児童ポルノ流通防止協議会

ブロッキングに関する報告書

平成２２年３月

目　次

１.はじめに

児童ポルノについては、その製造時に個々の児童への著しい性的虐待を伴うことや被害児童に対する脅迫の道具として利用され得るという問題点があるほか、児童ポルノがインターネット上に一旦流通した場合には、これを回収することは極めて困難であり、性的虐待の現場を永久に残し、被害児童の心を傷つけ続けることとなる問題や児童ポルノの流通によって児童を性欲の対象として捉える風潮を助長するという問題がある。

インターネット上の児童ポルノの流通防止に関しては、これまでにも警察による取締りやインターネット・ホットラインセンターによる削除依頼等の取組が行われている。しかし、インターネット上の掲示板等には、依然として多数の児童ポルノが流通しており、インターネット利用者がこれらの児童ポルノを容易に検索、閲覧することが可能な状態となっている。平成 20 年度総合セキュリティ対策会議において、インターネット上で流通している児童ポルノへの対策として、すべての関係者による重層的な対策を講じることが重要であると提言された。

更なる対策として、検索エンジンサービス事業者による検索エンジンの検索結果から児童ポルノに関する情報を排除する取組みやフィルタリング事業者による児童ポルノの URL のリストへの反映等の対策が考えられる。

また、ISP は、一般の利用者がインターネットにアクセスするために不可欠なサービスを提供する事業者であり、技術的には経路上での通信の遮断を行い得る。一部の諸外国では、民間の取組みとして ISP によるブロッキング が導入されている。ブロッキングは、児童ポルノが掲載されたウェブサイトへのアクセスを利用者の意思にかかわらず遮断するものであり、児童ポルノの流通防止における有効な手段の１つと考えられている。

一方で、ブロッキングについては、電気通信事業法で定める通信の秘密との関係、ブロッキングの導入に伴うコスト、実施に伴うリスク等の法的、技術的な問題も指摘されていることから、我が国において導入する際のこれらの問題点について検討を行った。

ブロッキング検討委員会は、以下の日程で 5 回実施された。

第 1 回ブロッキング検討委員会　2009 年 7 月 13 日（月）
第 2 回ブロッキング検討委員会　2009 年 10 月 8 日（木）
第 3 回ブロッキング検討委員会　2009 年 10 月 26 日（月）
第 4 回ブロッキング検討委員会　2009 年 12 月 10 日（木）
第 5 回ブロッキング検討委員会　2010 年 2 月 18 日（木）

ブロッキング検討委員会の委員名簿は図表１のとおりである。

図表 1　児童ポルノ流通防止対策推進協議会　ブロッキング検討委員会委員名簿

（敬称略）

お茶の水女子大学	教授	坂元　章
社団法人テレコムサービス協会	サービス倫理委員会委員長	桑子　博行
財団法人インターネット協会	副理事長	国分　明男
弁護士		後藤　啓二
財団法人日本ユニセフ協会	広報室室長	中井　裕真
文化女子大学	教授	野口　京子
社団法人日本インターネットプロバイダー協会	理事・行政法律部会副部会長	野口　尚志
ニフティ株式会社	コーポレート本部副本部長兼法務部長	丸橋　透
ECPAT/ストップ子ども買春の会	共同代表	宮本　潤子
WEB110	代表	吉川　誠司

（オブザーバ）

警察庁	生活安全局　情報技術犯罪対策課	
内閣官房	情報通信技術（IT）担当室	
総務省	総合通信基盤局　電気通信事業部　消費者行政課	
経済産業省	商務情報政策局　情報経済課	

（事務局）

財団法人インターネット協会		

２.ブロッキング手法の概要

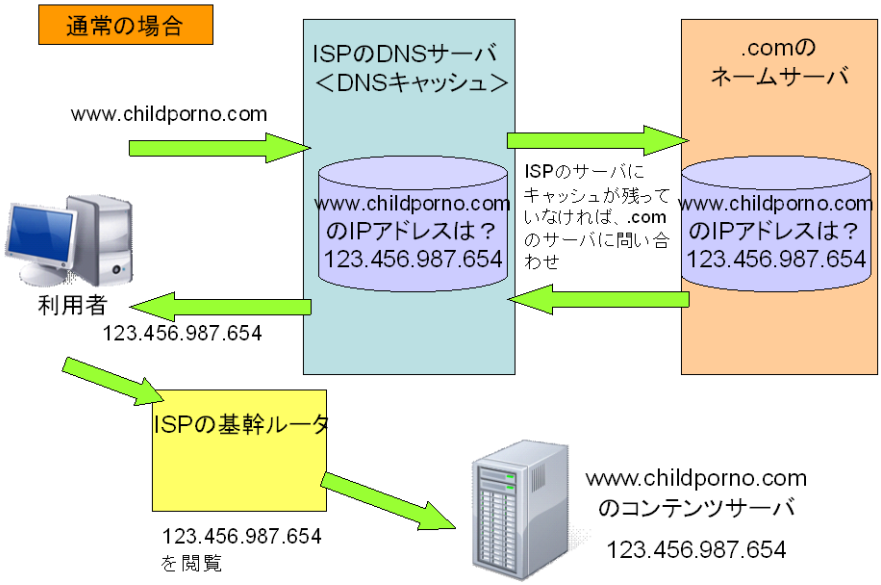
インターネット上の児童ポルノの流通防止ついて、民間ではインターネット・ホットラインセンターによるコンテンツ削除の依頼や、フィルタリング事業者や検索エンジンサービス事業者等における自主的な取組みが進められてきている。また、警察においても被疑者の検挙が行われているが、複製及び配布が容易に行えるというデジタルコンテンツの特性により、一旦、インターネット上に出回ってしまった場合に児童ポルノを回収するのは非常に困難であるといえる。

ブロッキングは、インターネットにアクセスするためのサービスを提供している ISP において、インターネット利用者による特定のサイト又はウェブページへのアクセスを遮断することによって、その閲覧を防止する措置のことをいい、諸外国では既に取組みを行っている ISP も多数存在する。ブロッキングの実施方法は、各国・各社で様々ではあるが、ここでは、DNS ブロッキング、パケットドロップ、URL フィルタリング、ハイブリットフィルタリングの 4 つの手法について概要を紹介する。

（１）http サイトへの一般的なアクセス

一般的に、利用者がインターネット上の http サイトにアクセスしようした場合には、下記のような流れになる。

図表 2　http サイトへの一般的なアクセス



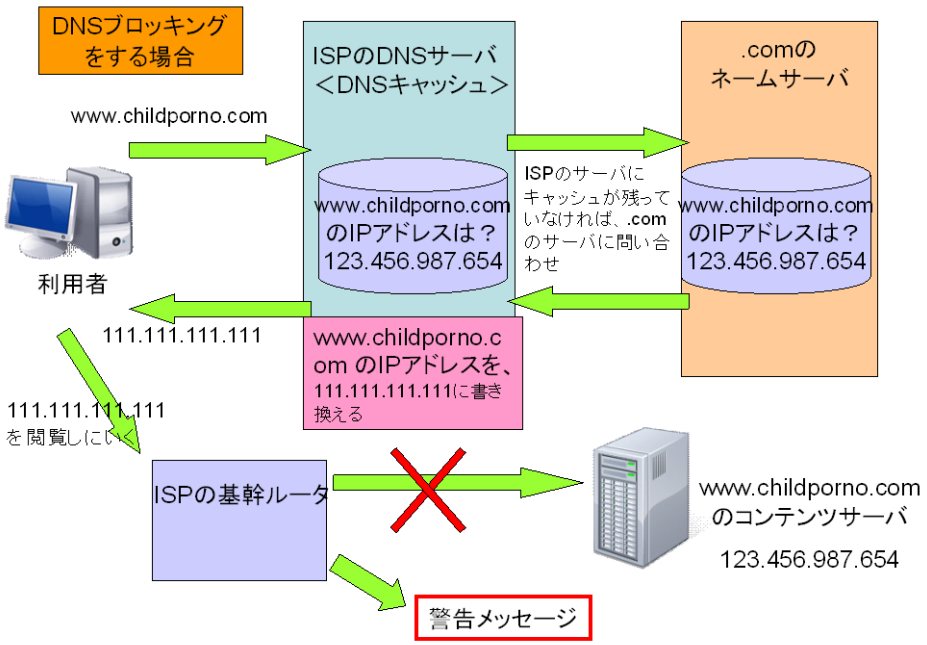
例えば、www.childporno.com というウェブサイトがあり、同サイトの IP アドレスが 123.456.987.654 であったとする。

利用者がそのコンテンツを閲覧したいと思った場合には、Internet Explorer 等のブラウザソフトで、「www.childporno.com」というホスト名を打ち込むか、検索エンジンの結果で示された URL をクリックすることになる。その際、利用者のコンピュータからの要求は、まず ISP の DNS サーバへ送られ、DNS サーバからは、www.childporno.com というサイトの IP アドレス 123.456.987.654 が利用者のコンピュータへ回答される。もし、ISP の DNS サーバに www.childporno.com のキャッシュが残っていなければ、.com のドメインを管理している.com のネームサーバへ www.childporno.com の IP アドレスを確認しにいき、利用者のコンピュータへ www.childporno.com というサイトの IP アドレス 123.456.987.654 が回答されることになる。利用者のコンピュータは、その IP アドレス 123.456.987.654 への接続を行い、ISP の基幹ルータを通って、www.childporno.com のコンテンツサーバ内のコンテンツを閲覧することができる。

（２）DNS ブロッキングによるアクセス遮断

ブロッキングの 1 つめの手法は、DNS ブロッキングである。DNS ブロッキングによって、利用者からのアクセスを遮断する場合には、以下のような流れになる。

図表 3　DNS ブロッキングによるアクセス遮断



例えば、www.childporno.com というウェブサイトがあり、そのコンテンツが児

童ポルノでありアクセスを遮断すべきリスト（ブロッキングリスト）に入っていたとする。コンテンツ利用者がそのコンテンツを閲覧したいと思った場合には、Internet Explorer 等のブラウザソフトで、「www.childporno.com」というホスト名を打ち込むか、検索エンジンの結果で示されたドメイン名をクリックすることになる。利用者のコンピュータからの要求は、まず ISP の DNS サーバへ送られ、ブロッキングされていなければ、DNS サーバ又は.com のネームサーバからは、www.childporno.com というサイトの IP アドレスが利用者のコンピュータへ回答される。

しかし、DNS ブロッキングを実施している場合は、DNS サーバにて、ブロッキングリストに掲載されているウェブサイトについては、正しい IP アドレスを回答するのではなく、警告ページの IP アドレスを回答することになる。仮に、警告ページの IP アドレスが 111.111.111.111 だとすれば、この IP アドレスが回答されることになる。利用者のコンピュータは、www.childporno.com の正しい IP アドレス 123.456.987.654 ではなく、警告ページへの IP アドレス 111.111.111.111 に接続することになるため、利用者は、www.childporno.com に存在する児童ポルノコンテンツを閲覧することはできず、警告ページを閲覧することになる。

ブロッキングの単位は、ホストとなるため、ブロッキングリストもホスト単位で児童ポルノコンテンツを含むウェブサイトを指定する必要がある。

（３）パケットドロップによるアクセス遮断

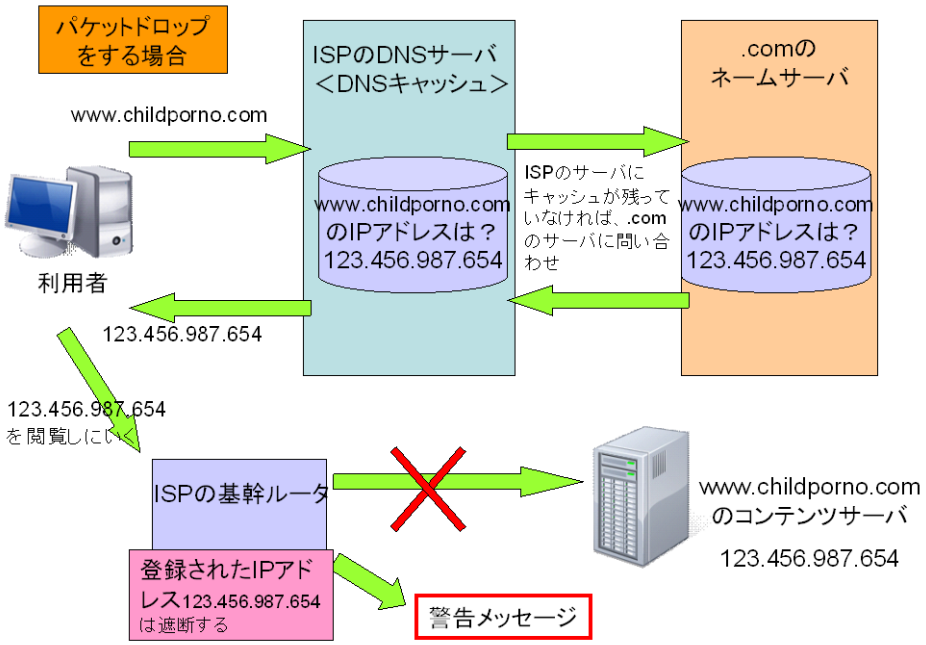
ブロッキングの 2 つめの手法は、パケットドロップである。パケットドロップによって、利用者からのアクセスを遮断する場合には、以下のような流れになる。

例えば、www.childporno.com というウェブサイトがあり、そのコンテンツが児童ポルノでありアクセスを遮断すべきリスト（ブロッキングリスト）に入っていたとする。コンテンツ利用者がそのコンテンツを閲覧したいと思った場合には、Internet Explorer 等のブラウザソフトで、「www.childporno.com」というホスト名を打ち込むか、検索エンジンの結果で示された URL をクリックすることになる。利用者のコンピュータからの要求は、まず ISP の DNS サーバへ送られ、DNS サーバ又は.com のネームサーバからは、www.childporno.com というサイトの IP アドレスが利用者のコンピュータへ回答される。仮に、www.childporno.com の IP アドレスが 123.456.987.654 だとすれば、この IP アドレスが回答され、利用者のコンピュータは、123.456.987.654 への接続を行うというところまでは、通常の http サイトへのアクセスと変わらない。

パケットドロップでは、利用者のコンピュータからの 123.456.987.654 への接続要求を ISP の基幹ルータでチェックする。ブロッキングリストに掲載されてい

るウェブサイトについては、基幹ルータにてアクセスを遮断することになるため、www.childporno.com の IP アドレス 123.456.987.654 へは接続されない。利用者は、www.childporno.com に存在する児童ポルノコンテンツを閲覧することはできず、警告ページを閲覧することになる。

図表 4　パケットドロップによるアクセス遮断

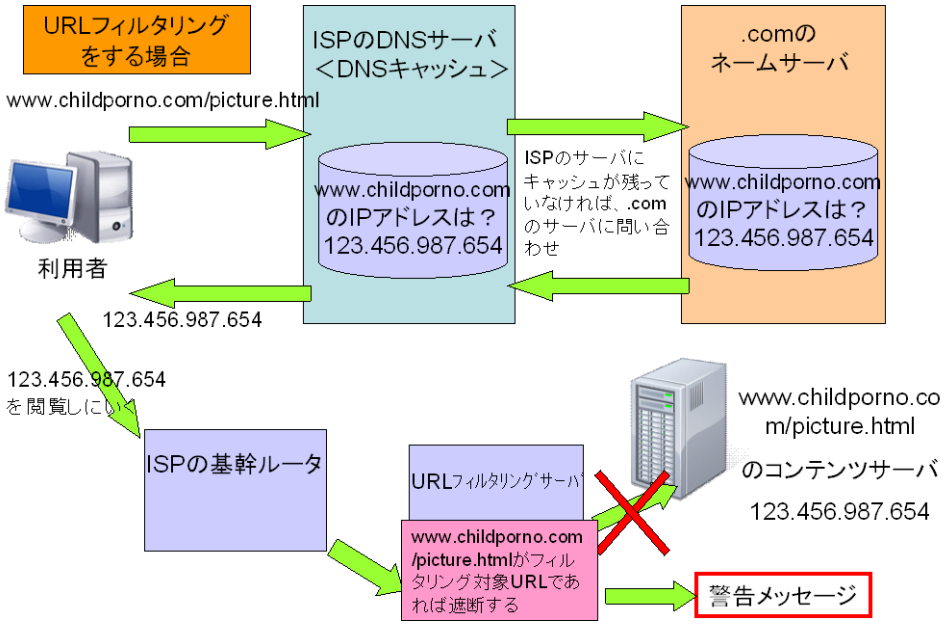


ブロッキング単位は、IP アドレスとなるので、ブロッキングリストも IP アドレス単位で児童ポルノコンテンツを含むウェブサイトを指定する必要がある。

（4）URL フィルタリングによるアクセス遮断

ブロッキングの 3 つめの手法は URL フィルタリングである。URL フィルタリングによって、利用者からのアクセスを遮断する場合には、以下のような流れになる。

図表 5　URL フィルタリングによるアクセス遮断



例えば、www.childporno.com というウェブサイトがあり、そのコンテンツが児童ポルノでありアクセスを遮断すべきリスト（ブロッキングリスト）に入っていたとする。コンテンツ利用者がそのコンテンツを閲覧したいと思った場合には、Internet Explorer 等のブラウザソフトで、「www.childporno.com」というホスト名を打ち込むか、検索エンジンの結果で示された URL をクリックすることになる。利用者のコンピュータからの要求は、まず ISP の DNS サーバへ送られ、DNS サーバ又は.com のネームサーバからは、www.childporno.com というサイトの IP アドレスが利用者のコンピュータへ回答される。仮に、www.childporno.com の IP アドレスが 123.456.987.654 だとすれば、この IP アドレスが回答され、利用者のコンピュータは、123.456.987.654 への接続を行うというところまでは、通常の http サイトへのアクセスと変わらない。

URL フィルタリングでは、利用者のコンピュータからの 123.456.987.654 への接続要求を、URL フィルタリングサーバにて、下位ディレクトリの www.childporno.com/picture.html の部分まで、ブロッキングリストに掲載されていないかをチェックする。ブロッキングリストに掲載されているウェブサイトについては、アクセスが遮断されるため、www.childporno.com/picture.html へは接続されない。利用者は、www.childporno.com に存在する児童ポルノコンテンツを閲覧することはできず、警告ページを閲覧することになる。

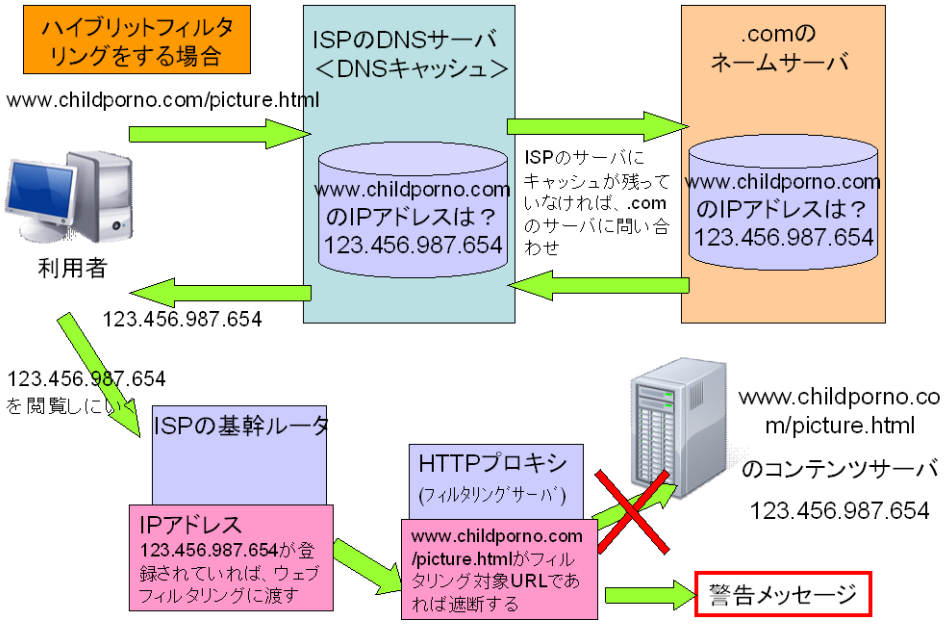
ブロッキングの単位は、URL となるため、ブロッキングリストは、www.childporno.com　といったホスト単位、www.childporno.com/filter/といった

フォルダ単位、www.childporno.com/picture.html といったファイル単位と細かいレベルで児童ポルノコンテンツを含むウェブサイトを指定する必要がある。

（５）ハイブリットフィルタリングによるアクセス遮断

4 つめのハイブリットフィルタリングは、2 段階でブロッキングリストに掲載されているウェブサイトをチェックする手法であり、第一段階ではパケットドロップによるブロッキングで IP アドレスをチェックし、第二段で URL フィルタリングによるページ単位までチェックを行う。利用者からのアクセスを遮断する場合には、以下のような流れになる。

図表 6　ハイブリットフィルタリングによるアクセス遮断



第一段階は、パケットドロップによるアクセス遮断を行うため、利用者のコンピュータから DNS サーバへの問い合わせ、DNS サーバからの回答までは、通常の http コンテンツへのアクセスと同様になる。基幹ルータにおいて、ブロッキングリストに掲載されている児童ポルノコンテンツのウェブサイトであれば、第二段階の URL フィルタリングへと送る。ブロッキングリストに掲載されている児童ポルノコンテンツのウェブサイトでなければ、利用者のコンピュータからの当該サイトを閲覧できる。

第二段階の URL フィルタリングでは、下位ディレクトリの

www.childporno.com/picture.html の部分まで含めて、ブロッキングリストに掲載されていないかをチェックする。ブロッキングリストに掲載されているウェブサイトについては、アクセスが遮断されるため、www.childporno.com/picture.html へは接続されない。利用者は、www.childporno.com に存在する児童ポルノコンテンツを閲覧することはできず、警告ページを閲覧することになる。

ブロッキングの単位は、IP アドレスおよび URL となるため、ブロッキングリストは、www.childporno.com といったホスト単位、www.childporno.com/filter/ といったフォルダ単位、www.childporno.com/picture.html といったファイル単位と細かいレベルで児童ポルノコンテンツを含むウェブサイトを指定する必要がある。

３.ブロッキングに係る問題点の整理

ブロッキングは、児童ポルノが掲載されたサイトへアクセスするための通信を当事者の同意なく遮断する措置であることから、通信の秘密を侵害する可能性が指摘されている。

また、リストに掲載された児童ポルノ以外のものをブロックしてしまうというオーバーブロッキングの問題も指摘されている。オーバーブロッキングが発生した場合には、適法な情報を発信している者の表現の自由を侵害する可能性がある。

また、ブロッキングの導入に係るコストは、手法により大きく開きがあり、ISP の規模等により、経費の観点からの実現可能な手法は異なってくるものと考えられる。ここでは、⑴DNS ブロッキング、⑵ハイブリッドフィルタリング、⑶パケットドロップ及び⑷URL フィルタリングの各種法ごとに問題点を整理することとした。

（１）DNS ブロッキングに係る問題点

ア．電気通信事業法上の通信の秘密との関係について

http サイトへの一般的なアクセスは、技術的には、大きく分けて第一段階の通信として、ISP の DNS サーバに対して、アクセスしようとするホスト名に係る IP アドレスを問い合わせる通信と、第二段階の通信として、この回答を受け当該 IP アドレスを有するサーバへのアクセスを行う通信から構成される。

第一段階の通信を ISP との通信と捉え、ISP が通信の一方当事者となり、当該通信に関しては、通信内容を用いて、ブロッキングに利用することは通信の秘密の侵害に当たらないと解釈し得るとの意見がある一方、①利用者の意思は ISP の DNS サーバとの通信を行うことではなく、あくまでも接続先のサーバへの通信を行うことであることから、DNS サーバとの通信と、IP アドレスを有するサーバへのアクセスを行う通信は一体不可分であると考えることが一般的であり各 ISP もその考えに基づき通信の秘密として保護していること、②仮に ISP が一方当事者としても、第一段階の通信の内容は第二段階の通信の秘密を実質的に推知せしめる事項であり、通信の秘密として保護されるべきものであることから通信の秘密の侵害に当たらないと解釈することについて、不適切であるとの意見もあった。

本報告書においては、DNS ブロッキングは通信の秘密を害するものとして扱い、このため論点は、違法性阻却事由[1]の有無となる。

イ．オーバーブロッキングの可能性について

DNS ブロッキングは、特定のホストに係るサイトへのアクセスをすべて遮断するも

[1] 違法性阻却事由とは、刑罰規定の構成要件に該当して違法性が推定される行為について、その違法性がないとされる事由。

のであることから、ブロッキングの範囲が過大となるオーバーブロッキングの可能性が指摘される。しかしながら、そのサイトが専ら児童ポルノの提供をするために開設されたものであると判断できる場合には、その影響は比較的小さくなるものと考えられる。アドレスリスト作成・維持の段階において考慮することにより回避できると考えられる。

ウ．導入に係るコストについて

ノルウェー国内に 300 万の加入者を有する Telenor への調査結果によると、DNS ブロッキングは、他のブロッキング手法と比較して、導入に係るコストが低いとされる。Telenor では、初期導入費用は DNS ブロッキング用のサーバを 1 台追加するのに要した約 5,000 ユーロ（約 65 万円）であり、運用費用も当該サーバの運用費用のみとされている。

エ．その他

Telenor への調査結果によると、DNS ブロッキングは、ネットワーク障害等にリスクが低いとされている。DNS ブロッキングを導入した場合に起こり得る障害としては、DNS サーバ又はエラーメッセージを表示する web サーバに関するものだけであり、アドレスリストに掲載された web サイトにアクセスしようとする者に対するものに限定される。また、ブロッキングリストの更新時に、リストの内容をチェックし、正常なもののみを読み込ませるような仕組みを講じることにより、事前にネットワーク障害等のリスクを軽減することが可能である。

DNS ブロッキングにおいては、web サイトにアクセスする際にホスト名を用いず、IP アドレスを直接入力することにより、web サイトにアクセス可能である。既知の web サーバの IP アドレスについては、この方法によりアクセスは可能となるものの、web サーバの IP アドレスを入手するためには、一般的には、DNS によりホスト名から IP アドレスを問い合わせる必要があることから、DNS ブロッキングが適切に機能していれば、新たに web サーバの IP アドレスを入手することは困難となるものと考えられる。

一方で、DNS ブロッキングにおいては、ユーザが DNS ブロッキングを導入していない DNS サーバを利用するなどによって回避されるおそれがある。また、DNS のセキュリティ向上のための仕組みである DNSSEC と干渉するおそれもあることから、DNS サーバにおける DNSSEC の導入が標準的となった場合には、新たな手法等を検討する必要がある。

（２）ハイブリッドフィルタリングに係る問題点

ア．電気通信事業法上の通信の秘密との関係について

ハイブリッドフィルタリングにおいては、第一段階の IP アドレスのチェックを経た上で、第二段階の URL のフィルタリングを行うこととなる。第二段階のフィルタリングは、第一段階のチェックにおいて児童ポルノが蔵置されたサーバへのアクセスを行うものに対してであり、その通信に対しては、アクセスを行おうとするファイル名等がチェックされることとなる。そのため経路情報をブロッキングに利用すること及び通信の内容をチェックすることが通信の秘密を侵害することとなり、違法性阻却事由の有無が論点となる

イ．オーバーブロッキングの可能性について

ハイブリッドフィルタリングは、ドメイン単位、ホスト単位、フォルダ単位、ファイル単位でのブロッキングが可能であり、児童ポルノの流通の態様に応じたきめ細かな設定が可能である。したがって、リストを適切に作成・維持することによりオーバーブロッキングの可能性を小さくすることが可能である。

ウ．導入に係るコストについて

ハイブリッドフィルタリングの導入に当たっては、ある程度の費用負担が発生する。イギリス国内に 4,800 万の顧客を有する BT においては、約 50 万ポンド（約 7,000 万円）である。導入に当たっては、基幹ルータの性能の増強、第二段階のフィルタリングを行うサーバの増設などの費用が必要となる。

エ．その他

BT への調査によると、BT のハイブリッドフィルタリング（クリーンフィードシステム（CFS)）においては、ネットワーク障害は現段階では、起こっていない。また、CFS では、障害が発生した場合に、CFS に向けているトラフィックを、CFS を経由しないルートに変更するような Fail Open Structure の発想でシステムが構築されているなど、障害発生時の被害も少なくなるような仕組みとなっており、技術的な措置を講じることにより、システム障害のリスクを減らすことは可能であると考えられる。

また、CFS に関しては、2008 年 12 月、Wikipedia に掲載された画像が児童ポルノとしてリストに加えられた結果、Wikipedia への通信がフィルタリングサーバを経由することとなり、Wikipedia 側での荒らし対策（同一の IP アドレスからの編集を制

限する措置）により、BT からの編集が困難となった事例等が報道されている。[2]

なお、ブロッキングにより信頼性が向上することは考えられず、明らかに信頼性を低下させる要因となることから、例え軽微なものであっても事故が増えることを国民が受け入れられるかについて配慮する必要がある。

（３）パケットドロップに係る問題点

ア．電気通信事業法上の通信の秘密との関係について

パケットドロップおいては、リストに掲げられた IP アドレスに対する通信について、これを遮断するものであることから、通信の秘密を侵害することとなり、違法性阻却事由の有無が論点となる。

イ．オーバーブロッキングの可能性について

パケットドロップは、特定の IP アドレスに係るサーバへのアクセスをすべて遮断するものであることから、ブロッキングの範囲が過大となるオーバーブロッキングの可能性が指摘される。その IP アドレスに係るサーバが専ら児童ポルノの提供を主として開設されたものであると判断できる場合には、その影響は比較的小さくなるものと考えられる。

しかしながら、同一の IP アドレスを持つサーバにおいて異なる者が異なるサイトを開設することは可能であり、一般にサーバの管理者以外の者がそのサーバ上で開設されたサイトすべてを把握することは困難であることから、オーバーブロッキングの可能性は DNS ブロッキングに比して大きくなり、また、リストに掲載される IP アドレスを専ら児童ポルノの提供を行っているものに限ることも困難であるといえる。

ウ．導入に係るコストについて

パケットフィルタリングに関しては、これを導入している外国の ISP からの情報が

---

[2]このほか、2008 年 2 月、パキスタンテレコムにおいて、CFS と同様に BGP による経路制御を使用する方法で YouTube へのアクセスを遮断しようとしたところ、世界的な規模で YouTube へのアクセスに障害が出た事例が報道されている（同社が YouTube のブロッキングのために経路情報を基幹ルータに送信したところ、本来同社内で配信されるべき経路情報が全世界に配信され、世界的な影響が発生した事故）直接の原因はパキスタンテレコムの設定が不適切だったためと考えられるものの、このような事例が報道されていることには留意が必要である。

ないことから、具体的な費用については持ち合わせていないものの、ハイブリッドフィルタリングの第二段階を簡略化したものと見ることも可能である。

（４）URL フィルタリングに係る問題点

ア．電気通信事業法上の通信の秘密との関係について

URL フィルタリングにおいては、http によるアクセスが児童ポルノに対するものか否かを判断するために、アクセスを行おうとするファイル名等のチェックが行われる。URL フィルタリングにおいては、すべての通信についてこのチェックが行われることとなり、通信の秘密を侵害することとなり、違法性阻却事由の有無が論点となる。

イ．オーバーブロッキングの可能性について

URL フィルタリングにおいても、ドメイン単位、ホスト単位、フォルダ単位、ファイル単位でのブロッキングが可能であり、児童ポルノの流通の態様に応じたきめ細かな設定が可能である。したがって、リストを適切に作成・維持することによりオーバーブロッキングの可能性を小さくすることが可能である。

ウ．導入に係るコストについて

URL フィルタリングにおいては、導入した ISP のユーザからの http アクセスをすべて処理する必要があることから、高い性能を有する機器が必要となり、導入に係るコストが高くなる。URL フィルタリングを導入している韓国においては、ブロッキングを実施している８社の合計の設備投資費用として約 300 億ウォン（約 23 億円）を要したとされている。

エ．その他

URL フィルタリングにおいては、導入した ISP のユーザからの http アクセスをすべて処理するものであり、その ISP を利用する限りにおいて、ブロッキングを回避することは比較的困難であると考えられる。一方、http アクセスをすべて処理する必要があることから、高い性能を有する機器が必要となる。一方で、大容量の通信を処理するためのブロッキングシステムは、未だ商用化されておらず、導入する ISP の規模によっては、処理速度の低下などによる通信速度の低下などの影響が発生する可能性がある。

４.まとめ

ブロッキングは、既に一部の諸外国において導入されており、技術的には、実績がある手法であり、児童ポルノの流通防止対策における有効な手法の一つであるといえる。

オーバーブロッキングの問題に関しては、ブロッキング手法によっては、リストの作成・維持のそれぞれの段階において考慮することにより、発生の可能性を減少させることが可能であると考えられる。

ハイブリッドフィルタリング及び URL フィルタリングにおいては、ブロッキングの対象を細かく指定できることから、リストが適切に作成・維持されているならば、オーバーブロッキングが起こる可能性は他の方式に比べて低いといえる。

また、DNS ブロッキングにおいては、ブロッキングの対象がドメイン単位となることから、オーバーブロッキングの可能性が大きくなるといえるものの、リストに掲載するドメイン名を、そのサイトが専ら児童ポルノの提供を主として開設されたものであると判断できるものに限定することにより、オーバーブロッキングの発生の可能性を小さくすることが可能となる。しかしながら、この場合、リストに含められたドメイン名以外のドメインに掲載された児童ポルノをブロックすることはできないため、ブロッキング以外の手段による流通防止対策を検討する必要がある。

ブロッキングの導入に係るコストは、手法により大きく開きがあり、ISP の規模等により、経費の観点からの実現可能な手法は異なってくるものと考えられる。BT においては、ブロッキングのシステムの仕様を無料で公開することにより、小規模な ISP の負担軽減に貢献しており、我が国においても、ブロッキングシステムの共同開発等の費用負担の低減策を検討する必要がある。

電気通信事業法上の通信の秘密との関係については、ある行為が通信の目的以外に利用されるなど、通信の秘密を侵害する行為に該当するとしても、これが正当行為（刑法 35 条）、正当防衛（刑法 36 条）、緊急避難（刑法 37 条）のいずれかに当たる場合には、違法性が阻却されるとされている。重要な論点は、児童ポルノの流通防止という目的に照らし、ブロッキングという手段（いずれの技術的方法を選ぶにせよ、通信の秘密の侵害になる。）をとることについて、違法性阻却事由を見いだせるかということになる。

まず、電気通信事業者の一般的な解釈においては、通信事業の「正当業務」とは、通信をその内容に関知せずそのまま媒介すること及び安定かつ確実な提供を維持することとされている。実際、これまでに「正当業務」に当たると整理されてきた事例は、「通信サービスの提供に必要不可欠な行為」、すなわち、それを行わなければ通信サービスの安

定的な提供が維持できないような場合に、相当な手段の範囲内で行う行為と評価される行為類型であった。例えば、通常の利用者の標準的なトラヒックを大きく上回る利用者について、他の利用者全体へのサービス品質を確保するために行う帯域制御や、迷惑メールの送受信上の支障を防止するための OP25B 等がこれに当たる。

これに当てはめる限り、帯域制御や OP25B 等は、安定した通信サービスの提供を目的とするため目的の正当性が認められるが、児童ポルノのブロッキングにそのような目的はなく、また、通信の内容に着目する手法が手段として相当でない懸念があり、「正当業務」とは整理できないのではないかとの意見があった。(NTT 脅迫電報事件判例参照)

一方、この意見に対しては、刑法 35 条の通説とされる解釈[3]に立った上で正当行為に該当するといえるためには、①目的の必要性、行為の正当性、②手段の相当性を充たすことが必要とされるところ、ブロッキングに関しては、①については、前述の児童の権利を保護する観点に加え、児童ポルノを送信する行為は、そもそも児童買春・児童ポルノ禁止法に違反する行為であること、ヨーロッパを中心に多くの国で既にとられている措置であることなどから、その目的の必要性、行為の正当性が認められることは明らかである。②については、侵害することとなる通信の秘密は通信の経路情報であり、目的達成のために必要な限度にとどまると言え、目的達成のために必要かつ相当な方法と考えられるとの意見があった。

以上のように、正当行為については、その適用範囲について議論があるところである。

また、緊急避難に関しては、顔がさらされているなど被写体が特定されうる児童ポルノについては、被写体とされた子どものプライバシーが著しく侵害されており、一方で、児童ポルノ送信行為はそもそも違法であるなどの事情からすると、このような場合に行うブロッキングは、刑法 37 条の緊急避難の要件を満たしており、違法性阻却が十分に認められるとの意見があった。

しかしながら、緊急避難の成立には、①現在の危難②補充性③法益権衡のそれぞれについて検討を要するところ、国民の表現の自由や通信の秘密という重大な人権と、「人命に比肩する侵害」と言われる児童ポルノによって深刻な被害を受ける児童

[3]大コンメンタール刑法（青林書院）第二版第 2 巻 207 頁によれば、「刑法 35 条は、「法令又は正当な業務による行為は罰しない」と規定する。これは、法令による行為、または、正当な業務による行為は、それが、構成要件に該当する場合であっても、違法性を阻却し、罪とならない旨を規定したものである。しかし、通説は、本条の趣旨を拡張して、もっと広い、一般的な意味をも認める。つまり、本条の後段の正当な業務による行為が違法性を阻却するとされるのは、業務であることに重点がおかれるのではなく、正当な業務であることに実質的な理由があると考えるべきであって、ここから、後段は、業務による行為を例示として、正当な行為一般が違法性を阻却する旨を明らかにしたもので、本条は、違法性阻却の一般的な原則を定めた規定である、と解している。」とされている。

の人権との関係という重大な問題等について結論を出すまでには至らなかった。

以上のように、ブロッキングの手法は、オーバーブロッキングや導入に係る費用においては、それぞれのメリット及びデメリットがあるところであるが、技術的には、コストやオーバーブロッキングの観点からハイブリッドフィルタリングや DNS ブロッキングに児童ポルノの流通防止対策としての可能性が認められる一方、児童ポルノ以外のコンテンツにも適用できるものであり、国民全体の表現の自由や通信の秘密の観点から、その対象となる範囲が野放図に広がることについての懸念もある。通信の秘密の侵害における違法性阻却事由の成否については、正当行為についてはその適用可能な範囲に関して考えが分かれ、緊急避難については法益権衡等について更に議論すべき課題があることから、引き続き検討が進められることが適当であると考えられる。

５．その他・参考資料

（１）海外 ISP に対する実態調査結果

以下では、ブロッキングの 4 手法のうち、DNS ブロッキングを導入しているノルウェーの Telenor、ハイブリットフィルタリングを導入しているイギリスの BT（旧 British Telecom）、URL ブロッキングを導入している韓国の KISPA において、それぞれのブロッキング手法の詳細について実態調査を行った結果を記載する。

■調査対象：児童ポルノに対するブロッキングを行っている ISP または ISP 団体
　⑴ノルウェー　Telenor
　⑵イギリス　BT
　⑶韓国　KISPA
■調査内容：児童ポルノに対するブロッキングの現状
■調査期間：2009 年 10 月～11 月
■調査方法：ヒアリング調査（電子メール、電話）

ア．ノルウェーTelenor の DNS ブロッキング

①ノルウェーTelenor の概要

Telenor はノルウェーに本社を置く通信サービス会社であり、グループ全体では世界最大規模となっている。携帯・ブロードバンド・テレビにおける音声通信・データ通信・コンテンツなどの通信サービスをヨーロッパ、アジアの 13 カ国で提供している。2009 年 3Q で、1 億 7200 万人の携帯利用者がおり、2008 年の売上高は 110 兆 NOK（ノルウェークローネ）、4 万人を超える人々が働いている。Telenor 自体はグローバル企業であり、スウェーデン等でも同様の DNS ブロッキングを行っているが、ここでは、ノルウェー国内で行われているブロッキングに限定して調査を行った。

②ブロッキングの流れ

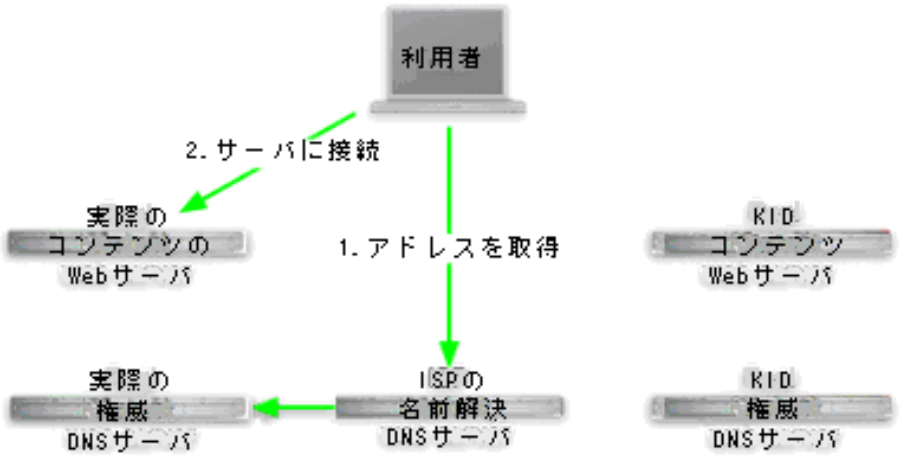
a).具体的な動作

ノルウェーの ISP である Telenor では、DNS ブロッキングを採用している。

通常、利用者のコンピュータから閲覧した URL（例えば、www.childporno.com）をリクエストすると、そのリクエストは、ISP のキャッシュ DNS サーバに名前解決の問い合わせを行う、利用者にキャッシュされている内容から該当する IP アドレス（例えば、123.456.987.654）を返されるか、権威 DNS サーバから該当する

IP アドレス（例えば、123.456.987.654）が返されることになる。利用者のコンピュータは、返された IP アドレスによる HTTP リクエストを実際のコンテンツサーバに送信すると、閲覧したかったコンテンツが返されるという仕組みになっている。

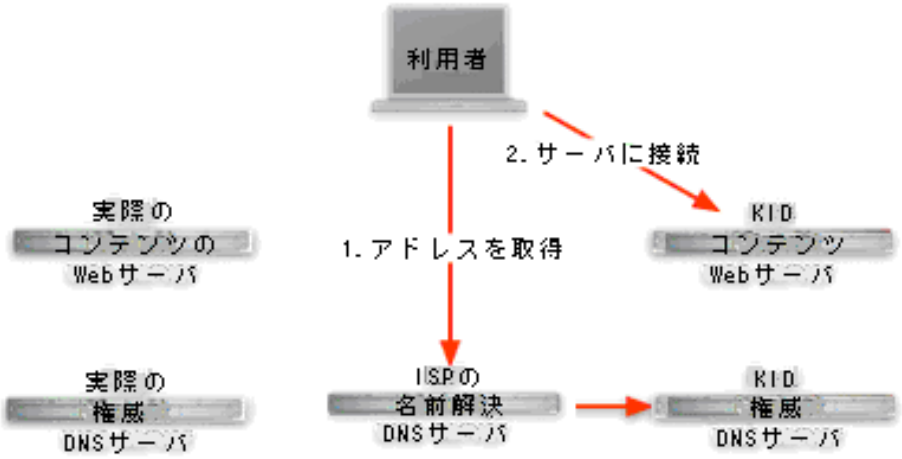
図表 7　通常の接続



資料出所：ノルウェーTelenor よりの提供資料

Telenor の DNS ブロッキングでは、利用者のコンピュータから児童ポルノコンテンツを含む URL（例えば、www.childporno.com）をリクエストすると、そのリクエストは、ISP の名前解決を行うキャッシュ DNS サーバに到着し、そこから KID 権威 DNS サーバにフォワードされて、そこで問い合わせを行う。利用者には、KID 権威 DNS サーバから、KID コンテンツ WEB サーバの IP アドレス（例えば、111.111.111.111）を返されるか、権威 DNS サーバにキャッシュされている応答が返されることになる。

図表 8　DNS ブロッキングが導入されている場合の接続



資料出所：ノルウェーTelenor よりの提供資料

利用者のコンピュータは、要求した URL とは実際には異なる KID コンテンツ WEB サーバの IP アドレス（例えば、111.111.111.111）が返されているため、KID コンテンツ WEB サーバにリクエストを送信することになり、そこで警告ページが返されるという仕組みになる。

DNS ブロッキングを行うシステムの設計では、もともと運用されている名前解決/キャッシュ DNS サーバに加えて、標準のソフトウェア上で動作する KID 権威 DNS サーバと KID コンテンツサーバの 2 つを新しい追加する必要がある。KID 権威 DNS サーバと KID コンテンツサーバが同じサーバ上で実行されても問題はない。複数の名前解決/キャッシュ DNS サーバを使用する複雑なネットワークの場合には、それらをすべてに共通の KID 権威 DNS サーバと KID コンテンツサーバのペアを指すように構成するとよい。これにより、複雑なネットワークでも実装が簡単になる。

もともと運用している名前解決/キャッシュ DNS サーバには、ブロッキングリストに掲載されている児童ポルノ掲載サイトについて、権威データを与えるのではなく、BIND を使用して、ブロッキングリストに掲載されている児童ポルノサイト用の KID 権威 DNS サーバへのフォワードを追加する。

KID 権威 DNS サーバには、すべてのブロッキングリストに掲載されている児童ポルノサイトを含むようにし、ワイルドカードを使用して設定する。それにより、ブロッキングリストに掲載されているすべての児童ポルノサイトが KID コンテンツサーバの IP アドレスを指すように名前解決する。

KID コンテンツサーバは、ブロッキングリストに掲載されているすべての児童

ポルノサイトを含むようにし、ワイルドカードを使用して設定する。具体的には、

- 「/」、「index.html」、「index.htm」へのアクセスに対しては、警告ページを返すべきである。
- 「/robots.txt」へのアクセスに対しては、すべてのエージェントに disallow 情報を返すべきである。
- 「favicon.ico」へのアクセスに対しては、利用者のお気に入りリストに警告アイコンが表示されるようにしてもよい。
- コンテンツサーバに対するそれ以外のすべてのリクエストに対しては、404 エラーメッセージを返すべきである。

Telenor のネットワークでは、DNS サーバを数台使用しているが、通常の DNS サーバやルータの構成について具体的な情報を開示することはできない。この種のフィルタにおいて特徴的なのは、ネットワークの構成に左右されないということであり、利用者が DHCP サーバから特定の DNS サーバを使用するように求められ、その DNS サーバにおいてこのフィルタリングを実装している。

利用者がブロッキングリストに掲載されている児童ポルノサイトに接続した際に表示される画面には、警告ページを使用している。このページでは、法的な文言に言及し、利用者がブロッキングについて苦情を申し立てたい場合や、他の類似のサイトについて報告したい場合にそれができるように、警察へのリンクを提供している。警告ページはノルウェー語と英語で提供されており、実際のページは下記のようになっている。

図表 9　Telenor の警告ページ

資料出所：http://kid.telenor.net/

b).ブロッキングの範囲

警察が評価を行っている児童ポルノサイトについては、ISP はそのドメイン名さえあれば、ブロッキングを行うことができる。警察が、児童ポルノ以外のサイトについてもブロッキングしたいと考えた場合には、ISP と警察の間には、児童ポルノ以外はリストに盛り込まないという合意を行っているため、現在の児童ポルノのブロッキングリストとは別に検討して実施する必要がある。

c).ブロッキングリストの更新

Telenor では、ブロッキングを行うためのリストは、ECPAT からではなく、ノルウェーの警察内の特別な部門からのみリストを受領している。ノルウェーの警察が ECPAT データベースに含まれているすべてのサイトを警察のリストに含めているかどうかについては不明である。

ブロッキングリストの更新は不定期で、1 日のうちに数回の更新がある場合もあれば、数週間更新がないこともある。リストは、PGP で暗号化した電子メールとして受領しており、受領したリストは、DNS の設定に影響する可能性のある不正な記号がないか検査するスクリプトで処理した後に、ブロッキングリストに転送している。ブロッキングリストの内容についてこれ以外の検証は行っていない。

③ブロッキングの技術的課題

a).ブロッキングの回避方法

特定の Web サイトへのアクセスをブロッキングするために利用できるすべての技術は、回避が可能である。具体的には以下のような方法で回避可能である。

・設定を変更して別の DNS サーバを指すようにする
・ローカルで DNS サーバを実行する
・対象ドメインを host リストに含める
・IP トンネリング
・Web プロキシを使用する
・d-name を使用する

ここで重要となるのは、利用者がどの程度までのブロッキングを受け入れるかということと、利用者にブロッキングを回避する手段を実装する力量がどの程度あるかということになる。

ファイル交換サイトの The Pirate Bay がデンマークでブロッキングされた際に

は、多くの利用者がそのブロッキングを受け入れず、http://thejesperbay.dk/などの Web サイトがすぐに立ち上げられ、ブロッキングの回避方法を手順ごとに説明する情報が掲載された。ノルウェーではブロッキングを始めてから 5 年が経過しているが、ブロッキングの対象は子供の性的虐待にかかわるコンテンツに限っており、ブロッキングそのものに関する思想的な面からの遺憾の表明がいくつかあった以外には苦情はなく、ブロッキングを回避する方法を掲載したサイトが立ち上げられたということも聞いていない。

b).ブロッキングの正確性

オーバーブロッキングについては、過去に一度、警察がいくつかのサブドメインをブロッキングリストに追加した後、そのドメイン全体をブロッキングリストに含めたことがあった。例えば、badsite1.mainsite.com、badsite2.mainsite.com、badsite3.mainsite.com などをブロッキングリストの対象とした後に、mainsite.com そのものをブロッキングリストに追加するといった行為になる。この場合、別のサブドメインで Web メールを利用していたロシア人から苦情があり、ドメイン全体のブロッキングをやめて、サブドメインのブロッキングを続けることとなった。しかし、苦情はすべて警察に直接向けられたため、Telenor が直接的にこの件に関与することはなかった。

Telenor では、ブロッキングを開始して 5 年を経過するが、その中で耳にしたオーバーブロッキングまたはフォールスポジティブの事例は、上記が唯一の事例ある。

オーバーブロッキングを解決する方策としては、警告ページに、オーバーブロッキングが行われていると思った場合に警察に連絡する方法が掲載されている。Telenor に対して利用者から連絡があった場合も、警察内の正しい連絡先に直接連絡してもらうようにしており、Telenor 自身がブロッキングの正確さについて制御することはない。

c).ネットワーク障害の可能性

DNS ブロッキングでは、エラーやネットワークパフォーマンスの低下のリスクが低いことが利点であるといえる。

DNS ブロッキングを導入した場合、起こりうるエラーとしては、DNS サーバまたはエラーメッセージを表示するために使用する Web サーバに関係するものだけである。それも、KID 権威 DNS サーバまたはエラーページを表示する KID コンテンツ web サーバのハードウェアまたはソフトウェアに障害があった場合、不正なサイトにアクセスを試みている人に対する応答速度が低いか応答がないだけといった問題にしかならない。

理論的には、不正な文字や構文を含んだ構成ファイルを読み込んだ場合、DNS サーバは停止するおそれはあるが、DNS サーバ再起動の前に、新しい構成ファイルでの再起動が可能かどうか、BIND サーバが検査する仕組みになっている。人為的なミスによって壊れたファイルを追加しようとしたとしても、ブロッキングリストが更新されないだけとなる。

ネットワーク障害の可能性を事前に回避するために、DNS サーバを停止させるおそれのある不正な記号や構文が含まれていないことを保証するためスクリプトを実行している。DNS サービスとブロッキングリストの整合性を確認するために自動化した検査も実行しているため、何らかの誤りがあれば、1 分もかからずに警告が発せられるようになっている。

ブロッキングリストの更新時に DNS のキャッシュ全体をリフレッシュすると、更新を適用した直後は一部のリクエストに対して遅延が発生することになるが、Telenor では、新しいリストにおいて変更のあったドメインのみをフラッシュしているので、DNS のパフォーマンスが低下することはない。

④ブロッキングの法的課題

a).ブロッキングの法的義務

ノルウェーでは、ISP が児童ポルノをブロッキングすることに法的義務はない。ブロッキングは自主的に行われており、主要なすべての ISP が対応している。ノルウェーの ISP 事業者は、児童ポルノの流通防止に自主的な解決策が見出されなければ、法律が制定されて施行されることになると理解している。またこの種のコンテンツについて一般の人々の注目や世論があったため、ISP にとってはこの自主的な解決策に参加しやすい土壌になっていたことも背景になっている。

ISP の間では、特定な技術的な解決策を法律によって義務付けられることは、次の点からよい考えとは受け取られていなかったため、自主的な取り組みが推進された。

- 解決策がすぐに陳腐化したり、最適でなかったり、既知のセキュリティ問題が生じたりするおそれがある
- 最良の技術的な解決策について自由な競争が阻害されるおそれがある
- 解決策が必要以上に高額になるおそれがある

b).ブロッキングに伴う訴訟リスク

ブロッキング実施に伴い、一旦ブロッキングをしたサイトについて実は児童ポルノ掲載サイトではないことが判明した場合、ISP が損害賠償請求されたケースは、ノルウェーではない。

c).ブロッキング導入にあたり検討した法律

ブロッキング導入にあたって検討されたのは、ごく少数の課題でしかない。

第一に、ブロッキングリストは誰が作成するべきかといった課題である。当初は、ある NGO 組織が何をブロッキングすべきかについて情報収集を始め、リスト作成に個人的に支援する人々も数人いて、それぞれ独自にオンラインで調査を行っていた。しかし、警察が関与することになったため、NGO によるブロッキングリスト作成の活動が停止した。

第二に、ブロッキング実施するにあたり、児童ポルノコンテンツに限定し、他の分類のコンテンツをブロッキングの対象にしないといった課題である。これについては、警察と ISP との間の合意事項に盛り込むことになった。これは、警察からの要望で、政治的な圧力を避けるという背景があった。過剰なブロッキングを行えば、現在得られているブロッキングに対する一般の人々の支持が得られなくなり、ブロッキングを回避する方法が出回ることにつながってしまうためである。

第三に、Telenor が企業として、ブロッキングの技術的な実装にのみ関与し、リブロッキングリストの作成には関与しないということである。Telenor の誰もが対象コンテンツを見る必要がないこと、コンテンツの合法性を評価する必要がないこと、利用者を特定するために使用できるいかなる情報も記録も転送もしないことが重視された。

⑤ブロッキング導入に伴う設備投資コスト

ブロッキングは、Telenor が提供するダイヤルアップ、xdsl、ケーブルモデム、モバイルのすべてのアクセス手段に適用されており、ノルウェーでは全体で 300 万のアクセス顧客（複数のアクセス手段所持も含む）が存在する。

初期投資費用は、ブロッキングを実装するために、KID 権威 DNS サーバと KID Web サーバの両方が稼動する 1 台のサーバを追加しただけである。また、もともと運用していた通常の DNS サーバの構成変更のために一定の作業工数はかかっており、技術的な実装には、5，000 ユーロ＝約 75 万円程度で可能である。

年間コストは、その 1 台のサーバをホスティングして運用するコストのみである。

ブロッキング実施のために必要となる作業は、通常の Web サーバと通常の DNS サーバの維持に必要な作業と、ときどき更新がある DNS の構成に関する作業だけである。これは、フルタイムの工数を 1 とした場合に、0.2 の工数でできる程度の作業量といえる。

また、スクリプトを使用して、リストの更新、チェックなどを自動化している。

イ．イギリス BT のハイブリットフィルタリング

①イギリス BT の概要

BT は、イギリスの電気通信事業者であり、世界 173 カ国でコミュニケーション事業を展開するグローバル企業である。以前は、国営通信事業者だったが、1984 年に民営化されている。固定電話事業、携帯電話事業、インターネットプロバイダ事業、ソリューションサービスから金融向けのネットワークやシステム、電話会議サービスなど多様な製品・サービスを提供している。世界で 3 万 7 千人の従業員が働き、2008 年で 207 億ポンドの売上となっている。

②ブロッキングの流れ

a).具体的な動作

イギリスの ISP である BT では、ハイブリットフィルタリング方式の一種である「Clean Feed System（以下 CFS)」を採用している。CFS の導入実験は 2004 年から行われたが、利用者への導入実験開始の広報は行わなかった。実験から 3～4 ヶ月後の 2004 年 6 月に、ジャーナリストにより CFS についての記事が新聞に書かれ、BT で児童ポルノコンテンツのブロッキングを行っていることが公となった。現在も、BT から公式に CFS 導入について発表は行っていない。

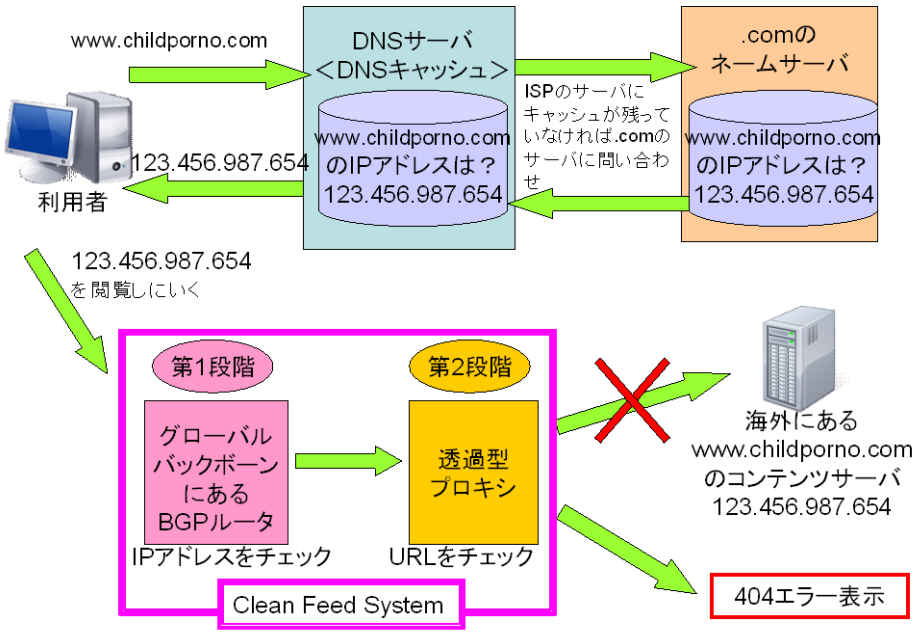
CFS によるブロッキングは、海外サーバにあるコンテンツが対象であり、BT の会員が、BT のネットワークの中で児童ポルノのコンテンツを掲載した場合には、ブロッキングとは別に積極的に探し、削除している。

BT では、IWF より提供されたリストにより児童ポルノコンテンツのブロッキングを行っている。例えば、www.childporno.com という児童ポルノサイトが海外サーバに存在し、そのサイトが IWF のリストに掲載されていた場合の CFS の具体的な動作を以下の図で示す。

BT の利用者から、www.childporno.com への接続要求がされた場合、www.childporno.com の IP アドレスが仮に 123.456.987.654 だとすると、DNS サーバから利用者のその IP アドレスが回答される。利用者のコンピュータは、123.456.987.654 に接続しようと、BT のインフラがグローバルバックボーンに接続している部分にある BGP ルータで、まず IP アドレスがチェックされる。その IP アドレスが、IWF のリストに該当するものであれば、次いで、透過型プロキシで URL がチェックされる。IP アドレスと URL の 2 つを IWF のリストと照らし合わせるシステムが CFS である。IP アドレスと URL の両方で、リストに該当すれば、利用者からの接続要求はブロックされ、404 エラーの表示が出されることに

なる。

図表 10　BT における Clean Feed System の仕組み



資料出所：BT からのヒアリングを元に作成

b).ブロッキングの範囲

ブロッキングを実施するにあたり必要な情報は、IWF から提供されるリストに掲載している児童ポルノコンテンツの URL だけである。第 1 段階のチェックで利用している IP アドレスは、リストに掲載してある URL から逆引きしている。IWF が指定するブロックキング対象 URL は非常に限定的であり、BT ではブロッキングを行う際に、IWF のリストに独自の URL を追加することは行っていない。IWF のリストで、ドメインを丸ごと指定していれば、ドメインごとブロックし（例：Blacksite.com）、フォルダレベル（例：Blacksite.com/forward/）、もしくはファイルレベル（例：Blacksite.com/forward/***.jpg）まで指定してあれば、そこでブロックしている。

c).ブロッキングリストの更新

IWF からのブロッキングリストのダウンロードおよび CFS のシステムへの書き換えは、自動的に行われるようになっている。IWF サイトでのリストの更新は 1 日 2 回あるが、CFS からのダウンロード・更新は、夕方 6 時に 1 日 1 回行うだけとなっている。ダウンロードしたリストの CFS のシステム側の更新作業も、リス

トのダウンロード時に自動で行われている。

③ブロッキングの技術的課題

a).ブロッキングの回避方法

ブロッキングを行う際の技術的な課題としては、ブロッキングを回避してしまう方法があるのではないかということになるが、CFS によるブロッキングにおいても、迂回の方法は存在するという。例えば、別にプロキシを立てて、それを利用する場合や、トンネリング[4]されても、中が見えないため迂回が可能である。https サイトのブロッキングは、システム上可能であるが、IWF のリストには現在、https のサイトが含まれていないため行っていない。

b).ブロッキングの正確性

ブロッキングしてはいけないサイトまでブロッキングしてしまうオーバーブロッキングについては、wikipedia での事例がある。これは、2008 年 10 月に Wikipedia に掲載されているがドイツのロックバンド Scorpions の「Virgin Killer」というアルバムのジャケット写真が、IWF によって児童ポルノと認識され、IWF のブロッキングリストに掲載されたために生じた事例である。しかし、BT では、IWF からダウンロードしたブロッキングリストをそのままブロッキングに利用しているだけであるため、技術的な問題によってオーバーブロッキングが起こったのではなく、リスト作成段階の該当性判断の問題であるといえる。その後、IWF はブロッキングリストから該当ページを削除したため、問題は解決している。

c).ネットワーク障害の可能性

CFS 導入によるネットワーク障害の可能性については、導入から現在までで、実際にはインフラ部分で技術な問題は起きていない。システム自体の更新アップグレードも何度か行っているが、その際にも問題は起きていないという。CFS は、利用者に対し、最小限の影響しか与えない仕組みになっており、トラフィックが遅くなるということも発生していない。また、CFS は、万が一、障害が生じた場合は、BGP ルータのレベルでルートを変えて、CFS に振り向けていたトラフィックをそのまま通せば、障害はなくなるような Fail Open Structure の発想でシステムが構築されている。そのため、障害発生時の被害も最小限で食い止められる仕組みとなっている。

CFS を運用していく上での課題は、WEB サイトによっては、DOS 攻撃の保護

[4] トンネリングとは、インターネットの公衆回線上に閉じられた 2 点の仮想的な直結通信回路を確立することで、PPTP（Point to Point Tunneling Protocol）や SoftEthe などがある。この技術を利用することで、VPN（Virtual Private Network）が可能になる。

機能により、CFS からのキャッシュがブラックリストに入ってしまい、BT の利用者からの接続ができなくなってしまうことがある。その場合は、その WEB サイトの管理者に連絡し、リストから外してもらうよう要請している。

④ブロッキングの法的課題

a).ブロッキングの法的義務

イギリスにおける児童ポルノに関する関連法令はいくつか存在する。1978 年に制定され、2003 年性犯罪法により修正された児童保護法の第 1 条では、「児童ポルノを作成することは撮影や頒布等と並んで重犯罪であり、10 年以下の禁錮、罰金又はその併科」と定められている。児童ポルノの作成には、コンピュータ上に児童ポルノ画像のコピーを作成すること、すなわち児童ポルノをコンピュータにダウンロードしたり、Web ページを見ることで児童ポルノのキャッシュがコンピュータに保存されることも含まれる。また、1988 年に制定された刑事司法法第 160 条でも、児童ポルノの単純所持は違法とされ、違反した場合は 5 年以下の禁錮、罰金又はその併科と定められている。

児童ポルノを所持したり、閲覧したりすることに厳しい法律が定められているイギリスではあるが、ISP が、児童ポルノコンテンツに対して、ブロッキングを行うことに対しての法的な義務は現在のところない。BT でも、他の ISP でもボランティアベースでブロッキングを行っており、政府からの補助金といったものも存在しない。ボランティアベースではあるが、イギリス政府からは「積極的にブロッキングシステムを導入するよう」に強く働きかけられており、イギリス議会でも、ブロッキング導入率を 100%すべきといった議論が行われたという。

b).ブロッキングに伴う訴訟リスク

ブロッキングに関して、コンテンツ提供者や一般の利用者から BT が訴訟されたということは、CFS 導入から 5 年間の経験でも一度もない。BT の中には、Abuse Team（苦情対策チーム）があるが、いくつか苦情はあった程度である。CFS では、ブロックされたとしても、エラー404 が表示される仕組みなので、利用者にはブロッキングされていることがはっきりとはわからないような仕組みとなっている。また、利用者から「このコンテンツを閲覧できないが、ブロッキングしているのではないか」と問い合わせがきても、BT がブロッキングを行っているか、行っていないかといった回答は行っていない。ブロックされたコンテンツ提供者が苦情を言えるような仕組みは、内務省（Ministry of Home Office）が別途定めている。

c).ブロッキング導入にあたり検討した法律

児童保護法は非常に厳しい法律であり、児童ポルノの単純所持も違法となる。「たまたま見ただけである」「児童ポルノの調査をしていた」といった理由は認められない。BT の立場としては、CFS を導入することで、BT の会員が児童ポルノを自分の意志ではなく見てしまう可能性があることを防止していると考えている。ただし、児童ポルノコンテンツをブロックすることは、まだ法律的に未審理の状態でもあるため、CFS 導入時には、このようなブロッキングのスキームについて、BT グループ PLC ボード（公開有限責任会社の経営陣）のレベルで検討した。ブロッキングについては、トラフィックを intercept（傍受）すること、通信を遮断することが、通信事業者の義務に反するのではないかという法的リスクも伴うという認識のもとで承認されている。

⑤ブロッキング導入に伴う設備投資コスト

BT の 2009 年 3 月末時点の一般消費者向けのブロードバンド顧客は約 4800 万人（IPTV、WiFi などのサービスも含む）となっている。この規模で、CFS というブロッキングシステムが導入されているが、初期投資費用は約 50 万ポンド（1 ポンド 150 円換算で約 7500 万円）と導入コストは極めて低かった。年間コストについては、全体運用コストに含まれてしまっているため、CFS だけの運用コストは算出していない。工数についても、CFS だけの工数については算出していない。

CFS をパッケージとして販売するということはしておらず、基本的には、他の ISP や政府に対し、システムの方法を開示している。開示する際には、守秘義務契約（NDA）を結び、無償で提供している。

ウ．韓国 KISPA の URL ブロッキング

①KISPA の概要

KISPA は、韓国インターネットサービスプロバイダー協会の略称であり、インターネットサービス品質向上と公正な競争環境を作るため、事業者による協力団体として 2000 年 4 月設立された。ISP 産業の国際動向分析のための国際交流活動、国内関連産業の動向を報告する韓国 ISP 便覧の発刊、健全なインターネット文化造成のための違法情報のフィルタリング事業、次世代インターネット政策に関連した各種コンファレンスの開催等により、ISP 産業の位置づけを確固たるものにしていくことに貢献している。

現在 35 社が加盟しており、KT、SK ブロードバンド、LG テレコムなど大手 ISP も含まれている。

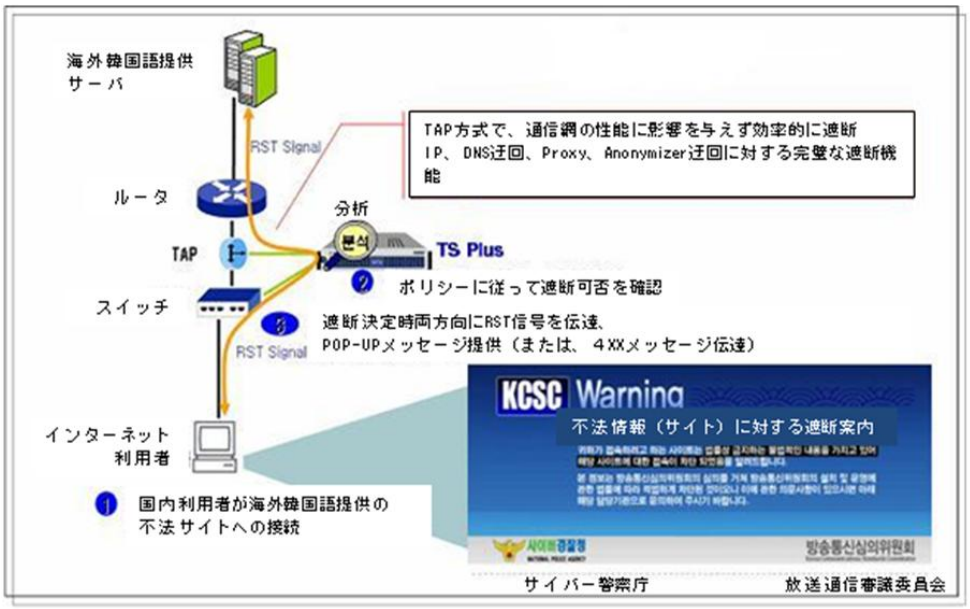
②ブロッキングの流れ

a).具体的な動作

韓国では、DNS ブロッキングやパケットドロップといったブロッキング手法が導入されていたが、2009 年 1 月から URL ブロッキングを採用している。韓国の URL ブロッキングは、下位ディレクトリおよびページ単位まで遮断できるシステムであり、DNS クエリ、DNS- Free(DNS 自動変更プログラム)迂回接続、IP 接続、中継サーバ(Proxy)迂回接続、Anonymizer に対してもブロッキングできるものとなっている。URL ブロッキングのシステムは、ISP の国際ゲートウェイに設置されており、海外サーバに保存されている児童ポルノコンテンツ等の違法コンテンツに対して、韓国国内から接続するトラフィックを分析して、違法サイトに対する接続をリアルタイムで制御している。韓国での URL ブロッキングの具合的な動作を以下の図に示す。

韓国国内の利用者が、海外の違法 URL への接続を行った場合、TAP によりそのトラフィックを TS Plus というトラフィック分析のための機器に振り向け、保存されているブロッキングリストとの比較を行い、ブロッキングの有無を決定する。利用者が接続しようとした URL が、ブロッキングリストに掲載されている場合は、接続が遮断され、「KSCS Warning」の警告画面が表示される。

図表 11　韓国における URL ブロッキングの仕組み



資料出所：韓国 KISPA よりの提供資料

b).ブロッキングの範囲

ブロッキングを実施するにあたり必要な情報は、KCSC から提供されるリストに掲載されている児童ポルノコンテンツの URL だけである。KCSC のブロッキングリストの対象は、海外にサーバを置き、韓国語で情報を提供しているサイトの中で、わいせつ・煽情的な情報、違法な賭博に関する情報、薬品などその他違法情報、長官命令権対象の国家保安法違反情報等となっており、児童ポルノコンテンツだけに限定したブロッキングではない。

c).ブロッキングリストの更新

KCSC からのブロッキングリストは、従来は電子メールにて ISP に送付されていたが、2009 年 9 月までにアドレスリスト自動配信プログラムで行えるように移行中である。

③技術的課題

a).ブロッキングの回避方法

ブロッキングを行う際の技術的な課題としては、ブロッキングを回避してしまう方法があるのではないかということになるが、韓国の URL フィルタリングにおいても迂回の方法はある。DNS、IP、URL 迂回接続など以外にも、他の形態の接続方式が出現する可能性は常にあるといえる。

b).ブロッキングの正確性

URL 単位でのブロッキングとなるため、ドメインレベル、フォルダレベル、ファイルレベルと細かい範囲でブロッキング行える。また、KCSC から提供されるブロッキングリストに基づき、ブロッキングを行っているため、オーバーブロッキングが発生した場合は、技術的課題というよりも、ブロッキングリストを作成する段階での該当性の問題となる。

c).ネットワーク障害の可能性

韓国の URL フィルタリングでは、TAP 方式によって、ネットワークの性能に影響を与えずに効率的にブロッキングできる仕組みがとられている。ただし、ISP では、現在、国際ゲートウェイに 10Giga 回線の導入を進行させているが、10Giga トラフィックを処理する URL ブロッキングのシステムはまだ商用化されておらず、また安定性も十分ではないという課題は将来的には発生する。

④ブロッキングの法的課題

a).ブロッキングの法的義務

韓国においても、通信の秘密に関しては、「情報通信網利用促進および情報保護などに関する法律」の「第 49 条　秘密の保護」において「何人も、情報通信ネットワークによって処理、保存または伝送される他人の情報を毀損し、他人の秘密を侵害し、盗用し、または、漏洩してはならない」と定められている。ブロッキングに関しては、「情報通信網利用促進および情報保護などに関する法律」の「第 44 条の 7　不法情報の流通禁止」の「情報通信網を通じてわいせつな情報、他人を誹謗したりその名誉を毀損したりする情報、恐怖心や不安感を誘発する内容を繰り返し相手に到達させる情報、年齢確認等を行わずに提供する青少年有害媒体物、国家保安法に違反する内容や、犯罪を助長する内容の情報を流通させてはならない」といった法律も定められている。このほかに、放送通信委員会が、審議委員会での審議を経て、情報通信サービス提供者又は掲示板管理若しくは運営者をしてその取扱いを拒否、停止、又は制限するよう命じることができるといった内容が定められる「放送通信委員会の設置および運営に関する法律および施行令」、「海外不法サイト遮断関連業務の処理指針」といったものを定められている。

ブロッキングに関して法的な義務があるのは、海外インターネット接続設備を保有した 8 ケ機関、別定通信事業者など、放送通信委員会で「海外不法サイト遮断関連是正命令および取り扱い制限命令および協力要請」対象業者に指定された ISP となっている。

ブロッキングの根拠となる「情報通信網利用促進および情報保護などに関する法律」の「第 44 条の 7」は 2007 年 7 月 21 日付に改正されたが、放送通信委員会は、放送通信審議委員会を通して ISP に対して、わいせつ、賭博などのサイトのブロッキング要請（是正要請）を行った。その上で、違法情報のブロッキングおよび迂回接続防止などのための長官命令権を発動して、2008 年 9 月 30 日までブロッキングを行うことを法的に義務付けられた ISP に対して、ブロッキング関連システム導入などの技術措置を完了することを指示している。

b).ブロッキングに伴う訴訟リスク

韓国では、海外ポルノサイトブロッキングについては既に判例がでている。その中で、ブロッキングは、韓国の法体系上全面的に禁止されるわいせつ物の国内流通を間接的に遮断しようとする行為であることから、既に適法だと判断されている。

違法情報のブロッキング効果を最大化するためには、まずブロッキングの法的義務が課せられている ISP が一貫性のあるブロッキング技術を適用することと、ブロッキングを各社が同時に実施することが必須となる。A 社は違法サイトをブロ

ッキングしたが、B 社はブロッキング導入が遅れたり、導入していない場合には、児童ポルノを閲覧したい利用者が、ブロッキングをしている A 社からブロッキングしていない B 社へ移ってしまうといった企業間での顧客離脱や、「B 社は閲覧できるのに、なぜ A 社は閲覧できないのか」といったクレームがブロッキングを導入した A 社に対して会員から寄せられるといった可能性があるという。

現在は、違法情報のブロッキングに関連して ISP をはじめとした各種事業者において引き起こされる訴訟とクレームなどに対する責任は、各事業者に任せられている。KISPA としては、今後は、別途の政府機関に一任して、ブロッキングを実施している事業者に不利益が生じないように業務改善が必要だと考えている。

c).ブロッキング導入にあたり検討した法律

ブロッキングの伴う法的な課題として、ブロッキングの義務が課せられている事業者とそうでない事業者の不公平のいう課題もある。義務のある ISP は、海外違法サイトをブロッキングするために努力しているが、海外ネットワークを借りて使っている MSO[5]、SO、VAN 事業者[6]などには何の制裁もなく、同業の企業であるにも関わらず不公平感があり、公平性ある法適用が必要となってきている。

次に、利用者への公示、同意の課題である。URL ブロッキングでは、DNS ブロッキングやパケットドロップとは異なり、ISP は、個人のすべての国際通信パケットを閲覧し、その関連記録を保存することになる。URL ブロッキングは、国家的な要求によって一方的に行われており、利用者に対し同意を得るということは行っていない。今後、URL ブロッキングを行っていることについて、利用者、市民団体、言論団体に公開するということになれば、大きい波紋が予想されるという。KISPA では、ブロッキング実施の根拠となっている情報通信網法を修正し、このような形でのパケット閲覧で違法サイトをブロッキングすることができるという根拠を明文化し、利用者、市民団体、言論団体にブロッキングの事実を公示して同意を求めていく必要があると考えている。

最後に、司法機関および捜査機関からの情報提出要求の懸念がある。海外サーバに置かれている違法情報のブロッキングに関しては、現在でも、国家情報院、放送通信委員会、行政安全部、文化観光部、保健福祉部などの各種の国家機関から現況報告とブロッキング要求が発生してきている。今後は、司法機関および捜査機関から必要な各種資料の提出を要求されるのではないかという懸念がある。

事業者に、国の色々な政府部署を相手にして説明しなければならない負担を加

[5] MSO は、Multiple Systems Operator の略で、複数のケーブルテレビ局を運営する事業者を指す。

[6] VAN 事業者とは、データ通信用に大容量の回線を保有し、その回線を一般のユーザに切り売りするサービスを行っている事業者を指す。

重させるのではなく、URL ブロッキングに対する政府各部署の業務を一元化して政府部署の効率性を高める一方、事業者には業務負担を減らす政策が必要であると KISPA では考えている。

⑤ブロッキング導入に伴う設備投資コスト

URL ブロッキングの導入に関わる費用は、すべて ISP 各社の負担であり、KISPA 会員会社の中で URL ブロッキングを導入している 8 社の設備投資コストは、合計金額で約 300 億ウォン＝23 億円になっている。各社のネットワークの状況等によっては、URL ブロッキングそのものの設備投資以外に、別途費用がかかっているところや、URL ブロッキングの設備に標準的な機器が導入できず、導入コストが高くなってしまっているところもある。KISPA からは、韓国政府に対し、URL ブロッキングの導入に関わる費用への補助金または税制上の優遇処置を申し立てたが通らなかったという経緯がある。政府レベルでの技術開発と税制支援などの対策必要と考えているという。

エ．海外 ISP 調査結果の比較表

調査項目		ノルウェーTelenor	英国BT	韓国KISPA
経緯	導入方式	○DNSブロッキング	○ハイブリットフィルタリング方式のClean Feed System（以下CFS）	○URLブロッキング(下位ディレクトリおよびページ単位まで遮断)
	導入年度	○2004年	○2004年	○2009年
ブロッキングの動作および運用	基本的なブロッキングの動作	○利用者のコンピュータから、ブロッキングリストに掲載されたサイトへの接続リクエストがあった場合は、通常のDNSサーバから見せかけのKID権威DNSサーバへフォワードされ、KID Webコンテンツサーバの IPアドレスが返される。利用者のコンピュータは、もともと要求していたサイトではなく、KID Webコンテンツサーバを閲覧しにいき、警告ページが表示される	○利用者のコンピュータから、ブロッキングリストに掲載されたサイトへの接続リクエストがあった場合は、ルータ・リダイレクションを使い、BGPルータで入ってくる通信をチェックし、IPアドレスが該当する通信はCFSに向け直す。CFSのシステムにキャッシュがあり、そこでIWFのリストとのマッチングが行われ、（透過型プロキシ）、マッチすれば、404エラーをだし、マッチしなければ、そのキャッシュから対象サイドに送信する	○利用者のコンピュータから、ブロッキングリストに掲載されたサイトへの接続リクエストがあった場合は、TAPによりそのトラフィックをTS Plusというトラフィック分析のための機器に振り向け、保存されているブロッキングリストとの比較を行い、ブロッキングの有無を決定する。利用者が接続しようとしたURLが、ブロッキングリストに掲載されている場合は、接続が遮断され、警告ページが表示される
	ネットワークのどこでブロッキングを行っているか	○数台あるDNSサーバのうち1台	○UKのグローバルバックボーンに直結しているBGPルータ	○国際ゲートウェイ（借りている回線も含む）
	ブロッキング実施に必要な情報項目	○ドメイン名	○URL	○URL
	ブロッキングリストの書き換え及びシステム更新	○自動	○自動	○自動
	DNSサーバや基幹ルータの数	○DNSサーバは数台（詳細は開示できない）	不明	不明
ブロッキングの技術的課題	ブロッキングの回避	○迂回方法あり	○迂回方法あり	○迂回方法あり
	オーバーブロッキングの事例	○事例あり －ブロッキングリスト作成段階における問題	○事例あり（Wikipedea） －ブロッキングリスト作成段階における問題	不明
	オーバーブロッキングの可能性	○上記事例はリストの問題 －Telenorは、リストに全く触れずに利用	○上記事例はリストの問題 －BTは、リストに全く触れずに利用	不明
	ネットワーク障害の可能性	○導入から現在までインフラ部分で技術的な問題は発生していない －発生するとしても、不正なサイトにアクセスを試みている人に対する応答速度が低いか応答がないだけ －人為的なミスによって壊れたファイルを追加しても、適用されない仕組み	○導入から現在までインフラ部分で技術的な問題は発生していない －万が一、障害が生じた場合は、BGPルータのレベルでルートを変えて、CFSに振り向けていたトラフィックをそのまま通せば、障害はなくなる（FailOpenStructure）	不明
	その他、ISP業務実施の上で障害となる問題や困難な点	○特になし	○WEBサイトによっては、DOS攻撃の保護機能により、キャッシュがブラックリストに入る	○違法情報のブロッキング効果を最大化するためには、一貫性のあるブロッキング技術の適用とブロッキングの同時施行が必須だが、ブロッキングの義務が課せられている事業者とそうでない事業者の不公平が存在
ブロッキングの法的課題	関連法令	不明	○1978年児童保護法（2003年性犯罪法により修正） ○1988年刑事司法法第160条	○情報通信網利用促進および情報保護などに関する法律(第49条秘密の保護） ○情報通信網利用促進および情報保護などに関する法律（第44条の7不法情報の流通禁止） ○電気通信事業法 ○放送通信委員会の設置および運営に関する法律および施行令 ○海外不法サイト遮断関連業務の処理指針
	ブロッキングを行うことの法的な義務	○法的な義務はなし	○法的な義務はなし	○法的な義務あり
	ISPに対する訴訟の可能性	○訴訟になったことはない －クレーム対応は警察	○訴訟になったことはない －クレーム対応は内務省	○海外ポルノサイトブロッキング関連の判例では、ブロッキング行為は適法だと判断されている
	ブロッキング実施に当たって検討した法律や事項	○ブロッキング対象が児童ポルノコンテンツから広がってしまう可能性 ○誰がブロッキングリストを作成し、Telenorは作成に関与せずにいられるかといった問題 ○ブロッキングの実施段階で、Telenorが対象コンテンツを見ない、利用者を特定するため情報は記録も転送もしないということが可能かという問題	○児童ポルノをブロックすることは、まだ法律的に未審理の状態であり、トラフィックをintercept（傍受）すること、通信を遮断することが、通信事業者の義務に反するのではないかという法的リスクも伴うという認識のもとで、BTでのブロッキング実施が社内で承認された	○URLフィルタリングの実施には、国際通信パケットを閲覧し、事業者はその関連記録を保存する。国家的な要求によって行われることであるため、今後顧客や市民団体、言論団体に公開される場合、大きい波紋が予想され、同意を求める必要がある ○国際区間での不法情報の遮断に関連して、司法機関および捜査機関から必要な各種資料の提出を要求することなどの懸念がある
ブロッキング導入に伴う設備投資コスト	ISPの規模	○ダイヤルアップ、xdsl、ケーブルモデム、モバイルのすべてのアクセス手段全体で300万のアクセス顧客（複数のアクセス手段所持も含む）が存在	○2009年3月末時点の一般消費者向けのブロードバンド顧客は4800万人（IPTV、WiFiなどのサービスも含む）	○ISPにより異なる
	初期投資費用、年間運用費用	○初期投資費用は、約5,000ユーロ（1ユーロ150円で75万円）程度 ○年間運用コストは、1台のサーバをホスティングして運用するコストのみ	○初期投資費用は約50万ポンド（1ポンド150円で7500万円）程度 ○年間運用コストは不明	○KISPA会員会社の中でURLブロッキングを導入している8社の設備投資コストは、合計金額で約300億ウォン＝23億円程度 ○年間運用コストはISPによって異なる
	ブロッキング実施のための人数と工数	○通常のWebサーバと通常のDNSサーバの維持に必要な作業と、更新時のDNSの構成に関する作業のみ ○フルタイムの工数を1とした場合に、0.2の工数	○ブロッキングの部分だけというのはわからない	不明

（２）「表現の自由」に係る判例

憲法では「第 21 条　集会・結社・表現の自由、検閲の禁止、通信の秘密」において、「1 集会、結社及び言論、出版その他一切の表現の自由は、これを保障する」「2 検閲は、これをしてはならない通信の秘密は、これを侵してはならない」と定められている。

一方で、「児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律」では、「第七条　児童ポルノ提供等」において、「児童ポルノを提供した者は、三年以下の懲役又は三百万円以下の罰金に処する。電気通信回線を通じて第二条第三項各号のいずれかに掲げる児童の姿態を視覚により認識することができる方法により描写した情報を記録した電磁的記録その他の記録を提供した者も、同様とする。」と定められている。このように、児童ポルノを電気通信回線を通じて提供することは法律で禁止されており、違反したものに刑罰が科せられることから、児童ポルノを掲載した者の「表現の自由」は既に制約されているといえる。

これについては、既に多くの判例が出されており、以下に判例の一部を示す。

①児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律違反、組織的な犯罪の処罰及び犯罪収益の規制等に関する法律違反被告事件（最高裁判所 平成 20 年 11 月 4 日　平成 20 年(あ)第 865 号）

この事件は、被告人が、児童ポルノＤＶＤを不特定多数の者に有償で提供し、犯罪収益であるＤＶＤ代金を被告人が管理する借名口座に振り込ませ、犯罪収益等の取得につき事実を仮装したというものである。

判決文には、

(1) 所論は、原判示第１の２の児童ポルノ提供目的所持罪について、同判示の外付けハードディスク自体を販売する目的がなかった被告人には同罪が成立しないのであり、これを処罰する原判決は、表現の自由を不当に侵害する点で憲法 21 条に違反し、財産権を侵害する点で憲法 29 条１項にも違反する、というのである。

しかしながら、関係証拠によれば、被告人は、本件外付けハードディスク自体を販売する目的はなかったけれども、必要が生じた場合には、本件外付けハードディスクに保存された画像データを使用し、これをＤＶＤに記憶させた上、このＤＶＤを販売する意思であったことが認められるから、本件外付けハードディスクの所持は、児童ポルノを提供する目的で行われたものということができる。また、児童の心身に有害な影響を与え、その成長にも重大な影響を及ぼす行為を防止し、児童を性欲の対象としてとらえる風潮を抑止するという児童買春、児童ポ

ルノに係る行為等の処罰及び児童の保護等に関する法律（以下「児童ポルノ法」という。）の立法趣旨等に照らすと、同法による処罰をすることにより、人権に制限が加えられたとしても、それは公共の福祉による合理的な制限であって、この点が憲法の諸規定に違反するなどといえないことは明らかである。

と示されている。

②児童売春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律違反、関税法違反被告事件（名古屋高等裁判所 平成 18 年 5 月 30 日 平成 18 年(う)第 67 号）

この事件は、被告人が 6 回にわたり、タイ王国から日本に向けて児童ポルノを輸出し、その購入者と共謀の上、輸入禁制品である児童ポルノを輸入しようとしてこれを遂げなかったという児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律違反及び関税法違反被告事件である。

判決文には、

所論は､児童ポルノの外国からの輸出を処罰する児童ポルノ処罰法 7 条 6 項は、有体物の場合のみを処罰する点で不合理な差別であって憲法 14 条 1 項に違反し無効であり、また、有体物に化体した情報の流通についてのみ重く処罰することは表現の自由に対する不当な制限であって憲法 21 条に違反し無効であるから、原判決は違憲、無効な処罰規定を適用した法令適用の誤りがある、というのであるが、児童ポルノ処罰法 7 条の法意に照らし、同条 6 項が憲法 14 条 1 項、21 条に違反しないのは明らかであり、この点につき原判決には法令適用の誤りはない。所論は独自の見解であり、理由がない。

しかしながら、児童ポルノ処罰法 7 条 6 項の輸出の意義は、前記 3 項に説示したとおりであるが、これについては一般人が社会通念に照らし容易に看取し得るところである上、同法 7 条 6 項の目的は、同条 4 項に掲げる行為の目的とされており、その行為は同条 4 項に明示されているから、児童ポルノ処罰法 7 条 6 項の犯罪構成要件が漠然不明確であり憲法 21 条（又は同 31 条）に違反し無効であるとはいえない。よって、この点につき原判決には法令適用の誤りはない。所論は前提を欠き、理由がない。

しかしながら、前記のとおり、児童ポルノ処罰法 7 条 6 項は、外国の児童が児童ポルノの描写の対象とされて性的に搾取されている実情があることなどにかんがみ、これに対する国際的な対処の必要から、日本国民が同条 4 項に掲げる行為

（児童ポルノの提供など）の目的で児童ポルノを外国に輸入する行為及び外国から輸出する行為をも処罰の対象にし、他方、関税法 109 条は、社会公共の秩序、衛生、風俗、信用その他の公益の侵害を防衛する目的で、関税定率法 21 条 1 項各号に掲げる輸入禁制品の輸入を防止するために規定されたものであって、それぞれの立法趣旨に照らし合目的的に、必要かつ相当な限度において処罰の範囲及びその要件を定めているものと解されるところ、所論の指摘する児童ポルノに関する関税法、関税定率法の規定が過度に広汎な規制であって、憲法 21 条に違反するとはいえないから、この点につき原判決には法令適用の誤りはない。所論は独自の見解であり、理由がない。

と示されている。

③わいせつ図画販売、同販売目的所持、児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律違反被告事件（最高裁判所　平成 18 年 2 月 20 日　平成 17 年(あ)第 1342 号　）

この事件は、被告人に対するわいせつ図画販売、同販売目的所持、児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律違反被告事件である。

判決文では、

上告趣意のうち、児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律（以下「法」という。）7 条 3 項の規定について憲法 21 条、35 条違反をいう点は、上記規定中の「姿態をとらせ」という文言が所論のように不明確であるとはいえず、上記規定が表現の自由に対する過度に広範な規制であるということもできないから、所論は前提を欠き、判例違反をいう点は、事案を異にする判例を引用するものであって、本件に適切でなく、その余は、憲法違反をいう点を含め、実質は単なる法令違反、事実誤認の主張であって、刑訴法 405 条の上告理由に当たらない。

と示されている。

④児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律違反被告事件（東京高等裁判所　平成 17 年 12 月 26 日　平成 17 年(う)第 2131 号）

本事件での判決文では、

そうすると、児童に法二条三項各号に規定する姿態をとらせて児童ポルノを製造する行為を処罰する法七条三項の規定が、過度に広汎な規制であって表現の自由を保障した憲法二一条に違反するものとはいえない。また、法七条三項にいう「姿態をとらせ」との文言は漠然不明確であるなどとの論旨についても、「姿態をとらせ」とは、行為者の言動等により児童が当該姿態をとるに至ったことをいい（所論のいう盗撮の事案はこれに含まれないことは文言上明らかであり、なお、本件はもとより所論のいう盗撮の場合とは事案を異にしている。）、併せて、法二条三項各号においてその姿態の内容が明記されているのであって、その文言は一般通常人が具体的場合に当該行為がその適用を受けるかどうかを判断することが可能な基準を示しているということができ、何ら不明確であるとはいえないのであるから（最高裁昭和五〇年九月一〇日大法廷判決・刑集二九巻八号四八九頁）、所論はいずれも採用できない。

⑤わいせつな図画である写真集を販売し、さらに販売目的で同様の画像データ等を記憶、蔵置したコンピュータのハードディスクを所持したほか、児童買春をするとともに児童ポルノを製造したという事案（名古屋高等裁判所金沢支部 平成17年6月9日　平成 17 年(う)第 12 号）

本事件は、被告人が、不特定の 3 名に対し、わいせつな図画である写真集を販売し、さらに販売目的で同様の画像データ等を記憶、蔵置したコンピュータのハードディスクを所持したほか、児童買春をするとともに児童ポルノを製造したという事案である。

判決文では、

1　法が憲法に違反する旨の各所論について（控訴理由第 1 ないし第 3）

（1）所論は、法 7 条 3 項は、真剣な交際をしている者が、児童の承諾のもとでその裸体を撮影する行為、16、17 歳で婚姻した夫婦間での撮影をも処罰の対象にする点で、過度に広汎な規制であるから、憲法 21 条に違反して違憲無効であるとする。しかし、過度に広汎な規制で憲法 21 条に違反するとの所論は採用しがたい上、記録によれば、本件は、所論が指摘するような場合でないことは明らかであるから、本件に適用する限りでは何ら憲法 21 条に違反するものではない。

（2）所論は、法 7 条 3 項の「姿態をとらせ」との文言は漠然不明確であり、憲法 35 条に違反して違憲無効であるとする。しかし、「姿態をとらせる」という文言は、児童に働きかけて法 2 条 3 項各号に規定する姿態をさせることであることは通常人であれば容易に理解することができるのであり、何ら漠然不明確ではない。

と示されている。

⑥児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律違反、わいせつ図書販売目的所持被告事件（大阪高等裁判所　平成 12 年 10 月 24 日　平成 12 年(う)第 649 号）

本事件での判決文では、

しかし、児童ポルノ法は、児童に対する性的搾取及び性的虐待が児童の権利を著しく侵害することの重大性にかんがみ、児童買春、児童ポルノに係る行為等を処罰するとともに、これらの行為などにより心身に有害な影響を受けた児童の保護のための措置等を定めることにより、児童の権利を擁護することを目的としている（法 1 条）ところ、児童買春の当事者となったり、児童をポルノに描写することは、その対象となった児童自身の心身に有害な影響を与えるのみならず、そのような対象となっていない児童においても、健全な性的観念を持てなくなるなど、児童の人格の完全かつ調和のとれた発達が阻害されることにつながるものであるから、児童ポルノ法は、直接的には児童買春の対象となった児童や児童ポルノに描写された児童の保護を目的とするものであるが、間接的には、児童一般を保護することをも目的としていると解される。したがって、このような同法の立法趣旨にかんがみると、18 歳未満の者を一律に児童とした上で、児童買春や児童ポルノを規制する必要性は高いというべきであるから、法 2 条 1 項が表現の自由に対する過度に広範な規制を定めたものとは言えないし、また、そのために所論にいわゆる児童の性的自己決定権が制約されることになっても、その制約には合理的な理由があるというべきであるから、同条項が憲法 13 条に違反するとも言えない。

と示されている。

⑦児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律違反、わいせつ図画販売目的所持被告事件（最高裁判所　平成 14 年 6 月 17 日　平成 12

年(あ)第 1769 号)

本事件での判決文では、

2　同弁護人の上告趣意第 4 前段、第 6 及び第 7 は、法 2 条 3 項 2 号、3 号にいう「性欲を興奮させ又は刺激するもの」の文言があいまいで不明確であるから、憲法 21 条、31 条に違反するというが、上記文言は、一般の通常人が具体的場合に当該行為がその適用を受けるかどうかを判断することが可能な基準を示しているということができ、不明確であるとはいえないから、所論は前提を欠き、適法な上告理由に当たらない。

と示されている。

⑧NTT 脅迫電報事件判決(平成 16 年7月7日大阪地裁判決)

主文

1　原告らの請求をいずれも棄却する。

2　訴訟費用は原告らの負担とする。

事実及び理由

第1　請求

1　甲事件請求

甲事件被告（以下「被告NTT西日本」という。）は，甲事件原告らに対し，それぞれ20万円及びこれに対する平成15年9月23日から支払済みまで年5分の割合による金員を支払え。

2　乙事件請求

乙事件被告（以下「被告NTT東日本」という。）は，乙事件原告らに対し，それぞれ20万円及びこれに対する平成16年2月28日から支払済みまで年5分の割合による金員を支払え。

第2　事案の概要

本件は，原告らが，電報の発信の委託を受けた被告NTT東日本及びこれを原告らに配達した被告らに対し，同電報が違法な金融業者又は債権取立業者からの債務者に対する脅迫を内容とするものであるところ，被告らには電報の発信の受付ないし電報の配達を差し止めるべき義務があり，かかる措置を採らなかった被告ら又はその従業者の不作為が違法である旨主張して，不法行為に基づく慰謝料の支払を求めた事案である（附帯請求は，各事件の訴状送達の日の翌日から支払済みまで民法所定年5分の割合による遅延損害金請求である。）。

第3　前提事実（証拠を付さない事実は，当事者間に争いがない。）

1　当事者

被告らは，日本電信電話株式会社等に関する法律（昭和59年12月25日法律第85号，以下「NTT法」という。）に基づき設立され，地域電気通信事業を営む株式会社である。

原告らは，多数の金融業者から多重に金員を借り入れ，支払遅滞ないし不能の状態となっている，いわゆる多重債務者である（弁論の全趣旨）。

2　電報の事業の概要及び被告らにおける電報の取扱い

(1)　被告らは，電気通信事業法（昭和59年12月25日法律第86号）上の第一種電気通信事業者に当たり，電報の事業を行う会社である。NTT法は，被告らの行うべき地域電気通信業務の地域につき，被告NTT東日本については北海道，青森県，岩手県，宮城県，秋田県，山形県，福島県，茨城県，栃木県，群馬県，埼玉県，千葉県，東京都，神奈川県，新潟県，山梨県及び長野県（以下「東日本地域」という。）において，被告NTT西日本については京都府及び大阪府並びに東日本地域以外の県（以下「西日本地域」という。）において，それぞれ地域電気通信業務を行うものと規定している（2条3項）。

(2)　電報の事業は，電気通信事業法上，配達の業務を含め，第一種電気通信事業とみなされ，被告らの行う電報の取扱いの役務は電気通信役務，当該役務の提供の業務は電気通信業務とそれぞれみなされ，同法が適用される（同法附則5条1項）。

(3)　西日本地域において配達される電報につき，東日本地域において発信が受け付けられる場合，電報の発信の受付は被告NTT東日本の担当者が行い，被告らの間の協定に従い，電報の内容が被告NTT西日本に送信され，これを受信した被告NTT西日本の配達担当者が電報をその宛先に配達することとされている。

3　電報配達の受付，配達及び電報の内容

(1)　被告NTT東日本は，別紙[7]電報一覧表「発信者名」欄記載の者らから，それぞれ同一覧表「電報の種類　お届け台紙名」欄記載の種類による電報（以下「本件各電報」と総称する。）の配達を受け付けた。被告NTT東日本は，本件各電報のうち配達先が西日本地域に属するものについて，配達先を管轄する被告NTT西日本との協定に基づき，被告NTT西日本に本件各電報の受付内容を伝達し，被告らの配達担当者は，同一覧表「発信日」欄記載の各日において，各被告の取扱区域に応じ，本件各電報を同一覧表原告欄記載の各原告の住所又は勤務先に宛てて配達した（弁論の全趣旨）。

(2)　本件各電報の内容は，別紙[7]のとおりである（弁論の全趣旨。各電報に

---

[7] 別紙については掲載しておりません。

付した丸囲み番号は，別紙[7]電報一覧表番号欄に対応するものである。）。

第4　争点及び当事者の主張

1　被告らないしその従業者らには，一般的に，電報の内容が他人に対する害悪の告知を内容とする場合に，電報の受付を拒否し，又は配達を差し止めるべき義務があるか。

(1)　原告らの主張

ア　作為義務の内容

被告らは，慶弔電報及びキャラクター電報（以下「慶弔電報等」と総称する。）につき，電報受付から配達までの過程において，電文内容が一見して明らかに脅迫文言を含むものであることを覚知した場合には，損害防止のために電報の受付を拒否し，又はその配達を差し止めるべき義務がある。

イ　作為義務の根拠

発信者たるヤミ金融業者ないし違法な債権取立業者と被告らとの関係は，準委任契約に基づく契約関係であるところ，脅迫電報の配達を内容とする契約は公序良俗に反し許されない。そして，電気通信事業という公益事業に従事する被告らには，条理上，一般人にもまして，事業の遂行により他人の権利を侵害しないよう注意すべき義務があるところ，被告らが脅迫電報を配達することにより，それを受け取る私人は，社会生活において他者から侵害行為を受けず，安全かつ平和な生活を享受する法益が侵害されることになる。したがって，被告らには，民法90条に基づき，又は条理上，脅迫文言を含む慶弔電報等の受付又は配達を差し止めるべき義務がある。

ウ　検閲の禁止（憲法21条2項前段，電気通信事業法3条）との関係

(ア)　そもそも，被告らは私企業であって，検閲の主体となり得ないから，被告らの採るべき措置が検閲の禁止に抵触しないことは明らかである。

(イ)　原告らは，被告らが，その受け付けたすべての電報の内容を1枚ずつ監視すべきであるというような閲覧監視義務を負う旨の主張をしているのではない。すなわち，電報の受付におけるオペレーターの作業から電報配達人による配達までの過程において，被告らないしその従業者らが電文内容を覚知する機会があるはずであるところ，電文が一見して明らかに脅迫文言を含むことを覚知した場合に，そのような脅迫的・犯罪的な内容の電報に限定して，受付を拒否し，又は配達を停止すべき義務を負うと主張しているに過ぎない。

(ウ)　また，原告らの主張する被告らの作為義務は慶弔電報等についてのみのものである。なぜなら，これらの電報は，その性質及び慣習上，伝達されるべき電文の内容が限定されており，また，電報取扱担当者において電報を受信ないし配達する際，その内容の不当性を確認する可能性が高い。また，これらの電報を

[7] 別紙については掲載しておりません。

受領した脅迫被害者において発生する恐怖心が大きいからである。したがって，電報一般に対してまで，その内容を確認して受付ないし配達を差し止めるべき義務があると主張するものではない。

（エ） したがって，被告らがかかる措置を採ることは，一般的・網羅的に通信内容を審査するものではないから，検閲に該当せず，禁止されていない。

エ　通信の秘密（憲法21条2項後段，電気通信事業法4条）との関係

通信の秘密の不可侵とは，＜１＞通信の秘密に属する通信内容や事務上の事項について調査・探求をなし得ないこと（積極的知得行為の禁止），及び＜２＞通信事務取扱者が通信の秘密について知り得たことを守秘すべきこと（漏洩行為の禁止）を意味するところ，被告らが負う作為義務の内容は，特定の内容の電報を受け付け，又は配達しないというものであって，積極的に通信内容を知得したり，漏洩行為をする義務があると主張するものではない。

また，ヤミ金融業者が脅迫電報を発信することは，公序良俗に反する犯罪的な表現を目的とする行為であり，このような犯罪的な表現に関する通信の秘密は，表現の自由に対する内在的な制約として，保障されるべきではない。むしろ，脅迫電報を配達されることにより被る被害者の生命，身体，精神的な侵害を保護すべき社会的な要請が高いというべきである。

したがって，被告らの採るべき上記措置は，通信の秘密の侵害となるものでもない。

オ　電気通信事業法7条，34条との関係

本件のような害悪の告知を内容とする不当な電報については，公序良俗違反を理由に受付及び配達を拒否しても不当な差別に当たらず，また，役務の提供を拒絶すべき正当な事由があるから，同法7条（提供義務）及び34条（利用の公平）に反することにならず，むしろ，電気通信事業という公益を遂行する者として，受付及び配達を拒否すべき作為義務を負うというべきである。

(2)　被告らの主張

ア　原告らは，被告らが民法90条に基づき受付及び配達を拒否すべき作為義務を負う旨主張するが，同条は，公序良俗に反する法律行為を無効とするに止まるものであって，作為義務を課すべき根拠たり得ない。

また，仮に電報発信者と被告らとの間における電報の受付に係る契約について民法90条違反が存在するとしても，原告らはその契約当事者でないから，直ちに被告らの原告らに対する作為義務を基礎づけるものとはならない。

イ　原告らの主張によれば，慶弔電報等の配達に先立ち，被告らないしその従業者が，受け付けた電報の一切につき自ら電文の内容を閲覧して検討・審査し，その結果に基づき配達の可否を決定することがその前提行為として不可欠なものとなる。

しかしながら，憲法21条を受けた電気通信事業法4条1項は，電気通信事業者の取扱中に係る通信の秘密の侵害を禁止し，その違反に対する罰則を設け（同法179条1項〔平成15年7月24日法第125号改正前の104条1項〕），さらに，電気通信事業従事者に対しては刑が加重されている（同条2項）。

また，電気通信事業法やNTT法には，原告らが主張するような閲覧・審査を義務づける規定はおろか，これを許容するような例外規定も何ら存在しない。

電文の内容は通信の秘密の核心をなすものであるところ，原告らの主張は，被告らに対し，まさに憲法21条及び電気通信事業法に違反して通信の秘密を侵害することを求めるものにほかならず，到底成り立ち得ないものである。

ウ　電気通信事業法7条は，電気通信事業者に対し電気通信役務の提供について不当に差別的な取扱いをすることを禁止しており，同法34条は，正当な理由なく電気通信役務の提供を拒むことを禁止している。

したがって，電気通信事業者は，利用者の通信内容の如何によってサービスの提供を拒絶することができないから，この点においても，本件において，被告らが電報の受付及び配達を拒否すべき法律上の義務及び権限が存しない。

エ　以上のとおり，被告らが，電報の内容に鑑み，その受付及び配達を差し止めるべき義務を負う余地はないというべきであるから，原告らの主張は失当である。

2　本件各電報のうち，別紙[7]の各電報は，客観的に，原告らに対する脅迫を内容とする違法なものといえるか。

(1)　原告らの主張

本件各電報は，いずれも，いわゆるヤミ金融業者ないしこれらの業者から債権回収の委任を受けた違法な債権取立業者が，原告らないしその家族を脅迫する内容のものであるから，違法性がある。

(2)　被告らの主張

電報の表示内容については，被告らにおいて内容を確認できないため不知といわざるを得ないが，電報の文面を前提としても，別紙[7]の電文が客観的に違法な脅迫を内容とするものと断定できるかは疑問である。

3　争点1，2を前提として，被告らないしその従業者が，本件各電報の受付を拒否せず，又は配達を中止しなかったことにつき，違法性があるか。

(1)　原告らの主張

ア　本件各電報の文言は，一見して明らかに脅迫的・犯罪的な内容であり，慶弔電報等の内容といえないものである。また，本件各電報の中には，お祝い電報とお悔やみ電報が同一日付けで同一の名宛人に発信されたり，日を違えて何通も

7 別紙については掲載しておりません。

発信されていたものも含まれている。したがって，被告らないしその従業者は，本件各電報が慶弔電報としては異常なものであり，ヤミ金融業者の債権回収目的による違法な脅迫を内容とする電報であることを理解できていたはずである。

イ　被告らは，マスコミを通じ，又は「全国ヤミ金融対策会議」からの申入れ文書を受けたことにより，ヤミ金融業者による脅迫電報を悪用した違法行為が横行していた事実を認識し，その防止を求められていたものである。にもかかわらず，被告らが漫然と本件各電報を受け付け，又は配達したことにより，ヤミ金融業者による不法行為を助長したものである。

ウ　したがって，被告らが本件各電報の受付を拒否せず，又は配達を差し止めなかったのは，被告らの上記作為義務に違反するものであり，違法である。

(2)　被告らの主張

ア　通信の秘密との関係上，被告らは，本件各電報がヤミ金融業者から委託を受けたものであるかどうか，また，電文が原告らに対する脅迫を内容とする電報であるかどうかを積極的に知得すべき立場にないし，現に電文の内容を把握していたものでもない。

イ　また，被告らは，ヤミ金融業者の慶弔電報等に対し，通信の秘密に抵触することなく速やかに実施し得る対策として，平成15年4月下旬から，電報の内容にかかわりなく全ての電報を受け取らない旨予め申し出る方法により，包括的に電報の受取を拒否することができる取扱いを開始し，同年5月21日付けで一般に公表し，利用者向けの告知を行う等の広報活動を行っている。

したがって，電報の受取を希望しない場合，かかる包括受取拒否の取扱いを利用することにより，ヤミ金融業者からの電報を受け取らないようにすることができる。

ウ　したがって，被告らないしその従業者が本件各電報の受付を拒否せず，又は配達を中止しなかったことに違法性はない。

4　被告らの不作為が違法である場合，これによる原告の精神的損害の有無及びこれに対する慰謝料額。

(1)　原告らの主張

原告らは，多数の債権者や違法な取立業者から日常的に債権取立てを受けて畏怖し，不安な生活を送っている社会的弱者であるところ，本件のような脅迫電報の配達を受けることにより，精神的に追い込まれ，ノイローゼ又はパニック状態に陥り，時には思いあまって自己の生命を絶つおそれさえある。

被告らの措置は，電報を受ける側の精神的事情を何ら考慮しなかったものであり，これにより，原告らに回復不可能な程度の精神的苦痛を負わせた。かかる精神的苦痛に対する慰謝料の額としては，各原告につき20万円が相当である。

(2)　被告らの主張

原告らの主張は争う。

第5　当裁判所の判断

1　争点1（被告らの作為義務の有無）について

(1)　原告らの主張は，要するに，被告らが受け付け，又は配達した慶弔電報等につき，その電文が明白に他人に対する害悪の告知を内容としているものである場合，かかる電報の受付を内容とする契約が公序良俗（民法90条）に反することや，電気通信事業という公益事業に携わる被告らには一般人にもまして他人に対する権利侵害を防止すべき条理上の注意義務があることを根拠として，被告らに電報の受付ないし配達を差し止めるべき作為義務があるというものである。

(2)　そこで判断するに，原告らが被告らの作為義務の根拠として主張するもののうち，民法90条は，そもそも公序良俗違反の法律行為を無効とする規定に止まるのであり，それを超えて何らかの法的作為義務を根拠づけるものと解することはできない。

また，原告らが条理として主張するところは，他者に対し危害を加えてはならないという観念的，抽象的なものに過ぎず，具体的にどのような事実関係を前提としていかなる行為義務が発生するのか，その主張の根拠とするところが全く不明であって，法的作為義務の発生原因とはなし得ないものというべきである。

したがって，原告らの主張はこの点において既に失当といわざるを得ない。

(3)　また，仮に，被告らに条理上何らかの作為をなすべき一般的義務が発生すると解する余地があるとしても，本件において原告らの求める行為の内容は，通信事業者たる被告らに求めることが適当でないのみならず，かえって公共的通信事業者としての職務の性質からして許されない違法な行為を内容とするものといわざるを得ない。その理由は，以下のとおりである。

ア　原告が作為義務の内容としている被告らの行為は，要するに，被告らが受付ないし配達を行おうとする電報の電文が脅迫を内容とすることを覚知した場合に，当該電報の受付ないし配達を差し止めるべきとするものであるが，仮にそのような作為義務を認めるとすれば，被告らがそのような行為を行うためには，被告らの取り扱う電報全てにつき，事前にその内容を個別的に審査せざるを得ないことになる。

なぜなら，被告らが原告らの主張する上記作為義務を果たそうとすれば，ある電報が原告らの主張するような内容の電報であるか否か（その内容が他人に対する脅迫を内容とするものか否か）を審査し，その電報の受付を拒絶し，配達を差し止める必要があるか否かをその都度判断することが不可欠であり，結局において，取り扱う全ての電報に対して予めその内容を個別的に審査し，検討しなければ，その義務を全うすることができなくなる関係にあるからである。

イ　ところで，被告らのような電気通信事業者が提供する電気通信役務とは，

電気通信設備を用いて他人の通信を媒介し，その他電気通信設備を他人の通信の用に供することをいうものとされている（電気通信事業法2条2号）。

すなわち，電気通信事業者は，利用者間で通信が行われるに際し，あくまでも物理的な通信伝達の媒体ないし手段として，発信者から発信された通信内容をそのまま受信者に伝達することが，その提供する役務の内容として予定されているものである。

そうすると，電気通信事業者ないしその従業者が電気通信役務を提供するに際し，その取扱いの過程において通信内容を事実上覚知することがあり得るとしても，その通信に係る情報の内容面については全く関知せず，受信者にそのまま伝達することが当然に求められているものである。したがって，電気通信事業者ないしその従業者が，その取扱いの過程において，通信の内容を何らかの方法で把握し，審査することも全く想定されていないところであると解すべきである。

けだし，電報や葉書などの公共的通信手段においては，通信内容が密封ないし秘匿されておらず，その性質上通信の過程で通信事業者ないしその従業者の目に触れることが避けられないものであるが，それにもかかわらず，このような通信手段が広く利用され，社会において大きな役割を果たしているのは，通信事業者ないしその従業者が，通信の内容面については一切関知せず，物理的伝達手段としての役割に徹するものであることが，社会一般に認知され，信頼されているからにほかならない。

ウ　しかるに，原告らの主張するような作為義務を電気通信事業者である被告らに課するとすれば，被告らとしては，前示アのとおり，取り扱う全ての電報についてその内容を個別的に把握し，審査しなければならないことになるところ，このことによる社会的な悪影響は極めて重大であり，ひいては電報，葉書といった社会的に有用な通信手段の存立を危うくするものとすらいい得るものである。

なぜなら，前記のとおり，原告らが求めるような取扱いは必然的に全ての通信内容の事前審査に通じるものであり，人が通信を利用して社会的生活を営むに際し，通信の内容が逐一吟味されるものとすると，これら通信による情報伝達の萎縮効果をもたらし，自由な表現活動ないし情報の流通が阻害されることになるからである（憲法が保障する基本的人権としての通信の秘密の保護の核心は，通信内容が第三者に把握ないし審査されない点にあるものであり，結果として通信がそのまま受信者に伝達されればそれで良いというものでないことは当然である。）。

このことは，憲法21条が通信の秘密を保障し，これを受けた電気通信事業法3条，4条が電気通信事業者の取扱中に係る通信につき検閲及び通信の秘密の侵害を禁止する趣旨に鑑みても明らかである。

そして，電気通信事業法4条の違反に対しては罰則が規定され（同法179条1項〔平成15年7月24日法律第125号改正前の104条1項〕），電気通信事業に従事する者が

これに違反した場合に刑が加重されている（同条2項）のも，電気通信事業者による通信の秘密への侵害の危険が，その性質上一般人によるものに比較して一層高いものであることに鑑み，これを強く禁止する趣旨によるものと解される。このことからしても，以上の理は一層明らかであるというべきである。

エ　以上のとおり，電気通信事業者である被告らないしその従業者に一定の内容の電報の受付，配達の差止を求める原告らの主張は，電報という公共的通信手段の本質と相容れないものというべきであり，到底採用の限りではない。

(4)　ア　原告らは，被告らが受け付けた全電報を逐一監視することまで要求しているものではなく，電報の受付から配達までの過程において電文内容を覚知する機会に限定して作為義務を負うから，検閲ないし通信の秘密に対する侵害に当たらない旨主張する。しかしながら，特定の電報の内容を覚知する前提として，必然的に全電報の内容を審査の対象とせざるを得なくなることは，前示のとおりである。

イ　また，原告らは，犯罪的な内容の電報の発信者の通信の秘密は法的保護に値しない旨主張する。しかしながら，ある電報が犯罪的な内容であるか否かを把握するためには，全電報を審査の対象としなければならないことは前示のとおりであって，結局，圧倒的に多数のその他の電報利用者の通信の秘密を侵害することになるのは明らかである。

ウ　さらに，原告らは，その主張する作為義務の対象は慶弔電報等に限るから通信の秘密に対する侵害の程度が大きくない旨主張するようであるが，慶弔電報等に限って通信の秘密の保護のらち外にあるということはできないし，原告らの主張を前提としても，原告らの主張する作為義務が，一定の範疇に属する全電報につき，その内容を審査することを内容とする点において，通信の秘密に対する重大な侵害となり得ることに変わりはないというべきである（なお，乙4によれば，慶弔電報等は，現実にも被告らが取扱う電報の圧倒的多数を占めていることが窺われる。）。

(5)　なお，原告らは，本件各電報のような脅迫的電報を受け取ることにより回復不可能な程度の精神的苦痛を被ったと主張している。本件各電報の内容は，別紙[7]とおりであり（前記第3の3(2)），少なくともその大半はこれを受け取った原告らをして少なからざる恐怖感，不快感を与え，精神的苦痛を与えたものと推測するに難くなく，その点に限れば，原告らの主張にも理解し得るところがある。しかしながら，これにより本件各電報を発信した者（ヤミ金融業者又はその委任を受けた債権取立業者であると推測される。）の不法行為責任を追及するのであれば格別，公共的通信事業を担う被告らを非難し，その不法行為責任を追及するのはおよそ筋違いであるといわざるを得ない。

---

[7] 別紙については掲載しておりません。

ちなみに，原告らは配達された電報を受け取る義務があるわけでもなく，その受取を拒否することも可能である（なお，乙8の1・2，9ないし12，丙3の1・2，4ないし6によれば，現在では，事前に届け出ることにより，電報の内容にかかわらず一切の電報の受取を拒否することも可能となっていることが認められる。）から，原告らとしては，今後そのような措置を採ることにより，いわゆる脅迫電報による被害を自ら防ぐことができるようになっている。

(6)　以上のとおり，原告らの主張は，現行制度上許されない作為義務を被告らに求めるものであり，被告らないしその従業者らに原告ら主張の措置を採るべき法的義務を認める余地は全くないというべきである。

2　結論

よって，その余の争点につき判断するまでもなく，原告らの被告らに対する請求はいずれも理由がないからこれを棄却することとして，主文のとおり判決する。

（３）帯域制御に関する「通信の秘密」に係る法的な留意点

憲法では「第 21 条　集会・結社・表現の自由、検閲の禁止、通信の秘密」において、「2 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。」と定められている。通信の秘密に関しては、電気通信事業法の「第 3 条　検閲の禁止」にて「電気通信事業者の取扱中に係る通信は、検閲してはならない」、「第 4 条秘密の保護」にて「1 電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」とも定められている。

個別の通信は、代表的には次のようなものとされている。[8]

－通信内容
－通信当事者が誰であるか
－発信場所、通信の相手方
－通信の存在そのもの
－これらを実質的に推知せしめる事項

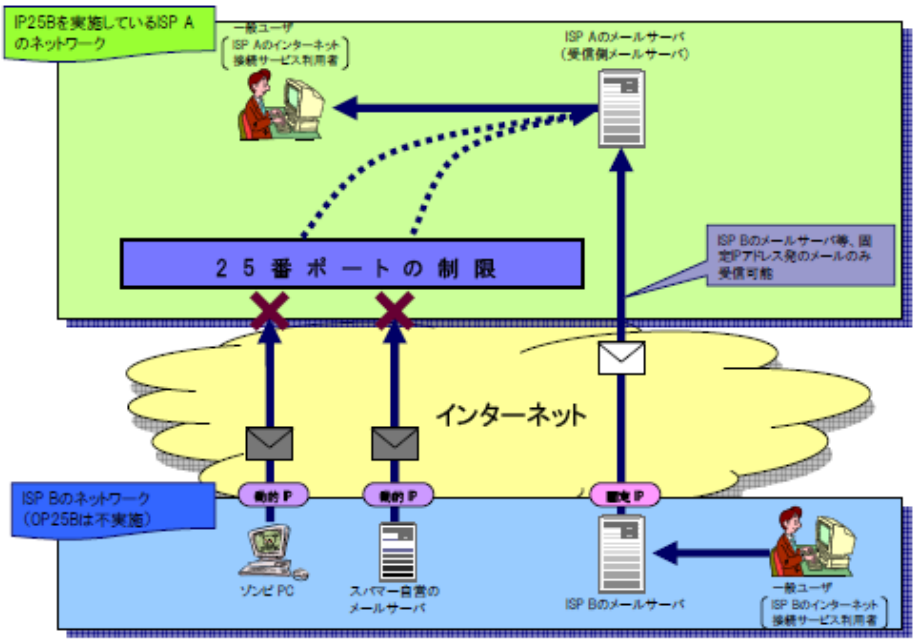
しかし、実際に通信を行う場合には、例えば、通信の相手先という内容を閲覧しなければ、相手先に届けることができない、つまり通信が成立しないことになる。そのため、「違法性阻却事由」という考えがあり、正当行為（業務上必要な知得、捜査令状による開示、プロバイダ責任制限法 4 条など）、正当防衛（自己又は他人への急迫不正の侵害からの防衛）、緊急避難（自殺予告事案における警察の情報提供、110

[8] 第 3 回ブロッキング検討委員会　野口尚志委員提出資料を参照

番の逆探知など）といった行為であれば、違法性が阻却されることになる。

違法性が阻却されると考えられると総務省が判断したものに、IP25B（Inbound Port 25 Blocking）、帯域制御などがある。IP25B は、迷惑メールを防止するために、電気通信事業者である ISP が、その支配・管理するルータを通過(流入）するすべての電子メールの送信元の IP アドレス及びポート番号を機械的に確認して、動的 IP アドレスと判断できる IP アドレス（または送信元 ISP から予め提供されている動的 IP アドレスのリストに掲載されている IP アドレス）から当該 ISP（受信側 ISP）の 25 番ポートに対して、ダイレクトに送信された電子メールを割り出し、当該電子メールをブロック（25 番ポートを閉じて接続できない状態にする）する運用をいう。

図表 12　IP25B の概要



資料出所：「Inbound Port 25 Blocking 導入に関する法的な留意点」総務省

「通信の秘密」とは、「個別の通信に係る通信内容」のほか、「個別の通信に係る通信当事者の住所、氏名、発信場所等、通信日時等の構成要素」を含む。通信の秘密を「侵害する行為」には、「発信者又は受信者の意思に反して通信の構成要素等を利用すること」（窃用すること）も含むため、電子メールの送信元の IP アドレス及びポート番号を機械的に確認するという行為は、当事者の同意がない限り、「通信の秘密」に該当すると判断された。しかし、ISP が適正にメールサービスを運営すると言う目的達成のためには、その支配・管理するルータを流入するすべての電子メールの送信元 IP アドレス・ポート番号を確認して、動的 IP アドレスから当該 ISP の 25 番ポートに対して直接送信された電子メールを割り出し、ブロックする行為は、

目的達成のために必要かつ相当な方法と認められるとして正当業務行為により違法性阻却事由があるという結論を総務省が示したことで、多くの ISP で IP25B による迷惑メール防止の措置がとられるようになっている。

帯域制御は、ISP 等が自らのネットワークの品質を確保するために実施する、特定のアプリケーションや特定ユーザの通信帯域を制限することで、P2P などの特定アプリケーションの帯域をネットワーク全体の何%までと制限し、利用料の基準を超えたヘビーユーザの通信帯域（速度）を制限する行為を指す。帯域制御においても、制御装置がアプリケーションの種類、通信の送信元、あて先を確認しているため「通信の秘密」を侵害すると判断される。しかし、帯域制御（ただし、特定のアプリケーションの通信を完全に遮断する行為は、正当業務行為と認められていない。）においても、正当業務行為にあたるとの判断を総務省が示したため、多くの ISP で実施されている。

ただし、これらの規制手法についての判例はなく、総務省の判断などを参考にしながら、自主ガイドラインを策定の上、最終的には各事業者が法務リスクを踏まえて判断の上で実施されている。

また、多くの場合、同意があれば違法性が阻却されることになる。ISP による迷惑メールフィルタリング、有害サイトフィルタリング、ウィルスチェックなどは、構成要件としては通信の秘密の侵害に当たるものの、利用者の同意（要請）があるということで、違法ではないと判断されている。