Activity of Protocol Study Sub Working Group

Jul/21/2010

Koh-ichi Ito

motivation

- 私事ですが…
- DNSのことは、そこそこ知っているつもり。
- でも電子署名とか暗号化とかは…ニガテ
- カミンスキー氏がアタック手法を発見して以来、DNSSECって、よく話題になるよね。
- いっちょRFCに目を通してみるか。
- さっぱりわかんねーぜ…

- Speaking on myself…
- I know DNS so-so well.
- But digital signature or cryptography are out of my field, rather poor at.
- DNSSEC is often mentioned since Kaminskey attack.
- Okey, let's study RFC.
- Ugh! it's quite difficult…

establish

- DNSSECジャパンが設立された。
- 活動の一環ってことでDNSSEC関連のRFCをネタにした勉強会、やりませんか?

- DNSSEC.jp has established.
- Let’s organize study group on DNSSEC related RFCs as a part of activity of DNSSEC.jp.

why RFC?

- Standards Trackの一次情報源。
- Informationalにも役に立つ情報がある。
- とっかかりになる本が、まだない!

- They’re primary source of Standards Track.
- Some useful Informational articles.
- No settled primer book yet!

meetings

- 隔週で会合をやってます。
- 「本日のRFC」を輪講しています。
- アドバイザーとしてJPRSの森さんにおいでいただいています。
- JPNICのご好意で会議室をご提供いただいています。

- Holding meetings every two weeks.
- Seminar style discussion on topic RFC of the day.
- Invite Mori-san from JPRS as an advisor.
- Meeting room is provided by JPNIC by there courtesy.

meetings(cont'd)

- 通算では11組織から26名が参加。
- 最近の実績としては15人程度が定着。
- お客様は無し。全員に分担あり。
- 今年3月から8月にかけて10回の会合を予定しています。
  - うち7回済んで残り3回。

- 26 guys from 11 organizations attended in the past.
- Approx 15 attendance on recently actual.
- No guest, everybody has each duty.
- 10 meetings are scheduled from last Mar. to coming Aug.
  - 7 of 10 has done, 3 left.

meetings(cont'd)

Photo by Miki Takata@Publication WG

RFCs(done)

- RFC 4033
  - DNS Security Introduction and Requirements
- RFC 4034
  - Resource Records for the DNS Security Extensions.
- RFC 4035
  - Protocol Modifications for the DNS Security Extensions
- RFC 5011
  - Automated Updates of DNS Security (DNSSEC) Trust Anchors
- RFC 5155
  - DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

RFCs(planned)

- RFC 4641/i-d *<- Now Working!*
  - DNSSEC Operational Practices./it's ver.2
- RFC 4509
  - Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs).
- RFC 5702
  - Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource
- RFC 4431
  - The DNSSEC Lookaside Validation (DLV) DNS Resource Record.
- RFC 4986
  - Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover.
- RFC 5074
  - DNSSEC Lookaside Validation (DLV).
- i-d
  - DNSSEC Key Timing Considerations

goal

- DNSSECは大変(だけど|だから)、正しい運用のための正しい情報を的確な人に。
- Though, or because, DNSSEC is hard, right knowledge for right operation to right person.

- ご清聴ありがとうございました。
- Thanks for your interest.