

ICANN Office of the CTO

概要と最近の話題



David Conrad
Chief Technology Officer

オープンセッション – Tokyo, Japan
2017年9月1日

本日のお話

- ◎ Office of the CTOの活動
- ◎ 技術的な話題をいくつか
 - DNSSEC Deployment
 - Key Signing Key Rollover
 - IPv6 Deploymentの状況
 - 識別子システムのアビュース
- ◎ PTIについて簡単に紹介
- ◎ Q&A

研究

- Identifier Technologies Health Indicators (ITHI)
- 将来の識別子システムの研究
- Open Data Initiative (ODI)
- DNSルートシステム分析
- DNS Server Test Lab
- 識別子システムトレーニング
- KSK Rollover

安全性、安定性、耐性/復旧力

- 識別子不正使用に関するリサーチ
- 識別子に関する脅威軽減/運用サポート
- SSRの能力開発とトレーニング
- DNS Abuse Analytics, and Reporting (DAAR)

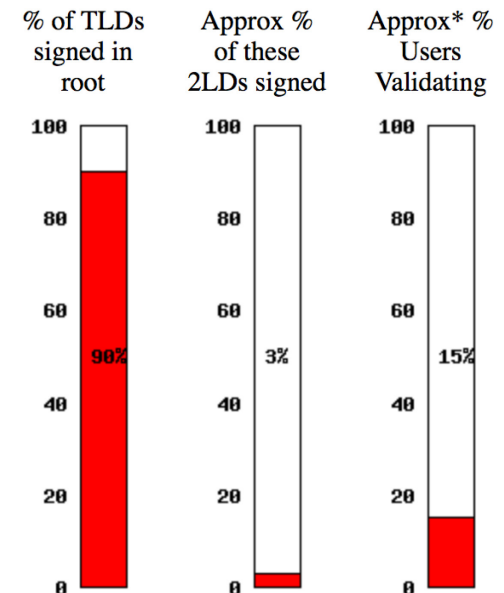
ICANNの「シンクタンク」

- アウトリーチとエンゲージメント
- 中立で先入観のないデータドリブン(data-driven)な分析
- 技術的に健全なポジションステートメント

技術的な話題: DNSSEC Deployment

DNSSEC: DNSの信頼性向上

- ◎ DNSプロトコルにはバグがある
 - リモートキャッシュポイズニングの可能性
- ◎ 解決策: DNSSEC
 - 異なるアクターによる2つの部分からなる
 - ・ DNSデータ公開時に暗号化した署名
 - ・ データを受け取る際に署名を確認
- ◎ DNSSECの展開(deployment): 遅い
 - “Solution in search of a problem”
 - 運用の点で複雑/もろい
 - 新たなリスクを造り出す
- ◎ 利点
 - バグをFIX、DNS応答は安全に
 - 新たな信頼の基盤を創造
 - 一定の種類DDoSに対応できる



技術的な話題: Key Signing Key Rollover

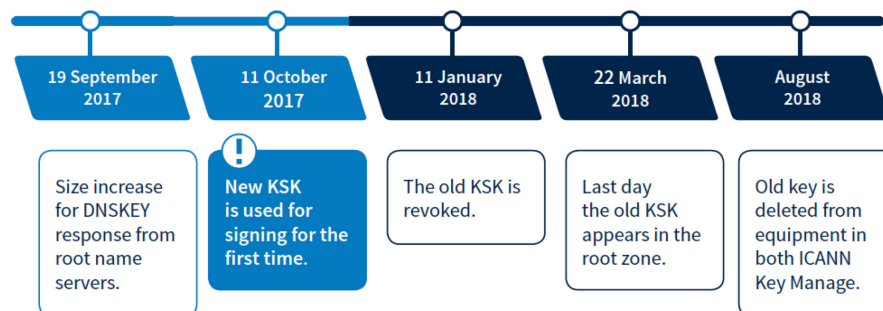
KSK Roll: インターネットのパスワード変更

↓↓避けたいのは...↓↓

- ◎ Root DNSSECは2010年7月に署名
 - 鍵の更新(roll)は「5年後に」
- ◎ リゾルバの運用者は設定の変更が必要
 - インターネット上には100Mのリゾルバがあると推定される
 - リスク: インターネットユーザーの15%が何も名前解決できなくなる
- ◎ この更新に対応できることをご確認ください



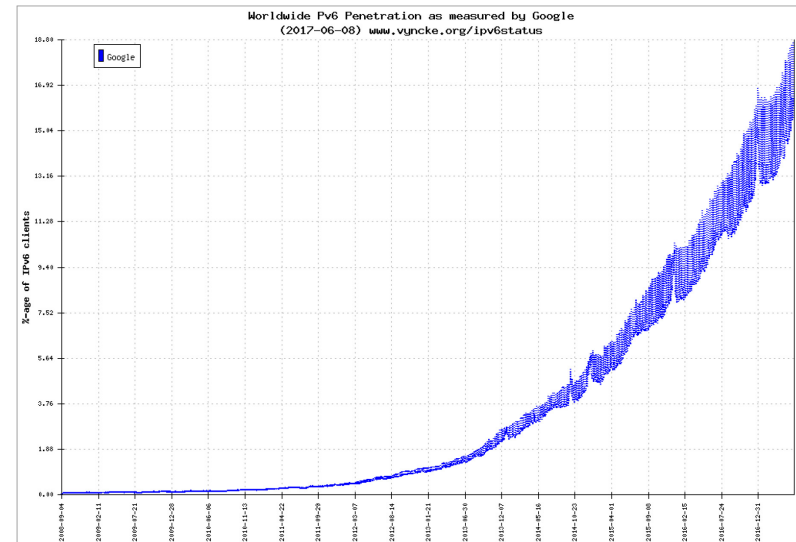
<https://automated-ksk-test.research.icann.org>



技術的な話題: IPv6 Deploymentの状況

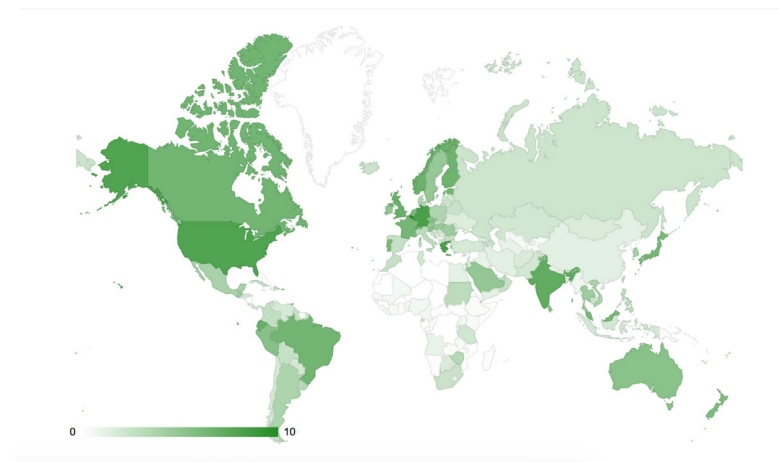
IPv6 Deploymentはゆっくり

- ◎ 標準化: 1996年
 - 現在: GoogleのクライアントのうちIPv6を使っているのは14~18%にとどまる
- ◎ なぜか?
 - 後方互換性がない
 - 無数の多種多様な移行戦略
 - 卵が先か鶏が先か:
 - 顧客の需要がないからインフラがないのか
 - インフラがないから顧客の需要がないのか
 - IPv4トランスレータを使う必要
- ◎ IPv4より技術的には優れたソリューション、しかしビジネスの観点で推進力が弱い



Updated on 2017-6-8

Display global data 
World | Africa | Asia | America | Europe | Oceania



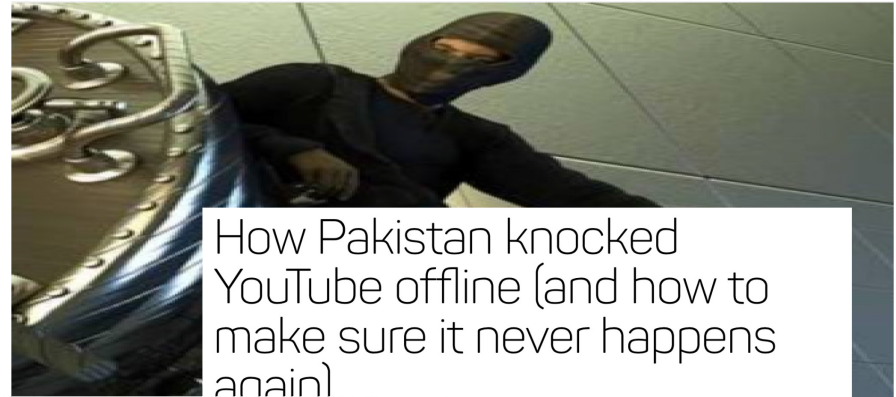
From: <http://6lab.cisco.com/stats/>

技術的な話題: 識別子システムのアビューズ

ICANN Meets Cybersecurity

- ◎ レジストリ/レジストラのセキュリティ侵害
 - 識別子を盗む/リダイレクトする
 - 登録システムのアビューズ
 - ・ 誤った登録データ
- ◎ Denial of Service
 - DNS Amp攻撃
 - DNSリフレクション攻撃
- ◎ DNSに関する脅威
 - フィッシング
 - ボットネットのC&C(Command and Control)サーバー
 - マルウェアの拡散
- ◎ ルーティング(経路制御)システムのセキュリティ侵害
 - 誤ったアナウンス

for hours, malware dropped on



How Pakistan knocked YouTube offline (and how to make sure it never happens again)

DDoS attack that disrupted internet was largest of its kind in history, experts say

the first time that Internet addresses better security, it may be the last.

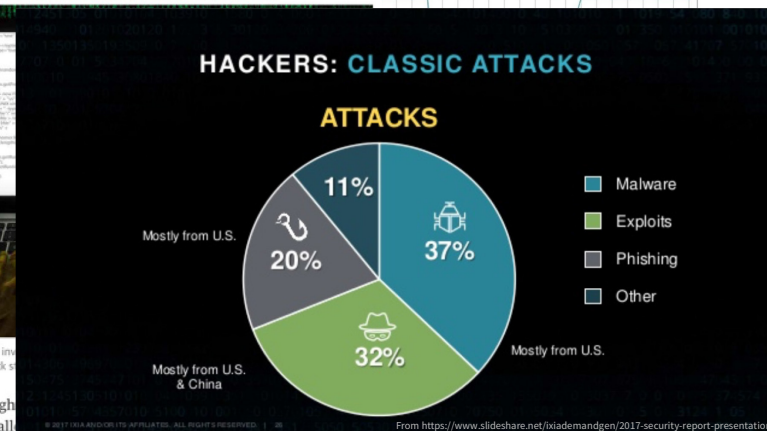
Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

● Major cyber attack disrupts internet service across Europe and US

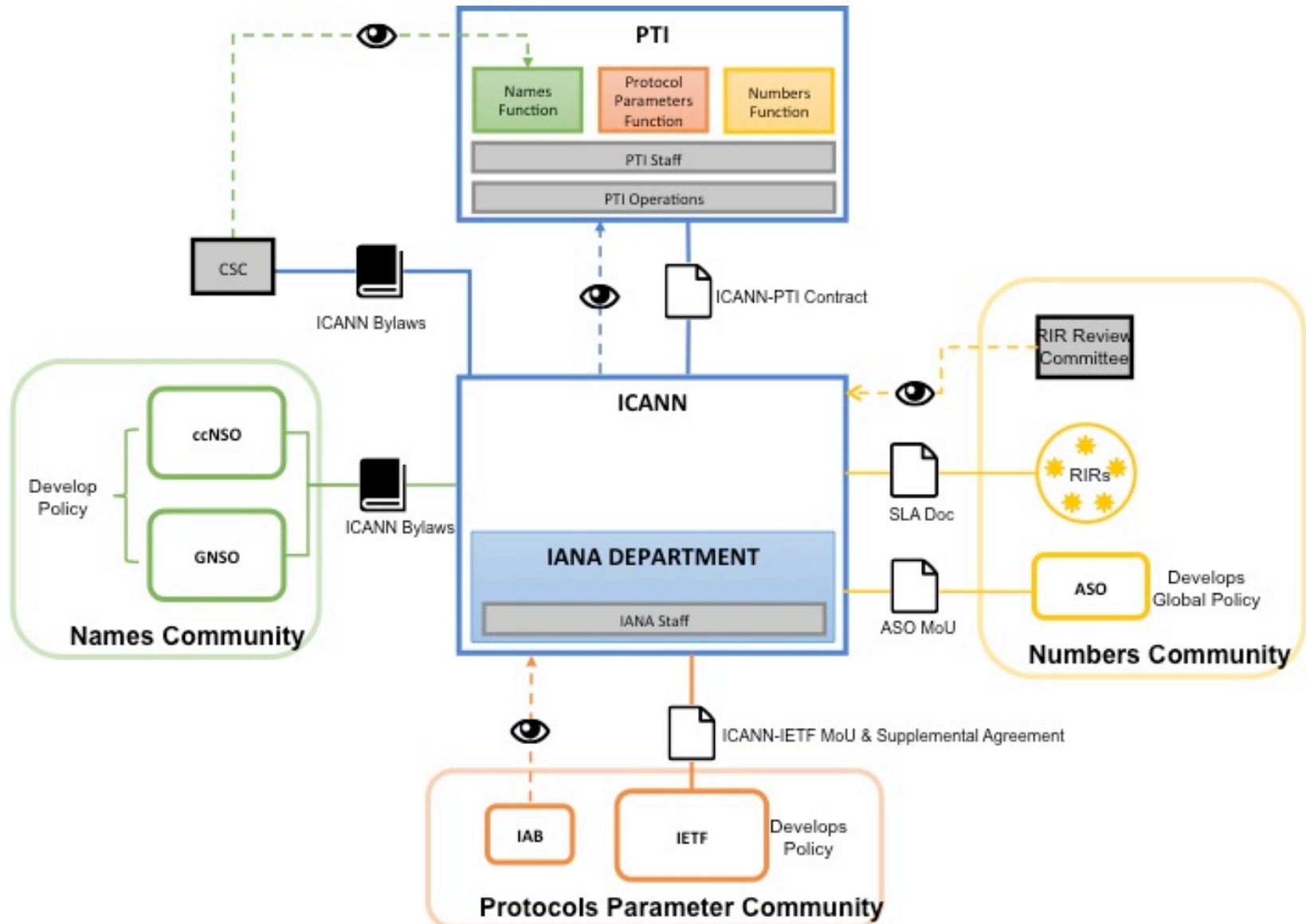


Dyn estimated that the attack had involved reports of an extraordinary attack

The cyber-attack that brought caused by a new weapon called kind in history, experts said.



Public Technical Identifiersと他組織との関係



まとめ

- ◎ **ICANN's Office of the CTO**
 - ICANNのシンクタンクとして、以下を提供：
 - ・ データと分析
 - ・ 能力開発とトレーニング
- ◎ **DNSSEC Deployment**
 - 進行中
- ◎ **KSK Rollover**
 - **2017年10月11日**
- ◎ **IPv6 Deployment**
 - ゆっくりではあるが、増えている
- ◎ **識別子システムのアビューズ**
 - 増えつつある問題、明確なソリューションはない

