検証進化可能電子社会
–情報科学による安心な電子社会の実現–

片山 卓也　北陸先端科学技術大学院大学情報科学研究科　katayama@jaist.ac.jp

「検証進化可能電子社会」拠点形成計画の目指すもの

我々の生活は複雑で大規模な情報システムによって支えられており，我々はすでにかなり電子化された社会に住んでいるが，その度合いは今後ますます加速されることが予想される．ビジネス効率化のために行われるIT化，政府が推し進めている電子政府計画などのほかに，遠隔教育や遠隔医療など，電子化の波は我々の社会活動のあらゆる側面に及ぼうとしており，我々は本格的な電子社会の時代を迎えようとしている．そこでは，政治，経済，司法，行政，医療，教育など社会生活の基幹部分のすべてが電子社会システムとして電子化され，これまでにない便利で住み良い社会を作ることが可能になると思われる．同時に，情報システムの持つ欠陥や不完全さなどから，不便や不利益を被り，さらには，生命や財産の危機に直面し，あるいは，システム変更の困難さから新しい要求や変化に対応できず，社会が硬直化する恐れもある．

電子社会のこのような負の側面を解決し，安心して生活を任せられる電子社会を構築するために，情報科学における最新の数理的方法やソフトウェアテクノロジー，人工知能などの研究成果を用い，安心な電子社会のための基本概念や技術のための研究教育拠点を確立することが，本COE拠点の目指すものである．すなわち，電子社会システムを形式的にモデル化し，それが安心性の要件を満たすことを，形式検証技術やシミュレーションを用いて確認するための方法論，社会情勢の変化に応じて電子社会システムを進化発展させるための方法論などの研究を行う．それと同時に，教育プログラムの整備により，安心電子社会システムを設計，開発する能力を持った研究者や高級技術者の育成を行う．本拠点は，平成16年度に「革新的分野」において採択され，これまでに約半年間活動を行ってきた．本稿では，拠点の内容や構想などを中心にして，本COEプログラムを簡単に紹介する．

安心な電子社会

電子社会とは，我々の社会システムのうちで，情報システムによって実現されている部分であり，その役割は，我々の行う社会活動の支援である．我々の社会活動は非常に多様であるが，電子社会は，我々がこれらの社会活動を円滑に行い，安心して生活を送ることができるベースでなければならない．その意味で，電子社会の安心性は電子社会に対する最も重要な要求である．最近の情報漏洩問題や，過去において大きな社会問題となった組織統合に起因するシステムの動作不全などは，電子社会に対する信頼を損ね，社会全体を機能不全に陥れる可能性がある．また，税金などの計算の間違いなど，さまざまなシステムの誤りや不備が報道されているが，安心な電子社会ではこれらの問題が解決されていなければならない．一方，複雑な年金システムなどのような社会制度自身の持つ分かりにくさなどを，情報技術を使って分かりやすく見せることも，安心できる電子社会では実現されなければならない問題である（図-1）．

電子社会の安心性に我々が期待するものはいろいろであるが，本拠点では，特に基本的なものと思われる，電子社会の中で行われるサービスや機能に誤りがないこと（正当性），それらのサービスや機能に関する質問に対して説明が可能であること（アカウンタビリティ），電子社会の中のデータへの不正なアクセスや漏洩がないこと（セキュリティ），社会の変化に応じて電子社会を進化させられること（進化性），および，耐故障高信頼情報基盤によって支えられていること（ディペンダブル基盤），などを主な研究対象とし研究を行う．

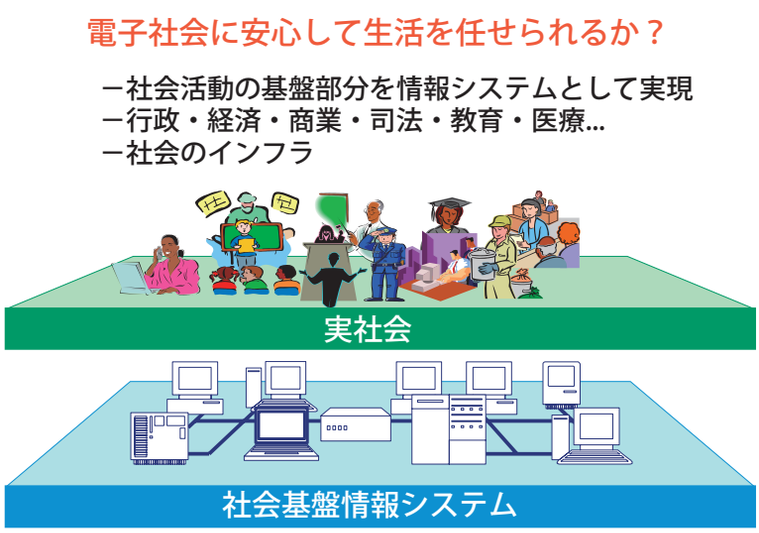

図-1　電子社会

安心電子社会の実現 ―形式仕様，検証，モデル

正当性の高いシステムの開発には，形式手法が優れている．これは，システムの仕様を形式論理などの数学的な概念を用いて厳密に与え，それに基づいてシステムの構築を行うものである．先進的あるいは研究的なシステム開発では効果を上げているが，一般システムの開発には用いられる段階にはなっていない．一方，進化性を要求されるシステムに対しては，モデル駆動開発方法論が良いとされる．これは，構築すべき情報システムの実装プラットフォームとは独立な（抽象的な）モデルをまず構成し，それをもとに実システムを作成するという方法論である．これにより理解性が高く，進化やプラットフォームの変更に強いシステムが構築可能であるというのが，最近のソフトウェア工学の見解である．したがって，電子社会システムのような高い正当性や進化性を要求される情報システムの構築は，

(1)仕様の形式化
(2)モデルの構築
(3)モデルが仕様を満たすことの検証
(4)モデルの実現

というステップで行われるべきである．仕様は，情報システムの提供する機能やサービスの内容あるいはそれらの満たす性質などを明確に表現したものであり，矛盾を含まず整合性のとれたものでなければならない．また，モデルは仕様を満たすものでなければならず，これは何らかの方法で検証されなければならない．正しいことが検証されたモデルは，実装プラットフォームに関する情報が加えられ，最終的には計算機システムとして実現される．

残念ながら，現実のほとんどの情報システムはこのような方法で開発されてはいない．事実，システム開発の失敗の主要な原因は，仕様の明確化を十分に行わずにシステム開発を行ったことによるものであるとされている．その理由は，合理的なコストと時間で厳密な仕様やモデルを構成するための技術が十分には開発されていないことによるものである．このような観点に立って，本COEプログラム「検証進化可能電子社会」では，電子社会の形式的仕様記述，モデル化，形式検証方法論，進化方式，高信頼プラットフォームによる実現などを中心にして，安心な電子社会の構築方法論の研究を行う．

電子社会の形式仕様化

電子社会の仕様は，基本的には，我々の実社会を規定している法律や法令などである．もちろん，このように明確に規定されているもの以外にも，社会慣行などによって暗黙的に規定される部分も考えなければならないが，いずれにしても，仕様が矛盾を含まず整合性がとれていることや，モデルが仕様を満たすことを確実に検証するためには，仕様は形式的あるいは機械的に処理可能な形に表現されなければならない．法律文を述語論理により表現する研究や，それから法律的結論を導き出すための推論の研究には長い歴史があるが，その目標は裁判などの法律適用場面の機械化を目指すという側面が強く，情報システムの仕様としての利用はあまり意識されていない．現実の法律業務での利用を考えると，法律文の持

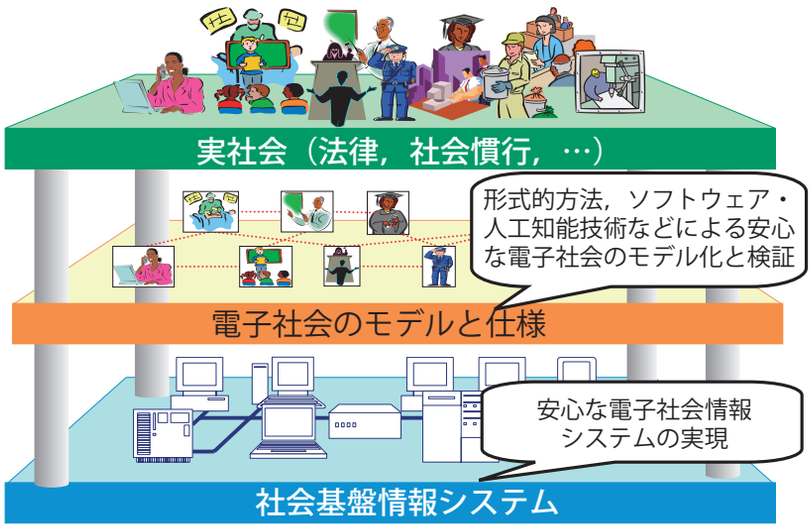

図-2　安心電子社会の実現

つ不完全さや法律の解釈の問題など機械化の困難な問題が多い．これに対し，最終的に情報システムとして実現可能な範囲内に限れば，法律文を電子社会の仕様として考えることは大いに可能性がある．現実の情報システムの開発では，信頼のおける仕様を限られたコストで作ることの困難さが指摘されてきたが，十分に推敲された法律文によって規定される電子社会や電子政府システムは，形式的開発に向いたシステムであるということができる．

電子社会のモデル構築

安心な電子社会の構築には，電子社会の明確なモデル化が必要である．これは，電子社会を実社会に存在する概念や性質を使って適切な抽象度でモデル化したものである．モデル化の目的は，実装に関する詳細から独立な形で電子社会情報システムを明確に表現することにより，検証や進化を行いやすくすることである．モデルの検証や進化を通して得られた適切なモデルは，計算機システムによる実現情報を与えられて，電子社会情報システムとして実現されることになる．電子社会は，究極的には，プログラムの集まりとしての情報システムとして実現されるが，プログラム自身を対象として電子社会の安心性を議論することは適当ではない．プログラムに表現されるものは，直接的にはプログラムの動作や振る舞いであり，電子社会の性質を論ずるには詳細すぎる．電子社会としての性質は，複雑なプログラムの構造と振る舞いの中に隠れてしまい，その検証や進化を適切に行うことはほとんど不可能である．電子社会の性質を論じるに必要十分なレベルでモデルを設定し，そのモデルに対して安心性に関する議論を行う必要がある（図-2）．

電子社会の検証

電子社会がモデルとして明確に与えられることにより，電子社会の満たすべき性質，とりわけ安心性を直接的に議論や検証の対象とすることが可能になる．検証は，モデルが電子社会の仕様に関して正しいか否かを判定することである．検証の方法としては，形式検証とモデル実行が考えられる．形式検証とは，定理証明などの形式論理学的手法によって電子社会の性質を検証（証明）しようとするものである．一方，モデル実行とは，電子社会のモデルを実際に実行させ，それによりモデルが適切か否かをテストするものである．もちろん，これには，電子社会モデルを実行させるためのメカニズムが必要になる．

電子社会の仕様やモデルが記述され，計算機による検証が可能なことの意義は大きい．新しい組織や制度の設計など，電子社会の進化や変更を行う場合には，それが意図したものであることを確認し，既存の制度と整合性があることを事前にチェックする必要がある．もし，計算機による検証や解析が可能であれば，より確実にかつ網羅的にチェックを行うことが可能になるからである．電子社会の時代には，それにふさわしい社会や組織の表現があるべきで，電子社会の仕様やモデルはそのようなものになり得ると考えられる．これらは自治体や政府レベルで管理，保守されるべき社会の設計図であり，これを機械的に検証や実行可能な形で保有することは透明性の高い社会の実現に有効である．

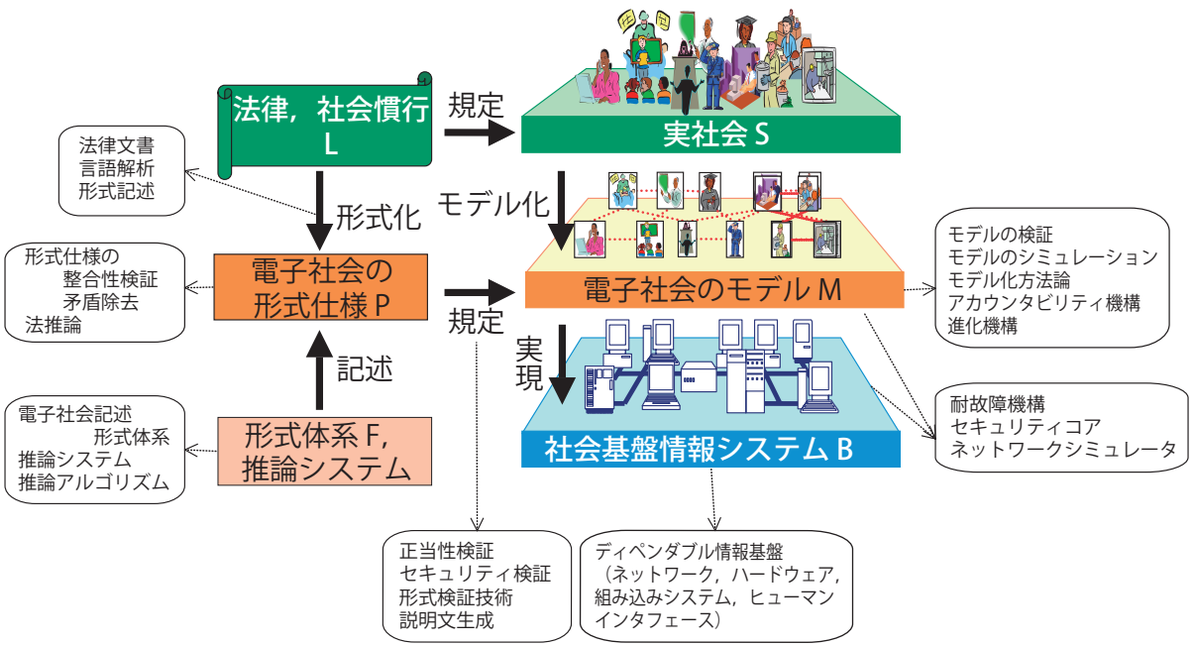

図-3　研究の概要

電子社会研究における「検証進化可能電子社会」の特徴

以上，COE プログラム「検証進化可能電子社会」の基本的な考え方を述べてきた．もちろん，現実の社会は複雑であり，人間的かつ柔軟な処理が求められる事柄も多く，上に述べたような方法がすべてにおいて可能になると主張するものではない．我々が研究の対象にしようとするものは，あくまでも社会活動のうちで情報システムによって実現可能，あるいは，実現すべきと思われるものである．現実には，このようなものについても，十分に明確な設計思想なしにシステムの設計や構築がなされ，その結果，不完全で使いにくいシステムが作られ，その保守管理に多額の費用が費やされていることが多い．我々のプログラムは，社会システムからの要求を，安心性の確保という観点で明確にしたうえで，安心性の高い情報システムを実現する科学的方法論を確立しようとするものである．

これまで電子政府や電子社会の研究としては，社会科学的な面では，(1) 電子社会のための法整備や制度設計などの研究，(2) 電子社会の中での人間の心理や人間関係などに関する研究，また，計算機科学的研究では，(3) 電子社会の中のデータの活用やデータベースに関する研究，(4) 情報セキュリティに関する研究，などが主に行われてきた．これに対して，我々のアプローチは，電子社会を情報システム的にとらえ，安心な電子社会の実現を目指すものである．

研究の概要と研究課題

これまで述べてきたように，本 COE では安心して住める電子社会の実現を情報システムの立場から，「検証と進化」というキーワードでとらえ，そのための科学的工学的方法論を展開しようとするものであり，図-3 はその研究内容を全体的に表したものである．我々の社会活動はきわめて多岐にわたるが，電子社会として実現されるものは，法律や社会慣行 L によって規定されており，情報システムとして実現される場合にはその内容は形式仕様 P として形式化される．P は電子社会仕様記述のための適切な形式論理体系 F によって記述される．一方，電子社会のモデル M は，実社会を反映して構築され，それは形式仕様 P を満たすものでなければならない．モデル M は，最終的には社会基盤情報システム B として実現される．図-3 は，このような観点に立って，安心な電子社会実現のために計画している研究項目を示したものである．以下では，これらの研究項目の内容を簡単に紹介する．

電子社会の形式仕様記述体系

電子社会の仕様とは，そこに存在する個人や組織，それらの間の関係，特に役割や権利・義務関係などの電子社会の構造と，それらの提供するサービスや機能などの満たすべき性質や定義を記述したものである．現実社会では，それらは法規や社会慣行などによって定められているが，これを形式的に記述することは，電子社会モデルの正しさなどの安心性要件の検証を計算機によって支援する基礎になる．これまでに，ソフトウェアの形式仕様記述に用いられる多様な形式体系が考えられてきたが，その基礎になっているものは，形式論理体系であり，述語論理や等式論理，あるいは，時間論理などの種々の非古典論理が研究されてきた．これらの研究をさらに推し進め，電子社会の形式的記述のための論理体系とそれらを支える数学的基礎理論の研究を行う．また，そのような論理体系のための推論システムの構築法やそのためのアルゴリズムの研究を行う．

法推論と言語処理

我々の社会の構造や機能は，その基本的部分には各種の法律や法規によって明示的に記述されている．したがって，法律や法規の機械処理は電子社会システム研究の中心である．法律の機械処理の研究は長い歴史を持つが，法律自身の持つ複雑さ，特に，現実の社会を法律で明確に定義することの難しさから，現実の法律適用の場面で法推論システムが使われるには至っていない．しかしながら，電子社会が最終的には情報システムによって実現されることを考えれば，電子社会を規定している法規や社会慣行は形式的に定義可能なはずであり，計算機による法推論が有効であると考えられる．この点に関して法律記述に適した論理体系やそこでの推論方式やアルゴリズム，法律論理表現からの矛盾除去などの研究を行う．それとともに，法律文書から形式論理表現への変換，推論結果からの説明文の生成などの自然言語処理の研究を行う．理論的研究のみならず，地方自治体業務などを実例として研究を進める．

電子社会のモデル化

電子社会のモデルとは，電子社会の中に存在する個人や組織，それらの機能や振る舞いなどを直接的に記述したものであり，検証や情報システムによる実現の対象となるものである．記述には，オブジェクトおよびワークフローなどが使われることが多い．オブジェクトとは，世界に存在する「もの」をその動作と内部データによって抽象化したものであり，大規模ソフトウェアの記述においてその有効性が実証された概念である．一方，ワークフローは，ものの流れを中心に企業組織を表現するものとして多用されている．これらのモデルによる電子社会のモデル化に関して，モデルの検証，シミュレーション，モデル化方法論についての研究を行う．モデルの検証では，データや制御の可到達性や非デッドロック性などモデルの動的振る舞いを中心に研究を行う．また，モデルのシミュレーション方式やネットワークエージェントによる性能解析の研究を行う．一方，モデル化方法論に関しては，進化性やアカウンタビリティの高いモデルの構築法の研究を自治体業務や企業情報システムを対象にして行う．

電子社会の正当性検証

電子社会の正当性検証とは，その機能やサービスが，その仕様である法規などに照らして正しいか，あるいは，特定の性質を満たしているかを決定することである．これには，電子社会モデルＭのシミュレーションにより，それが電子社会の仕様Ｐに対して正しく動作していることを確認するか，あるいは，何らかの論理的な方法で，Ｍの振る舞いのもとでＰが正しいことを証明する必要がある．前者はいわゆるテストであり，また，後者は通常，形式検証と呼ばれる．テストには電子社会モデルの実行メカニズムであるシミュレータが必要になり，形式検証には定理証明システムやモデルチェッカーなどの推論システムが必要である．プログラムやソフトウェアに関しては形式検証の長い歴史があり，多くの検証理論や検証ツールが作られてきたが，残念ながら，通常のソフトウェアに対しては，検証コストが高いのが現状である．電子社会モデルに対しては，記述の抽象度が高いことにより，形式検証の可能性は高いと期待される一方，数理的に定義しにくい社会システムを扱うことの新たな困難さも予想される．具体的な企業情報システムや自治体業務を対象にして形式検証の可能性を追求し，必要な検証技術の開発を行う．

電子社会のアカウンタビリティ

大規模情報システムでは，その全貌の詳細を知ることは，たとえシステム設計者でも困難であるといわれているが，電子社会に関しては，その公共性や透明性の確保という観点から，システムがどのようなものになっているかを利用者や住民に説明できることが必要である．電子社会のアカウンタビリティとは，このような観点から，電子社会の機能や構造についての説明が可能なこと，あるいは，それらについての質問に答えることができることを指す．一般のソフトウェアについては，その機能や操作について機能説明（What）のみで十分であるが，電子社会については，機能についての根拠や理由について

の理由説明（Why）が必要となる．たとえば，税金額の算出根拠についての説明が求められた場合，これに答えられなければならない．システムの進化や維持管理を行う立場からは，さらに，機構説明（How）が必要になる．理由説明や機構説明に関しては，これまで十分な研究が行われていないが，透明性の高い電子社会の実現にはきわめて重要である．モデル自身の内部にこのような説明機構を持たせるか，あるいは，外部の説明機構を利用するかなどを含めて，説明機構の研究を行う．

電子社会の情報セキュリティ

電子社会の情報セキュリティは，その正当性と並んで，電子社会の安心性にとって最も基本的な要件である．現在，情報漏洩や漏洩したデータによる犯罪が頻繁に報道されているが，我々が安心して電子社会で生活できるためには，プライバシーの保護やデータの不正アクセス防止などの情報セキュリティ技術の確立は必須である．ユビキタス技術が広く普及し，情報が漏洩にさらされる機会が増えることが予想される今後は，暗号技術や安全なプロトコルなどのセキュリティコア技術はますます重要であり，先進暗号技術やプライバシー保護技術などの高度なコア技術の研究を行う．それとともに，セキュリティ管理の立場から，電子社会におけるデータアクセスのルールやポリシーの明確な定義のもとに，組織の中で漏洩や不正アクセスが起こらないことの証明や，情報保護に関する諸法規との整合性，データの漏洩が発覚した時点での追跡可能性などを，定理証明技術やモデル検査技術などを用いて形式検証を行う方法についての研究を行う．

電子社会の進化

我々の社会は日々刻々変化しており，電子社会は新しい要求や変化に対応して変化し，その仕様やモデルを修正し，進化できなければならない．電子社会が進化できないと電子社会は硬直化し，我々の社会は住みにくく，時代遅れのものになってしまう．これまで，情報システムの進化には，ソフトウェアの研究開発の中で一貫して大きな努力が払われ，多くの新しい概念や方法論が生まれてきた．しかしながら，進化を合理的に行うことは，システム要求の変更をあらかじめ予測することが困難でそれを見越した設計が難しいことなどから，現在においてもいまだ困難な問題の1つであり，非常に大きなコストが，ソフトウェアの保守管理というかたちで払われている．本研究では，法律の改正や新しい法律の制定というかたちで電子社会の仕様が変化することを前提として，電子社会の進化問題を研究する．仕様間の整合性解析や差分仕様の構成，そのモデルへの伝播方法論，法律の改正と連係した電子社会仕様・モデルの版管理メカニズム，アスペクトやフィーチャ概念による進化容易モデルの構成法，オントロジーを利用した進化方式の研究などを行う．

耐故障高信頼情報基盤

電子社会のモデルは，最終的にはネットワークやハードウェアから構成される計算機システムによって実現され，また，ヒューマンインタフェース機構が付与されて社会基盤情報システムが構成される．これら電子社会のためのインフラストラクチャが安定して動作することが，電子社会の安心性の基礎である．これには，ネットワークや計算機の高信頼化と故障発生時における耐故障技術が必要である．耐故障性とは，ネットワークやプロセッサなどの故障に対しても電子社会が一定の機能を維持し続けることである．分散システムの耐故障技術として，誤りノード検出，高信頼マルチキャスト通信や合意形成などのためのプロトコルがこれまで研究されてきたが，これらの技術をもとに電子社会の耐故障性の研究を行う．

ネットワークの高信頼性に関しては，これまで行ってきたインターネットシミュレータ研究の高度化と，それによるネットワークの動作解析や実験的検証，情報家電やユビキタス機器を含んだヘテロなネットワークの運用管理の研究を行う．高信頼ハードウェアやアーキテクチャに関しては，仕様からの完全自動合成によるプロセッサの設計，耐故障アーキテクチャ，アーキテクチャによるセキュリティサポートの研究を行う．さらに，組み込みシステムやユビキタス機器が電子社会システムの要素としてますます広く用いられることを考え，モデル検査や定理証明などの形式手法の適用による組み込みシステムの高信頼化の研究を行う．

研究教育体制

研究教育組織の基本母体は，北陸先端科学技術大学院大学情報科学研究科であり，情報科学センターと知識科学研究科の一部の教員が参加している．拠点リーダー（片山卓也）のもと，以下のような体制で拠点の形成を行っている．

研究体制

(1)電子社会の形式的記述体系グループ

リーダー：小野寛晰

役　　割：電子社会の形式的仕様記述に用いられる各種形式体系とその論理学的研究，推論システムの研究，形式仕様記述言語の研究

(2)電子社会の安心性要件の検証グループ
リーダー：東条　敏
役　　割：電子社会の仕様としての法律に関する推論・検証とそれに伴う自然言語処理の研究，セキュリティコア技術とセキュリティ検証の研究，耐故障性とそのための検証方式の研究
(3)電子社会の検証方式グループ
リーダー：平石邦彦
役　　割：安心性要件の定理証明システムやモデル検査ツールによる形式検証の研究，モデルの実行による検証方式やメカニズムの研究
(4)電子社会のモデル化と進化グループ
リーダー：落水浩一郎
役　　割：電子社会のモデル化方法論，特にアカウンタビリティの実現を容易とするモデル化の研究，進化を容易とするモデル化と進化方法論の研究
(5)安心電子社会基盤グループ
リーダー：日比野靖
役　　割：安心電子社会の実現に必要な高信頼計算機システム（ネットワーク，ハードウェア）および高度ヒューマンインタフェースの研究，ディペンダブルシステムのためのアルゴリズムの研究

教育体制

安心電子社会の構築を行うことのできる研究者や博士レベル高級技術者を育成するための教育システムの開発を行い，COE プログラム実施中に30名の博士学生を養成する予定である．具体的には，講義科目については，
(1) 現在情報科学研究科において実施されている講義課目を含めて，形式論理，検証，高信頼電子社会情報システム関連の15科目
を用意し，それと同時に，
(2) NTTデータ（株）「電子社会システム学」連携講座の実施する「電子社会システム論」
による講義体制を確立する．また，学生は，各研究グループにおいて電子社会システム研究開発の実務を担当することにより，研究開発の実務経験を積む．

連携体制

電子社会の研究は，大学の内部だけで基礎的，理論的な研究を行うだけでは不十分であり，現実の社会や組織を理解し，それをもとにした研究を行うことが必要である．このような観点から，現在，以下の3つの国内組織と連携をとり，連携組織からの客員教員や客員研究員を交えた研究教育活動を行っている．

(1) NTTデータ（株）
連携内容：企業情報システムの分析と検証，連携講座の実施
(2) インテック・ウェブ・アンド・ゲノム・インフォマティックス（株），富山県庁
連携内容：富山県行政業務のための法推論システムとオブジェクトモデリング
(3)北陸NES(株)
連携内容：形式手法によるプロトコル検証

これらの国内組織との連携のほかに，以下の海外組織との連携を行っているが，今後の研究の進展に伴って新たな組織との連携も考える．
(1) AT&T Labs-Research
連携内容：高信頼情報システム構築法
(2)スイス連邦工科大学
連携内容：分散システムの耐故障技術
(3)オーストラリア情報通信 COE
連携内容：形式的仕様記述のための論理と推論システム
(4)ミラノ工科大学
連携内容：情報システムのモデル化と進化方法論

拠点形成支援体制

学長留保人事定員からCOE特別教員の採用や，大学事務局研究協力課によるCOE業務支援を含め，北陸先端科学技術大学院大学からの支援体制が確立されている．さらに，安心電子社会研究センターが大学内に設置され，COE活動の支援を行うと同時に，COE教員，研究員の日常的支援業務を行っている．

最後に

21世紀COEプログラム拠点形成計画「検証進化可能電子社会―情報科学による安心な電子社会の実現―」について，その目指すもの，研究内容，研究教育体制などについて述べた．本格的な電子社会時代の入り口にいる現在，最新の情報科学の研究成果を用いて，我々が安心して住むことのできる電子社会を構築するための基本概念や技術の確立に向けたCOEプログラムを実施するチャンスを与えられたことを感謝するとともに，世界レベルの研究教育拠点の形成に向けて精一杯の努力をしたい．また，研究対象が電子社会という実世界のものであり，実社会との連携は不可欠である．この点に関して連携を快くお引き受けいただいた諸機関に感謝いたします．

（平成17年4月5日受付）