［ディジタルエコノミー時代のサイバーセキュリティ―ディジタルトランスフォーメーション促進の基盤確立に向けて―］

⑦ サイバーセキュリティ経済学

―インセンティブの適正化を通じたサイバーセキュリティの確保―

応用

石黒正揮 （株）三菱総合研究所

サイバーセキュリティ経済学の必要性

セキュリティ技術が年々進歩しているにもかかわらず，セキュリティ事件・事故（以下，「インシデント」と呼ぶ）が多発し，大規模な被害が相次いでいる．米国FBIのサイバー犯罪に対処する組織 Internet Crime Complaint Centerによれば，2016年のサイバー犯罪による被害額は13億ドル（前年比24％増）を超え，年々増加傾向にある．

インシデントが減少しない理由としては，攻撃手法の進化も挙げられるが，サイバーセキュリティ分野に特有な要因として，**セキュリティ対策に投資するインセンティブが適切に働かないという，本質的な問題**（インセンティブの不整合 Misaligned Incentives [1]）を抱えていることが挙げられる．

たとえば，不正なソフト（マルウェア）の一種であるボットネットは，感染した多数のPCを踏み台として，標的とする組織等に対してDDoS攻撃を仕掛けるために悪用されるが，セキュリティ対策を行うべき者（組織）と被害を受ける者（組織）が異なっているため，コストをかけて十分に対策を行うインセンティブが働きにくい．また，ウィルス対策ソフトの性能評価は，技術の専門家ではない買い手（ユーザ）には難しく，そのため性能品質に見合った対価がつきがたく，良い製品が市場に普及しづらい．

一方，インシデントの被害にあった企業の信用失墜，顧客離れなどによる将来に渡る収益減少に伴う損失リスクが適切に認識されていないため，**セキュリティ投資が不十分となる傾向**がある．

このような問題に対して，経済学的なアプローチによりセキュリティ対策の意思決定を適正化する [2] ための手法について検討する分野が，**サイバーセキュリティ経済学**である．**技術的な観点だけでは解決できないセキュリティ分野に特有の問題**に対して，**経済メカニズム，人の行動モデル，インセンティブにまでスコープを広げることで，本質的な問題の解決を目指す分野**である．

以下では，サイバーセキュリティ経済学の中心テーマである市場メカニズムに関する問題と対策，リスク定量化と最適なセキュリティ投資額に関する取り組みについてまとめる．

市場の失敗と政府の役割

サイバーセキュリティ分野においては市場メカニズムが適切に機能しない状況（経済学における「市場の失敗」）があるため，適切なセキュリティ対策が進まない原因となっている．サイバーセキュリティ分野における「市場の失敗」の主な原因としては，「外部不経済」と「情報の非対称性」[3] が挙げられる．

(1) 外部不経済

サイバーセキュリティ分野では，コストを払い対策を実施すべき者が本来必要な対策を行わないために，第三者に悪影響を及ぼす状況がある．たとえば，IoT機器のセキュリティ対策が不十分なためにウィルス等の感染が増え，それを踏み台として第三者への攻撃に悪用されるような例がある．この場合，踏み台とされる感染者側の被害は少ないため，コストを払いセキュリティ対策を実施するインセンティブ

が十分に働かない点が問題となる．経済学においては，売り手と買い手の取引当事者以外の第三者に悪影響を及ぼすことを「外部不経済」と言う．典型的には，工場からの排出により生じる公害が取引相手以外の第三者に被害をもたらすことが例である．

このような問題を解決するためには，政府による規制，税金，課徴金などの政策的手段により外部不経済を解消する（「内部化」するという）ことが必要になる．**セキュリティ対策においても何らかの政策的取り組みがなければ外部不経済による市場メカニズムのゆがみを解消することができない．**

(2) 情報の非対称性

ウィルス対策ソフトの性能品質は，技術の専門家ではない利用者には評価が難しい．このような場合，性能品質に見合った価格付けがなされないため，コストをかけて開発した性能品質の高い製品が市場で競争力を持たなくなる．経済学では，「売り手」と「買い手」の専門知識の情報に格差がある場合，**良い技術が評価されず，市場において良い製品が普及しにくい問題**を「情報の非対称性」と言う．

このような問題を解決するためには，隠れた情報を見える化（「シグナリング」，「フィルタリング」等）することにより**購入者が必要な情報に基づく適正な判断をできるようにすることが必要**である．専門家による第三者認証，資格制度などがその例である．

(3) 政府の役割

以上のような**市場メカニズムが適切に機能しない状況（市場の失敗）においては，政府の役割が不可欠**となる．サイバーセキュリティ分野の場合，「外部不経済」，「情報の非対称性」により，セキュリティ対策が不十分となる方向に作用していることが大きな問題である．

市場の失敗は，市場参加者のインセンティブが適切に働かない状況であり，**どのようにインセンティブを適正化するかが問題**ともいえる．

インセンティブ（誘因）を適正化するアプローチは，大きく分けて「正の誘因」と「負の誘因」がある．**正の誘因は，期待される行動を積極的に選択するような便益を提供**するもので，**負の誘因は，期待される行動をとらない場合には相応のペナルティ（費用）を課すことで，行動を促す**ものである．これはアメとムチの両面からインセンティブを高めることを意味する．

サイバーセキュリティに関して，正の誘因と負の誘因について，政府の関与度に応じて3段階に分けた場合，表-1のような政策により市場の失敗を解消することが考えられる．

政府の関与度が低いもののうち，正の誘因としては，セキュリティ対策の高い企業に対する表彰制度や，セキュリティの政府調達基準があり，負の誘因としては，事故が発生した場合の法的責任，損害賠償を課すことで抑止力を高めることがある．また，脆弱性を発見・報告した人にベンダが報奨金を支払う脆弱性報奨金制度（バグ・バウンティ・プログラム）はすでに行われており，将来的にはそれを発展させて，脆弱性を含む製品を販売したベンダが，脆弱性を発見した人に対価の支払を義務付けるセキュリティ版の排出権取引による抑止策も考えられる．中程度の政府関与については，正の誘因として，標準化，政府R&Dファンディングのほか，ISP（Internet Service Provider）からユーザへの感染通知，感染ユーザへのウィルス駆除支援，政府への統計情報提供[☆1]などと引き換えにISPのセキュリティ障害時の法的責任の免除特権を与える措置などが考えらえる．負の誘因には，事故報告情報開示によるレピュテーションへの影響やペナルティ効果，強制保険などが考え

■表-1　市場の失敗に対する施策候補

政策関与	正の誘因（便益）	負の誘因（費用）
低	表彰制度，政府調達基準，ベンチマーク，推進団体設立	法的責任制度，脆弱性報奨金制度
中	標準策定，政府R&D，免責特権，認証，格付，実証事業，補助金	事故報告開示制度，強制保険
高	税額控除	規制，罰則金

☆1　通信の秘密等の制約の下で，メタ情報，匿名化情報の活用が考えられる．

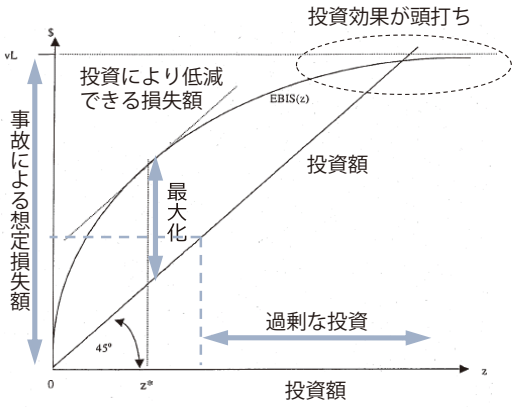
られる．政府の高い関与については，セキュリティ対策における税額控除，規制，罰金などが挙げられる．

リスク定量化と最適投資額

ソフトウェアの不具合（以下，「脆弱性」と呼ぶ）は完全に取り除くことは難しく，ましてや組織管理を含むセキュリティ全般について100％の完璧を期すことは困難である．完璧なセキュリティを追求すればコストは際限なく膨れ上がるため，企業等にとっては，**「セキュリティ対策をどこまで行うべきか？」ということが大きな悩み**となっている．

このような問いに対して，サイバーセキュリティ経済学においては，最適なセキュリティ投資額の考え方を示している．

サイバーセキュリティ経済学に関して国際的に代表的な会議としてはWEIS（Workshop on the Economics of Information Security）やSHB（Interdisciplinary Workshop on Security and Human behavior）がある．サイバーセキュリティ投資の最適額については，L. A. Gordon と M. P. Loeb の評価モデル（Gordon-Loeb モデル[4]）が代表的である．Gordon-Loeb モデルでは，一定の仮定を置いた上であるが，最適投資額についての考え方を示しており，多くの研究の基礎として参照されている．このモデルでは，脆弱性に対する対策投資により，攻撃を受けた場合に事故に至る確率が低減する関係性に基づき評価している．概念的に説明すると，図-1のようになる．グラフの曲線は，セキュリティ対策投資により低減できる損失額を示すもので，セキュリティ対策を増やすことで低減できる損失額を大きくできるが，投資額を増やすに従いその効果は頭打ちとなる．低減できる損失額から投資額（図中45度の直線）を差し引いた額が最大となるような投資額を最適投資額として解を求めている．

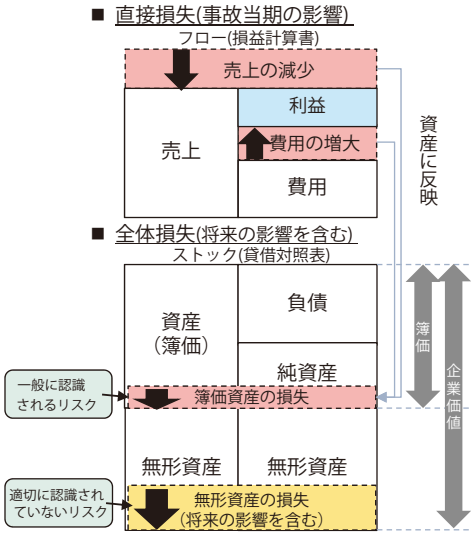


■図-1　投資額と低減できる損失額の関係

研究成果の1つとして，典型的なケースについては，**インシデントの発生により生じる最大損失額の37%以上の投資は過剰**であることが示されており，投資額の上限について一定の考え方を示している．

(1) セキュリティリスクと企業価値

セキュリティ事故や対策が企業価値に与える影響についても多くの研究が行われている．インシデントの損失額について，従来は，復旧コスト，損害賠償などの「費用の増大」やシステム停止による事業機会の損失（「売上の減少」）など**事故が発生した際に直接的に発生**する損失（**直接損失**）については企業においてある程度認識されていたが，インシデントによる企業の信用失墜や顧客離れなどによる**将来に渡り影響する収益減少**に伴う**ブランド価値毀損**（「**無形資産の損失**」と呼ぶ）については理解が進んでおらず，**リスクの認識が不十分であった**．これらの関係を図に示したものが図-2である．



■図-2　直接損失と無形資産を含む全体損失[5]

直接損失は主に企業会計の「フロー」に当たる損益計算書に現れる**事故による当期の損失**である．企業会計の「ストック」にあたる資産で見ると，**将来に渡る影響を含む無形資産の損失リスクは適切には認識されていなかった**．

企業の純資産に対して企業価値の比率（PBR：株価純資産倍率）が高いネット企業など将来の収益性が期待された企業や，不正アクセス，機密情報漏洩などの特定の事故種別に関しては，ひとたびインシデントが起きれば，**直接損失額よりも無形資産の損失額が大きい**傾向があることが統計的に示されている[5), 6)]．

2003年に国際財務報告基準（IFRS，International Financial Reporting Standards）において無形資産の会計について定義されて以来，国際的には無形資産を活用した企業価値向上の取り組みが進んでいる．**セキュリティ投資においても，直接損失だけでなく，無形資産の損失を含むリスク全体を適切に把握してセキュリティ投資を行うことが必要**である．

セキュリティ投資判断については，行動経済学[☆2]の視点でも議論がなされている．行動経済学の代表的な成果であるプロスペクト理論によれば，人の認知モデルとして，「**『確実な損失』よりは『不確実で，より大きな損失』の方を許容する**」という**認知の偏り（cognitive bias）**がある．これは，人は，大きな損失の可能性があっても，それが起きる見込みが低く不確実な場合には，**リスクを過小評価する傾向**があることを意味しており，セキュリティ投資が過小とならないように注意すべき点である．

2018年のWEIS会議においては，ビットコイン取引所へのサイバー攻撃の影響，身代金要求型マルウェアのランサムウェアにおけるビットコイン払いの経済的影響，仮想通貨の価値変動，規制など仮想通貨のサイバーセキュリティにかかわる経済的影響評価の研究が多数占めており注目されている．

☆2 人は合理的に行動するという前提を置いた従来の経済学に対して，人がかならずしも合理的には行動しないことに着目し，経済を説明しようとするもの．

(2) サイバーセキュリティ保険

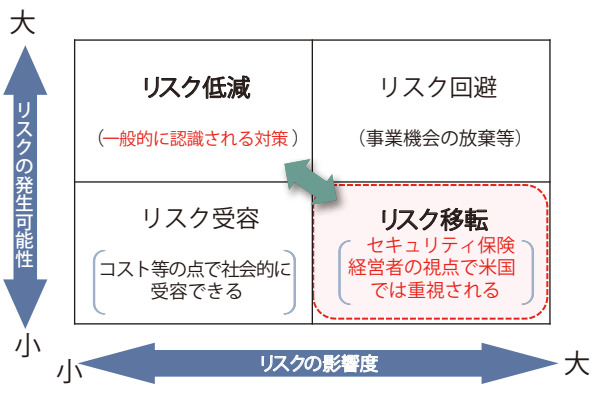
リスクの量は，損害の発生する可能性とその影響規模の積の概念として以下のように捉えられる．

（リスク）＝（発生可能性）×（影響規模）

すなわち，発生可能性が高いほどリスクは大きく，損害の影響規模が大きいほどリスクは大きいといえる．セキュリティ対策のアプローチは，これらの2つの要因の大小に応じて，一般に図-3の4象限に分類することができる．

通常想定されるセキュリティ対策は，4象限のうちの「リスク低減」に該当するものである．一方で，**リスクの発生可能性が非常に低く，発生した際の影響規模がきわめて大きい場合**には，稀にしか起こらないことに対して膨大な対策コストが必要となり，効果的な対策投資が難しい．このような場合，**サイバーセキュリティ保険を組み合わせることで「リスクを移転」することが現実的な解**となる．

2015年のサイバーセキュリティ保険の市場規模は，17億ドル（保険料ベース）で，米国の市場規模はその90％（15億ドル）を占める．日本のサイバーセキュリティ保険市場は2015年度で118億円で2015年から毎年15％程度の成長傾向と見積もられており，サイバーセキュリティ保険の活用が1つの選択肢として考慮することができる．



■図-3　セキュリティリスクと対策の4分類

非対称性とインセンティブ

サイバーセキュリティの経済学的な問題は，非対称性によって生じるインセンティブの不整合（ゆがみ）として捉えられる．本稿で挙げたものを含めたサイバーセキュリティにおける非対称性とそれに伴う問題を整理すると表 -2 のようになる

適正なセキュリティ対策を促すためにはこれらの非対称性を解消することが必要といえる．

今後の展望

サイバーセキュリティ分野においては，**技術的な課題だけではなく，インセンティブが適切に働かないために，セキュリティ対策が適切に進まないという本質的な問題**がある．それらに対して民間レベルでは，リスク定量化に基づく最適投資額の判断や，インシデントの直接的な損失リスクだけでなく，事故企業の信用失墜，顧客離れ等による将来に渡る収益減少などの無形資産の損失リスクについて適切に理解することがサイバーセキュリティ経済学により新たに示される知見である．

一方で，**市場の失敗に関しては，民間レベルだけでの解決は困難であり，政府の役割が不可欠**である．市場の失敗を解消するための施策についてはすでに表 -1 において全体像と具体的な施策案を示した．これらの方向性に向けて，今後重要となる課題を挙げると次のようになる．

■表 -2　セキュリティの非対称性と問題点

非対称性	セキュリティの問題
認識リスクと現実リスクの非対称性	現実のリスクに対して認識されるリスクが過小評価されるため，セキュリティ投資が過小となる
ベンダとユーザの技術情報の非対称性	良い技術に適正な対価がつけられず，市場での流通が低下する
投資者と受益者の非対称性	対策投資者と受益者が異なるため対策投資が低下する
攻撃と防御の非対称性	攻撃者は問題を 1 カ所でも見つければよく，防御者はすべての問題を解決することが必要なため，攻撃者に有利な状況にある
安全と安心の非対称性	必要な対策と実際に行われる対策にズレが生じる

- インシデントデータベースの整備

リスク定量化，無形資産の損失額評価，セキュリティ技術の性能品質の評価などにおいて**インシデントデータの蓄積と分析によるリスクや損失額の評価精度の向上がセキュリティ経済学の基盤**として重要になる．

- セキュリティ対策の見える化

情報の非対称性を解消するためには，技術の提供者が理解できればよいというのではなく，利用者，**社会を含む第三者に対しても，見える化し，客観的に理解が得られることが重要**である．そのために，機能安全におけるアシュアランスケース☆3 と同様の考え方をセキュリティ分野にも積極導入し，多様なステークホルダに対するセキュリティの見える化，説明の仕方について参考となる具体例を整備することが重要である．

参考文献

1) Center for Strategic and International Studies（戦略国際問題研究所）：Misaligned Incentives in Cybersecurity (2017).
2) The International Journal of eScience : Future Generation Computer Systems, Special Issue on Economic Aspects of Cybersecurity and Privacy, 2018 Call for Papers, Elsevier.
3) CCDCOE(NATO Cooperative Cyber Defence Centre of Excellence) : Economic Aspects of National Cyber Security Strategies (2015).
4) Gordon, L. A. and Loeb, M. P. : The Economics of Information Security Investment, ACM Transactions on Information and System Security, Vol.5, No.4 pp.438-457 (Nov. 2002).
5) 石黒正揮：情報セキュリティ事故等による企業価値に与える影響，講演資料，（独）情報処理推進機構 被害額調査委員会 (2012).
6) Ishiguro, M., Tanaka, H., Matsuura, K. and Murase, I. : The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market, Workshop on the Economics of Securing the Information Infrastructure (2006).

（2018 年 9 月 2 日受付）

☆3　テスト結果等を根拠に客観的・合理的にシステムの安全性を示し，利用者，ステークホルダに安全性の保証・確信を与えるための文書．

石黒正揮（正会員）　masa@mri.co.jp
博士（情報科学）．サイバーセキュリティ，ソフトウェア工学，AI/数理データ解析，リスク評価等に関する研究開発，日米欧アジアにおける ICT およびサイバーセキュリティ政策，技術戦略に関する調査に従事．東京大学大学院理学系研究科情報科学専攻修士課程修了．現在，(株)三菱総合研究所サイバーセキュリティ戦略グループ．