電子透かしによるレーティングサービスとセキュリティ対策

5G−5

澤田 修司　柴多 直樹　宮内 宏
NEC　C&Cメディア研究所

1.はじめに

近年，インターネットにおけるコンテンツのフィルタリング（チャイルドガードなど）の実現をめざして研究開発が行なわれている．例えば，W3C では PICS[1]を制定している．従来のレーティングサービスでは，画像を URL で識別していたため，画像ファイルをそのまま置換できるという問題があった．これに対し，画像ファイルに電子署名を行なうことが考えられるが，画像の改変（圧縮・拡大・縮小・フォーマット変換）には対応できない．また URL を変更すると PICS ラベルと対応しないという問題がある．

筆者らは電子透かしを応用してラベルと画像との対応関係の改竄を防止する方式を提案した[2]．本論文では，電子透かしとセキュリティ的技術とを組み合わせた手法による，改竄が困難なレーティング情報の提供サービスの実現について述べる．

なお，本論文では前提条件として，レーティングサービスのための表示制限機能付きブラウザの存在を仮定する．

2.レーティングサービスのセキュリティ

本章では電子透かしの応用として広く議論されている権利保護との比較をふまえつつ，レーティングサービスのセキュリティレベルを論じる．

電子透かしのアプリケーションを設計する場合，セキュリティ上の脅威としては，以下の4種類が考えられる．

透かし除去　信号処理レベルで透かし入り画像から透かしを除去する．

透かし置換・多重埋め込み　透かし入り画像から透かしを除去し，異なる透かしを埋め込む．または透かしを多重に埋め込む．

サーバ不正　電子透かしを登録するサーバなどが利用者に対して不正を行なう．

結託攻撃　複数の関係者（サーバ・利用者など）が結託して攻撃する．

ここではアプリケーションの例として権利保護とレーティングサービスをとりあげ，対策を考える．

透かし除去防止に関しては，権利保護と比較すると，レーティングサービスでは対策の必要性は低い．これは，レーティング情報が得られない場合に表示をブロックするという処理で充分であるからである．

透かし置換・多重埋め込み防止に関しては，権利保護と同様にレーティングサービスでも，原画像に対する電子署名を透かしとして埋め込むことで対処する．

サーバ不正防止に関しては，権利保護と異なりレーティングサービスでは，サーバが透かし入り画像を複数の利用者に配布することを防止する必要はない．ただし，サーバがレーティング情報を回答するときの不正を防止する必要がある．

結託攻撃防止に関しては，権利保護と異なりレーティングサービスでは，同一画像に複数の透かしが発行されることはないので，透かしの差分を利用する改竄には対策を必要としない．ただし，レーティング情報作成者と結託して改竄するような攻撃に対しては，レーティング情報作成者の電子署名により改竄を抑止する．

以上より，レーティングサービスのセキュリティ対策として，電子署名による透かし置換・多重埋め込み・結託攻撃防止対策と，サーバの不正回答防止対策とが必要であると考えられる．

3.レーティングサービスの設計

本章では，2章で示したセキュリティ機能を実現する具体的方式として，図 1のシステムを提案する．

A Rating Service Utilizing Digital Watermark Technology and Security
Shuji Sawada, Naoki Shibata, Hiroshi Miyauchi
NEC C&C Media Research Laboratories

3.1.設計方針

まず，電子署名と透かしの複合方式について説明する．電子署名は，原画像に対して行なうと画像を改変（圧縮・拡大・縮小）したときに署名検証できない．そこで，画像に対して DCT 変換を行なった結果の低周波部分の係数を用いて，画像を改変しても変化しない画像の固有情報を生成する[3]．この固有情報とレーティング情報に対して署名を行ない，署名を透かしとして原画像に埋め込むことにより，透かしと透かし入り画像との対応関係を改竄不可とし，透かし置換を防止する．また透かしに不正なレーティング情報を対応させることも防止する．

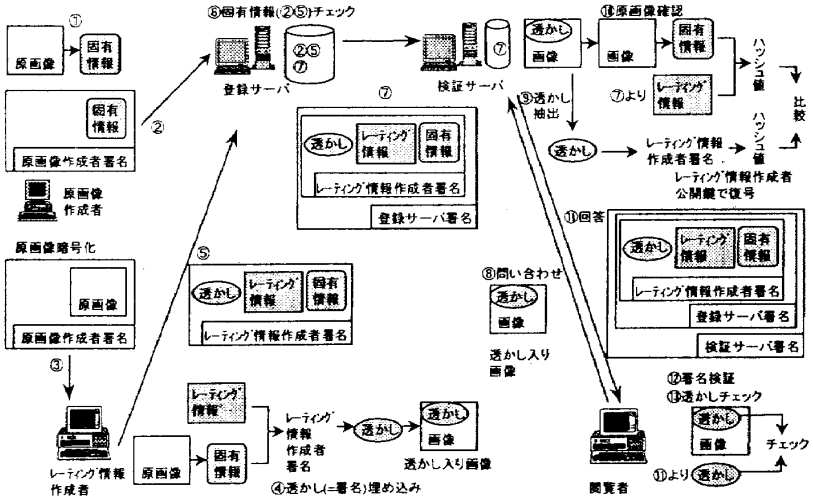

図 1 レーティングサービス構成図

透かしの検証では，透かし抽出・固有情報生成・レーティング情報検索を行ない，透かしを署名検証する．この検証により，透かしが正しい原画像に埋め込まれていること，透かしがレーティング情報と正しい対応関係にあること，レーティング情報作成者と結託して不正な固有情報が生成されていないこと，などを確認する．

サーバの不正回答防止対策は，閲覧者の透かしチェック・複数検証サーバ構成により行なう．

3.2.処理手順

上記の方針に基づいて以下の処理手順(図 1の手順①～⑬)を提案する．各処理手順のうち，安全性に関する部分のみを説明する．

原画像作成者は原画像の流出先を少なくするため，登録・検証サーバには原画像を送信しない(②)．レーティング情報作成者は，データベースに登録する透かし・レーティング情報・固有情報に対して署名を行ない，改竄を防止する．複数のレーティング情報作成者が付与したレーティング情報を比較する構成とすると，より安全性が高い(⑤)．登録サーバは，受信した固有情報が一致することをチェックする(⑥)．原画像が復元される可能性を避けるため，閲覧者は透かし抽出を行なわずに検証サーバに問い合わせる(⑧)．

検証サーバを複数構成として回答を比較すれば，透かし入り画像と対応しないレーティング情報を検証サーバが回答すること，レーティング情報がないと回答すること，または回答を送信しないこと，などのサーバ不正を防止できる(⑩⑪)．

閲覧者は，透かし入り画像と対応しないレーティング情報を検証サーバが回答していないことを透かしチェック処理で確認し，サーバ不正を防止する．検証サーバが無応答の場合は画像を表示しない(⑫⑬)．

以上の手順で閲覧者の透かしチェック・複数サーバ構成によりサーバ不正を防止できる．

4.まとめ

電子透かしの応用による，安全なレーティングサービスの実現について述べた．今後は，PICS に基づいた実現方式について検討する．なお，本研究は郵政省のプロジェクト「電子透かし技術に関する研究開発」の一環として通信・放送機構（ＴＡＯ）から委託されて日本電気株式会社が実施した．

参考文献

[1]Jim Miller, et. al., Rating Services and Rating Systems (and Their Machine Readable Descriptions), W3C Recommendation, 1996

[2]柴多，澤田，「電子透かしを用いて改竄を防ぐレーティングサービスシステムについての考察」，信学技報 ISEC97-75

[3]亀屋，田中，「画像情報のデジタル署名の一実現法」，SCIS93-13A