サブテーマ３　レジリエンスの計算モデル

2011 年 3 月 11 日の東日本大震災と、それに伴って発生した津波及び福島第一原発の事故は、いずれも想定外の事象であり、未曾有の大被害をわが国にもたらした。震災以降、外的な擾乱に対してレジリエント（resilient）なシステム設計が求められている。あるシステムがレジリエントであるとは、外的な擾乱に対して耐性があり（resistant）かつ、実際に擾乱が起きて機能が低下したとしても回復可能性がある（recoverable）ことをいう。レジリエンスとは、生態学、環境科学及び社会学など、様々な研究分野において広く知られているシステムレベルの性質に関する概念である。自然界、人工物及び社会システムを問わず、レジリエントなシステムの例は多数存在する。しかし、レジリエンスに関する統一的な基礎原理の研究はほとんどない。人工知能分野では、レジリエンスに類似した概念として、離散事象システムにおける安定性（stabilizability）や保全性（maintainability）に関する研究がある[参考文献 1]. また Bruneau は、失われたシステム機能を時間軸上で積分したものとして捉えることにより、レジリエンスを定量化する方法を示した[参考文献 2]。本サブグループは昨年度に引続き「レジリエンスの計算理論」に関する研究を行っている。

初年度の平成 24 年度には、システム・レジリエンスを議論するための制約モデリングに関する SR モデルを提案し、システムが満たすべき様々な評価尺度に対して多目的最適化による手法について研究し、さらにダイナミックシステムに関する推論・学習方式について検討した。平成 25 年度はこれらの研究を引き続き発展させている。本報告書では、これらの研究課題のうち、とくに多目的最適化に関する研究に焦点を当てる。この研究テーマに関しては、以下に示す 4 つのサブテーマに関してレジリエントなシステムに関する研究を行った。

A)　多目的制約最適化技術によるアプローチ
B)　多目的分散制約最適化アルゴリズムの開発
C)　動的環境における多目的分散制約最適化問題のモデル化とアルゴリズムの開発
D)　サイバーセキュリティ問題への応用

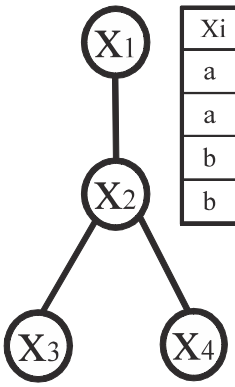
【参考文献】

1. C. Baral, T. Eiter, M. Bjreland, and M. Nakamura. Maintenance Goals of Agents in a Dynamic Environment: Formulation and Policy Construction. Artificial Intelligence, 172(12-13): 1429–1469, 2008.
2. M. Bruneau. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. In Earthquake Spectra, volume 19, 2003.

A．多目的制約最適化技術によるアプローチ

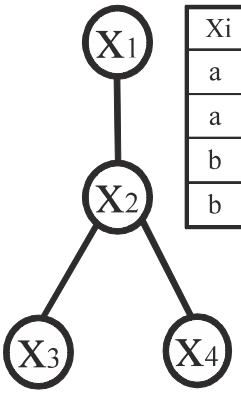
実世界に存在する様々な制約最適化問題では、複数の異なる評価基準を同時に考慮する場合が存在する。多目的制約最適化問題（Multi-Objective Constraint Optimization Problem, MO-COP）は、異なる評価基準をもつ複数の目的関数が存在する制約最適化問題（Constraint Optimization Problem, COP）である。COP とは、有限で離散的な領域から値をとる複数の変数に、ある目的関数を最適化するように値を割当てる問題である。図 1 に 4 個の変数からなる COP を表す。各変数は離散有限 集合 {a, b} の値を取る。各制約の利得は、図中の利得表で与えられているものとする。ただし、ここでは $i < j$ とする。たとえば、すべての変数の割当を a とするとき、得られる利得の総和は 3 である。この問題の解、すなわち、利得の総和を最大化するような割当（最適解）は $\{(x1, a), (x2, b), (x3, a), (x4, a)\}$ であり、このとき得られる利得の総和（最適値）は 8 である。MO-COP は、単一目的の COP を多目的へと拡張した問題である。この問題では、一般には、複数の異なる目的関数間にトレードオ

フの関係があるため、すべての目的関数を同時に最適化するような割当は存在しない。そのため、MO-COP ではパレート最適性の概念を用いて最適解を特徴づける。図２は２目的分散制約最適化問題を表す。各変数は離散有限集合 {a,b} の値を取る。各制約の利得ベクトルは図中の利得表で与えられているものとする。ただし、ここでは $i<j$ とする。r^1 及び r^2 は、それぞれ目的１及び２における利得を表す。この問題のパレート解は {{(x1,a), (x2,b), (x3,a), (x4,a)}, {(x1,b), (x2,a), (x3,b), (x4,b)}} であり、パレートフロントは {(8,7), (7,8)} である。本研究では、動的システムを定式化し、この問題のアルゴリズムを提案した。まず、動的システムを既存の多目的制約最適化技術を用いて定式化した。具体的には、動的システムを動的環境における多目的制約最適化問題（Dynamic Multi-Objective Constraint Optimization Problem, DMO- COP）を用いて定式化し、この問題における性質として、耐久性、回復可能性、レジリエンスを定義した。動的制約充足/最適化問題に関する既存研究はいくつか存在し、本研究でも、これらの既存研究と同様の方法、すなわち、DMO-COP を MO-COP の系列として定義した。この問題では、系列内の動的変化として、変数や目的関数の数、変数値、制約などが考えられる。本研究では、その第一歩として、制約にかかるコストの動的変化に着目した。次に動的システム、すなわち、DMO-COP におけるアルゴリズムを提案した。本アルゴリズムは COP の解法として広く用いられている分岐限定法に基づくアルゴリズムであり、あるシステムにおける、耐久性、回復可能性、レジリエンスなどの性質を満たす、すべてのトレードオフな解が求解可能である。また本アルゴリズムは、系列内の既に求解した問題の情報を用いて、次の問題を解いていくためリアクティブなアルゴリズムである。DMO-COP のアルゴリズムには、リアクティブなアプローチとプロアクティブなアプローチがある。系列内の各問題の情報は事前には分からない、すなわち、次の問題の情報は現在の問題を解いた後にのみ分かるようなモデルでは、各問題を一つ一つ独立に求解するリアクティブなアプローチが適用される。一方、系列内のすべての情報が事前に分かっている場合、一つの可能性として、系列全体における解、プランなどが求解可能となり、プロアクティブなアプローチが適用される。現在はプロアクティブなアプローチによるアルゴリズムを検討している。



Xi	Xj	r (Xi,Xj)
a	a	1
a	b	2
b	a	3
b	b	0

図1：制約最適化問題



Xi	Xj	(r^1, r^2)
a	a	(1,0)
a	b	(2,3)
b	a	(3,2)
b	b	(0,1)

図2：多目的制約最適化問題

B．多目的分散制約最適化アルゴリズムの開発

分散制約最適化問題（Distributed Constraint Optimization Problem, DCOP）とは、人工知能の基礎理論である制約最適化問題における変数及び、制約が複数のエージェント（自律的な主体：人や知的コンピュータ）に分散された問題である。各エージェントは自身の変数をもち、利得・コストの総和を最適化するように変数への割当を決定する。同じ環境内で動作する複数のエージェント行動間には、なんらかの制約が存在するのが通例である。分散制約最適化技術はエージェント間で整合の取れた行動を実現するための一般的な方法を与えることができ、エージェント間の協調を実現するためのインフラストラクチャとなる。マルチエージェントシステムで扱われている様々な応用問題、特にセンサ網やスケジューリング問題を含む分散資源割当問題が DCOP として形式化されている。多目的

分散制約最適化問題（Multi-Objective Distributed Constraint Optimization Problem, MO-DCOP）とは、MO-COP を分散環境に、DCOP を多目的へと拡張した問題である。MO-DCOP を解くとは、MO-COP のときと同様に、パレート解によって得られる利得ベクトルの集合であるパレートフロントを求めることである。分散資源割当問題など DCOP の多くの応用問題が、MO-DCOP の応用問題として拡張可能である。昨年度は DCOP における、効率的かつ、高速なアルゴリズムの開発を主な研究として行っていたが、本年度は MO-DCOP を解くアルゴリズムの開発を行った。MO-COP の既存研究では、すべてのパレート解を求解する完全なアルゴリズムがいくつか提案されている。これに対し、MO-DCOP では Bounded Multi-Objective Max-Sum（B-MOMS）と呼ばれる近似アルゴリズムが、最初かつ、唯一の MO-DCOP のアルゴリズムである。そこで、本研究ではまず、ハイブリッド型の完全なアルゴリズムを提案した。このアルゴリズムは、局所探索に基づく近似アルゴリズム（DCOP の近似アルゴリズムを拡張したもの）を用いて、パレートフロントの近似値を事前に求め、得られた情報を用いることにより、すべてのパレートフロントを求解する。本アルゴリズムは、すべてのパレートフロントを求解する最初の完全なアルゴリズムである。本研究成果により、井上と沖本は合同エージェントワークショップ＆シンポジウム（JAWS 2013）にて優秀論文賞を受賞した。

次に、MO-DCOP の近似アルゴリズム及び、パレートフロントのサブセットを求解するアルゴリズムを開発した。MO-DCOP では、一般に、パレート解の個数は変数の数に対して指数関数的に増加するため、大規模な実問題を考えた場合、すべてのパレート解を求解することは現実的ではない。近似アルゴリズムに関しては、上述したハイブリッド型のアルゴリズムの前処理として用いた、局所探索に基づくアルゴリズムを拡張したものを開発し、現在、既存の唯一の近似アルゴリズム（B-MOMS）との比較実験を行っている。また、沖本らが提案した DCOP の近似アルゴリズム（p-optimal algorithm）を多目的へと拡張したものも開発した。このアルゴリズムは最適化問題における、近似解の評価基準である p-最適性に基づく解法であり、得られる解の誤差の上界を事前に与える最初の近似アルゴリズムある。本アルゴリズムでは、パラメータ p を調整することにより、実行時間を犠牲にする代わりに、より高品質な解を得ることができる。事前に得られる誤差の上界は、グラフの誘導幅及び各利得関数の値の最大値に基づいて与えられるが、問題のインスタンスには依存しない。すなわち、すべてのインスタンスは、誘導幅及び各利得関数の値の最大値が同じである限り、同じ誤差の上界をもつ。誘導幅とは DCOP の解法の複雑度を決定する指標である。最初の近似アルゴリズムとの違いは本アルゴリズムは解の精度を理論的に保証できる点である。ただし、最初の近似アルゴリズムは解精度に関する保証はないが、高速かつ大規模な問題を扱うことが可能である。

パレートフロントのサブセットを求解するアルゴリズムに関しては、Aggregate Objective Function（AOF）を用いて、すべての評価基準における値の総和を最大化する解や、平等な解などを定義し、ある特定の解集合のみを効率的かつ、高速に求解するアルゴリズムの開発を行った。多目的最適化問題（Multi-Objective Optimization Problem, MOOP）のパレート解を求める古典的手法にスカラー化手法がある。線形化加重和法及び Lp-ノルム法は代表的なスカラー化手法である。線形化加重和法では、各目的関数に重みを与えることにより、単一の重み付き目的関数を作り、その最適解を求める。Lp-ノルム法は、ある基準点からの距離に基づいてパレート解を求める。この手法は、ある基準点、たとえば、ユートピア点を与えるだけで容易にパレート解が求解可能である。提案アルゴリズムは、パレート解を求める Lp-ノルム法、DCOP のアルゴリズムで広く用いられている擬似木、動的計画法を用いている。また本アルゴリズムの計算量は問題の誘導幅で抑えられる。さらに、本アルゴリズムでは、マンハッタンノルムを用いた場合は、パレート解を保証するが、ユークリッド/チェビシェフノルムを用いた場合は、パレート解を保証しないことを示した。MO-COP や MO-DCOP の研究でパレートフロントのサブセットに着目した研究はほとんどない。

C．動的環境における多目的分散制約最適化問題のモデル化とアルゴリズムの開発

MO-DCOP を動的環境へと拡張した動的多目的分散制約最適化問題（Dynamic Multi- Objective Distributed Constraint Optimization Problem, DMO-DCOP）のモデル化及び、この問題を解くアルゴリズムの開発を行った。DMO-DCOP は、いくつかの MO-DCOP からなる系列として定義される。系列内の各問題の動的変化としては、エージェント・変数の数、制約の数、目的関数の数、変数値等が考えられる。我々は、これらの各変化に特化したアルゴリズムの開発を行っている。例えば、目的関数の数のみが動的に変化する MO-COP 特有の動的変化に着目し、系列内の各問題は同じ制約グラフをもつものとし、次の問題で目的関数がいくつ追加/削除されるかは分からないモデルにおいて、各 MO-COP/DCOP を解くアルゴリズム（Dynamic Programming based on AOF-technique, DP-AOF）及び、DMO-COP/DCOP を解くアルゴリズム（Dynamic Programming based on Reused-technique, DPR）を提案した。DP-AOF は、m を MO-DCOP の目的関数の数として、線形化加重和法（AOF）を用いて（最大で）（m＋1）個のパレート解を求める。このアルゴリズムは、ある一つの目的関数の値のみを最大化するようなパレート解、すなわち、その他の目的関数の値は全く考慮しない極端な解と、すべての目的関数の値の平均値を最大化するようなパレート解を求解する。DPR は DP-AOF に基づくアルゴリズムであり、（最大で）2m −1 個のパレート解が求解可能である。このアルゴリズムは、既に求めた問題のパレート解の情報を用いて系列内の問題を順に解いていく。また実験では、本解法が、系列内で既に求解した情報を使うことなしに各問題を解いていくナイーブな手法と比べ、より高速に求解可能であることを示した。さらに、本アルゴリズムでは大規模な問題が求解可能であることを示した。DMO-DCOP のアプローチには、問題の系列が事前に与えられているものを対象とするプロアクティブなアプローチと、系列内の各問題の情報が事前には分からないもの、すなわち、系列内の次問題に関する情報は現在の問題を求解した後にのみ与えられるとするリアクティブなアプローチがある。前者では、系列内の各問題に関する情報を利用することにより、ある系列に対して一つの解（解の集合）を求解する方法があり、後者では、系列内の各問題の解の集合からなる解の系列を求解する必要がある。我々は、主にリアクティブなアプローチを研究してきたが、今後はプロアクティブなアプローチも検討していく。DMO-COP/DCOP 及び、パレートフロントのサブセットに着目した研究成果により、沖本は The 7th International Workshop on Multi-Disciplinary Trends in Artificial Intelligence (MIWAI 2013) にて、Best Presentation Award を受賞した。

D．サイバーセキュリティ問題への応用

応用問題として、セキュリティ・プライバシー・コストを評価基準にもつサイバーセキュリティ問題を多目的分散制約最適化を用いてモデル化し、トレードオフな解を求解するアルゴリズムを提案した。現代の情報社会において、「セキュリティ」と「プライバシー」のあり方は、最も重要な論点であると言える。インターネットの利便性は、情報システムのセキュリティ対策に関わる不備や、プライバシー侵害のリスクなどの要因によって、常に脅威に晒されている。インターネットそれ自体、そしてそれに関わる社会的・経済的諸活動の高度なセキュリティを実現するためには、限定された特定の主体や組織（典型的には政府当局や ISP 等）による、通信内容・通信履歴の解析が必要とされることがある。そして逆説的ではあるが、セキュリティのための施策そのものが、個人のプライバシーの侵害や、企業にとっての機密保持への脅威となる事態が生じ得る。同時にそのようなセキュリティ施策の実行は、関係企業や政府にとって一定の「(人的・金銭的) コスト」を強いることにもなる。本研究の目的は、サイバーセキュリティ政策に内在するこのようなセキュリティ・プライバシー・コストの三次元トレードオフへの解答を見出し、環境の変化に応じて迅速に更新・修正するための、多目的分散制約最適化によるモデル化と解法を提案し、検証を行うことにある。近年のセキュリティに関わる

法政策においても、このような多元的トレードオフの困難性に直面するものは枚挙に暇がない。例えば、2004 年から 2005 年にかけてのロンドンやマドリードのテロ事件を受け、EU（欧州連合）において 2006 年に採択された「データ保持指令（Data Retention Directive、2006/24/EC）」は、加盟国に対して、国内の ISP が全ての通信履歴（communications data）を 6 ヶ月から 24 ヶ月の期間保持するよう義務付ける国内法を制定するように求めている。保持対象とされる通信履歴の中には、電子メールや IP 電話を含む音声通話、テキストメッセージの送受信に関わる、IP アドレスや時刻等が含まれる。そして保持された通信履歴は、それぞれの国内法に規定される開示・提出手続きに基づき、テロリストの通信やサイバー攻撃、その他の深刻なサイバー犯罪の捜査・起訴のために用いられることが想定されている。より最近の例としては、2011 年に米国下院に提出されて以来大きな論争を呼んでいる、「サイバーインテリジェンス共有・保護法案（Cyber Intelligence Sharing and Protection Act）」を挙げることができるだろう。いまだ議会における議論の途上にあるものの、同法案は大規模なサイバー攻撃等の発生時において、インターネットに関わる幅広い企業が、顧客の通信履歴を含む広範なサイバー脅威情報（cyber threat information）を、プライバシー保護関連法の制約を受けず、政府や他の企業と共有することを可能とする内容を含んでいる。近年のサイバー攻撃の拡大を受け、多くのインターネット関連企業は同法案に賛同の意を示している。ここ数年間においては、国家間のいわゆる「サイバー戦争」の脅威が現実味を増す中で、サイバーセキュリティの問題は国防政策の文脈においても重要な位置付けを占めるに至っている。しかし、これらのサイバーセキュリティに向けた施策は、個人の自由やプライバシーを侵害するものとして、世界各国において市民団体等からの激しい批判に晒されている。セキュリティとプライバシー、そして施策の実行にかかるコストの適切なバランスをいかにして実現するかは、現代の情報社会の制度設計において、喫緊かつ最重要とも言うべき課題なのである。

サイバーセキュリティ問題では、セキュリティ、プライバシー、コストを同時に最適化する必要があるため、複数の評価基準を扱える多目的制約最適化によるモデル化が可能である。また本モデルは分散型であるため、集中型の多目的制約最適化と違い、すべての情報を管理するようなエージェントは存在しない。そのため、サイバー攻撃や一部の故障による被害に対して頑健なモデルであると言える。さらに、各エージェントは近傍（制約で関係するエージェント）とのみ情報交換を行うため、プライバシーの面でも適している。本研究では、

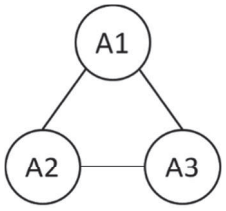


図3

リスク（セキュリティ）、監視（プライバシー）、コストを評価基準としてもつサイバーセキュリティ問題を MO-DCOP を用いて定式化する。この問題は、エージェントの集合を S、変数の集合を X、ドメインの集合を D、制約の集合を $C = \{C^1, C^2, C^3\}$、評価関数の集合を $O = \{O^1, O^2, O^3\}$ として、$< S, X, D, C, O >$ の組で定義される。エージェント i は自身の変数 x_i をもち、ドメインの集合 D_i、例えば、$D_i = \{scan, no\ scan\}$ に含まれる値を決定する。制約 (i,j) は x_i と x_j の間に制約があることを示す。例えば、2 エージェントの双方が{scan}を決定するときのみリスクが軽減する。各 C^1,C^2,C^3 はリスク、監視、コストに関する制約の集合を、各 O^1,O^2,O^3 はリスク、監視、コストに関する評価関数の集合をそれぞれ表す。各評価基準 $l\ (1 \leq l \leq 3)$ に関して、制約で関係する 2 変数間の、ある決定のコストは、コスト関数 $f^l: D \times D \rightarrow R$ により定義される。すなわち、制約で関係する 2 変数の各値の組み合わせに対して、リスク、監視、コストの値がコスト関数によって与えられる。すべての変数への決定を A とし、評価基準 l に関して、$R^l(A)=$ を評価基準 l に関するコスト関数の合計値として、サイバーセキュリティ問題の解はコストベクトル $R(A) = (R^1(A), R^2(A), R^3(A))$ で定義される。すべての評価関数を同時に最小化するような決定が存在すれば理想的であるが、一般には、評価関数間にトレードオフの関係があるため、そのような決定は存在しない。そのため、サイバーセキュリティ問題

では、パレート最適性の概念を用いて最適解を特徴づける。サイバーセキュリティ問題は、変数をノードに、制約をノード間のリンクに対応させることにより、グラフ（制約グラフ）を用いて表現可能である。

表1：A1, A2, A3 間のコスト表

A1	A2	(R, S)	A2	A3	(R, S)	A1	A3	(R, S)
No scan	No scan	(12,0)	Scan	Scan	(0,1)	No scan	Scan	(0,1)
No scan	Scan	(10,3)	Scan	No scan	(2,1)	No scan	No scan	(3,2)
Scan	No scan	(7,1)	No scan	Scan	(0,2)	Scan	Scan	(1,0)
Scan	Scan	(5,2)	No scan	No scan	(2,0)	Scan	No scan	(1,0)

例として、図3に3つのエージェント $\{A_1, A_2, A_3\}$ からなるサイバーセキュリティ問題の例を示す。各エージェントは協力して web を管理しているとし、web をスキャンする・スキャンしないかを決定する。表1にエージェント間の制約における値を示す。R（risk)はリスクを表し、S（surveillance）は監視をそれぞれ表すとする。例えば、エージェント A_1 と A_2 間の制約に関して、A_1 及び A_2 が {no scan} を選んだ場合、リスクレベルは 12 と非常に高いが、監視に費やすコストは 0 と低い。一方、双方が {scan} を選択した場合は、リスクレベルは改善され 5 となるが、監視にかかるコストは 2 に増える。この問題のパレート最適な決定は $\{(A_1, \text{scan}), (A_2, \text{scan}), (A_3, \text{scan})\}$, $\{(A_1, \text{scan}), (A_2, \text{no scan}), (A_3, \text{no scan})\}$ であり、トレードオフ解は (6, 3) と (10, 1) の2つである。サイバーセキュリティ問題の監視軽減解は、全員がスキャンすることで得られるトレードオフ解(6,3)であり、リスク対策重視解は、A_1 のみがスキャンすることで得られるトレードオフ解 (10,1) である。

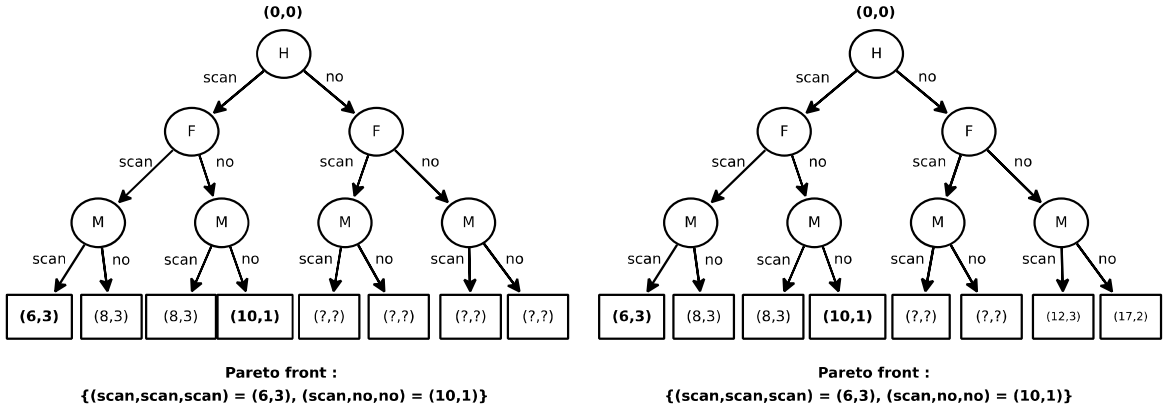


図4：アルゴリズム BnB の実行例

サイバーセキュリティ問題のトレードオフな解を求解するアルゴリズムとして Branch and Bound search algorithm (BnB) 及び、拡張版として Branch and Bound search algorithm with soft Arc Consistency (BnB+softAC) を提案した。BnB は分岐限定法と深さ優先探索を用いて、すべてのトレードオフな解を求解する。BnB+softAC は、BnB に最適化アルゴリズムの効率化として広く用いられている前処理技術 soft Arc Consistency を加えたものである。分岐限定法、深さ優先探索、soft Arc Consistency は、最適解の探索に用いられる代表的な手法である。図3のサイバーセキュリティ問題

の探索木を図４に示す。図中のノードH, F, Mは、エージェントA1, A2, A3がもつ変数を表し、各リンクはエージェントの決定を表す。ノードHの値がスキャンするならば左へ進み、スキャンしないならば右へ進む。ノードHを根ノードといい、四角のノードを葉ノードという。各葉ノードに、エージェントの決定によって得られるコストベクトルが記述されている。例えば、全エージェントがスキャンを選んだとき、根ノードから順に一番左側のリンクを辿ってコストベクトル（6,3）に着く。提案アルゴリズムBnBの実行例を、図４を用いて説明する。まず、探索木の左側の処理を行う(Step 1). BnBは、(i) {(H,scan),(F,scan),(M,scan)} を実行し、得られるコストベクトル（6,3）を解集合に加える。(ii) {(H, scan),(F, scan),(M, no)} を実行する。得られるコストベクトル（8,3）は、(6,3) により支配されているため、解集合には加えない。(iii) {(H, scan),(F, no),(M, scan)} を実行する。得られるコストベクトル（8,3）は、(6,3) により支配されているため、解集合には加えない。(iv) {(H, scan),(F, no),(M, no)} を実行する。得られるコストベクトル（10,1）は、(6,3) に支配されないかつ、(6,3) を支配しないため、解集合に加える。次に、探索木の右側の処理を行う(Step 2)。BnBは、(v) {(H, no),(F, scan)} を実行する。このときのコストベクトル（10,3）は、既に（6,3）や（10,1）に支配されているため、その先の探索は行わない（枝刈りという）。(vi){(H,no),(F,no)} を実行する。このときのコストベクトル（12,0）は、この時点では（6,3),(10,1）に支配されていないため探索を続ける。{(H, no),(F, no),(M, scan)} で得られるコストベクトル（12,3）は、(10,1）に支配されているため、解集合には加えない。(vii) 同様に、{(H,no),(F,no),(M,no)} で得られるコストベクトル（17,2）は、(10,1）に支配されているため、解集合には加えない。以上より、BnBによって得られるパレート最適な決定及び、トレードオフ解の集合は、{{(H, scan),(F, scan),(M, scan)}, {(H, scan),(F, no),(M, no)}} 及び {(6,3),(10,1)} である。さらに、提案アルゴリズムBnBの拡張として、soft Arc Consistencyと呼ばれる前処理を加えたBranch and Bound search algorithm with soft Arc Consistency（BnB+softAC）を提案した。Soft Arc Consistencyは、最適化アルゴリズムの効率化として広く用いられている前処理技術である。本研究では、この前処理技術をBnBに適用する。具体的には、BnB+softACでは、前処理として、soft arc consistencyを用いて問題の下界値を求め、得られる情報を利用してBnBを実行する。図５にsoft arc consistencyの実行例を示す。図中のH,F,Mはエージェント A1, A2, A3の変数を表し、ノード（左）及び、ノード（右）はno scan及びscanをそれぞれ表す。また、各リンクのラベルは、各エージェントの決定によって得られるコストベクトルを表す。例えば、Hのノード（左）とFのノード（左）間のリンクは、{(H, no scan), (F, no scan)} によって得られるコストベクトル（12,0）がラベル付けされている（表１を参照）。Step 1は、初期状態を表す。soft arc consistencyは、ノード（M）から根ノード（H）へと、各評価基準で最低限必要な値を伝播していく。Step 2では、Fがno scan及びscanを選んだときに、各評価基準において、最低限必要な（0,0）及び（0,1）がMから伝播される。

例えば、{(F, no scan),(M, no scan)} のコストベクトルは（2,0), {(F, no scan),(M, scan)} のコストベクトルは（0,2）であるため、Fがno scanを選んだ場合、評価基準１で少なくともかかるコストは0であり、評価基準2でも、少なくともコスト0がかかる。同様に、Fがscanを選んだときに、最低限必要な値は評価基準１では0、評価基準２では１となる。さらに、HとM間にはリンクが存在するので、HとM間でも同様の操作を行う。最後に、各リンクからは、伝播したコストベクトルをひく。例えば、（H, no scan）と（M, no scan）間のコストベクトルは（3,2)−(0,1)=(3,1）となる。Step 3では、FからHへ、最低限必要なコストを伝播する。最終的に、H が no scan を選んだ場合、最低限必要な値は（10, 2）となり、scan を選んだ場合は（6,2）必要となる(Step 4)。つまり、Hがno scanを決定したとき、その他のエージェントが何を選択しようとリスクは10以上、監視は2以上の値しか存在せず、Hがscanを決定したときは、リスクは6以上、監視は2以上の値となるBnB+softACは、softACで得られたコストベクトルを下界値として用いることにより、効率的にパレート解を探索

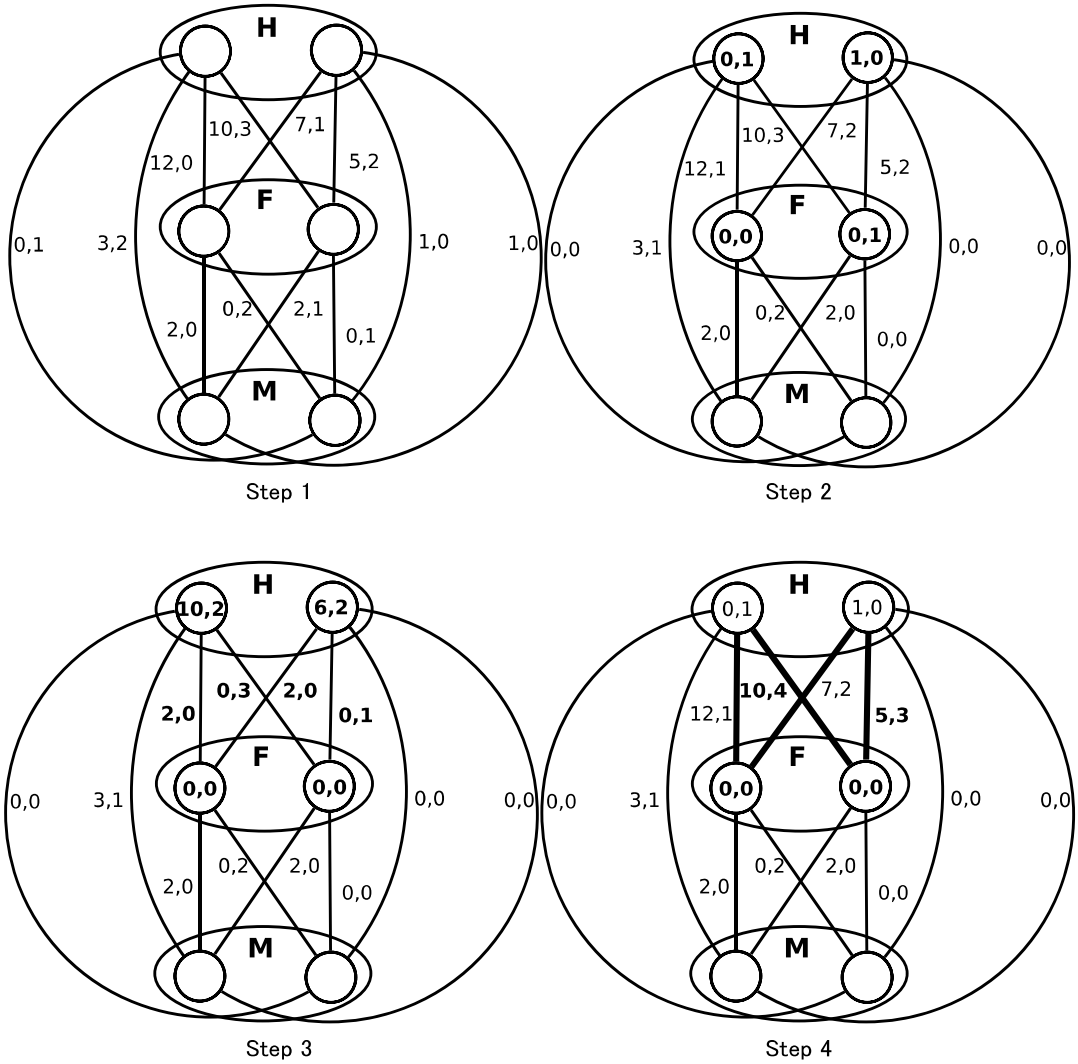


図5：soft arc consistency

する。図 2 の例の Step 2 において、H が no scan を選んだ場合、前処理 softAC より、少なくとも (10,2) のコストがかかることが分かっている。これは、既に Step 1 で求めたコストベクトル (9,1) に支配されている。したがって、BnB+softAC では、この時点で枝刈りが可能となり、BnB と比べ、探索空間の削減に成功している。 BnB+softAC では、BnB と比べ、より効率的にトレードオフ解が求解可能となることが期待できる。

実験では、例えば 10 の自治体・企業からなるソーシャルネットワークにおけるサイバーセキュリティ問題を想定したとき、提案アルゴリズムでは、どれぐらいの時間で、この問題が求解可能なのかを調べる。具体的には、各自治体・企業をエージェントし、リスク、監視、コストを評価基準としてもつサイバーセキュリティ問題における、提案アルゴリズム BnB 及び、前処理を加えた BnB+softAC の実行時間を調べる。実験では、評価 基準は 3 つ（リスク、監視、コスト）とし、各制約における評価基準の値は 0 から 100 の整数値を一様分布の乱数により選択した。各変数のドメインサイズは 3 (all scan, partial scan, no scan）とした。例えば、各エージェントは自身のメールを、すべてスキャンする/一部をスキャンする/全くしないを決定する。問題のインスタンスは、エージェント数（問題の規模）を変えながら制約密度 1.0 の完全グラフ（最も複雑なグラフ構造）を生成した。実験結果は 100 インスタンスの平均値を表す。提案アルゴリズム BnB 及び BnB+softAC は、C++を用いて実装し、各実験は 2.3GHz core、メモリ 4GB で行った。本実験では、提案アルゴリズムの実行時間を示す

ことを目的としており、実問題における評価基準の値やグラフ構造の違いについては、ここでは議論せず、今後の課題と考えている。

図 6 に規模が異なるサイバーセキュリティ問題における、提案アルゴリズム BnB および BnB+softAC の実行時間の平均値を示す。図 6 の X 軸はエージェント数（問題の規模）を表し、Y 軸はすべてのトレードオフ解を求めるのに必要とした実行時間をそれぞれ表す。10 個のエージェントからなるサイバーセキュリティ問題では、提案アルゴリズム BnB 及び BnB+softAC がすべてのトレードオフ解を求めるのに必要とした実行時間の平均値はそれぞれ 0.08 及び 0.06 秒であった。また 18 個のエージェントからなるサイバーセキュリティ問題では、BnB における実行時間の平均値は 528 秒、BnB+softAC では 330 秒であった。図 6 より、提案アルゴリズムの実行時間は、問題の規模が大きくなる（エージェント数が増える）につれ、増加することが分かった。このことは、サイバーセキュリティ問題では、最悪時におけるトレードオフ解の個数が問題の規模（エージェント数）に対して、指数関数的に増えるためである。実際、エージェント数が 10 のときのサイバーセキュリティ問題における、トレードオフ解の個数は 55 であったが、エージェント数が 18 のときは約 4 倍の 238 であった。さらに、BnB+softAC は、BnB と比べ、より高速に求解可能であることが分かった。また、両アルゴリズムの性能の差は、エージェント数が増えるにつれ大きくなった。また詳細な結果は割愛するが、10 個のエージェントからなるサイバーセキュリティ問題では、BnB+softAC におけるメッセージ数の平均値は、BnB におけるメッセージ数の平均値 44000 の約 38%少ない 30000 であった。また 18 個のエージェントからなるサイバーセキュリティ問題では、BnB+softAC のメッセージ数の平均値は約 49%減少した。すなわち、BnB+softAC を用いた場合、グラフ内の全エージェントが協力して、すべてのトレードオフ解を求めるのに必要なエージェント間のコミュニケーションは、BnB のときと比べ、約半分で充分であることが分かった。また 18 個のエージェントからなるサイバーセキュリティ問題では、BnB+softAC の実行時間の平均値は約 38%改善された。サイバーセキュリティ問題では、トレードオフな解を高速に求解することが重要である。例えば、ネットワークがサイバー攻撃を受けた際、平常時から緊急時へと対策（エージェントの決定）をシフトする必要があり、トレードオフな解をいかに早く提供できるかが重要な課題となる。提案アルゴリズムは、サイバーセキュリティ問題を高速に求解可能であるため、サイバーセキュリティ問題の有効なアルゴリズムになると考える。しかし、提案アルゴリズムの実行時間は、問題の規模が大きくなるにつれ増加することが分かった。そのため、今後は、すべてのトレードオフ解を求めるのではなく、多様な解をいくつか得られるようなアルゴリズムへと拡張する必要がある。その他にも、求解したトレードオフ解が解空間内にどのように分散/集中しているのか、また、そのときの実験結果に違いはあるのか、さらに、トレードオフ解が凹/凸性であるときの実験結果との関連性等の詳細な調査は今後の重要な課題である。この研究では、社会科学を専門とする TRIC メンバーの生貝と共同研究を行っており、文理融合の研究テーマとして現在も引続き行っている。本研究の貢献として、まずサイバ

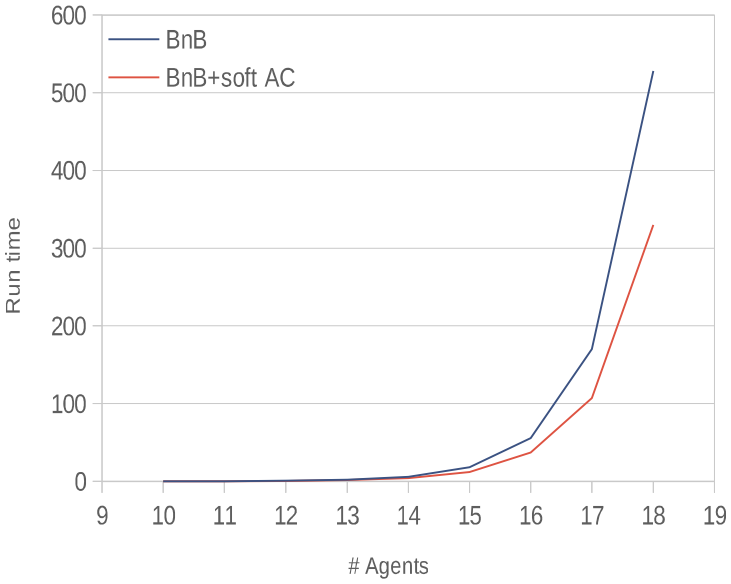


図6：BnB 及び BnB+softAC の実行時間．X 軸はエージェント数（問題の規模）を表し，Y 軸はすべてのトレードオフ解を求めるのに必要とした実行時間を表す．

ーセキュリティに関する社会科学領域に対しては、サイバーセキュリティをモデル化し、トレードオフな解を求めるアルゴリズムを提案した。サイバーセキュリティでは、多様な解が代表的に複数得られるようなアルゴリズムが望ましく、この研究では、その第一歩として、すべてのトレードオフな解を求めておくアルゴリズムを開発した。次に制約最適化の基礎研究に対しては、応用例として、サイバーセキュリティを提供した。我々は本研究が双方の研究を融合する第一歩となることを期待している。

サブテーマ４　社会システム・コミュニティにおけるレジリエンス

本サブグループの目的は、現代の複雑な社会システムをよりレジリエントなものとするための方法論を構築し、現実の政策や制度設計のあり方に資する知見を見出すことである。インターネットがもたらす急激な技術革新や、予見困難なリスクへの対応を行なうためには、従来のトップダウン型の法制度は必ずしも有効性を持たず、当事者の知識を適切に反映しつつも、その全体的な統御を政府が行なうという、ボトムアップとトップダウンの最適な組み合わせに基づく社会ルールの形成手法を確立する必要がある。本グループはプライバシーやセキュリティに関わる法制度の研究者によって構成されており、具体的な方法論として、(1)公私の共同規制という概念に基づく法制度の設計、および(2)計量的方法論に基づいた法制度に対する消費者受容の評価・計測手法の確立の 2 点を中心とした研究を進めてきた。以下ではそれぞれについての研究の概要と進捗状況を報告する。

(1)　公私の共同規制に基づく法制度の設計

インターネットの普及は、我々の社会システムに対して多くの変革を迫っているが、現代の法制度にとっての最大の影響は、インターネットが有する技術進化の速度と予見不可能性、断続的なイノベーションがもたらす法制度上の諸問題を、政府による伝統的な命令と統制に基づく直接的な法規制という政策手段が、適切に取り扱うことができないという問題である。政府による伝統的な法規制は、それを作り出す政府の側が、規制に必要な知識を包括的に有しているということを前提としてきた。しかし情報社会で生じる制度的課題を解決するための知識の多くは、その技術的進化の早さや専門性の高さを理由として、イノベーションを主導する当事者の側にしか有しえないことが多い。

そのためインターネット上においては、プライバシーや著作権、違法・有害情報への対策、あるいはサイバーセキュリティ等の課題を解決するにあたり、企業や産業界といった当事者の自律性に委ねる、ボトムアップ型の「自主規制（self-regulation）」による対応が重視されてきた。プライバシーの保護や違法・有害情報への対策といった問題においても、業界団体の策定する自主規制ルールに基づいた方法論が広く実践されている。このようなボトムアップの自主規制ルールは、制定や改正に数年を要する通常の法制度と比して、柔軟なルール形成・変更が可能であると共に、当事者の知識を反映し易いという利点を持つ。

しかし一方で、人権保護に関わる法制度上の問題全般を、純粋な民間の自主規制のみによって解決しようとすることには多くの限界が存在する。(1)そもそも必要とされる自主規制のルール自体が形成されない、(2)形成されたとしても利用者にとっての不公正性や新規参入企業にとっての競争阻害性を有する、(3)適切なルールであったとしても実効性を持たない、といった自主規制のリスクや不完全性をいかに解決するかが大きな課題となる。インターネットに関わる法制度の設計と運用は、その多くを自主規制によらざるを得ない一方で、自主規制に過度な期待をすることもできないという、望ましいルール形成主体の選択における二律背反性を有するのである。

本サブグループが中核に置く共同規制（co-regulation）という概念は、端的に言えば、柔軟性や当事者の知識の活用といった自主規制の利点を活かしつつも、その不完全性やリスクを政府が補完することにより、そのような二律背反の状況を解消し、環境変化の激しい状況に対応するよりレジリエン

トな法制度を実現するための政策手段であると位置付けることができる。情報社会で生じる幅広い問題に対して共同規制の方法論を適用しようとする英国情報通信庁は、2008 年に発行した「適切な規制の解を特定する：自主規制と共同規制を分析する上での原則」という文書において、下記のように共同規制を、自主規制と法的規制の中間的手法として位置付け、ボトムアップとトップダウンを組み合わせた共同規制の方法論によってこそ、情報社会の制度的課題は適切に解決されうるものとしている。

アプローチ	概　　要
規制なし	市場自身が求められる成果を出すことができている。市民と消費者は財やサービスの利点を完全に享受し、危険や害悪に晒されることがないようエンパワーされている。
自主規制	政府や規制機関による正式な監督なしに、産業界が集合的に市民・消費者問題およびその他の規制方針に対応する解決策を管理している。合意されたルールに関する事前の明確な法的補強措置は存在しない（ただし当該分野の事業者に対する一般的な義務規定は適用されうる）。
共同規制	自主規制と法的規制の両方により構成されるスキームであり、公的機関と産業界が、特定の問題に対する解決策を共同で管理している。責任分担の方法は多様だが、典型的には政府や規制機関は求められた目的を達成するために必要な補強力を保持している。
法的規制	関係者が従うべき目的とルールが法律や政府、規制者によって定義されており、公的機関によるエンフォースメントが担保されている。

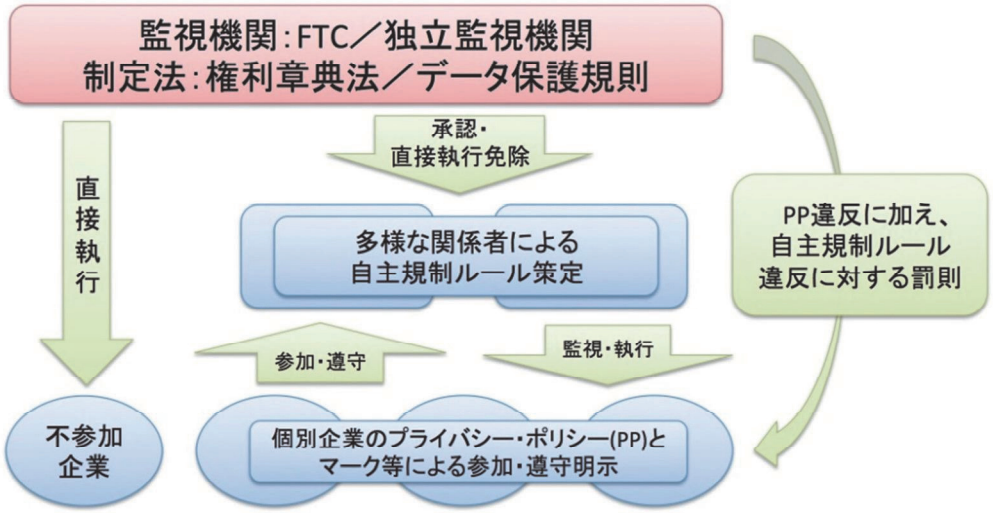
（英国情報通信庁による共同規制の定義）

本サブグループでは、この共同規制という政策手法を様々な法制度上の課題に適用する研究を行い、先行する EU や米国の共同規制への取組を調査し我が国の法制度と比較する作業を進め、特に本年度はプライバシー保護の問題に焦点を当てた研究を行なった。我が国では 2005 年に全面施行された個人情報保護関連 5 法を中心とする法整備が進められてきたが、個人情報を取り扱うにあたり求められる適切な「利用目的の明示」や「同意取得」のあり方、あるいは消費者行動履歴の統計データ等を利用するための「匿名化」などの概念は、その時々の技術的諸条件によっても大きく異なり得るため、一時点での技術的環境を前提としてその内容や手続きを法制度によって一義的に確定することは望ましくない。

このような問題を背景として、米国と EU ではいずれも自主規制の法的強化を軸とした多様な政策的措置が進められている。米国においては、我が国や EU のような包括的なプライバシー保護法制を持たないながらも、消費者保護法制を所管する連邦取引委員会（FTC）が民間の自主規制を促し、一定の原則の下に作られたプライバシー・ポリシーの違反等に対して FTC が罰則を適用するという自主規制の構造が構築されてきた。しかしこのような自主規制中心の措置は必ずしも実効性を有さない側面があり、2012 年にホワイトハウスが米国のプライバシー政策の大綱を示す「プライバシーの権利章典」を発表し、自主規制に対する公的関与を強化する方策を示している。そこではオンライン上の事業者全般に適用される包括的なプライバシー保護立法を行なうと同時に、多様な関係者を含むマルチステイクホルダー・プロセスによって形成された自主規制ルールに対して政府が審査・承認を行い、それを遵守した企業に対しては直接の法執行を免除するという、自主規制ルールに法的有効性と実効性を付与する新たな共同規制方法論の設計が中心に置かれている。

一方で EU においては、1995 年に採択された「データ保護指令」を中心とする直接的な法規制を重視した制度設計を進めてきており、同指令を全面的に改正する目的で 2012 年に公表された「一般データ保護規則」案においても、消費者に自己の情報の広範な消去権を与える「忘れられる権利」の導入をはじめとして、強固な法規制の措置が多く含まれている。しかし多様性を増すインターネット分野において統一的な基準を適用することの困難を背景として、そのような法規制の実際の運用にあたっては、分野ごとの自主規制ルールの策定を促し、独立のプライバシー保護監視機関がその適切性を

承認し法的な効力を与えるという、一定のボトムアップ性を導入するための措置を同時に拡大している。これら米国・EU で構築が進む共同規制構造は、下記のように図示することができる。



我が国においても現在、諸外国の制度改革の影響を受ける形で、個人情報保護法の改正や自主規制ルール策定の促進と実効性強化を視野に入れた検討が進められているものの、現行の法制度においては、自主規制ルールへの承認を公式に行なう制度や、自主規制ルール違反への罰則を適用するための有効な規定が存在しないため、上述のような法的確実性と実効性を伴う共同規制の実現にはいくつかの法改正を要する。本研究では欧米の状況との比較研究を基盤として、我が国の今後のプライバシー共同規制のあり方についての論点の検討を行なっている。

(2) 計量的方法論に基づいた法制度に対する消費者受容の評価・計測手法の構築

長い時間をかけて構築され、裁判所の判例の蓄積が存在する通常の法制度と異なり、情報技術に関わる法制度は、進展する技術的水準や国民意識に適合した形での迅速な変化を必要とする。こうした状況において、法制度の根幹となる民主的正統性、そして消費者・国民の受容を適切に反映する作業は、従来の法制度が依って立つ方法論のみによっては実現され得ない。このような認識の下、本サブグループでは、情報技術に関わる法制度や政策的措置に対する実際の消費者受容を計測し、立法政策に資する知見を得る方法論を構築するため、総務省情報通信政策研究所と共同でアンケート調査の設計と実査を行なった。

特に本年度の調査において重視したのは、情報社会のレジリエンスにとって急速に重要性を増す、サイバーセキュリティの問題である。増大するマルウェアやサイバー攻撃を検知・追跡し適切な対処を行なうためには、インターネットの通信内容や履歴に対する解析等が必要となるが、そうした措置は利用者のプライバシーや通信の秘密との矛盾を生じる。セキュリティとプライバシー保護のトレードオフ関係の下、通信解析等のセキュリティ施策を法制度がどこまで許容すべきかが論点となる。本研究では、次世代のサイバーセキュリティ政策を考慮するにあたり不可欠となるこのような要素間のトレードオフに焦点を当て、コンジョイント手法を用いたアンケート調査による消費者受容の調査を実施した。

コンジョイント手法とは、相互にトレードオフ関係にある複数の要素を消費者に提示することにより、その選好順位の回答を得るための調査手法である。たとえば通常のアンケートにより「プライバシーは重要か否か」という質問を行なったとしても、政策的に有為な回答を得ることはできないが、