# アプリケーションベース MapTB マーカの提案
# Application Based MapTB Marker

上野 隆資 † 安田 真悟 † 井上 朋哉 † 篠田 陽一 §
北陸先端科学技術大学院大学 情報科学研究科 † /情報科学センター §

**概要**

MapTB(Marking based APplication TraceBack) と呼ばれる、アプリケーショントレースバック手法がある。MapTB は、HTTP 通信中の HTML 文書内のハイパーリンクに MapTB マークを挿入し、そのマークをインターネット上の特定の観測点で観測することにより攻撃元を特定する技術である。MapTB において、Web サーバへの攻撃者を追跡対象とするには、MapTB マーカを Web サーバのリバースプロクシとして設置しなければならない。そのため、MapTB マーカを配置するための設計や、MapTB マーカのハードウェアを準備する必要があるため導入および管理コストが高くなる。また、MapTB マーカをリバースプロクシとして設置することは、処理負荷が大きいなどの問題がある。

本稿では、MapTB マーカの機能を Web サーバマシン上へ移行させた、アプリケーションベース MapTB マーカの提案を行う。これにより、MapTB マーカの導入および管理コストの低下、および、MapTB マーカを動作させるために必要な処理負荷の低減を可能にする。

## 1 はじめに

Web サービスは、社会生活の中で必要不可欠なものになってきた。そのため、Web サービスに対する不正アクセスなどの攻撃や、電子掲示板やブログへの不適切な書き込みなどが問題となっている。これらの攻撃や書き込みに対して、Web サービスの管理者が対策を行ったとしても完全に防ぐことは難しい。そこで、Web サービスに対して不正な行為を行った者を追跡するトレースバック技術が必要不可欠となる。

トレースバック技術には、IP トレースバック技術 [1] とアプリケーショントレースバック技術などがある。攻撃者が、Web サービスに対して攻撃および不適切な書き込みを行う場合、身元を隠すためにプロクシサーバを利用することが多い。

IP トレースバック技術は、ネットワーク層の情報を利用してトレースバックを行う。しかし、プロクシサーバを経由した場合にネットワーク層の情報は変わるため有効に機能しない。

アプリケーショントレースバック技術は、アプリケーション層の情報を利用して攻撃者を追跡する技術である。そのため、プロクシサーバを経由しても情報は変わらない。アプリケーション層の情報を利用することで、プロクシサーバを経由して攻撃する攻撃者を追跡することが可能になる。

アプリケーショントレースバックには、パッシブ検査手法とアクティブ検査手法がある。既存研究としてパッシブ検査手法に thumbprinting [2]、timing thumbprinting [3, 4] などや、アクティブ検査手法に Sleepy watermark tracing [5] などがある。これらの研究は、Web サービス向けに考案されていないため、Web サービスにとってスケーラビィリティに乏しかったり、HTTP 通信に向いていないなど Web サービスに適応するには向いていない。

アクティブ検査手法に分類され、Web サービスに特化したアプリケーショントレースバック手法として MapTB(Marking based APplication TraceBack) [6–8] がある。MapTB は、HTML 文

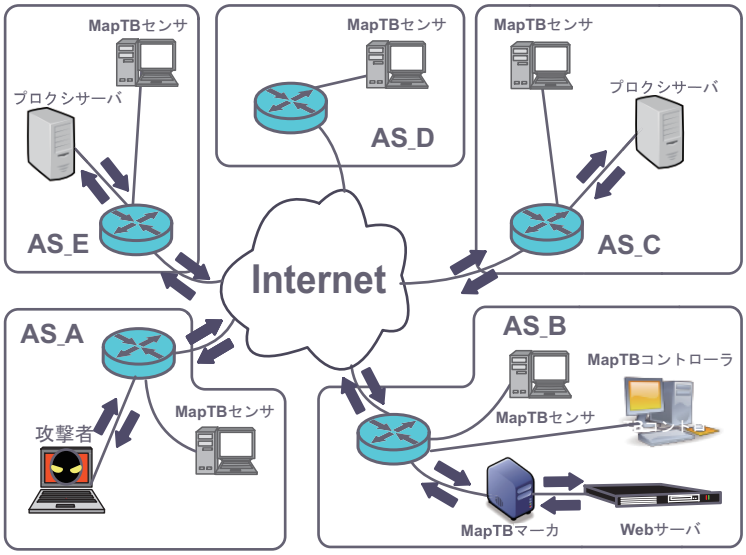


図 1　MapTB システム

書内のハイパーリンクに MapTB マークを挿入する。そのマークをインターネット上の特定の場所で観測することにより攻撃元を特定する技術である。MapTB システムの構成要素に、リバースプロクシサーバとして実装された MapTB マーカがある。

MapTB マーカを導入するには、Web サーバとは別に MapTB マーカのためのハードウェアが必要であるため導入、および管理するコストが高くなる。また、リバースプロクシとして設置することは処理負荷が大きくなる。

そこで、本稿では Web サーバと同じノードで稼動するアプリケーションベース MapTB マーカの提案を行う。これにより、MapTB マーカの導入・管理コストの低下および MapTB マーカによる処理負荷の低減を行う。

## 2　MapTB システム

MapTB システムは、MapTB マーカ、MapTB センサおよび MapTB コントローラにより構成される。

MapTB マーカは、HTTP レスポンス中の HTML 文書中に含まれるハイパーリンクに独自のアルゴリズムで生成されたユニークな MapTB マークを挿入する。一方で、ネットワーク上に配置された MapTB センサにより、HTML 文章中の MapTB マークを観測および記録する。そして、MapTB コントローラにより、MapTB センサが記録した情報を集め、集約し、攻撃元のトレースバックすを行う。MapTB システムをインターネット上に配置した例を図 1 に示す。

### 2.1　MapTB マーカ

MapTB マーカは、Web サーバのリバースプロクシとして設置される。MapTB マーカは、HTTP レスポンス中に含まれる MapTB マークの挿入や、HTTP リクエストに含まれる MapTB マークの削除を行う。また、MapTB マーカは、HTTP リクエストに含まれる MapTB マークなどによりアクセス制御を行う。

### 2.2　MapTB センサ

MapTB センサは、ネットワーク上の特定の地点に設置され MapTB マークの観測および記録を行う。

MapTB センサを設置する場所として、Intertnet Service Provider(ISP) や Internet eXchage(IX) など、より多くのトラフィックが観測できる地点が向いている。MapTB センサは、攻撃者が利用する多段プロクシ間を観測するように最適に設置する必要がある。

MapTB センサは、オーバレイネットワークを構築し、MapTB コントローラからのトレースバッククエリを全ての MapTB センサに効率的にブロードキャストする。

### 2.3 MapTB コントローラ

MapTB コントローラは、MapTB センサに対してトレースバッククエリを発行し、MapTB センサからトレースバック情報を受信する。MapTB コントローラは、そのトレースバック情報を集約して、追跡結果の表示を行う。

### 2.4 MapTB の特徴

従来のアクティブ検査手法では、攻撃者から被害者への一方向の通信のみにマークを付加し、そのマークを通信経路上で観測することにより攻撃元を特定していた。一方、MapTB は、攻撃者と被害者間の双方向の通信で MapTB マークを付加することが可能である。そのため、攻撃者と被害者の双方向において攻撃者をトレースバックが可能となる。

また、Web サービスにおいて攻撃や不適切な書き込みを行う場合、プロクシサーバを利用して身元を隠そうとすることが多い。そのような状況においても、アプリケーション層の情報を使用しているので、プロクシサーバを越えて攻撃元の追跡が可能である。

## 3 MapTB マーカの課題

前章で述べた MapTB マーカにはいくつかの課題が存在する。以下の 2 つの課題を述べる。

- MapTB マーカの導入および管理コスト
- MapTB マーカの処理負荷

### 3.1 MapTB マーカの導入および管理コスト

MapTB マーカを導入するためには、Web サーバだけで運用する場合に比べ、MapTB マーカをリバースプロクシとして稼動させるためのハードウェアが必要になる。そのため、設計が複雑になったり、ハードウェアを導入するための導入コストが高くなる。

また、Web サーバへの中継ノードである MapTB マーカが機能しなくなると、Web サービスも機能しなくなる。MapTB マーカが故障したときにハードウェアの交換が必要になる。また、Web サーバへのアクセス数が増えると、処理しなければならない負荷が増えるため、Web サーバマシンだけでなく、MapTB マーカの数も増やす必要がある。そのため、MapTB マーカを管理するためのコストは高くなる。

### 3.2 MapTB マーカの処理負荷

一般に、プロクシサーバは、Web サーバよりも処理負荷が大きい。その原因は、プロクシサーバは、Web サーバと比べてコネクション数が倍になるなど理由がある。従って、MapTB マーカを、リバースプロクシとして導入するには、Web サーバよりも高性能なハードウェアを設置しなければならない。

## 4 アプリケーションベース MapTB マーカの提案

本章では、3 章で述べた問題点を解決するためにアプリケーションベース MapTB マーカの提案を行う。本稿では、MapTB マーカのプロトタイプ実装 [8] を、リバースプロクシ型 MapTB マーカと呼ぶ。

アプリケーションベース MapTB マーカは、Web サーバマシン上で稼動する MapTB マーカの機能を備えたソフトウェアである。MapTB マーカの機能をリバースプロクシから Web サーバに移行させることで、MapTB マーカの導入や管理コストを下げると同時に、処理負荷の低減を可能にする。

### 4.1 導入および管理コストの低下

アプリケーションベース MapTB マーカは、リバースプロクシ用のハードウェアが減るため導入および管理コストが低下する。

### 4.2 処理負荷の軽減

アプリケーションベース MapTB マーカは、リバースプロクシ型 MapTB マーカを稼動させた場合に必要であったコネクション数を、半分に減らすことができる。そのため、MapTB マーカが稼動するために必要な処理負荷が軽減する。

表 1　既存研究および提案研究における MapTB マーカの比較

| | 導入および管理コスト | 処理負荷 | 既存の Web コンテンツへの対応 | Web サーバマシンへの変更 |
|---|---|---|---|---|
| プロクシ型 MapTB マーカ | 高い | 重い | 容易 | 不要 |
| Web サーバ型 MapTB マーカ | 低い | 軽い | 容易 | 必要 |
| Web アプリケーション型 MapTB マーカ | 低い | 軽い | 難しい | 必要 |

### 4.3 モジュール形式での導入

リバースプロクシ型 MapTB マーカが、リバースプロクシ型として実装されている理由は、Web サーバに対して一切手を加えることなく設置するためである。アプリケーションベース MapTB マーカにおいても、モジュール形式で導入を行うことにより Web サーバソフトウェアにできるだけ手を加えずに導入を行う。

## 5 アプリケーションベース MapTB マーカの実現方法

導入形式の多様化を行うために、リバースプロクシ型 MapTB マーカ以外に、導入形態の違う 2 種のアプリケーションベース MapTB マーカの検討を行う。以下にその 2 つを示す。

- Web サーバ型 MapTB マーカ
- Web アプリケーション型 MapTB マーカ

### 5.1 Web サーバ型 MapTB マーカ

Web サーバ型 MapTB マーカとは、Web サーバソフトウェアに MapTB マーカの機能を組み込んだソフトウェアである。

Web サーバ型 MapTB マーカのプロトタイプとして、Web サーバのデファクトスタンダードである Apache [9] のモジュールに MapTB マーカの機能を組み込む。Apache の outputfilter および inputfilter 機能を利用し、HTTP 通信中のリクエストおよびレスポンスに、変更を加えることにより実現する。これにより、既存の Web コンテンツに変更を加えずに MapTB マークの付加、削除およびアクセス制御などが可能となる。

### 5.2 Web アプリケーション型 MapTB マーカ

Web アプリケーション型 MapTB マーカは、wiki、ブログおよび電子掲示板などの Web アプリケーション上に、MapTB マーカの機能を移行したソフトウェアである。Web アプリケーション型 MapTB マーカは、Web サーバソフトウェアに依存せずに、MapTB マーカの機能を利用することができるという利点がある。

Web アプリケーション型 MapTB マーカのプロトタイプを、ブログ・ソフトウェアとして広く使われている Movable Type [10] のプラグインに、MapTB マーカの機能を組み込み実装を行う。MapTB 機能を持った Movable Type のプラグインは、HTML 文書中に MapTB マーカの機能を備えた PHP スクリプトを埋め込むことにより実現する。

## 6 MapTB マーカの比較

3 つの既存マーカと提案マーカの比較を行う。

A: リバースプロクシ型 MapTB マーカ
B: Web サーバ型 MapTB マーカ
C: Web アプリケーション型 MapTB マーカ

比較項目は下記の通りである。

- 導入および管理コスト
- 処理負荷
- Web サーバマシンへの変更の有無
- 既存 Web コンテンツへの対応の容易性

### 6.1 導入および管理コスト

リバースプロクシ型 MapTB マーカは、Web サーバマシンに加え、リバースプロクシ型 MapTB マーカを稼動させるためのハードウェアが必要になる。リバースプロクシ型 MapTB マーカの導入には、ハードウェアの数が増えるため、導入および管理コストが高くなる。

アプリケーションベース MapTB マーカは、Web サーバ上に MapTB マーカの機能を移行させたため、MapTB マーカ用のハードウェアが削減できるため、導入および管理コストは低くなる。

### 6.2 処理負荷

リバースプロクシ型 MapTB マーカは、リバースプロクシとして設置するため、Web サーバと比べて、コネクションの数が倍になるなど処理負荷は増える。しかし、アプリケーションベース MapTB マーカは、リバースプロクシ型 MapTB マーカと比べてコネクションの総数が半分になるため、リバースプロクシ型 MapTB マーカに比べて処理負荷が小さくなる。

### 6.3 Web サーバマシンへの変更の有無

リバースプロクシ型 MapTB マーカは、Web サーバに変更を加えずに導入できる。しかし、アプリケーションベース MapTB マーカを導入するためには、Web サーバに対して変更を加える必要がある。

### 6.4 既存 Web コンテンツへの対応の容易性

リバースプロクシ型 MapTB マーカおよび Web サーバ型 MapTB マーカは、HTTP 通信中のパケットに直接変更を加える。そのため、リバースプロクシ型 MapTB マーカおよび Web サーバ型 MapTB マーカは、Web サーバ上ある Web コンテンツがどういう形式であるかに依存せず、ユーザへ送信されるのが HTML 文書であればよいため、既存のコンテンツに変更を加えなくてもよい。

しかし、Web アプリケーション型 MapTB マーカは、MapTB マーカの保護対象としたい全ての Web コンテンツを PHP ファイルへ変換しなければならない。そのため、最終的に HTML を出力してユーザーに送信するような、CGI などで作成された既存の Web コンテンツに対応することが難しい。

### 6.5 考察

上記の比較結果から各 MapTB マーカの導入形態について考察を行う。

リバースプロクシ型 MapTB マーカは、導入および管理コストはかかるが、Web サーバマシンを変更したくない場合のよい選択肢になる。

一方、アプリケーションベース MapTB マーカは、導入および管理コストを下げたい場合によい選択肢となる。Web サーバ型 MapTB マーカは、Web アプリケーション型 MapTB マーカに比べて、既存の Web コンテンツへの対応のしやすさであったり、処理の量が減るなどの利点がある。Web サーバ型 MapTB マーカは、Web サーバソフトウェアに変更を加えても問題がない場合で、処理を軽くしたい場合によい選択肢となる。Web アプリケーション型 MapTB マーカは、Web サーバソフトウェアに対して変更を加えたくない場合や、加えれない状況においてよい選択肢となる。

これにより、MapTB マーカの導入形態の多様化を実現した。

## 7 今後の展望

本稿では、アプリケーションベース MapTB マーカの提案を行った。MapTB システムにも解決すべき課題は残っている。今後取り組むべき課題を述べる。

### 7.1 提案手法の設計および実装

本稿で提案を行った 2 種類のアプリケーションベース MapTB マーカをプロトタイプとして設計および実装を行う。

Web サーバ型 MapTB マーカは、Apache のモジュールとして実装を行った。Apache の output-filter および inputfilter 機能を利用している。

今後、MapTB マーカの機能を持った Movable

Type のプラグインの設計および実装を行う。

### 7.2 MapTB における HTTP 以外のプロトコルへの対応

MapTB は、HTTP 通信のみに対応している。しかし、Web サービスには、HTTP 以外にも頻繁に使用されている HTTPS や FTP などのプロトコルがある。MapTB により追跡対象となる攻撃者を増やすためには、これらのプロトコルにも対応していく必要がある。

#### 7.2.1 暗号化通信プロトコルへの対応

HTTP 通信は、パケットの中身が暗号化されていないためネットワーク上で HTML 文書中の MapTB マークを観測ができる。しかし、HTTPS 通信は、HTML 文章が暗号化されているので、ネットワーク上では MapTB マークを観測できない。暗号化通信に MapTB を対応するためには、新しい手法が必要である。

### 7.3 MapTB システムのアクセス制御

MapTB センサ上のトレースバック情報へのアクセス制御は不十分である。例えば、Web サイト A にある MapTB コントローラは、Web サイト A で生成された MapTB マークだけでなく、Web サイト B で生成された MapTB マークによるトレースバック情報も MapTB センサから取得できる。そのため、その情報が悪用される可能性がある。ある Web サイトの MapTB コントローラは、その Web サイトで生成した MapTB マークによるトレースバック情報だけ閲覧できるようにする制御が必要である。

## 8 おわりに

本稿では、MapTB システムのプロトタイプ実装 [8] の構成要素であるリバースプロクシ型 MapTB マーカに焦点を当て、リバースプロクシ型 MapTB マーカの課題をまとめた。その課題を解決するために、MapTB マーカの機能を Web サーバ上に移行したアプリケーションベース MapTB マーカの提案を行った。また、MapTB マーカの導入形式の多様化を行うために、Web サーバ型 MapTB マーカおよび Web アプリケーション型 MapTB マーカの実現方法の検討も行った。

アプリケーションベース MapTB マーカは、リバースプロクシ型 MapTB マーカよりも導入および管理コストを下げ、処理負荷を軽減する。そして、MapTB マーカ導入時の選択肢を増やした。今後、アプリケーションベース MapTB マーカの実装の作成およびその実装評価を行う。

## 謝辞

本研究において、貴重なご指導およびご助言を頂いた情報通信研究機構 (NICT) の吉岡克成氏、衛藤将史氏、新井貴之氏、中尾康二氏、ならびに北陸先端科学技術大学院大学 (JAIST) の高野 祐輝氏に感謝致します。

## 参考文献

[1] 門林雄基, 大江将史. IP トレースバック技術. 情報処理学会誌, Vol. 42, No. 12-006, 2001.

[2] S. Staniford-Chen and L. T. Helberlein. Holding intruders accountable on the internet. *Proceedings of the 1995 IEEE Symposium on Security and Privacy, Oakland, CA*, pp. 39–49, May 1995.

[3] Y. Zhang and V. Paxson. Detecting stepping stones. *In Proceedings of 9th USENIX Security Symposium*, August 2000.

[4] F. Bunchholz, T. E. Daniels, B. Kuperman, and C. Shields. Packet tracker final report. *Technical report. Purdue University*, 2000.

[5] Xinyuan Wang, Jim Yuill, Douglas S. Reeves, and S. Felix Wu. Sleepy watermark tracing: An active network-based intrusion response framework. *In Proceedings of 9th USENIX Security Symposium. North Carolina State University*, 2001.

[6] 吉岡克成, 衛藤将史, 新井貴之, 中尾康二. マーキングを用いたアプリケーショントレースバック　MapTB のセキュリティ向上に関する考察. 電子情報通信学会, Vol. 1, No. 5, pp. 29–34, 2006.

[7] 衛藤将史, 吉岡克成, 新井貴之, 門林雄基, 中尾康二. ハイパーリンクへのマーキングを用いた HTTP トレースバック手法 (MapTB) の提案. 2006 年暗号と情報セキュリティシンポジウム, 2006.

[8] 衛藤将史, 吉岡克成, 新井貴之, 中尾康二. ハイパーリンクへのマーキングを用いた HTTP トレースバック手法 (MapTB) の実装と評価. 電子情報通信学会, 2007.

[9] The Apache Software Foundation. The apache http server project. `http://www.apache.org`.

[10] Six Apart, Ltd. Blogging platforms for small businesses, enterprises & publishers at movable type. `http://www.sixapart.com/movabletype/`.