電子証明書を用いた情報の信頼性評価を伴う検索方式

宮川祥子† 清木康††

本論文では,電子証明書を用いて情報の信頼性を評価する機能を有する情報検索システムの実現方式を提案する.本方式では,情報検索システムに含まれているデータの信頼性を,インターネット上で属性の証明に用いられる属性証明書によって検証することにより,情報の信頼性評価を伴う検索を実現する.これによって,インターネット・オークションや求人求職データベースなど,不特定多数の利用者が情報を登録する環境において,検索された情報の信頼性を評価することが可能となる.本方式の特徴は,信頼性評価機能と情報検索機能の連結を,マルチデータベースシステムによって実現している点にある.マルチデータベースシステムは,異種のシステムを直接連結するのではなく,各既存システムを統合機能によって連結する.インターネット上には様々な種類の情報検索システムが存在するが,本提案方式ではマルチデータベースシステムを用いて既存システムを連結することでことにより,種々の既存システムにを対象として信頼性評価機構を連結させることが可能となる.さらに,本論文では,具体的に関係データベースシステムと信頼性評価機構の連結を,マルチデータベースシステム上で実現する方式を示し,その実現方式に従った実験システムを構築し,本提案方式の実現可能性及び有効性を明らかにする.

A Method of Information Retrieval with Credibility Evaluation using Digital Certificate

Shoko Miyagawa † and Yasushi Kiyoki††

In this paper we present a method for implementing an information retrieval method with the mechanism for ensuring data credibility by use of digital certificate. We use digital certificates distributed on the Internet to identify attributes. This method realizes information retrieval for ensuring credibility of the data in the environment where general unspecified people register their information to the database, as internet auctions or job matching systems. The feature of this method is to integrate the mechanism for ensuring data credibility with information retrieval by using a multidatabase system. Due to this integration mechanism, various kinds of new systems on the Internet can be combined with credibility evaluation mechanism. We also describe the concrete method of implementation which combines relational database system and credibility evaluation mechanism on the multidatabase system. We construct an experimental system accorging to the implementation method, and evaluate the availability and validity of the method.

1. はじめに

データベースシステムは,様々な組織内の情報を総合的に管理するシステムとして利用されてきたが,これまでの利用は,特定少数の管理者がデータベースの内容の登録や更新を行い,利用者がデータベースに対して検索を行うということを基本としていた.ここには,少数の管理者がデータの内容についても管理を行い,データ登録時にデータの正しさについて確認を行っているという暗黙の前提があった.

しかし,今日では,このようなデータベースの利用方法を前提としないアプリケーションが増加している.例えば,インターネット・オークションでは,物を売りたい利用者が,オークションサーバのデータベースに情報を登録し,買いたい利用者がその情報を参照してオークションに参加している[1),2)].また,求職者と求人者を結びつけるジョブ・マッチング・システムでも,求職者や求人者がそれぞれの情報を登録し,自由に検索をするという形式の機能が実際に提供されている[3)].このようなアプリケーションでは,情報の登録は少数の管理者によってではなく,不特定多数の利用者によって行われることを前提としている.

このような,不特定多数の情報登録者が存在する状

† 慶應義塾大学 政策・メディア研究科
Graduate School of Media and Governance, Keio University
†† 慶應義塾大学 環境情報学部
Faculty of Environmental Information, Keio University

況では,従来のデータベースシステムの利用方法を前提としてデータベース内の情報の「正しさ」を保証することは困難である.データベースに登録された情報の正しさが保証されない場合,電子商取引においては,商品や売り手の情報が詐称される可能性がある.また,ジョブ・マッチング・システムにおいては,求職者の経歴・資格や求人をしている会社の業績・規模などが詐称される可能性がある.このような可能性は,インターネットにおける情報提供および獲得のリスクを拡大し,その発展を阻害する要因となるため,このようなリスクを回避するためのシステムの構築が求められている[9),10)].

本論文では,従来のデータベースと,情報の正しさを保証する情報リポジトリを連結することにより,データベース中の情報の信頼性評価が可能な情報検索機構を提案する.本方式における情報リポジトリと信頼性評価は,現在インターネット上で標準化が進んでいる,公開鍵インフラストラクチャ (Public Key Infrastructure:PKI) の規格に則った形で実現する.PKI とは,広域分散ネットワークにおいて,公開鍵暗号系と公開鍵の正しさを証明する電子証明書(公開鍵証明書)などを用いた本人認証の方式である.PKI では,インターネット上において,公開鍵証明書を用いることにより,ある秘密鍵を持つ人物を一意に特定することが可能であり,これによって通信相手の認証を実現している.また,PKI では,ある人物の権限や資格といった属性情報の正しさを,属性証明書によって検証する仕組みが提案されている[29),33)].本方式では,データベースに登録された情報の正しさを保証する手段として,属性証明書を用いる.

本方式におけるデータベースと情報リポジトリの連結にあたっては,両者を直接結びつけるのではなく,これまで我々が提案してきたマルチデータベースの手法を用いた[4)~6),15)~17)].これにより,システムに新たな種類のデータベースが加わった場合でも,システム全体を改変することなく,新たなデータベースに対して信頼性評価機構を連結させることが可能となる.

本研究の関連研究としては,関係データベースにおけるセキュリティ手法,属性証明書を用いたアクセス制御,データベースとインターネット上の情報を連結する手法が挙げられる.従来の関係データベースシステムにおけるセキュリティ手法では,情報の正しさに関する検証は,パスワード等を用いたユーザ認証と,アクセス権の委譲によって実現される範囲に限られていた[18)].本提案がこれらの手法と本質的に異なる点は,上記の手法は,読み込み・書き込みなどのアクセス制御に関する情報の正しさについての検証が主とした目的であり,データベースに登録される情報の正しさの検証については,登録された時点で正しいものであるということが暗黙的な前提となっているのに対して,本提案では,データベースに登録される情報の正しさを検証しているという点である.

また,属性証明書を用いたアクセス制御については,PKI の分野における関連研究として,属性証明書や電子的に表現された属性情報を用いてアクセス制御を行う手法について提案がされている[14),32),33)].本提案がこれらの手法と異なる点は,上記の手法が属性情報や属性証明書をアクセス制御の手段として用いているのに対して,本提案では,属性証明書をデータベースに登録されている情報の信頼性を保証するために適用している点である.

データベースとインターネット上の情報を連結する手法については,データベースを用いてWWW 上の情報の一貫性を管理するシステムが提案されている[31)].本論文の提案がこの提案と本質的に異なる点は,データベースに登録されている情報の信頼性をインターネット上の情報を用いて保証する試みであるという点である.

2. 電子証明書による情報の信頼性付与

本章では,PKI の中核である,電子証明書と証明書リポジトリを用いた認証基盤について概説する.本論文における方式は,ここで示す認証基盤を利用することを前提とした方式として実現される.ただし,属性証明書については現在規格化が進行中であるため,独自の形式を用いることとする.本章では,本論文で前提とする属性証明書の形式についても述べる.

2.1 電子証明書と PKI

電子証明書とは,電子署名によって,内容の非改ざん性が保証されたデジタル情報である.現在,電子証明書は,主として公開鍵の証明に用いられている.公開鍵暗号系では,相手を識別し,安全に通信を行うためには,通信したい相手の公開鍵をあらかじめ入手しておく必要があるが,その公開鍵が本当に相手のものであるかについては,公開鍵暗号系では検証できない.そこで,現在,認証局 (Certificate Authority:CA) と呼ばれる「信頼できる第三者機関」が公開鍵証明書を作成し,その公開鍵の信頼性を保証するという手段が用いられている.公開鍵証明書には,CA の電子署名が付加されている.電子署名は,公開鍵証明書の内容の非改ざん性を保証しているとともに,電子署名を行った署名者が本当に自分が思っている相手であり,悪意を持った第三

者によるなりすましでないことを検証する手段として用いられている. 公開鍵証明書を受け取った検証者は, 電子署名を行ったCAを信頼することで, 証明書に記載された公開鍵が正しいものであることを確認できる.

このような, 公開鍵暗号系に基づく, 通信における本人確認とセキュリティの確保を実現するために, 公開鍵インフラストラクチャ(Public Key Infrastructure: PKI) と呼ばれる基盤の整備が進められている. 代表的なPKIとしては, ISO/IEC/ITUによるX.509[28]がある. インターネットにおける規格の標準化を進めている団体であるIETF(Internet Engineering Task Force) のPKIX Working Groupでは, X.509に基づいたPKIを利用するためのプロトコル群について検討を行っており, その成果はRFC(Request For Comment) とよばれる勧告としてまとまりつつある[12]. PKIX Working Groupでは, 公開鍵証明書の正しさを検証する際に, 解釈のばらつきが出ないようにするために, X.509 version3に対応した公開鍵証明書のフォーマットを定義している[19)~23)].

2.2 属性証明書

公開鍵証明書は, 公開鍵とその所有者とを対応づける認証の仕組みを提供しているが, 公開鍵証明書によって証明できるのは通信相手が本人であるかどうかという点のみであり, 公開鍵証明書では, 公開鍵の所有者がどのような資格などを持っているかという属性情報を表現することは困難である. X.509 公開鍵証明書に, 資格などの属性情報を組み込むこと自体は可能であるが, そのような情報を組み込んだ公開鍵証明書は, プライベートな情報を含んでいるため, 汎用的な利用が難しい. 例えば, 通信をする際に, 本人であることを確認するために公開鍵証明書を通信相手に送る場合, 公開鍵証明書に属性情報が記載されていると, 伝える必要の無い属性情報まで相手に伝わってしまう可能性がある. これは, OECDによるプライバシー保護に関するガイドライン[35]に抵触するため, 回避することが望ましい. また, 所属する組織や資格といった属性が変化した場合には, 属性を更新するために公開鍵証明書全体を更新しなければならないため, 公開鍵証明書を発行する認証機関との間に, 本来であれば不要なトランザクションが発生する.

公開鍵証明書に属性情報を組み込むことには, 上記のような問題点があるため, 公開鍵証明書とは別に, それぞれの属性情報を証明の対象として発行される属性証明書が提案されている. IETF のPKIX Working Groupでは, X.509v3 形式を用いた属性証明書が提案されているが, この他にもSPKI[33]やNetBill[34]など

バージョン番号
証明対象者名
発行者名
シリアル番号
有効期限
公開鍵 (空)
属性情報 (X.509 v3 extention)
署名

図1 X.509 v3 属性証明書フォーマット
Fig. 1 X.509 v3 attribute certificate format

の規格が提案されている. また, 属性証明書や属性情報を用いたアクセス制御機構も提案されている[14),32)].

公開鍵証明書は, SSLやS/MIMEなど, 本人確認を必要とするアプリケーションで用いられており, 実質上, インターネット上の本人確認の手段となっている. 他方で, 属性証明書には本人確認の手段となる公開鍵が含まれていないため, 属性証明書を用いる際には, 公開鍵証明書と組み合わせて利用する必要がある.

2.3 証明書リポジトリ

公開鍵証明書や属性証明書を用いたシステムを構築する際には, これらの証明書をいつでも確実に入手できる環境が必要である. また, 公開鍵証明書や属性証明書が確実に本人のものであるということを確認できる必要がある. このための仕組みとして, ディレクトリサーバを用いた証明書リポジトリが提案されている.[22)]証明書リポジトリとは, 電子証明書の貯蔵庫であり, X.500等の分散ディレクトリ技術を用いることで分散的に管理することができる. 公開鍵暗号系において, 公開鍵と秘密鍵のペアを持つ主体 (人物, サーバ, サービスなど) をエンティティと呼ぶ. あるエンティティの公開鍵証明書は, 認証機関を通じて証明書リポジトリ内の該当するエンティティを表現するエントリの下に登録される. 現時点では, 証明書リポジトリは公開鍵証明書と証明書失効リスト (CRL) を格納する機構として提案されている.

現在, IETF PKIX Working Groupにより, X.500ディレクトリを用いた証明書リポジトリが提案されている. X.500では, ディレクトリが管理する情報の構成要素であるエントリをDistinguished Name(DN) と呼ばれる識別子で一意に定める. 各エントリは, 上位のエントリからそのエントリを一意に識別可能とするためのRelative Distinguished Name(RDN) と呼ばれる名称を持つ[27)]. DNは, ディレクトリのルートからそのエントリまでのRDNの列として定義される. X.500ディレクトリにアクセスするためのプロトコルとして,

LDAP(Lightweight Directory Access Protocol)が用いられている[24),25)]. LDAP Version2を用いて証明書リポジトリへの読み出し,検索,書き込みの3オペレーションを実現するための規格として, OPP LDAPがRFCとして規格化されている[22)]. また, PKIにおけるエンティティやCAをLDAP version2で扱うためのオブジェクトクラスや属性が決められている.[26)]

2.4 電子証明書の検証

電子証明書の正しさは,証明書に添付されている認証局の電子署名をCAの公開鍵によって検証することにより確認することができる. しかし,一方で, CAの公開鍵が正しいものであるかどうかを判断するためには,認証局の公開鍵の公開鍵証明書が必要となる. X.509では上位のCAが下位のCAを証明するという階層的な構造が実現可能であるため,あるCAによって発行された電子証明書が正しいものであるかを確認するためには, CAの階層を上にたどっていき,最終的にルートCAと呼ばれる認証局にたどり着くことを確認すればよい. しかし,この方式を実現するための階層構造は実装されていないため, Netscape Navigatorなどの実際のインターネットアプリケーションでは,「信頼できるCA」の公開鍵をあらかじめアプリケーションに組み込んでおくという方式をとっている. この方式では,提出された証明書の署名が,アプリケーションに組み込まれたCAの公開鍵によって検証できれば,その証明書を信頼できる証明書であると検証する.

2.5 本提案における前提

本論文では,これまで概説したPKIの各種規格の利用を前提とした,情報の信頼性を評価する機構を提案する. 本提案では,現在のPKIにおける規格に則ると同時に,規格に反しないいくつかの前提を置く. 本提案で前提とする内容は,以下の通りである.

- X.509形式の公開鍵証明書及び属性証明書
  本提案では,公開鍵証明書及び属性証明書の形式として, X.509v3形式の電子証明書を用いることを想定する. 本提案における属性証明書は,公開鍵証明書のフォーマットのうち,公開鍵を格納するSubjectPublicKeyInfoを空とし, X.509 v3 Extensionに属性情報を格納することによって実現する(図1). 同様の方式は,文献11)においても提案されている.
- X.500ディレクトリにおける電子証明書の格納方式
  本提案では,証明書リポジトリとしてX.500ディレクトリを用いることを想定する. また,証明書リポジトリの各エントリにおける,電子証明書を格納する属性名として,文献26)で提案されているuserCertificateを用いる. また,本提案における属性証明書は,公開鍵証明書との対応づけの方法として,属性証明書と公開鍵証明書を,証明書リポジトリの同一エントリの下に置き,各証明書の上位エントリのDNの同一性を比較することで対応づけを行う. したがって,本提案では,同じエンティティの公開鍵証明書と属性証明書は,そのエンティティを表現する同一のエントリの下に置かれることを想定する.
  証明書リポジトリには,常に正しい公開鍵証明書と属性証明書が登録されていることを前提とする. また,権利を持たない利用者による不正な書き込みや読み出しを防ぐため,証明書リポジトリはセキュアに管理されていることが前提となる.
- 電子署名の検証
  電子署名の検証は,公開鍵暗号系に基づいて行うことを想定する. また,CAの信頼性の判断方法については,現在Netscape Navigator等で採られている方法と同様に,信頼できるCAの公開鍵をアプリケーション側で保持するという方法を採る.

3. 提案方式

本節では,提案する検索方式の概要を示す. 本方式では,パターンマッチング型検索システムに格納されたデータの信頼性を,インターネット上の証明書リポジトリに格納された属性証明書によって評価する機構を実現する.

3.1 提案方式の概要

本方式における情報の信頼性付与モデルを図2に示す. パターンマッチング型検索システムには,各エンティティ(図2ではAlice, Bob)に関する情報が,信頼性評価の対象となる属性情報とその属性を証明する属性証明書のDNとともに格納される. 図2では,資格(qualification)が信頼性評価の対象となる属性であり,それぞれの資格を証明する属性証明書のDNが資格とともにデータベースに格納されている. 他方,インターネット上に存在する証明書リポジトリには,認証局から発行された公開鍵証明書や属性証明書が格納されている. 同一のエンティティに対して発行された電子証明書は,証明書リポジトリにおいてそのエンティティを表現するエントリの下に格納される.

本方式は,このモデルに基づき,情報の信頼性評価を伴う検索を実現するためのものである. 本方式は,次の3基本機能によって実現される.

- パターンマッチングによる検索機能

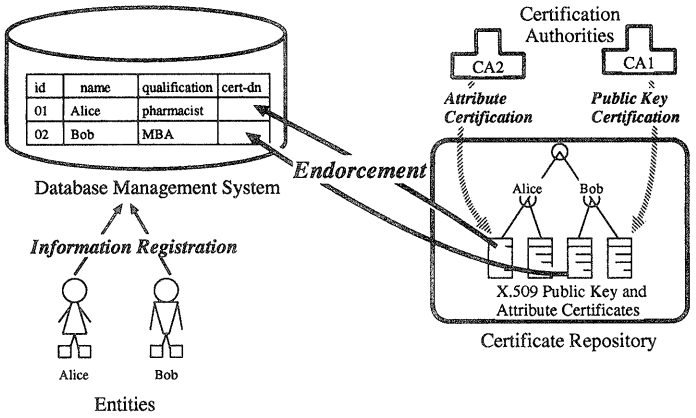


図2 属性証明書による情報の信頼性付与モデル
Fig. 2 Information endorcement model using attribute certificate

- 証明書リポジトリ検索機能
- 両機能の統合と属性証明書の検証を行う機能

3.2 基本機能1:パターンマッチングによる検索機能

データベースには,信頼性評価の対象となる属性とその属性を証明する属性証明書のDNなどが格納されている.関係データベースシステムの基本機能により,与えられたキーワードと同じパターンを持つデータ群を取得する.

パターンマッチングの対象となるデータが,以下に述べる証明書リポジトリ検索と属性証明書の検証の対象となるためには,パターンマッチングの対象となるデータには,以下の属性が含まれていることが前提となる.

- エンティティの公開鍵証明書のDN
- 信頼性評価の対象となる属性
- 属性証明書のDN
- エンティティによる,データベースに登録されたデータを対象とした電子署名

また,上記データ中の信頼性評価の対象となる属性と,対応する属性証明書中で証明されている属性は,同じドメインからの値を取るものと仮定する.すなわち,属性証明書が信頼性評価の対象となる,ある属性を証明しているかどうかは,信頼性評価の対象となる属性と属性証明書中で証明されている属性の値の同一性によって判定される.

3.3 基本機能2:証明書リポジトリ検索機能

証明書リポジトリ検索機能では,与えられた証明書DNに基づいて,証明書リポジトリから該当する属性証明書を取得する機能を実現する.この際,与えられたDNが本当に検証の対象となるエンティティの属性証明書を示すものであるかを検証する必要がある.これは,パターンマッチング型検索の対象となるデータに,検証の対象となるエンティティの電子署名を格納しておき,その電子署名を検証できる公開鍵を証明する公開鍵証明書のDNと,属性証明書のDNを比較することにより行う.

属性証明書DNの検証は,以下の手順によって実現される.

(1) パターンマッチング検索により得られた公開鍵証明書DNを用いて,証明書リポジトリを検索し,対応する公開鍵証明書を取得する.
(2) (1)で得られた公開鍵証明書に格納された公開鍵を用いて,パターンマッチング型検索システムに登録されているエンティティの電子署名を検証する.
(3) 属性証明書のDNと公開鍵証明書のDNを解析し,両証明書の最下位のRDNを除く上位RDNの同一性を検証する.
(4) (2)(3)の両者が正しく検証できれば,属性証明書が評価の対象となる属性を持つエンティティのものであることが確認できる.

3.4 基本機能3:両機能の統合と属性証明書の検証

基本機能3は,基本機能1および2を統合し,得られた属性証明書を検証する機能を実現する.本機能は,既存のシステムを直接連結するのではなく,各既存システムをメタデータベースシステムによって連結する.[4)~6)] 統合機能と各既存システムはそれぞれ以下のような方式により連結される.

- パターンマッチングによる検索機能との連結
  データベースに格納されたデータ群は,パターンマッチングによる検索によりフィルタリングされる.統合機能は,フィルタリングされたデータのう

ち, 検索者によって指定された属性群に対応するデータ集合に加えて
- 識別子
- エンティティの電子署名
- エンティティの公開鍵証明書の DN
- 信頼性評価の対象となる属性
- 属性証明書の DN

に対応するデータ群を得る.

- 証明書リポジトリ検索機能との連結
  統合機能は, 証明書リポジトリ検索機能に, フィルタリングされたデータ群のうち, 公開鍵証明書 DN, 属性証明書 DN に対応するデータを渡す. 証明書リポジトリ検索機能は, 属性証明書 DN と公開鍵証明書 DN の対応を検証した後, 該当する属性証明書を得る.

統合機能は, 基本機能 1 および 2 の連結により得られた属性証明書について, それが正しいものであるかを検証する. さらに, 検証結果に基づき,3.3(1) で得られたデータのうち, 属性証明書が正しく検証されたもののみをフィルタリングし, さらに, それらのデータ群のうち検索者によって与えられた属性群に対応するデータ集合を結果として出力する.

属性証明書検証の手続きは以下のような手順により行われる.

(1) 属性証明書の解析
  属性証明書を解析し, 証明書内の証明されている属性と電子署名を抽出する

(2) 属性の検証
  (1) で得た属性と検証の対象となる属性を比較し, 同一のもののみをフィルタリングする.

(3) 電子署名の検証
  検証者の保持する「信頼できる認証局リスト」に登録されている公開鍵で (1) で得られた電子署名が検証可能であれば, 証明書全体が正しいものであるということが検証される

4. データ構造と基本演算子

ここでは, パターンマッチングによる検索機能, 証明書リポジトリ検索機能の両機能を有し, 属性証明書の検証結果に基づく情報検索を行うシステムを実現するための基本データ構造と基本演算子について述べる.

4.1 パターンマッチングによる検索系におけるデータ構造と基本演算子

パターンマッチングにおける検索系として, 関係データベースシステムのデータ構造および基本演算子を用いる[5]. データ構造は, 関係 (relation) とし, 基本演算子を次のように定義する.

- (select [rel] [att] [cond] [val])
- (project [rel] [att-list])
- (join [rel1] [att1] [rel2] [att2] [cond])
- (union [rel1] [rel2])
- (diff [rel1] [rel2])

ここで, rel, rel1, rel2 は関係, att, att1, att2 は属性, att-list は属性リスト, cond は検索条件, val は値をそれぞれ意味する.

4.2 証明書リポジトリ検索系におけるデータ構造と基本演算子

証明書リポジトリ検索系におけるデータ構造, および基本演算子を示す.

証明書リポジトリ検索系におけるデータ構造として, X.500 ディレクトリを用いる. 基本演算子は, X.500 ディレクトリに対する検索である. パラメータとして, DN, フィルタ, 属性リストを指定する.

この演算子を次のように定義する.

- (repository_search [dn] [filter] [att-list])

ここで, dn は DN, filter はフィルタ, att-list は属性リストをそれぞれ表す.

4.3 提案方式のデータ構造と基本演算子

提案方式において対象とするデータ構造は, パターンマッチングによる検索系における関係, および, 証明書リポジトリを構成している X.500 ディレクトリ, および, X.509 属性証明書である.

パターンマッチングによる検索と証明書リポジトリ検索の両機能の統合を実現するために, これらの機能を合わせ持つ演算子を導入する.

本演算子の入力パラメータとして, 検索対象となる関係あるいは関係を生成する式, エンティティの電子署名を格納する属性, 公開鍵証明書の DN を格納する属性, 信頼できる認証機関の公開鍵リスト, 信頼性評価の対象となる属性を格納する属性, 属性証明書 DN を格納する属性を指定する. 返り値として, 引数で指定した関係に属性証明書の検証値が付加された関係が得られる. この演算子を次のように定義する.

- (credential_selection [rel] [sig] [cert-dn] [cert-list]([credible-att] [att-dn]))

ここで, rel は関係もしくは関係を生成する式, sig は電子署名を格納する属性, cert-dn は公開鍵証明書の DN を格納する属性, cert-list は信頼できる認証機関の公開鍵を格納するファイル名, credible-att は信頼性評価の対象となる属性, att-dn は属性証明書の DN を格納している属性をそれぞれ表している. credible-att と att-dn の組は, 複数個記述することができる.

この基本演算子の動作を次に示す.

(1) 入力として与えられた関係, 属性リスト, 検索条件に基づいて関係に対してパターンマッチング検索を行い, 得られた結果に
- 識別子
- エンティティの電子署名
- 公開鍵証明書の DN
- 信頼性評価の対象となる属性
- 属性証明書の DN

を付け加える. これらの値を格納している属性名は, 入力パラメータとして指定されている. これに加えてさらに,
- 属性証明書の検証結果

を格納する属性を付加する. この時点では, 属性証明書の検証結果は空である.

(2) (1) で得られた各タプルの公開鍵証明書 DN に対応する公開鍵証明書を証明書リポジトリから取得し, 得られた公開鍵証明書に格納された公開鍵を用いて, (1) で得られた電子署名の検証を行う.

(3) (1) で得られた各タプルの属性証明書 DN を抽出し, 公開鍵証明書 DN と比較して正しい DN であるかを検証し, 正しいと検証された属性証明書 DN について, 証明書リポジトリから対応する属性証明書を取得する.

(4) 属性証明書を解析し, 格納されている属性値と検証される必要のある属性値が同一かどうかを判定する. 同一のものについては, 電子署名の検証を行い, (1) で得られた識別子, 検証結果からなる組を生成する.

(5) (4) で得られた検証結果を (1) で作成した関係中の「属性証明書の検証結果」属性に格納する.

5. 提案方式の実現

提案方式は, マルチデータベースシステムによって, 関係データベースと X.500 ディレクトリを連結することによって実現される. このマルチデータベースシステムは,
- マルチデータベース管理システム
- ローカルシステム

の 2 システムによって実現される (図 3). マルチデータベース管理システムは, マルチデータベースシステムを実現するためのモジュールであり, マルチデータベース問い合わせ処理系, メタデータベースシステム, 関連性評価機構からなる.

マルチデータベース問い合わせ処理系は, マルチデータベースに与えられた問い合わせを処理するシステムである.

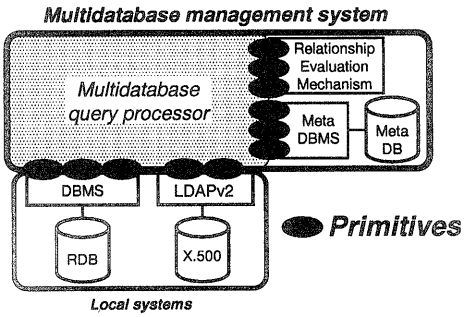


図 3 マルチデータベースシステムの構成
Fig. 3 The structure of a multidatabase system

メタデータベースシステムは, 異種のローカルシステムにおけるデータの結合と演算を実現するために必要な情報を管理するシステムである.

関連性評価機構は, メタデータベースに格納されたデータ群に対して, 同一性, 真正性, 包含性などの関連性を評価する機構である.

ローカルシステムは, それぞれが独自のサービスに必要なデータを管理し, 問い合わせに応じてローカルシステム内で処理を行い, 結果を出力するシステムである.

以下では, ローカルシステムを構成するパターンマッチングによる検索システムと証明書リポジトリ検索システム, マルチデータベース管理システムを構成するマルチデータベース問い合わせ処理系, メタデータベースシステム, 関連性評価機構について, それぞれの実現方式を述べる.

5.1 パターンマッチングによる検索システム

パターンマッチングによる検索システムは, 関係データベースシステムのアプリケーションとして実現される. 本実現では, パターンマッチングの対象となる関係は, 以下の属性を含んでいることを前提としている.
- エンティティの公開鍵証明書の DN
- 信頼性評価の対象となる属性
- 属性証明書の DN
- エンティティの電子署名

5.2 証明書リポジトリ検索システム

証明書リポジトリ検索システムは, X.500 ディレクトリのアプリケーションとして実現される. ディレクトリへのアクセスには LDAP v2 プロトコルを用いる. 証明書リポジトリは, 各エンティティを表すエントリの下位エントリとして公開鍵証明書と属性証明書が組み込まれているという構造を持つ.

5.3 マルチデータベース問い合わせ処理系

マルチデータベース問い合わせ処理系は,検索者の問い合わせを解釈し,パターンマッチング型検索システムと証明書リポジトリ検索システムへの基本演算子の列に変換する.また,生成した基本演算子の組みを,対応するローカルシステムに対して発行し,その検索結果をメタデータベースシステムに引渡す.さらに,検索者の問い合わせに基づき,関連性評価機構に対して,関連性評価問い合わせを発行し,得られた結果を統合して検索者に対し出力する.

5.4 メタデータベースシステム

メタデータベースシステムは,関係データベースのアプリケーションとして実現される.メタデータベースシステムは,マルチデータベース問い合わせ処理系を通じて得られた各ローカルシステムにおける問い合わせ実行結果を格納し,マルチデータベース問い合わせの対象となるデータ群を生成する.このデータ群は,パターンマッチング検索によって得られた関係に,4.3節の(1)で挙げた属性を加えたものである.

5.5 関連性評価機構

関連性評価機構は,メタデータベースシステムから得られたデータを対象として,関連性の評価を行う.関連性評価機構は,X.509電子証明書解析モジュールと,公開鍵暗号モジュールを用いて実現されている.関連性評価機構は,メタデータベースに格納されたデータのうち,電子署名と公開鍵証明書を用いて本人確認を行い,公開鍵証明書のDNと属性証明書のDNを比較することで属性証明書の証明対象者を確認し,さらに属性証明書を検証し,評価の対象となるデータの信頼性を評価する.

6. 実　　験

ここでは,パターンマッチングによる検索と証明書リポジトリの検索と属性証明書の検証をメタレベルによって連結することによって実現される,情報の信頼性評価機構を有する情報検索方式の有効性を検証する.

6.1 実験環境

5節で示した実現方式によって,実験システムを構築した.ローカルデータベースとメタデータベースにはPostgreSQL 6.4を,証明書リポジトリであるX.500ディレクトリにはOpenLdap1.2.8を用いた.また,属性証明書の発行と検証には,AiCA0.65b[30]を改変したものを用いた.マルチデータベース問い合わせ処理系はPerl5.004で実装した.使用した計算機は,Sun Ultra1,OSはSolaris2.5.1である.PerlからPostgreSQL6.4を呼び出すインタフェースとしてpgsql_perl5-1.8.1を,PerlからOpenLdap1.2.8を呼び出すインタフェースとしてperl-ldap0.13をそれぞれ用いた.

実験では,ジョブ・マッチング・システムにおける求職者データベースを想定したデータを用いた.データベース中で信頼性評価の対象となる属性は,各求職者の保有する資格と,業務における経験である.パターンマッチング型データベースには、登録者であるエンティティの名前,電子署名,公開鍵証明書のDN,居住地域,生まれた年,資格,資格を証明する属性証明書のDN,業務経験,業務経験を証明する属性証明書のDNが含まれている.実験に用いた関係データベースのスキーマおよびデータの一部を表1に示す.

証明書リポジトリには,パターンマッチング型データベースに格納されている各タプルに対応するエンティティの公開鍵証明書と,資格・業務経験のそれぞれの属性証明書を格納した.証明書リポジトリのディレクトリ構造は,地域的な階層構造によった.図4に証明書リポジトリのエントリの一部を,図5にエンティティの属性証明書の一部を示す.全ての公開鍵証明書は,単一の認証局によって発行されたものとし,その認証局の公開鍵証明書をCA.certというファイルに格納した.それぞれの属性証明書は,その資格や経験を証明する団体によって発行されていることを仮定している.例えば,第一種情報処理技術者の資格であれば,財団法人日本情報処理開発協会に,薬剤士の資格であれば厚生省にそれぞれ付属する認証局,あるいはそれぞれの組織から業務を委託された認証局が,該当する資格に関する属性証明書を発行と,証明書リポジトリへの登録を行う.同様に,ある病院での業務経験があることを証明する属性証明書は,その病院に付属する認証局,あるいはその病院から業務を委託された認証局が行うものとする.資格・業務経験保持者と証明書リポジトリの登録ポイントとのマッチングは,資格・業務経験保持者の電子署名を検証する等の方法によって,属性証明書を登録する際に,認証局によってあらかじめ確認されているものとする.

6.2 実験方法

6.2.1 実　験　1

実験1に用いた問い合わせを図6に示す.問い合わせは,4章で定義した基本演算子群を組み合わせて記述される.実験1では,基本演算子selectにより,資格(qualification)が第一種情報処理技術者(Class I Information-Technology Engineer)である集合をパターンマッチングにより選択し,その結果を対象として基本演算子credential_selectionを実行することにより,第一種情報処理技術者の資格が属性証明書によっ

表1 実験で用いた関係データベースのデータの一部
Table 1 A part of definitions used in the experiment.

name	signature	pubkey-cert-dn	region	year-of-birth	qualification
person1	05fc8f...	cn=person1, o=resident st=kanagawa, c=JP	kanagawa	1969	Class I Information-Technology Engineer
person2	ee11a8...	cn=person2, o=resident, st=kanagawa, c=JP	kanagawa	1965	Test of English Proficiency grade pre 1
person3	4e58cd...	cn=person3, o=resident, st=kanagawa, c=JP	kanagawa	1966	pharmacist
person4	3a316e...	cn=person4, o=resident, st=tokyo, c=JP	tokyo	1963	
person5	b8490...	cn=person5, o=resident, st=tokyo, c=JP	tokyo	1975	pharmacist

≈

q-cert-dn	experience	exp-cert-dn
serialNumber=1, cn=person1...	database programming	serialNumber=2, cn=person1...
serialNumber=1, cn=person...		serialNumber=2, cn=person2...
serialNumber=1, cn=person3...	service in hospital	serialNumber=2, cn=person3, o=resident...
	database programming	serialNumber=2, cn=person4...
serialNumber=1,cn=person5...		

≈

表2 実験1の結果
Table 2 The result of the experiment 1.

name	region
person1	kanagawa
person7	saitama
person12	kanagawa
person13	tokyo
person22	kanagawa
person23	chiba

表3 実験2の結果
Table 3 The result of the experiment 2.

name	region	year-of-birth
person3	kanagawa	1969
person7	saitama	1974
person8	chiba	1966
person13	tokyo	1971
person22	kanagawa	1971
person26	saitama	1970

て検証可能なデータ群のみをフィルタリングする. その後, 名前 (name) と居住地域 (region) を基本演算子 project により抽出している.

実験1の結果を表2に示す.

6.2.2 実 験 2

同様の実験を, 図7に示す問い合わせを対象として行った. 実験2の結果を表3 に示す. ここでは,1965年以降に生まれた人で, データベースプログラミング (database programming) の業務経験 (experience) を持ち, その業務経験に対する属性証明書が検証可能な人の名前 (name), 居住地域 (region), 生まれた年 (year_of_birth) を検索している.

6.2.3 実 験 3

同様の実験を, 図8に示す問い合わせを対象として行った. 実験2の結果を表4に示す. ここでは, 神奈川県在住 (kanagawa) で薬剤士 (pharmacist) の資格を持っており, 病院での業務経験 (searvice in hospital) があり, その資格と業務経験に対する属性証明書が検証可能な人の名前 (name) と生まれた年 (year_of_birth) を検索している.

表4 実験3の結果
Table 4 The result of the experiment 3.

name	year-of-birth
person3	1966
person15	1973
person29	1974
person30	1969

6.3 考 察

これらの実験を通じて, 指定した属性に対する属性証明書が検証可能なもののみが検索されることを確認した.

実験1においては, 求職者データベースから, 特定の資格を持ち, その資格が属性証明書によって証明できる人物を検索している.

実験2においては, 求職者データベースから, 特定の経験を持ち, その経験が属性証明書によって検証できる人物を検索している.

実験3においては, 求職者データベースから, 特定の資格を持ち, かつ特定の経験を持った人物のうち, それぞれの資格・経験が属性証明書によって検証できる人

```
issuer: /C=JP/ST=kanagawa/O=attribute_certificate_authority_2/
        CN=attribute_certificate_authority_2/
        EMAIL=aca2-adm@quattro.sfc.wide.ad.jp
subject: /C=JP/ST=kanagawa/O=resident/CN=person7/
         EMAIL=person7@resident.kanagawa.jp
serial: 1
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=JP, ST=tokyo,
            O=Japan Information Processing Development Center,
            CN=Japan Information-Technology Engineers Examination Center,
            /Email=email@certification_authority.or.jp
    Validity
      Not Before: Sat Dec 18 12:03:09 1999
      Not After : Sun Dec 17 12:03:09 2000
    Subject: C=JP, ST=saitama, O=resident, CN=person7,
             /Email=person7@resident.saitama.jp
    Subject Public Key Info:
    X509v3 extensions:
      Attribute Qualification:
        Class I Information-Tschnology Engineer
      Attribute Experience:
  Signature Algorithm: md5WithRSAEncryption
    19:47:42:6b:58:24:bd:6c:23:bf:ad:df:f9:a8:0e:9f:b5:87:
    0a:af:ba:e5:d8:61:7c:35:49:b0:c1:70:0d:06:63:07:91:f6:
    (以下略)
```

図4 実験に用いた属性証明書の例
Fig. 4 An sample attribute certificate for the experiment.

物を検索している.

従来のデータベース検索では, 登録されているデータの信頼性は, データ登録時に別の手段によって保証されているということを暗黙の前提としてきた. このため, ジョブ・マッチング・サービスにおける求職者データベースのように, 不特定多数の情報登録者が存在する状況では, 登録されている情報の信頼性を保証することが困難であった. 本論文の提案方式は, インターネット上において情報への信頼性付与に利用されている電子証明書を, データベースに登録されたデータの信頼性評価に用いることにより, 情報の信頼性評価に基づく検索を実現した.

7. 結 論

本論文では, 電子証明書を用いてデータベースに登録された内容の信頼性を評価する方式を提案した. 本提案方式は, マルチデータベースシステムを用いることにより, 情報検索機能および信頼性評価機能を直接連結するのではなく, 各機能を統合するメタレベル情報検索機能および信頼性評価のマルチデータベースシステム環境によって実現している. これによって, さらに異種の機能を連結する際にも, 連結する機能とメタレベルのシステムの間の基本演算を定義することにより, それらの機能を連結することが可能となる. インターネット上には, 関係データベース以外にも, 様々な種類の情報検索システムが存在するが, これらの情報

```
dn: serialNumber=1, cn=person1, o=resident, st=kanagawa, c=JP
serialNumber: 1
cn: attributeCertificate
cn: person1
sn: person1
st: kanagawa
organizationalStatus: resident
mail: person1@resident.kanagawa.jp
userClass: Graduate of A University
objectclass: person
userCertificate;binary:: MIICPzCCAaigAwIBAgIBATANBgkqhkiG9w
                         0BAQQFADCBqDELMAkGA1UEBhMCSlAxETAPBgNVBAg...
                         (PEM 形式でエンコードされた属性証明書)
```

図5 実験に用いたX.500ディレクトリエントリの例
Fig. 5 A sample of X.500 directory entry for the experiment.

```
(project
 (credential_selection
  (select job_matching qualification='Class I Information-Technology Engineer'),
  signature, pubkey-cert-dn, CA.cert, (qualification, q_cert_dn))
name,region)
```

図6 実験1に用いた問い合わせ
Fig. 6 The query of the experiment 1.

```
(project
 (credential_selection
  (select job_matching (experience='database programming' && year_of_birth >= 1965),
  signature, pubkey-cert-dn, CA.cert, (experience, exp_cert_dn))
name, region, year_of_birth)
```

図7 実験2に用いた問い合わせ
Fig. 7 The query of the experiment 2.

```
(project
 (credential_selection
  (select job_matching (qualification='pharmacist' && experience='service in hospital')),
  signature, pubkey-cert-dn, CA.cert, ((qualification, q_cert_dn),
  (experience, exp_cert_dn)))
name,year_of_birth)
```

図8 実験3に用いた問い合わせ
Fig. 8 The query of the experiment 3.

検索システムについても,情報の信頼性を評価する機能を実現することに対する要求が高まることが予想される.これらの要求を実現するために,本提案方式を拡張し,新しい情報検索システムに対して情報の信頼性評価機能を連結する場合にも,本提案方式では信頼性評価システムの全体を改変すること無く,新しい情報システムに対して信頼性評価機能を連結することが可能である.

本論文では,提案方式に基づいて,実験システムを構築し,問い合わせ実験を行った.この実験により,本方

式がデータベース上の情報の信頼性評価機能を有する検索機構を実現する方式として有効であることを明らかにした.

本論文では,属性証明書としてX.509公開鍵証明書のフォーマットを用いたが,今後は他の形式の属性証明書も扱うことができる方式について研究を行う.また,属性証明書によって証明する属性の値は,本論文では単純な文字列に限定したが,今後はXMLを用いるなど,構造化された複雑なフォーマットにも対応可能な方式についても研究を行う予定である.

謝辞

本研究において貴重な御助言を頂いた,慶應義塾大学 政策・メディア研究科 金子 郁容教授,同環境情報学部 村井 純教授に感謝致します.

参考文献

1) eBay Homepage: http://www.ebay.com/
2) ISIZE Homepage: http://www.isize.com/
3) Job Matching Square Homepage: http://jms.vcom.or.jp/
4) 細川 宜秀, 清木 康: 関数型計算によるマルチデータベースシステムの問い合わせ処理方式, 情報処理学会論文誌, Vol.39, No.7, pp.2217-2230, Oct. 1998.
5) 吉田 尚史, 清木 康, 北川 高嗣: 意味的連想検索機能を持つメディア情報検索システムの実現方式, 情報処理学会論文誌, Vol.39, No.4, pp.911-921, Apr. 1998.
6) 細川 宜秀, 石橋 直樹, 八代 夕紀子, 清木 康: マルチデータベース環境における時間的・空間的関連性評価によるデータ結合方式, 情報処理学会論文誌, Vol.40, No.SIG8(TOD4), pp.95-111, Nov. 1999.
7) 山崎 重一郎, 荒木 啓二郎: 信用情報と利用ポリシーの管理が可能な相互認証を実現する認証基盤の提案, 情報処理学会論文誌, Vol.40, No.1, pp.296-309, Jan. 1999.
8) 須賀 祐治, 山崎 重一郎, 荒木 啓二郎: 認証登録機関とX.500ディレクトリサービスの連携について, 情報処理学会 マルチメディア・分散・協調とモーバイルシンポジウム (DICOMO98) 論文集, pp.317-322, Jul. 1998.
9) 鈴木 寛: ECとリスクマネジメント, 計画行政, Vol.20, No.3, pp.49-55, Mar. 1997.
10) 鈴木 寛: わが国における電子商取引政策の現状と課題, 日本国際経済法学会年報, No.8, pp.195-217, Sep. 1999.
11) 須賀 祐治, 荒木啓二郎: 公開鍵インフラにおける属性証明書の利用について, 電子情報通信学会 ソフトウェア・シンポジウム99論文集, Jun. 1999.
12) 山口 英, 鈴木 裕信: 情報セキュリティ, 共立出版, Jan. 2000.
13) 宮川 祥子, 山崎 重一郎:インターネットにおける「信用」と「評判」—相互与信システムの社会的応用—, ビジネスレビュー Vol.46 No.2, pp50-pp74, Nov. 1998.
14) 山崎重一郎, 宮川祥子, 山本薫, 須賀祐治, 金子郁容, 荒木啓二郎: インターネット上の求人/求職マッチングシステムにおける登録情報の与信方法について, 情報処理学会コンピュータセキュリティシンポジウム CSS98 論文集, Oct. 1998.
15) Kitagawa, T. and Kiyoki, Y.: The mathematical model of meaning and its application to multidatabase systems, Proceedings of 3rd IEEE International Workshop on Research Issues on Data Engineering: Interoperability in Multidatabase Systems, pp.130-135, Apr. 1993.
16) Kiyoki, Y., Kitagawa, T. and Hayama, T.: A metadatabase system for semantic image search by a mathematical model of meaning, ACM SIGMOD Record, Vol.23, No.4, pp.34-41, 1994.
17) Kiyoki, Y.,Kitagawa, T. and Hitomi, Y.: A fundamental framework for realizing semantic interoperability in a multidatabase environment, Journal of Integrated Computer-Aided Engineering, Vol.2, No.1, pp.3-20, John Wiley & Sons, Jan. 1995.
18) Date, C., J.: An Introduction to Database Systems. Volume II, Addison Weslay, 1995.
19) Chokhani, C., Ford, W.: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC2527, 1999.
20) Housley, R., Ford, W.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC2459, 1999.
21) Adams, C., Farrell, S.: Internet X.509 Public Key Infrastructure Certificate Management Protocols, RFC2510, 1999.
22) Boeyen, S., Howes, T., Richard, P.: Internet X.509 Public Key Infrastructure Operation Protocols -LDAP v2, RFC2559, 1999.
23) Myers, M., Ankney, R., Malpani, AA., Galperin, S., Adams, C: Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP, RFC2560, 1999.
24) Yeong, W., Howes, T., Kille, S.: Lightweight Directory Access Protocol, RFC1777, 1995.
25) Mahl, M., Howes, T., Kille, S.: Lightweight Directory Access Protocol (v3), RFC2251, 1997.
26) Boeyen, S., Howes, T., Richard, P.: Internet X.509 Public Key Infrastructure LDAP v2 Schema, RFC2587, 1999.
27) ITU-T: Information Technology - Open

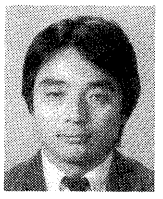
Systems Interconnection - The Directory: Overview of Concepts, Models and Services, ITU-T Recommendation X.500, 1993.
28) ITU-T: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, ITU-T Recommendation X.509, 1997.
29) Farrell, S., Housley, R.: An Internet Attribute Certificate Profile for Authorization, IETF Internet Draft, 1999.
30) 若山 公威, 奥野 啄人, 岩田 彰, 村瀬 晋二, 鈴木 春洋: 暗号ライブラリと認証局パッケージの開発, 第59回 (平成11年後期) 情報処理学会全国大会, Sep. 1999.
31) 久保田 和己, 石川 博:データベースとインターネットアプリケーションの連携に関する試み, 電子情報通信学会 データ工学研究会, Jul. 1995.
32) Johnston, W., Mudumbai, S., Thompson, M.:Authorization and Attribute Certificates for Widely Distributed Access Controll,Proceedings of IEEE 7th International Workshop on Enabling Technologies:Infrastructure for Collaborative Enterprises - WETICE '98, Nov. 1998.
33) 川倉康嗣: ID 証明書と属性証明書の併用によるアクセス制御方式, 情報処理学会 コンピュータセキュリティシンポジウム '98, pp.97-102, May. 1998.
34) Ellison, C.: Establishing Identity Without Certification Authority, Proceedings of USENIX Security Symposium, pp.67-76, 1996.
35) OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/dsti/sti/it/secure/prod/PRIV-en.HTM, 1997.

(平成11年12月20日受付)
(平成12年 3 月27日採録)

(担当編集委員 宝珍 輝尚)

宮川 祥子 (学生会員)

1994年一橋大学商学研究科経営学および会計学専攻修士課程修了. 現在, 慶應義塾大学政策・メディア研究科博士課程在学中. ネットワーク上のコミュニティ活動を支援するための情報システムに関する研究に従事.



清木 康 (正会員)

1978年慶應義塾大学工学部電気工学科卒業. 1983年同大学院工学研究科博士課程修了. 工学博士. 同年, 日本電信電話公社武蔵野電気通信研究所入所. 1984年～1995年筑波大学電子・情報工学系講師, 助教授, 1996年～1998年慶應義塾大学環境情報学部助教授を経て, 現在, 慶應義塾大学環境情報学部教授. データベースシステム, 知識ベースシステム, マルチメディアシステムの研究に従事. ACM, IEEE, 電子情報通信学会, 日本ソフトウェア科学会各会員.