X.501ディレクトリモデルのアクセス制御に関する考察

砌谷 佳子† 小川 高貞†† 森住 哲也‡ 辻井 重男‡‡

†,‡‡ 中央大学理工学部情報工学科
†† 中央大学大学院理工学研究科情報工学専攻
‡ 東洋通信機株式会社
†,††,‡‡ 〒112-8551 東京都文京区春日 1-13-27
‡ 〒253-0192 神奈川県高座郡寒川町小谷 2-1-1
†ytogiya@tsujii-lab.ise.chuo-u.ac.jp ††togawa@tsujii-lab.ise.chuo-u.ac.jp
‡moriz@toyocom.co.jp ‡‡tsujii@ise.chuo-u.ac.jp

あらまし

コンピュータネットワークのオープン化・グローバル化に伴い，ネットワークを介した情報提供システムに必要なセキュリティ機能の一つである，アクセス制御機能が注目されている．その中でも，正当なアクセス制御に従っているにも関わらず，結果的にシステムのセキュリティポリシーに反し，情報が漏洩してしまう情報の流れ，すなわち Covert Channel を考慮に入れたアクセス制御機能を構成することが重要な課題となっている．

本稿においては，各種の情報を組み合わせて効率良く得ることのできる総合案内システムである，X.501 ディレクトリモデルにおける Covert Channel の存在を指摘し，アクセス制御情報項目に所有者 ID を付加することで，その Covert Channel を回避するアクセス制御アルゴリズムを提案する．

キーワード：X.501 ディレクトリモデル，Covert Channel，所有者 ID，アクセス制御決定関数

Access Controls on the X.501 Directory Models

Yoshiko Togiya† Takasada Ogawa†† Tetsuya Morizumi‡ Shigeo Tsujii‡‡

†,‡‡Dept. of Information and System Engineering,Chuo University
††Dept. of Information and System Engineering,Graduate School of Science and Engineering, Chuo University
‡Toyo Communication Equipment Co., Ltd.
1-13-27, Kasuga, Bunkyo-ku, Tokyo, 112-8551, Japan
2-1-1, Koyato, Samukawa-cho, Kouza-gun, Kanagawa, 253-0192, Japan
†ytogiya@tsujii-lab.ise.chuo-u.ac.jp ††togawa@tsujii-lab.ise.chuo-u.ac.jp
‡moriz@toyocom.co.jp ‡‡tsujii@ise.chuo-u.ac.jp

Abstract

Recently, access control in computer networks has become of vital importance. A covert channel is an information flow that leaked out on access control. Therefore, access control function avoiding covert channels should be established.

This paper shows in the first part, the existence of covert channels in the X.501 directory models which provide us with multi information services efficiently. In the second part, we present access control algorithms that avoid covert channels in the X.501.

Key words: X.501 Directory Models, Covert Channel, The Owner's ID, The Access Control Function

1 はじめに

情報通信の発達した現在，提供される各種の情報も多岐に渡るようになり，世界規模での情報の体系化を目指した総合案内サービスが切望されている．そのようなシステムが汎用のシステムとなれば，ユーザは，様々な情報を組み合わせて効率よく得ることが可能となる．

それを実現すべく，本研究の対象である X.501 ディレクトリモデルは規定された．この X.501 ディレクトリモデルとは，各種の情報を共通の構成方法で格納し，多くのユーザが必要に応じてアクセスできるシステムである．以下，X.501 と呼ぶ．

しかし，コンピュータネットワークのオープン化・グローバル化の一方で，セキュリティ強化という課題が浮上してきた．本稿では，中でもアクセス制御機能に着目し，正当なアクセス制御に従っているにも関わらず，結果的にシステムのセキュリティポリシーに反し，情報が漏洩してしまうデータの流れ (Covert Channel) について考察していく．

まず第 2 章において，X.501 がどのような情報構造をもって，情報を管理しているかについて述べ，続いて第 3 章では，現存の X.501 のアクセス制御について説明する．そして，第 4 章において，X.501 アクセス制御における Covert Channel の存在を指摘し，第 5 章では，その Covert Channel 回避を目的とした新たなアクセス制御について提案する．

2 X.501 の情報構造

2.1 ディレクトリ情報ツリーの構造

ディレクトリとは，実世界の様々な事物に関する情報を提供するものである．このディレクトリの管理している情報全体を，ディレクトリ情報ベース (DIB) と呼び，それをツリー状に配置したものをディレクトリ情報ツリー (DIT) と呼ぶ．ツリー構造に着目する事により，ディレクトリ情報ベース内のオブジェクトを一意に指定でき，また，ディレクトリをいくつかに分散して管理できるようになる．DIT を木とみなしたときの根にあたるノードを，ルート (root) と呼ぶ．ここで，ディレクトリに管理されている実世界の事物をオブジェクトといい，オブジェクトがどのような性質のものであるかをオブジェクトクラスによって表す．

2.2 エントリの構造

エントリは，実世界のものであるオブジェクトに関する情報の集まりである．そして，そのオブジェクトに関する 1 つ 1 つの情報を属性と呼ぶ．属性は，属性型，および，単一あるいは複数の属性値の対で構成される．属性型は，ある属性がどのような種類の情報であるかをオブジェクト識別子により表したものである．また，その属性型によって示された種類の，オブジェクトに関する具体的な情報内容が属性値である．属性値は，単数の場合も複数の場合もある．

2.3 識別名

ツリー構造上のあるエントリから見て，まず，その直接下位に存在するエントリ全てを一意に識別できるような名称，相対識別名を各エントリに与える．これには，そのエントリのいずれかの属性が用いられるが，これを識別属性値と呼ぶ．そして，あるエントリの識別名とは，そのエントリ自体の相対識別名と，その上位エントリ全ての相対識別名を，列で表したものである．また，識別名は各エントリに対してただひとつ存在する．

3 X.501 のアクセス制御

3.1 アクセス制御管理モデル

ディレクトリは，大規模な情報を扱うため，通常，複数の管理機関が分担して管理・運用する．各管理機関の分担範囲は，システム管理の側面から見た場合にはディレクトリ管理領域と呼ばれ，情報管理の側面から見た場合には DIT 領域と呼ばれる．

ここで，X.501 のアクセス制御管理に着目すると，DIT は，複数の自治管理領域 (AAA) によって分割管理され，また，各 AAA は，アクセス制御特定管理領域 (ACSA) に分割管理される．そして，各 ACSA 内にもまた，複数のアクセス制御内部管理領域 (ACIA) が必要に応じて規定されるのである．そして，各管理機関が，それぞれを管理する形式を取る．

3.2 アクセス制御情報の種別

各アクセス制御管理領域には，その領域内のディレクトリ情報へのアクセス制御内容を記述したアクセス制御情報を配置しておく必要がある．基本アクセス制御におけるアクセス制御情報は以下の 3 つである．

- エントリアクセス制御情報 (entryACI)
  一般のエントリが持つ運用属性で，そのエントリ自体に対するアクセス制御内容を記述する．
- サブエントリアクセス制御情報 (subentryACI)
  各種管理エントリの持つ運用属性で，その管理エントリのサブエントリに対するアクセス制御内容を記述する．

- 包括アクセス制御情報 (prescriptiveACI)
  管理ポイントのサブエントリに格納される運用属性で，管理領域内のエントリ集合をひとまとめにした包括的なアクセス制御内容を記述する．

要するに，図1のような，ある制御対象エントリに対するアクセス制御は，そのエントリ自体のエントリアクセス制御情報運用属性の定義内容と，そのエントリの制御に関わる上位の管理エントリのサブエントリ中の包括アクセス制御情報運用属性の定義内容を総合する形で実行される．

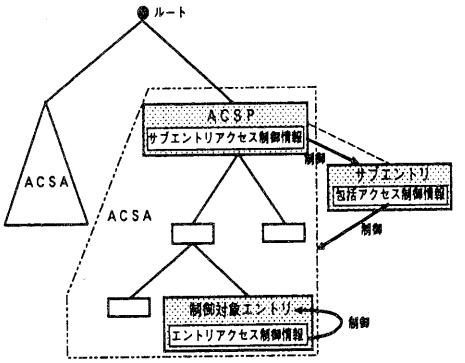

図 1: アクセス制御情報の適応範囲

3.3 アクセス制御情報項目

アクセス制御情報はアクセス制御情報項目の集合として表現される．個々のアクセス制御情報項目では，特定のユーザから特定の保護項目へのアクセスの許可または拒否に関する定義がなされている．アクセス制御情報を構成する主要なアクセス制御情報項目を挙げると，以下のようになる．

(i) 識別タグ…アクセス制御情報項目の管理に用いる識別子．

(ii) 優先順位…アクセス制御情報項目の優先順位．

(iii) 認証レベル…ユーザに要求される認証レベルを規定する部分．

(iv) ユーザクラス…制御の対象となるユーザを規定する部分．ユーザの指定方法としては，名前による単一ユーザの指定だけでなく，グループ，サブツリー仕様などによる複数ユーザの一括指定も可能である．

(v) 保護項目…制御の対象となる情報を規定する部分．エントリ，属性，属性値など，各種の単位で指定することができる．

(vi) 許可または拒否…指定したユーザクラスのユーザが指定した保護項目にアクセスする場合の，各種アクセス許可種別に関する許可または拒否の設定．

3.4 アクセス制御決定関数

以上のアクセス制御情報を用い，アクセスの可否を一意に決定するアクセス制御決定関数のアルゴリズムを以下に示す．

Step1. アクセス制御情報項目を分割する．

Step2. 対象となるユーザクラス，保護項目，許可種別のいずれかが該当しないアクセス制御情報項目をすべて捨てる．

Step3. 優先順位の最も高いアクセス制御情報項目を残し，それより低いアクセス制御情報項目をすべて捨てる．

Step4. 複数のアクセス制御情報項目が残っている場合，ユーザクラスの値を最も詳細に指定しているもののみを残す．ユーザクラスの指定が同一の場合，保護項目の値を最も詳細に指定しているもののみを残す．

Step5. 最終的に残ったアクセス制御情報項目の許可種別がすべて許可である場合，アクセスを許可する．

4 X.501 アクセス制御の問題点

ここでは，X.501のアクセス制御における問題点について考察する．

4.1 Covert Channel

正当なアクセス制御に従っているにもかかわらず，情報の添付などによって，結果的に予期せぬ情報流が生じ，情報が漏洩してしまう通信経路のことを，Covert Channel（カバートチャネル）と呼ぶ．

例えば，図2のような，データベースA，B，Cがあるとする．この時，Aの所有者は，Cの所有者とは敵対関係にあり，Aの内容はCの所有者には知られたくない．ここで，Aの所有者はBの所有者とだけやり取りするつもりでBの所有者にAの内容を知らせる．ところが，Bの所有者がこのAの内容を含んだBの内容をCに書き込んだ場合，結果的には，これはAの内容がCに書き込まれたことに等しく，情報リークが起こったことになる．このように，管理者のわからないところで，情報が漏洩する，この情報流がCovert Channelである．

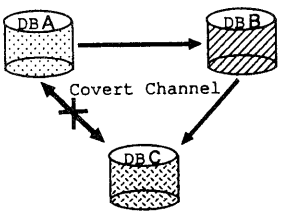

図 2: Covert Channel

4.2 X.501 における Covert Channel

それでは，X.501 において Covert Channel は存在するであろうか．ここでは，ひとつの例として，実際に図 5 を用いて，X.501 アクセス制御について考察する．この時，図 5 中の網掛け部分は考慮しないものとする．

まず，この例において，各組織 A，B，C は，その組織以下のサブツリーの管理エントリであり，アクセス制御サブエントリをもつ．また，個人 P と個人 T は対立しており，個人 P の「属性型＝携帯番号」の属性値「 090-####-#### 」は個人 T には伝えたくないが，一方，個人 R は緊急連絡先として個人 P の携帯番号をエントリの属性として所有したいものとする．

よって，ここでは X.501 における Covert Channel の存在の有無を知る為，個人 P の情報が対立している個人 T に，正当なアクセス制御に従っているにも関わらず伝わるかどうかを考察する．実際には，以下のようなアクセス要求に対して，アクセス制御決定関数を用いて適用されるアクセス制御情報を選択し，そのアクセスが許可されるかどうかを順を追って見ていけば良い．

(1) 個人 R が個人 P のエントリの読出要求
(2) 個人 R が個人 P のユーザ属性の読出要求
(3) 個人 R が個人 R のエントリに「属性型=緊急連絡先」である属性を新たに追加するエントリ更新操作要求
(4) 個人 T が個人 R のエントリの読出要求
(5) 個人 T が個人 R の「属性型=緊急連絡先」である属性の読出要求

故に，適用されるアクセス制御情報は，図 5 中の (A) から (H) を用いて表すならば，それぞれ (1)-(B), (2)-(B), (3)-(E), (4)-(F), (5)-(H) となり，すべてのアクセスは許可される．

この結果，個人 P の情報は個人 R を介することにより，個人 T に流れる．これは，X.501 において，Covert Channel が存在することを示す例であるので．X.501 において Covert Channel は存在するといえる．

5 Covert Channel の回避法

それでは，X.501 において Covert Channel を生じさせないようにするには，どのようにすればいいだろうか．本章では，アクセス制御情報項目に「所有者 ID」を増やすことによって，Covert Channel を回避する方法を提案する．

5.1 基本方針

まず，Covert Channel による一番の問題点として挙げられるのは，情報源であるエントリの知らないところでその情報がやり取りされる点にある．また，その情報の流れの中で，情報源であるエントリにとって情報を流したくない危険なエントリからのアクセスを回避する必要がある．そのためにも，その情報の行方を情報源であるエントリが認知しておかねばならない．そこで，アクセス制御情報項目に「所有者 ID」を増やすことでその情報に名前をつけ，その情報へのアクセスの際には必ず，所有者であるエントリのアクセス制御情報を参照させるようにする．ここで,「所有者 ID」と「所有者エントリ」を以下のように定義する．

定義 1　所有者 ID　エントリアクセス制御情報内のアクセス制御情報項目の一つで，保護項目によって規定された情報の所有者にあたるエントリの識別名を「所有者 ID」とする．

定義 2　所有者エントリ　所有者 ID によって指定されたエントリを「所有者エントリ」とする．

ここで，所有者 ID はエントリアクセス制御情報内のアクセス制御情報項目であるとした．なぜなら，包括アクセス制御情報は，管理領域内全てのエントリに関するアクセス制御を記述しているため，明確に所有者を定義することは困難だからである．

このように，情報に所有者の概念を付加することによって，常にその情報の所有者エントリのアクセス制御情報は参照されるので，所有者にとっての Covert Channel は回避できたことになる．

5.2 アクセス制御アルゴリズム

では，具体的にどのように「所有者 ID」を用い，Covert Channel を回避するかを見ていく．

まず，アクセスの際に問題となるのは，情報の読出添付においてである．この時，アクセス要求は「読出要求」「エントリ更新操作要求」の 2 段階に分けられる．そこで，あるエントリ X があるエントリ Y の情報 Z を読み (「読出要求」)，自分自身のエントリにその情報を追加する場合 (「エントリ更新操作要求」)，エントリ X のエントリアクセス制御情報に，情報 Z の所有者がエントリ Y であることを記述する必要がある．つまり，情報と共に，所有者 ID も引き継ぐようにするのである．この時，情報の内容は変更されないものとする．

具体的には，エントリ X のエントリアクセス制御情報に「保護項目＝情報 Z」で,「所有者 ID ＝ (所有者エントリ)Y の識別名」であるアクセス制御情報を新たに追加すればよい．その際記述するアクセス制御は，X に対するアクセス制御で良い．

そうすることによって，エントリ X の情報 Z に対するアクセスが要求された場合，エントリ X へ

のアクセス制御がなされた後，所有者IDとアクセス制御対象エントリのユーザが一致しないことから，所有者エントリのアクセス制御情報も参照できることになる．したがって，所有者にとってのCovert Channelは回避される．概念図を，図3に示す．

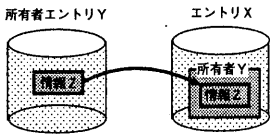

図 3: 所有者IDの概念図

5.3 アクセス制御決定関数

このアルゴリズムに基づくアクセス制御決定関数のアルゴリズムは以下のようになる．

Step1. ユーザクラスや保護項目に関して，統合指定されたアクセス制御情報項目を分割する．

Step2. 対象となるユーザクラス，保護項目，許可種別のいずれかが該当しないアクセス制御情報項目をすべて捨てる．

Step3. 優先順位の最も高いアクセス制御情報項目を残し，それより低い優先順位のアクセス制御情報項目をすべて捨てる．

Step4. 複数のアクセス制御情報項目が残っている場合，ユーザクラスの値を最も詳細に指定しているもののみを残す．ユーザクラスの指定が同一の場合，保護項目の値を最も詳細に指定しているもののみを残す．

Step5. 最終的に残ったアクセス制御情報項目の許可種別がすべて許可である場合，現時点でのアクセス制御対象エントリに対するアクセスは許可する．一つでも拒否があった場合やアクセス制御情報項目が1つも残らなかった場合は，アクセスを拒否する．すなわち，明らかに許可されていない場合は安全を見て常に拒否する．

Step6. 現時点でアクセス制御対象エントリに対するアクセスが許可と判断された場合，そのアクセス制御対象エントリと所有者IDとを比較する．そして，それが一致した場合，このアクセスは許可とする．一致しなかった場合，参照した所有者IDを新たなアクセス制御対象エントリとして，**Step.1**へ戻る．

また，このアクセス制御決定関数のアルゴリズムは，図4のように表せる．

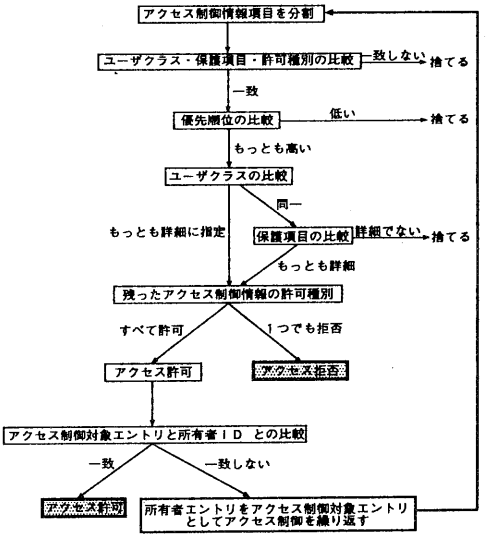

図 4: 所有者IDを付加したアルゴリズム

5.4 改善後のX.501アクセス制御の例

それでは，アクセス制御情報項目に「所有者ID」を付加した場合についてのアクセス制御を，図5に沿って考察していく．

前提条件とアクセス要求は，前に示した通りであるが，この場合，図5中の所有者ID(網掛け部分)は有効とする．また，情報の添付を行った場合，その情報の所有者IDを継承していくようにする．そして，あるアクセス要求に対して適用されたアクセス制御情報中の所有者IDが，制御対象エントリの識別名と一致しない場合は，所有者IDに記載されたエントリのアクセス制御情報を参照するようにする．

まず最初に，アクセス要求(1)に対して適用されるアクセス制御情報は(B)であり，Covert Channelの例と同様である．またこれは，包括アクセス制御情報であることから所有者IDは設定されていないので，制御対象エントリとの比較の必要はない．よって，「許可または拒否：参照系アクセス全て許可」より，このアクセスは許可される．同様に(2)-(B)であるので，このアクセスも許可される．

つぎに，アクセス要求(3)に対して適用されるアクセス制御情報は(E)となり，このアクセスも許可される．この時点において，個人Rは個人Pの「携帯番号＝ 090-####-#### 」という情報を手にいれたことになる．同様に，アクセス要求(4)に対しても，包括アクセス制御情報(F)が参照され，アクセスは許可される．

続いて，アクセス要求(5)を考えると，適用されるアクセス制御情報は(H)となる．しかし，(H)は

エントリアクセス制御情報であるため，アクセス制御対象エントリと所有者IDの比較を行う必要がある．そこで，所有者IDの比較を行うと，「(H)における所有者ID=個人P」であり，アクセス制御対象エントリである個人Rと所有者IDが一致しない．そこで，アクセス制御対象エントリを個人Pとして，再びアクセス要求(5)を行う．すると，この要求に対して適用される個人Pのアクセス制御情報は見あたらず，このアクセスは拒否される．

よって，この所有者IDを付加したアクセス制御においては，「携帯番号＝ 090-####-#### 」という個人Pの情報が，個人Rを介しても個人Tに伝わることはなくなった．故にこの場合，X.501におけるある情報所有者にとってのCovert Channelは，回避されたといえる．

6 むすび

本研究では，X.501のアクセス制御におけるCovert Channelの存在を指摘した．X.501は，大規模な分散データシステムの構築を目指すもので，それだけにCovert Channelの存在は，非常に問題である．そこでまず，Covert Channelが発生する一番の要因として，情報源であるエントリの知らないところでの情報の受け渡しに着目した．そして，その情報の行方を情報源であるエントリが認知するために，アクセス制御情報項目に「所有者ID」を付加することを新たに提案した．

このように，X.501アクセス制御に所有者の概念を与えることによって，その情報へのアクセスの際には必ず，所有者であるエントリのアクセス制御情報を参照することが可能となり，その結果，ある情報の所有者に対するCovert Channelが回避できた．

今後の課題としては，実装段階レベルまでの詳細なアルゴリズムの確立を行う事が挙げられる．

参考文献

[1] 大山 実，千田 昇一，戸部 美春，窪田 光裕，田中 博巳，空 一弘，“X.500ディレクトリ入門，”東京電機大学出版局，1997.

[2] 板垣 美幸，力石 徹也，森住 哲也，マリオ・カルドナ，辻井 重男，“Personal Security Routerによる Covert Channel 迂回制御，”1998年電子情報通信学会総合大会，A-7-4，1998.

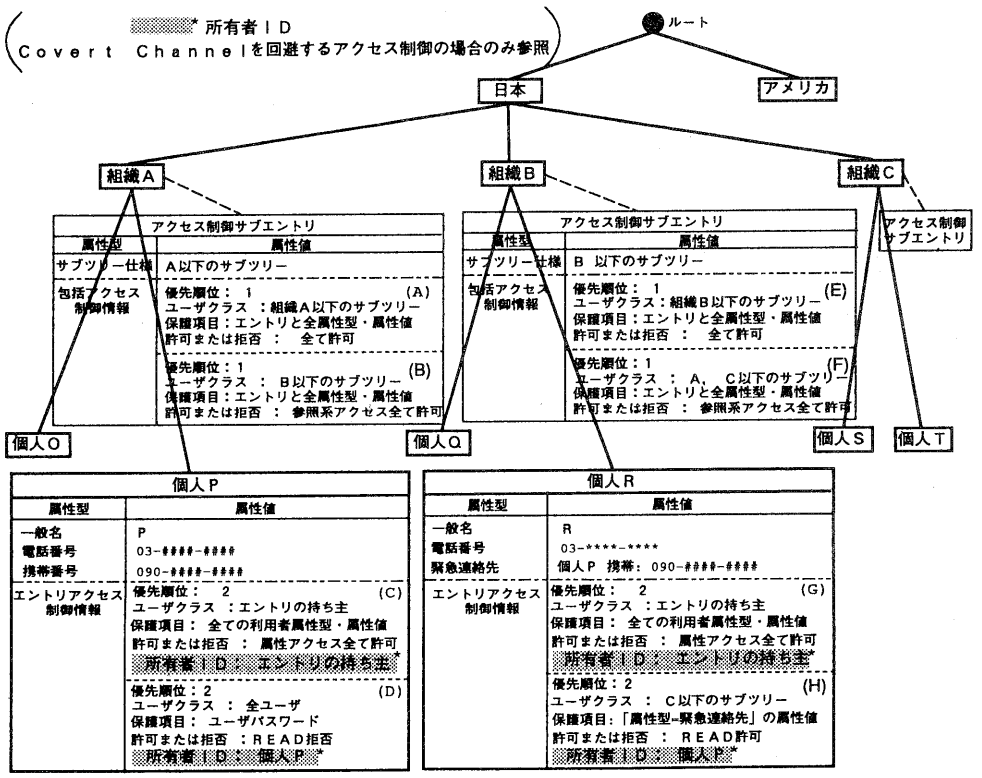

図 5: X.501 アクセス制御における Covert Channel の回避