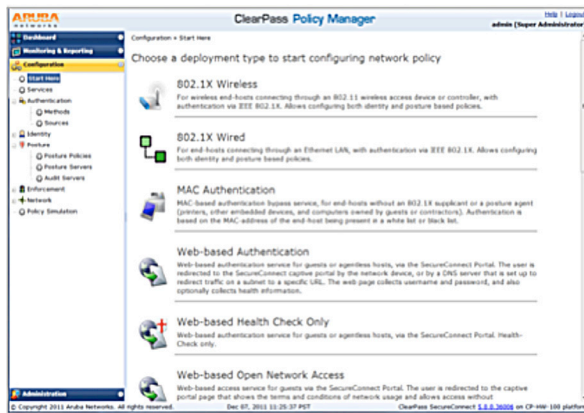


# ARUBA CLEARPASS POLICY MANAGER™

BYOD環境でネットワークアクセス・セキュリティと  
エンドポイント・コントロールをリアルタイムに実現



Aruba ClearPass Policy Manager™では、有線、無線、VPN インフラストラクチャで ID ベースとデバイス・ベースのネットワーク・アクセスコントロールを実行できます。

ClearPass Policy Manager が標準装備する RADIUS、SNMP、TACACS+ の各種プロトコルと、デバイス登録、デバイス・プロファイル、総合レポート作成の各種機能により、デバイスがネットワークに接続する前にユーザーとエンドポイントに自動的にアクセス・ポリシーを適用することができます。

その結果、BYOD(bring-your-own-device)要件に対応した一貫性のあるセキュアなネットワーク・アクセスを実現できます。ClearPass Policy Manager は、複数の場所に存在するローカル・ユーザーとリモート・ユーザーに対応し、ネットワーク、デバイスの所有者、接続方式を問いません。

## ClearPass の特長

ClearPass Policy Manager を使用すると、総合的なデバイス・プロファイルやポストチャ・アセスメントなどのポリシーを一元的に適用できます。ユーザー・ロール、デバイス・タイプ、エンドポイントの状態、場所、時間などに基づき、詳細なネットワーク・アクセス権限を与えることができます。

そのため、同じネットワークに同じ従業員がアクセスする場合でも、個人所有のデバイスよりも企業所有のデバイスに機密性の高いデータへのアクセスを許可することができます。

フル機能の AAA サービス (RADIUS と TACACS+) には、ワイヤレス・アクセスとワイヤード・アクセスのセキュリティを高める際に必要となる認証、承認、アカウントिंगの全機能が統合されています。

ClearPass Policy Manager には、Windows、Mac OS X、Linux の全デバイスがウイルス対策、スパイウェア対策、ファイアウォールという必須アプリケーションを確実に実行できるように、詳細なエンドポイント・ポストチャ機能と正常性チェック機能があります。ピアツーピア・アプリケーション、USB ストレージ・デバイス、仮想マシン (VM) アプリケーション、自動修復サービスを管理する高度な機能もあります。

## かつてないシンプルさ

中心となるプラットフォームでポリシー定義とアクセス・コントロールを簡単に実行できるため、複数のポリシー・システムを実装、管理する必要がなく、組織の全体的なセキュリティ・アーキテクチャが強化されます。

単一プラットフォームでユーザー/デバイスのネットワーク・アクセスと承認を効率的に管理し、ネットワーク・リソースを保護するためにエンドポイントの完全性を確保するため、セキュリティ運用/トラブルシューティング・システムとしての ClearPass Policy Manager の価値は向上します。

ClearPass Policy Manager は、運用効率を上げるために、ポリシーとセキュリティの脆弱性が一目で分かる前例のないユーザー/デバイス可視化機能を提供します。

## 高度なポリシー管理

### 従業員のアクセス

Aruba ClearPass Policy Manager は、無線、有線、VPN ネットワーク上で、802.1X、non-802.1X、または Web ポータルの各アクセス方法を使用してユーザーとデバイスを認証します。セキュリティを強化するためにどの環境でも PEAP、EAP-FAST、EAP-TTLS などの複数の認証プロトコルを使用できます。

詳細なコントロールを行うために、1つのポリシーの中で、Microsoft Active Directory、LDAP 準拠ディレクトリ、ODBC 準拠 SQL データベース、トークン・サーバー、内部データベースなどの複数の ID ストアの属性を使用できます。

さらに、ポストチャ・アセスメントと修復をいつでもポリシーに追加できます。

### 外部キャプティブ・ポータル

ClearPass Policy Manager では、中央のキャプティブ・ポータルから、Aruba とマルチベンダーのワイヤード機器とワイヤレス機器向けに共通のポリシーを作成できます。標準装備された Web ベースのデバイス ID 登録ツールを使用すると、MAC アドレス、デバイス・タイプ、オペレーティング・システム・バージョンなどの BYOD デバイス情報を自己登録できます。

### 管理対象外のエンドポイントのアクセス処理

プリンタ、IP フォン、IP カメラなど、管理対象外の non-802.1X デバイスをネットワーク接続時に既知のデバイスまたは未知のデバイスとして識別できます。これらのデバイスの ID は、外部または内部データベースにその MAC アドレスがあるかどうかで決まります。

また、これらのデバイスは、標準装備されている NMAP ベースのポート・スキャン機能または NESSUS ベースの脆弱性スキャン機能で監査することもできます。ポリシーをカスタマイズして、これらのデバイスにセキュア・リソースへのフル・アクセスまたは制限付きアクセスを与えることができます。

#### ClearPass Policy Manager の仮想アプライアンス

ClearPass Policy Manager の仮想アプライアンスは、最大 10,000 台のデバイスをサポートします。ハードウェア・アプライアンスだけでなく、仮想アプライアンスもクラスター内のパブリッシュまたはサブスクリバとして設定できます。仮想アプライアンスは、VMware ESX プラットフォーム (ESX 4.0) と ESXi プラットフォーム (ESXi 4.0 および 5.0) をサポートします。

#### ClearPass Policy Manager 用ソフトウェア・モジュール

ClearPass Policy Manager プラットフォームはそれ自身で機能を持ちますが、他の機能を持つ多様なソフトウェア・モジュールもサポートします。

##### デバイス・プロファイル

ClearPass Profile ソフトウェア・モジュールは、画期的な階層構造を持つ唯一のプロファイル・サービスです。接続エンドポイントの検出、分類、グループ化をデバイス・タイプに関係なく行います。

MAC organizational unique identifier (OUI)、DHCP フィンガープリンティング特性、ID 中心のデータなど、幅広い固有のコンテキスト・データを収集し、コンテキスト・ベースのアクセス・ポリシーを作成することができます。

また、格納されたデータは、デバイス・プロファイルの変更の識別と承認権限の動的変更の目的でも使用されます。たとえば、プリンタが Windows のノート PC として表示される場合、ClearPass Policy Manager は自動的にアクセスを拒否できます。

##### セキュアなデバイス・プロビジョニング

ClearPass Onboard ソフトウェア・モジュールは、標準装備の管理インターフェイスによって、IT 部門が行うデバイスのオンボーディングをほぼ自動化します。ClearPass Onboard は、Windows、Mac OS X、iOS、Android デバイスのセルフ・プロビジョニング機能を持ち、802.1X の設定のほか、固有のデバイス資格情報の配布と失効などを行います。

そのほかに、必要なアプリケーションをプッシュする機能や、一部のデバイス・タイプを対象とした Exchange ActiveSync クライアントと VPN クライアントによる携帯メールの設定もサポートします。

#### ゲスト管理

ClearPass Guest はワークフロー・プロセスを簡略化するため、IT 部門以外の受付担当者や従業員などのスタッフも Wi-Fi アクセス用の一時アカウントを作成できます。登録が完了すると、アカウント・ログインのための資格情報が SMS テキスト・メッセージまたは電子メールとして ClearPass Guest から送信されます。アカウントは、特定の時間または日数が経過した後で自動的に期限が切れるように設定できます。

ロールベースのアクセス・コントロールは、対象ユーザー数を数千まで拡張できます。カスタマイズ可能なゲスト・ポータルにより、組織は、ブランディングとユーザー倫理規定に関するメッセージを適用することができます。自己登録と資格情報の自動送信により、IT 部門の運用が効率化されます。

#### ポストチャ・アセスメント

Aruba ClearPass OnGuard ソフトウェア・モジュールのエージェントは、デバイスが接続を試みる時、セキュリティ・コンプライアンスを確保してネットワークを保護するために、従来のネットワーク・アクセスコントロール (NAC) 製品とネットワーク・アクセス保護 (NAP) 製品で行われる正常性チェックだけでなく、高度なエンドポイント・ポストチャ・アセスメントも実行します。

エンドポイントの完全性に関するすべての情報 (ウイルス対策、スパイウェア対策、ファイアウォール、ピアツーピア・アプリケーションのステータスなど) を使用して、承認ポリシーを強化できます。ユーザー・エクスペリエンスをシームレスにするために、コンプライアンス違反のデバイスには自動修復サービスも使用できます。



© 2011 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Wireless Networks®, 登録ロゴ「Aruba the Mobile Edge Company」、Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFPProtect®, および Green Island®はAruba Networksの商標です。All rights reserved. 他のすべての商標は、各社の所有物です。

DS\_PolicyManager\_12.0.301

#### ■ 開発元

##### アルバネットワークス株式会社

〒105-0004 東京都港区新橋5-27-1 パークプレイス3F  
TEL. 03-6809-1540 (代表) FAX. 03-6809-1541  
<http://www.arubanetworks.co.jp>

#### ■ お問い合わせ

##### NVC NETWORK VALUE COMPONENTS

株式会社ネットワークバリューコンポネンツ

東京オフィス  
〒144-0035 東京都大田区南蒲田2-16-2 テクノポート三井生命ビル  
Phone: 03-5714-2050 Fax: 03-5714-2051  
<http://www.nvc.co.jp/> E-mail: [sales@nvc.co.jp](mailto:sales@nvc.co.jp)