コンピュータセキュリティ 15－6
（２００１．１２．２１）

# 契約時に添える付加的なＭＡＣに関する総合的分析

小森　旭　　松浦 幹太　　須藤　修

東京大学大学院 情報学環・学際情報学府
〒113-0033 東京都文京区本郷 7-3-1

E-mail：komori.akira@iii.u-tokyo.ac.jp, kanta@iis.u-tokyo.ac.jp, sudoh@isics.u-tokyo.ac.jp

**あらまし：**PKI によるユーザ認証は，電子商取引の普及と拡大のために必要不可欠なセキュリティ技術である．したがって，もし電子署名生成用秘密鍵が第三者に漏洩すると，他者へのなりすましが可能となり，消費者に損害が生じてしまう．そこで我々は，論文 [1] において，証拠性を高めるために，電子署名とは別に新たに MAC を加えた方式を提案した．本稿では，我々の提案する方式と現行の法律との照合，ならびにその結果考えうる不正について，技術的・社会科学的な分析を行う．

# Total Analysis of Contract Agreement and Contribution of Extra MAC

Akira Komori　　Kanta Matsuura　　Osamu Sudo

Interfaculty Initiative in Information Studies,
Graduate School of Interdisciplinary Information Studies,
The University of Tokyo,
7-3-1 Hongo, Bunkyo-ku, Tokyo, 113-0033, Japan

E-mail：komori.akira@iii.u-tokyo.ac.jp, kanta@iis.u-tokyo.ac.jp, sudoh@isics.u-tokyo.ac.jp

Abstract：The user identification based on PKI is currently necessary for electronic commerce. Therefore, when a private key is revealed to an attacker, he can disguise himself as a legitimate holder of the key. This can cause a financial damage to the consumer. In order to solve this problem, we proposed a new security scheme which contains MAC as a stronger digital evidence [1]. In this paper, we discuss the problem and possible solution from the viewpoint of both technologies and social science.

## 1　はじめに

電子商取引において電子署名は，取引時におけるユーザ認証や契約文書の事後否認防止などの，重要な役割を担っている．それゆえ，もし電子署名生成用の秘密鍵が外部に漏洩すると，以下のような問題が生じ，ユーザは多大な損失を被る可能性がある．

- 他人が鍵の持ち主になりすませる
- 電子署名が契約の証拠として機能しなくなる

特に電子商取引におけるトラブル解決には，契約の証拠となるものが必要不可欠なので，電子署名が証拠として機能しなくなるのは重要な問題である．

このような問題に対し，さまざまな電子署名の偽

造対策技術が提案されている [2].

- タイムスタンプ
- Forward-Secure Digital Signature
- Fail-stop Signature
- ヒステリシス署名 [3],[4]

しかし，いずれの方式も何らかの欠点を抱えており，完全に偽造を防止することはできない．そこで我々は，論文 [1] において，秘密鍵が搾取され電子署名が偽造された場合を想定した上で，その際にどうすればユーザが被る損害を最小限に食い止めることができるかについて，**証拠性**に焦点を当てて考察を行った (この詳細は 2 章で述べる).

本稿では，我々が提案する方式を法律と照らし合わせて比較検討し，法律に準拠したプロトコルにした場合の問題点と解決策について考察する．

# 2 証拠性を重視した電子商取引プロトコル

## 2.1 研究背景

PKI を安全に利用するためには，きちんとした鍵管理が重要である．利用している PKI がセキュリティ的にどの程度安全かどうかは，秘密鍵の安全管理レベルに依存している．もし，秘密鍵が第三者に漏洩した場合，ユーザはすぐに公開鍵証明書の廃棄を CA(Certification Authority) に申請しなければならない．しかし，秘密鍵は紙の世界における印鑑とは異なりディジタルデータなので，鍵がコピーされ盗まれてもすぐにそれを検出することは容易ではない．つまり，一般にユーザが秘密鍵の漏洩に気づくのは，鍵を盗んだ第三者により悪用されてからであり，その間に被害が大きくなる可能性がある．しかも，仮にユーザが契約の取り消しを求める訴えを起こしたとしても，与えられた電子署名は正規ユーザが生成したものなのか，あるいは鍵を盗んだ第三者により偽造されたものなのかの区別がつかず，調停の判断材料に用いることができない．そこで我々は，このような脅威からユーザを保護するためには，取引の際に電子署名とは別のより強い証拠を残す必要があると考えた．

## 2.2 耐タンパ性の分類

そもそも，なぜ秘密鍵が搾取される可能性について考える必要があるのだろうか．本節では，この点について耐タンパ性の分類という面から考察を行う．一般に，秘密鍵のような機密性を必要とするデータは，IC カード等の耐タンパ性のある機器に格納することで，外部への漏洩を防止している．しかし，秘密鍵 (厳密には公開鍵証明書) には有効期限が定められており，更新する必要があるので以下のようなことが脅威になる．

- 耐タンパ内のデータを更新するときに，通信途中でそのデータを盗まれる．
- IC カードを R(Reader)/W(Writer) に挿入しているときに，偽造 R/W によって耐タンパ内のデータを不正にコピーされる．

つまり，秘密鍵は更新作業が必要な分，搾取される可能性があるものと考えられる．

以上の考察から，耐タンパ性をより厳密にかつ大まかに分類すると，以下の二つのレベルに分類することができる．

1. 更新する必要のないデータを格納する領域
2. 更新する可能性のあるデータを格納する領域

レベル 1 の領域に格納されるデータは，耐タンパ領域を最初に製造したときに格納され，そのとき以外は絶対に外部から読み出すことも書き込むこともできない．よって，この領域に格納されるデータは，外部に漏洩する可能性はない．これに対し，レベル 2 の領域に格納されるデータは，後から専用の機器を用いて読み書きすることが可能である．よって，この領域に格納されるデータは，更新するときに外部に漏洩する可能性がある．

## 2.3 証拠性を重視した方式の概要

そこで我々は，電子署名とは別のより強い証拠を残すために，レベル 1 の耐タンパ領域に機器固有のデータとして，MAC † (Message Authentication

† ふつうの鍵と管理の仕方が違い，デバイス固有の秘密領域に格納されている鍵と，電子商取引プロトコルにおいて署名をつけなければならないデータの 2 つから，一方向的に計算したもの．

Code) 生成用秘密パラメータ (鍵)K を格納する方式を論文 [1] で提案した．図 1 にその方式を示す．ここでは前提として，以下のようなことを想定している．

- IC カードを使った対面での取引である
- PKI を用いてユーザ認証を行う
- 他人の IC カードは使えない
- IC カードや R/W，端末機器の偽造はできない

よって，ユーザは IC カードから流れ出るデータを故意に改ざんしたりすりかえたりすることはできないものとする．また，IC カードごとなくせば，すぐ紛失に気づくと考えられるので，カード自体を紛失することは想定しない．

（論文で登場するエンティティの信用度）

ユーザ (消費者)A：IC カードの正規利用者．ただし信用はできない

販売店 B：カード会社に認められた正当なお店．ただし信用はできない

カード会社：信用できる (意図的に不正を働かない)

認証機関 (CA)：信用できる

調停者：信用できる

（論文で使用している記号の意味）

$S_A$：A さんの電子署名生成用秘密鍵
(耐タンパレベル 2 の領域に格納されている)

K：秘密のパラメータ (鍵)
(耐タンパレベル 1 の領域に格納されている)

X：契約書など

$SIG_A(X)$：秘密鍵 $S_A$ を使ってデータ X に電子署名を施したもの

$MAC_K(X)$：脚注† 参照

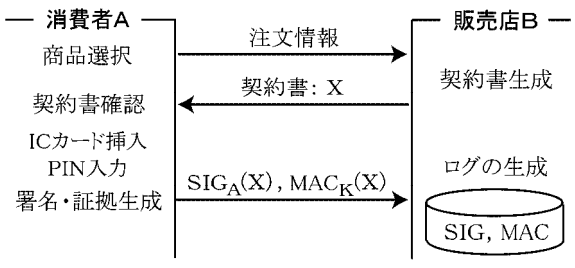


図 1: 提案する電子商取引プロトコル

何らかの商取引を行う際，消費者は電子署名 $SIG_A(X)$ に加えて，IC カード固有の鍵 K で生成した MAC を添えることで，より高い証拠性を実現している．

## 2.4 調停プロトコル

本節では，署名生成用秘密鍵の漏洩により，ユーザに何からのトラブルが発生した場合の，調停者による調停作業の手順について説明する．調停プロトコルを図 2 に示す．

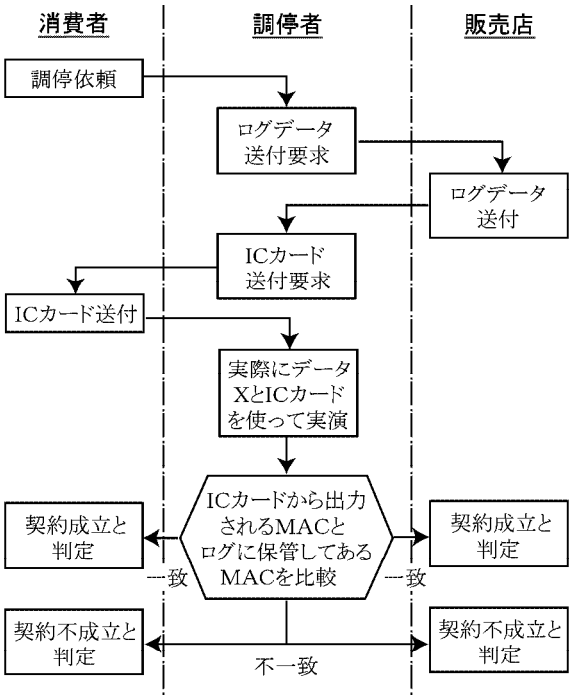


図 2: 紛争解決プロセス

調停を行うために，消費者は自分の IC カードを，店はログに保管してある $SIG_A(X)$ と $MAC_K(X)$ を調停者に提出する．そして，実際にデータ X と IC カードを使って実演してみて，IC カードから出力される MAC とログに保管してある MAC が異なるならば，契約は破棄される．

# 3 契約の成立時期

商取引を行う上で重要なのは，どの時点で契約が成立するかである．よって本章では，我々の提案方式と法律を照らし合わせながら，契約の成立時期について議論する．

## 3.1 発信主義と到達主義

通信販売などの郵便による隔地者間取引では，民法第 526 条第 1 項 (付録 A.1 節参照) により，承諾の通知を発信した時に契約が成立する (発信主義)．これに対し，Web やメールなどの電子的方法を用いた隔地者間取引では，平成 13 年 6 月 22 日に成立した『電子消費者契約及び電子承諾通知に関する民法の特例に関する法律』(以後『電子消費者契約法』と略す)[5] により，承諾の通知が到達した時点で契約が成立する (到達主義)．

## 3.2 提案方式と法律との比較

電子商取引において，一つの IC カードが対面とネットワークの両方で使えるほうが利便性は高い．そこでここからは，我々の提案する方式の前提条件を甘くし，ネットワーク上での支払いにも利用可能であると想定して議論を進める．

また，ここでの議論は，対面取引の契約時期に関する法律が，電子消費者契約法に準じて制定された場合の，システム作りの指針にもなる．我々の提案方式と到達主義のプロトコルを照らし合わせると，図 3 のようになる．

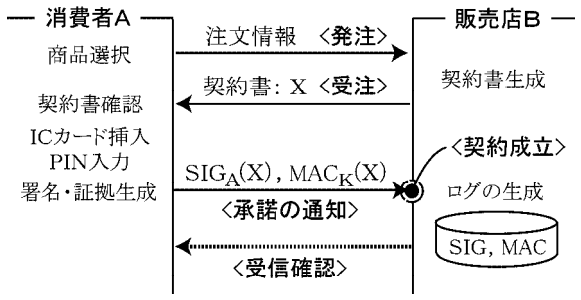


図 3: 到達主義のプロトコルとの比較

比較してみるとわかるように，$SIG_A(X)$ と $MAC_K(X)$ の送信が承諾の通知を表しており，このデータが店側に到着した時点で契約が成立する．しかし，このままだと消費者は，署名と MAC がきちんと店側に届いたかどうかわからず，契約が成立したのかどうかの判断ができない．そこで店側は，承諾通知が届いたあとで，メールや FAX のような契約の申込みとは別のインフラを使って，受信確認を知らせる必要がある．ここで，契約の申込みと受信確認の発信に別々のインフラを使う理由は，例えば次のような利点があるからである．

- 消費者に関する個人情報の誤りを発見できる (例えば，メールアドレス等)
- 故意に改ざんした個人情報を検出できる

これにより，注文情報に含まれる消費者に関する個人情報の信憑性を確認できるとともに，不正者がなりすましをするためのコストの増加が見込める．

## 3.3 通信データの消失

ネットワークを介した電子商取引では，通信途中でデータが消失したり，何らかの影響でデータが送信されなかったりする可能性がある．本節では，次の A，B の 2 つの場合について，契約の成立時期という観点から考察を行う．

A). 店側が受注データ (契約書) を発信したが，承諾の通知 (署名と MAC) が返信されない場合

このような事象が生じる原因として，

① 受注データが正常に消費者側に到達しなかった．

② 受注データが正常に到達したにもかかわらず，消費者側が承諾の通知の発信を怠った．

③ 受注データが正常に到着し，消費者側が承諾の通知を発信したが，それが正常に店側に到達しなかった．

という 3 通りが考えられる．いずれの場合も契約は成立しておらず，このままでは店側は一旦発信した受注データに縛られてしまい，取引の迅速性の要請を害することになる．

これらについて検討すると，まず①及び②の場合には，「店が受注データを発信後，一定期間内に店に承諾の通知が伝達されない場合，契約の申込みは効力を失う」ということを，発注前に消費者に提示するもしくは契約書に記載すれば，店をフリーハンドの状態に戻すことができ，問題なく解決が得られる．これに対し③の場合には，このような取り扱いをすると今度は消費者側において発信した承諾の通知に縛られてしまう．しかしこの場合，消費者は受信確認が届かないことで何らかの不具合が発生したことを知ることができ，契約を消滅させても消費

者側にさほど不利益は生じないと考えられるので，店側が承諾の通知の到達を確認できない場合には，一定時間の経過により，申込みの効力は失われるものとしても問題ない．ただし，契約書にトラブル発生時の連絡方法を記載し，それを消費者が利用して承諾通知の到達を確認できるようにしておくとより良い．

B). 消費者側が承諾の通知 (署名と MAC) を発信したが，受信確認 (確認メール等) が返信されない場合

このような事象が生じる原因として，

① 承諾の通知が正常に店側に到達しなかった．(上述した③のケース)

② 承諾の通知が正常に到達したにもかかわらず，店側が受信確認の発信を怠った．

③ 承諾の通知が正常に到達し，店側が受信確認を発信したが，それが正常に消費者側に到達しなかった．

という 3 通りが考えられる．①の場合には契約は成立していないが，②，③の場合には成立している．

これらについて検討すると，まず①の場合には，そもそも契約が成立していないので，消費者は受信確認の到達を確認できない旨を，契約書に記載された方法で店側に連絡し，確認してから改めて契約の申込みを行えばよい．これに対し②，③の場合には既に契約が成立しており，消費者側が一旦発信した承諾の通知に縛られてしまう．そこで，これらの場合にも，電話等の契約書に記載された方法により店側に連絡し，承諾の通知が到達したかどうかの確認をすればよい．ただし②の場合は，連絡をしても店が受信確認を送らず，承諾の通知で送った署名データを持ち逃げされ悪用される可能性があるので，何らかの対策を考える必要がある (この問題に関しては，3.4 節で論じる方法を用いることにより解決可能である)．

なお，店頭での電子商取引の場合は，仮に機器間を流れるデータが通信途中で消失しても，システムによりリアルタイムな検知可能なので NG を出力すれば良く，本節で議論したような問題は発生しない．

## 3.4 契約時における不正

論文 [1] では，秘密鍵搾取により起こり得る不正とその対策について考察を行った．これに引き続き本稿では，契約の成立時期に関連して起こり得る不正とその対策について考察を行う．

各エンティティの信用度は前述の通りである (2.3 節の枠内参照)．よって，店の行動は信用できないので，契約の成立時期を考慮に入れると以下に挙げるような不正を行う可能性がある．

A). 契約成立後 (受信確認がユーザに届いた後) に，店が手抜きをして商品を発送しない．

B). 例えば電子マネーのような，決済のタイミングが即時払いである決済方法で取引を行う場合，消費者は承諾の通知を送る際に一緒に電子マネーも送信すると，店に電子マネーを持ち逃げされる可能性がある．

不正 A が起こる原因は，消費者側に契約の証拠となるものが全く残っていない点にある．そこで，受信確認には店の電子署名を付与し，これを契約成立の証拠として保管するべきである．

また，不正 B が起こる原因は，電子マネーを送信したという証拠が残らないという点にある．そこで，契約書の中に「私は○○円受け取りました」というような記載を加え，さらに電子署名を付与し，これを電子マネーが持ち逃げされた場合の証拠とするべきである．ただし，そうすると今度は消費者が次のような不正を行う可能性がある．

b). 消費者は，店の署名付き契約書を受信するとセッションを打ち切り，後から署名付き契約書を証拠に，代金を支払っていないにもかかわらず，代金の返金もしくは商品の発送を要求する．

よって，不正 B と不正 b を防ぐには，2 者間で公平なデータ交換を実現するためのプロトコルが必要である．そこで，同時契約交換プロトコル [6]，もしくは電子仮捺印技術 [7] を用いて，「電子マネーデータ」と「それを受け取ったという証拠データ」の持ち逃げを防止すればよい．

以上まとめると，我々が提案する証拠性を高めた決済プロトコルは図 4 のようになる．

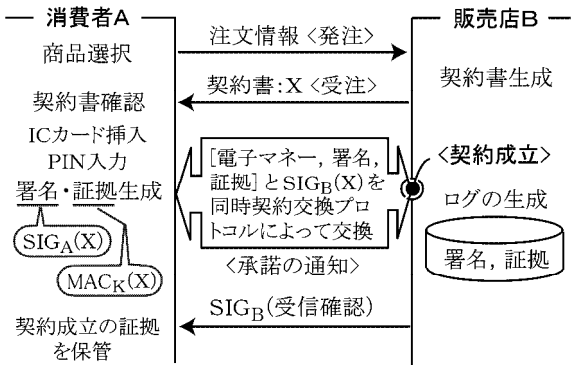


図 4: 法律を考慮に入れた EC プロトコル

### 3.5 考察

一般に，すべての消費者が契約の成立時期に関する法律を熟知しているとは考えにくい．よって，消費者保護を重視するのであれば，個々の契約書にどの時点で契約が成立するのかを明記した方がよい．

この点を含め，ネットワークを介した電子商取引における無用なトラブル防止のためには，契約書に記載される項目が重要になる．よって，契約書作成の際には内容を十分に熟慮する必要がある．

## 4 おわりに

本稿では，電子商取引プロトコルに MAC を加えることで，より証拠性を高めた方式について，契約の成立時期という面から考察を行った．その結果，紛争解決のためには，消費者と店の両者が何らかの証拠データを残しておく必要があるということが鮮明になった．しかし，電子商取引プロトコルとログ生成プロトコルの間にリンクはないので，店は受信したデータを故意に改ざんせずにログに保管するとは限らない．よって今後は，ログ生成時の不正による各エンティティの損得関係を分析する予定である．

## A 付録

### A.1 民法第 526 条

[隔地者間の契約の成立時期，意思実現による契約の成立]
①隔地者間ノ契約ハ承諾ノ通知ヲ発シタル時ニ成立ス

## 参考文献

[1] 小森 旭, 松浦幹太, 須藤 修: PKI に基づく C/S 型アプリケーションの安全性分析と証拠性評価, コンピュータセキュリティシンポジウム (CSS2001) 論文集, pp.319-324, Oct. 2001.

[2] 洲崎誠一, 松本 勉: 電子署名の偽造に関する一考察, コンピュータセキュリティシンポジウム (CSS2001) 論文集, pp.211-216, Oct. 2001.

[3] 松本 勉, 岩村 充, 佐々木良一, 松木 武: 暗号ブレイク対応電子署名アリバイ実現機構 (その 1) -コンセプトと概要-, 第 8 回コンピュータセキュリティ研究会 (CSEC), pp.13-17, Mar. 2000.

[4] 洲崎誠一, 宮崎邦彦, 宝木和夫, 松本 勉: 暗号ブレイク対応電子署名アリバイ実現機構 (その 2) -詳細方式-, 第 8 回コンピュータセキュリティ研究会 (CSEC), pp.19-24, Mar. 2000.

[5] 経済産業省: 報道発表, Mar. 2001. http://www.meti.go.jp/kohosys/press/0001428/

[6] 宇根正志: 電子文書の送受信証明を行うためのプロトコルの研究動向と安全性評価, IMES Discussion Paper Series 2000-J-33, 日本銀行金融研究所, Dec. 2000.

[7] 宝木和夫, 白石高義, 佐々木良一: IC カード利用の電子取引用認証方式, 電気学会論文誌 C 分冊, Vol.107, No.1, pp.46-53, 1987.