DNS Summer Day 2021

XACK meets DNSSEC

株式会社XACK
技術部　蜂巣　一輝

発表内容

- 会社・製品紹介
- DNSSEC対応にまつわるあれこれ

会社・製品紹介

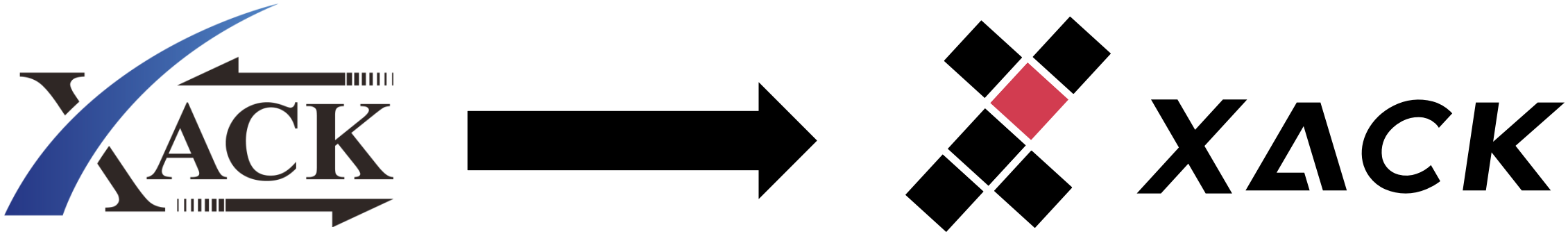
株式会社XACK 会社紹介

- 主な業務
  - ネットワークアプリケーションシステム全般に関するソフトウェア開発

製品名	概要
XACK RADIUS	大規模システム向け高性能RADIUSサーバー(GUI開発中) NEW!
XACK DNS	通信事業者向けセキュアDNSサーバー (GUI対応)
XACK DHCP	DHCPv4/v6両対応高性能DHCPサーバー (GUI対応) →サーバー、GUIともにDOCSIS対応しました NEW!
XACK DNS Zone Editor	マルチテナント編集システム (GUI)
XACK EAP Tester	RADIUSクライアントシミュレーター

株式会社XACK 会社紹介

- ロゴが変わりました！



株式会社XACK 会社紹介

- Webサイトもオシャレになりました

XACK

XACK DNS 製品紹介

XACK DNSの特徴

- フルスクラッチの国産DNSサーバー
- マスター/スレーブ権威機能・フルリゾルバー機能・フォワーダー機能・etc…
- モジュール化による機能の足し引きが可能
  - 例えばマスター権威機能→フォワーダー機能と組み合わせることで、自身が管理するゾーンについては権威ある応答を、そうでないゾーンについてはどこかに転送を、等
- 仮想サーバー機能
  - 1つのインスタンスで複数のサーバーが動作しているかのように振舞うことが可能
- 通信事業者様や企業・大学様での採用実績あり
- DNSSEC対応（権威サーバー） NEW!
- DNS Update対応も取り組んでいます NEW!

DNSSEC対応にまつわるあれこれ

DNSSEC対応中

- まだ製品ラインナップとしては挙げておりませんが、
  権威サーバー機能のDNSSEC対応が完了しています

- 対応や検証に当たってのあれこれをご紹介していきます

RRSIG主張強すぎ問題

RRSIG主張強すぎ問題

- DNSSECは人力で運用すべきでない

RRSIG主張強すぎ問題

- DNSSECは人力で運用すべきでない
  - 権威サービスのDNSSEC対応
  - BINDも自動署名してくれたり
  - アプライアンス製品だとGUIからボタン1発だったり
  - ZSKの自動更新もやってくれたり
  - XACK DNS Managerもやってくれます

RRSIG主張強すぎ問題

- DNSSECは人力で運用すべきでない
  - 権威サービスのDNSSEC対応
  - BINDも自動署名してくれたり
  - アプライアンス製品だとGUIからボタン1発だったり
  - ZSKの自動更新もやってくれたり
  - XACK DNS Managerもやってくれます

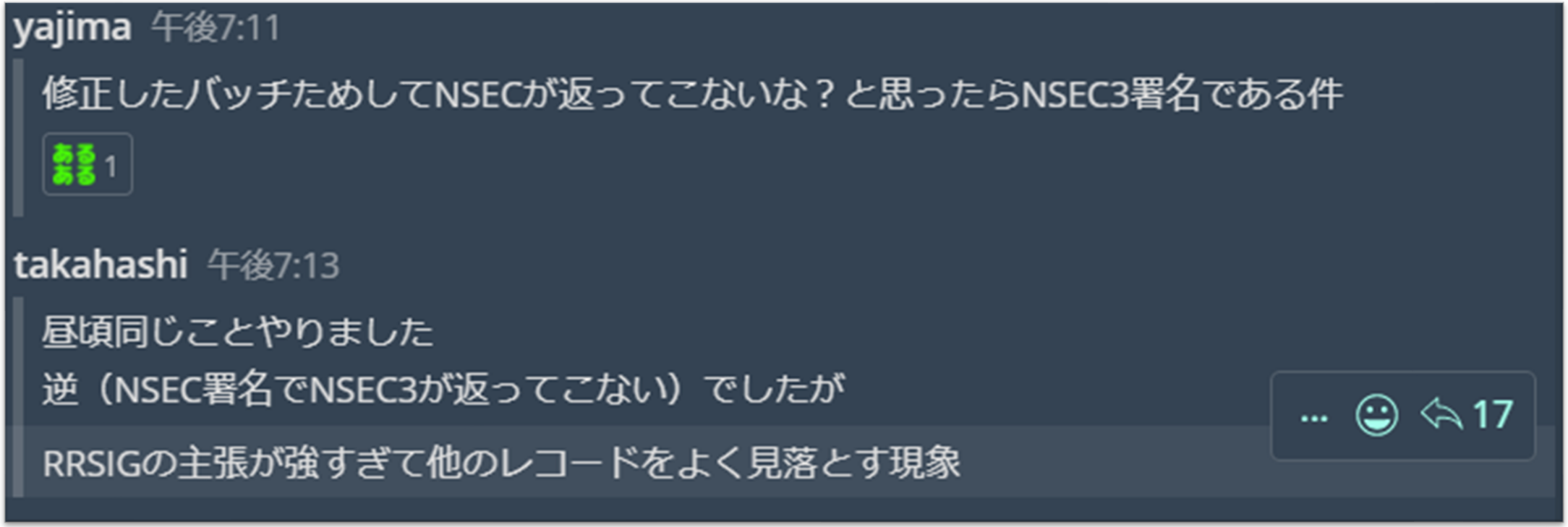
- 署名に関連するレコードを意識することなく利用できる（DS除く）

RRSIG主張強すぎ問題

- DNSSECは人力で運用すべきでない
  - 権威サービスのDNSSEC対応
  - BINDも自動署名してくれたり
  - アプライアンス製品だとGUIからボタン1発だったり
  - ZSKの自動更新もやってくれたり
  - XACK DNS Managerもやってくれます
- 署名に関連するレコードを意識することなく利用できる（DS除く）
- 提供する側としては当然署名済みゾーンを直接扱うわけで…

RRSIG主張強すぎ問題

RRSIG主張強すぎ問題



RRSIG主張強すぎ問題

- 署名済みゾーンってめちゃめちゃ見づらいですよね？

RRSIG主張強すぎ問題

- 署名済みゾーンってめちゃめちゃ見づらいですよね？
- ゾーンファイルのRRSIG占有率が高すぎる

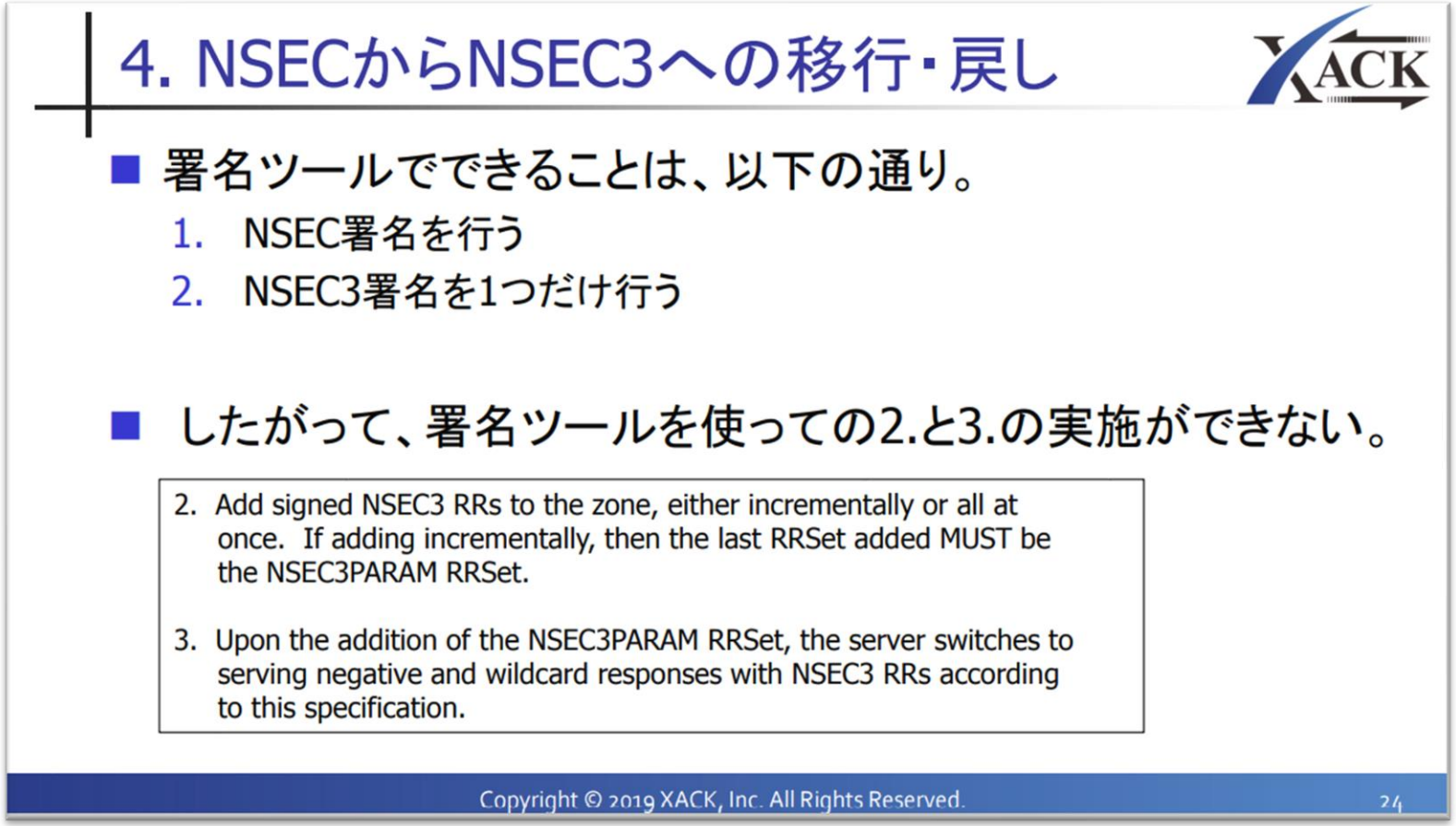
RRSIG主張強すぎ問題

- 署名済みゾーンってめちゃめちゃ見づらいですよね？
- ゾーンファイルのRRSIG占有率が高すぎる
- オチはない

RFCに書いてある作業が実現できない

再掲

- 2年前の発表資料です



4. NSECからNSEC3への移行・戻し

XACK

- 署名ツールでできることは、以下の通り。
  1. NSEC署名を行う
  2. NSEC3署名を1つだけ行う

- したがって、署名ツールを使っての2.と3.の実施ができない。

> 2. Add signed NSEC3 RRs to the zone, either incrementally or all at once. If adding incrementally, then the last RRSet added MUST be the NSEC3PARAM RRSet.
>
> 3. Upon the addition of the NSEC3PARAM RRSet, the server switches to serving negative and wildcard responses with NSEC3 RRs according to this specification.

XACK

RFCに書いてある作業が実現できない

- NSECからNSEC3へ移行する手順

> 2. Add signed NSEC3 RRs to the zone, either incrementally or all at once. If adding incrementally, then the last RRSet added MUST be the NSEC3PARAM RRSet.

RFCに書いてある作業が実現できない

- NSECからNSEC3へ移行する手順

2. Add signed NSEC3 RRs to the zone, either incrementally or all at once. If adding incrementally, then the last RRSet added MUST be the NSEC3PARAM RRSet.

徐々にまたは一度に、署名されたNSEC3 RRの全てをゾーンに追加する。

RFCに書いてある作業が実現できない

- NSECからNSEC3へ移行する手順

> 2. Add signed NSEC3 RRs to the zone, either incrementally or all at once. If adding incrementally, then the last RRSet added MUST be the NSEC3PARAM RRSet.

徐々にまたは一度に、署名されたNSEC3 RRの全てをゾーンに追加する。

- NSEC署名済みゾーンにNSEC3を徐々に追加するツールってご存知ですか

試験ケース爆増

試験ケース爆増

- NSEC, NSEC3, NSEC3 Opt-Outで試験ケース数が爆増する
  - 概ね同じようなパターンを3周

試験ケース爆増

- NSEC, NSEC3, NSEC3 Opt-Outで試験ケース数が爆増する
  - 概ね同じようなパターンを3周
  - …とでも思ったか
    - NSECとNSEC3が共存する

試験ケース爆増

- NSEC, NSEC3, NSEC3 Opt-Outで試験ケース数が爆増する
  - 概ね同じようなパターンを3周
  - …とでも思ったか
    - NSECとNSEC3が共存する
    - NSEC3がNSEC3PARAM違いで2つある

試験ケース爆増

- NSEC, NSEC3, NSEC3 Opt-Outで試験ケース数が爆増する
  - 概ね同じようなパターンを3周
  - …とでも思ったか
    - NSECとNSEC3が共存する
    - NSEC3がNSEC3PARAM違いで2つある
    - NSEC3 Opt-OutがNSEC3PARAM違いで2つある

試験ケース爆増

- NSEC, NSEC3, NSEC3 Opt-Outで試験ケース数が爆増する
  - 概ね同じようなパターンを3周
  - …とでも思ったか
    - NSECとNSEC3が共存する
    - NSEC3がNSEC3PARAM違いで2つある
    - NSEC3 Opt-OutがNSEC3PARAM違いで2つある
    - etc …

試験ケース爆増

- NSEC, NSEC3, NSEC3 Opt-Outで試験ケース数が爆増する
  - 概ね同じようなパターンを3周
  - …とでも思ったか
    - NSECとNSEC3が共存する
    - NSEC3がNSEC3PARAM違いで2つある
    - NSEC3 Opt-OutがNSEC3PARAM違いで2つある
    - etc …
- DNSKEYも複数置くパターンで試験ケース数が爆増する

試験ケース爆増

- NSEC, NSEC3, NSEC3 Opt-Outで試験ケース数が爆増する
  - 概ね同じようなパターンを3周
  - …とでも思ったか
    - NSECとNSEC3が共存する
    - NSEC3がNSEC3PARAM違いで2つある
    - NSEC3 Opt-OutがNSEC3PARAM違いで2つある
    - etc …
- DNSKEYも複数置くパターンで試験ケース数が爆増する
  - 委任元にDSが複数置いてあるパターンも

試験ケース爆増

- NSEC, NSEC3, NSEC3 Opt-Outで試験ケース数が爆増する
  - 概ね同じようなパターンを3周
  - …とでも思ったか
    - NSECとNSEC3が共存する
    - NSEC3がNSEC3PARAM違いで2つある
    - NSEC3 Opt-OutがNSEC3PARAM違いで2つある
    - etc …
- DNSKEYも複数置くパターンで試験ケース数が爆増する
  - 委任元にDSが複数置いてあるパターンも
  - ZSKとKSKが分かれていないケース

試験ケース爆増

- 応答が正しく取り扱ってもらえるかの検証をするため
  既存のリゾルバーを使うことになる

試験ケース爆増

- 応答が正しく取り扱ってもらえるかの検証をするため
  既存のリゾルバーを使うことになる
  - BINDだけだと不安じゃない？→Unboundでも同様の試験を、でケース数爆増

試験ケース爆増

- 応答が正しく取り扱ってもらえるかの検証をするため
  既存のリゾルバーを使うことになる
  - BINDだけだと不安じゃない？→Unboundでも同様の試験を、でケース数爆増
  - BINDとUnboundで挙動が違う→BINDバグってないですか？

さて…

今年まだRFCにケチ付けてないですね？

RFC未定義領域問題

RFC未定義領域問題

- ~~ノルマ達成~~

RFC未定義領域問題

- RRSIG, NSECレコードはその性質からCNAMEレコードと同所有者名での共存が認められるよう変更されている

> Because every authoritative RRset in a zone must be protected by a digital signature, RRSIG RRs must be present for names containing a CNAME RR. This is a change to the traditional DNS specification [RFC1034], which stated that if a CNAME is present for a name, it is the only type allowed at that name. A RRSIG and NSEC (see Section 4) MUST exist for the same name as a CNAME resource record in a signed zone.

RFC未定義領域問題

- RRSIG, NSECレコードはその性質からCNAMEレコードと同所有者名での共存が認められるよう変更されている

Because every authoritative RRset in a zone must be protected by a digital signature, RRSIG RRs must be present for names containing a CNAME RR. This is a change to the traditional DNS specification [RFC1034], which stated that if a CNAME is present for a name, it is the only type allowed at that name. A RRSIG and NSEC (see Section 4) MUST exist for the same name as a CNAME resource record in a signed zone.

署名ゾーンでは、CNAMEリソースレコードを持つ名前に対して、同じ名前を持つRRSIGとNSECセクション4参照)が存在しなければならない(MUST)。

RFC未定義領域問題

- RRSIG, NSECレコードはその性質からCNAMEレコードと同所有者名での共存が認められるよう変更されている

- 一方で、CNAMEと同名のRRSIG, NSECそのものを問い合わせられた場合に取るべき挙動は？

RFC未定義領域問題

- RRSIG, NSECレコードはその性質からCNAMEレコードと同所有者名での共存が認められるよう変更されている

- 一方で、CNAMEと同名のRRSIG, NSECそのものを問い合わせられた場合に取るべき挙動は？
  - それそのものを返す？CNAME先を返す？

RFC未定義領域問題

- RRSIG, NSECレコードはその性質からCNAMEレコードと同所有者名での共存が認められるよう変更されている
- 一方で、CNAMEと同名のRRSIG, NSECそのものを問い合わせられた場合に取るべき挙動は？
  - それそのものを返す？CNAME先を返す？
- RFC4033～4035にてこのケースは言及されていない

RFC未定義領域問題

- RRSIG, NSECレコードはその性質からCNAMEレコードと同所有者名での共存が認められるよう変更されている
- 一方で、CNAMEと同名のRRSIG, NSECそのものを問い合わせられた場合に取るべき挙動は？
  - それそのものを返す？CNAME先を返す？
- RFC4033～4035にてこのケースは言及されていない
  - やった！Summer Dayのネタにできるぞ！

RFC未定義領域問題

- RRSIG, NSECレコードはその性質からCNAMEレコードと同所有者名での共存が認められるよう変更されている
- 一方で、CNAMEと同名のRRSIG, NSECそのものを問い合わせられた場合に取るべき挙動は？
  - それそのものを返す？CNAME先を返す？
- RFC4033～4035にてこのケースは言及されていない
  - やった！Summer Dayのネタにできるぞ！
  - ところが…

原点回帰

- RFC1034 3.6.2. Aliases and canonical names

> CNAME RRs cause special action in DNS software. When a name server fails to find a desired RR in the resource set associated with the domain name, it checks to see if the resource set consists of a CNAME record with a matching class.

原点回帰

- RFC1034 3.6.2. Aliases and canonical names

CNAME RRs cause special action in DNS software. When a name server fails to find a desired RR in the resource set associated with the domain name, it checks to see if the resource set consists of a CNAME record with a matching class.

ネームサーバーがドメイン名に関連づけられたリソースの集合から
要求されたRRを発見することに失敗した場合、リソースの集合が
クラスの一致するCNAMEレコードで構成されていないかを確認する。

原点回帰

- RFC1034 3.6.2. Aliases and canonical names

CNAME RRs cause special action in DNS software. When a name server fails to find a desired RR in the resource set associated with the domain name, it checks to see if the resource set consists of a CNAME record with a matching class.

ネームサーバーがドメイン名に関連づけられたリソースの集合から要求されたRRを発見することに失敗した場合、リソースの集合がクラスの一致するCNAMEレコードで構成されていないかを確認する。

原点回帰

- RFC1034 3.6.2. Aliases and canonical names

> CNAME RRs cause special action in DNS software. When a name server fails to find a desired RR in the resource set associated with the domain name, it checks to see if the resource set consists of a CNAME record with a matching class.

> ネームサーバーがドメイン名に関連づけられたリソースの集合から要求されたRRを発見することに失敗した場合、リソースの集合がクラスの一致するCNAMEレコードで構成されていないかを確認する。

- 改訂するまでもなく問い合わせられたレコードそのものを返すのが正

原点回帰

- RFC1034 3.6.2. Aliases and canonical names

> CNAME RRs cause special action in DNS software. When a name server fails to find a desired RR in the resource set associated with the domain name, it checks to see if the resource set consists of a CNAME record with a matching class.

> ネームサーバーがドメイン名に関連づけられたリソースの集合から要求されたRRを発見することに失敗した場合、リソースの集合がクラスの一致するCNAMEレコードで構成されていないかを確認する。

- 改訂するまでもなく問い合わせられたレコードそのものを返すのが正

- ノルマ未達成

まとめ

- DNSSEC対応に当たってのあれこれをとりとめなくご紹介しました
- XACK DNSも（権威機能の）DNSSEC対応したので
  製品ラインナップ入りしたらぜひご検討ください
- 今後もより良い製品を目指して開発を進めてまいります

参考文献

- RFC（原文）
  - https://datatracker.ietf.org/doc/html/rfc1034
  - https://datatracker.ietf.org/doc/html/rfc4033
  - https://datatracker.ietf.org/doc/html/rfc4034
  - https://datatracker.ietf.org/doc/html/rfc4035
  - https://datatracker.ietf.org/doc/html/rfc5155
- RFC(JPRS様邦訳)
  - https://jprs.jp/tech/material/rfc/RFC1034-ja.txt
  - https://jprs.jp/tech/material/rfc/RFC4033-ja.txt
  - https://jprs.jp/tech/material/rfc/RFC4034-ja.txt
  - https://jprs.jp/tech/material/rfc/RFC4035-ja.txt
  - https://jprs.jp/tech/material/rfc/RFC5155-ja.txt

https://xack.co.jp