L-003

標的型サイバー攻撃に関する動的戦略モデル

Dynamic Strategy Model on Targeted Cyber Attacks

佐藤　直† 渡邉　均‡
Naoshi Sato Hitoshi Watanabe

1. まえがき

近年，標的型と呼ばれるサイバー攻撃[1]が増えており，対策手法の確立が求められている．標的型サイバー攻撃では，ソーシャルエンジニアリング的手法を駆使して，標的の情報システムのセキュリティ対策を調べあげ，対策の裏をかいて機密情報を搾取することが多い．このため，標的型サイバー攻撃に対抗するためには，事前のセキュリティ対策（予防策）を強化するだけではなく，サイバー攻撃が進行している過程において，攻撃の進行状況に合わせ適応的に防御する，いわば，インシデントレスポンス[2]の一環として対抗する，ことが必要と考えられる．

そこで，本検討では，標的型サイバー攻撃の過程において，攻撃者利得や防御者損失を動的に評価し，攻撃策と防御策をリアルタイムに逐次意思決定するプロセスをモデル化する．さらに，同モデルを用いて，効果的に標的型サイバー攻撃への防御を行うための方法を検討する．本検討では，この意思決定モデルにおいて，攻撃者と防御者はゲーム理論[3]の思考に基づいて行動すると仮定する．具体的には，攻撃者は得られる利益の最大化を，防御者は自身の損失の最小化を図るよう，それぞれ攻撃策および防御策を交互に選択するものとする．

以下，2. では，ゲーム理論と標的型サイバー攻撃の対応付けをおこなう．次に，3. ではモデル化の条件を示し，4. で標的型サイバー攻撃・防御モデルを提案する．5. では提案モデルの適用例を示す．6. で提案モデルの有効性および応用について考察し，7. で検討をまとめる．

2. ゲーム理論と標的型サイバー攻撃の対応

ゲーム理論では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．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．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であり，次の項目（1）から（7）を用いて特徴づけることができる．本検討では，標的型サイバー攻撃をこの 7 項目について以下のように特徴づけられるゲームとみなす．

（1）参加人数・・・2 人ゲーム
攻撃者 1 人，防御者 1 人の 2 人のプレイヤーで構成．

（2）交渉の方法・・・非協力ゲーム
攻撃者と防御者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
攻撃者は攻撃策を，防御者は防御策を，それぞれ時系列的に逐次選択する．

（4）交渉期間・・・繰り返しのあるゲーム
攻撃者と防御者が攻撃策・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，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
標的型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 標的となる情報資産（機密情報）と攻撃策の関係の有無
③ 攻撃者／防御者が実施した攻撃策／防御策
④ 攻撃者が選択しうる攻撃策の種類
⑤ 攻撃成功時に攻撃者が得る収益
⑥ 攻撃策を実施する場合のコスト（費用）
⑦ 防御者が選択しうる防御策の種類
⑧ 攻撃成功時に防御者が喪失する金額
⑨ 防御策を実施する場合のコスト（費用）

ここで，①から③は攻撃者と防御者の共通知識，④から⑥は攻撃者のみの知識，⑦から⑨は防御者のみの知識とする．このように，④から⑨の情報は共有されないので情報不完備とみなす．

（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
攻撃者と防御者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，ゲーム理論ではプレイヤーが同じ価値観で利得を得ようとする場合を扱う．しかし，標的型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，攻撃者が得る利益と防御者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が同じではない．例えば，機密情報の価値は攻撃者と防御者とでは異なると考えられる．従って，攻撃者は攻撃者利得を意思決定基準とするが，防御者損失は意思決定基準としないと仮定する．防御者も同様と考える．

3. モデル化の条件

前章で示したように，標的型サイバー攻撃における攻撃と防御の過程をゲーム理論的に特徴づけ，モデル化して扱うことを提案する[4]．このモデル化には以下の(a)から(d)の条件が与えられるものとする．

(a) 攻撃策と防御策の意思決定基準
攻撃者は攻撃によって，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，最近の標的型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

† 情報セキュリティ大学院大学
‡ 東京理科大学

ら，全て金額に換算できるものとする．本検討では，攻撃者収益から攻撃策の実施コストを差し引いたものを攻撃者利得とよび，攻撃者は攻撃者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，防御者は，標的型サイバー攻撃発生時の防御者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，防御者損失とは，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，防御者はこの防御者損失の最小化を図る．

(b)標的型サイバー攻撃の開始と終了の条件

攻撃と防御の過程は攻撃から開始するものとする．なお，攻撃者は攻撃開始前に防御者について事前調査するのが一般的であるが，簡単のため本検討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，標的型サイバー攻撃における一対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．標的型サイバー攻撃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者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者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，攻撃者が攻撃シナリオを全て実施し尽した場合である．

(c)攻撃策と攻撃者収益の条件

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．逆に，遅延がない場合，すなわち，事前に攻撃策に対応する防御策が実施される場合の攻撃策の成功確率はゼロとする（すなわち，予防策がとられている場合，攻撃者は該当する攻撃を選択・実施しないものとする）．以上から攻撃策は 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，一つの攻撃策が複数種類の攻撃者収益を得るために実施されることもあるものとする．

(d)防御策と防御者逸失の条件

標的型サイバー攻撃の過程で実施された一つの防御策は該当するラウンド以降標的型サイバー攻撃終了まで有効とし，後のラウンドで実施される他の攻撃を防御するのにも有効な場合があるものとする．なお，一つの防御策で複数種類の防御者逸失を防ぐことも可能とする．

4. 標的型サイバー攻撃・防御モデルの提案

4.1 概要

これまでの検討を踏まえて標的型サイバー攻撃・防御モデルを提案する．最初に提案モデルの概要を示す．ここで，標的型サイバー攻撃の目的はサーバ等に保存してある機密情報の搾取とする．攻撃者は複数の攻撃手段からなる攻撃シナリオ（複数の攻撃策のチェイン）を標的毎に予め定め実行する．攻撃者はこの攻撃シナリオ単位で各標的を攻撃するものとする．標的型メールとダウンローダ型マルウェアの組み合わせが提案モデルの代表的な攻撃シナリオである．本モデルでは攻撃シナリオ内の攻撃策に関して防御者が先読みできるものとする．また，普遍性を持たせるため，1 回の標的型サイバー攻撃において，複数の攻撃シナリオで複数の標的を対象に攻撃するものとする．ただし，一つの標的に対する攻撃シナリオが成功した場合，攻撃者／防御者にそれぞれ一種類の収益／逸失が発生するものとする．

4.2 提案モデルの定式化

これまでの検討から提案モデルを定式化する．

（1）変数（範囲）

ラウンド r（1≦r≦R．R は最大ラウンド数）．

標的および攻撃シナリオ m（1～M．M は攻撃可能な標的および攻撃シナリオの数）．

攻撃シナリオ m 中の p 番目の攻撃策 $J_m(p)$（p は 1～K(m)．K(m)は攻撃シナリオ m に含まれる攻撃策の数（＝ステップ数））．

攻撃シナリオ m 中の q 番目の攻撃策に対応する防御策 $I_m(q)$（q は p と同じ範囲）．

$S_m(r)$：攻撃シナリオ m について，第 r ラウンドの直前までに実施された防御策のステップ位置（0～K(m)-1）．

（2）集合

$\mathbf{b_r}$：第 r ラウンドより前に実施された防御策の集合．

（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．

$\varepsilon(r)$：第 r ラウンド終了時までの攻撃者利益の累積値（期待値）．

$C_m(p)$：攻撃策 $J_m(p)$の実施コスト．

G(m)：攻撃シナリオ m に対する攻撃が成功した場合の攻撃者収益

（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．

$\eta(r)$：第 r ラウンド終了時での防御者損失の累積値（期待値）．

$D_m(p)$：防御策 $I_m(p)$の実施コスト．

H(m)：攻撃シナリオ m に対する攻撃が成功した場合の防御者逸失．

（5）パラメータ（定数）

$\delta_m(p)$：攻撃策 $J_m(p)$が防御策 $I_m(p)$で防御される確率．防御策 $I_m(p)$が攻撃策 $J_m(p)$の実施前，すなわち，予防的に実施された場合は 1，攻撃策 $J_m(p)$の実施に合わせて実施された場合は 0 から 1 の間，攻撃策 $J_m(p)$が実施されても防御策 $I_m(p)$が実施されなかった場合は 0，の値をとる．

なお，実施された攻撃シナリオ m が成功した場合，関連する攻撃者収益 G(m)と防御者逸失 H(m)が発生する．

提案モデルにおいて，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．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一意に定まる．一方，防御策は実施された攻撃シナリオにおいて未実施の防御策の中から選択される．

以上から，提案モデルの攻撃策選択問題と防御策選択問題は次のように定式化することができる．

攻撃策選択問題

$$\alpha(r)=\{\, J_m(p+1) \mid \max_m(\mu_m),\ p=S_m(r),\ \mathrm{Flag}(m)=0,\ m\in(1\sim M)\} \quad (1)$$

$$\mu_m = G(m) - \sum_{j=1}^{K(m)} C_m(j)$$

式(1)において，攻撃者は選択した攻撃策は確率 1 で成功すると仮定している．

防御策選択問題

$$\beta(r)=\{\, I_m(q) \mid \min_{m,q}(\nu_m(q)),\ q\in (S_m(r)+1 \sim K(m)),\ Flag(m)=0,\ m\in(1\sim M)\} \quad (2)$$

$$\nu_m(q)=\delta_m(q)\,H(m)+\sum_{j=1}^{K(m)}\lambda\, D_m(j)+D_m(q)$$

$I_m(q)\in b_r$のとき$\lambda=1$．$I_m(q)\notin b_r$のとき$\lambda=0$

提案モデルにおいて，当該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予防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．攻撃者は失敗すると見込まれる攻撃シナリオについて攻撃策を選択しないものとする．すなわち，該当する攻撃シナリオに関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．攻撃シナリオｍの開始時は Flag(m)=0 にセットされる．攻撃シナリオｍが終了（中止あるいは完了）した場合 Flag(m)=1 となる．

また，第 r ラウンド終了時までの攻撃者利益の累積値（期待値） $\varepsilon(r)$と第 r ラウンド終了時での防御者損失の累積値（期待値） $\eta(r)$はそれぞれ以下のように与えられる．

$$\varepsilon(r)=\sum_{m=1}^{M}\tau_m(r) \quad (3)$$

$$\tau_m(r)=\omega_r G(m)-\sum_{j=1}^{Sm(r)} C_m(j)$$

$$\eta(r)=\sum_{m=1}^{M}\chi_m(r) \quad (4)$$

$$\chi_m(r)=\omega_r H(m)+\sum_{j=1}^{Sm(r)} D_m(j)$$

攻撃シナリオｍが完了していない場合 $\omega_r=0$

攻撃シナリオｍが完了している場合 $\omega_r=\prod_{q=1}^{K(m)}(1-\delta_m(q))$

5. 適用例

提案モデルの二つの適用例；適用例 1，適用例 2 について示す．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 M は両適用例共に 3．標的と攻撃シナリオは 1 対 1 に対応し，攻撃者収益 G(m)，防御者逸失 H(m)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，防御策の種類は 5．適用例 1，適用例 2 それぞれについて，5 つの攻撃策・防御策は，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．

適用例 1；
$J_1(1)$／$I_1(1)$←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

適用例 2；
$J_1(1)$／$I_1(1)$←攻撃策 1／防御策 1
$J_1(2)$／$I_1(2)$←攻撃策 4／防御策 4
$J_2(1)$／$I_2(1)$←攻撃策 2／防御策 2
$J_2(2)=J_3(2)$／$I_2(2)=I_3(2)$←攻撃策 5／防御策 5
$J_3(1)$／$I_3(1)$←攻撃策 3／防御策 3

・ラウンド数の最大値 R は攻撃策・防御策の種類と同じく 5.
・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，適用例 1 で 120，適用例 2 で 80.
・攻撃策の実施コスト；
攻撃策 1 と攻撃策 2 は 30，攻撃策 3 と攻撃策 4 は 10，攻撃策 5 は 20.
・攻撃者収益額は 3 つの攻撃シナリオ全て 1000.
・防御策の実施コスト；
防御策 1 と攻撃策 2 は 300，攻撃策 3，攻撃策 4，攻撃策 5 は 100.
・防御者逸失額は 3 つの攻撃シナリオ全て 1000.
・攻撃策の実施に合わせて対応する防御策が実施された場合の防御できる確率；
防御策 1，2 は 0.1，防御策 3 は 0.7，防御策 4 は 0.8，攻防御策 5 は 0.5.

適用例 1 と適用例 2 の結果を図 1 と図 2 に示す．

図 1 の適用例 1 では記号①~⑥の順に攻撃策，防御策が実施される．ラウンド数は 3 である．第 1 ラウンドではまず攻撃シナリオ 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（防御コストの小さい）防御策 3 が先行して選択される．第 1 ラウンドで防御策 3 が予防策として実施されると，攻撃者が攻撃シナリオ 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，攻撃者は第 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・実施される．このため，攻撃者は標的 2 からも収益を得ることはできない．次に，第 3 ラウンドでは攻撃シナリオ 3 に移行する．攻撃シナリオ 3 の最初のステップに対する攻撃策 2 はすでに第 2 ラウンドで成功しているため（防御策 2 が実施されなかったため），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 が実施されると対応する防御策 5 が実施される．以上から，適用例 1 では，攻撃者は全ての攻撃シナリオを実施し尽くして，すなわち，3.の(a)で示したケース 3 により標的型サイバー攻撃が終了する．

攻撃者の利得と防御者の損失は先に示した数値より与えられる．これらの利得と損失は攻撃シナリオ 3 すなわち標的 3 に対する攻撃シナリオが完了したことによって発生する．攻撃策 2 に対して防御策 2 が実施されず，攻撃策 2 は確率 1 で成功すること，および攻撃策 5 に対して防御策 5 が実施されるが，防御策 5 の成功確率は 0.5 なので，攻撃者は標的 3 から 500（期待値）の収益を得る．また，防御者は 500（期待値）を逸失する．攻撃者は攻撃策 1，2，5 を実施したので，結局，前述の収益 500 から攻撃コストの和 80 を引いた 420 の利益を得る．防御者は防御策 3，4，5 を実施したので，前述の逸失 500 と防御コストの和 300 を合わせた 800 の損失が発生する．

図 2 の適用例 2 では記号①~④の順に攻撃策，防御策が実施される．ラウンド数は 2 である．図 1 の適用例 1 と同

様にして，最初に攻撃シナリオ 1 が次に攻撃シナリオ 2 がそれぞれラウンド 1 とラウンド 2 で実施される．次に，攻撃者は攻撃シナリオ 3 に移行しようとするが，攻撃シナリオ 3 のチェインをなす防御策 5 がすでにラウンド 2 において予防的に実施されているため，攻撃シナリオ 3 においても収益を見込むことができず，攻撃シナリオ 3 に移行せずに攻撃を中止する．すなわち，3.の(a)で示したケース 2 により標的型サイバー攻撃が終了する．

適用例 2 では全ての攻撃シナリオが不完了となるため，攻撃者収益と防御者逸失は発生しない．攻撃者は攻撃策 1 と 2 を実施したので，結局，攻撃コストの和 60 が負の利得となる．防御者は防御策 4 と 5 を実施したので防御コストの和 200 の損失が発生する．

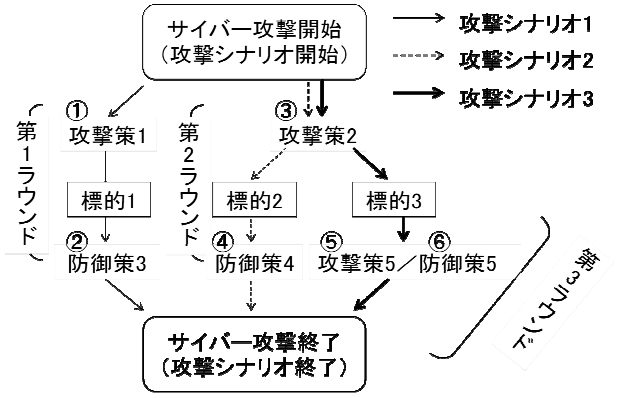

図１　適用例１

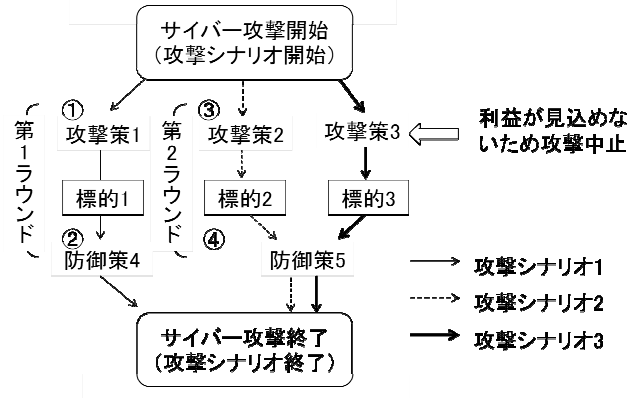

図２　適用例２

6. 考察

最初に，提案モデルの有効性について考える．本検討では，従来のような事前の静的な対策だけでなく，標的型サイバー攻撃の進行過程において動的に防御策を選択して実施することを提案した．標的型サイバー攻撃の検出の点において，本提案は従来の静的対策よりも高い検出精度が必要であり，別途この検出コストを加味する必要があるが，標的型サイバー攻撃の防御者損失自体については，従来の静的対策と提案モデルのような動的対策を比較することが可能である．例えば，適用例 1，2 における，防御者損失はそれぞれ 800，200 であった．従来の静的対策の場合，防御策を予防的に全て実施すると仮定すると，適用例 1，2 ともにコストは 900 であるから，両適用例ともに，提案モデルによる動的対策の方が従来の静的対策より経済的に優れているということになる．

次に，提案モデルの応用について考える．標的型サイバー攻撃は標的となる組織の情報システムやその利用形態，および利用者の特性を調べあげたうえで，弱点を突いて実施することが多い．これらの弱点を完全に克服することは困難と考えられるため，標的型サイバー攻撃を想定したインシデントレスポンスが従来よりも重要になる．例えば，公的機関で実施された標的型不審メール攻撃訓練[5]などを定期的に行うことが望ましい．提案モデルはそのような組織的訓練の設計や評価の基本的手法として応用できると考えられる．企業等の組織ごとに，何が標的となるのか，また，どのような攻撃シナリオが想定されるのか，提案モデルを自らの組織にあてはめ，標的型サイバー攻撃に備えた訓練を実施することが肝要と考える．

7. むすび

本検討では，標的型サイバー攻撃発生時における攻撃者と防御者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，攻撃者は攻撃者利益の最大化を図るように攻撃策を選択し，防御者は攻撃策の実施を受けて防御者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した．具体的には，複数の攻撃策を組み合わせた攻撃シナリオにより標的型サイバー攻撃・防御をシミュレーションするモデルを提案した．さらに，両モデルを定式化し適用例を示した．本検討は基本的なものであり，実用的にするには，攻撃者が防御者を事前調査する，防御者が実施された攻撃策を検出する，といった行動や関連する対策を含めたモデルとする必要がある．また，提案モデルで用いるコストや確率といった諸量をどのように与えるかについても今後の検討課題である．

文　献

[1]情報処理推進機構（IPA）；サイバー攻撃の事例分析と対策レポート，Jan. 2012.
[2]JPCERT/CC；技術メモーコンピュータセキュリティインシデントへの対応，JPCERT-ED-2002-0002，June 2002.
[3]例えば，岡田章；ゲーム理論・入門，有斐閣，2008 年.
[4]佐藤直，渡邉均；サイバー攻撃・防御戦略の動的意思決定モデルの提案，信学技報, vol. 111, no. 495, ICSS2011-47， pp. 49-54，Mar. 2012.
[5]内閣官房情報セキュリティセンター（NISC）；平成 23 年度 標的型不審メール攻撃訓練結果の概要（中間報告），Jan. 2012.