モデレータによる Web コンテンツの不整合解消について

宋　光顯† 　申　吉浩† 　久保山 哲二‡ 　田口 哲典† 　青木 輝勝† 　安田　浩†

†東京大学　先端科学技術研究センター　〒153-8904　東京都目黒区駒場 4-6-1
‡東京大学　国際産学共同研究センター　〒153-8904　東京都目黒区駒場 4-6-1

E-mail: †{song, kshin, taguchi, aoki, yasuda }@mpeg.rcast.u-tokyo.ac.jp, ‡kuboyama@ccr.u-tokyo.ac.jp

あらまし　インターネットは現代社会において不可欠の道具となっており、電子商取引などでは、インターネットで閲覧される Web ページの内容の真贋が経済的・社会的な影響をもつ。その一方で、インターネット上を流れるデータは原理的に窃取・改ざんの脅威を免れ得ない。このように、インターネットを社会制度の一部として今後一層活用するためには、作成者と閲覧者との間における Web ページの不整合は解決が避けられない問題である。本稿では、Web ページの不整合問題を解決するモデレーションモデルを提案する。このモデルはある共通のポリシーを有する認証局の下でお互いに協力する一つ以上のモデレータで構成されている。Web ページの不整合から自らを保護したいユーザ（作成者・閲覧者）は、モデレータを任意に選択し、Web ページの送信･受信をモデレータ経由で行う。モデレータは、自らを経由して送信･受信される Web ページのハッシュを後に検索可能な形式で記録するとともに、モデレータ同士で自律的な監査を行いコミュニティとしての健全性の保全を図る。

キーワード　不整合, 真正性

1. はじめに

インターネットは現代社会において不可欠の道具となっており、電子商取引などでは、インターネットで閲覧される Web ページの内容の真贋が経済的・社会的な影響をもつ。その一方で、インターネット上を流れるデータは原理的に窃取・改ざんの脅威を免れ得ない。

このように、作成者と閲覧者との間における Web ページの不整合は、閲覧者が受けたと主張するものと作成者が送ったと主張するものと一致しない状況として定義される。極端な場合では、作成者は Web ページの存在さえ否定するかもしれないし､その逆もありえる。作成者や閲覧者は、商品の発送や代金の支払い等の重要な社会的行為を、Web ページの内容に基づいて行う可能性があるので、不整合の解決は、インターネットを社会的なシステムの一部として利用するために解決が避けて通れない問題である。

本稿では、Web ページの不整合を調停し、少なくとも、紛争を和らげるのに有用な情報を提供することによって問題を解決に導くために有用な情報を Web ページの送受信において生成し、記録するフレームワークのメカニズムについて説明する。本稿で述べるフレームワークは、法的な強制力を担保するような証拠能力を提供することはできないが､ユーザが Web ページに関する「いいがかり」から自分自身保護する方法を提供することができる。さらに、本稿で述べるメカニズムは、自律的な監査機能を具備しており、第三者の監査機関を仮定しないことにより、導入のための社会的な障害を予め排除する。

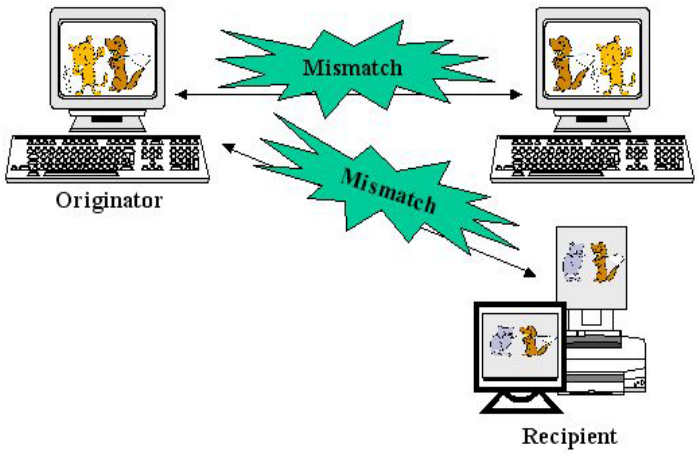

図 1　Web ページの不整合

2. 真正性

Web ページのセキュリティを考えるうえで、その真正性(authenticity)は、長年にわたる主要な関心事である。閲覧者が受信した Web ページが真正であるとは、Web ページの内容が、まさに作成者が見せようと意図した内容であるということである。Web ページの真正性を達成するための手法としては、既にいくつかの方法が知られている。

まず、Web ページに署名する方法について述べる。電子署名は PKI(Public Key Infrastructure)の主要な機能の 1 つである。Web ページの作成者は秘密鍵を使って Web ページに電子署名をする。Web ページを受け取る際、閲覧者は作成者の秘密鍵と対になっている公開鍵を使用することで電子署名を確かめる。PKI の規定により、公開鍵は信頼されている認証局(CA)が発行する

証明書に記されたデジタルデータとして閲覧者に提供される。Web ページに署名するこの方法は反復攻撃（replay attack）に対して脆弱であることが知られている。すなわち、攻撃者は、作成者が署名した Web ページを記録しておき、同じ作成者によって提出された新しい Web ページを、攻撃者が記録しておいた Web ページで置き換える。取り替えられた Web ページにある電子署名も、本物であるため、閲覧者は改ざんを検出することができない。作成者は Web ページを求める要求を受け取る際にタイムスタンプと共に Web ページに署名するように Web サーバを設定すれば、この脆弱性を回避することができる。しかし、Web サーバが、Web ページが閲覧されるたびに、電子署名を逐一付与するためのオーバーヘッドは、PKI の計算量の問題から非常に大きく、その性能に深刻な害を及ぼすことになる。

もう 1 つの方法は、エンティティ認証と完全性検証を支援する安全な通信プロトコルである SSL/TLS [6] の利用である。この手法は、脆弱性を回避しつつ、同時に、PKI 計算によって引き起こされるオーバーヘッドを実際に許容しているレベルにまで引き下げることができる。SSL/TLS では、Web ページに対する MAC(massage authentication code)は、現行セッションの始めに交換される秘密鍵を使用して生成、検証される。この鍵は、現行セッションの短い期間だけ有効なため、反復攻撃は使えない。さらに、PKI 計算はそれぞれのセッションの始めに一度だけ行なわれる。したがって、引き起こされるオーバーヘッドは限られている。しかしながら、SSL/TLS は、証拠能力を提供するいかなる情報も保持していない。電子署名と異なり、MAC を生成する鍵は、互いに通信するエンティティ間で共有される。したがって、作成者だけではなく、Web ページの閲覧者も任意の Web ページに対して MAC を生成することができる。

閲覧者が、意図した作成者によって署名されるか MAC が付与された Web ページを検証できる点において、署名による手法と SSL/TLS の利用により真正性問題は解決される。

しかし、別の脅威が生じる。攻撃者は、作成者の Web サーバに侵入し、サーバ内の Web ページを変更、もしくは置き換える可能性がある。作成者の Web サーバでは、変更された Web ページに対しても、自動的に MAC 生成するか署名するために、閲覧者は、それらが偽物であると検証することはできない。

この問題に対する解決手法として、Dynamic Security Surveillance Agent(DSSA) ([1])が提案されている。DSSA では、作成者があらかじめ発信するすべての Web ページのハッシュ値を計算し、Web サーバから独立した他のサーバにそのハッシュ値を格納する。また、作成者は以下のような作業ができるようにシステムを設定しておく。Web サーバは Web ページの要求を受け取る際はいつも要求された Web ページのハッシュ値を計算し、Web サーバと独立したサーバに格納されているそのページのハッシュ値と比較する。サーバがそれらの間の不整合を探知した場合、閲覧要求を拒否し、警告メールを作成者に送る。ハッシュ値を生成するために、DSSA は SHA-1 のように安全なハッシュ関数を利用する。DSSA は Web サーバが要求を受け取る各瞬間にハッシュ値を計算するが、計算から引き起こされるオーバーヘッドは、SHA-1 は RSA 署名生成より 1000 倍速く、RSA 署名検証より 100 倍速いために、大きな問題にはならない。

DDSA はクライアントサイド検証の機能を含んでいないので、SSL/TLS あるいは通信外クライアントサイド検証方法によって補完されるのが望ましい。

要約すれば以下の要件の両方が満足される場合のみ、Web ページの真正性は保証される。

- 閲覧者は、受け取った Web ページが、自分の要求に応じて意図した作成者から送られてきたものであることを検証することができること。特に、閲覧者は Web ページがインターネットを介して送信されている間に改ざんされないことを検証できること。
- 作成者は送信しようとしている Web ページを、際に閲覧者に確実に送ることができること。

DDSA は、署名による手法か、SSL/TLS 利用のいずれかの組み合わせにより前述の要件を満たす。さらに、署名による手法は、その他の重要な機能である作成者認証(メッセージ認証)と否認拒否と呼ばれる機能の要件を満たす。Web ページに付けられている電子署名を検証することによって、閲覧者は作成者を認証することができる。そして、検証がいったん成功すると、作成者がその Web ページに署名したという事実を支持する証拠として電子署名は使用できる。

3. 不整合解消

不整合解消では Web ページの不整合から作成者と閲覧者の間で引き起こされる紛争をどう調停するか、または少なくとも、どう軽減するかに焦点を当てる。その点において、不整合の発生を防ぐことを注視する真正性とは異なっている。つまり、真正性を維持する技術は防止技術に分類されるのに対して、不整合解消のための技術は after-the-fact 技術に分類されるものである。

したがって、不整合解決のためには、Web ページの作成者と閲覧者の間で通信が行われる際に、証拠能力のある情報を、何らかの形で生成することが必須とな

る。

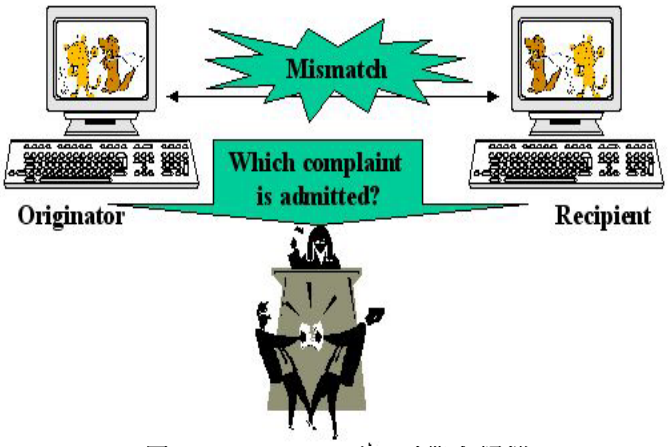

図 2　Web ページの不整合解消

前節で述べた手法の中では、電子署名による手法だけがこの要求を満たしている。しかしながら、これは不整合の問題を一部しか解決していない（表 1）。

表 1　電子署名技術による解決法の限界

項目 / 主張者	Web ページの存在証明	Web ページの非存在証明
善意の作成者	不可※1	不可※2
善意の閲覧者	可(署名時) ※3 不可（非署名時）※4	不可※5

※1　作成者が提示するウェブページに対して、作成者がウェブページの存在を証明する。作成者は、任意の時点で随意にページに電子署名を付すことができるので、電子署名を提示しただけでは証明とはならない。

※2　閲覧者が提示するウェブページに対して、作成者がウェブページが存在しなかったことを証明する。このケースでは、電子署名は付されないが、作成者は、故意に署名を付さなかったという非難を否定できない。

※3　閲覧者が提示するウェブページに対して、閲覧者がウェブページの存在を証明する。電子署名の否認拒否性により、作成者が作成の事実を拒否できない。

※4　署名が付されていなかったり、不正なアプリケーションにより虚偽の検証が行われた場合、閲覧者はウェブページの存在を証明できない。

※5　作成者が提示するウェブページに対して、閲覧者がウェブページが存在しなかったことを証明する。作成者は、随意に署名をつけられるので、閲覧者は非存在を証明できない。

したがって、電子署名による手法は、不整合解消問題を解決するための十分な機能を提供してないことがわかる。

不整合解消問題を解決する技術は、表 1 の 5 つの領域に提示されている全ての実効的機能を備えている必要がある。電子署名による手法は、Web ページの真正性の保証には、原理的に有効であるが、不整合解消問題の解決に用いるには不十分である。

4. モデレーションモデル

本稿では Web ページの不整合により生じる紛争を調停、もしくは、少なくとも紛争を軽減するモデルを提案する。このモデルをモデレーションモデルと呼ぶ。

本モデレーションモデルでは、Web ページの不整合を解消する機能は、モデレータと呼ばれる複数のエンティティのネットワークによって提供される。

モデレータは、インターネット上に存在するエンティティであり、以下の機能を提供する。

- 作成者、閲覧者を問わず、Web ページに関する悪意がある主張から自分を守りたいユーザは、少なくとも 1 つのモデレータを選ぶ。そして、Web ページに関するすべての要求と応答が、選択したモデレータを介して伝えられるように、自分の Web ブラウザや Web サーバを設定する。
- モデレータは自分を通って通信されるすべての Web ページのハッシュ値を計算し、署名を付ける。その他の補足的な情報（たとえば、URL、現在の時間、http メッセージのハッシュ値）も、Web ページとともにハッシュ値が計算され、署名が付けられる。この署名付きのハッシュ値は、必要に応じてすぐに検索できるような形で格納される。モデレータの実装には、署名付きハッシュ値を格納するためのデータベースも含まれる。
- 自分以外のモデレータ、または、その他の認証されたエンティティによって、署名付きハッシュ値の要求があった場合には、要求された署名付きハッシュ値を検索し提示する。提示された署名付きハッシュ値は、Web ページの不整合から引き起こされる紛争の調停や、モデレータの監査に用いられる。

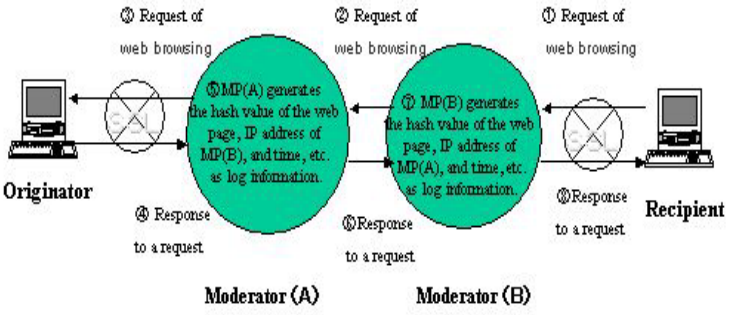

図 3　モデレータのフロー

したがって、閲覧者が受信し、作成者が発信するすべての Web ページの記録は、ユーザが選択したモデレータによって生成される。

モデレータによって署名された記録は、閲覧者が受

信したか、または作成者が特定の Web ページを発信したという事実を示す証拠として使用される。

モデレータによって生成された記録（署名付きハッシュ値）には証拠能力が必要である。実際、記録にはモデレータによって署名が付けられる。これは、モデレータが適切な認証ポリシーを持つ認証局(CA)によって発行された 1 つ以上の証明書を保有することを意味する。

不整合が発生した場合の調停では、まず、閲覧者のモデレータが生成したレコードと作成者のモデレータが生成したレコードとを、Web ページのハッシュ値、IP アドレス、タイムスタンプをキーとして、照合し、表 2 に従って調停する。

閲覧者のモデレータが生成したレコードが存在した場合、閲覧者の側の存在証明が認定され、作成者のモデレータが生成したレコードが存在した場合、作成者の側の非存在証明が認定される。

表 2　不整合が発生したときの調停表

閲覧者のモデレータ / 作成者のモデレータ	レコード有	レコード無
レコード有	信頼性がより高いモデレータのレコードの主張を優先する（但し、MP同士はＳＳＬで通信するので、このケースが発生する可能性は極めて少ない）	閲覧者の存在証明はないので、作成者の非存在証明が優先される。
レコード無	作成者の非存在証明はないので、閲覧者の存在証明が優先される。	N/A

5. モデレーションモデルの要件

この節では、モデレーションモデルが、機能性、導入の容易さ、および証拠能力について、満たすべき要件を示す。

5.1. 機能性

モデレーションモデルは、主張者が、作成者であるか閲覧者であるかの如何にかかわらず、もしくは、主張項目が、Web ページの存在証明であるか非存在証明であるかの如何にかかわらず、問題となっている Web ページの不整合を解消することを狙いとしている（表 3)。

表 3　モデレーションモデルの対象

主張者 / 項目	Web ページの存在証明	Web ページの非存在証明
善意の作成者	可	可
善意の閲覧者	可	可

5.2. 導入の容易さ

不整合解消問題は、できるだけ早く解決すべき緊急の課題である。 よって、我々は、モデレーションモデルにおいては、導入の容易さが、きわめて重要な問題であると考える。

特にモデレーションモデルが直ちに実施可能であるという基本的な要件を満足するために、以下の前提条件を置く。

- 閲覧者が公開鍵証明書を取得することを仮定しない。
- 新規のブラウザソフトを仮定しない。
- 閲覧者がダウンロードするヘルパーアプリケーション、アドイン、プラグインを信頼しない。

5.3. 証拠能力

我々は、十分に強力な証拠能力をもったモデルを提供することよりも、容易に導入できるモデルを提供することが、はるかに重要であると考える。実際に法的な強制力を持った証拠能力の提供をモデルに担わせることは現実的ではない。

6. まとめ

本稿では、作成者と閲覧者との間における Web ページの不整合問題に関して、直ちに実施可能なモデレーションモデルを提案した。今後は、モデレータ間のプロトコル設計を含むモデルの精緻化を行う。

文　献

[1] Soroush Sedaghat, Josef Pieprzyk, Ehsan Vossough: “ON-THE-FLY WEB CONTENT INTEGRITY CHECK BOOSTS USERS’CONFIDENCE”, Communications of the ACM November 2002/Vol. 45, No. 11, page33-37

[2] Rivest, R. and Shamir, A.: “PayWord and MicroMint—Two Simple Micropayment schemes” .In Proceedings of 1966 International Workshop on Securiy Protocols, pages 69-87, Springer, 1997. Lecture Notes in Computer Science No.1189

[3] Electronic commerce promotion conference: “Guideline concerning e-signature document long preservation”, Mar, 2002

[4] Fumikazu Taniguchi: “About PKI and the electronic certification in the financial industry”, Bank of Japan financial laboratory, Apr, 2000

[5] M. Waldman et al., A robust, tamper-evident, censorship-resident web publishing system, Proc. of 9th USENIX Security Symposium, Aug. 2000

[6] RFC 2246: The TLS Protocol Version 1.0, IETF, 1999