児童ポルノブロッキングとDNS

平成22年11月25日

安心ネットづくり促進協議会
ISP技術者SWG
北村　和広

Agenda

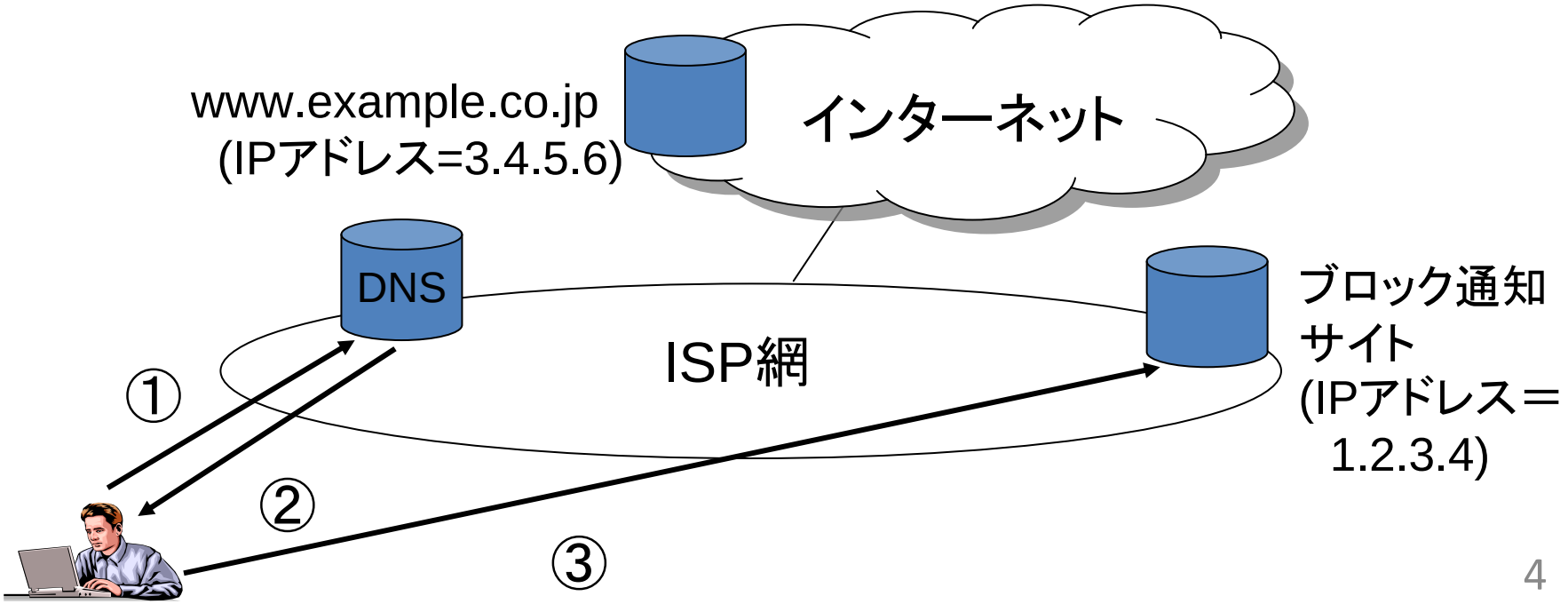
- 児童ポルノブロッキング導入検討の背景
- 児童ポルノブロッキングの手法について
- DNSSEC導入時の影響
- ブロッキング実施に向けての課題

ブロッキング導入検討の背景

- **ブロッキング＝「通信の秘密」を侵害**
  - 迷惑メール対策(OP25B)
  - P2Pに対する帯域制御
- 2010/5/18 総務省ICT諸問題研究会
  2010/7/27 犯罪対策閣僚会議　児童ポルノ排除総合対策
  - 2010年度中にブロッキング実施に向けた環境を整備
- **ブロッキングの対象範囲**
  - 基本は該当ファイルの削除
  - 「児童ポルノ掲載アドレスリスト作成管理団体運用ガイドライン」
    ① サイト管理者等へ削除要請を行ったが削除されなかったもの
    ② 海外サーバに蔵置されているもの
    ③ サイト管理者等への削除要請が困難であるもの
    ④ ….迅速かつ重層的な流出防止対策が必要で、事前に専門委員会の承認を得たもの

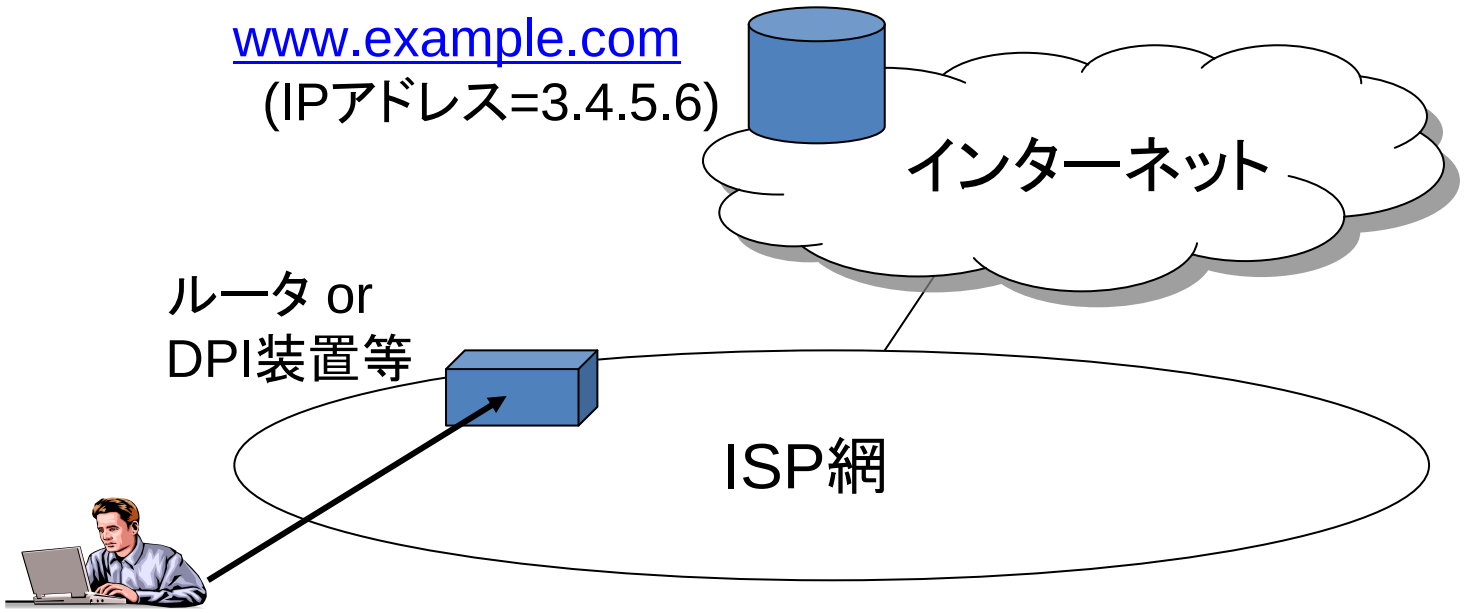
DNSポイズニング方式

- DNSに対する問合せに対して、別のサイトのIPアドレスを回答し、別なサイトへ誘導
- DNSを利用する通信にのみ有効（IPアドレス直打ちで回避可）
- ホスト名/ドメイン単位であるためオーバブロッキングが発生
- イタリア、ノルウェー、スウェーデン、フィンランド等で導入事例



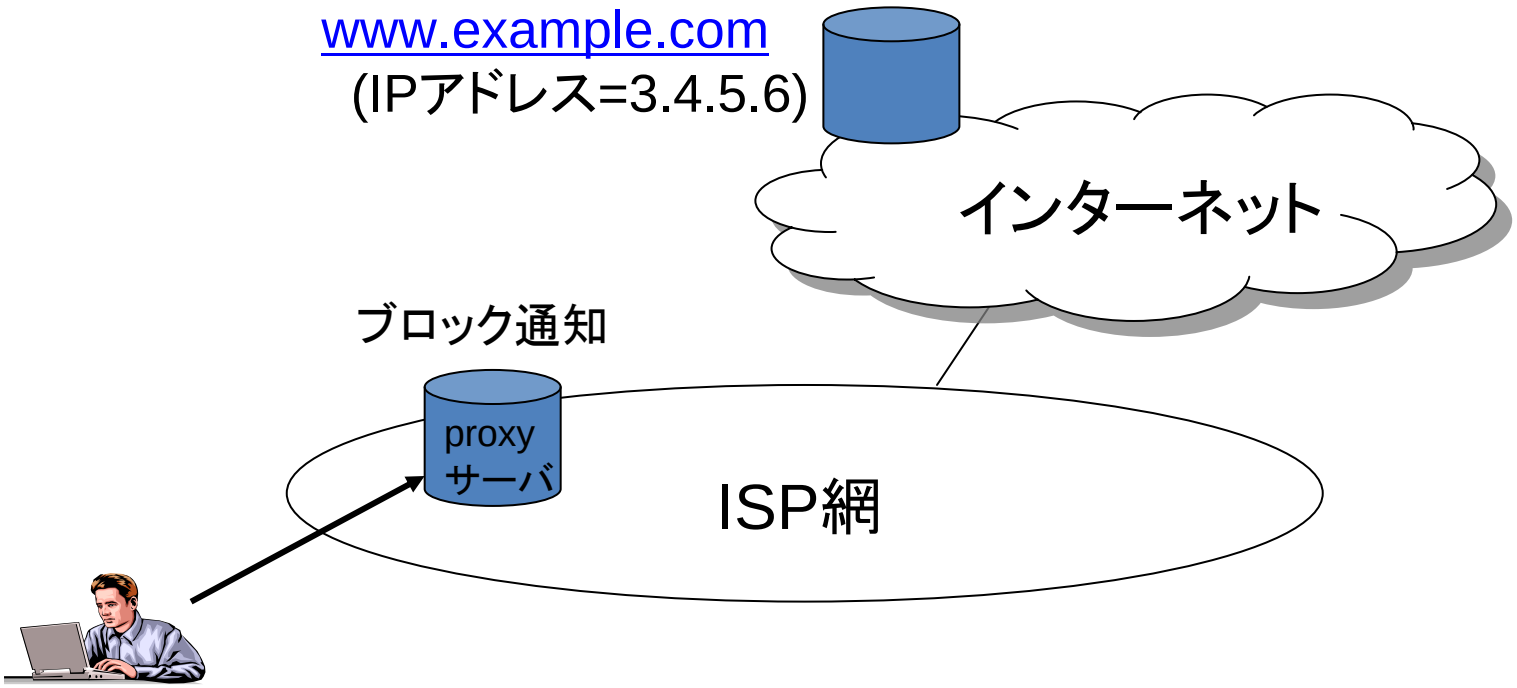
パケットフィルタリング方式

- 通信経路上の装置により、IPアドレスあるいはURL単位で該当サイト向け通信を遮断
- 複数サイトが同一IPアドレス上にある場合はオーバブロッキングが発生
- アクセスリストの運用管理が煩雑



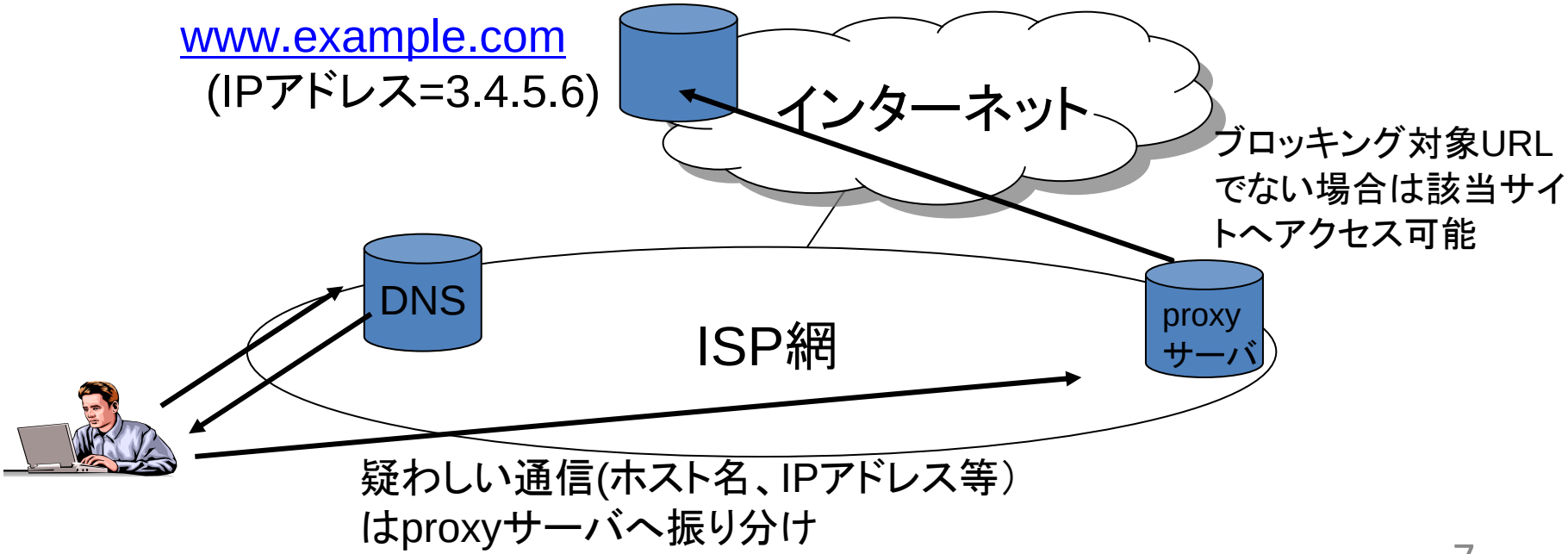
プロキシ方式

- Proxyサーバにてアクセス先URL情報を対象リストと突合
- URL単位でのブロッキング
- Proxy経由の正常通信の速度劣化の懸念



ハイブリッドフィルタリング方式

- 疑わしい通信のみをURL単位でブロック可能なproxy等を経由
- 経路制御やDNSを利用することで疑わしい通信を抽出
- BT(CleanFeed)で実績あり



ISPへのアンケート結果

- ブロッキングの4方式について、設備投資の必要性、コスト、採用可能な方式、導入可能時期等をアンケート実施

- DNSポイズニング方式が採用可能な方式として最多(約50%)

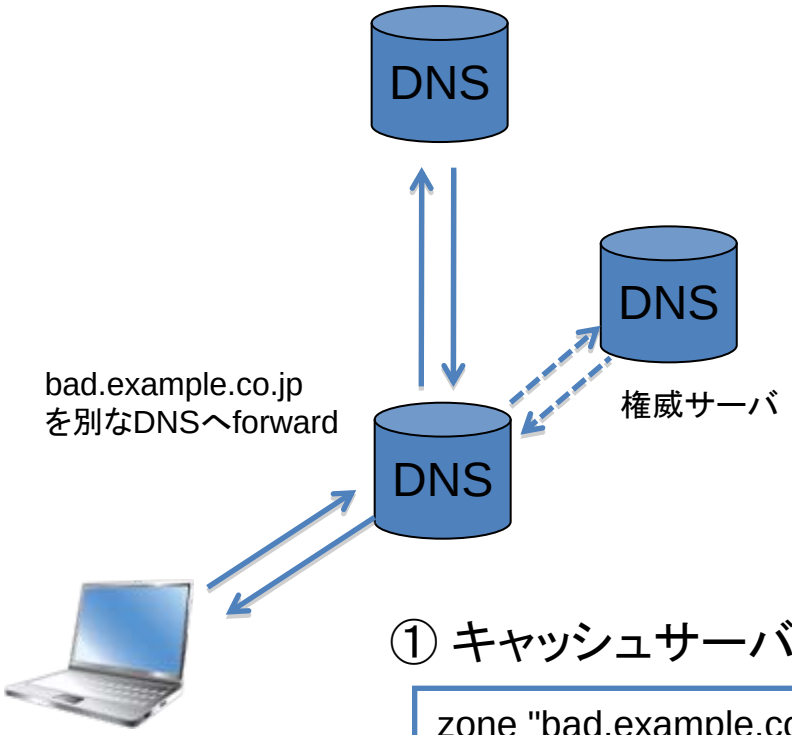
  理由は、現状設備のままで提供可能等コストが最も抑えられる方式であるからと考えられる

具体的なDNSの設定例 (BINDの場合）

BIND9.7.0-P1

② forward先のDNS named.conf

```
zone "bad.example.co.jp" in {
        type master;
        file "bad.example.co.jp.db";
};
```




```
$TTL 0
bad.example.co.jp.   0    IN SOA  root.bad.example.co.jp. admin.bad.example.co.jp. (
                          2010101527   ; serial
                          7200      ; refresh (2 hours)
                          3600      ; retry (1 hour)
                          604800    ; expire (1 week)
                          600       ; minimum (10 minutes)
                          )
      0           NS     ns.bad.example.co.jp.

ns    0     IN    A     192.168.11.134
bad.example.co.jp.    0     IN    A     1.1.1.1
```

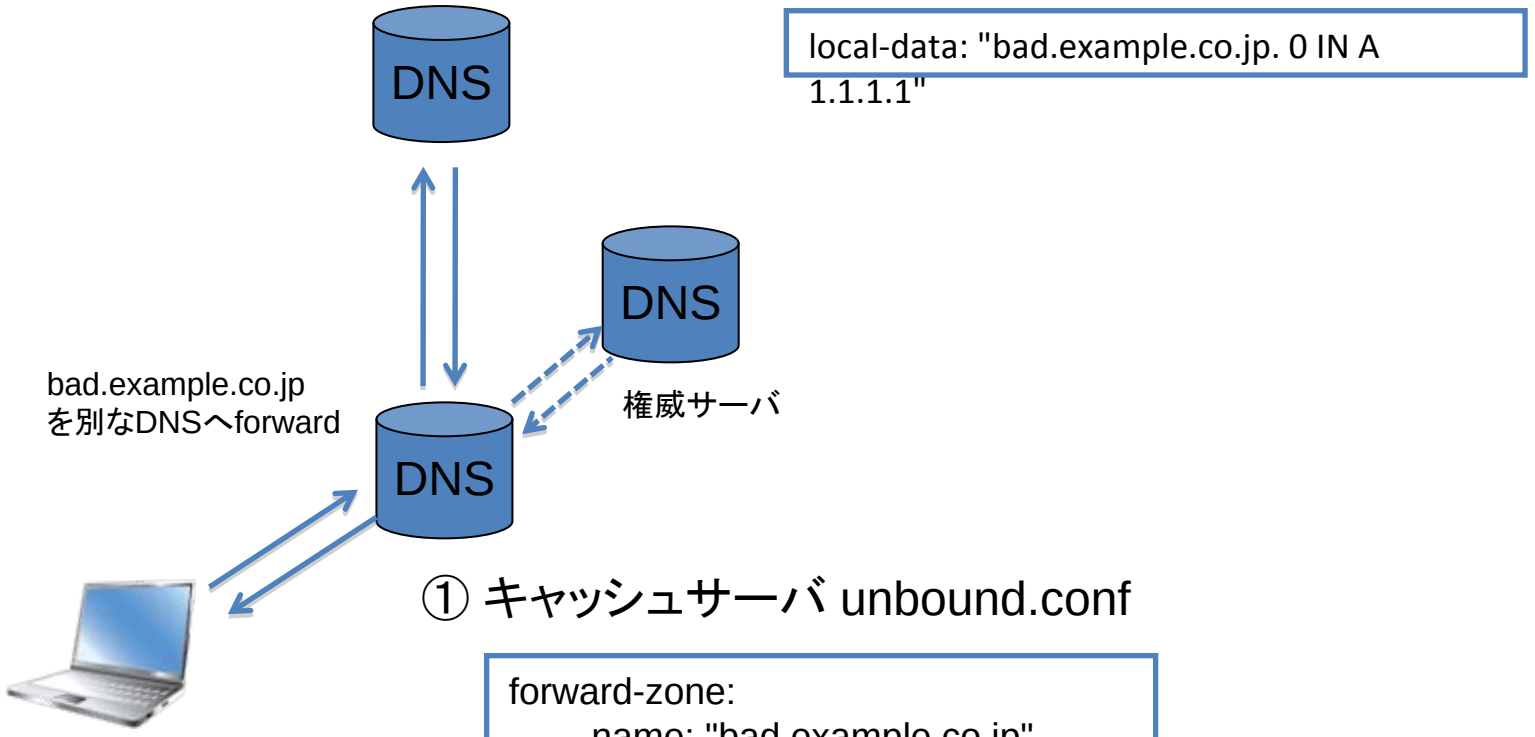
① キャッシュサーバ named.conf

```
zone "bad.example.co.jp." {
        type forward;
        forward only;
        forwarders { 192.168.11.134; };
};
```

具体的なDNSの設定例 (unboundの場合）

unbound 1.4.1

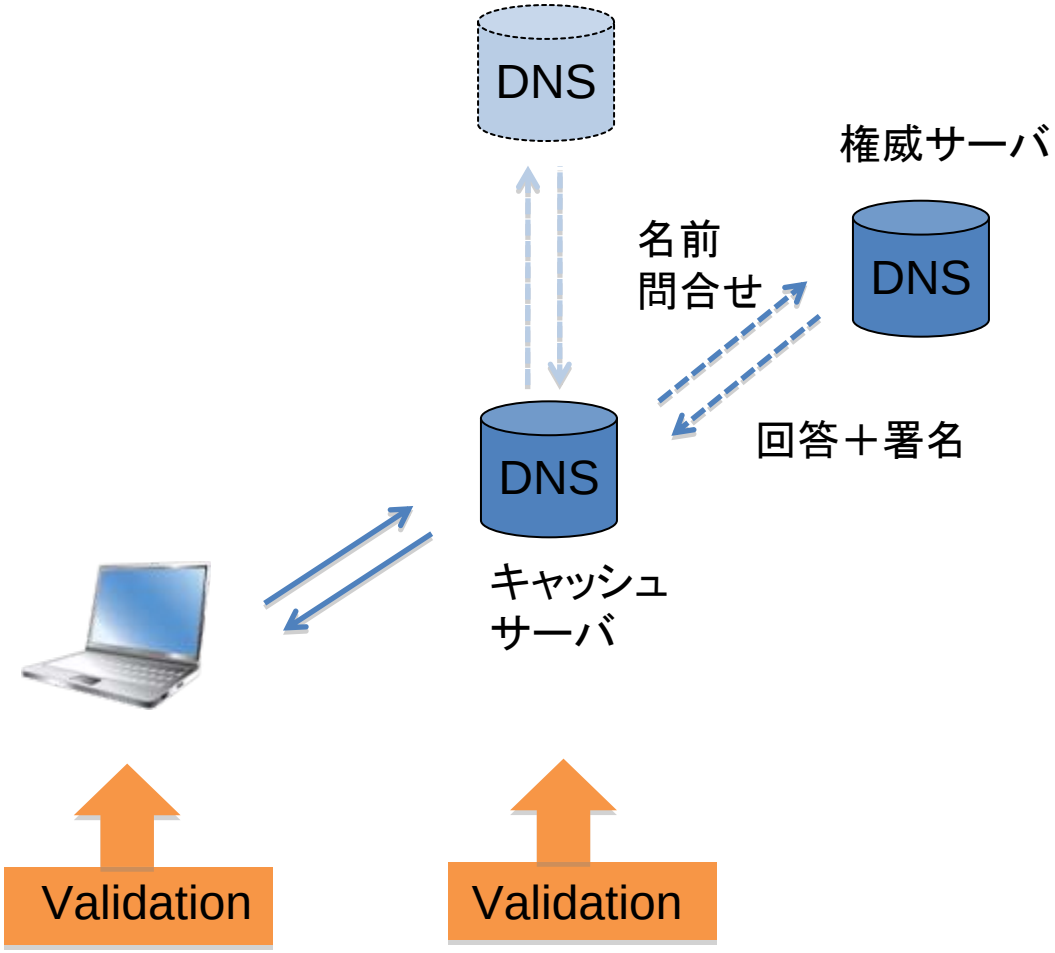
② forward先のDNS unbound.conf



① キャッシュサーバ unbound.conf

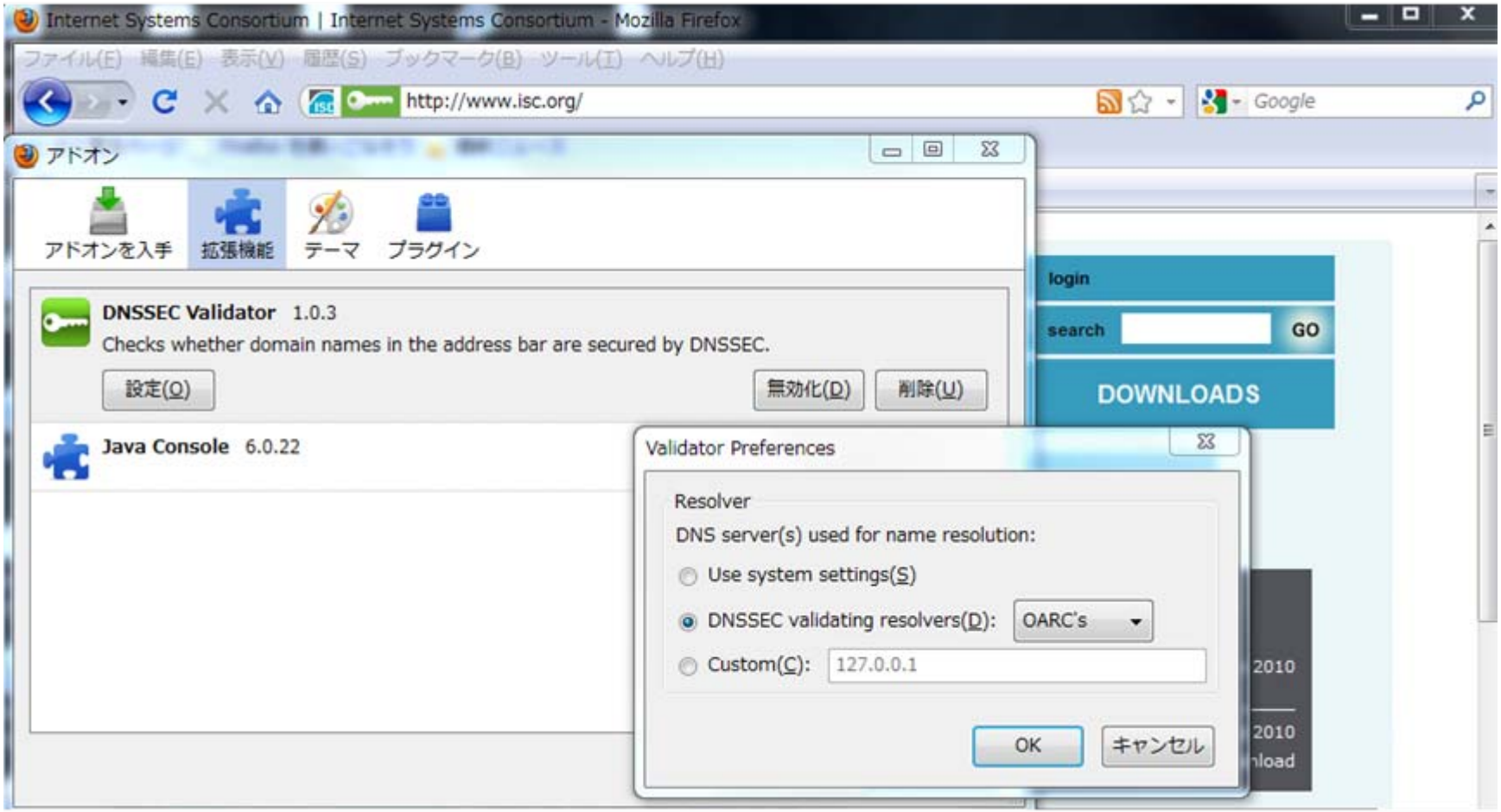
```
forward-zone:
        name: "bad.example.co.jp"
        forward-addr: 192.168.11.134
```

DNSSECの概要


DNS
権威サーバ
名前
問合せ
DNS
回答＋署名
DNS
キャッシュ
サーバ
Validation
Validation

リゾルバでのDNSSEC検証

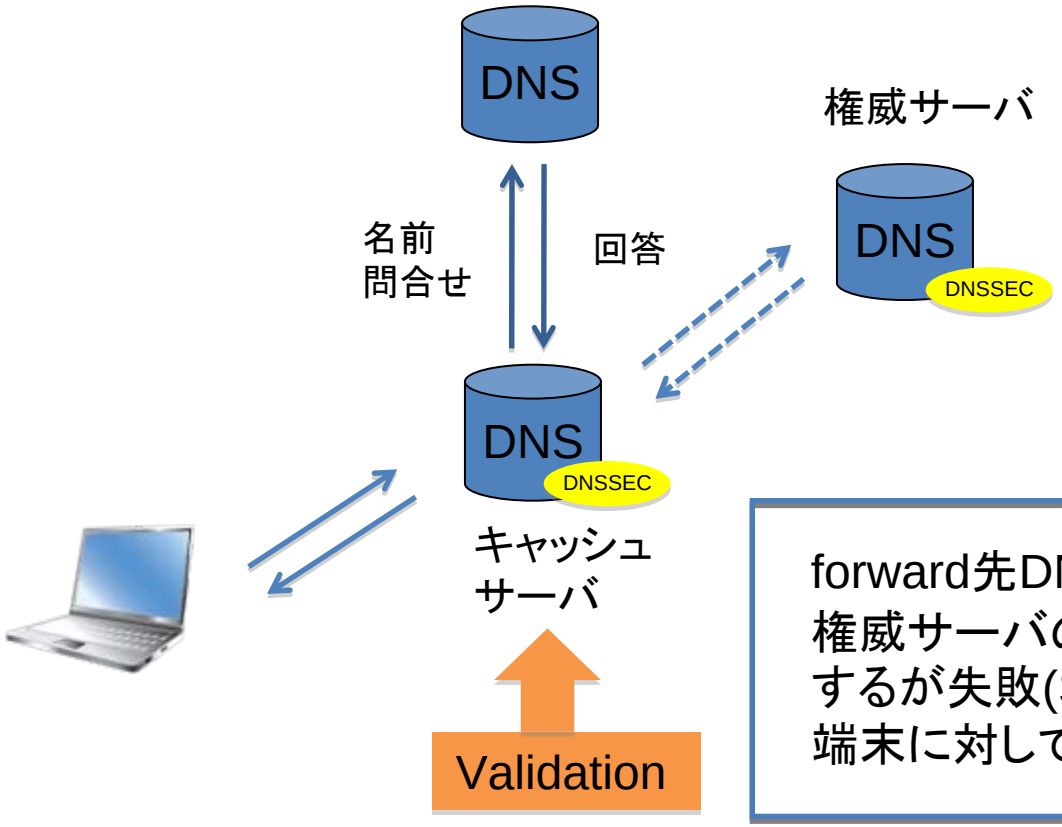
Firefoxへのプラグイン(DNSSEC Validator)



リゾルバでのDNSSEC検証

DNSSECに対応させた場合の影響

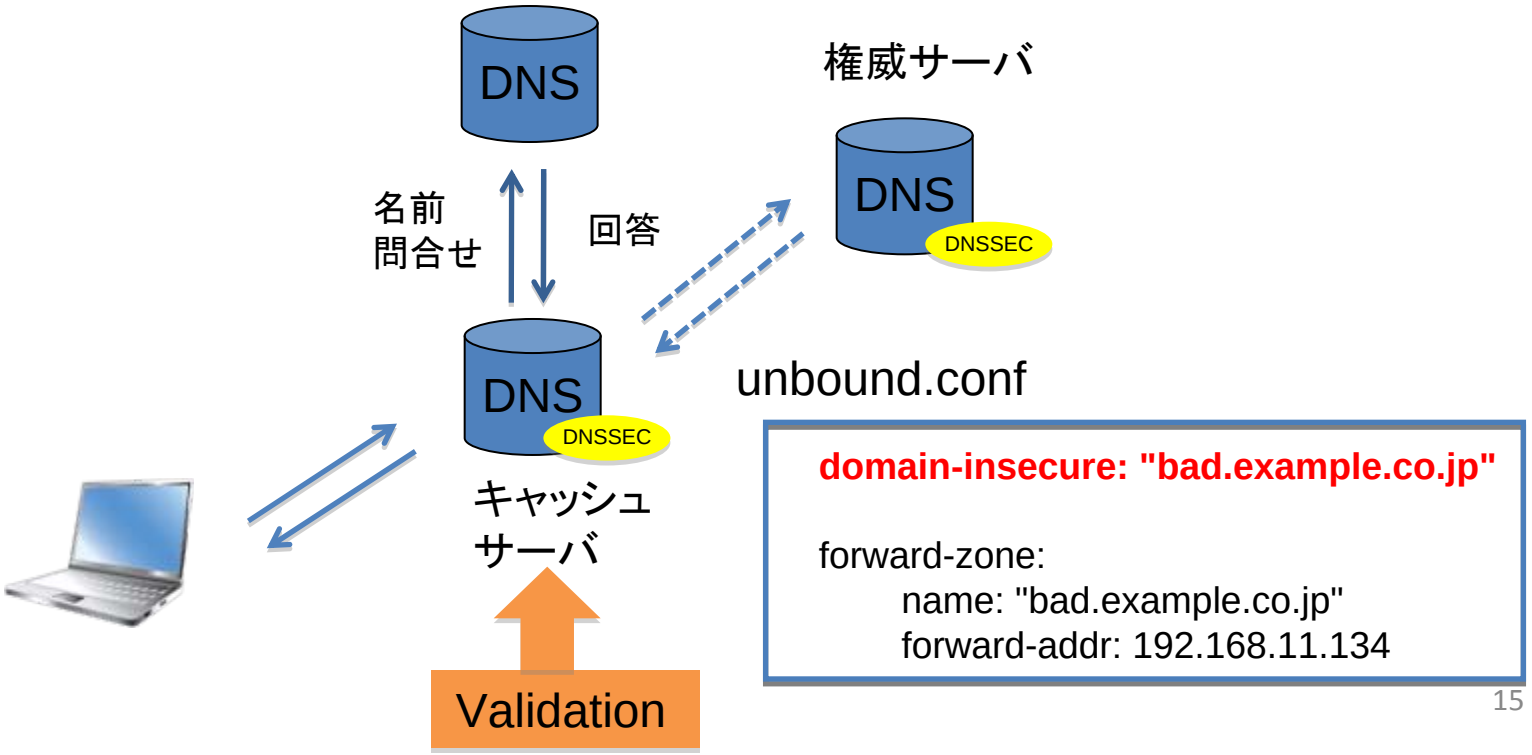
- キャッシュサーバをDNSSEC対応



forward先DNSからの回答を
権威サーバのゾーン情報と検証
するが失敗(ServerFail)
端末に対して名前解決はNG

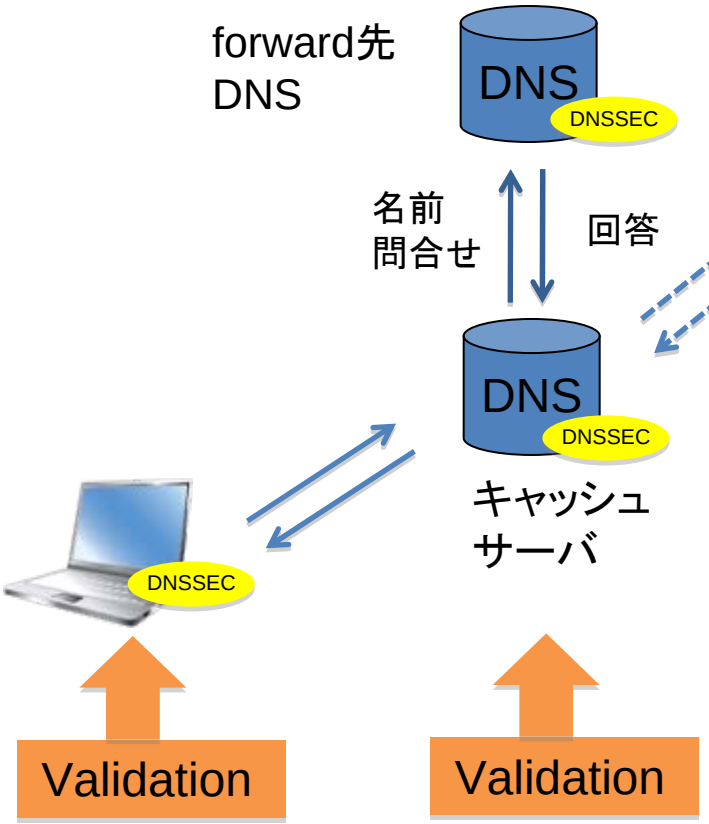
DNSSEC検証失敗を回避する方法

- 該当ホストの名前解決をDNSSEC検証対象外とする
- Unboundでは、domain-insecureとすることで対応可能(BINDには設定機能なし)
- クライアントからみるとDNSSEC未対応と認識



Forward先DNSがDNSSEC対応すると？

- キャッシュサーバではDNSSEC検証はOK
- クライアントでのDNSSEC検証はNG



キャッシュサーバでforwad先DNSの鍵を登録

```
zone "bad.example.co.jp." {
        type forward;
        forward only;
        forwarders { 192.168.11.134; };
};

trusted-keys {
“bad.example.co.jp.”  257 3 5
“ bad.example.co.jpの公開鍵” ;
};
```

DNSSEC対応時のブロッキング動作

- DNSSEC対応時のブロッキング用IPアドレスの名前解決の可否をパターン毎にまとめ

権威サーバ	forward 先DNS	キャッシュ DNSサーバ	キャッシュサーバ でのDNSSEC検証	クライアントでの DNSSEC検証
○	×	○	DNSSEC検証 NG(ServFail)	名前解決NG
○	×	○ (domain-insecure 設定あり)	DNSSEC検証 実施しない	名前解決OK (DNSSEC 検証なし)
○	○	○	DNSSEC検証 OK	名前解決OK DNSSEC検証NG

アドレスリストの例

- 2009年6月wikileaks.orgがブロッキングを実施しているイタリアのISPが使用している児童ポルノリストを調査し、公表(287サイト)

- イタリアのISP(CSINFO)のDNSに対して、ネット視聴率サイトから抽出した100万ドメインに対して名前問合せを行い該当ドメインを判別

- 該当の287サイトを目視確認（かなり主観的な判断）

-児童ポルノサイト　154サイト(54%)
-アダルトサイト　35サイト(12%)
-無関係なサイト　51サイト(18%)
（内、ホスティング事業者　12サイト）
-存在せず　47サイト(16%)
（売り出し中のドメインも存在）

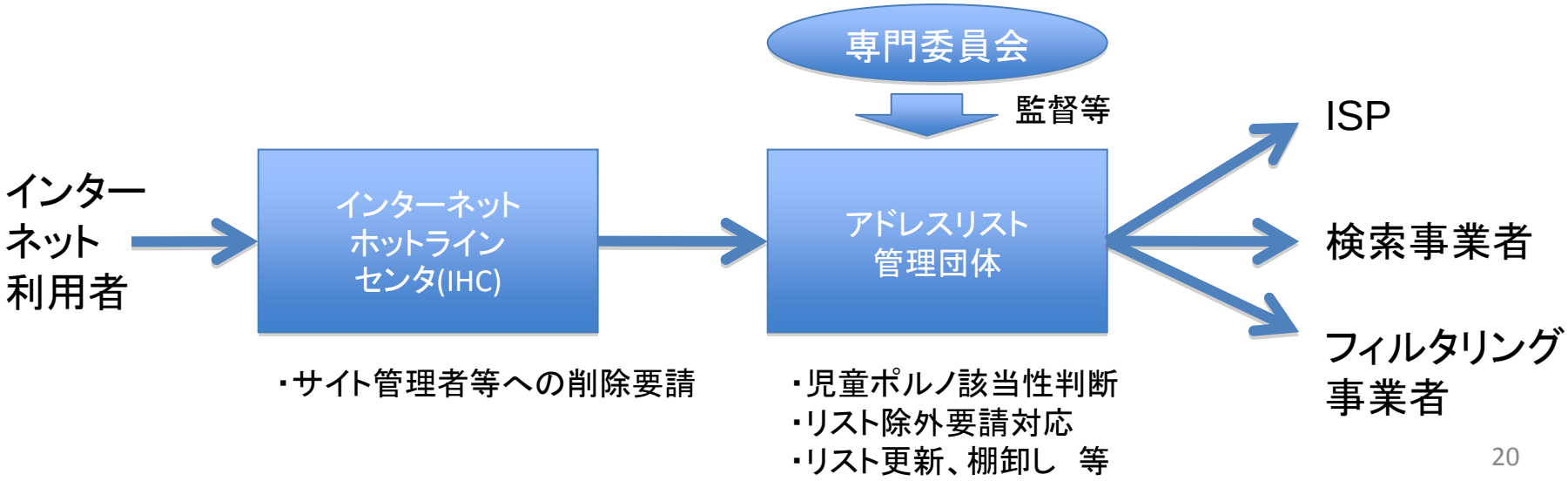
日本のホスティングサイトである
sakura.ne.jpやfc2.comもリストに存在


ATTENZIONE!! – POLIZIA POSTALE E DELLE COMUNICAZIONI – PAGINA BLOCCATA – Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り
アドレス(D) http://212.48.170.80/
Ministero dell'Interno
Dipartimento della Pubblica Sicurezza
Servizio Polizia Postale e delle Comunicazioni
polizia delle comunicazioni
STOP !!
PAGINA INTERDETTA DAL CENTRO NAZIONALE PER IL CONTRASTO ALLA PEDOPORNOGRAFIA SULLA RETE INTERNET
Il tuo browser sta tentando di raggiungere un sito Internet contenente immagini e filmati pedopornografici.
La detenzione, la distribuzione, la produzione, la commercializzazione di tale materiale prevedono l'applicazione di gravi sanzioni in base alla legge penale italiana e sono perseguibili anche ad opera di forze di polizia estere.
Nessun dato relativo al tuo ip address od altra traccia utile ad identificarti verrà registrato.
L'inibizione dell'accesso a questo sito è prevista dalla legge n. 38/2006 ed è stata operata al fine di impedire la commissione e la documentazione di violenze sessuali a minori degli anni diciotto. Questo servizio di protezione della navigazione sulla rete Internet è predisposto grazie alla collaborazione tra il "Centro Nazionale per il Contrasto alla Pedopornografia sulla rete Internet" e gli Internet Service Provider italiani.
Your browser is trying to contact an Internet site that is used in connection with distribution of photos depicting sexual abuse of children. This is a criminal offence in accordance with the italian penal code.
No information about your ip address or any other information that can be used to identify you will be stored when you this page is displayed.
The purpose of blocking access to these pages is only to prevent the commission of criminal dissemination of documented sexual abuse, and to prevent the further exploitation of children who have already been abused and photographed. This is a prevention service provide from italian Internet Service Provider and the italian "National Centre for Combating On-line child pornography".
EUROPOL
C.I.R.C.A.M.P.
Cospol Internet Related Child Abusive Material Project
Il filtro antidistribuzione del materiale pedopornografico è parte dell'iniziativa "CIRCAMP" (Cospol Internet Related Child Abusive Material Project).
Tale progetto è stato avviato dalla "Task-Force" dei capi delle polizie europee per combattere la criminalità organizzata che gestisce il commercio di materiale prodotto mediante l'utilizzo sessuale dei minori.
The Child sexual abuse anti-distribution filter in part of the "CIRCAMP" (Cospol Internet Related Child Abusive Material Project). The project is initiated by the european police chief task-force - aimed at combating organized criminal group behind commercial sexual exploitation of children.

リスト作成管理団体

- アドレスリストの作成、維持管理、提供を行うリスト作成管理団体を選定
- 今年度は警察庁からの委託研究によりインターネット協会が実証実験を実施中

  - アドレスリストを事業者に渡すところまで
  - 来年度からの正式なアドレスリスト管理団体が利用可能な「業務マニュアル」を策定



ブロッキング実施に向けての課題（1）

- リストの仕様、リスト管理団体とのリスト受渡方式
- リストはどのようにして、どう作られるのか？
  - 対象範囲、種別（方式毎）、項目、ボリューム　etc
- リストの受渡しのプロトコルは？
- リストに関わる運用方法は？
  - 更新周期、除外申請、利用者向けの告知用サイト etc

リスト受渡し仕様についての要望

- 2010/9/30に安心協より児童ポルノ防止協議会に要望を提出

- 具体的な要望としては、以下の項目を提示

  - インターネット経由でのhttpsで通信路を暗号化を実施
  - CSV形式で、ブロッキング方式毎の提供
  - リストファイルを取得する場合の認証機能
  - 極力短い周期でのリストのアップデート（更新）
  - インターネット利用者からの問合せ体制の整備
  - オーバブロッキング時の対応体制の整備
  - リストの棚卸しの実施
  - ブロッキング時の注意画面の統一、連絡先の明記
  - ブロッキング実施の周知の際のインターネット利用者への対応連携
  - リスト受渡しに関する設備の運用保守体制の整備

  等

ブロッキング実施に向けての課題（2）

- DNSを利用した方式の場合、DNSSECとの関係
- オーバブロッキングに対するISPのリスク
- リストの誤りに対するISPのリスク、リストの信頼性の担保
- リスト作成・管理に関わるコスト負担
- 実際に必要となる設備量は？
  - リスト対象サイトへのトラヒック量 etc
- ブロッキングによる児童ポルノ流通防止の効果は？
  - より精度の高いブロッキング方式、そのための設備投資
  - リスト管理団体との密な連携の必要性