インフラとしてのDNS
Contentsを守るには（DNSSEC）

IW2004 DNS Day
2004年12月3日
藤原和典 <fujiwara@jprs.co.jp>
株式会社日本レジストリサービス

内容

- DNSの用途
- DNSの動作
- DNSへの攻撃
- DNSSECプロトコル
- DNSSEC普及活動
- DNSSECの実際

DNSの用途(現在)

- ホスト名の解決　whois.jprs.jp
  - 各種サーバの名前として
    - メールサーバ、IP電話サーバ、認証サーバ、ゲームサーバ等
- 電子メールのアドレスの解決　info@jprs.jp
- web URIの解決　http://jprs.jp/

- DNSが検索できないと、IP的に接続できていても「インターネットが使えない」といわれてしまう。
- すでにDNSはインフラである

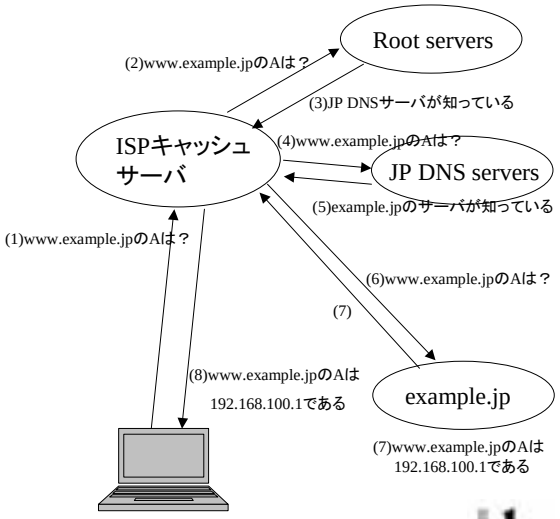
DNSの用途(これから)

- IP電話の名前解決
  - SIP URI
  - ENUM
- 認証情報
  - 電子メールのSPAM対策情報（SPFなど）
  - IPSECKEY
  - SSHKEY

- これまでよりも改竄されると社会的影響が大きい情報がDNSに載ろうとしている

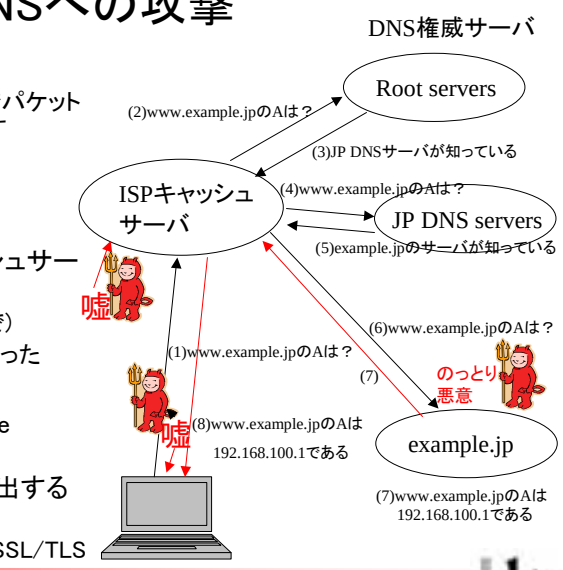
DNSの動作(復習)

- ユーザのマシンはISPのキャッシュサーバに問い合わせを行う(1)
- キャッシュサーバはRootから順にたどり、アドレスを解決する(2～7)
- キャッシュサーバはユーザのマシンに得られた結果を回答する(8)



DNSへの攻撃

- 盗聴
  - Monkey-in-the-middle
  - 共有イーサネットや無線LANでパケットを監視し、嘘の応答を先に返す
  - (1)を見て(8)より前に嘘を返す
- Cacheサーバへ嘘を注入
  - (3)や(5)、(7)を推定し、注入
- 嘘のglueを書いておき、キャッシュサーバに注入
  - 他人の名前のAを返すなど(7で)
  - 多くの実装で無視するようになった
- DNSサーバをのっとり
- RFC3833 Threat Analysis of the Domain Name System (DNS)
- 従来は、嘘をつかれたことを検出する方法がなかった
  - アプリケーションで対策 SSH, SSL/TLS



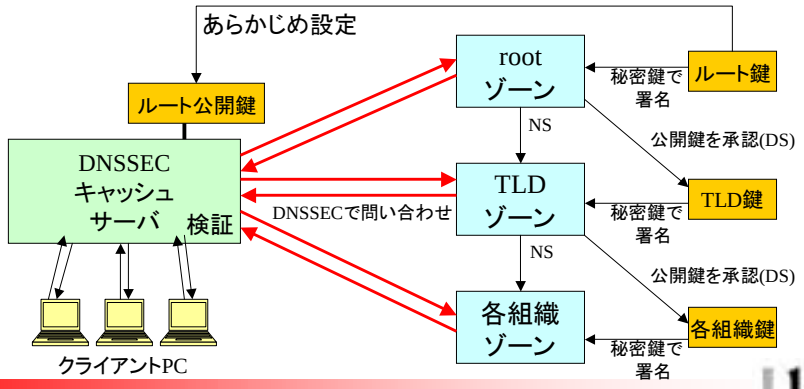
DNSSECプロトコルの概要

DNSSECとは

- DNS Security Extension
- DNSゾーンに権限を持つ管理者が、公開鍵暗号技術を用いて、自らのゾーン情報に秘密鍵で署名を行うDNSの運用方式
  - そのゾーン情報の第三者による改ざん・騙りを検証することが可能となる技術
    - ゾーンの公開鍵で検証
  - これにより、万一にも騙りを許したくないDNSレコードを守ることが可能となる

DNSSECの概念

- 鍵による信頼の連鎖 (chain of trust)を形成
- あらかじめ設定したルート鍵からキャッシュサーバが検証

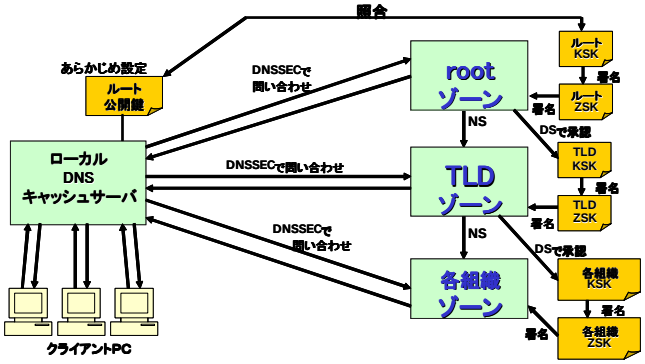


DNSSEC方式

- RFC2535で定義され、RFC3658で改良
  - 運用上のオーバーヘッド軽減
- ゾーン管理者は2つの鍵を使用
  - 弱めの鍵を自ゾーンの署名のために用いる(768bitや1024bit)
    - ZSK (Zone Signing Key): 自ゾーンの署名のための鍵
    - 署名コストが低い、頻繁に鍵を変えることを想定
  - 強めの鍵を上位からの信頼連鎖に使用 (2048bitや4096bit)
    - KSK (Key Signing Key): 自分のZSKの署名のための鍵
    - 強い鍵は有効期限を長くできるが、署名のコストが大きい
    - KSKの公開鍵情報を親ゾーンに登録
- DS(Delegation Signer)資源レコード
  - KSK公開鍵情報と暗号論的に等価なDS情報を作成
  - 親ゾーンの委任ポイント(NS)に子ゾーンのDS情報を登録
  - DSにより子ゾーンのKSKの正当性を親ゾーンが承認
- ルートの公開鍵情報を、DNSSEC検証者が持つ
  - 主にDNSキャッシュサーバ

DNSSECの概念(2)

- 鍵による信頼の連鎖 (chain of trust)を形成
- KSKとZSKの2つの鍵を使用



PKIとDNSSECの認証モデルの違い

	PKI(X.509)	DNSSEC
信頼関係	信頼できる第三者機関(認証局)が公開鍵の登録者を保証	レジストリが、登録者のドメイン名の公開鍵を保証
信頼ツリー	認証局→登録者 (認証局相互の相互認証などもあり)	ルート→TLD→登録者
登録手続き	登録者→認証局	登録者→レジストラ→レジストリ
信頼性確認	認証局が登録者を審査 (物理的手段による確認など) (認証局が提供する信頼度)	レジストリがレジストラ経由で登録された情報を信用 (ドメイン名と同じ信頼度)
認証局	登録者が選択可能	登録ドメイン名のレジストリ
ルート証明書	認証局ごとにあり	一つのみ(ルート公開鍵)
失効手続き	あり	不要(ルートの失効手続きは必要)

DNSSEC標準化(IETF)の現状

- IETF　dnsext wgにおいて、DNSSECプロトコルを策定
  - Delegation Signer (RFC3658)
  - NSEC RR (RFC3845)
  - http://www.ietf.org/html.charters/dnsext-charter.html
- 未解決の課題
  - ルート鍵の運用
    - DNSSEC普及のためのWG(後述)で検討中
  - 現在の仕様では、ゾーン内のデータを網羅検索可能
    - ラベルの非存在を証明するため
      - 前後する二つの名前の間に名前がないという応答を返す
    - セキュリティ、プライバシー的な懸念
    - IETF dnsext wgで対応方式を検討中

DNSSEC対応のDNSサーバ

- DNS権威サーバ(Authoritative server)
  - BIND 9.3系列で対応
    - 最新は9.3.0
  - NSD 2.0.0以降で対応
    - 最新は2.1.4
- DNSキャッシュサーバ
  - BIND 9.3系列で対応
    - 最新は9.3.0

DNSSECの課題

- キャッシュサーバの更新が必須
- 安全な鍵配布・鍵更新の手順が別途必要
  - ルート鍵の配布
  - 各組織の鍵の取り扱い
- アプリケーションのDNSSEC対応が必要
- ルートサーバ、TLDでの対応

DNSSECの普及活動

DNSSEC Deployment WG

- DNSSEC普及のためのWG
- http://www.dnssec-deployment.org/ (作成中)
- http://www.nanog.org/mtg-0410/crocker.html

- DNSSECプロトコル開発者、DNSサーバ開発者、IANA、ルートサーバオペレータ、TLDなどが参加

- 普及のためのロードマップ、普及のための課題の検討

各国の動向

- US政府
  - US政府はDNSSECの必要性を認識している
  - the U.S. Department of Homeland Security
    - DNSSEC Deployment WGをサポート
  - FCC
    - NANOG32での講演
    - http://www.nanog.org/mtg-0410/marcus.html

- .US Registry
  - 実際的なトライアルを開始
    - http://www.iepg.org/november2004/
- .NL Registry
  - http://www.nlnetlabs.nl/dnssec/

ETJP DNSSEC実験

- ENUM Trial JAPAN
- e164.jp, dnssec.jpにてDNSSEC実験
- ETJP参加者であれば参加可能
- e164.jp、dnssec.jpの鍵をもとに検証
- 実験概要
  - 1.8.e164.jp以下にENUM型ドメイン名を登録
  - dnssec.jp以下にドメイン名を登録
  - 登録したドメイン名の鍵を登録
  - DNSSECの検証が可能

- ETJP DNSSECテストベッド関連資料
  - http://etjp.jp/about/wg/dnssec.html

DNSSECの実際

DNSSEC対応の方法(概要)

- コンテンツサーバ
  1. BIND 9.3(9.3.0以降)をインストールする
  2. 鍵対(秘密鍵、公開鍵)を作成する
     - dnssec-keygenコマンド使用
     - 正しくは2つの鍵対(ZSK、KSK)を作成する
     - ゾーンごとに必要
  3. 鍵対の公開鍵情報をゾーンに設定する
  4. 秘密鍵を用いてゾーンに署名する
     - dnssec-signzoneコマンド使用
     - 上位に登録する情報が生成
       - dssetファイル
  5. 生成されたdssetを上位ゾーンに送り設定してもらう
  6. named.confのoptionsにdnssec-enable yes; を追加

DNSSEC対応の方法(概要)

- キャッシュサーバ
  1. BIND 9.3(9.3.0以降)をインストールする
  2. 上位(信頼ツリーの最上位)DNSサーバの公開鍵情報を取得する
     - 信頼ツリーが複数存在する場合は、その分だけ必要
  3. 取得した公開鍵情報をtrusted-keysとしてnamed.confに設定する
  4. named.confのoptionsにdnssec-enable yes; を追加

ETJP DNSSEC登録システムでの登録

日本での評価

- TAO(現NICT)委託研究としてJPRSが受託
  - 「次世代DNSに関する研究開発」
  - TAO(現NICT)委託研究
  - 2001年8月から2004年3月にかけて実施
  - JPでDNSSECを適用する場合の実現方法評価
    - レジストリシステム
    - DNSサーバ性能

JPドメイン名へのDNSSEC適用可能性

（平成15年度「次世代DNSに関する研究開発」研究開発成果報告書より引用）

- 2004年3月に実施
- DNSSEC署名時間
  - jp, co.jpゾーンで約1時間
- 上記で署名したゾーンの読み込み時間
  - 約1分
- 上記ゾーン導入後のDNSSECサーバのパフォーマンス
  - 約12,000qps
    ⇒JPドメイン名での実運用に**対応可能なレベル**であることを確認
- DNS応答時間
  - DNSSEC処理により応答時間が最大約10ms増加

  ⇒ユーザへの**影響がほとんどない**ことを確認

まとめ

- インターネットはいまやインフラストラクチャとなった
- DNSは未だにインターネットで唯一の名前解決手段
- 従来のDNSには応答の正しさを検証する手段がない
- DNSSECは必要である
  - DNSだけ守っても仕方がないという意見あり
  - セキュリティは安全の積み重ねで守るもの
- 手元でDNSSECの運用実験できる環境はできてきた
- 現在のDNSSECは技術的には運用可能である

- これからの展開は？

Q&A