDNSプロバイダに対してゾーン情報の更新
  - 対応するDNSプロバイダのゾーンをDNSControlの形式に変換
  - 変数やマクロが書ける
- Stack Exchange社が開発したOSS
- BIND、Route53など35以上の
  DNSプロバイダに対応

dnsconfig.js

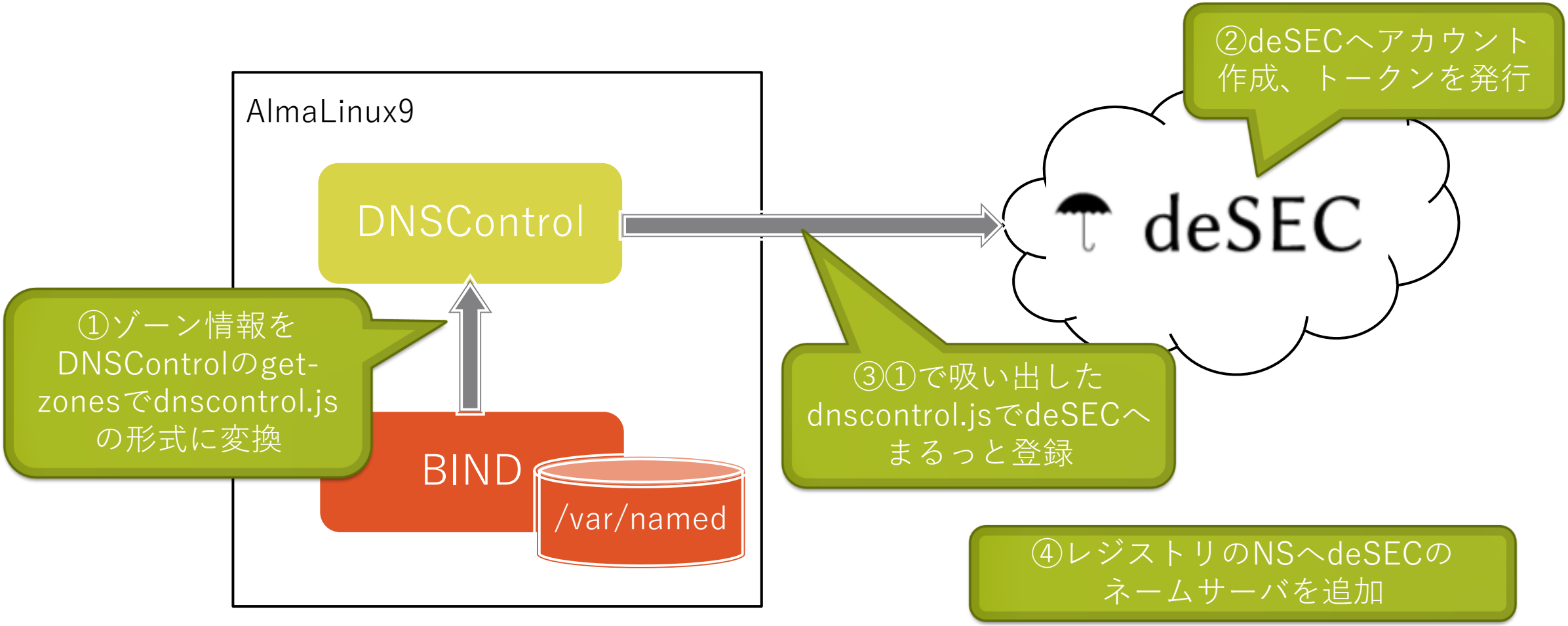
```
D('example.com', REG, DnsProvider('GCLOUD'),
    A('@', '1.2.3.4'),  // The naked or 'apex' domain.
    A('server1', '2.3.4.5'),
    AAAA('wide', '2001:0db8:85a3:0000:0000:8a2e:0370:7334'),
    CNAME('www', 'server1'),
    CNAME('another', 'service.mycloud.com.'),
    MX('mail', 10, 'mailserver'),
    MX('mail', 20, 'mailqueue'),
```

dnsconfig.js

```
var addrA = IP('1.2.3.4')

D('example.com', REG, DnsProvider('R53'),
    A('@', addrA), // 1.2.3.4
    A('www', addrA + 1), // 1.2.3.5
)
```

DNSControlでこれまでに試したこと

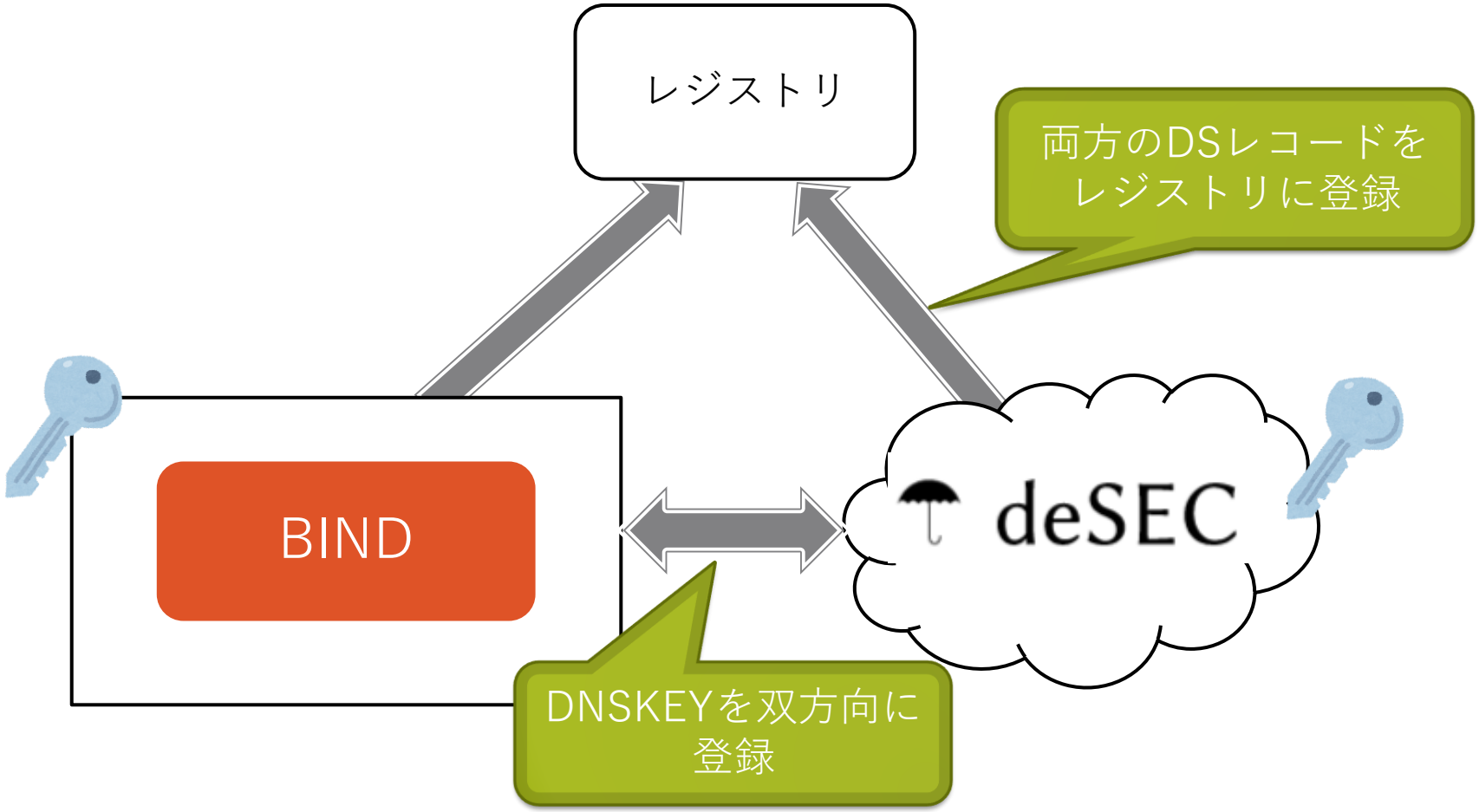


BINDからdeSECへのゾーン複製、二つのDNSプロバイダの管理

複数プロバイダでDNSSEC対応するには

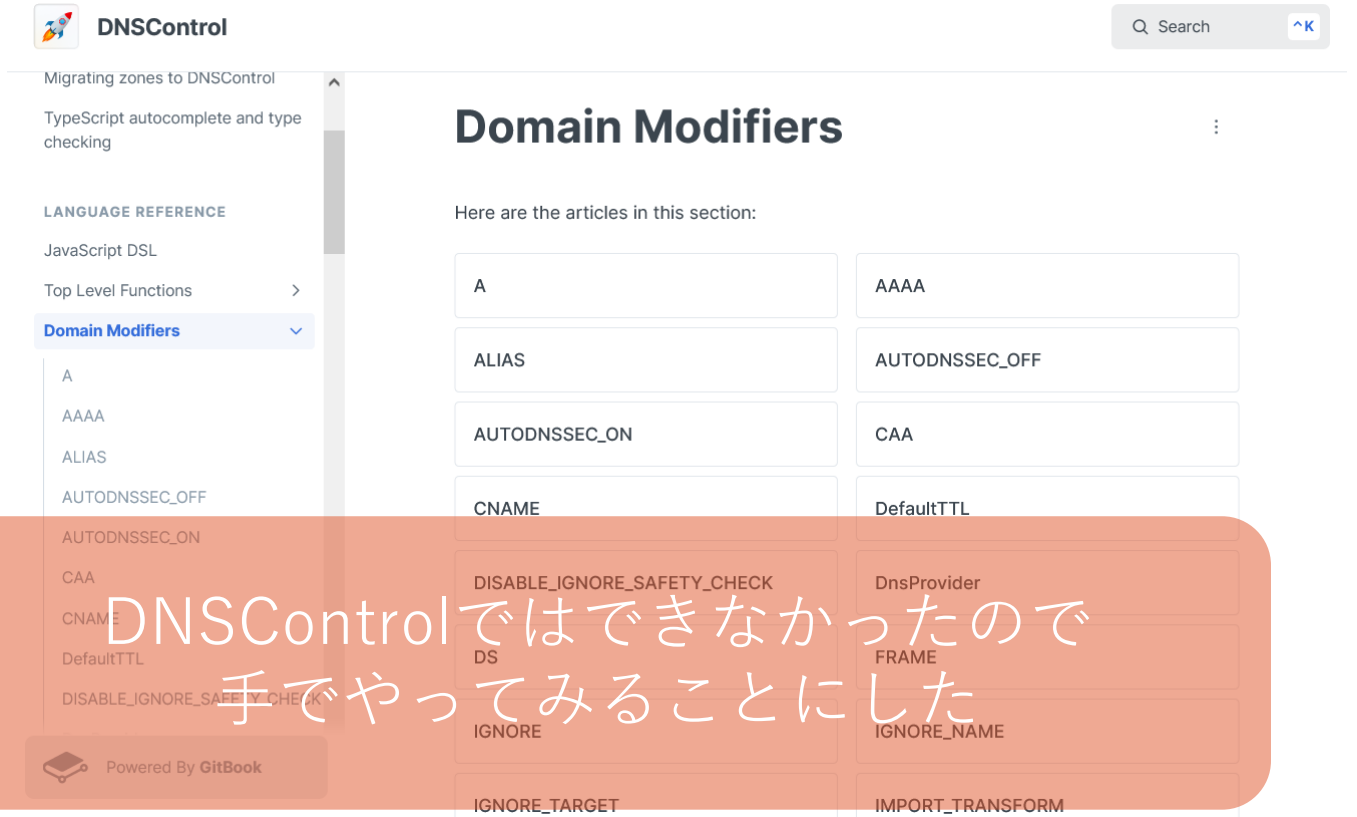
- 同じゾーンに対して、複数のプロバイダで署名する**Multi Signer Model**を未熟な頭で勉強して考えてみた
  - [Model 1]KSK鍵は共有、ZSK鍵はプロバイダ毎に別々
    - ゾーン所有者がKSK鍵を保持して署名し、各プロバイダに配布
    - ゾーン所有者が管理するDSレコードを登録
  - [Model 2]KSK鍵、ZSK鍵どちらも別々 
    - プロバイダが独自のKSK鍵で署名
    - 各プロバイダは他のプロバイダのDNSKEY(KSK,ZSKの公開鍵)をインポート
    - 各プロバイダのDSレコードを登録

BINDとdeSECでDNSSEC対応をやってみる



DNSControlでDNSKEYは管理できる？

- DNSKEYをとってくる、更新する、どちらもできなかった…



DNSControlではできなかったので
手でやってみることにした

個別でDNSSEC検証して確認

- BINDとdeSECそれぞれでDNSSECの検証に問題ないことを確認
  - digでadフラグがあること
  - VerisignのDNSSEC Analyzerで確認

```
$ dig +dnssec atana.jp

; <<>> DiG 9.16.23-RH <<>> +dnssec atana.jp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26240
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
```

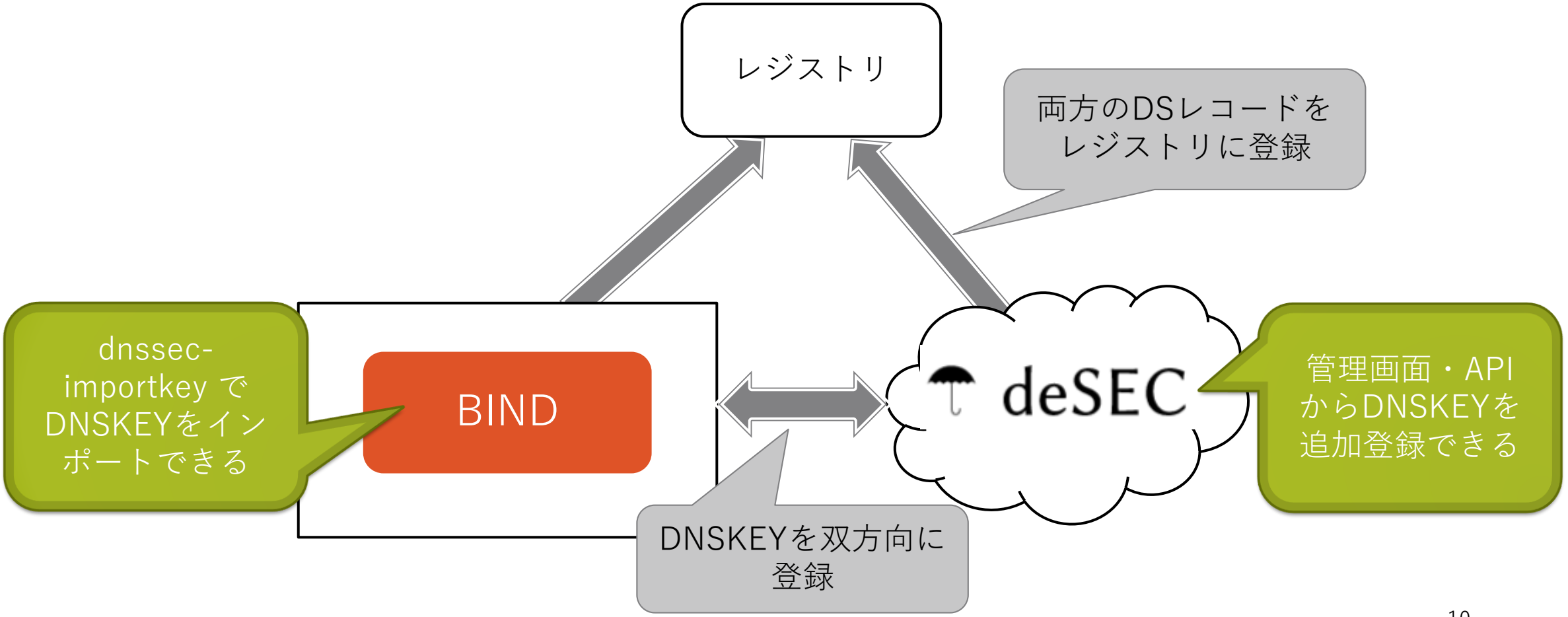
Analyzing DNSSEC problems for atana.jp

.	Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
jp	Found 1 DS records for jp in the . zone DS=39916/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=60955 and DNSKEY=60955 verifies the DS RRset Found 3 DNSKEY records for jp DS=39916/SHA-256 verifies DNSKEY=39916/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=39916 and DNSKEY=39916/SEP verifies the DNSKEY RRset
atana.jp	Found 1 DS records for atana.jp in the jp zone DS=18856/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=23526 and DNSKEY=23526 verifies the DS RRset Found 2 DNSKEY records for atana.jp DS=18856/SHA-256 verifies DNSKEY=18856/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=18856 and DNSKEY=18856/SEP verifies the DNSKEY RRset ns.work.mcnx.jp is authoritative for atana.jp Found 1 RRSIGs over NSEC RRset RRSIG=39346 and DNSKEY=39346 verifies the NSEC RRset NSEC proves no records of type A exist for atana.jp Found 1 RRSIGs over SOA RRset RRSIG=39346 and DNSKEY=39346 verifies the SOA RRset

Move your mouse over any ⊗ or ⚠ symbols for remediation hints.

Want a second opinion? Test atana.jp at dnsviz.net.

具体的にどうやって設定するか



deSEC → BINDへ設定(1)

- deSECのDNSKEYをBINDへdnssec-importkeyでインポートする

```
$ cat desec.key
atana.jp. IN DNSKEY 257 3 13
4Y7zop1sv2VmKb3Z9ojZ/SXOLelUgeljLT61BUtg/xlKrtOTEiNzfT8q7FjhsEDy328tQhPUq73VRo7kfgztlQ==
$ dnssec-importkey desec.key
Katana.jp.+013+30481.key
Katana.jp.+013+30481.private
```

DNSKEYを読み込んで
.key/.private ファイルを生成する

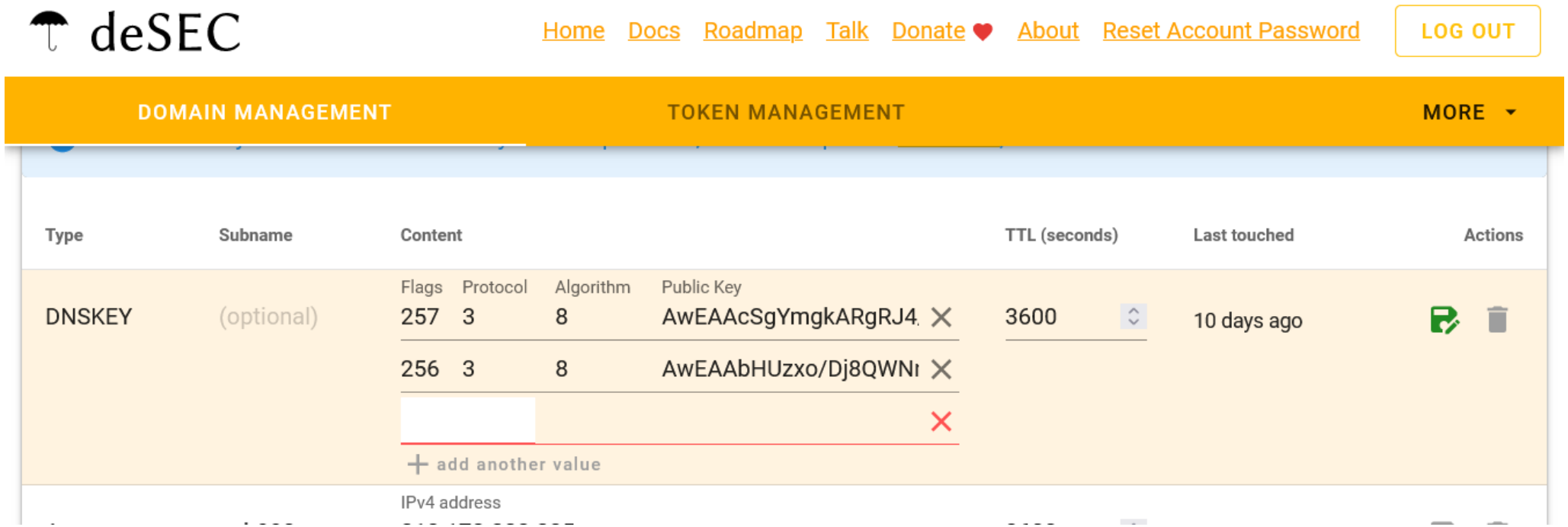
deSEC → BINDへ設定(2)

- zoneファイルに追記してdnssec-signzoneする

```
# echo "¥$INCLUDE ¥"Katana.jp.+013+30481.key¥"" >> atana.jp.zone
(シリアルあげる)
# dnssec-signzone -o atana.jp atana.jp.zone
Verifying the zone using the following algorithms:
- RSASHA256
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
Algorithm: ECDSAP256SHA256: KSKs: 0 active, 1 stand-by, 0 revoked
                            ZSKs: 0 active, 0 stand-by, 0 revoked
atana.jp.zone.signed
# named-checkzone atana.jp atana.jp.zone.signed
zone atana.jp/IN: loaded serial 2023061602 (DNSSEC signed)
OK
```

BIND → deSECへ設定

- BINDのDNSKEYを管理画面から登録



レジストリにDSレコード登録

- BIND、deSECのDSレコードをレジストリに登録

```
$ whois atana.jp
 :
[Name Server]              ns.work.mcnx.jp
[Name Server]              ns1.desec.io
[Name Server]              ns2.desec.org
[Signing Key]           18856 8 2 (
                C5F108595D02F7F2AE792A26803C12FA
                5ED01600770D1E115E977E7082E92841 )
[Signing Key]           18856 8 4 (
                609F1B682E20985005AC14D8504C9653
                E53D026EAD1385C048D370A3D7CBAF12
                065C74F069975EE002DCE7D3EF536E04 )
[Signing Key]           30481 13 2 (
                DDEF911B5830F219F191841B0816E4E3
                B2F3D622DA467B8C24B5A667A046259A )
[Signing Key]           30481 13 4 (
                663237E743DCBD354A8DFACF66FA6778
                5D687A655A0CDF24257C72815C768A99
                C17A73B9E733096D6403AAE9329974CE )
```

BINDのDSレコード

deSECのDSレコード

DNSOPS.jp DNS Operators Group, Japan　株式会社 ミライコミュニケーションネットワーク

動作確認

- 名前解決ができる
- digでadフラグがたっている
  - 署名が検証できた正しいデータである
- DNSSEC Analyzerでは対向の鍵の署名(RRSIG)がないよ！と×

```
$ dig +dnssec atana.jp

; <<>> DiG 9.16.23-RH <<>> +dnssec atana.jp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45709
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
```

Analyzing DNSSEC problems for atana.jp

.	Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
jp	Found 1 DS records for jp in the . zone DS=39916/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=60955 and DNSKEY=60955 verifies the DS RRset Found 3 DNSKEY records for jp DS=39916/SHA-256 verifies DNSKEY=39916/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=39916 and DNSKEY=39916/SEP verifies the DNSKEY RRset
atana.jp	Found 4 DS records for atana.jp in the jp zone DS=30481/SHA-384 has algorithm ECDSAP256SHA256 DS=18856/SHA-256 has algorithm RSASHA256 DS=18856/SHA-384 has algorithm RSASHA256 DS=30481/SHA-256 has algorithm ECDSAP256SHA256 Found 1 RRSIGs over DS RRset RRSIG=23526 and DNSKEY=23526 verifies the DS RRset Found 3 DNSKEY records for atana.jp DS=18856/SHA-256 verifies DNSKEY=18856/SEP DS=30481/SHA-384 verifies DNSKEY=30481/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=30481 and DNSKEY=30481/SEP verifies the DNSKEY RRset Found DNSKEY, but no RRSIG, for algorithm 8 ns2.desec.org is authoritative for atana.jp ns1.desec.io serial (2023063591) differs from ns.work.mcnx.jp serial (2023061902) Found 1 RRSIGs over SOA RRset RRSIG=30481 and DNSKEY=30481/SEP verifies the SOA RRset
atana.jp	ns.work.mcnx.jp is authoritative for atana.jp Found 1 RRSIGs over NSEC RRset RRSIG=39346 and DNSKEY=39346 verifies the NSEC RRset Found DNSKEY, but no RRSIG, for algorithm 13 NSEC proves no records of type A exist for atana.jp Found 1 RRSIGs over SOA RRset RRSIG=39346 and DNSKEY=39346 verifies the SOA RRset
atana.jp	ns1.desec.io is authoritative for atana.jp Found 1 RRSIGs over SOA RRset RRSIG=30481 and DNSKEY=30481/SEP verifies the SOA RRset Found DNSKEY, but no RRSIG, for algorithm 8

Move your mouse over any ⊗ or ⚠ symbols for remediation hints.

対向の鍵の署名RRSIGがないのはそれはそうだ

署名の検証は問題なし

まとめ

- 複数プロバイダのDNSSEC対応はハードルが高いと感じた
  - DNSControlでDNSKEYのレコード管理は現状はできない
    →OctoDNSやTerraformなど、他のDNS管理ツールでは対応しているのかな？
  - 手でやるのはつらい…
    →KnotDNSとか他ソフトウェアではどうなんだろう？
    →鍵のロールオーバーの時とか、対向のプロバイダの鍵更新をどうフックする？
  - ツールや、権威DNSサービスでの、Multi Signer Modelへの対応よろしくお願いします