L-031

偽装応答を用いた scan 攻撃抑制システムの提案
The Scan Attack Control System using Camouflage Response

兒玉 清幸[†1] 大塚 賢治[†2] 南 浩一[†3] 吉田 和幸[†4]
Kiyoyuki Kodama Kenji Otsuka Kouichi Minami Kazuyuki Yoshida

1．はじめに

セキュリティホールが残っているコンピュータや特定のサービスを動作させているコンピュータの存在等を探す scan 攻撃が後を絶たない．大分大学で運用している不正侵入検知装置でも日々多くの警告が通知されている[1]．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，spam 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．そのためネットワークの管理者は，こまめにログを監視し，適切なフィルタリングを行うなどの対策を行う必要がある．しかし，大学のような研究室単位で多くのコンピュータが管理されている環境では，全てのコンピュータにこのような対策を行なうのは難しい．そこで，我々は scan 攻撃への対策として throttling を用いてネットワーク単位で scan 攻撃を抑制するシステムを開発し運用している[2]．しかしパケットを遅延させる throttling だけでは scan 攻撃に対して効果が少ないことがわかった[3]．そこで，本稿では throttling による scan 攻撃抑制システムのログ情報に基づき，新たな scan 攻撃への対策として，偽装応答を用いた scan 攻撃抑制システムの提案を行う．

2 章で throttling による scan 攻撃抑制システムについて述べ，3 章では，その運用状況について評価解析を行う．4 章ではその解析に基づき偽装応答による scan 攻撃抑制システムを提案し，その効果について考察する．5 章はまとめである．

2．throttling による scan 攻撃抑制システム

2．1 概要

本システムは外部ネットワークから行われる scan 攻撃の抑制を目的とする．本システムで対象とする scan 攻撃は TCP[4]による scan 攻撃である． TCP コネクション

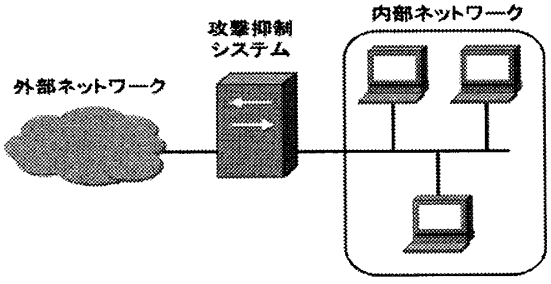

図 1 透過型ブリッジによる配置

†1 大分大学大学院工学研究科 †2 大分大学工学部
†3 大分大学工学部(現在 システム計画研究所)
†4 大分大学総合情報処理センター

要求（TCP オプションの SYN, ACK フラグがそれぞれ 1, 0 であるパケット）が外部の同一送信元アドレスから複数回送られたとき scan 攻撃が行なわれたと判断する．

本システムは設置場所を選ばない透過型ブリッジとしてネットワークの境界で動作する（図 1）．

2．2 構成

システムは外部ネットから来たパケットを全て受信し，throttling アルゴリズムを適用する．その後，内部ネットに送信する．内部ネットから来たパケットは，すべて無遅延で外部ネットに送信する．システムの内部構成を以下に示す（図 2）．システムは，パケットの受信・解析を行う受信部，パケットに必要に応じて遅延をかけ送信する送信部とそれらの間でデータの授受を行うキュー，ヒープとから構成されている．

受信部はネットワークデバイスからパケットの受信を行う．外部ネットワークから受信したパケットは解析部へと送り，内部ネットワークから受信したパケットについては直接送信部へと送る．解析部は受信部から送られたパケットを受け取り，パケットに throttling アルゴリズムを適用する．キューは，受信部もしくは解析部から送られたパケットを一時的に蓄え，送信部へとパケットを引き渡す．ヒープは，パケットとその送信可能時刻を蓄え，送信可能時刻が来るたびに送信部にパケットを渡す．

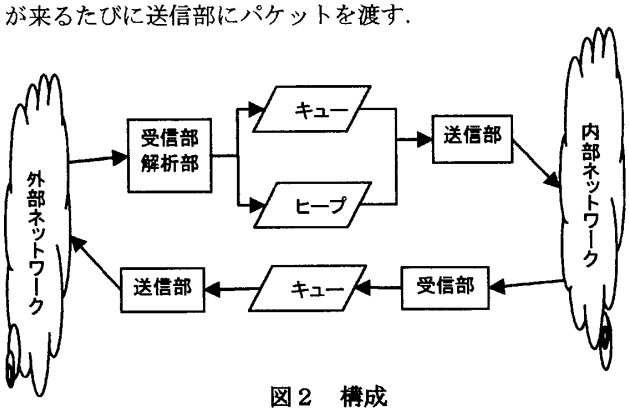

図 2 構成

2．3 throttling

throttling は spam メール対策などで利用され，アクセスに対して一定時間の遅延を設け意図的に応答を遅らせる手法である．本システムは短時間に複数回のコネクション要求が行なわれたとき TCP を用いた scan 攻撃だと判断し，throttling を実行し，相手への返答を遅らせる（図 3）．遅延量はコネクションの要求回数に応じて段階的に増加させてゆき，上限値を約 49 秒としている（図 4）．遅延をかけている間に攻撃者が TCP コネクションを破棄すれば，事実上 scan 攻撃を抑制したこととなる．また TCP コネクションを諦めなくとも，scan 攻撃終了までにかかる時間が長くなるため，攻撃者は多くのホストにアクセスすることが難しくなる．

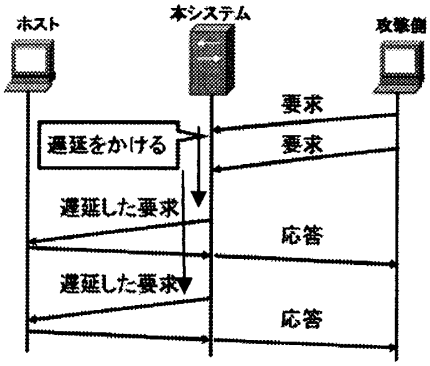

図３　攻撃に対する遅延

遅延時間　＝　$2^{(\beta-1)} \times 10^{-6}$秒
（β＝コネクション要求回数）

図４　遅延時間の計算式

３．運用評価

３．１　運用環境

システムを図５のように学内 LAN のメールサーバ等があるセグメントの入り口に設置して運用している．このセグメント内には SSH サーバも運用している．

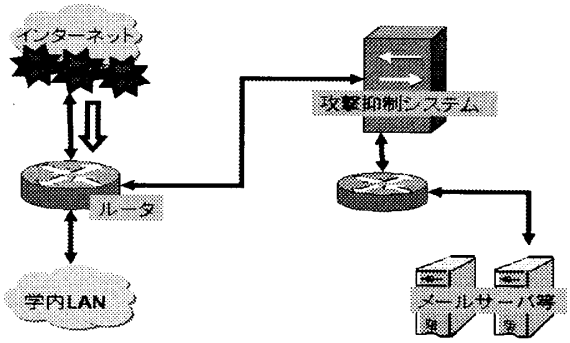

図５　運用環境

３．２　運用結果

2006 年 12 月 31 日から 2007 年 4 月 22 日までの 16 週間の SSH サービスに関する運用結果のログをグラフ化したものを図６に示す．図の攻撃数とは，SSH サービスの認証に失敗したログレコード数を指す．なお，2007 年 1 月 18 日を境に scan 攻撃抑制システムの運用前データと運用後データに分かれる．

３．３　運用評価

グラフより，131 と 134 以外のサーバでは 1 月 28 日以降にアクセス数が減少傾向にあるのがわかる．しかし，131 と 134 のサーバについての攻撃回数は他のサーバに比べ非常に大きい．そこで，攻撃回数が非常に多かった週のシステムログを解析した．

サーバ：134，日付：2007/3/18
・検出した攻撃回数は 2,760 回．そのうち 1,908 回が同一 IP アドレスからのものだった．
サーバ：134，日付　：2007/4/15
・検出した攻撃回数は 1,944 回．そのうち 1,676 回が同一 IP アドレスからのものだった．
サーバ：131，日付　：2007/4/15
・検出した攻撃回数は 2,000 回．そのうち 1,734 回が同一 IP アドレスからのものだった．

上の３種のログデータに共通する点は，同一 IP アドレスから連続して同一サーバへのアクセスを繰り返している攻撃者の存在である．これらの攻撃者は scan 攻撃によってターゲットの存在を確認している．また，throttling による遅延時間は 26 回以上のコネクション要求が行われた際に，最大遅延時間（約 49 秒）に設定されるが，上の例ではたとえ最大遅延時間が設定されているとしても攻撃を止めていない．つまり，この程度の遅延量は TCP コネクションを破棄する主たる理由となっていないことになる．

遅延量を増やすと，遅延中のパケットを記憶する主記憶の使用量が増加し，送出時刻順に並んでいるヒープにデータを追加する等の計算時間も増加する．そのため本システムのように抑制する側でパケットを一時的に保存して遅延を与える方式では有効な遅延量になる前に守る側が資源を使い果たしてしまう可能性がある．そこで攻撃側が待つ状況を作ることで，抑制装置の資源をあまり使わずに遅延量を確保し，scan 攻撃によるホストの発見をできる限り遅くする必要がある．

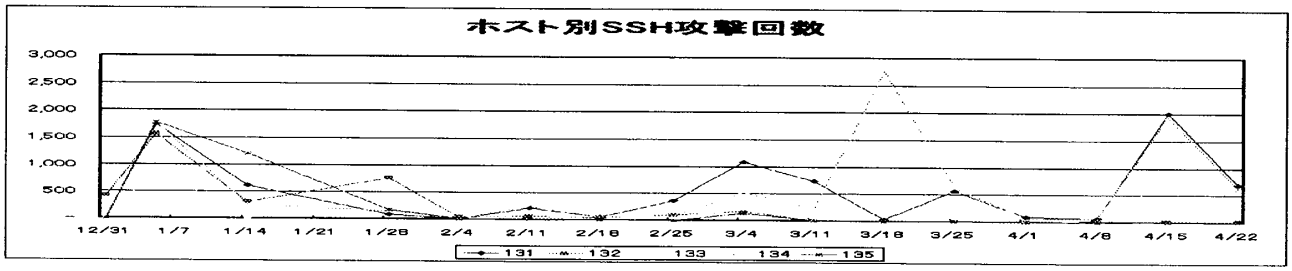

図６ ホスト別 SSH 攻撃回数

4．偽装応答を用いた scan 攻撃抑制システム

4．1 概要

throttling を用いた scan 攻撃抑制システムでは，内部ネットワークに存在しない IP アドレス，ポート番号に対する接続要求については，遅延を設けたとしても攻撃者に対して必ず ICMP host unreach 等で正常に応答していた．そのため，遅延時間経過後すぐに攻撃者はこちらの状態がわかってしまう．内部ネットワークに存在しない IP アドレス，ポート番号に対する接続要求について，scan 攻撃抑制システムが応答(偽装応答)を返すことにより，攻撃側がこの IP アドレス，ポート番号に対してその後 timeout するまで待つことになる．このシステムは throttling による scan 攻撃抑制システムに組み込んで動作する．

4．2 システムの構成

システムの内部構成を以下に示す（図 7）．新システムでは，throttling による scsn 攻撃抑制システムに偽装応答という新たな機能を追加する．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ホストへのコネクション要求を受け取った場合，外部ネットワークへの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．

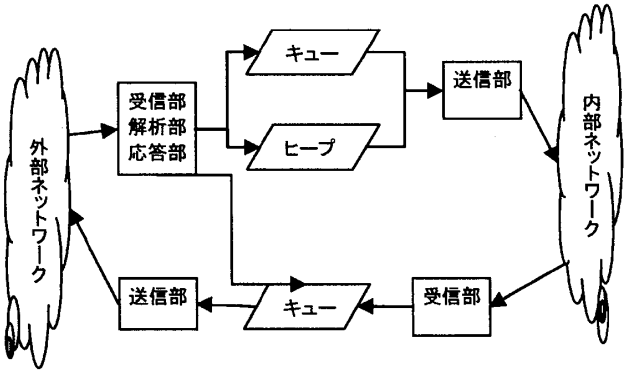

図 7 新システムの構成

4．3 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，偽装応答を行う．具体的には，攻撃者からの内部ネット中の存在しないホスト宛てに来た SYN パケットに対し，その宛先ホストとして 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．偽装応答は攻撃者を存在しないホストに向けて攻撃を誘導することで攻撃者の資源を使って待たせる処理である（図 8）．

4．4 期待される効果

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絞り込ませないことができると考えられる．同時に scan 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 scan 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 scan 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．

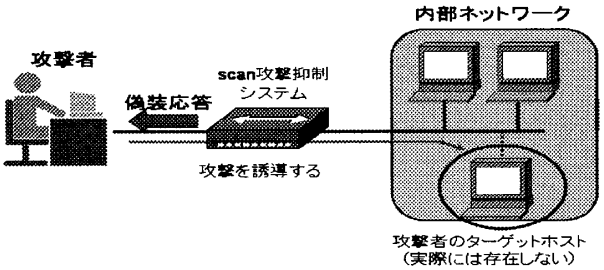

図 8 偽装応答と攻撃誘導

5．まとめ

本稿では throttling による scan 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 scan 攻撃抑制システムの提案を行った．今後の課題としては，throttling システムでは SSH 以外の攻撃に対しての評価と検証，適切な遅延量の設定方法などを検討する．同時に偽装応答システムを開発・運用し，throttling による scan 攻撃抑制システムのみの場合とログファイルも比較検討し，有効性を検証していきたい．

参考文献

[1] 三鑰,大野,吉田: 攻撃の規則性認識を支援する攻撃量時系列変化比較対照表示システム，分散システム/インターネット運用技術シンポジウム 2006 論文集，pp.55-60, 2006.11

[2] 吉田,南：throttling を利用した scan 攻撃抑制システム，分散／インターネット運用技術シンポジウム 2006 論文集 pp.43-48, 2006.11

[3] 吉田，南: throttling による攻撃抑制の効果について，情報処理学会研究報告(2007-DPS-130/2007-CSEC-36), pp.381-386, 2007.3

[4] J.Postel : "Transmission Control Protocol", RFC 793, Sep 1981.

[5] K. Yamamoto, A. Kato and A. Watanabe : "Radish- A Simple Routing Table Structure for CIDR", WIDE, 1995 http://citeseer.ist.psu.edu/yamamoto95radis.html