SCIS 2002 The 2002 Symposium on Cryptography and Information Security
Shirahama,Japan, Jan.29-Feb.1,2002
The Institute of Electronics, Information and Communication Engineers

電子商取引における紛争解決のための電子証拠物に関する分析

Analysis of Digital Evidence for Financial Dispute Settlement

小森 旭* 松浦 幹太* 須藤 修*
Akira Komori Kanta Matsuura Osamu Sudo

あらまし PKI による電子認証は，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，もし署名生成用秘密鍵が第三者に漏洩すると，他者による電子署名の偽造が可能になるとともに，電子署名が取引の証拠として機能しなくなり，消費者に損害が生じてしまう．そこで我々は，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，その方式について技術的・社会科学的な考察を行ってきた．これに引き続き本稿では，電子商取引において紛争解決のために用いる電子証拠物について分析を行う．

キーワード PKI，電子商取引，電子署名，耐タンパ性，証拠

1 はじめに

現在，公開鍵暗号は電子商取引に欠かせない技術であり，その確実な運用のために PKI(Public Key Infrastructure) は必要不可欠なインフラである [1]．PKI を利用する際に最も難しいのは，証明書の廃棄管理である．証明書には鍵の寿命や CA(Certification Authority) の責任範囲などとの関係で有効期限が設けられており，有効期限が切れる前に鍵を紛失したりした場合には，所定の手続きに基づいて CA が証明を取り消す．CA は取り消した証明書のシリアル番号と取り消した日付を管理して，定期的に CRL(Certificate Revocation List) としてまとめて発行し配布する [2]．そして，証明書が現在有効かどうかを確認するときに，証明が取り消されていないかを CRL のデータと突き合わせて電子的に調べることになっている．

PKI モデルでは，エンドエンティティが CRL を入手し，証明書の有効性を検証するのが基本である．しかし，1 つの証明書の有効性のみを検証したいだけであるのに，サイズの大きな CRL を入手したり，毎回 CRL のデータ全体を解析するのは非効率な場合がある．しかも，CRL は一定周期で発行されているので，証明書廃棄を申請してからそれが CRL に反映されるまでに，タイムラグが発生してしまう．このような問題の解決策として，基準となる CRL からの差分の失効情報のみをより短い間隔で発行するデルタ CRL や，オンラインで証明書が有効かどうかを問い合わせる OCSP(Online Certificate Status Protocol) といった方法が提案されているが，タイムラグが発生することに変わりはなく，問題の本質的な解決策にはなっていない [2][3].

以上，証明書廃棄の問題点について簡単に述べてきたが，CRL であれ OCSP であれ，実際に鍵の漏洩に気づくのは盗まれた鍵を使って悪用された後であり，漏洩した時点ですぐに廃棄を申請できるとは限らない．そこで我々は，証拠性を高めるために，電子署名とは別に新たに MAC(Message Authentication Code) を加えた方式を提案し，その方式について技術的・社会科学的な考察を行ってきた [4][5]．これに引き続き本稿では，電子商取引において紛争解決のために用いる電子証拠物について分析を行う．

本稿の構成は次の通りである．第 2 章で証明書廃棄時に発生するタイムラグの問題と，秘密鍵の管理方法とその安全性について述べ，第 3 章で記号の定義等の準備を行う．第 4 章で証拠性を高めた方式の概要を説明し，第 5 章で安全なログシステムとは何かについて考察する．最後に第 6 章で本稿をまとめる．

2 背景

2.1 証明書廃棄の限界

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，ユーザはすぐに証明書の廃棄を CA に申請しなければならない．図 1 に証明書廃棄の時間経緯を示す [6].

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

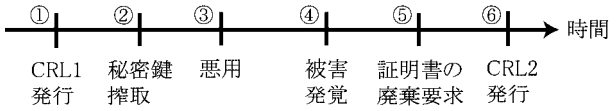

図 1: 公開鍵証明書廃棄の時間経緯

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 (図 1-②) すぐにそれを検出することは容易ではない．つまり，実際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何からの悪用をされ (図 1-③)，被害に遭ってからであり (図 1-④)，その間に被害が大きくなる可能性がある．しかも，被害発覚後すぐに証明書の廃棄を申請しても (図 1-⑤)，CRL は一定周期で発行されているので (図 1-①⑥)，申請がすぐに CRL に反映されない．さらに，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，提示された電子署名が，正規ユーザと鍵を盗んだ第三者のどちらが生成したものなのかの区別がつかないので，電子署名を調停の判断材料に用いることができない．

このような問題を解決するため，電子署名の偽造防止という観点からさまざまな対策技術が提案されている [7]．これに対し我々は，正当な電子署名付きメッセージに別のより強い証拠を付加することで，秘密鍵が搾取され電子署名が偽造された場合でも，ユーザが被る損害を最小限に食い止める方式を考えた．

2.2 IC カードのセキュリティ

PKI システムを構築した場合，ユーザの秘密鍵をどう保護するかという問題がある [8]．PKI において，秘密鍵の鍵管理は基本的にユーザ自身の義務であり，ユーザが責任を持って行わなければならない．しかし，これはユーザにとって容易なことではない．もし，秘密鍵が悪意を持った第三者に盗まれてしまうと，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．

- 第三者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

秘密鍵をハードディスク上にファイルの形で保存し，パスワードで保護することも可能であるが，これではパスワードの脆弱性から抜け出すことはできない [8]．そこで，利用されているのが IC カードである．IC カードは耐タンパ性 [9] という性質を持っており，耐タンパ内に格納されたデータは不正に読み出すことができない．よって，秘密鍵を IC カードに格納すれば，秘密鍵が搾取される可能性は低くなる．

カード自体の盗難に対しても，カード使用時に入力する PIN(Personal Identification Number) を連続して一定回数間違えると，IC カードがロックして使えなくなる機能により，高い確率で第三者による悪用を防ぐことができる．

2.3 耐タンパ性の分類

IC カードを使えば，耐タンパ性により機密データを保護することができると言われている．しかし，仮に秘密鍵を IC カードに格納したとしても，耐タンパ性はデータ搾取の可能性を少なくするための道具にすぎず，秘密鍵の外部への漏洩を完全に防止することはできない．例えば，秘密鍵が搾取される要因として以下のようなことが挙げられる．

- 運用も含めた鍵の管理方法に問題があり，物理的手段によって悪意を持った第三者に秘密鍵が盗まれてしまう．
- 各エンティティの秘密鍵を CA が生成・配布するような環境下では，物理的手段によって悪意を持った第三者に秘密鍵が盗まれてしまう．

特に，秘密鍵には有効期限が定められており，鍵を更新する作業が必要なので，その分，搾取される可能性があるものと考えられる．ただし，IC カードシステムの中には，IC カード内にあらかじめ複数の鍵情報を書き込み，期限到来により自動的にカード内部で別の鍵に切り替わる等の機能を持つ方式もあるが，本稿ではそのような方式は想定していない．

以上の考察から，耐タンパ性をより厳密に分類すると，次の二つのセキュリティ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

セキュリティレベル 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，セキュリティレベル 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．

3 準備

3.1 エンティティ

本論文で登場するエンティティとその信用度を以下に記す．

- **ユーザ** (消費者)：IC カードの正規利用者．ただし信用はできない

- **販売店**：カード会社と契約を結んだカード加盟店．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

3.2 表記

本論文で使用する記号の意味を以下に記す．

- S_A：A さんの電子署名生成用秘密鍵 (セキュリティレベル 2 の領域に格納されている)
- K：秘密のパラメータ (鍵) (セキュリティレベル 1 の領域に格納されている)
- X：契約書などのデータ
- $SIG_A(X)$：秘密鍵 S_A を使ってデータ X に電子署名を施したもの＋平文のデータ X
- $E_k(X)$：共通鍵暗号方式における秘密の鍵 k でデータ X を暗号化したもの
- H(X)：データ X のハッシュ値
- $MAC_K(X)$：脚注† 参照

4 証拠性を重視した方式

4.1 概要

我々は，電子署名とは別のより強い証拠を残すために，セキュリティレベル 1 の耐タンパ領域に機器固有のデータとして，MAC † 生成用秘密パラメータ (鍵)K を格納する方式を論文 [4] で提案した．図 2 にその方式の一例を示す．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商取引である
- PKI を用いてユーザ認証を行う
- オフライン攻撃が不可能な PIN 認証プロトコルを使う

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，秘密鍵の漏洩とは異なり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．

† 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．

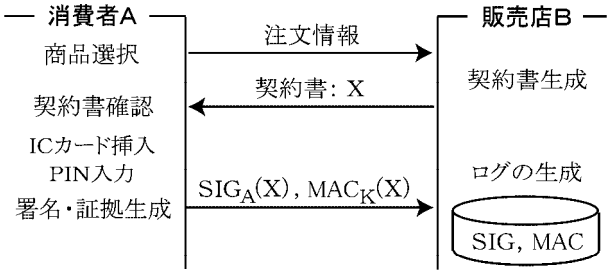

図 2: 提案方式の一例

例えば，図 2 のような，契約書 X に電子署名 $SIG_A(X)$ を付与するプロトコルであれば，そこに，IC カード固有の鍵 K で生成した MAC が加わる．これにより，強い証拠性を実現することができる．

4.2 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 3 に示す．

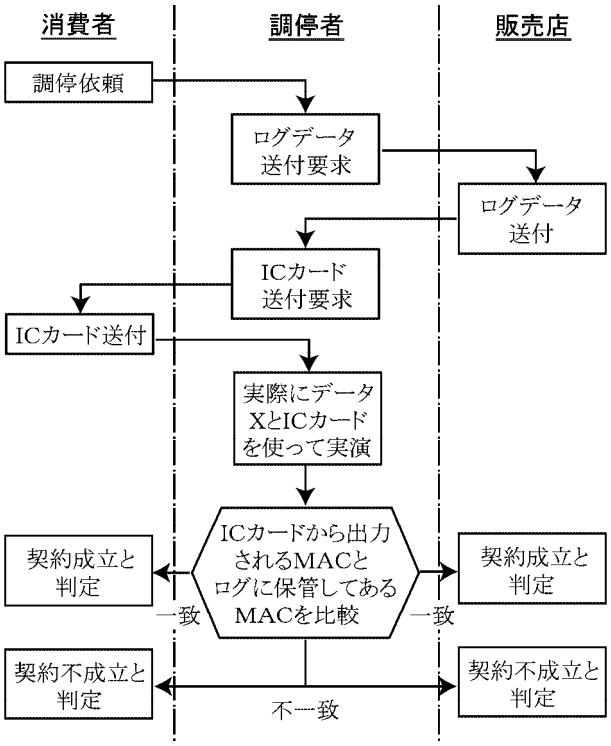

図 3: 紛争解決プロセス

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，調停者は実際にデータ 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．

5 議論

5.1 証拠データの保存

契約が成立すると，販売店はトラブル時に備えて，$SIG_A(X)$ と $MAC_K(X)$ を取引の証拠データとして安全なログに保管する．このログには次のような機能が必要である．

- 後から不正にログデータを改ざん，削除，追加すると，その事実を検出することができる．
- ログを保存するシステムを攻撃者に乗っ取られたとしても，攻撃者はログデータを読んだり，改ざんしたりすることができない．
- ログ生成者とは別の信頼できる第三者機関 (TTP：Trusted Third Party) が，ログデータの正当性を検証できる．

これらの機能を実現するログシステムとして，例えば Schneier と Kelsey は，暗号により保護された安全な監査ログシステムを提案した [10]．このログシステム (以後 SK 方式と呼ぶ) の構成を図示すると，以下のようになる．

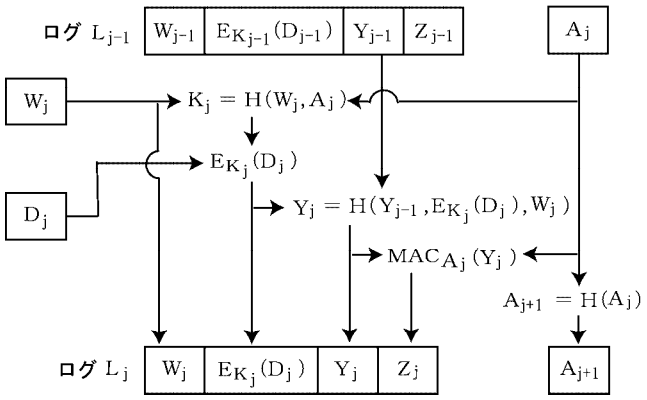

図 4: ログシステムの構成

図 4 で使用されている記号の意味は以下の通りである．

- D_j：j 番目のログに入力されるデータ
- A_j：j 番目のログに対するデータ認証用の鍵．A_{j+1} が計算されると A_j は削除される
- K_j：j 番目のログに入力されるデータ D_j を暗号化するための鍵．K_{j+1} が計算されると K_j は削除される
- Y_j：ログに入力されるデータのハッシュチェーン
- L_j：j 番目のログデータ

なお，論文 [10] の中では，W_j がどのようなデータであるかの具体的な記載はない．一般的には，データ D_j についている制御情報などのメタデータと考えられるが，W_j にどんなデータを加えることも可能である．W_j をどうするかで，電子商取引プロトコルとログ生成プロトコルのモデルが大きく異なってくるので，本稿では W_j に対応するデータは特定しない．

また，SK 方式の利点としては，以下のようなことが挙げられる．

- ハッシュチェーンを用いることで，ログ生成者や攻撃者によるログデータの事後的な改ざんを検出することができる．
- ログシステムを攻撃者に乗っ取られたとしても，ログデータは使い捨て鍵で暗号化されているので，元の入力データを読まれることはない．よって，ユーザのプライバシー保護についても一定の効果がある．
- 誰もがハッシュチェーンの正当性を検証できる．
- マスターシード A_0 を持っている，ログ生成者とは別の信頼できる第三者機関 (TTP) だけが，すべてのログデータを読むことができる．

このように，SK 方式を利用することにより，過去のログデータの改ざんを検出することができる．しかし，新たに入力されるログデータの改ざんは，検出することができない．つまり，電子商取引プロトコルとログ生成プロトコルの間にはリンクがないので，**最初に証拠データをログに入力する時点で，故意に改ざんしたデータをログに入力する**という不正は可能である．この手の不正は，ログシステムの代わりに電子公証 [11] を利用しても防ぐことができない．

5.2 電子帳簿保存法

電子取引行った場合，その取引情報[1] の保存は『電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律 (略称：電子帳簿保存法)』(平成 10 年 7 月 1 日施行) により義務づけられている．よって，基本的には，店は取引の証拠データをきちんとログに保管するものと考えられる．

5.3 ログ生成時における不正

我々が提案する方式は，店が $SIG_A(X)$ と $MAC_K(X)$ を取引の証拠データとして安全なログに保管することを前提としている．しかし，MAC は乱数にしか見えないので，店がでたらめなデータを MAC に見立てることが可能である．つまり，ログの入力時点で，店が故意に改

[1] 取引の際に受領または交付する注文書，契約書，送り状，領収書，見積書等

ざんしたMACをログに入力しても，それを検出することはできない．よって本節では，ログ生成時に不正が行われた場合の，各エンティティ間の損得関係について分析する．

5.3.1 ユーザによる攻撃

店が取引の証拠データ (署名と MAC) をログに保管することを，時々(もしくは完全に) 手抜きするような場合を考える．この場合，契約成立後に何もトラブルが発生しなければ全く問題ないが，悪意のあるクライアントを生み出す可能性がある．例えば，もし仮に，ある正規ユーザに証拠データの保管を手抜きしていることが知られてしまうと，そのことを利用したユーザによる攻撃が可能になる．以下にその攻撃を時系列で示す．

1. ユーザはふつうに正当な取引を行い，商品を受け取る．
2. 後日，ユーザは「それは鍵を盗んだ第三者により行われた取引である」と主張し，契約の取消を店に求める．
3. すると，調停者による実演の結果，ユーザの IC カードから出力される MAC と，店のログの保管してある MAC は一致しないので (なぜなら，店はでたらめなデータをログに保管していたからである)，ユーザの主張は認められ，決済方式の違いにより他のエンティティが損害を被る．

- 決済が後払いの場合：すでに，店とカード会社の間で決済処理が終わっているとした場合，ユーザに送った請求書の金額を回収することができないカード会社が損をする．ただし，カード会社がカードに関するトラブルの損失を補償してくれるような保険に加入していれば，多少の損失は保険によりまかなわれる．
- 決済が即時払いの場合：契約成立時に受け取った代金の返却を求められる店が損をする．よって，この場合，店がログの保管を怠ることは考えにくい．

このような攻撃が行われた場合の，各エンティティ間の損得関係をまとめると，表 1 のようになる．表において，U はユーザ，S は販売店，C はカード会社を表している．

表 1: 各エンティティの損得関係

		U	S	C
S がきちんとログを保管する[2]	後払い	×	-	-
	即時払い	×	-	-
S が完全にログの保管を怠る[2]	後払い	○	-	×
	即時払い	○	×	-

○:得する，×:損する，-:損得なし

5.3.2 ユーザと販売店の結託攻撃

店が故意に改ざんした証拠データをログに残せることを利用して，ユーザと店が結託攻撃を行う場合を考える．この攻撃の流れは以下の通りである．

1. ユーザと店との間で，架空の取引を行う．店はユーザの署名と，MAC としてでたらめな値をログに保管する．
2. 後日，ユーザは「それは鍵を盗んだ第三者により行われた取引である」と主張し，契約の取消を求める訴えを起こす．
3. すると，調停者による実演の結果，ユーザの IC カードから出力される MAC と，店のログの保管してある MAC は一致しないので (なぜなら，店はでたらめなデータをログに保管していたからである)，ユーザの主張は認められ，決済方式の違いにより他のエンティティが損害を被る．

- 決済が後払いの場合：店は架空の契約をでっちあげた後，すぐにカード会社との間で決済処理を行うものと考えられるので，ユーザに送った請求書の金額を回収することができないカード会社が損をする．ただし，攻撃するに値する高額のディジタル商品があるかどうかが疑問である．
- 決済が即時払いの場合：基本的には架空の契約が取り消されるだけなので，どのエンティティも損得はない．ただし，店がトラブル時の損失を保証してくれるような保険に加入していれば，保険料が下りることにより，一種の保険金詐欺が成立する．

このような攻撃が行われた場合の，各エンティティ間の損得関係をまとめると，表 2 のようになる．

表 2: 各エンティティの損得関係

		U	S	C
S が改ざんした証拠をログに保管する	後払い	-	○	×
	即時払い	-	△	-

○:得する，△:やや得，×:損する，-:損得なし

5.4 考察

総合的に分析すると，店がログ生成時に不正を行うことにより，損をするのはカード会社である．よって，カード会社の損失を防ぐためには，例えば次のような方法が考えられる．

- カード会社の社員が一般客のふりをして買い物をし，その後すぐに TTP と協力して，店が正当な MAC をログに保管しているか抜き打ち検査する．

[2] 店がたまにログの保管を怠る場合は，両方の場合に属する．

- TTP 自体をカード会社が運営する．

これらの方法により，店が故意に改ざんしたログを残す行為を抑制できると考えられる．

6 まとめ

PKI による電子認証は，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．今後も電子商取引の拡大と安定成長を継続していくには，消費者の信頼確保が必須条件であり，その実現には消費者保護の観点においてシステムを構築する必要がある．しかし，PKI は鍵が搾取される可能性のあるインフラである．それゆえ，PKI を用いて電子商取引を行う場合，電子署名に”認証”と”証拠”の両方の機能を持たせているので，鍵を搾取されると消費者は損失を被る可能性がある．これは，消費者保護の観点では，あまり好ましいことではない．よって我々は，電子商取引において証拠性を確保するためには，電子署名に証拠機能を持たせるのではなく，署名インフラとは別に新たに証拠インフラなるものを構築する必要があると考えた．そして，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システムについて，紛争解決のために必要な電子証拠物に焦点を当てて考察を行った．今回，証拠データとして MAC を使用したのは，単純で汎用性が高く，通信コストもかからないからである．しかし，トラブル時の行動を含めた，システム全体の効率性を考えると，次のようなことが未解決な問題として残っている．

- 契約の取り消し時に，わざわざ IC カードを使って実演する必要がある．
- MAC データから不正者を特定することができないので，不正者は同じ攻撃方法で何人ものユーザから署名用秘密鍵を搾取し，低コストで不正行為に成功する可能性がある．
- IC カードをなくしたり壊したりすると，キーリカバリ機能はないので，紛争解決時にユーザが提出する証拠物がなくなる．
- コンピュータの処理能力が向上すると，MAC データから機器固有の秘密のパラメータが算出可能になる．

そこで今後は，これらの問題を改善するため，情報量的に安全な証拠インフラの構築について考えていく予定である．

参考文献

[1] 谷口文一: 金融業界における PKI・電子認証について, IMES Discussion Paper Series No.99-J-30, 日本銀行金融研究所, Aug. 1999.

[2] R. Housley, et al.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, Jan. 1999.

[3] M. Myers, et al.: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, RFC2560, Jun. 1999.

[4] 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 2001 論文集, 情報処理学会, pp.319-324, Oct. 2001.

[5] 小森 旭, 松浦幹太, 須藤 修: 契約時に添える付加的な MAC に関する総合的分析, 情報処理学会研究報告, 2001-CSEC-15, pp.31-36, Dec. 2001.

[6] W. Ford, M. S. Baum: Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, Prentice Hall, 1997. (邦訳: 山田慎一郎: ディジタル署名と暗号技術, ピアソン, 1997.)

[7] 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 2001 論文集, 情報処理学会, pp.211-216, Oct. 2001.

[8] 能勢健一朗, 麻野間利行, 西岡 満: PKI 構築サービスと PKI カードシステム TARGUSYS, 東芝レビュー, Vol.56, No.7, 2001.

[9] Andrew J. Clark: Physical Protection of Cryptographic Devices, Advances in Cryptology - EUROCRYPT ’87, LNCS 304, Springer-Verlag, pp.83-93, 1988

[10] B.Schneier, J.Kelsey: Cryptographic Support for Secure Logs on Untrusted Machines, The Seventh USENIX Security Symposium Proceedings, pp.53-62, USENIX Press, Jan. 1998.

[11] 電子商取引実証推進協議会: 電子公証システムガイドライン (1.0 版), Dec. 1997.
http://www.ecom.jp/qecom/