Vol.2015-CSEC-71 No.3
2015/12/4

ゲーム理論的思考に基づくサイバー攻撃防御意思決定モデル

佐藤 直[†1]

概要：本文では，機密情報窃取型サイバー攻撃において，攻撃側と防御側それぞれがゲーム理論的な考え方に基づいて戦略をたてる（攻撃策と防御策を選択する）と仮定し，動的に意思決定する手法を検討する．すなわち，攻撃側は攻撃側利益の最大化を図るように攻撃策を選択し，防御側は攻撃策の実施を受けて防御側損失の最小化を図るよう防御策を選択する意思決定モデルを提案する．さらに，同モデルを定式化する．また，提案モデルの適用例を示し有効性を考察する．

キーワード：サイバー攻撃，ゲーム理論，意思決定

Decision Making Model for Defending against Cyber Attacks Based on Game-theoretic Concept

NAOSHI SATO[†1]

Abstract: This paper discusses dynamic decision making process on cyber attacks for stealing classified information, under the game-theoretical assumption that an attacker will act to maximize illegal gain while a defender does to minimize loss due to the attack. The paper develops a decision making model corresponding to the process, where the gain and loss are assessed alternately by the attacker and defender, and attack and defense plans are sequentially determined. The proposed model is formulated and applied to an example of the attack and its effectiveness is illustrated.

Keywords: Cyber Attacks, Game Theory, Decision Making

1. はじめに

近年，特定の組織や個人をターゲットにする標的型サイバー攻撃が相次いで発生しており，その対策の確立は国家的急務となっている．標的型サイバー攻撃は一般にサービス不能型攻撃と機密情報窃取型攻撃に分類される．サービス不能型攻撃の場合は標的組織が公開しているサーバに対して大量のサービス要求をおこなってサービス提供できなくする，あるいは，標的個人に無用な大量のパケットを送り付け，通信帯域を奪って通信できないようにするケースが多い．機密情報窃取型攻撃の場合は，標的型メールに添付されたマルウェアを用いて標的の情報システムに侵入し，機密情報ファイルにアクセスしてバックドアから個人情報などを攻撃側に転送するケースが多い．サービス不能型攻撃はいやがらせ目的でおこなわれることが多く短期間で終了することが多いが，機密情報窃取型攻撃は標的の情報システムの脆弱性や防御策を周到に調べ上げ，標的の情報システムに侵入したあと，長期にわたって密かに攻撃を継続するケースが多い．機密情報は裏社会において高価で取引されるため，機密情報窃取型攻撃は金銭目的におこなわれるといわれている．両者の攻撃のプロセスを比べると，前者は一，二ステップの比較的単純なものが多いのに対し，後者は数ステップ以上の複雑なものが多い．以上のことから，サービス不能型攻撃に比べ，機密情報窃取型攻撃の対策の方が困難となっているのが実状である．

サイバー攻撃の防御策として，ファイアウォールなどによるアクセス制御あるいは機密情報の暗号化保存などといった防御策が多く実施されている．攻撃側が機密情報ファイルに到達するにはこれら何重にも施された防御策（多重防御と呼ばれる）を突破する必要があるが，現実には機密情報窃取型攻撃の被害に会うケースが後を絶たない．この要因として，攻撃側が標的の脆弱性や防御策を事前に十分把握したうえで攻撃していることが挙げられる.すなわち，孫子の名言「敵を知り己を知れば百戦して危うからず」に当てはめれば，攻撃側が敵（＝防御側）をよく知り，防御側が敵（＝攻撃側）を殆ど知らずに，戦っていることになり，効果的な防御がおこなわれていない．敵（＝攻撃側）を全く知らないでいる，という実態は，機密情報窃取型攻撃が発覚するのに要する平均日数が約 200 日を超える[1]ということからもうかがえる．このような，攻撃側・防御側の戦略上の不均衡を是正するには，事前の対策は基本的なもののみとし，代わりに監視機能を強化して，攻撃の予兆や実施された攻撃をできるだけ早期に検出して，攻撃に見合った適切な防御を追加するという動的防御手法が有効であると考えられる．

2. 動的サイバー攻撃防御の提案

本文では，サイバー攻撃において，攻撃側と防御側のとる行動をゲーム理論的にモデル化し，動的に防御策を意思

†1 情報セキュリティ大学院大学情報セキュリティ研究科
Graduate School of Information Security
INSTITUTE of INFORMATION SECURITY

決定する手法を提案する．すなわち，攻撃側は攻撃による利益の最大化を図るように攻撃策を選択すると仮定し，防御側は攻撃策の実施を受けて損失(想定される被害コスト，防御策を実施するコスト，および防御策を実施することによって生じる利便性の低下コストの総和）の最小化を図るよう防御策を選択する，という動的サイバー攻撃防御を提案する．

2.1 提案法の考え方・従来法との比較

従来の防御策は事前に設定され固定しているため，多様な攻撃パタンに適応しにくい．これに対し，提案法では，攻撃開始以降，攻撃終了以前までの攻撃内容に応じて動的に防御策を適用するという特徴を有する．

従来の防御の考え方は,事前に防御策を選択し実施する，ことが基本になっている．この考え方は前述のような優位性を持つ攻撃側に対して必ずしも有効とはいえない．むしろ，事前に意思決定することで防御策が固定している分，攻撃しやすいし，厚い防御を常時適用する場合は運用コストが増大になったり，さらに平常時の情報システムの利便性が低下したりするという欠点が生じる可能性がある．

提案法の考え方は，機密情報窃取型攻撃の継続期間が比較的長期間であることに着目し，攻撃のない平常時には，最低限の防御策のみとし，攻撃に即した防御策を適応的に実施しようとするもので，上記の従来の防御の考え方の欠点が克服されることが期待される．また，攻撃側からみると，事前調査結果にはなかった防御が新たに実施されるため，攻撃の見直しが必要となり，攻撃が遅れ，攻撃成功の確度が低下する，といった不利な状況が発生する．

2.2 前提条件

提案法は，「敵を知る」，すなわち，高い精度でサイバー攻撃やその予兆を検知する監視機能が前提となる．この前提は，近年開発が進んでいる“セキュリティ情報とイベントの管理 SIEM（Security Information and Event Management)”[2]と呼ばれるシステムによって実現されつつある．SIEM は通信機器やコンピュータ端末のログ情報をリアルタイムで監視することによって怪しい動きをしている機器を特定するもので，機密情報窃取型攻撃のみならず，セキュリティインシデント全般をカバーする監視機能として普及すると考えられる．本文はこの SIEM によって攻撃側が実施した攻撃策がリアルタイムに把握できるという仮定のもとで検討する．

以下，第 3 章では，ゲーム理論とサイバー攻撃・防御過程の対応付けをおこなう．次に，第 4 章では機密情報窃取型サイバー攻撃を対象に，ゲーム理論的思考による動的意思決定モデルを提案する．第 5 章では提案モデルを定式化する．第 6 章で提案モデルの適用例を示し，第 7 章で有効性を考察する．

3. ゲーム理論とサイバー攻撃・防御過程の対応

ゲーム理論とは，自分の行動が他人に影響を与える一方で，他人の行動が自分に影響を与える，という相互依存状況を分析する理論体系とみなすことができる[3]．すなわち，自分の行動が相手の利益／損失に影響し，相手の行動が自分の利益／損失に影響するという相互依存状況を検討対象とする．この相互依存状況に関わる関係者のことをプレイヤーと呼ぶ.このプレイヤーは一般的に 2 人以上存在する．通常，プレイヤーにはいくつかの行動の選択肢が存在し，この行動の選択肢を戦略という．プレイヤーは何らかの戦略を採ることによって利得を得ようとする．ゲーム理論はこれら，プレイヤー，戦略，利得／損失を要素とした相互依存状況を定式化して，与えられた問題を解くための手段といえる．

ゲーム理論が取り扱う相互依存状況は次の項目（１）から（７）を用いて特徴づけることができる．本文では，この 7 項目について，以下のようにサイバー攻撃・防御過程の性格を当てはめて検討対象とする．

（１）参加人数・・・2 人ゲーム
攻撃側 1 人，防御側 1 人の 2 人のプレイヤーで構成される．

（２）交渉の方法・・・非協力ゲーム
攻撃側と防御側の間に協力関係が存在しない．

（３）行動の取り方・・・展開型ゲーム
攻撃側は攻撃策を，防御側は防御策を，それぞれ時系列に逐次選択する．

（４）交渉期間・・・繰り返しのあるゲーム
攻撃側と防御側が攻撃策・防御策を 1 つずつ選択し実施する行為を 1 ラウンドとし，サイバー攻撃が終了するまでラウンドを繰り返す．

（５）情報の完備性・・・情報不完備ゲーム
サイバー攻撃に関する情報として以下の①から⑨を仮定する．
①攻撃策に対する防御策の有効性
②標的となる情報システムや情報資産と攻撃策の関係の有無
③攻撃側と防御側が実施する攻撃策および防御策
④攻撃側が選択しうる攻撃策の種類
⑤攻撃成功時に攻撃側が得る収益
⑥攻撃策を実施する場合のコスト（費用）
⑦防御側が選択しうる防御策の種類
⑧攻撃成功時に防御側が喪失する金額
⑨防御策を実施する場合のコスト（費用）

ここで，①から③は攻撃側と防御側の共通知識，④から⑥は攻撃側のみの知識，⑦から⑨は防御側のみの知識とする．このように，④から⑨の情報は共有されず情報不完備である．

（6）主体の内部変化・・・適応型ゲーム
過去に実施された攻撃策と防御策を加味しながら，適応的に新たな攻撃策・防御策を決定する．
（7）合理性・・・限定合理的
攻撃側と防御側はともに情報不完備であることから，限定合理的に意思決定する．

なお，通常，ゲーム理論は同じ価値観で利得を得ようとするプレイヤーを扱う．しかし，サイバー攻撃を含む情報セキュリティインシデントではこのようなプレイヤー間の価値観の同質性が成立しない．すなわち，攻撃側が得る利益と防御側が失う損失の価値は一般には異なり，金額換算した場合，両者は比例する傾向はあると考えられるものの同じではない．例えば，機密情報の価値は攻撃側と防御側とでは異なると考えられる．従って，攻撃側は攻撃側利得を意思決定基準とするが，防御側損失は意思決定基準としないと仮定する．防御側も同様と考える．このように，プレイヤーに価値観の相違があると考えることから，サイバー攻撃をゲーム（理論）として扱うことの是非については別途議論する必要があるが，本文ではゲーム理論的な思考によりサイバー攻撃の攻防のモデル化を検討する．

4. ゲーム理論的思考による動的意思決定モデル

前章までの考察に基づき，ゲーム理論的思考による動的意思決定モデルを提案する．最初にモデル化するための条件を検討する．次に，提案法の機密情報窃取型攻撃への適用イメージを示す．

4.1 モデル化条件

提案法をモデル化にあたって以下の(a)から(d)の条件を与える．

(a) 攻撃策と防御策の意思決定基準

攻撃側は攻撃によって，なにがしかの収益を得ようとする．この収益の例として個人情報や機密情報を不正取得し裏市場で取引して得る収入がある．また，一方で，攻撃システムの構築費，さらに警察等の法執行機関によって逮捕されるリスクをコストとして見積もる必要がある．これらの収益やコストは同一尺度で計量できるとは限らないが，最近のサイバー攻撃は経済的なねらいを持つことが多いことから，全て金額に換算できるものとする．本文では，攻撃側収益から攻撃策の実施コストを差し引いたものを攻撃側利得とよび，攻撃側は攻撃側利得の最大化を図るように意思決定する（攻撃策を選択する）ものとする．一方，防御側は，サイバー攻撃発生時の防御側損失の最小化を図るように意思決定する（防御策を選択する）ものとする．ここで，防御側損失とは，攻撃が成功した場合に失われる資産額(以下逸失額と呼ぶ)と防御策実施コストの和であり，防御側はこの防御側損失の最小化を図る．また，本提案には高精度の監視機能が不可欠であるが，前述したように，この監視機能はセキュリティインシデント全般をカバーする機能と位置付けられることから，同機能の実施コストは勘案しないことにする．

(b)サイバー攻撃・防御過程の開始と終了の条件

サイバー攻撃･防御過程は攻撃から開始するものとする．なお，攻撃側は攻撃開始前に防御側について事前調査するのが一般的であるが，簡単のため本文ではこの事前調査の過程や関連するコストは考慮しない．

次に，サイバー攻撃・防御過程における一組の攻撃と防御をラウンドと呼び，時系列にラウンドが展開されるものとする．サイバー攻撃・防御過程の終了については以下の三つのケース 1，2，3 を想定する．ケース 1 は攻撃コストの累積値が予め設定した閾値（制限値）を超えた場合で，この場合攻撃を中止する．ケース 2 は，攻撃を続行しても攻撃側利益が見込めない場合で，この場合も攻撃を中止する．各ラウンド前に想定される攻撃側利益の最大値がゼロもしくは負の場合がこのケースに相当する．ケース 3 は，ケース 1 とケース 2 の判断がされないまま，攻撃側が可能な攻撃策を全て実施し尽した場合である．

(c)攻撃策と攻撃側収益の条件

全ての攻撃策について必ず防御策が存在するものとする．攻撃策が成功するのは対応する防御策の実施が遅れたためであると考える．この遅延が大きい程実施した攻撃策の成功確率は大きくなるものとする．しかし，実施された防御策は対応する攻撃策に対していずれ有効に機能すると考える．このことから，攻撃策は 1 つのラウンドでのみ実施され，後のラウンドで繰り返して実施されることはないものとする．同じ理由から，各ラウンドでは常に新しい攻撃策が実施されるものとする．なお，一つの攻撃策で複数種類の攻撃側収益を得ることも可能とする．

(d)防御策と防御側逸失の条件

サイバー攻撃・防御過程中に実施された一つの防御策は該当するラウンド以降サイバー攻撃・防御過程終了まで有効とし，後のラウンドで実施される他の攻撃策を防御するのにも有効な場合があるものとする．また，各ラウンドでは防御策が実施されないこともある．すなわち，過去のラウンドに実施した防御策が新しい攻撃策にも有効である場合や，全ての防御策を実施し尽した場合，新しい防御策は実施されない．一つの防御策で複数の防御側逸失を防ぐことも可能とする．

4.2 機密情報窃取型攻撃への適用イメージ

提案法を機密情報窃取型攻撃への適用するイメージを以下に示す．

一例として，ある会社の営業部が保有する顧客個人情報（営業部全員がアクセス可能）あるいは人事部が保有する社員個人情報（人事部長他数名のみアクセス可能）が狙われるものとする．攻撃策は標的型メールにマルウェアを添付して，同マルウェアにより直接外部に情報流出する攻撃

策 A と，標的型メールに記載した Web サイトの URL をクリックさせて同マルウェアをダウンロードして情報流出する攻撃策 B があるものとする．防御策として，LAN の境界にプロキシを設置し，外部に転送される全てのファイルをチェックする防御策 A，外部の Web サイトへのアクセスをファイアウォールで制御する防御策 B，およびファイルを暗号化して保存する防御策 C があるものとする．これら攻撃策・防御策はいずれも平常時は実施されない．攻撃側にとって個人情報を得ることは利得であり攻撃策の実施は損失（＝コスト）となる．一方，防御側にとって個人情報が漏えいすること，防御策の実施により利便性が低下すること，はともに損失（＝コスト）となる．前述したように，攻撃側は攻撃側の利益の最大化を図るように攻撃策を選択し，防御側は攻撃策の実施を受けて防御側の損失の最小化を図るよう防御策を選択する．この意思決定の考え方によって，攻撃策 A⇒防御策 A⇒攻撃策 B⇒防御策 C の順に実施される場合，このフローが意思決定モデルとなる．このようなフローとなった理由を時系列で示す．まず，攻撃側はより高値で売れそうな顧客個人情報を狙い，営業部に攻撃策 A を仕掛ける（理由：攻撃策 A は攻撃策 B より実施ステップが少なく低損失なため）．営業部はこの攻撃策 A を受けて防御策 A を選択する（理由：攻撃策 A に対抗しうる防御策は防御策 A と防御策 C であるが，前者の方が低損失と判断されるため）．これが第 1 ラウンドとなる．次に，攻撃側は攻撃策 A が防御策 A の実施により失敗したことを知り，残りの攻撃策 B を人事部長に仕掛け，社員個人情報の窃取を図る．人事部はこの攻撃策 B を受けて防御策 C を選択する（理由：攻撃策 B に対抗しうる防御策は防御策 B と防御策 C であるが，防御策 B は全社員の利便性を低下させるのに対し，防御策 C により利便性が低下するのは人事部長他数名のみであるため）．これが第 2 ラウンドとなる．なお，暗号化された情報を取得しても攻撃側は解読できないため，情報窃取されたとはみなさいものとする．

このフローでは，結局攻撃側はいずれの個人情報も窃取できず攻撃は失敗に終わる．なお，防御側は攻撃終了と判断した場合，実施した防御策を解除するものとする．

5. 提案法の定式化

以下，これまでの検討から提案法の定式化を考える．ここでは，攻撃側は複数の標的（機密情報など窃取の対象）に対していくつかの攻撃シナリオを用意して攻撃する場合を扱う．攻撃シナリオ中の攻撃は予め決められた順番で実施されるものとする．このため，各ラウンドの攻撃シナリオが選択されると攻撃策は自動的に定まるものとする．一方，防御策は選択された攻撃シナリオにおいて現在のラウンド以降の攻撃策に対応する防御策の中から選択される．従って，攻撃策選択問題は攻撃シナリオ選択問題として，および防御策選択問題は選択された攻撃シナリオに対する防御策の選択問題として定式化する．定式化に用いる諸量を以下に列挙する．

（１）変数（範囲）

r：ラウンド数（1≦r≦R．R は最大ラウンド数）

j：攻撃策の識別変数（1～J．J は可能な攻撃策の数）

i：防御策の識別変数（1～I．I は可能な防御策の数）

n：攻撃側収益（種類）の識別変数（1～N）

k：防御側逸失（種類）の識別変数（1～K）

m：攻撃シナリオの識別変数（1～M．M は可能な攻撃シナリオの数）

Jm(p)：攻撃シナリオ m 中の p 番目の攻撃策の識別変数（p は 1～K(m)．K(m)は攻撃シナリオ m の中の攻撃策の数（＝ステップ数））

Im(q)：攻撃シナリオ m 中の q 番目の攻撃策に対応する防御策の識別変数（q は p と同じ範囲を持つ）

なお，一つの標的に対する攻撃シナリオが成功した場合，攻撃側／防御側にそれぞれの収益／逸失が発生するものとする．

（２）集合

b0：（サイバー攻撃開始時の）防御策の母集合

br：第 r ラウンドより前に実施された防御策の集合

$s_m(r)$：攻撃シナリオ m について，第 r ラウンドの直前におけるステップ位置（1～K(m)）

（３）攻撃に関わる諸量

$\alpha(r)$：第 r ラウンドで実施される攻撃策 j

C(j)：攻撃策 j の実施コスト

G(n)：攻撃側収益 n の収益額

$\mu(r,m)$：攻撃シナリオ m について，第 r ラウンドでの攻撃側利益額

（４）防御に関わる諸量

$\beta(r)$：第 r ラウンドで実施される防御策 i

D(i)：防御策 i の実施コスト

H(k)：防御側逸失 k の逸失額

$\nu(r,m)$：攻撃シナリオ m について，第 r ラウンドでの防御側損失額

Cm(j)：攻撃シナリオ m が成功するのに必要なコスト（攻撃シナリオ m に含まれる攻撃策コストの和）

（５）パラメータ（定数）

Xj,i：攻撃策 j が防御策 i で防御できる確率

Yj,n：攻撃策 j の攻撃側収益 n に対する有効性
(j が n を得るのに有効なら 1，無効なら 0)

Zj,k：攻撃策 j の防御側逸失 k に対する有効性
(j が k を与えるのに有効なら 1，無効なら 0)

Si,k：防御策 i の防御側逸失 k に対する有効性
(i が k を防ぐのに有効なら 1，無効なら 0)

Ti,n：防御策 i の攻撃側収益 n に対する有効性
(i が n を防ぐのに有効なら 1，無効なら 0)

なお，実施された攻撃策 j が成功した場合，攻撃策 j が

関連する攻撃側収益と防御側逸失が発生する．

参考文献[4]を参考にして，攻撃策選択問題，および防御策選択問題は各々式(1)および式(2)として示される．

攻撃策選択問題

$$\alpha(r)=\{j=J_m(p+1)\mid p=s_m(r),m\in(1\sim M),\ Flag(m)=0,\max_m(\mu(r,m))\}$$
$$\mu(r,m)=\sum_i\sum_n G(n)\prod_{j=J_m(p+1)}^{J_m(K(m))}Y_{j,n}(1-\omega T_{i,n})-C_m(j) \quad (1)$$

$i\in b_0-b_r$のとき　ω=$X_{j,i}$
$i\in b_r$のとき　ω=1

防御策選択問題

$$\beta(r)=\{i=I_m(q)\mid q\in(s_m(r)+1\sim K(m)),\ \ Flag(m)=0,\min_q(\nu(r,m))\}$$
$$\nu(r,m)=\sum_k Z_{\alpha(r),k}(n)(1-\omega S_{i,k})H(k)+D(I_m(q)) \quad (2)$$

$I_m(q)\in b_0-b_r$のとき　ω=$X_{\alpha(r),i}$
$I_m(q)\in b_r$のとき　ω=1

$q>s_m(r)+1$が選択された場合，次 ラウンド以降　$Flag(m)=1$

なお，あるラウンドより後に予定されている攻撃に対して先行して防御策を事前対策として実施した場合，該当する攻撃シナリオは失敗するものとする．失敗すると見込まれる攻撃シナリオに対する攻防は次ラウンド以降におこなわれない．式(1)と式(2)ではこの状態を Flag(m)で示している．すなわち，Flag(m)=0 ／1 はそれぞれ攻撃シナリオ m の攻防の可能性がある／ない状態を表している．最初の攻撃開始時は Flag(m)=0 にセットされる．

6. 適用例

前章で定式化した提案モデルの適用例を示す. 用いた数値は以下の通りである．

・標的の数と攻撃シナリオの数は共に 3．標的と攻撃シナリオは 1 対 1 に対応し，攻撃側収益 n と防御側逸失 k も標的と各々1 対 1 に対応する．
・攻撃ステップ数は全て 2.
・攻撃策 j，防御策 i の種類は 5．それぞれ，攻撃シナリオ m の各ステップの攻撃策 $J_m(p)$，防御策 $I_m(q)$と下記のように対応する．
　$J_1(1)$／$I_1(1)$←攻撃策 1／防御策 1
　$J_1(2)$／$I_1(2)$←攻撃策 3／防御策 3
　$J_2(1)$=$J_3(1)$／$I_2(1)$=$I_3(1)$←攻撃策 2／防御策 2
　$J_2(2)$／$I_2(2)$←攻撃策 4／防御策 4
　$J_3(2)$／$I_3(2)$←攻撃策 5／防御策 5
・ラウンド数 r の最大値 R は攻撃策 j，防御策 i の種類と同じく 5.
・C(j)：攻撃策 j の実施コスト
　C(1)=C(2)=30，C(3)=C(4)=10，C(5)=20.

なお，実施コストの累積値に対する閾値（攻撃を中止するための制限値）は 70.

・G(n)：攻撃側収益 n の収益額
　G(1)=G(2)=G(3)=1000.
・D(i)：防御策 i の実施コスト
　D(1)=D(2)=300，D(3)=D(4)=D(5)=100.
・H(k)：防御側逸失 k の逸失額
　H(1)=H(2)=H(3)=1000.
・確率や有効性に関する定数
　$X_{j,i}$：攻撃策 j に対して防御策 i が即応する場合
　$X_{1,1}$＝0.1，$X_{2,2}$＝0.1，$X_{3,3}$＝0.7，$X_{4,4}$＝0.8，$X_{5,5}$＝0.9
　それ以外の $X_{j,i}$ は 0.
　$X_{j,i}$：攻撃策 j に対して防御策 i が即応しない場合
　$X_{1,1}$＝$X_{2,2}$＝$X_{3,3}$＝$X_{4,4}$＝$X_{5,5}$＝1，それ以外の $X_{j,i}$ は 0.
　$Y_{j,n}$: j=n なら 1, j≠n なら 0. $Z_{j,k}$, $S_{i,k}$, $T_{i,n}$ も $Y_{j,n}$ と同様.

適用結果を図 1 に示す．同図では記号①~④の順に攻撃策，防御策が実施されている．最初に攻撃シナリオ 1 の最初のステップの攻撃策 1 が実施される．これに対し，攻撃シナリオ 1 の防御上最も効果的な防御策 3 が先行して選択される．このように第 1 ラウンドで防御策 3 が先行実施されると，攻撃側が攻撃シナリオ 1 を完了して標的 1 から機密情報を搾取し収益を得ることができない．そこで，攻撃側は第 2 ラウンドで攻撃シナリオ 2 に移行し攻撃策 2 を実施するが，第 1 ラウンドと同様に防御策 4 が先行して選択されるため，標的 2 から収益を得ることはできない．そのため，第 3 ラウンドでは攻撃シナリオ 3 に移行しようとする．攻撃シナリオ 3 の最初のステップに対する防御策 2 が実施されておらず，攻撃策 2 が成功しているため，第 3 ラウンドは攻撃策 5 から開始可能である．この攻撃策 5 を実施すれば攻撃側は標的 3 から収益を得られるのであるが，攻撃策 5 の実施によって **4.1** の(b)のケース 1 が発生するため，攻撃側はこの攻撃策 5 の実施を断念する．結果，この

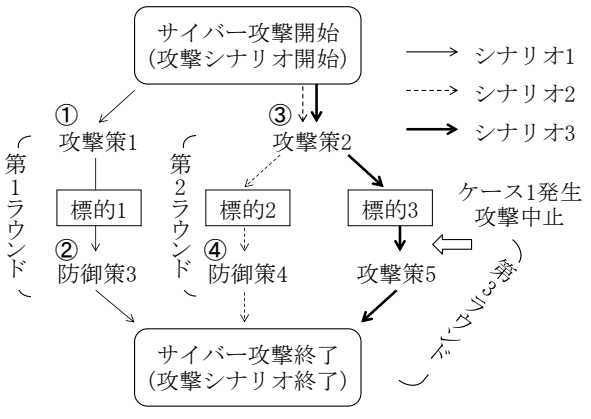

図 1　適用例

適用例では,攻撃側はいずれの標的からも収益が得られず,攻撃策 1 と攻撃策 2 を実施したことによる攻撃側損失額 60 が発生する．防御側については，防御策 3 と防御策 4 を実施したことによる防御側損失額 200 が発生する．

7. 考察

最初に，提案モデルの有効性について考える．本文では，従来のような事前対策でなく，サイバー攻撃発生過程において適応的に防御策を選択することを提案した．サイバー攻撃の検出という点において，本提案は従来の事前対策よりも高い検出精度が必要であり，別途このサイバー攻撃の検出コストを加味する必要があるが，サイバー攻撃の防御自体に関するコストについては適用例で比較することが可能である．例えば，前章の適用例において，防御側の損失額は 200 であった．仮に，事前対策を実施して，全ての防御策を実施した場合の防御策実施額は 900 であるから，この適用例の場合は提案モデルの方が経済的に優れているということになる．

次に，サイバー攻撃に対する提案モデルの適切性について考える．APT（Advanced Persistent Threat）と呼ばれるサイバー攻撃は本文で取り上げたタイプの攻撃である．適用例では，攻撃シナリオ内において直列的に実施される攻撃に即応して防御策を実施するよりも，最も効果的な防御策を選択して先行実施した方が望ましいという結果になった．APT のようなタイプのサイバー攻撃を入口で防ぐのが難しいため“出口対策”が有効である[5]とよくいわれるが，前章の適用例は，このような防御指針の通説と符合している例であることが分かる．

8. おわりに

本文では，サイバー攻撃発生時における攻撃側と防御側の戦略をゲーム理論的にモデル化し，動的に意思決定する手法を検討した．すなわち，攻撃側は攻撃側利益の最大化を図るように攻撃策を選択し，防御側は攻撃策の実施を受けて防御側損失の最小化を図るよう防御策を動的に選択する意思決定モデルを提案した．具体的には，機密情報搾取型のサイバー攻撃を想定し，複数ステップの攻撃で標的を攻略する攻撃について，防御モデルを提案した．さらに，提案モデルを定式化し適用例を示し，防御対策が適切に選択可能であるという見通しを得た．

本文の検討は基本的なものであり，適用する場合は，攻撃・防御に関する諸量の実態を調査する必要がある．

参考文献

1) 日経コンピュータ digital，keyword 標的型攻撃，
http://itpro.nikkeibp.co.jp/atcl/ncd/14/379246/071400027/（2015 年 11 月 8 日）
2) IBM，IBM Security QRadar，
http://www.scsk.jp/sp/sys/products/qradar/（2015 年 11 月 8 日）
3) 例えば，岡田章，ゲーム理論・入門，有斐閣，2008 年.
4) 中村逸一，兵藤敏之，曽我正和，水野忠則，西垣正勝，セキュリティ対策選定の実用的な一手法の提案とその評価，情報処理学会論文誌，Vol.45，No.8，pp.2022-2033，Aug. 2004.
5) 情報処理推進機構,「新しいタイプの攻撃」の対策に向けた設計・運用ガイド改訂第 2 版，
https://www.ipa.go.jp/files/000017308.pdf（2015 年 11 月 8 日）