

例の有償製品でDNS構築してみた。

KDDI株式会社

2018年6月26日



- 自己紹介
- 発表の目的・免責

- なぜ移行することにしたか

- 移行先製品

- 各製品について
 - 移行してよかったところ。
 - BINDと比較して。
 - 移行時の注意点。

■発表者

●名前

- ・松本 章

●所属

- ・KDDI株式会社 IPネットワーク部

●お仕事

- ・DNSとNTPのシステムの設計や構築をやっています。

■発表の目的

- BIND以外の有償DNSプロダクトを商用導入した結果を技術者視点で振り返り、導入事例の共有を行う。

■免責事項

- 記載事項の正確性や再現性を保障するものではありません。
- 内容はメーカー・ベンダの公式回答・見解ではありません。
- 本資料作成・公開にあたりメーカー・ベンダへの事前確認やスポンサー協賛を含んでおりません。
- ただし、DNS Summer Dayがスポンサー協賛イベントであることを鑑み、表現等に配慮している点がございます。

■BIND脆弱性多すぎ！

■台数多すぎ！

- 台数で性能を稼ぐ必要があるが、脆弱性出るたびに複数台のBINDのバージョンアップは大変。
 - ・年によっては片手では数え切れない脆弱性対応を、両手両足で数えられない台数分実施するのは苦痛。

■しかも落とされてDoS状態は非常にマズイ。

- 1時間超のサービス影響⇒総務省報告

■Nominum Vantio CacheServe 7

- フルサービスリゾルバ用

■BIG-IP DNS

- フルサービスリゾルバ用
 - ・BIG-IP内部のBINDのことではありません。

■XACK DNS

- 権威・キャッシュ権威共用DNS用。

Nominum Vantio Cache Serve 7

■噂どおりですが、運用が非常に楽。

- 攻撃に強く実質メンテフリー。
 - ・ 社内の運用部門からとても好評。
- BIND脆弱性が出ても怖くない。

■超高性能

会場限り

■導入費・維持費が高額。

- 噂とおりです。

■CPU物理コア単位でライセンスキャップがかかるため、CPUを高性能にすればするほど、性能が引き出せる。

- 実装に注意が払われておりコアあたりの性能が段違い。
- TurboBoost時より通常動作周波数が重要。

■内部にゾーンの的なものを持てるが要ライセンス。

- 特定用途(児ポ対策等)以外では有償。

- **高性能がゆえに限界性能試験が難しい。**
 - 試験中に隊列並べた権威サーバが先に落ちてしまう。
 - 試験環境・トラフィックパターンを作るのが難しい。

BIG-IP DNS

■BINDの脆弱性を受けない。

- BINDは同梱されているがBIG-IP DNSはBINDコアではない。

■LBが無くても2台以上あれば冗長が組める。

- LB同様、複数台で設定同期可。

■遠くからでもラックがわかりやすい。

- 最近明るさがすこし控えめになったような…

■DNSを処理する箱として考えた場合決して安くない。

- LBが不要になると考えれば高いわけでもない。

■処理性能と機能(セキュリティ)はトレードオフ。

- 使いたい機能とトラヒックを明示しましょう。

- **キャッシュ領域がデフォルトだと小さい。**
- **BINDと比較して実装されていない機能があるので注意。**
- **サービスIPが多数ある場合、クラスタの組み方に注意。**
 - **設計に工夫が必要。**
- **Domain Name Blocking対応が難しい(手間がかかる)。**
 - **ブラックリストは追記出来ず、全削除・全追加しか出来ない。**
 - **しかもブラックリストはプライベートIPの逆引きゾーンと共存。**

XACK DNS

■BIND脆弱性の影響を受けない。

■キャッシュ・権威共用DNSの運用が出来る。

- なかなか分離しきれない方でも候補になると思います。

■BINDみたいな機能メガ盛りのDNSではない。

- BINDをバリバリにチューニングして使いこなしていると移行が厳しいかもしれません。
- BINDを典型的な使い方をしている分には困らないと思います。

■今後の開発に期待

- 対応レコード種類が少なめ
 - ・ 現状で使用しているレコード種類が多いと移行が難しくなります。
- DNS防御機能はBINDと同等。
 - ・ 例えば、PRSD(水責め)を自動でいい感じに防御してくれるような機能はありません。

■リソースレコードの対応数が少ない。

- ゾーンによっては注意が必要

■ゾーンデータの書式チェックがBINDより厳しい。

- BINDのゾーン設定を手動で編集している方は特に要注意。

■BINDと動作が異なる点はある。

- BINDからの移行時は想定通りの動作しているか要確認。
 - ・ その動作、あなたの想定とおりですか？
 - ・ なぜ、BINDがその動作をするか考える必要がある。

Designing The Future



ご清聴ありがとうございました。