分散システム環境における認証プロトコルの検討

5G－3

小畠　雅典　杉山　広幸　田辺　克弘
ＮＴＴヒューマンインタフェース研究所

1. はじめに

近年、クライアント・サーバ・システムに代表されるような、ネットワーク上のファイル、データベース等の資源の共有化や処理の分散化を実現する分散システム環境が一般化しつつあるが、それと同時にデータの盗聴、改ざん、ノードのなりすましといったセキュリティ上の問題が顕在化している。また、ネットワーク上で分散管理される資源の不正アクセスに対する保護対策の必要性についても叫ばれている。

我々は、このような問題を解決するために、共通鍵暗号方式を採用した認証システムの検討を行った[1]。さらに、相手に自己の権限を譲渡することにより自己の代理として資源へのアクセスを許可するような権限委任を本認証システムで実現するための方法について検討したので報告する。

2. 権限委任について

2.1. 権限委任の必要性

分散トランザクション処理のように、ネットワーク上で分散管理される資源への複雑なアクセス制御が要求される処理では、サービスを要求するユーザのアクセス権限に基づいた統一的なアクセス制御が必要である。例えば物理的に離れた場所にあるクライアントとプリンタサーバとファイルサーバがそれぞれ同一ネットワークで接続されているような環境において、クライアントがプリンタサーバに、クライアントユーザのアクセス権に基づき管理されるファイルサーバ上のファイルを印刷するようなサービスを要求した場合に、ファイルサーバは、アクセス要求をするプリンタサーバのアイデンティティに基づいたアクセス制御を行うため、本来クライアントユーザのアイデンティティにより管理されるべきファイルに対するアクセス制御ができないという問題があった。

この問題を解決するために、クライアントは、自己の権限をプリンタサーバに与え（つまりプリンタサーバがクライアントの仲介者となる）、プリンタサーバは、クライアントの権限を使用してファイルサーバにアクセスする。これによりファイルサーバは、クライアント本人の権限に基づいたアクセス制御が可能となる。このように、クライアント（イニシエータ）の仲介者的な行動をするプリンタサーバのようなプリンシパルをデリゲートといい、イニシエータが、自己の代理としてターゲットにサービス要求するためにデリゲートに権限を与えることを権限委任(Delegation)という。第１図に上記で説明した権限委任の概念を示す。また、このような権限委任機能を取り入れた認証システムとしては、DEC社のSPX[2]、MIT Athenaプロジェクトの Kerberos V5 [3]等がある。

2.2. 権限委任の実現

権限委任のレベルとしては、一般的に次の３つが知られている。[4][5]

(a) 単純委任（Simple delegation）

単純委任とは、デリゲートがイニシエータの権限のみによりターゲットにサービスを要求することである。

(b) トレース委任（Traced delegation）

トレース委任とは、デリゲートがイニシエータの権限と、デリゲート自身の権限により、ターゲットにサービスを要求することである。

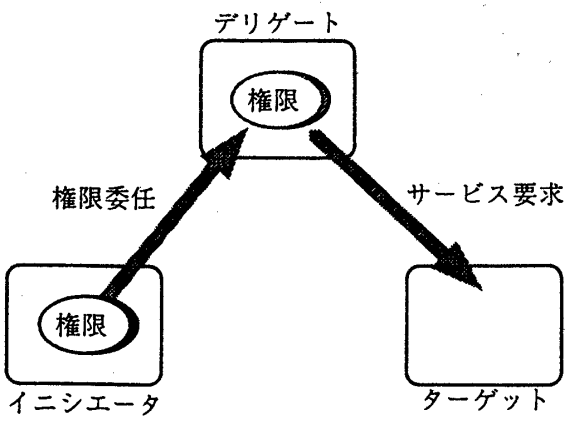

図１　権限委任の概念

A Study of Authentication Protocol for Distributed System .
Masanori OBATA, Hiroyuki SUGIYAMA, Katuhiro TANABE
NTT Human Interface Laboratories

(c) 制限委任（Restricted delegation）
制限委任とは、イニシエータがデリゲートに対して委任する自己の権限を制約することを許すことである。

今回、認証プロトコルに権限委任を実現するにあたり以下に示す点を考慮した。
◆対象とする認証プロトコルは、ISO/IEC9798-2[6]で提案されるＴＴＰ（Trusted Third Party）を用いた５パス認証方式とする。
◆委任機能を組み込むことにより認証プロトコル自体のシーケンスに大幅な変更を与えないこととする。
◆IETFから標準セキュリティインタフェースとして提案されているＧＳＳ-ＡＰＩ(Generic Security Service Application Program Interface) [7] に対応する。

3. 認証プロトコルへの権限委任の組み込み

図２に今回提案する権限委任を組み込んだ認証プロトコルを示す。委任方式は、前述の考慮点を最も満足できると考えられる単純委任方式とする。また、本認証プロトコルで提案する権限委任とは、イニシエータａとＴＴＰ間で共有する秘密鍵Katをデリゲートｂに与えることである。(1)～(5)は、ＴＴＰを介してイニシエータａとデリゲートｂとの間で相互認証し、秘密鍵Kabを共有するフェーズである。イニシエータａが、デリゲートｂに権限委任を要求する場合は、(4)でデリゲートｂの正当性の確認を行った後に、(5)で秘密鍵Katをメッセージ内に含んだ後、暗号化してデリゲートｂに送信することで、従来の認証方式でのシーケンスに何等変更も与えないで安全に権限委任を行うことが可能となる。さらに、権限委任されたデリゲートｂがターゲットｃにアクセス要求する場合は、(6)～(10)で示すように、自己の秘密鍵Kbtの代わりにイニシエータａから受け取った秘密鍵Katを用いることで、イニシエータａの代理として認証が行われ、ターゲットｃは、結果的にイニシエータａの権限に基づいたアクセス制御が実現できる。

4. おわりに

本稿では、ISO/IEC9798-2で提案されている認証プロトコルに対する権限委任の実現方法について提案した。また、今回提案した認証プロトコルをGSS-APIインタフェースに実装し、現在その評価を行っている。今後は、より厳密で、きめ細かなアクセス制御ができる制限委任の実現方式を検討していきたい。

参考文献

[1]杉山,小畠,田辺,"分散システムにおけるユーザ認証システムの実現",情報処理学会マルチメディア通信と分散処理 ,pp.85-90, July, 1995.
[2]Joseph J.Tardo, K.Alagappan, "SPX : Global Authentication Using Public Key Certificates", DEC, IEEE, 1991.
[3]J.Kohl, C.Neuman, "The Kerberos Network Authentication Service (V5)", RFC1510, Sep,1993.
[4]J.Pato, "EXTENDING THE DCE AUTHORIZATION MODEL TO SUPPORT PRACTICAL DELEGATION (Extended Summary)", OSF DCE RFC3.0, Jun, 1992.
[5]"Generic Security Service API (GSS-API) Security Attribute and Delegation Extensions", Snapshot, X/Open, 1994.
[6]ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication-Part2:Mechanisms using symmetric encipherment algorithms.
[7]J.Linn,"Generic Security Service Application Program Interface", RFC1508, Sep, 1993.

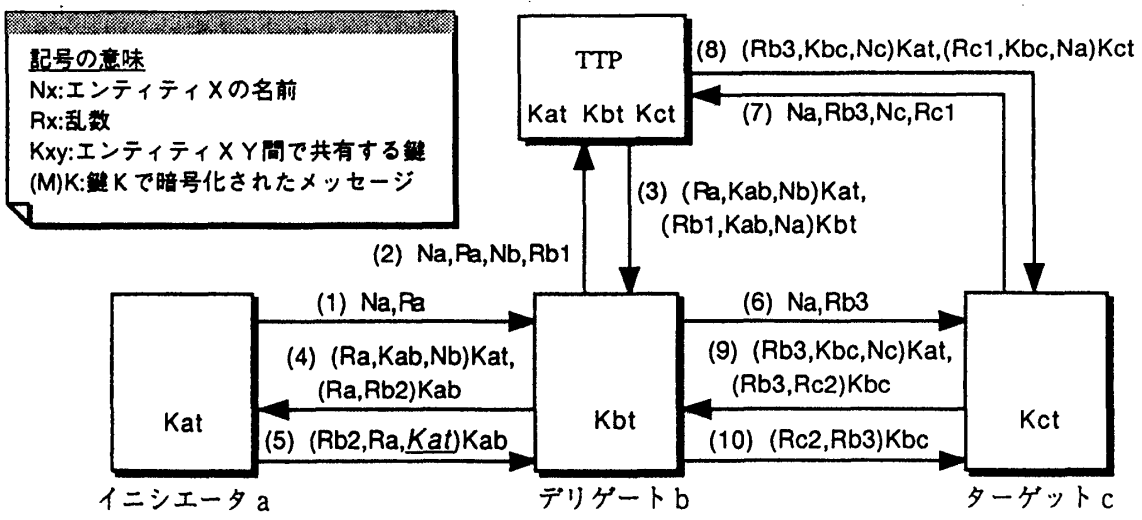

図２　権限委任を考慮した認証プロトコル　(Text field省略)