論文の内容の要旨

論文題目　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

氏　名　申　吉浩

本論文は、ユビキタス・コンピューティングにおけるプライバシーの問題を解決するアクセス制御方式、及び、そのデジタルコンテンツ流通への応用に関する研究結果を報告するものである。また、本研究は、経済産業省商務政策局「平成 17 年度新世代情報セキュリティ研究開発事業」及び「平成 18 年度新世代情報セキュリティ研究開発事業」の研究として行われた。

ユビキタス・コンピューティング(Ubiquitous Computing)という用語は、米 Xerox 社 PARC 研究所の Mark Weiser による論文「The computer for the 21st Century」（Scientific American, 1991）に由来する。この論文において、Weiser は、日常使用するあらゆる器具・機器に「見えない形で」コンピュータを組み込むことにより、ユーザに特別なコンピュータ・リテラシを要求することなく、コンピュータの効用を最大限に活用できると主張した。「Ubiquitous」とは、ラテン語で「遍在」を意味する。Weiser のこの考え方は、当時精力的に研究されていた人工知能（Artificial Intelligence）やバーチャルリアリティ（Virtual Reality）に対する強烈なアンチテーゼと受け止められ、命名の妙もあって、瞬く間に IT 研究者の耳目を集めるところとなった。爾来、ユビキタス・コンピューティングは、IT 技術の一つの集大成と目され、長年にわたる熱心な研究の対象となってきた。

近年の携帯端末の高機能化、移動体通信の広帯域化、無線 LAN によるホットスポットの普及など、コンピュータの利用環境の著しい進化に伴い、ユビキタス・コンピューティングは、いよいよ、研究室を飛び出し、実用化への道を歩み始めている。総務省においても政策懇談会が設置され、「u-Japan 政策」として、ユビキタス社会の実現に向けた提言がなされており、社会的な観点からも、ユビキタス・コンピューティングの実現が望まれている。

技術的に見ると、ユビキタス・コンピューティングとは、環境にネットワーク化されて埋め込まれた数多のコンピュータ群（センサー・ネットワーク）と、個人が携行するコンピュータ（ユーザ端末）との間の協調のためのアーキテクチャであり、ユーザに対して「シームレス」にサービスを提供することを目的とする。

「シームレス」とは、ドメイン間で機器やネットワークの構成が異なること、ドメインが各々独立のポリシーに支配されることとを前提とした上で、ユーザが複数のドメインの間を移動する場合においても、ドメインの違いをユーザに意識させること無く、継続的にサービスを提供する状態を指す。シームレスなサービス提供を実現するためには、ユーザが携行するコンピュータ（ユーザ端末）と環境中のコンピュータ（センサー・ネットワーク）とが不断に交信する必要がある。そして、ユーザ端末とセンサー・ネットワークの間の通信は、必要でない限り、ユーザを煩わせない、即ち、ユーザの目から隠蔽されて実行されることが求められる(透過性)。ユビキタス・コンピューティングにおけるプライバシーの問題は、センサー・ネットワークとユーザ端末とが透過的かつ不断に通信するアーキテクチャに由来し、ユーザによるサービスへのアクセスが検閲者によって追跡される脅威を指す。即ち、健全なユビキタス・コンピューティングの実現のためには、アクセス制御における追跡の防止は、避けて通れない問題である。本稿では、「ユビキタスアクセス制御」という言葉で、健全なユビキタス・コンピューティングにおけるアクセス制御を指すこととする。

本研究は、上記の問題意識に基づいて実施され、下記に述べる成果を報告する。

- プライバシーと公知との境界は、適用コンテクストによって動的に変化することは、広く認識されている（「Unpacking “privacy” for a networked world」, Palen and Dourish, 2003)。従って、ユビキタスアクセス制御においても、正しいプライバシーと公知の境界を定義する必要がある。本論文では、この問題に対する解として、Consensual Disclosure の考え方を提案する。Consensual Disclosure は、サービスへのアクセスが透過的に行われるユビキタス・コンピューティングの環境では、インフラストラクチャにおいては完全な追跡不能性が保証され、ユーザの明示的な同意なしには、一切の追跡情報が漏洩しないことを要求する。逆にいえば、環境の要請に対しユーザが明確な同意を与えた場合に限り、環境は、追跡情報を取得し、資源や社会の

安全等の用に供することができる。

- 追跡不能と Consensual Disclosure とを実現する具体的な認証方式を提案する。
  追跡不能性を有する認証方式としては、グループ署名技術が知られている。しかしながら、グループ署名は、計算量が大きく、高頻度のアクセスイベントが発生するユビキタスコンピューティングに適用するには欠点があると思われる。しかも、認証とアクセス制御の統合等、ユビキタスコンピューティング固有の要求に応えて機能を追加すると、更に、計算量が増加すると考えられる。
  本研究では、グループ署名ではない通常の高速な署名方式における鍵管理方式を工夫することで、追跡不能性と Consensual Disclosure を満足し、かつ、高速な認証方式を考案した。認証処理の計算量を楕円曲線上のスカラー倍演算の実行回数に換算して比較すると、20 倍～7 倍程度の改善を得られることが分かった。
- 本研究で提案する追跡不能認証方式は、証明可能な安全性を有している。方式が証明可能であるとは、広く受け入れられている暗号学的仮説にその方式の安全性が論理的に帰着されることを指し、近年、暗号アルゴリズム等を提案する際には、証明可能な安全性を示すことが求められる。
  本研究では、後述するユビキタスアクセス制御の要件を機能として満足するために、併せて 13 の基本的プロトコルを提案するが、その全てに対して、上記の意味での安全性の証明を与える。
- 認証とアクセス制御の統合等、ユビキタス・コンピューティングには、固有の要求があることが知られているが、アクセス制御の観点からこれらを網羅的に整理した事例は存在しなかった。本研究では、13 項目の要件項目に整理し、それらの要件をサポートするユビキタスアクセス制御のためのプロトコルを提案する。このプロトコルは、前記の追跡不能性と Consensual Disclosure を満足する効率的な認証方式をベースとし、要件をサポートするために機能を追加するに当たって、計算量の大きな暗号処理を共有する工夫を行うことで、効率的なプロトコルとなっている。
- 本研究では、前記プロトコルに対して、相互運用のためのメッセージ規定として UACML (Ubiquitous Access Control Message Layer)を提案する。UACML は、既存の公開鍵基盤に準拠し、また、データリンク層からセッション層における通信において追跡不能性を実現するための既存の技術との相互接続性を有するように設計される。UACML では、交換されるメッセージの構文、意味(セマンティクス)、符号化方式を紛れなく規定することにより、ドメインを横断した相互運用性を実現する。
- ユビキタスコンピューティングの特徴を最もよく反映したサービス例として、デジタルコンテンツ流通がある。本研究ではユビキタス・アクセス制御の要件を整理するにあたり、特に、網羅性を確保するために、デジタルコンテンツ流通への適用を指標としつつ、作業を進めてきた。一方、デジタルコンテンツ流通は、現実のアプリケーションとしても非常に重要であり、また、ユビキタス・コンピューティングの普及に当

たってはインパクトが大きいことも事実である。従って、本研究で提案する方式を実際にデジタルコンテンツ流通に適用することにも意義を見出すことができる。しかしながら、現実の適用のためには、よく知られた「コンテンツ保護」と「決済・著作権処理」の相互接続の問題を解決する必要がある。本論文の最後では、ブリッジレイヤによる、この問題の解決法を示した。

現在、本研究で提案したプロトコルのプロトタイプの実装を進めており、プロトタイプを利用して、下記の課題を検証していく計画である。

- 実運用に近いテスト空間における認証速度の実測
- ローミング技術やサービス探索技術等、ユビキタス環境における他の技術との整合性