

(続紙 1)

京都大学	博士（情報学）	氏名	五味 秀仁
論文題目	Fine-grained and Flexible Identity Management in Distributed and Open Environments（厳格な保護と柔軟な活用を両立するアイデンティティ管理技術）		
（論文内容の要旨） サイバー社会における人の活動が増えるにつれて、多くの個人に関する情報が管理され、また、やり取りされるようになってきている。これに伴い、サイバー社会上で唯一に識別される個人のデジタル表現(アイデンティティ)の適切な管理は重要な課題と認識されてきている。アイデンティティ管理は、アイデンティティ情報を、生成されてから廃棄されるまで、その情報保有者のプライバシーを保護しながらも、安全に保管し利用するプロセスであり、情報保有者や利用者の利便性とセキュリティとプライバシーのバランスが重要となる。しかし、従来のアイデンティティ管理に関する技術では、現在露見しており将来さらに顕著になると予見するプライバシーに関するリスクについて、十分に考慮していない。 本博士論文では、オープンかつ分散的な環境において、上記プライバシーを保護しつつセキュリティを担保しながらも利用者の利便性を備える、きめ細かで柔軟なアイデンティティ管理技術を提案し、それらの技術を用いて利用者が安全に安心してサイバー空間での活動を促進できるようにすることを目的とする。本博士論文の研究成果は以下の四項目にまとめられる。 第一は、アイデンティティの永続的な追跡とそのポリシー配備である。アイデンティティ管理に関する既存の技術では、利用者は自らのアイデンティティ情報がどのように管理され、用いられ、交換されているか明確に知ることができない。そこで、それら情報がドメインを越えて移動した後でもなお追跡し、移動後の環境における情報取り扱いポリシーにも自らの意向を反映したポリシーを矛盾なく融合するフレームワークを提案した。これにより、利用者は、自らのアイデンティティ情報の移動履歴や現在の状態を永続的に把握した上で、それら情報を自らの望む通りに管理し活用できる。 第二は、アイデンティティの信頼性メトリックとその評価方式である。既存のアイデンティティ連携技術では、利用者の認証アサーション(認証証明書)を発行する認証プロバイダやその送付に関わる仲介プロバイダが複数伴うと、利用者のアイデンティティの確からしさを正確に評価することが困難であった。そこで、認証すべき利用者のアイデンティティ、アサーション発行、アサーション送付仲介の三つの信頼性に対するメトリックを定義し、利用者のアイデンティティの確からしさの定量的表現を導出する方式を考案した。これにより、アイデンティティ情報の不正利			

用を厳格に防止しつつ、柔軟な活用が可能となる。

第三は、アクセストークンを用いた動的な権限委譲である。権限委譲とは、ある利用者が自らの保有する権限を他の利用者に委譲する行為であり、従来、企業内システムなど閉じた環境でよく実装されたが、分散環境においては十分に検討されていない。そこで、権限保有者の委譲したい権限をアクセストークン及び権限を行使するための制約条件と関連付けて管理するアクセス制御モデルと設計フレームワークを提案した。これにより、権限保有者は所定の権限を自らが指定した利用者にだけ一定の条件下でのみ委譲でき、きめ細かな権限付与と柔軟な情報活用を実現できる。

第四は、オープンな環境におけるソーシャルなアプローチによる権限付与である。本項目は、第二と第三の項目の研究成果を合わせて実現する本稿の最終目標である。従来の認証システムでは、利用者は認証されるためにはパスワードなどの事前登録が必要なため、未登録の利用者は、権限を委譲されても行使することができなかった。そこで、利用者自らが権限を委譲したい第二の利用者を認証した結果をシステム参加者間で共有し、前記第二の利用者のアイデンティティの確からしさを評価する方法を提案した。これにより、システムに未登録の利用者でも、その確からしさに応じて柔軟に権限を付与し、情報活用を促進できる。

注) 論文内容の要旨と論文審査の結果の要旨は1頁を38字×36行で作成し、合わせ

て、3,000字を標準とすること。

論文内容の要旨を英語で記入する場合は、400～1,100 wordsで作成し
審査結果の要旨は日本語500～2,000字程度で作成すること。

(論文審査の結果の要旨)

本論文は、サイバー社会上で唯一に識別される個人のデジタル表現をアイデンティティと定義し、オープンかつ分散的なアイデンティティ管理のための新たな技術を提案している。システムに参加するエンティティ間の信頼性は確立していない状況で、利用容易性、安全性、プライバシーの間のバランスを考慮した新たな技術を開発した点で提案手法の新規性が評価される。

永続的なアイデンティティ追跡においては、既存の技術がアイデンティティ連携や個人属性交換の標準化の支援などに偏重していたのに対し、利用者中心主義を徹底するために、利用者が自身の情報を制御するという観点からドメインを越えるアイデンティティ管理の枠組みを与える新たなアプローチに基づく方法を提案した。このアプローチに基づき、既存の方法とは異なりドメインを越えた二次配布を許容することにより移動を繰り返すアイデンティティ情報のライフサイクル管理をメモリのオーバフローや非効率化を最小限にしながら実現する方法を開発した。アプローチの新規性と共に、提案方法の新規性、有用性が認められる。

認証されたアイデンティティの信頼性メトリックとその評価方式では、アイデンティティ連携管理システムで必要となるアイデンティティに関する認証アサーションの生成、伝搬に関わるエンティティの信頼性を定量的に評価する手法を与えている。本研究では、信頼性の論理表現を用いた形式化及び定量化を行っている点に新規性が認められる。また、動的に生成されネットワークを伝搬するアサーションを用いて、評価が必要な認証アイデンティティに対する信頼性メトリックを与える点に新規性があり、有用性を認めることができる。

アクセストークンを用いた動的な権限委譲では、オープンで分散的な環境で権限委譲を実現するためのトークンに基づくアクセス制御の枠組みを提案している。権限保有者の依頼に応じアイデンティティ管理者により発行されるトークンに発行者の秘密鍵と権限IDを連結した値のハッシュ値を含めることにより改竄などの攻撃を防止しつつ、柔軟なアクセス権限付与を実現しており、また、権限保有者がトークンに代理者認証のタイプを指定することにより、なりすましを権限保有者の求める方法で防止可能としている。本手法は、従来の閉じた組織で利用されてきた権限委譲とは全く異なり、オープンで分散的な環境に適した方式であり、新規性が評価できる。

アイデンティティ管理者に未登録の利用者に対し、アイデンティティ情報利用を動的に認証するために、権限保有者が信じる程度に応じて柔軟にアクセスを認可する手法を与えている。この手法は、オープンな環境において上述の利用者間の認証スキーム及びアイデンティティ連携を用いて協同的に認証結果を共有することにより、システムに登録されていない利用者のアイデンティティの確実さを定量的かつ柔軟に評価するものであり、その新規性が評価できる。

よって、本論文は博士（情報学）の学位論文として価値あるものと認める。

また、平成24年2月22日に実施した論文内容とそれに関連した試問の結果合格と認めた。

注) 論文審査の結果の要旨の結句には、学位論文の審査についての認定を明記すること。

更に、試問の結果の要旨（例えば「平成 年 月 日論文内容とそれに関連した口頭試問を行った結果合格と認めた。」）を付け加えること。

Webでの即日公開を希望しない場合は、以下に公開可能とする日付を記入すること。

要旨公開可能日： 年 月 日以降