明治大学総合数理学部

2022 年度

卒　業　研　究

越境移転と個人関連情報に関するプライバシーポリシーでの記載調査と分析

学位請求者　先端メディアサイエンス学科

中 島 尚 斗

目次

第 1 章

はじめに

1.1　はじめに

デジタル技術の革新により，私たちの個人情報の利用は多様化している．そのため，個人情報保護法が改定され，2022 年 4 月より施行されている．プライバシーポリシーによって企業は利用者にどのように個人情報を保護しているかを示さなくてはならない．しかし度重なる法改正により，企業のプライバシーポリシーの改定が追いついていないことが多い．加えて, 長く難解な表現により生活者の理解が困難になる問題が生じている．

そこで，本研究では生活者の理解困難度を定量化するため，専門知識を持たない複数の評価者が，国内の主要な企業 198 社のプライバシーポリシーに対して企業の個人情報保護方針を生活者が正しく認識出来る十分な記載がなされているかを評価することを試みる．調査後に評価の結果に基づき，誤認を与える要因を分析をする．

第 2 章

個人情報保護法

2.1 概要

日本の個人情報保護規定は，個人情報の保護に関する法律 [1] で定められている．デジタル社会の進展に伴い個人情報の利用が著しく拡大していることを背景に作成された．令和 2 年改正の個人情報保護法 [2] では，漏えい等報告・本人通知の義務化，外国にある第三者への提供，保有個人データの開示方法，個人データの利用の停止・消去等の請求，公表等事項の充実，不適正利用の禁止，個人関連情報，仮名加工情報が変更や追加された．しかし，2021 年に行ったプライバシーポリシー分析 [3] がによると，多くの業界で第三者提供に関する記述が不足している傾向が明らかになった．

2.2 越境移転

外国にある第三者へ個人データの提供できる条件は次の 3 つである [4]．(1) 移転先の所在国の名称，当該国における個人情報の保護に関する制度，移転先が講ずる個人情報の保護のための措置の情報を提供し，本人の同意を得る．(2) 基準に適合する体制を整備した事業者が必要な措置をとり，本人の求めに応じて必要な措置等に関する情報を提供する．(3) 日本と同等の水準国である EU, 英国の場合であること．

2.3 個人関連情報

個人関連情報は，個人に関する情報であって，個人情報, 仮名加工情報及び匿名加工情報のいずれにも該当しないものである．個人関連情報を第三者に提供することで，提供先が個人データとして取得することが想定される時には，本人同意が必要となる [4]．例えば， Web サイトの閲覧履歴や利用環境を記録し， マーケティングや操作性の向上に利用するクッキーは， 現在多くの企業が導入している代表的な技術である．クッキーの他にも，IP アドレスや端末固有の識別子，購買履歴，閲覧履歴，位置情報など，特定の個人の識別には至らないものの個人に関連する情報が含まれるものが個人関連情報として定義された．

永井ら [5] は 2021 年にクッキーコンセントバナーに関する調査を行い,，生活者に誤解を与えるダークパターンの存在を明らかにしている．そのため企業には，生活者が自らの意思でクッキー等利用の可否を決定するための分かりやすい説明や拒否方法の呈示が求められる．

2.4 先行研究

永井ら [5] によると，クッキー使用に対してユーザの同意取得を果たすためのクッキーコンセンバナーにユーザを誘導するダークパターンの利用率が法規制のある国に高いと報告した.

また，森ら [3] によると，個人情報の保護に関するガイドラインを定めている業界では，企業によるプライバシーポリシーの記載が充実していると報告した.

第 3 章

プライバシーポリシー調査

3.1　調査目的と方法

企業のプライバシーポリシーを調査し，十分な記載の有無, 誤認を与える問題点を明らかにすることが調査の目的である．対象企業は，東洋経済 Online の「好感度が高い企業・ブランドトップ 200」[6] の内，プライバシーポリシーを公表していた 198 社を選定した．選定した企業を 22 の業種に分け，特に越境移転・個人関連情報を適切に記載しているかを調査した．調査は 20 代の男女各 1 名によるものであり，評価者 A，B ともに個人情報に関して専門的な知識を持たない．また，評価者は 1 社あたりの調査時間を計測した．

3.2　評価基準

越境移転は，当該外国における個人情報の保護に関する制度，当該第三者が講ずる個人情報の保護のための措置，当該本人に参考となるべき情報の条件の記載の有無で判断する．結果の表現記号を表 3.1 に示す．

3.3　調査結果

評価者 A，B の調査では，評価ずれが生じた．そのため，評価ずれ企業を再調査した．結果を表 3.2 に示す．個人関連情報については多くの業種で記載が多くある．情報通信 (66.7%)，旅行 (100.0%) の業種では，越境移転の記載が十分である．一方，自動車 (12.5%)，電気・精密機器 (17.6%)，医薬品 (0.0%) の業種では記述が不十分な傾向がある．ただし，調査した企業数が 5 社未満の業種は，傾向をつかむには不十分と考えた．

表 3.1　評価記号

	越境移転	個人関連情報
○	条件 3 つの記載あり	記述あり
△	条件 1,2 つの記載あり	(該当なし)
×	条件記載なし	(該当なし)
−	外国の記載なし	記述なし, 個人データとして第三者提供をしない

表 3.2　プライバシーポリシーの記載結果

		越境移転					個人関連情報		
	合計	○	△	×	−	○割合 (%)	○	−	○割合 (%)
百貨店・小売り	16	3	0	5	3	18.8	14	2	87.5
自動車	8	1	1	4	2	**12.5**	6	2	75.0
食品	56	1	2	22	31	55.4	43	13	76.8
衣料・生活用品	19	5	1	5	8	26.3	13	6	68.4
住宅設備	4	1	0	3	0	25.0	4	0	100.0
ゲーム	3	1	0	2	0	33.3	3	0	100.0
電気・精密機器	34	6	5	14	9	**17.6**	29	5	85.3
重・軽工業	4	1	0	3	0	25.0	3	1	33.3
運輸	5	1	0	3	1	20.0	2	3	40.0
スポーツ用品	6	0	3	1	2	0.0	5	1	83.3
情報通信	9	6	2	1	0	**66.7**	9	0	100,0
航空	2	1	1	0	0	50.0	2	0	100.0
レンタル	1	0	0	0	1	0.0	1	0	100.0
化粧品	5	1	0	1	3	20.0	4	1	80.0
ハウスメーカー	4	0	0	2	2	0.0	3	1	75.0
テーマパーク	2	0	0	2	0	0.0	1	1	50.0
組合	2	0	0	0	2	0.0	1	1	50.0
映画	1	0	1	0	0	0.0	1	0	00.0
医薬品	8	0	1	3	4	**0.0**	6	2	75.0
通信販売	4	2	0	0	1	50.0	0	1	0.0
警備	1	0	0	0	1	0.0	0	1	0.0
旅行	4	4	0	0	0	**100.0**	4	0	100.0

第 4 章

評価と分析

2 人で行った調査結果が不整合した企業数を表 4.1 に示す．越境移転・個人関連情報の記載が 2 人の評価ともに十分である企業は，記載が十分かつ理解がしやすいプライバシーポリシーを作成していると考えられる．

4.1　高評価企業

越境移転・個人関連情報の記載が 2 人の評価ともに十分である企業を高評価企業とした．高評価企業数は全 24 社である．この高評価企業の特徴を表 4.2 に示す．共通する特徴は，個人情報保護委員会の HP や PDF を利用していることである．これにより，越境移転の条件を満たしている．高評価企業の中には，プライバシーセンターを作成する企業もある．例として図 4.1 にヤフー株式会社のプライバシーセンターを示す．このプライバシーセンターでは，プライバシーポリシーがわかりやすくまとめてあるだけではなく，理解の助けとなるプライバシーポリシーの用語を解説している．

表 4.1　評価者 2 名の評価ずれ企業数

	評価者 A	評価者 B	合計
越境移転	○	△	2
		×	1
		−	2
	△	○	0
		×	1
		−	2
	×	○	1
		△	4
		−	8
	−	○	0
		△	2
		×	5
個人関連情報	○	-	9
	-	○	6

表 4.2　高評価企業の特徴

利用しているもの	企業数	割合 (%)
個人情報保護委員会の HP・PDF	22	91.7
図	1	4.2
表	11	45.8
プライバシーセンター	3	13.6
プライバシーマーク	6	25.0
動画	1	4.2

図 4.1　ヤフー株式会社のプライバシーセンター（[8] より引用）

・第三者提供

（中略）

・安全管理措置

（中略）

・外的環境の把握
当社では以下の国で個人情報の保管をしています。
アメリカ合衆国

図 4.2　評価ずれの生じたプライバシーポリシー例

4.2　評価ずれとその要因

評価がずれた企業数は全 38 社である．評価がずれた主な要因は，1. 越境移転の当該本人に参考となる情報であるか否か，2. 第三者提供の項目以外での越境移転に関する記載，3. 文字リンクの見逃しなどである．2 番目に挙げた要因は，越境移転の要件が記載されている箇所がまちまちであり安全管理措置が記載されている項目にあったため見逃しが生じていた．評価ずれが生じた例を図 4.2 に示す．

表 4.3　検証

	安全管理措置		文字リンク		テキストの隠れ	
	個数	割合 (%)	個数	割合 (%)	個数	割合 (%)
判断ずれ	7	18.4	27	71.0	2	5.3
全体	19	9.6	156	78.3	15	7.5

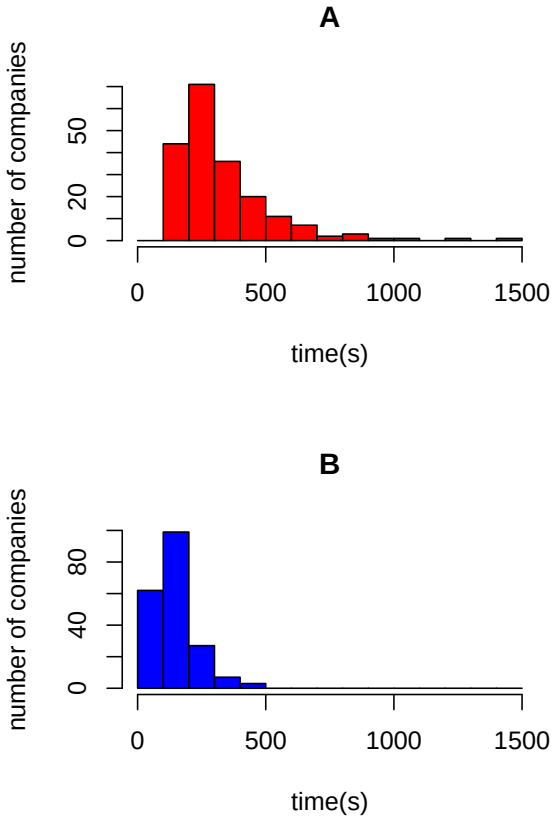

図 4.3　計測時間の分布

評価ずれの要因としてあげた第三者提供以外の項目での記載，文字リンクに読み逃し，アコーディオンメニューによるテキストの隠れなどがある．評価ずれの要因を全企業で調査した．結果を表 4.3 に示す．安全管理措置は，第三者提供の項目以外で越境移転に関する記載が多かった項目である．安全管理措置内での記載は全体より判断ずれの方が割合が高いため，誤認を与える要因の一つと考えられる．逆に文字リンクやテキストの隠れは全体の方が判断ずれ企業より割合が高い．

4.3　計測時間

二人の調査時間を図 4.3 に示す．評価者 A の平均 330.7 秒，評価者 B の平均 147.2 秒である．評価者 A が評価者 B よりも調査時間長い傾向にある．評価者 A は，一部の企業について著しく長く時間がかかっている．他より時間がかかる企業は，必要な情報を読み取りにくいプライバシーポリシーと考えられる．

4.4　考察

安全管理措置での越境移転記載が誤認の要因として大きかった理由は，誤認の要因と考えられる文字リンクをせずに，リンクをそのまま貼るなどの対策をすることでご認識を防止することができると考えられる．

第 5 章

おわりに

本稿では，プライバシーポリシーの調査と分析を行い，誤認を与える要因を明らかにした．いくつかの業種では調査した企業数が少なく，傾向がつかめない結果となり今後の課題とする．

また，改正された個人情報保護法の越境移転と個人関連情報の 2 項目だけを行ったため，他の項目の調査は今後の課題とする．

謝辞

本研究を行うにあたって，多くの方々よりご指導いただきました．特に明治大学総合数理学部先端メディアサイエンス学科，菊池浩明教授に深く感謝申し上げます．また，メンターとしてご指導いただいた堀米光さん，研究室の皆様に深く感謝の意を表するとともに，謝辞とさせていただきます．

参考文献

[1] e-Gov ポータル，“平成十五年法律第五十七号 個人情報の保護に関する法律”，(https://elaws.e-gov.go.jp/document?lawid=415AC0000000057，2022 年 11 月参照).

[2] 個人情報保護委員会,“改正個人情報保護法　特集”，(https://www.ppc.go.jp/news/kaiseihou_feature/，2022 年 11 月参照).

[3] 森 啓華，永井 達也，高田 雄太，神薗 雅, 紀，“プライバシーポリシー分類による法律遵守の分析”，Computer Security Symposium 2021，pp. 1061-1068，2021.

[4] 個人情報保護委員会,“マンガで学ぶ個人情報保護法”，(https://www.ppc.go.jp/news/anime_personalinfo/top/，2022 年 11 月参照).

[5] 永井 達也，高田 雄太，神薗 雅紀，“クッキーコンセントバナーにおけるダークパターンの実態調査”，Computer Security Symposium 2021，pp. 1053-1060,，2021.

[6] 東洋経済 Online,“好感度が高い企業・ブランド「トップ 200」”, (https://toyokeizai.net/articles/-/141280，2022 年 8 月参照).

[7] 個人情報保護委員会,“令和 2 年　改正個人情報保護法について”，(https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/，2022 年 11 月参照).

[8] ヤフー株式会社，“Yahoo! JAPAN プライバシーセンター”，(https://privacy.yahoo.co.jp/，2022 年 11 月参照).

付録 A

複数のホストに送信する ARP spoofing 攻撃の調査

A.1 はじめに

2008 年に ARP spoofing 攻撃を使用したサーバからの送信データの改ざんが行われた [4]．また，新型コロナウイルス感染症 (COVID-19) の流行とともに，ネットワークの需要が急激に拡大し，利用者層も多様化してきた．セキュリティ面に不安のある利用者が悪意ある人に狙われるような危険性も増加している．ARP spoofing の攻撃者は，対象機器に対して偽の ARP パケットを送信する．しかしながら，ARP spoofing のツールによっては，偽 ARP を送信する宛先を複数指定することもできる．

そこで，ARP パケットの宛先の数により，再送などの違いが生じ ARP spoofing に対する耐性が変わることと考えた．そのため，本稿では ARP spoofing の偽の ARP パケットの宛先所数と送信パケット総数の関係について明らかにする．

A.2 ARP spoofing

ARP spoofing は，対象の IP アドレスと MAC アドレスの対応付けを偽る不正行為である．通常，送信元 B は宛先 A の MAC アドレスを知るために，LAN 内で IP アドレスに対応している MAC アドレス問い合わせる ARP リクエストをブロードキャストする．A は，その IP アドレスに対応している MAC アドレスを示した ARP リプライをユニキャストする．これにより，B は IP アドレスと MAC アドレスの対応表を更新する．この対応付けを基に通信は行われる．攻撃者 C が B に対し A の IP アドレスの MAC アドレスは B のものとする偽の ARP リプライを返す．これにより，B では A の IP パケットを C に送ってしまう．以上の ARP spoofing の動作を図 A.1 に示す．

A.3 実験

A.3.1 目的

次の 2 つの ARP Spoofing により，送信パケット総数の違いを観測する．

(1) 攻撃者 C が対象 B に対してだけに偽の ARP パケットを送信する．

(2) 攻撃者 C がルータ A と B の両方に対して偽の ARP パケットを送信する．

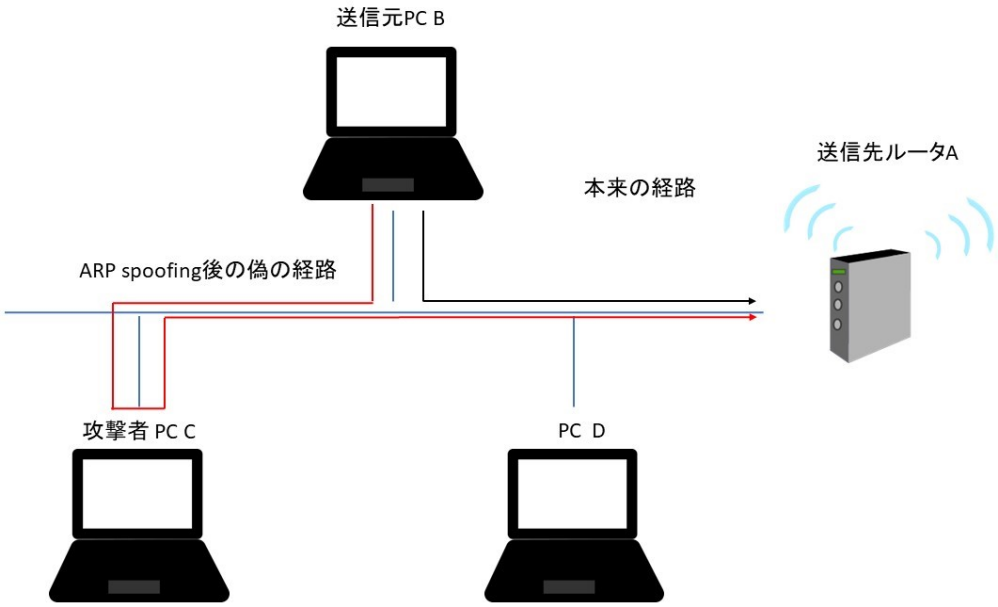

図 A.1　ARP Spoofing

A.3.2　準備

観測するパケットの始まりは，TCP コネクションが確立するところからである．つまり，SYN，ACK パケットが通信元・先の双方向に送信されるところから観測する．次に，観測するパケットの終わりは，TCP コネクションが切断するところまでである．つまり，FIN，ACK パケットが通信元・先の双方向に送信されるところで観測を終える．

A.3.3　実験環境と方法

実験環境を図 A.2 に示す．本実験は, 大きく 3 つに分けられる．

(1) 正常な場合のパケットを観測する．

(2) 対象 B にだけ偽の ARP パケットを送信し，攻撃 C を経由するパケットと経由しないパケットを観測する．攻撃 C が対象 B に対して，偽のパケットを送信することで，対象 B の ARP テーブルの IP アドレス I_A と MAC アドレス M_A の対応付けを I_A と M_C に変更させる．これにより，B から流れるパケットは C を経由し A へ流れる．しかし，往路は C を経由せ，,$S \rightarrow A \rightarrow B$ を流れる．

(3) ルータ A と対象 B に偽の ARP パケットを送信し，攻撃 C を経由するパケットと経由しないパケットを観測する．攻撃 C がルータ A，対象 B に対して，偽の ARP パケットを送信することで，ルータ A の

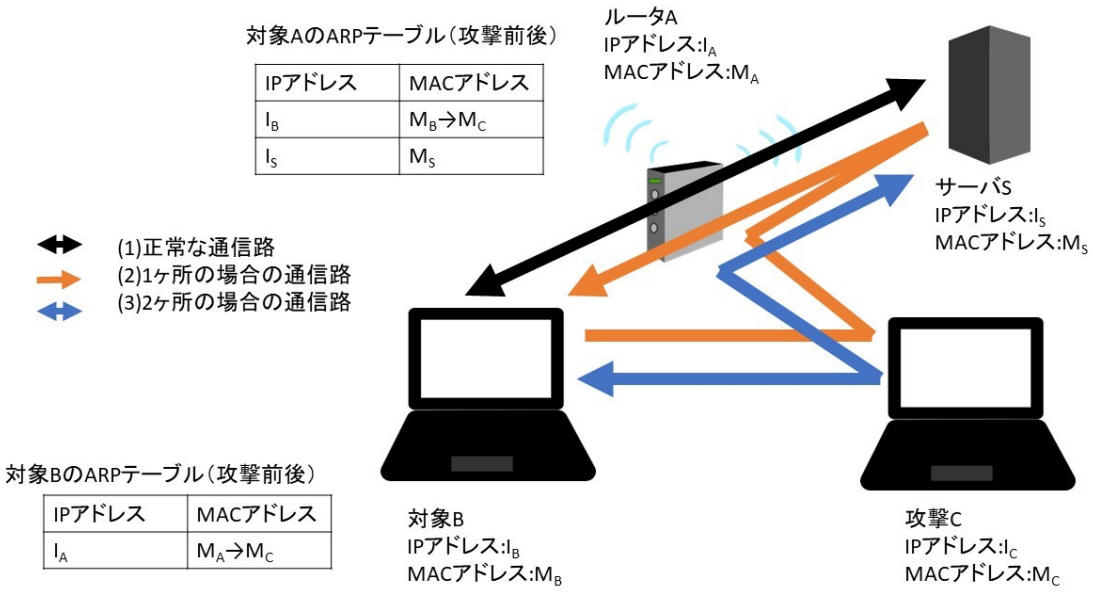

図 A.2　実験環境図

ARP テーブルの IP アドレス I_B と MAC アドレス M_B を M_C へ，B の ARP テーブルの I_A と MAC アドレス M_A を M_C に変更させる．これにより，ルータ A と B 間の通信は双方向とも C を経由する．パケットの観測は，対象 B と攻撃 C にて wireshark で行う．

A.3.4　実験結果

結果を表 A.1 に示す．1 列目は，通常時における観測結果である．1 ヶ所の場合で対象 B と攻撃 C の平均のパケット数を比較すると，対象 B のパケット数が 114.4 個多い．また，2 ヶ所の場合では攻撃 C のパケット数が対象 B の約 8.8 倍多い．対象 B と攻撃 C で観測されたパケットの一部を表 A.2 と表 A.3 に示す．TCP Out-Of-Order は，再送を求めていることを示している．

A.3.5　考察

ほとんどの場合，ARP spoofing 時のほうが送信パケット数が多い．従って，偽の ARP パケットが送信されると，送信パケットの再送要求や再送により，パケットが多くなる傾向がある．対象 B の 1 ヶ所にだけ偽のパケットを送信する場合，ルータ A から攻撃側 C を経由せずに対象 B に送信される．その場合，攻撃 C ではパケットの観測はできない．そのため，攻撃 C のパケット数は，対象 B の半分になると考えられる．けれども，実際には攻撃 C のパケット数は，対象 B の半分になっていない．これにより，通常の方がパケット

表 A.1　送信パケット総数

	(1) 通常	(2)1 ヶ所		(3)2 ヶ所	
試行	対象 A	対象 B	攻撃 C	対象 B	攻撃 C
1	137	146	112	160	1664
2	126	205	154	154	1443
3	157	239	156	146	1459
4	292	147	100	172	1498
5	208	391	34	212	1345
平均	184	225.6	111.2	168.8	1481.8

表 A.2　対象 B で観測されたパケットの一部（1 ヶ所）

No	Source	Destination	Protocol	length	Source port	Destination port	Flags	Seq	Win	Len
1	B	S	TCP	66	61235	80	SYN	0	64240	0
2	B	S	TCP	66	61236	80	SYN	0	64240	0
3	S	B	TCP	66	80	61235	SYN, ACK	0	1	29200
4	B	S	TCP	54	61235	80	ACK	1	1	131328
5	S	B	TCP	66	80	61236	SYN, ACK	0	1	29200

表 A.3　攻撃側 C で観測されたパケットの一部（1 ヶ所）

No	Source	Destination	Protocol	length	erro	Source port	Destination port	Flags	Seq
1	B	S	TCP	66		61235	80	SYN	0
1	B	S	TCP	66	TCP Out-Of-Order	61235	80	SYN	0
2	B	S	TCP	66		61236	80	SYN	0
2	B	S	TCP	66	TCP Out-Of-Order	61236	80	SYN	0
4	B	S	TCP	60		61235	80	1	1

数が多くなり，パケット数が増加していると考えられる．試行 5 は試行 1〜4 と比較して，パケット数が少ないことが，これらは同様の条件のもとで行っている．パケット数が明らかに少ないため，外れ値として考えられる．ルータ A と対象 B に偽のパケットを送信すると，攻撃 C では 1 ヶ所だけの場合の約 13 倍以上にパケット数が増加した．このことから，ルータ A に偽のパケットを送信すると，急激にパケット数が増加すると考えられる．

A.4　おわりに

本実験では，ARP spoofong 時の偽のパケットの宛先数と観測されるパケット総数の関係について明らかにした．1 ヶ所に ARP パケットを送る場合と比較して 2 ヶ所に偽の ARP パケットを送信すると，送信パケット数が急増した．この要因の究明を今後の課題とする．

参考文献

[1] 住友，“ARP スプーフィング攻撃の調査”，2020 年度菊池研究室卒業論文，2020.

[2] 平山，“ウイルスバスター for Home Network に関する調査研究”，2020 年度菊池研究室卒業論文，2020.

[3] 日経 BP 社, “特集 1 Python で学ぶサイバー攻撃の手口 〔Part 2〕 ARP キャッシュポイズニング編 アドレスの対応関係を改ざん 端末のアクセス先を自在に変える”，pp.26-27，日経 NETWORK2019/10 号，2019.

[4] 日経コミュニケーション，“特集 インターネット緊迫の裏側 〔Part3〕［ARP スプーフィング］通信内容改ざん，監視強化が先決”，pp.36-37，日経コミュニケーション 2009 年 2 月 1 日号，2009.

[5] 桧室和馬, 神屋郁子, 下川俊彦”家庭内無線 LAN における「無線 LAN ただ乗りおよび不正アクセスポイント」対策システムの開発”, 情報処理学会第 78 回全国大会,2016.