5Z-6

属性認証プロトコルとアクセス制御方式の提案，実装

矢田広志† 小林吉純‡
大阪工業大学大学院 情報科学研究科 情報科学専攻†
大阪工業大学 情報科学部 情報ネットワーク学科‡

1．まえがき

アクセス制御は利用者の所属や肩書等の属性に基づき行うことが本来の姿であるとの考え方に基づき，X509 属性証明書に基づくアクセス制御方式を提案してきた(1)．しかし，属性証明書をアクセス制御システムが直接扱うことには，以下の問題点がある．

・属性証明書が本人のものであることを確認するため，属性証明書は本人の名前を要素として含む X.509 公開鍵証明書との対応関係を持つが，この確認を行うと，本人の特定が可能となる．しかし，属性に基づくアクセス制御では本人のものであることの確認が取れればよく，本人の特定は必要でなく，本人特定による弊害も予想される．
・属性証明書が属性局(以降，AA と呼称)から発行されたものであることや属性証明書が本人のものであることの確認(これらを属性認証と呼称)，及び属性証明書からの属性取り出しは，アクセス制御システムに共通する処理であり，アクセス制御システムとは独立した箇所で行うことがシステムの効率的開発の観点から望ましい．

これらの問題点の解決策として，属性認証と属性証明書からの属性取出しを担当する通信プロトコルを規定し，これを属性認証プロトコル Attribute Authentication Protocol(以降，AAP と呼称)と名付けた．本稿では，AAP 仕様及びその仕様の妥当性や適用性の検証を目的として作成した AAP プログラム，アクセス制御システムに関して報告する．

2．AAP とアクセス制御本体の機能分担

AAP 仕様設計の前提として AAP プログラムとそれを利用するアクセス制御本体プログラム(アクセス制御システムから AAP プログラムを除いた部分)の機能分担を明確にする．

アクセス制御システムは一般的にクライアントサーバ型で実現される．これにより，AAP もクライアントサーバ型となる．以降，アクセス制御本体プログラムのサーバ部分を AC サーバ，クライアント部分を AC クライアントと呼び，AAP プログラムのサーバ部分を AAP サーバ，クライアント部分を AAP クライアントと呼ぶ．これらの役割は以下のように整理できる．

・AC サーバは正しい属性に基づき，その属性所有者のアクセス権限を判断する．
・AAP サーバは正しい属性を AC サーバに渡す必要があるので，属性認証を行い，妥当であれば，属性証明書の属性を AC サーバに渡す．
・属性証明書は利用者が所有しているため，利用者は AC クライアント，AAP クライアントを経由し，AAP サーバに属性証明書を送る．従って，AC クライアントは利用者と AAP クライアントの仲介，AAP クライアントは AC クライアントと AAP サーバの仲介の役割を持つ．

3．AAP 仕様

3.1 AAP の設計方針

AAP 仕様の設計方針を以下に示す．

・AAP はクライアントサーバ型のプロトコルとする．
・クライアントとサーバ間の通信は常にメッセージを交換する形態とする．即ち，メッセージはクライアントとサーバで交互に送信する．
・通信情報の秘匿化（暗号通信）を盛り込む．

3.2 AAP の機能

(1) 属性認証

属性証明書の発行元確認は属性証明書に付加された AA 署名を検証することにより行える．この処理の前提として，AAP サーバは AA の公開鍵証明書を保持する．属性証明書の本人性確認は，公開鍵証明書内に所有者名が存在し，属性証明書内に公開鍵証明書へのポインタが存在することにより，利用者が公開鍵証明書の所有者であることと，属性証明書内のポインタがその公開鍵証明書を指し示していることを検証すれば可能である．

(2) 利用者認証

属性認証を行う際，利用者が公開鍵証明書の所有者であることの検証が必要となる．これは利用者認証により達成できる．即ち，AAP サーバで作成した乱数に，利用者の秘密鍵で署名を作成させ，それを利用者の公開鍵証明書内の公開鍵で検証することが利用者認証であるが，これは利用者がその公開鍵証明書の所有者であることと等価である．

この場合，利用者の公開鍵証明書の正当性検証は公開鍵証明書に付加された CA 署名を CA の公開鍵証明書内の公開鍵で検証することにより行える．この処理の前提として，AAP サーバでは CA の公開鍵証明書を保持する．

(3) 通信の暗号化

通信の暗号化には共通鍵暗号方式を使用するが，その使用に当たっては，AAP クライアントと AAP

A proposal and prototype implementation of attribute authentication protocol and access control
†Hiroshi Yada: Graduate School of Information Science and Technology, Osaka Institute of Technology
‡Yoshizumi Kobayashi: Information Science and Technology, Osaka Institute of Technology

サーバ間での共通鍵共有が必要となる．鍵共有の代表的方式として，公開鍵暗号を適用する方式とDiffie-Hellman 鍵交換方式(以下，DH 鍵交換方式と呼称)とがあるが，公開鍵証明書の不要な DH 鍵交換方式を当面採用する．

3.3 通信手順

(1) ハンドシェーク

AAP 通信開始時に行うコネクションの確立と暗号方式のネゴシエーションをハンドシェークと呼ぶ．ネゴシエーションに関しては，暗号方式の選択は利用者に任せるべきとの観点から，AAP サーバで扱う暗号方式一覧から，利用者が暗号方式を選択し，AAP サーバに通知する方式とした．

(2) 属性認証

ハンドシェーク終了後，以下の手順で属性認証を行う．以下で括弧内は AAP メッセージである．

(a) 利用者認証

① AAP サーバで乱数を生成し，AAP クライアントへ送信する(SignatureRequest)．
② AAP クライアントでは受信した乱数を AC クライアントに通知する．
③ AC クライアントでは利用者の秘密鍵で乱数に署名し，公開鍵証明書，属性証明書，署名を AAP クライアントへ渡す．
④ AAP クライアントでは公開鍵証明書と利用者署名を AAP サーバへ送信する(SignatureResponse)．
⑤ AAP サーバでは公開鍵証明書の CA 署名と利用者署名を検証する．

(b) 共通鍵の共有

DH 鍵交換方式に基づき，AAP クライアントと AAP サーバ間で共通鍵を共有する．

(c) 利用者認証以外の属性認証

① AAP サーバが AAP クライアントへ属性証明書を要求する(AttrRequest)．
② AAP クライアントでは利用者の属性証明書を暗号化し，AAP サーバへ送信する(AttrResponse)．
③ AAP サーバでは属性証明書を復号した後，属性証明書の AA 署名，公開鍵証明書との対応関係を検証する．
④ 検証結果が妥当であれば，属性証明書内の属性を AC サーバに渡す．

4. ファイルアクセス制御システム

AAP 仕様の妥当性，適用性の検証を目的として，企業におけるファイルアクセス制御システム及び関連する CA，AA のプログラムを Java で作成した．全体構成を図 1 に，概略手順を以下に示す．

① CA が利用者の秘密鍵，公開鍵証明書を作成し，利用者に交付する．
② 利用者は公開鍵証明書を AA に提出し，属性証明書の発行を受ける．
③ 利用者は公開鍵証明書や属性証明書をアクセス制御システムに提示し，アクセス制御を受ける．

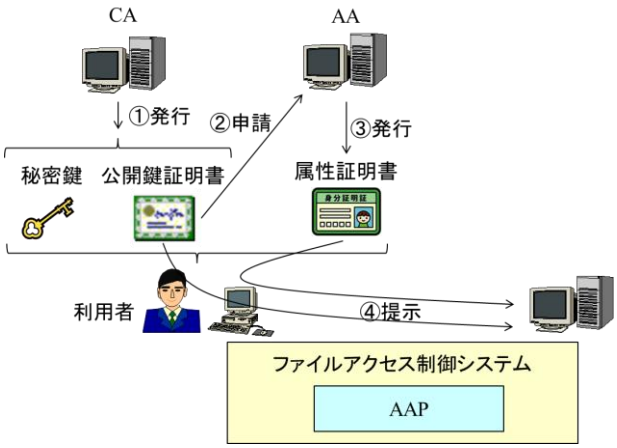

図 1 システム構成

(1) AAP プログラム

AAP プログラムの役割は AC サーバや AC クライアントに対する API の提供である．API は Java の Socket クラスや ServerSocket クラスのサブクラスで実現した．主なメソッドを以下に示す．

・ AC クライアントからの利用者の公開鍵証明書，属性証明書，署名の送信（SendAuthData）
・ AC サーバでの属性の取り出し（GetAttribute）

(2) ファイルアクセス制御本体プログラム

ファイルアクセス制御システムから AAP プログラムを除いた部分をファイルアクセス制御本体プログラム，そのサーバ部分を FAC サーバ，クライアント部分を FAC クライアントと呼ぶ．本体プログラムでは，属性として，所属（人事部，開発部等）と役割（部長，課長等）を規定し，ファイルに対するアクセス権を以下のように規定する．

・ 読み込み権：FAC サーバから FAC クライアントへファイル内容をダウンロードする権利
・ 書き込み権：FAC クライアントから FAC サーバへファイル内容をアップロードし，ファイル内容を書き換える権利

FAC サーバで，ファイル対応に属性とアクセス権の組合せを管理し，FAC クライアントからの利用者要求（ファイルの新規作成，閲覧，更新）と利用者属性に基づき，アクセス許可を判断する．なお，ファイル更新中の期間は，他の利用者による同一ファイルの操作はすべて禁止する．

5. おわりに

AAP 仕様とそれに基づく API を規定し，その適用により，属性認証部とアクセス制御部を分離でき，利用者を特定することなく，属性に基づくアクセス制御を実現できることを明らかとした．

参考文献

(1) 矢田・小林：属性証明書に基づく割引サービス構成方式の提案, 情報処理学会（2011）