コンピュータセキュリティ　10－4
（2000．　7．25）

インターネット上におけるプライバシーマークの認証方法について

ウェブブラウザに表示された画像データの認証方法について

北野博之、関本貢
財団法人日本情報処理開発協会 情報セキュリティ対策室
〒105-0011 東京都港区芝公園 3-5-8
Tel: 03-3432-9387 / FAX: 03-3432-9419 / E-mail: info@privacymark.gr.jp

あらまし　最近ではウェブサイトでいろいろな認定マークやロゴを見かけるようになってきた。プライバシーマーク制度のように、事業者認定サービスではマークの不正コピーなどによるなりすましは一般消費者にとって不利益なことになりかねない。バイナリデータである画像データは通常のテキストの認証方法とは異なり、現時点ではコンテンツ認証のメカニズムがない。そこで、事業者認定マークであるプラバシーマーク画像データの認証方法について試作の紹介と共に汎用的な検証方法を提案する。

キーワード　マーク認証、なりすまし、電子署名、公開鍵証明書

Authentication system of PrivacyMark on the Internet

Methods of authenticating the graphic date on the Internet

Hiroyuki Kitano and Mitsugu Sekimoto
Information Security Office, Japan Information Processing Development Center
Shiba-koen 3-5-8, Minato-ku, Tokyo 105-0011, JAPAN
Voice: +81-3-3432-9387 / Facsimile: +81-3-3432-9419 / E-mail: info@privacymark.gr.jp

Abstract

Recently, so many seals and logos appear in the Internet. For consumers, certification service providers like PrivacyMark award system, must afraid that someone can easily pretend as certified by copying seals and logos. There is no system to verify binary contents like graphic data, so a general scheme of verifying seals and logos is expected.

key words　Authenticaion of seal, Pretending, Digital Signature, and public-key infrastructure

1. まえがき

当協会では、情報化環境の中において、企業が行う一般消費者の個人情報取扱いについて、「個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q 15001）」[1]に準拠した取り組みを促進するために、事業者を認定する プライバシーマーク制度[2]を平成 10 年4月より運営している。認定を受けた事業者はパンフレットやウェブページ等でプライバシーマークを使用し、自社の個人情報の取扱が JIS Q 15001 に準拠していることを消費者にアピールすることができる。

しかし、プライバシーマークをインターネット上で、事業者のホームページに表示している場合、電子データであるが故にそれを簡単にコピーすることができる。その結果、不正を意図した事業者がプライバシーマークをホームページに表示して、あたかもプライバシーマークの付与認定を受けている事業者としてなりすますことが容易に可能となる。このような不正利用は、プライバシーマークを信頼している消費者をだますことになり、ひいては消費者から不当に個人情報を収集することにもなりかねないため、プライバシーマーク制度の健全な運用上にも、こうした不正行為を防止するための技術的解決が不可欠である。

現状では、汎用的な認定マーク認証検証の仕組みがないばかりに、ハイパーリンクで認定サービス者側の事業者一覧や詳細ページに飛ばせたり、CGI や JAVA Applet 等のプログラムを使って、動的にページを検証するなどの方法を行っているようである。このような通常の HTML 記述を利用した方法では簡単になりすましが行える可能性がある。

今後プライバシーマークのように、認定情報としてウェブページ上に“認定マーク”を貼る認定サービスが増えてくると思われ、同様の問題とその解決法を求められてくると思われる。特定の認定サービスに特化したシステムやアプリケーションを作成すると検証用のシステムやアプリケーションが混在することになり、ユーザの使い勝手が悪くなる。よって特定の認定サービスに限定しないオンラインでの認定マークの検証システムについての試行と考察を行う。

2. なりすまし対策

インターネット上で“認定マーク”を表示する際のなりすましの脅威について整理する。

(1) 不正事業者のなりすまし

認定を受けていない事業者がマークをコピーして使用し、あたかも正当に認定を受けているかのように見せる。

(2) 正当事業者のなりすまし

正当に認定を受けた事業者が認定範囲や認定期間を越えて利用する。

(3) 不正検証サーバのなりすまし

(1) の不正事業者自身、または第三者が検証サーバを構築し、あたかも正当に検証を行ったかのように振る舞わせる。

なりすましを防ぐには、現時点では以下の対策が考えられる。

(1) 画像データへの工夫

画像データ自体に認定番号等の識別番号を盛り込み、視覚的にもある程度の認定情報を表示する。さらに画像データに電子透かし等の技術を施して、オリジナリティと配布先をマーキングできるようにする。

(2) サーバの HTML 記述に依存しない検証方法

検証に必要な検証サーバの URI を改変できないように、専用のプラブインや別アプリケーションを用意する。

(3) 他の認証メカニズムの利用

現在 SSL や TLS 等を始め、さまざまな分野

で普及が広まっている公開鍵証明書の機構を利用する。マークの画像と公開鍵証明書をバインドさせ、検証システムとしては CA(認証局)を利用した公開鍵証明書の検証機構を利用する。

などの方法が考えられる。

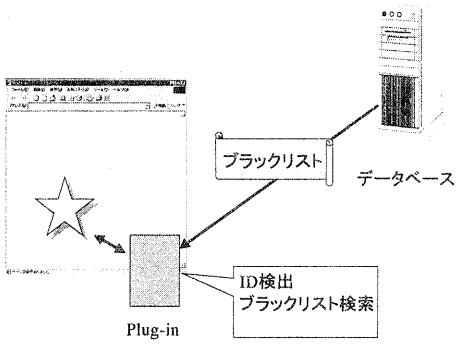

図 1 クライアントでの検証

3. システムのデザイン

3.1 検証メカニズム

なりすましの脅威に対し、以下のような手順に分割して検証を行うようにする。

手順1 マークに盛り込まれている情報の取得
手順2 マークの発行者の確認
手順3 マークが表示されているページ URI の確認
手順4 事業者の失効情報などの確認

3.1 マークに盛り込まれている情報の取得

認定マークを認定事業者それぞれ個別に発行し、予めユニークな情報を画像データの中に刷り込んでおく。現時点では、電子透かしを用いた方法が考えら得る。しかし、電子透かしでは

・盛り込める文字列が少ない

・単純な色彩のマークを劣化させる

・オープンソースではない

などの諸問題がある。

公開鍵と署名によるコンテンツ認証を行うには、利用する画像データのデータフォーマットなどの変更が必要となる。

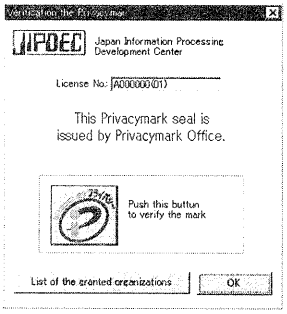

図 2 電子透かしを利用した検証プラグインの例

3.2 マーク発行者の確認と URI の確認

ブラウザに表示された画面にある認定マークを検証する上で操作性の面や、ブラウザの「場所(Location)カラム」に表示された URI との比較の点から、実装するアプリケーションはプラグインという形が望ましい。

プラグインプログラムはユーザが意識的にインストールしなければ利用することはできないが、汎用的なマーク認証機構ができれば、ブラウザにも標準で実装されるようになると思われる

3.3 事業者の失効情報などの確認

時系列的に認定マーク発行後のイベントであるため、失効情報を認定マーク自身に盛り込むことができない。したがって、必然的に検証サーバへ問い合わせる方法を取らざるを得なくなる。

4. 分散データベース

画像データに情報を持たせ、これを検証するということは、一種のサーバ-クライアント分散型の

データベースとして考えることができる。サーバとクライアントで、図3の

(8) 検証先CGIなどURI
(9) 有効・無効情報

が異なる情報である。

このように、検証先 URI を認定マークに刷り込むことにより、複数の認定サービスや階層的な分散管理も行えるようになる。

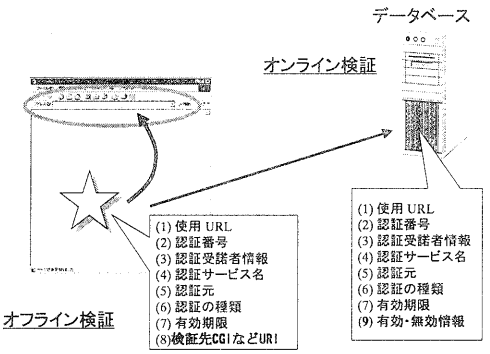

図3 サーバ-クライアント分散データベース

5. 考察

バイナリデータを通常のテキストコンテンツの認証と異なることを踏まえて、検証方法を検討した。PKI(公開鍵機構)を用いた汎用的な検証メカニズムは、電子透かし技術を用いたものと同様に著作権問題の解決にも役立つと思われる。

W3C(World Wide Web Consortium) [3] では XML コンテンツに対して署名を行うフォーマットである XMLSignature[4]を提案している。また、W3C ではテキスト表記のグラフィック言語 SVG (Scalable Vector Graphics)[5]をも提唱しており、今後普及していくものと思われるので、マーク認証のスキームも XMLSignature とも親和性の高いシステムが望まれるであろう。

例えば、GIF や PNG フォーマットでもテキストエリアと呼ばれるコメントを注入できるフィールドがあり、その部分に画像データ部分等の署名データと公開鍵証明書を盛り込むことが可能である。

6. むすび

本提案に対し、様々なご意見を述べていただいた W3C の LaLiberte 氏と小池氏に感謝する。

本研究の一部は、情報処理振興事業協会の平成10 年度第一次補正事業「先進的情報システム開発実証事業」、財団法人データベース振興センターの平成 11 年度「データベース構築及び技術開発促進事業」によるものである。

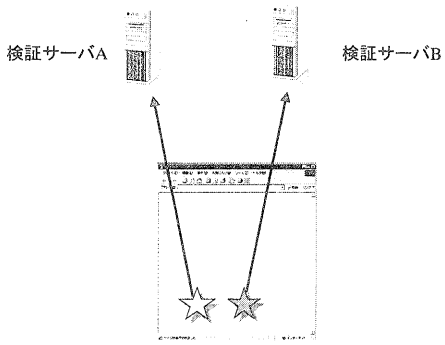

図 4 複数検証サーバの検証

参考資料

[1] http://www.jipdec.or.jp/security/privacy/JIS-kokuchi.htm
[2] http://www.jipdec.or.jp/security/privacy/
[3] http://www.w3.org/
[4] http://www.w3.org/Signature/
[5] http://www.w3.org/Graphics/SVG/