特集：情報のフィルタリング

UDC 34：342.738：007.001.37：002.5：025.4：681.3.02：02

フィルタリングと法

新保史生*

フィルタリングの利用に関する問題は，インターネット上における違法・有害情報対策との関係で論じられることが多い。とりわけ，それらへの効率的な対策を講じる上でのツールとして，技術的な側面から議論がなされることが通例である。しかしながら，情報セキュリティ対策の一環としてのフィルタリングの利用への期待も高まりと同時に法的側面からの検討も重要になっていることから，情報の選別や排除だけでなく，外部へのアクセスの遮断や情報の流通制限を含む「広義のフィルタリング」の利用に伴う法的問題について概観する。

キーワード：フィルタリング，プライバシー，個人情報保護，通信の秘密,表現の自由，情報セキュリティ

1. はじめに

「フィルタリング」の利用をめぐる問題は，インターネット上における違法・有害情報対策との関係で論じられることが多い。とりわけ，違法・有害情報への効率的な対策を講じる上でのツールとして，技術的な側面から議論がなされることが通例である。

法的な観点からの議論といえば，米国の「子供のインターネット利用保護法」[1]と呼ばれる法律をはじめとして，フィルタリングの利用を義務づける米国の法律に関する議論が中心となっている。この法律は，学校や図書館が連邦政府から“e-rate”と呼ばれる「割引料金の適用」および「ユニバーサル・サービス・プログラム」等のインターネット接続に係る財政的な間接支援や，政府による直接の財政的支援を受ける前提条件として，未成年者が利用するコンピュータのみならず，一般の利用者も利用するコンピュータも含めて，それらの機関が設置するコンピュータすべてにフィルタリング・ソフトをインストールすることを義務づけるものである。また，これを受けて，違法・有害情報のフィルタリングを目的として様々なツール[2]が法的義務を遵守するために用いられている。

一方，わが国においては，フィルタリングの利用に伴う法的問題の検討は必ずしも十分に行われてきたとはいえない状況がある。政府の対応についても，違法・有害情報への対応については様々な検討が行われてきたが[3]，フィルタリングの積極的な導入に関する議論はようやく始まったばかりといえる[4]。

しかしながら，フィルタリングを行うにあたって検討を要する事柄は多い。

違法・有害情報対策については，未成年者を対象としたフィルタリングの導入が，成人の表現の自由や知る権利の制約を伴うこともあり，政府による利用は場合によっては検閲の問題とも関係するおそれがある。

犯罪捜査，公共の安全確保，安全保障を目的とした利用については，公権力による適正な手続に基づく利用の確保が論点となる。

さらに，スパムメールのフィルタリング，ウィルス対策，不正アクセスやDDOs攻撃への対応など，外部からのアクセスに対する防御措置としてのフィルタリングの利用や，URLフィルタリングやコンテンツフィルタリングによる不適切なサイトへのアクセス制限，機密情報の漏えい防止，電子メールのモニタリング，Winnyトラフィック等の特定のトラフィックの遮断の実施による内部情報の漏えい防止など，情報セキュリティ対策の一環としてのフィルタリングの利用への期待も高い。

とりわけ，違法・有害な情報を排除することを目的として，ネットワーク上を流通する情報を対象に包括的に行われるフィルタリングではなく，特定の情報の選別や外部への流出を制御するために行われる個別的なフィルタリング（広義のフィルタリング）については，法的側面から十分な検討が行われないまま技術面や運用面での検討に重点が置かれる傾向がある。

そこで，本稿では，広義のフィルタリング技術を用いるにあたって，法的に検討を要する課題を概観したい。

2. 法的側面からみたフィルタリングの分類

フィルタリングには，それを実現するための技術手段（フィルタリング技術）の利用と，その取扱い（フィルタリングによる情報の選別）に伴う問題があるが，法的側面からの議論においては，情報の選別や排除を行う手段一般のことを「フィルタリング」と呼んでいるにすぎない。しかし，厳密に考えてみると，フィルタリングの機能に着目すると，情報の選別手段としての「フィルタリング」，選別や抽出を行う「スクリーニング」，監視や選別を行う「モニタリング」など，利用局面毎にその内容も大きく異なる。すなわち，フィルタリングについては，その機能や役割などの観点から様々な分類が考えられるが，本稿では，フィル

＊しんぽ　ふみお　筑波大学大学院　図書館情報メディア研究科
〒305-8550　つくば市春日1丁目2番地
Tel. 029-859-1336
（原稿受領　2006.8.16）

タリングに係る法的諸問題を検討するにあたって，フィルタリングの機能を以下の通り分類した上で，「広義のフィルタリング」に係る法的問題について検討を行う。

(1)最狭義のフィルタリング	情報のスクリーニング機能
	情報を一定の基準に基づいて選別し，必要な情報を抽出すること
(2)狭義のフィルタリング	一般的なフィルタリング機能
	情報を一定の評価基準で選別し，排除等を行うこと
(3) 広義のフィルタリング	情報のモニタリング機能
	情報の発信・流通過程において，一定の基準に適合または適合しない情報を自動的に選別し，不要な情報を排除し必要な情報を取得するとともに，外部へのアクセスの遮断や情報の流通を制限すること

なお，最狭義のフィルタリングおよび狭義のフィルタリングについては，主として，違法・有害情報対策との関係で様々な検討がなされ，法的観点からも主に表現の自由との関係で議論がなされてきた。

一方，広義のフィルタリングについては，情報の「選別」一般に係る問題とも関係するため，表現の自由の保障に係る問題にとどまらず，個人情報の保護やモニタリングの実施に伴う法的問題の発生など，様々な問題が関係する。つまり，情報と法の関係一般にまで検討事項は多岐にわたる。さらに，その利用に伴って利用者に対して様々な制約を課すことにもなることから，法的側面から制約を受ける権利利益についても厳密な検討が必要であり，フィルタリングの利用に伴う「法益侵害」の有無について慎重に検討を行うことが求められている。

3. 情報セキュリティの確保とフィルタリングの利用

広義のフィルタリングの利用に伴う法的問題の検討を行うにあたって，はじめに，「情報セキュリティの確保」のための利用との関係における問題を整理したい。

フィルタリング技術の利用を，情報セキュリティ確保の原則であるCIAの原則に当てはめて考えてみると，以下のようになると考えられる。

C	機密性 (Confidentiality)	フィルタリング技術を用いることによって，情報の不正流出を防止
I	完全性 (Integrity)	フィルタリングによる監視を行うことによって，ネットワークのトラフィックや情報の完全性を確保
A	可用性 (Availability)	不要な情報を排除したり，不適切な利用を遮断することによって，ネットワークの可用性を確保

社会に存在する組織は，様々な情報を取り扱っているが，個人情報の漏えい，営業秘密や企業秘密等の保護を考える上で，ネットワークの利用との関係で情報セキュリティの確保が極めて重要な課題となっている。

しかし，そのような必要性があるからといって何の手続も定めずに，直ちにフィルタリング技術を用いて何らかのモニタリングを実施することが適当ではないことは言うまでもない。情報システムのセキュリティを確保するにあたっては，不正アクセスやコンピュータ・ウィルスなど，現実の脅威に対して直ちに対応しなければならない問題にとどまらず，人的・物理的・技術的に対応すべき事項は多岐に渡るため，同時に，検討しなければならない事柄も必然的に多くなる。

さらに，情報の漏えい態様は，顧客名簿等の紙媒体の紛失等のように，明らかに紛失や漏えいを認識できる場合とは異なり，不知・不識のうちに情報の漏えい，改ざん，滅失等が発生する事例も増えている。例えば，悪質なワームに感染することによって，コンピュータ内に保存されているファイルが，当該端末のアドレス帳に登録されている第三者に勝手に送信されてしまうという事案や，Winny利用者がワーム感染することで，ファイル交換システムを介して保存されているファイルがネットワークに流通してしまうなど，今後もより一層深刻な事案の発生が懸念される。

このような漏えいの場合は，従業者の故意による漏えいではなく，システム的な問題が要因となっていて，結果的には，情報システムの運用にあたって適切なセキュリティ対策を講じていなかったことが要因であり，管理責任を問われることもあり得る。

以上のように，情報システムのセキュリティを確保することは，極めて重要な課題となっていることから，その一環として，適切な管理を実施する上で，利用状況やアクセス制限等を実現するために，フィルタリング技術を用いることで監視を行う必要性が出てくるといえる。

4. フィルタリングの利用と憲法

情報セキュリティの確保を目的としたフィルタリングの利用に見られるように，一般的に，フィルタリング技術は，民間の事業者において利用されることが多い。しかし，ネットワークの発達に伴い，公権力による利用機会も増えつつある。その場合，フィルタリングの利用は憲法上の問題を生起させることになるが，憲法論としてフィルタリングの利用について論じると，民間の事業者にとっては，自らの問題とは別次元の問題でしかないと認識されがちである。しかし，新たな技術を利用するにあたっては，個人の基本的人権を侵害しないことが大前提であり，その上で，法律上保護される利益を侵害しないための適切な仕組みと運営が求められる。したがって，フィルタリングの利用に伴い最低限度検討しなければならない問題として，まずは，憲法上保障される権利の侵害の有無について検討することが重要といえる。

政府がフィルタリングを行う場合には，憲法上保障される個人の基本的人権との関係において，いかなる人権が侵害される可能性があるのか，侵害される可能性がある場合

には，どのような問題が生ずるのか慎重な検討を行うことが不可欠である。なぜなら，公権力による強制力をもったフィルタリングの導入は，政府による集中管理社会の実現による弊害や，個人の表現の自由の制約など民主主義社会の根幹を揺るがしかねない事態さえ生ずるおそれもあり，個人の権利が大きく制約を受けることさえある。現に，一部の国では，政府がネットワーク上の情報のフィルタリングを行っている国があることは周知の通りである。

政府によるフィルタリングの利用に伴う憲法上の論点を整理すると，①プライバシーの権利の保障，②通信の秘密の保障，③表現の自由の保障，④適正手続の保障，⑤個人情報の保護などの問題が生ずる。(③表現の自由の問題については，違法・有害情報規制の問題との関連における議論が中心であることから本稿ではとりあげない)

なお，これらの問題は，憲法上の権利の保障との関係における問題であることから，私人間における問題，つまり，私人がフィルタリングを用いる際の問題には直接適用されるものではない。しかし，憲法の「趣旨」は，間接的に私人間においても適用（間接適用）されることから，私人によるフィルタリングの利用に伴う法益侵害については同様の論点があてはまることが多いことから，本稿では，この枠組みに基づいて論じたい。

その他，フィルタリングの実施基準については，憲法論以外にも，政治的な問題が関係することもある。例えば，フィルタリングの基準に一定の偏向的な要素が加わることによって，公平かつ公正なフィルタリングの利用に支障が生ずるおそれがあるような場合である。具体的には，フィルタリングの基準に，思想，信条，政治，個人の主観などが関わる場合には様々な問題が生ずると考えられるが，実際に米国においては，フィルタリングの基準について問題が指摘されてきた要素として，同性愛問題，人権，フィルタリング・ソフトそのものに対する批判などに関する情報については，フィルタリングの基準に政治的な要素も関わるため，フィルタリングの利用そのものが政治的に問題となることも指摘されてきた。

5. フィルタリングの利用とプライバシー

フィルタリングの利用は，特定の情報の抽出内容やそのパターンから，個人の趣味嗜好が明らかになるため，プライバシー利益の保護が問題となる。

フィルタリングの利用と個人のプライバシーの権利の保障に関する問題を考えるにあたっては，フィルタリングの利用に伴うプライバシー侵害の特徴をある程度明確にする必要がある。その特徴としては，大きく二つの側面があると考えられる。

一つは，本人が不知・不識のうちにフィルタリングが用いられる場合であり，他方は，本人が認識してはいるものの，他人に知られたくない情報が自動的に処理されることに伴う問題である。

前者は，本人が認識せずにプライバシーに係る情報が取得されるため，取得対象の情報によっては，センシティブな情報の取得を伴うことがある。また，後者については，取得対象の情報の内容について本人が認識しているものの，情報提供の裏返しとしてサービスやフィルタリングが行われていることが多い。

このように，個人のプライバシーに係る情報が取得される場合であっても，その情報が本人の同意の下で，必要な範囲で適切に管理されているのであれば法的に問題となることはない。しかし，本人が同意した範囲を逸脱した利用，情報の漏えいや不正利用などが発生するとプライバシー侵害に対する法的責任が問われる可能性がある。

なお，後述の個人情報保護法との関係において，個人情報保護法が制定されたことによって，プライバシーに該当する情報の不正利用について法的責任が問われるようになったと指摘する見解があるが，そのような指摘は誤りである。プライバシー侵害に対する法的責任は，個人情報保護法の定める罰則とは無関係であり，保護法が制定される以前から，プライバシー侵害については不法行為責任をはじめとする法的責任が問われている。

わが国において，プライバシーの権利性が判例において初めて認められたのは，1964年の「『宴のあと』事件」[5]判決においてである。

判決では，プライバシーの権利を，「私生活をみだりに公開されないという法的保障ないし権利」として承認し，プライバシー侵害による不法行為の成立要件として，①公開された内容が私生活の事実またはそれらしく受けとられるおそれのある事柄であること，②一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められること，③一般の人々に未だ知られない事柄であることを要すると判示した。

現在においても，この基準に基づいてプライバシー侵害としての不法行為の成否が判断されている。よって，フィルタリングの利用に伴って，個人のプライバシー侵害にあたるような利用が行われた場合，この基準によってプライバシー侵害か否かが判断されることになる。

また，電子メールを対象としたフィルタリングの実施については，2件の判例[6]においてモニタリングの実施とプライバシーの関係について判断が示されている。

電子メールをはじめとする通信内容の監視を行うということは，具体的な違法・不正行為の発見というよりは，むしろ，職務専念義務に反して，私的利用の許容限度を超えるような私的メールの使用の萎縮効果を狙う側面や，安易に外部に添付ファイル等個人情報が記された文書を送信しないといった萎縮効果に至るまで，主に情報セキュリティの確保を目的としてフィルタリングが用いられている。

その際に，フィルタリングの利用の適法性の判断について，プライバシー侵害にあたらないための基準としては，前記判例においては，①電子メールの監視手続，②電子メールの私的使用の許容範囲，③電子メールの私的使用とプライバシーの関係，および④電子メールの利用と合理的なプライバシーへの期待について基準を示した上で，モニタリングの実施とプライバシー侵害の成否について判断が示さ

れている。

その判断基準としては，電子メールのモニタリングを，①無権限，②職務上の合理的必要性がない場合，③個人的な好奇心や個人の恣意による場合など，監視の目的，手段およびその態様等を総合考慮し，監視される側に生じた不利益とを比較衡量の上，社会通念上相当な範囲を逸脱した監視がなされた場合に限り，プライバシー権の侵害となると解されている。

以上から，情報セキュリティの確保を目的として、従業員を対象としたフィルタリングを用いるにあたっては，モニタリングの対象となる者の権利利益を保護しつつ，監視の必要性とそれによって生ずる可能性がある不利益とを比較衡量した上で，どのようなフィルタリングをどの程度実施するのか十分に検討することが不可欠となっている。

6. フィルタリングの利用と通信の秘密

ネットワークにおけるフィルタリングの利用にあたっては，通信の秘密の保障の問題が生ずる場合がある。通信の秘密の保障とは，通信内容の秘密が第三者に知られないことを保障するものであるが，フィルタリングの利用に伴い，本来の通信当事者ではない第三者が積極的な知得行為をもって対象となる通信内容を把握することを目的として利用する場合には，通信の秘密の侵害が問題となる。

例えば，ネットワークを流れるパケット通信をネットワーク管理を目的として捕捉する「スニッファー」などは，本来はネットワークに過度の負荷がかかる通信を監視したり，子供が違法・有害情報に接することを防ぐために親がネットワーク利用を監視するために利用されたり，企業などにおいて内部の情報が外部に不正に漏えいしないように情報管理をするためのツールとして用いられてきた。ところが，第三者の通信内容を把握し，不正に情報を取得するために用いることも可能であり、そのように本来の目的とは異なる利用がなされる場合には，通信の秘密が侵害される可能性がある。

また，スパイウェア（ペスト）のように，コンピュータの利用者に関する情報を積極的に知得することを専らその目的とする悪意的なプログラムも用いられており，これらのツールを用いることで，悪意的に通信の秘密が犯される危険は高い。

なお，通信の秘密の保障について，それを「侵した」に該当するのは，通信当事者以外の第三者が積極的意思をもって通信内容を「知得」しようとする行為，第三者にとどまっている秘密をその者が「漏えい」する行為，第三者の通信を「窃用」する行為，本人の意思に反して自己または他人の利益のために用いることがこれに該当する。

以上の論点につき，現行法令においては，電気通信役務の提供においてフィルタリングを利用する場合，電気通信事業法（4条，40条，104条，105条），有線電気通信法（9条，14条），電波法（59条，109条），その他，不正アクセス禁止法等に基づいて，通信の秘密の保障や通信回線を用いてやりとりされる情報の適正な取扱いや不正アクセスの禁止等が法令において定められている。

なお，プライバシー侵害，名誉毀損，著作権侵害などの違法行為が行われ，被害者救済のためにその発信者を特定する必要がある場合には，「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（通称：プロバイダ責任制限法）に基づいて，事業者に課されている通信の秘密の保障義務の例外として発信者情報の開示が認められることがある。フィルタリングによって特定の人物の各種ログ等が記録されている場合には，それらの情報は開示の対象に当然含まれることになる。

7. フィルタリングの利用と適正手続

フィルタリングは，適正な手続きに基づいて利用しなければならない。この点につき，例えば，監視カメラの設置に関する訴訟が参考になる。例えば，監視カメラ訴訟としては，大阪府警察（西成警察署）が，大阪市西成区の日雇労働者が多く居住する通称「あいりん地区」において，同地区の街頭防犯用の目的のためとして，15か所の交差点等の高所にテレビカメラ（合計 15 台）を設置し，西成警察署等においてモニターテレビに映像を映し出すなどして使用した事件がある[7]。

本件は，同地区に居住または勤務し，あるいは同地区において労働組合活動やボランティア活動等を行っている原告らが，このようなテレビカメラの設置および使用は，原告らの「公権力から監視されない自由」等を侵すものであるなどとして，被告に対し，各テレビカメラの撤去および慰謝料の支払を求めた事案である。フィルタリングについても，それを用いて不当に監視されない自由の侵害が問題になる可能性は十分あるといえよう。

判決では，情報活動の一環としてテレビカメラを利用することは，基本的には警察の裁量によるものではあるが，国民の多種多様な権利・利益との関係で，警察権の行使にも自ずと限界があるうえ，テレビカメラによる監視の特質にも配慮すべきであるから，その設置・使用にあたっては，(1)目的が正当であること，(2)客観的かつ具体的な必要性があること，(3)設置状況が妥当であること，(4)設置および使用による効果があること，(5)使用方法が相当であることなどが検討されるべきであるとした上で，警察署が街頭防犯用の目的で設置した監視用テレビカメラが，プライバシー侵害にあたるとして撤去を命じている。

8. フィルタリングの利用と個人情報保護法

フィルタリングを利用するにあたって利用者毎に設定を行うと，同時に，当該利用者の個人情報の取得を伴うことになる。つまり，その利用者に関する情報のみならず，フィルタリングの設定によって取得または排除される情報についても，本人に関する情報として特定の個人を識別可能な情報にあたることから，その多くは個人情報にあたることになる。

一方，広義のフィルタリングの利用によって，情報の外部への流出の防止を行うにあたっては，その対象となる情

報が個人情報という場合も多いと考えられるが，フィルタリングの利用との関係において検討を要するのは，保護の対象となる情報が個人情報に該当するか否かではなく，その利用に伴って取得する個人情報の取扱いが，法令の定める手続に基づいて適正に取り扱われるべき個人情報にあたるか否かという点である。

なお，フィルタリングの利用と個人情報保護の問題について検討するにあたっては，最低限度，以下の点について検討を行う必要がある。

①フィルタリングの利用に伴う個人情報の取扱いの有無
②個人情報保護関連五法のうち，自らが所属する組織に適用される（されない）法律の把握
③個人情報の取扱いについて，法律の義務規定が適用されるか否かの判断
④個人情報を取り扱うにあたって遵守しなければならない義務の内容

9. 個人情報の取扱いの有無

個人情報保護法は，「個人情報」の取扱いを規制の対象する法律であるから，それを取り扱っていなければ，当然のことながらこの法律の適用は受けない。つまり，フィルタリングの利用に伴い，個人情報の取得を伴わない場合には個人情報保護法を遵守する必要はない。よって，「①フィルタリングの利用に伴う個人情報の取扱いの有無」について，はじめに検討を行うことが求められる。

では，法律の規制対象となる個人情報とは何か。本法の対象となる「個人情報」とは，「生存する個人に関する情報」であって，特定の個人を識別できる「個人識別性」があるものに限られる。なお，個人識別性の要件は，他の情報と容易に照合することによって特定の個人を識別できる場合も含まれる。よって，フィルタリングの利用に伴い，各種ログや設定情報など，その情報単独では特定の個人を識別できない情報が存在する場合，他の情報と容易に照合することで結果的に特定の個人を識別できる場合は，その情報も個人情報となる。

10. 個人情報データベース等とは

フィルタリングの利用に伴い取得した個人情報をデータベース化するような場合には，当該データベースは，保護法では「個人情報データベース等」と定義される。

個人情報データベース等とは，個人情報を含む情報の集合物であって，①特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの，②特定の個人情報を容易に検索することができるように体系的に構成したものである。

個人情報データベース等を保有して事業の用に供しているか否かによって，個人情報取扱事業者の義務規定の適用対象となるか否かが決まることから，これを保有しているかどうかについては，この二つの要件に基づいて検討することとなる。なお，検索性・体系性の要件にあてはまるデータベースとは，コンピュータ処理されたデータベースを思い浮かべるが，紙媒体であっても，検索性・体系性が認められれば個人情報データベース等にあたる。なお，個人情報データベース等を構成する特定の個人の数が 5,000 未満の場合は，それを事業の用に供しているとしても，保護法の義務規定の適用を受けない。

したがって，フィルタリングの利用に伴い個人情報データベース等を保有している場合であっても，小規模の事業者や個人が利用しているような場合には，特定の個人の数が 5,000 に満たないことはあるであろう。なお，5,000 の数え方は，一人の個人情報が複数登録されていても，その場合は一人分として計算する。また，たとえフィルタリングの利用に伴うデータベースに登録されている個人情報が 5,000 に満たないといっても，他に保有する個人情報と合計すると 5,000 を超える場合には，当然のことながら個人情報取扱事業者の義務が適用される。

なお，個人情報データベース等を構成する個人情報のことを，法律では「個人データ」と定義している。個人データについては，安全管理措置が義務づけられており，第三者に無断で提供したり，漏えいや不正利用などが発生しないよう安全に管理することが義務づけられている。

11. 個人情報保護関連五法とは

フィルタリングの利用に伴い，個人情報を取り扱うからといって，直ちに，法律の義務規定が適用されるわけではない。そこで，個人情報保護関連五法のうち，自らが所属する組織に適用される（されない）法律の把握が必要となる。

個人情報保護法と呼ばれている法律には，以下の五つの法律がある。

①「個人情報の保護に関する法律（平成 15 年法律第 57 号）」
②「行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号）」
③「独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）」
④「情報公開・個人情報保護審査会設置法（平成 15 年法律第 60 号）」
⑤「行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律（平成 15 年法律第 61 号）」

一般に，個人情報保護法と呼ばれているのは，「個人情報の保護に関する法律（平成 15 年法律第 57 号）」である。

これらの法律は，2003 年 5 月 23 日に成立し，同月の 30 日に公布され，義務規定以外の基本的な理念を定めた部分などは，同日に施行された。その後，個人情報保護法が定める個人情報取扱事業者の義務規定や行政機関・独立行政法人等を対象にした法律も含めて，2005 年 4 月 1 日に全面施行された。

さらに，個人情報保護関連五法に加えて，「個人情報の保護に関する基本方針」（平成 16 年 4 月 2 日閣議決定），規

則，政令，施行令および指針が制定され，各省庁が法を執行するための基準として個人情報の保護に関する法律第8条に基づいて定める「各省ガイドライン等」によってわが国の個人情報保護制度は構成されている。

個人情報保護関連五法のうち，自らが所属する組織に適用される（されない）法律を把握する必要がある理由として，これらの法令は，それぞれ民間部門や公的部門でそれぞれ適用分野が異なることがあげられる。

保護法第3条「基本理念」，第2章および第3章は，民間部門と公的部門を問わず，全分野に包括的に適用される。ここでは，基本理念，国および地方公共団体の責務等および個人情報保護に関する施策等について定めている。

次に，義務規定の適用関係は，民間部門と公的部門で区別される。民間部門に適用されるのは「個人情報保護法」である。公的部門については，行政機関については行政機関個人情報保護法，独立行政法人等については独立行政法人等個人情報保護法がそれぞれ適用される。

なお，地方公共団体については，個人情報保護関連五法の義務規定は直接適用されず，地方公共団体の個人情報保護条例が適用される。

12. フィルタリングの利用と個人情報取扱事業者の義務の適用

個人情報保護法の目的は，ネットワーク社会の進展に伴い個人情報の利用が著しく拡大していることから，「個人情報の有用性に配慮」しつつ，「個人の権利利益を保護」することにある。そのため，国および地方公共団体，そして，民間の事業者に対して，個人情報の適正な取扱いを求めることが，個人情報法保護法の主たる目的となっている。

個人情報保護法の義務規定が適用される民間の事業者とは，「個人情報取扱事業者」に限定される。個人情報取扱事業者とは，「個人情報データベース等」（個人情報を含む情報の集合物として検索性があって体系的に構築されているもの）を，事業の用に供している者のことをいう。ただし，個人情報データベース等を構成する特定の個人の数が，5,000 に満たない場合には，前述の通り個人情報取扱事業者の義務は適用されない。

13. 個人情報保護法の義務規定

個人情報取扱事業者に該当する場合，個人情報を取り扱うにあたっては，法律の定める手続を遵守しなければならない。

以下，個別の義務の内容について，フィルタリングの利用との関係で特に重要な部分をとりあげたい。

13.1 利用目的の特定

フィルタリングの利用に伴い個人情報を取り扱う場合には，当該フィルタリングの利用目的が，個人情報の利用目的になる場合もあれば，フィルタリングの利用そのものが，個人情報の利用目的になる場合もあるであろう。

法律では，個人情報を取り扱うにあたっては，利用目的を特定し，その範囲内で利用することを義務づけている。これにより，個人情報を利用するにあたっては，利用目的の特定が必要となり，目的外で利用する場合には原則として本人同意が必要となる。

フィルタリングの利用にあたって特定する個人情報の利用目的は，ある程度明確に特定できるものと思われる。しかし，フィルタリングを利用した結果，本人の不正行為が明らかになるなど，何らかの不利益処分を課すことが必要になる場合や，当該個人情報（個人データ）を別の目的で利用したり提供することが必要な場合もある。例えば，違法行為に従事した者の情報を令状に基づいて警察が提供を求めてきたような場合である。第三者に個人データを提供する場合，相手方が警察であっても法律の規定では本人同意を得ることが義務づけられているが，違法行為に従事した者から本人同意を取得することは困難である。

しかしながら、そのような場合であっても，個人データの利用や提供は可能である。なぜなら，法律では，法令に基づく場合，人の生命または財産といったような具体的な権利利益が侵害されるおそれがある場合，公衆衛生の向上や児童の健全な育成のために特に必要な場合，法令に基づく公的事務への協力の四つの適用除外が定められており，それに該当する場合には本人の同意を得る必要がないからである。令状に基づく提供は、法令に基づく提供にあたる。

昨今，問題となっている個人情報保護法への過剰反応は，そのような適用除外があるにもかかわらず，個人情報の利用や提供を取りやめる事例も多いことから，不用意な過剰反応や萎縮効果が発生しないよう留意する必要がある。

13.2 個人情報の取得関係

個人情報取扱事業者が個人情報を取得するにあたっては，偽りその他不正の手段により個人情報を取得してはならず，個人情報を適正な方法によって取得することが義務づけられている。例えば，不正競争防止法に抵触するような形で，不正に顧客名簿等を取得することがこれに該当するが，フィルタリングの場合，当初の設定や本人が認識している機能とは異なる方法で個人情報を取得しているような場合は，これに該当するおそれがある。

14. 終わりに

フィルタリング技術をはじめとして，新たな技術手段を用いる際には，「目に付く」法律についてのみ検討が行われがちであるが，「法の不知は違法性を阻却しない」のが原則である。つまり，関係する可能性がある法律を検討することは重要ではあるが，その法律にだけ着目し，他の法令を遵守しないことは法治国家においては許容されないため，本稿では，「フィルタリングと法」について最低限度検討を行わなければならない関係法令について検討した。

特定の技術を用いるにあたっては，それに関わる可能性がある法令や判例の示した判断など広く認識することが重要であり，特定の法令や偏った検討では，後々，重大な法益侵害が発生するなど現実の支障となってシステム全体の

構築・運用に致命的な影響を与えかねない。

例えば，論文データベースの構築などが行われる場合，データベースの仕様や公開方法などの議論が先行し，実際にデータベースを公開する段になって，公開の対象となる論文の著作権（特に複製権および公衆送信権の問題）の問題や，個人情報の取扱い（著者の個人情報）が問題となることが多い。そのような場合に，事前に，法的に本人の許諾を得ておくべき問題について，論文提出時に本人同意が得られていれば，データベースの公開にあたって特に講ずべき法的対応はみあたらない。ところが，その仕様など技術的問題に関する検討が中心となりがちなために，法的に本人に許諾を得ておくべき点について十分な検討がなされなかった結果，事後的に本人同意を取得しなければならないという事態に陥ることも多く，結果的に同意が得られなかった者の情報を公開できなかったり，そもそも，システムの全面的な見直しに迫れるといったこともある。

よって，フィルタリングの利用方法や利用局面は，今後も様々な方面での活用や利用方法が見いだされることは間違いないと思われるが，新たな技術的問題について検討するのと同時に，法的に解決しなければならない問題を十分認識した上で，必要な検討を行うことが肝要である。

参考文献

1) Childrens' Internet Protection Act,Public Law 106-554, §1(a)(4), 114 Stat. 2763Aa-335, amending 20 U.S. Code §6801 (the Eelementary & Secondary Eeducation Act); 20 U.S.Code §9134(b) (the Museum & Library Services Act and 47 U.S.Code §254(h) (the e-rate provision of the Ccommunications Act).
2) 各ツールの概要や機能，その評価については，Internet Filters -A Public Policy Report-, The Brennan Center for Justice at New York University School of Law, 2006 を参照．なお，当該報告書が対象として取り上げているツールは，以下の通りである．America Online Parental Controls, Bess, ClickSafe, Cyber Patrol, Cyber Sentinel, CYBER sitter, FamilyClick, I-Gear, Internet Guard Dog, Net Nanny, Net Shepherd, Norton Internet Security, SafeServer, SafeSurf, SmartFilter, SurfWatch, We-Blocker, WebSENSE, X-Stop.
3) 総務省．インターネット上の違法・有害情報への対応に関する研究会（中間取りまとめ）．平成 18 年 1 月 26 日 <http://www.soumu.go.jp/s-news/2006/060126_1.html>.
4) 内閣官房の IT 安心会議<http://www.it-anshin.go.jp/>において，「インターネット上における違法・有害情報対策について」（平成 17 年 6 月 30 日）が公表され，フィルタリングについては，「インターネット上の有害情報を排除するフィルタリングソフトの活用の推進」が盛り込まれている
5) 東京地判昭和 39 年 9 月 28 日判時 385 号 12 頁
6) 東京地判平 13 年 12 月 3 日判決労判 826 号 76 頁および東京地判平 14 年 2 月 26 日判決労判 825 号 50 頁
7) 大阪地判平成 6 年 4 月 27 日判時 1515 号 116 頁
8) 「個人情報の保護に関する基本方針」（平成 16 年 4 月 2 日閣議決定）

Special feature : Information filtering. Filtering and the law. Fumio SHIMPO (University of Tsukuba, 1-2 Kasuga, Tsukuba, Ibaraki-Pref 305-8550 JAPAN)

Abstract : Discussions concerning the use of filtering tends to examine a measure relating to the filtering of unlawful and/or harmful information. In general, when filters do not function properly, blame is placed on the technical side. This paper focuses on a survey of filtering from a legal perspective. Filters are used not only to block information but also to restrict access to the Internet and protect confidential information.

Keywaords : filtering / privacy / data protection / secrecy of communication / freedom of expression / information security