社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

URI免疫化：参加型システムにおけるスパム避けの一手法

北本　朝展†

† 国立情報学研究所 コンテンツ科学研究系
〒 101–8430 東京都千代田区一ッ橋 2–1–2
E-mail: †kitamoto@nii.ac.jp

あらまし　本論文は不特定多数を対象とする参加型システムにおいて、トラックバックスパム等のウェブスパムを防御するための手法である「URI 免疫化」を提案する。本手法は生物の免疫システムに触発されたものであり、「変化する」という生物の基本的な戦略を変化する URI に適用することで、スパム攻撃の回避に有効な手法を考案した。また筆者が運営する参加型台風情報サイトである「台風への眼」における実際のアクセス解析を分析することで、本手法の有効性を検証する。

キーワード　URI, 免疫化, 参加型システム, ウェブスパム, 可変領域

URI Immunization: Eluding Spams in Participatory Systems

Asanobu KITAMOTO†

† Digital Content and Media Sciences Research Division, National Institute of Informatics
2–1–2, Hitotsubashi, Chiyoda-ku, Tokyo, 101–8430 Japan
E-mail: †kitamoto@nii.ac.jp

Abstract　This paper proposes “URI Immunization” for eluding Web spams like Trackback spams in participatory systems open to the general public. The proposed method is inspired from the immune system of organisms, and by applying the basic strategy of organisms, “change,” on the construction of changing URIs, the author established an effective method for eluding spams. The effectiveness of the method is validated by the analysis of real accesses collected at our participatory Website, “Eyes on the Typhoon.”

Key words　URI, Immunization, Participatory System, Web Spam, Variable Region

1. まえがき

参加型システムは利用者からのコンテンツの提供によって成長するシステムであるが、このようなコンテンツの提供を受ける入口はスパムに対する弱点でもある。例えばブログの場合、トラックバックやコメントという形で利用者から提供されるコンテンツが、筆者の執筆する記事に広がりと奥行きを与えているが、一方でそこはトラックバックスパムやコメントスパムの温床にもなり、スパムへの対策が参加型システムとしての運営の重荷ともなっている。

本論文はこうしたスパムを防御するための一手法として「URI 免疫化 (URI Immunization)」[1] という方法を提案する。これは、生物の免疫システムに触発された枠組みであり、生物が生存していくために利用する基本的な戦略である「変化する」という戦略をスパム防御策に取り入れるものである。本論文は、通常は不変な URI (Uniform Resource Identifier) をむしろ素早く変化させることが、スパムからの攻撃を回避するために有効な戦略であることを主張し、その有効性を筆者が運用する「台風への眼」という参加型システムにおける実例を用いて具体的に示す。

2. 研究の背景

トラックバックスパムやコメントスパムへの対策はすでに多くの方法が提案されているが、本論文であえて新しい手法を提案するのは、筆者が運営する参加型システム「台風への眼」の特殊なコンセプトにより、従来からあるスパム防御策が採用しにくいことがその理由である。

「台風への眼」(http://eye.tc/) は「参加型メディアによる台風情報（トラックバック版）」という副題が示す通り、台風が接近する各地の状況を現地の人々からトラックバックを用いて集約することを目的としたウェブサイトである [8], [9]。台風番号と地域番号を用いたトラックバック URL の構成法によって、位置情報を付加した台風情報の集約が可能である点が特色である。またこれらの情報を地図上に可視化する「台風前線」

(http://front.eye.tc/) というウェブサイトも開設しており、この 2 サイトの統合によって参加型システムの情報集約と情報可視化を実現している（詳細は第 6. 節）。

台風情報という緊急的な情報を不特定多数から幅広く集約するというウェブサイトの特殊な目的を考えると、以下に述べる一般的なスパム対策 [2] は本システムのコンセプトにそぐわないことになる。

（1） **事前登録を要求する** 台風の接近で事態が緊急の度を増している時に情報発信のためにユーザ登録を要求するのでは、情報発信者に余計な負担を強いることになる。平常時であればともかく、緊急時にはこのような方法はふさわしくない。

（2） **承認プロセスを組み込む** 緊急情報は一刻も早く多くの人々に伝達する必要があるため、管理者の承認プロセスを間にはさむことは、よほど手厚く担当者を配置できる場合を除いて適切な選択ではない。

（3） **言及リンクを要求する** 本サイトの目的は各地の緊急情報をできるだけ多く迅速に集約することにある。したがっていわゆる「言及リンク」（トラックバック先 URL をリンクとして埋め込むこと）は本質的に必要ではないし、そのチェックにより情報発信者に余計な手間をかけることにもなる。

（4） **特定の文字コードを要求する** 台風は太平洋全体に影響を与える気象現象であるため、現地からの情報は英語などの外国語となる可能性があり、実際にウェブサイトも日英 2 か国語で構築されている。ゆえにトラックバックに日本語文字コードを要求するといったアプローチは本来の趣旨に反する。

（5） **トラックバック内容の特徴を学習する** トラックバックの構文的特徴（HTML タグ等）や語彙的特徴（テキスト等）を解析する方法は、スパムの特徴をあらかじめコーパスで学習する必要があるため、スパムの急速な進化に追従していくのが困難という弱点を抱えている。

また本論文ではローコスト・ローリターンの戦略、つまりスパムによる侵入を完全に防ぐことよりも、システムの管理コストを小さくすることを重視する。本論文で提案する URI 免疫化は、上に述べた従来のアプローチは全く用いず、システムとしても単純であり管理コストも小さい方法である。

3. URI 免疫化とは

URI 免疫化を端的に表現すれば、「変化する」という生物の基本的な生存戦略を取り入れたスパム防御策である。ウェブの世界の原則である「すべての情報リソースに URI という不変で一意の識別子をつける」という原則から一旦離れて、「動く標的 URI (moving target URI)」という考え方を導入するところが本論文のポイントである。

3.1 動く標的 URI

まず始めに、URI を定常領域 (Constant region) と可変領域 (Variable region) の連結として表現し、これを免疫的 URI (Immunized URI) と呼ぶ。

$$\text{URI} = \text{定常領域} + \text{可変領域} \tag{1}$$

ここで定常領域とは時間的に不変な領域であり、リソースを指定するための一意な記号列であるのに対し、可変領域とは時間的に変化する領域であり、リソース自身とは無関係な記号列である。従来の意味での URI は「定常領域」と呼んでいる部分に等しく、それに可変領域を連結したものが免疫的 URI である。可変領域が変化するため、全体としても変化する URI となる。

変化することがなぜスパムの防御に有用な方策となるのか。その理由は、スパムの情報収集段階と攻撃段階の間に、通常は、一定の時間差があるためである。例えばスパム攻撃の典型的な行動パターンとして以下を想定してみよう。

（1） 行動 1：クローラーを巡回させる、あるいは検索エンジンを利用する、などの方法によってトラックバック URI を収集し、これをデータベース化しておく。

（2） 行動 2：データベースからターゲットとなる URI を読み出し、自動スクリプトを用いて順々に攻撃していく。

ここで注目すべきなのは、行動 1 と行動 2 との時間差である。もし行動 1 で収集した URI を使って行動 2 の攻撃に出てきた時、肝心の URI が違うものに変化していたらどうなるだろうか。URI の定義により、スパムの攻撃が成功する必要条件は、スパムが攻撃する URI とトラックバックの入口となる URI が、完全に一致することである。逆に両者の URI が 1 文字でも異なっていれば、スパムの攻撃は失敗に終わる。すなわち、行動 1 と行動 2 の時間差の間に URI を変化させてしまえば、スパムの攻撃は失敗するのである。

このように、ウェブサイトの URI が動く標的のように「常に変化する」URI であれば、スパムはそもそも的を絞れず攻撃しようがない、というのが URI 免疫化のアイデアの核心である。

3.2 生物の免疫システムとの対比

ここで上記のアイデアを生物の免疫システム [3], [4] における抗体と対比してみよう。生物の免疫システムに課された任務は、自分の体内に侵入してきた外敵を捕えて無害なものとなるまで分解してしまうことであり、ここで重要なのが異物（抗原）を認識するという役割を担う抗体である。この認識が成功するためには、抗原の結合部位（エピトープ）と抗体の立体的な構造が一致しなければならないが、実際には日々新しい形状の抗原が登場してくることから、免疫システムは全く未知の抗原に対しても同じ形状の抗体をあらかじめ用意しておかねばならないという難題を抱えている。こうした抗原の多様性の問題を解決するため、抗体の遺伝子は以下のような特殊な構造を持つように進化した。

$$\text{抗体遺伝子} = \text{定常領域} + \text{可変領域} \tag{2}$$

この可変領域が非常に高い頻度で組換えと突然変異を起こすことにより、遺伝子から生成される抗体の立体形状にも変異が生まれ、この変異の多様性が十分に大きければ、未知の抗原と形状が偶然に一致する抗体が生まれる可能性も高まる。そして抗原と一致する形状をもつ抗体さえ発見できれば、あとはこれを速やかに増殖させることで外敵の侵入に対抗できる。これが生物の免疫システムの基本的な戦略である。

生物では一般に遺伝子は不変であると考えられていたため、このように遺伝子配列の組換えや突然変異が頻繁に発生する可

変領域が存在するという理論は常識を覆すものであった。このような画期的な理論を 1976 年に提案して後にノーベル生理学・医学賞を受賞したのが、日本人の利根川進である [5]。

以上に述べた生物の免疫システムと、本論文で提案する URI 免疫化とを対比させると、両者は以下のような対応関係にあることがわかる。

- 抗体も URI も定常領域と可変領域から構成される。
- 抗体の場合は抗原と立体形状が偶然に「一致する」ように遺伝子配列が変化するが、URI の場合はスパムが攻撃する URI と記号列が偶然に「一致しない」ように URI が変化する。

つまり抗体の免疫システムと URI 免疫化は、変化するという戦略は同じであるものの、その目的が正反対である。その意味で URI 免疫化を「逆免疫システム (Reverse Immune System)」と呼ぶこともできる。このような逆免疫システムの実現方法について、以下では細部にわたる検討を加えていく。

4. 免疫的 URI の生成

では免疫的 URI をどのように生成すればよいのだろうか。ここで重要なポイントは URI の分類、およびインポート URI と REST アーキテクチャとの関係である。

4.1 URI の分類

ここで議論を整理するために、URI の 3 種の分類を導入する。

（1） Import URI（インポート URI / I-URI）
（2） Export URI（エクスポート URI / E-URI）
（3） Symport URI（シンポート URI / S-URI）

第一のインポート URI とは、外部（インターネット）から内部（ウェブサイト）へと情報を取り込む URI である。トラックバックやコメントを受け付けるための URI がこれに相当する。それに対して第二のエクスポート URI とは、内部から外部へと情報を出す URI であり、一般にウェブページを提供するための URI がこれに相当する。最後のシンポート URI とは外部と内部で双方向に情報を出し入れする URI であり、例えば HTTP (Hypertext Transfer Protocol) のメソッドによって動作を変える URI（HTTP の GET と POST/PUT で動作を変える URI など）が相当する。

ここでエクスポート URI は情報を内部から外部へと出す一方向 URI であるため、スパム防御とはそもそも無関係である。それに対してインポート URI およびシンポート URI には、スパム防御のために可変領域を導入することに意味がある。なお煩雑さを避けるため、情報を取り込む受容体の役割を果たす URI をまとめてインポート URI と呼ぶ。

4.2 インポート URI の生成

インポート URI は基本的に固定領域＋可変領域として構成するが、ここで固定領域を情報リソースに対応する URI、可変領域を情報リソースと無関係な記号列と定めることにする。この場合可変領域は以下のような方法で生成できる。

（1） 規則的な変化（時刻などから規則的な変換式で生成）
（2） 無記憶的な変化（過去の履歴と関係なく生成）
（3） 記憶のある変化（過去の履歴に依存して生成）

URI が変化することが重要という意味では、可変領域の文字列が「ランダム」であることは本質的な条件ではない。なぜなら、たとえそれが規則的な変化であっても、スパム側がその生成規則を知らなければ可変領域の変化を予測できないからである。さらに、免疫的 URI が広く普及して各サイトが独自の更新ルールを利用するようになれば、スパム側が個々のサイトの更新規則を学習するために労力を割くことは困難となる。

このように、可変領域の記号列に十分な多様性を確保して、スパムが提示する可変領域と偶然に一致する可能性を限りなく低めていくと同時に、スパムが URI を取得して攻撃を仕掛けるよりも早く URI が変化するように可変領域の更新頻度を設定することで、スパムをほぼ 100%防御できるインポート URI を構成することができる。

4.3 REST アーキテクチャと URI 免疫化

このように変化する URI は、ウェブの基本的なアーキテクチャである REST (REpresentational State Transfer) [6] と矛盾しないだろうか。すなわち URI 免疫化は、REST で重要とされている「情報リソースを一意に識別する URI を与えること」を破ってしまうのではないか。一意な URI は Permalink として様々なウェブアプリケーションとも相性がよいことを考えても、免疫的 URI と REST アーキテクチャとの関係についてはあらかじめ整理しておく必要がある。

まずここで可変領域を含む URI を、いつも不安定で変化する URI という意味で Ephemelink (ephemeral link) と命名する。これは当然のことながら検索エンジンなどのウェブアプリケーションと相性が悪い。しかしここで重要なのはインポート URI とエクスポート URI の区別である。実は Permalink とすべきなのは、情報を提供する役割を果たすエクスポート URI であり、インポート URI については必ずしも Permalink である必要はない。むしろインポート URI を Permalink とすることは、スパムに的を絞りやすくさせるという意味で得策ではないとも言える。

そこで REST の考え方を拡張し、情報リソースに関する新しい定義を導入する。

> すべてのリソースは URI 集合で表される互いに素なアドレス集合を持つ

具体的にはリソースの URI は、. を文字列連結演算子として以下の式で定義する。

$$\text{リソースの URI} = c.v \tag{3}$$

$c =$ 一意なアドレス（固定領域）

$v \in V =$ 記号列の集合（可変領域）

リソースの URI は、固定領域の一意なアドレスと、可変領域記号列集合の任意の要素を連結したものであると定義する。ここで、固定領域のアドレスの一意性を保証し、可変領域の集合をうまく定義すれば、情報リソースの URI は互いに素なアドレス集合として相変わらず一意に識別可能であることがわかる。つまり免疫的 URI は、従来の意味での URI（固定領域）の拡張とみなすことができる。

5. 免疫的 URI の伝達

免疫的 URI で生成と並んで重要な問題は免疫的 URI の伝達という問題である。不特定多数が参加するオープンなシステムにおいては、スパムも人間も同じリソースにアクセス可能であるため、スパムによってインポート URI が簡単に取得できてしまっては、せっかく変化する URI を生成しても意味がない。ゆえに、人間には免疫的 URI を伝達しつつスパムにはその解釈を難しくするための工夫が重要となる。

5.1 人間とスパムの能力差と CAPTCHA テスト

現時点で一つの有力なソリューションは、人間とスパムの能力差を利用することで、人間のみが取得できる情報ゲートを通してインポート URI を伝達する仕組みである。例えば CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) [7] では、人間が解くのは簡単だが、現在のコンピュータプログラムでは解くのが困難なテストを提示することによって、人間とコンピュータプログラムとを識別するという枠組みを提案している。画像型 CAPTCHA では、文字認識における人間とスパムの能力差を活用し、変形文字を読み取らせるという作業を介在させることによって、人間とスパムが識別可能な情報ゲートを構成できる。

URI 免疫化の枠組みから見れば、画像型 CAPTCHA が提示して人間に読み取らせる記号列は、まさに URI の可変領域に相当するものである。またその伝達方法として変形文字を使うという方法は有効であり、実際にこの方法は世界でも幅広く利用されている。ただし画像型 CAPTCHA は、本論文で想定するローコスト・ローリターンという戦略においてはややオーバースペックでもある。そこで本論文では、ウェブページの自然言語を理解しないとインポート URI が再構成できないという形で、可変領域を伝達する方法を用いている。

5.2 機械可読性と免疫化

ここで問題となるのが機械可読なメタデータの存在である。免疫的 URI においては、スパムと人間が情報の解釈に要する時間に差をつけることによって、スパムの攻撃を回避することを狙っている。しかし機械可読なメタデータによって情報の解釈が瞬時に可能となれば、すべての戦略が台無しとなる。例えば Trackback Auto Discovery メタデータのように機械可読性の高い形式でインポート URI を公開すれば、スパムは情報を簡単に読み取ってその場で攻撃を開始することができる。これではスパムと人間との間に能力差が生じない。

従来のメタデータに関する議論は、その多くがクリーンな環境でのメタデータの有用性に関する議論であったと考えるが、細菌が繁殖するような「汚染された環境」におけるメタデータの有効性については再考の余地がある。例えば免疫的メタデータとして、メタデータを難読化してスパムがそれを解読するのに時間がかかるようにする等の方法が考えられる。

6. 「台風への眼」における実験結果

以下では、筆者が運用するウェブサイト「台風への眼」における URI 免疫化の実験結果を中心にして、URI 免疫化の有効性について検証する。

図 1 「台風への眼」における URL の構成法。「トラックバック URL」がインポート URL、「トラックバックを見る」がエクスポート URL に相当する。トラックバック URL の末尾にあるのが、最新の可変領域記号列である。

表 1 文字種と文字列長で定める対象指定記号列の意味。

英字 2 文字	国名コード (ISO-3166-1 Country Codes)
数字 2 文字	都道府県コード (JIS-X0401)
数字 5 文字	市区町村コード (JIS-X0402)
数字 6 文字	台風番号 (YYYYNN)
数字 7 文字	郵便番号
数字 8 文字	年月日 (YYYYMMDD)

6.1 「台風への眼」とは

「台風への眼」とは、参加者が各地から送信する台風情報を集約する参加型台風情報サイトであり、不特定多数のブログ筆者が適切な URL にトラックバックを送信することによって、台風ごと・地域ごとの台風情報を集約する仕組みを備えている [8], [9]。こうした参加型ウェブサイトは必然的に多数のインポート URI を公開することになるため、そのままではスパム攻撃に脆弱なウェブサイトとなってしまう。そこでこのウェブサイトに URI 免疫化を実装し、その効果を検証してみることにした。

6.2 URI 構成法

「台風への眼」は図 1 に示すように、トラックバックを閲覧する URI（エクスポート URI）と、トラックバックを受け付ける URI（インポート URI）の 2 種の URI から構成されており、いずれも以下のような要素から構成されている。

$$\text{URI} = \text{ベース URI} + \text{対象指定記号列} + \text{可変領域} \qquad (4)$$

ここでベース URI はインポート URI とエクスポート URI とで異なる記号列だが、対象指定記号列は台風番号や場所などを示し両者に共通する記号列である。そしてベース URI と対象指定記号列とを連結したものが固定領域である。

このシステムでは、表 1 のように文字種と文字列長の組によって記号列の意味を定義している。例えば台風 200601 号に関する東京都千代田区からの情報は、要素の出現順序を定める正規化を経て以下の URI で表現する。

表 2　本論文で用いる 3 種類の時刻の定義。

POST リクエスト時刻	HTTP サーバが POST リクエストを受け取った時刻
トラックバック時刻	サーバ側データベースにトラックバック・エントリが CREATE された時刻
可変領域生成時刻	ある可変領域記号列が生成された時刻

I-URI　`http://eye.tc/trackback/ping/200601/13101`
E-URI　`http://eye.tc/trackback/view/200601/13101`

このインポート URI に対して、英字 3 文字で無記憶的に生成した記号列を可変領域として連結したものが、本システムで用いる免疫的 URI である（PLz が可変領域の一例）。

I-URI　`http://eye.tc/trackback/ping/200601/13101/PLz`
E-URI　`http://eye.tc/trackback/view/200601/13101`

6.3　可変領域のマッチング

可変領域のマッチングは以下の手順でおこなう。

（1） 可変領域記号列をある頻度でシステム側が自動生成し、その履歴を記憶しておく。

（2） エクスポート URI を通じて最新の可変領域記号列を公開する。

（3） インポート URI へのリクエストを受け取り、そこに含まれる可変領域記号列がその時点で有効な可変領域記号列集合の要素と一致する場合のみ、有効なリクエストと判定して受理する。

有効な可変領域記号列集合は、直近 N 個の可変領域記号列として定義している。例えば可変領域生成頻度が 10 分、$N = 3$ とすれば、ある可変領域が有効な期間は 30 分ということになる。

6.4　実験の概要

「台風への眼」サイトでは、2006 年 6 月 6 日に可変領域を導入した。それ以来 7 月 17 日までの約 40 日間の実績についてはすでにまとめた [1]。この時点では 1 日に 1 回の更新としていたが、その後に 4 件の侵入が確認されたことから、より高い頻度での更新（最新では 10 分おき）と更新履歴の保存を開始した。本論文ではその後の 2006 年 7 月 21 日から 2006 年 10 月 11 日までの約 80 日間について調査と分析をおこなう。

6.5　調 査 方 法

本システムでは、トラックバックの受理を以下のような手順で進めている。

（1） トラックバックを HTTP POST リクエストとして受け取る（POST リクエスト時刻(注1)）。

（2） トラックバック URL の可変領域のマッチングをおこなう（第 6.3 節）。

（3） トラックバックが所定の条件を満しており、ナイーブなスパムチェックを通過すれば、トラックバックの内容からハッシュ値を計算する。

（4） データベースを検索し、もし同一ハッシュ値がすでに存在すれば、既存のトラックバック・エントリへの更新として UPDATE する。

(注1)：HTTP サーバが apache 2.2 の場合は取得できるが、サーバのソフトウェアによってはこの時刻が取得できない場合もある。

表 3　POST リクエスト（計 13360 件）の解析。時刻差は POST リクエスト時刻と可変領域生成時刻との差である。

受理アクセス	196
非受理アクセス	3882
時刻差 10 分以内	14 / 3882 = 0.36%
時刻差 30 分以内	81 / 3882 = 2.1%
時刻差 1 時間未満	183 / 3882 = 4.7%
時刻差 10 時間未満	55 / 3882 = 1.4%
時刻差 10 時間以上	3549 / 3882 = 91.4%
可変領域なし	1278
不正な URL	8004

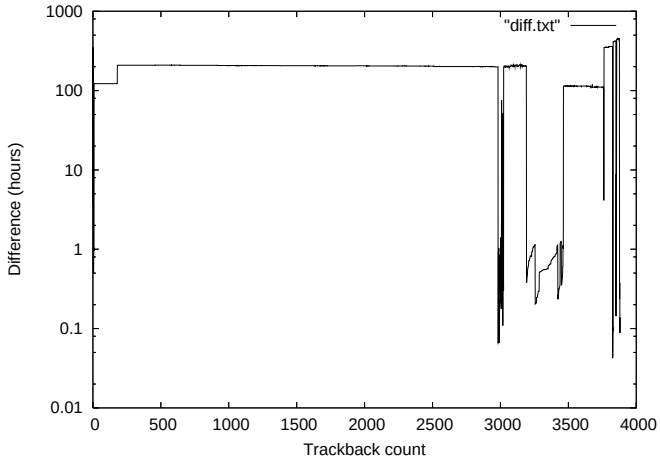

図 2　POST リクエスト時刻と可変領域生成時刻との時刻差の分布。横軸はトラックバックの個数、縦軸は時間差（時間）。横軸は個数であり、実時間には比例していないことに注意。

（5） もし同一ハッシュ値が存在しなければ、新規のトラックバック・エントリとして CREATE する（トラックバック時刻）。

本論文では上記の手順で登場する 2 つの時刻に加えて「可変領域生成時刻」という 3 つの時刻（表 2）(注2)を用いてスパムの特性に関する分析をおこなう。なおナイーブなスパムチェックとしては、以下の方法を用いる。

URL ブラックリスト　トラックバック送信元 URL のブラックリストを作成し、その文字列を含む URL があるトラックバックは拒否する。初期にはこれが主要な対策であったが、現在はリストの更新をほとんど停止した状態である。

ブログ名・タイトルと概要のチェック　ブログ名とタイトルが同じ、あるいはタイトルと概要が同じなど、通常のトラックバックにはあり得ない「手抜き」をチェックして拒否する。

6.6　調 査 結 果

まず POST リクエストの解析を表 3 に示す。約 80 日間に受けた POST リクエストは 13360 件であり、そのうち 196 件をトラックバックとして受理した。「非受理アクセス」とは、URL の形式としては適格であるものの何らかの理由で受理されな

(注2)：本システムのすべての処理は同一マシン上でおこなっているため、短い期間においては時刻合わせの不備が時刻の差分に与える影響は無視してよい。長期間においては時刻合わせの不備による誤差は無視できないが、誤差の比率としては結論に大きな影響は与えないと考える。

かったものであり、可変領域が適合しない、ナイーブなスパムチェックで拒否された、ユーザがトラックバックの UPDATE を実行した（いわゆる「重複トラックバック」の送信と同等）、などのケースがここに含まれる。次に「可変領域なし」とは、2006 年 6 月に可変領域を導入する以前のウェブサイトから収集した URL への POST リクエストである。最後に「不正な URL」とは、存在しない URL あるいはエクスポート URL への POST リクエストであり、これはすべての URL に手当たり次第に POST リクエストを送っているスパムの存在を示唆するものである。

次に POST リクエスト時刻と可変領域生成時刻との時刻差の分布を調べてみると、図 2 から、大半の POST リクエストが有効期間の過ぎたトラックバック URL （時刻差が数十時間以上）への連続的かつ大規模な攻撃であることがわかる。このような時間差は、トラックバック URL を収集する段階と、データベースに基づいて攻撃する段階とが分離していることを示していると考えられる。このタイプの攻撃の防御は URI 免疫化が得意とするところで、原理的に完全な防御が可能である。表 3 では時刻差 10 時間以上のトラックバックが全体の 90%以上を占めていることから、ほとんどのスパムの防御に URI 免疫化は有効であると判断できる。

ただし時刻差 1 時間未満のスパムへの対応は課題である。例えば時刻差 10 分以内の非受理アクセスは全部で 14 件あったが、その内容を詳細に調べたところでは、そのうち 7 件はユーザがトラックバックの UPDATE を実行したか送信ミスしたケース、残りの 7 件がスパムのようであった。このスパムはいずれも 2006 年 8 月 26 日に、可変領域生成時刻と比較して 3 分 56 秒から 10 分以内に攻撃しており、しかも複数の URL が攻撃されていることから、これはデータベース型ではないスパムによる攻撃であることが想像できる。この事例では、たまたまスパムがナイーブなスパムチェックを突破できなかったが、現在の可変領域有効期間が 30 分であることを考えると、これは侵入に成功しても不思議ではなかった事例であると言える。

この種の攻撃を防ぐためには、スパムにとって解釈にコストがかかるような形でトラックバック URL を公開する必要がある。現在はトラックバック URL をほとんど生のテキストとして表示しているが、例えば http という文字列を除く、可変領域のみを分離して表示する、といった工夫だけでもスパムの解釈は大幅に困難となることが予想できる。

最後に precision と recall について検討する。今のところ precision（トラックバックとして受信されたものの中でスパムでないものの割合）はほぼ 100%に近い。つまりスパムはほとんど混入していない。一方で recall（ユーザがトラックバックとして送信しようとしたものの中で実際に受信されたものの割合）については評価が難しいが、実際にウェブサーバのアクセスログを見る限りでは、トラックバック URL を取得してから実際に送信するまでの間に有効期間が切れて、トラックバックの送信に失敗したと想像できるケースが散見された。これはユーザビリティを損う大きな要因であり、可変領域の有効期間の短縮には限界があることの証拠でもある。実際に URI 免疫化が有効なのは、可変領域の有効期間が、スパムのインポート URI の解釈時間よりも短い場合であることを考えると、いたずらに有効期間ばかりを短縮するだけでなく、可変領域の機械難読性を向上させてスパムが短時間で解釈できないようにする方向での工夫も重要である。

7. 今後の課題

本論文は URI 免疫化の考え方を提案し、実際に「台風への眼」を運用しながら収集したアクセスログを分析することで、URI 免疫化の有効性を示した。ただし本格的に URI 免疫化の効果を調査するためには、囮のサーバを設置してすべてのリクエストを詳細に記録しておくことも必要になると考えている。

また本論文では、トラックバックスパムについての議論を展開したが、同様の方法はコメントスパムにも応用可能であると考えている。また、本論文ではインポート URI の免疫化を議論したが、さらにエクスポート URI までも免疫化することによって、外部からのリンクがアーキテクチャレベルで不可能なウェブサイトを構築することも可能になるなど、URI 免疫化にはさらに多様な展開がありうる。紙面の都合でこの点に関する議論は別論文 [1] に譲りたい。

生物の免疫システムは、長年にわたってウイルスなどの外敵と対決してきた中で進化してきたものであり、そこにはスパム対策などにも応用できるアイデアが豊富に見出されている。今後もこうした免疫的フレームワークを発展させ、インターネットという血管を流れる細胞（パケット）をつねに見張ることのできるような、インターネットの新しい免疫システムを考えていくことが大きな課題であると考える。

文　献

[1] 北本朝展. ウェブスパムをかわすための URI 免疫化. テクニカルレポート NII-2006-010J, 国立情報学研究所, 2006.

[2] 渡辺綾太, 愛甲健二. スパムメールの教科書. データハウス, 2006.

[3] 谷口克. 免疫、その驚異のメカニズム. ウェッジ, 2000.

[4] 岡村和夫. 抗体科学入門. 工学社, 2006.

[5] 立花隆, 利根川進. 精神と物質. 文春文庫. 文藝春秋, 1993.

[6] R. Fielding. *Architectual Styles and the Design of Network-based Software Architectures*. PhD thesis, University of California, Irvine, 2000.

[7] L.V. Ahn, M. Blum, and J. Langford. Telling humans and computers apart automatically. *Communications of the ACM*, Vol. 47, No. 2, pp. 57–60, 2004.

[8] A. Kitamoto. Digital typhoon: Near real-time aggregation, recombination and delivery of typhoon-related information. In *Proc. of 4th Int. Symp. on Digital Earth*, 2005.

[9] 北本朝展. 自然災害等の緊急時における情報集約のためのコンテンツ管理システム. 第 19 回人工知能学会全国大会, No. 3C3–02, 2005.

謝　辞

国立情報学研究所の藤山秋佐夫教授との議論は、本論文のモデルを形成する上で非常に有益だった。ここに謝意を表する。