様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　５　月　１９　日現在

機関番号：　１２６０１
研究種目：　基盤研究(B)（一般）
研究期間：　2013～2016
課題番号：　２５２８００４５

研究課題名（和文）サイバーセキュリティサイエンスの基盤モデルと共通データセットに関する研究

研究課題名（英文）Fundamental Models and Common Datasets for the Infrastructure of Cybersecurity Science

研究代表者

松浦　幹太（Matsuura, Kanta）

東京大学・生産技術研究所・教授

研究者番号：００２９２７５６

交付決定額（研究期間全体）：（直接経費）　　8,200,000円

研究成果の概要（和文）：サイバーセキュリティに関する客観的で再現性のある評価を実現するために、社会科学的理論基盤とデータ基盤に関する基本モデルを確立し、実際の活動やデータに適用するなどして有効性を示した。モデルは主としてセキュリティ投資理論と制度設計理論に根ざし、とくに、マルウェア対策研究用のデータ共有に関する事例研究、仮想通貨システムへのセキュリティ投資効果に関する仮説検証、匿名通信システムの体系的な評価で実際の活動等にインパクトを与える成果を得た。

研究成果の概要（英文）：For the purpose of objective and reproducible evaluation regarding cyber security, this project established basic social scientific models and data infrastructure models. The models are based mainly on security investment theories and mechanism design theories. Their applications in actual cybersecurity activities and implementations supported their effectiveness; successful empirical studies include case studies in data sharing for anti-malware researches, hypothesis testing regarding security investment into virtual currencies, and systematic evaluation of anonymous communication systems.

研究分野：　情報セキュリティ

キーワード：　暗号・認証等　セキュリティ評価・監査　サイバーセキュリティ　マルウェア　仮想通貨　セキュリティ経済学

１．研究開始当初の背景

客観性と再現性を重んじる科学的な評価が不十分なために実際のセキュリティレベルが下がり多くのインシデントにつながっているという意識が高まり、サイバーセキュリティの科学的評価を重視する「サイバーセキュリティサイエンス」に研究の焦点を当てることが喫緊の課題とされていた。実際、米国国防総省委託調査報告（The MITRE corporation:“Science of Cyber-Security”, JASON report, JSR-10-102, November 2010）でセキュリティサイエンス研究推進論の根拠となる学術的および実務的背景が明らかにされ、学会においてもIEEEの専門誌でセキュリティサイエンス特集号が組まれた（D. Evans and S. Stolfo:“The Science of Security”, IEEE Security & Privacy, Guest Editors’ Introduction, Vol.9, Issue 3, pp.16-17, May/June 2011）。これら主要文献で指摘されている共通の課題は、実践的な研究課題になればなるほど科学的な評価に欠けているということであった。

例えば、インシデントの多くは、ヒューリスティックな安全性評価に頼ったり、サービスの提供者や被提供者に適切なインセンティブがもたらされず導入や運用に問題が生じたりしたことが原因である。前者の問題解決には厳密な安全性証明を伴う工学的理論基盤の整備や実験的評価の質を高めるデータ基盤の整備が有効であり、後者の問題解決には多様な利害関係者のインセンティブを分析する社会科学的理論基盤の整備が有効である。しかし、工学的理論基盤の整備は狭義の暗号技術の範囲にとどまっており、データ基盤の整備は進んでいるもののその整備方法自体がヒューリスティックであった。また、社会科学的理論基盤の整備に関しては、有望なアプローチとしてセキュリティ経済学が台頭してきたものの、理論が有用であることを実証する研究が圧倒的に不足していた。

２．研究の目的

背景に示した問題は、サービス科学の観点で反省すれば、サービスの非有形性（無形であるがゆえサービスを受ける前に価値を確かめ難いこと）が大きな原因である。この非有形性が事前価値確認に与える問題を克服するために、サイバーセキュリティ評価基盤として「工学的理論基盤」「社会科学的理論基盤」「データ基盤」の３つを整備することが急務である。本研究では、３つの基盤のうち社会科学的理論基盤とデータ基盤に関する基本モデルを確立し、実際の活動やデータ等に適用して有効性を示すことを目的とした。

３．研究の方法

(1) 社会科学的理論基盤に関する研究は、多様な関与者のインセンティブを分析する情報セキュリティ投資モデルを応用した実証研究を中心として進めた。モデルに基づいた代理変数の選択（例えば、仮想通貨に対する脅威を代弁する観測可能な情報として、その仮想通貨がいかに使いやすく円滑に流通するかを表す「流動性」を選択するなど）を適切に行い、さらに関与者の分類を精査するなどして、理論研究と実証研究を有機的に連携させた研究を実施した。研究成果の社会実装では、実証研究で取り組んだ題材である仮想通貨と関連深いブロックチェーン技術に着目し、アカデミアを中心とした公開性の高い基盤へと展開した。また、当該基盤のインパクトを高めるための新たな要素技術を、暗号理論の手法で研究した。

(2) データ基盤に関する研究では、データの収集者と利用者を分けて考えたり、専門的なシステム設計のもとで実データとシミュレーションデータを混在させたりする手法、すなわちハイブリッドな手法に着目して研究を行った。また、有効性を示すために、実験的研究で取り組む防御対象を当初予定の「クライアントのみ」から「サーバとクライアント」へ広げるなど、積極的に発展的な研究手法を取り入れた。

４．研究成果

(1) 理論モデルは、直接的な応用だけでなく、一見異なる研究対象に取り組む際にも役立つことがある。本研究では、仮想通貨に関する実証研究を設計する際に、次のような最適投資モデルの理論的定式化から得た着想で、代理変数を選択した。即ち、システムを表現する主要パラメータとして、

- 損失金額：　攻撃等の脅威が成功した時の経済的損失。
- 脅威：　攻撃等の脅威が生起する確率。情報セキュリティ投資によって低減されることがあり得る。
- 脆弱性：　攻撃等の脅威が生起した際に、生起したという条件の下で、脅威が成功する条件付き確率。情報セキュリティ投資によって低減されることがあり得る。
- 投資金額

を採用した。そして、研究対象の仮想通貨として、ロイヤルティプログラム（顧客へ多様なサービスを提供し利用を促す手段として、利用実績に応じて付与したポイントやマイル等を利用するプログラム）のポイントやマイルを取り上げた。

多くのロイヤルティプログラム(LP: Loyalty Program)では、サイバー空間に会員専用のホームページを用意し、Web ブラウザの暗号化通信モードでパスワードによるユーザ認証を行う。そして、他の LP と提携して、互いにポイントやマイルを変換したり、商品やサービスに替えたりするサービスを提供している。顧客は、それらのサービスの多くを、会員専用ホームページにログインしてオンラインで請求できる。

実世界における活動とサイバー空間での付加的なサービスが結びついた場合、認証が破

られて実世界に影響するセキュリティ問題が生じかねず、経済活動と直結していれば具体的な金銭的被害のリスクも大きい。本研究では、脅威に関する指標としてポイントやマイルの流動性（相互変換による転々流通のしやすさ）を定義し、脆弱性の指標算出のために会員専用ホームページにおける認証方式・バックアップ認証方式（パスワードを忘れた顧客への対応方法等）・登録時に要求する情報とその確認方法等を一つ一つ分析した。そして、これらのデータを用いて、計量経済学的な手法（図１の回帰分析モデルなどを用いた手法）で LP のセキュリティに関する実証分析を行い、以下の３つを含むいくつかの仮説を支持する結果を得た（雑誌論文②、⑤、学会発表⑤、⑥、⑧など）。

- 仮説１：　LP の運営企業が登録、認証、バックアップ認証においてセキュリティの高い実装をしているほど、インシデントのインパクトを加味した損失（以下では単に「損失」と記述）は小さい。
- 仮説２：　LP におけるポイントやマイルの流動性が高いほど、インシデントの損失は大きい。
- 仮説３：　ポイントやマイルを互いに変換する提携を結んだ LP がある時、変換先の LP におけるインシデントが多いほど、変換元の LP におけるインシデントの損失は大きい。同じく、変換元の LP におけるインシデントが多いほど、変換先の LP におけるインシデントの損失は大きい。

体系的な理論的洞察に基づくパラメータ選択があって初めて成功した仮説検証であり、実務指向の学会における論文賞受賞（受賞②）が示唆しているように実践的に有用な知見をもたらしている。こうして、理論基盤の有効性を示すという研究目的を達成した。

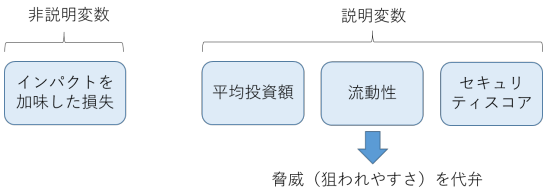

図 1．最適投資理論から着想を得た回帰分析モデル

以上の主要な成果から派生した成果として、社会実装と発展的な要素技術の開発にいくつか成功した。例えば、仮想通貨の基盤となるブロックチェーン技術に関して、セキュリティ評価に貢献するテストネットワーク立ち上げに知見を活用した（学会発表①など）。また、パスワードを忘れたユーザを補助する新たな仕組みを開発し、暗号理論的に厳密な安全性証明を与えた（学会発表⑪、受賞①など）。いずれも、理論基盤の有効性を示す上で、補強となる。

(2) 情報セキュリティ分野において、脆弱性情報などに関する情報共有の問題に関しては、実務的な議論がされるだけでなく、経済学を用いるなどして理論研究もなされてきた。概ね共通して指摘されているのは、共有される情報を誰がいかなる努力（コスト）を払って収集・提供・管理するかという観点でただ乗り問題が発生しやすいので、利害関係者の自由意志に任せるのではなく適切な制度設計を行って対応すべきということである。本研究では、焦点である「研究者が提案技術を評価するなどの目的で利用するデータを共有する問題（データ共有の問題）」の特徴を、上記の情報共有の問題と対比しながら分析し、マルウェア（不正ソフトウェア）対策研究に関する事例研究を行い、人材育成に配慮した枠組みの有効性を示すことに成功した（雑誌論文⑥、学会発表⑮など）。その際、データの収集者と利用者を分けて考えるハイブリッドな手法が重要な役割を果たした。さらに、マルウェア対策技術の研究として、いくつかの研究成果を派生した（学会発表⑨、⑭など）。いずれも、同様のハイブリッドなアプローチの効用が大きい。
情報セキュリティの評価においては、静的なデータ基盤だけでは限界がある。そこで、本研究では、動的にデータを生み出す実験基盤も研究対象とした。具体的には、匿名通信システム Tor に関する評価システムを構築した。専門的な設計のもとで実データとシミュレーションデータを混在さるハイブリッドな手法であることが特徴であり、異なる利害関係者を考慮するという点で静的なデータ基盤の研究との共通点も多い。そして、実際に同システムを活用して、実務的にも学術的にも有益な知見を得ることができた（雑誌論文③、学会発表②、④、⑦、⑩など）。国内の主要会議における論文賞受賞（受賞③）等が、そのインパクトを示唆している。
以上の成果により、データ基盤に関するハイブリッドな取り組みという基本モデルの有効性を示すという研究目的を達成した。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 6 件）

① Miodrag J. Mihaljevic, Aleksandar Kavcic, Kanta Matsuura: “An Encryption Technique for Provably Secure Transmission from a High Performance Computing Entity to a Tiny One,” Mathematical Problems in Engineering, Vol.2016, Article ID 7920495, 2016. （査読有り）
http://dx.doi.org/10.1155/2016/7920495

② Shiori Shinoda, Kanta Matsuura:

“Empirical Investigation of Threats to Loyalty Programs by Using Models Inspired by the Gordon-Loeb's Formulation of Security Investment,” Journal of Information Security, Vol.7, No.2, pp.29-48, 2016. （査読有り）
DOI: 10.4236/jis.2016.72003

③Fei Feng, Kanta Matsuura: “Stronger Bridge Mechanisms of Tor which Take into Consideration Exhaustive Adversarial Models,” Journal of Information Processing, Vol.23, No.5, pp.646-654, 2015. （査読有り）
http://dx.doi.org/10.2197/ipsjjip.23.646

④村山優子，松浦幹太，西垣正勝：“セキュリティ技術の人間的側面に関する研究領域の紹介，” ヒューマンインタフェース学会誌，Vol.17，No.3，pp.188-193，2015．（査読無し，解説論文）

⑤Bongkot Jenjarrussakul, Kanta Matsuura: “Japanese Loyalty Programs: An Empirical Analysis on their Liquidity, Security Efforts, and Actual Security Levels,” 日本セキュリティ・マネジメント学会誌，Vol.28, No.3, pp.17-32, 2015. （査読有り）

⑥ Kanta Matsuura, Takurou Hosoi: “Mechanism Design of Data Sharing for Cybersecurity Research,” IPSI Transactions on Advanced Research, Vol.11, No.1, pp.35-40, 2015. （査読有り）
http://vipsi.org/ipsi/journals/

〔学会発表〕（計 30 件）

①Kanta Matsuura: “BSafe: A Blockchain Research Network,” 13th Annual Forum on Financial Information Systems and Cybersecurity: A Public Policy Perspective, College Park, MD (USA), 2017 年 1 月 11 日発表.

②竹之内玲，松浦幹太：“Tor 秘匿サービスへの攻撃に対抗する偽装トラフィック生成，” 2017 年暗号と情報セキュリティ・シンポジウム(SCIS2017)，ロワジールホテル那覇（沖縄県那覇市），2017 年 1 月 27 日発表.

③ Kanta Matsuura: “Fundamental Principles and Evaluation of Cybersecurity,” 17th Counter-cybercrime Technology and Investigation Symposium (CTINS), Tokyo (Japan), 2016 年 12 月 6 日発表. (invited)

④中田謙二郎，松浦幹太：“匿名通信システム Tor に対する指紋攻撃の判定評価の拡張，” 2016 年暗号と情報セキュリティ・シンポジウム(SCIS2016)，ANA クラウンプラザホテル熊本ニュースカイ（熊本県熊本市），2016 年 1 月 19 日発表.

⑤篠田詩織，松浦幹太：“ロイヤルティプログラムのセキュリティに対するネットワーク分析指標に着目した考察，” 情報処理学会コンピュータセキュリティシンポジウム 2015(CSS2015)，長崎ブリックホール（長崎県長崎市），2015 年 10 月 22 日発表.

⑥篠田詩織，松浦幹太：“ロイヤルティプログラムのセキュリティインシデントに関する実証分析および制度設計の検討，” 第 29 回日本セキュリティ・マネジメント学会全国大会，東京大学生産技術研究所（東京都目黒区），2015 年 6 月 27 日発表.

⑦ 馮 菲，松浦幹太：“Evaluation of Anti-enumeration Defenses for Tor Bridges,” 2015 年暗号と情報セキュリティ・シンポジウム(SCIS2015)，リーガロイヤルホテル小倉（福岡県北九州市），2015 年 1 月 23 日発表.

⑧Bongkot Jenjarrussakul, Kanta Matsuura: “Impact from Security Incidents and Partnership in Japanese Loyalty Program,” 2015 年暗号と情報セキュリティ・シンポジウム(SCIS2015)，リーガロイヤルホテル小倉（福岡県北九州市），2015 年 1 月 22 日発表.

⑨碓井利宣，松浦幹太：“マルウェア検知および分類に向けたコンパイラ再最適化，” 2015 年暗号と情報セキュリティ・シンポジウム(SCIS2015)，リーガロイヤルホテル小倉（福岡県北九州市），2015 年 1 月 21 日発表.

⑩馮菲，松浦幹太：“網羅的な攻撃者モデルを考慮した Tor ブリッジ機構の強化，” 情報処理学会コンピュータセキュリティシンポジウム 2014(CSS2014)，札幌コンベンションセンター（北海道札幌市），2014 年 10 月 24 日発表.

⑪大畑幸矢，松田隆宏，松浦幹太：“証明可能安全なパスワード再発行プロトコルについて，” 情報処理学会コンピュータセキュリティシンポジウム 2014(CSS2014)，札幌コンベンションセンター(北海道札幌市)，2014 年 10 月 24 日発表.

⑫細井琢朗，松浦幹太：“TCP 再送タイマ管理の変更による低量 DoS 攻撃被害緩和の実験評価，” 情報処理学会コンピュータセキュリティシンポジウム 2014(CSS2014)，札幌コンベンションセンター(北海道札幌市)，2014 年 10 月 23 日発表.

⑬Kanta Matsuura: “Cybersecurity Science and Provable Security of Cryptography: Some Research Directions,” JSPS-DST Asian Academic Seminar 2013: Discrete Mathematics & its Applications, 東京大学教養学部（東京都目黒区）, 11 月 5 日発表. (invited)

⑭碓井利宣, 松浦幹太: “機械語命令列の差異によるマルウェア対策技術への影響の削減を目的とした隠れマルコフモデルに基づくコンパイラ推定手法,”2014 年暗号と情報セキュリティシンポジウム(SCIS2014), 城山観光ホテル（鹿児島県鹿児島市）, 2014 年 1 月 24 日発表.

⑮Kanta Matsuura, Takurou Hosoi: “Data Sharing for Cybersecurity Research and Information Sharing for Cybersecurity Practice,” The Eighth International Workshop on Security (IWSEC2013), 沖縄市町村自治会館（沖縄県那覇市）, 2013 年 11 月 18 日発表. (Poster Session)

〔図書〕（計 1 件）

①松浦幹太: “サイバーリスクの脅威に備える ～私たちに求められるセキュリティ三原則～,” 化学同人, 2015. （全 228 頁）

〔産業財産権〕

○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕

受賞（計 3 件）

①大畑幸矢, 松田隆宏, 松浦幹太: 辻井重男セキュリティ論文優秀賞. “Provably Secure Password Reset Protocol: Model, Definition, and Generic Construction.” 日本セキュリティ・マネジメント学会, 情報セキュリティ大学院大学, 情報処理学会コンピュータセキュリティ研究会, 日本ネットワークセキュリティ協会. （受賞日: 2016 年 3 月 18 日. 論文は３名共著, 表彰対象(応募時 40 歳未満)は筆頭から２名）

②Bongkot Jenjarrussakul, Kanta Matsuura: 平成 26 年度日本セキュリティ・マネジメント学会論文賞. “Japanese Loyalty Programs: An Empirical Analysis on their Liquidity, Security Efforts, and Actual Security Levels.” 日本セキュリティ・マネジメント学会. （受賞日: 2015 年 6 月 27 日）

③馮菲, 松浦幹太: コンピュータセキュリティシンポジウム 2014(CSS2014)優秀論文賞. “網羅的な攻撃者モデルを考慮した Tor ブリッジ機構の強化.” 情報処理学会. （受賞日: 2014 年 10 月 23 日）

報道等（図書①の書評）

①Books(書籍紹介): 「サイバーリスクの脅威に備える」, 日経コンピュータ, 第 902 号, p.82. 2015 年 12 月 24 日.

②書評(短評): 「サイバーリスクの脅威に備える」, 日本経済新聞. 2016 年 1 月 17 日.

③Books Trends: 「『サイバーリスクの脅威に備える』を書いた松浦幹太氏に聞く」, 週刊東洋経済(1 月 23 日号), pp.102-103. 2016 年 1 月 18 日.

④SD Book Review: 「サイバーリスクの脅威に備える」, Software Design, 技術評論社, p.54. 2016 年 2 月号. 2016 年 1 月 18 日.

⑤新刊書評（本の時間）: 鎌田浩毅「松浦幹太（著）『サイバーリスクの脅威に備える』」, PRESIDENT, p.132. 2016.2.29 号. 2016 年 2 月 8 日.

６．研究組織

(1)研究代表者
松浦　幹太（MATSUURA, Kanta）
東京大学・生産技術研究所・教授
研究者番号：００２９２７５６

(2)研究分担者　無し
（　　）
研究者番号：

(3)連携研究者　無し
（　　）
研究者番号：

(4)研究協力者
細井　琢朗（HOSOI, Takuro）
東京大学・生産技術研究所・技術専門職員