様式 C-19

科学研究費補助金研究成果報告書

平成　21　年　　6 月　　20 日現在

研究種目：基盤研究（C）
研究期間：2005～2008
課題番号：17500048
研究課題名（和文）　研究者の役に立つ著作権とセキュリティを考慮した知識の発見と流通に関する研究

研究課題名（英文）　Discovery and distribution with the copyrights management and the security for the researchers

研究代表者 木下　宏揚
神奈川大学・工学部・教授
研究者番号：70101041

研究成果の概要：

1.　著作権管理の基盤技術

著作権保護と 2 次利用促進を目的としたエージェントベースの情報カプセルを個人情報保護に応用した。配布済のデータの位置を特定し、匿名経路制御を行う方法を提案した。

2.　知識の流通と発見のための情報検索技術

研究者の保持している情報を体系化し検索が容易に行えるようにするたにオントロジーを用いたデータ記述を行った。オントロジーを構築する際に、コンテキスト間の関係を記述することによって、関連情報を検索する際の効率を改善した。また、ユーザが検索システムに検索意図を明確に伝えられるパネル型クエリ生成インタフェースを用いた画像検索システムを提案した.

3.　セキュリティを確保するアクセス制御技術

直観主義論理によるダイナミックなアクセス制御の記述し、Covert Channel を検出する機能がある情報フィルタに訂正を促す機能を追加して情報流出を防止する情報フィルタを提案した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
17 年度	1000000	0	1000000
18 年度	900000	0	900000
19 年度	900000	270000	1170000
20 年度	800000	240000	1040000
年度			
総　計	3600000	510000	4110000

研究分野：総合領域
科研費の分科・細目：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、著作権管理、アクセス制御、情報検索

１．研究開始当初の背景
研究者が研究を行う場合、同様の専門分野と情報を交換、共有したり、多分野の研究成果を取り込む必要がある。WWW の発達で情報を大量にしかも低コストで入手することが可能となっている。入手したい情報を検索する場合、検索エンジンが利用されているが、これらの情報の中から有益な情報のみを抽出し、目的の情報を発見することは容易ではない。一方、情報を発信する立場では、参考文献などの収集した資料、およびこれらを体系化したもの、さらにオリジナルの研究成果など保有する情報を有効に活用してもらうと考えても、検索エンジンベースでは適切なキーワードが指定されたり、上位にランクされていないと、参照される機会を逸してしまう。情報の入手先、提供先が見つかったあと、実際に情報を移動させる際には、データベースのアクセス制御技術、ファイアウォールの技術、著作権の制御、が重要となる。近年、Web アプリケーションは、シングルサインオンによる個人認証とファイアウォールや RBAC(Role based access control) によるアクセス制御によりセキュリティを確保している。しかし、複数の独立した組織が RBAC を採用している状況では、role （職務などの役割）の定義や role に対する permission （read、write、execute） がそれぞれ独立に決定されるので、組織間で情報をやり取りする時、組織間の role と permission の調整が問題となる。ファイアウォールでは複雑なセキュリティポリシーを正確に効率よく設計することは、容易ではない。次に、情報を流通させる場合、デジタル化されたデータのコピーが容易なことからオリジナリティや著作権の管理が困難となる。著作権の管理としては、電子透かしなど証拠の保証によるものとアクセス制御によるものがあるがデジタルデータの特性を生かした利便性との両立は困難である。さらに、情報の提供が有償の場合には、現在の現金の利点を継承した低額でも決済が可能な手法が求められる。また、これらの情報の流通はプライバシーの保護とセキュリティの確保を両立する必要がある。

２．研究の目的
研究者の利用を想定し、効率よく必要な知識を発見したり提供したりするために必要な基盤技術を開発する。具体的には、自己の専門などのプロファイル、収集希望・提供可能の知識などに基づく知識の発見提供モバイルエージェントを開発する。データベースは Web アプリケーションシステムとして実装し、そのアクセス制御法として、主体、客体の属性(アイデンティティ) に基づくアクセス制御を実行する Access Control Agent System を提案する。組織内に分散して配置されたファイアウォールのルールを各部署のセキュリティポリシーをもとに処理速度、記憶領域、配置コストの観点から生成する手法である分散ファイアウォールの最適化法を提案する。また、ファイアウォールのポリシーとアクセス制御を統合したアクセス制御モデル}を提案する。また、著作権を保護するために、画像配信に適した可視型電子透かしおよび個人情報のプライバシーや著作権情報を管理する情報カプセルエージェントを提案する。プライバシーを重視し、従来の現金のシステムの置換を目指した離散対数問題に基づく電子マネー超分散のディレクトリシステムによる決済手法を開発する。

３．研究の方法
1.著作権管理の基盤技術
① 可視型電子透かし
ロゴマーク入りのサンプル画像を放送し，視聴者が所望の番組を契約した後に可視型電子透かしを除去する番組毎の鍵を作ることによって，視聴者および放送局の要求を満たす有料放送のためのシステムが構築できる．また，ロゴマークを画像に表示させることで，番組の著作権を主張できる．さらに，番組提供スポンサーのロゴマークを用いることによって，宣伝にも応用できる．しかしながら，可視型電子透かしを単純に挿入するだけでは攻撃耐性が弱いため，対策として不可視型電子透かしとの併用が提案されている．しかしながら，静止画像のみで適用しているので放送には直接適用できない．そこで，有料放送において視聴者と放送局の双方が満足できる可視型電子透かしを用いたシステムを提案する．
②Agent Base の情報カプセル
新たな 2 次的コンテンツ（著作物）を作る際の DRM の対応は十分でなく，コンテンツの有効な活用が阻害されたり，著作権が侵害されてしまう場合がある．また，コンテンツ保護システムの一つである情報カプセルは，コンテンツにメタ情報を付与して暗号化をしたもので，安全な 2 次，3 次的な利用に対して柔軟ではない．そこで，まず著作物をデータベース側で管理するツールとして，Dublin Core に着目し，著作権の権利関係について拡張する．
③著作権制御とプライバシー情報の管理たのネットワーク
IT enable network において、著作権で管理された情報とプライバシー情報の配布は重要な問題となっている。そこで、著作権管理とプライバシー情報の管理に関連性があることを示す。

2.知識の流通と発見のための情報検索技術
①ユーザに適した画像検索
画像の内容に基づく画像検索（以下，CBIR:Content-Based Image Retrieval）はメタデータを計算機により自動的に算出できるため，画像に対するメタデータ付与が比較的容易に行える．クエリ生成手法としては思い描いている所望の画像をユーザ自身で生成する手法が提案されている．しかしながら，クエリ生成方法によっては(1)クエリ生成の手順が必要以上に多いとユーザの負担になる，(2) 検索するユーザが思い描いている所望の画像を適切にクエリとして生成できない，(3) ユーザが生成したクエリからユーザの検索意図をうまく汲み取ることができないといった問題点がある．したがって，画像検索システムはユーザが思い描いている所望の画像を負担なく適切にクエリとして生成できること，高い検索精度であることが望ましい．
②P2P ネットワークの関連情報の動的抽出
主観のズレを補う従来の研究として，キーワード間の関連性を用いた検索支援が行われていた．その検索支援方法では，各ノードにKRDB(キーワード関連性データベース) が分散管理されており，また，各ノードが所持するコンテンツ間のメタデータの関連性よりDB を作成していたそのため，作成者同士の主観のズレを補うことで関連語の一部には対応できるが，「雑感，思い入れ，価値」などの作成者と検索者間の主観のズレを補う方法を検討する．
③トピックマップを用いた非文字資料における Context の表現
民俗学研究資料の情報共有・情報流通の際に問題となるのが、社会的背景・歴史的背景などによって世界観が異なることによる視点の違いである。これは、人間が暗黙的に考慮しているもので Context といわれている。知識処理における Context は、重要な課題のひとつとされておりそのモデル化が望まれている。そこで、知識表現を行う標準規格であるトピックマップを用いて Context および Context 間の関連を表現し、民俗学研究資料の視点の違いによる問題を軽減し、非文字資料の共有・相互利用の促進を図る。

3.セキュリティを確保するアクセス制御
①┌ Access Control Agent System
異なる組織間での通信時に Covert channel が発生 Covert channel 分析の計算量の爆発前者は，組織間での role の統一性の欠如に起因するアクセス権の矛盾が生じ Covert channel が発生する問題である．後者は，Subject と Object の総数が増えるにしたがい Covert channel の分析に関わる計算量が膨大になってしまうことである．この様な RBAC と Covert channel に関する問題に対して，我々は Web アプリケーションシステムの枠組みを拡張し，Covert channel 分析制御を実行する手法を検討する．
② 情報フィルタ
Community Based Access Control に Prolog を用いたアクセスルールによる，推論機能の導入について言及する．推論機能は，演繹推論規則をもとにして動作する推論エンジンで実行され，その推論エンジンはアクセス制御するための情報フィルタに組み込まれる．推論機能により，導入するシステムのポリシーに基づきアクセス権限を決める事が出来る．
③形式的仕様記述言語による評価
Community Based Access Control Model を情報漏洩防止技術として導入するにあたり，アルゴリズムが安全であると言う保証を得たいが，容易に得る事は困難である．そこで，形式的仕様記述言語 CafeOBJ と呼ばれる安全性検証ツール導入による，アルゴリズムの安全性を検証を行う．
④直観主義論理によるダイナミックなアクセス制御の記述
　意味創発を支援し，かつ個人情報漏えい，改ざん，著作権侵害等を防止するセキュリティモデルの論理系としての必要条件は直観主義論理である事を示す．直観主義論理によるセキュリティモデルは，インターネット社会に於ける意味生成支援システムに於いて，制約条件として作用する．
⑤意味論的なクラウドのためのアクセス制御エージェントシステム
クラウドの中の社会システムと個人の環境に情報フロー制約機能を埋め込むためのエージェントシステムを検討する．エージェントシステムが持つべき制約とは，アクセス制御・情報フロー制御（covert channel 制御）・推論制御である． エージェントシステムは個人や組織のシステム内部からの情報漏えいを防止し，システム外部からの情報改竄を防止する．
⑥分散ファイアウォールのパケットフィルタリングの最適化
セキュリティ強化方法として，分散型ファイアウォールに注目する．ファイアウォールのなかではパケットフィルタリングが良く使われている．しかしながら，大学や企業などではコンテンツ等の大容量通信の増加により，莫大なパケットが送られてくるためネットワーク機器に負荷がかかり処理能力に限界がある．本研究ではまず，2 台のパソコンを繋げてパケットフィルタリングによるルール数とスループットの関係について予備実験を行い，そこから処理速度の向上における効率的な方法を提案する．
4.知識の流通のための価値の決済

①電子決済
現在普及している電子マネーの多くは、プリペイド型電子マネー（Suika、Edy など）であり、一回の決済にしか利用できないため現金との置き換えは不可能である。そこで、本稿では現金との置き換えを目指した電子マネーを検討する。
② 人間関係ダイアグラム評価を導入した地域 SNS での地域通貨の使用
多様な価値を表現可能な地域通貨を実現をするためには,「依頼事項の対価」「周りからの評価値」「依頼事項の経験値」が必要とされていた．しかし,「周りからの評価値」はなりすましユーザが架空の取引を繰り返し,それぞれの取引で良い評価を与えることによって周りからの評価値を上げることができてしまうなど，そのユーザがどれだけ信頼できるかを計るには不十分であるといった問題点があるので、これを検討する．
４．研究成果
1．著作権管理の基盤技
①可視型電子透かし
提案法では，番組に対して著作権や宣伝効果を示すロゴマークを可視型電子透かしとして埋込む．また，著作権情報または可視型電子透かしの埋込み情報を疑似乱数を用いて暗号化し，鍵として番組に埋込む．疑似乱数は放送局が保持する．なお，鍵に疑似乱数を用いれば埋込み情報を抽出できる．これより,番組単位での契約の成立後，放送局は保持する疑似乱数を視聴者に送信するだけで済み,かつ鍵が番組の著作権保護を強化する．一方,視聴者は，契約前において不可視型電子透かしの取出しアルゴリズム方法を用いれば鍵を知り得るが，放送局が管理する疑似乱数を知ることができず，可視型電子透かしが入っていない番組を視聴できない．そして，放送局は契約時に疑似乱数を送り，視聴者はそれらを用いて，番組の可視型電子透かしを除去する．また，鍵を変動させることで，各々の番組を管理する鍵として用いることができる．よって視聴者が所望の番組のみを購入することが可能になる．
②Agent Base の情報カプセル
既存の情報カプセルに Take-Grant と情報フィルタ，エージェントを導入し，コンテンツ利用の利便性を向上する方法を提案した．このシステムにより，コンテンツの利用の利便性の向上が期待される．また，エージェントを導入することで，カプセル側のカプセルエージェントとユーザ側のアクセス制御エージェントが交渉し，通信のトラフィックの低減,レスポンスの向上,権利の充足性の検査,充足させるための推論メカニズム，n 次利用の複雑な権利関係の調停ができるという利点がある．また，コンテンツの著作権情報・利用条件に関しても，権利記述言語を用いてエージェントとは別に定義することにより，簡単に提供者が権利情報を設定し,利用者がその情報を把握することを可能としている．
③著作権制御とプライバシー情報の管理のためのネットワーク
匿名通進路を通して情報配布者と管理すべき情報に伴ったモバイルエージェントとの通信を行う手法を提案する。また、配布済のデータの位置を特定し、匿名経路制御を行う方法を提案する。この方式では、ルータ上に経路制御の履歴を残し、これに基づいた経路制御を行う。この手法を適用することにより、デジタルコンテンツやプライバシー情報の利用目的を変更したり二次利用の際に発生する複数の権利者が関連した著作権の調停を自律的に行うことが可能となった。

2.知識の流通と発見のための情報検索技術
①ユーザに適した画像検索
ユーザが検索システムに検索意図を明確に伝えられるパネル型クエリ生成インタフェースを用いた画像検索システムを提案した．また、画像データの検索・絞り込みにあたり、曖昧で漠然としたユーザーの想像と類似した画像を所望する画像データの検条件として提出してもらい、その類似画像に存在するエッジ(輪郭線) を取り出して画像データの検索対象情報として抽出し、それらを検索対象情報の類似比較に用いた画像検索精度の絞込みを提案した。
②P2P ネットワークの関連情報の動的抽出
ニュースサイト上に提供されているコンテンツに対してユーザがフォークソノミーによってタグ付けした結果を解析し，上記に示したズレに対する有効性を検証している．また，その結果を元に検索支援の応用方法を提案した．
③トピックマップを用いた非文字資料における Context の表現
民俗文化を知的文化遺産とし，研究成果を電子化，情報発信することを目指した．Dublin Core を参考にした非文字資料に適したのメタデータの提案を最初に，意味情報を加味した非文字資料のディジタルアーカイブ化に関連する研究を行ってきた．その中で，Context の記述にはトピックマップが適しているとしてきた．そこで，トピックマップによる Context の記述を推し進め,意味情報ネットワークを構築する際に Context の適切な分割をどのように行えばよいのか，Context の特性を考察し実際にデータ構造を与えてみることでどのような利用法があり利点があるのかを示した．また，弱い紐帯を利用した連想のような検索を可能とするには，Context 間の結びつきをどのようにモデル化するのかを考察し提案した．まず、意

味に基づいた情報ネットワークの現状を説明した後にキーワードベースの情報検索システムでは起こらなかった問題点を示し，改善するべき課題を示した．

3.セキュリティを確保するアクセス制御
①Access Control Agent System
提案システムは，共通する Identity を持った小規模な Subject の集合を Community と定義し，Subject と Object の総数を抑制する．他 Community との通信時にはその都度 Covert channel 分析を行う事で上記の問題を解決している．以上のことから提案システムは，異なる組織間での通信においても Covert channel を効率よく防止することが出来るシステムである．
② 情報フィルタ
推論を導入した情報フィルタの推論エンジンを実装するにあたり，Prolog を用いた実装について述べている．まず，属性による処理について示し，統合方法についても述べている．そして，実際に属性を統合させた適用例について述べ，結果について考察した．
③形式的仕様記述言語による評価
CafeOBJ は現在最も研究開発が盛んに行われている言語であり，独自の処理系によりコンピュータの自動解析への応用が可能となる言語でる．CafeOBJ を用いて Community Based Access Control Model の，Covert Channel が完全にないと言う状態を形成するセキュリティモデルのアルゴリズムを形式的に記述し，安全性を証明する事が，本研究の目指す所である．
④直観主義論理によるダイナミックなアクセス制御の記述
モデルは，subject と object が持つ属性（競合，プライバシー，所有，役割，階層）を使い，アクセス行列内の covertchannel を直観主義論理によって分析し，情報フィルタを制御する．直観主義論理によって次に示す記述が可能となる．(1) アクセス制御属性及びアクセス規則の追加・改訂の可能性を記述する事．(2) 知識全てを知らずとも可能性の中から証明を記述する事．(3)アクセス行為の過程として covert channel のプロセスを記述する事．競合属性と階層属性のアクセス規則が組み合わされると言う可能性を記述する例によって，直観主義論理がアクセス制御属性の追加・改訂可能性を記述する事を示した．
⑤意味論的なクラウドのためのアクセス制御エージェントシステム
多元的価値を持つ SNS 的な community（社会システム）に組み込む情報フィルタ agent を設計する上で，なぜ哲学的考察が関与するのか，に関して述べる．agent は，covert channel を分析し，アクセス制御する． (1) セマンティック Web の情報検索やデータベース・スキームに使われる RDF(Resource Description Framework) は，『客体の存在の枠組みと，主体のアクセス行為の枠組みをグラフとして記述する“ 意味ネット ”』と見做せる．(2) 一方，主体の代理となってデータベースを管理する agent は，主体の認識行為，存在に対する主体の向き合い方が反映されなければならない．(3) しかし，agent は他の agent の意味ネット，即ち存在論と認識の規則が全て分かるわけではない．また，agent は自己自身に関しても世界の全てを意味ネットで記述可能ではない．(4) 従って，agent システムは，“ RDF（意味ネット）で推論する agent の振舞い ”に関して，存在論と認識論をオートポイエシス的なシステムの中で捉える必要がある．更に論文では，RDF をベースとするアクセス制御の哲学と，情報倫理との連関を指摘した．

⑥パケットフィルタリングの最適化
フィルタリングルールの各要素である，行動，プロトコル，発信元アドレス，発信元ポート，宛先アドレス，宛先ポート，プロコトル，フラグを定義し，ルール空間における結合則,吸収則，交換則，分配則の効率的な方法を示した．次に,処理能力の低下の一つとして，パケットフィルタリングで行われるマッチング処理回数の増加が考えられる.マッチング処理はフィルタリングルールの上位から順に行われる．そのため，多くのマッチング処理が行われるフィルタリングルールについては，ルールチェーン内の上位に持ってくることでフィルタリングによるマッチング処理回数を減少させることができ，処理速度の向上につながると考えられる．最後に，遺伝アルゴリズムを用いてルールをパラメータに変換し，交叉,淘汰を行いマッチング処理回数の削減を行う．フィルタリングの再配置を行うことで，再配置前と再配置後でマッチング処理回数における評価を確認した．

4.知識の流通のための価値の決済
①電子決済
前提条件として通信は全て匿名通信を用いる。Sx を 64bit の金額、Rx を 448bit の乱数とする。Mx(x の電子マネー)
=f(Sx,Rx)=2448Sx+RxDatabase に蓄積する電子マネーx の認証子 Dx は原始元を g とすると Dx=gMx mod n 電子マネーA から B への支払いを考える。取引前の User それぞれの電子マネーは MA1=f(SA1,RA1), MB1=f(SB1,RB1)金額を S、乱数を R として支払うと SA1+SB1=SA2+SB2,RA1+RB1=RA2+RB2 取引後の電子マネーは MA2=f(SA2,RA2), MB2=f(SB2,RB2)取引前後の Database 上で下記の式より A、B の電子マネーの合計が一致

していることを確認する。(gMA1gMB1 = gMA2gMB2 mod n)
② 人間関係ダイアグラム評価を導入した地域 SNS での地域通貨の使用
本論文では, 地域 SNS 上で電子地域通貨を使用することを想定した上で, その取り引きの際の信頼性評価として新たに, SNS の特徴でもある人間関係ダイアグラムを利用したユーザ評価指標を導入し, 既存方式の「周りからの評価値」をより信頼性のある数値した。

5.研究の位置づけと今後の展開
国内外において、これらは独創的な研究である。特にアクセス制御については、教育研究環境のみならず、産業分野や個人のネットワークとデータベース利用において、プライバシー保護と情報漏洩防止の本質的な要素技術になる。基礎的な部分については実装を行ったが、今後の展開は複数の組織で実装したシステムを用いて、有効性の検証と新たな問題点を検討することにある。

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　12　件）

1.Hirotsugu Kinoshita and Tetsuya Morizumi, "A network for copyright management and control of private information", The 2008 Symposium on Applications & the Internet The Workshop on ITeS: IT enabled Services (ITeS) , pp.448-451,(2008-7)査読有
2.野沢理倫、稲積泰宏、木下宏揚:"画像検索のためのパネルを用いたクエリ生成インタフェース"、画像電子学会誌,vol.36-3,2007-3. 査読有
3.森住哲也、木下宏揚:"インターネット社会のの情報漏えい・情報改ざんを防止するセキュリティモデルの提案",日本セキュリティ・マネジメント学会誌, (2007-1). 査読有
4.沖原健一, 稲積泰宏, 木下宏揚:"有料放送のための画像特徴を考慮した可視型電子透かし," 映像情報メディア学会誌, vol.60, no.2, pp.192-199(2006-2). 査読有
5.Kenichi Okihara, Yasuhiro Inazumi, and Hirotsugu Kinoshita:"A Visible Watermark Method for Sample Image in Video Delivery," IMQA2005(2005-9). 査読有
6.Masanori Nozawa, Yasuhiro Inazumi, Hirotsugu Kinoshita: "The Relationship between Human Memory and Image Resolution for Improving Accuracy of Image Retrieval," IMQA2005 (2005-9). 査読有

〔学会発表〕（計　44　件）

1.森住哲也,木下宏揚: "インターネットに於ける意味論的なクラウドのためのアクセス制御エージェントシステムの提案", 信学技報, vol. 108, no. 459, SITE2008-82, pp. 225-230, 2009 年 3 月.
2.清水孝治,戸田瑛人,木下宏揚,森住哲也, "人間関係ダイアグラム評価を導入した地域SNSでの地域通貨の使用",信学技報, vol. 108, no. 331, SITE2008-37, pp. 7-12, 2008 年 12 月.
3.森住哲也,,木下宏揚,辻井重男: "直観主義論理に基づく統合セキュリティモデルのアクセス規則について　ー 競合属性と階層属性を組み合わせた場合 ー", 信学技報, vol. 108, no. 244, SITE2008-31, pp. 9-14, 2008 年 10 月.
4.山下裕平,森住哲也,木下宏揚:"Context 表現のための手法の考察", 信学技報, vol. 108, no. 160, SITE2008-24, pp. 103-108, 2008 年 7 月.
5.森住哲也,木下宏揚,辻井重男 "多元社会の意味ネットにおける存在論と認識論の役割　ー 社会システムのアク セス制御 agent の視点から ー", 信学技報, vol. 108, no. 160, SITE2008-23, pp. 97-102, 2008 年 7 月.
6.森住哲也, 木下宏揚, 辻井重男 :“ 不確定な情報 “ covert channel ” の直 観主義論理による解釈と分析 “ , 信学技報, vol. 107, no. 139, SITE2007-19, pp. 65-70, 2007 年 7 月.

〔図書〕（計　0　件）
〔産業財産権〕
○出願状況（計　1　件）

カラー画像の圧縮符号化方法、復号化方法、カラー画像の圧縮符号化装置および復号化装置、発明者　稲積 泰宏, 木下 宏揚、権利者　神奈川大学、特許公開 2008-72254

○取得状況（計　件）
〔その他〕
６．研究組織
(1)研究代表者
木下　宏揚 (KINOSHITA Hirotsugu)
神奈川大学・工学部・教授
研究者番号 70202041

(2)研究分担者
稲積 泰宏 (INAZUMI Yasuhiro)
富山大学大学院・理工学研究部・講師
30367255

(3)研究協力者
森住 哲也 (MORIZUMI Tetsuya)
ネッツエスアイ東洋株式会社