

DNS Summer Day 2017

純国産！

XACK DNSのご紹介



2017-06-26

株式会社XACK 技術部 楠田 真矢

概要	製品名	XACK DNS
	コンセプト	純国産の商用DNS、脱BINDの受け皿となる
	棲み分け/強み	脆弱性の少なさ、日本語サポート、先進的なGUI、View対応
	役割	権威サーバ、キャッシュサーバ、フォワーダー、ENUM対応DNSサーバ
	提供形態	ソフトウェア、アプライアンス(予定)
性能	権威サーバ	100万ゾーン以上読み込み可能。 10万ゾーン、400万レコードの読み込みは18秒
	キャッシュサーバ	30万QPS/台 (Xeon® E5-2637v4(3.50GHz 4core 8スレッド)×2)
コスト	課金モデル	サーバライセンス (10Sに1ライセンス)
	初期コスト(最小構成)	50万円 (機能制限モデル) 、 100万円 (無制限モデル)
	継続コスト	2年目以降、初期コストの20%/年 (初年度は初期コストに含まれる)
保守・移行	サポート体制	弊社営業日平日の月曜日から金曜日までの 午前9時より午後5時まで
	脆弱性対応	メールアナウンス (日本語)
	EOLポリシー	新メジャーバージョンリリースの5年後にEOSL
	マイグレーション	BIND形式のゾーンファイルを読み込み可能。 BINDのnamed.confからXACK DNS設定ファイルへの移行ツール提供

機能・仕様

	ゾーンデータ保持形式	テキストファイル、インメモリDB	
	ローカルゾーン保持	可	
	水責め対策	受信制限機能	
	毒入れ対策	ソースポートランダムマイゼーション	
	DDoS対策	Rate Limit（権威側からの応答数）	
	サポートするRR Type	A, AAAA, NS, CNAME, SOA, WKS, PTR, HINFO, MX, TXT, SRV, NAPTR, SPF, AXFR, IXFR, TSIG, OPT, ANY	
	IPv6トランスポート対応	可	
管理	インターフェイス	Web GUI, CLI	
	統合管理	Web GUIで統合管理可能	
	ロギング	クエリログ、アプリログ、パケットログ（PCAP形式）	
	クエリログ検索	GUI, CLI	
DNSSEC	権威	署名更新	対応予定
		鍵更新	対応予定
		鍵更新方式	対応予定
		HSM対応	対応予定
	キャッシュ	Validation	対応予定
		TA更新	対応予定
		NTA対応	対応予定

DNS Summer Day 2017

純国産！

XACK DNSのご紹介

- 1. XACK DNSの特徴**
- 2. BINDからの移行**
- 3. DNS開発話**
- 4. 株式会社XACKの紹介**
- 5. ロードマップ**

XACK DNSの特徴

コード開発元比率

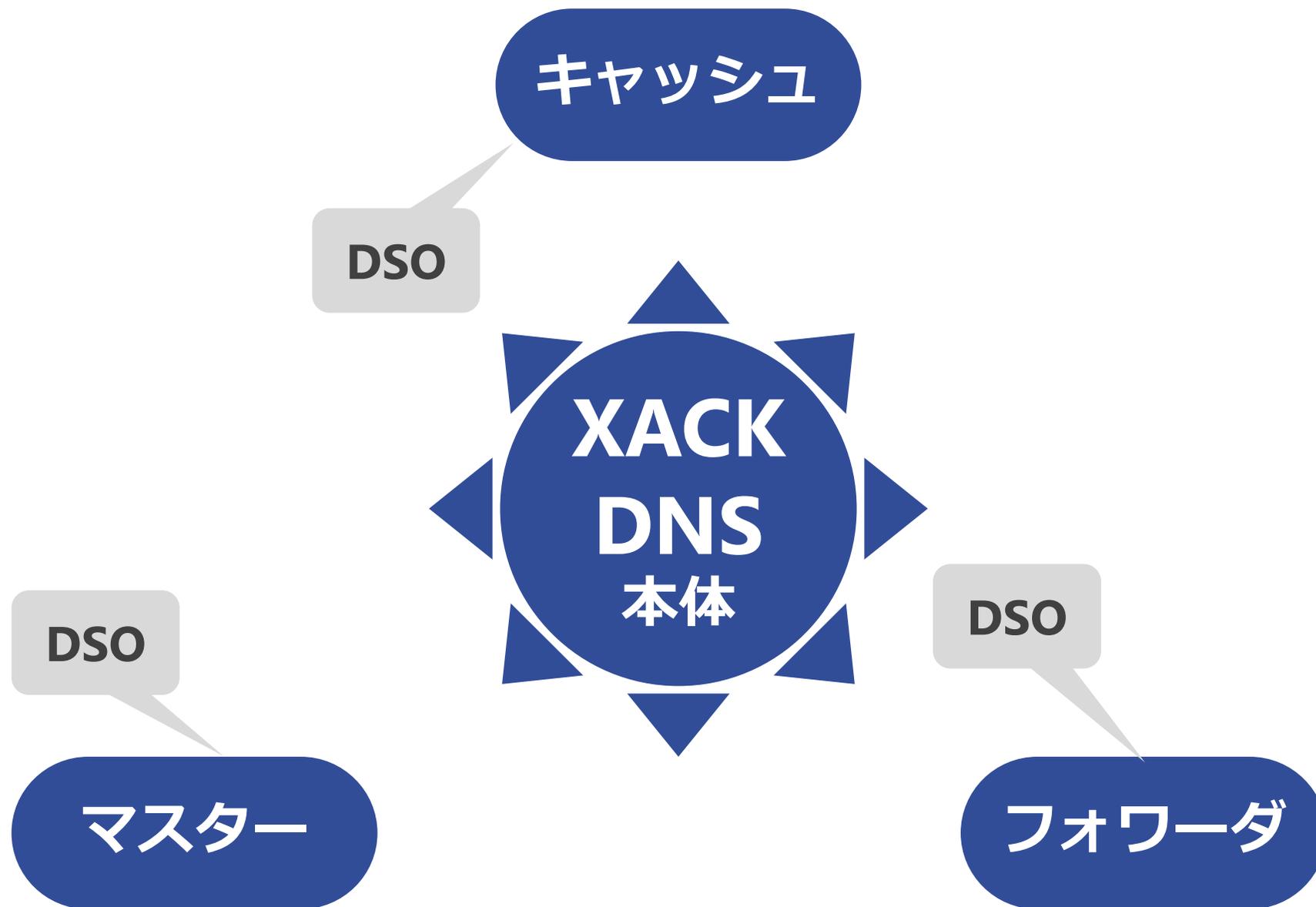


高い信頼性

緊急パッチ**0**件

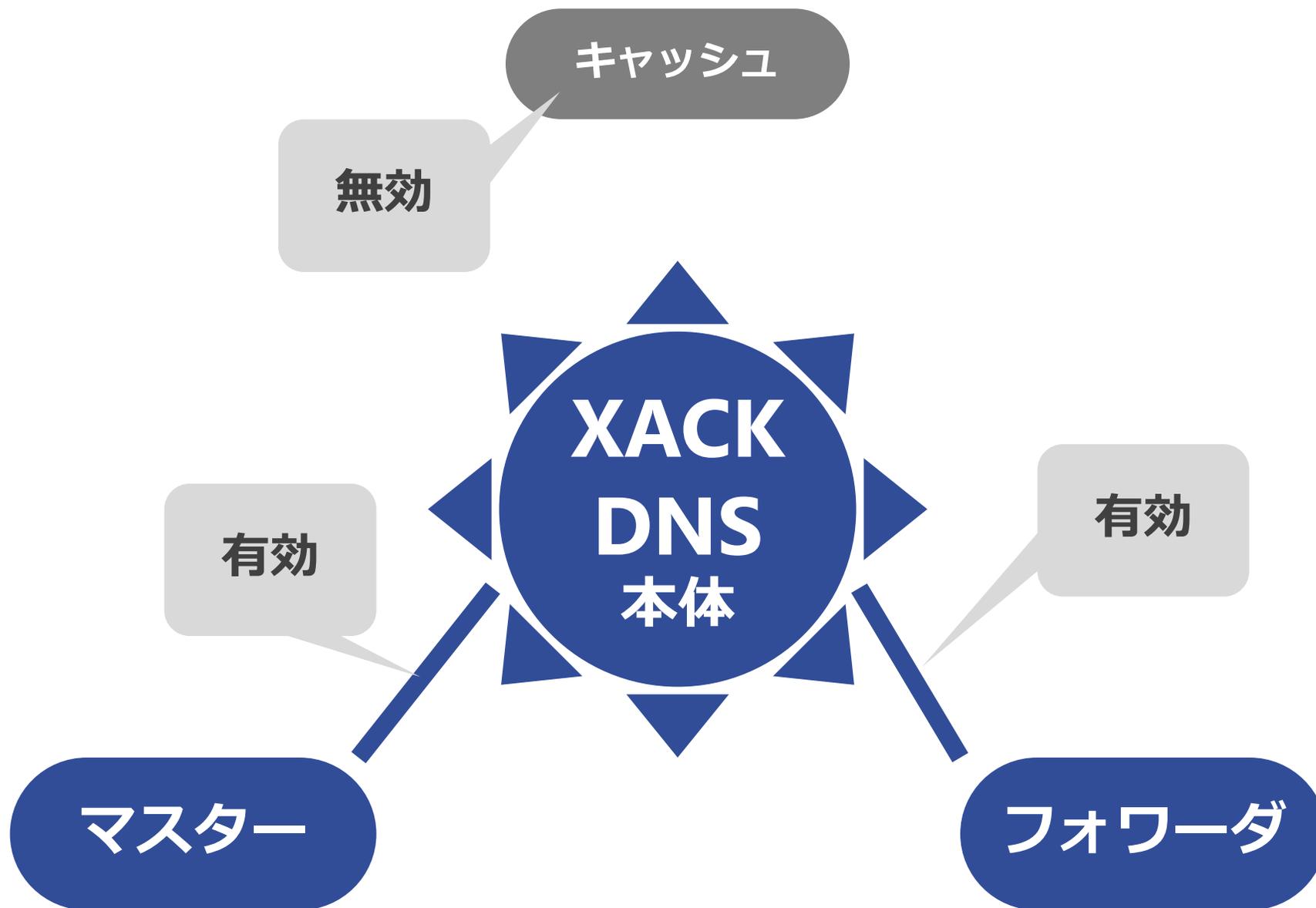
※ 2012年の販売開始時から、現在に致るまで

独立した各機能



※DSO = Dynamic Shared Object

独立した各機能



独立した各機能

キャッシュ

特定機能に**脆弱性**があっても

未使用なら**影響無し**

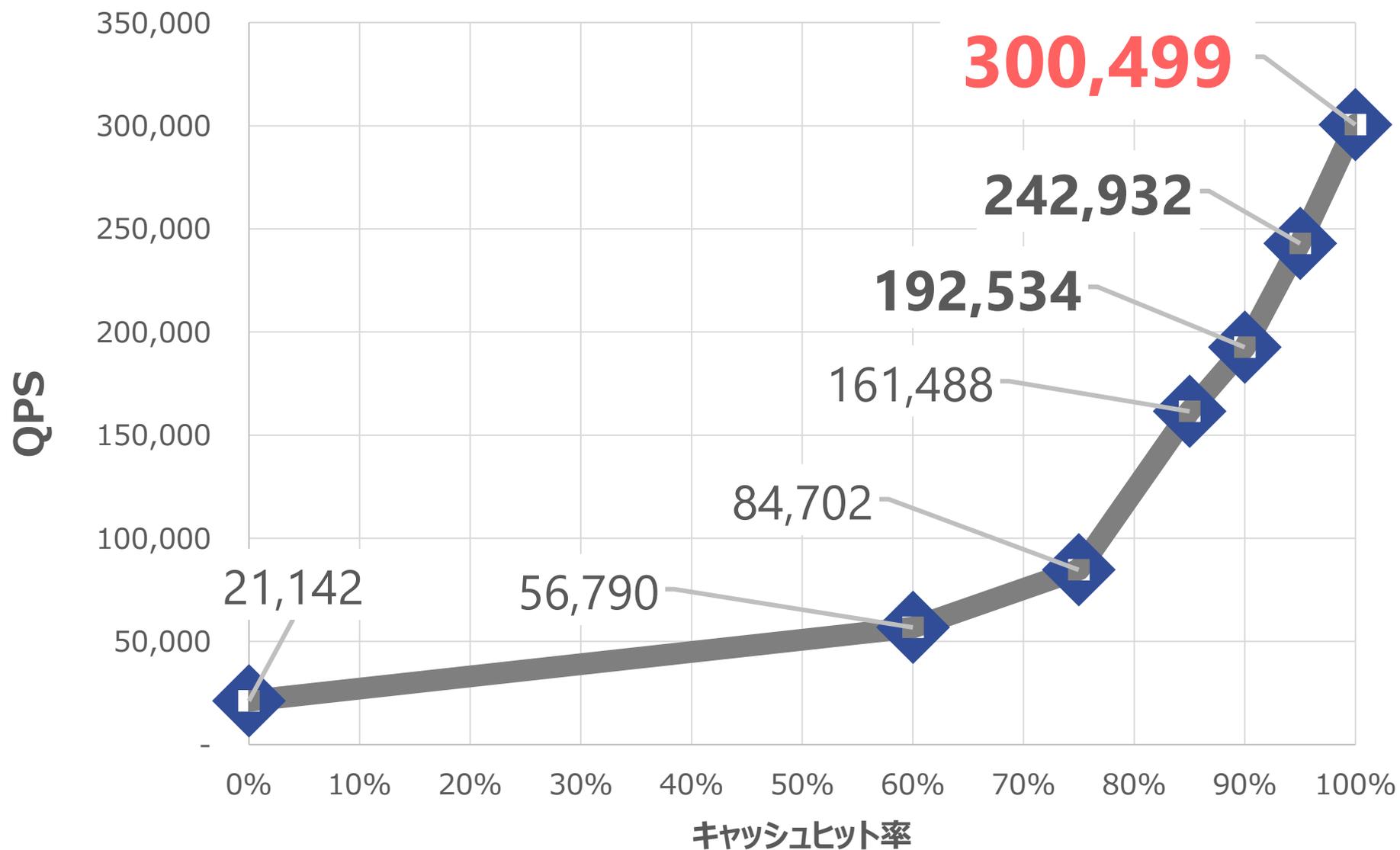


※現時点ではそのような致命的な脆弱性の存在は確認されておられません。

独立した各機能

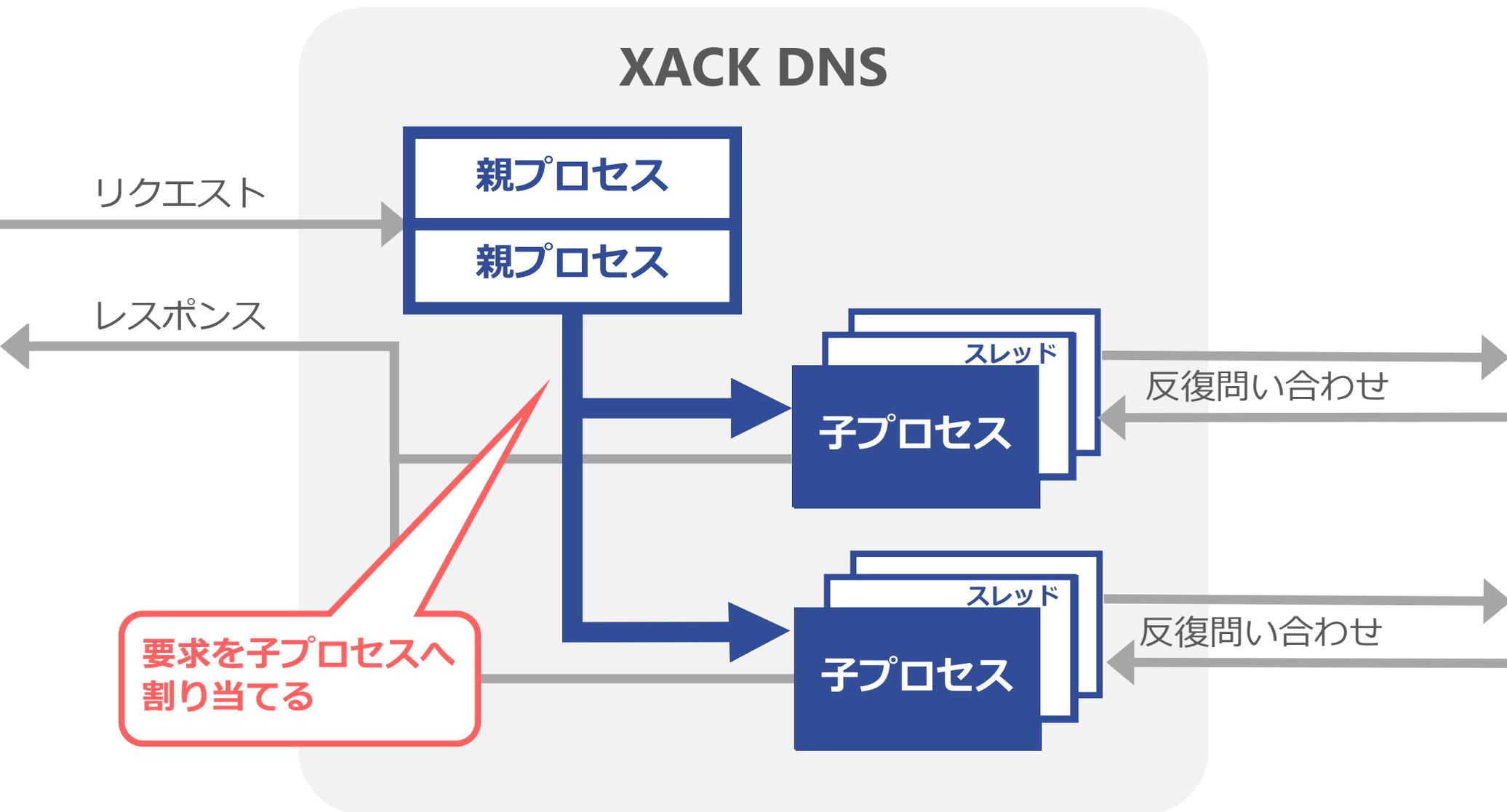
- ログモジュール
- 受信制限モジュール
- マスターモジュール
- スレーブモジュール
- ローカル名前解決モジュール
- キャッシュモジュール
- フォワーダーモジュール
- ゾーンモジュール
- ビューモジュール
- その他 (statistics、 filter、 rate、 policy)

高い処理性能

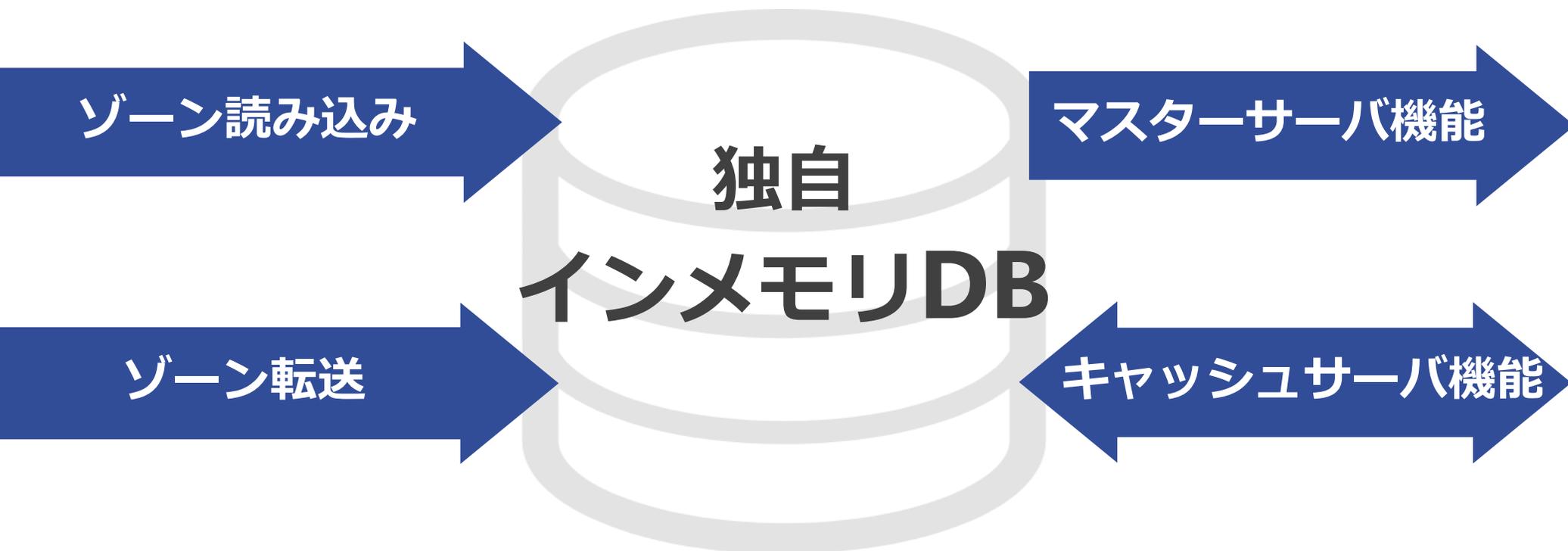


※ CPU: Xeon® E5-2637v4(3.50GHz 4core 8スレッド)×2、Memory: 64GB での実測値です。

マルチコアCPUを有効活用するアーキテクチャ



独自インメモリDB



大容量かつ高速

起動時間

18秒

10万ゾーン

400万レコード

DNSサーバーリスト 

[新規登録](#)

サーバー名	IPアドレス	状態	設定情報取得/反映日時	ロック						
xack-dns-01	192.168.3.179	起動中	2016-05-20 17:49:47	解除	運用メニュー	設定メニュー				編集
xack-dns-02	192.168.3.180	起動中	2016-05-20 17:59:42	取得	運用メニュー	設定メニュー			表示	編集
<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> 基本</div> <div style="text-align: center;"> マスター</div> <div style="text-align: center;"> スレーブ</div> <div style="text-align: center;"> キャッシュ</div> <div style="text-align: center;"> フォワーダー</div> <div style="text-align: center;"> グループ</div> <div style="text-align: center;"> クライアント</div> <div style="text-align: center;"> フィルター</div> <div style="text-align: center;"> ポリシー</div> <div style="text-align: center;"> 拡張</div> <div style="text-align: center;"> 反映</div> </div>										
xack-dns-03	192.168.3.181	エラー	DNS設定情報未取得	取得	運用メニュー	設定メニュー			表示	編集
xack-dns-04	192.168.3.182	起動処理中	2016-05-20 18:20:23	取得	運用メニュー	設定メニュー			表示	編集
xack-dns-05	192.168.3.183	停止処理中	2016-05-20 18:24:59	解除	運用メニュー	設定メニュー			表示	編集
xack-dns-06	192.168.3.184	停止中	2016-05-20 18:25:44	解除	運用メニュー	設定メニュー				編集
xack-dns-07	192.168.3.185	接続エラー	2016-05-20 18:40:08	取得	運用メニュー	設定メニュー			表示	編集
xack-dns-08	192.168.3.186	エラー	2016-06-14 11:00:03	取得	運用メニュー	設定メニュー			表示	編集

付属 Web インターフェイス

マスターゾーン編集

zone_name

ゾーンサイズ上限

保存

レコードリスト ※レコードはドラッグアンドドロップで順序を入れ替え

No	分類	名前	TTL							
1	\$TTL		3600							レコード操作
2	RR	@	TTL		IN	SOA	serial :	2017062701	+更新	レコード操作
シリアルを更新してください。										
							mname :	ns		
							rname :	kusuda.xack.co.jp.		
							refresh :	8	H	▼
							retry :	4	H	▼
							expire :	1	W	▼
							minimum :	10	M	▼
3	RR	オーナー名	TTL		IN	NS	ns			レコード操作
4	RR	ns	TTL		IN	A	192.168.3.			レコード操作

適切なIPv4アドレスではありません。

リソースレコード追加

レコード種別

リソースレコード
\$TTL
\$ORIGIN
\$GENERATE
\$INCLUDE
コメント

レコードタイプ

A
NS
CNAME
WKS
PTR
HINFO
MX
TXT
AAAA
SRV
NAPTR
SPF

追加

キャンセル

編集

最終更新 : admin / 2017-06-27 09:37:47

登録件数 : 4 / 最大件数 : 2000

ゾーンファイルをインポート

編集モード切替

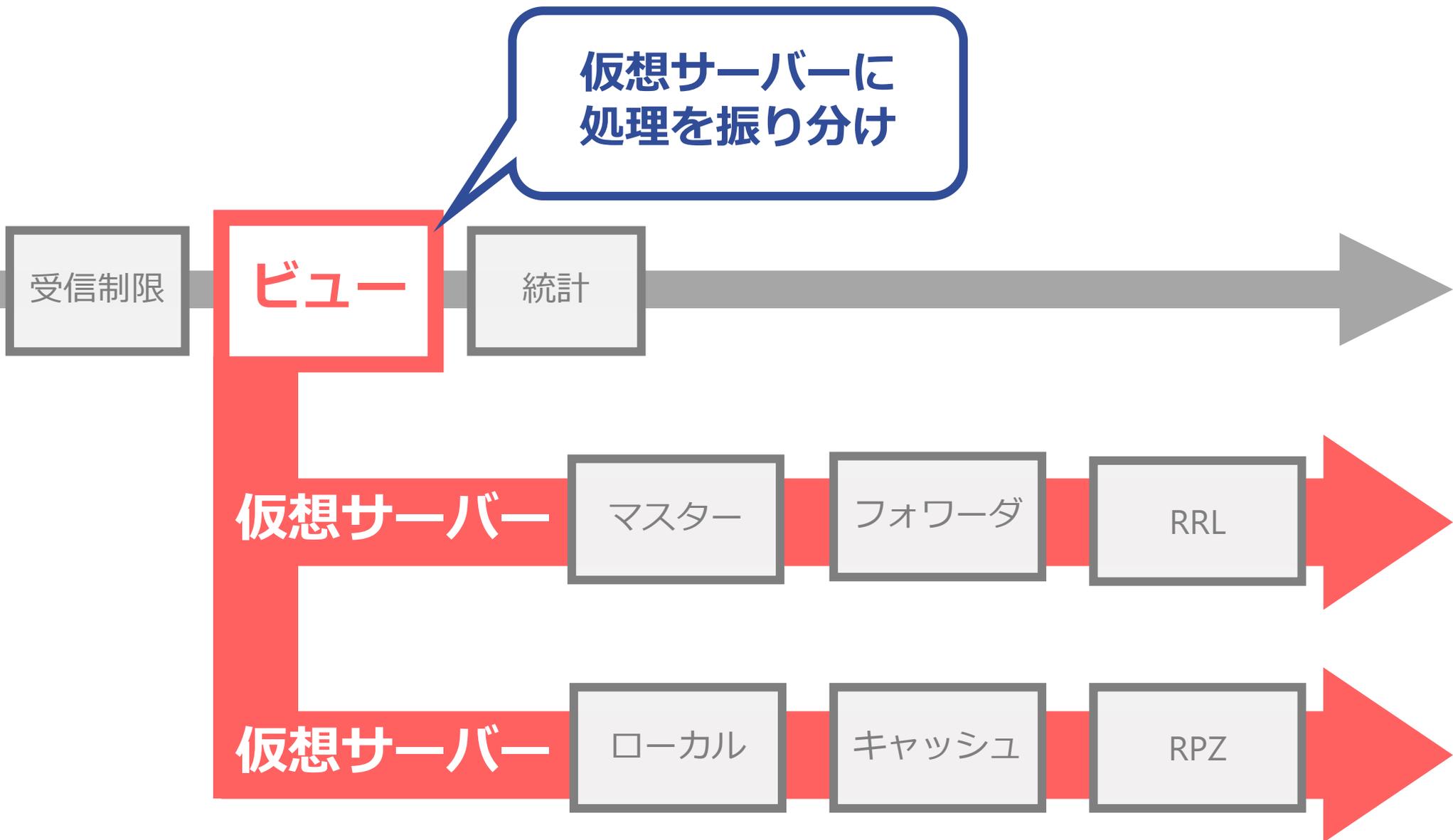
日本語サポート

1. **ドキュメント**
2. **Webインターフェース**
3. **お問い合わせ**

全て日本語対応

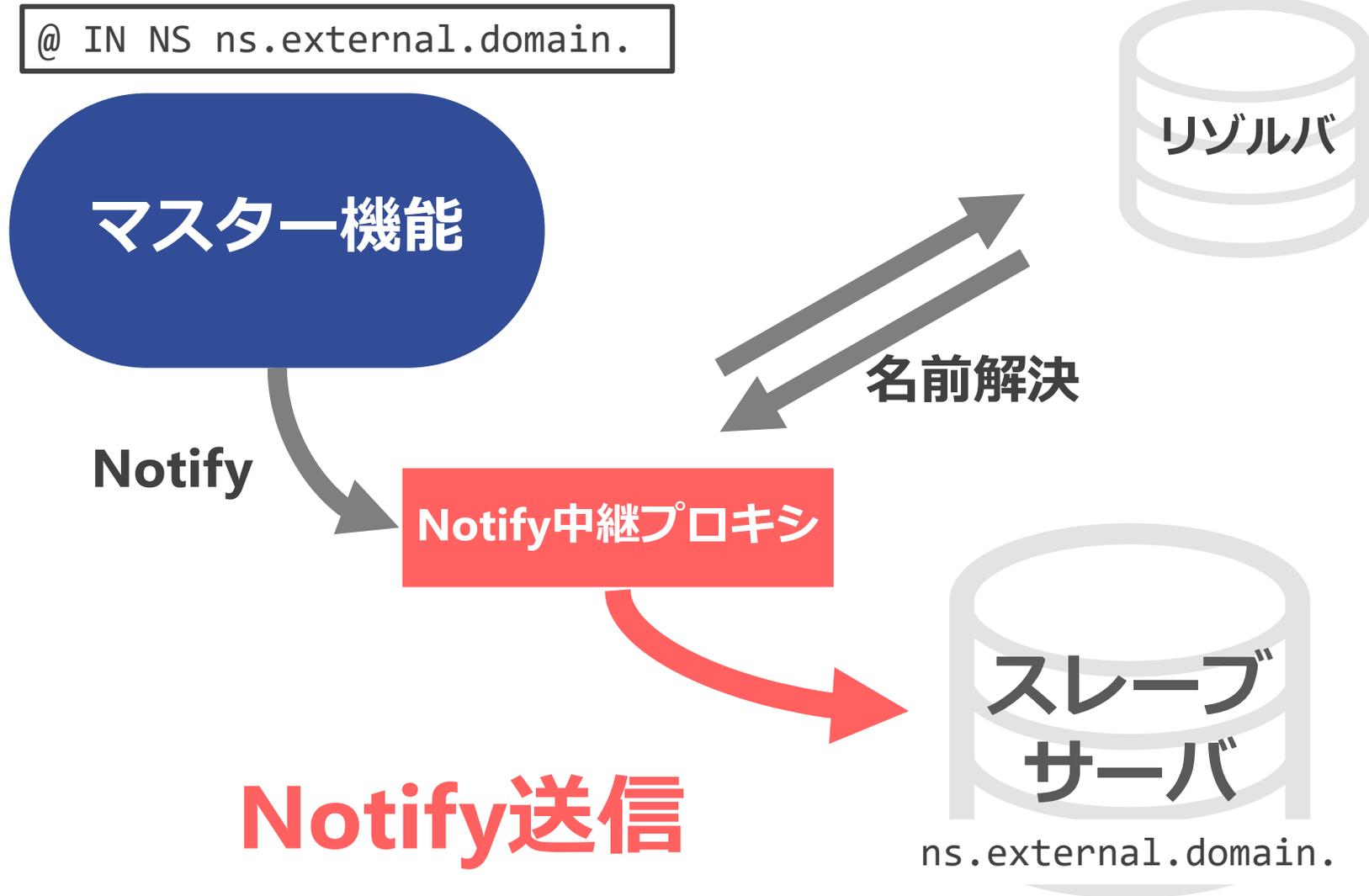
BINDからの移行

仮想サーバー機能

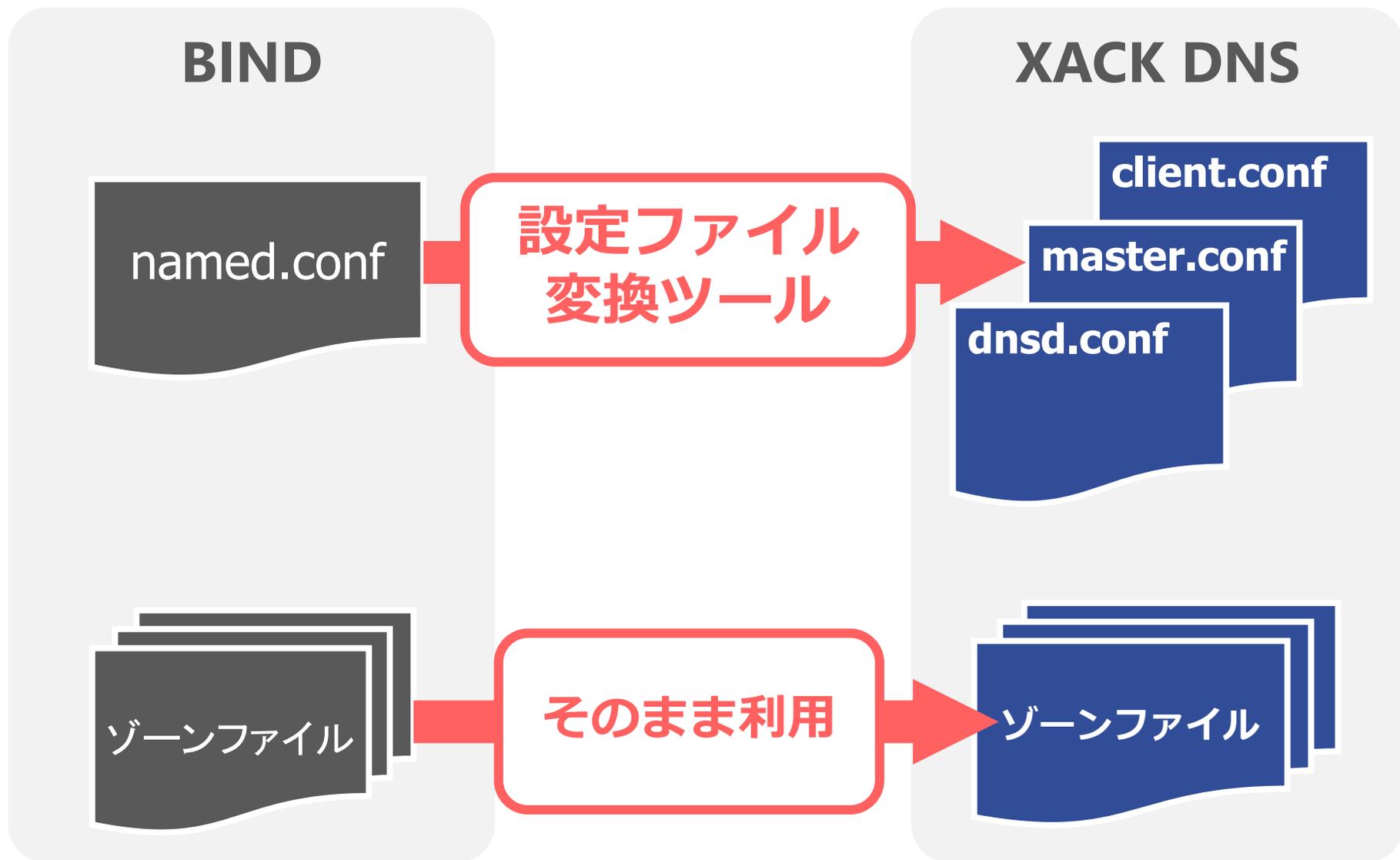


※BINDのビュー機能の上位互換になります。

外部NS名Notify送信機能（開発予定）



設定ファイル変換ツール



DNS開発話

ゾーンファイル対応

- **レコード先頭に「#」**
 - コメントを意図してる？
- **レコード先頭に「//」**
 - C++ ?
- **シブリンググループ**
 - 実装の対応が大変

変な権威DNSサーバーの存在 (1/4)

- **AAAAを問い合わせているのにA応答**
 - 何故か他のRTYPEにはNODATAを返す
- **Aに応答するがAAAAにはNXDomain応答**
 - AAAAフィルター？
- **IPv4アドレスではAを応答してIPv6アドレスではAAAAを応答**
 - 何か勘違いしている？
- **Queryを書き換えた応答をしてくる権威**
 - やめて

変な権威DNSサーバーの存在 (2/4)

- **CNAMEがゾーン頂点**
- **CNAMEが他レコードと共存**
- **CNAMEが複数**
 - むしろ設定できる実装の詳細が気になります
- **キャッシュっぽい挙動をしてる権威**
 - もはや権威ではない
- **NXDomainだが回答は付けてくる権威**
 - 何故そうなった
- **EDNS0付だと壊れた応答をしてくる権威**
 - AnswerにOPTレコードが、Additionalに回答が入る。

変な権威DNSサーバーの存在 (3/4)

- **CLASSをANYで問い合わせるとANYで応答**
 - 受けたQCLASSをそのまま使っている様子
- **NSレコードのRDATAが『localhost.』**
 - ADDITIONALに 『localhost. IN A 127.0.0.1』

変な権威DNSサーバーの存在 (4/4)

- **より深いゾーンの権威応答を返してくる**
 - やはり実装が気になる。
- **権威サーバーガチャ**
 - 再帰問合せ先によっては絶対に解決できない袋小路
- **2000個以上のPTRレコード応答**
 - 仕様の範疇ではありますが
- **俺はルートサーバーだ**
 - 違います

株式会社XACKの紹介

自社開発商品群

採用実績

RADIUS

ソフトバンク
Wi-Fi スポット

docomo Wi-Fi

他、移動／固定系
通信キャリア様

DHCP

auひかり ホーム

Wi2 300

他、移動／固定系
通信キャリア様

DNS

(非開示)

他、移動／固定系
通信キャリア様

企業プロフィール

会社名

株式会社XACK

設立

2003年4月

所在

東京都千代田区神田小川町

キャッチコピー

『誰もがXACKを通過する』



ロードマップ

ロードマップ

1.3 基本機能

1.4 rateモジュール

1.5 マルチマスター、マルチスレッド

1.6 RPZ対応、受信制限機能

現行版

1.7 **ビュー機能**

1.8 シブリンググループ対応

1.9 ENUM DNS対応、外部NS名Notify対応

2.0 **DNSSEC**



付録

各種攻撃対策

攻撃手法	概要	XACK DNSの対応
DNSキャッシュ ポイズニング攻撃	キャッシュサーバに偽のDNS情報をキャッシュさせることで、偽のウェブサイトなどに誘導する。	ソースIP、ソースポート、トランザクションIDのランダム化
DNS Amp攻撃 DNSリフレクター攻撃	多数のコンピュータから大量のデータを送りつけて対象を麻痺させるDDoS攻撃のひとつ。	Response Rate Limit(RRL)機能
水責め攻撃	ランダムに生成した存在しないサブドメイン名を大量に問合せることによって権威サーバを麻痺させる。	受信制限機能

サポートするRFC準拠の基本機能

機能	権威サーバー	キャッシュサーバー	参考
設定ファイル読み込み	○	○	独自形式
ゾーンファイル読み込み	○	○	RFC1035
ゾーンファイル\$GENERATE文	○	○	BIND形式
権威ゾーン回答	○	localhost 特定アドレスの逆引き	RFC1912, 1918, 3849, 3927, 4159, 4193, 4291
ゾーン転送 (AXFR)	○	—	RFC1034, 5936
ゾーン転送 (IXFR)	○	—	RFC1995
ゾーン変更の即時通知(NOTIFY)	○	—	RFC1996
キャッシュ	—	○	RFC1034, 1035
ワイルドカード	○	○	RFC1034
ネガティブキャッシュ	—	○	RFC1034, 2308
リゾルバー	—	○	RFC1034
ラウンドロビン	○	○	RFC1794
ENDSO	○	○	RFC1035, 6891
ローカル名前解決機能	—	○	RFC6303, 6761
Response Rate Limit機能	○	△(非推奨)	ISC-TN-2012-1-Draft2
Transaction Signatures (TSIG)機能	○	○	RFC2845
Response Policy Zone	—	○	ISC-TN-2010-1-B3