



標準化対応と企業ポリシーに基づいた 対応が進む検疫ネットワーク

(株)ソリトンシステムズ
事業開発本部
橋本 和也

はじめに

IT社会では、情報量が多いほど、ビジネスチャンスは大きくなり、顧客情報も必要となる反面、個人情報保護法等に基づく企業のリスクも大きくなっている。また、ウイルスやワームにより、ネットワークやPCが動作しなくなり、システム停止する被害も増大している。さらに、プライベートのPCで仕事をするケースも多くなっており、個人で利用するWinny等のアプリケーションからウイルスやワームに感染し、個人情報漏洩するケースも増えている。

これらの問題を解決するソリューションの一つとして、

プライベートのPCやウイルスやワームに感染する可能性のあるPCや、OSの脆弱性のあるPC等を業務で利用するネットワークに接続させないことを目的とした検疫ネットワークが必要となってきた。ここでは、検疫ネットワークの仕組みの概要について紹介する。

検疫ネットワークについて

検疫ネットワークとは、OSの脆弱性チェックやウイルス対策ソフトのエンジンおよびパターン番号等が最新のものであるかをチェックして、検疫条件を満たしているPCのみ

表1 検疫ネットワークの概要

	(1) DHCP型	(2) 認証ゲートウェイ型	(3) 802.1Xスイッチ型	(4) パーソナルFW型
構成概要図				
特徴	検疫用に暫定のIPアドレスを割り振り、検疫条件にパスすると正規のIPアドレスを払い出して、社内ネットワークに接続できる。	認証及び検疫条件をパスすると認証ゲートウェイを通過でき、社内ネットワークと通信できる。	デフォルトVLANで検疫サーバと検疫チェックし、802.1X認証を行い、条件をパスすると社内ネットワークに接続できる。	パーソナルFWにて検疫サーバとのみ通信できる制御を行い、検疫条件をパスすると社内ネットワークに接続できるよう、パーソナルFWの制御を変更する。
メリット	ネットワーク環境の変更が少ないため、導入が容易。	ネットワーク環境の変更が少なく、導入が容易で、導入コストも少ない。	末端のHUBレベルで制御可能。	端末レベルで制御可能。
デメリット	基本的には、固定IPでの対応ができない。	認証ゲートウェイ配下での制御ができない。(なるべく末端のレベルで設置する必要がある)	末端のHUBを802.1X対応スイッチに変更する必要があり、導入コストは高い。(スイッチのコストに依存)	パーソナルFWをインストールしていないPCの対応ができない。

ネットワーク接続を許可する仕組みとなっている。そのため、検疫条件を満たさないPCは治療してから再度ネットワークに接続する仕組みとなる。

現在、検疫ネットワークの方式として、以下のような方式が採用されている。

(1) DHCP型：DHCPサーバと連携して、IPアドレスを採番する際に検疫チェックする。導入は容易であるが、固定IPに対応できない。

(2) 認証ゲートウェイ型：認証ゲートウェイを設置して、検疫チェックするためのサーバとクライアント間で検疫し、条件を満たしたPCのみ、認証GWを通過できる。導入は容易だがつ安価であるが、セキュリティゲートウェイ配下のネットワークを保護できない。

(3) 802.1Xスイッチ型：802.1X対応スイッチを設置して、検疫チェックするためのサーバとクライアント間で検疫し、条件を満たしたPCのみ所属のVLANに接続される。802.1Xスイッチを設置すると、端末レベルでの制御は可能であるが、ネットワーク構成を変更する必要があり、スイッチの価格に依存するため、基本的には導入コストが高い。

(4) パーソナルFW型：パーソナルファイアウォール(パーソナルFW)と検疫チェックするサーバ間で検疫チェックし、条件を満たさない場合は、パーソナルFWでネットワーク接続を遮断する。端末単位の制御は可能であるが、パーソナルFWをインストールしていない端末の場合、対応

できない。

最近では、拡張検疫条件として、会社のポリシーに基づく端末を接続するために、インストールされているアプリケーションの有無、および会社で資産登録されている正規のPCであるか等をチェックする仕組みも重要な検疫条件になってきている。

今後の展開

検疫ネットワークには標準化の動向があり、TNC (Trusted Network Connect) *というオープンな標準規格がある。現行Ver1.0がドラフトとして公開されており、今後は、各社の対応が期待される。

構造としては、AR (Access Requestor) と PEP (Policy Enforcement Point) と PDP (Policy Decision Point) で構成される。

ARに相当する部分がTNCクライアント、PEPがネットワーク機器等 (FireWall、Router、SW-HUB、SSL VPNGW、Wireless AP)、PDPがTNCサーバとなる。

ネットワーク側は、FireWall、Router、SW-HUB、SSL VPNGW等複数あるため、認証方式はきめず、EAPとRADIUS認証のアトリビュートを利用して、各社がTNCで企画されているAPIにより検疫する仕組みとなっている。

また拡張性として、IF-PTS (Platform Trust Services Interface) というTNCそのものが信頼できることを保証するためのインターフェースがあり、セキュリティチップ (TPM) 等と連携する仕様も追加可能となっている。

さらに、日本版SOX対応等により、認証機能を強化する必要がある。今後は、ユーザー認証または接続する端末が正規PCであるかをチェックする仕組みとして、デジタル証明書やICカード等にストアして利用するケースが多くなり、資産管理サーバ等も連動する仕組みになると予測される。

* Trusted Computing Groupというセキュリティ関連団体で、TPM (Trusted Platform Module)、TNC (Trusted Network Connect)、PC、サーバ、携帯電話等へのセキュリティ対策を標準化している。

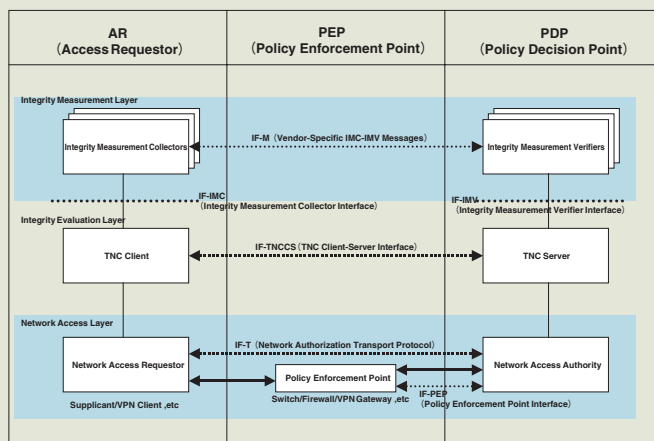


図1 TNCアーキテクチャの概要