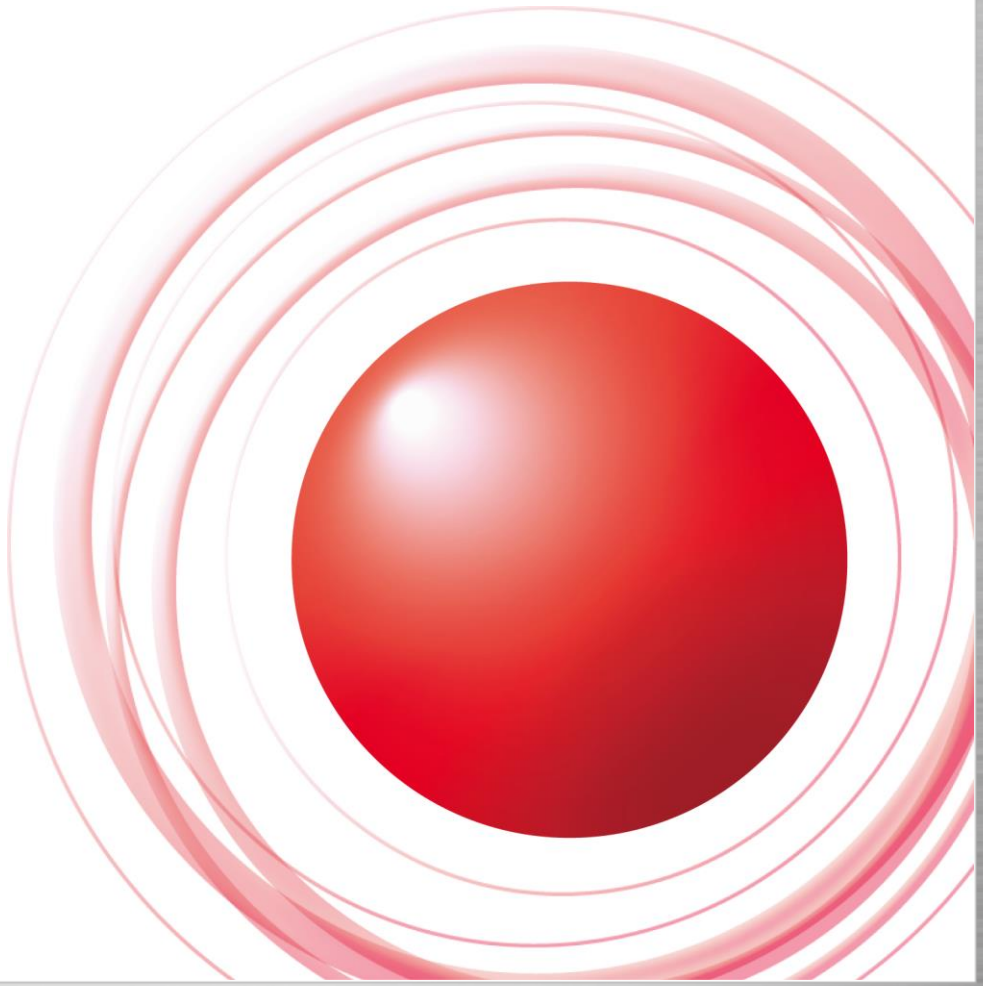
BIND辞められない理由 Q&A

IIJ
Internet Initiative Japan



株式会社インターネットイニシアティブ
島村 充 <simamura@iij.ad.jp>

Ongoing Innovation

アンケートご協力ありがとうございます

- 50件を超える、たくさんの回答を頂きました。
  - みなさんのBIND9への 愛♥ を感じました
    - 語り足りない人は懇親会で語ってください
- 全部は紹介しきれませんので、似ているのはまとめます

(取り上げられてなくても怒らないでくださいね)

おさらい

- BIND9を辞めたい理由とは??
  - DoS脆弱性が多すぎるから
    - 運用コストが高い
    - DoSられて可用性が損なわれる可能性がある
- BIND9を完全に捨てる必要はない
  - 周辺ツール (DNSSEC署名周り、dig など)
  - 複数台あるうち、半分だけ変える
  - (権威の場合)hidden masterはBIND9にして、slave(edge)は混在 とか
- パフォーマンスに関しては議論しない
  - まぁ、大概の場合BIND9に勝りますが

分類

- BIND9固有の機能に依存している
  - view, 権威・キャッシュ兼用, RPZなど
- クエリログ
- 周辺ツール、作業手順などの改修が大変
- 学習・教育コスト
- ログ・統計情報
- デファクトスタンダードの安心感
- 機能面の安定性
- 継続性
- 情報の豊富さ

分類

- オレンジさんありがとう
- 脆弱性、みんなで渡れば怖くない
- ベンダー・SIerが対応していない
- 有償サポートがある
- 社内(上司)のしがらみ
- 変わり種

BIND9固有の機能に依存している

- 権威・キャッシュ兼用
- そもそも、権威・キャッシュを兼用を継続したい理由とは? 変更(分離)できない??
  - キャッシュのIPアドレス変更はとても困難
  - 権威はIPアドレス変更できる (何度かやってます)
    - 困難な場合も (権威が顧客masterとnotifyをやりとりするslaveの場合)
  - PowerDNSにRDbitの立ったクエリを転送する機能があるらしい
- サーバーの台数を減らしたい?
  - 昨今、仮想化ありますよね

というわけで、教えてください

BIND9固有の機能に依存している

- view

viewってどういう時に使います?

- メールのMSAを国外と海外で同じ名前で別IPアドレスにしたい
- 簡易GeoIP
- 児ポブロックのOEM先ごとのON/OFF
- 社外用と社内用を1台でまかないたい?
  - 分けても、社内のキャッシュDNSサーバでforwarderで社内用権威サーバに向ければOK

BIND9固有の機能に依存している

- RPZ
  - unbound: local-dataで上書きできるが、RPZのように一箇所で集中管理という訳にはいかない。
    - deployの仕組みを作る必要がある
      - そこまで障壁になります?
  - Knot DNS Resolverなら対応しているそうです

BIND9固有の機能に依存している

- AAAA filter
  - もう止めていいじゃないですか…
    - Unboundにpatchがあり (動作未確認)
      - 縦読みする限り、Aがある場合だけ削除
    - Nominum Vantio CacheServeで対応
      - bindより柔軟にpolicy設定が可能

BIND9固有の機能に依存している

- Dynamic Update
  - nsdは対応していない
  - PowerDNS, Knotは対応
  - Dynamic Updateを受けるのはACLをかけたBIND9, slaveは他のソフトとか

BIND9固有の機能に依存している

- ゾーンファイル
  - $ORIGINの省略
    - nsd, PowerDNS, Knot、みんな大丈夫。
      - 昔のKnotでダメだった
  - $GENERATEマクロ
    - PowerDNSはそのまま読み込む(解釈する)
    - named-checkzone –Dで展開後のゾーンデータ
    - hidden master: BIND9,
      slave(edge): 他のソフト

BIND9固有の機能に依存している

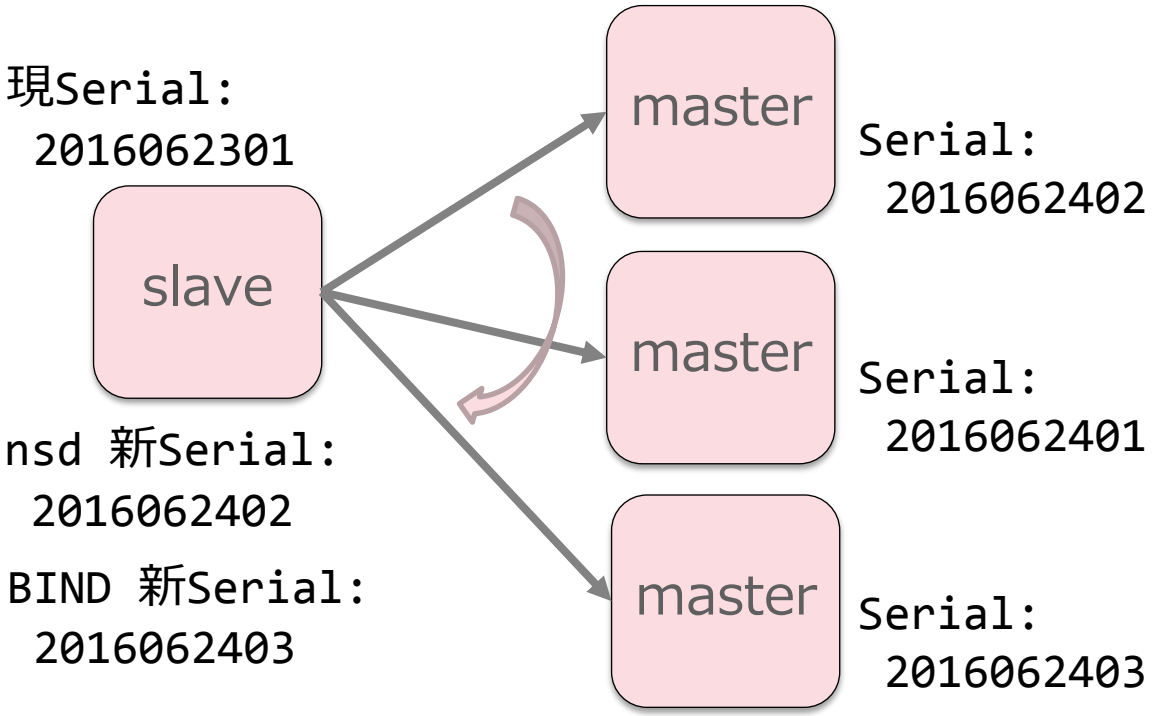
- DNSSECのsmart signing
  - 他のソフトでは無し
  - dnssec-siginzoneが署名されたゾーンファイルを生成するので、他のソフトでも平気なはず?
- DNSSECのautomatic signing, inline signing
  - named自身が署名するので、他のソフトでは無理
    - OpenDNSSECつかうとか
    - hidden master: BIND9, edge: 他のソフト

BIND9固有の機能に依存している

- 設定ファイル
  - 書き換えるのが大変
  - 設定ファイルを書き換えるツールの対応が…
  - bind2nsd
- 「ある用途で特殊(experimental)なRRを使っています。多分BINDしか対応していません。」

BIND9固有の機能に依存している

- 「マスターが複数な環境でslaveを運用している場合、BINDだと複数のマスターのうち一番Serialが大きいものを取ってきてくれるが、BIND以外の実装だと自分(slave)より大きいSerialのものにあたるとそこで終わってしまう」



BIND9固有の機能に依存している

- 「slave側でrefresh timeを操作する方法がない。（max-refresh-timeやmin-refresh-time等）」
  - masterの変なSOAの設定(refresh 1秒とか)に引きづられるのを防ぐため
    - nsdのpatchかいたよ by 山口さん
  - slave間で転送失敗した時でも早く末端に伝搬するように

クエリログ

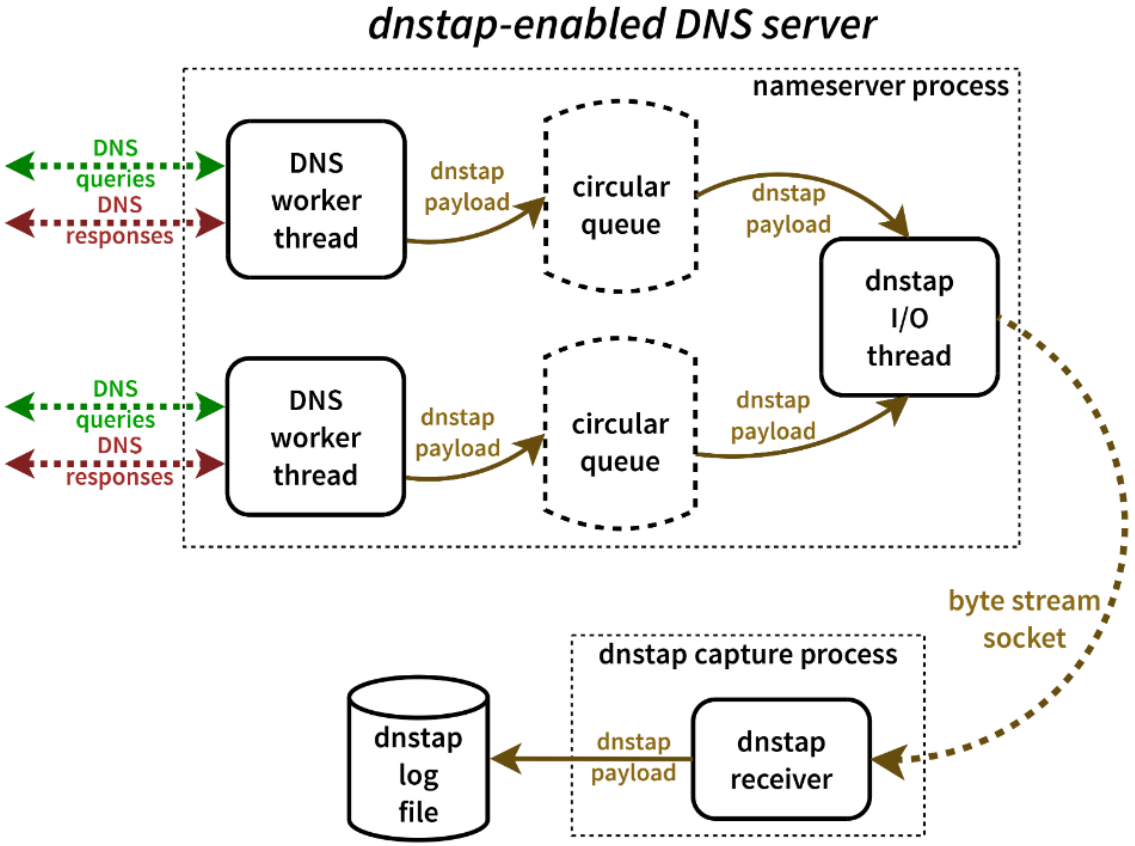
- 「クエリ」ログなので、応答はわからないんですけど、それはいいんでしょうか…
  - 結局トラブルシュートはtcpdump, tapする羽目に
- クエリ量が多いサーバーほど性能劣化(応答,I/O)が激しくて、非現実的
  - tapしたり、条件を絞ってtcpdump
- unboundは出せる
- PowerDNSも出せる
- nsdは無理(対応予定なし), Knotも無理

クエリログ

- 時代はdnstap

  “high speed DNS logging without packet capture”

  - 対応済み
    - Unbound
    - Knot
  - 対応予定
    - BIND9.11
  - 計画中
    - nsd
    - PowerDNS



周辺ツール、作業手順などの改修が大変

- 「運用ツールがBINDに特化している（設定系、アラート系）」
- 「社内の各種運用手順書の修正がたいへん」
  - “脆弱性対応の工数 << 作りなおす工数”なら仕方ないですね。BINDと心中してください。
- 「bindとbind以外のアプリを併用した時の作業コスト（設計、検証、運用、ログ監視）が倍になる」
  - ダイバシティによる可用性の向上を採るか、運用コストの少なさを採るかですかね

周辺ツール、作業手順などの改修が大変

- 「他のものを使う場合、レコード編集, ゾーン追加削除, バージョンアップ等に関する再教育や手順書更新が必要。BIND を前提とした各種連携プログラムも対処が必要。これらにかかるコストを短期 (1, 2 年) で回収できるとは思えない。中長期で考える場合、これより優先されるタスクが少なくない。新規システムなら良いと思うが、現時点ではまだ既存システムの変更に至る理由が足りないのではないか。」

学習・教育コスト

- 「 運用部隊に対して新しい環境の手引き(設定、障害対応ほか)を準備して再教育するのが面倒」
- 「運用チームがBINDにしか対応出来ないので」
  - 有料セミナーがあったら参加しますか?
  - というか、DNSサーバーソフト以外はどうしてるんですか?(つぶらな瞳)
    - 未来永劫同じソフトを使い続けろというんです?
- 「せっかくBINDを勉強したのにという気持ちがある」
  - お、おう…

ログ・統計情報

(クエリログはおいておいて…)

- 「BINDのほうがログ出力パターンが柔軟にできる。」
- 「statistics-channelが便利」
  - XML/JSONフォーマット
  - ゾーンのシリアル値一覧が取れる
    - master-master環境の差分チェックがdigだと遅い
    - nsdでもmaster-slave構成なら取れる

ログ・統計情報

- stats情報が豊富 (unboundだと足りない)
  - cache hitとかrecursive clientの数とかはUnboundの方が取りやすいと思う。
    - 特に時間毎のrequestlistの最大値total.requestlist.maxが取れるのが嬉しい。

デファクトスタンダードの安心感

- 「なんとなく安心感がある」
  - あのcrash bugの多さで安心感？！？？！
    - 冗談です
  - 細かい挙動が利用者数が多いから安心?
    - キャッシュに限って言えば、法人向けに3年以上運用して問い合わせが来たことなし
- 「 BIND以外のソフトウェアを使っている他社の実績が公開されておらず、安定稼働しているか不明なため使うことについて不安がある」

  nsd: root-server, Knot: .cz,

  PowerDNS: Wikipedia, チェコのT-Mobile

  Unbound: 世界中のFreeBSD10,IIJで3年以上

機能面の安定性

- 「BIND9で脆弱性が出てアップデートに迫られても、大きな動作変更が無いことが多く、アップデートに伴う副作用が出ないように配慮されてる(UnboundやNSDは、結構大きな変更が入ることがある)」
  - 脆弱性対応だけしたければpatchあてればいいんじゃなでしょうか
    - unbound, nsd, PowerDNSは脆弱性対応だけのpatchが出ていた

継続性

- bind以外は継続性とかが不安
  - BINDもいつまで安泰かは…
    - 開発者とか開発者とか
    - ライセンス変えるとかいう話もありますし

情報の豊富さ

- 「JPRS指定事業者向けセミナーで設定例や動向がbind中心」
  - JPNICさんのBGPセミナーとかだと色々なメーカーに対応しているそうです

    JPRSさん、よろしくおねがいします!
- 「ネットの様々な情報はBINDが多い(特殊な設定や関連ツールなど)」
  - まぁそうかもしれませんねえ…
  - 「バッタ本」に相当する本がない (誰か(略))
- 「DNS仕様検討する際の情報量が多い」
  - パフォーマンス比較とかは色々出回ってます

情報の豊富さ

- 「DNS系イベントの情報がBINDベースのものばかりで、『とにかくBINDが推奨ソフトウェアである』というイメージがある」
  - 最近の注意喚起の設定例にはBIND以外も書いてあります
  - 児ポブロッキングの設定例もBIND/unbound両方書いてある

ていうか、このコマでBIND9は一切オススメしてませんから!!

オレンジさんありがとう

- 「脆弱性が出た時に迅速に情報が多く出回る」
- Unbound, PowerDNS, nsd, Windows DNSもちゃんと(かなり早く)配信されています
- 一方で…、BINDに関しては発信が「義務」

■JPドメイン名登録管理業務移管契約に関する覚書 別紙

JPドメイン名登録管理業務移管契約第13条第1項、第2項及び第4項から第10項までの各項に定める株式会社日本レジストリサービス（以下「JPRS」という。）の責任事項について、以下を記した資料をJPRSから社団法人日本ネットワークインフォメーションセンター（以下「JPNIC」という。）に提出する。

1-4. DNSに関する重要情報の発信実績

+ 報告対象期間中の、DNSに関して「JPRSが知りえた情報で重要と判断したもの」(注)の日本語による情報発信実績
  - 情報発信した内容の全文（Webページの印刷）

注：ISCからのBINDのセキュリティに関する情報で、深刻度が「高（High）」以上であるもの

JPドメイン名登録管理業務移管契約に関する覚書

他のものがベストエフォートでなのか、任務なのかはわかりませんが

脆弱性、みんなで渡れば怖くない

- 「深刻な脆弱性が出た時には、世界中で同様の事象が発生しているという後ろ向きな安心感（赤信号みんなで渡れば怖くない発想）」
  - BIND免罪符?
  - 顧客がそれで納得しますか?

「BIND 9」の脆弱性を狙う攻撃が発生、国内レンタルサーバー会社でアクセス不能になる被害

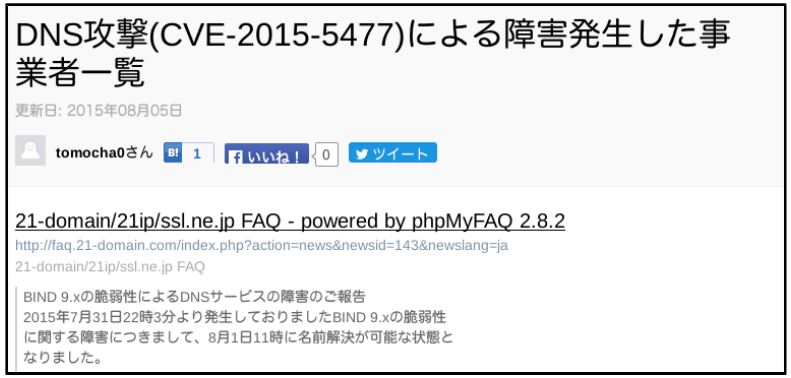
（2015/7/31 19:24）

Internet Systems Consortium（ISC）が開発・提供しているDNSソフト「BIND 9」においてサービス運用妨害（DoS）攻撃が可能な脆弱性（CVE-2015-5477）が見つかった件で、これを修正した最新バージョンへの更新または各ディストリビューターが提供する修正パッチの適用を速やかに実施するよう、株式会社日本レジストリサービス（JPRS）があらためて注意を促している。

JPRSによると、この脆弱性の実証（PoC）コードがすでにネット上で公開されており、日本国内のサービスプロバイダーからの被害事例も報告されているという。「即時の対応を強く推奨する」としている。

国内での被害としては、レンタルサーバーサービスを提供するカゴヤ・ジャパン株式会社が31日、この脆弱性に対する攻撃によって同社の権威DNSサーバーにおけるDNSサービスが停止。同日深夜に一時、名前解決が行えず、サーバーへアクセスできない障害が発生していたことを公表している。

http://internet.watch.impress.co.jp/docs/news/714526.html



ベンダー・SIerが対応していない

- 「OSベンダ(ていうかRedhat)のサポートがないとメンテナンスが大変、顧客に説明しづらい」
- 「『BIND以外で』と書いてもSIerが『プリインストールされるBINDでしか構築できない』」
- 「BIND以外のソフトウェアを構築・サポートしてくれるSIerさんが少ない」

- おめでとう。UnboundはRHEL7でbaseに入りました
  - 残念ながら権威DNSサーバーは無いです
    - どなたかRedhatにRHEL8に入るよう掛け合えませんかね?

ベンダー・SIerが対応していない

ベンダーPackageの対応状況

- 「ベンダーのサポートがないからBIND9以外使えない」とみなさんおっしゃいますが…
- 脆弱性公表からRHELパッケージリリースまで、ヤバイ脆弱性18件を調査

かかった日数	回数	運用者の気持ち
0-1日	5	早い。安心安心
2日	3	このくらいならまだ安心
3日	2	そろそろやばくね…?
4日	2	まだーー? (そろそろ攻撃が来るー)
5日	1	まだなのーーー?
6日	2	そろそろ1週間なんだけど (あわわ…)
7日	1	や、やっと出た… _(:3」∠)_
8日	1	遅いよ…
12日	1	攻撃来ないし、もう忘れかけてたわ…
13-15日	1	もうどうでもイイっす…

有償サポートがある

- ディストリビューションではなく開発元の。
- BINDのsubscriptionの内容

  脆弱性情報早期(事前)提供,機能追加リクエスト
  問い合わせへの対応,スペシャルカスタマイズ版
  プライベートトレーニングの値引き
  設定の監査(チェック), コンサルティング
- nsd, unbound, PowerDNS, Knot いずれも提供元による24H/7Dのサポート有り
  - というか、nsd/unboundは ISCもやってる
  - PowerDNS: デージーネットさんが近日対応予定!

社内(上司)のしがらみ

- 「BINDしか知らない、わからないものは使いたくない（＝責任をとりたくない）という人が上司（技術責任者）だから」
- 「上司がBINDに精通していて、BIND以外のソフトウェアを知らないため、BIND以外のソフトウェアを使った案が却下されてしまう。」
- 「移行に際してかかる工数を上司に認められない (脆弱性対応の工数は気にされない)」
  - うーん…
  - 工数に関しては、積み上げて提示してみては?

難しい? (手軽さがない?)

- 「小細工していないキャッシュサーバーで unbound 採用しているけど、設定項目が多すぎて気軽に使えない。キャリア向けの大規模キャッシュ運用するんじゃないのだから、性能パラメータは自動で良きに計らってほしい。」
  - `rrset-cache-size/msg-cache-size`以外で絶対に変更しなくてはいけないパラーメータはないような
    - それすら面倒と言われますと...
    - BINDも良きに計らうのはスレッド数くらい。逆にメモリなんかは無制限に使うので制限してあげないとダメ。

変わり種

- 「権威を引っ越ししたいが、ドメインの管理のユーザ名パスワードがわからない。登録されているメールアドレスなども既に使われてなさそうでお手上げ状態。」
  - 権威DNSサーバーが外部ゾーンならば、NSレコードのAを変えれば引っ越しできるはず
  - 管理指定事業者にお問い合わせください
    - 管理指定事業者がわからなければ、.jpならJPRSへお問い合わせ。whoisするとレジストラがわかるTLDも多い

こういった際、どういう手続を踏めば変更ができるのか…

変わり種

- 「重複祭りに参加したい」
  - お、おう…
- 「すべてをUnobund, NSDに変更すると、BIND 9の使い方を忘れたり、 落すための環境がなくなるため、BIND 9を辞められない。」
  - お、おう…
- 「BIND以外知らない」
  - 今日知りましたよね^^

結論

BIND9の脆弱性対応が苦にならない人はそのまま心中すればいいんじゃないでしょうか。

脆弱性対応頑張ってください。

自分はイヤなので乗り換えます。

(個人の感想です)

IIJ Internet Initiative Japan

さあ、愛♥ を語ってください!

Ongoing Innovation