

諸外国の違法有害情報対策と、 日本での検討状況と論点

画像電子学会
安全な暮らしのための情報技術研究会
マイクロソフト株式会社 楠 正憲
Masanori.kusunoki@microsoft.com

個人的な体験

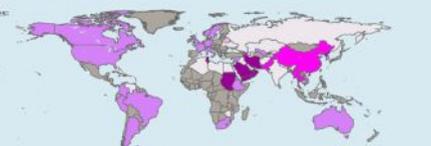


OpenNet Initiative Global Internet Filtering Map

select a map:
Political
Social
Conflict / Security
Internet Tools

SOCIAL

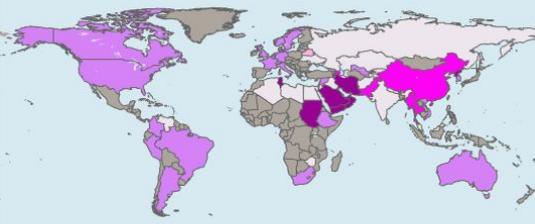
Regional Summaries:
asia
australia / nz
ca
eu
latin america
middle east / n. africa
sub-saharan africa
us / canada



Levels of Filtering: Pervasive Substantial Selective Suspected No evidence

出典: <http://map.opennet.net/filtering-soc.html>

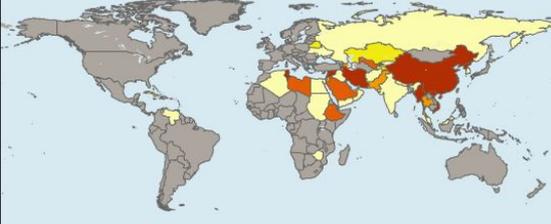
性的コンテンツ等の遮断



Levels of Filtering: Pervasive Substantial Selective Suspected No evidence

出典: <http://map.opennet.net/filtering-soc.html>

政治的主張の遮断



Levels of Filtering: Pervasive Substantial Selective Suspected No evidence

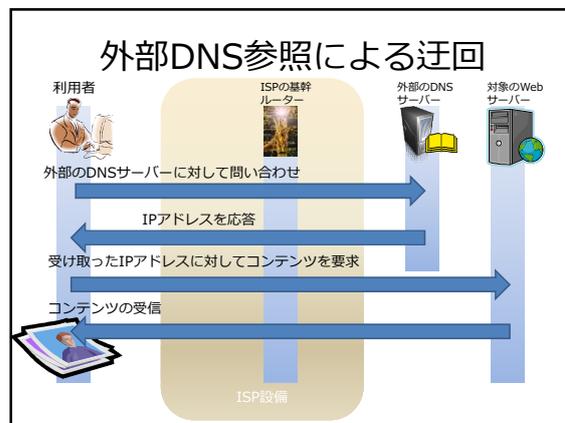
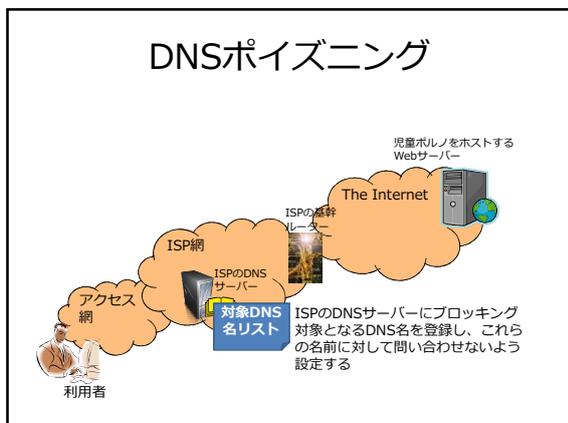
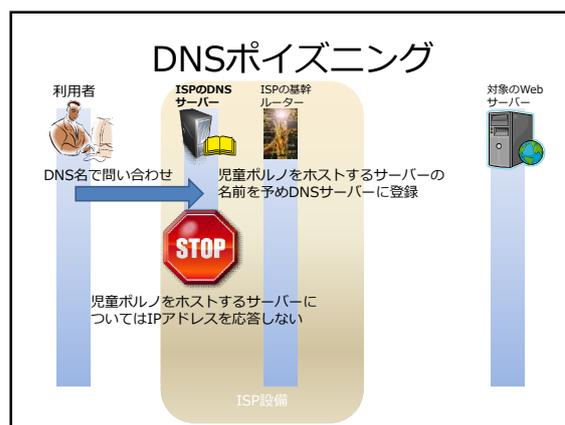
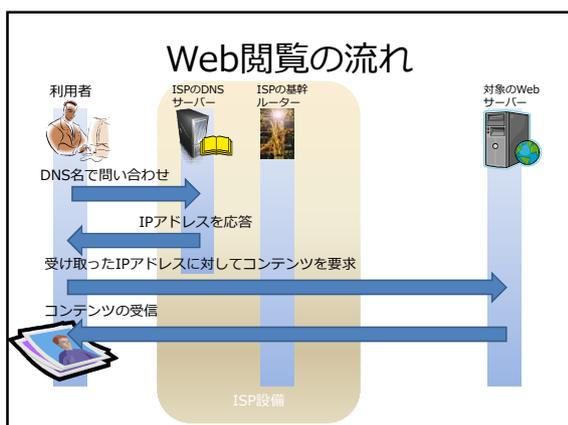
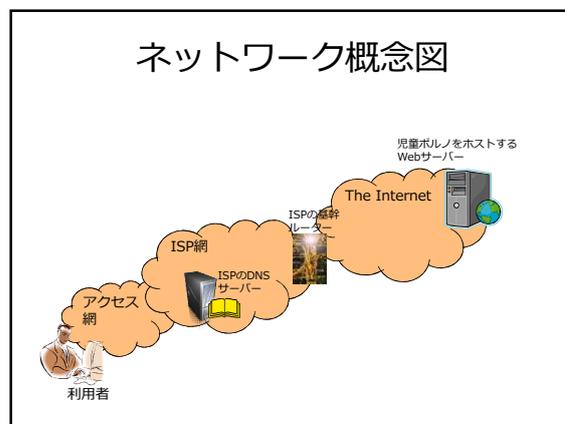
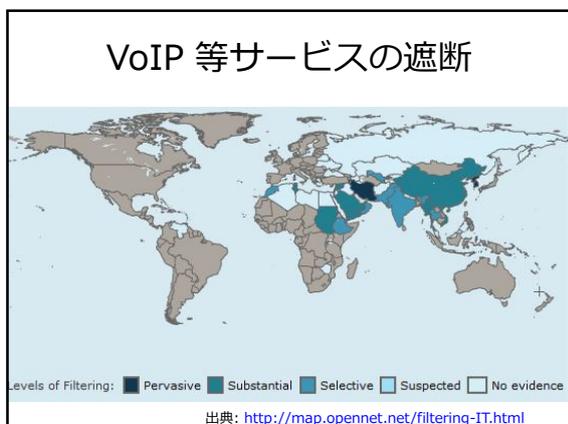
出典: <http://map.opennet.net/filtering-pol.html>

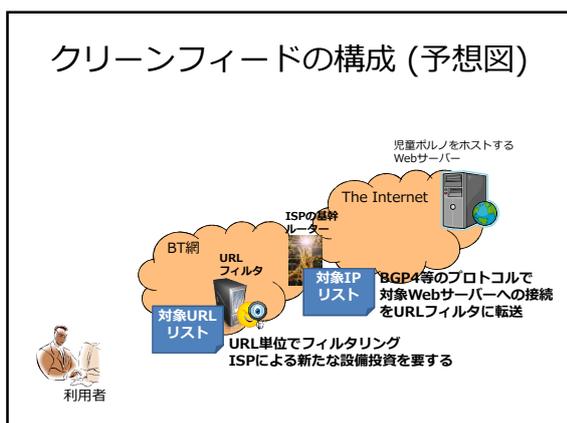
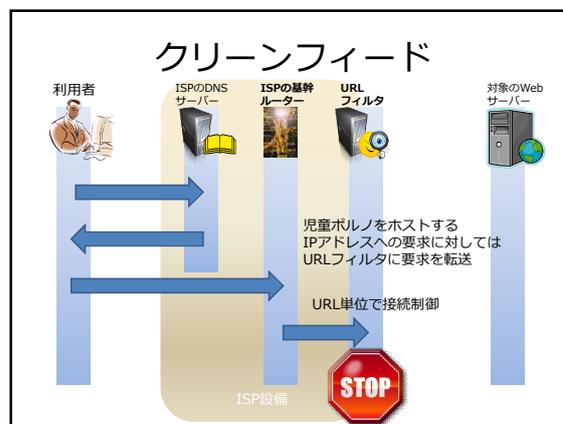
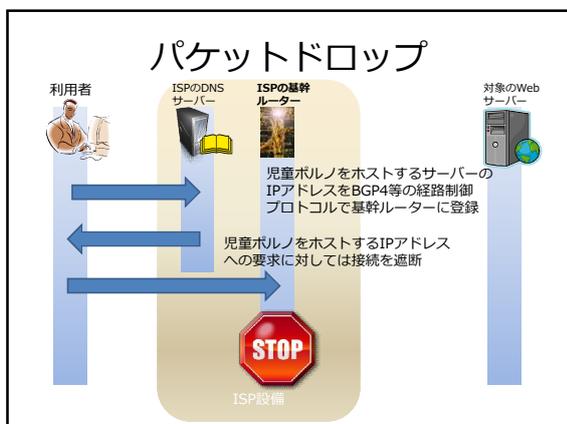
国家機密等の遮断



Levels of Filtering: Pervasive Substantial Selective Suspected No evidence

出典: <http://map.opennet.net/filtering-consec.html>





Youtube アクセス障害 事案

- 事実関係
 - 2008年2月24日 Pakistan Telecom がYoutube へのアクセスを規制した際、URLフィルタへの経路情報を誤って香港 PCCW に逆流させた
 - PCCW の経路フィルタが適切に設定されておらず Pakistan Telecom が伝播した URL フィルタへの経路を Youtube のアドレスブロックとして PCCW が全世界に広げてしまった
 - Youtube 宛の接続要求がパキスタンの設備に吸い込まれ、世界約 2/3 の利用者が、約40分間にわたり Youtube を利用できなくなった
- 論点
 - ISP間の経路交換に用いられる BGP4 プロトコルは脆弱で、ISPによる運用ミス等が世界中の利用者に影響を与える可能性がある
 - ブロッキングに BGP4 を用いることは、設計時に想定された用途ではなく、ISPによる運用ミス等を誘発する危険がある
 - 国内ISPが誤って大規模の合法サービスを妨害した場合、逸失利益について損害賠償請求を受けるリスクを考えると、責任制限等の制度的枠組みがない限り、ISPとして自主的取り組みは難しいのではないかと
 - 運用ミスだけでなく、合法サイト等へのDoS攻撃に悪用される虞も

ブロッキングによる弊害

- 英Wikipedia - Virgin Killer事案
 - Wikipediaに掲載された30年前レコードのジャケット写真が児童ポルノとして通報され、ブロッキングリストに掲載された
 - 英国からのWikipediaの編集が困難に
 - IWFがリストから削除
- 英Archives.org事案
 - ネットのアーカイブサイトの一部が児童ポルノとしてブロッキングされたところ、ISPのサーバー運用ミスでアーカイブ全体がブロッキングされるなどのトラブルが生じた

ブロッキングの方式

方式	遮断単位	実施例	回避手段	法的課題
ブロッキング				
DNSボイズニング	ホスト名	北欧	外部DNS, IP指定	利用の公平
パケットドロップ	IPアドレス	韓国	トンネリング等	利用の公平 ISP 賠償責任
クリーンフィード	URL	英国	トンネリング TLS・URL難読化	通信の秘密 ISP 賠償責任
その他の方式				
セーフサーチ	URL		手動での解除	特になし
フィルタリング	URL・内容		削除・無効化	特になし
アップロード抑止	ファイル		再エンコード	特になし

検出によるアップロード抑止

- CGMサイトへ違法画像等の検出機構を追加
 - End to Endで通信の秘密・利用の公平に抵触せず
- リスト管理団体がシグニチャ等を配布
 - 掲示板サイト等に検出口ジックを組み込む
 - SHA-256等 ハッシュ関数の利用
 - 汎用性は高いが、再圧縮など検出回避が容易
 - 画像検出アルゴリズムの利用
 - ライブラリの配布や移植性、False Positiveなどが課題
 - 年齢推定技術の利用
 - シグニチャ等に依存せず被写体の年齢・性別等を推定
 - 精度が不十分でオーバーブロッキングを招く

ブロッキング展開へ向けた課題

- 「利用の公平」「通信の秘密」との整理
 - ホスト名やIPアドレス単位の遮断では問題のないコンテンツまでブロックされてしまい、電気通信事業法の定める利用の公平に抵触する疑義がある
 - クリーンフィード等のURL単位の遮断は、URLフィルタが、パケットのペイロードに含まれる情報を参考に接続制御することから、電気通信事業法の定める通信の秘密に抵触する疑義がある
- 対象サイト選定・運用の透明性
 - 多くの国でブロッキングはISPによる自主的取り組みとして行われているが、国内であってもISPや地域によって対象サイトなど運用実態にはばらつきがあるようだ
 - 日本国内の大手ISP・プロダク等のサーバーもブロッキング対象となっているが、対象となるサーバー管理者への連絡は行われていないようだ
- 遮断・運用ミス等へのISPに対する損害賠償責任
 - Youtube アクセス障害事案にみられるように、BGPをブロッキングに用いることは、世界中でサイト障害を発生させるリスクがある
 - 大規模サイトの運営を国内ISPが妨害した場合、損害賠償訴訟を起こされるリスクを考えると、責任範囲なしに民間の自主的取り組みを求めることは難しいのではないかと
- 解析・悪用の危険
 - ブロッキングシステム経由で遮断対象のURL等が流出する虞がある
 - ブロッキング・追跡対象となっているDNSサーバーが、外部の合法サイトを参照することで、ブロッキングを合法サイトに対するDoS攻撃に利用される可能性がある

日本での検討状況と論点

- 電気通信事業法や、総合的な法体系での扱いをどうするか
- 児童ポルノの流通抑止を超えて表現の自由を侵害することのないよう担保できるのか
- リスト管理団体の中立性・独立性・透明性を如何に担保するのか
- ブロッキングの運用にかかる費用を誰が負担するのか
- 英仏など、児童ポルノ以外にブロッキング対象を広げる方向にあり、日本でも規制強化へ向けた社会的圧力が高まるのではないかと