

統計解析による攻撃検知に関する研究  
トラフィック解析の攻撃検知への適用



教授 中嶋 卓雄  
Prof. Takuo Nakashima

Attack detection based on statistical analysis

Application of the traffic analysis to attack detection

Keyword : 攻撃検知・トラフィック解析・統計解析  
Attack detection・Traffic analysis・Statistical analysis

近年、個人のみならず企業や国家機関にたいしても DoS/DDoS 攻撃などのサイバー攻撃が頻繁に行われています。ウイルスなどの固有な特徴を検出する研究は従来から行われていますが、新しいウイルスに瞬時に対応できないのが現状です。本研究では、特定の組織に対して、その前兆となる動作を監視し、その組織への全トラフィックを統計的に解析することにより、攻撃トラフィックを検知するシステムを開発しています。統計量としては、エントロピーおよび  $\chi^2$  値検定を利用しています。エントロピーによる検出では、エントロピーがバラツキの度合いを計測する指標であることから、エントロピーが通常より小さく、または大きく変動することにより、DoS または DDoS として検出することができます。統計量の計算は、パターンマッチング手法と比較して計算時間が非常に短く、早期に組織内のすべての攻撃を発見できるメリットがあります。

In recent years, DoS/DDoS attacks widely occurred to servers, companies and government sites. Researches of virus detection comparing the specified features are conducted in these days. New viruses, however, are hardly detected within short period. In this research, we observe the pre-attacking behavior and analyze all incoming traffic using statistical methods for the specified organization. These methods adopt the entropy method and chi-square method. Variation of entropy values is utilized in entropy method. If entropy value is lower than normal value, attacks seem to be DoS attacks. On the other hand, if entropy value is higher than the normal value, attacks seem to be DDoS attacks. The calculation times of these statistical methods is very short compared to the pattern matching method leading to the quick detection. These methods have the merit to find all incoming attacks of local organization.

