N-016

サイバーセキュリティ問題の分散型多元制約最適化によるモデル化と解法

Modeling and Algorithm for Cyber Security Problem based on Decentralised Multi-Dimentional Constraint Optimization

沖本 天太 [1,2] Tenda Okimoto
生貝 直人 [1,2] Naoto Ikegai
リベイロ トニー [3] Tony Ribeiro
井上 克巳 [2,3] Katsumi Inoue
岡田 仁志 [2,3] Hitoshi Okada
丸山 宏 [3,4] Hiroshi Maruyama

新領域融合研究センター [1]　国立情報学研究所 [2]　総合研究大学院大学 [3] 統計数理研究所 [4]

1 序論

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．本稿の目的は，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，分散型多元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、CISPA)」を挙げることができるだろう．本稿の執筆時点においては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．

本稿では，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分散型多元制約最適化を用いてモデル化し，トレードオフな解を求めるアルゴリズムを提案する．サイバーセキュリティ問題では，セキュリティ／リスク，プライバシー／監視，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元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，集中型の多元制約最適化と違い，すべての情報を管理するようなエージェント [*1] 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．

本モデルにおいて，トレードオフな解を求めるアルゴリズ

[*1] エージェントとは自律的な主体 (たとえば，知的なプログラム，人間，自治体，企業，国家) を指す．

ム Branch and Bound search algorithm (BnB) および，拡張版として Branch and Bound search algorithm with soft Arc Consistency (BnB+softAC) を提案する．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．提案アルゴリズムでは，サイバーセキュリティ問題のすべてのトレードオフな解が求解可能である．そのため，例えば，平常時における解と，緊急時の解を迅速に変更することができる．実験では，提案アルゴリズムの評価を行う．

本稿の貢献として以下の 2 つを挙げる．

1. サイバーセキュリティに関する社会科学の研究に対して：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，本稿では，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．
2. 制約最適化の基礎研究に対して：制約最適化問題の応用例として，サイバーセキュリティを提供した．著者らは，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する．

本稿は，序論と結論を含めて全体を 6 章で構成している． 2 章ではサイバーセキュリティについて述べる． 3 章で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する． 4 章では提案アルゴリズムの評価実験を行い， 5 章では関連研究について述べる．

2 サイバーセキュリティのトレードオフ

サイバーセキュリティの問題は，近年世界各国において多大な関心を呼び起こしている．増大を続けるマルウェアやコンピュータウィルス，頻発する大規模なサイバー攻撃は，我々の情報社会にとっての深刻なリスクとなっている．特に，スマートグリッドや政府システムをはじめとする，ネットワーク化された重要インフラ (networked critical infrastructure) の普及は，ある意味において，我々の社会そのものの脆弱性を増大させている側面を有する [3]．もし，そのような重要インフラが大規模なサイバー攻撃を受け，機能を停止した場合，我々の日常生活や経済的活動は甚大な被害を被ることになる．2007 年に生じた，エストニアに対するサイバー攻撃と政府・民間システムの大規模な停止は，そのようなリスクを考える上での象徴的な事例であると言うことができるだろう [7]．我々の社会と情報システムは，現代のサイバーリスクに対して，よりレジリエントであらなければならない。

匿名性が高いインターネットは，テロリストや麻薬の売買といった重大犯罪を行う側にとっても，きわめて利便性の高いコミュニケーション・ツールとして用いられる．警察や法執行機関は，それらのコミュニケーションの履歴 (ログ) を，捜査や起訴，そして，それら犯罪の抑止を目的として収集・利用する必要がある．このような政府の活動は，情報社会をより安全で，レジリエントなものとするための重要な要素として位置付けられる．多様な違法行為の検知・追跡において，政府機関や ISP による通信の解析や傍受は不可欠な手段となる．特に，近年の DPI (Deep Packet Inspection) 技術の進化は，そのような活動を飛躍的に効果的なものとしている [6]．さらに，過去の犯罪関連の通信履歴を入手するにあたり，前述したような ISP による通信履歴の長期保持はきわめて重要な役割を果たす．

これらの情報を合法的に収集・利用するにあたり，各種のプライバシー保護法制は，関連するサイバーセキュリティの施策に適合するよう調整が行われる必要がある．第 1 章で言及した EU のデータ保持指令，米国の CISPA 等は，このような理由によって提案が行われてきたものである．しかし，何よりも重要なことは，たとえその目的が社会の安全のためであったとしても，通信の傍受やデータの保持は，セキュリティとプライバシーとの間のきわめて解き難いトレードオフの下に位置しているということである．近年のサイバーセキュリティ法案は，市民社会や人権擁護団体からの激しい批判を呼び起こしている [10]．プライバシーや通信の秘密の保護は，多くの先進国において憲法によって保障される，民主主義社会において最も重要な概念である [*2]．実際に，いくつかの EU 諸国においては，データ保持指令の国内法化が，国内裁判所によって違憲の判決を受ける事態も生じている [4]．サイバーセキュリティの問題におけるもう一つの要素がコストである．通信履歴の長期間の保持や，大規模な DPI の運用といった活動は，ISP や関係企業に対して多大なコストを課す [2]．

要約すれば，サイバーセキュリティの問題は，セキュリティ，プライバシー，コストという，三次元のトレードオフの下に位置しているのである．我々の社会は，この困難なトレードオフにおいて，何かしらの解答を得なければならない．しかしながら，その解答に関わる社会的コンセンサスは，技術の進化，社会的・経済的状況，あるいはサイバーリスクの脅威の度合いなどの要素によって常に変動を続けることになる．以下では，このような複雑なトレードオフを解決するための，システマティックな手段の提案についての説明を行う．

3 モデルとアルゴリズム

本章では，複数の評価基準をもつサイバーセキュリティ問題を分散型多元制約最適化を用いて定式化する．さらに，この問題のすべてのトレードオフ解を求めるアルゴリズム Branch and Bound search algorithm (BnB) および，BnB の拡張版として，アルゴリズムの効率化として広く用いられている前

[*2] プライバシー保護をはじめとする，インターネットの安全性に関わる法政策の日米欧比較につき，文献 [18] を参照．我が国において，通信の秘密の概念の現代的意義を論じた文献は未だ少ないが，インターネットに関わる通信内容・履歴の区別，セキュリティや犯罪への対応に際しての通信の秘密の制約原理の検討を含む，憲法学における近年の代表的論考として，文献 [17] を参照．

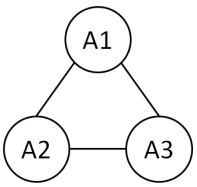


図 1　サイバーセキュリティ問題の例.

表 1　A_1, A_2, A_3 間のコスト表.

A_1	A_2	(リスク, 監視)
no scan	no scan	(12,0)
no scan	scan	(10,3)
scan	no scan	(7,1)
scan	scan	(5,2)
A_2	A_3	(リスク, 監視)
scan	scan	(0,1)
scan	no scan	(2,1)
no scan	scan	(0,2)
no scan	no scan	(2,0)
A_1	A_3	(リスク, 監視)
no scan	scan	(0,1)
no scan	no scan	(3,2)
scan	scan	(1,0)
scan	no scan	(1,0)

処理技術 soft Arc Consistency を加えた Branch and Bound search algorithm with soft Arc Consistency (BnB+softAC) を提案する．両アルゴリズムは最適解を探索する代表的な手法である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解を求める完全なアルゴリズムである．

3.1　サイバーセキュリティ問題

本稿では，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分散型多元制約最適化を用いて定式化する．この問題はエージェントの集合を $S = \{1, ..., n\}$，変数の集合を $X = \{x_1, ..., x_n\}$，ドメインの集合を $D = \{D_1, ..., D_n\}$，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．エージェントとは自律的な主体 (たとえば，知的なプログラムおよび人間) を指す．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，x_i および x_j 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 $\{(x_i, d_i), (x_j, d_j)\}$ のコストは，コスト関数 $f^l_{i,j} : D_i \times D_j \to \mathbb{R}$ 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，

$$R^l(A) = \sum_{(i,j) \in C^l, \{(x_i,d_i),(x_j,d_j)\} \subseteq A} f^l_{i,j}(d_i, d_j)$$

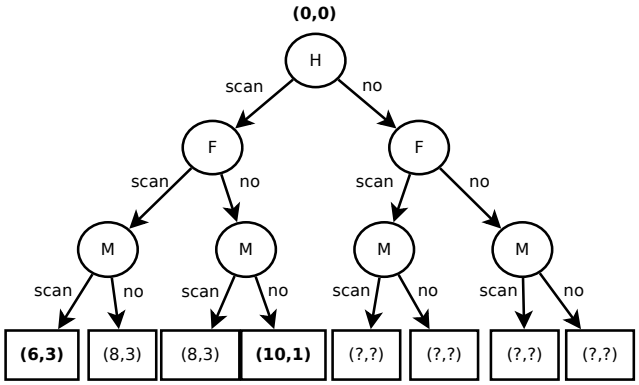
を評価基準 l に関するコスト関数の合計値として，サイバーセキュリティ問題の解はコストベクトル $R(A) = (R^1(A), R^2(A), R^3(A))$ で定義される．すべての評価関数を同時に最小化するような決定が存在すれば理想的であるが，一般には，評価関数間にトレードオフの関係があるため，そのような決定は存在しない．そのため，サイバーセキュリティ問題では，パレート最適性の概念を用いて最適解を特徴づける．本論文では，エージェントと変数が一対一に対応することから，記述の簡略化のために，必要に応じて両者の区別をせずに用いる．各評価基準に関して，すべてのコストは非負とする．サイバーセキュリ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，グラフを用いて表現可能である．

定義 1 (支配)**.** サイバーセキュリティ問題に関して，$R(A)$ および $R(A')$ を全エージェントの決定 A および A' によって得られるコストベクトルとし，(i) すべての評価基準 l $(1 \leq l \leq 3)$ に関して $R^l(A) \leq R^l(A')$ かつ，(ii) 少なくとも 1 つの l' $(1 \leq l' \leq 3)$ に関して $R^{l'}(A) < R^{l'}(A')$ が成立するとき，$R(A)$ は $R(A')$ を支配するといい $R(A) \prec R(A')$ と記述する．

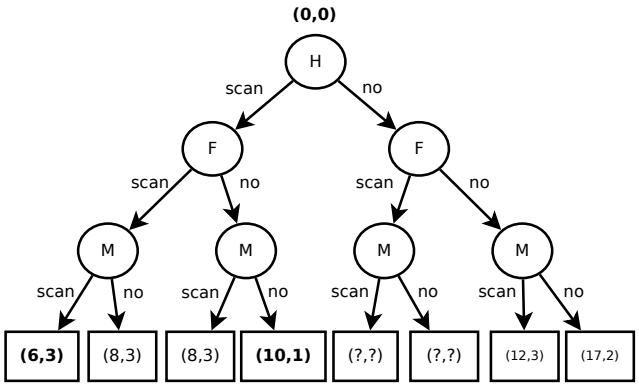
定義 2 (パレート最適)**.** サイバーセキュリティ問題に関して，ある決定 A がパレート最適であるとは，$R(A') \prec R(A)$ が成立するような，その他の決定 A' が存在しないことを意味する．

定義 3 (トレードオフ解)**.** サイバーセキュリティ問題に関して，パレート最適な決定によって得られるコストベクトルをトレードオフ解と呼ぶ．サイバーセキュリティ問題を解くとは，トレードオフ解の集合を求めることである．また，評価基準 $1, 2, 3$ の値が小さくなるように決定されたトレードオフ解をそれぞれリスク対策重視解，監視軽減解，コスト重視解と呼ぶ．

例 1 (サイバーセキュリティ問題)**.** 図 1 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．例えば，エージェント A_1 と A_2 間の制約に関して，A_1 および A_2 が $\{no\ scan\}$ を選んだ場合，リスクレベルは 12 と高いが，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 $\{\{(A_1, scan), (A_2, scan), (A_3, scan)\}, \{(A_1, scan), (A_2, no\ scan), (A_3, no\ scan)\}\}$ 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．



(a) Step 1



(b) Step 2

図 2　BnB の実行例．Step 1 は探索木の左側における BnB の処理，Step 2 は右側における BnB の処理を示している．

以降では，なぜサイバーセキュリティ問題のモデル化に分散型多元制約最適化を用いたかについて述べる．サイバーセキュリティ問題では，リスク，監視，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元制約最適化によるモデル化を行った．また本モデルでは，変数および制約が複数のエージェントに分散されている．このようなモデルでは，集中型の多元制約最適化と違い，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．

3.2 アルゴリズム

サイバーセキュリティ問題を解くアルゴリズム Branch and Bound search algorithm (BnB) を提案する．提案アルゴリズムは，探索木内を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解を求める．図 1 のサイバーセキュリティ問題の探索木を図 2 に示す．図中のノード H, F, M は，エージェント A_1, A_2, A_3 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．各葉ノードには，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 2 を用いて説明する．まず探索木の左側の処理を行う (Step 1)．提案アルゴリズムは，(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)．提案アルゴリズムは，(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，提案アルゴリズム BnB によって得られるパレート最適な決定およびトレードオフ解の集合は，$\{\{(H, scan),(F, scan),(M, scan)\}, \{(H, scan),(F, no),(M, no)\}\}$ および $\{(6,3),(10,1)\}$ 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) を提案する．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．本稿では，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 3 に soft arc consistency の実行例を示す．図中の H,F,M はエージェント A_1,A_2,A_3 の変数を表し，ノード (左) およびノード (右) は *no scan* および *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* および *scan* を選んだと

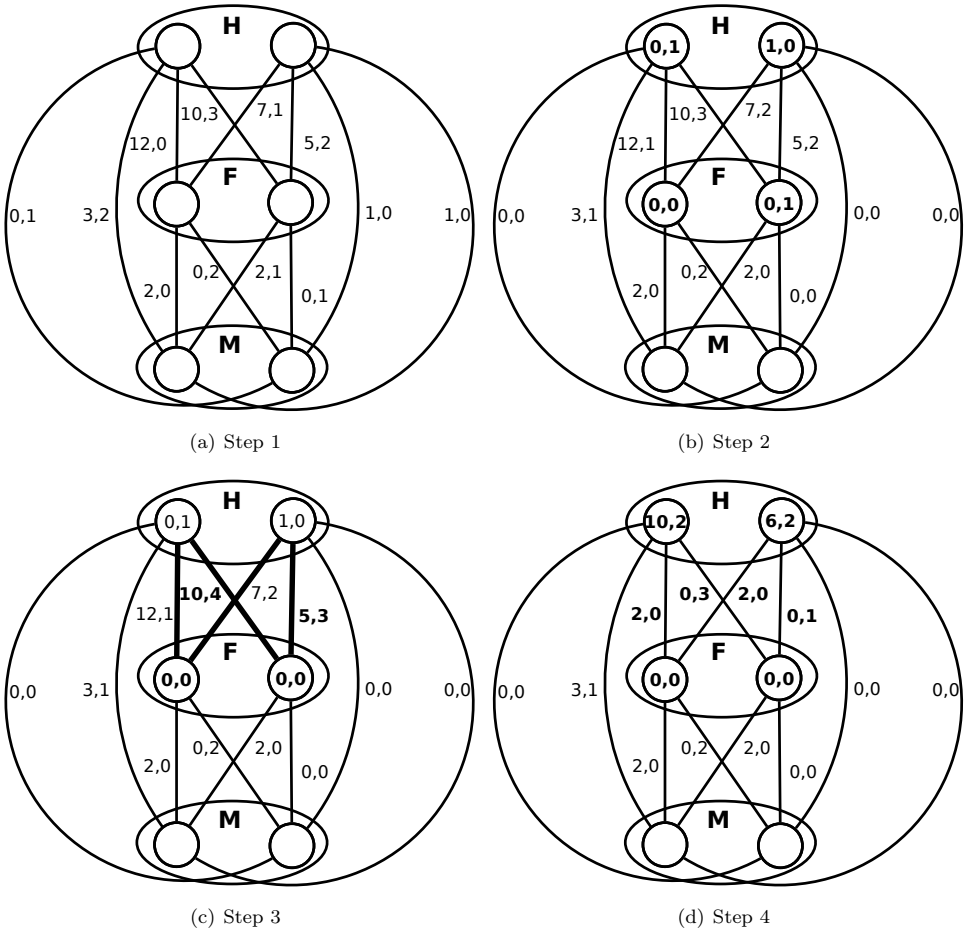


図 3　Soft Arc Consistency の実行例.

きに，各評価基準において，最低限必要な $(0,0)$ および $(0,1)$ 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．よって，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．

4　評価実験

本章では，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 および，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

表 2　提案アルゴリズム BnB および BnB+softAC の詳細な実験結果．*Agents* はエージェント数，*solutions* はトレードオフ解の個数，*Messages* はエージェント間で送受信されるメッセージ数，*Run Time* は実行時間をそれぞれ表す．

# Agents	# solutions	# Messages (BnB)	Run Time (BnB)	# Messages (BnB+softAC)	Run Time (BnB+softAC)
10	55	44 000	0,08	30 000 (38%)	0,06 (26%)
11	63	120 000	0,23	73 000 (35%)	0,17 (20%)
12	85	340 000	0,68	200 000 (40%)	0,50 (26%)
13	101	900 000	1,98	520 000 (42%)	1,41 (29%)
14	120	2 500 000	6,05	1 400 000 (43%)	4,19 (31%)
15	143	7 100 000	18	3 900 000 (45%)	12 (33%)
16	172	19 900 000	56	10 800 000 (46%)	37 (34%)
17	196	55 400 000	170	28 600 400 (48%)	107 (37%)
18	238	155 000 000	528	80 000 000 (49%)	330 (38%)

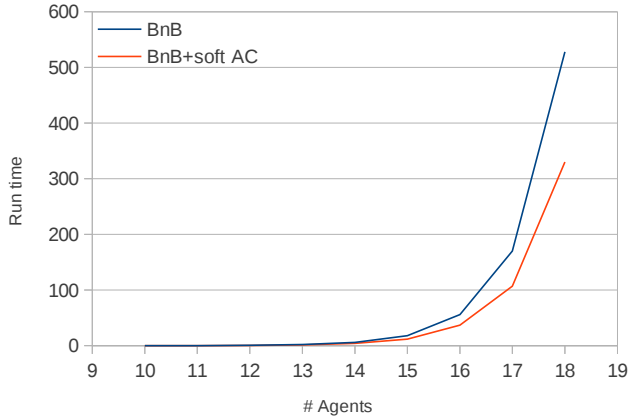


図 4　完全グラフにおける異なるエージェント数での提案アルゴリズム BnB および BnB+softAC の実行時間．X 軸はエージェント数 (問題の規模) を表し，Y 軸はすべてのトレードオフ解を求めるのに必要とした実行時間をそれぞれ表す．

た [*3]．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) [*4] 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 および 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．本稿の実験では，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，今後の課題とする．

図 4 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．また表 2 には詳細な実験結果を示す．図 4 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．また，表 2 の *Agents* はエージェント数，*solutions* はトレードオフ解の個数，*Messages* はエージェント間で送受信されるメッセージ数，*Run Time* は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 および 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 および 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 4 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．表 2 より，エージェント数が増えるにつれ，トレードオフ解の個数が著しく増加していることが分かる．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．表 2 より，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，

[*3] 今後は各評価基準の実データの調査も行う予定である．

[*4] 完全グラフ内の各エージェントは自分以外のすべてのエージェントとリンクをもつ (制約で関係している)．制約密度とは，グラフがもつリンク数を m，もちうるリンクの総数を n とし，$\frac{m}{n}$ により与えられる．

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．

5 関連研究

マルチエージェントシステムとは，エージェントの相互作用に関する研究分野であり，計算機科学，人工知能，経済学，社会学等の分野も関連する学際的な研究分野である．エージェントとは自律的な主体 (例えば，知的なプログラムおよび人間) を指す．近年，インターネットやコンピュータシステムの高度化に従い，超並列，分散環境における計算や知的処理のモデル／理論が求められている．このような場では，従来の単一体としてのプログラムモジュール群による制御は事実上不可能であり，多くの比較的独立したプログラム単位が相互作用する，マルチエージェントシステムによる設計／モデル化が必要となる．

分散型の制約最適化問題 [9] は，マルチエージェントシステムにおける様々な応用問題を表現できる一般的な枠組みである．この問題は，制約最適化問題 [14] における変数および制約が，複数のエージェント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，利得の総和を最適化するように変数への割当を決定する．分散型の制約最適化問題の応用例に分散センサ網 [9] や会議スケジューリング [13] を含む分散資源割当問題がある．例えば，分散センサ網では，地理的に分散された複数のセンサが環境をモニタしている．センサは指向性があり，モニタする方向を適切に選択する必要がある．環境内に存在する移動体の正確な位置，速度等を得るためには，複数のセンサが同時に移動体の存在する方向をモニタする必要がある．各センサのモニタする方向を変数の値と考えれば，この問題は制約最適化問題として表現できるが，地理的に分散された多数のセンサを集中制御することは現実的ではなく，分散型の制約最適化アルゴリズム [9, 12, 13] の適用が検討されている．

分散型多元制約最適化問題 (多目的分散制約最適化問題 [5, 16]) は，分散型の制約最適化問題／多元制約最適化問題 [8, 11] を多元／分散型へと拡張した問題である．この問題では，一般には，複数の異なる評価関数間にトレードオフの関係が存在するため，すべての評価関数を同時に最適化するような理想的な割当は存在しない．そこで，この問題では，パレート最適性の概念を用いて最適解が特徴づけられる．ある割当がパレート解であるとは，すべての評価基準において，その割当によって得られる利得ベクトルを改善するような他の割当が存在しないことを意味する．分散型多元制約最適化問題を解くとはパレートフロントを求めることである．パレートフロントとは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．この問題は，エージェントをノードに，制約をノード間のエッジに対応させることにより，グラフを用いて表現できる．分散型の制約最適化問題の多くの応用問題が，複数の評価基準をもつことにより分散型多元制約最適化問題として拡張可能である．

本論文で提案したアルゴリズムは，分散型多元制約最適化問題のすべてのパレート解が得られることを保証する完全なアルゴリズムである．分散型多元制約最適化問題の代表的なアルゴリズムに Bounded Multi-Objective Max-Sum algorithm (B-MOMS) [5] がある．このアルゴリズムと本アルゴリズムの違いとして，このアルゴリズムは近似アルゴリズムであるのに対し，本アルゴリズムは完全なアルゴリズムである．また，本アルゴリズムと類似した完全なアルゴリズムに Multi-objective AND/OR Branch-and-Bound search algorithm (MO-AOBB) [8] がある．このアルゴリズムは多元制約最適化アルゴリズムであるが，本アルゴリズムは分散型多元制約最適化アルゴリズムである．さらに，本アルゴリズムと遺伝的アルゴリズム [1] の違いとしては，本アルゴリズムではパレート解が得られることを保証している点が挙げられる．

6 結論

サイバーセキュリティの問題は，近年世界各国において多大な関心を呼び起こしている．増大を続けるマルウェアやコンピュータウィルス，頻発する大規模なサイバー攻撃は，我々の情報社会にとっての深刻なリスクをもたらしている．本稿では，サイバーセキュリティ問題を分散型多元制約最適化問題を用いて定式化した．さらに，分散型多元制約最適化問題のアルゴリズム Branch and Bound search algorithm (BnB) および，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答を求解する．BnB+softAC は，BnB に前処理として広く用いられている，soft Arc Consistency を加えたものである．実験では，異なるエージェント数のサイバーセキュリティ問題 (評価基準としてリスク, 監視，コストを考慮した最小化問題) における，BnB および BnB+softAC の実行時間を調べ，これらのアルゴリズムが高速に求解可能であることを示した．また，BnB の拡張版である BnB+softAC では性能向上が見られた．

今後の課題として以下を挙げる．第一に，より大規模な問題を解決し得る，高速なアルゴリズムを開発することである．トレードオフな解答の数は，問題の規模 (エージェント数) に対して，指数関数的に増加する．そのため，1 万や 10 万のエージェントからなる実問題を視野に入れた場合，すべてのトレードオ

フな解答を求めることは現実的ではない．したがって，すべてのトレードオフな解答を求める代わりに，一部の解答，例えば，すべての極小点を求めるアルゴリズムや，ユーザの選好を考慮した対話型アルゴリズムの開発が望ましいと考えられる．

第二に，実データを用いた実験の遂行である．本稿では，仮定の変数を用いることにより，アルゴリズムの設計と実装可能性を検証することに焦点を当てたが，プライバシーやセキュリティ，コストといった多元的なトレードオフ関係に対する消費者の選好は，コンジョイント手法等を用いた社会調査による集計と分析が可能である [15]．特に本稿で提案したようなシステマティックなトレードオフ問題の解決手法は，社会的コンセンサスを取り巻く社会的・経済的状況が急変する事態において，新たなコンセンサスを機動的に，動態的に得る必要が生じた際に一層の有効性を発揮するものと考えられる．平時におけるトレードオフな解答と，サイバー攻撃等緊急時におけるトレードオフな解答の双方を想定した社会調査を設計・実行することにより，本提案の実際に運用を視野に入れた，アルゴリズムの改良を行うための示唆を得る余地は大きいものと考えられる．

最後に，本稿は，数理アルゴリズムを専門とする数理科学者と，情報社会の法政策を専門とする社会科学者の共同研究による成果である．社会的合意形成や法政策に関わる語彙や概念を，精密な数理的表現と論理関係に化体することには多くの困難が伴うが，そのような学際的作業の蓄積こそが，離散的な情報と，有機的な社会の結合体としての情報社会に対する，より正確な理解と，セキュリティの実現に資することを期待したい．

謝辞．本研究を進めるにあたり，「システムズ・レジリエンス」プロジェクトの助成を受けました．ここに深く感謝致します．

参考文献

[1] K. Bringmann, T. Friedrich, F. Neumann, and M. Wagner. Approximation-guided evolutionary multi-objective optimization. In *Proceedings of the 22nd International Joint Conference on Artificial Intelligence*, pages 1198–1203, 2011.

[2] E. Commission. Evaluation report on the data retention directive. *COM(2011) 225 final*, 2011.

[3] S. M. Condron. Getting it right: Protecting american critical infrastructure in cyberspace. *Harvard Journal of Law Technology*, 20(2):403–422, 2007.

[4] K. de Vries. Proportionality overrides unlimited surveillance the german constitutional court judgment on data retention. *CEPS Papers in Liberty and Security in Europe*, 2010.

[5] F. M. D. Fave, R. Stranders, A. Rogers, and N. R. Jennings. Bounded decentralised coordination over multiple objectives. In *Proceedings of the 10th International Conference on Autonomous Agents and Multiagent Systems*, pages 371–378, 2011.

[6] C. Fuchs. Implications of deep packet inspection (dpi) internet surveillance for society. *The Privacy Security Research Paper Series*, (1), 2012.

[7] S. Herzog. Revisiting the estonian cyberattacks: Digital threats and multinational responses. *Journal of Strategic Security*, 4(2):49–60, 2011.

[8] R. Marinescu. Exploiting problem decomposition in multi-objective constraint optimization. In *Proceedings of the 15th International Conference on Principles and Practice of Constraint Programming*, pages 592–607, 2009.

[9] P. Modi, W.-M. Shen, M. Tambe, and M. Yokoo. ADOPT: asynchronous distributed constraint optimization with quality guarantees. *Artificial Intelligence*, 161(1-2):149–180, 2005.

[10] G. T. Nojeim. Cybersecurity and freedom on the internet. *Journal of National Security Law Policy*, 4(1):119–137, 2010.

[11] T. Okimoto, Y. Joe, A. Iwasaki, T. Matsui, K. Hirayama, and M. Yokoo. Interactive algorithm for multi-objective constraint optimization. In *Proceedings of the 17th International Conference on Principles and Practice of Constraint Programming*, pages 561–576, 2012.

[12] T. Okimoto, Y. Joe, A. Iwasaki, M. Yokoo, and B. Faltings. Pseudo-tree-based incomplete algorithm for distributed constraint optimization with quality bounds. In *Proceedings of the 17th International Conference on Princicles and Practice of Constraint Programming*, pages 660–674, 2011.

[13] A. Petcu and B. Faltings. A scalable method for multiagent constraint optimization. In *Proceedings of the 19th International Joint Conference on Artificial Intelligence*, pages 266–271, 2005.

[14] T. Schiex, H. Fargier, and G. Verfaillie. Valued constraint satisfaction problems: Hard and easy problems. In *Proceedings of the 14th International Joint Conference on Artificial Intelligence*, pages 631–639, 1995.

[15] 岡田 仁志, 高橋 郁夫. コンジョイント方式によるプライバシー分析 - 携帯電話電子マネーの位置情報の認知の実証的検証を例に - . **総務省情報通信政策レビュー**, *(4):1–16, 2012.*

[16] **沖本 天太**, **ジョ ヨンジュン**, **上田 俊**, **岩崎 敦**, **櫻井 祐子**, **横尾 真**, **井上 克巳**. **多目的分散制約最適化問題における厳密/非厳密解法の提案**. *In* 合同エージェントワークショップ&シンポジウム, *2012.*

[17] **宍戸 常寿**. **通信の秘密について**. 企業と法創造, *(35):14–15, 2013.*

[18] **生貝 直人**. **情報社会と共同規制: インターネット政策の国際比較制度研究**. 勁草書房, *2011.*