4V-03

属性証明書を利用した強制アクセス制御の実現

中本　泰貴†　　小林吉純‡

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

強制アクセス制御はシステム管理者がアクセス制御の方法を規定する方式であり，任意アクセス制御に比べ，管理がより徹底し，安全性が高いと言われている．強制アクセス制御は SELinux 等で実現されているが，普及が進んでいるとは言い難い．また，アクセス権限等の属性の真正性の証明を目的とした X.509 属性証明書では，強制アクセス制御のクリアランス（アクセス主体のラベル）も設定可能である[(1)]．本稿では，強制アクセス制御の多層セキュリティモデルとして最も有名な Bell-LaPadula モデル[(2)]を X.509 属性証明書を利用して実現し，その使用評価を行うことを目的とする．

2．Bell-LaPadula モデル

Bell-LaPadula モデルは情報の格上げは可，情報の格下げは不可という規則を基礎としたアクセス制御モデルである．アクセスの主体と対象に，機密種別とカテゴリ(情報種別)から成るラベルを付与しておき，アクセス時に両者のラベルを照合し，表 1 の規則に基づき，対象の読取りや書込みの許可/禁止を決定する．

表 1 Bell-LaPadula モデルのアクセス規則

		対象の読取り	対象の書込み
ラベル		主体≧対象	主体≦対象
内訳	機密種別	主体≧対象	主体≦対象
	カテゴリ	主体⊇対象	主体⊆対象

注：≧は機密の高さ，⊇はカテゴリの包含を意味する．

機密種別に関しては，表 1 は以下の解釈となる．

- 高い機密種別を持つ主体は低い機密種別の対象に書き込めない．
- 低い機密種別を持つ主体は高い機密種別の対象に書き込める．
- 高い機密種別を持つ主体は低い機密種別の対象を読める．
- 低い機密種別を持つ主体は高い機密種別の対象を読めない．

例えば，図 1 において対象のカテゴリが研究，特許で，機密種別が秘の場合，主体 A のカテゴリが特許で，機密種別が内部情報であれば，カテゴリは主体⊆対象，機密種別は主体≦対象となり，対象の書込みは可能であるが，対象の読取りは禁止される．

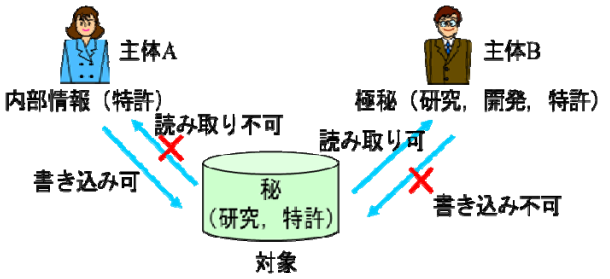

図 1 Bell-LaPadula モデルの例

3．強制アクセス制御の適用方針

(1) アクセス種別

Bell-LaPadula モデルは読取り，書込みの規定のみであり，書込みの意味に曖昧な点がある．そのため，一般に以下の左欄のアクセス種別が使用される．しかし，本稿では対象を文書に限定するため，以下の右欄のアクセス種別を使用する．

- write（読取りと書込み）　→　更新
- read（読取りのみ）　→　読込み
- append（書込みのみ）　→　追記
- execute（両方なし）　→　アクセス不可

(2) ラベル規定と新規文書のラベル付与

今回はある企業を想定し，以下のラベルを規定した．

- カテゴリ：人事，経営，営業，開発，研究
- 機密種別：公開，内部，秘，極秘

新規文書に対するラベル付与方法として，以下の 2 案が考えられる．

案 1：システム管理者が文書内容に基づき，ラベルを決定

案 2：文書作成者の申請カテゴリと作成者の機密種別に基づき，ラベルを決定

案 1 では正確，安全なラベル付与が期待できる反面，各カテゴリに精通した専門家が必要であり，付与の自動化もできない．これに対し，案 2 の場合，付与の自動化は可能であるが，申請者のミス又は悪意による不正なラベル付与が生じる恐れがある．安全性重視の観点からは案 1 を採用すべきであるが，今回は実験システムであり，不正なラベル付与は起こりえないため，案 2 の方式を採用することとした．

Implementing Mandatory Access Controls using X.509 Attribute Certificates

†Taiki Nakamoto: Information Science and Technology, Osaka Institute of Technology

‡Yoshizumi Kobayashi: Information Science and Technology, Osaka Institute of Technology

４．実現方式

4.1 アクセス主体のラベル付与

アクセス主体（以降，利用者と呼称）には事前にラベルを付与する必要があるが，これは企業内の責任部署が行い，ラベルを含む X.509 属性証明書を発行するものとする．その属性証明書が本人のものであることを証明するためには，属性証明書との対応関係を持つ X.509 公開鍵証明書と秘密鍵が必要となるが，これらも同時に発行するものとする．今回はこれらの発行機能を通常のアプリケーションとして実現した．

4.2 アクセス対象の処理

アクセス制御のシステムは Tomcat 上に Web アプリケーションとして実現した．アクセス種別における更新ではサーバが利用者に文書を送信し，利用者が更新した後，文書をサーバにアップロードする．読込みではサーバが利用者に文書を送信する．追記では利用者が追記内容をサーバにアップロードした後，それをサーバが既存文書に追加する．追記時の文書結合では文書形式毎に異なるプログラムの作成が必要なため，本稿では文書形式をテキスト，Word，PowerPoint の 3 種に限定した．

4.3 アクセス制御手順

アクセス制御は図 2 の手順で行うこととした．

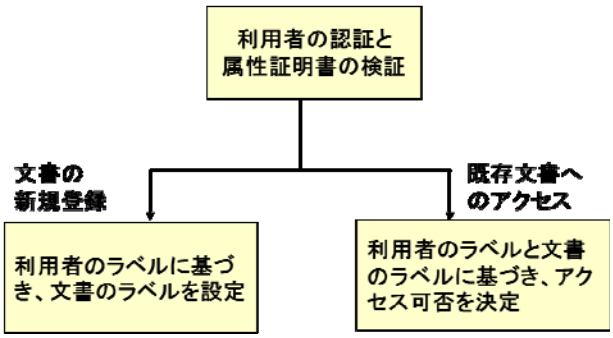

図 2 アクセス制御手順

(1) 利用者の認証と属性証明書の検証

属性証明書はやり取りの対象であるため，誰もがそのコピーを保持することができる．属性証明書提示者が本人か否かの確認は，属性証明書に紐付された公開鍵証明書とペアになっている秘密鍵の所有者が属性証明書を提示したか否かを検証することによって行う．

具体的には図 3 に示すように，サーバから送信された乱数に利用者の秘密鍵で署名させ，それを検証することにより，本人認証が可能となるので，その際に使用した公開鍵証明書と属性証明書が対応関係を持つことを検証することにより，属性証明書の所有者を確認できる．

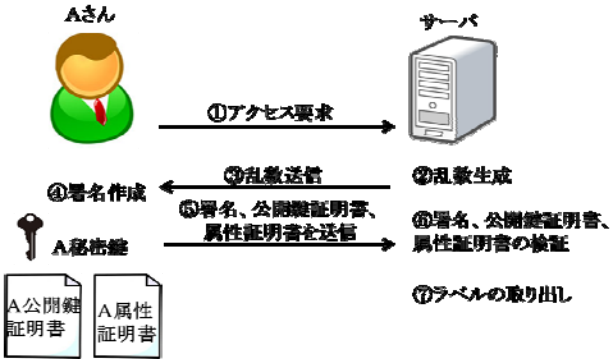

図 3 利用者の認証と属性証明書の検証

(2) 文書の新規登録

文書の新規登録手順を以下に示す．

① 利用者は文書のタイトル，概要，文書本体，カテゴリを指定して，登録要求を行う．

② サーバでは利用者のラベルがそのカテゴリを含むか否かをチェックし，含むのであれば，その文書にそのカテゴリと利用者が持つ機密種別を付与して文書の新規登録を行う．なお，この際は，一意となるファイル名を付与する．

(3) 既存文書へのアクセス

既存文書へアクセスする際の手順を以下に示す．

① 利用者はカテゴリを指定することにより，既存文書のタイトル一覧を取得する．

② 利用者は既存文書に対するアクセス種別(更新，読込み，追記)を指定し，アクセス要求を出す．

③ サーバでは利用者のラベルと文書のラベルを照合し，アクセス可否を判断する．

④ アクセス可の場合，更新や読込みであれば，サーバは既存文書を利用者に送信する．

⑤ 利用者は更新の場合，更新後の文書をサーバに送信する．追記の場合は，追記内容を送信する．

⑥ サーバでは更新時は既存文書と置換し，追記時は既存文書と結合する．

５．おわりに

属性証明書を利用し，Bell-LaPadula モデルの強制アクセス制御を実現した．今回，文書の新規登録時，利用者の機密種別とカテゴリ指示に従い，登録する仕様とした．この場合，利用者のミスや悪意による不正登録を防げない．しかし，登録時に，システム側要員を介在させると自動化ができず，運用コストがかかる．この点が強制アクセス制御の普及を妨げる要因と思われる．

参考文献

(1) RFC5755, An Internet Attribute Certificate Profile for Authorization, Jan. 2010.
(2) D. E. Bell and L. J. La Padula. Secure computer systems: Vol. I, Vol. II, Vol. III. Technical Report MTR-2547, Mitre Corporation, Bedford, MA, Mar.–Dec. 1973.