Vol. 44 No. 8 情報処理学会論文誌 Aug. 2003

賞金稼ぎの仕組みを利用したディジタルコンテンツの監視方式

松下哲也[†1] 西垣正勝[†2] 曽我正和[†3]
田窪昭夫[†4] 中村逸一[†5]

アルゴリズム公開型の電子透かしを利用して，著作者から管理の依頼があったディジタルコンテンツの不正コピーが掲載されている違法ホームページを一般ユーザの協力により発見する仕組みを提案する．すべてのユーザが不正者を見つける「賞金稼ぎ」となりうる本方式によれば，不正者はだれ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，世界中には無数のホームページが存在するため，これらすべてを公的機関などが一極集中管理することは事実上，不可能である．提案方式はすべ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ィジタルコンテンツの管理に適した仕組みであるといえよう．本論文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とともに，インターネットにおけるコンテンツ監視に関する問題について考察する．

A Bounty Hunting-based Copyright Protection System for Website Content

Tetsuya Matsushita,[†1] Masakatsu Nishigaki,[†2]
Masakazu Soga,[†3] Akio Takubo[†4] and Itsukazu Nakamura[†5]

This paper proposes a distributed copyright protection system for registered 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 Web page visitor can verify the authenticity of the content on the Web page he/she is visiting. It allows, essentially, every net surfer to be a kind of bounty hunter who finds illegal content or Web 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 Web pages over the Internet. Moreover, in the proposed system, illegal Web 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 shows the efficiency of a bounty hunting-based copyright protection system by comparing it with the related systems, and discusses about how to achieve effective copyright protection by the system.

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みせた．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，それゆえにディ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憑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いえない．著作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．

†1 株式会社富士通ソーシアルサイエンスラボラトリ
Fujitsu Social Science Laboratory
†2 静岡大学情報学部
Faculty of Information, Shizuoka University
†3 岩手県立大学ソフトウェア情報学部
Faculty of Software and Information Science, Iwate Prefectural University
†4 東京電機大学環境情報学部
Faculty of Information Environment, Tokyo Denki University
†5 株式会社NTTデータセキュリティビジネスユニット
Security Business Division, NTT Data Corp.

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2つに集約されるものと思われる．まず第1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．誤った情報を鵜呑みにしてしまった閲覧者にはなんらかの被害が生じるであろう．さらに，ホームページに無断で誹謗中傷記事を上書きされて名誉を毀損されたり，ホームページに記載されている商品の金額情報などが改竄されて商取引に支障をきたしたりする場合など，そのホームページの発信者が甚大なる被害をこうむるケースもけっして少なくない．そして第2が，著作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したり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ぐ．その結果，良質なコンテンツが提供されることがなくなり，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1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，ディジタル署名[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)]．筆者らのグループも，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2の問題である著作コンテンツの違法発信を取り締まる方法の確立である．

著作物・著作権の取扱いは非常にデリケートな問題であり[7),8)]，ディジタルコンテンツの一元管理[9)]の是非に対する社会的コンセンサスさえ得られていない現状においては，技術先行で著作コンテンツ管理システムを設計しても現実とは乖離したものとなってしまう可能性が高い．しかし，音楽や絵画など著作権と著作料徴収の仕組みが社会的に確立している分野もあり，商品価値の高い著作コンテンツに対しては著作者の申し出によって当該コンテンツの海賊版（を発信しているホームページ）を発見することができる技術を構築することはけっして無意味ではないと考える．

さて，著作者からの依頼を受けて著作コンテンツの違法発信を取り締まるにあたって問題になるのは，インターネット上に存在するホームページの数である．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著作コンテンツのすべてを一元管理することは事実上，不可能である．概念的には，無限個のホームページを取り締まるためには無限回の検査が必要であり，警察のような一極集中型の公的機関のみがこれを行うには限界がある．インターネットに無限個の検査ロボットを派遣して自動チェックをすることも考えられるが，そのために無限個のトラフィックが余分に発生することになり，やはり現実的ではない．

そこで本論文では，アルゴリズム公開型の電子透かし[10),11)]を利用して，ホームページ閲覧者だれでもが，特定のコンテンツを違法に発信しているホームページを摘発することのできるコンテンツ監視方式を提案する．一般の閲覧者に違法コンテンツの摘発を依頼するにあたり，閲覧者になんらかのインセンティブ[12)]を与える必要もあるだろう．本方式では，違法ホームページを発見したユーザに取り締まりを依頼した著作者から報奨金のようなものを与えるという方法を考えている．これにより，一般の閲覧者すべてが不正なホームページを摘発する「賞金稼ぎ」となりうる．

本方式においては，基本的には，閲覧者は各自思いおもいに通常のウェブサーフィンを行っており，その際に自身が閲覧しているホームページの正当性を検査する仕組みとなっている．各閲覧者1人1人が行う仕事は最小であるが，無数の閲覧者がホームページの検査を行うことによって「無数のホームページを無数の閲覧者により監視する」という世界を実現している．事前に著作情報を取得する手続きを除き，余分なトラフィックも発生しない．また，不正者はだれ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，それゆえに不正行為の抑止効果も高まると期待される．

提案方式はすべ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 におけるディジタルコンテンツの監視に適した方式であるといえる．本論文では以降，2章で既存の関連方式を概説した後，3章で本方式の詳細を説明する．4章で本方式の技術的考察を行い，本方式と関連方式とを比較することにより本方式の有効性を検討する．また，5章では本方式の運用に対する考察を行い，本方式によってディジタルコンテンツの管理を行う際の様々な問題について考察する．最後に6章で本論文をまとめる．

2. 関連方式

インターネット上の著作コンテンツ管理方式および

不正コピー防止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ィ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1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違法コンテンツを監視する仕組みまでを議論した研究は，著者ら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（たとえば，1枚の画像のみ）が取り出され，他のホームページで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13)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．すなわち，公的機関は閲覧者から寄せられた無数の報告に対し，それらの真正性のチェックを一手に引き受けて実行する必要があり，その処理能力には限界がある．

また，一般利用者から寄せられる報告により，公的機関には「どのユーザがどのURLを閲覧したか」というプライバシーに関する情報が集約されることになる．よって，公的機関はその取扱いに強く配慮しなければいけない．

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[14),15)]．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．

文献16)によると，最新のアルゴリズムで複数のロボットを制御することにより，1日で1億ページ以上のホームページ情報を収集・検索可能である．しかし，文献17)の「インターネット上のホームページは2001年3月頃の時点で40億ページになっていた」との予測に依拠すると，ロボットがインターネット上の膨大なホームページをすべてひととおり走査するのに1カ月以上を要することになる．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，すべ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．

さらに，ロボットの探索により，余分なトラフィックが発生することも大きな問題である．また，ロボットによる機械的な探索では，ロボットにアクセス権が与えられていないLANやサイトの中のコンテンツの検査は不可能であり，（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したりするなどの方法で）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も難しい．

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コンテンツのカプセル化[18)]と呼ぶことにする．厳密にいえば，コンテンツのカプセル化は不正コピーを監視するのではなく，不正コピーそのものを防止することが目的である．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．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[19)]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[20)]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であり，自らのコンテンツの管理（違法発信の取り締まり）を公的機関に依頼した者を指す．発信者とは（対価を支払う

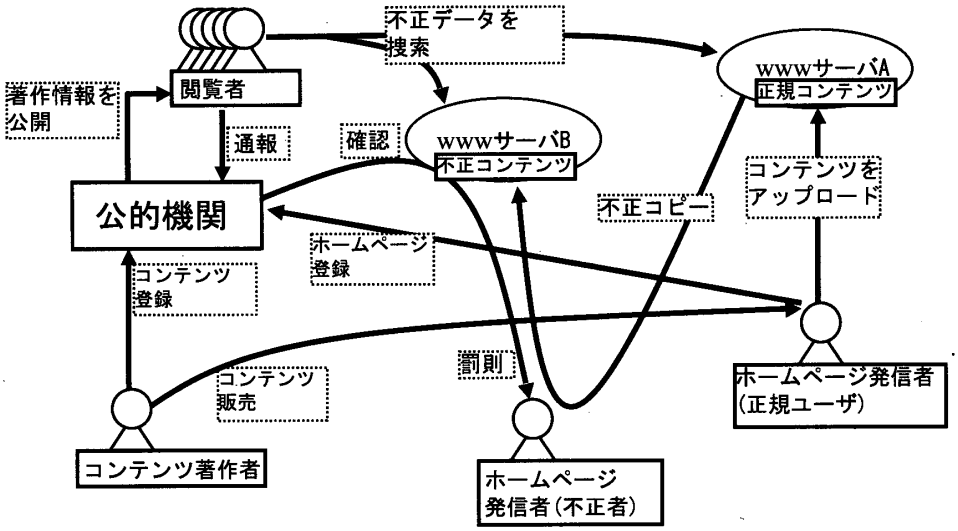


図1 賞金稼ぎ型監視方式
Fig. 1 A bounty hunting-based copyright protection system.

などにより）作成者の許可を得て，自らのホームページで当該作成者の著作コンテンツを発信する者である．作成者と発信者が同一である場合もある．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．公的機関は作成者から管理を依頼された著作コンテンツの著作情報を公開している．また，公的機関は賞金稼ぎに関する窓口となる．

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[10),11)]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．

(3) 著作情報の公開
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．

賞金首情報である「著作情報」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だれ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．

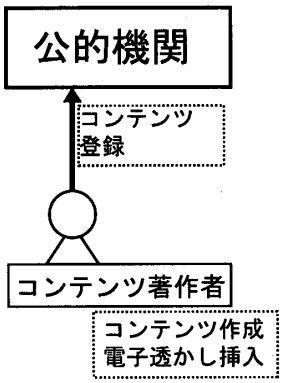


図2 コンテンツの登録
Fig. 2 Registration of a content.

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．

図1，図2には1つの公的機関しか記されていないが，単一の公的機関が多数のコンテンツの著作情報を一元管理できない場合には，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，たとえば著作者の所属（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．たとえば文献10)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．

なお，本方式では著作者は自らが作成したコンテンツのオリジナルデータをオンライン上に公開することはないという前提をおく．よって，クラッカーによりコンテンツのオリジナルデータが不正コピーされることはない．すなわち，不正に流出するコンテンツには必ず電子透かしが入っており，かつ，その著作情報がいずれかの公的機関に登録されていることになる．クラッカーが不正コピーの証拠を消すためには，透かしを削除または上書きして無効化する必要がある．それらの攻撃に対する耐性は採用する透かし方式に依存する．

また現実には，手順(iii)において，公的機関は著作者および著作物の認証を行う必要があると思われる．ただし本論文ではモデルの簡素化のため，これらの認証を行う機関については別途外部に設けられているという前提を置くことにする．

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（またはこれに相当するなんらかの契約）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) 著作者は当該発信者にコンテンツの使用を認めたことを公的機関に通知する．

(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．

発信者は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，発信者は変更のつど，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．

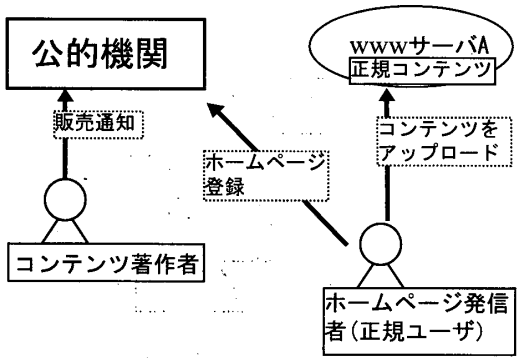


図3 ホームページの登録
Fig. 3 Registration of a home page.

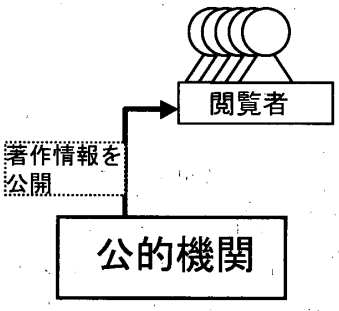


図4 著作情報の公開
Fig. 4 Publication of copyright information.

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．

なお現実には，手順(ii)，(iii)において，公的機関は著作者および発信者からの届け出を認証する必要があると思われる．ただし本論文ではモデルの簡素化のため，これらの認証を行う機関については別途外部に設けられているという前提を置くことにする．

3.3 著作情報の公開

公的機関が著作情報を公開する際の流れを示す（**図4**）．

(i) 公的機関は，著作者から管理（不正コピーの取り締まり）の依頼を受けたコンテンツに対して，それぞれのコンテンツ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「著作情報」としてデータ

ベース化する．

(ii) 公的機関は著作情報をホームページで公開する．著作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，著作情報を取得する．

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情報のみをデータベース化・公開する．

手順 (iii) において，a) どの公的機関の著作情報を取得するか，b) その公的機関が公開している著作情報のうち，どのコンテンツに対する著作情報を取得するか，c) 著作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コンテンツに対する著作情報を取得しておくと効率が良いだろう．c) に関しては，閲覧者は多数の著作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．また，閲覧者の PC の著作情報格納用ストレージの大きさにも左右される．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情報を渡すようにすればよい．この場合，基本的にはすべての著作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，特定の著作情報を重点的に高頻度で配布するようにしてもよい．

なお，著作権には有効期限があるため，公的機関はこれについても管理をする必要がある．具体的には，公的機関は著作コンテンツのそれぞれに対し，期限が切れた時点でコンテンツの著作情報の公開を取りやめる．著作情報の公開が中止となったコンテンツに対しては，その著作情報が閲覧者に届くことがなくなり，閲覧者による検査の対象から外される．なお，著作権の期限が切れてしばらくの間は，「時刻 T においてある閲覧者 A がコンテンツ a の著作情報を取得し，時刻 T+1 でコンテンツ a の著作権が切れ，時刻 T+2 で閲覧者 A が（時刻 T における著作情報に基づき）コンテンツ a を含む違法ホームページを発見し，これを公的機関に通報してしまう」という問題が発生しうる．しかし，本方式では通報があった際には公的機関がその真偽を確認するため（3.5 節参照），これについては誤報（悪意のない誤報）として取り扱えばよい．

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) 閲覧者は普段どお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．

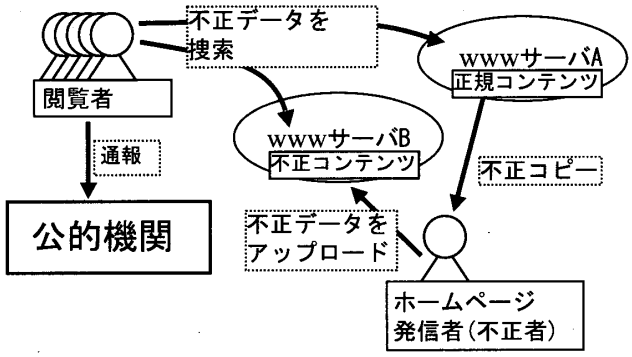


図 5 不正ホームページの通報
Fig. 5 Reporting an illegal home page.

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情報に対応する特定の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すべ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して，公的機関が公開しているすべての著作情報に関する正当性チェックが可能になると期待できる．

手順 (i) において，本方式ではアルゴリズム公開型の電子透かしを採用しているため，閲覧者は独力でコンテンツの透かしのチェックを行うことができる．すなわち，各閲覧者が透かしのチェックを行う際に余分なトラフィックは発生しない．ただし，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．しかし，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動で偽装を解いたうえで，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．

無限個のホームページを取り締まるためには無限回

の検査が必要であり，検査のために余分なネットワークトラフィックが発生することは好ましくない．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おう」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トラフィックは発生しない．ただし本方式は，一部のユーザが積極的に不正ホームページを発見する「賞金稼ぎ」として活動することを否定するものではない．たとえば，一部のユーザが透かし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してもよい．

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[14),15)]．また，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も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々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すべ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，いったんそこに不正コピー品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という要望がある．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，この要求も満足される．

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）になんらかの罰則を科す．また，通報者に対してはなん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．赤井らが提案しているインセンティブコンピューティング[12)]の概念によれば，この報酬が閲覧者に対するインセンティブとなる．著作権侵害の訴訟はしばしば裁判で争われるデリケートな問題であることを考えると，不正者から罰金を通報者への報奨金に転嫁することは難しいように思われる．この場合，公的機関はコンテンツの管理（不正コピーの取り締まり）を依頼した著作者から登録料や管理料などを徴集し，これを財源にして通報者への報酬金とするような運用が現実的かもしれない．具体的な通報者への報酬や不正者への罰則の方法を提示することは本論文の主旨ではないが，これについては5.3節で賞金稼ぎ型監視方式の運用における問題を考察する中である程度の検討を行う．なお，通報においては，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にも必要である．

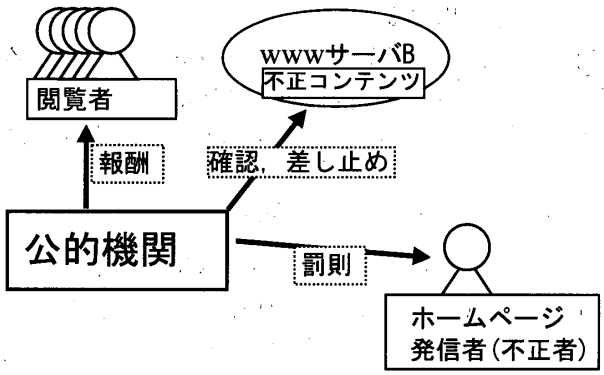


図6 不正者の検挙
Fig. 6 Punishing the illegal user.

4. 方式に関する考察

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おり，コンテンツの著作権管理のためにはホームページの1つ1つに対して当該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コンテンツ監視方式は，このような膨大な情報を監視するのに適しているといえる．閲覧者1人1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，「すべてのホームページに対して，公的機関に登録されているすべてのコンテンツが違法発信されていないかどうか」の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) すべ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が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すべ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，b) の方法においても法を破る者を漏らすことがないように完璧に運用することはやはり不可能であり，また，このような法的規制は一般ユーザの自由な情報発信を阻害する要因ともなりうる．

さらに，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う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，いつだれ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．さらに，いつだれ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

本論文において導入している「賞金稼ぎ」の仕組みは，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一方法である．一方，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必要がある．すなわち，本方式は「なんらかの利益を通報者に与えることによって一般ユーザに不正コンテンツの発見に対する協力を促し，かつ，罰則を与えることによって不正を抑止する」ものであり，インセンティブ・コンピューティング[12]の概念にペナルティという概念を追加した「インセンティブ & ペナルティ・コンピューティング」という位置付けに値すると考える．

このように，本論文の力点は賞金稼ぎ型のコンテンツの分散監視方式の提案におかれており，具体的な通報者への報酬や不正者への罰則の方法を提示することを意図するものではない．ただし，これについては5.3節で賞金稼ぎ型監視方式の運用における問題を考察する中である程度の検討を行う．

4.3 電子透かしの能力

本方式は正当性の検査を電子透かし[2]で行っているので，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．たとえば，電子透かしには，a) 情報中に膨大な冗長成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．

また，本方式において採用しているアルゴリズム公開型の電子透かし[10),11)]は，今のところまだ商用レベルまでの実用化には至っていない．適切なアルゴリズム公開型電子透かしの開発が今後の課題となる．

ただし，本論文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．著作物の使用権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，これを採用してかまわない．

4.4 関連方式との比較

本論文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**，**表2**に示す．本方式はすべ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っている．なお，比較結果における特筆すべき点については，関連方式の各々と本方式の差異という形でこれを以下にまとめる．

- インターネットマークとの差異：

  インターネットマークはホームページそのものの真正性を検査するものである．よって，インターネットマークが付されているホームページに掲載されている著作コンテンツを不正者が抜き出し，この著作コンテンツを使用して無断でホームページを作った場合，これを発見することはできない．一方，提案方式は当該コンテンツがどのURLで不正利用されたとしても，これを検出することができる可能性を有する．また，インターネットマークは閲覧者を保護するための仕組み（閲覧者が情報の信頼性を知るための仕組み）であり，著作者保護の観点に立つ提案方式とは立場が異なる．
- 海賊版摘発方式との差異：

  海賊版摘発方式においては，閲覧者は閲覧先のホームページのURLとそのホームページ上のコンテンツのIDを逐一，すべて公的機関に報告する．すなわち，公的機関には全閲覧者からの無数の報告が次々と届けられ，公的機関はその「無数の報告の中のすべてのURLとIDに対して」コンテンツの真正性の検査を行う．一方，提案手法においては，閲覧者が各自，閲覧先のホームページのコンテンツをチェックし，違法ホームページを発見した場合にのみ，そのコンテンツのIDとホームページのURLを公的機関に通報する．す

表1 関連方式との比較1
Table 1 Comparison of the related systems 1.

	対象	検証者	ネットワーク負荷
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繁に検査される	○ マークの署名を検査するための公開鍵証明書を事前に取得する必要があるのみ
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のみは閲覧者から取得 ・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	× 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
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	× 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
カプセル化	コンテンツ	ニ 該当しない	ニ 該当しない
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繁に検査される	○ ・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に通報する

表2 関連方式との比較2
Table 2 Comparison of the related systems 2.

	公的機関の作業	閲覧者の作業	閲覧者側の作業の自動化	特筆すべき点
インターネットマーク	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	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	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	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	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	多い ・ロボットの派遣 ・不正なコンテンツの検査	ニ 閲覧者側が行う作業はない	ニ 閲覧者側が行う作業はない	・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	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	・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	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は公的機関に通報する	○ ・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	・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

なわち，公的機関は通報の真偽を確認するために「通報があったURLとIDのみ」を検査する．提案手法は各閲覧者にコンテンツの不正を検査する手段を与えることにより，公的機関の仕事を劇的に減らすことに成功している．

- ロボット検索との差異：

ロボット検索は，結局はロボットを派遣する公的機関による一極集中型の検査であり，公的機関の負荷が高い．また，すべてのホームページを高頻度で検査することができない，ロボットがアクセスできないホームページはチェックできない，などの問題がある．一方，提案方式は各閲覧者が少しずつコンテンツの検査を分担することにより，公的機関の負荷を劇的に減らすことに成功している．また，人気のあるホームページほど多くの閲覧者により検査されることになる，閲覧者が閲覧可能なホームページをすべてチェック可能である，などの長所も有する．

- カプセル化との差異：

カプセル化は違法ホームページの発見を目的とするものではなく，不正コピーそのものを阻止するための方式である．正規購入者には復号鍵が渡

されるため，正規購入者はカプセル化コンテンツを復号してオリジナルコンテンツを手にすることが可能である．よって，正規購入者が悪意を持っていた場合には，正規購入者の手元からオリジナルコンテンツが漏洩する危険性をはらんでおり，かつ，オリジナルコンテンツの形で漏洩してしまったデータに対しては，その流布を防ぐ術がない．提案方式はコンテンツに埋め込まれている電子透かしによりコンテンツの真正性を検査するので，透かし入りコンテンツがどのホームページで不正使用されようとも，これをチェックすることができる．

5. 運用に関する考察

5.1 システムの完全性

ユーザが冤罪によって処罰されることがなく，悪用もされないように運用できなければ著作権管理システムとして社会的な同意を得られない．

冤罪に対しては，本論文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)~6)]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（または第三者に通報させる）ということはできない．しかし，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（または第三者に通報させる）ことにより，他人に濡れ衣を着せるという犯罪が起こりうる．

悪用に対しても，「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考えられる．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．

以上のように，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仕組みが必要不可欠である．

なお，冤罪に関連して，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（または第三者に通報させる）ことにより，そのホームページ所有者の社会的信用を失墜させるという，誤報に対する問題も存在する．誤報には，このように他人を陥れるための「悪意の誤報」と，閲覧者が本当に誤解をして通報をしてしまう「悪意のない誤報」がある．悪意の誤報に対しては，本論文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)~6)]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することはできない．悪意のない誤報に対しては，本方式では閲覧者からの通報に対して公的機関がその真偽を確認するという仕組みをとっており，その対処が可能である．

5.2 通報者のプライバシー保護

不正ホームページの通報により「通報者が当該ホームページを閲覧していた」という通報者のプライバシーに関する情報が通報者から公的機関に漏れることになる．よって基本的には，通報は匿名で行えるようにすべきであろう．通報者の匿名性は，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にも必要である．

ただし，通報の匿名性のみを求めると，虚偽や悪戯の通報が増えることになると思われる．通報が虚偽であっても通報があったというだけでそのホームページのイメージに傷がつき，名誉が毀損されることも往々にして起こりうる．よって，リング署名[21)]などを活用することにより，通報者の匿名性を保証しつつ通報の信頼性を保つような仕組みが必要である．

5.3 通報者への報酬と不正者への罰則

現在の著作権法においては著作権の侵害問題は親告罪（著作権法第123条）であり，著作者の告訴によってはじめて犯罪かどうかが裁判で争われることになる．そして，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る[7),8)]．すなわち，違法ホームページの差し止めや罰則としての損害賠償の請求には通常，金銭的，時間的にコストがかかり，よって，公的機関が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難しいといえる．

しかし，インターネットで公開されたディジタルコンテンツは短時間で大量に広がりうるため，不正コピーによりその経済価値は急速に失われていくという現状を考慮するに，実社会の既存の著作権法を電子社会に応じた形態で適用することを検討することも重要であると著者らは考える．

不正コピーを容易かつ迅速に摘発し，不正者に罰則を与える一方法としては，著作権侵害の非親告罪への移行と，現在の道路交通法における反則制度，点数制度のような体制の導入が効果的であろう．

具体的には，まず，著作者に認められているURL以外に著作コンテンツを置くことに対する罰則を定める（道路交通法8章に相当）．本賞金稼ぎ型監視方式においては，公的機関が公開している著作情報の中でコンテンツの掲載を認めているURLを著作者が宣言しているととらえることができるため，そのURL以

外のホームページ上に当該コンテンツが存在している場合には，著作者の告訴を待たなくてもこれを罪に問うことができるのではないかという考えに立脚し，この罰則に対しては非親告罪の扱いとする．そのうえで，反則行為に対する特例措置を設定して，たとえば反則金を支払うことにより公訴の提起を免ずる（道路交通法9章4節に相当）ことにより，公的機関（警察に相当）が容易かつ迅速に違法ホームページを差し止めたり，不正者に罰則を科すことができるようになる．この場合，徴収された反則金を発見者への報奨金として利用することが可能となり，違法ホームページが発見されるたびに不正者から反則金を徴集し，これを通報者に報奨金として支払うことが可能となる．

また，インターネットを電子社会における公共の道路であるととらえると，たとえばホームページを立ち上げるためには免許証が必要であるという制度を設けることも一考に値するのではないかという考えに立脚すれば，不正者は点数制度のような行政処分によって免許が取り消される（道路交通法103条に相当）というような方法も罰則として有効だと思われる．

なお，JASRACのような著作者の代行機関としての役割を公的機関に与えることにより，本賞金稼ぎ型監視方式を現在の著作権法のもとで運用することも可能であるかもしれない．本論文ではその詳細の検討については今後の課題とするが，著作者と公的機関との手続き（依頼または契約）や公的機関の種別などについて具体的な制度の取り決めが必要となるものと思われる．

5.4 コンテンツの著作権

著作権はコンテンツを創作したときに自動的に発生するが，ディジタルコンテンツはいつだれによって作成されたかが分かりにくい．提案方式も登録されたコンテンツの不正使用の有無を捜索するものであり，正当な著作権そのものを認定する能力はない．よって，たとえばある著作者Aが自分のコンテンツaを著作権フリーで公開しており，悪意を持つ者Bがそのコンテンツに「コンテンツaの著作者はBである」という電子透かしを埋め込み，その管理を公的機関に依頼した場合などには，大きな問題となる．登録された著作コンテンツを本方式を用いて管理するにあたり，管理の依頼を受けた著作コンテンツが確かにその依頼主の著作物であることが保証されている必要がある．

著作権フリーのコンテンツを他者に横取りされてしまうような問題を防ぐ1つの手段として，すべてのコンテンツにユニークIDを付し，これを公的機関に登録するという方法が考えられる[9),24)]．しかし，ディジタルコンテンツの一元管理は，一般ユーザの自由な情報発信を阻害する要因ともなりうるなどの理由で，その是非に対する社会的コンセンサスはいまだ得られていない．

また，著作コンテンツの認定に関しては，類似したコンテンツがあった場合にそれが盗作であるかどうか判断することが難しいという根本的な問題も潜在している．少なくとも日本では盗作裁判の事例自体がそれほど多くなく，かつ，盗作であるかの判断基準は2つの作品が似ているかどうかを判定しているにすぎない[22)]．

5.5 全コンテンツの管理

極端な仮定を設け，「世界中のすべてのディジタルコンテンツにはユニークIDが付され，アルゴリズム公開型電子透かしによりその著作情報が埋め込まれている場合に，無数の一般ユーザが賞金稼ぎに協力してくれる」のであれば，本方式により世界中のすべてのコンテンツを効率的に監視することも不可能ではないと期待される．

各閲覧者は一握りのコンテンツに対する著作情報のみを持ち，普段どおりのウェブサーフィンを行うのみである．閲覧者1人1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，無数のユーザが補い合うことにより，すべてのホームページに対して，世界中のすべ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．

ただし，ここではあくまでも「技術的な観点からは，インターネット上のすべてのディジタルコンテンツの著作権の管理を本方式により実施することも可能であるかもしれない」という技術的な実現可能性を述べているにすぎない．その技術を確立する前に，インターネット上のすべてのディジタルコンテンツの著作権を完璧に管理すべきか否かというところから十分に議論することが大切であろう（電子社会の著作権に関しては，これを否定するLessig[23)]などの意見が少なからず聞かれる一方で，コンテンツIDフォーラム[24)]などは「すべてのコンテンツの登録と管理」を提唱しており，著作権の是非に対しては現在のところに完全に二極化している状態であるといえる）．

6. まとめ

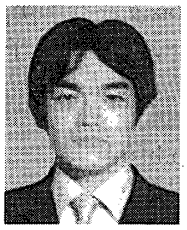
賞金稼ぎの仕組みを利用して，一般ユーザの協力による分散管理によって不正コピーからコンテンツを保護する方式を提案した．関連手法と比較することによっ

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．また，提案方式を運用した場合に生ずる，ディジタルコンテンツ管理の問題について述べた．今後は，本方式を実装し，技術的・社会的な視点に立って様々な実証実験を行い，本方式の実用性を評価したい．

参考文献

1) Goldwasser, S., Micali, S. and Rivest, R.: A Digital Signature Scheme against Adaptive Chosen Message Attack, *SIAM Journal on Computing*, Vol.17, No.2, pp.281–308 (1998).
2) Zhao, J. and Koch, E.: Embedding robust labels into images for copyright protection, *Proc. International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies*, Vienna, Austria, pp.242–251 (1995).
3) 洲崎誠一，吉浦 裕，永井康彦，豊島 久，佐々木良一，手塚 悟：Webサイトの真正性を確認可能とするインターネットマークの提案，情報処理学会論文誌，Vol.41, No.8, pp.2198–2207 (2000).
4) トリップワイヤ. http://www.tripwire.com/literature (2003.4.3 確認).
5) 可部孝二，西垣正勝，曽我正和，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 (2000).
6) 板垣 晋，西垣正勝，曽我正和，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 (2001).
7) 稲葉宏幸：IT時代の著作権を考える，*Computer Today*, No.105, pp.73–78(2001).
8) 中根哲夫：P2P技術によるデジタルコンテンツ流通と著作権の行方，*Computer Today*, No.109, pp.62–68 (2002).
9) 岸上順一，阪本秀樹，藤井 寛：デジタルコンテンツの著作権保護とコンテンツID，*Journal of Technology Transfer*, Vol.23, No.6 (2000).
10) 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 (1999).
11) 黒田圭一，西垣正勝，曽我正和，田窪昭夫：公開鍵暗号を用いたアルゴリズム公開型電子透かし，2002年暗号と情報セキュリティシンポジウム予稿集，pp.763–768 (2002).
12) 赤井健一郎，松本 勉：インセンティブコンピューティングとその特徴，コンピュータセキュリティシンポジウム2002論文集，Vol.2002, No.16, pp.355–360 (2002).
13) 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, p.2.C (1998).
14) エム研. http://www.mken.co.jp/index_jp.html (2003.4.3 確認).
15) インプレス：NTTインテリジェントテクノロジ，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 (2003.4.3 確認).
16) 日本電信電話株式会：国内の全Webページを網羅する「新鮮情報検索エンジン」の実証実験を開始，2002.12.3 報道発表資料. http://www.ntt.co.jp/news/news02/0212/021203.html (2003.4.3 確認).
17) 武田浩一，野美山浩：サイト・アウトライニング—インターネットからの情報収集と可視化技術，情報処理学会誌，Vol.42, No.8, pp.781–786 (2001).
18) 穴澤健明，武村浩司，常広隆司，長谷部高行，畠山卓久：コンテンツ保護の柔軟化を実現した開放型超流通基盤，情報処理学会研究報告 EIP-14-5 (2001).
19) 三菱商事株式会社：再暗号化. http://www.reencryption.com/ (2003.4.3 確認).
20) 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論文集，pp.67–76 (1994).
21) Rivest, R., Shamir, A. and Tauman, Y.: How to Leak a Secret, *ASIACRYPT2001*, Vol.2248 of Lecture Notes in Computer Science, pp.552–565 (2001).
22) 高等裁判所：知的財産権判決速報，H14.9.6 東京 高裁平成 12(ネ)1516 著作権 民事訴訟事件 (2002.9.6). http://courtdomino2.courts.go.jp/chizai.nsf/Listview01/7DC32FC8D5ABA0A749256C7F0023A165 (2003.4.3 確認).
23) Lessig, L.: *The future of Ideas*, Random House, Inc (2001).
24) コンテンツIDフォーラム. http://www.cidf.org/ (2003.4.3 確認).

(平成14年12月11日受付)
(平成15年 6月 3日採録)



松下　哲也

平成13年静岡大学情報学部情報科学科卒業．平成15年同大学大学院情報学研究科博士前期課程修了．現在，株式会社富士通ソーシアルサイエンスラボラトリに勤務．在学中，情報セキュリティに関する研究に従事．

西垣　正勝（正会員）

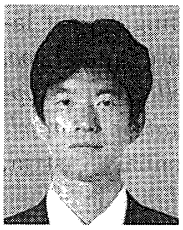
平成2年静岡大学工学部光電機械工学科卒業．平成4年同大学大学院修士課程修了．平成7年同大学院博士課程修了．日本学術振興会特別研究員（PD）を経て，平成8年静岡大学情報学部助手，平成11年同講師，平成13年同助教授，現在に至る．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シミュレーション等に関する研究に従事．

曽我　正和（正会員）

昭和33年京都大学工学部電子工学科卒業．昭和35年同大学大学院修士課程修了．昭和35年～平成8年三菱電機，計算機製作所副所長，情報電子研究所所長を経て平成8年静岡大学情報学部教授，平成11年岩手県立大学ソフトウェア情報学部教授，現在に至る．博士（工学）（東京大学）．汎用計算機，制御用計算機，制御用システムの開発．フォールトトレラントシステム，セキュリティシステムに関する研究に従事．IEEE，電子情報通信学会各会員．

田窪　昭夫（正会員）

昭和41年早稲田大学理工学部電気工学科卒業．昭和43年同大学大学院理工学研究科修士課程修了．同年三菱電機株式会社入社，平成10年静岡大学大学院博士後期課程修了．平成14年東京電機大学情報環境学部教授．博士（工学）．モバイルコンピューティング，ネットワーク・セキュリティ，個人情報保護，情報倫理等に興味を持つ．電気学会，IEEE，ACM各会員．



中村　逸一（正会員）

昭和60年茨城大学工学部卒業，昭和62年同大学大学院修了．同年日本電信電話株式会社入社．LANシステムの研究に従事．平成8年より（株）NTTデータでセキュリティ技術の研究・開発に従事．現在，同社セキュリティビジネスユニット部長．