# CSIRT の導入と組織内での情報の非対称性の影響に関する理論的考察

小　川　　賢

## 1. はじめに

従来のセキュリティ対策は，組織内からの情報の流出防止に主眼が置かれ，外部から侵入されない，情報漏えいを起こさないためのシステムの設計やスタッフの研修が中心で，機密性を最優先としたセキュリティ対策が行われ，それなりの成果を上げてきた。

攻撃が複雑かつ巧妙になった現代では，悪意のある攻撃者は，組織が従来から行っているセキュリティ対策を熟知し，システムの中で最も侵入しやすいところから侵入を試みる。完璧なセキュリティ対策は存在しないこと，防ぐ側の組織よりも攻撃を試みる側が技術的にも優位となる場合もあり，従来のセキュリティ対策で外部からの攻撃を完全に防ぐことは困難で，攻撃に気づくことすらないまま侵入を許し，情報が漏えいしてしまうこともある。自組織だけでのセキュリティ対策には限界があり，組織外とインシデント情報や攻撃の手口等セキュリティに関する動向や情報を共有し，自組織の対策に反映させることで，自組織のセキュリティ対策のレベルを上げることが必要となっている。

そのような状況のなか，一部の組織では CSIRT（Computer Security Incident Response Team）を設置することで，外部との連絡窓口，自組織以外から得られるインシデント情報の知見，自組織内でのインシデント対応を担うことで，迅速にインシデント対応が可能となりセキュリティ対策が有効になると考えられている。ただし，CSIRT が機能するためには，組織内で自由に活動できる権限が必要である。事前に組織内のリスクを認識するためには組織内の部署の情報や情報システムに関する様々な情報を把握しておくことが必要であるが，部署によっては部内秘にしておきたい情報も存在する。そのような情報ほど外部から狙われる可能性が高くなりがちであるが，十分な権限が付与されていない CSIRT では，事前の把握が困難で，迅速な対応が取れない。

本稿では，CSIRT と情報や情報システムを保有している部署との間で，セキュリティ対策に影響を与える部署の持つ情報セキュリティに関する指標について，情報の非対称性

が存在することで，組織におけるセキュリティ対策が，情報の非対称性が存在しない場合に比し非効率になってしまうことを契約理論のモデルを用いて明らかにする。

## 2．CSIRT

日本シーサート協議会によると，CSIRT とはコンピュータセキュリティにかかるインシデントに対処するための組織の総称[1)]と定義されており，具体的には，インシデント関連情報，脆弱性情報，攻撃予兆情報を常に収集，分析し，対応方針や手順の策定などの活動をします，とある。インシデントへの事後対応だけでなく，事前対応も含まれること，チームとの表現を用いることから，部署単位の場合もあれば，部署横断型，個人，インシデント対応の方針決定などを自社の CSIRT で行い，原因分析などの技術的かつ実務的な部分は，外部の専門業者に委託する等様々な形態があるとされており，統一的な体制の構築方法が存在せず，組織に応じたインシデントに対処するための最善の構成を取ることが肝要となっている。CSIRT を構築し導入することを支援するための協議会によるスターターキットも公開されている[2)]。

政府機関の情報セキュリティ対策の運用等に関する指針[3)]においても，情報セキュリティインシデントに備えた体制の整備として CSIRT を整備することを明記し，情報セキュリティインシデントの認知時における報告・対処として CSIRT を中心としたインシデント対応を明記している。経済産業省は，IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象として作成されたサイバーセキュリティ経営ガイドライン[4)]において経営者に対しセキュリティ対策の一つとして CSIRT の設置を要請し，多くの高等教育機関がセキュリティ対策の参考にしている高等教育機関の情報セキュリティ対策のためのサンプル規程集[5)]にも CSIRT 設置に関する規則が収録されており，各組織による CSIRT の導入に向けた支援環境は整いつつある。

CSIRT の導入は社会的要請，自組織でのセキュリティ対策の向上の観点から有効であり，導入を支援するツールまで提供されており，日本シーサート協議会の加盟チームも2016年１月４日時点で112チームから2017年12月１日時点で266チームに増加しており，CSIRT の設置，導入が進んでいる。

CSRIT の特徴でもある組織の枠を超えたインシデント情報の共有によって，組織外で発生した新たな脅威の情報を入手することで自組織での対応が可能となるが，情報共有は自組織のインシデント情報を組織外に提供することでもあり，インシデントのようなネガティブと解釈される情報を組織外に提供することに批判的な考えをもつ組織トップも少なくない。組織外からもたらされる新たな脅威への対応の知見を得られるメリットと，イン

シデントの発生を完全に防ぐとこが不可能であること，閉じられたコミュニティ内とはいえ内部情報を提供すること，これらのバランスを考慮しても導入は十分なメリットをもたらすと考えられる。

組織内外での情報共有のほかに，組織内での情報の共有も課題として挙げられる。ICT の普及によって組織内での情報共有が進んでいるとはいえ，新規事業や新商品の開発情報，他部署との競争等，部署内で情報を囲い込むインセンティブが存在する。これらの情報は概して価値が高く外部から標的とされやすいが，部外に存在を知られたくないため，組織全体のセキュリティ対策を担う CSIRT のような部署と，私的情報の存在を組織内に知られたくない部署との間で情報の非対称性が発生しやすい。セキュリティ対策を行う部署としては，部署の保有する情報や情報システムが外部からどの程度狙われやすいか，どのような対策を部署で実施されていて，組織全体でどのような対策が取られているか把握する必要があるが，それらがわからないために，組織全体では非効率な対策となってしまう可能性が考えられる。

セキュリティ対策を行う CSIRT に対してどの程度の権限を付与するかは，セキュリティ対策を行う上で重要であるが，権限が弱すぎては適切な対策が実施できず，強すぎては組織内の軋轢にもつながりかねず，セキュリティの確保と CSIRT と組織内の意思疎通の両立は容易ではない。

## 3．先行研究

### 3.1．CSIRT の活動に関する先行研究

見目他［2013a］では，CSIRT の活動が進んでいない要因として CSIRT の高コスト構造に着目し，運用面，特に人的資源管理方式に焦点を当て，提案したトリアージ戦略と脆弱性評価システムの評価基準を合わせたアルゴリズムが，高コスト構造の削減に寄与することを示しており，見目他［2013b］では，CSIRT の活動が進んでいない要因として CSIRT の高コスト構造に着目し，LoA（Level of Assurance）の適用を図ることでレベル分けを行うことで低コスト化の提案と効果の可視化が行えることで経営者の判断を容易にすることができることを示している。

菊池，谷本［2011］では，CSIRT の普及を促すための活動とコストとの関係について考察し，対象とするプロジェクトを構造化，細分化することでその規模を見積もる手法である WBS（Work Breakdown Structure）手法によって CSIRT のコスト構造の可視化を試みている。

### 3.2. 情報システムへの心理学的アプローチ

情報システムの運用や利用に関しては，利用者の行動を考察することの重要性から，心理学等の手法を用いた研究がなされており，セキュリティ対策の推進要因の分析においては，組織内や人的資源に注目されている。例えば，内田［2015］は，ソーシャルエンジニアの主要手法である誘導質問術等の観点から情報漏えいやその対応策としての教育・訓練について分析し，技術的な攻撃のみならず，ソーシャルエンジニアリングの観点からも対策，特に教育・訓練を実施することの有効性を述べている。

島他［2015］では，インシデントの発生は人に起因するものが高い割合を占めていることから，ロジスティック回帰分析を行うことで，インシデントとヒューマンエラーの関係を明らかにし，業務集中の防止や業務意欲低下の防止がインシデントに影響を及ぼすことを明らかにしその対策の必要性を述べている。

浜津他［2015］では，説得心理学の観点から集団防護動機理論に基づく情報セキュリティ対策のための意思決定モデルを考案し，共分散構造分析によりセキュリティ対策の実行意思に，深刻さ認知，効果性認知，生起確率認知が影響することを明らかにしている。

### 3.3. 情報の経済学的アプローチ

情報システムの運用やセキュリティに関してゲーム理論や契約理論等経済学の考え方で問題を分析するセキュリティエコノミクスのアプローチによる分析がなされている。

礒谷他［2010］では，組織の情報セキュリティ対策が進まない現状を，情報セキュリティの持つ不確実性と情報の非対称性から考察し，情報の非対称性が情報セキュリティ対策に及ぼす影響について分析し，情報の非対称性の階層構造が存在することを明らかにしている。

金子［2001］は，複雑で大きなシステムとなったクラウドコンピューティングのように，多数の利害関係者や要素からなる複雑なセキュリティ問題を扱うためのゲーム理論，特にナッシュ均衡モデルと確率モデルの併用を提案し，その有用性を示している。

田中［2011］では，クラウドサービスにおけるセキュリティ対策の情報の非対称性に着目し，米国における政府機関の取り組みと民間の取り組みを比較し，クラウドサービスのセキュリティ対策の社会的コスト負担は情報を保有する側が望ましいという結論を導いている。

インセンティブの考え方を用いて情報システムの特性を分析した研究としては，田仲他［2015］があげられる。ソーシャルネットワーク上での情報伝達の過程にインセンティブ報酬を付与するモデルを考案することで，インセンティブを付与する条件を比較すること

で，行動に違いがみられることを明らかにしている。

栗田，樋口［2012］はクラウドサービスの特性からクラウド事業者と利用者間の情報の非対称性に着目し，利用者にとって選定に必要な情報が得られないことが，普及を阻害する要因と仮定し，シグナリング及び情報不完備ゲームによる理論モデルでの戦略の分析，マルチ・エージェント・シミレーションによる検証を行い，事業者が第三者認証を取得することが，事業者及び利用者双方に情報の非対称性を解消し，利用の普及促進させる点で有効であることを示している。高田，藤田［2013］はスマートフォンンでのモバイルサービスの利用に関してアンケート調査を行い，サービスを利用するきっかけとなった要因について技術受容モデル TAM（Technology Acceptance Model）による分析を行い，周囲の意見や社会的影響が影響を与えていることを明らかにしている。

### 3.4. 契約理論の枠組み

契約理論は，伊藤［2003］によると，情報の非対称性が存在する状況において最適なインセンティブを設計する問題，と述べられており，依頼主であるプリンシパルと代理人であるエージェントの間に，利益に関係する変数について情報の非対称性が存在することで，非対称性が存在しない場合に比して利益に関係する変数がプリンシパルにとって非効率な状態になってしまうことをモデルで分析するものである。

Laffont and Tirole［1993］は，アドバースセレクションとモラルハザードが共存するモデルを構築し，独占企業と政府間の情報の非対称性による問題を分析している。エージェントが自分のタイプを過大に申告して生産費用を節約する効果と，自分のタイプを過少申告して得られる留保効用の過大する効果とが存在することで，エージェントの効用の単調性に議論が必要となる相殺インセンティブの枠組みは Lewis and Shappington［1989a］，［1989b］によって分析が始まった。Maggi and Rodor'igues-Clare［1995］は，彼らは参加制約がエージェントのタイプに依存する場合，その依存形態に従って利潤がどう変化するかを分析している。

### 3.5. 本稿における仮説

これまでの研究から，CSIRT を導入し十分な成果を上げるためには，CSIRT が組織内で自由に活動できる権限を付与されること，組織内の情報や情報システムを有する部署との信頼が醸成されること，部署内の情報や情報システムに関する様々なリスクを把握できること，が重要であることが明らかにされてきたが，情報や情報システムを有する部署と CSIRT のような部門の間での情報共有は容易ではなく非対称性が生じやすい。そこで，

本稿では次のような仮説を置く。

仮説：組織内で情報の非対称性が，CSIRT の運用において非効率な結果をもたらす

本稿での分析は，組織内で機密性が高く外部から狙われる価値のある情報を保有する部署が組織内でのセキュリティ対策の実施の履行等の決定権を有する形態を想定し，この決定権を部署の保有する私的情報のタイプに依存する参加制約とみなし，相殺インセンティブの手法を応用し，組織内での情報の非対称性が CSIRT の活動において非効率な状況をもたらすことを明らかにする。

## 4．分析モデル

ここでは，CSIRT と部署間での情報の非対称性に着目して契約理論を応用し，CSIRT の活動の自由度の高さと，CSIRT と情報や情報システムを保有する部署との間でのリスクに関する情報の共有が組織全体のセキュリティレベルに影響を与えることを理論的に検討する。

### 4.1．モデルの設定

CSIRT の活動レベルを $a$ とおく。具体的には，$a$ は組織内でのセキュリティ対応や事前の体制整備，組織外からのインシデント情報のやりとりの活動等が考えられる。十分なセキュリティ対策を行うためには，それなりの金銭的なコストや非金銭的なプレッシャーなどが生じるが，これを CSIRT の活動コストと呼び $c(a)$ で表す。$\theta$ は部署が持つ情報や情報システムに関するリスクをあらわすパラメーターであるとし，この値が小さいほどリスク管理に優れた部署とであるとする。$\theta$ の確率分布関数を $f(\theta)$ と表し，$\theta \in [\theta_0, \theta_1]$ と仮定する。

組織としての CSIRT 導入によるセキュリティ対策の効果 $r$ は，$r(a, e, \theta)$ と表されるとする。$e$ は，部署のセキュリティ対策の追加の努力レベルである。セキュリティ対策の努力レベルとは，例えば，情報の格付けや格付けに従った取扱い，サイバー攻撃に対応するためのインシデント対応の訓練，セキュリティ教育や研修の実施等，その部署で実施できるセキュリティ対策が考えられる。

従って CSIRT 導入によるセキュリティ対策の評価は，CSIRT の活動レベル $a$，部署のセキュリティ対策の追加の努力レベル $e$ 及び部署が持つ情報や情報システムに関するリスクをあらわすパラメーター $\theta$ に依存する。ここで簡単化のため $r$ の関係を次のような一次

関数で表す。

$$r=a+e-\theta$$

以上の説明から，CSIRT 導入によるセキュリティ対策の効果から，CSIRT の活動に伴うコスト $c(a)$ 及び部署に配当されるセキュリティ対策予算（移転額）$t$ を差し引いたものになるので，

$$r=a+e-\theta-c(a)-t$$

と表される。

次に，部署について説明する。前述のように部署のタイプ $\theta$ はエージェントたる部署の私的情報であり，真の値はエージェントのみが知っていると仮定する。プリンシパルは，部署の持つリスク $\theta$ の確率分布 $f(\theta)$ のみを知っているものとする。リスク $\theta$ の累積密度関数を $F(\theta)$ とし，hazard rate の単調性 $\dfrac{\mathrm{d}}{\mathrm{d}\theta}\dfrac{F(\theta)}{f(\theta)}\geq 0$ を仮定する[6)]。

部署のセキュリティ対策による効用レベルはセキュリティ対策予算と CSIRT の活動によるセキュリティレベルの向上からなる。この効果を効用で表し，それを $v$ と表記する。$v$ は $a$ と $\theta$ の関数であると仮定する。ただし，$v_\theta>0$, $v_{a\theta}>0$, $v_{\theta\theta}>0$ とする。部署の支出としては，努力による非効用 $d(e)$ がある。つまり，要求されたセキュリティレベル $e$ を実現するため，情報の格付けや取扱，研修等様々な努力が必要であるが，それを部署の非効用として $d(e)$ と表す。$d(e)$ の関数形については，$d'(e)>0$, $d''(e)>0$ と仮定する。従って，部署の利得を効用のタームで表すと次のようになる。

$$U=t-v(a,\theta)-d(e)$$

部署は $U$ が負になれば，CSIRT 導入による全組織でのセキュリティ対策の協力を放棄する。つまり，CSIRT 導入によってもたらされるメリットよりもデメリットが多い場合，部署としてセキュリティ対策に協力する意義がないからである。以下の分析では，この $v(a,\ \theta)$ を Lewis and Shappington [1989a], [1989b] によって考察された相殺インセンティブの項とみなして分析を進める[7)]。

CSIRT にとって $e$, $\theta$ は観察不可能で，$a$, $c$, $f(\theta)$ は観察可能である。

### 4.2. ベンチマーク

契約理論では，プリンシパルとエージェントの間に情報の非対称性がなく，エージェントの私的情報が観察できる理想的な状態をファースト・ベストと呼んでいる。本稿では，CSIRT が組織内で適切な権限が与えられ，十分に機能できる場合をベンチマークとして分析する。具体的には部署の持つ指摘情報であるリスク $\theta$ についても CSIRT が把握でき，

リスクに応じた対応が取れる状況を想定し，契約理論のファースト・ベストの解として求める。この CSIRT 導入による CSIRT の評価と部署の効用の総余剰 $W$ は

$$W=a+e-\theta-c(a)+v(a,\theta)-d(e)$$

であり，ファースト・ベストの解は以下の最大化問題を解くことにより得られる。

$$\max_{a,e} W$$

subject to $U=0$

ここで，制約式 $U=0$ は部署が CSIRT 導入による追加のセキュリティ対策を実施するための条件である。

一階の条件は以下のようになる。

$$d'(e)=1 \quad \cdots\cdots(1)$$

$$c'(a)+v_a(a,\theta)=1 \quad \cdots\cdots(2)$$

（１），（２）式より $e^{FB}$, $a^{FB}(\theta)$ が求まり，部署へ配分される予算（移転額）$t^{FB}$ は制約式 $U=0$ より次のように決定される。

$$t^{FB}(\theta)=d(e^{FB})+v(a^{FB},\theta)$$

ここで注意すべき点は，（１）式より部署の追加の努力水準 $e^{FB}$ はタイプ $\theta$ に依存せず一定となることである。

### 4.3. 不完全情報下での分析

#### 4.3.1. ゲームのタイミング

プリンシパルとエージェントの間の取引は，エージェントのタイプに応じた最適契約の設計であるので，ゲームとして記述することができる。このモデルでは，契約締結前にエージェントのみが自分の真のタイプを知っており，プリンシパルとエージェントの間に非対称情報が存在している。そのため，ゲームの開始時点の前に「確率分布 $f(\theta)$ に従って，エージェントの真のタイプが選択され，エージェントのみにそのタイプが知らされる」という手番を加えることで不完全情報ゲームとして記述する。

ゲームのタイミングは以下のようになる。

1．CSIRT が部署に設計したメカニズム（申告させる情報，追加のセキュリティ対策等などのルール）を提案する。

2．部署が受け入れるかどうかを決定する。

3．部署はレポート（申告する情報）を選択し，提出する。

4．CSIRT はメカニズムに従って部署へ配分される予算額（移転額）$t$，努力水準 $e$ を指示する。

5．両者のセキュリティ対策努力がなされ，利得が確定し，メカニズムによって予算額（移転額）が配分される。

### 4.4. セカンド・ベスト

ここでは，CSIRT に部署の間で部署の保有する情報に関するリスクのパラメーター $\theta$ について情報の非対称性が存在し，パラメーターの確率分布しかわからない場合を考える。この場合，目的関数は次のようになる。

$$\max_{a,\,e,\,t}\int_{\theta}^{\theta_1}\{a+e-s-c(a)-t\}f(s)ds \quad \cdots\cdots(3)$$

$$\text{subject to } \dot{U}=-\{d'+v_\theta\} \quad \cdots\cdots(4)$$

$$U\geq 0 \quad \cdots\cdots(5)$$

(4)式は誘因両立性条件で，エージェントがプリンシパルに自分のタイプを偽って申告しても効用は増加しないことを示している。

(5)式は参加制約で，部署がこの提案を受け入れるための条件である。

制約式(5)を目的関数(3)に代入して整理すると(3)式は次のように書き換えられる。

$$\max_{a,e,t}\int_{\theta}^{\theta_1}\{a+p-c(a)-d(p+s)+v(a,\,s)-U\}f(s)ds \quad \cdots\cdots(6)$$

$$\text{subject to } \dot{U}=-\{d'+v_\theta\} \quad \cdots\cdots(7)$$

(6),(7)式よりハミルトニアンは次のようになる。

$$H=\{a+p-c(a)-d(p+\theta)+v(a,\,\theta)-U(\theta)\}f(\theta)-\mu(\theta)\{d'+v_\theta\} \quad \cdots\cdots(8)$$

ただし，$\mu(\theta)$ は制約式の Pontryagin 乗数である。次に一階条件を求める。

このとき $U$ は $\theta$ の減少関数であるので，参加制約は $U(\theta_1)=0$ となる。Transversality Condition を考慮すると，$\mu(\theta)$ は次のようになる。

$$\mu(\theta)=F(\theta) \quad \cdots\cdots(9)$$

(8),(9)式よりハミルトニアンは次のようになる。

$$H=\{a+p-c(a)-d(p+\theta)+v(a,\,\theta)-U(\theta)\}f(\theta)-F(\theta)\{d'+v_\theta\}$$

$a,\,p$ に関する一階の条件は次のようになる。

$$d'(p(\theta))=1-\frac{F(\theta)}{f(\theta)}d''(p(\theta)) \quad \cdots\cdots(10)$$

$$c'(a)+v_a(a,\,\theta)+\frac{F(\theta)}{f(\theta)}v_{\theta a}(a,\,\theta)=1 \quad \cdots\cdots(11)$$

$\dfrac{\mathrm{d}}{\mathrm{d}e}d=\dfrac{\mathrm{d}}{\mathrm{d}p}d$ を考慮し，$e=p+\theta$ を代入して整理すると

$$d'(e(\theta))=1-\frac{F(\theta)}{f(\theta)}d''(e(\theta))$$

（１），(10)式と $d''(e(\theta))>0$，（２），(11)式と $v_{\theta a}(a, \theta)>0$ より解を $e^{SB}$, $a^{SB}$ とすると

$$e^{SB} \leq e^{FB}$$

$$a^{SB} \leq a^{FB}$$

等号は，$\theta=\theta_0$ のときに成立

となる。

情報の非対称性から生じるエージェントのレントは

$$U(\theta)=\int_{\theta}^{\theta_1}\{d'(e^{SB}(s))+v_{\theta}(a^{SB}(s), s)\}\,ds$$

となるので，これより移転額 $t^{SB}$ は

$$t^{SB}=d(e^{SB}(\theta))+v(a^{SB}(\theta), \theta)+\int_{\theta}^{\theta_1}\{d'(e^{SB}(s))+v_{\theta}(a^{SB}(s), s)\}\,ds$$

となる。

## 5. 考　　察

分析の結果，組織内での情報の非対称性が存在する場合，CSIRT の活動レベル，部署が行うセキュリティ対策のレベル，両方とも情報の非対称性が存在しない場合に比して低下している。移転額として部署へ配当される予算は増加している。本稿での仮定は，CSIRT と機密性の高い情報を保有する部署との間でリスクに関する情報が非対称的であるか，情報共有がなされて非対称性が存在しないか，の二つの場合の比較を行っているが，非対称性が存在することで，セキュリティ対策のレベルは全体では低下し，組織全体での費用は部署へ配当の移転額が増加してしまう。

CSIRT が有効に機能するためには，組織内でのリスクとなりうる情報や情報システムの把握，組織外の CSIRT 等との情報共有で新たな脅威に関する情報を入手し自組織での対策に反映させ，自組織でのインシデントの経験を閉じているとはいえ CSIRT のコミュニティに提供すること，が必要であるが，いずれの要素も組織内で簡単に合意形成ができるとは言い難い。それぞれの部署は競合企業のみならず，自組織内の他部署との競争にもさらされており，部署内の情報や情報システムを部署外に教えることには抵抗が多い。

組織外の CSIRT との情報共有は外部に自組織のインシデント情報を提供することに対して，自組織の機密性の高い情報を外部に提供することに対して，多くの組織は後ろ向きである。現在のサイバー攻撃を自組織だけで防ぎきることは困難で，適切なセキュリティ対策を実施していたにもかかわらずインシデント発生を防げなかったことで世間から非難されることはない。非難されるのは防ぐことができたインシデントを防げなかった場合で，完全に防ぐことは不可能でも実施できる対策を怠っていたことが非難されるべきであるが，

まだそのような考えが浸透しているとは言えない。

また，セキュリティ対策はどこまで実施しても万全というものではなく，いくら予算を投入し対策を実施しても，セキュリティ対策実施の効果は売り上げや利益等のような数値化が容易ではなくコストとして認識されがちで，先行研究で数値化の試みもなされているが，どの程度の予算を投入すればどの程度の効果が得られるかのコストベネフィットの推定も容易ではない。

## 6. 結　　論

本稿では，契約理論の枠組みを用いて，組織内での情報の非対称性がセキュリティ対策のレベルに与える影響について考察し，情報の非対称性が非効率な状況をもたらすことを示した。

現在の一組織での対応の限界を超えるようなサイバー攻撃をはじめとするインシデントへ対応するための CSIRT の有効性については議論の余地はないが，組織内のすべての部門が CSIRT とインシデントに関するリスクについて情報共有することがセキュリティレベルの低下とコストの増加を防ぎ，組織全体のメリットとなることを理解し，CSIRT との信頼関係を醸成し，リスクに関する情報を共有する体制を構築することが必要である。

CSIRT 導入の有効性は理論で示したが，さらなる普及促進に向けての課題を明らかにする必要がある。その為には，実際にインシデント対応を行う CSIRT のスタッフではなく，導入を決定する意思決定者の導入に対する要因分析を行うことで，組織における CSIRT 導入の推進要因，阻害要因を明らかにしていきたい。

### 注

1）http://www.nca.gr.jp/outline/index.html
2）http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf
3）http://www.nisc.go.jp/active/general/pdf/shishin.pdf
4）http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf
5）http://www.nii.ac.jp/csi/sp/doc/sp-sample-2015.pdf
6）Laffont and Tirole［1993］に従い，本稿でもその仮定を踏襲する。
7）相殺インセンティブに関する先行研究のモデルでは，留保効用はタイプにのみ依存する関数としてモデル化されているが，本稿においては $e$ にも依存するものとする。
8）Fudenberg and Tirole［1991］参照。

### 参 考 文 献

Fundenberg, D and J. Tirole.［1991］*Game Theory,* The MIT Press, Cambridge, MA.

浜津翔，栗野俊一，吉開範章［2015］“集団防護動機理論に基づく情報セキュリティ対策実行意思モデルの提案とその活用，”情報処理学論文誌，Vol. 56, No. 12 pp. 2200-2209.

礒谷洋平，廣松毅，高木知陽，伊東俊之，川又祥正［2010］“情報セキュリティ投資を促進するインセンティブの設計，”2010年日本社会情報学会（JSIS＆JASI）合同研究大会研究発表論文集，pp. 231-234.

伊藤秀史［2003］『契約の経済理論』，有斐閣.

金子格［2010］“クラウドコンピューティングのセキュリティ問題へのナッシュ均衡と確率モデル適用の最近の動向，”情報処理学会研究報告，Vol. 2010-EIP-48, No. 13, pp. 1-5.

菊池修，谷本茂明［2011］“CSIRT における組織形成に要するコスト構造定量化の検討，”プロジェクトマネジメント学会2011年度秋季研究発表大会予稿集，pp. 227-232.

栗田克己，樋口清秀［2012］“クラウド・コンピューティングにおける非対称情報の解消について―第三者認証の活用に向けて―，”情報通信学会誌，Vol. 30, No. 1, pp. 15-26.

Laffont, J. J. and J. Tirole［1993］*A Theory of Incentives in Procurement and Regulation,* The MIT Press, Cambridge, MA.

Lewis, T, R. and D, E. M. Shappington［1989a］“Countervailing Incentives in Agency Problems,” *Journal of Economic Theory,* Vol. 49, No. 2, pp. 294-313.

Lewis, T, R. and D, E. M. Shappington［1989b］“Inflexible Rules in Incentive Problem,” *American Economic Review,* Vol. 79, No. 1, pp. 69-84.

Maggi, G. and A. Rodor'igues-Clare［1995］“On Countervailing Incentives,” *Journal of Economic Theory,* Vol. 66, No. 1, pp. 238-263.

見目悠平，谷本茂明，菊池修，杉浦芳樹，佐藤周行，金井敦［2013a］“CSIRTにおける人的資源管理方式に関する研究，”プロジェクトマネジメント学会2013年度秋季研究発表大会予稿集，pp. 105-110.

見目悠平，谷本茂明，菊池修，杉浦芳樹，佐藤周行，金井敦［2013b］“情報セキュリティマネジメントにおける保証レベルに関する検討，”プロジェクトマネジメント学会2013年度秋季研究発表大会予稿集，pp. 308-313.

島成佳，安藤玲未，高木大資［2015］“情報漏えいにつながる行動に関する実証分析，”情報処理学会論文誌，Vol. 56, No. 12 pp. 2191-2199.

高田義久，藤田宣治［2013］“スマートフォン保有者のモバイルデータサービス需要要因に関する考察―国内スマートフォン保有者調査に基づく分析―，”情報通信学会誌，Vol. 31, No. 2, pp. 53-65.

田中絵麻［2011］“米国におけるクラウド・コンピューティングの市場形成とリスク縮減における合意形成要因の考察―アクターのネットワーク化のインセンティブの視点から―，”電子情報通信学会技術報告，Vol. ISEC2011-14, ICSS2011-19, EMM2011-13, pp. 31-38.

田仲理恵，新熊亮一，板谷聡子，小西琢，吉永直生，土井伸一，山田敬嗣，高橋達郎［2015］“ソーシャルネットワークにおけるクチクミに対するインセンティブ報酬を用いた行動促進手法，”情報処理学会論文誌，Vol. 56, No. 7 pp. 1549-1558.

高田義久，藤田宣治［2013］“スマートフォン保有者のモバイルデータサービス需要要因に関す

る考察―国内スマートフォン保有者調査に基づく分析―,”情報通信学会誌, Vol. 31, No. 2, pp. 53-65.
内田勝也［2015］“誘導質問術から見た個人情報漏えいの考察,”情報処理学論文誌, Vol. 56, No. 12, pp. 2219-2229.