標的型攻撃に対するゲーム理論を使った防御戦略

木下研究室　　前川　稔 (200902785)

1　まえがき

近年、サイバー攻撃の問題が深刻化しており、国益にまで影響を及ぼすようになっている. サイバー攻撃の対策として理想であるのは攻撃される前にそれを察知し防ぐことであるが、現実的ではない. 攻撃されることを前提にあらかじめある程度の防御策を講じ、損失を最低限に抑え、攻撃者に情報を与えないようにする必要がある. サイバー攻撃を攻撃側と防御側の２者間の行動とすることで、ゲーム理論を使い利益損失を予測する. 今研究の目標として、防御側の総費用、すなわち使用費用、損失、損失を０にする追加費用の総和を最小化することを目標する.

2　提案

攻撃者と防御者の二者に同じ能力のユニットを与え、攻撃側は最大利益を、防御側は最低損失となる様なコスト配分ゲームを行いコスト配分を検討する.
$c=$ コスト として攻撃側・防御側の両者に c = 100 をそれぞれ与え、$c=10$ の単位 でコスト配分を行う. 攻撃側のあらゆる戦略パターンを想定し防御側の使用コストと損失を調べ、損失が０になるよ対策費用の追加を行う. プレイヤーは攻撃と防御の２人なのでプレイヤー集合は $N=2$ 、各戦略の集合はそれぞれ S_1, S_2 で与えられ、２人のプレイヤーの利得関数はすべての $s \in S_1, t \in S_2$ に対して $\pi_1 = f(s,t), \pi_2 = -f(s,t)$ の２人ゼロ和ゲームを行う.
攻撃側はあらゆる攻撃を行い、防御側の損失を算出する.　損失の値から防御側はコストを追加し、損失が０になるようにする.　防御側の費用と損失を確かめ効率的な対策費用の投資となるかを確かめる.　攻撃と防御側の守るべきものが 5 つあり $S_1 = [1,2,3,4,5 \cdots s], S_2 = [1,2,3,4,5 \cdots \mathrm{t}]$ であり、それぞれ A,B,C,D,E としてユニットと呼ぶ.　それぞれ重みとして A=5,B=4,C=3,D=2,E=1 があるとする。$w=$ 費用 として w は $w = c \times [A,B,C,D,E]$ で求める. 利益損失は L で表し、攻撃の利益と防御の損失は同じものである. 防御側は被害を最小限に抑えるミニマックス定理を使用し、コストと損失からコストの追加とそれに伴う費用の増加について検討する. $\max_{s \in S1} f(s,t*) = \min_{t \in S2} \max_{s \in S1} f(s,t)$ を満たす戦略 $t*$ をミニマックス戦略と呼ぶ.

3　結果

すべての戦略を表すと、戦略の数は攻撃側と防御側でそれぞれ 124 通り あり、それぞれの計算を行うと膨大な数になるため利得表の一部を下表に記す.
費用は $w = c \times A + c \times B + c \times C + c \times D + c \times E$
利益損失は $L = c(A-A') + c(B-B') + c(C-C') + c(D-D') + c(E-E')$ で求める

表 1: 攻撃側のコスト配分× 10

	A	B	C	D	E	w	L
戦略 1	1	1	1	1	6	20	25
戦略 2	1	1	1	2	5	21	25
戦略 3	1	1	1	3	4	22	25
戦略 4	1	1	2	1	5	22	25
戦略 5	1	1	2	2	4	23	25

表 2: 防御側ののコスト配分× 10

	A'	B'	C'	D'	E'	w	L	追加
戦略 1	3	3	1	1	2	34	15	56
戦略 2	3	3	1	2	1	35	15	55
戦略 3	3	3	2	1	1	36	15	54
戦略 4	3	4	1	1	1	37	15	53
戦略 5	4	3	1	1	1	38	15	52

表１に攻撃側の戦略の組と使用費用と利益を表す. 表２に防御側の戦略の組と使用費用と損失、損失を０にするための追加コストを表す. L はその戦略をとった時の最大の利益損失である. 追加は損失が 0 となるようにコストを追加した場合の費用. w と L と追加費用の総和 を最終的に使用する最大費用と考える. 表１では $L-w$ がプラスとなる組み合わせで純利益が最大となる戦略の組を表している. 表２はミニマックス定理で最大損失が最小になる戦略の組み合わせである. 表２以外の戦略の組み合わせの場合、総費用は 1060〜1150 となるが、ミニマックス定理を使用した場合一律して最小の値となる 1050 になった. 表２からミニマックス時の使用する費用は最低ではないが、損失を０に近づけるための追加コストを含めた総費用は最小になり、防御側の総費用の最小化することができた. ゲーム理論を用いる事で、防御戦略を効率的に組み立てられると考えられる.