(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-187701
(P2008-187701A)
(43)公開日　平成20年8月14日(2008.8.14)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/66	(2006.01)	H04L	12/66	B	5B089
H04L 12/46	(2006.01)	H04L	12/46	E	5B285
G06F 13/00	(2006.01)	G06F	13/00	351Z	5K030
G06F 21/20	(2006.01)	G06F	15/00	330A	5K033

審査請求 未請求　請求項の数 2　ＯＬ　（全 15 頁）

(21)出願番号　特願2007-226724 (P2007-226724)
(22)出願日　平成19年8月31日 (2007.8.31)
(31)優先権主張番号　特願2007-184 (P2007-184)
(32)優先日　平成19年1月4日 (2007.1.4)
(33)優先権主張国　日本国 (JP)

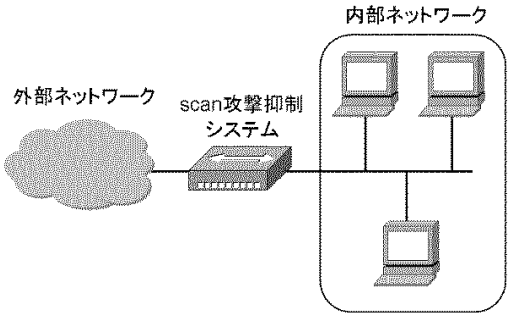
(71)出願人　304028726
国立大学法人　大分大学
大分県大分市大字旦野原７００番地
(72)発明者　吉田　和幸
大分県大分市大字旦野原７００番地
国立大学法人大分大学工学部内
(72)発明者　南　浩一
大分県大分市大字旦野原７００番地
国立大学法人大分大学工学部内

Ｆターム(参考)　5B089 HA10 KA17 KB04 KB13 MC08
5B285 AA05 AA06 BA01 CA32 CA34 DA05

最終頁に続く

(54)【発明の名称】スキャン攻撃不正侵入防御装置

(57)【要約】
【課題】不正侵入の試みの初期のスキャン攻撃段階で、不正に侵入しようとするパケットを検知し、侵入を未然に阻止することができるスキャン攻撃不正侵入防御装置を提供する。
【解決手段】スキャン攻撃検知の判定基準を設定しこれらを調整して、セキュリティレベルの低いPCを探したり、PCのセキュリティ上の欠陥を探すために多数のPCやPCにある多数のアプリケーションに対して通信開始要求を送ってくる（スキャン攻撃）パケットが使用するTCPコネクションを検知し、このTCPコネクションへの応答時間を選択的に遅くすることで攻撃の進行を遅らせることを用いて攻撃を抑制するスキャン攻撃不正侵入防御装置。
【選択図】図１



【特許請求の範囲】
【請求項１】
インターネット側から受信したパケットについて、予め登録してある信頼できる送信元及び適用外のアプリケーション（宛先ポート番号）であれば、後記の送信部にそのパケットを送信するよう指令し、それ以外のときは、判定部に送る受信・解析部と、
前記受信・解析部からのパケットが通信開始要求パケット（SYN）であれば、送信元IPアドレスを抽出し、後記のデーターベースに記録しているIPアドレスの要求回数に１を加え、参照時刻を現在の時刻に修正すると共に、すべてのパケットに関して送信元IPアドレスを抽出し、データーベースからそのIPアドレスに対応する要求回数を検索し、その要求回数に応じて遅延時間を計算し、前記現在の時刻と遅延時間に基づき送出時刻を算出し、当該パケットとともに送信部に送る判定部と、
前記受信・解析部から来た送出時刻がないパケットについては、すぐに送信し、判定部から来た送出時刻が指定されたパケットに関しては、送出時刻まで待機したのち送出する送信部と、
前記送信部から送出されたパケットと送出時刻を記憶し、これらについて、あらかじめ設定した所定時間間隔で、データーベース中に記録している各パケットのIPアドレスの参照時刻を検査し、参照時刻から所定時間経過しても送信開始要求がないものをデーターベースから消去するデーターベースと、
からなることを特徴とするスキャン攻撃不正侵入防御装置。
【請求項２】
インターネット側から受信したパケットについて、予め登録してある信頼できる送信元及び適用外のアプリケーション（宛先ポート番号）であれば、後記の送信部にそのパケットを送信するよう指令し、それ以外のときは、判定部に送る受信・解析部と、
前記受信・解析部からのパケットが通信開始要求パケット（SYN）であれば、送信元IPアドレスを抽出し、後記のデーターベースに記録しているIPアドレスの要求回数に１を加え、参照時刻を現在の時刻に修正すると共に、
すべてのパケットに関して送信元IPアドレスを抽出し、データーベースからそのIPアドレスに対応する要求回数を検索し、その要求回数に応じて遅延時間を計算し、前記現在の時刻と遅延時間に基づき送出時刻を算出し、当該パケットとともに送信部に送ると共に、前記受信・解析部からの通信開始要求パケット（SYN）の宛先が、内部ネットワーク内の予め偽装用に登録してあるIPアドレスであれば、その偽装IPアドレスの接続許可パケット（ACK/SYN）を送信部に送信するよう指令する判定部と、
前記受信・解析部から来た送出時刻がないパケットについては、すぐに送信し、判定部から来た送出時刻が指定されたパケットに関しては、送出時刻まで待機したのち送出し、判定部から来た偽装IPアドレスの接続許可パケット（ACK/SYN）を遅延後に送信元IPアドレスに偽装送信する送信部と、
前記送信部から送出されたパケットと送出時刻を記憶し、これらについて、あらかじめ設定した所定時間間隔で、データーベース中に記録している各パケットのIPアドレスの参照時刻を検査し、参照時刻から所定時間経過しても送信開始要求がないものをデーターベースから消去するデーターベースと、
からなることを特徴とするスキャン攻撃不正侵入防御装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、インターネットからLANへのスキャン攻撃不正侵入の試みに対して早期に検知し、スキャン攻撃による不正侵入を防御する装置に関するものである。
【背景技術】
【０００２】
近年、セキュリティホールが残っている古いソフトウェアの存在等を探すスキャン攻撃や、Transmission Control Protocol（以下単にTCPと言う）の22番ポートや135番ポート

等の特定のポート狙った攻撃が後を絶たない。不正アクセスによる侵入を許すと、侵入されたコンピュータが、他のコンピュータを攻撃するための踏み台や、受信者の意図を無視して無差別かつ大量に送信される電子メール（以下単にspamと言う）の中継、フィッシング詐欺などに利用され、他のユーザやネットワークに被害を及ぼすケースもある。そのため、コンピュータの管理者は、こまめにログを監視し、攻撃元のInternet Protocol（以下単にIPと言う）アドレスに対してフィルタリングを行うなど攻撃の対策を行う必要がある。

しかし、大学のように管理者が複数存在し、研究室単位で多くのコンピュータが運用されている環境では、対策が行われないままのコンピュータが存在することや、早めの対策が行われないことがある。

＜参考文献＞

【非特許文献１】鈴木,湯浅,“ブラックリストを用いたPAM遅延モジュールによるSSHへの攻撃抑制”,情報処理学会研究報告(2006-DSM-40),pp.1-5, Mar.2006

【非特許文献２】IPAコンピュータ不正アクセス被害防止対策集, http://www.ipa.go.jp/security/ciadr/cm01.html#DoS

【非特許文献３】nmap http://insecure.org/nmap/

【発明の開示】

【発明が解決しようとする課題】

【０００３】

インターネットからLAN内へのスキャン攻撃不正侵入を阻止するために従来は、その接続点にFireWallを設置し、その中で種々の方法で不正侵入を検知・阻止することを推進してきたが万全ではなく種々の問題を有する。

既存のスキャン攻撃の対策方法には、例えばパケットフィルタリングやIDS（Intrusion Detection System, 侵入検知装置）、IDP（Intrusion Detection & Prevention System, 侵入検知防御装置）が知られている。これらは、不正なパケットのデータをあらかじめパターンファイルとして保持し、すべてのパケットとそのデータを比較することでスキャン攻撃してきた不正パケットを検知して通信をブロックするものであるが、これでは攻撃を受けた後の処置となり被害もでる場合が多い。

本発明は不正侵入の試みの初期のスキャン攻撃段階で、不正に侵入しようとするパケットを検知し、侵入を未然に阻止することができるスキャン攻撃不正侵入防御装置を提供するものである。

【課題を解決するための手段】

【０００４】

即ち、本発明のスキャン攻撃不正侵入防御装置は、図１に示すように、外部ネットワークと内部ネットワークLANとの境界に透過型ブリッジとして動作する装置として設置するものでありその構成は、受信・解析部100、判定部200、送信部300の3つの部分と判定部200が参照するデーターベース400からなるものであり、それらの特徴とする技術手段は次の(１)～(２)のとおりである。

【０００５】

(１)インターネット側から受信したパケットについて、予め登録してある信頼できる送信元及び適用外のアプリケーション（宛先ポート番号）であれば、後記の送信部300にそのパケットを送信するよう指令し、それ以外のときは、判定部200に送る受信・解析部100と、

前記受信・解析部100からのパケットが通信開始要求パケット（SYN）であれば、送信元IPアドレスを抽出し、後記のデーターベース400に記録しているIPアドレスの要求回数に１を加え、参照時刻を現在の時刻に修正すると共に、すべてのパケットに関して送信元IPアドレスを抽出し、データーベース400からそのIPアドレスに対応する要求回数を検索し、その要求回数に応じて遅延時間を計算し、前記現在の時刻と遅延時間に基づき送出時刻を算出し、当該パケットとともに送信部300に送る判定部200と、

前記受信・解析部100から来た送出時刻がないパケットについては、すぐに送信し、判定

部200から来た送出時刻が指定されたパケットに関しては、送出時刻まで待機したのち送出する送信部300と、
前記送信部300から送出されたパケットと送出時刻を記憶し、これらについて、あらかじめ設定した所定時間間隔で、データーベース中に記録している各パケットのIPアドレスの参照時刻を検査し、参照時刻から所定時間経過しても送信開始要求がないものをデーターベースから消去するデーターベース400と、
からなることを特徴とするスキャン攻撃不正侵入防御装置。
(２)インターネット側から受信したパケットについて、予め登録してある信頼できる送信元及び適用外のアプリケーション（宛先ポート番号）であれば、後記の送信部にそのパケットを送信するよう指令し、それ以外のときは、判定部に送る受信・解析部と、
前記受信・解析部からのパケットが通信開始要求パケット（SYN）であれば、送信元IPアドレスを抽出し、後記のデーターベースに記録しているIPアドレスの要求回数に１を加え、参照時刻を現在の時刻に修正すると共に、
すべてのパケットに関して送信元IPアドレスを抽出し、データーベースからそのIPアドレスに対応する要求回数を検索し、その要求回数に応じて遅延時間を計算し、前記現在の時刻と遅延時間に基づき送出時刻を算出し、当該パケットとともに送信部に送ると共に、前記受信・解析部からの通信開始要求パケット（SYN）の宛先が、内部ネットワーク内の予め偽装用に登録してあるIPアドレスであれば、その偽装IPアドレスの接続許可パケット（ACK/SYN）を送信部に送信するよう指令する判定部と、
前記受信・解析部から来た送出時刻がないパケットについては、すぐに送信し、判定部から来た送出時刻が指定されたパケットに関しては、送出時刻まで待機したのち送出し、判定部から来た偽装IPアドレスの接続許可パケット（ACK/SYN）を遅延後に送信元IPアドレスに偽装送信する送信部と、
前記送信部から送出されたパケットと送出時刻を記憶し、これらについて、あらかじめ設定した所定時間間隔で、データーベース中に記録している各パケットのIPアドレスの参照時刻を検査し、参照時刻から所定時間経過しても送信開始要求がないものをデーターベースから消去するデーターベースと、
からなることを特徴とするスキャン攻撃不正侵入防御装置。
つまり、本発明のスキャン攻撃不正侵入防御装置は、スキャン攻撃検知の判定基準を設定しこれらを調整して、セキュリティレベルの低いPCを探したり、PCのセキュリティ上の欠陥を探すために多数のPCやPCにある多数のアプリケーションに対して通信開始要求を送ってくる（スキャン攻撃）パケットが使用するTCPコネクションを検知し、このTCPコネクションへの応答時間を選択的に遅くすることで、攻撃の進行を遅らせること（以下単にthrottlingと言う）を用いて攻撃を抑制するものである。
さらに、本発明のthrottlingを用いたスキャン攻撃抑制システムでは、パケットに遅延を設けたとしても攻撃者に対して必ず正常に応答しているため、結果としてネットワーク内で動作しているホストの情報を調べるというスキャン攻撃の目的達成に貢献している状況にある。そこで、throttlingを用いたスキャン攻撃抑制システムの利点を継承しながら、“外部ネットワークに対してホストの存在を隠蔽する”ことを指針とした偽装応答という機軸を追加するものである。
【発明の効果】
【０００６】
本発明のスキャン攻撃不正侵入防御装置は、ネットワーク単位でスキャン攻撃や不正アクセスを抑制する装置であり、設置場所を選ばない透過型ブリッジとして動作するため、図１に示す如く、外部ネットワークと内部ネットワークの境界に設置することができる簡便なものである。
即ち本発明の不正侵入防御装置は、インターネットなどの外部ネットワークから内部ネットワークLANへの不正侵入を試みる前に、セキュリティレベルの低いパーソナルコンピューター（以下単にPCという）を探したり、PCのセキュリティ上の欠陥を探すために多数のPCやあるPCの多数のアプリケーションに対して通信開始要求を送ってくること（スキャ

ン攻撃）を検知し、応答時間を遅くすることで、侵入の試みをあきらめさせることができるものである。これでセキュリティ上の脆弱性（セキュリティホール）が発見されたときに、問題の存在自体が広く公表される前にその脆弱性を悪用して行なわれる攻撃（ZeroDay攻撃）等の未知の攻撃に対してもまずスキャン攻撃から始まると考えられるので、本発明の効果が期待できる。

また攻撃検知の判定基準を調整することにより、1台のPCから発せられるスキャン攻撃ばかりでなく、外部のワーム等に感染したPCから同時に1台のPCにアクセスが集中するDDoS（distributed denial of service）攻撃にも対応することができる。

さらに、本発明の不正侵入防御装置は、インターネットなどの外部ネットワークから内部ネットワークLANへの不正侵入を試みる前に、セキュリティレベルの低いPCを探したり、PCのセキュリティ上の欠陥を探すために多数のPCやあるPCの多数のアプリケーションに対して通信開始要求を送ってくること（スキャン攻撃）を検知し、偽装応答を行うことで、攻撃者のターゲットホストを防御対象ネットワークから排除することができるものである。同時にスキャン攻撃を実在しないホストへと誘導することは、内部ネットワークのホストの存在をスキャン攻撃により確認するまでの時間を延長させることができるものである。

また、スキャン攻撃の際に使用されるTCPコネクションを検知し、TCPコネクションへの応答を選択的に遅くするthrottlingと併用することによりスキャン攻撃後のパスワードクラッキングなどの攻撃に対して対策を行うことが可能になる。

【発明を実施するための最良の形態】

【０００７】

＜スキャン攻撃の抑止＞

通常、ネットワークやコンピュータに不正アクセスが行われる前にはスキャン攻撃が行われることが多い。スキャン攻撃を許すと、攻撃者にネットワークやコンピュータの情報を与えることになる。攻撃者に情報を与えることは精度の高い攻撃につながることになるため、スキャン攻撃を防ぎ情報を提供しないことが不正アクセスを防ぐ上で重要である。また、早い段階でスキャン攻撃を検知することにより、攻撃が行われる前に対策を行うことが可能となる。

本発明装置は、スキャン攻撃の際に使用されるTCPコネクションを検知し、TCPコネクションへの応答を選択的に遅くするthrottlingを用いてスキャン攻撃を抑制する。また、本発明装置は、throttlingを用いたスキャン攻撃抑制システムの利点を継承しながら、“外部ネットワークに対してホストの存在を隠蔽する”ことを指針とした偽装応答という機軸を追加してスキャン攻撃を抑制する。Throttlingや偽装応答を用いることにより、次の効果を期待できる。

（１）スキャン攻撃自体を断念させる

（２）攻撃終了までの時間を長くする

（３）攻撃者のターゲットホストを防御対象ネットワークから排除できる

偽装応答を行うことにより、（３）の効果と同時にスキャン攻撃を実在しないホストへと誘導することは、内部ネットワークのホストの存在をスキャン攻撃により確認するまでの時間を延長させることができる。

以上のように、遅延をかけることにより、攻撃者がスキャン攻撃を諦めることを目的とする。Secure Shell（以下単にSSHと言う）によるパスワードクラッキング攻撃において、遅延をかけることで攻撃を断念されることができている（非特許文献１）。スキャン攻撃に対しても攻撃抑止の効果を期待できる。スキャン攻撃終了までの時間を長くすることで、その間に対策を行うことができる。

つまり前記した従来法が不正パケットを検知して通信をブロックするものであるのに対して本発明は、スキャン攻撃への反応を遅らせることに違いがある。

そこで本発明を実施するための最良の形態を、以下の実施例１と実施例２により、図２～図８及び表１、表２と共に詳細に説明する。

【実施例１】

【０００８】
先ずTCP接続を開始するとき、クライアントからサーバへSYNフラグを立てた通信開始要求パケットを送る。それに対して、サーバはSYNフラグとACKフラグを立てた要求確認パケットで応答し、さらにクライアントからACKフラグのみのパケットを送って通信開始手順が終了する。通常の通信では、この後、クライアント・サーバ間でデータの授受が行なわれる。
スキャン攻撃では、脆弱なサーバを見つけるため、あるクライアントから多数のサーバに向かってほぼ同時に通信開始要求パケットが送られる。
本実施例の装置のソフトウェアは、受信・解析部100、判定部200、送信部300の3つの部分と判定部が参照するデーターベース400からなる。
実施例１は、スキャン攻撃の際に使用されるTCPコネクションを検知し、TCPコネクションへの応答を選択的に遅くするthrottlingを用いてスキャン攻撃を抑制するものである。（図３参照）
【０００９】
1. 本実施例１のスキャン攻撃不正侵入防御装置におけるthrottlingのアルゴリズムについて
1.1 概要
スキャン攻撃はツールを用いて自動的に実行されることが多く、大抵は１つのIPアドレスから行われている。また、多くのTCPコネクションを短時間で試行する。そこで、同じIPアドレスからのTCPコネクションの開始を検知するたびに、その送信元IPアドレスに対して遅延を増加させていく。つまりTCPコネクション試行回数に応じて遅延をかけていく。これによりTCPコネクションを使用するスキャン攻撃に対してthrottlingを行う。
1.2 考慮点
TCPコネクションの試行回数から遅延時間を決定するときに次の3点について考慮する。
1.2.1 正規の利用者
SSHで、パスワードの入力を間違えるなど、正規の利用者もTCPコネクションを数回繰り返すころがある。TCPコネクションの試行回数に応じて遅延を増加させる方法だと、正規の利用者にも大きな遅延をかける可能性がある。このため、しきい値を導入する。TCPコネクション試行回数のしきい値を定め、それを超えない回数までは遅延の増加量を小さなものとする。TCPコネクション試行回数がしきい値を越えたならば、スキャン攻撃だと判断し、遅延の増加量を大きくしていく。一定時間、TCPコネクションが志向されなかったものについては、その試行回数を0にリセットする。
1.2.2 多くのTCPコネクションの試行を必要とするプロトコル
プロトコルの中には、多くのTCPコネクションを利用するものもある。HyperText Transfer Protocol（以下単にHTTPと言う）（80番）などが該当する。これらのプロトコルに関しては、遅延を行わないようにすることで解決を図る。throttlingの対象としないあて先ポート番号を記録する除外ポート番号リスト（ポート番号white listという）を作成する。TCPコネクションのあて先ポート番号がポート番号white listに該当する場合にはthrottlingを行わない。
1.2.3 信用できるホスト、公開されているサーバ
正規利用者がよく使うホストで、セキュリティ管理がきちんと行われているものからのTCPコネクション要求や、公開されているサーバで攻撃に対する対策をサーバ自身できちんと行っているものへのTCPコネクション要求に関しては、遅延をかける必要はない。これらのホスト、サーバのIPアドレスを記録する除外IPアドレスリスト（IPアドレスwhitelistという）を作成する。TCPコネクションの送信元あるいは宛先のIPアドレスがIPアドレスwhite listに該当する場合にはthrottlingを行わない。
1.3 遅延アルゴリズム
以上により、遅延アルゴリズムは以下のようになる。
(1)インターネット側からのパケットを１つ受け取る。
(2)パケットの送信元アドレス、宛先アドレス、宛先ポートのいずれかがポート番号white

list、IPアドレスwhite listにある、あるいは、プロトコルフィールドがTCP以外のときは、遅延なしの内部キューに置き、(1)へ戻る。
(3)パケットがTCPコネクション開始パケット(SYN=1, ACK=0)のとき、送信元アドレス、宛先アドレスそれぞれの試行回数、遅延時間を更新する。
(4)送信元アドレスに対する遅延時間、宛先アドレスに対する遅延時間を検索し、後述の関数例１～３によりパケットの遅延時間とする。
(5)送出時刻＝現在時刻＋遅延時間を計算し、パケット自身とともにヒープに置く。ヒープとは、パケットとその送信時刻とを蓄え、送信可能時刻が来るたびに送信部にパケットを渡す手段をいう。
(6)内部／外部の２つの送信部では、それぞれ「１」、「３」のキューを調べてパケットがあれば、すぐに送信し、さらに内部送信部では「５」のヒープ中にある一番古いパケットが送出時刻になって入れば送出する。
(7)あらかじめ設定した時間間隔（30分程度）で、データベース中に記録している各IPアドレスの参照時刻を検査し、参照時刻が古いもの（１時間程度送信開始要求がないもの）は、データベースから消去する。
ただし、LANからインターネットに向かうパケットに関しては、すべて外部キューに置き、遅延させない。

【００１０】

2. 実装

2.1 全体構成

装置全体の流れを図２に示す。装置は一方のネットワークに流れるパケットを全て受信し、もう一方のネットワークに送信する。ただし、送信の前に、受信したパケットの解析を行い、throttlingを行うかどうかを判断する。throttlingを行う場合は、パケットに遅延をかけた後に送信を行う。

2.2 受信・解析部100

ここでは受信したパケットにthrottlingを行うかを判断するために、表１、表２に示す例のように、パケットを解析し、解析結果を保存しておく。
まず、パケットを受信し、TCPヘッダ、IPヘッダの解析を行う。本装置で使用するものは、送信元IPアドレス、宛先IPアドレス、宛先ポート番号、TCPコントロールフラグビット、到着時刻の情報である。解析結果の保存では送信元IPアドレス毎および宛先IPアドレス毎に到着時刻とTCPコネクション試行回数を保存していく。到着時刻は最終アクセス時刻として使用する。TCPコントロールフラグビットのSYNフラグが１、ACKフラグが0である場合に、TCPコネクションが試行されたものとしてカウントを行う。既にIPアドレスの情報が保存されている場合には、回数、アクセス時刻の更新を行う。
解析結果をいつまでも保持していると、正規のユーザのTCPコネクションの試行回数がしきい値を超えるという問題が発生する。そのため、定期的に保存している情報を整理する。送信元IPアドレスにおいては、一定周期で、保存されている各IPアドレスの最終アクセス時間と現在時間を比較し、一定時間更新が無いアドレスの情報を破棄する。宛先IPアドレスにおいては一定周期で全ての情報を破棄する。

【００１１】

【表１】

送信元IPアドレス別の情報

IPアドレス	TCPコネクション試行回数	最終アクセス時間（到着時間）
133.37.xxx.112	16	20061010 03:00:56
133.37.yyy.213	8	20061010 03:48:33
133.37.zzz.154	5	20061010 03:50:12

⋮

【００１２】
【表２】

宛先IPアドレス別の情報

IPアドレス	TCPコネクション試行回数	最終アクセス時間（到着時間）
133.37.56.xxx	10	20061010 03:48:20
133.37.56.yyy	7	20061010 03:50:33

2.3　判定部200

判定部200では、受信・解析部100で得られた情報からthrottlingを行うかを判断する。throttlingを行わないのは、次の３つの場合である。

＜throttlingを行わない場合＞

（１）パケットがTCPを使用していない。

（２）ポートあるいは送信元、あて先IPアドレスが、white listに該当する。

（３）宛先IPアドレスのTCPコネクション試行回数と送信元IPアドレスのTCPコネクション試行回数がともに0回である。

throttlingを行わない場合は、パケットを送信部300が持つ遅延なしの内部キューに挿入する。

throttlingを行う場合は、まず遅延時間の計算を行う。遅延時間は、宛先IPアドレスのTCPコネクション試行回数と送信元IPアドレスのTCPコネクション試行回数からそれぞれ計算された値の合計となる。それぞれの計算時間は次の例１の関数例のとおりである。

例１

遅延時間＝試行回数×α
(試行回数が閾値未満のとき)
遅延時間＝(試行回数－閾値)×β＋閾値×α
(試行回数が閾値以上のとき)

閾値、α、βの現在の値を表３に示す。

次に、得られた遅延時間を現在時刻に加算して送信時刻を求める。最後に、パケットに送信時刻を設定し、送信部300が持つ遅延キューにパケットを挿入する。

【００１３】
【表３】

	閾値	α	β
送信元アドレス	16	1.0	0.1
宛先アドレス	256	0.1	0.0

また、遅延時間は、送信元IPアドレスのTCPコネクション試行回数から計算することが

出来る。スキャン攻撃でなくても数回通信開始要求を繰り返すことは考えられるので、要求回数（TCPコネクション試行回数）が少ないうちは遅延時間を緩やかに増加させ、要求回数（TCPコネクション試行回数）が多くなると急激に大きくなるような単調増加関数として定義する。関数例として以下の例２、例３を掲げる。

例２

遅延時間＝要求回数×aミリ秒（要求回数＜10）

遅延時間＝(要求回数－9)×bミリ秒（要求回数≧10）

ただし、a＜b

例３

遅延時間＝c×2＾(要求回数－1)ミリ秒

2.4　送信部300

送信部300はパケットの送信を行う。送信するパケットはthrottlingを行うパケットと、行わないパケットの２つに分けられる。それぞれのパケットに対する送信部300の働きについて述べる。

2.4.1　throttlingを行わない場合

遅延なしの内部キューからパケットを取り出し、すぐに送信する。

2.4.2　throttlingを行う場合

パケットに遅延をかける必要があるため、装置内でパケットを保持する機能が必要となる。このため、パケットを保持する遅延用の内部キューを持つ。遅延用の内部キューには、送信時刻が設定されたパケットが挿入される。

この挿入は判定部200が行う。各パケットは送信時刻が早い順に並ぶように挿入される。送信部300は遅延用の内部キューの先頭の送信時刻と現在の時刻を比較し、送信時刻をすぎているパケットを図４に示す遅延用の内部キューから取り出し、送信を行う。

【００１４】

3.　性能評価実験

性能評価実験として、実験環境を作成し、スキャン攻撃にどの程度の効果があるかを確認した。

3.1　実験方法

攻撃用コンピュータを一方のネットワークに配置し、もう一方のネットワークに攻撃対象とするコンピュータ設置し、その間に本抑制装置を配置する。そして、ポートスキャンツールであるnmap（非特許文献３）を用いてスキャン攻撃を行う。次に、本装置を外し、再度スキャン攻撃を行う。実験環境を図４の実験用ネットワークに示す。

3.2　実験結果

実験結果のログを以下に抜粋する。ログの分量が多いため、必要のない部分は省略してある。

3.2.1　装置使用時の結果を次に記載した。

```
Starting Nmap 4.11
Initiating SYN Stealth Scan against example.csis.oita-u.ac.jp (133.37.56.xxx) [1
680 ports] at 02:07
Discovered open port 80/tcp on 133.37.56.xxx
Discovered open port 22/tcp on 133.37.56.xxx
Discovered open port 21/tcp on 133.37.56.xxx
SYN Stealth Scan Timing: About 18.07% done; ETC: 02:10 (0:02:30 remaining)
Discovered open port 2601/tcp on 133.37.56.xxx
SYN Stealth Scan Timing: About 44.61% done; ETC: 02:14 (0:03:52 remaining)
SYN Stealth Scan Timing: About 45.74% done; ETC: 02:22 (0:08:23 remaining)
SYN Stealth Scan Timing: About 59.54% done; ETC: 02:54 (0:19:11 remaining)
Warning: Giving up on port early because retransmission cap hit.
SYN Stealth Scan Timing: About 76.66% done; ETC: 03:09 (0:14:26 remaining)
```

```
Discovered open port 111/tcp on 133.37.56.xxx
SYN Stealth Scan Timing: About 98.70% done; ETC: 03:25 (0:01:00 remaining)
The SYN Stealth Scan took 4700.06s to scan 1680 total ports.
Host example.csis.oita-u.ac.jp (133.37.56.xxx) appears to be up ... good.
Nmap finished: 1 IP address (1 host up) scanned in 4700.315 seconds
Raw packets sent: 2426 (106.742KB) | Rcvd: 2432 (111.982KB)
```

3.2.2　装置非使用時の結果を次に記載した。

```
Starting  Nmap 4.11
Initiating SYN Stealth Scan against example.csis.oita-u.ac.jp (133.37.56.xxx) [1
680 ports] at 04:30
Discovered open port 22/tcp on 133.37.56.xxx
Discovered open port 80/tcp on 133.37.56.xxx
Discovered open port 21/tcp on 133.37.56.xxx
Discovered open port 2601/tcp on 133.37.56.xxx
Discovered open port 111/tcp on 133.37.56.xxx
The SYN Stealth Scan took 1.58s to scan 1680 total ports.
Host example.csis.oita-u.ac.jp (133.37.56.xxx) appears to be up ... good.
Nmap finished: 1 IP address (1 host up) scanned in 1.820 seconds
Raw packets sent: 1683 (74.050KB) | Rcvd: 1679 (77.230KB)
```

装置の非使用時は1.820秒でスキャン攻撃が終了しているのに対し、装置の使用時は、攻撃終了まで4700.315秒の時間が経過している。終了までに2500倍以上の時間がかかっている。攻撃者がscanの終了を待たずに攻撃を断念する可能性は十分考えられる。また装置が無い場合に比べて、不正アクセスの前に対策を行える可能性は高いと考えられる。

4.　まとめ

本発明は、throttlingを利用したスキャン攻撃抑制装置について述べた。スキャン攻撃を抑止することで、スキャン攻撃につづく不正アクセスを予防できると考えられる。

本装置では、TCPコネクションの開始を検知してthrottlingを行うため、FINパケットやPUSHパケットを送りつけるXmasTree スキャン攻撃などに対応していない。これらの攻撃に対してもthrottlingを行えるよう判定部200の改良が必要である。

【実施例２】

【００１５】

実施例２を図７と図８に示し、その装置の基本ソフトウェアは、図３に示す実施例１と同様に受信・解析部100、判定部200、送信部300の3つの部分と判定部が参照するデーターベース400からなる。

実施例２は、実施例１のthrottlingを用いたスキャン攻撃抑制システムの利点を継承しながら、“外部ネットワークに対してホストの存在を隠蔽する”ことを指針とした偽装応答という機軸を追加するものである。

【００１６】

1.　本発明のスキャン攻撃不正侵入防御装置における偽装応答のアルゴリズムについて

1.1　概要

本発明のthrottlingを用いたスキャン攻撃抑制システムでは、パケットに遅延を設けたとしても攻撃者に対して必ず正常に応答しているため、結果としてネットワーク内で動作しているホストの情報を調べるというスキャン攻撃の目的達成に貢献している状況にある。

そこで、実施例１のthrottlingを用いたスキャン攻撃抑制システムの利点を継承しながら、図７に示すように、“外部ネットワークの攻撃者に対して偽装のターゲットホストの存在を隠蔽し時間を掛けて偽装ホストに誘導して応答することを一回又は数回繰り返すことにより攻撃者に無駄時間と通信費を嵩ませて諦めさせる所謂偽装応答撃退という機軸を追

加するものである。

1.2 システムの構成

システムの全体の流れを図５に示す。新システムでは、throttlingシステムの利点を継承しながら偽装応答という新たな機軸を追加する。従って、throttlingシステムと内部構成はほとんど変わらない。パケットの受信を行う受信部、パケットに対してthrottling又は偽装応答の処理を行う解析・応答部、パケットを送信する送信部から構成されている。

新たに導入された解析・応答部は従来システムでthrottlingの遅延時間を決定していた解析部に偽装応答のための機構を追加定義したものである。解析・応答部は内部ネットワーク内に存在しない偽装ホストへのコネクション要求を受け取った場合、送信部へ偽装応答を行うように指示する。なお、内部ネットワークに対しては偽装応答を適用しない。

1.3 偽装応答

外部ネットワークから内部ネットワークで動作していないホスト宛のコネクション要求が到着した場合、本システムでは偽装応答を行う。具体的には図８に示すように、攻撃者からの内部ネットワーク中の存在しないホスト宛に来たSYNパケットに対して、その存在しない宛先ホストとしてACK/SYNパケットを返信してコネクションが確立可能なように振舞う。その後の攻撃者からのサービス要求に対しては一切応答しない。つまり、偽装応答は攻撃者に存在しないホストに向けて攻撃を行うように誘導するための処理である。

1.4 偽装応答を組み込んだ遅延アルゴリズム

偽装応答を組み込んだ遅延アルゴリズムは以下のようになる。

(1)インターネット側からのパケットを１つ受け取る。

(2)パケットの送信元アドレス、宛先アドレス、宛先ポートのいずれかがポート番号white list、IPアドレスwhite listにある、あるいは、プロトコルフィールドがTCP以外のときは、遅延なしの内部キューに置き、(1)へ戻る。

(3)パケットがTCPコネクション開始パケット(SYN=1, ACK=0)のとき、送信元アドレス、宛先アドレスそれぞれの試行回数、遅延時間を更新する。

(4)宛先アドレスがあらかじめ偽装応答用に設定したIPアドレスであれば、偽装応答パケットを生成して、インターネットに向かう外部キューに置き所定時間遅延させた後送信部から送信元アドレスに偽装の応答送信を行う。

(5)送信元アドレスに対する遅延時間、宛先アドレスに対する遅延時間を検索し、前述の関数例１～３によりパケットの遅延時間とする。

(6)送出時刻＝現在時刻＋遅延時間を計算し、パケット自身とともに遅延キューへ送り、(1)へ戻る。ヒープに置く。

ヒープとは、パケットとその送信時刻とを蓄え、送信可能時刻が来るたびに送信部にパケットを渡す手段をいう。

(7)内部／外部の２つの送信部では、それぞれ「１」、「３」のキューを調べてパケットがあれば、すぐに送信し、さらに内部送信部では「５」のヒープ中にある一番古いパケットが送出時刻になって入れば送出する。

(8)あらかじめ設定した時間間隔（30分程度）で、データベース中に記録している各IPアドレスの参照時刻を検査し、参照時刻が古いもの（１時間程度送信開始要求がないもの）は、データベースから消去する。

ただし、LANからインターネットに向かうパケットに関しては、すべて外部キューに置き、遅延させない。

4. まとめ

本発明は、throttlingを用いたスキャン攻撃抑制システムの運用経験に基づき、攻撃側の資源を使って十分な遅延時間を確保する偽装応答を用いたスキャン攻撃抑制システムの提案を行った。

偽装応答を行うことにより、攻撃者のターゲットホストを防御対象ネットワークから排除することができると考えられる。同時にスキャン攻撃を実在しないホストへと誘導することは、内部ネットワークのホストの存在をスキャン攻撃により確認するまでの時間を延長させることができると考えられる。また、throttlingと併用することによりスキャン攻

撃後のパスワードクラッキングなどの攻撃に対して対策を行うことが可能になる。

【産業上の利用可能性】

【００１７】

既存のファイアウォール、IDP（Intrusion Detention and Prevention System）では、あらかじめ作成されたパターンのデーターベース400を持ち、それに合致するパケットのみの侵入を阻止するが、本発明装置は、怪しい動き（多数の通信開始要求）を検知し、本装置自身がデーターベース400を構築する優れた装置である。このため本装置単体で製品化することの他、本装置のアルゴリズムを、既存のファイアウォールの中に組み込可能であるなどインターネット通信産業などに広く活用されるものである。

【図面の簡単な説明】

【００１８】

【図１】本発明装置を外部ネットワークと内部ネットワークとの関係で配置する構成を示す説明図である。

【図２】本発明装置の実施例１における概要構成を示す説明図である。

【図３】本発明装置の実施例１における基本構成部を示す説明図である。

【図４】攻撃に対する遅延処理フローを示す説明図である。

【図５】本発明装置の実施例１における送信部300においてパケットを保持する遅延キューの説明図である。

【図６】本発明装置の実施例１で紹介の実験環境の実験用ネットワークを図示する説明図である。

【図７】本発明装置の実施例２における基本構成の概要を示す説明図である。

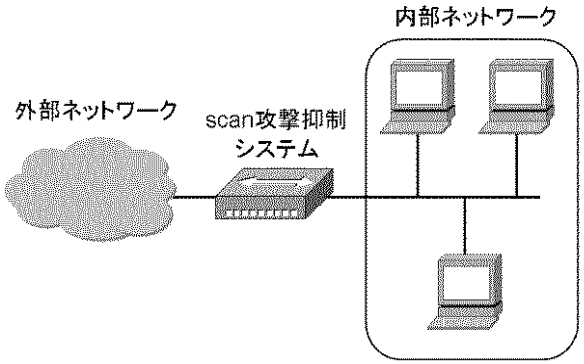
【図８】本発明装置の実施例２における概要構成を示す説明図である。

【符号の説明】

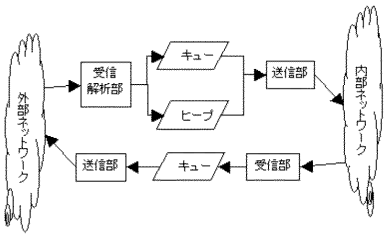
【００１９】

100　受信・解析部
200　判定部
300　送信部
400　データーベース

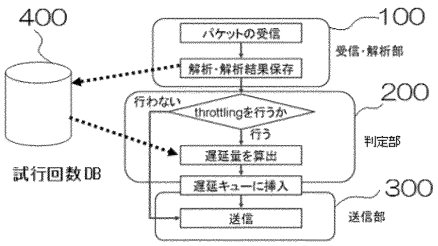
【図１】



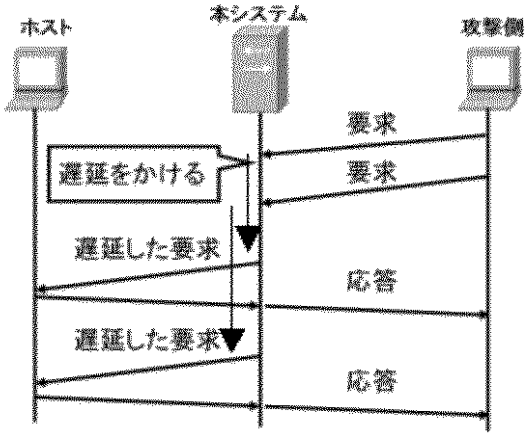
【図２】



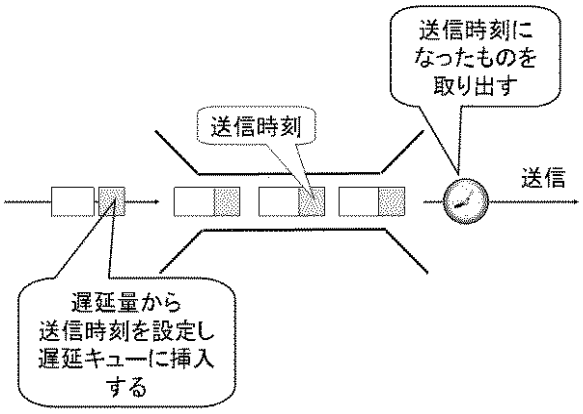
【図３】



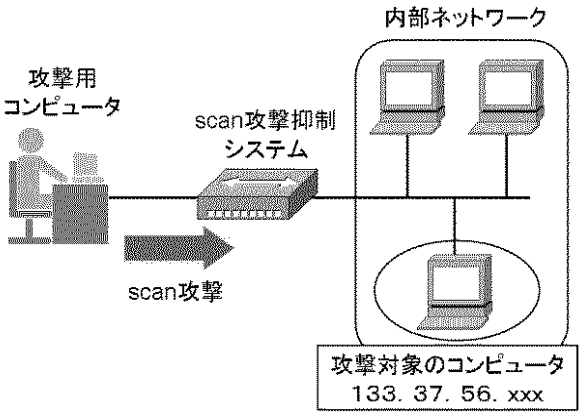
【図４】



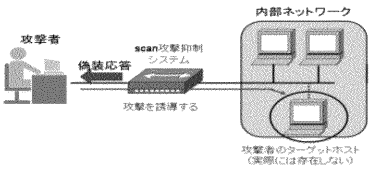
【図５】



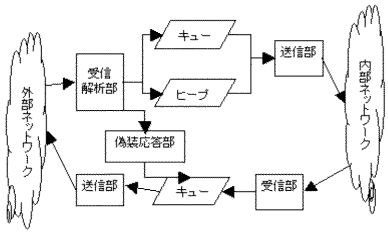
【図６】



【図７】



【図８】



フロントページの続き

Ｆターム(参考) 5K030 GA15 HA08 HB11 HB19 HC01 HC13 HD03 HD06 JT02 KA03
KA04 KA07 KX11 MC08
5K033 AA08 CB08 DA01 DA06 DB18 EA06