

LM-10

安全な電子商取引のための分割取引手法と保険の利用

Installment Methods and Insurance Institutions for Safety Electronic Trades

伊藤ちひろ[†]岩井原瑞穂[†]上林弥彦[†]

ITO Chihiro

Mizuho IWAHARA

Yahiko KAMBAYASHI

1 はじめに

インターネット利用の普及により、電子商取引の機会が増大している。電子商取引の特徴は、互いに会ったことのないような当事者間での金品の授受が行われることである。このため、相手の信用度は大きな問題になる。

既存の研究では、公正な取引のために信頼できる第三者機関 (Trusted Third Party: TTP) を経由して商品と代金を交換するプロトコルや機構が提案されてきた [2][3][1]。TTP を介した基本的な取引を図 1 に示す。客は金銭を、ベンダは品物をそれぞれ TTP に託す。両方が預けられたことを確認した後、TTP は、金銭をベンダに、品物を客に渡すことで取引が完了する。これらの方法では、TTP は両

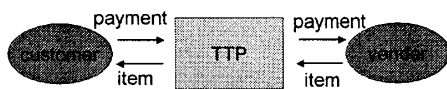


図 1: TTP を介した取引

方の参加者から常に信用されており、正直であり事故も発生しないことを前提としている。しかし、様々な参加者が多様な相手に対して行うインターネット上の商取引にこの仮定をそのまま適用することは困難である。

本稿では、このような取引を安全に行うため二つの手法を提案する。一つは、取引相手や仲介者のリスクを考慮した分割取引によって、受ける損害の量に限度を設定することである。もう一つは、補償制度を利用した取引であり、あらかじめ保険料を支払うことによって、受けた損失を補填する。本稿では特に、損失の全額を補填する場合について述べるが、分割取引と組み合わせることもできる。設定したリスク限度内での取引が不可能である場合にも、限度超過分を保険で補填することで取引が行えるようになる。

2 分割取引の前提条件と記法

2.1 対象商品

分割取引の対象となるのは、何らかの方法で分割してもそれぞれに商品価値が発生するような電子データである。

分割の方法は、商品によって様々である。例えば音楽データであれば、最初は低ビットレートでエンコードしたものを送付し、支払い毎に音質を上げていくことが考えられる。画像データでは、解像度や大きさ、色数を変化させることによって分割送付が可能となる。また、ソフトウェアの場

合、ライセンスを使用毎 (pay-per-use) や一定期間毎に配信する場合や、最初は機能制限版を販売し、支払いがある毎にその制限を外してゆく場合などに、本手法が利用できる。

2.2 リスクと限度枠

電子商取引においては、一般に商品と対価を同時に交換することは困難であるため、取引が中断されると参加者のいずれかが損害を被るような時点が存在する。ある時点において取引参加者に発生し得る損害の量をリスクと呼ぶ。

取引において、どれだけのリスクを許せるかということは取引相手の信頼度に依存する。また、取引参加者 A から B への信頼度と、 B から A への信頼度は等しいとは限らないので、リスク限度枠を有向グラフの枝の重みとして表現し、これをリスク限度枠グラフと呼ぶ。

図 2 の上部はリスク限度枠グラフの例である。買い手 C が仲介者 M を経由して売り手 S から商品を購入する場合のリスク限度を示している。例えば $L(C, M) = 9$ という表記は、 C が M に許容するリスク限度が 9 であることを示す。

$$\begin{array}{ccc} L(C, M) = 9 & L(S, M) = 8 \\ \textcircled{C} \xrightarrow{\quad} \textcircled{M} & \textcircled{S} \xleftarrow{\quad} \textcircled{M} \\ L(M, C) = 2 & L(M, S) = 3 \end{array}$$

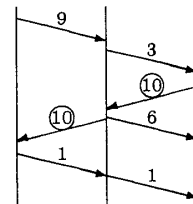


図 2: 仲介取引の例

3 限度枠による分割取引

ここでは仲介者を利用した分割取引について考える。仲介者は、買い手が支払い不能になった場合や売り手が商品送付不能になった場合、発生する損害を補填するものとする。仲介者が補填可能な最大額は、他の参加者に対し設定したリスク限度枠となる。仲介者にとってのリスクは、買い手と売り手に対してそれぞれ個別に設定することとする。例えば、買い手から代金を預かった場合に低減されるのは買い手に対するリスクであって、売り手に対するリスクではない。

図 2 のように、売り手 S から購買者 C が価格が $P(g) = 10$ である商品 g を購入する場合を考える。商品金額 $P(g) = 10$ が $L(S, M) = 8$ を越えているので、初期状態では商品の発送は行えない。したがって、 C が M に前払金 $L(C, M) = 9$

[†] 京都大学大学院情報学研究科

を委託することで取引を開始する。前払金を受け取った M は、そのうち $L(M, S) = 3$ だけを S に送金する。これを受け取った S が M に送付可能となる商品の最大額は、初期状態の $L(S, M) = 8$ に加え、 $\min(L(C, M) + L(M, S)) + L(S, M) = 11$ となり、 S は M に 10 円の商品を送付することが可能となる。また、 M の C へ送付可能なのは $L(C, M) + L(M, C) = 11$ であるため、 S からの商品を受け取った M は、これを C へ送付可能である。商品を受け取った C は、残金 1 円を M に送付し、 M は S に送付することで、取引は終了する。

このように仲介者 M を利用した g の分割取引が可能となるのは、 $L(M, S) + L(S, M)$ 、 $L(C, M) + L(S, M)$ 、 $L(C, M) + L(M, C)$ のいずれもが $P(g_i)$ 以上であることである。ただし $i = 1, 2, \dots, m$ とする。

取引不能と判定された場合は、商品の分割を細かくする、あるいは、次節で述べるような保険の利用が考えられる。

4 保険の利用

保険利用の前提として、保険の提供会社は信用でき、取引によって発生した損害は全て事前に購入した保険によって補填されるものとする。

4.1 買い手と仲介者間の保険料

買い手 C が、仲介者 M を通じて売り手 S から商品 g を購入するとき、 C が意図的にまたは事故によって代金不払いが起こる確率を p とする。また同様に、 M が業務続行不可能になる確率を αp とする。仲介者の信用度は十分高く、 $0 < \alpha < 1$ とする。またこれらの確率は、信用情報機関等から情報提供を受けるものとする。

C が M に前払金 x を委託することを考える。委託した直後に M が業務不能になった場合、 C が受ける損害は x に等しい。一般に、これを全て補填するような保険は $\alpha p x$ 以下で購入することはできないため、ここでは最小値である $\alpha p x$ を C の M に対する保険料とする。また、 M が S から委託された商品 g を C に発送した直後に事故が発生した場合、 M の受ける損害は商品価格を $P(g)$ として、 $r(M, C) = P(g) - x$ である。したがって、これを補填するための保険料は $pP(g) - px$ となる。

これらは仲介手数料として全て買い手が支払うこととすれば、保険料の合計は $R_1 = p[P(g) - (1 - \alpha)x]$ であり、 x を横軸にとれば R は図 3 のような直線となる。従って、信頼度の十分高い仲介者を利用する場合は前払金が多いほど少ない保険料で取引が可能になる。

4.2 仲介者と売り手間の保険料

M が C から預かった前払金を S に送金し、これを受け取った S が M に商品を委託する場合を考える。 S が業務不能になる確率を q 、 $r = \beta q$ ($1 < \beta < 0$) とすれば、保険料の合計 R_2 は、前の場合と同様にして、 $R_2 = q[(1 - \beta)x + \beta P(g)]$ と求められ、前払金が多いほど保険料は増大する。

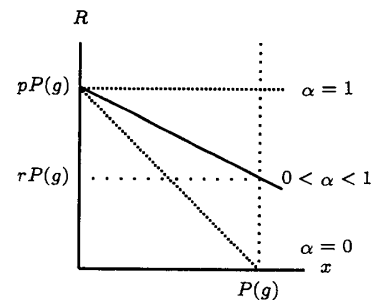


図 3: 前払金と保険料の関係

4.3 取引全体の保険料

取引全体としての保険料は、 R_1, R_2 を合計すると

$$R = R_1 + R_2 = p[(1 + \alpha)P(g) - (\frac{\alpha}{\beta} + \alpha - 2)x]$$

となる。これを最小にする前払金は、 $\alpha > \frac{2\beta}{1+\beta}$ より $2p < q + r$ のとき、 $x = P(g)$ であり保険料は $R = (r + q)P(g)$ となる。また、 $2p < q + r$ のとき、前払金 $x = 0$ のときに保険料は最小の $R = (p + r)P(g)$ となる。 $2p = q + r$ のときは、保険料は前払金によらず一定額 $R = (r + q)P(g)$ となる。

4.4 分割取引との併用

保険利用は、前節で述べた限度枠による分割取引と組み合わせることもできる。設定したリスク限度内での取引が不可能である場合にも、限度超過分を保険で補填することで取引が行えるようになる。

例えば $L(C, M) + L(S, M) < P(g)$ 、 $L(C, M) > L(M, S)$ の場合を考える。 g がこれ以上分割できないとき、このままでは S から M への商品発送が行えない。そこで、リスクの超過分 $P(g) - L(C, M) - L(S, M)$ を補填するような保険を C が購入すると、 C は $P(g) - L(S, M)$ の前払金を送付可能となる。もし事故などで商品が届かない場合、 C の受ける損害は、最初に設定された $L(C, M)$ となる。

5 おわりに

本稿では、電子商取引において参加者に与える信頼に限度を設け、分割取引を行うことによりリスクの分散を図る手法を提案した。また、保険制度を利用した取引における保険料と前払金との関係について述べた。

参考文献

- [1] M. K. Franklin, M. K. Reiter, "Fair Exchange with a Semi-Trusted Third Party", *Proc. 4th ACM Conf. on Computer and Communication Security*, April 1997.
- [2] S. P. Ketchpel, H. Garcia-Monia, "Making Trust Explicit in Distributed Commerce Transactions", *Proc. 16th ICDCS*, pp. 270-281, Hong Kong, May 1996.
- [3] J. Su, D. Manchala, "Building Trust for Distributed Commerce Transactions", *Proc. 17th ICDCS*, pp. 322-329, Baltimore, May 1997.