HP Client Automation

アウトバンド管理

Windows® オペレーティング システム用

ソフトウェア バージョン : 7.90

ユーザー ガイド

ドキュメントのリリース日 : 2010 年 5 月
ソフトウェアのリリース日 : 2010 年 5 月

ご注意

保証

HP の製品およびサービスで保証されるのは、製品およびサービスに添付される明確な保証文で説明されているものだけです。ここでの記載で追加保証を意図するものは一切ありません。ここに含まれる技術的誤り、編集上の誤り、または欠如について、HP はいかなる責任も負いません。

本書に記載した内容は、予告なしに変更することがあります。

権利の制限

機密性のあるコンピュータ ソフトウェアです。所有、使用、または複製を行う場合には、HP からの正規のライセンスが必要です。FAR 12.211 および 12.212 に従い、商用コンピュータ ソフトウェア、コンピュータ ソフトウェア ドキュメンテーション、および市販品の技術データは、各販売業者の標準営業許可のもとに米国政府にライセンスされています。

著作権

商標

Intel®、Intel® Active Management Technology、および Intel® vPro™ Technology は、Intel Corporation またはその米国内およびその他の国の子会社の米国における登録商標です。

Java™ は、Sun Microsystems, Inc. の登録商標です。

Linux は、Linus Torvalds の登録商標です。

Microsoft®、Windows®、および Windows® XP は Microsoft Corporation の米国における登録商標です。

Microsoft Windows™ Vista は、Microsoft Corporation の米国およびその他の国における登録商標または商標です。

OpenLDAP は、OpenLDAP Foundation の登録商標です。

ドキュメントの更新

本書のタイトル ページには、次の識別情報が含まれています。

- ソフトウェア バージョン番号。ソフトウェアのバージョンを示します。
- ドキュメントのリリース日。ドキュメントが更新されるごとに変わります。
- ソフトウェアのリリース日。ソフトウェアのこのバージョンのリリース日を示します。

最近の更新がないか確認したり、最新版ドキュメントを使用していることを確認したりするには、次の URL に移動してください。

http://h20230.www2.hp.com/selfsolve/manuals

このサイトでは、HP Passport に登録し、サインインする必要があります。HP Passport ID に登録するには、次を参照してください。

http://h20229.www2.hp.com/passport-registration.html

または、HP Passport サインインのページの [**New user registration**] のリンクをクリックしてください。

この製品のドキュメントは配布メディアで入手可能です。HP Client Automation ソフトウェアは **www.hp.com/go/clientautomation** からダウンロードできます。

適切な製品サポート サービスを購読している場合にも、更新版や新版を受け取ることができます。詳細は、HP 営業担当者までご連絡ください。

次の表には、前回のリリース以降に変更された箇所が示されています。

ドキュメントの変更点

章	バージョン	変更点
第 3 章、「アウトバンド管理設定」	7.80	48 ページの「IDE-R および SOL タイムアウト値の設定」に、IDE-R/SOL タイムアウト セッションの設定パラメータを追加しました。
第 3 章、「アウトバンド管理設定」	7.80	50 ページの「設定パラメータ」に、DASH テキスト リダイレクション時間遅延の設定パラメータを追加しました。
第 8 章、「デバイス管理」	7.80	128 ページの「デバイスの探索」に、増加的 vPro デバイス探索を追加しました。
第 8 章、「デバイス管理」	7.80	マルチデバイスの要約テーブルで SD カラムがリフレッシュされた場合について説明する 131 ページの「デバイス情報のリフレッシュ」を追加しました。

ドキュメントの変更点

章	バージョン	変更点
第 8 章、「デバイス管理」	7.80	161 ページの「DASH デバイスの起動設定の設定」に、DASH のブート設定の設定についてより詳細な情報を追加しました。
第 11 章、「トラブルシューティング」	7.80	175 ページの「[デバイス タイプの選択] ウィンドウで vPro デバイスを管理しているときに、SCS のプロパティを保存できない」で無効なドメイン名を置き換えました。
第 8 章、「デバイス管理」	7.90	154 ページの「vPro デバイスでの KVM リダイレクション」で説明している vPro デバイスの KVM リダイレクション機能を追加しました。

サポート

次の HP Software のサポート オンライン Web サイトを参照してください。

www.hp.com/go/hpsoftwaresupport

この Web サイトには、HP Software の製品、サービス、サポートに関するお問い合わせ先情報が掲載されています。

HP Software オンライン サポートでは、お客様自身が問題を解決するのに有益な情報を提供します。ビジネスを管理するために必要な対話型技術サポート ツールに素早く効率的にアクセスする方法を提供しています。サポートを受けるお客様は、サポート Web サイトを使って以下のことができます。

- 関心がある知識ドキュメントの検索
- サポート事例および機能強化リクエストの提出とサポート状況の追跡
- ソフトウェア パッチのダウンロード
- サポート契約の管理
- HP サポートの問い合わせ先の検索
- 利用可能なサービスに関する情報の確認
- 他のソフトウェア顧客とのディスカッションへの参加
- ソフトウェア トレーニングの検索と登録

多くのサポート エリアは、HP Passport のユーザー登録とサインインを必要とします。サポート契約が必要なエリアもあります。HP Passport ID に登録するには、次を参照してください。

http://h20229.www2.hp.com/passport-registration.html

アクセス レベルに関する詳細については、次を参照してください。

http://h20230.www2.hp.com/new_access_levels.jsp

目次

1 はじめに

HPCA コンソールにあるアウトバンド管理 (OOBM) 機能を使用すると、システムの電源またはオペレーティング システムの状態に関係なく、アウトバンド管理操作を実行できます。

インバンド管理は、コンピュータの電源がオンでオペレーティング システムが稼働しているときに実行される操作を指します。

アウトバンド管理は、コンピュータが次のいずれかの状態のときに実行される操作を指します。

- コンピュータは電源に接続されているが稼働していない (オフ、スタンバイ、休止)
- オペレーティング システムに読み込まれていない (ソフトウェア障害またはブートの失敗)
- ソフトウェア ベースの管理エージェントが使用できない

HPCA コンソールでは、Intel の vPro デバイスおよび DASH 対応デバイスのアウトバンド管理がサポートされます。

Intel vPro は、Intel Active Management Technology (AMT) によって有効化されています。AMT は vPro テクノロジの一部に過ぎません。Intel チップセットおよび Intel 製のネットワーク インターフェイス カード (NIC) も、vPro テクノロジ ソリューションの一部です。Intel AMT ファームウェアでは、不揮発性メモリに vPro デバイスの情報が格納されており、またリモート管理コンソールから起動できる一連の管理操作が提供されるため、Intel vPro デバイスは、電源がオフの状態でも探索および管理が可能です。

同様に、DASH 対応デバイスもアウトバンド管理を利用できます。DASH は、デスクトップおよびモバイル システムのセキュアなアウトバンド管理およびリモート管理の次世代標準を提供するように設計されています。DASH は、いくつかの DMTF (Distributed Management Task Force) 管理構想の 1 つです。マシンの状態、オペレーティング システム、またはベンダーとは関係なく、コンピュータ システムを管理するために必要な構文と語義の総合的なフレームワークを提供します。

OOB デバイスを探索および管理するために必要な唯一の条件は、デバイスが物理的にネットワークに接続されていて電源に接続されていることです。

両方のテクノロジでは、ハードウェア ベースのリモート ブートおよびテキスト コンソール リダイレクションを含む、リモート診断機能および修復機能が提供されます。vPro デバイスでは、IDE-R (Integrated Drive Electronics Redirect) を使用したリモート ブート機能が提供されます。また、SOL (Serial Over LAN) テクノロジを使用したテキスト コンソール リダイレクションも使用可能です。

Intel vPro テクノロジでは、リモートの vPro デバイスを自動的にプロビジョニングすることも可能です。さらに、このテクノロジはシステム防御およびエージェント存在機能を提供します。これらの機能は、vPro デバイスを悪意のある攻撃から保護し、システムを保護するローカル エージェントの削除を防止します。また、トラフィックの計測、分析、および対処によってワームのまん延を検出および防止するメカニズムである、ネットワーク攻撃の封じ込め (NOC、Network Outbreak Containment) ヒューリスティックを提供します。

すべての vPro OOBM 機能は、TLS によって保護されています。現在、DASH 対応デバイスに対しては、Digest 認証を使用したメカニズムのみがサポートされています。

このガイドでは、OOBM 機能について紹介し、OOBM の設定方法を示し、管理コンソールを使用するための詳細情報と手順について説明します。

機能

HPCA コンソールの OOBM には、次の機能があります。

- vPro テクノロジを搭載した PC や DASH 標準が実装された PC のハードウェア ベースの管理機能を利用することにより、電源がオフの状態、オペレーティング システムが動作していない状態、または管理エージェントが存在しない状態でもこれらの PC にアクセスできるようになります。
- 初期導入時からリース契約終了時まで、ハードウェアおよびソフトウェアのインベントリの正確性および完全性が改善されます。
- PC はリモートで電源オン、再起動および再イメージ化が可能なため、デスクサイドに向かう必要性が削減されます。
- vPro デバイスにシステム防御機能が提供されます。これにより、HPCA コンソールで作成したポリシーおよびフィルタに基づいた、Ethernet および IP プロトコル パケット フローの選択的なネットワーク分離が可能になります。
- HPCA コンソールで作成したエージェント ウォッチドッグにより、vPro システム上で動作しているローカル エージェントの監視を可能にするエージェント存在機能が提供されます。監視されているエージェントが停止した場合、エージェント存在ポリシーが有効化されます。イベントがログに記録される場合もあります。
- vPro デバイスのための、オペレーティング システムに依存しない、改ざん防止対策機能のあるワーム封じ込めシステムを提供します。ワームが検出されると、ホストが隔離され、HPCA コンソールに通知が送信されます。
- 管理対象 vPro デバイスのオペレーティング システム層より下層で実行される HTTP 認証と TLS (Transport Layer Security) によりセキュアで常に利用可能な通信チャネルが提供されます。

対象読者

このガイドは、HPCA コンソールの OOBM 機能を設定および使用して vPro デバイスおよび DASH 対応デバイスを管理する管理者およびオペレータを対象読者にしています。

各章の要約

はじめに

アウトバンド管理機能の概要を説明しています。

SCS および vPro のセットアップ

SCS Provisioning Server および Intel vPro デバイスのセットアップと設定の詳細な手順を説明しています。

アウトバンド管理設定

アウトバンド管理の設定方法を説明しています。

OOB デバイスの管理の概要

HPCA コンソールへログインして、初めてアウトバンド管理機能を使うときに、最初に知っておくべき手順を記載しています。

アウトバンド管理使用ケース シナリオ

HPCA コンソールを使用してネットワーク上の OOB デバイスの探索、修復、および保護を行う場合に使用できる一般的な実例シナリオについて説明しています。

管理タスク

Administrator ロールのユーザーが行う基本設定および操作タスクについて説明しています。

vPro デバイスのプロビジョニング

HPCA コンソールを使用して vPro デバイスをプロビジョニングする方法について説明しています。

デバイス管理

ネットワーク上の vPro デバイスおよび DASH 対応デバイスの管理方法について説明しています。この章では、これらのデバイスを管理する [デバイス管理] ウィンドウのすべての機能の使用法について詳細に記載しています。

グループ管理

ネットワーク上の vPro デバイスのグループを管理するグループ管理機能の使用法について説明しています。この章では、これらのデバイス グループを管理する [グループ管理] ウィンドウのすべての機能の使用法について詳細に記載しています。

警告の通知

イベントの発生時にプロビジョニング済みの vPro デバイスにより生成される警告の表示方法について説明しています。

トラブルシューティング

HPCA コンソールを使用して OOB デバイスを管理する際に発生しうる最も一般的な問題のトラブルシューティングの情報を掲載しています。

2 SCS および vPro のセットアップ

SCS Provisioning Server と vPro デバイスが相互に通信するには、次の各セクションで説明するように、両サイドで複数のセットアップ手順および設定手順を実行する必要があります。

SCS は Intel AMT のセットアップおよび設定サービスで、vPro デバイスのみに関連します。ここでは、DASH 対応デバイスがこれらのデバイスのドキュメントに従ってすでに設定されていることを前提にしています。OOB デバイスの管理の概要の章の DASH 設定関連ドキュメントを参照してください。詳細については、製品のドキュメントおよび HP サポート Web サイトを参照してください。

`Media\OOBM\AMT Config Server` ディレクトリにある HPCA Core 配布メディアにバンドルされているバージョンの SCS ソフトウェアを使用してください。また、前リリースから移行する場合は、SCS ソフトウェアも、現在のリリースの配布メディアに組み込まれているものに移行してください。そうしないと、エラーが発生することがあります。

概要

セキュリティは、多くの vPro 機能、とりわけリダイレクションには重要です。SOL (Serial Over LAN) および IDE-R (Integrated Drive Electronics Redirect) の使用モデルとして、リモートからの診断、ブート、および OS のインストールを可能にするリモート トラブルシューティングがあります。通常、これらの手順には、リダイレクション セッションの一部として認証手順が伴います。この認証手順には、LAN を介して送信するユーザー名およびパスワードが必要です。vPro デバイスが TLS をサポートする場合、HPCA コンソールは SOL または IDE-R セッションを開始する前に vPro デバイスとの TLS セッションを確立します。これにより、すべての関連するネットワーク通信がセキュアになります。

TLS を必要としない場合は、20 ページの「SCS Provisioning Server」に進みます。

信頼された証明書

SSL (Secure Sockets Layer) 接続が公開キー インフラストラクチャ (PKI) を使用して保護されます。PKI では、非対称キー ペア (公開と秘密) を使用して通信を保護します。このキーのペアを使用して、クライアントとサーバーの相互通信時に交換されるデータの暗号化と復号化を行います。公開キーは共有されており、データの暗号化に使用されます。秘密キーは、証明書の所有者により非公開で所持され、証明書の公開キーで暗号化されたデータを復号化するために使用します。

サーバー認証で PKI を使用する場合、クライアントはサーバー証明書の公開キーを使用してメッセージを暗号化し、サーバーは秘密キーを使用してメッセージを復号化します。逆に、クライアント認証では、サーバーはクライアント証明書の公開キーを使用してメッセージを暗号化し、クライアントは秘密キーを使用してメッセージを復号化します。

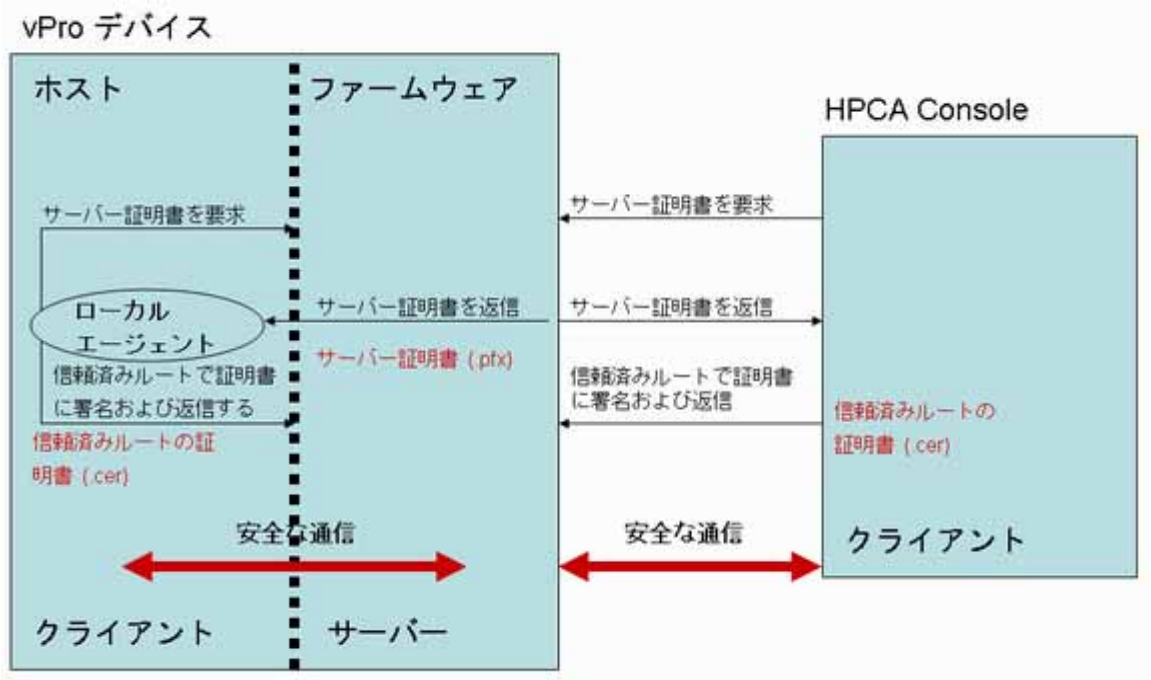
TLS (Transport Layer Security) プロトコルには、TLS サーバー認証 (一方向認証) および TLS 相互認証 (双方向認証) の 2 種類の認証方法があります。TLS プロトコルでは、vPro デバイスのファームウェアが SSL サーバーとなります。HPCA コンソールおよびホスト vPro デバイスで実行しているローカル エージェントは、クライアントとして動作します。

TLS サーバー認証

TLS サーバー認証で TLS セッションを確立するとき、クライアントは vPro デバイスのファームウェアから受信した SSL 証明書の有効性の検証を試みます。この検証を実行するには、クライアントは証明書に署名した証明機関 (CA) の公開キーを所有している必要があります。公開キーは、サーバー証明書を作成した CA と同じ CA が作成した信頼されたルート証明書内に存在します。信頼されたルート証明書は、ドメインの Active Directory に接続しているすべての vPro システム上にすでに存在します。クライアントは、サーバーの身元を証明する信頼されたルート証明書付きの証明書に署名し、サーバーに送り返します。これにより、クライアントがアプリケーション データをファームウェアに送信するときに、クライアントとして動作するコンポーネントと vPro デバイスのファームウェア間の通信が保護されます。

次の図では、ホスト デバイス上で実行しているローカル エージェントと HPCA コンソールは、両方とも vPro ファームウェアのクライアントです。ローカル エージェントの機能についての詳細は、この章で後述するほか、このガイドの各所で説明されています。

図 1　　TLS サーバー認証



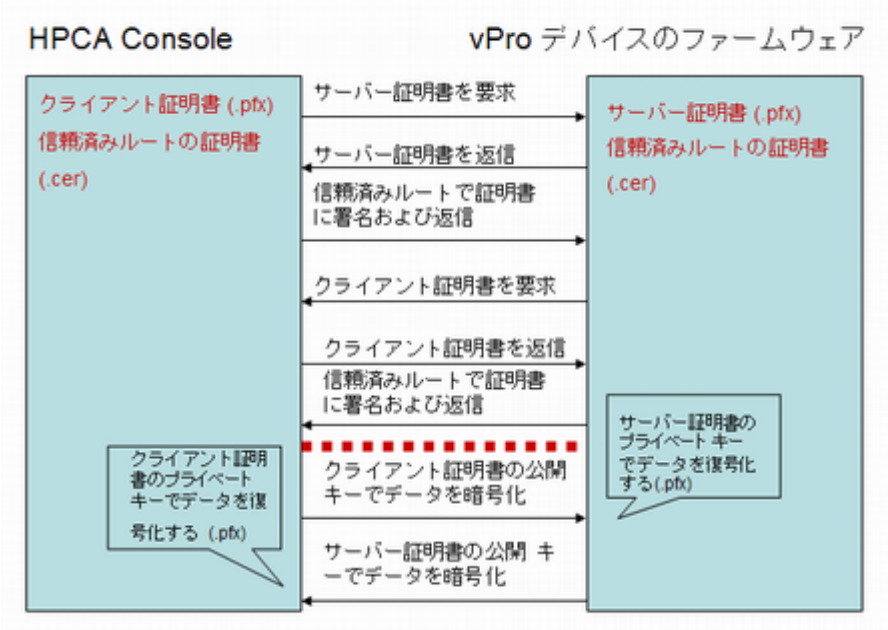
TLS 相互認証

クライアントとサーバー間で受け渡される証明書が 1 つのみの TLS サーバー認証に加え、TLS 相互認証は 2 つの証明書を受け渡して通信の両端の認証を行うため、より強力なセキュリティが提供されます。相互認証では、クライアントはサーバーによる署名が必要な証明書を送信し、同様にサーバーはクライアントにより署名される証明書を送信します。前述したように、公開および秘密の証明書キーを使用して、データを暗号化および復号化します。

このモデルでも、HPCA コンソールおよびローカル エージェントは SSL クライアントとして動作します。クライアントは、自身の SSL クライアント証明書を vPro デバイスに送信してクライアント認証を受ける必要があります。また、vPro デバイスは、検証 (クライアント証明書の署名) を行ために、ファームウェアにインポートされた信頼されたルート証明書 (公開キー) を所有している必要があります。

HPCA コンソールがクライアントである場合、信頼されるルート証明書は HPCA コンソール マシンの信頼キー ストアにもインポートされている必要があります。これにより HPCA コンソールは、サーバーを認証するために vPro デバイスが送信するサーバー証明書への署名が可能になります。HPCA コンソールにインストールされているクライアント証明書には、完全な証明書チェーンおよび証明書の秘密キーが含まれている必要があります。この機能によりクライアントとサーバー両方の相互認証が可能になり、TLS セッションのセキュリティ レベルが強化されます。次の図では、HPCA コンソールが vPro ファームウェアのクライアントとして動作しています。

図 2　　HPCA コンソールと vPro デバイス ファームウェア間の TLS 相互認証



vPro クライアント証明書の指定時にはいくつかの要件があります。タスクには次が含まれます。

- 証明書には、1.3.6.1.5.5.7.3.2 OID が含まれている必要があります。これは、TLS 証明書であることを示すものです。
- リーフ証明書の拡張キー使用法 OID リスト フィールドには、2.16.840.1.113741.1.2.1 OID が含まれている必要があります。OID は、HPCA コンソールを認証するために vPro デバイスにより使用されます。

26 ページの「クライアント認証テンプレートを作成するには」で説明しているサーバーおよびクライアント証明書テンプレートの作成手順で、これらの値を使用します。相互認証機能を使用するには、vPro デバイスは SSL クライアント証明書に署名しているルート証明書をデバイスの信頼リスト内に所有している必要があります。ルート証明書は、vPro デバイスのセットアップおよび設定プロセスで vPro デバイスに提供されます。詳細は、33 ページの「プロファイルの設定」で説明しています。

SCS Provisioning Server

Provisioning Server (Setup and Configuration Server とも呼ばれる) は、Intel Setup and Configuration Service (SCS) を実行するマシンです。SCS Provisioning Server は、vPro デバイスを動作させるために必要なすべての手順を実行します。

SCS のコンポーネント

SCS Provisioning Server の主なコンポーネントは次のとおりです。

- サーバーを起動するための Windows サービス (SCS Main Service)
- ルート証明書および PID/PPS キー ペアを格納するセキュアなデータベース
- SOAP API
- vPro デバイスをプロビジョニングする AMT SCS コンソール

vPro デバイスの SCS プロビジョニング

SCS Provisioning Server と vPro デバイス間の通信はセキュアです。SCS は vPro デバイスのセキュリティに関連する次の設定情報を生成して送信します。

- 公開キー インフラストラクチャ (PKI) からの証明書
- アクセス制御リスト (ACL)
- プラットフォームまたはプラットフォーム ファミリに特有なセットアップおよび設定情報のプロファイルで定義されたセットアップ パラメータ
- TLS (サーバー認証または相互認証) または TCP の認証タイプ
- プロビジョニング解除および再プロビジョニング オプション

SCS は、vPro デバイスに初期値を提供します。セットアップおよび設定には、プロファイルに含まれているか自動的に生成された次のパラメータの設定が含まれます。

- Administrator アカウントの認証情報 (ユーザー名とパスワード)
- Digest アカウント タイプのアクセス制御リスト (ACL)

  HPCA コンソールは Kerberos 認証をサポートしていません。Digenst 認証のみがサポートされます。

- ネットワーク設定 (ホスト名およびドメイン名)
- RSA キー ペアおよび TLS の X.509 証明書 (TLS 証明書および RSA 秘密キー) (自動)
- 疑似乱数生成器 (PRNG) の値
- 時刻と日付 (自動)
- 信頼されたルート証明書 (相互 TLS)
- 信頼されたドメイン名サフィックス (相互 TLS)
- 証明書失効リスト (CRL)
- 電源ポリシー オプション
- 代替 PID/PPS

SCS 設定シナリオ

公開キー インフラストラクチャ (PKI) に関する SCS Provisioning Server の設定には 2 通りの方法があります。

HPCA コンソールの OOBM 機能で必要とされるすべてのソフトウェア コンポーネント (Enterprise Root CA を含む) を、Provisioning Server という 1 台のマシンにインストールできます。これをセットアップ 1: Enterprise Root CA が Provisioning Server 上にあると呼びます。

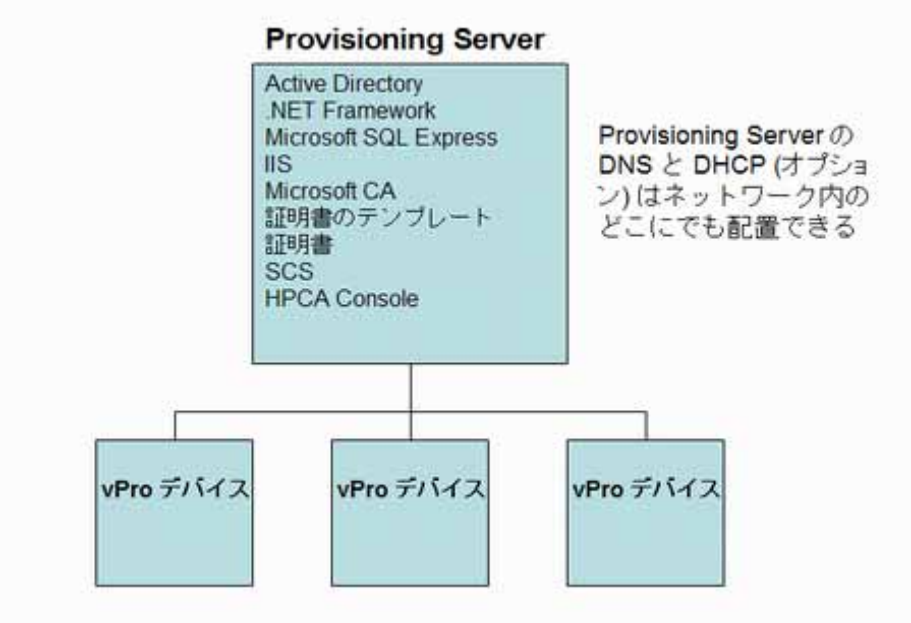
一方、Enterprise Root CA Server と Provisioning Server の 2 台のマシンを使用することもできます。これをセットアップ 2: Enterprise Root CA が Provisioning Server 上にないと呼びます。この設定では、証明書関連のコンポーネントと SCS 関連のソフトウェア コンポーネントが分離され、セキュリティが強化されます。

両方の設定で、vPro デバイス、Provisioning Server、Enterprise Root CA Server (該当する場合) は、同一のドメインに存在し、DHCP が有効になっている必要があります。

これらの 2 つの設定について、以降のセクションで詳細に説明します。

セットアップ 1: Enterprise Root CA が Provisioning Server 上にある

図 3　　セットアップ 1: Root CA が Provisioning Server 上にある



この設定では、すべてのソフトウェア コンポーネントが 1 台のマシン上に存在します。次のコンポーネントが含まれます。

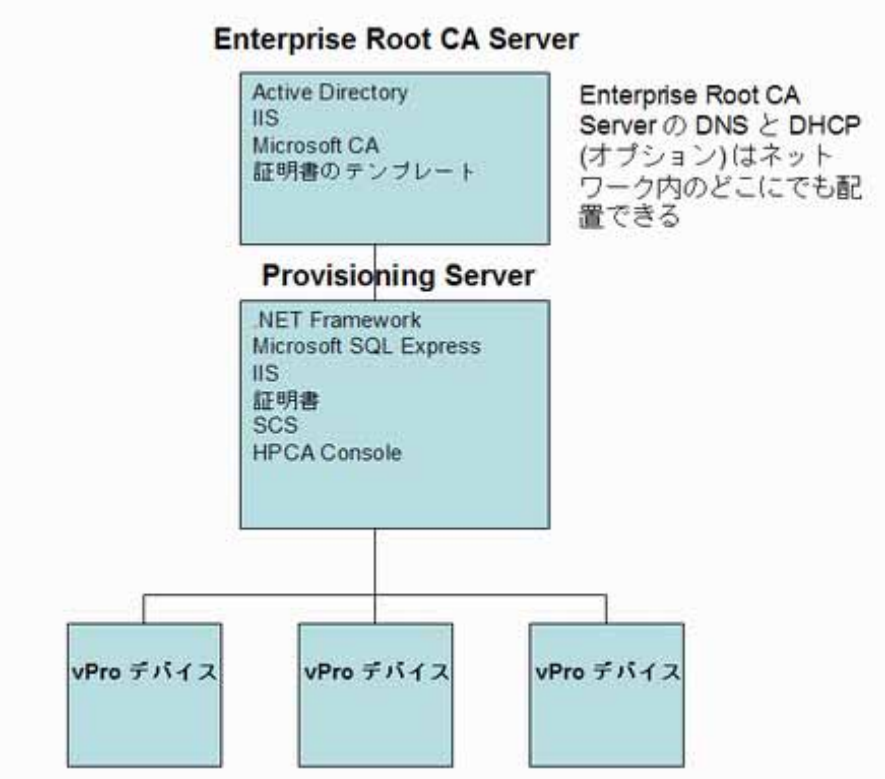
- Active Directory
- .NET Framework
- Microsoft SQL Server Express
- Internet Information Services (IIS)
- Microsoft CA および TLS 証明書のテンプレートと証明書
- SCS ソフトウェア
- HPCA コンソール

セットアップ 1 では、Enterprise Root CA が Provisioning Server 上にあり、Provisioning Server 上で証明書テンプレートが作成、発行、インストールおよびエクスポートされます。セキュリティ上の理由から Active Directory Service Server への管理アプリケーションのインストールは推奨されないため、このセットアップはプロダクション環境では実用的ではありません。Enterprise Root CA にはルート証明書の秘密キーが含まれているため、セキュアに扱う必要があります。

このセキュリティの点で、セットアップ 2 では、独立した Enterprise Root CA Server を使用して信頼されたルート証明書を取得し、TLS 認証で使用するクライアントおよびサーバーの証明書を作成するため安全です。

セットアップ 2: Enterprise Root CA が Provisioning Server 上にない

図 4　　セットアップ 2: Root CA が Enterprise Root CA Server 上にある



この設定では、Active Directory Service および Enterprise Root CA サービスが Enterprise Root CA Server にインストールされ、管理アプリケーションが Provisioning Server にインストールされています。ルート証明書の秘密キーが存在する Root CA Server の保護が強化されるため、この設定が推奨されます。

信頼されたルート証明書の取得、および TLS 認証で使用するサーバーおよびクライアントの証明書の作成には、Microsoft Enterprise Root CA Server が使用されます。証明書テンプレートは Enterprise Root CA Server 上で作成、発行、インストールおよびエクスポートされます。

異なるマシン上の HPCA と SCS

SCS と HPCA でサポートされるオペレーティング システムが異なるため、SCS ソフトウェアと HPCA ソフトウェアを別のマシンにインストールする場合があります。

SCS ドキュメントの最新のサポート マトリクスを確認して、SCS を正しくインストールできるプラットフォームを確認してください。これらのプラットフォームは、HPCA のインストールをサポートするプラットフォームのサブセットである場合があります。

非 TLS モード

TLS 認証を使用しない場合、SCS および HPCA コンソール ソフトウェアに別々のマシンを使用する場合は、設定に関して特別に考慮する事項はありません。すべての SCS 関連のソフトウェア (HPCA を除く) を 21 ページの「セットアップ 1: Root CA が Provisioning Server 上にある」に示すように Provisioning Server にインストールします。HPCA ソフトウェアを別のマシンにインストールします。

HPCA コンソールから、SCS サービスのログイン認証情報と URL を入力します。これにより、vPro デバイスにアクセスできるようになります。通常、URL は完全修飾ドメイン名 (FQDN) で指定します。

TLS モード

TLS 認証を使用している場合、HPCA コンソールと Provisioning Server 間の通信を確実にセキュアにするため、セキュリティ証明書のインストール場所を考慮する必要があります。

TLS 設定にセットアップ 1: Enterprise Root CA が Provisioning Server 上にあるを使用している場合、すべての SCS 関連のソフトウェア (HPCA を除く) を 21 ページの「セットアップ 1: Root CA が Provisioning Server 上にある」に示すように以前と同様に Provisioning Server にインストールします。HPCA ソフトウェアを別のマシンにインストールします。クライアント証明書を発行して、HPCA ソフトウェアをインストールするマシンにインストールする必要があります。クライアントおよびサーバー証明書を Provisioning Server にインストールする必要があります。

TLS 設定にセットアップ 2: Enterprise Root CA が Provisioning Server 上にないを使用している場合、Active Directory Service と Enterprise Root CA サービスを 22 ページの「セットアップ 2: Root CA が Enterprise Root CA Server 上にある」に示すように以前と同様に Enterprise Root CA Server にインストールします。その他のすべての SCS 関連ソフトウェア (HPCA を除く) を、22 ページの「セットアップ 2: Root CA が Enterprise Root CA Server 上にある」に示すように Provisioning Server にインストールします。HPCA ソフトウェアを別のマシンにインストールします。クライアント証明書を発行して、HPCA ソフトウェアをインストールするマシンにインストールする必要があります。クライアントおよびサーバー証明書を Provisioning Server にインストールする必要があります。

HPCA コンソールからでも、SCS ログイン認証情報、および SCS サービスの URL を入力する必要があります。これは、セキュリティ証明書があることにより、通信の安全性が確保されるためです。

全般要件

サーバーのオペレーティング システム要件は、Windows Server 2003 Standard Edition または Windows Server 2003 Enterprise Edition (32 ビットのみ) です。

Active Directory との統合

vPro デバイス、Provisioning Server、Enterprise Root CA Server (セットアップ 2 を使用している場合) は、同一のドメインに存在している必要があります。Intel vPro デバイスは、Active Directory の Computers (CN) ドメインに属している必要があります。

DHCP サーバーおよびドメイン ネーム サーバーが起動している必要があります。DHCP および DNS がすでにインストールされていることを想定していますが、Enterprise Root CA Server と同じマシンにインストールされている必要はありません。

.NET Framework 2.0 のインストール

Provisioning Server に、.NET Framework 2.0 をインストールします。HPCA Core 配布メディアの `Media\oobm\win32\AMT Config Server` ディレクトリにある、*Intel AMT SCS Version 5.0 Installation Guide* を参照してください。

Microsoft SQL Server Express のインストール

Provisioning Server に、Microsoft SQL Server Express をインストールします。*Intel AMT SCS Version 5.0 Installation Guide* を参照してください。

Internet Information Services (IIS) 6.0 のインストール

Provisioning Server および Enterprise Root CA Server (セットアップ 2 を使用している場合) に、Internet Information Services (IIS) 6.0 をインストールします。*Intel AMT SCS Version 5.0 Installation Guide* を参照してください。

サーバー証明書が IIS Web サーバー環境にインポートされている必要があります。SCS は IIS アプリケーションであることから、SCS コンソールとのセキュアな通信に HTTPS プロトコルが必要となるため、このサーバーには証明書が必要です。サーバー証明書の作成、発行、インストール、エクスポートおよびインポートの手順については、31 ページの「IIS Server 証明書の設定」で説明しています。

TLS の証明書のセットアップ

HPCA コンソールで TLS 認証をセットアップすると、TLS を使用するように設定されている vPro デバイスのみを管理できるようになります。逆に HPCA コンソールで TLS 認証をセットアップしていない場合は、TLS を使用するように設定されていない vPro デバイスのみを管理できます。

HPCA コンソールと vPro デバイスの間で TLS 相互認証をセットアップする場合に限り、このセクションに目を通してください。TLS を必要としない場合は、30 ページの「SCS の設定」に進みます。

Microsoft CA のインストール

Microsoft CA を使用すると、クライアント証明書を作成し、信頼されたルート証明書とともにエクスポートして、TLS 認証に使用できます。

Microsoft CA によってエクスポートされた信頼されたルート証明書は、CA の公開キーです。Microsoft CA で作成されたクライアント証明書およびサーバー証明書はすべて、このキーで署名されます。CA によってエクスポートされた信頼されたルート証明書は、その CA の証明書を確認する必要のあるすべてのコンピュータにローカルにインストールする必要があります。このため、ルート証明書は、HPCA コンソールと vPro デバイスの両方で必要になります。

クライアント証明書

前述のとおり、Microsoft CA は、クライアント証明書を作成するときに使用されます。Microsoft CA の秘密キーはエクスポートされ、ある形式に変換されます。この変換された秘密キーを使用することにより、HPCA コンソールは、vPro デバイスとセキュアな IDE-R/SOL 操作を実行することができます。

サーバー証明書

vPro デバイスのプロファイルを設定するときに TLS を選択すると、SCS Server がそのデバイスをプロビジョニングする際に、そのデバイスのサーバー証明書がデバイスのファームウェアに自動的にインポートされます。

ルート証明書

信頼されたルート証明書は CA の公開キーです。サーバーとクライアントは、この公開キーを使用して、TLS 相互認証の際に交換されるサーバー証明書およびクライアント証明書に付いているデジタル署名を確認します。

セットアップ 1 (単一マシン セットアップ) を使用する場合は、次の手順を Provisioning Server 上で実行してください。セットアップ 2 (デュアル マシン セットアップ) を使用する場合は、次の手順を Enterprise Root CA Server 上で実行してください。

Microsoft CA をインストールするには

1. Windows の **[スタート]** ボタンをクリックして、**[コントロール パネル]** を選択します。
2. **[プログラムの追加と削除]** をダブル クリックします。
3. 左側のパネルにある **[Windows コンポーネントの追加と削除]** をクリックします。
4. **[証明書サービス]** チェック ボックスをオンにします。証明書サーバーとして動作している間はコンピュータ名またはコンピュータのドメイン メンバーシップを変更できないという旨の警告メッセージが表示されます。**[はい]** をクリックしてメッセージ ウィンドウを閉じます。
5. **[詳細]** をクリックします。
6. **[証明書サービス CA]** チェック ボックスと **[証明書サービス Web 登録のサポート]** チェック ボックスをオンにして、証明書サービスのサブコンポーネントを指定します。**[OK]** をクリックします。
7. [Windows コンポーネント] ウィンドウで、**[次へ]** をクリックします。[CA の種類] ウィンドウが表示されます。
8. 設定する証明書の種類として **[エンタープライズのルート CA]** を選択します。**[次へ]** をクリックします。[CA 識別情報] ダイアログが表示されます。
9. [CA 識別情報] ダイアログで、次の項目を指定します。
   - **この CA の共通名** : CA をインストールするコンピュータの名前と同じ名前を指定する必要があります。

— **識別名のサフィックス** : 次のように指定します。例 : **DC=AMT,DC=HP,DC=COM**

10 Windows コンポーネントの設定ウィザードの残りの手順を完了します。すべての手順を完了したら **[完了]** をクリックします。

これで Microsoft CA ソフトウェアがインストールされます。Microsoft CA を使用すると、クライアント証明書の作成 (次のセクションを参照)、および認証プロセスでの署名に使用する信頼されたルート証明書のエクスポートを実行できます。エクスポートの手順については、29 ページの「ルート証明書のエクスポート」で説明します。

クライアント証明書テンプレートの作成

次に、TLS 相互認証を行うためのクライアント証明書を作成する必要があります。クライアント証明書は HPCA コンソールにインストールされ、PEM 形式に変換されて、リダイレクション操作をセキュリティ保護された状態で実行するために使用されます。詳細については、アウトバンド管理設定の章の 62 ページの「クライアント証明書を PEM 形式に変換するには」を参照してください。

証明書テンプレートは、証明書リクエスタが、CA によって使用されるポリシーに応じて証明書を要求するときの選択操作を簡略化するために使用します。したがって、証明書を作成するには、まず、証明書のテンプレートを作成します。

セットアップ 1 (単一マシン セットアップ) を使用する場合は、次の手順を Provisioning Server 上で実行してください。セットアップ 2 (デュアル マシン セットアップ) を使用する場合は、次の手順を Enterprise Root CA Server 上で実行してください。

クライアント認証テンプレートを作成するには

1 Windows の **[スタート]** ボタンをクリックして、**[ファイル名を指定して実行]** を選択します。

2 「MMC」と入力して **[OK]** をクリックします。[コンソール 1] が表示されます。

3 [ファイル] メニューで、**[スナップインの追加と削除]** を選択します。

4 **[追加]** をクリックします。[スタンドアロン スナップインの追加] ダイアログ ボックスが表示されます。

5 **[証明書テンプレート]** を選択し、**[追加]** をクリックして、**[閉じる]** をクリックします。

6 [スナップインの追加と削除] ウィンドウで **[OK]** をクリックします。

7 左側のペインで、**[証明書テンプレート]** をクリックします。既存のすべてのテンプレートがコンソールの右側のペインに表示されます。

8 Web サーバー テンプレートを右クリックして、**[テンプレートの複製]** を選択します。

9 **[全般]** タブで、次の各項目を指定します。

— **テンプレート表示名** : テンプレートを表示するときに使用するテンプレートの名前です。たとえば、「ClientAuthTmpl」などと指定します。

— **テンプレート名** : テンプレートの名前です。表示名と同じ名前でもかまいません。

— **[Active Directory の証明書を発行する]** チェック ボックスをオンにします。

10 **[要求処理]** タブで、**[秘密キーのエクスポートを許可する]** チェック ボックスをオンにします。

11 **[拡張]** タブで **[アプリケーション ポリシー]** を選択し、**[編集]** をクリックします。[アプリケーション ポリシーの拡張の編集] ウィンドウが表示されます。デフォルトで、[サーバー認証] ポリシーが表示されます。

12 **[サーバー認証]** ポリシーを選択し、**[削除]** をクリックします。アプリケーション ポリシーの一覧が空になります。

13 **[追加]** をクリックします。[アプリケーションのポリシーの追加] ウィンドウが表示されます。

14 [アプリケーションのポリシーの追加] ウィンドウで、**[クライアント認証]** ポリシーを選択して、**[OK]** をクリックします。[アプリケーションのポリシーの追加] ウィンドウが閉じ、[アプリケーション ポリシーの拡張の編集] ウィンドウが表示されます。アプリケーション ポリシーの一覧に [クライアント認証] ポリシーが表示されます。

15 [アプリケーション ポリシーの拡張の編集] ウィンドウで、**[追加]** をクリックします。[アプリケーションの追加] ウィンドウが表示されます。

16 **[新規]** をクリックします。[新しいアプリケーションのポリシー] ウィンドウが表示されます。

17 アプリケーション ポリシーの名前 (例 : AMTRemote) とオブジェクト識別子 (例 : 2.16.840.1.113741.1.2.1) を入力します。このポリシーは、サーバー証明書の秘密キーのエクスポートを許可します。

> 同じオブジェクト識別子を持つポリシーがすでに存在している場合は、そのポリシーを一覧から選択できます。同じオブジェクト識別子を持つポリシーを再作成することはできません。

18 **[OK]** を 3 回クリックします。アプリケーション ポリシーを追加すると、[アプリケーション ポリシー] の説明一覧に、クライアント認証ポリシーと AMTRemote ポリシーが表示されます。

19 発行ポリシーの編集で **[追加]** をクリックします。**[すべての発行ポリシー]** を選択し、**[OK]** を 2 回クリックします。すべての発行ポリシー オプションが [発行ポリシーの説明] 一覧に表示されます。

20 **[セキュリティ]** タブで、**[Domain Admins]** を選択し、読み取り、書き込み、登録、自動登録の各アクセス許可を設定します。**[Enterprise Admins]** を選択し、読み取り、書き込み、登録、自動登録の各アクセス許可を設定します。**[Authenticated users]** を選択し、読み取りアクセス許可を設定します。

21 その他のタブ (**[発行の要件]**、**[優先するテンプレート]**、および **[サブジェクト名]**) は一切変更する必要はありません。

22 **[適用]**、**[OK]** の順にクリックします。新規のクライアント認証用テンプレートが、[証明書テンプレート] の右側のペインに表示されます。

クライアント証明書テンプレートの発行

証明書をインストールするには、まず、証明書テンプレートを発行する必要があります。証明書テンプレートを発行すると、そのテンプレートが証明書になります。

セットアップ 1 (単一マシン セットアップ) を使用する場合は、次の手順を Provisioning Server 上で実行してください。セットアップ 2 (デュアル マシン セットアップ) を使用する場合は、次の手順を Enterprise Root CA Server 上で実行してください。

クライアント証明書テンプレートを発行するには

1 Windows の **[スタート]** ボタンをクリックして、**[管理ツール]**、**[証明機関]** の順に選択します。

2 インストールされている CA を展開します。証明書テンプレートを右クリックして、**[新規作成]**、**[証明書テンプレートの発行]** の順にクリックします。[証明書テンプレートの有効化] ウィンドウが表示されます。

3 26 ページの「クライアント証明書テンプレートの作成」で作成したクライアント認証テンプレートを選択します。例では、**ClientAuthTmpl** テンプレートを選択しています。

4 **[OK]** をクリックします。発行済みの証明書テンプレートが、[証明書テンプレート] ウィンドウの右側のペインに表示されます。

クライアント証明書のインストール

これで、テンプレートを使用して、Provisioning (SCS) Server の Windows 証明書ストアにクライアント証明書をインストールする準備が整いました。クライアント証明書は最終的に、このストアからエクスポートされ、HPCA コンソールにコピーされて、PEM 形式に変換されます。この証明書を使用してクライアント認証を行うことで、vPro デバイスに対するリダイレクション操作をセキュリティ保護された状態で実行できます。

クライアント証明書をインストールするには

1 Provisioning Server 上で、設定に応じて、次のいずれかの URL に移動します。

— セットアップ 1 (単一マシン設定): **http://***FQDN_ProvisioningServer***/certsrv**

— セットアップ 2 (デュアル マシン設定): **http://***FQDN_EnterpriseCARootServer***/certsrv**

コンピュータの完全修飾ドメイン名 (FQDN) は、そのコンピュータの Windows デスクトップで確認できます。**[マイ コンピュータ]** を右クリックして、**[プロパティ]** を選択し、**[コンピュータ名]** タブを選択します。

上記の URL が、ブラウザの信頼済みサイト一覧に追加されていることを確認します。上記のサイトを追加するには、次の手順を実行します。

a ブラウザで、**[ツール]**、**[インターネット オプション]**、**[セキュリティ]**、**[信頼済みサイト]** の順に選択します。

b **[サイト]** をクリックします。[信頼済みサイト] ウィンドウが表示されます。

c **[次の Web サイトをゾーンに追加する]** フィールドに追加するサイトの URL を入力します。

d **[追加]** をクリックします。

e **[このゾーンのサイトにはすべてサーバーの確認 (https :) を必要とする]** チェック ボックスをオフにします。

f **[OK]** をクリックします。

2 **[証明書の要求]** をクリックします。**[証明書の要求の詳細設定]** をクリックします。**[この CA への要求を作成し送信する]** をクリックします。

3 **[証明書テンプレート]** プルダウン リストでクライアント証明書テンプレートを選択します。例では、`[ClientAuthTmpl]` を選択しています。

4 **[オフライン テンプレート用の識別情報]** の **[名前 :]** フィールドには、Provisioning Server の完全修飾名を入力する必要があります。

5 **[エクスポート可能なキーとしてマークする]** チェック ボックスを選択します。

6 **[送信]** をクリックします。続くウィンドウで **[はい]** を選択して、証明書をインストールします。

クライアント証明書のエクスポート

この手順では、前の手順で、Windows 証明書ストアにインストールしたクライアント証明書の秘密キー ファイル (`.pfx`) をエクスポートします。クライアント 秘密キーは、HPCA コンソールにインストールされた後、PEM 形式に変換されます。TLS 相互認証が有効になっている場合は、この PEM 形式の秘密キーを使用することによって、IDE-R/SOL 操作をセキュリティが保護された状態で実行できます。具体的な変換方法については、アウトバンド管理設定の章の 62 ページの「クライアント証明書を PEM 形式に変換するには」を参照してください。

クライアント証明書をエクスポートするには

1 Provisioning Server 上で、Windows の **[スタート]** ボタンをクリックし、[ファイル名を指定して実行] を選択します。

2 「MMC」と入力して **[OK]** をクリックします。[コンソール 1] が表示されます。

3 [ファイル] メニューで、**[スナップインの追加と削除]** を選択します。

4 **[追加]** をクリックします。

5 **[証明書]** を選択し、**[追加]** をクリックします。

6 **[マイ アカウント]** を選択し、**[完了]** をクリックします。

7 **[閉じる]**、**[OK]** の順にクリックします。

8 [コンソール 1] の左側のパネルで、[証明書 - 現在のユーザー] ノードを展開します。

9 [個人] ノードを展開します。

10 **[証明書]** を選択します。

11 右側のパネルで、クライアント証明書を右クリックします。ポップアップ メニューが表示されます。**[目的]** タブに、インストール済みのクライアント証明書が表示されています。

12 **[開く]** を選択します。[証明書情報] ウィンドウが表示されます。

13 **[詳細]** タブを選択します。

14 **[ファイルにコピー]** をクリックします。証明書エクスポート ウィザードの [ようこそ] ウィンドウが表示されます。

15 **[次へ]** をクリックします。[秘密キーのエクスポート] ウィンドウが表示されます。

16 **[はい、秘密キーをエクスポートします]** を選択して、**[次へ]** をクリックします。[エクスポート ファイルの形式] ウィンドウが表示されます。**[次へ]** をクリックします。

17 秘密キーを保護するパスワードを入力し、確認用にもう一度入力します。このパスワードは、証明書をインポートするとき必要になります。**[次へ]** をクリックします。

18 ファイルの名前を入力します。フルパスを指定してください。ファイルの種類を示すファイルのサフィックス (.pfx) は自動的に生成されます。このフルパスは後の手順で使用するためメモしておきます。

19 **[次へ]**、**[完了]** の順にクリックします。

20 **[OK]** をクリックして [証明書情報] ウィンドウを閉じます。

21 HPCA コンソールと Provisioning Server が異なるマシンの場合は、証明書ファイルを HPCA コンソール コンピュータ上の特定の場所にコピーします。

ルート証明書のエクスポート

この手順では、Windows 証明書ストアに格納された信頼されたルート証明書を .cer ファイルとしてエクスポートして、TLS 相互認証プロセスで使用できるようにします。ルート証明書は、サーバー証明書とクライアント証明書に付いているデジタル署名を確認するために、vPro デバイスと HPCA コンソールの両方で必要になります。

- vPro デバイスでは、SCS によってルート証明書がプロビジョニングされ、デバイスのプロファイルが設定されます (33 ページの「プロファイルの設定」を参照)。vPro デバイスでルート証明書が必要になるのは、管理コンソールから vPro デバイスにクライアント証明書が送信されてきたとき、vPro デバイスが HPCA コンソール クライアントの ID を認証できるようにするためです。
- HPCA コンソールでは、ルート証明書を Java キー ストアに追加して (アウトバンド管理設定の章のルート証明書を Java キー ストアにインポートするにはで説明する手順を参照)、vPro デバイスから管理コンソールにサーバー証明書が送信されてきたとき、Pro デバイス サーバーの ID を認証できるようにします。信頼されたルート証明書は、vPro デバイスに署名するときに使用されます。これにより、ハードウェア / ソフトウェア クエリやリモート制

御機能を認証できます。また、信頼されたルート証明書は、PEM 形式に変換されます (アウトバンド管理設定の章の 62 ページの「ルート証明書を PEM 形式に変換するには」を参照)。TLS 相互認証が有効になっている場合は、この PEM 形式の秘密キーを使用することによって、IDE-R/SOL 操作をセキュリティ保護された状態で実行できます。

セットアップ 1 (単一マシン セットアップ) を使用する場合は、次の手順を Provisioning Server 上で実行してください。セットアップ 2 (デュアル マシン セットアップ) を使用する場合は、次の手順を Enterprise Root CA Server 上で実行してください。

ルート証明書をエクスポートするには

1. Windows の **[スタート]** ボタンをクリックして、**[管理ツール]**、**[証明機関]** の順に選択します。
2. ウィンドウの左側の、インストール済みの CA 上で右クリックします。ポップアップ メニューが表示されます。
3. **[プロパティ]** をクリックし、**[全般]** タブを選択します。
4. 証明書を選択し、**[証明書の表示]** をクリックします。
5. **[詳細]** タブを選択します。
6. **[ファイルにコピー]** をクリックします。ファイルの名前を入力します。フルパスを指定してください。ファイルの種類を示すファイルのサフィックス (`.cer`) は自動的に生成されます。このフルパスは後の手順で使用するためメモしておきます。
7. ウィザードの残りの手順を完了します。エクスポートに成功したことを示すメッセージが表示されます。**[OK]** をクリックします。**[詳細]** タブに戻ります。
8. **[OK]** を 3 回クリックします。認証機関管理コンソールに戻ります。コンソールを閉じます。
9. デュアル マシン セットアップを使用している場合は、Provisioning Server 上の特定の場所に証明書ファイルをコピーします。

SCS の設定

vPro デバイスとのすべての通信が安全に行われるように、Setup and Configuration Service (SCS) を設定する必要があります。

SCS のインストール

SCS は、Provisioning Server 上にインストールされます。21 ページの「SCS 設定シナリオ」を参照してください。

SCS をインストールするには

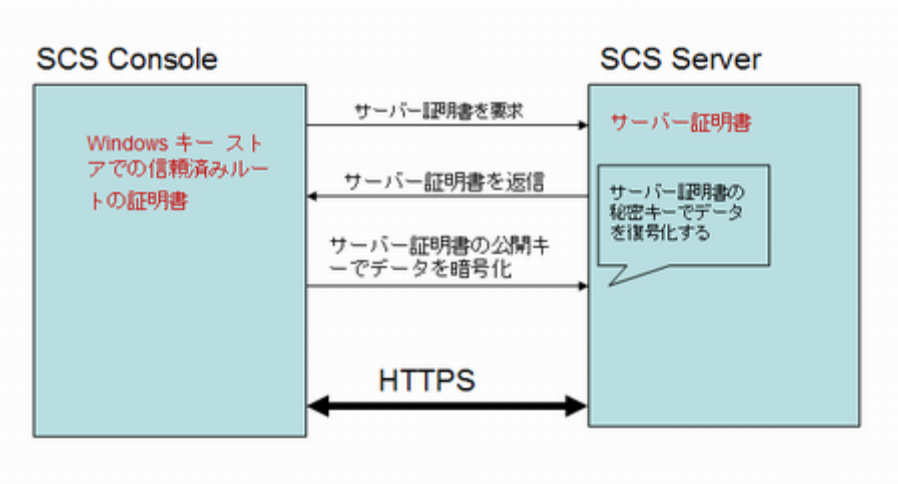
SCS のコンポーネントのインストール方法については、HPCA Core 配布メディアの `Media\oobm\win32\AMT Config Server` ディレクトリにある *Intel AMT SCS Version 5.0 Installation Guide* の「Installation」の章を参照してください。

SCS ドキュメントの最新のサポート マトリクスを確認して、SCS を正しくインストールできるプラットフォームを確認してください。これらのプラットフォームは、HPCA のインストールをサポートするプラットフォームのサブセットである場合があります。

IIS Server 証明書の設定

SCS Server と SCS コンソール間で安全な通信を行うには、サーバー証明書が必要です。次の図に、両者間で実行される認証プロセスを示します。

図 5　　SCS 認証



このような証明書を作成するには、Microsoft 証明機関を使用する方法があります。

Intel AMT SCS Version 5.0 Installation Guide の「Installing Microsoft's Certificate Authority」セクションにある「Securing the Connection to IIS Using SSL」の項を参照してください。

サーバー証明書は、32 ページの「SCS 認証」に示した手順に従って、SCS Provisioning Server 上にインストールする必要があります。

AMT SCS Console へのログイン

AMT SCS Console にログインするには

1. Provisioning Server 上で、Windows の **[スタート]** ボタンをクリックし、**[Intel AMT Configuration]**、**[Intel AMT SCS Console]** の順に選択します。ログイン ウィンドウが表示されます。
2. [Service Name] フィールドに、SCS Web サービスの URL パス (仮想ディレクトリを含む) を入力します。サービス名の形式は次のとおりです。**<**`http|https`**>://<***`Provision Server の完全修飾ドメイン名`***>/<***`SCS Web サービスの仮想ディレクトリ`***>**

   Intel AMT SCS Console が表示されます。

SCS サービスの設定

SCS サービスを設定するには

1. Intel AMT SCS Console を起動します。
2. **[Tools]**、**[Console Settings]** の順に選択します。[SCS Service Settings] ウィンドウが表示されます。
3. [SCS Service Settings] ウィンドウで、次の各項目を指定します。
   - **Active Directory の統合** : プルダウン リストから **[None]** を選択します。
   - **証明書件名の最初の共有名 (CN)**: プルダウン リストから **[Fully Qualified Domain Name]** を選択します。
   - **TCP リスナー ポート** : プルダウン リストから **[9971]** を選択します。
   - **AMT は、設定前に承認を必要とする** : このチェック ボックスをオフにします。
   - **リモート設定を許可** : このチェック ボックスをオンにします。

— **ワンタイム パスワードを必要とする** ：遅延リモート設定を実行する際にセキュリティを向上させる必要がある場合は、このチェック ボックスをオンにします。このチェック ボックスをオンにすると、ベア メタル リモート設定が異常終了します。詳細については、38 ページの「リモート設定による vPro デバイスの設定」を参照してください。

4 **[Apply]** をクリックします。

5 **[Logging]** タブを選択します。**[Log Level]** として **[Verbose]** を選択します (オプションですが、設定することを推奨します)。

6 **[Apply]** をクリックします。

7 **[Intel AMT Configuration]** タブを選択します。**[Retrieve configuration parameters from database]** オプションを選択します。

8 **[Apply]** をクリックします。

9 その他のデフォルトの設定はすべてそのまま使用できます。

詳細については、『Intel AMT SCS Version 5.0 Console User's Guide』の「Viewing and Configuring SCS Services」セクションを参照してください。

セキュリティ キーの設定

この手順は、Management Engine BIOS Extension (MEBx) を介して、事前共有キー (PSK) モードで、vPro デバイスを手動設定する場合のみ必要になります。37 ページの「MEBx による vPro デバイスの設定」を参照してください。

リモート設定を介して、公開キー インフラストラクチャ (PKI) モードで、vPro デバイスを自動的に設定する場合は、この手順を実行する必要はありません。38 ページの「リモート設定による vPro デバイスの設定」を参照してください。

セキュリティ キーを設定するには

1 Intel AMT SCS Console を起動します。

2 **[Advanced]**、**[TLS-PSK Security Keys]** の順に選択します。

3 [Result Area] を右クリックし、コンテキスト メニューから **[Add Security Keys]** を選択します。[Create TLS-PSK keys] ウィンドウが表示されます。

4 [Create TLS-PSK keys] ウィンドウでは、次の各項目を指定します。

— **格納するキーの数 (プラットフォームごとに 1 つのキー):** このオプションには、生成される PID/PPS キーのペア数を指定します。例では、2 に設定しています。

— **工場出荷時のデフォルトの MEBx パスワード** ：このフィールドには、工場出荷時のデフォルトのパスワードが表示されます。

— **新規の MEBx パスワード** : このフィールドには、新規のパスワードが表示されます。**[Fixed Password]** を選択して、新規のパスワードを設定することを推奨します。

5 **[OK]** をクリックします。

詳細については、『Intel AMT SCS Version 5.0 Console User's Guide』の「Using USB Drives for TLS-PSK Keys」セクションの「Configuring Pre-Setup and Configuration Security Keys」の項を参照してください。

プロファイルの設定

このプロファイルは、36 ページの「新規 vPro システムの作成」で説明するとおり、vPro デバイスに関連付けられます。プロファイルは、プロビジョニング プロセスで、vPro デバイスに初期値を与えるために使用されます。

無線インターフェイスを搭載した vPro デバイスのプロファイルを設定する場合は、まず、無線ルータの無線アクセス ポイントに WPA-TKIP プロファイルを設定する必要があります。詳細な手順については、無線ルータ付属のドキュメントを参照してください。

ルータの無線アクセス ポイントを介して WPA-TKIP プロファイルを設定するには、次のように値を設定する必要があります。

- 無線モードを WPA – Personal (Wi-Fi Protected Access) に設定する。
- 暗号化アルゴリズムを TKIP (Temporal Key Integrity Protocol) に設定する。

プロファイルを作成する際には、次のガイドラインに従ってください。

- ACL のユーザー タイプとして **[Digest User]** を選択します。Digest User は、HPCA コンソールでサポートされている唯一のユーザー タイプです。
- TLS では、HPCA コンソールと vPro デバイス間でリモート インターフェイスを使用できるように、**[Use mutual authentication]** を有効にします。

プロファイルを設定するには

1. Intel AMT Console を起動します。
2. **[Profiles]**、**[All Profiles]** の順に選択します。
3. [Result Area] を右クリックし、コンテキスト メニューから **[Add Profile]** を選択します。プロファイルの追加ウィザードが表示されます。
4. **[Next]** をクリックして続行します。[General Settings] ウィンドウが表示されます。
5. [General Settings] ウィンドウでは、次の各項目を指定します。
   - **プロファイル名** : プロファイルの名前を入力します (例 : **PSGProfile**)。
   - **説明** : プロファイルの説明を入力します (例 : **PSG のプロファイル**)。
6. **[Next]** をクリックします。[Advanced Settings] ウィンドウが表示されます。
7. [Advanced Settings] ウィンドウで、次の各項目を指定します。
   - プラットフォーム インターフェイスの設定 : **[Web UI]**、**[Serial Over LAN]**、**[IDE Redirection]** の各インターフェイスを有効にします。
   - 電源管理設定 : デフォルトの設定を受け入れます。
   - 追加の設定 : **[Set]** をクリックします。[Advanced profile settings] ウィンドウが表示されます。
8. [Advanced profile settings] ウィンドウで、次の各項目を指定します。
   - 新規 MEBx パスワード : **[New password for certificate based configuration]** には、PSK の MEBx パスワードを入力します。PSK は、vPro デバイスのプロビジョニングに使用されます。これは、33 ページの「セキュリティ キーを設定するには」の手順 4 で作成したパスワードです。
   - 設定暗号化モード : デフォルトの設定を受け入れます。
   - Kerberos: デフォルトの設定を受け入れます。
   - ネットワーク設定 : **[Enable ping responses]** を選択します。
9. **[OK]** をクリックします。
10. **[Next]** をクリックします。[Optional Settings] ウィンドウが表示されます。
11. [Optional Settings] ウィンドウでは、次の各オプションを有効にします。
    - **ACL**
    - **プラットフォームに対する操作に TLS で保護された通信を使用** (TLS による通信を使用する場合のみ必須)

— **WiFi ネットワークに対する接続を許可** (無線 NIC を使用して管理する場合のみ必須)

12 **[Next]** をクリックします。[ACL Details] ウィンドウが表示されます。

13 **[Add]** をクリックします。

14 [ACL Details] ウィンドウでは、次の各項目を指定します。

— **ユーザー タイプ :[Digest User]** を選択します。

— **ユーザー / グループ名** : このタイプのアカウントのユーザー名を入力します。

— **パスワード** : このアカウントのパスワードを入力し、**[Mask]** を有効にします。

— **アクセス タイプ** : プルダウン リストから **[Both]** を選択します。

— **領域** : 一覧表示された適切な領域にチェック マークを入れます。領域によって、HPCA コンソールで vPro デバイスを管理するとき、このユーザー アカウントが実行できる操作のタイプが決まります。最初に作成するアカウントでは、[Security Audit Log Realm] を除くすべての領域を選択することを推奨します。

15 **[OK]** をクリックします。

— [Optional Settings] で ACL と TLS のみを有効にした場合は、**[Next]** をクリックして手順 16 に進みます。

— [Optional Settings] で ACL と WiFi ネットワークのみを有効にした場合は、**[Next]** をクリックして手順 18 に進みます。

— [Optional Settings] で ACL、TLS、および WiFi ネットワークを有効にした場合は、**[Next]** をクリックして手順 16 に進み、以降のすべての手順を実行します。

— [Optional Settings] で TLS と WiFi ネットワークの両方を無効にした場合は、**[Next]** をクリックして **[Finish]**(最後の手順) をクリックします。

16 [TLS] ウィンドウでは、次の各項目を指定します。

— TLS 基本設定 : **[TLS Server Certification Authority]** では、プルダウン リストから [CA] を選択します。**[Server Certificate Template]** では、プルダウン リストから **[WebServer]** を選択します。

— 高度な TLS 設定 : **[Use mutual authentication]** を有効にします。一覧で、使用する信頼された TLS ルート証明書にチェック マークを付けます。

— **[Add]** をクリックします。[Add Trusted Root Certificate] ウィンドウが表示されます。このウィンドウで、**[From File]** を選択し、29 ページの「ルート証明書のエクスポート」で示した手順に従ってエクスポートしたルート証明書を参照します。ルート証明書の内容は表示することができます。**[OK]** をクリックして、作業を完了します。

17 [Optional Settings] ウィンドウで **[Next]** をクリックします。[Finish] ウィンドウが表示された場合は、**[Finish]** (最後の手順) をクリックします。それ以外の場合で、WiFi ネットワーク オプションを選択していた場合は、[Optional Settings: WiFi] ウィンドウが表示されます。

18 **[Add]** をクリックします。[WiFi Profile] ウィンドウが表示されます。

19 [WiFi Profile] ウィンドウでは、次の各項目を指定します。

— **プロファイル名** : 全般プロファイルの名前とは異なるプロファイルの一意な名前を入力します (例 : PSGWirelessProfile)。

— **SSID**: ルータの無線アクセス ポイントで WPA-TKIP プロファイルを設定するときに使用した SSID 値を入力します。無線ルータのドキュメントを参照してください。

— **キー管理プロトコル** : プルダウン リストから [WiFi Protected Access (WPA)] を選択します。

— **暗号化アルゴリズム** : プルダウン リストから [Temporal Key Integrity Protocol (TKIP)] を選択します。

— **パスフレーズ**：ルータの無線アクセス ポイントで WPA-TKIP プロファイルを設定するときに使用したパスフレーズを入力します。無線ルータのドキュメントを参照してください。

20 **[Apply]**、**[OK]** の順にクリックします。

21 作成した無線プロファイルにチェック マークを付けて、**[Next]** をクリックします。[Finish] ウィンドウが表示されます。

22 **[Finish]** をクリックします。プロファイルが作成されます。

詳細については、『Intel AMT SCS Version 5.0 Console User's Guide』の「Creating and Changing Profiles」セクションの「Creating a Profile」の項を参照してください。

新規 vPro システムの作成

PSK モードで vPro デバイスをプロビジョニングするには、そのデバイスに関する情報を SCS に入力しておく必要があります。次に、プロビジョニング情報の入力手順を示します。

この手順は、Management Engine BIOS Extension (MEBx) を介して、事前共有キー (PSK) モードで、vPro デバイスを手動設定する場合のみ必要になります。37 ページの「MEBx による vPro デバイスの設定」を参照してください。

リモート設定を介して、公開キー インフラストラクチャ (PKI) モードで、vPro デバイスを自動的に設定する場合は、この手順を実行する必要はありません。38 ページの「リモート設定による vPro デバイスの設定」を参照してください。

新規 vPro システムを作成するには

1 Intel AMT SCS Console を起動します。

2 **[プラットフォーム コレクション]**、**[すべてのプラットフォーム]** の順に選択します。

3 [結果領域] を右クリックし、コンテキスト メニューから **[新規プラットフォーム]** を選択します。[プラットフォームの設定] ウィンドウが表示されます。

4 [プラットフォームの設定] ウィンドウで、次の各項目を指定します。

— **FQDN**: 管理対象 vPro デバイスの完全修飾ドメイン名を入力します。

— **UUID**: 管理対象 vPro デバイスの UUID を入力します。UUID は BIOS から取得できます。

— **Active Directory OU**: LDAP 名を識別名形式で入力します。例では、「**CN=Computers,DC=AMT,DC=HP,DC=COM**」と入力しています。

— **プロファイル**：ドロップダウン リストから 33 ページの「プロファイルの設定」で作成したプロファイルを選択します。例では、PSGProfile を選択しています。

5 **[適用]**、**[OK]** の順にクリックします。

これで、次のセクションで説明するように vPro デバイスを設定するための準備が整いました。

詳細については、『Intel AMT SCS Version 5.0 Console User's Guide』の「Preparing and Managing Platforms」セクションの「Adding a Platform Definition」の項を参照してください。

vPro デバイスの設定

Intel vPro デバイスは、デフォルトでは、未設定状態 (工場出荷時モード) で出荷されます。管理アプリケーションで vPro デバイスにアクセスできるようにするためには、そのデバイスに、安全な通信に必要なユーザー名、パスワード、ネットワーク パラメータ、TLS 証明書、PID-PPS キーなどの設定情報を入力する必要があります。

vPro デバイスを設定するには、各デバイスの Management Engine BIOS Extension (MEBx) を入力し、必須情報を手動で入力します。手動でデバイスをプロビジョニングする場合は、事前共有キー (PSK) モードを使用して、SCS と vPro デバイス間の通信を保護します。

また、Intel Remote Configuration プロセスを利用してデバイスを設定することもできます。その場合、デバイスは自動的にプロビジョニングされます。デバイスを自動的にプロビジョニングする場合は、公開キー インフラストラクチャ (PKI) を使用して、通信を保護します。

次のセクションで、この 2 つの方法について説明します。

MEBx による vPro デバイスの設定

MEBx を使用して vPro デバイスを設定するには

1 システムを再起動します。再起動時に **Ctrl-P** キーを押すと、[Management Engine BIOS Extension (MEBx)] ウィンドウが表示されます。

2 ME パスワードとして、「**admin**」を入力します。このパスワードを使用できるのは一度のみです。

3 **[Intel ® ME Password]** を選択して、パスワードを 33 ページの「セキュリティ キーを設定するには」の手順 4 で指定した値に設定します。

4 **[Intel ® ME Configuration]** を選択します。**Y** キーを押してシステム設定をリセットします。この操作により、[Intel ® ME Platform Configuration] ウィンドウが表示されます。**[Intel ® ME State Control]** を選択し、**[Enable]** を選択します。

5 **[Intel ® ME Firmware Local Update Qualifier]** を選択し、**[Always Open]** を選択します。

6 **[Intel ® ME Features Control]** を選択します。**[Features Control Selection]** を選択し、**[Intel ® ME]** を選択します。

7 **[Intel ® Quiet System Technology]** を選択し、**[Enabled]** を選択します。前のメニューに戻ります。

8 **[Intel ® ME Power Control]** を選択します。**[Intel ® ME State Upon Initial Power On]** を選択し、**[ON]** を選択します。

9 **[Intel ® ME ON in Host Sleep States]** を選択し、**[Always]** を選択します。

10 **[LAN Power Well]** を選択して、**[WOL EN Pin]** が選択されていることを確認します。

11 **[Intel ® ME Visual LED Indicator]** を選択して、**[ON]** が選択されていることを確認します。前のメニューに戻ります。再度、前のメニューに戻ります。**[Exit]** を選択します。**Y** キーを押して確定します。設定が保存され、システムが自動的に再起動されます。システムが再起動されない場合は、手動で再起動してください。

12 システムの再起動中に、電源ケーブルと LAN ケーブルを引き抜きます。10 秒待ちます。

13 システムを再起動します。システムの再起動時に **Ctrl-P** キーを押すと、再度、[MEBx] ウィンドウが表示されます。

14 手順 3 で指定した新規パスワードを入力します。

15 **[Intel ® ME Configuration]** を選択します。

16 **[Hostname]** を選択し、vPro デバイスのホスト名を入力します。

17 **[TCP/IP]** を選択します。ネットワーク インターフェイスを無効にするかどうか尋ねられたら、**N** キーを押します。DHCP を無効にするかどうか尋ねられたら、**N** キーを押します。DHCP は常に有効な状態にしておいてください。

18 **[Provisioning Server]** を選択します。Intel SCS を実行するときに使用するコンピュータの IP アドレスを入力します。ポートは 9971 に設定します。

19 **[Provisioning Model]** を選択して、**N** キーを押し、**[Intel ® AMT 2.0]** モードが選択されていることを確認します。

20 適切なキー (**Y** または **N**) を押して、**[Enterprise Mode]** が選択されていることを確認します。

21 **[Set PID and PPS]** を選択します。

22 PID と PPS に、33 ページの「セキュリティ キーを設定するには」の手順 7 で指定した値を設定します。

23 **[Return to Previous Menu]** を選択して、**[Exit]** を選択し、**Y** キーを押して確定します。

Provisioning Server コンソールで、設定および設定プロセスが実行されプロセスが正常に完了したことを確認できます。

お使いの vPro デバイスによっては、上記の手順がそのまま当てはまらないことがあります。その場合は、ベンダーのドキュメントを参照して、正しい手順を確認してください。

リモート設定による vPro デバイスの設定

リモート設定とは、各デバイスに手動で PID/PPS のペアをインストールしてセットアップを有効にする必要がない vPro メカニズムです。リモート設定を活用するには、次を実行する必要があります。

- 信用できる証明機関 (CA) からセキュリティ証明書を購入します。CA ベンダーは、ルート証明書のハッシュ値が vPro ファームウェアに組み込まれているいずれかのベンダーと一致する必要があります。SCS Server がインストールされているシステム上のシステム証明書ストアに証明書をインストールする必要があります。40 ページの「リモート設定用証明書の取得」以降のセクションを参照してください。
- ホスト vPro デバイス上にローカル エージェントをインストールします。はじめてネットワークに接続されたときに、vPro デバイスが正常にプロビジョニングされなかった場合は、ローカル エージェントによって遅延設定プロセスが開始されます。

  デバイスをネットワークに接続後、vPro デバイスをネットワーク インターフェイスが開いている時間枠内にプロビジョニングできなかったときに、遅延設定が実行されます。39 ページの「ネットワーク アクセスの制限」を参照してください。遅延設定については、この章の 43 ページの「ローカル エージェントを vPro デバイスに手動でインストールするには」および vPro デバイスのプロビジョニング章の 120 ページの「vPro デバイスの遅延リモート設定」で説明します。

  通常、デバイスをネットワークに接続すると、vPro デバイスの即時セットアップが実行されます (リモート設定要件 を正しく実行した場合)。これを ベア メタル設定といいます。デバイスによって、セットアップ モードに遷移したことを示す SCS Server への「Hello」メッセージの送信が開始されます。ネットワーク インターフェイスが開かれている時間枠内にデバイスを正常にプロビジョニングできる場合は、さらにプロビジョニング タスクを実行する必要はありません。41 ページの「vPro デバイスのベア メタル リモート設定」を参照してください。

これらのコンセプトと手順は、次のセクションで詳細に説明します。

リモート設定機能

次の vPro 機能により、リモート設定が可能になります。

- 組み込まれたハッシュ化ルート証明書

  vPro デバイスには、世界中の SSL 証明書プロバイダからのファームウェア イメージでの複数のルート証明書ハッシュが含まれます。「Hello」メッセージの一部として、vPro デバイスによってすべてのハッシュが SCS に送信されます。SCS が vPro デバイスに対して認証するときは、ハッシュ化ルート証明書のいずれかと互換性のある証明書で行う必要があります。vPro デバイスによって、組み込まれたルート証明書ハッシュのリストがチェックされ、SCS によって送信された TLS クライアント証明書がリスト内のいずれかの CA ルート証明書によって署名された有効な証明書であることが検証されます。

- 自己署名証明書

  vPro デバイスにより、TLS サーバー証明書として使用して SCS に対して設定目的のみに認証する自己署名証明書が作成されます。自己署名証明書を承認するように SCS を設定する必要があります。

- ワンタイム パスワード

  遅延設定を実行する場合は、セキュリティ ポリシーでワンタイム パスワード (OTP) を使用してセキュリティを強化する必要がある場合があります。ローカル ホスト上で実行中のローカル エージェントは SCS に OTP を要求し、vPro デバイス上のファームウェアに送信します。SCS は特定の vPro デバイスに関連付けられたデータベース エントリに OTP を保存し、デバイスへの接続の検証に使用します。OTP は遅延設定のみに使用され、ベア メタルには使用できません。41 ページの「リモート設定プロビジョニング プロセス」を参照してください。

- ネットワーク アクセスの制限

  ネットワーク インターフェイスは制限された時間間隔内で開き、「Hello」メッセージを送信し、セットアップおよび設定プロセスを完了します。Intel マシンの場合、この時間間隔は 24 時間です。HP デスクトップの場合は、255 時間です。時間間隔が経過すると、セットアップと設定時間が SCS からのネットワーク コマンドによって延長されなかった場合、インターフェイスは終了します。

リモート設定要件

リモート設定プロセスを開始する前に、次の要件を満たす必要があります。

- vPro デバイスが DHCP サーバーから IP アドレスを受信するように設定されていること。DHCP がオプション 15 をサポートし、ローカル ドメイン サフィックスを検査のために vPro デバイスに戻せること。
- vPro デバイスが少なくとも 1 つのアクティブなルート証明書ハッシュで事前にプログラミングされていること。
- 遅延設定プロセスでは、vPro ホスト マシンにローカル エージェントがインストールされ実行中であること。43 ページの「ローカル エージェントを vPro デバイスに手動でインストールするには」を参照してください。
- SCS Server が `Provisionserver` という名前で vPro デバイスにアクセスできる DNS サーバーに登録され、デバイスと同じドメイン内、または同じサフィックスのドメイン内にあること。
- SCS Server に CA まで追跡する組織単位 (OU) または組織 ID (OID) 付きの証明書があり、ルート証明書ハッシュが vPro デバイスに格納されていること。詳細については、40 ページの「リモート設定の証明書の取得と設定」を参照してください。

- SCS Server がリモート設定ができるように設定されていること。32 ページの「SCS サービスの設定」を参照してください。

OTP オプションは、ベア メタル設定では有効にできません。

リモート設定用証明書の取得

リモート設定プロセスで vPro デバイスを設定するには、次のいずれかの認証局 (CA) から信頼できる証明書を購入する必要があります。

- VeriSign Class 3 Primary CA-G1
- VeriSign Class 3 Primary CA-G3
- Go Daddy Class 2 CA
- Comodo AAA CA

これらは、ルート証明書ハッシュが Intel vPro ファームウェアに組み込まれているベンダーです。SSL 証明書を購入するベンダーの Web サイトに移動します。各サイトには、SSL 証明書の要求、登録、インストール、移動に必要な手順が説明されています。

リモート設定の証明書の取得と設定

リモート設定の証明書を取得および設定するには、『*Intel AMT SCS Version 5.0 Console User's Guide*』の付録「Remote Configuration」の「Acquiring and Configuring a Certificate that Supports Remote Configuration」セクションを参照してください。このドキュメントは、HPCA Core 配布メディアの `Media\oobm\win32\AMT Config Server` ディレクトリにあります。

独自の証明書の作成およびインストール

独自の証明書を作成およびインストールしてリモート設定をすることもできます。リモート設定用の独自の証明書を作成およびインストールするには、『*Intel AMT SCS Version 5.0 Console User's Guide*』の付録「Remote Configuration」の「Creating and Installing Your Own Certificate」セクションを参照してください。このドキュメントは、HPCA Core 配布メディアの `Media\oobm\win32\AMT Config Server` ディレクトリにあります。

リモート設定用 SCS 証明書の選択

このセクションの情報は、多目的証明書のテンプレートを作成し、ユーザーの個人証明書ストアにインポートする場合のみ必要です。多目的証明書のテンプレートを作成するには、『*Intel AMT SCS Version 5.0 Console User's Guide*』の付録「Remote Configuration」の「Creating a Multipurpose Certificate Template」セクションを参照してください。

リモート設定用に SCS 証明書を選択するには、『*Intel AMT SCS Version 5.0 Console User's Guide*』の付録「Remote Configuration」の「Selecting the Certificate Used by the SCS for Remote Configuration」セクションを参照してください。このドキュメントは、HPCA Core 配布メディアの `Media\oobm\win32\AMT Config Server` ディレクトリにあります。

vPro デバイスのベア メタル リモート設定

セットアップ モードへの移行

vPro デバイスは、AC 電源とネットワークに接続されるとすぐに「Hello」メッセージの送信を開始します。Intel では、ネットワークに接続されていてネットワーク アクセスの制限時間がプロビジョニング用にまだ残っているデバイスを表すために、「ベア メタル設定」という用語を使用します。

ただし「ベア メタル」という用語は、通常、オペレーティング システムがインストールされていないシステムを表します。具体的には、vPro デバイスの場合は、vPro ホスト マシンにオペレーティング システムがインストールされていないシステムを表します。

オペレーティング システムがインストールされていない場合、ローカル エージェントを実行してワンタイム パスワード (OTP) をインストールし、セキュリティを強化することはできません。この概念については、vPro デバイスのプロビジョニングの章の 120 ページの「vPro デバイスの遅延リモート設定」で説明します。

簡素化されたワンタッチ設定

ベア メタル セットアップでは OTP を使用できませんが、SCS Server の FQDN をベア メタル vPro システムに入力すると、セキュリティを強化できます。これは簡素化されたワンタッチ設定と呼ばれます。

リモート設定プロビジョニング プロセス

セットアップと設定の流れは、OTP の交換がないことを除き、41 ページの「リモート設定プロビジョニング プロセス」で説明した、ローカル エージェントを採用した遅延設定と同じです 。

OTP が必要であるとき、SCS ではベア メタル システムをセットアップできません。このため、ベア メタル設定を正常に行うには、SCS Server で OTP オプションを有効にしないでください。

vPro デバイスのベア メタル設定を実行するには

1. SCS Server を含むネットワークに vPro デバイスを接続します。vPro デバイスは、SCS がインストールされているドメインに接続する必要があります。
2. vPro デバイスの電源を入れます。

   vPro デバイスは「Hello」パケットを自動的に送信します。vPro デバイスが SCS Server からメッセージを受信した後でプロビジョニング プロセスが始まり、vPro デバイスを有効にするために必要となるすべての設定とデータを SCS Server が読み込みます。
3. vPro デバイスが設定された後で、オペレーティング システムをインストールします。IT が指定するオペレーティング システムをネットワークから vPro デバイスにインストールすると、vPro システムの完全な「ノー タッチ」設定が可能になります。

ベア メタル リモート設定の失敗

ベア メタルのプロビジョニング プロセスは、vPro デバイスをネットワークと AC 電源に接続するとすぐに始まりますが、ネットワーク アクセスの制限時間枠内にデバイスのプロビジョニングが完了しないことがあります。失敗には次のような理由があります。

- SCS Server で OTP が有効になっている
- ネットワーク トラフィックが多い
- vPro デバイスで証明書がルート ハッシュと一致しない

ベア メタル設定が失敗した場合、遅延設定を使用してデバイスをプロビジョニングできます。遅延設定で vPro デバイスをプロビジョニングする方法は 2 つあります。この 2 つの方法は次のとおりです。

- この章の次のセクションで説明するローカル エージェント
- vPro デバイスのプロビジョニングの章の 120 ページの「vPro デバイスの遅延リモート設定」で説明する HPCA コンソール

OOBM ローカル エージェントのインストール

ワークフローのこの時点で、HP CA アウトバンド管理ローカル エージェントをインストールすることをお勧めします。ベア メタル設定の制限時間枠内に vPro デバイスが正常にプロビジョニングされなかった場合、ローカル エージェントはプロビジョニング解除済みデバイスのインストール プロセスの一部として遅延設定を実行します。

遅延設定のセットアップ モードへの移行とプロビジョニング プロセス中に実行されることについては、vPro デバイスのプロビジョニングの章の 120 ページの「vPro デバイスの遅延リモート設定」を参照してください。

ワンタイム パスワードの設定

ネットワーク セキュリティ ポリシーの一部としてセキュリティを強化する必要がある場合は、SCS セットアップに戻ってワンタイム パスワード (OTP) を有効にすることもお勧めします。32 ページの「SCS サービスの設定」を参照してください。

ローカル エージェントのインストール方法

vPro デバイスにローカル エージェントをインストールする方法は 2 つあります。1 つは、各 vPro デバイスでローカル エージェントを手動でインストールする方法です。あるいは、Client Automation Standard または Enterprise ソフトウェアにより、複数の vPro デバイスにローカル エージェントを自動的にインストールする方法もあります。

両方の方法について次のセクションで説明します。

設定クライアント ロール

ローカル エージェントで vPro デバイスをプロビジョニングできるようにするには、選択したインストール方法に関係なく、次のことを実行する必要があります。

- 設定クライアントのロールがあるユーザーを SCS Console で作成して追加する必要があります。たとえば SCS Console で作成して追加したユーザーに **SCSUser** という名前を付けることができます。
- このユーザーは、**SCSUser@vlan1.hp.com** などのドメイン **VLAN1** で作成する必要があります。

設定クライアント ロールがあるユーザーの認証情報は、ローカル エージェントのインストール中に指定する必要があります。SCS 設定クライアントのユーザー認証情報は正しく指定する必要があります。正しく指定しないと、ローカル エージェントは遅延セットアップでデバイスのプロビジョニングを開始できなくなります。

ローカル エージェントのインストール時には、遅延設定を使用してデバイスをプロビジョニングしない場合でも、「ダミー」ユーザー名とパスワードを指定する必要があります。ユーザー名とパスワードを指定しないと、インストールはエラー コード 1920 でエラーになります。

場合によっては、ローカル エージェントのインストールまたはサービスの再起動の結果、イベント ログにエラー コード 1063 のエラー メッセージが出力されることがあります。このメッセージは無害であるため、無視してかまいません。

個々の vPro デバイスへの手動インストール

ローカル エージェントを vPro デバイスに手動でインストールするには

1. HPCA Core 配布メディアの `\Media\client\default\win32\oobm\LocalAgent` ディレクトリにある `oobmclocalagent.msi` ファイルを vPro デバイスにコピーします。コピーしたファイルをダブル クリックします。または、配布メディア上の上記と同じディレクトリにある `setup.cmd` ファイルを vPro デバイスにコピーします。setup ファイルをダブル クリックするか、コマンド ラインに「`setup.cmd`」と入力します。`setup.cmd` ファイルによって、`oobmclocalagent.msi` ファイルが呼び出されます。
2. **[Next]** をクリックして、ライセンス契約に同意します。
3. **[Next]** をクリックします。[Remote Configuration Parameters] ウィンドウが表示されます。このウィンドウ内で次を指定します。
   - **[SCS Configuration Client User Name]**: 設定クライアントのロールを持つユーザーのユーザー名を入力します。ユーザー名の形式は、`SCS ユーザー名 @ ドメイン名`です。
   - **[SCS Configuration Client Password]**: 設定クライアントのロールを持つユーザーのパスワードを入力します。
   - **[SCS Profile ID]**: vPro デバイスのプロファイルを入力します。この情報は、SCS Console の [プロファイル] 領域に表示されます。
   - **[SCS Remote Configuration URL]**: Intel Setup and Configuration Service (SCS) リモート設定サービスの仮想ディレクトリを含む URL パスを入力します。たとえば、**https://provisionserver.yourenterprise.com/amtscs_rcfg** のように入力します。ここで、**provisionserver.yourenterprise.com** は、IIS ホスト コンピュータの完全修飾ドメイン名 (FQDN)、**amtscs_rcfg** は、同ホスト コンピュータ上の SCS リモート設定サービス仮想ディレクトリです。
4. **[Next]** をクリックします。[User Information] ウィンドウが表示されます。このウィンドウでは、SCS プロファイル ID (前の手順で参照) に定義したユーザーの vPro ダイジェスト ユーザー認証情報を入力できます。このウィンドウ内で次を指定します。
   - **[ユーザー名]**: SCS プロファイルに定義したダイジェスト ユーザーの vPro ユーザー名を入力します。
   - **[パスワード]**: SCS プロファイルに定義したダイジェスト ユーザーの vPro パスワードを入力します。
   - vPro デバイスが TLS モードでプロビジョニングされた場合は、**[TLS Mode]** チェックボックスをオンにします。
5. **[Next]** をクリックして、インストール ウィザードの残りの手順を実行します。

ローカル エージェントは NT サービスであり、インストールが完了次第、開始されます。

Client Automation による複数の vPro デバイスへの自動インストール

前述のとおり、ローカル エージェントは、Client Automation ソフトウェアの Standard/Enterprise エディションを介して、複数のデバイス上に自動的にインストールできます。

ただし、Client Automation ソフトウェアの Starter エディションでは、この方法でローカル エージェントをインストールすることはできません。

自動インストール手順には 2 つの部分があります。この 2 つの方法は次のとおりです。

- Client Automation Publisher を使用して、HP CA アウトバンド管理のローカル エージェント ソフトウェアを Client Automation データベースにパブリッシュする必要があります。
- Client Automation 管理コンソールを使用して、ローカル エージェントを vPro ターゲット デバイスに配布する必要があります。

ローカル エージェントを Client Automation データベースにパブリッシュするには

1 **[スタート] > [プログラム] > [HP Client Automation Administrator] > [Client Automation Publisher]** を選択し、Client Automation Publisher を呼び出します。[ログオン] ウィンドウが表示されます。

2 Client Automation のユーザー名とパスワードを使用して、Publisher にログインします。デフォルトでは、ユーザー名は `admin`、パスワードは `secret` です。[Publisher] ダイアログ ウィンドウが表示されます。

3 プルダウン リストから、**[Windows インストーラ]** を選択します。

4 **[OK]** をクリックします。Publisher の選択ウィザードが表示されます。

5 パブリッシュする Windows インストーラ ファイルとして、左側のナビゲーション メニューでローカル エージェントのインストーラ ファイル (`oobmclocalagent.msi`) を選択します。

6 **[次へ]** をクリックします。Publisher の編集ウィザードが表示されます。

7 **[プロパティ]** リンクをクリックします。インストーラ ファイルのプロパティが右に表示されます。**AMT** で始まるプロパティがすべて正しく設定されていることを確認します。これらのプロパティには、次が含まれます。

   — **AMTUSERNAME**: 管理者の vPro ユーザー名を入力します (ダイジェスト ユーザー名)。

   — **AMTPASSWORD**: 管理者の vPro パスワードを入力します (ユーザーのダイジェスト パスワード)。

   — **AMTTLSMODE**: vPro デバイスが TLS モードでプロビジョニングされている場合は「**1**」を、それ以外は「**0**」を入力します。

   — **AMTPROVSERVERADD**: Intel SCS (Setup and Configuration Service) リモート設定サービスの仮想ディレクトリを含む URL パスを入力します。

   — **AMTPROFILEID**: vPro デバイスのプロファイル ID を入力します。この情報は、SCS Console の [プロファイル] 領域に表示されます。

8 また、プロパティ ページで、次のプロパティが正しく設定されていることも確認します。

   — **SCSUSERNAME**: ユーザーのユーザー名と設定クライアントのロールを入力します。

   — **SCSUSERPASS:** ユーザーのパスワードと設定クライアントのロールを入力します。

9 **[次へ]** をクリックします。Publisher の設定ウィザードが表示されます。

10 このウィンドウで、次を指定します (一覧表示されないフィールドはオプションです)。

   — **[サービス ID]**: サービスを識別するテキスト文字列 (**HP_CA_OOB_LOCAL_AGENT** など) を入力します。

   — **[説明]**: ソフトウェアの説明 (**HP CA OOB Local Agent** など) を入力します。

   — **[ソフトウェア カタログ]**: プルダウン リストから **[ユーザー アプリケーション]** を選択します。

— **[パッケージを適用する対象システム]**: オペレーティング システムを選択しないと、オペレーティング システムにかかわらずすべての vPro デバイスにソフトウェアが配布されます。

11 **[次へ]** をクリックします。Publisher のパブリッシュ ウィザードが表示されます。要約および進捗情報が表示されます。

12 **[パブリッシュ]** をクリックします。ローカル エージェントのアプリケーションが Client Automation データベースにパブリッシュされます。

13 **[完了]** をクリックします。

14 ポップアップ ウィンドウの **[はい]** をクリックし、Publisher を終了します。

ローカル エージェントを複数の vPro デバイスに自動的に配布するには

次の手順の詳細については、『HP Client Automation Core および Satellite ユーザー ガイド』の Standard または Enterprise 版を参照してください。

1 Client Automation への vPro デバイスのインポート

2 ターゲット vPro デバイスへの Client Automation Management Agent の配布

3 スタティック グループの作成およびグループへのターゲット vPro デバイスの追加

4 vPro デバイス グループへの HP CA アウトバンド管理ローカル エージェントの配布

vPro デバイスのローカル エージェントのバージョン チェック

ローカル エージェントのバージョンをチェックするには

1 vPro デバイスのインストール ディレクトリ、`C:\Program Files\Hewlett-Packard\HPCA\OOBM Agent` に移動します。

2 `OOBMCLocalAgent.exe` ファイルを右クリックし、コンテキスト メニューから **[プロパティ]** を選択します。

3 **[バージョン]** タブを選択します。このウィンドウにバージョン情報が表示されます。

64 ビット プラットフォーム上のローカル エージェント

64 ビット プラットフォーム上にローカル エージェントをインストールする場合は、vPro デバイスに 32 ビットと 64 ビットの両方のプラットフォーム用の Intel 固有のドライバがインストールされていることを確認する必要があります。これらのドライバは **www.HP.com/support** にあります。デスクトップの場合、ドライバは [Software – System Management] セクションにあります。ドライバ名は Intel Local Management Service (LMS) および Serial-over-LAN (SOL) Support です。ノートブックの場合、通常、ドライバは Windows インストール ディレクトリの `SWSetup\AppInst` ディレクトリにあります。ない場合は、これらのドライバは上記の HP サポート サイトからダウンロードすることもできます。ドライバをインストールしたら、システムを再起動する必要があります。

vPro デバイスの表示

vPro デバイスをプロビジョニングすると、vPro SCS Console に表示できます。

デバイスがコンソールに表示されるまでしばらく待機する必要があります。

vPro デバイスを表示するには

1 vPro SCS Console を開きます。

2 [Intel AMT Systems] ブランチを展開し、ターゲット vPro デバイスを選択します。ターゲット vPro デバイスがそのプロビジョニングのステータスとともに表示されます。

3 [Logs] ブランチを展開し、[Log] ノードを選択します。ログ情報が表示されます。

認証モードの変更

このセクションは、TLS 認証をセットアップした場合のみ関連します。TLS をセットアップしていない場合は、アウトバンド管理設定の章に進みます。

vPro デバイスをプロビジョニングした後、vPro SCS Console を使用してデバイスの認証モードを変更できます。

TLS サーバー認証モードで vPro デバイスを設定するには

1 vPro SCS Console を開きます。

2 [Configuration Service Settings] ブランチを展開し、**[Profiles]** を選択します。さまざまな vPro デバイス用に作成されているプロファイルの一覧が表示されます。

3 vPro デバイスに適切なプロファイルを選択し、**[Edit]** をクリックします。

4 **[Network]** タブを選択し、次のオプションを選択します。

— [Use TLS]

— [Local Interface] と [Network Interface] の両方で [TLS Server Authentication]

5 **[Apply]**、**[OK]** の順にクリックします。メインの SCS Console に戻ります。

6 [Intel(R) AMT Systems] ブランチを展開し、[Global Operations] を選択します。[Global Operations] ウィンドウが表示されます。

7 このウィンドウの [Provisioning] ペインで **[Re-Provision]** をクリックします。この再プロビジョニング要求に要求 ID が割り当てられます。この ID をメモしてください。アクション ステータス ログでログ情報を検索するときに使用できます。**[OK]** をクリックします。

8 [Logs] ブランチを展開し、**[Actions Status]** を選択します。このログには、すべての要求のステータスが表示されます。前の手順で割り当てられた要求 ID を使用し、再プロビジョニング要求が正常に実行されたかどうかを確認できます。

TCP モード (非 TLS) で vPro デバイスを設定するには

1 vPro SCS Console を開きます。

2 [Configuration Service Settings] ブランチを展開し、**[Profiles]** を選択します。さまざまな vPro デバイス用に作成されているプロファイルの一覧が表示されます。

3 vPro デバイスに適切なプロファイルを選択し、**[Edit]** をクリックします。

4 **[Network]** タブを選択し、[Use TLS] オプションをオフにします。

5 **[Apply]**、**[OK]** の順にクリックします。メインの SCS Console に戻ります。

6 [Intel AMT Systems] ブランチを展開し、**[Global Operations]** を選択します。[Global Operations] ウィンドウが表示されます。

7 このウィンドウの [Provisioning] ペインで **[Re-Provision]** をクリックします。この再プロビジョニング要求に要求 ID が割り当てられます。この ID をメモしてください。アクション ステータス ログでログ情報を検索するときに使用できます。**[OK]** をクリックします。

8 [Logs] ブランチを展開し、**[Actions Status]** を選択します。このログには、すべての要求のステータスが表示されます。前の手順で割り当てられた要求 ID を使用し、再プロビジョニング要求が正常に実行されたかどうかを確認できます。

3 アウトバンド管理設定

この章では、HPCA Installer でインストール後、アウトバンド管理 (OOBM) を設定する方法を説明します。システム要件およびインストール情報については、『*HP Client Automation Core and Satellite Getting Started and Concepts Guide*』および『*HP Client Automation Release Notes*』を参照してください。

設定パラメータについての情報

SCS パスの再設定

必要に応じて、HPCA コンソールによって現在設定されている SCS パスを変更できます。50 ページの「設定パラメータ」を参照してください。

Client Automation Web サービスの再設定

必要に応じて、HPCA コンソールのゲートウェイ URL を変更できます。URL の例を挙げると、`http://CAhost:3466/ca` で、`CAhost` は Client Automation サーバーの完全修飾子名で、*ca* は Client Automation サーバー上の Client Automation Web サービスの仮想ディレクトリです。50 ページの「設定パラメータ」を参照してください。

IDE-R ドライブの設定

OOBM ソフトウェアは、IDE-R (Integrated Drive Electronics Redirect) を使用する際の CD とフロッピーのデフォルト設定でサーバー上にインストールされます。これらの設定は設定可能です。50 ページの「設定パラメータ」を参照してください。デフォルト設定がサーバー上のドライブ仕様と一致しない場合は、サーバーと一致するようにデフォルト ドライブ設定を変更する必要があります。CD とフロッピー ドライブのパスは、実際のドライブまたはイメージを参照する必要があります。

> フロッピー ドライブの起動オプションを使用している場合でも、CD/DVD を正しく設定する (つまり、実際の CD/DVD ドライブを参照する) 必要があります。CD/DVD ドライブの起動オプションを使用する場合も、フロッピー設定に対して同じことが言えます。HPCA コンソール サーバーに接続されたフロッピー ドライブがない場合、IDE-R 操作に対してフロッピー ドライブではなくローカルの起動可能 ISO イメージを参照できます。

CD またはフロッピー ドライブの設定を、物理 CD またはフロッピーではなく、それぞれ ISO または IMG ファイルを使用するように変更する場合、ISO または IMG ファイルへのドライブ パスが Tomcat を実行中のサーバーに可視的である必要があります。したがって、必要な ISO と IMG ファイルをすべて、Tomcat を実行中のサーバーのローカル ドライブにコピーします。

また、ISO または IMG ファイルが共有ネットワーク リソースの場合は、汎用命名規則 (UNC) 構文を使用してネットワーク ファイルにアクセスする必要があります。UNC 構文は、次のとおりです。

\\hostname\sharefolder\file

UNC 構文を使用する際は、IP アドレスではなくマシンの実際のホスト名を使用する必要があります。

SOL ポートの設定

OOBM ソフトウェアは、Serial over LAN (SOL) 開始ポートと、vPro デバイス上で複数の同時 SOL セッションを一度に表示できる最大数の SOL ポートのデフォルト設定で HPCA server 上にインストールされます。これらの値は変更できます。50 ページの「設定パラメータ」を参照してください。

vPro デバイス上では、SOL セッションによってほとんどの Windows オペレーティング システムにバンドルされている Windows HyperTerminal が起動されます。HPCA コンソールへのアクセスに使用する Web ブラウザ マシン上に HyperTerminal がインストールされているかどうかをチェックします。HyperTerminal がインストールされていない場合は、Microsoft のドキュメントを参照してインストール手順を確認してください。

HyperTerminal は、Windows Vista オペレーティング システムにはバンドルされていません。この場合、SOL セッションでは Telnet が起動されます。

SNMP ポートの設定

これは、vPro デバイスからの警告メッセージの取得に使用する SNMP ポートです。このポートは設定可能です。50 ページの「設定パラメータ」を参照してください。

IDE-R および SOL タイムアウト値の設定

これは、無線通信が遅延する傾向にあり、IDE-R セッションと SOL セッションのタイムアウト値を超えるため、vPro デバイス上で無線 NIC で実行するリモート操作は失敗することがあります。IDE-R と SOL のタイムアウト値とハートビート間隔値は設定可能です。50 ページの「設定パラメータ」を参照してください。

Web サービスのタイムアウト値の設定

OOBM Service では、Web サービスをデバイスに接続することによって vPro デバイスと通信します。タイムアウト値はこの通信に対して指定されます。現在のネットワーク条件に適していない場合は、この値を再設定できます。50 ページの「設定パラメータ」を参照してください。

DASH デバイスのキャッシュ サイズの設定

特定のユーザー セッションのメモリ内にキャッシュする DASH デバイス数を設定できます。50 ページの「設定パラメータ」を参照してください。この値を変更すると、パフォーマンスに影響します。この値はメモリ リソースがどれだけ試用できるかによって異なります。

セキュリティ パラメータの設定

この手順は TLS を設定している場合にのみ必要です。

TLS AMT 認証が有効の場合、Java キー ストアにアクセスするための適切な権限を得られるように Tomcat Server はドメイン ユーザー アカウントで実行する必要があります。

TLS 認証に対して設定する必要がある多数の設定パラメータがあります。これらのパラメータによって OOBM は信頼できるルートとクライアント証明書を検索でき、関連付けられたパスワードおよび証明機関サーバーの FQDN がわかります。

次を設定する必要があります。

- ルート証明書への PEM 形式の完全パス名 (root_certificate)
- クライアント証明書への PEM 形式の完全パス名 (client_certificate_pem)
- クライアント証明書への PFX 形式の完全パス名 (client_certificate_pfx)
- クライアント証明書 CN (ca_server_commonname)

これらのパラメータの設定方法の詳細については、50 ページの「設定パラメータ」を参照してください。

PEM 形式の証明書の詳細については、61 ページの「PEM 形式への証明書の変換」を参照してください。

さらに、次のコマンド ラインに示す PEM および PFX クライアント証明書のパスワードを指定する必要があります。

PEM クライアント証明書のパスワードを指定するには

1 「amtpem_chgpwd」と入力します。

2 パスワードの入力を促されたら、パスワードを入力します。

PFX クライアント証明書のパスワードを指定するには

1 「amtpfx_chgpwd」と入力します。

2 パスワードの入力を促されたら、パスワードを入力します。

エージェント ウォッチドッグの設定

エージェント ウォッチドッグを作成する場合、エージェント ウォッチドッグの設定は、ローカル エージェントのハートビート間隔 (ウォッチドッグへ送信されるハートビートの間隔) とエージェントがウォッチドッグへハートビートを送信開始する前の開始時間の 2 つです。デフォルト値を変更してネットワーク要件に反映させることができます。50 ページの「設定パラメータ」。

デバッグに使用する設定

設定するとデバッグのパフォーマンス関連の問題に役立つパラメータが 2 つあります。cache_update_thread_size パラメータと blocking_timer_time パラメータです。

cache_update_thread_size パラメータは、キャッシュ レイヤーの更新に使用するスレッド数を変更できます。通常の状態ではこの値は変更する必要はありません。ただし、この値は blocking_timer_time パラメータに関連して変更し、パフォーマンスの問題を解決できます。

blocking_timer_time 設定により、vPro Web サービスに接続するときに HPCA コンソール サーバー上にソケットの問題がある場合、タイムアウト値を変更できます。ソケット関連の問題がある場合は、タイムアウト値を上げることをお勧めします。

50 ページの「設定パラメータ」を参照してください。

設定パラメータ

<*HPCA_Install_DIR*>\oobm\conf\ ディレクトリにある 2 つのプロパティ ファイルを変更することで、設定パラメータを設定できます。

このディレクトリにあるプロパティ ファイルの設定パラメータを変更する場合は、Tomcat サービスを再起動する必要があります。

次のパラメータが config.properties ファイルにあります。または新たに追加できます。既存の **key=value** ペアに新規値を入力するか、新規 **key=value** ペアを追加することにより、一覧表示されたパラメータの値を再設定してこのファイルを編集できます。

config.properties でパスと完全修飾ファイル名を指定する場合は、「\\」または「/」をディレクトリ間の区切り文字として使用する必要があります。そうしないと、名前が正しく読み込まれません。たとえば、C:\\certs\\cc.pem または C:/certs/cc.pem は正しいですが、C:\certs\cc.pem は正しくありません。

次の表は、このファイルに含まれるパラメータと、そのデフォルト設定と説明を一覧にしたものです。

表 1　　config.properties ファイルの設定パラメータ

パラメータ (キー)	デフォルト値	説明
scsserver_url	デフォルト値なし	SCS Server の URL。現在設定されている SCS パスは変更できます。
radia_gateway	デフォルト値なし	HPCA コンソールの URL
default_cddrive_path	D:	デフォルト IDE-R CD ドライブ設定。CD パスは実際のドライブまたはイメージを参照する必要があります。
default_fddrive_path	A:	デフォルト IDE-R フロッピー ドライブ設定。フロッピー ドライブ パスは実際のドライブまたはイメージを参照する必要があります。

表 1　　**config.properties** ファイルの設定パラメータ **(cont'd)**

パラメータ (キー)	デフォルト値	説明
sol_port_start	9999	開始 SOL ポート
sol_number_of_port	10	SOL ポートの最大数
snmp_trapd_port	162	SNMP ポート
vPro_webservice_timeout	15000 ミリ秒	Web サービスのタイムアウト値
devices_cachequeuesize	50	DASH デバイスのキャッシュ サイズ。この値を変更すると、パフォーマンスに影響します。
root_certificate	デフォルト値なし	ルート証明書への PEM 形式の完全パス名
client_certificate_pem format	デフォルト値なし	クライアント証明書への PEM 形式の完全パス名
client_certificate_pfx	デフォルト値なし	クライアント証明書への PFX 形式の完全パス名
ca_server_commonname	デフォルト値なし	クライアント証明書 CN
apwatchdog_heartbeat_interval	60 秒	ウォッチドッグのローカル エージェントのハートビート間隔
apwatchdog_startup_time	300 秒	ウォッチドッグのローカル エージェントの起動時間間隔
device_synchronization_timeperiod	0	SCS リポジトリからデバイス リストをリロードする時間。この同期時間間隔のデフォルト値はゼロ (自動同期を行わない) です。自動的に同期させる場合は、ゼロ以外の値に設定します。単位は分です。
group_synchronization_timeperiod	0	CA リポジトリからグループ デバイス リストをリロードする時間。この同期時間間隔のデフォルト値はゼロ (自動同期を行わない) です。自動的に同期させる場合は、ゼロ以外の値に設定します。単位は分です。
cache_update_thread_size	25	キャッシュ スレッド サイズ (デバッグ専用)

表 1　　config.properties ファイルの設定パラメータ (cont'd)

パラメータ (キー)	デフォルト値	説明
blocking_timer_time	100	タイムアウト値のブロック (デバッグ専用)
devices_cachequeuesize	100	電源管理、システム防御機能の配布など、操作の実行に使用する vPro 関連 Java オブジェクトの格納に使用するキャッシュのサイズ (デバッグ専用)。
scsserver_url	デフォルト値なし	SCS Server の URL。現在設定されている SCS パスは変更できます。
radia_gateway	デフォルト値なし	HPCA コンソールの URL

追加設定パラメータは、<*HPCA_Install_DIR*>\oobm\conf\ ディレクトリにもある configuration.properties ファイルにあります。これらのパラメータのすべてにデフォルト値が割り当てられていますが、セットアップに応じて再設定が必要な場合があります。

このファイル内のデータは、アウトバンド管理を正しく機能させるために重要なものです。表 2 の **[説明]** カラムで、「非エンド ユーザー用」として一覧表示されているアイテムは変更または削除しないでください。

表 2 は、このファイルに含まれるパラメータとそのデフォルト設定と説明を一覧表示したものです。

表 2　　configuration.properties ファイルの設定パラメータ

パラメータ	デフォルト値	説明
Active_Directory_FQDN_or_Hostname_property	名前	AD から返されたデバイス ID 情報。ホスト名 (**名前**) または FQDN (**dNSHostName**) を選択できます。サブドメイン DNS により FQDN が失敗する可能性があるため、デフォルト値 (名前) を使用する方が安全です。
BEV_BOOT_SOURCE_VALUES	BEV	Boot Entry Vector の起動元名
CACHE_SIZE	50	OOBM Web サービス システムのキャッシュ サイズ。たとえば、`CACHE_SIZE=50` では、常時システムによって最大 50 のデバイスがキャッシュされることが指定されます。キャッシュがフルであるのに新規デバイスを追加する必要がある場合は、アクセスや使用が最も少ないデバイスを削除して新規デバイスに対応できるようにする必要があります。
CACHE_WAIT_DURATION	2000	ミリ秒単位のキャッシュ待機時間。たとえば、`CACHE_WAIT_DURATION=2000` では、キャッシュ マネージャの応答を 2000 ミリ秒を超えて待機しないことが指定されます。キャッシュ マネージャが 2000 ミリ秒を超えて使用中の場合、システムは現在の操作にキャッシュを使用しません。
CDDVD_BOOT_SOURCE_VALUES	CD/DVD,CD-ROM	CD の起動元名
DASH_PORTS	623	DASH ポートのコンマ区切りのリスト
DASH_TEXTREDIRECTION_TIME_DELAY	2	テキスト リダイレクション接続と電源操作呼び出し間の時間遅延 (秒単位)。
DISCOVERY_DELAY	100	探索遅延時間。この値を増やしてソケット接続時の消耗問題を克服できます。

表 2　　configuration.properties ファイルの設定パラメータ (cont'd)

パラメータ	デフォルト値	説明
DISCOVERY_REQUEST	DASH 検知要求の実際の内容が含まれます。	DASH　デバイスの探索に対する DASH 要求の内容。
DISCOVERY_SEQUENCE	dash、vpro	OOBM デバイスが探索される順序。たとえば、`DISCOVERY_SEQUENCE ="dash,vpro"` では、最初にデバイスが DASH デバイスかどうかがチェックされ、そうでない場合は、vPro デバイスかどうかがチェックされます。
ENABLE_BLIND_DISCOVERY	true	OOBM デバイスのブラインド探索。有効化されていると、システムは現在探索されていない OOBM デバイスに対してまず自動探索してから、次に要求された操作を実行するという操作要求を使用します。無効化されている場合は、OOBM デバイスは OOBM システムで検索済みです。または、エラーが表示されます。
FLOPPY_BOOT_SOURCE_VALUES	フロッピー、フロッピー ディスク ドライブ	フロッピーの起動元名
HDD_BOOT_SOURCE_VALUES	ハード ドライブ、ハードディスク	ハード ドライブの起動元名
HTTP_CONNECT_TIMEOUT	3000	HTTP 接続タイムアウト (HTTP 接続が応答を待機できる最大ミリ秒)
HTTP_READ_TIMEOUT	200	HTTP 読込時間 (HTTP 接続が読込応答を待機できる最大ミリ秒)

表 2　　configuration.properties ファイルの設定パラメータ (cont'd)

パラメータ	デフォルト値	説明
IDER_CLIENT_RX_TIMEOUT	10000	ミリ秒単位のクライアントの受信タイムアウト値。クライアントが OOBM Server からメッセージを受信する前にタイムアウト値が経過すると、クライアントは IDE-R セッションをシャットダウンします。IDE-R セッションが開かれている間は、OOBM Server はメッセージを継続して送信してクライアントの受信タイムアウト値が経過しないようにします (OOBM Server のハートビート間隔はクライアントの受信タイムアウト設定に基づきます)。 最小値 : 10000 最大値 : 65535 デフォルト値 : 10000
IDER_CLIENT_COMMAND_TIMEOUT	0	ミリ秒単位のクライアントのコマンド送信タイムアウト値。これは、クライアントが IDE コマンドを送信するときに待機する時間です。クライアントが指定時間内にコマンドに対する OOBM Server からの応答を受信しない場合、クライアントは IDE-R セッションを終了します。値が 0 の場合はコマンド送信タイムアウトが使用されないことを示します。 最小値 : 0 最大値 : 65535 デフォルト値 : 0

表 2　　configuration.properties ファイルの設定パラメータ (cont'd)

パラメータ	デフォルト値	説明
IDER_CLIENT_HB_INTERVAL	5000	ミリ秒単位のクライアントのハートビート間隔。これはクライアントがハートビート　メッセージを OOBM Server に送信するまでの待機時間です。値が 0 の場合はハートビート メッセージが送信されないことを示します。この場合、OOBM Server はクライアントが有効であることを示すアクティビティがないと、定期的に　IDE-R Keep-Alive Ping メッセージをクライアントに送信します。 最小値 : 0 最大値 : 65535 デフォルト値 : 5000
NETWORK_BOOT_SOURCE_VALUES	ネットワーク、PXE	PXE の起動元名
NUMBER_OF_DISCOVER_WORKER_THREADS	5	探索に使用できる最大スレッド数
PCMCIA_BOOT_SOURCE_VALUES	PCMCIA	PCMCIA の起動元名 (詳しくは、http://en.wikipedia.org/wiki/PC_Card を参照)
REVERTBACK_PREVIOUS_BOOT_ORDER	0	起動順リセット フラグ。特定の起動元でデバイスを起動する場合、無効 (**0**) または有効 (**1**) を選択して起動設定の前の起動順に戻すことができます。パフォーマンスに影響があるため、デフォルトでは前の状態に戻すことを無効にする設定です。
RevertBack_Previous_Boot_Order_Wait_Timer	10000	再起動操作を開始後、起動順を前の順序に戻すまでの待機時間 (ミリ秒単位)。デフォルト値が機能しない場合は、マシンのパフォーマンスに応じて値を増やします。

表 2　　configuration.properties ファイルの設定パラメータ (cont'd)

パラメータ	デフォルト値	説明
SOL_CLIENT_TX_BUFFERING_TIMEOUT	100	ミリ秒単位のクライアントの送信バッファリングのタイムアウト値。バッファ済み送信バイトを送信する前に送信バッファがフルになるまでクライアントが待機する時間。値が 0 の場合は、クライアントでバッファがフルになった場合のみデータを送信することを意味します。 最小値 : 0 最大値 : 65535 デフォルト値 : 100
SOL_CLIENT_TX_OVERFLOW_TIMEOUT	0	ミリ秒単位のクライアントの送信オーバーフローのタイムアウト値。送信バッファがフルになったときに送信バイトのドロップが開始されるまでのクライアントの待機時間。値が 0 の場合はタイムアウトがないことを意味します。 最小値 : 0 最大値 : 65535 デフォルト値 : 0
SOL_CLIENT_HB_INTERVAL	5000	ミリ秒単位のクライアントのハートビート間隔。OOBM Server へクライアントがアクティブであることを示すハートビート メッセージを送信する間のクライアントの待機時間。値が 0 の場合はハートビートが送信されないことを意味します。この場合、OOBM Server ではクライアントがアクティブがどうかを決定するクライアントからの受信アクティビティは監視されません。 最小値 : 0 最大値 : 65535 デフォルト値 : 5000

表 2　　configuration.properties ファイルの設定パラメータ (cont'd)

パラメータ	デフォルト値	説明
SOL_CLIENT_RX_TIMEOUT	10000	ミリ秒単位のクライアントの受信タイムアウト値。OOBM Server からメッセージを受信する前にこの時間が経過すると、クライアントは SOL セッションをシャットダウンします。SOL セッションが開かれていると、OOBM Server は定期的にハートビート メッセージを送信してクライアントの受信タイムアウトが切れないようにします (OOBM Server のハートビート メッセージの間隔はクライアントの受信タイムアウトに基づきます)。 最小値 : 10000 最大値 : 65535 デフォルト値 : 10000
SOL_CLIENT_FIFO_RX_FLUSH_TIMEOUT	100	ミリ秒単位のクライアントの FIFO 受信フラッシュ タイムアウト値。クライアントの受信 FIFO バッファがフルになったときに受信データがフラッシュされるまでのクライアントの待機時間。値が 0 の場合は、受信データがオペレーティング システムによって読み取られていないときはクライアントはフラッシュしないことを意味します。 最小値 : 0 最大値 : 65535 デフォルト値 : 100 (デフォルトでは、OOBM Server への間隔は 0 です。100 未満の値の使用は推奨しません。値が 0 になると、クライアントは受信データをフラッシュしなくなります。その結果、バッファがオーバーフローすると、クライアントはセッションをキャンセルします。)
SOL_THREADS_SLEEP_TIME	500	SOL スレッドのスリープ時間

表 2　　configuration.properties ファイルの設定パラメータ (cont'd)

パラメータ	デフォルト値	説明
USB_BOOT_SOURCE_VALUES	USB	USB の起動元名
WSMAN_MAX_ENUMERATION_RECORDS	5	単一 WSMAN Enumeration または Pull 呼び出しで取得できる最大要素数
WSMAN_TIMEOUT	30000	WSMAN 呼び出しのタイムアウト (WSMAN 呼び出しが応答を待機できる最大ミリ秒)

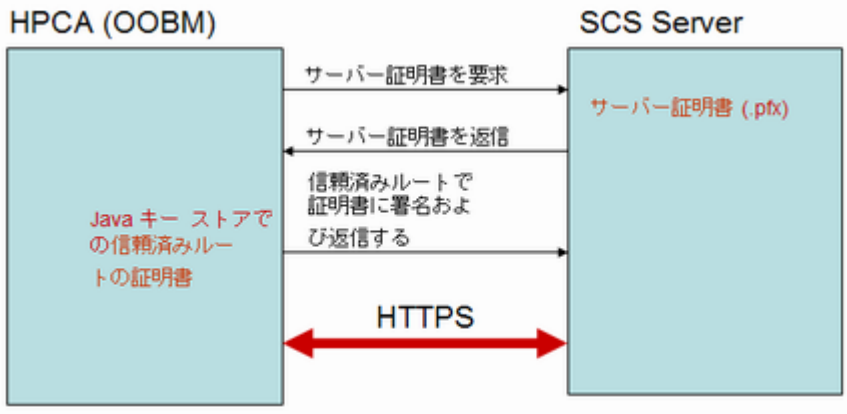
*BOOT_SOURCE_VALUES パラメータに指定する値は HPCA コンソール GUI で使用されるもので、これらの起動デバイスで使いやすい名前にします。これらのパラメータに値を指定しないと、これらの起動デバイスの名前としてわかりにくいテキスト文字列が表示されます。指定する文字列値は、DASH デバイスの起動元出力に基づいている必要があります。たとえば、起動元出力が BRCM:CD/DVD:3 の場合は、起動元を CD/DVD (CD ではない) と指定して GUI に CD/DVD を表示する必要があります。

OOBM Service と SCS 間の安全なアクセスの設定

SCS および vPro のセットアップ章の 31 ページの「IIS Server 証明書の設定」では、Microsoft CA を使用してサーバー証明書を作成しました。このサーバー証明書を IIS Manager にインポートして、SCS Server と SCS Console 間の安全な SCS 通信を確保しました。SCS および vPro のセットアップの章の 32 ページの「SCS 認証」を参照してください。

同じサーバー証明書で HPCA コンソール上で実行する SCS Server と OOBM Service 間の通信の安全も確保できます。これらの 2 つのコンポーネント間の通信を安全なものにするには、SCS Server 上の Microsoft CA の信頼できるルート証明書をエクスポートし、HPCA コンソール マシン上の Java キー ストアにインポートし、HPCA コンソールがサーバー証明書に署名して SCS Server を認証できるようにする必要があります。

図 6　　OOBM と SCS 間の安全なアクセス



ルート証明書をエクスポートするには

SCS および vPro のセットアップ章の 29 ページの「ルート証明書のエクスポート」で説明しているように TLS 相互認証セットアップの一部としてルート証明書をすでにエクスポートしている場合は、このタスクを再度実行する必要はありません。

SCS および vPro のセットアップ章の 30 ページの「ルート証明書をエクスポートするには」の手順に従います。

ルート証明書を Java キー ストアにインポートするには

1 HPCA コンソールで、既存の信頼できる証明書ファイルをバックアップします。これは、`cacerts` ファイルで、通常は `C:\Program Files\Hewlett Packard\HPCA\jre\lib\security` にあります。

2 コマンド プロンプトが表示されたら、次のコマンドを入力します。

```
keytool -import -noprompt -alias customcacert -keystore
..\lib\security\cacerts -storepass <store-password> -file <ca_file.cer>
```

— このコマンド ラインは、コマンドを JRE bin ディレクトリから実行中であることを想定しています。デフォルトでは、このディレクトリは `C:\Program Files\Hewlett Packard\HPCA\jre\bin` です。

— `<store-password>` は証明書ストアのパスワードです。デフォルトでは、このパスワードは **changeit** です。

— `<ca_file.cer>` は、SCS および vPro のセットアップ章の 29 ページの「ルート証明書のエクスポート」でエクスポートし、HPCA コンソール マシンにコピーした (SCS Server マシンと異なる場合) ルート証明書の完全パス名です。

このコマンドにより、ルート証明書が `cacerts` ストアにインポートされます。

3 確認するために、新規 `cacerts` ファイルとバックアップ バージョンのサイズを比較します。新規ファイルが 1 または 2 KB 大きくなります。

4 Tomcat Service を再起動します。

アプリケーションがデフォルト以外の場所にインストールされた場合は、`cacerts` ファイルと JRE bin ディレクトリの場所は異なります。HPCA コンソールのデフォルト インストール ディレクトリは、`C:\Program Files\Hewlett Packard\HPCA` です。

OOBM Service と SCS 間の安全なアクセスの無効化

OOBM をインストールして設定すると、Out of Band Management Service と SCS Server 間の安全なハイパーテキスト転送プロトコル (HTTPS) が有効化されます。HTTPS は、次の理由で有効化されます。

- OOBM デバイス タイプ設定の一部として HTTPS を使用する SCS パスを設定した、または `config.properties` ファイルで SCS パスを指定した。
- 信頼できるルート証明書をエクスポートし、HPCA コンソール サーバー上の Java キー ストアにインポートした。59 ページの「OOBM Service と SCS 間の安全なアクセスの設定」を参照してください。

安全な転送プロトコルの代わりに HTTP を使用する場合は、IIS Manager で HTTPS を無効化できます。

この方法は推奨しません。HTTPS を無効化すると、ユーザー資格情報は暗号化されなくなり、クリア テキストで送信されます。

HTTPS を無効化するには

1 SCS マシン上で IIS Manager を開きます。

2 ウィンドウ左側のナビゲーション パネルで、**[Web サイト] > [デフォルト Web サイト] > [AMTSCS]** に移動します。AMTSCS は SCS URL の仮想ディレクトリです。

3 **[AMTSCS]** を右クリックし、コンテキスト メニューから **[プロパティ]** を選択します。[AMTSCS プロパティ] ウィンドウが表示されます。

4 **[ディレクトリ セキュリティ]** タブを選択します。

5 ウィンドウ下部の **[セキュリティで保護された通信]** セクションで、**[編集]** をクリックします。[セキュリティで保護された通信] ウィンドウが表示されます。

6 ウィンドウ上部の **[セキュリティで保護されたチャネル (SSL) を要求する])** チェックボックスをオフにします。

7 **[OK]** を 2 回クリックして、IIS Manager を終了します。

config.properties ファイルで、scsserver_url パラメータの値を URL で HTTP プロトコルを指定する値に変更します。

Tomcat Service を再起動します。

Java キー ストアへのルート証明書のインポート

TLS 認証の場合は、信頼できるルート証明書を HPCA コンソールの Java キー ストアにインポートする必要があります。これは OOBM で vPro デバイスを認証する際に使用されます。このルート証明書は、60 ページの「ルート証明書をエクスポートするには」で .cer ファイルとしてエクスポートしました。

59 ページの「OOBM Service と SCS 間の安全なアクセスの設定」で説明したように、OOBM と SCS Server 間の安全な通信のために HPCA コンソールの Java キー ストアにルート証明書をインポート済みの場合は、この手順を再度実行する必要はありません。

ルート証明書を Java キー ストアにインポートするには

60 ページの「ルート証明書を Java キー ストアにインポートするには」の手順に従います。

PEM 形式への証明書の変換

この手順は TLS を設定している場合にのみ必要です。

TLS がオンのときに IDE-R と SOL セッションを安全なものにするには、HPCA コンソールで PEM 形式の証明書を使用できるようにする必要があります。60 ページの「ルート証明書をエクスポートするには」で説明したように、ルート証明書は .cer ファイルとしてエクスポートされました。SCS および vPro のセットアップ章の 28 ページの「クライアント証明書をエクスポートするには」で説明したように、クライアント証明書は .pfx ファイルとしてエクスポートされました。このマシンが証明書がエクスポートされた SCS Server マシンと異なる場合は、これらのファイルは HPCA コンソール マシンにコピーされています。

ルート証明書を PEM 形式に変換するには

HPCA コンソール マシンのコマンド ライン プロンプトに、次のように入力します。

```
Openssl x509 -inform DER -outform PEM -in <root.cer> -out <root.pem>
```

例 :

```
Openssl x509 -inform DER -outform PEM -in C:\SCS\RootCA.cer -out
C:\SCS\RootCA.pem
```

クライアント証明書を PEM 形式に変換するには

HPCA コンソール マシンのコマンド ライン プロンプトに、次のように入力します。

```
Openssl pkcs12 -in <client.pfx> -out <client.pem>
```

例 :

```
Openssl pkcs12 -in C:\SCS\ClientAuth.pfx -out C:\SCS\ClientAuth.pem
```

4 OOB デバイスの管理の概要

この章では、HPCA コンソールで実行できるアウトバンド管理 (OOBM) タスクの概要を説明します。これには、Administrator として実行する設定タスク、および Operator として実行するオペレーションが含まれます。

HPCA コンソールで結果を最大限に表示するには、ディスプレイ コンソールの画面解像度を 1280x1024 に設定してください。

設定

次のセクションでは、Administrator ロールで実行して OOB デバイスの管理を準備する設定タスクについて説明します。これらのタスクはすべて、HPCA コンソールの **[設定]** タブで利用可能です。タスクには次が含まれます。

- アウトバンド管理の有効化
- デバイス タイプの選択
- vPro システム保護の設定の管理

アウトバンド管理の有効化

OOBM タスクを実行するには、HPCA コンソールにログインしたとき、アウトバンド管理がまだ有効になっていない場合は、まずそれを有効にします。

[設定] タブの **[アウトバンド管理]** の下で、**[有効化]** をクリックします。[有効化] ウィンドウが表示されます。

詳細については、99 ページの「使用可能性」を参照してください。

デバイス タイプの選択

次に実行する設定タスクは、管理する OOB デバイスのタイプを選択することです。

[設定] タブの **[アウトバンド管理]** の下で、**[デバイス タイプの選択]** をクリックします。[デバイス タイプの選択] ウィンドウが表示されます。

DASH デバイス、vPro デバイス、両方 という 3 つのデバイス タイプのうち 1 つを選択できます。

選択したデバイス タイプに応じて、HPCA コンソールには、選択内容に関連するインターフェイスが表示されます (デバイス タイプの選択によって決まる設定および操作オプションを参照)。

DASH デバイス

DASH を選択した場合、DASH 管理者がすべてのデバイスに同じユーザー名とパスワードを設定していれば、DASH デバイスに共通の認証情報を入力することができます。

認証情報の入力を間違えたり、内容に変更があったりした場合は、次回このウィンドウにアクセスしたときに認証情報を変更できます。

vPro デバイス

vPro デバイスを選択した場合、vPro デバイスにアクセスするための SCS ログイン認証情報、および SCS サービスの URL を入力する必要があります。

認証情報の入力を間違えたり、内容に変更があったりした場合は、次回このウィンドウにアクセスしたときに認証情報を変更できます。

両方

両方のタイプのデバイスを選択した場合、DASH デバイスに共通の認証情報を入力することができます。また、vPro デバイスにアクセスするために必要な SCS ログイン認証情報、および SCS サービスの URL を入力する必要があります。

詳細については、102 ページの「デバイス タイプの選択」を参照してください。

デバイス タイプの選択によって決まる設定および操作オプション

デバイス タイプを選択したら、**[設定]** タブと **[操作]** タブに選択内容を反映したオプションが表示されます。次の表に、オプションの要約を示します。

表 3　　設定とオペレーションのオプション

	DASH	vPro
設定	追加オプションなし	vPro システム保護の設定
オペレーション	デバイス管理	vPro デバイスのプロビジョニング、デバイス管理、グループ管理、警告の通知

デバイス タイプを選択したり、選択内容を変更したりしたときに、**[設定]** タブと **[操作]** タブのナビゲーション パネルにデバイス タイプ関連のオプションを表示するには、HPCA コンソールからログアウトし、再度ログインする必要があります。

vPro システム保護の設定の管理

vPro デバイスおよびデバイス グループの管理を開始する前に、vPro システム保護の設定を定義します。

この設定オプションは、vPro デバイス タイプを選択した場合にのみ表示されます。システム防御設定は、DASH デバイスには適用されません。

[設定] タブの **[アウトバンド管理]** の下で、**[vPro システム保護の設定]** をクリックします。[vPro システム保護の設定] ウィンドウが表示されます。

vPro デバイスを管理するときは、ネットワーク全般のポリシー、フィルタ、ヒューリスティック、エージェント ウォッチドッグを作成できます。

- システム防御フィルタの管理 : vPro デバイスでは、システム防御フィルタを作成、変更、および削除できます。システム防御フィルタにより、ネットワーク上のパケットの流れが監視され、フィルタ条件が一致するとパケットのドロップやパケット レートの制限が可能になります。フィルタは、システム防御ポリシーに割り当てられ、ポリシーを有効化してネットワークを保護することができます。
- システム防御ポリシーの管理 : vPro デバイスでは、システム防御ポリシーを作成、変更、および削除して、そのポリシーをネットワーク上の複数の vPro デバイスに配布できます。システム防御ポリシーによって、ネットワークを選択的に分離し、vPro デバイスを悪意のあるソフトウェアの攻撃から保護することができます。
- システム防御ポリシーの管理 : vPro デバイスでは、ヒューリスティック仕様を作成、変更、および削除して、そのヒューリスティックをネットワーク上の複数の vPro デバイスに配布できます。これらのヒューリスティックにより、ワームの侵入を示す状況が検出され、他のデバイスが感染しないようにそのデバイスが制御されることで、ネットワーク上のデバイスが保護されます。
- エージェント ウォッチドッグの管理 : vPro デバイスでは、エージェント ウォッチドッグを作成、変更、および削除して、そのウォッチドッグをネットワーク上の複数の vPro デバイスに配布できます。エージェント ウォッチドッグは、vPro デバイス上のローカル エージェントが存在しているかどうかを監視します。ローカル エージェントの状態に変更があった場合にエージェント ウォッチドッグが取るアクションを指定できます。

詳細については、103 ページの「vPro システム保護の設定」を参照してください。

HPCA コンソールで OOB デバイスを管理できるようにするために **[設定]** タブで実行する管理タスクはこれで終わりです。Operator または Administrator ロールのユーザーは、**[操作]** タブに移動して、ネットワークの OOB デバイスの管理を始めることができます (オペレーションを参照)。

オペレーション

次のセクションでは、Operator ロールまたは Administrator ロールで OOB デバイスの管理のために実行する操作について説明します。これらのタスクは、HPCA コンソールの **[操作]** タブで実行できます。タスクには次が含まれます。

- プロビジョニングと設定情報
- デバイスの管理
- グループの管理
- 警告の表示

プロビジョニングと設定情報

vPro デバイスや DASH デバイスを検出したり管理したりできるようにするには、事前にそれらのデバイスをプロビジョニングする必要があります。vPro デバイスが、最初にネットワークに接続されたときに自動的にプロビジョニングされなかった場合は、HPCA コンソールからこれらのデバイスをプロビジョニングできます。

[操作] タブの **[アウトバンド管理]** の下で、**[vPro プロビジョニング]** をクリックします。[vPro プロビジョニング] ウィンドウが表示されます。このウィンドウでは、vPro デバイスの探索とプロビジョニングができます。

DASH デバイスのみを管理することを選択した場合、このオプションはこのタイプのデバイスに関連しないため、**[アウトバンド管理]** の下にある **[操作]** タブには表示されません。

詳細については、119 ページの「vPro デバイスのプロビジョニング」を参照してください。

DASH 設定関連ドキュメント

ここでは、DASH 対応デバイスがこれらのデバイスに付随するドキュメントに従って既にプロビジョニングされていることを前提にしています。DASH 設定の情報は、「Broadcom NetXtreme Gigabit Ethernet Plus NIC」のホワイト ペーパーに記載されています。このホワイト ペーパーは、この NIC をサポートする各製品の [マニュアル] のセクションにあります。

この情報は、当社の DASH 対応デバイスにのみ関連しています。

このドキュメントにアクセスするには

1. **http://www8.hp.com/jp/ja/home.html** に移動します。
2. **[サポート & ドライバ] > [製品マニュアル、トラブルシューティング、修理など]** を選択します。
3. この NIC をサポートする製品 (たとえば、dc5850) を入力します。
4. dc5850 モデルの 1 つを選択します。
5. [マニュアル] を選択します。
6. 「Broadcom NetXtreme Gigabit Ethernet Plus NIC」のホワイト ペーパーを選択します。

DASH 設定ユーティリティ

DASH 設定ユーティリティ (BMCC アプリケーション) は、この NIC をサポートする各製品のドライバ セクションにある Broadcom NetXtreme Gigabit Ethernet Plus NIC ドライバ Softpaq の一部です。

このユーティリティにアクセスするには

1. **http://www8.hp.com/jp/ja/home.html** に移動します。
2. [サポート & ドライバ] > **[ドライバ & ソフトウェア ダウンロード]** を選択します。
3. この NIC をサポートする製品 (たとえば、dc7900) を入力します。
4. dc7900 モデルの 1 つを選択します。
5. オペレーティング システムを選択します。
6. **[ドライバ - ネットワーク]** セクションまでスクロールし、NetXtreme Gigabit Ethernet Plus NIC ドライバを選択してダウンロードします。

デバイスの管理

デバイス管理オプションでは、複数の OOB デバイスおよび個々の OOB デバイスを管理できます。

[操作] タブの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。デバイス テーブルのツールバーにあるアイコンから、複数のデバイスに次のタスクを実行できます。

- データのリフレッシュ
- デバイス情報のリロード
- デバイスの探索
- デバイスの電源オン / オフおよび再起動
- vPro 警告メッセージの予約および予約解除
- vPro デバイスに関する共通ユーティリティの管理
- 選択された vPro デバイスへのシステム防御ポリシーの配布
- 選択された vPro デバイスへのヒューリスティック ワーム封じ込め情報の配布
- 選択された vPro デバイスへのエージェント ウォッチドッグの配布
- 選択された vPro デバイスへのエージェント ソフトウェア リストとシステム メッセージの配布

個々の OOB デバイスを管理するには、デバイス テーブル内のホスト名のリンクをクリックします。管理ウィンドウが開き、左側のナビゲーション ペインにいくつかのオプションが表示されます。使用可能なオプションは、選択した管理対象デバイスのタイプによって異なります。管理オペレーションの概要を参照してください。

詳細については、デバイス管理を参照してください。

グループの管理

グループ管理オプションでは、Client Automation ソフトウェアで定義された vPro デバイスのグループを管理できます。vPro デバイスを含む Client Automation グループに対して OOB 操作を実行できます。vPro デバイスのグループを管理することにより、さまざまな検出、自己回復、および保護タスクを実行できます。これには、電源管理、警告メッセージ予約のほか、システム防御ポリシー、エージェント ウォッチドッグ、ローカルのエージェント ソフトウェア リスト、およびヒューリスティックの配布が含まれます。

[操作] タブの **[アウトバンド管理]** の下で、**[グループ管理]** をクリックします。[グループ管理] ウィンドウが表示されます。グループ テーブルのツールバーにあるアイコンから、複数のグループに対して次のタスクを実行できます。

- データのリフレッシュ
- グループ情報のリロード
- グループの電源オン / オフおよび再起動
- vPro 警告メッセージの予約および予約解除
- 選択された vPro グループへのエージェント ソフトウェア リストとシステム メッセージの配布
- vPro デバイス グループのプロビジョニング
- 選択された vPro グループへのシステム防御ポリシーの配布および回収
- 選択された vPro グループへのエージェント ウォッチドッグの配布および回収
- 選択された vPro グループへのヒューリスティック ワーム封じ込め情報の配布および回収

掘り下げてグループ内の個々のデバイスを管理するには、テーブルの [説明] 列の下にあるグループ名のリンクをクリックします。[デバイス管理] ウィンドウが開き、選択されたグループに属するデバイスの一覧が表示されます。グループ内の複数のデバイスまたは個々のデバイスを管理できます。デバイスの管理を参照してください。

詳細については、グループ管理を参照してください。

警告の表示

vPro デバイスの場合、デバイスに警告のサブスクリプションを割り当てていれば、プロビジョニング済みの vPro デバイスによって生成された警告を表示できます。警告の通知を監視すると、ネットワーク上のデバイスの状態についての適切な情報が得られます。

[操作] タブの **[アウトバンド管理]** の下で、**[警告の通知]** をクリックします。[警告の通知] ウィンドウが表示されます。

詳細については、警告の通知を参照してください。

管理オペレーションの概要

次の表では、管理する OOB デバイスのタイプに応じて実行できる管理オペレーションの概要について説明します。

表 4　　アウトバンド デバイスの管理操作

管理オペレーション	vPro	DASH	参照先
プロビジョニング設定[1]	X		119 ページの「vPro デバイスのプロビジョニング」
デバイスの探索[2]	X	X	128 ページの「デバイスの探索」
複数のデバイスの管理	X	X	127 ページの「複数のデバイスの管理」
全般的な資産の探索	X		141 ページの「vPro 一般資産情報の表示」
ハードウェア資産の探索	X	X	141 ページの「ハードウェア資産の表示」
ソフトウェア資産の探索[3]	X	X	142 ページの「ソフトウェア資産の表示」
電源管理[4]	X	X	143 ページの「電源状態の変更」
再起動 [4]	X	X	147 ページの「システムの再起動」
IDE-R での再起動 [4]	X		148 ページの「IDE-R による vPro システムの再起動」
BIOS への再起動 [4]	X		150 ページの「vPro システムの再起動による BIOS 設定画面の表示」
LAN (PXE) への再起動 [4]	X	X	152 ページの「システムの再起動による起動前実行環境への移行」
より目立たないスリープ状態への再起動または電源投入 [4]		X	153 ページの「起動して DASH のみでサポートされている電源状態に移行」
テキスト コンソール リダイレクション	X	X	74 ページの「リモート操作」
デバイス グループ管理	X		163 ページの「グループ管理」

表 4　　アウトバンド デバイスの管理操作 (cont'd)

管理オペレーション	vPro	DASH	参照先
イベント管理	X		140 ページの「vPro イベント ログの表示」、140 ページの「vPro イベント フィルタの表示」、171 ページの「警告の通知」
システム防御	X		103 ページの「システム防御フィルタの管理」、106 ページの「システム防御ポリシーの管理」
エージェント存在	X		114 ページの「エージェント ウォッチドッグの管理」
ヒューリスティック ワーム封じ込め	X		110 ページの「ヒューリスティック情報の管理」
フロント パネル設定の設定	X		160 ページの「vPro デバイスのフロント パネル設定の設定」
フラッシュ制限リセット	X		160 ページの「vPro デバイスのフラッシュ メモリ書き換え回数制限のリセット」
起動設定の設定		X	161 ページの「DASH デバイスの起動設定の設定」

1. プロビジョニング設定 : vPro デバイスは複数の方法でプロビジョニングできます。HPCA コンソールでは、遅延リモート設定で実行する方法のうち 1 つのみを実行できます。マシンのマニュアルにあるとおり、DASH デバイスはすでにプロビジョニングされているものと想定されます。
2. デバイスの探索 : vPro デバイスは、SCS デバイス リポジトリを使用して探索されます。DASH デバイスは、IP アドレスを指定するか、Active Directory (AD) を使用することによって探索されます。
3. ソフトウェア資産の探索 : vPro デバイスのソフトウェア資産は、サード パーティ データ ストアにある情報によって探索されます。DASH デバイスの場合は、ネットワーク コントローラの NVRAM にある情報によって探索されます。
4. 電源および再起動オペレーション : 137 ページの「電源状態への電源操作のマッピング」を参照してください。

5　アウトバンド管理使用ケース シナリオ

この章では、OOB デバイス管理のいくつかの標準シナリオを実行するための HPCA コンソールの使用法について説明します。これらのシナリオには、デバイス上の資産を探索する方法、さまざまな修復機能を実行する方法、およびネットワーク上の vPro デバイスを悪意のあるソフトウェア攻撃から保護する方法が含まれています。HPCA コンソールを使用して、電源の状態、オペレーティング システムの状態、または管理エージェントの有無に関係なくデバイスをリモートで管理することができます。これらのシナリオは、企業において HPCA コンソールのアウトバンド管理 (OOBM) 機能を使用する方法を限なく提示するものではなく、説明に役立つ実例を示すものです。

この章は、大きく 2 つのセクションに分けられます。

- 概念的な概要 : 使用ケースを説明する前に、いくつかの概念的な情報を提示して、これらのシナリオの各タスクの背景を説明します。
- 使用ケース : 使用ケース シナリオを最初から最後まで実行するための手順を説明します。

概念的な概要

設定およびインストール作業の結果、次のタスクを完了したことになります。

- SCS コンソールを使用して SCS Server にアクセスし、vPro デバイスをプロビジョニングする。
- DASH デバイスのドキュメントに従い、DASH デバイスをプロビジョニングする。
- HPCA コンソールのインストールおよび設定を行い、SCS との通信を可能にしてプロビジョニング済みのすべての vPro デバイスのデバイス リストを取得できるようにする。

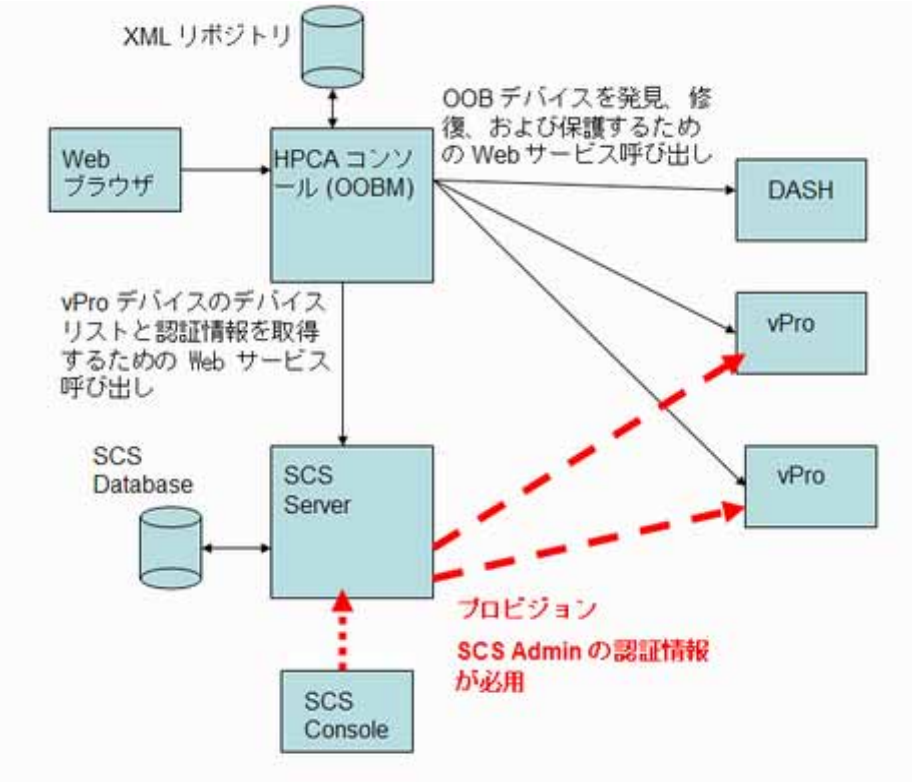
HPCA コンソールを使用して IP または Active Directory 情報を指定することにより、DASH デバイスが探索されます。

これで、次の操作が可能になります。

- Web ブラウザのインターフェイスを使用して HPCA コンソールにログインする。
- コンソールの OOBM オプションを使用して、ネットワーク内のプロビジョニング済みのデバイス上で、サポートされる探索、修復および保護操作をデバイスのタイプに基づいて実行する。

次の図は、この管理ソリューションの主要なコンポーネントを取り上げています。各コンポーネント間でどのように通信が行われているのかが図示されています。

図 7　　アウトバンド管理コンポーネントの概要



次の各セクションでは、ネットワーク上の OOB デバイスの探索、修復、および保護を可能にする OOBM の機能を詳細にわたって説明しています。

保護シナリオは、vPro デバイスのみに関連します。

探索

ネットワーク上のすべてのプロビジョニング済み OOB デバイスで、ハードウェア資産とソフトウェア資産を探索できます。

ハードウェア資産

Intel vPro デバイスは、フラッシュ メモリにハードウェア資産情報を格納します。DASH デバイスは、この情報をネットワーク コントローラの NVRAM に格納します。どちらのメモリも、デバイスの電源がオフであっても、常時読み取りが可能です。必要な条件は、デバイスが物理的にネットワークに接続されていて電源に接続されていることのみです。OOB デバイスは、不意のデータ喪失の防止についてはソフトウェア エージェントに依存しません。HPCA コンソールを使用してこの情報にアクセスし、次の目的でこの情報を使用できます。

- 交換する必要があるデバイスのハードウェア コンポーネントの正確な仕様を判断する。
- 互換性問題を特定する。
- 新しいオペレーティング システムをプロビジョニングする前に、デバイスの設定を検査する。
- マシンの電源がオフであっても、その時々のインベントリ情報を取得する。

ソフトウェア資産

Intel vPro では、vPro デバイスのサード パーティ データ ストレージ (3PDS) に登録されたアプリケーション リストの表示が可能です。3PDS に登録された HP アプリケーションについては、そのアプリケーションが vPro デバイスのスクラッチ パッド領域に書き込んだデータも表示できます。DASH デバイスは、ソフトウェア資産情報をネットワーク コントローラの NVRAM に格納します。HPCA コンソールを使用してこの情報にアクセスし、次の目的でこの情報を使用できます。

- vPro または DASH を利用しているデバイスにアプリケーションがインストールされているかどうかを確認する。各アプリケーションによって、データ ストレージの使用法が細かく異なります。
- 既知の vPro および DASH 対応 HP アプリケーションのアウトバンド情報を取得する。
- 既知の vPro および DASH 対応 HP アプリケーションが正しく登録されているか確認する。これは、一部のアプリケーションのトラブルシューティングに役立ちます。
- 既知の vPro および DASH 対応 HP アプリケーションが正しく動作しているか確認する。
- vPro デバイス上で動作するローカル エージェントに監視させるアプリケーションのソフトウェア リストを表示する。
- エージェント存在ポリシーがアクティブ化されたときにローカル エージェントが vPro デバイスのコンソールに表示するシステム メッセージを表示する。

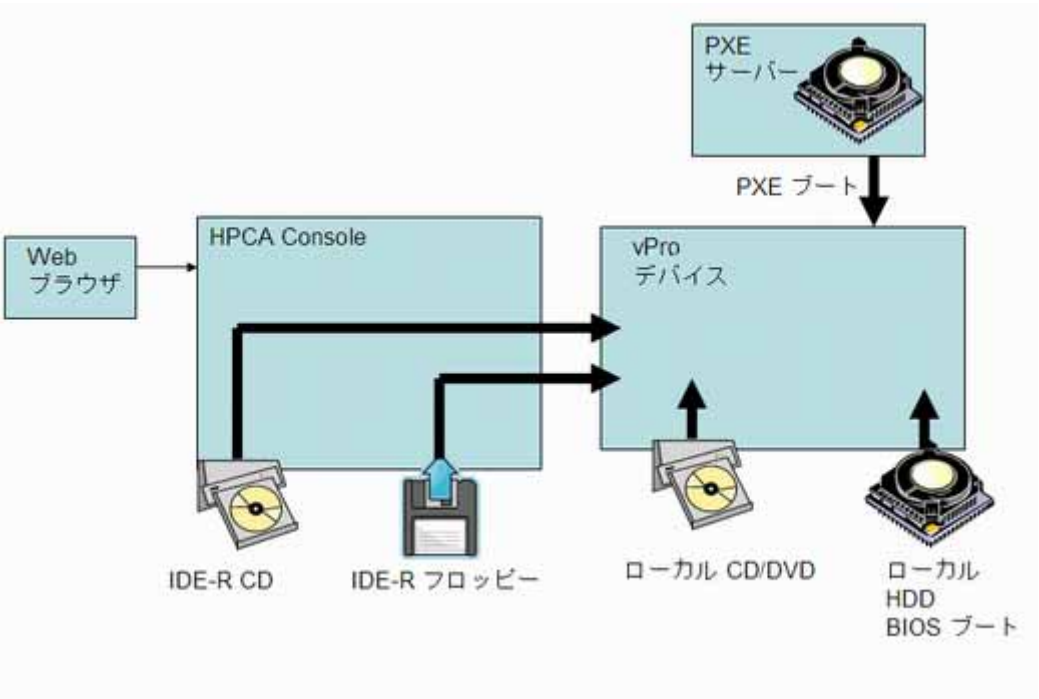
修復

修復操作には、リモート操作とイベント管理があります。

イベント管理は vPro デバイスのみに関連します。

次の図は、HPCA コンソールの OOBM オプションを使用して実行するさまざまなリモート管理操作を示しています (IDE-R は vPro のみに適用されます)。

図 8　　リモート管理操作の概要



リモート操作

Intel vPro および DASH デバイスでは、ソフトウェア、オペレーティング システム、およびハードウェアに障害が発生した後にリモートでデバイスの診断と修復を行うアウトバンド アクセスが可能です。HPCA コンソールを使用して、リモートでデバイスの電源状態の表示、デバイスのハードディスクからの再起動、デバイスのローカル CD/DVD 上のイメージからの再起動、リモートの CD またはフロッピー ドライブからの再起動、PXE Server からの再起動、および BIOS セットアップのための再起動が可能です。任意のリモート操作の実行時またはシステムがアイドル状態のときは、システムの電源状態が変更されます。

これらの機能を使用して、次のようなリモート電源管理を実行できます。

- デバイスの電源のオン / オフ
- テキスト コンソール リダイレクションおよび IDE-R を使用した OOB デバイスの再起動

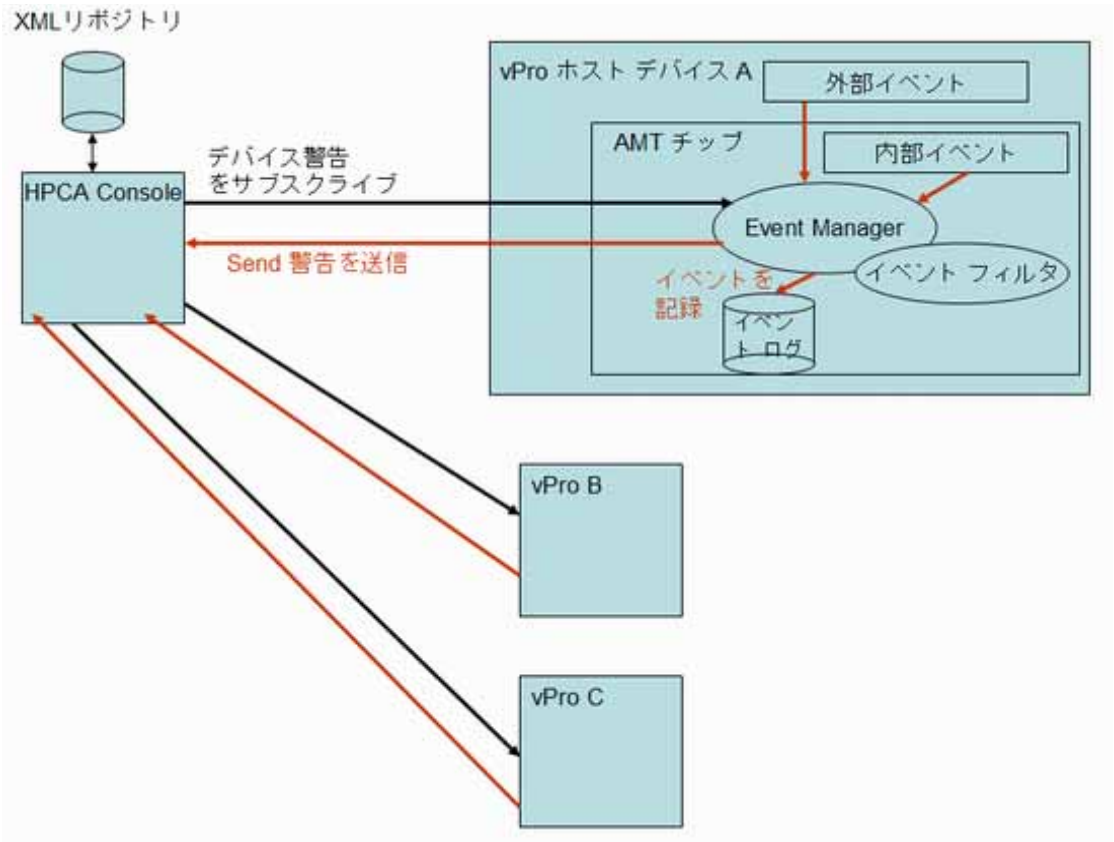
IDE-R (Integrated Drive Electronics Redirect) は、vPro デバイスでのみ使用できます。

電源管理操作で問題のある OOB デバイスを健全な状態に復元できます。

イベント管理

次の図は、vPro システムのイベント管理に関与する動きを示したものです。

図 9　　イベント管理の概要



Intel vPro には、問題を迅速に診断し、エンド ユーザーの休止時間を減らせる警告およびイベント ログ機能が用意されています。イベントは、システム管理 (SM) バスおよびハードウェア センサーなどの外部ソースから生成されます。内部の vPro 自己生成イベントもあります。これらの

内部イベントのソースは複数あります。システム防御フィルタ、エージェント存在障害、ファームウェア更新、およびその他の複数のシナリオによって生成されるイベントが含まれます。したがって、イベントはファン障害などの物理的オカレンス、またはウイルス攻撃などのトラフィック パターンの変更によるフィルタ検出オカレンスとなります。システム上でイベントが発生すると、vPro チップ上にある Event Manager によってイベントが立ち上げられ、イベント フィルタを参照してアクションが決定されます。イベント フィルタによって、各受信プラットフォーム イベントに適用する条件セットが定義されます。受信イベントが条件に一致すると、イベント フィルタによってアクションが指定されます。これらのアクションには、HPCA コンソールへの警告の送信、vPro ログへのイベントのログ記録、またはその両方が含まれます。

vPro デバイスに予約をして、そのデバイスによって生成されたイベント警告を HPCA コンソールに送信する必要があります。予約すると、イベント フィルタ内でのイベント警告の送信先が指定されます。HPCA コンソールにどのデバイス警告を表示するかを決定するイベント警告を予約またはキャンセルできます。

Intel vPro デバイスのファームウェア チップにはデフォルトのイベント フィルター式が組み込まれています。HPCA コンソールでは、特定の vPro デバイスに対してイベント ログのイベントを表示し、記録された各イベントのタイプ、重大度、日付、説明を特定することもできます。

この機能を使用してイベント警告およびログ記録を制御できます。コンソールに送信された警告とイベント ログに書き込まれたイベントを使用して、特定のデバイスに修復または保護のアクションが必要かどうかを判断できます。

保護

ネットワーク上の vPro デバイスを悪意のあるソフトウェア攻撃やワームのまん延から保護できます。Intel vPro では、パケットのフィルタおよびネットワークのデバイス上で実行中の重要なローカル エージェントの存在の監視によってこの機能が提供されます。送信トラフィックを継続的に観察してワームのまん延を検出し阻止するメカニズムを提供することでワームに感染しているデバイスを隔離することもできます。

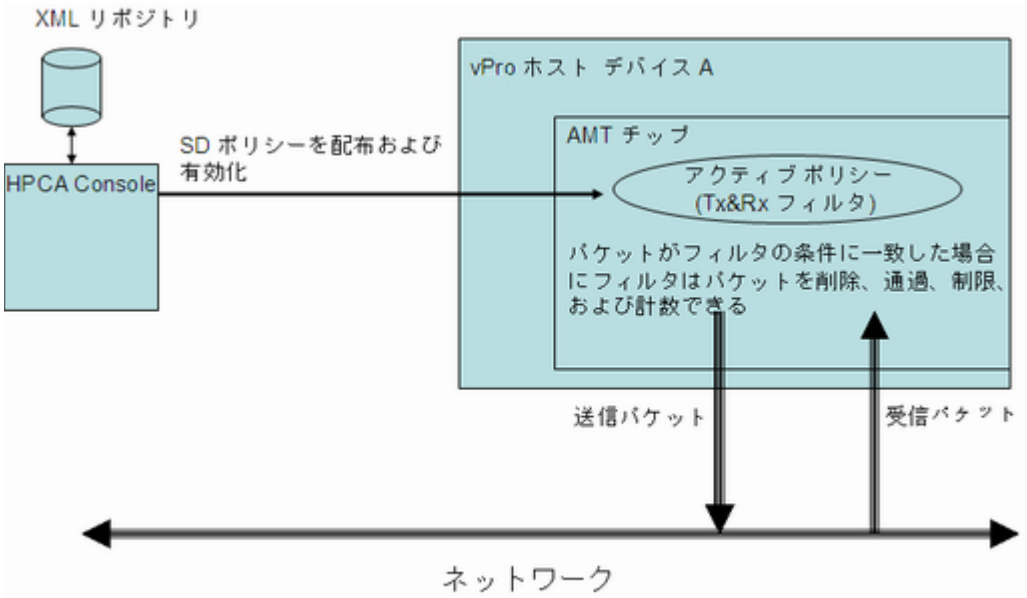
これらのトピックについては、次の各セクションで説明します。

- システム防御
- エージェント存在
- ネットワーク アウトブレイク封じ込めヒューリスティック

システム防御

次の図は、vPro デバイスによって送受信されるパケットを監視するポリシーおよびフィルタを使用したシステム防御の方法の概要を示しています。

図 10　　システム防御の概要



ポリシー

システム防御 vPro 機能を使用すると、HPCA コンソールでネットワークのセキュリティ ポリシーの定義と強制を行うことができます。システム防御ポリシーには、送受信ネットワーク パケットに適用されるフィルタ一式とともに、パケットがフィルタ内の条件に一致した (または一致しなかった) ときのアクションが含まれます。システム防御を使用すると、ポリシーに関連付けられたフィルタに基づき Ethernet および IP プロトコル フローの選択的なネットワーク分離ができます。これらのフィルタによって、管理コンソールは特定の IP ベースのネットワーク フローの通過、制限、またはブロックが可能になり、トラフィック カウントやこれらのフローのオカレンスを記録することができます。

HPCA コンソールでは、これらのフィルタとポリシーはその XML リポジトリに格納されます。コンソールは、システム防御ポリシーを複数の vPro デバイスに配布でき、ポリシーはデバイスのファームウェアに配置されます。

ポリシーを vPro デバイスに配布すると、HPCA コンソールを使用してそのデバイスのポリシーを有効にして、デフォルト システム防御ポリシーにできます。ポリシーをエージェント ウォッチドッグのアクションによって有効化できるエージェント存在ポリシーとして設定することもできます。これについては、77 ページの「エージェント存在」で詳細に説明します。高優先度で有効化されたポリシーが、デバイスのアクティブなポリシーとなります。ポリシーがアクティブ化されると、vPro デバイスによって各送受信パケットが検査され、ポリシーに関連付けられたフィルタによって指定された必要なアクションが実行されます。vPro デバイスに、複数の (すなわち有線および無線) ネットワーク インターフェイス カード (NIC) がある場合、システム防御ポリシーを有効化し、それぞれの NIC にエージェント存在ポリシーを設定できます。

フィルタ

フィルタに関連付けられた条件が一致すると、フィルタでは次のアクションを実行できます。

- パケットを通過させる
- パケットを廃棄する
- パケットを制限する

- 統計データを収集するパケットをカウントする

パケット関連アクションの実行のほかに、フィルタではイベントを発生させることもできます。

フィルタには 2 つのモードがあります。この 2 つの方法は次のとおりです。

- **送信**：このモードのフィルタは vPro デバイスからネットワークに送信されるパケットに適用されます。このフィルタを使用すると、感染が疑われるデバイスからのすべてのトラフィックをブロックし、ネットワーク上の他のデバイスに感染しないようにできます。送信モードのデフォルト フィルタによって、その他のポリシー送信フィルタと一致しないすべての送信パケットが取得されます。このモードのフィルタは、通過、制限、統計、または遮断タイプにできます。
- **受信**：このモードのフィルタは vPro デバイスへのネットワークから受信したパケットに適用されます。このフィルタを使用して、起動後デバイスが受信したすべてのパケットをウイルス対策エージェントなどのローカル エージェントが起動するまでブロックできます。受信モードのデフォルト フィルタによって、その他のポリシー受信フィルタと一致しない受信パケットがすべて取得されます。このモードのフィルタは通過または遮断タイプです。

フィルタのタイプは複数あります。この 2 つの方法は次のとおりです。

- **デフォルト Else**: これは、受信および送信方向モードのデフォルトの Else フィルタです。任意のポリシー フィルタの条件と一致しないすべてのパケットの取得に使用されます。Else フィルタに一致すると (つまり、パケットがその他のフィルタの条件に一致しないと)、フィルタ アクションを生成できます。
- **遮断**：これは受信および送信方向モードの両方の遮断フィルタです。フィルタ条件に一致するすべてのパケットが遮断されます。
- **通過**：これは受信および送信方向モードの両方の通過フィルタです。フィルタ条件に一致するすべてのパケットを通過させます。
- **統計遮断 / 通過**：これは受信および送信方向モードの両方の統計フィルタです。フィルタの条件に一致するパケット数がカウントされます。統計データの収集に使用されます。統計通過フィルタまたは統計遮断フィルタであるかに応じて、パケットを通過させるか遮断することができます。
- **速度制限**：これは受信および送信方向モードの両方の速度制限フィルタです。フィルタの条件に一致する特定タイプのパケットが 1 秒あたりに送受信される数を制限します。このフィルタにはしきい値があり、しきい値に達すると追加トラフィックは切断されます。

フィルタ タイプのほかに、送信フィルタでなりすまし防止を有効化できます。このプロパティを有効化すると、すべての送信パケットがチェックされ、送信元 IP とネットワーク インターフェイス IP アドレスが比較されます。IP アドレスが一致しない場合、パケットは遮断されます。このフィルタが有効な場合、割り当てられた IP アドレスとは異なる送信元 IP アドレスを含む IP パケットを送信してホストが身元を偽ることを防止します。

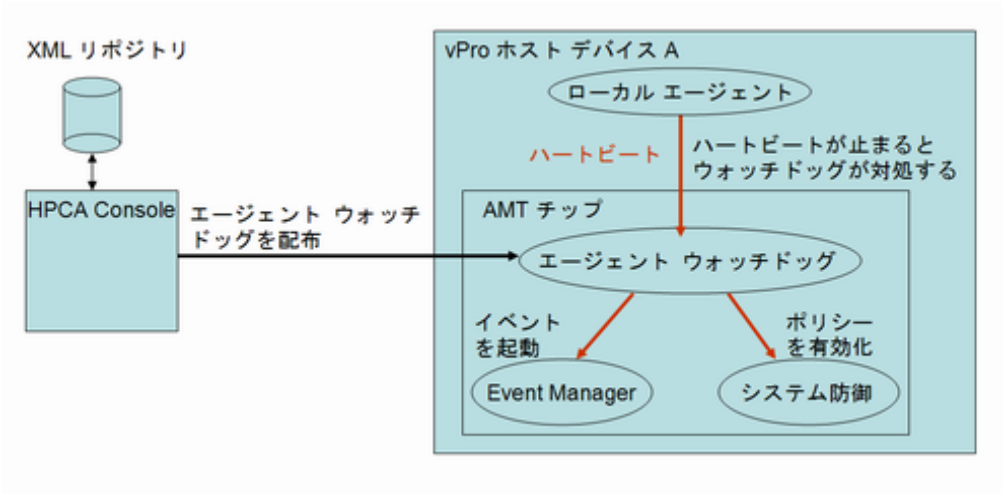
Intel vPro では、受信 (Rx) モードの 32 フィルタ、送信 (Tx) モードの 32 フィルタがサポートされます。32 の Tx および Rx モードのフィルタの各 1 つが Else (不一致) フィルタとして使用されます。なりすまし防止が有効化されている場合は、Tx モードのフィルタのいずれかが使用されます。これにより vPro デバイスに使用できるフィルタが受信用に 31、および送信用に 30 に減ります。

この制限に達すると、そのデバイス上の既存のフィルタの一部を削除するまで、フィルタを含むポリシーを vPro デバイス に配布することはできなくなります。

エージェント存在

次の図は、vPro ホスト デバイス上のローカル エージェントの存在を監視するときに関与するコンポーネントを示しています。

図 11　　エージェント存在の概要



エージェント存在機能により、HPCA コンソールは、vPro デバイスのホスト CPU で実行中のローカル エージェントの状態を監視するエージェント ウォッチドッグを作成できます。通常、ローカル エージェントはウイルス対策またはファイアウォール保護関連のセキュリティ アプリケーションの監視によって vPro デバイスを安全なものにするソフトウェアです。起動すると、ローカル エージェントによってウォッチドッグにハートビートが定期的に送信されます。ハートビートが停止すると、ウォッチドッグはデバイスを保護するアクションを実行します。

ローカル エージェントの詳細については、79 ページの「ローカル エージェント」で説明します。

ウォッチドッグ

エージェント ウォッチドッグが実行できるアクションは、次のとおりです。

- エージェント存在ポリシーが設定されている場合は、それを有効化します。デフォルトのシステム防御ポリシーより優先度が高い場合は、エージェント存在ポリシーがアクティブなポリシーとなり、このポリシーに関連付けられたフィルタがアクティブ化され、ネットワークが保護されます。
- イベントを発行します。Event Manager が イベント フィルタで検索するものに応じて、イベントは vPro チップ上のイベント ログに書き込まれ、または HPCA コンソールに予約されている場合はイベント警告が HPCA コンソールに送信されます。

HPCA コンソールを使用して、次のことができます。

- エージェント ウォッチドッグを作成する
- ローカル エージェントが初期化されるときを検知し、そのエージェント ウォッチドッグに「ハートビート」信号を定期的に送信するタイマーを指定する
- ウォッチドッグにアクションを起こさせるローカル エージェントの遷移状態を指定する。有効な状態は、次のとおりです。
  - 未起動
  - 停止
  - 実行中
  - 期限切れ
  - 中断
- 遷移条件 (エージェント存在ポリシーの有効化またはイベント ログ作成の有効化) に一致しない場合のエージェント ウォッチドッグのアクションを設定する
- 複数の vPro デバイスへエージェント ウォッチドッグを配布 (および回収) する

- ローカル エージェントによって監視されるアプリケーション リストを作成する
- エージェント存在ポリシーがアクティブ化されると表示されるメッセージを作成する

ローカル エージェント

説明したように、ローカル エージェントはデバイスで実行中の重要なアプリケーションの状態を監視することによって vPro デバイスを安全なものにします。ローカル エージェントが監視するアプリケーションのリストはユーザー定義されます。監視対象のアプリケーションが実行を停止すると、ローカル エージェントはウォッチドッグへのハートビートの送信を停止します。ウォッチドッグによってエージェント存在ポリシーが有効化され、アクティブなポリシーになると、vPro デバイスのコンソールにシステム メッセージが表示されます。デフォルト メッセージが提供されますが、システム メッセージはユーザー定義でもあります。アプリケーション リストとシステム メッセージは vPro デバイスの 3PDS に格納されます。

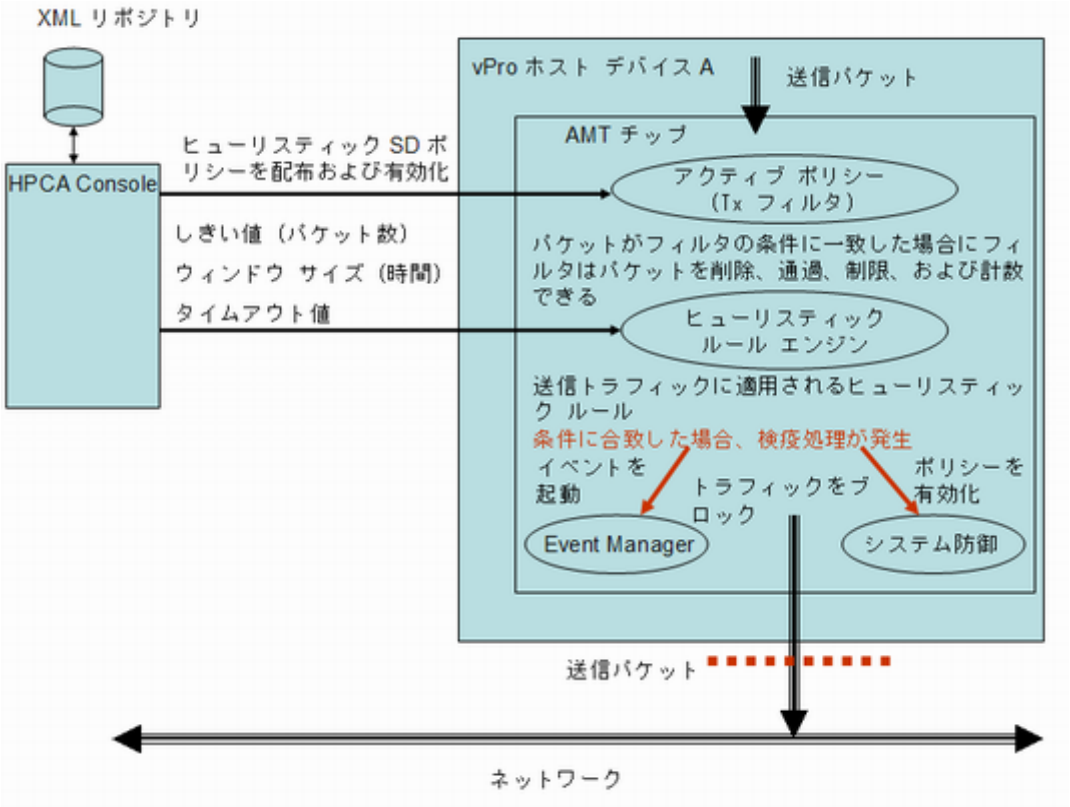
ローカル エージェントがインストールされると (そして、アプリケーションのソフトウェア リストが作成されデバイスに配布されると)、NT サービスとして自動的に起動されます。起動されると、ローカル エージェントは次を実行します。

1. エージェント ウォッチドッグに登録します。
2. vPro チップからハートビート間隔を取得し、エージェント ウォッチドッグにハートビートの送信を開始します。
3. 3PDS を読み込み、監視するアプリケーションのリストを取得して、アプリケーションの監視を開始します。アプリケーション リストの監視に同じハートビート間隔が使用されます。
4. アプリケーション リスト上のアプリケーションが実行を停止すると、ハートビートの送信を停止します。
5. エージェント ウォッチドッグをシャット ダウンし、3PDS から読み込まれるユーザー定義のシステム メッセージを表示します。

ネットワーク アウトブレイク封じ込めヒューリスティック

次の図は、ワーム封じ込めシステムのアーキテクチャの概要を示しています。

図 12　　ワーム封じ込めアーキテクチャ



ワーム封じ込めヒューリスティック メカニズムにより、ネットワーク上にファイアウォールや侵入検知システムが配置されている場合でも、ネットワークに付加価値がもたらされます。ファイアウォールと侵入検知システムは既知のワームに対してのみ効果的に使用できますが、ゼロデイワームの発生に対しては効果的ではありません。

vPro ワーム封じ込めシステムは、ヒューリスティック ルールをホスト vPro デバイスからの送信トラフィックに適用することで機能します。Heuristic Rules Engine が異常を検知すると、ワーム封じ込めシステムによってネットワークはホストから隔離されます。Active Policy フィルタはホスト トラフィックの IP および TCP/UDP プロトコル ヘッダー フィールドで動作します。このフィルタリングの結果、vPro チップはパケットの遮断などの特定のアクションを実行します。

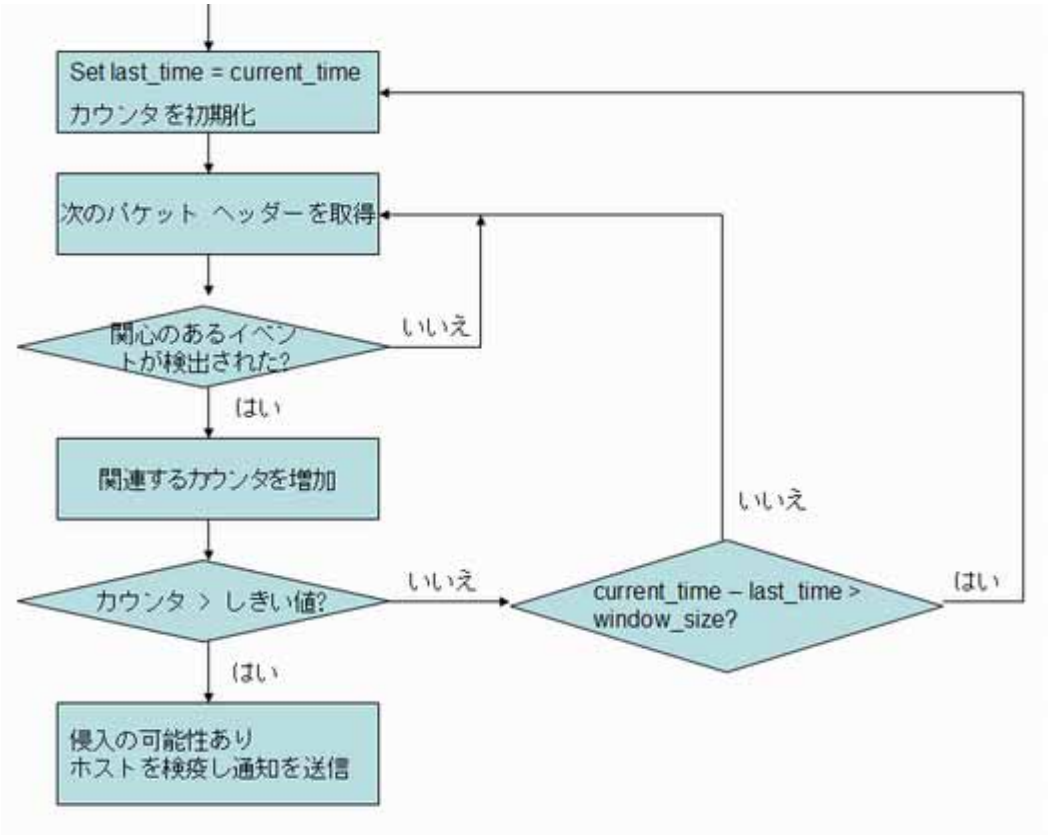
Heuristic Rules Engine によってトラフィックが分析されます。Heuristic Rules Engine によって異常トラフィックの証拠が検知されると、次のアクションのいずれかを実行します。

- イベント警告を発生させる
- イベント警告を発生させ、原因ポートからのすべての送信パケットをブロックする
- イベント警告を発生させ、すべてのポートからのすべての送信パケットをブロックする
- イベントを発生させ、vPro システム防御ポリシーを有効にする

ワーム封じ込めシステムでは、ヒューリスティック ルールに依存してワームによるスキャン アクティビティを示すトラフィック異常が検知されます。ヒューリスティック ルールはすべての自己増殖型ワームの基本特性に基づいています。つまり、ワームがネットワークに広がるには新規ホストにコンタクトする必要があります。その結果、すべてのヒューリスティック ルールでは新規ホストとのコンタクトを示唆するイベントが特定され、そのようなイベントに異常パターンがないかどうかが監視されます。

次の図は、すべてのヒューリスティックで採用される基本メカニズムを示しています。

図 13　　ヒューリスティックの基本操作



詳細情報については、**http://www.intel.com/technology/comms/download/worm_containment.pdf** でヒューリスティック ベースのワーム封じ込めシステムに関する Intel 調査を参照してください。

ウィンドウ サイズとしきい値

すべてのヒューリスティックによってパケット ヘッダーが調査され、指定時間内の「関連イベント」数がカウントされます。その結果、すべてのヒューリスティックによって、ウィンドウ サイズとしきい値という 2 つの設定可能パラメータが明らかにされます。時間枠サイズ (時間数) は、ヒューリスティックがそのカウンタをリセットする期間です。しきい値 (パケット数) は、限界値を表します。カウンタがこの値を超過する場合、異常イベントであることを示します。

HPCA コンソールでは、これらの 2 つのパラメータを設定できます。これらのパラメータを指定する場合は、別のヒューリスティック値が必要な 2 つのワーム タイプを考慮する必要があります。それは、迅速に広がるワームと感染が遅いワームです。迅速に広がるワームと感染が遅いワームについて、正常にワーム感染を検出するには、異なるウィンドウ サイズとしきい値を使用する必要があります。組み合わされたヒューリスティック (異なるウィンドウ サイズと適切なしきい値) を使用すると、より広範囲のワームに対してより効果があります。ウィンドウ サイズが小さめのヒューリスティックは迅速に広がるワームにより効果的で、ウィンドウ サイズが大きめのヒューリスティックは感染が遅いワームに効果的です。

感染が速いワームと遅いワームの設定可能な時間枠のサイズ範囲は、次のとおりです。

- 高速 : 10 ミリ秒～ 1 秒 (1000 ミリ秒)
- 低速 : 1 秒 (1000 ミリ秒) ～ 50 秒 (50000 ミリ秒)

両ヒューリスティックの設定可能なしきい値の範囲は 8 ～ 64 パケット カウントです。

ウィンドウ サイズとしきい値の組み合わせの推奨設定は、次のとおりです。

- 高速 : 10 ミリ秒に 8 パケット
- 低速 : 50 秒に 64 パケット

封じ込めアクションとタイムアウト値

HPCA コンソールでは、しきい値を超えたときにシステムで実行する必要がある自主アクションを指定することもできます。80 ページ で示すように、イベントのみを発生させるか、またはイベントとブロックされた送信ホスト トラフィックまたは有効化されたヒューリスティック システム防御ポリシーを組み合わせたイベントを発生させるかを選択できます。アクション実行後は、Heuristics Rules Engine は無効化されます。

HPCA コンソールによって vPro デバイスに封じ込めアクションを適用する時間を指定できます。0 以外のタイムアウト値 (20 秒以上) を指定すると、Heuristics Rules Engine によってパケットのスキャンが停止され、その時間に指定したアクションが適用されます。指定した時間が経過すると、自動的にアクションが削除され、チップによってパケットのスキャンが再度開始されます。タイムアウト値を 0 に指定すると、Heuristics Rules Engine によってパケットのスキャンが停止され、アクションが永久に適用されます。封じ込めアクションを削除し、再度パケットのスキャンを開始させるには、手動で HPCA コンソール経由で行われるようにする必要があります。

使用ケース

このセクションでは、次の使用ケースについて説明します。

1. ハードウェアの障害と置換
2. オペレーティング システムの障害と再起動
3. ウイルス感染の検出と検疫
4. デバイスの検疫と修復
5. 基幹ソフトウェアの監視
6. ワームの感染と封じ込め

ここで説明する使用ケースのほとんどは、vPro デバイス関連です。DASH デバイスは、該当個所で説明されています。ただし、ナビゲーションと手順の詳細は DASH デバイスごとに異なります。手順情報の詳細については、デバイス管理の章を参照してください。

1. ハードウェアの障害と置換

この使用ケースは、次の 2 つのセクションに分けられます。

- 概要
- 使用ケースで実行する手順

概要

ハードウェア センサー タイプの障害が発生します。この障害により、vPro チップに組み込まれている Event Manager によってイベントが生成されます。Event Manager は、イベント フィルタが提供する情報に基づいて、HPCA コンソールにイベント警告を送信します。

管理者は次の作業を行います。

- vPro デバイスのイベント警告通知を予約します (予約はハードウェア障害が発生する前に実施しておく必要があります)。
- vPro または DASH デバイス上のハードウェア資産を探索して、交換する必要のある部品を特定します。

vPro デバイスの警告通知を予約すると、イベント警告が自動的に HPCA コンソールに送信されます。警告を受信した管理者は、そのデバイスのハードウェア インベントリを調べ、デバイスを復旧させるために必要な交換部品を特定して注文します。

使用ケースで実行する手順

vPro デバイスのイベント警告通知を予約するには

1 **[操作]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

2 目的のデバイスのチェック ボックスをオンにするか、左上の [すべて選択] チェック ボックスをオンにして、警告通知を予約するデバイスを選択します。

3  警告メッセージ予約管理アイコンのプルダウン リストから、**[警告のサブスクライブ]** を選択します。

詳細については、132 ページの「警告メッセージ予約の管理」を参照してください。

警告を表示するには

1 **[操作]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理]** の下で、**[警告の通知]** をクリックします。[警告の通知] ウィンドウが表示されます。

2 HPCA コンソールに送信された、関連のある警告を表示します。このケースでは、ハードウェア障害によって発生したイベント警告を探します。

詳細については、171 ページの「vPro デバイスで発生した警告の表示」を参照してください。

ハードウェア資産を表示するには

1 **[操作]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

2 ハードウェア障害が発生した vPro デバイスの [ホスト名] リンクをクリックします。

3 ウィンドウ左側の **[診断]** の下にある表の [デバイス] カラムで、**[デバイス アセット]** リンクをクリックします。

4 **[ハードウェア情報]** をクリックします。

5 障害の発生したハードウェア コンポーネントをクリックします。そのコンポーネントの仕様がコンソールのコンテキスト領域に表示されます。

詳細については、141 ページの「ハードウェア資産の表示」を参照してください。

これで、HPCA コンソールを介して vPro デバイスまたは DASH デバイスから取得した情報に基づいて、交換部品を注文することができます。

2. オペレーティング システムの障害と再起動

この使用ケースは、次の 2 つのセクションに分けられます。

- 概要
- 使用ケースで実行する手順

概要

vPro デバイスまたは DASH デバイスのオペレーティング システムが応答していません。管理者は PC のユーザーから通知を受けています。

管理者は次の作業を行います。

- リモートの vPro デバイスのフロント パネルをロックして (この例では、問題の vPro デバイスでこの機能がサポートされているものとする)、リモート電源操作の実行中にユーザーが手動で直接操作できないようにします。DASH デバイスには、フロント パネル設定機能は用意されていません。
- HPCA コンソール サーバー上のオペレーティング システム イメージ ファイルを使用して PC を再起動し、問題を詳しく診断します。

使用ケースで実行する手順

vPro デバイスのフロント パネルをロックするには

1 **[操作]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

2 オペレーティング システム障害が発生した OOB デバイスの [デバイス] カラムにある [ホスト名] リンクをクリックします。

3 ウィンドウ左側の **[全般設定]** の下で、**[フロント パネル設定]** リンクをクリックします。

4 **[ここ]** リンクをクリックして、ダイアログの **[フロント パネルの設定]** セクションを有効化します。

5 キーボードと電源ボタンの設定が **[はい]** に設定されていることを確認します。

詳細については、160 ページの「vPro デバイスのフロント パネル設定の設定」を参照してください。

IDE-R CD ドライブからシステムを再起動するには

1 **[操作]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

2 オペレーティング システム障害が発生した vPro デバイスの [ホスト名] リンクをクリックします。

3 ウィンドウ左側の **[診断]** の下で、**[リモート操作]** リンクをクリックします。

4 リモート操作ウィザードで、リモート操作の **[IDE-R を再起動します]** を選択し、[フロント パネルの設定を適用] で **[はい]** を選択します。

5 [ドライブ パス] フィールドに、管理コンソール サーバー上にある ISO ファイルのパスを入力します。

6 ウィザードの残りの手順を実行します。

詳細については、148 ページの「IDE-R による vPro システムの再起動」を参照してください。

3. ウイルス感染の検出と検疫

この使用ケースは、次の 2 つのセクションに分けられます。

- 概要
- 使用ケースで実行する手順

概要

vPro デバイスによって、現在アクティブなシステム防御ポリシーのレート制限フィルタに一致するネットワーク トラフィックが検出されたため、ウイルス攻撃が疑われます。このトラフィックの検出により、vPro チップに組み込まれている Event Manager がイベントを生成します。Event Manager は、イベント フィルタが提供する情報に基づいて、HPCA コンソールにイベント警告を送信します。

管理者は次の作業を行います。

- vPro デバイスのイベント警告通知を予約します。
- 必要なフィルタを使用して検疫ポリシーを作成することにより、感染したデバイス内にウイルスを封じ込め、ネットワーク上の他のデバイスに感染が拡大しないようにします。
- ウイルス感染した vPro デバイスに対して、ポリシーの有効化、アクティブ化、配布を実行します。
- デバイスを修理、交換、または除去します。
- デバイスに脅威がなくなったら、ポリシーを無効化します。

ポリシーを作成、配布、アクティブ化すると、vPro デバイスは、パケットを検査し、検疫ポリシーに関連付けられたフィルタに指定されているアクションを実行します。この例では、フィルタによって、問題のデバイスから送信されるすべての TCP パケットを遮断します。問題のデバイスがネットワークから分離されたら、管理者は、vPro デバイスの復元に必要な修復タスクを実行してから、検疫ポリシーを無効化します。

使用ケースで実行する手順

vPro デバイスのイベント警告通知を予約するには

使用ケース 1. ハードウェアの障害と置換の vPro デバイスのイベント警告通知を予約するにはで説明した手順を実行します。

警告を表示するには

使用ケース 1. ハードウェアの障害と置換の警告を表示するにはで説明した手順を実行します。このケースでは、レート制限フィルタによって生成されたイベント警告を探します。

検疫フィルタを作成するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[フィルタ]** をクリックします。[フィルタ] ウィンドウが表示されます。

2 ツールバーの 追加アイコンをクリックします。システム防御フィルタ ウィザードが表示されます。

3 **[次へ]** をクリックして続行します。[フィルタの詳細] ウィンドウが表示されます。このウィンドウ内で次を指定します。

   — **[フィルタ名]: [Quarantine]** と入力します。

   — **[フィルタ タイプ]: [ドロップ]** を選択します。

   — **[フィルター致時にイベントを作成]: [はい]** を選択します。

4 **[次へ]** をクリックします。[パラメータ] ウィンドウが表示されます。このウィンドウ内で次を指定します。

- **[パケット タイプ]: [TCP]** を選択します。
- **[フィルタ モードまたは方向]: [送信]** を選択します。
- **[ネットワーク アドレス]: [ネットワークへのパケットをフィルタ]** を選択します。
- **ポート範囲 : [ソース ポートの範囲]** を選択します。**[最小のポート]** と **[最大のポート]** にそれぞれ、「1」と「655535」を入力します。これは、vPro デバイス上のポートを表します。この vPro デバイス上のすべての送信元ポートからネットワーク上のすべてのデバイス上のすべての宛先ポートへのパケットの送出をブロックして、この vPro デバイスから他のデバイスへの感染を防ぎます。

5 **[次へ]**、**[閉じる]** の順にクリックします。

詳細については、103 ページの「システム防御フィルタの管理」を参照してください。

検疫ポリシーを作成するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。

2 ツールバーの 追加アイコンをクリックします。システム防御ポリシー ウィザードが表示されます。

3 **[次へ]** をクリックして続行します。[ポリシーの詳細] ウィンドウが表示されます。このウィンドウ内で次を指定します。

- **[ポリシー名]: [Quarantine]** と入力します。
- **[優先度]: [98]** と入力します。
- **アンチ スプーフィング フィルタの有効化 : [はい]** を選択します。
- **[デフォルトの受信 (Rx) フィルタ タイプ]: [パス]** を選択します。
- **[デフォルトの転送 (Tx) フィルタ タイプ]: [パス]** を選択します。

4 **[次へ]** をクリックして、使用可能なすべてのフィルタを確認します。

5 Quarantine フィルタを **[ポリシーに割り当てるフィルタ]** 一覧にドラッグします。

6 **[ポリシーの追加]** をクリックします。

詳細については、106 ページの「システム防御ポリシーの管理」を参照してください。

vPro デバイスに対して検疫ポリシーを有効化、アクティブ化、配布するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。

2 Quarantine ポリシーの横のチェック ボックスをオンにします。

3 ツールバーの 配布アイコンをクリックします。ポリシー配布ウィザードが表示されます。

4 **[次へ]** をクリックして続行します。[デバイスの選択] ウィンドウが表示されます。

5 感染した vPro デバイスの横のチェック ボックスをオンにします。

6 **[次へ]** をクリックします。[ポリシーの設定] ウィンドウが表示されます。

7 有線 NIC のシステム防御ポリシーとして Quarantine ポリシーを選択します。これにより、感染した vPro デバイスのシステム防御ポリシーとして Quarantine ポリシーが有効化されます。この検疫ポリシーには、作成時に、(現在定義されている他のシステム防御ポリシーに対する相対値として) 最高優先度 (98) を指定したため、このポリシーが、感染した vPro デバイスのアクティブなポリシーになります。

8 ウィザードの残りの手順を実行します。

詳細については、106 ページの「システム防御ポリシーの管理」を参照してください。

vPro デバイスの検疫ポリシーを非アクティブ化するには

1 **[操作]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

2 ウイルスに感染した vPro デバイスの [ホスト名] リンクをクリックします。

3 ウィンドウ左側の **[システム防御]** セクションの下にある **[ポリシー]** リンクをクリックします。ウィンドウが開き、このデバイスに配布されているシステム防御ポリシーが表示されます。

4 Quarantine の横のチェック ボックスをオンにします。

5 ツールバーの  有効化 / 無効化アイコンをクリックします。Quarantine ポリシーが、有効化されたシステム防御ポリシーから除外され、無効化されます。

詳細については、156 ページの「vPro デバイスに対するシステム防御ポリシーの管理」を参照してください。

4. デバイスの検疫と修復

この使用ケースは、次の 2 つのセクションに分けられます。

- 概要
- 使用ケースで実行する手順

概要

外部からの攻撃を防ぐため、社内ネットワークの特定のデバイスを検疫する必要があります。ところが、このデバイスを修復するには、デバイスを管理サーバーに接続する必要があります。修復措置では、ウイルス定義の更新、ファイアウォール ソフトウェアの新規バージョンのインストール、管理者による問題のデバイスのリモート制御などが必要になります。

すべてのネットワーク トラフィックをブロックすると、デバイスの修復措置は事実上不可能になります。このため、管理者は、修復管理サーバーとやり取りされるトラフィックのみをブロックの対象から除外して、感染したデバイスを修復できるようにする必要があります。

管理者は次の作業を行います。

- 必要なフィルタが割り当てられた修復ポリシーを作成し、感染したデバイスを修復するために必要なソフトウェアが保管されている HP Client Automation Server に対するトラフィックがブロックの対象から除外されるようにします。
- ネットワーク上のすべての vPro デバイスに対して、ポリシーの有効化、アクティブ化、配布を実行します。
- デバイスの修復が完了したら、ポリシーを無効化します。

ポリシーを作成、配布、アクティブ化すると、vPro デバイスは、パケットを検査し、修復ポリシーに関連付けられたフィルタに指定されているアクションを実行します。この例のフィルタは、フィルタに指定された IP アドレスと一致する IP アドレスを持つデバイスから受信した (またはそのデバイスに送信された) TCP および UDP パケットをすべて通過させます。この例では、HP Client Automation Server の IP アドレスがフィルタに指定されています。その他のパケットは、修復ポリシーのデフォルトのアクション (パケットを遮断する) に基づいて遮断されます。

使用ケースで実行する手順

修復ポリシーに割り当てる 4 つのフィルタを作成します。次の手順を、作成する各フィルタについて 1 回ずつ、計 4 回実行してください。

修復フィルタを作成するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[フィルタ]** をクリックします。[フィルタ] ウィンドウが表示されます。

2 ツールバーの 追加アイコンをクリックします。システム防御フィルタ ウィザードが表示されます。

3 **[次へ]** をクリックして続行します。[フィルタの詳細] ウィンドウが表示されます。作成する各フィルタについて、次の項目を指定します。

表 5

フィルタ名	フィルタ タイプ	フィルター致時にイベントを作成
PassTCP_Recv	通過	はい
PassTCP_Xmit	通過	はい
PassUDP_Recv	通過	はい
PassUDP_Xmit	通過	はい

4 **[次へ]** をクリックします。[パラメータ] ウィンドウが表示されます。作成する各フィルタについて、次の項目を指定します。

表 6

フィルタ名	パケット タイプ	次へ プロトコル	フィルタ モード	ネットワーク アドレス
PassTCP_Recv	IP パケット (IPv4)	TCP	受信	デバイス :192.168.5.12
PassTCP_Xmit	IP パケット (IPv4)	TCP	送信	デバイス :192.168.5.12
PassUDP_Recv	IP パケット (IPv4)	UDP	受信	デバイス :192.168.5.12
PassUDP_Xmit	IP パケット (IPv4)	UDP	送信	デバイス :192.168.5.12

5 **[次へ]**、**[閉じる]** の順にクリックします。

1 つのデバイスではなく、1 つの特定のサブネットとの間でやり取りされるトラフィックを通過させ、その他のすべてのトラフィックを遮断するフィルタを作成することもできます。このようなフィルタは、単一のサブネットに複数の修復用サーバーが配置されている場合に便利です。

詳細については、103 ページの「システム防御フィルタの管理」を参照してください。

修復ポリシーを作成するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。

2 ツールバーの 追加アイコンをクリックします。システム防御ポリシー ウィザードが表示されます。

3 **[次へ]** をクリックして続行します。[ポリシーの詳細] ウィンドウが表示されます。このウィンドウ内で次を指定します。

— **[ポリシー名]: [Remediation]** と入力します。

— **[優先度]: [98]** と入力します。

— **アンチ スプーフィング フィルタの有効化 : [はい]** を選択します。

— **[デフォルトの受信 (Rx) フィルタ タイプ]: [ドロップ]** を選択します。

— **[デフォルトの転送 (Tx) フィルタ タイプ]: [ドロップ]** を選択します。

4 **[次へ]** をクリックして、使用可能なすべてのフィルタを確認します。

5 PassTCP_Recv、PassTCP_Xmit、PassUDP_Recv、PassUDP_Xmit の各フィルタを **[ポリシーに割り当てるフィルタ]** 一覧にドラッグします。

6 **[ポリシーの追加]** をクリックします。

詳細については、106 ページの「システム防御ポリシーの管理」を参照してください。

vPro デバイスに対して修復ポリシーを有効化、アクティブ化、配布するには

使用ケース 3. ウイルス感染の検出と検疫の vPro デバイスに対して検疫ポリシーを有効化、アクティブ化、配布するには で説明した手順を実行します。この例では、Remediation(修復) ポリシーを選択します。

vPro デバイスの Remediation ポリシーを非アクティブ化するには

使用ケース 3. ウイルス感染の検出と検疫の vPro デバイスの検疫ポリシーを非アクティブ化するには で説明した手順を実行します。この例では、Remediation(修復) ポリシーを選択します。

5. 基幹ソフトウェアの監視

この使用ケースは、次の 2 つのセクションに分けられます。

- 概要
- 使用ケースで実行する手順

概要

vPro デバイスにローカル エージェントをインストールして起動し、一連のセキュリティ関連アプリケーションを監視していますが、監視対象のセキュリティ アプリケーションが停止すると、ローカル エージェントによるウォッチドッグへのハートビート送信も停止します。このような遷移状態に入ると、ウォッチドッグは、エージェント ウォッチドッグの作成時に管理者によって指定されたアクションを実行します。この例では、ウォッチドッグがイベントを生成し、エージェント存在ポリシーを有効化します。

通常、このようなシナリオは、ユーザーが、パフォーマンスの低下を防ぐためにウイルス対策ソフトウェアを無効にしたときに発生します。セキュリティ管理者は、ウイルス対策ソフトウェアが実行されていない PC を社内ネットワークから除外するポリシーを実施する必要があります。

管理者は次の作業を行います。

- vPro デバイスのイベント警告通知を予約します。
- ローカル エージェント障害発生時に vPro デバイスを分離するシステム防御ポリシーを定義し、エージェント存在ポリシーとして設定します。
- エージェント ウォッチドッグを作成し、そのアクションを指定します。
- エージェント存在ポリシーとウォッチドッグを vPro デバイスに配布します。

- ローカル エージェントの設定を管理し、その設定を vPro デバイスに配布します。
- vPro ホスト オペレーティング システムにローカル エージェントをインストールします (ローカル エージェントはインストーラによって自動的に起動されます)。
- イベント警告が送信されたら、セキュリティ プロセスを再起動します。

ローカル エージェントを vPro デバイスにインストールして起動すると、そのローカル エージェントはウォッチドッグに登録され、ウォッチドッグに定義済みの間隔でハートビートの送信を開始します。エージェントで障害が発生すると、エージェントはウォッチドッグへのハートビートの送信を停止します。ウォッチドッグはイベントを生成し、配布済みのエージェント存在ポリシーを有効化します。エージェント存在ポリシーは、他のポリシーより優先度が高いため、アクティブなポリシーになります。エージェント存在ポリシーがアクティブ化されると、vPro デバイスはパケットを検査し、エージェント存在ポリシーに関連付けられたフィルタに指定されたアクションを実行します。管理者は、修復作業 (すなわちローカル エージェントが監視していたセキュリティ ソフトウェアの再起動) を行います。セキュリティ ソフトウェアが再起動されると、ローカル エージェントは、ウォッチドッグに再登録され、ウォッチドッグへのハートビートの送信を開始します。ウォッチドッグはエージェント存在ポリシーを無効化します。そして、有効化されているシステム防御ポリシーのうち、他のポリシーより高い優先度をもつものが、次のアクティブなポリシーになります。

使用ケースで実行する手順

vPro デバイスのイベント フィルタを表示するには

1 **[操作]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

2 イベント フィルタを表示する vPro デバイスの [ホスト名] リンクをクリックします。

3 ウィンドウ左側の **[診断]** セクションの **[イベント フィルタ]** リンクをクリックします。選択した vPro デバイス上に存在するデフォルトのイベント フィルタが、コンソールの内容領域に表示されます。

4 各イベント フィルタの [名前] リンクをクリックして、エージェントの障害を検出し管理コンソールに警告を送信するイベント フィルタを確定します。

詳細については、140 ページの「vPro イベント フィルタの表示」を参照してください。

vPro デバイスのイベント警告通知を予約するには

直前の使用ケースの vPro デバイスのイベント警告通知を予約するにはで説明した手順を実行します。

エージェント存在ポリシーに関連付けるフィルタを作成するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[フィルタ]** をクリックします。[フィルタ] ウィンドウが表示されます。

2 ツールバーの  追加アイコンをクリックします。システム防御フィルタ ウィザードが表示されます。

3 [次へ] をクリックして続行します。[フィルタの詳細] ウィンドウが表示されます。このウィンドウ内で次を指定します。

   — **[フィルタ名]: [PreventInfection]** と入力します。

   — **[フィルタ タイプ]: [ドロップ]** を選択します。

   — **[フィルター致時にイベントを作成]: [はい]** を選択します。

4 **[次へ]** をクリックします。[パラメータ] ウィンドウが表示されます。このウィンドウ内で次を指定します。

   — **[パケット タイプ]: [TCP]** を選択します。

   — **[フィルタ モードまたは方向]: [受信]** を選択します。

— **[ネットワーク アドレス]**: **[ネットワークからのパケットをフィルタ]** を選択します。

— **ポート範囲 : [宛先ポート範囲]** を選択します。**[最小のポート]** と **[最大のポート]** にそれぞれ、「1」と「655535」を入力します。これは、vPro デバイス上のポートを表します。ネットワーク上のすべてのデバイス上のすべての送信元ポートから、この vPro デバイス上のすべての宛先ポートへのパケットをブロックして、この vPro デバイスへの感染を防ぎます。

5 **[次へ]**、**[閉じる]** の順にクリックします。

詳細については、103 ページの「システム防御フィルタの管理」を参照してください。

エージェント存在ポリシーを作成するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。

2 ツールバーの 追加アイコンをクリックします。システム防御ポリシー ウィザードが表示されます。

3 [次へ] をクリックして続行します。[ポリシーの詳細] ウィンドウが表示されます。このウィンドウ内で次を指定します。

— **[ポリシー名]**: **[PreventInfection]** と入力します。

— **[優先度]**: **[99]** と入力します。

— **アンチ スプーフィング フィルタの有効化 : [はい]** を選択します。

— **[デフォルトの受信 (Rx) フィルタ タイプ]**: **[パス]** を選択します。

— **[デフォルトの転送 (Tx) フィルタ タイプ]**: **[パス]** を選択します。

4 **[次へ]** をクリックして、使用可能なすべてのフィルタを確認します。

5 PreventInfection フィルタを **[ポリシーに割り当てるフィルタ]** 一覧にドラッグします。

6 **[ポリシーの追加]** をクリックします。

詳細については、106 ページの「システム防御ポリシーの管理」を参照してください。

エージェント存在ポリシーを vPro デバイスに設定および配布します。

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。

2 PreventInfection ポリシーの横のチェック ボックスをオンにします。

3 ツールバーの 配布アイコンをクリックします。ポリシー配布ウィザードが表示されます。

4 **[次へ]** をクリックして続行します。[デバイスの選択] ウィンドウが表示されます。

5 ローカル エージェントを実行する vPro デバイスの横にあるチェック ボックスをオンにします。

6 **[次へ]** をクリックします。[ポリシーの設定] ウィンドウが表示されます。

7 有線 NIC のエージェント存在ポリシーとして **PreventInfection** ポリシーを選択します。これにより、PreventInfection ポリシーが、vPro デバイスのエージェント存在ポリシーとして設定されます。このエージェント存在ポリシーは、ローカル エージェントがエージェント ウォッチドッグへのハートビート送信を停止すると、そのウォッチドッグによって有効化されます。このエージェント存在ポリシーには、作成時に最高の優先度 (99) を指定してあるため、このポリシーがウォッチドッグによって有効化されると、アクティブなポリシーになります。

8 ウィザードの残りの手順を実行します。

詳細については、106 ページの「システム防御ポリシーの管理」を参照してください。

エージェント ウォッチドッグを作成するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理]** > **[vPro システム保護の設定]** の下で、**[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。

2 エージェント ウォッチドッグを作成するには、  追加アイコンをクリックします。エージェント ウォッチドッグ ウィザードが表示されます。

3 **[次へ]** をクリックして続行します。このウィンドウ内で次を指定します。

— **[エージェント タイプ]: [HP ローカル エージェント]** を選択します。

— **[名前]: [AlphaWatchdog]** と入力します。

— **[エージェント GUID]**: HP ローカル エージェントの GUID は既知であるため、このフィールドは、HP ローカル エージェントではグレー表示になっています。

— **[ハート ビート間隔 (秒)]**: デフォルト値を受け入れます。

— **[起動間隔 (秒)]**: デフォルト値を受け入れます。

4 **[次へ]** をクリックします。ウィザードの [ウォッチドッグ アクション] ページが表示されます。このウィンドウ内で次を指定します。

— **[遷移状態]:**

[接続元]: [エージェントは実行中です] を選択します。

[接続先]: [エージェントが停止しています] を選択します。

— **[アクション]:**

[エージェント存在] の場合は、**[有効化]** を選択すると、ローカル エージェントが指定済みの遷移状態に入ったときエージェント存在ポリシーが有効化されます。

[イベント生成] の場合は、**[有効化]** を選択すると、ローカル エージェントが指定済みの遷移状態に入ったときイベントが生成されます。

5 **[アクションの追加]** をクリックします。ウィンドウ下部のアクション テーブルにアクションが追加されます。

6 新しい遷移状態のアクションを追加します。ここでは、このウィンドウで次のように指定します。

— **[遷移状態]:**

[接続元]: [エージェントが停止しています] を選択します。

[接続先]: [エージェントは実行中です] を選択します。

— **[アクション]:**

[エージェント存在] の場合は、**[無効化]** を選択すると、ローカル エージェントが指定済みの遷移状態に入ったとき、エージェント存在ポリシーが無効化されます。

[イベント生成] の場合は、**[有効化]** を選択すると、ローカル エージェントが指定済みの遷移状態に入ったときイベントが生成されます。

7 **[アクションの追加]** をクリックします。ウィンドウ下部のアクション テーブルにアクションが追加されます。

8 ウィザードの残りの手順を実行します。

詳細については、114 ページの「エージェント ウォッチドッグの管理」を参照してください。

vPro デバイスにエージェント ウォッチドッグを配布するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。

2 AlphaWatchdog の横のチェック ボックスをオンにします。

3 ツールバーの  エージェント ウォッチドッグ配布アイコンをクリックします。ウォッチドッグ配布ウィザードが表示されます。

4 **[次へ]** をクリックして続行します。[デバイスの選択] ウィンドウが表示されます。

5 ローカル エージェントを実行する vPro デバイスの横にあるチェック ボックスをオンにします。

6 ウィザードの残りの手順を実行します。

詳細については、114 ページの「エージェント ウォッチドッグの管理」を参照してください。

システム メッセージおよびソフトウェア リストを設定するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。

2  ローカル エージェント設定アイコンをクリックします。[ソフトウェア リスト] ダイアログが表示されます。

3 **[システム メッセージ]** テキスト ボックスに入力されているデフォルトのメッセージを受け入れます。

4 **[ソフトウェア名]** ボックスに「**symantec.exe**」と入力します。

5 **[追加]** をクリックします。このプロセスを繰り返して、ローカル エージェントに監視させるソフトウェア アプリケーションのリストを作成できます。

6 **[保存]** をクリックします。情報メッセージが画面に表示されます。

7 **[閉じる]** をクリックして、ダイアログを終了します。システム メッセージおよびエージェント ソフトウェア リストは XML リポジトリに格納されます。

詳細については、117 ページの「システム メッセージおよびソフトウェア リストを設定するには」を参照してください。

システム メッセージとソフトウェア リストを配布するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。

2 ツールバーの  ソフトウェア リストとシステム メッセージの配布アイコンをクリックします。これで、ソフトウェア配布ウィザード開始されます。

3 **[次へ]** をクリックします。[ソフトウェア タイトル] ウィンドウが表示されます。

4 **[symantec.exe]** アプリケーションを選択します。

5 **[次へ]** をクリックします。[デバイス] ウィンドウが表示されます。

6 ローカル エージェントを実行する vPro デバイスの横にあるチェック ボックスをオンにします。

7 **[次へ]** をクリックして、ウィザードの残りの手順を実行します。

詳細については、117 ページの「システム メッセージとソフトウェア リストを配布するには」を参照してください。

ローカル エージェントを vPro デバイスにインストールして起動するには

1 HPCA Core 配布メディアの `Media\oobm\win32\LocalAgent` ディレクトリにある `oobmclocalagent.msi` ファイルを vPro デバイスにコピーします。コピーしたファイルをダブル クリックします。または、配布メディア上の上記と同じディレクトリにある `setup.cmd` ファイルを vPro デバイスにコピーします。setup ファイルをダブル クリックするか、コマンド ラインに「`setup.cmd`」と入力します。`setup.cmd` ファイルによって、`oobmclocalagent.msi` ファイルが呼び出されます。

2 **[次へ]** をクリックして、ライセンス契約に同意します。

3 **[次へ]** をクリックします。[リモート設定パラメータ] ウィンドウが表示されます。このウィンドウ内で次を指定します。

- **SCS 設定クライアント ユーザー名**: 設定クライアントのロールを持つユーザーのユーザー名を入力します。例では、「**SCSUser@vlan1.hp.com**」と入力しています。
- **SCS 設定クライアント パスワード** : SCSUser のパスワードを入力します。このロールの詳細については、SCS および vPro のセットアップの章の 42 ページの「設定クライアント ロール」を参照してください。
- **SCS プロファイル ID**: vPro デバイスのプロファイルを入力します。この情報は、SCS Console の [プロファイル] 領域に表示されます。
- **SCS リモート設定 URL**: Intel Setup and Configuration Service (SCS) Web サービスの仮想ディレクトリを含む URL パスを入力します。たとえば、**https://provisionserver.vlan1.hp.com /amtscs_rcfg** のように入力します。ここで、**provisionserver.vlan1.hp.com** は、IIS ホスト コンピュータの完全修飾ドメイン名 (FQDN)、**amtscs_rcfg** は、同ホスト コンピュータ上の SCS Web サービス仮想ディレクトリです。

4 **[次へ]** をクリックします。[ユーザー情報] ウィンドウが開き、vPro 管理者認証情報を入力できます。このウィンドウ内で次を指定します。

- **ユーザー名** : 管理者の vPro ユーザー名を入力します。
- **パスワード** : 管理者の vPro パスワードを入力します。
- この使用ケースでは、vPro デバイスを TLS モードでプロビジョニングしないため、**[TLS モード]** チェック ボックスはオフにします。

5 **[次へ]** をクリックして、インストール ウィザードの残りの手順を実行します。

詳細については、SCS および vPro のセットアップの章の 42 ページの「OOBM ローカル エージェントのインストール」を参照してください。

ローカル エージェントは NT サービスであり、インストールが完了次第、開始されます。

ソフトウェア リストに登録されているアプリケーションのうち、ローカル エージェントの監視対象となるアプリケーションはすべて、ローカル エージェントの起動時に実行状態である必要があります。監視対象のアプリケーションが実行されていないと、ウォッチドッグは、起動後すぐに、ローカル エージェントによってシャット ダウンされてしまいます。

エージェント存在ポリシーを vPro デバイスでアクティブ化するには

エージェント ウォッチドッグ作成時に、実行中から停止までの遷移状態に入ったときのアクションとして、このアクションを指定したため、エージェント存在ポリシーは、エージェント ウォッチドッグによって自動的に有効化されます。

システム防御ポリシーを作成し、エージェント存在ポリシーとして設定したとき、エージェント存在ポリシーの優先度を 99 に設定してあるため、エージェント存在ポリシーの優先度は現在のアクティブなシステム防御ポリシーよりも高くなり、自動的にアクティブなポリシーになります。

警告を送信するには

エージェント ウォッチドッグの作成時に、実行中から停止までの遷移状態に入ったときのアクションとして、イベントの生成を指定したため、イベントはエージェント ウォッチドッグによって自動的に生成されます。

このタイプのイベントのデフォルトのイベント フィルタには、イベントのログへの記録と警告の送信の両方が指定されているため、vPro デバイスの警告通知を予約していれば、イベント警告は自動的に管理コンソールに送信されます。

このケースでは、ローカル エージェントが実行されている vPro デバイスのイベント警告通知を予約しているため、イベント フィルタの警告の送信先は既知となり、警告が管理コンソールに送信されるようになります。

警告を表示するには

直前の使用ケースの警告を表示するにはで説明した手順を実行します。このケースでは、ローカル エージェントの障害によって発生したイベント警告を探します。

セキュリティ プロセスを再起動するには

コマンド ラインにコマンドを入力するか、実行可能ファイルをダブル クリックして、セキュリティ アプリケーションを起動します。

エージェント存在ポリシーを vPro デバイスで非アクティブ化するには

ローカル エージェントがウォッチドッグに対するハートビートの送信を再開すると、ウォッチドッグは、停止から実行中までの遷移状態に対応する定義済みアクションに基づいてエージェント存在ポリシーを自動的に無効化し、有効化されているシステム防御ポリシーのうち、他のポリシーより高い優先度をもつものが、新しいアクティブなポリシーになります。

6. ワームの感染と封じ込め

この使用ケースは、次の 2 つのセクションに分けられます。

- 概要
- 使用ケースで実行する手順

概要

ファイアウォールと侵入検知システムはすでにネットワーク上に配置されていますが、こうした仕組みが効力を発揮するのは既知のワームに対してのみであり、ゼロデイのワームの突発的大発生に対しては効果がないことを管理者は認識しています。こうした突発的大発生からネットワークを保護するには、ヒューリスティックによるワーム封じ込めシステムが必要です。

管理者は次の作業を行います。

- vPro デバイスのイベント警告通知を予約します。
- 封じ込めアクションを起動するしきい値 (パケット数) とウィンドウ サイズ (時間) を定義するヒューリスティック仕様を作成します。
- しきい値とウィンドウ サイズに基づいて、vPro チップに組み込まれている Heuristics Rules Engine がワーム大流行の可能性を示すネットワーク トラフィックを検出した場合のアクションを指定します。
- 封じ込めアクションの実効期間のタイムアウト値を指定します。
- 脆弱な vPro デバイスに対してヒューリスティック仕様を配布します。

- 突発的大流行の可能性が警告された場合に必要な修復タスクを実行します。

ヒューリスティック情報を vPro デバイスに配布すると、Heuristics Rules Engine によって、パケット数と更新回数がカウントされます。カウンタの値がヒューリスティック条件を満たすと、管理者の指定したアクションが起動されます。この使用ケースでは、イベントを生成し、攻撃元ポートの送信トラフィックをブロックします。ヒューリスティック条件が満たされると常に、vPro チップに組み込まれている Event Manager によってイベントが生成されます。この使用ケースでは、vPro デバイスのイベント フィルタに、このタイプのイベントに対応するエントリが定義されており、そのエントリでイベント警告が有効化されているものとします。

問題のデバイスがネットワークから分離されたら、管理者は、vPro デバイスの復元に必要な修復タスクを実行します。ヒューリスティック アクションの有効期間は、タイムアウト値に指定された期間です。タイムアウト値に指定された時間が経過すると、ヒューリスティック アクションは解除され、Heuristics Rules Engine がトラフィック フローの検査を再開します。

使用ケースで実行する手順

vPro デバイスのイベント警告通知を予約するには

直前の使用ケースの vPro デバイスのイベント警告通知を予約するにはで説明した手順を実行します。

ヒューリスティック仕様を作成するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ヒューリスティック]** をクリックします。[ヒューリスティック] ウィンドウが表示されます。

2 追加アイコンをクリックして、新しいヒューリスティック情報を作成します。ヒューリスティック ウィザードが表示されます。

3 **[次へ]** をクリックして続行します。[ヒューリスティックの詳細] ウィンドウが表示されます。このウィンドウ内で次を指定します。

- **[設定タイプ : [デフォルト] を選択します。**
- **パラメータ**
  - **[名前]**: 「Zero_Worm」と入力します。
  - **[高速パケットの総数]**: デフォルト値である 8 を受け入れます。
  - **[高速期間の総数]**: デフォルト値である 10 を受け入れます。
  - **[低速パケットの総数]**: デフォルト値である 64 を受け入れます。
  - **[低速期間の総数]**: デフォルト値である 50 秒 (50000 ミリ秒) を受け入れます。
  - **[タイムアウト発生]**: 「50」(秒) と入力します。

    詳細は、81 ページの「ウィンドウ サイズとしきい値」および 82 ページの「封じ込めアクションとタイムアウト値」を参照してください。
- **アクション**
  - **[TX トラフィックのブロック]**: プルダウン リストから **[攻撃元ポートのみ]** を選択します。
- **ポリシー**
  - **[ポリシー名]**: このケースでは、ヒューリスティック条件が満たされたとき、システム防御フィルタを有効化しないようにするため、プルダウン リストからポリシー名を選択しません。

4 **[次へ]** をクリックします。操作のステータスが表示されます。

5 **[閉じる]** をクリックして、ウィザードを終了します。ヒューリスティック テーブルに新しいヒューリスティック情報が表示されます。この情報はリポジトリに追加されます。

詳細については、110 ページの「ヒューリスティック情報の管理」を参照してください。

ヒューリスティック仕様を配布するには

1 **[設定]** タブの、左側のナビゲーション メニューにある **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ヒューリスティック]** をクリックします。[ヒューリスティック] ウィンドウが表示されます。

2 Zero_Worm ヒューリスティック仕様の横のチェック ボックスをオンにします。

3 ツールバーの  ヒューリスティック配布アイコンをクリックします。ヒューリスティック ウィザードが表示されます。

4 **[次へ]** をクリックして続行します。[デバイスの選択] ウィンドウが表示されます。

5 ヒューリスティック情報の配布先の各デバイスの横にあるボックスをオンにします。

6 **[次へ]** をクリックします。[ヒューリスティック設定] ウィンドウが表示されます。

7 選択したデバイスの有線 / 無線の両ネットワーク インターフェイスについて、Zero_Worm ヒューリスティック仕様を選択します。

8 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

9 **[次へ]** をクリックして配布プロセスを続行します。[結果] ウィンドウに操作結果が表示されます。

10 **[閉じる]** をクリックして、ウィザードを終了します。

詳細については、110 ページの「ヒューリスティック情報の管理」を参照してください。

警告を表示するには

直前の使用ケースの警告を表示するにはで説明した手順を実行します。このケースでは、Heuristics Rules engine によって生成されたイベント警告を探します。

6 管理タスク

この章では、HPCA コンソールを使用して、Administrator ロールで実行できるアウトバンド管理 (OOBM) タスクについて説明します。次のタスクが含まれます。

- 使用可能性
- デバイス タイプの選択
- vPro システム保護の設定

使用可能性

HPCA コンソールを使用して、OOBM 機能を有効化できます。

OOBM が無効な場合、**[使用可能性]** 以外のオプションは HPCA コンソールの **[設定]** タブおよび **[操作]** タブ内に表示されません。また、HPCA コンソールの **[管理]** タブからはアウトバンド デバイス コンソールにアクセスできません。

OOBM を有効化するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理]** の下で、**[使用可能性]** をクリックします。[使用可能性] ウィンドウが表示されます。

3 **[有効]** の横にあるボックスをオンにして、**[保存]** をクリックします。アウトバンド管理が有効になります。自動的にログオフします。

4 再度 HPCA 管理コンソールにログオンします。

HPCA 管理コンソールに再度ログインすると、後続のセクション設定、オペレーション、および管理で説明する OOBM オプションが追加表示されています。

設定

[使用可能性] に加え、**[設定]** タブの **[アウトバンド管理]** の下に **[デバイス タイプの選択]** が表示されます。

デバイス タイプの選択によっては、別のオプションが表示される場合もあります。vPro システム保護の設定を参照してください。

オペレーション

[アウトバンド管理] が、**[操作]** タブの左側のナビゲーション ペインに表示されます。

デバイス タイプの選択によって、[アウトバンド管理] の下に表示されるオプションが決まります。OOB デバイスの管理の概要の章のオペレーションを参照してください。

管理

HPCA コンソールの **[管理]** タブから [アウトバンド デバイスの詳細] に直接直接アクセスできるようになります。

このガイドのデバイス管理およびグループ管理の各章で説明している **[操作]** タブからの通常のアクセス方法のほかに、この方法が追加されます。

Client Automation Enterprise

CAE の **[管理]** タブから [アウトバンド デバイスの詳細] へアクセスするには多くの方法があります。

デバイスのプルダウン メニューを使用してデバイスを特定する

1 **[ディレクトリ]** の下で、**[ゾーン]** を展開して **[デバイス]** をクリックします。[ディレクトリ オブジェクト] ウィンドウが表示されます。

2 デバイス名の横にあるプルダウン メニューから、**[アウトバンド デバイスの詳細]** を選択します。デバイスが OOBM をサポートしている場合、[アウトバンド デバイスの詳細] ウィンドウが表示されます。サポートしていない場合は、エラー メッセージが表示されます。

アウトバンド デバイスの詳細アイコンを使用してデバイスを特定する

1 **[ディレクトリ]** の下で、**[ゾーン]** を展開して **[デバイス]** をクリックします。[ディレクトリ オブジェクト] ウィンドウが表示されます。

2 デバイス名のリンクをクリックします。情報セクションの上のツールバーに、 アウトバンド デバイス アイコンが表示されます。

3 デバイス テーブルでデバイスを選択して、 をクリックします。デバイスが OOBM をサポートしている場合、[アウトバンド デバイスの詳細] ウィンドウが表示されます。サポートしていない場合は、エラー メッセージが表示されます。

プロパティの表示 / 編集アイコンを使用してデバイスを特定する

1 **[ディレクトリ]** の下で、**[ゾーン]** を展開して **[デバイス]** をクリックします。[ディレクトリ オブジェクト] ウィンドウが表示されます。

2 デバイス名のリンクをクリックします。情報セクションの上のツールバーに、 プロパティの表示 / 編集アイコンが表示されます。

3 をクリックします。特定のデバイス用に開いた [ディレクトリ オブジェクト] ウィンドウに、 アウトバンド デバイス アイコンが表示されます。

4 をクリックします。デバイスが OOBM をサポートしている場合、[アウトバンド デバイスの詳細] ウィンドウが表示されます。サポートしていない場合は、エラー メッセージが表示されます。

グループからデバイスを特定する

1 **[ディレクトリ]** の下で、**[ゾーン]** を展開して **[グループ]** をクリックします。[ディレクトリ オブジェクト] ウィンドウが表示されます。

2 デバイスを含んでいる任意のグループを選択します。[ディレクトリ オブジェクト] ウィンドウが開き、選択したグループ内のデバイスが表示されます。

3 上で説明したデバイス特定手順、デバイスのプルダウン メニューを使用してデバイスを特定する、アウトバンド デバイスの詳細アイコンを使用してデバイスを特定する、プロパティの表示 / 編集アイコンを使用してデバイスを特定するのいずれかを使用して、[アウトバンド デバイスの詳細] ウィンドウにアクセスできます。

Client Automation Standard

CAS の **[管理]** タブから [アウトバンド デバイスの詳細] へアクセスするには多くの方法があります。

[デバイス管理] からアウトバンド デバイスの詳細アイコンを使用する

1 **[管理]** タブの左側のナビゲーション ペインから **[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

2 **[デバイス]** タブを選択します。デバイス テーブルのツールバーに、  アウトバンド デバイス アイコンが表示されます。

3 デバイス テーブルでデバイスを選択して、  をクリックします。デバイスが OOBM をサポートしている場合、[アウトバンド デバイスの詳細] ウィンドウが表示されます。サポートしていない場合は、エラー メッセージが表示されます。

[デバイス管理] からデバイス名のリンクを使用する

1 **[管理]** タブの左側のナビゲーション ペインから **[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

2 **[デバイス]** タブを選択します。

3 デバイス テーブルで、デバイス名のリンクをクリックします。[デバイスの詳細] ウィンドウが表示されます。

4 **[全般]** タブを選択します。

5 [タスク] の下で、**[アウトバンド]** をクリックします。デバイスが OOBM をサポートしている場合、[アウトバンド デバイスの詳細] ウィンドウが表示されます。サポートしていない場合は、エラー メッセージが表示されます。

[グループ管理] からアウトバンド デバイスの詳細アイコンを使用する

1 **[管理]** タブの左側のナビゲーション ペインから **[グループ管理]** をクリックします。[グループ管理] ウィンドウが表示されます。

2 **[グループ]** タブを選択します。

3 グループ テーブルでグループ名のリンクをクリックします。[グループの詳細] ウィンドウが表示されます。

4 **[デバイス]** タブを選択します。デバイス テーブルのツールバーに、  アウトバンド デバイスの詳細アイコンが表示されます。[デバイス管理] からアウトバンド デバイスの詳細アイコンを使用すると同じ手順を実行します。

[ソフトウェア管理] からアウトバンド デバイスの詳細アイコンを使用する

1 **[管理]** タブの左側のナビゲーション ペインから **[ソフトウェア管理]** をクリックします。[ソフトウェア管理] ウィンドウが表示されます。

2 全般的に [グループ管理] からアウトバンド デバイスの詳細アイコンを使用すると同じ手順に従います。手順 2 では **[ソフトウェア]** タブを選択します。

[パッチ管理] からアウトバンド デバイスの詳細アイコンを使用する

1 **[管理]** タブの左側のナビゲーション ペインから **[パッチ管理]** をクリックします。[パッチ管理] ウィンドウが表示されます。

2 全般的に [グループ管理] からアウトバンド デバイスの詳細アイコンを使用すると同じ手順に従います。手順 2 では **[パッチ]** タブを選択します。

[OS 管理] からアウトバンド デバイスの詳細アイコンを使用する

1 **[管理]** タブの左側のナビゲーション ペインから **[OS 管理]** をクリックします。[OS 管理] ウィンドウが表示されます。

2 全般的に [グループ管理] からアウトバンド デバイスの詳細アイコンを使用すると同じ手順に従います。手順 2 では **[オペレーティング システム]** タブを選択します。

デバイス タイプの選択

このオプションは、アウトバンド管理に対して管理対象のアウトバンド デバイスのタイプを通知します。選択したデバイス タイプに応じて、HPCA コンソールには、選択内容に関連するインターフェイスが表示されます。デバイス タイプは、DASH デバイス、vPro デバイス、または両方の 3 つの選択肢からいずれかを選択できます。

デバイス タイプを選択するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理]** の下で、**[デバイス タイプの選択]** をクリックします。[デバイス タイプの選択] ウィンドウが表示されます。

3 DASH デバイスを指定するには、**[DASH デバイスの管理]** をオンにします。DASH 管理者がすべてのデバイスに同じ認証情報を設定している場合は、DASH デバイスに共通の認証情報を指定できます。

   — **[すべての DASH デバイスに対して共通の認証情報を使用]** に対して **[はい]** を選択します。[DASH デバイスの認証情報] フィールドが表示されます。

   — DASH デバイスの **[ユーザー名]** と **[パスワード]** を入力します。

4 vPro デバイスを指定するには、**[vPro デバイスの管理]** をオンにします。[SCS のプロパティ] フィールドが表示されます。SCS ログイン認証情報、および SCS サービスの URL を入力する必要があります。

   — **[SCS サービスの URL]** を入力します (例 : http(s)://provisionserver.yourenterprise.com/amtscs)。

   — SCS 管理者の SCS **[ユーザー名]** と **[パスワード]** を入力します。

5 **[保存]** をクリックします。認証情報が保存されます。

   共通認証情報または SCS 認証情報を誤って入力した場合や、DASH または SCS の管理者がこれらの情報を変更した場合は、もう一度 [デバイス タイプの選択] ウィンドウへアクセスして、これらの情報を再入力できます。

6 HPCA コンソールをログアウトして再度ログインし、**[設定]** および **[操作]** タブに表示されているアウトバンド管理オプションに、選択したデバイス タイプが反映されていることを確認します。

vPro システム保護の設定

[デバイス タイプの選択] ウィンドウで vPro デバイスを管理するように選択した場合、HPCA コンソールへの再ログイン時に **[設定]** タブにこのオプションが表示されます。このオプションを選択すると、vPro デバイスのシステム保護設定の管理が可能になります。次の管理が可能です。

- システム防御フィルタの管理
- システム防御ポリシーの管理
- ヒューリスティック情報の管理
- エージェント ウォッチドッグの管理

システム防御フィルタの管理

HPCA コンソールを使用して、システム防御フィルタ リポジトリ内の vPro デバイスのシステム防御フィルタの表示、作成、更新、および削除が可能です。

システム防御フィルタは、システム防御ポリシーに割り当てられています。これらのフィルタは、対応するポリシーがアクティブ ポリシーになった場合にアクティブになります。

システム防御フィルタ リストのツールバー上のアイコンを使用してフィルタを管理できます。

表 7　　システム防御フィルタ リストのツールバー

アイコン	機能
	リストに表示されているシステム防御フィルタをリフレッシュします。
	リポジトリにシステム防御フィルタを追加します。
	リポジトリからシステム防御フィルタを削除します。

システム防御フィルタのビューをリフレッシュするには

1. HPCA コンソールにログインして、**[設定]** タブを選択します。
2. **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[フィルタ]** をクリックします。[フィルタ] ウィンドウが表示されます。[フィルタ] ウィンドウには、HPCA コンソールを使用して作成したシステム防御フィルタが表示されます。
3. ツールバーの  リフレッシュ アイコンをクリックします。

システム防御フィルタを追加するには

1. HPCA コンソールにログインして、**[設定]** タブを選択します。
2. **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[フィルタ]** をクリックします。[フィルタ] ウィンドウが表示されます。[フィルタ] ウィンドウには、HPCA コンソールを使用して作成したシステム防御フィルタが表示されます。
3. ツールバーの  追加アイコンをクリックします。ネットワーク フィルタ ウィザードが表示されます。
4. **[次へ]** をクリックして続行します。[フィルタの詳細] ウィンドウが表示されます。このウィンドウ内で次を指定します。

— **[フィルタ名]**: フィルタの名前を入力します。

— **[フィルタ タイプ]**: 作成するフィルタのタイプを選択します。各タイプについては、このページで説明されています。

— **毎秒パケット数**：このフィールドは、フィルタ タイプに [レート制限フィルタ] を選択した場合のみ有効になります。フィルタのパケット レートの限界値を入力します。毎秒単位のパケット レートを指定します。

— **フィルタの一致時にイベントを作成**：イベントを作成する場合は **[はい]** を選択します。イベントを作成すると、vPro ログにイベントが書き込まれます。また、Event Manager がイベント フィルタで検出したエントリに基づいてイベント警告が HPCA コンソールに送信されます。

5 **[次へ]** をクリックします。[パラメータ] ウィンドウが表示されます。このウィンドウ内で次を指定します。

— **[パケット タイプ]**: プルダウン メニューからパケットのタイプを選択します。[TCP パケット (IPv4)]、[UDP パケット (IPv4)]、[IP パケット (IPv4)]、または [Ethernet フレーム] から選択します。このフィールドで指定したパケットのタイプにより、フィルタが適用されるパケット ヘッダーが決定されます。

— **[次のプロトコル]**: このパラメータは IP パケットのフィルタリングのみに適用されるため、このフィールドは [パケット タイプ] フィールドで IP パケットを選択したときのみ表示されます。一つ上位のパケット プロトコルをプルダウン メニューから選択します。一つ上位のプロトコルは、TCP、UDP、および ICMP です。これらのプロトコルは、TCP/IP 抽象モデルのインターネット層内の上位レベルにあるプロトコルです。

— **[その他のプロトコル]**: このフィールドは、[パケット タイプ] フィールドで IP パケットを選択した場合のみに表示され、[次のプロトコル] で [その他] を選択した場合のみ有効になります。その他の IP プロトコルは、**http://www.iana.org/assignments/protocol-numbers** に記載されています。

— **[TCP フラグ]**: このパラメータは TCP パケットのフィルタリングのみに適用されるため、フラグのタイプは [パケット タイプ] フィールドで TCP パケットを選択したときのみ表示されます。必要なフラグ タイプをオンにします。必要なタイプはすべてオンにできます。これらのフラグはオプションです。フラグを指定しないで TCP フィルタを作成した場合、すべてのタイプの TCP パケットが一致します。

— **Ethernet フレーム タイプ**: このパラメータは Ethernet パケットのフィルタリングのみに適用されるため、このフィールドは [パケット タイプ] フィールドで Ethernet フレーム パケットを選択したときのみ表示されます。プルダウン メニューからフレームのタイプを選択します。[IPv4] または [IPv6] から選択します。

— **その他の Ethernet フレーム タイプ**：このフィールドは、[パケット タイプ] フィールドで Ethernet フレーム パケットを選択した場合のみに表示され、[Ethernet フレーム タイプ] フィールドで [その他] を選択した場合のみ有効になります。その他の Ethernet フレーム タイプを入力します。さまざまな Ethernet フレームのタイプが **http://www.iana.org/assignments/ethernet-numbers** に記載されています。

— **[フィルタ モードまたは方向]**: フィルタのモードを選択します。このオプションは、パケットが vPro デバイスによって受信される ([受信]) のか、vPro デバイスから送信される ([送信]) のかを指定します。

— **[ネットワーク アドレス]**: このパラメータは IP、TCP および UDP パケットのフィルタリングのみに適用されるため、このセクションは [パケット タイプ] フィールドで IP、TCP、または UDP パケットを選択したときのみ表示されます。次のいずれかのオプションを選択できます。

デバイスから送受信するパケットのフィルタリング」：このオプションは、単一のデバイスに対してパケットをフィルタリングできます。リモート デバイスの IP アドレスを入力します。フィルタ モードで [受信] を選択した場合、フィルタはこの IP アドレスから vPro デバイスに送信されるパケットに適用されます。フィルタ モードで [送信] を選択した場合、フィルタは vPro デバイスからこの IP アドレスに送信されるパケットに適用されます。

サブネットから送受信するパケットのフィルタリング：このオプションは、サブネット アドレス範囲のパケットをフィルタリングできます。IP アドレスとサブネット マスクを入力します。IP アドレスとサブネット マスクの組み合わせで、フィルタを適用するサブネット アドレス範囲を指定します。フィルタ モードで [受信] を選択した場合、フィルタはこのサブネット アドレス範囲のリモート デバイスから vPro デバイスに送信されるパケットに適用されます。フィルタ モードで [送信] を選択した場合、フィルタは vPro デバイスからこのサブネット アドレス範囲のリモート デバイスに送信されるパケットに適用されます。

ネットワークから送受信するパケットのフィルタリング ：このオプションは、ネットワーク全体に対してパケットをフィルタリングできます。フィルタ モードで [受信] を選択した場合、フィルタはすべてのリモート デバイスから vPro デバイスに送信されるパケットに適用されます。フィルタ モードで [送信] を選択した場合、フィルタは vPro デバイスからすべてのリモート デバイスに送信されるパケットに適用されます。

— **ポート タイプ**: この設定は TCP および UDP パケットのフィルタリングのみに適用されるため、このセクションは [パケット タイプ] フィールドで TCP、または UDP パケットを選択したときのみ表示されます。次のいずれかのオプションを選択できます。

ソース ポート範囲：このオプションでは、フィルタを適用するソース ポートの範囲 (最小および最大のポート値) を指定できます。このソース ポート範囲からすべての送信先ポートへ送信されるパケットにフィルタが適用されます。105 ページのポートの決定表を参照してください。

送信先ポート範囲：このオプションでは、フィルタを適用する送信先ポートの範囲 (最小および最大のポート値) を指定できます。すべてのポートからこの送信先ポート範囲へ送信されるパケットにフィルタが適用されます。105 ページのポートの決定表を参照してください。

表 8　　ポートの決定

		フィルタ モード	
		vPro デバイスから送信されるパケット	**vPro デバイスが受信するパケット**
IP ポートの方向	**送信元ポートの範囲**	vPro デバイス上のポートを参照します。vPro デバイス上のこのソース ポート範囲から送信先リモート デバイス上のすべてのポートに送信されるパケットがフィルタリングされま	リモート デバイス上のポートを参照します。送信元リモート デバイス上のこのソース ポート範囲から vPro デバイス上のすべてのポートに送信されるパケットがフィルタリングされま
	送信先ポート範囲	リモート デバイス上のポートを参照します。vPro デバイス上のすべてのポートから送信先リモート デバイス上のこのポート範囲に送信されるパケットがフィルタリングされます。	vPro デバイス上のポートを参照します。送信元リモート デバイス上のすべてのポートから vPro デバイス上のこの送信先ポート範囲に送信されるパケットがフィルタリングされます。

6　**[次へ]** をクリックします。確認メッセージが表示されます。

7　**[閉じる]** をクリックします。フィルタ リポジトリのシステム防御フィルタ テーブルに新しいフィルタが表示されます。

システム防御フィルタを更新するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[フィルタ]** をクリックします。[フィルタ] ウィンドウが表示されます。[フィルタ] ウィンドウには、HPCA コンソールを使用して作成したシステム防御フィルタが表示されます。

3 フィルタ テーブルの [フィルタ名] カラムで、変更するフィルタのフィルタ名のリンクをクリックします。ネットワーク フィルタ ウィザードが表示されます。

4 **[次へ]** をクリックして続行します。[フィルタの詳細] および [パラメータ] ページで、必要に応じてフィールドを編集します。

5 **[次へ]** をクリックします。確認メッセージが表示されます。

6 **[閉じる]** をクリックします。更新内容がフィルタ リポジトリに適用されます。

システム防御フィルタを削除するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[フィルタ]** をクリックします。[フィルタ] ウィンドウが表示されます。このウィンドウには、HPCA コンソールを使用して作成したシステム防御フィルタが表示されます。

3 フィルタ リポジトリから削除するすべてのフィルタの横にあるボックスをオンにします。

4 削除アイコンをクリックします。選択したフィルタが、フィルタ リポジトリのシステム防御フィルタ テーブルから削除されます。

システム防御フィルタのインターフェイスを使用して、次の作業を実行できます。

- ポリシーに適用可能な既存のフィルタ セットを表示する。
- ネットワークをウイルス感染から分離するフィルタを定義する。
- ネットワーク トラフィックを迂回させてさまざまな自己修復シナリオを実行するフィルタを定義する。
- 能動的にパケットを監視してシステム防御を行うフィルタを定義する。
- 今後必要とされないフィルタを削除する。

システム防御ポリシーの管理

HPCA コンソールを使用して、システム防御ポリシー リポジトリ内のシステム防御ポリシーの表示、作成、および削除が可能です。これらのポリシーは複数の vPro デバイスに配布することができます。ポリシーがアクティブ ポリシーになると、このポリシーに関連付けられているフィルタがアクティブになります。

システム防御ポリシー リストのツールバーにあるアイコンを使用してポリシーを管理できます。

表 9　　システム防御ポリシー リストのツールバー

アイコン	機能
	リストに表示されているシステム防御ポリシーをリフレッシュします。
	リポジトリにシステム防御ポリシーを追加します。
	システム防御ポリシーを vPro デバイスに配布します。

表 9　システム防御ポリシー リストのツールバー (cont'd)

アイコン	機能
	システム防御ポリシーを vPro デバイスから回収します。
	システム防御ポリシーおよびエージェント存在ポリシーを有線および無線インターフェイスに割り当てます。
	リポジトリからシステム防御ポリシーを削除します。

システム防御ポリシーのビューをリフレッシュするには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。[ポリシー] ウィンドウには、HPCA コンソールを使用して作成したシステム防御ポリシーが表示されます。

3 ツールバーの リフレッシュ アイコンをクリックします。

システム防御ポリシーを追加するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。[ポリシー] ウィンドウには、HPCA コンソールを使用して作成したシステム防御ポリシーが表示されます。

3 追加アイコンをクリックして、新しいポリシーを作成します。ネットワーク ポリシー ウィザードが表示されます。

4 **[次へ]** をクリックして続行します。このウィンドウ内で次を指定します。

- **[ポリシー名]**: ポリシーの名前を入力します。
- **[優先度]**: ポリシーの優先度を入力します。数字が大きいほど、優先度は高くなります。優先度は、システム防御ポリシーとエージェント存在ポリシーが両方とも有効である場合に、どちらのポリシーがアクティブになるかを決定するために使用されます。
- **アンチ スプーフィング フィルタの有効化 :** [はい] または [いいえ] を選択します。なりすまし防止には、送信フィルタを使用します。このフィルタが有効な場合、割り当てられた IP アドレスとは異なる送信元 IP アドレスを含む IP パケットを送信してホストが身元を偽ることを防止します。
- **[デフォルトの受信 (Rx) フィルタ タイプ]**: [パス] または [ドロップ] を選択します。デフォルト受信フィルタは、他のすべてのポリシー受信フィルタに一致しないすべての受信パケットを扱います。受信フィルタのタイプはパスまたはドロップのいずれかです。
- **[デフォルトの転送 (Tx) フィルタ タイプ]**: [パス] または [ドロップ] を選択します。デフォルト送信フィルタは、他のすべてのポリシー送信フィルタに一致しないすべての送信パケットを扱います。送信フィルタのタイプはパスまたはドロップのいずれかです。

5 **[次へ]** をクリックします。ウィザードの [フィルタ] ページが表示されます。

6 ポリシーと関連付けるフィルタを **[使用可能フィルタ]** リストから **[ポリシーに割り当てるフィルタ]** リストにドラッグします。

7 **[ポリシーの追加]** をクリックします。確認メッセージが表示されます。

8 **[閉じる]** をクリックします。ポリシー リポジトリのシステム防御ポリシー テーブルに新しいポリシーが表示されます。

システム防御ポリシーを更新するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。[ポリシー] ウィンドウには、HPCA コンソールを使用して作成したシステム防御ポリシーが表示されます。

3 ポリシー テーブルの [ポリシー名] カラムで、変更するポリシーのポリシー名のリンクをクリックします。ネットワーク ポリシー ウィザードが表示されます。

4 **[次へ]** をクリックします。必要に応じて各フィールドを編集します。

5 **[次へ]** をクリックして、現在ポリシーに関連付けられているフィルタを確認します。

6 リスト間でフィルタをドラッグ アンド ドロップして、選択したポリシーに対するフィルタの関連付けを変更します。

7 **[ポリシーの更新]** をクリックします。確認メッセージが表示されます。

8 **[閉じる]** をクリックします。更新内容がポリシー リポジトリに適用されます。

ポリシーが既に vPro デバイスに配布されている場合、更新されるのはリポジトリ内のポリシーのみで、デバイス上のポリシーは更新されません。

システム防御ポリシーを配布するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。[ポリシー] ウィンドウには、HPCA コンソールを使用して作成したシステム防御ポリシーが表示されます。

3 配布する各ポリシーの横にあるボックスをオンにします。

4 ツールバーの 配布アイコンをクリックします。ポリシー配布ウィザードが表示されます。

5 **[次へ]** をクリックして続行します。[デバイスの選択] ウィンドウが表示されます。

6 ポリシーを配布する各デバイスの横にあるボックスをオンにします。

7 **[次へ]** をクリックします。[ポリシーの設定] ウィンドウが表示されます。このウィンドウを使用して、選択したデバイス グループの有線および無線 NIC に割り当てるデフォルトのシステム防御ポリシーおよびエージェント存在ポリシーを選択できます。同じポリシーは、[システム防御] および [エージェント存在] の各フィールドの横にあるプルダウン メニューからも選択できます。デバイスに存在しない NIC (有線または無線) にポリシーを指定すると、[結果] ウィンドウに例外が表示されますが、これは配布プロセスには影響しません。

8 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

9 **[次へ]** をクリックして配布プロセスを続行します。[結果] ウィンドウが開いて、配布プロセスの結果が表示されます。

10 **[閉じる]** をクリックして、ウィザードを終了します。

システム防御ポリシーを回収するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。[ポリシー] ウィンドウには、HPCA コンソールを使用して作成したシステム防御ポリシーが表示されます。

3 回収する各ポリシーの横にあるボックスをオンにします。

4 ツールバーの  回収アイコンをクリックします。ポリシー回収ウィザードが表示されます。

5 **[次へ]** をクリックします。[デバイスの選択] ウィンドウが表示されます。

6 ポリシーを回収する各デバイスの横にあるボックスをオンにします。

7 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

8 **[次へ]** をクリックして回収プロセスを続行します。[結果] ウィンドウが開いて、回収プロセスの結果が表示されます。

9 **[閉じる]** をクリックして、ウィザードを終了します。

エージェント存在ポリシーを設定するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。[ポリシー] ウィンドウには、HPCA コンソールを使用して作成したシステム防御ポリシーが表示されます。

3 エージェント存在ポリシーとして設定するポリシーの横にあるボックスをオンにします。

4  ポリシー管理アイコン上のプルダウン メニューから、[エージェント存在ポリシーの設定 (有線 NIC)] を選択します。エージェント存在ポリシー設定ウィザードが表示されます。

5 **[次へ]** をクリックして続行します。[デバイスの選択] ウィンドウが表示されます。このウィンドウには、有線 NIC を装備した選択可能な vPro デバイスのみが表示されます。

6 選択したエージェント存在ポリシーを設定する各デバイスの横にあるボックスをオンにします。

7 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

8 **[次へ]** をクリックしてポリシー設定プロセスを続行します。[結果] ウィンドウが開いて、プロセスの結果が表示されます。

9 **[閉じる]** をクリックして、ウィザードを終了します。

10 無線 NIC にエージェント存在ポリシーを設定するには、ポリシーの設定アイコンのプルダウン メニューから [エージェント存在ポリシーの設定 (無線 NIC)] オプションを選択します。この場合、[デバイスの選択] ウィンドウには、無線 NIC を装備した選択可能な vPro デバイスのみが表示されます。有線 NIC の場合と同じ手順で、エージェント存在ポリシーを設定します。

システム防御ポリシーを有効化するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。[ポリシー] ウィンドウには、HPCA コンソールを使用して作成したシステム防御ポリシーが表示されます。

3 システム防御ポリシーとして有効化するポリシーの横にあるボックスをオンにします。

4  ポリシー管理アイコン上のプルダウン メニューから、[システム防御ポリシーの有効化 (有線 NIC)] を選択します。システム防御ポリシーの有効化ウィザードが表示されます。

5 **[次へ]** をクリックして続行します。[デバイスの選択] ウィンドウが表示されます。このウィンドウには、有線 NIC を装備した選択可能な vPro デバイスのみが表示されます。

6 選択したシステム防御ポリシーを有効化する各デバイスの横にあるボックスをオンにします。

7 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

8 **[次へ]** をクリックしてポリシーの有効化プロセスを続行します。[結果] ウィンドウが開いて、プロセスの結果が表示されます。

9 **[閉じる]** をクリックして、ウィザードを終了します。

10 無線 NIC に対してシステム防御ポリシーを有効化するには、ポリシーの設定アイコンのプルダウン メニューから [システム防御ポリシーの有効化 (無線 NIC)] オプションを選択します。この場合、[デバイスの選択] ウィンドウには、無線 NIC を装備した選択可能な vPro デバイスのみが表示されます。有線 NIC の場合と同じ手順で、システム防御ポリシーを有効化します。

システム防御ポリシーを削除するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ポリシー]** をクリックします。[ポリシー] ウィンドウが表示されます。[ポリシー] ウィンドウには、HPCA コンソールを使用して作成したシステム防御ポリシーが表示されます。

3 削除する各ポリシーの横にあるボックスをオンにします。

4 ツールバーの  削除アイコンをクリックします。このアクションによって選択したポリシーがリポジトリから削除され、また、すべてのプロビジョニング済みの vPro デバイスからこのポリシーが回収されるという警告メッセージが表示されます。

5 **[OK]** をクリックして続行します。ポリシーはリポジトリから削除され、システム防御ポリシーテーブルに内容が反映されます。また、プロビジョニング済みの vPro デバイスからも回収されます。

システム防御ポリシーのインターフェイスを使用して、次の作業を実行できます。

- 必要に応じて、新しいシステム防御ポリシーを定義する。
- ポリシーに関連付けられているフィルタの追加または削除を行い、より詳細にポリシーを微調整し、ネットワーク防御のニーズに適合させる。
- イベント警告またはログに基づいて、ポリシーを有効化してアクティブ ポリシーにする。
- なりすましフィルタを有効化して、割り当てられた IP アドレスとは異なる送信元 IP アドレスを含む IP パケットを送信してホストが身元を偽ることを防止する。
- 不要になったポリシーを削除する。
- 複数の vPro デバイスに対してポリシーを配布 (および回収) する。

ヒューリスティック情報の管理

HPCA コンソールを使用して、ヒューリスティック情報の表示、作成、削除、およびそれへのアクションの追加が可能です。これらのヒューリスティックは複数の vPro デバイスに配布できます。

ヒューリスティック リストのツールバーにあるアイコンを使用してヒューリスティック仕様を管理できます。

表 10　　ヒューリスティック リスト ツールバー

アイコン	機能
	リストに表示されているヒューリスティックをリフレッシュします。
	リポジトリにヒューリスティック情報を追加します。
	選択された vPro デバイスへヒューリスティック情報を配布します。
	選択された vPro デバイスからヒューリスティック情報を回収します。
	リポジトリからヒューリスティック情報を削除します。

ヒューリスティック ビューをリフレッシュするには

1　HPCA コンソールにログインして、**[設定]** タブを選択します。

2　**[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ヒューリスティック]** をクリックします。[ヒューリスティック] ウィンドウが表示されます。このウィンドウには、HPCA コンソールを使用して作成したヒューリスティックが表示されます。

3　ツールバーの  リフレッシュ アイコンをクリックします。

ヒューリスティックを追加するには

1　HPCA コンソールにログインして、**[設定]** タブを選択します。

2　**[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ヒューリスティック]** をクリックします。[ヒューリスティック] ウィンドウが表示されます。このウィンドウには、HPCA コンソールを使用して作成したヒューリスティックが表示されます。

3　  追加アイコンをクリックして、新しいヒューリスティック情報を作成します。ヒューリスティック ウィザードが表示されます。

4　**[次へ]** をクリックして続行します。[ヒューリスティックの詳細] ウィンドウが表示されます。このウィンドウ内で次を指定します。

- **設定タイプ :** 高速パケットの総数、高速期間の総数、低速パケットの総数、および低速期間の総数の各パラメータのデフォルト値を使用する場合は、[デフォルト] を選択します。これらの値は Intel の推奨値です。これらの値を変更する場合は、[カスタム] を選択します。これらの値を変更すると、深刻なネットワーク問題につながる恐れがある点に注意してください。
- **パラメータ**
  - **名前 :** ヒューリスティック仕様に一意の名前を入力します。
  - **[高速パケットの総数]:** デフォルトの設定タイプを選択しなかった場合、高速ワーム侵入のしきい値を入力します。しきい値 (パケット数) は、限界値を表します。カウンタがこの値を超過する場合、異常イベントであることを示します。設定可能なしきい値の範囲は 8 ～ 64 です。デフォルト値の 8 が推奨されます。
  - **高速タイム カウント** : デフォルトの設定タイプを選択しなかった場合、高速ワーム侵入の時間枠サイズ値を入力します。時間枠サイズ (時間数) は、ヒューリスティックがそのカウンタをリセットする期間です。設定可能な時間枠の範囲は 10 ミリ秒～ 1 秒 (1000 ミリ秒) です。デフォルト値の 10 ミリ秒が推奨されます。

— **[低速パケットの総数]**: デフォルトの設定タイプを選択しなかった場合、低速ワーム侵入のしきい値を入力します。しきい値 (パケット数) は、限界値を表します。カウンタがこの値を超過する場合、異常イベントであることを示します。設定可能なしきい値の範囲は 8 ～ 64 です。デフォルト値の 64 が推奨されます。

— **低速タイム カウント** : デフォルトの設定タイプを選択しなかった場合、低速ワーム侵入の時間枠サイズ値を入力します。時間枠サイズ (時間数) は、ヒューリスティックがそのカウンタをリセットする期間です。設定可能な時間枠の範囲は 1 秒 (1000 ミリ秒) ～ 50 秒 (50000 ミリ秒) です。デフォルト値の 50 秒が推奨されます。

— **[タイムアウト発生]**: 異常イベントの発生後に封じ込めアクションを vPro デバイスに適用する期間を指定する値を入力します。20 以上の値が推奨されます。封じ込めアクションを永久に適用する場合は、値 0 を入力します。

詳細は、81 ページの「ウィンドウ サイズとしきい値」および 82 ページの「封じ込めアクションとタイムアウト値」を参照してください。

- **アクション**

— **TX トラフィックのブロック** : プルダウン リストから、**[すべての TX トラフィック]** または **[攻撃ポートのみ]** を選択します。多くの場合、後者のオプション (ポート トラフィックのみ) が推奨されます。

- **ポリシー**

— **[ポリシー名]**: ヒューリスティックの条件が一致した場合にシステム防御フィルタを有効化するには、プルダウン リストからポリシー名を選択します。ポリシーを選択すると、**[ポリシー情報の表示]** リンクが表示されます。このリンクをクリックすると、ポリシーの詳細を確認できます。ポリシーの詳細を表示するウィンドウを閉じるには、**[閉じる]** をクリックします。

5 **[次へ]** をクリックします。操作のステータスが表示されます。

6 **[閉じる]** をクリックして、ウィザードを終了します。ヒューリスティック テーブルに新しいヒューリスティック情報が表示されます。この情報はリポジトリに追加されます。

ヒューリスティックを更新するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理]** > **[vPro システム保護の設定]** の下で、**[ヒューリスティック]** をクリックします。[ヒューリスティック] ウィンドウが表示されます。このウィンドウには、HPCA コンソールを使用して作成したヒューリスティックが表示されます。

3 ヒューリスティック テーブルの [ヒューリスティック名] カラムで、変更するヒューリスティック仕様のヒューリスティック名のリンクをクリックします。ヒューリスティック ウィザードが表示されます。

4 **[次へ]** をクリックして続行します。[ヒューリスティックの詳細] ウィンドウが表示されます。必要に応じて各フィールドを編集します。名前フィールド以外のすべてのフィールドを編集できます。

5 **[次へ]** をクリックします。操作のステータスが表示されます。

6 **[閉じる]** をクリックして、ウィザードを終了します。更新内容がヒューリスティック テーブルに表示され、リポジトリに適用されます。

ヒューリスティック情報が既に vPro デバイスに配布されている場合、更新されるのはリポジトリ内のヒューリスティックのみで、デバイス上のヒューリスティックは更新されません。

エージェント ヒューリスティックを配布するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ヒューリスティック]** をクリックします。[ヒューリスティック] ウィンドウが表示されます。このウィンドウには、HPCA コンソールを使用して作成したヒューリスティックが表示されます。

3 配布する各ヒューリスティックの横にあるボックスをオンにします。

4 ツールバーの  ヒューリスティック配布アイコンをクリックします。ヒューリスティックウィザードが表示されます。

5 **[次へ]** をクリックして続行します。[デバイスの選択] ウィンドウが表示されます。

6 ヒューリスティック情報の配布先の各デバイスの横にあるボックスをオンにします。

7 **[次へ]** をクリックします。[ヒューリスティック設定] ウィンドウが表示されます。

8 選択したデバイスの有線ネットワーク インターフェイスおよび無線ネットワーク インターフェイスに適用するヒューリスティックを選択します。両方のインターフェイスに同じヒューリスティック情報を設定できます。デバイスに存在しない NIC (有線または無線) にヒューリスティック情報を指定すると、[結果] ウィンドウに例外が表示されますが、配布プロセスには影響しません。

9 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

10 **[次へ]** をクリックして配布プロセスを続行します。[結果] ウィンドウに操作結果が表示されます。

11 **[閉じる]** をクリックして、ウィザードを終了します。

ヒューリスティックを回収するには

1 HPCA コンソールにログインし、[設定] タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ヒューリスティック]** をクリックします。[ヒューリスティック] ウィンドウが表示されます。このウィンドウには、HPCA コンソールを使用して作成したヒューリスティックが表示されます。

3 回収する各ヒューリスティックの横にあるボックスをオンにします。

4 ツールバーの  ヒューリスティック回収アイコンをクリックします。ヒューリスティック回収ウィザードが表示されます。

5 **[次へ]** をクリックします。[デバイスの選択] ウィンドウが表示されます。

6 ヒューリスティックを回収する各デバイスの横にあるボックスをオンにします。

7 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

8 **[次へ]** をクリックして回収プロセスを続行します。[結果] ウィンドウが開いて、回収プロセスの結果が表示されます。

9 **[閉じる]** をクリックして、ウィザードを終了します。

ヒューリスティックを削除するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で、**[ヒューリスティック]** をクリックします。[ヒューリスティック] ウィンドウが表示されます。このウィンドウには、HPCA コンソールを使用して作成したヒューリスティックが表示されます。

3 削除する各ヒューリスティックの横にあるボックスをオンにします。

4 ツールバーの  削除アイコンをクリックします。このアクションにより選択したヒューリスティックがリポジトリから削除され、また、すべてのプロビジョニング済みの vPro デバイスから回収されるという警告が表示されます。

5 **[OK]** をクリックして続行します。ヒューリスティックはリポジトリから削除されてヒューリスティック テーブルに反映され、プロビジョニング済み vPro デバイスから回収されます。

ヒューリスティック インターフェイスを使用して次の作業が実行できます。

- 時間枠のサイズ (タイム数) およびしきい値 (パケット数) を設定し、ワームが vPro デバイスに侵入したかどうかをヒューリスティックに判断する。
- ヒューリスティックの条件が適合した場合に実行してワームを封じ込めるアクションを指定する。
- 不要になったヒューリスティック情報を削除する。
- 複数の vPro デバイスに対してヒューリスティックを配布 (および回収) する。

エージェント ウォッチドッグの管理

HPCA コンソールを使用し、ウォッチドッグ リポジトリのエージェント ウォッチドッグの表示、作成、更新、削除、およびそれへのアクションの追加が可能です。このウォッチドッグは、複数の vPro デバイスに配布できます。エージェント存在ポリシーがアクティブになった場合にコンソールに表示されるようにカスタマイズしたシステム メッセージ、およびローカル エージェントで監視するアプリケーションのソフトウェア リストを作成することもできます。

ウォッチドッグ リストのツールバーのアイコンにより、ウォッチドッグを管理できます。

表 11　　ウォッチドッグ リスト ツールバー

アイコン	機能
	リストに表示されているウォッチドッグをリフレッシュします。
	リポジトリにウォッチドッグを追加します。
	選択したウォッチドッグを vPro デバイスに配布します。
	選択したウォッチドッグを vPro デバイスから回収します。
	リポジトリからウォッチドッグを削除します。
	ローカル エージェント システム メッセージおよびソフトウェア リストを設定します。
	ローカル エージェント システム メッセージおよびソフトウェア リストを配布します。

エージェント存在の表示をリフレッシュするには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で **[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。このウィンドウには、HPCA コンソールで作成されたウォッチドッグが表示されます。

3 ツールバーの  リフレッシュ アイコンをクリックします。

エージェント ウォッチドッグを追加するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で **[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。このウィンドウには、HPCA コンソールで作成されたウォッチドッグが表示されます。

3 エージェント ウォッチドッグを作成するには、  追加アイコンをクリックします。エージェント ウォッチドッグ ウィザードが表示されます。

4 **[次へ]** をクリックして続行します。このウィンドウ内で次を指定します。

- **[エージェント タイプ]**: HP ローカル エージェントまたはサード パーティ製ベンダー エージェントを選択し、vPro デバイスにインストールしてあるエージェントを指定します。デフォルトでは、HP ローカル エージェントが選択されています。
- **[名前]**: エージェント ウォッチドッグの一意の名前を入力します。
- **[エージェント GUID]**: サード パーティ製ベンダー エージェントの GUID を入力します。HP ローカル エージェントの GUID はわかっているため、HP ローカル エージェントを選択した場合、このフィールドはグレー表示になります。
- **[ハート ビート間隔]**: ローカル エージェントからエージェント ウォッチドッグへのハートビート間隔の時間を入力します。デフォルト値が指定されています。
- **[起動後から最初のハート ビートまでの時間]**: システムの起動後、エージェントが最初のハートビートをエージェント ウォッチドッグに送信する時間を入力します。デフォルト値が指定されています。

5 **[次へ]** をクリックします。ウィザードの [ウォッチドッグ アクション] ページが表示されます。このウィンドウ内で次を指定します。

- **[遷移状態]**:

  [初期状態]: アクションを起動するローカル エージェントの初期状態を選択します。

  [最終状態]: アクションを起動するローカル エージェントの最終状態を選択します。

- **[アクション]**:

  [エージェント存在ポリシー] では [有効] または [無効] を選択し、ローカル エージェントが指定した状態から移行した場合、およびその状態に移行した場合に、エージェント存在ポリシーを有効にするか無効にするかを指定します。ポリシーが有効である場合は、有効になっているシステム防御ポリシーより優先度が高いと、そのポリシーがアクティブ ポリシーになります。

  [イベント作成] では [有効] または [無効] を選択し、指定したローカル エージェントの移行が発生した場合にイベントを作成するかどうかを指定します。イベント作成が有効である場合、イベントはデバイスの vPro ログに記録され、イベント フィルタ処理および警告メッセージ予約に応じてイベント警告が HPCA コンソールに送信されます。

6 **[アクションの追加]** をクリックします。ウィンドウ下部のアクション テーブルにアクションが追加されます。アクションは、さまざまな有効な移行状態によって定義されるため、いくつでもウォッチドッグに追加できます。

7 **[保存]** をクリックします。確認メッセージが画面に表示されます。

8 **[閉じる]** をクリックして、ウィザードを終了します。新しいエージェント ウォッチドッグが、適切に設定されているアクションの数とともにエージェント ウォッチドッグ テーブルに表示されます。ウォッチドッグおよびアクションがリポジトリに適用されます。

エージェント ウォッチドッグを更新するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で **[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。このウィンドウには、HPCA コンソールで作成されたウォッチドッグが表示されます。

3 エージェント ウォッチドッグ テーブルの [ウォッチドッグ名] カラムで、変更するウォッチドッグのエージェント ウォッチドッグ名のリンクをクリックします。エージェント ウォッチドッグ ウィザードが表示されます。

4 **[次へ]** をクリックして続行します。必要に応じて各フィールドを編集します。

5 **[次へ]** をクリックします。ウィザードの [ウォッチドッグ アクション] ページが表示されます。このウィンドウでは、アクションを新たに追加したり、既存のアクションを削除したりすることができます。

— 114 ページの「エージェント ウォッチドッグを追加するには」の手順 5 に従い、アクションを追加します。

— ウィンドウ下部で削除する各ウォッチドッグ アクションの横にあるボックスをオンにして、削除アイコンをクリックし、アクションを削除します。

6 **[保存]** をクリックします。確認メッセージが画面に表示されます。

7 **[閉じる]** をクリックして、ウィザードを終了します。更新内容がウォッチドッグ テーブルに表示され、ウォッチドッグ リポジトリに適用されます。

ウォッチドッグが既に vPro デバイスに配布されている場合、更新されるのはリポジトリ内のウォッチドッグのみで、デバイス上のウォッチドッグは更新されません。

エージェント ウォッチドッグを配布するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で **[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。このウィンドウには、HPCA コンソールで作成されたウォッチドッグが表示されます。

3 配布する各ウォッチドッグの横にあるボックスをオンにします。HP の ローカル エージェント ウォッチドッグは 1 つしか配布できません。サード パーティ製のエージェント ウォッチドッグは複数配布できます。vPro デバイス上で動作しているサード パーティ製の各ローカル エージェントに対し、サード パーティ製エージェント ウォッチドッグを 1 つ配布できます。

4 ツールバーの エージェント ウォッチドッグ配布アイコンをクリックします。ウォッチドッグ配布ウィザードが表示されます。

5 **[次へ]** をクリックして続行します。[デバイスの選択] ウィンドウが表示されます。

6 ウォッチドッグを配布する各デバイスの横にあるボックスをオンにします。

7 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

8 **[次へ]** をクリックして配布プロセスを続行します。[結果] ウィンドウに操作結果が表示されます。

9 **[閉じる]** をクリックして、ウィザードを終了します。

エージェント ウォッチドッグを回収するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で **[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。このウィンドウには、HPCA コンソールで作成されたウォッチドッグが表示されます。

3 回収する各エージェント ウォッチドッグの横にあるボックスをオンにします。

4 ツールバーの エージェント ウォッチドッグ回収アイコンをクリックします。ウォッチドッグ回収ウィザードが表示されます。

5 **[次へ]** をクリックします。[デバイスの選択] ウィンドウが表示されます。

6 ウォッチドッグを回収する各デバイスの横にあるボックスをオンにします。

7 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

8 **[次へ]** をクリックして回収プロセスを続行します。[結果] ウィンドウが開いて、回収プロセスの結果が表示されます。

9 **[閉じる]** をクリックして、ウィザードを終了します。

エージェント ウォッチドッグ削除するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で **[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。このウィンドウには、HPCA コンソールで作成されたウォッチドッグが表示されます。

3 削除する各ウォッチドッグの横にあるボックスをオンにします。

4 ツールバーの  削除アイコンをクリックします。このアクションによって、選択したウォッチドッグがリポジトリから削除され、また、すべてのプロビジョニング済みの vPro デバイスからこのウォッチドッグが回収されるという警告メッセージが表示されます。

5 **[OK]** をクリックして続行します。ウォッチドッグはリポジトリから削除され、エージェント ウォッチドッグ テーブルに内容が反映されます。また、プロビジョニング済みの vPro デバイスからも回収されます。

システム メッセージおよびソフトウェア リストを設定するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で **[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。このウィンドウには、HPCA コンソールで作成されたウォッチドッグが表示されます。

3  ローカル エージェント設定アイコンをクリックします。[ソフトウェア リスト] ダイアログが表示されます。

4 **[システム メッセージ]** テキスト ボックスに、エージェント存在ポリシーがアクティブ化されたときに vPro デバイス上のコンソールに表示するシステム メッセージを入力します。デフォルトのメッセージが既に入力されており、これを編集できます。

5 **[ソフトウェア名]** ボックスに、ローカル エージェントに監視させる、vPro デバイスで動作しているセキュリティ アプリケーションの名前を入力します。例えば、**symantec.exe** と入力します。

拡張子が .exe のアプリケーションのみを監視できます。この製品では、その他のタイプの実行ファイルの監視はサポートされていません。

6 **[追加]** をクリックします。このプロセスを繰り返して、ローカル エージェントに監視させるソフトウェア アプリケーションのリストを作成できます。

7 **[保存]** をクリックします。情報メッセージが画面に表示されます。

8 **[閉じる]** をクリックして、ダイアログを終了します。システム メッセージおよびエージェント ソフトウェア リストは XML リポジトリに格納されます。

システム メッセージとソフトウェア リストを配布するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理] > [vPro システム保護の設定]** の下で **[ウォッチドッグ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。このウィンドウには、HPCA コンソールで作成されたウォッチドッグが表示されます。

3 ツールバーの  ソフトウェア リストとシステム メッセージの配布アイコンをクリックします。これで、ソフトウェア配布ウィザード開始されます。

4 **[次へ]** をクリックします。[ソフトウェア タイトル] ウィンドウが表示されます。

5 ローカル エージェントに監視させるソフトウェア アプリケーションを選択します。

6 **[次へ]** をクリックします。[デバイス] ウィンドウが表示されます。

7 リストとメッセージを配布するデバイスを選択します。

8 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

9 **[次へ]** をクリックして続行します。[結果] ウィンドウに操作結果が表示されます。

10 **[閉じる]** をクリックして、ウィザードを終了します。システム メッセージとアプリケーション ソフトウェア リストは、ターゲットの vPro デバイスのサード パーティ データ ストア (3PDS) に書き込まれます。特定の vPro デバイス用のこの情報を表示するには、[デバイス管理] ウィンドウ内のデバイスのホスト名をクリックして、次に、**[診断]** セクションの下で、**[デバイス アセット] > [ソフトウェア情報] > [登録済みアプリケーション] > [HPCA] > [HPCABlock]** の順に移動します。

アプリケーション ソフトウェア リストは、vPro デバイス上の 3PDS に書き込まれます。ローカル エージェントはこの 3PDS からリストを読み取るため、変更したリストを再配布する場合は、このデバイス上のローカル エージェントを停止し再起動する必要があります。

エージェント ウォッチドッグ インターフェイスを使用して、次の操作を実行できます。

- ウォッチドッグ エージェントを定義して、vPro デバイス上のローカル エージェントを監視する。
- ウォッチドッグによって監視されているローカル エージェントのハートビート送信間隔とスタートアップ間隔を設定する。
- 不要になったエージェント ウォッチドッグを削除する。
- 複数の vPro デバイスに対してエージェント ウォッチドッグの配布および回収を行う。
- エージェント存在ポリシーがアクティブ化されている場合、vPro デバイスのコンソールに表示されるシステム メッセージをカスタマイズおよび配布する。また、ターゲット vPro デバイス上でローカル エージェントに監視させるアプリケーションのリストの選択元となるソフトウェア アプリケーションのマスター リストをカスタマイズおよび配布する。

7 vPro デバイスのプロビジョニング

この章では、vPro デバイスのプロビジョニングの概要、および vPro デバイスの遅延リモート設定について説明します。

概要

HPCA コンソールから、最初の Setup and Configuration Service (SCS) プロビジョニング プロセス中にプロビジョニングされなかった vPro デバイスをプロビジョニングできます。最初のプロビジョニング プロセスについては、17 ページの「SCS および vPro のセットアップ」で説明しています。このプロセスは、ベア メタル リモート設定と呼ばれます。

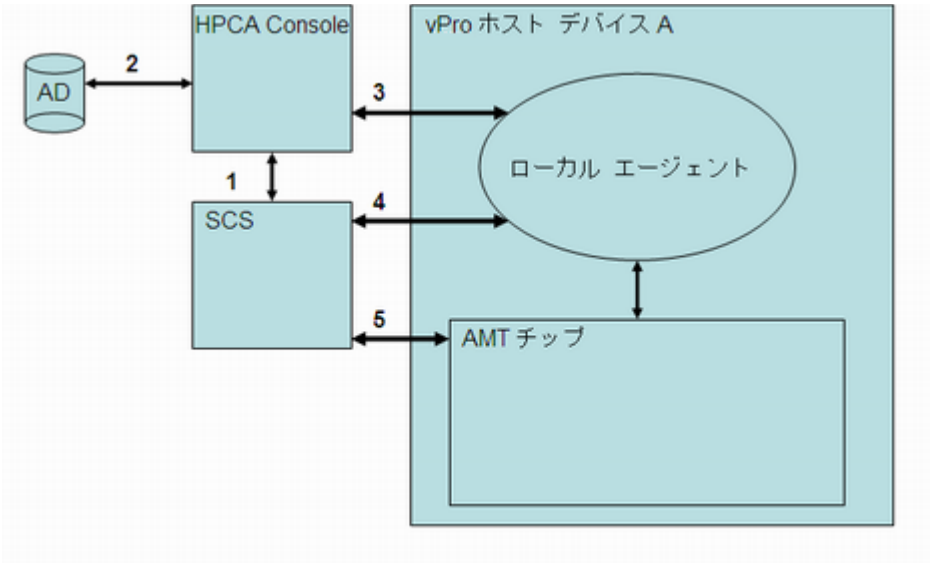
HPCA コンソールから実行されるタイプのプロビジョニングは、遅延リモート設定プロビジョニングと呼ばれます。セットアップを有効にするデバイスごとに PID と PPS のペアを手動でインストールする必要がなく、Provisioning Server のアドレスやドメイン名などに関する情報を入力する必要がないため、これはリモート設定であるとみなされます。このプロビジョニングは自動的に管理コンソールからリモートに実行されます。デバイスがネットワークに初めて接続されたときにそのデバイスに許可された時間内にプロビジョニングされないため、これは遅延設定とみなされます。

リモート設定を使用するには、SCS および vPro のセットアップの章の 38 ページの「リモート設定による vPro デバイスの設定」で説明するすべての要件を満たす必要があります。

vPro デバイスがプロビジョニングされていないかプロビジョニング中の状態である場合に限り、リモート設定を使用して vPro デバイスをプロビジョニングできます。すでにプロビジョニングされている vPro デバイスは、リモート設定を使用して再びプロビジョニングすることはできません。vPro デバイスの再プロビジョニングは手動で行ってください。

vPro デバイスのプロビジョニングに必要な情報を取得するため、HPCA コンソールでは、vPro デバイス、SCS Server、Active Directory で動作しているローカル エージェントと通信します。

図 14　　HPCA コンソールからの遅延リモート設定



次のような通信が交わされます。

1. HPCA コンソールは SCS と通信し、すでにプロビジョニング済みのデバイスおよび現在プロビジョニング中のデバイスのリストを取得します。
2. HPCA コンソールは Active Directory (AD) と通信し、その特定ドメインのデバイスのリストを取得します。管理コンソールは、すべてのデバイスおよびそれぞれのプロビジョニング状態をリストします。
3. HPCA　コンソールは、デフォルトのポートでローカル　エージェントとの通信を試します。エージェントがインストールされている場合は、プロビジョニングされていない状態のデバイスが HPCA コンソールに表示されます。HPCA コンソールは、ローカル エージェントとの通信が確立されると、遅延設定プロセスの開始をローカル エージェントに要求します。
4. デバイスがプロビジョニングされていないかプロビジョニング中の状態である場合、ローカル エージェントは SCS と接続し、デバイスの FQDN、UUID、プロファイル ID を保存しようとします。このとき hello パケットが生成されます。
5. SCS が PKI-CH プロトコルを使用して vPro デバイスをプロビジョニングします。

このプロセスの詳細については、vPro デバイスの遅延リモート設定を参照してください。

vPro デバイスの遅延リモート設定

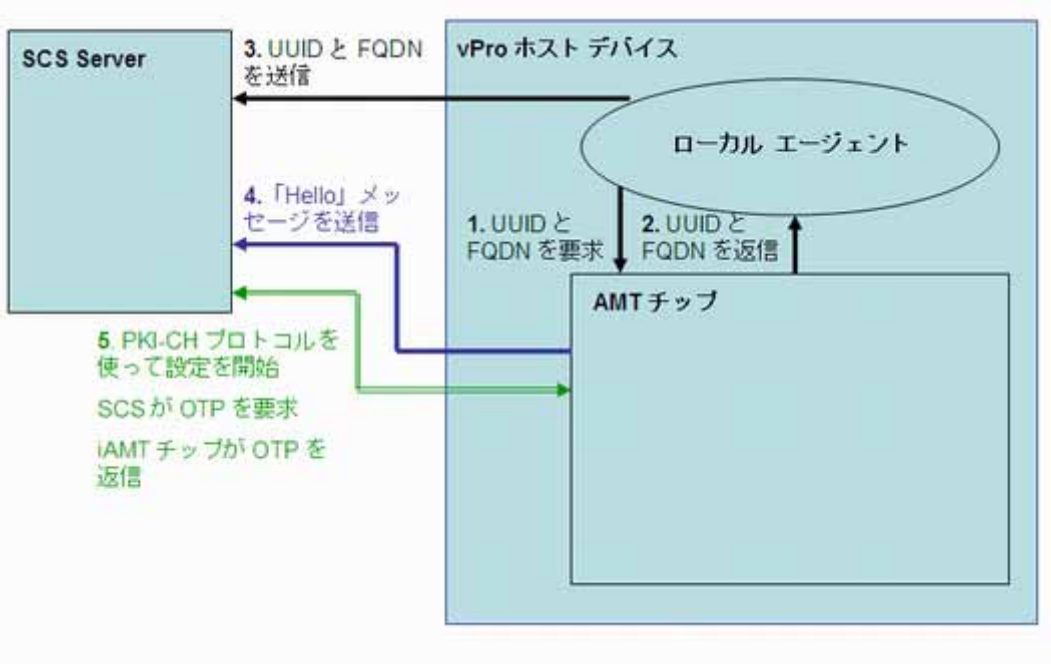
このセクションは、次のトピックで構成されています。

セットアップ モードへの移行

次の図は、リモート設定にローカル エージェントを使用している場合の、vPro デバイスのセットアップ モードへの移行に関連する手順を示しています。デバイスがネットワークへの接続時にすぐにプロビジョニングされていないため、これは遅延設定と呼ばれます。これに代わる (即時の) 設定については、41 ページの「vPro デバイスのベア メタル リモート設定」を参照してください。

vPro デバイスがセットアップ モードに移行した後で、プロビジョニングの準備ができたことを示す「Hello」メッセージが SCS Server に送信されます。

図 15　　遅延設定でのセットアップモードへの移行



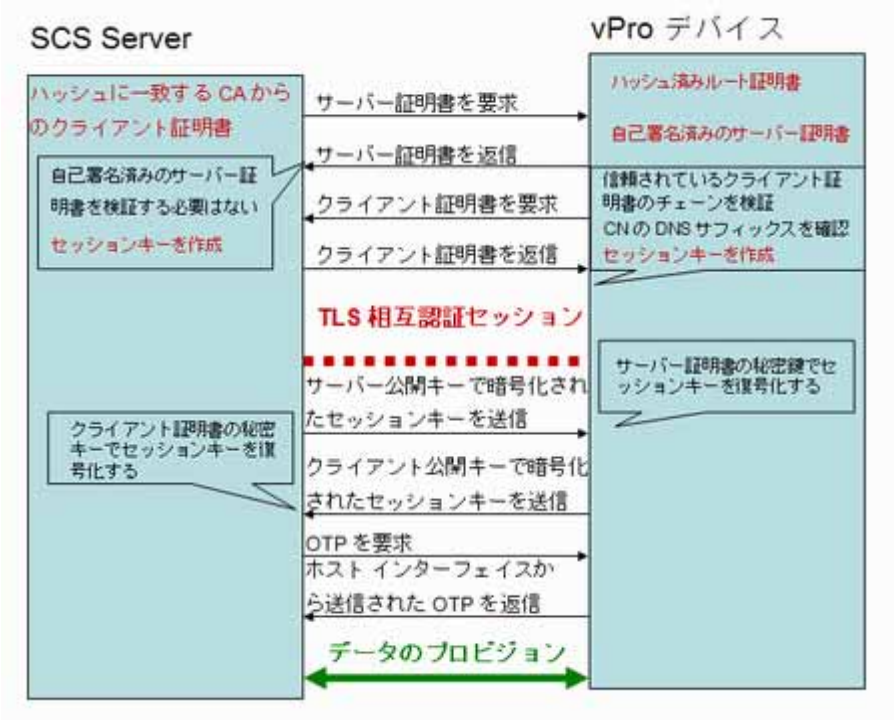
ローカル エージェントは、vPro ホスト デバイスにインストールされている必要があります。ローカル エージェントでは vPro デバイスが検出され、次のことが行われます。

1. ローカル エージェントが、vPro デバイスに UUID および FQDN を要求します。
2. vPro デバイスはその値をローカル エージェントに返します。
3. ローカル エージェントがその値を SCS Server に送信します。
4. vPro デバイスが SCS Server に「Hello」メッセージの送信を開始します。
5. SCS Server が PKI-CH プロトコルを使用してプロビジョニング プロセスを始めます。SCS Server と vPro デバイスの間で OTP が交換されます。

リモート設定プロビジョニング プロセス

リモート設定プロビジョニング プロセス中は、TLS 相互認証が使用されてセキュアなチャネルが作成されます。次の図はプロビジョニング プロセスの流れを示しています。

図 16　　リモート設定プロビジョニング プロセス



プロビジョニング プロセスは次の手順で実行されます。

1. vPro デバイスが設定プロセスを開始することをローカル エージェントが要求します。デバイスは、限られた時間 (Intel マシンの場合は 24 時間、HP デスクトップの場合は 255 時間) だけネットワーク インターフェイスを開き、「Hello」メッセージの送信を始めます。インターフェイスは、有効になった初回のみ、指定された時間 (設定可能) 開きます。セットアップと設定が完了する前に指定した時間が経過した場合、ローカル エージェントからの設定を開始するための呼び出しにより、6 時間に限り、インターフェイスが開きます。
2. SCS Server が次のことを行います。
   - ルート証明書ハッシュを「Hello」メッセージから抽出し、どのクライアント証明書を vPro デバイスの検証のために送信するかを認識します。
   - 受信したハッシュのものと一致する、信頼できるルート証明書を含む証明書チェーンを送信します。
3. vPro デバイスは次のことを行います。
   - SCS クライアント証明書を検証します。40 ページの「リモート設定の証明書の取得と設定」で説明しているように、OID または OU が正しく、ルート証明書ハッシュのものと一致する CA から証明書が派生していることを確認します。
   - ドメイン サフィックスが SCS 証明書の DNS サフィックスと一致することを確認します。
4. SCS Server と vPro デバイスが、完全な相互認証セッション キー交換を実行します。
   - vPro デバイスは自己署名証明書を使用し、公開キーを送信します。
   - SCS は TLS セッション キーを作成し、vPro デバイス公開キーで暗号化して vPro デバイスに送信します。

— vPro デバイスは秘密キーでセッション キーを復号化し、別のセッション キーを作成して、SCS Server が検証用に送信したクライアント公開キーで暗号化します。セットアップと設定の TLS セッション中は、トラフィックの対称暗号化にこのセッション キー ペアが使用されます。

5 SCS Server と vPro デバイスの間でワンタイム パスワード (OTP) 検証が行われます。SCS Server は vPro デバイスから OTP を要求します。デバイスは OTP を安全に送信し、SCS Server はそれが正しいかどうかを調べます。

6 デバイスがプロビジョニングされるまで、セットアップと設定プロセスが続きます。vPro デバイスのネットワーク インターフェイスは最初の「Hello」メッセージの送信後、限られた時間しか開かないため、SCS Server はこの時間を最長 24 時間まで延長することを vPro デバイスに指定して設定プロセスを完了させることができます。

プロビジョニング タスクの実行

HPCA コンソールの **[操作]** タブのアウトバンド管理オプションの中に、**[vPro プロビジョニング]** があります。

このオプションは、vPro デバイスの管理を選択した場合のみ HPCA コンソールに表示されます。

このオプションにより、vPro デバイスでいくつかのプロビジョニング タスクを実行できます。これらのタスクには、プロビジョニング、再プロビジョニング、部分的プロビジョニング解除、完全プロビジョニング解除が含まれます。ネットワークの管理中には、特定の vPro デバイスの再プロビジョニングやプロビジョニング解除をする必要が生じる場合があります。この作業を行うのには、次のような理由があります。

- 再プロビジョニング : vPro デバイスを完全に再プロビジョニングします。vPro デバイスで複数のパラメータが変った場合に、このオプションを使用します。
- 部分的プロビジョニング解除 : PID および PPS のみを vPro デバイスから削除します。Provisioning Server の情報 (IP アドレスとホスト名) は変えずに、キーのみを変更する必要がある場合にこのオプションを使用します。
- 完全プロビジョニング解除 : すべてのプロビジョニング情報を vPro デバイスから削除します。Provisioning Server の IP アドレスと名前が変った場合にこのオプションを使用します。このオプションにより、すべてをクリアして新しいプロビジョニングを進めることができます。

いずれかのプロビジョニング タスクを実行するには、最初に次のことを行う必要があります。

- ローカル エージェントを vPro デバイスにまだインストールしていない場合はインストールします。42 ページの「OOBM ローカル エージェントのインストール」を参照してください。
- ネットワーク セキュリティ ポリシーの一部としてセキュリティを強化する必要がある場合は、SCS セットアップに戻ってワンタイム パスワード (OTP) を有効にします。34 ページの「プロファイルを設定するには」を参照してください。

vPro デバイスをプロビジョニングするには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 **[アウトバンド管理]** の下で、**[vPro プロビジョニング]** をクリックします。[vPro プロビジョニング] ウィンドウが表示されます。

3 デバイス テーブルにデバイスが表示されない場合は、ツールバーの  探索アイコンをクリックします。[vPro 探索] ウィンドウが表示されます。

4 Active Directory (AD) のログイン認証情報および AD Server の完全修飾ドメイン名 (FQDN) を入力します。HPCA コンソールが AD と通信して特定ドメインのデバイスのリストを取得するため、これが必要となります。

例えば、Active Directory ホストの情報が次のとおりであるとします。

ドメイン名 : oobm.hp.com

ドメイン ユーザー : Administrator

ドメイン パスワード : password

ドメイン ホスト名 : DomainSystem.oobm.hp.com

次の情報を各フィールドに入力します。

[ユーザー名]: Administrator (唯一利用できる形式)

[パスワード]: password

[FQDN]: DomainSystem.oobm.hp.com (IP アドレスまたはホスト名は利用不可)

5 探索プロセスを開始するには、**[探索]** をクリックします。探索プロセスを停止するには、**[キャンセル]** をクリックします。探索が完了するか探索をキャンセルすると、[vPro プロビジョニング] ウィンドウに戻ります。

プロビジョニング済み、プロビジョニング解除済み、プロビジョニング中というプロビジョニングのステータス ([vPro ステータス]) とともにデバイスのリストが表示されます。vPro デバイスの UUID、および vPro デバイスのローカル エージェントのステータスも表示されます。

プロビジョニングを解除したデバイス、プロビジョニング中のデバイス、一部の完全プロビジョニング済みデバイスには、UUID が表示されません。これは正常な動作とみなされます。

6 プロビジョニングするデバイスを選択します。

7 ツールバーの プロビジョニング アイコンをクリックします。リモート設定ウィザードが表示されます。

8 [イントロダクション] ウィンドウで **[次へ]** をクリックして作業を続けます。[プロファイル] ウィンドウが表示されます。

9 vPro デバイスのプロビジョニングに必要なプロファイルを [プロファイル] ウィンドウで選択します。

10 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

11 確定するには **[次へ]** をクリックします。[完了] ウィンドウが開いて、操作の結果が表示されます。

12 ウィザードを終了して vPro ウィンドウに戻るには、**[閉じる]** をクリックします。選択した vPro デバイスのステータスが、デバイス リストで更新されます。

vPro デバイスを再プロビジョニングするには

1 **[アウトバンド管理]** の下で、**[vPro プロビジョニング]** をクリックします。[vPro プロビジョニング] ウィンドウが表示されます。

2 ツールバーの プロビジョニング タスク アイコンをクリックし、プルダウン リストから **[再プロビジョニング]** を選択します。

3 アクションが正常に行われたかどうかを追跡するには、 プロビジョニング タスク アイコンをクリックし、プルダウン リストから **[プロビジョニング ステータス ログ]** を選択します。アクションのステータスがログに表示されます。

vPro デバイスを部分的にプロビジョニング解除するには

1 **[アウトバンド管理]** の下で、**[vPro プロビジョニング]** をクリックします。[vPro プロビジョニング] ウィンドウが表示されます。

2 ツールバーの プロビジョニング タスク アイコンをクリックし、プルダウン リストから **[部分的にプロビジョニングを解除]** を選択します。

3 アクションが正常に行われたかどうかを追跡するには、  プロビジョニング タスク アイコンをクリックし、プルダウン リストから **[プロビジョニング ステータス ログ]** を選択します。アクションのステータスがログに表示されます。

vPro デバイスを完全にプロビジョニング解除するには

1 **[アウトバンド管理]** の下で、**[vPro プロビジョニング]** をクリックします。[vPro プロビジョニング] ウィンドウが表示されます。

2 ツールバーの  プロビジョニング タスク アイコンをクリックし、プルダウン リストから **[完全にプロビジョニング解除]** を選択します。

3 アクションが正常に行われたかどうかを追跡するには、  プロビジョニング タスク アイコンをクリックし、プルダウン リストから **[プロビジョニング ステータス ログ]** を選択します。アクションのステータスがログに表示されます。

8 デバイス管理

この章では、HPCA コンソールを介して OOB デバイスを管理する方法を説明します。OOB デバイスは、電源の状態、オペレーティング システムの状態、管理エージェントの有無に関係なく管理できます。

HPCA コンソールの **[操作]** タブに用意されているアウトバンド管理オプションの 1 つに、**[デバイス管理]** があります。デバイス管理オプションでは次の作業を実行できます。

- 複数のデバイスの管理
- 135 ページの「個々のデバイスの管理」

複数のデバイスの管理

一度に複数の OOB デバイスに対して管理タスクを実行するには、[デバイス管理] ウィンドウに表示されるデバイス リストから対象となる OOB デバイスを選択します。

複数のデバイスを管理する際には、表示するデバイスとそれらのデバイスのデバイス リストでのソート順を次のようにして指定できます。

- 検索条件に基づいて個々のデバイスを検索します。
- 一度に表示するデバイスの数を選択して、見やすいように一部のデバイスのみが表示されるようにします。
- カラムの見出しに基づいてデバイスをソートします。

デバイス リストのツールバーにある各種アイコンを使用すると、複数の OOB デバイスを一度に管理できます。次の表に示したアイコンの一部は、vPro デバイスのみで使用できるものです。表の機能説明を参照して、各デバイス タイプに対して適用可能な操作を把握してください。

表 12　デバイス リスト ツールバー

アイコン	機能
	OOBM データベースに格納されている情報で、リストに表示されている OOB デバイス情報をリフレッシュします。
	選択したデバイス、またはリストに表示されているすべてのデバイスの情報を、各デバイスに現在格納されている情報と同期させます。
	ネットワーク上の OOB デバイスを探索します。
	選択した OOB デバイスの電源のオン / オフと再起動を管理します。
	選択した vPro デバイスに対する警告メッセージ予約を管理します。
	vPro デバイスに共通のユーティリティを管理します。

表 12　デバイス リスト ツールバー (cont'd)

アイコン	機能
	選択した vPro デバイスにシステム防御ポリシーを配布します。
	選択した vPro デバイスにヒューリスティック ワーム封じ込め情報を配布します。
	選択した vPro デバイスにエージェント ウォッチドッグを配布します。
	選択した vPro デバイスにエージェント ソフトウェア リストとシステム メッセージを配布します。

HPCA コンソールに初めてログインする場合、リフレッシュ アイコンを数回クリックしないと、管理対象デバイスのリストがウィンドウに表示されないことがあります。

デバイス リスト ツールバーの表に示したとおり、探索アイコンをクリックすると、ネットワーク上の OOB デバイスを手動で探索できます。vPro デバイスの場合は、完全探索と増分探索があります。詳細は、デバイスの探索を参照してください。OOBM では、手動探索だけでなく、一定の時間間隔でデバイスを自動的に探索することもできます。この時間間隔は、(<HPCA_Install_DIR>\oobm\conf\ ディレクトリにある) config.properties ファイルで device_synchronization_timeperiod パラメータの値を設定することによって設定できます。この同期時間間隔のデフォルト値はゼロ (自動同期を行わない) です。自動同期を行う場合は、この値をゼロ以外に設定してください。単位は分です。OOBM による自動探索は増分探索です。OOBM は、新しいデバイスを検出すると、そのデバイスにアクセスして情報を取得します。

デバイスの探索

ツールバーの デバイス探索アイコンをクリックすると、ネットワーク上の OOB デバイスを探索できます。

DASH 対応デバイスの場合は、HPCA コンソールで、IP アドレスとホスト名、または Active Directory 情報を指定する必要があります。vPro デバイスの場合は、完全探索と増分探索のどちらを行うかを指定する必要があります。これにより、vPro デバイスが、SCS リポジトリに登録されているデバイス リストから読み込まれます。

デバイスを探索するには

1. HPCA コンソールにログインして、**[操作]** タブを選択します。
2. 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。
3. デバイス探索アイコンをクリックします。デバイスの探索ウィザードが表示されます。
4. **[次へ]** をクリックして続行すると、[探索オプション] ウィンドウが表示されます。
5. このページに表示される探索オプションは、HPCA コンソールの **[設定]** タブで選択したデバイス タイプによって決まります。両方のタイプのデバイスを選択した場合は、次に示すオプションがすべて表示されます。どちらか一方のタイプを選択した場合は、選択したタイプのオプションのみが表示されます。

DASH デバイスの場合 :

[DASH デバイスの探索] ラジオ ボタンをクリックすると、次の 2 つのオプションが表示され、IP アドレスおよび (または) ホスト名、または Active Directory (AD) 情報を入力できます。

— **[手動入力による DASH デバイスの探索]**: ホスト情報を指定する場合は、探索の対象とする複数のデバイスの IP アドレスとホスト名をカンマで区切られたリストとして指定します。

— **[Active Directory による DASH デバイスの探索]**: Active Directory から自動的にデバイス情報をインポートするには、**[LDAP ホスト]** (Active Directory サーバーのホスト名または IP アドレス)、**[LDAP ポート]**(デフォルトのポートは 386)、**[ユーザー ID]**、**[パスワード]** (管理権限を持つユーザーの Active Directory の認証情報)、および **[クエリする DN]**(Active Directory 内でクエリの対象となるドメイン名のリスト) を入力する必要があります。

例えば、Active Directory ホストの情報が次のとおりであるとします。

ドメイン名 : oobm.hp.com

ドメイン ユーザー : Administrator

ドメイン パスワード : password

ポート : 386 (デフォルト)

ドメイン ホスト名 : DomainSystem.oobm.hp.com

コンピュータのリストが、Active Directory の「computers」ノードに登録されている場合、

次の情報を各フィールドに入力します。

[LDAP ホスト]: DomainSystem.oobm.hp.com

[LDAP ポート]: 386

[ユーザー ID]: Administrator@oobm.hp.com

[パスワード]: password

[クエリする DN]: cn=computers, dc=oobm, dc=hp, dc=com

Active Directory (AD) による探索は、管理する必要のある DASH デバイスが大量に存在する場合のみ選択するようにしてください。Active Directory (AD) による探索は時間がかかるため、数百のデバイスを探索するにはかなりの時間を要します。AD 探索では、HPCA コンソールは、DASH デバイスかどうかを判別するために、各デバイスに対して呼び出しを実行します。呼び出したデバイスから応答がないと、Management Console は、指定されたタイムアウト値だけ待つため、デバイス探索の所要時間が長くなります。探索効率を上げるため、探索するデバイスの数が少ない場合は、手動探索を使用してください。

vPro デバイスの場合 :

[vPro デバイスの探索] ラジオ ボタンをクリックすると、次の 2 つのオプションが表示され、完全探索または増分探索を選択できます。

— **[すべての vPro デバイスの探索]**: ネットワーク上のすべての vPro デバイスを探索します。

— **[更新された vPro デバイスの探索]**: 新規の vPro デバイス、または前回の探索プロセス以降に変更された vPro デバイスのみを探索します。このオプションを選択すると、探索のパフォーマンスが大幅に向上しますが、前回の探索プロセス以降にネットワークから削除された vPro デバイスが通知されません。

6 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。入力した探索情報の要約が表示されます。

7 **[次へ]** をクリックして続行します。[完了] ウィンドウが開き、実行したオペレーションのステータスが表示されます。ステータスには、一部の DASH デバイスの探索に失敗した場合に、その旨が表示されます。IP アドレス / ホスト名を手動で入力してデバイスを探索した場合は、探索に失敗した理由を示すメッセージが表示されます。

8 **[閉じる]** をクリックして、ウィザードを終了します。新しく検出されたデバイスが、**[デバイス]** タブのデバイスのリストに表示されます。新しく検出されたデバイスがすぐに表示されない場合は、ツールバーの アイコンをクリックしてください。

デバイス探索機能を使用すると、ネットワーク上の OOB デバイスを容易に検出できます。検出されたデバイスは、HPCA コンソールを介して管理できます。

複数のデバイスの選択

デバイス管理操作は、一度に複数のデバイスに対して実行できます。

複数のデバイスを選択するには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 操作対象の OOB デバイスのチェック ボックスをオンにしてそのデバイスを選択するか、左上の [すべて選択] チェック ボックスをオンにします。選択しやすいように、特定の条件を満たすデバイスのみに検索を絞り込んだり、デバイスを並べ替えたりすることができます。

DASH デバイス管理の認証情報

DASH デバイスを管理するには、そのデバイスの設定時に指定したユーザー名とパスワードを入力する必要があります。この認証情報は、あらゆる管理操作において、DASH デバイスと HPCA コンソール間の通信を安全にするために使用されます。

各 DASH デバイスは、共通の認証情報を使用する (すべてのデバイスで同じ認証情報を使用する) ように設定することもできますし、デバイスごとに異なる認証情報を使用するように設定することもできます。認証情報は、デバイスを設定した管理者に問い合わせて確認してください。

共通認証情報、またはデバイスごとの個別認証情報のどちらか一方を選択できます。一部のデバイスに共通認証情報を使用し、残りのデバイスに個別認証情報を使用することはできません。共通認証情報を選択すると、個別認証情報は削除されます。共通認証情報オプションで **[無効]** を選択すると、既存の共通認証情報が削除されます。

共通認証情報を使用するように DASH デバイスを設定した場合は、[デバイス タイプの選択] ウィンドウに共通認証情報を入力できます (102 ページの「デバイス タイプの選択」を参照)。

共通認証情報を使用するように DASH デバイスを設定しなかった場合は、最初にそのデバイスにアクセスして管理操作を実行するときに、個別認証情報を入力する必要があります。認証情報は初回のアクセス時に“記憶”されるため、2 回目以降のアクセスでは、その DASH デバイスの認証情報を変更する場合を除き、認証情報を再入力する必要はありません。

DASH デバイスの個別認証情報を指定するには

1 HPCA コンソールにログインして、**[設定]** タブを選択します。

2 **[アウトバンド管理]** の下で、**[デバイス タイプの選択]** をクリックします。[デバイス タイプの選択] ウィンドウが表示されます。

3 **[DASH デバイスの管理]** をオンにします。

4 **[すべての DASH デバイスに対して共通の認証情報を使用]** で **[いいえ]** を選択します。

5 **[保存]** をクリックします。

6 **[オペレータ]** タブを選択します。

7 **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

8 DASH デバイスのホスト名リンクをクリックします。[認証情報の管理] ウィンドウが表示されます。

9 [認証情報の管理] ウィンドウは、DASH デバイスに初めてアクセスしたとき、または DASH デバイスの認証情報を変更したときに表示されます。それ以外の場合で、このウィンドウがログイン時に表示されることはありません。

10 DASH デバイスの **[デバイス ユーザー名]** と **[デバイス パスワード]** を入力します。

11 **[送信]** をクリックします。DASH デバイスの [デバイスの詳細] ウィンドウが表示されます。

後日、共通の認証情報を使用するように DASH デバイスを再設定する場合は、[デバイス タイプの選択] ウィンドウに戻って、**[はい]** を選択してください。これにより、HPCA コンソールから個別認証情報が消去されます。

デバイス情報のリフレッシュ

HPCA コンソールに表示されるデバイス情報は、ネットワーク上のデバイスに格納されているデバイス情報と同期させることができます。

デバイス情報をリフレッシュするには

1 複数のデバイスを選択するには に示した手順に従って、管理する OOB デバイスを選択します。

2  デバイス情報のリロード アイコンをクリックします。HPCA コンソールに表示されている選択したデバイスのデバイス情報が、OOB デバイスに格納されている情報と同期されます。

HPCA OOBM コンソールにシステム防御ポリシーが設定されていない場合は、そのコンソールの [要約] テーブルで、システム防御およびエージェント存在機能に関する 4 つのカラムに **N/A** と表示されます。

実際にシステム防御ポリシーを使用しない場合は、システム防御ポリシーを作成しないことを推奨します。vPro デバイスからシステム防御ポリシーを取得すると、リロード操作のパフォーマンスが大きく妨げられます。

電源管理

同時に複数のユーザーが同じターゲット OOB デバイスにリモートで電源操作を実行する場合、システム状態の結果は予測できません。たとえば、同じデバイスに対してあるユーザーが再起動タスクを実行中に、別のユーザーが電源を切るタスクを実行する場合、結果は確定できません。

複数のデバイスの電源管理をするには

1 複数のデバイスを選択するには に示した手順に従って、管理する OOB デバイスを選択します。

2 電源アイコン プルダウン メニューから、電源状態を選択します。ハードディスクの電源を入れたり、ハードディスクまたはネットワークを再起動したりすることができます。各デバイス上で電源操作を実行する場合は、ほかにもオプションがあります。確認メッセージが表示されます。

3 続行する場合は、**[OK]** をクリックします。プロセスを監視する進捗状況バーが表示されます。選択したデバイスの新規電源状態がデバイス リスト テーブルに表示されます。ウィンドウの右下に電源ステータスのリンクが作成されます。このリンクをクリックすると、電源管理プロセスの結果の要約を表示できます。

この機能を使用して、特定の時間に複数のデバイスの電源を効果的に入れたり、切ったりしてコストを削減できます。

警告メッセージ予約の管理

複数のデバイス上で警告メッセージ予約を管理するには

1 複数のデバイスを選択するには に示した手順に従って、管理する vPro デバイスを選択します。

2 警告メッセージ予約 アイコン プルダウン メニューから、警告メッセージを予約するかキャンセルするかを選択します。確認メッセージが表示されます。

3 続行する場合は、**[OK]** をクリックします。プロセスを監視する進捗状況バーが表示されます。進捗状況バーが非表示になると、選択したオプションに応じてメッセージ予約が作成またはキャンセルされます。メッセージ予約を作成すると、デバイスの [警告メッセージ予約] カラムにチェック マークが表示されます。メッセージ予約をキャンセルすると、[警告メッセージ予約] カラムに X マークが表示されます。

この機能を使用して、複数のデバイスのメッセージ予約を登録またはキャンセルし、関連するイベント警告を HPCA コンソールに送信できます。

共通ユーティリティの管理

ツールバーの 共通ユーティリティ アイコンを使用すると、次のセクションで説明するように vPro デバイス上でさまざまな維持管理タスクを実行できます。

実行できるタスクは、次のとおりです。

- フラッシュ制限リセット

すべての配布アクティビティは、プロビジョニング済みの vPro デバイス上のサード パーティ データ ストア (3PDS) に書き込むアクティビティです。この非揮発性メモリにはこの領域の誤用を防ぐフラッシュ制限保護メカニズムがあります。この制限を超えるアクションを実行すると、HPCA コンソールに次のメッセージが表示されます。

```
Error getting application blocks: Flash write limit exceeded - Click 'Reset Flash Limit' option to reset the flash limit
```

このフラッシュ制限リセット機能を使用すると、フラッシュ メモリのカウンタをリセットし、この非揮発性メモリ ストアへの書き込みアクティビティを継続できます。

vPro デバイス上で 3PDS のフラッシュ制限を超えることによる配布アクティビティの失敗を防ぐために、この制限を頻繁にリセットすることを推奨します。

複数の vPro デバイス上でフラッシュ制限をリセットするには

1 複数のデバイスを選択するには に示した手順に従って、管理する vPro デバイスを選択します。

2 共通ユーティリティ プルダウン メニューから、**[フラッシュ制限リセット]** オプションを選択します。確認メッセージが表示されます。

3 **[OK]** をクリックして続行します。選択した vPro デバイスのサード パーティ データ ストア (3PDS) のカウンタがゼロにリセットされます。

このオプションを使用して、3PDS カウンタをリセットできます。これはフラッシュの消耗を保護するメカニズムとして機能します。同じ vPro デバイス上で非揮発性メモリへの複数の読み取り / 書き込みアクセスを実行した場合に、フラッシュ制限例外が発生することがあります。カウンタをリセットすると、この非揮発性メモリを使用するアクションの実行を継続できます。

システム防御ポリシーの配布

複数のデバイスにシステム防御ポリシーを配布するには

1 複数のデバイスを選択するには に示した手順に従って、管理する vPro デバイスを選択します。

2 システム防御ポリシー配布アイコンをクリックします。ポリシー配布ウィザードが表示されます。

3 **[次へ]** をクリックして続行します。[ポリシーの選択] ウィンドウが表示されます。

4 配布するポリシーを選択します。

5 **[次へ]** をクリックします。[ポリシーの設定] ウィンドウが表示されます。このウィンドウを使用して、選択したデバイス グループの有線および無線 NIC に割り当てるデフォルトのシステム防御ポリシーおよびエージェント存在ポリシーを選択できます。同じポリシーは、[システム防御] および [エージェント存在] の各フィールドの横にあるプルダウン メニューからも選択できます。デバイスに存在しない NIC (有線または無線) にポリシーを指定すると、[結果] ウィンドウに例外が表示されますが、これは配布プロセスには影響しません。

   デバイス上の NIC 数にかかわらず、vPro デバイスに設定できるエージェント存在ポリシーは 1 つのみです。vPro デバイスに複数の NIC があり、各 NIC に異なるエージェント存在ポリシーを指定すると、直近の設定が適用されます。

6 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

7 **[次へ]** をクリックして続行します。[結果] ウィンドウに操作結果が表示されます。

8 **[閉じる]** をクリックして、ウィザードを終了します。

この機能を使用すると、複数の vPro デバイスに複数のシステム防御ポリシーを配布しやすくなるとともに、これらのシステムを悪意のある攻撃から保護することができます。

ヒューリスティックの配布

複数のデバイスにヒューリスティックを配布するには

1 複数のデバイスを選択するには に示した手順に従って、管理する vPro デバイスを選択します。

2 ヒューリスティック配布アイコンをクリックします。ヒューリスティック配布ウィザードが開始されます。

3 **[次へ]** をクリックして続行します。[ヒューリスティックの選択] ウィンドウが表示されます。

4 配布するヒューリスティックを選択します。

5 **[次へ]** をクリックします。[ヒューリスティックスの設定] ウィンドウが表示されます。

6 vPro　デバイス上の有線および無線ネットワーク　インターフェイスに適用するヒューリスティックを選択します。両方のインターフェイスに同じヒューリスティック情報を設定できます。デバイスに存在しない NIC (有線または無線) にヒューリスティック情報を指定すると、[結果] ウィンドウに例外が表示されますが、配布プロセスには影響しません。

7 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

8 **[次へ]** をクリックして続行します。[結果] ウィンドウに操作結果が表示されます。

9 **[閉じる]** をクリックして、ウィザードを終了します。

この機能を使用すると、複数の vPro デバイスに複数のヒューリスティックを簡単に配布し、感染したデバイスのワーム封じ込めができます。

エージェント ウォッチドッグの配布

複数のデバイスにエージェント ウォッチドッグを配布するには

1 複数のデバイスを選択するには に示した手順に従って、管理する vPro デバイスを選択します。

2  エージェント　ウォッチドッグ配布アイコンをクリックします。エージェント　ウォッチドッグ配布ウィザードが表示されます。

3 **[次へ]** をクリックして続行します。[ウォッチドッグの選択] ウィンドウが表示されます。

4 配布するウォッチドッグを選択します。HP の ローカル エージェント ウォッチドッグは 1 つしか配布できません。サード パーティ製のエージェント ウォッチドッグは複数配布できます。vPro デバイス上で動作しているサード パーティ製の各ローカル エージェントに対し、サード パーティ製エージェント ウォッチドッグを 1 つ配布できます。

5 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

6 **[次へ]** をクリックして続行します。[結果] ウィンドウに操作結果が表示されます。

7 **[閉じる]** をクリックして、ウィザードを終了します。

この機能を使用すると、複数の vPro デバイスに複数のエージェント ウォッチドッグを簡単に配布し、これらのシステム上のローカル エージェントを監視できます。ローカル エージェントを監視することにより、これらのエージェントが今度はプロビジョニング済みのデバイス上で実行中のセキュリティ ソフトウェアを監視するため、ネットワークのセキュリティが強化されます。ユーザーの誤った操作によりまたはその他の原因によりセキュリティ ソフトウェアの実行が停止した場合、ウォッチドッグによってこのイベントをシステム管理者に警告できます。

エージェント ソフトウェア リストとシステム メッセージの配布

エージェント ソフトウェア リストとシステム メッセージを複数のデバイスに配布するには

1 複数のデバイスを選択するには に示した手順に従って、管理する vPro デバイスを選択します。

2 ツールバーの  ソフトウェア リストとシステム メッセージの配布アイコンをクリックします。配布ウィザードが表示されます。

3 **[次へ]** をクリックします。[ソフトウェア リスト] ウィンドウが表示されます。

4 ローカル エージェントに監視させるソフトウェア アプリケーションを選択します。

5 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

6 **[次へ]** をクリックして続行します。[結果] ウィンドウに操作結果が表示されます。

7 **[閉じる]** をクリックして、ウィザードを終了します。システム メッセージとアプリケーション ソフトウェア リストは、ターゲットの vPro デバイスのサード パーティ データ ストア (3PDS) に書き込まれます。**[デバイス]** タブでデバイスを選択してから、**[診断]** セクションの下で、**[デバイス アセット] > [ソフトウェア情報] > [登録済みアプリケーション] > [HPCA] > [HPCABlock]** に移動すると、特定の vPro デバイスのこの情報を表示できます。

> アプリケーション ソフトウェア リストは、vPro デバイス上の 3PDS に書き込まれます。ローカル エージェントはこの 3PDS からリストを読み取るため、変更したリストを再配布する場合は、このデバイス上のローカル エージェントを停止し再起動する必要があります。

この機能を使用すると、ローカル エージェントのシステム メッセージとソフトウェア リストを複数の vPro デバイス上の 3PDS に簡単に配布できます。

個々のデバイスの管理

[デバイス管理] ウィンドウに表示されるデバイス リスト テーブルには、デバイスの電源状態、そのホスト名、その他の属性が表示されます。

個々のデバイスを管理するには、テーブルの [デバイス] カラムの下のホスト名リンクをクリックします。

選択したデバイスの管理ウィンドウが表示されます。このウィンドウでは、次を実行できます。

- 電源状態の表示 (139 ページ を参照)
- vPro イベント ログの表示およびクリア (140 ページ を参照)
- デバイス上でのイベント フィルタの表示 (140 ページ を参照)
- vPro デバイスの一般資産情報の表示 (141 ページ を参照)
- ハードウェア資産の表示 (141 ページ を参照)
- サード パーティ データ ストア (vPro) に登録された、またはネットワーク コントローラの NVRAM (DASH) にあるアプリケーションのリストの表示 (142 ページ を参照)
- 電源のオン、オフ、再起動などのリモート操作の実行 (143 ページ を参照)
- テキストまたはグラフィカル モードでの KVM リダイレクトの実行 (154 ページ を参照)
- vPro デバイス上でのシステム防御フィルタの表示および削除 (155 ページ を参照)
- vPro デバイス上でのシステム防御ポリシーの表示、削除、有効化およびエージェント存在ポリシーの設定 (156 ページ を参照)
- vPro 上でのヒューリスティック情報の表示および削除 (158 ページ を参照)
- vPro デバイス上でのエージェント ウォッチドッグの表示および削除 (159 ページ を参照)
- リモート電源操作中の vPro デバイス上でのフロント パネルの設定 (160 ページ を参照)

- vPro デバイス上でのフラッシュ制限のリセット (160 ページ を参照)

68 ページのアウトバンド デバイスの管理操作表 を参照し、デバイス タイプごとにサポートされている管理操作について理解してください。

電源状態の表示

ワークスペースの **[電源状態]** 領域では、OOB デバイスの電源状態が一目でわかります。

詳細設定および電源インターフェイス (ACPI) では複数の電源状態が定義されます。マザーボード、BIOS、およびオペレーティング システムのサポート状態によっては、これらの状態の一部は使用できない場合があります。

電源状態は S0 (通常の作業状態) から S5 (ソフト オフ状態) まで順次深くなっていくスリープ状態、および機械的オフ状態までの範囲があります。S0 から機械的オフ状態は、次のように G0 から G3 状態にマップされます。

- G0
  - S0: 覚醒。システムは完全に電源が入り、実行中です。電源は節約されません。
- G1
  - S1: スタンバイ。CPU が減速し、一部のコンポーネントの電源が切れます。システム状態は RAM で維持されます。システムはほぼ即座に覚醒状態になりますが、節約される電源量は小規模です。
  - S2: 同じくスタンバイ。CPU と一部のコンポーネントの電源が切れます。システム状態は RAM で維持されます。消費される電源量は少なくなりますが、システムが覚醒するまでの時間がより長くなります。
  - S3: RAM を中断。CPU とほとんどのコンポーネントの電源が切れます。システム状態のみが RAM で維持されます。電源の節約量は増えますが、覚醒するまでの時間も長くなります。
  - S4: 休止状態。システム状態 (RAM の内容を含む) が非揮発性ストレージに保存され、すべての電源が切れます。この状態の電源節約は最も大きいですが、覚醒するまでの時間は RAM のサイズに応じて非常に長くなります。
- G2
  - S5: ソフト オフ。オペレーティング システムがシャットダウンされ、システム電源が切れます。ユーザーが PC にシャットダウンを指示すると、PC はこの状態になります。これが適正シャットダウンです。
- G3
  - 機械的オフ状態。オペレーティング システムがシャットダウンされ、システムが電源から切断されます (通常、PSU の背面のスイッチによる)。再接続されると、システムは追加介入なしで G2 に入ります。

順次深くなっていく各スリープ状態は、その深さの程度に応じて、G0/S0 までの覚醒に要する待ち時間は長くなり、S4 のコンテキスト保存特性を除きシステム コンテキストの損失レベルも高くなります。S4 は、バッテリー レベルが非常に低くなる場合と同様、スリープ状態になる前にコンテキストを非揮発性ストレージに保存できる特別な状態です。S5 は「電源オフ」状態で、機械的オフ (G3) はバッテリーと外部電源が切断されていることを示します。

HPCA コンソールの vPro および DASH のデバイス上で実行できる電源操作は、次の表の ACPI 電源状態にマップされます。

すべての電源操作が両タイプの OOB デバイスでサポートされているわけではありません。さまざまな電源操作の手順を確認する際は、このテーブルを参照して関連するデバイス タイプを把握してください。

DASH デバイスの「サポート対象外」とは、DASH 標準が電源操作をサポートしていない、またはハードウェア ベンダーの一部がサポートしていないという意味です。

表 13　　電源状態への電源操作のマッピング

vPro 電源操作	DASH 電源操作	説明	ACPI 状態
ハード ドライブ電源オン	電源オン 起動元 : ハード ディスク	覚醒状態	G0/S0
ローカル CD/DVD 電源オン	電源オン 起動元 : CD/DVD	覚醒状態	G0/S0
IDE-R CD/DVD 電源オン	サポート対象外	覚醒状態	G0/S0
IDE-R フロッピー電源オン	サポート対象外	覚醒状態	G0/S0
BIOS セットアップ電源オン	サポート対象外	覚醒状態	G0/S0
BIOS 停止電源オン	サポート対象外	覚醒状態	G0/S0
プライマリ ブート デバイス電源オン	サポート対象外	覚醒状態	G0/S0
デバイス電源オフ	電源オフ (ソフト) 起動元 : なし	ソフト オフ状態	G2/S5
ハード ドライブ再起動	電源サイクル (ソフト) 起動元 : ハード ディスク	ソフト オフ状態に続き覚醒状態	S0 から S5、そして G0/S0 に戻る (S0 コンテキストが失われる場合は、システムのマスター バスのリセットまたは POST および BIOS からの完全起動が必要)
ローカル CD/DVD 再起動	電源サイクル (ソフト) 起動元 : CD/DVD	ソフト オフ状態に続き覚醒状態	S0 から S5、そして G0/S0 に戻る (S0 コンテキストが失われる場合は、システムのマスター バスのリセットまたは POST および BIOS からの完全起動が必要)

表 13　　電源状態への電源操作のマッピング (cont'd)

vPro 電源操作	DASH 電源操作	説明	ACPI 状態
プライマリ ブート デバイス再起動	サポート対象外	ソフト オフ状態に続き覚醒状態	S0 から S5、そして G0/S0 に戻る (S0 コンテキストが失われる場合は、システムのマスター バスのリセットまたは POST および BIOS からの完全起動が必要)
IDE-R CD/DVD 再起動	サポート対象外	ソフト オフ状態に続き覚醒状態	S0 から S5、そして G0/S0 に戻る (S0 コンテキストが失われる場合は、システムのマスター バスのリセットまたは POST および BIOS からの完全起動が必要)
IDE-R フロッピー再起動	サポート対象外	ソフト オフ状態に続き覚醒状態	S0 から S5、そして G0/S0 に戻る (S0 コンテキストが失われる場合は、システムのマスター バスのリセットまたは POST および BIOS からの完全起動が必要)
BIOS セットアップ再起動	サポート対象外	ソフト オフ状態に続き覚醒状態	S0 から S5、そして G0/S0 に戻る (S0 コンテキストが失われる場合は、システムのマスター バスのリセットまたは POST および BIOS からの完全起動が必要)
BIOS 停止再起動	サポート対象外	ソフト オフ状態に続き覚醒状態	S0 から S5、そして G0/S0 に戻る (S0 コンテキストが失われる場合は、システムのマスター バスのリセットまたは POST および BIOS からの完全起動が必要)
LAN (PXE) 再起動	電源サイクル (ソフト) 起動元 : ネットワーク	ソフト オフ状態に続き覚醒状態	S0 から S5、そして G0/S0 に戻る (S0 コンテキストが失われる場合は、システムのマスター バスのリセットまたは POST および BIOS からの完全起動が必要)
サポート対象外	サポート対象外	スタンバイ状態	S1 または S2
サポート対象外	中断 起動元 : なし	中断状態	S3

表 13　　電源状態への電源操作のマッピング (cont'd)

vPro 電源操作	DASH 電源操作	説明	ACPI 状態
サポート対象外	休止 (ソフト) 起動元 : なし	休止状態	S4
サポート対象外	電源オフ (ソフト正常) 起動元 : なし	ソフト オフ状態 (適正なシャットダウンの実行要求が先行)	G2/S5
サポート対象外	電源オフ (ハード正常) 起動元 : なし	機械的オフ状態 (適正なシャットダウンの実行要求が先行)	G3
サポート対象外	電源オフ (ハード) 起動元 : なし	機械的オフ状態	G3
サポート対象外	電源サイクル (ソフト正常) 起動元 : <*boot_source*>	ソフト オフ状態 (適正なシャットダウン実行要求が先行) に続き覚醒状態	S0 から S5、そして G0/S0 に戻る (S0 コンテキストが失われる場合は、システムのマスター バスのリセットまたは POST および BIOS からの完全起動が必要)
サポート対象外	電源サイクル (ハード正常) 起動元 : <*boot_source*>	機械的オフ状態 (適正なシャットダウン実行要求が先行) に続き覚醒状態	G0 から G3、そして G0/S0 に戻る
サポート対象外	電源サイクル (ハード) 起動元 : <*boot_source*>	機械的オフ状態に続き覚醒状態	G0 から G3、そして G0/S0 に戻る
サポート対象外	マスター バス リセット (正常) 起動元 : <*boot_source*>	オフ状態 (ハードウェア リセット) (適正なシャットダウン実行要求が先行) に続き覚醒状態	G2/S5 から G0/S0 に戻る
サポート対象外	マスター バス リセット 起動元 : <*boot_source*>	オフ状態 (ハードウェア リセット) に続き覚醒状態	G2/S5 から G0/S0 に戻る
サポート対象外	診断中断 起動元 : <*boot_source*>	オフ状態 (ハードウェア リセット) に続き覚醒状態	G2/S5 から G0/S0 に戻る

OOB デバイスの電源状態を表示するには

1　HPCA コンソールにログインして、**[操作]** タブを選択します。

2　左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する OOB デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[電源状態]** セクションの情報を確認します。

表示される電源状態は前回の最新状態です。したがって現在の電源状態と同じでない場合があります。現在の電源状態が表示されていることを確認するには、電源状態メッセージの横にある リフレッシュ アイコンを使用する必要があります。

vPro イベント ログの表示

ワークスペースの **[診断]** 領域を使用すると、リモート vPro デバイスのイベント ログを表示およびクリアできます。管理対象 vPro デバイスのさまざまなオカレンスによりイベントが作成され、vPro デバイスのイベント ログに記録されます。

vPro イベント ログを表示するには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[診断]** セクションの **[イベント ログ]** リンクをクリックします。イベント ログの内容がコンソールの内容領域に表示されます。ウィンドウの上部にログ属性の要約が表示されます。ログ内のイベント ログ数、最後のイベントが記録された時刻、ログの状態 (凍結または非凍結) が表示されます。ログが凍結されていると、イベントのログへの書き込みができません。要約の下に、イベント タイプ (イベントが作成された理由)、イベントの重大度、イベントがログに記録された日時、イベントの説明が表示されます。[詳細] カラムの 詳細アイコンをクリックすると、選択したイベントのプロパティの詳細を表示するウィンドウが表示されます。

5 イベント ログの表示をリフレッシュするには、ツールバーの リフレッシュ アイコンをクリックします。

6 イベント ログ ファイルをクリアするには、ツールバーの クリア アイコンをクリックします。

7 イベント ログのステータスを変更するイベント ログ ファイルを凍結または凍結解除するには、凍結アイコンをクリックします。

イベント ログ インターフェイスを使用すると、次のことが可能になります。

- 即時アクションが必要な注目すべきイベントが発生したかどうかを判断する。
- 新規イベントを確実にログに記録できるように定期的にログをクリアする。
- vPro デバイスの全般的なステータスまたは状態を判断する。

vPro イベント フィルタの表示

ワークスペースの **[診断]** 領域では、リモート vPro デバイス上にあるデフォルトのイベント フィルタを表示できます。イベント フィルタによって、デバイスでイベントが発生した場合のアクションが決まります。

vPro イベント フィルタを表示するには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[診断]** セクションの **[イベント フィルタ]** リンクをクリックします。選択した vPro デバイスにあるデフォルトのイベント フィルタがコンソールの内容領域に表示されます。

5 詳細を表示するイベント フィルタの名前リンクをクリックします。[イベント フィルタ詳細] ページが開き、選択したイベント フィルタのプロパティ詳細が表示されます。

6 イベント フィルタをリフレッシュするには、リフレッシュ アイコンをクリックします。

イベント フィルタの情報を使用して、選択したデバイスに発生する特定のタイプのイベントに対してどのようなアクションがとられるかが把握できます。

vPro 一般資産情報の表示

ワークスペースの **[診断]** 領域では、電源状態または全般的な状態のいかんにかかわらず、リモート vPro デバイスに関する一般資産情報を表示できます。

一般資産情報の表示

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[診断]** にある **[デバイス アセット]** リンクをクリックします。

5 **[一般情報]** をクリックします。

6 vPro デバイスの一般資産情報を表示するには、**[vPro 情報]** をクリックします。IP アドレス、リスン ポート、プロビジョニング モード、BIOS バージョンなど、そのデバイスの一般資産情報がコンソールの内容領域に表示されます。

7 セキュリティ関連の資産情報を表示するには、**[セキュリティ設定]** をクリックします。TLS の有効化、暗号化、SOL、IDE-R など、そのデバイスのセキュリティ関連の情報がコンソールの内容領域に表示されます。

この情報を使用すると、次のことが可能になります。

- vPro デバイスの一般資産を検査する。
- セキュリティ関連の vPro デバイスの資産情報を表示し、再設定アクションが必要かどうかを判断する。

ハードウェア資産の表示

ワークスペースの **[診断]** 領域では、リモート OOB デバイス上のハードウェア資産を表示できます。オペレーティング システムの状態や、デバイスの電源がオンまたはオフであるかは問題ではありません。デバイスの状態または電源状態を問わずデバイスを検索できるため、手動によるイ

ンベントリ監査の必要性が削減または除外されます。このようにハードウェア資産がリモートで正確に表示されることにより、フィールド交換可能ユニット (FRU) の適切な計画、効率的なアップグレード、迅速な配布、管理の改善が実現されます。

Centrino Pro ノートブック コンピュータは、電源モードがオフ、スタンバイ、または休止の場合、無線ネットワークで管理することはできません。

ハードウェア資産を表示するには

1. HPCA コンソールにログインして、**[操作]** タブを選択します。
2. 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。
3. 管理する OOB デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。
4. ウィンドウ左側の **[診断]** にある **[デバイス アセット]** リンクをクリックします。
5. **[ハードウェア情報]** をクリックします。
6. ハードウェア コンポーネントをクリックします。そのコンポーネントの仕様がコンソールのコンテキスト領域に表示されます。

   vPro デバイスのハードウェア情報を表示できない場合があります。その場合は、しばらく待機してから操作を再試行してください。

この情報を使用すると、次のことが可能になります。

- 交換する必要があるデバイスのハードウェア コンポーネントの正確な仕様を判断する。
- 互換性問題を特定する。
- 新規オペレーティング システムをプロビジョニングする前にその設定を検査する。
- マシンの電源がオフの場合でも一時的なインベントリ情報報を取得する。

ソフトウェア資産の表示

ワークスペースの **[診断]** 領域では、OOB が有効化されたリモート デバイス上のソフトウェア資産を表示できます。

vPro デバイスの場合、この機能により vPro デバイス上でローカル エージェントが監視中のソフトウェア アプリケーションのリストを表示できます。114 ページの「エージェント ウォッチドッグの管理」を参照してください。このリストは、そのデバイス上のサード パーティ データ ストレージ (3PDS) に登録されます。

DASH デバイスの場合、この機能によりそのデバイスのネットワーク コントローラの NVRAM にあるソフトウェア在庫情報を表示できます。

ソフトウェア アプリケーションを表示するには

1. HPCA コンソールにログインして、**[操作]** タブを選択します。
2. 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。
3. 管理する OOB デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。
4. ウィンドウ左側の **[診断]** にある **[デバイス アセット]** リンクをクリックします。
5. **[ソフトウェア情報]** をクリックします。

6 vPro デバイスでは **[登録済みアプリケーション]** を、DASH デバイスでは **[インストール済みソフトウェア]** をクリックします。

7 アプリケーションをクリックします。アプリケーションのリンクにより、そのアプリケーションの情報を表示できます。

この情報を使用すると、次のことが可能になります。

- vPro デバイス上でローカル エージェントが監視中のソフトウェア アプリケーションを特定する。
- DASH デバイスにインストールされたソフトウェア アプリケーションを特定する。

電源状態の変更

HPCA コンソールから、リモート電源管理操作を実行できます。コンソールのワークスペースの **[診断]** 領域では、リモート OOB デバイス上の電源状態を変更できます。

68 ページのアウトバンド デバイスの管理操作表 を参照し、デバイス タイプごとにサポートされている電源操作について理解してください。

コンソール リダイレクション機能により、ユーザーの介入なしに、または管理コンソールから離れることなく、HPCA コンソール上の電源管理プロセスを表示できます。

vPro デバイス上で、SOL セッションによって Windows HyperTerminal が起動されます。HyperTerminal セッションを終了すると、設定セッションの設定の保存を促すメッセージが表示されます。セッション設定を保存することを推奨します。これには 2 つの理由があります。HyperTerminal セッションをカスタマイズした場合、そのカスタマイズが保存されます。また、設定を一旦保存すると、再度保存を促されることはなくなります。設定は、HPCA コンソールへアクセスする際に Web ブラウザの起動に使用したマシンの `.ht` ファイルとして保存されます。HyperTerminal を使用できない (Vista システムの場合) または失敗した場合は、代わりに Telnet が使用されます。

SOL では、vPro デバイス上でローカル ドライブの電源を入れる場合を除いて、管理コンソールへのキーボードとテキスト リダイレクトが提供されます。

この機能のセキュリティは TLS を介して提供されます。

vPro デバイス上では KVM リダイレクションも使用でき、グラフィカルとテキストの両モードでコンソール リダイレクション機能が提供されます。JRE 1.6.x と VNC Viewer をマシンにインストールし、HPCA コンソールへアクセスするブラウザを実行する必要があります。KVM 機能はリリース 6.0 以前の AMT の vPro マシン上では使用できません。154 ページの「vPro デバイスでの KVM リダイレクション」を参照してください。

クライアントが DASH デバイスにインストールおよび設定されている場合、DASH デバイス上で HPCA コンソールは、テキスト コンソール リダイレクションに SSH PuTTY クライアントを使用しようとします。PuTTY クライアントを使用するようにデバイスを設定するには、`PUTTY_PATH` システム環境変数を `C:\Putty\putty.exe` のように、PuTTY 実行可能ファイルのフル パスに設定する必要があります。`PUTTY_PATH` 環境変数の値を変更する場合は、ログアウトしてからシステムに再ログインして新規の値を有効にする必要があります。PuTTY クライアントを使用できない場合、コンソールでは代わりに Telnet が使用されます。

デバイスの電源を入れるには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する OOB デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[診断]** セクションの **[リモート操作]** リンクをクリックします。[リモート操作ウィザード] ウィンドウが表示されます。

5 **[次へ]** をクリックして続行します。[タスク] ウィンドウが表示されます。デバイスの電源はさまざまなドライブから、または BIOS (vPro のみ) に電源を入れることができます (次表参照)。

[タスク] ウィンドウでは、次を指定することができます。

— vPro デバイスの場合は、そのデバイスにフロント パネル設定を使用するかどうかを指定できます。**[いいえ]** を選択すると、vPro デバイスのフロント パネル設定は無視されます。詳細については、160 ページの「vPro デバイスのフロント パネル設定の設定」を参照してください。

— DASH デバイスの場合は、コンソールにテキストを表示するかどうかを指定できる **[クライアント コンソールの表示]** オプションがあります。

vPro デバイスまたは両タイプの OOB デバイスでリモート操作オプションがサポートされている場合、次の表では vPro リモート操作の用語が使用されています。DASH リモート操作へのマッピングを確認するには、68 ページのアウトバンド デバイスの管理操作表 を参照してください。

表 14　　デバイスの電源オン

ドライブ / BIOS	手順
ローカル ハード ドライブ	1 **[リモート操作]** の横のプルダウン メニューから、**[ハード ドライブの電源オン]** を選択します。 2 **[次へ]** をクリックします。DASH デバイスの場合は、[起動設定] ウィンドウが表示されます。このウィンドウで、デバイス起動時に使用する起動元または起動設定を指定できます。起動元として、**[ハードディスク]** を選択します。161 ページの「DASH デバイスの起動設定の設定」を参照してください。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。管理コンソールに要約情報が表示されます。 5 **[閉じる]** をクリックします。
ローカル CD ドライブ	1 **[リモート操作]** の横のプルダウン メニューから、**[ローカル CD/DVD の電源オン]** を選択します。 2 **[次へ]** をクリックします。DASH デバイスの場合は、[起動設定] ウィンドウが表示されます。このウィンドウで、デバイス起動時に使用する起動元または起動設定を指定できます。起動元として、**[CD/DVD]** を選択します。161 ページの「DASH デバイスの起動設定の設定」を参照してください。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。管理コンソールに要約情報が表示されます。 5 **[閉じる]** をクリックします。

表 14　デバイスの電源オン (cont'd)

ドライブ / BIOS	手順
IDE-R CD ドライブ (vPro のみ)	1 **[リモート操作]** の横のプルダウン メニューから、**[IDE-R の電源オン]** を選択します。 2 **[IDE-R オプション]** の横のプルダウン メニューから、**[IDE-R CD/DVD]** を選択します。[ドライブ パス] フィールドに CD/DVD ドライブのデフォルト設定が入力されます。ドライブ パス フィールドでデフォルトのドライブを使用しない場合は、別のドライブ、または管理コンソール サーバー上の ISO ファイルへのパスを指定できます。ドライブ パスに共有ネットワーク リソースである ISO ファイルを指定する場合は、UNC 構文、つまり、*\\hostname\sharefolder\file.iso* を使用する必要があります。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。リモート操作ウィザードが終了し、[HyperTerminal] ウィンドウが開いて電源オン プロセスが表示されます。このウィンドウは閉じない限り開いたままです。
IDE-R フロッピー ドライブ (vPro のみ)	1 **[リモート操作]** の横のプルダウン メニューから、**[IDE-R の電源オン]** を選択します。 2 **[IDE-R オプション]** の横のプルダウン メニューから、**[IDE-R フロッピー]** を選択します。[ドライブ パス] フィールドにフロッピー ドライブのデフォルト設定が入力されます。ドライブ パス フィールドでデフォルトのドライブを使用しない場合は、別のドライブ、または管理コンソール サーバー上の IMG ファイルへのパスを指定できます。ドライブ パスに共有ネットワーク リソースである IMG ファイルを指定する場合は、UNC 構文、つまり、*\\hostname\sharefolder\file.img* を使用する必要があります。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。リモート操作ウィザードが終了し、[HyperTerminal] ウィンドウが開いて電源オン プロセスが表示されます。このウィンドウは閉じない限り開いたままです。
BIOS セットアップ (vPro のみ)	1 **[リモート操作]** の横のプルダウン メニューから、**[BIOS の電源オン]** を選択します。**[BIOS オプション]** が表示されます。 2 **[BIOS オプション]** の横のプルダウン メニューから、**[BIOS セットアップ]** を選択します。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。リモート操作ウィザードが終了し、[HyperTerminal] ウィンドウが開いて電源オン プロセスが表示されます。このウィンドウは閉じない限り開いたままです。
BIOS 停止 (vPro のみ)	1 **[リモート操作]** の横のプルダウン メニューから、**[BIOS の電源オン]** を選択します。**[BIOS オプション]** が表示されます。 2 **[BIOS オプション]** の横のプルダウン メニューから、**[BIOS 停止]** を選択します。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。リモート操作ウィザードが終了し、[HyperTerminal] ウィンドウが開いて電源オン プロセスが表示されます。このウィンドウは閉じない限り開いたままです。

表 14　　デバイスの電源オン (cont'd)

ドライブ / BIOS	手順
プライマリ ブート デバイス (vPro のみ)	1 **[リモート操作]** の横のプルダウン メニューから、**[プライマリ ブート デバイスの電源オン]** を選択します。このオプションで、vPro デバイスの BIOS に設定されたデフォルトのブート デバイスの電源をオンにできます。**[SOL オプション]** が表示されます。このローカル起動オプションにより、選択した場合に HPCA コンソールに表示される操作を表示できます。 2 **[SOL オプション]** では、**[コンソールに表示]** または **[コンソールに表示しない]** を選択できます。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックします。 — **[コンソールに表示]** を選択した場合は、[リモート操作ウィザードは終了し、[HyperTerminal] ウィンドウが開いて電源オン プロセスが表示されます。このウィンドウは閉じない限り開いたままです。 — **[コンソールに表示しない]** を選択した場合は、[要約情報] ウィンドウが表示されます。操作が完了すると操作結果が表示されます。**[閉じる]** をクリックし、[デバイスの詳細] ウィンドウに戻る必要があります。

デバイスの電源を切るには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する OOB デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[診断]** セクションの **[リモート操作]** リンクをクリックします。[リモート操作ウィザード] ウィンドウが表示されます。

5 **[次へ]** をクリックして続行します。

6 **[リモート操作]** の横のプルダウン メニューから、**[デバイスの電源オフ]** を選択します。

7 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。

8 **[次へ]** をクリックして続行します。管理コンソールに要約情報が表示されます。

9 **[閉じる]** をクリックします。

この機能を使用すると、次のことができます。

- 管理操作に備えてデバイスの電源オン / オフを確認する。
- 管理操作に備えてデバイスにリモートで電源を入れる。
- 非応答デバイスをトラブルシューティングする。
- 非応答デバイスをリモートで再起動する。

システムの再起動

ワークスペースの [診断] 領域では、リモート OOB デバイスを再起動できます。組み込みのリダイレクション機能により、ユーザーの介入なしに、または管理コンソールから離れることなく再起動プロセスを表示できます。vPro デバイス上の SOL と KVM には、管理コンソールへのキーボードとビデオのリダイレクション機能が提供されます (OOB デバイス上でローカル デバイスの電源を入れる場合を除く)。

ローカル デバイスからシステムを再起動するには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する OOB デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[診断]** セクションの **[リモート操作]** リンクをクリックします。[リモート操作ウィザード] ウィンドウが表示されます。

5 **[次へ]** をクリックして続行します。[タスク] ウィンドウが表示されます。ローカル ドライブから OOB デバイスにデバイスを再起動できます (161 ページの DASH デバイスの起動設定の設定表 を参照)。

   [タスク] ウィンドウでは、次を指定することができます。

   — vPro デバイスの場合は、そのデバイスにフロント パネル設定を使用するかどうかを指定できます。**[いいえ]** を選択すると、vPro デバイスのフロント パネル設定は無視されます。詳細については、160 ページの「vPro デバイスのフロント パネル設定の設定」を参照してください。

   — DASH デバイスの場合は、コンソールにテキストを表示するかどうかを指定できる **[クライアント コンソールの表示]** オプションがあります。

表 15　　ローカル ドライブからのデバイスの再起動

ドライブ	手順
ローカル ハード ドライブ	1 **[リモート操作]** の横のプルダウン メニューから、**[ハード ドライブの再起動]** を選択します。 2 **[次へ]** をクリックします。DASH デバイスの場合は、[起動設定] ウィンドウが表示されます。このウィンドウで、デバイス起動時に使用する起動元または起動設定を指定できます。起動元として、**[ハードディスク]** を選択します。161 ページの「DASH デバイスの起動設定の設定」を参照してください。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。管理コンソールに要約情報が表示されます。 5 **[閉じる]** をクリックします。

表 15　　ローカル ドライブからのデバイスの再起動 (cont'd)

ローカル CD ドライブ	1 **[リモート操作]** の横のプルダウン メニューから、**[ローカル CD/DVD の再起動]** を選択します。 2 **[次へ]** をクリックします。DASH デバイスの場合は、[起動設定] ウィンドウが表示されます。このウィンドウで、デバイス起動時に使用する起動元または起動設定を指定できます。起動元として、**[CD/DVD]** を選択します。161 ページの「DASH デバイスの起動設定の設定」を参照してください。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。管理コンソールに要約情報が表示されます。 5 **[閉じる]** をクリックします。
プライマリ ブート デバイス (vPro のみ)	1 **[リモート操作]** の横のプルダウン メニューから、**[プライマリ ブート デバイスの再起動]** を選択します。このオプションにより、vPro デバイスの BIOS に設定されたデフォルトのブート デバイスを再起動できます。**[SOL オプション]** が表示されます。このローカル起動オプションにより、選択した場合に HPCA コンソールに表示される操作を表示できます。 2 **[SOL オプション]** では、**[コンソールに表示]** または **[コンソールに表示しない]** を選択できます。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックします。 — **[コンソールに表示]** を選択した場合、リモート操作ウィザードは終了し、[HyperTerminal] ウィンドウが開いて再起動プロセスが表示されます。このウィンドウは閉じない限り開いたままです。 — **[コンソールに表示しない]** を選択した場合は、[要約情報] ウィンドウが表示されます。操作が完了すると操作結果が表示されます。**[閉じる]** をクリックし、[デバイスの詳細] ウィンドウに戻る必要があります。

この機能を使用すると、次のことができます。

- 非応答デバイスをリモートで再起動する。
- コンソール　リダイレクションを使用して非応答デバイスのトラブルシューティングを実行し、BIOS 再起動プロセスを表示し、このプロセス中に応答しない失敗したコンポーネントを識別します。

IDE-R による vPro システムの再起動

ワークスペースの **[診断]** 領域では、問題のある vPro デバイスのブート デバイスを別のリモート ドライブ上のクリーンなイメージにリダイレクトできます。IDE-R (Integrated Drive Electronics Redirect) ではこの CD/ フロッピー ドライブ リダイレクション機能が提供されます。

IDE-R テクノロジは現在 vPro デバイス上でのみサポートされています。

vPro デバイスでは、無線通信による OOBM サーバーとの通信にはより時間がかかります。このため、SOL/IDE-R リモート操作でタイムアウトが発生する場合があります。この問題を回避するには、アウトバンド管理設定の 48 ページの「IDE-R および SOL タイムアウト値の設定」で説明されている方法で `IDER*` と `SOL*` パラメータを設定してください。

組み込みのリダイレクション機能により、ユーザーの介入なしに、または管理コンソールから離れることなく再起動プロセスを表示できます。vPro デバイスの SOL および KVM 機能により、キーボードおよびビデオの管理コンソールへのリダイレクトが可能になります。

IDE-R 機能を使用してシステムを再起動するには

1. HPCA コンソールにログインして、**[操作]** タブを選択します。
2. 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。
3. 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。
4. ウィンドウ左側の **[診断]** セクションにある **[リモート操作]** リンクをクリックします。[リモート操作ウィザード] ウィンドウが表示されます。
5. **[次へ]** をクリックして続行します。[タスク] ウィンドウが表示されます。vPro デバイスは、IDE-R 機能によって、リモート デバイス上のさまざまなデバイスから再起動できます (次表参照)。

   また、vPro デバイスの [タスク] ウィンドウでは、vPro デバイスのフロント パネル設定を使用するかどうかを指定できます。**[いいえ]** を選択すると、vPro デバイスのフロント パネル設定は無視されます。詳細については、160 ページの「vPro デバイスのフロント パネル設定の設定」を参照してください。

表 16　　IDE-R 機能による vPro デバイスの再起動

ドライブ	手順
IDE-R CD ドライブ (vPro のみ)	1 **[リモート操作]** の横にあるプルダウン メニューから、**[IDE-R を使用して再起動]** を選択します。**[IDE-R オプション]** が表示されます。 2 **[IDE-R オプション]** の横のプルダウン メニューから、**[IDE-R CD/DVD]** を選択します。[ドライブ パス] フィールドに CD/DVD ドライブのデフォルト設定が入力されます。ドライブ パス フィールドでデフォルトのドライブを使用しない場合は、別のドライブ、または管理コンソール サーバー上の ISO ファイルへのパスを指定できます。ドライブ パスに共有ネットワーク リソースである ISO ファイルを指定する場合は、UNC 構文、つまり、*\\hostname\sharefolder\file.iso* を使用する必要があります。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。リモート操作ウィザードは終了し、[HyperTerminal] ウィンドウが開いて、再起動プロセスが表示されます。このウィンドウは閉じない限り開いたままです。
IDE-R フロッピー ドライブ (vPro のみ)	1 **[リモート操作]** の横にあるプルダウン メニューから、**[IDE-R を使用して再起動]** を選択します。**[IDE-R オプション]** が表示されます。 2 **[IDE-R オプション]** の横のプルダウン メニューから、**[IDE-R フロッピー]** を選択します。[ドライブ パス] フィールドにフロッピー ドライブのデフォルト設定が入力されます。ドライブ パス フィールドでデフォルトのドライブを使用しない場合は、別のドライブ、または管理コンソール サーバー上の IMG ファイルへのパスを指定できます。ドライブ パスに共有ネットワーク リソースである IMG ファイルを指定する場合は、UNC 構文、つまり、*\\hostname\sharefolder\file.img* を使用する必要があります。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。リモート操作ウィザードは終了し、[HyperTerminal] ウィンドウが開いて、再起動プロセスが表示されます。このウィンドウは閉じない限り開いたままです。

この機能を使用すると、次のことができます。

- 非稼働状態のデバイスを再起動して一時的なトラブルシューティング環境に移行し、ソフトウェアの問題ではなく、ハードウェアの問題を正確に特定する。
- オペレーティング システム イメージを非稼働状態のデバイス上で再ビルドする。
- オペレーティング システムをベアメタル デバイスにプロビジョニングする。
- 復旧または再配布用にデバイスのイメージをキャプチャする。

vPro システムの再起動による BIOS 設定画面の表示

ワークスペースの **[診断]** 領域では、起動前に BIOS 設定画面を表示して、設定情報を確認し、vPro デバイスの問題を解決するために必要に応じて設定を変更できます。

再起動時に BIOS 設定画面を表示できるのは、vPro デバイスのみです。

組み込みのリダイレクション機能により、ユーザーの介入なしに、また管理コンソールから離れることなく、BIOS 設定画面を表示できます。vPro デバイスの SOL および KVM テクノロジにより、キーボードとビデオの管理コンソールへのリダイレクトが可能になります。

システムを再起動して BIOS 設定画面を表示するには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[診断]** セクションにある **[リモート操作]** リンクをクリックします。[リモート操作ウィザード] ウィンドウが表示されます。

5 **[次へ]** をクリックして続行します。[タスク] ウィンドウが表示されます。次の表に示したとおり、デバイスを再起動して BIOS 設定画面を表示するには、さまざまな方法があります。

また、vPro デバイスの [タスク] ウィンドウでは、vPro デバイスのフロント パネル設定を使用するかどうかを指定できます。**[いいえ]** を選択すると、vPro デバイスのフロント パネル設定は無視されます。詳細については、160 ページの「vPro デバイスのフロント パネル設定の設定」を参照してください。

表 17　　vPro デバイスの再起動による BIOS 設定画面の表示

BIOS	手順
BIOS セットアップ (vPro のみ)	1 **[リモート操作]** のプルダウン メニューから、**[再起動して BIOS 設定画面を表示]** を選択します。**[BIOS オプション]** が表示されます。 2 **[BIOS オプション]** の横のプルダウン メニューから、**[BIOS セットアップ]** を選択します。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。リモート操作ウィザードは終了し、[HyperTerminal] ウィンドウが開いて、再起動プロセスが表示されます。このウィンドウは閉じない限り開いたままです。
BIOS 停止 (vPro のみ)	1 **[リモート操作]** のプルダウン メニューから、**[再起動して BIOS 設定画面を表示]** を選択します。**[BIOS オプション]** が表示されます。 2 **[BIOS オプション]** の横のプルダウン メニューから、**[BIOS 停止]** を選択します。 3 **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。 4 **[次へ]** をクリックして続行します。リモート操作ウィザードは終了し、[HyperTerminal] ウィンドウが開いて、再起動プロセスが表示されます。このウィンドウは閉じない限り開いたままです。

この機能を使用すると、次のことができます。

- 設定情報を確認する。
- 必要に応じて設定を変更し、非稼働状態のデバイスをトラブルシューティングする。
- デバイスに物理的にアクセスすることなく BIOS 設定を変更する。

システムの再起動による起動前実行環境への移行

ワークスペースの **[診断]** 領域では、OOB デバイスを再起動して起動前実行環境 (PXE) に移行することができます。この再起動オプションを使用すると、ローカル ハード ディスクやインストール済みのオペレーティング システムに依存せずに、ネットワーク インターフェイス カードを使用してコンピュータを起動できます。OOB デバイスは、PXE サーバー上のブート イメージから再起動できます。

このオプションを使用するには、PXE ブート サーバーがネットワーク環境に存在していることが前提となります。PXE ブート サーバーでは、DHCP サーバー、TFTP サーバー、PXE ブート要求を処理するブート サーバーが稼動している必要があります。

システムを再起動して PXE 状態に移行するには

1. HPCA コンソールにログインして、**[操作]** タブを選択します。
2. 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。
3. 管理するデバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。
4. ウィンドウ左側の **[診断]** セクションにある **[リモート操作]** リンクをクリックします。[リモート操作ウィザード] ウィンドウが表示されます。
5. **[次へ]** をクリックして続行します。[タスク] ウィンドウが表示されます。
6. **[リモート操作]** のプルダウン メニューから、**[再起動して LAN (PXE) 状態に移行]** を選択します。

   [タスク] ウィンドウでは、次を指定することができます。

   — vPro デバイスの場合は、そのデバイスにフロント パネル設定を使用するかどうかを指定できます。**[いいえ]** を選択すると、vPro デバイスのフロント パネル設定は無視されます。詳細については、160 ページの「vPro デバイスのフロント パネル設定の設定」を参照してください。

   — DASH デバイスの場合は、コンソールにテキストを表示するかどうかを指定できる **[クライアント コンソールの表示]** オプションがあります。
7. **[次へ]** をクリックします。DASH デバイスの場合は、[起動設定] ウィンドウが表示されます。このウィンドウで、デバイス起動時に使用する起動元または起動設定を指定できます。起動元として **[ネットワーク]** を選択します。161 ページの「DASH デバイスの起動設定の設定」を参照してください。
8. **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。
9. 続行する場合は、**[次へ]** をクリックします。管理コンソールに要約情報が表示されます。
10. **[閉じる]** をクリックして、ウィザードを終了します。

この機能を使用すると、次のことができます。

- 非稼働状態のデバイスを再起動して一時的なトラブルシューティング環境に移行し、ソフトウェアの問題ではなく、ハードウェアの問題を正確に特定する。
- オペレーティング システム イメージを非稼働状態のデバイス上で再ビルドする。
- オペレーティング システムをベアメタル デバイスにプロビジョニングする。

起動して DASH のみでサポートされている電源状態に移行

DASH 対応のデバイスは、vPro デバイスよりも多くの電源状態をサポートしています。HPCA コンソールで実行できる電源操作では、DASH デバイスの起動後、次のいずれかの電源状態に移行できます。

- 中断
- 休止 (ソフト)
- 電源オフ (ソフト正常)
- 電源オフ (ハード正常)
- 電源オフ (ハード)
- 電源サイクル (ソフト正常)
- 電源サイクル (ハード正常)
- 電源サイクル (ハード)
- マスター バス リセット (正常)
- マスター バス リセット
- 診断中断

これらの電源操作、および対応する電源状態については、137 ページの電源状態への電源操作のマッピング表の表を参照してください。

HPCA コンソールで DASH デバイスを起動してこれらの電源状態に移行する手順は、どの場合も基本的に同じです。次の手順で個々の電源操作を指定する箇所のみが異なります。

上記のいずれかの電源操作を使用して DASH デバイスを起動するには

1. HPCA コンソールにログインして、**[操作]** タブを選択します。
2. 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。
3. 管理する DASH デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。
4. ウィンドウ左側の **[診断]** セクションの **[リモート操作]** リンクをクリックします。[リモート操作ウィザード] ウィンドウが表示されます。
5. **[次へ]** をクリックして続行します。[タスク] ウィンドウが表示されます。
6. **[リモート操作]** のプルダウン メニューから、DASH デバイスを起動して目的の電源状態に移行する電源操作を選択します。

   [タスク] ウィンドウで、プルダウン メニューから **[クライアント コンソールの表示]** を選択することにより、コンソールにテキストを表示するかどうかを指定することもできます。
7. **[次へ]** をクリックします。[起動設定] ウィンドウが表示されます。このウィンドウで、デバイス起動時に使用する起動元または起動設定を指定できます。161 ページの「DASH デバイスの起動設定の設定」を参照してください。この手順は、停止およびスリープ操作では関連がありません。
8. **[次へ]** をクリックします。[要約の確認] ウィンドウが表示されます。このウィンドウ内の情報を確認します。
9. **[次へ]** をクリックして続行します。管理コンソールに要約情報が表示されます。
10. **[閉じる]** をクリックします。

この機能を使用して、DASH デバイスの起動後にさまざまな電源状態レベルに移行できます。

vPro デバイスでの KVM リダイレクション

ワークスペースの **[診断]** 領域では、Keyboard Video Mouse Redirection (KVM) テクノロジを使用して、テキスト モードまたはグラフィカル モードで、vPro デバイスのリモート コンソールにアクセスできます。

KVM を正しく機能させるための要件は次のとおりです。

- vPro デバイスに AMT 6.0 以降が搭載されていること。
- JRE 1.6.x と VNC Viewer をマシンにインストールし、HPCA コンソールへアクセスするブラウザを実行する必要があります。VNC ビューアは 5900 番ポートを使用します。
- HPCA コンソールにアクセスするマシンで、VNC ビューアのインストール先パスが **VNC_PATH** 環境変数に設定されていること。例 : **VNC_PATH=C:\viewer\VNCViewer.exe**。
- vPro Web サービスの管理者権限が必要です。これらの権限を取得するには、Intel AMT Console で SCS プロファイルを作成するときに **[PT 管理]** 領域を選択する必要があります。

vPro デバイスで KVM リダイレクションを実行するには

1. HPCA コンソールにログインして、**[操作]** タブを選択します。
2. 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。
3. 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。
4. ウィンドウ左側の **[診断]** セクションにある **[KVM リダイレクション]** リンクをクリックします。[KVM リダイレクションの設定] ウィンドウが表示されます。
5. [KVM セッションの設定] セクションで、次の各項目を指定します。
   - VNC セッションのパスワードを作成し、確認します。このパスワードは 1 回限りのパスワードであり、セキュリティ保護のため新規の VNC セッションを開始するたびにリセットする必要があります。
   - KVM セッションのタイムアウト値を分単位で入力します。この値は、KVM セッションが開かれた状態を維持する時間の長さを特定します。セッションがタイムアウトした場合は、HPCA コンソールを使用してセッションに再接続する必要があります。
   - ユーザーのマシンにアクセスする前に明示的なアクセス許可を取得する必要がある場合は、**[オプトインの有効化]** オプションの横のチェック ボックスをオンにします。この機能を有効化することにより、2 段階のパスワード認証を必要とするより強力なセキュリティが実現します。

     HPCA コンソールでこのオプションは、クライアント vPro デバイスでこのオプションが有効になっている場合に限り、有効化できます。vPro デバイスでこのオプションを有効化するには、クライアント vPro デバイスの MEBx コンソールを表示します。**[メイン メニュー] > [Intel AMT の設定] > [KVM 設定] > [リモート IT からのオプトイン設定] > [KVM オプトイン ポリシーのリモート制御の有効化]** を選択します。

     デフォルトではこのオプションは有効になっています。
6. **[送信]** をクリックします。VNC ビューアが開き、パスワードを入力するように要求されます。
7. [KVM リダイレクションのパスワード] ウィンドウで認証用に作成したセッション パスワードを入力します。

8 **[OK]** をクリックします。

このオプトイン オプションを有効化すると、[AMT KVM のオプトイン] ウィンドウが開き、2 番目のパスワードを入力するように要求されます。アクセス先の vPro デバイスのユーザーからこのパスワードを教えてもらいます。そのユーザーの vPro デバイスに、[KVM リモート アシスタンス] ポップアップ ウィンドウが開き (オプトインが有効な場合)、ユーザーの同意コードが表示されます。このユーザー同意コードをそのユーザーから教えてもらい、[AMT KVM のオプトイン] ウィンドウでこのコードを入力し、**[はい]** をクリックします。

vPro デバイスのリモート コンソールが表示されます。

vPro デバイスのシステム防御フィルタの管理

ワークスペースの **[システム防御]** 領域は、vPro デバイスのみで使用できます。この領域で、個々の vPro デバイスのシステム防御フィルタを管理できます。具体的には、個々の vPro デバイスに配布されたシステム防御フィルタを確認および削除できます。システム防御フィルタは、システム防御ポリシーに割り当てられています。ポリシーに割り当てられたフィルタは、対応するポリシーがアクティブなポリシーになった時点でアクティブ化されます。

システム防御フィルタの管理ウィンドウを開くには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[システム防御]** セクションにある **[フィルタ]** リンクをクリックします。ウィンドウが開き、HPCA コンソールを介して作成され vPro デバイスに配布されたシステム防御フィルタが表示されます。

システム防御フィルタのビューをリフレッシュするには

1 システム防御フィルタの管理ウィンドウを開くには で説明した手順に従って、[システム防御フィルタの管理] ウィンドウを開きます。

2 ツールバーの  リフレッシュ アイコンをクリックします。

システム防御フィルタの詳細を表示するには

1 システム防御フィルタの管理ウィンドウを開くには で説明した手順に従って、[システム防御フィルタの管理] ウィンドウを開きます。

2 システム防御フィルタの詳細な情報を表示するには、そのフィルタのフィルタ名リンクをクリックします。[ネットワーク フィルタの詳細] ウィンドウが開き、選択したフィルタの仕様が表示されます。

システム防御フィルタを削除するには

1 システム防御フィルタの管理ウィンドウを開くには で説明した手順に従って、[システム防御フィルタの管理] ウィンドウを開きます。

2 削除するフィルタの横にあるチェック ボックスをオンにします。

3  削除アイコンをクリックします。選択したフィルタが、その vPro デバイスのシステム防御フィルタ テーブルから削除されます。

システム防御フィルタのインターフェイスを使用して、次の作業を実行できます。

- vPro デバイスに配布されたポリシーに適用できる既存のフィルタを確認する。
- vPro デバイスで不要になったフィルタを削除する。

vPro デバイスに対するシステム防御ポリシーの管理

ワークスペースの **[システム防御]** 領域は、vPro デバイスのみで使用できます。この領域では、個々の vPro デバイスに配布されたシステム防御ポリシーを、表示、削除、および有効化することができます。有効化されたポリシーが優先度に基づいてアクティブなポリシーになると、そのポリシーに関連付けられたフィルタがアクティブになります。

[システム防御ポリシーの管理] ウィンドウを開くには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[システム防御]** セクションにある **[ポリシー]** リンクをクリックします。ウィンドウが開き、HPCA コンソールを介して作成され vPro デバイスに配布されたシステム防御ポリシーが表示されます。

システム防御ポリシーのビューをリフレッシュするには

1 [システム防御ポリシーの管理] ウィンドウを開くには で説明した手順に従って、[システム防御ポリシーの管理] ウィンドウを開きます。

2 ツールバーの  リフレッシュ アイコンをクリックします。

有線 NIC に配布されたポリシーと無線 NIC に配布されたポリシーの間で切り替えるには

この手順は、有線と無線の両方のネットワーク インターフェイス カード (NIC) を装着している vPro デバイスのみに適用されます。

1 [システム防御ポリシーの管理] ウィンドウを開くには で説明した手順に従って、[システム防御ポリシーの管理] ウィンドウを開きます。デバイスに 2 枚の NIC が装着されている場合、ウィンドウが開き、vPro デバイスの有線 NIC に配布されたシステム防御ポリシーが表示されます。

2  無線アイコンをクリックします (このアイコンは、vPro デバイスに、有線と無線の両方の NIC が装着されている場合に表示されます)。ウィンドウが開き、vPro デバイスの無線 NIC に配布されたシステム防御ポリシーが表示されます。

3  有線アイコンをクリックすると、ウィンドウが切り替わり、vPro デバイスの有線 NIC に配布されたシステム防御ポリシーが表示されます。

システム防御ポリシーの詳細を表示するには

1 [システム防御ポリシーの管理] ウィンドウを開くには で説明した手順に従って、[システム防御ポリシーの管理] ウィンドウを開きます。

2 システム防御ポリシーの詳細を表示するには、そのポリシーのポリシー名リンクをクリックします。[システム防御ポリシーの詳細] ウィンドウが開き、選択したポリシーの詳細が表示されます。

3 **[次へ]** をクリックすると、そのポリシーに関連付けられているフィルタが表示されます。

4 vPro デバイスに 2 枚の NIC が装着されている場合は、156 ページの「有線 NIC に配布されたポリシーと無線 NIC に配布されたポリシーの間で切り替えるには」で説明したとおり、トグル アイコンをクリックし、他方の NIC についても同じ手順を繰り返します。

エージェント存在ポリシーを設定するには

1 [システム防御ポリシーの管理] ウィンドウを開くには で説明した手順に従って、[システム防御ポリシーの管理] ウィンドウを開きます。

2 ウォッチドッグ アクションによって有効化されるエージェント存在ポリシーとして設定するポリシーの横のチェック ボックスをオンにします。エージェント存在ポリシーとして選択できるポリシーは 1 つのみです。

3 ツールバーの 設定アイコンをクリックします。選択したポリシーがエージェント存在ポリシーになります。このポリシーは、エージェント ウォッチドッグ アクションを介して有効にできます。有効化されているシステム防御ポリシーよりもこのポリシーの優先度が高ければ、このポリシーがアクティブなポリシーになります。

4 vPro デバイスに 2 枚の NIC が装着されている場合は、156 ページの「有線 NIC に配布されたポリシーと無線 NIC に配布されたポリシーの間で切り替えるには」で説明したとおり、トグル アイコンをクリックし、他方の NIC についても同じ手順を繰り返します。

システム防御ポリシーを有効化するには

1 [システム防御ポリシーの管理] ウィンドウを開くには で説明した手順に従って、[システム防御ポリシーの管理] ウィンドウを開きます。

2 有効にするポリシーの横にあるチェック ボックスをオンにします。選択できるポリシーは 1 つのみです。

3 ツールバーの 有効化アイコンをクリックします。選択したポリシーが、新しいデフォルトのシステム防御ポリシーになります。

4 vPro デバイスに 2 枚の NIC が装着されている場合は、156 ページの「有線 NIC に配布されたポリシーと無線 NIC に配布されたポリシーの間で切り替えるには」で説明したとおり、トグル アイコンをクリックし、他方の NIC についても同じ手順を繰り返します。

システム防御ポリシーを削除するには

1 [システム防御ポリシーの管理] ウィンドウを開くには で説明した手順に従って、[システム防御ポリシーの管理] ウィンドウを開きます。

2 削除する各ポリシーの横にあるボックスをオンにします。

3 ツールバーの 削除アイコンをクリックします。選択したポリシーが、その vPro デバイスのシステム防御ポリシー テーブルから削除されます。

4 vPro デバイスに 2 枚の NIC が装着されている場合は、156 ページの「有線 NIC に配布されたポリシーと無線 NIC に配布されたポリシーの間で切り替えるには」で説明したとおり、トグル アイコンをクリックし、他方の NIC についても同じ手順を繰り返します。

システム防御ポリシーのインターフェイスを使用して、次の作業を実行できます。

- vPro デバイスのシステム防御ポリシーを表示する。
- システム防御ポリシーを有効化し、優先度に基づいてアクティブなポリシーになることができるようにする。
- ポリシーをエージェント存在ポリシーとして設定し、エージェント ウォッチドッグ アクションによって有効化できるようにする。このポリシーの優先度のほうがが高ければ、このポリシーがアクティブなポリシーになります。
- 不要になったポリシーを削除する。

vPro デバイスのヒューリスティックの管理

ワークスペースの **[システム防御]** 領域は、vPro デバイスのみで使用できます。この領域では、特定の vPro デバイスに配布されたヒューリスティック情報を表示および削除できます。

ヒューリスティック管理のウィンドウを開くには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[システム防御]** セクションにある **[ヒューリスティック]** リンクをクリックします。ウィンドウが開き、HPCA コンソールを介して作成され vPro デバイスに配布されたヒューリスティック情報が表示されます。

ヒューリスティック ビューをリフレッシュするには

1 ヒューリスティック管理のウィンドウを開くには で説明した手順に従って、[ヒューリスティックの管理] ウィンドウを開きます。

2 ツールバーの リフレッシュ アイコンをクリックします。

ヒューリスティック仕様の詳細を表示するには

1 ヒューリスティック管理のウィンドウを開くには で説明した手順に従って、[ヒューリスティックの管理] ウィンドウを開きます。

2 詳細を表示するヒューリスティックのヒューリスティック名リンクをクリックします。[ヒューリスティックの詳細] ウィンドウが開き、ヒューリスティックの仕様が表示されます。

3 **[閉じる]** をクリックして、詳細ウィンドウを閉じます。

デバイスの NIC インターフェイスのヒューリスティック状態情報を表示するには

1 ヒューリスティック管理のウィンドウを開くには で説明した手順に従って、[ヒューリスティックの管理] ウィンドウを開きます。

2 ヒューリスティックの NIC インターフェイス状態情報を表示するには、そのヒューリスティックの NIC タイプ リンクをクリックします。[ヒューリスティック状態情報] ウィンドウが開き、個々の NIC インターフェイスの状態情報が表示されます。この情報により、ヒューリスティック条件に適合したことがあるかどうか、および実行されたアクションが分かります。

3 **[閉じる]** をクリックして、[ヒューリスティック状態情報] ウィンドウを閉じます。

ヒューリスティック アクションをクリアするには

1 ヒューリスティック管理のウィンドウを開くには で説明した手順に従って、[ヒューリスティックの管理] ウィンドウを開きます。

2 ヒューリスティックに関連付けられたアクションをクリアするには、そのヒューリスティックの横にあるチェック ボックスをオンにします。

3 ツールバーの ヒューリスティック アクションのクリア アイコンをクリックします。選択したヒューリスティックに関連付けられたアクションがクリアされます。その結果、送信パケットがブロックされなくなり、疑わしいポートが開き、指定したシステム防御ポリシーが非アクティブ化されます。

ヒューリスティックを削除するには

1 ヒューリスティック管理のウィンドウを開くには で説明した手順に従って、[ヒューリスティックの管理] ウィンドウを開きます。

2 削除する各ヒューリスティックの横にあるボックスをオンにします。

3 ツールバーの 削除アイコンをクリックします。選択したヒューリスティックが、その vPro デバイスのヒューリスティック テーブルから削除されます。

ヒューリスティック インターフェイスを使用して次の作業が実行できます。

- vPro デバイスのヒューリスティックを表示する。
- 不要になったヒューリスティック情報を削除する。

vPro デバイスのエージェント ウォッチドッグの管理

ワークスペースの **[システム防御]** 領域は、vPro デバイスのみで使用できます。この領域では、特定の vPro デバイスに配布されたエージェント ウォッチドッグを表示および削除できます。

エージェント ウォッチドッグの管理のウィンドウを開くには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[システム防御]** セクションにある **[エージェント ウォッチドッグ]** リンクをクリックします。ウィンドウが開き、HPCA コンソールを介して作成され vPro デバイスに配布されたエージェント ウォッチドッグが表示されます。

エージェント ウォッチドッグの表示をリフレッシュするには

1 エージェント ウォッチドッグの管理のウィンドウを開くには で説明した手順に従って、[エージェント ウォッチドッグの管理] ウィンドウを開きます。

2 ツールバーの リフレッシュ アイコンをクリックします。

エージェント ウォッチドッグの詳細を表示するには

1 エージェント ウォッチドッグの管理のウィンドウを開くには で説明した手順に従って、[エージェント ウォッチドッグの管理] ウィンドウを開きます。

2 詳細を表示するエージェント ウォッチドッグのエージェント ウォッチドッグ名リンクをクリックします。[エージェント ウォッチドッグの詳細] ウィンドウが開き、選択したウォッチドッグの詳細が表示されます。

3 **[閉じる]** をクリックして、詳細ウィンドウを閉じます。

エージェント ウォッチドッグ削除するには

1 エージェント ウォッチドッグの管理のウィンドウを開くには で説明した手順に従って、[エージェント ウォッチドッグの管理] ウィンドウを開きます。

2 削除する各ウォッチドッグの横にあるボックスをオンにします。

3 ツールバーの削除アイコンをクリックします。選択したエージェント ウォッチドッグが、その vPro デバイスのエージェント ウォッチドッグ テーブルから削除されます。

エージェント ウォッチドッグ インターフェイスを使用して、次の操作を実行できます。

- vPro デバイスのウォッチドッグ エージェントを表示する。
- 不要になったエージェント ウォッチドッグを削除する。

vPro デバイスのフロント パネル設定の設定

ワークスペースの **[全般設定]** 領域は、vPro デバイスのみで使用できます。この領域では、リモート電源操作の最中に、vPro デバイスのキーボードと電源ボタンをロックおよびロック解除できます。

フロント パネル設定は、ターゲット デバイスの機能に基づいて、ユーザーが設定できます。フロント パネル設定機能は、個々の vPro デバイスの BIOS に依存しています。デバイスの BIOS でフロント パネル設定がサポートされていない場合、この機能を HPCA コンソールから制御することはできません。サポート関連情報の詳細については、ハードウェア ベンダーに問い合わせてください。

フロント パネル設定を設定するには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[全般設定]** セクションにある **[フロント パネルの設定]** リンクをクリックします。[フロント パネルの設定] ダイアログが表示されます。

5 **[ここ]** リンクをクリックして、ダイアログの **[フロント パネルの設定]** セクションを有効化します。フロント パネル設定がデバイスによってサポートされている場合、デフォルトのロック設定は **[はい]** に設定されています。

6 リモート電源操作の最中に、vPro デバイスのキーボードや電源ボタンをロックする場合は、デフォルトの設定のままにします。

7 **[更新]** をクリックします。確認メッセージが画面に表示されます。

8 **[閉じる]** をクリックして、ダイアログを終了します。

フロント パネル設定を使用すると、HPCA コンソールからリモート電源操作を実行しているとき、そのデバイスに対する直接の操作を確実に回避できます。

vPro デバイスのフラッシュ メモリ書き換え回数制限のリセット

ワークスペースの **[全般設定]** 領域は、vPro デバイスのみで使用できます。この領域では、vPro デバイスのフラッシュ メモリ書き換え回数制限をリセットできます。フラッシュ メモリの詳細については、132 ページの「共通ユーティリティの管理」を参照してください。

フラッシュ メモリ書き換え回数制限をリセットするには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する vPro デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[全般設定]** セクションにある **[フラッシュ メモリ書き換え回数制限のリセット]** リンクをクリックします。[フラッシュ メモリ書き換え回数制限のリセット] ダイアログが表示されます。

5 **[リセット]** をクリックします。確認メッセージが表示されます。

6 **[OK]** をクリックして続行します。デバイスの 3PDS メモリのカウンタがゼロにリセットされます。

フラッシュ メモリ書き換え回数制限のリセットを使用すると、vPro デバイスの 3PDS カウンタ (フラッシュ メモリの劣化防止メカニズムとして機能) をリセットできます。この機能により、この非揮発性メモリ ストアへの書き込み操作を継続できるようになります。

DASH デバイスの起動設定の設定

ワークスペースの **[設定の設定]** 領域は、DASH デバイスのみで使用できます。DASH デバイスでは、複数のブート設定を設定することができます。使用可能なブート設定の設定の中から起動プロセスに使用するものを選択できます。

各ブート設定の設定には、使用可能な起動元 (ハード ドライブ、CD、USB など) をいくつでも関連付けることができます。また、各ブート設定の設定では、関連付けられた複数の起動元の起動順も設定できます。同じ起動元を複数の異なるブート設定の設定に関連付けることもできます。

ワークスペースのこの領域では、DASH デバイスに対してリモート操作を実行しているとき、使用可能なブート設定の設定の確認、一回限りのブート設定の設定、起動順の変更を行うことができます。143 ページの「電源状態の変更」を参照してください。

起動設定を設定するには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[デバイス管理]** をクリックします。[デバイス管理] ウィンドウが表示されます。

3 管理する DASH デバイスのホスト名リンクをクリックします。管理ウィンドウが表示されます。

4 ウィンドウ左側の **[設定の設定]** セクションにある **[ブート設定]** リンクをクリックします。ブート設定リストが表示されます。

> 現在、Broadcom DASH デバイスで使用可能なブート設定の設定は、**ブート設定の設定 1** と **ブート設定の設定 2** の 2 つのみです。

リストは、ブート設定の設定について次のことを示します。

— **[デフォルト]**: オンにすると、コンピュータ システム製造メーカーがデフォルトのブート設定としてタグ付けしたブート設定の設定になります。**[デフォルト]** の設定は、ブート プロセス中にどのブート設定が適用されるかに影響 *しません*。

— **[次へ]**: オンにすると、**[次回のみ]** が選択されている場合、ブート設定の設定が DASH デバイスの次のブート (およびその後の再起動) 中に使用されます。

> 現在の Broadcom DASH デバイスの場合、**[ブート設定の設定 1]** は常に **[次へ]** のブート設定の設定になり、変更できません。

— **[次回のみ]**: オンにすると、DASH デバイスの次のブート中にブート設定の設定が使用されますが、その次のブート中には使用されません。**[次回のみ]** のブート設定の設定は、**[次へ]** のブート設定の設定より優先されます。

— **[現在のブート設定]**: オンにすると、DASH デバイスが前回正常にブートされたときに使用されたブート設定の設定になります。

> 現在、**[一回限りのブート設定]** が選択されていると、**[次へ]** カラムおよび **[次回のみ]** カラムのみにチェック マークが表示されます。

— **[起動順序]**: ブート設定の設定に接続される起動元および起動順序。

> **[起動順序]** カラムの起動元が緑色のテキストで表示される場合は、これらの起動元デバイスが現在のブート プロセスで使用されていることを示すエラー条件を表します。これはハードウェアのエラーです。デバイスが緑色のテキストで表示される場合は、次の手順で説明するように、ブート設定ウィザードを使用して起動順序を変更する必要があります。

5 ブート設定リストで管理するブート設定の設定を選択します。

6 ブート設定リスト テーブルのツールバーにある  ブート設定パラメータ アイコンのプルダウン メニューから、実行するブート設定オプションを選択します。現在、次のオプションしか選択できません。

— **[一回限りのブート設定]**: デバイスの電源を次回入れるとき、またはデバイスを次回再起動するときの起動順序を変更します。この回以降は、現在のブート設定の起動順序に戻ります。

このオプションを選択すると、ブート設定の更新ウィザードが表示されます。

7 **[次へ]** をクリックして続行します。[設定] ウィンドウが表示されます。

8 **[現在の起動順序]** リストでブート デバイスを選択し、**[追加]** をクリックして **[新しい起動順序]** リストにそのブート デバイスを追加します。**[新しい起動順序]** リストからブート デバイスを削除するには、デバイスを選択して **[削除]** をクリックします。

[現在の起動順序] リストには、デバイスの起動元となるすべてのブート デバイスが表示されます。現在の起動順序で現在使用中のブートデバイスは、黒いテキストで表示されます。使用可能だが、現在の起動順序で使用されていないブート デバイスは、グレイで表示されます。

9 新しい起動順序で問題ない場合は、**[次へ]** をクリックします。[完了] ウィンドウにステータス情報が表示されます。

10 **[閉じる]** をクリックして、ウィザードを終了します。加えた変更内容はブート設定リストに反映されます。

DASH デバイスのブート設定の設定を表示したり変更したりする機能は、リモート電源管理の問題のトラブルシューティングに役立つツールとして使用できます。

9 グループ管理

この章では、HPCA コンソールを使用して vPro デバイスで構成される Client Automation デバイス グループを管理する方法について説明します。vPro デバイスで構成される Client Automation グループは、デバイスの電源の状態、オペレーティング システムの状態、または管理エージェントの有無に関係なくリモートで管理することができます。

HPCA コンソールの **[操作]** タブのアウトバンド管理オプションの 1 つに **[グループ管理]** があります。

このオプションは、vPro デバイスの管理を選択した場合のみ HPCA コンソールに表示されます。

このオプションにより、次の管理が可能になります。

- 複数の vPro デバイス グループの管理
- 個別の vPro デバイスの管理

複数の vPro デバイス グループの管理

グループを管理する場合、次の作業を行うことにより表示されるグループ、およびグループ リスト内でのグループの表示順を指定できます。

- 検索条件に基づいて特定のグループを検索する。
- 一度に表示するグループの数を選択して、見やすいように一部のグループのみが表示されるようにします。
- カラム見出しに基づいてグループをソートする。

グループ リストのツールバーにあるアイコンを使用して、複数のグループを同時に管理できます。

表 18　　グループ リストのツールバー

アイコン	機能
	リストに表示されているグループをリフレッシュします。
	リストに表示されているデバイス グループと Client Automation リポジトリを同期します。
	選択されているグループに対して電源管理タスクを実行します。
	選択されているグループに対して警告メッセージ予約を管理します。
	選択されているグループにローカル エージェント ソフトウェア リストを配布します。
	デバイス グループをプロビジョニングします。

表 18　　グループ リストのツールバー (cont'd)

アイコン	機能
	選択されているグループに対してシステム防御ポリシーを配布および回収します。
	選択されているグループに対してエージェント ウォッチドッグを配布および回収します。
	選択されているグループに対してヒューリスティックを配布および回収します。

デバイス リスト ツールバーの表に示しているように、アイコンを使用すると、グループ リストに表示されているグループ デバイス情報を現在のデバイス情報と同期して、情報を手動でリロードできます。手動によるリロードに加え、OOBM では定期的な間隔でのグループ リストの自動リロードも可能です。この時間間隔は、(*<HPCA_Install_DIR>*\oobm\conf\ ディレクトリにある) config.properties ファイルで group_synchronization_timeperiod パラメータの値を設定することによって設定できます。

この同期時間間隔のデフォルト値はゼロ (自動同期を行わない) です。自動同期を行う場合は、この値をゼロ以外に設定してください。単位は分です。

[複数グループ] セクション

複数のグループを選択するには

1. HPCA コンソールにログインして、**[操作]** タブを選択します。
2. 左側のナビゲーション ペインの **[アウトバンド管理]** の下で、**[グループ管理]** をクリックします。[グループ管理] ウィンドウが開いて、すべての Client Automation グループが表示されます。vPro デバイスで構成されているグループは、テーブル内でアクティブなリンクとして表示されます。アクティブなリンクは、コンソールを使用して管理可能であることを示しています。
3. グループのチェック ボックスをオンにするか、左上にあるすべてを選択するチェック ボックスをオンにして、アクセスするグループを選択します。選択しやすいように、特定の条件を満たすグループのみに検索を絞り込んだり、グループを並べ替えたりすることができます。

グループ リストと Client Automation リポジトリの同期

グループ リストと Client Automation リポジトリを同期するには

- グループ リストを直ちに Client Automation リポジトリからリロードするには、リロード アイコンのプルダウン メニューから **[[グループを直ちにリロード]** を選択します。このオプションを選択すると、直ちにリロードが実行され、プロセスが発生するとグループ リスト ウィンドウ内にその内容が表示されます。プロセスが完了すると、Client Automation リポジトリで検出された最新のグループがグループ リストに表示されます。
- バックグラウンド プロセスとして Client Automation リポジトリからグループをリロードするには、リロード アイコンのプルダウン メニューから **[バックグラウンドでグループをリロード]** を選択します。このオプションを選択すると、グループ リスト ウィンドウにはプロセス

の内容が表示されません。バックグラウンド プロセスのステータスは、  リロード アイコンのプルダウン メニューから **[リロード ステータスの表示]** を選択することにより確認できます。プロセスの完了時にリロードされたグループ リストを確認するには、  リフレッシュ アイコンをクリックする必要があります。

電源管理

デバイス グループの電源を管理するには

1 複数のグループを選択するには で説明した手順で管理するグループを選択します。

2 ツールバーの  電源管理アイコンをクリックします。電源操作ウィザードが表示されます。

3 **[次へ]** をクリックします。[オプション] ウィンドウが表示されます。

4 選択したグループで実行する電源操作を選択します。

5 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

6 **[次へ]** をクリックします。[完了] ウィンドウが開いて、操作の結果が表示されます。

7 **[閉じる]** をクリックして、ウィザードを終了します。

この機能を使用すると、複数のデバイス グループの電源のオン / オフを特定の時刻に効果的に行えるため、コストを抑えることが可能です。

警告メッセージ予約の管理

デバイス グループの警告メッセージ予約を管理するには

1 複数のグループを選択するには で説明した手順で管理するグループを選択します。

2  警告メッセージ予約管理アイコンをクリックします。警告メッセージ予約管理ウィザードが表示されます。

3 **[次へ]** をクリックします。[オプション] ウィンドウが表示されます。

4 警告メッセージ予約を実行するかキャンセルするかを選択します。

5 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

6 **[次へ]** をクリックします。[完了] ウィンドウが開いて、操作の結果が表示されます。

7 **[閉じる]** をクリックして、ウィザードを終了します。

この機能を使用して、適切なイベント警告が HPCA コンソールに送信されるように複数のデバイス グループに対して警告メッセージを予約およびキャンセルできます。

ローカル エージェント ソフトウェア リストの配布

ローカル エージェント ソフトウェア リストを配布するには

1 複数のグループを選択するには で説明した手順で管理するグループを選択します。

2  ソフトウェア リスト配布アイコンをクリックします。これで、ソフトウェア配布ウィザード開始されます。

3 **[次へ]** をクリックします。[ソフトウェア] ウィンドウが表示されます。

4 選択したグループに配布するソフトウェア リストに追加するソフトウェア名を選択します。

5 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

6 **[次へ]** をクリックします。[完了] ウィンドウが開いて、操作の結果が表示されます。

7 **[閉じる]** をクリックして、ウィザードを終了します。

この機能を使用して、ターゲットの vPro デバイス グループでローカル エージェントに監視させるアプリケーションのカスタム リストを作成する元となる、ソフトウェア アプリケーションのマスター リストを作成できます。

プロビジョニング

詳細については、vPro デバイスのプロビジョニングを参照してください。

プロビジョニング操作を実行するには

1 複数のグループを選択するにはで説明した手順で管理するグループを選択します。

2 プロビジョニング アイコンのプルダウン メニューから、**[プロビジョニング操作の実行]** を選択します。プロビジョニング操作ウィザードが表示されます。

3 **[次へ]** をクリックします。[オプション] ウィンドウが表示されます。

4 選択したグループに対して実行するプロビジョニング操作を選択します。プロビジョニング操作の説明については、123 ページの「プロビジョニング タスクの実行」を参照してください。

5 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

6 **[次へ]** をクリックします。[完了] ウィンドウが開いて、操作の結果が表示されます。

7 **[閉じる]** をクリックして、ウィザードを終了します。

プロビジョニング ステータス ログを表示するには

1 複数のグループを選択するにはで説明した手順で管理するグループを選択します。

2 プロビジョニング アイコンのプルダウン メニューから、**[プロビジョニング ステータス ログの表示]** を選択します。[プロビジョニング ステータス ログ] ウィンドウが表示されます。このログに、プロビジョニング操作のステータスが表示されています。

この機能を使用すると、デバイス グループで効果的なプロビジョニング操作を行うことができ、また最小限の操作で結果を表示できます。

システム防御ポリシーの配布

システム防御ポリシーを配布するには

1 複数のグループを選択するにはで説明した手順で管理するグループを選択します。

2 システム防御ポリシーの管理アイコンのプルダウン メニューから、**[システム防御ポリシーの配布]** を選択します。ポリシー配布ウィザードが表示されます。

3 **[次へ]** をクリックします。[ポリシー] ウィンドウが表示されます。

4 選択したグループに配布するシステム防御ポリシーを選択します。

5 **[次へ]** をクリックします。[設定] ウィンドウが表示されます。

6 プルダウン メニューから、デバイス グループの有線および無線 NIC に割り当てるエージェント存在ポリシーおよびシステム防御ポリシーを選択します。

7 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

8 **[次へ]** をクリックします。[完了] ウィンドウが開いて、操作の結果が表示されます。

9 **[閉じる]** をクリックして、ウィザードを終了します。

システム防御ポリシーを回収するには

1 複数のグループを選択するにはで説明した手順で管理するグループを選択します。

2 システム防御ポリシーの管理アイコンのプルダウン メニューから、**[システム防御ポリシーの回収]** を選択します。ポリシー回収ウィザードが表示されます。

3 **[次へ]** をクリックします。[ポリシー] ウィンドウが表示されます。

4 選択したグループから回収するポリシーを選択します。

5 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

6 **[次へ]** をクリックします。[完了] ウィンドウが開いて、操作の結果が表示されます。

7 **[閉じる]** をクリックして、ウィザードを終了します。

この機能を使用すると、複数の vPro デバイス グループに複数のシステム防御ポリシーを簡単に配布することができ、システムを悪意のある攻撃から保護することができます。

エージェント ウォッチドッグの配布

エージェント ウォッチドッグを配布するには

1 複数のグループを選択するにはで説明した手順で管理するグループを選択します。

2 エージェント ウォッチドッグの管理アイコンのプルダウン メニューから、**[エージェント ウォッチドッグの配布]** を選択します。ウォッチドッグ配布ウィザードが表示されます。

3 **[次へ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。

4 選択したグループに配布するウォッチドッグを選択します。

5 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

6 **[次へ]** をクリックします。[完了] ウィンドウが開いて、操作の結果が表示されます。

7 **[閉じる]** をクリックして、ウィザードを終了します。

エージェント ウォッチドッグを回収するには

1 複数のグループを選択するにはで説明した手順で管理するグループを選択します。

2 エージェント ウォッチドッグの管理アイコンのプルダウン メニューから、**[エージェント ウォッチドッグの回収]** を選択します。ウォッチドッグ回収ウィザードが表示されます。

3 **[次へ]** をクリックします。[ウォッチドッグ] ウィンドウが表示されます。

4 選択したグループから回収するウォッチドッグを選択します。

5 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

6 **[次へ]** をクリックします。[完了] ウィンドウが開いて、操作の結果が表示されます。

7 **[閉じる]** をクリックして、ウィザードを終了します。

この機能を使用すると、複数の vPro デバイス グループに複数のエージェント ウォッチドッグを簡単に配布することができ、これらのシステムのローカル エージェントを監視できます。ローカル エージェントを監視することにより、これらのエージェントが今度はプロビジョニング済みの

デバイス上で実行中のセキュリティ ソフトウェアを監視するため、ネットワークのセキュリティが強化されます。ユーザーの誤った操作によりまたはその他の原因によりセキュリティ ソフトウェアの実行が停止した場合、ウォッチドッグによってこのイベントをシステム管理者に警告できます。

ヒューリスティックの配布

ヒューリスティックを配布するには

1 複数のグループを選択するにはで説明した手順で管理するグループを選択します。

2 ヒューリスティックの管理アイコンのプルダウン メニューから、**[ヒューリスティックの配布]** を選択します。ヒューリスティック配布ウィザードが開始されます。

3 **[次へ]** をクリックします。[ヒューリスティック] ウィンドウが表示されます。

4 選択したグループに配布するヒューリスティックを選択します。

5 **[次へ]** をクリックします。[設定] ウィンドウが表示されます。

6 プルダウン メニューから、デバイス グループの有線および無線 NIC に割り当てるヒューリスティックを選択します。

7 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

8 **[次へ]** をクリックします。[完了] ウィンドウが開いて、操作の結果が表示されます。

9 **[閉じる]** をクリックして、ウィザードを終了します。

ヒューリスティックを回収するには

1 複数のグループを選択するにはで説明した手順で管理するグループを選択します。

2 ヒューリスティックの管理アイコンのプルダウン メニューから、**[ヒューリスティックの回収]** を選択します。ヒューリスティック回収ウィザードが表示されます。

3 **[次へ]** をクリックします。[ヒューリスティック] ウィンドウが表示されます。

4 選択したグループから回収するヒューリスティックを選択します。

5 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

6 **[次へ]** をクリックします。[完了] ウィンドウが開いて、操作の結果が表示されます。

7 **[閉じる]** をクリックして、ウィザードを終了します。

この機能を使用すると、複数の vPro デバイス グループに複数のヒューリスティックを簡単に配布することができ、ワームに感染したデバイスのワーム封じ込めを行えます。

個別の vPro デバイスの管理

[グループ管理] ウィンドウに表示されているグループ リスト テーブルには、グループ タイプ、グループ内のデバイス数、グループの作成日、およびその他の属性が表示されます。

掘り下げてグループ内の個々のデバイスを管理するには、テーブルの [説明] 列の下にあるグループ名のリンクをクリックします。[グループの詳細] ウィンドウが表示されます。このウィンドウには、次のタブ セクションあります。

- [全般] タブ
- [プロパティ] タブ

- [デバイス] タブ

[全般] タブ

[全般] タブには [共通のタスク] と [要約] 領域があります。[共通のタスク] 領域には、他のタブ セクションで提供される機能へのショートカットとして動作するリンクがあります。[要約] 領域にはデバイス グループに関する統計が表示されます。

[プロパティ] タブ

[プロパティ] タブには、選択したグループのプロパティが表示されます。グループのプロパティについて理解を深めるには、『HP Client Automation Core および Satellite Standard ユーザー ガイド』を参照してください。

[デバイス] タブ

[デバイス] タブには選択したグループに属する vPro デバイスのリストが表示されます。グループ内の複数のデバイスまたは個々のデバイスを管理できます。デバイス管理を参照してください。

10 警告の通知

この章では、vPro デバイスで発生した警告の表示 について説明します。

vPro デバイスで発生した警告の表示

HPCA コンソールでは、イベントの警告を表示できます。これらの警告は、プロビジョニング済みの vPro デバイスによってイベントの発生時に生成され、HPCA コンソールに送信されます。そのデバイスに対する警告メッセージ予約を登録していれば、警告が表示されます。

警告の表示をリフレッシュするには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 **[アウトバンド管理]** の下で、**[警告の通知]** をクリックします。[警告の通知] ウィンドウが表示されます。このタブには、警告メッセージ予約を登録してある vPro デバイスによって生成された警告が表示されます。

3 ツールバーの リフレッシュ アイコンをクリックします。

vPro 警告に関する詳細を表示するには

1 HPCA コンソールにログインして、**[操作]** タブを選択します。

2 **[アウトバンド管理]** の下で、**[警告の通知]** をクリックします。[警告の通知] ウィンドウが表示されます。このタブには、警告メッセージ予約を登録してある vPro デバイスによって生成された警告が表示されます。

3 [詳細] カラムの詳細アイコン をクリックします。ウィンドウが開き、選択した警告の詳細なプロパティが表示されます。

警告メッセージ予約を登録することで、即座の対応を必要とする重要度の高いイベント警告が発生しているかどうかを確認できます。

11 トラブルシューティング

この章では、HPCA コンソールのアウトバンド管理機能の使用時に起こりうる最も一般的な問題のデバッグに関する情報を一般的な問題に掲載しています。

また、OOBM データが破損した場合や製品の再インストールが必要になった場合に備えるバックアップの最善実践についても OOBM データのバックアップで説明します。

アウトバンド管理の通信に使用するポートの要件をポート情報の要約にまとめてあります。

さらに、HP サポートに連絡する前に答えを用意しておく必要がある質問のチェックリストを質問チェックリストに掲載しています。

一般的な問題

一般的に問題の発生時には、まず `C:\Program Files\Hewlett-Packard\HPCA\tomcat\logs` (HPCA をデフォルトの場所にインストールした場合) ディレクトリにあるログ ファイルを確認することをお勧めします。ログ ファイルには、HPCA コンソールからのすべての出力が含まれています。

また、エージェントに関連した問題の場合は、vPro クライアント デバイスのイベント ビューア (**[スタート] > [設定] > [コントロール パネル] > [管理ツール] > [イベント ビューア]**) を開きます。

このセクションでは、次の領域のトラブルシューティングについて取り上げます。

- 全般
- プロビジョニング
- 探索
- リモート操作
- 電源状態
- 再起動
- システム防御およびエージェント存在
- 無線
- 移行の問題

全般

vPro デバイス タイプの選択時に HPCA コンソールがハングアップする

表 19　　vPro デバイス タイプの選択時にコンソールがハングアップする

考えられる原因	解決策
CPU 使用率が過度に高いため (Tomcat が CPU の 100% を使用)、SCS サービスが Out of Band Management Service との通信に失敗しました。	この問題が持続する場合は、HPCA Tomcat Server を再起動します。

1 つのデバイス コンソールの場所に表示されるエラー ページがクリアされないエラー

表 20　　エラー ページがクリアされない

考えられる原因	解決策
Internet Explorer ブラウザのキャッシュがクリアされていません。Internet Explorer が再び開くまで、1 つのデバイス コンソールに表示されるエラー ページがクリアされない場合があります。	Internet Explorer のキャッシュを手動でクリアします。

HPCA コンソールでキーボードと電源ボタンをロックしない設定にしているのに、実際にはロックされている

表 21　　フロント パネルのロック動作の問題

考えられる原因	解決策
ロック動作は、vPro デバイスで動作している BIOS のバージョンにより異なります。一部のバージョンでは、デフォルトで電源ボタンとキーボードがロックされています。	ユーザーが BIOS の設定を変更できるデバイスもあります。設定変更可能な BIOS のバージョンについては、デバイスのドキュメントを参照してください。

有線 NIC を使用して vPro デバイスに接続できない

表 22　　有線 NIC を使用した vPro デバイスの接続問題

考えられる原因	解決策
次の原因が考えられます。 1. vPro デバイスがネットワークから削除されている。 2. vPro デバイス用の Web サービスが使用中である。	この場合、対象のデバイスを選択して、HPCA コンソールの Web サービス リクエストが vPro デバイスから再び取得されるように数秒待った後に、リポジトリ アイコンの [リフレッシュ] を使用して HPCA コンソール画面をリフレッシュします。

HPCA コンソールの使用時にタイムアウトが発生する

表 23　　HPCA コンソールのタイムアウト

考えられる原因	解決策
ネットワーク トラフィックが低速になっています。	タイムアウト期間を設定し直します。詳細については、48 ページの「IDE-R および SOL タイムアウト値の設定」を参照してください。

OOBM デバイス管理画面の警告のサブスクリプション ステータスが誤っている

表 24　　誤った警告のサブスクリプション ステータス

考えられる原因	解決策
この問題は、OOBM のサードパーティの依存関係が原因です。 HPCA が Windows Server 2008 にインストールされている場合、警告のサブスクリプション操作は正常に行われますが、[ステータス] カラムに誤ってレポートされます。このため、**[操作] > [アウトバンド管理] > [デバイス管理] > [警告のサブスクリプション]** を選択して、vPro デバイスで警告のサブスクリプション操作を実行するとエラーが発生します。	この問題に対する回避策はありません。

コンソールが長時間アイドル状態にあった後に [アウトバンド管理デバイスの詳細] ウィンドウにアクセスすると、ログイン画面に戻る。

表 25　　アイドル時間が長いと、ログイン画面に戻る

考えられる原因	解決策
データベースへのアクセスに関連した問題です。	ブラウザを閉じてから、新しいブラウザのセッションで HPCA コンソールに再ログインします。

[デバイス タイプの選択] ウィンドウで vPro デバイスを管理しているときに、SCS のプロパティを保存できない

表 26　　SCS にログインするために検証されるドメイン名

考えられる原因	解決策
SCS ログインに対して、ユーザー名がドメイン名 \ ユーザー名の形式で指定されていません。現在、この形式が必要とされ、この形式で認証が行われます。以前のリリースの OOBM では、ログイン名のドメイン名部分は無視されていました。その結果、正しくないドメイン名を入力しても受け付けられたように見えました。また、以前のリリースの OOBM では、例として示されたログイン ユーザー名 (provisionserver.yourenterprise.com \ Administrator) が正しくありませんでしたが、OOBM がドメイン名を無視するため動作していました。	SCS のプロパティを保存するには、ログイン ユーザー名を正しいドメイン名 \ ユーザー名の形式で指定する必要があります。

DASH の認証情報の変更後に DASH デバイスにアクセスできない

表 27　　DASH 認証情報の変更時の問題

考えられる原因	解決策
正しく動作しないのは、以前の認証情報がキャッシュされているためです。	DASH デバイスの認証情報を変更した場合は、Tomcat サービスを再起動して変更内容を有効化する必要があります。

vPro デバイスと SCS リポジトリの同期に長時間かかる

表 28　　vPro と SCS の同期の問題

考えられる原因	解決策
利用可能な vPro デバイスのリストを特定するには、いくつかの Web サービスの呼び出しが行われます。利用不可能なシステムの数、または現在のネットワーク経路指定の問題により、呼び出しには数分かかる場合があります。	Web サービスのタイムアウト値を減らすことでパフォーマンスを改善できます。ただし、タイムアウト値を減らすと、いくつかの利用可能なマシンにアクセスできなくなったり、電源や配布などのその他の操作を完了できなくなる可能性があります。

正しい vPro デバイスにアクセスできない

表 29　　vPro アクセスの問題

考えられる原因	解決策
IP アドレスの競合問題が発生しています。複数の vPro デバイスに同じ IP アドレスが割り当てられている可能性があります。	IP アドレスは一意である必要があります。ネットワーク管理者に連絡して、この問題を解決してください。

SOL 操作で、ハイパーターミナルにテキストが正しく表示されない

表 30　　ハイパーターミナルのテキスト表示の問題

考えられる原因	解決策
ハイパーターミナルの [右端で折り返す] オプションが有効になっている可能性があります。	ハイパーターミナルを開きます。[ファイル] から [プロパティ] を開きます。**[設定]** タブを選択します。**[ASCII 設定]** をクリックします。[ASCII 設定] ウィンドウで、[右端で折り返す] オプションをオフにします。

OOB デバイスへのソフトウェア リストの配布によって、TLS モードにネットワーク エラー 26 が発生する

表 31　　ソフトウェア リストの配布による TLS モードでのネットワーク エラーの発生

考えられる原因	解決策
HP Client Automation がインストールされたマシンのクライアント証明書が正しく設定されていません。 OOB デバイスへのソフトウェア リストの配布によって、TLS モードにネットワーク エラー 26 が発生します。このため、**[操作] > [アウトバンド管理] > [デバイス管理] > [ソフトウェア リストの配布]** を選択してソフトウェア リストの配布操作を実行するとエラーが発生します。	HP Client Automation がインストールされたマシンにクライアント証明書をインストールし、`config.properties` ファイルの「ca_server_commonname」プロパティの値に証明書の件名を指定してください。

管理対象の vPro デバイスに対して読み取り / 書き込み操作ができない

表 32　　メモリの書き換え回数制限の例外エラー

考えられる原因	解決策
vPro ストレージのフラッシュ メモリの書き換え回数が制限値を超過しました。 同じ vPro デバイスに対して読み取り / 書き込みアクセスを何度も繰り返すと、フラッシュ メモリの消耗保護メカニズムが働き、メモリの書き換え回数制限の例外エラーが発生する場合があります。カウンタが 200 に達すると、vPro デバイスはこれ以上の書き込み操作を受け付けません。	共通ユーティリティ アイコンのプルダウン メニューから、**[メモリの書き換え制限をリセット]** オプションを使用します。詳細については、132 ページの「共通ユーティリティの管理」を参照してください。

OOBM と SCS の I18N の問題

表 33　　SCS の I18N の問題

考えられる原因	解決策
ハードウェア BIOS や Intel SCS などの、基本となるコンポーネントや技術への依存関係。 HPCA コンソールは、英語以外のオペレーティング システムにもインストールできますが、ハードウェア BIOS や Intel SCS などの、基本となるコンポーネントや技術への依存関係からいくつかの制約があります。その結果、フィルタ、ウォッチドッグ、ポリシーなどユーザーが定義したアイテムのいくつかについては、**[設定] > [アウトバンド管理] > [vPro システム保護の設定]** を選択して英語以外の名前を入力することができません。BIOS セットアップ用の SOL コンソールは、サポートされる文字セットについてのみ機能します。同様に、その他の機能でも、英語以外のロケールでは期待通りには機能しないものがあります。数値、日付、時刻は、英語以外のオペレーティング システムのロケールでは表示されません。	この問題に対する回避策はありません。

OOBM 機能の日本語ロケールで、英語のパス区切り文字が表示される

表 34　英語以外のロケールで英語のパス区切り文字が表示される

考えられる原因	解決策
基盤の Intel SCS コンポーネントの制限です。 HPCA コンソールには、日本語ロケールで英語のパス区切り文字が表示されます。この問題は、OOBM 機能でのみ発生します。	この問題に対する回避策はありません。

管理対象の vPro デバイスに対して読み取り / 書き込み操作ができない

表 35　メモリの書き換え回数制限の例外エラー

考えられる原因	解決策
vPro ストレージのフラッシュ メモリの書き換え回数が制限値を超過しました。 同じ vPro デバイスに対して読み取り / 書き込みアクセスを何度も繰り返すと、フラッシュ メモリの消耗保護メカニズムが働き、メモリの書き換え回数制限の例外エラーが発生する場合があります。カウンタが 200 に達すると、vPro デバイスはこれ以上の書き込み操作を受け付けません。	共通ユーティリティ アイコンのプルダウン メニューから、**[メモリの書き換え制限をリセット]** オプションを使用します。詳細については、132 ページの「共通ユーティリティの管理」を参照してください。

プロビジョニング

プロビジョニング済みの vPro デバイスのステータスが、[vPro プロビジョニング] タブの [デバイス リスト] テーブルでプロビジョニング済みとして表示されない

表 36　vPrp ステータスの表示の問題

考えられる原因	解決策
テーブルが最新の情報でリフレッシュされていません。	Active Directory の探索機能を使用してデバイスを再探索します。この操作を行うと、デバイスのステータスが更新されます。

SCS 5.0 で、AMT ファームウェアのバージョンが 4.0 以前の vPro デバイスのプロビジョニング時に ACL を設定できない

表 37　vPro デバイスの ACL 設定の問題

考えられる原因	解決策
AMT ファームウェアのバージョンが 4.0 以前の vPro デバイスのプロファイルの作成時に、すべての領域が選択されています。	以前のバージョンの AMT ファームウェアのデバイスについては、別のプロファイルを作成します。このプロファイルでは、[リダイレクション]、[PT 管理]、[ハードウェア資産]、[リモート制御]、[回路ブレーカ]、[ネットワーク時間]、[全般情報]、および [ファームウェアの更新] 領域のみを選択してください。

vPro デバイスのプロビジョニング時に、コンソールで SCS エラーが発生する

表 38　　vPro デバイスのプロビジョニング時の SCS エラー

考えられる原因	解決策
Intel SCS から内部エラーが返されました。 HPCA コンソールを使用して vPro デバイスをプロビジョニングしようとする場合、コンソールに SCS エラーが発生する (エラーを知らせる以外、何も情報が無いエラー メッセージが表示される) 場合があります。	このエラーは無害であり、無視できます。プロビジョニング操作は vPro デバイス上で正常に開始されています。一定時間の経過後に操作の結果を検証して正常に開始されたことを確認できます。

vPro デバイスのプロビジョニングを複数回行うと、コンソールがログイン画面に戻る

表 39　　プロビジョニングによりログイン画面に戻る

考えられる原因	解決策
データベースへのアクセスに関連した問題です。	HPCA コンソールを使用して、ある vPro デバイスに複数回プロビジョニングを行うと、コンソールがログイン画面に戻る場合があります。このような場合、ブラウザを完全に閉じてから、HPCA コンソールに再ログインしてください。

探索

OOBM Agent がインストールされているが、vPro デバイスを探索できない

表 40　　vPro デバイス探索の失敗

考えられる原因	解決策
ポート 9998 がファイアウォールにブロックされている可能性があります。	vPro デバイスのポート 9998 がブロックされていないことを確認します。

管理対象の vPro デバイスに対してハードウェア資産が何も探索されない

表 41　　ハードウェア探索の問題

考えられる原因	解決策
この操作の間に、vPro デバイスで内部エラーが発生しました。	デバイスをシャット ダウンして電源コードを取り外し、10 ～ 15 秒待ってからデバイスを再起動します。

表 41　　ハードウェア探索の問題

vPro デバイスが正しくプロビジョニングされていません。	ターゲット vPro デバイスを再設定します。詳細については、37 ページの「MEBx による vPro デバイスの設定」を参照してください。
コンテナの容量が限られているため、追加の資産データを取得できません。システムに多数のデバイスがある場合に、この状態になることがあります。	一部のデバイスの接続を解除します。
ネットワークのトラフィック量が多いため、ハードウェア資産のクエリ中にネットワークエラーが発生しました。	しばらく待ってからコマンドを再発行します。

管理対象の vPro デバイスに対してソフトウェア資産が何も探索されない

表 42　　ソフトウェア探索の問題

考えられる原因	解決策
登録されているアプリケーションがありません。	VPro デバイスにインストールされているソフトウェアは、3PDS に登録する必要があります。HPCA コンソールは、アプリケーションの登録をサポートしません。
ネットワークのトラフィック量が多いため、ソフトウェア資産のクエリ中にネットワークエラーが発生しました。	しばらく待ってからコマンドを再発行します。

探索されたハードウェアおよびソフトウェア資産の一部のプロパティが空白である

表 43　　一部の探索されたハードウェアおよびソフトウェア資産の空白値

考えられる原因	解決策
デバイスのプロパティに情報がありません。	特定のプロパティの情報がデバイスに格納されていない場合、プロパティが空白なのは正常です。

Windows Server 2008 R2 が関連する一部の場合、HPCA を SCS に接続できず、vPro デバイスを探索できないことがある

表 44　　コンソールを SCS に接続できず、vPro デバイスを探索できない

考えられる原因	解決策
原因不明です。 Windows Server 2008-x64-R2 上に HPCA がインストールされており、SCS および Active Directory が Windows Server 2008-x64 が実行されているマシン上に両方インストールされている場合、HPCA を SCS に接続できません。	HPCA が Windows Server 2008-x64-R2 にインストールされており、Active Directory と SCS の両方を win2k8-x64 に配置する必要がある場合、Active Directory と SCS を win2k8-x64 が実行されているマシンとは異なる物理マシンまたは仮想マシン上にインストールします。

OOBM デバイス データベースに最新のデバイスがない場合、OOBM グループがリロードできない

表 45　　OOBM グループがリロードできない

考えられる原因	解決策
OOBM データベースは、最新のデバイスで更新されません。 OOBM グループがリロードできず、「指定された名前のデバイスはありません」エラーが表示されます。そのため、グループは更新されません。**[操作] > [アウトバンド管理] > [グループ管理] > [リロード]** を選択してグループのリロード操作を実行するとエラーが発生します。	OOBM デバイス探索操作をもう一度実行し、最新のデバイスに更新してください。この操作によって、グループのリロードに関するエラーは解決します。

有効な DASH デバイスの探索が失敗する

表 46　　DASH デバイス探索の失敗

考えられる原因	解決策
ネットワークのトラフィック量が多いことから、デバイスが時間内に応答できないために発生することがあります。	`HTTP_READ_TIMEOUT` および `HTTP_CONNECT_TIMEOUT` の設定値を増加させると、この問題が解決する場合があります。設定値の変更手順については、47 ページの「アウトバンド管理設定」を参照してください。

DASH デバイスが探索されるが、ホスト名ではなく IP アドレスで表示される

表 47　　DASH デバイスの探索の問題

考えられる原因	解決策
IP アドレスを指定してデバイスが探索されており、DNS Server で「DNS 逆探索」が設定されていません。	DASH デバイスの探索を試すときに、ホスト名を指定します。128 ページの「デバイスの探索」を参照してください。DNS Server で「DNS 逆探索」を設定していない場合は、デバイスの IP アドレスをホスト名に変換できません。表示されるのが IP アドレスかホスト名かに関係なく、すべての操作は期待どおりに動作します。

プロビジョニング済み vPro デバイスが探索されないか、使用不可として表示される

表 48　　vPro デバイスの探索の問題

考えられる原因	解決策
vPro デバイスは、以前にプロビジョニングされていても、プロビジョニングされなくなる場合があります。	vPro デバイスを再プロビジョニングします。詳細については、37 ページの「MEBx による vPro デバイスの設定」を参照してください。
vPro デバイスは、SCS データベースに存在していても、ドメイン コントローラから削除されていることがあります。	vPro デバイスが、正しい FQDN でドメイン コントローラに存在することを確認します。
DNS Server vPro デバイスの複数のエントリがあります。	vPro デバイスのエントリが DNS Server に 1 つしかないことを確認します。
HPCA コンソールのデバイス リストに表示されるものとは別の IP アドレスが、DHCP Server で vPro デバイス用に定義されています。	HPCA コンソールのデバイス ウィンドウに表示される vPro デバイスの IP アドレスが、DHCP Server のものと同一であることを確認します。

Client Automation グループのプロビジョニング済み vPro デバイスが、[グループの詳細] ウィンドウの [デバイス] タブに表示されない

表 49　　グループ デバイスの探索の問題

考えられる原因	解決策
Client Automation グループの vPro デバイスが FQDN とともにリストされていないことがあります。	FQDN を使用して Client Automation グループにデバイスをインポートし、このデバイスをグループに追加します。次に Client Automation グループを HPCA コンソールに再度読み込みます。

リモート操作

DASH デバイスでのリモート操作を実行するときに PuTTY コンソールが開かない

表 50　　PuTTY コンソールが開かない

考えられる原因	解決策
システムで別の PuTTY コンソールが実行されている可能性があります。ディスプレイをコンソール オプションを有効化した状態で DASH リモート操作を実行しているときに、別の PuTTY コンソールがシステムで実行されていると、PuTTY コンソールが開きません。	DASH リモート操作を実行する前に、他に PuTTY コンソールが実行されていないことを確認します。

リモート操作の実行時に telnet コンソールが表示されない

表 51　　telnet コンソールが表示されない

考えられる原因	解決策
特定のインターネット設定が正しく設定されておらず、telnet コンソールの表示が妨げられています。	[Internet Explorer] で **[ツール]** > **[インターネット オプション]** > **[詳細設定]** の順に移動します。**[スクリプトのデバッグを使用しない (Internet Explorer)]** オプションと **[スクリプトのデバッグを使用しない (その他)]** オプションが両方ともオンになっていることを確認します。
ActiveX コントロールのデフォルト セキュリティ設定により、telnet コンソールの表示が妨げられています。	[Internet Explorer] で、**[ツール]** > **[インターネット オプション]** > **[セキュリティ]** の順に移動します。**[レベルのカスタマイズ]** をクリックします。**[未署名の ActiveX コントロールのダウンロード]** および **[スクリプトを実行しても安全だとマークされていない ActiveX コントロールの初期化とスクリプトの実行]** で [有効にする] を選択します。

Windows Server 2003 64 ビット プラットフォームのクライアント コンソールで telnet セッションが開かない

表 52　　Windows Server 2003 64 ビットで telnet セッションが開かない

考えられる原因	解決策
OOBM はこのプラットフォームでは telnet 接続を開けません。	HyperTerminal を使用して vPro デバイスのテキスト コンソールを表示してください。また、DASH デバイスのテキスト コンソールを表示するには、PuTTY クライアントを設定してください。

PuTTY クライアントは、Windows 64 ビット プラットフォームで DASH クライアント コンソールを表示できない場合がある

表 53　　PuTTY クライアントは、Windows 64 ビットで DASH クライアント コンソールを表示できない

考えられる原因	解決策
PuTTY は、Windows 64 ビット システムではクライアント DASH デバイスと接続を確立できません。	この問題に対する回避策はありません。

デバイスのプロビジョン状態が変更後、vPro デバイスで OOBM リモート操作を行うとエラーが発生する

表 54　　プロビジョン変更後 vPro デバイスでリモート操作を行うとエラーが発生する

考えられる原因	解決策
OOBM データベースと SCS データベースの情報が一致していません。 vPro デバイスのプロビジョン状態を変更すると (TLS モードの変更および異なる SCS プロファイルでのデバイスの再プロビジョニングを含みます)、個別または複数の vPro デバイスでリモート操作ができません。	プロビジョン状態を変更するデバイスを選択し、**[操作]** > **[アウトバンド管理]** > **[デバイス管理]** の **[デバイス情報のリロード]** ボタンをクリックしてください。または、デバイスを選択せずに、**[デバイス情報のリロード]** ボタンをクリックしてください。後者は、完了までに時間がかかりますが、すべてのデバイス情報をリフレッシュするため、OOBM データベースに SCS データベースの情報と一致する最新の情報が読み込まれます。

vPro デバイスで OOBM リモート操作を実行しても何も起こらない

表 55　　リモート操作を実行しても何も起こらない

考えられる原因	解決策
• OOBM データベースと SCS データベースの情報が一致していません。 • ネットワークでデバイスが利用できない状態にあります。	[デバイスの詳細] ウィンドウを閉じて、新しいウィンドウを開いてください。エラー メッセージを確認できるようになります。この問題が OOBM と SCS データベース間の不整合によって発生している場合は、**[操作] > [アウトバンド管理] > [デバイス管理] > [すべてをリフレッシュ]** の **[デバイス情報のリロード]** ボタンをクリックしてください。

OOB DASH デバイスが起動順序に関係なくハードドライブから起動される

表 56　　DASH デバイスが必ずハードドライブから起動される

考えられる原因	解決策
Broadcom NetExtreme Gigabit Ethernet Plus NIC ベースのハードウェアに関する問題です。 起動順序に USB が含まれており、かつ USB から起動できない場合、起動順序のその他の起動元に関係なく、システムはハードドライブから起動されます。このため、**[操作] > [アウトバンド管理] > [デバイス管理] >** <*DASH Device*> **> [リモート操作]** を選択して、DASH デバイスで起動操作を実行するとエラーが発生します。	回避策はありません。

OOB DASH デバイスが、起動順序に指定されていないソースを含むすべての起動元を使用しようとする

表 57　　DASH デバイスが、指定に関係なく、すべての起動元を使用しようとする

考えられる原因	解決策
Broadcom NetExtreme Gigabit Ethernet Plus NIC ベースのハードウェアに関する問題です。 ユーザーが永続的な起動オプションを選択している場合、起動順序に指定されていないソースを含む、すべての起動元を使用しようとします。このため、**[操作] > [アウトバンド管理] > [デバイス管理] >** <*DASH Device*> **> [リモート操作]** を選択して、DASH デバイスで起動操作を実行するとエラーが発生します。	回避策はありません。

OOB DASH デバイスの初回起動元として不正なネットワーク コントローラが設定される

表 58　　DASH デバイスの初回起動元として不正なネットワーク コントローラが設定される

考えられる原因	解決策
Broadcom NetExtreme Gigabit Ethernet Plus NIC ベースのハードウェアに関する問題です。 Dash が有効なデバイスでは、ネットワークを初回ブート デバイスとして起動順序を変更すると、初回起動元として、Broadcom DASH NIC の代わりに埋め込みネットワーク コントローラが設定されます。その結果、Broadcom NIC からの PXE 起動に失敗します。	F10 の [セットアップ詳細] メニューを表示してください。[デバイス オプション] リストの [NIC PXE Option ROM のダウンロード] オプションを無効にすると、埋め込み NIC PXE オプション ROM の読み込みを防止できます。このオプションを無効にした後、Broadcom PXE からの起動を再試行してください。

リモート操作ウィザードの [タスク] ページから次のページに移動できない

表 59　　リモート操作ウィザードがフリーズする問題

考えられる原因	解決策
JRE のバージョンが正しくありません。	JRE バージョン 1.5 以降をインストールし、Internet Explorer のオプションを選択して JRE プラグインをインストールしてください。このオプションを選択するには、Internet Explorer で **[ツール] > [インターネット オプション] > [詳細設定]** の順に移動し、**[<applet> に JRE 1.5.*XX* を使用 (再起動が必要)]** オプションを選択します。JRE のインストールと有効化が完了したら、Internet Explorer を再起動します。

vPro デバイスで SOL/IDE-R 操作の telnet セッションを開始できない

表 60　　SOL/IDE-R 操作の telnet セッションを開始できない

考えられる原因	解決策
telnet クライアントがインストールされていない可能性があります。デフォルトで、telnet クライアントは Windows Server 2008 にインストールされません。 HPCA が Windows Server 2008 x64 (AMD64T) にインストールされている場合、SOL/IDER 操作で telnet セッションを開始できません。ただし、起動操作は正常に行われるため、正しいメディアからマシンが起動されます。この問題により、修復の使用ケースは完全にサポートされていません。たとえば、BIOS の更新は実行できません。	Windows Server 2008 のサーバー管理オプションを使用して、telnet クライアントをインストールします。

DASH デバイスのリモート操作ウィザードに進行状況バーが表示され続けて操作の完了が表示されない

表 61　　リモート操作ウィザードに進行状況バーが表示され続ける

考えられる原因	解決策
デバイス ハードウェアがリモート操作の応答をリモート操作ウィザードに送信していないため、リモート操作ウィザードが継続的に待機します。しかしリモート操作は正常に終了しています。	別の OOBM リモート操作を実行するには、ログアウトして現在の IE セッションを閉じ、新しい IE セッションでログインし直す方法しかありません。

DASH デバイスのブート設定の設定がしばらく有効のまま残る

表 62　　DASH デバイスのブート設定の設定が有効のまま残る

考えられる原因	解決策
操作が進行中であり、最終的に完了することを反映しています。	これは期待どおりの動作です。

休止 (ソフト) および中断などのリモート操作がターゲット DASH デバイスで動作しない

表 63　　休止および中断などの操作が DASH デバイスで動作しない

考えられる原因	解決策
Broadcom　管理エージェントがターゲット DASH デバイスで動作していないか、Windows OS が動作している状態に DASH デバイスがなっていない可能性があります。いずれかの状態である場合、HPCA コンソールで操作が正常終了と表示されても、休止操作と中断操作は DASH デバイスで機能しません。	最新の Broadcom Management Agent がインストールされていること、および管理エージェント サービスがターゲット DASH デバイスの Windows で動作していることを確認します。

vPro デバイスの IDE-R 操作の情報が HyperTerminal コンソールで適切に整列されない

表 64　　IDE-R 情報が HyperTerminal で整列されない

考えられる原因	解決策
タイミングの問題、またはハードウェア ベンダーが提供するファームウェアの問題です。	この問題に対する回避策はありません。

複数のユーザーが同一 OOBM デバイスで操作を実行すると、誤った動作を招く

表 65　　複数のユーザーが同一デバイスで操作を実行する

考えられる原因	解決策
アーキテクチャ上の制限です。	どの時点でも、デバイスでは単一のユーザーのみがリモート操作を実行してください。

vPro デバイスの電源が IDE-R 再起動後に切れない

表 66　　IDE-R 再起動後の vPro デバイスの電源の問題

考えられる原因	解決策
Web サービスが現在操作を実行中です。	vPro デバイスは、IDE-R 再起動後に電源切断コマンドを正常に実行しない場合があります。10 秒待ってから電源切断コマンドを実行すると、この問題を回避できます。

vPro デバイスのフロッピー IDE-R 再起動により、不可解な内容が SOL ディスプレイに出力される

表 67　　vPro デバイスにより、不可解な内容が SOL に出力される

考えられる原因	解決策
MS-DOS の MS Windows バージョンから起動可能フロッピーを作成したことが原因となる可能性があります (たとえば Windows のフォーマットを使用し、MS-DOS 起動ディスクを作成)。	別の方法で起動可能フロッピー ドライブを作成してください。

電源切断コマンドの後で vPro デバイスがグレー表示になる

表 68　　電源切断後、vPro デバイスがグレー表示になる

考えられる原因	解決策
ME 電源設定オプションが適切に設定されていない可能性があります。SCS プロファイルで、電源ポリシーが適切に設定されていない可能性があります。また、vPro デバイスの複数のエントリが DNS Server に存在する可能性もあります。	ME 電源設定オプションが、すべての電源状態で always on ME または wake on ME に設定されていることを確認します。SCS プロファイルで電源ポリシーが常にオンに設定されていることも確認してください。最後に、vPro デバイスのエントリが DNS サーバーに複数あるかどうかを確認します。複数のエントリがある場合は、誤っているエントリを削除して DNS Server を再起動し、HPCA コンソール サーバーで DNS をフラッシュして HPCA コンソール サーバーを再起動します。あるいは、HPCA Server で Web サービスのタイムアウト値を増加させることもできます。

S1/S2 または Sleep-Light の電源状態に移行している OOB デバイスが誤った動作をする

表 69　　S1/S2 または Sleep Light の電源状態で誤った動作をする

考えられる原因	解決策
一部のハードウェア ベンダーでは、S1/S2 または Sleep-Light の電源状態をサポートしていません。	詳細については、ハードウェア ベンダーのマニュアルを参照してください。

OOB デバイスが電源切断後、中断状態になる

表 70　　デバイスが電源切断後、中断状態になる

考えられる原因	解決策
特定のハードウェアでは、システムが中断状態になっていてユーザーが電源を切ると、HPCA コンソールは正常動作をレポートしますが、マシンは中断状態のままになります。このようなハードウェアでは、中断状態からの電源切断操作がサポートされていないためです。	このような動作がみられる場合、詳細については、ハードウェア ベンダーのマニュアルを参照してください。

DASH デバイスにおける適切な電源操作がサポート オプションとして表示されるが動作しない

表 71　　適切なリモート操作が DASH デバイスで動作しない

考えられる原因	解決策
Broadcom Management Agent がインストールされていません。	最新の Broadcom Management Agent を DASH デバイスにインストールします。

電源状態

管理対象 vPro デバイスの電源状態の表示または変更ができない

表 72　　電源状態の問題

考えられる原因	解決策
ネットワークのトラフィック量が多いため、システムをクエリしている間にネットワーク エラーが発生しました。	しばらく待ってからコマンドを再発行します。
アクティブな IDE-R/SOL セッションのため、電源切断で障害が発生しました。	アクティブな IDE-R/SOL セッションがあると、電源切断コマンドはサポートされません。コンソールには、「Parameters are valid but not supported by platform」例外が表示されます。アクティブなセッションがあるかどうか確認してください。アクティブなセッションがある場合は、セッションを終了してしばらくしてから電源を切断してみてください。

電源切断操作の後でデバイスの電源状態がグレー表示になる

表 73　　電源表示の問題

考えられる原因	解決策
タイムアウト時間を超過しました。	タイムアウト期間を設定し直します。詳細については、48 ページの「IDE-R および SOL タイムアウト値の設定」を参照してください。

再起動

再起動の問題をトラブルシューティングするには、IDE-R と SOL のグローバル設定の設定、およびリモート制御オプションを調べる必要があります。

一回限りのブート設定の OOB DASH デバイスを再起動する前に起動順序操作を実行する必要がある

表 74　　DASH デバイスを再起動する前に起動順序操作を実行する必要がある

考えられる原因	解決策
Broadcom NetExtreme Gigabit Ethernet Plus NIC ベースのハードウェアに関する問題です。 Broadcom NetExtreme Gigabit Ethernet Plus NIC ベースのハードウェアの再起動操作に一回限りの起動のブート設定の設定を選択している場合、ユーザーは、再起動前に起動順序操作を実行する必要があります。実行しない場合、リモート操作が誤って動作します。また、ユーザーが明示的な起動順序操作を実行しても、再起動後に、起動順序がデフォルトの起動順序にリセットされます。このため、**[操作] > [アウトバンド管理] > [デバイス管理] >** <*DASH Device*> **> [ブート設定]** を選択して起動操作を実行するとエラーが発生します。	回避策はありません。

DASH デバイスで、一回限りのブート設定がリセットされない

表 75　　DASH デバイスで、一回限りのブート設定がリセットされない

考えられる原因	解決策
システム BIOS に関する問題です。 DASH デバイスが再起動した後に、デバイスで一回限りのブート設定がリセットされません。リモート操作で一回限りのブート設定が選択または有効になっている場合、リモート操作が正常に完了した後に、選択解除または無効になりません。この問題が発生すると、以降のすべてのリモート操作は、常に一回限りのブート設定を使用するようになります。このため、**[操作] > [アウトバンド管理] > [デバイス管理] >** <*DASH Device*> **> [ブート設定]** を選択して、DASH デバイスで一回限りのブート設定を設定するとエラーが発生します。	**[操作] > [アウトバンド管理] > [デバイス管理] >** <*DASH Device*> **> [リモート操作]** を選択して再起動操作を実行する前に、一回限りのブート設定の起動順序を変更してください。

DASH デバイスのブート設定の設定をデフォルトおよび永続的な起動に変更できない

表 76　　DASH デバイスのブート設定を変更できない

考えられる原因	解決策
リストされている初回ブート設定の設定は永続的なブート設定の設定にハード コーディングされています。 ブート設定の設定をデフォルトおよび永続的な起動に変更できません。これを一回限りの起動に変更することはできませんが、ユーザーは、2 回目のブート設定の設定を一回限りの起動に変更できます。このため、**[操作] > [アウトバンド管理] > [デバイス管理] >** *<DASH Device>* **> [ブート設定]** を選択して DASH デバイスでブート設定の設定を行うときにエラーが発生します。	この問題に対する回避策はありません。

SOL を使用する HPCA コンソールで再起動プロセスを表示できない

表 77　　SOL を使用して再起動を表示する問題

考えられる原因	解決策
別のデバイスがポート 9999 を使用しています。	SOL 送信のためにポート 9999 を解放します。
プロビジョニング中に SOL リダイレクションが有効になりませんでした。	Intel SCS を使用して SOL リダイレクションを有効にします。詳細については、37 ページの「MEBx による vPro デバイスの設定」を参照してください。
Windows エクスプローラで起動可能フロッピーが作成されました。	Windows のフォーマットを使用して MS-DOS 起動ディスクを作成すると、起動可能ドライブが生成されますが、不可解な内容が SOL へ出力されます。別の方法で起動可能フロッピー ドライブを作成してください。

管理対象 vPro デバイスをリモートで再起動できない

表 78　　再起動の問題

考えられる原因	解決策
再起動パラメータが正しくありません。	ログを表示し、再起動パラメータを確認します。再起動パラメータが正しくない場合は、正しいパラメータで再起動を試みてください。
ファームウェアにおける特定オプションの既知の制限です。	HPCA Core 配布メディアの `Media\oobm\win32\AMT Config Server` ディレクトリにある『Intel vPro Provisioning Server リリース ノート』を確認してください。

表 79　　IDE-R での再起動の問題

考えられる原因	解決策
物理起動可能デバイス (ドライブまたはイメージ) が管理コンソールに存在しません。	管理コンソールの既存ドライブで起動します。物理デバイスが存在しない場合は、ISO イメージを代わりに使用します。
メディアのイメージが起動可能ではありません。	イメージが起動可能かどうかを確認します。起動可能でない場合は、起動可能イメージで置き換えます。
CD/DVD で再起動しようとした場合、HPCA コンソール サーバーの CD ドライブがデフォルトの D: ドライブ設定と一致していません。	デフォルトのドライブ設定を再設定し、HPCA コンソール サーバーの CD/DVDE ドライブと一致させます。詳細については、47 ページの「IDE-R ドライブの設定」を参照してください。

管理対象 vPro デバイスを BIOS 設定にリモートで再起動できない

表 80　　BIOS 設定への再起動の問題

考えられる原因	解決策
BIOS が BIOS 設定への起動をサポートしていません。	この機能がサポートされている BIOS のバージョンに、ターゲット デバイスの BIOS をアップグレードします。

管理対象 vPro デバイスの起動順序をリセットできない

表 81　　起動順序のリセットの問題

考えられる原因	解決策
原因を特定できません。	ローカル HDD 起動コマンドを実行し、ターゲット デバイスを再起動します。

システム防御およびエージェント存在

管理対象 vPro デバイスにシステム防御ポリシーを配布できない

表 82　　システム防御ネットワーク フィルタ追加のエラー

考えられる原因	解決策
vPro デバイスで、31 個の受信フィルタおよび 30 個の送信フィルタというフィルタ制限を超えています。	vPro デバイスで既存のフィルタの一部を削除します。詳細については、103 ページの「システム防御フィルタの管理」を参照してください。

無線ネットワーク ドライバを含む vPro デバイスで、システム防御ポリシーが適切に機能しないことがある

表 83　　無線 NIC を含むデバイスにおけるシステム防御ポリシー

考えられる原因	解決策
vPro デバイスの無線ネットワーク ドライバのバージョンが、インストールされている Intel AMT のバージョンと一致しません。	システム防御ポリシーを適切に機能させるには、vPro デバイスの無線ネットワーク ドライバのバージョンを、インストールされている Intel Active Management Technology のバージョンと一致させる必要があります。バージョンの互換性に関する詳細については、ハードウェア ベンダーにお問い合せください。

管理対象 vPro デバイスにエージェント ウォッチドッグを配布できない

表 84　　ウォッチドッグ配布エラー

考えられる原因	解決策
vPro デバイスに配布できる HP ローカル エージェント ウォッチドッグは 1 つのみです。複数のサード パーティ製エージェント ウォッチドッグを配布できますが、vPro デバイスにインストールされているサード パーティ製ローカル エージェント 1 つにつき 1 つのウォッチドッグです。1 つのデバイスに配布できるエージェント ウォッチドッグの総数は 16 です。	vPro デバイスからエージェント ウォッチドッグを削除するか回収します。詳細については、114 ページの「エージェント ウォッチドッグの管理」を参照してください。
無効で矛盾するアクションがウォッチドッグに定義されています。	エージェント ウォッチドッグに指定されているアクションを見直し、矛盾を修正してください。詳細については、114 ページの「エージェント ウォッチドッグの管理」を参照してください。

ローカル エージェントのインストールがエラー コード 1920 でエラーになる

表 85　　ローカル エージェントのインストールのエラー

考えられる原因	解決策
ローカル エージェントの以前のインストールまたはアンインストールに問題があります。	HPCA-OOBM ローカル エージェント サービスを vPro デバイスから削除します。削除するには [マイ コンピュータ] アイコンを右クリックし、**[管理] > [サービスとアプリケーション] > [サービス]** の順に移動します。HPCA-OOB ローカル エージェント サービスがあるか確認します。このサービスが存在する場合は、次のように操作します。 • コマンド プロンプト ウィンドウを開きます。 • タイプ `sc delete HPCA-OOBM` • システムを再起動します。
ローカル エージェントのインストール時に、ユーザー名とパスワードが指定されていません。	遅延設定でデバイスをプロビジョニングする意図がなくても、「ダミー」ユーザー名とパスワードを指定してください。ユーザー名とパスワードを指定しないと、インストールはエラー コード 1920 でエラーになります。

ローカル エージェントがシャット ダウンする

表 86　　ローカル エージェントのシャット ダウン動作

考えられる原因	解決策
ローカル エージェントが監視するアプリケーションが定義されていません。	ローカル エージェントが監視するアプリケーションのソフトウェア リストを作成して配布します。詳細については、114 ページの「エージェント ウォッチドッグの管理」を参照してください。

vPro デバイスのローカル エージェント ソフトウェア リストの配布で SOAP エラーが発生する

表 87　　エージェント ソフトウェア リストの配布が SOAP エラーを引き起こす

考えられる原因	解決策
vPro Web サービスがエラーを返します。ローカル エージェント ソフトウェア リストの配布では、「Network Error ñ SOAP error code: 22」、「Integrity check error」、「Not initialized」、「Invalid parameter」などのエラーのうちいずれかが発生することがあります。	しばらくしてから同じ操作を再び試します。それでもエラーが発生する場合は、HPCA コンソールをログアウトしてからログインし直します。

ローカル エージェントが vPro デバイスのソフトウェア リストに表示されない

表 88　エージェントが vPro デバイスのソフトウェア リストに表示されない

考えられる原因	解決策
あるユーザー アカウントでローカル エージェントをインストールし、別のアカウントでログインしたユーザーが表示すると発生する、アーキテクチャ上の制限です。	この問題に対する回避策はありません。

複数の NIC を搭載した vPro デバイスで片方の NIC にエージェント存在ポリシーを配布するとエラーが返される

表 89　複数の NIC を搭載した vPro デバイスへのエージェント存在ポリシーの配布

考えられる原因	解決策
内部エラーです。	両方の NIC にエージェント存在ポリシーを配布してから、必要としない NIC からエージェント存在ポリシーを回収します。

なりすまし防止フィルタが原因で、vPro デバイスのすべての送信トラフィックが取り消される

表 90　なりすまし防止フィルタが原因で、すべての送信トラフィックが取り消される

考えられる原因	解決策
環境検出を有効にした状態で SCS のプロファイルによって vPro デバイスがプロビジョニングされ、環境検出ドメインで指定されていないドメインにデバイスを接続すると、vPro デバイスのシステム防御ポリシーでなりすまし防止フィルタが有効になっている場合、すべての送信トラフィックは取り消されます。	環境検出ドメインで指定されているドメインにデバイスを接続します。

vPro デバイスのウォッチドッグにローカル エージェントを登録できない

表 91　ローカル エージェントの登録の問題

考えられる原因	解決策
ローカル エージェントをエージェント ウォッチドッグに登録できない場合は、Digest のユーザー名 (Intel AMT ユーザー名) に問題がある可能性があります。Intel AMT ファームウェアでは、Digest のユーザー名は大文字と小文字が区別されます。ローカル エージェントのインストール時には、大文字と小文字を区別して Digest のユーザー名を指定する必要があります。そうしないと、エージェント ウォッチドッグにローカル エージェントを登録できません。	大文字と小文字を区別して Digest のユーザー名を正しく指定します。

vPro デバイスでローカル エージェントが停止すると、メッセージが繰り返し表示される

表 92　　ローカル エージェント停止時のメッセージの繰り返し

考えられる原因	解決策
HPCA-OOBM エージェントの内部エラーです。	これが発生する場合は、クライアント vPro デバイスで HPCA-OOBM エージェント サービス (HPCA-OOBM) を再起動します。

Digest の認証情報の変更後、vPro デバイスにアクセスできない

表 93　　認証情報の変更後、vPro デバイスにアクセスできない

考えられる原因	解決策
エージェントはインストール時に限ってパスワードを取得し、変更時に動的に取得しません。SCS コンソールで vPro デバイスの Digest のユーザー名やパスワードを変更した場合、このデバイスにはアクセスできなくなります。	Digest の認証情報の変更後、このデバイスにアクセスして管理できるようにするには、vPro デバイスでローカル エージェント (HPCA-OOBM) サービスを停止する必要があります。エージェント存在機能を使用している場合は、新しいパスワードを使用して vPro デバイスでローカル エージェントをインストールし直す必要があります。

TLS プロファイルから TLS 以外のプロファイルに変更した後で、vPro デバイスでローカル エージェントが適切に動作しない

表 94　　ローカル エージェントと TLS プロファイル

考えられる原因	解決策
TLS プロファイルを使用してローカル エージェントをインストールし、ある時点で TLS 以外のプロファイルで vPro デバイスを再プロビジョニングした場合、ローカル エージェントは適切に動作しなくなります。同じように、TLS 以外のプロファイルを使用してローカル エージェントをインストールし、ある時点で TLS プロファイルで vPro デバイスを再プロビジョニングした場合も、ローカル エージェントは適切に動作しなくなります。	これが発生した場合は、適切なプロファイルを使用してローカル エージェントを再インストールする必要があります。

ローカル エージェントの管理ポップアップ メッセージが短時間表示されて消える

表 95　　ローカル エージェントの管理メッセージの表示

考えられる原因	解決策
エージェント存在ポリシーがアクティブな場合は、これが管理ポップアップ メッセージのデフォルト動作です。	vPro デバイスで Windows イベント ビューアを開き、すべてのエージェント関連のログ メッセージを表示します。

ローカル エージェント ソフトウェア リストとシステム メッセージを管理対象 vPro デバイスに配布できない

表 96　　ローカル エージェント ソフトウェア リストとシステム メッセージの配布エラー

考えられる原因	解決策
• 3PDS に対して複数のアクションが同時に発生しています。 • 1 つのセッション中に 3PDS に複数のアクセスがあります。 • ネットワークでのデータ転送に問題があります。	しばらくしてから配布を再び試します。

TLS モードでローカル エージェント ソフトウェア リストを配布できない、またはソフトウェア情報を表示できない

表 97　　TLS モデルのローカル エージェントの問題

考えられる原因	解決策
ドメイン管理者アカウントで Tomcat サービスが動作していない可能性があります。	ドメイン管理者アカウントで HPCA Tomcat Server サービスが動作していることを確認します。動作していない場合は、Tomcat の再設定と再起動を行います。
証明機関 (CA) で共通名が正しく指定されていない可能性があります。	CA の共通名が正しく指定されていることを確認します。この設定は、インストール ディレクトリの `local_settings.ini` ファイルにあります。

ローカル エージェントが正常にインストールされた後で、HPCA コンソール上のウォッチドッグの状態に変化がない

表 98　　ウォッチドッグ登録エラー

考えられる原因	解決策
ウォッチドッグの登録に失敗しました。	vPro デバイスで Windows イベント ビューアを開いて、ウォッチドッグの登録ログ メッセージがあるかどうか確認します。失敗が確認された場合、Host Embedded Controller Interface (HECI) ドライバおよび Local Manageability Service (LMS) サービスを vPro デバイスにインストールして、ウォッチドッグのステータスを再確認します。

配布されたエージェント存在ポリシーが、定義されたアクションの発生時にアクティブにならない

表 99　　エージェント存在ポリシーがアクティブにならない

考えられる原因	解決策
定義されたアクションが予想された順序で発生しなかった可能性があります。ローカル エージェントが指定された状態に遷移する前に、ローカル エージェントの期限が切れた可能性があります。	エージェント ウォッチドッグのアクションの指定時に、状態への遷移として [状態を考慮しない] を指定するのが最も安全です。

エージェント存在ポリシーが配布直後にアクティブになる

表 100　　エージェント存在ポリシーが即座にアクティブになる

考えられる原因	解決策
エージェント存在ポリシーをアクティブにしている遷移状態がすでに発生していることが、エージェント ウォッチドッグによるエージェント存在ポリシーの即座のアクティブ化を引き起こしていると考えられます。	既存のウォッチドッグを削除して、再配布します。

名前に特殊文字を含むシステム防御ポリシーを配布できない

表 101　　システム防御ポリシーの名前エラー

考えられる原因	解決策
フィルタおよびポリシーはその名前に ASCII 文字以外を使用して作成できますが、その場合配布はできません。また、フィルタおよびポリシーは、その名前に 「**:**」、「**,**」、「**>**」、「**<**」、「**&**」、および「**"**」などの特殊文字が含まれていると配布できません。この制限は、Intel AMT 仕様に示されています。	仕様に沿った名前でフィルタおよびポリシーを作成します。

無線

HPCA コンソールを使用して無線デバイスに接続できない

表 102　　無線デバイス接続の問題

考えられる原因	解決策
無線デバイスとの通信に長時間を要したため、Web サービスのタイムアウトが発生しました。HPCA コンソールで接続できない場合、デバイスはコンソールでグレー表示になります。	タイムアウト期間を設定し直します。詳細については、48 ページの「IDE-R および SOL タイムアウト値の設定」を参照してください。

無線 NIC を使用した vPro デバイスに接続できない

表 103　　無線 NIC を使用して接続できない

考えられる原因	解決策
デバイスが無線 NIC のみで設定され、デバイスが電源に接続されておらず、デバイスの電源がオフの場合、バージョン 2.5 の vPro デバイスでは予期された動作です。	vPro デバイスを電源に接続して、デバイスの電源をオンにします。

vPro デバイスの無線ネットワークで SOL/IDE-R セッションの確立に失敗する

表 104　無線ネットワークでの SOL/IDE-R セッションの失敗

考えられる原因	解決策
無線 NIC を装備した vPro デバイスは OOBM Server との通信に長時間を要するため、タイムアウトが発生しました。	アウトバンド管理設定 章の 48 ページの「IDE-R および SOL タイムアウト値の設定」の説明のとおりに IDER* および SOL* パラメータを設定します。

無線 NIC のポリシー設定に失敗する

表 105　無線 ポリシー配布の問題

考えられる原因	解決策
ポリシーが正常に配布されたように思われますが、vPro デバイスに無線 NIC が装備されていません。	ポリシーを回収するか、vPro デバイスに無線 NIC を取り付けてからポリシーを再配布します。

移行の問題

SCS 5.3 への移行後、SCS コンソールがプロファイルを正しく表示しない

表 106　プロファイルを表示するときに SCS 移行の問題が発生する

考えられる原因	解決策
SCS の前のバージョンから SCS データが移行されています。この場合、新しい SCS コンソールでは左側のツリー ビューに移行後のプロファイルが表示されません。	SCS コンソールの右側にあるプロファイル セクションにプロファイル情報を表示できます。

アウトバンド管理ソフトウェアの現行リリースへの移行後、ローカル エージェント ソフトウェア リストとシステム メッセージが表示されない

表 107　ローカル エージェントのメッセージとリストの移行の問題

考えられる原因	解決策
これは正常な動作です。ローカル エージェントのソフトウェア リストとシステム メッセージをアウトバンド管理ソフトウェアの以前のリリースで作成して配布すると、新バージョンに移行した場合、使用できなくなります。	現行リリースでローカル エージェントとシステム メッセージを作成して再配布します。詳細については、114 ページの「エージェント ウォッチドッグの管理」を参照してください。

後続のリリースに移行するときに増分探索で完全探索が実行される

表 108　後続のリリースに移行するときにデバイスの探索が実行される

考えられる原因	解決策
これは期待どおりの動作です。	以前のリリースから移行する場合、移行後のデバイスが HPCA コンソールでリストに表示されます。vPro 探索 (完全探索または増分探索) を初めて実行すると、コンソールの現在のバージョンでの初めての探索であるため、完全な vPro 探索が実行されます。

OOBM データのバックアップ

定期的に OOBM データをバックアップすることをお勧めします。次の 3 種類のファイルがバックアップの対象となります。

- 設定ファイル
- データ ファイル
- データベース

HPCA のデフォルトのインストール ディレクトリは、`C:\Program Files\Hewlett Packard\HPCA.` です。HPCA のデフォルトのデータ ディレクトリは、`C:\Program Files\Hewlett Packard\HPCA\data.` です。

HPCA のアンインストールまたはアップグレードを行う場合で、後から使用するために OOBM 設定ファイルとデータ ファイルを保持したい場合は、ファイルのバックアップと復元を行う移行スクリプトを使用する必要があります。移行と復元についての詳細は、『HP Client Automation Starter および Standard 移行ガイド』(`Docs\migrate` の配布メディアに格納されています) を参照してください。

設定ファイル

設定ファイルをバックアップするには

OOBM 設定ファイル、`configuration.properties` および `config.properties` は、*<HPCA_INSTALL_DIR>*`\oobm\conf` にあります。これらの 2 つのファイルを HPCA インストール ディレクトリ構造外の場所にコピーします。HPCA 製品を再インストールして既存の設定を維持する場合は、これらのファイルをコピーして元の場所に戻すことができます。

データ ファイル

データ ファイルをバックアップするには

vPro システム防御のフィルタ、ポリシー、ヒューリスティックおよびウォッチドッグに関するすべての設定情報は、XML ファイルで *<HPCA_DATA_DIR>*`\oobm\datafiles` に格納されています。`sd.xml` および `AgentPresence.xml` ファイルを HPCA インストール ディレクトリ構造外の場所にコピーします。HPCA 製品を再インストールして既存の vPro システム保護の設定情報を維持する場合は、これらのファイルをコピーして元の場所に戻すことができます。

データベース

データベースをバックアップするには

OOBM データベースには、探索されたデバイス、DASH 認証情報、および HPCA グループの情報が格納されています。このデータベースは、<*HPCA_DATA_DIR*>\oobm\OOBMDB にあります。OOBMDB ディレクトリ全体を HPCA インストール ディレクトリ構造外の場所にコピーします。HPCA 製品を再インストールしてこの設定を維持する場合は、このディレクトリをコピーして元の場所に戻すことができます。

ポート情報の要約

アウトバンド管理では、いくつかの TCP ポートを使用して通信を行います。企業または個人用のファイアウォール ソフトウェアがインストールされている場合、HP CA Console サーバーで次のポートを除外して、受信および送信トラフィックを許可する必要があります。

Out of Band Management Service から vPro デバイスへの通信

- ポート 16692 は、TCP 上の Web サービス トラフィックに使用されます。
- ポート 16693 は、TLS (クライアント認証を使用) 上の Web サービス トラフィックに使用されます。
- ポート 9999 は、SOL ディスプレイ アプレットとサーバーの Web アプリケーション間通信のデフォルトの開始ポートとして使用されます。この設定は変更可能です。
- ポート 16694 は、TCP 上の SOL/IDE-R に使用されます。
- ポート 16695 は、TLS (クライアント認証を使用) 上の SOL/IDE-R に使用されます。
- ポート 162 は、警告管理に使用されます。

ブラウザからサーバーへの通信

- ポート 9999 は、SOL のアプレットからサーバーへのソケット通信に使用されます。このポートは、同様にクライアント ブラウザ システム上でも利用できるようにする必要があります。
- ポート 5900 は、VNC ビューアに使用され、vPro デバイスの KVM リダイレクションを可能にします。

Out of Band Management Service からローカル エージェントへの通信

- ポート 9998 は、vPro デバイスのリモート設定におけるアウトバンド管理とローカル エージェント間の通信に使用されます。

DASH デバイスを使用した Out of Band Management Service

- ポート 623 は、アウトバンド管理と DASH デバイス間の通信に使用されます。

質問チェックリスト

HPCA コンソールのアウトバンド管理機能の問題を解決できない場合は、HP サポートにお問い合わせください。お問い合わせの前に、次の質問への答えを準備してください。この情報により、サポート チームはお客様が遭遇するいかなる問題に対しても迅速に対応できるようになります。

1 HPCA コンソール サーバーにインストールされているオペレーティング システムとサービス パックは何ですか ?

2 SCS Server の IIS のバージョンは何ですか？

3 SCS と HPCA コンソールは同じマシンにインストールされていますか？

4 SCS と SQL Server は同じマシンにインストールされていますか？

5 ネットワークに Active Directory がインストールされていますか？

6 ネットワークは DNS と DHCP に対応していますか？

7 SCS Server と HPCA コンソールの Out of Band Management Service 間の認証に NTLM v2 プロトコルを使用していますか？(ローカル ポリシーを調べると確認できます)

8 SCS のインストール時に使用したユーザー ID は何ですか？(ローカル ユーザーまたはドメイン ユーザーのどちらでも構いません)

9 そのローカルまたはドメイン ユーザーにはローカル管理者権限がありますか？

10 SQL との通信に使用している認証モードは何ですか？(Windows 認証が推奨されます)

11 HPCA コンソールにログインできますか？

12 HPCA コンソールの [デバイス] タブには何かデバイスが表示されていますか？

13 表示されているデバイスは無効 (グレー表示されていてアクセス不可) ですか？

14 SCS を使用してプロビジョニングされているデバイスはありますか？

15 プロビジョニングされたデバイスが SCS テーブルにリストされていますか？

16 SCS へのログインに、**http://IP/AMTSCS** または **https://IP/AMTSCS** を URL として使用していますか？

索引

に

ね

は

ほ

り

ろ