SNMP の役割

SNMP（Simple Network Management Protocol）

- サーバやネットワーク機器の監視のためのプロトコル
- デバイスのパフォーマンスやリソース状況の把握
- ネットワーク監視・制御、IT 資産管理のための情報
- 障害や兆候を通知する SNMP トラップ

SNMP（Simple Network Management Protocol）は、サーバや、ルータ、スイッチなどのネットワーク機器に対し、ネットワーク経由で監視や制御を行うためのアプリケーション層のプロトコルです。
ネットワーク監視といえば、ping コマンドなどを使った死活監視や、IDS などの侵入検知のための監視などがありますが、機器のトラブルの予兆検知をするためには、ディスクやメモリ、CPU 負荷やネットワーク帯域などのリソース不足を把握することも重要です。これらのリソースを監視するために、SNMP が活躍します。SNMP は、デバイスの状態、リソース、パフォーマンス、トラフィック等の監視を目的にして、どの機器に障害が発生したかなどが把握でき、迅速な障害対応のための情報収集のみならず、リソース状況のログを蓄積すればキャパシティプランニングにも有効です。
サーバについては、CPU やメモリ、ディスクの使用率、プロセスや Windows イベントログ、Syslog 等の監視を行います。ネットワーク機器は、送受信されたパケット数、エラーパケット数、ポートの状態、そして CPU やメモリの使用率などを監視します。
SNMP は、監視や制御を行う管理する側のソフトウェアの「SNMP マネージャ」と、管理される側の機器にインストールされる「SNMP エージェント」があり、これらが SNMP で通信を行います。こうした監視や制御を行うためのソフトウェアは多数在りますが、Zabbix や、Hinemos などのオープンソースのソフトウェアも選択できるため、幅広い分野での IT 関連機器のネットワーク監視等で使用されています。
SNMP の監視は、平常時は SNMP マネージャが、SNMP エージェント側に要求して情報をもらいます。これに対して、何か異常が発生したときや、あらかじめ設定しておいた閾値を超えた場合など、SNMP エージェント側が SNMP マネージャに対して通知することを、「SNMP トラップ」といいます。
異なる機器を一元的に監視するために、MIB（Management Information Base）という統一した規格の管理情報ベースがあります。MIB では、監視対象から取得した個々の情報に対し、OID（Object ID）という識別符号によりツリー構造の階層管理をしています。
SNMP と使用すれは、IP アドレス、プリンタの状態や累計枚数、ルーターの転送速度、スイッチのポート数、OS のバージョンなど多数の情報が把握できるため、異常検知だけでなく IT 資産管理にも有効な情報を得ることができます。