審 査 の 結 果 の 要 旨

氏 名 申 吉浩

本論文は、「安全性が証明可能な追跡不能アクセス制御プロトコルとデジタルコンテンツ流通への応用に関する研究」と題し、ユビキタス社会におけるユーザの行為の追跡の脅威を問題として捉え、この問題の解決として、ユビキタス社会の観点から整理した要件を満足するアクセス制御共通基盤の構築が必要かつ有効であることを主張するとともに、その具体的な実現方式を提案する。本論文の新規性として顕著な部分は、第一にユビキタス社会におけるアクセス制御基盤の要件の整理を他に先駆けて試みた点にあり、第二に要件を満足するアクセス制御プロトコルを安全性に関する証明付きで提案した点にある。本論文では、上記 2 点の論点に加え、ユビキタス社会での適用で特に重要となる相互運用性の問題へのアプローチとしてプロトコルにおいて交換するメッセージの構文・符号化規則を規定すると共に、ユビキタス環境における重要なアプリケーションであるコンテンツ流通に適用する際の問題点とその解決の提案をも行っており、実用の観点からも深く考察されている。

第 1 章では、ユビキタス社会におけるシームレスかつ透過的なサービス提供は、ユーザの行動を秘密裏に追跡するネットワーク検閲社会を生み出す危険をはらんでいることを、まず、指摘する。この問題を解決するためには、まず、プライバシーと公知との境界(boundary between private and public)を考察する必要があるが、本論文では、追跡情報の開示が必要な際には、ユーザによる明示的な同意と引き換えにサービスの提供が行われる、Consensual Disclosure の考え方が適切であると提唱する。本論文の以下の章では、Consensual Disclosure を要件のひとつとして満足する追跡不能アクセス制御プロトコルの実現がテーマとなる。

第 2 章では、追跡不能アクセス制御プロトコルの提案を行うために必要となる、先行技術・関連技術の知識を整理する。まず、ユビキタスにおける広く受け入れられているトラスト管理のモデルである Distributed Trust Management との整合のためには、認証とアクセス制御の統合及び権限の移譲の 2 項目が要件となることを指摘している。次いで、データリンク層において、追跡不能性を実現する手段について整理する。Ethernet、IrDA、NFC、非接触 IC カード等の通信方式を個別に取り上げ、既存技術の枠内でデータリンク層における追跡不能性の実現が可能であることを指摘し、従って、アプリケーション層における追跡不能性が課題となることを結論として導く。更に、追跡不能認証に関する先行技術であるグループ署名のユビキタス環境への適用では、計算量に問題がある可能性を指摘し、計算量の軽減が重要な技術課題であることを示す。

第 3 章では、ユビキタスアクセス制御プロトコルの実現に当たっての主要な研究課題を、追跡不能性と計算量の抑制との両立、安全性の検証（証明）、及び、ユビキタス社会におけるアクセス制御の要件のサポートの 3 点であるとした上で、それぞれに対する解決手法について概説する。追跡不能性と計算量の抑制の両立に関しては、通常の電子署名の公開鍵ペアの構成から複数の「アクセス ID」と「残余成分」のペアを構成することによる原理を述べる。安全性に関しては、健全性、ユーザ端末の Big Brother 化の回避、Consensual Disclosure の安全性に対して、定義を与える。要件のサポートに関しては、ユビキタスの特性を考慮して要件の整理が必要である点と、要件のサポートが計算量の抑制と両立することが必要であることを述べている。

第 4 章では、ユビキタス環境におけるアクセス制御プロトコルが満足するべき要件を整理し、提案している。本論文で提案するアクセス制御プロトコルは、まず基礎として、認可と認証に求められる要件を満足しなければならない。本論文では、認可と認証に関する要件に加えて、ユビキタス固有の特質を考察し、(1)Consensual Disclosure に基づく追跡不能性、(2)権限発行者と検証者の分離、(3)認証とアクセス制御の統合、及び、(4)相互運用性の 4 項目

の視点から要件を整理することが必要であるとする。その結果として、12 項目の個別の要件を抽出し、ユビキタスアクセス制御において満足されるべき要件として提案を行っている。

第 5 章から第 7 章は、それぞれ上記(1)から(3)までの視点から導出される要件を満足するアクセス制御プロトコルを具体的に定義・提案し、それぞれに対して、安全性の評価と計算量の評価とを行っている。安全性に関しては数学的な証明を与えている。

第 8 章は、(4)の視点から導出される要件を満足することを目的に、UACML (Ubiquitous Access Control Message Layer)を提案している。UACML は、第 5 章から第 7 章までのプロトコルを実現するメッセージの構文及び符号化規則の規定であり、環境側の計算機資源及びユーザの携帯端末が UACML に準拠することにより、ドメインに依存せず相互にアクセス制御のための通信を行い、アクセス制御機能を強調して実現することを可能とする相互運用性が実現される。UACML の設計に当たっては、下位通信層（主にデータリンク層）におけるプロトコルから独立であることに配慮すると共に、第 2 章でサーベイした現行技術によるデータリンク層での追跡不能性の実現では、通信の信頼性が保証されない可能性があるとの認識に基づき、UACML においてメッセージの信頼性やブロードキャストによる輻輳の解決が機能として盛り込まれている。

第 9 章では、デジタルコンテンツ流通への応用における課題について述べ、解決手法を提案している。デジタルコンテンツ流通は、特に音楽データを中心として急速に普及しつつあり、ユビキタス社会において真っ先に実現されるアプリケーションであると認識することができる。デジタルコンテンツ流通が直面している問題は、複数のコンテンツアーキテクチャや著作権保護機能（REL = Rights Expression Language）が乱立している現状に由来する。この課題は既に広く認識されており、REL を通信の 7 階層モデルにおける IP 層に見立て、REL 層を介して、上位の Application/Negotiation 層と下位の Enforcement/Physical 層とを連結する Jamkhedkary 等による階層モデルや、レンダリングフレームワークを共通のハブとして相互運用を目指す MPEG IPMP (Intellectual Property Management and Protection) 等の提案が存在する。これらの提案は、現行のアーキテクチャを分解し、再構成する必要がある点で、技術的に早期の実現が困難であるとともに、コンテンツ流通市場における利益関係の調整が必要であるという問題がある。本論文では、現行のコンテンツアーキテクチャと REL との間の橋渡しを行うブリッジレイヤを新たに設けることにより、現行アーキテクチャの構成と既存の利益関係に影響を与えない相互運用のモデルを提案している。更に、現行アーキテクチャの拡張性のモデルを分類し、モデルごとの拡張性を利用してブリッジレイヤに準拠できるレベルを考察し、安全性の限界についても評価を行っている。ブリッジレイヤでやり取りされるファイルの XML 定義やブリッジレイヤのレファランスモデルを併せて提案することで、実用という観点からも具体的な提案を行っている。

第 10 章の今後の課題では、提案しているプロトコルの機能及び性能を実証的に検証する項目を挙げている。本論文の研究は、経済産業省　平成 17 年度及び 18 年度新世代情報セキュリティ研究開発事業の委託研究として実施しており、本年度中にプロトタイプを作成する予定となっている。平成 19 年度以降に、プロトタイプの評価を行うものと期待される。

本論文の研究は、総務省「u-Japan 構想」等でも研究が進められている将来のユビキタス社会に関するものであり、特に、極めて重要な側面のひとつであるアクセス制御に焦点を当て、プライバシーを含めたアクセス制御共通基盤の要件を新たに整理している点、要件を満足する技術原理を提案している点、更に、実用に向けた考察を行い、直ちに実施可能な具体的な方式を提案している点、以上の 3 点において非常に意義がある研究であると考える。

よって、本論文は博士（工学）の学位請求論文として合格と認められる。