要 旨

不正アクセス検出のための
パイプライン型シグナチャ検索法

松本　拓也

アプリケーション層内のシグナチャ検索は，Firewall や IDS，そしてウィルス対策システム等のセキュリティシステムの中で必要不可欠なものになってきた．シグナチャ検索では，ポート番号や IP アドレス，そして文字列等の情報を検索している．ポート番号や IP アドレスといった固定長のものを検出することは比較的容易であるが，ネットワークパケット中のペイロードに含まれる可変長の文字列を検索することは処理負荷が高い．特に，検索対象の 1 つである HTTP パケットは，ネットワークトラフィック中の約 74% を占めており，文字列検索全体に占める割合が高い．そのため，高速な文字列検索が望まれている．

本研究では，文字列型シグナチャの並列かつパイプライン的なシグナチャ検索法を提案した．本方式はメモリ使用量が少なく検索に要する計算量が少ない Quick Search アルゴリズムを用いた．そして，このアルゴリズムの検索に必要な情報をデータパケットに保持させることで，無駄なメモリアクセスとデータハザードの発生を抑制し，単位時間あたりに検索可能な文字数を高めた．32 bit DDMP 用シミュレータを用いて評価した結果，4 つのプロセッサを用いた場合，23.02 Mbps の性能を確認できた．加えて，URL Filtering 用に最適化した場合，59.3 Mbps の性能を確認できた．

キーワード　パイプライン型シグナチャ検索法，並列検索，データ駆動型マルチプロセッサ

Abstract

Pipelined Signature Matching for Malicious Access Detection

Takuya Matsumoto

Based on the conception of deep packet inspection, signature matching (SM) of application layer content is becoming an indispensable portion of most of the security systems such as firewall, intrusion detection system (IDS) and so on. Compared with other security techniques like static packet filtering and stateful packet inspection (SPI), SM is more computation intensive because of the heavy processing load for matching all the variable length payloads of network packets with the large predefined keywords set. Since SM module dominants the performance of the entire security system, a fast SM mechanism is required to keep up with the increasing network bandwidth.

My work focuses on the development of pipelined parallel implementation of SM module, as well as its evaluation on the data driven multimedia processor (DDMP) simulator. When developing the SM module, the quick search (QS) algorithm is adopted owing to its fast performance.

The evaluation result shows that when 4 nano-processor (nPE) is used, the throughput of SM module can get to 23.02 Mbps. In addition, a higher throughput which is 59.3Mbps can be obtained if the SM module is optimized for URL filtering.

key words Pipelined Signature Matching, Parallel Searching, Data Driven MultiProcessor