平成18年度 情報工学コース卒業研究報告要旨

宮尾 研究室	氏　　名	成 田 輝 久
卒業研究題目	大規模ネットワークにおける侵入検知ログの解析と利用に関する研究	

教育研究機関のネットワークにおいては、性質上通信に厳しい制限を設ける事が難しく、常に内外から大量のセキュリティインシデントにさらされている。このようなネットワークの維持管理には侵入検知システム (IDS:Intrusion Detection System) のような支援ツールが重要だが、IDS は全てのインシデントを可能な限り検知するため得られるログが膨大な量になる。そのためリアルタイムに遮断等の処理をする事は困難であり、必ずしも維持管理の直接的な助けになっているとは言えない。名古屋大学では、IDS から得られたログによりウイルスの感染を事後に検知し、通信を遮断しているが、リアルタイムにインシデントを検知し、対応を行う仕組みはできていない。

本研究では名古屋大学学内ネットワークのファイアウォール内側に接続されている IDS から得られた 141 日分のログを元に、NICE(133.6.0.0/16) に対する TCP ポート 22 のスキャンについて特徴を分析する。TCP ポート 22 を分析対象としたのは SSH によるリモートのために外部からの通信をファイアウォールで遮断する事が出来ず、被害を受けたときの影響が大きいためである。さらに、分析結果に基づいて管理負荷の低いリアルタイムアラートシステムを提案する。

ポートスキャンは一般的に、連続して広範囲の IP アドレスに対して行われることから、同一 IP アドレスからの 30 分以上間隔を空けないスキャンを一連のスキャンとして纏めた。ログから得られるスキャンの数が約 56 万件だったのに対し、一連のスキャンは 1,497 件しかない事が分かった。これは一日に 10 件程度のペースであり、全てに対してアラートを出しても十分に管理可能と言える。また 1,497 件のスキャンのうち、6 割は 1 分以内で終了する 1 万個程度のアドレスへのスキャンであった。一方、残りの 4 割は NICE 全体を複数回スキャンしており、1 回の全体スキャンには平均で 20 分間かかることが分かった。

本研究で提案するリアルタイムアラートシステムはファイアウォールと連携してスキャン元の IP アドレスを遮断してスキャンを防止するために利用する。そこで、スキャン検知からアラート発行までの時間 (判断時間)、ファイアウォールでの遮断にかかる時間 (処理時間)、またファイアウォールにて遮断を継続する時間 (遮断時間) とスキャン防止効果について検証するためにシミュレーションを行った。シミュレーションソフトは java で実装した。処理時間を 60 秒、遮断時間を 3 時間に固定し、判断時間を変えてシミュレーションを行った結果、アラート数は判断時間 0 秒の場合 630 回、60 秒の場合 551 回と 1 日平均約 5 回であり大幅には変わらない事が判明した。さらに、被スキャン IP アドレス数の平均をとると、判断時間 0 秒の場合 4,268 個なのに対し 60 秒の場合 5,324 個であり、判断時間 0 秒の方が若干ながら効果が高い。これらより、スキャンを検知したら即座にアラートを発行する事が最も効果的であるという結論が導かれた。アラートを発行しない場合、被スキャン IP アドレス数の平均は 21,092 個であるから、本システムの効果は十分にある事が確認できた。また、アラート数は 1 日 5 回程度であり、十分に管理可能である。これらの結果から、本システムがインシデントのリアルタイムな対応を行うのに十分有用である事が示された。

今後の課題として、実環境への本システムの実装を行い実際の効果や問題点などを検証する事が挙げられる。