DNSSEC最新動向と
インターネット検閲の問題の話

NTTセキュアプラットフォーム研究所
佐藤 一道

2012/9/1

お題目

- DNSSEC最新動向
  - 失敗事例 (少し)
  - 普及状況
  - その他ツール

- 論文紹介
  - The Collateral Damage of Internet Censorship by DNS Injection

DNSSEC最新動向

情報源

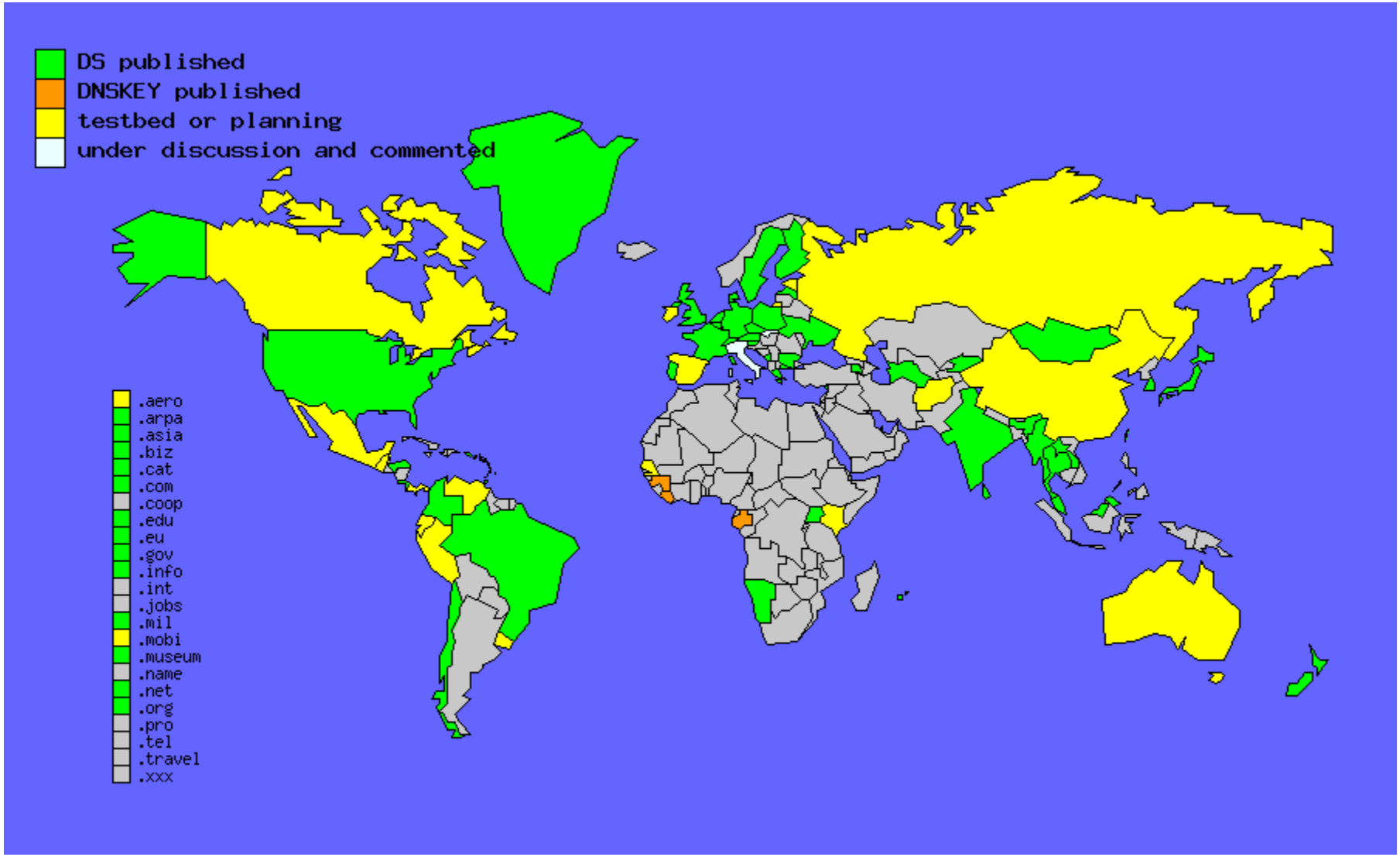
- Comcast DNS News
  - http://dns.comcast.net/
- DNSSEC Deployment Initiative
  - https://www.dnssec-deployment.org/
- その他、DNS-OARCやDNSSEC Deployment のメーリングリストなど

失敗事例

- earthquake.govのDNSSEC検証失敗
  - 2012/8/30
  - 原因は署名の有効期限切れ
- medicare.govのDNSSEC検証失敗
  - 2012/8/28
  - 新しい署名情報が有効になる前に古い署名情報を削除したため
- sba.govのDNSSEC検証失敗
  - 2012/8/27
  - 原因は署名の有効期限切れ
- ubm-us.netのDNSSEC検証失敗
  - 2012/8/27
  - 原因は署名の有効期限切れ
- glb.cdc.govの以下略

引用：http://dns.comcast.net/

DNSSEC普及状況



引用：http://www.ohmo.to/dnssec/maps/

DNSSEC普及状況

- TLDのDNSSEC対応状況 (2012年8月17日時点)
  - 署名済みTLD数：77
  - DS公開済みTLD数：82
  - 直近数ヶ月で大きな変化はない
- 最近署名またはDSが登録されたTLD

	2012年4月	5月	6月	7月	8月
署名	.fo .gn .lr	.lv .lb		.tt	.lk
DS登録	.ua	.lb		.mil	.lv .tt

引用：http://www.ohmo.to/dnssec/maps/

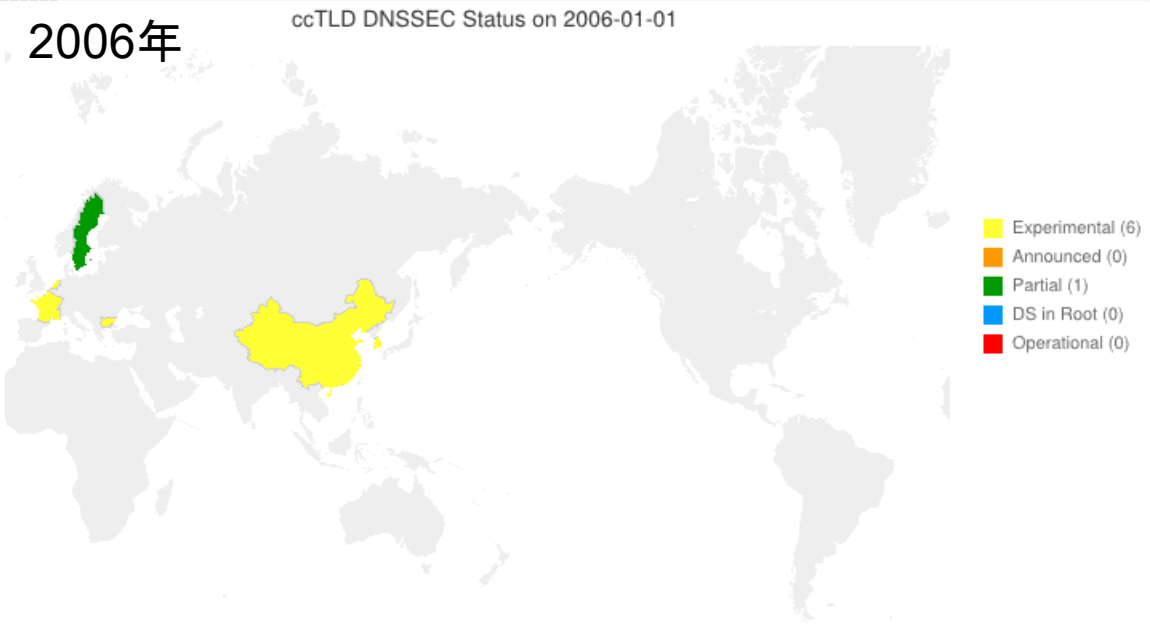
DNSSEC普及状況の可視化

NTT

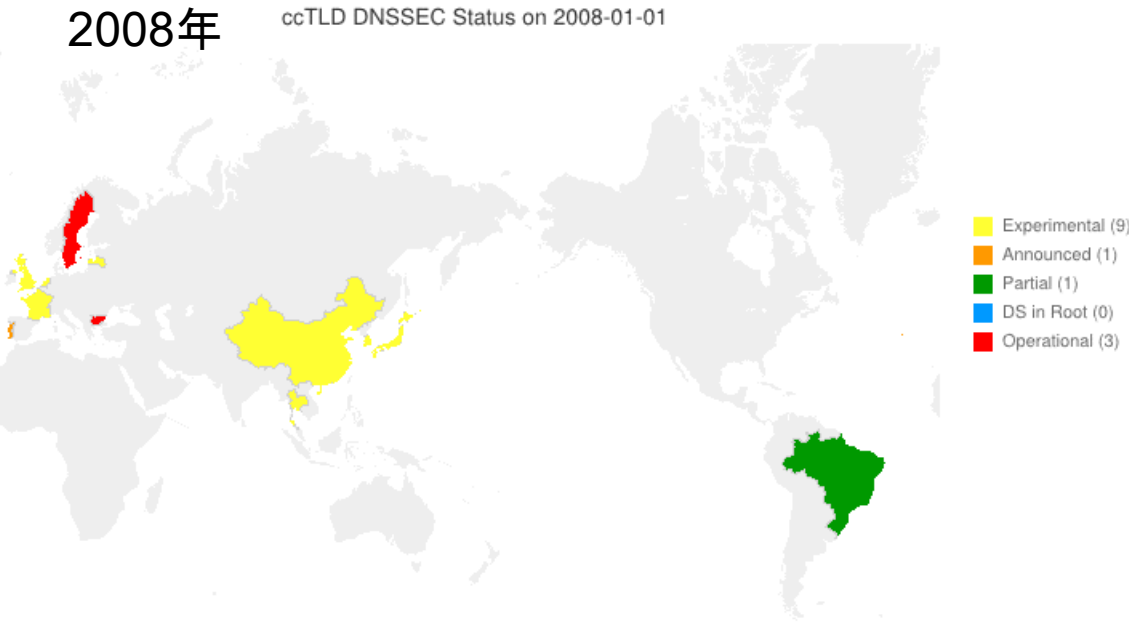
- 過去～未来のccTLDのDNSSEC普及状況を描いた地図が公開
  - 2006年1月～2014年7月の普及状況
  - 大本さんのライバル出現?
- 公開場所 (2012年8月29日時点の最新版)
  - https://www.dnssec-deployment.org/wp-content/uploads/2012/07/2012-07-02-animated.gif
- 凡例
  - 黄色:実験中
  - オレンジ:アナウンス済
  - 緑:署名済みであるが、DSは未公開
  - 青:署名済み、DS登録済み、子ゾーンからのDS登録を受け付けていない
  - 赤:署名済み、DS登録済み、子ゾーンからのDS登録を受け付けている

2006年～2008年の普及状況

2006年

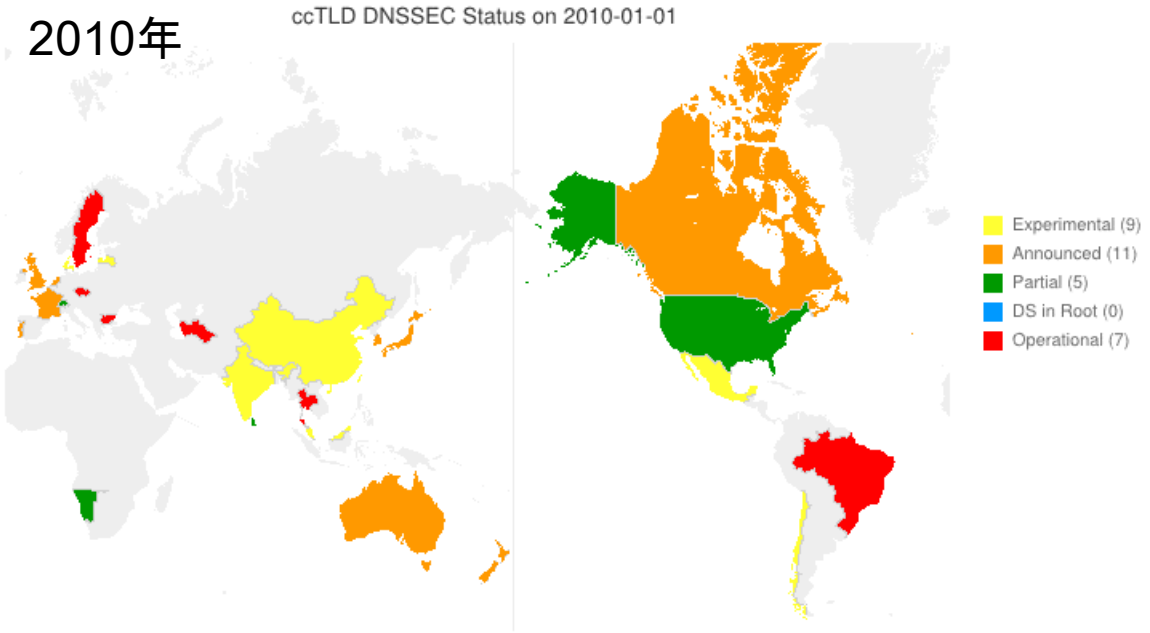


2008年

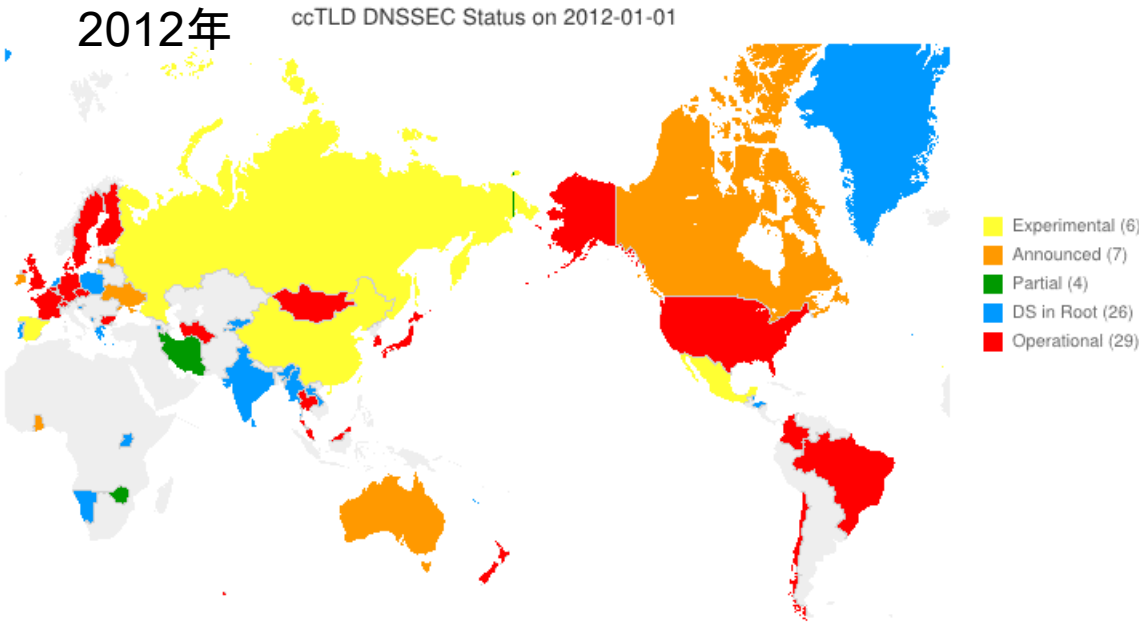


2010年～2012年の普及状況

2010年

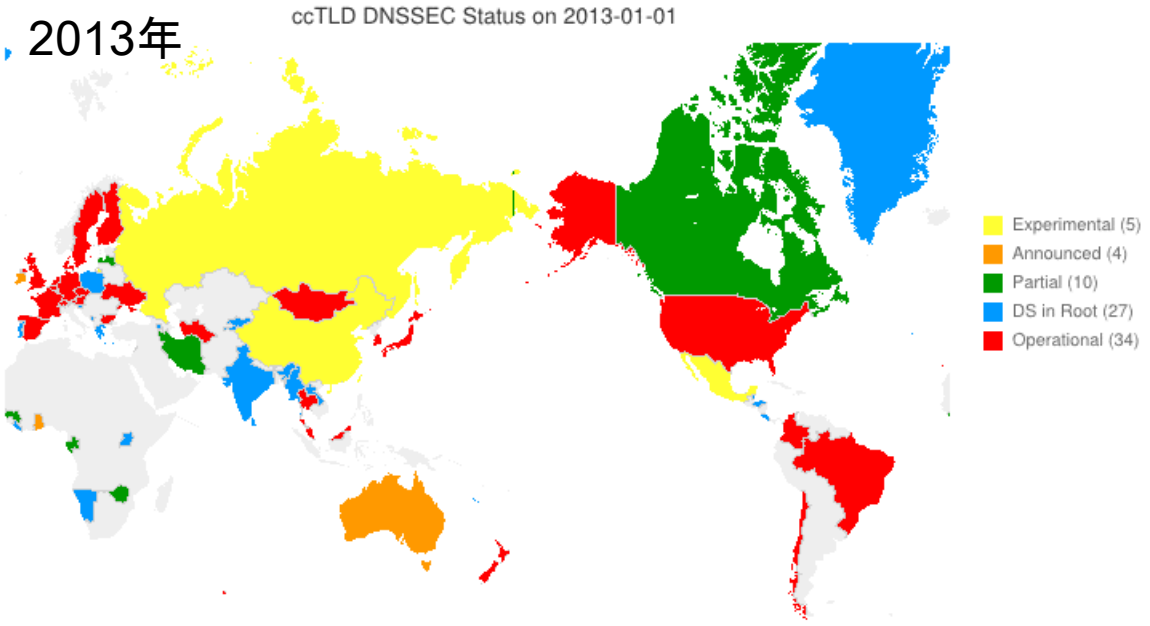


2012年

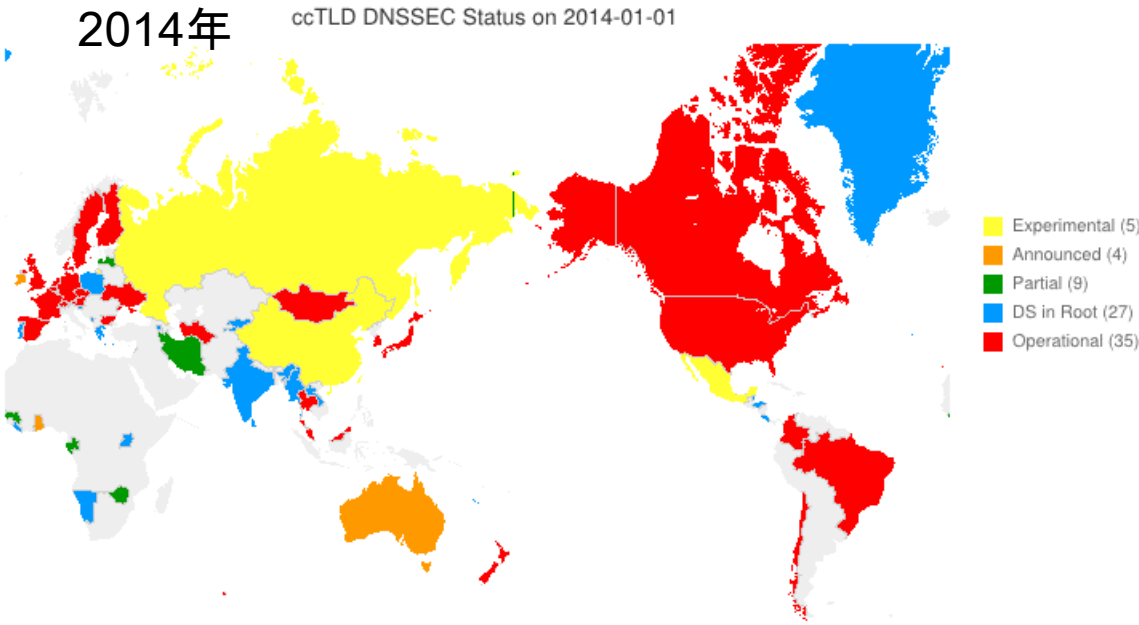


2013年～2014年の普及状況予測

2013年



2014年



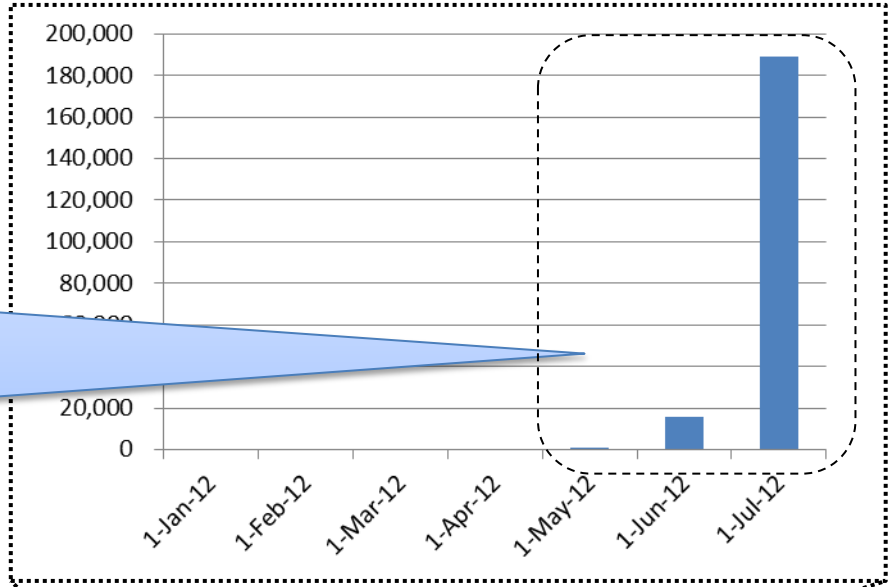
今、オランダが熱い

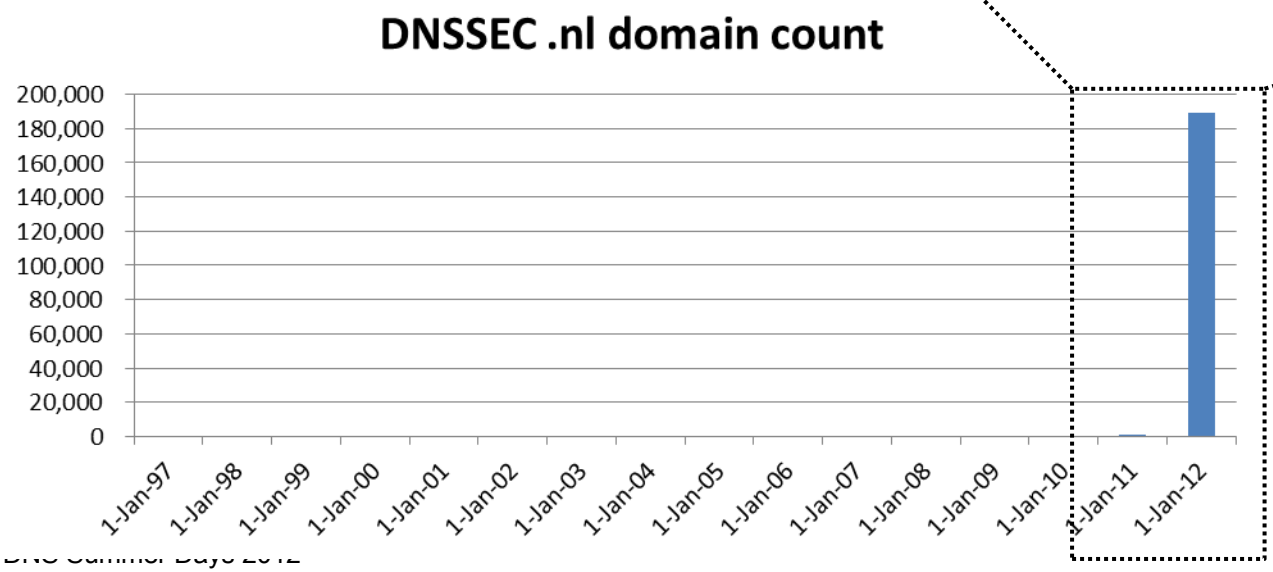
- 署名済み.nlドメイン名数がccTLDの中で一番多い
  - 署名済みドメイン名数はSIDNのWebサイトで確認することができる
    - https://www.sidn.nl/en/homepage-sidn/

- 8/29時点の署名済みドメイン名数
  - 約77万
  - 全ドメイン名数は500万
  - 約15%のドメイン名が署名済み

今、オランダが熱い

SIDNが今年5月に.nlの子ゾーンまでDNSSEC対応したとアナウンスしてから急激な伸びを見せている





ツールなど

- YADIFA
  - EURIDが開発したDNSSEC対応権威サーバ
  - 他のDNSサーバと比較して
    - メモリ使用量が少ない
    - 大量のクエリをさばける
    - ゾーンファイルのロード時間が短い
  - 対応OS
    - FreeBSD、GNU/Linux、OS X
    - 今後OpenBSD、SolarisなどのUNIX、Windowsにも対応予定
  - URL
    - http://www.yadifa.eu/

ツールなど

- dnssecmagic.js
  - Webサイトにアクセスしたユーザが DNSSEC検証ONのキャッシュサーバを使っているかを判定するスクリプト
  - DNSSEC検証ON

  - DNSSEC検証OFF

  - ソースコード
    - https://github.com/jpmens/dnssecmagic.js

感想

- 以前(1年前)と比較して変わったこと
  - xxの署名の有効期限が切れてる、などがメーリングリストに投稿されることが少なくなった
    →運用にこなれてきた?あまり興味がなくなった?
    - 検証失敗事例は依然としてたくさんあるのだが。。。
  - xx(上位ゾーン)が署名しました、などの投稿も少なくなった
    →主要なTLDは概ね署名およびDS登録済み

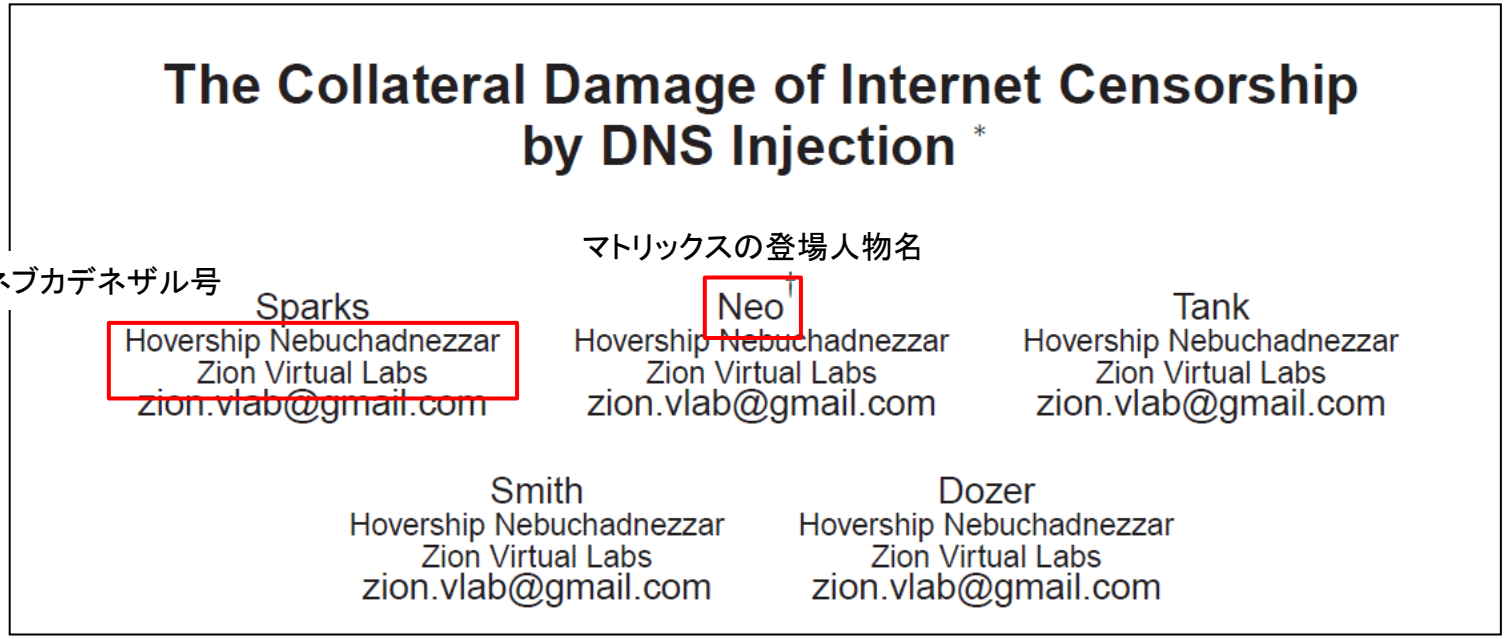
- 今後見たいニュース
  - インパクトのあるゾーンの署名ニュース
    - Google、Facebook、Twitterなど

論文紹介：The Collateral Damage of Internet Censorship by DNS Injection

投稿論文

- ACM SIGCOMM 2012に投稿された、DNSによるインターネット検閲の問題を調査した論文
  - http://conferences.sigcomm.org/sigcomm/2012/paper/ccr-paper266.pdf
  - http://www.sigcomm.org/sites/default/files/ccr/papers/2012/July/2317307-2317311.pdf

- 論文情報
  - タイトル
    - The Collateral Damage of Internet Censorship by DNS Injection
  - 著者
    - アノニマスのメンバ (論文ではマトリックスの登場人物名、偽名)



The Collateral Damage of Internet Censorship by DNS Injection *

マトリックスの登場人物名

所属はネブカデネザル号

Sparks
Hovership Nebuchadnezzar
Zion Virtual Labs
zion.vlab@gmail.com

Neo †
Hovership Nebuchadnezzar
Zion Virtual Labs
zion.vlab@gmail.com

Tank
Hovership Nebuchadnezzar
Zion Virtual Labs
zion.vlab@gmail.com

Smith
Hovership Nebuchadnezzar
Zion Virtual Labs
zion.vlab@gmail.com

Dozer
Hovership Nebuchadnezzar
Zion Virtual Labs
zion.vlab@gmail.com

論文概要

- DNSの応答を制御することでインターネット検閲を行っているISP (以下検閲ISP)が、網外の端末に与える影響を調査
  - 検閲ISP外のユーザが検閲を受けてしまう”巻き添え”の仕組み、影響を調査

- 調査内容
  - どのISPがインターネット検閲を行っているか
  - 偽装応答を受け取るキャッシュサーバはどの程度存在するか
  - 偽装応答はどの階層で受け取るか

- 調査期間
  - 2011年11月の1ヶ月間

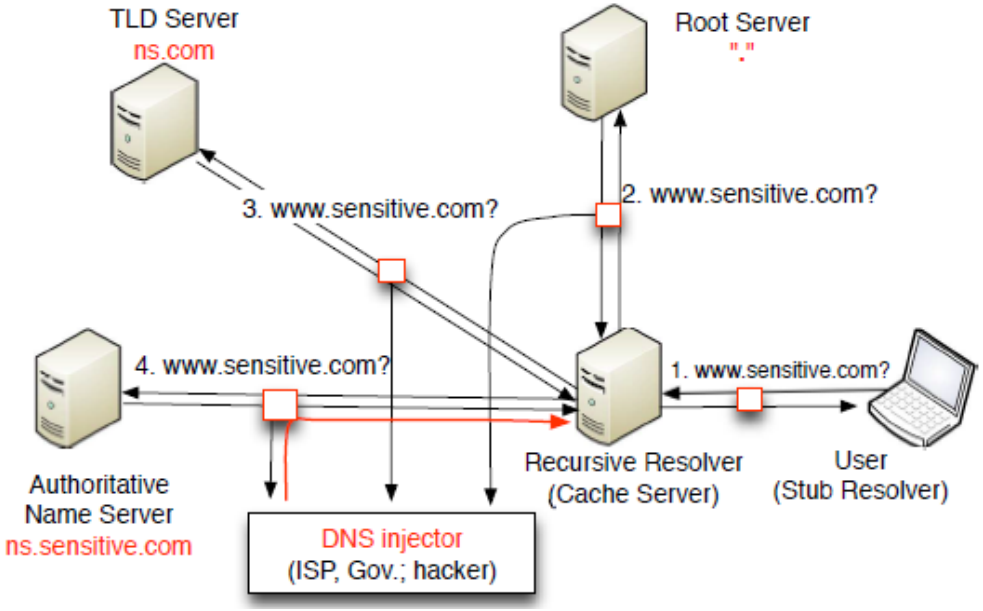
- 調査結果
  - 中国内の39のISP(AS)が検閲を行なっていることを確認
  - 109ヶ国、約11,000のキャッシュサーバが偽装応答を受け取った
  - 偽装応答を受け取る階層は主にTLDへの問い合わせ時

巻き添えの仕組み

- キャッシュサーバからのクエリが検閲ISPに到達したとき、巻き添えが発生する

- 巻き添えの要因
  - 権威サーバが検閲ISP内に設置されている
  - 途中経路に検閲を行っているISPがある

- 著者の仮説
  - 偽装応答は検閲ISPのルータが返す
  - クエリの送信元は考慮していない



やってみる

- www.cnnic.com、qq.comにクエリを投げてみる
  - $ dig @www.cnnic.com facebook.com
  - $ dig @qq.com facebook.com
  - など

(1) 検閲を受ける経路の特定

- 調査方法
  - 検閲対象と思われるドメイン名の名前解決を、様々な宛先に対して実施する
    - 宛先はDNSサーバではないため、通常であれば応答はない
  - 問い合わせに対して応答があった場合、その宛先までの経路のどこかに検閲ISPが存在するものとする

- 調査IPアドレス
  - 1,400万IPアドレス

- クエリ送信元
  - AS40676にあるVPS

調査対象ドメイン名

Domain Name	Category
www.google.com	Search Engines
www.facebook.com	Social Networks
www.twitter.com	Social Networks
www.youbube.com	Streaming Media
www.yahoo.com	News Portal
www.appspot.com	Web Hosting
www.xxx.com	Pornography
www.urltrends.com	Sites Ranking
www.live.com	Portal
www.wikipedia.org	Reference

調査結果(1)

- 応答のあった宛先
  - 16の地域、197のAS、388,988IPアドレス
    - CN、CA、US、HK、IN、AP、KR、JP、WT、DE、PK、AU、SG、ZA、SE、FI
    - ほぼ中国のIPアドレス

Region	IP Count	Percentage
CN	388206	99.80
CA	363	0.09
US	127	0.03
HK	111	0.03
IN	94	0.02
Total 16 regions		

(a) Top 5 regions.

AS number	Region	IP Count	Percentage
4134	CN	140232	36.05
4837	CN	88573	22.77
4538	CN	35217	9.05
9394	CN	24880	6.40
4812	CN	14913	3.83
Total 197 ASes			

(b) Top 5 ASes.

  - 偽装応答があったドメイン名
    - www.facebook.com、twitter.com、www.youtube.com、www.appspot.com、www.xxx.com、www.urltrends.com

(2) 検閲ISPの特定

- 調査方法
  - IPヘッダのTTLを1つずつ増加させながら問い合わせを行い、どの段階で検閲を受けたかを特定する
    - tracerouteと同様の手法
  - 調査対象の宛先は(1)の調査で応答があったIPアドレス

- 調査結果
  - 3,120のIPアドレスから偽装応答があることを特定
  - 上記IPアドレスは中国の39のASに属する

AS Number	AS Name	Router IPs
4134	Chinanet	1952
4837	CNCGROUP China169 Backbone	489
4812	China Telecom (Group)	289
9394	CHINA RAILWAY Internet(CRNET)	78
9929	China Netcom Corp.	67
4808	CNCGROUP IP network China169 Beijing Province Network	55
9808	Guangdong Mobile Communication Co.Ltd.	38
17633	ASN for Shandong Provincial Net of CT	25
4538	China Education and Research Network Center	22
17816	China Unicom IP network China169 Guangdong province	19
Total 39 ASes		

(3) 影響を受けるキャッシュサーバの特定

NTT

- 調査方法
  - 様々なオープンリゾルバから問い合わせを行う
    - 173ヶ国、43,842オープンリゾルバ
    - 問い合わせドメイン名は(1)の調査で応答があったものから生成 (生成ルールは次項で)
  - 応答IPアドレスが偽装されたものであれば、巻き添え被害を受けるキャッシュサーバ

Region	Count	Percentage
US	12519	28.76
JP	4889	11.23
RU	3306	7.60
DE	2345	5.39
TW	1733	3.98
GB	1580	3.63
CA	1150	2.64
IT	1053	2.42
Total 173 regions		

(3)影響を受けるキャッシュサーバの特定 (ドメイン名生成ルール)

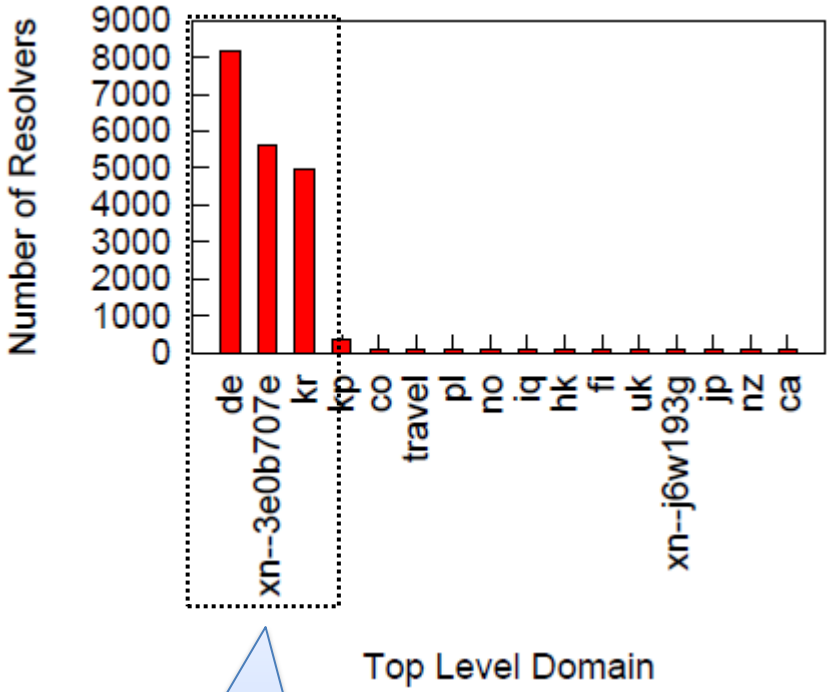
- 生成ルール1
  - {KEYWORD}.{RANDOM}
    - www.facebook.com.adsasdf
  - NXDomainではない応答が返れば、Rootサーバへのクエリに対する応答が偽装されている
- 生成ルール2
  - {KEYWORD}.{RANDOM}.*tld*
    - www.facebook.com.adsasdf.com
  - NXDomainではない応答が返れば、TLDサーバへのクエリに対する応答が偽装されている
- 生成ルール3
  - {KEYWORD}.{RANDOM}.*authority.tld*
    - www.facebook.com.adsasdf.ibm.com
  - NXDoaminではない応答が帰れば、Root、TLD以外の権威サーバへのクエリに対する応答が偽装されている
  - authority.tldはAlexaの上位82ドメイン (.cn除く)

調査結果(4)

- キャッシュサーバ ⇔ Rootサーバの偽装応答 (ルール1)
  - 偽装応答があったのは、台湾のオープンリゾルバ1つのみ (124.219.23.209、AS24154)
  - Rootサーバまでの経路に中国のISPが含まれていたと思われる
- キャッシュサーバ⇔TLDサーバの偽装応答 (ルール2)
  - 中国のTLD (.cn、.xn--fiqs8s、.xn--fiqz9s)
    - 43,322 (99.53%)のオープンリゾルバに偽装応答が返った
  - 中国以外のTLD
    - 11,573 (26.40%)のオープンリゾルバに偽装応答が返った
- キャッシュサーバ⇔その他権威サーバの偽装 (ルール3)
  - 99のオープンリゾルバに偽装応答が返った

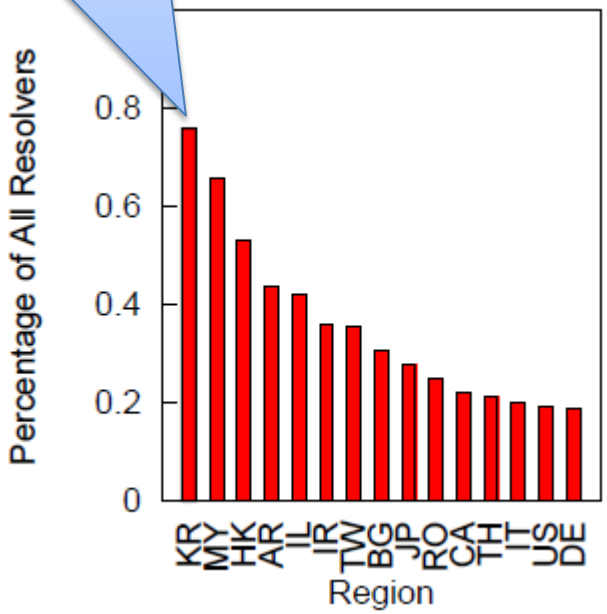
調査結果(4)続き

検閲を受けたオープンリゾルバ数 (TLD別)



多くのドイツまたは韓国のTLD
サーバへのクエリが検閲を受けた

韓国から.de DNSサーバへクエリを送信したとき、70%以上のオープンリゾルバに偽装応答が返った



.de DNSサーバへのクエリで検閲を受けたオープンリゾルバ割合 (クエリ送信元地域別)

まとめ

- 調査結果まとめ (再掲)
  - 中国内の39のISP(AS)が検閲を行なっていることを確認
  - 109ヶ国、約11,000のキャッシュサーバが偽装応答を受け取った
  - 偽装応答を受け取る階層は主にTLDへの問い合わせ時
- 著者の思い
  - DNSSEC検証を行えば、偽装応答を検知できる
  - 調査結果がDNSSECの普及につながることを願う

感想

- 調査内容としては非常に興味がある
  - 広範囲に渡る検閲ISPの調査、特定

- ただし、評価結果が大袈裟すぎる
  - 論文では109ヶ国、約11,000のキャッシュサーバが影響を受けると主張しているが、影響範囲は限定的
    - 韓国から.deのドメイン名を問い合わせたとき
  - この結果だけではDNSSEC普及に繋がるとは思えない