HP Quarantine System

検疫ネットワーク

悪意のある盗聴や侵入、不注意なウィルス・ワームの持ち込み…
企業が直面する様々な脅威に対し、ネットワークで防衛するしくみを提供します。

HP Quarantine System

セキュリティ対策

企業が直面する脅威と対策

- 不正アクセスの脅威
- ウィルス・ワームの脅威

対策

認証と検疫

企業が管理し、かつセキュリティ対策が十分なクライアントのみを接続可能

- 既存のネットワーク機器や構成はそのまま
- クライアントの種類、OSなどの制限なし

3つの構成と働き

Qu Manager

クライアントセキュリティ情報を集中管理検疫ポリシー管理

Qu Controller

セグメント毎の接続制御、検疫を実施

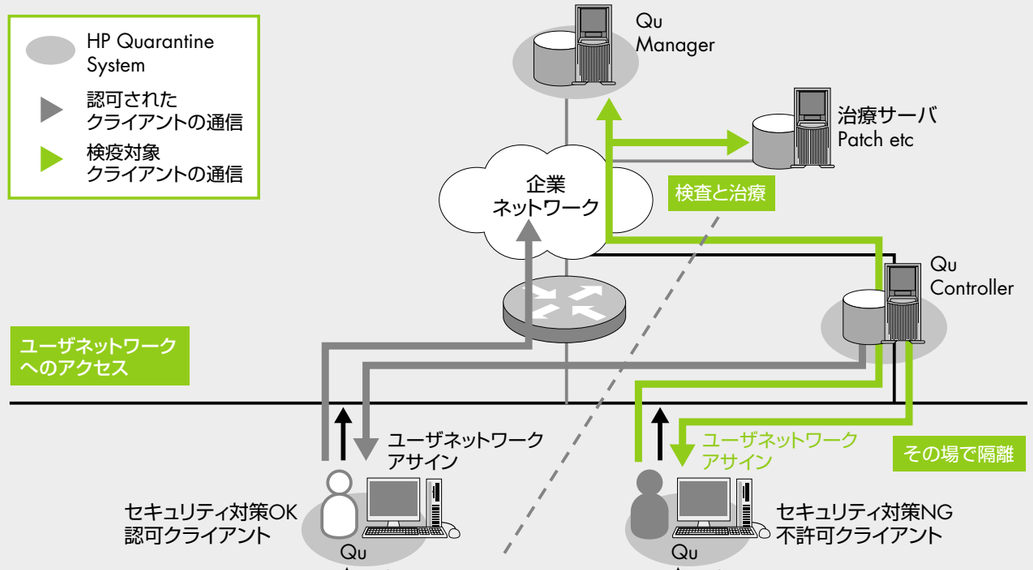
クライアント毎のコンプライアンステスト

Qu Agent

クライアントのセキュリテインベントリを Qu Controllerに報告

可能になること

- 認証 企業で認可されたクライアント認証
- 検疫 セキュリティステータスチェック
  - 隔離 疑わしい対象を隔離
  - 検査 治療の要/不要をチェック
  - 治療 治療環境への接続
  - 再生 ユーザネットワークへの再接続



HP Quarantine System

クライアント	認証	検疫と隔離	治療環境へのアクセスと復帰	治療とクライアント管理
Widnowsを中心とした様々なOS	企業が許可をしたクライアントのみ接続させる。	感染が疑わしきクライアントを隔離ネットワークへ接続	隔離対象を検疫ネットワークに移行する	治療 検疫済クライアント情報のアップデート
	HP Quarantine System			
WindowsXP/2000	**認証DHCP** ● 登録PCのみを接続制御	**認証DHCP +Forced ARP Reply** ● 不正クライアントの接続妨害 ● 検疫対象クライアントのネットワーク接続拒否 ● 不正アクセスログ管理	**オンライン検疫** ● 接続ポートが動的に検疫ポートとなる ● 隔離セグメント用専用ゲートウェイ ● モニタリング	**クライアント管理とパッチ管理** ● 検疫:検査と治療 ● Patch Management ● Virus definition ● アセット管理 ● 検疫状況管理
WindowsNT/98/95				
その他OS				
	接続ポートを変えずに、認証、検疫、隔離、治療、復旧			

クライアント認証接続と検疫（ワーム排斥）のための複合型システム