都市道路ネットワークにおける警備計画のシナリオ分析

○大堀耕太郎，穴井宏和（㈱富士通研究所）

蜂谷悠希，高橋真吾（早稲田大学）

Agent-based Scenario Analysis for Evaluating Security Plans in an Urban Road Network

* K. Ohori and H. Anai (Fujitsu Laboratories Ltd.)

Y. Hachiya and S. Takahashi (Waseda University)

概要－ ゲーム理論の警備計画問題への応用として，犯罪者から攻撃対象施設を守るための最適警備配置を導出する方法が提案されている．しかし，ゲームの解として得られた警備計画は，専門家の判断や過去の逮捕履歴との整合性といった部分的な評価に留まっている．本研究では，ゲーム理論の対象の一つである都市道路ネットワークの警備計画問題において，限定合理性を取り込んだ犯罪者エージェントモデルを用いて，警備の方法や箇所，期間などを変化させた多様なシナリオによって警備計画の効果について分析する．また，犯罪者エージェントの行動ログを分析することで，シナリオ間で得られた効果の違いを説明する．

キーワード: 警備計画，エージェントベース社会シミュレーション，セキュリティゲーム，都市道路ネットワーク

1 はじめに

テロや麻薬取引など様々な犯罪を防ぐための方法の一つとして，検問などの警備配置が考えられる．しかし，警備リソースは有限であるため，犯罪者が侵入してくる可能性のあるすべての箇所に警備を配置することはできない．そこで，犯罪者に推測されないように，警備箇所を乱択化し，警備計画を立てる必要がある．

ゲーム理論の分野では，セキュリティゲームと呼ばれる警備計画立案のためのアプローチが存在する[1]．犯罪者側と警備側の二人ゲームを考え，犯罪者側は施設等の攻撃対象を戦略として保持し，警備側は警備箇所を戦略として保持する．セキュリティゲームは連邦航空保安局[2]やロサンゼルス空港[3]などで実務的に利用されている．

しかし，セキュリティゲームの結果を評価することは非常に難しい．従来研究[4]では，数学的評価に加え，被験者実験，逮捕履歴などのデータ利用，専門家の指摘などが考えられているが，セキュリティという分野の性質上，取得できるデータは限られているため部分的な評価に留まっている．そのため，より多くの戦略を評価することが可能なシミュレーションの利用への期待が大きい．実際に，犯罪学の文脈においても，コンピュータによるシミュレーションへの期待は高く，理論補強や政策評価のために用いることを意図している[5]．

また，セキュリティゲームでは，最適解の導出にあたり，主として犯罪者の観測能力や行動について完全合理性を仮定していることが課題として挙げられている[6]．実際の犯罪者は限定的にしか警備に対する知識を持ちえないことや，警備や逮捕情報に基づいて動的に意思決定を変化させる．ゲーム理論の枠組みにおいても，より現実的な犯罪者の行動を要素として導入することは可能だが，意思決定空間が指数的に増加するため，解を得ることが困難になる．

本研究ではセキュリティゲームの問題クラスの一つである都市道路ネットワークにおける警備計画の問題を対象とし，前述した警備計画の評価の課題と犯罪者行動への限定合理性の導入の課題に対して，エージェントベース社会シミュレーション技法を用いて接近する．

まず，セキュリティゲームにおける都市道路ネットワーク警備問題とゲームの解から警備計画を立案する方法について説明する（2節）．次に，限定合理的な犯罪者行動を考慮するために，著者らの先行研究において構築された犯罪者エージェントモデルを提示する[7]（3節）．そのうえで，本モデルのパラメータをシナリオ変数として設定し（4節），シナリオ分析技法を用いて，立案された警備計画が犯罪者行動や警備の成否に与える影響について明らかにする（5節）．

2 都市道路ネットワーク警備問題

セキュリティゲームにおける都市道路ネットワーク警備問題[8]は，犯罪者側と警備側の2人ゼロ和ゲームである．ノードとエッジから構成されるネットワークによって道路網を表現し，犯罪者の発生地点のノード，犯罪者の攻撃対象のノード，各攻撃対象ノードの価値を表現する利得，警備リソースの数から問題が特徴づけられる．犯罪者は任意の発生地点ノードから出発し，ネットワーク上のエッジを移動し，任意の攻撃対象ノードを目指す．その経路上に警備リソースがなければ攻撃が成功して攻撃対象ノードが持つ利得を獲得する．このとき，警備側はこの利得の値の被害を受けるため，この被害を最小化するための警備リソースの配置パターンに関する最適な戦略を採用することを目指す．

これまでに，都市道路ネットワーク警備問題を解くアルゴリズムは複数提案されており，主に大規模な道路ネットワークでの解導出を目的としている[9, 10]．これらのアルゴリズムを用いて得られる解は，複数の重要な警備配置箇所とそれらの警備箇所が選択される確率である．警備計画を立案する際には，この選択確率に基づいて，警備リソース数分だけの警備の配置箇所を決定する．

3　モデル

シミュレーション空間は，施設や交差点を示すノードと，道路を示すエッジから構成されるネットワーク構造として表現される（Fig.1）．ノードには，犯罪者の発生地点ノード，攻撃対象ノード，それ以外の移動経路となるノードに分類される．攻撃対象ノードは攻撃成功時の価値を示す利得を持つ．エッジは，距離によって移動にかかる時間が異なることを示すために，移動コストを持つ．警備対象として選ばれたエッジには，警備員が配置される．

犯罪者は，エージェントしてモデル化され，その内部モデルに，「攻撃目標ノード」と，認知した警備箇所や過去に逮捕が生じた箇所を「リスク情報」として保有する．犯罪者は自身の行動開始時刻になると，攻撃対象ノードの中から攻撃目標ノードを選択し，リスク情報を考慮しながら，攻撃目標ノードを目指してノードからノードへ進む．ノード間を移動する際に，警備員が配置された警備対象エッジを通過しようとした場合，逮捕され行動不能となる．また，後述する条件を満たし場合に，犯罪者は撤退行動をとり，移動をやめる．

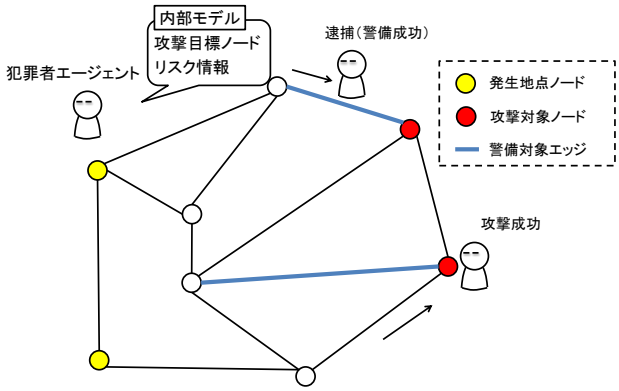

Fig. 1: モデルの概要

以下では，本モデルの特徴である，攻撃目標ノードの選択（3.1），リスク情報の更新（3.2），経路選択方法（3.3）について詳しく説明する．

3.1 攻撃目標ノードの選択

犯罪者は攻撃対象ノードの中から攻撃目標ノードを選択する際に，利得とは関係なく無作為に選択する，もしくは，利得の値に基づき確率的に選択するという 2 通りの方法を取りうる．セキュリティゲームでは犯罪者側と警備側は利得について共通の認識を持っていると仮定されているが，実際には認識が一致しない場合もあるため，本モデルでは無作為に選択することも可能とする．

3.2 リスク情報の更新

犯罪学における合理的選択理論[11]や窃盗犯の特徴に関する研究[12]によれば，犯罪者は犯罪が成功する可能性を考慮して行動をしている．本モデルでは犯罪者が感じるリスクに関する情報として，「警備箇所のエッジ」と「他の犯罪者が逮捕されたエッジ」の 2 種類を扱う．各犯罪者は，自身の行動開始時刻まで，都市道路ネットワークを観察していると仮定し，各時刻において確率的にこれらのエッジ情報を認知することができる．つまり，行動開始時刻が遅い犯罪者のほうが多くのリスク情報を獲得できる．また，行動開始後においても現在地のノードが持つ地理上の特性を表すインデックスから認知確率を導出し，現在地のノードの近傍内のエッジを確率的に認知することができる．

3.3 経路選択方法

犯罪者は新たなノードに到達するたびに，次に進むノードをリスク情報に基づき決定する．このときの手順は下記の通りである．

i. 現在地ノードと，その隣接ノードをつなぐエッジを次に移動する候補エッジ集合として列挙する．ただし，過去に通過したエッジやリスク情報として認知したエッジを除外する．このときに，候補エッジ集合が ϕ の場合には，犯罪者は撤退する．

ii. 候補エッジ集合内のエッジ j に接続するノードと攻撃目標ノードとの間の最短経路を求める．エッジ j までの移動コストと，エッジ j から攻撃目標ノードまでの最短経路での移動コストとの和を $mincost_j$ とする．

iii. エッジ j から攻撃目標ノードまでの最短経路上のエッジに犯罪者のリスク情報である「警備箇所のエッジ」や「他の犯罪者が逮捕されたエッジ」の数を計算する．それぞれの数を $guardedNum_j$，$ArrestedNum_j$ とし，これらに重みづけした値と，$mincost_j$ の値の和を犯罪者の次に移動する候補エッジ j に対する効用値 $Utility_j$ とする．

$$Utility_j = mincost_j + w_1 * guardedNum_j + w_2 * ArrestedNum_j$$

iv. 候補エッジ集合の中で効用値が最も小さいエッジを次の移動先として選択する．ただし，この効用値が撤退閾値よりも低い場合には，犯罪者は攻撃を中止し，撤退する．

4　シミュレーション設定

4.1 ネットワーク構造

本稿では，シミュレーション対象地域として，ドーハ市を取り上げ，警備対象として縦約 14km×横約 22km の主要道路のネットワーク情報を Open Street Map から抽出し，86 ノード，146 エッジで構成されるネットワーク構造を作成した(Fig.2).

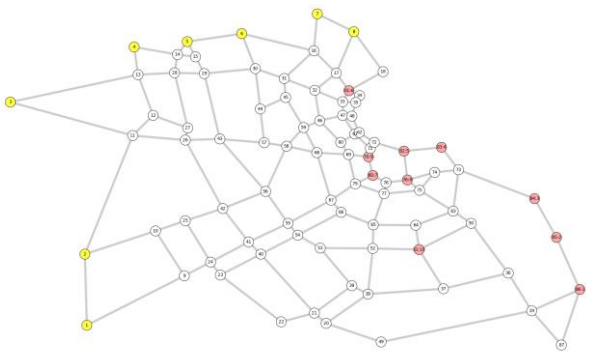

Fig. 2: 道路ネットワーク
黄：犯罪者の発生地点，赤：犯罪者の攻撃対象

4.2 基本設定

シミュレーション時間は 1 ステップを 2 分とし，1 日を午前と午後 2 つのタイムスロットに分けて警備を行う．警備計画を立案する際には，警備期間日数分のスロットを作成し，それぞれのスロットでの警備箇所を決定する．例えば，警備リソース数を 3，警備期間を 7 日とした場合には，14 スロット（2 スロット×7 日）を作成し，各スロットで警備する 3 箇所を決定することで警備計画が作成される．

犯罪者は試行ごとに 100 人発生する．また，本稿における実験では，犯罪者は逮捕者情報を取得できないと仮定し，w_2 は 0 に設定する．これ以外のパラメータはシナリオ変数として扱う．

4.3 シナリオ変数

本稿では，大きく分けて，犯罪者特性シナリオ（Table1），施策を表す警備計画シナリオ（Table2）の 2 種類のシナリオを扱う．

犯罪者の経路選択の方法として，経路変更を行わず常に最短経路を進む場合（$w_1 = 0$）と，経路変更を行う場合（$w_1 = 100$）の 2 通りを考える．また，攻撃目標の選択方法は，利得を無視して無作為に選択，利得の値に基づき確率的に選択，の 2 通り，撤退判断はリスクを取っても攻撃対象施設を目指す撤退判断閾値高（1000），少しでもリスクを感じた場合に撤退を行う撤退判断閾値低（600），その中間である撤退判断閾値中（800）の 3 通りをシナリオ変数として扱う．

Table1: 犯罪者特性シナリオ

犯罪者特性シナリオ	シナリオ変数			
	1	2	3	4
経路変更の有無	経路変更なし	経路変更あり	–	–
攻撃目標選択方法	無作為	利得ベース	–	–
撤退判断閾値	高(1000)	中(800)	低(600)	撤退なし

警備計画に関するシナリオとして，警備箇所選択方法，警備リソース数，警備期間の3つを扱う．警備箇所選択方法は，警備計画を立てる際に，セキュリティゲームで得られた解に基づいて警備箇所を選択，無作為に警備箇所を選択という2通りを考える．警備箇所数は 1, 3, 6, 9の4通り，警備期間は，1日，3日，7日，28日の4通りを考える．

Table2: 警備計画シナリオ

警備計画シナリオ	シナリオ変数			
	1	2	3	4
警備箇所選択方法	ゲームの解	無作為	–	–
警備リソース数	1	3	6	9
警備期間（日数）	1日	3日	7日（1週間）	28日（1か月）

5 シナリオ分析

シミュレーション実験では，4.3 節で示したシナリオ変数を組み合わせることでシナリオを作成し，各シナリオで 100 試行の実験を行い，警備成功率や平均獲得利得などの結果をランドスケープとして出力する．本稿では，図が膨大になるため，警備成功率のみの結果を載せるが，分析目的に合わせて，複数指標の結果を提示することが望ましい．シナリオ分析の結果から，立案した警備計画が警備成功数や犯罪者行動に与える影響について明らかにする．

5.1 経路変更の影響

犯罪者が攻撃目標ノードまで進む際に，経路変更を行わない場合と，犯罪者の学習を考慮して現在地点が変わるたびに経路を変更する場合の警備成功率を比較する（Fig.3）．他の犯罪者特性シナリオは，攻撃対象施設を無作為に選択，撤退なしとする．警備計画シナリオは，警備期間 7 日間分をゲームの解を用いて立案する．警備リソース数は 1,3,6,9 の 4 通りで実験を行う．

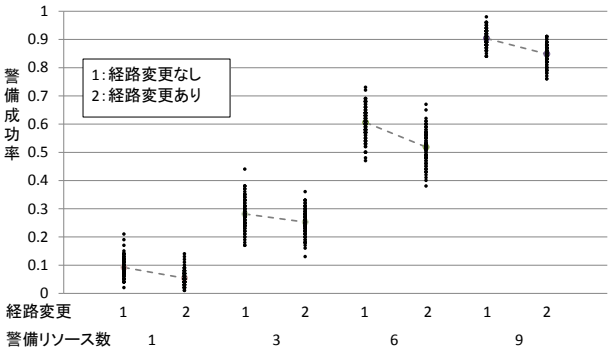

Fig. 3: 経路変更の有無による警備成功率.

この結果は，セキュリティゲームで仮定している経路変更なしに比べて，経路変更という要素を考慮した場合には，警備成功率が下がることを示している．つまり，警備計画は，犯罪者の学習行動も踏まえた評価を行うことが重要である．

一方で，この結果は，経路変更の要素を含んだ場合にも，警備箇所の乱択化がされていることで，必ずしも警備を避けることができないことも示唆している．

5.2 警備箇所選択方法の影響

警備箇所選択時にゲームの解から選択する場合と無作為に選択する場合での警備の効果を比較する．警備期間を 7 日間，警備リソース数は 1,3,6,9 の 4 通りとする．

犯罪者特性シナリオについては，攻撃目標を無作為に選択，撤退はなしとし，経路変更をなし（Fig.4），変更あり（Fig.5）の 2 通りでランドスケープを描く．

Fig.4，5 ともに，ゲームの解による警備は無作為の警備に比べて，概ね警備成功率が高く良い結果となっている．これより，セキュリティゲームによって求めた解は一定の有効性があるといえる．

しかし，犯罪者の経路変更あり（Fig.5）における警備リソース数 1 のシナリオでは，無作為による警備がゲームの解による警備よりも警備成功率の平均値が高い．この原因を分析するために，犯罪者の行動ログを分析する．

Table 3 は，犯罪者の経路変更あり（Fig.5）のゲームの解による警備，警備リソース数 1 のときの最も警備成功率の低かった一つの試行において，警備対象エッジを構成するノードを犯罪者が通過した回数を，全 14 スロットのうち前半 7 スロットと後半 7 スロットに分けて出力した結果である．この結果から，警備対象エッジのノードを通過する回数は前半 7 スロットから後半 7 スロットにかけて減少していることが分かる．この結果は他の試行でも同様の傾向がみられた．ゲーム

の解による警備では，無作為による警備に比べて警備箇所が絞られるため，警備リソース数が少ない場合には警備の多様性が減る．その結果として，犯罪者が容易に学習をすることができてしまう．そのため，セキュリティゲームの意図する乱択化による警備の効果が低くなるといえる．一方で，警備リソース数が増えるほど，ゲームの解でも警備の多様性が増加するため，無作為による警備よりも高い警備成功率を得ることができる．

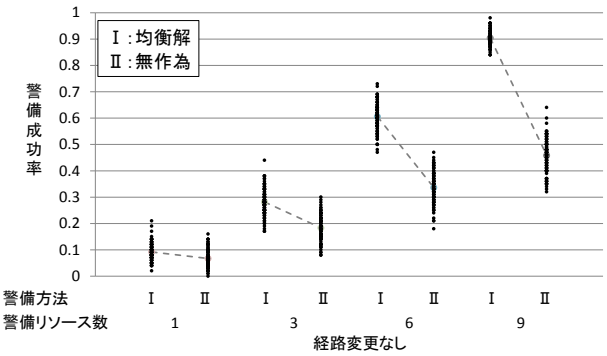

Fig. 4: 警備箇所選択方法の違いによる警備成功率（経路変更なし）．

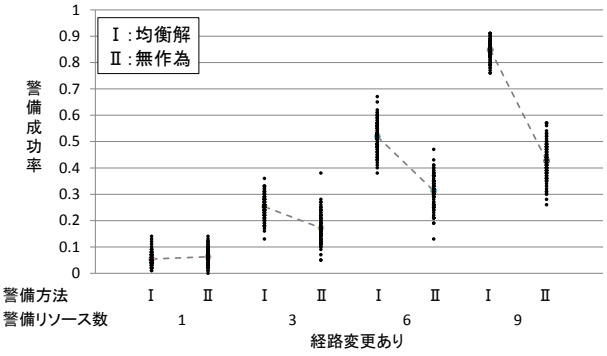

Fig. 5: 警備箇所選択方法の違いによる警備成功率（経路変更あり）．

Table 3: 犯罪者のノード通過回数.

ノード番号	前半7スロット	後半7スロット
70	12	8
71	2	2
74	3	0
75	1	0
76	8	2
78	6	0
80	12	7
82	27	22

5.3 警備期間の影響

セキュリティゲームでは，乱択化された警備計画は犯罪者の監視にも耐えられるとされている．そこで，警備期間を変化させた場合に，警備効果が保たれるのかを検討する．

警備期間を 1 日，3 日，7 日，28 日の 4 通りで実験を行い，警備成功率のランドスケープを描く（Fig.6）．警備箇所選択方法はゲームの解と無作為の 2 通り，警備リソース数は 3 とする．また，犯罪者特性については，経路変更あり，攻撃目標ノードを無作為に選択，撤退はなしとする．

Fig.6 より，3 日，7 日，28 日と警備期間を延ばしても，ゲームの解による警備成功率の平均値は低下することはなく，犯罪者の学習が生じた場合にも乱択化の効果が現れているといえる．

一方で，警備期間が 1 日の場合には，警備成功率の平均値はゲームの解による警備よりも無作為の警備の結果のほうが高くなる．5.2 節の結果と合わせると，リソース数が少なく，警備期間が短い場合には，無作為の警備が有効になる場合がある．ただし，無作為による警備の成功率は試行間でのばらつきが大きいので，安易に無作為による警備が有効であると考えることはできない．

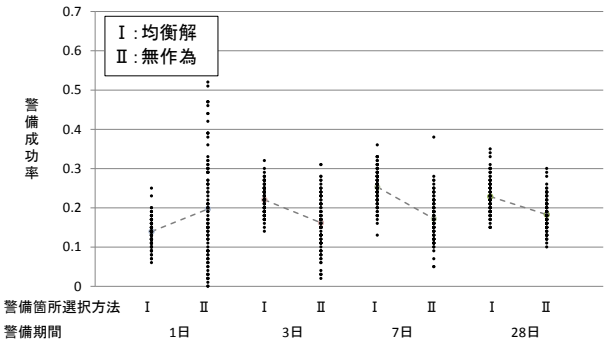

Fig. 6: 警備期間の違いによる警備成功率.

有効な警備を明らかにするために，無作為による警備で警備成功率の高かった上位 5 つの試行を取り出し，警備箇所について考察する．Fig.7 では，これら 5 つの試行において警備対象となったエッジを太線で示している．この図からは，特徴的な警備箇所の傾向を見ることはできない．次に，犯罪者行動について分析を行う．警備期間 1 日では犯罪者の学習はほとんど進まないため，ほぼ経路変更を行うことはなく，最短経路で攻撃目標ノードに進む．そこで，警備リソースを配置せず，犯罪者を行動させた場合の犯罪者の通過ノードについて調べる．Fig.8 は，犯罪者が通過したノードを通過回数の違いで色分けした図である．

Fig.7 と Fig.8 を比較すると，警備エッジが犯罪者の通過回数の多いノードと接続する関係にあることが分かる．つまり，犯罪者が警備状況を学習する期間が短い場合には，ゲームの解による警備よりも，ネットワーク構造における犯罪者の発生地点ノードと攻撃目標ノードとの位置関係から，通過する可能性の高い箇所に警備を置く方が高い効果が得られるといえる．

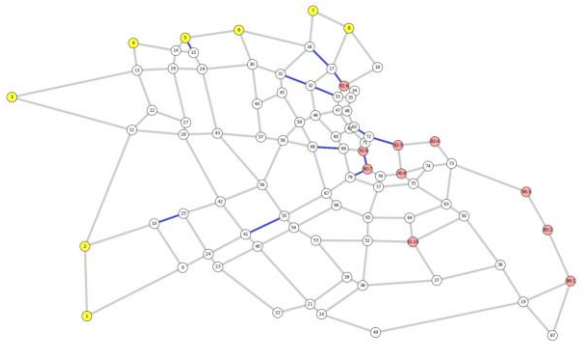

Fig. 7: 警備対象エッジ

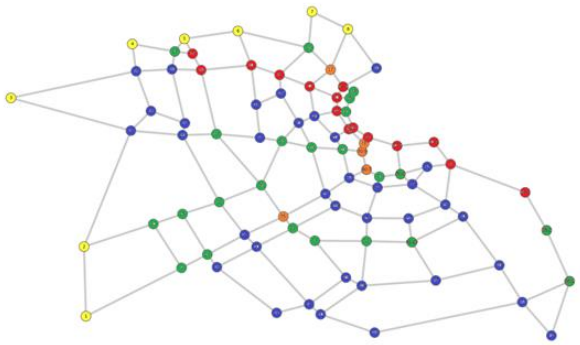

Fig.8：犯罪者のノード通過数

青：10 回未満，緑：10 回以上 20 回未満，橙：20 回以上 30 回未満，赤：30 回以上

5.4 攻撃目標選択方法の影響

5.3 節までは，犯罪者側と警備側の攻撃対象ノードに対する利得は非対称とし，犯罪者は無作為に攻撃目標ノードを選択していた．しかし，セキュリティゲームでは，攻撃対象施設に対する犯罪者側と警備側の重要度の認識は同じであると仮定している．そこで，犯罪者が攻撃対象ノードの保有する利得に基づいて確率的に攻撃目標ノードを選択した場合の警備成功率を分析する（Fig.9）．犯罪者特性シナリオは，犯罪者の経路変更をあり，攻撃目標ノードを利得の重みづけにより選択，撤退はなしとする．警備計画シナリオは，警備期間を 7 日とし，警備箇所選択方法をゲームの解と無作為の 2 通り，警備リソース数を 1，3，6，9 の 4 通り用いる．

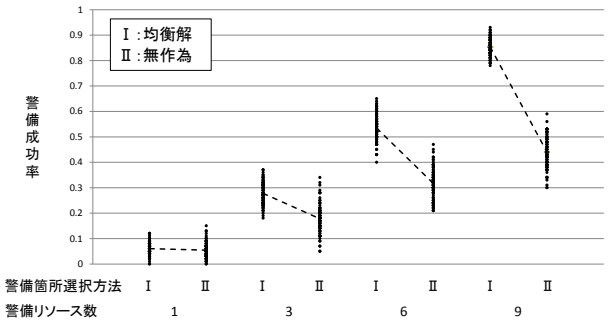

Fig.9：利得に基づいて攻撃目標ノードを選択した場合の警備成功率

無作為に攻撃目標ノードを選択し，他のシナリオが同条件の場合（Fig.5）と攻撃目標ノードを利得に基づいて選択した場合（Fig.9）を比較すると，ほぼ同じ形状のランドスケープが得られた．ただし，警備リソース数 1 のシナリオでは，Fig.5 では無作為による警備が有効だったのに対して，Fig.9 では，ゲームの解による警備の警備成功率の平均値が高いことが分かる．これは，ゲームの解は利得に基づく攻撃目標ノード選択を仮定して導かれているため，ゲームの解による警備に有利に働いたと考えられる．しかし，現実的には犯罪者側と警備側の攻撃対象施設に対する利得は一致しない可能性のほうが高いため，5.3 節までの設定のように，犯罪者側と警備側との間で認識の相違があることを前提とした評価も併せて行うことが必要である．

5.5 撤退閾値の影響

1 節で述べたように，犯罪者は犯罪が成功する可能性を考慮して犯行に及ぶことが指摘されている．このことから犯罪が失敗する可能性が高まった場合，撤退行動にうつると考えられる．そこで，撤退行動が警備の結果に与える影響を分析する．

本モデルでは，犯罪者がノードに到達するたびに行う経路選択行動において，次に移動する候補エッジがなくなった場合（3.3 節ⅰ），もしくは，選択した経路の評価値が撤退閾値を超えた場合（3.3 節ⅳ）に，撤退を選択し，シミュレーション上から消えることで犯罪者の撤退行動を表現している．ここで，撤退閾値の低い犯罪者は攻撃に慎重な犯罪者を，撤退閾値の高い犯罪者はリスクを冒してでも攻撃を行う犯罪者を意味している．

現実では，警備側は実際に攻撃目標に犯罪者が到着した場合，もしくは逮捕した場合に犯罪者の存在を知ることになる．そのため，撤退した犯罪者の存在を警備側は認知することができない．

シミュレーションの強みは撤退した犯罪者についても評価を行えることにある．そこで，撤退した犯罪者も含めた全体としての警備成功率（（逮捕数＋撤退数）／全ての犯罪者数）と，警備側が認知できた警備成功率（逮捕数／（攻撃成功数＋逮捕数））の両方を出力する（Fig.10,11）．

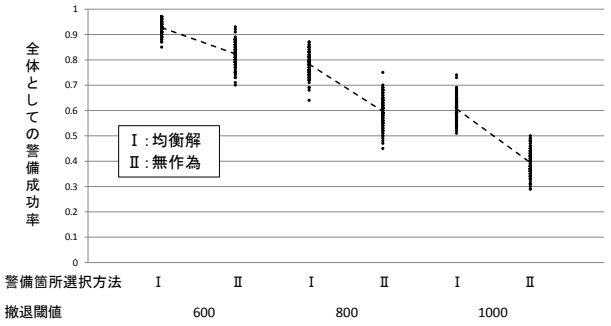

Fig.10：全体としての警備成功率

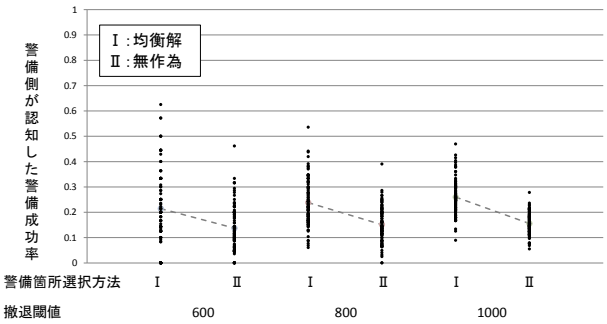

Fig.11：警備側が認知した警備成功率

犯罪者特性シナリオは，犯罪者の経路変更をあり，攻撃目標ノードを利得の重みづけにより選択，撤退閾値を高（1000），中（800），低（600）の 3 通りとする．警備計画シナリオは，警備リソース数を 3，警備期間を 7 日，警備箇所選択方法をゲームの解と無作為の 2 通りを用いる．

Fig.10 において，撤退閾値が増えるにつれて，全体

としての警備成功率が下がる原因は，犯罪者の撤退数が減るためである．一方で，Fig.11 において，警備側が認知した警備成功率は平均だけを見ると，撤退閾値を変えても大きな違いは見られない．これより，撤退閾値が低い犯罪者が多い場合には，全体としての警備成功率の方が，警備側が認知した警備成功率よりも大幅に高くなる．これは，撤退行動を増やすという警備の抑止力があるにもかかわらず，警備計画の効果が低いという判断を下す可能性があることを示唆している．

また，警備側が認知した警備成功率は，同じシナリオでも試行間のばらつきが大きい．実務では，警備の実績を得られることが少ないことを考えると，警備側が認知した警備成功率から警備計画を評価することは難しいといえる．

6 おわりに

本稿では，エージェントベース社会シミュレーション技法を用いて犯罪者特性や警備計画の違いが警備の効果に与える影響を明らかにした．以下では，本研究の貢献と今後の課題について述べる．

6.1 本研究の貢献

国家的行事などの大規模なイベント時にはその実施計画の主要テーマとして警備計画が挙がっている．セキュリティゲームをはじめとして，有効な警備計画立案の方法はあるが，その評価は大きな課題となっている．その原因は，大規模イベントは開催頻度が低く，警備効果に対する経験を蓄積できないことや，5.5 節に示したように撤退した犯罪者を認知できないことが挙げられる．また，イベント開催国や地域が変われば，犯罪者特性やイベント主催者の警備に対する考え方が変わるため，必ずしも過去の経験が活かされるとは限らない．

これに対して，本研究のシミュレーションは，犯罪者や警備計画に関する多様なシナリオで，繰り返し警備計画の評価を行うことができる．また，エージェントベースモデルを用いているため，個々のエージェント行動のログを分析することができ（これをミクロダイナミクス分析 [13] と呼ぶ），警備が成功（または失敗）したときの原因を詳細に理解できる．よって，イベント時の警備計画検討や事前の警備訓練時に，本シミュレーションを用いることで，警備計画がもたらす多様な可能性を考慮した行動をとることができる．

6.2 今後の課題

本研究では，犯罪学の理論と比較しながらモデル構築時の妥当性の検討を行ってきた．しかし，シミュレーション結果と実データとの整合性を確認することはできていない．今後は実現場の警備に関するステークホルダーとの対話を進め，シミュレーション結果の妥当性検討も進める必要がある．

また，本稿では単独犯の犯罪者を想定したが，従来研究 [6] でも指摘されているように，組織的な犯罪集団を考えることも重要である．その際には，犯罪者エージェント間の情報共有をモデル化する必要がある．

さらに，ネットワーク構造の違いによる分析も興味深い．ネットワークインデックスによる有効な警備箇所を見つけることができれば，地域に依存しない警備に関する新たな理論構築も可能になると考えられる．

参考文献

1) M. Tambe : Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned, Cambridge University Press (2011)
2) J.Tsai, S. Rathi, C. Kiekintveld, F. Ordonez and M. Tambe : IRIS - A Tool for Strategic Security Allocation in Transportation Networks, In Proceedings of the Industry Track of the Eighth International Joint Conference on Autonomous Agents and Multi-agent Systems (2009)
3) J. Pita, M. Jain, J. Marecki, C. Western, C. Portway, M. Tambe, F. Ordonez, 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 Industry Track of the 7th International Joint Conference on Autonomous Agents and Multi-Agent Systems (2008)
4) M. Taylor, C. Kiekintveld, C. Western, and M. Tambe : A Framework for Evaluating Deployed Security Systems: Is There a Chink in Your ARMOR?, Informatica, 34, 129/139 (2010)
5) G. Elizabeth and L. Mazerolle : Simulated experiment and their potential role in criminology and criminal justice, Journal of Experimental Criminology4-3, 187/193 (2008)
6) M. Tambe, A. Jiang, B. An and M. Jain : Computational game theory for security: Progress and challenges, Proceedings of the AAAI Spring Symposium on Applied Computational Game Theory (2014)
7) 蜂谷悠希，高橋真吾，穴井宏和，大堀耕太郎：エージェントベース社会シミュレーションによる警備計画の評価方法の提案，経営情報学会秋季全国大会（2014）
8) J. Tsai, Z. Yin, J. Kwak, D. Kempe, C. Kiekintveld and M. Tambe: Urban Security : Game-Theoretic Resource Allocation in Networked Physical Domains, In Proceedings of the National Conference on Artificial Intelligence (2010)
9) M. Jain, V. Conitzer and M. Tambe : Security Scheduling for Real-world Networks, In Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (2013)
10) 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 10th International Conference on Autonomous Agents and Multiagent Systems (2011)
11) D. Cornish and R.V. Clarke : Understanding crime displacement: An application of rational choice theory, Criminology 25-4, 933/947 (1987)
12) 大野宏：万引き犯の行動分析と検知に関する研究，電気通信大学大学院電気通信学研究科人間コミュニケーション学専攻博士論文 (2009)
13) K. Ohori and S. Takahashi: Market Design for Standardization Problems with Agent-based Social Simulation, Journal of Evolutionary Economics, 22, 49-77 (2012)