ディレクトリを利用した認証システム

3N−6

北角　智洋　　勝俣　雅司
ＮＴＴ情報通信網研究所

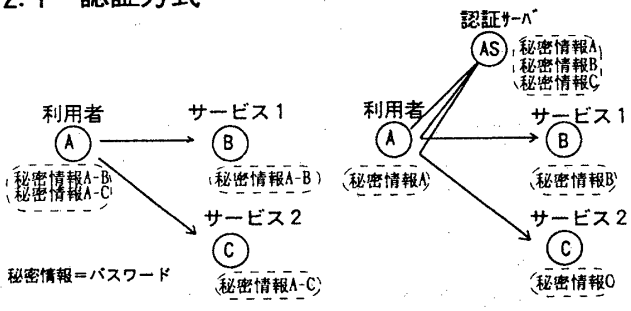
1　はじめに

ネットワークの大規模化／複雑化、通信による電子的な情報交換の普及に伴い、通信セキュリティの重要性がクローズアップされている。中でも、大きな課題の一つが、ネットワーク上のエンティティの認証をいかに行うかという問題である。従来、ネットワーク上のサービスは、独自に認証機構を構築してきた。今後のネットワーク環境の進展により、利用者がネットワーク上の資源（アプリケーション、情報）に自由にアクセスできるようになると、認証機構の統一、利用者情報の一元的管理が重要になってくる。

インターネット環境の認証システムとして開発されたKerberos[1]においては、認証情報の集中管理と秘密鍵暗号（慣用暗号）の利用によって、効率的かつ安全な認証を実現している。しかし、運用面や相互接続性に課題を残している他、きめ細かいアクセス制御を行うことができないといった欠点がある。筆者らは、公開鍵方式の暗号技術および国際標準に準拠したディレクトリを利用することでこれらの問題点を克服し、オープンなネットワーク環境での利用にも耐えうる認証システムを設計した。また、本認証システムを含むＯＳＩ環境のセキュリティ通信システムの試作を進めており、本報告ではその概要を示す。

2　認証システムの基本設計

2.1　認証方式



(a)パスワードによる認証方式　(b)Kerberosでの認証方式

図１　従来の認証方式

従来より用いられてきたパスワードによる認証方式では、利用するサービス毎にＩＤとパスワードを持つことになりかねず（図１の(a)参照）、ネットワーク上のサービスの多様化には対処しきれない。また、パスワードの盗用による不正なアクセスの危険性も大きい。

インターネット環境の認証システム、Kerberosでは、ネットワーク上に利用者認証を司るサーバを設置し、秘密鍵暗号を利用したプロトコルを用いることで、パスワード方式の弱点を解消している。利用者は認証サーバとのみ秘密情報（パスワード）を共有し、サーバを介して認証が行われる（図１の(b)参照）。しかし、秘密情報共有型であることに変わりなく、センタに秘密情報が集中してしまうため、センタのセキュリティの弱さがシステム全体を危険にさらすことになりかねない。

公開鍵暗号技術を利用した認証方式（[2]など）を用いることで、従来の秘密情報共有型認証の欠点をカバーすることができる。ＣＣＩＴＴ勧告Ｘ.５０９では、公開鍵方式のディジタル署名を用いた厳密認証のプロトコルを示している。

ネットワーク上のサービスがＸ.５０９厳密認証手順のような認証方式を共通に採用することで、認証インターフェースの統一が実現されるが、社内ネットワークのような比較的閉じたネットワーク環境ではアクセス権の集中的管理が有効である場合がある。そこで、本認証システムでは、図２に示すような集中型厳密認証プロトコルを提案、採用している。

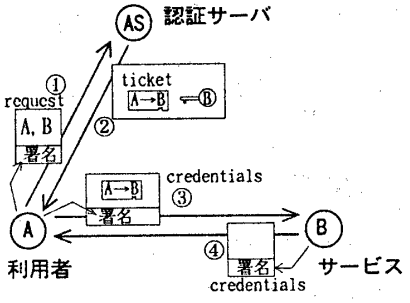


図２　集中型厳密認証方式

利用者ＡがサービスＢを利用したい場合、まず認証サーバにその旨を通知する。認証サーバは、Ａを認証した後、ＡのＢに対するアクセス権をチェックし、チケットを作成する。チケットは、サービスを利用するための切符のような役割を持ち、利用者の公開鍵等を含む。Ａは、認証サーバよりチケットとＢの公開鍵を受け取り、チケット、時刻、乱数等に署名を施したcredentialsを作成し、Ｂに送る。Ｂは、チケットからＡの公開鍵を取り出し、credentialsの署名を検証し、Ａを認証する。Ａ、Ｂの公開鍵はそれぞれ認証サーバの署名によって保護されている。

以上のような手順により、Kerberosと同形態の認証方式をより安全に実現できる。

2.2　ディレクトリの利用

ディレクトリは、通信に関わる情報を管理する分散データベースと考えることができ、ＣＣＩＴＴ勧告Ｘ.５００シリーズで標準化されている。メッセージ通信処理システム（ＭＨＳ）の国際標準であるＣＣＩＴＴ勧告Ｘ.４００シリーズでは、

An Authentication System using X.500 Directory
Tomohiro KITAKAKU, Masashi KATSUMATA
NTT Network Information Systems Laboratories

公開鍵暗号技術を利用した種々のＭＨＳセキュリティサービスを規定しており、公開鍵のディレクトリへの格納を前提としている。公開鍵の管理の枠組みは勧告Ｘ．５０９で述べられている。利用者の公開鍵は、信頼できる証明機関が作成した証明書（certificate）の形でディレクトリに格納されており、必要に応じて自由に取得できる。証明書は、公開鍵と公開鍵の所有者との関連付けの正当性を証明機関が保証するものであり、印鑑証明のようなものである。

本認証システムでは、国際標準に従い、公開鍵を含む利用者情報をディレクトリによって管理する。ディレクトリを用いる利点として、

・情報の分散管理、世界的な規模での相互接続が可能である。
・アクセスプロトコルを新たに規定する必要がなく、複数サービスでの共通利用が容易である。

といった点が挙げられる。今後、電子的な情報交換等でディジタル署名の利用がおおいに想定され、公開鍵を共通的なデータベースで管理することは大きな意義を持つ。

2.3 アクセス権管理

本認証システムでは、利用者がネットワーク上のサービスの利用を要求した時に、サービスへアクセスする権利があるかどうかをチェックすることができる。すなわち、認証サーバによって簡易なアクセス制御を行うことが可能である。本システムでは、アクセス可否を判断するためのアクセス制御情報をディレクトリの属性として保持し、ディレクトリ・ツリーの構造やディレクトリに格納された情報と連動したアクセス制御を可能としている。例えば、社内ネットワークへ適用すれば、ネットワーク上のサービスは独自にアクセス制御リストを保守する必要がなく、人事異動等があってもディレクトリの保守のみで適切なアクセス制御がネットワーク全体に提供される。

2.4 利用暗号技術

公開鍵暗号技術を用いた厳密認証では、署名の作成、署名の検証を数回行う必要があり、高速な処理が必要とされる。

代表的な署名方式であるＲＳＡ署名方式、および高速な署名方式であるＥＳＩＧＮ署名方式[3]について、本認証システムの集中型厳密認証方式を実現した場合の時間性能の予測・評価を行った。端末としてパーソナルコンピュータ（CPU:80286）クラス、センタとして高性能ワークステーションクラスを仮定している。また、処理時間の見積もりに用いた数値は、試作プログラムによる。

署名方式	所要時間
ＲＳＡ	80 (sec)
ＥＳＩＧＮ	6.5 (sec)

ＥＳＩＧＮを用いた場合の所要時間は、署名処理時間をさらに短縮することが可能であることを考え合わせると、十分実用的なレベルといえる。一方、ＲＳＡ方式では、ソフトによる実現では、実用的な性能が得られない。本認証システムではＥＳＩＧＮ署名方式を採用する。

3 セキュリティ通信システムの機能

本報告の認証システムを含むセキュリティ通信システムの試作を進めている。Ｘ．４００ＭＨＳ、Ｘ．５００ディレクトリの機能モデルをベースにした機能モデルを図３に示す。

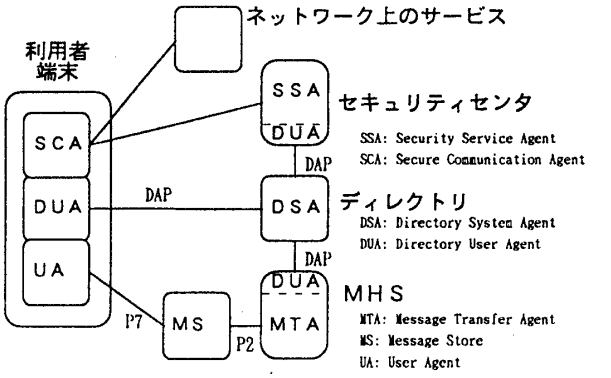


図３ セキュリティ通信システムの機能モデル

本モデルでは、ＭＨＳ／ディレクトリの枠内では実現できないセキュリティサービスを提供するネットワーク上のエンティティとして、セキュリティセンタ、ＳＳＡ（Security Service Agent）を置いている。利用者端末には、セキュリティセンタへアクセスする機能、ネットワーク上のサービスと安全な通信を行う機能が必要であり、この機能をＳＣＡ（Secure Communication Agent）としてモデル化している。ＳＳＡは、Ｘ．５０９の証明機関機能、認証サーバ機能、鍵配送センタの機能を持ち、ディレクトリの情報を利用してサービスを行う。ＭＨＳには、Ｘ．４００で規定されている種々のセキュリティサービスを実装し、電子メールに高度なセキュリティを提供する。また、ネットワーク上のエンティティ（利用者、ネットワーク上のサービス）はディレクトリで一元管理され、公開鍵等のセキュリティ関連情報もディレクトリに格納される。これら、ディレクトリ、ＭＨＳ、セキュリティセンタの提供するセキュリティサービスによって、利用者は、相互認証、通信情報の秘匿（暗号化）、通信情報の完全性保証等のセキュリティ機能を備えた安全な通信が可能である。

4 おわりに

公開鍵暗号技術を用いた次世代の集中型認証システム、さらには、ネットワーク環境に高度なセキュリティを提供するセキュリティ通信システムの構築をめざし、必要機能、実現方式、利用暗号技術等を検討した。

現在、ＩＳＯ等の標準化機関において、セキュリティ関連の標準化が精力的に行われており、これらの動向にも注目していきたい。

参考文献

[1] J.G.Steiner, C.Neuman and J.I.Schiller, "Kerberos: An Authentication Service for Open Network Systems," Proc. USENIX 1988 Winter Conference, pp.191-202, 1988

[2] R.M. Needham and M.D.Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Comm. ACM, Vol.21, No.12, pp.993-999, 1978

[3] 岡本，藤岡，岩田，"高速ディジタル署名方式 ESIGN," NTT R&D, Vol.40, No.5, 1991