警備ゲームの動向

宝崎　隆祐

警備ゲームとは，警備問題，大きくはセキュリティ問題に対するゲーム理論応用であり，特に危害を与えようと意図する侵入者に対する警備側や防御側の有効な対策を議論するモデルである．本稿では，警備ゲームの従来研究について振り返り，今後の動向について考察する．

キーワード：警備，ゲーム，attack-defense，ネットワーク

1. はじめに

警備ゲームとは，警備問題，大きくはセキュリティ問題に対するゲーム理論応用であり，特に危害を与えようと意図する侵入者に対する警備側や防御側の有効な対策を議論するモデルである．本稿では，警備ゲームの従来研究について振り返り，最後に今後の動向について考察する．本誌2016年4月号に掲載された「ネットワークを考慮した警備ゲームのモデルあれこれ」[1]もあわせて読んでいただけると，警備ゲームに関する研究の進捗が把握できるかと思う．

2019年6月のサイエンス誌オンライン版に掲載された記事[2]は，各国市民の公徳心に関する世界規模の社会実験を紹介したもので，対象とした場所が40カ国，355都市におよび総経費60万ドル（約6400万円）であったことは類を見ない．この実験は，これまでにもローカルな試みとしてはお馴染みの「財布の落とし物のどれだけが届けられるか？」の世界版である．概要を述べると，お金の入っていない財布と13.45ドル（約1,400円）相当が入った財布の届出率を比較すると，平均で前者が40%であったのに対し後者が51%と増加し，さらに3カ国で金額を94.15ドル（約1万100円）と高額にするとさらに72%に跳ね上がった．届出率はその国の汚職率，脱税率に相関があるため，国ごとに異なるものの，40カ国中38カ国で見られた“財布の金額が上がると届出率が上昇した”事実は，事前の専門家による予想を裏切るもので（的中率は29%），実験チームは「人は自分を盗っ人と考えることを避けたがり，また落とし主に対する利他主義からこのような行動を取る」と結論づけている．

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
hozaki@nda.ac.jp

一般市民の公徳心や良心に関するこのような肯定的な結果と関連して，1980～90年代に流行った**割れ窓理論**[3]をご存じの方も多いかと思う．これは，建物の窓が割れたままに放置されていると，それが軽微な犯罪への公権力の無関心さを人々に生起させ，その地域での犯罪を助長するとされる考え方で，逆に言えば，軽微な犯罪も見逃すことなく取り締まることで凶悪犯罪を抑止できるとする環境犯罪学の理論である．この理論を応用する形で，それまで犯罪多発都市であったニューヨークで1994年に市長となったルドフル・ジュリアーニは，警察職員を増員し，落書き，万引き，違法駐車や無賃乗車といった軽微な犯罪を徹底的に取り締まることで，5年間で殺人件数を67.5%，強盗を54.2%減少させ，ニューヨークの治安を回復させた．

さて，初期のORも，このように市民の公徳心が犯罪抑止や犯罪被害の程度に大いに影響を与える市井の警備問題を扱っている．Chaiken and Larson [4]は，警察，消防，救急などの緊急出動チームの配備や巡回計画に関するOR応用として68編の研究を解説している．また，Olson and Wright [5]は，米国シカゴの高犯罪発生率地域への警察出動件数から，都市型犯罪の発見率を高める巡回経路決定をマルコフ決定問題として論じている．1970年代に行われたこれらの研究や環境犯罪学の視点からのフィールドワークをもとに，1980年代には上記のWilson and Kellingによる割れ窓理論が提案されることになる．

2. テロ対策の国際標準化とAttack-defenseゲーム

2001年9月11日の米国で発生した同時多発テロは，それまで国ごとに異なるとされ，その実情に沿って行われてきたセキュリティ対策を一気に国際標準で議論する契機となった．当事国の米国は，テロ行為の予防や狙われる組織の脆弱性の低減，生じた被害の局限と

復旧を目的とした U.S. Policy of Homeland Security 法案を 2002 年に制定している [6]．この時期から，テロ対策や警備問題に対する OR 応用研究も加速する．一般市民も犯罪を犯しうるグレーゾーンを扱ったかっての OR 問題から，テロ犯のように，自らの目的と利益を明確に意識する確信犯に備える問題を扱うように近年の警備ゲームは変遷してきている．

警備体制における具体的な要員配備や警備巡回路の設定のほか，危険人物の移動経路も考えようとすれば，ネットワークで表現した道路網や施設構造の参照が必要となるから，警備ゲームは，大きくはネットワーク上で危険な対象者，対象物を阻止するモデル群である**ネットワーク阻止モデル** [7] の一分野である．ネットワーク阻止モデルも，長い研究の歴史とさまざまな適用分野をもっている．

警備ゲームをネットワーク上でのモデルではなく，警備側とその対抗勢力という二つの勢力の攻防の分析ツールだとすれば，警備ゲームは **Attack-defense ゲーム**と呼ばれる分野の一モデルであるとも言える．この分野の最も古い問題は 1921 年に提案されたブロットー・ゲーム [8] で，米国西部開拓時代における複数の砦の争奪戦の物語において，より大人数の攻撃隊を派遣したほうが砦を奪取できるというシナリオのゲームとして発案された．ネットワーク阻止モデルとの重複も少なからずあるものの，このような価値ある目標の奪取を巡って二つの対抗勢力が抗争する Attack-defense ゲームの研究履歴を少したどってみよう，

Scaparra and Church [9] は，先手（リーダー）がノードにある施設をまず補強し，次に後手（フォロワー）がそれを観察して施設を攻撃するというシュタッケルベルグ・ゲームによる分析を行っている．Hausken [10, 11] は，複数目標の並列または直列，あるいはそれらの混成配置の抗担性に関する非ゼロ和のゲームである．Yang et al. [12] も Scaparra and Church の研究と同じく，複数目標の守備可能数が限られた制約下でどの目標を防護するかを先手である警備側が決め，後手である攻撃側は，確率的に防護目標を決定する警備側の守備計画を観測して，一つの目標へのアタックを決定するゲームである．

Basilico et al. [13] の問題では，警備側はある地域を巡回し，攻撃者は，警備側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いくつかのノードにある目標を攻撃するかどうか決めるが，攻撃中に警備側がやってくれば逮捕される．Baykal-Gursoy et al. [14] でも，攻撃側がノードを選択して破壊を加え，警備側はノードの調査，あるいはネットワーク上でパトロールを実施し，破壊によるダメージの減災に努めるというモデルである．Garnaev et al. [15] も同じネットワーク上での警備ゲームであるが，攻撃者に二つのタイプがあるとしており，ベイジアンゲームにより問題をモデル化している．

リーダーとフォロワーのあるシュタッケルベルグ型の警備ゲームの中には，Shieh et al. [16] のように，複数警備員の協調性に焦点を当て，分枝限定法による解法を提案しているものもある．Fang et al. [17] は防護対象である目標が移動する問題を初めて取り扱った研究で，問題を線形計画問題に定式化して均衡解を導出するヒューリスティックな解法を提案し，これをフェリー防護問題に適用している．

警備ゲームを，情報通信ネットワークや電力グリッド，道路網，鉄道網といった特殊であるが重要なインフラに適用した研究もある．Kodialam and Lakshman [18] は，情報通信網へのマルウェアの侵入を検査予算内で効果的に探知するためのデータパケットのサンプリング問題を議論している．Salmeron et al. [19] は，電力グリッド網の抗担性に焦点を当て，電力コストを最も悪化させるような破壊工作の対象となる機器を明らかにしている．Bell et al. [20] は，テロの脅威のある中での VIP 輸送における道路網の脆弱性分析である．Perea and Puerto [21] は，破壊工作に強い鉄道網の設計問題を取り扱っている．

警備ゲームで用いられる稀なモデルとして，微分ゲームを採用している研究もある．**微分ゲーム** [22] は，ゲームの支払に影響を与える何らかの状態変化を微分方程式で分析しようとするものである．Feichtinger [23] は，泥棒と警察との警備ゲームを，泥棒が盗難を働く頻度と警察が強制捜査を行う頻度を戦略として用いて，両者の関係を 2 本の非線形の微分方程式で定式化し，そのナッシュ均衡解を求めることで両戦略の関係を求めている．

3. 実システムへの指向

空港の警備計画にゲーム理論をもち込んだ次の研究は，警備ゲームを組み入れた実システムが実際に運用されているという点で大変今日的で注目すべき活動である．Paruchuri et al. [24] は，ロサンゼルス国際空港 (LAX) の警備システムである ARMOR (Assistant for randomized monitoring over routes) に内蔵されているゲームのソルバーである DOBSS (Decomposed optimal Bayesian Stackelberg solver) の求解アルゴ

リズムを解説したものである．そこでは，攻撃者は警備側の戦略を一部知ることができ，それを認識して警備側が合理的な警備戦略を立案するシュタッケルベルグ・ゲームを考え，警備側の最適戦略導出のための混合整数 2 次計画問題の定式化と，その厳密解を求める解法アルゴリズムが提案されている．ARMOR システムは，LAX における日々の検問設置や警備犬を使った巡回警備計画の立案に使用されている．Pita et al. [25, 26] はいずれも上記の ARMOR システムに関するものである．Jain et al. [27] や Tasi et al. [28] は，ARMOR システムのほかに，連邦航空保安局からの航空保安員の国際線への乗り込み政策にゲーム理論を使った IRIS (Intelligent randomization in scheduling) システムを解説している．そのほかの実システムとしては，連邦運輸保安局から 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) が使用されているが，これらのシステムの概要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 Shieh et al. [29] や Tambe [30] が解説している．Pita et al. [31] では，警備ゲームでよく使われるシュタッケルベルグ・ゲームのモデルに，フォロワーの限定合理性や限定的観察性により生じる最適行動からのずれを考慮し，そのモデルを LAX での空港警備に応用した多数の変形モデルを比較している．

警備ゲームの中には，国境警備における効果的な巡視を目的とした研究もある．**待伏せゲーム** は Ruckle [32] により提案されたゲームで，地理空間における移動者の移動経路とそれを遮断する静止遮蔽物の配置を議論したモデルであり，国境監視活動に役立つ．広域に広がる国境線の監視では，近年知能化が進む監視ロボットやドローンによる自動化が進むものと思われる．Agmon et al. [33] は，ある閉領域での横断者に対する複数ロボットによる自動警備監視をシュタッケルベルグ・ゲームとして考えている．この論文は，警備情報を得ることのできる横断者が最小化しようとする自らの発見確率を最大化するため，警備ロボットの巡視路の最適なランダム化を考えている．Agmon et al. [34] はその拡張モデルであり，フォロワーの知る情報内容をさまざまに変化させた場合の実験を通して，情報の内容が横断阻止に及ぼす影響を調べている．Basilico et al. [35] も自動警備の可能性を模索した研究である．Vanek et al. [36] は，監視者とそのパトロールエリアを横断しようとする横断者の 2 人ゼロ和ゲームであるが，その均衡解を海賊の出没する海域での安全航行に関するシミュレーションに適用して，導出された横断経路の有効性を証明している．

Agmon et al. のように警備の自動化を意図した研究として，森田ら [37] や Hohzaki et al. [38] がある．前者は，警備空間をネットワークで表現し，複数巡回路を選択肢にもつ警備側と複数侵入路を選択できる侵入者の間のゲームにより，脆弱性のない警備巡回路の選択法を提案をしている．前者を発展させた後者の研究では，侵入者の侵入経路決定問題を考えるとともに，日本の防空問題への応用例を示した．

都市全体やそれ以上の大きな地域の道路網を警備対象とした研究として，Tsai et al. [39], Jain et al. [40, 41] および Iwashita et al. [42] がある．これらの研究では取り扱う警備ネットワークが大規模であるがゆえに，計算アルゴリズムの高速化に関する種々の工夫が提案されている．

警備問題にも応用できる問題として，公共交通システムにおける効果的な検札問題がある．いくつかの国では，乗車券（チケット）がなくても乗車可能なシステムを取り入れている．その場合，運賃検査が実施され，チケットのない利用者には高額の罰金が科されることで，利用者の合法的行為が促される．Jiang et al. [43] や Yin et al. [44] では，列車の運行に合わせた時間空間ネットワークを考え，そのうえを列車に乗車して検査 (on-train inspection) する場合と，駅の出口で検査 (in-station inspection) する場合における検査チームの最適スケジュール戦略を，検査チームがリーダーで利用者がフォロワーであるゼロ和のシュタッケルベルグ・ゲームとして論じている．このゲームでは，チケット売り上げと罰金の総額である州の歳入を支払として採用し，ロサンゼルスの地下鉄を適用例と考えている．

最後に，テロ犯のように凶悪化する侵入者と警備側との衝突を想定して，警備ゲームの中に損耗のモデルを組み入れた研究として Hohzaki and Chiba [45], Hohzaki and Sunaga [46], Hohzaki and Higashio [47] および Hohzaki and Tanaka [48] の一連の研究を挙げておく．そこでは，警備ネットワーク上を移動する侵入者とその阻止を目指して配備された警備側の衝突によって双方に生じる被害に関しランチェスター損耗モデルの 1 次則や 2 次則を想定し，目的ノードへの侵入者の到達数を評価尺度としたゲームが論じられている．次節では，その拡張モデルとして，テロ犯や密輸者といっ

た複数タイプの侵入者に対し複数種の警備体制を敷く警備側の警備ゲーム [49, 50] を紹介する．そこでは，侵入者の性格を考慮した定式化がなされている．

4. 侵入者の性格を考慮した警備ゲーム

このモデルは次の特徴をもつ：(1) ネットワークで表現された施設内へ侵入しようとする侵入者と警備側が対峙する非ゼロ和のシュタッケルベルグ・ゲーム，(2) 犯罪者，密輸者やテロリストなど，侵入者にはさまざまなタイプが存在し，タイプによる自らの残存に関する嗜好を考慮，(3) 一般警備やテロ対策班など，警備側にも複数の警備体制が存在，(4) 侵入者はあらかじめ一部の警備情報を収集でき，警備体制の弱点を突ける，(5) 過去の事案発生から，侵入者タイプに関する確率分布は警備側に既知，(6) 警備空間での移動時間，防犯カメラによる侵入者情報の取得を考慮．

次が，基本モデルの詳細な前提である．

A1 警備空間はノード集合 $\boldsymbol{N}$ とアーク集合 $\boldsymbol{A}$ から成るネットワーク $G(\boldsymbol{N}, \boldsymbol{A})$ であり，プレイヤーは侵入者および警備側である．

A2 侵入者のタイプ集合を $\boldsymbol{H}$ とする．タイプ $h \in \boldsymbol{H}$ の侵入者は，その侵入ノードから初期の手勢 R_0^h で侵入し，目的ノードに向かう．途中ノード i で生き残ったタイプ h 侵入者は，1 人当たり物的・人的被害 d_i^h を施設側に与え，同時に 1 人当たり p_i^h の利益を得る．

タイプ h 侵入者の純粋戦略は，その侵入経路全体 Ω_h から 1 本のパスを選択することである．

A3 警備側はいくつかの警備体制をもつ．警備体制の集合を $\boldsymbol{S}$ とし，警備体制 $s \in \boldsymbol{S}$ の警備人数は B_0^s で，これをアーク，ノードおよび待機場所に配備し，侵入者の阻止を図る．なお，待機場所の集合を $\boldsymbol{W}$ で表す．警備体制 $s \in \boldsymbol{S}$ の予算制限から，その使用頻度 $g(s)$ に上限 $U(s)$ がある．ノード，アークへ事前に配備した人員は再配置できないが，待機人員は，防犯カメラからの侵入者情報を得てノード，アークへ派遣可能である．警備側は，侵入者タイプ h の発生確率分布 $\{f(h), h \in \boldsymbol{H}\}$ を知っている．

警備側の戦略は，体制 s の配備頻度 $g(s)$ と，人員数 B_0^s のノード，アーク，待機場所への配備計画および待機場所からの派遣計画の決定である．

A4 侵入者の移動時間と警備員派遣時間として次が計算できる：タイプ h の侵入者がパス l をとった場合，最初に通過する防犯カメラの設置ノードからその後のノード j までの移動時間 $\widehat{t}_{hl}^A(j)$ およびアーク e までの移動時間 $\widehat{t}_{hl}^A(e)$，体制 s の警備員が待機ノード $r \in \boldsymbol{W}$ からノード j あるいはアーク e に移動するための移動時間 $t_s^D(r,j)$ および $t_s^D(r,e)$．

A5 ノード i またはアーク e で，タイプ h の侵入者 x 人と体制 s の警備員 y 人の衝突により，侵入者の残存数は次の線形モデルに従う．

$$f_i^{hs}(x,y) = \max\{0,\ x - \gamma_i^{hs} y\} \tag{1}$$
$$f_e^{hs}(x,y) = \max\{0,\ x - \gamma_e^{hs} y\} \tag{2}$$

パラメータ $\gamma_i^{hs}, \gamma_e^{hs}$ は，ノード i またはアーク e での侵入者に対する警備側の強さを表す．

A6 侵入者は，警備体制 $s \in \boldsymbol{S}$ の使用頻度 $g(s)$ とその配備計画を知る．ただし，侵入実行時の警備体制については確信をもてない．

守備側は，カメラ設置ノードを通過した侵入者のタイプ h と侵入ルート情報をリアルタイムに入手でき，それに基づき待機要員を現場に派遣できる．

A7 警備側は施設被害を小さくしようとし，侵入者は自らの利益を大きくしようとする．

前提 A 2 における侵入者による時系列的な被害や利益の前提により，たとえば空港における密輸者が空港出口を出て初めて利益を得る状況や，目的場所までの移動途中でさまざまな人的・物的被害を与えるテロの状況を表現できる．また，前提 A 6 は侵入者の情報優位と先手，後手の状況を示す．

紙数の関係で，この非ゼロ和シュタッケルベルグ・ゲームの定式化や最適戦略の導出要領を詳細には解説できないが，まずプレイヤーの戦略を定義してゲームの支払を表す．

タイプ $h \in \boldsymbol{H}$ の侵入者の純粋戦略は全パス Ω_h から一つのパスを選択することであるが，その混合戦略をパス l の選択確率 $\pi_h(l)$ で表す．一方の警備側の戦略を，警備体制 $s \in \boldsymbol{S}$ をとる確率 $g(s)$ と総員 B_0^s のノード i，アーク e および待機場所 r への配備人数計画 $\boldsymbol{y}^s = \{\{y_i^s, i \in \boldsymbol{N}\}, \{y_e^s, e \in \boldsymbol{A}\}, \{y_r^s, r \in \boldsymbol{W}\}\}$ で表す．さらに警備側は，侵入者のタイプ h とパス l の情報を防犯カメラから得て，各待機場所 r からノード i，アーク e への派遣人数計画 $\boldsymbol{z}_l^{hs} = \{\{z_l^{hs}(r,i), i \in \boldsymbol{N}\}, \{z_l^{hs}(r,e), e \in \boldsymbol{A}\}, r \in \boldsymbol{W}\}$ を立てる．

さて，警備体制 s の配備計画 $\boldsymbol{y}^s$，$\boldsymbol{z}^{hs}$ に対し，パス l をとるタイプ h の侵入者により，パス上のノード $i \in \boldsymbol{V}_l$（$\boldsymbol{V}_l$ は l 上のノード集合）での正負を問わない侵入者残存数は，式 (1), (2) から次式で書ける．ただし V_l^i, E_l^i は，パス l 上にあるノード i までのノード集

合，アーク集合である．

$$D^{+}_{hsi}(l,(\boldsymbol{y}^s,\boldsymbol{z}^s)) = \max\{0,\ D_{hsi}(l,(\boldsymbol{y}^s,\boldsymbol{z}^s))\}$$
$$D_{hsi}(l,(\boldsymbol{y}^s,\boldsymbol{z}^s)) \equiv R^h_0 - \sum_{j\in V^i_l}\gamma^{hs}_j\left(y^s_j + \sum_{r\in W|\widehat{t}^A_{hl}(j)\geq t^D_s(r,j)} z^{hs}_l(r,j)\right) - \sum_{e\in E^i_l}\gamma^{hs}_e\left(y^s_e + \sum_{r\in W|\widehat{t}^A_{hl}(e)\geq t^D_s(r,e)} z^{hs}_l(r,e)\right)$$

$D_{hsi}(l,(\boldsymbol{y}^s,\boldsymbol{z}^s))$ の第 2 項はノード j への事前配備と待機所からの派遣員による損耗，第 3 項はアーク e における同様の損耗を示す．したがって，残存侵入者によるノード i での被害量と利益は次式で表される．

$$N_{hsi}(l,(\boldsymbol{y}^s,\boldsymbol{z}^s)) \equiv d^h_i D^{+}_{hsi}(l,(\boldsymbol{y}^s,\boldsymbol{z}^s)) \quad (3)$$
$$R_{hsi}(l,(\boldsymbol{y}^s,\boldsymbol{z}^s)) \equiv p^h_i D^{+}_{hsi}(l,(\boldsymbol{y}^s,\boldsymbol{z}^s)) \quad (4)$$

この各ノード i での被害量と利益をもとに，警備側の混合戦略 $g(s)$ や侵入者の混合戦略 $\pi_h(l)$，侵入者タイプの出現分布 $f(h)$ による期待値が計算できる．かくして，各タイプの侵入者は警備側戦略 $(g,\boldsymbol{y},\boldsymbol{z})$ を知って期待総利益を最大にする π_h をとり，警備側はそれを予想したうえで，期待総被害量を最小にする $(g,\boldsymbol{y},\boldsymbol{z})$ を決定することになるが，実際の手番の順序は逆であり，最初に $(g,\boldsymbol{y},\boldsymbol{z})$ が決定された後，それを知る各タイプ h の侵入者が混合戦略 π_h を最適化する．

式 (3) および式 (4) は，侵入者残存量 $D_{hsi}(l,(\boldsymbol{y}^s,\boldsymbol{z}^s))$ が負となる場合はゼロとなる．この値が理論どおりに負となるかどうかは実際には不確実であるものの，仮に負ならば侵入者の侵入動機は全く失せることになる．しかし，ある種のテロ犯は，テロの不成功を示す負の残存量を気にせずに，死に物狂いで侵入計画を実行しようとする強い侵入動機をもつ．彼らはいわば**負値無関心**な侵入者である．また，窃盗犯は，窃盗が成功する（正の残存量の）楽しみ以上に，逮捕されること（負の残存量）を嫌う**負値嫌い**な侵入者と言える．このような性格の特徴をモデルに組み入れるには，正の残存量に対する従来の利益率 p^h_i とは別に，負の残存量に対する利益率 $\underline{p^h_i}$ を次のように導入すればよい；(i) **負値無関心**：$\underline{p^h_i} < p^h_i$, (ii) **負値嫌い**：$\underline{p^h_i} > p^h_i$．なぜなら，ケース (i) では残存量の負による利得の減少幅は正による増加幅より大きくないから，残存数の負値（逮捕されること）に敏感ではなく，逆にケース (ii) では，残存量の負による利得の減少幅は大きいから，負になることに抵抗感がある，という侵入者の性格を表現できるからである．

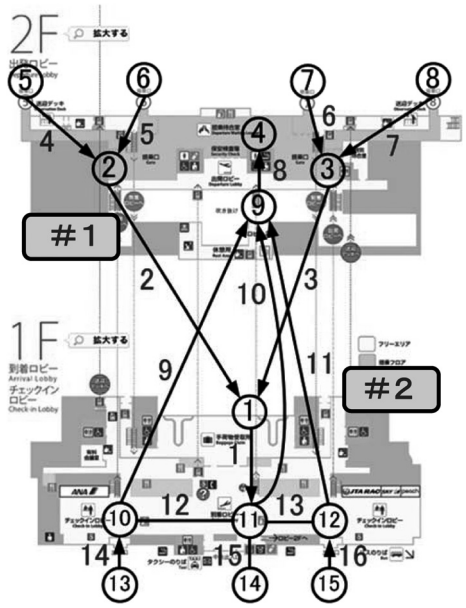

図 1　石垣空港ターミナルの警備ネットワーク
（図の著作権は石垣空港ターミナル（株）にある）

この非ゼロ和ゲームの均衡解導出のための，混合整数 2 次計画問題や工夫による混合整数線形計画問題への定式化については省略して，簡単な数値例により合理的な警備配備計画が得られることを示そう．

図 1 は，2 階建ての石垣空港ターミナル [51] 内に 15 個のノードと 16 本のアークの警備ネットワークを設定したものである．侵入者の一方向の移動しかないアークには矢印を付けてそれを示している．二つのタイプ $\boldsymbol{H}=\{1,2\}$ の侵入者のうち，タイプ 1 である $R^1_0=5$ 人の密輸者は，2 階の到着ゲートのノード 5〜8 から手荷物受取所のノード 1 を経て 1 階の空港出口のノード 14 に向かう 4 本のルートを，タイプ 2 であるテロ犯 $R^2_0=10$ 人は，空港入口のノード 13, 14, 15 から侵入し 2 階の搭乗待合室であるノード 4 での籠城を企図する 9 本のルートをもつ．両タイプの侵入者の発生比率は $f(1)=0.8$, $f(2)=0.2$ であり，密輸者はターミナルを出て初めて被害と利益を発生させるが，テロ犯は移動途中においても比較的大きな被害，利益を生じさせる．ここで密輸者は ‘負値嫌い’ であり，テロ犯については ‘負値無関心’ と ‘負値嫌い’ の両方の性格を考える．残念ながら，これらのパラメータ p^h_i, $\underline{p^h_i}$, d^h_i, $\underline{d^h_i}$ を掲載する余白はない．

警備側は，通常警備班 $s=1$ とテロ対策班 $s=2$ の 2 種類の警備体制 $\boldsymbol{S}=\{1,2\}$ それぞれの要員数 $B^1_0=20$, $B^2_0=60$ をもつ．その名のとおり，通常警備班は密輸者の取締りには有効であるが，テロ対策

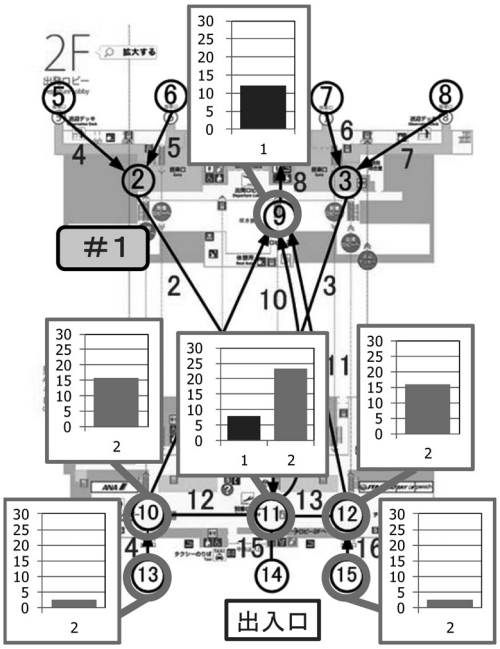

図2　負値無関心なテロ犯のいる最適警備員配備

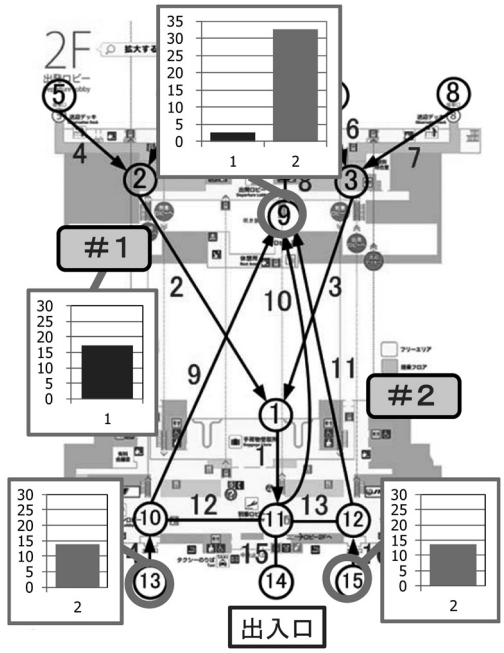

図3　負値嫌いなテロ犯のいる最適警備員配備

にはほぼ無力に近い．テロ対策班は両タイプの侵入者に抑止力があるものの警備費が高く，使用頻度に上限 $U(2) = 0.3$ をもつ．もちろん，対侵入者への有効性 γ_i^{hs}, γ_e^{hs} は場所にも依存するよう設定されている．ターミナル内には 2 カ所の警備員待機所 $\boldsymbol{W} = \{1, 2\}$ が 2 階と 1 階にあり，図 1 に#1, #2 の記号で示されている．ネットワーク上での警備員の派遣時間である $t_s^D(r, j)$, $t_s^D(r, e)$ は移動距離に比例して適切に設定されている．また，侵入者の移動時間である $\widehat{t}_{hl}^A(j)$, $\widehat{t}_{hl}^A(e)$ はカメラ設置ノードによるが，ここでは 2 台のカメラがノード 1, 11 に設置されていて，ここを通る侵入者情報しか警備側は得られない．

ここでテロ犯の性格の違いによる最適警備員配備を比較してみよう．どの場合もテロ犯への対処が優先され，警備体制 $s = 2$ は上限の $g(2) = U(2) = 0.3$ の頻度で配備される．したがって $g(1) = 0.7$ である．警備員の配備地点として侵入ルートの交わるノードがアークより重要である．図 2 に，‘負値無関心’ なテロ犯が想定される場合の各ノード，待機場所への配備人数 y_i^s, y_r^s が下部に $s = 1, 2$ の別が書かれた棒グラフで示されている．図 3 は ‘負値嫌い’ なテロ犯の場合である．

‘負値無関心’ なテロ犯は大きな被害が期待できる場所（特に被害率の大きな 1 階の到着ロビー）をうろついて被害を大きくしようとし，‘負値嫌い’ なテロ犯は自らの損耗を嫌って，警備側との衝突を避けながら，目的地である搭乗待合室のノード 4 に着こうとする傾向にある．したがって，前者の期待総被害量は 73，後者は 49 となり大きな差が生まれる．被害はすべてテロに起因し，密輸者は完全に制圧される．両ケースの最適配備の特徴は次のとおりである．

テロ犯が負値無関心な場合

(1) 一部の侵入経路しか視認できないので，警備員は待機させず，侵入経路の集まる 1 階ロビーの重要ノード 10, 11, 12 および 13, 15 へ前進配備し，早い段階での被害局限を目指す水際作戦をとる．(2) その効果はあまり期待できないものの，通常警備班員をノード 9 へ後退配備してテロ犯に備える．

テロ犯が負値嫌いな場合

(1) カメラ情報を得られないルートをとるテロ犯に備え，ノード 13 と 15 での水際作戦を実施する．(2) 目的ノード 4 への到着を急ぐテロ犯への対処のため，多くの警備員をノード 9 へ後退配備させ食い止める．(3) 通常警備班員の大多数は#1 に待機させ，主に密輸者発見に備える．

5. おわりに

本稿では，OR の分野でも近年研究が盛んな警備ゲームに関して，従来研究の概要と筆者たちのモデルについて解説した．一時は欧米各国で頻発した凶悪なテロ事案は，その対策により徐々に少なくなっているとは

いえ，原因となっている宗教間対立や移民問題での摩擦は解消されおらず，時に触れ発生する可能性がある．日本でも 2020 年の東京オリンピックに向けた警備体制の準備がなされているが，その際必要なのは，侵入者の真の意図を考慮した現実的で効率的な警備体制である．単なる重厚な警備体制では，その場限りの多大な警備コストを要するだけであり，ビックイベントに対し将来にわたって持続可能な警備を立案するには，侵入者の動機を刺激する警備上の弱点を補強するスリムな警備体制の立案システムが必要である．また，AI やロボットを用いた警備の自動化も時代の趨勢であるが，海外での実システムの稼働状況を見るに，これらのためのツール開発に警備ゲームが大いに寄与できそうである．

参考文献

[1] 宝崎隆祐，“ネットワークを考慮した警備ゲームのモデルあれこれ，”オペレーションズ・リサーチ：経営の化学，**61**(4), pp. 226–233, 2016.

[2] A. Cohn, M. A. Maréchal, D. Tannenbaum and C. L. Zünd, “Civil honesty around the globe,” *Science*, **365**, pp. 70–73, 2019.

[3] J. Q. Wilson and G. L. Kelling, “Broken windows: The police and neighborhood safety,” *The Atlantic Monthly*, **249**, pp. 29–38, 1982.

[4] J. M. Chaiken and R. C. Larson, “Methods for allocating urban emergency units: A survey,” *Management Science*, **19**, pp. 110–130, 1971.

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

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

[7] 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：経営の化学，**60**(5), pp. 266–273, 2015.

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

[9] 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.

[10] K. Hausken, “Defense and attack of complex and dependent systems,” *Reliability Engineering and System Safety*, **95**, pp. 29–42, 2010.

[11] K. Hausken, “Protecting complex infrastructures against multiple strategic attackers,” *International Journal of Systems Science*, **42**, pp. 11–29, 2011.

[12] 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.

[13] 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.

[14] M. Baykal-Gursoy, Z. Duan, H. V. Poor and A. Garnaev, “Infrastructure security game,” *European Journal of Operational Research*, **239**, pp. 469–478, 2014.

[15] 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.

[16] E. Shieh, M. Jain, A. X. Jiang and M. Tambe, “Efficiently solving joint activity based security games,” In *Proceedings of the Twenty-Third international Joint Conference on Artificial Intelligence*, pp. 346–352, 2013.

[17] F. Fang, A. X. Jiang and M. Tambe, “Optimal patrol strategy for protecting moving targets with multiple mobile resources,” In *Proceedings of the 2013 International Conference on Autonomous Agents and Multi-agent Systems*, pp. 957–964, 2013.

[18] 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*, **3**, pp. 1880–1889, 2003.

[19] 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.

[20] 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.

[21] 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.

[22] R. Isaacs, *Differential Games*, John Wiley & Son, 1965.

[23] G. Feichtinger, “A differential games solution to a model of competition between a thief and the police,” *Management Science*, **29**, pp. 686–699, 1983.

[24] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez and S. Kraus, “Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games,” In *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems*, pp. 895–902, 2008.

[25] J. Pita, M. Jain, J. Marecki, F. Ordonez, C. Portway, M. Tambe, C. Western, P. Paruchuri and S. Kraus, “Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles International Airport,” In *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems*, pp. 125–132, 2008.

[26] J. Pita, M. Jain, F. Ordonez, C. Portway, M. Tambe, C. Western, P. Paruchuri and S. Kraus, “Using game theory for Los Angeles airport security,” *AI Magazine*, **30**, pp. 43–57, 2009.

[27] M. Jain, J. Tsai, J. Pita, C. Kiekintveld, S. Rathi, M. Tambe and F. Ordonez, “Software assistants for randomized patrol planning for the LAX airport police and the federal air marshal service,” *Interfaces*, **40**, pp. 267–290, 2010.

[28] J. Tsai, C. Kiekintveld, F. Ordonez, M. Tambe and S. Rathi, "IRIS-a tool for strategic security allocation in transportation networks," In *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems*, pp. 881–886, 2009.
[29] E. Shieh, B. An, R. Yang, M. Tambe, C. Baldwin, J. DiRenzo, B. Maule and G. Meyer. "PROPTECT: A deployed game theoretic system to protect the ports of the united states," In *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems*, **1**, pp. 13–20, 2012.
[30] M. Tambe, *Security and Game Theory-Algorithms, Deployed Systems, Lessons Learned*, Cambridge University Press, 2012.
[31] J. Pita, M. Jain, M. Tambe, F. Ordenez and S. Kraus, "Robust solutions to Stackelberg games: Addressing bounded rationality and limited observations in human cognition," *Artificial Intelligence*, **174**, pp. 1142–1171, 2010.
[32] W. H. Ruckle, *Geometric Games and Their Applications*, Pitman, 1983.
[33] N. Agmon, S. Kraus and G. A. Kaminka, "Multi-robot perimeter patrol in adversarial settings," In *Proceedings of IEEE International Conference on Robotics and Automation*, pp. 2339–2345, 2008.
[34] N. Agmon, V. Sadov, G. A. Kaminka and S. Kraus, "The impact of adversarial knowledge on adversarial planning in perimeter patrol," In *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent System*, pp. 55–62, 2008.
[35] N. Basilico, N. Gatti and F. Amigoni, "Leader-follower strategies for robotic patrolling in environments with arbitrary topologies," In *Proceedings of the International Conference on Autonomous Agents and Multiagent System*, pp. 57–64, 2009.
[36] O. Vanek, B. Bosansky, M. Jakob and M. Pechoucek, "Transiting areas patrolled by a mobile adversary," In *Proceedinsg of the 2010 IEEE Symposium on Computational Intelligence and Games*, pp. 9–16, 2010.
[37] 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.
[38] 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*, pp. 104–111, 2013.
[39] 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.
[40] M. Jain, D. Korzhyk, O. Vanek, V. Conitzer, M. Pechoucek and M. Tambe, "A double-oracle algorithm for zero-sum security games on graphs," In *Proceedings of the International Conference on Autonomous Agents and Multiagent System*, pp. 327–334, 2011.
[41] M. Jain, V. Conitzer and M. Tambe, "Security scheduling for real-world networks," In *Proceedings of the International Conference on Autonomous Agents and Multiagent System*, pp. 215–222, 2013.
[42] H. Iwashita, K. Ohori, H. Anai and A. Iwasaki, "Simplifying urban network security games with cut-based graph contraction," In *Proceedings of the International Conference on Autonomous Agents and Multiagent System*, pp. 205–213, 2016.
[43] A. X. Jiang, Z. Yin, M. P. Johnson, M. Tambe, C. Kiekintveld, K. Leyton-Brown and T. Sandholm, "Towards optimal patrol strategies for fare inspection in transit Systems," Technical Report of 2012 AAAI Spring Symposium Series, pp. 31–36, 2012.
[44] Z. Yin, A. X. Jiang, M. Tambe, C. Kiekintveld, K. Leyton-Brown, T. Sandholm and J. P. Sullivan, "TRUSTS: Scheduling randomized patrols for fare inspection in transit systems using game theory," *AI Magazine*, **33**, pp. 59–72, 2012.
[45] R. Hohzaki and T. Chiba, "An attrition game on an acyclic network," *Journal of the Operational Research Society*, **66**, pp. 979–992, 2015.
[46] R. Hohzaki and K. Sunaga, "Attrition game models with asymmetric information on a network," *Journal of the Operations Research Society of Japan*, **59**, pp. 195–217, 2016.
[47] R. Hohzaki and T. Higashio, "An attrition game on a network ruled by Lanchester's square law," *Journal of the Operational Research Society*, **67**, pp. 691–707, 2016.
[48] R. Hohzaki and M. Tanaka, "Effects of a player's awareness of information acquisition and ability to change strategy in attrition games," *Journal of the Operations Research Society of Japan*, **60**, pp. 353–378, 2017.
[49] R. Hohzaki and G. Sakai, "Security games taking account of invasion routes and attrition," *Journal of the Operations Research Society of Japan*, **60**, pp. 156–177, 2017.
[50] 宝崎隆祐，"侵入者の性格を考慮した非ゼロ和警備ゲーム，" 日本オペレーションズ・リサーチ学会 2017 年秋季研究発表会アブストラクト集，pp. 36–37, 2017.
[51] 石垣空港ホームページ，http://www.ishigaki-airport.co.jp/en/facility.html （2019 年 7 月 10 日閲覧）