平成 25 年度卒業論文

論文題目

サイバー攻撃に対するゲーム理論を使用した防御戦略

神奈川大学 工学部 電子情報フロンティア学科
学籍番号　200902785
前川　稔

指導担当者　木下宏揚　教授

目 次

図 目 次

第1章　序論

1.1　背景

今現在、インターネットの普及により、あらゆるところでインターネットが使われるようになった。あらゆるところのあらゆる機能がシステム化されており、それにより管理されている。
サイバー攻撃の被害は増しており、その動機も「いたずら」や「能力の誇示」から「金銭目的」「組織活動の妨害」に変化している。
金銭目的の場合、攻撃者は組織の内部にある機密情報や個人情報などを狙っており、それらを使って最終的に金銭化することが目的で悪用される可能性が高くなる。組織活動の妨害の場合、社会的混乱を狙ったサイバー攻撃として、政治的・思想的な動機で標的の組織に対して打撃を与えることを目的とした事例も増えている。
多くの重要な情報がネットワーク上に存在しており、それを狙ったサイバー攻撃が増加している。我が国では2007年に標的型サイバー攻撃を受けた経験のある企業が5.4％であったところ、2011年には33％になるというように、標的型サイバー攻撃が急増している。そのため、情報を守るためにサイバー攻撃に対する警戒や対策を検討し行う必要がある。

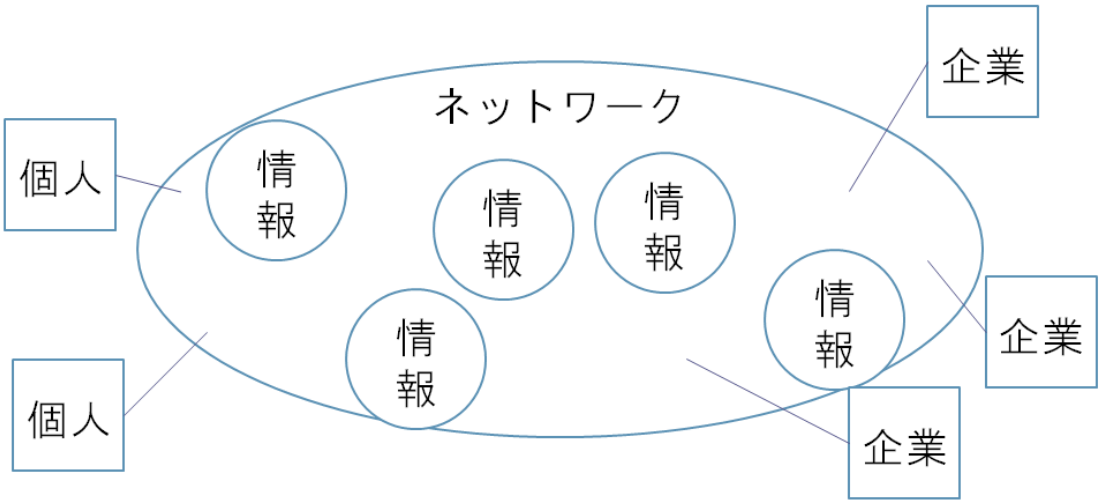

図 1.1: ネットワーク上の情報

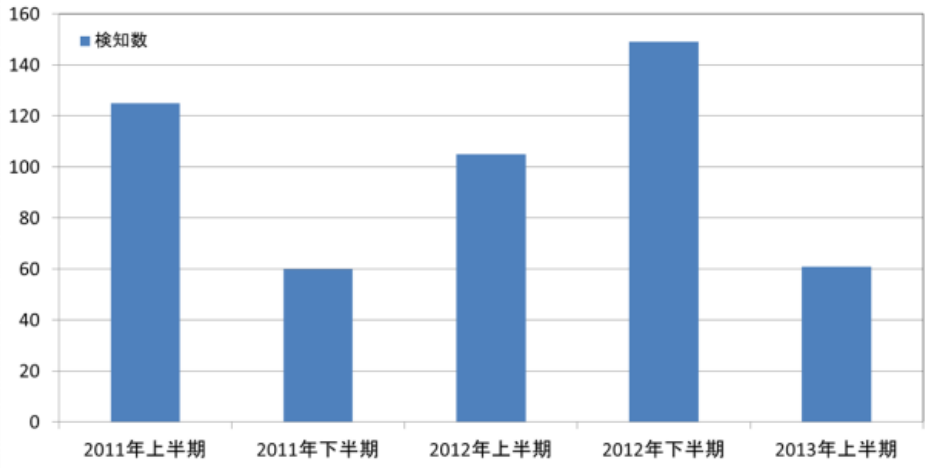

図 1.2: 標的型攻撃の検知件数

この図 1.2 では標的型攻撃は 2012 年下半期と比較して約 4 割減少しているが、攻撃そのものが減少したわけではなく、暗号化や難読化などのセキュリティ機器の検知を回避する手法によって、見えない化が進んだためと考えらる。

1.2 問題点

従来のセキュリティ対策の考え方では情報を、インターネット側を外部、イントラネット側を内部、DMZ という 3 つの境界線でセグメントを分けてセキュリティ対策を行ってきた。従来のえ方では、外から内側への攻撃の対策を考え対策を行っている。しかし、最近のサーバー環境ではデータセンターやクラウドサービスを利用することもあり、今までのセキュリティの考え方が当てはまらなくなってきている。サイバー攻撃に対する対策法として一番なのは攻撃の上流で攻撃に気づき攻撃を回避する事が望ましいが、100 %のセキュリティはなく、攻撃側も回避されないよう巧みに行動するため、完全に回避することは難しい。
防御側が情報を守るために使用する費用が無限であれば、すべての情報に等分に費用を配分すれば良いが、現実では費用は有限である。そのため情報の防御にも強弱が生まれてしまい、重要な情報が弱い防御であれば大きな損失を負ってしまう。情報の重要度に応じて効率的に防御を配分する必要がある。

1.3 提案

情報の防御のために配分できる費用は無限ではない。情報の重要度に応じて効率的に費用を配分し、被害を抑えなければならない。
利得・損失を分析するすることに有用であるゲーム理論を使用することによって、防御側の損失を最低に抑えるような手法を提案する。
ゲーム理論の定理を用いる事によってあらかじめ、ある程度の損失を算出することができ、効率的な戦略を組み立てることが可能になるはずである。最近サイバー攻撃に対する、攻撃側・防御側の戦略をゲーム理論を用いてモデル化している研究が行われている。

第2章　基礎知識

2.1　サイバー攻撃

サイバー攻撃とは、コンピュータシステムやインターネットなどを利用して、標的のコンピュータやネットワークに不正に侵入してデータの詐取や破壊、改ざんなどを行なったり、標的のシステムを機能不全に陥らせることをいう。
特定の標的に対して情報の詐取や破壊を行う攻撃を標的型攻撃と呼ぶ。システムそのものを機能不全に陥らせる攻撃をサービス不能攻撃（DoS/DDoS 攻撃）と呼ぶ。サイバー攻撃の手法として、

- Web サイトに侵入して内容を改ざんする。
- 大量のアクセスを集中させて機能不全に陥らせる (DoS 攻撃/DDoS 攻撃)
- コンピュータウイルスを添付した電子メールを大量に送信する。
  といったものがある。

このほかに、web サイトそのものにウィルスを添付しておく地雷型等々、様々な種類、形式が存在する。
特に標的型攻撃と呼ばれるものが複雑化しており、被害も金銭などと直接関係するためより注意が必要だと考える。

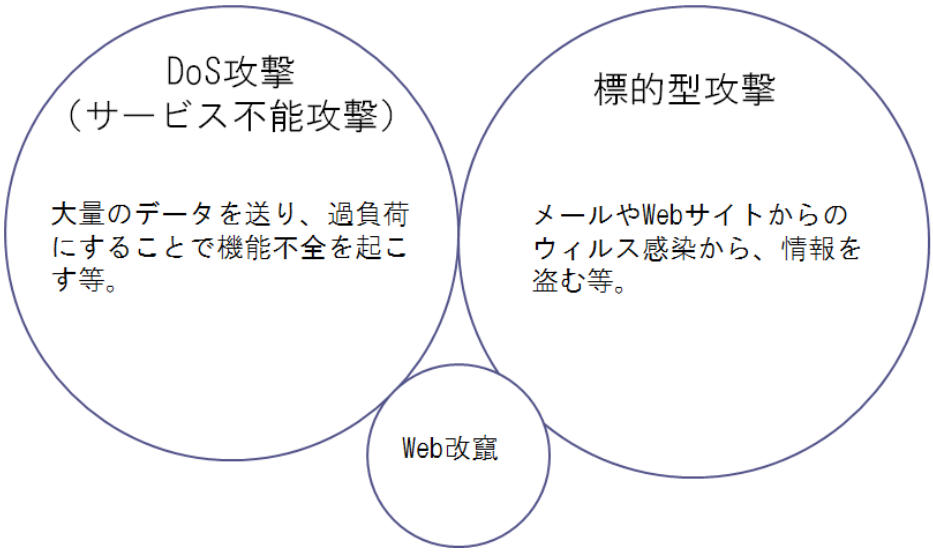

図 2.1: サイバー攻撃の種類

2.2 ゲーム理論

ゲーム理論とは、経済学、政治学、社会学など社会科学における人間の行動を厳密に数学を用いて分析することを目標とした学問である。[1]
ゲーム理論にはいくつかの主要な分類がある。

- プレイヤー間の関係を表現する用語として各プレイヤーが相談することなく自己決定のみによって行動する非協力ゲーム。
- 互いに相談を通じて行動を規制しあう協力ゲーム
- プレイヤーが行動を一回だけ選択して終了する一段階ゲーム。
- 複数の段階にわたって選択がなされる多段階ゲーム。また、ゲームにおいて全ての一連の行動を戦略と呼ぶが、プレイヤーが採る戦略の数が有限である有限ゲーム。
- 戦略が有限とは言い切れない無限ゲーム。
- 情報を参照することが可能である完全情報ゲーム。
- 情報を参照することが可能とは言い切れない不完全情報ゲームなどがある。

2.2.1 ゲームの種類

- 戦略型ゲーム
  戦略型ゲームまた標準型ゲーム（正規形ゲーム）ともいう。
  展開型ゲームと並び非協力ゲームの基本的表現形式であり、プレイヤー集合、戦略空間、利得関数の 3 つの要素から構成されるゲームである。

- プレイヤー集合
  ゲーム理論でのプレイヤーは，意思決定し行動する主体のことである。
  行動を決定する主体は，個人の場合もあるし，複数の個人からなる組織も 1 人のプレイヤーとなる。
  このゲームは相手プレイヤーが存在してはじめて成立する。
  1 対 1 だけではなく複数のプレイヤーでも成立するため，常にプレーヤーの数を明確にする必要がある。

- 戦略
  各プレイヤーは常に何らかのとりうる行動を持っている。
  行動とは, ある状況における選択肢のことであり、どのような行動をとるかは，その場の条件によって決まる。
  各プレイヤーは自分が選択できる行動から、行動計画を立てることがでる。
  この行動の計画が戦略である。

- 利得
  各プレイヤーが戦略を決定すると、それに応じて各プレイヤーの得ることができる利益が決定する。
  ゲーム理論ではこの利益のことを利得と呼ぶ。また，各プレーヤーの戦略と利得の関係を表す関数が利得関数である

2.2.2 戦略形ゲーム

ゲームを表現する場合、最もシンプルに表現する方法は戦略型ゲームである。戦略型ゲームは、プレイヤー集合、各プレイヤーのとることのできる戦略の集合、利得関数の記述によってゲームを表現する。なお、戦略形ゲームは標準型ゲームと呼ぶ場合もある。

戦略形ゲームの定義

戦略形 n 人ゲームの要素は $\langle N, \{S_i\}_i \in_N, \{f_i\}_i \in_N \rangle$ で表される。
ここで $N = \{1, 2, 3, ..., n\}$ はプレイヤー集合、S_i は戦略の集合 f_i は利得関数の集合である。

$N = \{1, 2, 3, ...n\}$ はプレイヤー集合であり、ゲームにおいて行動を決定する主体の集合である。
S_i は戦略の集合であり、プレイヤーのとりうる行動の計画を戦略という。
S_i はプレイヤー i の戦略の集合であり、戦略の数が m_i 個あれば $S_i =$ {戦略１、戦略２、戦略 3、...戦略 m_i} と表せられる。
各プレイヤーがそれぞれ戦略を決定すると、それに応じて各人の得る利益が決まる。ゲーム理論ではこの利益のことを利得と呼び、各プレイヤーのとる戦略と利得の関係を表す関数が利得関数となる。
プレイヤー i の利得を π_i で表すとき、利得関数は $\pi_i = f_i(s_1, s_2, s_3, ...s_n)(i = 1, 2, ..., n)$ のように表せられる。ここで、$s_1 \in S_1, s_2 \in S_2 ... s_n \in S_n$ である。

2.2.3 双行列ゲーム

プレイヤーの数が 2 のとき、この戦略形ゲームの利得関数は、2 つの要素を持つ利得ベクトルの行列として表現される。それが双行列ゲームという。

双行列ゲームの定義

$|N| = 2$ の戦略形ゲームを双行列ゲームと呼ぶ 双行列ゲームは図 2.2 のように表せられる。.

1＼2	戦略1	戦略2	・・・	戦略i
戦略1	a_{11}, b_{11}	a_{11}, b_{11}	・・・	a_{11}, b_{11}
戦略2	a_{11}, b_{11}	a_{11}, b_{11}	・・・	a_{11}, b_{11}
⋮	⋮	⋮	⋱	⋮
戦略m	a_{11}, b_{11}	a_{11}, b_{11}	・・・	a_{11}, b_{11}

図 2.2: 双行列の表

2.2.4 2 人ゼロ和ゲーム

2 人ゼロ和ゲームはゲーム理論の出発点となったものと言える。ゲーム理論を出発点はフォン・ノイマンとモルゲンシュテルンの著書『ゲームの理論と経済化行動』の中で最初に取り上げられたゲームである。

2 人ゼロ和ゲームの定義

プレイヤー集合が $N = [1, 2]$ であり、各人の戦略集合はそれぞれ S_1, S_2 で与えられているとき、2 人のプレイヤーの利得関数がすべての $s \in S_1$,$t \in S_2$ に対して $\pi_1 = f(s, t), \pi_2 = -f(s, t)$ を満たすときこのゲームを 2 人ゼロ和ゲームと呼ぶ。

2 人ゼロ和ゲームの利得行列

2 人ゼロ和ゲームでは相手と自分の利害が完全に対立している、プレイヤー 2 の利得はプレイヤー 1 の利得の符号を逆にしたものとなるので、一方のプレイヤーの利得を表示すれば、他方の利得はその符号を逆にしたものになる。
2 人ゼロ和ゲームは次のような行列で表現される。このときこの行列は 2 人ゼロ和ゲームの利得行列と呼ばれる。この 2 人ゼロ和ゲームにおいてプレイヤー 1 は通常の利得最大化を目標とするが、プレイヤー 2 は利得行列で表示されえている利得を最小化することが、自分の利得の最大化行動となる。そこで、プレイヤー 1 を最大化プレイヤー、プレイヤー 2 を最小化プレイヤーと呼ぶ。

マックスミニ戦略

一人の意思決定問題において慎重な、有名な行動基準がある。それは、自分のとる選択に応じて、その時起こり得る最悪のケースを考慮し、その中でも最善の結果が生じる選択をとる行動である。これをマックスミニ行動という。
まず、最大化プレイヤーの場合、自分のとる戦略に対する採取尾の利得を、その戦略の補償水準と呼ぶ。マックスミニ行動に対応する戦略はこの保障水運を最大にする戦略であり、マックスミニ戦略と呼ばれている。また、最小化プレイヤーの場合自分のとる選択に対する最大の利得を最小にする戦略となり、ミニマックス戦略と呼ばれている。

マックスミニ戦略とミニマックス戦略の定義

2 人ゼロ和ゲームにおいて、$\min_{t\in 2} f(s*,t)$ =$\max_S s_{\in S1} \min_{t\in S2} f(s,t)$　を満たす戦略　$s*$　をマックスミニ戦略と呼ぶ。さらに、その時この式の与える値をマックスミニ値と呼ぶ。
一方　$max_{s\in S1} f(s,t*) = min_{t\in S} 2max_{s\in S1} f(s,t)$　を満たす戦略　$t*$　をミニマックス戦略と呼ぶ、さらにそのときこの式の与える値をミニマックス値と呼ぶ。

マックス身に戦略とミニマックス戦略の特徴

- マックスミニ値とミニマックス値が一致する。最大化プレイヤーにとってはマックスミニ戦略をとると自分の保障水準を確実に達成できるが、もしこの値が一致していないときマックスミニ値以上の利得を現実する可能性があるため、後悔する可能性がある。この可能性がないことを保証している。

- 相手の戦略の変更に左右されない相手が戦略を変更したとしても、自分の利得が下がることはないので相手の戦略の変更に関して心配する必要がない。

- 利得が変わらない相手の戦略に応じてどの戦略をとるのかを決める必要がなく、どのマックスミニ戦略も相手がミニマックス戦略をとる限りナッシュ均衡となるので、強い行動指針となり得る。

マックスミニ戦略は 2 人の合理的なプレイヤーにとってこれ以上の戦略は見当たらない。その意味で、これらの戦略は 2 人ゼロ和ゲームの最適戦略と呼ばれている。またミニマックス値と一致するマックスミニ値のことをゲームの値という。最大化プレイヤーの得る利得はゲームの値となる。

2.2.5 支配戦略

2 つの戦略の間を比較する基本的関係の 1 つに戦略の間の支配関係がある。
他のプレイヤーの戦略が決まっている状態で考える。このとき，自分が持つ 2 つの戦略 a，b を比較したとき，単純に比較して戦略 a の利得が，戦略 b の利得よりも大きいとき，戦略 a をとったほうがよい。しかし，他のプレイヤーのとる戦略はさまざまに変わるので，比較は容易ではない。ただし，他のプレイヤーのとるすべての戦略の組に対して戦略 a の利得が，戦略 b の利得よりも大きいとき、比較が可能となり，戦略 a をとるべきである．このとき戦略 a は戦略 b を強支配するという。
言い換えると，戦略 b をとるほうが有利な状況は絶対に起こらないため，強支配される戦略はとるべきではない。

2.2.6 逐次消去均衡

すべてのプレイヤーは自分の戦略の中から支配される戦略を削除する。このように削除された戦略を取り除くことによって縮小された戦略型ゲームができる。さらに、このゲームにおいて、もう一度同じように全員にとって支配される戦略を削除する。これを続け、その結果として最終的に残された戦略の組を戦略の逐次消去の結果と呼ぶ。
戦略の逐次消去による結果がただ 1 つになる場合がある。これを逐次消去均衡と呼ぶ。

2.2.7 ナッシュ均衡

ナッシュ均衡は非協力ゲームの理論の基本的な解である。
他のプレイヤーの情報を取得したとき、どのプレイヤーも自分の戦略を変更する事によってより高い利益を得る事のない戦略の組み合わせのことである。

2.2.8 最適反応戦略

逐次消去のプロセスを考えた場合、n 人非協力ゲームの戦略の組 $(S_i, s-i)$ において、自分の i 以外の戦略の組 $s_i \in S_i$ に対し条件 $f_i(S_i, s-i) \geq f_i(t, s-i) \forall t \in S_i$ を満たす戦略 Si を戦略の組 $S-i$ に対するプレイヤー i の最適反応あるいは最適反応戦と呼ぶ。

定義

戦略の組 $S = (S_i, S - i)$ が以下の条件を満たすときナッシュ均衡と呼ぶ。

$$f_i(Si, S_i) \geq fi(t, s_i) \forall t \in Si, \forall i \in N \tag{2.1}$$

ナッシュ均衡を構成するそれぞれの戦略を、ナッシュ均衡戦略と呼ぶ。
ナッシュ均衡戦略とは他の人のある戦略の組と組み合わせてナッシュ均衡を構成することが可能な戦略のことである。
ナッシュ均衡は、自分の戦略を相手の戦略の組に対する最適反応になっているので、相手が戦略を変えない限り、自分は戦略を変える要因を持たないため、相手の戦略に依らず自身の戦略を決める方針とすることができる。
ゲームによってはナッシュ均衡が複数あったり、ナッシュ均衡そのものがないことがある。この場合ナッシュ均衡は戦略の選択の指針にならない。

2.2.9 ブロットー大佐のゲーム

交戦理論の戦闘モデルの双方的な兵力配分のゲームである。
古典的なゲーム問題であり、複数の陣地を一定の総兵力で守る防御側と、一定の総兵力で並べく多くの陣地を攻略したい攻撃側の双方的な最適兵力配分のゲームである。

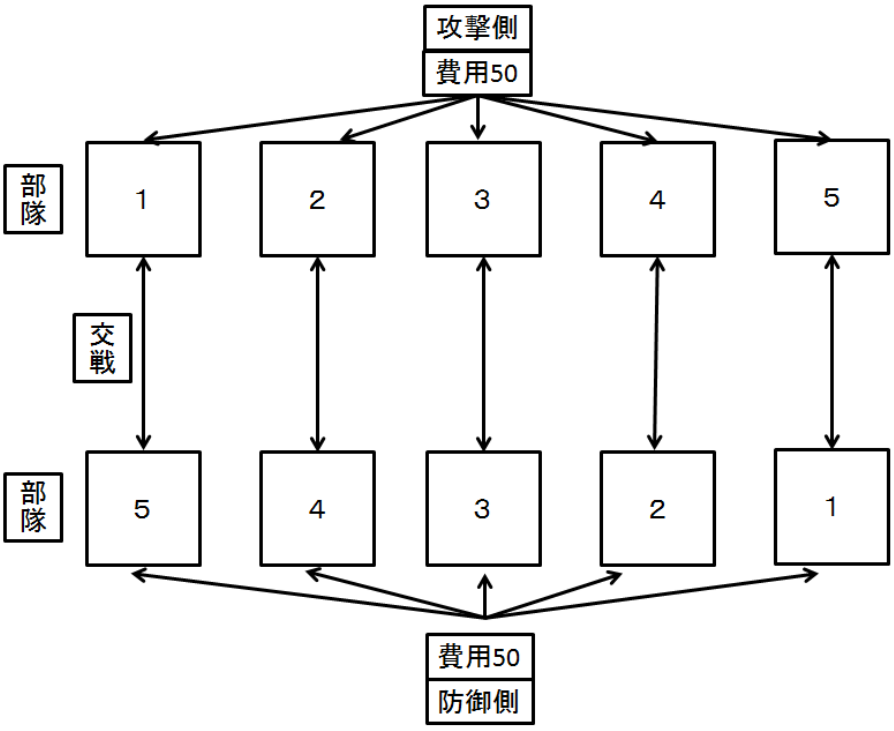

図 2.3: ブロットー大佐のゲーム

2.2.10 探索ゲーム

プレイヤーが参加する探索に関するゲームのこと、段階によっていくつかのゲームがある。
1 段階だけの場合潜伏探索ゲームや待ち伏せゲームといったものがあり、多段階ゲームでは逃避探索ゲーム等がある。
探索ゲームは例外もあるが探索ゲームには 2 人に設定されることが多く、2 人ゼロ和ゲームの研究が大半である。

ブロットー大佐のゲームや探索ゲームは軍事分野での研究が多く使われており、軍事 OR(Operation Research) 等での研究が多くされている。

第3章　提案

3.1　提案

攻撃側と防御側の戦略をあらかじめ想定することで、効率的な費用の分配を決定することができる。利益・損失の結果から、攻撃側は防御側のどの情報が重要であるかを予想でき、防御側はどの情報が危険にさらされているかを考察することができる。
自他の利益損失を計算することの出来るゲーム理論を用いる事で、問題をモデル化し実験を行う。

3.1.1　条件

情報を詐取する攻撃側、守る側の防御側として2人を想定する。
攻撃側は自身の利益を最大になるよう行動し、防御側は被害を最小に抑える行動をとる事とする。
攻撃と防御は単純に数字で表し、この数が大きいものの勝利とする。
情報の価値は両者共に同じであり、お互いにどの情報に価値があるかを知っているものとする。

3.1.2　順序

２人ゼロ和ゲームを基本に用いることによって、攻撃策と防御策を検討する。
攻撃側を最大化プレイヤー、防御側を最小化プレイヤーとすることで、攻撃側の利益を最大に、防御側の損失を最低になる均衡点となる戦略を探す。
戦略に掛ける費用の配分にはブロットー大佐のゲームを参考にする。
実際に交戦をさせ攻撃側と防御側の利益と損失を求める
その結果から、お互いの戦略に割いた費用の配分を考察し、お互いにより最適な戦略を組み立て交戦させる。
これを繰り返しその結果から、最も効率的な戦略を考察する。.

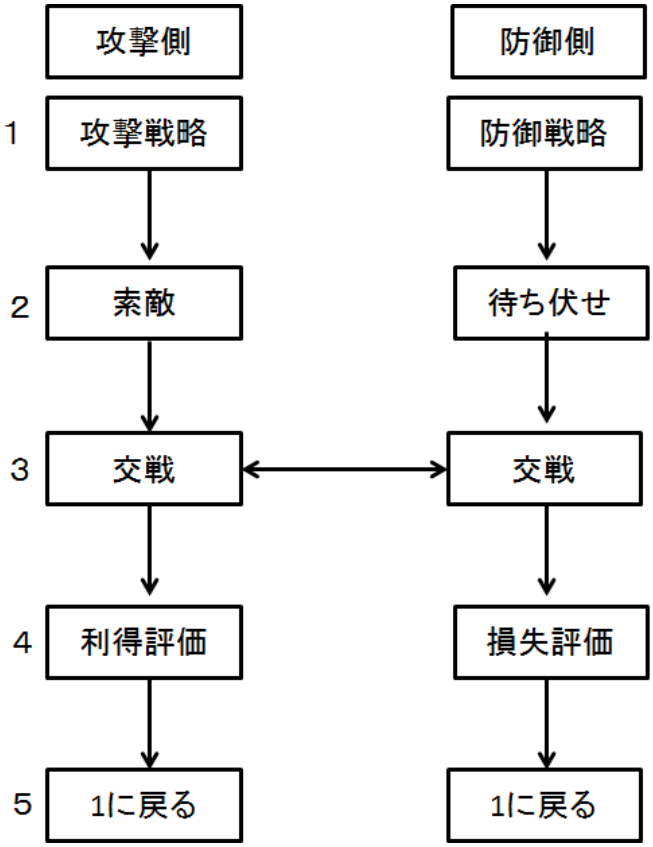

図 3.1: 順番

3.1.3 ゲームの条件

攻撃側と防御側の 2 者間の攻撃・防御戦略ゲームを考える。/2 人ゲーム
お互いに交渉などはしない/非協力ゲーム
お互いに情報の重要度は知っているものとする/情報完備ゲーム
適応動作の無いゲーム/適応型ゲーム
繰り返しのあるゲーム/繰り返しゲーム

第４章　質問された事

Q
戦略 a,b のパラメーターがわからない
どのような関係になっているのか？
A
具体的に答えることができなかった
a が攻撃側、攻撃の戦略とかかる費用とする
b が防御側、防御の戦略とかける費用とする
単純に多くの費用を割いているものが勝利すると考える。

参考文献

[1] 船木由喜彦　「ゲーム理論講義」、新世社、2012 年

[2] 最上　亮 「ゲーム理論を用いた標的型メール攻撃による防御戦略」 神奈川大学 2012 年

[3] 独立行政法人情報処理推進機構　「コンピュータウイルス・不正アクセスの届出状況 [2011 年 6 月分] について」　第 11-25-223 号　2011 年 7 月 5 日

[4] 経済産業省　「最近の動向を踏まえた情報セキュリティ対策の提示と徹底」 http://www.meti.go.jp/press/2011/05/20110527004/20110527004.html

[5] 株式会社リコー　「サイバー攻撃への対策　今、企業に求められるものとは」　情報提供元：トレンドマイクロ株式会社 http://www.rcc.ricoh-japan.co.jp/rcc/special/110712.html

[6] Xiannuan Liang and Yang Xiao, Senior Member, IEEE 「Game Theory for Network Security」 ,IEEE COMMUNICATIONS SURVEYS TUTORIALS, VOL. 15, NO. 1, FIRST QUARTER 2013

[7] 岡田　章　「ゲーム理論の新しい研究動向：限定合理性の探究」　The Operations Research Society of Japan

[8] R.J. オーマン著、丸山徹・立石寛訳　「ゲーム論の基礎」　勁草書房　1991 年

[9] 岡田　章　「ゲーム理論新版 Game Theory New Edition」　株式会社有斐閣　2011 年

[10] 菊田　健作　「文科系のゲーム理論入門」　牧野書店　2012 年

[11] 飯田耕司　「国防の危機管理と軍事 OR」　三恵社　2011 年