RFC 4034
DNSSEC.jp プロトコル理解SWG

インターネットマルチフィード㈱
豊野 剛
平塚 健太

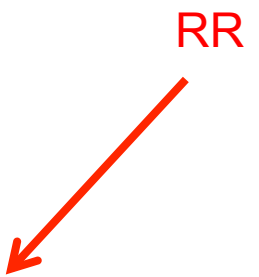
RFC4034の構成(1.intro)

- DNSSECにて新たに導入された4つのRR {DNSKEY, RRSIG, NSEC, DS}についての定義
  - RRの目的
  - RRの資源データ(RDATA)の目的
  - RRの表示フォーマット(ASCII表現)

```
example.com. 86400 IN DNSKEY 256 3 5   ( AQPSKmynfzW4kyBv015MUG
                                          2DeIQ3Cbl+BBZH4b/0PY1kxkm
                                          vHjcZc8no kfzj31GajIQKY+5CptL
                                          r3buXA10h WqTkF7H6RfoRqXQe
                                          ogmMHfpftf6zMv1LyBUgia7za6
                                          ZEzOJBOztyvhjL742iU/TpPSEDhm
                                          2SNKLijfUppn1U aNvv4w== )
```

RFC4034の構成(1.intro)

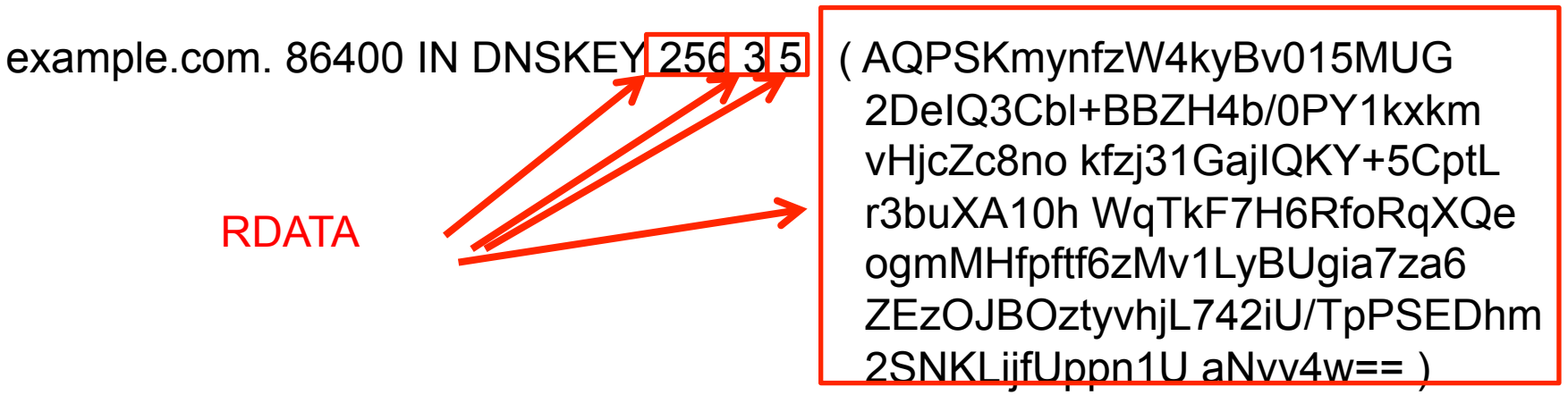
- DNSSECにて新たに導入された4つのRR {DNSKEY, RRSIG, NSEC, DS}についての定義
  - RRの目的
  - RRの資源データ(RDATA)の目的
  - RRの表示フォーマット(ASCII表現)




```
example.com. 86400 IN DNSKEY 256 3 5   ( AQPSKmynfzW4kyBv015MUG
                                          2DeIQ3Cbl+BBZH4b/0PY1kxkm
                                          vHjcZc8no kfzj31GajIQKY+5CptL
                                          r3buXA10h WqTkF7H6RfoRqXQe
                                          ogmMHfpftf6zMv1LyBUgia7za6
                                          ZEzOJBOztyvhjL742iU/TpPSEDhm
                                          2SNKLijfUppn1U aNvv4w== )
```

RFC4034の構成(1.intro)

- DNSSECにて新たに導入された4つのRR {DNSKEY, RRSIG, NSEC, DS}についての定義
  - RRの目的
  - RRの資源データ(RDATA)の目的
  - RRの表示フォーマット(ASCII表現)



RFC4034の構成(1.intro)

- DNSSECにて新たに導入された4つのRR {DNSKEY, RRSIG, NSEC, DS}についての定義
  - RRの目的
  - RRの資源データ(RDATA)の目的
  - RRの表示フォーマット(ASCII表現)

表示フォーマット

```
example.com. 86400 IN DNSKEY 256 3 5   ( AQPSKmynfzW4kyBv015MUG
                                         2DeIQ3Cbl+BBZH4b/0PY1kxkm
                                         vHjcZc8no kfzj31GajIQKY+5CptL
                                         r3buXA10h WqTkF7H6RfoRqXQe
                                         ogmMHfpftf6zMv1LyBUgia7za6
                                         ZEzOJBOztyvhjL742iU/TpPSEDhm
                                         2SNKLijfUppn1U aNvv4w== )
```

RFC4034の構成(1.intro)

- 章の構成
  - １．Introduction
  - ２．DNSKEYの定義
  - ３．RRSIGの定義
  - ４．NSECの定義
  - ５．DSの定義
  - ６．正規表現のルール
  - ７．IANAによるRFC変更の推移
  - ８．セキュリティについて

2.The DNSKEY RR

- DNSSECはRRsetの署名と認証に公開カギ暗号方式を使用します。

2.The DNSKEY RR

- DNSSECはRRsetの署名と認証に公開カギ暗号方式を使用します。

```
$TTL 86400
@           IN      SOA dns.example.jp. root.example.jp. (
                    2002122001 ; serial
                    3600       ; refresh 1hr
                    900        ; retry 15min
                    604800     ; expire 1w
                    86400      ; min 24hr
)
            IN      NS      dns-a.example.jp.
            IN      NS      dns-b.example.jp.
            IN      MX  10  mail-b.example.jp.
            IN      MX  10  mail-c.example.jp.

dns-b       IN      A       192.168.10.2
dns-b       IN      A       192.168.10.1
dns-b       IN      A       192.168.10.11
www         IN      A       192.168.10.3
```

ゾーンの中の
同じ署名者で
同じRRの集まり
||
RRset

2.The DNSKEY RR

- DNSSECはRRsetの署名と認証に公開カギ暗号方式を使用します。
- DNSKEY RRはRRsetの署名に使用した秘密鍵に対応する公開鍵を保存するRRです。
- このRRを公開鍵の保存以外に使用しないでください

2.The DNSKEY RR

- DNSKEY RRのタイプ値は48

2.The DNSKEY RR

- DNSKEY RRのタイプ値は48

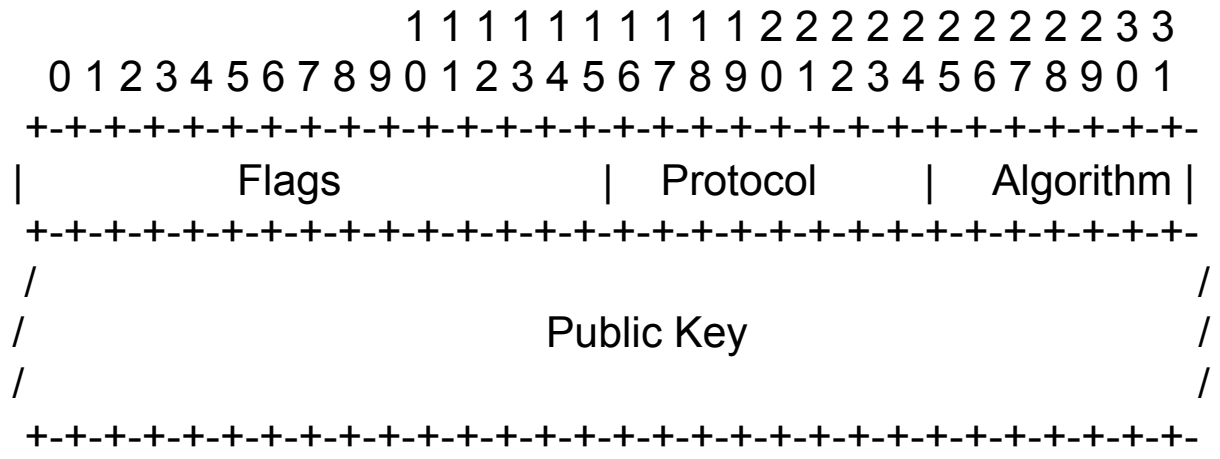
egistry:

TYPE	Value and meaning	Reference
A	1 a host address	[RFC1035]
NS	2 an authoritative name server	[RFC1035]
MD	3 a mail destination (Obsolete - use MX)	[RFC1035]
MF	4 a mail forwarder (Obsolete - use MX)	[RFC1035]
CNAME	5 the canonical name for an alias	[RFC1035]
SOA	6 marks the start of a zone of authority	[RFC1035]
MB	7 a mailbox domain name (EXPERIMENTAL)	[RFC1035]
MG	8 a mail group member (EXPERIMENTAL)	[RFC1035]
MR	9 a mail rename domain name (EXPERIMENTAL)	[RFC1035]
NULL	10 a null RR (EXPERIMENTAL)	[RFC1035]
WKS	11 a well known service description	[RFC1035]
PTR	12 a domain name pointer	[RFC1035]
HINFO	13 host information	[RFC1035]
MINFO	14 mailbox or mail list information	[RFC1035]
MX	15 mail exchange	[RFC1035]
TXT	16 text strings	[RFC1035]
.		
.		
.		
DS	43 Delegation Signer	[RFC4034][RFC3658]
SSHFP	44 SSH Key Fingerprint	[RFC4255]
IPSECKEY	45 IPSECKEY	[RFC4025]
RRSIG	46 RRSIG	[RFC4034][RFC3755]
NSEC	47 NSEC	[RFC4034][RFC3755]
DNSKEY	48 DNSKEY	[RFC4034][RFC3755]
DHCID	49 DHCID	[RFC4701]
NSEC3	50 NSEC3	[RFC5155]

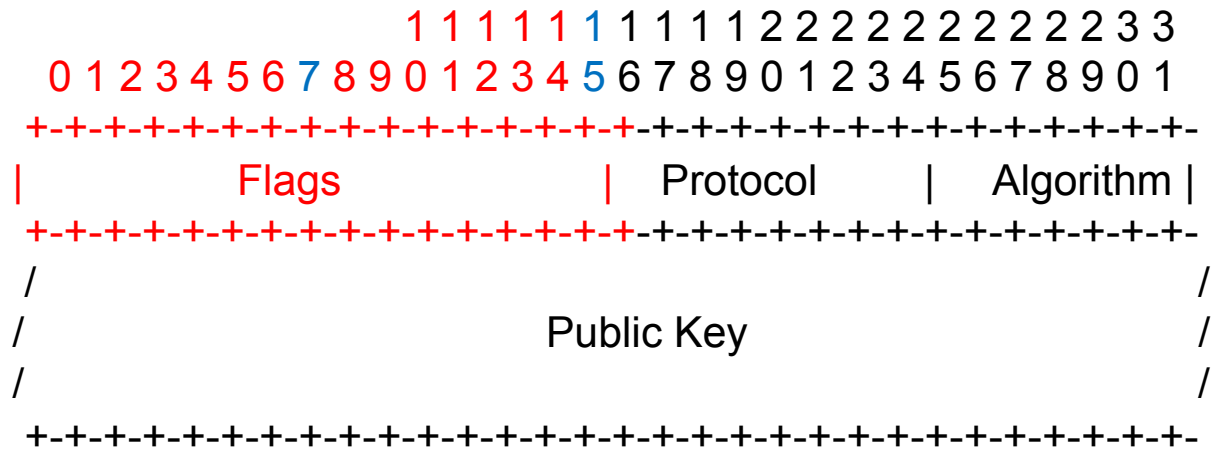
2.The DNSKEY RR

- DNSKEY RRのタイプ値は４８
- DNSKEY RRはクラス（ex. IN)に依存しません
- DNSKEY RRは特別なTTLを持っていません

2.1 DNSKEY RDATA Wire Format

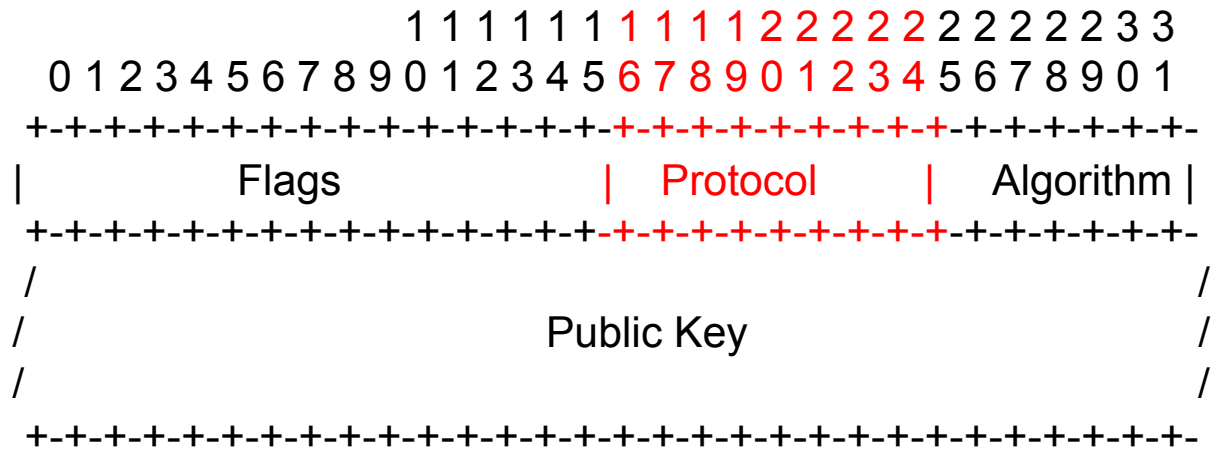


2.1.1 The Flags Field



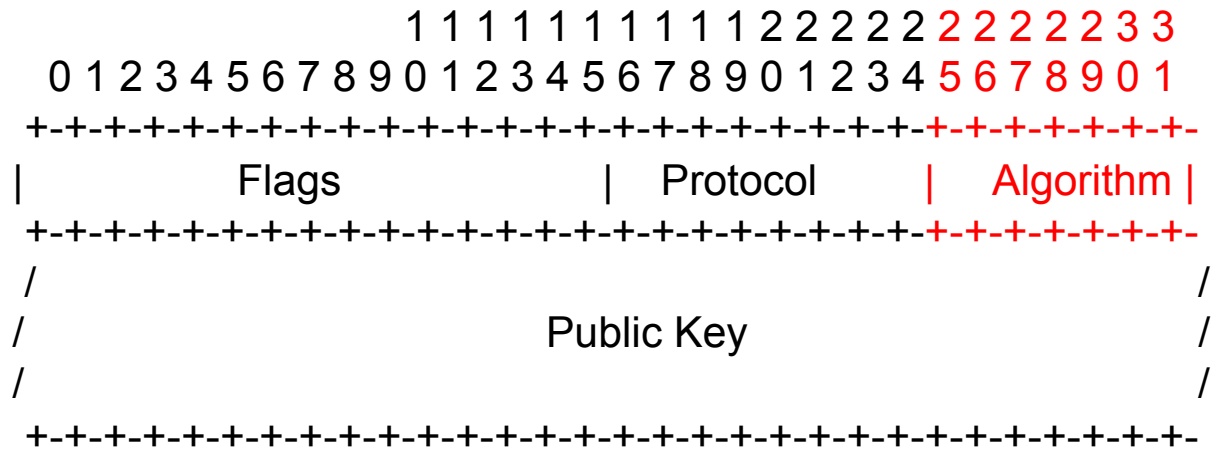
- ビット7の値が1(256)ならDNSSECの公開鍵が格納されています
- ビット15の値が1(257)ならSEPとして使用されます
  - 実際の運用ではビット7が立っていればZSKが格納されています
    ビット15が立っていればKSKが格納されています
- ビット0～6，8～14は予約です。

2.1.2 The Protocol Field



- プロトコルフィールドは3です。
- 3以外であれば不正データとして、エラー処理をしなければなりません。

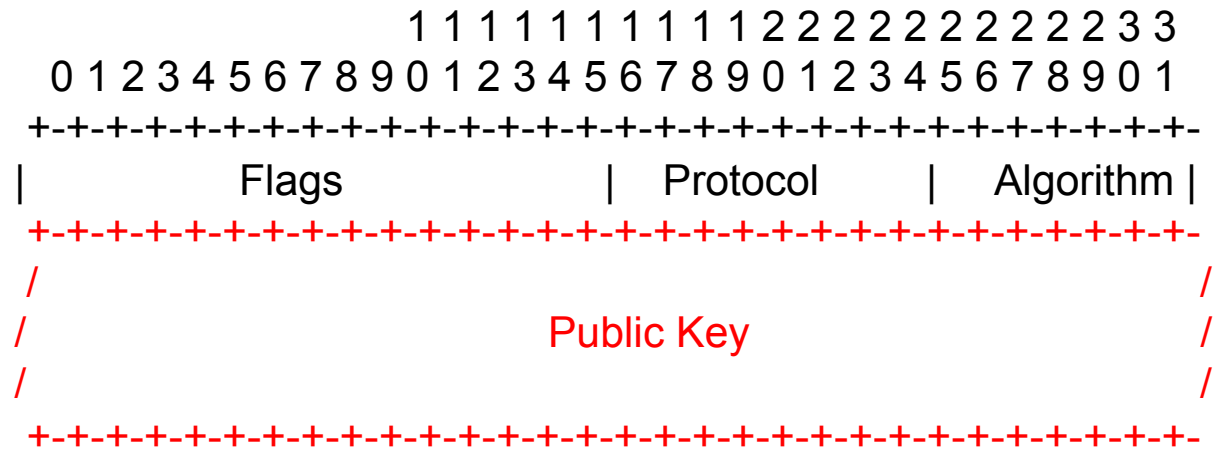
2.1.3. The Algorithm Field



- 公開鍵暗号のアルゴリズムを定義します。（付録A.1参照）

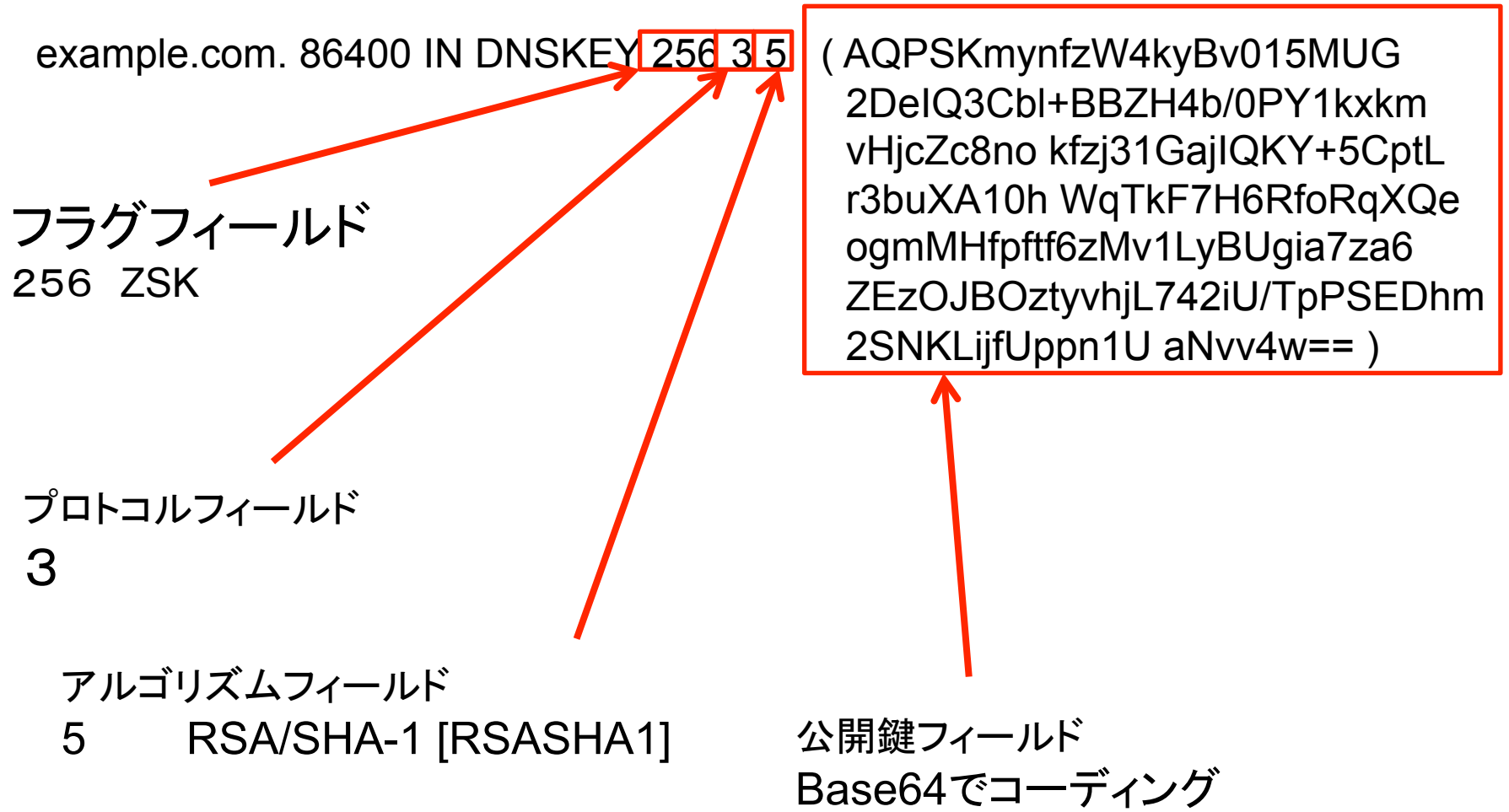
Value	Algorithm [Mnemonic]	Zone Signing	References	Status
0	reserved			
1	RSA/MD5 [RSAMD5]	n	[RFC2537]	NOT RECOMMENDED
2	Diffie-Hellman [DH]	n	[RFC2539]	
3	DSA/SHA-1 [DSA]	y	[RFC2536]	OPTIONAL
4	Elliptic Curve [ECC]			
5	RSA/SHA-1 [RSASHA1]	y	[RFC3110]	MANDATORY

2.1.4. The Public Key Field



- 公開鍵を格納します

2.2. The DNSKEY RR Presentation Format



3. The RRSIG RR

- RRSIG RRはRRsetに対して施されたデジタル署名を格納するRRです。

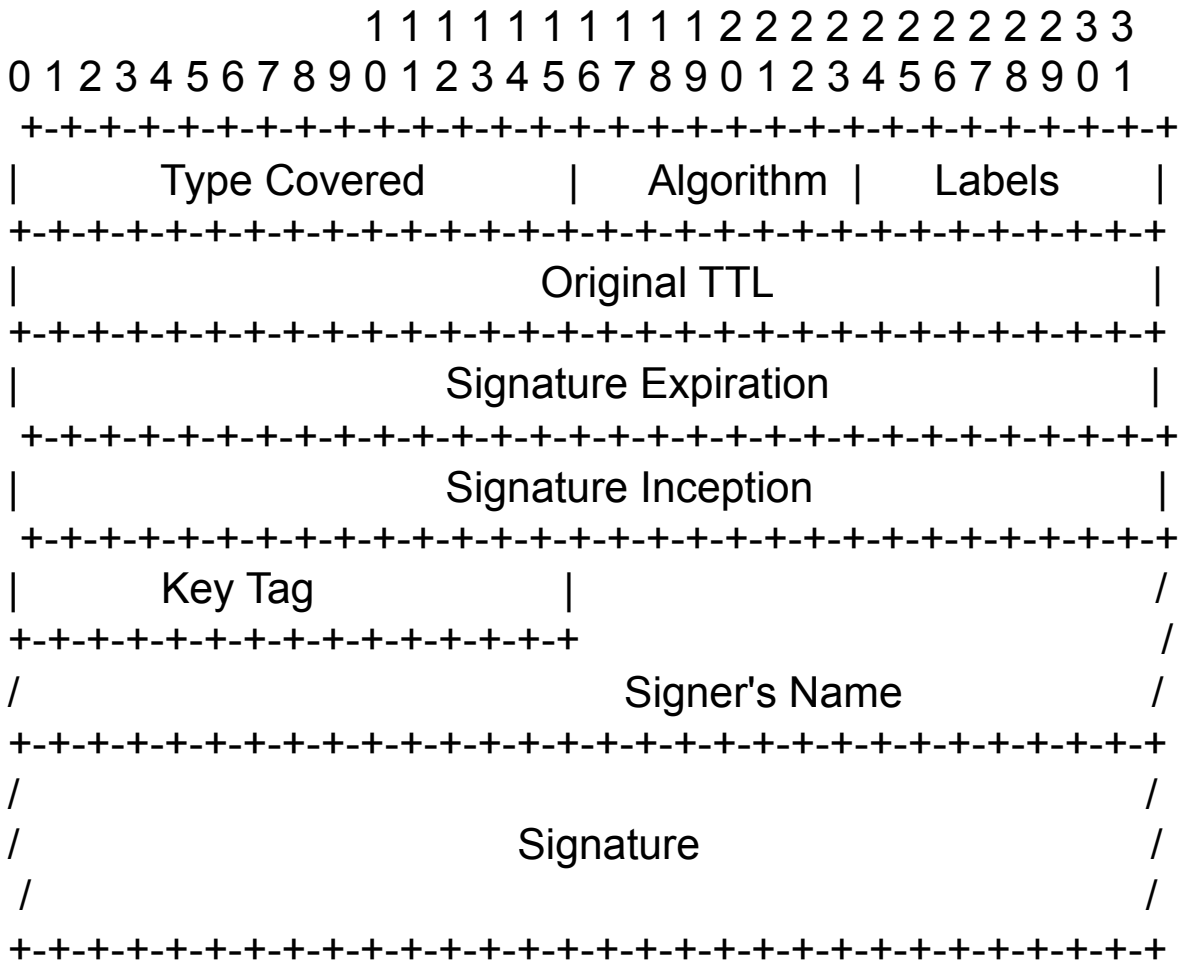
- それ以外には使用しないでください

- 全てのRRsetは署名によって守られている必要があるので、本来別のRRに利用されてはいけないCNAMEに対しても署名します。
これにより[RFC1034]で規定されているCNAMEに関する仕様が変更されています。

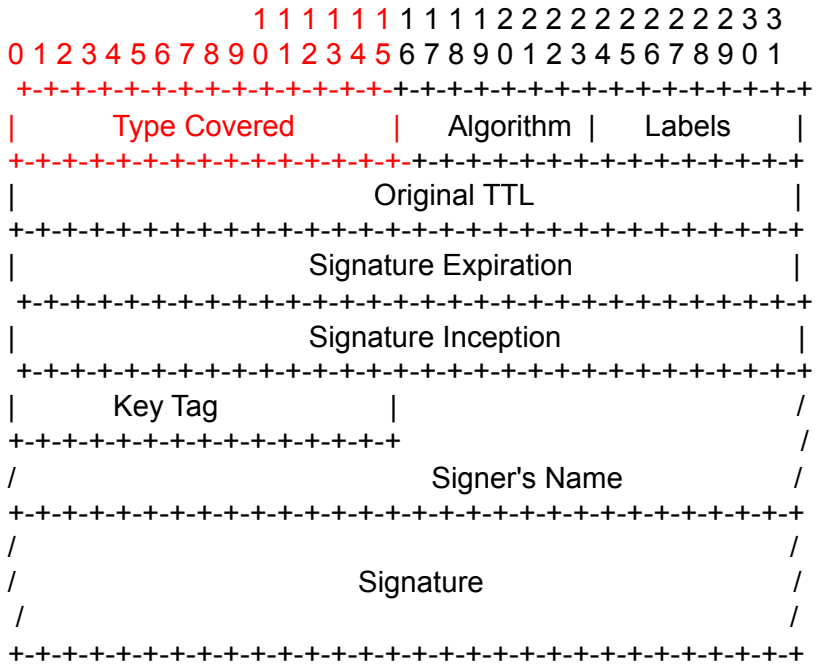
3. The RRSIG RR

- RRSIG RRのタイプ値は４６
- RRSIG RRはクラス（ex. IN)に依存しません
- RRSIG RRのTTLは必ず署名したRRsetのTTLと同じになります。

3.1. RRSIG RDATA Wire Format

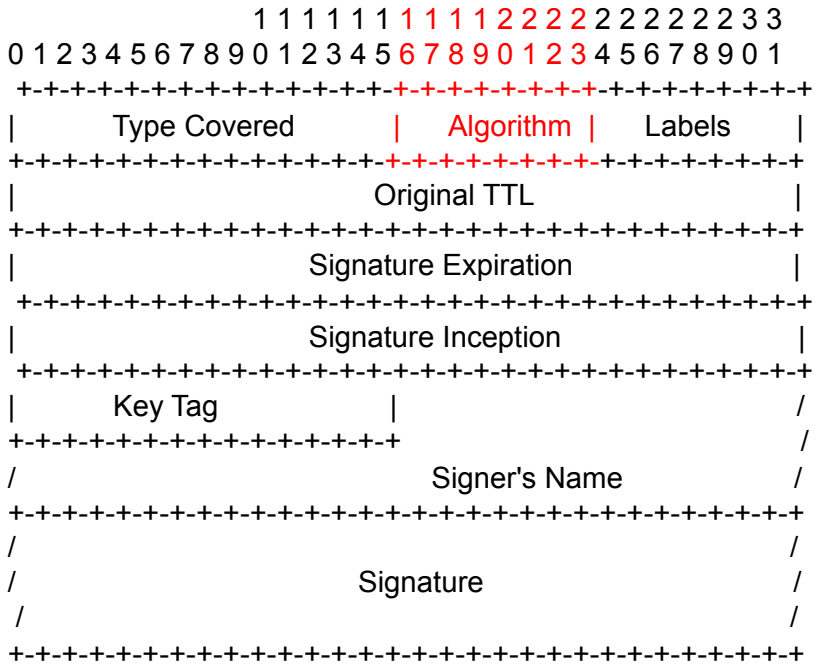


3.1.1. The Type Covered Field



- 署名されたRRの種類を識別します。（A,MX,NS・・・）

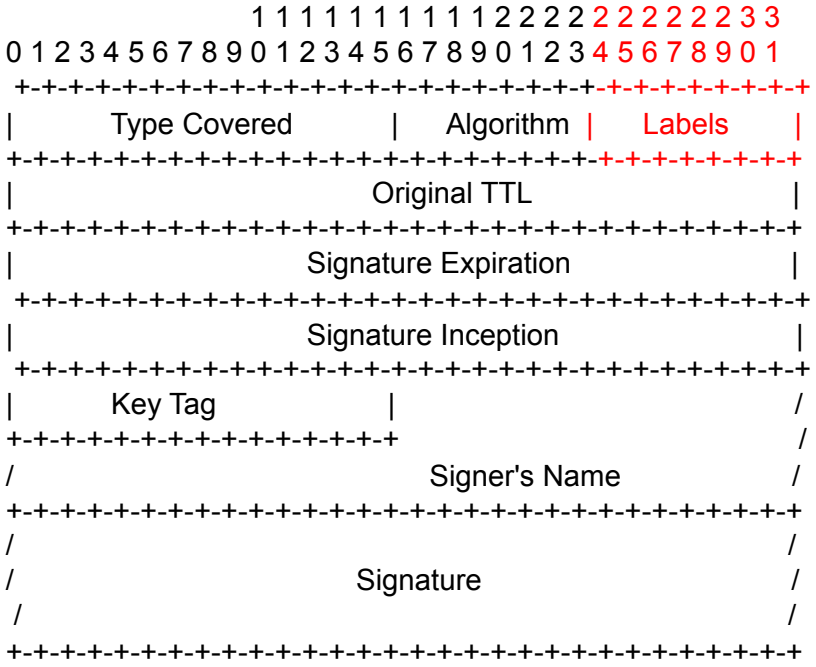
3.1.2. The Algorithm Number Field



- 公開鍵暗号のアルゴリズムを定義します。（付録A.1参照）

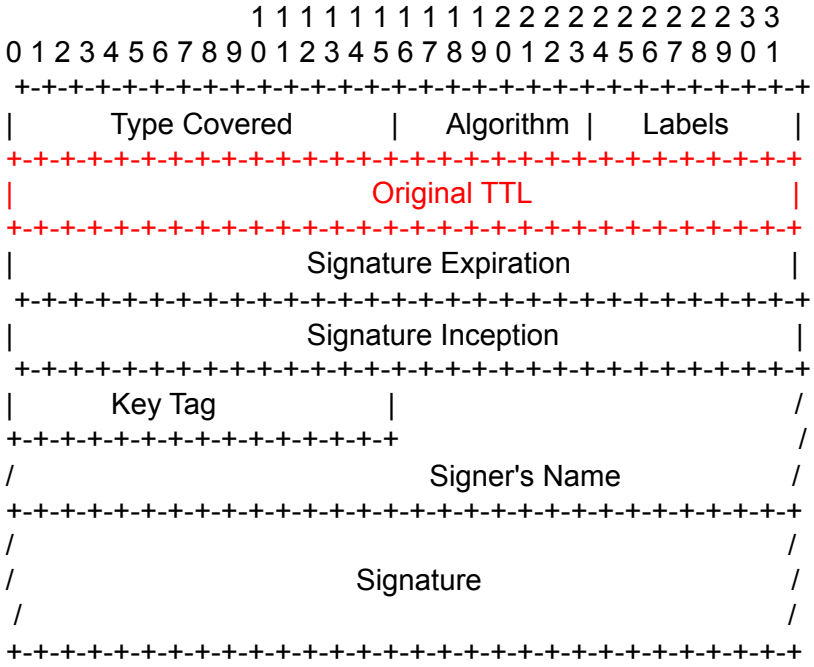
Value	Algorithm [Mnemonic]	Zone Signing	References	Status
0	reserved			
1	RSA/MD5 [RSAMD5]	n	[RFC2537]	NOT RECOMMENDED
2	Diffie-Hellman [DH]	n	[RFC2539]	
3	DSA/SHA-1 [DSA]	y	[RFC2536]	OPTIONAL
4	Elliptic Curve [ECC]			
5	RSA/SHA-1 [RSASHA1]	y	[RFC3110]	MANDATORY

3.1.3. The Labels Field



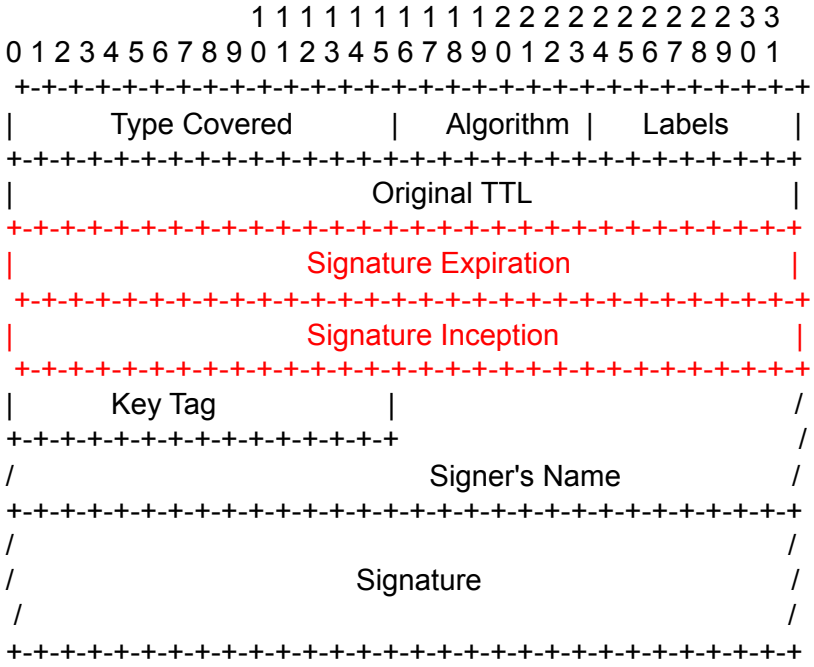
- 署名に使用されたowner(ゾーン名等）のラベル数を指定します。
  - host.example.jp = 3　　* . example.jp = 2　　ルートラベル = 0
- 検証するために元のowner名が必要だが、*を含んでいると回答処理で
  * .example.jp が host.example.jpに拡張されたかもしれない。
  その場合host.example.jp　label=2 となっており、* .example.jpが元ownerだと判別できます。

3.1.4. Original TTL Field

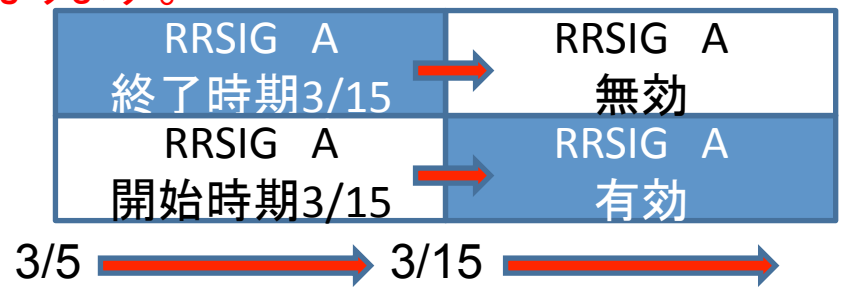


- 署名されたRRsetの元のTTLを指定します。
- 検証するには元のTTLが必要です。キャッシュリゾルバのTTLは常に減少していくので、使えません。

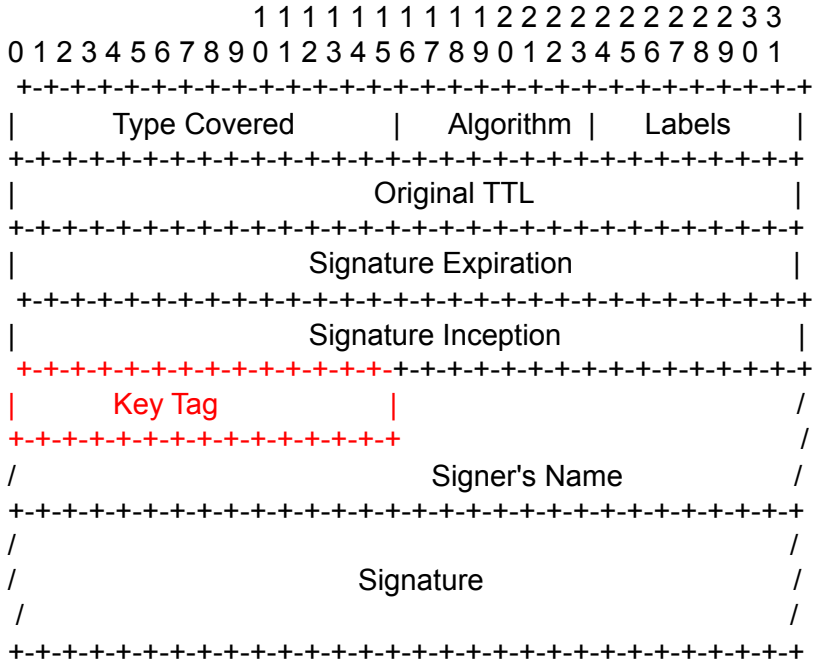
3.1.5. Signature Expiration and Inception Fields



- 署名の開始時間と終了時間を指定することで有効期間を示しています。
- 開始時間を指定できるということは、複数のRRSIG RRが共存することが可能になります。

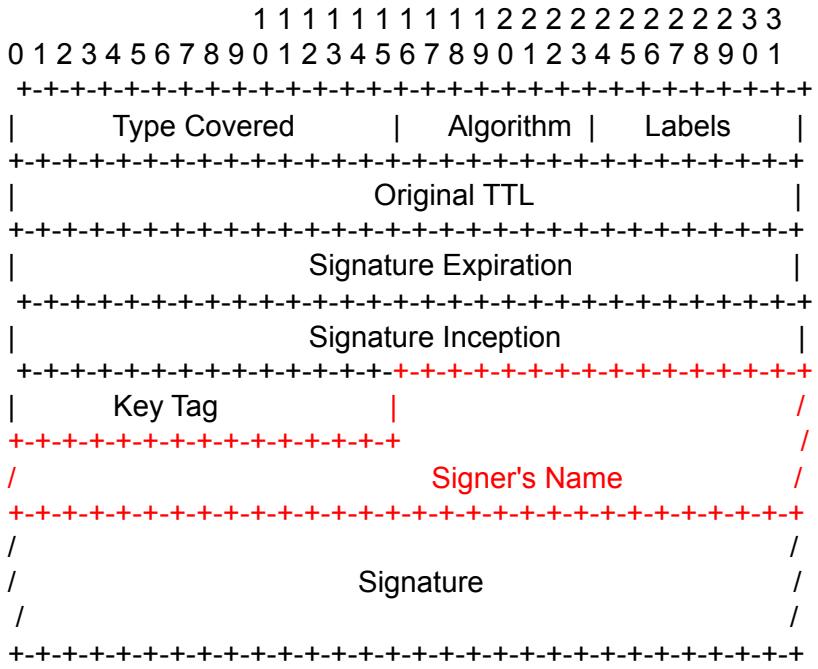


3.1.6. The Key Tag Field



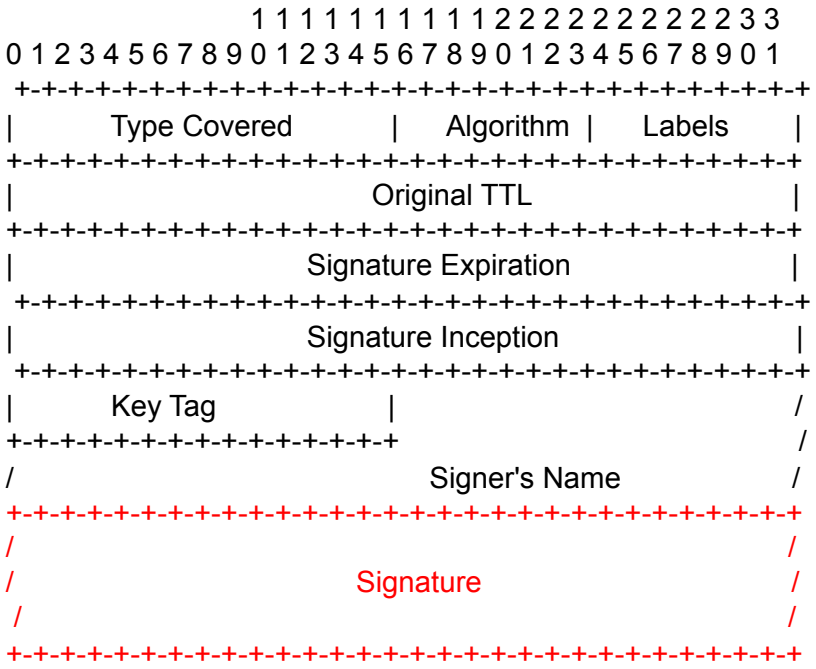
- 署名に使用された鍵の番号を鍵タグと呼びます
- Key tag fieldは鍵タグを含んでいます。
- DNSKEYを複数見つけた場合、どのDNSKEYで検証すればいいのかを示しています。
- 鍵タグの作り方は付録Bを参考

3.1.7. The Signer's Name Field



- この署名に使用するDNSKEY RRの所有者名を指定します。
  - 所有者名は署名されているRRsetのゾーン名を含んでいる必要があります。
  - このフィールドの所有者名は省略することはできません。

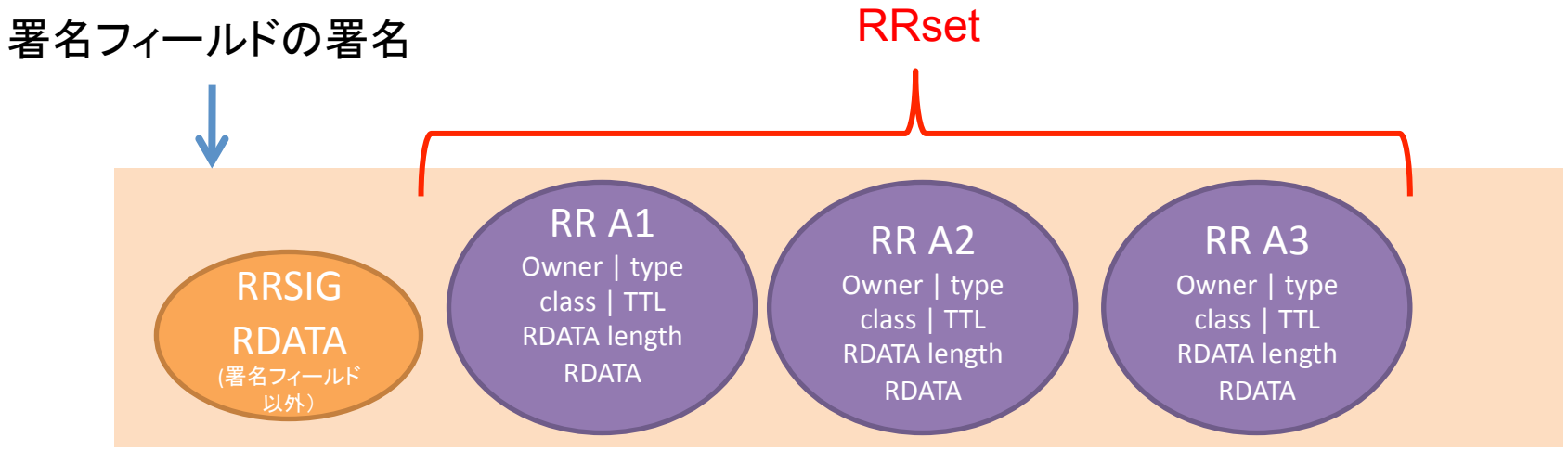
3.1.8. The Signature Field



- 署名を格納する署名フィールドです。
- 署名はRRSIG RDATAの署名フィールドを除いた部分と署名されたRRsetが含まれています。

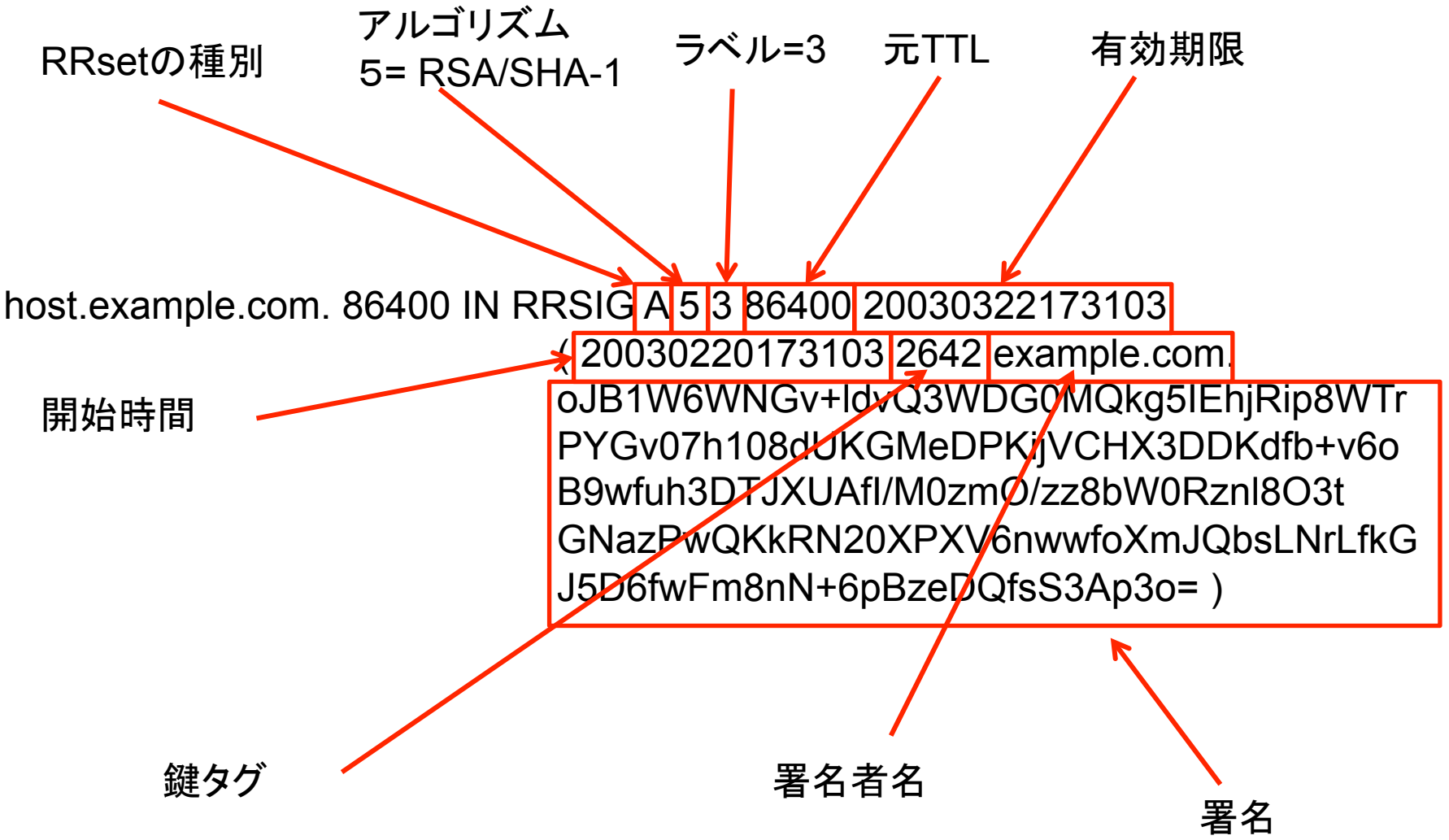
3.1.8.1. Signature Calculation

- 署名の計算は下記のように行われます。



- RRの数が多くなればなるほど、署名にかかる計算は増えます。
- Ownerは省略されず正規表現での完全所有者名になります。
- RRsetの所有者名はRRSIG RRの所有者名と同一でなければなりません。
- RRsetのクラスはRRSIG RRのクラスと同一でなければなりません。
- RRsetのRRはRRSIG のtype cover fieldと同一でなければなりません。

3.2. The RRSIG RR Presentation Format



4. The NSEC Resource Record

- NSEC RRの中には下記の二つが記載されます。
  - 権威をもつ、もしくは委譲先NSレコードをもつ、次の所有者名（owner name)
    - aaa.example.jp　IN　A　192.168.0.1
    - bbb.example.jp　IN　A　192.168.0.2
  - NSEC RRの所有者(owner)の全RR type
    - aaa.example.jp　IN　A　192.168.0.1
      MX　192.168.0.2
      RRSIG A 5 3 86400 ・・・・・

4. The NSEC Resource Record

- 次の所有者名を表記していくので・・・
  - aaa.example.jp
  - bbb.example.jp
  - zzz.example.jp

ccc.example.jpは存在しないと証明できる。
不在証明といわれる所以

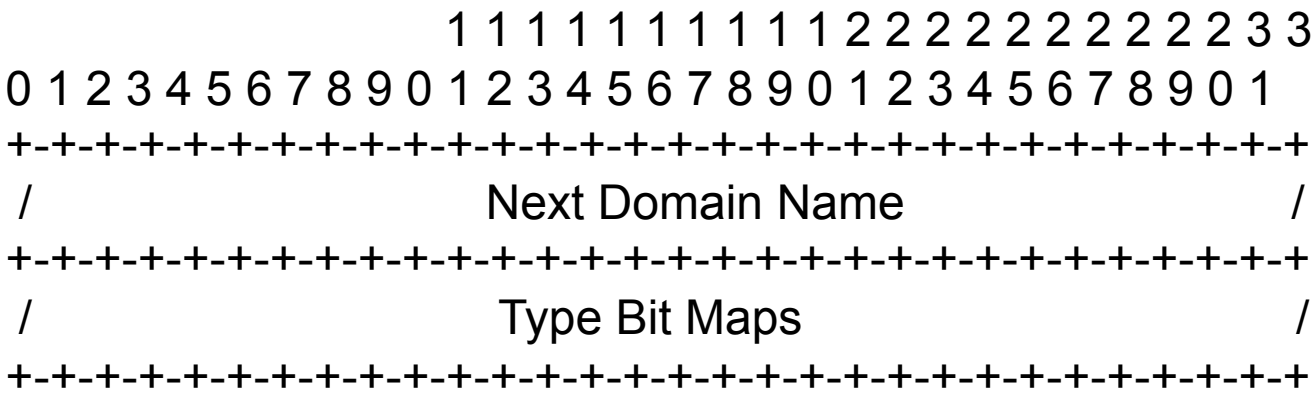
- 次の所有者名はCNAMEも含まれるため、本来別のRRに利用されてはいけないCNAMEに対してもNSECを付与します。
  これにより[RFC1034]で規定されているCNAMEに関する仕様が変更されています。

- ゾーン署名者がどのNSEC RRをゾーンに含めなくてはならないのかは[RFC4035]を見てください

4. The NSEC Resource Record

- NSEC RRのタイプ値は47
- NSEC RRはクラス（ex. IN)に依存しません
- NSEC RRのTTLはSOAの最小TTLと同じになるべきです。
  これはネガティブキャッシュの考え方と同じです。

4.1. NSEC RDATA Wire Format



4.1.1. The Next Domain Name Field

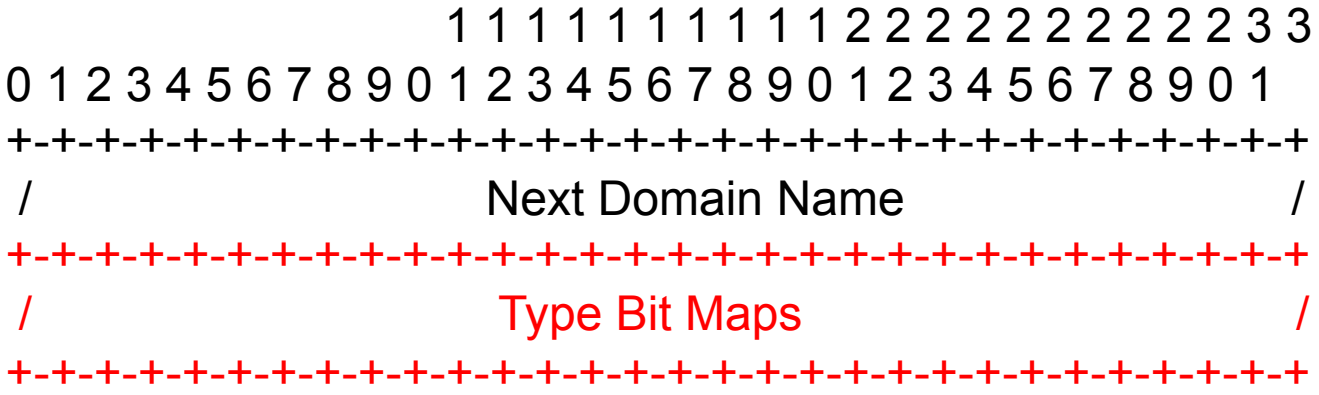
- 次の所有者名（owner name)については正規順序で指定します。
  正規順序については6.1章を参考

- ゾーン中、最後のNSEC RRは先頭のowner nameを指定します。これにより、最後であることを示します。

- このフィールドのowner nameは省略してはなりません。

- Next domain name にリストアップされるには、そのowner nameに最低でも一つ、権威をもつRRsetが必要になります。

4.1.2. The Type Bit Maps Field



- Owner name に存在するRRsetを識別し、全てを列挙します
- RRsetはビットマップで表記します。
- 注意点はNS RRに対してのNSECです
  - 権威をもっているowner nameのNS RRに対してはNSEC RRを作らなければなりません。
  - 権威をもっていない、単なるglue recordに対してはNSEC RRを付けてはいけません。

4.1.3. Inclusion of Wildcard Names in NSEC RDATA

*.example.jp

ワイルドカードは、文字として扱われます。
拡張はしません。

4.2. The NSEC RR Presentation Format

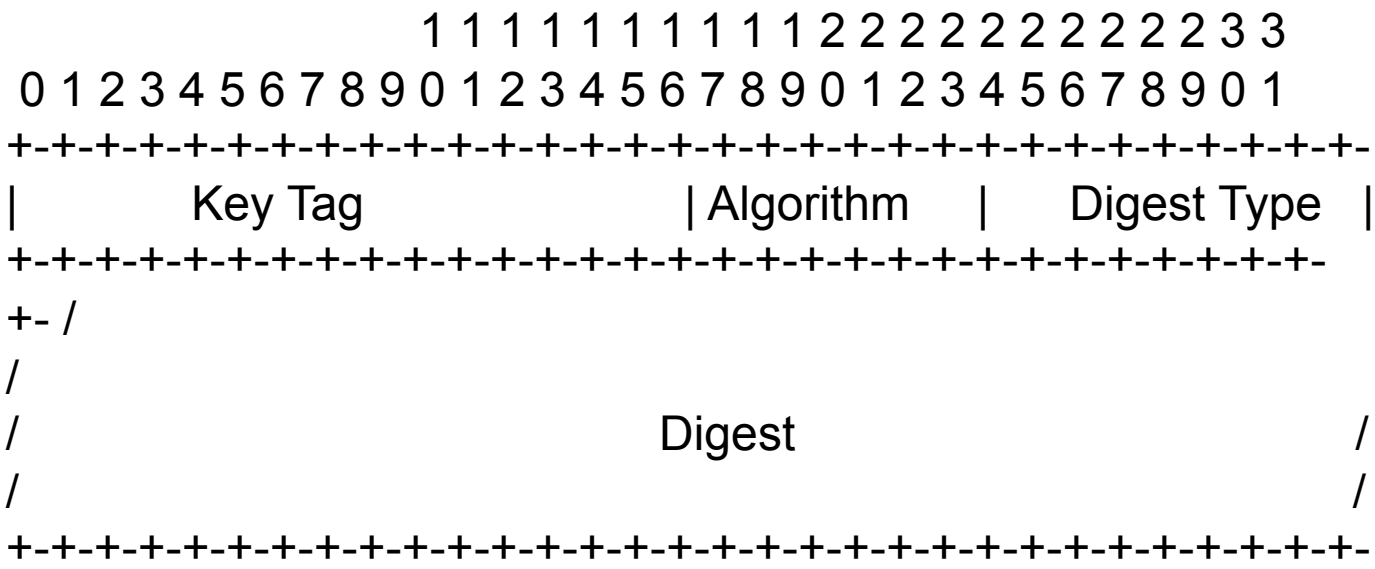
5. The DS Resource Record

- DS RRは鍵タグ・アルゴリズム・DNSKEY RRのハッシュ値を保存します
  - この段階ではZSK KSKの概念が存在しないので、単なるDNSKEYと言っているが、現在の運用ではKSKのDNSKEY RRである。
  - 鍵認証のプロセスは[RFC4035]で記述されます。
- DS RR は同じowner nameを持つが、保存場所は異なり、上位ゾーンのみに出現します。
  - プロセスは[RFC4035]で記述されます。

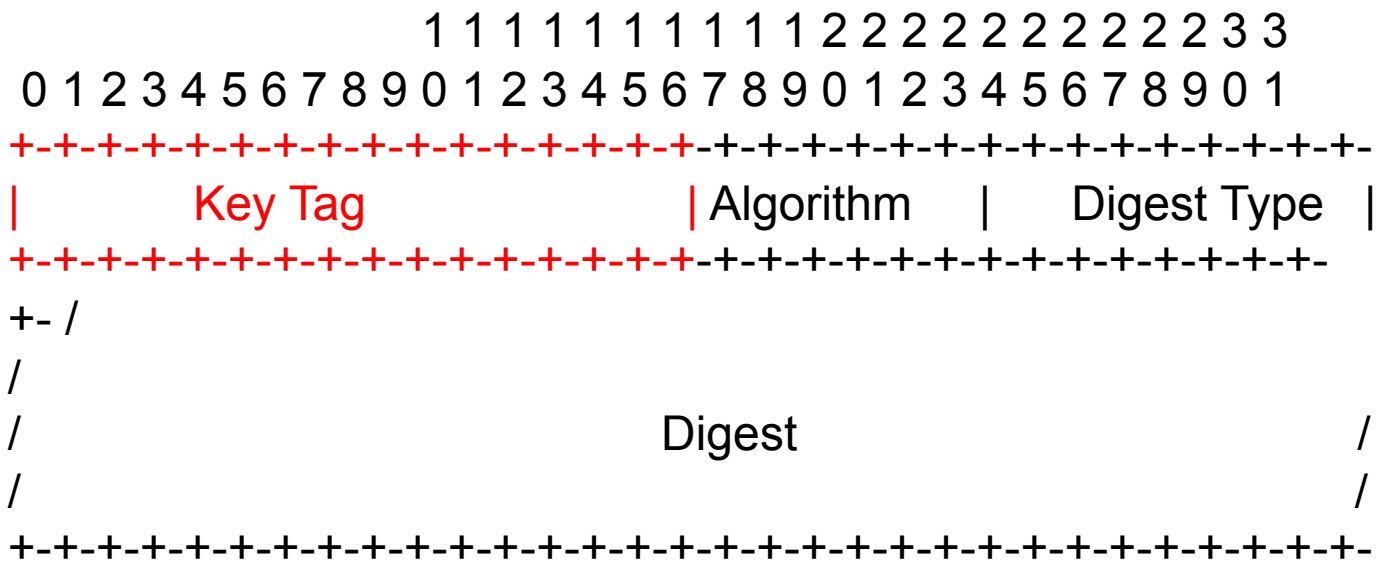
5. The DS Resource Record

- DS RRのタイプ値は43
- DS RRはクラス（ex. IN)に依存しません
- DS RRには特別なTTL条件がありません

5.1. DS RDATA Wire Format



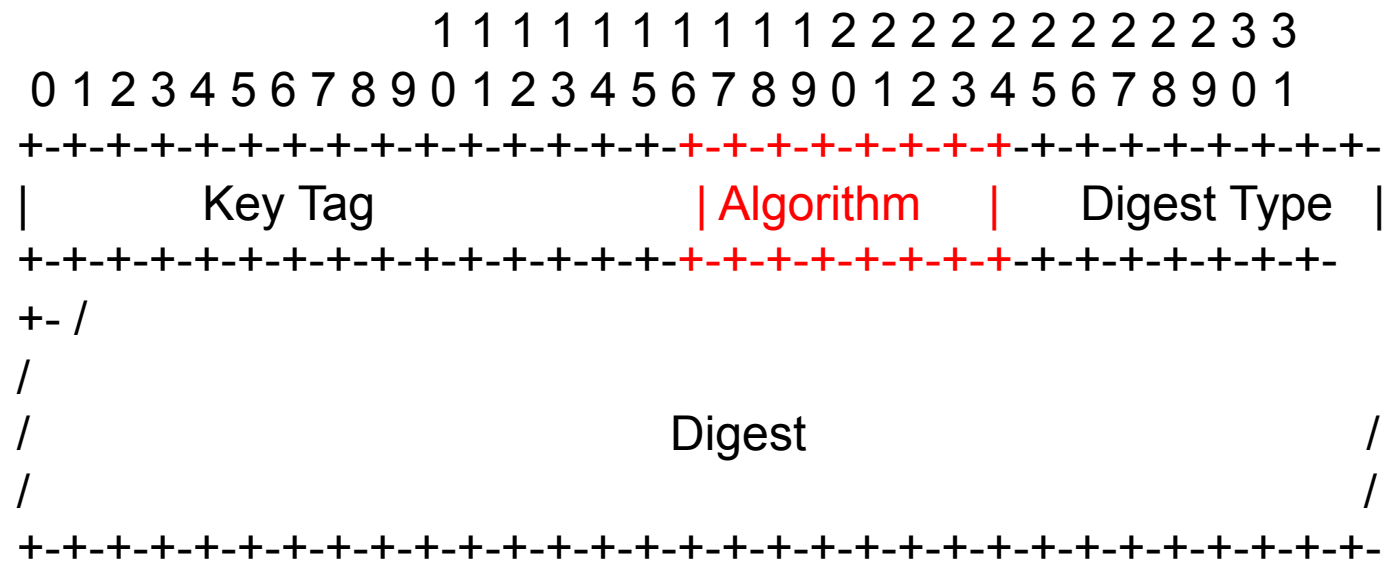
5.1.1. The Key Tag Field



- DNSKEY RRの鍵タグを指定します。

- 鍵タグはRRSIG RR の鍵タグと同一です。

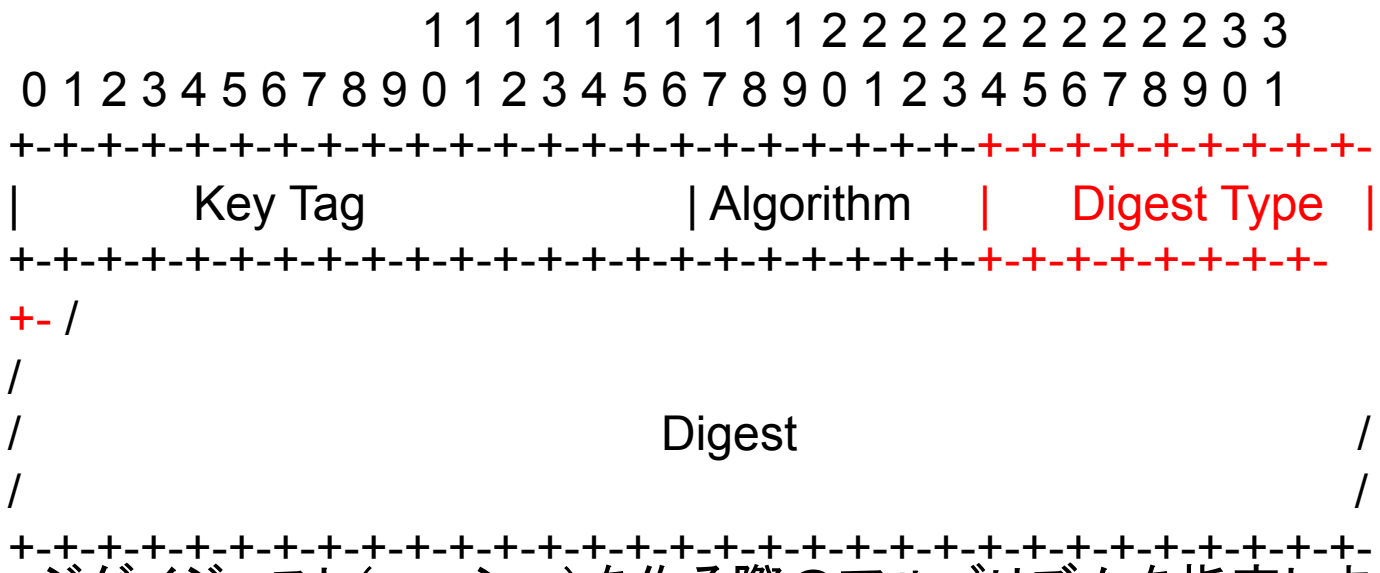
5.1.2. The Algorithm Field



- DNSKEY RRのアルゴリズムを指定します。

- アルゴリズムはRRSIG RR,DNSKEY RRのものと同一です。

5.1.3. The Digest Type Field



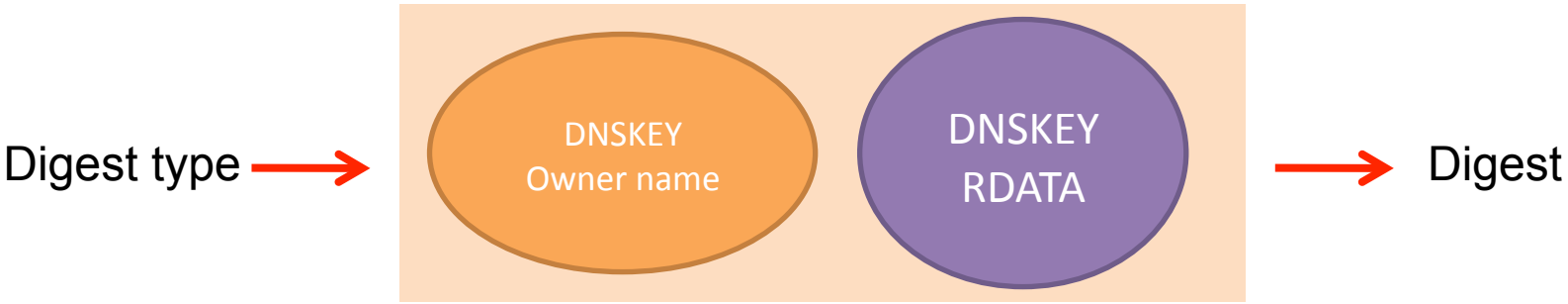
- メッセージダイジェスト（ハッシュ）を作る際のアルゴリズムを指定します。値は付録A.2を参照

VALUE	Algorithm	STATUS
0	Reserved	-
1	SHA-1	MANDATORY
2-255	Unassigned	-

5.1.4. The Digest Field

```
                            1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Key Tag              | Algorithm     |      Digest Type    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+- /
/
/                                   Digest                                      /
/                                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- DNSKEY RRのダイジェストを保存します

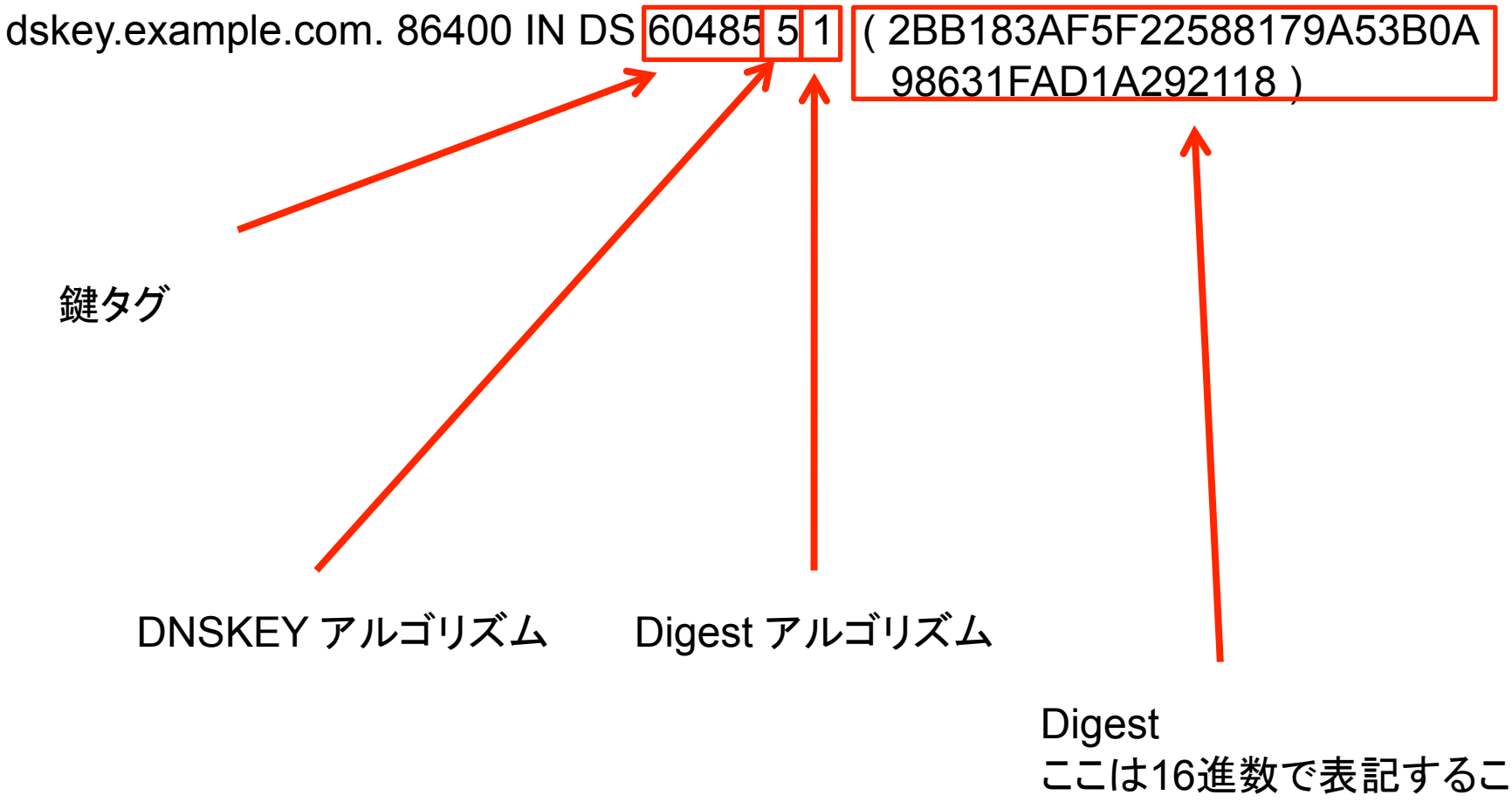


5.2. Processing of DS RRs When Validating Responses

- DS RRで指定されているDNSKEY RRはDNSSECの鍵でなくてはなりません。
  つまり、ビット7のフラグが立っている必要があります。

- もしビット7が立っていなければ、
  そのDNSKEY RRとDS RRは検証プロセスで使用されてはなりません。

5.3. The DS RR Presentation Format



6. Canonical Form and Order of Resource Records

- この章では下記を定義します
  - RRの正規表現
  - RRsetの正規順序
  - DNS名(owner name)の正規順序 for NSEC

6.1. Canonical DNS Name Order

- 所有者名は個別のラベルを、符号なし、左揃えのオクテット列と取り扱うことで順序づけられています。
- ASCII大文字はASCII小文字として扱います。
- 並べ替えは最上位ラベル(最右）から順番に行います。

example
a.example
yljkjljk.a.example
Z.a.example
zABC.a.EXAMPLE
z.example
\001.z.example
*.z.example
\200.z.example

6.2. Canonical RR Form

- ドメイン名を完全に拡張し、DNS名省略を行いません
- RRの大文字US-ASCIIは小文字に変換されます。
- RR typeがNS, MD, MF, CNAME, SOA, MB, MG, MR, PTR, HINFO, MINFO, MX, HINFO, RP, AFSDB, RT, SIG, PX, NXT, NAPTR, KX, SRV, DNAME, A6, RRSIG, or NSECであれば、RDATA内のUS-ASCII大文字は小文字に変換されます
- 「＊」ワイルドカードは拡張しません。
- RRのTTLは権威ゾーン、もしくはRRSIG のoriginal TTL fieldのTTLを設定します

6.3. Canonical RR Ordering within an RRset

- 同じ所有者名、クラス、typeのRRはRDATAを左揃え、符号なしのオクテット列として並べ替えます。

- [RFC2181]にてRRset内のRRは重複レコードを含めないと明示されている。
  通常であればプロトコルエラーの処理になるが、
  頑健性の一般原則（自分に厳しく、他人にやさしく）に従うなら、重複レコードを一つ残して他削除という処理をする

7. IANA Considerations

- 今までのプロトコルパラメータ変更の歴史を書いています。
- 興味がある方はご覧ください
- ただし、この後にも多々変更されていることに注意してください

8. Security Considerations

- このRFCは新しい4つのRRのフォーマットを記述するものであり、下記以外のセキュリティについては紹介しません。
  詳しくはRFC4033,4035
  - DS RRに登録するハッシュは破られる可能性があり、その強度はハッシュに変換するアルゴリズムに依存します。(SHA-1)

    しかし、DS RRのアルゴリズムと鍵タグとハッシュが一致する公開鍵をそこから作成するのは困難です。

  - 鍵タグは効率的にDNSKEY RRを探すために使われますが、DNSKEYが全く同じ鍵タグを持つことが可能です。
    そのため、鍵タグだけを使用する実装であれば、間違った更改鍵を選ぶ可能性があります。