2S-06　　Single Sign-On 技術を用いたモバイル通信における
暗号通信路確立のための一方式の検討

前川貴宏　松尾真一郎　橋川善之　坂本弘章　田村成美
株式会社　ＮＴＴデータ

１．はじめに

現在、携帯電話、PHS、ITS 等のモバイル通信を利用した広域の情報通信サービスが普及している。しかし、これらのサービスでは無線を利用するために通信相手との暗号通信を実現することが必要である。しかし、モバイル通信では通信帯域が小さく、また、移動中等、暗号通信路の確立のために必要な連続した時間が限られていることが多い。このような状況を踏まえ、連続した通信時間が限られているサービス利用時の通信コストをできるだけ減らしつつ、暗号通信路を確立する方法を提案する。

２．従来方式と問題点

暗号通信路の確立には認証と鍵共有処理が必要であるが、ある利用者が複数のサービスを利用する場合には、Single Sign-On (SSO) を利用することにより、これらの処理の回数を削減することが可能である。本稿では本技術を使用し、暗号通信路の確立を高速に実現するため、Kerberos[1]のスキームを改良した方式を提案する。

Kerberos のスキームを利用する際、以下の 2 つの問題点がある。

(1) 暗号通信路確立に要する時間に関する問題

Kerberos ではクライアント～サービス間で暗号通信路を確立するための処理は、事前認証のためのチケット発行とサービス利用の 2 つのフェーズからなっている。これらには各々2 パスの通信が必要であることから、モバイル通信のように連続した通信時間が限られるサービス環境では特に性能上大きな問題となる。

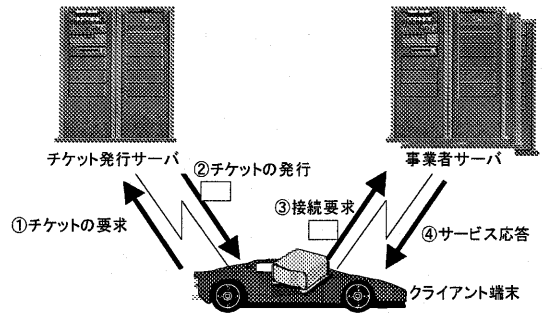

図1:Kerberosの処理内容

(2) チケット発行サーバの処理負荷に関する問題

Kerberos では、事前に共有している共通鍵暗号を用いてチケットを暗号化することにより、クライアント認証およびチケット発行時のクライアント～チケット発行サーバ間の暗号通信路を確立する。このため、クライアントの共通鍵の全てをチケット発行サーバで管理する必要がある。このために大規模なサービスではチケット発行サーバで管理すべき鍵の量が膨大になり、処理負荷が過大になる可能性がある。

３．提案方式

本研究では、サービス利用の都度発生するサービス利用時の通信コストは可能な限り削減する必要があるが、事前に処理が可能なチケット発行処理にはある程度の通信コストは許容でき

A Study of Efficient Secure Channel
Constructing Scheme for Wireless Network Services
Takahiro Maekawa, Shin'ichirou Matsuo, Yoshiyuki Hashikawa,
Hiroaki Sakamoto, Shigeyoshi Tamura
NTT DATA Corporation
1-21-2, Shinkawa, Chuou-ku, Tokyo 104-0033, Japan

ることを想定し、本方式では 2．で示した問題に対処するため、以下の改良を行う。

(1) 暗号通信路の確立に要する時間に関する問題

本方式では、Kerberos でサービス要求ごとに行っていたチケットの発行要求および発行の処理を事前に一括して行い、利用者側で必要なチケットを保持しておくことにより、本問題を解決する（図 2：①，②)。すなわち、サービスを利用する際は、一括して発行したチケットの中から該当するチケットを選択し、これを用いて事業者サーバに接続要求を行う（図 2：③，④)。これにより、サービス利用時にチケット発行サーバとの通信が不要となり、クライアント～サーバ間の暗号通信路確立のための通信時間が短縮可能である。

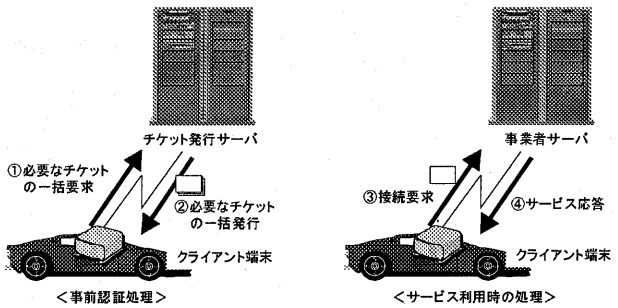

図2:チケット一括発行方式

(2) チケット発行サーバの処理負荷に関する問題

Kerberos では、2．で述べたように、クライアント認証およびクライアント～チケット発行サーバ間の暗号通信路の確立に共通鍵暗号を用いる。提案方式では、PKI(Public Key Infrastructure)を用い、チケット要求時にクライアントの公開鍵をチケット発行サーバに送付し、チケットをその公開鍵で暗号化することにより、正当なクライアントのみがチケットの復号が可能となる(図 3)。これにより、共通鍵を事前に共有することなく、暗号通信路の確立を実現することが可能となり、チケット発行サーバで管理すべき鍵の数を大幅に減らすことができる。上記の改良によりサービス利用時の通信の回数および処理時間は増加しない。

4．評価

Kerberos を直接適用する場合、暗号通信路の確立のための通信として毎回４パス必要であるが、本提案方式では、サービス利用時の通信は２パスで済み、サービス利用時の通信回数は半減する。また、利用者の共通鍵をチケット発行サーバで管理する必要がなくなり、チケット発行サーバでの処理負荷が軽減される。

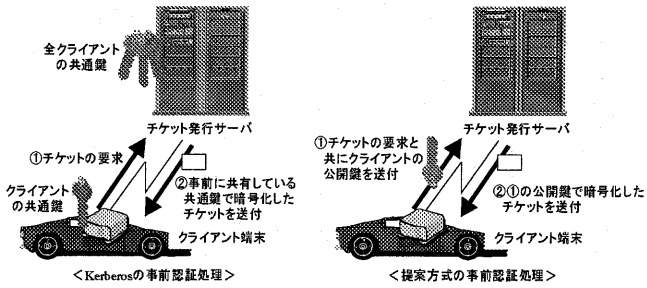

図3:公開鍵を用いた事前認証処理

5．おわりに

本稿では、広域の情報通信サービスにおけるモバイル通信に適した暗号通信路の確立を短時間で実現するため、Kerberos のスキームを用いた SSO 技術について、3．に示した 2 点について改良を行った。今後は、本方式に関し実装を行い、測定を行う予定である。

謝辞

本研究は、通信・放送機構 (TAO) の委託研究「走行支援システム実現のためのスマートゲートウェイ技術の研究開発」の一環として実施されています。この場をお借りしまして、御礼申し上げます。

参考文献

[1] The Kerberos Network Authentication Service (V5) RFC1510