Vol.2020-CSEC-90 No.21
Vol.2020-SPT-38 No.21
2020/7/21

リンクデコレーションおよび CNAME クローキングによるクッキー共有のリスク分析

高田 雄太[1,a)]　伊藤 大貴[1]　熊谷 裕志[1]　神薗 雅紀[1]

概要：ウェブトラッキングによるプライバシー侵害が問題になっている．トラッキングの手法の一つに，サードパーティクッキーを用いる手法がある．本手法は，ユーザのウェブサイトアクセスを記録したクッキーを，アクセス解析・広告仲介業者等のサードパーティベンダへ共有することにより，ユーザの趣味趣向を分析する．過剰なトラッキングにより高まるプライバシーリスクに対して，法規制やブラウザベンダによるクッキーの利用制限が検討，導入されてきた．しかしながら，サードパーティベンダは，クッキーを URL に埋め込むリンクデコレーションや，サードパーティクッキーのファーストパーティクッキー化を図る CNAME クローキングを導入し，依然としてトラッキングを続けている．そこで本稿では，リンクデコレーションおよび CNAME クローキングを通じたクッキーの外部共有に起因するプライバシーリスク，ならびに新たに顕在化するセキュリティリスクついて分析する．

キーワード：トラッキング，クッキー，リンクデコレーション，CNAME クローキング

Risk Analysis of Cookie Share via Link Decoration and CNAME Cloaking

Yuta Takata[1,a)]　Daiki Ito[1]　Hiroshi Kumagai[1]　Masaki Kamizono[1]

1. はじめに

ウェブ上のユーザの動きを追跡するトラッキングは，アクセス解析や広告のコンバージョン測定の仕組みとして知られている．大量のウェブアクセスを分析することにより，ウェブサイトのパフォーマンスを測定したり，ユーザの趣味趣向に基づくウェブ広告を出したりすることは，ウェブマーケティング戦略に欠かせないものとなっている [1]．トラッキング手法の一つとして，サードパーティクッキーを用いる手法が知られている．クッキーは，ブラウザに保存されるサイズの小さなデータであり，ステートフルなウェブアクセスを実現する．アクセス解析・広告仲介業者等のサードパーティベンダは，ユーザのウェブアクセスを記録したクッキーを収集し，トラッキングに活用している．しかしながら，サードパーティクッキーを用いた過剰なトラッキングは，プライバシーを侵害する問題を引き起こしている [2], [3]．

サードパーティクッキーを用いたトラッキングに対して，法規制の整備ならびにブラウザベンダによる制限が活発化している．具体的に，一般データ保護規則 (GDPR) や ePrivacy 規則は，クッキーを収集，分析するウェブサイトに，ユーザへの事前通知や明確な説明を求めている [4]．Apple や Google といったブラウザベンダの間では，サードパーティクッキーの使用を制限する動きが広がっている [5], [6]．

一方，サードパーティベンダは，上記サードパーティクッキーに対する制限を迂回すべく，リンクデコレーションや CNAME クローキングといった，サードパーティクッキーを用いずにクッキーを外部に共有する仕組みを導入している [7], [8]．そこで本稿では，これらサードパーティベンダへクッキーを共有する仕組みを分析し，クッキー共有によ

[1] デロイト トーマツ サイバー合同会社
Deloitte Tohmatsu Cyber LLC
[a)] yuta.takata@tohmatsu.co.jp

Vol.2020-CSEC-90 No.21
Vol.2020-SPT-38 No.21
2020/7/21

り顕在化するリスクについて調査する．本稿の貢献は以下のとおりである．

- リンクデコレーションのみまたは CNAME クローキングのみを用いて，クッキーを共有するウェブサイトの存在を明らかにする．
- リンクデコレーションの 147 件 (5.59%)，CNAME クローキングの 149 件 (35.28%) が，Session クッキーの共有であることを示す．
- 収集した SameSite クッキーの内 66 件 (1.86%) が，クロスサイトリクエストの制限を迂回し，共有されていることを明らかにする．
- ファーストパーティウェブサイトに必要不可欠な (Strictly Necessary) クッキーが，CNAME クローキングにより共有されていることを明らかにする．

2. 関連研究

2.1 クッキーの分析

これまで多くの研究者により，クッキーの収集・分析に基づく実態調査やリスク調査がなされてきた．クッキーそのものの特徴 [9] やクッキーを用いたトラッキング [2]，ネットワーク経路上のクッキー観測等によるプライバシーリスク [3] の調査がある．その他，エバークッキー [1] やクッキー連携 [10] 等，クッキーを維持するための仕組みも分析されてきた．しかしながら，上記の研究はいずれも主にサードパーティクッキーに着目した分析である．我々が知る限りでは，ファーストパーティクッキーを共有するリンクデコレーションや CNAME クローキングに着目した研究は存在しない．

2.2 クッキーの保護

クッキーを保護する機能として，HttpOnly，Secure，および SameSite 属性がある [11]．HttpOnly 属性は，JavaScript によるクッキーの参照 (document.cookie) を制限でき，クロスサイトスクリプティング (XSS) 攻撃によるクッキー漏えいを防ぐことができる．Secure 属性は，クッキーの送受信を HTTPS 通信に制限でき，ネットワーク経路上のクッキー漏えいを防ぐことができる．SameSite 属性は，クロスサイトリクエストを制限する “Strict” または “Lax” の設定により，クロスサイトリクエストフォージェリ (CSRF) 攻撃を防止できる．

その他，クッキーを保護するブラウザ拡張機能も存在するが，Franken らはこれら保護機能のいくつかはバイパスできてしまうと報告している [12]．

3. 研究背景

3.1 クッキー

クッキー (Cookie) とは，ブラウザに保存されるテキストデータであり，サーバの HTTP 応答ヘッダ Set-Cookie: name=value またはクライアントの HTTP 要求ヘッダ Cookie: name=value を用いて送受信される [11]．クッキーは，保存できる期間に応じて，Permanent クッキーと Session クッキーの 2 種類に大別される．Permanent クッキーは，Expires または Max-Age 属性を指定することにより，指定した日時までまたは指定した期間ブラウザにデータを維持できる．一方，Session クッキーは，これら属性を指定せずブラウザを閉じるまでデータを維持できる．したがってクッキーは，従来のステートレスなウェブアクセスに対して，ステートフルなウェブアクセスを実現するために考案された機能であり，主にセッション管理，パーソナライゼーション，トラッキングに用いられている．

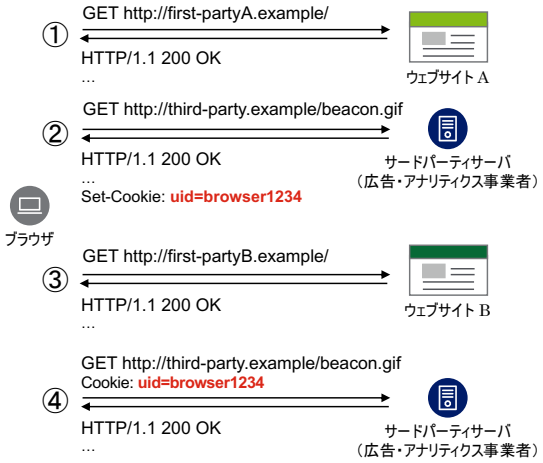

図 1 サードパーティクッキーを用いたトラッキング

3.2 クッキーの送受信

ユーザや認証セッションを識別するためにクッキーを用いる場合，機微なデータがクッキーとして送受信される可能性がある．制限なしにそのようなクッキーを送受信できてしまうと，セッションハイジャックや CSRF 攻撃が成立してしまう．したがって，クッキーを送受信できる URL は，Domain および Path 属性に指定されたスコープに従い制限される．Domain 属性は，クッキーを受信できるドメイン名を指定できる (そのサブドメイン名も含まれる)．Path 属性は，クッキーを送信するために必要な URL パスを指定できる．この時，Domain 属性のドメイン名が URL アドレスバーのドメイン名と一致する場合に，そのクッキーをファーストパーティクッキーと呼び，それ以外のクッキーをサードパーティクッキーと呼ぶ [13]．

3.3 サードパーティクッキーを用いたトラッキング

サードパーティベンダは，ウェブ上のユーザの動きをトラッキングし，ユーザの趣味趣向に基づく広告を掲載することにより，宣伝効果を最大化している [14]．図 1 を用いて，サードパーティクッキーによるトラッキングの仕組み

Vol.2020-CSEC-90 No.21
Vol.2020-SPT-38 No.21
2020/7/21

図 2　リンクデコレーションを用いたファーストパーティクッキーの共有

```
first-party.example.              IN A      192.168.0.1.
csec2020.first-party.example.     IN CNAME  user1.third-party.example.
```

図 3　ファーストパーティウェブサイト管理者が登録する DNS リソースレコード

```
user1.third-party.example.   IN A   172.16.0.1.
user2.third-party.example.   IN A   172.16.0.1.
user3.third-party.example.   IN A   172.16.0.1.
…
```

図 4　サードパーティベンダが登録する DNS リソースレコード

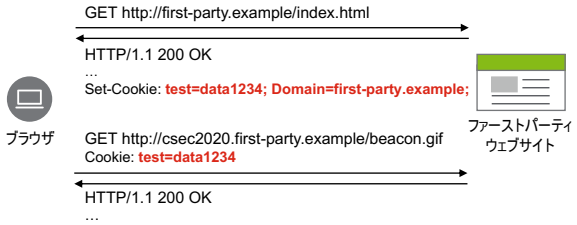

図 5　CNAME クローキングを用いたファーストパーティクッキーの共有

を説明する．1) まず，ブラウザでウェブサイト A にアクセス後，ウェブサイト A に含まれるサードパーティコンテンツの要求が発生する．2) 要求を受信したサードパーティサーバは，応答コンテンツに “Set-Cookie” ヘッダを用いてブラウザを識別するデータを設定し，ウェブサイト A へのアクセスを記録する．3) 次に，ブラウザで同一のサードパーティコンテンツを使用したウェブサイト B にアクセスする．4) この時，“Cookie” ヘッダを用いて先に記録したクッキーを自動的に付与したコンテンツ要求がサードパーティサーバへ送信される．以上のように，サードパーティサーバは，ブラウザによるウェブサイト A からウェブサイト B へのウェブサイトを跨ったアクセスを追跡できる．多くのファーストパーティウェブサイト管理者は，広告を掲載するスペースをサードパーティベンダに売ることにより利益を獲得しているため，サードパーティベンダにはこのようなクロスサイトリクエストが大量に蓄積され，ユーザの挙動分析が可能となる．

3.4　法規制およびブラウザベンダの動向

サードパーティクッキーを用いたトラッキングに対するプライバシーリスクが叫ばれ，法規制の整備ならびにブラウザベンダによる制限が活発化している．欧米諸国では，GDPR や ePrivacy 規則，CCPA 等の法規制が施行・検討され，クッキーの収集・処理に対して，ユーザへの事前通知や明確な説明が求められる [4]．ブラウザベンダは，サードパーティクッキーの利用そのものを制限する機能を検討している．Apple は，2019 年 4 月にトラッキング目的のサードパーティクッキーを即座に消去するとともに，ファーストパーティクッキーの保存期間を 24 時間に制限すると発表している [7]．Google は，2019 年 10 月に `SameSite=None` および `Secure` 属性のないサードパーティクッキーはブロックすると発表している [6]．

3.5　クッキー共有

サードパーティベンダは，前節の動向を受けて，クッキーを URL に埋め込む**リンクデコレーション (Link Decoration)** やサードパーティクッキーのファーストパーティ化を図る **CNAME クローキング (CNAME Cloaking)** といった仕組みを取り入れ，クッキーに対する制限を迂回しようと試みている．

3.5.1　リンクデコレーション

リンクデコレーションは，ブラウザに保存されたファーストパーティクッキーを参照し，それらをサードパーティ URL に埋め込み共有する手法である [7]．リンクデコレーションを用いて，ファーストパーティクッキーをサードパーティサーバに共有する例を図 2 に示す．ファーストパーティウェブサイトにアクセスすると，サーバからの応答に含まれる `Set-Cookie` ヘッダによりクッキーがブラウザに保存される．このクッキーは，JavaScript の `document.cookie` によりブラウザ上で参照され，サードパーティ URL に GET 変数として埋め込まれることにより，サードパーティサーバへ共有される．このような JavaScript により動的に共有する方法以外にも，あらかじめ情報を埋め込んだリンクを静的に生成する方法もある．リンクデコレーションは，主にファーストパーティサイトに設置されたサードパーティコンテンツにより用いられる．

3.5.2　CNAME クローキング

CNAME クローキングは，サードパーティベンダが設定したドメイン名 (IP アドレス) を別名としてファーストパーティのサブドメインに割り当てる手法である [8]．図 3，図 4，および図 5 を用いてその仕組みを説明する．まず，あらかじめファーストパーティウェブサイトの管理者とサードパーティベンダは，図 3 および図 4 に示すような DNS リソースレコードをそれぞれ設定する．この時，管理者はサードパーティベンダに指定されたドメイン名 `user1.third-party.example` をサブドメイン

csec2020.first-party.example の CNAME レコードとして設定する．次に管理者は，そのサブドメインを使用した URL のコンテンツをファーストパーティウェブサイトに設置する．以上の準備により，図 5 に示すとおり，ブラウザがファーストパーティウェブサイトにアクセスすると，Cookie ヘッダによりファーストパーティクッキーが付与された状態で設置コンテンツへの要求が発生する．この時の通信先は，サブドメイン csec2020.first-party.example の別名である user1.third-party.example，すなわち，サードパーティベンダの IP アドレス 172.16.0.1 となり，サードパーティベンダにファーストパーティクッキーが共有される．この手法は，クッキーが Domain 属性を指定した場合に，そのサブドメインに対してもクッキーが送信される仕様を巧みに利用している．

4. クッキー共有の検知と分析

リンクデコレーションおよび CNAME クローキングにより共有されるファーストパーティクッキーを検知し，それらクッキー共有により顕在化するリスクを分析する．

4.1 クッキー共有の検知

リンクデコレーションの検知. リンクデコレーションを検知するために，ウェブサイトアクセス時に観測したサードパーティ URL にファーストパーティクッキーの値が含まれているか分析する．もし含まれている場合には，それをリンクデコレーションによりサードパーティへ共有されたファーストパーティクッキーとして検知する．

CNAME クローキングの検知. CNAME クローキングを検知するために，ファーストパーティクッキーの Domain 属性に設定されたドメイン名の DNS リソースレコードを分析する．以下の項目すべてに該当する場合には，それを CNAME クローキングによりサードパーティへ共有されたファーストパーティクッキーとして検知する．

- Domain 属性のドメイン名に A レコードが設定されていない．
- Domain 属性のドメイン名に CNAME レコードが設定されている．
- 上記 CNAME レコードに設定されたドメイン名は，ファーストパーティのドメイン名ではない．
- 上記 CNAME レコードに設定されたドメイン名の IP アドレスは，入力した URL に割り当てられた IP アドレスではない．

4.2 クッキー共有の分析

まず，収集したクッキーについて，クッキーの総数，Permanent または Session の種別分類，Secure, HttpOnly, SameSite 属性の設定割合，そしてクッキーの値の一意性を集計，分析する．クッキーの値の一意性は，ウェブ上のユーザを一意に特定できる可能性を意味し，その値が高いとトラッキングによるプライバシー侵害のリスクが顕在化する．一意性の算出には，Sanchez-Rola らのアプローチ [4] と同様，パスワードの強度を算出できる zxcvbn [15] を使用した．

表 1 ウェブサイトアクセス結果

データセット	HTTP 200	HTTP エラー	アクセスエラー
Top5K	4,297	173	530
Rand5K	4,598	90	312
合計	8,895	263	842

次に，リンクデコレーションおよび CNAME クローキングにより共有された一意性の高いクッキーを対象に，どのような用途のクッキーが共有されているか (クッキーの目的) を調査する．本調査には，Cookiepedia [13] によるクッキー名の検索結果を使用した．

最後に，リンクデコレーションにより Secure クッキーが HTTP リンクを通じて漏えいしていないか，CNAME クローキングにより SameSite のクロスサイトリクエストの制限を迂回していないかを分析する．

4.3 クッキー共有先および共有元の分析

共有先として多く用いられるドメイン名を対象に，共有先のサードパーティベンダがどのようなサービスを提供しているかを調査する．本調査には，Cisco Talos [16] が提供するドメイン名のコンテンツカテゴリデータを使用した．

一方で，リンクデコレーションおよび CNAME クローキングによる共有元のウェブサイトが，クッキー共有自体を認識しているかどうかを調査する．クッキーを収集し，それらをウェブサイト外で使用したり，売買したりする場合は，その内容をプライバシーポリシーに明確に記載する必要がある [13]．そこで本分析では，共有元ウェブサイトにおけるプライバシーポリシーの有無やクッキーの取得・処理に関する記載の有無を手動で調査した．

4.4 分析環境

ウェブサイトにアクセスし，クッキーを収集するために，Ubuntu 18.04 にインストールした Chromium 79.0 [17] を用いた．アクセス後，JavaScript の実行や非同期通信によりクッキーが送受信されることを考慮し，コンテンツ読み込み後 3 秒間待機した．なお，3 分間でコンテンツの読み込みが終わらない場合は，ウェブサイトアクセスをタイムアウトした．また，ブラウザのシークレットブラウジング機能 [18] を用いて，アクセス履歴の影響を最小限にした．

分析するウェブサイトとして，AlexaTopSites [19] に掲載されたドメイン名から上位 5,000 件の Top5K と無作為に 5,000 件抽出した Rand5K の 2 つのデータセットを用意した．なお，アクセスする URL は，ドメイン名に “http://” を付与した URL である．

表 2　収集したクッキーの設定と一意性 (Top5K)

Domain	総数	Permanent	Session	HttpOnly	Secure	SameSite	zxcvbn_log10≥10
1st-party	19,481	14,211 (72.95%)	5,270 (27.05%)	4,012 (20.59%)	3,385 (17.38%)	2,296 (11.79%)	12,873 (66.08%)
3rd-party	66,609	61,714 (92.65%)	4,895 (7.35%)	9,587 (14.39%)	51,504 (77.32%)	50,931 (76.46%)	48,428 (72.70%)

表 3　収集したクッキーの設定と一意性 (Rand5K)

Domain	総数	Permanent	Session	HttpOnly	Secure	SameSite	zxcvbn_log10≥10
1st-party	13,118	10,160 (77.45%)	2,958 (22.55%)	2,689 (20.50%)	1,089 (8.30%)	1,247 (9.51%)	8,592 (65.50%)
3rd-party	28,994	25,838 (89.11%)	3,156 (10.89%)	5,553 (19.15%)	21,007 (72.45%)	20,443 (70.51%)	21,119 (72.84%)

表 4　SameSite 属性の設定状況

Domain	None	Lax	Strict
1st-party	1,002 (28.28%)	2,436 (68.76%)	105 (2.96%)
3rd-party	71,266 (99.85%)	103 (0.14%)	5 (0.01%)

表 5　クッキー共有の方法

サードパーティクッキー	リンクデコレーション	CNAME クローキング	Top5K	Rand5K
✗	✗	✗	832	1,605
✔	✗	✗	2,491	2,394
✗	✔	✗	54	58
✔	✔	✗	760	509
✗	✗	✔	7	1
✔	✗	✔	109	24
✗	✔	✔	0	0
✔	✔	✔	44	7

5. 分析結果

5.1 クッキーの収集

2020 年 2 月に合計 10,000 URL のウェブサイトにアクセスした．その結果，表 1 に示すとおり，8,895 件のウェブサイトがなんらかのコンテンツを応答し，それ以外は HTTP ステータスコード 400 番台 500 番台の HTTP エラー，DNS 名前解決エラー，またはタイムアウト等のアクセスエラーを応答した．アクセスできたウェブサイトでは，コンテンツの読み込みにより，ファーストパーティ URL 405,601 件，サードパーティ URL 551,791 件のアクセスが発生し，32,599 件のファーストパーティクッキーおよび 95,603 件のサードパーティクッキーを収集できた．Top5K データセットでは最大 218 件，Rand5K データセットでは最大 239 件のサードパーティクッキーを設定するウェブサイトが観測された．以降では，これら収集したクッキーを分析する．

5.2 クッキーの種別と設定状況

データセット Top5K および Rand5K に対して，収集したクッキーの種別および設定の集計結果を表 2 および表 3 にそれぞれ示す．サードパーティクッキーの総数は，Top5K のほうが 2 倍以上多く，人気ドメイン名であるがゆえに広告やアナリティクス等の導入が進んでいることが伺える．それ以外の種別や設定は，両データセットの間で大きな差異はなかった．

ファーストパーティおよびサードパーティ間の差異に着目すると，両データセットともサードパーティクッキーの方が総数が多く，ほとんどが Permanent クッキー，すなわちクッキーに保存期間があることがわかる．また，HttpOnly 属性の設定割合に大きな差異はなかったが，Secure および SameSite 属性は，いずれもサードパーティクッキーの方が普及しており，外部ドメインに対してより安全なクッキーの送受信がなされる傾向があるとわかる．これは Google が 2020 年 2 月に公開した Chrome バージョン 80 から SameSite=None および Secure 属性のないサードパーティクッキーをブロックするよう更新したことが影響していると推測できる [6]．実際にサードパーティクッキーの SameSite 属性に設定された値は，表 4 に示すとおりほとんどが “None” であり，“Lax” は数%，“Strict” は極僅かであった．多くのサードパーティベンダは，制限のかかる “Lax” や “Strict” ではなく，一時的な処置として “None” を設定したと推測できる．一方，ファーストパーティクッキーの SameSite 属性には，クロスサイトリクエストを防ぐ “Lax” が多く設定されていた．なお，SameSite 属性のないクッキーは，2020 年 2 月の更新以降 Google Chrome では SameSite=Lax として扱われる [6]．

次に，クッキーにどのような値が設定されているかを分析するため，その一意性を算出した．具体的には，zxcvbn の guesses_log10 の値を用いた [20]．guesses_log10 は，区別できるユーザ数を意味し，その値が 9 であれば $10^9 = 1,000,000,000$ 人のユーザを区別できることを意味する．世界のインターネットユーザ数は，2019 年 12 月時点で 45.7 億人と報告[*1]されているため，本分析では guesses_log10 の値が 10 を超えるクッキーを集計した．その結果，表 2 および表 3 に示すとおり，60%以上のファーストパーティおよび 70%以上のサードパーティクッキーが，一意性の高いデータを送受信していた．以降のクッキー共有の分析では，意味ある情報量の高いクッキー共有を対象とするため，これら zxcvbn_log10 ≥ 10 のクッキー共有を分析する．

[*1] “World Internet Users Statistics and 2020 World Population Stats”, https://www.internetworldstats.com/stats.htm

表 6 リンクデコレーションにより共有されたファーストパーティクッキーの設定

データセット	共有数	Permanent	Session	HttpOnly	Secure	SameSite
Top5K	1,480	1,379 (93.18%)	101 (6.82%)	22 (1.49%)	110 (7.43%)	97 (6.55%)
Rand5K	1,057	1,011 (95.65%)	46 (4.35%)	8 (0.76%)	23 (2.18%)	27 (2.55%)

表 7 リンクデコレーションによる共有数 Top5 のクッキー名 (Top5K)

クッキー名	共有数	目的
__asc	198	Targeting/Advertising
__auc	198	Targeting/Advertising
__utma	100	Performance
_fbp	83	Targeting/Advertising
__atuvs	67	Functionality

表 8 リンクデコレーションによる共有数 Top5 のクッキー名 (Rand5K)

クッキー名	共有数	目的
__utma	123	Performance
_fbp	103	Targeting/Advertising
__atuvs	100	Functionality
_shopify_y	59	Performance
_shopify_fs	59	Performance

5.3 クッキー共有の検知結果

サードパーティクッキーならびに，リンクデコレーションや CNAME クローキングの使用を検知したウェブサイトを集計した．その結果を表 5 に示す．サードパーティクッキーのみを使用するウェブサイトが半分以上を占める中，リンクデコレーションや CNAME クローキングを使用するウェブサイトは，16.10%，2.16% とそれぞれ存在した．また，リンクデコレーションのみまたは CNAME クローキングのみを使用するウェブサイトも 112 件と 8 件とそれぞれ存在した．このようなウェブサイトは，サードパーティベンダへのファーストパーティクッキー共有が意図したものであるか特に確認する必要があると言える．

5.4 クッキー共有の分析結果

5.4.1 リンクデコレーションによる共有の特徴

リンクデコレーションにより共有されたクッキーの種別および設定の集計結果を表 6 に示す．共有されたクッキーは，ほとんどが `Permanent` クッキーであるが，147 件 (5.79%) だけ `Session` クッキーが含まれていた．`Session` クッキーは，ユーザや認証セッションの識別等に用いられるが，このようなクッキーが漏えいするとセッションハイジャックや CSRF 攻撃が成立するセキュリティリスクが高まる [11]．また，`Secure` クッキーは 133 件共有されていたが，混合コンテンツ (Mixed Content) による HTTP リンクへの `Secure` クッキー漏えいは確認されなかった．なお，混合コンテンツも，2020 年 2 月更新の Google Chrome ではブロックされるため，`Secure` クッキーが漏えいするリスクは低減される [21]．一方で，`SameSite` クッキーは，“`Lax`” または “`Strict`” に設定されているにも関わらず，それらクッキーを共有していた事例が 54 件存在した．このようなクッキー共有は，`SameSite` による制限を迂回したクロスサイトリクエストとみなすことができ，上述したセキュリティリスクに加え，トラッキングによるプライバシーリスクも高まる [12].

次に，リンクデコレーションにより共有されたクッキーがどのような用途で用いられているか，その目的を調査した．データセット Top5K と Rand5K における共有数 Top5 のクッキー名に対する Cookiepedia の検索結果を表 7 および表 8 にそれぞれに示す．Top5K では広告目的である “Targeting/Advertising” のクッキー共有が最も多く，Rand5K では効果測定を目的とする “Performance” のクッキー共有が最も多かった．5.2 節と同様，共有されているクッキー名からも，Top5K データセットでは広告やアナリティクスの導入が進んでいることがわかる．

5.4.2 CNAME クローキングによる共有の特徴

CNAME クローキングにより共有されたクッキーの種別および設定の集計結果を表 9 に示す．表 9 のとおり，45% 以上の `Session` クッキーおよび 35% 以上の `SameSite` クッキーが CNAME クローキングにより共有されている．共有された `SameSite` クッキーの内，“`Lax`” または “`Strict`” が設定されたクッキーは 12 件存在した．前節のリンクデコレーションと同様のセキュリティおよびプライバシーリスクが顕在化する．

次に，前節と同様に，共有されたクッキーの目的を調査した．その結果を表 10 および表 11 に示す，総数は少ないものの，機能提供を目的とする “Functionality” やウェブサイトに必須なクッキーを意味する “Strictly Necessary” が観測された．これはファーストパーティクッキーを直接共有してしまう CNAME クローキングの特徴の表れであると考えられる．

5.5 クッキー共有先および共有元の分析結果

5.5.1 クッキー共有先のドメイン名

クッキー共有先のドメイン名は，どのようなサービスを提供しているか，ドメイン名のカテゴリを調査した．共有先として多く用いられるドメイン名 Top5 を対象に，データセット Top5K と Rand5K の結果を表 12，表 13，表 14 および表 15 に示す．リンクデコレーションは，カテゴリにばらつきがあるものの，Google や Facebook，Amazon といった巨大組織が保有するドメイン名が多く使用されている．一方で，CNAME クローキングは，“Infrastructure and CDN” や “SaaS and B2B” のカテゴリが多い．これらの CNAME レコードは，クローキング目的ではなく，複数ドメイン名および複数 IP アドレスの組み合わせによる

表 9　CNAME クローキングとして検知されたファーストパーティクッキーの設定

データセット	検知数	Permanent	Session	HttpOnly	Secure	SameSite
Top5K	352	221 (62.78%)	131 (37.22%)	156 (44.32%)	185 (52.56%)	136 (38.64%)
Rand5K	54	36 (66.67%)	18 (33.33%)	13 (24.07%)	25 (46.30%)	20 (37.04%)

表 10　CNAME クローキングによる共有数 Top5 のクッキー名 (Top5K)

クッキー名	共有数	目的
JSESSIONID	23	Strictly Necessary
AWSALB	14	Unknown
AWSALBCORS	14	Unknown
pardot	14	Targeting/Advertising
gmid	13	Unknown

表 11　CNAME クローキングによる共有数 Top5 のクッキー名 (Rand5K)

クッキー名	共有数	目的
anon_id	7	Targeting/Advertising
pardot	5	Targeting/Advertising
JSESSIONID	2	Strictly Necessary
__cfduid	2	Strictly Necessary
_sp_v1_uid	2	Functionality

負荷分散が目的であると推測できる．現状悪性なドメイン名ではないと考えられるが，これらドメイン名が乗っ取られたり，悪性化した場合に，クッキー漏えいのリスクが高まる．

5.5.2　クッキー共有元ウェブサイトのプライバシーポリシーおよびクッキーに関する記載の有無

前節の共有先 Top5 のドメイン名に対する共有元ウェブサイト 297 件において，英語表記のウェブサイト 139 件を対象に，プライバシーポリシーの規定があるか調査した．その結果，99 件 (71.22%) のウェブサイトにおいて，プライバシーポリシーが規定されていた．

次に，これらプライバシーポリシーに対して，クッキーに関する記述があるか調査した．その結果，85 件 (61.15%) のプライバシーポリシーにおいてクッキーに関する記述が存在した．しかしながら，一般的な内容が多く，具体的なサードパーティベンダ名も含めたプライバシーポリシーは 35 件 (25.18%) にとどまった．

6.　議論

6.1　クッキー共有のセキュリティリスクとその対応

不要なクッキー共有により，セッションハイジャックや CSRF 攻撃が成立するセキュリティリスクが顕在化する [12], [22].

リンクデコレーションによる共有では，機微データを URL に埋め込まないよう注意するとともに，HttpOnly 属性を用いて JavaScript のクッキー参照を制限することにより，一定のリスク削減効果が得られる．一方，CNAME クローキングは，URL ではなくクッキーそのものの仕組みを利用してクッキーを共有する．したがって，前述の HttpOnly 属性ではクッキー共有を制限できない．また，クロスドメインリクエストを制限する SameSite 属性を設定したとしても，CNAME クローキングのクッキーはファーストパーティクッキーとして動作するため，5.4.2 節に記載したとおり，その設定値に関係なくクッキーは共有されてしまう．したがって，このようなリスクを低減するためには，CNAME クローキングを採用するサードパーティベンダを使用しないことや DNS レベルのブロッキング対策 [8] が必要である．

6.2　クッキー共有のプライバシーリスクとその対応

不要なクッキーが共有されると，ユーザの意図しないところで趣味趣向が分析されたり，トラッキングされたり，個人を特定されたりするプライバシーリスクが顕在化する [2].

ウェブサイト管理者は，取得するクッキー (すなわちファーストパーティクッキー) に関する収集・処理を明快に説明する必要がある．サードパーティクッキーやクッキー共有についても，サードパーティベンダにおけるプライバシーポリシーを把握するとともに，該当するクッキーの種別や内容を明快に説明する必要がある．その他，欧米等諸外国からのアクセスに対しては，クッキーに関連する法規制が適用されることがあるため，上記に加え，オプトイン・オプトアウトできる機能等を提供する必要がある．

6.3　制限事項

本分析では，ブラウザでウェブサイトへアクセスし，コンテンツを読み込んだ後 3 秒間に送受信されたクッキーを収集した．したがって，3 秒後以降に送受信が発生するクッキーは収集対象外となる．また，日本国内からのアクセスで送受信したクッキーを収集，分析している．したがって，欧米等の諸外国からのアクセスにより送受信されるクッキーの分析は対象外である．これらの分析結果は，本稿の結果と多少異なると予想されるが，その収集と分析は今後の課題とする．

リンクデコレーションおよび CNAME クローキングの分析は，情報量の高いクッキーのみを対象としている．加えて，リンクデコレーションについては，クッキーの値が直接 URL に埋め込まれた場合のみを分析対象としており，難読化やエンコード等変換が施された場合は分析対象外となる．いずれの制限も結果に変化を与えると予想されるが，クッキー共有量の観点では少なく見積もって分析しているため，本研究成果への影響も少ないと考える．

表 12 リンクデコレーションの共有先 Top5 ドメイン名 (Top5K)

ドメイン名	共有数	カテゴリ
certify.alexametrics.com	399	SaaS and B2B
www.facebook.com	97	Social Networking
www.google-analytics.com	85	Computers and Internet
m.addthis.com	69	Business and Industry
ssl.google-analytics.com	63	Computers and Internet

表 13 リンクデコレーションの共有先 Top5 ドメイン名 (Rand5K)

ドメイン名	共有数	カテゴリ
v.shopify.com	342	Business and Industry
www.facebook.com	106	Social Networking
m.addthis.com	100	Business and Industry
www.google-analytics.com	92	Computers and Internet
ssl.google-analytics.com	61	Computers and Internet

表 14 CNAME クローキングの共有先 Top5 CNAME ドメイン名 (Top5K)

ドメイン名	共有数	カテゴリ
mms.fra.sp-prod.net	15	Infrastructure and CDN
cluster3.technolutions.net	9	Computers and Internet
Frontier-Airlines-lb -2074229919.us-east-2.elb .amazonaws.com	8	SaaS and B2B
pi-ue1-lba1.pardot.com	8	SaaS and B2B
lb.eu1.gigya.com	8	Business and Industry

表 15 CNAME クローキングの共有先 Top5 の CNAME ドメイン名 (Rand5K)

ドメイン名	共有数	カテゴリ
cs1143.wpc.chicdn.net	7	Infrastructure and CDN
pi-ue1-lba6.pardot.com	4	SaaS and B2B
pi-ue1-lba2.pardot.com	4	SaaS and B2B
mms.iad.sp-prod.net	4	Infrastructure and CDN
message200-iad.sp-prod.net	3	Infrastructure and CDN

7. おわりに

サードパーティベンダは，サードパーティクッキーに加えて，リンクデコレーションや CNAME クローキングにより共有されたクッキーを収集している．本稿では，そのようなクッキー共有を分析し，顕在化するセキュリティおよびプライバシーリスクを評価した．本評価により，法規制やベンダ，管理者による対策が進み，ユーザのセキュリティおよびプライバシー強化に繋がることを期待する．

参考文献

[1] G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, and C. Diaz, “The Web Never Forgets: Persistent Tracking Mechanisms in the Wild Categories and Subject Descriptors,” in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2014.

[2] J. R. Mayer and J. C. Mitchell, “Third-party web tracking: Policy and technology,” in *IEEE Symposium on Security and Privacy (S&P)*, pp. 413–427, IEEE, 2012.

[3] D. Reisman, S. Englehardt, C. Eubank, P. Zimmerman, and A. Naranyanan, “Cookies that give you away: Evaluating the surveillance implications of web tracking,” in *World Wide Web Conference (WWW)*, 2015.

[4] I. Sanchez-rola, M. D. Amico, D. Balzarotti, and I. Santos, “Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control,” in *ACM Symposium on Information, Computer and Communications Security (AsiaCCS)*, 2019.

[5] J. Wilander, “Preventing Tracking Prevention Tracking.” https://webkit.org/blog/7675/intelligent-tracking-prevention/.

[6] “Developers: Get Ready for New SameSite=None; Secure Cookie Settings.” https://blog.chromium.org/2019/10/developers-get-ready-for-new.html.

[7] J. Wilander, “Intelligent Tracking Prevention 2.2.” https://webkit.org/blog/8828/intelligent-tracking-prevention-2-2/.

[8] R. Cointepas, “CNAME Cloaking, the dangerous disguise of third-party trackers.” https://medium.com/nextdns/cname-cloaking-the-dangerous-disguise-of-third-party-trackers-195205dc522a.

[9] A. Cahn, S. Alfeld, P. Barford, and S. Muthukrishnan, “An Empirical Study of Web Cookies,” in *World Wide Web Conference (WWW)*, 2016.

[10] P. Papadopoulos, N. Kourtellis, and E. P. Markatos, “Cookie synchronization: Everything you always wanted to know but were afraid to ask,” in *The Web Conference (WWW)*, pp. 1432–1442, 2019.

[11] Mozilla, “HTTP Cookie.” https://developer.mozilla.org/ja/docs/Web/HTTP/Cookies.

[12] G. Franken, T. Van Goethem Imec-Distrinet, K. U. Leuven, and W. Joosen Imec-Distrinet, “Who Left Open the Cookie Jar? A Comprehensive Evaluation of Third-Party Cookie Policies,” in *USENIX Security Symposium*, 2018.

[13] Cookiepedia, “How We Classify Cookies.” https://cookiepedia.co.uk/classify-cookies.

[14] P. Papadopoulos, N. Kourtellis, P. R. Rodriguez, and N. Laoutaris, “If you are not paying for it, you are the product: How much do advertisers pay to reach you?,” in *ACM SIGCOMM Conference on Internet Measurement Conference (IMC)*, 2017.

[15] D. L. Wheeler, “zxcvbn: Low-budget password strength estimation,” in *USENIX Security Symposium*, pp. 157–173, 2016.

[16] Cisco, “Intelligence Categories - Cisco Talos Intelligence Group - Comprehensive Threat Intelligence.” https://talosintelligence.com/categories.

[17] “The Chromium Projects.” https://www.chromium.org/Home.

[18] “How private browsing works in Chrome.” https://support.google.com/chrome/answer/7440301.

[19] “Alexa Top Sites.” https://www.alexa.com/topsites.

[20] “zxcvbn.” https://github.com/dropbox/zxcvbn.

[21] “No More Mixed Messages About HTTPS.” https://security.googleblog.com/2019/10/no-more-mixed-messages-about-https_3.html.

[22] T. Watanabe, E. Shioji, M. Akiyama, K. Sasaoka, T. Yagi, and T. Mori, “User Blocking Considered Harmful? An Attacker-Controllable Side Channel to Identify Social Accounts,” in *IEEE European Symposium on Security and Privacy*, pp. 323–337, 2018.