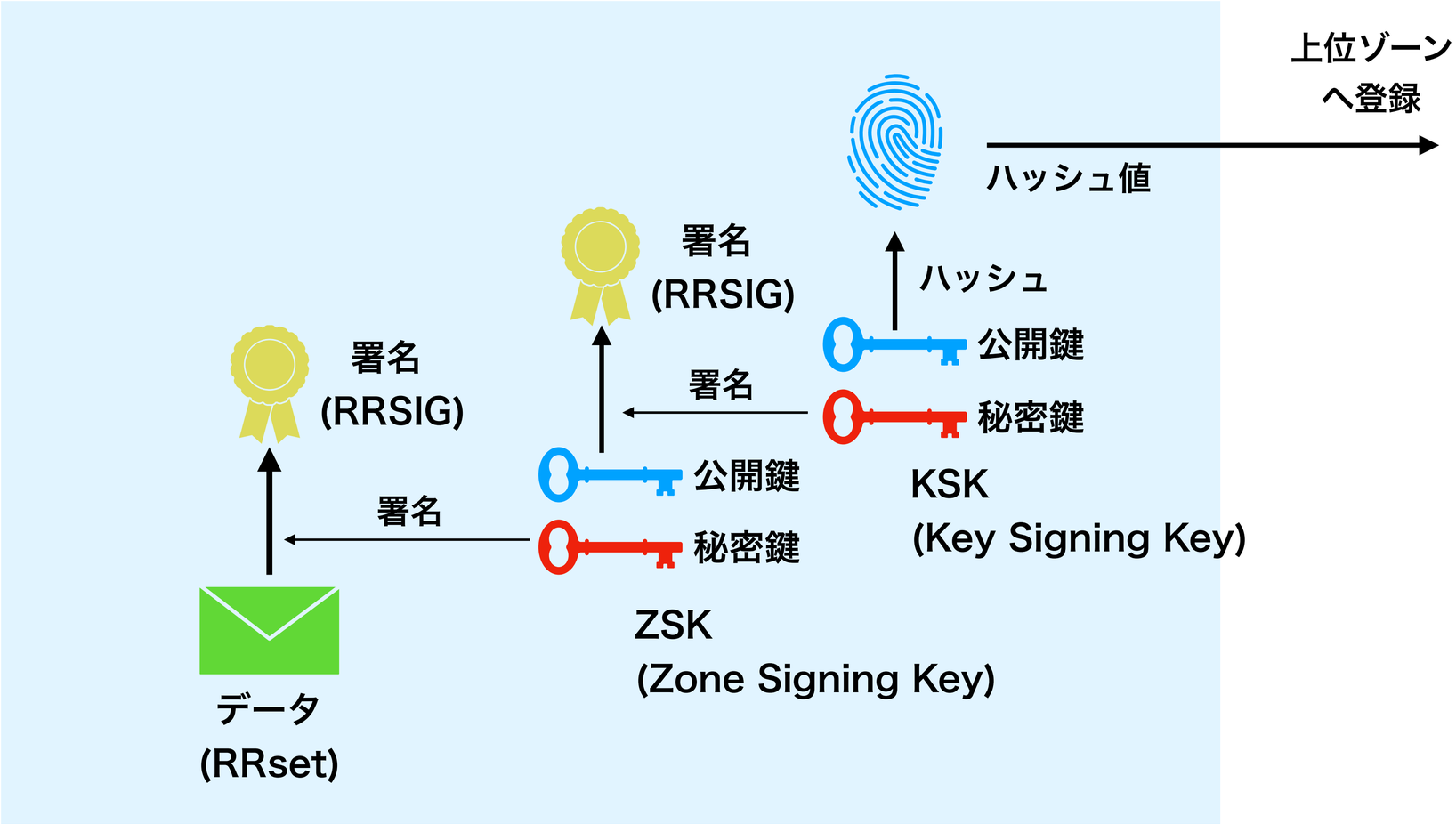
DNSSECの仕組みと KSKロールオーバへの対応

2017.9.5

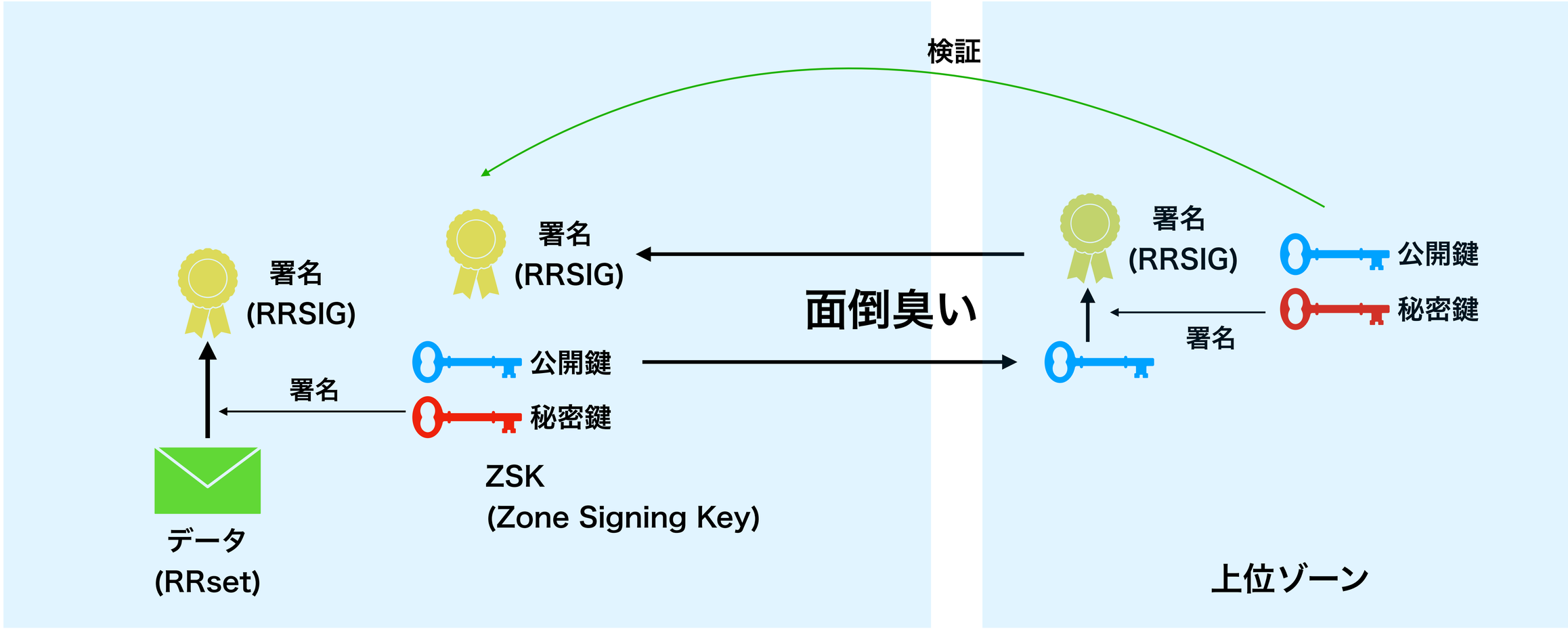
(9.17修正/9.29修正(新KSKによる署名延期))

(株) リフレクション
中京大学工学部
鈴木常彦 tss@e-ontap.com

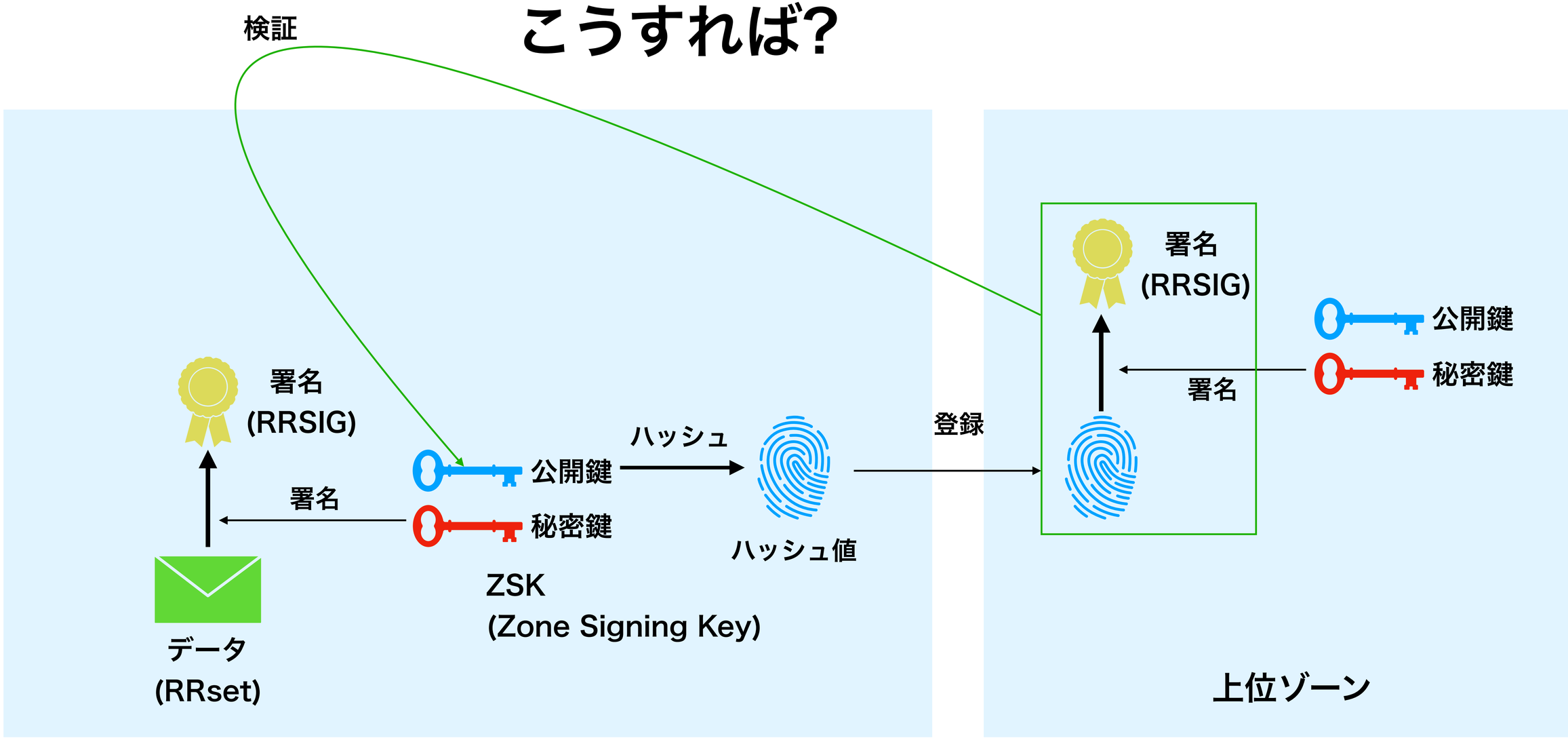
ゾーンデータの署名



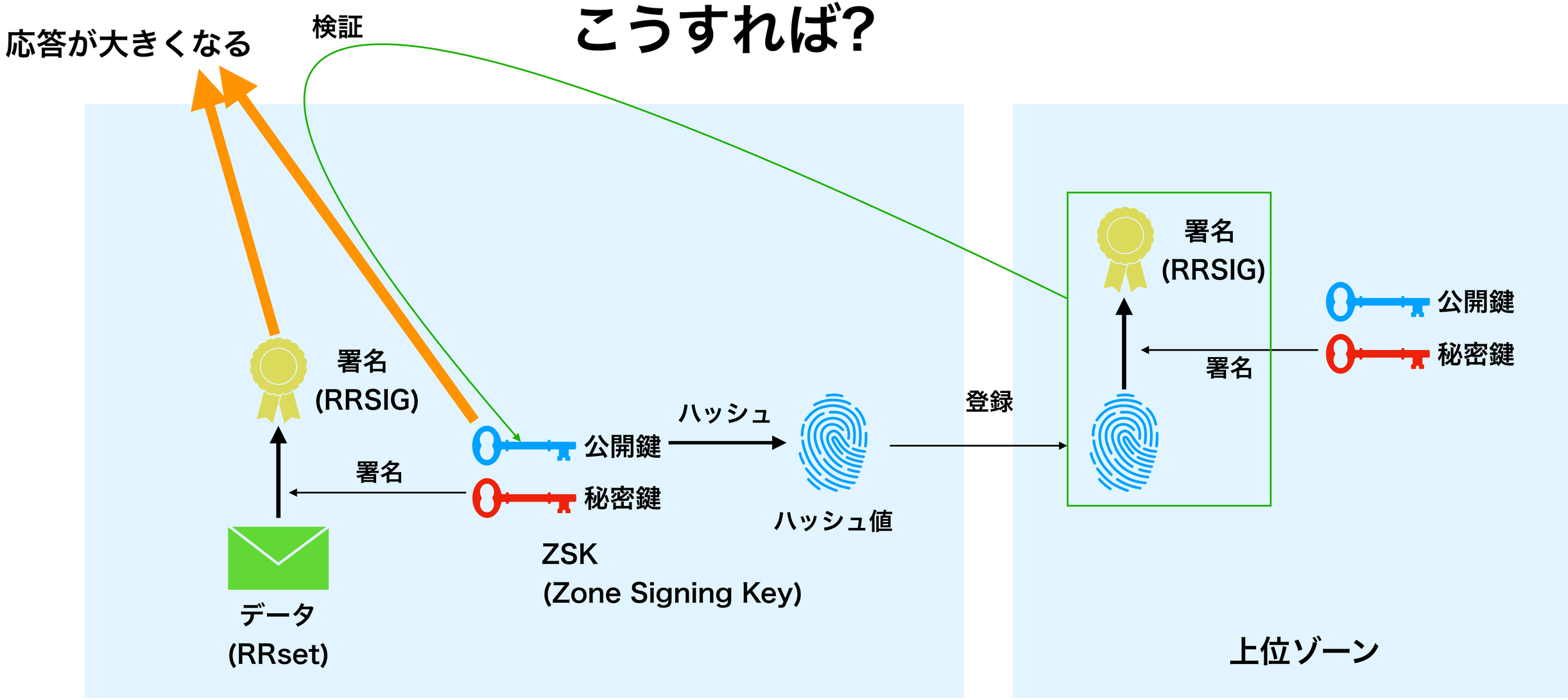
当初案



こうすれば?

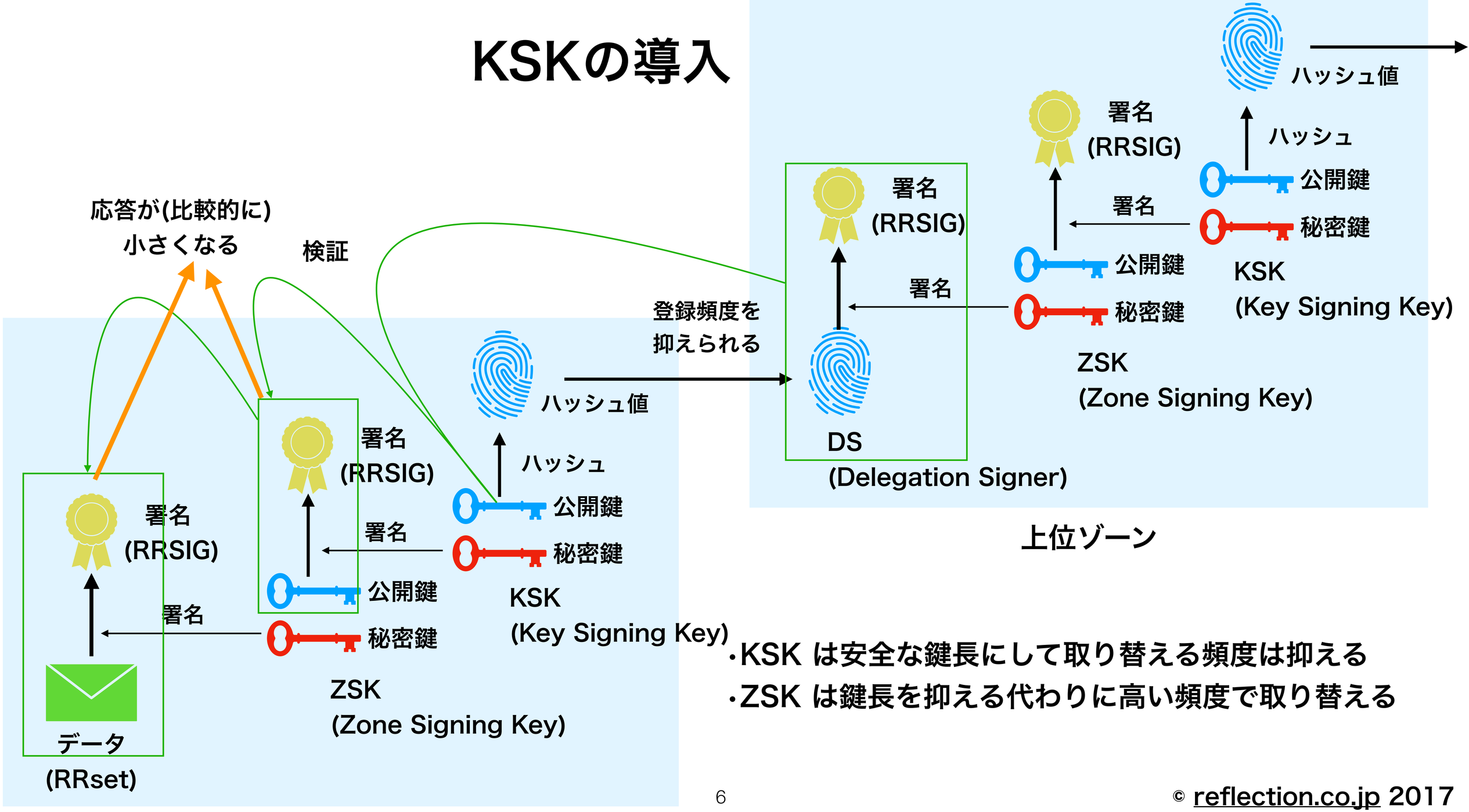


こうすれば?



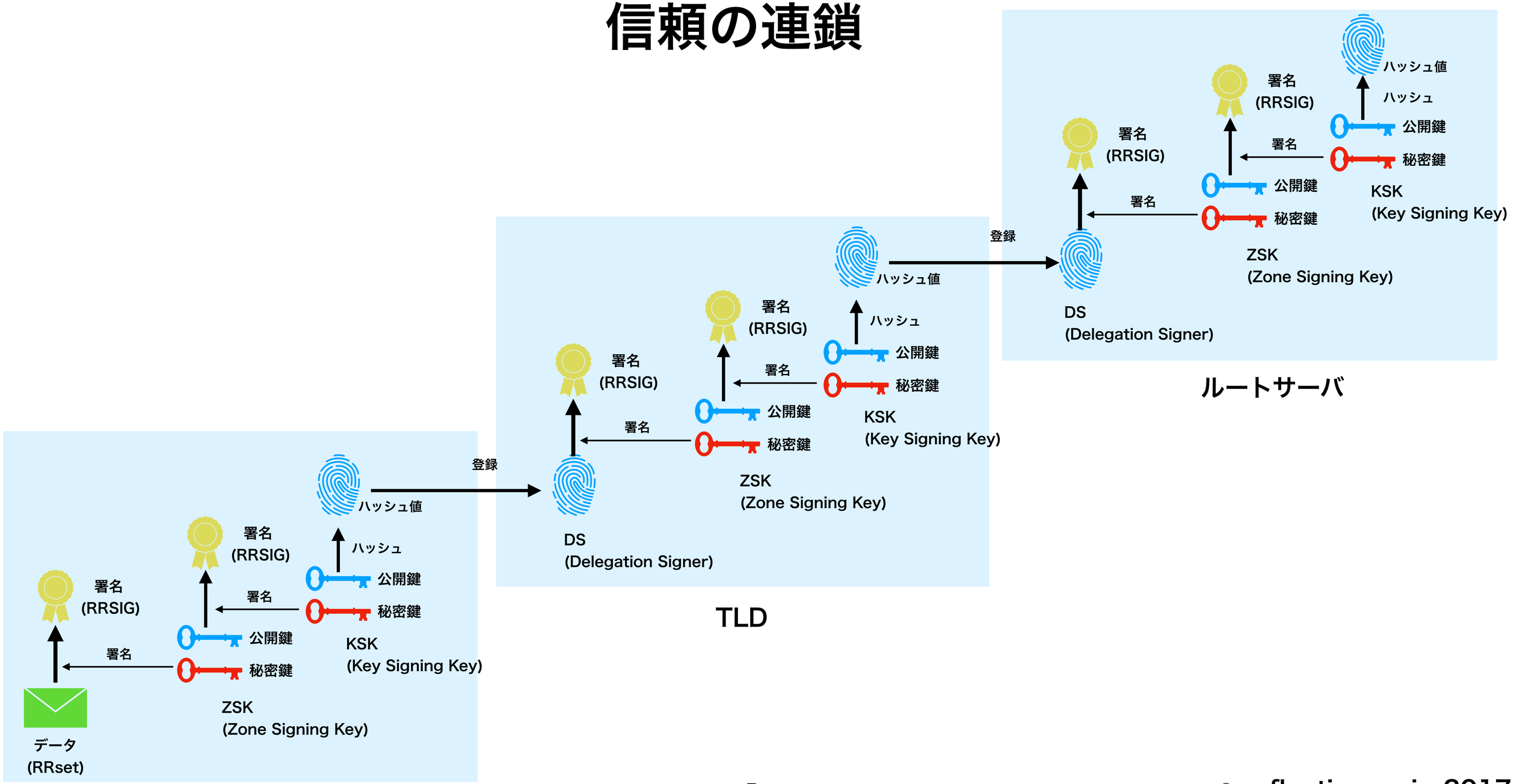
- 安全性の高い鍵 (ZSK) を使おうとすると鍵長も署名も (＝応答) が大きくなる
- 鍵長の小さい鍵 (ZSK) を使おうとすると安全性が低くなるので頻繁に鍵を交換したくなる
  →頻繁に登録して署名してもらうのが双方つらい

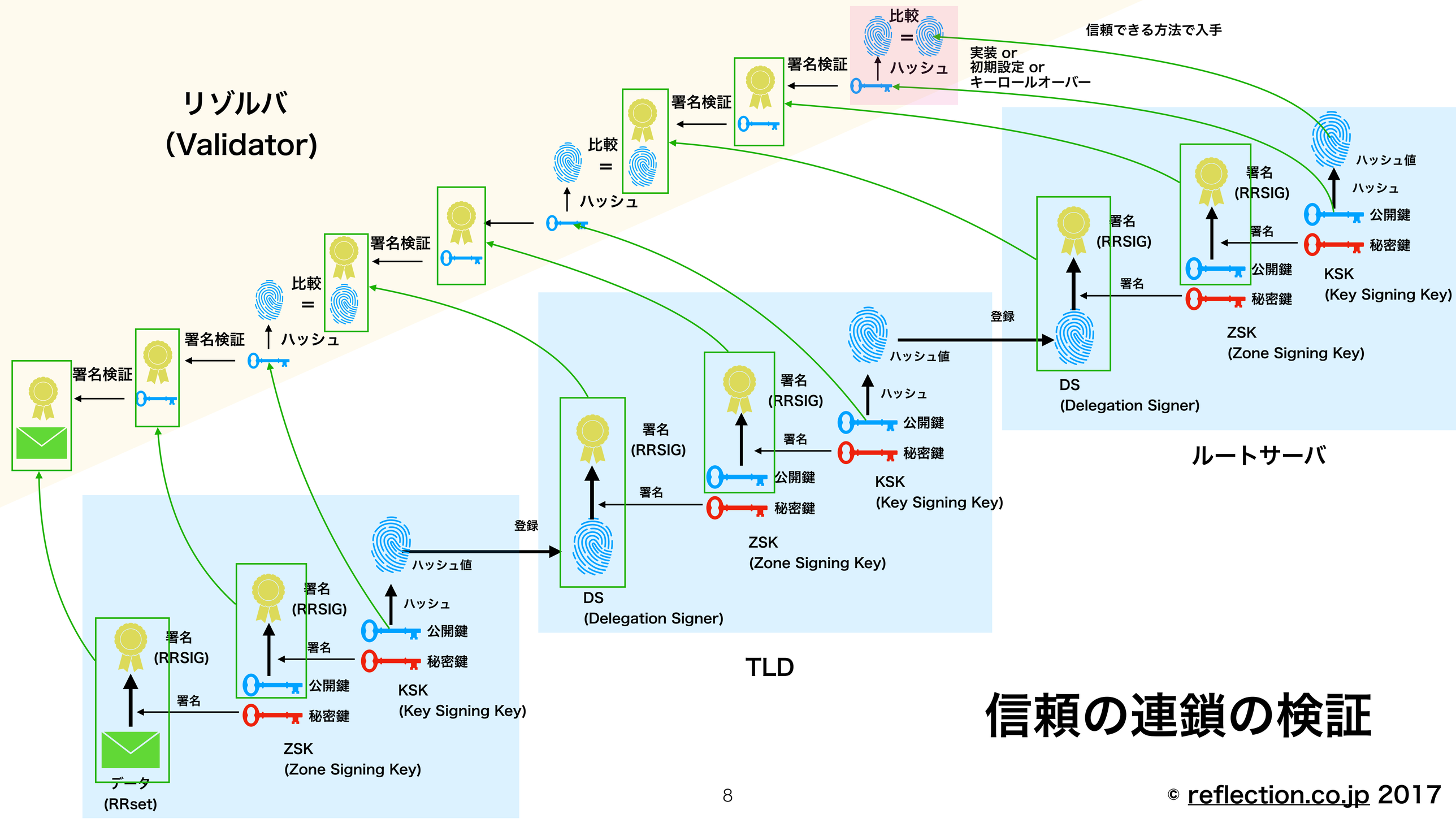
KSKの導入



- KSK は安全な鍵長にして取り替える頻度は抑える
- ZSK は鍵長を抑える代わりに高い頻度で取り替える

信頼の連鎖





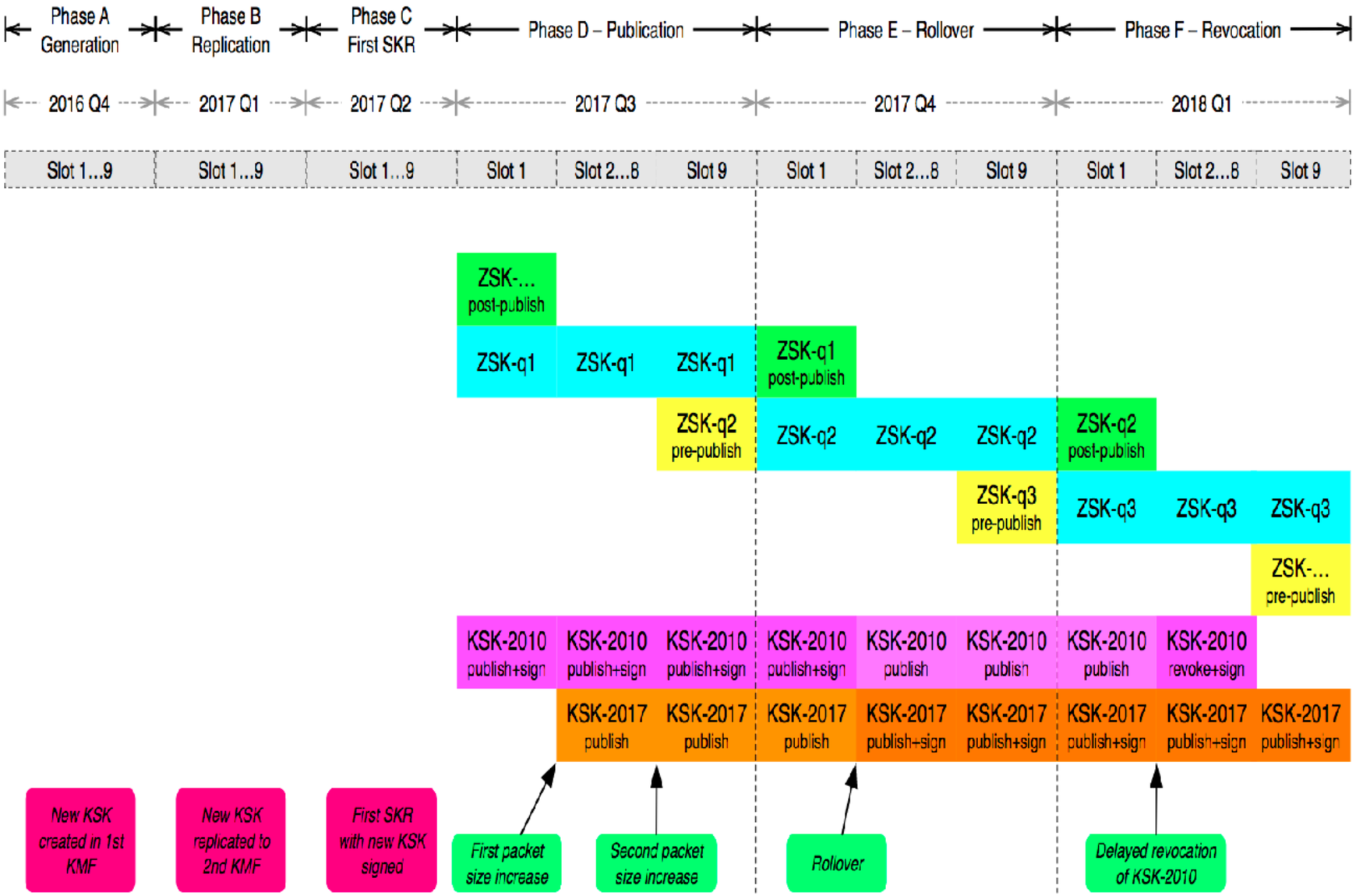
信頼の連鎖の検証

KSKキーロールオーバー

ドラフトタイムライン

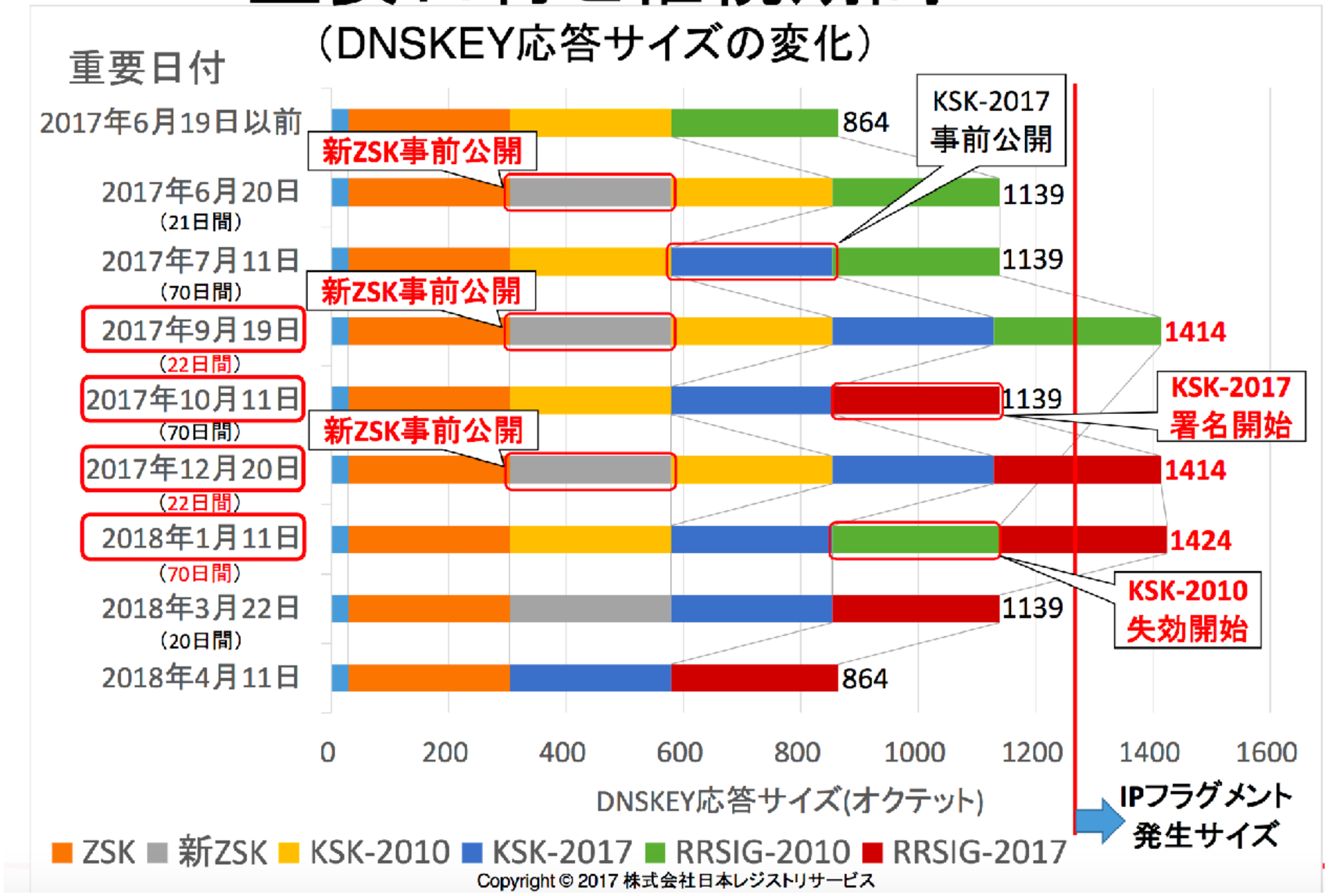
- 2016年10月27日: 新しいKSKが生成され、KSKロールオーバープロセスが開始
- 2017年7月11日:DNSで新しいKSKを公開
- 2017年9月19日:ルートネームサーバーからのDNSKEYレスポンスの規模を増大。(注: 新ZSK公開による)
  (日本時間では 23:00 頃)
- 2017年10月11日:新しいKSKによるルートゾーン鍵セットの署名開始（実際のロールオーバーイベント）
  (日本時間では12日AM 1:00 頃) … 9/29 追記: 延期決定　　9/19 よりこちらを心配するべき
- 2018年1月11日:古いKSKの失効
- 2018年3月22日:古いKSKがルートゾーンに表示される最終日
- 2018年8月: 古い鍵を、両方のICANN鍵管理ファシリティから削除

https://www.icann.org/resources/pages/ksk-rollover-2017-05-31-ja#timeline より



ICANN “2017年KSKロールオーバーの運用実施計画” より
(https://www.icann.org/en/system/files/files/ksk-rollover-operational-implementation-plan-22jul16-en.pdf)

重要日付と継続期間



JPRS “ルートゾーンのKSKロールオーバーについて” (2017年6月28日 DNSOPS.JP DNS Summer Day) より

https://dnsops.jp/event/20170628/20170628-RootKSKRO-02.pdf

総務省 報道資料の読み方

「DNSの世界的な運用変更に伴う キャッシュDNSサーバーの設定更新の必要性」

- 対象：DNSを用いた検索を実際に行う「キャッシュDNSサーバー」の運用者全て
  - **本当の対象者**
    - **「署名検証をしているキャッシュDNSサーバ」(DNSSEC検証が有効) あるいは「署名検証をしているクライアント」の運用者**
    - **「署名検証をしているクライアント」が利用してるキャッシュDNSサーバ (DNSSECが有効 = DO ビットが on) の運用者**
  - **非対象者**
    - **DNSSEC は有効 (DOビット on) でも検証しておらず、検証しているクライアントもいないキャッシュDNSサーバの運用者**
    - **DNSSEC が無効 （DOビット off) あるいは非対応のサーバやクライアントの運用者**
    - **単なる利用者**

付録 「DNS における電子署名鍵の更改について」

http://www.soumu.go.jp/main_content/000497803.pdf

(1) 「鍵の更改」に追従するために、

(注: DNSSEC検証しなければ不要、特に③)

①「キャッシュDNS サーバー」のソフトウェア（一般に「BIND」又はWindows Server を利用）を最新版に更新する（今回の対策だけでなく、脆弱性への対応のためにも、最新版への更新は必須。）
(注: BIND 9.11.0-P5/9.10.4-P8/9.9.9-P8以降、Unbound 1.6.1以降)

②「キャッシュDNS サーバー」において、「DNSSEC のトラストアンカーの自動更新」の設定を行う (注: 必ず新 DNSKEY の取り込みを確認のこと)

~~③念のため、「キャッシュDNS サーバー」において、「DNSSEC」が有効になっており、また「DNSSEC の検証」が有効になっていることを確認する~~

付録 「DNS における電子署名鍵の更改について」

http://www.soumu.go.jp/main_content/000497803.pdf

(2) 「鍵の移行期間」のデータ量増大に対応するために、

①「キャッシュDNS サーバー」において、UDP 受信サイズを4096 バイトの検索結果が受信できる設定（RFC6891 による推奨設定）を行う。

注: むしろ小さくするほうが無難 (後述)であり、大きくすることによって障害が発現する危険性が高まる

②「キャッシュDNS サーバー」において、「dig コマンド」などを使い、4096 オクテットの検索結果が受信できるか確認する。**注: TCP で構わない**

③不明点がある場合には、運用委託先や上位ISP に問い合わせを行う。

注: 運用委託先で不明な場合は当方で相談に応じます

確認方法

DNSSEC 無効/非対応 (DO bit off)

```
$ dig @127.0.0.1 dnskey . +dnssec

; <<>> DiG 9.9.5 <<>> @127.0.0.1 dnskey . +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 226
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;.      IN DNSKEY

;; ANSWER SECTION:
.       172753 IN DNSKEY 257 3 8 (
           AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTO
           iW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOLAJr5emLvN
           7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5
           LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8
           efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7
           pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLY
           A4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws
           9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
           ) ; KSK; alg = RSASHA256; key id = 20326
.       172753 IN DNSKEY 256 3 8 (
           AwEAAYvxrQOOujKdZz+37P+oL4l7e35/0diH/mZITGjl
           p4f81ZGQK42HNxSfkiSahinPR3t0YQhjC393NX4TorSi
           TJy76TBWddNOkC/IaGqcb4erU+nQ75k2Lf0oIpA7qTCk
           3UkzYBqhKDHHAr2UditE7uFLDcoX4nBLCoaH5FtfxhUq
           yTlRu0RBXAEuKO+rORTFP0XgA5vlzVmXtwCkb9G8GknH
           uO1jVAwu3syPRVHErIbaXs1+jahvWWL+Do4wd+lA+TL3
           +pUk+zKTD2ncq7ZbJBZddo9T7PZjvntWJUzIHIMWZRFA
           jpi+V7pgh0o1KYXZgDUbiA1s9oLAL1KLSdmoIYM=
           ) ; ZSK; alg = RSASHA256; key id = 15768
.       172753 IN DNSKEY 257 3 8 (
           AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQ
           bSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh
           /RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWA
           JQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXp
           oY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3
           LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGO
           Yl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGc
           LmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0=
           ) ; KSK; alg = RSASHA256; key id = 19036
```

DNSSEC 有効 (DO bit on)

```
$ dig @127.0.0.1 dnskey . +dnssec

; <<>> DiG 9.8.0rc1 <<>> @127.0.0.1 dnskey . +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42391
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;.          IN DNSKEY

;; ANSWER SECTION:
.       172800  IN DNSKEY  257 3 8 AwEAAaz/
tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3 +/
4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF 0jLHwVN8efS3rCj/
EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN R1AkUTV74bU=
.       172800  IN DNSKEY  256 3 8 AwEAAYvxrQOOujKdZz+37P+oL4l7e35/0diH/
mZITGjlp4f81ZGQK42H NxSfkiSahinPR3t0YQhjC393NX4TorSiTJy76TBWddNOkC/IaGqcb4er
U+nQ75k2Lf0oIpA7qTCk3UkzYBqhKDHHAr2UditE7uFLDcoX4nBLCoaH
5FtfxhUqyTlRu0RBXAEuKO+rORTFP0XgA5vlzVmXtwCkb9G8GknHuO1j
VAwu3syPRVHErIbaXs1+jahvWWL+Do4wd+lA+TL3+pUk+zKTD2ncq7Zb
JBZddo9T7PZjvntWJUzIHIMWZRFAjpi+V7pgh0o1KYXZgDUbiA1s9oLA L1KLSdmoIYM=
.       172800  IN DNSKEY  257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0=
.       172800  IN RRSIG  DNSKEY 8 0 172800 20170920000000
20170830000000 19036 .
YXI2idSxbVGutW9wwv58GP8cemeDKqJnwnMNh527Z5gPuT2TOiUsGYjP
3MHjnQwjWG1rd3DZjgCjfAEbwUh1ifd17tAOoLt7ZriFsXC9eHjTLKYl
gdWf3aJjowO04Av8ZUOJ9OB1X7M5wONFHMOW5NLtJnZN2K5PqKYW31DZ JXhTcdLOWf9QCluG6C1/
mUaH8HiEiMLb6wGmpkoor+4Od4x0n3v4fMZP MmEeOCJDoFoEIVHY7Iggh+HaYMifSq+7UDY4Gm7/
yHiEp78RrPnQKAZL qhdisgIYm5TJYrI5eNGSMsxOZNOjZSxtCXHPI2Vcc3nVA0H1Zf+5Vb18
OW8zIg==
```

DNSSEC 署名検証有効の確認

```
$ dig @127.0.0.1 dnskey . +dnssec  (もしくは drill -D @127.0.0.1 dnskey . )

; <<>> DiG 9.8.0rc1 <<>> @127.0.0.1 dnskey . +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32901
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;.                IN  DNSKEY

;; ANSWER SECTION:
.     172800  IN  DNSKEY256 3 8 AwEAAYvxrQOOujKdZz+37P+oL4l7e35/0diH/mZITGjlp4f81ZGQK42H
NxSfkiSahinPR3t0YQhjC393NX4TorSiTJy76TBWddNOkC/IaGqcb4er U+nQ75k2Lf0oIpA7qTCk3UkzYBqhKDHHAr2UditE7uFLDcoX4nBLCoaH
5FtfxhUqyTlRu0RBXAEuKO+rORTFP0XgA5vlzVmXtwCkb9G8GknHuO1j VAwu3syPRVHErIbaXs1+jahvWWL+Do4wd+lA+TL3+pUk+zKTD2ncq7Zb
JBZddo9T7PZjvntWJUzIHIMWZRFAjpi+V7pgh0o1KYXZgDUbiA1s9oLA L1KLSdmoIYM=
.     172800  IN  DNSKEY257 3 8 AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0=
.     172800  IN  DNSKEY257 3 8 AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3 +/
4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN R1AkUTV74bU=
.     172800  IN  RRSIG  DNSKEY 8 0 172800 20170920000000 20170830000000 19036 .
YXI2idSxbVGutW9wwv58GP8cemeDKqJnwnMNh527Z5gPuT2TOiUsGYjP 3MHjnQwjWG1rd3DZjgCjfAEbwUh1ifd17tAOoLt7ZriFsXC9eHjTLKYl
gdWf3aJjowO04Av8ZUOJ9OB1X7M5wONFHMOW5NLtJnZN2K5PqKYW31DZ JXhTcdLOWf9QCluG6C1/mUaH8HiEiMLb6wGmpkoor+4Od4x0n3v4fMZP
MmEeOCJDoFoEIVHY7Iggh+HaYMifSq+7UDY4Gm7/yHiEp78RrPnQKAZL qhdisgIYm5TJYrI5eNGSMsxOZNOjZSxtCXHPI2Vcc3nVA0H1Zf+5Vb18
OW8zIg==
```

DNSSEC 署名検証有効の確認

```
% dig @127.0.0.1 dnssec-failed.org +dnssec

; <<>> DiG 9.8.0rc1 <<>> @127.0.0.1 dnssec-failed.org +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 60370
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnssec-failed.org.  IN  A

;; Query time: 2582 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep  5 13:30:05 2017
;; MSG SIZE  rcvd: 46
```

こちらもどうぞ「DNSSEC 署名検証の有無判定」
http://www.e-ontap.com/dns/validation.html

鍵応答サイズテスト

#	Description	KSKs	ZSKs	Signed DNSKEY Size	Result
1	2048 ZSK Normal	2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish+sign	949	PASS
2	2048 ZSK Rollover	2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish 2048-bit RSASHA256 publish+sign	1237	PASS
3	KSK Rollover with 2048 ZSK	2048-bit RSASHA256 publish+sign 2048-bit RSASHA256 publish+sign+revoke	2048-bit RSASHA256 publish+sign	1571	PASS
4	KSK Rollover with 2048 ZSK rollover	2048-bit RSASHA256 publish+sign+revoke 2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish+sign 2048-bit RSASHA256 publish	1865	PASS
5	This should fail			0	FAIL

http://keysizetest.verisignlabs.com/

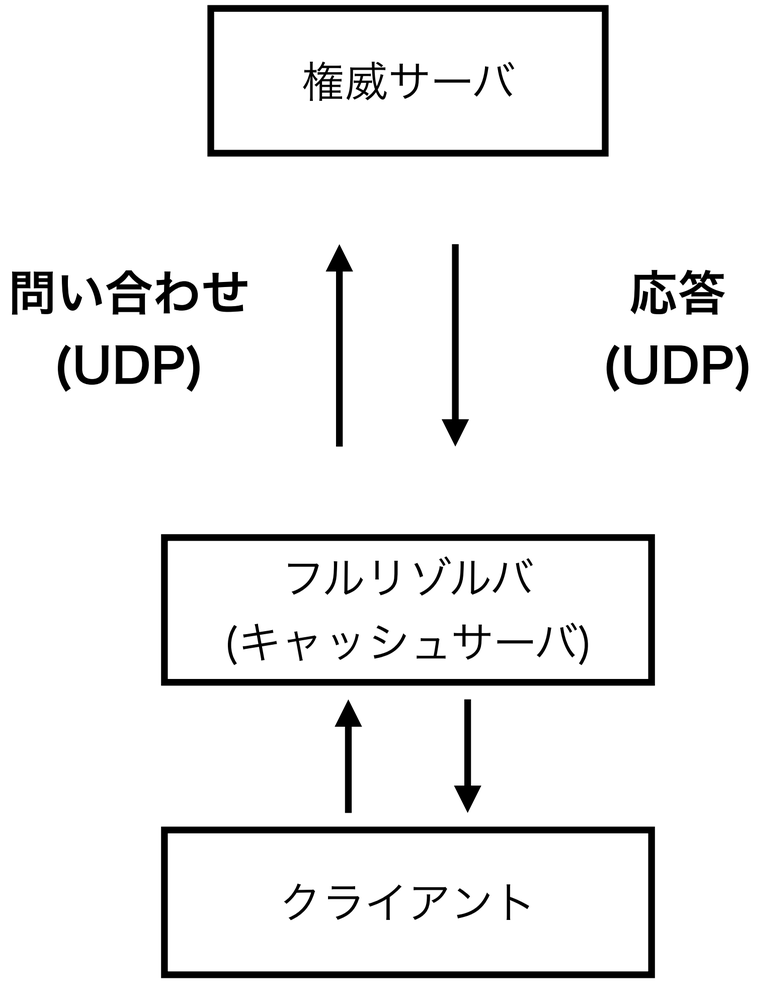
(他で紹介されている rs.dns-oarc.net を用いた確認方法は不確実なので推奨しない)

鍵応答サイズテスト

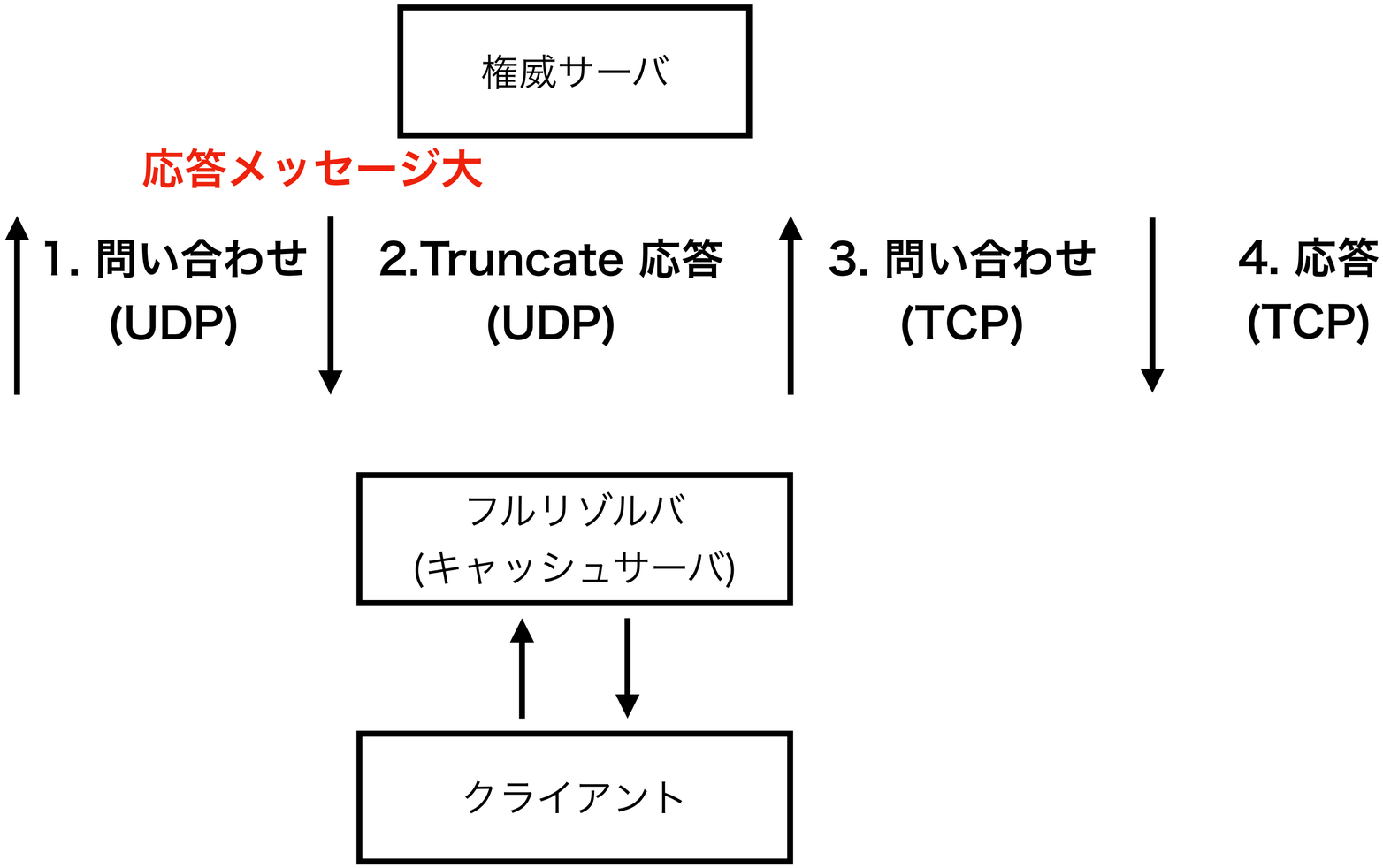
```
% dig any org @b0.org.afilias-nst.org +dnssec +bufsize=4096

; <<>> DiG 9.8.0rc1 <<>> any org @b0.org.afilias-nst.org +dnssec +bufsize=4096
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19768
;; flags: qr aa rd; QUERY: 1, ANSWER: 18, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;org.                    IN      ANY

;; ANSWER SECTION:
org.            900     IN      NSEC3PARAM 1 0 1 D399EAAB
org.            900     IN      RRSIG   NSEC3PARAM 7 1 900 20170922153100 20170901143100 3947 org. cYYQ5jt/6Z23RnlPziaiyjQanjoNKapH7Wy3ZfCIwArcWV0wsvJXGt0X
6oOh6RnVuWsoDmTJyIHO+FYyv6L4/ObPcKQ6euV7mamVDp7aNmzkaDGY fMAreuM1gIo2alELSXCPpw5vz0zboNdDgj6GSgihMJ3mQyRyP20KLEEZ Nwk=
org.            900     IN      DNSKEY 256 3 7 AwEAAXxsMmN/JgpEE9Y4uFNRJm7Q9GBwmEYUCsCxuKlgBU9WrQEFRrvA eMamUBeX4SE8s3V/TEk/TgGmPPp0pMkKD7mseluK6Ard2HZ6O3nPAzL4
i8py/UDRUmYNSCxwfdfjUWRmcB9H+NKWMsJoDhAkLFqg5HS7f0j4Vb99 Wac24Fk7
org.            900     IN      DNSKEY 256 3 7 AwEAAayiVbuM+ehlsKsuAL1CI3mA+5JM7ti3VeY8ysmogElVMuSLNsX7 HFyq9O6qhZVJz54Teuzf2EGjO8cbK/fUbyzFW+4i4BRk+pVx673NRgQq
DiB2oJDmQRK918Rmoxi/Sf8S7k9FB1XzxspIi9AJmn5tz4ACVsD2xTc1 wZtAKVjr
org.            900     IN      DNSKEY 257 3 7 AwEAAZTjbIO5kIpxWUtyXc8avsKyHIIZ+LjC2Dv8naO+Tz6X2fqzDC1b

(中略)

org.            86400   IN      NS c0.org.afilias-nst.info.
org.            86400   IN      NS d0.org.afilias-nst.org.
org.            86400   IN      RRSIG   NS 7 1 86400 20170922153100 20170901143100 3947 org. GE5qa4x4OySo8CdvNvAJ2YqjHPm1zHJtX3baam1b0/GRRhqFo7MwOhZB
3JbBLdtLFOQDlHN9YS/eDNJHEIaHrgT4Op25iYza70FuRutFk9xIRNOC LeyX2Utj3/mihxzHoN2HONqpJv5pspq2VVEn/kDWLyM1TAdWo/eYDCku Mvk=
org.            900     IN      SOA     a0.org.afilias-nst.info. noc.afilias-nst.info. 2012641966 1800 900 604800 86400
org.            900     IN      RRSIG   SOA 7 1 900 20170925152939 20170904142939 3947 org. UxHvbzdRLQ1m49svBQpZDeUKtGXr0gLXkKSAW4AULqa+k64ZxAXKzAZt i0Vzhfi/
pBrsZKgGBugwfydPMcafLILE3VJx9JPMYm0oq4sQk2NrfTRr js5Hsea4sD/WGoRZvFS4T3CLWHYMTpuEk4rFlew8xllIUNdjtK7UVWUE onw=

;; Query time: 263 msec
;; SERVER: 2001:500:c::1#53(2001:500:c::1)
;; WHEN: Tue Sep  5 00:30:41 2017
;; MSG SIZE  rcvd: 2313
```

データ量増大の問題
(IPフラグメント等)

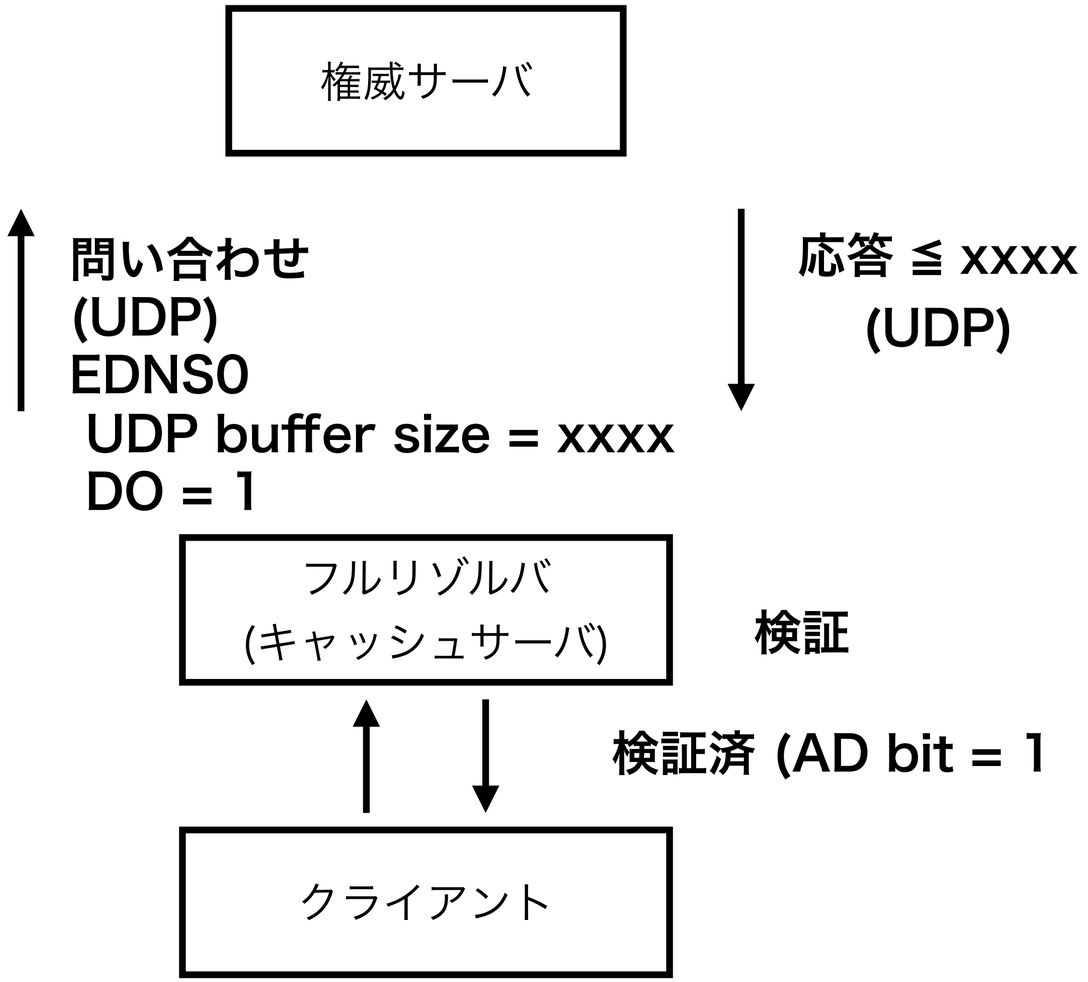
本来の DNS
(通常)



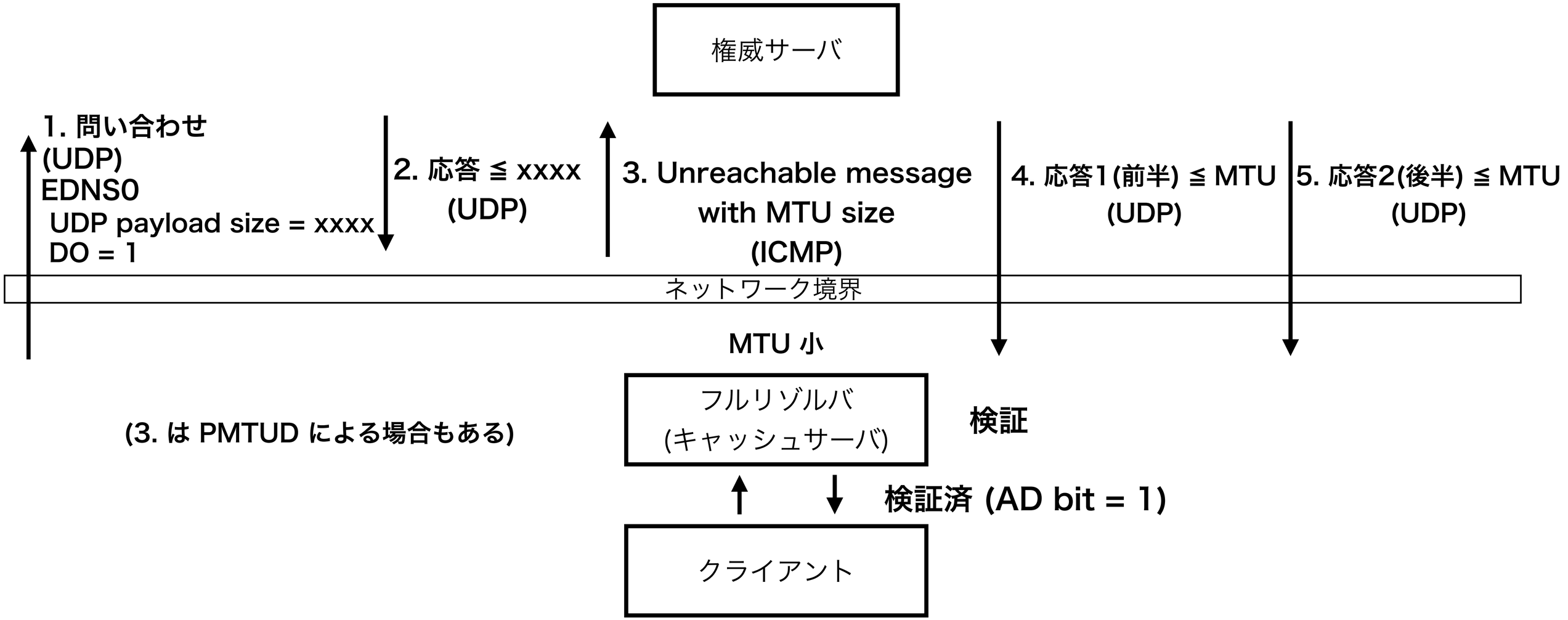
本来の DNS
(512バイトを越えるケース／TCPフォールバック)



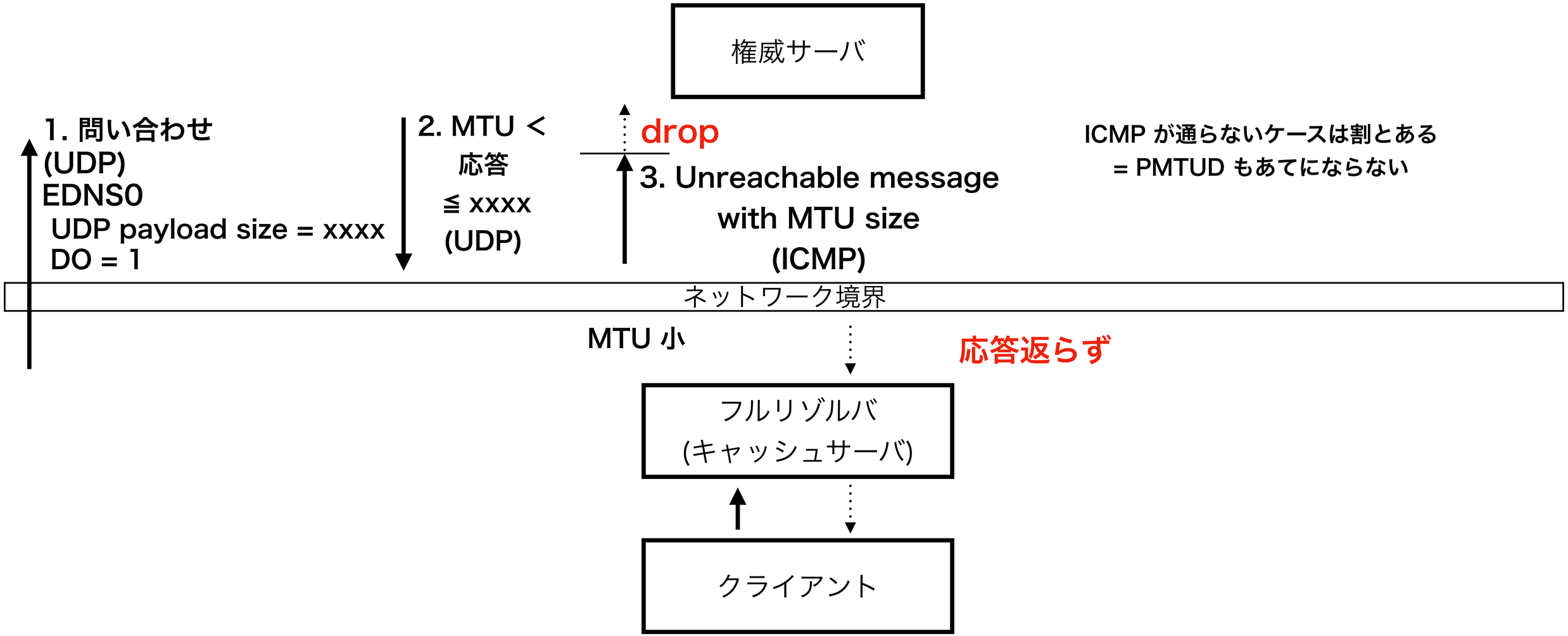
EDNS0 を用いる DNSSEC (指定サイズ以下の応答)



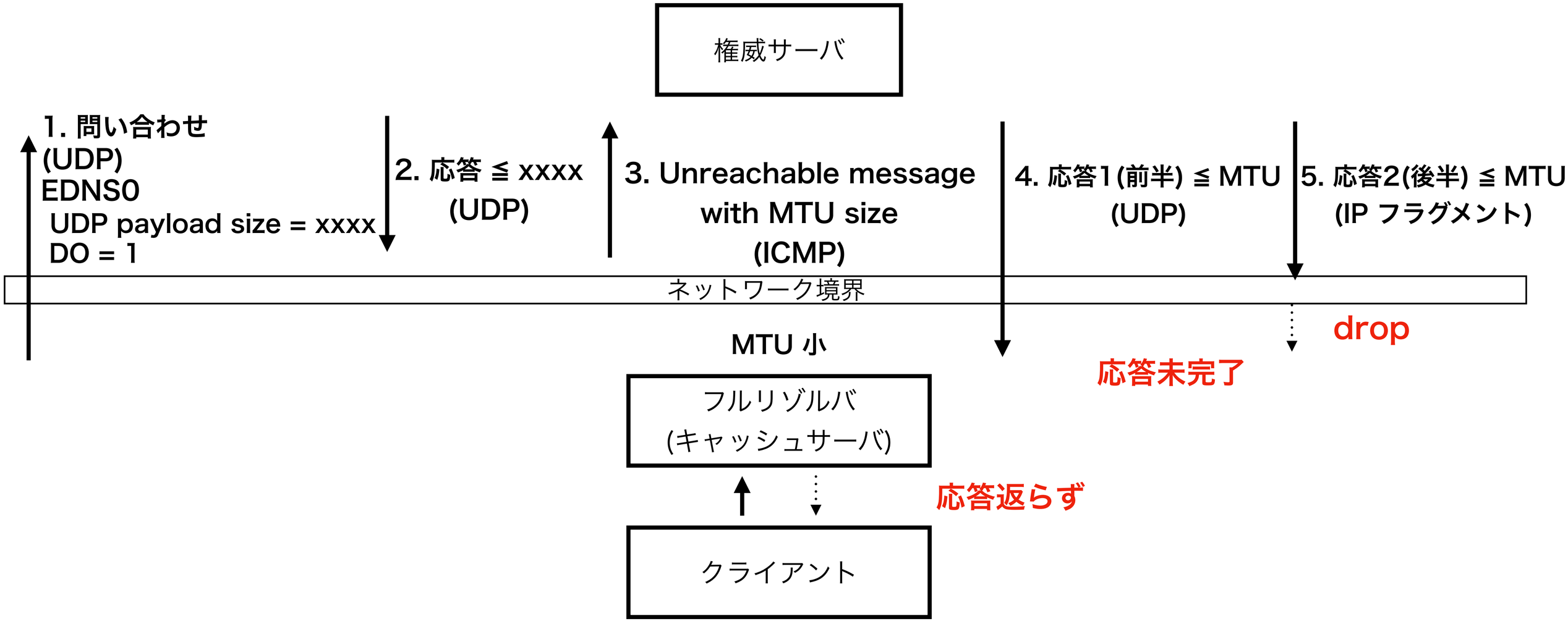
EDNS0 を用いる DNSSEC
(隘路＜応答サイズがある場合)



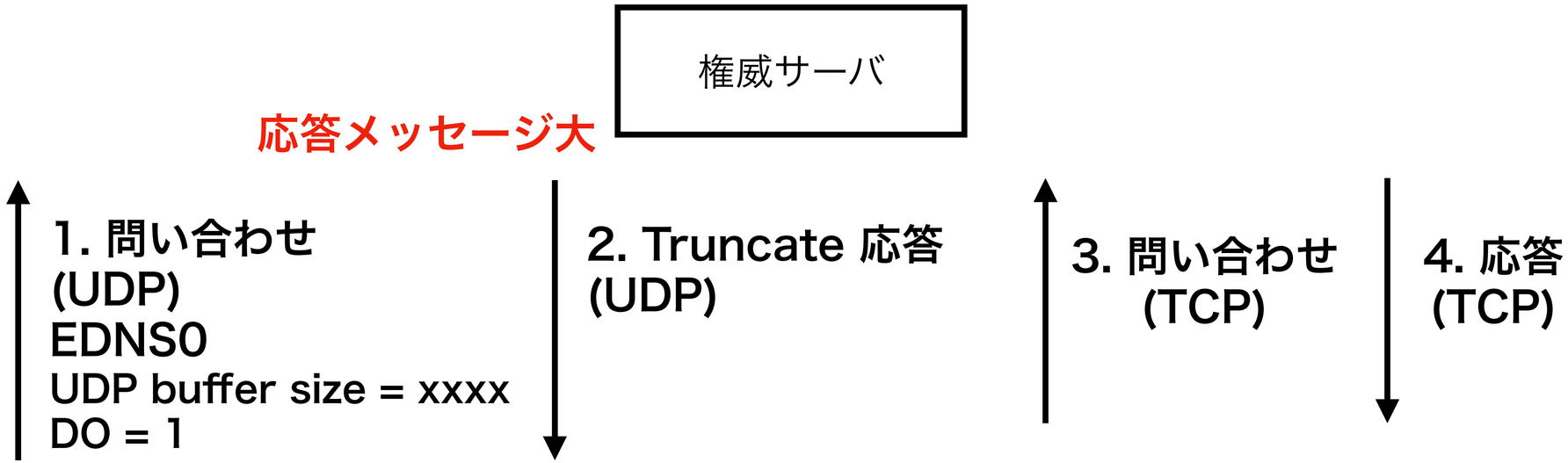
EDNS0 を用いる DNSSEC
(隘路<応答サイズがあり ICMP が drop される場合)



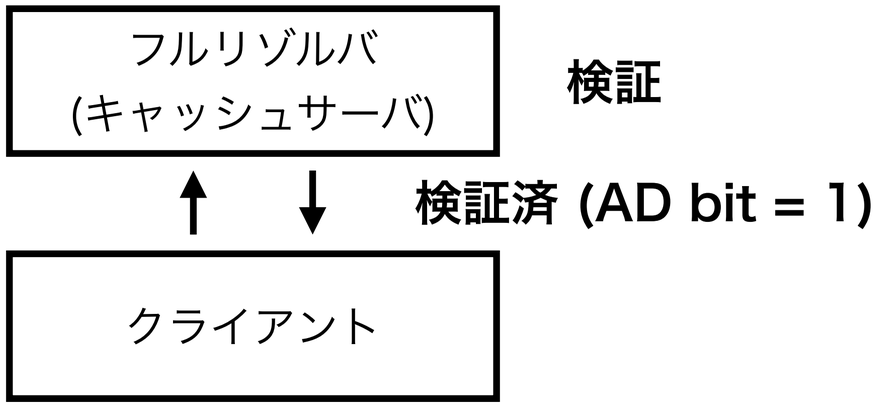
EDNS0 を用いる DNSSEC
(隘路く応答サイズがあり断片が drop される場合)



EDNS0 を用いる DNSSEC
(推奨：素直な TCP フォールバック)

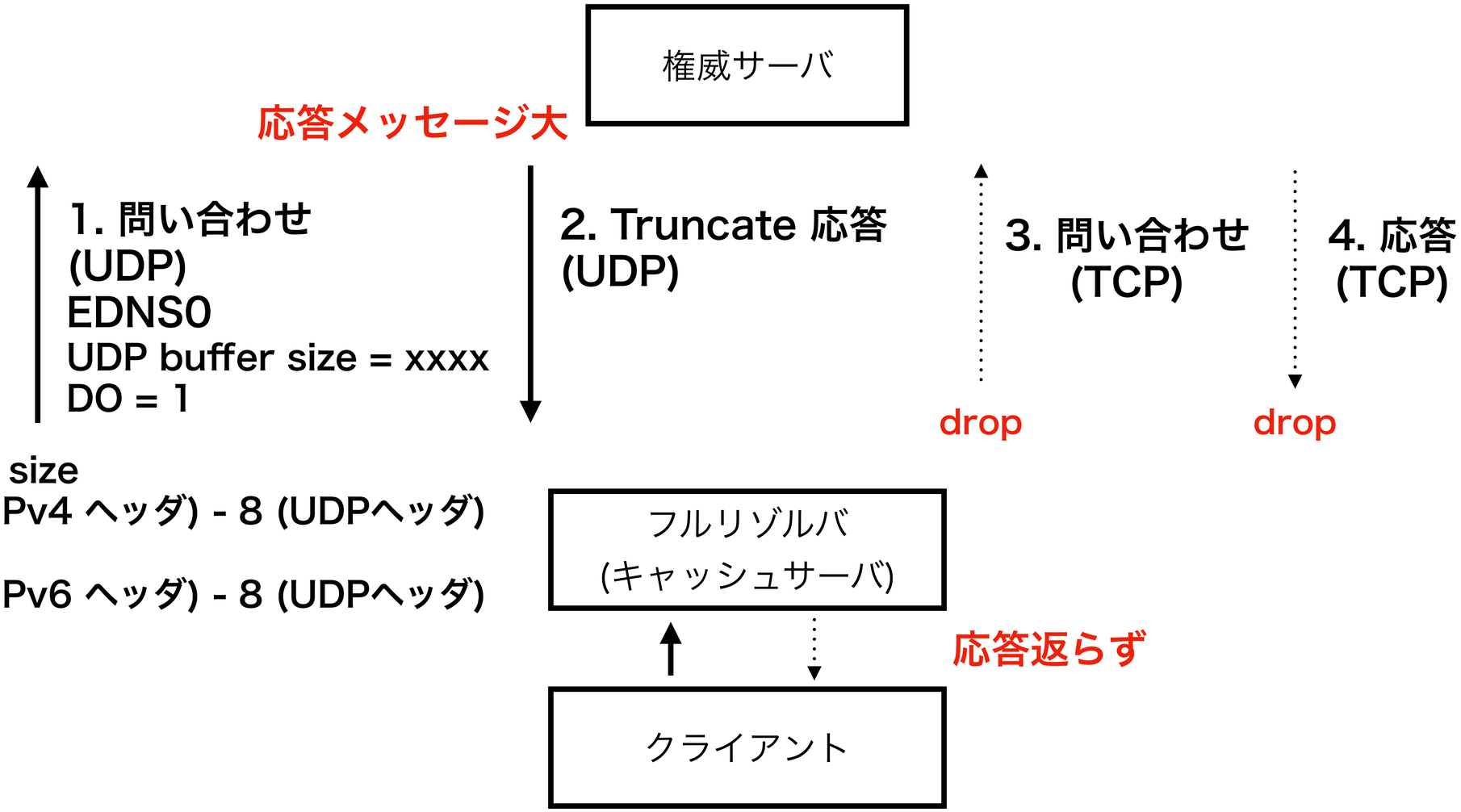


UDP payload size
≦ MTU - 20 (IPv4 ヘッダ) - 8 (UDPヘッダ)
または
≦ MTU - 40 (IPv6 ヘッダ) - 8 (UDPヘッダ)



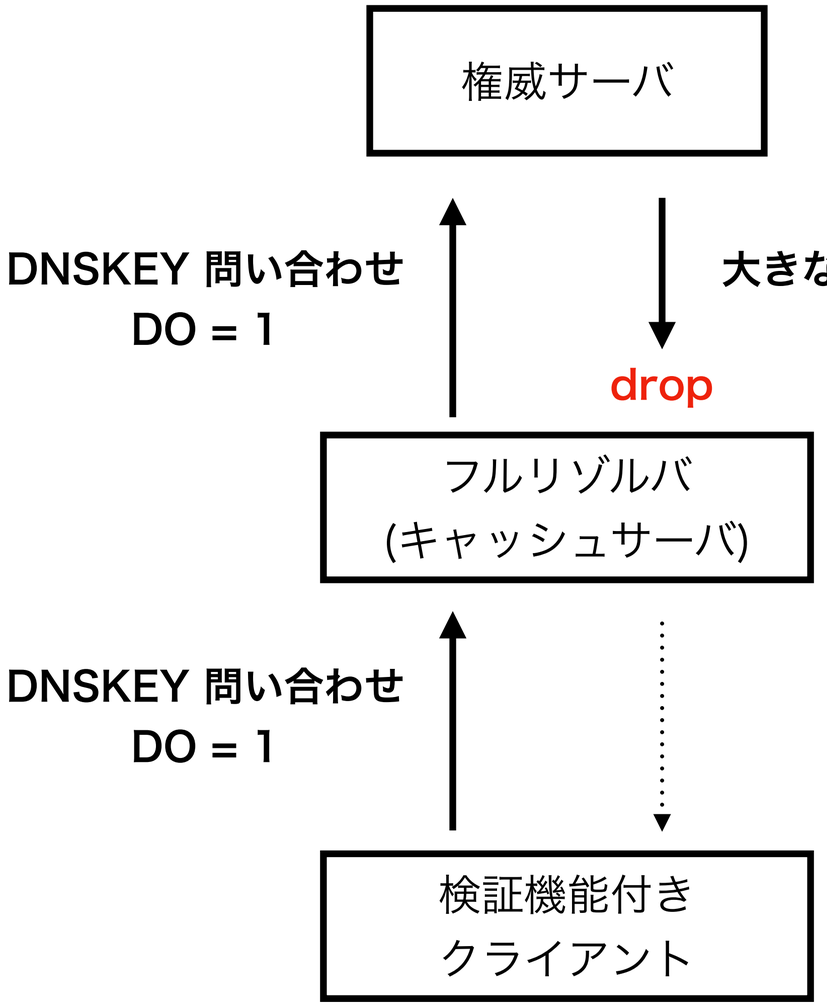
前ページまでのような様々なネットワークに起因するトラブルは UDP サイズを大きくすることにより発現しやすく、むしろ安全な UDP サイズを越えないよう TCP フォールバックしたほうが無難
MTU は 1500 より 1280（IPv6 最小 MTU）とみたほうが安全

EDNS0 を用いる DNSSEC (TCP 53 をブロックしないこと)



UDP payload size
≦ MTU - 20 (IPv4 ヘッダ) - 8 (UDPヘッダ)
または
≦ MTU - 40 (IPv6 ヘッダ) - 8 (UDPヘッダ)

DNSSEC未検証のサーバも要調査という一部の注意喚起の理由



クライアントとの仕様合意の問題

(途中の経路の問題もあり
保証できるとは思えない)

まとめ

- 一連の注意喚起 (特に総務省)
  1. DNSSEC を有効化 (総務省)
  2. ルートの鍵更新に追従する設定
  3. UDP のサイズ制限 (UDP payload size) を拡大 (推奨 4096)
  4. 9/19 に増大する KSK 応答のサイズを受け取れず名前解決に障害が発生する可能性がある場合、サーバのみならずネットワーク機器などを総合調査
- 推奨
  1. DNSSEC 署名の検証は無効化 (「DNSSEC はなぜダメなのか」参照)
  2. DNSSEC の署名をトラブルなく検証したい場合は DNSSEC (特に鍵更新) やネットワーク全判について深い知識が必要
  3. EDNS0 UDP payload size は小さく (以下の計算がわからなければ 512 が最も無難)

     推奨 512 等 ≦ 1232 = 1280 - 40 - 8 (IPv6 min)　(Unbound の 1480 という記述は間違い)
     ≦ 1452 = 1500 - 40 - 8 (IPv6 Ether) ≦ 1472 = 1500 -20 -8 (IPv4 Ether)
  4. ネットワークの調査・対策は急ぎません (ただし TCP 53 は必須)

参照リンク1

- ルートゾーンKSKのロールオーバー
  https://www.icann.org/resources/pages/ksk-rollover-2017-05-31-ja
- DNSの世界的な運用変更に伴うキャッシュDNSサーバーの設定更新の必要性 (総務省)
  http://www.soumu.go.jp/menu_news/s-news/02kiban04_04000212.html
- DNSにおける電子署名鍵の更改について (総務省総合通信基盤局データ通信課)
  http://www.soumu.go.jp/main_content/000497803.pdf
- ＤＮＳの世界的な運用変更に伴うキャッシュＤＮＳサーバーの設定更新の必要性について (NISC)
  http://www.nisc.go.jp/active/kihon/dns_taisaku.html
- 2017年9月19日以降に一部のDNS応答のサイズ増大によりインターネット利用に影響が出る恐れがあります ～DNS、ネットワーク機器の確認のお願い～ (JPNIC)
  https://www.nic.ad.jp/ja/topics/2017/20170802-01.html
- KSKロールオーバーについて (JPNIC)
  https://www.nic.ad.jp/ja/dns/ksk-rollover/
- ルートゾーンKSKロールオーバーによる影響とその確認方法について (JPRS)
  https://jprs.jp/tech/notice/2017-07-10-root-zone-ksk-rollover.html
- ルートゾーンKSKロールオーバーの概要と影響の確認方法 (JPRS)
  https://jprs.jp/tech/notice/2017-07-10-root-zone-ksk-rollover.pdf
- ルートゾーンKSKロールオーバーについてのご質問とその回答 (JPRS)
  https://jprs.jp/tech/notice/2017-08-10-root-zone-ksk-rollover-qa.html
- ルートゾーンのKSKロールオーバーについて (JPRS / DNSOPS Summer Seminar)
  https://dnsops.jp/event/20170628/20170628-RootKSKRO-02.pdf
- DNSSEC Key Size Test (verisignlabs.com)
  http://keysizetest.verisignlabs.com/
- SAC063 SSAC Advisory on DNSSEC Key Rollover in the Root Zone (ICANN)
  https://www.icann.org/en/system/files/files/sac-063-en.pdf

参照リンク2

- DNSSEC はなぜダメなのか
  http://www.e-ontap.com/dns/criticism/
- DNSSEC 署名検証の有無判定
  http://www.e-ontap.com/dns/validation.html
- フラグメンテーションの今後を考えよう (松平直樹 富士通株式会社 / JANOG 33.5)
  https://www.janog.gr.jp/meeting/janog33.5/doc/janog33.5_fragmentation.pdf
- DNSのメッセージサイズについて考える〜ランチのおともにDNS〜 (JPRS)
  https://jprs.jp/tech/material/iw2013-lunch-L3-01.pdf
- Dealing with fragmentation in EDNS0 Proposal for a recommendation (Surfnet / RIPE65)
  https://ripe65.ripe.net/presentations/167-20120926_-_RIPE65_-_Amsterdam_-_DNSSEC_reco_draft.pdf
- DNSSEC Protocol RFC (IETF)
  http://www.dnssec.net/rfc

- KSK Rollover Postponed
  https://www.icann.org/news/announcement-2017-09-27-en
- ICANNがルートゾーンKSKロールオーバーの実施延期を発表
  https://www.nic.ad.jp/ja/topics/2017/20170928-01.html