

情報セキュリティと経済学 Information Security and Economics

松浦幹太*

Kanta Matsuura

あらまし 情報セキュリティシステムのトータルな管理は、人間的側面や社会的側面の問題のため、きわめて難しい。実際、多くの惨事が、不十分な動機付けに起因する管理の甘さや不徹底によって発生する。多くの不安は、結局経済的にどのようなリスクを負っているのかが不確かであることによって生じている。その他、普及の困難さも含めて、根深い問題の多くは経済学的に定量化できる可能性を秘めている。本論文では、そのような視点で情報セキュリティシステムを論じることに役立つ研究の動向を概観する。さらに、情報セキュリティに対する投資の最適化理論を、保険まで含めたセキュリティマネジメントに活用するための方策について考察する。

キーワード セキュリティマネジメント, 経済的リスク, 最適投資, 保険, 動機付け.

1 はじめに

情報セキュリティと経済学にまたがる学際的研究が、電子社会へ向けて需要性を増している。例えば筆者は、2000年度からそのような領域に取り組み [1]、中でも公開鍵証明書廃棄問題のように予測不能な確率事象に起因するリスクの研究に注目している [2]–[9]。また、世界の情報セキュリティ研究者の中に、Ross Anderson [10], [11] らを中心として情報セキュリティと経済学との接点を見出そうとする動きが広がり、2002年5月にはカリフォルニア大学バークレー校で Workshop on Economics and Information Security が開催され、2回目をよりフォーマルな会議として開催することが決まっている。

確かに、情報セキュリティシステムのトータルな管理は、人間的側面や社会的側面の問題のためきわめて難しい。多くの惨事が、不十分な経済的動機付けに起因する管理の甘さや不徹底によって発生する。多くの不安は、結局経済的にどのようなリスクを負っているのかが不確かであることによって生じている。その他、「なかなか普及しないこと」も含めて根深い問題の多くは、経済学的に定量化できる可能性を秘めている。

本稿では、それらの問題意識を動機として、当該学際研究分野の動向を概観する。さらに、それらを保険まで含めた包括的セキュリティマネジメントに活用するための方策について、焦点を絞って考察する。

2 分類

本章では、広い意味で情報セキュリティと経済学にまたがる学際領域の研究を7つに分類する。最初の3つ(2.3節まで)は狭義には経済学と関係しないが、3章で整理する「研究の流れ」を見る上で必要なので、あえて割愛しない。

2.1 プリミティブ

電子社会における安全な経済活動のために役立つ情報セキュリティの要素技術が、情報セキュリティと経済学に関係する研究分野で最古のものであろう。電子マネーに利用されるブラインド署名 [12] が代表例である [13]。この範疇を学際的というのは無理があるかもしれないが、例えば Financial Cryptography 国際会議では、プリミティブに関する発表も少なくない [14]。

2.2 プロトコル

経済活動のためのセキュリティプロトコル技術として、数々の電子マネー・電子決済技術 [15]–[16]、オークションプロトコル、チケット(電子権利)プロトコル [17] などが研究されてきた。それらには、既存の金融インフラに強く依存するものとそうでないものがある。強く依存する代表例は、SET (Secure Electronic Transaction) のようにクレジットカードのインフラを利用するものである [18]。そうでない例には、セキュリティプロトコルの基礎研究として重要なものが少なくない [19]。

一方、経済学的に推奨される体制を実現するために役立つセキュリティプロトコルの研究も、この範疇に属す

* 東京大学生産技術研究所・大学院情報学環, 〒153-8505 目黒区駒場 4-6-1, Institute of Industrial Science, Interfaculty Initiative in Information Studies, University of Tokyo, Komaba 4-6-1, Meguro-ku, Tokyo 153-8505, JAPAN.

る。例えば、ネットワーク経済学の結果によれば [20]、セキュリティサービスの利用実績に応じて課金額などの定量化を図ると社会全体としてコストシェアリングが効率的になると考えられる。その実現のためには、課金額を裏付ける利用記録が信用できなければならず、しかるべき情報セキュリティのプロトコル技術が必要となる [21]–[26]。

2.3 流通促進

電子的な商品が流通する市場を普及させるための研究、具体的には、コンテンツやソフトウェアに関する権利を適切に管理するために役立つ技術 [27]–[30] や、運用管理方式のトータルな社会科学的分析や最適化 [31] の研究が重要になっている。ただし、方式を非公開とすることで安全性を確保するのは望ましくないが、多くの商用 DRM(Digital Right Management) システムがそうであるのは残念である [32]。

2.4 モデリング

セキュリティマネジメントでは、安全性・脆弱性の定量化に頭を悩ますことが少なくない。あるいはまた、情報セキュリティ機能をいかに価格付けするかということも難しい問題である。これらの問題に取り組むためには、まず、適切なモデリングが必要であり、経済学的な考え方を応用した研究がいくつも発表されている [33]。例えば、攻撃に要するコストをセキュリティの測度とする研究 [34] などは自然な試みであろう。公開鍵基盤における証明書廃棄問題のように予測不能な確率事象に起因するリスクを対象として筆者が行ってきた一連の研究 [1]–[9] も、その根幹はモデリングである。

2.5 動機付け

攻撃者に攻撃を控えさせるための動機付けとして、攻撃に要するコストを高めたり [35]–[39]、攻撃者の経済的リソースを制限したりする [40] という考え方がある。あるいはまた、情報セキュリティ機能を備えたシステムに関する責任 (liability) について、論理的に考察することも重要である。より積極的に、責任を系統的に移転させるための研究も行われている [41]。これらは、概ね抑止力としてはたらく経済的な動機・理由を利用している。

一方、2002 年 5 月の Workshop on Economics and Information Security において盛んに討論されたのは、情報セキュリティ技術を利用させるための経済学的な動機付けである [42]。標準化によるコスト削減がセキュリティ機能導入を後押しする効果 [43] や、プライバシー関連技術の費用対効果に関する疑問 [44] — これらの根幹にあるのは、「世の中にセキュリティ機能を利用してもらうために経済学的動機付けを与えることの重要性」である。広義に解釈すれば、努力 (effort) を入力として成功

(successful outcome) 確率を出力とする関数を考えて費用対効果を最適化することによりセキュリティ利用調整を考察するフレームワーク [45] も、この範疇に属する。

2.6 セキュリティ市場論

2.5 節で述べた動機付けの問題に取り組むための基礎研究として、セキュリティ市場論がある。その代表的な 2 つのアプローチは、以下の通りである。

第 1 のアプローチは、最適な情報セキュリティ投資を論じる研究である。それらは、現時点では、投資額・規模を論じている [46]–[48]。これは、金融工学的には極めて初歩的な手法に過ぎない。今後は、「いつ」どのような手順でなすべきかを考察するタイムシリーズとしての考え方が重要になると予想され、例えば real option の手法 [49], [50] を用いることが有効だと考えられる。

第 2 のアプローチは、情報セキュリティ市場における市場原理を考察する分析的な研究である。主流なのは、分散システム原理の観点から、一般市場と情報セキュリティとの相違やあるいは逆に類似性を論じる考え方である。ただし、情報セキュリティ分野では規制の問題などが相対的に顕著なため、この種の分析的な研究は難しいという指摘がある [51]。イノベーションのメカニズムや社会背景を分析して新たな提言を探る研究 [52] も、このアプローチの一種である。

2.7 経済社会インフラ

情報セキュリティのアプリケーションを安心して利用するためには、技術以外の経済社会的インフラの整備や調整も必要である。代表的なものが、保険である [53]–[55]。たとえ安全性が証明されている要素技術を利用しているとしても、現実世界では何らかの損害が発生し得る。そのリスクを負う主体が不適切ならばリスク移転を行う経済社会的仕組みが必要となり、保険やその他の金融商品を考えなければならない [1]–[9], [56]。保険や金融の健全な市場のためには健全な情報流通が必要であるが、「『情報セキュリティに関する情報』がなかなか周知徹底しない」という問題を、経済学的・社会制度的観点から分析する試みも重要な関連がある [57]。また、より基本的な経済インフラ調整として、電子マネーが顕在化するようになった時代のマネーサプライに関しても、独自の研究が重要である [58]。マネーの定義に立ち戻って、逆に必須技術とその性質・要件を導出する分析も重要である [59]。あるいはまた、電子マネー発行体の破綻への対処として、利用規約や信託を論じる必要もある [60], [61]。

2.2 節に分類される研究が本節に分類される研究を無視して行われれば、真に社会に普及するシステムは容易には登場しないであろう。

3 研究対象の変化

2章の分類にしたがって、当該学際領域における研究潮流の変化を見ることが出来る。実際、変化前を代弁する会議として Financial Cryptography 2001 (以下では FC2001 と表記)、変化後を代弁する会議として Workshop on Economics and Information Security (以下では WEIS と表記) を取り上げ、それぞれの発表論文(若干の分類不能論文を除き、各々27編、25編の論文を対象とした)を分類すると、表1のようになる。分類の微妙な論文についても筆者の独断で分類したのであまり細かな議論はできないが、一見学際的に思える FC2001 と比べても、WEIS の流れには経済学とのより強い連携を必要としている傾向が反映されていることがわかる。

表 1: 研究の流れの変化 (FC2001→WEIS). 数値は、各会議における割合を%で表示.

分類	FC2001	WEIS
プリミティブ	33.3	0.0
プロトコル	33.3	0.0
流通促進	18.5	4.0
モデリング	7.4	24.0
動機付け	3.7	32.0
セキュリティ市場論	0.0	32.0
経済社会インフラ	3.7	8.0

4 セキュリティマネジメントへの活用

これまでに論じてきた学際的な研究の中でもっともわかりやすい研究の1つは、情報セキュリティに対する最適投資の理論であろう。本章では、最近まとめられた最適投資理論 [48] を例にとり、保険まで含めた包括的セキュリティマネジメントに活用するための拡張方法を示す。

4.1 最適投資

Gordonらのモデル (Gordon-Loeb モデル)[48] では、ある情報セットを保護するために投じる情報セキュリティ投資額 z として最適な値を導出しその性質を論じるために、以下のパラメータを考える。

λ : 保護が破られた場合の損失

t : 攻撃などの脅威が発生する確率

v : 投資前に攻撃などの脅威が発生した場合にそれが成功する条件付き確率。脆弱性 (vulnerability) と呼ばれる。

S : 投資後に攻撃などの脅威が発生した場合にそれが成功する条件付き確率。 z と v の関数として $S(z, v)$ のように記述されるが、特定の関数系でモデル化した場合にはそのモデルパラメータも定数として記述に含まれる。

例えば

$$S(z, v) = v^{\alpha z + 1} \quad (1)$$

という関数系を仮定すると、「『脆弱性が高くなればなるほど最適な情報セキュリティ投資額が上昇する』というわけではないこと」が導かれる。ただし $\alpha > 0$ は、情報セキュリティがいかに有効に機能するかを表現するパラメータで、情報セキュリティの生産性 (productivity) と呼ばれる。最適な情報セキュリティ投資額は、その投資による純利益の期待値

$$ENBIS = \{v - S(z, v)\} t \lambda - z \quad (2)$$

を最大化する

$$z = z^*(v) = \frac{\ln \{-1 / (\alpha v t \lambda \ln v)\}}{\alpha \ln v} \quad (3)$$

として与えられる。

4.2 包括的最適化への拡張

Gordon-Loeb モデルでは、損失 λ が定数である。すなわち、技術や管理サービスとしての情報セキュリティに対する投資を考えている。また Gordon-Loeb モデルでは、投資額変数 z が連続的である。すなわち、投資対象は構成要素単位ではなく、総体として扱っている。ところが、実際のセキュリティマネジメントでは、このような Gordon-Loeb モデルにそぐわない「保険」も扱わなければならない。そこで、以下のように保険も包括的に扱う手法を提案する。

今、購入候補となっている保険商品 $1, 2, \dots, m$ の料金が $z_i (\geq 0)$ ($i = 1, 2, \dots, m$) であり、それらによって見込まれる被害額の減少が $(0 \leq) \lambda_i (\leq \lambda)$ ($i = 1, 2, \dots, m$) であるとする¹。この時我々は、次の最適化を行うべきである:

$$\max_{i, z} \{[v - S(z, v)] t (\lambda - \lambda_i) - z - z_i\} \quad (4)$$

我々は、この最大値を与える保険商品 j と情報セキュリティ投資 $z = z^*$ を求め、最適投資 (z_j, z^*) を構成したい。すなわち、保険と情報セキュリティ投資の両方を考慮した期待純利益を最大化する保険商品と情報セキュリティ投資額を求めたい。

この時、関数系として式 (1) を採用したモデルでは、次の定理が成り立つ。

¹ $z_i = \lambda_i = 0$ なる i は、「保険なし」を表現する。

定理 4.1 (包括最適解) 保険の導入が技術・管理サービスによる情報セキュリティの生産性に影響を与えないとすれば、最適投資 (z_j, z^*) は、

$$vt(\lambda - \lambda_i) + \frac{1 - \ln\{-1/(\alpha vt(\lambda - \lambda_i) \ln v)\}}{\alpha \ln v} - z_i$$

の最大値を与える i を j とし、

$$z^* = \frac{\ln\{-1/(\alpha vt(\lambda - \lambda_j) \ln v)\}}{\alpha \ln v}$$

とすることで与えられる。

(略証) 保険 i を固定した情報セキュリティの最適化問題に対する最適解は

$$z = z_i^*(v) = \frac{\ln\{-1/(\alpha vt(\lambda - \lambda_i) \ln v)\}}{\alpha \ln v} \quad (5)$$

で与えられる。これを包括的最適化問題の目的関数に代入すれば、定理が得られる。□

5 むすび

本論文では、情報セキュリティと経済学の学際的な研究動向を、7つの研究分類に基づいて整理した。さらに、情報セキュリティに対する投資の最適化理論を、保険まで含めたセキュリティマネジメントに活用するための方策について考察し、特定のモデルに対する最適投資定理を導いた。研究分野黎明期のモデルは、一見、単純すぎるようにも見える。重要なことは、包括的な取り組みによって実際の統計データを用いた実証研究を可能とする拡張であろうと思われる。

参考文献

- [1] K. Matsuura. “Security tokens and their derivatives”. Technical Report 29, Centre for Communications Systems Research, University of Cambridge, February 2001.
- [2] 松浦幹太. “デジタル・トークンの不確定性と二項モデルによるリスクヘッジ評価”. 情報処理学会研究報告, CSEC, No. 13, pp. 31–36, May 2001.
- [3] K. Matsuura. “Digital security tokens and their derivatives”. In *7th International Conference of the Society for Computational Economics (SCE'01)*, New Haven, CT, June 2001.
- [4] K. Matsuura. “Security token and its derivative in discrete-time models”. In *5th World Multiconference on Systemics, Cybernetics and Informatics*, Orlando, FL, July 2001.

- [5] K. Matsuura. “A Derivative of Digital Objects and Estimation of Default Risks in Electronic Commerce”. In S. Qing, T. Okamoto, and J. Zhou, editors, *Proceedings of Third International Conference on Information and Communications Security (ICICS'01)*, Lecture Notes in Computer Science 2229, pp. 90–94, November 2001. Springer-Verlag.
- [6] 松浦幹太. “電子セキュリティトークンのモデル化と応用”. 2002年暗号と情報セキュリティ・シンポジウム (SCIS2002) 予稿集, Vol. I, pp. 73–78, 2002.
- [7] K. Matsuura. “Digital security tokens in network commerce: Modeling and derivative application”. In *8th International Conference of the Society for Computational Economics: Computing in Economics and Finance (CEF 2002)*, Aix-en-Provence, France, June 2002.
- [8] 松浦幹太. “電子セキュリティトークンとその派生商品”. 情報処理学会論文誌, Vol. 43, No. 8, pp. 2372–2380, August 2002.
- [9] K. Matsuura. “Digital security tokens and their derivatives”. *Netnomics* (to appear)
- [10] R. Anderson. “Why Information Security is Hard—An Economic Perspective—”. 2002 Applied Computer Security Applications Conference.
- [11] R. Anderson. “Why Information Security is Hard—An Economic Perspective—”. *18th Symposium on Operating System Principles*, 2001.
- [12] D. Chaum. “Blind signatures for untraceable payments”. In *Advances in Cryptology: Proceedings of Crypto 82*, pp. 199–203, 1983. Plenum Press.
- [13] D. Chaum and S. Brands. “Minting electronic cash”. *IEEE SPECTRUM*, Vol. 34, No. 2, pp. 30–34, February 1997.
- [14] D. Naccache, D. Pointcheval, and C. Tymen. “Monotone signatures”. In P. F. Syverson, editor, *Financial Cryptography (FC2001)*, Lecture Notes in Computer Science 2339, pp. 305–318, 2001. Springer-Verlag.
- [15] T. S. Perry. “Electronic money: toward a virtual wallet”. *IEEE SPECTRUM*, Vol. 34, No. 2, pp. 18–19, February 1997.
- [16] P. S. Gemmell. “Traceable e-cash”. *IEEE SPECTRUM*, Vol. 34, No. 2, pp. 35–37, February 1997.

- [17] 寺田雅之, 花館威之, 藤村考, 関根純. “電子権利流通基盤のための汎用的な原本性保証方式”. 情報処理学会論文誌, Vol. 42, No. 8, pp. 2017–2029, August 2001.
- [18] M. A. Sirbu. “Credits and debits on the Internet”. *IEEE SPECTRUM*, Vol. 34, No. 2, pp. 23–29, February 1997.
- [19] T. Okamoto and K. Ohta. “Disposable zero-knowledge authentications and their applications to untraceable electronic cash”. In *Advances in Cryptology — CRYPTO’89*, pp. 481–496, Berlin, New York, Tokyo, 1990. Springer-Verlag. Lecture Notes in Computer Science 435.
- [20] N. Brownlee. “Internet pricing in practice”. In Lee W. McKnight and Joseph P. Bailey, editors, *Internet Economics*, pp. 77–90, 1997. MIT Press.
- [21] M. K. Franklin and D. Malkhi. “Auditable Metering with Lightweight Security”. In *Pre-Proceedings of Financial Cryptography’97*, pp. 1–9, February 1997.
- [22] M. Naor and B. Pinkas. “Secure and efficient metering”. In *Advances in Cryptology — EURO-CRYPT’98*, pp. 576–590, 1998. Springer-Verlag. Lecture Notes in Computer Science 1403.
- [23] M. Naor and B. Pinkas. “Secure Accounting and Auditing on the Web”. *Computer Networks and ISDN Systems*, pp. 541–550, 1998.
- [24] B. Schneier and J. Kelsey. “Cryptographic support for secure logs on untrusted machines”. In *Proc. of The Seventh USENIX Security Symposium*, pp. 53–62, January 1998.
- [25] B. Schneier and J. Kelsey. “Secure audit logs to support computer forensics”. *ACM Trans. on Information and System Security*, Vol. 2, No. 2, pp. 159–176, May 1999.
- [26] J. Kelsey and B. Schneier. “Minimizing bandwidth for remote access to cryptographically protected audit logs”. In *Second International Workshop on the Recent Advances in Intrusion Detection (RAID’99)*, September 1999.
- [27] S. H. Low, N. F. Maxemchuk, and A. M. Lapone. “Document identification for copyright protection using centroid detection”. *IEEE Trans. Commun.*, Vol. 46, No. 3, pp. 372–383, March 1998.
- [28] 森本典繁. “電子透かし技術”. 電子情報通信学会誌, Vol. 82, No. 8, pp. 836–838, August 1999.
- [29] Y. Watanabe, Y. Zheng, and H. Imai. “Software copyright protection in the presence of corrupted providers”. In *Proceedings of 2000 International Symposium on Information Theory and Its Applications (ISITA2000)*, pp. 501–504, 2000.
- [30] S. Katzenbeisser and F. Petitcolas (eds). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House Publishers, Boston, London, 2000.
- [31] R. A. Gehring. “Software Development, Intellectual Property Rights, and IT Security”. In *Workshop on Economics and Information Security*, May 2002.
- [32] M. Stamp. “Risks of Digital Right Management”. *Communications of the ACM*, Vol. 45, No. 9, p. 120, September 2002.
- [33] B. Arbaugh. “Security: Technical, Social, and Legal Challenges”. *IEEE Computer*, Vol. 35, No. 2, pp. 109–111, February 2002.
- [34] S. Schechter. “Quantitatively differentiating system security”. In *Workshop on Economics and Information Security*, May 2002.
- [35] K. Matsuura and H. Imai. “Protection of Authenticated Key-Agreement Protocol against a Denial-of-Service Attack”. *Científica*, Vol. 2, No. 11, pp. 15–19, September 1998.
- [36] A. Juels and J. Brainard. “Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks”. In S. Kent, editor, *Proc. of NDSS’99 (Networks and Distributed Security Systems)*, pp. 151–165, 1999.
- [37] K. Matsuura and H. Imai. “Modified Aggressive Modes of Internet Key Exchange Resistant against Denial-of-Service Attacks”. *IEICE Transactions on Information and Systems*, Vol. E83-D, No. 5, pp. 972–979, May 2000.
- [38] C. Dwork and M. Naor. “Pricing via processing or combatting junk mail”. In E. F. Brickell, editor, *Advances in Cryptology — CRYPTO’92*, Lecture Notes in Computer Science 740, pp. 139–147, August 1993. Springer-Verlag.

- [39] C. Dwork and M. Naor. “Pricing via processing or combatting junk mail”. Technical Report CS95-20, Faculty of Mathematical Sciences, The Weizmann Institute of Science, 1995.
- [40] Y. Yemini, A. Dailianas, D. Florissi, and G. Huberman. “MarketNet: Market-Based Protection of Information Systems”. In *Proceedings of First International Conference on Information and Computation Economics (ICE’98)*, October 1998.
- [41] R. Yahalom. “Liability transfers in network exchanges”. In *Workshop on Economics and Information Security*, May 2002.
- [42] A. Acquisti. “Privacy and security of personal information: Economic incentives and technological solutions”. In *Workshop on Economics and Information Security*, May 2002.
- [43] B. Fox. “Internet TAO: The Microeconomics of Internet Standards Setting”. In *Workshop on Economics and Information Security*, May 2002.
- [44] J. Feigenbaum, M. J. Freedman, T. Sander, and A. Shostack. “Economic Barriers to the Deployment of Existing Privacy Technologies”. In *Workshop on Economics and Information Security*, May 2002.
- [45] Hal R. Varian. “System reliability and free riding”. In *Workshop on Economics and Information Security*, May 2002.
- [46] Kin Sing Leung. “Diverging economic incentives caused by innovation for security updates on an information network”. In *Workshop on Economics and Information Security*, May 2002.
- [47] Kevin J. Soo Hoo. “How Much Is Enough? A Risk Management Approach to Computer Security”. In *Workshop on Economics and Information Security*, May 2002.
- [48] L. A. Gordon and M. P. Loeb. “The economics of information security investment”. *ACM Transactions on Information and System Security*, Vol. 5, No. 4, pp. 438–457, November 2002.
- [49] Lenos Trigeorgis. *Real Options: Managerial Flexibility and Strategy in Resource Allocation*. MIT Press, Cambridge, 1996.
- [50] Jeannette Capel. “A Real Options Approach to Economic Exposure Management”. *Journal of International Financial Management and Accounting*, Vol. 8, No. 2, pp. 87–113, 1997.
- [51] C. E. Landwehr. “Improving information flow in the information security market”. In *Workshop on Economics and Information Security*, May 2002.
- [52] 江波戸謙, 松浦幹太. “SCISにおける産学連携の状況”. 2003年暗号と情報セキュリティ・シンポジウム (SCIS2003), 浜松, January 2003.
- [53] M. K. Reiter and S. G. Stubblebine. “Toward acceptable metrics of authentication”. In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, pp. 10–20, May 1997.
- [54] M. K. Reiter and S. G. Stubblebine. “Authentication metric analysis and design”. *ACM Transactions on Information and System Security*, Vol. 2, No. 2, pp. 138–158, May 1999.
- [55] W. Yurcik and D. Doss. “CyberInsurance: A Market Solution to the Internet Security Market Failure”. In *Workshop on Economics and Information Security*, May 2002.
- [56] B. Blakley. “The measure of information security is dollars”. In *Workshop on Economics and Information Security*, May 2002.
- [57] L. A. Gordon, M. P. Loeb, and W. Lucyshyn. “An Economic Perspective on the Information Related to Security Breaches: Concepts and Empirical Evidence”. In *Workshop on Economics and Information Security*, May 2002.
- [58] 石田和彦, 川本卓司. “電子マネーとマネーサプライ”. *IMES Discussion Paper Series*, 日本銀行金融研究所, No. 00-J-8, April 2000.
- [59] L. J. Camp and M. Sirbu. “Critical Issues in Internet Commerce”. *IEEE Communications*, Vol. 35, No. 5, pp. 58–62, May 1997.
- [60] 小澤徹夫. “電子マネーのスキームを約款上, 明確にする必要”. *日経デジタルマネー・システム*, Vol. 13, pp. 22–23, March 1998. “連載企画 電子マネー・電子決済の法的・実務的検討 (1) 契約関係の整理”.
- [61] 寺本振透. “第40回 電子マネーの発行体が倒産したら?”. *INTERNET magazine*, pp. 318–321, July 1998. ネットワーク時代の知的所有権入門.