BIND 9.9から9.11へ移行のポイント(フルリゾルバ編)
- 9.9系サポート終了まであと３日！-

2018年6月27日
DNS Summer Day 2018

株式会社QTnet
技術本部　サービスオペレーションセンター

末松慶文 (yo_suematsu at qtnet.co.jp)

自己紹介

- 末松慶文(すえまつ よしぶみ)
  - DNSを含むサーバ関連の構築と保守などを10年くらい。
- 株式会社QTnet （旧 九州通信ネットワーク株式会社）
  - 新社名のお知らせ
    http://www.qtnet.co.jp/massmedia/2017/20170614.html
  - QTmobile (QTモバイル)
    http://www.qtmobile.jp
  - DNSの耐障害性強化に向けてJPRSと共同研究を開始 (2015年7月13日)
    JPRS: JPRSが新gTLD「.jprs」でDNSの耐障害性強化に向けてISPとの共同研究を開始　http://jprs.co.jp/press/2015/150713.html
    QTNet: JPRSとの共同研究について　http://www.qtnet.co.jp/massmedia/2015/20150713_2.html
  - APRICOT 2017 TLD Anycast DNS servers to ISPs (JPRS, QTnet)
    https://2017.apricot.net/program/schedule/#/day/9/network-operations-2
  - JPRSおよび電力系通信事業者8社が共同研究の成果を公開
    http://www.qtnet.co.jp/massmedia/2017/20171031_1.html
    https://tldlabs.jprs/acts/s001/

どのような局面においても名前解決を継続的に提供し続けたい！

目次

■ BINDのサポート期限について

・さまざまなBIND

・BIND 9.9(OSS版)のサポート期限について

・とっておき？の話

■BIND 9.9から9.11への変更について(フルリゾルバ編)

・変更点一覧

・特に注意すべき変更点と機能について

■まとめ

さまざまなBIND

・オープンソース版 例:BIND 9.9.6-P8
　サポート: コミュニティサポート bind-users
今回はこちらを対象にお話しします。

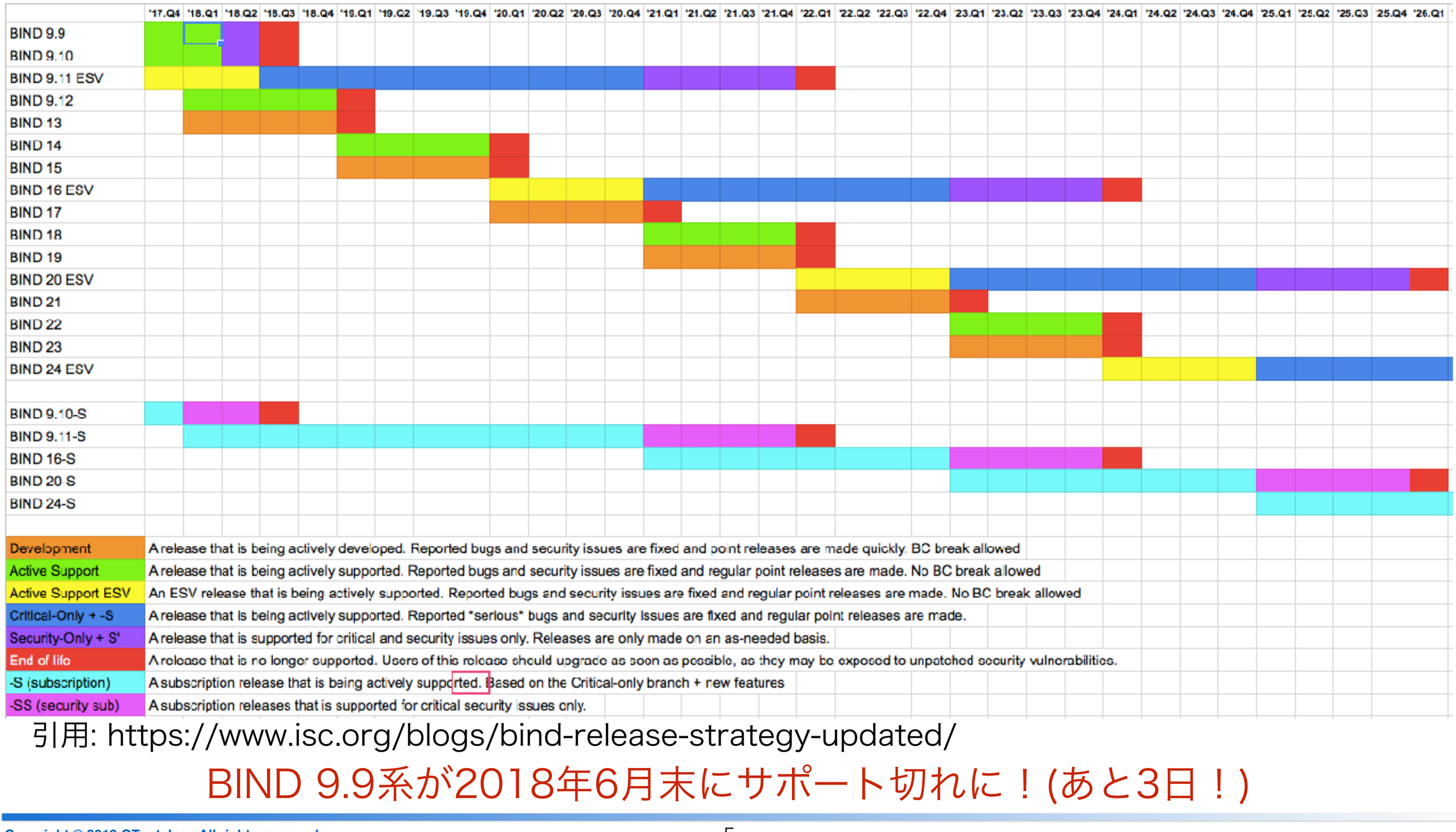
・Subscription版 例:BIND 9.9.8-S1
　サポート: 有償のサポート契約、　脆弱性情報の事前通知

・OSに付属するパッケージのBIND 例：BIND 9.9.4-RedHat-9.9.4-50.el7
　各ディストリビューションのサポートポリシーに準じる。

・アプライアンス　例：infoblox
　各製品のサポートポリシーに準じる。

今回はオープンソース版のBINDの話をします

BINDロードマップ



Development	A release that is being actively developed. Reported bugs and security issues are fixed and point releases are made quickly. BC break allowed
Active Support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made. No BC break allowed
Active Support ESV	An ESV release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made. No BC break allowed
Critical-Only + -S	A release that is being actively supported. Reported "serious" bugs and security issues are fixed and regular point releases are made.
Security-Only + S'	A release that is supported for critical and security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.
-S (subscription)	A subscription release that is being actively supported. Based on the Critical-only branch + new features
-SS (security sub)	A subscription releases that is supported for critical security issues only.

引用: https://www.isc.org/blogs/bind-release-strategy-updated/

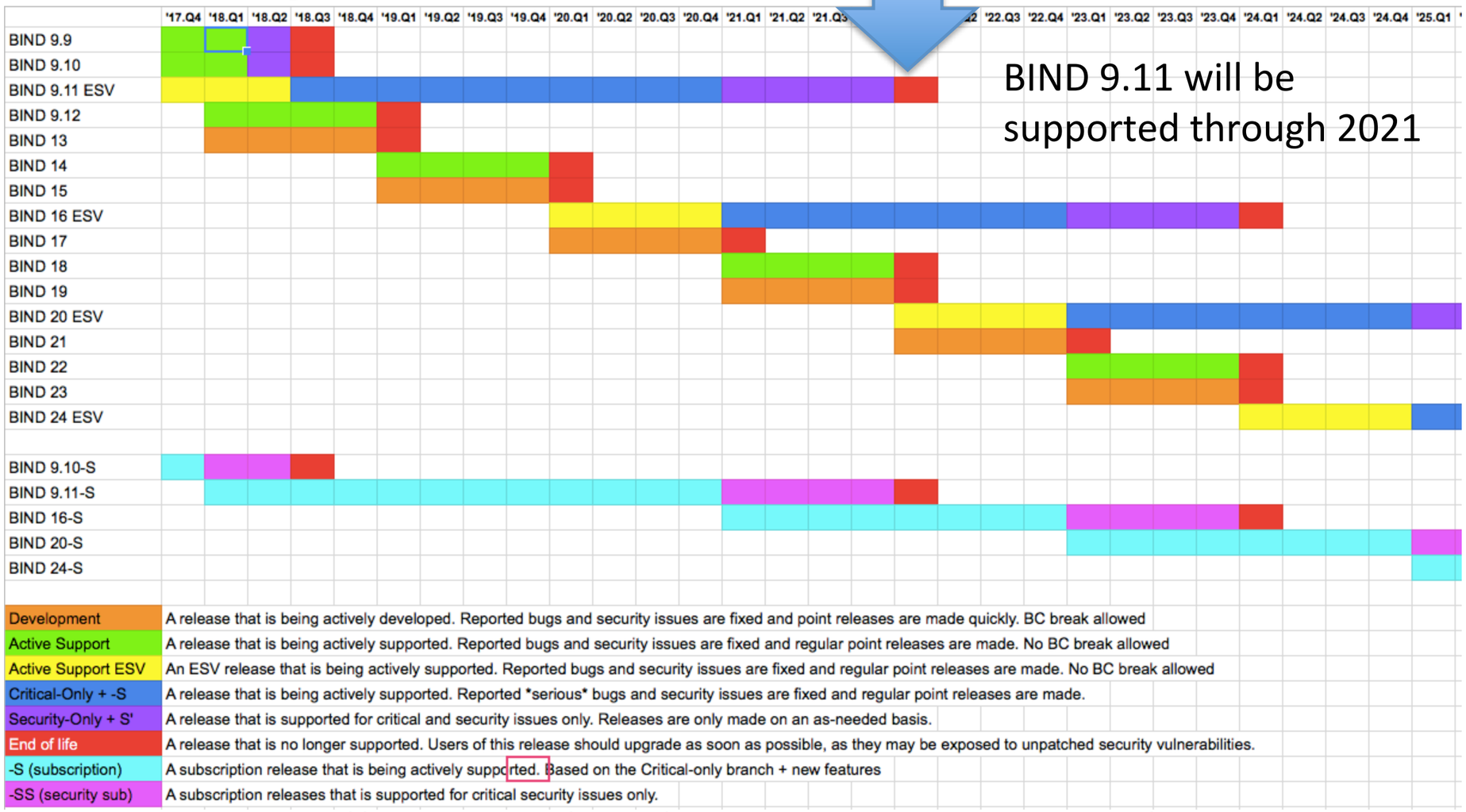
BIND 9.9系が2018年6月末にサポート切れに！(あと3日！)

ISCから日本のBIND-Usersへ

From ISC

BIND 9.9 and 9.10 EOL dates extended to end of June, 2018 with security patches for a further quarter if needed

BIND 9.11 will be supported through 2021



Development	A release that is being actively developed. Reported bugs and security issues are fixed and point releases are made quickly. BC break allowed
Active Support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made. No BC break allowed
Active Support ESV	An ESV release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made. No BC break allowed
Critical-Only + -S	A release that is being actively supported. Reported *serious* bugs and security issues are fixed and regular point releases are made.
Security-Only + S'	A release that is supported for critical and security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.
-S (subscription)	A subscription release that is being actively supported. Based on the Critical-only branch + new features
-SS (security sub)	A subscription releases that is supported for critical security issues only.

https://www.isc.org/blogs/bind-release-strategy-updated/

BIND 9.11 – June 2016

- BIND 9.11, supported for 2 years already, will be supported through the end of 2021
- Many new features: Catalog zones, DNS cookies, RNDC improvements, Negative trust anchors, Dyndb interface, DNSTAP
- https://www.isc.org/downloads/bind/bind-9-11-new-features/

BIND 9.12 – January 2018

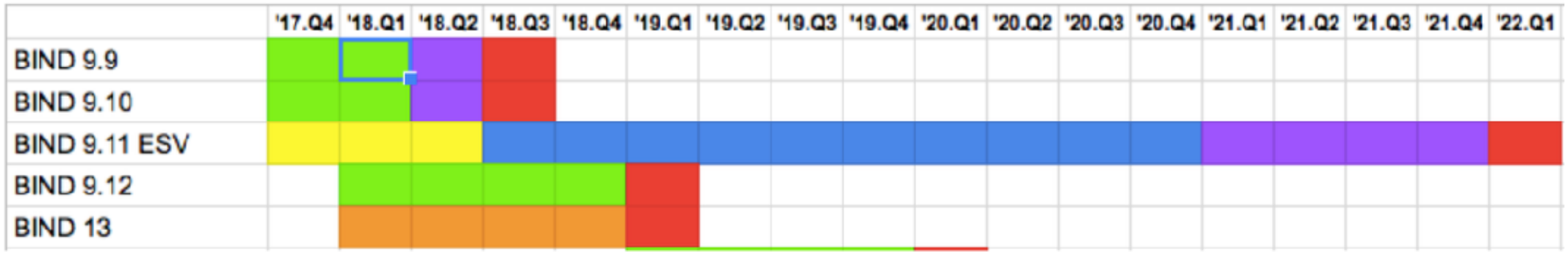
- NSEC aggressive use, sponsored by APNIC, reuses cached information to provide negative answers
- Serve Stale, contributed by Akamai, to address the problems like the October 2017 Dyn outage
- New glue cache provides dramatic improvement in performance for TLDs, glue-heavy scenarios
- [Significant refactoring, which will facilitate adding QNAME minimization and Local Copy of the Root zone in 9.13.2]

BINDバージョンアップに向けて

■バージョンの選定

- BIND 9.11 ESV(**E**xtended **S**upport **V**ersion)
- BIND 9.12
- BIND 9.13

必要な機能を具備しているのであれば、
サポート期間の長いESVの選択がおすすめ。



引用: https://www.isc.org/blogs/bind-release-strategy-updated/

■機能の差分の確認と試験

- BIND9.9と9.11の機能差分　　今回はこちらを。
  - 機能試験
  - 性能試験(応答性能)
  - 応答差異の確認

フルリゾルバ機能関連(1/8)

・正確な情報と詳細は公式のドキュメントをご確認ください。

BIND9 Significant Features Matrix

https://kb.isc.org/article/AA-01310/0/BIND9-Significant-Features-Matrix.html

BIND 9.11 New Features

https://www.isc.org/downloads/bind/bind-9-11-new-features/

[Knowledge Base]　BIND 9.11 Features

https://kb.isc.org/category/219/0/10/Software-Products/BIND9/Features/BIND-9.11-Features/

・BIND 9.11(フルリゾルバ)への影響についてまとめました。

BIND9.9 9.11機能比較　(**後ほど配布の予定です**)

https://dnsops.jp/XX…..

・権威DNS機能関連、ログ周りの変更

JPRS 阿波連さんの資料をご確認ください。

フルリゾルバ機能関連(2/8)

※全ては網羅、説明しきれないので・・
　特に重要なもの、知っておいた方が良いと思われる部分を紹介します。

・OpenSSLのサポートが1.0.2e以上に
- コンパイル時に“—without-openssl”でOpenSSLを無効可能
- この場合、PKCS#11を代わりに使用しない限り、DNSSECは使用不可

マニュアルにはこう書いてあるけどCentOS 7のOpenSSL 1.0.1eでもコンパイル通った

・DNSSEC Lookaside Validation(DLV)の一部機能削除

DLVレジストリからDLVレコードを参照してDNSSEC Validation行う機能
- BIND 9.12でdlv機能の削除
- 2010年にルートゾーンが署名され、dlv.isc.orgの運用が終了した。

フルリゾルバ機能関連(3/8)

・DNSSEC: Negative trust anchors(NTA)

BIND9.11(フルリゾルバ)では、この機能はデフォルトで特定のドメインは指定されていない

- 特定のドメインのDNSSEC Validationを無効化する機能
- BIND 9.9 (Subscription版を除く)では、すべてを無効化することしかできなかった。
- 無効化はデフォルトで1時間、最長は一週間 (nta-lifetime)
- デフォルトで5分おきに、Validationが有効か確認。
  確認の結果、問題ない場合はntaを無効になる。(nta-recheck)

・Trust Anchor Telemetry https://kb.isc.org/article/AA-01528/0/BIND-Trust-Anchor-Telemetry-in-BIND-9.9.10-9.10.5-and-9.11.0.html

BIND9.11(フルリゾルバ)では、この機能はデフォルトで**有効** (BIND9.9.10から有効)

- KSK Rolloverに向けた機能。
  問い合わせ先の権威DNSに対して、自身が持っているトラストアンカーの情報を通知する。
- trust-anchor-telemetry no;で無効化が可能。

【参考】KSK2010で応答するリストが公開されました。

http://root-trust-anchor-reports.research.icann.org/rfc8145-addresses.txt

フルリゾルバ機能関連(4/8)

・DDOS Mitigation: DNSCOOKIE (previously called SIT)

BIND9.11(フルリゾルバ)では、この機能はデフォルトで**有効**です。

- パケットサイズの増大に注意。
- クライアント側のCookieは"send-cookie"オプションで無効にすることができる。
- サーバ側は"answer-cookie"オプションでBIND 9.11.4から無効化する機能が追加予定。
- 某有名ドメインで・・
- 他のISPで・・
- 弊社も・・
- 他にも・・

この機能の詳細な説明は権威DNS編をご確認ください。

フルリゾルバ機能関連(5/8)

IPv6 Changes in BIND 9.11.0, BIND 9.10.4 and BIND 9.9.9
https://kb.isc.org/article/AA-01349/0

・Resolver: Prefer IPv6 when querying authoritative servers

BIND9.11(フルリゾルバ)では、この機能はデフォルトで**有効**です。

- ２つの機能(preferred-glue,v6-bias)が加わった。
- preferred-glue

9.11:デフォルトはクエリを受信したIPバージョンを優先,9.9:デフォルトnoneで特別扱いなし

BIND 9.11のデフォルトでは、クエリを受信したIPバージョンのグルーレコードを優先させる。

たとえば、IPv6でクエリを受信した場合、AAAAレコードを先にadditional sectionに追加し、余裕があればAレコードを追加する。

- v6-bias (デフォルトは50ms)

フルリゾルバが応答時間に基づいて権威DNSを選択する際に、IPv6を優先して選択させる機能。

フルリゾルバ機能関連(6/8)

・Resolver: Cache prefetch

Early refresh of cache records (cache prefetch) in BIND
https://kb.isc.org/article/AA-01122/0

BIND9.11(フルリゾルバ)では、この機能はデフォルトで**有効**です。(prefetch 0;で無効化)

- TTLが切れる前に、再度問い合わせを行いキャッシュする機能
- 全てを永続的にキャッシュする機能ではなく、トリガーとなるクエリーが発生した場合のみ。

・DDOS Mitigation: SERVFAIL caching

BIND9.11(フルリゾルバ)では、この機能はデフォルトで**有効**です。(servfail-ttl 0;で無効化)

- ServFailとなった結果をキャッシュする。
- デフォルトは1秒、最大30秒

・Performance: Large server tuning

BIND9.11(フルリゾルバ)では、この機能はデフォルトで**無効**、--with-tuning=largeで有効化

- 高性能なサーバ向けパフォーマンスチューニング
- 低性能なサーバだと問題を引き起こす可能性がある。

フルリゾルバ機能関連(7/8)

・EDNS: Improved EDNS fallback processing

- BIND 9.10からの仕様変更
- フルリゾルバが新たに権威DNSに問い合わせる際に、EDNSのbuffer sizeを
  512byteで問い合わせを行う。
  成功した場合より大きなサイズでアドバタイズし、EDNSパケットサイズを調整する。
- cacheをdumpするとAddress database dumpセクションに調整に関する情報が確認可

Testing authoritative server support for EDNS and large UDP buffer sizes in BIND 9.10
https://kb.isc.org/article/AA-01350/0

・Management: DNSTAP query/response logging

- BIND9.11(フルリゾルバ)では、この機能はデフォルトで**無効**、—enable-dnstapで有効化

dnstap http://dnstap.info/
Using DNSTAP with BIND https://kb.isc.org/article/AA-01342/0

・EDNS Client-Subnet (ECS) for resolver

・EDNS Client-Subnet (ECS) option support for authoritative servers

権威DNSはExprimentalな実装なため注意！

フルリゾルバ機能関連(8/8)

・DDOS Mitigation: Fetch limits (DDoS mitigation for recursiveservers)
BIND 9.11(フルリゾルバ)では、この機能はデフォルトでは**無効**です。
BIND 9.9.8からコンパイルオプション指定時に使用可(with --enable-fetchlimit) ,
BIND 9.9.6-S1では指定なしで使用可

・水責め攻撃に対する対策機能
- fetches-per-server　The default is zero.（no limit)
- fetch-quota-params　default is 100 (fetches-per-server関連するパラメータ
- fetches-per-zone　The default is zero.（no limit)

2018年4月半ば頃から水責め攻撃が再開した模様

まとめ

BIND9.9は6月末ですが、セキュリティーパッチは数ヶ月リリースされる予定です。

・BIND9.9と9.11の機能差分について
  - デフォルトで影響のある機能が多数
  - 仕様変更もあり。
  - BIND9.11に移行済の方も、不要な機能が有効になっていないことを要確認
  - 機能差分を9.9に近づけるのではなく、必要な機能を吟味することが大事。

機能差分をうめるのが目的になってはいませんか？
9.9と同等/同等以上に名前が引けること、応答差分があれば原因調査することが重要！