Hewlett Packard Enterprise

HPE Quarantine System Version 3

企業ネットワークのセキュリティを飛躍的に向上させる
クライアント機器の認証・検疫・情報漏えい防止ソリューション

ユーザー負担を増やさずに高度な検疫ネットワークを実現
既存ネットワークの機器/構成の変更も必要ありません

不正クライアントの接続で危険にさらされる企業ネットワーククライアントの“認証”と“検疫”は安全性確保の必須条件

いまやほとんどの企業で当たり前になっている、1人1台のクライアント環境。個人所有のクライアントや関連企業からの常駐者が持ち込むクライアントが、企業内ネットワークに接続されるケースも珍しくありません。しかしきちんと管理されていないクライアントを無条件に社内ネットワークに接続することは、多くのセキュリティ上の脅威をもたらすことになります。たとえば社外から持ち込まれたクライアントが“トロイの木馬”や悪質なワームに感染していたらどうなるでしょうか。社内に不正に持ち込まれたクライアントによって、個人情報が漏洩する可能性もあります。企業のセキュリティポリシーに合致しないクライアントでも接続できるネットワークでは、安全性の確保など不可能だといえます。しかしクライアントの接続管理を人手で行っていたのでは、膨大な管理負担が発生します。またユーザーの利便性も損なわれてしまうでしょう。ネットワークに接続されるクライアントの“認証”と、セキュリティポリシーに合致しないクライアントの“検疫”を、管理者やユーザーの負担を最小限に抑えながら行える仕組みが必要です。これを可能にするのが「HPE Quarantine System」です。ネットワークに接続されるすべてのクライアントの認証はもちろんのこと、セキュリティポリシーに合致しないクライアントの隔離や治療、再接続、さらには不正アクセスを試みるクライアントの通信妨害までが、このソリューションによって実現できるのです。

認証から隔離、検査、治療、再接続まで自動的に実施するHPE Quarantine System

「HPE Quarantine System」は、セキュリティ情報を集中管理する「Qu Manager」と、クライアントの認証や検疫をネットワークセグメント毎に実施する「QuController」、クライアント上でセキュリティインベントリ情報を管理/通知する「QuAgent」によって構成されています。これらが次のように働くことで、検疫ネットワークを実現しています。

1.認証

クライアントがネットワークに接続されると、まずQuControllerはクライアントから通知されたMACアドレスをもとに、そのクライアントが接続認可されているか否かを判断します。認可されているクライアントであれば、次の検疫のステップに進みます。認可されない場合は、IPアドレスが付与されず接続不可となります。

2.検疫

2-1 検査（コンプライアンステスト）

次にQuControllerは、MACアドレスでの認証がOKであったクライアントに対して、セキュリティ対策状況とポリシーを参照し、セキュリティのコンプライアンステストを行います。

2-2 接続

認証と、コンプライアンステストの結果が両方ともOKであったクライアントには、ユーザーネットワークへアクセスが可能なIPアドレスが配布されます。

2-3 隔離

セキュリティのコンプライアンステストの結果がNGであれば、感染等の疑いのあるクライアントとして、隔離ネットワーク用のIPアドレスが付与され、治療が終了するまでユーザーネットワークからは隔離されます。この隔離セグメントへの移行は、物理的に接続ポートを変更することなく行われます。

2-4 治療

必要なセキュリティパッチの適応や、ウイルス対策ソフトウェアの導入、パターンファイルの更新など、セキュリティポリシーに合致させるための対策を実施します。

※この処理はウイルス対策ソフトや、パッチサーバーとの連携によって実施されます。

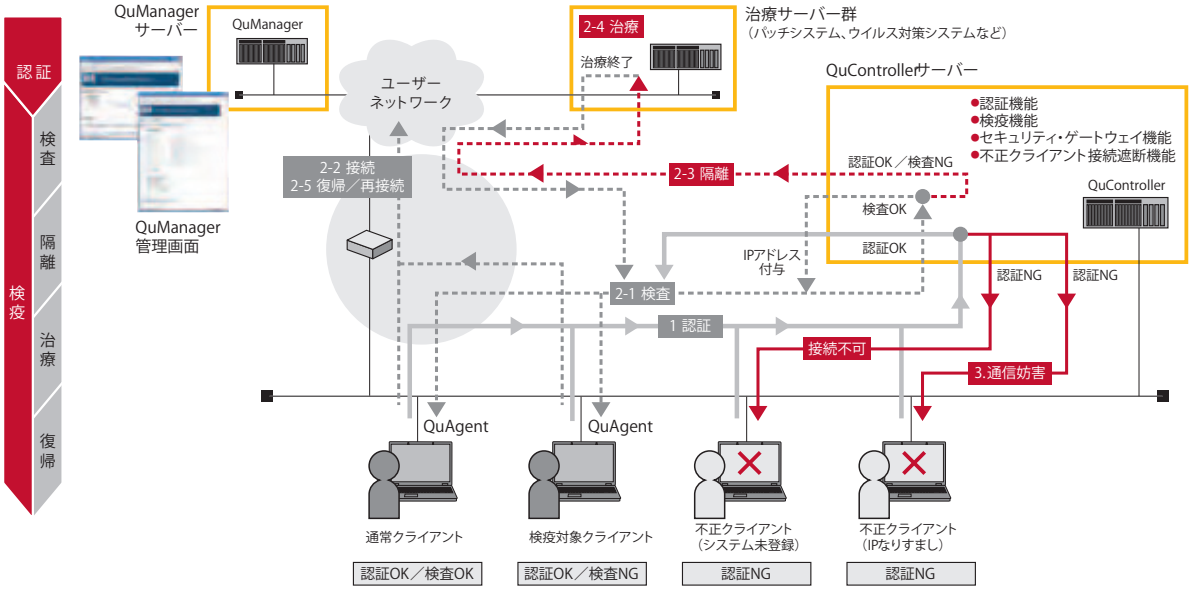
2-5 復帰/再接続

治療が完了したクライアントには、再びセキュリティのコンプライアンステストが行われます。このテストでセキュリティポリシーに合致していると見なされた場合には、ユーザーネットワーク用のIPアドレスが付与され、ユーザーネットワークへの接続が許可されます。

3.不正アクセスへの通信妨害

固定IPアドレスを設定した「なりすまし」クライアントなど、クライアントが不正なIPアドレスでネットワーク接続を行おうとした場合には、ARPで自動検知し、通信妨害を実施し、IPレベルでの通信を不可能にします。

HPE Quarantine Systemによる検疫ネットワーク



HPE Quarantine Systemの特長とメリット

■厳密性の高い認証

クライアントの認証はMACアドレスに基づいて実施されます。事前に登録されていないクライアントはネットワークに接続できないため、不正アクセスを容易に防止できます。

■クライアントのセキュリティ状況を集中管理

OSのホットフィックスやパッチ、ウイルス対策ソフトウェアの定義ファイルなど、多岐にわたるセキュリティ要素を、QuManagerが管理するセキュリティポリシーによってコントロールできます。

■管理者やユーザーの負担を最小化

認証と検疫に必要なオペレーションは、すべて自動的に実施されます。また隔離セグメントへの移行や検疫も、最初に接続した物理ポートのままで行われます。

■高い投資保護効果

既存のネットワーク機器やネットワーク構成の変更は必要ありません。ネットワーク全体を管理するQuManagerと、セグメント毎のQuControllerを配置するだけで、既存のネットワークが検疫ネットワークになります。また、既存DHCPサーバーとの連携、DHCP Relay対応などにより、柔軟な構成をとることもできます。

■多様なクライアントに対応

Windows® 2000やWindows® XP、Windows Vista®はもちろんのこと、Windows® 98などのクライアントOSも認証/検疫を行えます。

複数拠点で構成される大規模ネットワークには ステップバイステップの段階的な導入も可能

数多くの拠点で構成される大規模ネットワークをお持ちの企業では、新たなセキュリティシステムを一気に導入することが難しいケースもあります。しかしこのような場合でも、HPE Quarantine Systemなら問題ありません。次に示すように、拠点やネットワークセグメント毎のステップバイステップの導入も可能だからです。

1）まずセンターにQuManagerを導入します。QuManagerはネットワーク全体のセキュリティ情報を集中管理するためのものであり、ネットワーク全体に対して1台（冗長構成を取る場合には1セット）設置すればOKです。

2）検疫ネットワークとして機能させたい拠点もしくはセグメントに、QuControllerを導入します。QuControllerはセグメント毎の認証を行うため、セグメント毎に1台（冗長構成の場合には2台/1セット）設置します。

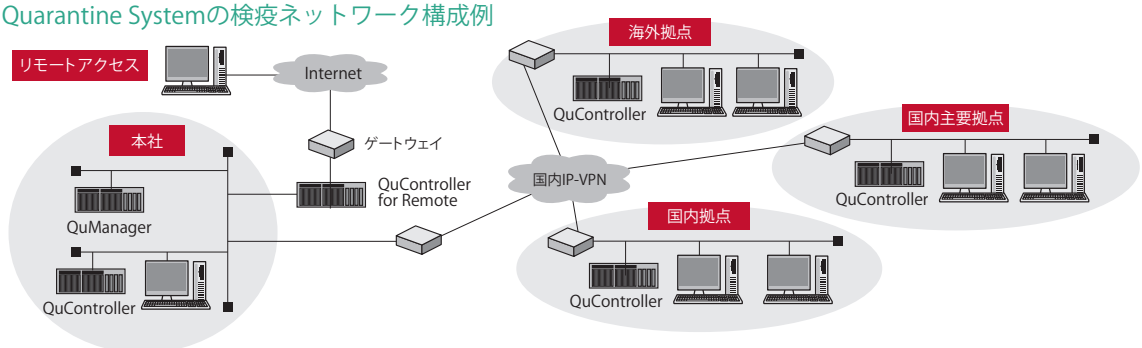
3）必要に応じて、QuControllerを設置する拠点/セグメントを増やしていきます。QuController for Remoteを設置することで、リモートアクセスを行うクライアントも認証/検疫可能になります。

4）最初は認証DHCP機能だけを導入し、DHCP運用が安定してからクライアントの検疫機能を稼動させることも可能です。

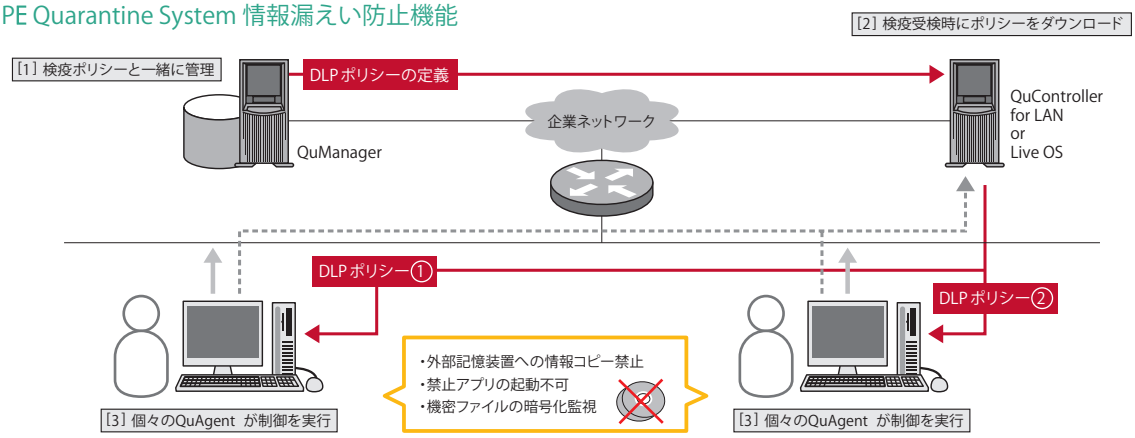
小規模拠点への導入がさらに容易に

QuController Live OSはデスクトップ型PC上でCDより起動して動作する、小規模拠点向けの軽量QuControllerです。不正クライアント隔離処理とDHCPリレーは拠点のQuController Live OSで行い、検疫検査とDHCP払い出し処理はセンターのQuController（QuController Central）でまとめて行うことにより、小規模拠点ごとにQuControllerを置いた場合と同等レベルの認証・検疫サービスを提供します。各種設定情報の管理はセンターのQuController Centralで集中して行うので、拠点での設定作業、運用管理は不要です。

HPE Quarantine Systemの検疫ネットワーク構成例



HPE Quarantine System 情報漏えい防止機能



既存DHCPシステムとの連携

HPE Quarantine Systemは、すでにDHCPシステムを構築運用されている環境にも適用できます。HPE Quarantine Systemで認証と検疫に合格したクライアントは、既存DHCPサーバーから払い出すIP構成情報を取得します。一方、認証検疫に不合格のクライアントにはHPE Quarantine Systemが独自の一時的な隔離用IP構成情報（アドレス等）をクライアントに払い出します。

情報漏えい防止オプション

機密情報や顧客情報の流出事故は後を絶ちません。
HPE Quarantine Systemの情報漏えい防止（追加オプション）では以下の機能を提供します。

1）外部記憶装置制御
USBメモリー、CD/DVD-R、SDカードなどの使用可否をクライアントごとのポリシーで定義し、制御します。

2）実行禁止アプリ制御
ファイル共有ソフトなどの実行を制限します。

3）ファイルシステム暗号化の監査
クライアントPCの紛失や盗難の際の情報流出を防ぐため、マイドキュメントやデスクトップ、メールフォルダなどが暗号化されているかどうかのチェックを行います。

これらの制御機能を検疫ポリシーの枠組みで運用、管理します。
QuAgentはダウンロードされたポリシーに従って制御を実施します。
専用の情報漏えい防止ソフトに比べて、安定した運用、容易な導入が可能です。

HPE Quarantine Systemの基本機能

■QuManager

- 認証情報（MACアドレス）の集中管理
- クライアントセキュリティ機能の集中管理
- 検疫ポリシーの管理

■QuController for LAN

- MACアドレスベースの認証
- DHCPによるIPアドレスの提供
- セグメント毎のコンプライアンステスト
- 隔離セグメントへのセキュアゲートウェイ
- IPアドレスをなりすました不正クライアントの接続妨害

■QuController Central/Live OS

- QuController for LANの機能を分割し、現場LAN セグメントにはPlug&Play方式の小型コントローラー（Live OSと呼ぶ）を配備することで、システム構築・運用をより容易にできます。特に、IT 管理者不在の小規模拠点に対してセキュリティ対策を施したいときに威力を発揮します。

■QuAgent

- クライアントのセキュリティインベントリの管理
- QuControllerに対する管理情報の通知

■QuController for Remote

HPE Quarantine Systemにより提供される認証・検疫の機能は、社内LANに接続されるクライアントだけではなく、インターネットVPNやWAN 経由でアクセスするクライアントにも適用可能です。
（リモートアクセスを行うクライアントの認証/検疫機能は「QuController for Remote 」によって提供されます。）

■他システムとの連携

主要なウィルス対策ソフトウェアやパッチサーバーとの連携をサポートしています。

システム要件

■QuManager/QuController

- HP ProLiantサーバーにて使用できるソフトウェアパッケージとしてご提供。

■QuController Live OS

- HP Compaq Business Desktop PCベースのソフトウェアアプライアンス形態でご提供。詳細につきましては、弊社営業担当者へお問い合わせください。

■QuAgent

- 利用可能なOSはWindows® 98, Windows® ME, Windows NT® Workstation, Windows® 2000, Windows® XP, Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, Windows®10。

お問い合わせはカスタマー・インフォメーションセンターへ
0120-268-186 または 03-5749-8279(携帯電話・PHSから)
HPE Quarantine Systemに関する情報は **http://www.hpe.com/jp/quarantine**

Hewlett Packard Enterprise

日本ヒューレット・パッカード株式会社
〒136-8711 東京都江東区大島2丁目2番1号

JCI08157-03