HP Manageability Integration Kit ホワイトペーパー

株式会社 日本HP サービス・ソリューション事業本部 技術本部 2017年4月



目次

		ページ
概要		4
システム要件		5
HP Manageability Integration Kit σ) 入手方法	6
Configuration Manager $\sim \sigma$ HP MI	Kのインストール	7
HP Client Support Packagesの配す	ក	8
HP MIKプラグイン	HP MIKプラグイン	10
	コンプライアンス設定	11
	HP BIOS Configuration	12
	HP BIOS Password	19
	HP Client Security	20
	Device Guard (Windwos 10のみ)	31
	HP Sure Start	34
	TPM Firmware Update	40
	HP WorkWise (Windows 10のみ)	43

目次

		ページ
ソフトウェアライブラリ	ソフトウェアライブラリ	48
	HP Client Driver Pack	49
	HP Client Boot Image	64
	HP Client Task Sequence	68
本書の取り扱いについて		91

概要

HPのコンピュータは以下の2つの主旨に基ずき、容易に管理できるように設計されています。

- IT管理者がコンピュータに付属のHP BIOS、ハードウェア、およびプリインストールされたソフトウェアを管理するのに役立つ手段を提供します。
- 管理者が選択したクライアント管理コンソールで動作するソリューションを提供します。

これらの2つの原則に対処するために作成されたソリューションがHP Manageability Integration Kit (MIK) です。

HP MIKは、管理面をHPのハードウェア、BIOS、およびソフトウェアの機能にまで拡張する、クライアント管理コンソールに依存しないソリューションです。

HP MIKの目的は、既存のツールとワークフローに統合することで、日常のエンタープライズプロセスとタスクを簡素化するユーザーエクスペリエンスを実現することです。

HP MIKを導入して、次のような主なメリットを享受してください。

・管理の基本をスピードアップ-イメージ、BIOS、システムセキュリティの作成、展開、および管理に必要なステップ数を減らし、ビジネスに集中できます。

•データ保護 - BIOS設定を保護し、認証と資格情報の要件を設定し、Device Guardを有効にし、TPM(Trusted Platform Module)ファームウェアの更新を管理します。

•ソフトウェアの管理 - IT管理者は、HP Client Securityなど、ソフトウェアでサポートされている機能をリモートで管理できます。

HP MIKは、Microsoft[®]System Center Configuration Managerで動作するように最適化されていますが、スクリプトを使用して他のクライアント 管理コンソールと連携します。このドキュメントには、Configuration Manager内のHP Manageability Integration Kitプラグインの例とスクリー ンショットのみが含まれています。完全なユーザーガイドについては、HPの管理機能のWebサイト (http://www.hp.com/go/clientmanagement)を参照してください。

システム要件

HP Manageability Integration KitサポートされているバージョンのMicrosoft System Center Configuration Manager (SCCM) およびサポートされているWindows®オペレーティングシステムを実行しているクライアントにインストールでき ます

サポートされているMicrosoft System Center Configuration Managerのバージョン

- Microsoft System Center 2012 R2 Configuration Manager service pack 1 (SP1) with or without cumulative update 1 (CU1) or later
- Microsoft System Center 2012 R2 Configuration Manager
- Microsoft System Center 2012 Configuration Manager SP2 with or without CU1 or later and
- Microsoft System Center 2012 Configuration Manager SP1 and
- Microsoft System Center Configuration Manager 1511, 1602, or 1606

サポートされているクライアントOS

※いくつかのHP Manageability Integration Kitの機能には追加の要件があります

- Windows 10
- Windows 8.1
- Windows 7



HP Manageability Integration Kitの入手方法

HP Manageability Integration Kit**は以下の**URLより無償でダウンロード可能です。 http://ftp.hp.com/pub/caps-softpaq/cmit/HPMIK.html





Configuration ManagerへのHP MIKのインストール

- 1. Configuration Managerコンソールのインスタンス がすべて閉じていることを確認します。
- 2. 2. HP Client Integration Kit (CIK) がシステムにイン ストールされている場合は、アンインストール します。
- 3. Microsoft System Center Configuration Manager SoftPaq用にダウンロードしたHP管理容易性統合 キット(MIK)を実行し、画面の指示に従ってイ ンストールを完了します。
- 4. 4. Configuration Managerコンソールを開き、 [Assets and Compliance]にHP Manageability Integration Kitが表示されていることを確認します。



HP Client Support Packagesの配布

インストールが完了した後、HP Client Support Packages内のコンテンツを配布ポイントに配布します。

1. Configuration Managerで、ソフトウェアライブラリ→概要→アプリケーション管理→パッケージ→HP Client Support Packagesを選択します。

注記

依存するタスクシーケンスの失敗を防ぐために、このフォルダのパッケージを削除したり、名前を変更したりしない でください。

パッケージが削除されている場合は、HP Manageability Integration Kitを再インストールし、インストールウィザードで修 復を選択します。次に、パッケージを使用してタスクシーケンスをリフレッシュします。詳細については、「タスク シーケンスの更新」を参照してください。

- 初めてのインストールの場合は、[HP Client BIOS Configuration Utility]を右クリックし、[コンテンツの配布] を選択し、画面の指示に従ってウィザードを完了します。アップグレードの場合は、HP Client BIOS Configuration Utilityを右クリックし、配布ポイントの更新を選択し、画面の指示に従ってウィザードを完 了します。
- 3. [HP Client Support Tools]に対しても2と同様の内容を実行します。







HP MIKプラグイン

HP Manageability Integration Kitをインストールすると管理とコンプライアンスにHP Manageability Integration Kit が追加されます。 HP Manageability Integration Kitノードの下には7つのプラグインがあります。

- HP BIOS Configuration: BIOS設定のポリシーを作成します
- HP BIOS Password: BIOSパスワードを作成しSCCMに保存します
- Client Security: HP Client Security設定のポリシーを作成します
- Microsoft Device Guard:システムのBIOS設定をDevice Guard-CapableからDevice Guard-Readyに変更します
- Sure Start: Sure Start関連のBIOS設定の変更とSure Startのイベントログ収集の有効・無効を設定します
- TPM Firmware Update: TPMファームウェアのアップデートを行います
- WorkWise: WoekWiseアプリケーションソフトウェアの有効・
 無効を設定します



コンプライアンス設定

HP MIKプラグインを使用して作成したポリシーはConfiguration Managerのコンプライアンス設定として保存されます。場所は、資産とコンプライアンス→コンプライアンス設定→構成項目になります。

構成項目はHPMIKのプラグインごとに作成され、デフォルトでは名前にプラグイン名が含まれます。

1つの構成基準には1つまたは複数の構成項目が含まれています。構成基準はコレクションごとに展開する事ができます。

作成検索			構成項	目	移	b	分類	10/	パティ
 → ▼ 🔐 ¥ ・ 資産とコンプライアンス ・ 	概要 ▶	コンプライアンス設定 ・ 構成工	頁目						•
産とコンプライアンス	《 構成項	目 2 項目							
🧬 デバイス コレクション	検索						×	○ 検索	条件の追
🌜 ユーザーの状態の移行	アイコン	名前		種類	デバイスの種類	リビジョン	子	関係	ューザー
▶ 🧰 資産インテリジェンス		MIK Test - Device Guard	# at	7704-2-5.	Windowa	71	いいえ	はい	いいえ
1 ソフトウェア使用状況の測定		MIK Test - Trusted Platfo		子構成項目の作成(C)		1	いいえ	はい	いいえ
● 🧰 コンプライアンス設定			*	リビジョン喧歴(H)					
📸 構成項目				XML 正義の表示(X)					
🔄 構成基準			6	1974-L(F)					
📸 ユーザー データとプロファイル					FF				
101 リモート接続プロファイル			¥	取初の用物に更初	FJ				
🛃 コンプライアンス ポリシー					Delete				
🕨 🔛 条件付きアクセス				移動		-			
🕨 🚞 会社のリソースへのアクセス				カテゴリ化(I)	•	4			
三 使用条件	-		6	セキュリティ スコープの設定	(S)				
Windows 10 エディションのアップガレード			(755)	ສຳລະຍິສະ ເ					



BIOS Configurationプラグインを使用してBIOS設定のポリシーを作成してクライアントコンピュータに展開する事ができます。

サポート対象のクライアントコンピュータ

・2015年モデル以降のHPコマーシャルコンピュータ

サポート対象のOS

- Windows 10
- Windows 8.1
- Windows 7

前提条件

- Microsoft .NET Framework 4.0以上
- HP Manageability Integration Kit



ユーザーインタフェース

HP BIOS Configuration ウィンドウには3つの列があります。

Select**列ではポリシーで強制する**BIOS設定を選択します。

Settings**列には**BIOS設定の名前が表示されます。

Values列には値を入力するかドロップダウンメニューから値を選択します。BIOS設定によっては入力した値に特定の構 文が必要な場合は、構文が正しい場合はボックスの背景が緑色になり、構文を修正する必要がある場合は赤色に変わ ります。

注記

Category Viewの場合、3つの列全てを表示するにはカテゴリを展開する必要があります。

いくつかの設定の隣にあるアイコンはそれぞれ以下を示します。



-設定は次の再起動時に一度だけ有効になり、その後は初期値に戻ります。



一設定は次の再起動時にユーザーの確認が要求されます。

確認のためのキー入力が実施されるまでは再起動が完了しません。



List View/Category Viewボタン

BIOS設定の表示を一覧表示(List View) またはカテゴリ表示(Category View) に切り替えます。

		MIK Test - BIC	S Configuration		×
HP BIOS Config	guration				
List View	Expand All	Show only selected	Filter to settings containing : Search		
Select		Settings		Values	*
✓ 1 setting(s)					
 12 setting(s) 					
✓ 8 setting(s)					
✓ 35 setting(s)					-
✓ 18 setting(s)					#
✓ 8 setting(s)					
 10 setting(s) 					
✓ 21 setting(s)					
 11 setting(s) 					
 29 setting(s) 					
✓ 5 setting(s)					
✓ 7 setting(s)					
✓ 5 setting(s)					
✓ 7 sottina(s)					•
					Next



Expand All/Collapse Allボタン

カテゴリ表示の際に全ての設定を表示または非表示にします。

	MIK Test - BIOS Configuration		
	Configuration		
List View	Collapse All Show only selected Filter to settings containing : Search	:h	
Select	Settings	Values	4
 1 setting(s) 			
	AMD DASH Enable or disable support for DMTF DASH specification	Enable	•
 12 setting(s) 			
	Intel Active Management (AMT) Enable or disable Intel Active Management (AMT)	Enable	•
	Wireless Manageability Enable Wireless Manageability	Enable	•
	Verbose AMT Boot Messages Display verbose AMT boot messages	Enable	•
	USB Redirection Support Configure support for USB Redirection	Enable	•
	USB Key Provisioning Enable or disable AMT provisioning using a USB disk	Enable	-
	Unconfigure AMT	Enable	T

ПП

Show only selected/Show Allボタン

選択した設定のみを表示するかまたは全ての設定を表示するか切り替えます。

	MIK Test - BIOS Configuration			×
	Configuration			
List View	Collapse All Show only selected Filter to settings containing : Search			
Select	Settings	Values		*
	Allow spaces in passwords If enabled, the Administrator and User passwords may contain spaces	No	-	
	Require a lowercase character in BIOS passwords If enabled, the Administrator and User passwords must contain at least one lowercase letter	No	•	
10 setting(s)				
	Serial Port A Enable or disable serial port A, where available	Enable	•	
	Serial Port B Enable or disable serial port B, where available	Enable	•	
	I/O Address A Port I/O Address A	Default Address	-	
	I/O Address B Port I/O Address B	Default Address	•	
	I/O Address C Port I/O Address C	Default Address	•	
	I/O Address D Port I/O Address D	Default Address	•	-

Next

(hT)

ポリシーの作成

- 1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
- 2. HP Manageability Integration Kitを展開し、[BIOS Configuration]を右クリックして、[Create Policy]を選択します。
- 3. ベースライン名を入力し、ポリシー作成ウィザードを開始します。
- 4. 設定を選択し、新しい値を選択して設定を変更します。
- 5. BIOS設定を選択して変更したら、[次へ]を選択します。
- 6. Summaryページで設定内容を確認して[Save Policy]をクリックします。
- 7. ポリシーの保存が完了したら、[Deploy]をクリックします。
- 8. ポリシーを適用するターゲットのコレクションを選択し、[Deploy]をクリックします。
- クライアントコンピュータにポリシーが適用された後、クライアントコンピュータを再起動して設定が 変更されている事を確認します。



ポリシーの編集

- 1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
- 2. HP Manageability Integration Kitを展開し、[BIOS Configuration]を右クリックして、[Edit Policy]を選択します。
- 3. ベースライン名を選択し、[OK]をクリックしてます。
- 4. ポリシー作成ウィザードのSummary画面が表示されますので[Previous]をクリックします。

5. ポリシーの作成の4~9と同じ手順を実行します。

注記

クライアントコンピュータにBIOSパスワードが設定されている場合は、次のHP BIOS Passwordの手順を先に実行しておく 必要があります。

クライアントコンピュータでHP MIK BIOS Configurationのログは%PROGRAMDATA%¥HP¥HP MIK¥Logsに保存されます。

HP BIOS Password

クライアントコンピュータにBIOSパスワードが設定されている場合はこの機能を使用してHP Manageability Integration KitがHP BIOS Configuration等の機能でBIOS設定を変更する際に使用するためのBIOSパスワードを登録します。

この機能からはクライアントコンピュータのBIOSパスワードを変更する事は出来ません。BIOSパスワードの 設定・変更はHP BIOS Configurationプラグインから行います。

MIK E	BIOS Password Management	x
BIOS Pas	ssword	
Password Confirm Password	Cancel Apply	

HP Client Securityプラグインを使用してConfiguration ManagerからHP Client Securityを管理できます。また Intel®Authenticate™の設定を行う事ができます。

サポート対象のクライアントコンピュータ

- ・2015年モデル以降のHPコマーシャルコンピュータ
- サポート対象のOS
 - Windows 10
 - Windows 8.1
 - Windows 7

前提条件

- Microsoft .NET Framework 4.6.1以上
- HP Client Security Manager 9.3.0.2368以上
- ・ HP Device Access Manager 8.4.6.0以上
- Intel Authenticate Engine (オプション)

注記

Intel Authenticate Engineには次のドライバー要件があります。

- Intel Management Engine Driver 11.6.0.1019以上
- Intel Bluetooth[®] Driver 19.00.00.1626.3453以上
- Intel Graphics Driver 21.20.16.4481以上
- Synaptics Touch Fingerprint Driver 5.2.5002.26以上

Intel Authenticate EngineではIntel Authenticate supportへのアクセスが要求されます。

ユーザーインタフェース

HP Client SecurityはClient Security ManagerとDevice Access Managerの2つに分かれています。

HP Client Security プラグインを開くとClient Security Managerの概要紹介画面が表示されます。[Start Policy]をクリックします。

	HP Client Security_1 - Client Security	x
HP Client Secu	rity Suite	
Search Client Security Manager Authentication Intel Authenticate (TM) Windows Logon Policy Windows Session Policy Advanced Options Device Access Manager Hardware Removable Media Summary	<image/> <image/> <text><text><text><text></text></text></text></text>	



Client Security Manager

Authenticationタブ

このタブではHP Client Security Managerのセキュリティ機能を設定します。

以下の設定の有効化・無効化が可能です。

- Windows Logon—強力な認証を使用してWindowsアカウントを保護します。
- Power On Authentication—電源投入時認証を有効にして Windows起動前のシステムを保護します。
- One Step Logon 一電源投入時認証が有効な場合に電源 投入時に入力した資格情報をWindowsログオンに使用 できます。
- Password Manager—Windowsログオン後にWebサイトや アプリケーションに入力したパスワードをHP Password Managerに安全に保存し、そのパスワードを 入力する代わりにHP Client Securityの認証で自動的に使 用できます。

	HP Client Security_1 - Client Security		×
HP Client Securit	ty Suite		
earch	Authentication	sers authentication environment.	_
Authentication			
Intel Authenticate (TM) Windows Logon Policy		Enabled	
Windows Session Policy	Windows Logon Require authentication after the OS start		
Device Access Manager	Power On Authentication Require authentication before the OS start		
Hardware	One Step Logon Require authentication only once at first login prompt		
Removable Media Summary	Password Manager Allow users to safely store passwords so that they can be managed and used securely		
	Spare Key Allows secure logon in case of forget password or lose card	V	
		Next	



Intel Authenticateタブ

このタブではIntel Authenticateを設定します。クライア ントコンピュータにIntel Authenticate Engineがインス トールされている必要があります。

以下の設定ができます。

Enable Intel Authenticate—Intel Authenticateサポートを有効にします。

この設定が有効の場合、クライアントコンピュータの Intel Authenticate Engineが使用する証明書を選択できます。

- Type the location of the security certificate—Personal Information Exchange(PFX)形式のX.509証明書ファイルを選 択します。
- Enter the password to unlock your certificate 証明書がパス ワードで保護されている場合はこのオプションを選択して パスワードを入力します。
- My Certificate does not have a password—証明書がパスワード で保護されていない場合はこのオプションを選択してパス ワードを入力します。

	HP Client Security_1 - Client Security
HP Client Secu	rity Suite
Search	(intel Authentication (TM)
Client Security Manager Authentication	Intel Authenticate is a platform solution that improves security by strengthening authentication through the use of Intel ME capabilities. Intel Authenticate is supported on Intel Core platforms with Intel Bluetooth and Intel graphics. You must install HP Client Security Manager and Intel Authenticate software on the client
Intel Authenticate (TM)	computers in order to take advantage of these capabilities.
Windows Logon Policy Windows Session Policy	A security certificate is needed to sign the Intel Authenticate enabling policies. Provide the path below to the security certificate you wish to use.
Advanced Options	Enable Intel Authenticate
Device Access Manager	Type the location of the security certificate:
Hardware	Browse
Removable Media	Enter the password to unlock your certificate
Summary	Password
	O My certificate does not have a password
	Save
	Previous Next

Windows Logon Policyタブ

このタブではWindowsログオン認証で使用する資格情報 のポリシーを設定します。

以下の設定ができます。

- Add Credential—Windowsログオンで使用する追加の認 証方式を追加します。追加した認証方式を削除するに は認証のアイコンの右上のXアイコンをクリックしま す。
- Restore Default—設定を初期状態に戻します。

	HP Client Security_1 - Client Security	x
HP Client Secu	rity Suite	
Search	🕞 Windows Logon Policy	
Authentication	You can configure logon policies for users of this computer. Logon policies set here govern the credentials required for users to log on to Windows.	
Intel Authenticate (TM)	Allowed Credential Options	
Windows Logon Policy Windows Session Policy Advanced Options Device Access Manager Hardware Removable Media	Image: Password OR Image: Password Image: Password Image: Password OR Image: Password Image: Password Image: Password Image: Password Image: Pas	
Summary	+ ADD CREDENTIAL RESTORE DEFAULT Previous Next	

Windows Session Policyタブ

このタブではWindowsセッションで使用する資格情報の ポリシーを設定します。

以下の設定ができます。

- Use Logon Policy—設定済みのログオンポリシーを使用します。
- Add Credential—Windowsログオンで使用する追加の認 証方式を追加します。追加した認証方式を削除するに は認証のアイコンの右上のXアイコンをクリックしま す。

	HP Client Security_1 - Client Security
HP Client Secu	rity Suite
Search	<image/> <complex-block><complex-block><complex-block><complex-block><complex-block><complex-block></complex-block></complex-block></complex-block></complex-block></complex-block></complex-block>



Advanced Optionsタブ

このタブではHP Client Securityで使用する資格情報の詳細 設定をします。

以下の設定ができます。

- Fingerprint Options
 - Minimum number of fingerprints—1人のユーザーが登録可能 な指紋の数の最小値
 - Maximum number of fingerprints—1人のユーザーが登録可能 可指紋の数の最大値

Force number of fingerprints to enrollが有効な時にのみ設定可能

- Fingerprint recognition accuracy—指紋リーダーの性格率を設 定します。
- Smart Card Options
 - Lock PC When smart card is removed—スマートカードが取り 外された際にPCを自動的にロックします。
- PIN Options
 - —Set allowed PIN length—PINの最小文字数を設定します。



Device Access Manager

Hardwareタブ

このタブでは様々はデバイスやデバイスクラスのアクセス権を設定します。アクセス権は管理者(Allow Access for Administrator)と一般ユーザー(Allow Access for Standard User)ごとに設定できます。

以下のデバイスやデバイスクラスについて設定ができま す。

- Biometric Devices (生体認証デバイス)
- Bluetooth (ブルートゥース)
- Imaging Devices (イメージングデバイス)
- Network adapters (ネットワークアダプタ)
- Ports(COM & LPT) (πF (COM & LPT))

arch P	Device Access Mana	ger - Hardware	
ient Security Manager Authentication	Manage access permission to each device class or devices across your users. Let's start with hardware devices that do not store data but extend your corporate network.		
Intel Authenticate (TM) Windows Logon Policy		Allow Access for Administrator	Allow Access for Standard User
Windows Session Policy	Biometric Devices		
Advanced Options	Bluetooth	2	>
evice Access Manager	Imaging Devices		
Hardware	Network adapters		
Removable Media Immary	Ports (COM & LPT)	V	



Removable Mediaタブ

このタブではUSBドライブなどのリムーバブルストレー ジやCD/DVDドライブへのアクセス権を設定します。ア クセス権は管理者(Allow Access for Administrator)と一 般ユーザー(Allow Access for Standard User)ごとに設定 できます。

選択したリムーバブルメディアに対して以下のアクセス 権を設定できます。

- Full Access-ファイルの追加、読み取り、編集、削除 を許可します。
- Read Only—ファイルの読み取りのみを許可します。
- JITA(Just In Time Authentication)—ユーザーが資格情報を 入力した後、一定時間(ドロップダウンボックスで指 定して時間)ファイルへのフルアクセスを許可します。
- No Access—ファイルへのアクセスを禁止します。

	HP Client Security_1 - Cli	ecurity		
HP Client Secu	ity Suite			
Search	Device Access Manager -	Removable M	edia	
Client Security Manager Authentication Intel Authenticate (TM)	Configure the access of removable media suc choose to assign a set of users to use these of Just in Time Authentication (JITA) allows you to successful authentication. You can also custom	Configure the access of removable media such as USB drive and CD/DVD-ROM devices. You can also choose to assign a set of users to use these devices as full access, read only or for limited time only. Just in Time Authentication (JITA) allows you to provide time-limit based access to the device upon successful authentication. You can also customize the time-limit.		
Windows Logon Policy Windows Session Policy		Allow Access for Administrator	Allow Access for Standard User	
Advanced Options		• Full Access	O Full Access	
Device Access Manager	Removable Storage (e.g. USB drive)	Read Only	O Read Only	
Hardware	nemetable storage (eigi oob ante)	O JITA	● JITA 15 Min 👻	
Removable Media		O No Access	O No Access	
Summary		• Full Access	O Full Access	
	CD/DVD-ROM Drive	Read Only	Read Only	
		ATIL O	O JITA	
		O No Access	O No Access	
			Previous Next	

ポリシーの作成

- 1. Configuration Managerで、[資産とコンプライアンス] を選択し、「概要」を選択します。
- 2. HP Manageability Integration Kitを展開し、[Client] Security]を右クリックして、[Create Policy]を選択しま す。
- 3. ベースライン名を入力し、ポリシー作成ウィザード を開始します。
- 4. Client Securityの設定を変更したら、[次へ]を選択しま す。
- 5. Summaryページで設定内容を確認して[Save Policy]を クリックします。
- 6. ポリシーの保存が完了したら、[Deploy]をクリックし ます。
- 7. ポリシーを適用するターゲットのコレクションを選 択し、[Deploy]をクリックします。

Search Summary Client Security Manager Almost done! Let's make sure all settings are correct. Authentication Intel Authenticate (TM) Windows Logon Policy Manager Windows Session Policy Enabled Advanced Options Device Access Manager Hardware Removable Media Summary Policy Credentials Session Policy Credentials Password (OR) Smart Card (OR) Contactless Card (OR) Advanced Options Policy Credentials Maintum number of fingerprints to be enrolled Enabled Minimum number of fingerprints 2 Maintum allowed PIN length 4 Set mainmum allowed PIN length 12 It is the main allowed PIN length 12	x
Search	
Client Security Manager Almost done! Let's make sure all settings are correct. Authentication Intel Authenticate (TM) Windows Logon Policy Enabled Windows Logon Policy Enabled Windows Session Policy Enabled Advanced Options Enabled Device Access Manager Enabled Hardware Removable Media Summary Session policy credentials Advanced Options Policy Credentials Minimum number of fingerprints to be enrolled Enabled Minimum number of fingerprints 2 Maxium number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set maximum allowed PIN length 4 Set maximum allowed PIN length 12 11	
Authentication Authentication options Intel Authenticate (TM) Vindows Logon Enabled Windows Logon Policy Password Manager Enabled Windows Session Policy Password Manager Enabled Advanced Options Disabled Vindows Logon Policy Device Access Manager Enabled Undows Logon Policy Hardware Session Policy Credentials Password (OR) Smart Card (OR) Contactless Card (OR) Summary Advanced Options Poicy credentials Summary Advanced Options Poicy Credentials Session policy Credentials Password (OR) Smart Card (OR) Contactless Card (OR) Summary Advanced Options Poice recognition accuracy Summary Inimum number of fingerprints to be enrolled Enabled Minimum number of fingerprints 7 Fingerprint recognition accuracy Lock PC when smart card is removed Enabled Set maximum allowed PIN length Set maximum allowed PIN length 12 Image: State Sta	
Authentication Windows Logon Enabled Intel Authenticate (TM) Power On Authentication Enabled Windows Logon Policy Password Manager Enabled Windows Session Policy Password Manager Enabled Advanced Options Intel Authenticate (TM) Disabled Device Access Manager Enabled Disabled Hardware Session Policy Windows Logon Policy Password (OR) Smart Card (OR) Contactless Card (OR) Summary Session policy credentials Password (OR) Smart Card (OR) Contactless Card (OR) Summary Advanced Options Porce number of fingerprints to be enrolled Enabled Kery Inimum number of fingerprints 2 Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set maximum allowed PIN length 4 Set maximum allowed PIN length 12	^
Intel Authenticate (TM) Power On Authentication Enabled Windows Logon Policy Password Manager Enabled Windows Session Policy Intel Authenticate (TM) Enabled Advanced Options Intel Authenticate (TM) Disabled Device Access Manager Enabled Disabled Hardware Session Policy Windows Logon Policy Hardware Session Policy credentials Password (OR) Smart Card (OR) Contactless Card (OR) Summary Advanced Options Force number of fingerprints to be enrolled Enabled Summary Kernovable Media Core number of fingerprints 2 Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Enabled Set maximum allowed PIN length 4 Set maximum allowed PIN length 12	
Intel Authenticate (IM) One Step Logon Enabled Windows Logon Policy Password Manager Enabled Windows Session Policy Intel Authenticate (TM) Disabled Advanced Options Intel Authenticate (TM) Disabled Device Access Manager Windows Logon Policy Password (OR) Smart Card (OR) Contactless Card (OR) Hardware Session Policy Credentials Password (OR) Smart Card (OR) Contactless Card (OR) Removable Media Advanced Options Password (OR) Smart Card (OR) Contactless Card (OR) Summary Advanced Options Force number of fingerprints to be enrolled Enabled Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set maximum allowed PIN length 4 Set maximum allowed PIN length 12 Image: Contactless Card (CR)	
Windows Logon Policy Password Manager Enabled Spare Key Enabled Advanced Options Disabled Device Access Manager Windows Logon Policy Hardware Session Policy Credentials Password (OR) Smart Card (OR) Contactless Card (OR) Removable Media Advanced Options Password fingerprints to be enrolled Enabled Summary Force number of fingerprints to be enrolled Enabled Enabled Summary 100000 Colored (Colored Colored C	
Windows Session Policy Intel Authenticate (TM) Advanced Options Disabled Device Access Manager Windows Logon Policy Hardware Session Policy Credentials Removable Media Session policy credentials Summary Advanced Options Vinimum number of fingerprints to be enrolled Enabled Minimum number of fingerprints 2 Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set maximum allowed PIN length 12 11	
Windows Session Policy Intel Authenticate (TM) Advanced Options Enable Intel Authenticate Disabled Device Access Manager Windows Logon Policy Password (OR) Smart Card (OR) Contactless Card (OR) Hardware Session Policy Credentials Password (OR) Smart Card (OR) Contactless Card (OR) Summary Advanced Options Password (OR) Smart Card (OR) Contactless Card (OR) Summary Advanced Options Force number of fingerprints to be enrolled Enabled Summary Maximum number of fingerprints 2 Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set maximum allowed PIN length 4 Set maximum allowed PIN length 12	_
Advanced Options Enable Intel Authenticate Disabled Device Access Manager Windows Logon Policy Password (OR) Smart Card (OR) Contactless Card (OR) Hardware Session Policy Credentials Password (OR) Smart Card (OR) Contactless Card (OR) Summary Advanced Options Force number of fingerprints to be enrolled Enabled Minimum number of fingerprints 2 Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set maximum allowed PIN length 4 Set maximum allowed PIN length 12	=
Advanced Options Device Access Manager Hardware Removable Media Summary Vindows Logon Policy Password (OR) Smart Card (OR) Contactless Card (OR) Summary Maximum number of fingerprints to be enrolled Fingerprint recognition accuracy Lock PC when smart card is removed Set maximum allowed PIN length 12 C	
Device Access Manager Windows Logon Policy Password (OR) Smart Card (OR) Contactless Card (OR) Hardware Session Policy Credentials Password (OR) Smart Card (OR) Contactless Card (OR) Removable Media Advanced Options Force number of fingerprints to be enrolled Enabled Maximum number of fingerprints 2 Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set maximum allowed PIN length 4 Set maximum allowed PIN length 12	
Hardware Session policy Credentials Password (OR) Smart Card (OR) Contactless Card (OR) Advanced Options Advanced Options Enabled Summary Force number of fingerprints to be enrolled Enabled Minimum number of fingerprints 2 Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set maximum allowed PIN length 4 Set maximum allowed PIN length 12	Fi
Hardware Session policy credentials Password (OR) Smart Card (OR) Contactless Card (OR) Removable Media Advanced Options Summary Force number of fingerprints to be enrolled Enabled Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set maximum allowed PIN length 4 Set maximum allowed PIN length 12	
Removable Media Summary Advanced Options Force number of fingerprints to be enrolled Enabled Maximum number of fingerprints 2 Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set maximum allowed PIN length 4 Set maximum allowed PIN length 12	Pi
Kernovable Media Force opports Summary Force number of fingerprints to be enrolled Enabled Maximum number of fingerprints 2 Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set maximum allowed PIN length 4 Set maximum allowed PIN length 12	
Summary Minimum number of fingerprints to 2 closed Maximum number of fingerprints Additional constraints Additiona constraints Additional constraints Additiona	
Maximum number of fingerprints 7 Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set minimum allowed PIN length 4 Set maximum allowed PIN length 12	
Fingerprint recognition accuracy 100000 Lock PC when smart card is removed Enabled Set minimum allowed PIN length 4 Set maximum allowed PIN length 12 <	
Lock PC when smart card is removed Enabled Set minimum allowed PIN length 4 Set maximum allowed PIN length 12 < III	
Set minimum allowed PIN length 4 Set maximum allowed PIN length 12 < III	
Set maximum allowed PIN length 12	
<	~
	>
Previous Save Poli	У



ポリシーの編集

- 1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
- 2. HP Manageability Integration Kitを展開し、[Client Security]を右クリックして、[Edit Policy]を選択します。
- 3. ベースライン名を選択し、[OK]をクリックしてます。
- 4. ポリシー作成ウィザードのSummary画面が表示されますので[Previous]をクリックします。

5. ポリシーの作成と同じ手順を実行します。

追加情報

HP Client SecurityのポリシーにはClient Security ManagerとDevice Access Managerの両方の設定が含まれます。

ポリシーを作成する前に、必ずIntel Authenticateを設定してください。お使いのコンピュータがサポートされているかどうか、およびインテルの認証を設定する方法の詳細については、「インテルの認証」マニュアルを参照してください。

Device Guard(Windows 10のみ)

Device GuardはWindows 10 Enterprise Editionの機能で、ハードウェアおよびソフトウェアベースのマルウェア 対策機能です。アプリケーションやドライバーを実行する前にそれらが信頼された提供元からのものであ るかを確認し、信頼されない場合は実行されません。HP MIKのDevice Guardポリシーを使用してDevice Guard を有効化するための設定を簡単に行う事ができます。

サポート対象のクライアントコンピュータ

- ・2015年モデル以降のHPコマーシャルコンピュータ
- サポート対象のOS
 - Windows 10

前提条件

- Microsoft .NET Framework 4.0以上
- HP MIK



Device Guard

ポリシーの作成

- 1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
- 2. HP Manageability Integration Kitを展開し、[Device Guard]を 右クリックして、[Create Policy]を選択します。
- ベースライン名を入力し、ポリシー作成ウィザードを 開始します。
- 4. 以下のオプションのどちらかを選択します。
- A) Create a policy to activate device guard support—Device Guardを有効にするために対象デバイスのレジストリ設 定を変更し、仮想化技術を有効にします。
- B) Create a policy to deactivate device guard support—Device Guardを無効にするために対象デバイスのレジストリ設 定を変更し、仮想化技術技術を無効にします。
- 5. Summaryページで設定内容を確認して[Save Policy]をク リックします。
- 6. ポリシーの保存が完了したら、[Deploy]をクリックします。
- 7. ポリシーを適用するターゲットのコレクションを選択 し、[Deploy]をクリックします。



Next

Device Guard

Device GuardポリシーでDevice Guard supportを有効に した際に変更される設定

レジストリ設定

[HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control ¥DeviceGuard]

"EnableVirtualizationBasedSecurity"=dword:0000001

"HypervisorEnforcedCodeIntegrity"=dword:0000001

"RequirePlatformSecurityFeatures"=dword:0000002

[HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control ¥Lsa]

"LsaCfgFlags"=dword:0000001

Windowsの機能

Microsoft Hyper-Vと Isolated User Mode を有効にします

BIOS設定

- SVM CPU Virtualization を有効にします(AMD プラット フォーム)
- Virtualization Technology (VTx) を有効にします(Intelプ ラットフォーム)
- Virtualization Technology for Directed I/O (VTd) を有効にし ます(Intelプラットフォーム)
- TPM Device を利用可能にします
- TPM State を利用可能にします
- CD-ROM Boot を無効にします
- PXE Boot を無効にします
- USB Storage Boot を無効にします
- Legacy Boot を無効にします
- UEFI Boot を有効にします
- Configure Legacy Boot Supportを Legacy Support Disable and Secure Boot Enableにします

Device Guard

ポリシーの編集

- Configuration Managerで、[資産とコンプライアン ス]を選択し、[概要]を選択します。
- 2. HP Manageability Integration Kitを展開し、[Device Guard]を右クリックして、[Edit Policy]を選択します。
- 3. ベースライン名を選択し、[OK]をクリックしま す。
- 4. ポリシーの作成と同じ手順を実行します。

追加情報

クライアントコンピュータでHP MIK Device Guardのログ は%PROGRAMDATA%¥HP¥HP MIK¥Logsに保存されます。 次のエラーコードが発生する可能性があります

エラーコード	説明
0	正常終了
1	不明なエラー。インストールエラーの可能性
2	OSがサポートされていません
3	CPU/チップセットがサポートされていません
4	古いグラフィックスドライバです
5	BIOSのCPU仮想化の有効化に失敗
6	BIOS の TPMデバイスの利用可能に失敗
7	BIOSのUSBブートの無効化に失敗
8	BIOS の PXE ブートの無効化に失敗
9	BIOSのフロッピーブートの無効化に失敗
10	BIOSのCD-ROMブートの無効化に失敗
11	BIOS Boot ModeのUEFI Nativeへの変更に失敗
12	BIOS セキュアブートの有効化に失敗
13	Hyper-Vの設定に失敗
14	分離ユーザーモードの設定に失敗
15	レジストリ設定の変更に失敗
16	Windows機能の変更に失敗

HP Sure Start

HP Sure Startは、デフォルトでコンピュータの起動時または再起動時にBIOSの整合性を確認することにより、マルウェアやウイルスの脅威からHP BIOSを保護します。 追加のポリシーでは、BIOSを検証する頻度の増加や、HP Sure Startのイベントログを収集する事ができます。

HP MIKのHP Sure Startポリシー管理では、ポリシーをリモートで管理し、BIOSの悪意のある攻撃やセキュリティ侵害の適切なログと通知、およびその後の修復を保証します。

サポート対象のクライアントコンピュータ

- 2014年モデルのHP 700シリーズ以上の コマーシャルノートPC
- 2015年モデル以降のHP 700シリーズ以上の コマーシャルコンピュータ

サポート対象のOS

- Windows 10
- Windows 8.1
- Windows 7

前提条件

Microsoft .NET Framework 4.0以上

HP MIK

	HP Client Security_1 - Sure Start
HP Sure Start	
Search	HP Sure Start
BIOS Security Settings	HP's industry-leading firmware ecosystem enables robust remote configurability and manageability of your PC fleet, automates data protection and helps reduce down time for users
Events and Recovery Settings	and IT due to BIOS attack or corruption, with exclusive HP Sure Start technology. Self-healing HP Sure Start technology can automatically restore productivity after BIOS attach or corruption with little or no interruption to user productivity. This Policy will allow you to manage HP Sure Start
Audit Log	across your network.
Juliniary	create a policy to apply various available ne sure start reatures and assign them to your users.
	Start Policy

HP Sure Start

ユーザーインタフェース

BIOS Security Settingsタブ

- Verify Boot Block on every boot --システムブートイメージへの許可された変更が不揮発性メモリに格納されていることを確認します。
- Dynamic Runtime Scanning of Boot Block—コン ピュータが起動していてOSが動作している時にHP ブートイメージの完全性を定期的に確認します。
- Lock BIOS Version—BIOS**のアップデートを禁止しま** す。
- Sure Start BIOS Setting Protection 全てのBIOS設定の変更を無効にしてHP Sure Startの不揮発性メモリからこれらのBIOS設定の保護を強化します。この設定を有効にするにはBIOS管理者パスワードの設定が必要です。
- Enhanced HP Firmware Runtime Intrusion Protection and Detection—OSが動作している時にメインメモ リで実行されているHPシステムファームウェアを 監視します。

	HP Client Security_1 - Sure Start		X
HP Sure Start			
Search	BIOS Security Settings		
HP Sure Start BIOS Security Settings	Sure Start solution is based on the HP BIOSphere includes the HP BIOS and a secure embedded co solution offerings for users.	e, HP's industry-leading firr ntroller. These settings all	nware ecosystem that ow you to customize the
Events and Recovery Settings	Show Information		
Audit Log Summary	Verify Boot Block on every boot	Enable	O Disable
	Dynamic Runtime Scanning of Boot Block	Enable	O Disable
	Lock BIOS Version	○ Enable	Disable
	Sure Start BIOS Settings Protection 🔺	Enable	O Disable
	Enhanced HP Firmware Runtime Intrusion Prevention and Detection	Enable	O Disable
	Some settings may not apply Some versions of HP Sure Start may require a	y to all devices. user to accept the chang	e during reboot. Next


Events and Recovery Settingsタブ

これらの設定ではBIOSが攻撃を受けたり破損するなどの危機的なセキュリティイベントが確認された際のHP Sure Startの動作を制御します。

- Sure Start Security Event Policy—ログレベルを選択します。
 - Log Event Only—HP Sure Start不揮発メモリ内の監査ログの 全てのクリティカルセキュリティイベントをWindowsイベ ントログに収集します
 - Log Event and Power Off System—セキュリティイベントを 検出してログ収集した後システムの電源を強制的に切り ます。
- BIOS Data Recovery Policy—Manualを選択した場合BIOS データの復旧にEsc+Windows+↑+↓キーの入力が必要 になります。
- Prompt on Network Controller Configuration Change-ネットワークコントローラの構成を監視して工場出 荷状態からの変更を検出した際にユーザーに通知し ます。
- Save/Restore Hard Drive Partition Table—システムドラ イブのMBRまたはGPTを保存します。



Audit Logタブ

[Gather Sure Start event logs]を選択するとクライアン トコンピュータからHP Sure Startイベントログを Configuration Managerのハードウェアインベントリに 収集します。

	HP Client Security_1 - Sure Start
HP Sure Start	
Search	Audit Log
HP Sure Start	When HP Sure Start heals the BIOS, an event log is generated to make you aware of a BIOS attack.
BIOS Security Settings	of these event logs through this policy.
Events and Recovery Settings	
Audit Log	
Summary	Gather Sure Start event logs
	You can retrieve the audit log data from this location:
	Device > Resource Explorer > Hardware Inventory
	Previous Next

ポリシーの作成

- Configuration Managerで、[資産とコンプライアンス]
 を選択し、[概要]を選択します。
- 2. HP Manageability Integration Kitを展開し、[Sure Start]を 右クリックして、[Create Policy]を選択します。
- 3. ベースライン名を入力し、[Start Policy]をクリックし ます。
- 4. 設定を変更し、[Next]をクリックします。
- 5. Summaryページで設定内容を確認して[Save Policy]を クリックします。
- 6. ポリシーの保存が完了したら、[Deploy]をクリックします。
- 7. ポリシーを適用するターゲットのコレクションを選 択し、[Deploy]をクリックします。



ポリシーの編集

- 1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
- 2. HP Manageability Integration Kitを展開し、[Sure Start]を右クリックして、[Edit Policy]を選択します。
- 3. ベースライン名を選択し、[OK]をクリックします。
- 4. ポリシー作成ウィザードのSummary画面が表示されますので[Previous]をクリックします。
- 5. ポリシーの作成と同じ手順を実行します。

追加情報

システムによっては一部の機能がサポートされていない場合があります。特定のシステムでは、構成の変更後に手動で再起動す る必要がある場合があります。

監査ログ

クライアントコンピュータでHP MIK Sure Startのログは%PROGRAMDATA%¥HP¥HP MIK¥Logsに保存されます。

設定が有効の場合、HP MIKはHP Sure StartログをConfiguration Managerのハードウェアインベントリとして収集します。 以下の手順で監査ログを表示します。

- 1. Configuration Managerで[資産とコンプライアンス]を選択し、[概要]を選択します。
- 2. [デバイス]を選択します。対象のデバイスを右クリックし、[開始]→[リソースエクスプローラー]を選択します。
- 3. [ハードウェア]を選択し、[HP Sure Start Audit Logs]を選択します。

TPM Firmware Update

TPM Firmware Updateポリシーでは以下の事ができます。ノートPC

- 古いTPM1.2から新しいTPM1.2へのアップグレード
- 古いTPM2.0から新しいTPM2.0へのアップグレード
- TPM1.2からTPM2.0への変換
- TPM2.0からTPM1.2への変換

サポート対象のクライアントコンピュータ

デスクトップPC

- HP EliteDesk 800 G2 Desktop Mini PC
- HP EliteDesk 800 G2 Small Form Factor PC
- HP EliteDesk 800 G2 Tower PC
- HP EliteOne 800 G2 23-inch Non-Touch All-in-One PC
- HP ProDesk 400 G2 Desktop Mini PC
- HP ProDesk 400 G3 Small Form Factor PC
- HP ProDesk 600 G2 Desktop Mini PC
- HP ProDesk 600 G2 Microtower PC
- HP ProDesk 600 G2 Small Form Factor PC
- HP ProOne 600 G1 All-in-One PC
- HP RP9 G1 Retail System Model 9015 / 9018

- HP EliteBook 1030 G1 Notebook PC
- HP EliteBook 725 G3 Notebook PC
- HP EliteBook 755 G3 Notebook PC
- HP EliteBook 820 G3 Notebook PC
- HP EliteBook 840 G3 Notebook PC
- HP EliteBook 850 G3 Notebook PC
- HP EliteBook Folio G1 Notebook PC
- HP Elite x2 1012 G1
- HP ProBook 430 G3 Notebook PC
- HP ProBook 450 G3 Notebook PC
- HP ProBook 455 G3 Notebook PC
- HP ProBook 470 G3 Notebook PC
- HP ZBook 15 G3 Mobile Workstation 26
- HP ZBook 17 G3 Mobile Workstation
- HP ZBook Studio G3 Mobile Workstation

サポート05

- Windows 10
- Windows 8.1
- Windows 7

前提条件

- Infineon SLB9670 TPMチップ
- 最新バージョンのBIOS
- Microsoft .NET Framework 4.0以上
- HP MIK

TPM Firmware Update

ポリシーの作成

- Configuration Managerで、[資産とコンプライアンス]
 を選択し、[概要]を選択します。
- 2. HP Manageability Integration Kitを展開し、[TPM Firmware Update]を右クリックして、[Create Policy]を 選択します。
- 3. ベースライン名を入力し、[Start Policy]をクリックします。
- 変更後のTPMのバージョンを選択し、[Next]をクリックします。警告と制限については追加情報をご参照ください。
- 5. Summaryページで設定内容を確認して[Save Policy]を クリックします。
- 6. ポリシーの保存が完了したら、[Deploy]をクリックします。
- 7. ポリシーを適用するターゲットのコレクションを選択し、[Deploy]をクリックします。

	HP Client Securi	ty_1 - Trusted Platform Module
HP Trusted Pla	tform Module Firm	ware Update
A TPM (Trusted Platform Modu platform measurements, certifi	ile) processor provides basic s cates, ad encryption keys.	security-related functions, primarily related to the creation or secure storage of
This policy will provide the user from version 2.0 to version 1.2.	rs the ability to update Trustec	d Platform Module (TPM) firmware from version 1.2 to version 2.0 and also mo
Which version of the firmwar	re do you want to move to?	
Which version of the firmwar Select TPM Firmware Version	re do you want to move to? Version 2.0	~
Which version of the firmwar Select TPM Firmware Version TPM Firmware Version 2.0 TPM 2.0 enables greater crypto	re do you want to move to? Version 2.0 o agility by being more flexible	vith respect to cryptographic algorithms. TPM 2.0 also offers a more



TPM Firmware Update

ポリシーの編集

- 1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
- 2. HP Manageability Integration Kitを展開し、[TPM Firmware Update]を右クリックして、[Edit Policy]を選択します。
- 3. ベースライン名を選択し、[OK]をクリックします。
- 4. ポリシー作成ウィザードのSummary画面が表示されますので[Previous]をクリックします。
- 5. ポリシーの作成と同じ手順を実行します。

追加情報

警告

データの消失を防ぐためにプライマリドライブの暗号化を解除してからこのポリシーを展開してください。このポリシーではBitLockerとWinMagic ドライブ暗号化のみをチェックします。BitLockerやWinMagicドライブ暗号化を使用している場合、このポリシーはエラーコードを出して終了しま す。このポリシーではその他のドライブ暗号化ソリューションを検出しません。

TPM1.2とTPM2.0の間の変換は最大64回可能です。

TPMを変換すると新しいバージョンのTPMファームウェアにアップグレードされます。

- TPM1.2からTPM2.0に変換するとTPM2.0が有効になり、TPM2.0の新しいバージョンにアップグレードされます。
- TPM2.0からTPM1.2に変換するとTPM1.2が有効になり、TPM1.2の新しいバージョンにアップグレードされます。
- TPM1.2からTPM1.2に変換するとTPM1.2の新しいバージョンにアップグレードされます。
- TPM2.0からTPM2.0に変換するとTPM2.0の新しいバージョンにアップグレードされます。

HP WorkWise(Windows 10のみ)

HP WorkWiseはスマートフォンを利用するアプリケーションで、PCのセキュリティ向上、監視、操作の簡略 化などの機能があります。ユーザーは各自のスマートフォンにHP WorkWiseアプリをストアからダウンロー ドしてインストールできますが、IT管理者はクライアントコンピュータでどの機能の利用を許可するかを指 定する事ができます。

サポート対象のクライアントコンピュータ

・2017年モデル以降のHPコマーシャルコンピュータ

サポート対象のOS

• Windows 10 Anniversary Update

前提条件

- Microsoft .NET Framework 4.0以上
- ・ HP WorkWise ソフトウェア

HP WorkWiseの各機能に固有の要件ついてはHP WorkWiseのドキュメントをご参照ください。



HP WorkWise

ユーザーインタフェース

HP WorkWiseの機能の有効/無効を設定できます。

- All Features—全ての機能を有効にします。
- Security—Lock/UnLockとTamper Detectionの機能を 有効/無効にします。
- Performance—PC DashboardとHot PC remedation機 能を有効/無効にします。
- Printer—Printer Driver Installerの機能を有効/無効にします。

	HP Client Security_1 - Work Wise		×
✓ All Features			
✓ Security			
Lock/Unlock	• On	○ Off	
Tamper Detection	• On	○ off	
✓ Performance			
PC Dashboard	On	○ off	
Dashboard Details	• On	○ Off	
Hot PC remediation	• On	○ off	
☑ Printer			
Printer Driver Installer	• On	⊖ off	
		Next	

HP WorkWise

ポリシーの作成

- 1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
- 2. HP Manageability Integration Kitを展開し、[HP WorkWise]を右クリックして、[Create Policy]を選択します。
- 3. ベースライン名を入力し、[Start Policy]をクリックします。
- 4. 変更後のTPMのバージョンを選択し、[Next]をクリックします。警告と制限については追加情報をご参照 ください。
- 5. Summaryページで設定内容を確認して[Save Policy]をクリックします。
- 6. ポリシーの保存が完了したら、[Deploy]をクリックします。
- 7. ポリシーを適用するターゲットのコレクションを選択し、[Deploy]をクリックします。

ソフトウェアライブラリ

ソフトウェアライブラリ

HP Manageability Integration Kitをインストールするとソフトウェアライブラリに以下の項目が追加(青色実線)または作成可能(緑色破線)になります。



ドライバーパッケージとは

ドライバパッケージは1つまたは複数のデバイスドライバの内容を含むConfiguration Managerのパッケージです。ド ライバーパッケージはタスクシーケンスの中で05イメージに追加します。05イメージに新しいPCの機種のための ドライバーパッケージを追加する事でその05イメージを新しいPCの機種で利用する事ができるようになります。

HP MIKの機能

HP MIKをインストールするとドライバーパッケージを作成するための以下の3つの機能が追加されます。

- Create and Import Driver Pack
 - 複数の機種用のドライバーをHPからダウンロードして複数の機種に対応するドライバーパッケージを作成する事ができます。
 - HPドライバーパックの作成をサポートする機種でのみ利用可能です。
- Download and Import Driver Pack
 - 1つのHPドライバーパックをHPからダウンロードして1つのドライバーパッケージを作成する事ができます。
 - HPドライバーパックが提供されている機種(600シリーズ以上のビジネスPC製品)でのみ利用可能です。
- Import Downloaded Driver Pack
 - 自分で作成したドライバーパックをインポートして1つのドライバーパッケージを作成する事ができます。
 - HPドライバーパックが提供されていない機種(400シリーズ以下のビジネスPC製品)ではこの方法を使用します。





HPドライバーパックの作成とインポート

Create and Import Driver PackオプションではサポートされるHP製品のドライバーが表示されます。

- 1. Configuration Managerで、[ソフトウェアライブラリ]→[概要]→[オペレーティングシステム]→[ドライ バー パッケージ]を選択します。
- 2. リボンメニューのHP Client PCsセクションの[Create and Import Driver Pack]を選択します。 Create and Import Driver Packウィザードが表示されます。
- 3. [Operating System]を選択します。
- 4. ドライバーパックの作成をサポートする製品のみが、Available Products列に表示されます。必要に応じて キーワードをHP製品名ボックスに入力し、Enterキーを押して使用可能な製品の一覧をフィルタします。
- 5. 使用可能な製品を選択し、右矢印ボタンを選択してSelected製品列に製品を追加します。
- 必要に応じて手順5を繰り返して、別の製品を選択します。同じファミリモデルの製品を選択すること をお勧めします。最適なドライバを使用してドライバパックを作成します。また、ドライバーパックご とに5つ以下の製品を選択することをお勧めします。例えば、HP ProBook 640 G1ノートブックPCとHP ProBook 650 G1ノートブックPCを選択して、HP ProBook 600シリーズG1ノートブックPCドライバパックを 作成することができます。





- 8. [Next]をクリックします。
- デフォルトではimport optionに[Create driver package with the selected drivers below]が選択されています。このオプションでは選択したドライバーを含むドライバーパッケージを作成します。
 A.ドライバーパッケージに付ける名前を入力します。必要に応じてバージョンとコメントを入力します。
 B.Driversの下で、ドライバーパッケージに含めるドライバーが選択されている事と、その他のドライバーのチェックが外れている事を確認します。

または、自動適用するドライバをインポートして 後でドライバパックを作成するには、[Import driver(s) only]オプションを選択します。デフォルト では、インポートされたドライバのドライバカテ ゴリはHP Client Driverです。必要に応じて、別のド ライバカテゴリを選択します。

10. [Next]をクリックします。

Enter a drive	er package name and select	drivers to import.	
Import options:	Oreate driver package with the s Import driver(s) only.	elected drivers below.	
Driver package:			
Name:	FliteBookG4DriverPack		Version: 1.0
Comment:	EliteBookG4Series		
Drivers:	Select/Deselect all		Q
Name		Version	Category
Alcor Micro Smar Alps HID Mouse Alps HID Mouse AMD IO Driver AMD Video Drive ASMedia eXtensi Broadcom Ethern Conexant HD Au Conexant HD Au Conexant HD Au Conexant HD Au Conexant USB A HP 3D DriveGuar C	rt Card Reader Driver Driver er and Control Panel ible Host Controller (xHCI) Driver let Controller Drivers -64bit (BNB) dio Driver dio Driver dio Driver udio Driver dio Driver III material: 25	17.45.10 A 1 82206.1717.610 A 3 12.0.60 T 1 16.40.2805.1001 C 1 1.16.43.1 A 1 17.4.0.1 A 4 11.29.1680.44 Q 52 11.22.1300.39 Q 5 11.30.1680.45 Q 52 13.13.6.18 A 1 6.0.41.1 A 2	Driver - Storage Driver - Keyboard, Mouse and Input Dev E Driver - Chipset Driver - Graphics Driver - Chipset Driver - Audio Driver - Audio Driver - Audio Driver - Audio Driver - Storage ➤
		< Previous	Next > Close

- ドライバーパッケージを作成している場合は、 以下の手順で配布ポイントとネットワーク共有 を設定します。
 A.配布ポイントを選択します。クラウド配布ポ イントはサポートされていません。
 B.Configuration ManagerがDriversとDriver Package(s)を保存するためのネットワーク共有を 選択します。
- 11. ドライバーをインポートするだけの場合は、 Configuration ManagerがDriversを保存するための ネットワーク共有を選択します。
- 12. エラーが発生したときにインポートを停止する 必要がある場合は、[Continue on errors]オプショ ンをオフにします。デフォルトでは、このボッ クスが選択されています。複数のドライバが選 択されている場合、現在のドライバがインポー トに失敗した場合は、次に選択されたドライバ がインポートされます。

D	Create	and Import HP Client Driver Pack	×
Select distrit	oution point(s), netwo	ork shares and other settings.	2
Distribution point(s			Select all
Select network sha	re(s) and other settings.		
Drivers:	¥¥HPI-SCCMhpi.local¥SMS_H0	1¥OSD¥Lib¥Drivers¥HP¥Client	Browse
Driver package(s):	¥¥HPI-SCCMhpi.local¥SMS_H0	Browse	
Error handling:	✓ Continue on errors File transfer protocol: HTTP		Save settings
		< Previous Import	Close

חח

- 12. デフォルトではFile transfer protocolがHTTPになっており、HP MIKは選択したドライバーのダウンロードに HTTPを使用します。必要に応じて[FTP]を選択してください。
- 13. ネットワーク共有の選択やその他の設定の設定を変更すると、[Save Settings]ボタンが有効になります。 後続のドライバおよびドライバパッケージの作成またはインポート手順の設定を保存するには、このボ タンを選択します。

注記

このプロセスではConfiguration Managerから<u>ftp.hp.com</u>へのインターネット接続が必要となります。イン ターネット接続できない場合は次の手順の方法でドライバーパックを入手した後、[Import Downloaded Driver Pack]メニューを使用してインポートします。

	(DD)		(hp)
ドライバー パッ ドライバー パッケー ケージの作成 ジのインポート	Create and Import Driver Pack	Download and Import Driver Packs	Import Downloaded Driver Pack
作成	HP Client PCs	HP Client PCs	HP Client PCs

HPドライバーパックのダウンロードとインポート

Download and Import Driver PackオプションではサポートされるHP製品とドライバーパックが表示されます。

- 1. Configuration Managerで、[ソフトウェアライブラリ]→[概要]→[オペレーティングシステム]→[ドライ バー パッケージ]を選択します。
- 2. リボンメニューのHP Client PCsセクションの[Download and Import Driver Pack]を選択します。
- 3. [Operating System]を選択します。
- 4. ドライバーパックの作成をサポートする製品のみが、Available Products列に表示されます。必要に応じて キーワードをHP製品名ボックスに入力し、Enterキーを押して使用可能な製品の一覧をフィルタします。
- 5. 対象となるオペレーティングシステムの展開に含めるドライバパックを選択し、右矢印ボタンを選択し て、Selected products列に製品を追加します。選択した製品の関連するドライバーパックがAvailable driver packsの一覧に表示されます。
- 6. 配布ポイントを選択して、インポートされたドライバパックを特定の宛先に割り当てます。クラウド配 布ポイントはサポートされていません。
- 必要に応じてConfiguration Managerがドライバーやドライバーパッケージを保存するデフォルトの場所を 変更します。保存先の選択やその他の設定の設定を変更すると、[Save Settings]ボタンが有効になります。 後続のドライバおよびドライバパッケージのダウンロードおよびインポート手順の設定を保存するには、 このボタンを選択します。

- エラーが発生したときにインポートを停止する必要がある場合は、[Continue on errors]オプションをオフ にします。デフォルトでは、このボックスが選択されています。複数のドライバが選択されている場合、 現在のドライバがインポートに失敗した場合は、次に選択されたドライバがインポートされます。
- 9. デフォルトではFile transfer protocolがHTTPになっており、HP MIKは選択したドライバーパックのダウン ロードにHTTPを使用します。必要に応じて[FTP]を選択してください。
- 10. [Download and Import]をクリックするとドライバーパックのダウンロードとインポートのプロセスが開始します。

ダウンロードとインポートのプロセスの最中には処理内容と進捗状況のダイアログボックスが表示され ます。このプロセスでは選択したドライバーパックをダウンロードして、Configuration Managerにイン ポートします。選択したドライバーパックがConfiguration Managerの中に既に存在している場合は既存の ドライバーパックを上書きするか、またはスキップするかを選択するためのプロンプトが表示されます。 プロセスが完了すると各ドライバーパックごとのインポート状態のサマリが表示されます。 インポートしたドライバーパックは[ドライバーパッケージ]→[HP Driver Packages]の下に作成されます。 インポートしたドライバーパックをタスクシーケンスで使用するには配布ポイントに展開されている必 要があります。Download and Import Driver Packsウィザードで配布ポイントを選択していなかったり、追 加の配布ポイントを使用したい場合はドライバーパックを選択して[コンテンツの配布]を選択します。 注記

このプロセスではConfiguration Managerから<u>ftp.hp.com</u>へのインターネット接続が必要となります。イン ターネット接続できない場合は次の手順の方法でドライバーパックを入手した後、[Import Downloaded Driver Pack]メニューを使用してインポートします。

HPドライバーパックのダウンロードとインポート

Select an operating		
	system and HP product(s).	
Operating system:	Microsoft Windows 10 64-bit	×
HP product name:	Type HP product name (with no special	characters).
Available products:		Selected products:
HP EliteDesk 800 HP EliteDesk 800 HP EliteDesk 800 HP EliteDesk 800 HP EliteDesk 800 HP EliteDesk 800 HP EliteDesk 880 HP EliteOne 705 G HP EliteOne 800 G HP EliteOne 800 G	15W G2 Desktop Mini PC 15W G3 Desktop Mini PC 15W G3 Desktop Mini PC 28 Small Form Factor PC 29 Small Form Factor PC 21 Tower PC 22 Tower PC 23 Tower PC 2 23-inch Touch All-in-One PC 2 23-inch Non-Touch All-in-One PC 2 23-inch Touch All-in-One PC	A) A HP EliteDesk 800 G3 Small Form Factor PC K K
Available driver pa	ks:	
Name	Versi	on Released Date Size (MB) Driver Pack ID View Release Notes Re
Distribution point(-)	
Select network sh	re(s) and other settings.	
Select network sh	re(s) and other settings. ¥¥HPI-SCCM.hpi.local¥SMS_H01¥OSD4	Lib¥Drivers¥HP¥Client Browse
Select network sh Drivers: Driver package(s)	Are(s) and other settings. ¥¥HPI-SCCMhpi.local¥SMS_H01¥OSD4 ¥¥HPI-SCCMhpi.local¥SMS_H01¥OSD4	✓ Select all
Select network sh Drivers: Driver package(s) Error handling:	Prescent HPILOCAL are(s) and other settings. ¥¥HPI-SCCM.hpi.local¥SMS_H01¥OSD4 ¥¥HPI-SCCM.hpi.local¥SMS_H01¥OSD4 ✓ Continue on errors	#Lib¥Drivers¥HP¥Client Browse #Lib¥DriverPackages¥HP¥Client Browse File transfer protocol: HTTP Save settings

HPドライバーパックの入手方法

HPドライバーパックにはいくつかの入手方法があります。

注記

ー部のドライバーはHP MIKで利用できないものもあります。例えばシステム—ソフトウェア管理の下のカテゴリのドライバーはHP MIKからインポートできません。

- HP Client Management Solutionウェブサイト
- HP Softpaq Download Manager(SDM)

HP Client Management Solution ウェブサイトからのドライバーパックの入手方法

- 1. <u>http://www.hp.com/go/clientmanagement</u> にアクセスします。
- 2. Resourcesの下の[HP Driver Packs]をクリックします。
- 3. 32-bit**または**64-bit**を選択します**。
- 4. 対象のクライアントコンピュータとOSに対応したドライバーパックをダウンロードします。



HP SDMを使用したドライバーパックの入手方法

- 1. <u>http://www.hp.com/go/clientmanagement</u>にアクセスします。
- 2. Resourcesの下の[HP Download Library]をクリックします。
- 3. [SoftPaq Download Manager]をダウンロードします。
- 4. ダウンロードしたSDMをインストールします。
- 5. SDMを起動します。[すべてのプログラム]→[HP]→[HP Softpaq Download Manager]。
- 6. [すべての製品を表示]を選択します。
- 7. [ツール]→[構成オプション]を選択します。
- 8. Filter→OSICSDMで表示するOSの種類を選択します。
- 9. Filter→Languageに[English International]を選択します。

10.構成オプションで[OK]をクリックします。

11. 製品カタログで、対象の製品名とOSを選択し、[利用可能なSoftPaqの検索]をクリックします。

12. CategoryがManageability – Driver Packにあるドライバーパックをダウンロードします。

HP SDMを使用したドライバーパックの作成方法

HP SDM(バージョン3.5.2.0以上)を使用してドライバーパックする事ができます。ドライバーパックが提供 されていないコンピュータではこの方法を使用して自作します。

- 1. SDMを起動します。[すべてのプログラム]→[HP]→[HP Softpaq Download Manager]。
- 2. [Driver Packをビルド]を選択します。
- 3. [ツール]→[構成オプション]を選択します。
- 4. Filter→OSでSDMで表示するOSの種類にチェックを付けます。
- 5. Filter→Languageに[English International]を選択します。
- 6. 構成オプションで[OK]をクリックします。
- 7. 製品カタログで、対象の製品名とOSを選択し、[利用可能なSoftPaqの検索]をクリックします。
- 8. すべての利用可能なSoftPagで、ドライバーパックに含めるSoftPagを選択します。
- 9. ダウンロードされたSoftPaqで、ダウンロードボタンの隣のドロップダウンメニューから[CABファイルの ビルド]を選択します。

10.[ダウンロード]をクリックします。

- 11. 使用許諾契約書画面が表示されたら[使用許諾契約書に同意します。]を選択して、[続行]をクリックします。
- 12. Driver Pack BuilderウィンドウでOS-BitnessにOSと ビット数を選択します。
- 13. ドライバーパックの名前や出力先のフォルダを 設定して[Build]をクリックします。
- 14. ドライバーパックの圧縮が完了しましたのダイ アログが表示されたら[OK]をクリックします。
- ドライバーパックと関連のログが出力先フォルダに 作成されます。

	HP SoftPaq Download Manager
ファイル ツール ヘルプ 🔗 更新を確認 🔗 このコンビューターを表示 🔗 すべての製品を表示 <u>용</u> ロ)river Packをビルド
品力タログ	すべての利用可能なSoftPaq
利用可能なSoftPaqの検索 🔩 すべてクリア 🔍 モデルの検索 🛛 📓 ウィサ	fード 💊 SoftPaqを選択 🕶 🔍
 HP Notebook PCs HP EliteBook Notebook PCs HP ProBook Notebook PCs HP ProBook Notebook PCs HP Business Desktop PCs HP 200 Business Desktop PC series HP 400 Desktop PC series HP EliteDesk 700 Desktop PC series HP EliteDesk 800 Desktop PC series HP EliteDesk 800 Desktop PC series HP ProDesk 400 G1 Small Form Factor PC HP ProDesk 400 G2 Desktop Mini PC Wicrosoft Windows 10 64-Bit Wicrosoft Windows 10 64-Bit HP ProDesk 400 G2 Small Form Factor PC HP ProDesk 400 G3 Desktop Mini PC 	Name Intel Management Engine Interface Driver Intel Rapid Storage Technology Driver and Configuration Software Intel Rapid Storage Technology Driver and Configuration Software Intel Windows x64 Graphics Driver - 15.40-64bit Intel Windows x64 Graphics Driver - 15.40-64bit Intel Windows x64 Graphics Drivers (DTO) Realtek Ethernet Controller Drivers (DTO) Controller Drivers (DTO) Realtek Ethernet Controller Drivers (DTO) Controller Dr





HPドライバーパックのインポート

- 1. Configuration Managerで、[ソフトウェアライブラリ]→[概要]→[オペレーティングシステム]→[ドライ バー パッケージ]を選択します。
- 2. リボンメニューのHP Client PCsセクションの[Import Downloaded Driver Pack]を選択します。
- 3. [Browse]をクリックしてインポートするドライバーパックを選択します。
- 配布ポイントを選択して、インポートされたドライバパックを特定の宛先に割り当てます。クラウド配 布ポイントはサポートされていません。
- 5. 必要に応じてConfiguration Managerがドライバーやドライバーパッケージを保存するデフォルトの場所を 変更します。
- 6. 保存先の選択やその他の設定の設定を変更すると、[Save Settings]ボタンが有効になります。後続のドラ イバおよびドライバパッケージのダウンロードおよびインポート手順の設定を保存するには、このボタ ンを選択します。
- 7. [Import]をクリックします。

ダウンロードとインポートのプロセスの最中には処理内容と進捗状況のダイアログボックスが表示されま す。インポートしたドライバーパックは[ドライバーパッケージ]→[HP Driver Packages]の下に作成されます。 インポートしたドライバーパックをタスクシーケンスで使用するには配布ポイントに展開されている必要 があります。Download and Import Driver Packsウィザードで配布ポイントを選択していなかったり、追加の配 布ポイントを使用したい場合はドライバーパックを選択して[コンテンツの配布]を選択します。

HP Client Driver Pack HPドライバーパックのインポート

D	Import Downloaded HP Client Driver Pack		X
Select an HP client d	iver pack to import.		
Driver package:	C:#HPSDM#ProDesk400G2DMDriverPack#ProDesk400G2DM_DriverPack_wt64_2017-03-	Browse	
Driver pack title:	ProDesk400G2DM DriverPack		
Distribution point(s):	HPI-SCCM.HPILOCAL	✓ Select all	
Select network share(Drivers:	s) and other settings. ¥¥HPI-SCCM.hpi.local¥SMS_H01¥OSD¥Lib¥Drivers¥HP¥Client	Browse	_
Driver package(s):	¥¥HPI-SCCM.hpi.local¥SMS_H01¥OSD¥Lib¥DriverPackages¥HP¥Client	Browse	٦
		Save settings	1
	Import	Close	

WinPE**ドライバーパックの入手**

- 1. <u>http://www.hp.com/go/clientmanagement</u> にアクセスします。
- 2. Resoucesの下の[HP Download Library]をクリックします。
- 3. [HP WinPE Driver Pack 32-bit]または[HP WinPE Driver Pack 64-bit]をダウンロードします。

注記

Configuration Managerの各バージョンは、特定のバージョンのWinPEのみにドライバやコンポーネントをカス タマイズまたは追加することをサポートしているため、HP MIK Create Boot Imageは限定的なサポートを提供 します。WinPEのカスタマイズの要件の詳細については、

http://technet.microsoft.com/en-us/library/dn387582.aspx

を参照してください。

HP MIKブートイメージの作成機能は、ブートイメージ用のConfiguration ManagerとADKカスタマイズサポート を活用しているため、HP MIKの制限は、Configuration Managerのバージョン、ADKのバージョン、およびサイ トサーバーのオペレーティングシステムのバージョンに依存します。





WinPEドライバーパックのインポートとブートイメージの作成

- 1. Configuration Managerで、[ソフトウェアライブラリ]→[概要]→[オペレーティングシステム]→[ブートイ メージ]を選択します。
- 2. リボンメニューのHP Client PCsセクションの[Create Boot Image]を選択します。
- [Browse]をクリックしてインポートするWinPEドライバーパックを選択します。HP MIKには、選択した WinPEドライバパックに適したブートイメージのみが表示され、Configuration Managerによるカスタマイ ズがサポートされています。
- 対象のブートイメージ(Base boot image)を選択します。[Create]をクリックして選択したHP WinPEドライバパックを含んだブートイメージを作成します。
- 5. 配布ポイントを選択して、インポートされたドライバパックを特定の宛先に割り当てます。しかし、ク ラウド配布ポイントはサポートされていません。
- 必要に応じてConfiguration Managerがドライバーやドライバーパッケージを保存するデフォルトの場所を 変更します。
- 7. 保存先の選択やその他の設定の設定を変更すると、[Save Settings]ボタンが有効になります。後続のドラ イバおよびドライバパッケージのダウンロードおよびインポート手順の設定を保存するには、このボタ ンを選択します。

Ø	Create HP Client Boot Image(s)		x
Specify an HP client WinPE d	river pack and base boot image(s) to create HP client boot images.		
HP client WinPE driver pack:	C#Users#Administrator#Downloads¥sp78464.exe	Browse	
Driver pack title:	HP Client WinPE 10.0 x64 Driver Pack [1.30.A.1]		
	Boot image (x64)		
Base boot image(s):			
		8	
Distribution point(s):		Select all	
Select network share(s) and c	ther settings.		
Drivers:	¥¥HPI-SCCM.hpi.local¥SMS_H01¥OSD¥Lib¥Drivers¥HP¥Client	Browse	
Driver package(s):	¥¥HPI-SCCM.hpi.local¥SMS_H01¥OSD¥Lib¥DriverPackages¥HP¥Client	Browse	
Boot image(s):	¥¥HPI-SCCMhpi.local¥SMS_H01¥OSD¥Lib¥BootImages¥HP¥Client	Browse	
		Save settings	
	Create	Close	



- ベースイメージのアーキテクチャとWindowsプレインストール環境ブートイメージでサポートされている アーキテクチャに応じて、x86および/またはx64イメージが作成されます。
- Windows 10用のHP WinPEドライバーパックには、64ビットのブートイメージ用のドライバが含まれています。
- 以前のバージョン用のWinPEドライバーパックには32ビットと64ビットの両方のブートイメージ用のドライバが含まれています。
- プロセスが完了すると、新しいブートイメージが[ブートイメージ]→[HP Client Boot Images]に作成されます。 WinPEでデバッグ目的でコマンドプロンプトを使用するためには以下の設定を行います。
- 1. ブートイメージを右クリックして[プロパティ]を選択します。
- 2. [カスタマイズ]タブを選択し、[コマンドサポートを有効にする(テストのみ)]を有効にします。
- これらのブートイメージをタスクシーケンスで使用する前に、ブートイメージを配布ポイントに展開する 必要があります。
- インポートプロセスで配布ポイントが選択されていない場合、または追加の配布ポイントが必要な場合、 またはブートイメージのプロパティを変更した場合は、ブートイメージを選択して、[コンテンツの配布]を 選択します。

חה

デプロイメントタスクシーケンスの作成

- 1. Configuration Managerで、[ソフトウェアライブラリ]→[概要]→[オペレーティング システム]→[タスク シーケンス]を選択します。
- 2. リボンメニューのHP Client PCsセクションの[Create Deployment Task Sequence]を選択します。
- Task Sequence Template ドロップダウンメニューからテンプレートを選択します。次のテンプレートが選択可能です。
 - Default template for Windows 10 : Windows 10用のテンプレート
 - Default template for Windows 7 or Windows 8: Windows 7/8用のテンプレート
 - Configure RAID example : RAID構成用のテンプレート
- 4. Task sequence nameとNetwork account情報を入力します。
- 5. BitLocker **ドライブ暗号化**(BDE)を使用しない場合は[Include BitLocker Drive Encryption steps]のチェックを外しま す。

Configuration ManagerのBDEタスクシーケンスステップの情報は以下を参照してください。 https://technet.microsoft.com/enus/library/hh846237.aspx

- 6. [Create]をクリックします。
- 7. Successのダイアログで[OK]をクリックします。

Task sequence template:	Default template for Windows 10		Ŷ
	A default task sequence example for W BIOS settings in a task sequence using user guide on how to configure the HP	Vindows 10 that shows you how to change g HP BIOS Configuration Utility. Please read BIOS using the Set BIOS Configuration ste	HP Ithe p.
Task sequence name:	HP Client Task Sequence		
Network (Administrator) ac	count:		
Enter administra	tor-level credentials to access shares an	nd WMI on the site server.	
Account name:	Domain¥UserName		
Password:		0	
Confirm passwo	rd:		
Operating system installation Use an OS 1 Scripted OS Operating system	nn: NIM m package to use		
0		v 🧿	
🗹 Include BitL	ocker Drive Encryption steps		
Required HP client packag	ges:		
HP Client HP Client	BIOS Configuration Utility Support Tools		

重要

選択したテンプレートに応じて、以下のステップは データの削除を伴います。

- Remove Disk Partitions(diskpart clean)
- Format and Partition Disk
- Call Intel RSTCli Utility Delete All Metadata
- Call Intel RSTCli Utility Configure RAID Volume

作成したタスクシーケンスはテスト環境で十分に検 証してから本番環境で実行するようにしてください。 HPではこれらのタスクシーケンスの実行によるいか なるデータ消失に対して責任を負いかねます。

タスクシーケンスの設定

タスクシーケンスのリストを更新して、作成したタスクシーケンスを表示します。タスクシーケンスを使用する前に、タスクシーケンスが正常に実行されるように設定する必要があります。

Configure RAID Exampleテンプレートに含まれている特定のステップは「Configure RAID Exampleテンプレートの使用」で説明します。

- 対象のクライアントコンピュータのドライバーパックがインポートされている事を確認します。詳細は 「HP Client Driver Pack」の章を参照してください。
- 2. 対象のタスクシーケンスを右クリックして[編集]を選択します。
- タスクシーケンスで参照されているオブジェクトが見つからない事のダイアログが表示されますので [OK]をクリックします。

以下の画像はDefault Template for Windows 10テンプレートを使用して作成したタスクテンプレートのものです。

Windows 10の場合、推奨されるWindows回復ツールパーティションはドライブの最後にあります。デフォルトのパーティションはディスク容量の1%となっています。必要に応じてこの値をWindowsリカバリイメージのサイズ(通常500 MB以上)に変更します。

חח



HP Windows	10 Client Task Se	quence タスク シーケンス エディター		
追加(<u>A</u>) • 削除(<u>R</u>) 計 (量)	プロパティ オプション			
🔮 Restart in WinPE	種类頁:	Windows と ConfigMer のセットアップ		
Set BIOS Configuration (Input F	名前(<u>N)</u> : [说明(<u>D</u>):	Setup Windows and ConfigMgr		
 Install Operating System Remove Disk Partitions (diskpa Partition Disk 0 - BIOS Partition Disk 0 - UEFI Apply Operating System Image Apply Windows Settings Apply Driver Package Apply Network Settings Setup Windows and ConfigMer 		Actions to setup Windows and Configuration Manager		
	サイトの書的当てと構成は自動的に指定されます。Configuration Manager クライアントの インストール時に使用する追加のインストール プロパティを指定してください。			
	クライアント パッケージ(<u>C</u>): 参照(B)		
	□ 使用可能な場合は、実稼働前クライアントパッケージを使用する(U) 実稼働前クライアントパッケージ 参照(W)			
	ፈንጋኑ~ルወታወለም ው			
< III >		✓ OK キャンセル 通用(Y)		

П

- 4. デプロイメントの対象OSに応じて以下のステップを設定します。
 - Set BIOS Configuration (Input file)—BIOS Config Utilityを使用してBIOS設定を変更できます。TPMを使用する 場合はこのステップでTPMを有効にして初期化する必要があります。詳細は「Set BIOS Configurationタ スクステップの設定」を参照してください。
 - Remove Disk Partitions(diskpart clean) ーこのステップの設定は不要です。タスクシーケンスが適切に実行 されるにはネットワーク上のコンテンツディレクトリにアクセスできるように設定されている必要が あります。詳細は「Allowing access to deproyment content」を参照してください。このステップが不要 な場合はステップを無効にしてください。
 - Format and Partition Diskーディスクを必要に応じてフォーマットおよびパーティション化するための適切な手順を有効にします。たとえば、UEFIまたはUEFI Hybrid (CSMを使用)に設定されているシステムに展開する場合は、EFIフォーマットステップを有効にして、BIOSフォーマットステップを無効にします。
 - Apply Driver Packages ーデプロイメント対象のOSイメージに追加するHPドライバーパックを選択します。
 - Apply Network Settingsーデプロイメント対象をワークグループにするかドメインに参加するかを選択し、
 必要に応じてActive Deirectoryドメインのアカウント情報を入力します。

追加のタスクシーケンスステップを参照し、必要に応じて追加およびパラメータを設定します。

5. すべてのタスクシーケンスステップの設定が完了したら[OK]または[適用]をクリックして変更を保存します。
| HP Client | Task Sequen | ce |
|------------------|-------------|----|
|------------------|-------------|----|

HP Windows	10 Client Task S	equence	タスク シーケンプ	スエディター	- 🗆 X
追加(A) • 削除(R) 👘 🕻	プロパティ オプション				
追加(A) - 削除(R) 日 (A) We Restart in WinPE Configure Hardware Set BIOS Configuration (Input F Install Operating System Remove Disk Partitions (diskpa Partition Disk 0 - BIOS Partition Disk 0 - UEFI Apply Operating System Image Apply Windows Settings Partiver Package Apply Network Settings Setup Windows and ConfigMer	プロパティ オブション 種類 名前(<u>N</u>): 説明(<u>D</u>): 	ドライバー / Apply Driv (に利用可能に (に利用可能に (): [回]: (): [回]: (): [回]: (): [回]: (): []: (): []: (): []: (): : (): <td>《ッケージの適用 er Package なるドライバーが含 G4DriverPack 1.0 Fィング システムをセ ドーをパッケージから</td> <td>まれるドライバー パー コントアップする前にイ ジェボする(S)</td> <td>>ッケージを選択 参照(E)</td>	《ッケージの適用 er Package なるドライバーが含 G4DriverPack 1.0 Fィング システムをセ ドーをパッケージから	まれるドライバー パー コントアップする前にイ ジェボする(S)	>ッケージを選択 参照(E)
< <u> </u>	▶ でドライバーの無人	インストールを 	行う(W) のK	年初七川	適用(ゾ)



ブートイメージの割り当て

- 1. 対象のタスクシーケンスを右クリックして[プロ パティ]を選択します。
- 2. [詳細設定]タブを選択し、[ブートイメージを使用する]をクリックして有効にします。
- 3. [参照]をクリックしてHP Client Boot Imagesフォル ダーから適切なブートイメージを選択します。
- 4. [OK]をクリックします。

注記

ブートイメージはデプロイメント対象のOSと同じ アーキテクチャのものを選択します。X86/32-bit OS の場合はx86イメージを、x64/64-bit OSの場合はx64 イメージを選択します。

	ask Sequence 0/1////
全般 詳細設定 セキュリティ	
別のプログラムを最初に実行する(E):	
パッケージ(<u>P</u>):	参照(<u>R</u>)
プログラム(<u>M</u>):	
□ このプログラムを必ず最初に実行する(S)	
タスクシーケンスの通知を表示しない(E)	
── 展開先のコンピューターでこのタスク シーケンスを	無効にする(<u>D</u>)
許容最長実行時間(分)(T):	0
HP Client Boot Image (x64)	参照(<u>W</u>)
HP Client Boot Image (x64) ● 任意のプラットフォームで実行する(U)	参照())
HP Client Boot Image (x64) 任意のプラットフォームで実行する(U) 指定したクライアント プラットフォームだけで実行する 	参照(W) する(Q)
HP Client Boot Image (x64) ● 任意のプラットフォームで実行する(U) ● 指定したクライアント プラットフォームだけで実行す ■ すべての Windows RT ■ すべての Windows RT 81 	<u>参照(W)</u> する(Q)
HP Client Boot Image (x64) 任意のブラットフォームで実行する(U) 指定したクライアント ブラットフォームだけで実行す すべての Windows RT すべての Windows RT 8.1 すべての埋め込み Windows XP 	
HP Client Boot Image (x64) ● 任意のプラットフォームで実行する(山) ● 指定したクライアント プラットフォームだけで実行する ■ すべての Windows RT ■ すべての Windows RT 8.1 ■ すべての Windows RT 8.1 ■ すべての Windows NT 8.1 ■ すべての Windows NT 8.1 ■ すべての Windows 10 (32 ビット) ■ すべての Windows 10 (64 ビット)	<u>参照(W)</u> する(Q)
HP Client Boot Image (x64) ● 任意のプラットフォームで実行する(U) ● 指定したクライアント プラットフォームだけで実行する □ すべての Windows RT □ すべての Windows RT 8.1 □ すべての Windows RT 8.1 □ すべての Windows 10 (32 ビット) □ すべての Windows 10 (64 ビット) □ すべての埋め込み Windows 7 (64 ビット)	参照(W) する(Q) ▲
HP Client Boot Image (x64) ● 任意のプラットフォームで実行する(U) ● 指定したクライアント プラットフォームだけで実行する ■ すべての Windows RT ■ すべての Windows RT 8.1 ■ すべての埋め込み Windows XP ■ すべての Windows 10 (32 ビット) ■ すべての埋め込み Windows 7 (64 ビット)	参照(W) する(Q) へ 、 のK キャンセル 適用(,

デプロイメントコンテンツへのアクセス許可設定

HP MIKタスクシーケンスのRemove Disk Partitions(diskpart clean)ステップはネットワークから直接実行する必要があります。そのためには、ブートイメージを含むタスクシーケンスのすべてのパッケージとコンテンツが以下のように設定されている必要があります。

1. コンテンツ/パッケージを右クリックして[プロパティ]を選択します。

- 2. [データアクセス]タブを選択し、[このパッケージのコンテンツを配布ポイントのパッケージ共有にコ ピーする]をクリックして有効にします。
- 3. [OK]をクリックします。

Set BIOS Configurationタスクステップの設定

Set BIOS Configuration (Input File)タスクステップではBIOS設定 を行う事ができます。このコマンドラインの実行タスクで はBIOS Config Utility(BCU)を使用します。

このタスクシーケンスステップでは以下のコマンドライン を実行します。

RunBCU.cmd <BCUに渡すパラメータ>

パラメータやオプションの一覧はHP BIOS Configuration Utility User Guideを参照してください。

サンプルのBIOS設定(REPSET)ファイル (BCUSettingExampleOnly.REPSET)がBCUのソースフォルダ内 のConfigフォルダにあります。この設定ファイルを使用する 場合のコマンドラインは以下のようになります。

RunBCU.cmd /setconfig:"Config¥BCUSettingExampleOnly.REPSET"

REPSETファイルはコマンドラインを簡単にするためにBCU ソースフォルダまたはそのサブフォルダに置くことを推奨 します。



BIOS設定ファイルの追加および編集

注記

このタスクシーケンスステップを使用する際には以下を注意してください。

- パッケージフォルダのBIOS設定ファイルの追加や編集した時には、新しいBIOS設定ファイルがこのタスク シーケンスステップで使用できるようにHP BIOS Configuration Utilityパッケージを配布ポイントにアップ デートしてください。
- いくつかのBIOS設定変更はターゲットコンピュータが再起動するまで反映されません。全ての設定が適用 されるには再起動が必要な場合があります。
- 特定のBIOS設定を変更するとタスクシーケンスが失敗する場合があります。タスクシーケンスを広く展開する前に必要なBIOS設定ファイルをテストしてください。
- BIOSパスワードで使用される特定の文字は、正しく動作するために特別なエスケープが必要な場合があり ます。詳細については、HP BIOS Configuration Utility User Guideを参照してください。

- 1. 対象のコンピュータからBIOS設定ファイルを抽出します。BIOS設定ファイルの設定を変更したい箇所を 編集して残りの部分は削除します。
- BCUのパッケージソースフォルダを確認します。Configuration Managerで[ソフトウェアライブラリ]→[概 要]→[パッケージ]→[HP Client Support Tools]を右クリックして[プロパティ]を選択します。データソース タブのソースフォルダーを確認します。
- 3. BIOS設定(REPSET)ファイルをBCUソースフォルダにコピーします。
- 4. 配布ポイントを更新して新しいREPSETファイルがタスクシーケンスで利用できるようにします。

Configure RAID Exampleテンプレートの使用方法 タスクシーケンスで使用するブートイメージの準備

- 1. ブートイメージに必要なドライバーが含まれて いる事を確認します。
- この後のステップで追加するドライバーとの競合を避けるためにIntel Rapid Storage Technology (Intel RST) RAID ドライバーを削除します。
- 3. 対象のクライアントコンピュータをサポートす るバージョンのInrel Rapid Storage Technology RAID ドライバーをブートイメージに追加します。

注記

Windows 7 および Windows 8.1 でのみ利用可能です。

	ドライバーの選択					×
フォルダー(<u>F</u>):	КЭЛЛ−(<u>B</u>):					
in−۲ 🛄	 □ 記憶域クラスおよびネットワーク クラス以外のドライバーを非表 ✓ デジタル署名されていないドライバーを非表示にする(D) 	示にする (ブートイ	メージの場合)(<u>V</u>)		
	フィルター					P
	ドライバー名	カテゴリヘ	バージョン	クラス	署名済み	~
	✓ Intel(R) 8 Series/C220 Chipset Family SATA AHCI	"BPC Networ	13.2.0.1016	HDC	はい	
	Intel(R) 82580 Gigabit Network Connection	"BPC Networ	12.13.27.0	Net	はい	
	Intel(R) 82580 Gigabit Network Connection	"BPC Networ	12.11.97.0	Net	はい	
	✓ Intel(R) Desktop/Workstation/Server Express Chips	"BPC Networ	13.2.0.1016	SCSIAdapter	はい	
	Intel(R) Ethernet Connection I217-LM	"BPC Networ	12.15.23.1	Net	はい	
	Intel(R) Ethernet Connection I217-LM	"BPC Networ	12.12.80.1920	Net	はい	
		"BPC Networ	3.0.3.60	System	はい	
		"DBC Networ	4.0.0.35	System	(40)	
	A JT MRV USB 3.0 extensible #7 kr J/FU-7-	"PPC Networ	0.0.0.32	USB	(#()	~
			-1			
			すべ()進択(5)	a	へ(クリハ <u>A</u>)	
	名前: Intel(R) C600 series chipset SATA AHCI Controller					
	プロバイダー: Intel Corporation					
	デジカリ 男々主 Minnerst Windows Undows Compatibility	. Dublisher				
	DE T (II : AUOT (y i ublisher				
	INF 77170: IAAHOLINT					
	アーキテクチャ: ×64					
	サポートされているブラットフォーム: すべての) Windows 10 (64 ヒ bit), すべての Windows Server 2012 R2 (64 ビット), すべての 1 (64 ビット)	ジト)、すべての Win Windows Server 2	dows 8 (64 분ッ) 016 (64 분ット), 3	-), すべての Wind すべての Windows	ows 8.1 (64- Server 2012	_
				0K(<u>0</u>)	キャンセル	

タスクシーケンスで使用するパッケージの準備

- 対象のクライアントコンピュータのドライバーパックがインポートされている事を確認します。
- https://downloadcenter.intel.com にアクセスして、 [RST Cli]を検索します。ドライバーのバージョンに 対応したツールのバージョンを選択してダウンロー ドします。

注記:

ドライバーとツールのメジャーバージョンとマイナー バージョンを合わせる必要があります。バージョン 12.8.Xのツールはドライバーバージョン12.8.Xで動作し ます。

- 3. ダウンロードしたファイルを解凍します。解凍した フォルダの中にあるX64とx86のZIPファイルをさら に解凍します。
- 4. 解凍したファイルとフォルダをソフトウェアパッ ケージのソースフォルダーにコピーします。
- 5. ソースフォルダーを参照するソフトウェアパッケー ジを作成します。

3	バッケージとプログラムの作成ウィザード
 ♪ パッケージ パッケージ パッケージ プログラムの種類 標準プログラム 要件 報要 進行状況 完了 	バッケージとプログラムの作成ウィザード X このパッケージに関する情報の指定 新しいパッケージの名前と他の詳細を入力します。アプリケーション カタログなどの新機能を利用するには、代わりにアプリケーションを使用してくたさい。 名前(M): RST132.0.1016_CLI_Tools 説明(D): 製造元(E): Intel
進行状況 完了	名前(位): RST13.2.0.1016_CLL_Tools 説明(D): 製造元(E): Intel 言語(L): パージョン(ソ): マ このパッケージにソース ファイルを含める(T) ソース フォルダー(C): ¥¥192.168.1.251¥sms_h01¥OSD¥Lib¥Packages¥Deployment¥HP¥Client¥HWConfig: 参照(O)
	< 前へ(P) 次へ(N) > 概要(S) キャンセル

日本国内での動作確認が取れていないため本機能は現時点ではサポート対象外となります

タスクシーケンスステップの設定

- 1. タスクシーケンスを右クリックして[編集]を選択 します。
- [Call Intel RSTCli Command Line Utility Delete All Metadata]のステップを選択します。このステッ プではIntel RSTコマンドラインツールを使用して 既存のディスクのメタデータを削除します。

- パッケージの[参照]ボタンをクリックして、前の 手順で作成したIntel RSTコマンドラインツールの パッケージを選択します。
- 4. コマンドラインを実際の環境に合わせて書き換 えます。コマンドラインツールのドキュメント を参照してください。

コマンドラインの例

x86¥rstcli.exe -manage -delete-all-metadata

このコマンドライン例の、x86¥rstcli.exeはパッ ケージのソースフォルダーからの相対パスです。 X64のブートイメージを使用する場合、この例で はx64¥rstcli64.exeになります。





日本国内での動作確認が取れていないため本機能は現時点ではサポート対象外となります

- [Call Intel RSTCli Command Line Utility Configure RAID Volume]のステップを選択します。このス テップではIntel RSTコマンドラインツールを使用 してRAIDボリュームを作成します。
- パッケージの[参照]ボタンをクリックして、前の 手順で作成したIntel RSTコマンドラインツールの パッケージを選択します。
- コマンドラインを実際の環境に合わせて書き換えます。コマンドラインツールのドキュメントを参照してください。
 コマンドラインの例

x86¥rstcli.exe –create –level 1 –n Volume 0-0-0-0 0-1-0-0

このコマンドライン例の、x86¥rstcli.exeはパッ ケージのソースフォルダーからの相対パスです。 X64のブートイメージを使用する場合、この例で はx64¥rstcli64.exeになります。

日本国内での動作確認が取れていないため本機能は現時点ではサポート対象外となります



- 7. デプロイメントの対象OSに応じて以下のステップを設定します。
 - Remove Disk Partitions(diskpart clean) ーこのステップの設定は不要です。タスクシーケンスが適切に実行 されるにはネットワーク上のコンテンツディレクトリにアクセスできるように設定されている必要が あります。詳細は「Allowing access to deproyment content」を参照してください。このステップが不要 な場合はステップを無効にしてください。
 - Format and Partition Diskーディスクを必要に応じてフォーマットおよびパーティション化するための適切な手順を有効にします。たとえば、UEFIまたはUEFI Hybrid (CSMを使用)に設定されているシステムに展開する場合は、EFIフォーマットステップを有効にして、BIOSフォーマットステップを無効にします。
 - Apply Driver Packages ーデプロイメント対象のOSイメージに追加するHPドライバーパックを選択します。
 - Apply Network Settingsーデプロイメント対象をワークグループにするかドメインに参加するかを選択し、
 必要に応じてActive Deirectoryドメインのアカウント情報を入力します。

追加のタスクシーケンスステップを参照し、必要に応じて追加およびパラメータを設定します。

8. すべてのタスクシーケンスステップの設定が完了したら[OK]または[適用]をクリックして変更を保存します。

ブートイメージの割り当て

- 1. 対象のタスクシーケンスを右クリックして[プロ パティ]を選択します。
- 2. [詳細設定]タブを選択し、[ブートイメージを使 用する]をクリックして有効にします。
- 3. [参照]をクリックしてHP Client Boot Imagesフォル ダーからIntel RST RAIDドライバーを追加したブー トイメージを選択します。
- 4. [OK]をクリックします。

注記

ブートイメージはデプロイメント対象のOSと同じ アーキテクチャのものを選択します。X86/32-bit OS の場合はx86イメージを、x64/64-bit OSの場合はx64 イメージを選択します。

🗎 HP Client RAID Task Sequence のプロパティ
全般 詳細設定 セキュリティ
□ 別のプログラムを最初に実行する(E):
パッケージ(P): 参照(R)
プログラム(<u>M</u>):
□ このプログラムを必ず最初に実行する(S)
□ タスク シーケンスの通知を表示しない(E)
□ 展開先のコンピューターでこのタスク シーケンスを無効にする(D)
許容最長実行時間(分)(T): 0 V
▲ 実行時間を無制限にするには 0 を選択します。実行時間が 0 のタスク シーケンスはメンテ +>>2 期間を超える可能性があります。
● 任意のプラットフォームで実行する(山)
○ 指定したクライアント ブラットフォームだけで実行する(○)
g すべての埋め込み Windows XP
すべての Windows 10 (32 ビット) すべての Windows 10 (64 ビット)
□ すべての埋め込み Windows 7 (64 ビット) ✓
OK キャット/フリ. 適田(A)

デプロイメントコンテンツへのアクセス許可設定

HP MIKタスクシーケンスのRemove Disk Partitions(diskpart clean)ステップはネットワークから直接実行する必要があります。そのためには、ブートイメージを含むタスクシーケンスのすべてのパッケージとコンテンツが以下のように設定されている必要があります。

1. コンテンツ/パッケージを右クリックして[プロパティ]を選択します。

- 2. [データアクセス]タブを選択し、[このパッケージのコンテンツを配布ポイントのパッケージ共有にコ ピーする]をクリックして有効にします。
- 3. [OK]をクリックします。

タスクシーケンスの実行のフロー

タスクシーケンスは次の3つのタスクグループに分類されます。

- [Configure Hardware] (ハードウェアの設定)
- [Configure RAID] (RAIDの設定)
- [Install Operating System] (OSのインストール)

3つのグループの条件とコンピュータ変数を使用して、PXE/USB経由で複数回再起動したときのタスクシー ケンスの処理を制御します。Set RebootStep Variableタスクは、実行されるたびにRebootStep変数を1ずつ増 やします。変数が存在しない場合は、変数が作成され、0に設定されます。

タスクシーケンスの最初の実行中に、[Configure Hardware]グループのタスクが実行されます。再起動後タス クシーケンスを再実行すると、RebootStep変数の設定タスクはRebootStepの値を2に増やします。[Configure Hardware]グループには、RebootStep変数の値が1の場合にのみ実行されるという条件がありますのでこのグ ループは再起動後にスキップされます。

次のグループであるConfigure RAID Volumeは、RebootStepの値が2であることを確認してから実行されます。

最後のグループであるInstall Operating Systemは、RebootStepの値が3であることを確認します。この条件が 満たされると、3番目のステップ群が実行されます。

タスクシーケンスの終了時に、Reset RebootStep VariableタスクはRebootStepを0にリセットします。

_{ります}

日本国内での動作確認が取れていないため本機能は現時点ではサポート対象外となります

タスクシーケンスの展開に関する次の点に注意してください

- PXE / USBで再起動してタスクシーケンスを展開するときは、配布ポイント画面で、実行中のタスクシーケンスによって必要になったときに配布ポイントから配布コンテンツから直接コンテンツにアクセスするように展開オプションを設定します。このオプションをタスクシーケンスで参照される各パッケージで使用できるようにするには、[プロパティ]ダイアログボックスの[データアクセス]タブを選択し、[このパッケージの内容を配布ポイントのパッケージ共有にコピーする]を選択します。
- タスクシーケンスが[利用可能]としてデプロイされ、[必須]としてデプロイされていない場合は、再起動時にタスクシーケンスを選択して展開を続行する必要があります。
- このステップが正常に動作するには、ターゲット・クライアント・システムにリブート用の適切なブート 順序が設定されている必要があります。(つまり、PXE経由でブートする場合、PXE NICはブート順序内の 他のブートデバイスの前にある必要があります)。ターゲットクライアントシステムで必要なタスクシー ケンスを再実行するには、PXE アドバタイズメントを消去します
 - A) Configuration Managerで資産とコンプライアンスを選択します。
 - B) デバイスを選択します。
 - ターゲットクライアントシステムを選択します。
 - D) リボンから[要求されたPXE展開を削除する]を選択します。



- タスクシーケンスの実行に失敗してしまう場合は以下のようにRebootStep変数の値をクリアまたはリセットが必要になる場合があります。
 - A) ターゲットクライアントシステムを右クリックして[プロパティ]を選択します。
 - B) [変数]タブを選択します。
 - C) RebootStep変数を選択し、削除ボタンを選択します。

本書の取り扱いについて

- 本書は、株式会社日本HPが販売する製品を検討されているお客様が実際のご利用方法に合わせた設定を行う際に役立つ手順の一例を示すものです。いかなる場合においても本書の通りになる事を保証するものではありません。
- 本書の内容は、将来予告なしに変更されることがあります。HP製品およびサービスに対する保証については、該当製品およびサービス保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、省略に対して責任を負いかねますのでご了承ください。
- この文書の著作権は株式会社日本HPに帰属します。株式会社日本HPの許可なく一部または全体の複製・転載・編集 等を行うことや、許可されていない第三者への開示等の行為全てを禁止します。

本文中使用される企業名、製品名、商標などはそれを保持する企業・団体に帰属します。

keep reinventing