

輻輳型 DoS 攻撃を対象にした優先制御・帯域制御の研究

A Study on Priority Control and Bandwidth Control against Congestion-type DoS Attacks

安齋 孝志
Takashi Anzai

近年 DoS/DDoS (分散サービス拒否) 攻撃による被害が多数報告されている。本研究では輻輳型 DoS 攻撃に着目し、この攻撃により http によるアップロードサービスが困難になる場合を例に、正常なトラフィックの可用性を確保する手法を提案する。

提案法では、最初に、TCP のフロー制御および輻輳制御のメカニズムを利用して DoS 源を識別する。さらにその識別結果に基づいて優先制御、帯域制御を実行し、DoS 源からのトラフィックと正常な送信者からのトラフィックの差別化することで、正常なトラフィックの可用性を維持する。最後に、提案法の計算機シミュレーションを行い、その有効性を例証する。

In these years a lot of damages due to DoS or DDoS attacks have been reported, This study focuses the congestion-type DoS attacks suffering up-loading services with http, as an example, and proposes a method for assuring availability of normal traffic.

First, the method classifies sources of the DoS attacks from normal sources, by using mechanism of the flow control and congestion control in TCP. It further discriminately operates priority control and bandwidth control on the classified normal traffic and DoS traffic and then maintains the availability of normal traffic. In the end, software simulation illustrates the effectiveness of the proposed method.