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

洲崎誠一[†] 吉浦裕[†] 永井康彦[†]
豊島久[††] 佐々木良一[†] 手塚悟[†]

WWWシステムを単なる情報伝達の手段としてだけでなく，電子商取引システムのようにビジネスに活用しようという動きが顕著である．電子商取引システムでは，様々なマークが利用されている．販売者のWebページ上に，決済方法に関する情報として，利用可能なクレジットカード会社のロゴマークが貼付されているのはその一例である．しかし，従来のマークは単なる画像データなので，偽造や改ざん，不正コピーなどが容易にできてしまう．そこで，本稿では，販売者のWebページを閲覧する消費者が，当該Webサイトの真正性を確認可能とするインターネット・マークを提案する．インターネット・マークでは，Webページを構成するコンテンツや，そのWebページを公開するURL，IPアドレスなどといった複数の情報に対して，ディジタル署名を施し，その結果をマークに透かし込む．ブラウザを使ってWebページを閲覧した消費者は，当該Webページに貼付されたインターネット・マークに透かし込まれている埋め込み情報を抽出し，現在閲覧しているWebページのコンテンツ，URL，IPアドレスなどと比較・検証することで，不正の有無を確認することができる．実際にプロトタイプシステムを開発して評価を行い，インターネット・マークの有用性を確認した．

Internet-Marks: Reliable Visual Marks for the Web Site Authentication

Seiichi Susaki,[†] Hiroshi Yoshiura,[†] Yasuhiko Nagai,[†]
Hisashi Toyoshima,[††] Ryoichi Sasaki[†] and Satoru Tezuka[†]

Recently, various values visual marks are effectively used in business applications. For example, in many Web pages different credit card company's logo are attached as a source for payment information. In this case, one glance at these logos will make the customer able to recognize automatically the payment method. However, these marks are easy to forge, tamper with and copy into unauthorized Web site because they are only graphic data. And no method is offered to consumers to confirm the authenticity of logo marks. This insecurity causes serious problems with business application. To resolve these problems, in this paper, we propose Internet-Marks; reliable visual marks for the Web site authentication. Internet-Marks enables to detect illegal acts by the combination of traditional digital signature and digital watermarking techniques.

1. はじめに

近年，インターネットのようなオープンなネットワークを介して複数のユーザに情報を開示・伝達する手段として，World Wide Web（WWW）サーバとブラウザとを用いるWWWシステムが急速に普及している．また最近では，このWWWシステムを単なる情報伝達の手段としてだけでなく，ビジネスに活用しようという動きが顕著であり，たとえば，電子商取引などはそのようなビジネス利用の代表例である．

電子商取引を目的としたWebサイトの総数は，1998年にはすでに1万サイト以上に達している．ところが，電子商取引では，消費者と販売者との間の交渉がネットワークを介した非対面なやりとりであり，消費者はWebサイトのアドレスやWebページの情報だけを頼りに取引を行うため，以下のような様々な問題が生じている[1),2)]．

- Webサイトのなりすまし
  他の販売者のWebサイトになりすますことによっ

† 日立製作所システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.
†† 日立製作所公共情報事業部
Government & Public Corporation Information Systems Division, Hitachi, Ltd.

て消費者をだまして取引する．

- 悪意を持ったWebサイト
  料金を受け取ったにもかかわらず商品を送らないなどといった不正行為を意図的に行う．
- 不明確なサービス内容によるトラブル
  提供される商品（サービス）の内容や価格，支払方法などが不明確なため，取引後になって様々なトラブルが発生する．

上記のような問題に対し，ビジュアルなマークを用いた以下のような対策がなされている．

- 販売者が自己のロゴマークをWebページに貼付することにより，どの販売者のサイトであるかを消費者が確認可能とし，なりすましを防止する．
- サイト認定機関が各販売者のWebサイトを評価し，優良サイトであることを示す認定マークや，評価値を示すレイティングマークを交付する．販売者が交付されたマークを自己のWebページに貼付することにより，消費者が悪意を持ったサイトを避けたり，サービスレベルを認識できるようにする．欧米では，この認定業務が新たなビジネスとなりつつある[3),4)]．また，日本でも，公的な立場から認定機関の設立が進められている[4),5)]．
- 販売者が利用可能なクレジットカード会社のロゴマークを自己のWebページに貼付することにより，消費者が支払手段を確認可能とする．

このようなマークは，それ1つで消費者に対して多くの情報を伝えている．なぜなら，マークを見た消費者は，自己の経験や知識に基づいてイメージを膨らませ，総合的に物事を判断しているからである．たとえば，同じクレジットカード会社のロゴマークであっても，そのクレジットカード会社のWebページに貼付されていれば，消費者は単なるロゴマークと判断するが，販売者のWebページに貼付されていれば，文字による説明がなくても，消費者は，その販売店が当該クレジットカード会社の正規加盟店であり，そのクレジットカードを使って支払い可能だと判断する．

上記対策は，以上のようなマークの特性を有効に利用したものであり，リアル世界の商取引においても広く用いられているものである．

ところが，バーチャル世界の電子商取引で用いられるマークは単なる画像データである．そのため，偽造や改ざん，不正コピーなどが容易であり，以下のような新たな不正が生じている．

- Webページの改ざん
  マークが貼付された他の販売者のWebページの内容を不正に変更する．これにより，他の販売者の商行為を妨害する．
- マークの不正貼付
  他の販売者のWebページからマークを不正にコピーし，自己のWebページに貼付する．これにより，他の販売者になりすましたり，サイト認定機関から認定を受けた販売者であるかのように見せかける．
- マークの改ざん
  マーク自体の外観を不正に書き換える．たとえば，サイト認定機関からBランクであると認定され，Bランク用マークを受け取っているにもかかわらず，それをAランク用マークに書き換えて自己のWebサイトに貼付する．これにより，サイト認定機関から高い評価を受けた販売者であるかのように見せかける．

そこで，これらの課題を解決するために，本稿では，消費者がWebサイトの真正性を確認可能とするインターネット・マークを提案する[6),7)]．

本稿では，2章において，インターネット・マークのコンセプトを明確にするとともに，その実現方式や特徴について述べる．3章では，インターネット・マークの基本的な利用例として，Webサイト認証システムについて説明する．さらに，4章では，開発したプロトタイプシステムを用いてインターネット・マークの評価を行う．

2. インターネット・マークの概要

2.1 基本コンセプト

インターネット・マークは，Webページに貼付するための不正検出手段を備えたマークであり，Webページを閲覧する消費者に対して，Webページの内容が真正なものであるかどうか，当該Webページに当該マークが貼付されているという事実が真正なものであるかどうか，当該マークが明示する情報が信用するに足るものであるかどうか，などといったことを確認する手段を提供するものである．

このようなことを実現するために一般に用いられる技術はディジタル署名である．ただし，ディジタル署名は単なるビット列であり，視認性がないため，真正性を検証した結果を消費者に伝える手段が別途必要となる．しかし，検証結果をダイアログボックスなどを用いて表示するようなシステムの場合，そのダイアログボックスが何を意味しているのか（検証結果が表示されたのか，何らかのエラーが発生したのかなど）を消費者がその都度判断しなければならないなど，技術に不案内な一般の消費者にとって，必ずしも分かりや

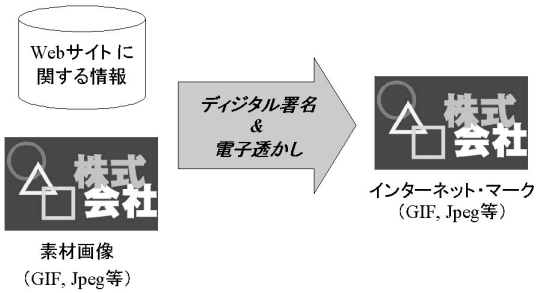


図1 基本コンセプト
Fig. 1 Basic concept.

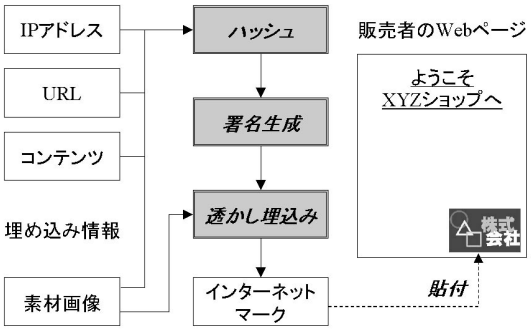


図2 インターネット・マークの生成
Fig. 2 Issuing Internet-Mark.

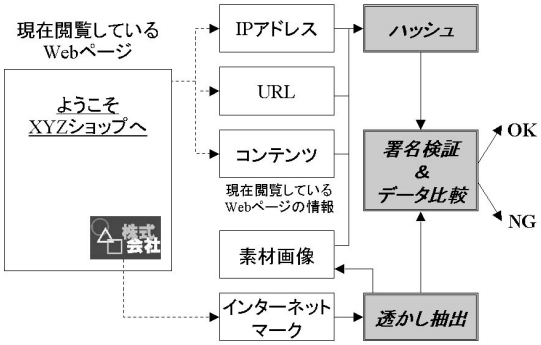


図3 インターネット・マークの検証
Fig. 3 Verifying Internet-Mark.

すいシステムであるとはいえない．また，同一 Web ページに検証すべきディジタル署名がいくつも付加されていた場合に，複数のダイアログボックスが表示されるようなシステムでは使い勝手も悪くなってしまう．

そこで，インターネット・マークでは，ビジュアルなマークを利用して消費者に様々な情報を伝達するという枠組みが，リアル世界，バーチャル世界のいずれにおいてもすでに広く利用され，浸透していることや，消費者の使い勝手などを考慮し，従来のディジタル署名技術と電子透かし技術[8]とを組み合わせることによって，安全性だけでなく視認性をも確保し，一般消費者にとって分かりやすく，受け入れられやすいシステムとした（**図1** 参照）．

2.2 実現方式

図2 はインターネット・マークの生成方法であり，**図3** はその検証方法である．

図2に示すように，インターネット・マークは，Web ページを構成するコンテンツ〔インターネット・マークの素材となる画像（素材画像）も含む〕や，その Web ページを公開する URL，IP アドレスなどといった複数の埋め込み情報に対して，ディジタル署名を施し，その結果を当該素材画像に透かし込むことによって生成する．販売者は，このインターネット・マークを上記 Web ページに貼付した後，WWW サーバを使って公開する．

一方，ブラウザを使って Web ページを閲覧した消費者は，図3に示すように，当該 Web ページに貼付されたインターネット・マークから透かし込まれている情報を抽出して，施されているディジタル署名を検証した後，それら埋め込み情報と現在閲覧している Web ページのコンテンツ，URL，IP アドレスなどが一致しているかどうかを確認する．

このような処理を行うことにより，インターネットマークでは以下を保証している．

- Web ページのコンテンツに対するディジタル署名を埋め込み，検証することで，当該インターネット・マークが貼付された Web ページの内容が，インターネット・マーク発行時から何ら変わっていないことを保証している（Web ページの改ざんの検出）．
- Web ページの URL や IP アドレスに対するディジタル署名を埋め込み，検証することで，当該インターネット・マークが正規の Web サイトに貼付されたものであり，別サイトからの不正コピーではないことを保証している（マークの不正貼付の検出）．
- 素材画像に対するディジタル署名を埋め込み，検証することで，当該インターネット・マークのデザインが，それを発行したときから何ら変わっていないことを保証している（マークの改ざんの検出）．

ただし，何を埋め込み情報とするかということは，そのシステムでインターネット・マークを利用する目的によって様々なバリエーションがあり，上記情報のすべてを必ずしも埋め込む必要はない．また，これ以外の情報を埋め込み情報とする場合もある．たとえば，マークに有効期限を持たせたければ，利用開始日時と

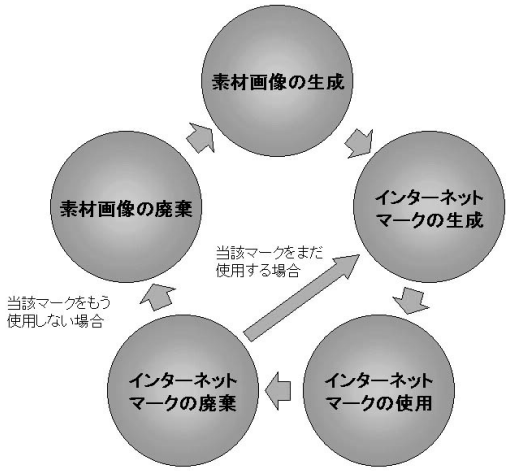


図 4 ライフサイクル
Fig. 4 Lifecycle.

終了日時とを埋め込むようにすればよい．また，有効期限内でのマークの無効化を行いたければ，マークの識別番号を埋め込むようにすればよい．

2.3 運用サイクル

実際にインターネット・マークを利用する際には，以下に示すようなライフサイクルに基づいて運用する（**図 4** 参照）．

- 素材画像の生成
  インターネット・マークの元となる画像データを生成する．この素材画像の状態では，特定の Web ページとの相関はない．
- インターネット・マークの生成
  素材画像と埋め込み情報とからインターネット・マークを生成する．インターネット・マークの状態になることによって，はじめて特定の Web ページとの相関が生じる．
- インターネット・マークの使用
  Web ページにインターネット・マークを貼付して公開する．また，インターネット・マークを用いて Web サイトの真正性を検証する．
- インターネット・マークの廃棄
  使用する必要がなくなったインターネット・マークを廃棄する．
- 素材画像の廃棄
  使用する必要がなくなった素材画像を廃棄する．

2.4 特　　徴

インターネット・マークの特徴を以下にまとめる．

(1) 安全性

インターネット・マークの安全性は，基本的にはディジタル署名技術の安全性と同等である．

(2) 視認性

インターネット・マークでは，電子透かし技術を用いて，素材画像の外観をほとんど変化させないように情報を埋め込んでおり，従来のマークと同等の視認性を有している．

(3) 操作性

インターネット・マークでは，マークとディジタル署名とを一体不可分としており，販売者は従来のマークと同じように Web ページに貼付するだけでよい．

(4) 応答性

インターネットマークでは，それ自体に透かし込まれている情報のみを用いて不正の有無を検証しており，基本的にすべての検証処理は消費者が使用する端末に閉じて行われる．

3. Web サイト認証システム

本章では，クレジットカードを用いて決済する電子商取引システムを例に，インターネット・マークを利用した Web サイト認証システムの概要を説明する．

3.1 システム構成

本システムは以下に示す 4 つのエンティティによって構成される．各エンティティは，ネットワークを介して互いにデータのやりとりを行うことができる．

- 認証局
  認証局とは，本システムの各エンティティに対して，公開鍵暗号を用いてディジタル署名の生成・検証を行う際に使用する電子証明書を発行する Trusted Third Party である．
- インターネット・マーク発行者
  インターネット・マーク発行者（以降では，単に発行者と略す）とは，販売者からの要求に応じてインターネット・マークを発行するクレジットカード会社，あるいは，クレジットカード会社から委託されてインターネット・マークの管理業務を行う組織である．
- 販売者
  販売者とは，自己の Web ページに発行者から受け取ったインターネット・マークを貼付する Web サイトのオーナであり，また，クレジットカード会社の加盟店である．
- 消費者
  販売者の Web サイトを閲覧する一般消費者である．

3.2 認 証 手 順

本システムにおいて，販売者の Web サイトの認証は，以下の手順に従って行う．ただし，認証局による電子証明書の発行は事前に行われており，各エンティ

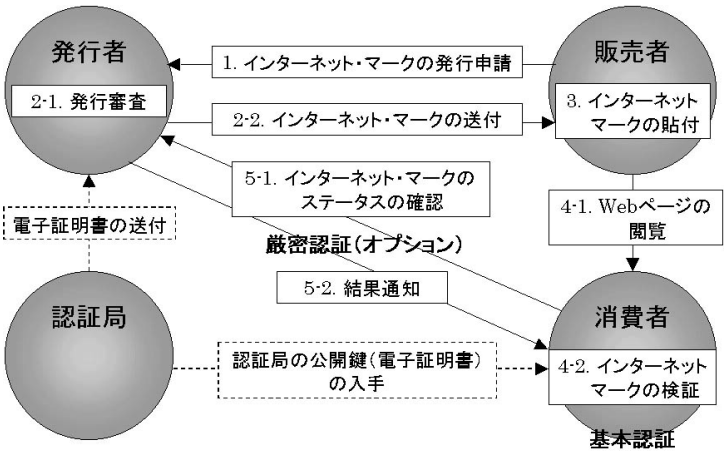


図 5 Web サイト認証システム
Fig. 5 Web site authentication system – Protocol.

ティはディジタル署名の生成，検証を正しく行うことができる環境にあるものとする（**図 5** 参照）．

(1) 販売者は，自己の Web ページのコンテンツや，URL，IP アドレスなどといった申請情報を発行者に送ってインターネット・マークの発行申請をする．

(2) 発行者は，インターネット・マークの発行申請のあった販売者に対してインターネット・マークを発行するか否かを審査し（発行者がクレジットカード会社から委託されてインターネット・マークの管理業務を行う組織の場合，審査はクレジットカード会社が行う），発行することに決めた場合にのみ，前記販売者から送られてきた申請情報と，有効期限などといった発行者が設定する付加的な属性情報に対してディジタル署名を施す．さらに，これら申請情報，属性情報，ディジタル署名と，自己の電子証明書とをひとまとめにし，素材画像（当該クレジットカード会社のロゴマーク）に透かし込んで当該 Web ページ用のインターネット・マークを生成し，それを販売者に返送する．

(3) 販売者は，発行者から送られてきたインターネット・マークを自己の Web ページに貼付した後，WWW サーバで公開する．

(4) ブラウザを使って Web ページを閲覧する消費者は，販売者の Web ページに貼付されているインターネット・マークから透かし込まれている各種情報を抽出し，発行者の電子証明書を使ってディジタル署名を検証する．さらに，ディジタル署名の正当性が確認できた場合にのみ，現在，ブラウザで閲覧している Web ページのコンテンツ，URL，IP アドレスと，インターネット・マークから抽出したものとが一致しているかどうかを検証する．また，有効期限など発行者が設定した属性情報も併せて確認する．

上記手順に従うことにより，消費者は，販売者がクレジットカード会社の正規加盟店であるかどうか，Web ページの内容が真正なものであるかどうか，などといったことを正しく確認することができる．この認証手順を基本認証と呼ぶ．

しかし，発行者がインターネット・マーク発行後に当該インターネット・マークを発行した事実を取り消す必要が生じた場合（たとえば，加盟店の取消し），基本認証では対応することができない．そのような場合，消費者は，上記手順に加えて，インターネット・マークのその時点でのステータスを発行者に別途確認することが必要となる．この認証手順を基本認証に対して厳密認証と呼ぶ（図 5 の 5-1，5-2 の処理）．ただし，厳密認証はオプションであり，実行するかどうかは消費者が選択可能としている．

4. 評　　価

3 章で説明した Web サイト認証を行うプロトタイプシステムを開発した．**図 6** にその画面例を示す．本章では，そのプロトタイプシステムを用いて行ったインターネットマークの評価について述べる．

4.1 プロトタイプシステムの概要

本プロトタイプシステムの概要を以下に示す．

(1) 埋め込み情報と素材画像

コンテンツ，URL，IP アドレス，有効期限，識別番号，発行者の公開鍵証明書など 2 K バイト程度のデータを埋め込み情報とした．また，素材画像として

マーク検証成功時　　マーク検証失敗時

図 6　プロトタイプの画面例
Fig. 6　Implementation – Result display.

は JPEG 画像を使用した．

(2)　ディジタル署名方式

公開鍵暗号アルゴリズムとして鍵長 1024 ビットの RSA 暗号を，また，ハッシュ関数として SHA-1 を使用した．

(3)　電子透かし方式

本プロトタイプシステムでは，JPEG 圧縮の中間データである DCT（Discrete Cosine Transformation）係数に情報を埋め込んでいる．JPEG 圧縮の DCT は，8×8 ピクセルの部分画像ごとに実行され，この部分画像が，8×8 の DCT 係数に変換される．本方式では，この DCT 係数のうち中および高周波成分に相当する 36 個の係数について，その下位 2 ビットを，埋め込み情報で置き換えている．すなわち，8×8 ピクセルの部分画像ごとに 72 ビットを埋め込む．具体的な埋め込みのアルゴリズムは以下のとおりである．

① 埋め込み情報を 72 ビットのブロックに分割するとともに，素材画像を 8×8 ピクセルの部分画像に分割する．
② 所定の規則に従って情報ブロックを部分画像に対応付ける．
③ 上記の DCT 係数変更により，各情報ブロックの 72 ビットを対応する部分画像に埋め込む．

情報の検出は，埋め込みの逆操作によって実行される．すなわち，JPEG 圧縮された画像を DCT 係数に変換し，その下位 2 ビットを取り出すことで埋め込み情報を検出している．

(4)　プラグイン・プログラム

本プロトタイプシステムは，ブラウザのプラグイン・プログラムとして開発した．なお，実際には，プラグイン・プログラムを以下に安全に配布するかも考慮する必要がある（たとえば，Object Signing 技術を使用するなど）が，ここでは，消費者がすでにプラグイン・プログラムをインストールしていることを前提としている．

(5)　インターネット・マークのデータフォーマット

上記電子透かし方式からも分かるように，インターネット・マークのデータフォーマットは JPEG フォーマットと同一である．ただし，ブラウザからプラグイン・プログラムへ処理を引き継ぐために，拡張子を独自のものに変更するとともに，インターネット・マーク用の MIME TYPE も定義している．

4.2　サイト認証を行うその他の方式との比較

Web サイトを認証するための方法としては，インターネット・マークのほかにも以下のようなやり方が考えられる．インターネット・マークとそれらの方式との定性的な比較を**表 1** に示す．

- マーク
  単純なマークを Web ページに貼付する．
- マークとハイパーリンク
  Web ページに貼付するマークに，そのマークの真正性を保証するオーソリティとのハイパーリンクを設定し，消費者が当該マークを指定（マウスでクリック）したときにオンラインで検証処理が行われるようにする．
- ディジタル署名
  コンテンツや URL，IP アドレスなどにディジタル署名を施したものを Web ページに貼付し，消費者が当該ディジタル署名の検証処理を行うようにする．
- マークとディジタル署名
  コンテンツや URL，IP アドレスなどにディジタ

表 1 他方式との比較
Table 1 Comparison with alternative methods.

	安全性			視認性	販売者の操作性	応答性(オフライン検証)
	不正貼付	マークや署名の改竄	Webページの改竄			
マーク	検出不可	検出不可	検出不可	あり	簡単	可
マーク & ハイパーリンク	検出可	検出不可	検出不可	あり	複雑	不可
ディジタル署名	検出可	検出可	検出可	なし	簡単	可
マーク & ディジタル署名	検出可	検出可	検出可	あり	複雑	可
インターネット・マーク	検出可	検知可	検知可	あり	簡単	可

ル署名を施したものをマークと関連付けて Web ページに貼付し，消費者が当該ディジタル署名の検証処理を行うようにする．

表 1 に示すように，単純なマークは安全性が欠落し「マークにオーソリティとのハイパーリンクを設定する方式は，サイトのアドレスやページの内容をオーソリティにオンラインで送信し，オーソリティ側でデータベースを検索して，発行審査時のサイトアドレスやページ内容と比較する必要があるので，オーソリティに負荷が集中することになり応答性が問題となる．さらに，1 つの Web ページ上に複数種類のマークがあり，それぞれ異なるオーソリティとのハイパーリンクを設定することが必要な場合，販売者にとって煩雑な設定操作が必要であった．これに対し，インターネット・マークでは，消費者が Web サイトを閲覧したときに，当該 Web サイトの認証に必要な情報を入手できるので，オフラインでの認証処理が可能であり，実際には数秒で検証結果を画面表示することができた．また，このようにオフラインで認証できることは，消費者が 1 日に何回も同じ販売店の Web ページを閲覧するような場合に，オンラインでの認証処理を省略することを可能とし，検証プロセスを行う時間や手間を省けることが分かった．加えて，インターネット・マークでは，販売店は通常の画像データと同じように Web ページ上にマークを貼付するだけの操作でよく，処理が簡単であり，手間もかからないことを確認した．

通常のディジタル署名を用いる方式は，視認性が欠落している．すなわち，通常のディジタル署名は単なるビット列なので，消費者は検証プロセスを実行しない限り，Web サイトに関して何ら情報を得ることができない．これに対し，インターネット・マークでは，マークのデザイン自体に意味があるので，消費者は検証プロセスを実行しなくても，どの機関がどの点について認定しているかなどといった情報を得ることができる．このことは，たとえば実際の電子商取引において，販売店の Web ページにクレジットカード会社のロゴのインターネット・マークが貼付されていた場合に，消費者は，商品を閲覧しているときには当該クレジットカードで決済可能であるらしいとの情報だけを認識し，最終的に商品を購入することに決めてクレジットカード番号などといった個人情報を入力する必要が生じたときにはじめて，検証プロセスを実行して認証処理を行うといったことを可能とする．これにより，消費者が特に被害をこうむる恐れのない場合などで検証プロセスを行う時間や手間を省けることが分かった．

マークとディジタル署名とを組み合わせる方式は，販売者にとって操作が煩雑である．すなわち，マークとディジタル署名の両方を Web ページに貼付するとともに，マークをクリックするとディジタル署名が検証されるなどといったように両者の間に何らかのリンクを設ける必要がある．1 つの Web ページ上に複数種類のマークがあり，それぞれ異なるディジタル署名を対応させる必要がある場合などでは，かなり複雑な設定操作が必要であった．これに対し，インターネット・マークでは，マークとディジタル署名が一体不可分であるため，マークとディジタル署名との対応付けを気にする必要がなく，販売者にとって操作の煩雑さが少ないことが判明した．

このように，インターネット・マークは安全性の面だけでなく，視認性（ユーザの利便性）や運用性の面でも他方式より優れているといえる．

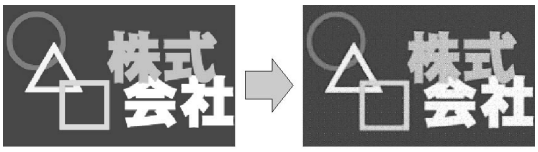
4.3 素材画像に埋め込むデータ量

電子透かしは，静止画や動画などといったディジタル・コンテンツの著作権保護の目的で利用されている

技術である．電子透かしでは，対象とするディジタル・コンテンツに微細な変更を加えて著作権情報などを透かし込む．このような著作権保護の対象となるディジタル・コンテンツは，それ自体が価値のある情報である場合がほとんどであるため，人間が判別できない程度の変更しか許されない．そのため，埋め込み情報のデータ量は限られたものであった．

これに対し，インターネット・マークでは，たとえば，素材画像の形状や輝度などが多少変わったとしても，当該画像が明示する情報，すなわち，消費者がインターネット・マークを見て判断するであろう情報さえ変わらなければ何ら問題とはならない．したがって，インターネット・マークは従来の電子透かしに比べて，小さな画像に大量のデータを透かし込むことが可能である．具体的には，通常の電子透かしでは，128×128ピクセルの静止画に数十〜数百ビットのデータしか透かし込むことができないのに対して，インターネット・マークでは2Kバイト程度のデータを透かし込むことができた．2Kバイト程度のデータを透かし込んだ場合の視認性の変化の例を**図7**に示す．

電子透かしの画質評価については，PSNR（Peak signal noise ratio）などを用いた客観評価法や，評点を用いた主観評価法，両者の組合せなどが提案されているが，いずれの方法も確立されてはいない．また，これらの画質評価方法は，美術画像に情報を埋め込む場合のような，画質を重視する場合を対象としているが，インターネット・マークでは，マークの識別が可能な範囲内では画質は重要でない．したがって，従来の電子透かしの画質評価方法をインターネット・マークの画質評価に適用することは難しい．一方，テレビやプリンタなどの画質評価については，評点を用いた主観評価法が確立されている．以上を考慮し，ここでは，テレビジョン学会での主観評価法[9]を修正して用いることにした．テレビジョン学会での主観評価法では，10人の画像処理技術者が各々5段階評価し，その平均点を最終的な評価値とするが，この点はそのまま踏襲した（評価者は無作為に選出した研究者で，画像処理技術の専門家ではない）．一方，評点の定義については，**表2**のように変更した．また，情報埋め込み後のマークが使用可能か否かを判定する基準を設け，3点以上を合格点とした．その結果，10人全員が3点以上と評価し，このことから視認性の面で何ら問題ないことを確認した．



埋め込み前　　埋め込み後

図7　電子透かしによる画質変化の例
Fig. 7　An example of Internet-Mark visibility.

5. おわりに

本稿では，マークが貼付されたWebページを閲覧する消費者が，当該Webページに当該マークが貼付されているという事実が真正なものであるかどうか，当該Webページの内容が真正なものであるかどうか，当該マークが明示する情報が信用するに足るものであるかどうか，を確認するための手段であるインターネット・マークを提案した．インターネット・マークでは，Webページを構成するコンテンツや，そのWebページを公開するURL，IPアドレスなどといった複数の情報に対して，ディジタル署名を施し，その結果をマークに透かし込む．ブラウザを使ってWebページを閲覧する消費者は，当該Webページに貼付されたインターネット・マークに透かし込まれている埋め込み情報を抽出し，現在閲覧しているWebページのコンテンツ，URL，IPアドレスなどと比較・検証することで，不正の有無を確認することができる．

実際にプロトタイプシステムを開発して評価を行ったところ，4章で示したように，安全性だけでなく，運用性や利便性も含めて有用な方式であることを確認

表2　主観評価法
Table 2　Subjective evaluation method for Internet-Marks.

評点	[テレビジョン学会]の定義	インターネット・マークでの定義
5	画質劣化が分からない	画質の劣化が認められない
4	画質劣化が分かるが気にならない	画質の劣化は認められるが，気にはならない
3	画質劣化が分かるが少し気になる	画質の劣化が気になるが，マークを識別する上では妨害にならない
2	画質劣化が分かり気になる	画質の劣化が気になり，マークを識別する上で妨害になる
1	画質劣化が分かり大変気になる	画質の劣化が気になり，マークの識別が困難である

した．

インターネット・マークは，有害コンテンツのフィルタリングや類似サイトの検索手段などとしても利用できると考えており，今後さらなる検討を進めていく予定である．

謝辞 本研究は，郵政省殿ならびに通信・放送機構殿からの委託研究として行っているものであり，関係者の方々に深謝いたします．また，本研究に関し，有益なご意見をいただいた（株）日立製作所の宝木和夫氏，本城信輔氏，斎藤司氏に心より感謝いたします．

参 考 文 献

1) 郵政省（編）：平成 11 年版通信白書，p.30 (1999).
2) 松井茂記，高橋和之（編）：インターネットと法，有斐閣 (1999).
3) 木村忠正，土屋大洋：ネットワーク時代の合意形成，NTT 出版 (1998).
4) 日本経済新聞：ネット上の個人情報保護・米で指針，日欧統一も，平成 10 年 12 月 18 日 (1998).
5) 白井 均，三浦 修，谷川正治，赤津 茂，森谷文彦（著），磯部朝彦（監修），日立総合計画研究所（編）：日本版デジタル革命，東洋経済新報社 (1998).
6) Yoshiura, H., Sasaki, R. and Takaragi, K.: Secure Fingerprinting Using Public-Key Cryptography, *Proc. 1998 Cambridge International Workshop on Security Protocols* (1999).
7) Susaki, S., Yoshiura, H., Nagai, Y., Toyoshima, H., Sasaki, R. and Tezuka, S.: Internet-Marks: Reliable Visual Marks for the Web Site Authentication, *Proc. 1999 International Conference on Computer Communication*, T-17-03 (1999).
8) Swanson, M., Kobayashi, M. and Tewfik, A.: Multimedia Data-Embedding and Watermarking Technologies, *Proc. the IEEE*, Vol.86, No.6, pp.1064–1087 (1998).
9) 宮川 洋（監修），テレビジョン学会（編）：テレビジョン画像の主観評価とデータ処理，コロナ社 (1986).

(平成 11 年 12 月 9 日受付)
(平成 12 年 6 月 1 日採録)

洲崎 誠一（正会員）

1991 年横浜国立大学電子情報工学科卒業．同年（株）日立製作所システム開発研究所に入所．以来，情報セキュリティ技術の研究開発に従事．現在，同研究所セキュリティシステム研究センタ研究員．1996 年情報処理学会第 52 回全国大会優秀賞受賞．

吉浦 裕（正会員）

1981 年東京大学理学部情報科学科卒業．同年（株）日立製作所入社．日立研究所を経て，現在，システム開発研究所セキュリティシステム研究センタ勤務．自然言語処理，知識処理，情報セキュリティ，著作権保護の研究開発に従事．理学博士（東京大学）．電子情報通信学会，人工知能学会各会員．1990 年情報処理学会学術奨励賞受賞．

永井 康彦（正会員）

1983 年日本大学理工学部航空宇宙工学科卒業．1985 年同大学院理工学研究科修士課程修了．同年（株）日立製作所入社．システム開発研究所横浜ラボラトリ勤務．情報セキュリテイ，ネットワーク管理システム，グループウエア等の研究開発に従事．現在同研究所セキュリティシステム研究センタ主任研究員．電気学会，電子情報通信学会，日本航空宇宙学会各会員．

豊島 久

1977 年千葉大学卒業．同年（株）日立製作所入社．現在，公共システム事業部インターネットマークス事業推進センタ長．公共分野のシステム構築に従事し，「インターネット・マーク」の研究開発およびその後の事業化・普及活動を推進．著書に，「グローバル競争に勝つ地域経営」（共著，東洋経済新報社，1998 年）．

佐々木良一（正会員）

1971年東京大学医学部保健学科卒業．同年（株）日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．現在同研究所主管研究長兼セキュリティシステム研究センタ長．工学博士（東京大学）．1983年電気学会論文賞受賞．1998年電気学会著作賞受賞．著書に「インターネットセキュリティ—基礎と対策技術」（共著，オーム社，1996年),「インターネットセキュリティ入門」（岩波新書，1999年）等．IEEE，電子情報通信学会，電気学会各会員．

手塚　悟（正会員）

1984年慶応義塾大学工学部数理工学科卒業．同年（株）日立製作所マイクロエレクトロニクス機器開発研究所を経て，現在，システム開発研究所セキュリティシステム研究センタ勤務．パーソナルコンピュータのオペレーティング・システム，デバイス・ドライバ，LANシステム，セキュリティシステムの研究開発に従事．