

# ネットワーク理論を活用した サイバーセキュリティ・リスクシェアリング

—中小企業サイバーセキュリティ対策促進に向けて—

## Cybersecurity Risk-Sharing Utilizing Network Theory: Towards Promoting Cybersecurity Measures for Small & Medium Enterprises

山下 実若 (Yamashita, Miwaka)

1. はじめに
2. リスクシェアリング
  - (1) リスクシェアリングとは
  - (2) リスクシェアリングの優位性
  - (3) サイバーセキュリティでの留意点
3. プーリング
  - (1) 損失が不透明な中でのプーリング
  - (2) モラルハザード対策
4. ネットワーク理論
  - (1) 隣接行列
  - (2) リスクシェアリングへの活用
5. サイバーセキュリティ対策の促進に向けて
  - (1) コンサルティング
  - (2) サイバーセキュリティ保険機能の強化
  - (3) サイバー事故伝播
6. おわりに

### 1. はじめに

電子記憶媒体の紛失などによる個人情報の遺漏リスクに端を発した情報セキュリティリスクが、直近では情報通信システム・端末へのウイルス感染、標的型攻撃といったサイバーセキュリティリスクへと拡大し脅威となっている。サイバーセキュリティとは、個人や企業の機密情報や保護すべき個人情報データが悪意のある者により遺漏、破壊させられるリスクから防御するための対策であり、サイバーセキュリティ保険とはそうしたリスクによる損害を補填する保険である。

サイバーにおける事件・被害の増大について簡単に触れる。警察庁(2023)のデータによると、サイバーセキュリティの被害で代表的なランサムウェア被害報告は、日本国内で、2021年146件が2022年230件に急増している。NAIC(2020)も米国のサイバーセキュリティ被害拡大傾向を憂慮し、CSIS and McAfee(2020)によると、世界で2020年のサイバーセキュリティ被害総額は1兆ドルを超える

と推定している。サイバーリスクに対するサイバーセキュリティ保険の在り方や動向は辰巳（2020）や石井・櫻井（2015）に詳しいが、リスクのモデル化などは緒についたばかりである。

日本・世界のサイバーセキュリティ対策やその保険の実態は、三菱総研（2023）（日本・世界）、Nieuwesteeg et al. (2018)（米国）、土井（2021）及び教学（2021）（日本）を参照されたいが、サイバーセキュリティ保険の喫緊の課題は、

- ・保険事故による支払いの額の不確実性の高さから保険提供が容易でない。
- ・安定した保険を提供するためのデータ整備や国も巻き込んだ制度が未発達。という点であるが、佐久間・猪俣(2019)のアンケート調査からは以下指摘がある。
- ・中小企業のサイバーセキュリティ対策が遅れており、保険の利用も極低い。
- ・これらは、リスクやその対策、保険商品の内容の不透明さが背景にある。

現在例えば、保険とコンサルティングを兼ね備えた形の支援策が官民一体となりでてきている（例：経済産業省・独立行政法人情報処理推進機構のお助け隊サービス）が、今後一層の対応強化が望まれている。

本論文は、サイバーセキュリティ保険の提供を容易にし、かつ保険加入やサイバーセキュリティ対策が促進される保険商品性・仕組みは何かとのリサーチクエストを設定し、

- ・リスクシェアリングの形態をとる透明性の高い商品性（団体保険と類似）
- ・プーリング（当該保険集団プール）のモラルハザード防止機能を高める工夫
- ・ネットワーク理論を活用、プールの質を高めるインセンティブの仕組み
- ・免責額設定、保障上限設定、国の関与(巨大リスク・戦争対応を含めた Last Resort 提供、各種データ整備)などの実務的な提案

を論じていく。この過程で、リスクシェアのメリットを効用関数を使い簡易に提示したこと、ネットワーク理論を応用したリスクシェアリングのルール設定により集団のプールの質に配慮し、かつ、質を高めるインセンティブのある工夫を施したこと、中小企業の対応策を念頭にサイバーセキュリティ上特有な被害伝播を考慮した対応策を提起したことが新規性である。なお、リスクシェアリングは新しい形態の保険機能として扱う。

過去の文献について、サイバーセキュリティのリスクシェアリング/プーリングは Faure and Nieuwesteeg (2018) で論点整理がなされているのみであり、本論文ではより具体的な商品性、仕組みを提起する。なお、リスクシェアリングのルールの普遍的性質については Feng, Liu, and Zhang (2022)や Denuit, Dhaene, and Robert (2022)がそのリスクシェアリングのルールの在り方を提起し、Denuit and Dhaene (2012)、Denuit and Robert (2021a, 2021b, 2021c)はリスクシェアリングの一般的特徴を分析しており、こうした議論を踏まえて論じる。一方、ネットワーク理論について、隣接行列(Adjacency Matrix)を活用して保険プールの性質にかかわる分析が Abdikerimova and Feng (2022)、Charpentier, Kouakou, Lowe, Ratz, and Vermet (2021)、Feng, Lui, and Taylor (2020)、Denuit and Robert (2021a, 2021b, 2021c)により行われ、Bienenstock and Bonacich (2022)、Chen, Chong, Giudici, and Huang (2022)、Afuah (2013)や Iacobuccia, McBrideb,

and Popovicic (2017) においてはモラルハザード対策やモラルハザード軽減機能強化の視点で分析がなされている。また、ネットワーク理論以外でもモラルハザード対策効果については Belhaj, Bourlès, and Deroian (2010) でリスクシェアリング/プーリングの意義が論じられている。本論文はこれらを踏まえ具体的なモラルハザード対策となるリスクシェアリングのルールを提示した。加えてサイバーセキュリティで特徴的な被害伝播に即した対応の議論においては Marotta, Martinelli, Nanni, Orlando, and Yautsiukhin (2017) を参照した。

以下、本論文は 2 節でリスクシェアリングの導入とその優位性を論じ、3 節でリスクシェアリング/プーリングでのモラルハザード対策をまとめる。4 節ではネットワーク理論を論じ、リスクシェアリングへ応用を論じる。そして 5 節でサイバーセキュリティ保険の普及に向けてコンサルティング付加や保険機能の高度化、サイバー事故の伝播に留意することなどを提起する。最後に、6 節でまとめと今後の課題を記す。なお、リスクシェアリングのような Peer to Peer 型保険の法的な運営主体、リスク引受主体、プールの存在 (佐野(2021)参照) などについては本論文では厳密に区別しない。また、近年、拡大する DeFi 及び FinTech と呼ばれる金融における新たな潮流の中での上記議論の位置づけについては、補遺 A を参照されたい。これらの発展・工夫を取り入れていくことは今後の課題としていきたい。

## 2. リスクシェアリング

### (1) リスクシェアリングとは

Denuit et al. (2022) に則って、 $n$  人の個人が集まってプールを形成し、 $X_i$  を個人  $i$  ( $i=1$  から  $n$ ) の損失として確率的に決定されるとし、一定期間におけるプール全体の損失を  $n$  人で一定のルールでリスクシェアリングすることを考える。 $X_i$  は一般的な確率空間  $(\Omega, \mathcal{F}, \mathcal{P})$  における確率変数として、その平均値は有限とする。損失のベクトル  $\mathbf{X}_n = (X_1, X_2, \dots, X_n)$  をプールと呼ぶ。プールの損失の合計を  $S_n$  とし、小文字  $x_i$  は  $X_i$  の実現値とする。一期間経過した後の実現した損失について事前に  $i$  が  $H_i(\mathbf{X}_n)$  の損失を負担することに決める (リスクシェアリング・ルール)。すなわち、以下の通り。

$$\mathbf{H}(\mathbf{X}_n) = (H_1(\mathbf{X}_n), H_2(\mathbf{X}_n), \dots, H_n(\mathbf{X}_n))$$

$$\sum_{i=1}^n H_i(\mathbf{X}_n) = \sum_{i=1}^n X_i$$

例えば、全員が公平に等分のリスクシェアリングする場合 ( $H^u$ ) は以下の通り。

$$H_i^u(\mathbf{X}_n) = \frac{S_n}{n}, (S_n = \sum_{i=1}^n X_i)$$

$$\mathbf{E}[\sum_{i=1}^n H_i^u(\mathbf{X}_n)] = \mathbf{E}[\sum_{i=1}^n \frac{S_n}{n}] = \mathbf{E}[\sum_{i=1}^n X_i]$$

この場合、個々の単体の損失期待値はリスクシェアリング前後で異なる。

$$\mathbf{E}[H_i^u(\mathbf{X}_n)] = \frac{S_n}{n} \neq \mathbf{E}[X_i]$$

## (2) リスクシェアリングの優位性

こうしたリスクシェアリングについては Arrow(1964)や Buhrmann and Jewel(1979)、Skogh(1999)がそのメリットをモデルより示している。国内の具体的なリスクシェアリングの保険商品例は癌疾病わりかん保険（例：株式会社 Just in Case(2023)による）がある。海外ではかつての中国・相互宝の仕組みが代表的。

（個別商品の内容については伊藤（2019）及び伊藤（2020）で、個人のリスク回避度をアンケート質問から推定しつつ、Just in Case と相互宝のわりかん保険を具体的に使い、プールの中の各人がその支払い保険料や保険金の結果がどうなるかシミュレーションしており、ご参照されたい。）

ここではシンプルな割り勘保険が通常の保険よりも優位性があることを簡易な例で示す（詳細は補遺 B 参照）。損失について、 $p$  ( $0 < p < 1$ ) の確率で  $\ell$  ( $> 0$ ) の損失が発生、 $1-p$  の確率で損失が発生しない (0) ようなリスクを考える。比較は、一期間モデルにおいて、保険に入らずリスクシェアしない (①)、保険に入るのみ (②)、 $n$  人でリスクシェアリングするのみ (③) の 3 つを考える。個人の資産  $w_i$  は当初資産はすべて  $w_0$  とし、 $n$  人は同一の損失発生と損失のリスクを抱えるとする。各人の効用関数  $u_i(w_i)$  はリスク回避的(convex)とし各人同一とする。それぞれ  $t=0$  から始めて  $t=1$ 、即ち、期間終了後の期待効用を比較する。

$$\text{ケース①} : \mathbf{E}[u_i(w_i)] = p \times u_i(w_0 - \ell) + (1-p)u_i(w_0)$$

$$\text{ケース②} : \mathbf{E}[u_i(w_i)] = u_i(w_0 - p\ell(1 + \varphi)) \quad (\varphi \text{ は純保険料からのバッファ率})$$

$$\begin{aligned} \text{ケース③} : \mathbf{E}[u_i(w_i)] &= p^n \times u_i\left(w_0 - \frac{n\ell}{n}\right) + n \times p^{n-1}(1-p) \times u_i\left(w_0 - \frac{(n-1)\ell}{n}\right) + \\ &\dots + {}_n C_k p^{n-k}(1-p)^k \times u_i\left(w_0 - \frac{(n-k)\ell}{n}\right) + \dots + (1-p)^n \times u_i(w_0) \end{aligned}$$

効用関数は convex であることから、 $\varphi$  が一定程度小さいと期待効用は①<②である。同じく③は①よりも損失の可能性が細かく細分化され、①<③であり、細分化により③は、ほぼ  $u_i(w_0 - p\ell)$  なので、 $\varphi$  が十分小さくないと、②<③となる。

## (3) サイバーセキュリティでの留意点

プーリングし参加者間でリスクシェアリングすることについては、一般に、①保険会社の会社としてのコスト・建付けが不要な分、運営等のコストが安くなる可能性があること、②プーリング参加者が保険金発生事由が起こらない努力をするモラルハザード防止機能が期待できること等のメリットが謳われる一方、③プールのモニタリングコスト(事故の査定、不正防止等)が大きくなる可能性がある

このデメリットも指摘される。Nieuwesteeg et al.(2018) ではサイバーセキュリティに関するプーリングの議論をしており、プーリングにそうしたメリット・デメリットがある中でサイバーセキュリティ保険を提供しようにも事前分布、特に損失の額が未知であることでプーリングも前向きにならない要因となりうること、リスクシェアリングのプールにはいる参加者は同様なリスクにさらされている質の良いプールである可能性がある一方、加入者を追加する場合はどのような参加者か不透明なこと（逆選択の可能性、この点はCYDEF(2021)でも指摘）、保険金発生状況のチェック等コストはかかるが、こうしたモニタリングが不十分ではリスクシェアリングの機能が損なわれるため節約できない上に額が不透明である可能性もあることに留意する必要があることを指摘している。これらの点は次節で議論する。

### 3. プーリング

#### (1) 損失が不透明な中でのプーリング

サイバーセキュリティでは事故による支払いの額の不確実性の高さはあるものの、Skogh and Wu(2005)は損失が未知の状態であっても、通常の保険よりもプーリングしてリスクシェアリングすることの意義があることを示した。また、Mahul(2003)では巨大リスク（損失填補できる能力を超えた損害）に関するリスクシェアリングの方法・あり方が整理されている。実務的には後に触れる国のLast Resort機能が解決策となろう。

#### (2) モラルハザード対策

プーリングのリスクシェアリングのルールが公平であれば、プール内の参加者が事故を起こさないようにする個々の努力が、プール全体の利益につながり、個々の全員に恩恵があり、モラルハザード対策が自然になされていることとなる。中丸（2020）によると、罰とインセンティブを用意した実験で、プーリング機能が維持されていることを示している。

改めてサイバーセキュリティでのモラルハザードを多面から整理すると以下の通り(CYDEF, 2021)。

- ・初期のプーリングの参加者はセキュリティ意識の高い参加者である場合が多いが、その後追加的に参加する者は意識が低くなる可能性も十分にあり、逆選択される事態もある。
- ・保険に加入したことで、安心して対策がおろそかになるリスク有り。
  - ・保険支払いの上限を設定すると、それ以下の被害に抑えようとするインセンティブがある。
  - ・また、サイバーセキュリティでの特徴から、Zhao et al.(2013)は、サイバー対策は個にとってはプラスでも他の個にとってマイナスになる場合がある（自分が対策強化しても相対的に弱くなったネットワーク内の他が狙われる事態）。これらに対して、Belhaj et al.(2014)ではリスクシェアする参加者の透明性が

あることがモラルハザード対策となることが論じられ、保険を利用した場合ではあるが Dou et al. (2020)は適切な透明性対策がプール全体の効用を高めていることを論じていて、透明性の高いプーリングはモラルハザード対策に資する。また、後述する、ネットワーク内の最も弱い部分の強化も重要である。

#### 4. ネットワーク理論の活用

前節のプーリングでの課題（モラルハザード対策）を解決するために、リスクシェアリングのルールにおいて、中丸（2020）による罰とインセンティブに相当するような仕組みを取り入れることを念頭に以下ネットワーク理論の活用を論じる。

##### (1) 隣接行列(Adjacency Matrix)

$n$  個からなるプールの質を計測する方法として、ネットワーク理論の隣接行列を使った中心度 (centrality) を利用する。隣接行列の各要素  $G_{i,j}$  を 0 か 1 とし、

$$G_{i,j} = 1 \text{ (} i \text{ と } j \text{ が信頼関係にある場合。自分自身と自分自身は } 0 \text{ とする。)}$$

$$G_{i,j} = 0 \text{ (上記以外)}$$

と決める。プールの質は、どのくらい信頼関係にあるペアをプール内の人々が持っているか、で測ることとして、

$$\sum_{i,j}^{n,n} G_{i,j} \div 2$$

は信頼関係ペアの数であり、活用できる。(固有値(eigenvalue)も踏まえた議論は補遺 C: 隣接行列を利用したリスクシェアリングを参照)

##### (2) リスクシェアリングへの応用

リスクシェアリングのルールとして、 $H^{MR}$  を以下のように定義する。

$$H^{NAM}(\mathbf{X}_n) = (H_1^{NAM}(\mathbf{X}_n), H_2^{NAM}(\mathbf{X}_n), \dots, H_n^{NAM}(\mathbf{X}_n))$$

$$H_i^{NAM}(\mathbf{X}_n) = \frac{S_n}{n} + k \left[ \frac{X_i^2}{2n} - \frac{1}{2n^2(n-1)} \sum_{i,j}^{n,n} G_{i,j} X_i X_j \right]$$

$$G_{i,j} = \text{network adjacency matrix, } G_{i,i} = 0, k: \text{定数}$$

この提案のリスクシェアリングのルールの特徴であるが、

- ・上記は、個人の努力を誘引(通常のプール損額等額負担に加えて、個人の  $(X_i^2)$  に比例した負担がかかる) しつつ、
- ・第二項の 2 乗の項で弱い人ほど弱点補強を促し、後述の Minimax にも叶い、
- ・過剰に安心してしまわないようなインセンティブにもなっている。
- ・また、信頼関係のある他人がより多くいるほど負担が下がる仕組み。

となっている。(補遺 C 参照)

#### 5. サイバーセキュリティ対策の普及に向けて

CYDEF(2021)は直近のサイバーセキュリティ保険の動向について、

- ・保険事故増加で保険料が急上昇中

- ・中小企業ではランサムウェア被害が増加、かつ、付随のビジネス停止の悪影響被害も増大
  - ・大企業では守るべきデータの巨大化に苦しむ
- としている。また、Ogut et al.(2011)では、
- ・セキュリティ対策で保険料が安くなるような商品の熟成が未達
- が論じられている。このような状況下、次節以降具体的なサイバーセキュリティ保険機能を提案する。

### (1) コンサルティング

サイバーセキュリティは、リスクマネジメントにおけるロス・コントロール（被害低減努力）とロス・ファイナンス（保険などの移転・転嫁）の両方ともが意義の大きい、そんなリスクである。サイバーセキュリティ対策の資金捻出がままならないことが多い中小企業にとって、サイバーセキュリティ対策のコンサルティングを受けつつ、一定の損害は何らかの形でリスク移転・転嫁する、コンサルティング型の保険機能の仕組み（例：経済産業省/独立行政法人情報処理推進機構のお助け隊サービス）が意義が大きい。Faure and Nieuwesteeg (2018)の海外におけるサイバーセキュリティ保険と付随サービスの実態調査をみると、そうしたコンサルティング型が充実している。

### (2) サイバーセキュリティ保険機能の強化

加入しやすい保険料相当額（リスクシェアリングのルールにもとづく負担の期待値）、理解や扱いが容易な保険機能を実現するため、ここでは以下を提案する。

- ・少額は保険機能の免責とする。（プール参加者のモラルハザード対策）
- ・一定額以上の巨額損失は保険機能の免責とする。（保険機能の保全）
- ・巨額損失や戦争等では国が **Last Resort** の役割を果たす。（保険機能の補完）
- ・定額支払いの組み入れ。（保険金支払い事務の効率化）

少額免責は、モラルハザード対策や損失調査コストの効率化に資する。また、サイバーセキュリティの損失の不透明な状況に鑑み、巨額損失免責と巨額損失での国の **Last Resort** としての役割を提案する。巨大災害の保険関連、国の支援機能としては、英国では **Pool Re for catastrophe in UK** といった制度があり、同様に仏国では **GAREAT agency in France** 制度がある。日本においても地震保険、原子力保険は国が **Last Resort** として機能している上、国として支援している自賠責保険、預金保険、油濁事故対策、住宅保証、貿易保険等が存在している。なお、定額支払い型の採用は支払い事務・支払い調査のコスト効率化に資する。

### (3) サイバー事故の伝播

Marotta et al.(2017)にあるように、サイバーセキュリティ事故はネットワークを通じて伝播する。あるコンピューターシステムがハッキングされる・不正なプログラムをダウンロードされるといった事故が起きれば、ネットワークを通じて他のコンピューターシステムに伝播する。

具体的にはコンピューターシステムがハッキングなどの被害を受ける事故発生確率を考える。そもそもそのコンピューターシステムは多くの他の関連コンピューターシステムや他の一般のコンピューターシステムとネットワークでつながっている中、あるコンピューターシステムが事故発生となったときに一定の確率でネットワークでつながっているコンピューターシステムも被害を受ける確率が高まるとの計算を行う。一定の確率は相関係数を使い、以下のように  $q_i$  を最悪事態確率（ネットワーク考慮）として定める。(Marotta et al. 2017)

$$q_i = 1 - (1 - p_i) \times \prod_{j \neq i}^n (1 - \rho_{i,j} p_j)$$

このため、一層、プーリングにおける協力が意味を持ち、また、防衛最適化（攻撃グラフ(Attack Graph)を使った防御考案等）においては、最も弱い部分になるべく強くする Minimax 的な効用最大化が重要となる。

## 7. おわりに

（特に中小企業を念頭に）サイバーセキュリティ対策の強化・向上のため、新しい保険機能の制度を検討した。ネットワークを共有している企業グループ等の一群の集団で保険機能を発揮させる、団体保険のような概念であるリスクシェアリングを出発点とした。本論文は、

- ・サイバーセキュリティ保険加入障壁となっている料率・損害に対する不透明さに関し、リスクシェアリングの形で保険機能を提供することで透明性を向上させること。(団体保険に類似)
- ・当該リスクシェアリング（またはプーリングすること）では、期待される効用が通常の保険の場合より高いこと、モラルハザード防止機能があること、プールの質向上インセンティブ（プーリングのもつ参加者の協力体制を利用）があること、といったメリットを享受できること。
- ・リスクシェアリングのルールについて、協力体制を向上させる罰とインセンティブを考慮するようなルールを作成（4.(2)のルール）すること。
- ・コンサルティング機能を付加すること。(ロス・コントロールを支援しつつ、ロス・ファイナンス)
- ・国が保険の Last Resort の役割を提供することが望まれること。

がエッセンスである。また、

- ・少額免責、巨額免責、定額支払い、国の関与といった商品性・仕組み
- ・国主導のサイバーセキュリティ事故のデータベース整備
- ・サイバーセキュリティ対策におけるもっとも脆弱な部分の強化（Minimaxの考え方）

の重要さも指摘した。

今後の課題としては、リスクシェアリングの学術研究で急速に導入が進んできた Holmstrom-Milgrom model の活用である。とりわけ、Principal と Agent とのインセンティブ付けとリスクシェアリングのルールに関して、確率過程を導入し



て Hamilton Jacobi Bellman 型動的制御問題 に落とし込むことが進んでいる (Lundesgaard, 2001、Cvitanic, Possamaï, & Touzi, 2018、Martin and Villeneuve, 2023)。筆者は山下(2016)で確率過程動による動的制御問題の枠組みを探索し整理しており、こうした角度からの保険機能や商品性高度化を検討したい。

謝辞：本研究は東洋大学奨学寄附金の支援をいただいた。また、内閣官房内閣サイバーセキュリティセンター、経済産業省サイバーセキュリティ課他の関係者のご協力に感謝申し上げます。

## 参考文献

- Abdikerimova, S. & Feng, R. (2022). Peer-to-peer multi-risk insurance and mutual aid. *European Journal of Operational Research*, 299(2), 35-749.
- Afuah, A. (2013). Are Network Effectis Really All About Size? The Role of Structure and Conduct. *Strategic Management Journal*, 34, 257-273.
- Arrow, K. (1963). Uncertainty and the Welfare Economics of Medical Care. *The American Economic Review*, 53, 941-973.
- Faure, M. & Nieuwesteeg, B. (2018). The Law and Economics of Cyber Risk Pooling. *New York University Journal of Law & Business*, 14(3), 923-963.
- Belhaj, M., Broulès, R., & Deroian, F. (2014). Risk-Taking and Risk-Sharing Incentives under Moral Hazard. *American Economic Journal: Microeconomics*, 6(1), 58–90. <http://dx.doi.org/10.1257/mic.6.1.58>
- Bienenstock E.J. & Bonacich, P. (2022). Eigenvector centralization as a measure of structural bias in information aggregation. *The Journal of Mathematical Sociology*, 46 (3), 227-245. <https://doi.org/10.1080/0022250X.2021.1878357>
- Buhlmann, H. & Jewell, W. (1979). Optimal Risk Exchanges. *ASTIN Bulletin*, 10, 243-245.
- Charpentier, A., Kouakou, L., Lowe, M., Ratz, P., & Vermet, F. (2021). Collaborative Insurance Sustainability and Network Structure. Papers 2107.02764, *arXiv.org*, revised Sep 2022. <https://arxiv.org/pdf/2107.02764.pdf>
- Chen, X., Chong, Z., Giudici, P., & Huang, B. (2022). Network centrality effects in peer to peer lending. *Physica A: Statistical Mechanics and its Applications*, 600, 15 August 2022, 127546. <https://doi.org/10.1016/j.physa.2022.127546>
- CSIS (The Center for Strategic and International Studies) & McAfee (2020). The Hidden Costs of Cybercrime. Research Paper.
- Cvitanic, J., Possamaï, D., & Touzi, N. (2018). Dynamic programming approach to principal-agent problems. *Finance Stochastic*, 22(1), 1–37

- CYDEF (2021). Moral Hazard of Cyber Insurance. April 28, 2021. <https://cydef.ca/blog/cyber-insurance-cyber-risk-management/> (2023年6月1日閲覧)
- Denuit, M. & Dhaene, J. (2012). Convex order and comonotonic conditional mean risk sharing. *Insurance: Mathematics and Economics*, 51, 265-270.
- Denuit, M. & Robert, C.Y. (2021a). From risk sharing to pure premium for a large number of heterogeneous losses. *Insurance: Mathematics and Economics*, 96, 116-126.
- Denuit, M. & Robert, C.Y. (2021b). Risk sharing under the dominant peer-to-peer property and casualty insurance business models. *Risk Management and Insurance Review*, 24, 181-205.
- Denuit, M. & Robert, C.Y. (2021c) Conditional Mean Risk Sharing in the Individual Model with Graphical Dependencies, *Annals of Actuarial Science*, 16(1) 1-27
- Denuit, M., Dhaene, J., & Robert, C. Y. (2022). Risk-sharing rules and their properties, with applications to peer-to-peer insurance. *Journal of Risk and Insurance*, 89(3), 615-667.
- Dou, W., Tang, W., Wu, X., Qi, L., Xu, X., Zhang, X., & Hu, C. (2020). An insurance theory based optimal cyber-insurance contract against moral hazard. *Information Sciences*, 527, 576-589
- Feng, R., Liu, C., & Taylor, S. M. (2020). Peer-to-Peer Risk Sharing with an Application to Flood Risk Pooling (December 23, 2020). *SSRN*: <https://ssrn.com/abstract=3754565> or <http://dx.doi.org/10.2139/ssrn.3754565>
- Feng, R. and Liu, M., & Zhang, N., A Unified Theory of Decentralized Insurance (January 20, 2022). *SSRN*: <https://ssrn.com/abstract=4013729> or <http://dx.doi.org/10.2139/ssrn.4013729>
- Ogut, H., Raghunathan, S., & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, 31(3) 497-512. DOI: 10.1111/j.1539-6924.2010.01478.x
- Iacobucci, D., McBride, R., & Popovich, D. L. (2017). Eigenvector Centrality: Illustrations Supporting the Utility of Extracting More Than One Eigenvector to Obtain Additional Insights into Networks and Interdependent Structures, *Journal of Social Structure*, 18 (1), 1-23. DOI: <https://doi.org/10.21307/joss-2018-003>
- Lundesgaard, J. (2001). The Holmstrom-Milgrom model: a simplified and illustrated version. *Scandinavian Journal of Management*, 17(3), 287-303.
- Mahul, O. (2003). Efficient Risk Sharing within a Catastrophe Insurance Pool. *NBER Insurance Project Workshop*, Cambridge, MA, The USA, January 31-

- February 1, 2003.
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey, *Computer Science Review* 24, 35-61.
- Martin, J. & Villeneuve, S. (2023). Risk-Sharing and optimal contracts with large exogenous risks. *Decision in Economics and Finance*, 46 1-43  
<https://doi.org/10.1007/s10203-023-00386-1>
- NAIC (National Association of Insurance Commissioners) (2022). Report on the Cyber Insurance Market. Property and Casualty Insurance Committee, Research Paper Oct. 18, 2022.
- Nieuwesteeg, B., Visscher, L. & de Waard, B. (2018). THE LAW & ECONOMICS OF CYBER INSURANCE CONTRACTS: A CASE STUDY. *European Review of Private Law*, 3, 371-420. DOI:10.54648/ERPL2018027
- Skogh, G. (1999). Risk-sharing Institutions for Unpredictable losses, *Journal of Institutional and Theoretical Economics*, 155, 505-515.
- Skogh, G. and Wu, H. (2005). The diversification theorem restated: Risk-pooling without assignment of probabilities. *The Journal of Risk and Uncertainty*, 31(1), 35-51.
- Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing Interdependent Information Security Risks: Cyber insurance, Managed Security Services, and Risk Pooling Arrangements. *Journal of Management Information Systems*, 30(1), 123-152. DOI: 10.2753/MIS0742-1222300104
- 石井朝久・櫻井幸一 (2015). 「サイバーリスク保険を利用したセキュリティマネジメントの一考察」 『情報処理学会』 Computer Security Symposium 2015 (21-23 Oct 2015). 348-355.
- 伊藤 晴祥 (2019). 「InsurTech を活用した相互支援プログラムの実現可能性の検証 —相互宝を事例として—」 『生命保険文化センター 研究報告書・技術報告書』, 208-SpecialIssue, 31-100  
[https://doi.org/10.51107/jilijournal.2019.208-SpecialIssue\\_31](https://doi.org/10.51107/jilijournal.2019.208-SpecialIssue_31)
- 伊藤 晴祥 (2020). 「InsurTech を活用した相互支援プログラムは保険需要者の効用を高めるか —相互宝及びわりかん保険を事例として—」 『生命保険文化センター 研究報告書・技術報告書』, 213, 263-328.  
[https://doi.org/10.51107/jilijournal.2020.213\\_263](https://doi.org/10.51107/jilijournal.2020.213_263)
- 株式会社 Just in Case (ジャストインケース) (2023). web home page  
<https://p2p-cancer.justincase.jp/entry> (2023年6月1日閲覧)
- 教学大介 (2021). 「サイバー保険の開発と日本企業のセキュリティ実態」 『日本セキュリティ・マネジメント学会誌』, 35(2), 30-38.
- 警察庁 (2023). 「サイバー事案の被害の潜在化防止に向けた検討会報告書 2023」
- 佐久間朱里・猪俣敦夫 (2019). 「サイバー保険の調査・分析による加入率向上への提案」 『情報処理学会研究報告』, 44(9)

佐野 誠 (2021). 「P2P 保険における近時の展開と法的論点」『生命保険論集』, 第 214 号, 1-34.

辰巳憲一 (2020). 「サイバーセキュリティ保険の役割に係わる諸問題—サイバー攻撃対策との比較—」『損害保険研究』, 82 (2) , 79-99.

[https://doi.org/10.24746/giij.82.2\\_79](https://doi.org/10.24746/giij.82.2_79)

土井剛 (2021). 「サイバー保険概要」 『日本セキュリティ・マネジメント学会 2021』, 35(2), 24-29.

中丸麻由子 (2020). 『社会の仕組みを信用から理解する』 共立出版

三菱総合研究所 (2021). 「令和 3 年度サイバー・フィジカル・セキュリティ対策促進事業 (サイバーセキュリティ法制度の国際動向等に関する調査) 報告書」 経済産業省委託庁調査

山下実若 (2016). 『動的資産配分の理論と応用』 中央経済社

## 補遺 A 金融における新たな潮流

表 A1 Peer to Peer 金融の例 一覧

P2P 保険	Risk Sharing	わりかん保険 Takaful
P2P 貸出	Lending	マイクロファイナンス
P2P 資金調達	Funding	クラウドファンディング
ROSCA	Mutual Aid	無尽(頼母子講、模合)
プーリング	Pooling	プール
その他	Credit/FinTech	BNPL

表 A2 金融における新たな技術等

DeFi 理論
ネットワーク(Network)理論
ブロックチェーン(Block Chain)
暗号資産(Cryptocurrency)

表 A3 保険のファイナンス論からの議論

再保険政策問題と、リスク資産投資の資産配分問題
-------------------------

出所：各種資料より筆者作成

## 補遺 B リスクシェアリングのメリット

図 B1 上左により、リスクにさらされる場合の効用の期待値と、資産が期待値分減価した効用について、効用関数がリスク回避的だとリスクにさらされた場合の効用の期待値は必ず効用曲線の下となることが示されている。これを念頭に、まず図 B1 上右のリスクにさらされる場合の効用の期待値と、保険を利用した場合の効用を比較すると、保険料として期待値にバッファをある程度見込んだ保険

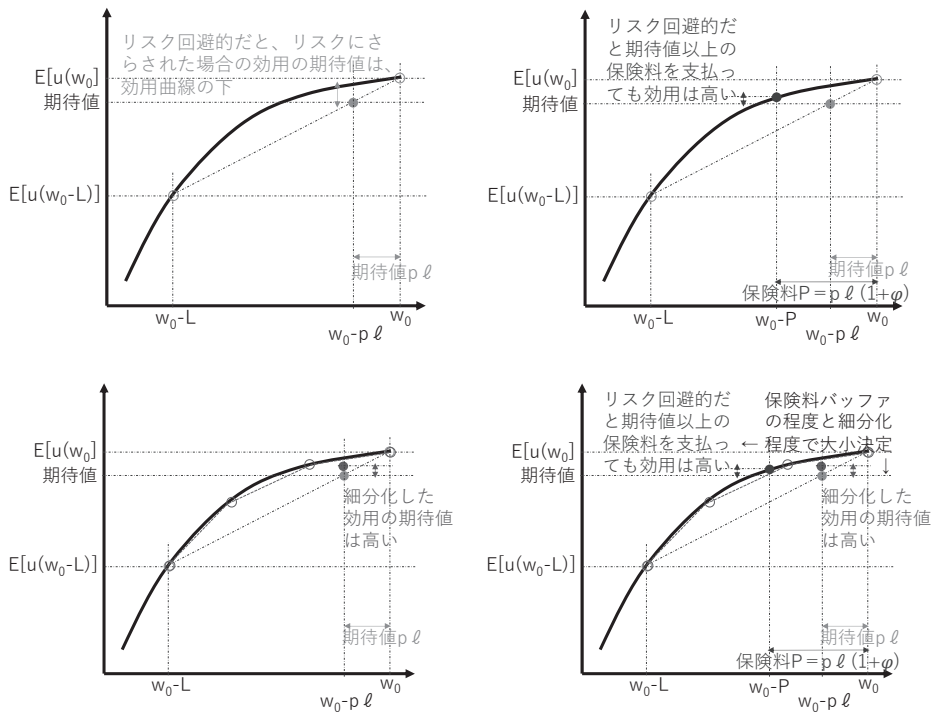
料を支払っても、保険に入の方が効用は高い。

また、図 B1 下左はリスクにさらされる場合で、その場合分けを細分化したことの効果を見たものである。リスクシェアは個人個人にとってみれば、リスクが起る場合分けの細分化にあたり、細分化したほうがその効用の期待値は高い。

次に保険に入ることとリスクシェアリングすることの比較であるが、図 B1 下右のとおり、細分化したリスクにさらされる場合の効用の期待値は保険料のバッファが相当小さくないとリスクシェアリングより小さくなると考えらえる。

図 B1 効用関数の期待値比較

上左：リスクにさらされる場合の効用の期待値と、資産が期待値分減価した効用  
 上右：リスクにさらされる場合の効用の期待値と、保険を利用した場合の効用  
 下左：リスクにさらされる場合で、その場合分けを細分化したことの効果  
 下右：細分化したリスクにさらされる場合の効用の期待値と、保険を利用した場合の効用



出所：筆者作成

## 補遺 C 隣接行列を利用したリスクシェアリング

リスクシェアリングのルール  $\mathbf{H}(\mathbf{X}_n) = (H_1(\mathbf{X}_n), H_2(\mathbf{X}_n), \dots, H_n(\mathbf{X}_n))$  は  $\sum_{i=1}^n H_i(\mathbf{X}_n) = \sum_{i=1}^n X_i$  であればフェアである。なお、 $H_i^u(\mathbf{X}_n) = \frac{S_n}{n}$ , ( $S_n = \sum_{i=1}^n X_i$ ) のような各人均等負担であっても  $\mathbf{E}[\sum_{i=1}^n H_i^u(\mathbf{X}_n)] = \mathbf{E}[\sum_{i=1}^n \frac{S_n}{n}] = \mathbf{E}[\sum_{i=1}^n X_i]$  ではあるが、 $\mathbf{E}[H_i^u(\mathbf{X}_n)] = \frac{S_n}{n} \neq \mathbf{E}[X_i]$  であり、個々人の負担の期待値とは異なる場合あり。

本論文でのリスクシェアのルールの提案は、以下の通りである。

$$\mathbf{H}^{NAM}(\mathbf{X}_n) = (H_1^{NAM}(\mathbf{X}_n), H_2^{NAM}(\mathbf{X}_n), \dots, H_n^{NAM}(\mathbf{X}_n))$$

$$H_i^{NAM}(\mathbf{X}_n) = \frac{S_n}{n} + k \left[ \frac{X_i^2}{2n} - \frac{k1}{2n^2(n-1)} \sum_{i,j}^{n,n} G_{i,j} X_i X_j \right]$$

$G_{i,j} = \text{network adjacency matrix}$ ,  $G_{i,i} = 0$ ,  $k$ : 定数

第二項は個々の損失発生のパナルティ部分でそれを第三項が抑える形。 $\sum_{i=1}^n H_i(\mathbf{X}_n) = \sum_{i=1}^n X_i$  が必ずしも満たされないが、ネットワークが他のプールの構成員とすべて信頼ができていて、 $\mathbf{X}_n$  の要素がすべて同一であればパナルティが消える仕組みで、 $\sum_{i=1}^n H_i(\mathbf{X}_n) = \sum_{i=1}^n X_i$  も満たされる。(それ以外の場合、この部分はプールのプラス収益なので事業費にあてる等が考えられる。)

$$H_i^{NAM}(\text{Full Network}) = \frac{S_n}{n} + k \left[ \frac{X_i^2}{2n} - \frac{1}{2n^2(n-1)} \sum_{i,j}^{n,n} (1 - \delta_{i,j}) X_i X_j \right]$$

$$\mathbf{E} \left[ \sum_{i=1}^n H_i^{NAM}(\text{Full Network}) \right] = \mathbf{E} \left[ \sum_{i=1}^n \frac{S_n}{n} \right] + 0 = \mathbf{E} \left[ \sum_{i=1}^n X_i \right]$$

これは個々人の損失の大きさでパナルティをかけつつ、プールの質を向上させる(ネットワークができていて、信頼が醸成されている、すなわち、プールとしてより損失発生を防ぐ協力体制ができていて) インセンティブを与える。

ここで、固有値 **eigen value** の最大のもの(固有値 **centrality**) との関係を見る。個々の信頼関係がすべてできていれば ( $G_{i,j} = 1$ ,  $G_{i,i} = 0$ ) であり、(最大の) 固有値は  $n-1$  である。

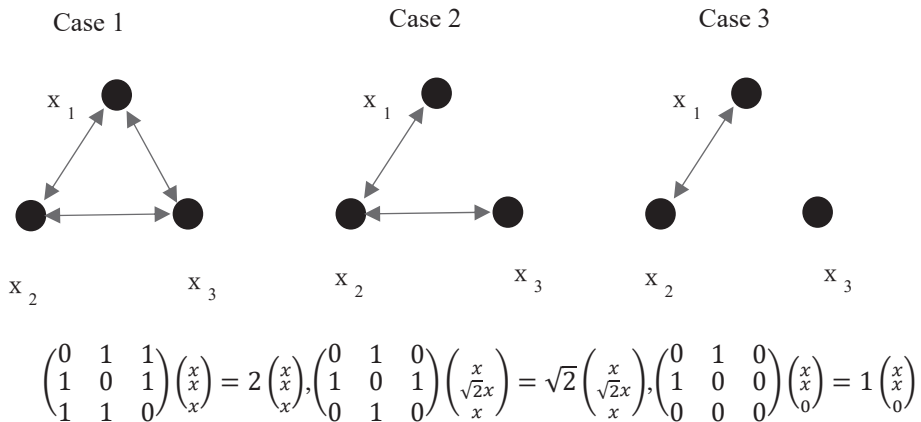
$$\begin{pmatrix} 0 & 1 & \dots & 1 & 1 \\ 1 & 0 & \dots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \dots & 0 & 1 \\ 1 & 1 & \dots & 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ x \\ \dots \\ x \\ x \end{pmatrix} = (n-1) \begin{pmatrix} x \\ x \\ \dots \\ x \\ x \end{pmatrix}$$

$$(n-1)(x \ x \ \dots \ x) \begin{pmatrix} x \\ x \\ \dots \\ x \\ x \end{pmatrix} = n(n-1)x^2$$

これからも、 $\frac{1}{2n^2(n-1)} \sum_{i,j}^{n,n} G_{i,j} X_i X_j$  の項は  $\frac{X_i^2}{2n}$  と打ち消し合うことがわかる。

また、3人の場合（図 C1 参照）を考え具体的な数値でみる。Xi が同一  $x$  であると、Case 1 の  $\sum_{i,j}^{n,n} G_{i,j} X_i X_j$  は  $6 E(x^2)$  であり、全体の期待値をとると、第三項期待値は  $E(x^2) \times 1/6$  となり、 $1/6 \times E(x^2)$  である第二項期待値と打ち消し合いゼロとなる。Case 2 の場合は  $\sum_{i,j}^{n,n} G_{i,j} X_i X_j$  が  $4 E(x^2)$  で、第三項期待値は  $E(x^2)/9$  となり第二項期待値と打ち消しあわない。Case 3 では第三項期待値は  $E(x^2)/18$  であり、同じく第二項と打ち消さない。

図 C1 3人によるネットワーク 3 例と対応する隣接行列の固有値



出所：筆者作成

$\sum_{i,j}^{n,n} G_{i,j} X_i X_j$ （信頼関係ペアの数の 2 倍）の減少と同じくして（Case 1, Case 2, Case 3）の固有値も減少、 $(6, 4, 2) E(x^2)$  に対して、 $(2, \sqrt{2}, 1)$  となっている。

別の視点から解説すると、Case 1 では  $x_1, x_2, x_3$  が互いにすべて信頼関係があるので、リスクシェア負担は各人同一で平等、かつ、他の Case と比較して最も負担が低い。Case 2 は固有値が小さくなり Case 1 よりも信頼関係の数で劣る。Case 2 ではまず  $x_2$  のリスクシェア負担が  $x_1, x_3$  より小さい。これは  $x_2$  は  $x_1$  と  $x_3$  から両方の信頼関係があるのでリスクシェアが相対的に負担が少なくなるが、 $x_1$  と  $x_3$  は相対的に  $x_2$  よりも高めの負担が必要である。Case 3 でもっとも固有値が小さいため信頼関係はもっとも希薄。 $x_3$  が独立しておりネットワークによる恩恵のない形でのリスクシェア負担となる。また、 $x_1$  と  $x_2$  は信頼関係があるので若干はリスクシェア負担が軽減される。

（2023 年 7 月 27 日受理）