

Hitachi Ops Center

インストールガイド

4010-1J-101-70

対象製品

Hitachi Ops Center 10.9.3

輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並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

HITACHI は、株式会社 日立製作所の商標または登録商標です。

Active Directory は、マイクロソフト 企業グループの商標です。

Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標です。

Microsoft は、マイクロソフト 企業グループの商標です。

Oracle®、Java 及び MySQL は、Oracle、その子会社及び関連会社の米国及びその他の国における登録商標です。

PowerShell は、マイクロソフト 企業グループの商標です。

Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries.

Red Hat は、米国およびその他の国における Red Hat, Inc.の登録商標です。

Red Hat Enterprise Linux is a registered trademark of Red Hat, Inc. in the United States and other countries.

Red Hat Enterprise Linux は、米国およびその他の国における Red Hat, Inc.の登録商標です。

Windows は、マイクロソフト 企業グループの商標です。

Windows Server は、マイクロソフト 企業グループの商標です。

その他記載の会社名、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。

発行

2023 年 9 月 4010-1J-101-70

著作権

All Rights Reserved. Copyright© 2021, 2023, Hitachi, Ltd.

目次

はじめに.....	7
対象読者.....	8
マニュアルの構成.....	8
このマニュアルで使用している記号.....	8
1.概要.....	11
1.1 Hitachi Ops Center の各製品の概要.....	12
1.2 Hitachi Ops Center Common Services の概要.....	12
1.2.1 Active Directory または LDAP サーバとの連携.....	12
1.2.2 ID プロバイダーとの連携.....	13
1.3 Hitachi Ops Center のシステム構成例.....	14
1.3.1 1 台の管理サーバで運用する場合の構成例.....	14
1.3.2 複数台の管理サーバで運用する場合の構成例.....	14
2.Hitachi Ops Center 製品のインストールとアップグレードインストール.....	17
2.1 Hitachi Ops Center のインストールとセットアップの流れ.....	18
2.2 管理サーバを準備する.....	18
2.3 Common Services をインストールまたはアップグレードインストールする.....	19
2.4 各製品をインストールまたはアップグレードインストールする.....	21
2.5 SSL 通信の設定をする.....	22
2.6 Hitachi Ops Center 製品を Common Services に登録する.....	22
2.7 Hitachi Ops Center Portal にログインする.....	23
2.8 Hitachi Ops Center Portal で初期設定をする.....	24
3.Hitachi Ops Center 製品のアンインストール.....	25
3.1 Common Services をアンインストールする.....	26
4.SSL 通信の設定.....	27
4.1 SSL セットアップツールを使用した SSL 通信の設定.....	28
4.1.1 SSL セットアップツールが提供する機能.....	29
4.1.2 秘密鍵と証明書署名要求の作成 (SSL セットアップツール)	30
4.1.3 SSL サーバの設定 (SSL セットアップツール)	31

4.1.4 Active Directory または LDAP サーバの SSL サーバの設定をする	32
4.1.5 ID プロバイダーサーバの SSL サーバの設定をする	32
4.1.6 SSL クライアントの設定と証明書検証機能の有効化 (SSL セットアップツール)	32
4.2 SSL セットアップツールを使用しない SSL 通信の設定	34
4.2.1 Common Services のサーバ証明書を用意する	34
4.2.2 プロパティファイルにサーバ証明書および秘密鍵のパス情報を設定する	35
4.2.3 各製品の SSL サーバの設定をする	36
4.2.4 Active Directory または LDAP サーバの SSL サーバの設定をする	36
4.2.5 ID プロバイダーサーバの SSL サーバの設定をする	36
4.2.6 認証局の証明書を各製品にインポートする	36
4.2.7 認証局の証明書を Common Services のトラストストアにインポートする	37
4.2.8 サーバ証明書の検証機能を有効にする	38
5.ID プロバイダーとの連携	39
5.1 サポートする ID プロバイダー	40
5.2 AD FS と連携するための設定の流れ	40
5.3 AD FS と連携するための設定 (OIDC)	41
5.3.1 AD FS に Common Services をアプリケーショングループとして登録する	41
5.3.2 AD FS に発行変換規則を設定する	42
5.3.3 AD FS の OpenID connect 検出エンドポイントを確認する	43
5.3.4 Common Services に AD FS を登録する	43
5.3.5 Hitachi Ops Center Portal に ID プロバイダーのユーザーでログインする	44
5.4 AD FS と連携するための設定 (SAML)	45
5.4.1 AD FS のメタデータエンドポイントを確認する	45
5.4.2 Common Services に AD FS を登録する	45
5.4.3 Common Services のメタデータをエクスポートする	46
5.4.4 AD FS に Common Services を証明書利用者信頼として登録する	47
5.4.5 要求発行ポリシーを設定する	47
5.4.6 Hitachi Ops Center Portal に ID プロバイダーのユーザーでログインする	49
5.5 ID プロバイダーの認証用証明書の更新 (SAML)	50
5.5.1 認証用証明書の更新の概要	50
5.5.2 Common Services の証明書の次回更新日を確認する	50
5.5.3 AD FS の証明書の次回更新日を確認する	50
5.5.4 Common Services の証明書を更新する	51
5.5.5 AD FS の証明書を更新する	51
5.5.6 シングルサインオンができないときの対処	52
(1) AD FS で Common Services のメタデータを更新する	52
(2) Common Services で AD FS のメタデータエンドポイントを指定する	53
6.Hitachi Ops Center の保守	55
6.1 Common Services のサービスを起動、停止する	56
6.2 トラストストア内の証明書の有効期限を確認する	56
6.3 サーバ証明書の有効期限を確認する	56
6.4 サーバ証明書の失効状態を確認する	57
6.4.1 Web ブラウザーを使用したサーバ証明書の失効確認	57
6.4.2 コマンドを使用したサーバ証明書の失効確認	58
6.4.3 定期的にサーバ証明書の失効状態を確認する	58
(1) 失効状態の確認結果をファイルに出力する	58
(2) 失効状態の確認結果を syslog に出力する	60

6.5 管理サーバのホスト名または IP アドレス、ポート番号を変更する.....	61
6.6 内部通信で使用するポート番号を変更する.....	62
6.7 Common Services のデータをバックアップする.....	64
6.8 Common Services のデータをリストアする.....	64
6.9 各製品との信頼関係をリセットする.....	65
6.10 セッションのアイドルタイムアウト設定をする.....	66
6.11 ウィルス検出プログラムを使用する場合に必要な設定.....	67
6.12 Amazon Corretto 17 をアップグレードする.....	67
6.13 PostgreSQL 15 をアップグレードする.....	68
付録 A トラブルシューティング.....	69
A.1 障害情報を収集する.....	70
A.2 Common Services のログ.....	70
A.2.1 ログのプロパティを変更する.....	71
A.3 Common Services の監査ログ.....	72
A.3.1 監査ログのプロパティを変更する.....	73
A.4 Common Services のメッセージ.....	75
A.5 LDAP サーバ登録時のパラメーターを決定する.....	92
付録 B このマニュアルの参考情報.....	95
B.1 関連マニュアル.....	96
B.2 このマニュアルでの表記.....	96
B.3 このマニュアルで使用している略語.....	96
B.4 KB（キロバイト）などの単位表記について.....	97
索引.....	99



はじめに

このマニュアルは、Hitachi Ops Center のインストールおよび設定方法について説明したものです。

- 対象読者
- マニュアルの構成
- このマニュアルで使用している記号

対象読者

このマニュアルは、Hitachi Ops Center 製品を管理および使用するシステム管理者を対象としています。

システム管理者は、次の製品の知識があることを前提としています。

- Oracle Linux または Red Hat Enterprise Linux の基本的な知識
- 前提ソフトウェアに関する基本的な知識（外部認証サーバ、または ID プロバイダーとの連携機能を使用する場合）

マニュアルの構成

このマニュアルは、次に示す章から構成されています。

第 1 章 概要

Hitachi Ops Center の各製品の概要、およびシステム構成について説明しています。

第 2 章 Hitachi Ops Center 製品のインストール

Hitachi Ops Center 製品をインストールする方法について説明しています。

第 3 章 Hitachi Ops Center 製品のアンインストール

Hitachi Ops Center 製品のアンインストールについて説明しています。

第 4 章 SSL 通信の設定

正式なサーバ証明書を適用した SSL 通信の設定方法について説明しています。

第 5 章 ID プロバイダーとの連携

Hitachi Ops Center Portal の認証を ID プロバイダーと連携して実施する場合の設定方法について説明しています。

第 6 章 Hitachi Ops Center の保守

Hitachi Ops Center のシステムの保守について説明しています。

付録 A トラブルシューティング

メッセージやログファイルを参照して障害に対処する方法、および保守情報の採取方法について説明しています。

付録 B 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を説明しています。

このマニュアルで使用している記号

このマニュアルでは、次に示す記号を使用しています。

記号	意味と例
[] (角括弧)	画面、メニュー、ボタン、キーボードのキーなどを示します。 表示項目を連続して選択する場合には、[] を一でつないで説明しています。
< >	可変値であることを示します。

記号	意味と例
(山括弧)	
文字列	

また、コマンドの記述方法については、次に示す記号を用いて説明します。

記号	意味と例
 (ストローク)	複数の項目に対して項目間の区切りを示し、「または」の意味を示します。 (例) 「A B C」は、「A, B, または C」を示します。
{ } (波括弧)	この記号で囲まれている複数の項目の中から、必ず一組の項目を選択します。項目と項目の区切りは「 」で示します。 (例) 「{A B C}」は、「A, B, または C のどれかを必ず指定する」ことを示します。
[] (角括弧)	この記号で囲まれている項目は、任意に指定できます (省略できます)。 (例) 「[A]」は、「必要に応じて A を指定する」ことを示します (必要でない場合は、A を省略できます)。 「[B C]」は、「必要に応じて B, または C を指定する」ことを示します (必要でない場合は、B および C を省略できます)。
...点線 (リーダー)	記述が省略されていることを示します。この記号の直前に示された項目を繰り返し複数個指定できます。 (例) 「A,B,C...」は、「A と B の後ろに C を複数個指定できる」ことを示します。

概要

Hitachi Ops Center 製品は、分析、自動化などの機能を統合し、データセンターの運用を最適化する製品です。Hitachi Ops Center の機能を利用することで、ストレージインフラストラクチャーの管理、自動化ができます。

Hitachi Ops Center は複数の製品から構成されるシステムです。システム構成の概要について説明します。Hitachi Ops Center 製品のコンポーネントおよびシステム構成の概要について説明します。

- 1.1 Hitachi Ops Center の各製品の概要
- 1.2 Hitachi Ops Center Common Services の概要
- 1.3 Hitachi Ops Center のシステム構成例

1.1 Hitachi Ops Center の各製品の概要

Hitachi Ops Center のシステムは、次のソフトウェアで構成されます。

Hitachi Ops Center Common Services

ポータル画面、ユーザー管理、シングルサインオンなど、Hitachi Ops Center の共通の基盤機能を提供します。

Hitachi Ops Center Automator

データセンターやストレージシステムの管理者にストレージプロビジョニングプロセスを自動化、簡略化する機能を提供します。

Hitachi Ops Center Viewpoint

複数のデータセンターをまたがるシステム監視の機能を提供します。
システム監視に必要なリソース情報は、Hitachi Ops Center Viewpoint のコンポーネントである Hitachi Ops Center Viewpoint data center proxy から収集します。

Hitachi Ops Center API Configuration Manager

ストレージシステムの情報取得、操作に関する API を提供します。

1.2 Hitachi Ops Center Common Services の概要

Hitachi Ops Center Common Services は、Hitachi Ops Center 製品のシングルサインオン機能およびポータルサイト機能を提供するコンポーネントです。

Hitachi Ops Center Portal にログインすると、登録された Hitachi Ops Center 製品の一覧が表示され、製品名のリンクをクリックするとログイン後の画面を起動できます。製品ごとにユーザー認証をする必要がないため、各製品にスムーズにアクセスできます。

シングルサインオン機能に対応している Hitachi Ops Center 製品は次のとおりです。

- Hitachi Ops Center Automator
- Hitachi Ops Center Viewpoint

シングルサインオンのユーザー情報は、Common Services で一元管理されるため、ユーザーの作成、削除および変更は Hitachi Ops Center Portal から操作できます。



ヒント Common Services のシングルサインオン機能を使用しないで Hitachi Ops Center 製品を運用することもできます。この場合のインストールやセットアップの手順については、使用する Hitachi Ops Center 製品のマニュアルを参照してください。

1.2.1 Active Directory または LDAP サーバとの連携

Common Services では、外部の Active Directory または LDAP サーバと連携することで、Hitachi Ops Center を利用するためのユーザー認証を Active Directory または LDAP サーバで一元的に行うことができます。Active Directory または LDAP サーバとの連携は、Hitachi Ops Center Portal 上で設定できます。

Common Services が連携できるサーバは次のとおりです。

- Active Directory サーバ
- LDAPv3 および LDAPS をサポートする LDAP サーバ

Active Directory または LDAP サーバとの連携は、1 つだけ設定できます。Active Directory サーバの連携と LDAP サーバの連携の両方を設定することはできません。

Common Services の Active Directory または LDAP サーバとの連携には、次の条件があります。

Active Directory サーバの場合

- ・ 認証プロトコルは、LDAP(S)および Kerberos の両方をサポートしています。
- ・ Kerberos 認証の場合、レルム（領域）は 1 つだけ設定できます。
- ・ ベース DN の配下のオブジェクトのうち、objectclass が person のオブジェクトを Common Services のユーザーとします。
- ・ Hitachi Ops Center Portal へのログインには、Active Directory の sAMAccountName をユーザー ID として使用します。
- ・ ベース DN の配下の任意のグループを指定して、Common Services のユーザーグループとしてインポートできます。

LDAP サーバの場合

- ・ 認証プロトコルは、LDAP(S)だけサポートしています。
- ・ LDAP サーバからインポートできるユーザー数は 100 件です。
インポート対象のユーザーは、LDAP 属性で検索条件をフィルタリングすることで絞り込みできます。
- ・ LDAP サーバと Common Services とのユーザーグループの同期機能は非サポートです。



メモ

- ・ Hitachi Ops Center Viewpoint を使用する場合は、mail 属性にメールアドレスが設定されている必要があります。
- ・ Common Services のローカルユーザーと同じユーザー ID またはメールアドレスを持つユーザーは、Hitachi Ops Center Portal にログインできません。
連携する前に Hitachi Ops Center Portal でローカルユーザーを削除するか、ローカルユーザーのメールアドレスを変更する必要があります。
- ・ LDAP サーバの証明書の有効期限が切れた場合、Common Services のローカルユーザーを含めたすべてのユーザーが Hitachi Ops Center Portal にログインできなくなります。
これを防ぐには、有効期限が切れる前に LDAP サーバの証明書を更新し、その証明書を Common Services のトラストストアにインポートする必要があります。

Active Directory または LDAP サーバとの連携の設定手順、ユーザーやユーザーグループの詳細については、Hitachi Ops Center Portal のオンラインヘルプを参照してください。

1.2.2 ID プロバイダーとの連携

Common Services では、外部の ID プロバイダーと連携することで、Hitachi Ops Center を利用するためのユーザー認証を ID プロバイダーで一元的に行うことができます。ID プロバイダーが提供する多要素認証の機能を利用することもできます。

ID プロバイダーと連携すると、Hitachi Ops Center Portal へのログイン時に ID プロバイダー側でユーザー認証を行えます。ID プロバイダーのユーザー認証に成功すると、ユーザーが Common Services のローカルユーザーとしてインポートされます。

Common Services では、AD FS (Active Directory Federation Services) との連携をサポートしています。AD FS との連携設定は、AD FS サーバと Hitachi Ops Center Portal の両方で行います。設定手順については、[5 ID プロバイダーとの連携](#)を参照してください。



メモ

- 1つの Active Directory サーバに対して、ディレクトリサービスの連携と AD FS の連携の両方を設定することはできません。
- Common Services のローカルユーザーと同じユーザー ID またはメールアドレスを持つユーザーは、Hitachi Ops Center Portal にログインできません。
連携する前に Hitachi Ops Center Portal でローカルユーザーを削除するか、ローカルユーザーのメールアドレスを変更する必要があります。

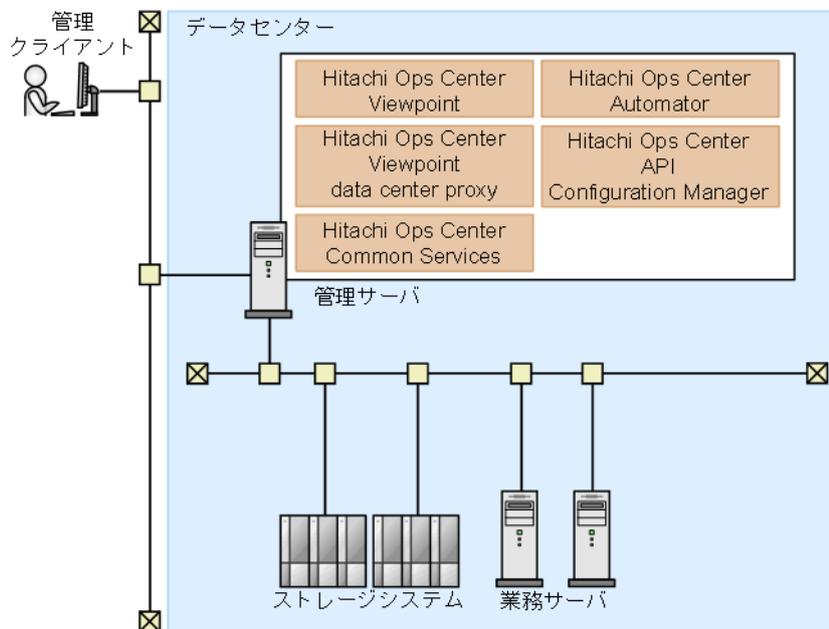
1.3 Hitachi Ops Center のシステム構成例

Hitachi Ops Center のシステムは、利用するソフトウェア、管理対象のリソースの規模などに応じて、1台または複数台の管理サーバから構成されます。Common Services は1台の管理サーバで稼働し、各製品は Common Services に登録することで共通基盤の機能を利用できます。

Hitachi Ops Center の基本的なシステム構成例と、推奨するインストール方法について説明します。

1.3.1 1台の管理サーバで運用する場合の構成例

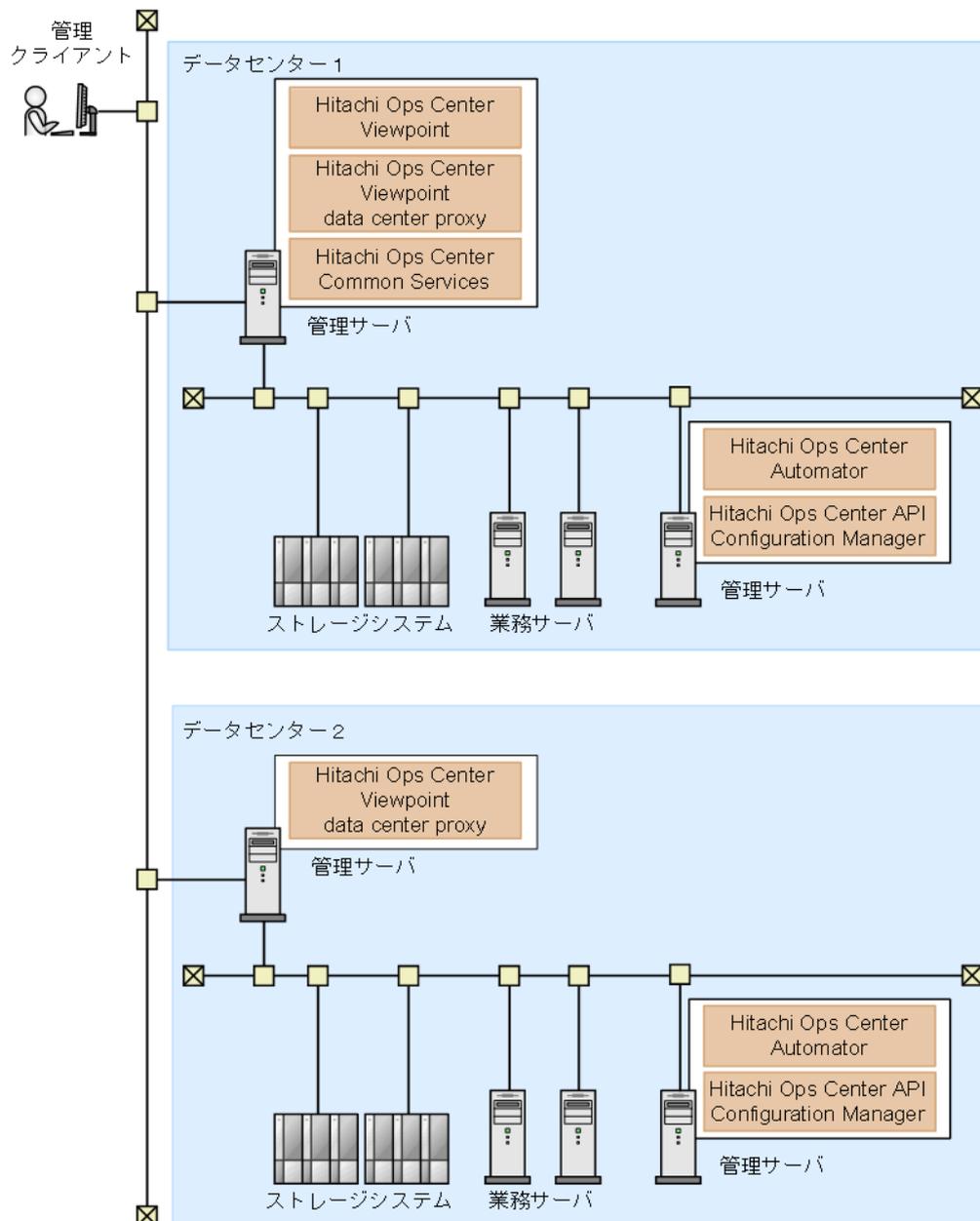
1台の管理サーバで Hitachi Ops Center 製品を運用する場合のシステム構成例を次に示します。



管理サーバに必要な製品をインストールします。シングルサインオン機能を使用する場合は、Common Services もインストールします。

1.3.2 複数台の管理サーバで運用する場合の構成例

大規模なデータセンターのリソースを管理する場合は、次の図に示すように、複数の管理サーバを使用した構成にすることができます。



複数のデータセンターにまたがって Hitachi Ops Center 製品を運用する場合、システムでは1つの Common Services を使用します。上記の構成例では、データセンター1で稼働する管理サーバの Common Services を使用しています。



メモ Hitachi Ops Center のシステムが複数の管理サーバで構成される場合、各管理サーバの時刻にずれがあると、Hitachi Ops Center Portal から各製品の起動に失敗します。時刻の同期を保つために、NTP を使用して時刻を自動的に修正することをお勧めします。

Hitachi Ops Center 製品のインストールとアップグレードインストール

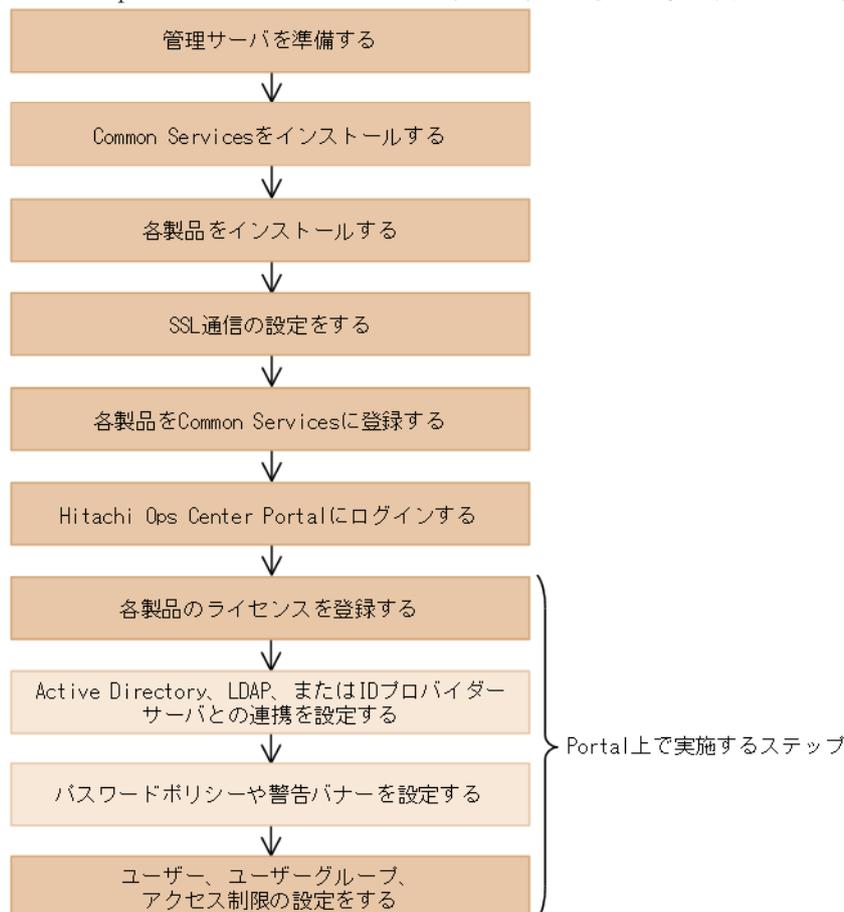
Hitachi Ops Center 製品をインストールおよびセットアップして、Hitachi Ops Center の環境を構築します。

Common Services 以外の製品のインストール方法については各製品のドキュメントを参照してください。

- 2.1 Hitachi Ops Center のインストールとセットアップの流れ
- 2.2 管理サーバを準備する
- 2.3 Common Services をインストールまたはアップグレードインストールする
- 2.4 各製品をインストールまたはアップグレードインストールする
- 2.5 SSL 通信の設定をする
- 2.6 Hitachi Ops Center 製品を Common Services に登録する
- 2.7 Hitachi Ops Center Portal にログインする
- 2.8 Hitachi Ops Center Portal で初期設定をする

2.1 Hitachi Ops Center のインストールとセットアップの流れ

Hitachi Ops Center のインストールとセットアップの流れを次の図に示します。



凡例：

必須 任意

アクセス制御の設定完了後は、各製品で必要な設定を行ってください。設定方法については、各製品のマニュアルを参照してください。

アップグレードインストールする場合、以前の設定は引き継がれます。Common Services に登録済みの Hitachi Ops Center 製品をアップグレードする場合、SSL 通信の設定以降のステップは実施不要です。

2.2 管理サーバを準備する

Hitachi Ops Center 製品をインストールする管理サーバが、必要な要件を満たしているか確認してください。

Common Services のシステム要件については、Common Services のソフトウェア添付資料を参照してください。そのほかの Hitachi Ops Center 製品のシステム要件については、各製品のマニュアルまたはソフトウェア添付資料を参照してください。



メモ

- 管理サーバには、企業ポリシーで規定されているウイルス検出プログラムや監視エージェントなどを除き、ほかのソフトウェア製品をインストールしないでください。
管理サーバにインストールしたソフトウェア製品と **Common Services** との間で発生した問題については、サポート対象外となります。
- **Common Services** をインストールすると、次の RPM パッケージがインストールされます。
 - Amazon Corretto 17
 - PostgreSQL 15
- Red Hat Enterprise Linux または Oracle Linux のバージョン 7 に **Common Services** をインストールする場合、PostgreSQL 15 の依存パッケージの libzstd は、**Common Services** のインストールメディアからインストールされます。
- **Common Services** は、管理サーバに作成された postgres ユーザーと postgres グループを使用して **Common Services** のサービスを起動します。
管理サーバに postgres ユーザーと postgres グループが存在しない構成はサポート対象外となります。
管理サーバのユーザーが外部認証サーバで管理されている場合、OS の起動時に **Common Services** のサービスが起動できません。

次に示すポート番号が競合していないことを確認してください。

Common Services にアクセスするポート：

443/tcp (デフォルト)

内部通信用のポート：

- 20951/tcp
- 20952/tcp
- 20954/tcp
- 20955/tcp
- 20956/tcp

必要に応じて、ファイアウォールの例外設定に **Common Services** にアクセスするポート番号を登録してください。設定方法については、OS のドキュメントを参照してください。

2.3 Common Services をインストールまたはアップグレードインストールする

インストーラーを使用して、管理サーバに **Common Services** をインストールまたはアップグレードインストールします。



メモ **Common Services** をインストールすると、Amazon Corretto 17 と PostgreSQL 15 がインストールされます。**Common Services** をアップグレードした場合、以前のバージョンでインストールされた Amazon Corretto 11 (バージョン 10.6.1 から 10.9.1)、および PostgreSQL 11 (バージョン 10.9.2 以前) は、アンインストールされずに残ります。これらのプログラムが不要な場合は、**rpm** コマンドでアンインストールしてください。アンインストールに失敗する場合、**rpm** コマンドに **--no-preun** オプションを指定してアンインストールしてください。

パッケージ名は次のとおりです。

- Amazon Corretto 11 : java-11-amazon-corretto-devel
- PostgreSQL 11 : postgresql11, postgresql11-server, postgresql11-libs

前提条件

- インストール先の管理サーバで、次のいずれかの設定がされていることを確認してください。

- 管理サーバがアクセスできる DNS サーバの情報が設定されている。
 - `hosts` ファイルにホスト名が設定されている。
- 管理サーバのホスト名が名前解決ができない場合、`Common Services` の起動に時間が掛かることがあります。
- `Hitachi Ops Center Portal` にログインしている場合は、アップグレードインストールする前に Web ブラウザーを終了してください。`Hitachi Ops Center Portal` にログインしている状態で `Common Services` をアップグレードインストールすると、`Internal Server Error` が発生する場合があります。エラーが発生した場合は、Web ブラウザーを再起動してください。
 - `Common Services` のバージョン 10.9.1 以降では、デフォルトのユーザーグループに **support-services** という名前の特種なグループが追加されます。これはシステムで予約されたグループのため、通常の用途には使用できません。そのため、バージョン 10.9.0 以前からアップグレードインストールをする場合、**support-services** グループが存在していないことを事前に確認してください。
 - `Active Directory` サーバとの連携で **support-services** グループがインポートされている場合、削除してください。また、`Hitachi Ops Center Portal` でユーザーディレクトリの [グループ DN] の設定を変更して、**support-services** グループがインポートされないようにしてください。
 - `Active Directory` サーバとの連携以外でシステム管理者が **support-services** グループを作成していた場合は、バージョン 10.9.0 以前からアップグレードインストールをする前に削除するか、名称を変更してください。



メモ **support-services** グループが存在している状態のまま、`Common Services` のバージョン 10.9.0 以前からアップグレードインストールした場合は、グループを削除または名称を変更してから、再度 `Common Services` を上書きインストールする必要があります。

操作手順

1. 管理サーバに `root` ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は `sudo` コマンドで `root` ユーザーとして実行してください。
2. インストールメディアの次の場所にある `install.sh` を実行します。
<インストールメディアのルートディレクトリ>/`COMSERV/install.sh`
3. メッセージに従って必要な項目を入力し、`Common Services` をインストールします。
インストール時に指定する項目は次の通りです。

新規インストールの場合：

- `Common Services` のインストール先
 - `Common Services` のデフォルトのインストール先は次のとおりです。
`/opt/hitachi/CommonService`
 - `Common Services` のユーザーデータは、次のユーザーデータディレクトリに格納されます。
`/var/<Common Services のインストールディレクトリ>`
- ホスト名 (FQDN 形式でも指定可) または IP アドレス
 - ここで指定したホスト名または IP アドレスが、`Hitachi Ops Center Portal` へのアクセス URL に使われます。インストール後に `Hitachi Ops Center Portal` にアク

セスするためのホスト名または IP アドレスを変更するには、**cschgconnect** コマンドを実行してください。**cschgconnect** コマンドについては、[6.5 管理サーバのホスト名または IP アドレス、ポート番号を変更する](#)を参照してください。

- ホスト名または FQDN を指定する場合、Hitachi Ops Center Portal にアクセスする Web ブラウザー、Common Services および各製品をインストールする管理サーバで、名前解決できる必要があります。
- ホスト名または FQDN を指定する場合、128 文字以内で指定してください。
- ホスト名または FQDN には、大文字は指定できません。大文字を指定した場合、小文字に変換されて登録されます。
- アクセス URL のポート番号
Common Services と Hitachi Ops Center Viewpoint を同じ管理サーバにインストールする場合、デフォルトのポート番号 443 が競合します。製品間で競合しないように、ポート番号を変更してください。Common Services のポート番号を 443 以外に変更する場合、20950 を推奨します。
- IP アドレスでのアクセスも許可するか
Hitachi Ops Center Portal へのアクセス URL にホスト名または FQDN を指定した場合に、IP アドレスでも Portal にアクセスできるようにするかどうかを指定します。
 - デフォルトの設定のままで IP アドレスでのアクセスを許可しない場合は y を指定します。
 - IP アドレスでのアクセスを許可する場合は n を指定します。
アクセス URL には、システムから取得した IP アドレスが自動的に設定されます。

アップグレードインストールまたは上書きインストールの場合：

- Common Services のデータベースをバックアップするか
 - データベースのバックアップ先
 - バージョン 10.9.1 以前からアップグレードインストールする場合、ディスクの空き容量が不足しているときにインストールを続行するか中断するか
4. 入力内容、および表示されるメッセージを確認します。
問題が無ければ、[y] を入力してインストール処理を開始します。
 5. インストールが完了したメッセージを確認します。
 6. SAML プロトコルを使用して AD FS と連携を行っている場合、Common Services をバージョン 10.9.2 以前からアップグレードしたときには、アップグレード完了後に、Common Services から再取得したメタデータを AD FS に登録する必要があります。
登録の手順は下記を参照してください。
 - [5.4.3 Common Services のメタデータをエクスポートする](#)
 - [5.4.4 AD FS に Common Services を証明書利用者信頼として登録する](#)

2.4 各製品をインストールまたはアップグレードインストールする

Common Services のインストールが完了したら、ほかの製品をインストールします。インストール方法については、各製品のマニュアルを参照してください。

すでにインストールされている製品をアップグレードインストールする場合、または上書きインストールする場合、製品のインストール先はインストール前と同じです。



メモ Hitachi Ops Center Automator をバージョン 10.0 未満からアップグレードインストールする場合、SSL 通信の設定がされていることを確認してください。

2.5 SSL 通信の設定をする

Common Services は、デフォルトで SSL/TLS で通信を行います。インストール直後は、動作確認の目的で自己署名証明書を使用して SSL 通信をする設定になっています。正式なサーバ証明書を使った SSL 通信の設定をしてください。

SSL 通信の設定方法については、[4 SSL 通信の設定](#)を参照してください。

次の作業

SSL 通信の設定が完了したら、この章に戻り、次のセクションに進んでください。

2.6 Hitachi Ops Center 製品を Common Services に登録する

Common Services が提供するポータル画面、ユーザー管理、シングルサインオンなどの機能を利用する場合、`setupcommonservice` コマンドを実行して、各製品を Common Services に登録します。



メモ `setupcommonservice` コマンドを使用して Hitachi Ops Center 製品を削除することはできません。製品の削除は、Hitachi Ops Center Portal で行います。

Common Services に各製品を登録する必要がない場合、[2.7 Hitachi Ops Center Portal にログインする](#)に進んでください。

前提条件

- 各製品で Common Services がインストールされている管理サーバのホスト名が名前解決できることを確認してください。FQDN 以外のホスト名を使用する場合は、名前解決のために `/etc/hosts` ファイルに IP アドレスとホスト名を設定してください。ホスト名の代わりに IP アドレスを使用する場合は、Common Services がインストールされている管理サーバで `cschgconnect.sh` コマンドを実行します。
- Common Services および各製品の管理サーバが起動されている必要があります。
- `setupcommonservice` コマンドで指定する Common Services のユーザーアカウントは、`opscenter-administrator` グループに所属するユーザーを指定してください。



メモ Common Services のホスト名、IP アドレス、または管理サーバのポート番号を変更する場合は、各製品を Common Services に再登録する必要があります。

各製品の `setupcommonservice` コマンドの格納先、構文、および実行例を次に示します。

Hitachi Ops Center Automator

Linux の場合：

デフォルトの格納先：`/opt/hitachi/Automation/bin/`

コマンド構文：

```
setupcommonservice {[-csUri <Common Services の URL > | -csUri <Common Services の URL > -csUsername <Common Services のユーザー ID >] [-appName <
```

```
Portal に表示する製品名 >] [-appDescription < Portal に表示する説明 >] [-auto]
| -help}
```

コマンド実行例：

```
setupcommonservice -csUri https://example.com/portal -appName
MyAutomator1
```

Windows の場合：

デフォルトの格納先：< Program Files フォルダ >%hitachi%\Automation\bin\

コマンド構文：

```
setupcommonservice {[/csUri < Common Services の URL > | /csUri < Common
Services の URL > /csUsername < Common Services のユーザー ID >] [/appName <
Portal に表示する製品名 >] [/appDescription < Portal に表示する説明 >] [/auto]
| /help}
```

コマンド実行例：

```
setupcommonservice /csUri https://example.com/portal /appName
MyAutomator1
```

Hitachi Ops Center Viewpoint

デフォルトの格納先：/opt/hitachi/analyzer_viewpoint/bin/

コマンド構文：

```
setupcommonservice --csUri < Common Services の URL >
```

コマンド実行例：

```
setupcommonservice --csUri https://example.com
```

Hitachi Ops Center Viewpoint data center proxy

デフォルトの格納先：/opt/hitachi/data_center_proxy/bin/

コマンド構文：

```
setupcommonservice [--applicationName < Portal に表示する製品名 >] --cs-uri
< Common Services の URL > [--dataCenterProxyUri < Viewpoint data center
proxy の URL >] [--tlsVerify] --cs-username < Common Services のユーザー ID >
```

コマンド実行例：

```
setupcommonservice --cs-uri https://example.com --cs-username sysadmin
```

2.7 Hitachi Ops Center Portal にログインする

Web ブラウザーから Hitachi Ops Center Portal にログインします。

前提条件

操作画面が正しく表示されない場合があるため、Web ブラウザーで次の設定を行ってください。

- Cookie を許可するか、Portal のアクセス URL を信頼済みサイトに登録する。
- セキュリティの設定でアクティブスクリプトを許可する。

操作手順

1. Web ブラウザーから次の URL にアクセスします。
https://<Portal のホスト名または IP アドレス>:<ポート番号>/portal/
インストール時に指定したホスト名または IP アドレス、およびポート番号でアクセスします。
2. 次のビルトインアカウントでログインします。
ユーザー ID : sysadmin
パスワード : sysadmin
Hitachi Ops Center Portal のメインウィンドウが開きます。



メモ セキュリティ面を考慮して、ビルトインアカウントのパスワードは必ず変更してください。

2.8 Hitachi Ops Center Portal で初期設定をする

Hitachi Ops Center 製品を新規インストールした後に、Hitachi Ops Center Portal 上で次の設定を構成する必要があります。



メモ アップグレードインストールした場合は、以前の設定が引き継がれます。

次の必要な設定を行ってください。

- 製品のライセンスを適用する
製品を使用する前に、製品のライセンスを適用する必要があります。
- ユーザーの作成、ユーザーグループの設定をする
Hitachi Ops Center Portal へのアクセスを制御するために、設定が必要です。

次の設定は、必要に応じて行ってください。

- Active Directory、LDAP、または ID プロバイダーサーバとの連携を設定する
Active Directory または LDAP については [1.2.1 Active Directory または LDAP サーバとの連携](#)、ID プロバイダーについては [1.2.2 ID プロバイダーとの連携](#) を参照してください。
- パスワードポリシーを設定する
セキュリティ要件に基づいて、ユーザーアカウントのパスワードの複雑さや、認証に連続して失敗したときのロックの制御を設定できます。
- Hitachi Ops Center Portal の警告バナーを設定する
Hitachi Ops Center Portal のログイン画面にメッセージを表示することができます。

詳細については、Hitachi Ops Center Portal のオンラインヘルプを参照してください。

Hitachi Ops Center 製品のアンインストール

Hitachi Ops Center の環境を廃棄する場合、製品をアンインストールします。Common Services 以外の製品のアンインストール方法については、各製品のドキュメントを参照してください。

- [3.1 Common Services をアンインストールする](#)

3.1 Common Services をアンインストールする

Common Services は次の手順でアンインストールします。



メモ Common Services をアンインストールしても、Amazon Corretto 17 および PostgreSQL 15 はアンインストールされません。また、Common Services を以前のバージョンからアップグレードしていた場合は、Amazon Corretto 11 (バージョン 10.6.1 から 10.9.1)、および PostgreSQL 11 (バージョン 10.9.2 以前) が管理サーバにインストールされている可能性があります。これらのプログラムが不要な場合、**rpm** コマンドでアンインストールしてください。アンインストールに失敗する場合、**rpm** コマンドに `--nopreun` オプションを指定してアンインストールしてください。

各プログラムのパッケージ名は次のとおりです。

- Amazon Corretto 17 : `java-17-amazon-corretto-devel`
- Amazon Corretto 11 : `java-11-amazon-corretto-devel`
- PostgreSQL 15 : `postgresql15`, `postgresql15-server`, `postgresql15-libs`
- PostgreSQL 11 : `postgresql11`, `postgresql11-server`, `postgresql11-libs`

前提条件

Common Services をアンインストールする前に、次の操作を実施してください。

- 必要に応じてバックアップを取得する。
- Common Services に登録されている製品がある場合、Hitachi Ops Center Portal にログインして、すべての製品の登録を解除する。

操作手順

1. 管理サーバに `root` ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は `sudo` コマンドで `root` ユーザーとして実行してください。
2. ルートディレクトリに移動します。
3. 次のコマンドを実行します。

```
<Common Services のインストールディレクトリ>/inst/uninstall.sh
```

SSL 通信の設定

インストールが完了したら、SSL セットアップツール (`cssslsetup` コマンド) の実行、または手動で必要な手順を実行して SSL 通信の設定を行います。Common Services はデフォルトで自己署名証明書を使用して SSL/TLS 通信を行います。正式なサーバ証明書を使った SSL 通信の設定をしてください。

SSL 通信の設定方法は、次のとおりです。

- 各製品に対して SSL セットアップツール (`cssslsetup` コマンド) を実行する場合は、[4.1 SSL セットアップツールを使用した SSL 通信の設定](#)の手順に従い設定をします。
- SSL 通信を手動で設定する場合、または公開鍵の暗号化方式に RSA と楕円曲線暗号 (ECDSA) の両方を使用する場合は、[4.2 SSL セットアップツールを使用しない SSL 通信の設定](#)の手順に従い設定をします。

□ 4.1 SSL セットアップツールを使用した SSL 通信の設定

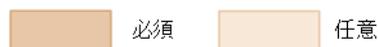
□ 4.2 SSL セットアップツールを使用しない SSL 通信の設定

4.1 SSL セットアップツールを使用した SSL 通信の設定

SSL セットアップツール (**cssslsetup** コマンド) を使用した SSL 通信の設定の流れを次の図に示します。



凡例:



- **cssslsetup** コマンドを使って、SSL 通信の設定ができる Hitachi Ops Center 製品は次のとおりです。
 - Hitachi Ops Center Common Services
 - Hitachi Ops Center Automator
 - Hitachi Ops Center Viewpoint
 - Hitachi Ops Center Viewpoint data center proxy
 - Hitachi Ops Center API Configuration Manager



メモ

- **cssslsetup** コマンドは、Common Services のソフトウェア添付資料に記載されている各製品のバージョンに対して使用できます。
- Hitachi Ops Center API Configuration Manager が root ユーザー以外のユーザーでインストールされている場合、一覧に表示されず SSL 通信の設定ができません。Hitachi Ops Center API Configuration Manager のマニュアルを参照して設定してください。
- **cssslsetup** コマンドに指定する証明書は、X.509 PEM 形式で指定します。**cssslsetup** コマンドに指定する証明書のファイルに-----BEGIN CERTIFICATE-----から-----END CERTIFICATE-----までの文字列だけが記載されていることを確認してください。それ以外の文字列が含まれていると、証明書の設定に失敗することがあります。

- **cssslsetup** コマンドは、次の場所にあります。
 - 管理サーバに Common Services をインストールしている場合：
< Common Services のインストールディレクトリ > /utility/bin
 - 管理サーバに Common Services をインストールしていない場合：
utility.tar を展開して使用します。格納場所は次のとおりです。
< Common Services のインストールメディアのルートディレクトリ > /utility.tar
cssslsetup コマンドは、utility.tar を展開した次の格納場所にあります。

<utility.tar を展開したディレクトリ>/utility/bin

- 次の設定は **cssslsetup** コマンドでは実行できません。
 - 公開鍵の暗号化方式に、RSA と楕円曲線暗号 (ECDSA) の両方を使用する設定
設定については、[4.2 SSL セットアップツールを使用しない SSL 通信の設定](#)の手順で設定してください。
 - ストレージシステムや Active Directory、LDAP、および ID プロバイダーサーバの設定

4.1.1 SSL セットアップツールが提供する機能

SSL セットアップツールは次の機能を提供します。

秘密鍵および証明書署名要求 (CSR) の作成

各製品共通で使用する秘密鍵と CSR を作成します。



メモ 暗号化方式は RSA をサポートします。RSA と楕円曲線暗号 (ECDSA) の両方を使用する場合は、[4.2 SSL セットアップツールを使用しない SSL 通信の設定](#)の手順で設定してください。

SSL サーバの設定

SSL サーバとして動作するための次の設定を行います。

製品	設定内容
Common Services	サーバ証明書と秘密鍵の登録
Automator	<ul style="list-style-type: none">• サーバ証明書と秘密鍵の登録• SSL 通信の有効化
Viewpoint	サーバ証明書と秘密鍵の登録
Viewpoint data center proxy	サーバ証明書と秘密鍵の登録
API Configuration Manager	<ul style="list-style-type: none">• サーバ証明書と秘密鍵の登録• ストレージシステム構成変更の通知受信設定

SSL クライアントの設定と証明書検証機能の有効化

SSL 通信のクライアントとして動作する場合の設定と、証明書の検証機能を有効にするための次の設定を行います。

製品	設定内容
Common Services	<ul style="list-style-type: none">• ルート証明書をトラストストアにインポートする• Active Directory、LDAP、または AD FS サーバのサーバ証明書のルート証明書をトラストストアにインポートする• 証明書検証機能を有効にする
Automator	<ul style="list-style-type: none">• ルート証明書をトラストストアにインポートする• Active Directory サーバのサーバ証明書のルート証明書をトラストストアにインポートする• 証明書検証機能を有効にする
Viewpoint	<ul style="list-style-type: none">• 信頼する証明書を Viewpoint に登録する• 証明書検証機能を有効にする

製品	設定内容
Viewpoint data center proxy	<ul style="list-style-type: none"> ルート証明書をトラストストアにインポートする 証明書検証機能を有効にする
API Configuration Manager	<ul style="list-style-type: none"> ストレージシステムの証明書検証機能を設定する SSL 通信を有効にする

証明書検証機能の有効化、無効化

SSL 通信のメンテナンスのために、証明書検証機能の有効、無効を切り替えることができます。

4.1.2 秘密鍵と証明書署名要求の作成（SSL セットアップツール）

SSL セットアップツールを使用して、Hitachi Ops Center 製品で共通に使用する秘密鍵と証明書署名要求（CSR）を作成します。



メモ 証明書の有効期限が切れている場合、または認証局により証明書が失効した場合は、証明書を更新する必要があります。このセクションの手順に従い、新しい証明書を要求して既存の証明書に上書きします。また、[「4.1.3 SSL サーバの設定 \(SSL セットアップツール\)」](#)と [4.1.6 SSL クライアントの設定と証明書検証機能の有効化 \(SSL セットアップツール\)](#) を実施する必要があります。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
2. 次の場所にある **cssslsetup** コマンドを実行します。

管理サーバに Common Services をインストールしている場合：

```
<Common Services のインストールディレクトリ>/utility/bin
```

管理サーバに Common Services をインストールしていない場合：

```
<utility.tar を展開したディレクトリ>/utility/bin
```

次のメインメニューが表示されます。

```
Main menu Ver:<cssslsetup コマンドのバージョン>
1. Create certificate signing request and private key.
2. Set up SSL server.
3. Set up SSL client.
4. Enable/disable certificate verification(optional).
5. Restart services for each product.
Enter a number or q to quit:
```

3. [1] を選択します。必要な証明書情報の入力を求められます。
 - Hitachi Ops Center 共通で使用する秘密鍵ファイルの出力先を絶対パスで指定します。
 - CSR ファイルの出力先を絶対パスで指定します。
 - RSA 暗号の署名アルゴリズムを指定します。
 - キーサイズを指定します。
 - ホスト名を指定します。
 - 組織の構成単位を指定します。
 - 組織名を指定します。
 - 市区町村名または地域名を指定します。

- 都道府県名または州名を指定します。
 - 2文字の国コードを指定します。
 - SubjectAltName のホスト名（または FQDN）と IP アドレスのいずれか、または両方を指定します。
4. 設定内容に誤りがないかを確認して、正しければ [1. Yes] を選択します。設定をやり直す場合は [2. No (Cancel)] を選択してメインメニューに戻ります。
 5. CSR が正常に作成されると、作成結果が表示され、メインメニューに戻ります。[q] を選択してコマンドを終了します。
 6. 認証局に CSR を提出し、署名済み証明書を発行するよう要求します。詳細については、認証局の手順に従ってください。
 7. 証明局によって署名されたサーバ証明書を取得したあとで、次のコマンドを実行してサーバ証明書の作成結果を確認します。

管理サーバに Common Services をインストールしている場合：

```
<Common Services のインストールディレクトリ>/openssl/bin/openssl x509 -text -in <証明書ファイルのフルパス名>
```

管理サーバに Common Services をインストールしていない場合：

```
<utility.tar を展開したディレクトリ>/utility/lib/openssl/bin/openssl x509 -text -in <証明書ファイルのフルパス名>
```

4.1.3 SSL サーバの設定（SSL セットアップツール）

SSL セットアップツールを使用して、管理サーバ上の Hitachi Ops Center 製品に対して、サーバ証明書および秘密鍵を指定します。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
2. 次の場所にある **cssslsetup** コマンドを実行します。

管理サーバに Common Services をインストールしている場合：

```
<Common Services のインストールディレクトリ>/utility/bin
```

管理サーバに Common Services をインストールしていない場合：

```
<utility.tar を展開したディレクトリ>/utility/bin
```

次のメインメニューが表示されます。

```
Main menu Ver:<cssslsetup コマンドのバージョン>
1. Create certificate signing request and private key.
2. Set up SSL server.
3. Set up SSL client.
4. Enable/disable certificate verification(optional).
5. Restart services for each product.
Enter a number or q to quit:
```

3. [2] を選択します。
インストール済みの製品の一覧が表示されます。
4. SSL サーバの設定を行う対象の製品を指定します。
複数の製品を指定する場合は、コンマで区切って指定してください。
5. Hitachi Ops Center 共通で使用する秘密鍵のファイル名を絶対パスで指定します。
6. Hitachi Ops Center 共通で使用するサーバ証明書のファイル名を絶対パスで指定します。
7. 指定したサーバ証明書が、中間認証局によって発行されたかどうかを指定します。



メモ 中間認証局で発行されたサーバ証明書を指定した場合、ファイル名に-chained が追加された証明書ファイルが作成されます。このファイルは削除しないでください。

8. 手順 7 で [Yes] を指定した場合は、中間認証局の証明書のファイル名を絶対パスで指定します。
9. Hitachi Ops Center API Configuration Manager を設定する場合、Hitachi Ops Center 共通で使用するサーバ証明書のルート証明書のファイル名を絶対パスで指定します。
10. CSR 作成時に指定したホスト名を指定します。
11. Hitachi Ops Center Automator を設定する場合、各製品で楕円曲線暗号 (ECC) 用の証明書の設定が有効のときは、ECC 用の証明書の設定を有効のままにするかどうかを指定します。
12. SSL サーバの設定を実行する場合は [1. Yes] を選択します。
設定が完了すると、メッセージが表示され、メインメニューに戻ります。
13. [5] を選択して各製品のサービスを再起動します。

4.1.4 Active Directory または LDAP サーバの SSL サーバの設定をする

Active Directory または LDAP サーバとの通信に LDAPS を利用する場合は、Active Directory または LDAP サーバで SSL サーバの設定をします。設定方法については、Active Directory または LDAP サーバのドキュメントを参照してください。

4.1.5 ID プロバイダーサーバの SSL サーバの設定をする

ID プロバイダーと連携する場合、AD FS サーバで SSL サーバの設定をします。設定方法については、AD FS サーバのドキュメントを参照してください。

4.1.6 SSL クライアントの設定と証明書検証機能の有効化 (SSL セットアップツール)

SSL セットアップツールを使用して、管理サーバ上の Hitachi Ops Center 製品に対して、SSL クライアントとして必要な設定を行い、証明書の検証機能を有効化します。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は `sudo` コマンドで root ユーザーとして実行してください。
2. 次の場所にある `cssslsetup` コマンドを実行します。

管理サーバに Common Services をインストールしている場合 :

```
< Common Services のインストールディレクトリ >/utility/bin
```

管理サーバに Common Services をインストールしていない場合 :

```
< utility.tar を展開したディレクトリ >/utility/bin
```

次のメインメニューが表示されます。

```
Main menu Ver:< cssslsetup コマンドのバージョン >
1. Create certificate signing request and private key.
2. Set up SSL server.
3. Set up SSL client.
4. Enable/disable certificate verification(optional).
5. Restart services for each product.
Enter a number or q to quit:
```

3. [3] を選択します。
4. SSL クライアントの設定を行う対象の製品を指定します。
複数の製品を指定する場合は、コンマで区切って指定してください。

5. 共通で使用するルート証明書をインポートします。
 - a. 共通で使用するルート証明書のファイル名を絶対パスで指定します。

Active Directory、LDAP、または AD FS サーバと連携する場合の設定だけを実施する場合は、何も指定しないで [Enter] を入力します。



メモ Common Services のサーバ証明書のルート証明書をインポートする必要があります。

- b. トラストストアファイル名が表示されるので、トラストストアのパスワードを指定します。ただし、Viewpoint の場合はトラストストアファイル名は表示されません。
- c. エイリアス名（サーバ識別名）を指定します。

トラストストアに同名のエイリアス名が使用されている場合、再登録を行うか確認するメッセージが表示されるので、必要に応じて再登録します。エイリアス名は大文字と小文字の区別はしません。エイリアス名を確認するには、次のコマンドを実行してください。

```
keytool -v -list -keystore <トラストストアファイルのパス>
```

6. Active Directory、LDAP、または AD FS サーバと連携する場合は、各サーバのサーバ証明書をインポートします。
 - a. Active Directory、LDAP、または AD FS サーバのサーバ証明書のファイル名を絶対パスで指定します。

Active Directory、LDAP、または AD FS サーバと連携しない場合は、何も指定しないで [Enter] を入力します。
 - b. トラストストアファイル名が表示されるので、トラストストアのパスワードを指定します。
 - c. エイリアス名（サーバ識別名）を指定します。

トラストストアに同名のエイリアス名が使用されている場合、再登録を行うか確認するメッセージが表示されるので、必要に応じて再登録します。エイリアス名は大文字と小文字の区別はしません。エイリアス名を確認するには、次のコマンドを実行してください。

```
keytool -v -list -keystore <トラストストアファイルのパス>
```

7. Hitachi Ops Center API Configuration Manager に対して、ストレージシステムとの SSL 通信の設定を行います。
 - a. 設定を行う場合は、[1. Yes] を選択します。
 - b. 設定を行う場合は、対象のストレージシステムのストレージデバイス ID を指定し、サーバ証明書のファイル名を絶対パスで指定します。
 - c. SSL 通信の設定を行うストレージシステムがほかにある場合は [1. Yes] を選択します。なければ [2. No] を選択します。
 - d. すべてのストレージシステムの登録が完了するまで、この手順を続行します。
8. 証明書検証機能を有効にするか、無効にするかを指定します。



メモ 証明書検証機能を有効にする場合は、証明書のインポートが必要です。手順 5~7 を実施してください。

証明書検証機能を無効にする場合でも、Common Services で Active Directory 連携、LDAP サーバ連携、または ID プロバイダー連携をするときは、認証連携先サーバのルート証明書のインポートが必要です。

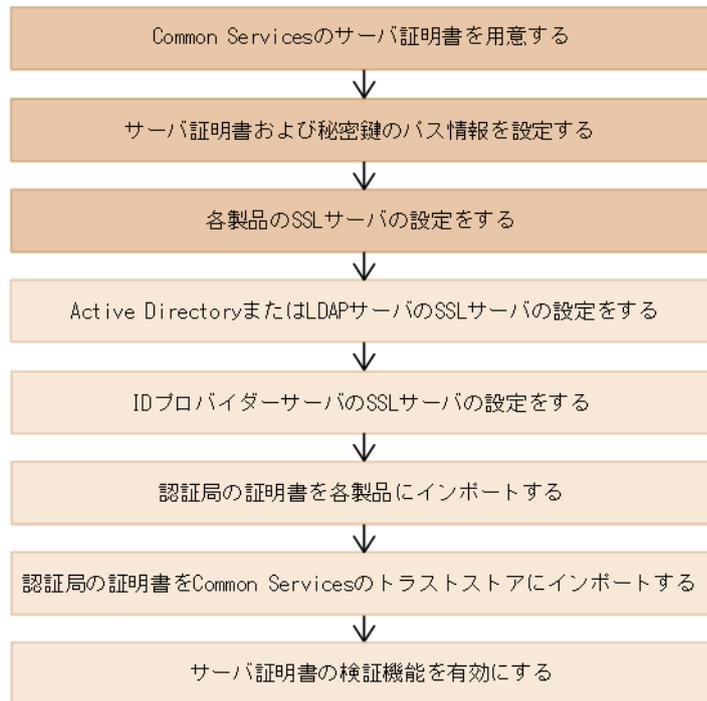
9. SSL クライアントの設定を実行する場合は [1. Yes] を選択します。
10. 設定が完了すると、メッセージが表示され、メインメニューに戻ります。[5] を選択して各製品のサービスを再起動します。

操作結果

SSL 通信の設定は完了です。

4.2 SSL セットアップツールを使用しない SSL 通信の設定

SSL セットアップツールを使用しないで、SSL 通信の設定をする流れを次の図に示します。



凡例：

 必須  任意

4.2.1 Common Services のサーバ証明書を用意する

事前に Common Services のサーバ証明書を用意します。証明書の有効期限が切れていないかどうか確認してください。確認方法については、[6.3 サーバ証明書の有効期限を確認する](#)を参照してください。Common Services では、RSA と楕円曲線暗号(ECDSA)の両方をサポートしています。ECDSA だけの設定はできません。RSA だけ、または RSA と ECDSA の両方の秘密鍵およびサーバ証明書を準備してください。



メモ Common Services で RSA と ECDSA の両方の設定をした場合、Hitachi Ops Center Automator との通信には RSA を使用します。そのほかの製品との通信には、ECDSA を使用します。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
2. 次のコマンドを実行して、X.509 PEM 形式で秘密鍵、および証明書署名要求 (CSR) を作成します。

RSA の場合の実行例：

```
<Common Services のインストールディレクトリ>/openssl/bin/openssl req -new -newkey rsa:4096 -nodes -keyout privateRSA.pem -sha256 -out serverRSA.csr -subj "/C=US/ST=xx/L=yy/O=zz/CN=<ホスト名または IP アドレス>" -addext 'subjectAltName = {DNS:<ホスト名>|IP:<IP アドレス>|
```

```
DNS:<ホスト名>,IP:<IP アドレス>}' -config <Common Services のインストールディレクトリ>/openssl/openssl.cnf
```

ECDSA の場合の実行例 :

```
<Common Services のインストールディレクトリ>/openssl/bin/openssl req -new -newkey ec:<(<Common Services のインストールディレクトリ>/openssl/bin/openssl ecparam -name secp384r1) -nodes -keyout privateECDSA.pem -sha256 -out serverECDSA.csr -subj "/C=US/ST=xx/L=yy/O=zz/CN=<ホスト名または IP アドレス>" -addext 'subjectAltName = {DNS:<ホスト名>|IP:<IP アドレス>|DNS:<ホスト名>,IP:<IP アドレス>}' -config <Common Services のインストールディレクトリ>/openssl/openssl.cnf
```

コマンド実行時には、Common Services がサポートする Cipher Suite に沿ってパラメーターを指定してください。Common Services がサポートする Cipher Suite については、Common Services のソフトウェア添付資料を参照してください。

/C=US/ST=xx/L=yy/O=zz は、ご利用の環境に応じて設定してください。CN には、Hitachi Ops Center Portal にアクセスできるホスト名 (FQDN 形式でも指定可) または IP アドレスを指定してください。

subjectAltName には、CN にホスト名を指定した場合は DNS:<ホスト名>を指定してください。CN に IP アドレスを指定した場合は、IP:<IP アドレス>を指定してください。CN にホスト名を指定し、IP アドレスでも Hitachi Ops Center Portal にアクセスできるように設定する場合は、DNS:<ホスト名>,IP:<IP アドレス>を指定してください。

Common Services のインストールディレクトリ以下にある **openssl** コマンドを使用して CSR を発行する場合、-config オプションを指定して、設定ファイルを読み込む必要があります。

3. 次のコマンドを実行して、CSR の作成結果を確認します。

```
<Common Services のインストールディレクトリ>/openssl/bin/openssl req -text -in <CSR ファイル> -config <Common Services のインストールディレクトリ>/openssl/openssl.cnf
```

4. 認証局に CSR を提出し、署名済み証明書を発行するよう要求します。詳細については、認証局の手順に従ってください。
5. 認証局が署名したサーバ証明書を手に入れたら、次のコマンドを実行して、サーバ証明書の作成結果を確認します。

```
<Common Services のインストールディレクトリ>/openssl/bin/openssl x509 -text -in <認証局が署名したサーバ証明書>
```

4.2.2 プロパティファイルにサーバ証明書および秘密鍵のパス情報を設定する

認証局から取得した署名済みのサーバ証明書および秘密鍵を Common Services のプロパティファイルに設定します。

前提条件

認証局から取得した署名済みのサーバ証明書は、次に示すとおり中間認証局の証明書とチェインして、1つのファイルにしてください。中間認証局の証明書が複数ある場合は、すべてチェインしてください。

```
awk 1 <認証局が署名したサーバ証明書> <中間認証局の証明書> [<中間認証局の証明書> ...] > <チェインしたサーバ証明書>
```

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
2. 認証局から取得した署名済みのサーバ証明書、および秘密鍵を安全な方法で管理サーバに転送します。
3. サーバ証明書、秘密鍵を次の場所に格納します。
`/var/<Common Services のインストールディレクトリ>/tls/`
4. 次のプロパティファイルに、サーバ証明書および秘密鍵の絶対パスを設定して保存します。

プロパティファイルの格納場所

```
/var/<Common Services のインストールディレクトリ>/userconf/  
config_user.properties
```

設定項目

- RSA の設定 :

```
CS_GW_SSL_CERTIFICATE=<証明書 (RSA) ファイルへの絶対パス>  
CS_GW_SSL_CERTIFICATE_KEY=<秘密鍵 (RSA) ファイルへの絶対パス>
```

- ECDSA の設定 :

```
CS_GW_SSL_CERTIFICATE_ECDSA=<証明書 (ECDSA) ファイルへの絶対パス>  
CS_GW_SSL_CERTIFICATE_KEY_ECDSA=<秘密鍵 (ECDSA) ファイルへの絶対パス>
```

5. Common Services のサービスを再起動します。



メモ すでに SSL 通信の設定が完了している環境で、ECDSA の設定を追加したり、サーバ証明書の再発行をしたりして、`config_user.properties` の設定を変更した場合は、Common Services のサービスを再起動する前に、以降の SSL 通信の設定手順で各製品および Common Services の設定を行ってください。設定を行わずに Common Services のサービスを再起動した場合、通信エラーとなるおそれがあります。

4.2.3 各製品の SSL サーバの設定をする

Common Services と連携する各製品でも SSL 通信の設定をします。Common Services と同様に認証局の署名済み証明書を準備し、SSL サーバの設定をします。

SSL サーバの設定方法については、各製品のマニュアルを参照してください。

4.2.4 Active Directory または LDAP サーバの SSL サーバの設定をする

Active Directory または LDAP サーバとの通信に LDAPS を利用する場合は、Active Directory または LDAP サーバで SSL サーバの設定をします。設定方法については、Active Directory または LDAP サーバのドキュメントを参照してください。

4.2.5 ID プロバイダーサーバの SSL サーバの設定をする

ID プロバイダーと連携する場合、AD FS サーバで SSL サーバの設定をします。設定方法については、AD FS サーバのドキュメントを参照してください。

4.2.6 認証局の証明書を各製品にインポートする

Common Services と連携する各製品に、Common Services のサーバ証明書のルート証明書をインポートします。また、ID プロバイダーとの連携設定時に、Common Services のメタデータをネットワーク経由で AD FS にインポートする場合は、AD FS サーバにも同様にインポートしてください。

い。環境によっては、認証局の証明書がすでにインポートされている可能性があります。この場合、インポートは不要です。



メモ Common Services で RSA と ECDSA の両方の設定をする場合、Hitachi Ops Center Automator には RSA のルート証明書をインポートしてください。そのほかの製品には ECDSA のルート証明書をインポートしてください。

証明書のインポート手順については、各製品のマニュアルを参照してください。

4.2.7 認証局の証明書を Common Services のトラストストアにインポートする

Common Services のトラストストアに、Common Services、および各製品のサーバ証明書のルート証明書をそれぞれインポートします。Active Directory、LDAP、または AD FS サーバと連携する場合は、それらのサーバ証明書のルート証明書もインポートします。

前提条件

各証明書を安全な方法で管理サーバに転送します。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
2. 次のコマンドを実行して、Common Services のサーバ証明書のルート証明書をトラストストアにインポートします。
環境によっては、認証局の証明書がすでにインポートされている場合があります。この場合、この手順は不要です。

書式

```
keytool -importcert -alias <エイリアス名> -keystore <トラストストアファイルのパス> -storetype jks -storepass <トラストストアファイルのパスワード> -file <インポートする認証局の証明書のパス>
```

オプション

- alias <エイリアス名>
トラストストア内で証明書を識別するための名前を指定します。
- keystore <トラストストアファイルのパス>
トラストストアファイルのパスとして、次の絶対パスを指定します。
/var/<Common Services のインストールディレクトリ>/tls/cacerts
- storepass <トラストストアファイルのパスワード>
トラストストアファイルのパスワードを指定します。デフォルトのパスワードは changeit です。



メモ トラストストアのパスワードを変更することをお勧めします。

- file <インポートする認証局の証明書のパス>
インポートする認証局の証明書の絶対パスを指定します。
3. 同様に各製品のサーバ証明書のルート証明書をトラストストアにインポートします。

4. Active Directory または LDAP サーバとの通信に LDAPS を利用する場合、Active Directory または LDAP サーバのサーバ証明書のルート証明書も同様にインポートしてください。
5. AD FS サーバと連携する場合は、AD FS サーバのサーバ証明書のルート証明書も同様にインポートしてください。
6. Common Services および各製品のサービスを再起動します。
Common Services の再起動については、[6.1 Common Services のサービスを起動、停止する](#)を参照してください。各製品のサービスの再起動方法については、各製品のマニュアルを参照してください。

4.2.8 サーバ証明書の検証機能を有効にする

Common Services のインストール直後は、Common Services が SSL クライアントとなる通信において、通信相手のサーバ証明書を検証しない設定になっています。なりすましを防止する目的で通信相手のサーバ証明書を検証するには、検証機能を有効にしてください。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は `sudo` コマンドで root ユーザーとして実行してください。
2. 次のプロパティファイルを変更して、サーバ証明書の検証機能を有効にします。

プロパティファイルの格納場所

```
/var/<Common Services のインストールディレクトリ>/userconf/  
config_user.properties
```

設定項目

```
CS_PORTAL_SSL_CERTIFICATE_CHECK=true
```

3. Common Services のサービスを再起動します。

ID プロバイダーとの連携

ID プロバイダーと連携することで、Hitachi Ops Center Portal への認証を ID プロバイダーに委譲することができます。ID プロバイダーが提供する多要素認証の機能を利用できます。

- 5.1 サポートする ID プロバイダー
- 5.2 AD FS と連携するための設定の流れ
- 5.3 AD FS と連携するための設定 (OIDC)
- 5.4 AD FS と連携するための設定 (SAML)
- 5.5 ID プロバイダーの認証用証明書の更新 (SAML)

5.1 サポートする ID プロバイダー

Common Services がサポートする ID プロバイダーを次に示します。

項目	内容
ID プロバイダー	Active Directory Federation Services (AD FS)
プロトコル	<ul style="list-style-type: none">OpenID Connect (OIDC)Security Assertion Markup Language (SAML)
OS	次の OS 上で動作する AD FS をサポートします。 <ul style="list-style-type: none">Windows Server 2016 DatacenterWindows Server 2019 DatacenterWindows Server 2022 Datacenter
連携可能な ID プロバイダーの最大数	1

5.2 AD FS と連携するための設定の流れ

次に示す流れに従って、AD FS と連携するための設定をします。

連携に使用するプロトコルによって、設定の流れが異なります。

OIDC の場合

1. AD FS に Common Services をアプリケーショングループとして登録する
2. AD FS に発行変換規則を設定する
3. AD FS の OpenID connect 検出エンドポイントを確認する
4. Common Services に AD FS を登録する
5. Hitachi Ops Center Portal に ID プロバイダーのユーザーでログインする

SAML の場合

1. AD FS のメタデータエンドポイントを確認する
2. Common Services に AD FS を登録する
3. Common Services のメタデータをエクスポートする
4. AD FS に Common Services を証明書利用者信頼として登録する
5. 要求発行ポリシーを設定する
6. Hitachi Ops Center Portal に ID プロバイダーのユーザーでログインする

Common Services で ID プロバイダーとの連携の設定をする前に、AD FS のインストールと構成が完了している必要があります。

AD FS と連携する場合、Common Services から AD FS サーバへの通信経路に対して、事前に SSL 通信の設定をする必要があります。SSL 通信の設定については、[4 SSL 通信の設定](#)を参照してください。



メモ Common Services のアクセス URL にホスト名を使用している場合は、管理サーバのホスト名が ID プロバイダーのサーバで名前解決できる必要があります。

5.3 AD FS と連携するための設定（OIDC）

OIDC プロトコルを使用して AD FS と連携する場合の設定方法について説明します。

5.3.1 AD FS に Common Services をアプリケーショングループとして登録する

AD FS に Common Services をアプリケーショングループとして登録することで、Hitachi Ops Center Portal への認証を AD FS に委譲できます。

前提条件

登録する際に、次の項目を入力する必要があります。Common Services に AD FS を登録する際にも必要となるため、事前に決定しておいてください。

- AD FS のエイリアス名
エイリアス名は、Common Services で AD FS を一意に識別するための識別子です。64 文字以内で、半角の英字（小文字のみ）、数字、ハイフン、アンダースコアの文字が使用できます。登録した値をあとで変更することはできません。

(例)

```
adfs_oidc_ad5
```

- Web API 識別子の URI
Web API 識別子は、AD FS が Common Services を一意に識別するための識別子です。任意の文字列を指定できますが、Common Services の管理サーバのホスト名など、識別しやすい名称にすることをお勧めします。

(例)

```
https://common_services_host
```

操作手順

1. AD FS サーバにログインします。
2. [スタート] - [Windows 管理ツール] - [AD FS の管理] を選択します。
3. 左側のツリーから [AD FS] - [アプリケーショングループ] を選択し、右側のペインで [アプリケーショングループ] - [アプリケーショングループの追加] をクリックします。
4. ようこそ画面で、次の項目を設定して [次へ] をクリックします。

[名前]

任意の名称を入力します。

[テンプレート]

[Web API にアクセスするサーバー アプリケーション] を選択します。

5. サーバー アプリケーション画面で、次の項目を設定して [次へ] をクリックします。

[クライアント識別子]

表示されている内容を控えておいてください。あとで Common Services に AD FS を登録する際に必要な情報です。

[リダイレクト URI]

Common Services の管理サーバのホスト名とポート番号、および AD FS のエイリアス名を次の形式で指定します。

```
https://<ホスト名>:<ポート番号>/auth/realms/opscenter/broker/<エイリアス名>/endpoint
```

<エイリアス名>には、事前に決めておいた AD FS のエイリアス名を指定します。

- アプリケーションの資格情報の構成画面で、[共有シークレットを生成する] のチェックボックスをオンにします。
[シークレット] にシークレットが表示されるので、控えておいてください。あとで Common Services に AD FS を登録する際に必要な情報です。
- [次へ] をクリックします。
- Web API の構成画面で、事前に決めておいた Web API 識別子の URI を [識別子] に指定し、[追加] をクリックします。そのあと、[次へ] をクリックします。
- アクセス制御ポリシーの選択画面で、任意のアクセス制御ポリシーを指定して [次へ] をクリックします。
- アプリケーションのアクセス許可の構成画面で、[許可されているスコープ] の次のチェックボックスをオンにして、[次へ] をクリックします。
 - [allatclaims]
 - [email]
 - [openid]
 - [profile]
- 概要画面で、設定内容に間違いがないことを確認して [次へ] をクリックします。
- 完了画面で [閉じる] をクリックします。

5.3.2 AD FS に発行変換規則を設定する

AD FS にアプリケーショングループとして登録した Common Services に対して、発行変換規則を設定します。ID プロバイダーのユーザーで Hitachi Ops Center Portal にログインした際にインポートされるユーザーの属性情報は、発行変換規則の設定に基づいて Common Services に伝達されます。

操作手順

- AD FS サーバにログインします。
- [スタート] - [Windows 管理ツール] - [AD FS の管理] を選択します。
- 左側のツリーから [AD FS] - [アプリケーション グループ] を選択します。中央のペインで Common Services のアプリケーション グループを選択して、右側のペインで [プロパティ] をクリックします。
アプリケーション グループのプロパティ画面が表示されます。
- [アプリケーション] の [<アプリケーショングループ名> - Web API] を選択して、[編集] をクリックします。
Web API のプロパティ画面が表示されます。
- 発行変換規則タブで [規則の追加] をクリックします。
変換要求規則の追加ウィザードダイアログが表示されます。
- 規則テンプレートの選択画面で、[要求規則テンプレート] に [LDAP 属性を要求として送信] を選択して、[次へ] をクリックします。
- 規則の構成画面で、次の項目を設定して [完了] をクリックします。

[要求規則名]

任意の名称を指定します。

[属性ストア]

[Active Directory] を選択します。

[LDAP 属性の出力方向の要求の種類への関連付け]

次に示す値を指定します。

LDAP 属性に指定する値	出力方向の要求の種類に指定する値
システムにメールアドレスが登録されている次の LDAP 属性のどちらか ・ User-Principal-Name ・ E-Mail-Addresses	電子メールアドレス
Given-Name	指定名
Surname	Surname
Token-Groups - ドメイン名を含む	グループ



メモ Hitachi Ops Center Portal にログインする Active Directory ユーザーのメールアドレス、名、姓がここで指定した LDAP 属性に設定されていることを確認してください。未設定の場合、そのユーザーは Hitachi Ops Center Portal へのログインに失敗します。

8. 発行変換規則タブに要求規則が追加されたことを確認して、[OK] をクリックします。

5.3.3 AD FS の OpenID connect 検出エンドポイントを確認する

Common Services に AD FS を登録するために必要な OpenID connect 検出エンドポイントを確認します。

操作手順

1. AD FS サーバにログインします。
2. [スタート] - [Windows 管理ツール] - [AD FS の管理] を選択します。
3. AD FS の OpenID connect 検出エンドポイントを確認します。

左側のツリーから [AD FS] - [サービス] - [エンドポイント] を選択して、表示されるエンドポイントの情報で、種類の値が OpenID Connect 検出となっている行の [URL パス] の値を確認します。

この URL に AD FS のベース URI を付加したものが、OpenID connect 検出エンドポイントとなります。

(例)

`https://adfs.example.com/adfs/.well-known/openid-configuration`

OpenID connect 検出エンドポイントは Common Services に AD FS を登録する際に必要なので控えておいてください。

5.3.4 Common Services に AD FS を登録する

Common Services に AD FS を ID プロバイダーとして登録します。

操作手順

1. sysadmin ユーザー、または opscenter-administrators グループに所属するユーザーで Hitachi Ops Center Portal にログインします。
2. ナビゲーションバーから [ユーザー管理] をクリックします。
3. ユーザー画面の [資産種別] から [ID プロバイダー] をクリックします。
4. ID プロバイダー画面で [+] をクリックします。
5. ウィザード形式で必要な項目を入力し、登録します。

項目	内容
プロバイダー種別	Active Directory フェデレーションサービス (AD FS) を指定します。
フェデレーションプロトコル	OpenID Connect 1.0 を指定します。
表示名	ID プロバイダーの表示名を 64 文字以内で指定します。
エイリアス	5.3.1 AD FS に Common Services をアプリケーショングループとして登録する で決めたエイリアス名と同じ値を指定します。
OpenID connect discovery エンドポイント	5.3.3 AD FS の OpenID connect 検出エンドポイントを確認する で確認した OpenID connect 検出エンドポイントを指定します。
有効	[はい] を指定した場合に有効となり、ログイン画面に [外部 ID プロバイダーを使用したログイン] というリンクが表示されます。
クライアント ID	5.3.1 AD FS に Common Services をアプリケーショングループとして登録する で表示された AD FS のクライアント識別子を指定します。
クライアントシークレット	5.3.1 AD FS に Common Services をアプリケーショングループとして登録する で表示された AD FS のシークレットを指定します。
Web API 識別子	5.3.1 AD FS に Common Services をアプリケーショングループとして登録する で決めた Web API 識別子の URI を指定します。
許容される時刻の誤差 (秒)	Common Services がインストールされている管理サーバと AD FS サーバ間で許容可能な時差を指定します。サーバ間の時差がこの値を超えると、AD FS によるログインはできなくなります。 指定可能な値は、0~300 (単位: 秒) です。 デフォルト: 300
全ユーザーに割り当てるグループの設定	ローカルユーザーグループを指定します (任意)。 AD FS のユーザー認証が成功すると、ユーザーが Common Services にローカルユーザーとしてインポートされ、この項目で指定したローカルユーザーグループが割り当てられます。 指定できるグループの数は最大 10 個です。
グループ単位のマッピングの設定	AD FS のユーザーグループとローカルグループのペアを指定します (任意)。 AD FS のユーザー認証が成功すると、ユーザーが Common Services にローカルユーザーとしてインポートされます。その際に、この項目で指定した AD FS のユーザーグループに所属している場合は、対応するローカルユーザーグループが割り当てられます。 指定できるペアの数は最大 10 個です。 AD FS のユーザーグループ名は、Windows ドメイン修飾名形式で指定してください。 (例) <code>domain%cs_admin_group</code>

5.3.5 Hitachi Ops Center Portal に ID プロバイダーのユーザーでログインする

ID プロバイダーとの連携の設定が完了したら、Web ブラウザーから ID プロバイダーのユーザーで Hitachi Ops Center Portal にログインできることを確認します。

操作手順

1. Web ブラウザーから次の URL にアクセスします。

`https://<Portal のホスト名または IP アドレス>:<ポート番号>/portal/`

2. ログイン画面で [外部 ID プロバイダーを使用したログイン] をクリックします。
ID プロバイダーのログイン画面が表示されます。
3. ID プロバイダーのユーザーでログインします。
ID プロバイダーのユーザー認証に成功すると、Hitachi Ops Center Portal にログインした状態になります。
4. 次に、sysadmin ユーザー、または opscenter-administrators グループに所属するユーザーでログインしなおし、 [ユーザー管理] - [ユーザー] を選択して、ID プロバイダーのユーザーの次の項目が正しく設定されているか確認します。
ユーザー ID、姓、名、メールアドレス、全ユーザーに割り当てるグループの設定とグループ単位のマッピングの設定で指定したユーザーグループ

操作結果

ID プロバイダーとの連携の設定は完了です。

5.4 AD FS と連携するための設定 (SAML)

SAML プロトコルを使用して AD FS と連携する場合の設定方法について説明します。

5.4.1 AD FS のメタデータエンドポイントを確認する

Common Services に AD FS を登録するために必要なメタデータエンドポイントを確認します。

操作手順

1. AD FS サーバにログインします。
2. [スタート] - [Windows 管理ツール] - [AD FS の管理] を選択します。
3. AD FS のメタデータエンドポイントを確認します。

左側のツリーから [AD FS] - [サービス] - [エンドポイント] を選択して、表示されるエンドポイントの情報で、種類の値がフェデレーション メタデータとなっている行の [URL パス] の値を確認します。

この URL に AD FS のベース URI を付加したものが、メタデータエンドポイントとなります。

(例)

```
https://adfs.example.com/FederationMetadata/2007-06/  
FederationMetadata.xml
```

エンドポイントは AD FS を Common Services に登録する際に必要なもので控えておいてください。

5.4.2 Common Services に AD FS を登録する

Common Services に AD FS を ID プロバイダーとして登録します。

操作手順

1. sysadmin ユーザー、または opscenter-administrators グループに所属するユーザーで Hitachi Ops Center Portal にログインします。
2. ナビゲーションバーから [ユーザー管理] をクリックします。
3. ユーザー画面の [資産種別] から [ID プロバイダー] をクリックします。
4. ID プロバイダー画面で [+] をクリックします。
5. ウィザード形式で必要な項目を入力し、登録します。

項目	内容
プロバイダー種別	Active Directory フェデレーションサービス (AD FS) を指定してください。
フェデレーションプロトコル	SAML 2.0 を指定してください。
表示名	ID プロバイダーの表示名を 64 文字以内で指定します。
エイリアス	ID プロバイダーを一意に識別するエイリアス名を 64 文字以内で指定します。 指定可能な文字種は、半角の英字 (小文字のみ)、数字、ハイフン、アンダースコア。 登録した値をあとで変更することはできません。
AD FS エンドポイントメタデータ URI	5.4.1 AD FS のメタデータエンドポイントを確認する で確認した AD FS のフェデレーションメタデータをインポートするためのエンドポイントを指定します。
有効	[はい] を指定した場合に有効となり、ログイン画面に [外部 ID プロバイダーを使用したログイン] というリンクが表示されます。
NameID フォーマット	AD FS のユーザーを Common Services のローカルユーザーとしてインポートする際に、ユーザー ID に使用するフォーマットを指定します。 <ul style="list-style-type: none"> Windows ドメイン修飾名 Email Unspecified
許容される時刻の誤差 (秒)	Common Services がインストールされている管理サーバと AD FS サーバ間で許容可能な時差を指定します。サーバ間の時差がこの値を超えると、AD FS によるログインはできなくなります。 指定可能な値は、0~300 (単位: 秒) です。 デフォルト: 300
全ユーザーに割り当てるグループの設定	ローカルユーザーグループを指定します。(任意) AD FS のユーザー認証が成功すると、ユーザーが Common Services にローカルユーザーとしてインポートされ、この項目で指定したローカルユーザーグループが割り当てられます。 指定できるグループの数は最大 10 個です。
グループ単位のマッピングの設定	AD FS のユーザーグループとローカルユーザーグループのペアを指定します。(任意) AD FS のユーザー認証が成功すると、ユーザーが Common Services にローカルユーザーとしてインポートされます。その際に、グループ単位のマッピングの設定で指定した AD FS のユーザーグループに所属している場合は、対応するローカルユーザーグループが割り当てられます。 指定できるペアの数は最大 10 個です。 AD FS のユーザーグループ名は、Windows ドメイン修飾名形式で指定してください。 (例) <code>domain¥cs_admin_group</code>

5.4.3 Common Services のメタデータをエクスポートする

AD FS と連携するには、AD FS に Common Services のメタデータを登録する必要があります。Hitachi Ops Center Portal でメタデータをファイルに出力して、AD FS サーバに転送します。

操作手順

1. sysadmin ユーザー、または opscenter-administrators グループに所属するユーザーで Hitachi Ops Center Portal にログインします。
2. ナビゲーションバーから [ユーザー管理] をクリックします。
3. ユーザー画面の [資産種別] から [ID プロバイダー] をクリックします。
4. ID プロバイダー画面から対象の AD FS をクリックします。
5. 詳細画面で [メタデータダウンロード] をクリックします。
Common Services のメタデータのファイルがダウンロードされます。AD FS サーバにファイルを転送してください。

5.4.4 AD FS に Common Services を証明書利用者信頼として登録する

AD FS に Common Services を証明書利用者信頼として登録することで、Hitachi Ops Center Portal への認証を AD FS に委譲できます。

操作手順

1. AD FS サーバにログインします。
2. [スタート] - [Windows 管理ツール] - [AD FS の管理] を選択します。
3. 左側のツリーから [AD FS] - [証明書利用者信頼] を選択し、右側のペインで [証明書利用者信頼] - [証明書利用者信頼の追加] をクリックします。
4. ようこそ画面で、[要求に対応する] を選択して [開始] をクリックします。
5. データソースの選択画面で、[証明書利用者についてのデータをファイルからインポートする] を選択し、[フェデレーションメタデータファイルの場所] に、Common Services のメタデータをエクスポートしたファイルを指定して、[次へ] をクリックします。
6. 表示名の指定画面で、[表示名] に任意の表示名を指定して [次へ] をクリックします。
7. アクセス制御ポリシーの選択画面で、任意のアクセス制御ポリシーを指定して [次へ] をクリックします。
8. 信頼の追加の準備完了画面で、設定内容に間違いがないことを確認して [次へ] をクリックします。
9. 完了画面で [このアプリケーションの要求発行ポリシーを構成する] のチェックボックスをオンにし、[閉じる] をクリックします。

5.4.5 要求発行ポリシーを設定する

AD FS に証明書利用者信頼として登録した Common Services に対して、要求発行ポリシーを設定します。ID プロバイダーのユーザーで Hitachi Ops Center Portal にログインした際にインポートされるユーザーの属性情報は、要求発行ポリシーの設定に基づいて Common Services に伝達されます。

操作手順

1. AD FS サーバにログインします。
2. [スタート] - [Windows 管理ツール] - [AD FS の管理] を選択します。
3. 左側のツリーから [AD FS] - [証明書利用者信頼] を選択します。中央のペインで Common Services の証明書利用者信頼を選択して、右側のペインで [要求発行ポリシーの編集] をクリックします。
要求発行ポリシーの編集ダイアログが表示されます。
4. 発行変換規則タブで [規則の追加] をクリックします。
変換要求規則の追加ウィザードダイアログが表示されます。
5. 要求規則テンプレートに [入力方向の要求を変換] を指定して、[次へ] をクリックします。
6. 次の項目を指定します。

[要求規則名]

任意の名称を指定します。

[出力方向の要求の種類]

[名前 ID] を指定します。

[入力方向の要求の種類] と [出力方向の名前 ID の形式]

[5.4.2 Common Services に AD FS を登録する](#) で NameID フォーマットに指定した値に応じて、次に示す値を指定します。

NameID フォーマットの指定値	入力方向の要求の種類に指定する値	出力方向の名前 ID の形式に指定する値
Windows ドメイン修飾名	Windows アカウント名	Windows ドメイン 修飾名
Email	システムにメールアドレスが登録されている次の LDAP 属性のどちらか ・ UPN ・ 電子メール アドレス	電子メール
Unspecified	UPN	UPN

[すべての要求値をパス スルーする]

この項目を選択してオンにします。

7. [完了] をクリックします。

要求発行ポリシーの編集ダイアログに要求規則が追加されます。ここで指定した値は、次の要求で Common Services に伝達されます。

<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier>

8. 要求発行ポリシーの編集ダイアログで、再度 [規則の追加] をクリックします。

変換要求規則の追加ウィザードダイアログが表示されます。

9. 要求規則テンプレートに [LDAP 属性を要求として送信] を指定して、[次へ] をクリックします。

10. 次の項目を指定します。

[要求規則名]

任意の名称を指定します。

[属性ストア]

Active Directory を指定します。

[LDAP 属性の出力方向の要求の種類への関連付け]

次の項目を設定します。

LDAP 属性	値
システムにメールアドレスが登録されている次の LDAP 属性のどちらか ・ User-Principal-Name ・ E-Mail-Addresses	電子メールアドレス
Given-Name	指定名
Surname	Surname
Token-Groups - ドメイン名を含む	グループ



メモ Hitachi Ops Center Portal にログインする Active Directory ユーザーのメールアドレス、名、姓がここで指定した LDAP 属性に設定されていることを確認してください。未設定の場合、そのユーザーは Hitachi Ops Center Portal へのログインに失敗します。

11. [完了] をクリックします。

要求発行ポリシーの編集ダイアログに要求規則が追加されます。ここで指定した値は、次の Claim で Common Services に伝達されます。

- 電子メールアドレス :

`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`

- 指定名 :

`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`

- Surname :

`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`

- グループ :

`http://schemas.xmlsoap.org/claims/Group`

12. 要求発行ポリシーの編集ダイアログで優先順位を次の順番になるよう変更して、[OK] をクリックします。

- [LDAP 属性を要求として送信] で指定した要求規則
- [入力方向の要求を変換] で指定した要求規則

13. [AD FS] - [サービス] - [要求記述] を選択して、設定内容に間違いがないことを確認します。

5.4.6 Hitachi Ops Center Portal に ID プロバイダーのユーザーでログインする

ID プロバイダーとの連携の設定が完了したら、Web ブラウザーから ID プロバイダーのユーザーで Hitachi Ops Center Portal にログインできることを確認します。

操作手順

1. Web ブラウザーから次の URL にアクセスします。

`https://<Portal のホスト名または IP アドレス>:<ポート番号>/portal/`

2. ログイン画面で [外部 ID プロバイダーを使用したログイン] をクリックします。

ID プロバイダーのログイン画面が表示されます。

3. ID プロバイダーのユーザーでログインします。

ID プロバイダーのユーザー認証に成功すると、Hitachi Ops Center Portal にログインした状態になります。

4. 次に、sysadmin ユーザー、または opscenter-administrators グループに所属するユーザーでログインしなおし、[ユーザー管理] - [ユーザー] を選択して、ID プロバイダーのユーザーの次の項目が正しく設定されているか確認します。

ユーザー ID、姓、名、メールアドレス、全ユーザーに割り当てるグループの設定とグループ単位のマッピングの設定で指定したユーザーグループ

操作結果

ID プロバイダーとの連携の設定は完了です。



メモ ID プロバイダーと SAML プロトコルで連携する場合は、ユーザー認証で使用する証明書を定期的に更新する必要があります。詳細については、[5.5 ID プロバイダーの認証用証明書の更新 \(SAML\)](#) を参照してください。

5.5 ID プロバイダーの認証用証明書の更新 (SAML)

ID プロバイダーとの連携で使用する Common Services の認証キーと AD FS のトークン署名について、次回更新日を確認する方法、証明書を手動で更新する方法、および証明書の更新間隔を変更する方法を説明します。

ID プロバイダーと OIDC プロトコルで連携している場合は、このセクションで説明している手順は実施不要です。

5.5.1 認証用証明書の更新の概要

ID プロバイダーとの連携では、ユーザー認証時に Common Services および AD FS が相互に保持している証明書を使用します。

Common Services の証明書を認証キー、AD FS の証明書をトークン署名と呼びます。

証明書には有効期限が設定されています。有効期限切れによる失効を防ぐため、証明書は設定された更新間隔の日数に基づき、有効期限が切れる前に自動更新されます。

しかし、証明書が自動更新されると、連携の設定時に登録した証明書と差異が発生するため、ID プロバイダーのユーザーで Common Services にログインできなくなります。この現象を防ぐため、証明書の次回更新日を確認して、有効期限が切れる前に証明書を手動で更新する必要があります。

Common Services の認証キーをすぐに更新することが難しい場合は、更新間隔の日数を延長することで、認証キーの自動更新を一時的に抑止することもできます。なお、AD FS のトークン署名も更新間隔の日数を変更できますが、現行の証明書には適用されません。変更後の更新間隔は、次回更新される証明書に適用されます。



ヒント Common Services の認証キーと AD FS のトークン署名の更新間隔を同じ日数にして、証明書の更新作業を同じ日に実施することをお勧めします。更新作業はユーザーがログインしていない時間帯（休日や夜間など）に実施してください。

5.5.2 Common Services の証明書の次回更新日を確認する

Common Services の認証キーの次回更新日を確認します。

操作手順

1. sysadmin ユーザー、または opscenter-administrators グループに所属するユーザーで Hitachi Ops Center Portal にログインします。



メモ 認証キーの次回更新日が 30 日以内の場合、ログインしたあとに次回更新日を知らせるメッセージが表示されます。

2. [設定] - [認証キー] を選択して、[認証キーの次回更新日 (UTC)] の表示内容を確認します。

5.5.3 AD FS の証明書の次回更新日を確認する

AD FS のトークン署名の次回更新日を確認します。

操作手順

1. AD FS サーバにログインします。
2. [スタート] - [Windows 管理ツール] - [AD FS の管理] を選択します。
3. 左側のツリーから [AD FS] - [サービス] - [証明書] を選択します。
4. 中央のペインで [トークン暗号化解除] と [トークン署名] の [有効期限] の表示内容を確認します。

5.5.4 Common Services の証明書を更新する

Common Services の認証キーの次回更新日が近付いていたら、認証キーと、メタデータの更新を実施します。認証キーの更新間隔の変更だけをすることもできます。

操作手順

1. sysadmin ユーザー、または opscenter-administrators グループに所属するユーザーで Hitachi Ops Center Portal にログインします。
2. [設定] - [認証キー] を選択します。
認証キー画面が表示されます。
3. 認証キーの更新間隔を変更する場合は、[認証キーの更新間隔 (日数)] を変更します。
デフォルトは 180 日で設定されています。90 日から 3650 日の間で変更できます。セキュリティの観点から認証キーの更新間隔は 90 日から 180 日を推奨します。
4. [認証キーの即時更新] に [はい] を選択します。
認証キーは更新しないで、更新間隔の変更だけをする場合は [いいえ] を選択します。
5. [実行] をクリックします。
[認証キーの即時更新] に [いいえ] を選択した場合は、以降の手順は実施不要です。
6. Common Services のメタデータをエクスポートします。エクスポートする方法については、[5.4.3 Common Services のメタデータをエクスポートする](#)を参照してください。
7. AD FS サーバにログインします。
8. [スタート] - [Windows 管理ツール] - [AD FS の管理] を選択します。
9. 左側のツリーから [AD FS] - [証明書利用者信頼] を選択します。
10. [証明書利用者信頼] で、登録されている Common Services の [識別子] の内容を確認します。
11. PowerShell で次のコマンドを実行します。

```
Update-AdfsRelyingPartyTrust -MetadataFile <メタデータファイルの格納先> -  
TargetIdentifier <証明書利用者信頼の識別子>
```

<証明書利用者信頼の識別子>には、前の手順で確認した Common Services の [識別子] の内容を指定します。

コマンド実行例：

```
Update-AdfsRelyingPartyTrust -MetadataFile metadata.xml -  
TargetIdentifier https://www.example.com:8443/auth/realms/  
opscenter
```

コマンドの詳細については、AD FS のマニュアルを参照してください。

5.5.5 AD FS の証明書を更新する

AD FS の **Update-AdfsCertificate** コマンドで、トークン署名を更新します。証明書を更新したあと、Hitachi Ops Center Portal で AD FS のメタデータエンドポイントを指定して Common Services に登録された AD FS の情報を更新します。



メモ トークン署名およびコマンドの詳細については、AD FS のマニュアルを参照してください。

操作手順

1. AD FS サーバにログインします。
2. トークン署名の更新間隔を変更する場合は、PowerShell で次のコマンドを実行します。

```
Set-AdfsProperties -CertificateDuration <更新間隔 (日数)>
```

変更後の更新間隔は、トークン署名を次回更新したときに反映されます。

更新間隔を 3 年に変更する場合のコマンド実行例：

```
Set-AdfsProperties -CertificateDuration 1095
```

3. 更新間隔を即時変更したい場合は、PowerShell で次のコマンドを実行して、トークン署名を更新します。

```
Update-AdfsCertificate -CertificateType Token-Decrypting -Urgent  
Update-AdfsCertificate -CertificateType Token-Signing -Urgent
```

4. sysadmin ユーザー、または opscenter-administrators グループに所属するユーザーで Hitachi Ops Center Portal にログインします。
5. ナビゲーションバーから [ユーザー管理] をクリックします。
6. ユーザー画面の [資産種別] から [ID プロバイダー] をクリックします。
7. 登録済みの ID プロバイダーにある [編集] のアイコンをクリックします。
8. [AD FS エンドポイントメタデータ URI] に、AD FS のメタデータエンドポイントを指定します。
メタデータエンドポイントの確認方法については、[5.4.1 AD FS のメタデータエンドポイントを確認する](#)を参照してください。
9. その他の内容は変更しないで [次へ] をクリックします。
10. ID プロバイダー編集 - 確認画面で [実行] をクリックします。

5.5.6 シングルサインオンができないときの対処

ID プロバイダーとの連携でシングルサインオンができなくなった場合、次の 2 つの原因が考えられます。

- Common Services の証明書が更新された場合
ID プロバイダーを使用してログインできない場合、AD FS のイベントログの [アプリケーションとサービス ログ] - [AD FS] - [Admin] に次のメッセージが出力されます。
「ID6013: The signature verification failed」
対処方法については、[\(1\) AD FS で Common Services のメタデータを更新する](#)を参照してください。
- AD FS の証明書が更新された場合
ID プロバイダーを使用してログインできない場合、Common Services のログファイル (デフォルトの格納先：/var/log/hitachi/CommonService/idp/log/server.log) に次のメッセージが出力されます。
「ERROR [org.keycloak.broker.saml.SAMLEndpoint] (default task-14) validation failed」
対処方法については、[\(2\) Common Services で AD FS のメタデータエンドポイントを指定する](#)を参照してください。

(1) AD FS で Common Services のメタデータを更新する

AD FS で Common Services のメタデータを更新する方法を説明します。

操作手順

1. Common Services のメタデータをエクスポートします。エクスポートする方法については、[5.4.3 Common Services のメタデータをエクスポートする](#)を参照してください。
2. AD FS サーバにログインします。
3. [スタート] - [Windows 管理ツール] - [AD FS の管理] を選択します。
4. 左側のツリーから [AD FS] - [証明書利用者信頼] を選択します。
5. [証明書利用者信頼] で、登録されている Common Services の [識別子] の内容を確認します。
6. PowerShell で次のコマンドを実行します。

```
Update-AdfsRelyingPartyTrust -MetadataFile <メタデータファイルの格納先> -  
TargetIdentifier <証明書利用者信頼の識別子>
```

<証明書利用者信頼の識別子>には、前の手順で確認した Common Services の [識別子] の内容を指定します。

コマンド実行例：

```
Update-AdfsRelyingPartyTrust -MetadataFile metadata.xml -  
TargetIdentifier https://www.example.com:8443/auth/realms/  
opscenter
```

コマンドの詳細については、AD FS のマニュアルを参照してください。

(2) Common Services で AD FS のメタデータエンドポイントを指定する

Common Services で AD FS のメタデータエンドポイントを指定する方法を説明します。

操作手順

1. sysadmin ユーザー、または opscenter-administrators グループに所属するユーザーで Hitachi Ops Center Portal にログインします。
2. ナビゲーションバーから [ユーザー管理] をクリックします。
3. ユーザー画面の [資産種別] から [ID プロバイダー] をクリックします。
4. 登録済みの ID プロバイダーにある [編集] のアイコンをクリックします。
5. [AD FS エンドポイントメタデータ URI] に、AD FS のメタデータエンドポイントを指定します。
メタデータエンドポイントの確認方法については、[5.4.1 AD FS のメタデータエンドポイントを確認する](#)を参照してください。
6. その他の内容は変更しないで [次へ] をクリックします。
7. ID プロバイダー編集 - 確認画面で [実行] をクリックします。

Hitachi Ops Center の保守

Hitachi Ops Center のシステム管理者は、サービスの起動・停止、ユーザーデータのバックアップ・リストア、アクセス URL の変更など、システムの運用、保守を実施します。

- 6.1 Common Services のサービスを起動、停止する
- 6.2 トラストストア内の証明書の有効期限を確認する
- 6.3 サーバ証明書の有効期限を確認する
- 6.4 サーバ証明書の失効状態を確認する
- 6.5 管理サーバのホスト名または IP アドレス、ポート番号を変更する
- 6.6 内部通信で使用するポート番号を変更する
- 6.7 Common Services のデータをバックアップする
- 6.8 Common Services のデータをリストアする
- 6.9 各製品との信頼関係をリセットする
- 6.10 セッションのアイドルタイムアウト設定をする
- 6.11 ウィルス検出プログラムを使用する場合に必要な設定
- 6.12 Amazon Corretto 17 をアップグレードする
- 6.13 PostgreSQL 15 をアップグレードする

6.1 Common Services のサービスを起動、停止する

Common Services のサービスを起動、停止するには、`systemctl` コマンドを使用します。

操作手順

1. 管理サーバに `root` ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は `sudo` コマンドで `root` ユーザーとして実行してください。
2. `systemctl` コマンドを実行します。

サービスを起動する

```
systemctl start csportal
```

サービスを停止する

```
systemctl stop csportal
```

サービスを再起動する

```
systemctl restart csportal
```

6.2 トラストストア内の証明書の有効期限を確認する

トラストストア内の証明書の有効期限が切れていないかどうかを確認します。

操作手順

1. 次のコマンドを実行し、キーストアパスワードを入力します。

```
<Common Services のインストールディレクトリ>/jdk/bin/keytool -list -v -  
keystore /var/<Common Services のインストールディレクトリ>/tls/cacerts
```

6.3 サーバ証明書の有効期限を確認する

管理サーバ証明書の有効期限が切れていないかどうかを確認します。



メモ 証明書の有効期限が切れている場合、証明書を更新する必要があります。[4.1.2 秘密鍵と証明書署名要求の作成 \(SSL セットアップツール\)](#) の手順に従い、新しい証明書を要求して既存の証明書に上書きします。また、SSL サーバの設定と SSL クライアントの設定を再設定する必要があります。

操作手順

1. 次のコマンドを実行します。

```
<Common Services のインストールディレクトリ>/jdk/bin/keytool -printcert -  
file <サーバ証明書のパス>
```

6.4 サーバ証明書の失効状態を確認する

Hitachi Ops Center 製品のサーバ証明書の失効状態を、OCSP (Online Certificate Status Protocol) を使用して確認します。



メモ 証明書が失効している場合、証明書を更新する必要があります。[4.1.2 秘密鍵と証明書署名要求の作成 \(SSL セットアップツール\)](#) の手順に従い、新しい証明書を要求して既存の証明書に上書きします。また、SSL サーバの設定と SSL クライアントの設定を再設定する必要があります。

前提条件

管理サーバで、次の設定がされていることを確認してください。

- OCSP レスポンダーが機能している。機能しているか不明な場合は、認証局にお問い合わせください。
- サーバ証明書に AIA (Authority Information Access) レコードがあり、OCSP レスポンダーの正しいアドレスが含まれている。
- 管理サーバから OCSP レスポンダーにアクセス可能で、プロキシなどでブロックされないこと。

AIA レコードに OCSP レスポンダーの正しいアドレスが含まれているかは `openssl` コマンドで確認します。AIA レコードの OCSP-URI 項目のアドレスを確認してください。設定されていない場合は、サーバ証明書を署名した認証局にお問い合わせください。構文および実行例を次に示します。

コマンド構文：

```
echo "Q" | <Common Services のインストールディレクトリ>/openssl/bin/openssl s_client -connect <製品の URL のホスト名または IP アドレス>:<製品の URL のポート番号> 2> /dev/null | openssl x509 -noout -text
```

コマンド実行例：

```
echo "Q" | /opt/hitachi/CommonService/openssl/bin/openssl s_client -connect example.com:443 2> /dev/null | openssl x509 -noout -text
```

サーバ証明書の失効状態は、次の方法で確認できます。

- Web ブラウザー：[6.4.1 Web ブラウザーを使用したサーバ証明書の失効確認](#)
- `openssl` コマンド：[6.4.2 コマンドを使用したサーバ証明書の失効確認](#)
- 定期的に自動でコマンドを実行：[6.4.3 定期的にサーバ証明書の失効状態を確認する](#)

6.4.1 Web ブラウザーを使用したサーバ証明書の失効確認

Web ブラウザーの OCSP チェック機能を使用して、サーバ証明書の失効状態を確認します。確認方法については、Web ブラウザーのドキュメントを参照してください。

Firefox を使用した場合の確認手順を説明します。

操作手順

1. Firefox の設定画面で、[プライバシーとセキュリティ] を選択し、[OCSP レスポンダーサーバに問い合わせで証明書の現在の正当性を確認する] のチェックボックスをオンにします。

- Firefox で、確認したい製品の URL にアクセスしエラーの確認を行います。サーバ証明書が失効している場合は SEC_ERROR_REVOKED_CERTIFICATE エラーが表示されます。



メモ Hitachi Ops Center API Configuration Manager などの Web GUI を持たない製品は、Web ブラウザーを使用した失効状態の確認はできません。[6.4.2 コマンドを使用したサーバ証明書の失効確認](#)を参照してください。

6.4.2 コマンドを使用したサーバ証明書の失効確認

`openssl` コマンドの OCSP チェック機能を使用して、サーバ証明書の失効状態を確認します。コマンドの詳細については、`openssl` のドキュメントを参照してください。

操作手順

- 管理サーバで、次の `openssl` コマンドを実行します。

コマンド構文：

```
<Common Services のインストールディレクトリ>/openssl/bin/openssl ocsp -no_nonce -issuer <issuer 証明書> -cert <サーバ証明書> -url <OCSP レスポンダーの URI > -text
```

<issuer 証明書>は、ルート証明書、または中間証明書がある場合はルート証明書と中間証明書を結合した、PEM 形式の証明書を指定してください。

コマンド実行例：

```
/opt/hitachi/CommonService/openssl/bin/openssl ocsp -no_nonce -issuer cacert.cer -cert httpsd.cer -url http://ad.example.com/ocsp -text
```

- 実行結果から Cert Status の値が good であることを確認してください。revoked の場合は、サーバ証明書は失効しています。

6.4.3 定期的にサーバ証明書の失効状態を確認する

Hitachi Ops Center 製品がインストールされている管理サーバで、`cron` を使用してサーバ証明書の失効状態を定期的に確認します。失効状態の結果はファイル、または `syslog` に出力します。

(1) 失効状態の確認結果をファイルに出力する

サーバ証明書の失効状態をファイルに出力する方法を説明します。`cron` にコマンドを登録して確認結果をファイルに出力します。

操作手順

- 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は `sudo` コマンドで root ユーザーとして実行してください。
- `crontab` ファイルを変更します。次のコマンドを実行してください。コマンドの詳細については、`crontab` のドキュメントを参照してください。

```
crontab -u root -e
```

- 失効状態の確認を行う製品ごとに、`crontab` ファイルへコマンドを追加します。追加する製品のサーバ証明書の参照方法により設定するコマンドが異なります。

Hitachi Ops Center 製品の URL からサーバ証明書をダウンロードして確認する場合：

実行時間、サーバ証明書をダウンロードするコマンド、および OCSP レスポンダーに問い合わせるコマンドを次の形式で指定します。

```
***** <サーバ証明書をダウンロードするコマンド>; <OCSP レスポンダーに問い合わせるコマンド>
```

- サーバ証明書をダウンロードするコマンド構文：

```
<Common Services のインストールディレクトリ>/openssl/bin/openssl  
s_client -connect <製品の URL のホスト名または IP アドレス>:<製品の URL  
のポート番号> [-cipher <Cipher Suite>] </dev/null 2> <標準エラー  
出力ファイルのパス> | sed -ne '/-BEGIN CERTIFICATE-/,/-END  
CERTIFICATE-/p' > <サーバ証明書のダウンロード先のパス>
```

RSA および ECDSA のサーバ証明書を両方使用している製品の場合、RSA 用のコマンドと ECDSA 用のコマンドをそれぞれ設定する必要があります。-cipher オプションには、対象の製品がサポートしている RSA または ECDSA の Cipher Suite の 1 つを指定してください。

(例)

```
ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-GCM-SHA384
```

- OCSP レスポンダーに問い合わせるコマンド構文：

```
<Common Services のインストールディレクトリ>/openssl/bin/openssl  
ocsp -no_nonce -issuer <issuer 証明書> -cert <サーバ証明書のパス>  
> -url <OCSP レスポンダーの URI> [ -proxy [http[s]://][<プロキシ  
のuserinfo >@]<プロキシのホスト名または IP アドレス>[:<プロキシのポート  
番号>] [/<プロキシのパス>] ] [-CAfile <OCSP レスポンダーサーバのルート  
証明書>] -text -out <結果出力ファイルのパス> 2>> <標準エラー出力フ  
ァイルのパス>
```

Hitachi Ops Center 製品に設定した証明書ファイルを参照して確認する場合：

実行時間と OCSP レスポンダーに問い合わせるコマンドを次の形式で指定します。

```
***** <OCSP レスポンダーに問い合わせるコマンド>
```

- OCSP レスポンダーに問い合わせるコマンド構文：

```
<Common Services のインストールディレクトリ>/openssl/bin/openssl  
ocsp -no_nonce -issuer <issuer 証明書> -cert <サーバ証明書のパス>  
> -url <OCSP レスポンダーの URI> [ -proxy [http[s]://][<プロキシ  
のuserinfo >@]<プロキシのホスト名または IP アドレス>[:<プロキシのポート  
番号>] [/<プロキシのパス>] ] [-CAfile <OCSP レスポンダーサーバのルート  
証明書>] -text -out <結果出力ファイルのパス> 2> <標準エラー出力フ  
ァイルのパス>
```



メモ

- 実行時間はコマンドごとに指定します。「*****」に値を指定してください。毎日 4 時にコマンドを実行したい場合、「04*****」で指定します。詳細は、crontab のドキュメントを参照してください。
- <結果出力ファイルのパス>と<標準エラー出力ファイルのパス>は、コマンドごとに異なるパスを指定してください。
- OCSP レスポンダーに問い合わせるコマンドの<issuer 証明書>は、ルート証明書、または中間証明書がある場合はルート証明書と中間証明書を結合した、PEM 形式の証明書を指定してください。

- OSCP レスポンダーに問い合わせるコマンドでプロキシを使用する場合、`-proxy` オプションを指定します。
- <標準エラー出力ファイル>に、`Response Verify Failure` のエラーが出力される場合は、`-CAfile` オプションを指定してください。
- `openssl` コマンドの詳細については、`openssl` のドキュメントを参照してください。

4. 各製品に対して、手順 3 の設定を繰り返してコマンドを追加します。

構成例：

```
10 4 * * * <製品 1 に対するコマンド>
20 4 * * * <製品 2 に対するコマンド>
30 4 * * * <製品 3 に対するコマンド>
...
```

5. 設定が完了したら、`crontab` ファイルを保存します。
6. 次のコマンドを実行して、`crond.service` を有効にします。

```
systemctl enable crond.service
```

7. `crond` の設定を反映するため、サービスを再起動します。次のコマンドを実行してください。

```
systemctl restart crond
```

操作結果

- 指定した時間に、<結果出力ファイルのパス>で指定したディレクトリへファイルが出力されます。出力されたファイルを参照して、`Cert Status` の値を確認してください。
 - `good` の場合：サーバ証明書は有効
 - `revoked` の場合：サーバ証明書は失効
 - `unknown` の場合：不明
- 出力ファイルに `Cert Status` の行が見つからない場合は、エラーが発生している可能性があります。エラー内容については、<標準エラー出力ファイルのパス>で指定したディレクトリに出力されたファイルを確認してください。

(2) 失効状態の確認結果を `syslog` に出力する

サーバ証明書の失効状態を `syslog` に出力する方法を説明します。

操作手順

1. 失効状態の確認を行う製品ごとに、`cron` にコマンドを登録します。設定の手順は、[\(1\) 失効状態の確認結果をファイルに出力する](#)を参照してください。`syslog` に出力する場合は、`-out` オプションは指定不要です。
2. `crond` の設定を変更します。`vi` などのテキストエディタで `crond` を開き、`CRONDARGS` の値に `-s` を追加してください。デフォルト値の場合、確認結果は `/var/log/cron` へ出力されます。

```
CRONDARGS=-s
```

3. `crond` の設定を反映するため、サービスを再起動します。次のコマンドを実行してください。

```
systemctl restart crond
```

操作結果

指定した時間に、syslog へ出力されます。syslog ファイルで Cert Status を検索します。結果は、good、revoked、または unknown になります。

6.5 管理サーバのホスト名または IP アドレス、ポート番号を変更する

管理サーバのホスト名または IP アドレスを変更する場合、または Common Services が使用するポート番号を変更する場合、**cschgconnect** コマンドを実行して、Hitachi Ops Center Portal へのアクセス URL を変更します。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
2. **cschgconnect** コマンドを実行します。

コマンドの格納場所

```
<Common Services のインストールディレクトリ>/utility/bin/  
cschgconnect.sh
```

書式

```
cschgconnect.sh [-h <ホスト名または IP アドレス>] [-p <ポート番号>] |  
-enableip {true|false} | -list
```

オプション

-h <ホスト名または IP アドレス>

Hitachi Ops Center Portal にアクセスする際のホスト名 (FQDN 形式でも指定可) または IP アドレスを指定します。ホスト名または FQDN を指定する場合、128 文字以内の文字列で指定してください。ホスト名または FQDN には、大文字は指定できません。大文字を指定した場合、小文字に変換されて登録されます。ホスト名または FQDN を指定する場合、Hitachi Ops Center Portal にアクセスする Web ブラウザー、Common Services および各製品をインストールする管理サーバで、名前解決できる必要があります。

-p <ポート番号>

Common Services が使用するポート番号を指定します。



メモ ポート番号を変更した場合は、ファイアウォールの設定も変更する必要があります。

-enableip {true|false}

Hitachi Ops Center Portal にアクセスする URL にホスト名または FQDN を使用する場合に、IP アドレスでもアクセスできるようにするかを指定します。IP アドレスでもアクセスできるようにする場合は true を、IP アドレスでアクセスできないようにする場合は false を指定します。Portal にアクセスするための IP アドレスは、システムから自動的に取得したものが使用されます。このオプションは、ほかのオプションと同時に指定できません。

-list

現在の設定内容を表示します。このオプションは、ほかのオプションと同時に指定できません。

-h、-p、-enableip オプションで設定を変更した場合、-list に表示される設定内容は Common Services のサービスを再起動するまでシステムには反映されません。



メモ このコマンドでホスト名や IP アドレスを、SSL 通信用のサーバ証明書の作成時に CN や subjectAltName に指定したもから変更した場合、サーバ証明書を発行しなおす必要があります。

3. Common Services のサービスを再起動します。
4. `cschgconnect.sh -list` を実行して、変更結果を確認します。
5. Web ブラウザーから次の URL でログイン画面にアクセスできることを確認します。
`https://<ホスト名またはIPアドレス>:<ポート番号>/Portal/`
6. Common Services に登録していた各製品で、`setupcommonservice` コマンドを再度実行します。
`setupcommonservice` コマンドについては、各製品のマニュアルを参照してください。

6.6 内部通信で使用するポート番号を変更する

Common Services が内部通信で使用するポート番号を変更することができます。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は `sudo` コマンドで root ユーザーとして実行してください。
2. ポート番号を変更します。
変更対象のポート番号に応じて、手順が異なります。

ポート番号	変更手順
20951	<ol style="list-style-type: none">1. 次のプロパティファイルに変更後のポート番号を指定して保存します。 プロパティファイルの格納場所 <code>/var/<Common Services のインストールディレクトリ>/userconf/ config_user.properties</code> 設定内容 <code>CS_PORTAL_PORT=<変更後のポート番号></code> <code>CS_GW_PORTAL_PORT=<変更後のポート番号></code>2. Common Services のサービスを再起動します。
20952	<ol style="list-style-type: none">1. 次のプロパティファイルに変更後のポート番号を指定して保存します。 プロパティファイルの格納場所 <code>/var/<Common Services のインストールディレクトリ>/userconf/ config_user.properties</code> 設定内容 <code>CS_PORTAL_IDP_PORT=<変更後のポート番号></code> <code>CS_IDP_OP_HTTP_PORT=<変更後のポート番号></code> <code>CS_GW_IDP_PORT=<変更後のポート番号></code>

ポート番号	変更手順
20954	<p>2. Common Services のサービスを再起動します。</p> <p>1. 次のプロパティファイルに変更後のポート番号を指定して保存します。</p> <p>プロパティファイルの格納場所</p> <pre data-bbox="667 322 1390 383">/var/<Common Services のインストールディレクトリ>/userconf/ config_user.properties</pre> <p>設定内容</p> <pre data-bbox="667 454 1294 483">CS_PORTAL_IDP_POSTGRESQL_PORT=<変更後のポート番号></pre> <p>2. 次の構成定義ファイルに変更後のポート番号を指定して保存します。</p> <p>構成定義ファイルの格納場所</p> <pre data-bbox="667 607 1362 667">/var/<Common Services のインストールディレクトリ>/pgdata/ csidp/data/postgresql.conf</pre> <p>設定内容</p> <pre data-bbox="667 739 1353 768">port = <変更後のポート番号> # (change requires restart)</pre> <p>3. Common Services のサービスを停止します。</p> <p>4. systemctl コマンドを実行して、postgresql-15@csidp を再起動します。</p> <p>5. Common Services のサービスを再起動します。</p>
20955	<p>1. 次のプロパティファイルに変更後のポート番号を指定して保存します。</p> <p>プロパティファイルの格納場所</p> <pre data-bbox="667 1032 1390 1093">/var/<Common Services のインストールディレクトリ>/userconf/ config_user.properties</pre> <p>設定内容</p> <pre data-bbox="667 1164 1238 1193">CS_PORTAL_POSTGRESQL_PORT=<変更後のポート番号></pre> <p>2. 次の構成定義ファイルに変更後のポート番号を指定して保存します。</p> <p>構成定義ファイルの格納場所</p> <pre data-bbox="667 1317 1362 1377">/var/<Common Services のインストールディレクトリ>/pgdata/ csportal/data/postgresql.conf</pre> <p>設定内容</p> <pre data-bbox="667 1449 1353 1478">port = <変更後のポート番号> # (change requires restart)</pre> <p>3. Common Services のサービスを停止します。</p> <p>4. systemctl コマンドを実行して、postgresql-15@csportal を再起動します。</p> <p>5. Common Services のサービスを再起動します。</p>
20956	<p>1. 次のプロパティファイルに変更後のポート番号を指定して保存します。</p> <p>プロパティファイルの格納場所</p> <pre data-bbox="667 1742 1390 1803">/var/<Common Services のインストールディレクトリ>/userconf/ config_user.properties</pre> <p>設定内容</p> <pre data-bbox="667 1874 1238 1904">CS_PORTAL_MANAGEMENT_PORT=<変更後のポート番号></pre>

ポート番号	変更手順
	2. Common Services のサービスを再起動します。

6.7 Common Services のデータをバックアップする

Common Services のデータをバックアップするには、**csbackup** コマンドを実行します。取得したバックアップデータは、インストール構成およびバージョンが同じ環境の Common Services にリストアすることができます。

操作手順

1. 必要に応じて、Common Services に登録されている各製品のバックアップを取得してください。
バックアップ方法については、各製品のマニュアルを参照してください。
2. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
3. Common Services のサービスを停止します。
4. **csbackup** コマンドを実行します。

コマンドの格納場所

<Common Services のインストールディレクトリ>/utility/bin/csbackup.sh

書式

```
csbackup.sh -dir <バックアップ先ディレクトリ>
```

オプション

```
-dir <バックアップ先ディレクトリ>
```

バックアップデータを格納するディレクトリパスを指定します。相対パスでも指定できます。指定したディレクトリに、次のファイル名でバックアップファイルが出力されます。

```
csbackup_YYYY-MM-DD-hh-mm-ss.jar
```



メモ バックアップを実行するたびにバックアップファイルが増えるため、定期的にバックアップを実行する運用では、長期間運用するとディスクスペースを圧迫するおそれがあります。不要になったバックアップファイルは削除してください。

5. サーバ証明書および秘密鍵を次に示すデフォルトの格納先以外の場所に格納している場合、サーバ証明書および秘密鍵を手動でバックアップします。

```
/var/<Common Services のインストールディレクトリ>/tls/
```



メモ **cssslsetup** コマンドで SSL 通信の設定をした場合、サーバ証明書の秘密鍵は、コマンド実行時にユーザーが指定した場所に格納されています。

6. Common Services のサービスを起動します。

6.8 Common Services のデータをリストアする

Common Services のバックアップデータをリストアするには、**csrestore** コマンドを実行します。

前提条件

リストア先のシステムの Common Services のインストール構成とバージョンが、バックアップ取得元のシステムの Common Services と同じであることを確認してください。インストール構成およびバージョンが異なるシステムには、バックアップデータをリストアできません。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
2. Common Services のサービスを停止します。
3. **csrestore** コマンドを実行します。

コマンドの格納場所

<Common Services のインストールディレクトリ>/utility/bin/csrestore.sh

書式

```
csrestore.sh -file <バックアップファイルのパス>
```

オプション

-file <バックアップファイルのパス>

リストア対象のバックアップファイルのパスを指定します。相対パスでも指定できます。

4. サーバ証明書および秘密鍵を /var/<Common Services のインストールディレクトリ>/tls/以外の場所に格納していて、手動でバックアップした場合は、バックアップ時と同じ場所にサーバ証明書と秘密鍵を配置します。



メモ バックアップ前に **cssslsetup** コマンドで SSL 通信の設定をした場合、サーバ証明書および秘密鍵は、コマンド実行時に指定した場所に配置してください。

5. リストア先の Common Services のホスト名、IP アドレス、またはポート番号が変わる場合は、**cschgconnect** コマンドを実行して、設定を変更してください。
cschgconnect コマンドについては、[6.5 管理サーバのホスト名または IP アドレス、ポート番号を変更する](#)を参照してください。
6. Common Services のサービスを起動します。
7. 必要に応じて、Common Services に登録されている各製品についてもバックアップデータをリストアしてください。
バックアップデータをリストアするための前提条件、リストアの方法については、各製品のマニュアルを参照してください。
8. Common Services に登録されている製品がある場合は、Hitachi Ops Center Portal で各製品を削除してから再登録してください。
Common Services に再登録するには、各製品ごとに **setupcommonservice** コマンドを実行してください。**setupcommonservice** コマンドについては、各製品のドキュメントを参照してください。

6.9 各製品との信頼関係をリセットする

Common Services への不正なアクセスや Common Services の各種設定に対する不正な操作が行われたことが判明した場合、Common Services と各製品との間でやり取りするトークンなどの情報が漏洩しているおそれがあります。それらの情報をリセットし、漏洩したおそれのある情報を無効化します。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
2. **csresettrustrelationship** コマンドを実行します。

コマンドの格納場所

```
< Common Services のインストールディレクトリ >/utility/bin/  
csresettrustrelationship.sh
```

書式

```
csresettrustrelationship.sh -f
```

オプション

-f

このコマンドを実行する場合に指定してください。省略した場合は、コマンドの **usage** が表示されます。

出力ファイル

実行結果が次のファイルに出力されます。

```
/var/log/hitachi/CommonService/utility/result_reset_secert.json
```



メモ

- このコマンドを実行すると、ログイン中のユーザーが強制的にログアウトされることがあります。
 - このコマンドの実行には、システム構成によって数分～数十分の時間が掛かります。
 - コマンドの実行が終了すると、Common Services が再起動されます。
-

3. 出力ファイルの内容を確認します。

resetSecretResult オブジェクト、および resetKeyResult オブジェクトの status キーの値が SUCCESS であることを確認してください。

ERROR の場合は、Common Services を再起動してコマンドを実行し直してください。再実行しても解決しない場合は、障害情報を収集して、カスタマーサポートに問い合わせてください。

4. ID プロバイダーと SAML プロトコルで連携している場合は、AD FS で Common Services のメタデータを更新します。

これは、信頼関係をリセットすると、Common Services の認証キーが強制的に更新されるためです。

手順の詳細については [\(1\) AD FS で Common Services のメタデータを更新する](#) を参照してください。

5. Common Services に登録している各製品で、**setupcommonservice** コマンドを実行します。
6. Common Services に登録している各製品のサービスを再起動します。

6.10 セッションのアイドルタイムアウト設定をする

Common Services のシングルサインオン機能を使用して Hitachi Ops Center Portal にログインした後、画面の操作をしない状態で一定の時間が経過すると、セッションがタイムアウトします。

アイドルタイムアウト設定では、次の 2 つを設定できます。

- アイドルタイムアウト時間

画面操作がない状態でタイムアウトするまでの時間を設定します。デフォルトでは 20 分に設定されています。

- 自動更新画面でタイムアウトするかどうか
自動的に表示内容が更新される画面で、画面操作がない状態でアイドルタイムアウト時間が経過した場合に、タイムアウトするかどうかを設定します。デフォルトではタイムアウトしないように設定されています。

アイドルタイムアウト設定は、Hitachi Ops Center Portal で設定できます。設定内容は、各 Hitachi Ops Center 製品に数分で適用されます。



メモ

- アイドルタイムアウト設定が適用されるのは、Common Services と各 Hitachi Ops Center 製品のバージョンが 10.9.0 以降の場合です。各 Hitachi Ops Center 製品のバージョンが 10.9.0 未満の場合、タイムアウトしない場合があります。
- セッションのタイムアウトは、設定したアイドルタイムアウト時間から数分の誤差が発生する場合があります。

6.11 ウィルス検出プログラムを使用する場合に必要な設定

ウィルス検出プログラムで Common Services が使用するデータベース関連のファイルにアクセスすると、I/O 遅延やファイル排他などによって障害が発生することがあります。障害を防止するため、Common Services の稼働中は、ウィルス検出プログラムのスキャン対象から、次のディレクトリを除外してください。

- /usr/pgsql-11/bin
- <Common Services のインストールディレクトリ>/nginx/temp
- /var/<Common Services のインストールディレクトリ>

ほかの Hitachi Ops Center 製品の対象外のディレクトリについては、各製品のマニュアルを参照してください。

6.12 Amazon Corretto 17 をアップグレードする

Amazon Corretto 17 に脆弱性が見つかった場合、Amazon Corretto 17 をアップグレードしてください。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
2. Amazon Corretto 17 をダウンロードして、Common Services がインストールされている管理サーバに配置します。
Common Services がサポートしている Amazon Corretto 17 のバージョンについては、Common Services のソフトウェア添付資料を参照してください。
3. Common Services のサービスを停止します。



メモ 管理サーバに Amazon Corretto 17 を使用する製品がインストールされている場合、その製品のサービスも必要に応じて停止してください。

4. `--nopost` オプションを付けて `rpm` コマンドを実行し、Amazon Corretto 17 をアップグレードします。
5. Common Services のサービスを起動します。



メモ 管理サーバに Amazon Corretto 17 を使用する製品がインストールされている場合、その製品のサービスも必要に応じて起動してください。

6.13 PostgreSQL 15 をアップグレードする

PostgreSQL 15 に脆弱性が見つかった場合、PostgreSQL 15 をアップグレードしてください。

操作手順

1. 管理サーバに `root` ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は `sudo` コマンドで `root` ユーザーとして実行してください。
2. PostgreSQL 15 をダウンロードして、Common Services がインストールされている管理サーバに配置します。
Common Services がサポートしている PostgreSQL 15 のバージョンについては、Common Services のソフトウェア添付資料を参照してください。
3. Common Services のサービスを停止します。
4. 次のコマンドを実行して Common Services のデータベースを停止します。

```
systemctl stop postgresql-15@csportal.service  
postgresql-15@csidp.service
```

5. `rpm` コマンドを実行して、PostgreSQL 15 の RPM パッケージをアップグレードします。

```
rpm -Uv <PostgreSQL 15 のパッケージ名> <postgresql15-libs のパッケージ名>  
> <postgresql15-server のパッケージ名>
```

6. 次のコマンドを実行して Common Services のデータベースを開始します。

```
systemctl start postgresql-15@csportal.service  
postgresql-15@csidp.service
```

7. Common Services のサービスを起動します。

トラブルシューティング

メッセージまたはログファイルを参照して、障害の要因を特定し、対処してください。障害要因を特定できない場合や、障害を回復できない場合には、Common Services の保守情報を採取して、障害対応窓口ご連絡してください。

- A.1 障害情報を収集する
- A.2 Common Services のログ
- A.3 Common Services の監査ログ
- A.4 Common Services のメッセージ
- A.5 LDAP サーバ登録時のパラメーターを決定する

A.1 障害情報を収集する

Hitachi Ops Center の運用中に障害が発生した場合、原因の解析に必要な障害情報を収集します。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
2. Common Services の障害情報を収集するため、**csgetras** コマンドを実行します。

コマンドの格納場所

```
< Common Services のインストールディレクトリ > /utility/bin/csgetras.sh
```

書式

```
csgetras.sh -dir <出力先ディレクトリのパス>
```

オプション

```
-dir <出力先ディレクトリのパス>
```

収集した障害情報を出力するディレクトリのパスを指定します。相対パスでも指定できます。

コマンドを実行すると、収集した情報を圧縮しアーカイブしたファイルが作成されます。

3. 必要に応じて、Common Services に登録されている各製品の障害情報を収集します。
障害情報の収集方法については、各製品のマニュアルを参照してください。
4. Common Services がインストールされていないサーバで実施した次の障害情報については、実施したサーバにログインして収集してください。

SSL セットアップツール (utility.tar にある **cssslsetup** コマンドを使用)

次に示すログファイルを手動で保存してください。

ログファイル	格納場所	説明
cssslsetup_YYYY-MM-DD-hh-mm-ss.log	/tmp	SSL セットアップツール (cssslsetup コマンド) 実行時のログファイルです。

A.2 Common Services のログ

Common Services では、障害発生時の要因解析のためにログファイルを出力します。

Common Services は、3 種類のログファイルを出力します。

出力先ディレクトリ

```
/var/log/hitachi/CommonService
```

ログファイル

ログファイル	説明
error.log	Common Services のエラーログが出力されるログファイルです。必要に応じて内容を確認してください。

ログファイル	説明
debug.log	障害要因が特定できない場合や障害を回復できない場合に、カスタマーサポートが要因解析を行うのに必要なログファイルです。
server.log	障害要因が特定できない場合や障害を回復できない場合に、カスタマーサポートが要因解析を行うのに必要なログファイルです。

error.log に出力される内容は次のとおりです。

項目	説明
日時	ログの出力日時が出力されます。
レベル	ログレベルが出力されます。
スレッド名	Common Services の内部処理の名称が出力されます。
メッセージ ID	メッセージ ID が出力されます。
メッセージテキスト	メッセージ ID に対応したメッセージが出力されます。
例外	発生した例外についての情報が出力されます。

メッセージ ID およびメッセージテキストの詳細については、[A.4 Common Services のメッセージ](#)を参照してください。

A.2.1 ログのプロパティを変更する

ログのプロパティを変更することで、Common Services のログ出力の動作を変更できます。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は `sudo` コマンドで root ユーザーとして実行してください。
2. 次のプロパティファイルを編集します。
`/var/<Common Services のインストールディレクトリ>/userconf/config_user.properties`
ログのプロパティを次に示します。

プロパティ	説明
CS_PORTAL_LOG_LEVEL_DEBUG	デバッグログの出力レベルを指定します。 指定できる値は、詳細度の高い順に TRACE、DEBUG、INFO のいずれかです。 デフォルト値：DEBUG
CS_PORTAL_LOG_MAX_FILESIZE	各ログファイルの最大サイズを指定します。 ログファイルのサイズが指定値を超えた場合は、新しいログファイルが作成されます。 指定できる値の形式は、整数値+単位です。 単位には KB、MB、GB を指定できます。KB を指定した場合は KiB 単位、MB を指定した場合は MiB 単位、GB を指定した場合は GiB 単位となります。単位の指定を省略した場合は、バイト単位とみなします。 デフォルト値：20MB
CS_PORTAL_LOG_MAX_INDEX_ERROR	エラーログファイルの最大バックアップ数を指定します。

プロパティ	説明
	<p>エラーログファイルのサイズが、CS_PORTAL_LOG_MAX_FILESIZE プロパティで指定した最大サイズに達すると、元のファイル名の後ろに数字がついた形式でファイルがバックアップされます。ログファイルのサイズが最大サイズに達するたびに、バックアップファイルが増え、このプロパティで指定した数までバックアップファイルが作成されます。その後は、新しいバックアップファイルが作成されるたびに最も古いバックアップファイルが削除されます。</p> <p>指定できる値の範囲は、1～21 です。</p> <p>デフォルト値：10</p>
CS_PORTAL_LOG_MAX_INDEX_DEBUG	<p>デバッグログファイルの最大バックアップ数を指定します。デバッグログファイルのサイズが、CS_PORTAL_LOG_MAX_FILESIZE プロパティで指定した最大サイズに達すると、元のファイル名の後ろに数字がついた形式でファイルがバックアップされます。ログファイルのサイズが最大サイズに達するたびに、バックアップファイルが増え、このプロパティで指定した数までバックアップファイルが作成されます。その後は、新しいバックアップファイルが作成されるたびに最も古いバックアップファイルが削除されます。</p> <p>指定できる値の範囲は、1～21 です。</p> <p>デフォルト値：20</p>
CS_PORTAL_LOG_MAX_INDEX_APPLOG	<p>サーバログファイルの最大バックアップ数を指定します。サーバログファイルのサイズが、CS_PORTAL_LOG_MAX_FILESIZE プロパティで指定した最大サイズに達すると、元のファイル名の後ろに数字がついた形式でファイルがバックアップされます。ログファイルのサイズが最大サイズに達するたびに、バックアップファイルが増え、このプロパティで指定した数までバックアップファイルが作成されます。その後は、新しいバックアップファイルが作成されるたびに最も古いバックアップファイルが削除されます。</p> <p>指定できる値の範囲は、1～21 です。</p> <p>デフォルト値：20</p>

3. Common Services のサービスを再起動します。

A.3 Common Services の監査ログ

Common Services は、いつ、だれが、何の操作をしたかの情報を監査ログとして出力できます。デフォルトでは監査ログ出力の機能は無効になっています。必要に応じて監査ログのプロパティを変更し、監査ログ出力の機能を有効にしてください。

出力先

監査ログは、syslog に出力されます。

出力項目

監査ログに出力される項目は次のとおりです。

出力箇所	項目	出力内容	出力例
PRI	プライオリティ	Facility と Log level を数値化したプライオリティ値 Facility は、監査ログの CS_PORTAL_AUDIT_FACILITY プロパティに指定した値を基に数値に変換されます。	<11>
HEADER	日時	監査事象が発生した日時	Sep 2 13:15:04
	ホスト名	監査事象が発生したホストのホスト名	WIN-00ABCD11EFG
MSG	プロセス ID	プロセス ID	5828
	スレッド ID	スレッド ID	http-nio-8081-exec-2
	ログレベル	ERROR、DEBUG などのログレベル	ERROR
	日時	監査ログの出力日時	2019-09-02T13:15:04.362+0900
	メッセージ ID	メッセージ ID	KAOP91111-E
	監査事象の種別	StartStop、Authentication などの種別	Authentication
	監査事象の結果	成功、失敗など、事象の結果	Success
	サブジェクト識別情報	ユーザー ID、URI など	User ID=system,URI=/portal
	メッセージテキスト	メッセージ	KAOP91111-E Audit Log.

メッセージ ID およびメッセージテキストの詳細については、[A.4 Common Services のメッセージ](#)を参照してください。

監査事象の種別に出力される値と、severity の関係を次に示します。監査ログのプロパティを変更することで、出力する severity を絞り込むことができます。

監査事象の種別	説明	対応する severity
Authentication	ログイン、認証に関する監査事象であることを表します。	成功時：6 失敗時：4
ConfigurationAccess	ユーザー、ユーザーグループの作成、参照、変更、削除に関する監査事象であることを表します。	成功時：6 失敗時：3

A.3.1 監査ログのプロパティを変更する

監査ログのプロパティを変更することで、Common Services の監査ログ出力の動作を変更できます。

操作手順

1. 管理サーバに root ユーザーとしてログインします。
一般ユーザーでログインする場合、以降の手順は **sudo** コマンドで root ユーザーとして実行してください。
2. 次のプロパティファイルを編集します。

/var/<Common Services のインストールディレクトリ>/userconf/
 config_user.properties
 監査ログのプロパティを次に示します。

プロパティ	説明
CS_PORTAL_AUDIT_ENABLED	<p>監査ログの取得可否を次の値で指定します。</p> <ul style="list-style-type: none"> • true : 監査ログを取得する • false : 監査ログを取得しない <p>デフォルト値 : false</p>
CS_PORTAL_AUDIT_SYSLOGHOST	<p>Common Services がインストールされている管理サーバ以外のサーバに監査ログを出力したい場合に、出力先サーバのホスト名または IP アドレスを指定します。</p> <p>デフォルト値 : localhost</p>
CS_PORTAL_AUDIT_PORT	<p>syslog サーバのポート番号を指定します。</p> <p>デフォルト値 : 514</p>
CS_PORTAL_AUDIT_FACILITY	<p>メッセージの送信元を区別するための情報を指定します。 指定できる値は次のいずれかです。</p> <ul style="list-style-type: none"> • KERN • USER • MAIL • DAEMON • AUTH • SYSLOG • LPR • NEWS • UUCP • CRON • AUTHPRIV • FTP • NTP • AUDIT • ALERT • CLOCK • LOCAL0 • LOCAL1 • LOCAL2 • LOCAL3 • LOCAL4 • LOCAL5 • LOCAL6 • LOCAL7 <p>デフォルト値 : USER</p>
CS_PORTAL_AUDIT_LEVEL	<p>監査ログの出力レベルを指定します。 指定できる値は次のいずれかです。</p> <ul style="list-style-type: none"> • DEBUG : Severity0~7 に該当するログを出力します。 • INFO : Severity0~6 に該当するログを出力します。

プロパティ	説明
	<ul style="list-style-type: none"> WARN : Severity0~4 に該当するログを出力します。 ERROR : Severity0~3 に該当するログを出力します。 デフォルト値 : INFO

3. Common Services のサービスを再起動します。

A.4 Common Services のメッセージ

Common Services が出力するメッセージについて説明します。また、エラー状態を解消するために推奨する対処を説明します。

Common Services のメッセージは、GUI、CLI、およびログファイルなどに出力されます。

出力されるメッセージは、メッセージ ID とメッセージテキストから構成されます。メッセージ ID の形式を次に示します。

プレフィックス *nnnnn-Z*

メッセージ ID は次の要素から構成されます。

プレフィックス

メッセージの出力元コンポーネントを示します。Common Services のメッセージのプレフィックスは KAOP です。

nnnnn

メッセージの通し番号を示します。

メッセージの番号と対応する機能は次のとおりです。

- KAOP10000~KAOP19999 : GUI のメッセージ
- KAOP20000~KAOP29999 : REST API のメッセージ
- KAOP60000~KAOP69999 : コマンドのメッセージ
- KAOP70000~KAOP79999 : インストーラーのメッセージ

Z

メッセージの種類を示します。メッセージの種類と意味を次に示します。

- E (Error) : 処理が続行できないエラーをユーザーに通知するメッセージです。
- W (Warning) : 処理は続行されますが、制限があることをユーザーに通知するメッセージです。
- I (Information) : ユーザーに情報を通知するメッセージです。

メッセージテキストは、GUI のメッセージを除いて英文で出力されます。

Common Services が出力するメッセージを次に示します。

メッセージ ID	メッセージテキスト	要因と対処
KAOP10000-E	予期しないエラーが発生しました。	要因 - 対処 操作を再度実行してください。それでも解決しない場合、原因究明と問題の解決には、詳細な調

メッセージID	メッセージテキスト	要因と対処
		査が必要です。障害情報を収集し、障害対応窓口 に連絡してください。
KAOP10001-E	セッションが無効です。	要因 - 対処 再ログインしてください。
KAOP10002-I	認証キーは<日付>に更新されます。	要因 ID プロバイダー連携で使用する Common Services の認証キーの有効期限が近づいていま す。 対処 表示されている日付までに、Common Services の認証キーを更新してください。
KAOP10003-W	NameID フォーマットを変更する場 合は、この ID プロバイダーからインポ ートされたすべてのユーザーを削除する 必要があります。	要因 - 対処 この ID プロバイダーからインポートされたす べてのユーザーを削除してください。
KAOP10004-E	管理者に連絡してください。ログイン ユーザー属性情報を取得できません。	要因 - 対処 操作を再度実行してください。それでも解決し ない場合、原因究明と問題の解決には、詳細な調 査が必要です。障害情報を収集し、障害対応窓口 に連絡してください。
KAOP10005-E	このアカウントは既存のローカルアカ ウントと競合します。管理者に連絡し てください。	要因 - 対処 操作を再度実行してください。それでも解決し ない場合、原因究明と問題の解決には、詳細な調 査が必要です。障害情報を収集し、障害対応窓口 に連絡してください。
KAOP10006-E	無効なユーザー名またはパスワードで す。	要因 - 対処 有効なユーザー名またはパスワードを入力して ください。
KAOP10007-E	アカウントが無効です。管理者に連絡 してください。	要因 - 対処 操作を再度実行してください。それでも解決し ない場合、原因究明と問題の解決には、詳細な調 査が必要です。障害情報を収集し、障害対応窓口 に連絡してください。
KAOP10008-W	インポートされるユーザー数が<最大 人数>を超えています。インポート されるユーザー数が 1~<最大人数> となるよう再設定してください。	要因 - 対処 インポートされるユーザー数が 1~100 となるよ う再設定してください。
KAOP10009-W	インポートされるユーザー数は 0 人で す。パラメーターを再設定してくださ い。	要因 - 対処

メッセージID	メッセージテキスト	要因と対処
		インポートされるユーザー数が1~100となるよう再設定してください。
KAOP10010-E	警告バナーの取得に失敗しました。「ログインへ戻る」をクリックしてください。同じ問題が発生する場合は管理者に連絡してください。	<p>要因 次の要因が考えられます。</p> <ul style="list-style-type: none"> ネットワークの不調。 警告バナー機能で使用する banner.json ファイルが不正です。 <p>対処 ネットワークが正常かどうかを確認してください。 banner.json ファイルが不正な場合は、次のコマンドを実行してファイルを回復してください。</p> <pre>cp -af /var/<Common Services のインストールディレクトリ>/banner/ banner.json.template /var/<Common Services のインストールディレクトリ>/ banner/banner.json</pre> <p>それでも解決しない場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口ご連絡してください。</p>
KAOP20008-E	Bad Request.	<p>要因 リクエストパラメーターに誤りがあります。</p> <p>対処 操作を再度実行してください。それでも解決しない場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。</p>
KAOP20009-E	Unauthorized.	<p>要因 認証されていません。</p> <p>対処 操作を再度実行してください。それでも解決しない場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。</p>
KAOP20011-E	Forbidden.	<p>要因 次のいずれかの原因が考えられます。</p> <ul style="list-style-type: none"> リクエストのパスに誤りがあります。 アクセス権限がありません。 <p>対処 次のいずれかで対処してください。</p> <ul style="list-style-type: none"> 正しいパスを指定してください。 アクセス権のあるユーザーで再実行してください。
KAOP20012-E	Not Found.	<p>要因 次のいずれかの原因が考えられます。</p> <ul style="list-style-type: none"> リクエストのパスに誤りがあります。 指定されたオブジェクトがありません。 <p>対処 次のいずれかで対処してください。</p> <ul style="list-style-type: none"> 正しいパスを指定してください。

メッセージID	メッセージテキスト	要因と対処
		<ul style="list-style-type: none"> 正しいオブジェクトを指定して再実行してください。
KAOP20013-E	Method Not Allowed.	<p>要因 サポートされていない HTTP メソッドが使用されました。</p> <p>対処 正しい HTTP メソッドを使用して再実行してください。</p>
KAOP20015-E	Request Timeout.	<p>要因 リクエストがタイムアウトしました。</p> <p>対処 csportal サービスが起動しているか、ネットワークが正常かどうかを確認してください。</p>
KAOP20016-E	Conflict.	<p>要因 あるオブジェクトを登録または更新操作をした際、登録済みオブジェクトの一意である属性値と重複しました。</p> <p>対処 重複した値を変更して再実行してください。</p>
KAOP20033-E	An unexpected error has occurred. Contact Support Center.	<p>要因 予期せぬエラーが発生しました。</p> <p>対処 操作を再度実行してください。それでも解決しない場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口に連絡してください。</p>
KAOP20035-E	Bad Gateway.	<p>要因 ゲートウェイが無効なレスポンスを受け取りました。</p> <p>対処 ゲートウェイが正しく動作しているか確認してください。</p>
KAOP20037-E	Gateway Timeout.	<p>要因 ゲートウェイがタイムアウトしました。</p> <p>対処 ゲートウェイとネットワークが正しく動作しているか確認してください。</p>
KAOP20047-E	The built-in role (<orion.portal.builtin-object.role.role-userのプロパティ値>) cannot be removed.	<p>要因 ユーザーグループからのビルトインオブジェクトの opscenter-user ロールを削除しようとした。</p> <p>対処 ユーザーグループから、ビルトインロールの opscenter-user は削除できません。</p>
KAOP20048-E	The built-in group cannot be deleted.	<p>要因 ビルトインオブジェクトの opscenter-administrators または opscenter-users ユーザーグループを削除しようとした。</p> <p>対処</p>

メッセージID	メッセージテキスト	要因と対処
		ビルトインオブジェクトの opscenter-administrators または opscenter-users ユーザーグループは削除できません。
KAOP20049-E	The built-in user cannot be deleted.	要因 ビルトインオブジェクトの sysadmin ユーザーを削除しようとした。 対処 ビルトインユーザーの sysadmin は削除できません。
KAOP20050-E	Users cannot be removed from < <i>orion.portal.builtin-object.group.group-user</i> のプロパティ値 >.	要因 ユーザーが所属するグループから、ビルトインオブジェクトの opscenter-users ユーザーグループを削除しようとした。 対処 ユーザーが所属するユーザーグループからビルトイングループの opscenter-users は削除できません。
KAOP20051-E	An error occurred during registration of the user. Delete the registered user and then register the user again.	要因 ユーザーの追加時に予期せぬエラーが発生しました。 対処 操作を再度実行してください。それでも解決しない場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。
KAOP20052-E	An error occurred during registration of the group. Delete the registered group and then register it again.	要因 ユーザーグループの追加時に予期せぬエラーが発生しました。 対処 操作を再度実行してください。それでも解決しない場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。
KAOP20053-E	An error occurred during registration of the Active Directory. Delete the registered Active Directory and then register it again.	要因 ユーザーディレクトリの追加時に予期せぬエラーが発生しました。 対処 操作を再度実行してください。それでも解決しない場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。
KAOP20054-E	An error occurred during an update of the Active Directory. Delete the registered Active Directory and then register it again.	要因 ユーザーディレクトリの更新時に予期せぬエラーが発生しました。 対処 操作を再度実行してください。それでも解決しない場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。
KAOP20055-E	An invalid value is specified for a parameter. Revise the value, and then try again.	要因 リクエストパラメーターに誤りがあります。 対処

メッセージID	メッセージテキスト	要因と対処
		リクエストパラメーターを見直して操作を再度実行してください。
KAOP20056-E	The specified product already exists in the database. Revise the specified type, host name, or port.	要因 登録済みの製品と同じ type、hostname、port を指定して、製品の登録または更新を行いました。 対処 登録パラメーターを見直して再実行してください。
KAOP20057-E	The specified data center already exists in the database. Revise the specified name.	要因 登録済みのデータセンターと同じ name を指定して、データセンターの登録または更新を行いました。 対処 登録パラメーターを見直して再実行してください。
KAOP20058-E	The specified product is not in the database.	要因 指定した製品は存在しません。 対処 指定するパラメーターを見直して再実行してください。
KAOP20059-E	The specified data center is not in the database.	要因 指定したデータセンターは存在しません。 対処 指定するパラメーターを見直して再実行してください。
KAOP20060-W	During processing to delete the product, the product was successfully unregistered from the server, but deletion of the SSO configuration information was not reported on the product side. Delete the SSO configuration information on the product side. For details, see the product's configuration guide.	要因 Hitachi Ops Center 製品を削除した際に、Common Services からは削除されましたが、各 Hitachi Ops Center 製品側への通知が失敗しました。 対処 対処は不要です。 別の管理サーバにインストールされた Common Services と連携する場合は、各 Hitachi Ops Center 製品側で再度製品登録を行ってください。
KAOP20061-E	An unexpected error occurred. Contact the support center.	要因 予期せぬエラーが発生しました。 対処 操作を再度実行してください。それでも解決しない場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。
KAOP20062-E	Roles cannot be added to built-in groups.	要因 ビルトインオブジェクトの opscenter-administrators または opscenter-users ユーザーグループにロールを割り当てようとした。 対処 ビルトインオブジェクトの opscenter-administrators または opscenter-users

メッセージ ID	メッセージテキスト	要因と対処
		ユーザーグループにロールを割り当てることはできません。
KAOP20063-E	Roles cannot be removed from built-in groups.	要因 ビルトインオブジェクトの opscenter-administrators または opscenter-users ユーザーグループからロールを削除しようとしてしました。 対処 ビルトインオブジェクトの opscenter-administrators または opscenter-users ユーザーグループからロールを削除することはできません。
KAOP20064-E	The built-in user cannot be removed from a group.	要因 ビルトインオブジェクトの sysadmin ユーザーからユーザーグループを削除しようとしてしました。 対処 ビルトインオブジェクトの sysadmin ユーザーからユーザーグループを削除することはできません。
KAOP20065-E	The built-in user cannot be added to a group.	要因 ビルトインオブジェクトの sysadmin ユーザーにユーザーグループを追加しようとしてしました。 対処 ビルトインオブジェクトの sysadmin ユーザーにユーザーグループを追加することはできません。
KAOP20066-E	The file was not found.	要因 警告バナー機能で使用する tags.json ファイルが存在しません。 対処 Common Services を上書きインストールしてファイルを回復してください。
KAOP20067-E	A file read error occurred.	要因 警告バナー機能で使用する tags.json ファイルを読み込めません。 対処 Common Services を上書きインストールしてファイルを回復してください。
KAOP20068-E	The text is invalid.	要因 警告バナー機能で使用する banner.json ファイルが不正です。 対処 <Common Services のインストールディレクトリ>/banner/banner.json ファイルを削除した上で、Common Services を上書きインストールしてファイルを回復してください。
KAOP20069-E	The specified group already exists. Revise the specified name.	要因 登録済みのグループと同じ name を指定して、グループの登録または更新を行いました。 対処 name を見直して再実行してください。

メッセージID	メッセージテキスト	要因と対処
KAOP20070-E	The claim of idtoken was not found.	要因 予期せぬエラーが発生しました。 対処 操作を再度実行してください。それでも解決しない場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。
KAOP20071-E	The claim of userinfo was not found.	要因 予期せぬエラーが発生しました。 対処 操作を再度実行してください。それでも解決しない場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。
KAOP20075-E	The specified realm already exists in the database. Revise the specified realm.	要因 登録済みの領域と同じ領域を登録または更新を行いました。 対処 領域を重複しない値に変更して再実行してください。
KAOP20076-E	The specified realm is not in the database.	要因 指定した領域は存在しません。 対処 指定するパラメーターを見直して再実行してください。
KAOP20085-E	Update of users belonging to External Identity Provider is prohibited.	要因 ID プロバイダーに所属するユーザーを更新しようとして失敗しました。 対処 ID プロバイダーに所属するユーザーは更新できません。
KAOP20086-E	Password reset for external Identity Provider users is prohibited.	要因 ID プロバイダーに所属するユーザーのパスワードを変更しようとして失敗しました。 対処 ID プロバイダーに所属するユーザーのパスワードは変更できません。
KAOP20087-E	The metadata endpoint is incorrect or the certificate is not set correctly.	要因 ID プロバイダーからメタデータをインポートしようとして失敗しました。 対処 次を確認して再実行してください。 URL が正しいこと、ID プロバイダーのアドレス解決ができること、ID プロバイダーのサーバ証明書のルート証明書が Common Services のトラストストアにインポートされていること。
KAOP20088-E	Failed to get group member information. This can be caused by an email address shared between a Common Services user and an Active Directory user. Remove or change the	要因 ユーザーグループのメンバーの取得に失敗しました。 対処 Common Services ユーザーとユーザーディレクトリのユーザーのメールアドレスが重複した可

メッセージ ID	メッセージテキスト	要因と対処
	email address belonging to the Common Services user.	可能性があります。該当する Common Services ユーザーのメールアドレスを変更してください。
KAOP20089-E	Invalid ldap search filter or objectclasses.	要因 検索フィルターまたはオブジェクトクラスに誤りがあります。 対処 正しい値を指定して操作を再度実行してください。
KAOP20090-E	Invalid SSL/TLS settings.	要因 LDAP サーバとの SSL/TLS の設定に誤りがあります。 対処 LDAP サーバとの SSL/TLS の設定を見直して操作を再度実行してください。
KAOP20091-E	Invalid hostname, address, or port number.	要因 LDAP サーバのホスト名、アドレスまたはポート番号に誤りがあります。 対処 LDAP サーバのホスト名、アドレスまたはポート番号を見直して操作を再度実行してください。
KAOP20092-E	Invalid bind DN or bind password.	要因 LDAP サーバのバインド DN またはパスワードに誤りがあります。 対処 LDAP サーバのバインド DN またはパスワードを見直して操作を再度実行してください。
KAOP20093-E	Invalid connection URL or user DN.	要因 LDAP サーバの URI または DN に誤りがあります。 対処 LDAP サーバの URI または DN を見直して操作を再度実行してください。
KAOP20094-E	Invalid URI syntax.	要因 LDAP サーバの URI に誤りがあります。 対処 LDAP サーバの URI を見直して操作を再度実行してください。
KAOP20095-E	One or more of the supplied parameters is incorrect.	要因 LDAP サーバのパラメーターに誤りがあります。 対処 LDAP サーバのパラメーターを見直して操作を再度実行してください。
KAOP20096-E	Update of users belonging to user directory is prohibited.	要因 ユーザーディレクトリに所属するユーザーを更新しようとした。 対処 ユーザーディレクトリに所属するユーザーは更新できません。
KAOP20097-E	Password reset for user directory users is prohibited.	要因 ユーザーディレクトリに所属するユーザーのパスワードを変更しようとした。

メッセージID	メッセージテキスト	要因と対処
		対処 ユーザーディレクトリに所属するユーザーのパスワードは変更できません。
KAOP60005-E	An error occurred. To determine the cause and resolve the problem, detailed investigation is required. Contact Support Center, who may ask you to collect troubleshooting information.	要因 内部エラーが発生しました。 対処 原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口に連絡してください。
KAOP60311-W	Cannot delete the temporary directory (directory name: <ディレクトリ名>).	要因 一時ディレクトリが他プロセスで使用されている可能性があります。 対処 要因を解消してメッセージが示すディレクトリを手動で削除してください。
KAOP60312-W	Cannot archive the directory (directory name: <ディレクトリ名>).	要因 アーカイブファイルの作成に失敗しました。 対処 アーカイブファイルの格納先に、十分なディスク容量を確保してください。ディスク容量を確保してもエラーが発生する場合は、原因究明と問題の解決のため、詳細な調査が必要です。障害情報を収集し、障害対応窓口に連絡してください。
KAOP60621-E	An option is invalid.usage: csgetras.sh -dir DirectoryName	要因 シンタックスが誤っています。 対処 オプションまたはディレクトリパスを見直して、再実行してください。
KAOP60622-E	Collection of RAS log data Common Service failed (maintenance information: <メンテナンス ID >).	要因 内部処理に必要なファイルが見つかりません。 対処 原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口に連絡してください。
KAOP60623-E	Cannot make the directory (directory name: <ディレクトリ名>).	要因 次の要因が考えられます。 1. 指定したパスが適切ではない。 2. 権限が不足している。 対処 次の対処をしてください。 1. パスが適切か確認してください。 2. 指定したディレクトリまでの権限を確認してください。
KAOP60624-E	The output directory is included in the RAS source directory. (directory name: <ディレクトリ名>)	要因 -dir オプションに指定されたディレクトリが、RAS 情報収集対象ディレクトリ内です。 対処 別のディレクトリを指定して再実行してください。
KAOP60629-E	Invalid format of hostname or IP address	要因

メッセージ ID	メッセージテキスト	要因と対処
		入力したホスト名または IP アドレスの形式が誤っています。 対処 入力した値を確認し、再実行してください。
KAOP60630-E	The package info file was not found. Common Service is not installed or has already been uninstalled.	要因 内部処理に必要なパッケージ情報ファイルが存在しません。 対処 原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口ご連絡してください。
KAOP60631-E	An attempt to execute the csresettrustrelationship command has failed. Verify the contents of the output file(<ファイル名>).	要因 コマンド実行中に Common Services の停止に失敗しました。 対処 マニュアルに従い Common Services のサービスの停止を実施して下さい。それでも解決しない場合は、障害情報を収集し、障害対応窓口ご連絡してください。
KAOP61003-E	An option is invalid.usage: csbackup.sh -dir DirectoryName	要因 シンタックスが誤っています。 対処 オプションまたはディレクトリパスを見直して、再実行してください。
KAOP61004-E	Collection of backup data Common Service failed (maintenance information: <メンテナンス ID >).	要因 内部処理に必要なファイルが不足しています。 対処 Common Services を上書きインストールしたあと、再度実行してください。
KAOP61005-E	Common Service is running.	要因 Common Services のサービスが起動されているので、このコマンドは実行できません。 対処 Common Services のサービスを停止して再度実行してください。
KAOP61624-E	Output directory is included in the backup source directory. (directory name: <ディレクトリ名>).	要因 -dir オプションに指定されたディレクトリが、バックアップ対象ディレクトリ内です。 対処 別のディレクトリを指定して再実行してください。
KAOP62003-E	An option is invalid.usage: csrestore.sh -file ArchiveName	要因 シンタックスが誤っています。 対処 オプションまたはアーカイブ名を見直して、再実行してください。
KAOP62004-E	Restoration of backup data Common Service failed (maintenance information: <メンテナンス ID >).	要因 内部エラーが発生しました。 対処 原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口ご連絡してください。

メッセージ ID	メッセージテキスト	要因と対処
KAOP62032-E	Cannot make the temporary directory (directory name: <ディレクトリ名>).	<p>要因 次の要因が考えられます。</p> <ol style="list-style-type: none"> 1. 指定したパスが適切ではない。 2. 権限が不足している。 <p>対処 次の対処をしてください。</p> <ol style="list-style-type: none"> 1. パスが適切か確認してください。 2. 指定したディレクトリまでの権限を確認してください。
KAOP63003-E	The -enableip true option is only valid when the hostname has been used in the access URL. You cannot use this option if you have already used an IP address in the access URL.	<p>要因 -h オプションに IP アドレスを指定しているの で、-enableip オプションに true を指定でき ません。</p> <p>対処 次の対処をしてください。</p> <ol style="list-style-type: none"> 1. -h オプションにホスト名を指定して実行し てください。 2. --enableip オプションに true を指定し て実行してください。
KAOP64002-E	Signing request and private key creation failed.	<p>要因 証明書署名要求と秘密鍵の作成に失敗しました。</p> <p>対処 マニュアルの手順に従い手動で作成してくださ い。それでも解決しない場合、詳細な調査が必要 です。障害情報を収集し、障害対応窓口に連絡し てください。</p>
KAOP64003-E	An error occurred. Contact support, who may ask you to collect troubleshooting information of the corresponding product. Product=<製品名>	<p>要因 内部エラーが発生しました。</p> <p>対処 原因究明と問題の解決には、詳細な調査が必要で す。障害情報を収集し、障害対応窓口に連絡して ください。</p>
KAOP64006-W	Setting SSL for server failed for some products.	<p>要因 一部の製品で、SSL サーバの設定に失敗しまし た。</p> <p>対処 マニュアルの手順に従い手動で作成してくださ い。それでも解決しない場合、詳細な調査が必要 です。障害情報を収集し、障害対応窓口に連絡し てください。</p>
KAOP64007-E	Setting SSL for server failed.	<p>要因 SSL サーバの設定に失敗しました。</p> <p>対処 マニュアルの手順に従い手動で作成してくださ い。それでも解決しない場合、詳細な調査が必要 です。障害情報を収集し、障害対応窓口に連絡し てください。</p>
KAOP64009-W	Setting SSL for client failed for some products.	<p>要因 一部の製品で、SSL クライアントの設定に失敗し ました。</p> <p>対処</p>

メッセージID	メッセージテキスト	要因と対処
		マニュアルの手順に従い手動で作成してください。それでも解決しない場合、詳細な調査が必要です。障害情報を収集し、障害対応窓口ご連絡してください。
KAOP64010-E	Setting SSL for client failed.	要因 SSL クライアントの設定に失敗しました。 対処 マニュアルの手順に従い手動で作成してください。それでも解決しない場合、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。
KAOP64012-E	Enable/disable certificate verification failed.	要因 サーバ証明書の検証機能の有効化/無効化に失敗しました。 対処 マニュアルの手順に従い手動で設定してください。
KAOP64013-E	Failed to start service. Refer to the product manual to resolve the error and try again. Product=<製品名>	要因 サービスの起動に失敗しました。 対処 メッセージが示す製品のマニュアルを参照し、サービスを手動で起動してください。起動できない場合は SSL 設定に問題がある場合があります。マニュアルの手順に従い手動で SSL を設定してください。それでも解決しない場合は、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。
KAOP64014-E	Failed to stop service. Refer to the product manual to resolve the error and try again. Product=<製品名>	要因 サービスの停止に失敗しました。 対処 メッセージが示す製品のマニュアルを参照し、サービスを手動で停止してください。停止できない場合は、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。
KAOP64015-E	Failed to restart service. Refer to the product manual to resolve the error and try again. Product=<製品名>	要因 サービスの再起動に失敗しました。 対処 メッセージが示す製品のマニュアルを参照し、サービスを手動で再起動してください。再起動できない場合は SSL 設定に問題がある場合があります。マニュアルの手順に従い手動で SSL を設定してください。それでも解決しない場合は、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。
KAOP64016-W	Since the access URL of Common Services changed, re-register each product in Common Services using setupcommonservice command.	要因 Common Services のアクセス URL が変更されたので、他製品との連携に失敗する可能性があります。 対処 setupcommonservice コマンドを使用して、各製品を Common Services に再登録してください。

メッセージID	メッセージテキスト	要因と対処
KAOP70000-E	The installer cannot start because there is insufficient disk space.	要因 /tmp または /var/tmp の一時使用領域が不足しています。 対処 /tmp または /var/tmp の必要な容量を確保してください。
KAOP70001-E	The removal function cannot start because there is insufficient disk space.	要因 /tmp または /var/tmp の一時使用領域が不足しています。 対処 /tmp または /var/tmp の必要な容量を確保してください。
KAOP70002-E	This location does not have enough space for the installation. Add more space.	要因 以下のいずれかのディスク容量が足りません。 ・ インストール先ディレクトリ ・ データ格納先ディレクトリ ・ ログ格納先ディレクトリ 対処 以下のディレクトリに対応するディスクの空き容量を確認し、システム要件に記載されたディスク容量を確保してください。 ・ インストール先ディレクトリ ・ データ格納先ディレクトリ ・ ログ格納先ディレクトリ
KAOP70003-E	A non-root user cannot perform an installation. Log in as root, and then start the installer.	要因 root ユーザーではないので、実行権限がありません。 対処 root ユーザーでログインしてからインストールを実行してください。
KAOP70004-E	A non-root user cannot perform a removal. Log in as root, and then restart the removal program.	要因 root ユーザーではないので、実行権限がありません。 対処 root ユーザーでログインしてからアンインストールを実行してください。
KAOP70005-E	Remove this software by using the same user account that was used for the installation.	要因 インストール時のユーザーと異なるので、実行権限がありません。 対処 インストール時と同一ユーザーでログインして削除してください。
KAOP70006-E	An error occurred. Common Service installation will stop. To determine the cause and resolve the problem, detailed investigation is required. Contact Support Center, who may ask you to collect troubleshooting information.	要因 内部エラーが発生しました。 対処 原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口に連絡してください。

メッセージ ID	メッセージテキスト	要因と対処
KAOP70007-E	The database backup failed. The installation will now end. There might not be enough unused capacity at the backup destination. Free up enough capacity at the backup destination, and then retry the installation. If the problem persists, detailed investigation is required to determine the cause and resolve the problem. Contact the support center, who may ask you to collect troubleshooting information.	要因 バックアップ先のディレクトリのディスクの空き容量が不足しているおそれがあります。 対処 バックアップ先のディレクトリに対応するディスクの空き容量を確保し、再度インストールしてください。同じエラーが発生する場合、原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口ご連絡してください。
KAOP70009-E	File "<ファイル名>", required for installation, cannot be read. Causes include: - The files on the installation media are insufficient, or you do not have execution permission. - The name of the mount point includes a character other than one-byte alphanumeric characters or "_". If you cannot resolve this problem, to determine the cause and resolve the problem, detailed investigation is required. Contact Support Center, who may ask you to collect troubleshooting information.	要因 インストールに必要なファイルを読み込めません。 次の要因が考えられます。 ・ メディア上のファイルが不足している、または実行権限がない。 ・ マウントポイントの名前には、1バイトの英数字以外の文字または _ が含まれます。 対処 要因に応じて、問題を解決してください。それでも解決しない場合、原因の究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口ご連絡してください。
KAOP70010-E	Common Service cannot be installed in this OS version. Verify the supported OS versions for the Common Service.	要因 インストールを実行した OS のバージョンは未サポートであり、インストールできません。 対処 Common Services がサポートする OS のバージョンを確認してください。
KAOP70012-W	Common Service is not supported on this OS. Verify which OSs are supported for the Common Service.	要因 インストールを実行した OS は未サポートです。 対処 Common Services がサポートする OS のバージョンを確認してください。
KAOP70014-E	Installation will stop because the evaluation version of Hitachi Ops Center is already installed. You cannot use the full version of Hitachi Ops Center together with the evaluation version. Uninstall the evaluation version, and then retry installation.	要因 評価版の Common Services がインストールされています。評価版と一緒に使用することはできません。 対処 評価版の Common Services をアンインストールしたあと、再度インストールをしてください。
KAOP70015-E	You cannot perform the installation. An Common Service from a different vendor is installed. The installation will stop. Contact Support.	要因 異なるベンダーの Common Services がインストールされています。 対処 顧客問い合わせ窓口ご連絡してください。

メッセージID	メッセージテキスト	要因と対処
KAOP70016-E	You cannot downgrade. A more recent version of Common Service is installed. The downgrade will stop.	要因 ダウングレードインストールはできません。 対処 インストールする Common Services のバージョンを確認してください。
KAOP70017-E	Specify up to 64 bytes for the installation path.	要因 インストール先として指定したパスが長過ぎます。 対処 インストール先として指定するパスは、64 バイト以内で指定してください。
KAOP70018-E	The installation path contains an invalid character. Valid characters are: A-Z a-z 0-9 _ / Note that these directories cannot be specified: - /usr - /usr/local - /var - The root directory (/)	要因 インストール先として指定したパスに使用できない文字が含まれています。 対処 インストール先のパスは、次の文字で指定してください。 A~Z a~z 0~9 _ / 次のパスは指定できません。 • /usr • /usr/local • /var • ルートディレクトリ (/)
KAOP70019-E	Specify up to 150 bytes for the backup file path.	要因 バックアップファイルの格納先として指定したパスが長過ぎます。 対処 バックアップファイルの格納先として指定するパスは、150 バイト以内で指定してください。
KAOP70020-E	An invalid character is included in the backup file path. Valid characters are: A-Z a-z 0-9 _ /	要因 バックアップファイルの格納先として指定したパスに使用できない文字が含まれています。 対処 バックアップファイルの格納先として指定するパスは、次の文字で指定してください。 A~Z a~z 0~9 _ /
KAOP70023-E	The mount path contains an invalid character. Valid characters are: A-Z a-z 0-9 _ /	要因 マウントパスに使用できない文字が含まれています。 対処 マウントパスは、次の文字で指定してください。 A~Z a~z 0~9 _ /
KAOP70028-E	An internal error occurred. The installation will stop. To determine the cause and resolve the problem, detailed investigation is required. Contact Support Center, who may ask you to collect troubleshooting information.	要因 内部エラーが発生しました。 対処 原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口に連絡してください。

メッセージID	メッセージテキスト	要因と対処
KAOP70029-E	The removal has been canceled because you cannot use this directory. Specify another directory and try again.	要因 カレントディレクトリが削除対象のため、アンインストールを中止します。 対処 別のディレクトリに移動して再実行してください。
KAOP70030-W	The program that is being used by the Common Service could not be removed. To re-install, you must remove this program. For details about the removal procedure, contact customer support. If you do not want to install the Common Service, there is no problem.	要因 Common Services のアンインストールが不完全な状態で終了しました。 対処 原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口に連絡してください。
KAOP70038-W	A connectivity check was performed for <IP アドレス>, but there was no response. A communication error may have occurred because Hitachi Ops Center products perform communications using <IP アドレス> as the destination. Verify the value. Depending on network settings, this message may appear even if there is no problem with the specified value. If this is the case, ignore this message and continue the installation.	要因 入力されたホスト名または IP アドレスにアクセスできません。 対処 アクセス可能なホスト名または IP アドレスを指定してください。
KAOP70039-W	The entered value is invalid. Type y to continue or n to cancel. (y/n):	要因 Y または N 以外の値が指定されました。 対処 Y または N を指定してください。
KAOP70040-W	The entered port number is invalid. Enter a value between 1 and 65535:	要因 指定できない範囲のポート番号が指定されました。 対処 1~65535 のポート番号を指定してください。
KAOP70041-E	The IP address or host name is too long. Specify up to 128 bytes for the IP address or host name.	要因 ホスト名または IP アドレスが長過ぎます。 対処 ホスト名または IP アドレスは、128 バイト以内で指定してください。
KAOP70042-E	An invalid character is included in the IPv6 address. Valid characters are: A-F a-f 0-9 . :	要因 IPv6 アドレスに使用できない文字が含まれています。 対処 IPv6 アドレスは、次の文字で指定してください。 A~F a~f 0~9 . :
KAOP70043-E	The IPv6 address is too long. Specify up to 47 bytes for the IPv6 address.	要因 IPv6 アドレスが長過ぎます。 対処

メッセージID	メッセージテキスト	要因と対処
		IPv6 アドレスは、47 バイト以内で指定してください。
KAOP70044-E	An error occurred. Hitachi Ops Center installation will stop. To determine the cause and resolve the problem, detailed investigation is required. Contact customer support, who may ask you to collect troubleshooting information.	要因 予期しないエラーが発生しました。 対処 原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口ご連絡してください。
KAOP70046-E	The installation of the RPM package failed. (RPM Package = <パッケージ名>)	要因 パッケージのインストールに失敗しました。 対処 顧客問い合わせ窓口にご連絡してください。
KAOP70048-E	Some required libraries are not installed. Install any missing libraries.	要因 前提ライブラリがインストールされていません。 対処 メッセージに表示された前提ライブラリをインストールしてください。
KAOP70050-E	Virtual memory free space for the management server is <空き容量> MB. Common Service requires <必要な容量> MB of virtual memory, so you must add more. Lack of free space may lead to unstable system and unable to run program.	要因 仮想メモリーの容量が不足しています。 対処 仮想メモリーの設定を見直して、必要な容量を確保してください。
KAOP70051-E	The database services could not be activated.	要因 データベースのサービスを起動できません。 対処 原因究明と問題の解決には、詳細な調査が必要です。障害情報を収集し、障害対応窓口にご連絡してください。

A.5 LDAP サーバ登録時のパラメーターを決定する

LDAP サーバと連携する場合、Common Services での LDAP サーバの連携登録時に、ユーザーをインポートするためのパラメーターを設定する必要があります。

パラメーターは、LDAP サーバで `ldapsearch` コマンドを実行し、検索されたエントリーの情報を基に決定してください。

操作手順

- LDAP クライアントから LDAP サーバにログインして、`ldapsearch` コマンドを実行します。

コマンド構文例：

```
ldapsearch -h <LDAP サーバのホスト名または IP アドレス> -b <検索対象のベース DN> -D <バインド DN> -w <バインド DN のパスワード> -L -s <検索範囲のスコープ>
```

指定できるオプションの詳細については、LDAP サーバのドキュメントを参照してください。

コマンド実行例：

```
ldapsearch -h example.com -b "CN=Users,DC=example,DC=com" -D "CN=admin,CN=Users,DC=example,DC=com" -w sysadmin -L -s sub (objectclass=*)
```

LDIF データの表示例（一部）：

```
dn: CN=John Smith,CN=Users,DC=example,DC=com
objectClass: person
objectClass: organizationalPerson
uid: j_smith
cn: John Smith
sn: Smith
givenName: John
distinguishedName: CN=John Smith,CN=Users,DC=example,DC=com
whenCreated: 20200710022002.0Z
whenChanged: 20210603075422.0Z
memberOf: CN=opscenter_users,CN=Users,DC=example,DC=com
mail: j_smith@example.com
objectGUID:: hMekv/PMMkyVnykQ5AeMyQ==
description: type1

dn: CN=Tom Brady,CN=Users,DC=example,DC=com
objectClass: person
objectClass: organizationalPerson
uid: t_brady
cn: Tom Brady
sn: Brady
givenName: Tom
distinguishedName: CN=Tom Brady,CN=Users,DC=example,DC=com
whenCreated: 20200710022057.0Z
whenChanged: 20210601074245.0Z
memberOf: CN=hcs_users,CN=Users,DC=example,DC=com
mail: t_brady@example.com
objectGUID:: pZtOMo29j0CSofnJrkL3EQ==
description: type2
```

- 表示された LDIF データの内容を基に、Common Services に設定するパラメーター情報を決定します。

Common Services での設定項目と、LDAP 属性との対応例を次に示します。

Common Services での設定項目	設定する LDAP 属性
ユーザー ID に割り当てる LDAP 属性	uid
メールアドレスに割り当てる LDAP 属性	mail
姓に割り当てる LDAP 属性	sn
フルネーム※	cn
名※	givenName
RDN として使われている LDAP 属性	cn
UUID として使われている LDAP 属性	objectGUID
ユーザーオブジェクトクラス	organizationalPerson
カスタムユーザー LDAP フィルター	(description=type1)

注※

どちらか一方を設定します。

[カスタムユーザー LDAP フィルター] で検索フィルターを指定すると、インポート対象のユーザーを絞り込むことができます。検索フィルターの文法は、RFC2254 に準拠します。

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を示します。

- [B.1 関連マニュアル](#)
- [B.2 このマニュアルでの表記](#)
- [B.3 このマニュアルで使用している略語](#)
- [B.4 KB \(キロバイト\) などの単位表記について](#)

B.1 関連マニュアル

このマニュアルの関連マニュアルを次に示します。必要に応じてお読みください。

- ・ 『Hitachi Ops Center Viewpoint ユーザーズガイド』 (4010-1J-027)
- ・ 『Hitachi Ops Center API Configuration Manager REST API リファレンスガイド』 (4010-1J-031)
- ・ 『Hitachi Ops Center Automator インストールガイド』 (4010-1J-035)

B.2 このマニュアルでの表記

このマニュアルでは、製品名を次のように表記しています。

表記	製品名
Automator	Hitachi Ops Center Automator
Common Services	Hitachi Ops Center Common Services
API Configuration Manager	Hitachi Ops Center API Configuration Manager
Portal	Hitachi Ops Center Portal
PowerShell	Windows PowerShell
Viewpoint	Hitachi Ops Center Viewpoint
Viewpoint data center proxy	Hitachi Ops Center Viewpoint data center proxy

B.3 このマニュアルで使用している略語

このマニュアルで使用する英略語を次に示します。

略語	正式名称
AD FS	Active Directory Federation Services
API	Application Programming Interface
CLI	Command Line Interface
CN	Common Name
CSR	Certificate Signing Request
DN	Distinguished Name
DNS	Domain Name System
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
I/O	Input/Output

略語	正式名称
ID	Identifier
IP	Internet Protocol
IPv6	Internet Protocol Version 6
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over Secure Sockets Layer
LDIF	Lightweight Directory Interchange Format
NTP	Network Time Protocol
OIDC	OpenID Connect
OS	Operating System
PEM	Privacy Enhanced Mail
RDN	Relative Distinguished Name
REST	Representational State Transfer
RFC	Request for Comments
RPM	Red Hat Package Manager
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
SSO	Single Sign - On
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UPN	User Principal Name
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
UUID	Universally Unique Identifier

B.4 KB（キロバイト）などの単位表記について

1KB（キロバイト）、1MB（メガバイト）、1GB（ギガバイト）、1TB（テラバイト）は、それぞれ1KiB（キビバイト）、1MiB（メビバイト）、1GiB（ギビバイト）、1TiB（テビバイト）と読み替えてください。

1KiB、1MiB、1GiB、1TiBは、それぞれ1,024バイト、1,024KiB、1,024MiB、1,024GiBです。

索引

A

- Active Directory Federation Services (AD FS) 13
 - Common Services のメタデータを更新 [SAML] 52
 - Common Services のメタデータをエクスポート [SAML] 46
 - Common Services を登録 [OIDC] 43
 - Common Services を登録 [SAML] 45
 - OpenID connect 検出エンドポイントの確認 [OIDC] 43
 - アプリケーショングループに登録 [OIDC] 41
 - サポート対象 40
 - 証明書の更新 [SAML] 51
 - 証明書の次回更新日の確認 [SAML] 50
 - 証明書利用者信頼の登録 [SAML] 47
 - シングルサインオンができないときの対処 [SAML] 52
 - 設定の流れ 40
 - 認証用証明書の更新の概要 [SAML] 50
 - 発行変換規則の設定 [OIDC] 42
 - メタデータエンドポイントの確認 [SAML] 45
 - 要求発行ポリシーの設定 [SAML] 47
 - ログイン 44, 49
- Active Directory サーバ 12
- Amazon Corretto 17 18
 - アップグレード 67
 - アンインストール 26

C

- csbackup コマンド 64
- cschgconnect コマンド 61
- csgetras コマンド 70
- csresettrustrelationship コマンド 65
- csrestore コマンド 64
- cssslsetup コマンド 28
 - SSL クライアントの設定 32
 - SSL サーバの設定 31
 - 機能 29
 - 証明書検証機能の有効化 32
 - 証明書署名要求 (CSR) の作成 30
 - 秘密鍵の作成 30

D

- debug.log ファイル 70

E

- error.log ファイル 70

H

- Hitachi Ops Center API Configuration Manager 12
- Hitachi Ops Center Automator 12
- Hitachi Ops Center Common Services 12
- Hitachi Ops Center Portal 12
 - アクセス URL の変更 61
 - 各種設定 24
 - ログイン 23
- Hitachi Ops Center Viewpoint 12
- Hitachi Ops Center Viewpoint data center proxy 12

I

- ID プロバイダー 13
 - サポート対象 40
 - 設定の流れ 40
- IP アドレスの変更 [管理サーバ] 61

L

- ldapsearch コマンド 92
- LDAP サーバ 12
 - パラメーターの決定 92

O

- OpenID connect 検出エンドポイント [AD FS] 43

P

PostgreSQL 15 18
アップグレード 68
アンインストール 26

S

setupcommonservice コマンド 22
SSL 通信の設定
設定の流れ [cssslsetup コマンド] 28
設定の流れ [複数の管理サーバ向け] 34
systemctl コマンド 56

U

URL の変更 [管理サーバ] 61

W

Web API 識別子 [AD FS] 41, 43

あ

アイドルタイムアウト設定 66
アップグレードインストール 18, 21
アプリケーショングループ [AD FS] 41
アンインストール
Amazon Corretto 17 26
Common Services 26
PostgreSQL 15 26

い

インストール
Common Services 19
アップグレードインストール 18, 21
インストールの流れ 18
各製品 21
インストール先 [Common Services] 19

う

ウイルス検出プログラムを使用する場合に必要な設定
67

え

エイリアス名 [AD FS] 41, 43

か

監査ログ [Common Services] 72
プロパティの変更 73
管理サーバ 14
IP アドレスの変更 61
準備 18
ポート番号 18
ポート番号の変更 61
ポート番号の変更 [内部通信] 62
ホスト名の変更 61

さ

サーバ証明書
失効状態の確認 57
サーバ証明書 [Common Services]
証明書検証機能の有効化 38
プロパティファイルに設定 35
有効期限の確認 56
用意する 34
サービス
起動 56
停止 56

し

システム構成例
1 台の管理サーバで運用する場合 14
複数台の管理サーバで運用する場合 14
システム要件 18
障害情報の収集 [Common Services] 70
証明書 [認証局]
Common Services にインポート 37
証明書利用者信頼 [AD FS] 47
シングルサインオン 12
setupcommonservice コマンド 22
トラブルシューティング [AD FS] 52
信頼関係のリセット [Common Services] 65

せ

設定の流れ
ID プロバイダー [AD FS] 40
SSL 通信の設定 [複数の管理サーバ向け] 34
インストール [Common Services] 18

と

トークン署名 50
更新 51
次回更新日の確認 50
トラストストア
証明書の有効期限を確認 56

トラブルシューティング
 監査ログ [Common Services] 72
 障害情報の収集 [Common Services] 70
 ログファイル [Common Services] 70

に

認証キー 50
 更新 51
 次回更新日の確認 50

は

バックアップ [Common Services] 64
 発行変換規則 [AD FS] 42

ふ

ファイアウォールの例外設定 18
 不正なアクセスや操作への対処 65

ほ

ポート番号 [Common Services] 18
 ポート番号の変更 [Common Services]
 管理サーバ 61
 内部通信 62
 ホスト名の変更 [管理サーバ] 61

め

メタデータエンドポイント [AD FS] 45, 53
 メッセージ ID 75
 メッセージ一覧 [Common Services] 75

ゆ

有効期限
 サーバ証明書 [Common Services] 56
 トラストストアの証明書 56
 ユーザーデータディレクトリ [Common Services]
 19
 ユーザー認証
 Active Directory Federation Services (AD FS)
 13
 Active Directory サーバ 12
 ID プロバイダー 13
 LDAP サーバ 12

よ

要求発行ポリシー [AD FS] 47

り

リストア [Common Services] 64

ろ

ログイン
 Hitachi Ops Center Portal 23
 ID プロバイダー [AD FS] 44, 49
 ログファイル [Common Services] 70
 プロパティの変更 71

