DNS を用いた IP トレースバック情報連携方式の提案

A proposal of DNS based information cooperation system for IP traceback

佐々木　達典
Tatsunori　Sasaki

概 要

外部ネットワークから DoS（Denial of Service）等のサイバー攻撃を行う際，攻撃者は送信元の IP アドレスを詐称することにより，発信源の特定を著しく困難とすることが多い．詐称時においても，攻撃経路を特定する技術が IP トレースバック技術であり，詐称攻撃に対する効果的な防御や抑止の手法として期待されている．しかし，実際に経路を特定するためにはインターネットを構成する各組織間における保有情報の連携が必須であり，その連携基盤導入におけるコストや運用負担の増加等の理由から未だ普及にはいたっておらず，大きな課題となっている．本稿では，インターネットを利用するために必須の基幹設備である DNS を用いて組織間の情報連携を行い，同課題に対処する手法を提案する．既存の共通インフラを利用する事で，新たな連携基盤を導入せずとも既知の技術を用いて追跡が可能となる手法を設計した．また，提案方式の有効性をインターネットを模した検証環境を構築して試験した結果，設計内容の妥当性，及び懸念された追跡所要時間や情報保有可能時間等の性能面について充分現実的な利用が見込めることが分かった．

Abstract

Generally information security attackers spoof their IP addresses so as not to be identified their attacking from other networks like DoS (Denial of Service) attack. Some IP traceback techniques have been developed to detect attacking routes on the Internet, and were expected to prevent attacks with IP address spoofing. But there is a problem common to the conventional techniques that related organizations such as ISPs are loaded with much cost and increase operational works for the IP traceback. Therefore we suggest a new method which the organizations could perform the IP traceback with less cost and low burden in cooperative use of a DNS (Domain Name System) based information exchange infrastructure. We designed it which could trace by using the existing facilities and techniques. In addition, we verified it functions effectively and the performance problem is not caused, by using some tests using the environment that is similar to the Internet.