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

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：qq16111@iii.u-tokyo.ac.jp, kanta@iis.u-tokyo.ac.jp, sudoh@isics.u-tokyo.ac.jp

PKI において秘密鍵が第三者に漏洩した場合，証明書廃棄を申請する必要がある．しかし，実際に漏洩に気づくのは，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．よって，本稿では取引の際により強い証拠を残すことにより，鍵が漏洩した場合でもできる限り消費者を保護するシステムの構築について考察する．

Security Analysis and Digital Evidence in Client/Server Application based on PKI

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：qq16111@iii.u-tokyo.ac.jp, kanta@iis.u-tokyo.ac.jp, sudoh@isics.u-tokyo.ac.jp

When a private key is stolen to an attacker in PKI, it is necessary to revoke the corresponding certificate. The revocation occurs after finding that the key has been abused. This implies some financial damage to the legitimate holder of the key. In order to solve this problem, we construct a system which helps consumers by a stronger digital evidence.

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，デルタ CRL や 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，既存の証明書廃棄方法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．したがって，本稿では取引の際により強い証拠を残すことにより，鍵が漏洩した場合でもできる限り消費者を保護するシステムについて考察する．

2　証明書廃棄の限界

図 1 に証明書廃棄の時間経緯を示す [4]．ただし，ここでは PKI を使った電子商取引のうち，SET(Secure Electronic Transaction) のような，決済のタイミングが後払いであるクレジット型電子決済を想定している [5].

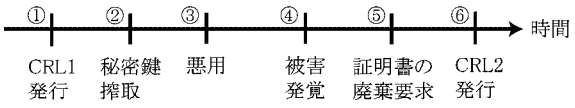

図 1: 公開鍵証明書廃棄の時間経緯

① ある時刻において CRL1 が発行されたとする．

② その後，ある正規ユーザーの秘密鍵搾取に攻撃者が成功したとする．この時点で搾取に気づくユーザーはほとんどいないだろう．

③ 攻撃者はすぐにその秘密鍵を使って何らかの悪さをする．

④ 数日後，正規ユーザーの元へ身に覚えのない請求書が届く．

⑤ すぐにユーザーは証明書の廃棄を CA に申請する．しかし，PKI のモデルにより多少の違いはあるものの，CRL はある一定の間隔で発行されているので，申請がすぐに CRL へ反映されない．

⑥ 次の CRL の発行時刻になり，初めて廃棄の申請が CRL に反映される．

このように，秘密鍵が搾取されてから，証明書廃棄が CRL に反映されるまでには，かなりのタイムラグがあり，この間に被害がどんどん拡大する恐れがある．これは，消費者保護の観点では望ましいことではない．

3　耐タンパー性の分類

前章までは，証明書廃棄における問題点について考察を行ってきたが，そもそもなぜこのような問題が発生するのだろうか．それは，PKI では秘密鍵が搾取される可能性があるからである．よって本章では，どうして秘密鍵が搾取されるのかについて，耐タンパー性の分類という面から考察を行う．

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．しかも，PKI を普及させるには，重要な秘密鍵を誰にでも簡単に扱えるようにする工夫が必要である．安全性と利便性の両方を満たす秘密鍵の管理方式については，耐タンパー性をもつ IC カードや専用ハードウェアと組み合わせる方式が一般的である．耐タンパー性というと，「中身を見ようとすると壊れる性質」と記述されているのが一般的だが，より厳密に定義すれば，以下の 4 つのレベルに分類することができる．

1. 絶対に内部の情報は不正に読み出せないし書き込めない．(最初に製造したとき以外は書き込めない．)

2. 絶対に内部の情報は不正に読み出せないが，後から書き込むことはできる．(専用の機器を用いれば書き込める．)

3. 不正に読み出そうとすると，データ自体が壊れる．
4. 普通の人は見れないが，知識のある人には見られてしまう．

大まかに分類すると，レベル 1 には更新する必要のないデータ，レベル 2-4 には更新する可能性のあるデータが格納されている．

耐タンパーが後者のレベルの場合，以下のようなことが脅威になる．

- データを更新するときに，そのデータを盗まれる．
- IC カードをリーダ/ライタに挿入しているときにデータを抜き取られる．

PKI における秘密鍵は，有効期限が定められており更新する必要があるので，後者のレベルの耐タンパー領域に格納されている．

4 提案するシステムの概要

4.1 前提条件

4.1.1 IC カードの認証

本システムは，鍵を格納した IC カードを使って，対面で何らかの取引を行うことを想定している．

IC カードを利用する上では，特に次のことが脅威になる．

- 他人の IC カードの使用
- IC カードの偽造・変造
- 端末機器の偽造

これらのリスクに対抗するには，PIN(Personal Identification Number) による本人確認や，IC カードと端末機器の間の相互認証といった手法を用いる必要がある [6].

また，IC カードの製造・配布の段階で，カード固有の秘密情報が外部に漏洩することはない．さらに，リーダ/ライタと端末機器の間と，端末機器とホストシステムの間を流れるデータは，セキュアな通信路を確保することにより，外部から盗聴・改ざんされることはない．よって，カード利用者も 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．

4.1.2 証拠生成用秘密パラメータ K

取引の際に，PKI における電子署名とは別のより強い証拠を残すために，IC カードの耐タンパーレベル 1(**3** 章参照) の部分に MAC(Message Authentication Code) 生成用秘密パラメータ (鍵)K を格納する．K は IC カード製造時に格納され，IC カード固有のものであり，他の場所には保管されない．K は更新する必要はなく，IC カードを破棄すると K も破棄される．また，ID と鍵が結びついている X.509 証明書とは異なり，K は ID と結びついていないので，匿名性を必要とするシステムとも相性がよい．

4.1.3 主体

カード発行会社は完全に信頼できる会社であり，一人の人間に複数の有効な IC カードを発行することはない．また，カード利用者が自分の IC カードを紛失することは想定していない．なぜなら，IC カードごとなくせば，すぐ紛失に気づくからである．

4.2 証拠データの生成

図 2 に示すように，主体として消費者 A と販売者 B の二人がいて，何らかのデータ X(契約書等) に A の秘密鍵 S_A で電子署名を施したものを B へ送信する場合を考える．このとき，消費者 A は署名データに加えて，IC カード固有の鍵 K とデータ X を使って生成した認証子 $MAC_K(X)$ を販売者 B に送る．この認証子は以下のような性質を持っている．

- 鍵漏洩に対する安全性は極めて強い．
- 参照するのは紛争の時のみで，頻繁には参照されない．

（図で使用している記号の意味）

P_A：A の公開鍵
S_A：A の秘密鍵 (耐タンパーレベル 2 以下の領域に格納されている)
K：秘密のパラメータ (鍵) (耐タンパーレベル 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
$MAC_K(X)$：K を使って生成したデータ X の認証子

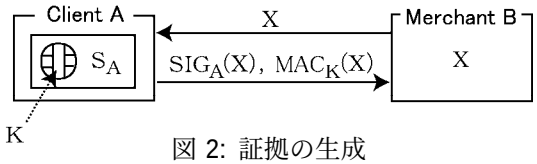

図 2: 証拠の生成

販売者 B は，A の公開鍵 P_A で $SIG_A(X)$ を復号し，確かに通信相手が A であることと通信データが改ざんされていないことを確認する．ここで，$MAC_K(X)$ は検証する必要はない．(仮に検証しようとしても，K は消費者 A の持っている IC カード固有の秘密パラメータであり，絶対に取り出すことはできないので，販売者 B は検証できない)．$MAC_K(X)$ は A から「$SIG_A(X)$ など身に覚えがない」と異議を申し立てられた時に使用する証拠データである．

4.3 ログの生成

$SIG_A(X)$ と $MAC_K(X)$ を受け取った販売者 B は，トラブル時に備えてこれらを安全なログに保管する．ここで B がログの保管を怠ると，後でトラブルが生じたときに自分が損をするだけなので，ログは確実に残される．

5 提案するシステムの評価

5.1 第三者による攻撃

第三者による攻撃として，例えば攻撃者 C が A の秘密鍵 S_A の搾取に成功し，それを自分の IC カードに格納することができたとしよう (図 3 参照)．そうすると，C は偽の電子署名 $SIG_A(X)$ を作成することが可能になるので，A になりすますことができる．しかし，C は A が持っている IC カードの秘密のパラメータ K は知ることができないので，$MAC_K(X)$ までは作成することができない．よって，例えば C が持っている正当な IC カードを使って $MAC_K(X)$ を送り，契約を成立させたとする．その後，A の元へ身に覚えのない請求書が届き，A は自分の秘密鍵 S_A が搾取されたことに気づいたとする．そこで A は,「この契約は鍵を盗んだ第三者により行われたものである」と主張し，契約の取り消しを B に求める．このとき，A が持っている IC カードでは，X に対して暗号化して得られるデータとしては $MAC_K(X)$ はあり得ないということが証明できれば，契約は破棄され，A に損害は生じない．

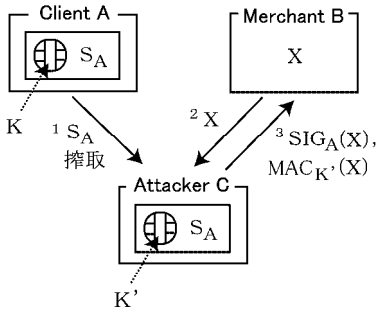

図 3: 第三者の攻撃

具体的には，消費者 A は自分の IC カードを，販売者 B はログに保管してある $SIG_A(X)$ と $MAC_K(X)$ を調停者に提出し，実際にデータ X を使って実演してみて，出力が $MAC_K(X)$ と異なるならば契約は破棄される．

5.2 Client A による不正

消費者 A による不正として，例えば A が別の消費者 D と結託する場合を考える．そこで仮に A が自分の IC カードから秘密鍵 S_A の搾取に成功したとする (図 4 参照)．そして A は S_A を D に渡し，D の IC カードに S_A を格納できたとする．そうすると，D は自分の IC カードで $SIG_A(X)$ を作成することが可能になるので，A になりすますことができる．以下 **5.1** 節同様の方法で不正を行う．そして A は,「この契約は鍵を盗んだ第三者により行われたものである」と主張し，自分の持っているカードを調停者に提出すれば，初犯のときは **5.1** 節の攻撃と区別がつかないので，攻撃が成立する．

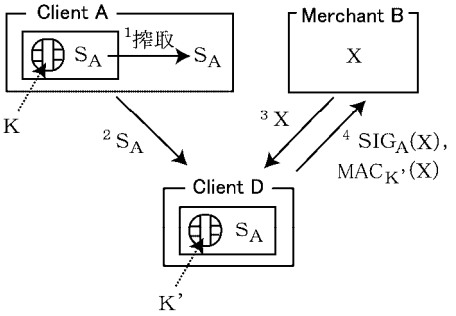

図 4: 消費者の結託攻撃

攻撃後，すぐに S_A は廃棄され，新しい鍵が A に発行される．

一般に悪いことをする人は，一回成功すれば味を占めて何回も同じ悪さをすることが予想される．そこで,「一定期間に何回も鍵を更新するときは，サービス提供を一時停止する」といったようなセキュリティポリシーを，鍵の更新状況を把握している機関が作成しておけば，複数回この攻撃を受けることはない．

5.3 考察

本システムは消費者保護を第一の目的としている．よって，**5.1**，**5.2** 節で述べた攻撃をされて損をするのは，請求書を送っても，その代金を回収できないカード会社である．この損失については，カード会社が保険等に加入することにより補てんするしかないだろう．また，$MAC_K(X)$ から不正者を追跡することが可能になれば，**5.1**，**5.2** 節で述べた攻撃も抑制することができると考えられる．

6 電子マネーへの応用

ここまでは，決済のタイミングが後払いである，クレジット型電子決済を想定し説明してきた．本章では，決済のタイミングが即時払いの C/S 型アプリケーションとして電子マネーを取り上げ，我々が提案する方式を用いることでどのようなご利益があるか考察を行う．

6.1 NTT 電子マネー

既存の電子マネーはその形態により様々な方式が考案されているが，ここではより現実のお金に近い形態であり PKI をベースにしている，NTT 電子マネー方式 (1996 年 9 月発表) を例に説明する [7]. 電子マネーは不正コピーを防止するため，IC カード等の耐タンパー性をもつ機器の，耐タンパーレベル 2-4(**3** 章参照) の部分に格納されている．よって，もし仮に電子マネー用の秘密鍵が漏洩すると，IC カードに格納されている電子マネーを悪用される危険性がある．そこで，電子マネー支払いプロトコルにおいて，我々が提案する方式を組み込むことにより，支払者 A は支払者署名に加えて，IC カード固有の鍵 K とチャレンジデータ X を使って生成した認証子 $MAC_K(X)$ を受領者 B に送る．$SIG_A(X)$ と $MAC_K(X)$ を受け取った B は，トラブル時に備えてこれらを安全なログに保管する．

6.2 不正者による攻撃とその安全性評価

電子マネーシステムにおいて不正を行うには，正規ユーザーの秘密鍵を搾取することに加えて，電子マネーデータも搾取する必要がある．よってその分 **5.1**，**5.2** 節の攻撃よりも，不正を行うのにコストがかかる．もし仮に，第三者が正規ユーザーの秘密鍵と電子マネーの搾取に成功したとしても，正規ユーザーが持っている IC カードの秘密パラメータ K は知ることができないので，$MAC_K(X)$ までは作成することができない．よって，正規ユーザーが自分の電子マネーを誰かに使われてしまったことに気づいた時点で,「この契約は鍵と電子マネーを盗んだ第三者により行われたものである」と主張し，契約の取り消しを販売店に求めれば，契約は破棄され，正規ユーザーに損害は生じない．

6.3 考察

電子マネーの場合，不正者に攻撃されて損をするのは，商品を不正者に送ってしまい，その代金を回収することができない販売店である．この損失については **5.3** 節同様，販売店が保険等に加入することにより補てんするしかないだろう．また，電子紙幣型電子マネーの場合，オンラインで電子マネーの二重使用をこまめにチェックすれば，クレジット型電子決済よりも早期に秘密鍵搾取に気づくことができる．さらに，現在考えられている電子マネーシステムでは，格納できる電子マネーの金額には上限が定められているので，大金を IC カードに格納していることは考えにくい．よって，消費者が膨大な金額の損失を被ることはないものと思われる．

7 制度面からの展望

本稿で提案するシステムを構築することにより，消費者が被る損失を保護することはできる．しかし，もし仮に取引金額が小さく，時間的余裕もなく，言葉の壁等がある場合，わざわざ法廷でトラブ

ルを処理しようと考えるだろうか．時間的にもコスト的にも，とても現実的な解とは言い難い．そこで，裁判というプロセスを経ることなく，消費者取引に関する紛争を解決するメカニズムとして，近年ADR(Alternative Dispute Resolution) が注目されている [8]．ADR は，いわゆる裁判による紛争処理と比較して，以下のような利点がある．

- 低コストで迅速な解決が可能
- 対立的でなく相互の合意に基づく解決が可能
- プロセスを対外的に開示しないので，個人情報の保護が可能
- 法律のみならず，様々な状況を反映した解決が可能
- 法律家のみならず，当該分野に関する専門家の参画が可能
- 国際的なルールを設定することにより，国境をまたぐトラブルについても適切な処理が可能

しかし，適切な ADR メカニズムを構築するためには，以下の課題をクリアする必要がある．

- 消費者にとってのアクセスの容易性
- 低廉なコストと迅速な解決
- ADR 実施機関の独立性と判断の中立性
- 公正性及び調停・仲裁人の能力
- 訴訟プロセスとの関係

よって，上記の条件を満たす ADR メカニズムの構築を実現するため，ADR 基本法を制定することも視野に入れた，法律・制度面の整備が必要である．

8　おわりに

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．よって本稿では，PKI に基づく C/S 型アプリケーションにおいて，消費者の秘密鍵が搾取された場合の消費者保護について，技術と制度の両面から考察を行ってきた．

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，消費者が損失を被る可能性がある．電子商取引における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証拠インフラなるものを構築する必要があるのではないだろうか．

参考文献

[1] 山口 英, 鈴木裕信: 情報セキュリティ, 共立出版, pp.245-254, Sep. 2000.

[2] R. Housley, et al.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC2459, Jan. 1999.

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

[4] 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.)

[5] SETCo: SET Secure Electronic Transaction Specification Book1: Business Description, May. 1997. http://www.setco.org/

[6] ECOM IC カード WG: IC カード利用ガイドライン (1.0 版), Mar. 1998.

[7] 松本隆明, 岡本龍明: 情報セキュリティ技術, オーム社, Aug. 2000.

[8] OECD: The Guidelines for Consumer Protection in the Context of Electronic Commerce, Dec. 1999.
http://www.oecd.org/dsti/sti/it/consumer/prod/guidelines.htm