

児童ポルノブロッキングの 現状と課題

児童ポルノ対策作業部会
副主査 兼 ISP技術者サブワーキンググループ
リーダー 北村 和広

ブロッキング導入検討の経緯

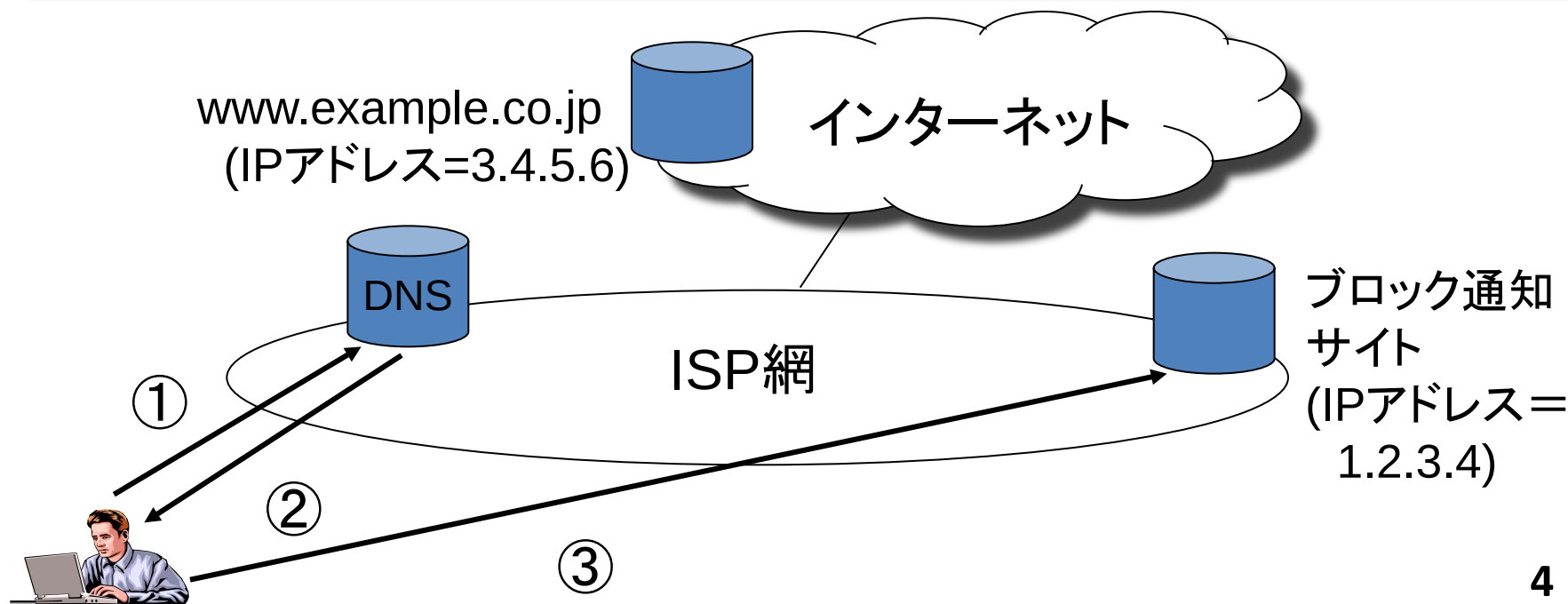
- 2009/2 安心協においては、2010/2発足時より「児童ポルノ対策作業部会」(主査:森亮二弁護士)を設置し、検討を実施
- 2010/5/18 総務省ICT諸問題研究会
2010/7/27 犯罪対策閣僚会議 児童ポルノ排除総合対策
 - 2010年度中にブロッキング実施に向けた環境を整備
- 2011/3 ICSA設立、アドレスリスト管理団体に選定
- 2011/4/1～ ICSAがブロッキングアドレスリストの提供開始
- 2011/4/21～ ISP9社、検索サービス事業者4社、フィルタリングサービス事業者3社が対応開始
 2011.10末時点で51社・4団体が参加

ブロッキングアドレスリストの対象範囲

- 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」によると、
 - 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 その他、既に多くのウェブサイト又はウェブページを通じて流通が拡大しているなど、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

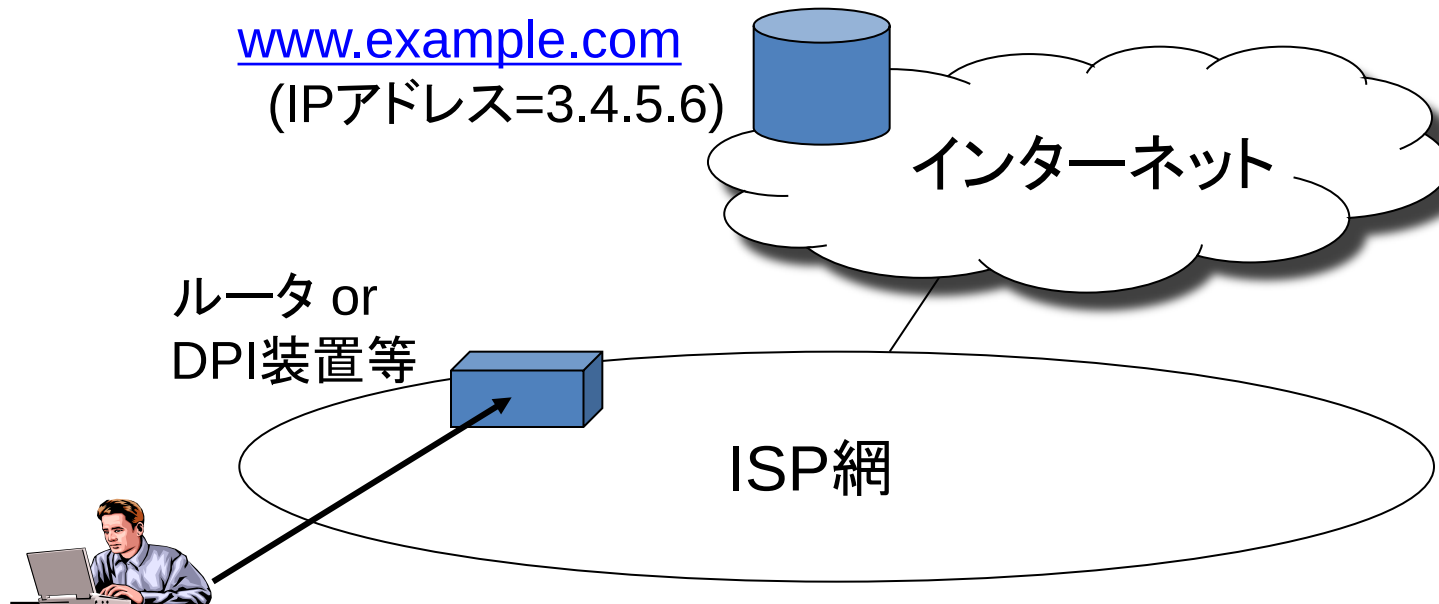
DNSブロッキング方式

- 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



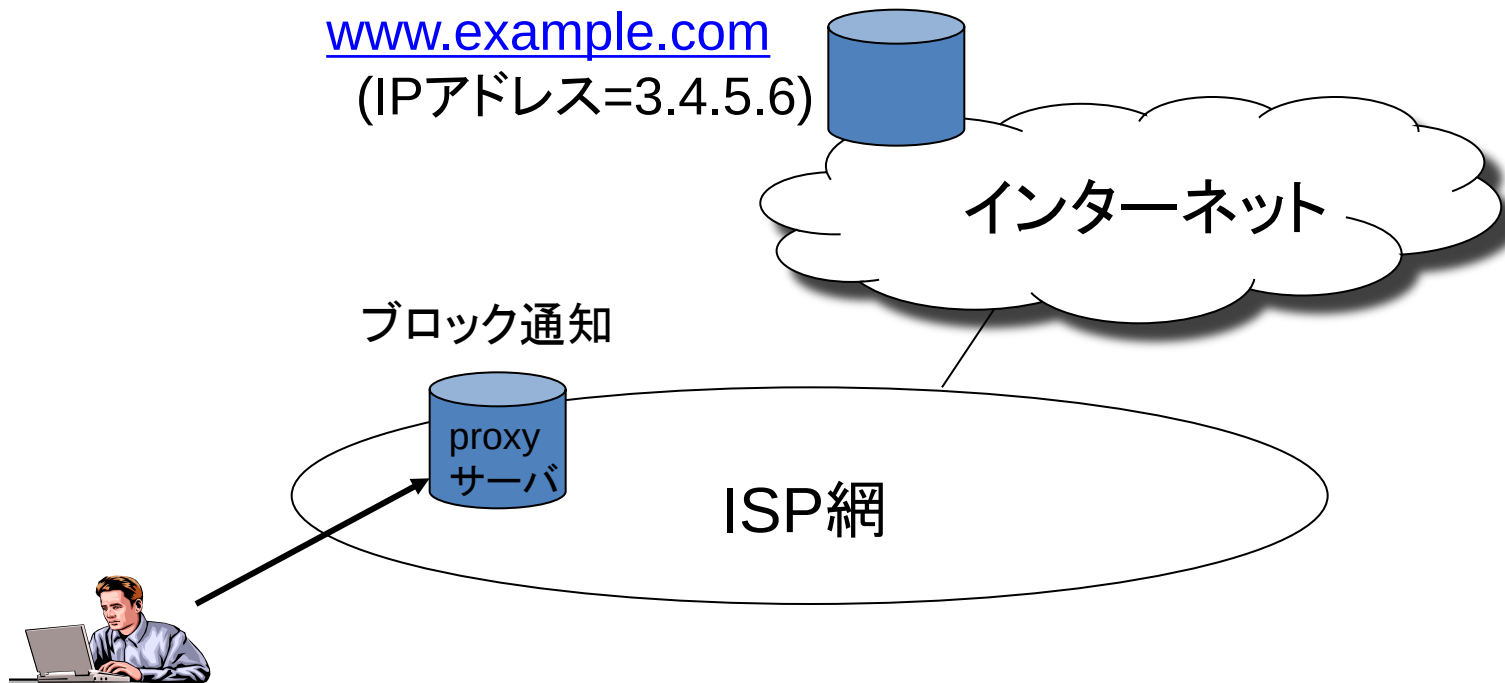
パケットフィルタリング方式

- 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



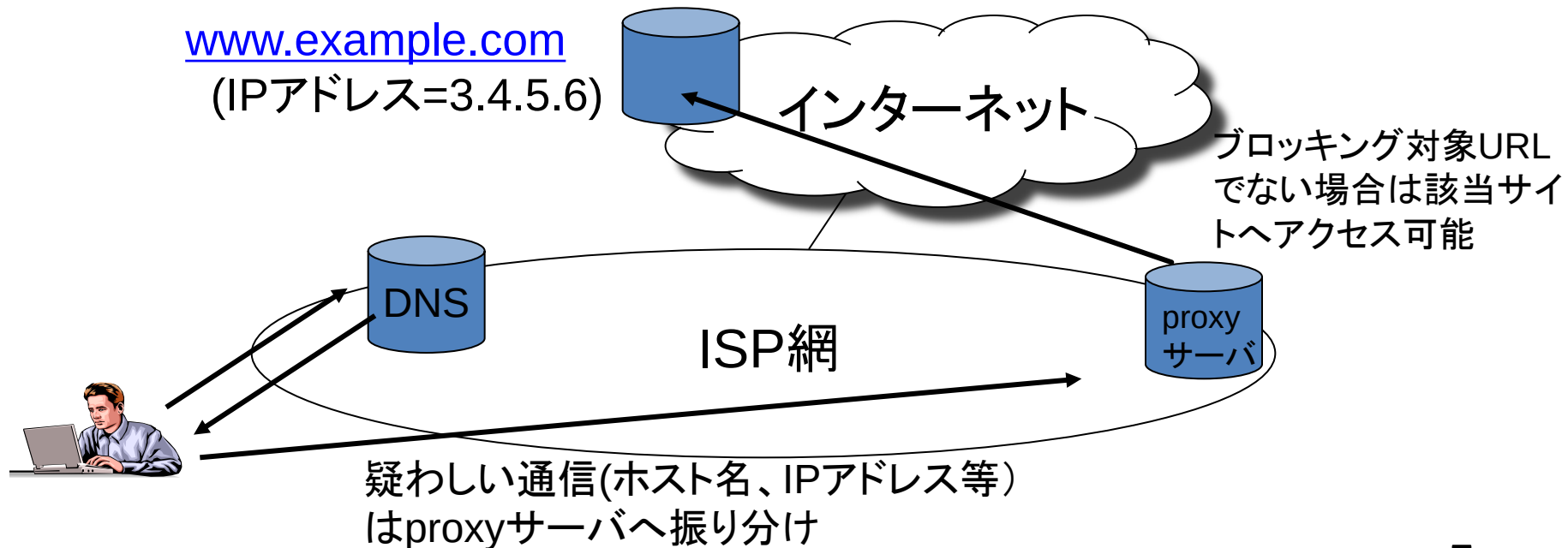
プロキシ方式

- 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



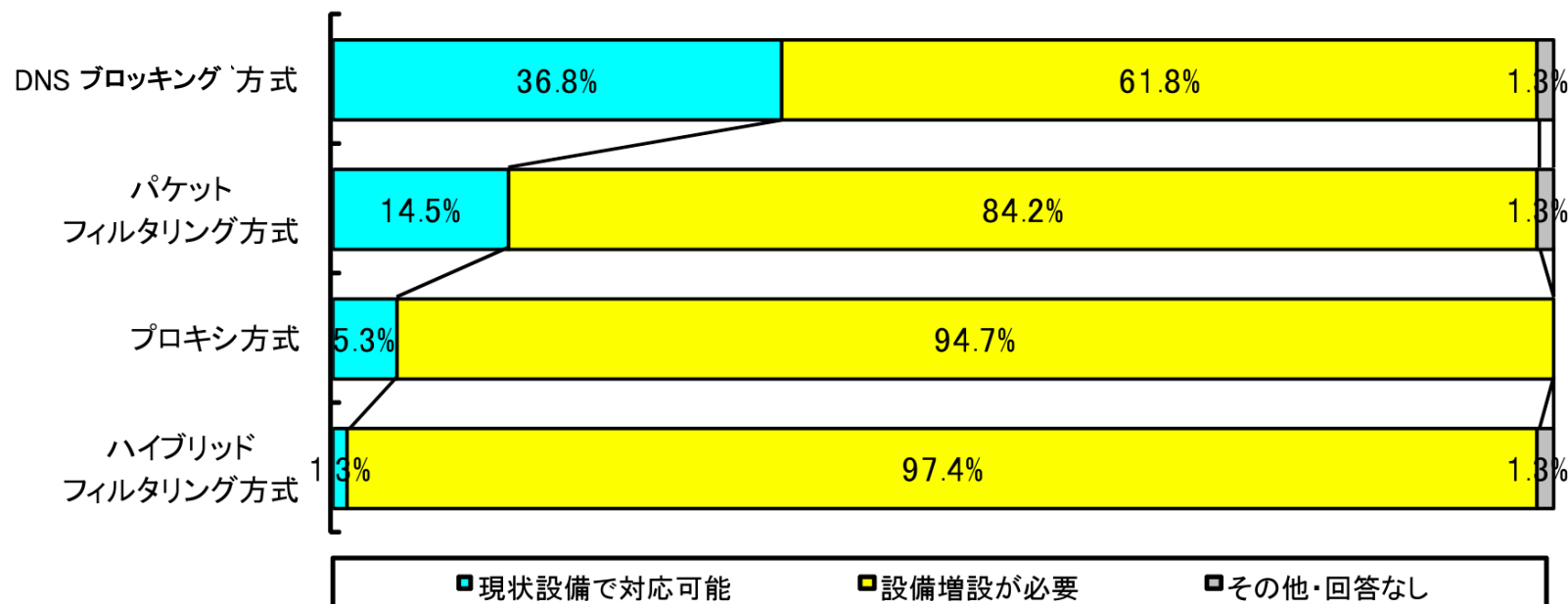
ISPへのアンケート結果

- 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(2010年)
- DNSブロッキ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
- 今年度さらにアンケートを実施予定

ISPアンケート結果①

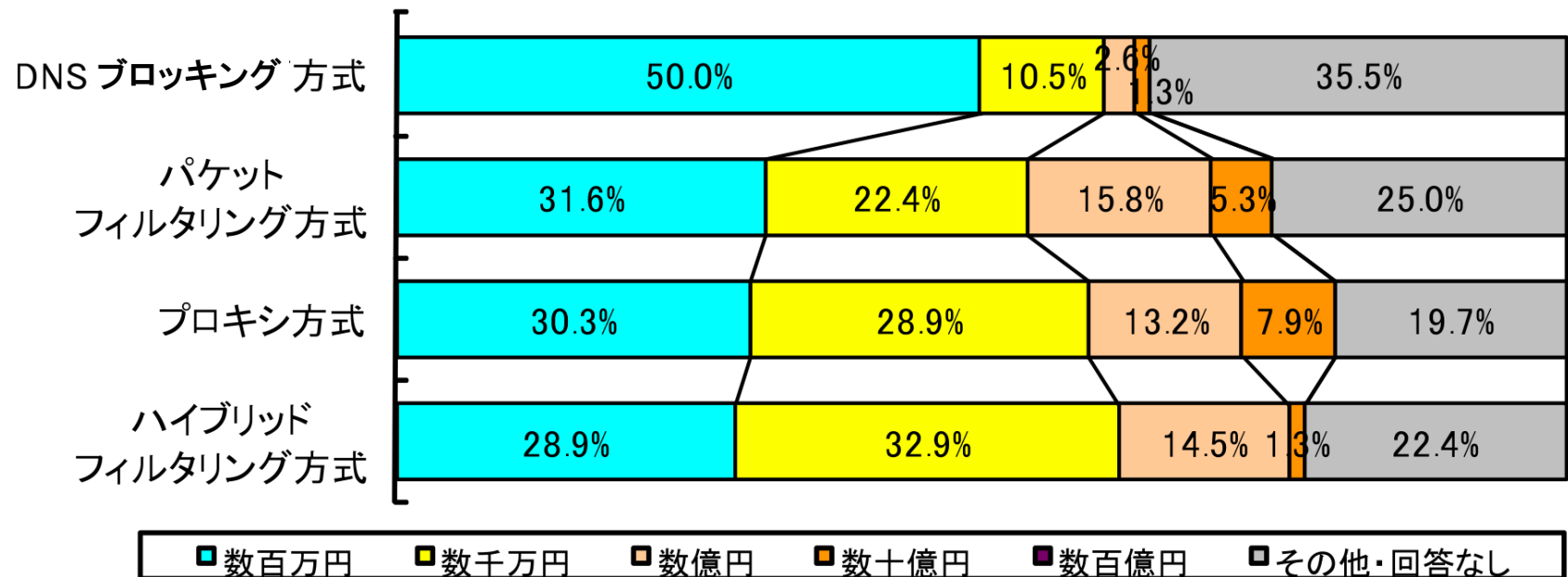
(設備投資の必要性)

- DNSブロッキング方式が比較的設備投資を必要としない手法と考えられている
- 大規模事業者ほど設備投資が必要との意見が多い



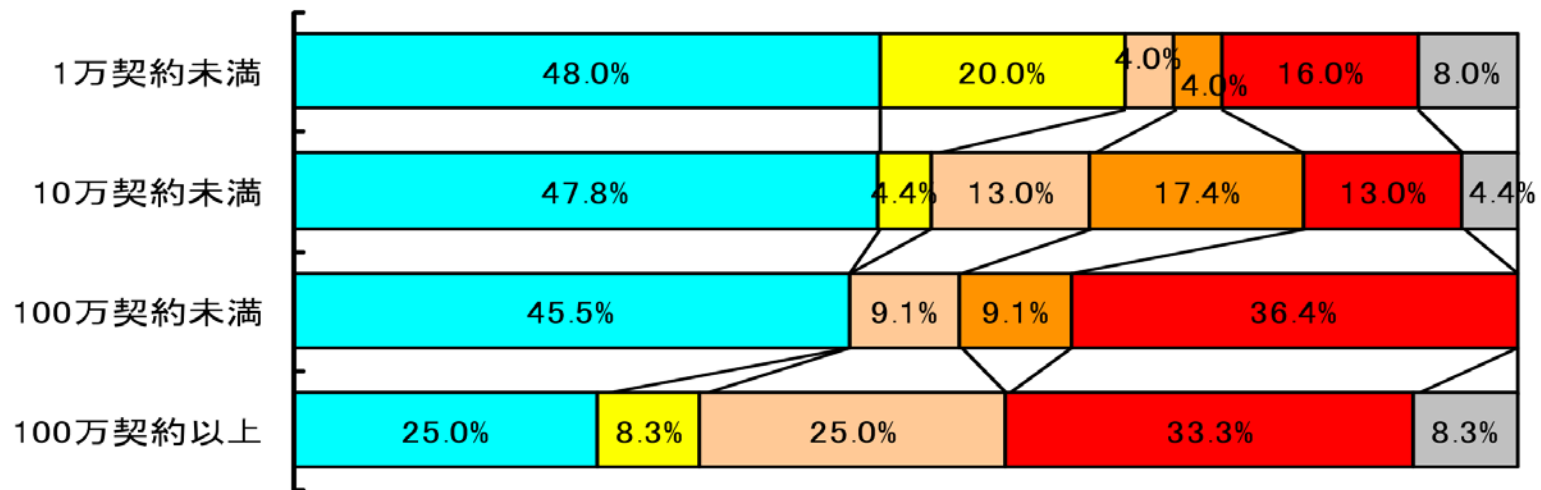
ISPアンケート結果② (コストの試算)

- 初期費用が抑えられる方式としてDNSブロッキング方式をあげるISPが多い
- ランニング費用およびサポート費用については方式間で大きな差はないが、どちらも事業規模に比例してコストも増大
- 総コストではDNSブロッキング方式が最も低廉に導入可能



ISPアンケート結果③ (採用可能な方法)

- DNSブロッキング方式が採用可能であるという意見の割合大
- 事業規模の拡大に伴いDNSブロッキング方式の導入回答率が減少し、いずれも不可との回答率が増加
オーバブロッキングに対するカスタマサポートへの懸念か？



■DNS:ブロッキング方式 ■パケットフィルタリング方式 ■プロキシ方式 ■ハイブリッドフィルタリング方式 ■いずれも不可 ■回答なし

ISPアンケート結果④

(実施までに要する期間)

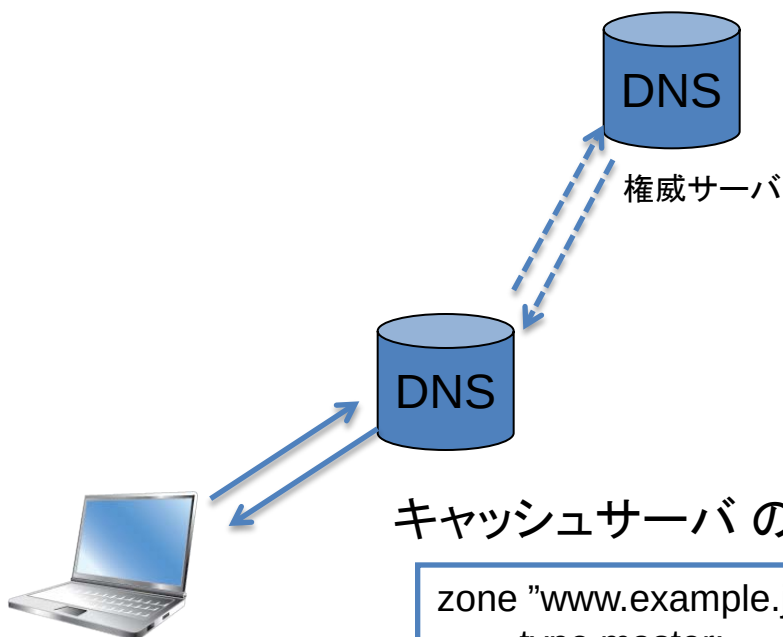
- DNSブロッキング方式が最も短期間で実現可能だと考えられている
- 追加的投資の社内オーソライズ期間、運用に関わるトレーニング等の準備期間が必要とされている

手法\期間	3ヶ月程	6ヶ月程	1年程	2年程	その他・回答なし	平均期間(月)
DNSブロッキング方式	18.4%	25.0%	27.6%	2.6%	26.3%	8.2
パケットフィルタリング方式	7.9%	10.5%	25.0%	13.2%	43.4%	12.3
プロキシ方式	3.9%	14.5%	26.3%	15.8%	39.5%	13.4
ハイブリッドフィルタリング方式	2.6%	14.5%	28.9%	13.2%	40.8%	12.7

具体的なDNSの設定例 (BINDの場合)

BIND9.7.0-P1

www.example.jp.db



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

ns      10      IN      A      192.168.11.134
Ns      10      IN      AAAA   fe80::216:36ff:fed9:5790
www.example.jp. 0   IN      A      192.168.0.10
www.example.jp. 10  IN      AAAA   fe80::216:36ff:fe68:51e4
```

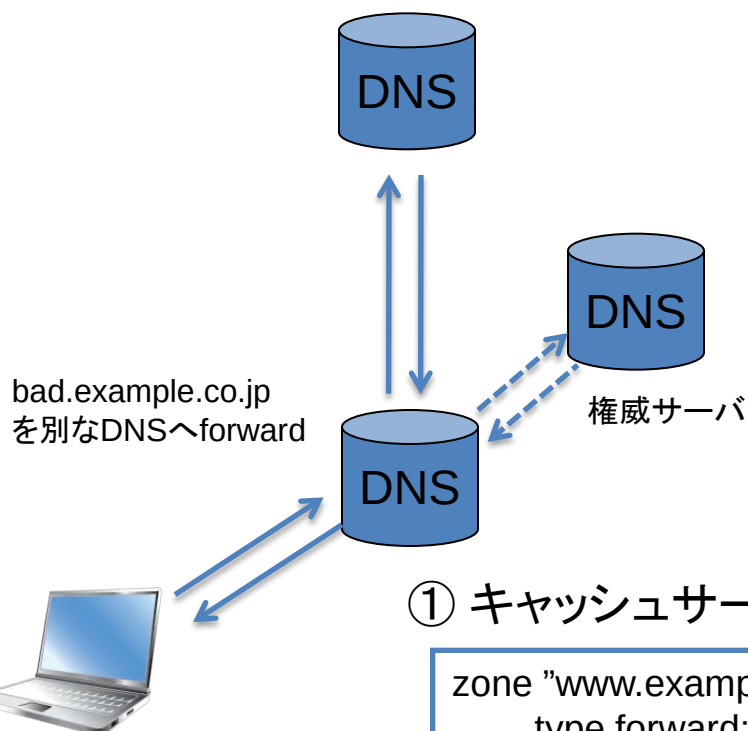
キャッシュサーバのnamed.conf

```
zone "www.example.jp." {
    type master;
    file www.example.jp.db;
};
```

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 "www.example.jp" {  
    type master;  
    file "www.example.jp.db";  
};
```

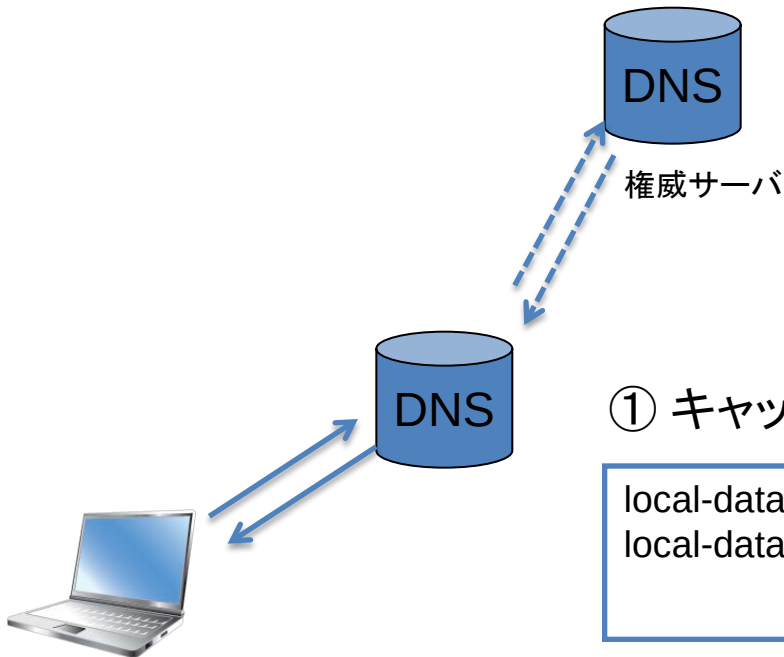
```
$TTL 0  
www.example.jp. 10 IN SOA admin.www.example.jp. admin.www.example.jp. (  
    2010101527 ; serial  
    7200      ; refresh (2 hours)  
    3600      ; retry (1 hour)  
    604800    ; expire (1 week)  
    600       ; minimum (10 minutes)  
)  
10 IN NS ns.www.example.jp.  
ns.www.example.jp 10 IN A 192.168.11.134  
ns.www.example.jp 10 IN AAAA fe80::216:36ff:fe92:9fb  
www.example.jp. 10 IN A 192.168.0.10  
www.example.jp 10 IN AAAA fe80::216:36ff:fe68:51e4
```

① キャッシュサーバ named.conf

```
zone "www.example.jp." {  
    type forward;  
    forward only;  
    forwarders { 192.168.11.134;  
                 fe80::216:36ff:fe92:9fb;  
    };  
};
```

具体的なDNSの設定例 (unboundの場合)

unbound 1.4.1



① キャッシュサーバ unbound.conf

```
local-data: "www.example.jp 10 IN A 192.168.0.10"  
local-data: www.example.jp 10 IN AAAA fe80::216:36ff:fe68:51e4
```

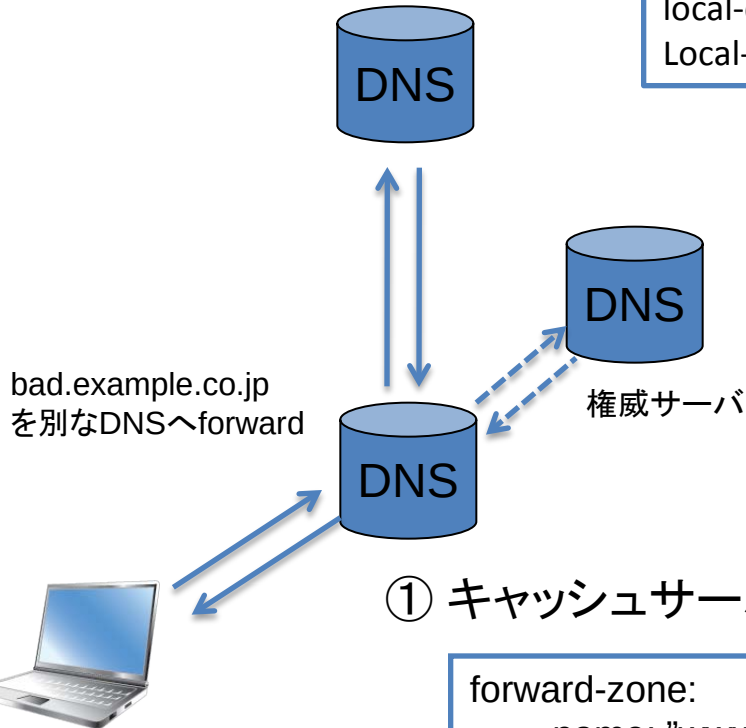
具体的なDNSの設定例 (unboundの場合)

unbound 1.4.1

② forward先のDNS unbound.conf

local-data: www.example.jp 10 IN A 192.168.0.10

Local-data:www.exapmle.jp 10 IN AAAA fe80::216:36ff:fe68:51e4"



① キャッシュサーバ unbound.conf

forward-zone:

name: "www.example.co.jp"

forward-addr: 192.168.0.200

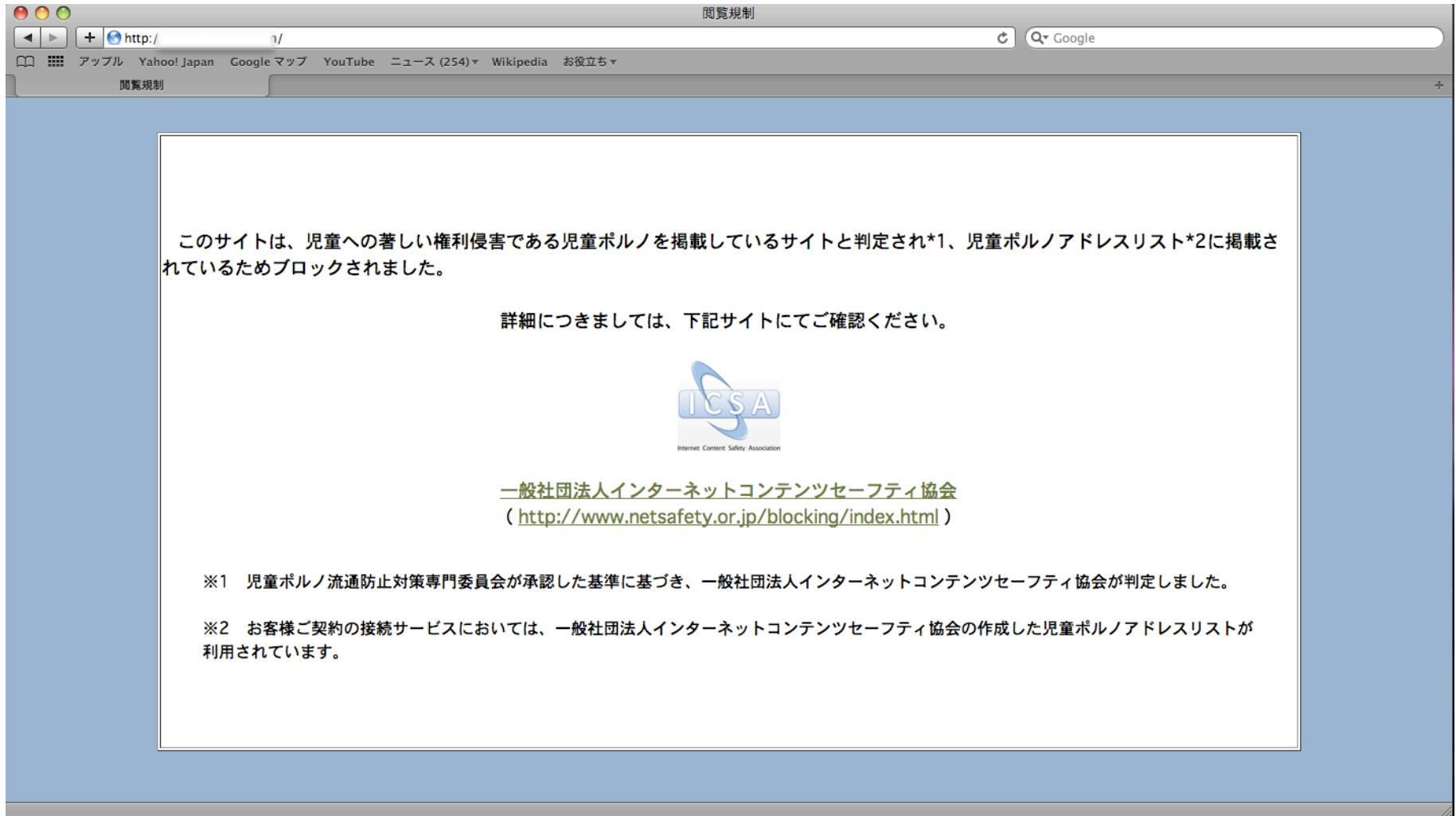
リダイレクトWebサーバの設定例

- ブロッキング警告画面ドメインへリダイレクト(307 Temporary Redirect)
- ブロッキング警告画面仕様はリスト管理団体により提供され、画面は各ISP毎に設置

```
# ブロッキング警告画面へのリダイレクト用 VirtualHost
<VirtualHost 192.168.0.10:80>
RedirectMatch 307 (.*) http://www.redirect-example.jp/index.html ←リダイレクト先
ServerName *
ErrorLog /var/log/httpd/bad_error_log
TransferLog /var/log/httpd/bad_access_log
</VirtualHost>
```

```
# ブロッキング警告画面表示用
<VirtualHost 192.168.0.10:80>
DocumentRoot /var/www/html/redirect
ServerName www.redirect-example.jp ←警告画面ホストのドメイン名を指定する
ErrorLog /var/log/httpd/redirect_error_log
TransferLog /var/log/redirect_access_log
</VirtualHost>
```

ブロッキング警告画面



ブロッキングがDNS処理に与える影響

以下のパラメータを変化させて評価を実施

- ① DNS問合せクエリ数(500qps、1,000qps)
- ② アドレスリスト数(500、1,000、3,000、5,000)
- ③ DNSキャッシュヒット率(0%、50%、80%)
- ④ ハードウェアスペック(Intel Pentium4 2.4GHz/
メモリ1GB、Intel Xeon X5650 2.67GHz/メモリ8GB)
- ⑤ DNSソフトウェア(BIND9.7.2-P3、unbound1.4.7)

ブロッキングがDNS処理に与える影響

(1) DNS名前解決処理に与える影響

CPU、メモリ等システムリソースへ与える影響はほとんどなし

(2) アドレスリスト更新処理の影響

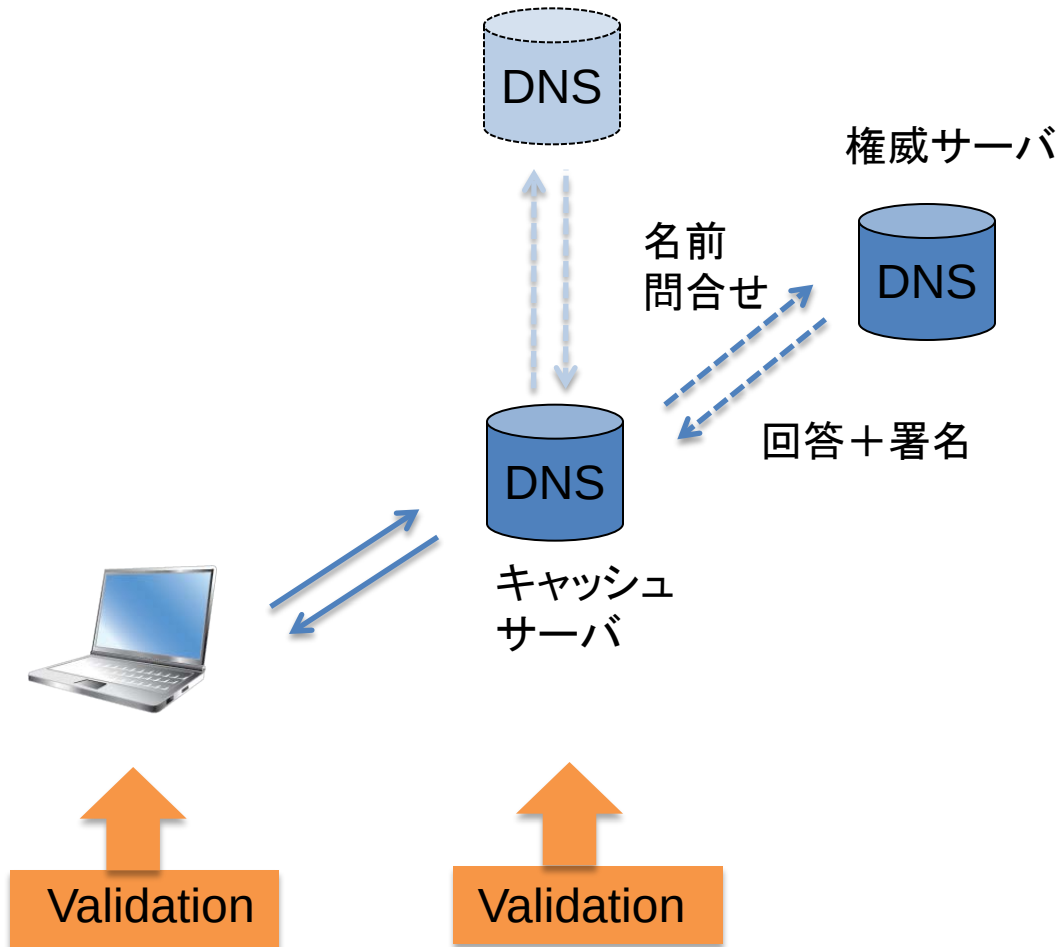
- ・BINDの場合、低スペックマシンではリスト更新処理時にリスト数300で影響あり(キャッシュヒット率0%)

高スペックマシンでは改善するものの3,000リストでクエリ落ち

- ・unboundの場合、低スペックマシンではリスト更新処理時にリスト数300で影響あり(キャッシュヒット率0%)

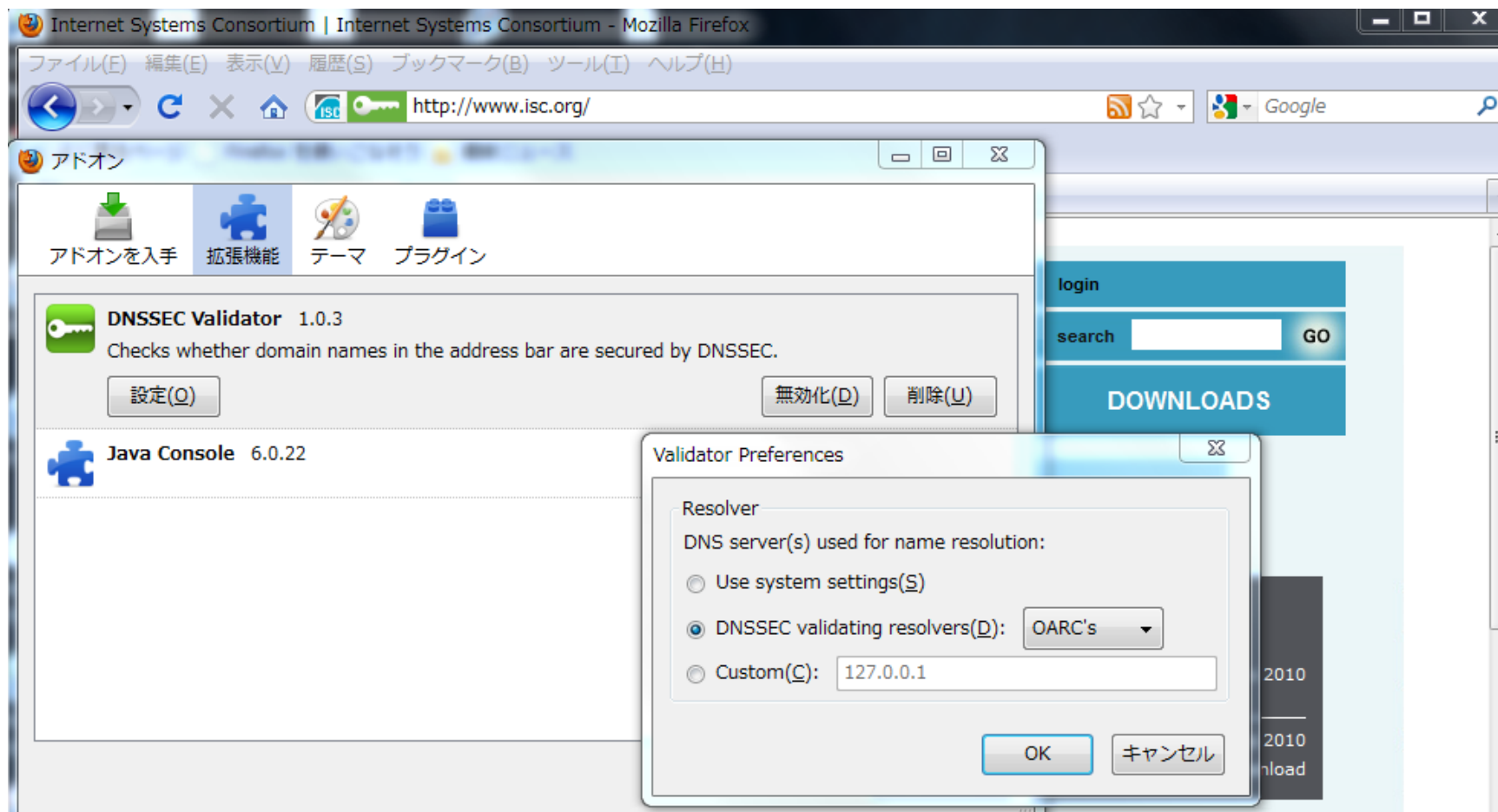
高スペックマシンでは10,000リストでも影響はなくクエリ処理可

DNSSECの概要



リゾルバでのDNSSEC検証

Firefoxへのプラグイン(DNSSEC Validator)

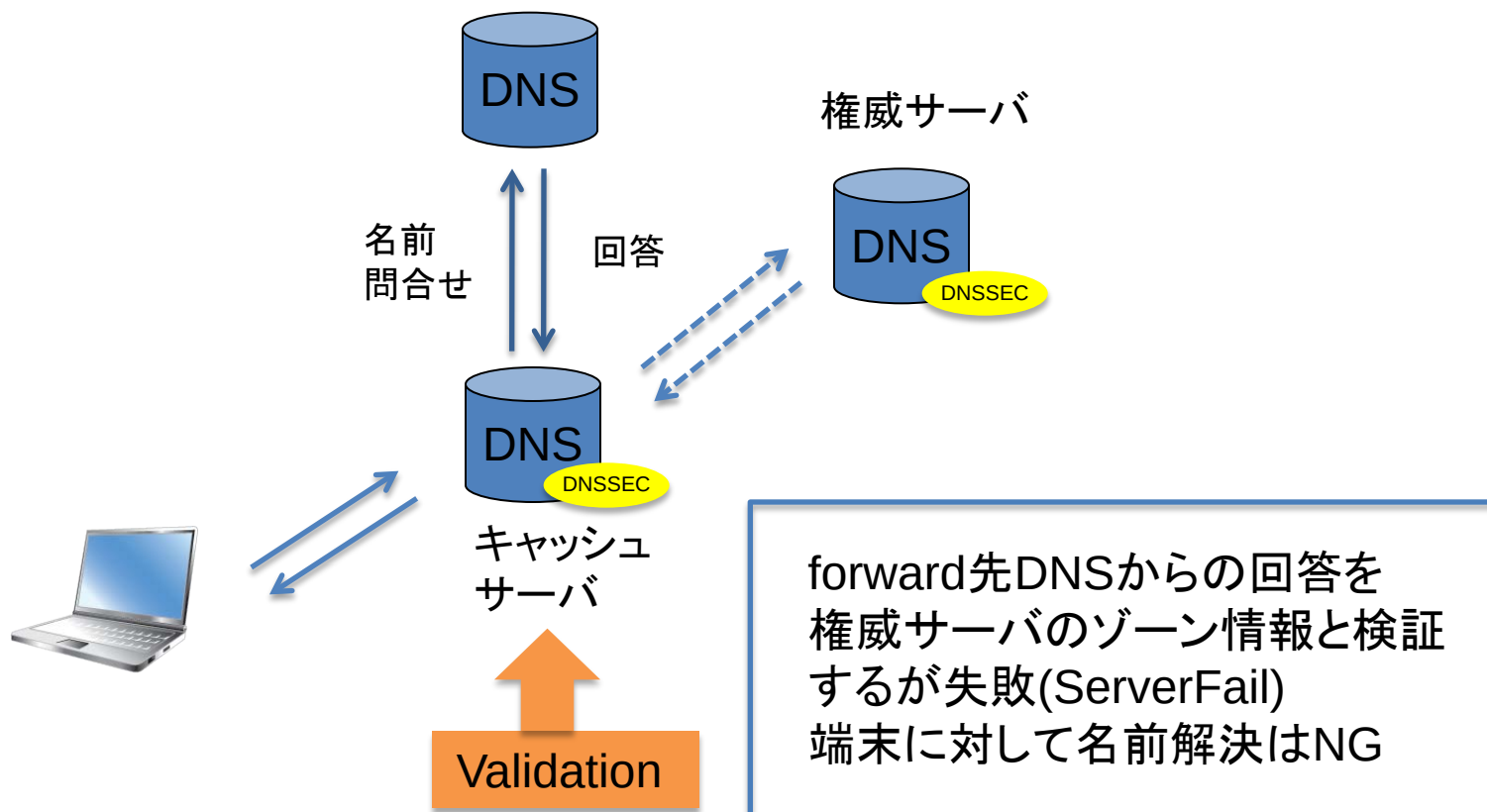


リゾルバでのDNSSEC検証



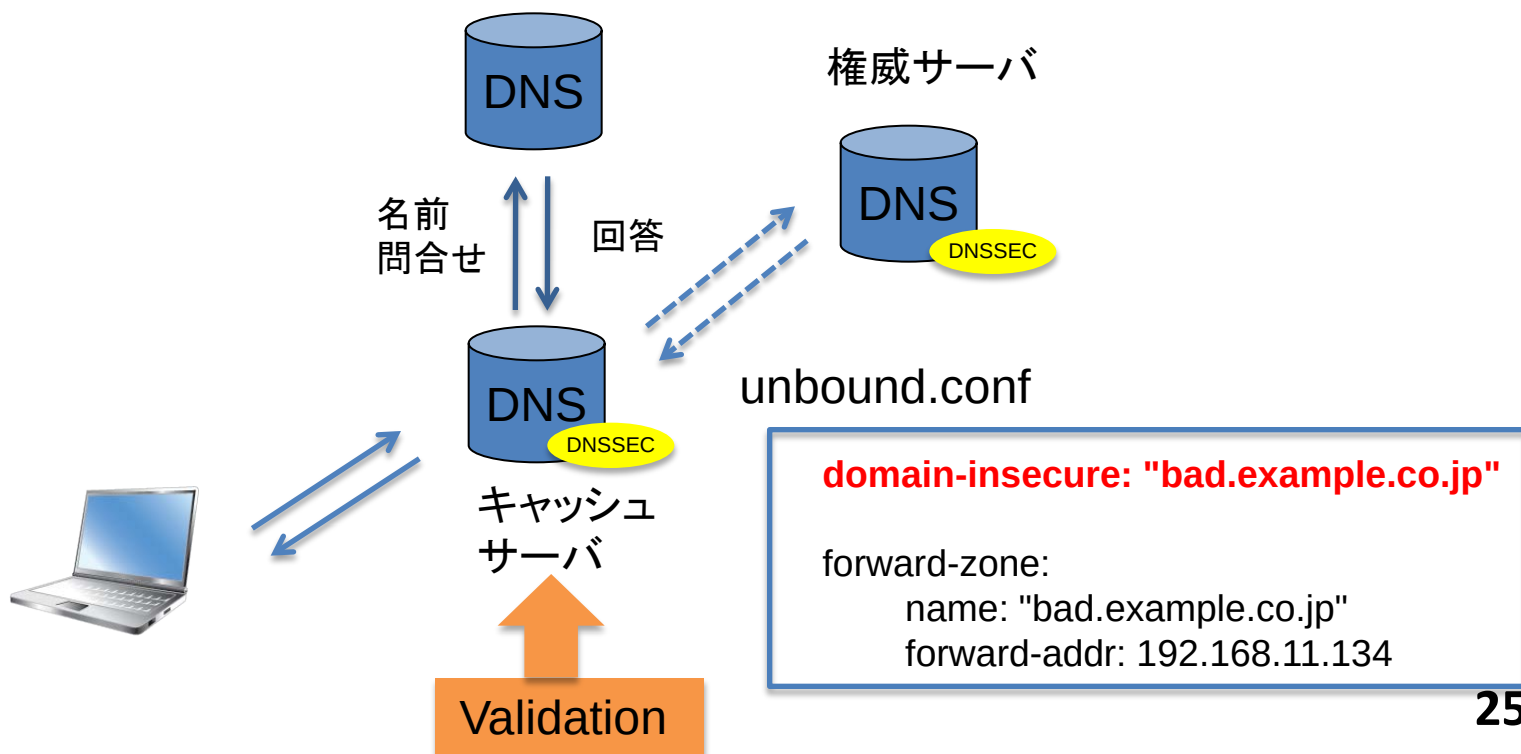
DNSSECに対応させた場合の影響

- キャッシュサーバをDNSSEC対応



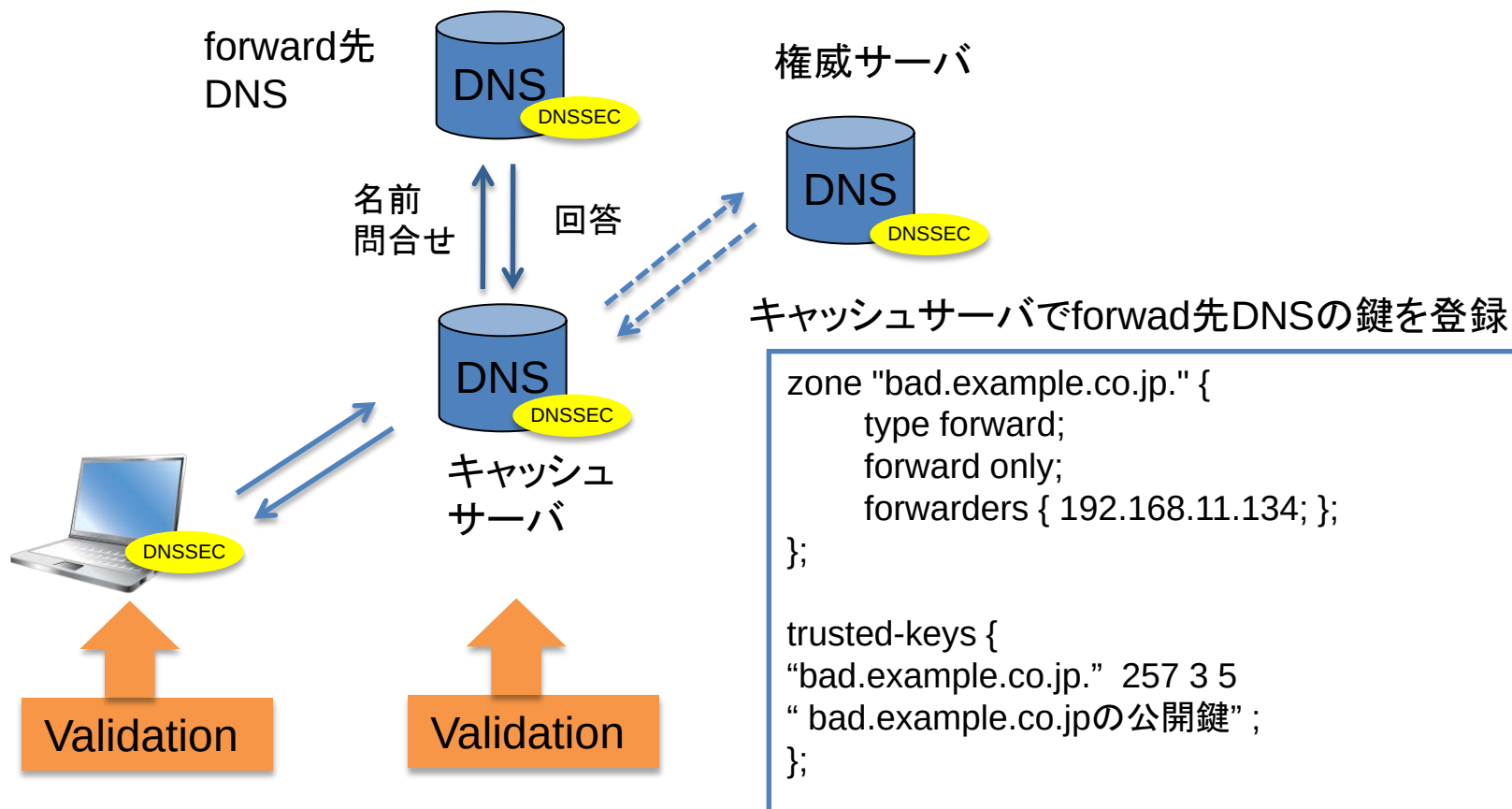
DNSSEC検証失敗を回避する方法

- 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



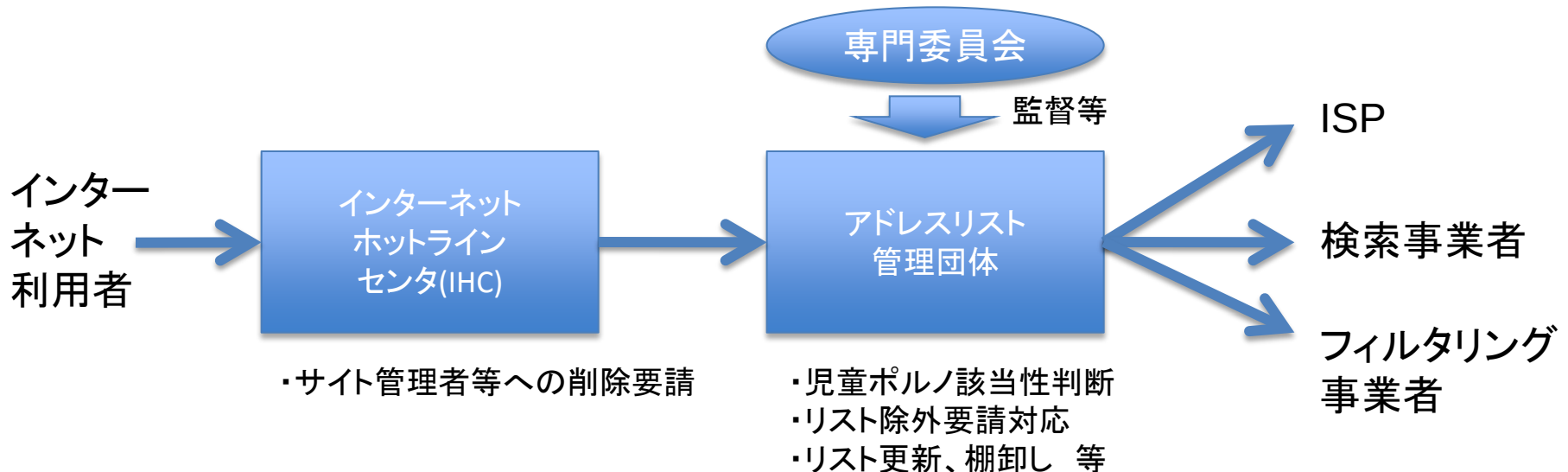
DNSSEC対応時のブロッキング動作

- 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

リスト作成管理団体

- 児童ポルノ掲載サイトのアドレスリストの作成・管理・提供
- 2011/3 インターネットコンテンツセーフティ協会(ICSA)が児童ポルノ流通防止対策専門委員会により選定
- 民間の21社・団体(ISP、検索サービス事業者、フィルタリングサービス事業者)により設立



DNSブロッキングリスト対象判定基準(1)

① サイト開設の目的

当該ドメインに含まれるサイトの相当部分の開設目的の全部又は一部が、児童ポルノの画像等をそれと知りながらインターネット上で流通させることにありと認められること

② 児童ポルノ画像の数量

当該ドメインに含まれるサイトの中に、

(ア) 児童の権利等を著しく侵害するものであることが明白な画像等が存在するか、

(イ) 児童の権利等を著しく侵害する画像等が相当数存在するか、

(ウ) 児童の権利等を著しく侵害する画像等が相当の割合で存在するか、のいずれかであること。

DNSブロッキングリスト対象判定基準(2)

③ 発信者の同一性

(ア) 当該ドメイン内に複数のサイトがある場合には、各サイトの管理者が同一であること。

(イ) (略)

④ 他の実効的な代替手段の不存在

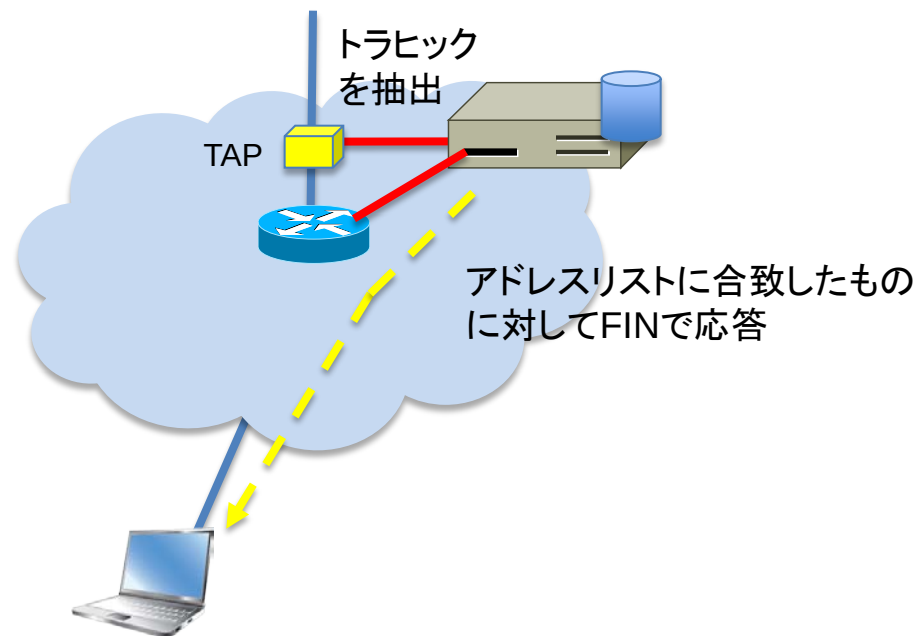
当該ドメインをDNSブロッキングの対象とすることが、①ないし③及びその他の諸般の事情を総合的に考慮した上で、やむを得ないと認められること

アドレスリストを入手するには？

- ICSAに入会 & リスト利用申込契約
- リスト利用の場合は発起時会員2名からの推薦が必要
- 会費 契約数に応じて、年5万円(1口)～
- アドレスリストの構成要素
 - 掲載ページのホスト名/IPアドレス/URL/DNSブロッキングの可否
 - 該当画像のホスト名/IPアドレス/URL/画像ハッシュ値/DNSブロッキング可否
 - 掲載ページのIPアドレス確認日/最終存在確認日
 - 該当画像のIPアドレス確認日/最終存在確認日
 - 事業者提供日(アドレスリスト提供日) 等
- アドレスリストの取得方法

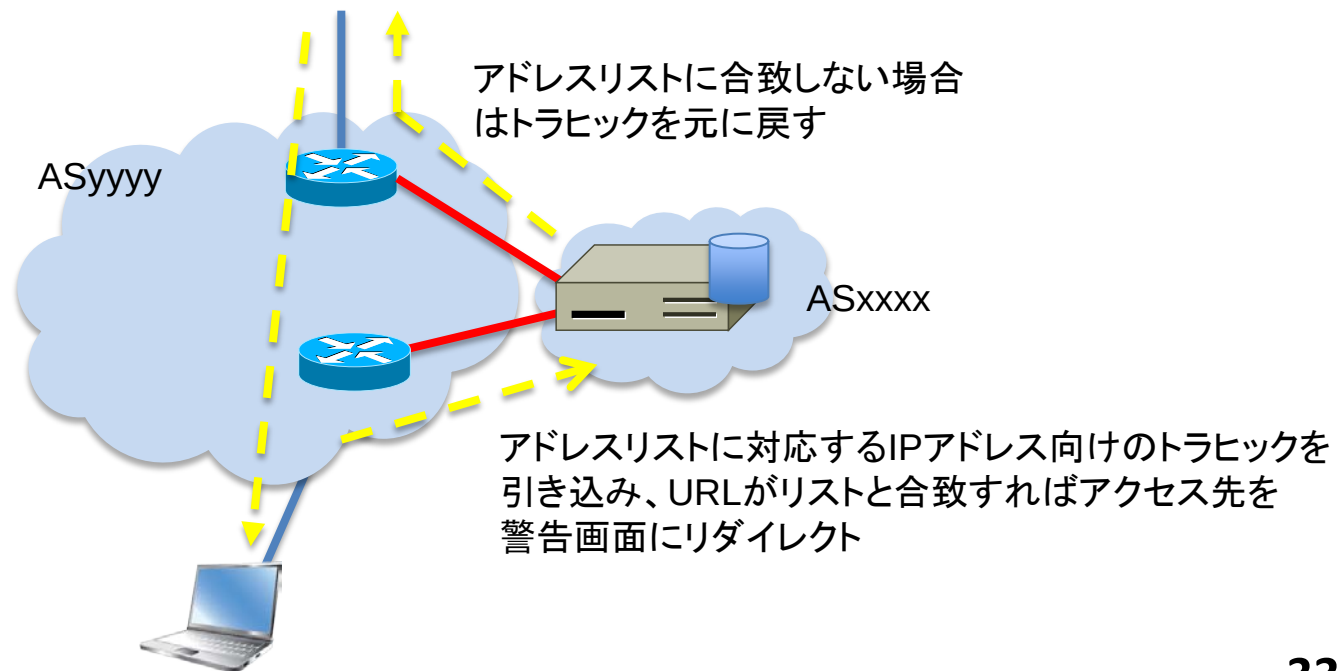
より高精度なブロッキング手法(1)

- パケットフィルタリング方式
 - URL単位に実施可能な装置が既に導入済であれば対応可能だが、新規に導入するには投資負担が懸念
 - ブロッキングに特化した安価なソリューションの出現



より高精度なブロッキング手法(2)

- ハイブリッドフィルタリング方式
 - トラフィック集約方法としては、DNSや経路制御
 - URL単位でのブロッキング装置としては、proxyやDPI



今後の課題

- ISP内、ISP～ICSA間の運用（自動化etc）
- DNSブロッキング方式の効果検証（指標、計量化et）
- 高精度（URL単位ブロッキング）方式の具体的方式検討、課題抽出、ガイドライン策定（総務省実証実験の場を活用して実践的な議論をとりまとめ）
- 中小規模ISPへの展開