RFC 4509

DNSSEC Delegation Signer (DS) Resource Records (RRs) での SHA-256 の利用

DNSSEC.jp プロトコル理解SWG

2010 dnssec.jp

要旨

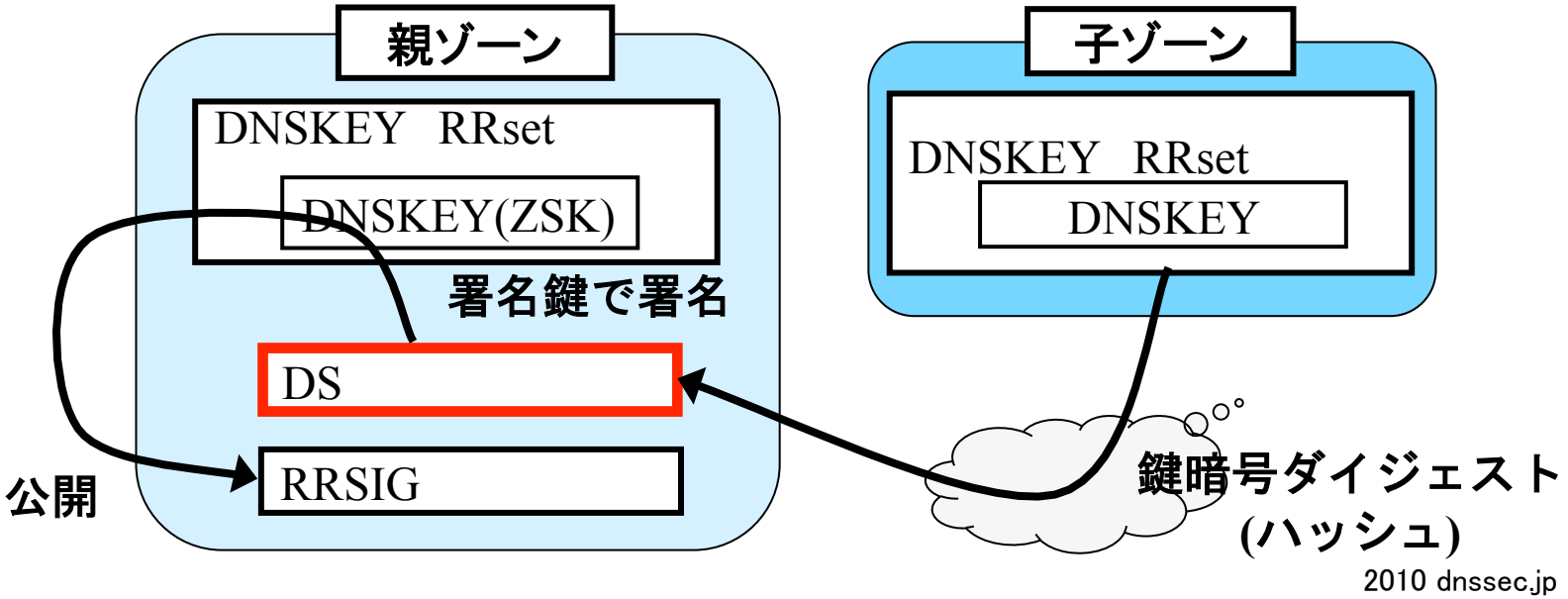
- DSレコードにおいては、基本的にSHA256アルゴリズムを使うべき。
- 運用面からは、SHA-1ベースとSHA-256ベースの両方のDSレコードを配置するのが望ましいが、SHA-1ベースは今後攻撃対象とされる可能性もあることに留意する。

1. Introduction

- DNSSEC [RFC4033] [RFC4034] [RFC4035] DS(Delegation Signer) RR は、子ゾーンの DNSKEY RRset の1つの鍵暗号ダイジェスト(ハッシュ)を配布するために親ゾーンで公開される。

  DS RRset は、親ゾーンが使用するアルゴリズムを使い、親ゾーンのゾーンデータ署名鍵(ZSK)で署名される。

  各署名は、DS RRset と同じドメイン名で RRSIG RR で公開される。



2010 dnssec.jp

2. DSレコードサポートのためのSHA-256アルゴリズムの実装

- DSレコードに使用するために、ダイジェストタイプ コード2に SHA-256 [SHA256] [SHA256CODE] を割り当てる。
- ダイジェストアルゴリズムの結果は切り捨てられてはならない。(MUST NOT)
- 全部で32バイトのダイジェスト結果はDSレコードで公開される。

2.1. DSレコードフィールド値

- DSレコードの中でSHA-256ダイジェストアルゴリズムを使う時は、次のDSレコードフィールドを利用する:

  ダイジェストタイプ: 2

- ダイジェスト：次の式を使って計算したSHA-256ダイジェスト値。 (“|” は結合を意味する)

  結果の値は切り捨てない。32バイトの結果は DSレコードと関連する計算で使われる。

  digest = SHA_256(DNSKEY owner name | DNSKEY RDATA)

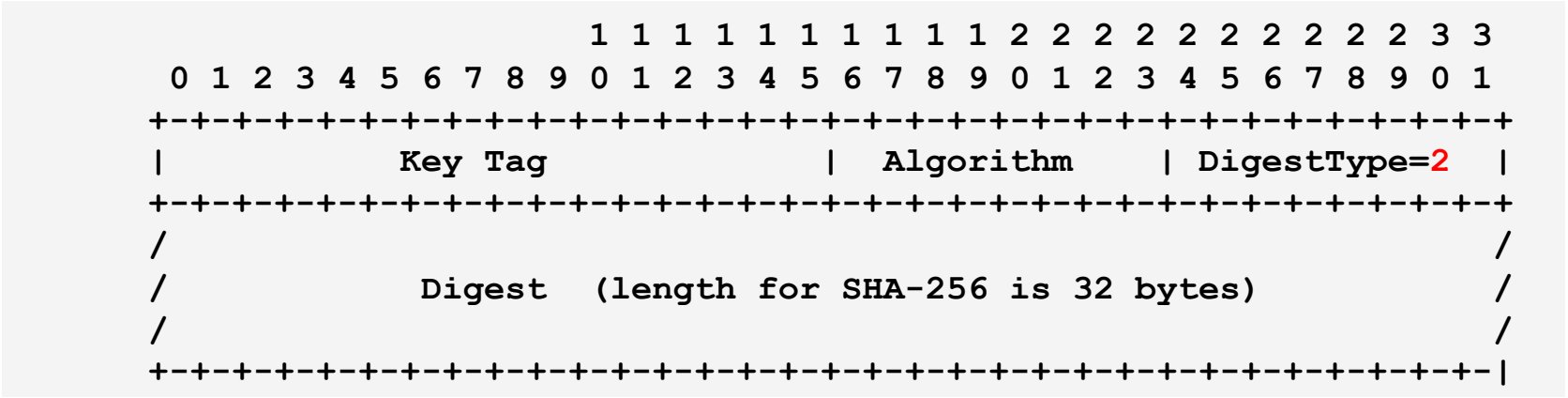
- DNSKEY RDATAは [RFC4034] で定義された通り：

  DNSKEY RDATA = Flags | Protocol | Algorithm | Public Key

- KeyTagフィールドとアルゴリズムフィールドは [RFC4034] で指定される。

2.2. SHA-256 を伴うDSレコード

- DSレコードのワイヤフォーマット:



2.3. SHA-256 を使う DSレコードの例

DSレコードに一致するDNSKEYの例:

[RFC4034] の 5.4節にある DNSKEY/DSレコードの例である。

```
The DNSKEY record:
dskey.example.com. 86400 IN DNSKEY 256 3 5 ( AQOeiiR0GOMYkDshWoSKz9Xz
                                            fwJr1AYtsmx3TGkJaNXVbfi/
                                            2pHm822aJ5iI9BMzNXxeYCmZ
                                            DRD99WYwYqUSdjMmmAphXdvx
                                            egXd/M5+X7OrzKBaMbCVdFLU
                                            Uh6DhweJBjEVv5f2wwjM9Xzc
                                            nOf+EPbtG9DMBmADjFDc2w/r
                                            ljwvFw==
                                            ) ;  key id = 60485
```

- SHA-256ダイジェストを使って、上記のDNSKEYレコードをカバーする DSレコード:

```
dskey.example.com. 86400 IN DS 60485 5 2  ( D4B7D520E7BB5F0F67674A0C
                                            CEB1E3E0614B93C4F9E99B83
                                            83F6A1E4469DA50A )
```

KeyTag フィールド

アルゴリズムフィールド 5
RSA/SHA-1 [RSASHA1]

ダイジェストタイプ 2
SHA-256

ダイジェスト(16進)

2010 dnssec.jp

3. 実装に必要な要件

- DS RR においては、SHA-256アルゴリズムの実装をサポートしなければならない。 (MUST)

- SHA-256ダイジェストを持っている DS RRが DS RRset に存在するならば、検証者(Validator)の実装は SHA-1ダイジェストを含んでいる DS RRを無視するべきである。(SHOULD)

4. 展開の検討

- 検証者(Validator)が SHA-256 ダイジェストタイプをサポートしておらず、ゾーンの DS RRset に他にサポートするダイジェストタイプが存在しないならば、検証者(Validator)には親ゾーンから子ゾーンへ認証する経路は存在しない。

- リゾルバは、［RFC4035］の5.2節で述べているように、DS RRset が存在しないことを証明している署名つき NSEC RRset の場合のように扱うべきである。

【RFC4035】 5.2 Authenticating Referrais:

親ゾーンから得られた参照がDS RRsetを含まない場合、委任された名前に関するDS RRsetが存在しないことを証明する署名付きNSEC RRsetを含めること。

4. 展開の検討 (続き)

- ゾーン管理者は、ゾーンを参照している検証者(Validator)のSHA-256に対するサポート具合を把握することができないことから、ゾーン運用者はSHA-1ベースとSHA-256ベースのDSレコードの両方を配置することを考慮したほうが良い。

  これは、あらゆるDSレコードが対象。

- 両方のダイジェストタイプを利用するべきかどうか、そしていつまでサポートすべきかは、この文書の範疇ではない。

5. IANA の検討 (割り当て)

- DSレコードでSHA-256のために使われるダイジェストタイプはIANAによって割り当てられている。

- 執筆の時点で、DSレコードの使用のために割り当てられている最新のダイジェストタイプは次の通り：

VALUE	Digest Type	Status
0	Reserved	-
1	SHA-1	MANDATORY(必須)
2	SHA-256	MANDATORY(必須)
3-255	Unassigned	-

6. セキュリティの検討

6.1. ダイジェストタイプ格下げ攻撃の可能性

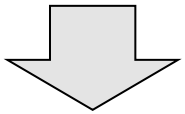
- もし次の条件が成立するなら、強いダイジェストタイプを弱いダイジェストタイプに格下げする攻撃が可能である:
  - 複数のDSレコードが、それぞれ異なるダイジェストタイプを使っている。
  - 強いダイジェストが存在するが無効になっている場合、検証者(Validator)は弱いほうのダイジェストを受け入れる。

6.1. ダイジェストタイプ格下げ攻撃の可能性 (続き)

○ 攻撃例:

– ある子ゾーンのDNSKEYに対し、SHA-1ベースとSHA-256ベースのダイジェストの両方が親ゾーンのDSレコードで公開される。

- SHA-1ダイジェストを持つDSレコードは、子ゾーンのDNSKEYを使って計算されたダイジェストと一致する。
- SHA-256ダイジェストを持つDSレコードは、子ゾーンのDNSKEYを使って計算されたダイジェストと一致しない。



検証者(Validator) が安全であると判断するなら、SHA-256ダイジェストは無視される。

6.2. DSレコードにおける SHA-1対SHA-256の検討

→ SHA-256 を使いましょう

- DNSSECのユーザはソフトウェアの実装が可能になり次第、SHA-256を有効にするよう奨励される。
- SHA-256はSHA-1より攻撃に強いと広く信じられている。そしてSHA-1の強度は最近公表された攻撃により脅かされている。
- 執筆の時点ではSHA-1に対する攻撃がDNSSECに影響を与えるであるかどうかにかかわらず、DSレコードではSHA-256を使うのがより良い選択肢であると信じている。
- 執筆の時点では、SHA-256ダイジェストアルゴリズムはしばらくの間は十分な強度であると考えられる。そして、DNSSEC DS RRでの用途にも十分であると考えられる。

  しかしながら、将来公開される攻撃手法によって DS RRでのアルゴリズムの有用性を弱めるかもしれない。
- SHA-256ダイジェストアルゴリズムの暗号強度について推測することはこの文書の範疇ではない。