氏　　名	廣田　啓一
学位（専攻分野）	博士（情報学）
学位記番号	総研大甲第1200号
学位授与の日付	平成２０年９月３０日
学位授与の要件	複合科学研究科　情報学専攻 学位規則第６条第１項該当
学位論文題目	秘密分散法を用いた電子権利二次流通方式の研究
論文審査委員	主　査　教授　曽根原　登 教授　東倉　洋一 准教授　岡田　仁志 教授　山田　茂樹 教授　安田　浩（東京電機大学）

論文内容の要旨

本研究は，近年著しく普及が進んでいる電子権利を対象として，利用者間で権利取引を行う二次流通を可能とする，安全かつ簡便な権利二次流通方式を実現することを目的とする．

従来の権利流通方式は，安全性を確保するために，公開鍵・秘密鍵の複雑な管理と電子署名や検証などの演算処理，端末間での複数回の通信処理を必要とし，直接的かつ同期的な権利流通に限られ，利便性に欠けていた．

本研究では，利便性の問題を解決するために，有限体上の多項式を用いた比較的簡易な演算処理で情報量的安全性を実現する情報保管技術である秘密分散法の，権利流通方式への適用を検討し，秘密情報の一部分を一意に復元可能とする部分情報の復元制御が可能となる方式を考案した．また，これにより権利流通方式への適用を可能とし，権利取引に必要な情報を分散流通させることにより安全かつ簡便な権利取引を行う，新たな電子権利二次流通方式を実現した．

提案方式は口座管理型の電子権利を対象とするもので，譲渡元ユーザが生成した権利取引を宣言する取引情報を，秘密分散法を用いて分散符号化して流通させることで，秘密情報の解読や取引情報の改竄，偽造といった攻撃に対して安全な権利流通を可能とする．また，提案方式では，譲渡元ユーザと譲渡先ユーザ，権利管理機関の３者間において，最少となるただ２回の非同期なトランザクションで権利取引が完了するため，任意のコミュニケーション手段を使った取引情報の流通を行うことができ，また第三者への安全な権利取引の預託が可能となり，利便性の問題が解決される．

本研究の成果は，比較的簡易な演算処理で情報量的安全性を実現するセキュリティ技術である秘密分散法に着目し，秘密分散法を用いた新たな権利二次流通方式を実現したことにある．本研究で実現した権利交換プロトコルは，安全性だけでなく匿名性や健全性といった権利取引の要件を満たし，かつ取引情報の安全性が情報量的に保証されることを明らかにした．このため，従来の権利流通方式では困難であった，第三者への権利取引の預託が可能となった．

また，提案プロトコルに基づくC2B2C型の権利二次流通システムを設計し，提案方式の安全性と利便性を理論的に示すだけでなく，その有用性を検証した．今後，技術とビジネス（市場）の関係にとどまらず，社会の規範（商習慣）や公共政策，法制度との関係を含めて提案方式を実用化する．

以下、本論文の構成とその概要について示す．

第１章では，本研究の背景を述べ，電子権利の流通市場と二次流通について示す．また，本研究が対象とする権利取引の要件と，既存の権利流通方式および権利流通システムの課題の簡単な整理を行い，本研究の目的を示した後に，本論文の構成を概観する．

第２章では，本研究が対象とする電子権利の定義とその実現方式，および権利流通のモデルについて整理した上で，従来研究の調査に基づいて既存方式の分類を行い，権利流通方式に求められる要求条件を整理する．また，権利流通方式の分類として，口座管理型の電子権利と価値保存型の電子権利のそれぞれについて概要を示し，既存の権利譲渡プロト

コルおよび権利交換プロトコルの方式例を示す．さらに，本研究が主眼とする電子権利流通の安全性と利便性の両立の観点から，既存方式に対する評価を行うとともに，既存方式の課題について示し，本研究で解くべき技術的課題について整理を行う．

第３章では，比較的簡易な演算処理により情報量的安全性を実現するセキュリティ技術である秘密分散法について概説し，権利流通方式への応用に向けた検討を行う．秘密分散法は，秘密情報を複数の分散情報に分散符号化することで秘匿化するもので，一定数未満の分散情報からは秘密情報を復元できず，情報量的に安全である．本研究では秘密分散法の従来手法における部分情報復元の原理を明らかにし，分散関数への適用を行うことで，特定の分散情報の組み合わせにより任意の部分情報一意な復元を可能とする，復元制御型の秘密分散法を考案した．考案方式について述べるとともに，低次の分散関数における構成例を示す．また，アクセス構造と情報量に関する既存手法との比較評価を行い，その安全性を示す．

第４章では，復元制御型の秘密分散法を用いた権利二次流通方式として，情報量的に安全な権利交換プロトコルについて示す．提案プロトコルは，口座管理型の電子権利を対象とするもので，電子権利の所有者が権利取引を宣言する情報を生成して複数の分散情報に分散符号化し，譲渡元ユーザと譲渡先ユーザおよび権利管理機関の３者間においてこの分散情報を流通させることで，権利取引を実行する．利便性の向上を目的にトランザクション数の削減を図って譲渡元ユーザから権利管理機関への分散情報の送付を不要とし，３者間において２回のトランザクションで権利取引が完了する，最少のトランザクション数による権利交換プロトコルを実現した．プロトコルの安全性および利便性についての評価を行い，その有効性を確認する．

第５章では，提案プロトコルを用いた権利二次流通システムの実現に向けて，まずC2B2C型の権利取引を行う二次流通の市場モデルについて調査し，プロトコルの適用を検討する．市場モデルの比較の結果として，譲渡元ユーザによる権利取引の提案をブローカが仲介することにより取引機会の増加を図る，ブローカ仲介モデルによるC2B2C型権利二次流通システムの設計を行った．電子チケットを対象とした権利二次流通システムの構成を示し，譲渡元ユーザおよび譲渡先ユーザの持つユーザクライアント，ブローカの持つ取引仲介サーバ，権利管理機関の持つ権利管理サーバのそれぞれにおける処理の概要と，各装置間のトランザクション，および権利取引の管理と制御について記述する．また，設計したシステムの安全性と利便性について議論し，その有用性を示す．

最後に第６章で本研究の成果をまとめるとともに，提案方式の実用化に向けた課題の整理を行って，本論文のまとめとする．

論文の審査結果の要旨

本博士論文は，近年普及の著しい電子権利を対象として，利用者間での安全かつ利便性の高い権利取引を実現する電子権利流通方式を提案するものである．従来の権利流通方式は，安全性を確保するために，公開鍵・秘密鍵などの複雑な管理と電子署名や検証などの演算処理，端末間での複数回の通信処理を必要とし，直接的かつ同期的な権利流通に限られ，第三者への預託ができないなど利便性に欠けていた．本研究は，秘密分散法を用いた電子権利二次流通方式の実現による問題の解決を行った．提案する方式は，権利管理機関が管理する利用者の電子権利の取引情報（権利取引情報）を分散流通させることで，強い安全性と権利取引の匿名性，健全性を保証し，かつ権利取引情報の間接・非同期での流通と第三者への預託を可能とする．このため，効率的かつ利便性の高い電子権利流通システムを実現することができる．

本研究では，特に利便性の問題を解決するために，権利取引情報の分散流通と復元を行うための，権利流通方式への適用が可能な秘密分散法について研究した．まず秘密分散法による秘密情報の分散と復元について検討し，従来方式における部分情報の復元の原理について明らかにした．さらに部分情報の復元の原理を応用して，秘密情報の一部分を一意に復元可能とする部分情報の復元制御が可能となる方式を考案した．考案方式は，分散関数により秘密情報を分散符号化した複数の分散情報の組み合わせによって，秘密情報の部分復元と完全復元を制御するもので，有限体上の多項式を用いた比較的簡易な演算処理で実現することができる．また，考案方式が従来方式技術と同等の情報量的安全性を有していることを理論的に示した．

次に，考案した秘密分散法を用いた権利流通方式について検討し，権利取引情報を分散流通させることにより，安全かつ簡便な権利取引を実現する権利流通方式を提案した．提案方式は口座管理型の電子権利を対象とするもので，譲渡元ユーザが任意に生成した権利取引を宣言する権利取引情報を，秘密分散法を用いて分散符号化して流通させることで，譲渡先ユーザにおける権利取引情報の部分復元と権利管理機関における完全復元を制御し，秘密情報の解読や取引情報の改竄，偽造といった攻撃に対して安全な権利取引流通を可能とする．また，提案方式では，譲渡元ユーザと譲渡先ユーザ，権利管理機関の３者間において，最少となるただ２回の非同期な通信で権利取引が完了するため，任意の手段を使った間接的な権利取引情報の流通を行うことができ，また第三者への安全な権利取引の預託が可能となるため，利便性の問題が解決される．

本研究成果は，比較的簡易な演算処理で情報量的安全性を実現するセキュリティ技術である秘密分散法を用いて，利便性と安全性を両立する新たな権利二次流通方式を実現したことにある．本研究で実現した権利交換プロトコルは，安全性だけでなく匿名性や健全性といった権利取引の要件を満たし，かつ取引情報の安全性が情報量的に保証されることを明らかにした．このため，従来の権利流通方式では困難であった，第三者への権利取引の預託が可能となった．また，提案方式によるブローカ仲介モデルに基づくC2B2C型の権利二次流通システムを設計し，安全性と利便性に関する評価を行ったことで，提案方式の安全性と利便性を理論的に示すだけでなく，その有用性を検証した．

本論文は，秘密分散法を権利流通方式に用いるという独創的な発想を現実的な方式として実現したもので，新規性，有効性，信頼性を十分に備えており，かつ新たな秘密分散法の考案による学術的価値も十分に認められる．さらに権利流通および電子商取引市場の普及とその拡大に不可欠な技術的進歩だけでなく，サービス科学の側面からも情報通信産業界での実用化や社会貢献が十分に期待できる．さらに，出願者は，要件となる学術業績を達成しており，本論文が複合科学研究科における博士授与の基準に達しているものと判定した．