サイバーリスク情報の非協力的な共有ゲーム

西野 卓也[1,2,a)]　大久保 隆夫[2]

概要：サイバー攻撃の観測は，攻撃者による攻撃手法の共有とみなすことができる．一方，攻撃者は攻撃対象が管理できていないサイバーリスク情報を保有することに関心があるため，自身の攻撃手法をなるべく秘匿したいと考えている．本研究では，非協力なプレイヤーによるサイバーリスク情報共有の戦略を，ゲーム理論的な解析が行えるポーカーのモデルに帰着できることを示す．また，その結果から，非協力的な情報共有戦略を分析できる「CRI ホールデム」というセキュリティゲームを新たに提案する．

キーワード：サイバーリスク情報共有，脅威インテリジェンス共有，ゲーム理論，ルダックホールデム

Cyber Risk Information Sharing as a Non-cooperative Game

Takuya Nishino[1,2,a)]　Okubo Takao[2]

Abstract:
Monitoring of cyber attacks can be regarded as sharing of attack methods by attackers. In contrast, since the attackers are interested in holding cyber risk information that can not be managed by the defenders, They want to hide their attack methods as much as possible. In this paper, we show that game theoretic analysis can be performed on strategy of cyber risk information sharing by non-cooperative players.We also propose a game model called "CRI Hold'em" that can be used to analyze for cyber risk information sharing as a non-cooperative game.

Keywords: Cyber Risk Information Sharing, Threat Intelligence Sharing, Game Theory, Leduc Hold'em

1. はじめに

サイバー攻撃の成功は，資産を侵害できるサイバーリスクがあるかどうかで決まる．資産を侵害できるサイバーリスクはカスケードモデル [1] で表され，そこで扱われるサイバーリスク情報は「攻撃情報」「制御情報」「影響情報」という 3 種類 [1] に分類される．一方，いつどのタイミングで，誰にどのような情報を共有するのかは，情報保有者に一任されている．秘密にされた攻撃情報の共有に経済的インセンティブを与えるバグバウンティのような仕組みも存在するが，制御情報・影響情報の観点を含めた場合，非協力的な情報保有者が情報の共有に関してどのような戦略をとるのかは定かでない．

[1] NTT コミュニケーションズ株式会社
NTT Communications Corporation
[2] 情報セキュリティ大学院大学
Institute of Information Security
[a)] takuya.nishino@ntt.com

2. サイバーリスク情報の共有戦略

サイバーリスク情報の共有戦略とは，「誰が」「誰に」「何を」「いつ」共有するのかを考えることである．特に，サイバーリスク情報は，「いつ」共有されたかによって，その情報の価値が大きく左右される．例えば，「周知になった脆弱性に関する情報」と「自分しか知らない脆弱性に関する情報」があった場合，攻撃者がなるべく秘匿したいと考えるのは後者の情報である．合理的な攻撃者は利益最大化を試みるが，それを阻害する要因としは以下の 3 つが挙げられる．

(1) 攻撃対策がなされてしまう
　　（情報資産の直接的な価値低下）
(2) 攻撃手法を分析され，自分以外の人間も知ってしまう
　　（情報資産の間接的な価値低下）

(3) まだ攻撃していない対象へ先に攻撃されてしまう
(攻撃対象の減少)

つまり，攻撃者は自己の利益最大化のため，戦略的に攻撃をしない，攻撃手法を観測させないということが考えられる．これらの関係は，以下のようなフレームワーク [1] によって定義できる．

2.1 登場人物

登場人物は大きく分けて二種類に分けられる．自らの経済的な利点のために， ICT システムのセキュリティを戦略的に弱体化させる者を**攻撃者**と呼ぶ．**防御者**は，攻撃者の行動によって発生するサイバーリスクを戦略的に管理する．攻撃者と防御者は一般的に非協力的な関係にある．

2.2 情報の種類

サイバーリスク情報は三種類に分けられる．**攻撃情報（Attack infomation）**とは脅威や脆弱性に関する情報を指す．**制御情報（Control infomation）**とは，予防や検知に関する情報を指す．**影響情報（Impact infomation）**とは，資産や損失に関する情報を指す．攻撃情報と制御情報と影響情報を組み合わせることで，サイバー攻撃による損失（攻撃者にとっての利得）を評価できる．

2.3 タイミング

情報の共有状態は，タイミングによって三種類に分けられる．自分しか情報を知らない状態を**シークレット**と呼ぶ．信頼できるアクター間でのみ情報が共有されている状態を**プライベート**と呼ぶ．不特定多数のアクターに情報が通知されている状態を**パブリック**と呼ぶ．サイバーリスク情報は，まずシークレットな状態から始まり，シークレットからプライベート，プライベートからパブリックな状態に変化するのが一般的である．

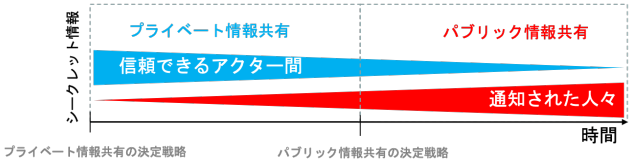

図 1 サイバーリスク情報の共有状態変化

3. チャレンジ

攻撃情報・制御情報・影響情報の観点から，非協力的な情報保有者が情報の共有に関してどのような戦略をとるのか定かでない．

本研究では，攻撃情報・制御情報・影響情報という観点から，非協力なプレイヤーによるサイバーリスク情報共有に関する戦略を，ゲーム理論的な解析が行えるポーカーのモデルに帰着できることを示す．

また，その結果から，サイバーリスク情報の非協力的な共有戦略の分析に使用できる「CRI ホールデム」と呼ばれるセキュリティゲームを新たに提案する．

4. 非協力的な情報共有ゲームの性質

複数のアクターが，自身の利得を最大化するために独立に動くようなゲームを考える．このゲームにおける情報共有とは，利益を確定するための行動である．n 人が参加するような情報共有ゲーム（$n \geq 2$）が考えられるが，本研究では $n = 2$ の場合について考える．

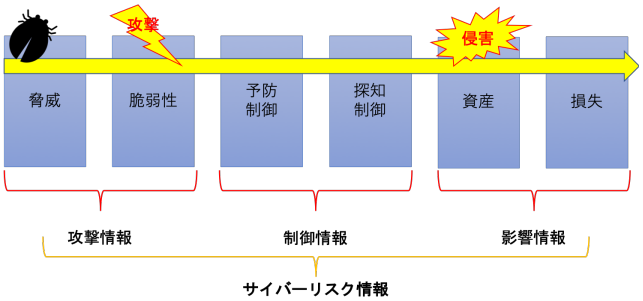

図 2 サイバーリスク侵害のカスケードモデル

プレイヤー P_1, P_2 はそれぞれサイバーリスク情報を保有している．各プレイヤーは，保有しているサイバーリスク情報を組み合わせることで，**サイバー攻撃で資産を得られる状態**を作る．

サイバー攻撃が成功する状態とは，**「攻撃情報」「制御情報」「影響情報」**が図 2 のようにカスケード状に組み合わさっている状態を指す．

プレイヤー P_1 が保有する ICT システムの制御情報を C_1，影響情報を I_1 とすると，プレイヤー P_1 が保有するサイバーリスク情報 $\mathcal{R}_1$ を式 (1) に示す．

$$\mathcal{R}_1 = \{C_1, I_1\} \tag{1}$$

同様に，プレイヤー P_2 が保有するサイバーリスク情報 $\mathcal{R}_2$ は

$$\mathcal{R}_2 = \{C_2, I_2\} \tag{2}$$

このとき，プレイヤー P_2 が，P_1 が保有する ICT システムの情報 (C_1, I_1) だけでなく，C_1 では防ぐことができない攻撃情報 A_1 を保有していたとする．この場合のサイバーリスク情報 $\mathcal{R}_2$ を式 (3) に示す．

$$\mathcal{R}_2 = \{A_1, C_1, I_1, C_2, I_2, \} \tag{3}$$

プレイヤー P_2 は，保有しているサイバーリスク情報 $\{A_1, C_1, I_1, \}$ の組み合わせにより，サイバー攻撃で P_2 の資産を得られる状態を達成している．A_1 の評価額を V_{A_1}，影響情報 I_1 の評価額を V_{I_1} とすると，合理的な攻撃者 P_2

による防御者 P_1 への情報共有 (攻撃) は式 (4) の場合に行われる．

$$V_{I_1} > V_{A_1} \tag{4}$$

このとき，プレイヤー P_1, P_2 の得られる利得 E_1, E_2 は．

$$E_1 = -V_{I_1} + V_{A_1} \tag{5}$$
$$E_2 = V_{I_1} - V_{A_1} \tag{6}$$

4.1 複数の攻撃情報を保有していた場合

プレイヤー P_2 は，C_1 では防ぐことができない攻撃情報として，A_1 の他に $A_1{}', A_1{}''$ を保有していたとする．そのとき，A_2 の評価額を $V_{A_1{}'}$，$A_1{}''$ の評価額を $V_{A_1{}''}$ とし，式 (7) の大小関係を仮定すると．

$$V_{A_1} > V_{A_1{}'} > V_{A_1{}''} \tag{7}$$

プレイヤー P_2 の得られる最大の利得 E_2 は．

$$E_2 = V_{I_1} - V_{A_1{}''} \tag{8}$$

つまり，複数の攻撃情報を保有していた場合は，成功する攻撃手法の中で最もコストが低い組み合わせを利用すると考えられる．今回の仮定の元では $\{A_1{}'', C_1, I_1, \}$ の組み合わせが最適反応となる．

4.2 複数の攻撃情報の組み合わせで利得が変わる場合

プレイヤー P_2 は，C_1 によって対処可能な攻撃情報 A_α, A_β を保有していたとする．このとき，$\{A_\alpha, A_\beta\}$ の組み合わせよって，C_2 では防ぐことができない攻撃情報 A_γ が生じたとする．A_α, A_β それぞれで攻撃した場合の利得 $E_{A_\alpha}, E_{A_\beta}$ と A_γ で攻撃した場合の利得 E_{A_γ} は

$$E_{A_\alpha} = -V_{A_\alpha} \tag{9}$$
$$E_{A_\beta} = -V_{A_\beta} \tag{10}$$
$$E_{A_\gamma} = V_{I_1} - V_{A_\gamma} \tag{11}$$

となる．

4.3 複数の制御情報の組み合わせで利得が変わる場合

プレイヤー P_1 は，A_1 を防ぐことができない制御情報 C_α, C_β を保有していたとする．

このとき，$\{C_\alpha, C_\beta\}$ の組み合わせよって，A_1 を防ぐことができる制御情報 C_γ ができたとする．プレイヤー P_2 において，C_α, C_β それぞれで制御した場合の利得 $E_{C_\alpha}, E_{C_\beta}$ と C_γ で制御した場合の利得 E_{C_γ} は

$$E_{C_\alpha} = V_{I_2} - V_1 \tag{12}$$
$$E_{C_\beta} = V_{I_2} - V_1 \tag{13}$$
$$E_{C_\gamma} = -V_1 \tag{14}$$

となる．

4.4 影響情報の評価額を自己申告する場合

ここでは，影響情報 I の評価額 V_I を参加プレイヤーが自己申告する場合を考える．つまり，ゲーム開始時にプレイヤーが影響情報の評価額を参加プレイヤーに情報共有する．

$$\mathcal{R}_1 = \{C_1, I_1, V_{I_2}\} \tag{15}$$
$$\mathcal{R}_2 = \{C_2, I_2, V_{I_1}\} \tag{16}$$

このとき，プレイヤー P_2 が，P_1 が保有する ICT システムの情報 (C_1, I_1) だけでなく，C_1 では防ぐことができない攻撃情報 A_1 を保有していたとする．この場合のサイバーリスク情報 $\mathcal{R}_2$ を式 (17) に示す．

$$\mathcal{R}_2 = \{A_1, C_1, C_2, I_2, V_{I_1}\} \tag{17}$$

プレイヤー P_2 は，保有しているサイバーリスク情報 $\{A_1, C_1, V_{I_1}\}$ の組み合わせにより，影響情報 I_1 そのものを知らなくとも，式 (4) より合理的な情報共有 (攻撃) かどうか判断できる．

自身が保有するシークレットな情報に関する自己申告の評価付けは，非協力ゲームにおいて掛け金となりえることがある．

4.5 攻撃情報の評価額を自己申告する場合

ここでは，攻撃情報 A の評価額 V_A を参加プレイヤーが自己申告する場合を考える．つまり，ゲーム開始後に攻撃情報を保有しているプレイヤーが，その評価額を参加プレイヤーに情報共有する．

$$\mathcal{R}_1 = \{C_1, I_1, V_{I_2}\} \tag{18}$$
$$\mathcal{R}_2 = \{C_2, I_2, V_{I_1}\} \tag{19}$$

プレイヤー P_2 が攻撃情報 A_1 を得て．ゲームの途中で自己申告する．

$$\mathcal{R}_1 = \{C_1, I_1, V_{A_1}\} \tag{20}$$
$$\mathcal{R}_2 = \{A_1, C_2, I_2, V_{A_1}\} \tag{21}$$

このとき，プレイヤー P_1 は，攻撃情報 A_1 が C_1 では防ぐことができないものであると考えた場合，I_1 が侵害され

る可能性が高いと予想できる．

つまり，プレイヤー P_1 は，保有しているサイバーリスク情報 $\{C_1, I_1, V_{A_1}\}$ の組み合わせにより，攻撃情報 A_1 そのものを知らなくとも，式 (4) の関係から最終的に情報共有 (攻撃) が行われる可能性が高いかどうか判断できる．

自身が保有するシークレットな情報の組み合わせの変化は，非協力ゲームにおいて掛け金を変化させたり，降参する動機になりえることがある．

4.6 攻撃に公開情報が使われる場合

公開情報 $\mathcal{S} = \{A_1, ..., A_n, C_1, ..., C_m, I_1, ..., I_k\}$ があったとする．プレイヤーは公開情報 $\mathcal{S}$ を, 自身が保有するサイバーリスク情報 $\mathcal{R}$ において，$\mathcal{S} \in \mathcal{R}$ とみなしてよい．

つまり，公開情報は参加プレイヤーであれば誰でも自由に使え，攻撃可能なサイバーリスク情報 $\{A_x, C_y, I_z, \}$ のように組み合わせて，任意の参加プレイヤーを攻撃しても良い．逆に，攻撃を受けるプレイヤーは，公開情報を使用して自分に対する攻撃の可能性を予想することができる．

4.7 ルダックホールデム

ポーカーの一種のフロップポーカーだが，フロップポーカーといえば「テキサスホールデム」(Texas hold 'em) が有名だ．フロップポーカーの大きな特徴といえばコミュニティカードの存在である．これは全プレイヤが共通して利用できるカードであり，それて手札を組み合わせることで役をつくることが可能である．

勝ち負けに関するルールは普通のポーカーと変わらず，最終的には残ったプレイヤー同士で手札を見せ合うことで勝敗を決定する．勝ったプレイヤーが参加プレイヤーによって賭けられたチップを全て総取りするゲームである．

テキサスホールデムは非常に状態数が多く，理論的な解析が難しいことが知られているが，これを簡略化したゲームとして，「ルダックホールデム」(Leduc Hold'em)[2] と呼ばれる状態数を削減したトイゲームが存在する．トイゲームとはいっても，テキサスホールデムの基本的な特徴を残しつつ，状態数を削減したゲームであり，有効な戦略を調査する上で非常に役立つと考えられている [3].

本研究では，サイバーリスク情報の非協力的な共有をルダックホールデム (Leduc Hold'em) に帰着させることで，その共有戦略をポーカーゲームのように解析することを可能にする「CRI ホールデム」というゲームを提案する．

5. 非協力的な情報共有ゲームのモデリング

5.1 ルダックホールデムの基本的なルール

ルダックホールデムでは 2 つのスーツ（ハート，スペードなど）と 3 種類のカード（キング，クイーン，ジャック）の計 6 枚のカードを利用する．

ゲームの流れは以下の通りである．

(1) 各プレイヤー（2 名）はチップを 1 枚かけると，手札が一枚ずつ配られる．
(2) 1 回目のベッドラウンド（掛け金を上乗せするフェーズ）開始．プレイヤーは掛け金を増やすか（1 回目の宣言では 2 枚増, 2 回目の宣言ではで 4 枚増），掛け金に同意し同じだけチップをかけるか，ゲームから降りるかを選択できる，
(3) ベッドラウンドのあと，デッキから一枚，コミュニティカードを開示して，各プレイヤーは手札とコミュニティカードを組み合わせて役を作る．
(4) 2 回目のベッドラウンド（掛け金を上乗せするフェーズ）開始．1 回目と同じように，掛け金を増やすか，勝負を続けるか，ゲームから降りるかを選択できる．
(5) 最終的にショーダウン（シークレットな情報の共有）を行い，残っているプレイヤーは手札を見せ合う．このとき，手札とコミュニティカードがペアであれば全てのチップを獲得する．どのプレイヤーもペアになっていない場合は，上位のカードを持っているプレイヤーが勝利する．

5.2 CRI ホールデム

それでは，CRI ホールデム（サイバーリスク情報ホールデム）のルールを説明する．

基本的なルールに変更はないが，トランプの代わりにサイバーリスク情報を使う点が大きな変更点となっている．第 2 章のカスケードモデルを踏まえたペアの作り方，第 4 章の分析を踏まえたカードの強さの関係性の定義を行なっている．

5.2.1 CRI ホールデムで利用するカード

CRI ホールデムでは計 6 種類のカードを利用する．

$$\mathcal{R}_U = \{A_1, A_2, A_3, C_1, C_2, C_3\} \tag{22}$$

トランプのスーツ（ハートやスペード等）に相当する概念として，サイバーリスク情報の種類がある．ここでは「攻撃情報 A」と「制御情報 C」を使用する．影響情報は，掛け金のチップの形で評価されたものとする．

5.2.2 CRI ホールデムのペア

CRI ホールデムでは，以下のようなカードの組み合わせをペアと表現する．

$$\{A_n, C_n\} \tag{23}$$

これは，「制御情報 C_n では防ぐことができない攻撃情報 A_n」と「制御情報 C_n」の組み合わせを意味し，サイバー攻撃で資産（チップ）を得られる状態を示す．

5.2.3 CRI ホールデムにおける情報の強さ

CRI ホールデムにおいて，プレイヤーはなるべく評価額が高い攻撃情報を出したくないモチベーションがある．例

えば，攻撃情報の評価額の関係がこのようなとき

$$V_{A_1} > V_{A_2} > V_{A_3} \tag{24}$$

この中で最も強い攻撃情報は A_1 だと考えられるが，A_1 を共有することは攻撃者にとって大きな損失である，よって，攻撃情報を共有するという観点から考えると，A_3 が最も損失が少ないため出しやすく，A_1 は最も損失が大きいため共有しにくい情報となる．以上を踏まえると，カードの強さ（情報の共有のしやすさ）という関係から式 (25) が成り立つ．

$$A_3 > A_2 > A_1 \tag{25}$$

逆に，制御情報に関しては，弱い制御情報を出すと攻撃される危険性があるため，強い制御情報の共有の方が安全だと考えられる．

$$C_1 > C_2 > C_3 \tag{26}$$

強い制御情報は共有しても安全で，強い攻撃情報はなるべく共有したくないというモチベーションから，式 (27) が成立する．

$$C_n > A_n \tag{27}$$

式 (25) (26) (27) を組み合わせることで，それぞれのカードの強さを一意に決定できる．

$$C_1 > C_2 > C_3 > A_3 > A_2 > A_1 \tag{28}$$

5.3 ゲームの流れ：ペアができた場合

それでは実際にゲームの流れを確認していく．まずはペアができる場合を例示する．

プレイヤー P_1，P_2 は互いにチップを一枚ずつ賭けて，ゲームを開始する．このとき，プレイヤー P_1，P_2 の掛け金（チップの枚数）をそれぞれ V_1，V_2 とすると，以下の状態からゲームが始まることが分かる．

$$V_1 = 1 \tag{29}$$
$$V_2 = 1 \tag{30}$$

各プレイヤーに一枚ずつ手札が配られ，保有するサイバーリスク情報 $\mathcal{R}$ が決まる．

$$\mathcal{R}_1 = \{A_1\} \tag{31}$$
$$\mathcal{R}_2 = \{C_2\} \tag{32}$$

1 回目のベッドラウンドが開始．プレイヤー P_1 は最弱の手札だがチェック（金額はそのまま）を選択，プレイヤー P_2 は 2 番目に強い手札なのでベッド (チップを 2 枚追加).

$$V_1 = 1 \tag{33}$$
$$V_2 = 3 \tag{34}$$

プレイヤー P_1 はコール（金額を揃える），プレイヤー P_2 は 2 番目に強い手札なので更にベッド (チップを 4 枚追加).

$$V_1 = 3 \tag{35}$$
$$V_2 = 7 \tag{36}$$

プレイヤー P_1 はコール（金額を揃える）．2 回レイズしたのでベッドラウンドが終了．

$$V_1 = 7 \tag{37}$$
$$V_2 = 7 \tag{38}$$

デッキから一枚コミュニティカードを引いて公開する．

$$\mathcal{S} = \{C_1\} \tag{39}$$

コミュニティカードによって，プレイヤー P_1 はペアが成立．プレイヤー P_2 はハイカード（何も揃ってない）．

$$\mathcal{R}_1 = \{A_1, C_1\} \tag{40}$$
$$\mathcal{R}_2 = \{C_2, C_1\} \tag{41}$$

2 回目のベッドラウンドが開始．プレイヤー P_1 は P_2 にペアが揃ったことを悟られたくないのでチェック (そのままの金額)．プレイヤー P_2 はペア以外には負けはないのでレイズ (チップを 2 枚追加)．を選択．

$$V_1 = 7 \tag{42}$$
$$V_2 = 9 \tag{43}$$

プレイヤー P_1 はコール（金額を揃える），プレイヤー P_2 は更にベッド (チップを 4 枚追加)．プレイヤー P_1 は負けるはずがないためコール（金額を揃える）を宣言．2 回レイズしたのでベッドラウンドが終了．

$$V_1 = 13 \tag{44}$$
$$V_2 = 13 \tag{45}$$

最終的に手札を見せ合い（ショーダウン）し，ペアのできたプレイヤー P_1 が総取り．プレイヤー P_1, P_2 の利得

E_1, E_2 は以下の通り．

$$E_1 = 26 \tag{46}$$
$$E_2 = -13 \tag{47}$$

5.4 ゲームの流れ：ペアができなかった場合

プレイヤー P_1，P_2 は互いにチップを一枚ずつ賭けて，ゲームを開始する．

$$V_1 = 1 \tag{48}$$
$$V_2 = 1 \tag{49}$$

各プレイヤーに一枚ずつ手札が配られ，保有するサイバーリスク情報 $\mathcal{R}$ が決まる．

$$\mathcal{R}_1 = \{A_2\} \tag{50}$$
$$\mathcal{R}_2 = \{C_3\} \tag{51}$$

1 回目のベッドラウンドが開始．プレイヤー P_1 はチェック（金額はそのまま），プレイヤー P_2 もチェック（そのまま）．ベッドラウンドが終了．

デッキから一枚コミュニティカードを引いて公開する．

$$\mathcal{S} = \{C_1\} \tag{52}$$

両者ペアならず．2 回目のベッドラウンドが開始．両プレイヤーのチェックにより，ベッドラウンドが終了

$$V_1 = 1 \tag{53}$$
$$V_2 = 1 \tag{54}$$

最終的に手札を見せ合い（ショーダウン）し，強いカードを所持していた $(C_3 > A_2)$ プレイヤー P2 がチップを総取り．プレイヤー P_1, P_2 の利得 E_1, E_2 は以下の通り．

$$E_1 = -1 \tag{55}$$
$$E_2 = 2 \tag{56}$$

5.5 ゲームの流れ：試合を降りる場合

プレイヤー P_1，P_2 は互いにチップを一枚ずつ賭けて，ゲームを開始する．

$$V_1 = 1 \tag{57}$$
$$V_2 = 1 \tag{58}$$

各プレイヤーに一枚ずつ手札が配られ，保有するサイバーリスク情報 $\mathcal{R}$ が決まる．

$$\mathcal{R}_1 = \{A_1\} \tag{59}$$
$$\mathcal{R}_2 = \{C_2\} \tag{60}$$

1 回目のベッドラウンドが開始．プレイヤー P_1 は最弱の手札のためフォールド（降参）．残ったプレイヤー P2 がチップを総取り．プレイヤー P_1, P_2 の利得 E_1, E_2 は以下の通り．

$$E_1 = -1 \tag{61}$$
$$E_2 = 2 \tag{62}$$

5.6 結果

本研究では，非協力的な情報共有ゲームの性質を分析することで，非協力的な情報共有の戦略をポーカーの一種とみなして解析できるようなセキュリティゲームを提案した．

サイバーリスク情報の共有戦略，特に脆弱性情報の公開に関しては，多くの研究で議論 [4][5][6][7] されているが，間接的な有益性の議論が多く，攻撃者と防御者の直接的な損得を判断できるものではなかった．今回，直接的に判断できるゲームのモデルを提案したことで，サイバーリスク情報の共有戦略に関してより踏み込んだ解析ができるようになると考えられる．

また，ルダックホールデムに帰着したことにより，攻撃者が攻撃情報を相手に出したくないという部分がナッシュ均衡で説明できるようになった．状態数が増えても CFR[[3]] 等のオンライン学習手法を適用することで，サイバーリスク情報の共有戦略に関してより現実的な解析が可能になると考えられる．

5.7 考察

サイバーリスク情報の共有戦略において，シークレットな状態の情報をいつ誰とプライベートに共有して，いつプライベートな情報をパブリックな状態にするのかは非常に重要な問題 [1] である．

今回提案した「CRI ホールデム」において，ペアを完成させてゲームに勝利した流れは，セキュリティベンダが報告している APT 攻撃の流れに近いものであった．

つまり，「評価が高い制御情報 C_x では防ぐことができない攻撃情報 A_x（ゼロデイ攻撃）」を使って攻撃を仕掛けようとする攻撃者は，相手の影響情報 I_x の評価額 V_{I_x} が大きければ大きいほど，相手がゲームから降りないように慎重な戦略をとるということである．

本研究では 2 人だけの情報共有ゲームを分析の対象としたが，コンピュータを用いたシミュレーション等も含め，

今後はさらに人数を増やしたモデルでの共有戦略の決定に挑戦してみたいと考えている．

参考文献

[1] Stefan Laube and Rainer Böhme. Strategic aspects of cyber risk information sharing. *ACM Comput. Surv.*, Vol. 50, No. 5, pp. 77:1–77:36, November 2017.

[2] Finnegan Southey, Michael Bowling, Bryce Larson, Carmelo Piccione, Neil Burch, Darse Billings, and D. Chris Rayner. Bayes' bluff: Opponent modelling in poker. *CoRR*, Vol. abs/1207.1411, , 2012.

[3] 敬大古居, 晃浦, 誠三輪, 慶雅鶴岡, 隆近山. 相手の抽象化による多人数ポーカーでの戦略の決定. ゲームプログラミングワークショップ 2012 論文集, Vol. 2012, No. 6, pp. 211–218, nov 2012.

[4] Nicholas G. Carr. It doesn't matter. 2003.

[5] Andy Ozment. Improving vulnerability discovery models. In *Proceedings of the 2007 ACM Workshop on Quality of Protection*, QoP '07, pp. 6–11, New York, NY, USA, 2007. ACM.

[6] Ross Anderson, Rainer Böhme, Richard Clayton, and Tyler Moore. Security economics and the internal market. 2008.

[7] Arman M. H. R. Khouzani, Viet Pham, and Carlos Cid. Strategic discovery and sharing of vulnerabilities in competitive environments. in decision and game theory for security, radha poovendran andwalid saad (eds.),lecture notes in computer science, vol.8840. 2014.