

令和 6 年 6 月 10 日現在

機関番号：32411

研究種目：基盤研究(C)（一般）

研究期間：2018～2023

課題番号：18K11993

研究課題名（和文）匿名化技術とそれを用いた内部通報プラットフォームに関する調査研究

研究課題名（英文）Research on Anonymizing Technology and Whistleblowing Platforms

研究代表者

八田 真行（Hatta, Masayuki）

駿河台大学・経済経営学部・教授

研究者番号：70608893

交付決定額（研究期間全体）：（直接経費） 2,900,000 円

研究成果の概要（和文）：本研究の目的は、TorやI2Pに代表されるいわゆる通信匿名化の現実的な問題点と法的・社会的な位置づけを、特にこれらの技術を利用した匿名内部告発プラットフォームに焦点を当てて明らかにすることである。この研究では、ダークウェブやセキュア・メッセージングに関連する技術開発に注目した。法的保護の文脈では見過ごされがちな内部告発の技術的保護の文脈を提示し、技術的基盤としてのエンド・ツー・エンドの暗号化の重要性を強調した。また、ダークウェブにおける技術開発の背景として、オープンソースとハッカー文化の重要性を指摘した。

研究成果の学術的意義や社会的意義

学術的な意義としては、従来は法的保護という文脈で言及されることが多かった内部通報に関して、情報技術を用いた技術的保護という文脈を提示したこと、とりわけ技術的要素としてエンド・ツー・エンド暗号化の重要性を指摘したことが挙げられる。社会的意義としては、依然脆弱な日本の内部通報制度を補完する可能性がある技術を確認したこと、不明な点が多かったダークウェブの実態を実装レベルで明らかにし、またそうした技術開発の背景として、オープンソースやハッカー文化の重要性を指摘したことが挙げられる。

研究成果の概要（英文）：The research aimed to identify the actual problem and legal/social positioning of so-called communication anonymization, as represented by Tor and I2P, with a special focus on anonymous whistleblowing platforms that use these technologies. The study looked at technological developments related to the dark web and secure messaging. It presented the context of technical protection for whistleblowing, which is often overlooked in the context of legal protection, and highlighted the importance of end-to-end encryption as a technical foundation. The study also highlighted the importance of open source and hacker culture as a backdrop for technological development on the Dark Web.

研究分野：経営情報学

キーワード：匿名化通信技術 オープンソース ダークウェブ 内部通報 セキュアメッセージング

## 1. 研究開始当初の背景

ドナルド・トランプ大統領を生んだ 2016 年米国大統領選に影響したとされる、「ハッカー」ジュリアン・アサンジ率いるウィキリークスの活動や、米軍人切尔西（ブラッドリー）・マニングによるイラク戦争での米軍の不祥事や米国外交公電の暴露、米情報機関職員だったエドワード・スノーデンによる米国の国際的な大規模通信監視プログラム PRISM の暴露、あるいはパナマの法律事務所から流出した大量のデータがタックスヘイブンを駆使した富裕層の蓄財の実態を暴露し、アイスランド等いくつかの国では政治指導者らの辞任にまでつながった「パナマ文書」事件など、内部通報(リーク)が社会に大きな影響を与える事案が増えてきた。日本においても、三菱自動車や雪印食品、オリンパスなど、内部告発が長年続いた企業不祥事の発覚につながったケースは多い[1]。規制コストの増大を抑え、コーポレート・ガバナンスを補う存在としても内部通報は世界的に重視されつつあった[2]。

しかし、内部通報者はその正体が知られた場合、国によっては死刑を含む厳罰にさらされる可能性がある。たとえ日本のように内部通報者保護制度がある程度整えられていたとしても、隠微な左遷など様々な形で報復されることが多い[3]。また、ベトナム戦争の行き詰まりを暴き、米軍撤退の遠因となった「ペンタゴン・ペーパーズ」事件や、正体は FBI 副長官だった「ディープスロート」による新聞記者へのリークが引き金となってニクソン大統領の辞任にまでつながったウォーターゲート事件など、いわばリーク成功の歴史がある米国と違い、他の国では内部通報者は第三者にまで裏切り者扱いされることが多く、社会的なプレッシャーも大きいと考えられる。

こうした問題を解決すべく、ウィキリークスが採用したことで一般にも有名になったのが匿名化通信技術(Anonymizing Technology)である。具体的な実装としては、Tor(The Onion Router)や I2P(Invisible Internet Project)が知られている。複数のリレー・サーバを経由して対象へアクセスすること、あるいはアクセスされる側のサーバの物理的な位置をも隠蔽することを可能とする匿名化通信技術を用いることで、内部通報者は自らの素性を、通報対象や第三者はもとより、内部通報が送られる相手にすら知られずにコンタクトを取ることが可能となる[4]。この技術、特に Tor を用いた内部通報プラットフォームは、米プロパブリカや米インターセプトなど新興のオンラインニュースメディアのみならず、米ニューヨーク・タイムズ紙や英ガーディアン紙など従来からある大手メディアにも採用され、主流ジャーナリズムの一角を担うようになっている。

## 2. 研究の目的

このような背景と問題意識に鑑み、本研究で明らかにしようとしたのは、匿名化技術と、それを用いた内部通報プラットフォームの社会的位置づけ、特に正しい規制のあり方である。

匿名化技術は、内部通報プラットフォームのような社会的に好ましいと考えられる利用も多くされている一方、その匿名性を活かして一時は世界最大の薬物密売サイトとなったシルクロードの事件や、日本においても無実の人をなりすましで陥れた 2012 年のいわゆる PC 遠隔操作事件など悪用されたケースもある。これに対して、匿名化技術をいかに規制するかという議論がようやく立ち上がりつつあるが、匿名化技術を構成する要素の多くは、暗号技術を始めとして現在のインターネットを支える基幹技術でもあり、近年注目されるビットコインのような仮想通貨においても同じ技術が用いられているため、不用意な法規制は市民のプライバシーや言論の自由、イノベーション、あるいは安全な電子商取引にまで甚大な影響を与えかねず、例えば匿名化技術を用いたアクセスを遮断するなど、技術的な対策のほうが有用と考えられるケースもある。本研究では、匿名化技術とその応用の実態を技術的詳細にまで下りて正確に捉えることで、こうした議論に資することを目的とした。

## 3. 研究の方法

本研究は、以下の 3 点を当面の目標とした。

1. 匿名化技術を用いた内部通報プラットフォームの実態調査
2. 匿名化通信技術の合法性に関する検討
3. 匿名化通信技術や暗号技術の応用に関する正しい規制のあり方の検討

研究方法としては、技術的背景を重視しつつ、適宜調査や分析を行った。社会的な貢献も重視した。

## 4. 研究成果

### (1) 技術的成果

匿名化通信技術関係

匿名化通信技術を応用した内部通報支援サイトとして、whistleblowing.jp を作成・設置した。

また、匿名化通信技術と実態把握の一環として、I2P ネットワーク用の検索エンジンである legwork.i2p/ransack.i2p を開発し、公開した。ダークウェブ向けの検索エンジンは、Tor 向け

のものはすでに存在したが、I2P 向けの本格的、実用的なものはこれが事実上初であり、これによって、従来把握が難しかったダークウェブ上のコンテンツの把握が容易となった。2023 年現在 legwork.i2p は約 30 万件のデータを蓄積しており、I2P ネットワークにおいて最もアクセスされたサイトに成長した。

これに関連して、Tor クライアントの Java 実装である Orchid の開発を行った。いわゆる出口ノードが存在し、通常のウェブへのアクセスが可能な Tor と違い、I2P は基本的に閉じたネットワークとして設計されていたが、I2P の Java 実装に Orchid プラグインを組み込むことで、Tor ネットワーク経由で通常のウェブへ容易にアクセスできるようになった。これにより、I2P の内部通報プラットフォームへのさらなる応用が見込めると考えられた。

#### セキュア・メッセージング関係

Whistleblowing.jp のような匿名内部通報支援サイトは技術的には実用段階に達しているが、通報を受け付けるジャーナリストの理解や協力を得る、技術的トレーニングを行うといった、いわば人間的な部分で困難があった。一方、近年報道されているように、香港やベラルーシでの市民運動では Telegram や Signal といった匿名メッセージング・アプリが活用されるようになってきた。

そのため、プラットフォームとして内部通報支援サイトを用意するのではなく、個々人の日常的なコミュニケーションを匿名化、暗号化する、いわゆるセキュア・メッセージングに研究の軸足を移すことにした。

そこで、サーバ上での運用が原則となる従来の内部通報プラットフォームとは違い、ユーザ個々人の手元での実行が基本となる、分散型、非同期型の匿名コミュニケーションプラットフォームのあり方を模索し、その一つである Syndie を改良した。これにより、Syndie は最新の Java 環境でも機能するようになった。

さらに、I2P を介した完全匿名・分散型のメッセージング・サービスである I2P-Bote の開発を行った。従来の匿名化通信技術の弱点の一つは、技術的な素養がないユーザにとっては極めて使いにくく敷居が高いところにあったが、I2P-Bote は、I2P プラグインとしては SMTP/IMAP サービスを提供して従来の電子メールをそのまま代替することが可能であり、スマートフォン向けに Android 用のアプリも用意した。

#### (2) 研究発表など

以上のような技術的成果を踏まえ、研究内容の学術論文文化や学会発表を行った。

ダークウェブに直接関係あるものとしては、混同されがちなディープウェブ、ダークウェブ、ダークネットの概念を整理し、オニオン・ルーティングに関して技術的検討を加えた英語論文を公刊した (Hatta 2020b)。この論文はこの種のものとしてはよく引用されており、ダークウェブの研究においては基本的な文献の一つとなっている。

また、ダークウェブやセキュア・メッセージングに関して世界の開発者が集まる国際会議等に数度にわたって参加し、意見交換を行った。これらの経験から、こうした技術開発を支えるエートスとしてのオープンソース文化やハッカー文化、DIY 精神の重要性に気づき、いわゆる「修理する権利」についての歴史的経緯をまとめた英語論文 (Hatta 2020a) や、オープンソース文化の変遷とセキュリティに関する現代的課題に関する英語論文 (Hatta 2021, 2022) を公刊した。前者では、「修理する権利」を消費者の重要な権利の一つでありイノベーションの根幹を成すものとして位置づけ、にも関わらず近年ではそれが法的、技術的に制約されつつあるという問題を論じ、後者に属する一連の論文では、オープンソース文化の変質がソフトウェアのメンテナンスに危機をもたらしている状況について論じた。これらも引用・言及されることが多く、学術的な理解に貢献したと自負している。

さらに、この種の技術の法的規制という文脈では、特にエンド・ツー・エンド暗号化技術の重要性に着目することとなった。エンド・ツー・エンド暗号化は内部通報という文脈に留まらず、民主主義的社会が機能するために重要であり、我々の経済のあらゆる部門にとって不可欠なものという理解に基づき、世界的な規制の動きや社会への影響、およびサイバー主権とスプリンターネット(インターネットの分裂)の問題に関して研究し、国際シンポジウムで発表した。また、エンド・ツー・エンド暗号化の規制のあり方については他の専門家と共同で、強力な暗号化の保護と促進を求める国際声明[5]をとりまとめて発表することにも成功した。

加えてオンライン・プラットフォームの規制のあり方や、ネットにおける匿名の誹謗中傷の伝播に関して研究を行い、国際学会等で発表した。

#### < 参考文献 >

[1] 奥山俊宏. (2004). 内部告発の力: 公益通報者保護法は何を守るのか. 現代人文社.

[2] Andreadakis, S., & Morrison, S. (2016). Whistleblowers under the Spotlight: The cases of Japan and the UK. *European Journal of Comparative Law and Governance*, 3(4), 353-384.

- [3] 櫻井稔. (2006). 内部告発と公益通報: 会社のためか、社会のためか. 中央公論新社.
- [4] 八田真行, (2011). ウィキリークスを支えた技術と思想. 「日本人が知らないウィキリークス」所収. 洋泉社.
- [5] <https://news.yahoo.co.jp/expert/articles/d6f31ce0449071d9e235fa64027ef9b2f70f8967>

## 5. 主な発表論文等

〔雑誌論文〕 計5件（うち査読付論文 5件／うち国際共著 0件／うちオープンアクセス 2件）

1. 著者名 Masayuki Hatta	4. 巻 21
2. 論文標題 The Nebraska problem in open source software development	5. 発行年 2022年
3. 雑誌名 Annals of Business Administrative Science	6. 最初と最後の頁 91-102
掲載論文のDOI（デジタルオブジェクト識別子） 10.7880/abas.0220914a	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 -

1. 著者名 Masayuki Hatta	4. 巻 20
2. 論文標題 Cowboys and the Eternal September: Transfiguration of hacker aesthetics	5. 発行年 2021年
3. 雑誌名 Annals of Business Administrative Science	6. 最初と最後の頁 223-237
掲載論文のDOI（デジタルオブジェクト識別子） 10.7880/abas.0210923a	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 -

1. 著者名 Masayuki Hatta	4. 巻 19
2. 論文標題 Deep web, Dark web, Dark net: a taxonomy of "hidden" internet	5. 発行年 2020年
3. 雑誌名 Annals of Business Administrative Science	6. 最初と最後の頁 277-292
掲載論文のDOI（デジタルオブジェクト識別子） 10.7880/abas.0200908a	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Masayuki Hatta	4. 巻 22
2. 論文標題 Growing an open source community	5. 発行年 2023年
3. 雑誌名 Annals of Business Administrative Science	6. 最初と最後の頁 33-46
掲載論文のDOI（デジタルオブジェクト識別子） 10.7880/abas.0230320a	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Masayuki Hatta	4. 巻 19
2. 論文標題 The Right to Repair, the Right to Tinker, and the Right to Innovate	5. 発行年 2020年
3. 雑誌名 Annals of Business Administrative Science	6. 最初と最後の頁 143-157
掲載論文のDOI（デジタルオブジェクト識別子） 10.7880/abas.0200604a	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

〔学会発表〕 計11件（うち招待講演 6件 / うち国際学会 4件）

1. 発表者名 八田真行
2. 発表標題 systemdを巡る論争とオープンソースにおける思想的対立
3. 学会等名 2022年度秋季情報通信学会大会
4. 発表年 2022年

1. 発表者名 Masayuki Hatta
2. 発表標題 End-To-End Encrypted Anonymous Messaging through the Dark Web
3. 学会等名 HEK.SI（招待講演）（国際学会）
4. 発表年 2022年

1. 発表者名 八田真行
2. 発表標題 エンド・ツー・エンド暗号化：規制の動きと社会への影響
3. 学会等名 IGF2021国内事前会合（招待講演）
4. 発表年 2021年

1．発表者名 八田真行
2．発表標題 サイバー主権とスプリンターネット：分裂するインターネットの現状と課題
3．学会等名 IGF2021国内事前会合（招待講演）
4．発表年 2021年

1．発表者名 Masayuki Hatta
2．発表標題 Face recognition technology and state surveillance in East Asia in the wake of COVID-19
3．学会等名 RightsCon 2020（招待講演）（国際学会）
4．発表年 2020年

1．発表者名 八田真行
2．発表標題 ソフトウェアの「自由」や「オープンネス」の客観的定義とその変遷
3．学会等名 2020年度秋季情報通信学会大会
4．発表年 2020年

1．発表者名 Masayuki Hatta
2．発表標題 Debunking toxic "Matome sites" in Japan
3．学会等名 REVULN 19Q4（国際学会）
4．発表年 2019年

1．発表者名 八田真行
2．発表標題 プロトコル・ベースのプラットフォーム規制
3．学会等名 2019年度秋季情報通信学会大会
4．発表年 2019年

1．発表者名 Masayuki Hatta et al.
2．発表標題 Beyond North: Effects of weakening encryption policies
3．学会等名 IGF2023（招待講演）（国際学会）
4．発表年 2023年

1．発表者名 Masayuki Hatta et al.
2．発表標題 Consumer data rights from Japan to the world
3．学会等名 IGF2023（招待講演）
4．発表年 2023年

1．発表者名 八田真行
2．発表標題 揺らぐオープンソース WYRIWYGの確保における著作権 ライセンスの限界
3．学会等名 2023年度春季情報通信学会大会
4．発表年 2023年



〔図書〕 計0件

〔産業財産権〕

〔その他〕

Legwork.i2p (I2P経由でのみアクセス可能) <a href="http://legwork.i2p">http://legwork.i2p</a> Ransack.i2p (I2P経由でのみアクセス可能) <a href="http://ransack.i2p">http://ransack.i2p</a> I2P-Bote <a href="https://github.com/mhatta/i2p.i2p-bote">https://github.com/mhatta/i2p.i2p-bote</a> Orchid <a href="https://github.com/mhatta/Orchid">https://github.com/mhatta/Orchid</a> Orchidの紹介と利用方法 (英文) <a href="https://mhatta.medium.com/best-of-two-worlds-accessing-i2p-and-tor-and-clearnet-seamlessly-with-orchid-171b8351c65e">https://mhatta.medium.com/best-of-two-worlds-accessing-i2p-and-tor-and-clearnet-seamlessly-with-orchid-171b8351c65e</a> Syndieの紹介と利用方法 (英文) <a href="https://medium.com/@mhatta/easy-censorship-resistant-communication-with-syndie-e063a6c9cf35">https://medium.com/@mhatta/easy-censorship-resistant-communication-with-syndie-e063a6c9cf35</a> Kyoto Statement on End-To-End Encryption <a href="https://www.globalencryption.org/2023/10/kyoto-statement-on-end-to-end-encryption/">https://www.globalencryption.org/2023/10/kyoto-statement-on-end-to-end-encryption/</a>
---

6. 研究組織

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
--	---------------------------	-----------------------	----

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関
---------	---------