Trusted Tag Provider(TTP) を導入したセキュア広告プラットフォームの提案

坂本 一仁[1]　稲垣 俊[1]　島岡 政基[1]　松永 昌浩[1]

概要：Malvertising が猛威を振るっている．Malvertising は，攻撃者が広告プラットフォームの広告配信サーバへ不正侵入する，または正当な広告事業者を偽ることによって，多くのインターネットユーザにマルウェアを配信する攻撃である．本稿では広告プラットフォームに認証事業者 (TTP: Trusted Tag Provider) と電子署名・検証のプロトコルを導入することにより，広告配信サーバへの攻撃に耐性のある広告配信方式を提案する．さらに TTP と従来の広告事業者によってトラストフレームワークを構築することにより，攻撃者を広告プラットフォームから排除する枠組みを示し，その展望を述べる．

キーワード：広告プラットフォーム，Malvertising，広告配信方式，署名プロトコル，トラストフレームワーク

A Proposal of Secure Ad Platform with Trusted Tag Provider

Takahito Sakamoto[1]　Shun Inagaki[1]　Masaki Shimaoka[1]　Masahiro Matsunaga[1]

Abstract: Malvertising is a coined word combining malware with advertising. Malvertising attacks users via ad platform hacked by an adversary or scammed by a malicious advertising provider. This paper proposes an advertising method which is tolerant against attacking the ad server via using the verifier (TTP: Trusted Tag Provider) and signature protocols. Furthermore, this paper shows the secure ad platform without adversaries, by constructing trust framework with TTP and advertising providers.

Keywords: Ad Platform, Malvertising, Advertising Method, Signature Protocol, Trust Framework

1. はじめに

インターネットが発展すると共にインターネット広告も発展してきた．現在では多くの広告事業者がインターネット広告配信プラットフォーム（以下，広告プラットフォーム：詳細は 2 節）へ参入し，インターネットを利用するユーザへ広告を届けている．しかし，広告プラットフォームが成長する一方で，広告プラットフォームを悪用してマルウェアを拡散する **Malvertising** と呼ばれる攻撃が顕著になっている．Malvertising は Malware と Advertising を組み合わせた造語である．Cyphort の調査 [1] では，Malvertising の手口は年々巧妙になっており，短期間で数多くのユーザに影響を与える危険性を示している．

Malvertising の対策としては，ユーザがウィルス対策ソフト等を導入することや，広告プラットフォームが広告配信サーバのセキュリティおよび関係事業者や広告コンテンツの検証を強化することがあげられている [1]．しかしながら，大小さまざまな事業者が相互に接続している複雑な環境 [2] において，攻撃手法も巧妙になっている状況では，上記の取り組みで Malvertising を完全に撲滅することは困難である．

そこで本稿では，新たにセキュアな広告プラットフォームを構築し，その広告プラットフォームでは正当な広告のみが配信される仕組みを提案する．具体的には，広告配信に公開鍵暗号方式による電子署名・検証のプロトコルを導入する．まず認証事業者として **TTP（Trusted Tag**

[1] セコム株式会社 IS 研究所
Intelligent Systems Laboratory, SECOM CO., LTD.

Provider）を仮定し，TTP が全ての広告配信情報（リダイレクト先や広告コンテンツ）について事前に電子署名を付与して，広告配信時に TTP のタグ（iframe タグと JavaScript）がユーザ端末上で署名検証を行う．これにより，外部からの不正侵入によって正規の広告配信情報をマルウェア配信情報に改ざんされていないことを保証する．さらに，TTP と広告事業者がトラストフレームワークを構築することによって，悪意のある広告事業者や広告主が広告プラットフォームで活動できない状態を維持する．

本稿の取組みは，TTP のタグが導入されている Web サイトでは，ユーザはそのタグからの広告に関して安全に利用できることを意味している．例えば，情報セキュリティに詳しくないユーザであっても，自主的なセキュリティ強化を行うことなく高いセキュリティを得られる可能性がある．

本稿の構成は下記の通りである．2 節では広告プラットフォームについて説明し，対象とする広告プラットフォームのモデルを明確にする．3 節では，Malvertising の動向および攻撃手法と現状の対策について説明する．4 節では，提案する広告配信方式について説明する．5 節では，提案方式を技術要素としたトラストフレームワークについて説明する．6 節では，提案するセキュア広告プラットフォームについて考察し，その実現性を述べる．7 節では関連研究を紹介し，8 節でまとめとする．

2. 広告プラットフォーム

ニュースやブログサイト等を運営している**媒体（Publisher）**は，広告タグを自身のサイトに設置し，広告を表示することで収益を得ている．媒体は自身のサイトに広告タグを設置する際に，**SSP（Supply Side Platform）**の広告事業者に広告タグの申請を行う．SSP 事業者は各媒体サイトの広告枠を取得・管理しており，広告枠の需要と供給（どのような媒体サイトおよび閲覧ユーザに価値があるか）の調整を行っている．また，インターネット広告を出したい**広告主（Advertiser）**は **DSP（Demand Side Platform）**の広告事業者に広告の入稿を行う．DSP 事業者は広告コンテンツと共に，広告の単価（表示単価やクリック単価），ターゲット層を管理しており，広告の需要と供給を調整している．DSP 事業者は一般に広告コンテンツの送信に **CDN（Contents Delivery Network）**を利用する場合がある．

現在の広告配信では，広告事業者が Cookie を利用してユーザをトラッキングし，Cookie にユーザの閲覧履歴等を紐付けることによって，行動ターゲティング広告を配信している．さらに，広告事業者同士が Cookie Sync[3] と呼ばれる手法によって，閲覧ユーザの Cookie 情報を共有し，閲覧ユーザの属性の共有を実現している．また，ユーザが媒体サイトを閲覧し，広告枠が表示される際には，リアルタイムに広告価格を決定して広告を表示している．これは **RTB（Real Time Bidding）**と呼ばれ，広告枠を管理している SSP 事業者と広告を管理している DSP 事業者の間において，広告枠及び閲覧ユーザ属性に最適な価格の広告を自動的に選択する手法である．例えば，SSP 事業者は複数の DSP 事業者へ RTB リクエスト送り，最高値を提示した DSP の広告を配信するという仕組みである．

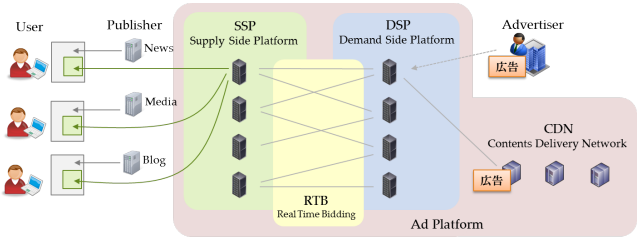

図 1 広告プラットフォーム

本稿では，SSP，DSP，CDN の広告事業者および RTB による広告配信を**広告プラットフォーム**として定義し，図 1 に示す．また，SSP，DSP，CDN の実サーバを**広告配信サーバ**，広告配信のために必要なリダイレクト先 URL や広告コンテンツ（PNG 等）を**広告配信情報**と定義する．

3. Malvertising

本節では，Malvertising の動向と攻撃方法の分類，および Malvertising 対策として喚起されている事柄を紹介し，本稿で提案する方式のモチベーションを述べる．

3.1 Malvertising の動向と攻撃種別

近年の Malvertising の動向を紹介する．2016 年 3 月 13 日から数日間，大手広告事業者の AppNexus の広告配信サーバが悪用され，AppNexus の広告配信を通じて大手ニュースサイト等の閲覧ユーザ数万人がマルウェアの脅威にさらされたと報告されている [4]．また，2015 年 1 月 3 日の大手ニュースサイト Huffington Post における AOL Ad-Network からのマルウェア発生事例では，配信時に HTTPS のドメインを経由するという巧妙な手法がとられている [5]．

日本においても，2010 年 9 月 24 日に広告事業者の MicroAd が，広告配信サーバが攻撃されることによってマルウェアが配信されたという報告をしている [6]．また，2014 年 6 月 19 日には MicroAd と連携している Yahoo! AdExchange からマルウェアが配信されたと報告している [7]．

上記のような動向から，Malvertising は短い期間に多くのユーザに影響を与え，手法が巧妙になっている．さらに事例から Malvertising には 2 種類の攻撃タイプが存在していると考えられる．

不正侵入型

攻撃者が，外部から広告事業者の脆弱な広告配信サーバに不正侵入して，正規の広告配信情報を改ざんし，攻撃サーバへアクセスさせマルウェアを配信する．

詐欺型

悪意のある広告主がマルウェアを正当な広告に偽造して入稿する．または悪意のある広告事業者が，正当な広告事業者を偽って広告プラットフォームに参加し，マルウェアを配信する．

3.2 Malvertising 対策

前節で示したように，Malvertising は不正侵入型と詐欺型の大きく 2 つに分類できる．Malvertising を防止するためには，その両方の対策に取り組む必要がある．

既存の Malvertising 対策としてあげられている内容 [1][8][9][10][11] から，ここではクライアント側とプラットフォーム側に分類して，対策を紹介する．

クライアント側対策

ユーザが，自身の端末にソフトウェアを導入することによって，広告配信の挙動（リダイレクトパスなど）や実行される JavaScript，広告画像を検査して，Malvertising を検知する方法である．例えば，下記のような対策例があげられている [1][8][9].

- ウィルス対策ソフト
- 広告ブロッキングツール（Adblock Plus 等）

この手法はマルウェア配信に至る過程を端末上で自動的に検知するため，不正侵入型と詐欺型の両方に効果があるが，手法の巧妙化やゼロデイ攻撃などから，Malvertising を 100%検出できるものではない．また，ユーザ自身で対策が必要なため，全てのユーザが十分なセキュリティ対策を導入できない可能性がある．

プラットフォーム側対策（自主的）

広告事業者それぞれが広告配信サーバのセキュリティを強化し，怪しい広告配信の挙動をフィルタリングする．また，接続先の広告事業者が正当な事業者かどうか，広告を入稿する広告主が正当かどうか，広告コンテンツは安全かどうかなどのチェックを行う．

例えば，下記のような対策があげられている [1][9][10][11].

- 脆弱性対策
- フィルタリング
- 接続先の広告事業者および広告主のチェック

この対策は，広告事業者の技術面と運用面において，不正侵入型と詐欺型の攻撃を防ぐことを目的としており，広告プラットフォームが安全であれば，エンドユーザに特別な対策は必要ない．しかし，広告プラットフォームは多数の事業者が相互に接続し，RTB 等により活発な広告配信を行うことで市場を活性化している側面がある．現状，大小さまざまな広告事業者が相互に接続している環境 [2] で，全ての広告事業者が上記のセキュリティ強化に十分に取り組むとは言い難い．例えば，セキュリティ強化に積極的な SSP であっても，セキュリティ強化に消極的な DSP と接続している場合があり，マルウェア配信に加担してしまう可能性がある [*1]．また，Web サイト 1 つにおいても，そこでの広告配信に関与する全ての広告事業者が十分なセキュリティ強化に取り組んでいる保証はない．

3.3 本稿での提案

本稿では，広告プラットフォーム側の対策として，ある種強制的にセキュアな広告プラットフォームを構築する手法を提案する．まず，認証事業者と電子署名・検証のプロトコルを導入して，不正侵入型に耐性のある広告配信方式を提案する．次に，認証事業者と広告事業者がトラストフレームワークを構築することにより，詐欺型への耐性も維持できるセキュア広告プラットフォームを提案する．

提案するセキュア広告プラットフォームの枠組みでは Malvertising に高い耐性を維持できるものになり，そこから配信される広告は安全であると保証される．また，ユーザは自主的なセキュリティ対策を行うことなく，Web 閲覧時にその広告配信に関して高いセキュリティを享受できる．

以降 4 節では，提案する広告配信方式について説明し，5 節では，トラストフレームワークに基づくセキュア広告プラットフォームについて説明する．

4. 提案方式

本節では，認証事業者と署名・検証プロトコルを導入した不正侵入型の Malvertising に耐性のある方式を説明する．

4.1 プレーヤーと役割

不正侵入型への対策を説明する前に，想定するプレーヤーと役割について説明する．

認証事業者：TTP

本稿では新たに認証事業者として TTP（Trusted Tag Provider）の存在を仮定する．TTP は正当な事業者であり，外部からの攻撃を成功させない．さらに自身が生成した暗号鍵等の秘密情報を適切に管理し，漏洩しないものとする．TTP は広告事業者の広告配信情報に署名を実施し，さらに署名検証ができる広告タグを提供して広告配信時にユーザの端末上で署名検証を行う．

広告事業者：SSP，DSP，CDN

本節では SSP，DSP，CDN は正当な事業者と仮定する．ただし，外部からの攻撃によって広告配信サーバ等に不正侵入される可能性があるとする．SSP と DSP は RTB による広告配信を行う．広告事業者は TTP から発行さ

[*1] いわゆる経済学（情報セキュリティ経済学）の外部性にあたる．

れた署名付きの広告配信情報や署名検証ができる広告タグを利用する．

広告主：Advertiser

本節では，広告主は正当な事業者であり，（マルウェアではない）正しい広告を入稿すると仮定する．

媒体：Publisher

本稿では，媒体は正当な事業者であり，外部からの攻撃によって Web サーバ等に不正侵入されないと仮定する．媒体は広告事業者から提供された広告タグを自身のサイトに設置する．

ユーザ：User

本稿では，ユーザは一般的なブラウザによる媒体サイトの閲覧者であり，マルウェア対策はしていないと仮定する．

攻撃者：Adversary

本節では，攻撃者は広告プラットフォーム外から広告事業者（SSP,DSP,CDN）の広告配信サーバ等に不正侵入できると仮定する．

4.2 攻撃モデル

不正侵入型の攻撃モデルとして，下記を仮定する．

- 攻撃者は，広告事業者の広告配信サーバ等に不正侵入し，広告配信情報の書き換えを行うとする．

ここで，上記の攻撃より前に，TTP と広告事業者は，次節で提案する広告配信方式によって，媒体サイトに広告を配信できる状態にあるとする．

4.3 提案する広告配信方式

前節の攻撃モデルによる攻撃を防止するための具体的な広告配信方式を説明する．

4.3.1 署名鍵生成

TTP は署名と署名検証のための非対称鍵ペアを生成する．

$\texttt{GenerateKey}() \rightarrow (\mathrm{PK}, \mathrm{SK})$

ここで，GenerateKey() は任意の暗号方式による非対称鍵ペア生成機能であり，PK は検証用公開鍵，SK は署名用秘密鍵である．暗号方式に関しては，暗号文から平文の取得が計算量的に困難と証明されている方式を利用する．

4.3.2 署名実施

SSP や DSP は TTP に対して広告配信情報の署名要求を行う．TTP は署名要求に対して SK を用いて署名を実施し，署名情報を返す．

$\texttt{Sign}_{\mathrm{JWS}}(\mathrm{SK}, M) \rightarrow \alpha$

ここで，$\texttt{Sign}_{\mathrm{JWS}}()$ は JWS（JSON Web Signature: RFC7515[12]）形式の署名情報 α を出力する機能である．入力 SK は GenerateKey() で生成した署名用秘密鍵である．入力 M は，JWS で規定されている JSON 形式の値であり，下記のように JWS Header と JWS Payload によって構成されている．

```
JWS Header
 {“alg”:“RS256”}
JWS Payload (R_Sign)
 {“url”:“http://ads.dsp01.com”}
```

JWS Header は TTP が定義する．“alg”は GenerateKey() で利用した暗号方式に該当し，かつ JWA（JSON Web Algorithms: RFC7518[13]）で規定されている値を設定する．JWS Payload は広告配信情報の署名要求 R_{Sign} に相当する．

4.3.3 広告タグ生成

SSP は TTP に対して広告タグの発行要求を行う．TTP は発行要求に対して広告タグを返す．

$\texttt{GenerateTag}(R_{\mathrm{Tag}}) \rightarrow \tau$

ここで，GenerateTag() は発行要求 R_{Tag} を入力に，下記のような広告タグ τ を発行する機能である．

```
<script>
 var adtag_id=“ad123456”;
</script>
<script src=“https://ads.ttp.com/ttp.js”></script>
```

発行要求 R_{Tag} は SSP の広告配信サーバや Publisher の広告タグ設置ページの URL 情報と，広告パラメータ情報（広告のサイズ等）を含む HTTP リクエストパラメータとする．広告タグ τ の adtag_id は発行要求 R_{Tag} を識別するために付与される識別子である．SSP は発行された τ を Publisher に提供する．

4.3.4 署名検証

ユーザ端末で広告タグ τ が実行されたとき，TTP の iframe（TTP オリジン）を作成し，TTP に署名検証要求を adtag_id の値を含んで発行する．TTP は adtag_id をもとに発行要求 R_{Tag} の SSP や Publisher ページを判定し，検証用公開鍵 PK と署名検証スクリプト verify.js を TTP の iframe 内に返す．上記の処理は，下記のような HTTP リクエストとレスポンスの例になる．

```
HTTP リクエスト（TTP iframe からの署名検証要求）
 GET https://ads.ttp.com/frame?adtag_id=ad123456
HTTP レスポンス
 <script>var pk=PK;</script>
 <script src=“https://ads.ttp.com/verify.js”></script>
```

また，署名検証スクリプトは XML HTTP Request（XHR）を用いて HTTP リクエストを実行する．まずは，SSP の広告配信サーバへのリダイレクトを実行し，以降 SSP や DSP から送られる署名情報 α を検証する [*2]．

$\texttt{Verify}_{\mathrm{JWS}}(\mathrm{PK}, \alpha) \rightarrow \mathrm{true/false}$

[*2] SSP や DSP は TTP に対して Cross-Origin Resource Sharing を許可しなければならないが，この方式において SSP や DSP は

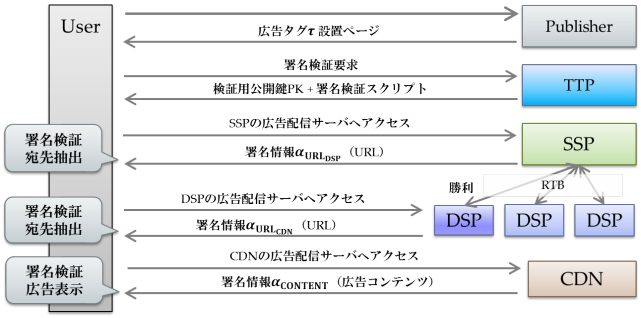

図 2　広告配信フロー

ここで，$\mathtt{Verify}_{\mathrm{JWS}}()$ は，署名検証スクリプトにおける検証用公開鍵 PK を用いた署名情報 α（JWS 形式）の署名検証機能であり，成功または失敗を出力する．署名検証スクリプトは α の検証に成功すると，JWS Payload から URL 情報や広告コンテンツを取り出し，処理を実行する．α の検証に失敗すると，警告表示等の任意の例外処理に切り替える．

4.3.5　広告配信

2 節で示した広告プラットフォームをもとに，提案方式による広告配信の流れを図 2 に示す．ユーザは媒体サイト（Publisher）にアクセスすると，広告タグ τ を含むページがロードされる．広告タグ τ が TTP オリジンの iframe を生成し実行すると，TTP から PK と署名検証スクリプトをロードする．署名検証スクリプトがまず SSP の広告配信サーバへアクセスすると，SSP は DSP 間で RTB を実施する．RTB に勝利した DSP は SSP へ自身の広告配信サーバ URL に対する署名情報 $\alpha_{\mathrm{URL_{DSP}}}$ を SSP へ返し，SSP は $\alpha_{\mathrm{URL_{DSP}}}$ を署名検証スクリプトへ返す．署名検証スクリプトは $\alpha_{\mathrm{URL_{DSP}}}$ を検証し，改ざんがないことを確認すると，そこに含まれる DSP の広告配信サーバ URL にアクセスする．DSP は広告コンテンツが設置された CDN の広告配信サーバ URL に対する署名情報 $\alpha_{\mathrm{URL_{CDN}}}$ を返し，署名検証スクリプトは $\alpha_{\mathrm{URL_{CDN}}}$ を検証して改ざんがなければ内部の URL にアクセスする．最終的に CDN から送られる署名情報 $\alpha_{\mathrm{CONTENT}}$ が改ざんされていなければ，広告コンテンツを表示する．

以上の過程で 1 回でも署名検証に失敗した場合，その時点で広告配信処理を中断し，例外処理に切り替えることで，不正侵入型の攻撃によって書き換えられた広告配信情報によるマルウェア感染を未然に防止することができる．

5.　トラストフレームワーク

4 節では，不正侵入型の Malvertising に耐性のある広告配信方式を提案した．本節では，4 節の提案方式を基礎としてトラストフレームワークを構築することにより，詐欺型の Malvertising を防止する枠組みを説明する．

事前に TTP から署名を発行されているため，TTP を信頼するのは自然な流れである．

5.1　プレーヤーと役割

詐欺型への対策のため，4.1 節で想定したプレーヤーと役割を下記についてのみ変更する．

広告事業者：SSP,DSP,CDN

SSP，DSP，CDN は正当な事業者を偽った不正な事業者の可能性がある．

広告主：Advertiser

広告主は正当な事業者を偽った不正な事業者の可能性がある．

攻撃者：Adversary

攻撃者は広告事業者または広告主の可能性がある．新規に広告事業者または広告主を偽って広告配信に関わる，または既存の事業者がある時点で不正な広告配信を行うと仮定する．

5.2　攻撃モデル

前節で変更した役割において，下記のように詐欺型の攻撃モデルを仮定する．

- 攻撃者が広告事業者であれば，自身の広告配信サーバを利用または経由してマルウェアを配信するための署名要求を認証事業者に対し行う．
- 攻撃者が広告主であれば，正当な広告と偽ってマルウェアを広告事業者に入稿する．

ここで，認証事業者と広告事業者は，提案方式に対応した広告配信を行っていると仮定する．

5.3　トラストフレームワークのモデル

ID 連携では，Open Identity Trust Framework（OITF）モデル [14] と呼ばれるトラストフレームワークモデルが普及しており，国内では学認 [15] などが採用している．OITF モデルでは，TFP（Trust Framework Provider）と呼ばれる機関を設置し，IdP（Identity Provider）および SP（Service Provider）が遵守すべき技術・運用要件などを規定する．TFP が従う上位の制度や規格を策定する人または組織を Policy Maker と呼ぶ．また，TFP は IdP および SP が規定する各種規準を継続的に遵守していることを確認するため，査定人/監査人（Assessor/Auditor）を認定し，査定や監査を行う．

TFP は Policy Maker のポリシーを参照し，下記のようなドキュメントスイートを IdP，SP に対して策定する [16]．

- 契約関係規程
  IdP と SP の要件や債務，免責等についての規程であり，後述の規程の上位文書である．
- 保証レベル規準
  提供する認証結果の信頼性を保証するための規準であり，いくつかの評価軸にもとづいて保証レベルを規定する．
- 技術・運用規準

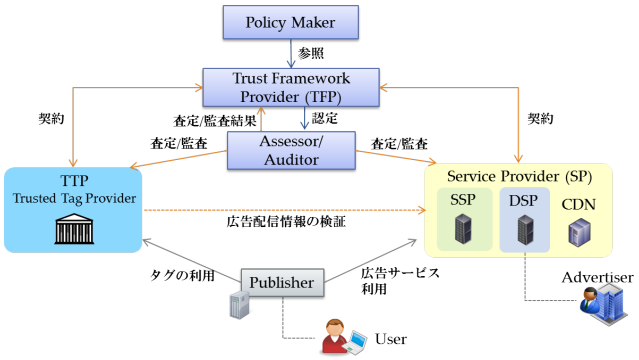

図 3　提案するトラストフレームワーク

上記で決定した保証レベルを保証するために遵守すべき各種技術・運用要件について規定する．

- プロファイルセット
  IdP と SP の相互運用性確保のために利用される認証方式である．
- 査定/監査規準
  IdP や SP を査定/監査するための査定/監査要件や査定人/監査人の資格などについて規定する．

5.4　提案方式におけるトラストフレームワークの構築

図 3 は OITF モデルと提案方式を基礎として構築したトラストフレームワークである．提案方式では，Publisher は SSP に広告掲載の申込を行い，SP（SSP，DSP，CDN 等の広告事業者）による広告サービスを利用する際に，Malvertising 対策を実施している TTP を信頼して，TTP の広告タグを導入するという関係になる．TFP は，前節で示したようなドキュメントスイートを TTP，SP に対して策定することになり，TTP，SP がドキュメントスイートを継続的に遵守していることを TFP が確認することで，5.2 節で仮定した攻撃の対策を行う．

まず，プロファイルセットは本稿での提案方式とする．詐欺型の攻撃モデルの対策となる各種規準と実施について説明する．

攻撃者が広告事業者

TFP は TTP，SP のトラストフレームワーク加入時の契約において，TTP，SP が不正な事業者でないことを確認するため，監査人を利用して実在性等の身元や運用実績を厳しく監査する．またプロファイルセット（提案方式）を実施する際に，TTP や SP の作業担当者が不正な署名要求を行うかもしれないため，TFP は TTP，SP に対し，内部不正が発生しないよう技術・運用規準を規定し，査定人を利用して規準を遵守しているかどうかを継続的に査定する必要がある．例えば，TTP としては，SP からの要求である広告タグ発行要求や署名要求のコードの検証，SP としては，広告タグ発行要求や署名要求実施者のアクセス制御等があげられる．

攻撃者が広告主

TFP は SP（DSP）の保証レベルとして広告主の身元確認レベルを規定し，技術・運用規程によって SP が保証レベルを遵守しているかどうか，査定人による継続的な査定を実施する必要がある．また TFP は SP（DSP）に対し，広告主からの広告入稿（広告コンテンツ等）に対するマルウェア検知等の規準を規定し，SP に準拠させる．

以上により，悪意のある広告事業者または広告主が，新たにトラストフレームワークに加入すること，トラストフレームワーク内で広告事業者または広告主の悪意ある担当者が活動することを防止し，攻撃モデルのような詐欺型の Malvertising を抑制する．提案方式をもとに構築したトラストフレームワークは，不正侵入型の Malvertising だけでなく，詐欺型の Malvertising にも耐性がある強固なセキュア広告プラットフォームとなる．

6.　考察

本節では，4 節で示した提案方式や 5 節で示したトラストフレームワークについて考察を行い，提案するセキュア広告プラットフォームの実現性について述べる．

6.1　提案方式について

6.1.1　広告配信情報の構造

4.3.4 節において，署名検証スクリプトは署名情報 α の検証に成功すると，広告配信情報の署名要求 R_{Sign}（JWS Payload）を取り出し，処理を行う．この JSON の構造と処理については事前に TTP のポリシーまたは，標準化等で規定しておけばよいと考えられる．例えば，JSON の name が “img-png” なら value の “fjai4t0gha9efnja...” の Base64 PNG をデコードして表示することを規定しておく．TTP が発行する署名検証スクリプトが，広告事業者の広告配信時に想定する様々な処理について対応していれば，TTP 管理のもとで広告事業者は柔軟な広告配信が実現できると考えられる [*3]．

6.1.2　ユーザのターゲティング方法

現在の広告プラットフォームでは Cookie Sync[3] によって，ユーザの Cookie 情報を共有し，行動ターゲティング広告を配信している．提案方式について，ユーザのトラッキングを実現させるには下記の方法が想定される．

(1) TTP が発行する ID で一元管理
(2) SSP や DSP が広告配信情報の中に Cookie 情報を含めて管理

上記 1 に関しては，4.3.4 節の署名検証要求に対するレスポンス Header に，TTP のユーザ ID を “Set-Cookie” で返し，署名検証スクリプトの URL アクセス時にユーザ ID を

[*3] 当然ながら処理によってセキュリティホールを作らないようにする必要はある．

パラメータで送ることで，ユーザ ID を広告配信に係わった事業者で共有することができる．さらに，広告事業者がユーザ ID を TTP に問い合わせることができれば，閲覧ユーザの属性をもとに RTB の実施と行動ターゲティング広告の配信が可能となる．

また上記 2 に関しては，例えば 4.3.5 節で示した署名情報 $\alpha_{\mathrm{URL_{CDN}}}$ の広告配信情報について，JSON の name に “cookie”，value に “Cookie の name” を指定し，署名検証スクリプトがパラメータで Cookie 値を送ることを規定すれば，TTP に依存しないユーザへのターゲティングが可能であると考えられる．さらに Cookie Sync が必要な場合は下記のように構成し，Cookie 情報をパラメータとして各事業者に送信すればよいと考えられる．

```
{“url”:“http://ads.cdn01.com?content=1”,
 “cookie”:“dsp01_user_id”,
 “sync”:[“http://ads.dsp02.com”,
         “http://ads.dsp03.com”]}
```

その他には，ユーザ自身がトラッキングのための ID を発行し，ユーザ自身で管理する方法も考えられる [17]．

6.2 トラストフレームワークについて

TFP が規定する SP（DSP）の広告主の身元確認レベルとして，サーバ証明書発行時の身元確認レベル [18] を利用できる可能性がある．例えば，EV（Extended Validation）証明書等の発行に係る身元確認である．EV 証明書はサーバ運営組織の実在性等の確認やドメイン名と運営組織との関係についても確認した上で発行される．このように，広告主の実在性・法人性を確認することで，i) 名称と実態が乖離している広告主を排除できる (実在性確認)，ii) 万一の係争時に迅速に対応できる (法人性確認) などの効果が期待できる．

また，広告コンテンツの質やユーザのトラッキングポリシーについて，現在では広告業界団体がガイドライン等 [19] を発行しているが，TFP がその内容を規程として取り入れて，継続的に TTP や SP に遵守させることができれば，さらに健全な広告配信が実現できる可能性がある．

6.3 セキュア広告プラットフォームの実現性

はじめに，セキュア広告プラットフォームでの新たなプレーヤーについて考察する．TTP の具体的なプレーヤーとしてはサーバ証明書を発行する認証局や，コード署名を実施している事業者等が考えられる．Policy Maker はユーザの消費者団体および広告主の企業団体等が担当し，TFP は広告業界団体および認証事業者が担当することで，最終的に広告を利用するユーザや広告主のポリシーのもと，中立的なトラストフレームワークの運用が実現すると考えられる．また，査定人/監査人は情報セキュリティ監査等を実施している事業者が考えられる．上記のように新たなプレーヤーにとっては新たなビジネス領域と捉えることができる．

次に，既存のプレーヤーについて考察する．広告事業者，広告主にとっても，セキュア広告プラットフォームからの広告配信は広告にセキュリティの付加価値がある新たな広告商材と捉えることができる．媒体にとっては，自身のサイト閲覧ユーザを Malvertising の脅威から保護できるため [*4]，媒体がこの新たな広告商材を選ぶ需要は高いと考えられる．そうなれば，広告事業者にとっては提案方式や TFP の規程に対応するコストはかかるとしても，この新たな広告商材を導入する動機付けになると考えられる．

以上のようにセキュア広告プラットフォームには一定の実現性があると考察できる．ただし，各プレーヤーの金銭的なインセンティブや運用コストの原資等に関しては，より詳細な分析が必要である．

ユーザに関しては，媒体のセキュア広告プラットフォームの利用によって，そのサイトの広告配信については自主的にセキュリティ対策を行うことなく安全に利用できる．なお，ユーザにとっては全ての媒体サイトの広告について安全を得られるわけではない．例えば，ユーザ端末にセキュア広告プラットフォームからの広告のみを受け取るようなソフトウェアを導入すれば，Zarras ら [9] の主張のように，セキュリティ対策のために全ての広告をブロックするようなツールを導入しなくてもよくなると考えられる．

7. 関連研究

本節では Malvertising を対象とした過去の研究を紹介する．Malvertising の調査として，Zarras ら [9] は，60 万もの広告を調査し，媒体サイトや広告ネットワークによる不正な広告の傾向を報告しており，対策としては広告ブロッキングツールが有効と述べている．また，Sakib ら [20] は，広告のみならず広告のランディングページまで自動収集するアプリケーションを開発し，ランディングページから送られるバイナリのマルウェアを調査している．

Malvertising の対策として，Li ら [21] は，9 万の Web サイトを 3 ヶ月にわたり観測し，観測結果のドメインに出現頻度，役割（媒体または広告など），ドメイン期限，URL(.co や.cc など）のアノテーションを付け，3 ノードのリダイレクトパスを特徴量として Malvertising 判別を行っており，誤検知率は 5%程度と報告している．Dong ら [22] は，信頼できない JavaScript をサンドボックスで実行し，オリジナルの実行環境とはポリシーで定めた内容のみをやり取りできるようにしている．また，Ter ら [23] は，媒体サイトが広告に対して厳しいポリシーを規定して広告を制御して

[*4] 実際に自身のサイトの広告からマルウェアが配信されれば，少なからずその媒体の信用も落ちるだろう．

いる．

[21][22] は，ユーザが主体的に自身の端末にソフトウェアを導入して，広告を制御することを想定しているが，[23] では，媒体が主体的に広告を制御することを想定している．

本稿の提案は，広告プラットフォーム自体をセキュアにする枠組みであり，媒体やユーザはセキュアな広告プラットフォームを信頼することで，セキュリティを享受するモデルである．

8. まとめ

本稿では，複雑化・巧妙化する Malvertising への対策を提案した．まず，提案方式として，認証事業者 TTP と電子署名・検証のプロトコルを導入することによって，不正侵入型の Malvertising に耐性のある広告配信方式を示した．次に，提案方式を技術要素としたトラストフレームワークに発展させることよって，詐欺型の Malvertising にも耐性のあるセキュア広告プラットフォームの提案を行った．本稿で提案したセキュア広告プラットフォームは一定の実現性があると考察され，ユーザにとってはその広告プラットフォームからの広告配信について，自主的なセキュリティ対策を行うことなく高いセキュリティを享受できるようになる．

本稿での提案は，セキュア広告プラットフォームを通した広告事業者の広告配信情報および広告主の広告コンテンツは，正当なものであるということを保証する枠組みである．しかし，ユーザのインターネット利用全体を考えると，媒体サイトや広告をクリックしたときに遷移する広告主のページ（ランディングページ）のセキュリティも重要な課題となる．媒体サイトやランディングページも含めた総合的なセキュリティの確保は今後の課題とする．また，提案方式のオーバーヘッド等の評価，提案するトラストフレームワークの詳細な設計についても今後の課題とする．

参考文献

[1] Cyphort: The Rise of Malvertising, http://go.cyphort.com/Malvertising-Report-15-Page.html (2015). (accessed 2016-08-12).

[2] LUMA Partners: LUMAscapes, http://www.lumapartners.com/resource-center/lumascapes-2/ (2016). (accessed 2016-08-12).

[3] Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A. and Diaz, C.: The Web never forgets: Persistent tracking mechanisms in the wild, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp. 674–689 (2014).

[4] Trustwave: Angler Takes Malvertising to New Heights, https://www.trustwave.com/Resources/SpiderLabs-Blog/Angler-Takes-Malvertising-to-New-Heights/ (2016). (accessed 2016-08-12).

[5] Cyphort: HuffingtonPost Serving Malware via AOL Ad-Network, https://www.cyphort.com/huffingtonpost-serving-malware/ (2015). (accessed 2016-08-12).

[6] MicroAd: 【障害報告】弊社サービスの改ざんに関するお詫びと報告，http://www.microad.co.jp/news/information/detail.php?newid=News-0118 (2010). (accessed 2016-08-12).

[7] MicroAd: 広告配信障害に関するプレスリリースの追記に関して，https://www.microad.co.jp/news/detail.php?News_ID=252 (2014). (accessed 2016-08-12).

[8] TrendLabs: 米国で大規模な不正広告攻撃、大手ニュースサイト等の汚染を確認，http://blog.trendmicro.co.jp/archives/13063 (2016). (accessed 2016-08-12).

[9] Zarras, A., Kapravelos, A., Stringhini, G., Holz, T., Kruegel, C. and Vigna, G.: The dark alleys of madison avenue: Understanding malicious advertisements, *Proceedings of the 2014 Conference on Internet Measurement Conference*, ACM, pp. 373–380 (2014).

[10] TrustInAds.org: TrustInAds.org - Keeping people safe from bad online ads, https://trustinads.org/. (accessed 2016-08-12).

[11] Google's Anti-Malvertising Team: Anti-Malvertising.com, http://www.anti-malvertising.com/. (accessed 2016-08-12).

[12] IETF: JSON Web Signature (JWS), https://tools.ietf.org/html/rfc7515. (accessed 2016-08-12).

[13] IETF: JSON Web Algorithms (JWA), https://tools.ietf.org/html/rfc7518. (accessed 2016-08-12).

[14] Rundle, M., Maler, E., Nadalin, A., Reed, D. and Thibeau, D.: The Open Identity Trust Framework (OITF) Model, http://iop.projectliberty.org/confluence/download/attachments/45059055/OITF+Trust+Model.pdf (2010). (accessed 2016-08-12).

[15] 学術認証フェデレーション：学認（GakuNin），https://www.gakunin.jp. (accessed 2016-08-12).

[16] 島岡政基，佐藤周行：学認における属性交換フレームワーク，コンピュータセキュリティシンポジウム 2013 論文集，Vol. 2013, No. 4, pp. 486–493 (2013).

[17] 坂本一仁，松永昌浩：ファーストパーティ，サードパーティを考慮した自己情報制御の提案，コンピュータセキュリティシンポジウム 2014 論文集，Vol. 2014, No. 2, pp. 627–634 (2014).

[18] CRYPTREC: SSL/TLS 暗号設定ガイドライン，http://www.cryptrec.go.jp/report/c14_oper_guideline_SSLTLS_web.pdf (2015). (accessed 2016-08-12).

[19] 日本インタラクティブ広告協会（JIAA）：JIAA ガイドライン，http://www.jiaa.org/guideline.html. (accessed 2016-08-12).

[20] Sakib, M. N. and Huang, C.-T.: Automated Collection and Analysis of Malware Disseminated via Online Advertising, *Trustcom/BigDataSE/ISPA, 2015 IEEE*, Vol. 1, IEEE, pp. 1411–1416 (2015).

[21] Li, Z., Zhang, K., Xie, Y., Yu, F. and Wang, X.: Knowing your enemy: understanding and detecting malicious web advertising, *Proceedings of the 2012 ACM conference on Computer and communications security*, ACM, pp. 674–686 (2012).

[22] Dong, X., Tran, M., Liang, Z. and Jiang, X.: AdSentry: comprehensive and flexible confinement of JavaScript-based advertisements, *Proceedings of the 27th Annual Computer Security Applications Conference*, ACM, pp. 297–306 (2011).

[23] Ter Louw, M., Ganesh, K. T. and Venkatakrishnan, V.: AdJail: Practical Enforcement of Confidentiality and Integrity Policies on Web Advertisements., *USENIX Security Symposium*, pp. 371–388 (2010).