DNSハンズオン (1)

ドメイン名登録, DNSサービス
権威DNSサーバ, DNSSEC編

藤原和典 fujiwara@jprs.co.jp
株式会社日本レジストリサービス

2016/11/30

Internet Week 2016

Last Update: 2016/11/28 1340 JST

配布物の確認

- VMのIPアドレス、パスワード
- JP Directのドメイン名、ID、パスワード

概要

- DNSを使うまで (藤原)
  - DNS概要
  - 実習: ドメイン名登録
  - 実習: 権威DNSサービスの使用
  - 実習: DNS設定の確認
  - 実習: Public DNSの使用
  - 実習: フルサービスリゾルバの設定 (高田)
  - 実習: 権威DNSサーバの設定
  - DNSSEC概要
  - 実習: DNSSECの設定
- 実習:DNSSECトラブルシュート編(其田)

ハンズオンでやらないこと

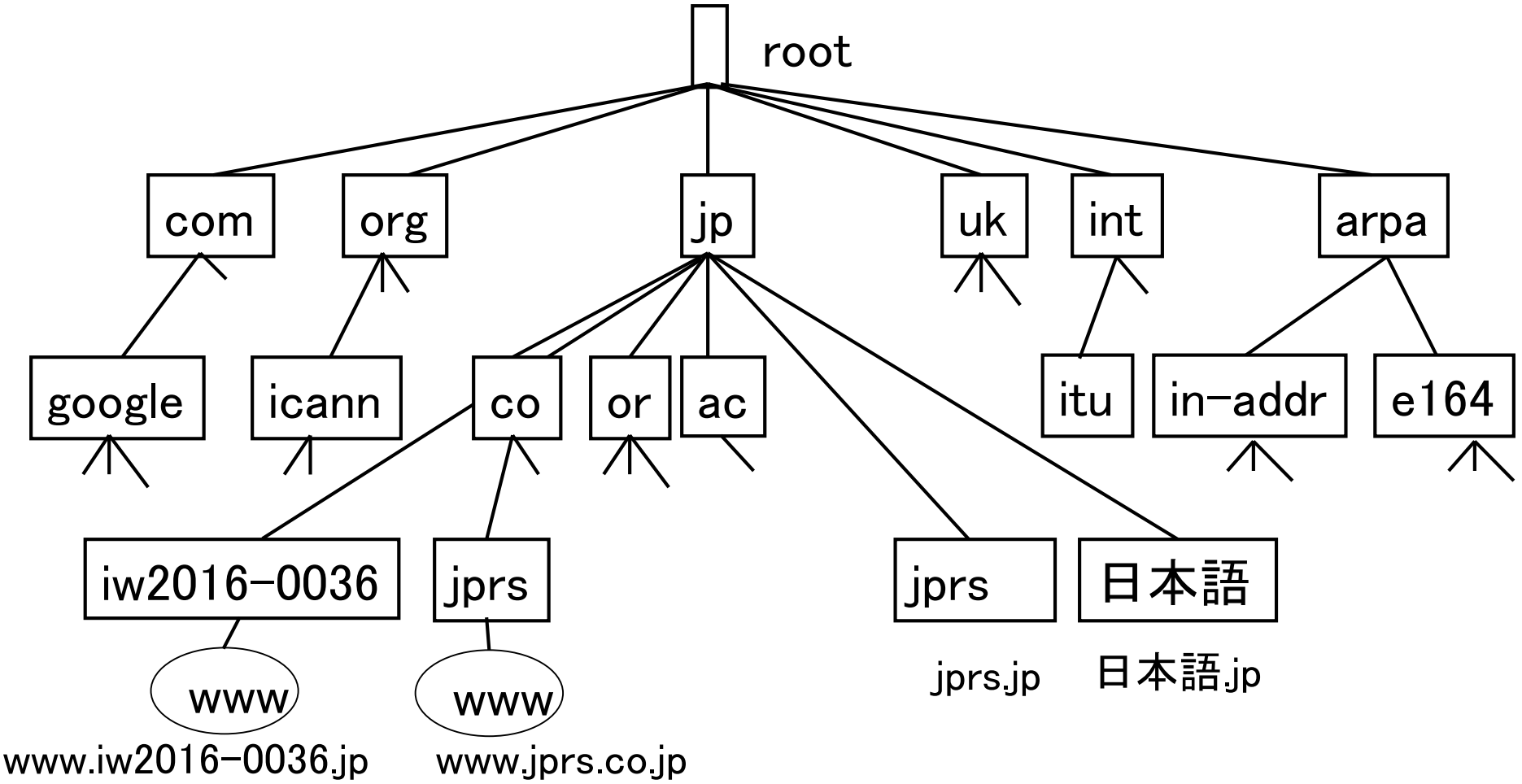
- 実際のドメイン名の登録
  - 登録にはクレジットカードが必要なため
  - 準備したドメイン名を使用
- Firewall設定/パケットフィルタ
  - iptablesなどの設定はOSによって違うため
  - 用意した環境では、DNS, ssh のポートは開放済み
  - 設定ミスすると実習できないため
- NSD, Unboundの自動起動の設定
  - OSによって設定方法が異なるため
  - Linuxでもdistribution, versionによって異なる
- VMのreboot
  - 起動しなくなったら実習できないため

DNS概要

ドメイン名

- ドットで区切られた文字列
- インターネットにおける一意な識別子
- URL, メールアドレスなどの構成要素
  - http://www.nic.ad.jp
  - fujiwara@wide.ad.jp
  - ssh sh.wide.ad.jp
- ドメイン名を使わないと、
  - http://192.168.100.1/
  - ssh 2001:0DB8:1234:5678:9abc:def0:fdb9:7531
- IPアドレスなどの情報を抽象化するもの

ドメイン名ツリー



Domain Name System (DNS)

- ドメイン名と対応する情報の対応づけを行うインターネット上の分散データベース
  - 階層的に管理
- 基本機能: ドメイン名に対応する情報を登録・検索
  - IPアドレス(IPv4, IPv6）: Webサーバ, ホスト
  - メールサーバ情報 (MX)
  - SIPサーバなどのサービス情報 (SRV)

前DNS時代

- ホスト名とIPアドレスの対応表(HOSTS.TXT)を共有
  - HOSTS.TXTをインターネットの全ノードにコピー
- 更新はファイル管理者(SRI-NIC)にメールで通知
- ホスト増加で破綻
- 1985年3月，最初のDNS登録

委任(delegation)

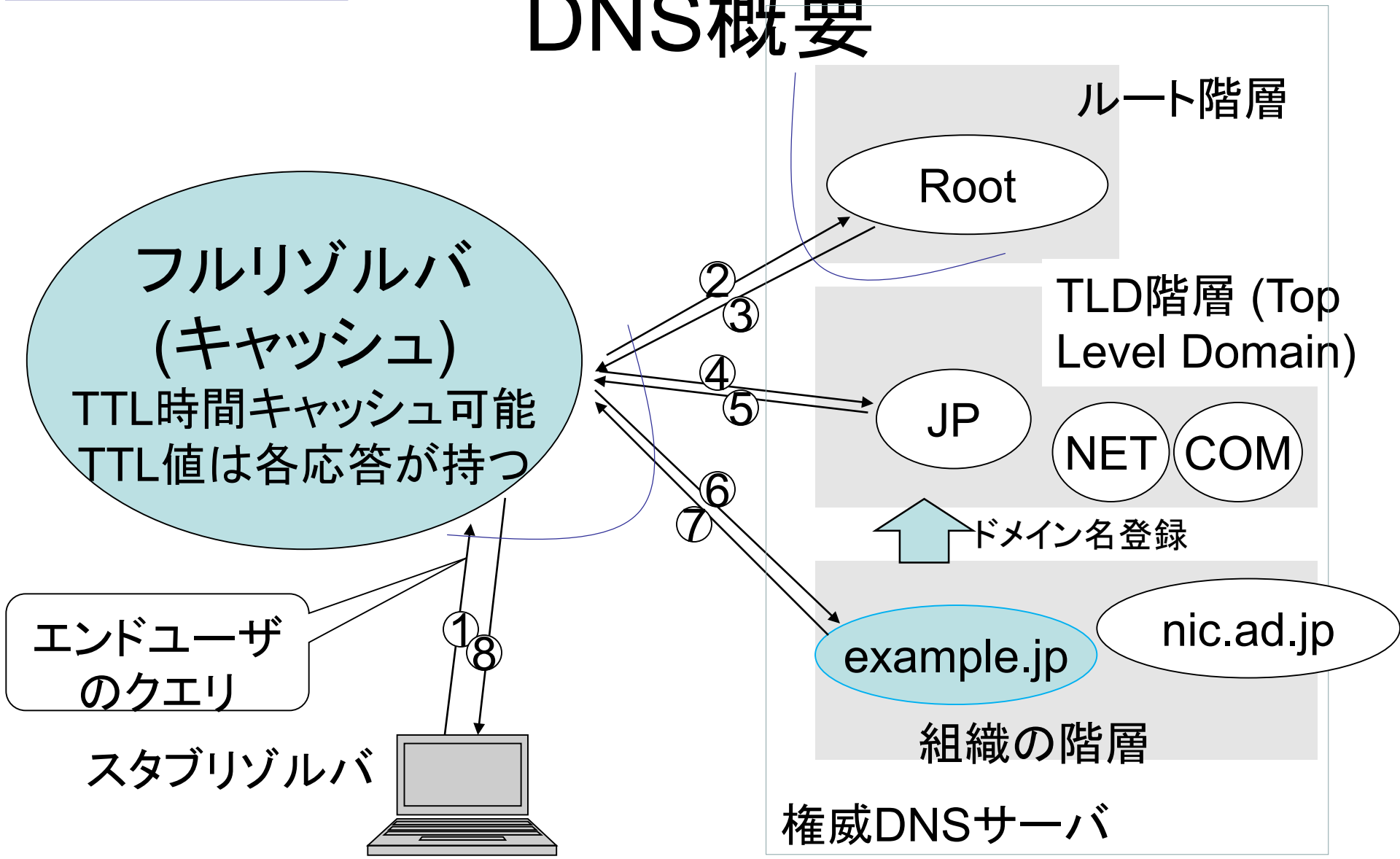
- 各階層において下位の名前管理を委任
  - RootからJPを委任 (委任先のネームサーバ指定)
  - JPからinternetweek.jpを委任 (委任先のネームサーバ指定)
  - 委任された単位をゾーンと呼ぶ
- 委任先(下位)
  - その階層の名前の登録管理
  - さらに下位に委任
- ラベル(ドット区切り)ごとに委任可能
  - 委任しなくてもよい (ac.jp, go.jpなどは委任ではない)
  - ゾーンの中に複数のドット区切りを含む委任/名前があってもよい (例: jpからnic.ad.jpを委任)

DNSサーバ(ネームサーバ)

- 権威DNSサーバ
  - ゾーンの情報を保持するもの
  - ゾーンごとに存在
    - ルート
    - TLD (Top Level Domain) … JPなどのラベル一つのもの
    - 各組織
- フルサービスリゾルバ (フルリゾルバ)
  - 名前解決を行う機構をリゾルバと呼ぶ
  - そのうち、ルートから各階層をたどるものをフルサービスリゾルバと呼ぶ
  - 名前解決の効率化のために、途中結果をキャッシュする

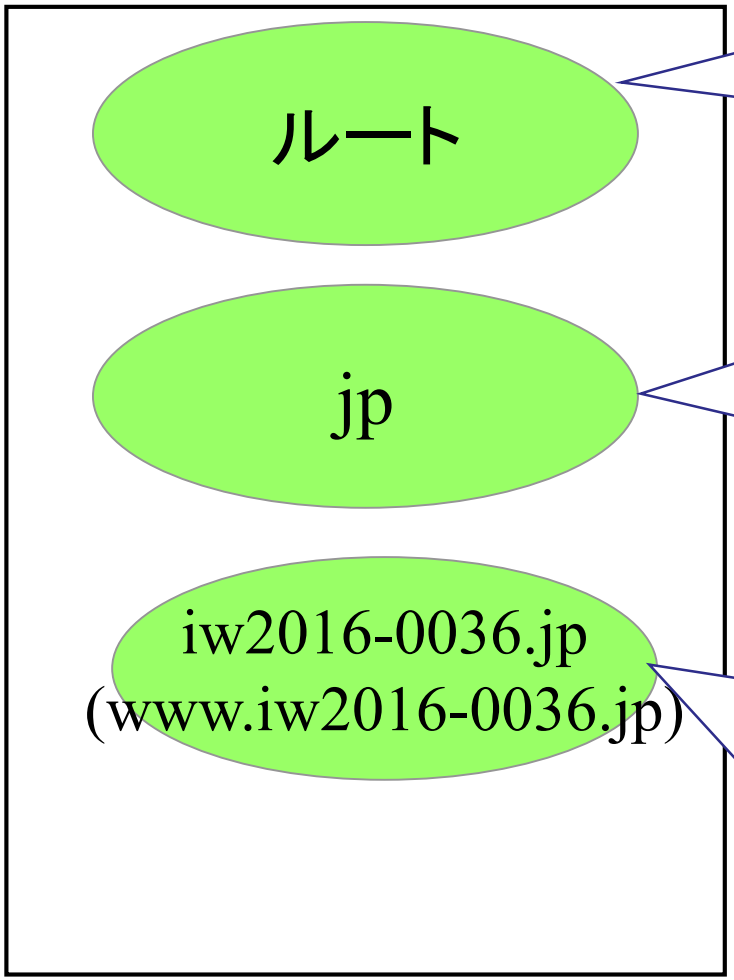
本日の実習範囲

DNS概要



(0)http://www.example.jp/ とブラウザに入力

委任例

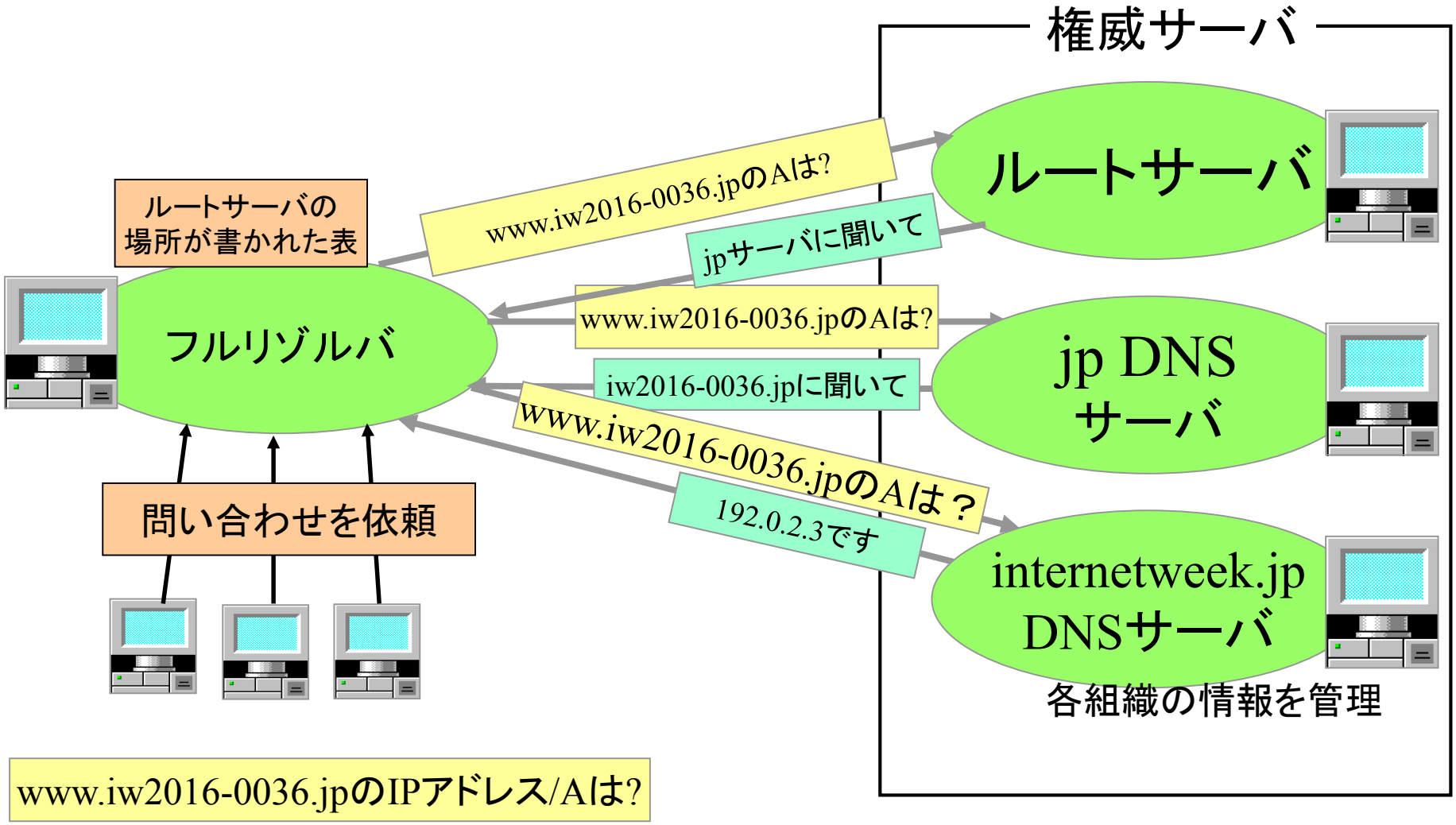


jp. IN NS a.dns.jp.
jp. IN NS b.dns.jp.
…
a.dns.jp. IN A 203.119.1.1
a.dns.jp. IN AAAA 2001:dc4::1

iw2016-0036.jp. IN NS ns1.iw2016-0036.jp.
(委任と委任先ネームサーバ情報)
ns1.iw2016-0036.jp. IN A 192.0.2.2
(ホスト情報　ホスト名とIPアドレス)
ドメイン名登録窓口から設定

iw2016-0036.jp. IN SOA iw2016-0036.jp.
root.iw2016-0036.jp.
1 300 900 120960 300
iw2016-0036.jp. IN NS ns1.iw2016-0036.jp.
ns1.iw2016-0036.jp. IN A 192.0.2.2
www.iw2016-0036.jp. IN A 192.0.2.3
ドメイン名登録者が設定、DNSサーバ運用

問い合わせの方法



www.iw2016-0036.jpのIPアドレス/Aは?

DNSサーバに登録する情報(1)

- リソースレコード
- 管理情報: Authority情報(SOA)
  - owner IN SOA MNAME RNAME SERIAL REFRESH RETRY EXPIRE MINIMUM
    - MNAME: ゾーンのマスターサーバ名
    - RNAME: ゾーン管理者のメールアドレス
    - SERIAL: ゾーンのシリアル番号 (32ビット正数)
    - REFRESH: ゾーン転送パラメータ、ゾーン転送の間隔(秒)
    - RETRY: ゾーン転送パラメータ、転送失敗時のリトライ間隔(秒)
    - EXPIRE: ゾーン転送パラメータ、ゾーン転送からのゾーン情報有効期間(秒)
    - MINIMUM: negative cache TTL値
  - 例: iw2016-0036.jp IN SOA iw2016-0036.jp. root.iw2016-0036.jp 1 3600 900 120960 300

DNSサーバに登録する情報(2)

- 委任情報(NS)とネームサーバ情報に対応する情報
  - iw2016-0036.jp IN NS ns1.iw2016-0036.jp
  - ns1.iw2016-0036.jp IN A 192.0.2.2
- IPアドレス(A, AAAA)
  - www.iw2016-0036.jp IN A 192.0.2.3
  - www.iw2016-0036.jp IN AAAA 2001:0db8::1
- user@iw2016-0036.jpのメールサーバー(MX)
  - iw2016-0036.jp. IN MX 100 mail-server.iw2016-0036.jp

TLD(JP)に登録する情報(例)

- 委任ドメイン名とネームサーバ名(委任情報, NS)
  - 例: iw2016-0036.jp IN NS ns1.iw2016-0036.jp
- ネームサーバのアドレス情報(Glue records)
  - 例: ns1.iw2016-0036.jp IN A 192.0.2.2
- Glue recordsを添付できる条件
  - 上位ゾーン (jp) の子孫のホスト名(上位ゾーンの内部名)であること
  - jpゾーン内には、jp以外のホスト名のアドレス情報を添付できない
- Glue recordsを添付しないといけない条件
  - 委任の子孫のホスト名(委任の内部名)であること
  - 委任の子孫のホスト名のアドレス情報を添付しないと、名前解決できない

ハンズオン実習環境

端末

- 各自のノートPC
  - Webブラウザ
  - sshクライアント(Tera Term, Putty, Cygwinなど)
  - コマンドプロンプト
  - ターミナルエミュレータ
- ネットワーク: 会場ネットワーク

ハンズオンの実習環境

- VM
  - 株式会社インターネットイニシアティブ (IIJ) 提供
  - 本日中のみ有効
  - CentOS 6.8
  - IPアドレス、パスワードを記した紙配布
  - Rebootしないでください
  - 起動しなくなると実習できなくなります
  - iptablesの設定やinit.dの設定変更などはしないこと
- Login方法
  - OpenSSH: ssh admin@IPアドレス
    - パスワード認証で、パスワードを入力
  - Tera Term
    - New connection → TCP/IP, SSH, Host入力, OK
    - 接続できたところでユーザ名、パスワード入力

ハンズオンで使用するドメイン名

- 登録済ドメイン名を実習用に提供
  - 株式会社日本レジストリサービス(JPRS) 提供
  - 本日中だけ有効
  - 配布したID, パスワードで、jd-login.jp にログイン
  - ドメイン名: iw2016-0036.jp など (0001~)
  - IDはドメイン名と同じ
  - 新規登録や廃止、支払い、パスワード変更、移転などは行なわないでください
    - 実習ができなくなります

実習
ドメイン名登録

ドメイン名の登録

- レジストラ、リセラ (ISPなど) の受付窓口
  - JPドメイン名:　jpshop.jp
  - gTLD: ICANN-Accredited Registrars
    - https://www.icann.org/registrar-reports/accredited-list.html
  - gTLD Registrarのシェア
    - http://www.domainstate.com/registrar-stats.html
    - 資料公開時には表を削除

1	GoDaddy	US	6	HiChina	CN
2	eNom	US	7	1&1 INTERNET	DE
3	Tucows	CA	8	eName	CN
4	Network Solutions	US	9	GMO Internet	JP
5	Direct Internet Solutions	IN	10	Wild West Domains	US

ドメイン名の登録手順

- レジストラを選ぶ (あるいはISPに依頼)
  - 実習: 世界シェア9位のGMO Internet を試す
  - ブラウザで onamae.com を開く
- 登録したい文字列を入力し、検索ボタンを押す
- 空いていれば、値段が出る
- 新規契約者はアカウントを作成する
- レジストラのID, パスワードでログインする
- 金を払う (クレジットカード情報の入力など)
- 登録完了
- (属性型JPドメイン名などは登録要件があるので、その他の手続きが必要)

ドメイン名の使い方

- ドメイン名の使い方
  - レジストラのほとんどはDNSサービスやホスティングサービスを提供しているので、そのままクリックするだけでメールサーバやWebサーバを契約できる
  - 本日は、DNSサービスの設定と、ネームサーバ設定をして自分で動かす実習を行う

実習: ドメイン名設定(1)

- JPDirectは株式会社日本レジストリサービスが提供するドメイン登録管理サービス
- ブラウザで jd-login.jp を開く
  - ID, パスワードを入力して「ログイン」を押す
  - 「次へ」を押す
  - ドメイン名管理の画面が表示される
  - 左に操作メニュー、右に案内や操作画面
- お願い
  - 新規登録や廃止、支払い、パスワード変更、移転などは行なわないでください
  - (実習ができなくなります)

実習: ドメイン名設定(2)

- (クリックして画面遷移を確認するだけ)
  - 何か行なったあとは「戻る」や左の各操作を押す
- “登録ドメイン名一覧参照”をクリック
  - 登録されているドメイン名が一つ見える
  - 例: iw2016-0036.jp
- “ネームサーバ設定・変更・解除申請”をクリック
  - ドメイン名が表示されるので選び「次へ」をクリック
  - 現在の設定内容が表示され、設定変更できる
- “ホスト情報”
- “DNSサービス設定”
  - 自前でDNSサーバを運用しなくてもドメイン名を運用できる

事業者のDNSサーバの使用

- 自分でDNSサーバを動かさなくても、簡単なことならできることを学ぶ

実習: DNSサービス使用

1. “DNSサービス設定”をクリック
2. ドメイン名を選択して、次へ
3. ホスト名を入れる項目と、タイプごとの値を入れる項目が表示されるので、入力する
    1. Aに、ホスト名 “@”, IPアドレス “202.221.128.104”
    2. Aに、ホスト名”www”, IPアドレス “202.221.128.104”
    3. それ以外の項目は空のままとする
4. 「同意して次へ」を押す
5. 設定確認画面が表示されるので、「この内容で確定する」を押す
6. 一定時間後、使用可能になる

この設定をすることで、自分でDNSサーバを動かさなくてもDNSの使用ができる

例 www.iw2016-0036.jp の A は 202.221.128.104

DNS設定の確認

DNS設定の確認方法

- 確認ツール
  - dig: BIND 9付属
  - nslookup (BIND 9付属だが古いため非推奨)
    - 標準添付の場合あり
  - drill: NLnet Labs製 (NSD, Unbound開発元)
- 確認方法
  - drill @IPアドレス ドメイン名 タイプ
  - drill @202.12.27.33 com A
  - オプション多数 (dig, drillで異なる)
- RDビットを意識してオプションを追加すること
  - drill -o rd / -o RD
  - dig +recurse / +norecurse
  - RDビットの説明と、今後のオプションの使用を省略

DNS設定の確認

- コマンドプロンプト/ターミナルでdrillまたはdigコマンドを使用
- 開発者作成の非公式バイナリ
  - http://www.nlnetlabs.nl/~willem/drill.exe
- 例: drill.exe @8.8.8.8 internetweek.jp A
  dig @8.8.8.8 internetweek.jp A

- ブラウザでダウンロードすると多くの場合は以下の場所にdrill.exeがあるので好きな場所にコピーして使うこと
  - %USERPROFILE%¥Downloads

DNS設定の確認方法(ブラウザ)

- dnsviz.net
  - Sandia National LaboratoriesとVerisignが提供するチェックツール
- dnscheck.jp

実習: DNSサービスの確認

- 割り当てられたドメイン名をブラウザでアクセス
  - 例: www.iw2016-0036.jp
  - ホスト名(Host:) を確認
    - 例: www.iw2016-0036.jp と表示される
- drill / dig で確認
  - drill @a.dns.jp ドメイン名 NS
  - 例: drill @a.dns.jp iw2016-0036.jp NS
  - drill @dns1.sys.jpdirect.jp ドメイン名 A
  - 例: drill @dns1.sys.jpdirect.jp iw2016-0036.jp A
- dnsviz.netで確認

実習: DNSサービス使用解除

- 次の実習の都合上、設定を解除する

1. jd-login.jp にログイン、次へ
2. 「DNSサービス設定」をクリック
3. ドメイン名を選択して、「次へ」
4. 「設定解除」をクリック
5. 「この内容で確定する」をクリック

Public DNSサービスの確認

Public DNS サービス

- だれでも使用できるフルサービスリゾルバサービス
  - Google
    - https://developers.google.com/speed/public-dns/
    - 動作確認: drill @8.8.8.8 internetweek.jp A
  - OpenDNS
    - https://use.opendns.com/
    - 動作確認: drill @208.67.222.222 internetweek.jp A
  - Verisign
    - https://www.verisign.com/en_US/security-services/public-dns/index.xhtml
  - など
- 使い方
  - /etc/resolv.conf や、クライアントOSで設定するだけ
- Public DNSサービスを使用すると、フルサービスリゾルバの設定をする必要がありません
  - Unboundなど

DNSサーバの導入

使用するソフトウェア

- ISC BIND 9を使用しません
- NLnet Labs製ソフトウェア使用
  - www.nlnetlabs.nl
  - ldns　ライブラリとツール
    - Cで書かれたDNSライブラリ+drill+DNSSECツール
  - NSD　権威DNSサーバ
    - version 1.0が2002年にリリース
  - Unbound　フルサービスリゾルバ

VMへのssh login

- OpenSSH (ssh), Tera Team, Puttyなどで VM へログイン
  - ユーザ名　　admin
  - パスワード　配布の紙

ソフトウェアのインストール

- 必要なソフトウェアを導入
  - sudo yum install gcc make libevent-devel openssl-devel expat-devel
- ソースコードのダウンロード
  - www.nlnetlabs.nl Project → NSD/LDNS → Download
  - www.unbound.net/download.html → Current version
  - ダウンロードしたファイルをサーバにコピー
  - あるいはサーバで直接ダウンロードしてもよい
  - 導入時点で最新のものを使うこと
- インストールは基本的には標準手順
  - tar ball を展開、configure; make; make install
- 自分でinstallすると/usr/local/に入るが、パッケージは/usr (/usr/bin; /usr/sbinなど)に入ることに注意
- 今回はホームにコピー済 (~/src)

ソフトウェアのinstall: ldns

- (CentOSには少し古いパッケージがあるのでそれを使用してよい
  - yum install ldns)
- 最新のldnsを導入する
  - tar xvzf src/ldns-1.6.17.tar.gz
  - cd ldns-1.6.17
  - ./configure --with-drill --with-examples
  - make
  - sudo make install
  - cd ..
  - 確認: ls -l /usr/local/bin/drill /usr/local/bin/ldns-signzone
  - # drill, example (keygen, signzone)を作るという指定

ソフトウェアのinstall: NSD

- パッケージはないので、以下の手順で導入する
  - tar xvzf src/nsd-4.1.13.tar.gz
  - cd nsd-4.1.13
  - ./configure
  - make
  - sudo make install
  - cd ..

  - 確認: ls -l /usr/local/sbin/nsd /usr/local/sbin/nsd-control
  - 必要に応じてconfigure optionを確認すること

サーバアドレスの設計

- 今回は一台のサーバでNSDとUnboundを動かすため、慎重な設定が必要
- NSD
  - インターネットから検索できる必要があるのでグローバルアドレスが必要
    - 紙に指定してあるアドレスを使用
- Unbound
  - サービス自体はインターネットからアクセスされる必要がないため、loopback 127.0.0.1

フルサービスリゾルバ
Unbound

実習
権威サーバの設定

まずはDNSSECなし

NSD設定の設計

- 基本的には標準設定を使用: 最小限の設定
- DNSSEC署名は設定しない
- nsd-control を有効にする
  - Remote-control: <改行><tab>control-enalble: yes
- サーバアドレスはglobal addressのみ
- アクセス制限なし
  - 権威サーバにはアクセス制限不要
  - ゾーン転送はIPアドレスとTSIGキー指定で許可
- ゾーン一つ、ゾーン転送なし

NSDの設定 (1)

- “nsd” user作成
  - sudo groupadd nsd
  - sudo useradd -M -g nsd nsd
- nsd-controlのためのキーファイル生成
  - sudo /usr/local/sbin/nsd-control-setup

ゾーンファイル

- ドメイン名と同じファイル名のゾーンファイルを作成
  - sudo vi /etc/nsd/ドメイン名

```
$TTL 60
$ORIGIN 割り当てられたドメイン名.
@       IN SOA ns1 root (1 3600 900 120960 900)
        IN      NS      ns1
        IN      A       202.221.128.104
ns1     IN      A       サーバのIPアドレス
www     IN      A       202.221.128.104
```

- 今回は実習のため$TTL 60としているが実運用では3600や86400などの値を推奨する
- ドメイン名ラベルの最後の"."を省略すると $ORIGINで指定したドメイン名が追加される
- $ORIGINの最後の"."に注意

ゾーンファイルの入力例

- ゾーン名と同じファイル名のファイルを作成する
  - sudo vi /etc/nsd/iw2016-0036.jp

```
$TTL 60
$ORIGIN iw2016-0036.jp.
@       IN SOA ns1 root (1 3600 900 120960 900)
        IN      NS      ns1
        IN      A       202.221.128.104
ns1     IN      A       202.221.128.115
www     IN      A       202.221.128.104
```

- 今回は実習のため$TTL 60としているが実運用では3600や86400などの値を推奨する
- ドメイン名ラベルの最後の"."を省略すると $ORIGINで指定したドメイン名が追加される
- $ORIGINの最後の"."に注意

ゾーンファイルのチェック

- nsd-checkzoneでゾーンファイルのチェック
  - nsd-checkzone ゾーン名 ファイル名
  - 例: nsd-checkzone iw2016-0036.jp /etc/nsd/iw2016-0036.jp

nsdの設定: nsd.conf

- sudo vi /etc/nsd/nsd.conf

```
server:
        ip-address: 指定されたIPアドレス
        database: ""
        verbosity: 2

remote-control:
        control-enable: yes
        control-interface: 127.0.0.1

zone:
        name: "指定されたドメイン名"
        zonefile: "ドメイン名と同じファイル名"
        provide-xfr: 指定されたIPアドレス NOKEY
```

nsdの設定例: nsd.conf

- sudo vi /etc/nsd/nsd.conf

```
server:
        ip-address: 202.221.128.115
        database: ""
        verbosity: 2

remote-control:
        control-enable: yes
        control-interface: 127.0.0.1

zone:
        name: "iw2016-0036.jp"
        zonefile: "iw2016-0036.jp"
        provide-xfr: 202.221.128.115 NOKEY
```

nsd.confのチェック

- nsd-checkconfでnsd.confのチェック
  - nsd-checkconf ファイル名
  - 例: nsd-checkconf /etc/nsd/nsd.conf
  - 何も出なければよい

NSDの起動と確認

- NSD起動
  - sudo /usr/local/sbin/nsd-control start
- 動作確認
  - drill @指定されたIPアドレス 指定されたドメイン名 A
  - 例: drill @202.221.128.115 iw2016-0036.jp A
- ゾーン転送の確認
  - drill @指定されたIPアドレス 指定されたドメイン名 AXFR
  - 例: drill @202.221.128.115 iw2016-0036.jp AXFR
- ログの確認
  - sudo less /var/log/messages

表示例: drill @202.221.128.115 iw2016-0036.jp A

```
$ drill @202.221.128.115 iw2016-0036.jp a
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 37221
;; flags: qr aa rd ; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;; iw2016-0036.jp.      IN      A

;; ANSWER SECTION:
iw2016-0036.jp. 60      IN      A       202.221.128.104

;; AUTHORITY SECTION:
iw2016-0036.jp. 60      IN      NS      ns1.iw2016-0036.jp.

;; ADDITIONAL SECTION:
ns1.iw2016-0036.jp.     60      IN      A       202.221.128.115

;; Query time: 0 msec
;; SERVER: 202.221.128.115
;; WHEN: Tue Nov 22 14:59:35 2016
;; MSG SIZE  rcvd: 82
```

表示例: drill @202.221.128.115 iw2016-0036.jp axfr

```
$ drill @202.221.128.115 iw2016-0036.jp axfr
iw2016-0036.jp. 60      IN      SOA     ns1.iw2016-0036.jp.
root.iw2016-0036.jp.  1 3600 900 120960 900
iw2016-0036.jp. 60      IN      NS      ns1.iw2016-0036.jp.
iw2016-0036.jp. 60      IN      A       202.221.128.104
ns1.iw2016-0036.jp.     60      IN      A
202.221.128.115
www.iw2016-0036.jp.     60      IN      A
202.221.128.104
iw2016-0036.jp. 60      IN      SOA     ns1.iw2016-0036.jp.
root.iw2016-0036.jp.
 1 3600 900 120960 900
```

JPへのネームサーバ登録 (1)

- ドメイン名管理システム jd-login.jp にログイン、「次へ」
- 「ホスト情報登録申請」をクリック
- ゾーンファイルに指定したネームサーバのホスト名とIPアドレスを入力
  - 例:　　ホスト名=ns1.iw2016-0036.jp
    IPアドレス=202.221.128.115
- 「次へ」を押し、正しければ「この内容で確定する」を押す
  - 「申請に失敗しました。登録済みのドメイン名またはネームサーバホスト名です。」→ TAを呼ぶ
  - あるいは「ホスト情報削除申請」をクリックして、ホスト名を入力し、ホスト情報を削除

JPへのネームサーバ登録 (2)

- 「ネームサーバ設定・変更・解除申請」をクリック
- ドメイン名を選択して、「次へ」
- ゾーンファイルに指定したネームサーバホスト名を入力
  - 例: ホスト名=ns1.iw2016-0036.jp
- 「次へ」を押し、正しければ「この内容で確定する」を押す

JPへのネームサーバ登録の確認

- 一定時間後、確認する
  - drill @a.dns.jp 登録ドメイン名
  - 例: drill @a.dns.jp iw2016-0036.jp

ドメイン名使用の確認

- これで、インターネットから設定したドメイン名が使用できるようになったので確認する
- DNSチェックサービスでの確認
  - dnsviz.net
  - dnscheck.jp
- フルリゾルバでの確認
  - キャッシュクリア: sudo /usr/local/sbin/unbound flush_zone .
  - drill @127.0.0.1 ドメイン名 A
  - 例: drill @127.0.0.1 iw2016-0036.jp A

    ;; ANSWER SECTION:

    iw2016-0036.jp. 60 IN A 202.221.128.104
  - 例: drill @8.8.8.8 iw2016-0036.jp A

NSDの自動起動

- OSによって異なることと、rebootが必要なため実習を行なわない
- FreeBSD
  - ports, pkg経由でいれると、/etc/rc.conf に nsd_enable="YES" と書くことで自動起動
- Linux
  - パッケージ経由でいれれば自動起動できる
  - そうでなければ init.d や systemd の設定
- /etc/rc.local に書けば自動起動可能
  - /usr/local/sbin/nsd-control start &

DNSSEC概要

DNSSECとは

- DNSセキュリティ拡張(DNS Security Extensions)
- DNS利用者が受け取ったDNS応答の正統性を検証できる仕組み
  - 正統とは、DNSゾーン管理者が作成・公開したデータと同じであること
  - DNSゾーン管理者が自ゾーンに電子署名を追加
  - jpゾーンにはJPレジストリが電子署名を追加
  - example.jpゾーンにはexample.jp管理者が電子署名を追加
- 署名に使用した鍵情報を親ゾーンに登録
  - example.jp管理者はexample.jpの電子署名に使用した鍵の公開鍵情報をJPレジストリに登録
- DNS利用者は電子署名が追加されたDNS応答の正統性を検証
  - ルートからの信頼の連鎖をもとにルートから末端まで検証

公開鍵暗号

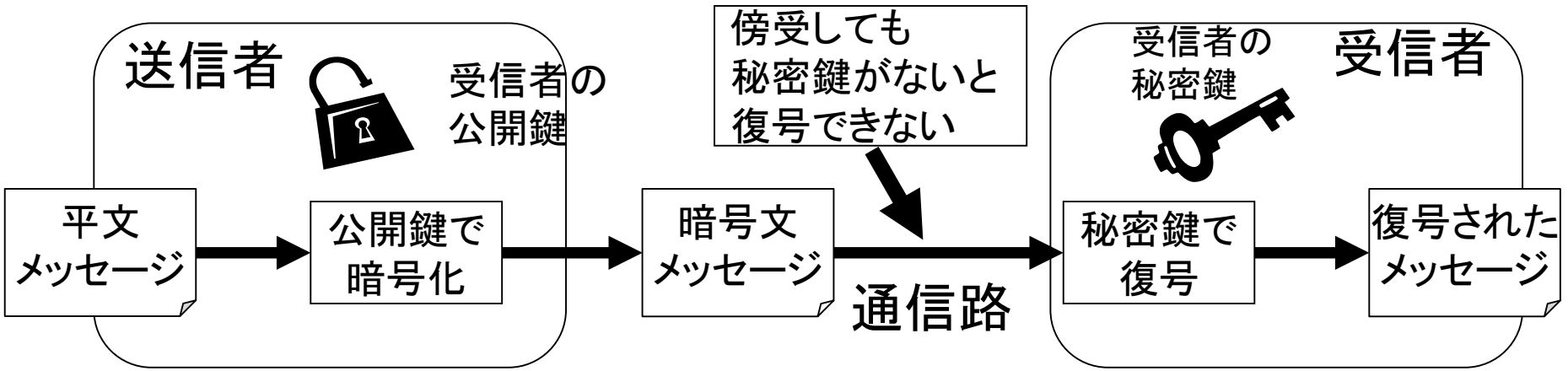
暗号化・復号に異なる鍵(秘密鍵と公開鍵)を用いる暗号方式

- 受信者の公開鍵で暗号化したものを、受信者の秘密鍵で復号(暗号通信)
- 送信者の秘密鍵で暗号化したものを、送信者の公開鍵で復号(電子署名)
- 代表的な公開鍵暗号方式: RSA暗号

秘密鍵

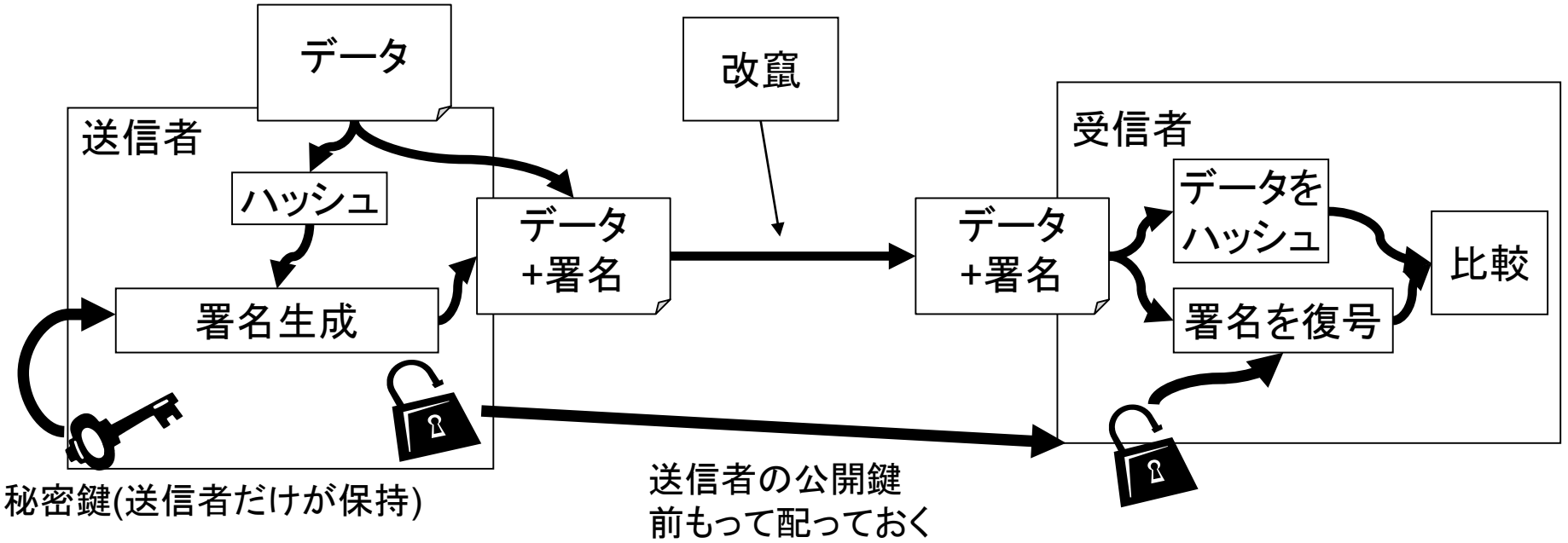
公開鍵
広く配布

- 暗号通信
  1. 受信者はあらかじめ公開鍵を広く公開
  2. 送信者は受信者の公開鍵で暗号化
  3. 受信者は本人の秘密鍵で復元
  - 秘密鍵は受信者のみが秘密に管理、秘密鍵を持つ受信者のみが復号可能
  - 秘密鍵を他人に伝える必要がない



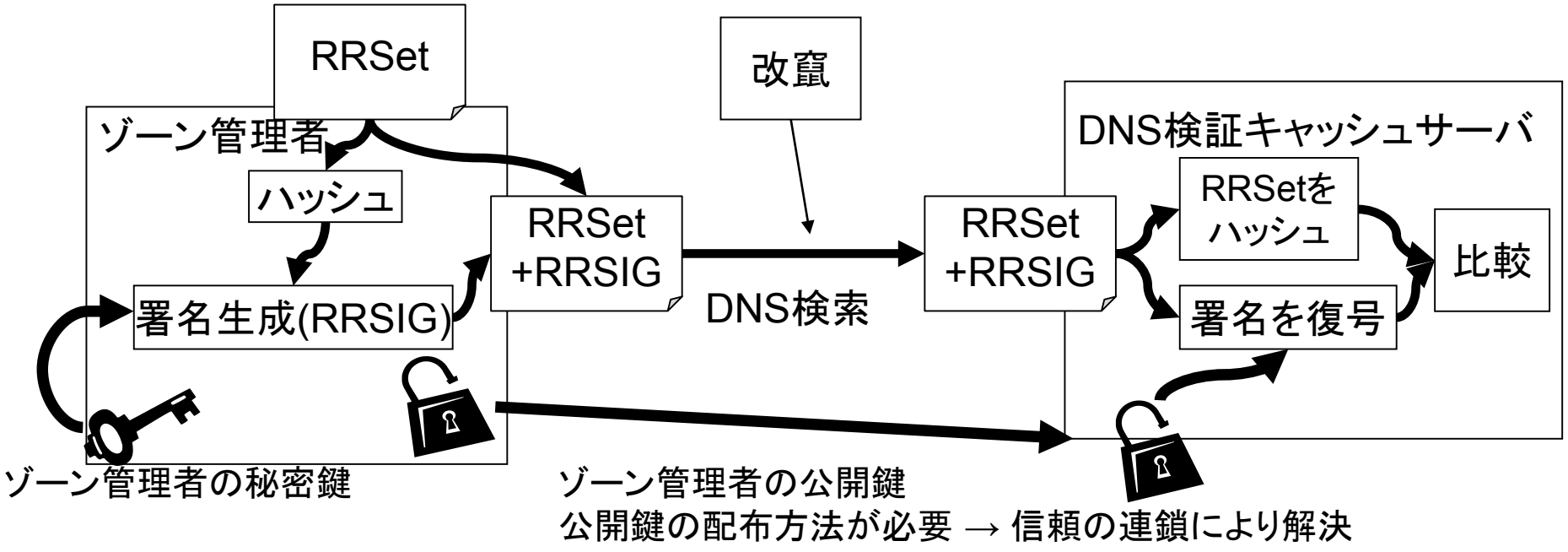
電子署名の概念

- 署名には、元データを圧縮した値(ハッシュ値)を用いる
- 送信者の秘密鍵でデータのハッシュ値を暗号化したものが署名
- 公開鍵で署名を復元するとハッシュ値が得られる
- 受信者は、データのハッシュ値と、復号したハッシュ値を比較、同じであれば、送信者が電子署名したデータであると判断できる
  - 送信者の秘密鍵は送信者しか持たないため



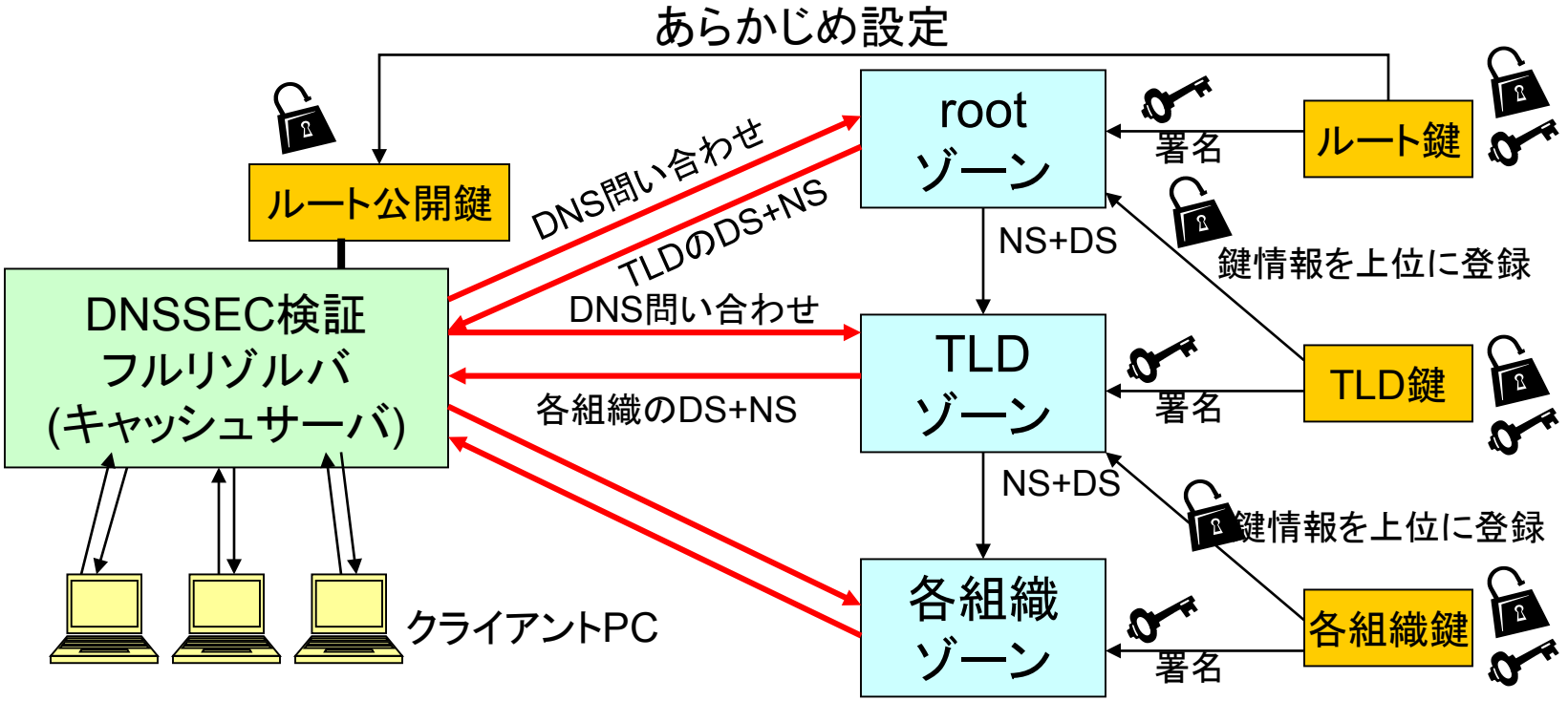
DNSへの応用 (DNSSEC)

- ゾーン管理者は、署名のための鍵対(秘密鍵、公開鍵)を作成する
- ゾーン内のリソースレコード(RRSet)を秘密鍵で署名する
  - www.example.jpのAや、AAAA
- DNSサーバはDNS応答に署名(RRSIG)を添付する
- ゾーンの公開鍵を知っていれば、RRSIG RRの署名を復号してゾーン情報と比較し、署名の検証が可能



信頼の連鎖

- 公開鍵の情報を上位レジストリに登録し、鍵による信頼の連鎖 を形成
  - 公開鍵のハッシュを鍵情報(DS)としてレジストリ(親ゾーン)に登録
  - レジストリは、NSとグルーに追加して鍵情報DSをルート/TLDゾーンに記述
- ルート公開鍵をフルリゾルバ(DNSキャッシュサーバ)に登録するだけで、各組織までのデータを検証可能



DNSSECで追加されたリソースレコード

- DNSKEY
  - 公開鍵を保持
  - DNSKEY フラグ プロトコル アルゴリズム 公開鍵
- RRSIG
  - 電子署名を保持
  - RRSIG Type Algorithm Labels OriginalTTL 署名有効期限 署名有効開始時刻 鍵タグ 署名者名 署名
  - 署名対象のリソースレコードと同じパケット内に入る
  - 対象とするタイプ (A, AAAA, NS, DS, MX, SOAなど)
  - 署名有効期間
  - 署名に使われた鍵の情報 (署名ドメイン名、鍵タグ)

DNSSECで追加されたリソースレコード(2)

- DS
  - DS 鍵タグ アルゴリズム DigestType DNSKEY のハッシュ

- 不存在証明のために用いられるRR
  - NSEC
  - NSEC3
  - NSEC3PARAM

DNSKEYの例

```
% drill -D @a.root-servers.net . dnskey
;; ANSWER SECTION:
.                   172800  IN      DNSKEY  256 3 8
AwEAAYbinauHA9oUb4aGNtJIrepyGoYy0OL01rvIhvo3RWN/Ch8p2C4Z
EkpvUYkx74r9JpgrOsjKOv+JQdKtT2u8AxGjUoH8x8HdpDiMV7XnpWJo
9wAxlFtDtbMnPwRQ3dWsT1p5myrGcm7EFJ9j7KmiAEG5hGsevZqcnqMO
W9QFkmp/zM0TFYXYWq6AsAof2uZqLUyd+nHIW0TGsaHMzcTNfA8Ww+
OY V7R4bcR/8edCEo6OAh9j48R1hRtuO1e2MQdnkITc9DJljB4Cq1gQKwv/
ku7mAvmFuWkRotMZIFN3vDhpmpmy7M0C1EHSRAgP+HkblLRQKOPnwI
/V ksJEU4fmnhk=
.                   172800  IN      DNSKEY  257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
QxA+Uk1ihz0=
```

DSの例

```
% drill -D @a.root-servers.net  jp DS
;; ANSWER SECTION:
jp.     86400   IN      DS      53899 8 1
00ded0bb8203cfb6abb054318ec95c4f13f4b5b0
jp.     86400   IN      DS      53899 8 2
c02ba0e5a47e49181ee132bb0612d950766ad9c62fd29bdeeafbc
463b9d37fde
jp.     86400   IN      RRSIG   DS 8 1 86400 20161120170000
20161107160000 39291 .
XjW9wErbdFwgJU3u9gqFeRxrHHR6jme49K42abv0AcmOI0KA
XO5YhP/BUD3JHG6FJ380wZa/dSDgI/uZIiIsZx5RAAq2+VMv9r5
am0evImi6SJAu4sVrJHgzr5FP0pkwUgFMzOObBpuIa/I91JkMbC
dIM7CgojJXjIQn6dP1OdIMsc0BhUDJqaT0JOvWyH3Qci23xtJw
DiaXqI7LoMf0pLPnWnVI8Wj5Qy+NMYEuQ9jzreYPCYrnqwuqX
gx2hvAhWp+TYSSvvt/FntAk3c8wkyGGdkQ7xO1f8BDI5Uh2Um/
5tCF8BFRaXqDrKrd1ob5lqZyL74P5FjecDN8MYDWMoQ==
```

- Signerはroot

MX+署名の例

```
% drill -D @ns0.amsl.com ietf.org mx
;; ANSWER SECTION:
ietf.org.       1800    IN      MX      0 mail.ietf.org.
ietf.org.       1800    IN      RRSIG   MX 5 2 1800
    20171102223706 20161102213718 40452 ietf.org.
    DE49Rq7bRFwnmy69gmNXOI1cNd5fcEAQKQftBOcWY
    8DaYnhqYfIy6UBH9L1zhStAvpPDRhPe9Yz8I+h/BmDxY
    nPOzMD/tM5ObnwMVPwpM0pN0/kqzTcsIB2QU7isHwP
    Uct7C2wt++nOPFWDEDBwhcJ9vNzNLfbqbG/iVdS4qi2k
    WZzqP4Ira8Qy3qq2kUQBguFd6p71Y2CNR8APuIIj845V
    GbwGeMVawUoM5BhrMd1LYPPHvwPC260cFwT5zK/E
    GeQDnpfuzPEj/qwFIV9pru3nr0WP9BJuCRIFS09Li0ajY
    APwKGbK48brSZST6+e6dFoT0fu7vh0XbCGodCDRPQ
    w==
```

DNSSECでの検証結果

- ルートからの検証が成功

- 信頼の連鎖が成立しない
  - DSが登録されていない → DNSSEC非対応
  - DSに対応する公開鍵がない → エラー

- 署名検証失敗 → エラー
  - 署名有効期間ではない
  - 署名と署名対象データが異なる

DNSSECが解決しないこと

- DNS応答の改竄・騙りは発見できるが、正しいDNS検索結果は別途得る必要がある
  - キャッシュポイズニングなどの攻撃で検証エラー
    - TCPで再検索？
  - そのままではアクセスできない
- DNS応答の正統性が保証されたとしても、その後の通信の安全を保証するわけではない
  - 通信路のハイジャック、盗聴はDNSでは防げない
  - TLS/SSLやIPsecなどと併用
- FAQ
  - DNSSECではDNS応答を暗号化するのか？
    - 暗号化しない

DNSSEC Status

- プロトコル
  - 2005年3月に標準化完了 RFC 4033~4035
  - 2008年3月にTLDで必要となるRFC 5155
- ソフトウェア: プロトコル標準化とともに実装
- Root: 2010年7月に対応
- TLD: ほとんどのTLDが登録者の鍵情報受付対応
  - org: 2009年6月, com, net: 2011年, jp: 2011年1月
- 各組織
  - .govはDNSSEC対応が必須
  - 日本国内の一部の組織: iij.ad.jp, jprs.co.jp, …
  - CloudFlareなどの事業者がDNSSECサービス提供
- 名前解決(DNSSEC検証)
  - Google Public DNS, Comcast (US CATV)など対応
- 2011年から使える状態

DNSSEC実習

ldns examples

- LDNSはCで書かれたDNSライブラリで、使用例のプログラムが同梱
- ldns-keygen : 署名鍵生成ツール
  - BIND 9のdnssec-keygenに対応
- ldns-signzone : 署名ツール
  - BIND 9のdnssec-signzoneより機能が低い
    - $INCLUDEなし
    - -N unixtime なし (SERIALをunixtimeにするオプション)
    - マルチスレッド非対応 (CPU増やしても性能伸びない)
- ldns-key2ds : DNSKEYからDSを作る
- drill

署名鍵生成

- KSK 2048 bit RSA, ZSK 2048 bit RSAで生成
  - ldns-keygen -k -a RSASHA256 -b 2048 -r /dev/urandom ドメイン名
  - ldns-keygen -a RSASHA256 -b 2048 -r /dev/urandom ドメイン名
  - -a RSASHA256: 暗号方式RSA, ハッシュSHA256の暗号アルゴリズム
  - -b 2048 … RSAビット長 2048
  - -k … KSKを作成する
  - -r /dev/urandom … よくないが速い乱数生成機使用
  - 例: ldns-keygen -k -a RSASHA256 -b 2048 -r /dev/urandom iw2016-0036.jp
  - 例: ldns-keygen -a RSASHA256 -b 2048 -r /dev/urandom iw2016-0036.jp

実習: 署名鍵生成

- KSK生成
  - cd /etc/nsd
  - sudo ldns-keygen -k -a RSASHA256 -b 2048 -r /dev/urandom ドメイン名
  - 例: ldns-keygen -k -a RSASHA256 -b 2048 -r /dev/urandom iw2016-0036.jp
- ZSK生成
  - sudo ldns-keygen -a RSASHA256 -b 2048 -r /dev/urandom ドメイン名
  - 例: ldns-keygen -a RSASHA256 -b 2048 -r /dev/urandom iw2016-0036.jp
- 生成したキーの情報が表示されるので記録する
  - KSK: Kiw2016-0036.jp.+008+42061
  - ZSK: Kiw2016-0036.jp.+008+59733

実習: 署名

- cd /etc/nsd
- sudo ldns-signzone ゾーンファイル ZSK名 KSK名
  - 例: ldns-signzone iw2016-0036.jp ￥
    Kiw2016-0036.jp.+008+59733 ￥
    Kiw2016-0036.jp.+008+42061
- 署名結果
  - 確認: ls -l iw2016-0036.jp.signed
  - 確認: less iw2016-0036.jp.signed

署名結果の有効化

- NSDへの読み込み
  - /etc/nsd/nsd.conf を編集し、ゾーンファイル名をゾーン名.signedに変更
    - 例: sudo vi /etc/nsd/nsd.conf

    zonefile: “iw2016-0036.jp.signed”
  - sudo /usr/local/sbin/nsd-control reconfig
  - sudo /usr/local/sbin/nsd-control reload
  - これで署名済みゾーンファイルが有効になる

ゾーン情報の確認

- DNSKEY
  - drill -D @サーバIPアドレス ドメイン名 DNSKEY
  - 例: drill -D @202.221.128.115 iw2016-0036.jp DNSKEY
  - ドメイン名 DNSKEYとRRSIGが表示される
- A
  - drill -D @サーバIPアドレス ドメイン名 DNSKEY
  - 例: drill -D @202.221.128.115 www.iw2016-0036.jp A
  - ドメイン名 AとRRSIGが表示される

JPへのDS登録

- KSKのDSをJPに登録する必要がある
- cat {KSK}.ds して確認する
  - 例: cat Kiw2016-0036.jp.+008+42061.ds

    iw2016-0036.jp. IN DS 42061 8 2
    55635a068aecedee2271470b0de005b0534d0ad3540e49e2
    afa7b92772c22676
- ドメイン名管理システム jd-login.jp にログイン
- 「ネームサーバ設定・変更・解除申請」をクリック
- ドメイン名を選んで「次へ」
- 申請内容入力画面で、「署名鍵入力」をクリック
- DSの後を入力して、「次へ」
  - 例: “42061 8 2
    55635a068aecedee2271470b0de005b0534d0ad3540e49e
    2afa7b92772c22676”を入力
- 設定内容を確認して、「この内容で確定する」を押す
- 「設定検証」してもよい

JPへのネームサーバ登録の確認

- 一定時間後、確認する
  - drill -D @a.dns.jp 登録ドメイン名
  - dig +dnssec @a.dns.jp登録ドメイン名
  - 例: drill -D @a.dns.jp iw2016-0036.jp

DNSSEC確認

- これで、インターネットから設定したドメイン名がDNSSEC検証できるようになったので確認する
- DNSチェックサイトでの確認
  - dnsviz.net
  - dnscheck.jp
- フルリゾルバでの確認
  - drill -D @127.0.0.1 ドメイン名 A
  - dig +dnssec @127.0.0.1 ドメイン名 A
  - 例: drill -D @127.0.0.1 iw2016-0036.jp A
  - 例: drill -D @8.8.8.8 iw2016-0036.jp A
    - Flagsに ad があればよい

ldnsを直接使う問題点

- 現在使用しているキーの名前を覚えていないといけない
- DNSSECでは定期的に署名しないといけない
- 署名のたびにゾーンファイルのシリアルを増やさないといけない
- 鍵更新の場合は自分でキーの名前を管理する必要がある

- 最大の問題点は面倒であること
  - すなわち、ミスの原因になる

DNSSECサポートツール

- Infoblox
  - BIND 9ベースのアプライアンス、DNSSEC対応
- Secure64
  - DNSSECの鍵管理、署名のアプライアンス
- BIND 9 (DNSSEC for humans)
  - ldnsと比べて鍵管理などが便利になっている
  - 今回のハンズオンの目的からはずれる
- OpenDNSSEC
  - DNSSECの鍵管理、署名に特化したソフトウェア
  - すこし大規模
- 小規模なものがほしい → 2009年にはなかった

dnsseczonetool

- 鍵管理するツールを試作
  - 作者: 藤原
  - 作成時期: 2009～2010
  - 公開場所: http://member.wide.ad.jp/~fujiwara/
- 作成の動機
  - dnssec-keygen, dnssec-signzoneはよいツールだが、鍵を覚えておくのが面倒
  - 再署名も面倒
  - BIND 9のDNSSEC for Humansはやりすぎ
    - DNSSECの鍵には有効期間がないのに、独自に追加
    - 個人ドメイン名では鍵更新不要、定期再署名で十分
  - 鍵番号などを適度に管理してくれ、signとかrolloverとするだけで動くようなwrapper scriptがほしい
  - NLnet LabsのIdnsでも使いたい
  - なにをやっているかわかる簡単なものがほしい (shell)

dnsseczonetoolのコマンド

- 鍵セット生成
  - dnsseczonetool keygen ドメイン名
- 署名
  - dnsseczonetool sign ドメイン名
- DS表示
  - dnsseczonetool status ドメイン名
- ZSK更新
  - dnsseczonetool add-next-zsk ドメイン名
  - dnsseczonetool zsk-rollover ドメイン名
- KSK更新
  - dnsseczonetool add-next-ksk ドメイン名
  - dnsseczonetool ksk-rollover ドメイン名

定期的な再署名

- DNSSECでは署名に有効期間がある
  - 標準では30日
  - 鍵を変更しなくても定期的に再署名する必要あり
  - 再署名するとシリアル番号を増やす必要あり
  - シリアル番号として時刻を使うとよい (unixtime)
  - ゾーンファイルのシリアル値を _SERIAL_ にする
    - BIND 9のdnssec-signzoneにはシリアル番号変更機能があるが、ldns-signzoneにはないため
- cronによる自動再署名設定
  - crontabに、dnsseczonetool sign ドメイン名

実習の準備

- ドメイン名管理システム jd-login.jp でDSの削除
  - ネームサーバ設定変更解除申請
  - ドメイン名を選択
  - 署名鍵フィールドを空にして、設定

- 古い鍵ファイルの削除
  - sudo rm /etc/nsd/Kiw2016-*

- キャッシュのクリア
  - sudo /usr/local/sbin/unbound-control flush_zone "."

実習: dnsseczonetool

- dnsseczonetoolを /etc/nsd にコピー
  - http://github.com/kfujiwara/dnsseczonetool
  - cd /etc/nsd
  - sudo cp ~/src/dnsseczonetool .
  - sudo chmod +x dnsseczonetool
- /etc/nsd/dnsseczonetool.confを作成 (次スライド)
- ゾーンファイルを、ゾーン名に一致させること (済)
  - 例: /etc/nsd/iw2016-0036.jp
- nsd.confに指定するゾーンファイル名は、ゾーン名.signedとする(済)
  - 例: zonefile: “iw2016-0036.jp.signed”

/etc/nsd/dnsseczonetool.conf

BIND 9のツール用に作っていたため、NSD/ldnsで使用するための変更点を記述

% sudo vi /etc/nsd/dnsseczonetool.conf

```
MASTERDIR="/etc/nsd"
keygen="/usr/local/bin/ldns-keygen"
signzone="/usr/local/bin/ldns-signzone"
dsfromkey="/usr/local/bin/ldns-key2ds -n"
RNDC_OPTION="OFF"
UNIXTIME=`date +%s`
ZONE_PREPROCESS="sed s/_SERIAL_/$UNIXTIME/"
RELOADALL_COMMAND="/usr/local/sbin/nsd-control reload"
ZSK_PARAM="-a RSASHA256 -b 2048 -r /dev/urandom"
KSK_PARAM="-a RSASHA256 -b 2048 -k -r /dev/urandom"
SIGN_PARAM=""
```

実習:ゾーンファイルの変更

- ゾーン名と同じファイル名のファイルを作成する
  - sudo vi /etc/nsd/ゾーン名

```
$TTL 3600
$ORIGIN 割り当てられたドメイン名.
@     IN SOA ns1 root (_SERIAL_ 3600 900
120960 900)
      IN    NS    ns1
      IN    A     202.221.128.104
ns1   IN    A     サーバのIPアドレス
www IN    A     202.221.128.104
```

実習:鍵生成と署名

- sudo /etc/nsd/dnsseczonetool keygen ドメイン名
  - 例: /etc/nsd/dnsseczonetool keygen iw2016-0036.jp
- sudo /etc/nsd/dnsseczonetool sign ドメイン名
  - 例: /etc/nsd/dnsseczonetool sign iw2016-0036.jp
  - 自動的にreload実施

ゾーン情報の確認

- DNSKEY
  - drill -D @サーバIPアドレス ドメイン名 DNSKEY
  - 例: drill -D @202.221.128.115 iw2016-0036.jp DNSKEY
  - ドメイン名 DNSKEYとRRSIGが表示される
- A
  - drill -D @サーバIPアドレス ドメイン名 DNSKEY
  - 例: drill -D @202.221.128.115 www.iw2016-0036.jp A
  - ドメイン名 AとRRSIGが表示される

ゾーン情報の確認

- SOAを見てシリアルが違うことを確認
  - drill -D @サーバIPアドレス ドメイン名 SOA
  - 例: drill -D @202.221.128.115 iw2016-0036.jp SOA

iw2016-0036.jp. 60 IN SOA ns1.iw2016-0036.jp. root.iw2016-0036.jp. 1479799303 3600 900 120960 900

iw2016-0036.jp. 60 IN RRSIG SOA 8 2 60 20161220072143 20161122072143

34440 iw2016-0036.jp. 署名

JPへのDS登録

- KSKのDSをJPに登録する必要がある
  - sudo /etc/nsd/dnsseczonetool status ドメイン名
  - 例: /etc/nsd/dnsseczonetool status iw2016-0036.jp
  - DSが表示される
- ドメイン名管理システム jd-login.jp にログイン、次へ
- 「ネームサーバ設定・変更・解除申請」をクリック
- ドメイン名を選んで「次へ」
- 申請内容入力画面で、「署名鍵入力」をクリック
- DSの後を入力して、「次へ」
  - 例: “42061 8 2 55635a068aecedee2271470b0de005b0534d0ad3540e49e2afa7b92772c22676”を入力
- 設定内容を確認して、「この内容で確定する」を押す
- 「設定検証」してもよい

JPへのネームサーバ登録の確認

- 一定時間後、確認する
  - drill -D @a.dns.jp 登録ドメイン名
  - 例: drill -D @a.dns.jp iw2016-0036.jp

DNSSEC確認

- これで、インターネットから設定したドメイン名が使用できるようになったので確認する
  - ただし、反映に15分程度はかかる
- DNSvizでの確認
  - http://dnsviz.net/　　ドメイン名を入力
- フルリゾルバでの確認
  - drill -D @127.0.0.1 ドメイン名 A
  - 例: drill -D @127.0.0.1 iw2016-0036.jp A
  - 例: drill -D @8.8.8.8 iw2016-0036.jp A
    - Flagsに ad があればよい

再署名するとシリアル値を変更

- 再署名
  - sudo /etc/nsd/dnsseczonetool keygen ドメイン名
  - 例: sudo /etc/nsd/dnsseczonetool sign iw2016-0036.jp
- SOA RRを見てシリアルが違うことを確認
  - drill -D @サーバIPアドレス ドメイン名 SOA
  - 例: drill -D @202.221.128.115 iw2016-0036.jp SOA

  iw2016-0036.jp. 60 IN SOA ns1.iw2016-0036.jp. root.iw2016-0036.jp. 1479799303 3600 900 120960 900

  ↓

  iw2016-0036.jp. 60 IN SOA ns1.iw2016-0036.jp. root.iw2016-0036.jp. 1479805803 3600 900 120960 900
- ゾーン転送可能

自動再署名

- crontabに、署名コマンドを記述
  - crontab も OSによって異なる可能性あり
- sudo vi /etc/crontab

分 時 日 月 曜 root /etc/nsd/dnsseczonetool sign ドメイン名

例:

5 6 * * 0 root /etc/nsd/dnsseczonetool iw2016-0036.jp

(毎週日曜日の6時5分にiw2016-0036.jpの再署名を行なう)

DNSSECの運用

- 定期的に鍵更新を行うこと
  - ただし、まだ2048bit RSAは破られていないので5年ほど放置でも問題はない
    - Rootも5年間同じKSKを使ってきた
    - 来年更新予定

dnsseczonetoolの注意点

- シリアル番号の生成にsedを使っているため、ゾーンファイルの他の部分に _SERIAL_ と書かないこと
  - あるいは、dnsseczonetool.confのZONE_PREPROCESSを変更すること
  - ZONE_PREPROCESS="sed s/_SERIAL_/$UNIXTIME/"
- 無保証です
  - 個人的に作り、公開したものです
  - 問題があればメールやgithub経由で連絡をください
  - できる範囲で対応します
  - https://github.com/kfujiwara/dnsseczonetool

ゾーン転送

- 今回は実習時間・環境の制約でゾーンあたりのネームサーバ数を1とした
- 通常は複数のネームサーバを用意して冗長化・分散を行なう
  - NS設定とグルーの設定
  - ゾーンファイルを管理する(hidden)master
  - ゾーンファイルを受け取って提供するslave
  - NSD, BIND 9, Knot DNSなどを組み合わせるとよい

NSDでのゾーン転送設定

- ゾーンごとに nsd.confの "zone:" 節に記述
- 転送設定、転送要求、notifyをIPアドレスごとにTSIGキーと組み合わせて記述
  - provide-xfr: ゾーン転送の許可 (master)
  - request-xfr: ゾーン転送の要求 (slave)
  - notify: notify送信 (master)
  - allow-notify: notifyの受信 (slave)
- TSIGを使用していない場合はNOKEYと書く
- 設定後 nsd-control reconfig

ゾーン転送: master

- nsd.conf のゾーン設定に provide-xfrとnotifyをIPアドレスごとに記述

```
zone:
        name:           "ドメイン名"
        zonefile:       "ゾーンファイル名"
        provide-xfr:    IPアドレス TSIG_key-name
        notify:         IPアドレス TSIG_key-name
```

  - 例

```
zone:
        name:           "iw2016-0036.jp"
        zonefile:       "iw2016-0036.jp.signed"
        provide-xfr:    2001:db8:1111:2222::1 NOKEY
        notify:         2001:db8:1111:2222::1 NOKEY
        provide-xfr:    203.0.113.5 NOKEY
        notify:         203.0.113.5 NOKEY
```

ゾーン転送: slave

- nsd.conf のゾーン設定に request-xfrと allow-notifyをIPアドレスごとに記述

```
zone:
        name:           "ドメイン名"
        zonefile:       "ゾーンファイル名"
        request-xfr:    IPアドレス TSIG_key-name
        allow-notify:   IPアドレス TSIG_key-name
```

– 例

```
zone:
        name:           "iw2016-0036.jp"
        zonefile:       "slave/iw2016-0036.jp"
        provide-xfr:    2001:db8:3333:4444::1 NOKEY
        notify:         2001:db8:3333:4444::1 NOKEY
        provide-xfr:    203.0.113.5 NOKEY
        notify:         203.0.113.5 NOKEY
```

NSDがゾーンファイルを書くため、/etc/nsd/slave/ を作成し、ownerをnsdとしておくとよい

ネームサーバ情報の追加

- ゾーンファイルへの追加
  - ネームサーバ名を決め、NS行とアドレスを追加

    例:　iw2016-0036.jp. IN NS ns2.iw2016-0036.jp.

    ns2.iw2016-0036.jp. IN A 203.0.113.5
  - reloadする、あるいは再署名してreloadする
- JPへのネームサーバ追加
  - ホスト情報の追加
    - 例: ホスト名=ns2.iw2016-0036.jp アドレス＝203.0.113.5
  - ネームサーバ情報の追加
    - 例: ホスト名=ns2.iw2016-0036.jp

リゾルバの動作

(予備)
時間が余ったら実施する

名前解決実習

- 名前解決を行うリゾルバになりきってルートから名前ツリーをたどる
  - コマンド: drillまたはdig
  - drill @ルートサーバ　解決したい名前　タイプ
- 課題
  - 自分で設定したドメイン名 iw2016-00xx.jp A
  - www.nic.ad.jp A
  - internetweek.jp A
  - www.google.co.jp A
  - www.asahi.com A
  - 逆引き　44.129.178.203.in-addr.arpa PTR

名前解決例 www.asahi.com (1)

- drill @198.41.0.4 www.asahi.com A
  - com. IN NS a.gtld-servers.net.
  - com. IN NS b.gtld-servers.net.
  - 略
  - a.gtld-servers.net. IN A 192.5.6.30
  - b.gtld-servers.net. IN A 192.33.14.30
  - 略
  - comの情報は、[a-m].gtld-servers.netが知っていて、それらのIPv4, IPv6アドレスが添付
- 次はそれらのアドレスに聞く

名前解決例 www.asahi.com (2)

- drill @192.5.6.30 www.asahi.com A
  - asahi.com. IN NS dns-a.iij.ad.jp.
  - asahi.com. IN NS dns01.asahi-np.co.jp.
  - asahi.com. IN NS dns02.asahi-np.co.jp.
  - asahi.comの情報は、dns-a.iij.ad.jp, dns01.asahi-np.co.jp, dns02.asahi-np.co.jpが知っている
  - com DNSサーバはそれらのアドレスを知らない
    - なぜなら、それらはasahi.com以下の名前ではない
- 次はそれらのアドレスを調べないといけない
  - dns-a.iij.ad.jp, dns01.asahi-np.co.jp, dns02.asahi-np.co.jpのA, AAAA
  - ルートから調べること

名前解決例 www.asahi.com (3)

- dns01.asahi-np.co.jpのアドレスを調べたとする (3ステップ省略)
- drill @133.173.150.100 www.asahi.com A
  - www.asahi.com. IN CNAME www.asahi.com.edgesuite.net.
  - www.asahi.comは、www.asahi.com.edgesuite.netの別名である
  - 次はwww.asahi.com.edgesuite.net Aを検索
  - ルートから調べること

関連資料

- オランダ製ソフトウェアによるDNSSEC遊び, 21 July 2010, DNSOPS.JP BoF, Shinagawa, JP.
  - http://dnsops.jp/bof/20100721/dnsops-20100721.pdf
  - https://github.com/kfujiwara/dnsseczonetool
- 開発元: www.nlnetlabs.nl
- DNSプロトコル
  - RFC 1034, 1035, 2181, 2308, 4033, 4034, 4035, 5011, 5155 などと、それらをUpdateしているもの