社会の安全とネットワーク阻止モデル

宝崎　隆祐

情報通信ネットワーク等のインフラストラクチャー・ネットワークをはじめ，ネットワーク構造を使って分析する研究分野は数多くある．ネットワーク阻止モデル (network interdiction model, NIM) とは，ネットワーク上での阻止活動が絡む意思決定問題のモデル群である．この報告では，その多くが社会の安全に寄与すべく現実問題の解決を目指す NIM 研究を解説し，その中でゲーム理論を応用したいくつかのモデルについて具体的に触れる．

キーワード：ネットワーク，ゲーム理論，阻止

1. はじめに

情報通信ネットワーク等のインフラストラクチャー・ネットワークをはじめ，ネットワーク構造を使って分析する研究分野は数多くある．ネットワーク阻止モデル (network interdiction model, NIM) とは，ネットワーク上での阻止活動が絡む意思決定問題のモデル群である．この報告では，その多くが社会の安全に寄与すべく現実問題の解決を目指す NIM 研究を解説し，その中でゲーム理論を応用したいくつかのモデルについて具体的に触れる．

モース，キンボールによって著された有名な著書『オペレーションズ・リサーチの方法』 [1] では，格子に見なした海峡において潜水艦の通峡阻止のための対潜航空機の戦略をすでにゲームにより議論していることはご存知だろうか．このような阻止や査察の戦略を取り扱う査察ゲーム (inspection game) [2] は，必ずしもネットワーク環境を前提としてはいないが，国防や国際・国内的なセキュリティに寄与する目的で議論されてきた．このゲームは，囚人のジレンマで有名な Dresher [3] が軍縮問題や関係国に対する査察の有効性を分析する目的で始めたが，それ以降も，米国軍備管理軍縮局 (ACDA)，国際原子力機関 (IAEA) や核拡散防止条約 (NTP) の関連する活動や他の国際条約の分析手法として使用された長い歴史がある．

1980 年から 1990 年代になると，査察ゲームは米合衆国の関税局，麻薬取締局や国防総省といった組織が直面した麻薬問題の分析に適用され，新しく密輸取締ゲーム (smuggling game) へと拡張・発展させられた．Thomas and Nisgav [4] は，密輸者と取締機関との間の攻防をゲーム理論を使って議論している．密輸取締ゲームの多くは，ネットワークとは無関係に多段ゲームとしてモデル化されたものが多いが，その一部には非合法薬物の密輸や輸送ルートをネットワークと見なしてその阻止を論じたものもあり，Mitchell and Bell [5]，Caulkins ら [6]，Washburn and Wood [7]，Salmeron [8] や Bakir [9] の研究がある．Caulkins らは陸，海，空経由のルートを想定したシミュレーションによる分析であり，密輸者のルート選択と取締者のルート監視による阻止確率をシミュレーションの途中結果により変化させる手法を用いている．一方，Washburn and Wood は整数計画法とグラフ理論を用いた 2 人ゼロ和ゲームによるやや理論的な研究である．Salmeron の研究は，侵入してくる侵入者に対し阻止側が複数種の探知センサーを用いて探知しようとするもので，総探知確率を支払としたゲームを 0-1 整数計画問題により定式化している．Bakir は，輸送コンテナーに紛れ込ませて港湾経由で密輸される禁止武器等を阻止する問題をシュタッケルベルグ・ゲームにより分析している．

上記の密輸問題以外にもネットワーク阻止モデルに関しては多くの研究があり，グラフ・ネットワーク理論の一般的な拡張問題を議論した研究から，軍事輸送網の航空破壊，テロに対する施設防御，流行病の感染ルート阻止，危険な化学物質による汚染阻止の問題等，多くの具体的な適用例が考えられている．そして，これら問題解決型のモデルの一部にゲーム理論による分析が使われている．

Ford and Fulkerson [10] は，その一般的なネットワーク技法の解説本の中で，最小カットの応用例として，出発ノード (s) から目的ノード (t) までのすべてのパスを遮断するためのアークの削除を取り上げている．

ほうざき　りゅうすけ
防衛大学校
〒 239–8686　神奈川県横須賀市走水 1–10–20

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

Wollmer [11] は，ある与えられた数のアークを破壊し最大流をできるだけ減少させる方策を問う研究である．McMasters and Mustin [12] や Ghare ら [13] は，ネットワークでの最大流手法を利用し，予算制約の下で敵の軍事補給量をできるだけ減少させる輸送網の破壊を応用例と考える研究である．Fulkerson and Harding [14] や Golden [15] では，アークの破壊をアーク長の増大になぞらえ，s, t 間の最短経路長を予算内にできるだけ増加させる手法について議論している．Cappanera and Scaparra [16] はネットワークにおける最短経路に支障をもたらす損傷を予防するための防護資源の配分問題を論じている．Wood [17] はゲームの枠組みを使い，攻撃側が予算制約下でネットワークの一部を破壊し，次にネットワーク使用者が生き残ったネットワークでのフローを最大化するというモデル化においてシュタッケルベルグ均衡点を求めている．Akgun ら [18] もシュタッケルベルグ型ゲームを取り扱い，複数ターミナル最大流ネットワーク阻止問題 (multi-terminal maximum-flow network-interdiction problem, MT-NIP) と呼ばれる多品種最大流の阻止問題を議論している．

ネットワーク上で考えるフローに関しては一般的に保存則が成り立つとするモデルが多いが，アークを流れる際に増減することが可能とするのが一般化フロー (generalized flow) である．Lawler の著書 [19] では，アーク (i, j) 上を流れる間に定数倍となるモデルをロスとゲインのあるネットワークとして簡単に解説しており，各国間の通貨の換金問題やジョブ割当問題を表現するネットワークとして使用している．Ahuja ら [20] も一般化フローを適用した多くの例を示しており，投資入力に対し利益率がかけられるファイナンス問題，原材料の精製や原材料が製品化されるプロセス表現，あるいは原材料の製造機械投入計画や航空機の航空路割当問題等がこのモデルにより取り扱いうることを示している．Hohzaki and Chiba [21] では，定数倍による増減ではなく，阻止側戦略によりフローそのものに損耗が起きる阻止側と流入側との損耗ゲームを扱っており，プレイ中の情報取得に関する影響分析も行っている．

Salmeron ら [22] の研究は，テロリストによる発送電網の被害を緩和するゲームを扱ったものである．施設の防御問題を論じたものとして，Church ら [23], Scaparra and Churce [24] や Desai and Sen [25] がある．Church らは施設とそのロジスティクスサービスを受ける需要点のあるネットワークを対象に，需要量確保の点からどの施設が損害を受けた場合が最もダメージが大きいかの問題を考え，Scaparra and Churce は，先手が施設をまず補強し，次に後手がそれを観察後，施設を攻撃するというシュタッケルベルグ・ゲームの枠組みでの施設防御を議論している．Desai and Sen の施設防御問題は，アークを補強する複数種の資源の配分問題も組み込んだものであるが，同時に輸送網，情報通信網といったネットワーク全体の信頼性を確保するためにどのアークを作成するかといったネットワーク設計も含んだ問題を扱っている．施設警備へのゲーム理論応用では，直接的にはネットワークを場としてはいないが，Pita ら [26] は，侵入者としてテロリストや密輸者等の複数タイプを考慮したベイジアン・シュタッケルベルグ・ゲームをロサンゼルス国際空港警備に利用したシステムの実例を報告している．これに対し，施設内で警備側の巡回路や侵入者の侵入経路を陽に取り入れた 2 人ゼロ和ゲームを，森田ら [27] や Hohzaki ら [28] が取り扱っている．

ネットワーク設計に関しては，1 本のアークの欠落に対しノード対間の要求流量を確保する問題を Gibbens and Kelly [29] が，2 本のアーク欠落に対する問題を Ouveysi and Wirth [30] が研究している．IT 社会となり最も重要となっている情報通信ネットワークに NIM を適用した研究もある．Kodialam and Lakshman [31] は検査予算の制約の下で，通信網へのウィルスその他の侵入行為を探知するパケット検査のサンプリング戦略を提案している．Smith ら [32] は，ネットワーク設計の観点から，攻撃から通信網を防御する方法を議論し，Alveras ら [33] は，携帯電話通信網のどのノードが通信不能に陥っても要求通信量を確保できるネットワーク設計問題を議論している．また Myung ら [34] は，ノード欠落による通信容量の減少率を通信ネットワークの Survivability として定義し，Survivability を計算するアルゴリズムによって通信網の脆弱性について分析している．上記した Gibbens and Kelly や Ouveysi and Wirth の研究も，情報ネットワークの設計に関する研究に分類することができる．

大量輸送網はテロの標的になりやすく，特に欧州では多くの事件が発生している．ゲーム理論は交通ネットワーク防護にも応用されているが，Perea and Puerto [35] は攻撃に強い鉄道網の設計問題を考えている．また，道路交通網に関する阻止問題の研究としては Bell ら [36] がある．彼らは，まずテロ行為により道路の一部が破壊され，次に公的機関による交通量確保の行動がとられるとするモデルを用い，ロンドン

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

における道路網の脆弱性をゲーム論的に検証している．

Assimakopoulos [37] は病原菌の感染ルート遮蔽問題であり，ギリシャの病院における適用事例を述べている．Whiteman [38] や Brown ら [39] は軍事分野に対する応用研究である．特に Brown らの研究は，戦術弾道弾 (theater ballistic missile, TBM) に対する米国およびその同盟国のミサイル防衛モデルを議論したものである．防御側態勢を知ったうえでの攻撃側 TBM による最悪の被害を最小に局限する防御側のミサイル防御問題を，シュタッケルベルグ・ゲームにより分析している．

待ち伏せゲーム (ambush game) [40] は伝統的には阻止ゲームよりは狭い範囲の問題を扱うものの，その問題設定には阻止ゲームと重複する部分は多い．阻止ゲームが一般的なネットワーク上で設定されることが多いのに対し，待ち伏せゲームは離散的な長方形格子や連続的な四角領域を空間として設定する．Ruckle [40, 41] が待ち伏せゲームのモデルを最初に提案したが，そこでは青軍がある領域の通過を目指すのに対し，赤軍が待ち伏せし，青軍の拿捕もしくは損耗を図ろうとする．最初に引用したモース，キンボールによる海峡における対潜問題も，問題設定からいえば，待ち伏せゲームの起源と見なしてもよいかもしれない．

以上のようにネットワークにおける阻止問題は，ゲーム的取り扱いをするしないにかかわらず，多くの従来研究をもつ．阻止ゲームは，阻止側と敵対する側の立場から，ときに侵入ゲーム (infiltration game) [42] と呼ばれることもある．

これまで NIM に関する従来研究を概観したが，以下ではその中のゲーム理論を応用したいくつかのモデルを解説する．2 節では社会の基盤的ネットワークとしての鉄道網の設計問題と電力発送電網の防護問題を，3 節では密輸阻止と施設防御・警備の問題をその問題設定を中心に説明するため，解法について興味のある方は個々の参考文献をご参照願いたい．

2. インフラネットワーク防護のゲーム

2.1 鉄道網設計問題

ここではまず，我々にとって身近な交通網の設計および防護にゲーム理論を応用した研究を解説する．この分野での参考文献は Hollander and Prashker [43] に詳しいが，ここでは Perea and Puerto [35] による鉄道網設計問題 (railway network design, RND) を取り上げる．

鉄道網もネットワークで表現できる代表的な例である

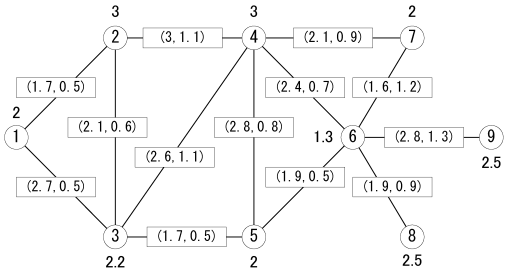

図 1　建設可能鉄道網 [35]

が，図 1 には駅をノードで，建設可能鉄道軌道をアークで表している．ノードの横の数字は駅の建設費用，アーク上に書いてある数字の組は，前の数字が建設費，後ろが列車の通過所要時間である．このネットワーク上に起点となる出発駅と経由駅，終点となる到着駅を設定して 1 つの路線ができあがる．鉄道事業でしばしば評価尺度となるのが旅客カバー率 (trip coverage) や総旅行時間 (total traveling time) である．旅客カバー率は出発地，到着地間を他の代替交通より速く運ぶことのできる旅客数の割合である．路線網設計の問題は，与えられた建設費の範囲内でこれらの評価尺度を最適化する路線を設計することである．

いま図 1 のような建設可能鉄道網のアーク集合を $\boldsymbol{E}$ で，考えられる路線網の集合を $\boldsymbol{R}$ で表し，その 1 つ $r \in \boldsymbol{R}$ を採用することによる評価尺度の値を $K(r)$ としよう．また，鉄道網防護の観点から 1 つのアーク e に不備があった場合の評価尺度を $K(r,e)$ で表す．$K(r)$ を旅客カバー率のように最大化すべき評価尺度であるとすると，次のような問題設定ができる．

$$\max_{r\in R}\min_{e\in E}\ K(r,e)$$

$$\max_{r\in R}\ \left\{\left(1-\sum_{e\in E}\delta_e\right)K(r)+\sum_{e\in E}\delta_e K(r,e)\right\}$$

第 1 の問題は，記述された最適化の順番からマックスミニ最適化問題と呼ばれるゲーム理論のアプローチが使われ，意図的な軌道破壊に対し頑強性のある路線網設計を求めようとするものである．すなわち，路線網が知られている中で破壊工作が行われ，そのダメージを最大限和らげる路線網設計をしようとする問題である．第 2 の問題は，アーク e の軌道の故障率 δ_e を考えた期待評価尺度の最大化を目指すものである．第 1 の問題の拡張問題として，積極的な鉄道網防護と柔軟性のある防護戦略をとる観点から，保安員やセキュリティ担当スタッフなどの防護資源を配備することにし，

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

$K((r,x),e)$ を，路線網 r に防護資源配備の追加戦略 x がとられた後にアーク e へ破壊活動がなされた場合の評価尺度であるとする．通常，戦略 x もセキュリティ関連費用内でとられることになるだろうし，もし x が e への破壊行為の防止に十分な効果があれば，ダメージのない値 $K((r,x),e)=K(r)$ と考えられる場合もある．尺度 $K((r,x),e)$ そのものの評価の難しさはさて置くとして，マックスミニ問題 $\max_{(r,x)}\min_e K((r,x),e)$ も，防護戦略を加味して，意図的な破壊工作に強い路線網を設計しようとする問題である．

2.2 電力発送電網防護問題

電力の発送電網（電力グリッド）は国の基幹ネットワークといってよい．産業や国民生活で必要とされる電力供給に支障が生じた場合の影響と損害は極めて大きい．そのような電力グリッドの主要な要素として，発電所や変電所，送電線，母線があり，これらがテロの対象になりうる．Salmeron ら [22] は抗担性のある電力グリッドに焦点をあて，電力会社の電力コストを最も悪化させるようなテロによる破壊工作が何かを明らかにしようと，シュタッケルベルグ・ゲーム型のモデルを考えた．

発電設備，変電設備，送電線および母線 (bus) の 4 つの要素に対する軽微な破壊工作が行われると，障害のない電力グリッドで実現されていた経済的な電力コスト（発電コストと送電コストの和）は増加の影響を受ける．彼らのモデルは，障害のあるグリッドを使用して電力需要を満足させるために電力会社が行う電力コスト最小化を考慮して，どの場所に破壊工作を行えば最小化される電力コストを最大に悪化させることができるかを導出するモデルとなっている．現在ある電力グリッドで電力コストを最小化するための発電量および発送電網への送電量を求める問題は DC-OPF (DC-optimal power flow) 問題と呼ばれ，この最小電力コストを最大化する最適破壊計画問題は I-DC-OPF (interdiction DC-OPF) 問題と呼ばれる．彼らは，この問題を上記 4 要素の破壊点を示す 0-1 変数を使用して定式化したが，最適化問題としては凸最大化を含んでいるため厳密解法は難しい．そこで彼らは，繰り返し計算により I-DC-OPF 問題を近似的に解くアルゴリズムを提案している．

ここでは，彼らの定式化とアルゴリズムを提示することはやめ，どのような答えが得られるかを読者に把握していただくため，彼らの数値例を図 2 に示した．ある破壊工作資源量制約の下での近似的な最適破壊点として 2 つの案が求められる．1 つは黒丸に白字の 1 で示された 1 つの発電所と 3 つの発送電ラインの破壊，もう 1 つは 2 で示されている 6 つの送電線の破壊である．

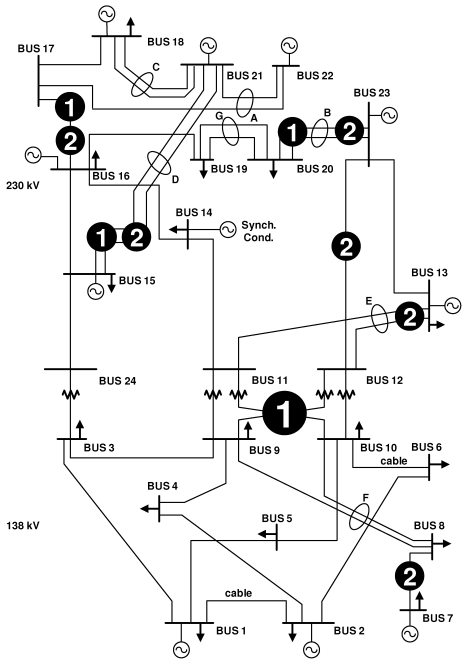

図 2 電力グリッドとその攻撃 [22]

3. 密輸阻止と施設防御・警備のゲーム

3.1 密輸取締ゲーム

米国は，中南米を供給源とする麻薬密輸問題に長く苦しめられてきた．密輸阻止に対する 1 つの試みがゲーム理論の活用であった．Washburn and Wood [7] は，密輸ルートを経由する密輸阻止を 2 人ゼロ和ゲームにより分析している．彼らはいくつかのモデルを議論しているが，その基本モデルは次のとおりである．

密輸網をネットワークで表現する．阻止者は 1 カ所のアークに取締官を駐在させ密輸者を発見しようとし，密輸者は出発ノード s から目的ノード t までの密輸ルートを選択して発見されずに移動したい．取締官のいるアーク k を密輸者が通る場合の発見確率は p_k である．このネットワークに関し，アーク k がパス l に含まれるならば 1 をとり，そうでなければ 0 となる値 d_{kl} を k 行 l 列の要素にもつ行列を $\boldsymbol{D}$ とし，k 行 k 列の対角要素が p_k でありその他の要素はゼロである対角行列を $\boldsymbol{P}$ とする．阻止者がアーク k に取締官を駐在させる確率を x_k とするベクトル $\boldsymbol{x}$ の混合戦略をとり，一方の密輸者はパス l を確率 y_l で選択するベクトル $\boldsymbol{y}$ の混合戦略をとるとする．ゲームの支払を発見確率とすれ

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

ば，期待支払は行列演算 $\sum_k \sum_l x_k p_k d_{kl} y_l = \boldsymbol{x}PD\boldsymbol{y}$ で与えられ，阻止側をこれを大きく，密輸者は小さくしたい．この式は支払行列を PD とする行列ゲームの期待支払でもあるから，有限個の戦略をもつ通常の行列ゲームの解法である線形計画問題への定式化ができる．ここで，密輸側のパス選択確率をノード s から t まで保存されるフローと見なして，問題をネットワークフロー問題としてとらえ直すところがこの研究の面白いところである．

さらに，彼らはこの基本問題を，(1) 複数出発ノードおよび複数到着ノードをもつケース，(2) ノードでの取締りが行われるケース，(3) 複数密輸者のいるケース，および (4) 複数の取締官駐在が可能なケース，に拡張している．最後のケースでは，取締官の総数を m とし，z_k をアーク k 上に配備する取締官数を表す阻止側の純粋戦略（$\sum_k z_k = m$ を満たす）として，発見確率を含めいくつかの支払に議論を広げている．すなわち，阻止側戦略 $\boldsymbol{z}$ と密輸者側のパス l に対する支払として，（ア）探知できる人数の期待数 $AD(z,l) = \sum_{k\in A(l)} p_k z_k$，（イ）発見確率 $IND(z,l) = 1 - \prod_{k\in A(l)}(1-p_k)^{z_k}$，および（ウ） 阻止が最も期待できるルート上での最大発見確率 $MAX(z,l) = \max_{k\in A(l)} p_k I(z_k)$ を取り上げた．ただし，$A(l)$ はパス l の構成アーク群であり，$I(z_k)$ は指示関数 $\{1(z_k > 0$ ならば)，0 $(z_k = 0$ ならば)$\}$ である．

3.2 施設防護ゲーム

Scaparra and Church [24] のモデルと定式化は，施設防護ゲームを簡単に解説するには都合がよい．まず，先手である防護側がネットワーク上のノードにある q カ所の供給施設を防護する．次に，それを観測した後手である攻撃側が防護されていない r カ所の施設に攻撃を仕掛ける．この 2 人ゼロ和のシュタッケルベルグ・ゲームの支払は需要点の需要を賄うためのロジスティクスコストであり，彼らの研究は攻撃側による最悪の被害を最小化する防護を事前に施す問題を議論したものである．この問題は RIMF (r-interdiction median problem with fortification) と呼ばれる．

定式化のためのパラメータとして次を用いる．F：供給施設群，N：需要点群，T_{ij}：需要点 i に対し施設 j よりも輸送コストのかかる供給施設群，a_i：需要点 i の需要量，d_{ij}：施設 j から需要点 i への単位供給量当たりのロジスティクスコスト．また，決定変数として次を定義する．z_j：施設 j を補強するかどうかを示す 0-1 変数，s_j：施設 j を攻撃するかどうかの 0-1 変数，x_{ij}：施設 j から需要点 i へサービスを行うかどうかを示す 0-1 変数．以上のパラメータ，決定変数を用いて次式で示される問題が施設防護ゲームである．

$$\min_z H(z) \;\; s.t. \;\; \sum_{j\in F} z_j = q,\; z_j \in \{0,1\}\ (j \in F).$$

ただし，$H(z)$ は次の問題から求めた最大値である．

$$\begin{aligned} H(z) = \max_{x,s} \;& \sum_{i\in N}\sum_{j\in F} a_i d_{ij} x_{ij} \\ s.t. \;& \sum_{j\in F} x_{ij} = 1\ (i \in N), \quad \sum_{j\in F} s_j = r, \\ & \sum_{h\in T_{ij}} x_{ih} \le s_j\ (i \in N, j \in F), \\ & s_j \le 1 - z_j\ (j \in F), \quad s_j \in \{0,1\}\ (j \in F), \\ & x_{ij} \in \{0,1\}\ (i \in N, j \in F). \end{aligned}$$

最大ロジスティクスコスト $H(z)$ を求める問題の第 1〜4 の条件のそれぞれは，どの需要点 i もどこかの供給施設から需要を満たされること，攻撃が仕掛けられる施設数が r であること，攻撃のない供給設備からは通常どおり最もコストの安価な需要地に供給すること，および防護された施設は攻撃しないこと，を示す．最初の問題は，最悪の結果をもたらす攻撃を見越して，q 施設を防護する最適な防護計画を求める問題である．この整数計画問題を含むゲームに対し著者たちは数値解法アルゴリズムを提案しているが，その説明は省略する．

3.3 施設警備ゲーム

2000 年代になりテロ活動とその防止に世界的な関心が集まるようになって以来，これまで述べたような空港等の施設や電力グリッド等のインフラネットワークの防護・警備が見直されるようになった．これまでのややもすればマンネリ化しがちであった防護・警備体制は，事前の監視により警備情報を取得された後の意図的な破壊工作には弱いことが指摘され始め，それに対する対抗策の一つとして，ゲーム理論が提供する混合戦略の概念を警備体制の合理的なランダム化に用いようとする試みがなされた．同時に，破壊工作を行う非合法組織の動機や意図に関する合理的な推測も，ゲーム理論による分析から明らかになることが期待されている．

Pita ら [26] は，ロサンゼルス国際空港警察と協働して，空港警備システムにゲーム理論によるソルバーを組み入れ，日々の時間帯ごとに道路の検問および警備犬による巡視行動をスケジュールする ARMOR (assistant for randomized monitoring over routes) システムを稼働させた．ゲーム理論を用いたソルバー名が DOBSS (decomposed optimal Bayesian Stackelberg solver) であることからわかるように，ベイジアン・シュタッ

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

ケルベルグ・ゲームの均衡解が求められ警備に使用されている．ベイジアン・ゲームを採用したのは，空港に侵入する不審者にテロ犯，密輸人等のいくつかのタイプを考えているところからきており，先手・後手のあるシュタッケルベルグ・ゲームのモデルは，前述したようないくぶんかの警備情報が侵入者に取得されることを前提としている．また，警備計画が侵入者や警備側へ与える影響は異なるとする非ゼロ和の仮定をし，経験的な評価から支払行列を作成している．ARMORシステムでは，警備関係者とシステムの間のマンマシン・インターフェースのバックステージでDOBSSが稼動している．

Pitaらの研究にはネットワーク構造は陽には使われていないため，以下では，施設内での巡視ルートや侵入ルートを陽に考慮した警備問題として，森田ら [27] およびHohzakiら [28] による研究を解説する．

まず，施設内の出入口，廊下，交差点等を表すネットワークと警備員の視界を妨げる敷居や壁，備品等の位置情報が2次元ユークリッド平面上で与えられる．警備員の複数の巡回ルートには，いつどこを通るかについての概略のスケジュールがある．施設の脆弱性その他に関する知識から，侵入口と重要物品や重要エリアを結ぶ経由点データのみの属性をもつ複数侵入ルートが見積もられ，侵入者はこれらのいずれかの侵入ルートを通るであろうと予測される．警備側，侵入者側双方の評価尺度は視認度と呼ばれる値で定義され，各時点におけるその値は，(1) 障害物の位置関係から侵入者位置が警備員から見える位置にあるかどうか ($\delta \in \{1, 0\}$)，(2) 双方の距離 (d)，および (3) 侵入者のいる地点の明るさ (α)，の3つの項目による値 $\delta\alpha/d^2$ で与えられるとする．この値が大きいほど，侵入者が警備員から発見される可能性は高いと思われる．したがって，侵入者は総視認度を小さくするように動き，警備員は大きな視認度を好むものとする．侵入者側からの警備に関する観測性は，一度施設に侵入した侵入者は，物陰からの観察により，警備員が現に巡回しているルートを予想できるとする仮定により与えられる．

以上の状況設定に対し，著者らは3つの問題を考えている．第1の問題は，個々の警備巡回ルートに対し各侵入ルートを侵入者が移動する場合の総視認度を最小にする経由地点での停留時間を求める「侵入スケジューリング問題」である．これによって得られる最小視認度は，侵入路に対する巡回路の定量的な有効性を示す．第2は，第1の問題で明らかにした巡回路と侵入路の相性を考慮し，複数ある巡回路をどのように選択すべきかの「巡回路選択問題」であり，この問題を行列ゲームとして解き，得られる均衡解の混合戦略により巡回路選択の合理的なランダム化を可能としている．最後の問題は，警備員が1つの巡回路をたどっている間，複数想定される侵入路を考慮してどの方角にどの程度の注意を払えばよいかの「注視配分問題」である．この問題設定には，警備ロボット搭載のセンサー制御のように，警備の自動化の要請に対応しようとする研究動機がある．この問題に対する2人ゼロ和ゲームとしてのモデル化から，侵入者の最適戦略としての侵入

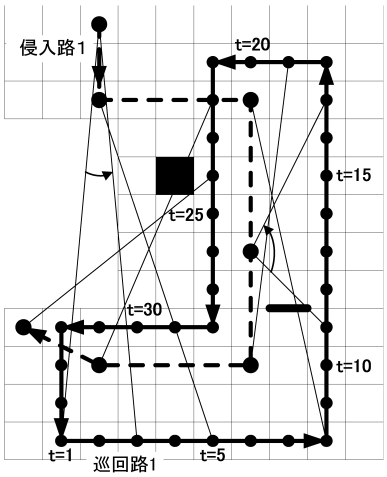

図 3　巡回路に対する最適侵入スケジュール

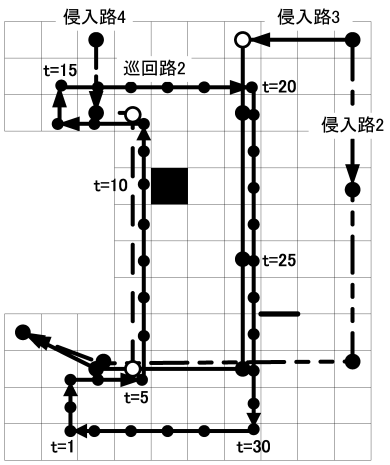

図 4　他の巡回路と侵入路

表 1　警備巡回路 (s) と侵入路 (j) との支払行列

$s \setminus j$	1	2	3	4
1	0.5801	0.9912	0.5295	0.6259
2	0.8814	0.1679	0.5625	2.4993

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

路選択確率と，警備員の最適戦略としての各時点での注視配分に関する均衡解が求められる．

2 人ゼロ和ゲームの均衡解の性質から，「巡回路選択問題」における警備側の均衡解は，個々の侵入路に対する個々の巡回路の脆弱性を第 1 の問題から求めた最小視認度により定量化したうえで，各々の侵入路に対しどれか 1 つでも強い巡回路があれば，それを混合戦略の中で採用することにより，どの侵入路に対しても平均的に頑強な巡視計画を作ろうとするやり方である．一方の「注視配分問題」では，1 つの巡回路からの注視量を複数侵入路全体へ平滑化して配分し，どの侵入路へもバランスよく目配りをする均衡解が得られる．

図 3 には，複数の四角形のセルで分割された施設平面図が描いてある．中央左上の 4 角形と右下の幅広の直線はともに障害物である．左下の点から出発して一巡して戻ってくる実線のループが警備巡回路 1 であり，左上の点から左下の点に延びた太い破線が侵入者の侵入路 1 である．途中の経由点ノードが黒丸で描かれているのは，そこが外からは見えない場所であることを示している．その他の詳細なパラメータ設定は省略するとして，巡回路を移動する警備員に対しこの侵入路上で最小の視認度を得るための移動スケジュールが，巡回路上での警備員位置と同時刻における侵入路上での最適位置とを結んだ細い直線で示されている．このスケジュールを詳しく解析すれば，（ア）障害物の死角を利用した移動，（イ）後の効果的移動を可能にするための経由点での時間調整，（ウ）経由点での警備員のやり過ごし，（エ）警備員の視角に入る場合の遠距離位置関係の維持，といったまるで人間が行いそうな行動がスケジュールされている．このケースでの最小視認度は 0.5801 である．図 4 には他の 1 つの巡回路と 3 つの侵入経路が示されていて，これら全体で 4 本の侵入路に対する 2 本の巡回路の有効性を示す最小視認度の支払行列が表 1 で示されている．この行列ゲームを解けば，警備巡回路の最適な選択確率あるいは使用頻度として，巡回路 1 と 2 の合理的な選択確率 0.461，0.539 を得る．

4. おわりに

この報告では，社会の安全に関わる意思決定問題の解決を目指すネットワーク阻止モデル (NIM) について解説した．その中でも特にゲーム理論が適用できる例を中心に紹介したが，紙数の関係でほんの数例を挙げることができたにすぎない．複数の意思決定者の存在する問題のモデル化には，ゲーム理論を利用することが現在のところ最も科学的な説得力があるといえるものの，ゲーム理論が提供する定番の解法は極めて少なく，問題ごとに工夫して均衡解を導出しなければならないことが多い．また今回の調査を通じて感じたのは，欧米においてはオペレーションズ・リサーチ (OR) のような数理的分析の現場適用を手助けする仲介者が日本に比べ多く，現場の意思決定者が OR に触れ，それを積極的に活かそうとする機会が多いことである．したがって，実業界とアカデミアとの意見交流も盛んであり，それがまた理論家のやりがいも生んでいるように思える．この解説で紹介したモデルが日本の現場で少しは話題になり，現実的な観点から適応可能性のふるいにかけられるかと問われると，まだ遠い状況にあるのではと思う．

参考文献

[1] P. M. Morse and G. E. Kimball, *Methods of Operations Research*, MIT Press, 1951.

[2] R. Hohzaki, *Inspection Games*, Wiley Encyclopedia of Operations Research and Management Science, pp. 1–9, 2013.

[3] M. Dresher, *A Sampling Inspection Problem in Arms Control Agreements: A Game-Theoretic Analysis*, The RAND Corporation, Memorandum RM-2972-ARPA, 1962.

[4] M. Thomas and Y. Nisgav, “An infiltration game with time dependent payoff,” *Naval Research Logistics Quarterly*, **23**, pp. 297–302, 1976.

[5] T. Mitchell and R. Bell, *Drug Interdiction Operations by the Coast Guard*, Center for Naval Analysis, 1980.

[6] J. P. Caulkins, G. Crawford and P. Reuer, “Simulation of adaptive response: A model of drug interdiction,” *Mathematical and Computer Modeling*, **17**, pp. 27–52, 1993.

[7] A. Washburn and K. Wood, “Two-person zero-sum games for network interdiction,” *Operations Research*, **43**, pp. 243–251, 1995.

[8] J. Salmeron, “Deception tactics for network interdiction: A multiobjective approach,” *Networks*, **60**, pp. 45–58, 2012.

[9] N. O. Bakir, “A Stackelberg game model for resource allocation in cargo container security,” *Annals of Operations Research*, **187**, pp. 5–22, 2011.

[10] L. R. Ford and D. R. Fulkerson, *Flows in Networks*, Princeton University, pp. 14–15, 1962.

[11] R. D. Wollmer, “Removing arcs from a network,” *Operations Research*, **12**, pp. 934–940, 1964.

[12] A. W. McMasters and T. M. Mustin, “Optimal interdiction of a supply network,” *Naval Research Logistics Quarterly*, **17**, pp. 261–268, 1970.

[13] P. M. Ghare, D. C. Montgomery and W. C. Turner, “Optimal interdiction policy for a flow network,” *Naval Research Logistics Quarterly*, **18**, pp. 37–45, 1971.

[14] D. R. Fulkerson and G. C. Harding, “Maximizing the minimum source-sink path subject to a budget

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

constraint," *Mathematical Programming*, **13**, pp. 116–118, 1977.
[15] B. Golden, "A problem in network interdiction," *Naval Research Logistics Quarterly*, **25**, pp. 711–713, 1978.
[16] P. Cappanera and M. P. Scapara, "Optimal allocation of protective resources in shortest path networks," *Transportation Science*, **45**, pp. 64–80, 2010.
[17] K. Wood, "Deterministic network interdiction," *Mathematical and Computer Modeling*, **17** (2), pp. 1–18, 1993.
[18] I. Akgun, B. Tansel and R. K. Wood, "The multiterminal maximum flow network-interdiction problem," *European Journal of Operational Research*, **211**, pp. 241–251, 2011.
[19] E. L. Lawler, *Combinatorial Optimization: Networks and Matroid*, Holt, Rinehart and Winston, pp. 134–138, 1976.
[20] R. K. Ahuja, T. L. Magnanti and J. B. Orlin, *Network Flows*, Prentice-Hal Inc., pp. 566–597, 1993.
[21] R. Hohzaki and T. Chiba, "An attrition game on an acyclic network," *Journal of the Operational Research Society*, 2014. DOI: 10.1057/jors.2041.61
[22] J. Salmeron, R. K. Wood and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Transactions on Power Systems*, **19**, pp. 905–912, 2004.
[23] R. L. Church, M. P. Scaparra and R. S. Middleton, "Identifying critical infrastructure: The median and covering facility interdiction problems," *Annals of the Association of American Geographers*, **94**, pp. 491–502, 2004.
[24] M. P. Scaparra and R. L. Church, "A bilevel mixed integer program for critical infrastructure protection planning," *Computers and Operations Research*, **35**, pp. 1905–1923, 2008.
[25] J. Desai and S. Sen, "A global optimization algorithm for reliable network design," *European Journal of Operational Research*, **200**, pp. 1–8, 2010.
[26] J. Pita, M. Jain, F. Ordonez, C. Portway, M. Tambe and C. Western, "Using game theory for Los Angeles airport security," *AI Magazine*, **30**, pp. 43–57, 2009.
[27] 森田修平，宝崎隆祐，畠山雄介，"数理計画法を用いた警備員の巡視路選択問題，" 数理モデル化と応用，**4**, pp. 19–35, 2011.
[28] R. Hohzaki, S. Morita and Y. Terashima, "A patrol problem in a building by search theory," *Proceedings of 2013 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, pp. 104–111, 2013.
[29] R. J. Gibbens and F. P. Kelly, "Dynamic routing infully connected networks," *IMA Journal of Mathematical Control Information*, **7**, pp. 77–111, 1990.
[30] I. Ouveysi and A. Wirth, "On design of a survivable network architecture for dynamic routing: Optimal solution strategy and efficient heuristic," *European Journal of Operational Research*, **117**, pp. 30–44, 1999.
[31] M. Kodialam and T. V. Lakshman, "Detecting network intrusions via sampling: A game theoretical approach," *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications (IEEE INFOCOM)*, **3**, pp. 1880–1889, 2003.
[32] J. C. Smith, C. Lim and F. Sudargho, "Survivable network design under optimal and heuristic interdiction scenarios," *Journal of Global Optimization*, **38**, pp. 181–199, 2007.
[33] D. Alveras, M. Grotschel, P. Jonas, U. Paul and R. Wessaly, "Survivable mobile phone network architectures: Models and solution methods," *IEEE Communications Magazine*, **36**, pp. 88–93, 1998.
[34] Y. S. Myung, H. J. Kim and D. W. Tcha, "Design of communication networks with survivability constraints," *Management Science*, **45**, pp. 238–252, 1999.
[35] F. Perea and J. Puerto, "Revisiting a game theoretic framework for the robust railway network design against intentional attacks," *European Journal of Operational Research*, **226**, pp. 286–292, 2013.
[36] M. Bell, U. Kanturska, J. Schmocker and A. Fonzone, "Attacker-defender models and road network vulnerability," *Philosophical Transactions of the Royal Society*, **366**, pp. 1893–1906, 2008.
[37] N. Assimakopoulos, "A network interdiction model for hospital infection control," *Computers in Biology and Medicine*, **17**, pp. 413–422, 1987.
[38] P. S. Whiteman, "Improving single strike effectiveness for network interdiction," *Military Operations Research*, **4** (4), pp. 15–30, 1999.
[39] G. Brown, M. Carlyle, D. Diehl, J. Kline and R. K. Wood, "A two-sided optimization for theater-ballistic missile defense," *Operations Research*, **53**, pp. 745–763, 2005.
[40] W. H. Ruckle, *Geometric Games and Their Applications*, Pitman, 1983.
[41] W. H. Ruckle, R. Fennell, P. T. Holmes and C. Fennemore, "Ambushing random walks I: Finite models," *Operations Research*, **24**, pp. 314–324, 1976.
[42] J. M. Auger, "An infiltration game on k arcs," *Naval Research Logistics*, **38**, pp. 511–529, 1991.
[43] Y. Hollander and J. Prashker, "The applicability of non-cooperative game theory in transport analysis," *Transportation*, **33**, pp. 481–496, 2006.

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.