電子商取引の高セキュリティ化に関する研究

田村 裕子
北陸先端科学技術大学院大学

平成 16 年 3 月 30 日

論文の内容の要旨

高度情報化・ネットワークの進展に伴い，多種多様な電子商取引が普及しつつある反面，悪意ある取引相手による情報の改ざん，漏洩などの犯罪が深刻化している．このような問題を防ぐ方法として，犯罪の未然防止，情報の漏洩防止，また電子商取引の高セキュリティ化が考えられる．未然防止とは，取引にまつわる情報が信頼できるものであるか判断し，信頼できると確認できたときに限り取引をおこなうことを意味する．また，漏洩防止とは，取引の際，相手ユーザに個人情報を与えないことを意味し，電子商取引の高セキュリティ化とは，現在広くインターネット上で普及しているオークション等にセキュリティ技術を導入したシステムの再構築を意味する．

未然防止技術として，信頼できる第三ユーザによる保証という概念を取り入れた保証付署名技術，漏洩防止技術として匿名証明書システム，また電子商取引の高セキュリティ化としては，現在最も広く普及している代理入札システムをとりあげる．

保証付ディジタル署名に関する研究 あらゆるユーザの参加を可能とする電子商取引にまつわる犯罪の増加はインターネットの裾野が広がるにつれ深刻化しており，見知らぬユーザとの取引はリスクを伴うものとなっている．このような犯罪を未然に防ぐには，取引内容の信用性，取引相手の信頼性の確保が必要不可欠である．このような取引内容，または取引相手といった情報の正当性を保証するには，実社会にある信頼できる第三ユーザによる保証という習慣が有効に働く．本稿では，保証付ディジタル署名を厳密に定義し，それを実現するための手法を提案する．

匿名証明書システムに関する研究 ユーザが病院，クレジットカード会社，商店等の各機関と取引をおこなう場合，各機関はユーザに関する情報を保有することになる．仮に，各機関が取引のあるユーザの個人情報を流出した場合，普及したインターネット網はまたたく間に個人情報を拡散することになるだろう．それによって，各機関が独自に所有していたユーザの情報が結合し，個人情報はユーザの意図しない範囲にまで拡散する結果となる．このような機関の結託による情報の拡散・漏洩から個人情報を守ることのできる匿名証明書システムは，個人ユーザが各機関に提供する情報の利用方法を制御できる手法であり，ユーザと機関の間に安全な関係を構築する．しかしながら，既存の方式は必要以上の情報を検証者に与える恐れがあり，完全な匿名性を実現しているといえない．また，機関がユーザの属性，権限を証明できるものであったとき，このようなシステムを属性認証システムとして，オンラインサービスなどにおける利用者認証に利用することができる．本稿では，匿名性を強化した証明書システムと，複数の属性を効率的に示すことのできる複数匿名証明書システムの提案をおこなう．

電子オークションに関する研究 あらゆる電子商取引のなかでも，とりわけ電子オークションは広く世界中で普及しているが，オークション参加者のプライバシを守ることのできる安全なオークションシステムの構築が求められている．現在のインターネット・オークションにおいては，入札値の管理・個人データの管理をオークション管理者が一括しておこなっているため，高セキュリティなシステムであるとはいえない．本稿では，対象とするオークションスタイルをインターネットの利点を生かした代理入札とし，安全でかつ効率的なシステムの構築をおこなう．