ISSN 1346-5597

National Institute of Informatics

NII Technical Report

ウェブスパムをかわすための URI 免疫化
URI Immunization to Elude Web Spam

北本　朝展
Asanobu KITAMOTO

NII-2006-010J
July 2006

URL: http://www.nii.ac.jp/　Tokyo 101-8430, JAPAN　+81-3-4212-2000　FAX: +81-3-3556-1916

ウェブスパムをかわすためのURI免疫化

北本 朝展*
国立情報学研究所 コンテンツ科学研究系
http://agora.ex.nii.ac.jp/~kitamoto/

1 はじめに

ウェブスパム [1] の隆盛はインターネットの利便性を損なう大きな要因となっており、その効果的な防御策が多くの人々から求められている。本論文は生物の免疫システムに触発された「URI 免疫化 (URI Immunization)」という方法を提案し、この方法がいかにしてスパムを防御できるかについて詳しく論じる。この方法は、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、通常は不変なものと考えられている URI (Uniform Resource Identifier) を素早く変化させることによりスパムを防御する。スパムの内容ではなくスパムの行動に着目した防御策であるため、スパムの内容を解析するなどの面倒な処理が不要であるという利点がある。実際に著者が運営するウェブサイトにおける実験では、約 40 日間に受けた約 2800 件のトラックバックスパムを 100%防御することに成功した。さらに、こうした「URI 免疫化」という戦略を他のインターネットサービスに幅広く適用していく可能性についても論じる。

2 ウェブスパムの隆盛と従来の防御策

ウェブに関連するスパムには、検索エンジンを攻撃するスパム（リンクスパムやタグスパム）、ウェブサイトを攻撃するスパム（トラックバックスパムやコメントスパム）などがある。本論文で扱うのは後者のウェブサイトを攻撃するスパムである。ウェブサイトが双方向性を高めていけばいくほど、ウェブサイトにスパムが入り込む経路が増え、ウェブサイト管理者はスパムに悩まされることになる。こうしたスパムの隆盛は、参加のアーキテクチャを重視し、ユーザが参加しながらコンテンツを生成していくウェブサイトにおいては、特に深刻な問題になりつつある。

こうしたスパムに対する自明な防御策の一つに、事前に登録したユーザを認証してユーザのみからの情報入力を受け付けることで、不特定多数からのスパムを防御するという方法がある。むろんこの手法はスパム防御に一定の効果を発揮するが、その効果は不特定多数に対するシステムの利便性を大幅に低下させたことと引き換えに得られたものである。しかし、不特定多数からの参加を目的とするウェブサイトにおいては、できるだけ間口を広く空けておくことが重要であるため、ユーザ認証に頼る方法はできれば最後の手段としておきたいというのが本音である。

そこで問題となるのが、スパムだけが入ってこられないような入口（ゲート）をどのように作り出すのかという問題である。こうした理想的なゲートを実現するために、これまでもスパムの特徴を学習するための研究に多大な努力が注がれてきた。この種の方法には多くのバリエーションがあるが、そのいくつかを下にまとめた。

1. ある特定の IP アドレスから発信されたスパムを排除する方法
2. ある特定の URL を含むスパムを排除する方法
3. スパムのメッセージの構文的特徴 (HTML タグ等）や内容的特徴（テキスト等）を計算して識別する方法
4. スパムのメッセージに埋め込まれた URL（リンク先）のウェブサイトを解析して識別する方法

*Asanobu KITAMOTO, Digital Content and Media Sciences Research Division, National Institute of Informatics

第一と第二の方法は、スパムに関する大規模なデータベースを多数で共有することによって精度を徐々に高めていくことが可能であるが、スパム側もそうしたデータベースの存在を心得て素早く IP アドレスや URL を変化させてくるため、データベース側がそうした動きに追従していくことが難しいという問題がある。

第三と第四の方法は、スパムの特徴を徐々に学習していきスパムの識別性能を向上させていくことが可能であるが、識別誤りなどを許容しつつ精度を高めていくという忍耐強い取り組みが必要となる。

これらの手法は確かにスパムの特徴を分析して役立ててはいるが、スパム側もそうした学習に対して先回りで変化してくるため、全般的にスパムの戦略に振り回されている感は否めない。ここで採用すべき戦略は、むしろこちらがスパムを振り回すような戦略である。そうした戦略の一つとして本論文が提案するのが、URI 免疫化という方法である。

3 URI 免疫化とは

URI 免疫化 (URI Immunization) とは簡単に言えば、「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。すべての情報リソースに URI という一意の識別子をつける、というのがウェブの世界の基本的な原則である。この原則から考えると、どうしても URI を不変のものと考えてしまいがちであるが、本論文はこの原則を拡張し、URI を定常領域と可変領域の連結として表現することを提案する。

$$\text{URI} = \text{定常領域 (Constant region)} + \text{可変領域 (Variable region)} \tag{1}$$

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。それに対して可変領域とは時間的に変化する領域であり、リソースそのものとは無関係な記号列である。従来の意味での URI は、(1) 式で「定常領域」と呼んでいる部分に等しい。したがって URI 免疫化とは、従来の URI に可変領域を付け足すという提案に他ならない。たったこれだけのことでなぜスパムが防御できるのか。これを以下では考えていきたい。

まず現在のスパムがどのような行動パターンなのかを推測してみる。するとウェブサイトのアクセスログなどを見る限り、以下のような行動パターンを取っているものと推測できる。

1. スパムが攻撃するための URI を収集するためにクローラーを自ら巡回させるか、または既存の検索エンジンの助けを借りてスパムが攻撃するための URI を収集し、これをデータベース化しておく。
2. データベースから攻撃ターゲットとなる 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。ウェブの世界は広大なため、よほど対象を絞りこんで（フォーカスして）URI を収集しない限り、行動 1 はすぐには完了しない。したがって行動 2 を開始するまでには若干の時間を要する。

そこでこの時間差に着目する。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。ここで 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、ウェブサイトの入口となる URI が、完全に一致することである。逆に考えれば、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。以上より、行動 1 と行動 2 の時間差を利用して URI を変化させれば、スパムの攻撃は失敗する。

つまり、ウェブサイト側の 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。ではこの戦略をなぜ「免疫化」と呼ぶのかを、以下で生物の免疫システムと対比させながら論じていく。

4 生物の免疫システム

生物が生き残っていく上でも、変化するということが一つの重要なキーワードである。その代表的な存在が生物の免疫システムである [2]。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、無害なものとなるまで分解してしまうことである。そのためにはまず外敵を認識してはりつく必要がある。しかし、

体内に侵入してくる外敵は無限とも思えるバリエーションを持っており、これまで見たこともないような外敵にも対応しなければならないため、形状を一致させてはりつくことも簡単ではない。

こうした要請に沿って生まれてきたのが、免疫系の抗体システムである。まず体内に侵入してくる異物は抗原と呼ばれ、これを認識するものが抗体である。抗体は実際には免疫グロブリンというタンパク質であり、その形状はアミノ酸配列によって決定される。またアミノ酸配列は遺伝子配列から決定されるため、結局は遺伝子配列によって抗体の形状が定まることになる。

抗体が抗原の存在を認識できるのは、抗原の結合部位（エピトープ）と抗体の立体的な構造がぴったりと一致し、両者が強く結合できた場合に限られる。しかし、抗原がどのような形状をしているかは未知であり、抗体はそれを事前に予測することはできない。このような状況で、抗体はどのようにして抗原に形状を一致させればよいのか。こうした問題を解決するために、抗体は以下のような構造に進化してきた。

$$\text{抗体} = \text{定常領域 (Constant region)} + \text{可変領域 (Variable region)} \tag{2}$$

抗体は、どのような形状の抗原とも一致する可能性を備えるため、多様に変化する可変領域というのものを備える必要があった。この可変領域では、遺伝子配列の組換えや突然変異が頻繁に発生しているため、あらゆる抗原に対して立体的な構造が一致するような抗体が偶然に生み出される可能性がある。そうして偶然に一致した抗体を速やかに増植させることができれば、外敵の侵入に対して対抗することが可能となる。こうした免疫システムの基本的な原理を 1976 年に発見したのが利根川進であり、この研究成果が後のノーベル生理学・医学賞受賞につながった。

以上に説明した生物の免疫システムと、3 章で提案した URI 免疫化とを対比させてみると、両者は以下のような対応関係にあることがわかる。

- URI も抗体も、ともに定常領域と可変領域から構成されている。
- URI の場合は、スパムと記号列が偶然に一致しないように URI が変化するが、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。

つまり、URI 免疫化と抗体の免疫システムは、変化するという戦略は同じだが、その目的は正反対である。つまり URI 免疫化は「逆免疫システム (Reverse Immune System)」でもある。このような逆免疫システムの実現方法について、以下ではもう少し細部にわたる検討を加えていく。

5　URI 免疫化に関する検討

5.1　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）
2. Export URI（エクスポート URI）
3. Symport URI（シンポート 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、例えばパラメータ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。

ここで改めて考えてみると、エクスポート URI はそもそも情報を内部から外部へと出していくだけの一方向 URI なので、スパムの影響をうけることがない。したがってエクスポート URI に関しては、スパム防御のために可変領域を導入する必要はない。それに対してインポート URI およびシンポート URI については、スパム防御のために可変領域を導入する必要がある。なお煩雑さを避けるため、区別する必要がない限りインポート URI とシンポート URI とをまとめてインポート URI と呼ぶ。

5.2 インポート URI の構成方法

そこでインポート URI の構成方法を次に検討する。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、ここで固定領域は情報リソースに対応する URI とし、可変領域は情報リソースとは全く無関係な記号列と定める。可変領域の構成方法としては、以下のような方法が考えられる。

1. 規則的な変化（時刻などを変換するルールに従って生成）
2. ランダムウォーク的な変化（ランダムではあるが累積的な変化）
3. 無記憶的な変化（完全にランダムに変化）

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。たとえ規則的な変化であっても、スパム側がそのルールを発見して学習しない限り、基本的に変化に追従することはできないからである。しかも、各サイトがばらばらな更新ルールを利用するような状況になれば、個別のサイトのルールを学習するために労力を割くことはほとんど不可能となる。ゆえに、記号列の生成方法よりも重要なのは、可変領域を変化させる頻度である。スパムがその変化を察知して素早く攻撃を仕掛けてくる前に、URI は別のものに変化していなければならないのである。

ここで一つの試算をしてみる。可変領域の記号列が、それぞれ個別にランダムに変化する場合を考えてみよう。生物学では個別の ATCG 塩基に突然変異を起こす操作を random mutagenesis と呼ぶ。しかし URI の random mutagenesis では、突然変異で変異する記号集合をもっと大きくすることができる。例えば A-Z の大文字・小文字を合わせた 52 個の記号を可変領域に利用し、可変領域の記号列の長さを 3 とする。この場合に可変領域がとりうる変異の場合の数は、$52^3 = 140608$ 通りである。1 年を 365 日とすれば、たとえ毎日 URI を変化させたとしても、この可能性の空間すべてを使い切るには 385 年以上を要する。つまり、英文字 3 文字程度の可変領域（これを遺伝子にならってコドンと呼ぶ）であっても、実際的な利用には十分な変異の可能性を備えているのである。

もしスパムがより素早く行動するようになれば、URI が変化を起こす間隔をもっと短縮すればよい。例えば 1 日 1 回を 1 時間 1 回にする。またそれに合わせて可変領域の記号列の長さも長くしていく。こうした戦略により、スパムが攻撃する URI とインポート URI とが偶然に一致する確率を限りなくゼロに近付けていくことができる。言い替えれば、スパムを 100%防御することが可能なインポート URI を構成することができる。

5.3 可変領域の伝達

以上がスパムを完全に防御する仕組みである。ただし実際には、話はこれほど単純ではない。残された最大の課題は、可変領域 URI をどのように相手に伝達すればよいのかという問題である。インポート URI を変化させることによって確かにスパムは防御できる。しかし同時に人間もインポート URI を利用できなくなっては意味がない。したがって、人間が利用できてスパムには利用できないような形で、最新の可変領域を相手に伝達しなければならない。

もしあらかじめユーザが限定されていれば、ワンタイムパスワードのような方法を用いて、現在時刻とキー文字列の組み合わせから可変領域を自動生成し、外部に公表することなしに双方で共有することが可能である。しかし不特定多数を対象とする場合には、この方法は使えない。

そこでより一般的な方法として、エクスポート URI を経由してインポート URI を伝達するという方法を考える。インポート URI およびシンポート URI は固定領域を持っており、これが情報リソースと結びついている。そこで、これに対応するエクスポート URI を設けて、そこに最新のインポート URI を公開することで、インポート URI を不特定多数に伝達することができる。またシンポート URI では、固定領域 URI への HTTP GET により、HTTP PUT または HTTP POST 用のインポート用 URI を提示する、といった実装も可能であろう。つまり、エクスポート URI（固定領域のみ）を通して利用者にインポート URI を伝達するというのが、基本的な方法となる。

しかしまだ問題は残っている。このエクスポート URI は、人間だけでなくスパムも同じようにアクセスできる。したがって、スパムがその情報を素早く読みとって即座に攻撃を始めてしまえば、結局のところ問題は解決していない。ではどうすればよいのか。

5.4 人間とスパムの能力差と CAPTCHA テスト

現時点で最も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形でインポート URI を伝達するという方法である。すなわち、人間にとっては簡単だが、あまり賢くないスパムには解けないようなテストを作ることで、人間だけがインポート URI の情報を取得できるような情報ゲートを作ってしまうのである。こうした方法で有名なのは CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)[3] である。

CAPTCHA は、人間が解くのは簡単であるが、現在のコンピュータプログラムでは解くのが困難な問題を提示することにより、人間とコンピュータプログラムとを識別する方法である。こうした問題は人工知能が苦手とする認識系の問題に多く、画像認識、音声認識、自然言語理解などの問題がほとんどあてはまることになる。こうした問題はコンピュータプログラムが比較的苦手とする問題であり、そのどれかを必要とする形で可変領域を提示することが一つの有効な戦略となる。

実際に CAPTCHA は特に画像認識の分野でよく用いられており、すでにメールや掲示板におけるスパムの防止には有効であることが示されている。例えば自動文字認識の困難さを利用して、変形したりノイズを加えたりして読みにくくした文字画像を提示することにより、スパム側ではその情報を自動的に読み取れないようにする。つまり文字認識能力における人間とスパムの能力差が、そのまま人間とスパムとが入手できる情報に差をつける結果となっているのである。

こうした CAPTCHA テストを破るための最も簡単な方法は、実際に人海戦術を用いてテストを通過してしまうという方法であるが、よほど経済的に見合うような重要な場合を除けば、現実的に人海戦術を継続することは困難である。したがって、スパムが情報を読み取るために要するコストが割に合わないような形で情報を提示すれば、スパムはわざわざ苦労して情報を読み取ることはしないと考えられる。

このようなコストの問題を考えれば、現状では自然言語文に URI を埋め込むという程度の簡単な方式であっても、スパムがあまり賢くない現在では十分に効果的であると考えられる。ただし将来的にはスパムがかなり賢くなる可能性もあり、そうなれば画像型 CAPTCHA のようなシステムを用いて、スパムをより厳しく排除する必要があるかもしれない。

5.5 人間が送信するスパム

URI 免疫化によるスパム防御策は、そもそも人間とスパムとの行動と能力差を利用しているため、人間が一つ一つ確認しながら送信してくるスパムには無力である。また、特定サイトを狙い打ちにしたスパムや、侵入する価値が非常に高いサイトに対するスパムなどでも効果は限定される。したがってこうした場合には、従来から用いられるスパム防御策などを併用する必要がある。

しかし、現在大きな問題となっている大量のスパム攻撃では、人間が一つ一つ確認しながら送信しているケースはかなり少ないのではないかと考えられる。また、人間が確認しながら送信するスパムは運用にコストが嵩むため、スパムの広がりは小規模であることが多い。したがって、世の中の大多数のウェブサイトにおいては、こうしたスパムの除去はたとえ手動であってもそれほど問題ではなく、URI 免疫化による防御策が有効に働くものと考える。

5.6 Permalink との関係

ウェブの世界では、Permalink の重要性、すなわち情報リソースに一意な URI を与えて永続的にアクセス可能とすることが重要であることがよく論じられる。この考え方は特に、検索エンジンの発展とともに重要性を増してきた。というのも、こうした Permalink がなければ検索エンジンはその情報を安定して検索可能とできないからである。そこで可変領域の考え方が Permalink に不都合を生じさせないかを検討する。

まずここで、可変領域を含む URI を Ephemelink と名づけよう。すなわち、いつも不安定で移り行く URI である。これは当然のことながら検索エンジンと相性が悪い。しかしここで注意すべきなのは、インポート URI とエクスポート URI の違いである。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、こちらは通常は固定領域のみをもつ。一方のインポート URI は確かに可変であるが、情報を取り込

むための URI であることから、検索エンジンで検索すべきコンテンツはそこには存在しないはずである。

したがって重要なのは、エクスポート URI が Permalink となっており、そこから最新のインポート URI が安定的に入手できるようになっていることである。そうなっている限り、インポート URI そのものが固定である必要は全くない。むしろ、インポート URI までも Permalink でなければいけないという従来の考え方が、スパムに的を絞りやすくさせていたというのがこれまでの状況である。

5.7 REST アーキテクチャとの関係

さらに URI に可変領域が存在することが、ウェブの基本的なアーキテクチャである REST (REpresentational State Transfer)[4] において不都合を生じさせないかを検討する。REST には以下のような基本的な考え方がある。

> すべてのリソースは URI で表される一意的なアドレスを持つ

これをそのまま受け取れば、リソースが可変 URI を持つことはリソースが複数の URI を持つことを意味するので、ウェブの基本原理を破ってしまうということになる。そこでここでは上記の定義を少し拡張し、以下のような定義を用いることになる。

> 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、リソースに対応する URI を、以下のような URI 集合として定義するのである。

$$\text{リソースの URI 集合} = \text{一意なアドレス（固定領域）} + \text{記号列の集合（可変領域）} \tag{3}$$

すなわち、あるリソースに対しては一意的なアドレスではなく、互いに素なアドレス集合を考えるのである。互いに素な URI 集合であることは、固定領域のアドレスの一意性によって保証する。そしてある時点での URI は、リソースの URI 集合の要素のどれか一つが選ばれるということになる。固定領域のアドレスの一意性は、そもそも従来の意味での URI の一意性と同じことなので、こうすることには特に困難はない。したがってリソースを URI 集合と対応付けることにより、従来のウェブの世界をあまり変更せずに使い続けていくことができるのである。

ただし、異なるリソースの区別はあくまで固定領域でおこなうべきで、可変領域の偶然性に頼ってリソースを区別するような設計をおこなってはならない。また、この方式が世界規模で正しく動くためには、すべてのサーバとキャッシュサーバとが、固定領域と可変領域を正しく解釈できる必要がある。ただし現状では、インポート URI のみが可変領域を持っており、しかもそれは本来的にキャッシュすべきでない情報であるため、現実的にウェブ上で混乱が起きる可能性は低いと考えられる。

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」(http://eye.tc/) 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。

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、不特定多数のウェ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 [5, 6]。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 免疫化を実施し、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）とがある。この 2 種類の URI はいずれも以下のような方法で組み立て

図 1: 「台風への眼」における URL の構成法。「トラックバック URL」がエクスポート URL、「トラックバックを見る」がインポート 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)

られている。

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

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 URI となる部分だが、対象指定記号列は台風番号や場所などを示す記号列であるため、両者に共通する記号列となる。そしてベース URI と対象指定記号列とを連結したものが、固定領域となる。

このシステムで特徴的なのは、表 1 に示すように、文字種と文字列長ごとに記号列にあらかじめ意味が定められている点にある。したがって文字種と文字列長をチェックするだけで記号列を意味付けできることになる。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、以下のような URI で表現されることになる。

インポート URI	http://eye.tc/trackback/ping/200601/13101
エクスポート URI	http://eye.tc/trackback/view/200601/13101

さてこのインポート URI に可変領域を導入する方法として、英字 3 文字のコドンを導入する。この文字種と文字列はまだ他の目的に利用されていないため、可変領域の生成と認識は簡単である。いまここで、英字 3 文字に突然変異を加え、たまたま出現した文字列が PLz だったとすると、可変領域を含む URI を以下のように構成することができる。

インポート URI	http://eye.tc/trackback/ping/200601/13101/PLz
エクスポート URI	http://eye.tc/trackback/view/200601/13101

ここで末尾にある可変領域は、現状では 1 日ごとに変化させている。また可変領域の記号列は、固定領域の意味とは一切関係のない、ランダムな英字記号列である。

なお、可変領域は末尾に位置することが重要なのではなく、あくまで可変領域と固定領域とが区別可能な形で URI に表現されているということが重要である。上記の URI 構成法では、たまたま文字種と文字列長のみで可変領域を区別することが可能であったが、一般的にはこうした方法は利用できないため、以下のような URI 構成法で可変領域の識別をおこなうことになる。

インポート URI	http://www.example.jp/uri?variable=PLz

すなわち、システム全体で variable という引数が可変領域を表すことを定義しておけばよい。

6.3 可変領域のマッチング

インポート URI の活用は、以下のような手順で進めていく。

1. 現在有効な可変領域記号列をシステム側で生成し記憶しておく。
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 にリクエストがあれば、まず可変領域記号列を認識し、現在有効な可変領域記号列と比較する。両者が一致した場合のみ有効なリクエストとして受け入れ処理を行う。

ただし上記の方法をそのまま実装すると、可変領域記号列が切り替わる瞬間を偶然にまたいだ場合にシステムがうまく動作しない。そこで実際には、直近 N 個の可変領域記号列を有効可変領域文字列集合として記憶しておき、その集合の要素のどれか一つと完全一致した場合にリクエストを受け入れるというロジックになる。そして可変領域の更新頻度を短くすればするほど、N の値は大きめに設定する必要がある。

6.4 実験の結果

「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 日間の実績から、可変領域導入の効果を評価する。

まずウェブサーバのアクセスログをチェックし、インポート URI への HTTP POST リクエストをすべてトラックバックのリクエストとみなした。すると、この期間にそうしたリクエストは 2855 件あった。つまり平均して 1 日に 70 件のリクエストがあったことになる。

この中で、正しい可変領域を備えた有効なトラックバックとして受け入れられたのは 37 件であり、その中にはスパムと判断できるものは存在しなかった。したがって、受け入れたトラックバックについては precision は 100%となる。

一方、すべての非スパムトラックバックの中で、実際に受け入れることのできたトラックバックの割合、すなわち recall についてはどうだろうか。これについては、受け入れを拒否したトラックバックに関するデータが残っていないために正確に算出することはできないが。可変領域が導入された後もトラックバックの送信には特に困難はなく、送信ミスが発生した可能性も低いと考えられるので、recall についても 100%に近い値なのではないかと予想している。

以上の実験結果から、可変領域の導入による URI 免疫化は、ほぼ完全にトラックバックスパムを排除する効果があると結論する。

6.5 変化に対するスパムの追従

可変領域の履歴を記録していなかったという実験の不備により、スパム側がどのくらいの速さで可変領域に追従しているのかを検証することはできていないが、間接的な証拠はウェブサーバのアクセスログに残っている。

6 月 6 日に可変領域の導入を開始して以来、しばらくの間は可変領域なしのトラックバック URI への攻撃が続いていたが、6 月 14 日になって初めて、可変領域のあるトラックバック URI へのアタックが始まった。もちろんその時点ではすでに可変領域は別の URI に変化しているので、スパムの攻撃は失敗している。そして、この一

連のアタックが同じ日に終了して以来、スパムからは相変わらず可変領域なしのトラックバック URI への攻撃が続いている。

以上の記録を考えれば、トラックバック URI への追従スピードについては、例外的に数日で追従した場合があったものの、大部分については 1ヶ月が経過しても未だに追従できていないことがわかる。したがって、現状では 1 日単位での更新頻度でも、十分であるという結論が得られる。

7 議論

7.1 エクスポート URI の免疫化

これまでインポート URI の免疫化について議論してきた。インポート URI に可変領域を付加することには、スパムをかわすために素早く変化する URI を用いるという明確な目的があった。ではエクスポート URI に可変領域を付加することに意味はあるだろうか。

一見するとエクスポート URI を可変にすることは有害なだけのように思える。検索エンジンにとってはアクセスのたびに URI が変化してしまってはインデックス化することができないし、ユーザにとってもブックマークしても次回からはアクセスできないなど、使いにくいこと甚しいからである。

しかし発想を変えてみれば、こうしたアイデアが全く無意味なわけでもないことに思い当たる。例えばこうした方法は、外部からリンクが不可能なウェブサイトを構築することに利用できる。アクセスするたびに URI が変化し、次に出現する URI が予測不可能であれば、外部からリンクを張るのは理論的に不可能である。

またこの変種として、一部のページのみ固定 URI とし、他のページを可変 URI にしたウェブサイトも考えられる。この場合は固定 URI にしか外部からリンクを張ることができないので、例えばトップページのみ固定 URI にしておけば、トップページにしかリンクできないウェブサイトを実現することができる。トップページのみにしかリンクを許可しないというポリシーをもつウェブサイトが世の中には存在するが、そうしたウェブサイトではエクスポート URI にも可変領域を持たせれば、こうしたリンクポリシーをウェブサイトのアーキテクチャレベルでユーザに強制することが可能である。

そしていずれの場合にもウェブサイト内部のリンクに関しては、可変領域をうまく共有すれば、ナビゲーションに問題が生じないように URI を構成できることに注意されたい。これはウェブサイトを設計する際の技術的な問題として解決できる。

さらにこの自然な拡張として、複数のウェブサーバ群内で可変領域を共有することにより、ウェブサーバ群内では普通にナビゲーションできるが、外部からはリンクを張れないウェブサイトも実現することができる。

7.2 他のインターネットサービスの免疫化

上記の結果は、ウェブサーバにおけるウェブスパムへの対応を主眼としたものであった。しかし同様の免疫化というアイデアは、他のインターネットサービスにおけるスパム防御にも適用できるものと考えている。

例えばもし実現すればインパクトの大きいものとして、メールスパムの防御への応用が考えられる。これも同様に、メールアドレスという URI に可変領域を設けることで、同様の防御効果を持たせるというアイデアである。例えば、自分のウェブサイトに CAPTCHA 画像化された可変領域文字列を示しておき、それを送信者に入力させるというような方法を利用すれば、可変メールアドレスによるスパム防御は可能である。もちろんメールクライアントの改良により、CAPTCHA 画像の自動取得や、RSS フィードなどを利用した可変メールアドレスの自動更新など使い勝手を良くする方法がある。

ただしメールのサービスはより複雑であるため、トラックバックスパムの場合のように単純なソリューションは使えないことに注意しておく必要がある。トラックバックのようにピアツーピアの形で情報をやり取りする場合には、比較的単純なソリューションでも十分である。可変メールアドレスに関する上述の例もピアツーピア型のメール送受信の場合である。しかしメールの場合には、メーリングリストなど他の形式のサービスもあり、このように中継が入るような複雑な環境での可変メールアドレスの実現には、かなり慎重な考察が要求されてくる。したがって可変メールアドレスに関しては将来の検討課題として残しておく。

また IP 電話化によってスパム電話が増えるという予測もある現在、可変電話番号の実現もスパム防御の有力

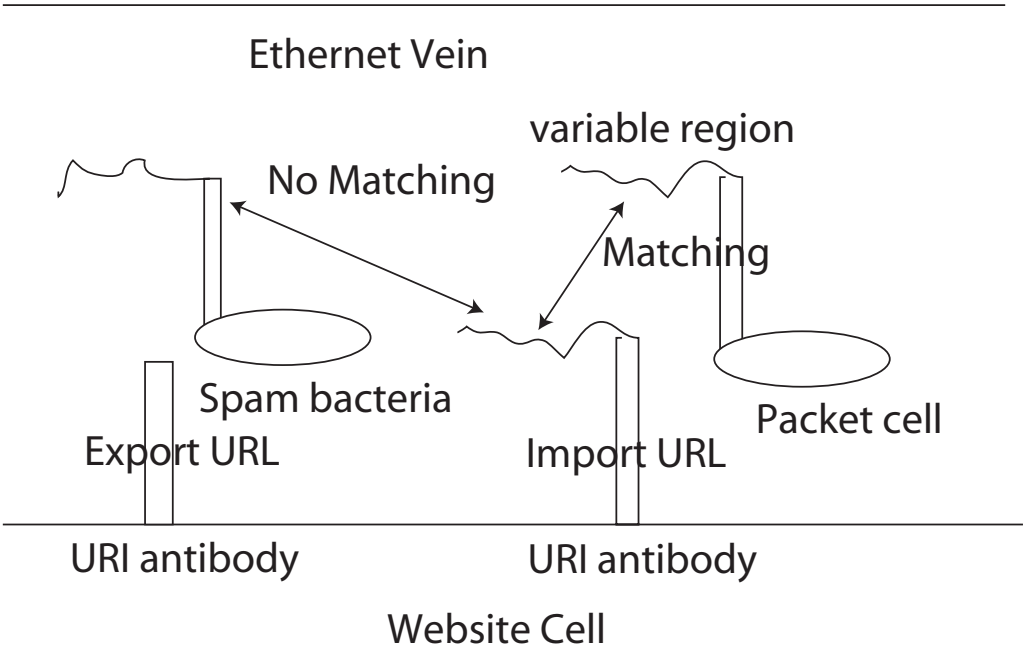

図 2: インターネットの逆免疫系モデル。

なソリューションとなるかもしれない。電話はピアツーピア型の通信である場合が多いことを考えれば、むしろ可変電話番号の方が実現しやすい可能性がある。

いずれにしろ、こうした可変領域の考え方は、インターネットの様々なサービスにおけるスパムを防御する統一的なソリューションとなりうる可能性を秘めているといえる。

7.3 機械可読性と免疫化

先述したように、可変領域の最大の問題は、最新の可変領域情報を相手にどのように伝えるかという問題、言い替えれば人間には正確に伝え、スパムには伝えないという方法を、どのように実現すればよいのかという問題にある。その意味では、すべての情報を機械可読性の高い状態で提供すうることは、人間とスパムとの能力差を縮めるので好ましくないということになる。例えば、Trackback Auto Discovery メタデータのような形式を用いてインポート URI を機械可読性の高い形式で外部に公開してしまうと、スパムはその情報を簡単に読み取ることができる。このように機械可読性とスパム耐性のバランスをどのように取っていくかは、今後の大きな課題である。

8 逆免疫システムの全体像

本論文の最後に、逆免疫システムの全体像を再びアナロジーとして確認しておくことで、本論文で提示したアイデアを補強しておきたい。また、免疫系という自然界ですでに有効に機能しているモデルを参照することは、スパムという外敵を退治するための様々な方法を生み出すためのアイデアの宝庫なのではないかと考える。

図 2 のように、ウェブサイトという細胞が、URI という抗体（受容器）をイーサネットという血管の中に出している。また血管の中には、パケットという細胞の他に、スパムというバクテリアが混じって流れており、これらは URI との結合を試みている。もし両者がピタリと結合すれば、インポート URI の場合には彼らはウェブサイト内部に情報を送り込むことができ、エクスポート URI の場合には彼らはウェブサイト内部から情報を取り出すことができる。

いま、スパムがこの血管に入り込んできたとしよう。スパムは以前に集めておいた URI の形状にぴたりと合わせた形状の URL を提示しており、あわよくばインポート URI にくっついて有害情報を中に送り込もうとしている。しかしスパムが提示する可変領域 URI の形状はもはや古いものであり、現在は血管中に出ている URI は別

の形状に変化している。したがってスパムはそこにくっつくことさえできず、あえなくそこで死滅してしまうことになる。一方、きちんと最新の可変領域を読んでそれと一致する URI を提示している細胞は、インポート URI にくっつき、無事に情報を内部に送り込めることになる。

こうしたアナロジーで考えていけば、URI が一致することがスパムにとっていかに大事なことであるかが、一目瞭然でわかるのではないだろうか。

自然界では、こうした変化する戦略を攻撃側も防御側も利用している。免疫系の抗体システムでは、抗体側が素早く変化することによって外敵をつかまえられるようになったが、マラリアや AIDS などではその裏をかくように、攻撃側の方が防御側よりも素早く変化してい仕組みを備えている。このように、できるだけ素早く変化することで、敵をつかまえたりかわしたりしているのが生物の世界であり、免疫系の導入によりインターネットの世界もそうした終わりなき戦いに突入していく可能性がある。

9 おわりに

本論文では、逆免疫システムにおける URI 免疫化という方法を提案し、これがスパムの防御に効果的であることを示した。一般的に URI は不変であるし、そうあるべきだと考えられているが、そこに可変領域を導入してウェブサイトが変化し続けることが、スパムの防御策となることを説明した。

今後はこうした免疫化という方法を他のインターネットサービスに適用する方法を検討する。また、こうした手法が普及すれば当然スパム側も進化してくることが予想され、さらに強固な免疫システムを進化させていくことも今後の課題である。

参考文献

[1] G. Zoltan and H. Garcia-Molina. Web spam taxonomy. *Technical Report, Stanford University*, 2004. http://dbpubs.stanford.edu/pub/2004-25.

[2] 岡村和夫. 抗体科学入門. 工学社, 2006.

[3] 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.

[4] REST - Wikipedia. http://ja.wikipedia.org/wiki/REST.

[5] 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.

[6] 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。