HITACHI
Inspire the Next

Hitachi Ops Center
インストールガイド

4010-1J-601-40

前書き

■ 対象製品

Hitachi Ops Center 11.0.5

■ 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

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

2025 年 9 月　4010-1J-601-40

■ 著作権

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

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。

- Windows Server の基本的な知識
- 前提ソフトウェア関する基本的な知識（外部認証サーバー、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 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　SSL 通信の設定

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

第 4 章　ID プロバイダー（AD FS）との連携

Hitachi Ops Center Portal の認証を AD FS 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 5 章　ID プロバイダー（AD FS 以外）との連携

Hitachi Ops Center Portal の認証を AD FS 以外の 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。

第 7 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。

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－でつないで説明しています。
＜ ＞ （山括弧）	可変値であることを示します。
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。

目次

1 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 製品の概要と、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 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 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。

1.2 Hitachi Ops Center Common Services の概要

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、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製品は、Hitachi Ops Center Viewpoint です。

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 サーバーとの連携

Common Services では、外部の Active Directory または LDAP サーバ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 Active Directory または LDAP サーバーで一元的に行うことができます。Active Directory または LDAP サーバーとの連携は、Hitachi Ops Center Portal 上で設定できます。

Common Services が連携できるサーバーは次のとおりです。

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

Active Directory または LDAP サーバーとの連携は、どちらか 1 つだけ設定できます。Active Directory サーバーの連携と LDAP サーバー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 サーバーとの連携には、次の条件があります。

Active Directory サーバーの場合

- 設定できる Active Directory サーバーは最大で 4 台です。
- 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。

- ユーザーベース 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。
- グループベース 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。
- 複数の Active Directory サーバーを設定する場合は、ユーザー名とメールアドレスが各サーバー間で重複しないようにしてください。

LDAP サーバーの場合

- 設定できる LDAP サーバーは 1 台です。
- 認証プロトコルは、LDAP(S)だけサポートしています。
- LDAP サーバー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 サーバーと 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

- 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 サーバー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 サーバーの証明書を更新し、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 サーバー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、および Common Services に組み込まれている Keycloak に登録した ID プロバイダーとの連携をサポートしています。ID プロバイダーとの連携設定は、使用する ID プロバイダーの種類によって異なります。連携の設定手順については、4. ID プロバイダー（AD FS）との連携または 5. ID プロバイダー（AD FS 以外）との連携を参照してください。

メモ

- 連携できる ID プロバイダーは、AD FS または AD FS 以外の ID プロバイダーのどちらか一方です。
- 1 つの Active Directory サーバーに対して、ディレクトリーサービスの連携と 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。

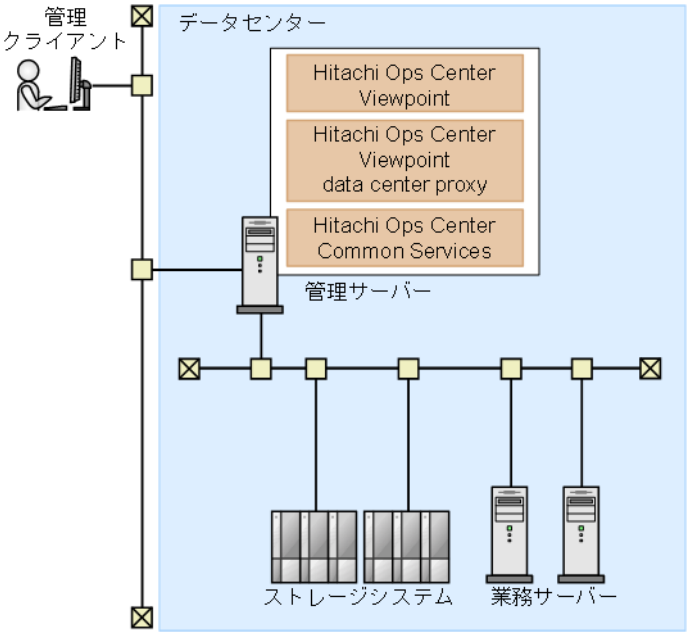
1.3　Hitachi Ops Center のシステム構成例

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ーから構成されます。Common Services は 1 台の管理サーバーで稼働し、Hitachi Ops Center 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 台の管理サーバーで運用する場合の構成例

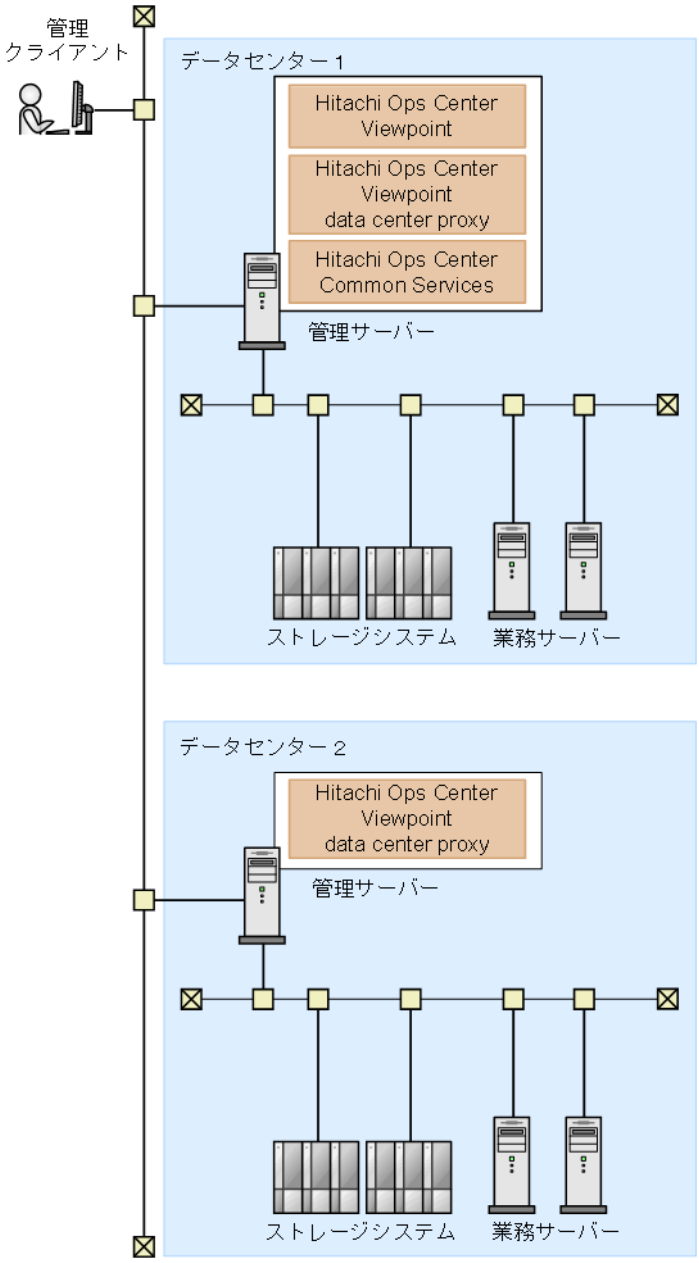
1 台の管理サーバーで Hitachi Ops Center 製品を運用する場合のシステム構成例を次に示します。



管理サーバー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ー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、複数の管理サーバー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ーの 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ーで構成される場合、各管理サーバーの時刻にずれがあると、Hitachi Ops Center Portal から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。

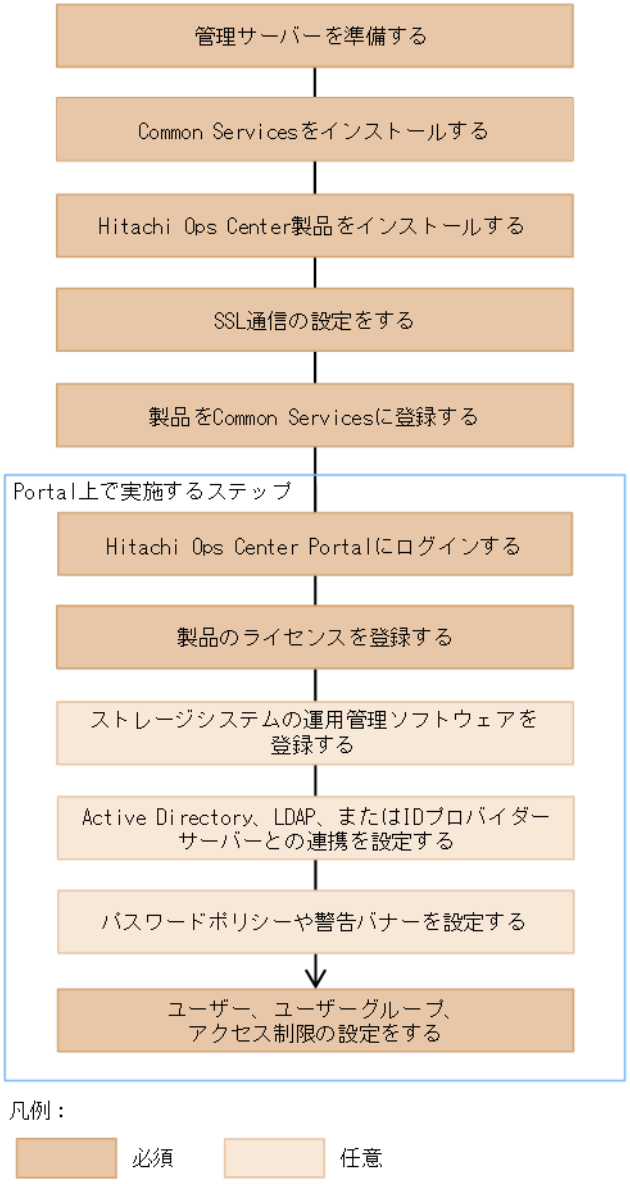
2 Hitachi Ops Center 製品のインストールとアップグレードインストール

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該当する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

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。



アクセス制御の設定完了後は、インストールした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、該当する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 管理サーバーを準備する

Hitachi Ops Center 製品をインストールする管理サーバーが、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、該当する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

- 管理サーバーには、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。

  管理サーバー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。

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

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、管理サーバーに 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、次のソフトウェアが Common Services のインストールフォルダーに展開されます。

- Amazon Corretto
- PostgreSQL

Common Services を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すると、インストールフォルダーに展開された Amazon Corretto と PostgreSQL のファイルは上書きされます。

Amazon Corretto または PostgreSQL を手動でアップグレードしている環境で、Common Services を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した場合は、必要に応じて次の作業をしてください。

- Amazon Corretto をアップグレードしている場合
  JDK のシンボリックリンク先の設定が Common Services のインストール時の設定に戻ってしまうため、再設定してください。詳細については、6.10　Amazon Corretto をアップグレードするを参照してください。
- PostgreSQL をアップグレードしている場合
  再度 PostgreSQL をアップグレードしてください。詳細については、6.11　PostgreSQL をアップグレードするを参照してください。

前提条件

- インストール先の管理サーバーで、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。
  - 管理サーバーがアクセスできる DNS サーバー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。

  管理サーバーのホスト名の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 では、デフォルトのユーザーグループに support-services という名前の特殊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。

- Active Directory サーバーとの連携で 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 のユーザーディレクトリ画面で Active Directory サーバーの［編集］アイコンをクリックし、［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 または LDAP サーバーと連携している環境で Common Services のアップグレードインストールをする場合、事前に Hitachi Ops Center Portal の Active Directory または LDAP サーバーの編集画面で［接続のテスト］と［認証のテスト］を実行して、正常に接続および認証できることを確認してください。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。
  正常に接続および認証されていない状態でアップグレードインストールをすると、アップグレード完了後、Active Directory ユーザーが Hitachi Ops Center Portal にログインできなくなるおそれがあります。

> **メモ**
>
> Active Directory ユーザーが Hitachi Ops Center Portal にログインできなくなった場合は、Active Directory サーバーとの接続および認証を確認してください。その後、Hitachi Ops Center Portal にログインし、ユーザーディレクトリ画面の［ユーザーグループの同期］をクリックして Active Directory グループを Common Services に同期させてください。

操作手順

1. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。

2. インストールメディアの次のフォルダーにある setup.exe を実行して、インストールウィザードを起動します。
   ＜インストールメディアのルートフォルダー＞¥CS_Server

3. インストールウィザードの指示に従って、各画面で必要な情報を指定して Common Services をインストールします。

設定項目	内容
インストール先	新規インストールの場合 Common Services をインストールするフォルダーを指定します。 • 次の場所にインストールされます。 *＜指定したフォルダー＞*¥CommonServices • Common Services のユーザーデータは、次のユーザーデータフォルダーに格納されます。 *＜Common Servicesのインストールフォルダー＞*¥data • インストール先パスに、マウントしたフォルダーは指定できません。
ホスト名または IPv4 アドレス	新規インストールの場合 Hitachi Ops Center Portal へのアクセス URL に使用するホスト名（FQDN 形式でも指定可）または IPv4 アドレスを指定します。

設定項目	内容

ホスト名または IPv4 アドレス	• ホスト名または FQDN を指定する場合
	  • 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、128 文字以内で指定してください。
	• ホスト名（FQDN）や IP アドレスは、Common Services と Hitachi Ops Center 製品をインストールする管理サーバー、および Hitachi Ops Center Portal にアクセスする Web ブラウザーで、名前解決ができ、アクセスできる必要があります。
	• 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、6.3　管理サーバーのホスト名または IP アドレス、ポート番号を変更するを参照してください。

ポート番号	新規インストールの場合 Hitachi Ops Center Portal へのアクセス URL に使用するポート番号を指定します。 Common Services と Viewpoint を同じ管理サーバーにインストールする場合、製品間でポート番号が競合しないようにしてください。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。
データをバックアップするかどうか	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 のデータをバックアップするかどうかを指定します。バックアップをする場合は、データのバックアップ先を指定します。 バックアップ先のデフォルトは次のとおりです。 *＜Common Servicesのインストールフォルダー＞*¥data¥backup

4. 入力内容を確認します。問題が無ければ、［インストール］をクリックしてインストール処理を開始します。

5. インストール完了の画面が表示されたら［完了］をクリックします。

6. Hitachi Ops Center Portal でビルトインアカウント（sysadmin ユーザー）の初期パスワードを変更します。

   初期パスワードのまま Hitachi Ops Center Portal にログインしようとすると、パスワード変更画面が表示されます。新しいパスワードを設定してください。詳細については、2.7　Hitachi Ops Center Portal にログインするを参照してください。

2.4 Hitachi Ops Center 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、該当する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 Portal のビルトインアカウント（sysadmin ユーザー）のパスワードが初期パスワードの場合は、製品をインストールする前に、パスワードを変更する必要があります。初期パスワードのまま Hitachi Ops Center Portal にログインしようとすると、パスワード変更画面が表示されます。新しいパスワードを設定してください。詳細については、2.7 Hitachi Ops Center Portal にログインするを参照してください。

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。正式なサーバー証明書を使った 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、3.　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、2.6　Hitachi Ops Center 製品を Common Services に登録するに進んでください。

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、インストールした Hitachi Ops Center 製品を Common Services に登録します。
Common Services に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。

> **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。

前提条件

- Common Services のインストール後、Hitachi Ops Center Portal のビルトインアカウント（sysadmin ユーザー）のパスワードを初期パスワードから変更してください。初期パスワードのまま Hitachi Ops Center Portal にログインしようとすると、パスワード変更画面が表示されます。新しいパスワードを設定してください。詳細については、2.7 Hitachi Ops Center Portal にログインするを参照してください。
- インストールした製品で Common Services がインストールされている管理サーバー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 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ーでcschgconnect コマンドを実行します。
- Common Services およびインストールした製品の管理サーバー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-administrators 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、または管理サーバーのポート番号を変更する場合は、製品を Common Services に再登録する必要があります。

setupcommonservice コマンドの格納場所、構文、および実行例を次に示します。

Viewpoint

デフォルトの格納場所：*<Program Files フォルダー>*¥hitachi¥Viewpoint¥bin¥

コマンド構文：

```
setupcommonservice --csUri <Common ServicesのURL> [--csUsername <Common ServicesのユーザーID>] [--applicationName <Portalに表示する製品名>]
```

コマンド実行例：

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

Viewpoint data center proxy

デフォルトの格納場所：<Program Filesフォルダー>¥hitachi¥DataCenterProxy¥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。
- セキュリティー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. ビルトインアカウントでログインします。
   初めてログインする場合は、次のユーザー ID とパスワードでログインします。
   ユーザー ID：sysadmin
   パスワード：sysadmin
   パスワード変更画面が表示された場合は、新しいパスワードを入力して［実行］をクリックします。
   ログインに成功すると、Hitachi Ops Center Portal のメインウインドウが開きます。

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。

- 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。
- ストレージシステムの運用管理ソフトウェアを登録する（任意）
  Common Services にストレージシステムの運用管理ソフトウェアを登録することで、Hitachi Ops Center Portal からストレージシステムの運用管理ソフトウェアのログイン画面を起動することができます。
- Active Directory、LDAP、または ID プロバイダーサーバーとの連携を設定する（任意）
  Active Directory または LDAP については 1.2.1　Active Directory または LDAP サーバーとの連携、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（任意）
  セキュリティー要件に基づいて、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（任意）
  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。
- 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。

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。

3 SSL 通信の設定

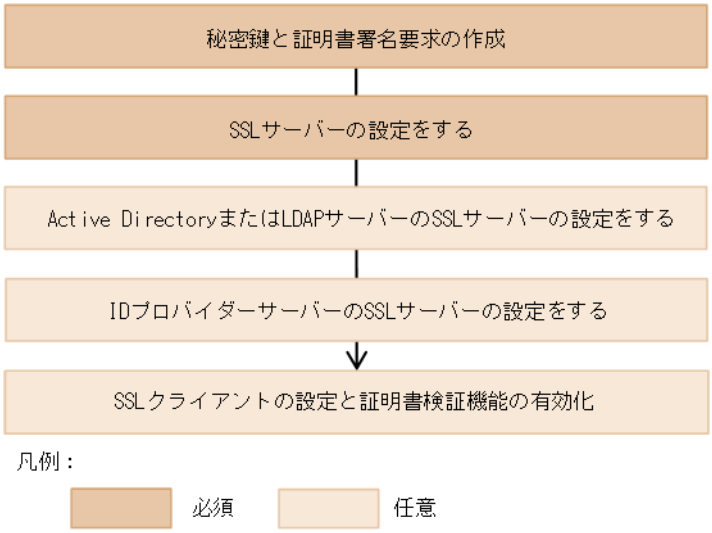
インストールが完了したら、SSL セットアップツール（cssslsetup コマンド）の実行、または手動で必要な手順を実行して SSL 通信の設定を行います。Common Services はデフォルトで自己署名証明書を使用して SSL/TLS 通信を行います。正式なサーバー証明書を使った SSL 通信の設定をしてください。

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、3.1　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、3.2　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。

3.1 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。



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 Viewpoint
- Hitachi Ops Center Viewpoint data center proxy
- Hitachi Ops Center Viewpoint RAID Agent

メモ

- SSL セットアップツールは、サポート対象のバージョンがインストールされている製品に対して使用できます。サポート対象外のバージョンがインストールされている場合は、アップグレードしてから使用してください。SSL セットアップツールがサポートする各製品のバージョンは、Common Services のソフトウェア添付資料を参照してください。
- 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、各管理サーバーで実行します。Common Services がインストールされていない管理サーバーでは、インストールメディアからcssslsetup コマンドを入手してください。cssslsetup コマンドの格納場所は次のとおりです。

- 管理サーバーに Common Services をインストールしている場合：
  <Common Servicesのインストールフォルダー>¥utility¥bin
- 管理サーバーに Common Services をインストールしていない場合：

Common Services のインストールメディアのルートフォルダーに格納されているutility.zip を展開してください。

cssslsetup コマンドは、utility.zip を展開した次のフォルダーに格納されています。

＜utility.zipを展開したフォルダー＞¥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、3.2　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ーの設定

3.1.1　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、3.2　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 サーバーの設定

SSL サーバー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	サーバー証明書と秘密鍵の登録
Viewpoint	サーバー証明書と秘密鍵の登録
Viewpoint data center proxy	サーバー証明書と秘密鍵の登録
Viewpoint RAID Agent	• サーバー証明書と秘密鍵の登録 • SSL 通信の有効化

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	• ルート証明書をトラストストアにインポートする

製品	設定内容
Common Services	• Active Directory、LDAP、または ID プロバイダーサーバーのサーバー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	• 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
Viewpoint data center proxy	• 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 RAID Agent	• 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

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。

3.1.2 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、3.1.3 SSL サーバーの設定（SSL セットアップツール）と 3.1.6 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. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. 次のフォルダーにあるcsssslsetup コマンドを実行します。

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

＜Common Servicesのインストールフォルダー＞¥utility¥bin

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

＜utility.zipを展開したフォルダー＞¥utility¥bin

次のメインメニューが表示されます。

```
Main menu   Ver:＜csssslsetup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. 証明書情報の入力時に指定したフォルダーに作成された CSR を、署名済み証明書を発行する認証局に提出します。
   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ー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ー証明書の作成結果を確認します。
   管理サーバーに Common Services をインストールしている場合：

```
"<Common Servicesのインストールフォルダー>¥openssl¥bin¥openssl" x509 -text -in "<証明書ファイルのフルパス名>"
```

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

```
"<utility.zipを展開したフォルダー>¥utility¥lib¥openssl¥bin¥openssl" x509 -text -in "<証明書ファイルのフルパス名>"
```

3.1.3　SSL サーバーの設定（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、管理サーバー上の Hitachi Ops Center 製品に対して、サーバー証明書および秘密鍵を指定します。

> **メモ**
>
> 複数台の管理サーバーで SSL サーバーの設定を行う場合は、各管理サーバーで SSL セットアップツールを使用してください。

操作手順

1. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. 次のフォルダーにあるcssslsetup コマンドを実行します。

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

   ＜Common Servicesのインストールフォルダー＞¥utility¥bin

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

   ＜utility.zipを展開したフォルダー＞¥utility¥bin

   次のメインメニューが表示されます。

```
Main menu   Ver:＜csssslsetup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 サーバー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ー証明書のファイル名を絶対パスで指定します。
7. 指定したサーバー証明書が、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ー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. Viewpoint RAID Agent の設定を行う場合、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。

   ECC 用の証明書を使用する場合、設定を有効のままにしてください。SSL セットアップツールでは、ECC 用の証明書の設定が有効の場合でも、RSA 用の証明書を設定します。

10. SSL サーバー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。

11. [5] を選択して各製品のサービスを再起動します。

3.1.4 Active Directory または LDAP サーバーの SSL サーバーの設定をする

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

3.1.5 ID プロバイダーサーバーの SSL 通信の設定をする

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

メモ

AD FS の証明書利用者信頼の監視機能を使用する場合、Common Services のサーバー証明書を署名した認証局のルート証明書を、AD FS サーバーの［信頼されたルート証明機関］にインポートしてください。

3.1.6 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、管理サーバー上の 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。

メモ

複数台の管理サーバーで SSL クライアントの設定を行う場合は、各管理サーバーで SSL セットアップツールを使用してください。

前提条件

Viewpoint RAID Agent の SSL 設定をする場合、ストレージシステムのインスタンス環境は、事前に作成してください。詳細は、Viewpoint のマニュアルを参照してください。

操作手順

1. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. 次のフォルダーにあるcssslsetup コマンドを実行します。

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

   ＜Common Servicesのインストールフォルダー＞¥utility¥bin

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

   ＜utility.zipを展開したフォルダー＞¥utility¥bin

   次のメインメニューが表示されます。

   ```
   Main menu   Ver:＜csssslsetup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. 共通のルート証明書をインポートします。

   Active Directory、LDAP、または ID プロバイダーサーバー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 のサーバー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。

   設定対象の製品に応じて、次の手順を実施してください。

   Viewpoint RAID Agent 以外の場合：

   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。
   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（サーバー識別名）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。

Viewpoint RAID Agent の場合：

次の手順で Viewpoint RAID Agent のインスタンス環境にトラストストアファイルを作成し、ストレージシステムのサーバー証明書のルート証明書をインポートします。インスタンス環境に既存のトラストストアファイルがある場合は削除され、新しいトラストストアファイルが作成されます。

a. 設定を行う場合は、[1. Yes] を選択します。

> **メモ**
>
> KAOP64020-W または KAOP64021-I メッセージが表示された場合は、Viewpoint RAID Agent の設定はされず、次のステップに進みます。Viewpoint RAID Agent の SSL クライアントの設定が必要な場合は、メッセージ内容に従って必要な設定を行った後、`cssslsetup` コマンドを再度実行してください。

b. 設定を行うインスタンス環境を選択します。

複数のインスタンス環境を指定する場合は、コンマで区切って指定してください。

c. ストレージシステムのサーバー証明書のルート証明書を絶対パスで指定します。

d. インスタンス環境の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。

e. エイリアス名を指定します。

エイリアス名には、どのストレージシステムのサーバー証明書であるか識別できる名称を指定してください。

f. 選択したインスタンス環境への登録がすべて完了するまで、トラストストアのパスワードとエイリアス名の指定を繰り返します。

6. Active Directory、LDAP、または ID プロバイダーサーバーと連携する場合は、各サーバーのサーバー証明書をインポートします。

Active Directory、LDAP、または ID プロバイダーサーバーと連携しない場合は、何も指定しないで [Enter] を入力します。

a. Active Directory、LDAP、または ID プロバイダーサーバーのサーバー証明書のファイル名を絶対パスで指定します。

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（サーバー識別名）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。

7. 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 5～6 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、LDAP、または ID プロバイダーサーバーと連携をするときは、認証連携先サーバーのルート証明書のインポートが必要です。

8. 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。
   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。

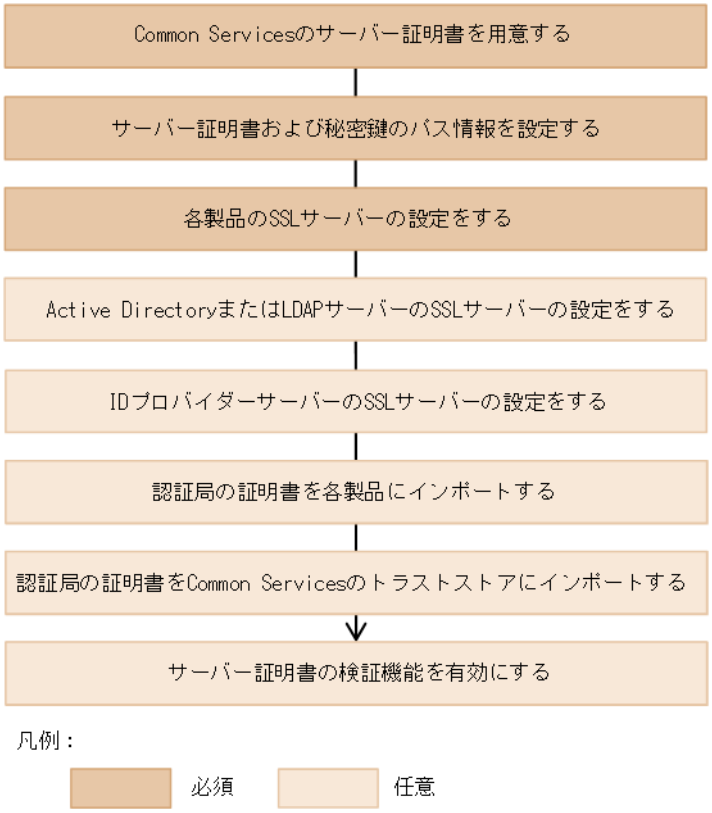
9. [5] を選択して各製品のサービスを再起動します。

操作結果

SSL 通信の設定は完了です。

3.2　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。



3.2.1　Common Services のサーバー証明書を用意する

事前に Common Services のサーバー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もしてください。確認方法については、6.2.2　サーバー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ー証明書を準備してください。

操作手順

1. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
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のインストールフォルダー>¥openssl¥bin¥openssl" req -new -newkey rsa
:4096 -nodes -keyout privateRSA.pem -sha256 -out serverRSA.csr -subj "/C=<ww>/ST=<x
x>/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のインストールフォルダー＞¥openssl¥openssl.cnf”
```

ECDSA の場合の実行例：

```
”＜Common Servicesのインストールフォルダー＞¥openssl¥bin¥openssl” ecparam -name secp384r1 > ecparam.txt

”＜Common Servicesのインストールフォルダー＞¥openssl¥bin¥openssl” req -new -newkey ec:ecparam.txt -nodes -keyout privateECDSA.pem -sha256 -out serverECDSA.csr -subj ”/C=＜ww＞/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のインストールフォルダー＞¥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=＜*ww*＞/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 のインストールフォルダー以下にある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のインストールフォルダー＞¥openssl¥bin¥openssl” req -text -in ＜CSRファイル＞ -config ”＜Common Servicesのインストールフォルダー＞¥openssl¥openssl.cnf”
```

4. 作成された CSR を、署名済み証明書を発行する認証局に提出します。

   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ー証明書を入手したら、次のコマンドを実行して、サーバー証明書の作成結果を確認します。

```
”＜Common Servicesのインストールフォルダー＞¥openssl¥bin¥openssl” x509 -text -in ＜認証局が署名したサーバー証明書＞
```

3.2.2 プロパティファイルにサーバー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ー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ー証明書は、次に示すとおりに中間認証局の証明書とチェーンして、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、すべてチェーンしてください。

```
echo.>> <改行のみ記載されたファイル>※

copy /b <認証局が署名したサーバー証明書>+<改行のみ記載されたファイル>+<中間認証局の証明書>[+<改行のみ記載されたファイル>+<中間認証局の証明書> ...] <チェーンしたサーバー証明書>
```

注※ はじめにecho コマンドを実行して、改行のみ記載されたファイルを出力します。作成されたファイルを利用して、サーバー証明書と中間認証局の証明書の間に改行が追記された 1 つのファイルを作成します。

操作手順

1. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. 認証局から取得した署名済みのサーバー証明書、および秘密鍵を安全な方法で管理サーバーに転送します。
3. サーバー証明書、秘密鍵を次のフォルダーに格納します。

   <Common Servicesのインストールフォルダー>¥data¥tls¥
4. 次のプロパティファイルに、サーバー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

   <Common Servicesのインストールフォルダー>¥data¥userconf¥config_user.properties

   設定項目

   - RSA の設定：

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

   - ECDSA の設定：

     ```
     CS_GW_SSL_CERTIFICATE_ECDSA=<証明書(ECDSA)ファイルの絶対パス>
     CS_GW_SSL_CERTIFICATE_KEY_ECDSA=<秘密鍵(ECDSA)ファイルの絶対パス>
     ```
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、サーバー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。

3.2.3 各製品の SSL サーバーの設定をする

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 サーバーの設定をします。
SSL サーバー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。

3.2.4 Active Directory または LDAP サーバーの SSL サーバーの設定をする

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

3.2.5 ID プロバイダーサーバーの SSL 通信の設定をする

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

メモ

AD FS の証明書利用者信頼の監視機能を使用する場合、Common Services のサーバー証明書を署名した認証局のルート証明書を、AD FS サーバーの［信頼されたルート証明機関］にインポートしてください。

3.2.6 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 のサーバー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 ID プロバイダーにインポートする場合は、ID プロバイダーのサーバーにも同様にインポートしてください。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。
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。

3.2.7 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ー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 ID プロバイダーのサーバーと連携する場合は、それらのサーバー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ーに転送します。

操作手順

1. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. 次のコマンドを実行して、Common Services のサーバー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

   ```
   "<Common Servicesのインストールフォルダー>¥jdk¥bin¥keytool" -importcert -alias <エイリアス名> -keystore "<トラストストアファイルのパス>" -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。

   <Common Servicesのインストールフォルダー>¥data¥tls¥cacerts

   > **メモ**
   >
   > コマンドを実行するとパスワードの入力を求められます。トラストストアのデフォルトのパスワードはchangeit です。パスワードは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ー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 サーバーとの通信に LDAPS を利用する場合、Active Directory または LDAP サーバーのサーバー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. ID プロバイダーと連携する場合は、ID プロバイダーのサーバー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。

3.2.8　サーバー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、通信相手のサーバー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ー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. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. 次のプロパティファイルを変更して、サーバー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

   ＜Common Servicesのインストールフォルダー＞¥data¥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。

4 ID プロバイダー（AD FS）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。

連携の設定手順は、使用する ID プロバイダーの種類によって異なります。この章では、AD FS と連携する場合の手順について説明します。AD FS 以外の ID プロバイダーと連携する場合の手順については、5. ID プロバイダー（AD FS 以外）との連携を参照してください。

4.1 サポートする AD FS

Common Services がサポートする AD FS 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	• 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。 • Windows Server 2016 Datacenter • Windows Server 2019 Datacenter • Windows Server 2022 Datacenter • Windows Server 2025 Datacenter
連携可能な ID プロバイダーの最大数	1 AD FS と連携した場合、それ以外の ID プロバイダーとの連携はできません。

4.2 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 AD FS 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 AD FS のユーザーでログインする

Common Services で AD FS 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 サーバー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、3. 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、管理サーバーのホスト名が AD FS のサーバーで名前解決できる必要があります。

4.3 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。

4.3.1 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 の管理サーバーのホスト名など、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 サーバーにログインします。
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 の管理サーバー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。

6. 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。

7. [次へ] をクリックします。

8. 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。

9. 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。

10. 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]

11. 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。

12. 完了画面で [閉じる] をクリックします。

4.3.2　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。AD FS 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

1. AD FS サーバーにログインします。
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。
4. [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。
5. 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。
6. 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。
7. 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

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
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。

4.3.3 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 サーバーにログインします。
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。

4.3.4 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	4.3.1　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	4.3.3　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	4.3.1　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	4.3.1　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	4.3.1　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ーと AD FS サーバー間で許容可能な時差を指定します。サーバー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。

項目	内容
グループ単位のマッピングの設定	（例） domain¥cs_admin_group

4.3.5 Hitachi Ops Center Portal に AD FS のユーザーでログインする

AD FS との連携の設定が完了したら、Web ブラウザーから AD FS 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。

   AD FS のログイン画面が表示されます。

3. AD FS のユーザーでログインします。

   AD FS 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直し、［ユーザー管理］－［ユーザー］を選択して、AD FS 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

AD FS との連携の設定は完了です。

4.4　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。

4.4.1　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 サーバーにログインします。
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ので控えておいてください。

4.4.2　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	4.4.1　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。 • 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ーと AD FS サーバー間で許容可能な時差を指定します。 サーバー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） `domain¥cs_admin_group`

4.4.3 Common Services のメタデータをエクスポートする（AD FS）

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 サーバーに転送します。

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 サーバーにファイルを転送してください。

4.4.4 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 サーバーにログインします。
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。

4.4.5　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。AD FS 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 サーバーにログインします。

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］
   　4.4.2　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

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
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。

    1. [LDAP 属性を要求として送信] で指定した要求規則
    2. [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。

4.4.6 Hitachi Ops Center Portal に AD FS のユーザーでログインする

AD FS との連携の設定が完了したら、Web ブラウザーから AD FS 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。

   AD FS のログイン画面が表示されます。

3. AD FS のユーザーでログインします。

   AD FS 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直し、［ユーザー管理］ − ［ユーザー］を選択して、AD FS 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

AD FS との連携の設定は完了です。

> **メモ**
>
> AD FS 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、4.5　AD FS の認証用証明書の更新（SAML）を参照してください。

4.5 AD FS の認証用証明書の更新（SAML）

AD FS 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。

AD FS 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。

4.5.1 認証用証明書の更新の概要（AD FS）

AD FS 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、AD FS 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 の証明書を手動で更新する場合、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。

4.5.2 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。

4.5.3 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 サーバーにログインします。
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。

4.5.4 Common Services の証明書を更新する（AD FS）

Common Services の証明書は、有効期限切れによる失効を防ぐため自動更新されます。自動更新された場合、AD FS サーバーでは、登録されている Common Services の証明書を更新する必要があります。証明書の更新は、自動で更新する方法と手動で更新する方法があります。

Common Services の証明書を自動で更新する

Common Services の証明書を自動的に更新する手順について説明します。AD FS の証明書利用者信頼の監視機能を使用して、Common Services のメタデータが自動で更新されるように設定します。

> **メモ**
>
> Common Services で証明書が自動更新されてから、AD FS の監視機能で証明書が更新されるまで最大で 24 時間かかる場合があります。更新されるまでは、Hitachi Ops Center Portal に AD FS のユーザーでログインができなくなります。

前提条件

次の設定がされていることを確認してください。

- Windows Server のバージョンが 2019 以前の場合は、Common Services の証明書が ECDSA で署名されている。
- AD FS サーバーの.NET Framework の設定で、TLS1.2 以上が有効となっている。

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。対象の ID プロバイダー詳細画面で［SAML SP メタデータ URI］を確認します。
4. AD FS サーバーにログインします。
5. ［スタート］－［Windows 管理ツール］－［AD FS の管理］を選択します。
6. 左側のツリーから［AD FS］－［証明書利用者信頼］を選択します。中央のペインで対象の証明書利用者信頼を選択して、右側のペインで［プロパティ］をクリックします。
7. プロパティ画面の［監視］タブを選択して、［証明書利用者のフェデレーション メタデータの URL］に Hitachi Ops Center Portal の ID プロバイダーの詳細画面で確認した［SAML SP メタデータ URI］を入力します。
8. ［URL のテスト］をクリックして確認します。エラーになった場合は、Windows の SSL/TLS の設定を見直してください。
9. ［証明書利用者を監視する］のチェックボックスをオンにします。
10. ［証明書利用者を自動的に更新する］のチェックボックスをオンにします。
11. ［適用］をクリックします。

Common Services の証明書を手動で更新する

Common Services の証明書を手動で更新する方法を説明します。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。セキュリティー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、4.4.3 Common Services のメタデータをエクスポートする（AD FS）を参照してください。
7. AD FS サーバーにログインします。
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絶対パス> -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 C:¥temp¥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。

4.5.5　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 サーバーにログインします。
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、4.4.1　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。

4.5.6　シングルサインオンができないときの対処（AD FS）

AD FS 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
  AD FS 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
  AD FS を使用してログインできない場合、Common Services のログファイル (デフォルトの格納場所：*＜Common Servicesのインストールフォルダー＞*¥logs¥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、4.4.3　Common Services のメタデータをエクスポートする（AD FS）を参照してください。
2. AD FS サーバーにログインします。
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絶対パス＞ -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 C:¥temp¥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、4.4.1 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。

5 ID プロバイダー（AD FS 以外）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。

連携の設定手順は、使用する ID プロバイダーの種類によって異なります。この章では、AD FS 以外の ID プロバイダーと連携する場合の手順について説明します。AD FS と連携する場合の手順については、4. ID プロバイダー（AD FS）との連携を参照してください。

5.1　ID プロバイダー（AD FS 以外）と連携するための設定の流れ

AD FS 以外の ID プロバイダーと連携するための設定の流れを説明します。

Common Services には、ユーザー認証機能として Keycloak が組み込まれています。ID プロバイダーとの連携では、Common Services に組み込まれている Keycloak を使用します。ID プロバイダーへの接続には、フェデレーションプロトコルとして OIDC（OpenID Connect）または SAML（Security Assertion Markup Language）を使用できます。

Keycloak および ID プロバイダーの設定方法については、それぞれのドキュメントを参照してください。Keycloak のドキュメントについては、Common Services に組み込まれている Keycloak のバージョンを次のファイルで確認し、それに対応するバージョンのドキュメントを参照してください。

```
＜Common Servicesのインストールフォルダー＞¥keycloak¥version.txt
```

AD FS 以外の ID プロバイダーと連携するためのワークフローを次に示します。

1. ID プロバイダーを準備する
   ID プロバイダーのソフトウェアをインストールし、ID プロバイダーが利用できるようにします。
2. 5.2　ID プロバイダー（AD FS 以外）との連携機能を有効にする
3. 5.3　ID プロバイダー（AD FS 以外）を登録する
4. 5.4　ユーザー属性のマッピングを設定する（任意）
5. 5.5　ユーザーグループへのマッピングを設定する
6. ID プロバイダー側で認証の設定をする
   Common Services を Relying Party として登録するなど、Common Services のユーザー認証に必要な設定を実施します。
7. Hitachi Ops Center Portal に ID プロバイダーのユーザーでログインする

メモ

- このマニュアルでは、「Keycloak」は Common Services に組み込まれている Keycloak を指します。
- Keycloak での ID プロバイダーの設定は、ユーザー自身で実施する必要があります。Keycloak と ID プロバイダー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。
- Keycloak に ID プロバイダーを登録、または登録後に設定を変更する際は、設定内容によって Common Services が正常に動作しなくなるおそれがあります。事前に、csbackup コマンドで Common Services のバックアップを取得することをお勧めします。詳細については、6.5　Common Services のデータをバックアップするを参照してください。
- Common Services と AD FS 以外の ID プロバイダーを連携した場合、AD FS との連携はできません。

5.2 ID プロバイダー（AD FS 以外）との連携機能を有効にする

AD FS 以外の ID プロバイダーと連携するには、csembeddedkeycloak コマンドを実行して、連携機能を有効にする必要があります。

csembeddedkeycloak コマンドを実行すると、Hitachi Ops Center Portal から Keycloak にアクセスできるように設定が変更されます。また、Keycloak にログインするためのユーザー（idpadmin）が作成されます。

連携機能を有効にした場合、無効に変更することはできません。

操作手順

1. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. 次のコマンドを実行します。

   ```
   <Common Servicesのインストールフォルダー>¥utility¥bin¥csembeddedkeycloak.exe /enable
   ```

3. 設定を有効にするか確認するメッセージが表示されます。設定を変更すると、Common Services のサービスが再起動されるため、問題がなければ［y］を指定します。
   ［n］を指定した場合は、設定は変更されずに終了します。
4. 作成される idpadmin ユーザーのパスワードを指定します。
   パスワードは、Common Services のパスワードポリシーに従って設定してください。
5. 設定が完了すると、Common Services のサービスが再起動されます。

5.3 ID プロバイダー（AD FS 以外）を登録する

Hitachi Ops Center Portal から Keycloak にログインし、ID プロバイダーを登録します。

前提条件

Common Services と ID プロバイダーのサーバー間で SSL 通信の設定をしてください。ID プロバイダーのサーバー証明書、またはサーバー証明書のルート証明書を Common Services のトラストストアに登録する必要があります。SSL 通信の設定については、3. SSL 通信の設定を参照してください。

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 (その他)］をクリックします。
4. ID プロバイダー (その他)画面から［組み込み Keycloak］をクリックします。
5. idpadmin ユーザーで Keycloak にログインします。
6. Identity providers 画面から連携したい ID プロバイダーをクリックします。
7. 画面の指示に従って ID プロバイダーを登録します。

> **メモ**
>
> 登録した ID プロバイダーは Hitachi Ops Center Portal の ID プロバイダー画面には表示されません。ID プロバイダーの設定を参照、更新、または削除するには、Hitachi Ops Center Portal から Keycloak にログインして操作してください。Keycloak の操作の詳細については、Keycloak のドキュメントを参照してください。

5.4　ユーザー属性のマッピングを設定する

AD FS 以外の ID プロバイダーのユーザーのメールアドレス、姓、名を Common Services と同期させる場合は、ID プロバイダーのユーザー属性を Keycloak のユーザー属性にマッピングしてください。同期する必要がない場合、この設定は不要です。

設定内容は ID プロバイダーとの連携に使用しているフェデレーションプロトコルによって異なります。

- 5.4.1　OIDC プロトコルで連携する
- 5.4.2　SAML プロトコルで連携する

5.4.1　OIDC プロトコルで連携する

AD FS 以外の ID プロバイダーのユーザーのメールアドレス、姓、名を Common Services と同期させる場合、ID プロバイダーが発行する ID トークンに、Keycloak のユーザー属性に対応する Claim が含まれるよう ID プロバイダーで設定する必要があります。Keycloak での設定は不要です。マッピングするユーザーの属性は、任意に選択できます。ID プロバイダーの Claim の設定については、ID プロバイダーのドキュメントを参照してください。

Keycloak のユーザー属性と ID プロバイダーの ID トークンの Claim の対応は次のとおりです。

Keycloak のユーザー属性	ID プロバイダーの ID トークンの Claim
email	email
lastName	family_name
firstName	given_name

5.4.2　SAML プロトコルで連携する

AD FS 以外の ID プロバイダーのユーザーのメールアドレス、姓、名を Common Services と同期させる場合、ID プロバイダーのアサーションの属性と Keycloak のユーザー属性のマッピングを設定する必要があります。マッピングするユーザーの属性は、任意に選択できます。

前提条件

ID プロバイダーでアサーションの設定をしてください。ID プロバイダーから送信されるアサーションには、Keycloak のユーザー属性に必要な属性が含まれている必要があります。ID プロバイダーのアサーションの属性の設定については、ID プロバイダーのドキュメントを参照してください。

Keycloak のユーザー属性と ID プロバイダーのアサーションの属性の対応例は次のとおりです。

Keycloak のユーザー属性	ID プロバイダーのアサーションの属性の例
email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
lastName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
firstName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

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 (その他)］をクリックします。
4. ID プロバイダー (その他)画面から［組み込み Keycloak］をクリックします。
5. idpadmin ユーザーで Keycloak にログインします。
6. Identity providers 画面から登録した ID プロバイダーをクリックします。
7. Provider details 画面の［Mappers］タブをクリックします。
8. 同期させる属性ごとに、マッピングに必要な項目を設定します。
   a. [Add mapper］をクリックします。
   b. Add Identity Provider Mapper 画面で次の項目を設定します。
   - メールアドレスを設定する場合

項目	指定する値	指定する値の例
Name	任意の名称	email-mapper
Sync mode override	リストから選択	Force
Mapper type	Attribute Importer	Attribute Importer
Attribute Name	ID プロバイダーのアサーションの属性	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Name Format	ATTRIBUTE_FORMAT_BASIC	ATTRIBUTE_FORMAT_BASIC
User Attribute Name	email	email

   - 姓を設定する場合

項目	指定する値	指定する値の例
Name	任意の名称	lastName-mapper
Sync mode override	リストから選択	Force

項目	指定する値	指定する値の例
Mapper type	Attribute Importer	Attribute Importer
Attribute Name	ID プロバイダーのアサーションの属性	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Name Format	ATTRIBUTE_FORMAT_BASIC	ATTRIBUTE_FORMAT_BASIC
User Attribute Name	lastName	lastName

- 名を設定する場合

項目	指定する値	指定する値の例
Name	任意の名称	firstName-mapper
Sync mode override	リストから選択	Force
Mapper type	Attribute Importer	Attribute Importer
Attribute Name	ID プロバイダーのアサーションの属性	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Name Format	ATTRIBUTE_FORMAT_BASIC	ATTRIBUTE_FORMAT_BASIC
User Attribute Name	firstName	firstName

c. 設定が完了したら［Save］をクリックします。

d. 同期させるすべての属性の設定が完了するまで、この手順を繰り返します。

5.5　ユーザーグループへのマッピングを設定する

AD FS 以外の ID プロバイダーのユーザーに Hitachi Ops Center のアクセス権限を付与するために、ユーザーグループへのマッピングを設定します。

Keycloak の Group mapper を使用すると、ID プロバイダーで認証されたユーザーを、指定した Common Services のユーザーグループに自動的にマッピングできます。Group mapper を使用しない場合は、Hitachi Ops Center Portal でユーザーごとに手動でユーザーグループを割り当てます。

ここでは、次の事例に基づいて、ID プロバイダーのユーザーにユーザーグループをマッピングする手順を説明します。

- すべてのユーザーに Hitachi Ops Center へのアクセス権限を付与する：
  5.5.1　Hardcoded Group mapper を使用する
- 特定のユーザーに Hitachi Ops Center の権限を付与する：
  5.5.2　Advanced Claim to Group mapper または Advanced Attribute to Group mapper を使用する
- ID プロバイダーはユーザー認証の機能だけを使用し、アクセス権限は Common Services で管理する：
  5.5.3　Hitachi Ops Center Portal でユーザーグループを割り当てる

5.5.1　Hardcoded Group mapper を使用する

Hardcoded Group mapper を使用すると、AD FS 以外の ID プロバイダーで認証されたすべてのユーザーを、特定のユーザーグループに自動的にマッピングできます。ID プロバイダーのすべてのユーザーに同じ権限を付与する場合に使用します。

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 (その他)］をクリックします。
4. ID プロバイダー (その他)画面から［組み込み Keycloak］をクリックします。
5. idpadmin ユーザーで Keycloak にログインします。
6. Identity providers 画面から登録した ID プロバイダーをクリックします。
7. Provider details 画面の［Mappers］タブをクリックします。

8. [Add mapper] をクリックし、Add Identity Provider Mapper 画面で次の項目を設定します。

項目	指定する値	指定する値の例
Name	任意の名称	hardcoded-group
Sync mode override	リストから選択	Force
Mapper type	Hardcoded Group	Hardcoded Group
Group	所属させる Common Services のユーザーグループ名	opscenter-users

9. 設定が完了したら［Save］をクリックします。

5.5.2 Advanced Claim to Group mapper または Advanced Attribute to Group mapper を使用する

Advanced Claim to Group mapper または Advanced Attribute to Group mapper を使用すると、AD FS 以外の ID プロバイダーで認証されたユーザーを、指定した条件に基づくユーザーグループに自動的にマッピングできます。Hitachi Ops Center にログインできるユーザーを制限する場合や、特定のユーザーに管理者権限を付与する場合などに使用します。

これらの Group mapper は、ID プロバイダーから提供されるユーザーの情報を基にマッピングします。具体的には、次に示す Key と Value のペアで条件を指定します。複数の条件を指定することもできます。

- OIDC プロトコルで連携する場合：Key には ID トークンの Claim を、Value には Claim の値を指定します。
- SAML プロトコルで連携する場合：Key にはアサーションの属性を、Value には属性の値を指定します。

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 (その他)］をクリックします。
4. ID プロバイダー (その他)画面から［組み込み Keycloak］をクリックします。
5. idpadmin ユーザーで Keycloak にログインします。
6. Identity providers 画面から登録した ID プロバイダーをクリックします。
7. Provider details 画面の［Mappers］タブをクリックします。

8. [Add mapper] をクリックし、Add Identity Provider Mapper 画面で次の項目を設定します。

- OIDC プロトコルで連携する場合

項目	指定する値	指定する値の例
Name	任意の名称	Advanced-Claim-to-Group-mapper
Sync mode override	リストから選択	Force
Mapper type	Advanced Claim to Group	Advanced Claim to Group
Claims - Key	ID プロバイダーの Key	グループに相当する Claim OIDC プロトコルでは、グループを示す標準の Claim はありません。ID プロバイダー固有の Claim を指定する必要があります。
Claims - Value	Key に対応する値	Storage Administrators
Regex Claim Values	Claims - Value で正規表現を使用する場合は On、使用しない場合は Off	Off
Group	所属させる Common Services のユーザーグループ名	opscenter-administrators

- SAML プロトコルで連携する場合

項目	指定する値	指定する値の例
Name	任意の名称	Advanced-Attribute-to-Group-mapper
Sync mode override	リストから選択	Force
Mapper type	Advanced Attribute to Group	Advanced Attribute to Group
Attributes - Key	ID プロバイダーの Key	http://schemas.xmlsoap.org/claims/Group
Attributes - Value	Key に対応する値	Storage Administrators
Regex Attribute Values	Attributes - Value で正規表現を使用する場合は On、使用しない場合は Off	Off
Group	所属させる Common Services のユーザーグループ名	opscenter-administrators

9. 設定が完了したら［Save］をクリックします。

5.5.3 Hitachi Ops Center Portal でユーザーグループを割り当てる

Group mapper を使用しないで、Common Services のユーザーグループに AD FS 以外の ID プロバイダーのユーザーを割り当ててアクセス権限を付与することもできます。ID プロバイダーはユーザー認証の機能だけを使用し、アクセス権限は Common Services で管理する場合などに使用します。

操作手順

1. ユーザーグループを割り当てたい ID プロバイダーのユーザーで、Hitachi Ops Center Portal でログインを試行します。
   この時点では Hitachi Ops Center へのアクセス権限がないため、ログインは失敗しますが、ユーザーはローカルユーザーとして Common Services に登録されます。
2. 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。
3. ナビゲーションバーで、[ユーザー管理] をクリックし、[資産種別] から [ユーザー] を選択します。
4. ID プロバイダーのユーザーアカウントの [ユーザーグループ設定] アイコンをクリックします。
   (ユーザーアカウントが表示されていない場合は、検索ボックスを使用してください。)
   ユーザーグループ設定画面が表示されます。
5. [割り当て可能グループ] リストから割り当てたいグループを選択し、[←] をクリックします。
6. 完了後、画面左上隅にある [<] をクリックして、ユーザーリストに戻ります。

5.6 Hitachi Ops Center Portal に ID プロバイダー（AD FS 以外）のユーザーでログインする

ID プロバイダー（AD FS 以外）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直し、［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、5.7 ID プロバイダー（AD FS 以外）の認証用証明書の更新（SAML）を参照してください。

5.7 ID プロバイダー（AD FS 以外）の認証用証明書の更新（SAML）

ID プロバイダーとの連携で、SAML プロトコルのアサーションに署名または暗号化を設定している場合、Common Services または ID プロバイダーの証明書が更新されたときは、次の作業が必要です。

- Common Services の証明書が更新された場合は、ID プロバイダーに登録している Common Services の証明書を更新してください。
- ID プロバイダーの証明書が更新された場合は、Keycloak に登録している ID プロバイダーの証明書を更新してください。

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。

5.7.1 Common Services の証明書を更新する

Common Services の証明書は、有効期限切れによる失効を防ぐため自動更新されます。自動更新された場合、AD FS 以外の ID プロバイダーのサーバーでは、登録されている Common Services の証明書を更新する必要があります。

Common Services の証明書を更新するには、Keycloak からメタデータをファイルに出力して、ID プロバイダーにインポートしてください。

操作手順

1. Hitachi Ops Center Portal から Keycloak にログインします。
2. 登録した ID プロバイダーの Provider details 画面を開きます。
3. [Endpoints] の [SAML 2.0 Service Provider Metadata] のリンクからメタデータを取得します。
4. 取得したメタデータを ID プロバイダーにインポートします。
   ID プロバイダーにインポートする方法については、ID プロバイダーのドキュメントを参照してください。

5.7.2 ID プロバイダー（AD FS 以外）の証明書を更新する

有効期限が近づいたなどの理由で、ID プロバイダーの証明書が更新された場合は、Keycloak に登録している ID プロバイダーの証明書を更新する必要があります。

証明書を更新する方法については、Keycloak および ID プロバイダーのドキュメントを参照してください。

5.8 ID プロバイダー（AD FS 以外）との連携で出力されるログ

AD FS 以外の ID プロバイダーとの連携では、Keycloak の操作ログが出力されます。連携でエラーとなった場合は、Keycloak の操作中に表示されるメッセージやログの内容を確認して、障害の要因を特定してください。

Keycloak のログファイルは、次のフォルダーに出力されます。

＜Common Servicesのインストールフォルダー＞¥logs¥idp¥log

6 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

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

操作手順

1. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. csportalservice コマンドを実行します。

コマンドの格納場所

＜Common Servicesのインストールフォルダー＞¥portal¥bin¥csportalservice.exe

サービスを起動する

```
csportalservice.exe /start
```

サービスを停止する

```
csportalservice.exe /stop
```

サービスを再起動する

```
csportalservice.exe /restart
```

サービスの起動状態を確認する

```
csportalservice.exe /status
```

6.2　証明書の有効期限または失効状態を確認する

証明書には有効期限が設定されています。また、セキュリティー上の理由などで認証局により証明書が失効されることがあります。証明書の有効期限切れや失効によって、Hitachi Ops Center 製品の SSL 通信が正常にできなくなることを防ぐため、次の方法で証明書の有効期限および失効状態を定期的に確認してください。

証明書の有効期限を確認する方法

- 6.2.1　トラストストア内の証明書の有効期限を確認する
- 6.2.2　サーバー証明書の有効期限を確認する

証明書の失効状態を確認する方法

- 6.2.3　サーバー証明書の失効状態を確認する

6.2.1　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のインストールフォルダー>¥jdk¥bin¥keytool" -list -v -keystore "<Common Servicesのインストールフォルダー>¥data¥tls¥cacerts"
```

6.2.2　サーバー証明書の有効期限を確認する

管理サーバーのサーバー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。3.1.2　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 サーバーの設定と 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のインストールフォルダー>¥jdk¥bin¥keytool" -printcert -file "<サーバー証明書のパス>"
```

6.2.3　サーバー証明書の失効状態を確認する

Hitachi Ops Center 製品のサーバー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。3.1.2　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 サーバーの設定と 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

管理サーバーで、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、認証局に問い合わせてください。
- サーバー証明書に 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。
- 管理サーバーから OCSP レスポンダーにアクセス可能で、プロキシー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、サーバー証明書を署名した認証局に問い合わせてください。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のインストールフォルダー>¥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> nul | "<Common Servicesのインストールフォルダー>¥openssl¥bin¥openssl" x509 -noout -text
```

コマンド実行例：

```
echo "Q" | "C:¥Program Files¥hitachi¥CommonServices¥openssl¥bin¥openssl" s_client -connect example.com:443 2> nul | "C:¥Program Files¥hitachi¥CommonServices¥openssl¥bin¥openssl" x509 -noout -text
```

サーバー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：(1)　Web ブラウザーを使用したサーバー証明書の失効確認
- openssl コマンド：(2)　コマンドを使用したサーバー証明書の失効確認
- 定期的に自動でコマンドを実行：(3)　定期的にサーバー証明書の失効状態を確認する

(1)　Web ブラウザーを使用したサーバー証明書の失効確認

Web ブラウザーの OCSP チェック機能を使用して、サーバー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ーに問い合わせて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。
2. 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。
   サーバー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。

(2)　コマンドを使用したサーバー証明書の失効確認

openssl コマンドの OCSP チェック機能を使用して、サーバー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

1. 管理サーバーで、次のopenssl コマンドを実行します。
   コマンド構文：

```
"＜Common Servicesのインストールフォルダー＞¥openssl¥bin¥openssl" ocsp -no_nonce -issuer ＜issuer証明書＞ -cert ＜サーバー証明書＞ -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：

```
"C:¥Program Files¥hitachi¥CommonServices¥openssl¥bin¥openssl" ocsp -no_nonce -issuer cacert.cer -cert httpsd.cer -url http://ad.example.com/ocsp -text
```

2. 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、サーバー証明書は失効しています。

(3) 定期的にサーバー証明書の失効状態を確認する

Hitachi Ops Center 製品のサーバー証明書の失効状態を定期的に確認します。タスクスケジューラにバッチファイルを登録して、失効状態の結果が定期的にファイルへ出力されるように設定します。

操作手順

1. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。

2. サーバー証明書の失効状態を確認する製品ごとに、管理サーバーの任意の場所に設定ファイルを作成します。RSA と ECDSA のサーバー証明書の両方を使用している製品は、設定ファイルを RSA と ECDSA で別に作成してください。設定ファイルのファイル拡張子は.conf で作成します。

   設定ファイルには、次の属性と値を指定します。対象の製品が Common Services と同じ管理サーバーにある場合と Common Services とは別の管理サーバーにある場合で、属性の指定が異なります。対象製品が別の管理サーバーにある場合は、サーバー証明書をダウンロードするための属性の指定が必要です。指定する項目は次のとおりです。

   設定ファイル

   ```
   DL_URL_HOSTNAME_IP=＜製品のURLのホスト名またはIPアドレス＞
   DL_URL_PORT=＜製品のURLのポート番号＞
   DL_SIGALGS=＜署名アルゴリズムリスト＞
   OCSP_ISSUER_CERT=＜issuer証明書＞
   OCSP_URI=＜OCSPレスポンダーのURI＞
   OCSP_PROXY_PROTOCOL=＜プロキシーの通信プロトコル＞
   OCSP_PROXY_USERINFO=＜プロキシーのuserinfo＞
   OCSP_PROXY_HOSTNAME_IP=＜プロキシーのホスト名またはIPアドレス＞
   OCSP_PROXY_PORT=＜プロキシーのポート番号＞
   OCSP_PROXY_PATH=＜プロキシーのパス＞
   OCSP_ROOT_CERT=＜OCSPレスポンダーサーバーのルート証明書のパス＞
   OCSP_RESULT_FILE=＜結果出力ファイルのパス＞
   STDERROR_LOG=＜標準エラー出力ファイルのパス＞
   SRV_CERT=＜サーバー証明書のダウンロード先のパスまたはサーバー証明書のパス＞
   ```

   設定項目

属性	説明
DL_URL_HOSTNAME_IP	（製品が別の管理サーバーにある場合）製品の URL のホスト名または IP アドレス 製品が同じ管理サーバーにある場合は属性の指定は不要です。
DL_URL_PORT	（製品が別の管理サーバーにある場合）製品の URL のポート番号 製品が同じ管理サーバーにある場合は属性の指定は不要です。
DL_SIGALGS	（製品が別の管理サーバーにある場合）署名アルゴリズムリスト RSA または ECDSA の署名アルゴリズムリストを指定します。次の値を指定してください。 RSA の場合：RSA+SHA256:RSA+SHA384:RSA+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512 ECDSA の場合：ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512 製品が同じ管理サーバーにある場合は属性の指定は不要です。

属性	説明
OCSP_ISSUER_CERT	issuer 証明書の絶対パス 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。
OCSP_URI	OCSP レスポンダーの URI
OCSP_PROXY_PROTOCOL	(任意) プロキシーの通信プロトコル OCSP レスポンダーの問い合わせにプロキシーを使用する場合に指定します。 http かhttps を指定してください。
OCSP_PROXY_USERINFO	(任意) プロキシーサーバーの認証情報 <*ユーザー名*>:<*パスワード*>の形式で指定します。 OCSP レスポンダーの問い合わせにプロキシーを使用する場合に指定します。
OCSP_PROXY_HOSTNAME_IP	(任意) プロキシーのホスト名または IP アドレス OCSP レスポンダーの問い合わせにプロキシーを使用する場合に指定します。
OCSP_PROXY_PORT	(任意) プロキシーのポート番号 OCSP レスポンダーの問い合わせにプロキシーを使用する場合に指定します。
OCSP_PROXY_PATH	(任意) プロキシーのパス OCSP レスポンダーの問い合わせにプロキシーを使用する場合に指定します。パスの先頭は/ (スラッシュ) で始めてください。
OCSP_ROOT_CERT	(任意) OCSP レスポンダーサーバーのルート証明書の絶対パス <*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、ルート証明書のパスを指定してください。
OCSP_RESULT_FILE	結果出力ファイルの絶対パス 製品の失効状態の結果を出力します。製品ごとに異なるパスを指定してください。
STDERROR_LOG	標準エラー出力ファイルの絶対パス openssl コマンドの標準エラー出力ファイルのパス。製品ごとに異なるパスを指定してください。
SRV_CERT	(製品が別の管理サーバーにある場合) サーバー証明書のダウンロード先の絶対パス (製品が同じ管理サーバーにある場合) サーバー証明書の絶対パス

設定ファイルの例 (製品が同じ管理サーバーにある場合):

```
OCSP_ISSUER_CERT=C:¥Users¥Administrator¥graviton.crt
OCSP_URI=http://example.com/ocsp
OCSP_PROXY_PROTOCOL=https
OCSP_PROXY_USERINFO=user:password
OCSP_PROXY_HOSTNAME_IP=hostname_proxy
OCSP_PROXY_PORT=8080
OCSP_PROXY_PATH=/proxy/path
OCSP_ROOT_CERT=C:¥Users¥Administrator¥root.crt
OCSP_RESULT_FILE=C:¥Users¥Administrator¥task_result.txt
STDERROR_LOG=C:¥Users¥Administrator¥task_ocsp_stderror.log
SRV_CERT=C:¥Users¥Administrator¥certificate.crt
```

設定ファイルの例（製品が別の管理サーバーにある場合）：

```
DL_URL_HOSTNAME_IP=hostname
DL_URL_PORT=443
DL_SIGALGS=RSA+SHA256:RSA+SHA384:RSA+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA5
12
OCSP_ISSUER_CERT=C:¥Users¥Administrator¥graviton.crt
OCSP_URI=http://example.com/ocsp
OCSP_PROXY_PROTOCOL=https
OCSP_PROXY_USERINFO=user:password
OCSP_PROXY_HOSTNAME_IP=hostname_proxy
OCSP_PROXY_PORT=8080
OCSP_PROXY_PATH=/proxy/path
OCSP_ROOT_CERT=C:¥Users¥Administrator¥root.crt
OCSP_RESULT_FILE=C:¥Users¥Administrator¥task_result.txt
STDERROR_LOG=C:¥Users¥Administrator¥task_ocsp_stderror.log
SRV_CERT=C:¥Users¥Administrator¥certificate.crt
```

3. バッチファイルを管理サーバーの任意の場所に作成します。

バッチファイルは、対象の製品が Common Services と同じ管理サーバーにある場合と Common Services とは別の管理サーバーにある場合で内容が異なります。同じ管理サーバーにある製品と別の管理サーバーにある製品の両方を確認する場合は、2 つのバッチファイルが必要です。

バッチファイルの内容（製品が同じ管理サーバーにある場合）：

```
@echo off
setlocal enabledelayedexpansion

set REG_ROOT="HKEY_LOCAL_MACHINE¥SOFTWARE¥Hitachi¥Common Services"
set REG_KEY="InstallDir"
FOR /F "TOKENS=1,2,*" %%I IN ('REG QUERY %REG_ROOT% /v %REG_KEY%') DO (
 IF "%%I"==%REG_KEY% set INSTALL_DIR=%%K¥CommonServices
)

set CMD_OPENSSL="%INSTALL_DIR%¥openssl¥bin¥openssl"

set CONF_FILE=%1

FOR /F "usebackq tokens=1,2 delims==" %%I IN (%CONF_FILE%) DO (
 set KEY=%%I
 set VAL=%%J

 set !KEY!=!VAL!
)

set CMD_OCSP_RESPONSE=%CMD_OPENSSL% ocsp ^
-no_nonce -issuer "%OCSP_ISSUER_CERT%" -cert "%SRV_CERT%" -url %OCSP_URI%

IF NOT "%OCSP_PROXY_HOSTNAME_IP%" == "" (

 set CMD_OCSP_RESPONSE_PROXY=

 IF NOT "!OCSP_PROXY_PROTOCOL!" == "" (
  set CMD_OCSP_RESPONSE_PROXY=!OCSP_PROXY_PROTOCOL!://
 )
 IF NOT "!OCSP_PROXY_USERINFO!" == "" (
```

```
  set CMD_OCSP_RESPONSE_PROXY=!CMD_OCSP_RESPONSE_PROXY!!OCSP_PROXY_USERINFO!@
 )
 set CMD_OCSP_RESPONSE_PROXY=!CMD_OCSP_RESPONSE_PROXY!!OCSP_PROXY_HOSTNAME_IP!
 IF NOT "!OCSP_PROXY_PORT!" == "" (
  set CMD_OCSP_RESPONSE_PROXY=!CMD_OCSP_RESPONSE_PROXY!:!OCSP_PROXY_PORT!
 )
 IF NOT "!OCSP_PROXY_PATH!" == "" (
  set CMD_OCSP_RESPONSE_PROXY=!CMD_OCSP_RESPONSE_PROXY!!OCSP_PROXY_PATH!
 )

 set CMD_OCSP_RESPONSE=!CMD_OCSP_RESPONSE! -proxy !CMD_OCSP_RESPONSE_PROXY!

)

IF NOT "%OCSP_ROOT_CERT%" == "" (
 set CMD_OCSP_RESPONSE=%CMD_OCSP_RESPONSE% -CAfile "%OCSP_ROOT_CERT%"
)

set CMD_OCSP_RESPONSE=%CMD_OCSP_RESPONSE% -text -out "%OCSP_RESULT_FILE%"

call %CMD_OCSP_RESPONSE%  2> "%STDERROR_LOG%"

exit /b 0
```

バッチファイルの内容（製品が別の管理サーバーにある場合）：

```
@echo off
setlocal enabledelayedexpansion

set REG_ROOT="HKEY_LOCAL_MACHINE¥SOFTWARE¥Hitachi¥Common Services"
set REG_KEY="InstallDir"
FOR /F "TOKENS=1,2,*" %%I IN ('REG QUERY %REG_ROOT% /v %REG_KEY%') DO (
 IF "%%I"==%REG_KEY% set INSTALL_DIR=%%K¥CommonServices
)

set CMD_OPENSSL="%INSTALL_DIR%¥openssl¥bin¥openssl"

set CONF_FILE=%1

FOR /F "usebackq tokens=1,2 delims==" %%I IN (%CONF_FILE%) DO (
 set KEY=%%I
 set VAL=%%J

 set !KEY!=!VAL!
)

set CERT_FLG=0
IF EXIST "%SRV_CERT%" del /q "%SRV_CERT%"

FOR /F "tokens=1 delims=" %%I IN (
 'echo "Q" ^| %CMD_OPENSSL% s_client ^
 -connect %DL_URL_HOSTNAME_IP%:%DL_URL_PORT% ^
 -sigalgs %DL_SIGALGS% 2^> "%STDERROR_LOG%"'
) DO (

 echo %%I | find "-BEGIN CERTIFICATE-" >NUL
 IF !ERRORLEVEL! EQU 0 set CERT_FLG=1
```

```
 IF !CERT_FLG! EQU 1 echo %%I>> "!SRV_CERT!"
 echo %%I | find "-END CERTIFICATE-" >NUL
 IF !ERRORLEVEL! EQU 0 goto END_CMD_CERT_DL

)

:END_CMD_CERT_DL

set CMD_OCSP_RESPONSE=%CMD_OPENSSL% ocsp -no_nonce ^
-issuer "%OCSP_ISSUER_CERT%" -cert "%SRV_CERT%" -url %OCSP_URI%

IF NOT "%OCSP_PROXY_HOSTNAME_IP%" == "" (

 set CMD_OCSP_RESPONSE_PROXY=

 IF NOT "!OCSP_PROXY_PROTOCOL!" == "" (
  set CMD_OCSP_RESPONSE_PROXY=!OCSP_PROXY_PROTOCOL!://
 )
 IF NOT "!OCSP_PROXY_USERINFO!" == "" (
  set CMD_OCSP_RESPONSE_PROXY=!CMD_OCSP_RESPONSE_PROXY!!OCSP_PROXY_USERINFO!@
 )
 set CMD_OCSP_RESPONSE_PROXY=!CMD_OCSP_RESPONSE_PROXY!!OCSP_PROXY_HOSTNAME_IP!
 IF NOT "!OCSP_PROXY_PORT!" == "" (
  set CMD_OCSP_RESPONSE_PROXY=!CMD_OCSP_RESPONSE_PROXY!:!OCSP_PROXY_PORT!
 )
 IF NOT "!OCSP_PROXY_PATH!" == "" (
  set CMD_OCSP_RESPONSE_PROXY=!CMD_OCSP_RESPONSE_PROXY!!OCSP_PROXY_PATH!
 )

 set CMD_OCSP_RESPONSE=!CMD_OCSP_RESPONSE! -proxy !CMD_OCSP_RESPONSE_PROXY!

)

IF NOT "%OCSP_ROOT_CERT%" == "" (
 set CMD_OCSP_RESPONSE=%CMD_OCSP_RESPONSE% -CAfile "%OCSP_ROOT_CERT%"
)

set CMD_OCSP_RESPONSE=%CMD_OCSP_RESPONSE% -text -out "%OCSP_RESULT_FILE%"

call %CMD_OCSP_RESPONSE% 2>> "%STDERROR_LOG%"

exit /b 0
```

4. Windows のタスクスケジューラで、失効状態の確認を行う製品ごとにタスクを登録します。タスクスケジューラの詳細については、Windows のドキュメントを参照してください。

   a. [スタート] − [Windows 管理ツール] − [タスク スケジューラ] を選択します。

   b. [基本タスクの作成] または [タスクの作成] で新規にタスクを作成します。

   c. [トリガー] にバッチファイルの起動時間を指定してください。指定した時間に結果ファイルが出力されます。

   d. [操作] を指定します。次の値を指定してください。

   - *プログラム/スクリプト：<バッチファイルのパス>*

- 引数の追加（オプション）：<*設定ファイルのパス*>
- 開始（オプション）：空白

操作結果

- タスクスケジューラで指定した時間に、<*結果出力ファイルのパス*>で指定したフォルダー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：サーバー証明書は有効
  - revoked の場合：サーバー証明書は失効
  - 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、設定ファイルの<*標準エラー出力ファイルのパス*>で指定したフォルダーに出力されるファイルを確認してください。

6.3 管理サーバーのホスト名または IP アドレス、ポート番号を変更する

管理サーバーのホスト名または 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. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. cschgconnect コマンドを実行します。

コマンドの格納場所

＜Common Servicesのインストールフォルダー＞¥utility¥bin¥cschgconnect.exe

書式

```
cschgconnect.exe [/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（FQDN）と IP アドレスは、Common Services や Hitachi Ops Center 製品をインストールする管理サーバー、および Hitachi Ops Center Portal にアクセスする Web ブラウザーで、名前解決ができ、アクセス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。

/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 通信用のサーバー証明書の作成時にCN や subjectAltName に指定したものから変更した場合、サーバー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. 次のコマンドを実行して、変更結果を確認します。

```
cschgconnect.exe /list
```

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://<*Portalのホスト名または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、該当する製品のマニュアルを参照してください。

6.4 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. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。

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	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 *＜Common Servicesのインストールフォルダー＞*¥data¥userconf¥config_user.properties 設定内容 CS_PORTAL_PORT=*＜変更後のポート番号＞* CS_GW_PORTAL_PORT=*＜変更後のポート番号＞* 2. Common Services のサービスを再起動します。
20952	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 *＜Common Servicesのインストールフォルダー＞*¥data¥userconf¥config_user.properties 設定内容 CS_PORTAL_IDP_PORT=*＜変更後のポート番号＞* CS_IDP_OP_HTTP_PORT=*＜変更後のポート番号＞* CS_GW_IDP_PORT=*＜変更後のポート番号＞* 2. Common Services のサービスを再起動します。
20954	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 *＜Common Servicesのインストールフォルダー＞*¥data¥userconf¥config_user.properties 設定内容 CS_PORTAL_IDP_POSTGRESQL_PORT=*＜変更後のポート番号＞* 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。 構成定義ファイルの格納場所 *＜Common Servicesのインストールフォルダー＞*¥pgdata¥csidp¥postgresql.conf 設定内容 port = *＜変更後のポート番号＞* # (change requires restart) 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、CommonServicesDBIdpService を再起動します。 net stop CommonServicesDBIdpService net start CommonServicesDBIdpService 5. Common Services のサービスを再起動します。

ポート番号	変更手順
20955	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 *＜Common Servicesのインストールフォルダー＞*¥data¥userconf¥config_user.properties 設定内容 CS_PORTAL_POSTGRESQL_PORT=*＜変更後のポート番号＞* 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。 構成定義ファイルの格納場所 *＜Common Servicesのインストールフォルダー＞*¥pgdata¥csportal¥postgresql.conf 設定内容 port = *＜変更後のポート番号＞* # (change requires restart) 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、CommonServicesDBPortalService を再起動します。 net stop CommonServicesDBPortalService net start CommonServicesDBPortalService 5. Common Services のサービスを再起動します。
20956	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 *＜Common Servicesのインストールフォルダー＞*¥data¥userconf¥config_user.properties 設定内容 CS_PORTAL_MANAGEMENT_PORT=*＜変更後のポート番号＞* 2. Common Services のサービスを再起動します。

6.5 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 Hitachi Ops Center 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、該当する製品のマニュアルを参照してください。
2. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
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のインストールフォルダー>¥utility¥bin¥csbackup.exe

   書式

   ```
   csbackup.exe /dir "<バックアップ先フォルダー>"
   ```

   オプション

   /dir "*<バックアップ先フォルダー>*"

   バックアップデータを格納するフォルダーパスを指定します。相対パスでも指定できます。指定したフォルダーに、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*_*VVRRSS*.jar
   VVRRSS は、Common Services のバージョンを表しています。

   (例)

   11.0.1-01 の場合、*VVRRSS* は 110101 になります。

   > **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. サーバー証明書および秘密鍵を次に示すフォルダー以外の場所に格納している場合、サーバー証明書および秘密鍵を手動でバックアップします。
   <Common Servicesのインストールフォルダー>¥data¥tls¥

メモ

cssslsetup コマンドで SSL 通信の設定をした場合、サーバー証明書の秘密鍵は、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。

6.6 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. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
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のインストールフォルダー>¥utility¥bin¥csrestore.exe

   書式

   ```
   csrestore.exe /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. サーバー証明書および秘密鍵を次に示すフォルダー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ー証明書と秘密鍵を配置します。

   <Common Servicesのインストールフォルダー>¥data¥tls¥

   > **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、サーバー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、6.3 管理サーバーのホスト名または 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 Hitachi Ops Center 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、該当する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、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、該当する製品のドキュメントを参照してください。

6.7 Hitachi Ops Center 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 Hitachi Ops Center 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. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. csresettrustrelationship コマンドを実行します。

   コマンドの格納場所

   <Common Servicesのインストールフォルダー>¥utility¥bin¥csresettrustrelationship.exe

   書式

   ```
   csresettrustrelationship.exe /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。

   <Common Servicesのインストールフォルダー>¥logs¥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、IDプロバイダーで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、連携しているIDプロバイダーに応じて下記を参照してください。

   - AD FSと連携している場合：(1)　AD FSでCommon Servicesのメタデータを更新する
   - AD FS以外のIDプロバイダーと連携している場合：5.7.1　Common Servicesの証明書を更新する

5. Common Servicesに登録している製品で、`setupcommonservice`コマンドを実行します。

6. Common Servicesに登録している製品のサービスを再起動します。

6.8 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、Hitachi Ops Center 製品に数分で適用されます。

メモ

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。

6.9　ウイルス検出プログラムを使用する場合に必要な設定

ウイ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、ウイルス検出プログラムのスキャン対象から、次のフォルダーを除外してください。

- *＜Common Servicesのインストールフォルダー＞*¥pgsql¥bin
- *＜Common Servicesのインストールフォルダー＞*¥nginx¥temp
- *＜Common Servicesのインストールフォルダー＞*¥data

ほかの Hitachi Ops Center 製品の対象外のフォルダーについては、該当する製品のマニュアルを参照してください。

6.10 Amazon Corretto をアップグレードする

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

操作手順

1. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. 脆弱性対応版の Amazon Corretto のバイナリーファイルを Zip 形式でダウンロードして、任意の場所で展開します。
3. Common Services のサービスを停止します。

   メモ

   管理サーバーに Amazon Corretto 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. 次のコマンドを実行して、Common Services で使用する JDK のシンボリックリンク先を変更します。

   ```
   rmdir "<Common Servicesのインストールフォルダー>¥jdk"
   mklink /d "<Common Servicesのインストールフォルダー>¥jdk" "<展開先に作成されたフォルダーのパス>"
   ```

5. Common Services のサービスを起動します。

   メモ

   管理サーバーに Amazon Corretto 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。

6.11 PostgreSQL をアップグレードする

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

操作手順

1. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. 脆弱性対応版の PostgreSQL のバイナリーファイルを Zip 形式でダウンロードして、Common Services がインストールされている管理サーバーに配置します。
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。

```
net stop CommonServicesDBIdpService
net stop CommonServicesDBPortalService
```

5. 次のコマンドを実行して、インストール済みの PostgreSQL を削除します。

```
rmdir /s "<Common Servicesのインストールフォルダー>¥pgsql"
```

6. ダウンロードしたファイルを Common Services のインストールフォルダーに展開します。

> **メモ**
>
> 作成されたフォルダー名がpgsql ではない場合、フォルダー名をpgsql に手動で変更してください。

7. 次のコマンドを実行して、Common Services のデータベースを起動します。

```
net start CommonServicesDBIdpService
net start CommonServicesDBPortalService
```

8. Common Services のサービスを起動します。

7 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、該当する製品のドキュメントを参照してください。

7.1 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。

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. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. コントールパネルを開いて、[プログラムと機能] を選択します。
3. [Hitachi Ops Center Common Services] を選択し、[アンインストール] をクリックします。
4. アンインストールウィザードの指示に従って、アンインストール前の確認画面で [削除] をクリックします。
5. ターゲットフォルダー（Common Services のインストールフォルダー）を削除するメッセージが表示されます。[OK] をクリックするとターゲットフォルダーは削除され、アンインストールを開始します。

   ターゲットフォルダーのデータが必要な場合は、[キャンセル] をクリックして確認画面に戻り、データを退避してください。
6. アンインストール完了の画面が表示されたら、[完了] をクリックします。

付録

付録 A　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、障害対応窓口に連絡してください。

付録 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. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
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のインストールフォルダー＞¥utility¥bin¥csgetras.exe

   書式

   ```
   csgetras.exe /dir ”＜出力先フォルダーのパス＞”
   ```

   オプション

   /dir ”*＜出力先フォルダーのパス＞*”

   収集した障害情報を出力するフォルダー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、該当する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ーで実施した次の障害情報については、実施したサーバー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.zip 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	*＜システムドライブ＞*¥Users¥*＜ユーザー名＞*¥AppData¥Roaming¥cs_utility	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。

付録 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。

出力先フォルダー

＜Common Servicesのインストールフォルダー＞¥logs

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。
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、付録 A.4　Common Services のメッセージを参照してください。

(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. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. 次のプロパティファイルを編集します。

   ＜Common Servicesのインストールフォルダー＞¥data¥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。 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。 指定できる値の範囲は、1～21 です。 デフォルト値：10
CS_PORTAL_LOG_MAX_INDEX_DEBUG	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。 指定できる値の範囲は、1～21 です。 デフォルト値：20
CS_PORTAL_LOG_MAX_INDEX_APPLOG	サーバー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。 指定できる値の範囲は、1～21 です。 デフォルト値：20

3. Common Services のサービスを再起動します。

付録 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、イベントログに出力されます。

出力項目

監査ログに出力される項目は次のとおりです。

項目	出力内容	出力例
ログの名前	イベントログの作成先	Application
ソース	Common Services	Common Services
日付	メッセージが出力された時刻	2024/02/21 11:22:33
イベント ID	1	1
タスクのカテゴリ	なし	なし
レベル	情報、警告、エラーなどのレベル	情報
キーワード	クラシック	クラシック
ユーザー	SYSTEM	SYSTEM
コンピュータ	コンピュータ名	WIN-00ABCD11EFG
説明	以下の内容がコンマで区切られて出力されます。 • メッセージ ID • 監査事象の種別（ConfigurationAccess、Authentication などの種別） • 監査事象の結果（成功、失敗など、事象の結果） • サブジェクト識別情報（ユーザー ID、URI、HTTP Method など） • メッセージ	KAOP90001-I,Authentication,Success,User ID=system,URI=/portal,HTTP Method=GET,get user (status = 200 OK)
オペコード	情報	情報

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、付録 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

監査ログに出力される監査事象

Common Services では、次に示す種別の監査事象が監査ログに出力されます。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-x

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。監査ログ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。種別により通し番号が異なります。

- KAOP9800*N*：Authentication のメッセージ
- KAOP90*NNN*：ConfigurationAccess のメッセージ

x

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。
- I（Information）：ユーザーに情報を通知するメッセージです。

種別がAuthentication の場合

詳細種別	監査事象	メッセージ
ユーザーの認証	ログイン成功	KAOP98001-I,Authentication,Success,type=LOGIN
	ログイン失敗	KAOP98002-E,Authentication,Failed,type=LOGIN_ERROR
	ログアウト成功	KAOP98001-I,Authentication,Success,type=LOGOUT
	ログアウト失敗	KAOP98002-E,Authentication,Failed,type=LOGOUT_ERROR
プロファイル	アカウント編集成功	KAOP98001-I,Authentication,Success,type=UPDATE_PROFILE
	アカウント編集失敗	KAOP98002-E,Authentication,Failed,type=UPDATE_PROFILE_ERROR

詳細種別	監査事象	メッセージ
プロファイル	パスワード変更成功	KAOP98001-I,Authentication,Success,type=UPDATE_PASSWORD
	パスワード変更失敗	KAOP98002-E,Authentication,Failed,type=UPDATE_PASSWORD_ERROR

- 監査ログには、この表に記載されているメッセージ ID 以外のログも出力されますが、Common Services の内部処理で出力されるものです。
- メッセージ ID と type の値で監査ログの事象を判定してください。

種別がConfigurationAccess の場合

詳細種別	監査事象	メッセージ
ユーザー	ユーザー作成成功	KAOP90001-I
	ユーザー作成失敗	KAOP90002-E
	ユーザー一覧の取得成功	KAOP90003-I
	ユーザー一覧の取得失敗	KAOP90004-E
	特定のユーザー情報の取得成功	KAOP90005-I
	特定のユーザー情報の取得失敗	KAOP90006-E
	特定のユーザー情報の更新成功	KAOP90007-I
	特定のユーザー情報の更新失敗	KAOP90008-E
	ユーザーの削除成功	KAOP90009-I
	ユーザーの削除失敗	KAOP90010-E
	特定のユーザーが属するユーザーグループ一覧の取得成功	KAOP90011-I
	特定のユーザーが属するユーザーグループ一覧の取得失敗	KAOP90012-E
ユーザーグループ	ユーザーグループへのユーザーの追加成功	KAOP90013-I
	ユーザーグループへのユーザーの追加失敗	KAOP90014-E
	ユーザーグループからのユーザー削除成功	KAOP90015-I
	ユーザーグループからのユーザー削除失敗	KAOP90016-E
	ユーザーパスワードリセット成功	KAOP90017-I
	ユーザーパスワードリセット失敗	KAOP90018-E
	ユーザーグループの登録成功	KAOP90019-I
	ユーザーグループの登録失敗	KAOP90020-E
	ユーザーグループ一覧の取得成功	KAOP90021-I
	ユーザーグループ一覧の取得失敗	KAOP90022-E

詳細種別	監査事象	メッセージ
ユーザーグループ	ユーザーグループの登録情報の更新成功	KAOP90023-I
	ユーザーグループの登録情報の更新失敗	KAOP90024-E
	特定のユーザーグループ情報の取得成功	KAOP90025-I
	特定のユーザーグループ情報の取得失敗	KAOP90026-E
	ユーザーグループの削除成功	KAOP90027-I
	ユーザーグループの削除失敗	KAOP90028-E
	特定のユーザーグループに属するユーザー一覧の取得成功	KAOP90029-I
	特定のユーザーグループに属するユーザー一覧の取得失敗	KAOP90030-E
	特定のユーザーグループに割り当てられているロール一覧の取得成功	KAOP90031-I
	特定のユーザーグループに割り当てられているロール一覧の取得失敗	KAOP90032-E
	ユーザーグループへのロールの割り当て成功	KAOP90033-I
	ユーザーグループへのロールの割り当て失敗	KAOP90034-E
	ユーザーグループに割り当てられているロールの削除成功	KAOP90035-I
	ユーザーグループに割り当てられているロールの削除失敗	KAOP90036-E
	特定のユーザーグループに割り当てることができるロール一覧の取得成功	KAOP90037-I
	特定のユーザーグループに割り当てることができるロール一覧の取得失敗	KAOP90038-E
ユーザーディレクトリ	Active Directory または LDAP サーバーの登録成功	KAOP90039-I
	Active Directory または LDAP サーバーの登録失敗	KAOP90040-E
	Active Directory または LDAP サーバーの一覧の取得成功	KAOP90041-I
	Active Directory または LDAP サーバーの一覧の取得失敗	KAOP90042-E
	特定の Active Directory または LDAP サーバーに関する情報の取得成功	KAOP90043-I
	特定の Active Directory または LDAP サーバーに関する情報の取得失敗	KAOP90044-E
	Active Directory または LDAP サーバーに関する情報の更新成功	KAOP90045-I
	Active Directory または LDAP サーバーに関する情報の更新失敗	KAOP90046-E
	Active Directory または LDAP サーバーに関する情報の削除成功	KAOP90047-I
	Active Directory または LDAP サーバーに関する情報の削除失敗	KAOP90048-E
	ユーザーグループの同期成功	KAOP90049-I
	ユーザーグループの同期失敗	KAOP90050-E

詳細種別	監査事象	メッセージ
ユーザーディレクトリ	Active Directory サーバーの接続テストと認証テストの実行成功	KAOP90051-I
	Active Directory サーバーの接続テストと認証テストの実行失敗	KAOP90052-E
setupcommonservice コマンド	製品の登録成功	KAOP90053-I
	製品の登録失敗	KAOP90054-E
プロダクト	Common Services に登録されている製品一覧の取得成功	KAOP90055-I
	Common Services に登録されている製品一覧の取得失敗	KAOP90056-E
	Common Services に登録された特定の製品に関する情報の取得成功	KAOP90057-I
	Common Services に登録された特定の製品に関する情報の取得失敗	KAOP90058-E
	製品の登録情報の更新成功	KAOP90059-I
	製品の登録情報の更新失敗	KAOP90060-E
	製品の削除成功	KAOP90061-I
	製品の削除失敗	KAOP90062-E
	Common Services に登録されている特定製品の構成情報の取得成功	KAOP90063-I
	Common Services に登録されている特定製品の構成情報の取得失敗	KAOP90064-E
	Common Services に登録されている特定製品のバージョン情報の取得成功	KAOP90065-I
	Common Services に登録されている特定製品のバージョン情報の取得失敗	KAOP90066-E
	Common Services に登録されている特定製品のステータス情報の取得成功	KAOP90067-I
	Common Services に登録されている特定製品のステータス情報の取得失敗	KAOP90068-E
	Common Services に登録されている特定製品のライセンス情報の取得成功	KAOP90069-I
	Common Services に登録されている特定製品のライセンス情報の取得失敗	KAOP90070-E
データセンター	データセンターの登録成功	KAOP90071-I
	データセンターの登録失敗	KAOP90072-E
	データセンターの一覧の取得成功	KAOP90073-I
	データセンターの一覧の取得失敗	KAOP90074-E
	特定のデータセンターに関する情報の取得成功	KAOP90075-I
	特定のデータセンターに関する情報の取得失敗	KAOP90076-E
	データセンターの登録情報の更新成功	KAOP90077-I

詳細種別	監査事象	メッセージ
データセンター	データセンターの登録情報の更新失敗	KAOP90078-E
	データセンターの削除成功	KAOP90079-I
	データセンターの削除失敗	KAOP90080-E
	特定のデータセンターに登録されている製品一覧の取得成功	KAOP90081-I
	特定のデータセンターに登録されている製品一覧の取得失敗	KAOP90082-E
	Common Services に登録した製品のデータセンターへの登録成功	KAOP90083-I
	Common Services に登録した製品のデータセンターへの登録失敗	KAOP90084-E
	Common Services に登録されている製品のデータセンターからの削除成功	KAOP90085-I
	Common Services に登録されている製品のデータセンターからの削除失敗	KAOP90086-E
パスワードポリシー	パスワードポリシーの取得成功	KAOP90087-I
	パスワードポリシーの取得失敗	KAOP90088-E
	パスワードポリシーの更新成功	KAOP90089-I
	パスワードポリシーの更新失敗	KAOP90090-E
警告バナー	バナーの取得成功	KAOP90091-I
	バナーの取得失敗	KAOP90092-E
	バナーの更新成功	KAOP90093-I
	バナーの更新失敗	KAOP90094-E
	バナーのプレビュー成功	KAOP90095-I
	バナーのプレビュー失敗	KAOP90096-E
	バナーのタグの取得成功	KAOP90097-I
	バナーのタグの取得失敗	KAOP90098-E
バージョン情報	Common Services のバージョン情報の取得成功	KAOP90099-I
	Common Services のバージョン情報の取得失敗	KAOP90100-E
アクセストークン	アクセストークン取得成功	KAOP90103-I
	アクセストークン取得失敗	KAOP90104-E
	アクセストークンを取得したユーザーに関する情報の取得成功	KAOP90105-I
	アクセストークンを取得したユーザーに関する情報の取得失敗	KAOP90106-E
登録済みの製品が定期的に実行	連携製品の状態通知成功	KAOP90109-I
	連携製品の状態通知失敗	KAOP90110-E

詳細種別	監査事象	メッセージ
ログイン	ログインユーザーのプロファイル取得成功	KAOP90111-I
	ログインユーザーのプロファイル取得失敗	KAOP90112-E
ログインバナー	ログインバナーの取得成功	KAOP90113-I
	ログインバナーの取得失敗	KAOP90114-E
GUI 各操作時のセッションおよびトークン状態のチェック	ログインユーザーステータス取得成功	KAOP90115-I
	ログインユーザーステータス取得失敗	KAOP90116-E
プロダクト削除	製品への削除通知失敗	KAOP90125-W
Kerberos 接続設定	Kerberos 認証接続情報の取得成功	KAOP90126-I
	Kerberos 認証接続情報の取得失敗	KAOP90127-E
	Kerberos 接続設定の更新成功	KAOP90128-I
	Kerberos 接続設定の更新失敗	KAOP90129-E
	Kerberos 領域の作成成功	KAOP90130-I
	Kerberos 領域の作成失敗	KAOP90131-E
	Kerberos 領域の削除成功	KAOP90132-I
	Kerberos 領域の削除失敗	KAOP90133-E
	Kerberos 認証のための特定領域に関する情報の取得成功	KAOP90134-I
	Kerberos 認証のための特定領域に関する情報の取得失敗	KAOP90135-E
	Kerberos 認証用領域情報の一覧の取得成功	KAOP90136-I
	Kerberos 認証用領域情報の一覧の取得失敗	KAOP90137-E
	Kerberos 領域情報の更新成功	KAOP90138-I
	Kerberos 領域情報の更新失敗	KAOP90139-E
ID プロバイダー	メタデータのインポート成功	KAOP90172-I
	メタデータのインポート失敗	KAOP90173-E
	ID プロバイダーの登録成功	KAOP90174-I
	ID プロバイダーの登録失敗	KAOP90175-E
	メタデータのエクスポート成功	KAOP90176-I
	メタデータのエクスポート失敗	KAOP90177-E
	ID プロバイダーの一覧の取得成功	KAOP90178-I
	ID プロバイダーの一覧の取得失敗	KAOP90179-E
	特定の ID プロバイダーに関する情報の取得成功	KAOP90180-I

詳細種別	監査事象	メッセージ
ID プロバイダー	特定の ID プロバイダーに関する情報の取得失敗	KAOP90181-E
	ID プロバイダーの登録情報の更新成功	KAOP90182-I
	ID プロバイダーの登録情報の更新失敗	KAOP90183-E
	ID プロバイダーの削除成功	KAOP90184-I
	ID プロバイダーの削除失敗	KAOP90185-E
認証キー	認証キー設定の取得成功	KAOP90186-I
	認証キー設定の取得失敗	KAOP90187-E
	認証キーの更新間隔の更新成功	KAOP90188-I
	認証キーの更新間隔の更新失敗	KAOP90189-E
	認証キーの更新成功	KAOP90190-I
	認証キーの更新失敗	KAOP90191-E
ユーザーディレクトリ	外部認証サーバーの全てのユーザーの同期成功	KAOP90192-I
	外部認証サーバーの全てのユーザーの同期失敗	KAOP90193-E
	Active Directory または LDAP サーバーから取得するユーザー数の確認成功	KAOP90196-I
	Active Directory または LDAP サーバーから取得するユーザー数の確認失敗	KAOP90197-E
プロダクト	製品のセッション情報の取得成功	KAOP90198-I
	製品のセッション情報の取得失敗	KAOP90199-E
セッション制御	セッション設定情報の取得成功	KAOP90200-I
	セッション設定情報の取得失敗	KAOP90201-E
	セッション設定情報の更新成功	KAOP90202-I
	セッション設定情報の更新失敗	KAOP90203-E

(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. 管理サーバーに Administrator 権限を持つユーザーとしてログインします。
2. 次のプロパティファイルを編集します。
   <Common Servicesのインストールフォルダー>¥data¥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_ENABLE	監査ログの取得可否を次の値で指定します。 • true：監査ログを取得する • false：監査ログを取得しない デフォルト値：false
CS_PORTAL_AUDIT_LEVEL	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。 • 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。 • 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。

付録 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 とインストーラー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**

メッセージ ID	メッセージテキスト	要因と対処
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。	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 100 人を超えています。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。	**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** 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。	**要因**
		次の要因が考えられます。
		• 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。
		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。
		`cd <Common Servicesのインストールフォルダー>¥data¥banner`
		`copy /y banner.json.template banner.json`
		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。

KAOP10013-W	条件に一致するユーザー数が 1000 人を超えています。条件を変更して再実行してください。	**要因** - **対処**

メッセージ ID	メッセージテキスト	要因と対処
KAOP10013-W	条件に一致するユーザー数が 1000 人を超えています。条件を変更して再実行してください。	条件に一致するユーザー数が 1～1000 となるよう再設定してください。
KAOP10014-W	結果はありませんでした。条件を変更して再実行してください。	**要因** - **対処** 条件に一致するユーザー数が 1～1000 となるよう再設定してください。
KAOP20008-E	Bad Request.	**要因** リクエストパラメーターに誤りがあります。 **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。
KAOP20009-E	Unauthorized.	**要因** 認証されていません。 **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。
KAOP20011-E	Forbidden.	**要因** 次のいずれかの原因が考えられます。 • 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。 **対処** 次のいずれかで対処してください。 • 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.	**要因** 次のいずれかの原因が考えられます。 • 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。 **対処** 次のいずれかで対処してください。 • 正しいパスを指定してください。 • 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.	**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。 **対処** 正しい HTTP メソッドを使用して再実行してください。
KAOP20015-E	Request Timeout.	**要因**

メッセージ ID	メッセージテキスト	要因と対処
KAOP20015-E	Request Timeout.	リクエストがタイムアウトしました。 **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。
KAOP20016-E	Conflict.	**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。 **対処** 重複した値を変更して再実行してください。
KAOP20033-E	An unexpected error has occurred. Contact 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、障害対応窓口に連絡してください。
KAOP20035-E	Bad Gateway.	**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。 **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。
KAOP20037-E	Gateway Timeout.	**要因** ゲートウェイがタイムアウトしました。 **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。
KAOP20047-E	The built-in role (＜*orion.portal.builtin-object.role.role-user のプロパティ値*＞) cannot be removed.	**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ました。 **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。
KAOP20048-E	The built-in group cannot be deleted.	**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ました。 **対処**

メッセージ ID	メッセージテキスト	要因と対処
KAOP20049-E	The built-in user cannot be deleted.	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 <*orion.portal.builtin-object.group.group-user 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ました。 **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** 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。

メッセージ ID	メッセージテキスト	要因と対処
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、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。 別の管理サーバーにインストールされた Common Services と連携する場合は、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 ユーザーグループにロールを割り当てることはできません。

メッセージ ID	メッセージテキスト	要因と対処
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のインストールフォルダー＞*¥data¥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。

メッセージ ID	メッセージテキスト	要因と対処
KAOP20069-E	The specified group already exists. Revise the specified name.	**対処** name を見直して再実行してください。
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ー証明書のルート

メッセージ ID	メッセージテキスト	要因と対処
KAOP20087-E	The metadata endpoint is incorrect or the certificate is not set correctly.	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 email address belonging to the Common Services user.	**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 サーバーとの SSL/TLS の設定に誤りがあります。 **対処** LDAP サーバーとの 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 サーバーのホスト名、アドレスまたはポート番号に誤りがあります。 **対処** LDAP サーバーのホスト名、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 サーバーのバインド DN またはパスワードに誤りがあります。 **対処** LDAP サーバーのバインド 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 サーバーの URI または DN に誤りがあります。 **対処** LDAP サーバーの 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 サーバーの URI に誤りがあります。 **対処** LDAP サーバーの URI を見直して操作を再度実行してください。

メッセージ ID	メッセージテキスト	要因と対処
KAOP20095-E	One or more of the supplied parameters is incorrect.	**要因** LDAP サーバーのパラメーターに誤りがあります。 **対処** LDAP サーバー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ました。 **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ました。 **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。
KAOP20098-E	Renaming of built-in groups 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ました。 **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: *<フォルダー名>*).	**要因** 一時フォルダー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フォルダーを手動で削除してください。
KAOP60312-W	Cannot archive the directory (directory name: *<フォルダー名>*).	**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。

メッセージ ID	メッセージテキスト	要因と対処
KAOP60621-E	An option is invalid: csgetras.exe /dir DirectoryName	**要因** シンタックスが誤っています。 **対処** オプションまたはフォルダーパスを見直して、再実行してください。
KAOP60623-E	Cannot make the directory (directory name: *<フォルダー名>*).	**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. 指定したフォルダー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: *<フォルダー名>*)	**要因** /dir オプションに指定されたフォルダーが、RAS 情報収集対象フォルダー内です。 **対処** 別のフォルダー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** 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。
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、障害対応窓口に連絡してください。
KAOP60646-E	Collection of RAS log data for Common Services failed. The required Common Services file for csgetras is missing. Perform a repair installation of Common Services and run csgetras again. If you are unable to resolve this error, contact the Support Center.	**要因** *<Common Servicesのインストールフォルダー>*¥utility¥conf¥ras_collect_list.conf ファイルまたは、*<Common Servicesのインストールフォルダー>*¥utility¥conf¥ras_acl_list.conf ファイルが存在しません。 **対処** Common Services の修復インストールを実施し、csgetras コマンドを再度実行してください。 解決できない場合、障害対応窓口に連絡してください。
KAOP61003-E	An option is invalid: csbackup.exe /dir DirectoryName	**要因** シンタックスが誤っています。

メッセージ ID	メッセージテキスト	要因と対処
KAOP61003-E	An option is invalid: csbackup.exe /dir DirectoryName	**対処** オプションまたはフォルダーパスを見直して、再実行してください。
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。
KAOP61006-E	Collection of backup data for Common Services failed. The required Common Services file for csbackup is missing. Perform a repair installation of Common Services and run csbackup again. If you are unable to resolve this error, contact the Support Center.	**要因** *＜Common Servicesのインストールフォルダー＞*¥utility¥conf¥backup_file_list.conf ファイルが存在しません。 **対処** Common Services の修復インストールを実施し、バックアップを再度実行してください。 解決できない場合、障害対応窓口に連絡してください。
KAOP61007-E	Collection of backup data for Common Services failed. The backup target file is missing. Perform a repair installation of Common Services and run csbackup again. If you are unable to resolve this error, contact the Support Center.	**要因** バックアップ対象のファイルが存在しません。 **対処** Common Services の修復インストールを実施し、バックアップを再度実行してください。 解決できない場合、障害対応窓口に連絡してください。
KAOP61008-E	Common Services backup failed. If the Common Services directory and the backup destination directory permissions differ, change the permissions of the destination directory to match. If you cannot resolve this error, contact the Support Center.	**要因** バックアップ先のアーカイブファイルに対して、backup_file_list.conf ファイルのコピーに失敗しました。 **対処** コピー元とコピー先、両方のユーザー権限を確認してバックアップを再度実行してください。 解決できない場合、障害対応窓口に連絡してください。
KAOP61009-E	Collection of backup data for Common Services failed. Perform a repair installation of Common Services and run csbackup again. If you are unable to resolve this error, contact the Support Center.	**要因** データベースのバックアップに失敗しました。 **対処** Common Services の修復インストールを実施し、バックアップを再度実行してください。 解決できない場合、障害対応窓口に連絡してください。
KAOP61624-E	Output directory is included in the backup source directory. (directory name: *＜フォルダー名＞*).	**要因** /dir オプションに指定されたフォルダーが、バックアップ対象フォルダー内です。 **対処** 別のフォルダーを指定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
KAOP62003-E	An option is invalid: csrestore.exe /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。
KAOP62006-E	The target backup file cannot be restored for the following reason:	**要因** 「次の理由によります」以降の原因によるエラーが発生しました。 **対処** 「次の理由によります」以降に表示されるメッセージに、原因と対処方法が表示されますので、その方法に沿って対処してください。
KAOP62007-E	The backup file name is incorrect. (file name: <*ファイル名*>)(format: csbackup_*YYYY-MM-DD-hh-mm-ss*_VVRRSS.jar	**要因** `csrestore.exe` の`/file` オプションに指定したファイル名が、所定の書式に一致していません。 **対処** ファイル名の書式に沿って、正しいバックアップファイル名を指定してください。
KAOP62008-E	Restoration of backup data for Common Services failed. The specified backup file cannot be found. Please check the file path and run csrestore again.	**要因** 指定されたバックアップのアーカイブファイルが存在しません。 **対処** 実在するバックアップファイルを指定して、リストアを実施してください。 解決できない場合、障害対応窓口に連絡してください。
KAOP62009-E	The Common Services restore failed. If the user permissions for both Common Services directories differ from those at the time of the backup, change the permissions in the current directory to match. If you cannot resolve this error, contact your Support Center.	**要因** バックアップ元からバックアップ先へのフォルダーとファイルのコピーに失敗しました。 **対処** コピー元とコピー先、両方のユーザー権限を確認してリストアを再度実行してください。 解決できない場合、障害対応窓口に連絡してください。
KAOP62032-E	Cannot make the temporary directory (directory name: <*フォルダー名*>).	**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. 指定したフォルダー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	**要因**

メッセージ ID	メッセージテキスト	要因と対処
KAOP63003-E	access URL. You cannot use this option if you have already used an IP address in the access URL.	/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。 **対処** 次の対処をしてください。 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.	**要因** 証明書署名要求と秘密鍵の作成に失敗しました。 **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、障害対応窓口に連絡してください。
KAOP64003-E	An error occurred. Contact support, who may ask you to collect troubleshooting information of the corresponding product. Product=<*製品名*>	**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。
KAOP64006-W	Setting SSL for server failed for some products.	**要因** 一部の製品で、SSL サーバー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、障害対応窓口に連絡してください。
KAOP64007-E	Setting SSL for server failed.	**要因** SSL サーバー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、障害対応窓口に連絡してください。
KAOP64009-W	Setting SSL for client failed for some products.	**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。 **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。
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
KAOP64012-E	Enable/disable certificate verification failed.	**要因** サーバー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、Hitachi Ops Center 製品を Common Services に再登録してください。
KAOP64017-W	The IP address information cannot be obtained. Therefore, accessing the URL by IP address is not possible. Check the connection and try again later.	**要因** IP アドレスを取得できなかったため，設定値の登録をおこないません。 **対処**

メッセージ ID	メッセージテキスト	要因と対処
KAOP64017-W	The IP address information cannot be obtained. Therefore, accessing the URL by IP address is not possible. Check the connection and try again later.	ネットワークの設定を確認してから再実行します。 ipconfig で自ホストの IP アドレスが表示されるか確認してください。
KAOP64019-E	Configuring SSL failed because the following definitions do not exist in *<製品名>*. Please check the configuration file.	**要因** 対象のプロパティが存在しません。 **対処** 対象の製品のマニュアルに従い、未定義のプロパティを設定ファイルに追加してください。
KAOP64020-W	The following command generated an error. Use the return value to determine the cause and take action. Refer to the manual for *<製品名>*. command: *<コマンドのパス>* return code: *<コマンドの戻り値>*	**要因** インスタンス取得コマンドがエラー終了しました。 **対処** エラーコードから原因を特定し、対象製品のマニュアルに従って対処してください。
KAOP64021-I	The instance environment does not exist. Please create one or more instances and try again. Refer to the manual for *<製品名>*.	**要因** インスタンスが存在しません。 **対処** 対象製品のマニュアルに従ってインスタンスを作成してから再実行してください。
KAOP70000-E	ディスク領域が不足しているため、インストーラを起動できません。	**要因** システムドライブのディスク領域が不足しています。 **対処** システムドライブのディスク領域について、必要な容量を確保してください。
KAOP70001-E	ディスク領域が不足しているため、削除機能を開始できません。	**要因** システムドライブのディスク領域が不足しています。 **対処** システムドライブのディスク領域について、必要な容量を確保してください。
KAOP70002-E	この場所には、インストール用の十分なスペースがありません。スペースを追加します。	**要因** 以下のいずれかのディスク容量が足りません。 • インストール先フォルダー • データ格納先フォルダー • ログ格納先フォルダー **対処** 以下のフォルダー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。 • インストール先フォルダー • データ格納先フォルダー • ログ格納先フォルダー

メッセージ ID	メッセージテキスト	要因と対処
KAOP70006-E	エラーが発生しました。Common Services のインストールは停止します。 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。	**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。
KAOP70007-E	データベースのバックアップに失敗しました。 これでインストールが終了します。バックアップ先に十分な未使用容量がない可能性があります。バックアップ先で十分な容量を解放してから、インストールを再試行してください。 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。	**要因** バックアップ先のフォルダー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** バックアップ先の別のフォルダー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、障害対応窓口に連絡してください。
KAOP70010-E	この OS バージョンでは、Common Services をインストールできません。Common Services のサポートされている OS バージョンを確認します。	**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	この OS では、Common Services はサポートされていません。Common Services でサポートされている OS を確認します。	**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	Hitachi Ops Center の評価版が既にインストールされているため、インストールが停止します。Hitachi Ops Center のフルバージョンを評価版と一緒に使用することはできません。評価版をアンインストールしてから、インストールを再試行してください。	**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	インストールを実行することはできません。別のベンダからの Common Services がインストールされています。インストールが停止します。サポートにお問い合わせください。	**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に連絡してください。
KAOP70016-E	ダウングレードすることはできません。Common Services のより新しいバージョンがインストールされています。ダウングレードは停止します。	**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。

メッセージ ID	メッセージテキスト	要因と対処
KAOP70028-E	内部エラーが発生しました。インストールが停止します。 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。	**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。
KAOP70029-E	このディレクトリを使用できないため、削除は取り消されました。別のディレクトリに移動して再実行してください。	**要因** 現在参照しているフォルダーが削除対象のため、アンインストールを中止します。 **対処** 別のフォルダーに移動して再実行してください。
KAOP70030-W	Common Services によって使用されているプログラムを削除できませんでした。 再インストールするには、このプログラムを削除する必要があります。削除手順の詳細については、カスタマーサポートにお問い合わせください。 Common Services をインストールしたくない場合は、問題ありません。	**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	＜*IP アドレス*＞ に対して接続チェックが行われましたが、応答がありませんでした。 Hitachi Ops Center 製品が宛先として ＜*IP アドレス*＞ を使用して通信を実行するため、通信エラーが発生した可能性があります。 値を確認します。 ネットワーク設定によっては、指定した値に問題がなくてもこのメッセージが表示されることがあります。この場合は、このメッセージを無視してインストールを続行してください。	**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。
KAOP70040-W	入力されたポート番号が無効です。1 ～ 65535 の値を入力します。	**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。
KAOP70044-E	エラーが発生しました。 Hitachi Ops Center インストールは停止します。 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。	**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、障害対応窓口に連絡してください。
KAOP70050-E	管理サーバの仮想メモリの空き領域は、＜*空き容量*＞ MB です。Common Services には、＜*必要な容量*＞ MB の仮想メモリが必要であるため、さらに追加する必要があります。空き領域が不足すると、システムが不安定に	**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。

メッセージ ID	メッセージテキスト	要因と対処
KAOP70050-E	なり、プログラムを実行できなくなる可能性があります。	**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	データベースサービスをアクティブ化できませんでした。	**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、障害対応窓口に連絡してください。
KAOP70054-E	IP アドレスまたはホスト名に無効な文字が含まれています。 有効な文字: a-z 0-9 . -	**要因** IP アドレスまたはホスト名に使用できない文字が含まれています。 **対処** IP アドレスまたはホスト名は、次の文字で指定してください。 a～z 0～9 . -
KAOP70055-E	非管理者ユーザーは、インストールを実行できません。管理者ユーザーとしてログイン後、インストーラを起動します。	**要因** 管理者権限がないユーザーでsetup.exe を実行しました **対処** 管理者権限を持つユーザーでsetup.exe を実行してください。
KAOP70057-E	インストールに必要なファイル<*ファイルパス*>は読み取れません。 原因: インストールメディア上のファイルが不足しているか、実行権限がありません。 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。	**要因** インストールメディア上のファイルが不足しているか、実行権限がありません。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。 **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、障害対応窓口に連絡してください。
KAOP70058-E	インストールパスには最大 64 文字を指定してください。	**要因** インストール先のパスには 65 文字以上は指定できません。 **対処** インストール先のパスには 64 文字以下を指定してください。
KAOP70059-E	インストールパスに無効な文字が含まれています。 有効な文字: A ～ Z a ～ z 0-9 . _ 半角スペース	**要因** インストールフォルダーに無効な文字が含まれています。 有効な文字:A～Z a～z 0～9 . _ 半角スペース これらのフォルダーやパスは指定できないことに注意してください:

メッセージ ID	メッセージテキスト	要因と対処
KAOP70059-E	これらのディレクトリーやパスは指定できないことに注意してください: • ドライブ直下 • UNC • OS 予約語 • ネットワークドライブ • CD/DVD ドライブ • 存在しないドライブ • 禁止パス • シンボリックリンクやジャンクションを含むパス	• ドライブ直下 • UNC • OS 予約語 • ネットワークドライブ • CD/DVD ドライブ • 存在しないドライブ • 禁止パス • シンボリックリンクやジャンクションを含むパス **対処** 要因に応じて、問題を解決してください。
KAOP70060-E	バックアップファイルのパスには最大 150 文字を指定します。	**要因** バックアップファイルのパスには 151 文字以上は指定できません。 **対処** バックアップファイルのパスには最大 150 文字以下を指定してください。
KAOP70061-E	無効な文字がバックアップファイルのパスに含まれています。 有効な文字: A ～ Z a ～ z 0-9 . _ 半角スペース これらのディレクトリーやパスは指定できないことに注意してください: ・ドライブ直下 ・UNC ・OS 予約語 ・ネットワークドライブ ・CD/DVD ドライブ ・存在しないドライブ ・禁止パス ・シンボリックリンクやジャンクションを含むパス	**要因** 無効な文字がバックアップファイルのパスに含まれています。 有効な文字:A～Z a～z 0～9 . _ 半角スペース これらのフォルダーやパスは指定できないことに注意してください: • ドライブ直下 • UNC • OS 予約語 • ネットワークドライブ • CD/DVD ドライブ • 存在しないドライブ • 禁止パス • シンボリックリンクやジャンクションを含むパス **対処** 要因に応じて、問題を解決してください。
KAOP70062-E	IP アドレスまたはホスト名が長すぎます。IP アドレスまたはホスト名は最大 128 文字で指定してください。	**要因** IP アドレスまたはホスト名には 129 文字以上は指定できません。 **対処** IP アドレスまたはホスト名には 128 文字以下を指定してください。
KAOP70063-E	IP アドレスまたはホスト名に無効な文字が含まれています。 有効な文字: A ～ Z a ～ z 0-9 . -	**要因** IP アドレスまたはホスト名に無効な文字が含まれています。

メッセージ ID	メッセージテキスト	要因と対処
KAOP70063-E	IP アドレスまたはホスト名に無効な文字が含まれています。 有効な文字: Ａ ～ Ｚ ａ ～ ｚ 0-9 . -	有効な文字:A～Z a～z 0～9 . - **対処** 要因に応じて、問題を解決してください。
KAOP70064-E	アンインストールに必要なファイル *<インストーラファイル>* は読み取れません。 原因: -対象のファイルが不足しているか、実行権限がありません。 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。	**要因** アンインストールに必要なファイルは読み取れません。 原因: -対象のファイルが不足しているか、実行権限がありません。 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。 **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、障害対応窓口に連絡してください。
KAOP70065-E	_cs_.exe は直接実行できません。インストールはsetup.exe から実行してください。	**要因** _cs_.exe は直接実行することはできません。 **対処** インストールはsetup.exe から実行してください。
KAOP70066-E	デフォルトポート (443) またはユーザ指定ポートが接続待ち状態のため、代替推奨ポート (20950) を設定します。	**要因** 指定したポート番号の状態が「Listen」のため、状態が「開放」の推奨ポート番号(20950)を使用します。 **対処** -
KAOP70067-E	デフォルトポート (443) またはユーザ指定ポートが接続待ち状態のため、別のポート番号を指定してください。	**要因** 指定したポート番号と推奨ポート番号(20950)の状態が「Listen」で使用不可です。 **対処** 次のいずれかで問題を解決してください。 ・指定したポート番号の状態を「開放」にする ・推奨ポート番号(20950)の状態を「開放」にする ・状態が「開放」の別のポート番号を指定する
KAOP70070-E	システム環境変数 PATH に必要な値が設定されていないため、処理を続行できません。	**要因** cmd.exe を実行するための環境変数PATH の値が未設定です。 **対処** cmd.exe が存在するパスを環境変数PATH の値に設定してください。
KAOP70071-E	*<設定値が空欄の項目名>*を指定してください。	**要因** 対象の項目が未入力です。 **対処**

メッセージ ID	メッセージテキスト	要因と対処
KAOP70071-E	*<設定値が空欄の項目名>*を指定してください。	対象の項目は入力してください。
KAOP70080-E	セキュリティによって義務付けられたsysadminユーザーのパスワード変更またはパスワードポリシーの更新が失敗しました。Ops Center Portal GUI を使用して、sysadmin ユーザーのパスワードを手動で変更してください。Hitachi Ops Center Portal ヘルプの「パスワードポリシーを変更する」トピックを参照して、パスワードポリシーを手動で更新してください。	**要因** 新規インストールでcspasswd.exe が異常終了しました。 **対処** Hitachi Ops Center Portal でsysadmin ユーザーのパスワードを変更し、パスワードポリシーを見直してください。
KAOP70081-E	セキュリティによって義務付けられたsysadminユーザーのパスワード変更が失敗しました。Ops Center Portal GUI を使用して、sysadmin ユーザーのパスワードを手動で変更してください。	**要因** 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でcspasswd.exe が異常終了しました。 **対処** Hitachi Ops Center Portal でsysadmin ユーザーのパスワードを変更してください。

付録 A.5　LDAP サーバー登録時のパラメーターを決定する

LDAP サーバーと連携する場合、Common Services での LDAP サーバーの連携登録時に、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、ldp 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。ldp コマンドの詳細については、Windows のドキュメントを参照してください。

操作手順

1. 管理サーバーで、ldp コマンドを実行します。
   a. [スタート] − [Windows システム ツール] − [ファイル名を指定して実行] を選択します。
   b. [名前] にldp を入力し、[OK] をクリックします。
2. LDAP サーバーに接続します。[Connection] − [Connect] を選択し、次の項目を設定して [OK] をクリックします。

   [Server]
   LDAP サーバーのホスト名（FQDN）を指定します。

   [Port]
   LDAP サーバーのポート番号を指定します。
   LDAPS のデフォルトは 636 です。
   LDAPS のポート番号を指定した場合は、[SSL] のチェックボックスをオンにします。

3. LDAP 検索権限があるユーザーでバインドします。[Connection] − [Bind] を選択し、次の項目を設定して [OK] をクリックします。

[User]

バインド DN を指定します。

[Password]

バインド DN のパスワードを指定します。

[Bind type]

[Simple bind] を選択します。

4. LDAP サーバーを検索します。[Browse] − [Search] を選択し、次の項目を設定して [Run] をクリックします。

[Base DN]

検索対象のユーザーベース DN を指定します。

[Filter]

検索フィルターを指定します。

(例) フルネームがJohn Smith またはTom brady に一致するユーザーオブジェクトを検索する場合

```
(&(objectclass=person)(|(cn=John Smith)(cn=Tom brady)))
```

[Scope]

検索スコープを指定します。

ユーザーベース DN の 1 階層下のレベルだけを検索対象とする場合は [One Level] を選択、ユーザーベース DN とその配下のすべてのレベルを検索対象とする場合は [Subtree] を選択します。

[Attributes]

必要な属性を指定します。全属性を検索する場合は、アスタリスク (*) を指定します。

5. 表示された検索結果の内容を基に、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

Common Services での設定項目	設定する LDAP 属性
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。

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示します。

付録 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-616)

付録 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
Common Services	Hitachi Ops Center Common Services
Portal	Hitachi Ops Center Portal
PowerShell	Windows PowerShell
Viewpoint	Hitachi Ops Center Viewpoint
Viewpoint data center proxy	Hitachi Ops Center Viewpoint data center proxy

付録 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

略語	正式名称
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
I/O	Input/Output
ID	Identifier
IP	Internet Protocol
IPv4	Internet Protocol Version 4
JDK	Java Development Kit
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over Secure Sockets Layer
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
UDP	User Datagram Protocol
UPN	User Principal Name
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
UUID	Universally Unique Identifier

付録 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

よ

り

ろ

日立ヴァンタラ株式会社
〒 244-0817 神奈川県横浜市戸塚区吉田町 292 番地