HITACHI

JP1 Cloud Service エンドポイント管理 利用ガイド

JCSM31-0260-01

前書き

■ 対象サービス

＜ V02-60 以降＞

●エンドポイント管理 - スタンダード

SD-527318233 JP1 Cloud Service/Endpoint Management - Standard 02-60 以降

●エンドポイント管理 - ライト A

SD-527318243 JP1 Cloud Service/Endpoint Management - Light A 02-60 以降

●エンドポイント管理 - ライト B

SD-527318253 JP1 Cloud Service/Endpoint Management - Light B 02-60 以降

●エンドポイント管理 - 管理用中継サーバ追加オプション

SD-527318263 JP1 Cloud Service/Endpoint Management - Additional Management Relay Server Option 02-60 以降

●エンドポイント管理 - 操作ログ拡張オプション

SD-527318273 JP1 Cloud Service/Endpoint Management - Extended Operation Log Option 02-60 以降

●エンドポイント管理 - 暗号化オプション

SD-527318283 JP1 Cloud Service/Endpoint Management - Data Encryption Option 02-60 以降

■ 輸出時の注意

本製品を輸出される場合には、外国為替および外国貿易法の規制ならびに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。

なお、不明な場合は、弊社担当営業にお問い合わせください。

■ 商標類

記載の会社名，製品名などは，それぞれの会社の商標もしくは登録商標です。

■ マイクロソフト製品のスクリーンショットの使用について

マイクロソフトの許可を得て使用しています。

■ 発行

2026 年 9 月　JCSM31-0260-01

■ 著作権

Copyright (C) 2024, 2026, Hitachi, Ltd.
Copyright (C) 2024, 2026, Hitachi Solutions, Ltd.

変更内容

変更内容　JP1 Cloud Service エンドポイント管理 V02-60

追加・変更内容	変更個所
秘文サービス管理ページで，シングルサインオン（SSO）機能を利用できるようになりました。	1.4.1，4.3.1，4.3.2，4.3.3，4.3.5(3)
エンドポイント管理で使用するポート番号に関する記載を追加しました。	1.4.2
JP1/ITDM2 が出力する保存用の変更履歴をポータルシステムからダウンロードできるようにしました。これに伴い，「操作ログ一覧」を「ログ一覧」に変更しました。	3.2，表 4-1，4.3.6，4.3.8，表 B-1
ポータルシステムの機能一覧に，「認証設定」を追加しました。	表 4-1，4.3.7
エンドポイント管理のポータルシステムで，API が利用できるようになりました。	5

単なる誤字・脱字などはお断りなく訂正しました。

はじめに

このマニュアルは JP1 Cloud Service で提供する，エンドポイント管理の利用方法について説明したものです。

■ 対象読者

このマニュアルは次の方にお読みいただくことを前提に説明しています。

- JP1 Cloud Service / エンドポイント管理の導入を検討されている方
- JP1 Cloud Service / エンドポイント管理の概要や基本的な使い方を理解しようとされている方
- JP1 Cloud Service / エンドポイント管理を利用されているお客さまで，IT 資産の管理とセキュリティ対策の設計や運用をする方

■ マニュアルの構成

このマニュアルは，次に示す章と付録から構成されています。

第 1 章　エンドポイント管理の概要
エンドポイント管理の機能概要と特長，利用するための準備について説明しています。

第 2 章　エンドポイント管理を利用するための構築
エンドポイント管理を利用するための環境の構築について説明しています。

第 3 章　エンドポイント管理の利用方法
エンドポイント管理の基本的な操作方法について説明しています。

第 4 章　エンドポイント管理のポータルシステムの利用方法
エンドポイント管理のポータルシステムの基本的な操作方法について説明しています。

第 5 章　API リファレンス
エンドポイント管理のポータルシステムが提供する API について説明しています。

付録 A　このマニュアルの参考情報
このマニュアルを読むに当たっての参考情報について説明しています。

付録 B　機能の提供有無一覧
JP1/ITDM2 および秘文の提供機能とエンドポイント管理の提供機能差異について説明します。

付録 C　用語解説
このマニュアルでの用語について説明しています。

付録 D　各バージョンの変更内容

各バージョンの変更内容について説明しています。

■ マニュアルの読み方

このマニュアルでは，エンドポイント管理を利用するための準備，およびエンドポイント管理での基本的なシステムの管理，運用，操作の方法について説明しています。応用的な機能や操作を知りたい場合は，次の表を参考に，JP1/IT Desktop Management 2 または秘文のマニュアルをお読みください。

項番	利用目的	対象マニュアル
1	エンドポイント管理を利用したエンドポイント管理の設計方法の詳細を知りたい。	• JP1 Version 13 JP1/IT Desktop Management 2 導入・設計ガイド
2	エンドポイント管理を利用するための構築の詳細を知りたい。	• JP1 Version 13 JP1/IT Desktop Management 2 構築ガイド • 秘文 Endpoint Protection Service 基本ガイド（管理者用）
3	エンドポイント管理を利用した業務の運用例，操作方法の詳細を知りたい。	• JP1 Version 13 JP1/IT Desktop Management 2 運用ガイド • 秘文 管理者ガイド（運用編）
4	リモートインストールマネージャを使用した配布機能の機能詳細，運用方法，および操作方法について知りたい。	• JP1 Version 13 JP1/IT Desktop Management 2 配布機能 運用ガイド
5	エンドポイント管理で表示されるメッセージの原因や対処方法について知りたい。	• JP1 Version 13 JP1/IT Desktop Management 2 メッセージ • 秘文 メッセージガイド（管理者用） • 秘文 メッセージガイド（ユーザ用）
6	エンドポイント管理の持ち出し制御やデバイス制御などの詳細を知りたい。	• 秘文 管理者ガイド（機能解説編）
7	データの暗号化機能について詳細を知りたい。	• 秘文 管理者ガイド（機能解説編）
8	ファイルサーバ上の共有フォルダの暗号化について詳細を知りたい。	• 秘文 管理者ガイド（機能解説編）
9	エンドポイント管理の秘文クライアントのインストール媒体作成手順について知りたい。	• 秘文 セットアップガイド（管理者用）

目次

前書き　2
変更内容　4
はじめに　5

1　エンドポイント管理の概要　10
1.1　エンドポイント管理の特長　11
1.2　システム構成　12
1.3　エンドポイント管理の機能　15
1.3.1　提供機能　15
1.3.2　機能ごとの対応プラットフォーム　18
1.4　エンドポイント管理利用の準備　20
1.4.1　エンドポイント管理への接続　20
1.4.2　使用するポート番号　21

2　エンドポイント管理を利用するための構築　25
2.1　構築の流れ　26
2.1.1　運用管理コンピュータの構築の流れ　26
2.1.2　利用者コンピュータの構築の流れ　27
2.1.3　ファイルサーバの構築の流れ　27
2.2　運用管理コンピュータの構築　29
2.2.1　リモートインストールマネージャのインストール　29
2.2.2　パッケージャのインストール　29
2.2.3　秘文管理ツールのインストール　30
2.3　利用者コンピュータの構築　31
2.3.1　インストールセットの作成　32
2.3.2　秘文インストール媒体の作成　32
2.3.3　エージェントのインストール　32
2.3.4　秘文クライアントのインストール　32
2.4　ファイルサーバの構築　34
2.4.1　エージェントのインストール　34
2.4.2　ファイルサーバのインストール　34
2.4.3　ファイルサーバの設定　35

3　エンドポイント管理の利用方法　36
3.1　システムの概況把握　37

3.2 機器の管理 38
3.3 機器のリモートコントロール 39
3.4 資産の管理 40
3.5 配布機能 41
3.6 機器のネットワーク接続の管理 42
3.7 セキュリティの管理 43
3.8 操作ログの管理 44
3.9 ポリシーの反映 45
3.10 暗号化機能 46
3.11 ファイル保護機能 47

4 エンドポイント管理のポータルシステムの利用方法 48
4.1 ポータルシステムの概要 49
4.2 利用できる Web ブラウザ 50
4.3 ポータルシステムの利用方法 51
4.3.1 シングルサインオン（SSO）の利用方法 51
4.3.2 ユーザーアカウント管理 52
4.3.3 ログインとログアウト 55
4.3.4 ログインユーザーのパスワード変更 60
4.3.5 サーバー一覧の表示 61
4.3.6 タスク一覧の表示 68
4.3.7 認証設定の表示 72
4.3.8 ログの表示 74
4.3.9 製品媒体一覧の表示 76
4.3.10 マニュアル一覧の表示 78
4.3.11 提供ファイル一覧の表示 79
4.3.12 サポート情報一覧の表示 80
4.3.13 お知らせの表示 81
4.3.14 ライセンス情報の表示 82

5 API リファレンス 84
5.1 API 一覧 85
5.2 API 共通仕様 86
5.2.1 認証方式 86
5.2.2 API 利用時の注意事項 86
5.2.3 リクエスト形式 87
5.2.4 レスポンス形式 88
5.2.5 ステータスコード 89
5.2.6 エラー情報 90

5.3 API の詳細 92
5.3.1 パッケージのインストール API 92
5.3.2 クライアントユーザによるインストール API 95
5.3.3 ジョブの実行 API 96
5.3.4 ジョブの削除 API 97
5.3.5 ジョブ定義の削除 API 99
5.3.6 タスク実行状態の取得 API（サーバ名指定） 100
5.3.7 タスク実行状態の取得 API（タスク ID 指定） 103

付録 106

付録 A このマニュアルの参考情報 107
付録 A.1 製品名の表記 107
付録 A.2 Windows 版と UNIX 版との差異 109
付録 A.3 英略語 109
付録 B 機能の提供有無一覧 111
付録 B.1 JP1/ITDM2 との差異 111
付録 B.2 秘文との差異 118
付録 C 用語解説 121
付録 D 各バージョンの変更内容 123
付録 D.1 02-60 の変更内容 123
付録 D.2 02-50 の変更内容 123
付録 D.3 02-40 の変更内容 123
付録 D.4 02-30 の変更内容 124
付録 D.5 02-20 の変更内容 124

索引 125

1 エンドポイント管理の概要

エンドポイント管理の機能概要と特長，利用するための準備について説明します。

1.1　エンドポイント管理の特長

エンドポイント管理は，多様化，複雑化するエンドポイントでの IT 資産やセキュリティの一元管理を SaaS 型サービスで提供することで，初期コストを抑えて効率よく運用できます。また，資産管理の現状の問題点を解決できるため，企業全体のコンプライアンス向上を実現します。

エンドポイント管理の特長を次に示します。

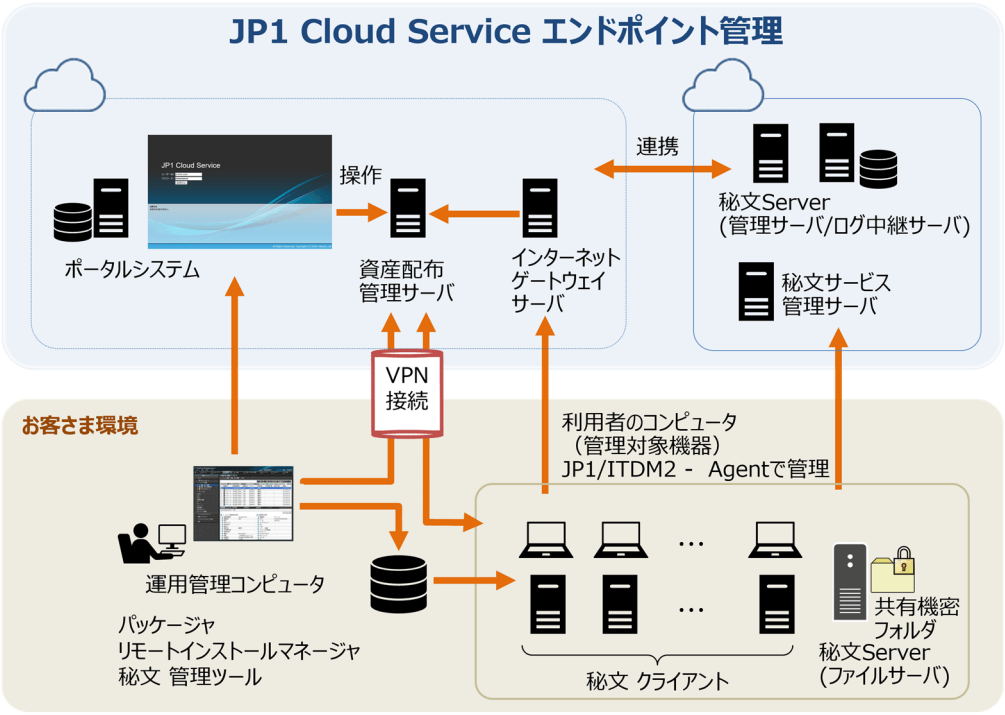
- IT 機器の現状の把握
- IT 機器に対するセキュリティのルールの徹底
- セキュリティに問題があるコンピュータの把握と対策
- IT 機器のネットワーク接続の監視
- ソフトウェアの導入と保守
- 操作ログおよび変更履歴の取得
- デバイスの使用制限
- 許可ネットワーク制御
- 持ち出し制御
- 暗号化機能
- ファイル保護機能

エンドポイント管理を利用すると，これらの特長によって，複雑な管理作業を簡素化できます。

1.2　システム構成

エンドポイント管理のシステム構成例を次に示します。

図 1–1　エンドポイント管理のシステム構成例

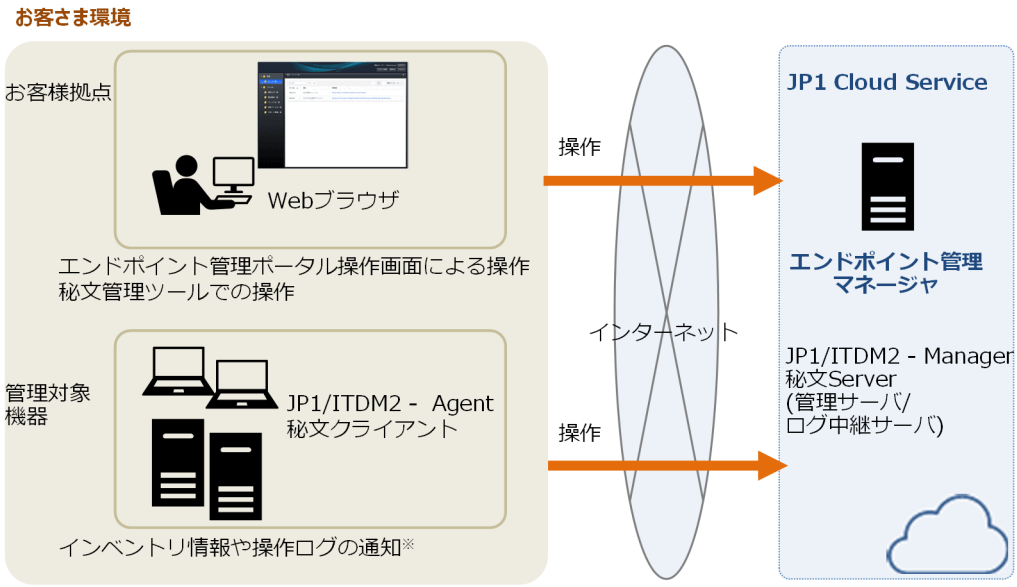


サービスプランごとにお客さまの環境と接続するために必要な環境が異なります。サービスプランによるシステム構成例を次に示します。

- インターネット接続だけで利用する場合

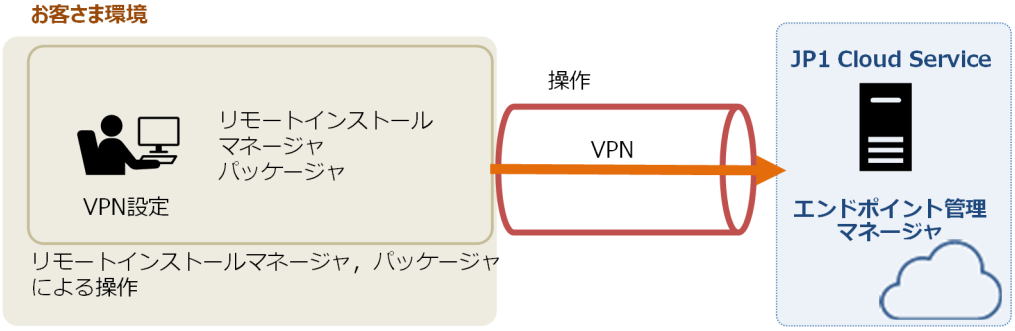
  サービスプランのスタンダード，ライト A，およびライト B が該当します。

  エンドポイント管理ポータルシステムへの接続，利用者のコンピュータから資産配布管理サーバへの接続，および秘文 Server への接続は，インターネットを使用して接続します。

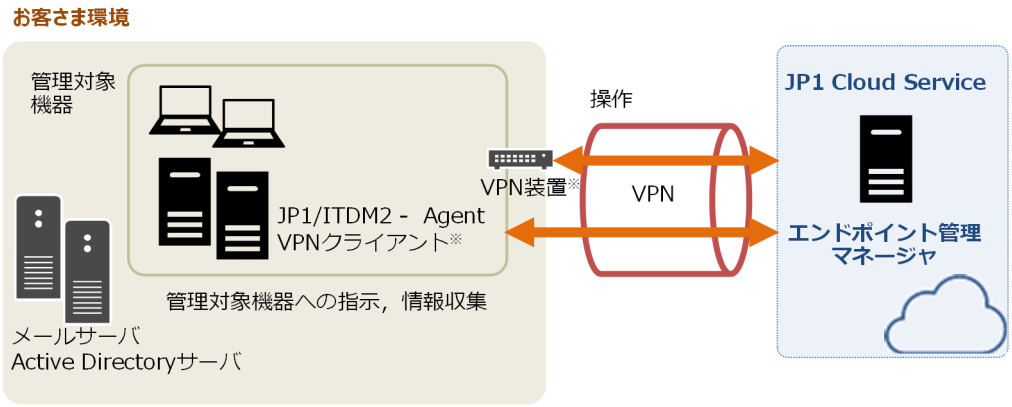


注※　httpsポートのアウトバウンド通信の許可が必要です。

- リモートインストールマネージャによる配布をする場合
  サービスプランのスタンダード，ライト A が該当します。
  お客さまの環境と，資産配布管理サーバを VPN で接続します。VPN 設定が必要です。



- その他 VPN が必要となる機能を使用する場合
  次の場合，VPN 接続が必要です。
  - 管理対象機器の電源制御
  - UNIX/Linux/Mac OS 機器の管理
  - ネットワークの探索
  - 中継システムの設置
  - Active Directory との連携（お客さま環境の Active Directory サーバ）
  - メール通知機能（お客さま環境のメールサーバ）



注※　VPN装置または各管理対象機器にVPNクライアントのインストールが必要です。

この利用ガイドでは，ご使用になるプランに必要な上記接続が完了しているという前提で後続の作業を説明します。

1.3　エンドポイント管理の機能

1.3.1　提供機能

エンドポイント管理が提供する機能をサービスプランごとに示します。

表 1–1　サービスプランごとの提供機能一覧

項番	サービスプラン	提供機能			
		資産管理	配布管理	セキュリティ管理	
		JP1/ITDM2	JP1/ITDM2	JP1/ITDM2	秘文
1	スタンダード	○	○	○	○
2	ライト A	○	○	○	×
3	ライト B	○	×	○	○

（凡例）○：使用できる　×：使用できない

エンドポイント管理が提供する機能の概要は次のとおりです。

表 1–2　エンドポイント管理の機能一覧

項番	提供機能	機能	機能概要	サービスプラン		
				スタンダード	ライト A	ライト B
1	資産管理	システムの概況把握	大量の管理情報に対して管理者が状況を把握するためのホーム画面とダッシュボードから，さまざまな観点で，運用状況を把握できます。 機能の利用方法については，「3.1　システムの概況把握」を参照してください。	○	○	○
2		機器の管理	管理対象にした組織内の機器の情報を収集して確認したり，電源状態を把握して制御したりできます。 機能の利用方法については，「3.2　機器の管理」を参照してください。	○	○	○
3		機器のリモートコントロール	コントローラから利用者のコンピュータの画面を呼び出して遠隔操作できます。 機能の利用方法については，「3.3　機器のリモートコントロール」を参照してください。	○	○	○
4		資産の管理	組織が所有するハードウェア資産やソフトウェアライセンスを登録して，運用状況を管理できます。	○	○	○

項番	提供機能	機能	機能概要	サービスプラン		
				スタンダード	ライト A	ライト B
4	資産管理	資産の管理	機能の利用方法については，「3.4　資産の管理」を参照してください。	○	○	○
5	配布管理	配布機能	リモートインストールマネージャを使用してソフトウェアやデータなどを管理対象のコンピュータへ配布できます。 機能の利用方法については，「3.5　配布機能」を参照してください。 また，JP1/ITDM2 の配布機能の一部のコマンドは，API を使用して実行できます。 詳細は，「5　API リファレンス」を参照してください。	○	○	×
6	セキュリティ管理	機器のネットワーク接続の管理	ネットワークを監視して，未許可の機器のネットワーク接続を防いだり，危険なコンピュータを自動的にネットワークから切断したりできます。 機能の利用方法については，「3.6　機器のネットワーク接続の管理」を参照してください。	○	×	○
7		セキュリティの管理	セキュリティポリシーを作成し，コンピュータに適用することで，セキュリティ状況を判定します。また，セキュリティ上問題があるコンピュータを自動対策することもできます。 機能の利用方法については，「3.7　セキュリティの管理」を参照してください。	○	×	○
8		操作ログの管理	利用者がコンピュータ上で操作した履歴を，操作ログとして収集する機能です。収集した操作ログは，操作画面から一覧で確認できます。 機能の利用方法については，「3.8　操作ログの管理」を参照してください。	○	×	○
9		ポリシー（持ち出し/読み込み制御，デバイス制御，および許可ネットワーク制御）の反映	PC からのデータの持ち出し，PC へのデータの読み込み，デバイスの使用，および PC のネットワークへの接続を制御する機能です。この機能によって，不正な持ち出しと読み込みの防止ができます。 機能の利用方法については，「3.9　ポリシーの反映」を参照してください。	○	×	○
10		暗号化機能	管理対象機器のローカルドライブ，ファイルを暗号化します。PC やメディアの紛失・盗難時の情報漏洩の防止ができます。 機能の利用方法については，「3.10　暗号化機能」を参照してください。	○	×	○

項番	提供機能	機能	機能概要	サービスプラン		
				スタンダード	ライト A	ライト B
11	セキュリティ管理	ファイル保護機能	機密データ（保護対象ファイル）に対して，マルウェアなどの不正なプログラムによる情報窃取や破壊を防止する機能です。 機能の利用方法については，「3.11　ファイル保護機能」を参照してください。	○	×	○

このバージョンでは，JP1/ITDM2，秘文ともに従来の機能をそのまま使用するため，次の注意事項があります。

注意事項

- JP1/ITDM2 と秘文で同じ情報漏えい対策機能を使用すると，同一の操作ログが重複して操作ログ一覧画面に表示されることがあります。
- JP1/ITDM2 の次の操作ログを使用する場合は，秘文のファイル・ドライブ操作ログは使用しないでください。
  ・ファイル操作/印刷操作
  ・フォルダ操作不審操作の取得
  ・添付ファイル付きメールの送受信
  ・Web/FTP サーバの使用
  ・外部メディア（リムーバブルディスク）へのファイルコピーと移動
- JP1/ITDM2 の操作ログのポリシーである［情報漏えいに係わりの深い操作を取得対象にする（推奨)］を使用する場合は，秘文のファイル・ドライブ操作ログは使用しないでください。
- 秘文で印刷抑止を実施している場合は，JP1/ITDM2 の印刷ログは取得できません。
- 秘文で印刷抑止を実施している場合は，JP1/ITDM2 による印刷抑止はできません。

また，お客さま拠点からエンドポイント管理へのインターネット回線の通信速度や通信状況によって，次の注意事項があります。

注意事項

- 機器の管理で，資産管理サーバへの機器の登録や最新の機器情報の更新に時間がかかることがあります。
- 配布機能で，利用者のコンピュータへの配布に時間がかかることがあります。特に配布するパッケージのサイズが大きい場合，数時間かかることがあります。
- セキュリティの管理で，利用者のコンピュータへのセキュリティポリシーの適用に時間がかかることがあります。
- 操作ログの管理で，利用者のコンピュータから資産管理サーバや秘文 Server への操作ログの取得に時間がかかることがあります。

- その他の注意事項は，JP1 のマニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」での，インターネット接続管理機器の注意事項を参照してください。

電源制御について次の制限事項があります。

制限事項

- Wake on LAN によるリモートからの電源オンには対応していません。
- リモートからのシャットダウン（電源オフ）は Windows マシンに限り対応しており，UNIX マシンには対応していません。
- Intel Active Management Technology（AMT）には対応していません。

1.3.2　機能ごとの対応プラットフォーム

エンドポイント管理が提供する機能で対応しているプラットフォームを示します。

表 1–3　機能ごとの対応プラットフォーム一覧

OS		資産管理	配布管理	セキュリティ管理		暗号化オプション※1
				JP1/ITDM2	秘文	
Windows	Windows 7	○	○	○	×	×
	Windows 8	○	○	○	×	×
	Windows 8.1	○	○	○	×	×
	Windows 10	○	○	○	○	○
	Windows 11	○	○	○	○	○
	Windows Server 2012	○	○	○	×	×
	Windows Server 2012 R2	○	○	○	×	×
	Windows Server 2016	○	○	○	×	×
	Windows Server 2019	○	○	○	×	×
	Windows Server 2022	○	○	○	×	×
	Windows Server 2025	○	○	○	×	×
AIX		○※2	○※2	×	×	×
HP-UX		○※2	○※2	×	×	×
Linux	Red Hat Enterprise Linux Server	○※2	○※2	×	×	×
	Oracle Linux	○※2	○※2	×	×	×
Solaris		○※2	○※2	×	×	×

OS		資産管理	配布管理	セキュリティ管理		暗号化オプション※1
				JP1/ITDM2	秘文	
Mac		○※2	○※2	×	×	×
Chrome OS	ChromeOS	○※3	×	×	×	×
	ChromeOS Flex	○※3	×	×	×	×
スマートフォン OS	iOS	○※4	×	×	×	×
	iPadOS	○※4	×	×	×	×
	Android	○※4	×	×	×	×

（凡例）○：使用できる　×：使用できない

注※1

エンドポイント管理 - 暗号化オプションサービスを指します。

注※2

VPN 接続が必要です。

注※3

Google Workspace が必要です。

注※4

Microsoft Intune が必要です。

1.4　エンドポイント管理利用の準備

エンドポイント管理の利用を開始するために，必要な準備について説明します。

1.4.1　エンドポイント管理への接続

エンドポイント管理を利用するには，事前に次の設定が必要です。

お客さま環境のファイアウォールやプロキシサーバで，必要な接続先およびポートへの通信を許可し，お客さま拠点からエンドポイント管理へ通信できるようにしてください。

- エンドポイント管理ポータルシステム接続情報
  宛先：https://portal.epm.hitachi-solutions.co.jp/login
  ポート番号：443
  宛先：https://keycloak.epm.hitachi-solutions.co.jp
  ポート番号：444
- JP1/ITDM2（統括マネージャまたは中継マネージャ）の管理画面への接続情報
  ポータルシステムのサーバ一覧画面で確認します。詳細は，「4.3.5　サーバ一覧の表示」を参照してください。
- 秘文サービス管理ページ
  秘文サービス管理ページの SSO は，エンドポイント管理 V02-50 以前では利用できません。
  - SSO 利用時
    宛先：https://hibun-sv.hitachi-solutions.co.jp/console/*カスタマーコード*※
    ポート番号：443
    注※
    　ご利用環境情報でお知らせするカスタマーコードを指定します。
  - SSO 非利用時
    宛先：https://hibun-sv.hitachi-solutions.co.jp/console/
    ポート番号：443
- エージェント接続情報（インターネット接続）と JP1/ITDM2 の REST API 接続時の接続情報
  「JP1 Cloud Service のご利用環境の情報（エンドポイント管理）」を参照してください。
- 秘文 Server への接続
  秘文クライアント，ファイルサーバ，クライアント通知サーバ，秘文管理ツールを使用する PC から秘文 Server へ接続できるように設定してください。詳細は，秘文サービスのマニュアル「秘文 Endpoint Protection Service 基本ガイド（管理者用）」での，システム要件にあるネットワーク要件の記載を参照してください。

1.4.2　使用するポート番号

エンドポイント管理で使用するポート番号は，原則として JP1/ITDM2 のデフォルト設定に従います。

ただし，マネージャやインターネットゲートウェイへの接続に使用するポート番号のうち，デフォルトから変更されているものについては，ご利用環境情報で通知します。

ただし，機能の仕様により，ご利用環境情報で個別に通知されないポート番号についても，一部のポート番号がデフォルトから変更される場合があります。

JP1/ITDM2 のデフォルト設定から変更されるものについて説明します。

管理者のコンピュータ（リモートインストールマネージャ）

JP1/ITDM2		共通		エンドポイント管理		
ポート番号	接続対象［ポート番号］	方向	プロトコル	ポート番号	接続対象［ポート番号］	説明
ephemeral	管理用サーバ［31002］	→	TCP	ephemeral	管理用サーバ［ポート番号※］	JP1/ITDM2 の管理画面で［設定］－［エージェント］－［Windows エージェント設定とインストールセットの作成］－［基本設定］－［配布用ポート番号（中継システム）］の値が使用されます。
ephemeral	管理用サーバ［31021］	→	TCP	ephemeral	管理用サーバ［ポート番号※］	ご利用環境情報の「■エージェント接続情報　統括マネージャの配布用ポート番号」が使用されます。
ephemeral	管理用サーバ［31080］	→	TCP	ephemeral	管理用サーバ［ポート番号※］	ご利用環境情報の「■配布管理ツール（RIM，パッケージャ）使用時の接続情報　統括マネージャのポート番号」が使用されます。
ephemeral	中継システム［31021］	→	TCP	ephemeral	中継システム［ポート番号※］	ご利用環境情報の「■エージェント接続情報　統括マネージャの配布用ポート番号」が使用されます。

注※

お客さま環境ごとに異なります。

中継システム

JP1/ITDM2		共通		エンドポイント管理		
ポート番号	接続対象［ポート番号］	方向	プロトコル	ポート番号	接続対象［ポート番号］	説明
31014	管理用サーバ［ephemeral］	←	UDP	ポート番号※	管理用サーバ［ephemeral］	JP1/ITDM2 の管理画面で［設定］－［エージェント］－［Windows エージェント設定とインストール

JP1/ITDM2		共通		エンドポイント管理		
ポート番号	接続対象［ポート番号］	方向	プロトコル	ポート番号	接続対象［ポート番号］	説明
31014	管理用サーバ［ephemeral］	←	UDP	ポート番号※	管理用サーバ［ephemeral］	セットの作成］−［通信設定］−［マルチキャスト配布の設定］−［通常の受信時］の値が使用されます。
ephemeral	管理用サーバ［31015］	→	UDP	ephemeral	管理用サーバ［ポート番号※］	JP1/ITDM2 の管理画面で［設定］−［エージェント］−［Windows エージェント設定とインストールセットの作成］−［通信設定］−［マルチキャスト配布の設定］−［再送の場合の受信時］の値が使用されます。
ephemeral	管理用サーバ［31021］	→	TCP	ephemeral	管理用サーバ［ポート番号※］	ご利用環境情報の「■エージェント接続情報　統括マネージャの配布用ポート番号」が使用されます。

注※

お客さま環境ごとに異なります。

コントローラおよびリモコンエージェントのポート番号一覧

JP1/ITDM2		共通		エンドポイント管理		
ポート番号	接続対象［ポート番号］	方向	プロトコル	ポート番号	接続対象［ポート番号］	説明
リモコンエージェント［31016］	コントローラ［ephemeral］	←	TCP	リモコンエージェント［ポート番号※］	コントローラ［ephemeral］	JP1/ITDM2 の管理画面で［設定］−［エージェント］−［Windows エージェント設定とインストールセットの作成］−［リモートコントロールの設定］−［接続設定］−［コントローラとの接続時に使用するポート番号］の値が使用されます。
リモコンエージェント［31017］	コントローラ［ephemeral］	←	TCP	リモコンエージェント［ポート番号※］	コントローラ［ephemeral］	JP1/ITDM2 の管理画面で［設定］−［エージェント］−［Windows エージェント設定とインストールセットの作成］−［リモートコントロールの設定］−［接続設定］−［コントローラとの接続時に使用するポート番号］に設定されている値に 1 を加算したポート番号が使用されます。
リモコンエージェントまたはコントロー	リモコンエージェントまたは	← →	TCP	リモコンエージェントまたはコントロー	リモコンエージェントまたはコントロー	JP1/ITDM2 の管理画面で［設定］−［エージェント］−［Windows エージェント設定とインストール

JP1/ITDM2		共通		エンドポイント管理		
ポート番号	接続対象［ポート番号］	方向	プロトコル	ポート番号	接続対象［ポート番号］	説明
ラ［31018］（チャットサーバとして使用している場合）	コントローラ［ephemeral］	← →	TCP	ラ［ポート番号※］（チャットサーバとして使用している場合）	ラ［ephemeral］	セットの作成］−［リモートコントロールの設定］−［接続設定］−［コントローラとの接続時に使用するポート番号］に設定されている値に 2 を加算したポート番号が使用されます。
リモコンエージェント［ephemeral］	コントローラ［31019］	→	TCP	リモコンエージェント［ephemeral］	コントローラ［ポート番号※］	JP1/ITDM2 の管理画面で［設定］−［エージェント］−［Windows エージェント設定とインストールセットの作成］−［リモートコントロールの設定］−［接続設定］−［コントローラとの接続時に使用するポート番号］に設定されている値に 3 を加算したポート番号が使用されます。
リモコンエージェント［ephemeral］	コントローラ［31020］	→	TCP	リモコンエージェント［ephemeral］	コントローラ［ポート番号※］	JP1/ITDM2 の管理画面で［設定］−［エージェント］−［Windows エージェント設定とインストールセットの作成］−［リモートコントロールの設定］−［接続設定］−［コントローラとの接続時に使用するポート番号］に設定されている値に 4 を加算したポート番号が使用されます。

注※

お客さま環境ごとに異なります。

JP1/IT Desktop Management 2 - Agent のポート番号一覧

JP1/ITDM2		共通		エンドポイント管理		
ポート番号	接続対象［ポート番号］	方向	プロトコル	ポート番号	接続対象［ポート番号］	説明
31014	管理用サーバまたは中継システム［ephemeral］	←	UDP	ポート番号※	管理用サーバまたは中継システム［ephemeral］	JP1/ITDM2 の管理画面で［設定］−［エージェント］−［Windows エージェント設定とインストールセットの作成］−［通信設定］−［マルチキャスト配布の設定］−［通常の受信時］の値が使用されます。
ephemeral	中継システム［31002］	→	TCP	ephemeral	中継システム［ポート番号※］	JP1/ITDM2 の管理画面で［設定］−［エージェント］−［Windows エージェント設定とインストールセットの作成］−［基本設定］−

JP1/ITDM2		共通		エンドポイント管理		
ポート番号	接続対象［ポート番号］	方向	プロトコル	ポート番号	接続対象［ポート番号］	説明
ephemeral	中継システム［31002］	→	TCP	ephemeral	中継システム［ポート番号※］	［配布用ポート番号（中継システム）］の値が使用されます。
ephemeral	管理用サーバまたは中継システム［31015］	→	UDP	ephemeral	管理用サーバまたは中継システム［ポート番号※］	JP1/ITDM2 の管理画面で［設定］－［エージェント］－［Windows エージェント設定とインストールセットの作成］－［通信設定］－［マルチキャスト配布の設定］－［再送の場合の受信時］の値が使用されます。
ephemeral	管理用サーバ［31021］	→	TCP	ephemeral	管理用サーバ［ポート番号※］	ご利用環境情報の「■エージェント接続情報　統括マネージャの配布用ポート番号」が使用されます。
ephemeral	IGW［443］	→	TCP	ephemeral	IGW［ポート番号※］	ご利用環境情報の「■エージェント接続情報　インターネットゲートウェイサーバのポート番号」が使用されます。

注※

お客さま環境ごとに異なります。

2 エンドポイント管理を利用するための構築

エンドポイント管理を利用してセキュリティ管理や資産管理の観点から IT 機器の管理を始めるために，まずは利用するための環境の構築をしましょう。この章では，エンドポイント管理の利用に必要な環境を構築する方法を説明します。

2.1　構築の流れ

エンドポイント管理の利用に必要な環境を構築し，利用を開始するまでの流れを次に示します。

> **重要**
>
> 構築に必要な製品媒体は，エンドポイント管理のポータルシステムからダウンロードできます。
>
> サービスポータルでの製品媒体のダウンロードについては，「4.3.9　製品媒体一覧の表示」を参照してください。

2.1.1　運用管理コンピュータの構築の流れ

運用管理コンピュータの構築の流れを次に示します。

それぞれのサービスプランで実施する作業は，次のとおりです。

- 「スタンダード」の場合
  すべて実施してください。
- 「ライト A」の場合
  秘文管理ツールのインストールは不要です。
  図 2-1 の 1～3 を実施してください。
- 「ライト B」の場合
  リモートインストールマネージャとパッケージャのインストールは不要です。
  図 2-1 の 1 と 4 を実施してください。

図 2–1　運用管理コンピュータの構築の流れ



2.1.2　利用者コンピュータの構築の流れ

利用者コンピュータの構築の流れを次に示します。

それぞれのサービスプランで実施する作業は，次のとおりです。

- 「スタンダード」の場合
  すべて実施してください。
- 「ライト A」の場合
  秘文インストール媒体の作成および秘文クライアントのインストールは不要です。
  図 2-2 の 1 と 3 を実施してください。
- 「ライト B」の場合
  すべて実施してください。

図 2–2　利用者コンピュータの構築の流れ

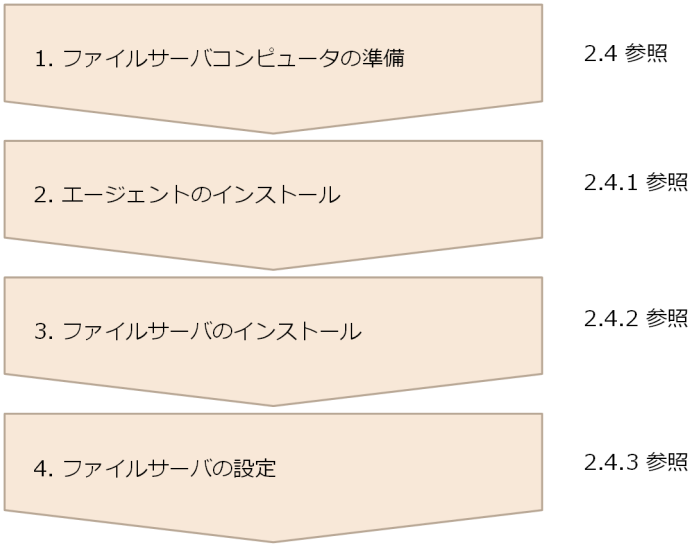


2.1.3　ファイルサーバの構築の流れ

サービスプランが「スタンダード」または「プラン B」の場合で，かつ暗号化オプションをご契約されている場合は，暗号化機能およびファイル保護機能を使用できます。共有フォルダの暗号化機能を使用する場合はファイルサーバを構築してください。共有フォルダの暗号化機能を使用しない場合は，ファイルサーバの構築は不要です。なお，サービスプラン「ライト A」は，暗号化機能を提供していないため，共有フォルダの暗号化機能を使用できません。

ファイルサーバの構築の流れを次に示します。

図 2–3　ファイルサーバの構築の流れ



2.2　運用管理コンピュータの構築

運用管理者が使用する次の条件を満たしているコンピュータを準備してください。

適用 OS のバージョンの詳細は，JP1/IT Desktop Management 2 および秘文のリリースノートで確認してください。

表 2–1　運用管理コンピュータに必要な条件

項目	内容
OS	次のどれかの OS がインストールされていることが前提です。 • Windows 10 • Windows 11 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025
CPU	2GHz 以上
メモリ	2GB 以上
ディスクの空き容量	200MB 以上
ブラウザ	次のどれかのブラウザがインストールされていることが前提です。 • Microsoft Edge • Google Chrome

2.2.1　リモートインストールマネージャのインストール

運用管理コンピュータを使用して資産配布管理サーバから利用者のコンピュータへ，ネットワークを経由してソフトウェアおよびファイルを一括で配布するには，Remote Install Manager を使用します。

JP1 のマニュアル「JP1 Version 13 資産・配布管理 基本ガイド」での，「JP1/IT Desktop Management 2 - Manager をインストールする」を参照し，管理者の端末に Remote Install Manager をインストールしてください。

2.2.2　パッケージャのインストール

リモートインストールするソフトウェアを，管理用サーバに登録するには，パッケージャを使用します。

JP1 のマニュアル「JP1 Version 13 資産・配布管理 基本ガイド」での，「JP1/IT Desktop Management 2 - Agent をインストールする」を参照し，管理者の端末にパッケージャをインストールしてください。

2.2.3　秘文管理ツールのインストール

ユーザーの追加・更新・削除，ポリシーの設定，インストール媒体の作成などの秘文の各設定をするには，秘文管理ツール（秘文マネージャ，インストール媒体作成ツール）を使用します。

秘文サービスのマニュアル「秘文 Endpoint Protection Service 基本ガイド（管理者用）」での，「秘文管理ツールのインストール」を参照し，管理者の端末に秘文管理ツールをインストールしてください。

重要

秘文の管理者として，「カスタマーコード*_XXXXXX*」が登録されています。エンドポイント管理が提供する機能に必要な管理者となりますので削除しないでください。

カスタマーコードはご利用環境情報でお知らせするカスタマーコードです。*XXXXXX* はランダムな英数字 6 文字です。

2.3　利用者コンピュータの構築

利用者のコンピュータ（管理対象機器）を管理するための，インストールセット（JP1/IT Desktop Management 2 - Agent のプログラムと，プログラムのセットアップ情報を含んだファイル）および秘文インストール媒体ファイルを作成して，配布します。

適用 OS のバージョンの詳細については JP1/IT Desktop Management 2 および秘文のリリースノートで確認してください。

利用者のコンピュータの前提となる OS を次の表に示します。

表 2–2　利用者コンピュータの前提となる OS

OS	内容
Windows	• Windows 10 • Windows 11 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025
Linux	• Red Hat Enterprise Linux Server • Oracle Linux
UNIX	• AIX • Solaris • HP-UX
Mac	• Mac OS
スマートデバイスの OS※	• iOS • iPadOS • Android

注※

スマートデバイスを管理するためには，Microsoft Intune が必要です。

重要

OS ごとに機能差異があります。

- JP1 のマニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」での，「Windows エージェント，UNIX エージェント，Mac エージェントの機能差異」を参照してください。
- 持ち出し/読み込み制御，デバイス制御，および許可ネットワーク制御ができるのは，Windows のクライアント OS だけです。

2.3.1　インストールセットの作成

利用者のコンピュータに JP1/IT Desktop Management 2 - Agent をインストールすると，そのコンピュータのハードウェア情報，ソフトウェア情報，利用者情報などを管理できるようになります。

JP1 のマニュアル「JP1 Version 13 資産・配布管理 基本ガイド」での，「JP1/IT Desktop Management 2 - Agent をインストールする」を参照し，利用者のコンピュータへのインストールの準備をしてください。

2.3.2　秘文インストール媒体の作成

管理対象機器にインストールするための，インストール媒体を作成します。

秘文サービスのマニュアル「秘文 Endpoint Protection Service 基本ガイド（管理者用）」での，「インストール媒体の作成」を参照し，インストール媒体を作成してください。

2.3.3　エージェントのインストール

利用者のコンピュータを管理するために，JP1/IT Desktop Management 2 - Agent を利用者のコンピュータにインストールします。

(1)　Windows の場合

JP1/IT Desktop Management 2 - Agent のインストールについては，JP1 のマニュアル「資産・配布管理 基本ガイド」での「JP1/IT Desktop Management 2 - Agent をインストールする」を参照し，インストールしてください。

(2)　UNIX または Mac の場合

JP1/IT Desktop Management 2 - Agent のインストールについては，JP1 のマニュアル「JP1/IT Desktop Management 2 - Agent（UNIX(R)用）」での「インストール」を参照し，インストールしてください。

2.3.4　秘文クライアントのインストール

秘文クライアントをインストールすると，PC からのデータの持ち出し，PC へのデータの読み込み，デバイスの使用，および接続するネットワークを制御できます。USB メモリなどのリムーバブルメディアへの持ち出し，USB メモリなどのリムーバブルメディアからの読み込み，ネットワーク上のフォルダへの持ち出し，印刷，デバイスの使用，ネットワークの接続などを禁止できます。また，これらの持ち出しと読み込み行為をログとして取得し，ログ中継サーバに送信します。

秘文サービスのマニュアル「秘文 Endpoint Protection Service 基本ガイド（管理者用）」での，「秘文クライアントの新規インストール手順」を参照し，管理者の端末に秘文クライアントをインストールしてください。

2.4　ファイルサーバの構築

ファイルサーバとして次の条件を満たしているコンピュータを準備してください。

適用 OS のバージョンの詳細は，秘文のリリースノートで確認してください。

表 2–3　ファイルサーバに必要な条件

項目	内容
OS	次のどれかの日本語版 OS がインストールされていることが前提です。 • Windows Server 2016※1 • Windows Server 2019※1 • Windows Server 2022※1
CPU	2GHz 以上
メモリ	4GB 以上
ハードディスク （インストール時）	55MB の空き容量
ハードディスク （運用時）	1GB 以上の空き容量
ネットワーク	• TCP/IP および Microsoft Network サービスがインストールされていて，かつサーバに IPv4 形式の固定 IP アドレスが設定されていることが前提です。なお，IPv6 形式のアドレスだけが設定されたネットワーク環境には対応していません。 • 秘文サービスの URL（https://hibun-sv.hitachi-solutions.co.jp/）へアクセスできることが前提です。※2

注※1

Server Core および Nano Server の構成には対応していません。

注※2

秘文サービスの URL（https://hibun-sv.hitachi-solutions.co.jp/）へのアクセスは次のどちらかとなるように，必要に応じてネットワーク環境（プロキシやファイアウォールなどの設定）を変更してください。

・プロキシを経由しないで直接アクセスできる。

・PAC ファイルを指定していない場合は，複数プロキシではないプロキシを経由してアクセスできる。

2.4.1　エージェントのインストール

利用者のコンピュータを管理するために，JP1/IT Desktop Management 2 - Agent を利用者のコンピュータにインストールします。2.3.3 エージェントのインストールを参照してください。

2.4.2　ファイルサーバのインストール

コンピュータにファイルサーバをインストールします。

ファイルサーバの構築については，秘文サービスのマニュアル「秘文 Endpoint Protection Service 基本ガイド（管理者用）」での，「ファイルサーバのインストールと設定」を参照し，管理対象機器にファイルサーバをインストールしてください

2.4.3　ファイルサーバの設定

ファイルサーバで共有機密フォルダ（共有フォルダの暗号化）として登録するフォルダを設定します。

詳細については，秘文サービスのマニュアル「秘文 Endpoint Protection Service 基本ガイド（管理者用）」での，「ファイルサーバのインストールと設定」を参照してください。

3 エンドポイント管理の利用方法

エンドポイント管理を利用して，コンピュータやデバイス機器の管理をする場合の設定について説明します。

3.1　システムの概況把握

IT 機器のセキュリティ管理を徹底するためには，ルールを適用する機器をすべて把握しておく必要があります。また，IT 機器を組織内の資産として管理するためには，使用しているハードウェア，ソフトウェアは何かという情報とそれらが今どのような状態になっているかを把握しておく必要があります。

大量の管理情報に対して管理者が状況を把握するためのホーム画面とダッシュボードを使用して概況を把握し，確認したい内容のリンクをたどることで詳細情報を確認します。

JP1 のマニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」での，「システムの概況表示」で詳細情報を確認してください。

3.2 機器の管理

組織内のネットワークには，コンピュータやサーバ，プリンタ，ネットワーク装置など，さまざまな機器が接続されています。組織内の機器の状況を把握し，セキュリティ管理や資産管理を始めるためには，まず，組織内の機器を JP1/IT Desktop Management 2 の管理対象にします。

JP1 のマニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」での，「機器の管理」で管理できる情報を設定してください。

なお，エンドポイント管理では JP1/ITDM2 が出力する保存用の変更履歴をポータルシステムからダウンロードできます。

3.3　機器のリモートコントロール

リモートコントロール機能を利用すると，管理者の手もとのコンピュータから問題の発生したコンピュータを遠隔操作して，操作内容を共有したり，データを送受信したりして問題に速やかに対応できます。

JP1 のマニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」での，「機器のリモートコントロール」で管理できる情報を設定してください。

3.4　資産の管理

組織内で管理している機器，ソフトウェアライセンス，契約などの資産情報をまとめて管理できます。

各資産を一覧化して台帳のように管理できるほか，資産情報同士の関係を定義することで，機器に対して結んでいる契約を即座に把握したり，ソフトウェアライセンスの利用状況を把握したりできるため，資産管理業務の効率化を図ることができます。

JP1 のマニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」での，「資産の管理」で管理できる情報を設定してください。

3.5 配布機能

JP1/IT Desktop Management 2 のリモートインストール機能を使用して，日立プログラムプロダクト，他社ソフトウェア，更新プログラムなどを管理対象のコンピュータへ配布できます。

リモートインストール機能では，配布する日時を指定したり，条件と一致したコンピュータだけに配布したりできます。また，配布されるソフトウェアを利用者が指定してインストールしたり，JP1/IT Desktop Management 2 がインストールされているスタンドアロン PC にソフトウェアをインストールしたりもできます。

JP1 のマニュアル「JP1 Version 13 資産・配布管理 基本ガイド」での，「運用 2：ファイルの配布」または JP1 Version 13 JP1/IT Desktop Management 2 配布機能 運用ガイド」での，「更新プログラムを管理する」を参照し，配布してください。

3.6　機器のネットワーク接続の管理

無線 LAN やモバイルコンピュータの普及に伴い利便性が向上してきたことで，組織の従業員または組織外の人によって個人が使用するコンピュータが意図的に持ち込まれ，容易に組織内のネットワークに接続されるおそれがあります。セキュリティ対策がされていない機器がネットワーク接続することによるウィルス感染や，機密情報の不正持ち出しといった被害を防ぐためには，ネットワーク接続されている機器を把握して管理します。

JP1 のマニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」での，「機器のネットワーク接続の管理」で管理できる情報を設定してください。

3.7　セキュリティの管理

組織内のセキュリティ状況を安全に保つためには，ウィルス対策製品の未インストール，ファイル共有ソフトウェアのインストール，OS セキュリティ設定の不備など，多くの要素に対するセキュリティのルールを決め，そのルールを各コンピュータの利用者に遵守させる必要があります。また，セキュリティの現状を把握して，問題点を適宜対策することも必要です。

組織内のセキュリティのルールを「セキュリティポリシー」として設定し，それらを各コンピュータに適用することで，問題点を発見して管理者に通知したり，自動的に対策したりできます。

なお，UNIX エージェントは，セキュリティポリシーによるセキュリティ状況の判定やセキュリティ上の問題点の自動対策の対象外です。Mac エージェントは，セキュリティ上の問題点の自動対策の対象外です。

JP1 のマニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」での，「セキュリティの管理」を参照し，セキュリティ管理に関するさまざまな設定をしてください。

3.8　操作ログの管理

セキュリティポリシーに操作ログの取得を設定して，対象のコンピュータにセキュリティポリシーを割り当てると，対象のコンピュータから操作ログを取得できます。

取得する操作ログの種類は，セキュリティポリシーの設定で変更できます。不審操作を検知するかどうかも，セキュリティポリシーの設定で変更できます。

なお，UNIX エージェント，Mac エージェントは，操作ログ収集の対象外です。

JP1 のマニュアル「JP1/IT Desktop Management 2 導入・設計ガイド」での，「操作ログの管理」を参照し，操作ログの設定をしてください。

3.9　ポリシーの反映

持ち出し制御/読み込み制御，デバイス制御，および許可ネットワークの制御をするには，そのポリシーを反映したインストール媒体を作成し，利用者のコンピュータ（管理対象機器）にインストールする必要があります。

なお，ポリシーを変更する場合は，ポリシーを変更したインストール媒体を作成し，上書きインストールする必要があります。

秘文のマニュアル「秘文 セットアップガイド（管理者用）」での，「インストール媒体の作成（パラメータシートからの読み込み）」，または，「インストール媒体の作成（画面入力による詳細設定）」を参考に，インストール媒体を作成してください。

3.10　暗号化機能

指定した管理対象機器のローカルドライブ，管理対象機器から持ち出すファイル，およびファイルサーバ上で保存するファイルを暗号化できます。

詳細は秘文のマニュアル「秘文 管理者ガイド（機能解説編）」での，「暗号化機能」を参照してください。

3.11　ファイル保護機能

機密データ（保護対象ファイル）に対して，マルウェアなどの不正なプログラムによる情報窃取や破壊を防止する機能です。

詳細は秘文のマニュアル「秘文 管理者ガイド（機能解説編）」での，「秘文 DE の暗号ファイル保護機能」を参照してください。

4 エンドポイント管理のポータルシステムの利用方法

エンドポイント管理のポータルシステムの利用方法について説明します。ポータルシステムでは，エンドポイント管理のサービス利用での定型作業を支援し，運用作業を効率化する機能を提供します。

4.1　ポータルシステムの概要

ポータルシステムで提供する機能の一覧を次に示します。

表 4–1　ポータルシステムの機能一覧

機能	説明
ログインとログアウト	不正なユーザーによるアクセスを防止するために，ログイン認証します。
ログインユーザーのパスワード変更	ログインしているポータルシステムのユーザーのパスワードを変更できます。
サーバー覧の表示	サービスの利用者が利用できるサービスの管理画面の一覧を表示します。クリックすると，それぞれの管理画面に連携します。 • JP1/ITDM2 Manager へのリンク • 秘文管理コンソールのリンク JP1/ITDM2 Manager のサーバの場合，次のタスクの実行ができます。 • 操作ログのエクスポート • 管理項目定義のインポート • 管理項目定義エクスポート
タスク一覧の表示	サーバー覧でサービスの利用者が実行したタスクの一覧を表示します。
認証設定	サービスの利用者が認証関連の設定を変更できます。 スタンダードまたはライト A のプランを契約されている場合に利用できます。
ログの表示	サービスの利用者が参照できる操作ログおよび変更履歴をダウンロードできます。
製品媒体一覧の表示	サービスの利用者がダウンロードできる製品媒体の一覧を表示できます。
マニュアル一覧の表示	サービスの利用者が利用できるサービスに関連する製品マニュアル，取扱説明書，利用ガイドなどのマニュアルドキュメントを表示できます。
提供ファイル一覧の表示	サービスの利用者が利用できるサービスに関連する設定ファイルやツールなどのファイルを表示できます。
サポート情報一覧の表示	サービスの障害回避・予防に関する情報や注意喚起情報などのサポート情報を確認できます。
お知らせの表示	サービス提供者からのお知らせを表示できます。
ライセンス情報の表示	ログインしているアカウントにひもづく契約に基づいたライセンス情報を表示します。

4.2　利用できる Web ブラウザ

ポータルシステムを利用できる Web ブラウザを次に示します。

- Google Chrome
- Microsoft Edge

4.3　ポータルシステムの利用方法

ポータルシステムの利用方法について説明します。

エンドポイント管理では次に示すモバイル認証アプリをサポートしています。

- FreeOTP
- Google Authenticator
- Microsoft Authenticator

4.3.1　シングルサインオン（SSO）の利用方法

シングルサインオン（SSO）はポータルシステムと JP1/ITDM2 管理画面および秘文サービス管理ページの認証プロセスを統合し，一度の認証で両画面にアクセス可能とする仕組みです。

(1)　SSO 導入時の設定概要

- SSO 利用時，ポータルシステムと JP1/ITDM2 および秘文サービス管理ページのユーザー ID が完全一致している必要があります。該当システムで異なる ID の場合，ログインできませんので注意してください。
- JP1/ITDM2 のアカウントを追加・削除・変更する場合は，必ずポータルシステムのアカウント追加申請や同一 ID への変更も同時に実施してください。
- 秘文サービス管理ページのアカウントを追加する場合は，必ずポータルシステムのアカウント追加申請も同時に実施してください。アカウントの追加方法は，「4.3.2(1)　アカウント追加」を参照してください。

  追加したアカウントは自動的に SSO の対象になります。

(2)　注意事項

- SSO 利用時は，JP1/ITDM2 および秘文サービス管理ページで自由に作成された ID ではログインできません。ポータルシステムと同一 ID で JP1/ITDM2 および秘文サービス管理ページのアカウントを作成してください。
- SSO 利用開始後は，SSO 認証を無効化することはできません。
- SSO 利用時でも，JP1/ITDM2 の API 利用時は SSO に連動しないで，JP1/ITDM2 の認証情報（ユーザー ID／パスワード）を利用します。
- 秘文サービス管理ページの SSO は，エンドポイント管理 V02-50 以前では利用できません。

4.3.2　ユーザーアカウント管理

ユーザーアカウントは，管理者の役割に応じて適切に管理してください。

ここでは，ポータルシステムおよび JP1/ITDM2 管理画面でのユーザーアカウントの追加・削除・変更手順と注意事項を説明します。SSO 利用時と非利用時で設定方法や反映範囲が異なるため，ご利用環境に応じて該当する手順を確認してください。

契約したプランによって付与できる権限，業務分掌が異なりますので，詳細は契約情報をご確認ください。

(1)　アカウント追加

ポータルアカウントが不足する場合は，追加申請してください。

SSO 利用時

JP1/ITDM2 および秘文サービス管理ページへの新規ユーザーアカウントは，ポータルシステムのユーザー ID と同一 ID で作成してください（「JP1 Cloud Service のご利用環境の情報（エンドポイント管理）」を参照してください）。

JP1/ITDM2 の場合

JP1/ITDM2 のユーザーアカウントの追加の詳細は，JP1 のマニュアル「JP1/IT Desktop Management 2 運用ガイド」の「ユーザーアカウントを追加する手順」を参照してください。

秘文の場合

秘文サービス管理ページへの新規ユーザーアカウントの追加は，次の手順で実施してください。

1. ご利用環境情報でお知らせする管理者名で秘文サービス管理ページにログインします。



ユーザー認証に成功すると，ダッシュボード画面が表示されます。

重要

- ポータルシステムにログイン中のユーザ ID と同一のユーザがサービス管理ページに登録されていない場合，サービス管理ページを開くとログイン画面に「EPSSV_MSGID_E0176」メッセージが表示されます。その場合は，ご利用環境情報に記載の管理者アカウントでログインしてください。

- ポータルシステムにログイン中のユーザ ID と同一のユーザがサービス管理ページに登録されている場合は，SSO 認証によりサービス管理ページのダッシュボード画面が表示されます。

2. ダッシュボード画面の［ユーザ管理］メニューをクリックします。

   ユーザ管理画面が表示されます。



> **メモ**
>
> ユーザ認証設定のメニューは，SSO 有効のユーザでログインした場合は表示されません。

3. ［ユーザ追加］ボタンをクリックします。

   ユーザ追加画面が表示されます。



   ユーザ ID にポータルシステムのアカウントと同じユーザ ID を入力します。

4. ［OK］ボタンをクリックするとユーザが追加されます。

秘文サービス管理ページからログアウトしたあと，ポータルシステムにある秘文サービス管理ページへのリンクから再度開くと SSO 認証され，秘文サービス管理ページにアクセスできることを確認してください。

(2)　アカウント変更

SSO 利用時

パスワードを変更する場合はポータルシステムの画面で変更してください。

JP1/ITDM2 の場合

パスワード以外（権限，メールなど）は JP1/ITDM2 の管理画面で個別に変更してください。

秘文の場合

パスワード以外に変更できるユーザーアカウントの設定はありません。

SSO 非利用時

JP1/ITDM2 管理画面または秘文サービス管理ページで変更してください。

(3)　アカウント削除

JP1/ITDM2 および秘文サービス管理ページからログイン制限したいアカウントは直接削除します。

JP1/ITDM2 の場合

初期設定で登録されている保守用の ITDM2 アカウントは削除しないでください。

JP1/ITDM2 のユーザーアカウントの削除の詳細は，JP1 のマニュアル「JP1/IT Desktop Management 2 運用ガイド」の「ユーザーアカウントを削除する手順」を参照してください。

秘文の場合

秘文のユーザーアカウントは秘文コンソールのユーザ管理画面から削除してください。



削除対象のユーザ ID のチェックボックスを選択して，［ユーザ削除］ボタンをクリックします。

表示される確認メッセージで削除対象のユーザ ID に間違いがないことを確認して削除してください。

(4)　モバイル認証アプリの変更

ログインで使用するモバイル認証アプリを変更する場合は，モバイル認証アプリの登録を解除します。

サポートサービスに登録の解除を申請してください。

登録が解除されたあと，ポータルシステムの初回ログインと同じ操作で新しいモバイル認証アプリを使用してログインしてください。

4.3.3　ログインとログアウト

ポータルシステム，JP1/ITDM2 管理画面，および秘文サービス管理ページでは，SSO の利用有無によって，ログイン認証方式とログアウト動作が異なります。

SSO 利用有無に応じて該当手順を確認してください。

(1)　ログイン手順

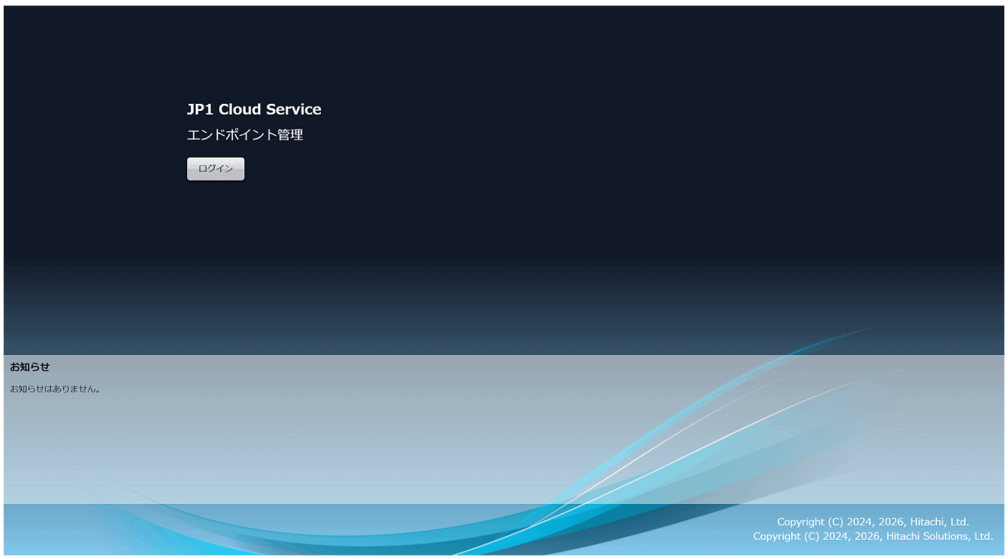
ログインする手順を次に示します。

> **重要**
>
> - ポータルシステムのログイン期限が切れている場合は，ポータルシステムのログイン時と同様にモバイル認証アプリによるワンタイムコードの入力が必要です。
> - SSO 利用時は，ポータルシステムと JP1/ITDM2 管理画面および秘文サービス管理ページが連動して認証されます。

1. Web ブラウザを起動して，ポータルシステムの URL にアクセスします。

   ポータルシステムの URL や，初期提供されるユーザー ID，ユーザーの初期パスワードは，ご利用環境情報でお知らせする接続情報でご確認ください。

   なお，ログインユーザーの追加・変更をご希望の場合は，ヒアリングシートへ必要事項をご記入のうえ，申請をお願いいたします。

   ログイン画面に表示する各エリアの説明を次に示します。

項目	説明
お知らせエリア	システムメンテナンスによるサービス停止など，サービス提供元からのお知らせが表示されます。

2. ［ログイン］ボタンをクリックします。

表示されたログイン画面で，ユーザー ID とパスワードを入力して［ログイン］ボタンをクリックします。



3. ユーザー ID とパスワードの認証に成功すると，ワンタイムコード認証情報画面が表示されます。

■初回

QR コードを読み込んで表示されたモバイル認証アプリから取得したワンタイムコードとデバイス名を入力して［送信］ボタンをクリックします。

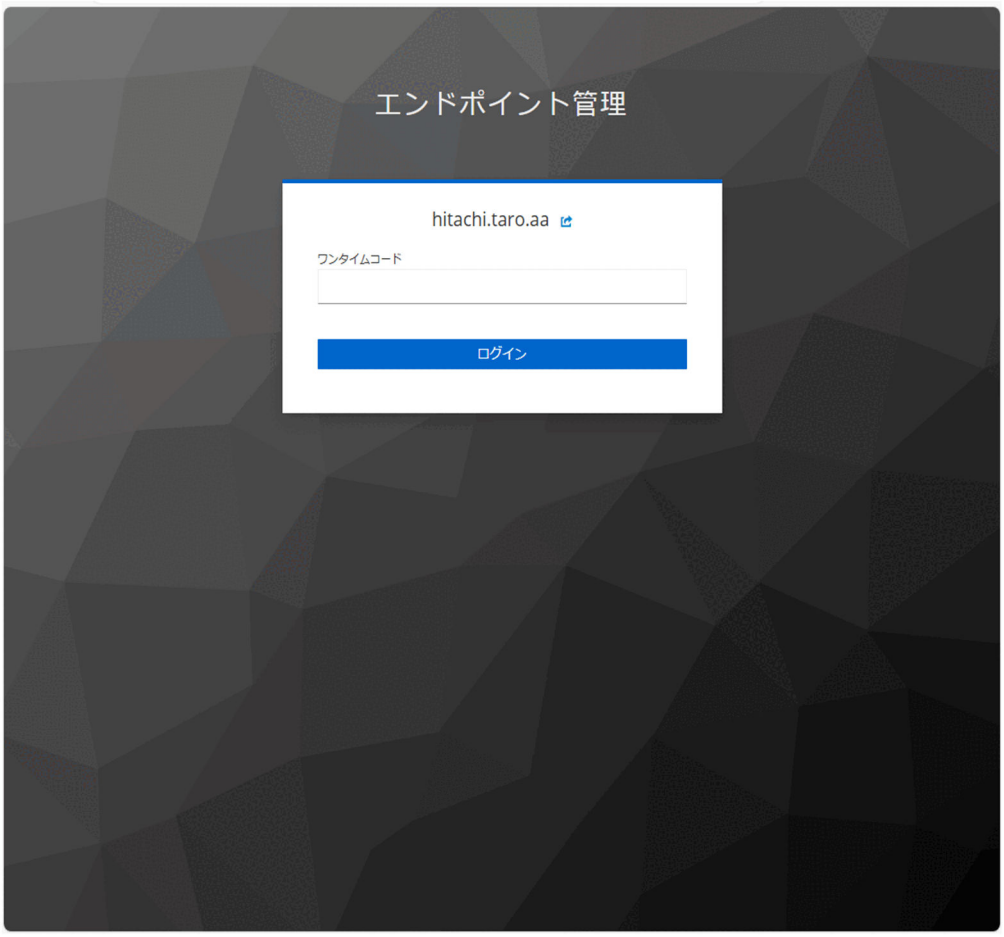


ワンタイムコード認証情報画面に表示する項目と説明を次に示します。

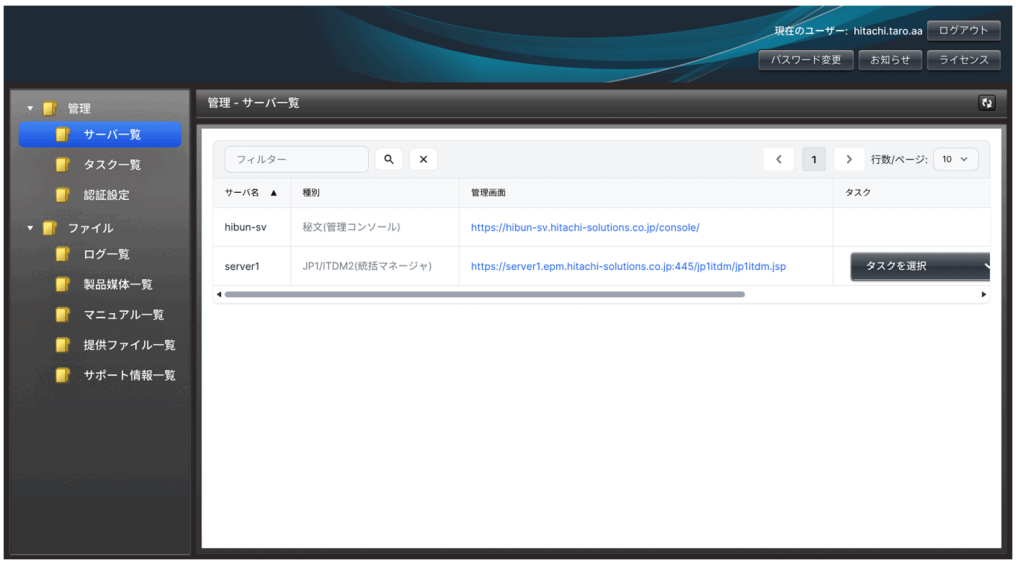
項目	説明
QR コード	スキャンしてアプリケーションを開き，ワンタイムコードを取得します。
ワンタイムコード	上記で取得したワンタイムコードを入力します。
デバイス名	デバイス名を入力します。必須ではありません。
Sign out from other devices	他のデバイスからサインアウトする場合，チェックします。

■2 回目以降

モバイル認証アプリに表示されたワンタイムコードを入力してログインします。



1. ログインに成功すると，メイン画面が表示されます。



メイン画面に表示する項目と説明を次に示します。

画面	説明
共通	画面上部で共通の次の機能を提供します。 • ログインユーザーの情報表示（「現在のユーザー」で示されたユーザー ID）

画面	説明
共通	• ログインユーザーのパスワード変更（[パスワード変更] ボタン） • お知らせの表示（[お知らせ] ボタン） • ライセンスの表示（[ライセンス] ボタン） • ログアウト（[ログアウト] ボタン）
管理	エンドポイント管理で管理するサーバの情報，および特定のサーバに対し実行されるタスクの実行状態などを提供します。 • サーバ一覧 JP1/ITDM2（統括マネージャ），JP1/ITDM2（中継マネージャ），および秘文（管理コンソール）のサーバ一覧を表示します。 SSO 利用時，JP1/ITDM2（統括マネージャ），JP1/ITDM2（中継マネージャ），および秘文（管理コンソール）へのログイン操作は不要です。 SSO 非利用時，JP1/ITDM2（統括マネージャ），JP1/ITDM2（中継マネージャ）のユーザー ID／パスワード入力画面，および秘文サービス管理ページで認証します。 • タスク一覧 サーバ一覧画面から開始した操作ログのエクスポート，管理項目定義のインポートおよびエクスポートのステータス（実行状態），操作結果詳細，および関連情報を表示します。 • 認証設定 サービスの利用者が，API 認証に関する設定を変更できます。
ファイル	次のファイルを提供します。 • ログ一覧 サービスの利用者が参照できる操作ログと変更履歴の一覧を表示します。 • 製品媒体一覧 サービスの利用者が利用できる製品媒体の一覧を表示します。 • マニュアル一覧 サービスの利用者が利用できるマニュアルの一覧を表示します。 • 提供ファイル一覧 サービスの利用者が利用できる提供ファイルの一覧を表示します。 • サポート情報一覧 サービスの利用者が利用できるサポート情報の一覧を表示します。

ポータルシステムのログイン状態の有効期限は 30 分です。有効期限を過ぎると，再認証が必要です。

特定回数連続してパスワード入力不正によるログインエラーが続いた場合，当該ユーザー ID を一定時間ロックアウトします。

ロックアウトしきい値は 10 回で，ロックアウト時間は 30 分です。

ロックアウトの詳細については，「(3)　ロックアウト機能」を参照してください。

(2)　ログアウト手順

ログアウトする場合は，メイン画面の右上の［ログアウト］ボタンをクリックします。ログアウトすると，ログイン画面が表示されます。

- SSO 利用時

  ポータルシステムからログアウトしてください。

  なお，表示中の JP1/ITDM2 の管理画面および秘文サービス管理ページはログアウト後も操作可能であるため，必ず画面を閉じてください。

- SSO 非利用時
  - JP1/ITDM2 の管理画面のログアウト

    JP1/ITDM2 の管理画面からログアウトしてください。
  - 秘文サービス管理ページのログアウト

    秘文サービス管理ページからログアウトしてください。

(3)　ロックアウト機能

10 回連続でパスワードの認証に失敗した場合，アカウントがロックされます。11 回目以降はログイン不可とし，30 分経過すると再度ログインができるようになります。

4.3.4　ログインユーザーのパスワード変更

ログインユーザーのパスワード変更は，メイン画面の右上の［パスワード変更］ボタンから行います。

SSO 利用時にパスワードを変更する場合は必ずポータルシステムの画面で変更してください。JP1/ITDM2 管理画面からの変更は反映されませんので注意してください。

［パスワード変更］ボタンをクリックすると表示される次のダイアログから変更を実施してください。



パスワード変更ダイアログに表示する項目と説明を次に示します。

項目	説明
ユーザー ID	ログインしているユーザーのユーザー ID が表示されます。
現在のパスワード	現在のパスワードを入力します。
新しいパスワード※	8〜128 バイトの任意文字列（半角英数字および記号）を指定します。
新しいパスワード（確認）※	上記の新しいパスワードと同じ文字列を指定します。
ワンタイムコード	モバイル認証アプリで取得した半角数字 6 桁のコードを入力します。

注※

次のパスワードポリシーを満たしている必要があります。

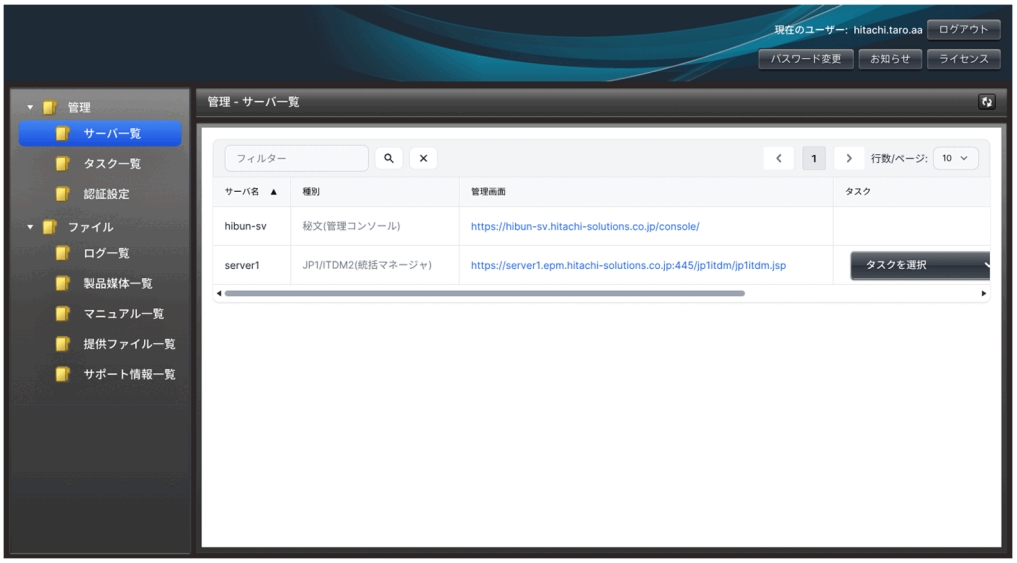
- 8 文字以上 128 文字以下
- 半角英数字または次に示す記号

  !，"，#，$，%，&，'，(,)，*，+，,（コンマ），-，.（ピリオド），/，:，;，<，=，>，?，@，[，¥,]，^，_，`，{，|,}，~，および半角スペース
- 2 種類以上の文字の組み合わせ
- ユーザー ID と異なる文字列
- 現在のパスワードと異なる文字列

4.3.5　サーバー一覧の表示

サービスの利用者が利用できるサーバー一覧が表示されます。

管理したいサーバー一覧の種別を選択し，管理画面項目の URL をクリックすると，それぞれの管理画面が表示されます。



サーバー一覧画面に表示する項目と説明を次に示します。

項目		説明
フィルタリング	フィルター	検索したい文字列を入力します。
		フィルターに入力した文字列で検索します。
	×	フィルター条件を解除します。
ページネーション	＜	表示している前のページが表示されます。
	n（ページ）	選択したページが表示されます。
	＞	表示している次のページが表示されます。
	表示行数	サーバ一覧画面に表示される件数は，次のどれかから選択できます。 • 10 • 30 • 50 初期設定（デフォルト）は「10」です。
サーバ名		利用できるサーバの名称が表示されます。
種別		サーバの種別が表示されます。 JP1/ITDM2（統括マネージャ） 複数サーバ構成の最上位に設置されたサーバのことです。 JP1/ITDM2（中継マネージャ） JP1/IT Desktop Management 2 - Manager を管理用中継サーバとして設定したサーバのことです。 管理用中継サーバ追加オプションを契約されている場合に表示されます。 秘文（管理コンソール） 秘文サービス管理ページのことです。 次のプランを契約されている場合に表示されます。 ・スタンダード ・ライト B
管理画面		サーバの URL が表示されます。
タスク		JP1/ITDM2 サーバに対して実行可能なタスクを選択することができます。ただし，各サーバでは同時に 1 件のタスクしか実行できません。 選択できるタスクの種別は次のとおりです。 操作ログのエクスポート 操作ログをエクスポートします。 次のプランを契約されている場合に表示されます。 ・スタンダード ・ライト B 管理項目定義のインポート 管理項目定義をインポートします。 管理項目定義のエクスポート 管理項目定義をエクスポートします。

(1)　JP1/ITDM2（統括マネージャ）

SSO 利用時と非利用時で，管理画面項目で表示されている URL をクリックしたときの操作が異なります。

- SSO 利用時

  ログイン操作は不要です。URL をクリックすると，直接 JP1/ITDM2 の管理画面が表示されます。

- SSO 非利用時

  URL をクリックすると，JP1/ITDM2 のログイン画面が表示されます。ユーザー ID とパスワードを入力し，ログインしてください。ログインに成功すると，JP1/ITDM2 の管理画面が表示されます。

JP1/ITDM2 の管理画面では，JP1/ITDM2 で管理している情報の概況を各パネルで確認できます。

ヒント

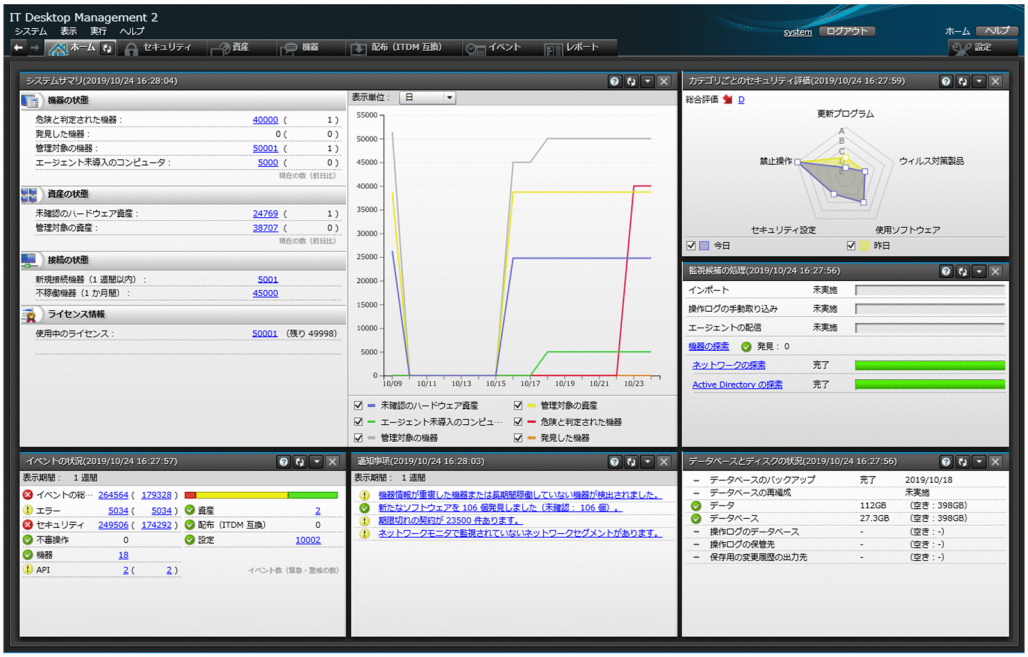
JP1/ITDM2（統括マネージャ）の URL に直接アクセスする場合の操作

- SSO 利用時

  ポータルシステムのログイン画面が表示されます。ログイン手順については，「4.3.3(1)　ログイン手順」の手順 2.以降を参照してください。

- SSO 非利用時

  JP1/ITDM2 のログイン画面が表示されます。ログインに成功すると，JP1/ITDM2 の管理画面が表示されます。



管理している最新情報を基に，日々の運用で把握しておく必要がある内容が表示されます。各項目をクリックすることで，詳細な情報を確認できる画面を表示できます。

(2)　JP1/ITDM2（中継マネージャ）

JP1/ITDM2（統括マネージャ）の場合と同様です。詳細については，「(1)　JP1/ITDM2（統括マネージャ）」を参照してください。

管理用中継サーバ追加オプションを契約されている場合に表示されます。

(3)　秘文（管理コンソール）

SSO 利用時と非利用時で，管理画面項目で表示されている URL をクリックしたときの操作が異なります。

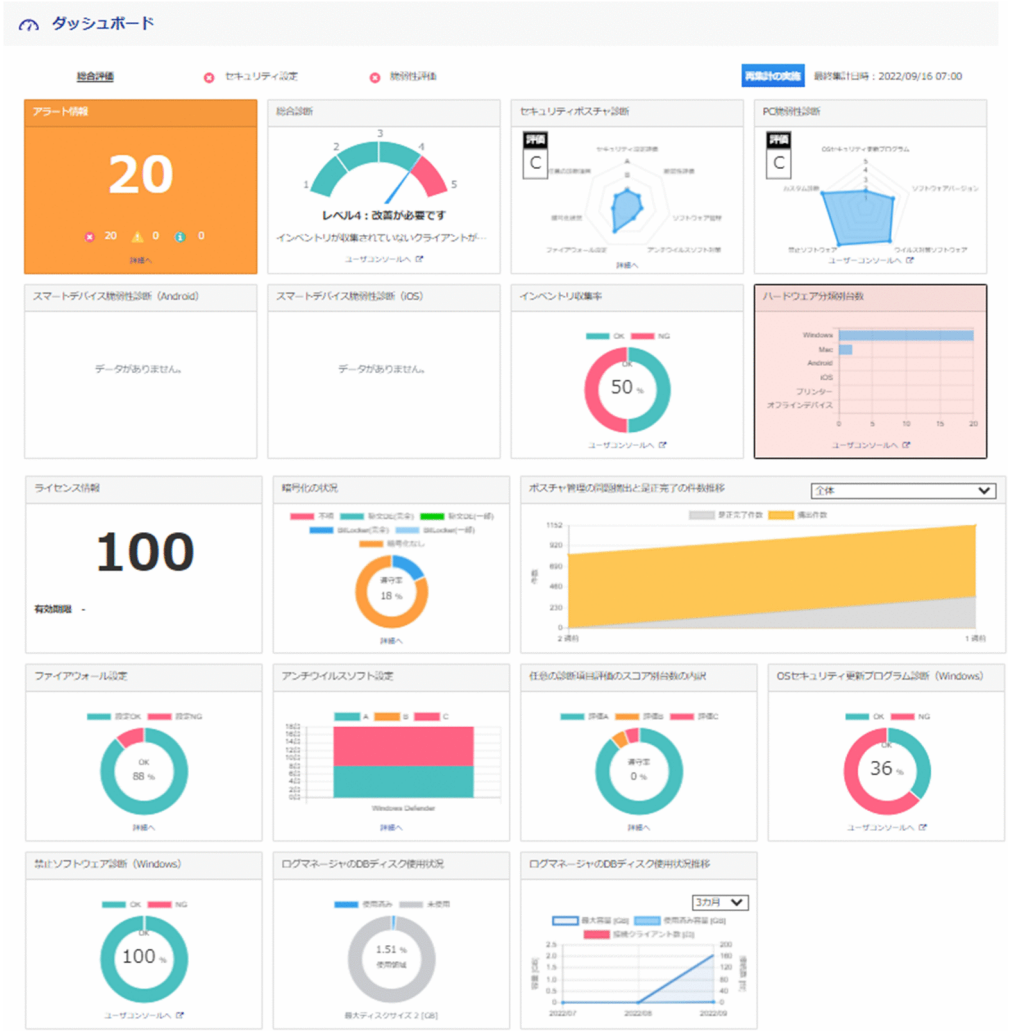
- SSO 利用時

  ログイン操作は不要です。URL をクリックすると，直接秘文コンソールのダッシュボード画面が表示されます。

- SSO 非利用時

  URL をクリックすると，サービス管理ページが表示されます。ユーザ ID とパスワードを入力し，ログインしてください。ログインに成功すると，秘文（管理コンソール）のダッシュボード画面が表示されます。

> **ヒント**
>
> 秘文（管理コンソール）の URL に直接アクセスする場合の操作
>
> - SSO 利用時
>
>   ポータルシステムのログイン画面が表示されます。ログイン手順については，「4.3.3(1) ログイン手順」の手順 2.以降を参照してください。
>
> - SSO 非利用時
>
>   秘文（管理コンソール）のログイン画面が表示されます。ログインに成功すると，秘文（管理コンソール）のダッシュボード画面が表示されます。



ダッシュボードの詳細な内容については，秘文サービスのマニュアル「秘文 Endpoint Protection Service 基本ガイド(管理者用)」での，「サービス管理ページにログインする」を参照してください。

(4)　JP1/ITDM2 サーバで実行可能なタスク

サーバ一覧画面から実行したタスクの進捗状況と最終結果は，「4.3.6　タスク一覧の表示」で確認できます。

(a)　操作ログのエクスポート

サーバ一覧画面の［タスク］で［操作ログのエクスポート］をクリックすると，選択したサーバの操作ログをエクスポートできます。

エクスポートできる期間は，標準で過去最大 180 日分までです。1 回のエクスポートで指定できる期間は最大 30 日です。ただし，取得する操作ログの種類または管理対象機器の使用状況によって保管できる期間が短くなることがあります。なお，「エンドポイント管理 - 操作ログ拡張オプション」を契約すると，操作ログの保管期間を延長することができます。

無効な日付範囲やエクスポート期間の最大日数よりも長い期間を指定した場合はエラーメッセージを表示します。

重要

操作ログの件数は，管理対象の機器台数や各機器で発生するログの量に依存し，非常に膨大になる可能性があります。そのため，出力期間を長く指定すると，次のような問題が発生することがあります。

- タスクの処理時間が長くなる
- タスクがタイムアウトし，エラーとなる
- 一度開始したタスクは途中で中止できないため，タイムアウトまでの間，対象サーバで他のタスクを実行できなくなる

操作ログの件数が多くなると予想される場合は，次の対応を推奨します。

- 出力対象期間を短く設定する
- タイムアウトが発生した場合は，対象期間をさらに短縮して再実行する

これにより，タスクの安定した実行が期待できます。



操作ログのエクスポートダイアログに表示する項目と説明を次に示します。

項目	説明
開始日※	エクスポートするログの開始日をカレンダーメニュー から「YYYY/MM/DD」形式で指定します。
終了日※	エクスポートするログの終了日をカレンダーメニュー から「YYYY/MM/DD」形式で指定します。
OK	操作ログのエクスポートの確認ダイアログが表示されます。
キャンセル	操作ログのエクスポートダイアログを閉じます。

注※

指定は必須です。

(b)　管理項目定義のインポート

サーバ一覧画面の［タスク］で［管理項目定義のインポート］をクリックすると，選択したサーバの管理項目定義をインポートできます。



管理項目定義のインポートダイアログに表示する項目と説明を次に示します。

項目	説明
ファイル	をクリックして表示されるファイル選択ダイアログから管理項目定義の CSV ファイルを選択します。指定は必須です。 CSV ファイルだけが選択できます。 文字コードは「UTF-8」を使用してください。 エクスポートしたファイルを基に編集してください。 インポートファイルの設定項目については，JP1 のマニュアル「JP1/IT Desktop Management 2 運用ガイド」での，「共通管理項目と追加管理項目の定義のインポートファイルの設定項目」を確認してください。
OK	管理項目定義のインポートの確認ダイアログが表示されます。
キャンセル	管理項目定義のインポートダイアログを閉じます。

(c)　管理項目定義のエクスポート

サーバ一覧画面の［タスク］で［管理項目定義のエクスポート］をクリックすると，選択したサーバの管理項目定義をエクスポートできます。

エクスポートできる管理項目定義は，JP1/ITDM2 の次の共通管理項目と追加管理項目のうち，データ型が階層型と選択型のものです。

- ハードウェア資産情報と機器情報の共通管理項目

- ハードウェア資産情報の追加管理項目
- ソフトウェアライセンス情報の追加管理項目
- 契約情報の追加管理項目

> **ヒント**
>
> 対象サーバのタスクを選択し，確認ダイアログの OK ボタンをクリックしたあと対象サーバに他の実行中のタスクがなければ，タスクを受け付けた旨のメッセージが表示されます。このメッセージが表示されると，他の画面を操作することができます。対象サーバに他の実行中のタスクがある場合は，タスクが実行中の旨のメッセージが表示されます。実行中のタスクが完了するまでお待ちください。

(5)　タスクの同時実行について

タスクの実行方法には，サーバ一覧画面から実行する方法と API で実行する方法があります。

タスクの実行方法やタスク種別にかかわらず，同一サーバに対して同時に実行できるタスクは 1 件だけです。実行中のタスクがある場合は，同一サーバに対して他のタスクを実行できません。

4.3.6　タスク一覧の表示

サーバ一覧画面から開始したタスク，「操作ログのエクスポート」，「管理項目定義のインポート」，または「管理項目定義のエクスポート」のステータス（実行状態），操作結果詳細，および関連情報を確認できます。

ログインユーザーおよび同じライセンスで使用している他のユーザーが開始したタスクの一覧が表示されます。





タスク一覧画面に表示する項目と説明を次に示します。

項目		説明
フィルタリング	フィルター	検索したい文字列を入力します。
	🔍	フィルターに入力した文字列で検索します。
	×	フィルター条件を解除します。
ページネーション	＜	表示している前のページが表示されます。
	n（ページ）	選択したページが表示されます。
	＞	表示している次のページが表示されます。
	表示行数	タスク一覧画面に表示される件数は，次のどれかから選択できます。 • 10 • 30 • 50 初期設定（デフォルト）は「10」です。
タスク名		システムが自動生成した次の形式のタスク名称が表示されます。 *ServerName*-タスク種別-*YYYYMMDDHHmmss* ServerName：サーバ名 タスク種別：次のどれかが表示されます。 ・操作ログのエクスポート ・管理項目定義のインポート ・管理項目定義のエクスポート YYYYMMDDHHmmss：タスク実行日時
ステータス		タスクのステータスとして，次のどれかが表示されます。 • 実行待ち※1 タスクの受け付けは完了しましたが，実行はまだ開始されていない状態です。

項目	説明
ステータス	• 実行中※2 タスクの実行が開始されましたが，まだ終了していない状態です。 • 正常終了 タスクの実行が正常に終了した状態です。 • エラー タスクの実行中に発生したエラーやタイムアウトによって，タスクが不正に終了した状態です。 • 中止待ち※3 「実行待ち」のタスクに対するユーザーの中止操作の受け付けは完了しましたが，タスクはまだ中止されていない状態です。 • 中止 タスクがユーザーの操作によって中止された状態です。
開始日時	タスクの実行を開始した日時が表示されます。
終了日時	タスクが終了した日時が表示されます。
サーバ名	タスクを実行する対象サーバ名が表示されます。
タスク種別	タスクの実行種別として，次のどれかが表示されます。 • 操作ログのエクスポート • 管理項目定義のインポート • 管理項目定義のエクスポート
実行ユーザー	操作をしたユーザー名が表示されます。
タスク詳細	タスクの状態によって表示される内容が変わります。 • 実行待ち 中止ボタンが表示されます。 • 実行中と中止待ち 何も表示されません。 ただし，ユーザーの中止要求がタイムアウトした場合は，中止がタイムアウトした旨のメッセージが表示されます。 • 正常終了 実行結果の詳細が表示されます。 ・操作ログのエクスポート：出力した操作ログファイルをログ一覧画面からダウンロードできる旨のメッセージが表示されます。 ・管理項目定義のインポート：何も表示されません。 ・管理項目定義のエクスポート：管理項目定義エクスポートファイル（assetsfield_def.csv）のダウンロードリンクが表示されます。 • エラー エラーの詳細情報のリンクが表示されます。クリックすると詳細なエラーメッセージが表示されます。 • 中止待ち 何も表示されません。 • 中止

項目	説明
タスク詳細	ユーザーによって中止された旨のメッセージが表示されます。

注※1

「実行待ち」は，タスクがシステムに受け付けられたものの，実行可能になるまで待機している状態を示します。この状態のタスクだけが中止可能であり，中止ボタンが表示されます。

注※2

「実行中」のタスクは中止できません。

注※3

「実行待ち」のタスクに対して中止操作を実行すると，「中止待ち」のステータスになります。タスクの中止が受け付けられた旨のメッセージが表示され，最新の状態はタスク一覧画面で確認できます。

重要

タスク一覧画面には，サーバごとに直近 10 回分の操作結果が表示されます。例えば，JP1/ITDM2 サーバ（統括マネージャまたは中継マネージャ）を 3 台持つサービスの利用者の場合，最大 30 個のタスクが表示されます。

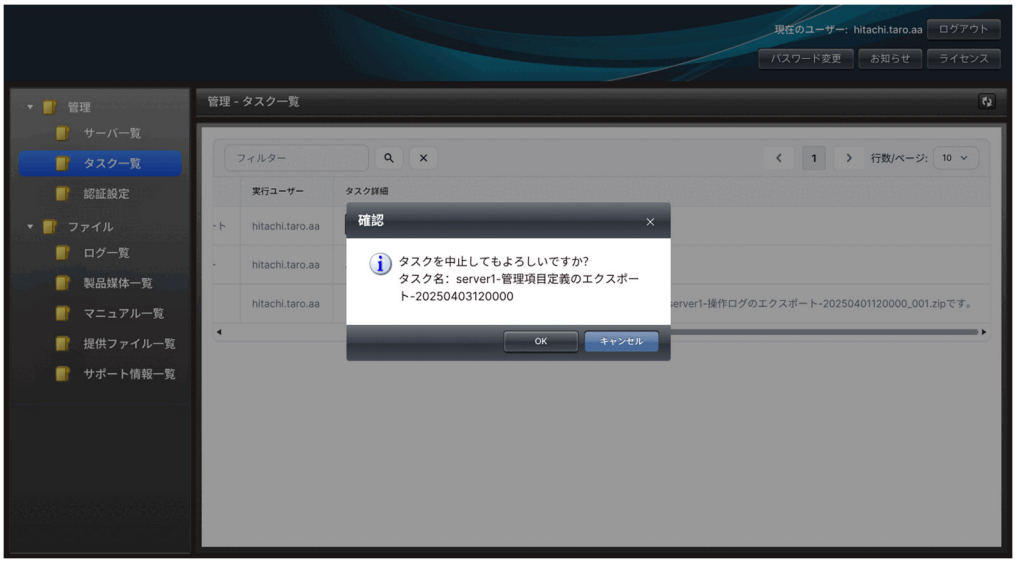
サーバ一覧画面からタスクを実行する際，対象サーバにすでに 10 個のタスクがある場合は，最も古いタスクが自動的に削除されます。また，そのタスクで出力した操作ログもログ一覧画面から削除されます。削除されたタスクは以後表示されません。

(1) タスクの中止

タスクのステータスが「実行待ち」の場合，タスクを中止することができます。

タスク一覧画面で中止したいタスクの「操作結果詳細」から［中止する］ボタンをクリックすると，タスク中止の確認ダイアログが表示されます。

- ［OK］ボタンをクリックすると，タスクの中止処理が開始され，ダイアログが閉じます。
- ［キャンセル］ボタンをクリックすると，タスクを中止しないでダイアログが閉じます。



重要

- タスクの中止はすぐに完了しないことがあります。その場合は，しばらくしてからタスク一覧のステータスでタスクの状態を確認してください。また，中止ボタンをクリックした際に，すでにタスクの実行が開始していることがあります。この場合は，タスクの実行がすでに開始されているため中止できなかった旨のメッセージが表示されます。
- 中止操作の受け付けは完了しましたが，タスクの実行が先に開始された場合もあります。この場合は，タスクの実行がすでに開始されているため中止できなかった旨のメッセージが表示されます。また，「実行待ち」のタスクに対して中止ボタンをクリックした際に，すでに他のユーザーが該当タスクに対し中止操作をしている場合があります。この場合も同様に受け付けのメッセージは表示されますが，ステータスの更新はされません。

(2)　注意事項

タスクの実行で出力されたファイルは，当該タスクを削除すると同時に削除されます。

そのため，ファイルをダウンロード中に他のユーザーが新しいタスクを実行するなどして，既存の出力ファイルが削除された場合，ダウンロードエラーが発生する可能性があります。

ダウンロードに失敗した場合は，該当のタスクを再度実行し，ファイルをエクスポートしてください。

4.3.7　認証設定の表示

認証設定では，サービスの利用者が，API 認証に関する設定を変更できます。スタンダードまたはライト A のプランを契約されている場合に利用できます。ライト B のプランを契約されている場合は，［再生成］ボタンは無効となり，「ご契約のプランでは使用できません。」と表示されます。

［管理］－［認証設定］をクリックすると API 認証用 Client Secret の再生成画面が表示されます。



［再生成］ボタンをクリックすると，確認ダイアログが表示されます。

- ［OK］ボタンをクリックすると，Client Secret の再生成が実行されます。
- ［キャンセル］ボタンをクリックすると，確認ダイアログを閉じます。

再生成が成功すると，Client ID および Client Secret が結果ダイアログに表示されます。



- Client ID および Client Secret はコピーできます。
- Client Secret は初期状態ではマスク表示され，表示／非表示を切り替えできます。
- 結果ダイアログを閉じると，再表示できないため，必要に応じて控えを取得してください。

重要

Client Secret を再生成すると，従来の Client Secret は即時無効になります。

認証情報を紛失した場合は，再度再生成を行ってください。

Client Secret の再生成には，再生成間隔を設けています。前回の再生成から一定時間が経過していない場合，再生成はできません。

4.3.8　ログの表示

サービスの利用者が参照できる操作ログと変更履歴をダウンロードできます。

変更履歴は，JP1/ITDM2 が出力する保存用の変更履歴である CSV ファイルを収集し，ZIP 形式に圧縮して提供されるファイルです。

変更履歴を出力するには，JP1/ITDM2 の設定画面で「変更履歴を取得する」を有効にしてください。この設定が無効の場合，変更履歴ファイルは出力されません。

変更履歴ファイルはサーバごとに 1 日単位で作成されます。ポータルシステムにはサーバごとの直近 180 日分の変更履歴ファイルが保存され，180 日を超えた古いファイルは自動的に削除されます。

［ファイル］－［ログ一覧］のログ一覧画面から，操作ログまたは変更履歴の内容表示およびダウンロードができます。



ログ一覧画面に表示する項目と説明を次に示します。

項目		説明
フィルタリング	フィルター	検索したい文字列を入力します。
	🔍	フィルターに入力した文字列で検索します。
	×	フィルター条件を解除します。

項目		説明
ページネーション	＜	表示している前のページが表示されます。
	n（ページ）	選択したページが表示されます。
	＞	表示している次のページが表示されます。
	表示行数	ログ一覧画面に表示される件数は，次のどれかから選択できます。 • 10 • 30 • 50 初期設定（デフォルト）は「10」です。
一括ダウンロード		［チェックボックス］で選択した操作ログまたは変更履歴を一括でダウンロードします。
［チェックボックス］		操作対象を示すチェックボックスです。
ログ名		JP1/ITDM2 の操作ログファイルまたは変更履歴のファイル名称が表示されます。ファイル名称のリンクをクリックすると，ダウンロードができます。 •「操作ログのエクスポート」で出力されたログファイル名称 *タスク名*※*_NNN*.zip 注※　*タスク名*：サーバ名-タスク種別-*YYYYMMDDHHmmss* • 上記以外のログファイル名称 oplog_*YYYYMMDD*-*yyyymmdd*_*NNN*.zip （注） *YYYYMMDD*：zip に含まれる操作ログの開始日 *yyyymmdd*：zip に含まれる操作ログの最終日 *YYYYMMDDHHmmss*：zip に含まれる操作ログのエクスポート日時 *NNN*：001～999 の連番 • 変更履歴の場合 *サーバ名*-変更履歴-*YYYYMMDD*.zip （注） *サーバ名*：変更履歴の出力元サーバ名 *YYYYMMDD*：出力元サーバで出力された年月日
登録日時		JP1/ITDM2 の操作ログまたは変更履歴の圧縮ファイルが登録された日時が「YYYY/MM/DD hh:mm:ss」形式で表示されます。
保管期限		操作ログをポータルシステムに保管する期限が「YYYY/MM/DD hh:mm:ss」形式で表示されます。 保管期限が過ぎると削除されます。 ただし，「操作ログのエクスポート」で出力されたログまたは変更履歴は，保管期限が適用されないため，「-」が表示されます。
サイズ		操作ログまたは変更履歴ファイルのサイズが「KB/MB/GB」の形式で表示されます。

(1)　一括ダウンロード

複数ログを選択し，一括ダウンロードできます。

最大選択件数は 50 件で，ページを切り替えると，選択状態はクリアされます。

ログ一覧画面で一括ダウンロードする操作ログまたは変更履歴を選択し，［一括ダウンロード］ボタンをクリックすると，一括ダウンロード確認ダイアログが表示されます。

- ［OK］ボタンをクリックすると，操作ログまたは変更履歴の一括ダウンロード処理が開始され，一括ダウンロードダイアログが表示されます。一括ダウンロードダイアログは，完了件数／合計件数，成功件数，失敗件数，処理中件数などが表示され，ダウンロードの進捗状況をお知らせします。
- ［キャンセル］ボタンをクリックすると，一括ダウンロード処理をしないでダイアログが閉じます。

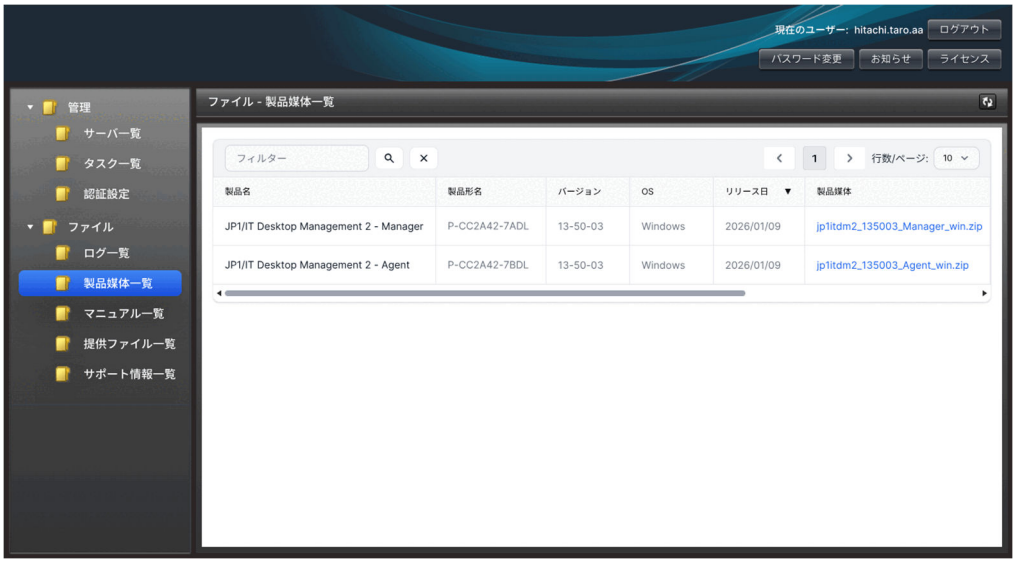


一括ダウンロード処理中，一括ダウンロードダイアログで［中止］ボタンをクリックすると，未開始のダウンロードについては中止ができます。ただし，すでに処理を開始したダウンロードは中止できません。

4.3.9　製品媒体一覧の表示

サービスの利用者が利用できる製品媒体に付属するドキュメント（リリースノートなど）が一覧で表示されます。

［ファイル］－［製品媒体］の製品媒体のファイル名をクリックすると，対象の製品媒体がダウンロードできます。また，ドキュメント名をクリックすると付属ドキュメント（リリースノートなど）をダウンロードできます。



製品媒体一覧画面に表示する項目と説明を次に示します。

項目		説明
フィルタリング	フィルター	検索したい文字列を入力します。
	🔍	フィルターに入力した文字列で検索します。
	×	フィルター条件を解除します。
ページネーション	＜	表示している前のページが表示されます。
	n（ページ）	選択したページが表示されます。
	＞	表示している次のページが表示されます。
	表示行数	製品媒体一覧画面に表示される件数は，次のどれかから選択できます。 • 10 • 30 • 50 初期設定（デフォルト）は「10」です。
製品名		製品媒体の製品名が表示されます。
製品形名		製品媒体の製品形名（媒体形名）が表示されます。
バージョン		製品媒体のバージョン番号が「VV-RR-SS」の形式で表示されます。
OS		製品媒体の対象 OS 名が表示されます。
リリース日		製品のリリース日が「YYYY/MM/DD」形式で表示されます。 日付はブラウザのタイムゾーンで表示されます。
製品媒体		製品媒体のファイル名が表示されます。 ファイル名のリンクをクリックすると，ファイルをダウンロードできます。
製品媒体のサイズ		製品媒体のファイルのサイズが「KB/MB/GB」の形式で表示されます。

項目	説明
ドキュメント	製品媒体に付属するドキュメントのファイル名が表示されます。 ファイル名のリンクをクリックすると，ファイルをダウンロードできます。
ドキュメントのサイズ	製品に付属するドキュメントのサイズが「KB/MB/GB」の形式で表示されます。

4.3.10　マニュアル一覧の表示

サービスの利用者が利用できるサービスに関連する製品マニュアル，取扱説明書，利用ガイドなどのマニュアルドキュメントが表示されます。

［ファイル］－［マニュアル一覧］から，マニュアル名称をクリックするとダウンロードできます。



マニュアル一覧画面に表示する項目と説明を次に示します。

項目		説明
フィルタリング	フィルター	検索したい文字列を入力します。
	🔍	フィルターに入力した文字列で検索します。
	×	フィルター条件を解除します。
ページネーション	＜	表示している前のページが表示されます。
	n（ページ）	選択したページが表示されます。
	＞	表示している次のページが表示されます。
	表示行数	マニュアル一覧画面に表示される件数は，次のどれかから選択できます。

項目		説明
ページネーション	表示行数	• 10 • 30 • 50 初期設定（デフォルト）は「10」です。
マニュアル名称		マニュアル名が表示されます。 ファイル名のリンクをクリックすると，ファイルをダウンロードできます。
資料番号		マニュアルの資料番号が表示されます。
サイズ		マニュアルのファイルサイズが「KB/MB/GB」の形式で表示されます。

4.3.11　提供ファイル一覧の表示

サービスの利用者が利用できるサービスに関連する設定ファイルやツールなどのファイルが一覧で表示されます。

［ファイル］－［提供ファイル一覧］から，ファイル名をクリックするとダウンロードできます。



提供ファイル一覧画面に表示する項目と説明を次に示します。

項目		説明
フィルタリング	フィルター	検索したい文字列を入力します。
	🔍	フィルターに入力した文字列で検索します。
	×	フィルター条件を解除します。
ページネーション	＜	表示している前のページが表示されます。

項目		説明
ページネーション	n（ページ）	選択したページが表示されます。
	＞	表示している次のページが表示されます。
	表示行数	提供ファイル一覧画面に表示される件数は，次のどれかから選択できます。 • 10 • 30 • 50 初期設定（デフォルト）は「10」です。
ファイル名		ファイル名が表示されます。 ファイル名のリンクをクリックすると，ファイルをダウンロードできます。
説明		提供ファイルの説明が表示されます。
最終更新日時		提供ファイルの最終更新日時（リリースの日時）を「YYYY/MM/DD hh:mm:ss」形式で表示されます。
サイズ		提供ファイルサイズが「KB/MB/GB」の形式で表示されます。

4.3.12　サポート情報一覧の表示

サービスの障害回避・予防に関する情報や注意喚起情報などのサポート情報が一覧で表示されます。

［サポート］－［サポート情報一覧］から，ファイル名をクリックすると当該サポート情報のファイルをダウンロードできます。



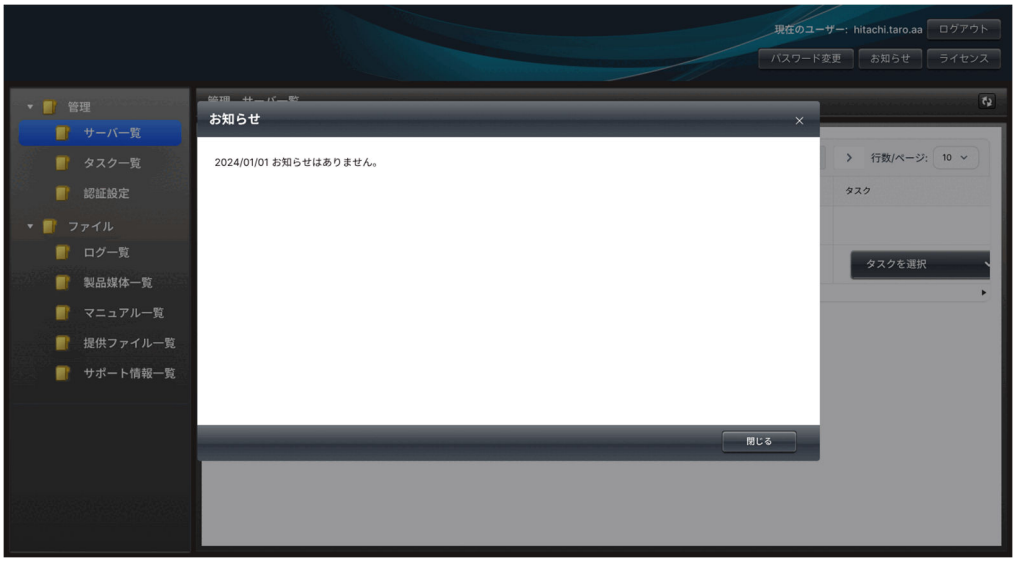
サポート情報一覧画面に表示する項目と説明を次に示します。

項目		説明
フィルタリング	フィルター	検索したい文字列を入力します。
		フィルターに入力した文字列で検索します。
	×	フィルター条件を解除します。
ページネーション	＜	表示している前のページが表示されます。
	n（ページ）	選択したページが表示されます。
	＞	表示している次のページが表示されます。
	表示行数	サポート情報一覧画面に表示される件数は，次のどれかから選択できます。 • 10 • 30 • 50 初期設定（デフォルト）は「10」です。
最終更新日		サポート情報の最終更新日が「YYYY/MM/DD」形式で表示されます。日付はブラウザのタイムゾーンで表示されます。
タイトル		サポート情報のタイトルが表示されます。 タイトルのリンクをクリックすると，当該サポート情報のファイルをダウンロードできます。
製品		サポート情報の対象製品が表示されます。
重要度		サポート情報の重要度が次のどれかで表示されます。 • **AAA** 発生頻度が高く，業務システムの運用が停止する。 • **AA** 業務システムの運用が停止する可能性がある。 • **A** 業務システムの運用が停止する可能性は低い。 • **B** 業務システムの運用に与える影響が少ない。 • **C** 業務システムの運用に与える影響はほとんどない。 • **-** 特になし（予防保守情報や使用時の注意事項など）
公開日		サポート情報が最初に公開された日が「YYYY/MM/DD」形式で表示されます。日付はブラウザのタイムゾーンで表示されます。

4.3.13　お知らせの表示

システムメンテナンスによるサービス停止など，サービス提供元からのお知らせを表示できます。

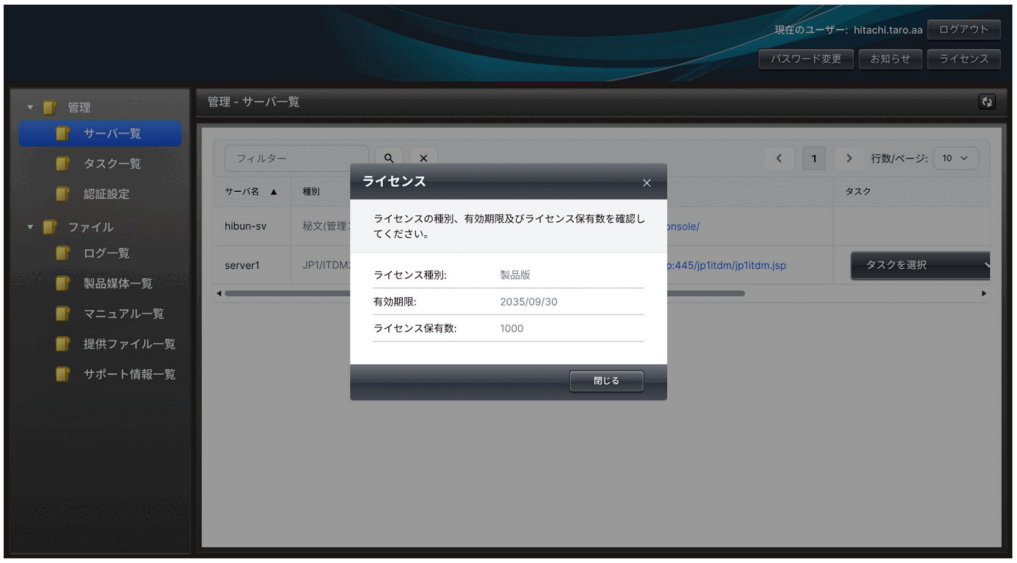
お知らせ画面は，メイン画面右上の［お知らせ］ボタンをクリックすると表示されます。



4.3.14　ライセンス情報の表示

運用管理者は契約しているライセンス情報の確認ができます。

ライセンス情報画面は，メイン画面右上の［ライセンス］ボタンをクリックすると表示されます。



ライセンス情報画面に表示する項目と説明を次に示します。

項目	説明
ライセンス種別	ライセンスの種別が次のどちらかで表示されます。 製品版 　契約しているライセンスが製品版（正規版）であることを示します。

項目	説明
ライセンス種別	評価版 　契約しているライセンスが評価版であることを示します。
有効期限	当該ライセンスでサービスを利用できる有効期限（利用終了日）が「YYYY/MM/DD」形式で表示されます。 日付はブラウザのタイムゾーンで表示されます。
ライセンス保有数	ライセンスで管理できるクライアントの上限数が表示されます。

5 API リファレンス

この章では，エンドポイント管理のポータルシステムが提供する API について説明します。

なお，API は対象ライセンスの契約プランがスタンダードまたはライト A の場合に利用できます。

5.1　API 一覧

エンドポイント管理のポータルシステムが提供する API 一覧を次の表に示します。

表 5–1　API 一覧

機能	説明
パッケージのインストール API	対象の JP1/ITDM2 サーバに対して「パッケージのインストール」タスクを実行します。
クライアントユーザによるインストール API	対象の JP1/ITDM2 サーバに対して「クライアントユーザによるインストール」タスクを実行します。
ジョブの実行 API	対象の JP1/ITDM2 サーバに対して「ジョブの実行」タスクを実行します。
ジョブの削除 API	対象の JP1/ITDM2 サーバに対して「ジョブの削除」タスクを実行します。
ジョブ定義の削除 API	対象の JP1/ITDM2 サーバに対して「ジョブ定義の削除」タスクを実行します。
タスク実行状態の取得 API（サーバ名指定）	指定したサーバに実行したすべてのタスクの実行状態を取得します。
タスク実行状態の取得 API（タスク ID 指定）	指定したタスクの実行状態を取得します。

5.2 API 共通仕様

エンドポイント管理のポータルシステムが提供している API に共通する仕様について説明します。

このシステムは REST 形式の Web API を提供します。

通信プロトコルには HTTPS を使用します。

API のリクエストおよびレスポンスデータは JSON 形式とし，文字コードは UTF-8 を使用します。

5.2.1 認証方式

この API は，HTTP Basic 認証を使用します。

API を利用するには，事前にポータルの認証設定画面で Client Secret を再生成し，表示された Client ID および Client Secret を取得してください。

API の呼び出し時は，Client ID と Client Secret を「clientId:clientSecret」の形式で連結して Base64 エンコードし，その値を Authorization ヘッダーに設定します。

なお，API はステートレスであり，サーバ側でセッション情報を保持しません。そのため，すべてのリクエストに Authorization ヘッダーを設定する必要があります。

5.2.2 API 利用時の注意事項

API 利用時の注意事項について説明します。

(1) タスクの同時実行について

タスクの実行方法には，サーバ一覧画面から実行する方法と API で実行する方法があります。

タスクの実行方法やタスク種別にかかわらず，同一サーバに対して同時に実行できるタスクは 1 件だけです。実行中のタスクがある場合は，同一サーバに対して他のタスクを実行できません。

(2) タスク情報の保持について

API で実行したタスクの情報は，サーバごとに 100 件まで保持されます。

保持件数が上限に達した場合は，新しいタスクの実行時に古いタスクから順に削除されます。

(3) 認証情報の管理について

API を利用するための Client ID および Client Secret は，お客さまのシステムから API を呼び出す際に使用する認証情報です。

これらの認証情報の管理および保管は，お客さまの責任において実施してください。取り扱いにあたっては，漏えいや不正利用を防止するため，十分に注意のうえ適切に管理してください。

特に，次の点に注意してください。

- 認証情報を第三者に開示しないこと
- 認証情報をソースコードなどに直接記載しないこと
- 不正アクセスを防止できる適切な管理方法により保護すること

万一，漏えいや不正利用の可能性がある場合は，速やかにポータルシステムの認証設定画面から Client Secret を再生成し，設定を更新してください。

(4)　レート制限について

このサービスでは，システムの安定稼働およびセキュリティ確保のため，API に対して一定時間あたりのリクエスト数に制限を設けています。

短時間に多数のリクエストを送信した場合，一時的にアクセスが制限され，HTTP ステータスコード 429（Too Many Requests）が返されることがあります。

レート制限が発生した場合は，一定時間待機したあとに再実行してください。

5.2.3　リクエスト形式

リクエスト形式は，リクエスト行，リクエストヘッダー，およびリクエストのメッセージボディで構成されます。リクエスト行およびリクエストヘッダーは ASCII 文字を指定します。URL で使用できない文字を指定する場合は，URL エンコードが必要です。

形式

```
method https://portal.epm.hitachi-solutions.co.jp/api/v1/resource/other?query HTTP/1.1
Content-Type: application/json
Authorization: Basic Base64エンコードしたclientId:clientSecret

messageBody
```

リクエスト形式の構成内容について，次の表で説明します。

表 5–2　リクエスト形式の構成内容

項目		区分	説明
リクエスト行	method	必須	メソッドを指定します。次のどれかを指定します。 • GET • POST • PUT

項目			区分	説明
リクエスト行		method	必須	• DELETE 指定できるメソッドは API によって異なります。詳細は各 API の説明を参照してください。
		resource	必須	リソースを指定します。指定するリソースは API によって異なります。詳細は各 API の説明を参照してください。
		other	任意	必要に応じて，リソースまたはリソースの操作を一意に識別できる値を指定します。詳細は各 API の説明を参照してください。
		query	任意	必要に応じて，クエリ文字列を指定します。詳細は各 API の説明を参照してください。
リクエストヘッダー	Content-Type	application/json	※	必ず「application/json」を指定します。
	Authorization	Basic Base64 エンコードした clientId:clientSecret	必須	Base64 エンコードした clientId:clientSecret には，認証設定画面から取得した Client ID と Client Secret を，「clientId:clientSecret」の形で Base64 エンコードした文字列を指定します。
リクエストのメッセージボディ		messageBody	任意	必要に応じて，JSON 形式で指定します。詳細は各 API の説明を参照してください。

注※

- method が「GET」の場合
  指定不要
- 上記以外の場合
  必須

5.2.4　レスポンス形式

リクエストに対するレスポンス形式は，ステータス行，レスポンスヘッダー，およびレスポンスのメッセージボディで構成されます。ステータス行およびレスポンスヘッダーは ASCII 文字を指定します。

形式

```
HTTP/1.1 statusCode statusCodeText
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: camera=(), microphone=(), geolocation=()
Cache-Control: private, no-store, no-cache, must-revalidate
Content-Type: application/json

messageBody
```

レスポンス形式の構成内容について，次の表で説明します。

表 5–3　レスポンス形式の構成内容

項目			説明
ステータス行		statusCode	ステータスコードが格納されます。詳細は「5.2.5　ステータスコード」を参照してください。
		statusCodeText	ステータスコードのテキストが格納されます。詳細は「5.2.5 ステータスコード」を参照してください。
レスポンスヘッダー	X-Frame-Options	DENY	必ず「DENY」が返却されます。
	X-Content-Type-Options	nosniff	必ず「nosniff」が返却されます。
	X-XSS-Protection	1; mode=block	必ず「1; mode=block」が返却されます。
	Referrer-Policy	strict-origin-when-cross-origin	必ず「strict-origin-when-cross-origin」が返却されます。
	Permissions-Policy	camera=(), microphone=(), geolocation=()	必ず「camera=(), microphone=(), geolocation=()」が返却されます。
	Cache-Control	private, no-store, no-cache, must-revalidate	必ず「private, no-store, no-cache, must-revalidate」が返却されます。
	Content-Type	application/json	必ず「application/json」が返却されます。
レスポンスのメッセージボディ		messageBody	API が呼び出された時に返却されるレスポンスデータが，JSON 形式で格納されます。詳細は各 API の説明を参照してください。 また，エラーが発生した場合は，エラー情報が JSON 形式で格納されます。詳細は「5.2.6　エラー情報」を参照してください。

5.2.5　ステータスコード

API 実行によって返却されるレスポンスメッセージのステータスコードを次の表に示します。

表 5–4　レスポンスメッセージのステータスコード

ステータスコード	ステータスコードのテキスト	説明
200	OK	正常終了しました。
201	Created	タスクの処理時間が 1 回のリクエストの応答時間上限を超えました。タスク実行状態の取得 API（サーバ名指定またはタスク ID 指定）で進捗や結果を確認してください。
400	Bad Request	リクエスト情報が不正です。
401	Unauthorized	認証に失敗しました。

ステータスコード	ステータスコードのテキスト	説明
403	Forbidden	ライセンスが利用不可，または契約プランが API をサポートしていません。
404	Not Found	対象サーバまたは対象タスクが見つかりません。
409	Conflict	対象サーバで別のタスクが実行中のため，新規タスクを開始できません。
413	Content Too Large	リクエストのメッセージボディが大きすぎます。
415	Unsupported Media Type	GET 以外の API で Content-Type: application/json が設定されていないか，値が不正です。
429	Too Many Requests	短時間に多数のリクエストが送信されたため，一時的にアクセスが制限されました。
500	Internal Server Error	サーバ内部エラーが発生しました。

5.2.6　エラー情報

API のリクエストがエラーになった場合，エラー情報がレスポンスのメッセージボディに JSON 形式で格納されて返却されます。エラー情報の形式を次に示します。

形式

```
{
  "error": {
    "code": "エラーコード",
    "message": "エラーメッセージ"
  }
}
```

属性		データ型	説明
error		オブジェクト	エラー情報のオブジェクト
	code	文字列	エラーコード
	message	文字列	エラーメッセージ

主なエラーコードと対処方法を次の表に示します。

表 5–5　エラーコードと対処方法

ステータス	コード	内容	対処
400	EMER0001	パラメタファイル形式不正	Shift-JIS 形式であることを確認してください。
	EMER0002	ファイルサイズ超過	ファイルサイズを 100KB 以内に調整してください。
	EMER0003	必須パラメタ不足／値不正	リクエスト内容を確認してください。

ステータス	コード	内容	対処
400	EMER0004	サーバ種別不正	JP1/ITDM2 のマネージャサーバを指定してください。
401	EMER0005	認証失敗	Authorization ヘッダーに設定した Client ID または Client Secret を確認してください。
403	EMER0006	ライセンス無効	ライセンスの状態を確認してください。
	EMER0007	非対応プラン	契約プランを確認してください。
404	EMER0008	サーバが存在しない	サーバ名を確認してください。
	EMER0009	タスクが存在しない	タスク ID を確認してください。
409	EMER0010	サーバ実行中	時間をおいて再度実行してください。
413	EMER0011	リクエストサイズ超過	リクエストのサイズを減らしてください。
415	EMER0015	Content-Type 不正	Content-Type に application/json を指定してください。
500	EMER0012	内部エラー	時間をおいて再度実行してください。

次のコードはエラーではありませんが，エラー情報が返却されます。

表 5–6　処理時間超過時のエラーコードと対処方法

ステータス	コード	内容	対処
201	EMER0014	処理時間超過により受付のみ完了（処理は継続）	タスク実行状態の取得 API（サーバ名指定またはタスク ID 指定）で進捗状況や実行結果を確認してください。

出力例

認証情報不正で認証失敗の場合のレスポンス

```
HTTP/1.1 401 Unauthorized
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: camera=(), microphone=(), geolocation=()
Cache-Control: private, no-store, no-cache, must-revalidate
Content-Type: application/json

{
  "error": {
    "code": "EMER0005",
    "message": "認証に失敗しました。Client IDまたはClient Secretが正しくありません。"
  }
}
```

5.3 API の詳細

エンドポイント管理のポータルシステムが提供している各 API で説明する項目を次に示します。ただし，API によっては説明の無い項目もあります。

形式

API のリクエスト形式およびレスポンス形式について説明します。

パラメタ

リクエストのメッセージボディに指定するパラメタについて説明します。

戻り値

API が返却する戻り値の情報について説明します。

使用例

API を使用するためのリクエスト例およびレスポンス例について説明します。

5.3.1 パッケージのインストール API

「パッケージのインストール」タスクを実行します。「パッケージのインストール」タスクは，対象サーバでリモートインストールマネージャを使用した配布機能のコマンドである dcminst コマンドを実行し，パッケージのインストールジョブを作成，実行します。

dcminst コマンドの機能やパラメタについては，マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の「dcminst.exe（ジョブの作成、実行）」を参照してください。

形式

リクエスト行

```
POST https://portal.epm.hitachi-solutions.co.jp/api/v1/distribution-jobs/package-install
HTTP/1.1
```

リクエストのメッセージボディ

```
{
  "serverName": "サーバ名",
  "parameters1": "Base64エンコードした文字列",
  "parameters2": "Base64エンコードした文字列",
  "overwritePackage": true | false,
  "saveOnly": true | false
}
```

パラメタ

リクエストのメッセージボディに指定するパラメタを次の表に示します。

表 5–7　リクエストのメッセージボディの構成内容

パラメタ	型	区分	説明
serverName	文字列	必須	対象サーバ名を指定します。 サーバ一覧画面の JP1/ITDM2 のサーバ名を指定してください。
parameters1	文字列	必須	dcminst コマンドに指定するパラメタファイル 1 の内容を Base64 エンコードした文字列を指定します。
parameters2	文字列	任意	dcminst コマンドに指定するパラメタファイル 2 の内容を Base64 エンコードした文字列を指定します。
overwritePackage	ブール	任意	dcminst コマンドの/f オプション（パッケージを上書きインストールするかどうか）を指定します。 • true：上書きインストールする • false：上書きインストールしない（省略時のデフォルト）
saveOnly	ブール	任意	dcminst コマンドの/s オプション（ジョブを作成後，実行しないで保存するかどうか）を指定します。 • true：実行しないで保存 • false：実行する（省略時のデフォルト）

重要

パラメタファイルに多数のあて先やパッケージを指定すると，コマンドの実行時間が非常に長くなる可能性があります。（大量のあて先が含まれるあて先グループを指定するなど）

それにより，次のような問題が発生することがあります。

- タスクの処理時間が長くなる
- タスクがタイムアウトし，エラーとなる
- 一度開始したタスクは途中で中止できないため，タイムアウトまでの間，対象サーバで他のタスクを実行できなくなる

タイムアウトが発生した場合は，一度に指定するあて先やパッケージを減らして実行してください。

戻り値

ステータスコードが 200 および 201 の場合に，レスポンスボディに次の情報を返却します。リクエストの処理でエラーが発生した場合は，エラー情報が JSON 形式で返却されます。

表 5–8　レスポンスのメッセージボディの構成内容

パラメタ	型	区分	説明
taskId	文字列	必須	API の呼び出しによって作成されたタスクのタスク ID
taskType	文字列	必須	タスク種別
status	文字列	必須	タスクステータス

パラメタ	型	区分	説明
status	文字列	必須	次のどれかが返却されます。 • QUEUED：実行待ち • RUNNING：実行中 • COMPLETED_SUCCESS：正常終了 • COMPLETED_ERROR：エラー
submittedAt	日時	必須	タスク作成日時（UTC）
startedAt	日時	必須	タスク開始日時（UTC） 未開始の場合は null が返却されます。
endedAt	日時	必須	タスク終了日時（UTC） 未終了の場合は null が返却されます。
targetServerName	文字列	必須	対象サーバ名
resultMessage	文字列	必須	結果メッセージ 正常終了時，エラー時，または受付完了時のメッセージが返却されます。
outputFile	文字列	任意※	結果出力ファイルの内容を Base64 エンコードした文字列 正常終了し，結果出力ファイルが出力された場合に返却されます。
errorCode	文字列	任意※	タスクがエラーになった場合のエラーコード

注※

任意の項目は条件に応じて返却されます。条件に該当しない場合は，項目自体が返却されないことがあります。

使用例

リクエストの例

```
POST https://portal.epm.hitachi-solutions.co.jp/api/v1/distribution-jobs/package-install
HTTP/1.1
Content-Type: application/json
Authorization: Basic Y2xpZW50SWQ6Y2xpZW50U2VjcmV0

{
  "serverName": "server1",
  "parameters1": "44OR44Op44Oh44K/44OV44Kh44Kk44OrMQ==",
  "overwritePackage": false,
  "saveOnly": false
}
```

レスポンス（メッセージボディ）の例

```
{
  "taskId": "b706152b-6321-47fa-a617-f78bc4ab2393",
  "taskType": "PACKAGE_INSTALL",
  "status": "COMPLETED_SUCCESS",
  "submittedAt": "2026-01-15T10:30:00.000Z",
  "startedAt": "2026-01-15T10:30:05.000Z",
  "endedAt": "2026-01-15T10:32:15.000Z",
  "targetServerName": "server1",
  "resultMessage": "タスクが正常終了しました。",
```

```
  "outputFile": "b3V0cHV0RmlsZQ=="
}
```

補足事項

201（EMER0014）が返却された場合，タスクはバックグラウンドで継続中です。タスク実行状態の取得 API（サーバ名指定またはタスク ID 指定）で結果を確認してください。

5.3.2　クライアントユーザによるインストール API

「クライアントユーザによるインストール」タスクを実行します。「クライアントユーザによるインストール」タスクは，対象サーバでリモートインストールマネージャを使用した配布機能のコマンドである dcminst コマンドを実行し，クライアントユーザによるインストールジョブを作成，実行します。

dcminst コマンドの機能やパラメタについては，マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の「dcminst.exe（ジョブの作成、実行）」を参照してください。

形式

リクエスト行

```
POST https://portal.epm.hitachi-solutions.co.jp/api/v1/distribution-jobs/client-user-install HTTP/1.1
```

リクエストのメッセージボディ

リクエストのメッセージボディは，パッケージのインストール API と同じです。「表 5-7　リクエストのメッセージボディの構成内容」を参照してください。

戻り値

ステータスコードが 200 および 201 の場合に，レスポンスボディに情報を返却します。リクエストの処理でエラーが発生した場合は，エラー情報が JSON 形式で返却されます。

レスポンスボディは，パッケージのインストール API と同じです。「表 5-8　レスポンスのメッセージボディの構成内容」を参照してください。

正常時は，タスク情報が JSON 形式で返却されます。処理が 180 秒以内に完了しない場合は，201 Created（EMER0014）で受付完了を返却することがあります。

使用例

リクエストの例

```
POST https://portal.epm.hitachi-solutions.co.jp/api/v1/distribution-jobs/client-user-install HTTP/1.1
Content-Type: application/json
Authorization: Basic Y2xpZW50SWQ6Y2xpZW50U2VjcmV0

{
  "serverName": "server1",
  "parameters1": "44OR44Op44Oh44K/44OV44Kh44Kk44OrMQ==",
  "parameters2": "44OR44Op44Oh44K/44OV44Kh44Kk44OrMg==",
  "overwritePackage": true,
```

```
  "saveOnly": false
}
```

レスポンス（メッセージボディ）の例

```
{
  "taskId": "610e6388-554a-4274-a782-2dc02e1299f9",
  "taskType": "CLIENT_USER_INSTALL",
  "status": "RUNNING",
  "submittedAt": "2026-01-15T10:35:00.000Z",
  "startedAt": "2026-01-15T10:35:10.000Z",
  "endedAt": null,
  "targetServerName": "server1",
  "resultMessage": "タスクの実行を受け付けました。タスクはバックグラウンドで実行中です。"
,
  "errorCode": "EMER0014"
}
```

補足事項

201（EMER0014）が返却された場合，タスクはバックグラウンドで継続中です。タスク実行状態の取得 API（サーバ名指定またはタスク ID 指定）で結果を確認してください。

5.3.3　ジョブの実行 API

「ジョブの実行」タスクを実行します。「ジョブの実行」タスクは，対象サーバでリモートインストールマネージャを使用した配布機能のコマンドである dcmjexe コマンドを実行します。

dcmjexe コマンドの機能やパラメタについては，マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の「dcmjexe.exe（ジョブの実行）」を参照してください。

形式

リクエスト行

```
POST https://portal.epm.hitachi-solutions.co.jp/api/v1/distribution-jobs/job-execute HTTP
/1.1
```

リクエストのメッセージボディ

```
{
  "serverName": "サーバ名",
  "parameters": "Base64エンコードした文字列"
}
```

パラメタ

リクエストのメッセージボディに指定するパラメタを次の表に示します。

表 5–9　リクエストのメッセージボディの構成内容

パラメタ	型	区分	説明
serverName	文字列	必須	対象サーバ名を指定します。

パラメタ	型	区分	説明
serverName	文字列	必須	サーバ一覧画面の JP1/ITDM2 のサーバ名を指定してください。
parameters	文字列	必須	dcmjexe コマンドに指定するパラメタファイルの内容を Base64 エンコードした文字列を指定します。

戻り値

ステータスコードが 200 および 201 の場合に，レスポンスボディに情報を返却します。リクエストの処理でエラーが発生した場合は，エラー情報が JSON 形式で返却されます。

レスポンスボディは，パッケージのインストール API と同じです。「表 5-8　レスポンスのメッセージボディの構成内容」を参照してください。

正常時は，タスク情報が JSON 形式で返却されます。処理が 180 秒以内に完了しない場合は，201 Created（EMER0014）で受付完了を返却することがあります。

使用例

リクエストの例

```
POST https://portal.epm.hitachi-solutions.co.jp/api/v1/distribution-jobs/job-execute HTTP
/1.1
Content-Type: application/json
Authorization: Basic Y2xpZW50SWQ6Y2xpZW50U2VjcmV0

{
  "serverName": "server1",
  "parameters": "44OR44Op44Oh44K/44OV44Kh44Kk44Or"
}
```

レスポンス（メッセージボディ）の例

```
{
  "taskId": "b706152b-6321-47fa-a617-f78bc4ab2393",
  "taskType": "JOB_EXECUTE",
  "status": "COMPLETED_SUCCESS",
  "submittedAt": "2026-01-15T10:30:00.000Z",
  "startedAt": "2026-01-15T10:30:05.000Z",
  "endedAt": "2026-01-15T10:32:15.000Z",
  "targetServerName": "server1",
  "resultMessage": "タスクが正常終了しました。",
  "outputFile": "b3V0cHV0RmlsZQ=="
}
```

補足事項

201（EMER0014）が返却された場合，タスクはバックグラウンドで継続中です。タスク実行状態の取得 API（サーバ名指定またはタスク ID 指定）で結果を確認してください。

5.3.4　ジョブの削除 API

「ジョブの削除」タスクを実行します。「ジョブの削除」タスクは，対象サーバでリモートインストールマネージャを使用した配布機能のコマンドである dcmjbrm コマンドを実行します。

dcmjbrm コマンドの機能やパラメタについては，マニュアル「JP1/IT Desktop Management 2 配布機能 運用ガイド」の「dcmjbrm.exe（ジョブの削除）」を参照してください。

形式

リクエスト行

```
POST https://portal.epm.hitachi-solutions.co.jp/api/v1/distribution-jobs/job-delete HTTP/1.1
```

リクエストのメッセージボディ

```
{
  "serverName": "サーバ名",
  "parameters": "Base64エンコードした文字列"
}
```

パラメタ

リクエストのメッセージボディに指定するパラメタを次の表に示します。

表 5–10　リクエストのメッセージボディの構成内容

パラメタ	型	区分	説明
serverName	文字列	必須	対象サーバ名を指定します。 サーバ一覧画面の JP1/ITDM2 のサーバ名を指定してください。
parameters	文字列	必須	dcmjbrm コマンドに指定するパラメタファイルの内容を Base64 エンコードした文字列を指定します。

戻り値

ステータスコードが 200 および 201 の場合に，レスポンスボディに情報を返却します。リクエストの処理でエラーが発生した場合は，エラー情報が JSON 形式で返却されます。

レスポンスボディは，パッケージのインストール API と同じです。「表 5-8　レスポンスのメッセージボディの構成内容」を参照してください。

正常時は，タスク情報が JSON 形式で返却されます。処理が 180 秒以内に完了しない場合は，201 Created（EMER0014）で受付完了を返却することがあります。

使用例

リクエストの例

```
POST https://portal.epm.hitachi-solutions.co.jp/api/v1/distribution-jobs/job-delete HTTP/1.1
Content-Type: application/json
Authorization: Basic Y2xpZW50SWQ6Y2xpZW50U2VjcmV0

{
  "serverName": "server1",
  "parameters": "440R440p440h44K/440V44Kh44Kk440r"
}
```

レスポンス（メッセージボディ）の例

```
{
  "taskId": "0c6f5117-e247-4d3b-9f52-1bdda2c0c3ad",
  "taskType": "JOB_DELETE",
  "status": "COMPLETED_SUCCESS",
  "submittedAt": "2026-01-20T02:00:00.000Z",
  "startedAt": "2026-01-20T02:00:04.000Z",
  "endedAt": "2026-01-20T02:00:11.000Z",
  "targetServerName": "server1",
  "resultMessage": "タスクが正常終了しました。"
}
```

補足事項

201（EMER0014）が返却された場合，タスクはバックグラウンドで継続中です。タスク実行状態の取得 API（サーバ名指定またはタスク ID 指定）で結果を確認してください。

5.3.5　ジョブ定義の削除 API

「ジョブ定義の削除」タスクを実行します。「ジョブ定義の削除」タスクは，対象サーバでリモートインストールマネージャを使用した配布機能のコマンドである dcmrmgen コマンドを実行します。

dcmrmgen コマンドの機能やパラメタについては，マニュアル「JP1/IT Desktop Management 2 配布機能運用ガイド」の「dcmrmgen.exe（ジョブ定義の削除）」を参照してください。

形式

リクエスト行

```
POST https://portal.epm.hitachi-solutions.co.jp/api/v1/distribution-jobs/job-def-delete HTTP/1.1
```

リクエストのメッセージボディ

```
{
  "serverName": "サーバ名",
  "parameters": "Base64エンコードした文字列"
}
```

パラメタ

リクエストのメッセージボディに指定するパラメタを次の表に示します。

表 5–11　リクエストのメッセージボディの構成内容

パラメタ	型	区分	説明
serverName	文字列	必須	対象サーバ名を指定します。 サーバ一覧画面の JP1/ITDM2 のサーバ名を指定してください。
parameters	文字列	必須	dcmrmgen コマンドに指定するパラメタファイルの内容を Base64 エンコードした文字列を指定します。

戻り値

ステータスコードが 200 および 201 の場合に，レスポンスボディに情報を返却します。リクエストの処理でエラーが発生した場合は，エラー情報が JSON 形式で返却されます。

レスポンスボディは，パッケージのインストール API と同じです。「表 5-8　レスポンスのメッセージボディの構成内容」を参照してください。

正常時は，タスク情報が JSON 形式で返却されます。処理が 180 秒以内に完了しない場合は，201 Created（EMER0014）で受付完了を返却することがあります。

使用例

リクエストの例

```
POST https://portal.epm.hitachi-solutions.co.jp/api/v1/distribution-jobs/job-def-delete H
TTP/1.1
Content-Type: application/json
Authorization: Basic Y2xpZW50SWQ6Y2xpZW50U2VjcmV0

{
  "serverName": "server1",
  "parameters": "44OR44Op44Oh44K/44OV44Kh44Kk44Or"
}
```

レスポンス（メッセージボディ）の例

```
{
  "taskId": "0c6f5117-e247-4d3b-9f52-1bdda2c0c3ad",
  "taskType": "JOB_DEF_DELETE",
  "status": "COMPLETED_SUCCESS",
  "submittedAt": "2026-01-20T02:00:00.000Z",
  "startedAt": "2026-01-20T02:00:04.000Z",
  "endedAt": "2026-01-20T02:00:11.000Z",
  "targetServerName": "server1",
  "resultMessage": "タスクが正常終了しました。"
}
```

補足事項

201（EMER0014）が返却された場合，タスクはバックグラウンドで継続中です。タスク実行状態の取得 API（サーバ名指定またはタスク ID 指定）で結果を確認してください。

5.3.6　タスク実行状態の取得 API（サーバ名指定）

指定したサーバに実行したすべてのタスクの実行状態を一覧情報として取得します。API で実行したタスクだけが対象です。

ソート項目，ソート順を指定することができます。

形式

リクエスト行

```
GET https://portal.epm.hitachi-solutions.co.jp/api/v1/tasks?server=server&sort=sort&order
=order HTTP/1.1
```

リクエストのメッセージボディ

なし

パラメタ

リクエスト行のパラメタに指定する検索条件を次の表に示します。

表 5–12　パラメタに指定する検索条件

パラメタ	型	区分	説明
server	文字列	必須	一覧情報を取得する対象サーバのサーバ名 サーバ一覧画面の JP1/ITDM2 のサーバ名を指定してください。
sort	文字列	任意	ソート項目 このパラメタを第 1 ソート条件とし，タスク名の昇順を第 2 ソート条件として検索されます。 指定できる値は次のとおりです。 • id：タスク ID • taskType：タスク種別 • status：タスクステータス • submittedAt：タスク作成日時 • startedAt：タスク開始日時 • endedAt：タスク終了日時 省略した場合は startedAt が設定されます。 なお，文字列項目のソート順は Unicode 順です。
order	文字列	任意	ソート順 指定できる値は次のとおりです。 • asc：昇順 • desc：降順 省略した場合は desc が設定されます。

戻り値

ステータスコードが 200 の場合に，レスポンスボディに次の情報を返却します。リクエストの処理でエラーが発生した場合は，エラー情報が JSON 形式で返却されます。

表 5–13　レスポンスのメッセージボディの構成内容

パラメタ		型	区分	説明
data		配列	必須	取得した複数件のタスク情報配列 タスクごとに 1 つのオブジェクトの配列で返却されます。
	taskId	文字列	必須	タスク ID
	taskType	文字列	必須	タスク種別 次のどれかが返却されます。

パラメタ		型	区分	説明
	taskType	文字列	必須	• PACKAGE_INSTALL：パッケージのインストール • CLIENT_USER_INSTALL：クライアントユーザによるインストール • JOB_EXECUTE：ジョブの実行 • JOB_DELETE：ジョブの削除 • JOB_DEF_DELETE：ジョブ定義の削除
	status	文字列	必須	タスクステータス 次のどれかが返却されます。 • QUEUED：実行待ち • RUNNING：実行中 • COMPLETED_SUCCESS：正常終了 • COMPLETED_ERROR：エラー
	submittedAt	日時	必須	タスク作成日時（UTC）
	startedAt	日時	必須	タスク開始日時（UTC） 未開始の場合は null が返却されます。
	endedAt	日時	必須	タスク終了日時（UTC） 未終了の場合は null が返却されます。
	targetServerName	文字列	必須	対象サーバ名
	resultMessage	文字列	必須	結果メッセージ タスクがまだ実行中の場合は，タスクはバックグラウンドで実行中である旨のメッセージが返却されます。この場合は時間をおいてから再度 API を実行して，タスクの最新状況および実行結果を確認してください。
	outputFile	文字列	任意※	結果出力ファイルの内容を Base64 エンコードした文字列 正常終了し，結果出力ファイルが出力された場合に返却されます。
	errorCode	文字列	任意※	タスクがエラーになった場合のエラーコード

注※

任意の項目は条件に応じて返却されます。条件に該当しない場合は，項目自体が返却されないことがあります。

使用例

リクエストの例

```
GET https://portal.epm.hitachi-solutions.co.jp/api/v1/tasks?server=server1&sort=startedAt
&order=desc HTTP/1.1
Authorization: Basic Y2xpZW50SWQ6Y2xpZW50U2VjcmV0
```

レスポンス（メッセージボディ）の例

```
{
  "data": [
    {
      "taskId": "b706152b-6321-47fa-a617-f78bc4ab2393",
```

```
      "taskType": "PACKAGE_INSTALL",
      "status": "COMPLETED_SUCCESS",
      "submittedAt": "2026-01-15T10:30:00.000Z",
      "startedAt": "2026-01-15T10:30:05.000Z",
      "endedAt": "2026-01-15T10:32:15.000Z",
      "targetServerName": "server1",
      "resultMessage": "タスクが正常終了しました。",
      "outputFile": "57WQ5p6c5Ye65Yqb44OV44Kh44Kk44Or"
    },
    {
      "taskId": "610e6388-554a-4274-a782-2dc02e1299f9",
      "taskType": "CLIENT_USER_INSTALL",
      "status": "RUNNING",
      "submittedAt": "2026-01-15T10:35:00.000Z",
      "startedAt": "2026-01-15T10:35:10.000Z",
      "endedAt": null,
      "targetServerName": "server1",
      "resultMessage": "タスクの実行を受け付けました。タスクはバックグラウンドで実行中です。"
    }
  ]
}
```


5.3.7　タスク実行状態の取得 API（タスク ID 指定）

指定したタスクの実行状態を取得します。API で実行したタスクだけが対象です。

形式

リクエスト行

```
GET https://portal.epm.hitachi-solutions.co.jp/api/v1/tasks/taskId HTTP/1.1
```

リクエストのメッセージボディ

なし

パラメタ

リクエスト行のパラメタに指定する検索条件を次の表に示します。

表 5–14　パラメタに指定する検索条件

パラメタ	型	区分	説明
taskId	文字列	必須	取得対象タスクのタスク ID API の呼び出しによって作成されたタスクのタスク ID（API の戻り値として返却されたタスク ID）を指定します。

戻り値

ステータスコードが 200 の場合に，レスポンスボディに次の情報を返却します。

表 5–15　レスポンスのメッセージボディの構成内容

パラメタ	型	区分	説明
taskId	文字列	必須	タスク ID
taskType	文字列	必須	タスク種別 次のどれかが返却されます。 • PACKAGE_INSTALL：パッケージのインストール • CLIENT_USER_INSTALL：クライアントユーザによるインストール • JOB_EXECUTE：ジョブの実行 • JOB_DELETE：ジョブの削除 • JOB_DEF_DELETE：ジョブ定義の削除
status	文字列	必須	タスクステータス 次のどれかが返却されます。 • QUEUED：実行待ち • RUNNING：実行中 • COMPLETED_SUCCESS：正常終了 • COMPLETED_ERROR：エラー
submittedAt	日時	必須	タスク作成日時（UTC）
startedAt	日時	必須	タスク開始日時（UTC） 未開始の場合は null が返却されます。
endedAt	日時	必須	タスク終了日時（UTC） 未終了の場合は null が返却されます。
targetServerName	文字列	必須	対象サーバ名
resultMessage	文字列	必須	結果メッセージ タスクがまだ実行中の場合は，タスクはバックグラウンドで実行中である旨のメッセージが返却されます。この場合は時間をおいてから再度 API を実行して，タスクの最新状況および実行結果を確認してください。
outputFile	文字列	任意※	結果出力ファイルの内容を Base64 エンコードした文字列 正常終了し，結果出力ファイルが出力された場合に返却されます。
errorCode	文字列	任意※	タスクがエラーになった場合のエラーコード

注※

任意の項目は条件に応じて返却されます。条件に該当しない場合は，項目自体が返却されないことがあります。

使用例

リクエストの例

```
GET https://portal.epm.hitachi-solutions.co.jp/api/v1/tasks/b706152b-6321-47fa-a617-f78bc4ab2393 HTTP/1.1
Authorization: Basic Y2xpZW50SWQ6Y2xpZW50U2VjcmV0
```

レスポンス（メッセージボディ）の例

```
{
  "taskId": "b706152b-6321-47fa-a617-f78bc4ab2393",
  "taskType": "PACKAGE_INSTALL",
  "status": "COMPLETED_SUCCESS",
  "submittedAt": "2026-01-15T10:30:00.000Z",
  "startedAt": "2026-01-15T10:30:05.000Z",
  "endedAt": "2026-01-15T10:32:15.000Z",
  "targetServerName": "server1",
  "resultMessage": "タスクが正常終了しました。",
  "outputFile": "57WQ5p6c5Ye65Yqb44OV44Kh44Kk44Or"
}
```


補足事項

指定したタスク ID が存在しない場合は，404 Not Found を返します。

付録

付録 A　このマニュアルの参考情報

付録 A.1　製品名の表記

このマニュアルでは，製品名称を次のように表記します。

表記			正式名称
JP1/IM	JP1/IM - Agent		JP1/Integrated Management 3 - Agent
	JP1/IM - Manager		JP1/Integrated Management 3 - Manager
JP1/ITDM2	JP1/IT Desktop Management 2		JP1/IT Desktop Management 2 - Manager
秘文クライアント	秘文 DC		秘文 Device Control
	秘文 DE		秘文 Data Encryption
Firefox			Firefox(R)
Mac	Mac OS		OS X 10.10
			OS X 10.11
			macOS 10.12
			macOS 10.13
			macOS 10.14
			macOS 10.15
			macOS 11
			macOS 12
			macOS 13
			macOS 14
			macOS 15
Microsoft Edge			Microsoft(R) Edge
UNIX	AIX		AIX V6.1
			AIX V7.1
			AIX V7.2
			AIX V7.3
	HP-UX		HP-UX 11i V3(IPF)
	Linux	Red Hat Enterprise Linux Server	Red Hat Enterprise Linux(R) Server 8
			Red Hat Enterprise Linux(R) Server 9

表記				正式名称
UNIX	Linux	Oracle Linux		Oracle Linux(R) Operating System 8
				Oracle Linux(R) Operating System 9
	Solaris			Solaris 10 (SPARC)
				Solaris 11 (SPARC)
Windows	Windows 7	Windows 7 Enterprise		Microsoft(R) Windows(R) 7 Enterprise
		Windows 7 Home Premium		Microsoft(R) Windows(R) 7 Home Premium
		Windows 7 Professional		Microsoft(R) Windows(R) 7 Professional
		Windows 7 Ultimate		Microsoft(R) Windows(R) 7 Ultimate
	Windows 8	Windows 8（無印）		Windows(R) 8
		Windows 8 Enterprise		Windows(R) 8 Enterprise
		Windows 8 Pro		Windows(R) 8 Pro
	Windows 8.1	Windows 8.1（無印）		Windows(R) 8.1
		Windows 8.1 Enterprise		Windows(R) 8.1 Enterprise
		Windows 8.1 Pro		Windows(R) 8.1 Pro
	Windows 10	Windows 10 Enterprise		Windows(R) 10 Enterprise
		Windows 10 IoT Enterprise		Windows(R) 10 IoT Enterprise
		Windows 10 Pro		Windows(R) 10 Pro
		Windows 10 Pro for Workstations		Windows(R) 10 Pro for Workstations
	Windows 11	Windows 11 Enterprise		Windows(R) 11 Enterprise
		Windows 11 Pro		Windows(R) 11 Pro
		Windows 11 Pro for Workstations		Windows(R) 11 Pro for Workstations
	Windows Server 2012	Windows Server 2012（R2 除く）	Windows Server 2012 Datacenter	Microsoft(R) Windows Server(R) 2012 Datacenter
			Windows Server 2012 Standard	Microsoft(R) Windows Server(R) 2012 Standard
		Windows Server 2012 R2	Windows Server 2012 R2 Datacenter	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
			Windows Server 2012 R2 Standard	Microsoft(R) Windows Server(R) 2012 R2 Standard
	Windows Server 2016	Windows Server 2016 Datacenter		Microsoft(R) Windows Server(R) 2016 Datacenter
		Windows Server 2016 Standard		Microsoft(R) Windows Server(R) 2016 Standard

表記			正式名称
Windows	Windows Server 2019	Windows Server 2019 Datacenter	Microsoft(R) Windows Server(R) 2019 Datacenter
		Windows Server 2019 Standard	Microsoft(R) Windows Server(R) 2019 Standard
	Windows Server 2022	Windows Server 2022 Datacenter	Microsoft(R) Windows Server(R) 2022 Datacenter
		Windows Server 2022 Standard	Microsoft(R) Windows Server(R) 2022 Standard
	Windows Server 2025	Windows Server 2025 Datacenter	Microsoft(R) Windows Server(R) 2025 Datacenter
		Windows Server 2025 Standard	Microsoft(R) Windows Server(R) 2025 Standard

付録 A.2　Windows 版と UNIX 版との差異

UNIX 版と Windows 版では一部の用語が異なります。

UNIX 版の用語	Windows 版の用語
組み込み※	インストール
資源登録システム	パッケージャ
パッケージ配布（ソフトウェア配布）	リモートインストール
ファイル収集	リモートコレクト

注※

UNIX では，インストールからセットアップまでを「組み込み」と称します。

付録 A.3　英略語

エンドポイント管理で使用する英略語を次に示します。

英略語	英字での表記
HTTPS	Hyper Text Transfer Protocol Secure
IDaaS	Identity as a Service
IT	Information Technology
MDM	Mobile Device Management
OS	Operating System

英略語	英字での表記
SSO	Single Sign-On
URL	Uniform Resource Locator
UTC	Universal Time, Coordinated
VPN	Virtual Private Network

付録 B　機能の提供有無一覧

オンプレミスの JP1/ITDM2 および秘文の提供機能とエンドポイント管理の提供機能差異について説明します。

付録 B.1　JP1/ITDM2 との差異

JP1/ITDM2 の製品が提供している機能一覧を基に，エンドポイント管理での機能の提供有無および機能差異を次に示します。

重要

- JP1/ITDM2 Manager のインストール時のパラメーターは，カスタマイズできません。
- JP1/ITDM2 Manager の管理用サーバのセットアップおよびリモートインストールマネージャを使用した配布のセットアップのパラメーターは，カスタマイズできません。
- コンフィグレーションファイルの設定は，カスタマイズできません。

表 B–1　JP1/ITDM2 との機能差異

機能	提供有無	概要
システムの概況表示	●	ホーム画面や各画面のダッシュボードから，さまざまな観点で，運用状況を把握できます。
ユーザーアカウントの管理	○	権限，業務分掌，または管轄範囲を設定することで，JP1/ITDM2 を利用する管理者の役割に応じたユーザーアカウントを作成できます。 ただし，system アカウントは使用できません。また，JP1/Base 認証はできません。 なお，サービス利用者に発行するアカウントに付与する業務分掌は，契約したサービスのプランによって変わります。 エンドポイント管理のユーザーアカウントの管理については，「4.3.2　ユーザーアカウント管理」を参照してください。
運用準備の支援	●	ウィザードを利用して，JP1/ITDM2 の運用を開始するための準備ができます。
エージェントの導入	●	利用者のコンピュータにエージェントを導入することで，JP1/ITDM2 の管理対象となり，各種機能を実行できます。 エージェントは，管理者が手動でインストールしたり，管理用サーバから自動で配信したり，さまざまな方法で導入できます。
機器の管理	○	機器を管理対象にすると，情報を収集して確認したり，電源状態を把握して制御したりできます。また，セキュリティポリシーによる判定，レポートの集計など，各種機能の対象になります。なお，UNIX エージェント，Mac エージェントのソフトウェア情報を管理することができ，特定の OS では他社ソフトウェア/パッチ情報の一部の情報を拡張して取得できます。また，UNIX エージェント，Mac エージェントは，電源制御の対象外です。

機能	提供有無	概要
機器の管理	○	探索機能，ネットワーク監視機能を利用することで，組織内の機器を自動で発見して管理対象にできます。 ただし，探索機能および UNIX/Linux/Mac OS 機器の管理は，VPN 接続が前提になります。 JP1/ITDM2 が出力する保存用の変更履歴をポータルシステムのログ一覧画面から ZIP 形式でダウンロードできます。
機器のリモートコントロール	●	コントローラから利用者のコンピュータの画面を呼び出して遠隔操作できます。このほかに，ファイルの送受信，操作内容の録画と再生，チャットなどもできます。なお，UNIX エージェントは，遠隔操作の対象外です。また，Mac OS のコンピュータは，RFB 接続によるリモートコントロールだけができます。
機器のネットワーク接続の管理	●	ネットワークを監視して，未許可の機器のネットワーク接続を防いだり，危険なコンピュータを自動的にネットワークから切断したりできます。UNIX エージェントの接続/遮断は手動での操作となります。
セキュリティの管理	●	セキュリティポリシーを作成し，コンピュータに適用することでセキュリティ状況を判定できます。セキュリティ上問題があるコンピュータを自動で対策できます。 また，コンピュータに対してリモートで対策したり，メッセージを通知したりできます。なお，UNIX エージェントは，セキュリティポリシーによるセキュリティ状況の判定やセキュリティ上の問題点の自動対策の対象外です。Mac エージェントは，セキュリティ上の問題点の自動対策の対象外です。 最新の更新プログラムやウィルス対策製品の情報をサポートサービスサイトから定期的にダウンロードする機能は有効に設定されています。
操作ログの管理※	●	利用者がコンピュータ上で操作した履歴を，操作ログとして収集できます。収集した操作ログは，操作画面から一覧で確認できます。 また，情報漏えいにつながるような不審操作を検知して，操作の履歴の追跡調査ができます。定期エクスポートされた CSV ファイルには IP アドレスの情報が出力されます。なお，UNIX エージェント，Mac エージェントは，操作ログ収集の対象外です。 秘文で取得した操作ログは日次で JP1/ITDM2 に自動的に取り込まれます。ただし，秘文拡張ログのクリップボードデータは取得できません。 検索可能な操作ログの保持期間は標準で 180 日間です。 ポータルシステムのサーバ一覧画面からタスク実行することで，操作ログのエクスポートができます。
資産の管理	○	組織が所有するハードウェア資産やソフトウェアライセンスを登録して，運用状況を管理できます。JP1/ITDM2 の操作画面（資産画面）を使用して簡単に資産管理ができます。 なお，ソフトウェアライセンス情報のライセンス種別は SAMAC 辞書の情報が表示されます。 ポータルシステムのサーバ一覧画面からタスク実行することで，部署・設置場所などの共通管理項目と追加管理項目の定義のエクスポートおよびインポートができます。 JP1/ITDM2 の Asset Console を使用した資産管理はできません。
ソフトウェアおよびファイルの配布	○	管理者が利用者のコンピュータの場所まで行くことなく，ソフトウェアおよびファイルを配布できます。

機能	提供有無	概要
ソフトウェアおよびファイルの配布	○	配布には，次の 2 つの方法があります。 • リモートインストールマネージャを使用して配布する方法 更新プログラム管理の更新プログラム一覧はサポートサービスサイトから更新プログラム情報を取得して表示されます。 リモートインストールマネージャを使用して配布します。この方法では，配布先のコンピュータの条件や，配布先のコンピュータでの動作を詳細に指定できます。 ただし，リモートインストールマネージャとパッケージャはエンドポイント管理との VPN 接続が前提です。 • 操作画面を使用して配布する方法（ITDM 互換配布） 操作画面の配布（ITDM 互換）画面を使用して配布します。リモートインストールマネージャを使用した配布とは異なり，条件や動作を詳細に指定できませんが，ウィザード形式の少ない手順で，インストーラーが MSI ファイルのソフトウェアを，配布先のコンピュータに自動的にインストールできます。また，利用者のコンピュータにインストールされている一部のソフトウェアのアンインストールもできます。インストーラーが MSI ファイルのソフトウェアを，週または月に数回だけ配布したい場合に適した方法です。 リモートインストールマネージャを使用した配布と ITDM 互換配布は，異なる機能です。このため，それぞれの機能に関するデータは，それぞれの機能だけで使用できます。たとえば，リモートインストールマネージャで管理しているソフトウェアは，ITDM 互換配布機能で配布できません。 なお，UNIX エージェント，Mac エージェントへの配布と実行状況の確認は，リモートインストールマネージャを使用して配布する方法を利用する必要があります。
優先配布	●	パッケージングするときに，パッケージに優先度を指定します。
ファイルの収集	×	利用者のコンピュータに格納されているファイルを収集できます。利用者が作成したデータや，利用者が使用したソフトウェアが出力した障害ログなどを，一括で収集できます。 なお，Mac エージェントからのファイルの収集はできません。
イベントの表示	●	JP1/ITDM2 の各機能の実行結果，発生した事象などをイベントとして確認できます。 ただし，JP1/IM のイベント連携はできません。
レポートの表示	●	システム全体の運用状況，セキュリティの診断結果，省電力化の状況，資産に掛かっている費用など，目的に応じた多様なレポートを表示できます。
フィルタの利用	●	フィルタを利用して，操作画面の各一覧に表示されている情報を絞り込めます。設定したフィルタの条件は，保存しておくこともできます。
複数の部門やネットワークで構成される大規模システムの管理	●	管理するシステムの規模やネットワーク構成に合わせて複数の管理用サーバを導入することで，管理者や管理用サーバの負荷を分散したり，NAT 環境での運用に対応したりできます。 ただし，管理用中継サーバの設置はオプション（管理用中継サーバ追加オプション）の契約が必要です。また，管理用中継サーバはエンドポイント管理マネージャのクラウド環境内に設置して提供されます。
クラスタシステムでの運用	×	クラスタシステムで JP1/ITDM2 を運用できます。

機能	提供有無	概要
データベースの管理	×	データベースマネージャを利用して，JP1/ITDM2 のデータベースのバックアップやメンテナンスを実行できます。
コマンドの利用	△	コマンドを利用して，管理情報のインポート，エクスポート，データベースのバックアップ，メンテナンスなどを実行できます。 エンドポイント管理では，ポータルシステムのサーバー一覧画面から次のコマンドに相当する操作ができます。 • ioutils exportoplog（操作ログのエクスポート） 操作ログのエクスポートができます。 ＜コマンドとの差異＞ ・文字コードの指定はできません。「UTF-8」になります。 ・フィルタを使用して特定の操作ログをエクスポートすることはできません。 ・1 ファイルにエクスポートする行数を指定することはできません。1 ファイルには最大 2GB 分の操作ログが出力されます。 ・操作日時を出力するタイムゾーンを指定することはできません。 • ioassetsfieldutil import（共通管理項目と追加管理項目の定義のインポート） ＜コマンドとの差異＞ ・文字コードの指定はできません。「UTF-8」になります。 ・利用者の入力開始のタイミングは指定できません。設定画面の［資産管理］－［資産管理項目の設定］－［利用者情報の入力開始日時］に表示されている設定のまま実行します。 • ioassetsfieldutil export（共通管理項目と追加管理項目の定義のエクスポート） ＜コマンドとの差異＞ ・文字コードの指定はできません。「UTF-8」になります。 エンドポイント管理では，JP1/ITDM2 の一部のコマンドに相当する機能を API として提供しています。詳細は，「5　API リファレンス」を参照してください。
利用者のコンピュータ上での操作	●	利用者のコンピュータでは，管理用サーバから通知されるメッセージを確認したり，利用者情報を入力したりできます。なお，UNIX エージェント，Mac エージェントについては，管理用サーバから通知されるメッセージを確認したり，エージェントの利用者情報を入力したりはできません。
スマートデバイスの制御	○	MDM システムと連携して，スマートデバイスをロックしたり，初期化したりできます。 ただし，連携できる MDM システムは Microsoft Intune と Google Workspace だけです。MDM 連携の設定画面で，他の MDM システムを選択しても連携できません。 マルウェア感染機器の制御はエージェントのポーリング方法によって，時間が掛かる場合があります。
インターネットを介したコンピュータの管理	●	インターネットを介して接続されている利用者のコンピュータを管理できます。管理用サーバと利用者のコンピュータが VPN を介して接続している場合だけでなく，VPN を使用しないで接続している場合も管理できます。
IDaaS 連携（多要素認証対応）	○	IDaaS の共通認証基盤での認証（Keycloak 連携，Entra ID 連携）やシングルサインオン（Open ID Connect 認証対応，SAML 認証）が使用できます。

機能	提供有無	概要
IDaaS 連携（多要素認証対応）	○	ただし，連携する IDaaS はエンドポイント管理が提供する認証基盤に限定されます。他の IDaaS は利用できません。

（凡例）●：提供あり　○：提供ありだが一部制約あり　△：一部提供あり　×：提供なし

注※

JP1/ITDM2 および秘文とエンドポイント管理で提供が異なる操作ログについて次に示します。

操作種別	操作種別（詳細）	提供有無	内容
コンピュータの起動と停止，ログオンとログオフ	コンピュータ起動	●	ユーザーがコンピュータを起動した。
	コンピュータ停止	●	ユーザーがコンピュータを停止した。
	ログオン	●	ユーザーが Windows にログオンした。
	ログオフ	●	ユーザーが Windows からログオフした。
Web 参照操作	Web アクセス	●	ユーザーが Web ブラウザを利用して Web にアクセス
ウィンドウ操作	アクティブウィンドウの変更	●	ユーザーがアクティブウィンドウを変更した。
コンソール操作	コマンドプロンプトで実行されたコマンド	●	コマンドプロンプトでコマンドが実行された。
	PowerShell で実行されたコマンド	●	PowerShell でコマンドが実行された。
	実行されたバッチファイル	●	バッチファイルが実行された。
	実行された PowerShell スクリプトファイル	●	PowerShell スクリプトファイルが実行された。
抑止ログ	プログラム起動抑止	●	使用禁止ソフトウェアを設定している場合に，プログラムの起動を抑止した。
	印刷抑止※1	●	禁止操作を設定している場合に，印刷を抑止した。
	デバイス接続抑止	●	禁止操作を設定している場合に，デバイスの使用を抑止した。
クリップボード操作	クリップボード操作 コピー	●	クリップボードのコピーを実行したプロセス
	クリップボード操作 ペースト	●	クリップボードのペーストを実行したプロセス
ファイル/フォルダ操作※2	ファイル作成	●	ユーザーがファイルを作成
	ファイルコピー	●	ユーザーがファイルをコピー
	ファイル移動	●	ユーザーがファイルを移動
	ファイル名変更	●	ユーザーがファイル名を変更
	ファイル削除	●	ユーザーがファイルを削除

操作種別	操作種別（詳細）	提供有無	内容
ファイル/フォルダ操作※2	ファイルオープン	×	ユーザーがファイルをオープン
	フォルダコピー	●	ユーザーがフォルダをコピー
	フォルダ移動	●	ユーザーがフォルダを移動
	フォルダ名称変更	●	ユーザーがフォルダ名を変更
	フォルダ作成	●	ユーザーがフォルダを作成
	フォルダ削除	●	ユーザーがフォルダを削除
デバイス操作	デバイス接続	●	ユーザーが機器にデバイスを接続
	デバイス接続抑止	●	ユーザーが機器に接続したデバイスの接続を抑止
	デバイス接続許可	●	ユーザーが機器に接続したデバイスの使用を許可
アプリケーション操作	ファイル作成	●	ユーザーがエクスプローラ，コマンドプロンプト，Windows PowerShell，Windows Script Host でファイルを作成
	ファイルコピー	●	ユーザーがエクスプローラ，コマンドプロンプト，Windows PowerShell，Windows Script Host でファイルをコピー
	ファイル移動	●	ユーザーがエクスプローラ，コマンドプロンプト，Windows PowerShell，Windows Script Host でファイルを移動
	ファイル名変更	●	ユーザーがエクスプローラ，コマンドプロンプト，Windows PowerShell，Windows Script Host でファイル名を変更
	ファイル削除	●	ユーザーがエクスプローラ，コマンドプロンプト，Windows PowerShell，Windows Script Host でファイルを削除
	ファイルオープン	●	ユーザーが Office 製品，Windows 標準のプログラムでファイルをオープン
	ファイル上書き保存	●	ユーザーが Office 製品，Windows 標準のプログラムでファイルを上書き保存
	ファイル圧縮	●	ユーザーがエクスプローラ，Windows PowerShell でファイルを圧縮
ネットワーク経由ファイル操作	FTP 送信	●	ユーザーがブラウザを介し FTP サーバにファイルを送信
	FTP 受信	●	ユーザーがブラウザを介し FTP サーバからファイルを受信
	メール送信（添付ファイル付）	●	ユーザーが特定のメーラー（MUA）で添付ファイル付きのメールを送信

操作種別	操作種別（詳細）	提供有無	内容
ネットワーク経由ファイル操作	メール送信（添付ファイル付）	●	添付ファイルがない場合は，操作ログを取得しません。
	メール受信（添付ファイル付）	●	ユーザーが特定のメーラー（MUA）で添付ファイルありのメールを受信 添付ファイルがない場合は，操作ログを取得しません。
	添付ファイル保存	●	ユーザーが特定のメーラー（MUA）で添付ファイルありのメールを受信したあと，添付ファイルを保存
	ファイルアップロード	●	ユーザーがファイルをアップロード
	ファイルダウンロード	●	ユーザーがファイルをダウンロード
プログラム起動/停止	プログラムの起動抑止	●	ユーザーが起動したプログラムの起動を抑止
リモートデスクトップ接続	リモートデスクトップ接続	●	リモートデスクトップへの接続
ネットワークアクセス	ネットワークの接続	●	有線 LAN への接続／無線 LAN への接続
	ネットワークの切断	●	有線 LAN の切断／無線 LAN の切断
	ネットワーク通信	×	ネットワーク通信（TCP/IP）
暗号ファイル保護	許可プログラムからの保護対象ファイルへのアクセス	●	許可プログラムからの保護対象ファイルへのアクセス
	禁止プログラムからの保護対象ファイルへのアクセス	●	禁止プログラムからの保護対象ファイルへのアクセスまたは禁止プログラムからのディスクの管理領域への書き込み
マルウェア追跡	マルウェア検知イベント	●	マルウェア検知イベント発生（CylancePROTECT）
	メモリ保護イベントおよびスクリプト禁止イベント	●	メモリ保護イベントまたはスクリプト禁止イベント発生（CylancePROTECT）
印刷操作	印刷※1	●	ユーザーがプリンタで印刷

（凡例）●：提供あり　×：提供なし

注※1

操作ログを取得できるプリンタを次に示します。

- ローカルプリンタ
- ネットワーク共有プリンタ
- 仮想プリンタ

注意事項

インターネット接続のプリンタでは操作ログを取得できません。また，ローカルプリンタで File ポートを使用する場合は「印刷抑止」の操作ログを取得できません。LAN Manager ポートを使用する場合は「印刷抑止」の操作ログを取得できません。

注※2

内蔵ハードディスクのファイル/フォルダ操作は取得されません。

付録 B.2　秘文との差異

秘文の製品が提供している機能一覧を基に，エンドポイント管理での機能の提供有無および機能差異を次に示します。

表 B–2　秘文との機能差異

機能	提供有無	概要
持ち出し制御	○	次のようなデータの持ち出しを許可したり，禁止したりできます。 • 外付けハードディスクやリムーバブルメディア（USB メモリなど）などの外部記憶媒体へのファイルのコピー • ライティングソフトや OS 標準の書き込み機能による CD/DVD メディアへのデータの書き込み • ネットワーク（共有フォルダ）経由でのファイルのコピー • 印刷（プリンタ）によるデータの出力 ただし，暗号化されたファイルを持ち出す場合は，暗号化オプションが必要です。
読み込み制御	●	媒体の持ち出し制御やデバイスの個体識別制御で持ち出しを禁止した場合に，持ち出しだけではなく，読み込みも禁止します。 • リムーバブルメディアからの読み込み制御 • 外付け HDD からの読み込み制御 • ライティングソフトからの読み込み制御
デバイス使用可否制御	●	クライアント PC に接続できるデバイス（PC 用の周辺機器）の使用を許可したり，禁止したりできます。
許可ネットワーク制御	●	特定のネットワークの利用を許可したり，禁止したりできます。次の機能があります。 • アクセスポイント制限機能 許可された Wi-Fi アクセスポイントだけ使用できるようにする機能です。 • 接続ネットワーク確認機能 クライアント PC が許可ネットワーク環境に接続されているかを確認し，許可されていないネットワーク環境に接続されている場合，ネットワークを切断する機能です。 • エリア探知によるスクリーンロック機能 エリア探知によるスクリーンロック機能は，スクリーンロックによって，ユーザーが PC を操作できる環境をエリア内（社内，工場内など）だけに限定する機能です。

機能	提供有無	概要
許可ネットワーク制御	●	• 利用モード切り替え機能 接続を許可するネットワークを切り替える機能です。 出張など社外で利用するクライアント PC は，社内および社外のどちらのネットワークにも自由に接続できます。利用モード切り替え機能は，社外で利用するクライアント PC を社内で利用するとき，接続先を社内ネットワークだけに限定します。 • VPN 強制機能 ネットワークへのアクセスを，VPN サーバを経由する通信だけに制限する機能です。ネットワークへのアクセスが必ず社内の VPN サーバを経由するため，常に社内と同じセキュリティポリシーを適用できます。 • 許可ネットワーク制御一時解除機能 許可ネットワーク制御一時解除機能は，出張先（社外）で許可ネットワーク制御の機能を一時的に無効化（解除）する機能です。
マルウェア対策製品連携機能	●	マルウェア対策製品と連携することによって，感染 PC に警告画面を表示したり，感染 PC をネットワークから遮断したりすることができます。
認証強化	●※	次に示す二つのユーザー認証を連続して行う拡張認証と iKey 認証/eToken 認証ができます。 • 秘文ログイン画面または Windows 標準認証画面でのユーザー認証 • 拡張認証パスワード入力画面でのユーザー認証
スクリーンロック	●※	スクリーンロックによって，ユーザーが PC を操作できる環境をエリア内（社内，工場内など）だけに限定します。
端末ロック	●※	秘文へのログイン時に，ログイン失敗回数が，インストール媒体作成時に設定した回数に達すると，PC にロックが掛かります。
暗号化機能	●※	ハードディスクや USB メモリなどをドライブ単位で暗号化することができます。また，ファイル単位でも暗号化することができます。
ファイル保護機能（暗号ファイル保護機能）	●※	マルウェアなどの不正なプログラムからファイルの保護ができます。
ログ取得	○	クライアント PC 上で行われたユーザーのアクセス操作などの履歴（ログ）を取得できます。 ただし，次のログを取得するには，暗号化オプションが必要です。 • ローカルの暗号化ドライブへのアクセスログ • 秘文ファイルサーバへのアクセスログ • ファイルアクセス制御ログ なお，オフライン PC のクライアントログは取得できません。
共有フォルダの暗号化機能（共有機密フォルダ）	●※	秘文サービスから秘文クライアントの修正パッチプログラムがリリースされた場合に，自動的に秘文クライアントを導入している PC に修正パッチを配信できます。
ポリシー管理	○	管理する拠点のネットワーク環境に合わせて，アクセスポイント制限機能で許可する SSID を設定したり，接続ネットワーク確認機能で使用する認証先を設定したりできます。なお，ポリシー管理は，次の単位で設定できます。 • ユーザー単位での管理 • グループ単位での管理

機能	提供有無	概要
ポリシー管理	○	• オフラインログイン時のポリシー管理 • 許可ネットワーク制御機能のポリシー管理 • デバイス使用可否制御機能のポリシー管理 • 暗号ファイル保護機能のポリシー管理※ • 拡張ログのポリシー管理
クライアントパッチ自動配信機能	●	秘文サービスから秘文クライアントの修正パッチプログラムがリリースされた場合に，自動的に秘文クライアントを導入している PC に修正パッチを配信することができます。
秘文クライアント未導入端末検知機能	●	ネットワークを自動的に探索して，秘文クライアントが未導入の端末を検知する機能です。
アプリインストール制御	●	アプリケーションのインストールを禁止する機能です。
アラート通知機能	●	秘文の制御によって操作や入出力の処理を禁止した場合に，PC 利用者に対してアラートを通知する機能です。
インシデント発生時の詳細調査用のログ取得機能	×	長期間にわたって，クライアント PC 上で発生したイベントのログを記録できます。
IDaaS 製品連携機能	×	クラウドサービスなどのユーザー認証に Okta などの IDaaS 製品を使用している場合に，IDaaS 製品と連携することによって，秘文 資産管理で管理しているデバイスだけ，認証を許可できます（デバイス認証機能）。また，ポスチャの状態が適切に保たれているデバイスだけ認証を許可できます（ポスチャ認証機能）。
ポスチャ管理機能	×	組織でのセキュリティ態勢のことです。秘文サービスでは，エンドポイントで次の状態を適切に維持することで，ゼロトラストネットワーク時代のセキュリティ確保を実現します。 • セキュリティ設定 • アプリケーション管理 • ソフトウェア脆弱性 • アンチウイルス設定 • ファイアウォール設定 • 任意の診断項目
Active Directory 連携機能	×	オンプレミス環境の Active Directory と連携して，Active Directory のグループ情報である OU（組織単位）および SG（セキュリティグループ）情報を秘文サービスにインポートし，秘文のグループとして登録する機能です。Active Directory と連携することでユーザー管理が容易になり，システム管理者の負荷が軽減されます。
ログ連携 WebAPI 機能	×	秘文のログを外部システムに連携するための機能を Web API として提供します。
ユーザ管理	●	秘文管理ツールを使用して，ユーザの追加，更新，および削除ができます。
機密情報分類サービス連携機能	×	機密情報分類サービスと連携する機能です。

（凡例）●：提供あり　○：提供ありだが一部制約あり　×：提供なし

注※

暗号化オプションを使用する場合に限ります。

付録 C　用語解説

（英字）

IDaaS 連携

ID プロバイダーと連携した JP1/IT Desktop Management 2 の認証機能です。

ID プロバイダーが提供する多要素認証や他のアプリケーションとのシングルサインオンが可能です。

ID プロバイダー

ユーザーの認証機能および認証情報を提供するシステムやサービスです。

複数のアプリケーションにログインするユーザー情報を一元管理し，多要素認証をはじめとする認証強化の目的でも利用されます。

JP1/ITDM2（中継マネージャ）

JP1/IT Desktop Management 2 - Manager を管理用中継サーバとして構築されたサーバです。部門やネットワーク構成ごとに JP1/IT Desktop Management 2 を運用したい場合に設置します。また，中継システムと同様，リモートインストールマネージャを使用した配布でジョブの実行やパッケージの配布でネットワークに掛かる負荷を軽減できます。

JP1/ITDM2（統括マネージャ）

JP1/IT Desktop Management 2 - Manager のサーバのうち，複数サーバ構成の最上位に設置されたサーバです。

（ア行）

インストールセット

JP1/IT Desktop Management 2 - Agent のインストールとセットアップを一度に実行できる，エージェントの導入を支援するプログラムです。JP1/IT Desktop Management 2 の管理画面で作成します。

運用管理コンピュータ

サービスの利用者が，エンドポイント管理のポータルシステムにログインするコンピュータです。

エージェント

JP1/IT Desktop Management 2 で管理される側のコンピュータにインストールするプログラムです。JP1/IT Desktop Management 2 - Manager に情報を通知したり，JP1/IT Desktop Management 2 - Manager からの指示でコンピュータを制御したりします。プログラム名は「JP1/IT Desktop Management 2 - Agent」です。

エージェント設定

JP1/IT Desktop Management 2 の管理画面で管理する，エージェントのセットアップの設定内容です。JP1/IT Desktop Management 2 の管理画面でエージェント設定を作成し，エージェントに割り当てることで，エージェントのセットアップをリモートで変更できます。

（カ行）

管理対象機器

エージェントがインストールされているかどうかに関係なく，JP1/IT Desktop Management 2 の管理対象に設定した機器を指します。

機器一覧

コンピュータや周辺機器を含めた，IT 機器の一覧を指します。JP1/IT Desktop Management 2 で作成できます。

（タ行）

中継システム

管理用サーバと管理対象のコンピュータの間で，リモートインストールやファイル転送などのジョブを中継する JP1/IT Desktop Management 2 - Agent のことです。

（ハ行）

パッケージ

リモートインストールマネージャを使用して配布するソフトウェアの単位です。パッケージャでパッケージを作成すると，JP1/IT Desktop Management 2 - Manager のキャビネットに保管されます。保管されたパッケージは，リモートインストールマネージャで配布できます。

パッケージャ

リモートインストールするソフトウェアを，管理用サーバに登録するプログラムです。

付録 D　各バージョンの変更内容

付録 D.1　02-60 の変更内容

02-50 向けマニュアルから 02-60 向けマニュアルでの変更点を次に示します。

- 秘文サービス管理ページで，シングルサインオン（SSO）機能を利用できるようになりました。
- エンドポイント管理で使用するポート番号に関する記載を追加しました。
- JP1/ITDM2 が出力する保存用の変更履歴をポータルシステムからダウンロードできるようにしました。これに伴い，「操作ログ一覧」を「ログ一覧」に変更しました。
- ポータルシステムの機能一覧に，「認証設定」を追加しました。
- エンドポイント管理のポータルシステムで，API が利用できるようになりました。

付録 D.2　02-50 の変更内容

02-40 向けマニュアルから 02-50 向けマニュアルでの変更点を次に示します。

- エンドポイント管理で使用できる機能を，サービスプラン別に確認できるようになりました。
- エンドポイント管理の利用に必要な事前設定について，説明を追加しました。
- ポータルおよび JP1/ITDM2 管理画面で，シングルサインオン（SSO）機能を利用できるようになりました。
- オンプレミス版の JP1/ITDM2 の提供機能と，エンドポイント管理の提供機能の差異に関する説明を変更しました。

付録 D.3　02-40 の変更内容

02-30 向けマニュアルから 02-40 向けマニュアルでの変更点を次に示します。

- サーバ一覧画面から次のタスクを実行できるようになりました。
  - 操作ログのエクスポート
  - 管理項目定義のインポート
  - 管理項目定義のエクスポート
- サーバ一覧画面から開始したタスクのステータス（実行状態），操作結果詳細，および関連情報を確認できるタスク一覧画面を追加しました。
- 操作ログのエクスポート機能の追加に伴い，操作ログ一覧でエクスポートされた操作ログを参照できるようになりました。

- オンプレミス版の JP1/ITDM2 の提供機能と，エンドポイント管理の提供機能の差異に関する説明を変更しました。

付録 D.4　02-30 の変更内容

02-20 向けマニュアルから 02-30 向けマニュアルでの変更点を次に示します。

- サービスプランごとの提供機能の説明を追加しました。また，サービスプランで異なるシステムの構成例の説明を追加しました。
- エンドポイント管理の機能ごとに対応するプラットフォームの説明を追加しました。
- ポータルシステムのログイン認証およびパスワード変更を多要素認証に変更しました。
- オンプレミスの JP1/ITDM2 および秘文の提供機能とエンドポイント管理の提供機能差異について説明を追加しました。

付録 D.5　02-20 の変更内容

02-10 向けマニュアルから 02-20 向けマニュアルでの変更点を次に示します。

- エンドポイント管理に暗号化オプションを追加したことに伴い，暗号化機能とファイル保護機能についての記述を追加しました。

索引

I

IDaaS 連携〔用語解説〕 121
ID プロバイダー〔用語解説〕 121

J

JP1/ITDM2（中継マネージャ）〔用語解説〕 121
JP1/ITDM2（統括マネージャ）〔用語解説〕 121

あ

暗号化機能 46

い

インストールセットの作成 32
インストールセット〔用語解説〕 121

う

運用管理コンピュータの構築 29
運用管理コンピュータ〔用語解説〕 121

え

エージェント設定〔用語解説〕 122
エージェントのインストール
  UNIX または Mac の場合 32
  Windows の場合 32
エージェント〔用語解説〕 121
エンドポイント管理の概要 10
エンドポイント管理の機能 15
エンドポイント管理の特長 11
エンドポイント管理のポータルシステムの利用方法 48
エンドポイント管理の利用方法 36
エンドポイント管理への接続 20
エンドポイント管理利用の準備 20
エンドポイント管理を利用するための構築 25

か

管理対象機器〔用語解説〕 122

き

機器一覧〔用語解説〕 122
機器の管理 38
機器のネットワーク接続の管理 42
機器のリモートコントロール 39

こ

構築の流れ 26
  運用管理コンピュータの構築の流れ 26
  ファイルサーバの構築の流れ 27
  利用者コンピュータの構築の流れ 27

し

資産の管理 40
システム構成 12
システムの概況把握 37

せ

セキュリティの管理 43

そ

操作ログの管理 44

ち

中継システム〔用語解説〕 122

て

提供機能 15

は

配布機能 41
パッケージャのインストール 29
パッケージャ〔用語解説〕 122
パッケージ〔用語解説〕 122

ひ

秘文インストール媒体の作成 32

秘文管理ツールのインストール　30
秘文クライアントのインストール　32

ふ

ファイルサーバのインストール　34
ファイルサーバの構築　34
ファイルサーバの設定　35
ファイル保護機能　47

ほ

ポータルシステムの概要　49
ポータルシステムの利用方法
　お知らせの表示　81
　サーバー一覧の表示　61
　サポート情報一覧の表示　80
　シングルサインオン（SSO）の利用方法　51
　製品媒体一覧の表示　76
　タスク一覧の表示　68
　提供ファイル一覧の表示　79
　認証設定の表示　72
　マニュアル一覧の表示　78
　ユーザーアカウント管理　52
　ライセンス情報の表示　82
　ログインとログアウト　55
　ログインユーザーのパスワード変更　60
　ログの表示　74
ポリシーの反映　45

り

リモートインストールマネージャのインストール　29
利用者コンピュータの構築　31
利用できる Web ブラウザ　50

株式会社 日立製作所

〒 100–8280　東京都千代田区丸の内一丁目 6 番 6 号