コピー及びアクセスを抑止・追跡する技術

コンテンツの不正利用の抑止を目的とする技術、及び不正利用されたコンテンツを追跡するための技術（特に、不正利用監視・追跡を中心に）等について述べる。

１．　不正利用監視・追跡に関する社会的･技術的背景

（１）社会的背景

警察庁の広報資料[1]によれば、いわゆるハイテク犯罪は、近年、増加の傾向にあり、その検挙件数は平成 14 年には 1,000 件の大台を突破した。そのうち、著作権法違反の件数は、約 3%である。実際の違反の数はもっと多いと推定されるが、その発見、さらには検挙に至るものは少ないのが実状であろう。

その原因としては、著作権法違反、とりわけ、コンテンツの不正利用を発見するための技術が、まだ完全には確立していないことが第一に挙げられる。したがって、法制度等のそのような技術の運用に関しても、十分議論されているとは言えない。このことが、さらに、不正利用の抑止効果を十分に働かせるに至らない、という悪循環に陥っているのではないだろうか。

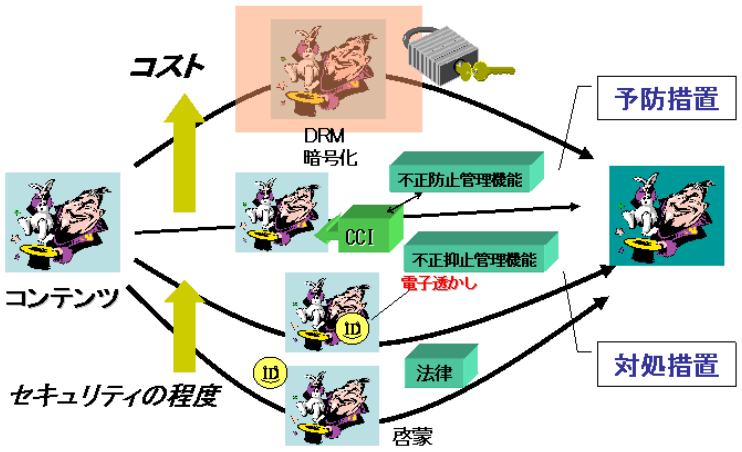
（２）技術的背景

デジタルコンテンツを不正利用から保護する手段としては、セキュリティの程度とコストとの兼ね合いから、いくつか存在する。最もコストがかからない手段は、技術というより法律等であり、啓蒙によるものであるが、コンテンツの保護に対しては何らの技術的保証はない。一方、コストをどんどんかけることにより、暗号化や DRM（Digital Rights Management）という技術により強固に保護することもできる。これらの技術は、暗号化や DRM のような不正利用そのものを防止する、もしくは予防する予防処置と、不正コピーは出来てしまうが、それがあっても不正を見つけることが出来るという対処処置との二つに大別される。（図 1 参照）

まず、予防処置であるが、これはコンテンツの暗号化等によって事前に不正コピーを防止するものである。ユーザは鍵をもらい、その鍵で暗号化されたコンテンツを開けることにより、コンテンツを視聴することができる。さらに、暗号化する際に、利用時間や利用回数等、各種の制御データを併せてコンテンツに付加する(“カプセル化”と称する)というような細かい利用制御もできる。この場合には、基本的には専用のビューアでコンテンツを見たり聴いたりすることになる。このような DRM 技術が、昨年辺りから各社から出てきているという状況である。

[1] http://www.npa.go.jp/hightech/

図1　デジタルコンテンツの保護手段



一方、対処処置は、不正コピーは出来てしまうものの、後でそれを見つけて鎮火や特定等の対処を行う事後の処置である。“不正利用監視・追跡”と称するのはこのためである。したがって、特にコンテンツ自体にあまり余計な処理を施すことがないので、一般的な装置やソフトで見たり聴いたりできる。市場にはまだ出ていないが、何ヶ所かで実験的に行われている。

技術的には、予防措置が DRM であり、対処措置が不正利用監視・追跡ということなる。（図 2 参照）

図2　権利侵害に対する予防措置と対処措置

<出典> [5]

- **予防措置**
  - コンテンツを暗号化する事前の措置．鍵の取得により視聴可能．
  - コンテンツ利用制御（利用時間，利用回数など）が可能．
  - 一般に専用ビューアでコンテンツを視聴する．
  - 市場を形成しつつあり

DRM
(Digital Rights Management)

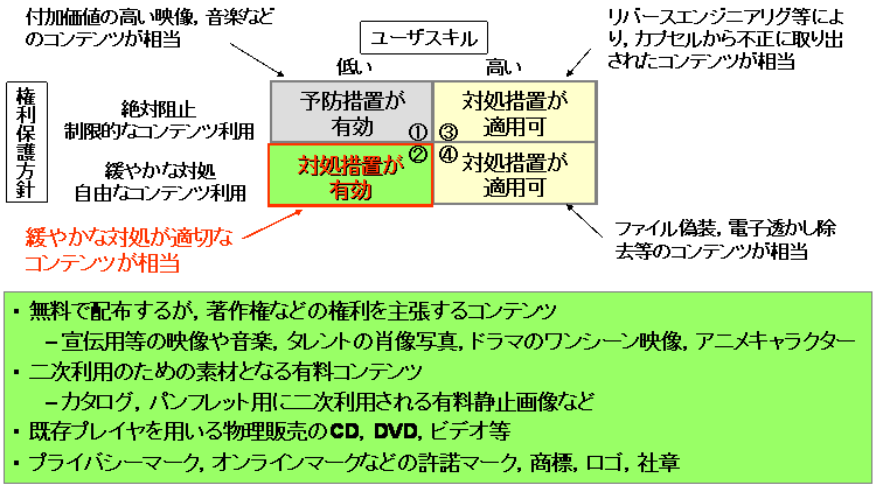
- **対処措置：発見～鎮火～犯人特定**
  - コンテンツの不正利用を発見して対処する事後措置．
  - 不正利用発見のため不正探索等を行う．
  - 汎用装置による視聴が可能であり，利便性が高い．
  - 市場形成はこれから

不正利用監視・追跡

これらの各措置技術がそれぞれ使用される領域に関し、次のような考え方がある。すなわち、まず，非常に価値の高いコンテンツで予防措置をとらないと怖くてネットワークに流せない、絶対に不正は阻止したいという領域がある。（①）次に、そんなに厳しく保護しないで、むしろ自由に使ってもらいたいが、ある程度の不正利用には対処したいという領域がある。（②）また、ハッカーのようなユーザスキルが高い人達に対しては、予防措置を施しても破られたりする。そのような領域（③、④）に対しては予防措置を施した上でさらに不正を発見して対処するような措置が使われることになる。（図 3 参照）

図3　予防措置と対処措置の適用領域

<出典> [5]



対処措置が有効な領域のコンテンツとしては、たとえば、無料で配布するが権利はしっかりと主張したいコンテンツ、二次利用の素材、たとえばカタログやパンフレットに使われるようなものや物理的に販売するパッケージに入れるコンテンツ、ロゴや商標等が対象になると考えられる。

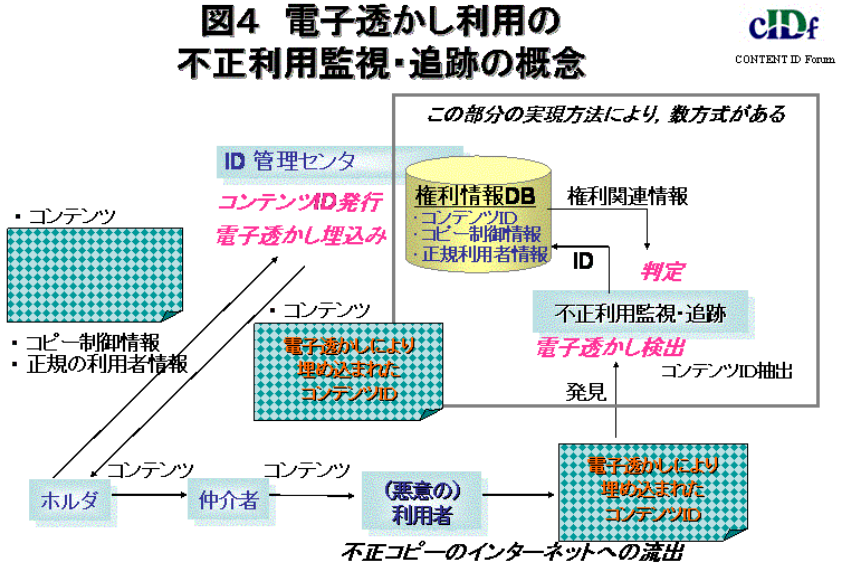
２．　不正利用監視・追跡

（１）方式

不正利用監視・追跡の方式は多数あるが、共通の基本的な技術は、コンテンツに対して電子透かしにより ID や情報を埋め込んでおき、それを流通させるというものである。そして、インターネット上からコンテンツを持ってきて、電子透かし情報を抽出し、それを流通の権利情報と比較することにより、不正

か否かを判定することが基本的な概念である。(図 4 参照)

これにより、悪意の利用者がそのようなコンテンツを不正にコピーし、自分のホームページに掲載する等、インターネット上に流通させた場合には、不正の発見が可能となる。不正利用監視・追跡には、この共通な概念をどのように実現するのかということにより、いくつかの方式が考えられる。すなわち、コンテンツを発見するところや判定するところが、方式により異なるということになる。



不正利用監視・追跡の方式としては、大きく三つある。(図 5 参照)

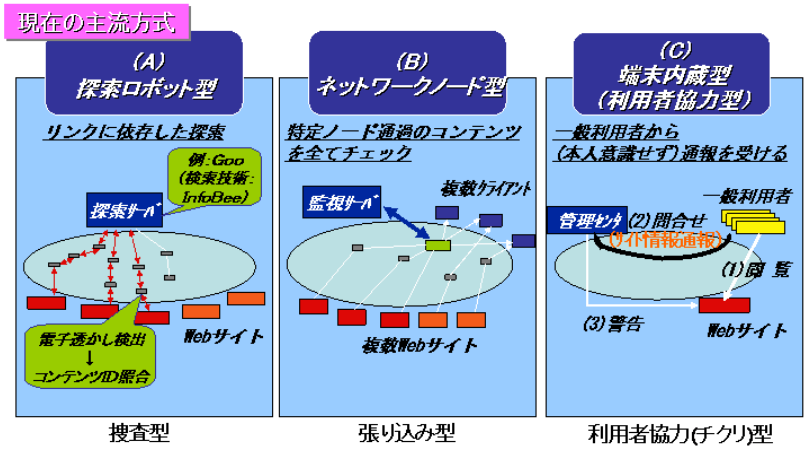
まず、現在主流の探索ロボット型(A)。これは、サーチエンジンという技術を使ってインターネット上の Web サイトからコンテンツを持ってきて、そのコンテンツの電子透かしを検出してその中の ID を抽出し、その ID をキーとするデータベースの検索により得られる権利情報を参照し、その権利情報と対象コンテンツの置いてあった Web サイトの URL の情報とを比較するものである。その結果、この Web サイトにこのコンテンツがあるのは正しいか否かというような判定を行う。

次は、ネットワークノード型(B)。これは、P2P や B2C 等のどのような形態においても、コンテンツが流通するのはネットワーク内のメールサーバやファイルサーバ、プロキシ等のノードを経由することから、ネットワーク内のこれらノードに不正利用監視・追跡の論理や機能を置いておくものである。そしてコンテンツがそれらのノードを通過する時にそれをトラックし、電子透かしを検出し、前述の探索ロボット型と同様に不正の有無をチェックする。

三番目は、端末内蔵型あるいは利用者協力型(C)。これは、一般の利用者も

しくは何らかの利用者が Web サイトのコンテンツを閲覧する時に、利用者には気付かれないように利用者の端末のバックグラウンドで閲覧しているホームページのコンテンツをチェックし、不正かどうかを判定するものである。

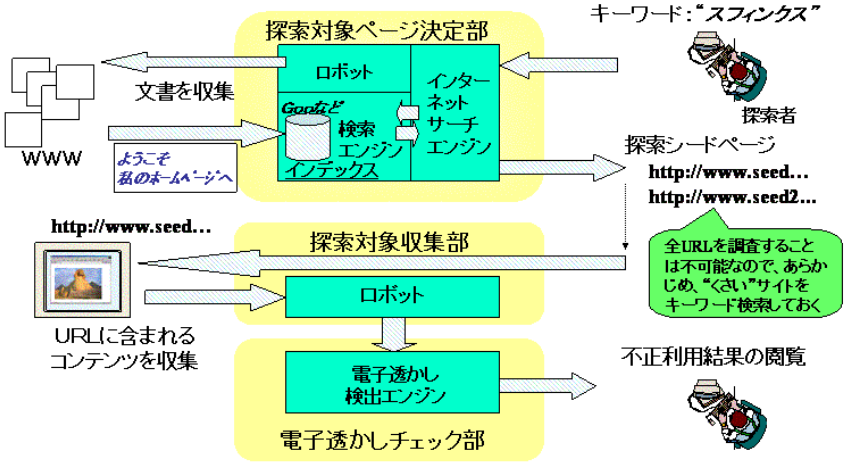
図5 電子透かし利用の不正利用監視・追跡方式



以降、これらの三方式について、例を用いてもう少し詳しく説明する。

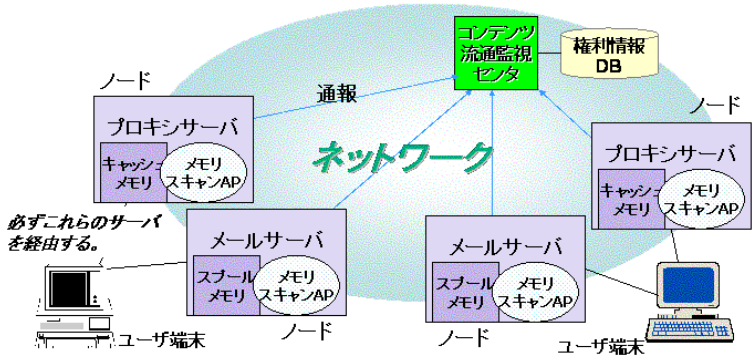
まず、探索ロボット型であるが、これは呼んで字のごとく、インターネットの探索ロボットを使うものである。基本動作としては、ロボットで各 URL を探索することによりコンテンツを収集し、その電子透かしを検出して不正の有無をチェックする。ただ、実際には、世界中の全ホームページを探すと時間がかかりすぎて実用性が無いため、たとえば最初に怪しいサイトをある程度絞り込んでおき、それらのサイトからのみコンテンツを収集するということが行われる。例としては、“スフィンクス”がテーマのコンテンツに関する不正探索を行う場合には、まず、“スフィンクス”というキーワードによりインターネットのホームページを検索し、キーワードの載っているホームページをリストアップしておく。その後、リストに載っているホームページを対象にコンテンツを収集してチェックする。(図 6 参照)

図6 （A）探索ロボット型
不正利用監視・追跡方式



次に、ネットワークノード型であるが、これは、ノード内のメールサーバやプロキシサーバ等を使用するものである。たとえば、ある人のユーザ端末から相手のユーザ端末宛にメールが送られる場合にはメールサーバを経由するが、このメールサーバの中に、メールの添付ファイルをチェックして電子透かしを検出する論理を組み込んでおくのである。これにより、電子透かしにより検出された ID に紐づけられた権利情報と流通情報とを比較し、送り手と受け手の妥当性をチェックする。（図 7 参照）

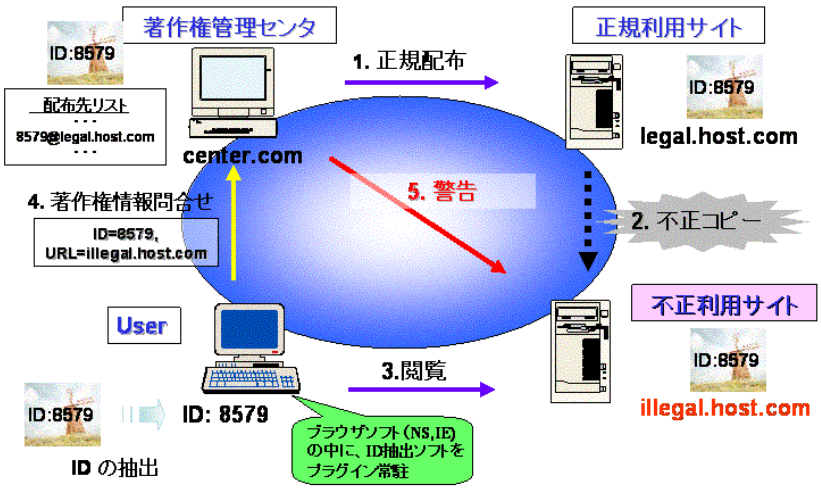
図7 （B）ネットワークノード型
不正利用監視・追跡方式



■**Proxy**のキャッシュや**Mail**サーバのスプール内をスキャンし、コンテンツ**ID**付きコンテンツ流通状況を把握
■コンテンツ流通監視センタでは、ネットワーク内のコンテンツ流通情報を収集

三番目が端末内蔵型・利用者協力型であるが、この基本的な動作例は、次の通りである。まず、対象コンテンツが掲載されていてよい正規のサイトの情報[8579@legal.host.com]をそのコンテンツの ID と共に著作権管理センタに登録しておく。一方、利用者の端末には、ブラウザによりホームページを閲覧した際に、そのバックグラウンド、すなわち利用者に気づかれない処理により、閲覧しているホームページに掲載されるコンテンツの電子透かしを検出し、抽出した ID を閲覧中のホームページの URL と共に著作権管理センタに送出する機能を組み込んでおく。正規のサイト[8579@legal.host.com]が閲覧された場合には、その情報が著作権管理センタに登録されているため、正当と判定される。ところが、ある人が、このコンテンツを正規のホームページからダウンロードし無許可で自分のホームページ[illegal.host.com]にアップロードしたとする。このホームページをある利用者が閲覧した際に ID と URL とが著作権管理センタに送られるが、この組み合わせ情報が著作権管理センタのデータベースに存在しないことから、不正と判定され、そのサイトに警告が送られる。(図 8 参照)

図8 (C) 端末内蔵(利用者協力)型 不正利用監視・追跡方式



以上説明した三つの代表的な不正利用監視・追跡方式の比較を、表 1 に示す。

探索範囲の観点では、探索ロボット型は全てのサイトのコンテンツを対象にできる。ネットワークノード型はコンテンツがノードを通過するポイントでそれをトラックするため、手渡しでの流通には対応できない。しかし、P2P 流通

にも適用可能である。端末内蔵型は利用者が閲覧するホームページのみしかチェックできない。探索ロボット型はサーチエンジンを利用するため、「探索されたくない」という設定がなされた（クローズドな）ホームページはチェックできないが、そのようなホームページも端末からは閲覧できるので、端末内蔵型を用いることによりチェックすることが出来る。

ネットワーク負荷に関しては、探索ロボット型は各サイトを検索するため、一般的にトラフィックが大きい。ネットワークノード型は特定のノードにおいての処理であり、当該ノードにのみ高負荷がかかる。端末内蔵型は利用者が閲覧する際にチェックするため、ネットワーク負荷は相対的に少ない。

簡便さという観点からは、サーチエンジン等を使う探索ロボット型は容易である、ネットワークノード型はメールサーバやプロキシサーバに細工が必要である。また、端末内蔵型も利用者端末へ所要機能を組み込む必要があるが、利用者がそのようなことをやってくれるかという、インセンティブの問題がある。たとえば、Windows 環境では、インターネットエクスプローラ等にこのような機能が標準で組み込まれていればよいが、それが良いのか悪いのかということも問題になる。さらに、ネットワークノード型の場合、電子メールの添付ファイルを勝手に覗いて良いのかという、プライバシーの問題がある。

以上から、それぞれの方式に一長一短があり、状況や環境に応じていくつかの方式を選択し組み合わせて使用することが必要ということになる。

表1　各不正利用監視･追跡方式の比較

方式	探索範囲	ネットワーク負荷	簡便さ
(1) 探索ロボット型	○ インターネットのオープンサイト全てが対象	× 探索サーバに接続するネットワークトラフィック大	○ Web 検索エンジン等利用で容易
(2) ネットワークノード型	○ 監視対象ノード通過コンテンツの全てが対象 P2P 流通にも適用可能	△ 特定ノードの負荷大	× メール/プロキシ等のサーバに細工が必要 プライバシ問題あり
(3) 端末内蔵 (利用者協力) 型	△ 監視対象端末内で扱うコンテンツは全て可能 (クローズドサイトも可)	○ ネットワークの負荷はなし	△ 利用者の端末への組込み手段(インセンティブなど)が必要

さらに、いくつかの方式がある

評価基準) ○:ほぼ完全(容易)に満足, △:条件付きで満足, ×:かなり実現は困難

それぞれ、一長一短があるため、選択／組み合わせが必要

ここで、端末内蔵型の不正利用監視・追跡方式には、詳細にみると、さらに三つの方式がある。(表 2 参照)

表2 端末内蔵型 不正利用監視・追跡方式の比較

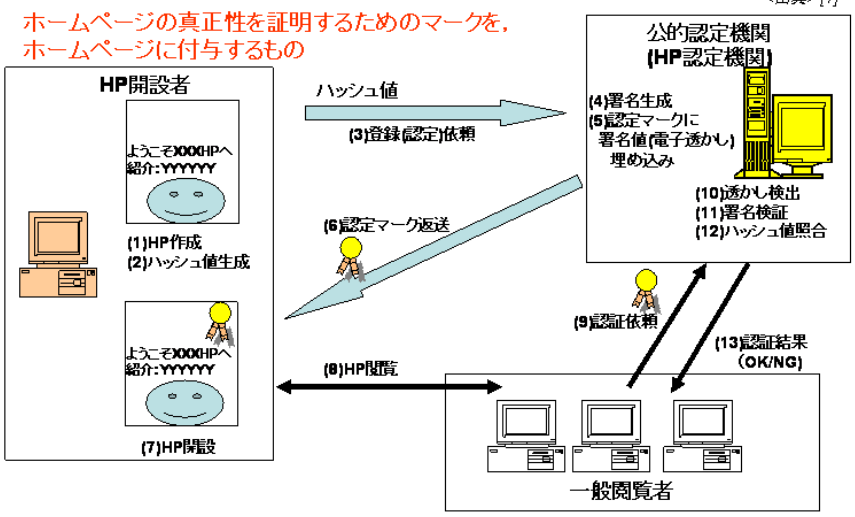
<出典> [3]

	対象	検証者	公的機関の作業量	閲覧者の作業量	ネットワーク負荷	特記事項
インターネットマーク方式 [1]	ホームページ	閲覧者 -アクセス可能なHP全て -高人気のHPほど頻繁に検査	中程度 (マークの発行)	中程度 (閲覧先HPのマークの検査)	○ マークの署名を検査するための公開鍵を事前に取得する必要あり	コンテンツのみの監視は不可
一般利用者の協力に基づく方式 [2]	コンテンツ 電子透かしが挿入可能なコンテンツ	公的機関 -透かし検出は閲覧者が実行(判定は公的機関)	多い 毎回のコンテンツの正当性/違法性の判定	少ない (閲覧者の無意識のうちにバックグラウンドで実施)	× 毎回、コンテンツ情報がネットワーク経由で公的機関にアップロード	複数分散する公的機関により負荷分散が可能 全世界の閲覧者の協力が可能 インセンティブが必要
アルゴリズム公開型電子透かしを用いた方式 [3][4]	コンテンツ 電子透かしが挿入可能なコンテンツ	閲覧者 -アクセス可能なHP全て -高人気のHPほど頻繁に検査される	中程度 著作情報取得要求及び、通報があった際の処理	やや多い -事前取得の著作情報に基づきコンテンツの正当性/違法の検査 -違法コンテンツの場合、公的機関に通報	○ -著作情報を事前に取得する場合 -不正コピー発見時の通報の場合	無数のユーザが補い合うことにより、インターネット上のコンテンツの常時監視が可能

まず、インターネットマーク方式は、ホームページの開設者が公的な認定機関から、「このホームページは正しいものですよ」といったような認定マークをもらってそれをホームページに掲載しておくものである。(図 9 参照)

図9 インターネットマーク方式

<出典> [1]

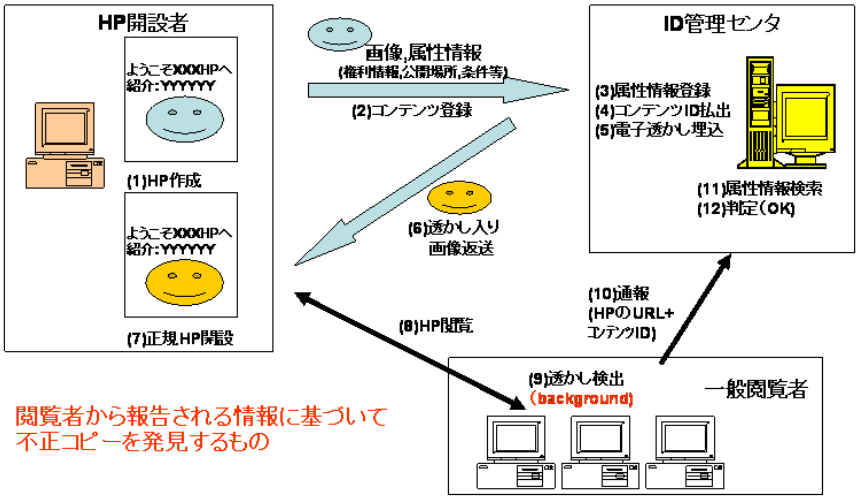


利用者がホームページ閲覧中にこの認定マークを見つけた場合、正規のホームページか否かについてのチェックを公的機関に依頼し、認証されればこのホームページは正しいということが分かる。これは、かつて郵政省が進めたプロジェクトにおいて検討された方式[2]であるが、実際には現時点では使われていないと考えられる。

次に、利用者協力型は前述の端末内蔵型そのものであり、ホームページの開設者がコンテンツを掲載するときに電子透かしで ID を埋め込んでおくと共に、その情報を管理センタに登録しておき、利用者がそれを閲覧する時にバックグラウンドで掲載コンテンツの正当性がチェックされる。（図 10 参照）

図10　利用者の協力に基づく方式
（1）正規ホームページの場合

<出典> [2]

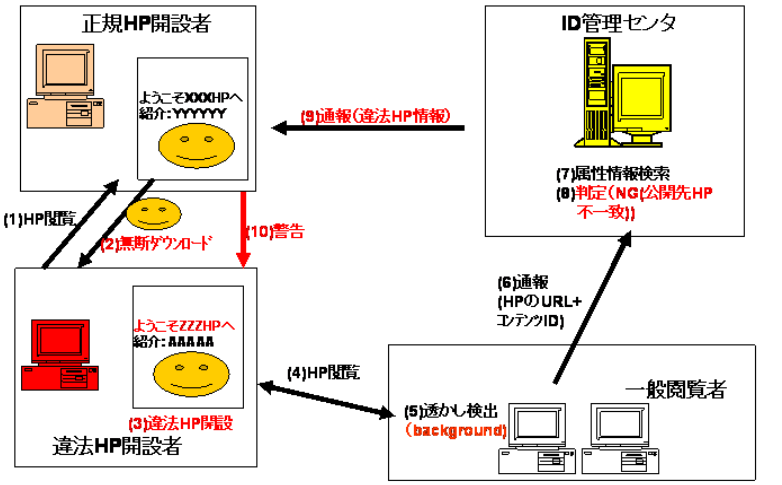


不正の場合には、管理センタの権利データベースの登録内容に基づいて比較することにより判定されるため、違法の警告がホームページ開設者に届くことになる。（図 11 参照）

[2] http://www.watch.impress.co.jp/internet/www/article/971224/imark.htm

図11　利用者の協力に基づく方式
（2）違法ホームページの場合

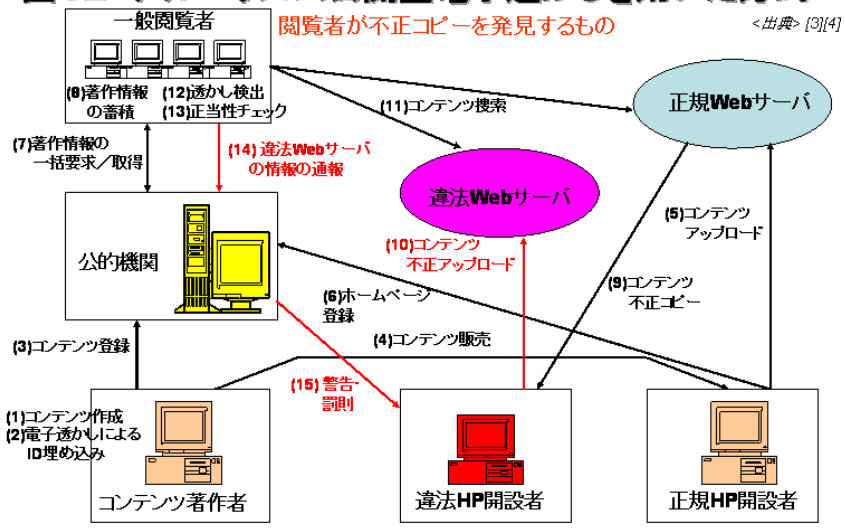
<出典> [2]



三番目の、アルゴリズム公開型電子透かしを用いた方式は、コンテンツに電子透かしにより ID を埋め込み、掲載サイト情報と共に公的機関に登録しておくことは、他の方式と同様である。相違は、公的機関に登録する権利情報を一般の閲覧者（利用者）に渡し、各閲覧者で蓄積しておくことにある。他方式では、閲覧者が ID を検出した後に権利データベースのある機関にその ID を送って不正の有無を判定するが、アルゴリズム公開型電子透かしを用いた方式では、一般の閲覧者が登録情報を持っているため、不正は一般の利用者の閲覧処理のバックグラウンドでチェックされ、公的機関に通報される。（図 12 参照）

図12　アルゴリズム公開型電子透かしを用いた方式

<出典> [3][4]

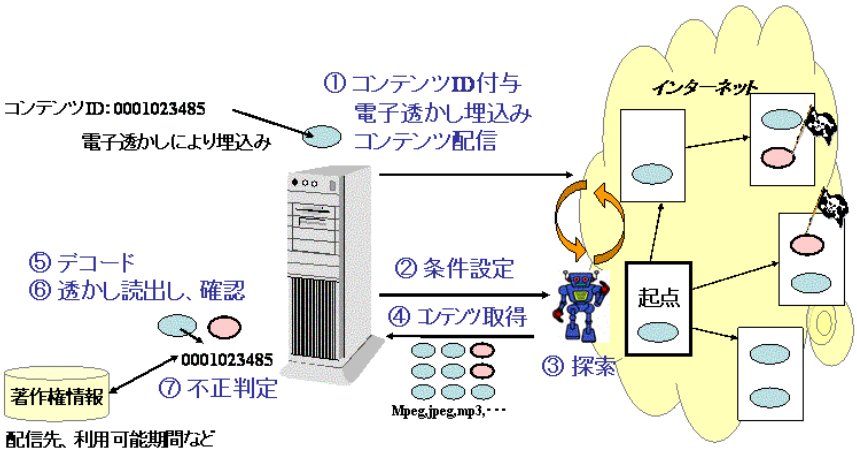


（２）運用

不正利用監視・追跡の運用においては、まず、準備と（不正の）発見がある。準備としては、コンテンツに対してユニークな ID を電子透かしにより埋め込む機関が必要となる。たとえば、前述のロボット探索型不正利用監視・追跡では、探索機能が必要であることはもちろんであるが、探索の前に怪しいサイトを絞り込むための条件設定も効率的な探索のためには必要であり、絞り込みの条件は、たとえばこのコンテンツについて探索して欲しいというようなお客さんの要望に基づいて設定する。発見のためには、探索の結果として収集したコンテンツについて、電子透かしにより ID を検出する機能と、ID に基づいて著作権情報データベースを参照し不正の有無を判定する機能が必要となる。これらをまとめてどこかで判定する場合には、一つのサーバが必要となる。（図 13 参照）

図13 運用の流れ - 準備と発見 -

<出典> [5]

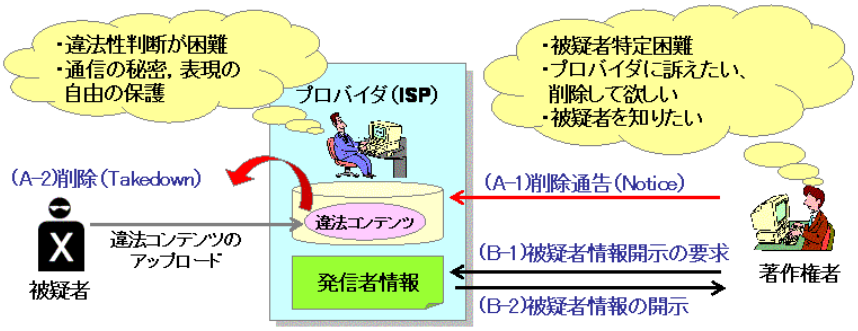


不正利用監視・追跡の運用において、不正と判明した後に必要となることは、鎮火（不正コンテンツの除去）と犯人特定である。Notice&Takedown ということが言われるが、不正が見つかったホームページを運用するサービスプロバイダ（ISP）に対し、このコンテンツは違法だから削除してくれと著作権利者が要求し、それが妥当であればプロバイダがそれを削除することが可能となる。

ただし、削除の妥当性に関しては、難しい問題がある。さらに、著作権者は、削除だけでは足りず、不正を行った人や会社を特定したいと考えて ISP に対して被疑者情報開示の要求を出すことがある。それが本当に妥当であれば開示することもできるが、通信の秘密や個人情報保護等の観点から問題があり、開示しないこともある。これは最近各所で議論されていることであるが、このように、発見された後にも対処が必要になるということである。（図 14 参照）

図14 運用の流れ - 鎮火と犯人特定 - <出典> [5]

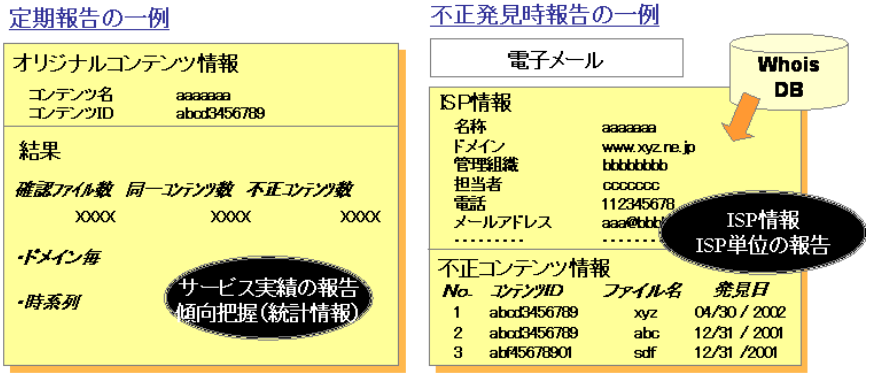
(A) 鎮火 → Notice & Takedown (N&T)
(B) 犯人特定 → 被疑者情報の開示
➢ **プロバイダの行為に対する免責 → プロバイダ責任法**



さらに、不正利用監視・追跡に関する報告は、さまざまな意味で重要である。常時不正の有無を探索しているが、不正利用監視・追跡の運用者は、第一にはその顧客に対して報告する。定期報告としての統計情報、不正発見時の報告として、たとえば、不正の種類や不正発見時の詳細情報等が考えられる。(図 15 参照)

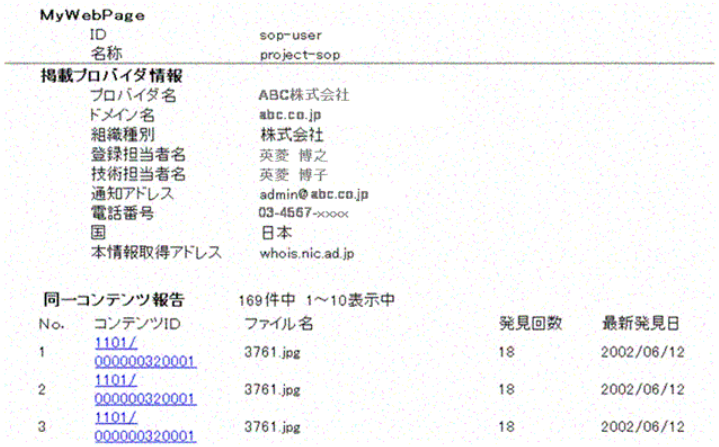
図15 運用 -不正利用監視・追跡に関する報告 -
<出典> [5]

- 定期報告と不正発見時報告
- N&T、被疑者情報の要求のためのユーザへの情報提供
  - 形式的要件を満たす通知



不正発見時の報告のイメージとして、プロバイダ名や不正と判定したコンテンツの情報を含むものの例がある。ただし、これはプロバイダの情報であり、不正をしていると推定した犯人の情報ではない。(図 16 参照)

図16 不正発見時報告のイメージ <出典> [5]



MyWebPage

ID	sop-user
名称	project-sop

掲載プロバイダ情報

プロバイダ名	ABC株式会社
ドメイン名	abc.co.jp
組織種別	株式会社
登録担当者名	英菱 博之
技術担当者名	英菱 博子
通知アドレス	admin@abc.co.jp
電話番号	03-4567-xxxx
国	日本
本情報取得アドレス	whois.nic.ad.jp

同一コンテンツ報告　169件中 1～10表示中

No.	コンテンツID	ファイル名	発見回数	最新発見日
1	1101/000000320001	3761.jpg	18	2002/06/12
2	1101/000000320001	3761.jpg	18	2002/06/12
3	1101/000000320001	3761.jpg	18	2002/06/12

これらの不正利用監視・追跡を上手く運用するためには、技術ばかりではなく、社会的なシステムを整理する必要があるということから、その例が提案されている。探索ロボットで不正を発見して報告した場合、たとえば被疑者の開示等については、第三者機関にきちんとチェックされた上で、プロバイダに開示要求を行うといった仕組みを設けないと、プロバイダに直接開示要求を行うことは難しいと考えられる。また、不正利用監視・追跡運用者が不正を発見しても、それが本当に不正なのか否か、あるいは被疑者情報の開示に対してもある程度の法律関係の機関（法的機関か、監視システムの運用者が個別に契約するかという議論はある）からアドバイスを受けるというような仕組みも必要となる。そうしないと、不正利用監視・追跡のユーザに情報を開示することは出来ない。（図 17 参照）

３．　不正利用監視・追跡の適用例

実際に不正利用監視・追跡サービスが運用されている例はほとんど無く、何カ所かで実験的に行われているというのが実状である。

たとえば、電子透かし技術の会社であるエム研では、「インターネット監視ロボット」と称するロボット探索型の不正利用監視・追跡を運用している。（図 18 参照）

図17　不正利用監視・追跡に関わる社会システムの例

<出典> [5]

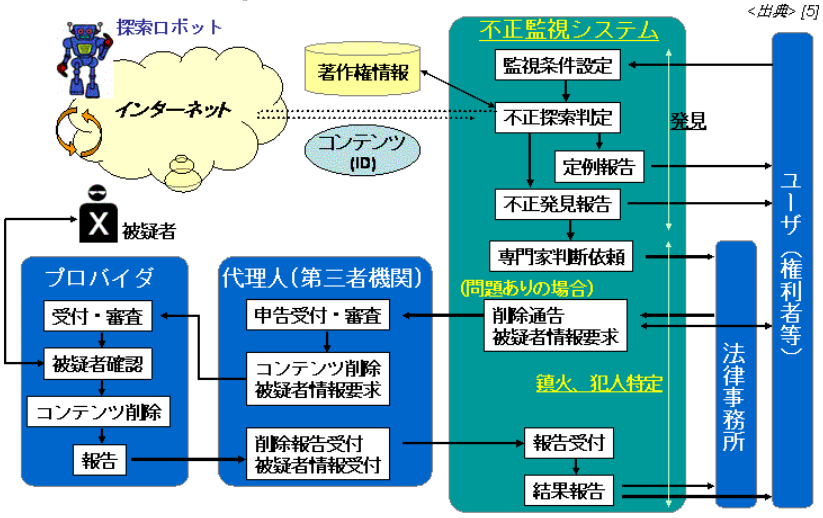
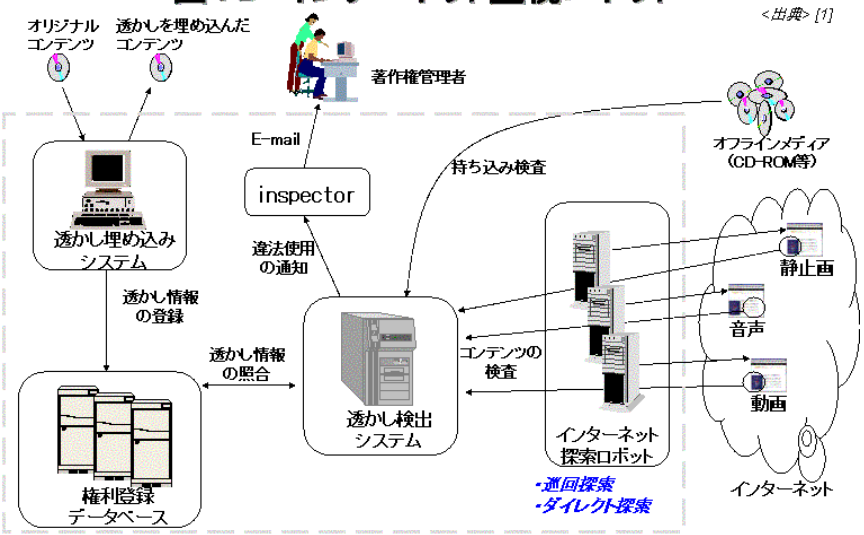


図18　インターネット監視ロボット

<出典> [1]



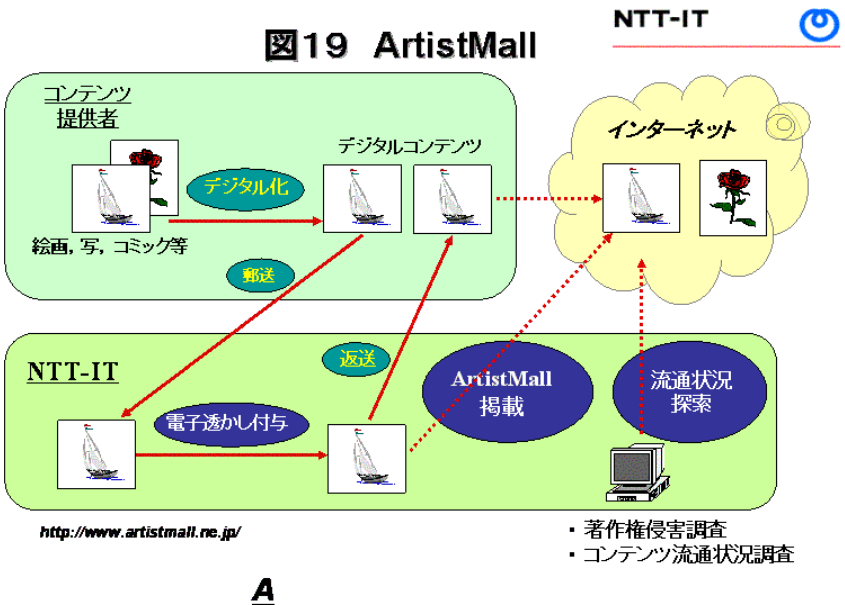
また、JASRAC 構築する一連のシステム、「JASRAC NETWORCHESTRA SYSTEM （ネットワーケストラ)」の中に、J-MUSE という監視システムがあり、探索ロボット型の不正音楽コンテンツの監視を行っている[3]。JASRAC は、昨年、日本レコード協会(RIAJ)と共同で音楽の不正探索の技術検証を行っている。この実験では、インターネット上の不正コンテンツ探索だけではなく、放送された不正コンテンツも同様の技術を用いてチェックするということを実施

[3] http://www.jasrac.or.jp/network/contents/networchestra.html

している[4]。放送コンテンツの不正探索実験では、電子透かしにより ID を埋め込んだコンテンツを放送し、電波を受信して電子透かしを検出するような装置を用いている。チェック自体は権利データベースの内容との比較により行うのはインターネット上の場合と同じであるが、そのようなことを実際に FM 東京と大阪とで実施したという。これを実際に使うかということは未定であるが、技術的に確認したということである[5]。

また、NTT の研究所でも不正利用監視・追跡システムのプロトタイプを開発し、不正コンテンツ探索の実験を行っているという。方式は、探索ロボット型であり、コンテンツに電子透かしによりコンテンツ ID を埋め込み、権利情報を登録しておき、インターネットのサーチエンジンでコンテンツを収集し ID を抽出した後、権利情報との比較によりチェックした後、レポートを送るというものである。レポートは、不正利用監視・追跡の運用者向けに報告するメールであり、ID や日時等の情報や不正と判定した時のホストや時間の情報をまとめている。また、不正と判定した理由を示す詳細画面を設けており、たとえば、ホームページにアップすることが許可されていないコンテンツがアップされているとか、アップして良い期間を外れてホームページ上に存在するとかといったような判定条件にチェックされた場合に、運用者向けに報告がなされ、それを元に実際にコンテンツの保持者にレポートを送付するというようなことを想定している。

図19 ArtistMall



[4] http://www.jasrac.or.jp/release/03/01_2.html

[5] http://internet.watch.impress.co.jp/www/article/2003/0122/watermark.htm

NTT のグループ会社である NTT-IT は、アーティストの人達が自分のコンテンツを紹介する ArtistMall と称するサイトを運用している[6]。（図 19 参照）

この ArtistMall に掲載するコンテンツに対し、希望があれば、ID を付与し、それを電子透かしにより埋め込んで掲載している。サーバに不正利用監視・追跡を設置し、探索ロボットによりインターネットを検索し、ArtistMall に掲載されているコンテンツが不正に何処か他のホームページに無いかをチェックしている。この時、探索範囲を絞るため、お客さんから提供されたキーワードで引っ掛かったホームページを探索の対象としている。探索時間やリンクの深さ等を指定していかないと判定できないので、お客さんから指定情報をもらって探索していく。ただし、探索ロボットでも勝手に見られないように設定されているサイトは対象外になってしまう。（図 20 参照）

図20　顧客指定情報とサービス対象範囲

指定情報
- キーワード（複数可能 and or条件）
- 直接ホームページURL（事前に使われそうなHPの指定）
- 探索時間上限
- 探索の深さ（リンクのどこまでたどる？）

探索対象外サイト
- ＩＤ／パスワードを要求するサイト（会員制等）
- どこからもリンクされていない孤立サイト*
- 探索ロボット拒否フラグのあるサイト
- ダウンロード型のサイト（CGIによりダウンロード）

*直接URLを指定すれば可能（キーワード指定では不可能）

その他、ベリマトリックスジャパンも実験運用を行っている[7]。沖電気工業とムービーネットインターナショナルも、一昨年、ブロードバンドの映画コンテンツに MPEG4 で圧縮したコンテンツのネット探索の実験も実施した[8]。

最後に、電子透かしではないが似たような技術として、NTT コミュニケーションズがコンテンツそのものの特徴（コンテンツはそれぞれが個別の特徴を持っており、その特徴を圧縮した形で抽出し、その特徴を比較することによって不正を検索する）を利用した技術を開発している[9]。

---

6 http://www.artistmall.ne.jp/
7 http://www.asahi.com/tech/feature/K2002020802166.html
8 http://www.oki.com/jp/Home/JIS/New/OKI-News/2001/06/z0131.html
9 http://www.asahi.com/tech/feature/K2002020802166.html

４．　不正利用監視・追跡に関する議論例

Notice&Takedown、被疑者情報開示について、所定の要件を満たした場合にのみ通知したり、第三者機関を設置して手続きを行ったり、あるいは裁判所や法律事務所などが絡んだりするような対応が必要ではないかという議論がある。（表 3 参照）

たとえば、GBDe では、形式的要件を満たす通知に対する削除については免責したり、第三者を通じてプロバイダへ通知したりというような議論がある。被疑者情報の開示についてもしっかりした手続きを整備する必要があり、総務省の研究会でも、開示が免責となるケース等の議論がされている。わが国のプロバイダ責任法（正式名称：「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」）は、このような議論を反映したものとなっている。つい最近、米国で、裁判所が、RIAA の要求に基づき、Vedrizon という ISP に不正にコンテンツを公開した顧客の情報を開示するよう命令したという事例もある[10]。

表3　Notice & Takedown, 被疑者情報開示への対応

<出典> [5]

- **形式的要件を満たした通知**
- **第三者を介した通知**
- **裁判所や法律事務所等の照会のある通知**
- **被疑者への確認**

	N&T	被疑者情報の開示
GBDe Global Business Dialogue on Electronic Commerce 2000.9	(1)形式的要件を満たす通知に対する削除について免責 (2)有資格の第三者を通じてプロバイダへ通知	プロバイダ保管の違反者情報を入手するための手続きを整備
インターネット上の情報流通の適正確保に関する研究会（郵政省） 2000.12	次の場合に免責： (1)問題となる情報を知らず削除しない場合 (2)知った後に直ちに削除した場合 (3)形式的要件を満たす通知に対して被疑者に確認して反論が無い場合に削除	・裁判所の事前許可を経て開示請求 ・仲裁役として第三者機関を設ける、被疑者主張の代弁も行う
プロバイダ責任法 2001.11.22可決 2002.5.27施行	次の場合に免責：(a)上記の(1)、(2)と同様、(b)形式的要件を満たす通知に対して被疑者に確認し7日を経過しても反論が無い場合に削除	被害者からの要求に対し被疑者の意見を聞く必要あり。プロバイダの判断で開示できるが、責任はない。
米連邦地裁判決 (原)RIAA、(被)Verizon 2002.1.22		600件以上の海賊版音楽ファイルを不法にネット経由で公開したと疑われる加入者の個人情報を、VerizonはRIAAに提示せよ

ネットノード型、すなわち、ネットワークのサーバにおいて、あるいはネットワークを通過する情報をトラックして不正チェックをすることに関しても議論されている。ISP は通信事業者であるので通信の秘密を守る義務があり、勝手にネットワークを通過するコンテンツを見ることは一般的にはできないが、ある程度コンセンサスが得られれば将来的にはできるようになる可能性もある。ただ、現時点でも既に実施しているという報告例もある[11]。　パブリックでは

[10] http://www.zdnet.co.jp/news/0301/22/nebt_18.html
[11] http://www.zdnet.co.jp/news/0302/28/ne00_p2p.html

制約が多いが、社内や学内などプライベートな環境であれば、それぞれの機関のポリシーに基づいて行う場合にはあまり問題は無いのではないかという議論もされている。

〔参考文献〕

[1] 「コンテンツIDオープンセミナーat映像ソフト協会」資料，エム研，2001.6.6.

[2] 松井龍也，高嶋洋一：“電子透かしの応用：一般の利用者の協力に基づく海賊版データ摘発手法”，1998年　暗号と情報セキュリティシンポジウム予稿集，SCIS98-10.2.C，Oct.1998.

[3] 松下哲也，西垣正勝他：“Web上の著作コンテンツを監視する方式検討－賞金稼ぎの仕組みを利用したディジタル著作物の監視方式の有効性－”,情報処理学会研究報告　コンピュータセキュリティ（CSEC)，18-9，2002.7.18.

[4] 山口和彦，岩村恵一，今井秀樹：“誤り訂正符号を用いたアルゴリズム公開型電子透かし”，1999年暗号と情報セキュリティシンポジウム予稿集，pp.713-718，Jan.1999.

[5] 佐竹康宏，松浦正明，松崎隆一，井上貴司，徳永裕史：“デジタルコンテンツにおける権利侵害の対処システムについて”，電子情報通信学会技術研究報告 Vol.102, No.138，DC-2002-15，2002.6.21.