

Web上の著作権コンテンツを監視する方式の比較検討
—賞金稼ぎの仕組みを利用したデジタル著作物の監視方式の有効性—

松下 哲也¹ 西垣 正勝² 曾我 正和³ 田窪 昭夫⁴ 中村 逸一⁵

1 静岡大学大学院情報学研究科 〒432-8011 静岡県浜松市城北 3-5-1

2 静岡大学情報学部情報科学科 〒432-8011 静岡県浜松市城北 3-5-1

3 岩手県立大学ソフトウェア情報学部 〒020-0193 岩手県岩手郡滝沢村滝沢字菓子 152-52

4 東京電機大学 情報環境学部 〒270-1382 千葉県印西市武西学園台 2-1200

5 (株)NTT データ セキュリティ事業部 〒212-0058 川崎市幸区鹿島田 890-12

E-mail: nisigaki@cs.inf.shizuoka.ac.jp

あらまし アルゴリズム公開型の電子透かしを利用して、一般ユーザが誰でも違法コンテンツを含むホームページを摘発することができる社会的機構を構築することを提案する。全てのユーザが不正者を摘発する賞金稼ぎとなり得る本方式によれば、不正者は誰に自分の犯罪を発見されるか分からず、不正者にとって大きな脅威になると思われる。また、世界中に無限のコンテンツが散在するインターネットにおいては、ホームページ上のデジタル著作物を一元管理することは事実上、不可能である。提案方式は全ての一般ユーザによる究極の分散チェック機構と位置付けることができ、インターネットにおけるデジタル著作物の管理方式に適していると言える。本稿では、本方式と関連方式を比較し、本方式の有効性を検討する。

キーワード 著作権保護, 不正コピー防止, インターネット, ホームページ, 電子透かし

Copyright protection system for website content

—The efficiency of a bounty hunting-based copyright protection system for website content—

Tetsuya Matsushita¹ Masakatsu Nishigaki² Masakazu Soga³ Akio Takubo⁴ Itsukazu Nakamura⁵

1 Graduated School of Informatics, Shizuoka University 3-5-1Johoku, Hamamatsu, Shizuoka 432-8561, Japan

2 Faculty of Information, Shizuoka University 3-5-1Johoku, Hamamatsu, Shizuoka 432-8561, Japan

3 Faculty of Software and Information, Iwate Prefectural University 152-52 Sugo, Takizawa, Iwate 020-0193, Japan

4 School of Information Environment, Tokyo Denki University 2-1200 Muzai-Gakuendai, Inzai, Chiba 270-1382, Japan

5 NTT Data Corp., Security Business Division 890-12 Kashimada, Saiwai Kawasaki, Kanagawa 211-8567, Japan

E-mail: nisigaki@cs.inf.shizuoka.ac.jp

Abstract This paper proposes a distributed copyright protection system for digital content which is based on the idea of bounty hunting. The system employs a digital watermark method in which all information for extracting watermarks can be opened, so that any home page visitor can verify the authenticity of the content on the home page he/she is visiting. It allows, essentially, every net surfer to be a kind of bounty hunter who finds illegal content or home pages. We believe this type of self-policing system is necessary because it is impossible for a limited number of trusted parties to check the vast number of content in all home pages over the Internet. Moreover, in the proposed system, illegal home page owners can not know if or when they have been discovered, as each and every visitor has the potential to discover and report them. Therefore, this distributed-type check of the proposed system promises to be a much greater deterrent than a centralized-type check could ever be. Thus, a copyright protection on the Internet is successfully achieved by the system. This paper discusses the efficiency of a bounty hunting-based copyright protection system by comparing it with the related systems.

Keyword copyright protection, copy protection, internet, home pages, digital watermark

1. はじめに

近年のインターネットの普及と計算機(PC)の低価格化にともない、World Wide Web(WWW)は爆発的な広がりを見せた。各個人が自由に情報を発信・受信することができるようになり、無数の各種ホームページが乱立した。このような高度情報化社会においては「情報」の持つ価値は非常に高く、それ故にデジタルコンテンツの著作権は強く保護されなければならない。また、特に電子商取引の世界では、コンテンツに含まれる情報に対して高い信頼性が問われることになる。しかし、このような要求に対し、現在の計算機ネットワーク環境におけるセキュリティは完璧とは言えない。著作権コンテンツを不正コピーすることは基本的に容易であり、また、ホームページの改竄による被害も増加・深刻化している。

上記の問題は、特にホームページにおける情報発信に焦点を当てて考えた場合、次の二つに集約されるものと思われる。まず第一が、正規のホームページがクラッカーに改竄されるという問題である。ホームページが改竄されると閲覧者に発信者の意図しない情報が伝わることになる。誤った情報は閲覧者と発信者の双方に被害を与える可能性が高い。そして第二が、著作権コンテンツの違法発信である。他人のコンテンツを無断に使用して自分のホームページを作成したり、海賊版などをホームページに置いてコンテンツを違法に配信するケースがこれにあたる。不正コピーを野放しにしてしまうと、コンテンツの持つ経済価値は失われ、コンテンツ製作者(著作者)はその利益を享受できない。これは著作者のコンテンツ創作意欲を削ぎ、インターネットや電子商取引の発展に影響を与えるであろう。

ここで、第一の問題であるホームページの改竄については、それを未然に防止することは難しいものの、デジタル署名[1]や電子透かし[2]を利用して、改竄の有無を検出することは可能である[3][4]。著者らのグループも、WWWサーバがホームページの改竄の有無を定期的に検査する「ホームページ改竄パトロール」による改竄チェック方式を提案している[5][6]。したがって残る課題は、第二の問題である著作権コンテンツの違法発信を取り締まる方法の確立である。近年、実際にP2P型コンテンツ配布[7][8]における不正コピーが大きな問題になっており、その対策は急務といえる。

そこで著者らは、アルゴリズム公開型の電子透かし[9]を利用して、著作権を侵害している違法コンテンツを含むホームページを一般のユーザ誰でもが摘発することのできる不正コピー監視方式を提案している[17]。本方式においては、一般の閲覧者全てが不正なホームページを摘発する「賞金稼ぎ」となり得る。不正者は誰に自分の犯罪を発見されるか分からない。これは不正

者にとって大きな脅威になると思われる、それ故に不正行為の抑止効果も高まると期待される。また、世界中に無限のコンテンツが散在するWWWにおいては、ホームページ上のデジタル著作物の全てを一元管理することは事実上、不可能である。提案方式は全ての一般ユーザに不正コピーの監視を任せる「究極の分散チェック機構」と位置付けることができ、WWWにおけるデジタル著作物の監視方式に適していると言える。本稿では、本方式と関連方式とを比較し、本方式の有効性を検討する。

2. 関連方式

インターネット上の不正コピー防止および不正コピー監視方式の代表的なものとして、以下が提案されている。

2.1. インターネットマーク

インターネットマーク[3]は、ホームページの真正性を示すためのマークを当該ホームページに添付する方式である。マークには、ホームページのデータやURLのハッシュに対する公的機関のデジタル署名が電子透かしとして埋め込まれている。閲覧者は閲覧先のホームページに添付されているマークに埋め込まれた電子透かしを検証することにより、当該ホームページが真正のものであるかを確認する。

インターネットマークは、閲覧者が閲覧先のホームページの正当性を確認する手段を提供するものであり、閲覧者の保護が第一目的である。インターネットマークを積極的に活用してインターネット上の不正コピーを監視する仕組みまでを議論した研究は、著者の知る限り見当たらない。また、マークはホームページ全体の正当性を検証するためのものであり、ホームページに含まれるコンテンツ(例えば、一枚の画像のみ)が取り出され、他のホームページにて使用された場合には、その不正を検出することはできない。

2.2. 一般利用者の協力に基づく海賊版摘発手法

文献[10]では、閲覧者から報告される情報に基づいて不正コピーを発見する手法が提案されている。コンテンツ(画像)には透かしが入っており、閲覧者は閲覧先のホームページに掲載されている画像に埋め込まれたIDを取り出して、当該URLの情報とともに公的機関に報告する。公的機関は閲覧者からの報告を蓄積し、著作画像の分布状況に関するデータベースを作成する。

閲覧者にはコンテンツの所在情報の提供が依頼されているのみであり、不正コピーを発見・監視するのは公的機関の役目である。

2.3. ロボットによる不正コピー探索

検索エンジンのようなロボットを用いてインター

ネット上の不正コピーを探索するサービスが、すでに商用ベースで始まっている[11][12]. 対象となるコンテンツは画像や音声であり、事前に電子透かしが埋め込まれている。ロボットは次々とインターネット上のホームページを訪れ、自動的にコンテンツの電子透かしを検査する。

ロボットは黙々と仕事をこなすであろうが、一台のロボットが一日の内に探索できるホームページの数は(テキストのみの探索で)およそ1000万URLであり、インターネット上の膨大なホームページを全て一通り走査するのに約一ヶ月を要するという事が1997年の文献[13]にて報告されている。実際には、ホームページは毎日のように更新され、その数も急激な勢いで増加しているので、全てのコンテンツを高頻度で検査するには限界があると思われる。ロボットを複数用意する方式も考えられているが、探索範囲を効率的に分配するアルゴリズムが重要であり、適切な負荷分散が実現されていないというのが現状である[13]. また、ロボットによる探索では、ロボットにアクセス権が与えられていないLANの中のコンテンツの検査は不可能である。更に、ロボットによる機械的な探索では、(コンテンツを分割したり、ファイル名の拡張子を変更して掲載するなどの方法で)コンテンツを巧みに偽装して違法発信しているような悪質なホームページを発見することは難しい。

2.4. コンテンツのカプセル化

コンテンツを暗号化して発信する方式を総称してカプセル化と呼ぶことにする。この方式では保護対象のコンテンツは暗号化されて発信される。正規購入者には暗号化コンテンツを復号するための鍵が渡される。

不正コピーを監視するのではなく、すなわち、コンテンツのカプセル化は、不正コピーそのものを防止することが目的である。

復号鍵を持っていないクラッカーが配信経路中などから暗号化コンテンツを不正入手したとしても、これを復号することはできない。しかし、正規購入者が悪意を持っていた場合には、復号鍵や復号後のコンテンツが不正に流出することになる。したがって、コンテンツの再暗号化[14]が完全に実現しなければ、コンテンツのカプセル化による不正コピー防止は無意味となる。なお、再暗号化が完全に動作した場合、コンテンツの利用(復号)に応じて課金することにより、超流通[15]の世界を実現することも可能となる。

3. 賞金稼ぎ型監視方式

賞金稼ぎ型監視方式[17]を図1に模式的に示す。ここで、著作者とは著作コンテンツの作成者、発信者とは自らのホームページを公開している者、閲覧者とは全世界のホームページをネットサーフィンしている一般のユーザである。公的機関は全ての著作コンテンツの著作権情報を管理・公開している。

本方式の流れは次のようになる。

1. 著作コンテンツの登録
著作者は、自分が作成したコンテンツにアルゴリズム公開型の電子透かし[9]によりIDを埋め込み、これを公的機関に登録する。
2. ホームページの登録
発信者が著作コンテンツを購入して、そのコンテンツを含むホームページを作成した場合には、発信者は当該ホームページを公的機関に登録する。

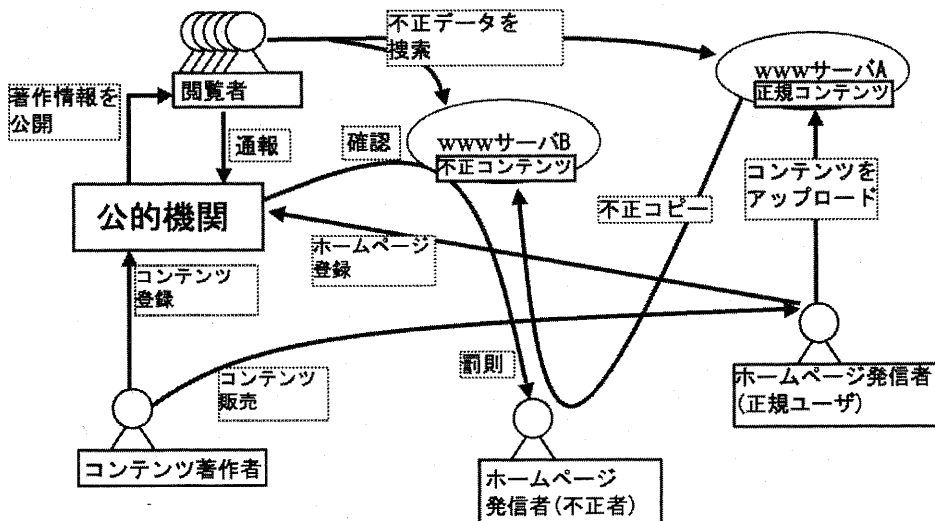


図 1. 賞金稼ぎ型監視方式

3. 著作権の公開

公的機関は、閲覧者がホームページ内のコンテンツの正当性を検査するために必要となる情報(以下、これを「著作権情報」と呼ぶ)を公開する。

4. 不正ホームページの通報

閲覧者は自由に各種ホームページを閲覧する。その際に、自分が閲覧したホームページに含まれるコンテンツの正当性を著作権情報に基づいて検査し、不正なホームページが見つかった場合にはこれを通報する。

5. 不正者の検挙

通報を受けた公的機関は当該ホームページを差し止める。そのホームページを作成した不正者に罰則を科し、通報者に報酬を与える。

賞金首情報である「著作権情報」が公開されており、ホームページを閲覧している一般のユーザが誰でも賞金稼ぎとなって、不正ホームページを通報することが可能である。

以下、それぞれの詳細を説明する。

3.1. 著作コンテンツの登録

著作者が著作コンテンツを公的機関に登録する際の流れを示す(図2)。

- i. 著作者がコンテンツを作成する。
- ii. 著作者はコンテンツにアルゴリズム公開型の電子透かしにより、IDを透かし情報として埋め込む。
- iii. 著作者は、透かし入りコンテンツとそのIDおよび透かしを検査するための情報を公的機関に登録する。公的機関は適切な方法により著作者を認証した上で、この登録を受理する。

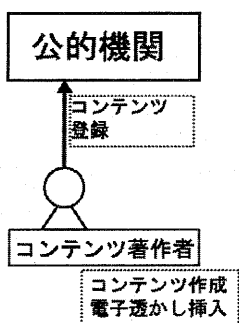


図2. コンテンツ登録

図1、図2には一つの公的機関しか記されていないが、単一の公的機関では世界の全てのコンテンツの著作権情報を一元管理できない。よって実際には、全世界を適切なドメインに分け、各ドメインごとに公的機関を置くことになる。ドメインの分割方法は任意であり、

例えば著作者の所属(国籍や会社名など)に応じて分けてもよいし、コンテンツのジャンルごとにドメインを用意してもよいだろう。著作者は、ドメインごとに置かれている公的機関のうちの適切な公的機関に自らのコンテンツを登録する。

通常の電子透かしにおいては、透かし情報がどこに入っているかということが知られてしまうと、その部分を改竄されて透かしが消されてしまう。よって、透かしを検出するアルゴリズムを公開することはできない。これに対し、手順iiで用いるアルゴリズム公開型の電子透かしは、透かしの検出アルゴリズムを公開しても透かしの改竄を許すことのない電子透かしである。例えば文献[9]では、オリジナルデータを誤り訂正符号化して透かしを埋め込み、透かしの検出アルゴリズムの公開を可能にしている。

3.2. ホームページの登録

正規ホームページが公的機関に登録される際の流れを示す(図3)。

- i. 発信者は著作者からコンテンツを購入し、そのコンテンツを含んだホームページを作成して公開する。
- ii. 著作者はコンテンツ(の使用権)を発信者に売ったことを公的機関に通知する。公的機関は適切な方法により著作者を認証した上で、この通知を受理する。
- iii. 発信者は購入したコンテンツをどこのホームページに掲載しているかという情報を公的機関に登録する。公的機関は適切な方法により発信者を認証した上で、この登録を受理する。

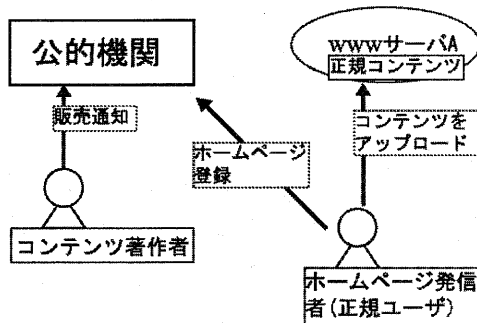


図3. ホームページ登録

コンテンツを正規に購入した発信者は、購入の際の契約に反しない範囲であれば、自由にそのコンテンツを使用してホームページを作成することができる。ただし、当該コンテンツが含まれるホームページのURLを公的機関に登録する必要がある。ホームページの更

新にともない当該コンテンツを別のホームページに移動したりすることも自由であるが、発信者は変更の都度、その旨を公的機関に通知する必要がある。なお、当該コンテンツの著作権情報は著作者の属するドメインの公的機関(著作者がコンテンツを登録した公的機関)が管理することになるので、手順 ii の通知、手順 iii の登録は当該公的機関に対して行われることになる。

コンテンツを掲載するホームページが固定されているような場合には、発信者がコンテンツ購入時に著作者にその旨を伝え、URLをも電子透かしとしてコンテンツに埋め込んでもらってもよい。この場合は、発信者がホームページの URL を公的機関に登録するフェーズは不要となる。

3.3. 著作権情報の公開

公的機関が著作権情報を公開する際の流れを示す(図 4)。

- i. 公的機関は、コンテンツ ID、当該コンテンツの透かしを検査するための情報、当該コンテンツが掲載されている正規ホームページの URL などをまとめ、これを「著作権情報」として管理する。
- ii. 公的機関は著作権情報をホームページにて公開する。著作権情報は定期的に更新される。
- iii. 閲覧者は公的機関のホームページを訪れ、著作権情報を取得する。

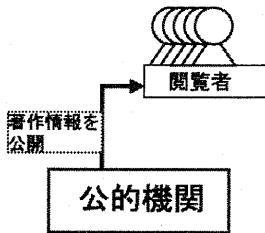


図 4. 著作権情報公開

各ドメインの公的機関は、自ドメイン内の著作物に対する著作権情報のみを管理・公開する。

手順 iii において、

- a) 各ドメインごとに存在する公的機関のうち、どの公的機関の著作権情報を取得するか、
- b) その公的機関が公開している著作権情報の内、どのコンテンツに対する著作権情報を取得するか、
- c) 著作権情報をいくつ取得するか、

などについては閲覧者が自由に選ぶことができる。

a), b)に関しては、閲覧者が自らの嗜好に合わせ、自分が閲覧する可能性の高いジャンルの著作権コンテンツに対する著作権情報を取得しておくこと効率がよいだろう。もちろん閲覧者の PC の著作権情報格納用ストレージの大きさにも左右される。また、c)に関しては、閲覧者

は多数の著作権情報を取得しておくほど、不正ホームページを発見して報酬を手にする確率は高まるが、ホームページを検査するために要する時間が長くなる。

a)~c)の指定がない場合には、閲覧者に任意の公的機関を訪れてもらい、当該公的機関が適当に著作権情報を渡すようにすれば良い。この場合、基本的にはすべての著作権情報が複数の閲覧者に対して偏りなく配布されるようにするが、必要があれば、特定の著作権情報を重点的に高頻度で配布するようにしても良い。

3.4. 不正ホームページの通報

閲覧者が不正ホームページを発見し、通報する際の流れを示す(図 5)。

- i. 閲覧者は普段通りのネットサーフィンを行い、趣味や目的に応じて自由に各種ホームページを閲覧する。その際に、自分が閲覧したホームページ内の全コンテンツに対して著作権情報に基づいて電子透かしを検査することにより、コンテンツの正当性をチェックする。
- ii. 不正なコンテンツを含むホームページが発見された場合には、閲覧者はその旨を公的機関に通報する。

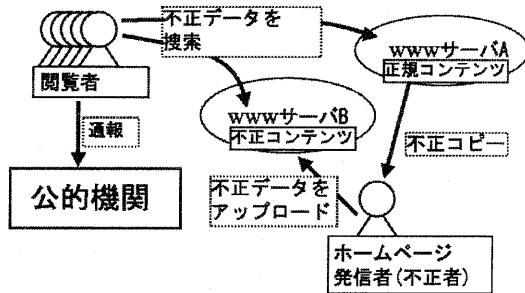


図 5. 不正ホームページ通報

閲覧者は自分が閲覧しているホームページの中に、自分が取得している著作権情報に対応する著作権コンテンツが不正に掲載されていないかどうかを調べることになる。各閲覧者それぞれは限られた著作権情報の検査を行うのみであるが、無数の閲覧者が訪問先のホームページ全てに対して個別の検査を行うことにより、全ホームページに対する全著作権情報に関しての正当性チェックが可能になると期待できる。

手順 ii において、コンテンツの透かしの検査が閲覧者の負担になってしまうことは避けるべきである。したがって、実際には透かしの検査機能を WWW ブラウザに組み込んで、ホームページデータを読み込んだ際にバックグラウンドで自動的に検査が行われるようにするなどの方策が必要となるだろう。ただし、現在、コンテンツを巧みに偽装して違法発信しているような悪質なホームページも実在する。巧妙な不正に対して

は、その正当性を自動的に（機械的に）チェックすることは難しい。積極的に賞金稼ぎを行いたいユーザは、このような悪質なホームページに対し手で偽装を解いた上で、著作情報に基づいてそのコンテンツの正当性をチェックすることができる。

本手法のコンセプトは、「ウェブサーフィンのついでに不正コンテンツのチェックも行ってしまう」というところにあり、基本的に（著作情報を取得するフェーズを除いて）閲覧者が通常のウェブサーフィンを行っている以外にコンテンツチェックのための余分なネットワークトラフィックは発生しない。ただし、一部のユーザが透かしの検査機能を持つエージェントロボットをインターネットに派遣するという方法を探ったとしても問題はないであろう。この場合、ロボットを派遣したユーザはまさしく「賞金稼ぎ」に相当することになる。なお、ロボットによる不正コピー探査はすでに商用ベースで行われている[11][12]。現時点においてはすでに goo や Google などの Web 検索エンジンサービス会社がホームページの情報を集めるためにロボットを使用しており、これらの会社がロボットに透かし検出機能を追加することにより、賞金稼ぎをも行うことなどが可能になると思われる。

ただし、ロボットによる探索では、ファイアウォール内の LAN 内部のコンテンツやアクセス制限が設定されているホームページのコンテンツの検査は不可能である。本手法は基本的にはユーザ個人に基づく不正コピー防止を提案するものであり、この方式ならば、閲覧者が訪れることができる全てのホームページにおけるコンテンツの正当性を検査することが可能である。また、多くの人が集まるホームページほど、一旦そこに不正コピーが掲載されると多数の閲覧者にその不正コピーが拡散し、被害が甚大となる。よって、人気の高いホームページほど不正コピーの監視を強化したいユーザ自身に不正コピーの監視を行わせる本方式ならば、人気のあるホームページほど多く閲覧者による検閲がかかることになるので、この要求も満足する。

3.5. 不正者の検挙

閲覧者からの通報の後、不正者が検挙されるまでの流れを示す(図 6)。

- i. 通報を受けた公的機関は、自らも当該ホームページを検査することにより、通報の真偽を確認する。
- ii. 通報が真実であった場合には、公的機関は当該ホームページを差し止め、ホームページ作成者(不正者)に何らかの罰則を科す。また、通報者に対しては何らかの報酬を与える。

当該ホームページの不正を最初に通知した通報者に報酬を与える。例えば、通報者への報酬として賞金

を与える場合には、不正者から罰金をとるなどしてその財源を確保することになる。

なおここで、通報者のプライバシーが外部に漏れないように配慮する必要がある。これは、摘発の後に通報者が不正者から報復を受けることを防ぐためである。

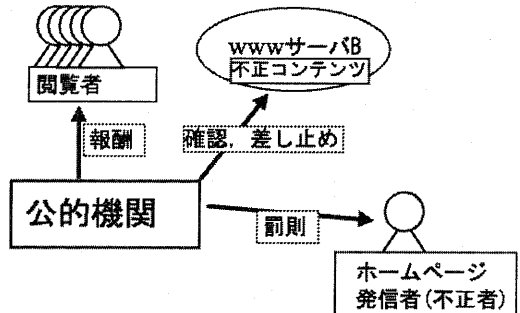


図 6. 不正者の検挙

4. 考察

4.1. 分散型監視方式の有用性

ホームページは世界中に限りなく散在している。著作コンテンツの数も無限である。すなわち、インターネットにおけるコンテンツの著作権管理のためには、ホームページの一つ一つに対して、全世界に存在する全ての著作コンテンツが不正に掲載されているかどうか調べなくてはならない。各閲覧者に不正のチェックを任せるという分散型監視方式は、このような膨大な情報を監視するのに適している。閲覧者一人一人は自分が閲覧しているホームページの中に、自分が取得している著作情報に対応する著作コンテンツが不正に掲載されていないかどうかを調べるのみであるので、その負担は軽い。そして、無数のユーザがこれを行うことによって、互いが互いを補いあい、全てのホームページに対して、全ての著作コンテンツに関する正当性チェックが実現するものと期待される。

集中型の監視を行おうと考えた場合、a) 公的機関が定期的に全ホームページをパトロールする方法や、b) 全てのホームページが WWW サーバにアップロードされる際にその正当性を検査されるような法的枠組みを整える方法をとることになると思われる。しかし、a) の方法においては、限られた数の公的機関がインターネット上に無数に存在する全てのホームページをパトロールすることは事実上、不可能である。また、両方法とも、一つのホームページに対し、全世界に存在する全ての著作コンテンツが不正に掲載されていないかどうかを調べる必要があり、現実的ではない。更に、a) の方法には、パトロールが巡回している間だけ不正なホームページを一時休止させるといったセキュリティホールが存在する。分散型監視方式であれば、いつ誰に

コンテンツの正当性をチェックされるか予想がつかないため、ホームページを一時休止して監視を逃れるということができない。更に、いつ誰に自分の不正が告発されるか分からないという状況は不正者にとって大きな脅威として感じられるため、不正に対する抑止効果も高いと期待される。

4.2. 通報者の利益と不正者への罰則

本稿において導入している「賞金稼ぎ」の仕組みは、あくまでも、不正コンテンツの発見に対する協力を一般ユーザに誘引するための一方法に過ぎない。少なくとも現在の日本の法制度においては、大規模な犯罪でない限り、不正コピーの犯罪に対する刑事罰、不正コピーによる損害賠償の民事請求が成立することは稀であり、不正者からの罰金をもって通報者への賞金にあてることは机上の空論と言えらる。

しかし、本方式における公的機関に JASRAC のような役割を与えるということや、警察のような機関が公的機関を運営することが電子社会の常識となれば、本方式の現実味は急激に高まると思われる。公的機関に JASRAC のような役割を与える場合、著作権者が著作権コンテンツを登録する際に公的機関に管理費用を支払うことになり、この一部が通報者への賞金の財源となる。警察が公的機関を兼ねる場合、公的機関は税金で運営されることになり、また、現在の交通違反者に反則金を支払わせるのと同様の仕組みにより不正者から罰金を徴収し、これを通報者への賞金に充てることが可能となる。

更に、ホームページを立ち上げる者は必ずデポジット金を預けるという方法も考えられなくもない。この場合、ホームページ発信者には、公的機関からのアクティベート情報が与えられた時点で初めて効力が発生するような電子マネー（例えば、Fair blind 署名技術 [16]）をホームページに添付することが義務付けられる。不正が発見されたホームページの電子マネーは、公的機関にアクティベートされた上で公的機関に徴収される。電子マネーはアクティベートされた時点で実際に口座からお金が引き出されるので、一般のユーザは実質的にはデポジット金なしでホームページを立ち上げているに等しい。

総括するに、本方式においては、一般ユーザに不正コンテンツの発見に対する協力を促すための何らかの仕組みが不可欠。すなわち、通報者に利益を与える必要がある。更に、不正を抑止するためには、不正者にはなんらかの罰則を与えることが望まれる。

4.3. 不正者の特定

例えば、不正を発見したユーザに対して賞金が支払われるとなると、「不正を行っておいて自ら通報する」という自作自演の問題が発生すると思われる。また、

発見者への賞金を不正者の罰金から支払うようにした場合、不正者が特定されない限り賞金を支払うことができない。更に、不正者が他人の身元情報を用いて不正なホームページを作成し、これを不正者が自ら通報することにより、濡れ衣を着せるといふ犯罪も考えられる。この場合は、身元を悪用された被害者に対して罰金が課せられてしまう。本方式を着実に機能させるためには違法ホームページを作成した不正者を確実に特定する必要がある。ただし、本稿は不正者を特定するための技術や方法を論ずることが目的ではないので、その具体的な方策についてはここでは考察の対象から除外することとする。

なお、本稿では、ホームページの改竄をチェックすることは可能である [3][4][5] という前提をおいているので、不正者が他人のホームページを改竄して違法なコンテンツを挿入し、これを自ら通報するということができないとしている。

4.4. 電子透かしの能力

本方式は正当性の検査を電子透かしにて行っているので、本方式における不正検出の能力は電子透かしの能力に依存することになる。例えば、電子透かしには、a) 情報中に膨大な冗長性分を持つ画像には適用しやすいが、プログラムなどへの適用が難しい、b) ユーザ A が購入したコンテンツがユーザ B のホームページから見つかった場合、B が当該コンテンツを盗み出したのか、A が B に不正に譲渡した (B は当該コンテンツが著作物であることは知らされていなかった) のか分からない、c) コンテンツが不正者により盗み出されて不特定多数にばら撒かれた場合、犯人を特定する手段はない、などの限界がある。

ただし、本方式は賞金稼ぎ型のコンテンツの分散監視方式を提案するものである。著作物の使用权の有無を検証できる手法であれば、電子透かし以外であっても、これを採用して構わない。

4.5. 関連方式との比較

本稿で提案した賞金稼ぎ型コンテンツ管理方式を 2 章で示した関連方式と比較した結果を表 1 に示す。本方式は全ての項目で他の方式とほぼ同等またはそれ以上の結果となり、本方式の有効性が示された。

5. まとめ

賞金稼ぎの仕組みを利用して、ホームページ上の著作コンテンツを分散管理する方式を提案し、関連手法と比較することによって本方式がインターネットのような広大な環境に無数に散在する情報を管理するのに有効であることを示した。今後は、本方式を実装すべく、具体的な詳細設計を行う。

表 1. 提案方式と関連方式の比較

	対象	検証者	公的機関の作業	閲覧者の作業	閲覧者側の作業の自動化	ネットワーク負荷	特筆すべき点
インターネットマーク	ホームページ	閲覧者 ・閲覧者がアクセス可能なホームページは全て検査可能 ・人気の高いホームページほど頻りに検査される	中程度 マークの発行	中程度 閲覧先のホームページのマークの検査	○ ブラウザのプラグインなどにより自動検証可能	○ マークの署名を検査するための公開鍵証明書を手前に取得する必要があるのみ	ホームページから抜き出されたコンテンツの監視は不可能
海賊版摘発方式	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 ・コンテンツの分布状況の情報は閲覧者から取得 ・実際に不正なコンテンツが存在するかの検査は公的機関側が行う	多い ・コンテンツの分布状況をデータベース化 ・不正なコンテンツの検査	中程度 閲覧先のホームページのコンテンツの情報の送信	○ ブラウザのプラグインなどにより自動通報可能	○ 閲覧者から全てのコンテンツの情報が公的機関に報告される	結局は、公的機関が一局集中でコンテンツを監視する方式
ロボット検索	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 ロボットを派遣	多い ・ロボットの派遣 ・不正なコンテンツの検査	二 閲覧者側が行う作業はない	二 閲覧者側が行う作業はない	○ ユーザのホームページ閲覧とは別にロボットがホームページにアクセスする	・全てのホームページを高頻度で検査することは難しい ・アクセスの許されていないホームページは検査できない
カプセル化	コンテンツ	二 該当しない	中程度 コンテンツを暗号化し、購入者に送信	中程度 暗号化コンテンツを復号する	○ ソフトウェアなどにより暗号化コンテンツを利用時にのみ自動的に復号することが可能	二 該当しない	・不正コピー監視ではなく、不正コピー防止が目的 ・正規購入者から復号鍵や復号されたコンテンツがの漏洩する危険あり
賞金稼ぎ型管理方式	コンテンツ 電子透かしが挿入可能なコンテンツ	閲覧者 ・閲覧者がアクセス可能なホームページは全て検査可能 ・人気の高いホームページほど頻りに検査される	中程度 ・著作情報の管理・通報があった際に、その事実の確認	やや多い ・自分の所有している著作情報に基づき、閲覧先のホームページに含まれるコンテンツが不正であるものかどうか検査 ・不正なコンテンツを発見した場合に公的機関へ通報する	○ ブラウザのプラグインなどにより自動検証・通報可能 ・悪質なホームページに対しては手動で検証することも可能	○ 著作情報を事前に取得する必要があるのみ ・不正コピーを発見した場合には公的機関へ通報する	・無数のユーザが漏い合うことにより、インターネット上の全てのコンテンツの常時監視が可能になると思われる ・積極的なユーザがロボットを派遣することも可能

文 献

- [1] S.Goldwasser, S.Micali, and R.Rivest, "A Digital Signature Scheme against Adaptive Chosen Message Attack," SIAM Journal on Computing, 17, 2, pp.281-308, 1998.
- [2] J.Zhao and E.koch, "Embedding robust labels into images for copyright protection," Proceedings of International Conference on Intellectual Property Rights for Information, knowledge and New Techniques, pp.242-251, Aug.1995.
- [3] インターネットマークス,
<http://www.tao.go.jp/prsr10102.htm>.
- [4] トリップワイヤ,
<http://www.tripwire.com/literature>.
- [5] 可部孝二, 西垣正勝, 曾我正和, 田窪昭夫, "ホームページ改竄パトロール方式," 情報処理学会研究報告, 2000-CSEC-8-30, pp.173-178, Mar.2000.
- [6] 板垣晋, 西垣正勝, 曾我正和, 田窪昭夫, "強化型ホームページ改竄パトロール方式," コンピュータセキュリティシンポジウム 2001, No.15, pp.403-408, Nov.2001
- [7] Napster, <http://www.napster.com/>
- [8] Gnutella, <http://www.gnutelliums.com/>
- [9] 山口和彦, 岩村恵市, 今井秀樹, "誤り適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.
- [10] 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.
- [11] エム研, http://www.mken.co.jp/product/acua_pict.html
- [12] インプレス, "NTT インテリジェントテクノロジー, 電子透かしによる著作権保護ビジネスを開始," <http://www.watch.impress.co.jp/internet/www/article/1999/0428/nttit.htm>
- [13] 山名早人, "WWW情報検索サービスの動向," <http://www.edtl.go.jp/http://www.edtl.go.jp/~yamana/Research/WWW/survey.html>
- [14] 三菱商事株式会社, "再暗号化," <http://www.reencryption.com/>
- [15] 森亮一, 河原正治, "歴史的必然としての超流通," 超編集・超流通・超管理のアーキテクチャシンポジウム講演論文集, pp.67-76, Feb.1994.
- [16] Markus Stadler, Jean-Marc Piveteau, Jan Camenisch, "Fair Blind Signatures," Advances in Cryptology, Eurocrypt'95, volume 921 of Lecture Notes in Computer Science, pp.209-219, Springer-Verlag, 1995.
- [17] 松下哲也, 西垣正勝, 曾我正和, 田窪昭夫, "賞金稼ぎの仕組みを利用したデジタル著作物の監視方式," 情報処理学会第62回全国大会(平成13年前期)特別トラック(3)講演論文集, No.8H-2, pp.103-108, Mar.2001.