Webサーバへの攻撃の検知・防御技術とMAGNIA$_{TM}$ 2000Ri/Anti-Hackerへの適用

Application of Intrusion Detection and Prevention Technology to MAGNIA$_{TM}$ 2000Ri/Anti-Hacker System

進藤　修一　■ SHINDO Shuichi
吉村　政彦　■ YOSHIMURA Masahiko
菅野　伸一　■ KANNO Shinichi

インターネットの普及により，Webサーバは企業・組織における情報発信やサービス・業務を行ううえで必要不可欠なものとなっている。しかし，一方でサーバへのサービス妨害，不正アクセスによるWebページの改ざんやデータの流出などの被害も増加している。

東芝はこれらの問題に対するソリューションとして，Webサーバへの攻撃を検知し防御するMAGNIA$_{TM}$ 2000Ri/Anti-Hackerを他社に先駆けて開発し，提供している。この製品を使用することにより，簡単にWebサーバのセキュリティを高めることができる。

Due to the diffusion of the Internet, Web servers now play an indispensable role in the transmission of information and the execution of business and services by companies and other organizations. At the same time, damage caused by illegal access, such as denial of service (DoS) to servers, alteration of Web pages, and leakage of data, is also increasing.

Toshiba has developed the first product to solve these problems, the MAGNIA$_{TM}$ 2000Ri/Anti-Hacker system, which can detect such attacks and defend a Web server from them, and has been supplying it to the market. Users can easily enhance the security of a Web server using this product.

1　まえがき

今日，インターネットの普及・拡大によって，Webサーバは企業・組織における情報発信やサービス・業務を行ううえで重要な役割を担っている。このWebサーバが不正アクセスにより誤った情報を発信したり，攻撃によってサービスが提供できなくなると，企業・組織の信用低下のほか，ビジネスとして重大な損失となる場合もある。

MAGNIA$_{TM}$ 2000Ri/Anti-Hacker（以下，Anti-Hackerと略記）は，サーバ管理者のセキュリティ管理の手間を軽減するために，Webサーバへの攻撃を検知するだけではなく，防御が可能な製品として開発したものである。また，導入や保守を容易に行えるようにハードウェアとソフトウェアを一体にしたアプライアンスサーバ（専用機）として提供している（**図1**）。

Anti-Hackerの特長は，攻撃の防御を行えるように従来の侵入検知システム（IDS：Intrusion Detection System）のようなネットワーク傍受型ではなく，インライン型を採用している点にある（**図2**）。

ここでは攻撃のタイプとAnti-Hackerに適用した攻撃の検知・防御技術について述べる。

図1．MAGNIA$_{TM}$ 2000Ri/Anti-Hackerの外観― 1U（高さ約4.45 cm）サイズのラックマウント型筐体（きょうたい）を採用している。
MAGNIA$_{TM}$ 2000Ri/Anti-Hacker system

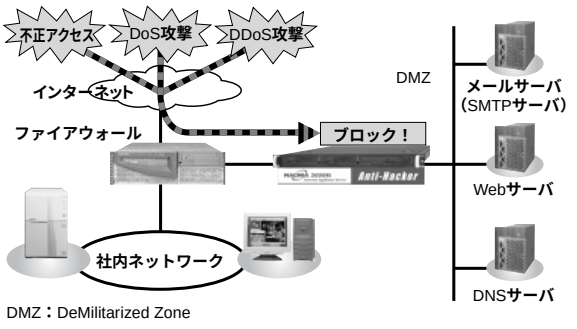

図2．Anti-Hackerの使用環境― Webサーバの前にインライン型で置かれる。
Installation environment of Anti-Hacker system

2　攻撃のタイプ

Webサーバに対する攻撃は以下の三つに分けられる。

(1)　不正アクセス　　Webサーバの基本ソフトウェア（OS）やWebアプリケーションに存在するセキュリティの脆弱（ぜいじゃく）性（セキュリティホール）を利用して，情報を不正に入手したり情報の改ざんを行う。脆弱性の内

容によってはサーバ上で任意のコマンドを実行することや，OSやWebアプリケーションをダウンあるいはロックさせることも可能である。

⑵ DoS（Denial of Service：サービス妨害）攻撃　大量のリクエストをサーバに集中させてサーバのサービス能力を低下させる攻撃である。

⑶ DDoS（Distributed DoS：分散型サービス妨害）攻撃　複数の踏み台サーバを利用し，複数箇所から一斉にDoS攻撃を行い，サーバのメモリ資源やCPU資源を枯渇させてサーバを過負荷状態にする攻撃である。

3 不正アクセスの防御方法

3.1 不正アクセスの検知手順

Anti-Hackerは，入力パケットについて，下記の手順で検査を行い不正なパケットを検知する。

⑴ サイズの検査　パケットのヘッダ部に記されているデータのサイズ情報と実際のデータのサイズが異なるような不正なパケットを検知する。

⑵ IP（Internet Protocol）アドレスの検査　送信元アドレスとあて先アドレスが同じ，送信元アドレスがブロードキャストアドレスといった不正なアドレスのパケットを検知する。

⑶ IPフラグメントの再構成　IPでは，パケットを複数のフラグメントに分割して送ることを許している。

不正アクセスのパケットが複数に分割されると，一つのパケットだけでは，それが不正であるか否かを判断することはできない。したがって，分割されている場合には，いったん元の状態に再構成してから検査する。

また，ping-of-deathと呼ばれるOSのフラグメント再構成のバグを突く攻撃もここで検査する。

⑷ TCP/UDP（Transmission Control Protocol/User Datagram Protocol）プロトコル解析　HTTP（HyperText Transfer Protocol），SMTP（Simple Mail Transfer Protocol），DNS（Domain Name System）のプロトコルを解析し，リクエストを再構成する。

長いデータをTCPで送る場合，データは複数のセグメントに分かれて送られる。したがって，攻撃が複数のセグメントにまたがっていると，フラグメントの場合と同様に，単独のセグメントでの比較による検査では不十分である。そのため，各セグメントをつなげてTCPストリームを再構成する。

⑸ シグネチャとの比較　不正アクセス，DoS攻撃のパケットのパターンを記したシグネチャをパターンファイルと呼ぶデータベースとして持ち，入力パケットとシグネチャとを比較し，不正なパケットを検知する。

Anti-Hackerは，不正なパケットを検知すると，直ちにそのパケットを破棄してサーバにそのパケットが届かないようにしている。したがって，不正アクセスをリアルタイムに防御できる。また，TCPの場合，サーバにリセットパケットを送り，リソースの早期解放を促してサーバのリソース枯渇を防いでいる。

この不正アクセスの検査は，Anti-Hacker を通過するパケットだけでなく，Anti-Hacker 自身へのパケットに対しても行っているため，Anti-Hacker 自身をも防御している。

3.2 IDS欺瞞への対応

近年，IDSが使われ始めたのに対抗し，IDSの目をかいくぐる手法も現れてきている。ここでは，IDS欺瞞（ぎまん）の手法とAnti-Hackerでの対策を述べる。

⑴ リクエストをエスケープしてパターンマッチを回避

HTTPの仕様では，任意の文字を%XX（XXはASCII コードの16進表現）という形式でエスケープすることを許している。これは通常，リクエストにおいて特別な意味を持った文字を単なる文字として使いたいときに使うものである（例えば，'|'は%7c，'&'は%26となる）。

攻撃者はこれを利用し，不正なアクセスを構成する文字列をエスケープして，パターンマッチを行っているIDSを欺瞞しようとする。

Anti-Hackerでは，リクエストのエスケープされた文字を元に戻した後，パターンマッチを行うことで，このように細工された攻撃も検知可能になっている。

⑵ フラグメントの重複を利用しての欺瞞　フラグメントは，データの重複も許されている。複数のフラグメントの重複部分は，元は一つのパケットであり同じ内容のはずであるが，攻撃者は，重複部分に別のパターンを入れることでIDSを欺瞞しようとする。

重複のあるフラグメントの再構成において，重複部分をどのフラグメントから再構成するかは実装に依存している。つまり，重複部分の内容が異なる場合，どのフラグメントの内容が有効になるか一意には決まらない。

例えば，mailto="|cat /etc/passwd"という不正アクセスパターンを二つのフラグメントに分ける場合を考える。一つのフラグメント（A）にはmailto="foo@123bar.comという内容を入れ，もう一つのフラグメント（B）には，|cat /etc/passwd"という内容を入れたフラグメントを作成する。

フラグメントの重複部分は，本来同じ内容のはずなので，どちらのデータを使ってもよいはずである。OSによって（B）に（A）を上書きする場合，（A）に（B）を上書きする場合の両方がありうる。前者の場合，不正アクセスにはならないが，後者の場合には不正アクセスとなる（**図3**）。

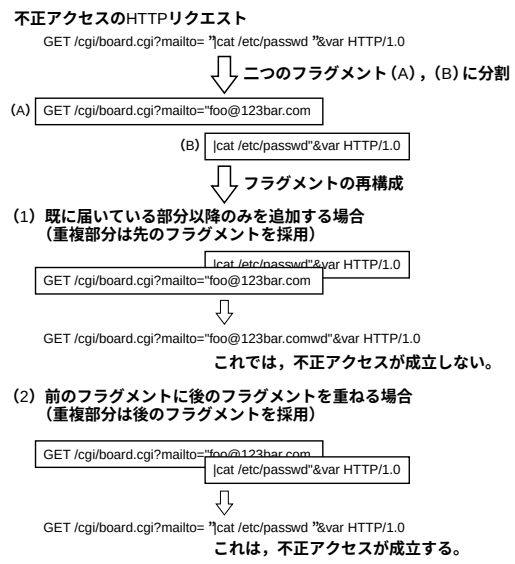

図3．重複フラグメントの再構成 ― 重複部分が異なる場合，どのフラグメントの内容を使うかによってできあがりが異なる。
Reassembly of overlapping fragments

組み合わせのすべてを検査しなければ，攻撃を検知できないことになるが，三つ四つと多くのフラグメントに分けられていた場合，すべての組合せを再構成して検査するのは現実的ではない。

Anti-Hackerでは，本来は一つのパケットであり，重複部分は同じ内容であるという点に着目し，重複部分に相違がないかだけを調べる。相違がある場合にはIDS欺瞞を試みていると判断し，不正アクセスとして検知する。

⑶ TCPセグメントの重複を利用しての欺瞞　　TCPでは，ストリームデータを複数のセグメントで送ることができる。

TCPセグメントもフラグメントの場合と同様に，複数のセグメントでデータが重複する可能性がある。

この場合もフラグメントの場合と同様に，重複部分の相違の検査を行い，相違がある場合を不正アクセスとして検知する。

⑷ IDSを過負荷状態にしての欺瞞　　意図的にIDSに検知されうるいろいろな攻撃パケットを大量に送り，IDSの負荷を上げて，本来の攻撃パケットを隠ぺいしようとする。

ネットワーク傍受型IDSの場合，自身の負荷が上がりすぎると，パケットのすべてを取り込むことができなくなり，パケットの一部を取りこぼし始める。その結果，攻撃者が本来意図した攻撃パケットを見過ごし，攻撃が達成されてしまう。

Anti-Hackerはインライン型であり，サーバに届くパケットはすべてAnti-Hackerを通過するので，原理的にパケットの見過ごしはありえない。つまり，Anti-Hackerに対しては，この手法によるIDSの欺瞞は効果がない。

4 DoS攻撃／DDoS攻撃の防御方法

DoS攻撃とDDoS攻撃は攻撃の本質が同じであるため，以下，DDoS攻撃の防御方法に的を絞って説明する。

4.1 DDoS攻撃とは

DDoS攻撃とは特定のサーバやネットワークに対して複数箇所から大量のパケットを送り，サーバやネットワークを資源的に飽和させ，ユーザーに対してのサービスに障害をもたらす攻撃である。この攻撃はOSやサーバのソフトウェアに欠陥がない場合でも成立して多大な被害をもたらすため，注意が必要である。

サーバに対してのDDoS攻撃は，サーバのメモリ資源を浪費させることが極めて効果的であるのでしばしば行われている。このような攻撃のうち，もっとも代表的なのがSYN floodと言われる攻撃である。この攻撃は，Webサーバで利用されるTCPプロトコルのうち，接続開始要求だけを，接続元のIPアドレスやポート番号を変化させながらサーバに大量に送りつける攻撃である。この攻撃は接続元のIPアドレスが正当なものである必要がないので，攻撃元の隠ぺいが比較的容易である。また，攻撃元で必要な資源も少ないことから，成功すると極めて効果の高い攻撃となる。

サーバはこのような攻撃を受けると，接続要求だけでは攻撃か正当なユーザーかを判別できないので，接続要求応答を行うと同時に，接続を管理するためのリソースやサーバのサービスを行うためのメモリ資源をサーバ内部で確保する。しかしながら攻撃の場合は，正当なアクセスなら後に続くはずのパケットが来ないため，サーバは資源を確保しておいたままの状態を長時間続けることになる。そのため，サーバは資源を攻撃によって食いつぶされてしまい，正当なユーザーに対するサービスができなくなってしまう。

近年は，接続要求だけ送られて来たものに関しては，資源管理を工夫することによりこのような障害が起きないように対策されたOSも使われてきているが，未対策OSを利用する場合には，このような接続要求を通さないような保護装置が必要になる（**図4**）。

また，この攻撃を一歩進めた攻撃も考えられる。接続元のIPアドレスを偽ることはできなくなるが，TCPによる接続処理を行った後にサーバにデータの要求を送らずに放置するという攻撃である。この攻撃に対する対策は通常であればサーバソフトウェア側で行う必要があるが，現在のところサーバソフトウェアでの対策は困難である。

この攻撃はSYN floodではないため，SYN flood対策を行ったとしても攻撃によりサーバのサービスが妨害されてしまう。

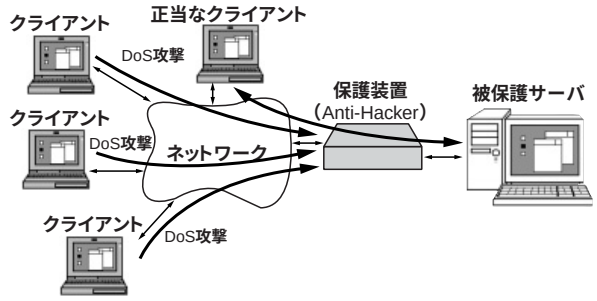

図4．DDoS攻撃防御機能 ― 正当なアクセスのみをWebサーバへ通過させる。
Distributed denial of service (DDoS) attack defending function

4.2 DDoS攻撃防御技術

このAnti-Hackerでは，攻撃の影響が極めて深刻な接続状態を放置するタイプの攻撃を防御できることを念頭に開発を行った。

このAnti-Hackerは，ネットワークとサーバの間に保護装置として配置することを前提に，クライアントからサーバへの接続要求パケットを途中で横取りして，TCPの接続処理をサーバに成り代わって行い，以後，クライアントとの接続を確立し，クライアントからのデータ要求を受領するまでの処理をサーバと同様に行う。そして，クライアントからのデータ要求の内容を検査し，DDoS攻撃かどうかを判断する。そして，攻撃ではないと判断できたものだけに関して，今度はサーバとの間でクライアントのふるまいを模擬して接続処理を行い，クライアントからのデータ要求をサーバに伝達する。そして，それが終了した時点でサーバとクライアントの通信を中継する動作に移行し，それをデータ伝送終了まで継続する。これにより，正当なアクセスについては，通常どおりのサービスを可能としている。

一方，攻撃を意図したアクセスについては，Anti-HackerでDDoS攻撃と判定されるか，判定に至る前にアクセスが止まるかのいずれかである。攻撃と判定されたものについてはその時点で接続に関する情報を消去し，以後のアクセスを遮断する。判定前にアクセスが止まったものはサーバにそのアクセス情報は伝達されないので，サーバは完全にこれらの攻撃から保護されることになる。

なお，保護装置のDDoS攻撃に対する耐性を完全にするため，回線速度に対して十分大きな接続管理資源を用意する。また，新規アクセス要求が届いたときに，保護装置の管理資源の利用量を調査し，一定量を超えていた場合にはもっとも古いアクセス停止状態の情報を消去することによって，安全性を確保している。

5 あとがき

以上述べてきたように，MAGNIA$_{TM}$2000Ri/Anti-Hackerは，高度な独自のセキュリティ技術を適用したセキュリティアプライアンス製品であり，攻撃の検知・防御技術では他社の同様製品を大きくリードしている。

Anti-HackerをWebサーバの前に入れるだけで簡単にWebサーバのセキュリティを高めることができ，ホームページの改ざんやサービス妨害などを防ぐことができる。

進藤　修一　SHINDO Shuichi
e-ソリューション社　プラットフォームソリューション事業部　ソフトウェア開発担当主務。ネットワークソフトウェアの開発に従事。情報処理学会会員。
Platform Solutions Div.

吉村　政彦　YOSHIMURA Masahiko
e-ソリューション社　プラットフォームソリューション事業部　要素技術開発担当主務。ネットワークセキュリティソフトウェアの開発に従事。情報処理学会会員。
Platform Solutions Div.

菅野　伸一　KANNO Shinichi
研究開発センター　コンピュータ・ネットワークラボラトリー研究主務。計算機アーキテクチャー，計算機ネットワークなどの研究に従事。IEEE，電子情報通信学会，情報処理学会会員。
Computer & Network Systems Lab.