様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月１日現在

機関番号：14603
研究種目：基盤研究（Ｃ）一般
研究期間：2008～2010
課題番号：20560356
研究課題名（和文）　次世代型グループ情報共有・流通のセキュリティ基盤に関する研究

研究課題名（英文）　Security mechanism for sharing and distributing information in various groups of the next-generation

研究代表者
楫 勇一 （KAJI YUICHI）
奈良先端科学技術大学院大学・情報科学研究科・准教授
研究者番号：70263431

研究成果の概要（和文）：本研究では，情報ネットワーク上に出現している多様なグループサービスにおいて，情報共有，情報流通を安全に行うための基礎技術を開発した．具体的には，ハフマンアルゴリズムを導入することにより，長期にわたり性能を維持することのできるグループ鍵管理方式を開発した．また，複数組織にわたってユーザの役割情報を共用することのできるクロスドメインロールベースアクセス制御の定式化を行い，階層型ＩＤベース暗号を利用して実現する方式を提案・試作した．

研究成果の概要（英文）：This study develops fundamental technologies for sharing and distributing information in various groups of users The study covers two major subjects. In the group key management, we developed an algorithm which makes use of the Huffman algorithm and keeps the good efficiency for long term of use. In the authentication issue, we give a formal model of the cross-domain role-based access control mechanism, and developed a concrete scheme based on the hierarchical ID-based cryptosystem.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,700,000	510,000	2,210,000
2009 年度	700,000	210,000	910,000
2010 年度	700,000	210,000	910,000
年度			
年度			
総　計	3,100,000	930,000	4,030,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：情報セキュリティ，暗号鍵，グループ通信，LKH法，マルチキャスト通信，放送暗号

１．研究開始当初の背景

通信基盤の普及と各種端末の性能向上を背景とし，様々な情報サービスが実用化されつつあるが，これらのサービスの多くは，本質的には，特定ユーザ集合を対象とした情報共有・流通サービスであると解することもできる．特定ユーザの集合，すなわちグループ単位の情報共有では，グループ外への情報漏洩を防ぐ仕組みの実現が重要となる．従来は，機密性の高い情報を取り扱うユーザはきわめて限定されていたこともあり，比較的小規模で組織化されたグループを前提としてセキュリティ方式が検討されることが多かった．一方，携帯電話を含む情報通信システム

が一般の人々にも広く浸透したことを受け，グループ規模の大規模化，ユーザの多様化，グループ管理権限の分散化等が近年顕著になりつつある．これら，従来とは異なるタイプのグループにおいて情報や権限を適切に管理するためには，従来とは異なるセキュリティ技術を確立する必要がある．とくに，以下に挙げる二種類の情報共有形態については社会的な重要性も高いと考えられるため，早急に安全確保の手段を確立することが強く望まれていた．

大規模同報通信向けグループ鍵管理方式：

マルチキャスト技術を利用し，多数の契約者に映像コンテンツ等を配信するサービスが，当時，実用化されつつあった．配信コンテンツはグループ鍵を用いて暗号化され，グループ鍵保有の有無がコンテンツ利用の可否を制御することとなる．グループ鍵管理の代表的な手法として，LKH法が広く知られている．LKH法では，ある種の木構造を利用することで，ユーザの新規加入・脱退にともなうグループ鍵の更新作業等を効率よく行うことを目指している．大規模サービスでは，複数のユーザ加入・脱退操作をとりまとめ，「バッチ作業」的に鍵更新を行うことが一般的になるが，そのような運用に対応したバッチ型LKH法も既存研究にて提案されている．ただし申請者による予備的検討では，バッチ型LKH法を長期間運用した場合，木構造にある種の偏りが生じ，鍵更新の効率が悪化することが明らかになっていた．長期的なサービス提供においては，この問題の解決が必要であった．

自律分散的なグループにおける認証方式：

既存サービスの多くでは，サービス提供者としての管理者と，サービス享受者としてのユーザとが明確に区別されている．一方，SNSに代表されるいくつかのサービスでは，緩く連携したユーザ同士が対等な立場で情報共有を行うため，サービスの提供者と享受者という単純な図式は成立しない．ここでは，グループ（コミュニティ）を一元管理する管理者の存在は希薄であり，ユーザは，他ユーザからの勧誘・推薦という形でグループに参加することが一般的となる．いわば，グループのメンバが新しいグループメンバを認定する権限を持ち，グループは自律分散的に変化していくと解釈することができる．中央集権的にユーザを管理する管理者・サーバがいる場合，あるユーザがグループに属するか否かを判定することは容易に可能であるが，自律分散的なグループにおいては，そのようなユーザ認証，所属認証は容易に行えない場合もあり得る．自分が特定のグループのメンバであることを立証するには，たとえばPKI技術と証明書連鎖を用いることも可能であるが，電子証明書の利用は技術的・コスト的負担が大きくなるため，個人ユーザや小規模グループに対しては実用的であるとはいえない．グループの実態に対応可能であり，かつ低コストで所属認証等を可能とする技術の確立が必要であると考えられた．

２．研究の目的

本研究の目的は，情報通信技術の普及にともなって急速に多様化しているグループの在り方に留意し，様々なグループにおける情報共有および情報流通に適したセキュリティ基盤構築に貢献するような基礎技術の確立を目的として研究を行った．

同報通信向けグループ鍵管理方式については，LKH方式をベースにし，木構造を常に最適にバランスするようなバッチ型鍵更新手順の確立を具体的目標とした．研究開始当初は，放送と通信の融合に関する議論が開始されており，マルチキャストサービスの大規模化が予想されていた．グループ鍵管理にも高いスケーラビリティが求められることになり，従来の小規模グループを前提とした方式では，十分な効率が確保できない恐れがあった．また，商用サービスを念頭に置いた場合，長期にわたって性能劣化を抑えることができるような方式が求められることになる．これら，実用上の要求に応えることのできるグループ鍵管理手法の確立が，本研究における第一の目的であった．

一方，自律分散グループの所属認証については，大きく二段階の目的設定をする必要があった．最初の段階の目的は，必要となる要求仕様の明確化を行うことである．計算機ネットワークにおいて出現しつつあった「新しい形態のグループ」は，ネットワーク上に突発的に出現した特異なものではなく，あくまでも実世界におけるグループ，組織，あるいは，もっと「緩い」コミュニティに対応するものであると考えられる．多様で多彩なグループが実世界には存在するが，従来のセキュリティ研究では，「一人の管理者とその他大勢の一般ユーザ」という単純なグループモデルしか想定されていなかったのが実情である．絶対的な管理者がいる場合，所属認証方式が提供すべき機能は明確に記述することができるが，管理権限があいまいで自律的・分散的であるようなグループにおいては，そのような単純な使用記述を行うことは困難であると予想された．本課題における最初の目標は，安全性とは実世界における「グループ」の在り方について十分な考察を行い，汎用性と具体性を兼ね備えた「要求仕様」を確立することであった．その結果を踏まえ，要求仕様を実現するような具体的な手順等を提案することが，本課題の最終目的となる．

３．研究の方法

グループ鍵管理方式に関する研究については，大きく二つの段階を設定して研究に取り組んだ．研究の第一段階は，研究開始当初に「標準的」と目されていたLKH法の振る舞いに関する詳細な分析である．研究開始段階では，既存のバッチ型LKH法を長期間運用すると，鍵更新のオーバヘッドが最適値よりも大きく乖離することが実験的に判明していたが，その理由等については明確になっていなかった．LKH法が内部的に利用する「鍵木」と呼ばれる木構造のアンバランスが原因であると予想されたが，直接的なオーバヘッド増加要因が何であるのかは，研究開始当初には明確でなかった．研究の第一段階では，オーバヘッド増加要因が何であるのかを特定し，制御すべきパラメータの明確化を行った．第一段階の評価結果を受け，研究のダニ段階では，制御すべきパラメータを最小化（あるいは最大化）するよう木構造再構成法について検討を行った．バッチ型LKH法は，概念的には，木構造を部分木集合にいったん分割し，再度部分木を併合する手続きであると考えることができる．部分木を併合する際，ハフマン符号等の情報源符号を設計する最適木構成アルゴリズムを利用することで，制御パラメータを最適とするよう木を再構成する手順を検討し，具体化を行った．構成した手順（アルゴリズム）について，いくつかのユーザ変動シナリオを設定し，スケーラビリティや各種コストについての評価を行った．

自律分散グループにおける所属認証について，いたずらに対象を広げると議論が発散するおそれもあるため，ロールベースアクセス制御（RBAC）の枠組みを前提として想定し，緩く連携した複数組織が，それぞれのロールを相互に参照しあうようなモデルを想定した．現実世界のグループ（組織，コミュニティ）は互いに独立して存在しているわけではなく，その間に，なんらかの相互関係が定義されている場合も多い．たとえば，ある大学で「学生」の身分を持っている者は，提携先大学においてなんらかのサービス（たとえば図書館や無線ネットワーク）を利用できたり，あるいは博物館等に割引料金で入場できたりする．これは，ある大学が発行した「学生」という身分（ロール）を多組織が参照し，利用していると考えることができる．「組織」は必ずしも一様に管理されたものである必要はなく，たとえば内部に階層構造があったり，推薦ベースで誰でも入会できたり，多様な形態が考え得る．そのような多彩なグループが複数存在し，互いにロール情報を相互利用するような環境を想定モデルとして設定し，その設定のもとで安全かつ効率的に所属認証（ロール認証）を行えるための仕組みを開発した．開発にあたっては，公開鍵暗号の一種である階層型ＩＤベース暗号の技術を流用し，電子法名所やＰＫＩといった高コストな仕組みを利用しない方式を検討した．

４．研究成果

４．１ グループ鍵管理方式について

バッチ型LKH法を改良し，鍵木が最適構成を取り続けることができるような方式を提案した．

鍵木 T=(V, E) は，すべての節点に暗号鍵が個別に対応付けられた木である．本研究では，鍵木が一般のm分木である場合についても検討を行っているが，本報告においては簡単のため，鍵木は二分木であると仮定する．節点 v に対応付けられた鍵を k(v) と表記し，v のノード鍵と呼ぶ．鍵木の葉節点とグループに属するユーザ（メンバ）とは一対一に対応しており，葉 l に対応するユーザには，ノード鍵の集合 {k(v) | vはlの先祖節点} が与えられる．根節点のノード鍵はグループのメンバ全員が知る鍵となっており，これをとくにグループ鍵と呼ぶ．グループ鍵以外のノード鍵は，その親節点のノード鍵を暗号化して配送する際に用いられるため，鍵暗号化鍵とも呼ばれる．

LKH 法において葉l に対応するメンバをグループから脱退させる（排除する）には，l の所有するノード鍵を全て破棄し，破棄されたノード鍵を置き換える新しいノード鍵を，l以外の適当なメンバに対して配送する必要がある．具体的には，葉lを木Tから除去し，木を適当に縮退（子を一個しか持たない節点を，その子節点で置き換える操作)した上で，l の先祖節点のノード鍵更新をボトムアップ的に行うこととなる．ノード鍵更新にあたっては，鍵更新が必要となる節点vの子節点vl, vrのノード鍵が利用される．たとえば，v のノード鍵を k に置き換えるには，2 つの暗号文 E(k(vl), k) およびE(k(vr), k)を適当なユーザ集合に対して配送する．節点 vl, vr の子孫にあたるユーザはノード鍵k(vl), k(vr)を所持するため，これら暗号文から v の新しいノード鍵vを入手することができる．ノード鍵更新をボトムアップ的に行うことにより，脱退メンバl以外のグループメンバに対して適切に鍵配送を行うことができる．新規メンバをグループに追加する場合は，T において深さ最小の位置に存在する葉の一つを高さ 1 で 2 個の葉節点を持つ木に置き換え，上述したのと同様の手順でノード鍵の更新を行えばよい．

本研究では，LKH法をバッチ型処理に拡張し，かつ，鍵木の再構成法に工夫を加えることで，グループ鍵の更新を繰り返しても性能の劣化が起こらない方式を開発した．提案手法におけるグループ鍵の更新は，鍵木分解，

鍵木再構成，ノード鍵配送の 3 段階の手順から成り立っている．以下では，新規加入ユーザの集合をJ，グループから脱退するメンバの集合をLとする．

鍵木分解:
グループへ新規加入する |J| 人のユーザからなる鍵木T'を構成する．また，全体の鍵木 T から，Lに対応する葉およびその先祖節点をすべて削除する．内部節点が削除されることにより，鍵木は複数の部分木に分解されることになるが，このとき得られた部分木の集合にT'を加えて得られる木の集合をSと書くことにする．

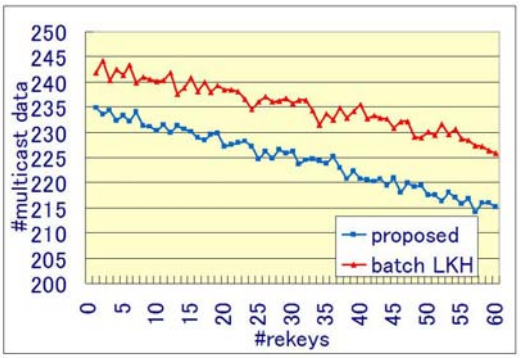
鍵木再構成:
鍵木の再構成は，実質的には，木の葉数を重みとするハフマンアルゴリズムの実行である．木の集合Sから，葉の数が 1 番目，2 番目に少ない木 t1, t2 を特定する．次に，新しい節点を一個作成し，その節点の子の位置に t1, t2 を配置することで，新しい木tを作成する．その後，S←{t} ∪ S – t1, t2} として木の集合Sを更新する．Sがちょうど一個の木を含むようになるまで，同じ手順を繰り返す．

ノード鍵配送:
バッチ型 LKH 法と同様の手順により，更新されたノード鍵の子のノード鍵で暗号化され，ボトムアップ的に同報通信される．

グループ鍵更新に必要となるコストはノード鍵更新に必要となる暗号文の個数であり，これは，ノード鍵の更新が必要となる節点数の 2 倍に等しい．提案法においてノード鍵更新が必要となるのは，鍵木再構成の過程において新しく作成された節点である．一般に，新しい節点の追加を繰り返してn個の木を併合していく場合，全部でn – 1 個の新しい節点が導入される．この n – 1 という値は，最終的に得られる木の構造や，併合を行う順番とは関係なく，常に一定である．したがって，提案法を利用して木を併合しても，あるいはLKH 法のように当初の鍵木の構造をできるだけ再現するようにしても，ノード鍵の更新に必要となるコストは変わらない．これより，以上より，鍵木再構成の際に木の構造を大幅に変更しても，グループ鍵更新コストには直接的には影響しないことがわかる．一方，鍵木再構成後の木の構造は，それ以降のグループ鍵更新の効率に影響を与えることとなる．詳細な議論は省略するが，鍵更新のコストは木の外部経路長と強い関係がある．鍵更新のコストを抑制するためには，与えられた部分木集合Sに対し，最終的な外部経路長が最小になるように木を併合していくことが有効であると考えられる．これに関連し，以下の補題を示すことができる．

補題：
提案法の鍵木再構成手続きによって得られた鍵木は，Sの木を併合して得られる鍵木の中で最小の外部経路長を持つ．

提案手法の性能を実験的に評価した結果を下図に示す．



４．２ 自律分散グループ所属認証について
本研究では，組織（ドメイン）の壁を越えてユーザのロール情報を行使することのできるクロスドメインロールベースアクセス制御技術を考える．
RBAC では，ユーザのサービスへのアクセスは，そのユーザに割り当てられたロールによって決定される．一個の組織でRBAC を採用する場合，考慮すべきロールは，その組織内で定義されたロールだけで良いが，クロスドメイン環境下では，他の組織によって管理・発行されたロールについても考慮する必要がある．クロスドメイン環境下におけるRBAC について明確に記述するため，以下に形式的な定義を与える．以下では，U をユーザの集合，0 を組織の集合とする．各組織o ∈ 0 は，以下の要素を定義し，保持するものとする．

- ロールの集合Ro．ただしo1≠ o2 ならば，Ro1 ∩Ro2 = □と仮定する．すなわち，各ロールは一個の組織により排他的に管理されていると仮定する．以下の議論のため，R = ∪Ro と書くものとする．
- サービスの集合So．ロール集合と同様，o1≠o2 ならばSo1∩So2 = □とする．
- ユーザ・ロール割り当てUAo⊂U×Ro． もし(u, r)∈UAoならば，組oがユーザuにロールrを割り当て又は発行し，ユーザuはロールrを持つという．組織oは，Roのロール，すなわち，自ら管理するロールしか発行することができない．これは，他の組織によって管理されたロールを勝手に発行できないという当然の事実の反映となっている．一方，ユーザ集合U は組織に対して共通となっており，一人のユ

ーザが，複数の組織から複数のロールを割り当てられる可能性があることに注意が必要である．

- ロール・サービス割り当てSAo⊂Ro×So．ロールr に属するユーザがサービスs へアクセスすることを許可したいとき，組織o は，(r, s) ∈ SAo となるようSAoを定義する．
- 解釈関数Io ： R → Ro ∪ {⊥}．ここで⊥はロールの表記には用いられない特殊記号である．解釈関数は，他の組織によって定義されたロールを，組織o でどのように解釈するかを定義する．もしIo(r1) = r2 ならば，組織o は，他組織で定義されたロールr1 の所有者を，自分の管理するロールr2 の所有者と同等に遇することを意味する．Io(r1) = ⊥の場合，ロールr1 の所有は，組織o において全く意味を持たないものと解釈する．

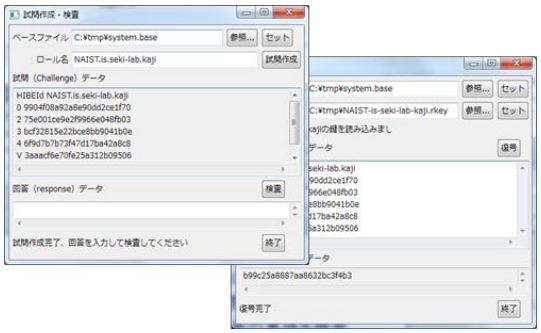
上記に定義したRBACの仕組みは，階層型ＩＤベース暗号の機能を用いて実現することができる．実現手法を構成する主要な要素は，組織セットアップ，ロール発行，ロール確認の３つの手順である．

組織セットアップ：
組織o ∈ 0 は，組織の識別子となる文字列so を選定し，so を使用することについてルート鍵生成器に審査を要求する．ルート鍵生成器は，組織o の要求を承認するなら復号鍵dksoを計算し，安全なオフライン通信路を用いて組織o に鍵を送付する．組織o は，so に対する正しい鍵のペア(ekso, dkso) を受領した後，ロールの集合Ro を定義する．Ro に属する全てのロールは，so のサブロールとして定義するものとする．組織o は，so に対する正しい鍵のペア(ekso, dkso) とロールの名称（so のサブID) を用い，抽出操作により，Ro に属するロールS の復号鍵を決定することができる．一方，鍵生成器は他の組織にdksoを与えないことが仮定されているため，o 以外の組織は，Ro に属するロールの復号鍵を決定することができない．組織o は，Ro に属するロールの名称，識別子を公開することはできるが，各ロールに対する復号鍵は，秘密に保持する．

ロール発行：
組織o は，自機関のユーザ・ロール割り当てUAo を定義することができる．ユーザu に対してロールr ∈ Ro を発行するときは，安全な通信路を用い，ユーザu にr の復号鍵dkrを渡すものとする．ユーザはロール名称r と復号鍵dkrを関連付け，安全に保持する．

ロール確認：
ユーザu が組織o1 を訪問，あるいはo1 のサーバにアクセスし，他の組織o2 により発行されたロールr を用いて，o1 のサービスs にアクセスする場合を考える．このとき，組織o1 は，このユーザu がサービスs にアクセスして良いかどうかを判断する必要がある．もしIo1(r) □= ⊥かつ(Io1(r), s) がSAo1 に含まれているならば，組織o1 は，ユーザu がロールr を本当に保持するか，すなわち，(u, r) □∈ UAo2 か否かを確認する必要がある．もしIo1(r) ＝⊥または(Io1(r), s) がSAo1 にない場合は，o1 はユーザu を無視してよい．(u, r) □∈ UAo2 か否かは，組織o2 に照会しなくとも，チャレンジレスポンス認証によって確認することができる．

以上の方式を実装し，プロトタイプシステムを試作した．図は，試作システムの実行画面例である．



５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計３件）
①野田潤，楫勇一，中尾敏康，複数の大規模グループに同時参加するセンサノード向けグループ鍵管理方式，情報処理学会論文誌，**52**，3，pp. 1160-1172，2011，査読有

②K. Sugiyama, Y. Kaji, On the Minimum Weight of Simple Full-Length Array LDPC Codes, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E91-A, pp. 1502-1508, 2008, 査読有

③H. Mohri, R. Matsumoto, Y. Kaji, Key Predistribution Schemes for Sensor Networks Using Finite Plane Geometry, IEICE Transactions on Information Systems, E91-D, pp. 1416-1423, 2008, 査読有

〔学会発表〕（計２０件）
①K. Zhou, Y. Kaji, Anti-Phishing Mutual Authentication Using the Visual Secret

Sharing Scheme, 2010 International Symposium on Information Theory and Its Applications, Taichung, Taiwan, 2010.10.19, 査読有

②R. Yoshinaka, Y. Kaji, H. Seki, Chomsky Schutzenberger Type Characterization of Multiple Context-Free Languages, 4th International Conference on Language and Automata Theory and Applications, Trier, Germany, 2010.05.27, 査読有

③ K. Zhou, Y. Kaji, A Mutual Authentication Using Visual Secret Sharing - an easy way to protect novice users from phishing fraud, 2011 Workshop on Error-Correcting Codes and Cryptography, Yangzhou, China, 2010.04.23, 招待講演

④Y. Kaji, On the Error Performance and Parameter Choices of the Array-Type LDPC Codes, Tenth International Symposium on Communication Theory and Applications, The Lake District, UK., 2009.07.18, 査読有

⑤Y. Kaji, On the Number of Minimum Weight Codewords of SFA-LDPC Codes, 2009 International Symposium on Information Theory, Seoul, Korea, 2009.6.29, 査読有

⑥R. Aoyama, Y. Kaji, Improvement of the Forced-Convergence Decoding for LDPC Codes, 2008 International Symposium on Information Theory and Its Applications, Auckland, New Zealand,, 2008.12.7, 査読有

⑦T. Sakamoto, T. Tsuji, Y. Kaji, Group Key Rekeying Using the LKH Technique and the Huffman Algorithm, 2008 International Symposium on Information Theory and Its Applications, Auckland, New Zealand,, 2008.12.8, 査読有

他１３編

〔産業財産権〕
○出願状況（計１件）

名称：鍵管理装置、サービス提供装置、アクセス管理システム、アクセス管理方法、制御プログラム、およびコンピュータ読み取り可能な記録媒体
発明者：楫勇一, 関浩之
権利者：奈良先端大
種類：特許出願
番号：2010-149517
出願年月日：2010.06.30
国内外の別：国内

６．研究組織
(1)研究代表者
楫 勇一 (KAJI YUICHI)
奈良先端科学技術大学院大学・情報科学研究科・准教授
研究者番号：70263431

(2)研究分担者
なし

(3)連携研究者
なし