DNSSEC最新動向

NTTサービスインテグレーション基盤研究所
佐藤 一道
2011.4.20

本日のお題目

- 最新動向を得るための情報ソースの紹介
  - Webページ
  - メーリングリスト
- 普及状況やこれまで発生した障害、技術動向などの簡単な報告
  - TLDのDNSSEC導入状況
  - インシデントレポート
  - DNSSECを利用したアプリケーション

主な情報ソース – Webページ

- DNSSEC.jp (日本語)
  - DNSSEC導入、運用における課題の整理、それに対する検討に関する資料などが公開されている
  - 参考URL: http://dnssec.jp/
- JPRS DNSSEC関連情報 (日本語)
  - 各種RFCの日本語訳、DNSサーバの脆弱性情報などが公開されている
  - 参考URL: http://jprs.jp/dnssec
- DNSSEC Deployment initiative (英語)
  - TLDのDNSSEC対応情報、インシデント事例などが公開されている
  - 参考URL: http://www.dnssec-deployment.org/

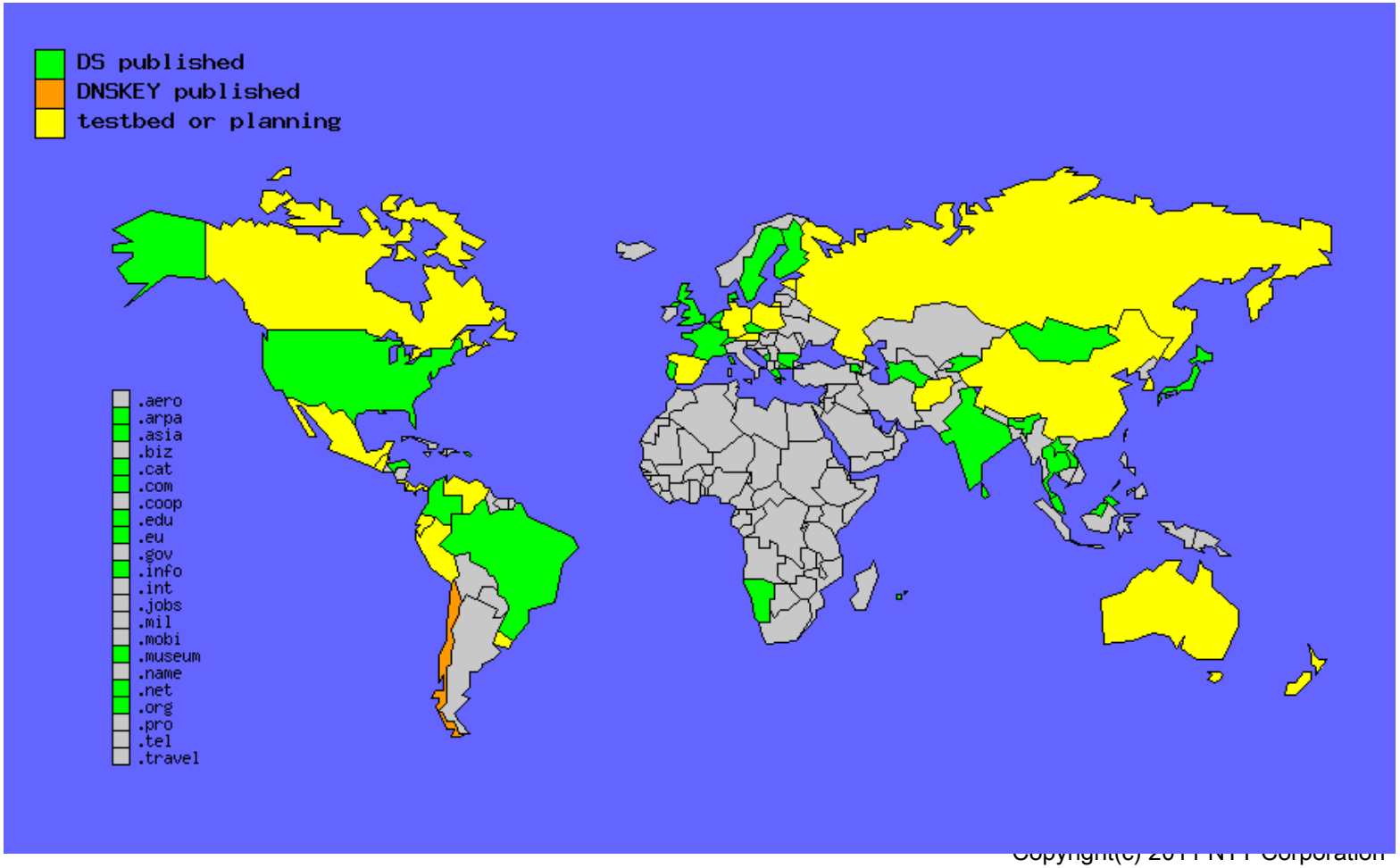
主な情報ソース – メーリングリスト

- dnsops.jp (日本語)
  - DNSに関する情報共有、議論がされている
  - 参考URL: http://dnsops.jp/ml.html
- DNS-OARC (英語)
  - DNSに関する情報共有、議論がされている
  - 参考URL: https://lists.dns-oarc.net/mailman/listinfo/dns-operations
- The DNSSEC-Deployment Working Group (英語)
  - DNSSECに特化した情報共有、議論がされている
  - 参考URL: https://www.dnssec-deployment.org/index.php/dnssec-deployment-working-group/
- IETF dnsop WG discussion (英語)
  - 各種ドラフトの議論などがなされている
  - 参考URL: https://www.ietf.org/mailman/listinfo/dnsop

TLDのDNSSEC導入状況

TLDのDNSSEC導入状況

- 導入状況の世界地図
  - http://www.ohmo.to/dnssec/maps/
  - 詳細は次の大本さんの発表で!!



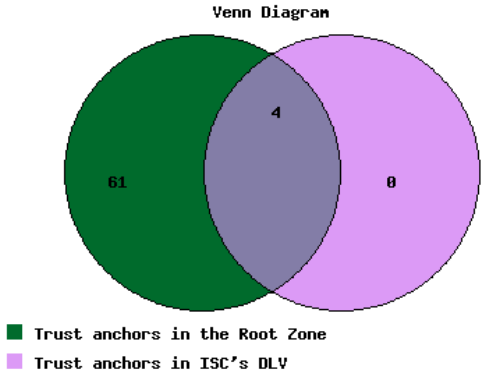
TLDのDNSSEC導入状況

NTT

- ICANNが公開しているDNSSEC導入状況
  - http://stats.research.icann.org/dns/tld_report/

Summary

- 307 TLDs in the root zone in total
- 69 TLDs are signed;
- 65 TLDs have trust anchors published as DS records in the root zone;
- 4 TLDs have trust anchors published in the ISC DLV Repository.



TLD	Signed?	DS in Root?	ISC DLV?
ac.	NO	NO	NO
ad.	NO	NO	NO
ae.	NO	NO	NO
aero.	NO	NO	NO
af.	NO	NO	NO
ag.	YES	YES	NO
ai.	NO	NO	NO
al.	NO	NO	NO
am.	YES	YES	YES

インシデントレポート

arpaの失敗

- 発生事象
  - 2010.6.4にarpaゾーンの署名検証が失敗する事象が発生
- 原因
  - 署名の期限切れ
- 参考情報
  - http://dnssec-deployment.org/pipermail/dnssec-deployment/2010-June/003881.html

ukの失敗

- 発生事象
  - 2010.9.11にukゾーンの署名検証が失敗する事象が発生
- 原因
  - 署名システム(HSM)の故障
- 対応
  - 別システムに切り替え、鍵の再生成、ゾーンの再署名を実施
  - DNSキャッシュサーバの運用者に向けて、ukゾーンのキャッシュ情報を”flush”するように要請
- インシデントレポート
  - http://blog.nominet.org.uk/tech/wp-content/uploads/2010/09/dnssec-incident-report.pdf

mozilla.orgの失敗

- 発生事象
  - 2010.9.16にmozilla.orgゾーンの署名検証が失敗する事象が発生
- 原因
  - 鍵更新の手順を間違えたことが発生原因
    - 新たに署名したゾーン情報の公開よりも前に、新しい鍵(DS)を上位ゾーンに公開してしまった
- インシデントレポート
  - http://blog.mozilla.com/it/2010/09/16/mozilla-outage-report-mozilla-org-dnssec-09162010/

beの失敗

- 発生事象
  - 2010.10.7にbeゾーンの署名検証が失敗する事象が発生
- 原因
  - 署名の期限切れ
- 参考情報
  - https://lists.dns-oarc.net/pipermail/dns-operations/2010-October/006166.html

frの失敗

- 発生事象
  - 2011.2.12にfrゾーンの署名検証に失敗する事象が発生
- 原因
  - BINDのバグによりNSEC3レコードの更新に失敗
- インシデントレポート
  - http://operations.afnic.fr/en/2011/02/18/study-and-action-plan-following-the-incident-with-validating-resolvers-on-12-february-2011.html

e164.arpaの失敗

- 発生事象
  - 2011.2.15にe164.arpaゾーンの署名検証が失敗する事象が発生
- 原因
  - 署名システムのバグで、鍵更新の際にKSKのRRSIGが生成されなかった
- インシデントレポート
  - http://dnssec-deployment.org/pipermail/dnssec-deployment/2011-March/004842.html

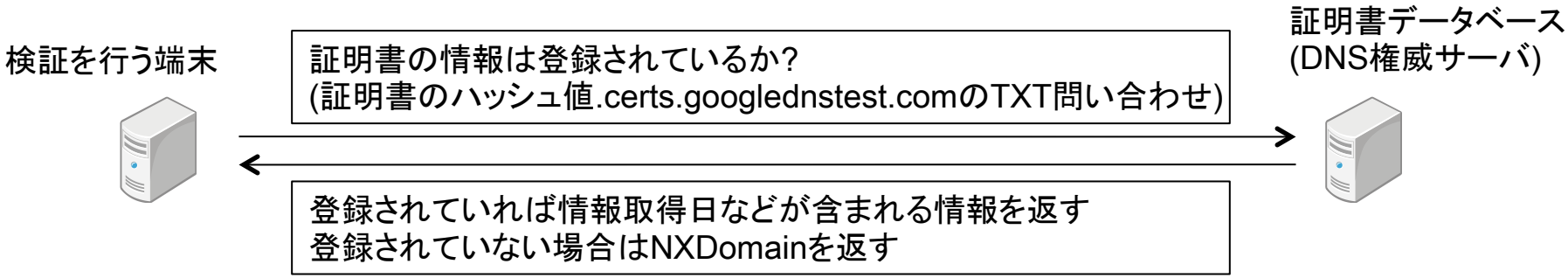
kgの失敗

- 発生事象
  - 2011.2.22にkgゾーンの署名検証が失敗する事象が発生
- 原因
  - RRSIGレコードの有効期間の開始時刻が未来の時刻になっていた
- 参考情報
  - http://dnssec-deployment.org/pipermail/dnssec-deployment/2011-February/004816.html

DNSSECを利用したアプリケーション

DNSを用いたSSL証明書の検証

- SSL証明書の情報をDNSのリソースレコードに登録しておき、情報の有無によって証明書の信頼性を検証する技術が提案されている
  - GoogleやIETFのWGで提案されている
  - 検証結果の信頼性のために、DNSSECが必須
- Googleが提案している技術の例



- 参考情報
  - Googleが公開しているブログ記事
    - http://googleonlinesecurity.blogspot.com/2011/04/improving-ssl-certificate-security.html
  - IETFのDNS-based Authentication of Named Entities (dane) WG
    - https://datatracker.ietf.org/wg/dane/charter/