

# 権威DNSサービス調査

～たまに行くならこんな店（DNSControlではしごしてみた）～

---

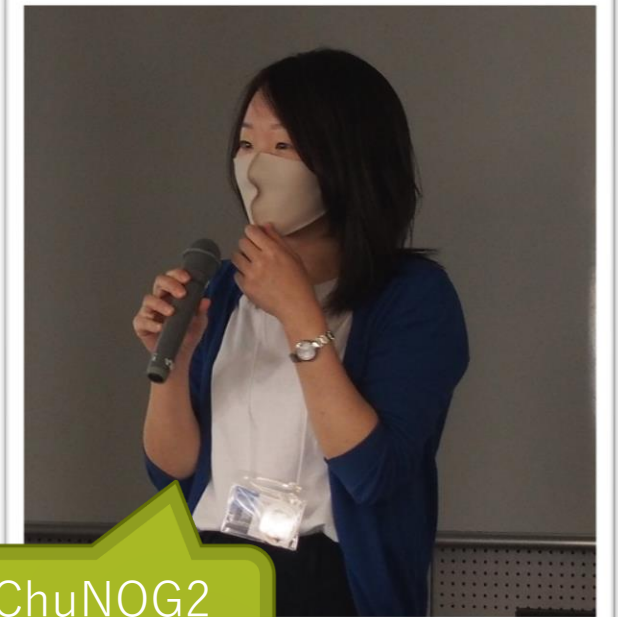
2023年4月21日

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
- 最近の出来事
  - 新卒入社で運用チームに配属された2人を育成中
    - 教案作って毎日講義（今はメールサーバ）
  - 娘とバレーボールにハマる
    - 家の中でやって照明を破壊
    - 調子に乗って腰を痛める



8/3 ChuNOG2  
in 松本やるよ

# 今日の内容

- 複数のDNSプロバイダを管理する**DNSControl**を使ってみたお話
  - 「たまに行くならこんな店」（権威DNSサービスを使ってみた調査）の”寄り道”編



# 調査のきっかけ

無料のdeSECいいな、でも無保証だし単独では使いづらいな



オンプレとdeSECを併用するしても、一度に更新できるツールないのかな



DNSControlが対応してるらしい



ちょっと使ってみよう

# 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('GICLOUD'),  
  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'),  
  TXT('test', 'example.com'))
```

dnsconfig.js

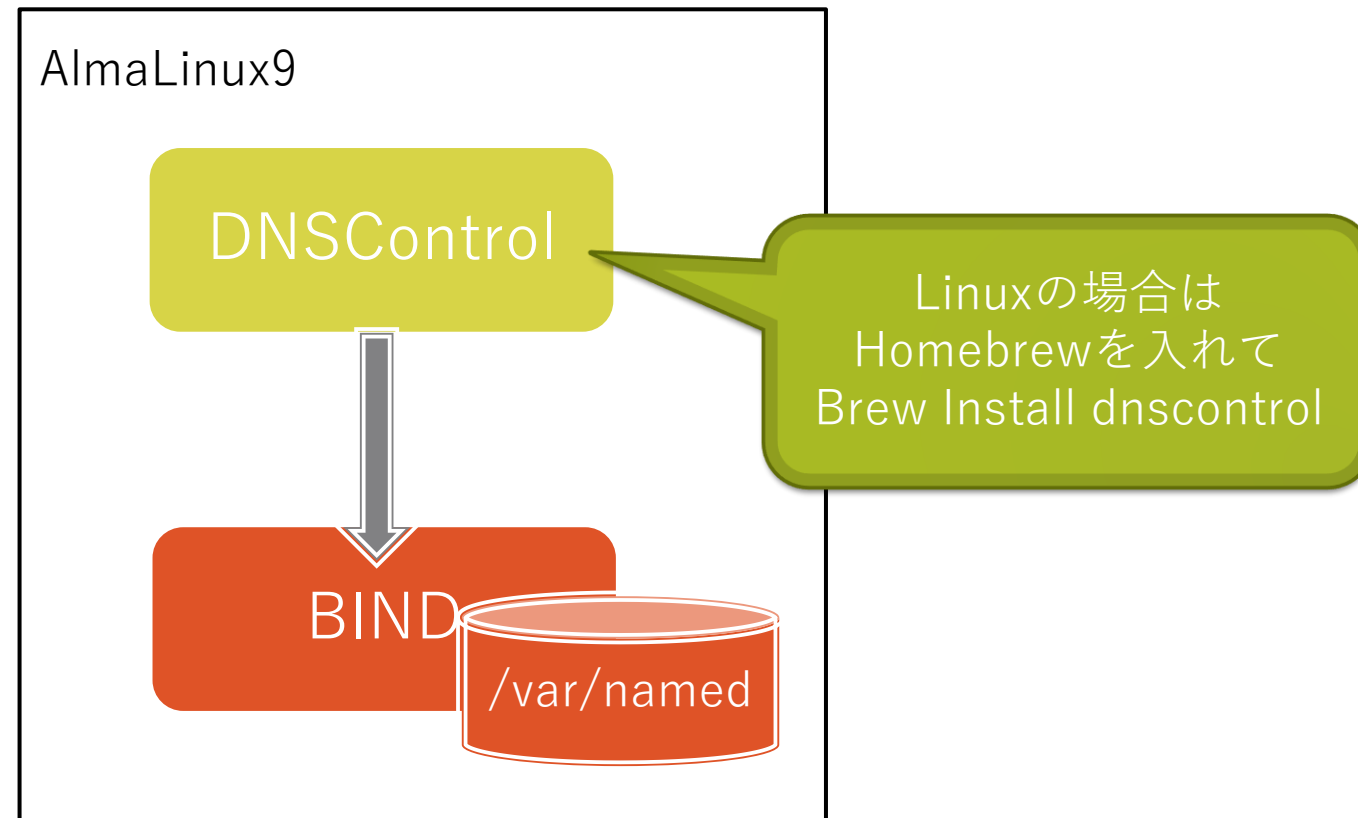
```
var addrA = IP('1.2.3.4')
```

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

```
'), // use different nameservers  
) // for department2.example.com
```

# 使い方(1)

- ローカルのBINDで使うシンプルな例でやってみる



# 使い方(2)

(1) creds.jsonを作る

```
{  
  "bind":{  
    "TYPE":"BIND",  
    "directory":"/var/named"  
  }  
}
```

更新先のDNSプロバイダを書く

(2) dnscontrols.jsを作る

```
// Providers:  
  
var REG_NONE = NewRegistrar('none'); // No registrar.  
var DNS_BIND = NewDnsProvider('bind'); // ISC BIND.  
  
// Domains:  
D('tanaka.jp', REG_NONE, DnsProvider(DNS_BIND),  
  A('test', '1.2.3.4')  
);
```

更新対象のゾーン名と、  
ゾーンの全レコードを書く

# 使い方(3)

(3)書式チェック

```
$ dnscontrol check  
No errors.
```

(4)Dry-Run

```
$ dnscontrol preview
```

(5)実行

```
$ dnscontrol push  
***** Domain: tanaka.jp  
1 correction  
#1: GENERATE_ZONEFILE: 'tanaka.jp'. Changes:  
CREATE A test.tanaka.jp 1.2.3.4 ttl=300  
DELETE A awawa.tanaka.jp 192.168.220.237 ttl=3600  
WRITING_ZONEFILE: /var/named/tanaka.jp.zone  
SUCCESS!  
Done. 1 corrections.
```

ゾーンファイルがdnsconfig.js  
の内容に更新される  
(namedのreloadはされない)



# どんなシーンで使えるか考えてみた

- 会社のドメインを、オンプレのDNSサーバだけで運用していて心配…
- コストをかけずに外部にもDNSサーバ立てたい
- レジストラが二つ以上のDNSサーバを要求する



- オンプレのDNSサーバ (BIND) のみの構成から、+deSECを使用する構成にDNSControlを使えば簡単に変更できそう

やってみよう!

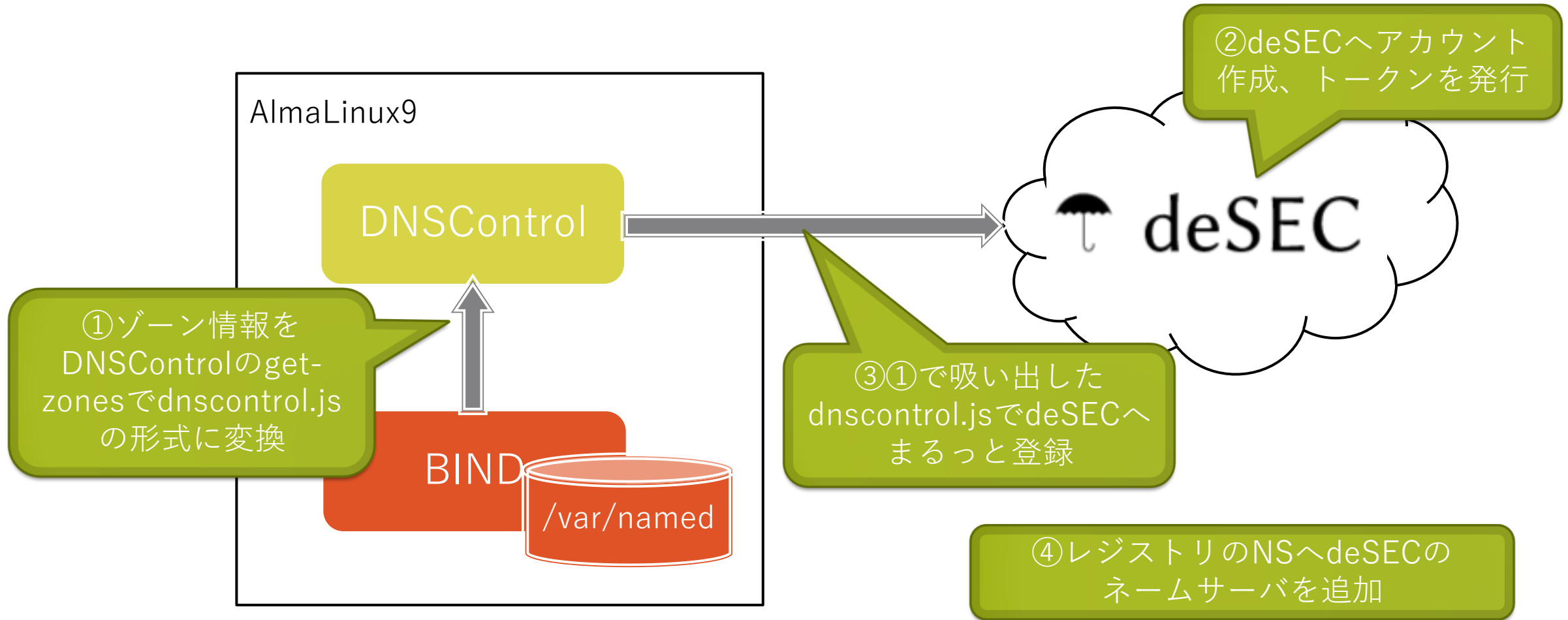


# BIND+deSECの検証 前提

- atana.jpというゾーンがあるとする

```
$TTL 3600
@      3600 IN SOA  ns.atana.jp. postmaster.atana.jp. 2023030300
       7200 1800 1209600 86400
       IN NS   ns.atana.jp.
ns     IN A     210.172.xxx.xxx
www    IN A     210.172.xxx.xxx
mail   IN A     210.172.xxx.xxx
@      IN MX    10 mail.atana.jp.
tomato IN A     210.172.xxx.xxx
```

# BIND+deSECの検証 導入の流れ



# BIND+deSECの検証 BINDから吸い出す

- DNSControlでget-zonesするための準備をする
  - Creds.jsonファイルを作る

```
{  
  "bind":{  
    "TYPE":"BIND",  
    "directory":"/var/named"  
  },  
}
```

# BIND+deSECの検証 get-zonesの実行

- dnscontrol get-zonesを実行してdnsconfig.jsの形式に変換する

```
$ dnscontrol get-zones --format=js bind - atana.jp > dnsconfig.js
$ cat dnsconfig.js
var DSP_BIND = NewDnsProvider("bind");
var REG_CHANGEME = NewRegistrar("none");
D("atana.jp", REG_CHANGEME,
  DnsProvider(DSP_BIND),
  //SOA('@', 'ns.atana.jp.', 'postmaster.atana.jp.', 2023030300, 7200, 1800, 1209600,
86400, TTL(3600)),
  //NAMESERVER('ns.atana.jp.'),
  A('ns', '210.172.xxx.xxx'),
  A('www', '210.172.xxx.xxx'),
  A('mail', '210.172.xxx.xxx'),
  MX('@', 10, 'mail.atana.jp.'),
  A('tomato', '210.172.xxx.xxx')
)
```

deSEC側で無効な行は  
自動的にコメントアウト  
された

# BIND+deSECの検証 トークンの発行

- deSECでアカウントを作成、トークンを発行
  - 有効期限、アクセス元IPアドレスを指定する

deSEC

[Home](#) [Docs](#) [Roadmap](#) [Talk](#) [Donate](#) [About](#) [Reset Account Password](#)

LOG OUT

DOMAIN MANAGEMENT

TOKEN MANAGEMENT

MORE

Tokens

Search



Show advanced

**New feature:** You can now configure your tokens for finer access control. Check out the advanced settings switch above!

Name	Valid	Secret	Created	Last
(optional)	<input checked="" type="checkbox"/>	(only displayed once)	less than a minute ago	less
<u>dnscontrols-test</u>	<input checked="" type="checkbox"/>	(only displayed once)	3 months ago	3 m

Rows per page

ent subnets

Generate New Token



✔ Your new token's secret value is:  
qTzJf4JiPbqHUZP6obDiZ5drevxB  
It is only displayed once.

You can create a new API token here. The token is displayed after submitting this form.

一度だけ表示されるので  
トークンを保存

# BIND+deSECの検証 登録の準備

- deSECへ登録する準備 (creds.jsonとdnsconfig.jsを編集)

```
{  
  "desec": {  
    "TYPE": "DESEC",  
    "auth-token": "FKrKk6mY*****"  
  },  
  "bind": {  
    "TYPE": "BIND",  
    "directory": "/var/named"  
  }  
}
```

deSECの記述を追加  
取得したトークンを指定

```
var REG_NONE = NewRegistrar("none"); // No registrar.  
var DSP_DESEC = NewDnsProvider("desec"); // deSEC  
var DNS_BIND = NewDnsProvider('bind'); // ISC BIND.  
D("atana.jp", REG_NONE, DnsProvider(DSP_DESEC), DnsProvider(DNS_BIND),
```

BINDとdeSECに対して  
更新をかけるよう編集

# BIND+deSECの検証 deSECへ登録

- deSECへレコードを登録する

```
$ dnscontrol push
```

```
***** Domain: atana.jp
```

```
1 correction
```

```
#1: GENERATE_ZONEFILE: 'atana.jp'. Changes:
```

```
DELETE NS atana.jp ns.atana.jp. ttl=3600
```

```
WRITING_ZONEFILE: /var/named/atana.jp.zone
```

```
SUCCESS!
```

```
1 correction
```

```
#1: Changes:
```

```
CREATE A ns.atana.jp 210.172.xxx.xxx ttl=3600
```

```
DELETE A test.atana.jp 1.2.3.4 ttl=3600
```

```
MODIFY A tomato.atana.jp: (1.2.3.5 ttl=3600) -> (210.172.xxx.xxx ttl=3600)
```

```
:
```

```
SUCCESS!
```

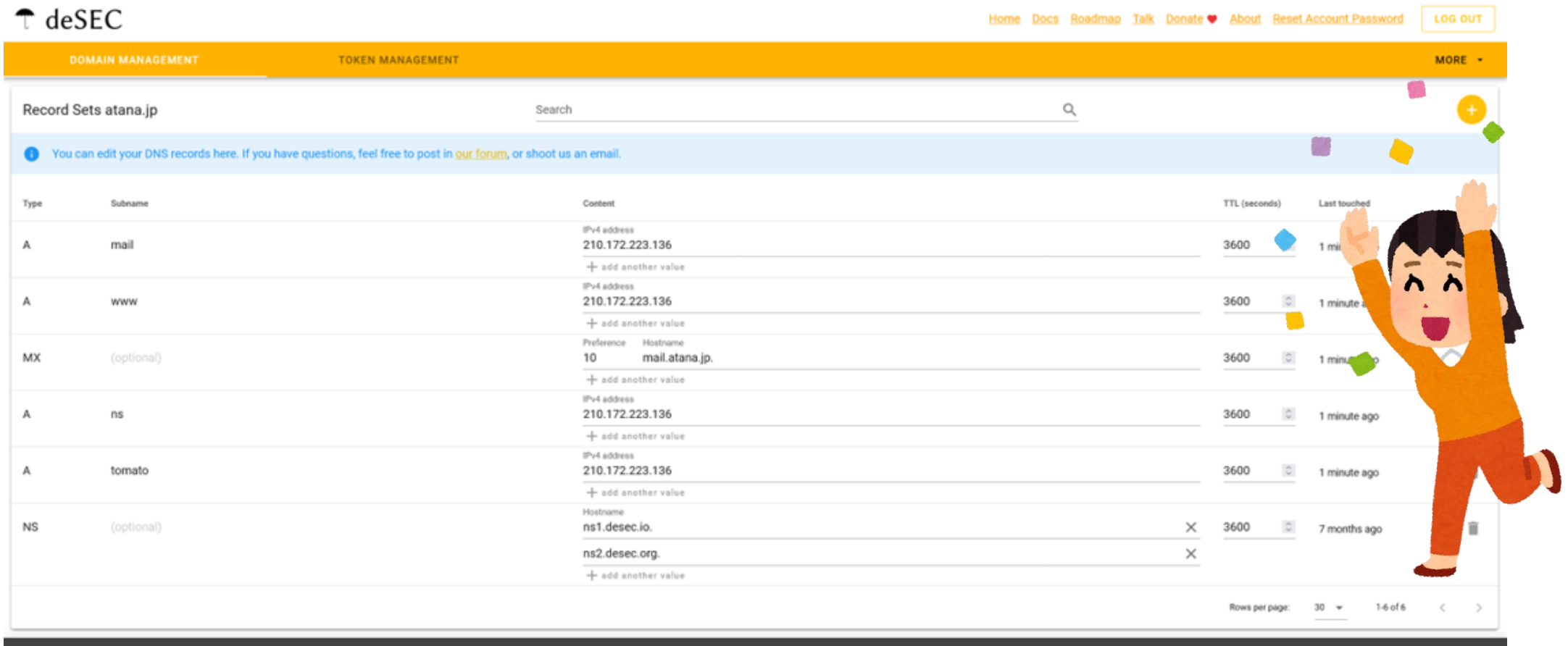
```
Done. 2 corrections.
```

deSECへ登録が  
SUCCESS!



# BIND+deSECの検証 deSECで確認

- deSECの管理画面で確認する



deSEC

Home Docs Roadmap Talk Donate About Reset Account Password LOG OUT

DOMAIN MANAGEMENT TOKEN MANAGEMENT MORE

Record Sets atana.jp Search

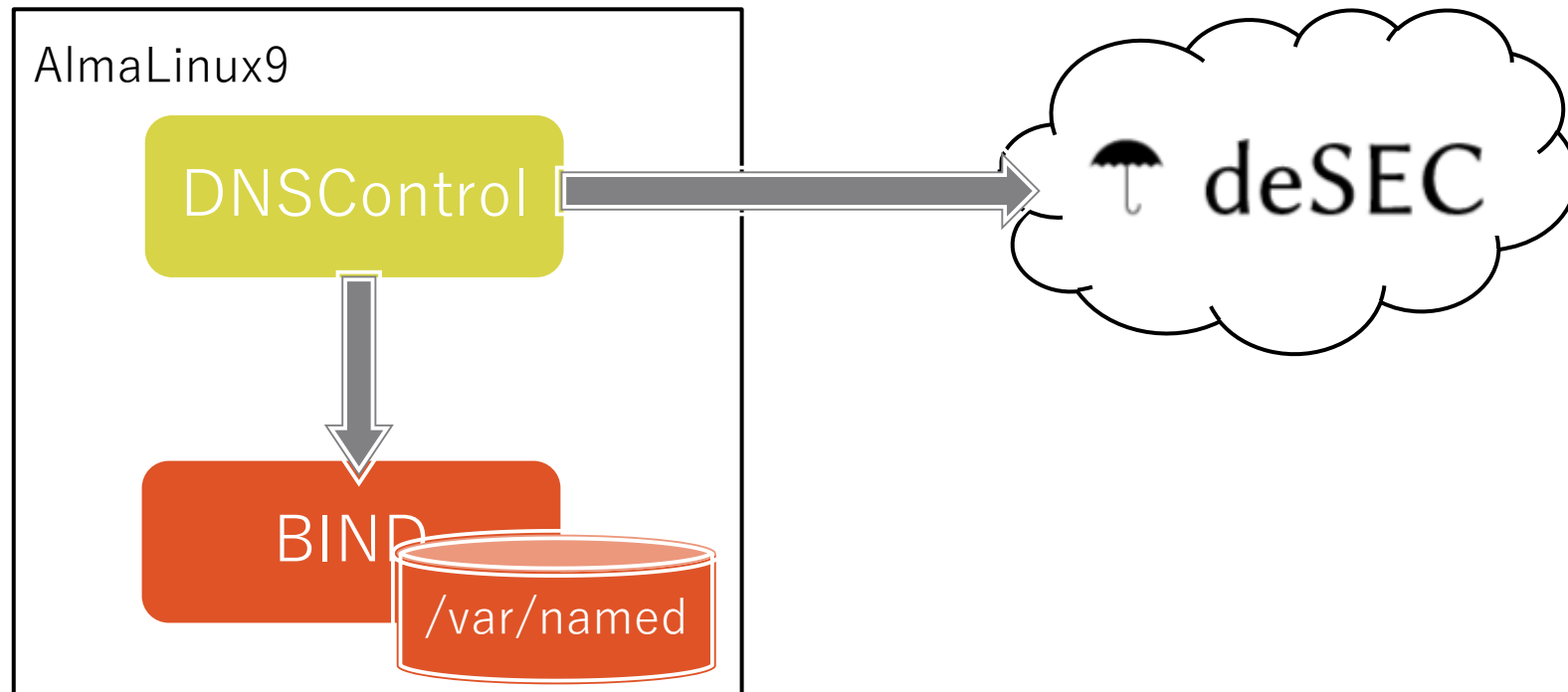
You can edit your DNS records here. If you have questions, feel free to post in [our forum](#), or shoot us an email.

Type	Subname	Content	TTL (seconds)	Last touched
A	mail	IPv4 address 210.172.223.136 + add another value	3600	1 minute ago
A	www	IPv4 address 210.172.223.136 + add another value	3600	1 minute ago
MX	(optional)	Preference Hostname 10 mail.atana.jp. + add another value	3600	1 minute ago
A	ns	IPv4 address 210.172.223.136 + add another value	3600	1 minute ago
A	tomato	IPv4 address 210.172.223.136 + add another value	3600	1 minute ago
NS	(optional)	Hostname ns1.desec.io. X ns2.desec.org. X + add another value	3600	7 months ago

Rows per page: 30 14 of 6

# BIND+deSECの検証 その後の運用

- その後のレコード更新などの運用はDNSControlで管理できそう



# 使ってみて気になったこと

- BINDはゾーンファイルの更新まででreloadはされない  
→ファイルのタイムスタンプをみてreloadをかける仕組みなど必要そう
- 複数のDNSプロバイダに更新を行い、片方が失敗したときはどうなるの？  
→両方更新されなかった
- SOAレコードは一緒にできる？ →deSECは自動なのでできなかった…

```
$ host -t SOA atana.jp ns1.desec.io  
atana.jp has SOA record get.desec.io. get.desec.io. 2023043881 86400 3600 2419200 3600
```

→SOAレコードがDNSプロバイダごとに違っているとどんな問題あるだろう？

- DNSプロバイダへはどのポートでアクセス？ →deSECはhttps

# まとめ

- DNSControl、使ってみるための最初の導入はやさしい
- 各DNSプロバイダのAPIの仕様を吸収してくれるので、DNSプロバイダ間の移行が簡単にできる
  - オンプレからクラウドへの移行も簡単
  - 管理画面からひとつひとつ登録したり、APIの使い方を学習する手間がはぶける
  - 変数やマクロが使えるのは便利
- DNSSEC署名ありは今後ためせるといい

