ISP 技術者サブワーキング　報告書

目次

別紙

第1　検討の視点

インターネット上で児童ポルノを公開することは現行法上も違法であり、すでに違法情報ガイドライン[1]や契約約款モデル条項[2]等においても禁止行為として自主的な削除の対象とされており、インターネットホットラインセンターでも警察への通報、プロバイダへの削除依頼等の対応を取っている。

しかしながら、これらの活動は児童ポルノを蔵置しているサーバが海外にあり、かつ、その管理者が海外ないし不明である場合には実効性が乏しいとの指摘がなされている。ここで、現在注目されている手法が、ISPにおいて個々のユーザの同意を得ることなく児童ポルノサイトへのアクセスを阻止するブロッキングと呼ばれる手法である。ブロッキングは、すでに北欧諸国、イギリス、イタリア等のヨーロッパ諸国において、主として自主的取組として実施されている。

もっとも、ブロッキングには、いくつかの方式があり、それによって、設備投資の要否・コスト負担の程度、ブロッキングの精度等が異なると言われているほか、通信内容を監視することになるため通信の秘密との関係、無関係なサイトまでブロックしてしまうような過剰なブロッキングによる表現の自由の侵害などの法的な問題も指摘されており、慎重な検討が求められる手法と言える。

児童ポルノ対策作業部会では、こうした課題があることを踏まえ、インターネット上の児童ポルノ対策としてブロッキングについて検討しているところであるが、その際には、設備負荷や実効性などの技術的課題のほかコスト負担等の面から、現実にいかなる手法であれば我が国の ISP において採用の可能性があるかにつき検討することが不可欠である。そこで、本サブワーキングでは、さしあたり法的課題は度外視し、専ら技術的・コスト的な観点から、実施可能性及び実効性のある手法は何なのか、また、仮に実施するとした際に条件を付すべき必要があるか否か等につき検討することを目的とするものである。

第2　ブロッキングの各手法について

ブロッキングを行うためには、通信の内容のある部分に注目することでブロッキングの可否を判断することが必要となるが、通信パケットのどの部分を識別して、どの装置でブロッキングを行うか等によりいくつかの手法が考えられる。具体的には、①DNS により、ホスト名あるいはドメイン名を IP アドレスに変換する際にブロッキングを行う「DNSポイズニング方式」、②本通信の際にIPヘッダ内の宛て先IPアドレスもしくは HTTP コンテンツ部に含まれるアクセス先URL情報を元にブロッキングを行う「パケットフィルタリング方式」、③HTTPプロキシによりHTTP通信を一旦終端した上でアクセス先URL情報を元にブロックを行う「プロキシ方式」、④これらの方式の組み合わせによりブロックを行う「ハイブリッドフィルタリング方式」の4つの手法に分類することができる（4つの手法の概略図を別紙に記載）。以下、これら4つの手法それぞれについて具体的な説明を行う。

---

[1] 電気通信関連４団体（(社) 電気通信事業者協会、(社) テレコムサービス協会、(社) 日本インターネットプロバイダー協会、(社) 日本ケーブルテレビ連盟）が、平成 20 年 12 月に制定した「インターネット上の違法な情報への対応に関するガイドライン」である。本違法情報ガイドラインは、
（http://www.telesa.or.jp/consortium/illegal_info/pdf/20100115guideline.pdf）に掲載されている。

[2]電気通信関連４団体（(社) 電気通信事業者協会、(社) テレコムサービス協会、(社) 日本インターネットプロバイダー協会、(社) 日本ケーブルテレビ連盟）が、平成 18 年 11 月に制定した「違法・有害情報への対応等に関する契約約款モデル条項」である。本契約約款モデル条項は、
（http://www.telesa.or.jp/consortium/illegal_info/pdf/20100115model.pdf）に掲載されている。

1. DNS ポイズニング方式

DNS ポイズニング方式は、通信の際に行う DNS への名前解決要求に対して、該当のドメインあるいはホスト名が児童ポルノ掲載サイトアドレスリストに存在する場合においては実際の名前解決結果のIPアドレスを端末側に応答するのではなく、児童ポルノ掲載サイトへ通信しようとしていることを警告するサイトのIPアドレスを応答することで、利用者が児童ポルノ掲載サイトを閲覧することをブロックする方式である。ISPは自社のキャッシュ DNS に児童ポルノ掲載サイトアドレスリストの情報を記述することで、児童ポルノ掲載サイトへの通信をブロックすることが可能になる。既存の DNS への記述追加で対応可能であるためISPにとっては投資負担も少なく、導入障壁は低いものと考えられる。児童ポルノサイトへのブロッキングを行っている海外の国ではこの方式で行われている場合が多く、イタリア、ノルウェー、スウェーデン、フィンランド、オランダ、デンマーク、等で本方式が利用されている。

ただし、本方式は DNS を利用する方式であるため、DNS を利用しない通信、例えばIPアドレスをブラウザに直打ちすることによる閲覧行為や、ブロッキング対策を行っていない他者のキャッシュ DNS を利用しての閲覧行為については効果がない。また、該当のドメイン名あるいはホスト名に属するコンテンツ全体がブロッキング対象となるため、一部の児童ポルノ掲載サイトのために児童ポルノと無関係なサイトについてもブロッキングされて閲覧できないオーバーブロッキングが発生するという問題もある。

2. パケットフィルタリング方式

パケットフィルタリング方式は、通信パケットに含まれる宛先IPアドレスもしくは HTTP コンテンツ部に含まれる URL 情報に基づいて通信をブロッキングする方式である。前者は ISP が所有する既存のルータ機器等にアクセスリストを記述することによりブロッキングを実現するものであり、後者は HTTP コンテンツ部分まで認識可能な DPI(Deep Packet Inspection)装置等を利用してブロッキングを行うものである。

ルータ機器等による IP アドレスベースでのブロッキングを行う場合は、児童ポルノ掲載サイトアドレスリストの該当コンテンツが存在するサーバ等の IP アドレスをアクセスリストに記述することでブロッキングを行う。この場合、ISPネットワーク内の利用者に近いエッジルータにてブロッキングを行う場合には、規模の大きなISPでは大量のルータ機器への設定が必要になるため、リスト更新が運用上難しくなることが想定される。外部のネットワークと接続する部分においてアクセスリストの設定を行うこともできるが、この場合は ISP のバックボーンでの設定作業となるためミスオペレーションした場合のサービス停止による影響ユーザ数が大きくなるため、これについても運用上課題になることが想定される。また、DPI装置を利用する場合は、児童ポルノ掲載サイトアドレスリストをそのまま URL 単位でブロック可能とできるため実行上は非常に有効であるが、新規に DPI 装置を導入するには莫大な投資が必要となることが想定される。

IPアドレスベースでのブロッキングの場合は、DNSポイズニング方式であったIPアドレス直打ちによる閲覧行為も含めてブロッキング対象に含めることが可能となるが、DNS ポイズニング方式と同様に児童ポルノ掲載サイトが含まれるサイト全体への閲覧がブロックされてしまうため、同一サイト内にある児童ポルノと無関係なサイトについても閲覧できないオーバーブロッキングの問題が発生する。

3. プロキシ方式

プロキシ方式は、全ての通信をHTTPプロキシ経由で行わせることで、該当のHTTPプロキシにて通信の宛先となるURL情報を児童ポルノ掲載サイトアドレスリストと突合することで児童ポルノ掲載サイトへの通信をブロッキングする方式である。この方式では、URL単位でのブロッキングが可能となるため、ブロッキングを行いたいページあるいは画像のみをファイル単位でブロックすることが可能となる。ブラウザのHTTPプロキシ設定を利用者に委ねると実効性が限定されることから、利用者の意思にかかわらず通信全体をHTTPプロキシ経由にすることで実効性をあげる必要がある。そのためには、HTTPによる通信をL7スイッチ等によりHTTPプロキシにリダイレクトしたり、経路制御により全通信をHTTPプロキシ経由で通信させたりすることで、透過型のHTTPプロキシとして運用する必要がある。

本方式では、透過型プロキシとして必要となるL7スイッチや全てのHTTP通信をプロキシさせることを可能とするプロキシサーバが必要となるが、これらの導入には大規模な投資が必要となることが想定される。

児童ポルノ掲載サイトアドレスリストの管理については、HTTPプロキシにおいてウィルスチェックやURLフィルタ等のサービス実装は一般的に行われていることから、運用上は比較的容易な対応が可能だと思われる。

4. ハイブリッドフィルタリング方式

上記1から3の方式を見た場合、ブロッキングの精度はIPアドレス単位よりはURL単位の方が精度が高いブロッキングが可能である反面、URL単位での実装は比較的大規模な投資を必要とすることがわかる。これらの方式を組み合わせることで、URL単位で精度が高く、かつ、投資を抑えようという方式がハイブリッドフィルタリング方式である。プロキシ方式では全通信を処理するためのプロキシサーバを必要としたが、児童ポルノ掲載サイトへの疑わしい通信のみHTTPプロキシ経由とすることで投資を抑えてURL単位でのブロッキングを可能とすることを意図している。

主なハイブリッドフィルタリング方式は、経路制御によりIPアドレスベースで疑わしい IP アドレスへの通信のみをHTTPプロキシ経由とする方式とDNSにより疑わしいドメイン向けの名前解決をHTTPプロキシのIPアドレスで応答することでHTTPプロキシ経由とする方式の2つがある。前者は、イギリスのブリティッシュテレコム(BT)において行われており、CleanFeed という名前で有名である。また、後者はオーストラリアで実証実験ベースでの確認が行われている。

以上、1から4までの方式の解説を行ったが、それらを方式の選択は各ISPの設備・ネットワーク構成や運用方法等の状況により評価が変わってくることが想定される。そのため、これら各方式に対して広くISPに対して意見を募り、現実的な問題点・課題をさらに掘り下げていくことが必要となる。

第3 ISP アンケート結果

1. 調査目的

既に述べたとおり、ブロッキングの各手法については、児童ポルノ画像の閲覧防止という観点から、実施の精度やコスト、リストの運用性など様々な特徴が指摘されており、各国の市場環境や事業状況等に応じて適切な手法が採用されている状況にある。

我が国においても、諸外国と同様、ISP 等の民間事業者が法令を遵守しつつ自主的取組として行うことが想定されている以上、ブロッキングの実施に向けた検討を進めるに当たっても、実際の担い手である事業者が必要な情報を十分に得た上で、事業環境等を踏まえた実際的な検討を進めていくことが望ましい。すなわち、各手法の技術的特徴を踏まえた上で、対策の実効性と実施費用・期間等に基づく費用対効果を適切に把握し、ブロッキング実施に際して参照可能な情報として蓄積していくことが求められている。

以下、本項は、我が国の電気通信市場の環境や技術的動向に関して知見を有するISP76 社に対して実施したアンケートの結果に基づき、手法別に有効性と課題を整理したものである。調査に当たっては、法的課題はいったん考慮しないこととした上で、ブロッキングの対象となるサイトは数千程度との前提で行われたものであり、主として技術的知見に立脚した回答となっている点に留意が必要である。今後、ブロッキングの担い手となる可能性のある各事業者が、それぞれの事情に応じて採用すべき手法に関して行う判断に資するよう、本とりまとめが、法的課題の整理や諸外国の状況に関する記述とともに、関係機関を通じて広く周知されることを期待するものである。

2. 調査結果

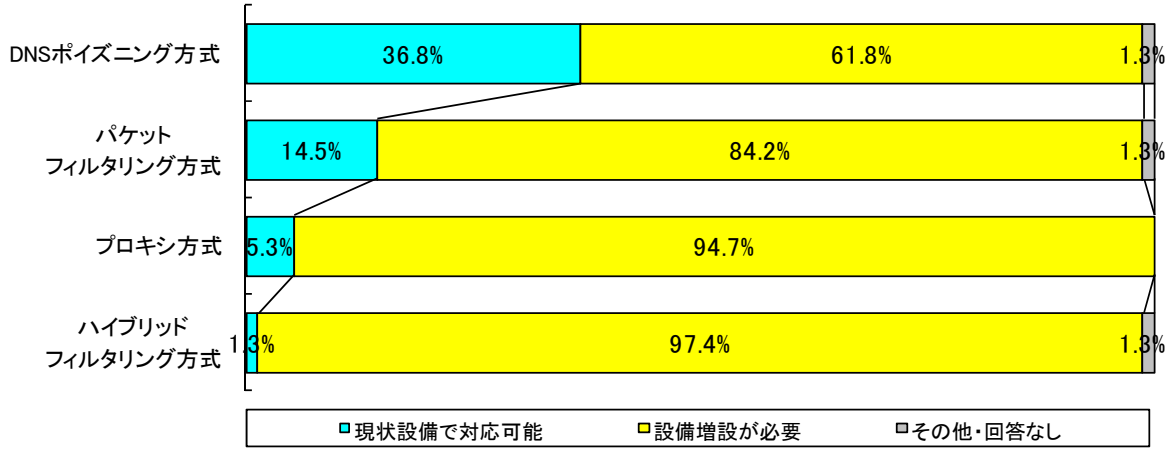
国内 ISP76 社に対して実施したアンケートの概要

- **ブロッキング対象として、HTTP ベースのアクセスに限定して検討**
- **手法として、①DNS ポイズニング方式、②パケットフィルタリング方式、③プロキシ方式、④ハイブリッドフィルタリング方式、の4手法に分類し、項目毎に回答を集計**

（１）　設備投資の必要性

【グラフ・表　01】設備投資の必要性（手法別）

現状の通信品質を維持する事を前提として、各手法に関して設備増強の要否を選択下さい。



手法別に見ると、DNS ポイズニングにつき現状設備で対応可能との回答（36．8%、76社中28社）が比較的多かったのに比べ、その他手法については、パケットフィルタリング方式が14．5%、プロキシ方式が5．3%、ハイブリッドフィルタリング方式が1．3%と軒並み低くなっていることから、DNS ポイズニング方式は設備投資を比較的要しない手法と考えられていることがわかる。

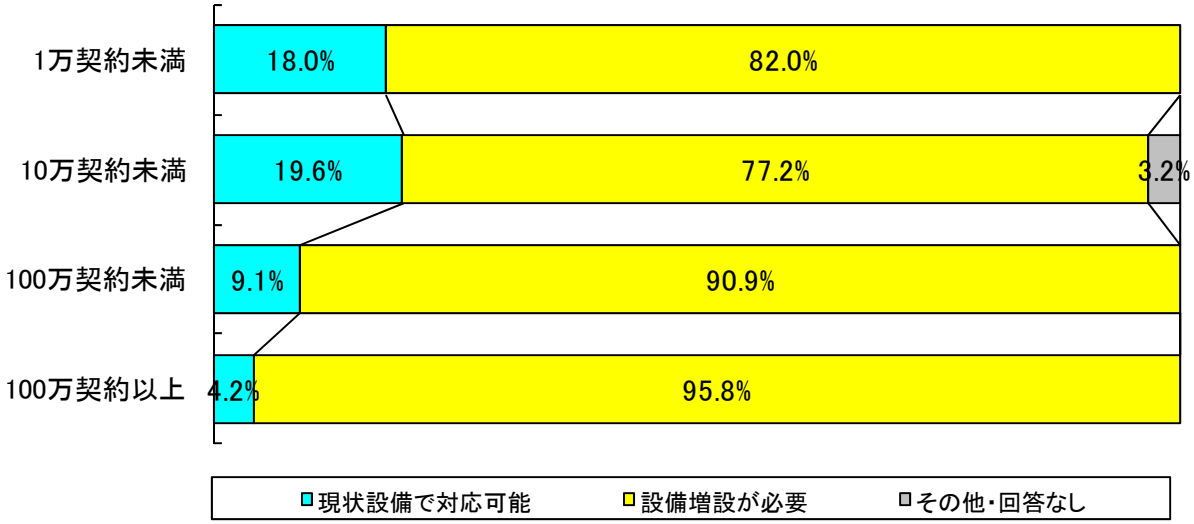
【グラフ・表　02】設備投資の必要性（ＩＳＰ規模別）

DNSポイズニング方式				
回答＼ISP規模	1万契約未満	10万契約未満	100万契約未満	100万契約以上
現状設備で対応可能	44.0%	47.8%	27.3%	8.3%
設備増設が必要	56.0%	47.8%	72.7%	91.7%
その他・回答なし	0.0%	4.3%	0.0%	0.0%
パケットフィルタリング方式				
回答＼ISP規模	1万契約未満	10万契約未満	100万契約未満	100万契約以上
現状設備で対応可能	12.0%	26.1%	9.1%	8.3%
設備増設が必要	88.0%	69.6%	90.9%	91.7%
その他・回答なし	0.0%	0.0%	0.0%	0.0%
プロキシ方式				
回答＼ISP規模	1万契約未満	10万契約未満	100万契約未満	100万契約以上
現状設備で対応可能	12.0%	4.3%	0.0%	0.0%
設備増設が必要	88.0%	95.7%	100.0%	100.0%
その他・回答なし	0.0%	0.0%	0.0%	0.0%
ハイブリッドフィルタリング方式				
回答＼ISP規模	1万契約未満	10万契約未満	100万契約未満	100万契約以上
現状設備で対応可能	4.0%	0.0%	0.0%	0.0%
設備増設が必要	96.0%	95.7%	100.0%	100.0%
その他・回答なし	0.0%	4.3%	0.0%	0.0%

他方、事業規模別の内訳を見ると、DNS ポイズニング方式についても、1 万契約未満の ISP では現状設備で対応可能との回答（44．0%）と設備増設が必要との回答（56．0%）が拮抗しており、10万契約未満に広げても同様（増設不要と増設必要の回答数が同数）であるのに対し、契約数が増えるほど設備増設が必要と考える比率が上昇している。また、その他の手法についても、契約数と設備増設の必要性については基本的には同様の傾向が見られる。

このことから、手法別に見れば、DNS ポイズニング方式が最も設備投資負担の少ない形で導入可能なものであると言えるが、中小の ISP であれば追加的な設備投資は不要であるケースもあるものの、事業規模が拡大するにつれて一定の負担を伴うと考えられていることがわかる。また、その他の手法についても、事業規模に比例して負担が拡大するとの回答傾向が見られる。

【グラフ・表　03】設備投資の必要性（ＩＳＰ規模別）



また、手法の如何を問わず、事業規模別に設備投資負担に対する考え方を見ると、1万契約未満のISP では現状設備で対応可能との回答が全体の18．0%、10万未満契約で19．6%と比較的高いのに対して、100万未満契約では9．1%、100万以上契約では4．2%と低下していく傾向にあり、一般的に、大規模事業者ほど設備投資負担に対して厳しい見方をしていることがわかる。

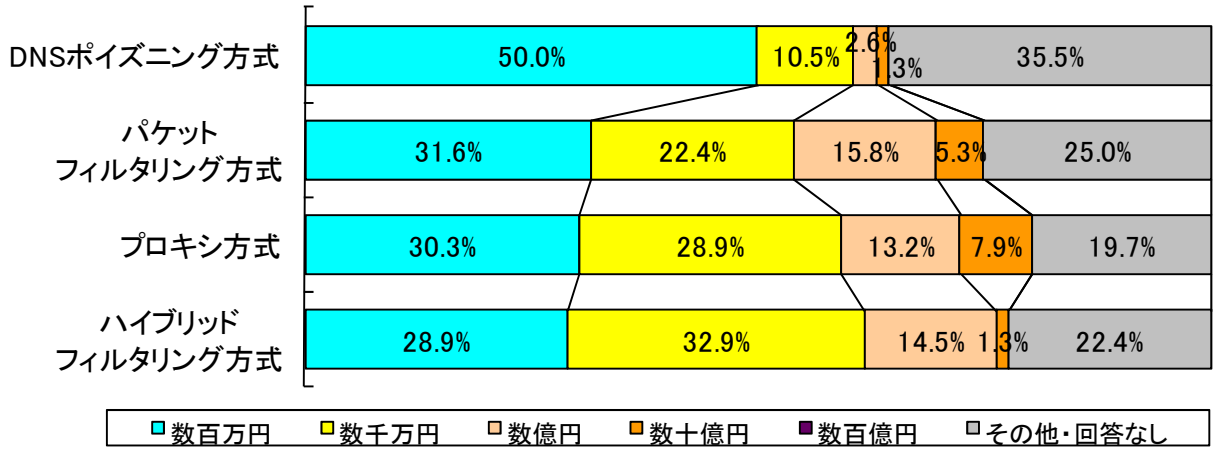
これは、契約者が増えれば増えるほど、処理トラヒックの増大によるサーバ設置やネットワーク増強、ブロッキング対象契約者の増加による顧客サポート体制の充実等により、追加的な負担が求められる蓋然性が高まることがその一因であるとも考えられる。

（２）　コストの試算

具体的なコストについて、初期コスト（サーバ設置等）、ランニングコスト（メンテナンス等）、サポートコスト（顧客相談対応等）に分けて、手法毎の試算を集計したものである。

【グラフ・表　04】初期導入費用想定（手法別）

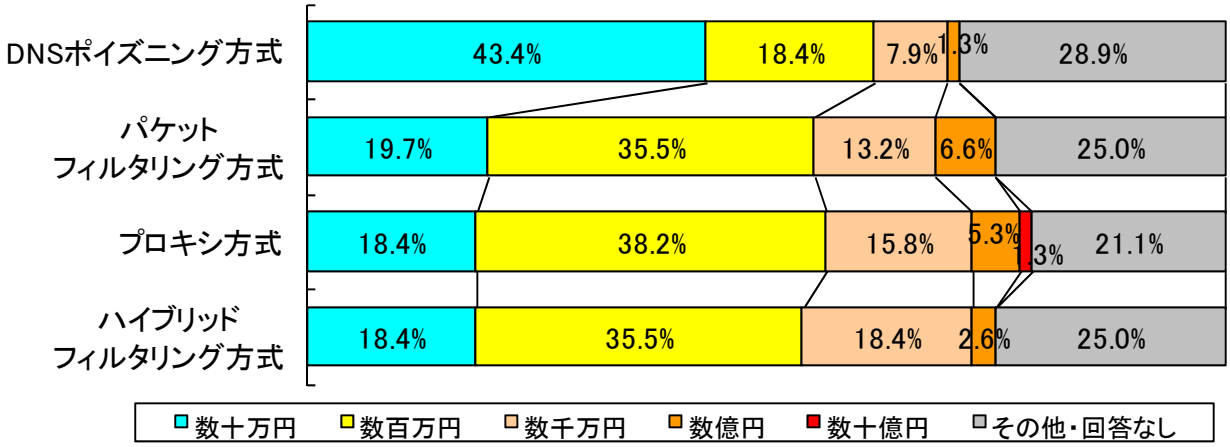
各手法を御社で導入する場合、費用について、【イニシャル（初期導入費用）・ランニング（年間維持管理費用）・顧客サポート（年間対応費用）】それぞれどの程度と想定されますか？
※手法①・④については、通信エラーのみ発生させ、警告ページへの遷移は無いものと仮定して下さい。



DNS ポイズニング方式では、初期投資につき、数百万円以内との回答が50．0%、数千万円台を合わせると60．5%となる一方、数億円では2．6%、数十億円では1．3%となっており、多くの ISP が1億円以内で開始可能と考えていることがわかる。他方、その他の方式については、例えば、パケットフィルタリング方式では、数百万円以内が31．6%、数千万円台を合わせると54．0%となる一方、数億円かかるとの回答（15．8%）と数十億円との回答（5．3%）も一定の割合を占めている等、総じて DNS ポイズニング方式に比べて、初期投資コストが1億円以上に膨らむ可能性を大きく見ていることが確認できるが、その他3方式の間で見積もり額の分布に大きな差があるわけではなく、概ね半数程度の事業者が1億円以内で開始可能と考えている点も注目されよう。ただし、DNS ポイズニング方式についてみても、10万契約未満の ISP では1億円以上と見積もる事業者がいないのに対して、100万契約未満では9．1%、100万契約以上では16．7%となる等、事業規模に応じてコストが高く見積もられる傾向にある。

【グラフ・表　05】ランニング費用想定（手法別）

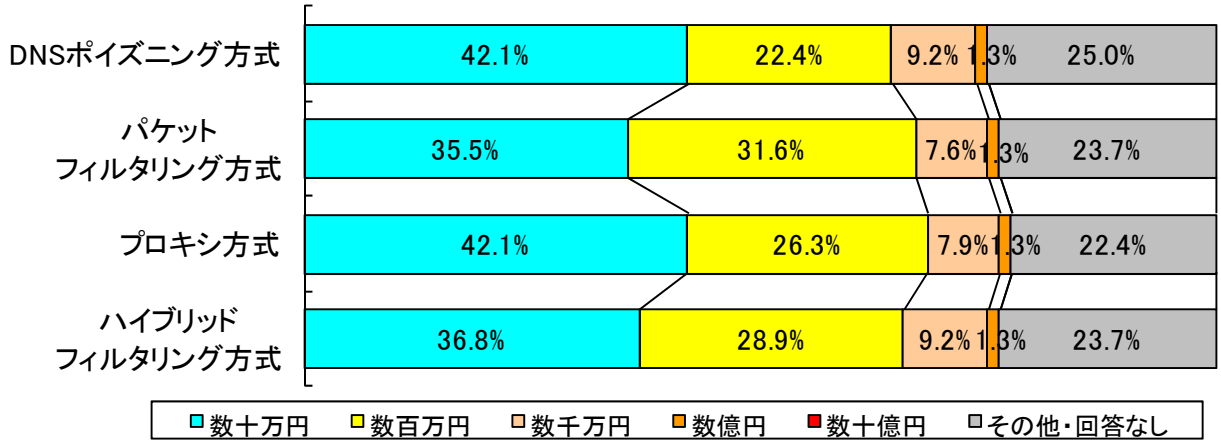
各手法を御社で導入する場合、費用について、【イニシャル（初期導入費用）・ランニング（年間維持管理費用）・顧客サポート（年間対応費用）】それぞれどの程度と想定されますか？
※手法①・④については、通信エラーのみ発生させ、警告ページへの遷移は無いものと仮定して下さい。



次に、ランニングコストについては、DNS ポイズニング方式は数十万円以内との回答が43．4%、数百万円以内に広げると61．8%、数千万円台を合わせると69．7%となる一方、数億円では1．3%、数十億円では0%となっており、初期投資と同様に毎年1億円以内の支出で運用可能と考えられているが、その他の方式について数千万以内と回答した比率を見ても、パケットフィルタリング方式で68．4%、プロキシ方式及びハイブリッドフィルタリング方式で72．4%となっており、総体的には、ランニングコストについて方式間で大きな差が認められない結果となっている。ただし、ルータ等による経路制御を用いるパケットフィルタリング方式については、リスト運用負荷が高くなると指摘されているところであり、他方式に比べて1億円以上のコストを見込んでいるISPの比率が大きくなっている。DNSポイズニング方式については、他方式に比べ、数十万円で運用可能との回答率が大きくなっており、設定箇所が少なく運用が比較的容易と考えられていることを裏付ける結果となっている。他方、事業規模別に見ると、各方式について規模の拡大に応じてコスト見積もりが増大する傾向が見られ、1万契約から100万契約の ISP のうち概ね7～8割は数千万円以内で運用可能と回答しているのに対し、100万契約を超える ISP になると5割未満に低下している。これは、ランニングコストは、リストの運用と機材の保守・点検等に要する費用から構成されるため、トラヒックの増大により製品に対する負荷が高まるにつれてコストが増えると想定されていることが原因と考えられる。

【グラフ・表　06】サポート費用想定（手法別）

各手法を御社で導入する場合、費用について、【イニシャル（初期導入費用）・ランニング（年間維持管理費用）・顧客サポート（年間対応費用）】それぞれどの程度と想定されますか？
※手法①・④については、通信エラーのみ発生させ、警告ページへの遷移は無いものと仮定して下さい。



さらに、サポートコストについても、①方式間で有意の差が見られない点、②数億円台との回答率が各方式とも1．3%に留まるなど比較的廉価に対応可能と考えられている点はランニングコストの回答結果と同様である。加えて、ランニングコストの場合とは異なり、10万円以内で対応可能との回答率にも方式間で有意の差が見られない点が注目されるが、これは DNS ポイズニング方式の場合にはドメイン単位のブロッキングとなるためオーバーブロッキングの可能性が他方式に比べて高く、より丁寧なサポート体制の構築が求められると考えられていることも原因の一つと考えられる。他方、事業規模に比例して対応コストが増大する傾向は、ランニングコストにおける場合と同様に観察され、1万契約から100万契約の ISP のうち概ね7～9割は数千万円以内で対応可能としているのに対し、100万契約を超える ISP では6割前後となっている。これは、契約者数が多いほど、ブロッキングの実施自体に対する問い合わせやオ

ーバーブロッキング時の苦情対応等が比例的に増えると考えられていることが原因と思われる。

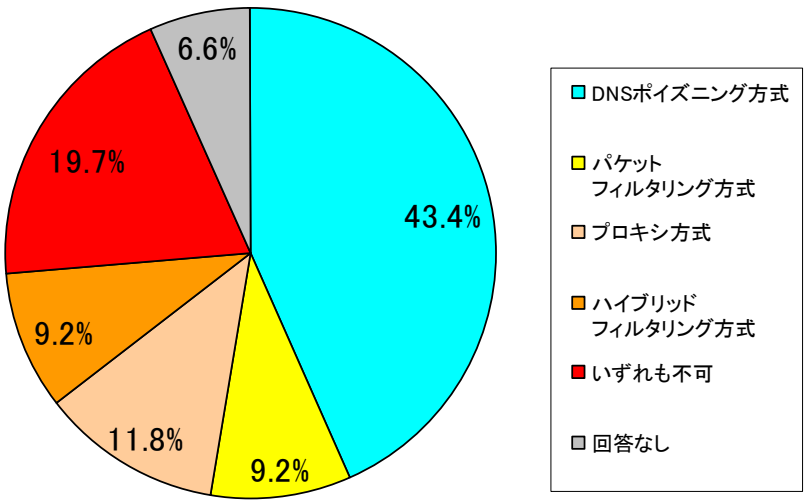
こうした調査結果から、初期投資コストについては、DNS ポイズニング方式が他に比べて優位と考えられているものの、運用の複雑性に照らして特に負担が大きいと指摘されることの多いハイブリッドフィルタリング方式が特筆して高コストと考えられているわけではない点にも留意する必要がある。また、ランニングコストとサポートコストについては、経路制御時の運用の複雑化やDNSポイズニング方式におけるオーバーブロッキング対応の増加等の事情がコスト試算に一部反映されていると考えられるものの、必ずしも方式の違いによって大きな差が生じているというわけではない。

従って、方式別に見れば、DNS ポイズニング方式が初期投資、ランニング、サポートを合わせた全体として最も低廉に導入可能な手法である一方、パケットフィルタリング方式及びプロキシ方式は初期投資コストを中心に総体的にコストが高くなり、ハイブリッドフィルタリング方式についてもDNS ポイズニング方式よりは高くなると考えられている。しかしながら、いずれの方式であったとしても、コストの実質的な多寡を左右するのは事業規模による差であるが、中小規模事業者においても相当な費用がかかると想定する事業者が一定規模存在することから、今後、ブロッキングの実施に向けた検討を行っていくに際しては、中小事業者への配慮が不可欠である。

なお、ISP からの個別意見として、リストの規模や更新等の運用に関する責任の在り方、具体的な機器・ソフトウェアの製品価格等の事情によりコストは大きく変わりうるため、現時点でのコスト算定が困難であるとの指摘が複数寄せられているところであり、本調査結果で得られた全体傾向を踏まえた上で、技術的動向の把握やコスト分析を一層深めていく必要がある。

（３） 採用可能な手法

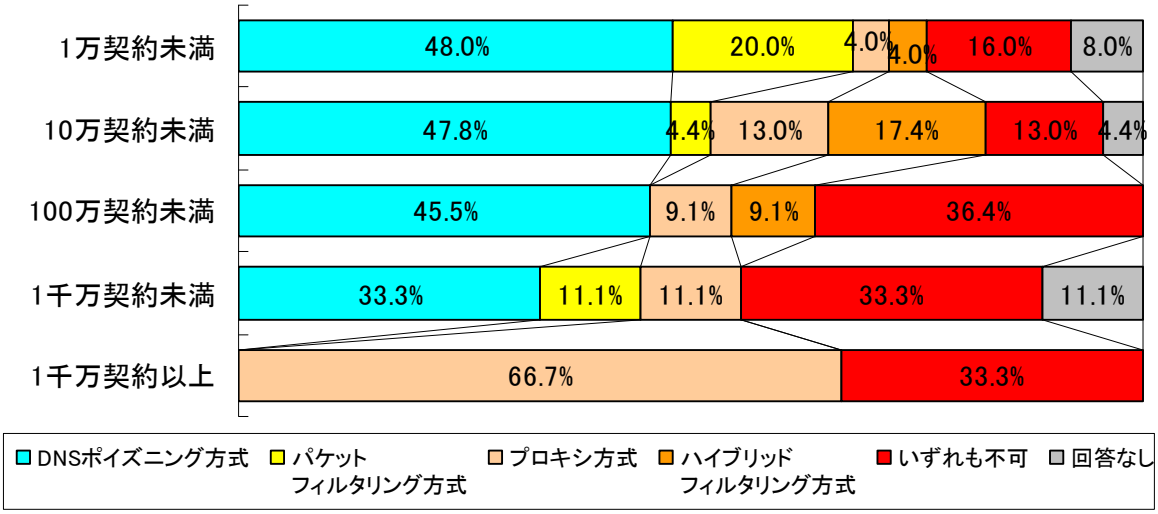
【グラフ・表　07】採用可能な手法
仮に導入を求められた場合、御社で導入する手法を一つ選択するとすればどれですか？



仮にブロッキングの導入を求められた場合にどの手法を選択するかという問いに対する回答にも、方式や事業規模に応じた一定の傾向が見られる。方式別に見ると、DNS ポイズニング方式が43．4%と最も多く、その他の方式については、パケットフィルタリング方式（9．2%）、プロキシ方式（11．8%）、ハイ

ブリッドフィルタリング方式（9．2%）となっているが、いずれの方式も導入できないとの回答も19．7%と多かった点については、更なる調査・分析が求められるといえよう。

【グラフ・表　08】採用可能な手法（ＩＳＰ規模別）



事業規模による導入手法の違いを見ると、DNS ポイズニング方式が最も差が大きく、その他の方式（いずれも不可を含む）については大きな差が生じていない。具体的には、1万契約未満の ISP では DNS ポイズニング方式との回答が48．0%、パケットフィルタリング方式が20．0%となっているが、他の2方式については4．0%ずつと低くなっている。10万契約未満の ISP についても、DNS ポイズニング方式が47．8%と最大になっている一方、その他の手法については、パケットフィルタリング方式が減少して4．4%となっている反面、プロキシ方式が13．0%、ハイブリッドフィルタリング方式が17．4%と増加している。以降、事業規模の大きい ISP ほど、DNS ポイズニング方式の回答率が減少していくものの選択肢のなかでは最大であり続ける一方、その他方式については事業規模との関係で必ずしも一定の傾向が見られるわけではなく、むしろ大手になればなるほど、いずれも不可との回答率が高くなっている（1万契約未満では16．0%だが、100万契約以上では33．3%に上昇）。

こうした調査結果を踏まえると、①DNS ポイズニング方式を導入するとの回答率が事業規模の拡大に伴って減少していること等から、中小事業者が DNS ポイズニング方式を選択する原因の一つが廉価性と考えられ、また、②ハイブリッドフィルタリング方式よりも高コストのパケットフィルタリング方式が小規模事業者によって選好されていること、いずれも不可との回答率が事業規模の拡大に比例して高まっていること等から、DNS ポイズニング方式以外の方式についてブロッキングを実施するかどうかの判断に当たっては、コスト以外の要因が考慮されていると考えられる。

それぞれの方式について採用可能と回答した理由を見ると、コスト負担の程度や運用上の手間、利用者の利便性への影響、検知精度の問題（オーバーブロッキングの懸念）等が指摘されているが、とりわけ実効性について、DNSポイズニング方式については、DNSSEC[3]の導入が本格的に検討されていること、

[3] DNS サーバから送られてくる IP アドレスとホスト名の対応関係の信頼性を証明するセキュリティ機能であり、実装に

IPアドレスの直接入力等により簡単に回避可能であること等に基づく疑問が多く寄せられている点に注意を要する。

（４） 実施までに要する期間

【グラフ・表　09】実施までに要する期間（手法別）
（前設問にて）お伺いした導入可能な手法について、導入までに必要な時間はいかほどですか？

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ポイズニング方式	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

実施までに要する期間については、各方式についての回答の平均値を比較すると、DNS ポイズニング方式は8．2ヶ月、パケットフィルタリング方式は12．3ヶ月、プロキシ方式は13．4ヶ月、ハイブリッドフィルタリング方式は12．7ヶ月となっており、DNS ポイズニング方式が最も短期間で実施可能な手法であり、プロキシ方式が最も長期間を要する手法と考えられている。同様の傾向は、各事業規模の ISP につき共通して見られるところであるが、これは追加的な設備投資を要する手法であればあるほど予算計画の策定や社内決裁に期間を要すること、運用が複雑な手法であればあるほど運用管理の教育に期間を要すること等を背景としているものと考えられる。いずれの手法についても、顧客への事前の周知期間を十分に設けることが必要であるとの指摘が該当するものと考えられる。

向けて本格的な検討が進行中。DNSSEC が完全実装されれば、DNS ポイズニング方式が依拠する名前解決システムを利用したサイトへの誘導行為そのものが行えなくなる。

【グラフ・表　10】実施までに要する期間（ＩＳＰ規模別）

DNSポイズニング方式						
ISP規模＼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）
1万契約未満	36.0%	24.0%	16.0%	0.0%	24.0%	5.8
10万契約未満	17.4%	21.7%	34.8%	4.3%	21.7%	9.0
100万契約未満	0.0%	36.4%	36.4%	0.0%	27.3%	9.0
100万契約以上	8.3%	8.3%	33.3%	8.3%	41.7%	11.6
パケットフィルタリング方式						
ISP規模＼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）
1万契約未満	12.0%	16.0%	24.0%	0.0%	48.0%	8.1
10万契約未満	8.7%	8.7%	30.4%	21.7%	30.4%	13.9
100万契約未満	0.0%	9.1%	45.5%	9.1%	36.4%	12.9
100万契約以上	8.3%	0.0%	8.3%	25.0%	58.3%	17.4
プロキシ方式						
ISP規模＼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）
1万契約未満	8.0%	24.0%	24.0%	0.0%	44.0%	8.1
10万契約未満	4.3%	8.7%	34.8%	21.7%	30.4%	14.4
100万契約未満	0.0%	9.1%	36.4%	18.2%	36.4%	14.6
100万契約以上	0.0%	0.0%	16.7%	41.7%	41.7%	20.6
ハイブリッドフィルタリング方式						
ISP規模＼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）
1万契約未満	0.0%	28.0%	24.0%	4.0%	44.0%	9.9
10万契約未満	8.7%	8.7%	26.1%	21.7%	34.8%	14.0
100万契約未満	0.0%	9.1%	45.5%	9.1%	36.4%	12.9
100万契約以上	0.0%	0.0%	41.7%	16.7%	41.7%	15.4

事業規模別に詳細に見ると、DNS ポイズニング方式では、1万契約未満の ISP では3ヶ月程度との回答が36．0%であり最長でも1年程度で導入可能と回答しているのに対し、10万契約未満では半年～1年程度との回答が半数以上を占める一方で、2年程度との回答もあった。平均所要期間で見ると、1万契約未満が5．8ヶ月、10万契約未満が9．0ヶ月、100万契約未満が9．0ヶ月、100万契約以上が11．6ヶ月となっており、総体的には規模と比例して期間が伸びる傾向がある。こうした傾向は、他の手法についても共通して見られるところである。

こうした調査結果から、実施に要する期間については、小規模 ISP ほど、既存の設備で対応可能であること、多大な顧客対応・サポート教育等を要しないこと等の事情から短く見積もっていることが見て取れる。このことから、より多くの準備を要する大手事業者に対する配慮が求められるといえよう。

（５）　各手法に対する個別の指摘など

DNS ポイズニング方式の場合、コストや設備の面で最も容易に導入可能とする ISP が多いが、共用サービスにおいて一部のページがブロッキング対象となった場合、他の正常なページもブロッキングされるという、いわゆるオーバーブロッキング問題の発生とこれに起因する顧客対応やクレーム対応の負担の増加に対する懸念も多く示されている。さらに、IP アドレスの直接入力や，ユーザによる PC の設定変更により海外など他の DNS サーバを指定するなどの方法によりブロッキングを回避可能であるとの指摘も多い。ただし、他の手法のコスト負担や設備負荷との兼ね合いから、本手法以外に現実的な選択肢はないという意見も少なくないところである。

パケットフィルタリング方式の場合、まずルータでの経路制御により IP 単位でブロッキングする場合には、ルータの過負荷による処理能力の低下などの問題や、DNS ポイズニング方式と同様に、共有型 Web など同一 IP アドレスに収容されている Webサイトの閲覧ができなくなる、IP アドレスを共有する HTTP 以外のサービスについてのアクセスもブロックされるなどオーバーブロッキングの問題が生じる。他方、DPI による URL 単位のブロッキングでは、コストの増大や設備障害による影響のおそれが指摘されている。いずれにせよ、設備の負荷の大きさと、それを回避する場合のコスト負担の増大がネックとなっており、本手法を選択肢とする ISP は多くない。非現実的とする ISP すら存在する。

プロキシ方式の場合、全 HTTP トラフィックをプロキシサーバで処理する必要があるため、プロキシサーバへの負荷が上昇し、レスポンス（通信速度）の低下など通信環境の悪化に対する懸念が多く示されている。他方、こうした問題を回避するためには大量のトラフィックを処理可能な高性能なプロキシが必要となるため、設備投資や維持費用の負担が障害となる。また、透過プロキシ経由の場合、株価などのリアルタイムで表示されることが重要なサイトで弊害が出る可能性があること、プロキシ経由でのアクセスを拒むサイトもあり、問題のないサイトへのアクセスができなくなるなどの問題が指摘されている。

ハイブリッドフィルタリング方式の場合、第一段階では、ルータによる経路制御による場合と DNS ポイズニング方式による場合とでそれぞれが持つ問題が基本的に当てはまるが、オーバーブロッキングなどの問題は一定程度解消されると認識されている。第 2 段階では、プロキシ方式の問題点が妥当するが、全トラフィックをプロキシサーバで処理するのではなく、疑わしいもののみを処理するため設備負荷やそれを回避するためのコストは、通常の方式よりも低廉にとどめることができ、負担の問題を部分的に解消可能である。そのため、現実的・実効的な手法と肯定的に評価する意見が複数寄せられているが、他方で、他の手法と比較して機構が複雑になることから、障害発生のリスクが高まること、社内に対応できる人材がいないこと等の指摘もある。

（６） 児童ポルノ掲載サイトアドレスリスト及びその管理団体への要望

多くの ISP が、リストの更新につき ISP が手動で行う仕組みでは対応が困難であり、例えば CSV ファイルで設置して ISP の特定の IP のみからアクセスできるようにするなど機械的・自動的に提供・更新されるシステムにする必要性を指摘している。また、①リストが漏洩した場合に備えて暗号化しておくこと，②ISP が採用するブロッキング手法にあわせたリストを提供すること，③追加、又は除外申請に応じて対応するだけでなく，リストの無意味な肥大化を防ぐために定期的に棚卸しをすること，④ISP が加入者から問い合わせを受けた場合の対応のために、ISP がリスト掲載・不掲載を確認できる専用のサイトを設けること，⑤ユーザは通信に異常が起きているとしか認識できない可能性が高いためブロッキングの告知等の対応をすること等の必要性も指摘されている。ブロッキングは、削除が困難なケースについてのみ実行すべきものとの理解を前提に、リストに登録するに当たっては、事前に当該ホスティング事業者への削除要請と対応のための一定の猶予期間を前置し，海外のサイトだけをリストアップするべきであるとの意見もみられた。

なお，リストの更新間隔については、24 時間程度で概ね適切と考えられているが、それでは遅いとの意見も散見される。

オーバーブロッキングへの対策として、除外申請に対する迅速な対応を求める意見は非常に多くみられた。具体的には、365 日 24 時間の対応を求めるもの、数時間以内の対応が必要とするものなどがある。

特に、DNS や IP 単位でのブロッキングではオーバーブロッキングの影響が大きくなりがちであることから、除外申請への即応性を求める声が強い。また，ブロッキングに関するユーザ等からの問い合わせや除外申請については，リスト掲載に関与していない ISP において対応することは困難であるため，リスト管理団体において一元的に対応してほしいという要望も多く出ている。

リスト管理団体そのものについても，その法的位置づけを明確にするとともに、正当性を社会に対して広く周知することが求められている。また，リスト掲載ないし除外の手続きに対する公平性や透明性の担保の要請も強く、中にはリストの公開を求める意見もあるが、それが困難であるとしてもリスト掲載基準や除外基準について明確化を求める指摘は多い。リスト管理団体につき，複数存在することが望ましいとする指摘もみられた。

（７） ブロッキング以外の効果的な児童ポルノ閲覧防止策

本作業部会では、主にブロッキングに関わる各種問題点を検討しているが、併せて、技術的・専門的な知見を有する ISP にブロッキング以外に効果的な児童ポルノ閲覧防止策があるかどうかという点についても調査対象としている。例えば、アンケートの中では，ユーザの PC 側でのフィルタリングソフトでの閲覧防止などクライアント側での対応、管理者への警告、広く普及しているブラウザに URL によるブロッキング機能を設ける、画像認識技術を用いて児童ポルノと思われるものは表示できない機能を OS に組み込む、検索サイト側で検索結果表示対象から除外する、サイバーパトロール、普及啓発活動や検挙の強化など様々な意見がみられた。これらの意見をみるに、単独で決定的な対策となり得る手法は存在しないが、ブロッキング以外で一定の有効性を持つと思われる対策が全く存在しないわけではない。なお，アンケートの結果によれば，ブラウザやウィルスチェックなどクライアント側での対応がもっとも現実的かつ効果的であるとの指摘が比較的多くみられる。

第４　総括　～我が国におけるブロッキング実施の技術的実現可能性とその課題～

今回のアンケート結果によれば、コスト面については、DNS ポイズニング方式が初期投資、ランニング、サポートを合わせた全体として最も低廉に導入可能な手法である一方、パケットフィルタリング方式及びプロキシ方式は初期投資コストを中心に総体的にコストが高くなり、ハイブリッドフィルタリング方式についてもDNSポイズニング方式よりは高くなると考えられている。そのため，中小ISPを中心として、DNSポイズニング方式を現実的な選択肢として挙げるところが多い。しかし、DNS ポイズニング方式はオーバーブロッキング問題に対する懸念もあり、児童ポルノ掲載サイトアドレスリストの作成段階においてホスト名もしくはドメイン単位でのリストを別に用意する等、本方式を利用することを想定した考慮がなされることが望ましいと考えられる。

各方式を比較する場合，コスト負担の程度や運用上の手間、利用者の利便性への影響、検知精度の問題（オーバーブロッキングの懸念）、実効性等の要素を考慮する必要があるが、コスト面と実効性のバランスの観点からは、ハイブリッドフィルタリング方式に一定の利点が認められている。

しかしながら、コスト負担や機構が複雑に成ることによる弊害等ハイブリッドフィルタリング方式にも課題がないわけではなく、特に設備コストについては、児童ポルノ掲載サイトアドレスリストの量や実際のブロッキング対象サイトへのトラヒック等に大きく影響されることから、今後は ISP における実際の利用者の利用

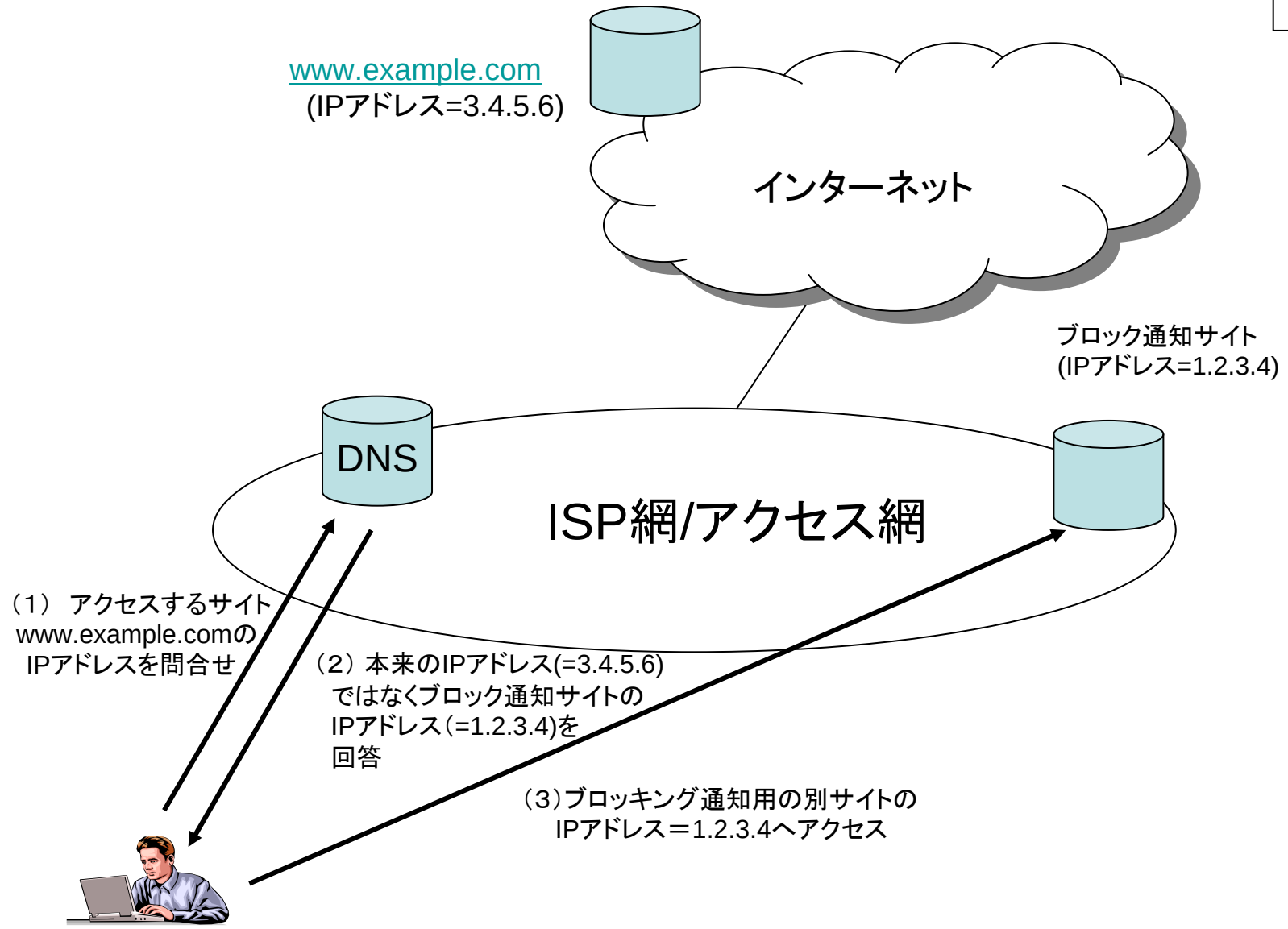
状況を想定した上でのコストや運用方法の検討の詳細化を行っていく必要がある。また、アドレスリスト管理団体との具体的なリストの受渡し方式、例えばファイル形式や受渡しプロトコル、更新頻度等についても、今後リスト管理団体と検討を詳細化していくことが必要である。それらの事項および今回 ISP から寄せられた意見も踏まえ、引き続き，ISP の事業規模等に配慮しつつ，適切な範囲・手法によるブロッキング実施の可能性につき検討することが必要である。

児童ポルノ作業部会 ISP 技術者サブワーキング　構成員

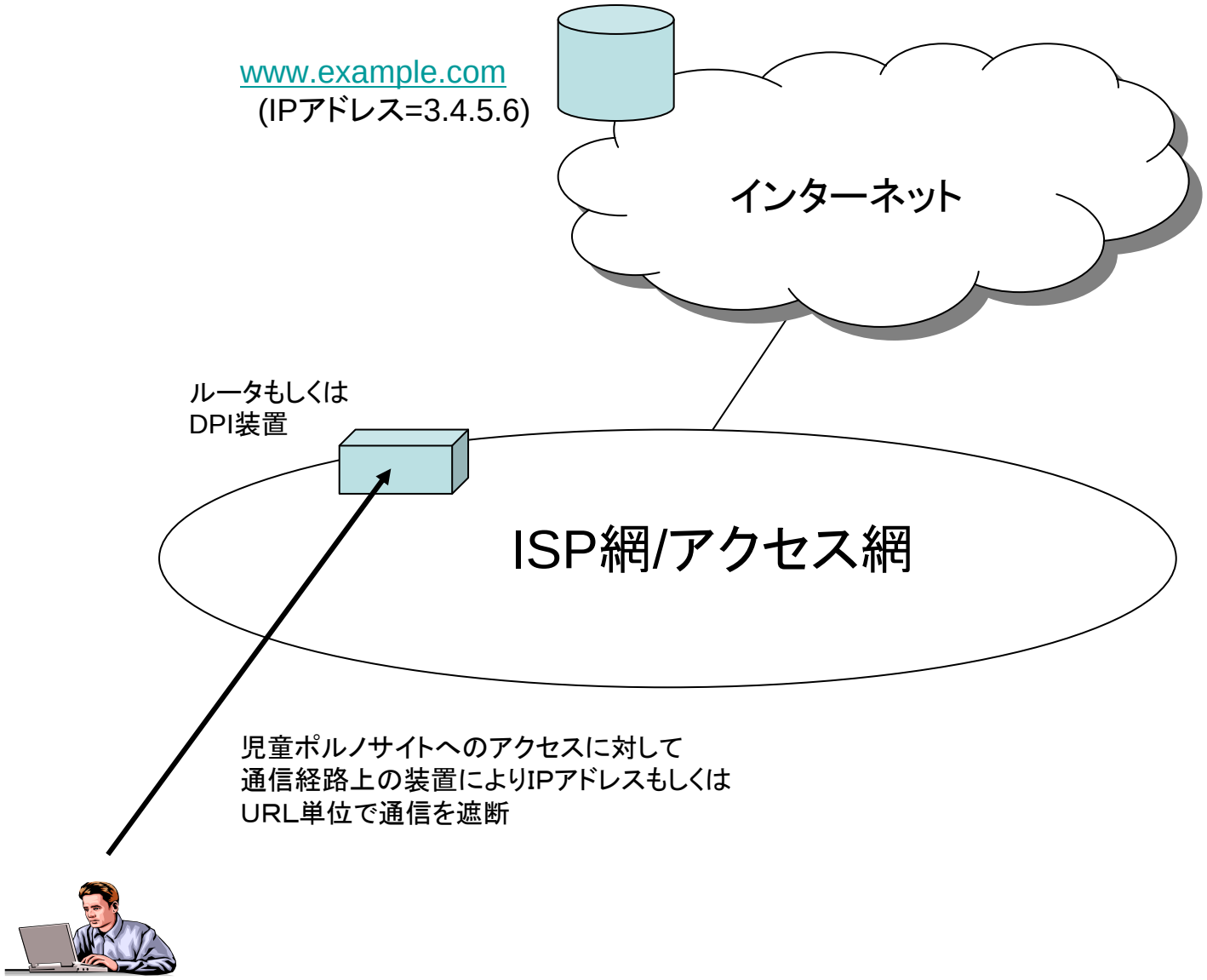
リーダー	北村 和広	NTTコミュニケーションズ株式会社　グローバル事業本部　担当部長
構成員	岸川徳幸	NEC ビッグローブ株式会社 基盤システム本部 統括マネージャー
	持麾　裕之	NECビッグローブ株式会社　経営企画本部 調査シニアエキスパート
	山崎　文生	ソネットエンタテインメント株式会社 システム技術部門プラットフォーム部 IT インフラ課
	柳舘　一彦	ニフティ株式会社 CSビジネス部 部長
	松本　修	KDDI 株式会社 au one プラットフォーム開発部
	立石 聡明	社団法人日本インターネットプロバイダー協会 副会長
	明神　浩	社団法人テレコムサービス協会　企画部長
	林 英雄	社団法人日本ケーブルテレビ連盟　第三業務部　部長

（手法1：DNSポイズニング方式）

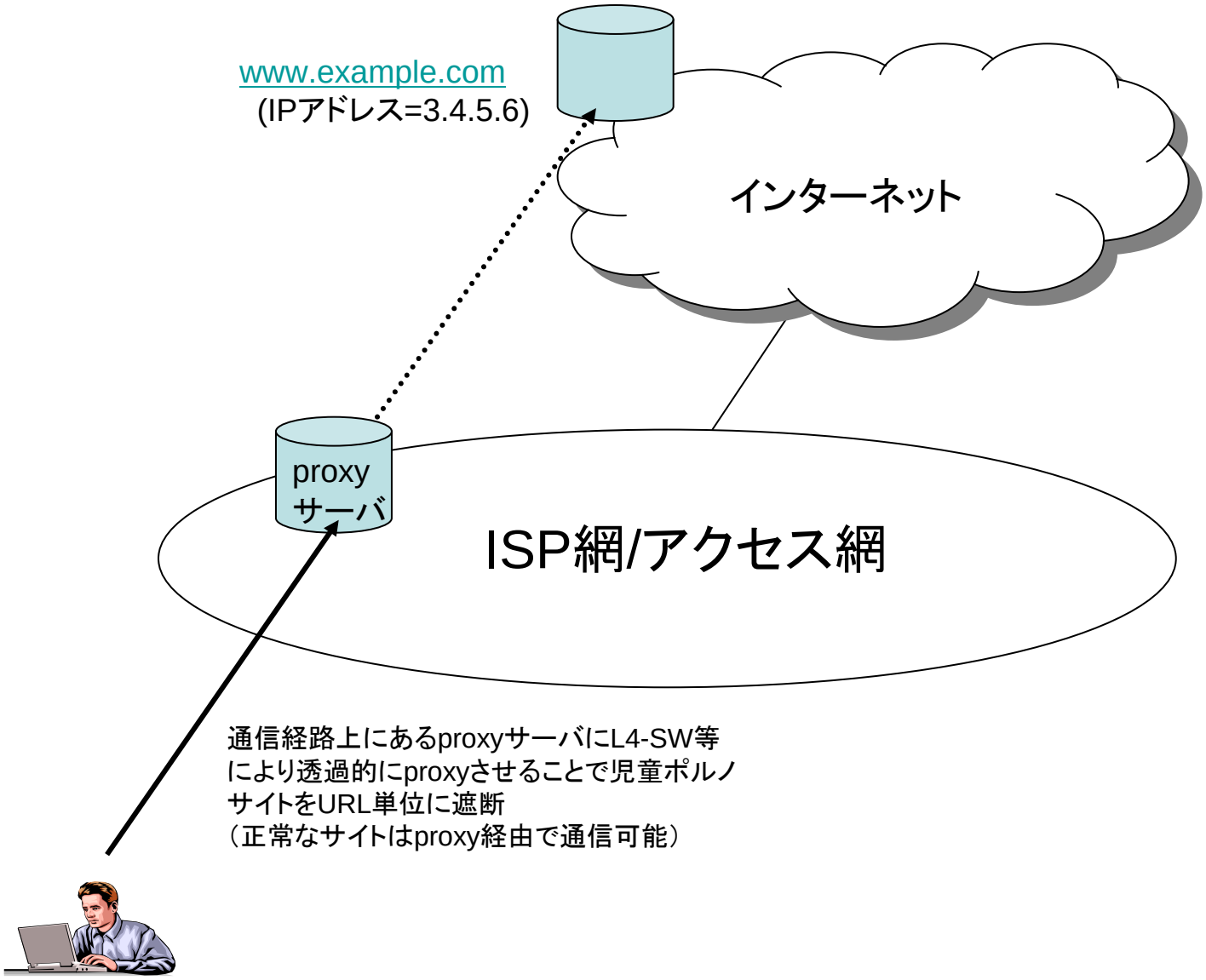
別　紙



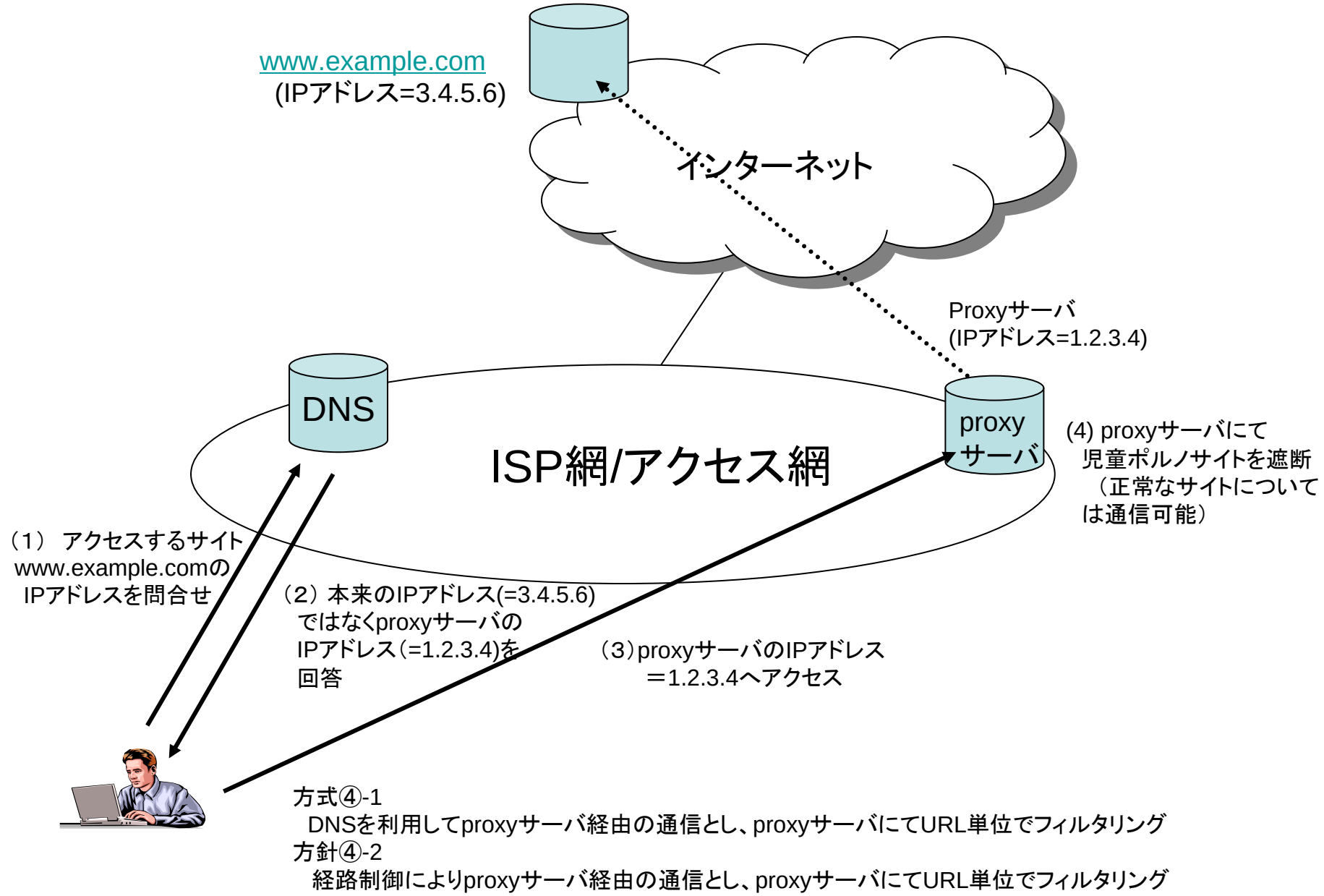
（手法2：パケットフィルタリング方式）



（手法3：プロキシ方式）


www.example.com
(IPアドレス=3.4.5.6)
インターネット
proxy
サーバ
ISP網/アクセス網
通信経路上にあるproxyサーバにL4-SW等
により透過的にproxyさせることで児童ポルノ
サイトをURL単位に遮断
（正常なサイトはproxy経由で通信可能）

（手法4：ハイブリッドフィルタリング方式）



方式④-1
DNSを利用してproxyサーバ経由の通信とし、proxyサーバにてURL単位でフィルタリング
方針④-2
経路制御によりproxyサーバ経由の通信とし、proxyサーバにてURL単位でフィルタリング