ゲーム理論を用いた標的型メール攻撃による防御戦略

木下研究室　　最上　亮 (200902794)

1　まえがき

近年，サイバー攻撃の中で標的型メール攻撃が増加し，日本では 4 年前に比べ 6 倍もの被害を受けているのが現状である．標的型メール攻撃とは，不特定多数をターゲットにした攻撃ではなく，特定の個人や企業を狙った攻撃であり，ソーシャルエンジニアリング的手法などを使い攻撃を仕掛ける．その動機として「金銭目的」や「組織活動の妨害」などがあげられ，その企業の実施している対策を調べ上げ攻撃を仕掛けることが多い．標的型メール攻撃の対策としては，攻撃に対して適応的に防御していく必要があるため，プレイヤーの状況が逐次的に変化する意思決定問題の分析に効果的なゲーム理論を用いることにする．ゲーム理論とは，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分析するのに有効である．

現在サイバー攻撃における攻撃者，防御者の戦略をゲーム理論を用いてモデル化した研究がおこなわれているが，今回は個人情報に特化し，攻撃者は得られる利得の最大化を，防御者は損失の最小化を図るようなモデル化を提案する．

2　提案モデル

2.1　展開形ゲーム

提案するモデルは，話し合いや相談は行わず協力関係が存在しない展開形ゲームを使った，繰り返しのあるゲームである．複数行われる各ラウンド r において攻撃側 (プレイヤー A) は最大の利得が得られる攻撃策 $\alpha(r)$ を，防御側 (プレイヤー B) は最小の損失で効果的に防ぐことができるような防御策 $\beta(r)$ をともに交互に 1 回ずつ行ったものを 1 ラウンドとし，サイバー攻撃が終了するまで行うモデルである．

これにより，事前に計算を行うことができ，ある程度かかるコストを想定することができるため，サイバー攻撃を効果的に防ぐことができる．

2.2　意思決定

攻撃者利得 $\lambda(r,x)$ は，攻撃者収益 $E(i)=a\times i$，攻撃実施コスト $C(x)$，攻撃成功確率 ω_{xy} から決定し，同様に防御者損失 $\mu(r,y)$ は，攻撃が成功した時に失う財産 $F(j)=a\times j$，防御実施コスト $D(y)$，攻撃成功確率 ω_{xy} から決まるものとする．

攻撃側意思決定

$$\alpha(r)=\{x|x\in m_0-m_r,\max(\lambda(r,x))\} \tag{1}$$

$$\lambda(r,x)=E(i)\times\omega_{xy}-C(x) \tag{2}$$

防御側意思決定

$$\beta(r)=\{y|y\in n_0,\min(\mu(r,y))\} \tag{3}$$

$y\in n_0-n_r$ のとき

$$\mu(r,y)=F(j)\times\omega_{xy}\times T_{\alpha(r)y}+D(y) \tag{4}$$

$y\in n_r$ のとき

$$\mu(r,y)=F(j)\times\omega_{xy}\times T_{\alpha(r)y}\times\quad S \tag{5}$$

$i=j$　：　人数
x　：　攻撃策の選択肢 $(1<x<X)$
y　：　防御策の選択肢 $(1<y<Y)$
m_0　：　攻撃開始時の攻撃策の母集合
m_r　：　第 r ラウンドより前に行われた攻撃策の集合
n_0　：　防御開始時の防御策の母集合
n_r　：　第 r ラウンドより前に行われた防御策の集合
$T_{\alpha(r)y}$　：　攻撃策に対して防御策が有効であれば 1，無効ならば 0

終了条件として，攻撃側の攻撃策がなくなるか，利益が見込めない場合，または閾値を超えたとき攻撃終了とする．

防御策は，過去のラウンドに実施された防御策が新しい攻撃策にも有効な場合，新しい防御策は実施されない．(S：過去のラウンドに防御が成功していれば 0，失敗していれば 1)

2.3　利得の条件

今回のような情報関係の場合，攻撃側，防御側の収益やコストなどの価値観は異なる．個人情報で考えると，攻撃側は 1 件につき a 円で売ることができるとする．しかし，防御側の個人情報漏えいは会社の信頼を失うことにつながるため，価値の相違が生まれる．また実施コストに関しても，攻撃側の捕まるリスクなども含めるため，両者の価値観の同質性が成立することは難しい．そのため，攻撃者の目的として，情報を売買し収入を得たり，経済的なねらいを持つことが多いため金銭換算した場合で考えることとする．

3　評価方法

今回のモデルでは，攻撃側の利得最大，防御側の損失最小になるような値を，ゲーム理論を使用した場合とそうでない場合で比較した結果，使用した場合のほうが防御側の損失が最小になる値を得ることができる．