

セキュリティ評価基盤と周辺制度および活動に関する考察

松浦 幹太^{1,a)} 細井 琢朗^{1,b)}

概要：情報セキュリティへの科学的なアプローチ（サイバーセキュリティサイエンス）では、セキュリティ評価の客観性と再現性を確保することが重要である。そのために求められる基盤や制度への要件は、実務用と研究用でそれぞれの特徴があり、具体的なソリューションのあり方も異なる。本稿では、それらを総括して論じるとともに、国際的な視野も取り入れてマルウェア対策研究の分野における事例研究を行った結果をまとめる。

キーワード：マルウェア, セキュリティ評価, サイバーセキュリティサイエンス

On the Infrastructures, Mechanisms, and Activities for Information-Security Evaluation

Abstract: When we want to have a scientific approach (sometimes called cybersecurity science) to information security, we need objective and reproducible evaluation of security. The requirements and typical solutions would be different for practice and for research when we design related infrastructures and mechanisms. We comprehensively discuss these "information sharing" and "data sharing" issues, and report some case studies in the field of malware analysis with an international perspective.

Keywords: Malware, security evaluation, cybersecurity science

1. はじめに

サイバーセキュリティは、米国において、2009年サイバーセキュリティ推進法に基づいて巨額の研究費を国が投じる喫緊の研究課題とされている。そして、研究の焦点の一つは、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」に当てられている。厳密さ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、顧客情報流出事件などのように我々の生活の脅威となるインシデントが後を絶たないという反省が背景にある。実際、米国国防総省委託調査報告 [1] 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 のセキュリティ専門誌でセキュリティサイエンス特集号が組まれた [2]。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る。

サイバー空間におけるセキュリティの確保は、生活に不可欠なサービスである。セキュリティに関する要求仕様を満たす品質保証が、その本来の姿だと言ってもよい。しかし、保証するどころかそもそも科学的評価に欠けているという状況では、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）が大きな脅威の原因となってしまう。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（具体的な攻撃手順を考え、その手順に実行困難なステップが含まれているから安全であるとする評価。他の攻撃に関しては何の保証にもならない。）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。

後者すなわちインセンティブの問題に関しては、経済学的アプローチ [3], [4] など制度の評価を行う研究が盛んになっている。本稿では、前者すなわちヒューリスティックな安全性評価の問題に関して論じることとする。

¹ 東京大学
The University of Tokyo, Meguro-ku, Tokyo 153-8505, Japan

a) kanta@iis.u-tokyo.ac.jp

b) hosoi@iis.u-tokyo.ac.jp

2. 安全性評価の再現性

2.1 理論的評価

暗号分野においては、再現性のある安全性評価のアプローチが既にいくつか確立されている。

証明可能安全性： 攻撃者などの利害関係者をモデル化し、満たすべき安全性到達度を定義し、「そのモデルのもとで安全性を損ねる攻撃が存在すると仮定すると矛盾が生じる」ことを示し、いかなる手順の攻撃も成功し得ないと主張する。

情報理論的安全性： 攻撃者の入手可能な情報が情報理論的に不足していることから、無条件に安全であると主張する。

形式検証： 暗号技術の利用をプロトコルの観点から厳密な形式で記述し、その実行で安全性を損なう状態になり得ないことを論理的なツールで検証する。

これらのアプローチを暗号技術以外に適用することも試みられているが、全てのセキュリティ技術に適用できているわけではなく、むしろ適用成功例は少ない。しかし、もし適用できれば、ケルクホフスの原則すなわち

- 攻撃者は防御方式を知っている。セキュリティ技術の安全性評価においては、知った上で防御を破るべく工夫してくる攻撃者に対しても安全であるかどうかを調べるべきである。

を満たす^{*1}という意味で優れた安全性評価である。今後、適用を試みる研究が広がるであろう。

2.2 実験的評価

できるだけ再現性のある現実的な環境のもとで体系的に実験的評価を行うというアプローチは、工学において広く適用可能である。セキュリティ分野も例外ではない。しかし、セキュリティ分野には、特有のトレードオフが存在する。

共通の環境で共通のデータを用いれば、再現性を確保することはできる。その上で、さらに、採用された環境やデータの妥当性が求められる。例えば、画像処理分野で、同じ少女の画像を見たことのある読者も多いだろう。標準画像として皆が同一画像を使えば、再現性は確保できる。しかし、この再現性のためには、少なくとも一つ代償を払っている。少女のプライバシーである。

セキュリティ分野では、この代償がより一層顕在化しがちである。例えば、電子メールフィルタの研究で多くの研究者が用いる公開コーパスに含める問題メール（スパムメールなど）を集めることは、比較的容易である。こちらが努力せずとも、問題メールの方から自動的に来てくれると言ってもよい。しかし、正常なメール（ハムメール）は、

個人のプライバシーや企業秘密などの観点から、必要な質と量のメールを集めることは容易ではない。研究対象の技術によっては、プライバシーが問題になる一次データを直接公開せず、何らかの処理をした二次データを公開するだけでも共通データとして研究に有効な場合がある。例えば、生体認証分野においては、指紋データ自体ではなく、要素技術となる指紋照合アルゴリズムで各指紋対の類似度を求めた類似度のデータセットが公開され、それをを用いたフュージョンやシステム化の研究（複数種類の生体認証を併用する研究など）に活用される場合がある [5]–[7]。

プライバシー問題に加えて、セキュリティ分野におけるもう一つの課題は、不正データ悪用防止の問題（あるいは、データ観測収集能力のある組織などが、悪用を懸念してデータを公開しないという問題）である。この課題は、サイバーセキュリティ分野や、マルウェア（不正ソフトウェア）研究の分野において、顕著である。対策として実践されている代表的な例として、次の3つのアプローチがある。

- (1) 学術団体の当該活動に継続的に参加し、所定の利用法遵守契約を結んだ研究グループなどにデータの利用者を限定する。しかしその範囲では、共通データとして広く利用を推奨する [8], [9]。
- (2) データ提供あるいは利用に伴う責任などについて定めた一定の制度のもとで、基本的には自発的なデータ提供に頼る [10]。アプローチ (1) と併用することもできる [9]。
- (3) データではなく、環境をテストベッドとして提供する [11]。

本稿では、我が国におけるアプローチ (1) とその発展について、次章以降でより詳しく考察する。

3. 情報共有とデータ共有

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的にも研究されてきた [12]–[14]。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。

ここで、本稿の焦点である「研究者が提案技術の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把握してみたい（表 1）。

3.1 情報/データ提供者

共有する情報やデータとして信頼できるものの提供は、第一義的にはスキルの高い主体に頼ることになる。情報セキュリティの公共性から、社会的責任感（あるいは広報効

^{*1} ただし、主張はモデルの範囲に限られる。

表 1 情報共有とデータ共有（直感的対比）

Table 1 Information sharing and data sharing (intuitive comparison).

	情報共有	データ共有
提供者 そのスキル インセンティブ	事業者，協力者 高い 中程度	研究者，協力者 高い 中程度
一次利用者 そのスキル インセンティブ	事業者 高い 大きい	研究者 中程度 大きい
二次利用者 そのスキル インセンティブ	消費者（の機器等） 低い 小さい	関連研究者 中程度 大きい
更新頻度 網羅性 不正データ 正規データ	高い 高い 必要 たいてい不要	低い 低い 必要 たいてい必要
教育との関係 利用結果の公開性	小さい 低い	大きい 高い

果への期待感）として，提供者のインセンティブはけっして小さくはない．しかし，特別な制度がない限り利益には直結しないので，インセンティブが大きいともいえない．提供者に着目して研究用データ共有の問題を考える際には，実務用情報共有で経験的に得られている知見を活用する努力が有効である．

3.2 一次利用者

情報共有の場合には，提供者並みの高いスキルを想定できる．

一方，研究用データ共有の場合には，専門外ではないけれども提供者ほどのスキルではない一次利用者（例えば研究を始めたばかりの学生）も想定する必要がある．技術的スキルだけでなく，問題発生時の対応あるいは問題発生の予防に関する責任能力など，管理のスキルも高くはない．利用するインセンティブは高いので，制度設計を工夫するなどして，環境を整備する必要がある．

3.3 二次利用者

情報共有の場合には，自動パッチ機能などを通じて，幅広く一般ユーザにまで情報共有の効果を浸透させる．すなわち，インセンティブ付与のメカニズムに関しては，一次利用者の場合とは異なる考察が必要となる．

一方，研究用データ共有の場合には，比較のために関連研究の評価実験を迫試するなど，一次利用者と基本的には同様の利用者が想定される．専門外ではないけれども提供者ほどのスキルではない二次利用者（例えば研究を始めたばかりの学生）も想定する必要がある．技術的スキルだけでなく，問題発生時の対応あるいは問題発生の予防に関する責任能力など，管理のスキルも高くはない．利用するイ

ンセンティブは高いので，制度設計を工夫するなどして，環境を整備する必要がある．

3.4 データの管理

情報共有の場合とデータ共有の場合では，脅威に関する情報が必要である点を除けば，データ管理に求められる特徴が異なる．データ共有の場合にもっとも重要なことは，利用結果の公開性である．すなわち，研究成果を学会発表するなどして，その内容を共有することによって初めて，科学としての発展を見込むことができる．

3.5 制度設計

提供者や利用者の観点でもデータ管理の観点でも異なる考察が必要であることから，情報共有とデータ共有とは制度設計が異なるのが自然である．実際，我が国における事例（MWS: マルウェア対策研究人材育成ワークショップ）では，学会（研究会）が情報共有の場合よりも極めて強く関与し，また，教育（人材育成）への配慮が強くなされている．次章において，この事例を詳しく取り上げる．

4. データ共有活動と人材育成

4.1 MWS

MWS は，サイバークリーンセンターハニーポット^{*2}で収集しているボット観測データと，研究者から提供されたデータを「研究用データセット」として活用するワークショップである．MWS 組織委員会は情報処理学会のコンピュータセキュリティ (CSEC) 研究会のもとに設置されており，ワークショップは CSEC 研究会主催のシンポジウムとともに開催されている．MWS において，現時点では，次の 3 つの研究が対象とされている．

- マルウェア（不正ソフトウェア）検体解析技術の研究
- 感染手法の検知ならびに解析技術の研究
- ボットの活動傾向把握技術の研究

これらは情報セキュリティ研究のごく一部に過ぎないが，利用者のインセンティブがとくに大きい分野である．すなわち，共有どころかそもそも独自では利用できる本格的なデータがほとんど無かったという研究者も少なくない．そのため，人材育成にも力を入れる必要があり，ワークショップでは，一つの活性化策としてマルウェア分析競技会（MWS カップ）も行われている．

4.2 MWS カップ

MWS では共通データを利用した結果はワークショップを通じて研究成果として発表される．これだけでは研究としての新規性や有用性が顕著でない成果は発表されず，ま

^{*2} サイバークリーンセンター (CCC) の活動を民間主導で引き継ぐために設立された CCC 運営連絡会が運用しているハニーポット．

た表 1 における一次・二次利用者に含まれているスキルの高くない利用者の参加が進まないことも危惧される。そこで人材育成への配慮も加え、2009 年の第 2 回ワークショップからマルウェア分析競技会 (MWS カップ) を開催している。競技会ではハニーポットで収集した感染通信データやマルウェア検体などの解析を出題してきた。これらの多くは MWS の枠組みで共有されている研究用データセットと同種のデータであり、競技会への参加者は共有されている研究用データセットの解析をすることで競技への準備をすることができる。

競技会へはチームを組んで参加する。このチームの編成には人数制限は無く、また異なる組織の人員が一つのチームを組んでも構わない。この運用により、MWS の研究用データセット利用者として想定される、データ提供者と同程度に高いスキルを持つ者から学生に代表されるあまりスキルの高くない者までが、それぞれに適したチームを編成することができる。実際にこれまでの参加チームは、初心者を含めた学生が研究室単位で参加するチーム、マルウェア対策を本務とする上級者が少数精鋭で参加するチーム、他組織の上級者の指導の下で学生が作業を行うチームに大別される。特に学生のみで編成されたチームについては、チーム内で担当する解析データを分担して準備することで上級者に引けを取らない成績を上げている例が多く見られる。この事例は、この競技会が表 1 の一次・二次利用者の幅広い候補を MWS へ参加させる動機付けとして有効に働いていること、また情報セキュリティ分野でのデータ共有制度の一環として初心者への教育的効果を持つことを示している。

4.3 IWSEC カップ

国内会議で発表される研究であっても、研究の新規性や有効性は、本来、国際的な視野で議論される。すなわち、関連研究調査や比較評価においては、世界中の研究に目を向けるべきである。人材育成においても、世界を意識する姿勢は重要である。そこで、CSEC 研究会が共催する国際会議 IWSEC(International Workshop on Security)において、国際競技会を行うこととなった (IWSEC カップ)。

競技会で用いられるデータに関しても、提供者と利用者の間には表 1 におけるデータ共有の列と同様の違いがある。参加者が世界から集まれば、スキルやインセンティブなど、違いはより多様になる可能性がある。そのため、本稿著者が主体となって競技参加者の意見聴取を行い、人材育成を伴うデータ共有活動の改善に役立てることとした。

競技会では 3 つの競技用データ (Drive-by-download 攻撃の通信データ、マルウェアが仕込まれた PDF ファイル、個人情報などを勝手に送信する Android アプリ) の解析を出題した。これらのデータは各参加者が初めて触れる種類のものではないが、その内容は今回初めて目にするもので

ある。ただし今回は競技会の短い時間で解析を完了できるように、これらのデータには正規データを含めなかった。競技会に参加した 13 名は、情報セキュリティの研究を始めたばかりの学生から、マルウェアを専門的に解析・研究している学生までおり、表 1 における一次利用者にそのまま対応している。特に参加者の意見聴取からデータ利用のインセンティブが高いことが確認できた。またその意見聴取からは、出題された競技用データが、参加者がこれまで触れたことのある他の情報セキュリティ研究用データ (参加者が独自に収集したものも含まれる) に比べて、人材育成の点で遜色無い、もしくは優れたデータであるとの評価を受けた。競技結果からは、研究初心者の学生のみならず、専門的に研究を続けてきている学生でも競技の各課題を正解することが難しいことがわかった。意見聴取では解析時間が短いとの意見が多くあったが、各課題のデータ作成者は自身ではこの時間内で解ける課題を出題していることから、この正解の困難さは他組織で収集・作成したデータの共有が研究や人材育成の面で有用であることを示している。

5. むすび

本稿では、情報セキュリティ分野における実務情報共有の問題と研究用データ共有の問題を制度設計の観点で考察した。とくに、後者の評価基盤としての性格と、人材育成に配慮した活動の特徴に着目し、いくつかの事例に言及した。今後は、理論的な制度設計とより融合した議論を行い、当該分野の発展に寄与したい。

参考文献

- [1] The MITRE corporation: “Science of Cyber-Security”, JASON report, JSR-10-102 (2010).
- [2] D. Evans and S. Stolfo: “The Science of Security”, *IEEE Security & Privacy*, Guest Editors’ Introduction, Vol. 9, Issue 3, pp. 16–17 (2011).
- [3] 松浦幹太: “情報セキュリティと経済学”, 2003 年暗号と情報セキュリティ・シンポジウム (SCIS2003) 予稿集, Vol. 5, pp. 475–480 (2003).
- [4] R. Anderson and T. Moore: “The Economics of Information Security”, *Science*, Vol. 314, pp. 610–613 (2006).
- [5] NIST Biometric Scores Set — Release 1 (BSSR1), <http://www.nist.gov/itl/iad/ig/biometricscores.cfm>.
- [6] N. Poh, T. Bourlai, and J. Kittler: “A Multimodal Biometric Test Bed for Quality-Dependent, Cost-Sensitive and Client-Specific Score-Level Fusion Algorithms,” *Pattern Recognition Journal*, Vol. 43, No. 3, pp. 1094–1105 (2010).
- [7] T. Murakami, K. Takahashi, and K. Matsuura: “Towards Optimal Countermeasures against Wolves and Lambs in Biometrics”, *Proceedings of the IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems*, IEEE (2012).
- [8] 竹森敬祐, 細井琢朗: “MWS Cup 2009”, 情報処理, Vol. 51, No. 3, pp.296–299 (2010).
- [9] 情報処理学会 コンピュータセキュリティ研究会 MWS 組織委員会: “MWS について”,

- <http://www.iwsec.org/mws/2012/about.html>
- [10] The Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT). <https://www.predict.org/>
 - [11] T. Benzel and J. Wroclawski: “The DETER Project: Towards Structural Advances in Experimental Cybersecurity Research and Evaluation”, *Journal of Information Processing*, Vol. 20, No. 4 (preprint) (2012).
 - [12] H. R. Varian: “System Reliability and Free Riding”, *The 1st Workshop on Economics and Information Security*, Berkeley, CA (2002).
 - [13] L. A. Gordon, M. P. Loeb and W. Lucyshyn: “Sharing Information on Computer Systems Security: An Economic Analysis”, *Journal of Accounting and Public Policy*, Vol. 22, Issue 6, pp. 461–485 (2003).
 - [14] 田沼均, 大塚玲, 松浦幹太, 今井秀樹: “Gordon-Loeb-Lucyshyn モデルを拡張した情報セキュリティ情報共有のインセンティブ分析”, *日本セキュリティ・マネジメント学会誌*, Vol. 23, No. 2, pp. 3–16 (2009).