ネットワークに対する未知攻撃の検知・防御技術とその応用

Network Anomaly Detection and Prevention Technologies and Their Application

今野　徹　　楯岡　正道
■KONNO Toru　■TATEOKA Masamichi

ウェブサーバなどをインターネット上の様々な攻撃から守るため，既知の攻撃パターンとのマッチングにより防御する不正侵入防御（IDP：Intrusion Detection Prevention）装置が企業に導入されている。しかし今日，セキュリティホールの存在が知られてからそれを利用した攻撃が現れるまでの時間が非常に短くなり，従来の手法では対処しきれなくなっている。

東芝ソリューション（株）は，こうしたセキュリティ上の問題に対するソリューションの一つとして，IDP装置であるAntiHacker-Pro™の未知攻撃検知・防御技術を実現した。この技術は，ネットワークのアプリケーション層で常に学習しながら統計分析するL7パラメトリック分析方式™をコア技術として開発し，タグチメソッドを用いて高い検知精度を実現している。

Many corporate users have deployed intrusion detection and prevention systems in order to protect their Web servers from various attacks on the Internet. However, new attack incidents that exploit unveiled security holes have begun to rapidly proliferate, making it difficult to respond using legacy pattern matching techniques.

To solve this security issue, Toshiba Solutions Corp. has developed unknown-attack detection and prevention technologies in the AntiHacker-Pro™ product. We have implemented L7 parametric analysis™, which statistically analyzes network application data in real time. We have also leveraged the Taguchi method to accomplish a highly accurate attack detection rate.

1 まえがき

インターネットビジネスの拡大に伴い，ウェブサーバは企業や公共機関で重要な役割を担っている。一方，ウェブサーバは不正アクセス，データの改ざん，サービス不能攻撃などの脅威に常にさらされている。過去にMS BlusterやSasserといった有名な事件があった。また，ホームページ書換え事件は，今でも日々報告されている[(1)]。こうしたウェブサーバへの攻撃は，企業の社会的信用の失墜やビジネス機会の損失につながっている。このような被害を防ぐためには，ウェブサーバのセキュリティ対策を行うことが急務であり，セキュリティを維持することが重要となっている。

東芝ソリューション（株）は，そのソリューションの一つとして不正侵入防御（IDP：Intrusion Detection Prevention）装置であるMAGNIA™2000Ri/Anti-Hacker™を開発し，2000年12月から販売してきた[(2)]。今回，新機種として，未知攻撃の検知・防御機能を搭載したAntiHacker-Pro™100/300シリーズを開発し[(3)]，未知の攻撃を検知し防御する際に大きな課題となる，検知率の向上と誤検知率の削減の両立を達成した。

ここでは，このシリーズに採用されている未知攻撃検知・防御技術について説明するとともに，この技術の今後の応用について述べる。

2 未知攻撃検知・防御技術の必要性

MAGNIA™2000Ri/Anti-Hacker™では不正侵入防御機能を提供しており，既知の攻撃パターンをデータベース（DB）として持ち，通信パケットをDBと比較することで，攻撃検知を行っている。しかし，未知のセキュリティホールを利用する未知の攻撃は，そのセキュリティホールが既知となり，攻撃パターンDBが更新されるまで防御できないという課題がある。このような攻撃はゼロデイアタックとも言われ，特に今日では，セキュリティホールの存在が知られてからそのセキュリティホールを利用した攻撃が現れるまでの時間が非常に短くなってきている。こうした未知の攻撃への対処はほかのIDP装置でもできておらず，この問題点の解決がIDP装置として求められている。

そこで上記課題の解決のため，当社はAntiHacker-Pro™100/300シリーズにおいて，業界初のL7パラメトリック分析方式™による未知攻撃の検知・防御機能を開発した。

3 L7パラメトリック分析方式™による未知攻撃の防御

L7パラメトリック分析方式™とは，ウェブサーバへの通信をネットワークのアプリケーション層（L7：レイヤ7）で常に学

習しながら統計分析を行う方式である[4]。不正アクセスや攻撃のほとんどは，通常のリクエストパターンを逸脱するという特徴がある。そこで統計分析を行い，正常・異常のしきい値を決め，正常を逸脱したものを攻撃として検知する。この機能により，攻撃パターンDBで対応していない未知の攻撃でも検知することができる。

図1に示すように，ウェブサーバの前段に置かれたAnti-Hacker-Pro$_{TM}$は，ウェブサーバへの通信データをすべてL7パラメトリック分析方式$_{TM}$により未知の攻撃を検知する。検知された通信データはウェブサーバに到達する前に破棄するとともに，通信内容と統計分析結果について管理者へ通知する。このようにして，攻撃パターンDBとの比較だけでは成しえなかった未知攻撃の検知・防御を実現している。

次に，L7パラメトリック分析方式$_{TM}$の概略を説明する。ウェブアプリケーションへの攻撃の大半は，バッファオーバフロー攻撃又はメタキャラクタなどの挿入によるものであることがわかっている。そこでウェブアプリケーションへ渡されるパラメータの各々について，値の文字列長や値に含まれる文字セットなどの特徴を数値化して統計処理を行い，異常値検知を行っている。**図2**のHTTP（HyperText Transfer Protocol）リクエストを例にすると，パラメータ（year，month）について，その値（“2005”，“5”）の長さや文字セットを数値化して統計処理する。

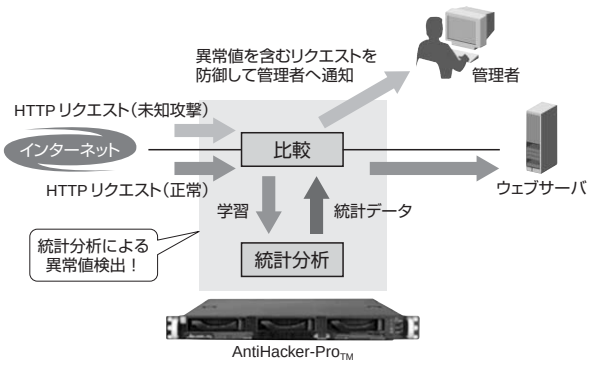


図1．未知攻撃検知・防御機能 ― ネットワークのアクセスデータを常に学習しながら，統計分析により未知の攻撃を検知・防御する。

Unknown-attack detection and prevention

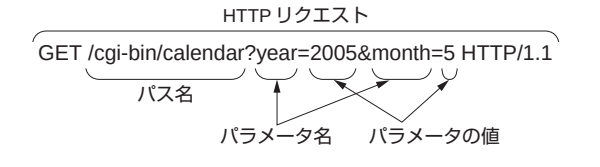


図2．HTTPリクエストの分解例 ― HTTPリクエストはパス名，各種パラメータ名及びその値に分解される。

Example of analyzed HTTP request

十分な学習を終えると，**図3**のような対象パラメータ値についての統計分布を計算することができる。この統計分布から，あるしきい値を超えたものを異常値であると判断する。例えば，図2のパラメータ（year）に関して言えば，その長さは4けたであり，5けた以上の値は通常ありえない。パラメータ（year）のバッファをオーバフローさせる**図4**のようなHTTPリクエストを受信すると，その長さは図3の分布図から異常値であると判定される。

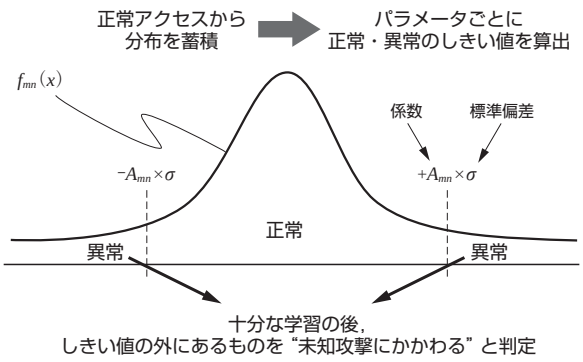


図3．統計分布と異常値の判定方法 ― mはパラメータの種類を表し，nは数値化された特徴の種類を表している。また，$f_{mn}(x)$はHTTPリクエストxに関して数値化された値の統計分布である。

Statistical distribution and anomaly judgment

```
GET /cgi-bin/calendar?year=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa&month=5 HTTP/1.1
```

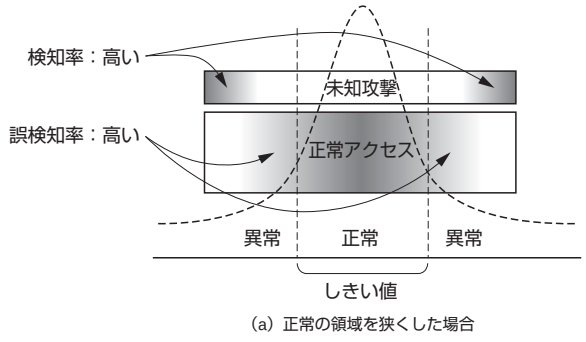
図4．バッファオーバフロー攻撃例 ― あるパラメータに与えられる値の長さが，統計的に異常に長いことが検知される。

Example of buffer overflow attack

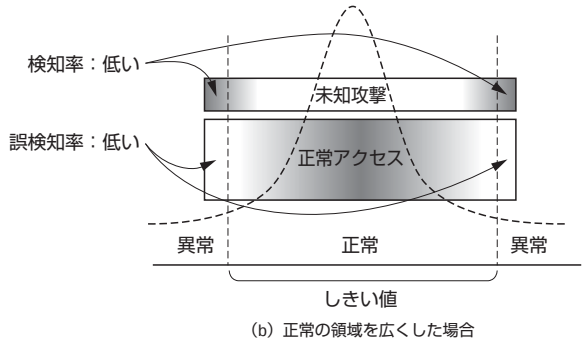
4 しきい値係数の最適化

L7パラメトリック分析方式$_{TM}$では，正常か異常かを分けるしきい値の係数A_{mn}（図3参照）が鍵となるパラメータであり，これの設定によって未知攻撃の検知率と誤検知率が大きく左右される。検知率とは，未知の攻撃を見逃さずに検知する割合であり，高いほうがよい。一方，誤検知率とは，正常なアクセスを未知攻撃として誤検知する割合であり，ゼロであることが望ましい。しかしながら，一般的に検知率と誤検知率にはトレードオフの関係があって，しきい値の設定を変えることによって一方を良くすれば他方が悪くなるという傾向がある。

このトレードオフの関係を**図5**に沿って説明する。いま，あるしきい値の係数について，正常と異常を分ける値を調整し，異常の領域を広くして正常の領域を狭くしたとする（図5（a））。そうすると，その特徴により異常をより多く検知



(a) 正常の領域を狭くした場合



(b) 正常の領域を広くした場合

図5．検知率と誤検知率のトレードオフ ― 未知攻撃についての検知率は高いほど望ましく，正常アクセスについての誤検知率は低いほど望ましい。

Trade-off between true detection rate and false detection rate

することができるので，未知攻撃の検知率を高くすることができる反面，本来攻撃ではない正常アクセスを異常とみなす誤検知が多くなってしまうおそれがある。逆に，しきい値の調整により正常の領域を広くして異常の領域を狭くすると，誤検知を減らすことができる反面，未知攻撃を見逃してしまう可能性が高くなる(図5(b))。

このようにトレードオフの関係にある検知率と誤検知率について，双方を損なうことなく，特に誤検知率についてはゼロに近い精度にしなければならない。更に，m×n通りのしきい値の組合せがあるため，最適値を求めることは容易ではない。そのため，当社は多くのウェブサイトを対象とした評価を行い，しきい値の係数について入念なチューニングを施した。その評価にあたっては，タグチメソッドを活用している[(5),(6)]。

タグチメソッドとは実験計画法が発展したものであり，現在，工業における様々なシステムの品質向上に用いられているパラメータチューニング手法である。特徴としては，対象システムをチューニングする際に，システム性能をばらつかせるノイズをあえて取り入れ，最適なパラメータ推定値が効率よく得られるノイズに強い手法である。ソフトウェアの分野では，タグチメソッドを使った事例はまだ少ないが，当社はこの有用性を見いだし積極的に活用している。

L7パラメトリック分析方式TMの場合，ウェブサーバへの通信内容を学習することで未知攻撃の検知を行っているため，守るウェブサーバによって検知率と誤検知率にある程度の影響を受ける。そこで，ウェブサーバの違いをノイズとみなし，様々なウェブサーバでの評価を取り入れてチューニングすることで，検知率と誤検知率に関してウェブサーバの違いによらない最適なしきい値の設定を実施している。

更に，検知率と誤検知率のトレードオフの関係を克服するために，“デジタルデータの標準SN(信号と雑音)比”という評価手法を用いている。これは，システムの出力が論理値(ここでは検知率と誤検知率)に関するものであって，両者がトレードオフの関係にあるとき，両者を統合化して単一の指標として扱うことができるようにしたものであり，この問題に適している。

これらの指標を用いることで，しきい値の最適な設定値が求められ，また，数多いしきい値の係数A_{mn}の中で，どれがどの程度影響しているかもわかる。このような一連の評価によりしきい値の係数チューニングを施すことで，未知攻撃の検知率を高い値に保ったまま，極めてゼロに近い誤検知率の値を達成している。

5 未知攻撃の検知・防御技術の応用

以上説明したように，AntiHacker-ProTMの未知攻撃検知・防御技術は，ウェブアプリケーションへ渡されるパラメータが持つ構造の特徴を数値化して統計処理を行い，その異常値を攻撃として精度よく検知する技術である。

この技術は，ウェブサーバを防御する目的にとどまらず，幅広く応用できると考えられる。

以下に，この技術の応用として考えられるものを，いくつか例示する。

5.1 HTTP以外のプロトコルへの応用

この技術はウェブサーバへのHTTPリクエスト，特にウェブアプリケーションへのリクエストの特徴を数値化し，未知攻撃の検知・防御技術を実現している。文字列長や含まれる文字セットなどにより特徴を数値化できるものであれば，ほかのプロトコルであっても，この技術を応用することは容易であると考えられる。

適用可能なプロトコルの例としては，例えば，AntiHacker-ProTMシリーズで攻撃パターンDBによる防御を行っている，SMTP(Simple Mail Transfer Protocol)やDNS(Domain Name System)プロトコルなどが考えられる。

また，最近では音楽や映像など，いわゆるマルチメディアコンテンツの配信が普及してきたが，それに伴い，これらのコンテンツ配信プロトコルに潜むセキュリティホールを狙った攻撃も現れてきている。この技術は，これらコンテンツ配信プロトコルでの未知攻撃検知・防御にも応用できると

考えている。

5.2 XML技術に基づくサービスへの応用

ウェブサーバへのHTTPリクエストの中で，現在，この技術に基づく統計処理の対象としているのは，HTTPリクエストに含まれるCGI（Common Gateway Interface）パラメータである。

近年，ウェブサーバ上で動作させるウェブアプリケーションに，SOAP（Simple Object Access Protocol），UDDI（Universal Description, Discovery and Integration），WSDL（Web Services Description Language）などのXML（eXtensible Markup Language）技術が用いられるようになってきている。これらのXML技術に基づくサービスへの攻撃の検知・防御にこの技術を応用して，ウェブサーバを更に強固に防御するために利用することもできると考えている。

5.3 DBサーバからの情報漏えい検知への応用

個人情報保護法の完全施行などを背景に，DBサーバからの情報漏えいを検知する技術への要求が高まってきている。

DBサーバの操作は，SQL（Structured Query Language）言語によって行われるが，このSQL言語によるアクセスの特徴を数値化することで，この技術に基づく異常検知を行い，情報漏えいを検知・防御することができると考えられる。

5.4 組込みソフトウェアへの応用

情報家電に代表されるように，組込みソフトウェアの分野でもネットワークへの接続機能が備えられてきている。したがって，情報家電が攻撃対象となる可能性は十分にある。

組込み分野では，攻撃パターンDBを備えて防御する場合，個々の機器ごとに異なるDBを作成する必要があり，種類が非常に多い情報家電に対しては現実的ではないと考えられる。組込み機器の限られたリソースの中で効率よく学習する技術を開発する必要はあるが，この技術を適用することが望ましいと思われる。

5.5 セキュアなシステム開発ツールとしての応用

この技術は，未知攻撃の検知を目的に開発した技術ではあるが，本質的には学習により正常範囲を識別し，異常を精度よく検知する技術である。

このことから，例えば，リモートプロシージャコールなどのリクエスト－レスポンスについて，パラメータ値を統計分析することで異常値を検知する。この異常値に対し正しく実装されているかを解析することで，実運用を開始する前の開発段階で，予測しないバグや不備を補うことができる。こうした使い方をすることで，セキュアなシステム開発プロセスにおける一つのツールとなりうると考える。

攻撃に対する防御というネガティブな要請に基づき開発を行った技術であるが，その技術の本質に立ち戻ると，ポジティブな恩恵をもたらすための更に多くの応用も可能であると思われる。

6 あとがき

ここでは未知攻撃検知・防御技術についてIDP装置Anti-Hacker-Pro$_{TM}$に実装されている方式について述べるとともに，パラメータの最適化手法及び今後の応用について考察した。

この技術は，これまで述べたとおり幅広い活用が期待できる。今後は，セキュアなシステム開発ツールとしての応用や，セキュリティをより高めるための継続的な技術開発を行っていく。

文　献

(1) 独立行政法人 情報処理推進機構（IPA）．セキュリティセンター．＜http://www.ipa.go.jp/security/index.html＞，（参照 2005-02-17）．

(2) 進藤修一，ほか．Webサーバへの攻撃の検知･防御技術MAGNIA$_{TM}$2000Ri/Anti-Hacker$_{TM}$への適用．東芝レビュー．**58**，8，2003，p.27－30．

(3) 東芝ソリューション（株）．情報セキュリティ セキュリティ製品．＜http://pf.toshiba-sol.co.jp/prod/security/index_j.htm＞，（参照 2005-02-17）．

(4) 今野　徹，ほか．HTTPリクエスト解析による未知攻撃防御システム．情報処理学会研究報告 コンピュータセキュリティ．**2003**，74，p.91－96．

(5) 今野　徹．HTTPリクエストの未知攻撃検知における精度向上．情報処理学会研究報告 コンピュータセキュリティ．**2004**，22，p.121－126．

(6) T.Konno, M.Tateoka.“Accuracy Improvement of Anomaly-Based Intrusion Detection System Using Taguchi Method”. Proceedings of SAINT2005 workshop. Trento, Italy, 2005-01, IEEE Computer Society. p.90－93.

今野　　徹　KONNO Toru

東芝ソリューション（株）プラットフォームソリューション事業部 要素技術開発部主任。ネットワークセキュリティ技術の開発に従事。情報処理学会会員。技術士（情報工学部門）。
Toshiba Solutions Corp.

楯岡　正道　TATEOKA Masamichi

東芝ソリューション（株）プラットフォームソリューション事業部 要素技術開発部主任。ネットワークセキュリティ技術の開発に従事。情報処理学会会員。
Toshiba Solutions Corp.