管理者に対しても秘匿性を持つユーザ評価システムの実装

中田　博之†　　中西　透†　　渡邊　寛†　　舩曳　信生†

†岡山大学大学院自然科学研究科
700-8539 岡山県岡山市北区津島中 3-1-1
nakada@sec.cne.okayama-u.ac.jp, {nakanisi, can, funabiki}@cne.okayama-u.ac.jp

あらまし　本研究グループでは，管理者に対しても秘匿性を持つユーザ評価システムを提案している．このシステムでは，各ユーザ自身が評価点を証明書として保持することで管理者に対して評価点を秘匿することができる．しかし現状，本システムは Web システムへの実装がなされておらず，実用性に関する評価が行われていない．そこで本研究では，プロキシを用いた Web システムを実装し，各プロトコルの処理時間を測定した．各プロトコルとも 0.3 秒程度で動作しており，実用的な時間であることを確認した．

An Implementation of Reputation System with Secrecy Even for Administrators

Hiroyuki Nakada†　　Toru Nakanishi†　　Kan Watanabe†　　Nobuo Funabiki†

†Graduate School of Natural Science and Technology, Okayama Univercity
3–1–1 Tsushima-naka, Kitaku, Okayama, 700-8530, Japan
nakada@sec.cne.okayama-u.ac.jp, {nakanisi, can, funabiki}@cne.okayama-u.ac.jp

Abstract　Our research group has proposed a reputation system with the secrecy even for administrators. In this system, each user keeps his/her reputation point in the certificate, and thus can keep it secret even from the administrators. However, any concrete Web system has not been implemented and evaluated in terms of practicality. In this study, we implemented the Web system using proxies and measured the processing time of each protocol. The results show that each protocol works in about 0.3 seconds, which is practical.

1　はじめに

現在，インターネットオークションなどのユーザ間サービスが盛んに利用されている．ユーザ間サービスでは，プライバシーを保護するためにユーザ同士を互いに匿名にしたいという要望がある．しかし，ユーザを完全に匿名にすると，悪意のあるユーザが不正行為を行った場合に，どのユーザが不正行為を行ったかが分からず，不正行為に悩まされ続けることになる．

その対策として，ユーザ間で互いに評価し合い，各ユーザが信頼できるかどうかを判断できるようにする評価システムが利用されている．その際，現在利用されているシステムでは，管理者は各ユーザの評価点をデータベースで管理するため，各ユーザ間サービスのユーザ ID を知る必要がある．こうして，ユーザの個人を特定できる情報が渡ってしまうため，管理者はユーザのサービス利用履歴を知り得てしまう．

これらの問題を解決するため，匿名証明書を用いてユーザ側で評価点を管理することにより，管理者に対して強固な秘匿性を持つ評価システ

ム [1] が提案されている．この評価システムでは，各ユーザは自身の評価点を証明書として保持する．この証明書は管理者にしか作成できないため，偽造不能性が満たされる．評価点の更新では，ユーザは保持している証明書，現在の評価点，更新後の評価点をそれぞれ暗号化して管理者に対して送信し，管理者はゼロ知識証明を用いてそれらの正当性を確認する．そして，管理者は暗号化されたまま評価点が加算された証明書を生成してユーザに送信する．ここで，ユーザが送信する各データは暗号化されており，かつゼロ知識証明によってその正当性を示すため，管理者に対しても秘匿性が満たされる．しかしながら、このシステムは Web システムにおいて実装・評価されていない．

そこで本研究では，本評価システムを Web システムに導入するために，プロキシを用いた実装を行う．本システムには評価点の更新・公開のプロトコルがあり，本研究ではそれらの実装を行った．本システムは取引を行うユーザの他に取引を管理する取引サーバ，評価点の更新を行う評価サーバが参加する．評価点更新プロトコルでは，取引サーバと評価サーバとで処理が分かれており，取引サーバではデータベースを用いた取引情報の管理と，ユーザが評価サーバに取引の正当性を証明するための取引証明書の発行を行う．また，評価サーバでは，証明書更新処理を行う．評価点公開プロトコルではユーザ，取引サーバ間のみで通信が行われ，出品登録の際に評価点の範囲を示す情報の登録を行う．

本実装においては，本研究グループで開発しているプロキシを用いた匿名認証システム [2] を利用する．このシステムでは，ユーザとサーバの双方に匿名認証システムを実装したプロキシを配置し，認証に必要な手続きはすべてプロキシが行うことで，現行のブラウザや Web サーバをそのまま利用することを可能とする．

実装したシステムの評価として，評価点更新プロトコル，評価点公開プロトコルともに，ユーザによるリンクアクセスからブラウザに完了ページが表示されるまでの処理時間を測定した．その結果，評価点更新には平均約 0.36 秒，評価点公開には平均約 0.34 秒という結果が得られ，秘匿性を持つ本ユーザ評価システムが実用的であることが確認された．

最後に，本論文の章構成について述べる．まず，2 章で本評価システムのモデルと安全性の定義，各プロトコルについて述べ，3 章で Web システムおよび各プロトコルを実装するための設計と実装方法を述べる．そして 4 章で評価実験の結果と評価を行い，最後に 5 章で本論文をまとめる．

2 既存技術

2.1 管理者に対しても秘匿性を持つユーザ評価システム

本章では，[1] で提案されている管理者に対しても秘匿性を持つユーザ評価システムの概要と，満たすべき安全性の定義，本研究で実装する評価点更新プロトコル，評価点公開プロトコルの概要，実装において利用する技術について述べる．

2.1.1 システムの概要

図 1 に示すように，この評価システムでは，評価者，被評価者の 2 人のユーザに加えて，システムの管理者として評価サーバと取引サーバが参加する．2 人のユーザは，評価サーバ・取引サーバを通じて評価を行う．評価サーバは，ユーザ間の評価点の更新処理を保証する．この保証のために，ユーザの総評価点が加点される度に証明書を発行する．取引サーバは，取引を行うサービスを提供しているサーバを想定しており，ユーザ間の取引の正当性を保証する．これらのサーバは評価点の改ざんなどの不正を行わないと仮定する．このとき，評価システムにおける各手続きを以下のように定義する．

鍵生成: 評価サーバにおけるアルゴリズムであり，評価サーバの公開鍵と秘密鍵，そして評価点公開プロトコルで必要となる補助公開情報を生成する．

証明書の発行: ユーザ･評価サーバ間のプロトコルであり，評価サーバは自身の公開鍵と秘

密鍵を用いて 0 点の証明書を生成し，ユーザに対して発行する．

評価点の更新: 評価者・被評価者・評価サーバ・取引サーバ間のプロトコルであり，被評価者は評価サーバと通信を行い，自身の証明書を更新することで評価点の更新を行う．

評価点の公開: 被評価者・取引サーバ間のプロトコルであり，被評価者は取引サーバに対して，具体的な評価点の値を知られないように自身の所持する評価点の属する範囲のみを公開する．

2.1.2 安全性の定義

評価システムが満たす安全性は以下の通りである．

偽造不能性: 各ユーザは，保持している自身の評価点を改ざんすることができない．

秘匿性: ユーザ本人以外は，管理者さえもユーザの評価点を知ることができない．

匿名性: 管理者がユーザの評価点を加点する場合や自身の評価点を公開する場合など，取引からユーザを特定することができない．

リンク不能性: ユーザ本人以外は，各取引のユーザが同一かどうかを特定できない．

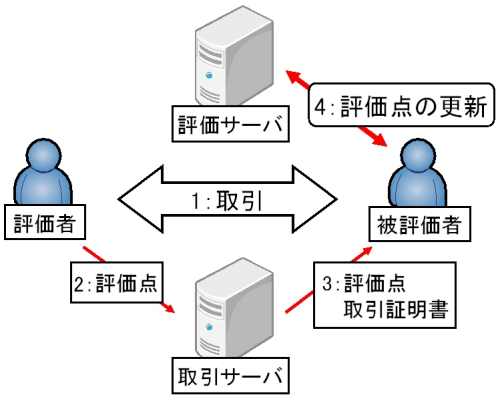

図 1: 管理者に対しても秘匿性を持つ評価システムの概要

2.2 実装対象のプロトコル

本研究では，[1] の評価システムのうち評価点更新プロトコル，評価点公開プロトコルの実装を行う．

2.2.1 評価点更新プロトコル

評価者・被評価者の間で取引が行われた後，このプロトコルにより被評価者は評価点の更新を以下のように行う．

1. 取引サーバは行われた取引に対し取引番号を与える．
2. 評価者は取引サーバに評価点を送信する．
3. 取引サーバは被評価者に評価点と取引の正当性を示す取引証明書を送信する．
4. 被評価者は取引証明書と現在所持している評価点の証明書，更新後の評価点を暗号化して評価サーバに送信する．
5. 認証に成功すれば評価サーバは新しい評価点の証明書を被評価者に送信する．

これにより評価点証明書の更新が完了し，ユーザは更新された証明書を新たに所持する．

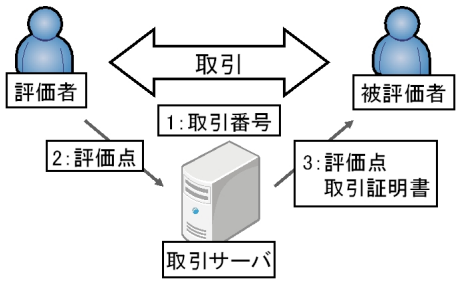

図 2: 評価点更新プロトコル 1

2.2.2 評価点公開プロトコル

本研究で想定するオークションサービスでの出品登録を行う際に，このプロトコルにより，被評価者は所持している評価点の範囲情報を以下のように公開する．

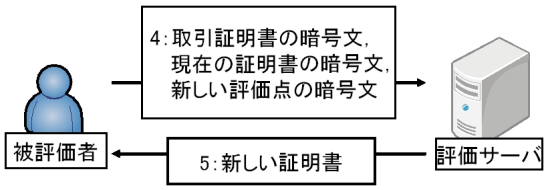

図 3: 評価点更新プロトコル 2

1. 被評価者は出品登録を行う際に，自身の所持する評価点の属する範囲を証明するデータを補助公開情報を用いて生成し取引サーバに送信する．
2. 取引サーバは証明データが正しいものであると判断できれば，受け取った情報を公開情報として登録する．

これにより取引を行うユーザは出品ユーザの評価点の範囲を知ることができる．

2.3 プロキシを用いた匿名認証システム

本研究グループでは，プロキシを用いた匿名認証システム [2] を提案している．このシステムの概要を図 4 に示す．このシステムでは，クライアント PC とサーバ PC の双方に，匿名認証システムを実装したプロキシを配置する．既存の Web システムを変更することなく，匿名認証を導入するために，認証に必要なすべての手続きをプロキシ間のみで行う．この 2 つのプロキシ間の通信では，TLS によるサーバ認証と暗号化を利用する．この暗号通信路を使って，独自の匿名認証プロトコルによるクライアント認証を行い，その後，HTTP のリクエストとレスポンスの転送を行う．

3 ユーザ評価システムの Web 実装

本研究では，ユーザ評価システムを実装するにあたり，オークションサービスでのユーザ評価を想定し，商品の出品登録時および取引終了以降のユーザ評価処理を Web システムとして実装した．出品登録では，出品に関する情報に加

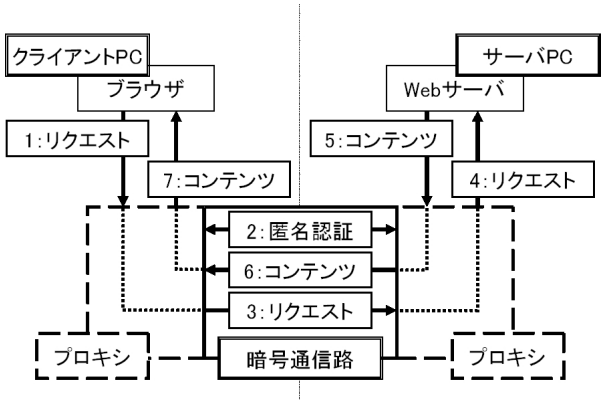

図 4: プロキシを用いた匿名認証システム

えて，評価点公開プロトコルを用いてユーザの所持する評価点の範囲が登録される．また，ユーザ評価処理では評価点更新プロトコルを用いて，ユーザの評価点とその証明書が更新される．

3.1 設計

3.1.1 Web システム

以下に，実装した出品登録処理およびユーザ評価処理を示す．

出品登録処理 被評価者は以下のように取引サーバに対して出品登録を行う．

1. 被評価者は取引サーバにアクセスし，表示された Web ページのフォームに出品情報を入力する．入力した情報の送信と同時に評価点公開プロトコルを実行し出品情報の登録を行う．
2. 取引サーバでは、取引 ID と出品者である被評価者，評価者となる落札者専用のパスワードをそれぞれ作成し，出品情報とともにデータベースに保存する．

ユーザ評価処理 被評価者は以下のように評価サーバとの間で評価点の更新を行う．

1. 取引サーバは両ユーザに取引 ID と専用のパスワードを送信する．
2. 評価者は送られてきた ID とパスワードを用いて評価点を取引サーバに送信する．

3. 認証に成功した場合，取引サーバは評価点をデータベースに保存する．

4. 被評価者は ID とパスワードを用いて取引サーバに評価点受け取りの申請を行う．

5. 認証に成功した後，取引サーバは取引証明書と評価点を被評価者に送信する．ここで，取引証明書とは被評価者が証明書の更新を行う際に取引の正当性を証明するための署名であり，RSA 暗号を用いて作成される．

6. 被評価者は取引サーバより送信された取引証明書と評価点をダウンロードする．この際，ブラウザには認証成功時のページを表示し，そのページに評価サーバによる評価点更新のためのリンクを載せておく．

7. 被評価者は評価点更新ページにアクセスし，ここで評価点更新プロトコルが実行され，評価点の更新が行われる．

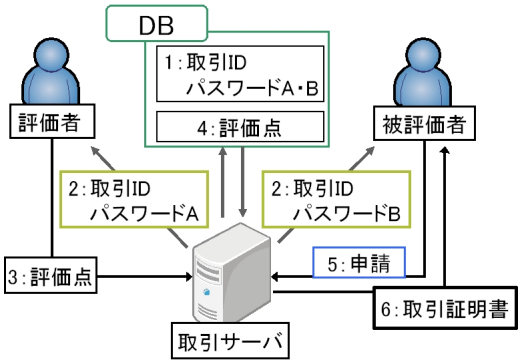

図 5: 評価点更新プロトコルの取引サーバにおける処理

3.1.2 評価点更新プロトコル

3.1.1 節のユーザ評価処理のステップ 7 における評価点更新プロトコルを図 6 に示す．その詳細は以下の通りである．

1. ClientStart メッセージにより，被評価者は評価サーバに対して認証要求を行う．その際，取引証明書を送信する．

2. 評価サーバは取引サーバの公開鍵を用いて送られてきた取引証明書の検証を行う．

3. ServerStart メッセージにより，評価サーバは被評価者に認証データ作成に必要な乱数を送信する．

4. 被評価者は受け取った乱数を元に，評価サーバの公開鍵・評価点・現在の証明書である自身の秘密鍵を用いて認証データとなる署名を作成する．

5. Signature メッセージにより，被評価者は評価サーバに署名を送信する．

6. 評価サーバは送られてきた署名の検証を行い，正当であれば署名と評価サーバの公開鍵・秘密鍵を用いて評価点の更新された新しい証明書を作成する．

7. Certificate メッセージにより，評価サーバは作成した新しい証明書を送信する．

8. 被評価者は送られてきた新しい証明書の検証を行い，正当であればその証明書を出力する．

9. Finish メッセージを相互に送信して，認証が正しく終了したことを確認する．

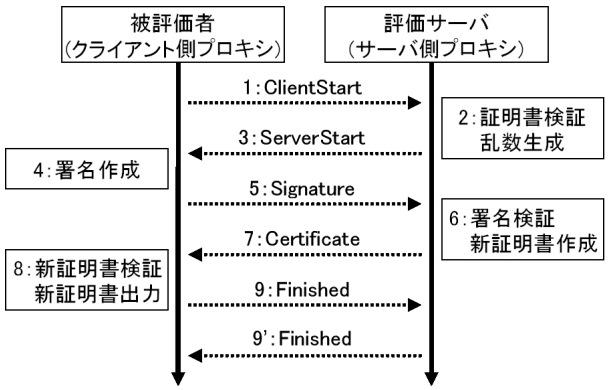

図 6: 評価点更新プロトコル

3.1.3 評価点公開プロトコル

3.1.1 節の出品登録処理のステップ 1 における評価点公開プロトコルを図 7 に示す．プロトコ

ルの流れは評価点更新プロトコルとほぼ同様であるが，証明書の作成・検証がなく，検証を通った後に公開情報をデータベースに保存する．

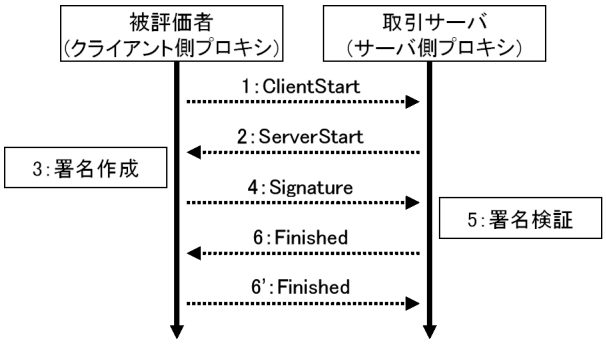

図 7: 評価点公開プロトコル

3.2 実装方法

3.2.1 Web システム

取引サーバ部における Web システムの実装について述べる．取引 ID・パスワードの生成には JavaScript を利用し，MySQL を用いてデータベースに保存した．また，MySQL との接続には JDBC ドライバを用いるため，JDBC ドライバ API のインターフェイスを実装した．取引証明書の生成については RSA 署名を利用して Java により実装した．

3.2.2 評価点更新・公開プロトコル

これらのプロトコルは，2.3 節のプロキシを用いた匿名認証システムと同様にプロキシを用いて実装した．各プロトコル中で行う暗号処理ではペアリングライブラリを用いている．このライブラリの開発には C 言語を用いており，多倍長演算ライブラリに GMP を用いた Tate ペアリングライブラリ [3] を使用している．これに対して，プロキシは標準のライブラリとして多くのネットワーク API を持つ Java で実装した．そのため，プロトコル中で暗号処理を行う際のライブラリの呼び出しには JNI(Java Native Interface) を利用した．

4 実験と評価

4.1 実験方法

実装した Web システムにおける各プロトコルの実用性を評価するために，ユーザによる各サーバへのリンクアクセスから処理が終了し完了ページがブラウザに表示されるまでの時間を測定した．また，ブラウザに依存しないプロキシの呼び出しから処理終了までの時間，プロキシ内での評価点更新処理，公開情報生成・検証のみに要する時間についても測定した．

4.2 実験環境

クライアント PC と取引サーバ PC・評価サーバ PC の計 3 台を準備し，学内 LAN 環境に接続した．クライアント PC の CPU は Core 2 Duo (2.53GHz)，メモリは 2.9GByte であり，取引サーバ PC の CPU は Core 2 Quad (2.83GHz)，メモリは 3.2GByte，評価サーバ PC の CPU は Core 2 Duo (2.66GHz)，メモリは 3.25GByte である．また，取引サーバ PC・評価サーバ PC はそれぞれ有線 LAN で接続されており，速度は 100Mbps である．クライアント PC は無線 LAN(802.11n) で接続されており，速度は 300Mbps である．

4.3 実験結果と評価

測定結果として 10 回の試行での平均時間を算出した．算出した平均値を以下の表 1 に示す．

表 1: 実験結果 (平均時間 単位:秒)

	評価点更新	評価点公開
全処理	0.36	0.34
プロキシ処理	0.29	0.28
内部処理	0.19	0.17

実験結果より本実験環境では全体の処理時間が評価点更新プロトコルで平均 0.36 秒，評価点公開プロトコルで平均 0.34 秒と十分に実用的な

時間で動作することが確認できた．また，プロキシの処理のみの時間，各プロトコルにおけるプロキシ内部の処理も極めて短い時間で動作することが確認でき，本評価システムの実用性が示せた．

5　むすび

本研究では，管理者に対しても秘匿性を持つユーザ評価システムを，オークションサービスを想定してWebシステムとして実装した．実装したシステムでは，出品登録時に評価点公開プロトコルを，ユーザ評価処理時に評価点更新プロトコルを行う．そして，それぞれのプロトコルの処理時間を測定することにより評価を行った．実験の結果，平均してそれぞれ0.36秒，0.34秒と実用的な時間で動作することが確認できた．

今後の課題としては，今回実装したシステムでは考慮していないネガティブな評価点への対処や，本評価システムのスマートフォンにおける実装などが考えられる．

参考文献

[1] 野村智也，中西透，舩曳信生，“管理者に対して強固な秘匿性を持つ評価システムの提案”，情報セキュリティ研究会 (ISEC)，pp.15-20，2011-12.

[2] 大林弘樹，中西透，舩曳信生，“Webサービスにおけるプロキシを用いた匿名認証システムの実装”，コンピュータセキュリティシンポジウム (CSS)，pp.163-168，2008-10.

[3] M.Akane, Y.Nogami, and Y.Morikawa, “Fast Ate pairing computation of enbedding degree 12 using subfield-twisted eliptic curve”, IEICE Trans. Fundamentals, Vol. E92-A, No.2, pp.508-516, 2009.