ISPでのIP53B運用経験

InternetWeek2014 DNS DAY

2014/11/20

●自己紹介

鵜野　直樹 （うの　なおき）

株式会社帯広シティーケーブル （北海道帯広市）
技術開発部所属


択捉島
稚内市
択捉島
国後島
網走市
旭川市
色丹島
歯舞諸島
小樽市
富良野市
根室市
釧路市
札幌市
帯広市
奥尻島
函館市
Copyright(C) T-worldatlas All Rights Reserved.

アジェンダ

1. 事の始まり
2. 調査しました
3. 決断しました
4. 実施しました
5. その後

DNSについて

DNSサーバー

1998～2007：権威、キャッシュを兼用

2007 ～　　：権威、キャッシュを分離

日常運用は、脆弱性対応程度

事の始まり

コールセンターの受電記録から

事の始まり

5/30

NETの繋がりが悪い。ページが開けません・・・とかで、ONU/無線ルータをいつもリセット掛けているが、リセット掛けるのが面倒なので調査してほしい。携帯へ折電のお伝え。

→保守業者対応 ONU交換し対応完了しました。

事の始まり

6/4

インターネット接続できませんと表示出る。PCとルーターの再起動してもらったが改善されず。
技術課へ

→本人より：直ったみたいですと連絡有。様子見て頂き、頻繁に起こるようなら連絡頂く事に。

この時点では、
DNSに起因する問題とは認識していなかった

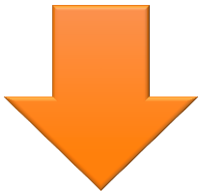
調査しました

大手ISPでDNSの障害

http://information.myjcom.jp/sp/outage/99.html

複数のISPにおいてDNSサーバー障害が発生

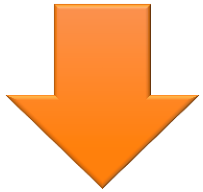
http://it.slashdot.jp/story/14/06/02/115247/



同様の状況が発生している？

調査しました

DNSサーバーのログ、統計情報を確認



クエリーを相当数dropしていた
あきらかにおかしい状況

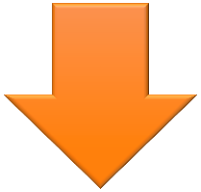
決断しました

・DNSサーバーの負荷
・運用回避導入の負荷
・サーバー増強はすぐにはできない
・コールセンター、２次エスカレーション部署、訪問保守会社の負荷

・利用者が、インターネット接続の不安定性を感じている可能性は高い

決断しました

「安定した接続サービスの提供」

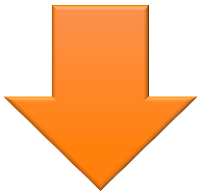


緊急避難措置でIP53B導入決断

実施しました

IP53Bを実施する前に、
DNSサーバーの設定を改めて確認

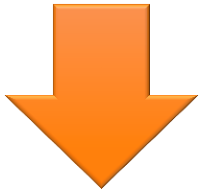
recursive設定：1000（default）



段階的に設定値を増やした
（2000-3000-3500）

実施しました

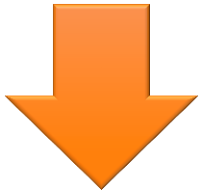
DNSサーバーの状況を確認



recursive設定内に収まっているが、
クエリー数は依然多い

実施しました

IP53B をアクセス系集線SWに対して設定



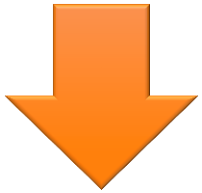
クエリー数が大幅に減少
キャッシュヒット率改善

その後

事前資料では未公開

その後

パケットキャプチャー実施



bot感染PC?からのクエリーはまだまだある

どうする？

その後

事前資料では未公開

その後

事前資料では未公開

その後

運用で困った点．．．．

利用者からの問い合わせ．．．．

IP53Bを継続する？やめる？．．．．

IP？？Bは増えていくのか？ ．．．．

その後

JANOG34高松でBoF開催

・DNS関連BoF共同で実施
「我慢する？ あきらめる？ 工夫する？ 大量攻撃トラフィック対応」
「ブロッキング・フィルタリングぶっちゃけBoF」

http://www.janog.gr.jp/meeting/janog34/tutorial/index.html