DNSSEC UPDATE

VALIDATION編

IIJ

其田　学

自己紹介

- 今年からIIJで仕事してます。
- 主にお守りしてるもの
  - 回線系のFull Resolver
  - とあるccTLDのSlave

最近の話題

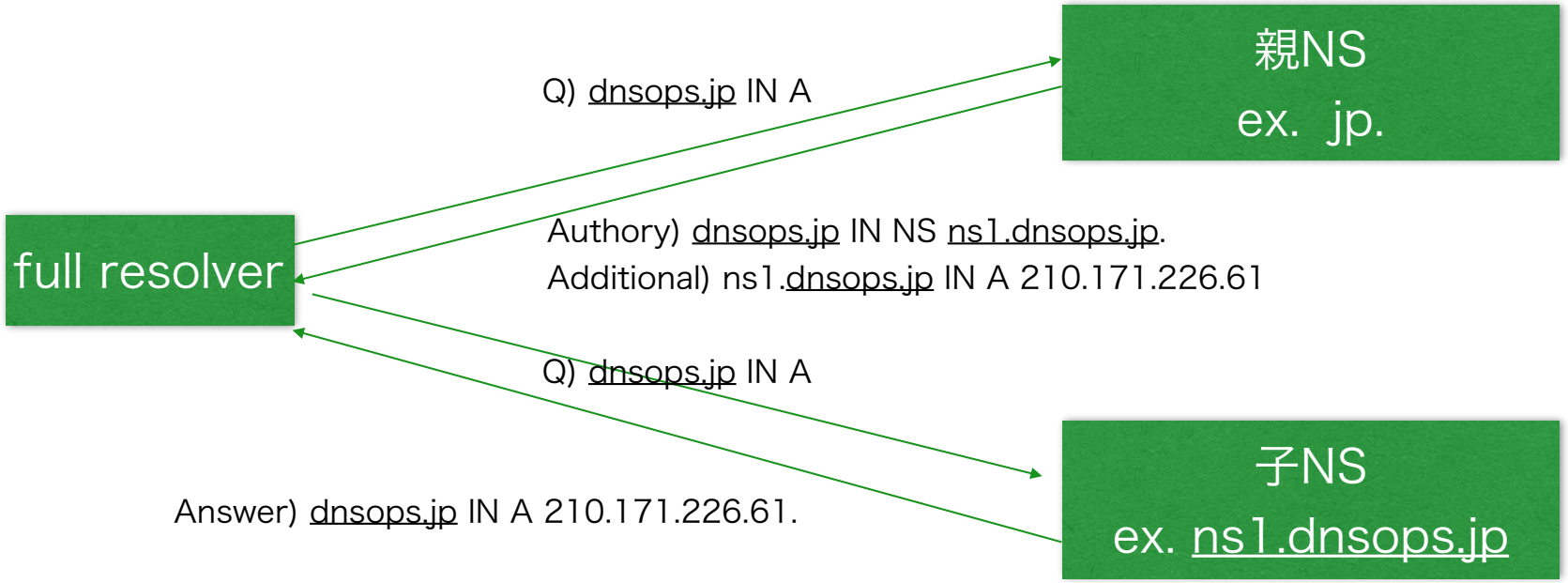
- 最近、キャッシュサーバへの攻撃ふえてますよねー
- 毒入りされたらどうしよう
- Validationしたら毒入れされたとき、どこまで対応できるの？（つぶらな瞳で）

なんとなく想像

- DoSは防げません。（当然）
- 毒入れされても、信頼の連鎖がつながっているゾーンで、署名があるRRだったら、SERVFAILになってくる。
- 最近問題になってる、Delegationを狙った毒入れって成功するのかな。信頼の連鎖を崩すような攻撃ってできるのかな。
  - empty non-terminalへの毒入れとか

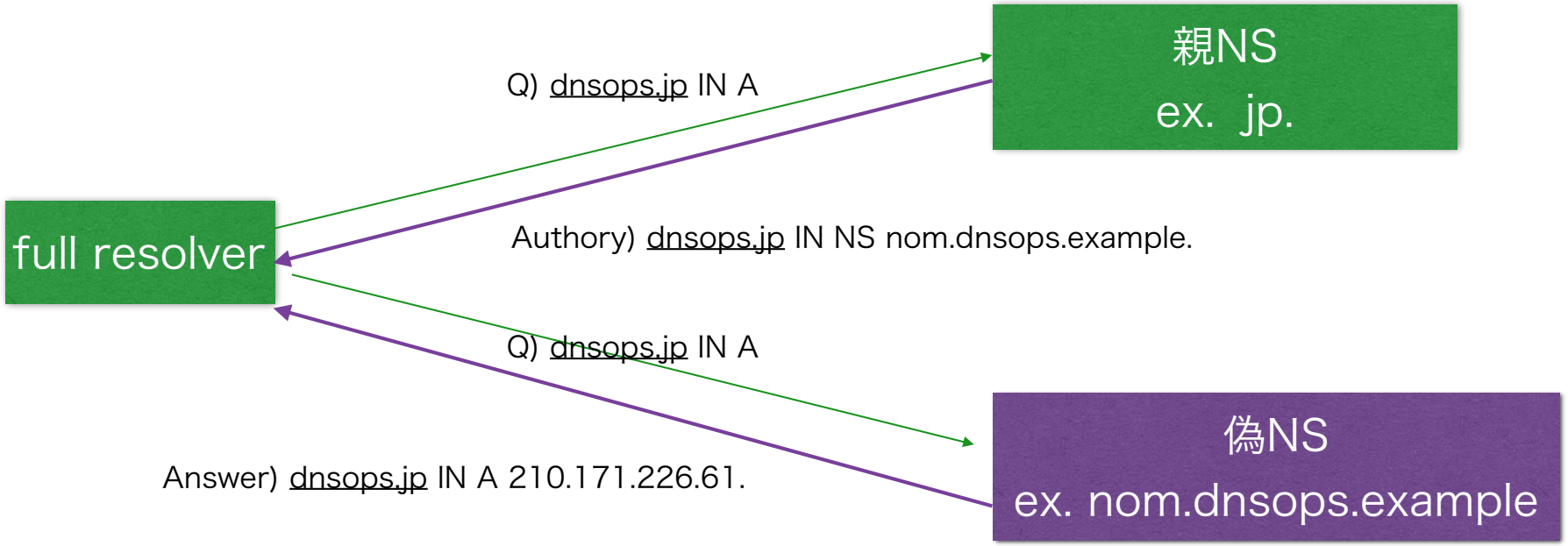
Delegationを狙った毒入れ

- Delegationで使用されるNSとglueは署名されないので、毒入れが可能です。



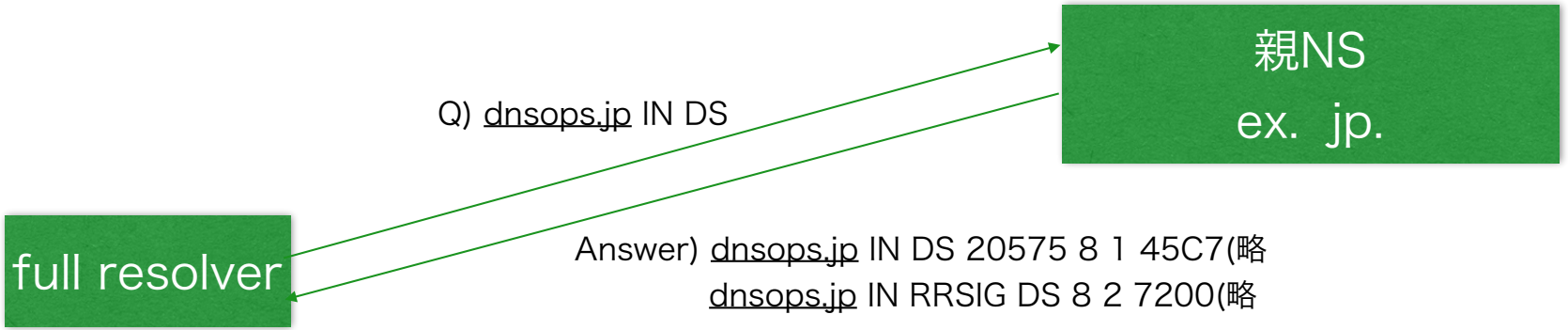
Delegationを狙った毒入れ

- Delegationで使用されるNSとglueは署名されないので、毒入れが可能です。



Delegationを狙った毒入れ

- 一方、Validationを有効にすると、DSレコードを問い合わせるようになります。
- DSレコードのリクエスト応答が適切でないと、Delegationされたゾーンの検証ができず、Validation Errorになります。



- DSレコードに対する応答を改ざんする必要があります。

- ２種類の方法が考えられます。

  - 誘導先のゾーンをDNSSEC署名して、それに対応するDSとRRSIGを親から返す。（RRSIGを作る為には親ゾーンの秘密鍵が必要なので、実質無理）

  - 2.有効な不在証明を返す。

DSレコードの
応答別に考えてみる

DSが存在する場合

- DS RRが既にある場合、対応するNSEC or NSEC3 レコードが作られます。

ex. dnsops.jp NSEC

```
dnsops.jp    900 NSEC    a.b.c.d.e.f.g.jp.jp. NS DS RRSIG NSEC
dnsops.jp    900 RRSIG    NSEC 8 2 900 20140730014020(略
```

ex. dnsops.jp NSEC3 RR

```
JSDBON82LMO72B73S2439HFUQH722TEP.jp. 900 IN NSEC3 1 1 5 40FCE57413 (
                MDI5NI1S58IVP315UTKJ6CPH7G8JVG7D
                NS DS RRSIG )
JSDBON82LMO72B73S2439HFUQH722TEP.jp. 900 IN RRSIG  (略
```

DSが存在する場合

- NSEC3,NSECにDSが存在するとあるので、DSの不在証明ができません。DS RRを無いことにできません。つまり、DSの応答が検証できず、DSと子ゾーンはValidation Errorになります。

ex. dnsops.jp NSEC

```
dnsops.jp    900 NSEC    a.b.c.d.e.f.g.jp.jp. NS DS RRSIG NSEC
dnsops.jp    900 RRSIG    NSEC 8 2 900 20140730014020(略
```

ex. dnsops.jp NSEC3 RR

```
JSDBON82LMO72B73S2439HFUQH722TEP.jp. 900 IN NSEC3 1 1 5 40FCE57413 (
                    MDI5NI1S58IVP315UTKJ6CPH7G8JVG7D
                    NS DS RRSIG )
JSDBON82LMO72B73S2439HFUQH722TEP.jp. 900 IN RRSIG  (略
```

DSレコードが存在しない場合

- DNSSEC的に守れるゾーンじゃないので、基本的に毒入れできます。
  - 毒入れ対象のNS RRが存在する場合
    （既存のDelegationへの毒入れ）
  - 毒入れ対象のNS RRが存在しない場合
    （新規にDelegationを作る場合）

NSレコードが存在する場合

- NSEC3 RR、NSEC RRがある場合
  - DSは元からないので、不在証明できます。
    （通常の応答そのもの）

ex. dnsops.jp NSEC

dnsops.jp　900 NSEC　a.b.c.d.e.f.g.jp.jp. NS RRSIG NSEC

DSを持ってない既存のドメインは守れません

NSレコードが存在しない場合

- NSEC,NSEC3（非opt-out)の場合で、NSEC,NSEC3レコードが無い場合

ex1. dnsops.jp NSEC

```
a.dns.jp   900 NSEC     a.b.c.d.e.f.g.jp. A RRSIG NSEC
```

ex2. dnsops.jp NSEC3

```
IJNUTC2O54Q9I4ANJJNN0N4KCD40BGV0.jp. 900 IN NSEC3 1 0 5 40FCE57413 (
                    MDI5NI1S58IVP315UTKJ6CPH7G8JVG7D
                    NS DS RRSIG )
```

- 毒入れ対象名をカバーするNSEC,NSEC3があるため、毒入れ対象名のレコードは存在できない。
- にも関わらず、NSレコードは毒入れである状態なので、DSの不在証明がValidation Errorになる。

NSレコードが存在しない場合

- NSEC3（opt-out)の場合で、NSEC3レコードがある場合

ex3. dnsops.jp NSEC3

```
JSDBON82LMO72B73S2439HFUQH722TEP.jp. 900 IN NSEC3 1 1 5 40FCE57413 (
                MDI5NI1S58IVP315UTKJ6CPH7G8JVG7D
                txt RRSIG )
```

- NSEC3レコードでNSレコードの存在がないのにも関わらず、NSレコードが毒入れで存在する状態。
- DSの不在証明ができずにValidation Error

NSレコードが存在しない場合

- NSEC3(opt-out)の場合で、毒入れ対象のNSEC3レコードが存在しない場合
- opt-outの場合は、NSレコードはNSEC3の対象外

ex2. dnsops.jp NSEC3

```
IJNUTC2O54Q9I4ANJJNN0N4KCD40BGV0.jp. 900 IN NSEC3 1 1 5 40FCE57413 (
                NV9FF42TA5ANGDF350VPBSTD3CDIVVQV
                NS DS RRSIG )
```

- 毒入れ対象名をカバーするNSEC,NSEC3があるため、毒入れ対象名のレコードは存在できない。
- が、opt-outの場合はNSに対応するNSEC3がなくてもいいので、エラーにはならない。
- DSの不在証明ができたので、移譲先はValidationしない。

NSEC3(optout)でNSEC3 RRを持つ必ず場合

- 権威のあるRRがあるとき（NS RRとglue以外のRR）
- empty non-terminalで、子孫にSecureなDelegationがあるとき。

例 example.zone

secure.em2.em1.example.	DS有
em2.em1.example.	RRが無くてもNSEC3有
em1.example.	RRが無くてもNSEC3有

- なお子孫にDSが無い場合は守るDelegationが無いのでNSEC3は無くてもよい

empty non-terminalを狙った攻撃も大丈夫そうですね。

まとめ

- 署名したゾーンと、SecureなDelegationがあれば、権威がある応答は毒入れされてもstub resolverに偽の応答を返しません。
- Delegationと、信頼の連鎖は別ものです。
- DSを制するものがDNSSECを制す。
- 詳しく知りたい方はNSEC3 沼に嵌まればいいかと