2T－2

SNMPによるネットワーク不正アクセス検出エージェントの実現

緒方 彰*，中嶋 卓雄*，中村 良三*
*熊本大学 工学部

1 はじめに

インターネットに接続されるホストが増加し，リーチャビリティが広がるにつれ不正なアクセスも増える傾向にある．組織全体として不正アクセスに対しファイアウォールによりアクセス制限することは可能だが，大学などのようにオープンな接続をする組織では，重要なマシンに個別にアクセス制限をする場合が多い．従来，個別にアクセス制限させたいホストにおいて，不正アクセスを検出する機構は単にログに書き込むのみで，システム管理者に通知する有効な機構をあまり持ち合わせていなかった．

一方，ネットワーク管理はネットワークから様々な情報を収集し，もし障害が発生していればそれを取り除く他に，セキュリティを持たせ不正な利用を制限する必要がある．ネットワークを管理するプロトコルとしてSNMP(Simple Network Management Protocol)[1]があるが，SNMPの欠点としてセキュリティ・メカニズムが弱いという点が挙げられる．この欠点を補うためにセキュアSNMPが開発された．現在はSNMPv2においてセキュアSNMPのセキュリティメカニズムを備えている．しかし，このセキュリティはSNMP自身のセキュリティであって，ネットワーク全体のセキュリティを考慮したものではない．

そこで本稿では，SNMPを用いてネットワークからの不正アクセスを検出するエージェントを実現する．具体的には，RMON MIBのフィルタグループ，イベントグループを使用し，不正アクセスを検出した時点でエージェントはtrapを発生させマネージャに通知する．この機能の実現によりSNMPによるネットワーク管理が，故障などの検出のみならずセキュリティチェックも統合した機構となり，システム管理者が独自にスクリプトを用意する必要がなくなり，SNMPマネージャで一括して管理することによりネットワーク全体のセキュリティも監視することが可能となる．

Implementation of the Illegal Access Detecting Agent on SNMP

Akira Ogata*, Takuo Nakashima*, Ryozo Nakamura*
*Faculty of Engineering, Kumamoto University

2 エージェントの構造

2.1 概要

エージェントは入ってくるパケットをチェックし，許可されていないホストからの不正なアクセスを検出した時点でSNMPのTrapメッセージを使ってマネージャに不正アクセスを通知する．

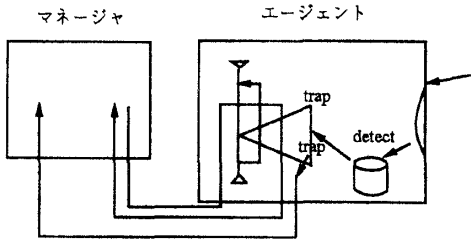

図1：エージェントの概要

2.2 データ構造

本稿ではRMON MIBのフィルタグループとイベントグループを使用する．以下に主に使用するMIBの項目を示す．

フィルタグループ

- filterIndex
  filterTable中のエントリを一意に識別する整数値．
- filterPktData
  パケットをフィルタリングするビットパターンを設定する．他にfilterPktDataOffset，filterPktDataMask，filterPktDataNotMaskなどもフィルタリングの条件として使用できる．
- filterChannelIndex
  フィルタをどのチャネルに含ませるかを指定する．
- channelAcceptType
  チャネルに対するフィルタのアクションを制御する．この値がMatchedの時は，関連フィルタのうちの少なくとも1つにおいてデータフィルタとステータス・フィルタの両方を通過すれば，そのパケットはこのチャネルに関して受け入れられることになる．

- channelDataControl
  on の場合，データ，ステータス，イベントはこのチャネルを流れる．

- channelEventIndex
  対応する channelDataControl がオンで，パケットが合致した場合に生成されるイベントを識別するインデックス．このオブジェクトの値は，event グループで eventIndex のインデックスが同じ値を持つオブジェクトを示す．

- channelEventStatus の設定
  eventReady,eventFired,eventAlwaysReady のいづれかの値を持つ．eventAlwaysReady の値が設定されている場合，パケットが合致するたびにイベントが生成される．

イベントグループ

- eventIndex
  eventTable 内の 1 つのエントリを一意に識別する整数値．

- eventType
  none,log,snmp-trap,log-and-trap のいづれかの値を持つ．

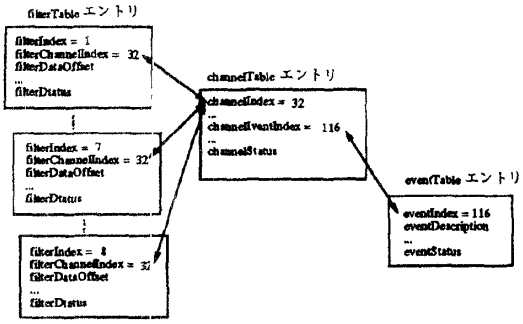

図 2 ：フィルタグループとイベントグループの関係

2.3 動作アルゴリズム

本稿では RMON MIB のフィルタグループとイベントグループを使用し，不正アクセスエージェントを実現する．

フィルタグループにパケットをフィルタリングする条件を設定するが，ここではパケットの IP アドレスが保持されている部分にフィルタをかけるように設定しておき，不正なアクセスを検出できるようにする．イベントグループには条件に応じたイベントを設定しておく．

具体的には filterPktData にフィルタリングのビットパターンを設定し，filterChannelIndex で設定したフィルタがどのチャネルに含まれるかを指定する．channelAcceptType，channelDataControl でパケットをチャネルに対して受け入れられるように設定しておく．channelEventIndex，chanelEventStatus でフィルタグループからイベントを発生できるように設定し，eventIndex，eventType でイベントの種類を設定する．

エージェントは，入ってくるパケットに対してフィルタリングを行い，条件に合致したらイベントを生成し Trap メッセージでマネージャに不正アクセスを通知する．

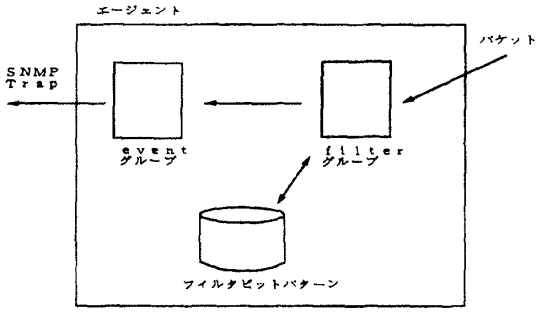

図 3 ：エージェントの動作

3 おわりに

今回は，従来の SNMP の機能に加えて，セキュリティに関する機能を付加した SNMP エージェントを提案した．このエージェントにより，SNMP によるネットワーク管理が，故障などの検出のみならずセキュリティも統合した機構をもつことになり，スクリプトを独自に用意する必要がなくなり，システム管理者の負荷を軽減することができる．

参考文献

[1] J. Case,M. Fedor,M. Schoffstall,J. Davin: A Simple Network Management Protocol (SNMP), RFC 1157,1990.

[2] J. Case,M. Fedor,M. Schoffstall,J. Davin: Textual of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2), RFC1442,1993.

[3] S. Waldbusser: Remote Network Monitoring Management Information Base RFC1271,1991.

[4] 山口英: SNMP(1),SNMP(2), UNIX MAGAGINE Vol.10,4,5 月号,1995.

[5] CMU snmp package, Ver. 2.1, Carnegie Mellon University, 1993