ネットワークを考慮した警備ゲームのモデルあれこれ

宝崎　隆祐

この解説は警備問題に関する OR 応用の紹介である．2015 年 5 月号に「社会の安全とネットワーク阻止モデル」[1] のタイトルで，情報通信，ライフライン，交通網，インフラといった現代社会において活用されているさまざまなネットワークへの有害なエンティティの侵入阻止を目的とした OR モデルを取り上げた．本稿ではその中の警備やセキュリティに係わるゲーム理論応用のモデルに焦点を当てる．

キーワード：警備，ゲーム，ネットワーク，巡回・監視，防空

1. はじめに

2001 年 9.11 のテロ発生後にとった Homeland Security に関する米国の政策は，その後の世界に大きな影響を与えた．この政策は『米国内のテロ行為の予防や，テロに対する脆弱性の低減並びに実際にテロが起こった際の被害の最小化と復旧』のためのものと定義されているものの，その後に連続して発生したテロ事案の影響もあり，各国にとっては「米国」を自国に置き換えた緊急性のある共通の施策となりつつある．移動による時間地理的な感覚では世界は確実に小さくなっており，一般市民を狙った他国でのテロ行為が日本でも身近に感じられるものとなっている．このように全世界的なテロ活動が世界共通の問題となったため，オペレーションズ・リサーチ (OR) でもセキュリティに関する多くの提案がなされるようになっている [2].

しかし，このようなテロ活動が問題視されるずっと以前から，街角のセキュリティは OR の題材であった．1972 年の Chaiken and Larson [3] では，警察，消防，救急などの緊急支援システムに関し，(1) 人数やビークルの数，(2) その配置，(3) パトロールや対処地域の指定，(4) 対策チームの配置，(5) 警察車両による犯罪予防のための警備巡回計画，といった個別の問題への OR 応用として 68 編の研究を紹介している．また Olson and Wright [4] は，米国シカゴの犯罪発生率の高い地域における地元警察の出動件数の調査をもとに，都市型犯罪の発見率を高め予防効果のある街区内の巡回経路決定をマルコフ決定問題として議論している．そこでは，この問題には Koopman [5] を創始者とする探索理論の適用が有効であるものの，地域特性や地理的ネットワークを考慮した巡回スケジューリングの必要性が述べられている．

以上のようなセキュリティに係わる古くからの研究は，Homeland Security の概念に対応するためにいくつかの修正を余儀なくされた．それは，特にテロ活動を行う人間の知力と情報収集能力の高さから，それまでのマンネリ化された警備計画の見直しが求められ，また彼らの意図を正しく推測することも必要となったのである．それに対する答えの一つがゲーム理論であった．ゲーム理論における混合戦略（実際に取りうるいくつかの方法を確率的に混合して使う方法）と，警備側のみならずテロ犯その他も複数意思決定者として考慮すべき状況，いわゆるゲーム的状況のモデリングが有効だからである．さらに，公共施設での警備行動が部分的にせよテロ犯に観測可能であることを考えれば，ゲームのモデルとして，意思決定者の行動に先手（リーダー）と後手（フォロワー）を設けたシュタッケルベルグ・ゲーム (Stackelberg game) と呼ばれるモデルが重要となる．かくして，Homeland Security の概念まで考えた警備問題は，近年 Patrolling security game (PSG) や Stackelberg security game (SSG) と呼ばれる警備ゲーム (Security game) として議論されることが多くなっている．

以上の経緯を踏まえ，以下では PSG や SSG の典型的な研究を概観した後，Olson and Wright の指摘に対処すべく，警備の場としてのネットワークを陽に考慮した警備ゲームに関する筆者たちの研究を紹介する．

2. 警備ゲームに関するいくつかの従来モデル

以下では，警備側とその対抗勢力との間の汎用的な

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
hozaki@nda.ac.jp

警備ゲームのモデルとして三つの研究を紹介する．

Garnaev et al. [6] はネットワーク上での守備側と攻撃側とのゲームの研究であるが，攻撃側には二つの意図をもつタイプを考える．第一のタイプは，攻撃による被害を最大にしたい攻撃者である．N 個のノードに対する攻撃側の攻撃資源配分 $\boldsymbol{x}^1 = (x_1^1, \ldots, x_N^1)$ と守備側の守備資源配分 $\boldsymbol{y} = (y_1, \ldots, y_N)$ により，共通の価値 C_i をもつノード i の被害確率が $v_i(\boldsymbol{x}^1, \boldsymbol{y})$ で与えられる場合に，総被害価値 $u_A^1(\boldsymbol{x}^1, \boldsymbol{y}) = \sum_{i=1}^N C_i v_i(\boldsymbol{x}^1, \boldsymbol{y})$ を攻撃側は最大にしたい．第二のタイプは，ネットワークへの侵入を意図する攻撃者である．この場合，攻撃者の資源配分 $\boldsymbol{x}^2$ と守備計画 $\boldsymbol{y}$ による支払を，侵入確率とその価値の積 $u_A^2(\boldsymbol{x}^2, \boldsymbol{y})$ とする．ここで，守備側がタイプ 1 と 2 の攻撃者の現れる確率を q, $1-q$ と推測し，攻撃側の利益を最小にしたければ，$u_D(\boldsymbol{y}, (\boldsymbol{x}^1, \boldsymbol{x}^2)) = -\{qu_A^1(\boldsymbol{x}^1, \boldsymbol{y}) + (1-q)u_A^2(\boldsymbol{x}^2, \boldsymbol{y})\}$ が守備側の最大化したい評価尺度となる．攻撃側のタイプを攻撃者自身は知っているから，このゲームのナッシュ均衡点としては，相手の戦略に対して最適な戦略をとっているという条件を満たすように，任意の $\boldsymbol{x}^1, \boldsymbol{x}^2, \boldsymbol{y}$ に対し次式を満足する特定の $\boldsymbol{x}^{*1}$, $\boldsymbol{x}^{*2}$, $\boldsymbol{y}^*$ を探すことになる．

$$
\begin{aligned}
&u_A^1(\boldsymbol{x}^1, \boldsymbol{y}^*) \le u_A^1(\boldsymbol{x}^{*1}, \boldsymbol{y}^*),\\
&u_A^2(\boldsymbol{x}^2, \boldsymbol{y}^*) \le u_A^2(\boldsymbol{x}^{*2}, \boldsymbol{y}^*),\\
&U_D(\boldsymbol{y}, (\boldsymbol{x}^{*1}, \boldsymbol{x}^{*2})) \le U_D(\boldsymbol{y}^*, (\boldsymbol{x}^{*1}, \boldsymbol{x}^{*2})).
\end{aligned}
$$

論文では，$u_A^k(\boldsymbol{x}^k, \boldsymbol{y})$ の具体的な例として，情報通信ネットワークにおける

$$
u_A^1(\boldsymbol{x}^1, \boldsymbol{y}) = \sum_{i=1}^N C_i x_i^1 (1 - d_i y_i), \tag{1}
$$

$$
u_A^2(\boldsymbol{x}^2, \boldsymbol{y}) = D \sum_{i=1}^N x_i^2 (1 - d_i y_i), \tag{2}
$$

$$
C_i = \frac{h_{Ei} P_i}{\sigma_E^2}, \quad d_i = \frac{g_{Ej} J}{\sigma_E^2 + g_{Ei} J}
$$

の式を与えている．P_i はチャネル i を攻撃する場合の攻撃シグナルの強さ，h_{Ei} と σ_E はこのチャネルの信号ゲインと背景ノイズ，J, g_{Ej} は攻撃阻止のために守備側が送信する防御ジャミングの強さと衰調ゲインである．また，D は攻撃側がネットワークに侵入できた場合の価値を表す．この場合の $\boldsymbol{x}^k, \boldsymbol{y}$ は，一つのチャネルを攻撃する確率および防御する確率を表す混合戦略である．(1), (2) 式のように，支払関数が比較的単純な式であるため，彼らはこのゲームに対し解析的な均衡解を提示している．

Yang et al. [7] はネットワークを考慮しない SSG のモデルである．リーダーは警備側であり，複数ターゲットのうち守備の可能な数が限られた中でどのターゲットを防護するかを決める．フォロワーは攻撃側であり，警備側のランダム化された守備計画を観測して，一つのターゲットへのアタックを決定する．このモデルは，警備側による守備と攻撃側によるアタックの組み合わせによりアタックの成功確率が決まり，この成功・失敗から得られる両プレイヤーの異なる利益・損失がターゲットに依存する非ゼロ和の SSG である．

上記の Garnaev et al. や Yang et al. は，2 人のプレイヤーのターゲットに対する資源配分がターゲットからの利益／損失を生み，その総和で支払の決まるゲームであるが，このように記述されるゲームは古くからブロット・ゲーム [8] と呼び慣らわされている．

Basilico et al. [9] による PSG は，Olson and Wright の研究とよく似た状況設定をしており，守備側はある地域の地理ネットワーク上を巡回する巡視者である．一方の侵入者は，巡視者の現在の位置を観測しつつ，ネットワーク上を移動しながらターゲットのあるいくつかのノードに到着した場合，ターゲットを攻撃するかどうか決める．ただし，攻撃にはある時間を要し，この間に巡視者がやって来れば逮捕される．ターゲットの攻撃成功や侵入者の捕獲に際しては，両プレイヤーとも異なる価値をもつから，問題は非ゼロ和の SSG である．

ほかにも，Tsai et al. [10] や岩下ら [11] のように，都市を含む大きな地域を警備対象とした警備ゲームの研究もある．そこでは，取り扱うネットワークが大規模であるがゆえに，計算アルゴリズムに関する種々の工夫がなされている．また，特殊な施設である電力グリッド，空港，情報通信ネットワーク，鉄道網や道路網を対象とした警備ゲーム [12–16] も研究されているが，これらに関しては宝崎 [1] を参照願いたい．

さて，警備ゲームを現実のシステムの中で活用する試みもすでになされており，2007 年以降のロサンゼルス国際空港における検問設置や警備犬を使った巡回警備には ARMOR (Assistant for randomized monitoring over routes) が配備され，2009 年以降連邦航空保安局による民間機への係員配置計画では IRIS (Intelligent randomization in scheduling) が使用されている．ARMOR のバックステージでは DOBSS (Decomposed optimal Bayesian Stackelberg solver) と呼ばれるソルバーが稼働しているが，その名称自身がそこで

使用されているゲームのモデルを示している．また，連邦運輸保安局による 400 カ所以上の空港への保安要員の配備に GUARDS (Game-theoretic unpredictable and randomly deployed security) が，米国沿岸警備隊による港湾でのテロ対策には PROTECT (Port resilience operational/tactical enforcement to combat terrorism) が試験運用されている．これらのシステムの説明からゲーム理論を用いた解法アルゴリズムに至るまでの詳細を解説しているのが，Tambe [17] である．

これまで警備ゲームに関する従来モデルを概観してきたが，以降では比較的小規模の施設を対象とした警備モデルを詳しく解説し，さらに防空問題やテロ犯などとの衝突による損耗現象を考慮した拡張問題を紹介する．

3. 侵入経路を陽に考慮した施設警備ゲーム

森田ら [18] や Hohzaki et al. [19] は，図 1 のように廊下，交差点や侵入口などを表す警備ネットワークと敷居や壁，備品といった警備にとっての障害物のある 2 次元平面上での警備問題を考えている．いくつかある警備巡回路の中の s 番目のルートが，時点 t で通る概略の位置ベクトル $p_s(t)$ が点と実線で描かれている．また，これもいくつか想定される侵入ルートの j 番目ルートの経由地点ベクトル $q_j(i), i = 1, \ldots, L_j$ が点線上の点で与えられている．この問題での警備側，侵入者側の共通の評価尺度は，侵入者の見つかりやすさを示す視認度と呼ばれる値である．視認度は，障害物の位置関係から侵入者が警備員から見える位置にあるかどうかの可視性 ($\delta \in \{1, 0\}$)，(2) 双方の距離 (d)，および (3) 侵入者のいる地点の明るさ (α) に依存して，$\delta\alpha/d^2$ により計算される．これは警備員の視覚に入る光量の強さを考えた値であり，時々刻々変化する警備側，侵入者の位置関係による総視認度が侵入者の見つかりやすさを表すとして，これを警備側は大きく，侵入者は小さくすることを望んでいるとする．このような状況設定の下で，彼らは四つの問題を考えている．

第一の問題は，図 1 で描いた一つの巡回路 p_s に対する一つの侵入路 q_j の侵入者の見つかりにくさを評価するため，総視認度を最小にする q_j 上での侵入スケジュールを求める『侵入スケジュール問題』である．これは，一度施設に侵入した侵入者は，物陰からの観察により巡回中の巡視者の動きを観測できると想定するからである．

図 1 に例として描いた 35 時点で一巡して戻ってくる巡回路に対し，7 経由地点からなる侵入路の各経由

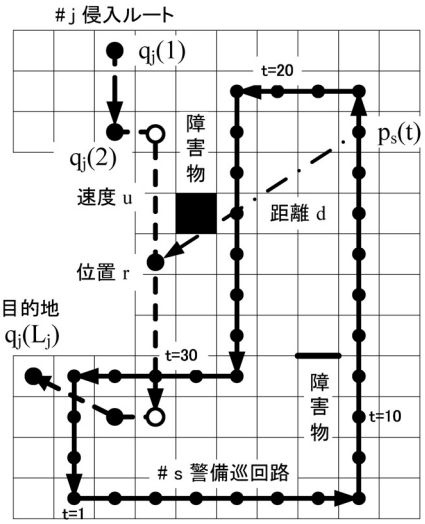

図 1　一つの巡回路と一つの侵入ルートの例

表 1　経由点における最適スケジュール

経由点	最小累積視認度	到着時点	出発時点
1	0	1	3
2	0.0962	5	5
3	0.2118	8	8
4	0.2118	11	17
5	0.4281	19	19
6	0.5801	22	22
7	0.5801	24	

点までの最小累積視認度とそこでの最適な到着時点／出発時点が，動的計画法により表 1 のように得られる．ある経由点と次の経由点の最小累積視認度が同じであれば，その間における侵入者の移動は巡回者からは全く視認されないことを示している．

表 1 の侵入スケジュールでは，侵入者による（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）経由点での巡視者のやり過ごし，（エ）巡視者の視角に入る場合の遠距離位置の維持，といったまるで人間がかくれんぼで使いそうな手練手管が披露されている．

動的計画法による定式化は，時点 t に j 番目の経由点から出発するスケジュールの中で，そこまでの最適なスケジュールにより得られる最小累積視認度を $f_j(t)$ と定義することから始まる．このとき $f_{j-1}(\cdot)$ と $f_j(\cdot)$ の間には次の漸化式が成立する．

$$f_j(t) = \min_z \left\{ f_{j-1}(z) + D_{j-1}(z) + E^j(t) \right\} \quad (3)$$

ただし，$D_{j-1}(z)$ は時点 z に $j-1$ 番目の経由点を出

発した後 j 番目の経由点到着までの移動中の累積視認度を表し，$E^j(t)$ は j 番目の経由点到着後時点 t に出発するまでの停止中の累積視認度を表す．この漸化式は，各経由点までの最短到達時間や各経由点から目的ノードまでの最短所要時間などを考慮して計算ステップを短縮することが可能である．

第二の『巡回路選択問題』では，第一の問題による一つの侵入路に対する一つの巡回路の脆弱性評価を，複数巡回路と複数侵入路の支払行列として用い，行列ゲームの均衡解として巡回路に関する合理的な混合戦略を得る．同時に，侵入者に採択されやすい侵入路についての情報も得られる．第三の問題は，一つの巡回路を通る際に，複数侵入路における最悪の侵入スケジュールを考慮して，限られた視角をもつ注視力を各時点でどの方角に向ければよいかに答える『注視配分問題』である．これもゲームであり，各時点の注視力配分の純粋戦略と侵入者による侵入路選択の混合戦略の組合せに均衡解が存在し，侵入者のどの侵入路に対しても脆弱性のない注視力の配分計画が得られる．警備の自動化の立場で言えば，この計画は，警備ロボットに設置された CCD カメラその他のセンサーに関する合理的な角度制御のアルゴリズムとして使用できる．

第四の『侵入路決定問題』は第一の問題に侵入ルートの決定も含めた問題であり，漸化式 (3) における $f_j(t)$ を，ノード j を時点 t に出発するとした場合の，それまでの最適なルートとスケジュールにより得られるこのノードまでの最小累積視認度を表すと定義し直し，次の漸化式を用いる．

$$f_j(t) = \min_i \min_z \left\{ f_i(z) + D_i^j(z) + E^j(t) \right\}$$

ただし，$D_i^j(z)$ として，ノード j の隣接ノード i を時点 z に出発後ノード j に到着するまでの累積視認度を計算したものを用いる．この漸化式により，侵入者の目的ノード到着までの最小総視認度を求めることになるが，$f_j(t)$ にノード j と時点 t の二つの添字が使われていることからも想像できるように，この計算アルゴリズムとしては，いわゆる時空間ネットワーク（時間拡大ネットワークとも呼ばれる）に適用したダイクストラ法や避難問題に関連して提案された加藤と瀧澤 [20] の手法を用いることができる．問題設定で述べた巡回路を設置場所の固定された防犯カメラに置き換えてもよく，提案手法は身近な警備の自動化に援用することも可能である．

以上の施設内における警備問題は，定式化やアルゴリズムの本質を変えずに，防空問題に応用することができる．この場合の大きな変更点は次のとおりである．まず，警備側は E2C ホークアイや AWACS (Airborne warning and control system) に代表される早期警戒機や固定レーダーサイトであり，それらのもつレーダーが侵入航空機や侵入ミサイルを見つける主要な目となっている．したがって，警備問題で視認度により定義された評価尺度は，防空問題ではレーダー伝搬損失などを考慮した結果受信できるレーダー受波機への目標シグナルパワーとすることが妥当である．これは，レーダー送信パワー (P_{TR})，レーダーゲイン (G_A)，波長 (λ)，目標のレーダークロスセクション (σ) およびレーダーと目標との距離 (R) に依存し，$P_{TR}G_A^2\lambda^2\sigma/(4\pi)^3R^4$ により評価される．その際，レーダークロスセクションは，捜索レーダー波の照射方向に対する目標の体勢に依存する．また侵入者の可視性は，防空側のレーダー波が山脈などで遮断されるかを 3 次元空間で評価して決める．

また，侵入者の侵入スケジュールは，施設警備問題では侵入経路上の経由点での待ち時間によって決まるが，防空問題では二つの経由地点間における経路（飛行レグ）での飛行高度によって表されるとすればよい．通常，高高度を飛ぶ侵入機はレーダーに捕捉されやすいが高速度で飛行でき，防空レーダーに自らを晒す時間を短くできる．逆に，低高度での飛行では飛行速度を遅くせざるを得ず飛行時間は大きくなるものの，山脈などの影に紛れて飛行できる．防空問題の『侵入スケジュール問題』では，動的計画法による定式化 (3) 式は本質的には変える必要はなく，経由点からの出発時点を表す変数 z による最小化が，防空問題では飛行レグでの飛行高度（すなわち速度）による最小化に焼き直される．

図 2 は関東空域での状況設定図であり，日本海側から侵入し太平洋側の目的地まで飛行しようとする不審侵入機に関して予想される 6 本の侵入ルート IR1〜IR6 が実線で描かれている．関東平野を縦断するルート IR4 のほかに，北部，南部を走る山脈に沿って侵入するルートもある．早期警戒機の 4 本の警戒監視ルート PR1〜PR4 は点線で描かれており，またこのエリアをカバーする複数の固定レーダーサイト FR も山頂に存在する．早期警戒機搭載のレーダーの探知半径は大きく関東平野を十分にカバーするものの，山肌を縫う飛行物体を捉えるために移動する．その詳細は省略するが，現実的なパラメータを使って防空問題に関する『侵入スケジュール問題』から警戒監視ルートと侵入

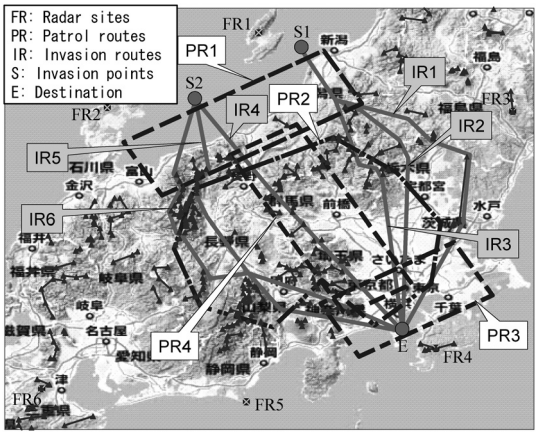

図 2　関東空域の侵入ルートと警戒監視ルート

ルートの相性に関する支払行列が得られ，それから得られる『巡回路選択問題』からは次のような均衡解が求められた．防空監視側にとって太平洋側と関東平野中央を監視する二つの監視ルート PR3 および PR4 が重要であり，それぞれを 0.725 および 0.275 の確率で飛行すべきであり，侵入ルートとしては IR4 および IR5 が危険であり，侵入者はそれぞれを確率 0.309 および 0.691 でとることが予想される．ちなみに『侵入スケジュール問題』の結果から，侵入者にとって，関東平野中央を通る IR4 では短時間飛行を目指した高高度飛行がよく，IR5 では飛騨山脈および木曾山脈中にある飛行レグでは低高度で飛行することがどの警戒監視ルートに対しても最適な飛行プロファイルとなる．

4.　損耗を陽に考慮したシュタッケルベルグ・警備ゲーム

Hohzaki and Chiba [21] には，2 節で解説したいくつかのモデルと同じく，攻撃側と守備側が対峙する 2 人ゼロ和ゲームが取り扱われているが，そこでは損耗現象を陽に扱った損耗ゲーム (Attrition game) が議論されている．情報通信ネットワークにおける悪意あるマルウェアの検知・ブロックや密輸ルートにおける密輸品の阻止などでは，ネットワーク上に配置されたセキュリティ・ソフトや税関の検問により徐々に駆逐される複数の侵入者が想定されるからである．彼らのモデルでは，出発ノードから侵入した侵入者はできるだけ多くの生存数を目的ノードに到達させたいとし，守備側はできるだけ少なくしたいと努力する．ただし，侵入者に種類の違いはないものの，情報取得のない同時手番ゲームと情報取得によりプレイの途中でプレイヤーが戦略を変更できる 2 段階ゲームを論じている．

一方，宝崎 [22] の警備ゲームモデルでは，侵入者にはいくつかのタイプがあり，また警備側の部分的な配備計画を知ることができるベイジアン・シュタッケルベルグ・ゲームが議論の対象となっている．ここでは，後者のモデルとその数値例について簡単に紹介する．

ノード集合 $\boldsymbol{N}$ とアーク集合 $\boldsymbol{A}$ をもつ通常のネットワークを警備の場として，警備対象としての侵入者に対していくつかのタイプ（集合 $\boldsymbol{H}$）を考える．空港であれば，犯罪者，密輸者，テロリストなどである．侵入者はタイプ $h \in \boldsymbol{H}$ ごとに，その初期侵入数 R_0^h と侵入途中でのアーク e で与える 1 人当たりの被害率 d_e^h が変わり，また複数本の侵入経路（集合 Ω^h）が想定される．一方の警備側は，空港における一般警備やテロ対策警備などのように，複数の警備体制（集合 $\boldsymbol{S}$）を取りえて，体制 $s \in \boldsymbol{S}$ ごとに変わる初動の警備人数 B_0^s をアークに配備して警備する．ただし，警備体制によってはコストのかかるものがあるから，体制 s をとる割合には上限 $U(s)$ がある．また，これまでの事案発生数の統計から，侵入者タイプ h の発生確率 $f(h)$ を警備側は予想できる．侵入者は，現に侵入を実行する時点における警備体制については確信をもてないとするが，長期の観測により，警備体制が敷かれる割合と警備員配置に関しては予測できるとしよう．

さて，侵入事案発生時の損耗は警備員の配備されたアークで起きるとし，アーク e でのタイプ h の侵入者に対する警備体制 s の警備員の強さをパラメータ γ_e^{hs} で表す．その意味は，このアークへ侵入したタイプ h の侵入者 x 人と警備体制 s の配備警備員 y 人との衝突による侵入者の残存数を，y に対し線形な式

$$f_e(x,y) = \max\{0,\ x - \gamma_e^{hs} y\} \tag{4}$$

でモデル化するからである．0 は全滅を表す．ただし，パラメータ設定においては，侵入者のタイプごとに妥当な意味づけを与えるべきである．たとえば，密輸者は空港ターミナルを出て初めてその後の密輸品の広まりにより社会的な被害を発生させると考え，ターミナル内での移動中の被害率はゼロと設定すべきであろうし，(4) 式は，暴力的なテロ犯に対しては物理的な人的被害のモデルを示すが，密輸者に対しては，密輸行為が発覚せずに素通りできる人数・件数が警備配備員数によりどのように減少するかを示すモデルとして見るべきである．

以上の前提において，各タイプの侵入者の目的は自らによる被害量の最大化であり，警備側の目的は総被

害量の最小化である．警備側はどのタイプが侵入してくるかの可能性を考慮して，総被害量の期待値を最小化するように警備体制をランダム化し，かつそれぞれの警備体制でのアークにおける警備員配備計画を立てることになる．このゲームも 2 節で述べた従来研究のいくつかと同じく，警備側が侵入者タイプを考慮し，侵入者は警備側の情報をもつベイジアン・シュタッケルベルグ・ゲームである．さて，ゲームの大切な構成要素であるプレイヤーの戦略と支払を詳細に説明しよう．

タイプ $h \in \boldsymbol{H}$ の侵入者の混合戦略を，パス l を選択する確率 $\pi_h(l)$ をもつ $\pi_h = \{\pi_h(l), l \in \Omega^h\}$ で表す．警備側の戦略は，警備体制 s の場合のアーク e への警備員配備数 y_e^s をとる配備計画 $\boldsymbol{y}^s = \{y_e^s, e \in \boldsymbol{A}\}$ と警備体制 s を敷く割合 $g(s)$ とする．

E_l を侵入経路 l のアーク集合とし，E_l^e を経路 l 上での出発ノードからアーク e までのアーク集合として，以下でゲームの支払を導出しよう．タイプ h の侵入者のパス l と警備体制 s の警備員配置 $\boldsymbol{y}^s$ に対する総被害量は，侵入者が各アーク e を生き延びるごとに与える被害の総和として次式で与えられる．

$$R_{hs}^I(l, \boldsymbol{y}^s) = \sum_{e \in E_l} d_e^h \max \left\{ 0, R_0^h - \sum_{e' \in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right\} \quad (5)$$

したがって，警備体制に関する混合戦略 $g(s)$ による期待支払やタイプ h の侵入者の混合戦略 π_h による期待支払は，次式で与えられる．

$$R_h^I(l, (g, \boldsymbol{y})) = \sum_{s \in S} g(s) R_{hs}^I(l, \boldsymbol{y}^s)$$

$$R_h^I(\pi_h, (g, \boldsymbol{y})) = \sum_{l \in \Omega^h} \pi_h(l) R_h^I(l, (g, \boldsymbol{y}))$$

侵入者は警備側の混合戦略 $(g, \boldsymbol{y}) = \{(g(s), \boldsymbol{y}^s), s \in \boldsymbol{S}\}$ を観測可能としているから，タイプ h の侵入者は，その被害量を最大にする $\max_{\pi_h} R_h^I(\pi_h, (g, \boldsymbol{y}))$ を実現する混合戦略 π_h をとるであろう．そのことを予想しつつ，侵入者のタイプについてはその分布 $f(h)$ しか知らない警備側は，$\sum_{h \in H} f(h) \max_{\pi_h} R_h^I(\pi_h, (g, \boldsymbol{y}))$ を最小化する混合戦略 $(g, \boldsymbol{y})$ を採用することが合理的である．かくして，各タイプの侵入者の最適戦略 $\{\pi_h, h \in \boldsymbol{H}\}$ と警備側の最適戦略 $(g, \boldsymbol{y})$ は次の期待支払に対するミニマックス最適化問題を解くことで得られる．

$$R^I(\pi, (g, \boldsymbol{y})) = \sum_{h \in H} f(h) \sum_{l \in \Omega^h} \pi_h(l) \sum_{s \in S} g(s) R_{hs}^I(l, \boldsymbol{y}^s)$$

詳細は省くが，ミニマックス最適化問題は 2 次計画問題に定式化され，市販の最適化ソルバーを使って解くことができる．

ゼロ和の警備ゲームへのモデリングでは，支払関数の妥当性に関する配慮も必要である．(5) 式では，侵入者は正の生残り数を得ることを唯一の侵入動機とする．しかしテロ犯の中には，全滅の事態を覚悟し自らの残存数に関する理論上の値が負となるにしても，その値を大きくすべく，小さな突破の可能性に賭ける強い侵入動機をもつ者がいるであろう．一方の警備側は，ある経路上を進む侵入者の残存数が負となる十分な警備が計画できれば，余った警備員をほかの経路の備えとして，弱みのない警備を目指すのが妥当である．そのような状況を表す適切な支払として，侵入者の残存数の正／負により被害率を変化させることが考えられるが，その場合の期待支払が次式である．

$$R^{II}(\pi, (g, \boldsymbol{y})) = \sum_{h \in H} f(h) \sum_{l \in \Omega^h} \pi_h(l) \sum_{e \in E_l} \max \left\{ \overline{d_e^h} \left(R_0^h - \sum_{s \in S} \sum_{e' \in E_l^e} \gamma_{e'}^{hs} g(s) y_{e'}^s \right), \underline{d_e^h} \left(R_0^h - \sum_{s \in S} \sum_{e' \in E_l^e} \gamma_{e'}^{hs} g(s) y_{e'}^s \right) \right\}$$

$\overline{d_e^h}$ および $\underline{d_e^h}$ は，全警備体制で平均を取った場合のアーク e 通過後の侵入者の期待残存数が正の場合および負の場合の被害率である．この期待支払に関するミニマックス最適化問題は線形計画問題に定式化できる．

最後に，後半のモデルを図 3 で描画した石垣空港 [23] の警備に適用した分析を紹介する．ネットワークのもつ 15 個のノードと 16 本のアークには番号を記載している．パラメータ設定に関しては十分に説明するスペースがないから，かいつまんだ説明となることをご容赦願いたい．侵入者には二つのタイプ $\boldsymbol{H} = \{1, 2\}$ がある．タイプ $h = 1$ の侵入者である密輸者は，2 階にある到着航空機の四つある降客ゲート（ノード 5, 6, 7, 8）から手荷物受取所（ノード 1）を抜けて中央出口（ノード 14）から空港ターミナルビルを出る四つの経路を選択肢としてもつ．タイプ $h = 2$ の侵入者であるテロ犯

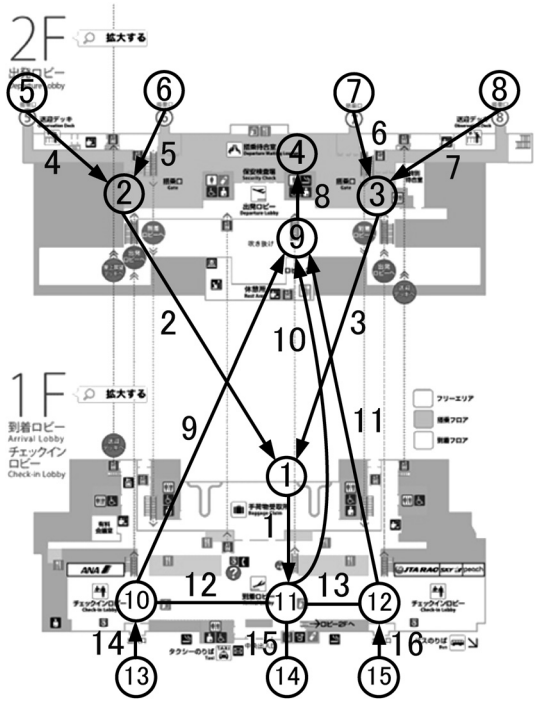

図 3　空港ターミナルの警備ネットワーク

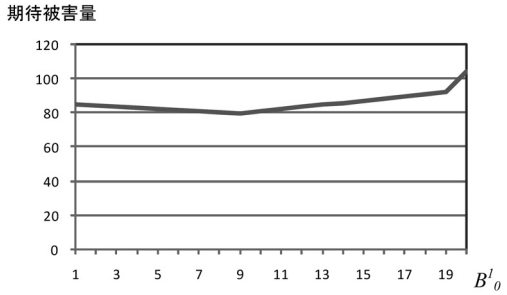

図 4　B_0^1 に対する期待被害量の変化

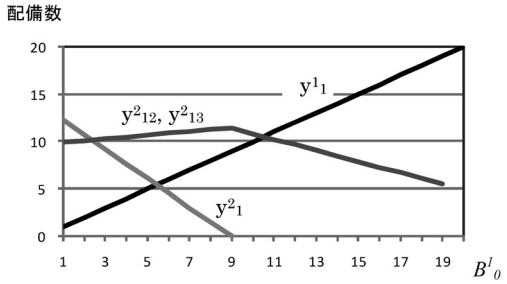

図 5　B_0^1 に対する警備配備数の変化

は，ターミナルビル 1 階の出入口（ノード 13, 14, 15）から侵入し，2 階にある搭乗待合室（ノード 4）で籠城する目的をもちつつ 9 本の経路を選択肢としてもち，その移動途中では多くの被害を出そうとしている．密輸者は，目的ノード 14 を出て初めて被害を与え，テロ犯は目的ノード 4 へ行く途中でも被害を与えるが，特に旅客の多い 1 階到着ロビーで大きな被害率を，2 階出発ロビーや搭乗待合室でも次に大きな被害率をもつ．また，侵入者タイプの分布は $f(1) = 0.8$, $f(2) = 0.2$ であり，侵入者の初期人数は $R_0^1 = 5$, $R_0^2 = 10$ である．

警備側は $\boldsymbol{S} = \{1, 2\}$ の 2 種類の警備体制をもつ．$s = 1$ は通常警備班である．$s = 2$ はテロ対策班であるが，使用頻度に上限 $U(2) = 0.3$ がある．γ_e^{hs} の設定では，通常警備班は密輸者に対しほどほどの阻止効果があり，手荷物受取所で最も大きな値をもつが，テロ犯に対してはほとんど無力である．テロ対策班 $s = 2$ のテロ犯に対する阻止効率 γ_e^{hs} としては，出発ロビーから搭乗待合室へ抜ける密閉区域では大きな値をもつが，到着ロビーのようなオープンな区画では小さい．

ここでは限られた総警備コストの下で，警備員数 B_0^1, B_0^2 の最適な配分を検討する．その際，警備体制 $s = 2$ は $s = 1$ の 2 倍のコストがかかるものとする．$g(s)$ は警備体制 s の使用頻度であるから，$C \equiv g(1)B_0^1 + 2g(2)B_0^2$ は 1 回の警備における平均警備コストを $s = 1$ の通常警備員数で表したものであり，この警備コストを固定しつつ B_0^1 を変化させ，ゲームの値（期待被害量）と最適警備配備量の変化を分析してみた．警備体制 $s = 2$ による阻止効率 γ_e^{hs} は $s = 1$ より十分大きいため，取り上げたケースではその上限使用率 $g(2) = 0.3$ でテロ対策班 $s = 2$ を配備させる結果となった．したがって，通常警備員数 B_0^1 に対し，テロ対策警備員数 B_0^2 は $(C - 0.7B_0^1)/(2 \cdot 0.3)$ で決まることになる．以下では，$C = 20$ の結果を掲載した．

図 4 および図 5 は，B_0^1 を変えた場合の期待被害量（ゲームの値）と最適な警備配備 y_e^s の変化を示したものである．図 4 には，被害量を最小にする最適警備体制の構成として，$s = 1$ と 2 の初動配備数を $B_0^1 = 9$, $B_0^2 = 22.8$ として共存させる最適な点が存在する．このような最適な警備数の構成比率の存在は，ほかの警備コスト C の例でも見られた．

図 5 の警備員配備計画に関しては，$s = 1$ の通常警備班員は，常に手荷物受取所のあるアーク 1 へ集中配備される．$s = 2$ のテロ対策班員は，通常警備班員数 B_0^1 が少ない場合にはその補完のため密輸者対処に充当されるが，B_0^1 が多くなってくると，テロ犯が最初に侵入し，かつ被害率の高いターミナル出入り口のアーク 12, 13 での対処が主任務となる．その他の警備コスト C の場合にあっても，(1) 通常警備班はテロ犯には効果が薄いため，常に密輸者対策に専従する．(2) テロ

対策班は，通常警備班員の少ない場合は密輸者対策の補完として使用されるが，通常警備班が多くなればテロ対策に専従する．その効果的な配備には，(i) 制圧効果 γ_e^{hs}，(ii) 被害率 d_e^h，および (iii) 早い段階でのテロ犯の制圧が考慮される．(3) 警備コストの制約下では，通常警備班とテロ対策警備班への割当人数には，バランスのとれた最適な構成比率が存在する．

5. おわりに

本稿では，全世界的なテロ事案発生により近年注目されている警備ゲームに関して，研究の経緯といくつかの代表的なモデルについて解説した．その多くは，ゲーム特有の概念を利用して，情報取得の点で優位にある侵入者に対し効果的に対応できるように，合理的にランダム化した警備計画を立案しようとするものである．この方向性に対し，さらに改善の要のある次の点に言及して，本解説を終わる．

一般のゲーム理論においては情報の価値についての研究が盛んである．この視点は警備に関してはさらに重要であり，何らかの事案が発生した後の侵入者情報を活用するモデルが必要である． 4 節で引用した最初の研究は情報取得を考えているが，単一タイプの侵入者のみを取り扱っており，もう一方の研究は侵入者タイプを考慮しているが，情報取得のないモデルである．警備ゲームにおいて情報の価値を分析することは，侵入者の発見・検知のための警備システムの設置場所などの具体的な対策を立てるうえでよい指針を与えてくれると思う．

参考文献

[1] 宝崎隆祐，“社会の安全とネットワーク阻止モデル，”オペレーションズ・リサーチ：経営の科学，**60**, pp. 266–273, 2015.

[2] J. Herrmann (ed.), *Handbook of Operations Research for Homeland Security*, Springer Science & Business Media, 2012.

[3] J. M. Chaiken and R. C. Larson, “Methods for allocating urban emergency units: A survey,” *Management Science*, **19**, pp. 110–130, 1972.

[4] D. G. Olson and G. P. Wright, “Models for allocating police preventive patrol effort,” *Operational Research Quarterly*, **26**, pp. 703–715, 1975.

[5] B. O. Koopman, “Search and screening,” Operations Evaluation Group Report No. 56, 1946.

[6] A. Garnaev, M. Baykal-Gursoy and H. V. Poor, “Incorporating attack-type uncertainty into network protection,” *IEEE Transactions on Information Forensics and Security*, **9**, pp. 1278–1287, 2014.

[7] R. Yang, C. Kiekintveld, F. Ordonez, M. Tambe and R. John, “Improving resource allocation strategies against human adversaries in security games: An extended study,” *Artificial Intelligence*, **195**, pp. 440–469, 2013.

[8] A. R. Washburn, “TPZS applications: Blotto games,” *Wiley Encyclopedia of Operations Research and Management Science*, **7**, pp. 5504–5511, 2011.

[9] N. Basilico, N. Gatti and F. Amigoni, “Patrolling security games: Definition and algorithms for solving large instances with single patroller and single intruder,” *Artificial Intelligence*, **184**, pp. 78–123, 2012.

[10] J. Tsai, Z. Yin, J. Y. Kwak, D. Kempe, C. Kiekintveld and M. Tambe, “Urban security: Game-theoretic resource allocation in networked physical domains,” In *Proceedings of the 24th AAAI Conference on Artificial Intelligence*, pp. 881–886, 2010.

[11] 岩下洋哲，大堀耕太郎，穴井宏和，“ゲーム理論に基づく警備リソース配分の最適化，”日本オペレーションズ・リサーチ学会 2015 年春季研究発表会アブストラクト集，pp. 4–5, 2015.

[12] 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.

[13] J. Pita, M. Jain, F. Ordonez, C. Portway, M. Tambe and C. Western, “Using game theory for Los Angeles airport security,” *AI Magazine*, pp. 43–57, 2009.

[14] M. Kodialam and T. V. Lakshman, “Detecting network intrusions via sampling: A game theoretical approach,” In *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications (IEEE INFOCOM)*, **3**, pp. 1880–1889, 2003.

[15] 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.

[16] 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.

[17] M. Tambe, *Security and Game Theory-Algorithms, Deployed Systems, Lessons Learned*, Cambridge University Press, 2012.

[18] 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.

[19] R. Hohzaki, S. Morita and Y. Terashima, “A patrol problem in a building by search theory,” In *Proceedings of 2013 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, pp. 104–111, 2013.

[20] 加藤直樹，瀧澤重志，“最速避難計画のモデリングと解法，”オペレーションズ・リサーチ：経営の科学，**60**, pp. 437–442, 2015.

[21] R. Hohzaki and T. Chiba, “An attrition game on an acyclic network,” *Journal of the Operational Research Society*, **66**, pp. 979–992, 2015.

[22] 宝崎隆祐，“警備問題へのゲーム理論応用とその周辺，”確率モデルシンポジウム報文集，pp. 141–150, 2015.

[23] 石垣空港ホームページ，http://www.ishigaki-airport.co.jp/facility.html（2015 年 12 月 1 日閲覧）