DNSSECの提供する信頼性に関する一考察 + root blackout対策案

個人

Kazunori Fujiwara

<fujiwara@wide.ad.jp>

2012/4/25 dnsops.jp

Wikipediaより

- 公開鍵基盤(PKI)は、利用者の身元について「信頼できる第三者」が審査を行い、保証を実現する仕組みのことである。

- DNS Security Extensions（略称DNSSEC）は、DNSにおける応答の正当性を保証するための拡張仕様である。
  - # 保障するのはだれ？
    - Zone operator本人？ Registrar？ Registry?

DNAE

- The DNS-Based Authentication of Named Entities (DANE) Protocol for Transport Layer Security (TLS)
  - draft-ietf-dane-protocol
- TLSA RRにTLSで使われる証明書を登録するもの
- name IN TLSA Usage Selector Type Data
  - Usage: 0..CA certificate, 1..end entity certificate, 2..trust anchorなど?, 3..自己署名証明書Certificate
  - Selector: 0..Full certificate, 1..SubjectPublicKeyInfo
  - Type: 0..証明書をそのままDataへ, 1..Dataは証明書のSHA256, 2..Dataは証明書のSHA512
  - Data: 証明書そのもの、ハッシュ

DANEの使い方

- 自己署名証明書を作る
- TLSA RRに書く

- ブラウザなどは、ドメイン名を入力されると
  - TLSA RRを検索 (with DNSSEC validation)
  - 自己署名証明書を信用してTLS通信開始
  - ということで、新規にTLSクライアントを書く必要あり

サーバ証明書の種類

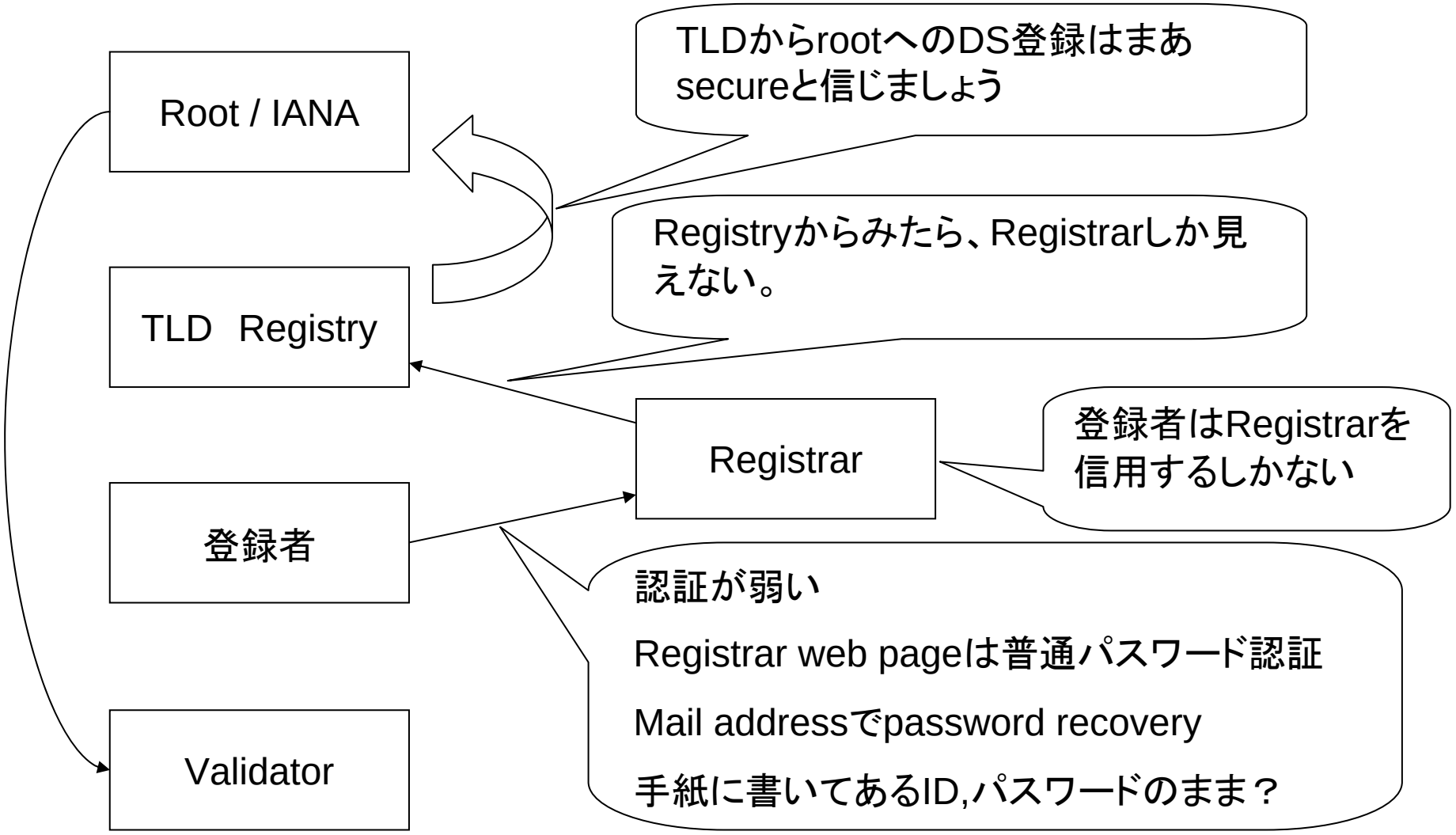
- 参考にしたページhttp://rs.impressrd.jp/e/2009/03/31/402
- ドメイン認証
  - メールが届けば発行してもらえるのもある
  - 安いのもある (年$10とか)
  - 組織が実在するかは証明してもらえない
- 組織認証
  - 法人などに限定、組織の確認あり、電話？登記簿？
- EV SSL
  - 組織認証よりきつい調査？
  - 高い値段
  - ブラウザの色が変わる
- 買い物や銀行口座を扱うときはどれを使うのがよいか？
  - 組織認証かEV SSLがいいけど
  - ドメイン認証と組織認証の証明書の違いがブラウザでわかりにくいので、組織認証の立ち位置が不明瞭
    (ユーザからみたら手間と高いだけ？)

DANEで設定したサーバ証明書

- 自ゾーン内にTLSA RRを書き、自己署名証明書を登録し、DNSSECでsign
- ドメイン名を登録したのと同じインターフェースでDS登録

- ドメイン認証と同レベル
  - メールが受け取れれば出してもらえるサーバ証明書
  - 自分でTLSA RRを用いて設定した自己署名証明書

DNSへの登録の悩みどころ



DANEのみに頼るモデル

- 高いサーバ証明書いらないという主張をしたい場合

- ある名前空間(TLD)において
  - TLDレジストリがレジストラを完全に信用でき
  - レジストラは「組織認証」レベルのチェックを行い
  - DSの取次ぎを行う
    - DS設定には、なんらかの強力な認証手段を使う
- 専用のTLDがあれば解決するかも

結論と雑感

- DNSSEC+DANEでサーバ証明書がいらなくなるわけではない
  - 組織認証やEVはない
- 個人で使う用途ならばDNSSEC+DANEで十分だが、アプリケーションが対応していないので、しばらくは安いサーバ証明書を使うのがよいのではないか

root blackout対策

- dnsops 1189
- Root DNS serversが攻撃されて到達できなくなること？
- 対策案
  - Full-Resolverにroot zoneを持たせる
  - 問題
    - Unboundじゃできない？
    - BIND 9では、Root trust anchorを設定してもDNSSEC validationしなくなる

Root zoneを持たせる方法

- BIND 9の場合はFull-Resolver viewの中にroot zoneを持たせる
- Root zone供給元は3とおり
  - http://www.internic.net/domain/root.zone
    - zone “.” { type master; file “root.zone”; };
    - 定期的にアップデートすること
  - f.root-servers.net
    - https://lists.dns-oarc.net/pipermail/dns-operations/2007-August/thread.html#1891
    - zone “.” { type slave; file “……/root.slave”; masters {192.5.5.241;};notify no;};
  - ICANN　http://dns.icann.org/services/axfr/
    - zone “.” { type slave; file “……/root.slave”; masters {….;};notify no;};

- でも、rootにいけないなら、TLDやら各組織にもいけない可能性が強い

- がんばる必要はないような気がします