WWWのユーザ主導個人情報管理システム

佐々木 一教 † 藤田 茂 ‡ 菅原 研次 §

千葉工業大学大学院工学研究科情報工学専攻 † 千葉工業大学情報科学部情報工学科 ‡
千葉工業大学情報科学部情報ネットワーク学科 §

1. はじめに

WWW を利用する上で個人情報管理の重要性は増すばかりである．商用サイトなど，あらゆるサイトで個人情報の収集が行われている．不用意な個人情報の提供は，必要以上の個人情報の漏洩，ユーザの追跡や複数サイトの結託による個人情報の漏洩などの問題をはらんでいる．この問題に対して，本城らは以下のような機能を持つシステムを提案している [1].

- ユーザ追跡不可能な認証・アクセス制御機構
- ユーザ合意による個人情報公開
- 信頼性のある個人属性によるアクセス制御

しかし，[1] のシステムではチケットの発行に公開鍵暗号方式が多用され，システム全体の処理速度が遅いという課題が残されている．本研究では，[1] のシステムにおいて RS/TGS と WWW サーバが SSL で結ばれた形態であるシステムを提案し，共通鍵暗号方式を主に用いることによりシステム全体の処理速度の向上を目指す.

2. チケット処理とシステムの処理速度

[1] のシステムでは，チケットの発行時に公開鍵暗号方式の署名と暗号を実施し，チケットの検証時には公開鍵暗号方式の復号と署名の検証を行うのでシステムの処理速度が低下する．さらに，一般にクライアントが WWW サーバにアクセスするときには，短時間の内にその WWW サーバ内の複数のページにアクセスするものであるが，チケットの検証の度に公開鍵暗号方式の復号と署名の検証を実行しなくてはならず，これもまた処理速度の低下を招く．[1] において，短時間の内に何度もアクセスする場合には，チケットの検証結果をキャッシュしておくという手法が挙げられている．この手法は安全性を損なうので，キャッシュしておく時間を数秒程度の短い時間に限る必要がある [1]．また，クライアントが同一の WWW サーバにアクセスする際でも，サービスごとに要求される個人情報が違えば，漏洩する個人情報を最小限にするためにチケットを再生成しなければならない．以上のことから，チケットの署名，暗号化，復号，検証をより効率よく処理する方法が求められる．

チケットが常に RS/TGS で生成され，ユーザを通して WWW サーバに渡されることを前提とし，処理速度を向上させるためには，公開鍵暗号方式による署名，暗号化，復号，検証を，共通鍵暗号化方式によって実現する手法がある．この実現のために，RS/TGS と WWW サーバを SSL によって結び，チケットを暗号化するのに用いた共通鍵を RS/TGS から WWW サーバに通知する．これにより，チケットの公開鍵暗号方式による署名，暗号，復号，検証が，共通鍵暗号方式の暗号，復号によって代替でき，処理時間を短縮できる．

システムについては，3. で，チケットの構造については，4. で述べる．

3. 処理速度を向上するシステムの提案

提案するシステム図を図 1 に示す.

- RS/TGS：個人情報登録サーバ/チケット発行サーバ
- クライアント：ユーザが操作する WWW ブラウザおよびチケット処理ソフトウェア

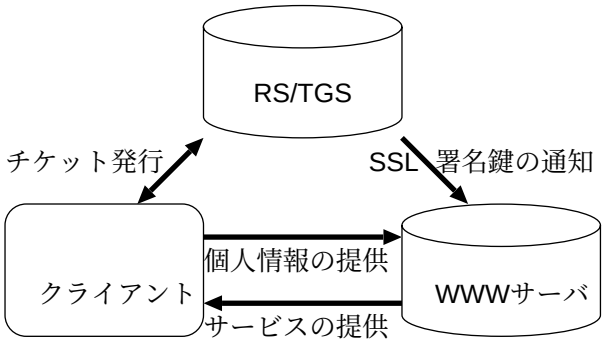

図 1: システム図

- WWW サーバ：ユーザの個人情報によりアクセス制御を行う

本システムと [1] との違いは，RS/TGS と WWW サーバが SSL によって結ばれるところにあり，RS/TGS がチケットを署名した鍵 K_c を WWW サーバに通知することで，チケットの署名に共通鍵暗号方式が使用でき，システム全体の処理速度が向上するという利点がある．

この署名は「否認防止」は保証しないが，RS/TGS から WWW サーバに通知される共通鍵 K_c によって，WWW サーバにとってはその署名された個人情報が RS/TGS から発行されたものであり，信頼できることが分かれば十分であると考えられる．ただしそのためには，RS/TGS と WWW サーバ間の SSL は相互認証をしている必要がある．

4. 提案システムのプロトコル

プロトコル処理の流れを図 2 に示す.

4.1 チケット

チケットの構造は以下のようになる．

[1] のシステム	$P_S(S_R(R, L_{Ticket}, PIs, K_{Ticket}, S))$
本システム	$E_c(R, L_{Ticket}, PIs, K_{Ticket}, S)$

ただし，
R：RS/TGS の情報
L_{ticket}：チケットの有効期間
PIs：個人情報
K_{Ticket}：チケットの保持証明に利用される鍵でクライアントも保持
S：WWW サーバの情報
$P_S(\cdot)$：WWW サーバ S の公開鍵による暗号化
$S_R(\cdot)$：RS/TGS R による署名
$E_c(\cdot)$：RS/TGS の共通鍵暗号方式による署名
である．

両者のチケットの違いは，[1] のチケットは 2 回の公開鍵暗号方式による署名，暗号化が行われているが，本システムのチケットでは 1 回の共通鍵暗号方式による署名のみであり，処理速度と負荷を改善できる．その署名に使われた鍵 K_c は SSL を通して，WWW サーバに渡され，この鍵は RS/TGS と WWW サーバしか知り得ないので，本システムのチケットは [1] のチケットと同様に機能する．

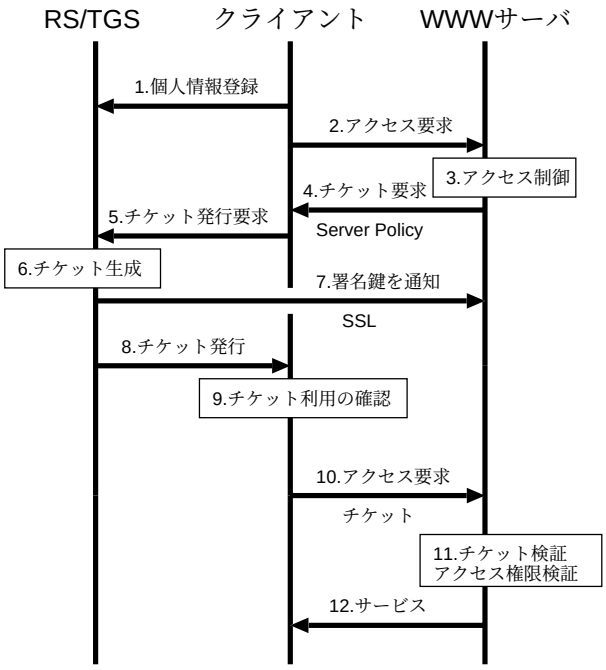

図 2: プロトコル処理の流れ

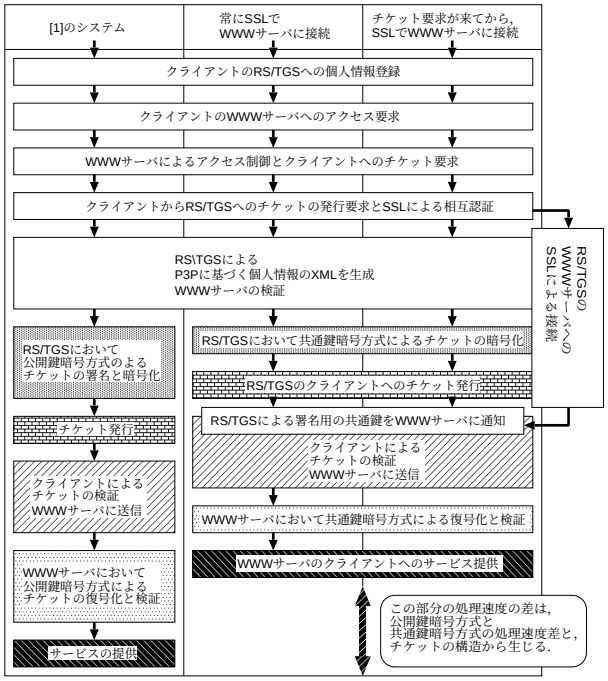

図 3: 処理時間の差

4.2 RS/TGS と WWW サーバ間の SSL

RS/TGS はクライアントからチケット発行要求を受ける際に，WWW サーバのサーバ情報も同時に得る．RS/TGS は WWW サーバに SSL でアクセスし，WWW サーバの最新の公開鍵によって検証する．クライアントだけでなく，RS/TGS も WWW サーバを検証することによって，安全性を向上させることができる．

SSL による RS/TGS と WWW サーバ間の相互認証が終了した後に，RS/TGS は WWW サーバにチケットの署名で用いた鍵 K_c を SSL を通して渡す．

4.3 チケット検証

WWW サーバは RS/TGS により送られた鍵 K_c を管理し，クライアントがチケットを添付してサービスを要求してきたときに，そのチケットに対応する鍵 K_c を用いて署名の検証をする．WWW サーバは署名が確認できたときには，クライアントにサービスを提供する．

署名に使われる鍵 K_c は使い捨てである．RS/TGS はチケット発行の度に，異なる K_c を生成する．よって K_c を用いてユーザを追跡することは不可能である．WWW サーバは鍵 K_c を用いて，チケットの管理をすることができる．WWW サーバは，RS/TGS から鍵 K_c が送られてきてから一定期間経っても，それに対応したチケットが送られて来ない場合には，WWW サーバは K_c を破棄することで，チケットの有効期限を設定することができる．チケット自体は有効期間内であれば何度も使用できるが，WWW サーバがそのチケットに対応する鍵を破棄して，クライアントに対して新たにチケットの発行を求めることもできる．またユーザ側からすると，同一のチケットを複数回使用すると，WWW サーバにアクセス回数やアクセス時間などを蓄積されるので，アクセス毎に新たにチケットの発行を要求することも可能である．

5. 処理時間

システムの処理時間の差の見積りを図 3 に示す．図は，縦に時間軸をとる．図において，左から「 [1] のシステム」,「本システムにおいて，RS/TGS と WWW サーバが SSL で常時つながっている場合」,「本システムにおいて，RS/TGS にクライアントからチケット発行要求が来てから，WWW サーバに SSL で接続しようとする場合」となる．

図において，公開鍵暗号方式による処理時間は，共通鍵暗号方式による処理時間の 2 倍の長さをとって描写した．これは，最低でも公開鍵暗号方式と共通鍵暗号方式の処理速度が同じであったとしても， [1] のシステムでは，署名，暗号化 (復号化，検証) という 2 度の処理があり，本システムでは，署名 (検証) という 1 度の処理だけであるからである．これによって，本システムの方が処理時間を短縮できる．

SSL で新たに WWW サーバに接続する場合には RS/TGS は，チケットをクライアントに発行し，クライアントが WWW サーバにチケットを添付してアクセスするまでの間に，SSL によって WWW サーバに接続が完了し，署名に用いた共通鍵を通知している必要がある．また，一度接続が完了したら，すぐには切断せずに，図の真中にある「常に SSL で WWW サーバに接続」の場合に移行することになり，クライアントが何度も WWW サーバにアクセスする度にチケットを発行する際には，処理速度と負荷を改善できる．

6. おわりに

本研究では， [1] で提案されたユーザ追跡不可能な認証・アクセス制御，ユーザ主導の個人情報管理，信頼性を付与した個人情報といった機能を実現する個人情報管理システムにおいて，チケットの署名に共通鍵暗号方式を導入することを目的として，RS/TGS と WWW サーバ間を SSL で結んだシステムを提案した．システムを実装し，実機による評価実験を行っている．

本システムは，クライアントが何度も WWW サーバにアクセスする毎に，チケットを発行しなければならないときに，より効率良く処理することができる．

参考文献

[1] 本城信輔 洲崎誠一 斎藤司 三浦信治：プライバシに配慮した WWW における個人属性認証・アクセス制御システム，情報処理学会論文誌，Vol.43，No.8，pp2573-2586(2002)

[2] P3P：http://www.w3.org/P3P