数理解析研究所講究録 第2126巻 2019年 9-18

サイバーセキュリティにおける ゲシュタルトナッシュ均衡の分析

大阪府立大学大学院 工学研究科
兵藤 壮泰 (Takeyasu Hyodo), 北條 仁志 (Hitoshi Hohjo)
Graduate School of Engineering, Osaka Prefecture University

1 はじめに

昨今ではモノがインターネットに繋がる、所謂 IoT(Internet of Things) が注目を浴びるようになってきた。そして、この IoT と密接に関わってくるものが CPS(cyber-physical systems) である。CPS は実世界にある多様なデータを集め、サイバー空間で分析して機械、人、社会に反映させるものである。これらの技術によって今までにない様々なサービスの実現が可能である。例えば車がインターネットに繋がれば、クラウドソーシングを利用して現在地を送信し、これらの情報を解析して車の混み具合を判断し、渋滞情報をクラウドソーシングを用いて車に送り、渋滞緩和を促すといったサービスを将来的に生み出すことができる。

このような CPS/IoT 社会を実現させるためには安心かつ安全で相互に通信し運用可能なネットワーク上の関係が必要である。しかし、新しい技術には新たなサイバー攻撃のリスクも付きまとう。特定のネットワークに対して大量のアクセスによる負荷をかける DoS 攻撃や、特定の組織や個人に狙いを定め、それに適した攻撃を組み合せて継続的に攻撃を仕掛ける APTs(持続的標的型攻撃) 等がその例として挙げることができる。

これらの攻撃の中でも、我々は APTs による攻撃に焦点を当てる。APTs は前述したように特定の相手に対して継続的に攻撃を仕掛ける。多大なリソースを要するため、巨大な組織による攻撃が多く、社会に大きな影響を与える攻撃であるといえる。IoT などの新しい技術は作られて間もないので脆弱性が発見されておらず、その修正が入る前に脆弱性をつくようなゼロデイ攻撃のリスクも高く、APTs はこのゼロデイ攻撃を組み合わせたものが多くなり、通常のサービスに対する APTs よりも危険性が高くなると考える。この攻撃によってデバイスへ信号を送るためのクラウドの所有権が攻撃者に乗っ取られる可能性がある。

これらの将来的な CPS/IoT 社会に対する APTs の状況を分析するためにゲーム理論を用いて様々な研究がなされてきた。2015 年、Pawlick et al.[2] は自動車の遠隔操作について、ゲーム理論のシグナリングゲームとフリップイットゲームを合わせたクラウドコントロールゲームモデルを提案し、そのゲームの均衡点であるゲシュタルトナッシュ均衡 (GNE) を求めた。2017 年には、Pawlick et al.[1] はインスリン自動注射デバイスにおける分野でも GNE を用いて均衡点を求めた。しかし、これらの研究においては攻撃者、防御者の戦略が単純で静的なモデルであった。

本研究では、クラウドコントロールゲームモデルにおけるフリップイットゲームの戦略を動的にし、より現実へと近づけたモデルにおいても GNE は存在することを明らかにする。これによって、より高度な戦略をとる攻撃者に対する防御者、そして IoT デバイスの最適行動を導くことができる。GNE は、サイバー上の保険、商業投資、企業方針に対して役立つと考えられる。

2　モデル化

クラウドの所有権の取り合いをフリップイットゲームで表現し、クラウドと IoT デバイスのやりとりをシグナリングゲームで表現する。この二つのゲームを合わせて行うクラウドコントロールゲームモデルを用いた。

2.1　シグナリングゲーム (SG)

SG のプレイヤーは受け手 (デバイス r) と二人の送り手 (攻撃者 (t_A)、防御者 (t_D)) である。ゲームのルールを以下に記す。

1. 状態集合 T から、ランダムに 1 つの状態 t が選ばれる。
2. 送手が状態 t を見て、シグナル集合 M から 1 つのシグナル m を選ぶ。
3. 受手がシグナル m を見て、行動集合 A から行動 a を選ぶ。
4. 状態 t と行動 a のセットで評価が決まる。(a が t において最適な行動ならシグナリング成功となる)

上記の 1〜4 を繰り返し、プレイヤーは 4 の評価により戦略を更新し最適戦略を導く。

2.1.1　SG の期待利益

プレイヤー i の SG における戦略を σ_i^S、利益を u_i^S、受手の信念を μ とおくと、防御者、攻撃者、デバイスの SG におけるそれぞれの期待利益は式 (1)、(2)、(3) の様になる。式 (4) は受け手がシグナル m を受けた時、送り手のタイプが t_A だと信用する信念である。p は攻撃者がシグナルを送ってくる (クラウド所有権を得る) 確率である。戦略 σ_i^S は後述の ARP モデルを用いて更新を行った。

$$\overline{u}_{t_D}^S(\sigma_r^S, \sigma_{t_D}^S) = \sum_{a\in A}\sum_{m\in M} u_{t_D}^S(m,a)\sigma_r^S(a|m)\sigma_{t_D}^S(m) \tag{1}$$

$$\overline{u}_{t_A}^S(\sigma_r^S, \sigma_{t_A}^S) = \sum_{a\in A}\sum_{m\in M} u_{t_A}^S(m,a)\sigma_r^S(a|m)\sigma_{t_A}^S(m) \tag{2}$$

$$\overline{u}_r^S(\sigma_r^S|m,\mu) = \sum_{t\in T}\sum_{a\in A} u_r^S(t,m,a)\mu(t|m)\sigma_r^S(a|m) \tag{3}$$

$$\mu(t_A|m) = \frac{\sigma_{t_A}^S(m)p}{\sigma_{t_A}^S(m)p + \sigma_{t_D}^S(m)(1-p)} \tag{4}$$

2.1.2　SG における均衡

- 分離均衡

  送り手は一つの状態に一つのシグナル、受け手は一つのシグナルに一つの行動が割り振られている。受け手は送り手の状態の判断が容易にできる。

  例：状態 t_D はシグナル 1 、状態 t_A はシグナル 2

- 一括均衡

  送り手が状態によらず、同じシグナルを送る。これにより、受け手は送り手の状態の判断ができない。

  例：状態 t_D、t_A ともにシグナル 1

2.1.3 ARP モデル

Bereby-Meyer & Erev[5] は人間の学習能力を参考にして ARP モデルを提案した。現在の報酬の値と過去の報酬の値を参照して学習をすることによって、より人間のモデルに近づけたものである。

$$str_n(time) = \frac{q_n(time)}{\sum q_n(time)} \tag{5}$$

$$q_n(time+1) = \max\{v, (1-\phi)q_n(time) + E_j(n, L_{time}(X_j))\} \tag{6}$$

$$E_j(n, L(X_j)) = \begin{cases} L_{time}(X_j)(1-\varepsilon) & (j=n) \\ L_{time}(X_j)\varepsilon & (otherwise) \end{cases} \tag{7}$$

$$L_{time}(X_j) = X_j - \rho(time) \tag{8}$$

$$\rho(time+1) = \begin{cases} (1-c^+)\rho(time) + (c^+)X_j & (X_j \geq \rho(time)) \\ (1-c^-)\rho(time) + (c^-)X_j & (X_j < \rho(time)) \end{cases} \tag{9}$$

$str_n(time)$ は時間 $time$ に戦略 n を取る確率であり、$q_n(time)$ は戦略 n の純粋値である。v は純粋値の最低値であり、X_j は戦略 j を取った時の利益である。$\rho(time)$ は時間 $time$ までの利益の記憶値である。ϕ は忘却率であり、$c+, c^-$ は利益の学習率である。ε は報酬の重みである。

2.2 フリップイットゲーム (FG)

FG は攻撃者と防御者で、1 つのリソース (クラウド所有権) を時間軸に沿って取り合うゲームである。両プレイヤーは各時間 ($time$) 毎に自身の戦略に従い、コストを支払って動くかどうか判断する。動いた時リソースを相手が所有していれば、リソースを自身の所有物に変更する。しかし、自身の所有権だった場合は動いた意味がなく、リソースの所有権はそのまま変わらない。これを繰り返し、コストとリソース所有による利益を考慮してプレイヤーは最適な戦略を導く。

2.3 クラウドコントロールゲーム (CCG)

CCG は前述の二つのゲームの組み合わせであり、クラウドの所有権をフリップイットゲーム、デバイスとクラウドの通信をシグナリングゲームで表している。具体的には、フリップイットゲームのリソースを所有しているプレイヤーによってシグナリングゲームの送手の状態が決定される。FG におけるリソースの所有権が t_A の場合は SG における送り手のタイプは t_A になり、t_D の場合は送り手のタイプは t_D となる。図 1 は CCG を表現したものである。本研究のモデルはこの CCG に基づく。

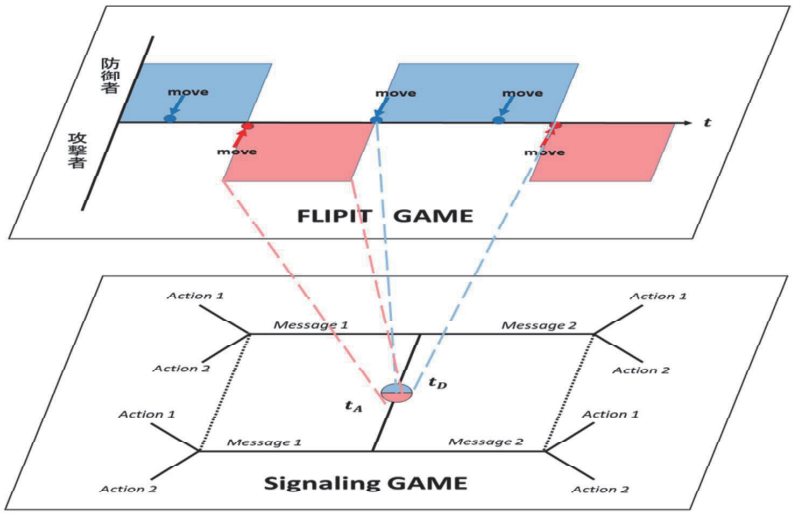


図 1: CCG モデル

2.3.1 CCG における FG の期待利益

プレイヤー i の FG における戦略 (動く確率) を f_i、一回動いた時のコストを k_i とおくと、防御者、攻撃者の FG における期待利益は式 (5)、(6) のようになる。$\bar{u}_i^S$ はプレイヤー i の SG における期待利益であり、p は SG と同様に攻撃者がクラウドを所有する確率であり、攻撃者と防御者の戦略対 (f_{t_A}, f_{t_D}) によって決まる。

$$\bar{u}_{t_D}^F(f_{t_D}, f_{t_A}) = \bar{u}_{t_D}^S(1-p) - k_{t_D} f_{t_D} \tag{10}$$

$$\bar{u}_{t_A}^F(f_{t_D}, f_{t_A}) = \bar{u}_{t_A}^S p - k_{t_A} f_{t_A} \tag{11}$$

2.3.2 CCG における FG の均衡

まず、リソースの所有による利益が正の値でなければ各プレイヤーは動かないという戦略を取る。だが、現実問題としてリソースを所有して利益がでないという状況はおかしいので、条件 $\bar{u}_{t_D}^S > 0, \bar{u}_{t_A}^S > 0$ を仮定する。その上で、以下の条件を満たさなければならない。

$$\frac{\partial \bar{u}_{t_D}^F}{\partial f_{t_D}} = 0 \tag{12}$$

$$\frac{\partial \bar{u}_{t_A}^F}{\partial f_{t_A}} = 0 \tag{13}$$

3 ゲシュタルトナッシュ均衡 (GNE)

ゲシュタルトナッシュ均衡とは CCG のようにゲームが複数組み合わさっているゲームにおける、各ゲーム単体での均衡はなくゲーム全体での均衡である。

3.1 均衡の定義

以下の式 (14)〜(18) を満たす戦略の組 $(f^*_{t_D}, f^*_{t_A}, \sigma^{S*}_{t_D}, \sigma^{S*}_{t_A}, \sigma^{S*}_r)$ はゲシュタルトナッシュ均衡 (GNE) であるという。

$$
\begin{aligned}
\bar{u}^F_{t_D}(f^*_{t_D}, f^*_{t_A}) &\geq \bar{u}^F_{t_D}(f_{t_D}, f^*_{t_A}) \text{ for any } f_{t_D} && (14)\\
\bar{u}^F_{t_A}(f^*_{t_D}, f^*_{t_A}) &\geq \bar{u}^F_{t_A}(f^*_{t_D}, f_{t_A}) \text{ for any } f_{t_A} && (15)\\
\bar{u}^S_{t_D}(\sigma^{S*}_r, \sigma^{S*}_{t_D}) &\geq \bar{u}^S_{t_D}(\sigma^{S*}_r, \sigma^S_{t_D}) \text{ for any } \sigma^S_{t_D} && (16)\\
\bar{u}^S_{t_A}(\sigma^{S*}_r, \sigma^{S*}_{t_A}) &\geq \bar{u}^S_{t_A}(\sigma^{S*}_r, \sigma^S_{t_A}) \text{ for any } \sigma^S_{t_A} && (17)\\
\bar{u}^S_r(\sigma^{S*}_r|m, \mu) &\geq \bar{u}^S_r(\sigma^S_r|m, \mu) \text{ for any } \sigma^S_r && (18)
\end{aligned}
$$

Pawlick et al.[1] が示したように、FG における戦略対 (f_{t_D}, f_{t_A}) は SG の期待値 $\bar{u}^S_{t_D}, \bar{u}^S_{t_A}$ によって変動し、期待値 $\bar{u}^S_{t_D}, \bar{u}^S_{t_A}$ と SG の戦略の組 $(\sigma^S_{t_D}, \sigma^S_{t_A}, \sigma^S_r)$ は攻撃者のクラウド所有確率 p によって変動する。また、確率 p は FG における戦略 (f_{t_D}, f_{t_A}) によって変動する。

これらのことから値 (f_{t_D}, f_{t_A}) と $(\bar{u}^S_{t_D}, \bar{u}^S_{t_A})$ が一定の値に収束するならば GNE が存在すると言える。

3.2 SG における GNE

Pawlick et al.[1] では GNE が各ゲームでどのような状況で存在するかを明らかにしている。まず CCG における SG の利得関係は表 1 の条件を満たさなければならない。m_L, m_H はそれぞれ危険度の低いシグナルと高いシグナルで、a_Y, a_N はデバイスが信号を信用する行動と信用しない行動を表している。

表 1: 利得条件

番号	条件
1	$u^S_r(t_D, m_L, a_Y) > u^S_r(t_D, m_L, a_N)$
2	$u^S_r(t_A, m_H, a_Y) < u^S_r(t_D, m_H, a_N)$
3	$u^S_{t_D}(m_L, a_Y) > u^S_{t_D}(m_H, a_Y)$
4	$u^S_r(t_D, m_L, a_Y) > u^S_r(t_D, m_H, a_Y)$
5	$u^S_{t_D}(m_L, a_Y) > u^S_{t_A}(m_H, a_Y)$
6	$0 > u^S_{t_D}(m, a_N) > u^S_{t_A}(m, a_N)$
7	$u^S_{t_A}(m_H, a_Y) > u^S_{t_A}(m_L, a_Y)$
8	$u^S_r(t_A, m_H, a_Y) < u^S_r(t_A, m_L, a_Y)$

ここで SG の均衡点を探るためにデバイスの信用行動の信念を以下の式 (19) で定義する。$YB_H(p)$ は送り手からシグナル m_H を送られた時デバイスが信用行動 a_Y を取る信念、$YB_L(p)$ は送り手からシグナル m_L を送られた時デバイスが信用行動 a_Y を取る信念である。

$$
\begin{aligned}
YB_H(p) = {} & p\{u_r(t_A, m_H, a_Y) - u_r(t_A, m_H, a_N)\}\\
& + (1-p)\{u_r(t_D, m_H, a_Y) - u_r(t_D, m_H, a_N)\}\\
YB_L(p) = {} & p\{u_r(t_A, m_L, a_Y) - u_r(t_A, m_L, a_N)\}\\
& + (1-p)\{u_r(t_D, m_L, a_Y) - u_r(t_D, m_L, a_N)\}
\end{aligned}
\qquad (19)
$$

SG には大きく分けて分離均衡と一括均衡の二つの均衡がある。

まず、分離均衡を表 1 の条件で考える。防御者がシグナル m_L、攻撃者がシグナル m_H を送る状態だと仮定したとき、デバイスの最適行動はシグナル m_L が送られてきた場合は行動 a_Y、シグナル m_H の場合は行動 a_N となる。この場合攻撃者は m_H を送るよりは m_L を送ったほうが利益が高いので上記の仮定での均衡は存在しない。次に、防御者がシグナル m_H、攻撃者がシグナル m_L を送る状態だと仮定したとき、もし利益条件が $u_r^S(t_A, m_L, a_Y) < u_r^S(t_A, m_L, a_N), u_r^S(t_D, m_H, a_Y) < u_r^S(t_D, m_H, a_N)$ であればデバイスの最適行動は a_N となり、分離均衡が存在する (この均衡を EQ_S0 とする)。

今度はシグナル m_L での一括均衡での場合を考える。もし、信用行動信念が $YB_L(p) > 0$, $YB_H(p) < YB_L(p)$ の時は、デバイスの最適行動は a_Y となり一括均衡が存在する (この均衡を EQ_L1 とする)。また、信用行動信念が $YB_L(p) < 0, YB_H(p) < 0$ の場合のデバイスの最適行動は a_N であり、均衡が存在する (この均衡を EQ_L2 とする)。m_L のシグナルにおける最後の一括均衡は、信用行動信念の条件が $YB_L(p) = 0, YB_H(p) < 0$ のときに、デバイスの最適行動が混合戦略となる均衡が存在する (この均衡を EQ_L3 とする)。

同様にシグナルが m_H の場合の均衡も求めることができ、それぞれの均衡を (EQ_H1, EQ_H2, EQ_H3) と定める。それぞれの均衡における状態と条件を表 2 にまとめた。 b

表 2: SG の均衡一覧

名前	条件	攻撃者	防御者	デバイス
EQ_S0	$u_r^S(t_A, m_L, a_Y) < u_r^S(t_A, m_L, a_N)$, $u_r^S(t_D, m_H, a_Y) < u_r^S(t_D, m_H, a_N)$	m_L	m_H	a_N
EQ_L1	$YB_L(p) > 0, YB_H(p) < YB_L(p)$	m_L	m_L	a_Y
EQ_L2	$YB_L(p) < 0, YB_H(p) < 0$	m_L	m_L	a_N
EQ_L3	$YB_L(p) = 0, YB_H(p) < 0$	m_L	m_L	Mix
EQ_H1	$YB_L(p) < YB_H(p), YB_H(p) > 0$	m_H	m_H	a_Y
EQ_H2	$YB_L(p) < 0, YB_H(p) < 0$	m_H	m_H	a_N
EQ_H3	$YB_L(p) < 0, YB_H(p) = 0$	m_H	m_H	Mix

ここで FG における均衡の条件を考える。FG の均衡は $\bar{u}_{t_D}^S > 0, \bar{u}_{t_A}^S > 0$ の条件を満たさなければならない。よってデバイスの最適行動が a_N の均衡は、表 1 の条件 6 より GNE は存在しないことになる。GNE はデバイスの最適行動 a_Y の均衡に存在することになるが、デバイスの最適行動が a_Y の場合は表 1 の条件 3 より、防御者の最適行動はシグナル m_H を送ることになるため、GNE が存在する SG における均衡状態は EQ_L1 である。

4 本研究モデル

2015 年 Pawlick et al.[2] や 2017 年 Pawlick et al.[1] は上記の GNE の存在を明らかにし、いくつかの現実問題に適用した。しかしながら、これらの既存モデルは FG における攻撃者、防御者の戦略が単純であり、一定時間間隔を空けて動くといった静的なモデルであった。

APTs を行う攻撃者は持続的にシステムを攻撃してくるため、システムのパス等が使えなくなった場合は、防御者がどのタイミングでパスを変更したかといった情報を得ることができると考えられる。攻撃者はこの情報を用いた高度で動的な戦略を行うはずである。2013 年 van Dijk

et al.[3] は FG においてこの動的な戦略のモデルを提案した。本研究では動的な戦略を用いた攻撃者をもつ CCG において GNE が存在することを明らかにする。

4.1 動的モデル

4.1.1 LM Attacker(LMA)

この攻撃者モデルは前述した通り、防御者がいつ動いたのかという情報を元に動的に動く間隔を決める。具体的には、攻撃者は相手が動いた時間から自分が動いた時間の間隔 τ を取得し、次は τ の時間を空けてから、一定の間隔 δ を待って動く。

2013 年 van Dijk et al.[3] はこの LMA と一定間隔で動く静的なモデルの防御者 (DP) で FG をプレイさせた。$f_{t_D} \leq \frac{1}{k_{t_A}}$ の場合は $\bar{u}^F_{t_D} \leq 0$, $\bar{u}^F_{t_A} \geq 0$ となり、$f_{t_D} \geq \frac{1}{k_{t_A}}$ の場合は、$\bar{u}^F_{t_D} \geq 0$, $f_{t_A} = 0 (\bar{u}^F_{t_A} = 0)$ となる。これらから、初期のランダムな状況では前者での防御者が不利になるパターンが存在することがわかる。よって防御者はよりよい LMA に対する戦略を模索しなければならない。

4.1.2 Defender playing with Delayed-Exponential Distribution(DDED)

これは LM に対応するための防御者の動的な戦略である。防御者は前回動いた時点から間隔 Δ を空け、その後に確率密度関数 $f(x) = \lambda e^{-\lambda x}$ に従って動く。$\Delta = 0$ の場合は Defender playing with Exponential Distribution(DED) の戦略となる。

4.1.3 動的モデルにおける FG の期待利益

上記の LMA と DED で CCG を行った場合の FG の期待利益は、防御者が式 (20)、攻撃者が式 (21) のようになる。δ は攻撃者の戦略 (次に動くまでの間隔) であり、λ は防御者の戦略 (確率密度関数のパラメータの値) である。式 (10)、(11) における p はこのモデルにおいて $\frac{1-e^{-\lambda\delta}}{\lambda\delta}$ となる。

$$\bar{u}^F_{t_D} = \bar{u}^S_{t_D}(1 - \frac{1 - e^{-\lambda\delta}}{\lambda\delta}) - \lambda k_{t_D} \tag{20}$$

$$\bar{u}^F_{t_A} = \bar{u}^S_{t_A}(\frac{1 - e^{-\lambda\delta}}{\lambda\delta}) - \frac{k_{t_A}}{\delta} \tag{21}$$

4.2 均衡条件

式 (12), (13) に式 (20), (21) を当てはめて均衡点 (GNE) の条件を求めた。以下の式 (22)〜(26) 全てを満たす FG における戦略を攻撃者、防御者がとったとき、SG における均衡状態が EQ_L1

の場合 GNE が存在する。また $w = \lambda\delta$ とする。

$$\lambda < \frac{\bar{u}^S_{t_A}}{k_{t_A}} \tag{22}$$

$$e^{-\lambda}(1+\lambda\delta) = 1 - \frac{\lambda k_{t_A}}{\bar{u}^S_{t_A}} \tag{23}$$

$$\frac{\bar{u}^S_{t_A} k_{t_D}}{\bar{u}^S_{t_D} k_{t_A}} = \frac{e^w - w - 1}{w^3} \tag{24}$$

$$\bar{u}^S_{t_D} = u^S_{t_D}(m_L, a_Y) \tag{25}$$

$$\bar{u}^S_{t_A} = u^S_{t_A}(m_L, a_Y) \tag{26}$$

5 数値実験

下記の 1〜3 のセットを 100 回繰り返し、攻撃者、防御者それぞれの SG の期待利益、FG の戦略の変動の有無を調べた。また、SG の戦略更新に用いた ARP モデルの値は、Bereby-Meyer & Erev[5] の研究から $(\phi, v, \varepsilon, c^+, c^-, q_n(0)) = (0.001, 0.0001, 0.2, 0.01, 0.02, 1000)$ とした。

1. 最初はランダムな戦略の LMA と DED, DDED で FG $(time < 10000)$ を行い、その毎にリソースを所有している方が、デバイスと SG(攻撃者、防御者合わせて 10000 回 SG) を行う。1 回 SG を行う毎に SG を行ったプレイヤーは SG の戦略を更新していく。

2. 上記 1 の後、SG の期待利益を求める。SG の期待利益から攻撃者、防御者は自身の FG の期待利益が最大になるような FG の戦略を求める。その戦略同士がナッシュ均衡となるまでお互いの戦略を更新する。

3. 2 で更新した FG の戦略で再度 1 を行う。SG の戦略はランダムにリセットを行う。ここまでで 1 セット。

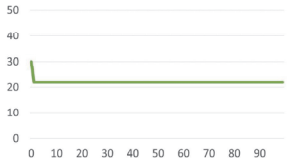
また、SG の利得は表 3 のように設定した。左の数字が送り手側、右の数字が受け手側の利得である。

表 3: SG の利益表

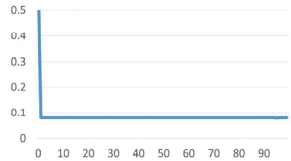
(送り手, 受け手)		デバイス	
		a_Y	a_N
攻撃者	m_L	$(12, -1)$	$(-40, 10)$
	m_H	$(30, -40)$	$(-40, 10)$
防御者	m_L	$(16, 20)$	$(-10, -5)$
	m_H	$(3, 3)$	$(-10, -5)$

5.1 結果

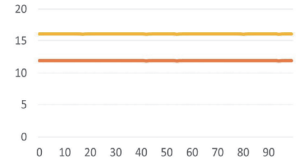
結果を図 2〜5 にまとめた。(1) のグラフは攻撃者の戦略 δ の偏移であり、縦軸が戦略である。(2) のグラフは防御者の戦略 λ の偏移であり、縦軸が戦略である。(3) のグラフは攻撃者と防御者の SG における期待利益の偏移であり、縦軸が期待利益である。濃い色 (赤) が攻撃者の期待利益で、薄い色 (黄色) が防御者の期待利益である。どのグラフも横軸はセット数を表している。



(1) 攻撃者の戦略 δ

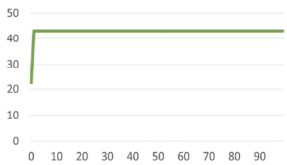


(2) 防御者の戦略 λ

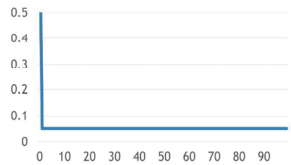


(3) 期待利益 $\bar{u}^S_{t_D}, \bar{u}^S_{t_A}$

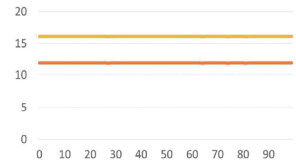
図 2: $(k_{t_D} = 60, k_{t_A} = 80, \Delta = 0)$ での $\delta, \lambda, \bar{u}^S_{t_D}, \bar{u}^S_{t_A}$ の偏移



(1) 攻撃者の戦略 δ

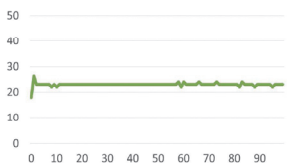


(2) 防御者の戦略 λ

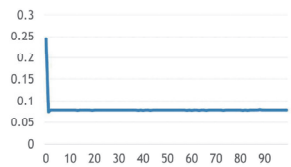


(3) 期待利益 $\bar{u}^S_{t_D}, \bar{u}^S_{t_A}$

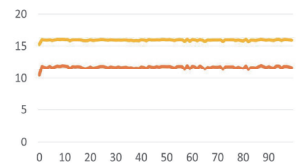
図 3: $(k_{t_D} = 90, k_{t_A} = 150, \Delta = 0)$ での $\delta, \lambda, \bar{u}^S_{t_D}, \bar{u}^S_{t_A}$ の偏移



(1) 攻撃者の戦略 δ

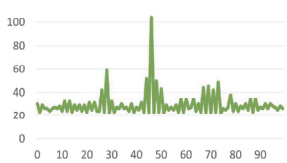


(2) 防御者の戦略 λ

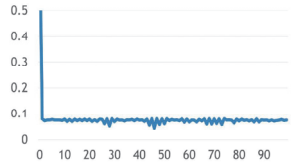


(3) 期待利益 $\bar{u}^S_{t_D}, \bar{u}^S_{t_A}$

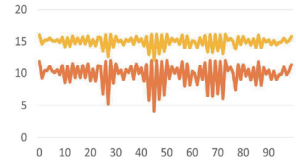
図 4: $(k_{t_D} = 60, k_{t_A} = 80, \Delta = 15)$ での $\delta, \lambda, \bar{u}^S_{t_D}, \bar{u}^S_{t_A}$ の偏移



(1) 攻撃者の戦略 δ



(2) 防御者の戦略 λ



(3) 期待利益 $\bar{u}^S_{t_D}, \bar{u}^S_{t_A}$

図 5: $(k_{t_D} = 60, k_{t_A} = 80, \Delta = 30)$ での $\delta, \lambda, \bar{u}^S_{t_D}, \bar{u}^S_{t_A}$ の偏移

5.2 考察

高等な戦略 (LM) をとる攻撃者 (APTs) に対しては防御者は DED や DDED などの戦略をとることで、初期のランダムな状況の劣勢を回避できた。そして LM, DED, DDED 等の動的な戦略を用いても GNE は存在した。だが、k_{t_D}, k_{t_A} や SG の利得設定 ($k_{t_D} << k_{t_A}$ など) によっては SG の利益条件を満たしていても均衡式を満たしておらず、攻撃者が動かない選択をする場合も存在した。また、DDED の Δ の値によっては均衡点が存在しない結果が得られた。値 δ と比較して値 Δ が大きすぎると防御者の戦略は DP を行った後、DED の動きになるので、攻撃者に防御者が DP を行っている間は隙を与えることになる。よって、適切な値 Δ を模索しなければならないと推測される。

6 まとめ

GNE は動的なモデルにおいても存在することがいえる。この均衡を利用することで、サイバー上の保険、商業投資、企業方針に役立つと考えられる。今後の研究では、DDED の値 Δ によって均衡にどういった影響を与えるのかを解明することが重要な課題となる。また、DED、DDED 以外に LM に対する有効な戦略を発見し、その戦略における GNE の存在を明らかにしたい。

参考文献

[1] Pawlick, J., Q. Zhu (2017) Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control, *IEEE Transactions on Information Forensics and Security*, 12, 2906 - 2919.

[2] Pawlick, J., S. Farhang, Q. Zhu (2015) Flip the cloud: cyber-physical signaling games in the presence of advanced persistent threats, *Lecture Notes in Computer Science*, 9406, Springer, 289-308.

[3] van Dijk, M., A. Juels, A. Oprea, R. L. Riveat (2013) Flipit: the game of "stealthy takeover", *Journal of Cryptology*, 26, 655-713.

[4] Barrett, J. A. (2006) Numerical simulations of the Lewis signaling game: learning strategies, pooling equilibria, and the evolution of grammar, *Technical Report MBS* 06-09, University of California.

[5] Bereby-Meyer, Y., I. Erev (1998) On learning to become a successful loser: A comparison of alternative abstractions of learning processes in the loss domain, *Journal of Mathematical Psychology*, 42, 266-286.