

<研究ノート>

警備ゲームの大規模ネットワークへの現実的適用

宝崎 隆祐*

A Realistic Application of the Security Game to Large-Size Networks

Ryusuke HOHZAKI*

抄 録

ここでは、施設の警備空間ネットワークにおける侵入者と警備側の警備問題をシュタッケルベルグ・ゲームにより議論し、両プレイヤーの合理的な戦略を導出する。このモデルでは、侵入者は警備側情報の一部を知ることができ、密輸者やテロ犯といった様々なタイプをもつことで、施設に与える被害や警備側に対する頑強さ、捕まることに対する嗜好といった特徴が考慮されている。警備側も一般警備やテロ対策といった複数タイプの警備体制を採用でき、さらには侵入情報を得た後の警備員の現場への派遣など、現実的な要素を加味したモデルとなっている。侵入者は施設への侵入経路を決め、警備側は警備体制の選択、施設内での警備員配備計画及び侵入事案発生時の現場への派遣計画を立案する。このゲームの均衡解を導出する2次計画問題による従来の定式化に対し、この報告では線形計画問題による定式化を提案することで、実用的な計算時間で現実的な施設警備計画が求められることを検証している。

キーワード: ゲーム理論、警備ゲーム、損耗、ネットワーク阻止

1. はじめに

この報告は施設警備へのゲーム理論応用に関する我々の一連の研究^{1, 24, 25)}を拡張し、そこで提案していた解法を大規模な警備空間にも応用できるように改善したものである。

警備に対するゲーム理論応用モデルは警備ゲーム (security game) と呼ばれ、今日的な研究は2001年の9.11米国同時多発テロ事案を境に活発になった。9.11テロを契機に強化された米国の Homeland Security に関する政策は、その後の欧州でのテロ続発により欧米

にも波及し、セキュリティ問題は数理工学の学術分野でも大きなテーマとなっている²⁾。

数理工学のオペレーションズ・リサーチの分野では、9.11以前においても警察や消防、救急等の緊急支援システムに関するモデル研究が1960年代から始まっており、Chaiken and Larson³⁾はそのような約70編ほどの研究を紹介している。Olson and Wright⁴⁾も、米国シカゴの犯罪発生率を下げるためのマルコフ決定を用いた議論を行っている。これらの試みが、落書きや万引き、違法駐車といった軽微な犯罪防止への小さな努力によりその

* 筑波学院大学経営情報学部、Tsukuba Gakuin University

地域での重犯罪がある程度抑止できるとする、いわゆる『割れ窓理論』と呼ばれる環境犯罪学の視点を醸成し、1990年代におけるニューヨークでの犯罪率低減に役立った⁵⁾。

米国における9.11テロ以降は、テロ犯等の非合法活動者の動機を科学的に取り扱うため、警備問題にゲーム理論を適用した警備ゲームに関する多くの研究がなされた。ここでは、施設や価値あるシステムに非合法活動を仕掛ける攻撃者とそれを防衛する防衛者にプレイヤーを代表させた **Attacker-and-Defender** ゲームと呼ばれる研究分野が作られた。その初期モデルとして、先手である防衛者がまず施設を補強し、次に後手である攻撃者がそれを観察して施設への攻撃を行うシュタッケルベルグ・ゲームによる分析を行った **Scaparra and Church**⁶⁾ や **Yang et al.**⁷⁾、並列及び直列に配列された複数目標物の信頼性をめぐる非ゼロ和ゲームを扱った **Hausken**^{8,9)} が挙げられる。

ネットワーク上でプレイさせる **Attacker-and-Defender** ゲームをネットワーク阻止モデルと呼ぶこともある^{10,11)}。**Basilico et al.**¹²⁾ は、地理ネットワーク上を巡回する防衛者と、防衛者の現在位置を観測しつつ、ネットワーク上を移動して各所に位置する目標物を時間を掛けて攻撃する攻撃者との駆け引きを分析した。**Baykal-Gursoy et al.**¹³⁾ は、ネットワーク上で、ノードを破壊する攻撃者とパトロールしつつノードの状況を調査して減災に努める防衛者のモデルである。**Garnaev et al.**¹⁴⁾ は2タイプの攻撃者を考えたネットワーク上での警備ゲームに関し、そのベイジアン均衡解を求めている。

Attacker-and-Defender ゲームを情報通信網や電力網、道路網、鉄道網、航空網といった重要なインフラ防衛に適用した研究もある。**Kodialam and Lakshman**¹⁵⁾ は、コンピュータマルウェア対策としての情報通信網におけ

るデータパケットの検査法について議論した。テロ工作に対する電力網の抗担性を高めるためのシュタッケルベルグ・ゲーム型のモデルを考えたのが、**Salmeron et al.**¹⁶⁾ である。道路網及び鉄道網の防衛策を応用例としたのが、それぞれ **Bell et al.**¹⁷⁾ 及び **Perea and Puerto**¹⁸⁾ である。

Attacker-and-Defender ゲームの研究が実際のシステムで実用化された例が、**Paruchuri et al.**¹⁹⁾ である。彼らは、ロサンゼルス国際空港における警備犬を用いた巡回警備や空港周辺の車の検問設置の計画を担う **ARMOR** と呼ばれるシステムにゲーム理論による解法アルゴリズムを組み込んだ。**Jain et al.**²⁰⁾ には、米国連邦航空保安局からの航空保安員の国際線航空機への乗り込み計画立案にゲーム理論を応用した **IRIS** システムが紹介されている。このような公的機関におけるテロ対策の実例として、400カ所以上の空港への連邦運輸保安局保安要員の配備システムである **GUARDS** や、沿岸警備隊のシステムである **PROTECT** におけるゲーム理論応用の詳細を解説しているのが **Tambe**²¹⁾ である。

以上のような警備ゲームに関し、当時の日本で盛んになりつつあったロボット技術を活用して警備の自動化に資するべく、著者達は **Morita et al.**²²⁾ や **Hohzaki et al.**²³⁾ において、施設警備に関するゲーム理論応用の研究を行った。施設内の警備空間をネットワークで一般的に表現し、複数警備巡回路の脆弱性を複数侵入路を通る侵入者の発見確率により予想し、この発見確率を支払関数としたゲーム問題を解くことにより、合理的な巡回路選択と警備ロボットのセンサー制御を提案した。警備ゲームにおいて攻撃者と防衛者の間で発生する損耗現象を明示的に取り入れた最初のモデルが **Hohzaki and Sakai**¹⁾ である。それは、攻撃側が施設被害をできるだけ大きく、防衛側がこれを小さくする2人ゼロ和ゲームのモデルであった。このモデルの支払いを非

ゼロ和とすることで、両プレイヤーの評価尺度の差異を考慮したのが宝崎²⁴⁾であり、攻撃側の性格を考慮できるモデルとしたのが宝崎²⁵⁾である。いずれもそのアイデアをモデルとして作成し、定式化によりゲームの均衡解の導出法を提示したが、最終的な定式化は2次計画問題となっており、現実問題への適用性の確認はされていない。そこでこの報告では、問題の解法を線形計画問題へ定式化し、均衡解導出が実用的な計算時間内に収まることを現実的な数値例で検証した。

次節2節では、取り扱う警備ゲームのモデルを厳密に記述する。3節ではプレイヤーのタイプ別の特徴をモデルに組み込むパラメータ設定法を説明し、それに基づいて、4節では各プレイヤーの利得関数を導出する。5節では、これら2つの利得関数の最適化問題を解くことで警備ゲームの均衡解を求める線形計画問題による定式化を提案する。最後に6節では、現実の施設を用いた数値例により、以前の解法と提案解法との計算時間を比較することで、提案手法の優位性を検証する。

2. 警備ゲームのモデルとプレイヤーの戦略

ここでは、ある施設内空間内へ侵入しようとする侵入者と、それを阻止しようとする警備側との警備ゲームを考える。施設は、プレイヤーの可動領域を表すネットワークで表現する。空港における犯罪人や密輸者、テロリスト等のように侵入者には複数タイプがあり、警備体制にも通常警備やテロ対策チームのような複数タイプを考える。また、侵入者が一部の警備情報を知り得るとの状況下で、警備側を先手、侵入者を後手とするシュタツケルベルグ型の警備ゲームを考える。このモデルは宝崎²⁵⁾とほぼ同じである。

(A1) ノード集合 \mathbf{N} とアーク集合 \mathbf{A} から成る

ネットワーク $G(\mathbf{N}, \mathbf{A})$ を警備空間とする。このゲームのプレイヤーは、侵入者及び警備側である。

(A2) 侵入者には幾つかのタイプがあり、そのタイプ集合を \mathbf{H} とする。タイプ $h \in \mathbf{H}$ の侵入者は、その侵入ノードから初期の手勢 R_0^h でもって侵入し、その目的ノードへ進もうとする。タイプ h の侵入者が侵入途中のノード i に生き残って到着した場合、1人あたり物的・人的被害 d_i^h を施設側に与える。同時に、施設側被害とは別に、1人あたり p_i^h の利益を得る。

タイプ $h \in \mathbf{H}$ の侵入者は、目的地到達までの利益の和（総利益）を最大にすべく、侵入ノードから目的ノードに至る閉路の無い侵入経路全体 Ω_h から1本のパスを選択する。

(A3) 警備側にはネットワーク上に幾つかの待機場所をもち、その集合を \mathbf{W} で表す。警備側のもつ有限複数の警備体制の集合を \mathbf{S} で表す。警備側は警備体制 $s \in \mathbf{S}$ をとる頻度（確率） $g(s)$ を決める。警備体制 s では、初期の警備人数 B_0^s をノード、アーク及び待機場所に配備し、侵入者を阻止しようとする。ただし、人目に立つノード、アークへの配備人数は M^s 人を上限とし、残りの警備員は待機場所で待機する。また、警備レベルの高い体制は一般に負担が大きいので、警備体制 $g(s)$ の使用頻度にはその負担に応じた上限 $U(s)$ がある。

警備側は最初にノード、アークに配備した人員を再配備できないが、待機場所に待機させた人員は、侵入者の侵入事案が発生後その情報を得て、ノードやアークに急派できる。

警備側は、これまでの発生事案データから、侵入者タイプに関する発生確率分布 $\{f(h), h \in \mathbf{H}\}$ を知っているとする。 $f(h)$ は侵入者がタイプ h である確率である。

(A4) ネットワーク上をタイプ h の侵入者がパス l をとった場合の侵入口からノード j までの移動時間を $t_{hl}^A(j)$ 、侵入口からアーク e までの移動時間を $t_{hl}^A(e)$ で表す。一方のタイプ s の警備人の待機場所ノード $r \in \mathbf{W}$ からノード j までの移動時間を $t_s^D(r, j)$ 、アーク e までの移動時間を $t_s^D(r, e)$ で表す。

(A5) ノード $i \in \mathbf{N}$ 上での x 人の侵入者と y 人の警備員との衝突の結果生じる損耗は線形モデルに従うとする。線形モデルによる侵入者の残存人数 $f_i^{hs}(x, y)$ は、侵入者のタイプ h 及び警備体制 s に依存する次式で与えられ、負の値も許す。

$$f_i^{hs}(x, y) = x - \gamma_i^{hs} y$$

同じ状況におけるアーク $e \in \mathbf{A}$ 上での衝突による侵入者の残存人数 $f_e^{hs}(x, y)$ も、同様な次式で与えられる。

$$f_e^{hs}(x, y) = x - \gamma_e^{hs} y$$

係数 γ_i^{hs} , γ_e^{hs} は、ノード i 、アーク e における侵入者に対する警備側の相対的な強さを表し、これを戦力交換比と呼ぶ。

(A6) 侵入者は、事前の調査から、警備体制 $s \in \mathbf{S}$ における警備員配備とそれをとる確率 $g(s)$ を知り得るが、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持ってないとする。一方の警備側は、侵入事案が発生した

直後に侵入者のタイプ h とその経路を情報として入手でき、これを用いて待機場所に配備した警備員を派遣できる。

(A7) 警備側は侵入者による被害を最小化する警備計画を立て、侵入者は各タイプごとに自らの総利益を最大化するように侵入経路を決定する。

前提 (A2) における侵入者による時系列的な被害や利益に関するパラメータ設定により、侵入者のタイプに依存する様々な状況が考慮できる。また、前提 (A3) においては、警備体制ごとに準備される装備品や警備員の質や量といった警備資源が異なる。前提 (A5) において侵入者残存量が負の場合は、この値が侵入者に対する警備側の優位さの度合を表している。

以後この問題を非ゼロ和のシュタッケルベルグ・ゲームとして定式化してゆくが、まずプレイヤーの戦略を定義する。タイプ $h \in \mathbf{H}$ 侵入者の純粋戦略は、全パス Ω_h から 1 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。その実行可能性条件は次式で与えられる。

$$\sum_{l \in \Omega_h} \pi_h(l) = 1, \quad \pi_h(l) \geq 0, \quad l \in \Omega_h.$$

タイプ h 侵入者のこの混合戦略を $\pi_h = \{\pi_h(l), l \in \Omega_h\}$ で、全タイプの混合戦略を $\pi = \{\pi_h, h \in \mathbf{H}\}$ で表す。

一方の警備側は、警備体制 $s \in \mathbf{S}$ をとる確率 $g(s)$ とその総員 B_0^s の配備として、 $\mathbf{y}^s = \{\{y_i^s, i \in \mathbf{N}\}, \{y_e^s, e \in \mathbf{A}\}, \{y_r^s, r \in \mathbf{W}\}\}$ を計画する。 y_i^s , y_e^s , y_r^s は、それぞれノード i 、アーク e 及び待機ノード r への配備人数である。さらに、侵入事案発生直後に侵入者のタイプ h とそのパス l の情報を得て、各待機場所 r から各ノード i 、各アーク e への派遣人員数である $\mathbf{z}^{hs} = \{\{z_i^{hs}(r, i), r \in \mathbf{W}, i \in \mathbf{N}\}, \{z_e^{hs}(r, e), r \in \mathbf{W}, e \in \mathbf{A}\}\}$ の計画

も必要である。またこれらの集合体として、 $g = \{g(s), s \in \mathbf{S}\}$, $\mathbf{y} = \{\mathbf{y}^s, s \in \mathbf{S}\}$ や $\mathbf{z}^s = \{z_l^{hs}, l \in \Omega_h, h \in \mathbf{H}\}$, $\mathbf{z} = \{z^s, s \in \mathbf{S}\}$ といった表記も適宜用いるものとする。モデルの前提から、警備側戦略に関する実行可能性条件は次のように表される。

$$\sum_{s \in \mathbf{S}} g(s) = 1, \quad 0 \leq g(s) \leq U(s), \quad s \in \mathbf{S}$$

$$\sum_{i \in \mathbf{N}} y_i^s + \sum_{e \in \mathbf{A}} y_e^s + \sum_{r \in \mathbf{W}} y_r^s \leq B_0^s, \quad s \in \mathbf{S} \quad (1)$$

$$\sum_{i \in \mathbf{N}} y_i^s + \sum_{e \in \mathbf{A}} y_e^s \leq M^s, \quad s \in \mathbf{S} \quad (2)$$

$$\sum_{i \in \mathbf{N}} z_l^{hs}(r, i) + \sum_{e \in \mathbf{A}} z_l^{hs}(r, e) = y_r^s, \\ r \in \mathbf{W}, s \in \mathbf{S}, l \in \Omega_h, h \in \mathbf{H} \quad (3)$$

$$y_i^s, y_e^s, y_r^s, z_l^{hs}(r, i), z_l^{hs}(r, e) \geq 0, \quad i \in \mathbf{N}, \\ e \in \mathbf{A}, r \in \mathbf{W}, s \in \mathbf{S}, l \in \Omega_h, h \in \mathbf{H} \quad (4)$$

4節以降で、この警備ゲームの均衡解を導出する。侵入者側、警備側の戦略の組合せとして得られる均衡解では一方のプレイヤーだけが戦略を変更してもそのプレイヤーの利得が大きくなるため、均衡解により戦略変更の動機のないバランスのとれた状況が何かを知ることができる。

3. 警備側及び侵入者の特徴を考慮した被害率と利益率

現実の侵入事案における不確定要素を考えると、理論どおりに侵入者の残存量が正、あるいは負となったりはしない。そのような考慮の下、侵入者及び警備側の特徴を被害率 d_i^h と利益率 p_i^h の設定で表現できることを説明しよう。これは2節の仮定 (A2) のパラメータ設定における一例である。

(1) 警備の省力化

警備コストに関する現実的な要請は大きく、侵入者の阻止が予想できる場合には警備を省力化することが求められる。こ

れは、定式化において侵入者の残存量が負であるノード i では、その被害率 d_i^h を正の場合の被害率 d_i^h よりも小さく設定することで対処できる。

(2) 侵入者の侵入動機の特徴

負の残存量は侵入者の侵入阻止を意味するから、窃盗犯のように、窃盗が成功する正の残存量の場合以上に負の残存量を嫌うような特徴付けがあり得る（負値嫌い）。一方、テロ犯のように負の残存量を気にすることなく侵入を執行しようとする（負値無関心な）侵入者もいる。両者の嗜好の特徴付けは利益率で表現することができる。「負値嫌い」のタイプ h では、残存量の負が期待されるノード i での利益率 \underline{p}_i^h を、正である場合の利益率 p_i^h より大きく設定する。すなわち $\underline{p}_i^h > p_i^h$ とし、「負値無関心」の侵入者には逆の設定 $\underline{p}_i^h < p_i^h$ とすればよい。

分かり易いように、警備側、侵入者側の上記の性格付けを与えるパラメータ設定法を次表で示したが、これらのプレイヤーを6節での数値例で使っている。

| 性格 | パラメータの設定法 |
|------------|-----------------------------|
| 省力化された警備体制 | $\underline{d}_i^h < d_i^h$ |
| 負値嫌いな侵入者 | $\underline{p}_i^h > p_i^h$ |
| 負値無関心な侵入者 | $\underline{p}_i^h < p_i^h$ |

上のプレイヤーの特徴を加味して、以下でモデルの定式化を行う。

4. モデルの定式化と利得関数

まず、各プレイヤーの利得を表す式を導出する。記号として、パス l 上のノード集合とアーク集合をそれぞれ \mathbf{V}_l 、 \mathbf{E}_l で表す。また、 \mathbf{V}_l^i を、パス l 上での出発ノードからノード i に到るまでに通過する i 自身を含むノード

集合、 E_l^i を、パス l 上での出発ノードからノード i に到るまでに通過するアーク集合とする。

タイプ h の侵入者がパス $l \in \Omega_h$ をとり、警備体制 s が配備計画 \mathbf{y}^s 、 \mathbf{z}^{hs} をとることにより、パス l 上のノード $i \in V_l$ での侵入者残存数は次式で書ける。

$$D_{hsi}(l, (\mathbf{y}^s, \mathbf{z}^s)) = R_0^h - \sum_{j \in V_l^i} \gamma_j^{hs} \left(y_j^s + \sum_{r \in W | t_{hl}^A(j) \geq t_s^D(r,j)} z_l^{hs}(r,j) - \sum_{e \in E_l^i} \gamma_e^{hs} \left(y_e^s + \sum_{r \in W | t_{hl}^A(e) \geq t_s^D(r,e)} z_l^{hs}(r,e) \right) \right)$$

第2項はノード j での事前配備と待機所からの派遣人数の総警備員数による損耗、第3項はアーク e における同様の損耗である。これを警備側混合戦略 g により期待値をとった期待残存数 $D_{hi}(l, (g, \mathbf{y}, \mathbf{z}))$ は次式で表される。

$$D_{hi}(l, (g, \mathbf{y}, \mathbf{z})) = \sum_{s \in S} g(s) D_{hsi}(l, (\mathbf{y}^s, \mathbf{z}^s)) = R_0^h - \sum_{s \in S} \sum_{j \in V_l^i} \gamma_j^{hs} \left(g(s) y_j^s + \sum_{r \in W | t_{hl}^A(j) \geq t_s^D(r,j)} g(s) z_l^{hs}(r,j) - \sum_{s \in S} \sum_{e \in E_l^i} \gamma_e^{hs} \left(g(s) y_e^s + \sum_{r \in W | t_{hl}^A(e) \geq t_s^D(r,e)} g(s) z_l^{hs}(r,e) \right) \right)$$

上式では変数 \mathbf{y} 、 \mathbf{z} は $g(s)$ と掛けられて使用されるから、 \mathbf{y} 、 \mathbf{z} の代わりに次の変数を用いるものとする。

$$x_i^s \equiv g(s) y_i^s, \quad x_e^s \equiv g(s) y_e^s, \quad x_r^s \equiv g(s) y_r^s, \\ v_l^{hs}(r, i) \equiv g(s) z_l^{hs}(r, i),$$

$$v_l^{hs}(r, e) \equiv g(s) z_l^{hs}(r, e)$$

これらの新しい変数を使うことにより、利得計算の基礎となる式 $D_{hi}(l, (g, \mathbf{y}, \mathbf{z}))$ は $g(s)$ を含まない次の式 $D_{hi}(l, (\mathbf{x}, \mathbf{v}))$ となる。

$$D_{hi}(l, (\mathbf{x}, \mathbf{v})) = R_0^h - \sum_{s \in S} \sum_{j \in V_l^i} \gamma_j^{hs} \left(x_j^s + \sum_{r \in W | t_{hl}^A(j) \geq t_s^D(r,j)} v_l^{hs}(r, j) - \sum_{s \in S} \sum_{e \in E_l^i} \gamma_e^{hs} \left(x_e^s + \sum_{r \in W | t_{hl}^A(e) \geq t_s^D(r,e)} v_l^{hs}(r, e) \right) \right)$$

さて、この新しい変数 \mathbf{x} 、 \mathbf{v} の実行可能性条件は、(1)、(2)、(3) 及び (4) 式に対応して次式で与えられる。

$$\sum_{i \in N} x_i^s + \sum_{e \in A} x_e^s + \sum_{r \in W} x_r^s \leq g(s) B_0^s, \quad s \in S \\ \sum_{i \in N} x_i^s + \sum_{e \in A} x_e^s \leq g(s) M^s, \quad s \in S \\ \sum_{i \in N} v_l^{hs}(r, i) + \sum_{e \in A} v_l^{hs}(r, e) = x_r^s, \\ r \in W, s \in S, l \in \Omega_h, h \in H \\ x_i^s, x_e^s, x_r^s, v_l^{hs}(r, i), v_l^{hs}(r, e) \geq 0, \quad i \in N, \\ e \in A, r \in W, s \in S, l \in \Omega_h, h \in H$$

逆に、非負の変数 \mathbf{x} 、 \mathbf{v} から条件 (1)-(4) を満たす元の非負変数 \mathbf{y} 、 \mathbf{z} も再構成できる。

さて、パス l 上のノード i での侵入者のこの期待残存数が正であれば d_i^h を、負であれば小さな被害率 d_i^h ($< d_i^h$) をとるとしたノード i での被害量は次式で表される。

$$N_{hi}(l, (\mathbf{x}, \mathbf{v})) = \max \left\{ \frac{d_i^h}{d_i^h} D_{hi}(l, (\mathbf{x}, \mathbf{v})), \frac{d_i^h}{d_i^h} D_{hi}(l, (\mathbf{x}, \mathbf{v})) \right\} \quad (5)$$

この式から、パス $l \in \Omega_h$ をとるタイプ h 侵入者による期待総被害は次式で与えられる。

$$N_h(l, (\mathbf{x}, \mathbf{v})) = \sum_{i \in V_l} N_{hi}(l, (\mathbf{x}, \mathbf{v}))$$

一方の侵入者の特徴に依存した利得率の変化に関しても、同様の表現が可能である。

$$(i) \text{ 負値嫌いなタイプ } h : \underline{p}_i^h > p_i^h \\ R_{hi}(l, (\mathbf{x}, \mathbf{v})) = \min \left\{ \frac{p_i^h}{\underline{p}_i^h} D_{hi}(l, (\mathbf{x}, \mathbf{v})), \right. \\ \left. p_i^h D_{hi}(l, (\mathbf{x}, \mathbf{v})) \right\}$$

$$(ii) \text{ 負値無関心なタイプ } h : \underline{p}_i^h < p_i^h \\ R_{hi}(l, (\mathbf{x}, \mathbf{v})) = \max \left\{ \frac{p_i^h}{\underline{p}_i^h} D_{hi}(l, (\mathbf{x}, \mathbf{v})), \right. \\ \left. p_i^h D_{hi}(l, (\mathbf{x}, \mathbf{v})) \right\}$$

これらの評価式から、タイプ h 侵入者のパス $l \in \Omega_h$ 上での期待総利益及び混合戦略 π_h による期待総利益は次式で与えられる。

$$R_h(l, (\mathbf{x}, \mathbf{v})) = \sum_{i \in V_i} R_{hi}(l, (\mathbf{x}, \mathbf{v}))$$

$$R_h(\pi_h, (\mathbf{x}, \mathbf{v})) = \sum_{l \in \Omega_h} \pi_h(l) R_h(l, (\mathbf{x}, \mathbf{v}))$$

警備計画 (\mathbf{x}, \mathbf{v}) の情報を得て、自らの利益を最大化しようとするタイプ h 侵入者は、次の問題を考えることになる。

$$(P_A) \\ \max_{\pi_h} R_h(\pi_h, (\mathbf{x}, \mathbf{v})) = \max_{l \in \Omega_h} R_h(l, (\mathbf{x}, \mathbf{v}))$$

この最適混合戦略を π_h^* 、あるいは右辺による最適パスを l_h^* とすれば、警備側の支払は、侵入者の出現確率 $f(h)$ を加味した次式で表される。

$$\sum_{h \in \mathbf{H}} f(h) \sum_{l \in \Omega_h} \pi_h^*(l) N_h(l, (\mathbf{x}, \mathbf{v})) \\ = \sum_{h \in \mathbf{H}} f(h) N_h(l_h^*, (\mathbf{x}, \mathbf{v}))$$

警備側はこのような侵入者側の最適反応を予想し、次の最小化問題を考えることで先手としての最適警備計画 $(\mathbf{x}^*, \mathbf{v}^*)$ を求めることになる。

$$(P_D) \min_{(\mathbf{x}, \mathbf{v})} \sum_{h \in \mathbf{H}} f(h) \sum_{l \in \Omega_h} \pi_h^*(l) N_h(l, (\mathbf{x}, \mathbf{v})) \\ = \min_{(\mathbf{x}, \mathbf{v})} \sum_{h \in \mathbf{H}} f(h) N_h(l_h^*, (\mathbf{x}, \mathbf{v}))$$

ここでのゲームは、警備側が先手で警備計画 (\mathbf{x}, \mathbf{v}) (あるいは $(g, \mathbf{y}, \mathbf{z})$) を決め、次に各タイプ h の侵入者がこの警備計画を知って問題 (P_A) を解こうとするシュタツケルベルグ・ゲームである。

5. 侵入者及び警備側の最適戦略

これまで述べたシュタツケルベルグ型ゲームを解くための定式化として、Paruchuri et al.¹⁹⁾ が利用できる。ただし、当該モデルでは、彼らのモデルと異なる次のような特徴があるため、解法の定式化には工夫を要する。(1) 後手である侵入者の戦略空間は一定でなく、そのタイプ h に依存して変化する。(2) 先手である警備側の戦略は、その混合戦略 $\{g(s), s \in S\}$ の他に配備計画 (\mathbf{y}, \mathbf{z}) があり、これらは離散変数でなく連続変数である。(3) プレイヤーの利得関数には $\max\{\}$ といった取り扱いの難しい演算が含まれている。定式化の工夫については解説する余白がないため、結果だけ述べると、次の2次混合整数計画問題に定式化される。

$$(P_D)$$

$$\min_{g, \mathbf{x}, \mathbf{v}, \pi, \eta, \alpha, \zeta, \xi} \sum_{h \in \mathbf{H}} f(h) \sum_{l \in \Omega_h} \pi_h(l) \sum_{i \in V_i} \eta_i^h$$

制約条件：

$$d_i^h D_{hi}(l, (\mathbf{x}, \mathbf{v})) \leq \eta_i^h, \\ i \in V_i, l \in \Omega_h, h \in \mathbf{H} \quad (6)$$

$$\underline{d}_i^h D_{hi}(l, (\mathbf{x}, \mathbf{v})) \leq \eta_i^h, \\ i \in V_i, l \in \Omega_h, h \in \mathbf{H} \quad (7)$$

$$\sum_{l \in \Omega_h} \pi_h(l) = 1, h \in \mathbf{H}$$

$$\pi_h(l) \in \{0, 1\}, l \in \Omega_h, h \in \mathbf{H}$$

$$0 \leq a_h - \sum_{i \in V_i} \zeta_i^h \leq (1 - \pi_h(l))M, \\ l \in \Omega_h, h \in \mathbf{H} \quad (8)$$

$$IT_h = 1 \text{ ならば, } 0 \leq \zeta_i^h - p_i^h D_{hi}(l, (\mathbf{x}, \mathbf{v}))$$

$$\leq (1 - \xi_{li}^h(1))M, i \in V_i, l \in \Omega_h, h \in \mathbf{H}$$

$$0 \leq \zeta_i^h - \underline{p}_i^h D_{hi}(l, (\mathbf{x}, \mathbf{v}))$$

$$\leq (1 - \xi_{li}^h(2))M, i \in V_i, l \in \Omega_h, h \in \mathbf{H}$$

$$IT_h = 2 \text{ ならば, } 0 \leq p_i^h D_{hi}(l, (\mathbf{x}, \mathbf{v})) - \zeta_i^h$$

$$\leq (1 - \xi_{li}^h(1))M, i \in V_i, l \in \Omega_h, h \in \mathbf{H}$$

$$0 \leq \underline{p}_i^h D_{hi}(l, (\mathbf{x}, \mathbf{v})) - \zeta_i^h$$

$$\leq (1 - \xi_{li}^h(2))M, i \in V_i, l \in \Omega_h, h \in \mathbf{H}$$

$$\begin{aligned} \xi_{li}^h(1) + \xi_{li}^h(2) &= 1, \quad i \in V_l, l \in \Omega_h, h \in \mathbf{H} \\ \xi_{li}^h(1), \xi_{li}^h(2) &\in \{0, 1\}, \quad i \in V_l, l \in \Omega_h, h \in \mathbf{H} \\ \xi_{li}^h(1) &\leq \xi_{lj}^h(1), \\ & \quad j \in V_l^i, i \in V_l, l \in \Omega_h, h \in \mathbf{H} \quad (9) \end{aligned}$$

$$\begin{aligned} \xi_{li}^h(2) &\leq \xi_{lj}^h(2), \\ & \quad j \notin V_l^i, j \in V_l, i \in V_l, l \in \Omega_h, h \in \mathbf{H} \quad (10) \end{aligned}$$

$$\begin{aligned} \sum_{s \in \mathbf{S}} g(s) &= 1 \\ 0 \leq g(s) &\leq U(s), \quad s \in \mathbf{S} \\ \sum_{i \in \mathbf{N}} x_i^s + \sum_{e \in \mathbf{A}} x_e^s + \sum_{r \in \mathbf{W}} x_r^s &\leq g(s)B_0^s, \quad s \in \mathbf{S} \\ \sum_{i \in \mathbf{N}} x_i^s + \sum_{e \in \mathbf{A}} x_e^s &\leq g(s)M^s, \quad s \in \mathbf{S} \\ \sum_{i \in \mathbf{N}} v_i^{hs}(r, i) + \sum_{e \in \mathbf{A}} v_i^{hs}(r, e) &= x_r^s, \\ & \quad r \in \mathbf{W}, s \in \mathbf{S}, l \in \Omega_h, h \in \mathbf{H} \\ x_i^s, x_e^s, x_r^s, v_i^{hs}(r, i), v_i^{hs}(r, e) &\geq 0, i \in \mathbf{N}, \\ & \quad e \in \mathbf{A}, r \in \mathbf{W}, s \in \mathbf{S}, l \in \Omega_h, h \in \mathbf{H} \end{aligned}$$

定式化の中の M はいわゆる“ビック M ”と呼ばれる十分大きな数字である。また、 $IT_h = 1$ 及び $IT_h = 2$ により、侵入者タイプ h が「負値無関心」か「負値嫌い」かを区別する。(6)、(7)の不等式と目的関数に関する最小化の結果、この問題が解かれた際には、変数 η_{li}^h は(5)式を与えることになる。

条件(9)は以下の知見を表す条件である。すなわち、 $\xi_{li}^h(1) = 1$ はノード i での侵入者残存量が正であることを示すが、この場合パス l 上をノード i 以前に通過しているノード j では必ず侵入者は残存しており、 $\xi_{lj}^h(1) = 1$ であるはずである。同様に、 $\xi_{li}^h(2) = 1$ はノード i での侵入者残存量が負であることを示すが、この場合はそれ以降のノード j でも残存量は負となり、 $\xi_{lj}^h(2) = 1$ であるはずである。このことを意味しているのが条件式(10)である。この条件により、この2次混合整数計画問題を解く際の分枝限定法が効率良く機能する。

さらに、次のように目的関数を線形にすることが可能である。後手である侵入者は

警備情報を得て侵入経路を選ぶことができるため、各 $h \in \mathbf{H}$ ではいずれか1本のパス $l \in \Omega_h$ が選択され $\pi_h(l) = 1$ となるから、目的関数に対しては、選択されたパス l に対してのみ $\sum_{i \in V_l} \eta_{li}^h$ が影響を与える。そこで、最終的にこの値となる変数 $b(h)$ を導入すれば、線形の混合整数計画問題に定式化できる。制約条件(11)は、 $\pi_h(l) = 1$ なるパス $l \in \Omega_h$ に関してのみ $\sum_{i \in V_l} \eta_{li}^h \leq b(h)$ なる制約を課すが、目的関数を最小化しようとするため、最終的には $b(h) = \sum_{i \in V_l} \eta_{li}^h$ となる。

$$(P_D^L) \quad \min_{g, x, v, \pi, \eta, a, \zeta, \xi, b} \sum_{h \in \mathbf{H}} f(h)b(h)$$

制約条件：

$$\begin{aligned} \sum_{i \in V_l} \eta_{li}^h - b(h) &\leq (1 - \pi_h(l))M, \\ & \quad l \in \Omega_h, h \in \mathbf{H} \quad (11) \end{aligned}$$

$$\begin{aligned} d_i^h D_{hi}(l, (\mathbf{x}, \mathbf{v})) &\leq \eta_{li}^h, \\ & \quad i \in V_l, l \in \Omega_h, h \in \mathbf{H} \end{aligned}$$

$$\begin{aligned} \underline{d}_i^h D_{hi}(l, (\mathbf{x}, \mathbf{v})) &\leq \eta_{li}^h, \\ & \quad i \in V_l, l \in \Omega_h, h \in \mathbf{H} \end{aligned}$$

$$\sum_{l \in \Omega_h} \pi_h(l) = 1, \quad h \in \mathbf{H}$$

$$\pi_h(l) \in \{0, 1\}, \quad l \in \Omega_h, h \in \mathbf{H}$$

以下、(8)式以下と同じであるため省略

6. 数値実験

ここでは前節で新たに提案した均衡解導出の線形計画問題による定式化(P_D^L)と従来の2次計画問題による定式化(P_D)の違いを、2つの施設に対する警備ゲームを解くことで比較する。1つ目の施設は図1にフロアマップとその上のネットワークで警備空間を示した沖縄県の石垣空港である。第2の施設は図2のキャンパスマップと道路ネットワークで示した神奈川県横須賀市にある防衛大学の敷地である。前者を小規模な警備空間、後者を大規模な警備空間として取り上げ、2つの解法による計算時間を計測する。

因みに、使用した計算機環境は PC Windows 7 professional, Intel(R) Xeon(R) CPU E5-1660 (3.30GHz) であり、5 節で提案した数理計画問題を解くための最適化ソルバーとして NTT データ・数理システムの NUOPT Ver.17.1.1 を使った。

2 節で述べたモデルには多数のパラメータが含まれており、それらをすべて記載することはスペースの関係で不可能であるため、警備ネットワーク $G(N, A)$ のサイズ、侵入者のタイプとそれぞれの侵入者数 R_0^i 、さらには警備側のタイプとそれぞれのタイプに割り当てられる警備員数 B_0^i のみを示す。また、すべてのパラメータが総合された結果として、計算時間に最も影響する 2 次計画問題 (P_D) と線形計画問題 (P_L^i) に含まれる変数と制約式の数を示し、均衡解導出の計算時間を 2 つの警備ネットワーク (石垣空港と防衛大学校) について計測したのが表 1 及び表 2 である。因みに、パラメータ R_0^i や B_0^i は定式化を構成する各式の係数を変えるものの、変数

や制約式の構成には影響を与えないため、変数の数や制約式の数は変わらない。

(ア) 石垣空港

- ・ネットワークサイズ： $|N|=15, |A|=16$
- ・侵入者のタイプ：密輸者 (T1)、テロ犯 (T2) の 2 種類
- ・警備側のタイプ：通常警備 (体制 1)、テロ対策班 (体制 2) の 2 種類

(イ) 防衛大学校

- ・ネットワークサイズ： $|N|=44, |A|=62$
- ・侵入者のタイプ：窃盗犯 (T1)、銃狙いのテロ犯 (T2)、立て籠りテロ犯 (T3) の 3 種類
- ・警備側のタイプ：通常警備 (体制 1)、戒支援 (体制 2)、テロ対策班 (体制 3) の 3 種類

表 1 及び表 2 から、2 つの解法について次のことが見て取れる。

- (1) どちらも 0-1 整数計画問題であるため、パラメータの値によって解き易さや解き難さが変化するため、計算時間は予測しがたい。したがって、線形計画が常に 2 次計画より計算が速いとは言えないものの、多くのケースにおいて線

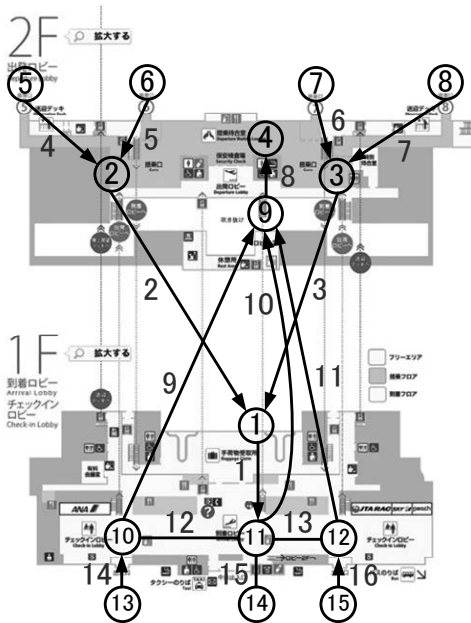


図 1 石垣空港の警備ネット
(注) 石垣空港ターミナル (株) WEB より



図 2 防衛大学校キャンパスの警備ネット
(注) google アースより

表 1 計算時間 (石垣空港)

| 侵入者 | | 警備体制 | | 2次計画 | 線形計画 | |
|---------|---------|---------|---------|----------|----------|-------|
| T1 | T2 | 体制1 | 体制2 | 変数の数、制約数 | 変数の数、制約数 | 比率 |
| R_0^1 | R_0^2 | B_0^1 | B_0^2 | 809,532本 | 811,737本 | |
| | | 10 | 72 | 44.2秒 | 1.7秒 | 0.038 |
| 5 | 10 | 20 | 60 | 7.9秒 | 2.7秒 | 0.342 |
| | | 30 | 48 | 4.7秒 | 2.1秒 | 0.447 |
| | | 40 | 37 | 1.4秒 | 1.7秒 | 1.214 |

表 2 計算時間 (防衛大学校)

| 侵入者 | | | 警備体制 | | | 2次計画 | 線形計画 | |
|---------|---------|---------|---------|---------|---------|------------|------------|---------|
| T1 | T2 | T3 | 体制1 | 体制2 | 体制3 | 変数の数、制約数 | 変数の数、制約数 | 比率 |
| R_0^1 | R_0^2 | R_0^3 | B_0^1 | B_0^2 | B_0^3 | 2338,1027本 | 2441,1618本 | |
| | | | 5 | 10 | 10 | 2.7秒 | 3.3秒 | 1.222 |
| 3 | 5 | 10 | 5 | 20 | 20 | 548.6秒 | 49.8秒 | 0.091 |
| | | | 5 | 30 | 30 | 10分以上 | 13.5秒 | 0.021以下 |

形計画の方が計算時間に関し優位である。

- (2) 警備ネットワークが石垣空港から防衛大学校となり、定式化における変数や制約式の数が2~3倍となった場合、2次計画による計算時間は指数関数的な増大を見せるが、それに比べると線形計画による計算時間はやや抑え気味となり、ここでの数値例では1分以内に均衡解を出す。
- (3) ノード数やアーク数から、防衛大学校を例にとった警備ネットワークは現実的な例と考えられ、従来の2次計画による解法に比べ、提案した線形計画による解法は現実的適用性を有するといえる。

この警備ゲームモデルに含まれるパラメータや構成要素がかなり多いため、今回の数値実験ではいくつかの例に対する計算を行ったに過ぎない。したがって、上記の知見を確信をもって言うためには、すべての要素を網羅的

に変化させた数値実験を行う必要があり、このことが今後の課題の一つである。

7. おわりに

この報告では、警備問題を現実的な計算時間で解くために、従来の解法を改善した。現実的な問題を解くという観点からは、さらに柔軟性のあるモデル作りも必要である。例えば、モデルの前提(A2)で述べた閉路が無いという仮定を緩和したり、複数侵入経路の考慮など、まだまだ改善が必要である。また、この報告でも追求していた解法の厳密性にこだわらず、ヒューリスティックな解法の提案による計算時間の更なる短縮なども新たな研究方向かも知れない。

謝辞

この研究の一部は、2021年度筑波学院大学共同研究資金の補助を受けて実施されています。ここに感謝申し上げます。

参考文献

- 1) 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.
- 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) 宝崎隆祐, 警備ゲームの動向, オペレーションズ・リサーチ, **64**, pp.614-621, 2019.
- 6) 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.
- 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) K. Hausken, Defense and attack of complex and dependent systems, *Reliability Engineering and System Safety*, **95**, No.1, pp.29-42, 2010.
- 9) K. Hausken, Protecting complex infrastructures against multiple strategic attackers, *Int. J. of Systems Science*, **42**, No.1, pp.11-29, 2011.
- 10) 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, **60**, pp.266-273, 2015.
- 11) 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, **61**, pp.226-233, 2016.
- 12) 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.
- 13) M. Baykal-Gursoy, Z. Duan, H.V. Poor and A. Garnaev, Infrastructure security game, *European J. of Operational Research*, **239**, pp.469-478, 2014.
- 14) 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.
- 15) 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, San Francisco, 2003.
- 16) 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.
- 17) 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.
- 18) 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.
- 19) P. Paruchuri, J.P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kaus, Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games, Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems, **2**, pp.895-902, 2008.
- 20) M. Jain, J. Tsai, J. Pita, C. Kiekintveld, S. Rathi,

- M. Tambe, 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.
- 21) M. Tambe, *Security and Game Theory- Algorithms, Deployed Systems, Lessons Learned*, Cambridge University Press, New York, 2012.
- 22) 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, 情報処理学会論文誌「数理モデル化と応用」, **4**, pp.19-35, 2011.
- 23) 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.
- 24) 宝崎隆祐, 非ゼロ和の施設警備ゲーム, 京都大学数理解析研究所講究録 2126, pp.35-43, 2019.
- 25) 宝崎隆祐, 非ゼロ和警備ゲームの現実適用性の拡張, 京都大学数理解析研究所講究録 2220, pp.167-174, 2022.