**Sterling B2B Integrator**

# セキュリティー **(V5.2.3** 以降**)**

バージョン ***5.2.3***

**Sterling B2B Integrator**

# セキュリティー **(V5.2.3** 以降**)**

バージョン ***5.2.3***

注記

本書および本書で紹介する製品をご使用になる前に、 153 ページの『特記事項』に記載されている情報をお読みください。



お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： Sterling B2B Integrator
Security (V5.2.3 or later)
Version 5.2.3

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

# 目次

# セキュリティー (V5.2.3 以降)

Sterling B2B Integrator で使用されるさまざまなセキュリティー・メカニズムとしては、管理機能用のシステム・パスワード、自社のセキュリティー・ポリシーに基づいたパスワード・ポリシー、組織内のユーザーごとに異なるアクセス・レベルを提供するための役割ベースのセキュリティーなどが挙げられます。

Sterling B2B Integrator で提供されているセキュリティー機能は次のとおりです。

- 役割ベースのセキュリティーは、ユーザー・アカウントに関連付けられた許可に従って、ファイル、ビジネス・プロセス、Web テンプレート、サービス、および製品機能に対するアクセス権をユーザーに提供します。
- パスワード・ポリシーは一連のセキュリティー規則であり、管理者は自社のセキュリティー・ポリシーに従って、これらのセキュリティー規則を策定して、さまざまなユーザー・アカウントに適用します。これらの規則としては、パスワードの有効日数やパスワードの最大長と最小長などが挙げられます。
- LDAP 認証を使用すると、外部ユーザー・アカウントの認証を LDAP ディレクトリーに委任して、自社内の他のアプリケーション用に使用されているのと同じセキュリティー情報を使用して認証を実行できます。自社で LDAP を既に導入済みの場合は、既存の LDAP ディレクトリーを当アプリケーションで使用できます。
- インストール環境用のシステム・パスフレーズ - インストール時に、Sterling B2B Integrator のインストール環境用のシステム・パスフレーズを作成します。このパスフレーズは、17 文字以上で構成される非常に複雑なストリングです。このシステム・パスフレーズは、システムを始動するため、および保護されたシステム情報にアクセスするために必要です。
- 暗号化、署名、およびトランスポート層セキュリティー用の X.509 証明書のサポート
- 連邦情報処理標準 (FIPS) 140-2 で認定されたソフトウェア・モジュールと、FIPS 140-2 で認定された nCipher と Safenet のハードウェアのサポート
- Secure Socket Layering (SSL) と Transport Layer Security (TLS)

また、次のセキュリティー機能を構成できます。

- セキュリティー・タイムアウト機能を使用すると、ユーザー・セッションのタイムアウトを構成できます。
- カスタム・パスワード・ポリシー機能を使用すると、新たなパスワード・ポリシー・ルールを追加できます。これらの追加のパスワード・ルールは、安全性が低く破られやすいパスワードの使用を防止して、条件を満たしていないパスワードを拒否するのに役立ちます。
- シングル・サインオン (SSO) 機能は、ユーザーがユーザー名とパスワードを 1 回入力するだけで、複数のアプリケーションを利用できるようにする認証プロセスです。
- ドキュメント暗号化機能を使用すると、従来のファイルやデータベースに設定される許可に加えて、追加のセキュリティー層を構成できます。

# 役割ベースのセキュリティー

## 役割ベースのセキュリティーの概要

役割ベースのセキュリティーを使用すると、ユーザー・アカウントに関連付けられた許可に従って、特定のファイル、ビジネス・プロセス、Web テンプレート、サービス、および製品機能に対するアクセス権をユーザーに提供できます。

役割ベースのセキュリティーの管理方法を理解するには、グループ、許可、およびユーザー・アカウントがどのように連係して機能するのかを理解する必要があります。

- 許可は、ユーザー・インターフェースのページとそのページで提供されている機能へのアクセス権を提供します。
- グループは、許可の集合です。
- ユーザー・アカウントは、許可とパスワード・ポリシーに割り当てられます。

役割ベースのセキュリティーの管理に関する作業は次のとおりです。

- 許可の作成
- グループの作成
- パスワード・ポリシーの作成
- ユーザー・アカウントの作成

## グループ

グループは、許可の集合です。グループを使用すると、複数ユーザーのアクセス許可を 1 箇所で保持できます。グループは、特に複数のユーザーが同じ職務を実行する場合に、アカウント管理の作業量を最少化するのに役立ちます。

グループをユーザーごとではなく職務ごとに作成することで、多数の許可をさまざまなユーザーに割り当てることができます。グループをサブグループとして別のグループに割り当てることもできます。

例えば、調達部門には、すべて同じ職務を実行する 5 人の調達担当者がいるとします。個別の調達担当者のユーザー・アカウントに許可を割り当てる代わりに、調達グループを作成して、すべての調達担当者用のアクセス許可をその 1 つのグループ内で保持できます。この調達グループ内で複数のサブグループを割り当てることで、担当者が実行する調達のタイプに従って、アクセス許可を細分化できます。例えば、事務用品、機械、備品、または乗り物という名前のサブグループを調達グループに割り当てて、アクセス許可を細分化できます。

アップグレードやパッチの適用時に上書きを防ぐために、システムで事前に構成されているグループを変更しないでください。

グループを対象にした作業は次のとおりです。

- グループの作成
- グループの検索
- グループの編集
- グループの削除

## 構成済みグループ

ユーザーに許可を割り当てるために、構成済みのグループを割り当てることができます。ユーザーは、そのグループに関連付けられたすべての許可を継承します。構成済みグループをユーザーに割り当てることができるのは、そのユーザー・アカウントに対してアクセシビリティーとテーマが定義されている場合です。

グループを作成するには、「アカウント」モジュールに対する許可を持っている必要があります。

## グループの命名規則

グループの命名規則には一連の規則があります。

次のグループ命名規則に従ってください。

- グループ ID は固有である必要があります。
- 名前では大文字と小文字が区別されます。
- つづりが同じでも大文字/小文字の使われ方が異なる 2 つのグループ名は別々の名前として扱われます。
- 既に使用されているグループ名を新しいグループの名前として使用することはできません。使用しようとすると、エラー・メッセージが表示されます。

## グループの検索

「管理」メニューから、グループを検索できます。

### このタスクについて

グループを検索するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「グループ」を選択します。
2. 次のいずれかの操作を実行します。
    - 「検索」の「グループ名」フィールドに、検索するグループ名の一部または全体を入力して、「実行」をクリックします。「グループ」ページに、検索条件に一致するすべてのグループが一覧表示されます。
    - 「リスト」の「英数字別」フィールドで、「すべて」を選択するか、検索するグループ名の先頭文字を選択して、「実行」をクリックします。「グループ」ページに、検索条件に一致するすべてのグループが一覧表示されます。

## グループの作成

「管理」メニューから、グループを作成できます。

### このタスクについて

始める前に、以下のことを把握する必要があります。

- 作成するグループのグループ ID
- 作成するグループのグループ名
- このグループの所有者の名前

- このグループと関連付ける取引パートナーの ID。1 つのグループには 1 つの取引パートナーしか関連付けることはできませんが、1 つのユーザー・アカウントを複数のグループに関連付けることができます。これにより、ユーザー・アカウントを複数の取引パートナーに関連付けることができます。「ID」フィールドは、メールボックス内のメッセージのルーティングに使用されます。

グループを作成するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「グループ」を選択します。
2. 「新規グループの作成」の横にある「実行」をクリックします。
3. 「新規グループ」ページで、「グループ **ID**」を入力します。
4. 「グループ名」を入力します。
5. 「所有者」を入力します。
6. 「**ID**」を選択します。
7. 「次へ **(Next)**」をクリックします。
8. 「サブグループの割り当て」ページで、グループを名前に基づいてフィルタリングするには、「データのフィルタリング」の「名前別」フィールドに、フィルター表示するグループの名前の一部または全体を入力して、「フィルター」ボタンをクリックします。
9. このグループに割り当てるグループを選択します。それらのグループを「使用可能 (Available)」ペインから「割り当て済み」ペインに移動します。
10. 「次へ **(Next)**」をクリックします。
11. 「許可の割り当て」ページで、希望に応じて許可をフィルタリングします。
    - 名前に基づいてフィルタリングするには、「データのフィルタリング」の「名前別」フィールドに、フィルター表示する許可の名前の一部または全体を入力して、「タイプ別」フィールドの右側にある「フィルター」ボタンをクリックします。
    - タイプに基づいてフィルタリングするには、「データのフィルタリング」の「タイプ別」リストからフィルター表示する許可のタイプを選択して、「タイプ別」フィールドの右側にある「フィルター」ボタンをクリックします。
12. このグループに割り当てる許可を選択します。それらの許可を「使用可能 (Available)」ペインから「割り当て済み」ペインに移動します。 デフォルトでは、このグループに割り当てられたサブグループに関連付けられた許可があらかじめ選択されています。これらの関連付けられた許可は「使用可能 (Available)」列には表示されませんが、「確認」ページには表示されます。
13. 「次へ **(Next)**」をクリックします。
14. このグループの情報を確認します。
15. 「終了」をクリックします。

## グループの編集

設定、サブグループ、および許可を更新するためにグループを編集できます。

### このタスクについて

グループを編集する際は、以下を変更できます。

- 設定
- サブグループ
- 許可

グループ ID を変更することはできません。グループ ID を変更する必要がある場合は、新しいグループを作成する必要があります。

グループを編集するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「グループ」を選択します。
2. 「グループ名の検索 (Group Name Search)」または「アルファベット順にリスト (Alphabetically List)」を使用して編集するグループを検索して、「実行」をクリックします。
3. 更新するグループの「編集」をクリックします。
4. 任意のグループ設定を変更して、「次へ **(Next)**」をクリックします。
5. 任意の割り当て済みサブグループを変更して、「次へ **(Next)**」をクリックします。
6. 任意の割り当て済み許可を変更して、「次へ **(Next)**」をクリックします。
7. 「次へ **(Next)**」をクリックします。
8. このグループの情報を確認します。
9. 「終了」をクリックします。

## グループの削除

「管理」メニューから、グループを削除できます。

### このタスクについて

Sterling B2B Integrator の Admin グループおよび UI アカウントの許可を管理者ユーザーから削除することはできません。これらは、システム管理者がシステムを管理することを可能にします。

グループを削除するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「グループ」を選択します。
2. 「グループ」ページで、「検索」または「リスト」のオプションを使用して削除するグループを探します。
3. 「グループ」ページで、削除するグループの横にある「削除」をクリックします。

   そのグループが削除されて、次のメッセージが表示されます。

   ```
   The system update has completed successfully.
   ```

### グループの名前と ID の確認

グループ名と ID は、「管理」メニューから確認できます。

#### このタスクについて

グループの名前と ID を確認するには、以下を実行します。

#### 手順

1. 「管理メニュー」から、「アカウント」 > 「グループ」を選択します。
2. 「グループ」ページで、「検索」または「リスト」のオプションを使用して確認するグループを探します。
3. グループを選択します。 グループの名前と ID が表示されます。

## 許可

許可は、Sterling B2B Integrator 内のさまざまなモジュールへのアクセス権を提供することで、役割ベースのセキュリティーの基盤となっています。ユーザーの許可は、グループの許可と個別ユーザーに割り当てられた許可で構成されています。

許可を使用すると以下が可能になります。

- 複数のユーザーのアクセス権を 1 箇所から管理できます。
- ユーザー・アカウントを簡単に管理できます (特に同じ職務を実行する複数ユーザーの場合)。

許可に関する作業は次のとおりです。

- 許可の作成
- 許可の検索
- 許可名の編集
- 許可の削除

許可を作成、編集、または削除する前に、そのグループのユーザーが各自の職務を実行するためにアクセスする必要があるモジュールとアクセスする必要がないモジュールを特定してください。許可を作成するには、「アカウント」モジュールに対する許可が自身に割り当てられている必要があります。

アップグレードやパッチの適用時に上書きを防ぐために、システムであらかじめ用意されている許可を変更しないでください。カスタマイズされた許可グループが必要な場合は、新しいグループを作成してください。

### 許可の命名規則

許可の名前では大/小文字が区別され、重複は許可されません。

許可の命名規則は次のとおりです。

- 名前は大/小文字の区別があり、つづりが同じでも大文字/小文字の使われ方が異なる 2 つの許可名は別々の名前として扱われます。例えば、「Any document」と「Any Document」は 2 つの異なる許可名です。
- 既に使用されている許可名を新しい許可の名前として使用することはできません。使用しようとすると、エラー・メッセージが表示されます。

2 つの許可に大文字/小文字の使われ方が異なる同じ名前を付けることは可能ですが、推奨はされません。

## グループから継承される許可

ここでは、許可グループがユーザー・アカウントに割り当てられたときに継承される事前インストール済みのグループと許可を紹介します。グループがサブグループとして割り当てられた場合も、同じ許可が継承されます。

各グループには、メニュー項目に対する許可と、そのページへのアクセス権を付与するために使用される対応する UI 許可が含まれています。例えば、EBXML には UI EBXML が含まれています。

| グループ名 | グループ **ID** | グループから継承される許可 |
|---|---|---|
| アカウント | ACCOUNTS | PasswordPolicy、Permissions、UI Accounts、UserNews |
| ADAPTER_UTILITIES | ADAPTER_UTILITIES | BEATuxedo、CDNetmaps、CDNetmapXref、CDNodes、SAPRoutes、SAPRouteXREF、SAPSuiteBuilder、UI Adapter Utilities |
| ADVANCED_SETUP | ADVANCED_SETUP | DeliveryChannels、DocumentExchange、Identities、Packaging、Profiles、 Transports、UI Advanced Trading Profile Setup |
| AS2 エディション | as2admin | 「BPMONITOR」サブグループのすべての許可と、AS2 UI、TestNow、UI AS2 Trading Profile Setup、UI BP Manager、UI Ca Certs、UI Delete Trading Partner Data、UI Logs、UI Scheduler、UI System Certs、UI trading Parners |
| 異常イベント通知 | eventAbnormal | なし |
| アカウント | acctadmin | 「アカウント」サブグループのすべての許可と、UI Groups、UI User Accounts |
| アラート通知 | notifications | なし |
| BPMONITOR | BPMONITOR | BPSSCorrelation、BusinessProcesses、 CentralSearch、CommunicationSessions、 Correlation、CurrentActivities、CurrentDocuments、CurrentProcesses、DataFlows、Documents、EBXMLCorrelation、EDICorrelation、EDIINT、GentranServerforUnix、 Message Entry Workstation Home、 SWIFTNETCorrelation、UI BP Monitor、 RosettaNet |
| ビジネス・プロセス | bpadmin | 「BPMONITOR」サブグループと「サービス」サブグループのすべての許可と、UI BP Manager、UI Business Process、UI Delete BP |
| CD サーバー・プロキシー管理者 | cdsp_admin | 「アカウント」、「BPMONITOR」、「CD サーバー・プロキシー・ユーザー」、「操作」、および「サービス」というサブグループのすべての許可と、UI Groups、UI Licenses、UI Password Policy、UI SQL Tool、UI User Accounts |

| グループ名 | グループ **ID** | グループから継承される許可 |
| --- | --- | --- |
| CD サーバー・プロキシー・ユーザー | cdsp_user | このグループは、CDSP アクセシビリティーを使用してユーザー・アカウントが作成されたときにデフォルトで割り当てられます。<br><br>「アカウント」、「BPMONITOR」、「操作」、および「サービス」というサブグループのすべての許可と、CDSP Services、UI CA Certs、UI Import/Export、UI Lock Manager、UI Logs、UI Perimeter Servers、UI Reports、UI Support Case Tool、UI System Certs、UI Trusted Certs |
| コマンド・ライン・ユーザー | commandlineuser | eInvoicing、eInvoicing ALL BUYERS、eInvoicing ALL SUPPLIERS、eInvoicing Archive、eInvoicing Configuration、eInvoicing CREATE/EDIT AGREEMENT、eInvoicing DELETE AGREEMENT、VIEW AGREEMENT |
| 展開 | DEPLOYMENT | UI Deployment、Resource Tags |
| ダッシュボード・ユーザー | dashboardUsers | このグループは、以下のいずれかのダッシュボード・テーマと「ダッシュボード UI」アクセシビリティーを使用してユーザー・アカウントが作成されたときにデフォルトで割り当てられます。<br>• AFT<br>• デフォルト<br>• コミュニティー管理オペレーター、参加者、参加者スポンサー、またはスポンサー<br><br>Administration Management Console、Business Process Search Portlet、Cache Statistics Portlet、Cache Usage Portlet、Community Management Portlet、Community Statistics Portlet、Database Pool Usage Portlet、Database Status Portlet、Database Usage Portlet、Document Search Portlet、Document Tracking Portlet、Documents Processed Bar Chart Portlet、Documents Processed Time Series Portlet、Event Viewer Portlet、IFrame Portlet、Log File Viewer Portlet、Log File Viewer Portlet 2、ParticipatingCommunities Portlet、Peers Portlet、Queue Priority Statistics Portlet、Quick Links Portlet、RSS Feed Portlet、Sponsored Communities Portlet、System Alerts Portlet、Web Search Portlet、Web View Plus Portlet |
| 展開 | deploymentadmin | 「ADAPTER_UTILITIES」、「展開」、「EBXML」、「メールボックス」、「マップ」、「サービス」、「WEB_EXTENSIONS」、および「WEB_SERVICES」というサブグループのすべての許可と、UI Connect:Direct、UI Delete CPA と CPSS Schema/Extension、UI Delete Map、UI Delete PGP Profile、UI Delete SAP Routes、UI Delete Schema、UI Delete Service Instance、UI Delete SWIFTNet Routing Rule、UI Delete Web Resource、UI Delete Web Templates、UI Delete WSDL、UI Delete XSLT Template、UI Generate/Download WAR Files、UI Import/Export、UI Scheduler、UI Schemas、UI SSH Local Identity Key、UI SWIFTNet Routing Rule、UI XSLT |

| グループ名 | グループ **ID** | グループから継承される許可 |
| --- | --- | --- |
| EBICS 管理者 (EBICS Administrators) | EBICS_ADM | UI EBICS Bank Profile Configuration、UI EBICS Contract Configuration、UI EBICS File Format Configuration、UI EBICS Offer Configuration、UI EBICS Order Type Configuration、UI EBICS Partner Profile Configuration、 UI EBICS User Permission Configuration、UI EBICS User Profile Configuration、UI EBICS Bank Profile Configuration、UI EBICS Contract Configuration、UI EBICS Subscriber Key Validation |
| EBICS オペレーター (EBICS Operators) | EBICS_OPERATOR | UI EBICS Bank Profile Configuration、UI EBICS Contract Configuration、UI EBICS File Format Configuration、UI EBICS Offer Configuration、UI EBICS Order Type Configuration、UI EBICS Partner Profile Configuration、UI EBICS Subscriber Key Validation、UI EBICS User Permission Configuration、UI EBICS User Profile Configuration |
| EBXML | EBXML | BPSS、BPSSExtension、CPA、UI EBXML |
| エンベロープ | ENVELOPES | ControlNumberHistory、ControlNumbers、EDISequenceCheckQueue、Envelopes、TransactionRegister、UI Envelopes |
| 例外イベント通知 | eventExceptional | なし |
| メールボックス | MAILBOX | Configuration、Messages、Routing Rules、UI Mailbox、VirtualRoots |
| マップ | MAPS | ExtendedRuleLibraries、Maps、Standards、UI Maps |
| メールボックス管理者 | mboxadmins | 「メールボックス」グループと「メールボックス・ブラウザー・インターフェース・ユーザー」グループのすべての許可と、DeadLetter Mailbox、Mailbox Global Delete、Mailbox Global Query、EBICS_DEADLETTER Mailbox |
| メールボックス・ブラウザー・インターフェース・ユーザー | mbiusers | Mailbox Add Business Process、Mailbox Extract Business Process、Mailbox Path List Process、Mailbox Query Business Process、Mailbox Search Business Process、Mailbox Self Registration Business Process、Mailbox View Business Process、MBISearch JSP |
| 操作 | OPERATIONS | JDBCMonitor、MessageMonitor、Perfdumps、SequenceManager、Statistics、ThreadMonitor、Troubleshooter、 Tuning、UI Federated Systems、 UI Operations |
| 暫定取引パートナー | provisionalpartners | なし |
| サービス | SERVICES | Configuration、Installation/Setup、UI Services |
| SSH | SSH | AuthorizedUserKey、KnownHostKey、 RemoteProfiles、UI SSH、UserIdentityKey |

| グループ名 | グループ **ID** | グループから継承される許可 |
| --- | --- | --- |
| セッション・デモ Web スイート・バイヤー | sd_buyer | WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Invoice Template、WebSuite Invoice View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite PO Ack Template、WebSuite PO Ack View Template、WebSuite Query Business Process、WebSuite RA Send Business Process、WebSuite Self Registration Business Process、WebSuite Session Demo Confirm Send Template、WebSuite Session Demo PO Send Business Process、WebSuite Session Demo PO Template、WebSuite Session Demo PO View Template、WebSuite Session Demo Query List Template |
| セッション・デモ Web スイート・サプライヤー | sd_supplier | WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Invoice Template、WebSuite Invoice View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite PO Ack Template、WebSuite PO Ack View Template、WebSuite PO to Advance Ship Notice Template、WebSuite PO to Invoice Template、WebSuite PO Turn Business Process、WebSuite Query Business Process、WebSuite RA Send Business Process、WebSuite Self Registration Business Process、WebSuite Session Demo Confirm Send Template、WebSuite Session Demo PO Send Business Process、WebSuite Session Demo PO View Template、WebSuite Session Demo Query List Template |

| グループ名 | グループ **ID** | グループから継承される許可 |
| --- | --- | --- |
| Sterling B2B Integrator Admin | super | 「アカウント」、「ADAPTER_UTILITIES」、「ADVANCED_SETUP」、「BPMONITOR」、「展開」、「EBXML」、「エンベロープ」、「メールボックス」、「マップ」、「メールボックス管理者」、「操作」、「サービス」、「SSH」、「WEB_EXTENSIONS」、および「WEB_SERVICES」というサブグループのすべての許可と、UI Archive、UI AS2 Trading Profile Setup、UI Basic Trading Profile Setup、UI BP Manager、UI Business Process、UI CA Certs、UI CodeLists、UI Connect:Direct、UI Contracts、UI Delete BP、UI Delete CPA と CPSS Schema/Extension、UI Delete Map、UI Delete PGP Profile、UI Delete SAP Routes、UI Delete Schema 、UI Delete Service Instance、UI Delete SWIFTNet Routing Rule、UI Delete Trading Partner Data、UI Delete Web Resource、UI Delete Web Templates、UI Delete WSDL、UI Delete XSLT Template、UI Federated、UI Generate/Download WAR Files、UI Groups、UI Import/Export、UI Licenses、UI Lock Manager、UI Logs、UI Notify、UI Perimeter Servers、UI PGP Profile Manager、UI Reports、UI Scheduler、UI Schemas、UI SQL Tool、UI SSH Local Identity Key、UI Support Case Tool、UI SWIFTNet Routing Rule、UI System Certs、UI Trading Partners、UI Trusted Certs、UI User Accounts、UI XSLT |
| システム操作 | operator | 「操作」サブグループのすべての許可と、UI Archive、UI Licenses、UI Lock Manager、UI Logs、UI Notify、UI Perimeter Servers、UI Reports、UI Scheduler、UI SQL Tool、UI Support Case Tool |
| 取引プロファイル | tpadmin | 「ADVANCED_SETUP」、「エンベロープ」、および「SSH」というサブグループのすべての許可と、UI AS2 Trading Profile Setup、UI Basic Trading Profile Setup、UI CA Certs、UI CodeLists、UI Contracts、UI Delete Trading Partner Data、UI System Certs、UI Trading Partners、UI Trusted Certs |
| WEB_EXTENSIONS | WEB_EXTENSIONS | Utilities、WebResources、WebTemplates |
| WEB_SERVICES | WEB_SERVICES | SchemaMappings、SecurityToken、UI Web Services、WebServicesManager、WSDLCheckin |

| グループ名 | グループ **ID** | グループから継承される許可 |
| --- | --- | --- |
| Web スイート・バイヤー | wsbuyers | WebSuite ASN View Template、WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Invoice View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite PO Ack View Template、WebSuite PO Send Business Process、WebSuite PO Template、WebSuite PO View Template、WebSuite Query Business Process、WebSuite Query List Template、WebSuite RA Send Business Process、WebSuite Remittance Advice Template、WebSuite Remittance Advice View Template、WebSuite Self Registration Business Process |
| Web スイート従業員 | wsemployees | WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite ER Send Business Process、WebSuite Expense Report Template、WebSuite Expense Report View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite Purchase Req Send Business Process、WebSuite Purchase Req Template、Websuite Purchase Req View Template、WebSuite Query Business Process、WebSuite Query List Template、WebSuite Self Registration Business Process、WebSuite TimeSheet Template、WebSuite TimeSheet View Template、WebSuite TS Send Business Process |
| Web スイート財務 | wsfinance | WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Expense Report View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite Query Business Process、WebSuite Query List Template、WebSuite Self Registration Business Process |
| Web スイート人事 | wshr | WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite Query Business Process、WebSuite Query List Template、WebSuite Self Registration Business Process、WebSuite TimeSheet View Template |

| グループ名 | グループ **ID** | グループから継承される許可 |
| --- | --- | --- |
| Web スイート・マネージャー | wsmanagers | WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite ER Send Business Process、WebSuite Expense Report View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite Purchase Req Send Business Process、WebSuite Purchase Req View Template、WebSuite Query Business Process、WebSuite Query List Template、WebSuite Self Registration Business Process、WebSuite TimeSheet View Template、WebSuite TS Send Business Process |
| Web スイート購入者 | wspurchaser | WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite Purchase Req View Template、WebSuite Query Business Process、WebSuite Query List Template、WebSuite Self Registration Business Process |
| Web スイート・サプライヤー | wssupplier | WebSuite ASN Send Business Process、WebSuite ASN Template、WebSuite ASN View Template、WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Invoice Send Business Process、WebSuite Invoice Template、WebSuite Invoice View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite PO Ack Send Business Process、WebSuite PO Ack Template、WebSuite PO Ack View Template、WebSuite PO to Advance Ship Notice Template、WebSuite PO to Invoice Template、WebSuite PO to PO Ack Template、WebSuite PO Turn Business Process、WebSuite PO View Template、WebSuite Query Business Process、WebSuite Query List Template、WebSuite Remittance Advice View Template、WebSuite Self Registration Business Process |

## UI リソースにアクセスするために必要な許可

ここでは、メニュー項目およびそれに関連するページと機能にアクセスするために必要な最低限の許可のセットを紹介します。最低限の許可のセットを割り当てると、そのユーザーが追加の機能も使用可能になる場合があります。いずれかのメニュー項目とそれに関連する機能に対する許可を持っていない場合は、そのメニュー項目は表示されません。

| 「管理メニュー」**>**「ビジネス・プロセス」から、**UI** リソース | 許可名 **/** 許可 **ID** |
|---|---|
| 「ビジネス・プロセス」>「マネージャー」 | UI BP Manager (BPMANAGE)、UI Business Process (BUSINESS_PROCESS) |
| 「ビジネス・プロセス」>「モニター」>「拡張検索」>「ビジネス・プロセス」 | BusinessProcesses (PLTADM2)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「拡張検索」>「SWIFTNet 相関」 | SWIFTNETCorrelation (GISADM9)、UI BP Monitor (BPMONITOR)、UI SWIFTNet Routing Rule (SWIFTNET_ROUTING_RULE) |
| 「ビジネス・プロセス」>「モニター」>「拡張検索」>「データ・フロー」 | DataFlows (GISADM1)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「拡張検索」>「ドキュメント」 | Documents (GISADM2)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「拡張検索」>「通信セッション」 | Communication Sessions (GISADM3)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「拡張検索」>「相関」 | Correlation (GISADM4)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「拡張検索」>「BPSS 相関」 | BPSSCorrelations (GISADM5)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「拡張検索」>「EBXML 相関」 | EBXMLCorrelation (GISADM6)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「拡張検索」>「EDI 相関」 | EDICorrelation (GISADM7)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「拡張検索」>「EDIINT」 | EDIINT (STDSADM6)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「集中検索」 | CentralSearch (GISADM10)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「現行プロセス」 | CurrentProcesses (PLTADM3)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「現行ドキュメント」 | CurrentDocuments (GISADM11)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「モニター」>「現行アクティビティー」 | CurrentActivities (PLTADM4)、UI BP Monitor (BPMONITOR) |
| 「ビジネス・プロセス」>「メッセージ入力ワークステーション」 | Message Entry Workstation Home (MESSAGE_ENTRY_HOME) |

| 「管理メニュー」**>**「取引パートナー」から、**UI** リソース | 許可名 **/** 許可 **ID** |
|---|---|
| 「取引パートナー」>「設定」>「基本」 | UI Basic Trading Profile Setup (BASIC_SETUP) |

| 「管理メニュー」>「取引パートナー」から、**UI** リソース | 許可名 / 許可 **ID** |
| --- | --- |
| 「取引パートナー」>「設定」>「拡張」>「ID」 | Identities (GISADM12)、UI Advanced Trading Profile Setup (ADVANCED_SETUP)<br><br>削除を行うには、UI Delete Trading Partner 許可 (TP_DELETE) も必要です。 |
| 「取引パートナー」>「設定」>「拡張」>「トランスポート」 | Transports (GISADM13)、UI Advanced Trading Profile Setup (ADVANCED_SETUP)<br><br>削除を行うには、UI Delete Trading Partner 許可 (TP_DELETE) も必要です。 |
| 「取引パートナー」>「設定」>「拡張」>「ドキュメント交換」 | DocumentExchange (GISADM14)、UI Advanced Trading Profile Setup (ADVANCED_SETUP)<br><br>削除を行うには、UI Delete Trading Partner 許可 (TP_DELETE) も必要です。 |
| 「取引パートナー」>「設定」>「拡張」>「デリバリー・チャネル」 | DeliveryChannels (GISADM15)、UI Advanced Trading Profile Setup (ADVANCED_SETUP)<br><br>削除を行うには、UI Delete Trading Partner 許可 (TP_DELETE) も必要です。 |
| 「取引パートナー」>「設定」>「拡張」>「パッケージ」 | Packaging (GISADM16)、UI Advanced Trading Profile Setup (ADVANCED_SETUP)<br><br>削除を行うには、UI Delete Trading Partner 許可 (TP_DELETE) も必要です。 |
| 「取引パートナー」>「設定」>「拡張」>「プロファイル」 | Profiles (GISADM17)、UI Advanced Trading Profile Setup (ADVANCED_SETUP)<br><br>削除を行うには、UI Delete Trading Partner 許可 (TP_DELETE) も必要です。 |
| 「取引パートナー」>「デジタル証明書」>「CA」 | UI CA Certs (CA_CERTS)、UI System Certs (SYSTEM_CERTS) UI<br><br>System Certs によって「システム」オプションが追加されます。 |
| 「取引パートナー」>「デジタル証明書」>「トラステッド」 | UI Trusted Certs (TRUSTED_CERTS) |
| 「取引パートナー」>「デジタル証明書」>「システム」 | UI System Certs (SYSTEM_CERTS) |
| 「取引パートナー」>「ドキュメント・エンベロープ」>「エンベロープ」 | Envelopes (STDSADM1)、UI Envelope (ENVELOPE) |

| 「管理メニュー」**>**「取引パートナー」から、**UI** リソース | 許可名 **/** 許可 **ID** |
| --- | --- |
| 「取引パートナー」>「ドキュメント・エンベロープ」>「コントロール番号」 | ControlNumbers (STDSADM2)、UI Envelope (ENVELOPE) |
| 「取引パートナー」>「ドキュメント・エンベロープ」>「トランザクション登録」 | TransactionRegister (STDSADM3)、UI Envelope (ENVELOPE) |
| 「取引パートナー」>「ドキュメント・エンベロープ」>「コントロール番号履歴」 | ControlNumberHistory (STDSADM4)、UI Envelope (ENVELOPE) |
| 「取引パートナー」>「ドキュメント・エンベロープ」>「EDI シーケンス検査キュー」 | EDISequenceCheckQueue (STDSADM5)、UI Envelope (ENVELOPE) |
| 「取引パートナー」>「契約」 | UI Contracts (CONTRACTS)、UI Advanced Trading Partner Setup (ADVANCED_SETUP) |
| 「取引パートナー」>「コード・リスト」 | UI CodeLists (CODELISTS) |
| 「取引パートナー」>「AS2」 | UI AS2 Trading Profile Setup<br><br>(AS2_SETUP) |
| 「取引パートナー」>「SSH」>「リモート・プロファイル」 | RemoteProfiles (ASSETADM1)、UI SSH |
| 「取引パートナー」>「SSH」>「既知ホスト・キー」 | KnownHostKey (ASSETADM2)、UI SSH |
| 「取引パートナー」>「SSH」>「ユーザー ID キー」 | UserIdentityKey<br><br>(ASSETADM3)、UI SSH |
| 「取引パートナー」>「SSH」>「許可ユーザー・キー」 | AuthorizedUserKey<br><br>(ASSETADM4)、UI SSH |
| 「取引パートナー」>「AS3」 | UI AS3 Trading Profile Setup<br><br>(AS3_SETUP) |
| 「取引パートナー」>「Odette FTP パートナー・プロファイル」>「物理パートナー」 | OftpPhysicalPartner (ASSETOFTP1)、UI Adapter Utilities (ADAPTER_UTILITIES) |
| 「取引パートナー」>「Odette FTP パートナー・プロファイル」>「物理パートナー契約」 | OftpPhysicalPartnerContract (ASSETOFTP3)、UI Adapter Utilities (ADAPTER_UTILITIES) |
| 「取引パートナー」>「Odette FTP パートナー・プロファイル」>「論理パートナー」 | OftpLogicalPartner (ASSETOFTP2)、UI Adapter Utilities (ADAPTER_UTILITIES) |
| 「取引パートナー」>「Odette FTP パートナー・プロファイル」>「論理パートナー契約 (Logical Partner Contract)」 | OftpLogicalPartnerContract (ASSETOFTP4) |
| 「取引パートナー」>「PGP」>「サーバー・マネージャー (Server Manager)」 | PGP Server Manager (ASSETADM55)、UI PGP Profile Manager (PGP) |
| 「取引パートナー」>「PGP」>「スポンサー・マネージャー (Sponsor Manager)」 | PGP Sponsor Manager (ASSETADM56)、UI PGP Profile Manager (PGP) |
| 「取引パートナー」>「PGP」>「パートナー・マネージャー (Partner Manager)」 | PGP Partner Manager (ASSETADM57)、UI PGP Profile Manager (PGP) |

| 「管理メニュー」>「展開」から、**UI** リソース | 許可名 / 許可 **ID** |
| --- | --- |
| 「展開」>「サービス」>「インストール/設定」 | Installation/Setup (PLTADM9)、UI Services (SERVICES) |
| 「展開」>「サービス」>「構成」 | Configuration (PLTADM10)、UI Services (SERVICES)、UI BP Manager (BPMANAGE)。V5.2.4.3 以上では、 UI Adapters StartStop も必要です。 |
| 「展開」>「スケジュール」 | UI Scheduler (SCHEDULER) |
| 「展開」>「マップ」 | Maps (ASSETADM5)、UI_Maps |
| 「展開」>「標準」 | Standards (STDSADM7)、UI_Maps |
| 「展開」>「拡張ルール・ライブラリー」 | ExtendedRuleLibraries (ASSETADM6)、UI_Maps |
| 「展開」>「XSLT」 | UI XSLT (XSLT) |
| 「展開」>「Web 拡張」>「Web リソース」 | WebResources (GISADM19)、UI Web Extensions、UI Web Services (WEB_SERVICES)<br><br>UI Web Services は、ユーザーが新しい Web リソース・ファイルをチェックインすることを許可します。 |
| 「展開」>「Web 拡張」>「ユーティリティー」 | Utilities (GISADM20)、UI Web Extensions.<br><br>旧バージョンからのアップグレードの場合にのみ表示されます。 |
| 「展開」>「スキーマ」 | UI Schemas (SCHEMAS) |
| 「展開」>「メールボックス」>「構成」 | Configuration (MBXADM1)、UI Mailbox (MAILBOX) |
| 「展開」>「メールボックス」>「仮想ルート」 | VirtualRoots (MBXADM2)、UI Mailbox (MAILBOX) |
| 「展開」>「メールボックス」>「ルーティング・ルール」 | RoutingRules (MBXADM3)、UI Mailbox (MAILBOX) |
| 「展開」>「メールボックス」>「メッセージ」 | Messages (MBXADM4)、UI Mailbox (MAILBOX) |
| 「展開」>「EBXML」>「BPSS」 | BPSS (ASSETADM7)、UI EBXML (EBXML) |
| 「展開」>「EBXML」>「BPSS 拡張機能」 | BPSSExtension (ASSETADM8)、UI EBXML (EBXML) |
| 「展開」>「EBXML」>「CPA」 | CPA (ASSETADM9)、UI EBXM (EBXML) |
| 「展開」>「リソース・マネージャー」>「リソース・タグ」 | Resource Tags (PLTADM1)、UI Deployment (DEPLOYMENT) |
| 「展開」>「リソース・マネージャー」>「インポート/エクスポート」 | UI Import/Export (IMPORT_EXPORT) |
| 「展開」>「アダプター・ユーティリティー」>「SAP スイート・ビルダー」 | SAPSuiteBuilder (ASSETADM10)、UI Adapter Utilities |
| 「展開」>「アダプター・ユーティリティー」>「SAP ルート」>「SAP ルート」 | SAPRoutes (ASSETADM11)、UI Adapter Utilities |

| 「管理メニュー」>「展開」から、**UI** リソース | 許可名 / 許可 **ID** |
| --- | --- |
| 「展開」>「アダプター・ユーティリティー」>「SAP ルート」>「SapRouteXRef (SapRouteXRef)」 | SAPRouteXREF (ASSETADM12)、UI Adapter Utilities |
| 「展開」>「アダプター・ユーティリティー」>「BEATuxedo (BEATuxedo)」 | BEATuxedo (ASSETADM13)、UI Adapter Utilities<br><br>BEATuxedo jar がインストールされていない場合は、メニュー項目は表示されません。 |
| 「展開」>「アダプター・ユーティリティー」>「SWIFTNet ルーティング・ルール」 | UI SWIFTNet Routing Rule (SWIFTNET_ROUTING_RULE) |
| 「展開」>「アダプター・ユーティリティー」>「SWIFTNet サービス・プロファイル」 | UI SWIFTNet Service Profile (SWIFTNET_SVC_PROFILE) |
| 「展開」>「アダプター・ユーティリティー」>「SWIFTNet コピー・サービス・プロファイル」 | UI SWIFTNet Copy Profile (SWIFTNET_COPY_PROFILE) |
| 「展開」>「アダプター・ユーティリティー」>「ロックアウト・ポリシー・マネージャー (Lockout Policy Manager)」 | LockoutPolicyManager (ASSETADM50) |
| 「展開」>「アダプター・ユーティリティー」>「C:D ネットマップ (C:D Netmaps)」>「C:D ノード (C:D Node)」 | CDNetmaps (ASSETADM51)、UI Adapter Utilities (ADAPTER_UTILITIES) |
| 「展開」>「アダプター・ユーティリティー」>「C:D ネットマップ (C:D Netmaps)」>「C:D ネットマップ (C:D Netmaps)」 | CDNodes (ASSETADM52)、UI Adapter Utilities (ADAPTER_UTILITIES) |
| 「展開」>「アダプター・ユーティリティー」>「C:D ネットマップ (C:D Netmaps)」>「C:D ネットマップ X-REF (C:D Netmap X-REF)」 | CDNetmapXref (ASSETADM53)、UI Adapter Utilities (ADAPTER_UTILITIES) |
| 「展開」>「アダプター・ユーティリティー」>「ポリシー構成」 | Adapter Policies (ASSETADM54) |
| 「展開」>「アダプター・ユーティリティー」>「ファイル・システムの仮想ルート (File System Virtual Root)」 | File System Virtual Root (ASSETADM58) |
| 「展開」>「SSH ホスト ID キー」 | UI SSH Local Identity Key (SSH_LCL_ID_KEY)、UI SSH (SSH) |
| 「展開」>「Web サービス」>「マネージャー」 | WebServicesManager (ASSETADM16)、UI Web Services (WEB_SERVICES) |
| 「展開」>「Web サービス」>「スキーマ・マッピング」 | SchemaMappings (ASSETADM17)、UI Web Services (WEB_SERVICES)、UI EBXML (EBXML) |
| 「展開」>「Web サービス」>「WSDL チェックイン」 | WSDLCheckIn (ASSETADM18)、UI Web Services (WEB_SERVICES) |
| 「展開」>「Web サービス」>「セキュリティー・トークン」 | SecurityToken (ASSETADM18)、UI Web Services (WEB_SERVICES) |

| 「管理メニュー」>「電子インボイス」から、**UI** リソース | 許可名 / 許可 **ID** |
| --- | --- |
| 「電子インボイス」>「契約」 | eInvoicing VIEW AGREEMENT (EINV_VIEW_AGREEMENT)<br><br>削除を行うには、eInvoicing DELETE AGREEMENT (EINV_DELETE_AGREEMENT) という許可も必要です。 |
| 「電子インボイス」>「統合アーカイブ」 | eInvoicing Archive (EINVOICING_ARCHIVE)、eInvoicing VIEW INVOICE (EINV_VIEW_INVOICE) |
| 「電子インボイス」>「構成」 | eInvoicing Configuration (EINVOICING_CONFIGURATION) |

| 「管理メニュー」>「操作」から、**UI** リソース | 許可名 / 許可 **ID** |
| --- | --- |
| 「システム」>「トラブルシューター」 | Troubleshooter (PLTADM17)、UI Operations (OPERATIONS) |
| 「システム」>「パフォーマンス」>「調整」 | Tuning (PLTADM18)、UI Operations (OPERATIONS) |
| 「システム」>「パフォーマンス」>「統計」 | Statistics (PLTADM19)、UI Operations (OPERATIONS) |
| 「システム」>「パフォーマンス」>「JVM モニター」 | Perfdumps (GISADMIN27)、UI Operations (OPERATIONS) |
| 「システム」>「サポート・ツール」>「SQL マネージャー」 | UI SQL Tool (SQLMANAGER) |
| 「システム」>「サポート・ツール」>「サポート・ケース」 | UI Support Case Tool (SUPPORT_CASE) |
| 「システム」>「ログ」 | UI Logs (SYSTEM_LOGS) |
| 「システム」>「ライセンス」 | UI Licenses (LICENSES) |
| レポート | UI Reports (REPORTS) |
| 「スレッド・モニター」 | ThreadMonitor (PLTADM24)、UI Operations (OPERATIONS) |
| 「JDBC モニター」 | JDBCMonitor (PLTADM25)、UI Operations (OPERATIONS)、UI SQL Tool (SQLMANAGER) |
| 「アーカイブ・マネージャー」 | UI Archive (ARCHIVE-UI)、UI Operations (OPERATIONS)、UI BP Manage (BPMANAGE)、UI Business Process (BUSINESS_PROCESS) |
| 「ロック・マネージャー」 | UI Lock Manager (LOCK_MANAGER) |
| 「メッセージ・モニター」 | MessageMonitor (GISADM24)、UI Operations (OPERATIONS) |
| 周辺サービス | UI Perimeter Servers (PSERVERS) |

| 「管理メニュー」>「操作」から、**UI** リソース | 許可名 / 許可 **ID** |
|---|---|
| 「プロキシー・サーバー」 | UI Proxy Servers (PROXYSERVERS)、Sterling B2B Integrator Admin グループ |

| 「管理メニュー」>「アカウント」から、**UI** リソース | 許可名 / 許可 **ID** |
|---|---|
| 「グループ」 | UI Groups (GROUPS)、UI Accounts (ACCOUNTS) |
| 許可 | Permissions (PLTADM27)、UI Accounts (ACCOUNTS) |
| 「ユーザー・アカウント」 | UI User Accounts (USER_ACCOUNTS)、UI Accounts (ACCOUNTS) |
| 「パスワード・ポリシー」 | PasswordPolicy (PLTADM29)、UI Accounts (ACCOUNTS) |
| 「ユーザー・ニュース」 | UserNews (GISADM25)、UI Accounts (ACCOUNTS) |
| 「マイ・アカウント」 | MyAccount (PLTADM30) |

## 構成済み許可

構成済み許可は、システム側で用意されています。カスタム許可と同様に、構成済み許可はシステム内のさまざまなモジュールに対するアクセス権を提供します。

## 許可名の検索

「管理」メニューから、許可を検索できます。

### このタスクについて

許可を検索するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「許可」を選択します。
2. 「許可」ページで、次のいずれかの操作を実行します。
   - 「検索」の「許可名」フィールドに、検索する許可名の一部または全体を入力して、「実行」をクリックします。「許可」ページに、検索条件に一致するすべての許可が一覧表示されます。
   - 「リスト」の「英数字別」フィールドで、「すべて」を選択するか、検索する許可名の先頭文字を選択して、「実行」をクリックします。「許可」ページに、検索条件に一致するすべての許可が一覧表示されます。

## 許可の作成

旧バージョンのシステムからアップグレードした場合は、既存の許可はデフォルトでは「その他 (Other)」に設定されています。必要に応じて、それぞれの許可を編集して新しい許可タイプを適用してください。

## このタスクについて

開始前に、次の情報を把握する必要があります。

| フィールド | 説明 |
| --- | --- |
| 許可 ID | 作成する許可の許可 ID。許可 ID は、その許可を設定する対象となるビジネス・プロセス、XSLT ドキュメント、Web テンプレート、またはリソースの名前です。 ID の後ろにそのリソースの拡張子を追加します。必須。<br><br>許可 ID の条件:<br>• 一意である必要があります。<br>• 大文字と小文字が区別されます。<br>• 対象のビジネス・プロセス、XSLT ドキュメント、Web テンプレート、またはリソースの名前と一致する必要があります。許可 ID と対象リソースの名前が完全には一致しない場合は、そのリソースをロックダウンできません。 |
| 許可名 | 作成する許可の名前。必須。<br><br>許可名は固有であることが必要です。許可名は大/小文字の区別があります。例えば、「Any document」と 「Any Document」は 2 つの異なる許可名です。 |
| 許可タイプ | 作成する許可の許可タイプ。必須。許可タイプには以下があります。<br>• UI –インターフェース内の特定のメニュー項目へのアクセスを許可します。<br>• メールボックス - システム内の特定のメールボックスへのアクセスを許可します。<br>• テンプレート - 特定の Web テンプレートへのアクセスを許可します。<br>• BP - 特定のビジネス・プロセスへのアクセスを許可します。<br>• 追跡 - 特定のドキュメント追跡オプションへのアクセスを許可します。<br>• コミュニティー - 特定のコミュニティー管理オプションへのアクセスを許可します。<br>• Web サービス<br>• サービス<br>• 電子インボイス<br>• その他 (Other) – 上記のどのタイプにも該当しないリソースへのアクセスを許可します。 |

許可を作成するには、以下を実行します。

## 手順

1. 「管理メニュー」から、「アカウント」 > 「許可」を選択します。
2. 「新規許可の作成」の横にある「実行」をクリックします。
3. 「許可」ページで、「許可 **ID**」を入力します。

4. 「許可名」を入力します。
5. 「許可タイプ」を選択します。
6. 「次へ **(Next)**」をクリックします。
7. この許可の設定内容を確認します。
8. 「終了」をクリックします。

## 許可名の編集

許可の内容に応じて許可名を変更する必要がある場合は、許可名を編集します。許可名は固有であることが必要で、大文字と小文字が区別されます。許可 ID を変更することはできません。許可 ID を変更する必要がある場合は、新しい許可を作成する必要があります。

### このタスクについて

許可名を編集するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「許可」を選択します。
2. 「許可名の検索 (Permission Name Search)」または「アルファベット順にリスト (Alphabetically List)」を使用して編集する許可を検索して、「実行」をクリックします。
3. 編集する許可の横にある「編集」をクリックします。
4. 新しい「許可名」を入力します。
5. 必要に応じて許可タイプを更新して、「次へ **(Next)**」をクリックします。
6. この許可の設定情報を確認します。
7. 「終了」をクリックします。

## 許可の削除

ユーザー・アカウントに関連付けられた許可を削除できます。許可を削除すると、その許可はすべてのユーザー・アカウントで使用できなくなります。

### このタスクについて

削除する許可が、あるユーザー・アカウントに関連付けられた唯一の許可である場合は、そのユーザー・アカウントを編集して、別の許可を関連付ける必要があります。そのユーザー・アカウントに新しい許可をまったく関連付けない場合は、そのユーザーはログインできますが、どのメニュー項目にもアクセスできません。

許可を削除するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「許可」を選択します。
2. 「許可名の検索 (Permission Name Search)」または「アルファベット順にリスト (Alphabetically List)」を使用して削除する許可を検索して、「実行」をクリックします。
3. 「許可」ページで、削除する許可の「削除」をクリックします。

4. 許可情報が削除する許可と一致することを確認して、「削除」をクリックします。

その許可が削除されて、次のメッセージが表示されます。

```
The system update completed successfully.
```

### 許可の名前と ID の確認

許可の名前と ID は、「管理」メニューから確認できます。

#### このタスクについて

許可の名前と ID を確認するには、以下を実行します。

#### 手順

1. 「管理メニュー」から、「アカウント」 > 「許可」を選択します。
2. 「許可名の検索 (Permission Name Search)」または「アルファベット順にリスト (Alphabetically List)」を使用して確認する許可を検索して、「実行」をクリックします。
3. 許可を選択します。 許可の名前と ID が表示されます。

## ユーザー・アカウント

ユーザー・アカウントは、セキュア環境を提供するためにグループ、許可、およびパスワード・ポリシーによって定義されます。このタイプのユーザー・アカウント定義は、役割ベース・セキュリティー・モデルとして定義されます。

新規ユーザー・アカウントを作成する前に、各自のビジネス環境で必要なグループ、許可、およびパスワード・ポリシーを特定する必要があります。グループ、許可、およびパスワード・ポリシーの割り当ては必須ではありません。

作成の許可が割り当てられたアカウントのみが新規ユーザー・アカウントを作成できます。ユーザー・アカウントを対象にした作業は次のとおりです。

- ユーザー・アカウントの作成
- ユーザー・アカウントの検索
- ユーザー・アカウントの編集
- ユーザー・アカウントの削除

### ユーザー・アカウントのデフォルトの許可

MyAccount および Admin Web App Permission は、ユーザー・アカウントに自動的に割り当てられます。

次の許可は、ユーザー・アカウントに自動的に割り当てられます。

- MyAccount (許可 ID: PLTADM30) – 「マイ・アカウント」ページ (「アカウント」>「マイ・アカウント」) へのアクセスが許可されます。
- Admin Web App Permission (許可 ID: WebAppAdminPermission) – 他の Web アプリケーションにアクセスするために使用されます。

これらの許可は、ユーザー・アカウントから削除しないでください。これらの許可が間違って削除された場合は、そのユーザー・アカウントを編集して保存します。これにより、削除された許可が復元されます。

## ユーザー・アカウント認証

ユーザー・アカウント認証は、ローカルまたは外部のいずれかにできます。

ユーザー・アカウント認証は、次のいずれかを実行できます。

- ローカル – データベースに対する認証が実行されます。
- 外部 – LDAP サーバーに対する認証が実行されます。外部認証には LDAP アダプターは必要ありません。LDAP アダプターは、Java Naming and Directory Interface (JNDI) を使用してローカルまたはリモートの LDAP サーバーと通信するために、ビジネス・プロセスとともに使用されます。シングル・サインオンや LDAP のライセンスを持っていない場合は、作成するすべてのユーザーはローカル・ユーザーになり、当アプリケーションのデータベースに対して認証されます。外部ユーザー・アカウントを作成するには、シングル・サインオンまたは LDAP に対するアプリケーション・ライセンスを持っている必要があります。

## ユーザー・アカウント作成のチェックリスト

ユーザー・アカウントを作成できます。

次のチェックリストに従って、ユーザー・アカウントを作成してください。

| タスク | 役割ベースのセキュリティーのチェックリスト | メモ欄 |
|---|---|---|
| 1 | 新しい許可を作成するか、あらかじめインストールされている構成済み許可を確認します。 | |
| 2 | 新しいグループを作成するか、あらかじめインストールされているグループを確認します。 | |
| 3 | ユーザーに割り当てるカスタム・パスワード・ポリシーを作成します。 | |
| 4 | 外部認証を使用している場合は、外部認証用の環境を構成します。 | |
| 5 | ユーザー・アカウントを作成して、許可、グループ、およびパスワード・ポリシーを割り当てます。 | |

## 外部ユーザー・アカウント認証用の環境の構成

外部ユーザーを作成する場合は、代替認証方式を指定できます (通常は LDAP)。

### このタスクについて

外部ユーザー・アカウントを作成する前に、以下を実行する必要があります。

### 手順

1. Sterling B2B Integrator を停止します。
2. authentication_policy.properties.in ファイルで認証構成を追加または変更して、代替認証方式を指定します。 設定するプロパティーは、authentication_4.*xxx*=*xxx*_value という形式に従う必要があります。
3. `setupfiles.sh` と入力します。
4. Sterling B2B Integrator を開始します。

## ユーザー・アカウントの検索

「管理」メニューから、ユーザー・アカウントを検索できます。

### このタスクについて

ユーザー・アカウントを検索するには、以下を実行します。

### 手順

1. 「管理」メニューから、「アカウント」 > 「ユーザー・アカウント」を選択します。
2. 次のいずれかの操作を実行します。
   - 「検索」の「アカウント名」フィールドに、検索するユーザー・アカウント名の一部または全体を入力して、「実行」をクリックします。「アカウント」ページに、検索条件に一致するすべてのすべてのユーザー・アカウントが一覧表示されます。
   - 「リスト」の「英数字別」フィールドで、「すべて」を選択するか、検索するユーザー・アカウント名の先頭文字を選択して、「実行」をクリックします。「アカウント」ページに、検索条件に一致するすべてのすべてのユーザー・アカウントが一覧表示されます。

## ユーザー・アカウントの作成

「管理」メニューから、新規ユーザー・アカウントを作成します。

### このタスクについて

開始前に、ローカル認証または外部認証のどちらを使用しているのかを確認する必要があります。

- ローカル – アプリケーションのデータベースに対する認証が実行されます。これがデフォルトです。
- 外部 – LDAP サーバーに対する認証が実行されます。外部認証は LDAP アダプターを必要としません。LDAP アダプターは、ビジネス・プロセスとともに使用され、システムが Java Naming and Directory Interface (JNDI) を使用してローカル、またはリモートの LDAP サーバーと通信できるようにします。

このアカウントに 1 つ以上の許可ユーザー・キーを割り当てる場合は、ユーザー・アカウントの作成前に、それらのキーを取引パートナーから取得してチェックインする必要があります。

注: 複数の言語がサポートされていますが、ユーザー・インターフェースの表示に関する問題を避けるために、1 つのユーザー・アカウントを複数の言語で使用しないでください。

また、以下の情報も認識しておく必要があります。

| フィールド | 説明 |
|---|---|
| ユーザー ID | 作成するユーザー・アカウントのユーザー ID。ユーザー ID は 5 文字以上長さの英数字であることが必要です。特殊文字や句読点は許可されません。必須。<br><br>MySQL データベースに限っては、ログインで大文字と小文字が区別されません。常に、固有スペルの ID を使用して、ユーザーが偶発的に別のユーザーの ID を使用することがないようにします。 |
| パスワード (ローカル認証のみ) | 作成するユーザー・アカウントのパスワード。パスワードは 6 文字以上の長さの英数字であることが必要です。特殊文字は許可されます。ローカル・ユーザーの場合は必須。外部ユーザーにはこのフィールドは表示されません。 |
| パスワードの確認 (ローカル認証のみ) | 2 回目のパスワード入力です。ローカル・ユーザーの場合は必須。外部ユーザーにはこのフィールドは表示されません。 |
| ポリシー (ローカル認証のみ) | ユーザー・アカウントに関連付けられるパスワード・ポリシー。関連付けるポリシーをリストから選択します。オプション。外部ユーザーにはこのフィールドは表示されません。<br><br>有効期限は、システムによってユーザーが初めてこのパスワードを使用してログインした日付から計算されます。 |
| 認証ホスト (Authentication Host) (外部認証のみ) | ユーザーの認証が実行される Lightweight Directory Access Protocol (LDAP) サーバー。このフィールドに表示されるサーバー (複数の場合もあり) は、authentication_policy.properties.in ファイルで指定されています。 |
| セッション・タイムアウト | 非アクティブな状態で保持できる期間 (分)。この期間を経過すると再ログインが必要になります。分単位の時間です。必須。 |
| アクセシビリティー (Accessibility) | ユーザー・アカウントがアクセスできるダッシュボード・ユーザー・インターフェースの部分。オプション。<br><br>アクセシビリティーには以下のオプションがあります。<br>• 管理 UI – ダッシュボードの管理コンソール・ペインのみにアクセスします。<br>• AS2 UI – AS2 Edition インターフェースのみにアクセスします。<br>• ダッシュボード UI – ダッシュボード・インターフェースにアクセスします。ダッシュボード・テーマの選択によって絞り込まれます。 |

| フィールド | 説明 |
| --- | --- |
| ダッシュボード・テーマ | ユーザー・アカウントにアクセスが許可される事前定義のダッシュボード。アクセシビリティーがダッシュボード UI に設定されている場合は必須。<br><br>以下は、ダッシュボード・テーマのオプションです。<br>• デフォルト<br>• オペレーター<br>• 参加者<br>• 参加者スポンサー (Participant Sponsor)<br>• スポンサー<br>• AFT |
| 名 (Given Name) | ユーザーの名。必須。 |
| 姓 (Surname) | ユーザーの姓。必須。 |
| E メール | ユーザーの E メール・アドレス。 |
| ポケットベル (Pager) | ユーザーのポケットベルの番号。 |
| 優先言語 | 「クライアント・アプリケーションの設定を使用」という値に設定します。<br>**注:** この値に設定した場合は、Sterling B2B Integrator はユーザーのブラウザーで指定された言語およびクライアント・オペレーティング・システムのロケールで指定された言語、またはそのいずれかを使用します。<br>**注:** これはデフォルト値です。 |
| マネージャー ID (Manager ID) | ユーザーのマネージャーのユーザー ID。 |
| ID | ユーザー・アカウントに関連付ける取引パートナーの ID。1 つのユーザー・アカウントに関連付けることができる取引パートナーは 1 つのみです。ユーザー・アカウントは、それぞれが独自の取引パートナー ID の関連付けを持つ多数のグループに関連付けることができます。これにより、ユーザー・アカウントを複数の取引パートナーに関連付けることができます。「ID」フィールドは、メールボックス内のメッセージのルーティングに使用されます。取引パートナー ID をリストから選択します。<br><br>デフォルト値は、ハブ組織です。 |

ユーザー・アカウントを作成するには以下のようにします。

## 手順

1. 「管理」メニューから、「アカウント」 > 「ユーザー・アカウント」を選択します。
2. 「新規アカウントの作成 **(Create a new Account)**」の横にある「実行 **(Go!)**」をクリックします。

3. 「新規アカウント」ページで、「認証タイプ」を選択します。
4. 「ユーザー **ID**」を入力します。
5. 「パスワード」を入力します。
6. パスワードを確認します。
7. 「ポリシー」を選択します。
8. 「セッション・タイムアウト」を入力します。
9. 「アクセシビリティー **(Accessibility)**」を選択します。
10. 「ダッシュボード・テーマ **(Dashboard Theme)**」を選択します。
11. 「次へ **(Next)**」をクリックします。
12. 「SSH 許可ユーザー・キー (SSH Authorized User Key)」ページで、1 つ以上の公開鍵を割り当てます。それらの鍵を「使用可能 **(Available)**」ペインから「割り当て済み」ペインに移動して、「次へ **(Next)**」をクリックします。
13. 「グループ」ページで、権限のグループを割り当てます。グループ名を「選択可能 **(Available)**」 ペインから「割り当て済み **(Assigned)**」ペインに移動して、「次へ **(Next)**」をクリックします。
14. 「許可 (Permissions)」ページで個別の許可を割り当てます。権限を「選択可能 **(Available)**」ペインから「割り当て済み **(Assigned)**」ペインに移動して、「次へ **(Next)**」をクリックします。 デフォルトでは、このユーザーが割り当てられたグループに関連付けられた許可が既に選択されています。必須の許可は、「Admin Web App および MyAccount」です。
15. 「ユーザー情報」ページで、「名 **(Given Name)**」を入力します。
16. 「姓 **(Surname)**」を入力します。
17. 「**E** メール・アドレス」を入力します。
18. 「ポケットベル番号 **(Pager number)**」を入力します。
19. 「優先言語」を選択します。「クライアント・アプリケーションの設定を使用」という値を選択します。

    注**:** この値に設定した場合は、Sterling B2B Integrator はユーザーのブラウザーで指定された言語およびクライアント・オペレーティング・システムのロケールで指定された言語、またはそのいずれかを使用します。
20. 「マネージャー **ID (Manager ID)**」を入力します。
21. 「**ID**」を選択します。
22. 「次へ **(Next)**」をクリックします。
23. ユーザー・アカウントの設定を確認します。
24. 「終了」をクリックします。 ユーザー・アカウントが作成され、次のメッセージが表示されます。

    ```
    The system update completed successfully.
    ```

    外部ユーザーを作成した場合は、システムからログアウトしてから、外部ユーザー ID またはアカウントを使用してログインしなおします。外部ユーザー ID は、外部 LDAP サーバー上でシステムにより認証されます。

## ユーザー・アカウントの編集

「管理」メニューから、ユーザー・アカウントを編集できます。

### このタスクについて

注**:** 複数の言語がサポートされていますが、ユーザー・インターフェースの表示に関する問題を避けるために、1 つのユーザー・アカウントを複数の言語で使用しないでください。

ユーザー・アカウントを編集するには、以下を実行します。

### 手順

1. 「管理」メニューから、「アカウント」 > 「ユーザー・アカウント」を選択します。
2. 「検索」または「リスト」のオプションを使用して、編集するユーザー・アカウントを探します。
3. 編集するユーザー・アカウントの「編集」をクリックします。
4. 必要に応じて、このユーザーの認証タイプを変更します。

   認証タイプを外部からローカルに変更した場合は、このユーザーのパスワードを作成する必要があります。認証タイプをローカルから外部に変更した場合は、このユーザーのパスワードやパスワード・ポリシーを変更することはできません。
5. 必要に応じて「新規パスワード」を変更して、新規パスワードを確認入力します。
6. 必要に応じて「ポリシー」を変更します。
7. 必要に応じて「セッション・タイムアウト」を変更して、「次へ **(Next)**」 をクリックします。
8. 必要に応じて「**SSH** 許可ユーザー・キー」を変更して、「次へ **(Next)**」をクリックします。
9. 必要に応じてグループについて変更して、「次へ **(Next)**」をクリックします。
10. 必要に応じて許可について変更して、「次へ **(Next)**」をクリックします。

    「Admin Web App Permission」や「MyAccount」を削除することはできません。
11. 必要に応じてユーザー情報を変更して、「次へ **(Next)**」をクリックします。

    注**:** サポートされている言語でユーザー・インターフェースを表示するユーザー・アカウントについては、「優先言語」の値が「クライアント・アプリケーションの設定を使用」に設定されていることを確認します。この値に設定した場合は、Sterling B2B Integrator はユーザーのブラウザーで指定された言語およびクライアント・オペレーティング・システムのロケールで指定された言語、またはそのいずれかを使用します。
12. ユーザー・アカウントの設定を確認します。
13. 「終了」をクリックします。

## ユーザー・アカウントの削除

「管理」メニューから、ユーザー・アカウントを削除できます。

### このタスクについて

ユーザー・アカウントを削除するには、以下を実行します。

### 手順

1. 「管理」メニューから、「アカウント」 > 「ユーザー・アカウント」を選択します。
2. 「検索」または「リスト」のオプションを使用して、削除するユーザー・アカウントを探します。
3. 削除するユーザー・アカウントの「削除」をクリックします。
4. 「**OK**」をクリックします。
5. ユーザー・アカウントの設定を確認します。
6. 「削除」をクリックします。 選択したユーザー・アカウントが削除されて、次のメッセージが表示されます。

   ```
   The system update completed successfully.
   ```

## マイ・アカウント情報の更新

マイ・アカウント情報は自身のユーザー名とパスワードに関連付けられているため、ログインすると、自身の個人情報が「マイ・アカウント」ページに表示されます。自身のアカウント情報を編集して、システムにログインしたときに表示される初期ページを変更できます。

### このタスクについて

個人アカウント情報が変わったために、自身のアカウント情報の編集が必要になることがよくあります。また、セキュリティー上の理由からパスワードの変更が必要になることもあります。

注**:** 複数の言語がサポートされていますが、ユーザー・インターフェースの表示に関する問題を避けるために、1 つのユーザー・アカウントを複数の言語で使用しないでください。

アカウント情報を更新するには、以下を実行します。

### 手順

1. 「管理」メニューから、「アカウント」 > 「マイ・アカウント」を選択します。
2. アカウント・パスワードを更新するには、「旧パスワード」フィールドに現在のパスワードを入力して、「新規パスワード」フィールドに新しいパスワードを入力します。新しいパスワードをもう一度「新規パスワードの確認」フィールドに入力します。
3. 「名」、「姓」、「**E** メール」、または「ポケットベル」の各フィールドの値を、必要に応じて変更します。
4. このアカウントに割り当てられた「**SSH** 許可ユーザー・キー」を変更するには、「使用可能 (Available)」ペインから「割り当て済み」ペインに鍵を移動します。
5. 「優先言語」を変更するには、任意の言語を選択します。

注**:** サポートされている言語でユーザー・インターフェースを表示するユーザー・アカウントについては、「優先言語」の値が「クライアント・アプリケーションの設定を使用」に設定されていることを確認します。この値に設定した場合は、Sterling B2B Integrator はユーザーのブラウザーで指定された言語およびクライアント・オペレーティング・システムのロケールで指定された言語、またはそのいずれかを使用します。

6. ログイン時に表示される「ウェルカム・ページ」 (管理コンソール・ホーム) を変更するには、リストから選択します。
7. 「現行プロセス」ページに同時に表示されるプロセスの数を変更するには、「現行プロセスのページ・サイズ」で新しい値を選択します。
8. 「現行ドキュメント」ページに同時に表示されるドキュメントの数を変更するには、「現行ドキュメントのページ・サイズ」で新しい値を選択します。
9. ブラウザー・ウィンドウを再利用してショートカットを起動するには、「ショートカットの起動にウィンドウを再使用します」を選択します。
10. 過去に入力したストリングに基づいて検索値がオートコンプリートされるようにするには、「検索のオートコンプリート」を選択します。
11. システム側で検索値が記憶されるようにするには、「検索に使用した値を記憶」を選択します。 このオプションを選択すると、各検索フィールドで前回に入力された値が保存されます。
12. 「保存 **(Save)**」をクリックします。 新しいアカウント情報が保存されて、次のメッセージが表示されます。

    ```
    Your update has completed successfully.
    ```

## ログインするためのユーザー・アカウントのユーザー出口 (V5.2.5 以上)

Sterling B2B Integrator には、Active Directory 同期ユーザー出口があり、これは、Sterling B2B Integrator ユーザー・インターフェースの代わりに Active Directory でユーザー・アカウントを管理するために使用できます。これらのユーザー出口は、IBM サービスの顧客エンゲージメントが締結されている場合に IBM サービスが構成することができます。詳しくは、IBM 営業担当員にお問い合わせください。

| ユーザー出口 | 説明 |
|---|---|
| IUserLoginUserExit_preAuthenticate | 認証の前にカスタム・コードを挿入するために使用します。 |
| IUserLoginUserExit_postAuthenticateFail | 認証に成功した後にカスタム・コードを挿入するために使用します。 |
| IUserLoginUserExit_postAuthenticateSuccess | 認証に失敗した後にカスタム・コードを挿入するために使用します。 |

## ログアウトするためのユーザー・アカウントのユーザー出口 (V5.2.6 以上)

Sterling B2B Integrator には、Active Directory 同期ユーザー出口があり、これは、Sterling B2B Integrator ユーザー・インターフェースの代わりに Active

Directory でユーザー・アカウントを管理するために使用できます。これらのユーザー出口は、IBM サービスの顧客エンゲージメントが締結されている場合に IBM サービスが構成することができます。詳しくは、IBM 営業担当員にお問い合わせください。

| ユーザー出口 | 説明 |
| --- | --- |
| ILogoutUserExit_OnSessionInvalidate | セッションが無効になる前にカスタム・コードを挿入するために使用します。 |

# シングル・サインオン

## シングル・サインオン

### シングル・サインオン

シングル・サインオン (SSO) とは、ユーザーがユーザー名とパスワードを 1 回入力するだけで、複数のアプリケーションを利用できるようにする認証プロセスです。以前、各アプリケーションにログインしたユーザーは、複数のユーザー名とパスワードを管理する必要がありました。

SSO のユーザー認証には LDAP アダプターは必要ありません。LDAP アダプターは、JNDI (Java Naming and Directory Interface) を使用してローカルまたはリモートの LDAP サーバーと通信するために、ビジネス・プロセスとともに使用されます。

Sterling B2B Integrator で SSO を可能にする手段は、Netegrity SiteMinder と統合すること、または他のシングル・サインオン・アプリケーションおよびサーバー上の SSO プラグイン用のカスタム実装クラスを使用することです。

シングル・サインオンは、次のコンポーネントに限定されています。

- 管理インターフェース
- メールボックス・インターフェース
- ダッシュボード・インターフェース
- 拡張ファイル転送 (AFT) インターフェース
- MyAFT インターフェース

### シングル・サインオン・プロバイダーのデフォルト・クラス

ダッシュボードを除くすべてのインターフェースの SSO ログイン URL は、通常のログイン・インターフェースと似ています。ダッシュボード・インターフェースの URL は、http://Host:port/dashboard/sso.jsp です。ダッシュボード・インターフェースの要求ヘッダーには、SM_USER=SSO User Name のように値が含まれる必要があります (またはこの値を security.propertiesファイル内の SSO_USER_HEADER で構成できます)。

SSOProviderDefault インターフェースを使用すると、シングル・サインオン (SSO) プラグインは、Netegrity SiteMinder 用のシングル・サインオン機能を処理できます。

ユーザーが SSO セッションからログオフした後に、(Sterling B2B Integrator のログオフ・ページにリダイレクトする代わりに) 外部 HTTP ページにリダイレクトするように SSO を構成できます。 SSO サーバーからの外部ページは、ログイン・ページでもログオフ・ページでもかまいません。

次の例では、SSOProviderDefault.java クラスを示しています。

```
package com.sterlingcommerce.server_name.security.authentication;
import javax.servlet.*;
import javax.servlet.http.*;
import com.sterlingcommerce.server_name.security.SecurityManager;
import com.sterlingcommerce.server_name.util.frame.log.Logger;
import java.util.Properties;
import com.sterlingcommerce.server_name.util.frame.Manager;
import java.util.*;
/**
 * Default Single Sign On implementation for ISSOProvider that will use
* Request Header to get SSO_USER
 *
 * @author developer name
 */
public final class SSOProviderDefault implements ISSOProvider  {
    private static final String CLASS_NAME = "SSOProviderDefault";
    private static final Logger LOG = SecurityManager.getInstance().getLogger();
    private static final Logger AUTHLOG =
            SecurityManager.getInstance().getAuthenticationLogger();
/**
* Authenticate SSO processing (login)
*
* @param Request : The http request.
*
* @return String : The SSO User ID if the authentication is passed
*                : null if authentication is denied
* << No Exception thrown for the default SSO Provider - Either have value or null >>
*/
public String authenticate(HttpServletRequest request)
                        throws SSOAuthenticationException, SSOException
{
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (AUTHLOG.debug) {
          AUTHLOG.logDebug(CLASS_NAME + " Authenticate user tag : " +
              SecurityManager.getInstance().getSSOAuthenticationHeader() +
              " value : " + sso_user);
    }
    return sso_user;
}
/**
 * AuthenticatePage SSO processing (Page)
 *
 * @param Request : The http request.
*
 * @return boolean : True if the SSO authentication on the Page is passed or no Page
 *                   authentication is needed because not enable or not SSO User.
 *                 : False if authentication is denied
 *                   (Must throw SSOException if return false!!!!)
 */
public boolean authenticatePage(HttpServletRequest request)
                         throws SSOAuthenticationException, SSOException
{
    return true; // Always pass Page Validation for SSOProviderDefault
    /*****  Uncomment if want to do SSO_USER_HEADER (SM_USER) check on Page
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (sso_user != null) {
       passed = true;
```

```
    } else {
       passed = false;
       throw new
   SSOAuthenticationException(ISSOProvider.REASON_SSO_AUTHENTICATION_FAILURE);
    }
    return passed;   ******/
}
/**
 * When user logs out, calling this to do any extra actions
*
 * @param Response : The http response
 * @param Request : The http request.
 * @param int reason : An id to to tell where we called from
* @param String : The String identify the session type: WS, DASHBOARD, MAILBOX,
 *            AFT, MYAFT, or null if don't know
*
 * @return boolean : True if executes sucessfully,
 *           False if not & should use default logout logic
 *
 */
public boolean invalidate(HttpServletRequest request, HttpServletResponse response,
int reason, String sessionType)
{
    HttpSession session = request.getSession(false);
    String forward = "SSO_FORWARD_URL";
    if (sessionType != null)   {
       forward = forward + ".";
       forward = forward + sessionType;
    }
    if (reason == REASON_GIS_SESSION_EXPIRED) {
       forward = forward + ".GIS_TIMEOUT";
    }
    else if (reason == REASON_LOGOUT)  {
       forward = forward + ".LOGOUT";
    }
    else {  // Others reason : send all to VALIDATION_FAILED
       forward = forward + ".VALIDATION_FAILED";
    }
    String forwardUrl = getForwardURLParameter(forward);
    if (AUTHLOG.debug) {
       AUTHLOG.logDebug(CLASS_NAME + " Forward properties: " + forward +
" is forwardUrl: " + forwardUrl);
    }
    if (forwardUrl != null) {
       try {
           // Dashboard Timeout - Use JSP to kick outof IFrame
           if ((reason == REASON_GIS_SESSION_EXPIRED)&&
  (sessionType != null) &&
               (sessionType.equalsIgnoreCase(DASHBOARD_SESSION))) {
              if (AUTHLOG.debug) {
                   AUTHLOG.logDebug(CLASS_NAME + " Set ExternalSsoUrl = "
                                                 + forwardUrl);  }
              request.setAttribute("ExternalSsoUrl", forwardUrl);
              return false; // Set to false, we need to handle redirect in JSP
           } else {
              response.sendRedirect(response.encodeRedirectURL(forwardUrl));
           }
       } catch (Exception e) {
           return false;
       }
       return true;
   }
   return false;   // Use default logic (ie: GIS Logout/Login Page)
}
}
```

# シングル・サインオン・プラグイン・コンポーネント

Sterling B2B Integrator では、他のシングル・サインオン・アプリケーションおよびサーバー上のシングル・サインオン (SSO) プラグイン用のカスタム実装クラスを使用できます。SSO プラグインを実装するには、security.properties ファイルに SSO_AUTHENTICATION_CLASS.<n>=<New class entry> という実装クラスを追加する必要があります。

次の ISSOProvider.java インターフェース・クラスに基づいて、SSO プラグイン用のカスタム実装クラスを記述できます。

## SSOProvider.java インターフェース・クラス

```
import javax.servlet.*;
import javax.servlet.http.*;
public interface ISSOProvider {
public static final int REASON_UNKNOWN = -1;
public static final int REASON_SSO_SESSION_EXPIRED = 1
public static final int REASON_HTTP_SESSION_EXPIRED = 2;
public static final int REASON_LOGOUT = 3;
public static final int REASON_SSO_AUTHENTICATION_FAILURE = 4;
public static final int REASON_GIS_AUTHENTICATION_FAILURE = 5;
public String authenticate(HttpServletRequest request)
throws SSOAuthenticationException, SSOException;
public boolean invalidate(HttpServletRequest request,
HttpServletResponse response, int reason, String sessionType)
throws SSOAuthenticationException;
public boolean authenticatePage(HttpServletRequest request)
throws SSOAuthenticationException, SSOException;
}
```

## SSOException クラス

```
public class SSOException extends Exception {
private int reason = -1;
public int getReason() { return reason; }
public void setReason(int reason) { this.reason = reason; }
}
```

## SSOAuthenticationException クラス

```
public class SSOAuthenticationException extends SSOException { }
```

### ユーザー認証メソッド

authenticate メソッドは、ログイン時に初期化されます。認証に合格した場合は、authenticate メソッドはユーザー ID を返します。認証に合格しなかった場合は、SSOAuthenticationException がスローされます。この例外には、適切な理由コードが含まれている必要があるとともに、SSO ヘッダーが存在する場合は処理対象のリダイレクト・ページが含まれている必要があります。 SSO ヘッダーが存在しない場合は、制御はシステム・ログイン画面に戻されます。

### ページ認証メソッド

authenticatePage メソッドは、各ページで初期化されます。SSO サーバーからのページ遷移の際に行われる追加の検証は、このメソッドで処理されます。例えば、SSO サーバーに対して ping を実行して、SSO セッションがタイムアウトになっているかどうかを確認できます。認証に合格しなかった場合は、例外がスローされる

必要があり、この例外には適切な理由コードとリダイレクト・ページが含まれている必要があります。

### 無効な SSO 要求

invalidate メソッドが初期化されるのは、ユーザーがログオフしたとき、ログインまたはページの認証に合格しなかったとき、またはセッションが時間切れになったときです。SSO 要求を無効化するために、HTTP リダイレクト・メソッドが実行される必要があります。認証に合格しなかった場合は、次のメソッドが初期化されます。

- SSO サーバーの認証には合格したものの、Sterling B2B Integrator の認証には合格しなかった場合は、REASON_GIS_AUTHENTICATION_FAILURE メソッドが初期化され、理由コードが示されます。
- SSO サーバーの認証に合格しなかった場合は、REASON_SSO_AUTHENTICATION_FAILURE メソッドが初期化され、理由コードが示されます。
- ユーザーがログオフした場合は、REASON_LOGOUT メソッドが初期化され、理由コードが示されます。
- HTTP セッションが期限切れになった場合は、REASON_HTTP_SESSION_EXPIRED メソッドが初期化され、理由コードが示されます。
- ユーザーの SSO セッションが時間切れになった場合は、REASON_SSO_SESSION_EXPIRED メソッドが初期化され、理由コードが示されます。

## Netegrity SiteMinder を使用したシングル・サインオンのチェックリスト

シングル・サインオン (SSO) を構成するには、SSO と Netegrity SiteMinder に関する知識が必要です。

このチェックリストに従って、Netegrity SiteMinder を使用して SSO を構成してください。

| タスク | **Netegrity SiteMinder** を使用したシングル・サインオンのチェックリスト | メモ |
|---|---|---|
| 1 | Netegrity SiteMinder をインストールして、リバース・プロキシー・サーバーを使用して Netegrity SiteMinder を構成します。 | |
| 2 | Netegrity SiteMinder で使用するプロパティー・ファイルを構成します。 | |
| 3 | Netegrity セキュア・プロキシー・サーバーを構成します。 | |

| タスク | **Netegrity SiteMinder** を使用したシングル・サインオンのチェックリスト | メモ |
|---|---|---|
| 4 | Netegrity サーバーのセキュア・レルムを作成します。 | |

他のシングル・サインオン・アプリケーションおよびサーバー用の SSO プラグインのカスタム実装については、『シングル・サインオン・プラグイン・コンポーネント』を参照してください。

## IBM Global High Availability Mailbox (V5.2.6 以上) を使用したシングル・サインオン

適切な許可を持つ Sterling B2B Integrator ユーザーは、Sterling B2B Integrator からシングル・サインオンにより IBM® Global High Availability Mailbox 管理ツールに直接アクセスして、Global Mailbox を管理することができます。

### 始める前に

Sterling B2B Integrator から Global Mailbox 管理ツールに直接アクセスするには、Sterling B2B Integrator ユーザーは以下のいずれかのグループに属している必要があります。

- メールボックス
- 展開
- メールボックス管理者
- *Sterling B2B Integrator* 管理

### このタスクについて

シングル・サインオンによる Global Mailbox 管理ツールへのアクセスを選択すると、 Sterling B2B Integrator セッションは使用可能なまま、Web ブラウザーの新規タブに Global Mailbox の新規セッションが開かれます。

シングル・サインオンにより Global Mailbox にアクセスできるのは、Sterling B2B Integrator からのみです。 Global Mailbox 管理ツールからサインアウトしても、Sterling B2B Integrator セッションからサインアウトされるわけではありません。

Global Mailbox 管理者パスワードを変更したい場合は、Global Mailbox 管理ツールに直接サインインする必要があります。

制約事項: シングル・サインオンで Global Mailbox 管理ツールにサインインした場合、Global Mailbox 管理者パスワードを変更することはできませんし、「管理者」メニューに「パスワード変更」も表示されません。

シングル・サインオンにより Global Mailbox 管理ツールにアクセスするには、次の手順を実行します。

### 手順

1. 「管理コンソール」ページで、「管理メニュー」にある「展開」を展開します。
2. 「**Global Mailbox**」を展開します。
3. 「メールボックス管理 **(Mailbox Administration)**」を選択します。
4. 「**Global Mailbox** 管理ツールの起動」ハイパーリンクをクリックして、Global Mailbox 管理ツールで新規セッションを開きます。

   要確認**:** 「**Global Mailbox** 管理ツールの起動」ハイパーリンクをクリックすると、Web ブラウザーの新規タブに Global Mailbox の新規セッションが開きます。

## Netegrity SiteMinder を使用したシングル・サインオン用のプロパティー・ファイルの構成

Netegrity SiteMinder を使用してシングル・サインオン用のプロパティー・ファイルを構成できます。

### このタスクについて

neo-ui.properties ファイルと security.properties ファイルを編集するには、以下を実行します。

### 手順

1. Sterling B2B Integrator を停止します。
2. /*install_dir*/install/properties にナビゲートします。
3. neo-ui.properties ファイルを開きます。
4. 各インターフェースの関連付けられた SSO エントリーを追加します。次のコード・サンプルでは、同じ HTTP サイトに対する、関連付けられたエントリーを示しています。

```
url.host=%(host)
url.port=10200
url.cm=http://%(host):10200/communitymanagement/
url.cm.sso=http://%(host):10200/communitymanagement/
url.ob=http://%(host):10233/onboard/
url.ws=http://%(host):10200/ws/
url.ws.sso=http://%(host):10200/ws/
url.dash.sso=http://%(host):10233/dashboard/
url.ds=http://%(host):10200/datastore/
url.help=http://%(host):10200/help/index.htm?context=webhelplocal&single=true&topic=
url.help.ja=http://%(host):10200/help_ja/index.htm?context=webhelplocal&single=true& topic=
url.dash=http://%(host):10233/dashboard/
portlet.refresh.interval.seconds=60
url.aft=http://%(host):10200/aft/
url.aft.sso=http://%(host):10200/aft/
url.dmi=http://%(host):10200/dmi/
url.dmi.sso=http://%(host):10200/dmi/
```

5. neo-ui.properties ファイルを保存して閉じます。
6. テキスト・エディターで /*install_dir*/install/properties/security.properties ファイルを開きます。

7. security.properties ファイルで、次のコード・サンプルで示している ## SSO Authentication の構成パラメーターを探します。

```
## SSO Authentication configuration
## enable sso authentication  (true, false) default=false
SSO_AUTHENTICATION_ENABLED=true
## enable sso authentication on each Page (true, false) default=false
#SSO_PAGE_AUTHENTICATION_ENABLED=false
## http header variable that contains externally authenticated userid
SSO_USER_HEADER=SM_USER
## List of SSOProvider Classes that are supplied to use - If SSO Authentication is
## enable, should have at least one class, the following is the default one that we
## supplied.
## SSO_AUTHENTICATION_CLASS.1= <SSOProvider Class 1> Will try to use this first
## SSO_AUTHENTICATION_CLASS.2= <SSOProvider Class 2> Will try to use this if first
## one failed
## SSO_AUTHENTICATION_CLASS.3= <SSOProvider Class 3> Will try to use this if second ## one failed too
## SSO_AUTHENTICATION_CLASS.<n>= <SSOProvider Class n> Will try to use this if all
## first –1 classes failed
SSO_AUTHENTICATION_CLASS.1=com.sterlingcommerce.woodstock.security.authentication.SS OProviderDefault
## External Page for SSO when Logout (Specify the SSO Server external page for each of
## the cases)
## Example: SSO_FORWARD_URL.MAILBOX.LOGOUT=http://sterlingcommerce.com
## After SSO User logout from Mailbox, instead of display the Mailbox Login Screen
## display IBM Web page.
SSO_FORWARD_URL.AFT.LOGOUT=
SSO_FORWARD_URL.MYAFT.LOGOUT=
SSO_FORWARD_URL.MAILBOX.LOGOUT=
SSO_FORWARD_URL.WS.LOGOUT=
SSO_FORWARD_URL.DASHBOARD.LOGOUT=
## Default handling for LOGOUT if don't know source
SSO_FORWARD_URL.LOGOUT=
## External Page for SSO when Timeout (Specify the SSO Server External page for each ## of the case)
SSO_FORWARD_URL.AFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MYAFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MAILBOX.GIS_TIMEOUT=
SSO_FORWARD_URL.WS.GIS_TIMEOUT=
SSO_FORWARD_URL.DASHBOARD.GIS_TIMEOUT=
## Default handling for TIMEOUT if don't know source
SSO_FORWARD_URL.GIS_TIMEOUT=
## External Page for SSO on Validation/Authentication failure (SSO User Validation
## Failed - At login or Page Validation)
SSO_FORWARD_URL.AFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MYAFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MAILBOX.VALIDATION_FAILED=
SSO_FORWARD_URL.WS.VALIDATION_FAILED=
SSO_FORWARD_URL.DASHBOARD.VALIDATION_FAILED=
##Default handling for VALIDATION FAILED if don't know source
SSO_FORWARD_URL.VALIDATION_FAILED=
```

8. ##SSO Authentication 構成エントリーの下で、SSO パラメーターに次の変更を加えます。

| パラメーター | 説明 | 初期値 | 新しい値 |
|---|---|---|---|
| SSO_AUTHENTICATION_ENABLED | SSO を使用可能または使用不能にします。 | False | True |
| SSO_USER_HEADER | Netegrity SiteMinder またはご使用の SSO アプリケーションの構成内のユーザー・ヘッダー名。 | SM_USER<br><br>これは、Netegrity SiteMinder 内の値です。 | Netegrity SiteMinder 内またはご使用の SSO アプリケーション内のエントリーと一致する必要があります。 |

| パラメーター | 説明 | 初期値 | 新しい値 |
| --- | --- | --- | --- |
| SSO_PAGE_ AUTHENTICATION_ ENABLED | すべてのページで SSO 認証を有効または無効にします。 | False | True – すべてのページで SSO を認証します。<br><br>カスタム SSO プロバイダー・クラスが提供されている場合にのみ変更します。 |
| SSO_AUTHENTICATION_ CLASS.n | 認証をサポートする実装クラス。 | com.sterling commerce.woodstock. security.authentication .SSOProviderDefault | 提供されている SSOProvider クラスのリストから選択します。 |
| SSO_FORWARD_ URL URL | ユーザーがメールボックスからログオフした後に、指定された URL のページを表示します。URL が指定されていない場合は、デフォルト・ページを表示します。 | コメント化された状態<br><br>デフォルト・ページを表示します。 | URL を指定します。 |

9. security.properties ファイルを保存して閉じます。
10. Sterling B2B Integrator を開始します。

## Netegrity セキュア・プロキシー・サーバーの構成

転送ルールを proxyrules.xml ファイルに追加することで、Netegrity セキュア・プロキシー・サーバーを構成できます。

### このタスクについて

Netegrity セキュア・プロキシー・サーバーを構成する前に、次のことを実行する必要があります。

- Sterling B2B Integrator を acme.si.com などのサーバーにインストールします。
- メールボックス・ブラウザー・インターフェース (MBI) がインストールされているポート番号を確認します。この情報を適切な転送ルールで使用する必要があります。
- Sterling B2B Integrator のダッシュボードのユーザー・インターフェースがインストールされているポート番号を確認します。この情報を適切な転送ルールで使用する必要があります。

Netegrity セキュア・プロキシー・サーバーを構成するには、以下を実行します。

### 手順

1. Sterling B2B Integrator 用の必要な転送ルールを /opt/netegrity/proxy-engine/conf/proxyrules.xml ファイルに追加します。

   次の例では、Sterling B2B Integrator のコンポーネントにアクセスするための転送ルールを追加した後の、完成した proxyrules.xml ファイルの内容を示しています。

```
<?xml version="1.0"?>
<?cocoon-process type="xslt"?>
<!DOCTYPE nete:proxyrules SYSTEM "file:////home/netegrity/proxy-engine/conf/dtd/proxyrules.dtd">
<!-- Proxy Rules-->
<nete:proxyrules xmlns:nete="http://acme.com/">
   <nete:cond criteria="beginswith" type="uri">
<nete:case value="/gbm">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/help">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/webxtools">
   <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/mailbox">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/dashboard">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:case value="/portlets">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:case value="/datastore">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:default>
   <nete:forward>http://acme.portalserver.com$0</nete:forward>
</nete:default>
</nete:cond>
</nete:proxyrules>
```

2. 次の行を proxyrules.xml ファイルに追加して、セキュア・プロキシー・サーバーでのクロス・サーバー・スクリプト・チェックを無効にします。その理由は、Sterling B2B Integrator は、Netegrity クロス・サーバー・スクリプト・ポリシーの適用をサポートしていないからです。

   ```
   # Web Agent.conf
   <WebAgent>
   ...." existing web agent configuration parameters"
   badurlchars=""
   badcsschars=""
   CSSChecking="NO"
   </WebAgent>
   ```

3. proxyrules.xml ファイルを保存して閉じます。

## Netegrity ポリシー・サーバーのセキュア・レルムの作成

Netegrity ポリシー・サーバーの管理者は、セキュア・プロキシー・サーバーによって転送されるそれぞれの URL パターンに関してセキュア・レルムを作成する必要があります。これらのセキュリティー・レルムには、認証と許可のための必要なルールが割り当てられている必要があります。

### このタスクについて

また、セキュア・プロキシー・サーバー内の Web エージェントは、ポリシー・サーバーと通信するように構成されている必要があります。

以下の URL パターンのそれぞれについて 1 つのセキュア・レルムを作成します。

| URL パターン | 以下へのアクセスを可能にします |
|---|---|
| /mbi/* | アプリケーション・メールボックス・インターフェース |
| /dashboard/* | アプリケーション・ダッシュボード・インターフェース (http://host:port/dashboard というフォーマットを使用) |
| /datastore/* | データ・ストア・コンポーネント |
| /portlets/* | ダッシュボード・インターフェース内のアプリケーション・ポートレット・コンポーネント |
| /help/* | コンテキスト依存ヘルプ・コンポーネント |
| /webxtools/* | Web エクステンション・ユーティリティー |
| /gbm/* | グラフィカル・プロセス・モデラー・コンポーネント |

# パスワード

## パスワード・ポリシー

パスワード・ポリシーは一連のセキュリティー規則であり、管理者は自社のセキュリティー・ポリシーに従って、これらのセキュリティー規則を策定して、さまざまなユーザー・アカウントに適用します。これらの規則としては、パスワードの有効日数やパスワードの最大長と最小長などが挙げられます。

パスワード・ポリシーを使用すると、新規ユーザーを追加する際のセキュリティー関連作業を効率化できます。ユーザーごとに個別のポリシーを適用する代わりに、1つのパスワード・ポリシーを作成して、同じアクセス権を必要とするすべてのユーザーにそのパスワード・ポリシーを適用できます。

パスワード・ポリシーを作成したら、そのパスワード・ポリシーを内部ユーザー・アカウントのみに適用できます。これにより、セキュリティー・ポリシーの管理について最大限の柔軟性が得られます。LDAP を使用している場合は、パスワード・ポリシーを外部アカウントに適用することはできません。

パスワード・ポリシーのデフォルト値は次のとおりです。

| パラメーター | デフォルト値 |
|---|---|
| ポリシー ID | default_user |
| ポリシー名 | デフォルト・ユーザー・ポリシー (Default User Policy) |
| 有効な日数 | 60 |
| 最小長 | 6 |
| 最大長 | 28 |
| 履歴に保持するパスワード数 | 5 |
| パスワードに必ず特殊文字を含める | 選択済み |
| 初回のログイン試行時にパスワード変更が必要 | 選択済み |

パスワード・ポリシーを対象にした作業は次のとおりです。

- パスワード・ポリシーの作成

- パスワード・ポリシーの検索
- パスワード・ポリシーの編集
- パスワード・ポリシーの削除
- ロックアウト・パラメーターの編集
- パスワード期限切れメッセージの編集

## カスタム・パスワード・ポリシー

Sterling B2B Integrator のカスタム・パスワード・ポリシーは、パスワード・ポリシー・ルールを追加するセキュリティー機能です。これらの追加のパスワード・ルールは、安全性が低く破られやすいパスワードの使用を防止して、条件を満たしていないパスワードを拒否するのに役立ちます。

この機能を有効にするには、以下を実行する必要があります。

- プラグ・ポイントを通じてカスタム Java コードを実装します。有効化されたら、このプラグ・ポイントは、パスワード・ポリシーと関連付けられたシステム内のすべてのユーザー用に使用されます (これはグローバル設定です)。
- passwordPolicyExtensionImpl プロパティーを customer_overrides.properties ファイルに追加します。
- カスタム・パスワード・ポリシーをユーザー・アカウントに適用します。

デフォルト・パスワード・ポリシーの前にカスタム・パスワード・ポリシー拡張が適用されます。パスワードが複数のポリシー要件 (拡張クラスによって設定されている要件とデフォルト実装によって設定されている別の要件) に違反している場合は、拡張クラスから返されるエラー・メッセージのみがユーザーに表示されます。

## 例: パスワード・ポリシーの例

この例では、パスワード・ポリシーに使用できる設定を示します。

例えば、Test という名前のパスワード・ポリシーで、次のパスワード条件が指定されているとします。

- 有効期間は 10 日
- 最小長は 10 文字
- 最大長は 20 文字
- 少なくとも 2 つの特殊文字を含む必要がある
- ユーザーは初回ログイン時にデフォルト・パスワードを変更する必要がある
- 履歴に保存するパスワードの数

上記の例に従って、ユーザーにはシステム管理者からユーザー名とパスワードが付与されます。ユーザーは、付与されたユーザー名とパスワードを使用してログインしてから、このパスワードを変更することをプロンプトで求められます。ユーザーが指定した新しいパスワードが、10 文字以上、20 文字以下、および 2 つ以上の特殊文字を含んでいるという 3 つの条件のうち 1 つ以上に違反している場合は、パスワードの修正を求めるプロンプトがユーザーに表示されます。ユーザーの修正により、パスワード・ポリシーで規定されたすべての条件が満たされた場合は、その新しいパスワードが保存されて、ユーザーはアクセスを許可されます。各ユーザ

ー・アカウントには、1 つのパスワード・ポリシーしか関連付けることはできませんが、1 つのパスワード・ポリシーを複数のユーザー・アカウントに適用できます。

インターフェースでのパスワード・ポリシーの変更に加えて、ログインしようとしているユーザーのユーザー・アカウントがロックされるまでのログイン失敗回数を変更できます。

例えば、エラーとなる連続ログイン失敗回数が 3 回に設定されている場合に、間違ったパスワードを連続して 3 回入力した場合は、そのコンピューターからはログインできなくなります。その場合は、対象システムへのアクセスが可能な他のコンピューターを使用してログインできます。

## インストール環境のパスワードまたはパスフレーズ

インストール時に、Sterling B2B Integrator のインストール環境用のシステム・パスフレーズを作成します。このパスフレーズは、17 文字以上で構成される非常に複雑なストリングです。このシステム・パスフレーズは、システムを始動するため、および保護されたシステム情報にアクセスするために必要です。

このパスフレーズを更新または変更できる唯一の人物は、当ソフトウェアを作成/インストールした人物です。ご使用のパスフレーズを紛失したり忘れたりした場合は、システムを始動できなくなります。システム・パスフレーズを更新できる唯一のユーザーは、インストールを実行したユーザーです。

システム・パスフレーズはシステム側で保管されませんが、例外として Windows のインストール環境では、暗号化された状態で security.properties ファイルに保管されるため、システムを非対話式サービスとして実行しやすくなります。システム・パスフレーズは、他のプラットフォーム上では暗号化されない状態で security.properties ファイルに保管できるため、システムの始動時にコマンド・ラインでシステム・パスフレーズを入力する必要はありません。ただしその場合は、システム・パスフレーズを保護する手段は、オペレーティング・システムのファイル・アクセス制御のみになります。

## カスタム・パスワード・ポリシーのチェックリスト

カスタム・ポリシー・パスワードを実装できます。

次のチェックリストに従って、カスタム・パスワード・ポリシーを実装します。

| タスク | カスタム・パスワード・ポリシーのチェックリスト |
|---|---|
| 1 | テスト、ポリシー、および拡張機能のために <SI_Install_Dir> 内にディレクトリー構造を作成します。 |
| 2 | 拡張ディレクトリー内に Java クラスを作成します。 |
| 3 | パスワード・ポリシー (passwordPolicyExtensionImpl プロパティー) を実装する Java クラスを customer_overrides.properties ファイルで指定します。 |
| 4 | 実装クラスの jar をクラスパスに追加します。 |
| 5 | エラー・メッセージを定義します。 |

## 例 - カスタム・パスワード・ポリシー

この例では、カスタム・パスワード・ポリシー拡張を示します。

ここでは、カスタム・パスワード・ポリシー拡張の例を紹介します。

com.sterlingcommerce.woodstock.security.PasswordPolicyExtension インターフェースが次のようにシステムに追加されました。

```
public interface IPasswordPolicyExtension {
    /**
     * Implements extended validation on passwords and
returns null if password
     * validation is successful. If validation fails,
an error message key
     * that may be looked up in Login_*.properties* should
be returned.
     * @param password - The password string to validate
     * @param policyId - The PWD_POLICY.POLICY_NAME of
the policy associated with the user in case the extension needs
it.
     * @return String Return null if password validation
was successful, the error message key if password validation fails
     */
    public String validateNewPassword (String password,
String policyName);
}
```

このメソッドから NULL が返された場合は、パスワードが受け付けられたということです。NULL 以外が返された場合は、パスワードが有効ではなかったということです。

### 実装例

```
package test.policy.extension;
import java.util.regex.Pattern;
public class PwdPolExtnImpl implements com.sterlingcommerce.woodstock.security.IPasswordPolicyExtension
{
   public String validateNewPassword(String
pwd,
                  String policyName) {
           // Additional password validation checks
                  boolean match=Pattern.matches(".*[a-z].*",
pwd) && Pattern.matches(".*[A-Z].*", pwd) && (Pattern.matches(".*[0-9].*",
pwd) || Pattern.matches(".*[^A-Za-z0-9].*",pwd));
                  if (match==true) return null;
                  else return "nogood";
      }

}
```

## パスワード・ポリシーの検索

「管理」メニューから、パスワード・ポリシーを検索できます。

### このタスクについて

パスワード・ポリシーを検索するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「パスワード・ポリシー」を選択します。
2. 「パスワード・ポリシー」ページで、次のいずれかの操作を実行します。
   - 「検索」の「パスワード・ポリシー名」フィールドに、検索するパスワード・ポリシー名の一部または全体を入力して、「実行」をクリックします。「パスワード・ポリシー」ページに、検索条件に一致するすべてのパスワード・ポリシーが一覧表示されます。
   - 「リスト」の「英数字別」フィールドで、「すべて」を選択するか、検索するパスワード・ポリシー名の先頭文字を選択して、「実行」をクリックします。「パスワード・ポリシー」ページに、検索条件に一致するすべてのパスワード・ポリシーが一覧表示されます。

## パスワード・ポリシーの作成

パスワード・ポリシーを作成して、そのポリシーをユーザー・アカウントに割り当てることができます。パスワード・ポリシーをユーザー・アカウントに割り当てることは必須ではありませんが、セキュリティーを管理するのに役立ちます。

### このタスクについて

開始前に、次の情報が必要です。

| フィールド | 説明 |
|---|---|
| ポリシー ID | データベース内でこのパスワード・ポリシーを識別するID。 |
| ポリシー名 | このパスワード・ポリシーの参照時にユーザー・インターフェースに表示されるポリシー名。 |
| 有効な日数 | ユーザー・パスワードが有効である日数。デフォルト値である 0 の場合は、パスワードは永続的に有効になります。<br><br>1 から 999 までの値を指定した場合、この期間が経過すると、パスワードの変更を求めるプロンプトがユーザーに表示されます。有効期間の起算日は、パスワードがユーザー・アカウントに割り当てられた後に初めてユーザーがログインしたときです。 |
| 最小長 | パスワードの下限の長さ。必須。有効な値は任意の数字です。この値は 6 以上に設定する必要があります。デフォルト値は 6 です。どのポリシーも適用されていない場合は、6という最小長がシステムにより自動的に指定されます。 |
| 最大長 | パスワードの上限の長さ。必須。有効な値は任意の数字です。この値は「最小長」の値以上に設定する必要があります。デフォルト値は 28 です。 |
| 履歴に保持するパスワード数 | 1 ユーザーについてデータベース内の PWD_HISTORY 表に保持するパスワードの数。このパスワード数を超えると、最も古いパスワードがこの表から削除されて、そのユーザー用に再利用可能になります。デフォルト値は 0 です。 |

| フィールド | 説明 |
| --- | --- |
| パスワードに必ず特殊文字を含める | パスワードに 1 つ以上の特殊文字を含める必要があることを指定します。有効な値には、数字、大文字、!、@、#、$、%、^、&、* が含まれます。 |
| 初回のログイン試行時に必ずパスワードを変更する (Required password change on first login attempt) | 初回のログイン後にユーザーによるデフォルト・パスワードの変更が必要であることを指定します。このオプションを選択すると、ユーザーが初めてログインした後にパスワードの変更を要求するプロンプトが表示されます。 |

パスワード・ポリシーを作成するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「パスワード・ポリシー」を選択します。
2. 「新規パスワード・ポリシーの作成」の横にある「実行」をクリックします。
3. 「パスワード・ポリシー」ページで、「ポリシー **ID**」を入力します。
4. 「ポリシー名」を入力します。
5. 「有効な日数」を入力します。
6. 「最小長」を入力します。
7. 「最大長」を入力します。
8. 「履歴に保持するパスワード数」を入力します。
9. パスワードに特殊文字を含める必要があることを指定するには、「パスワードに必ず特殊文字を含める」チェック・ボックスを選択します。
10. ユーザーが初回のログイン試行時にパスワードを変更する必要があることを指定するには、「初回のログイン試行時に必ずパスワードを変更する (Required password change on first login attempt)」チェック・ボックスを選択します。
11. 「次へ **(Next)**」をクリックします。
12. このパスワード・ポリシーの設定内容を確認します。
13. 「終了」をクリックします。

## パスワード・ポリシーの編集

「管理」メニューから、パスワード・ポリシーを編集できます。

### このタスクについて

パスワード・ポリシーを編集するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「パスワード・ポリシー」を選択します。
2. 「検索」または「リスト」のオプションを使用して、編集するパスワード・ポリシーを探します。
3. 編集するパスワード・ポリシーの「編集」をクリックします。

4. 「パスワード・ポリシー設定」ページで、適切な変更を加えて、「次へ **(Next)**」をクリックします。
5. このパスワード・ポリシーの設定内容を確認します。
6. 「終了」をクリックします。

次のメッセージが表示されます。

```
The system update completed successfully.
```

## パスワード・ポリシーの削除

パスワード・ポリシーを削除すると、そのパスワード・ポリシーに関連付けられたユーザー・アカウントは引き続きログインできますが、そのユーザーはパスワードの変更を要求されなくなります。そのユーザーがパスワードを変更した場合でも、新しいパスワードの妥当性検査は行われません。

### このタスクについて

パスワード・ポリシーを削除するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「パスワード・ポリシー」を選択します。
2. 「検索」または「リスト」のオプションを使用して、削除するパスワード・ポリシーを探します。
3. 削除するパスワード・ポリシーの「削除」をクリックします。
4. 「確認」ページで、「削除」をクリックします。

次のメッセージが表示されます。

```
The system update completed successfully.
```

## ユーザー・パスワードの期限切れメッセージを表示するタイミングの変更

パスワードの期限切れが近づくと、そのことを通知するメッセージが管理コンソールのホーム・ページの「システム警告」セクションに表示されます。システム管理者は、ユーザーに通知する有効期限切れ前の日数を変更することができます。

### このタスクについて

このメッセージでは、パスワードの有効期限が何日後に切れるのかが示されます。毎日、この日数が 1 日ずつ減っていき、最終的にパスワードの有効期限日になると、パスワードを変更することを求めるプロンプトが表示されます。

システム管理者は、期限切れの何日前にこのメッセージを表示するのかを ui.properties.in ファイルで変更できます。すべての変更は、ui.properties ファイルではなく ui.properties.in ファイルで行う必要があります。ui.properties ファイルに変更を加えた場合は、その後にシステムを再始動すると、ui.properties ファイルに加えた変更内容が ui.properties.in ファイルによって上書きされるからです。

パスワードの期限切れメッセージを表示するタイミングを変更するには、以下を実行します。

### 手順

1. Sterling B2B Integrator を停止します。
2. /*install_dir*/install/properties にナビゲートします。
3. ui.properties.in ファイルを開きます。
4. MsgPwdExpires= 15 というエントリーを探します。
5. 15 を、ユーザー・パスワードの有効期間切れに先立ってメッセージが表示される新しい日数値に変更します。
6. ファイルを保存します。
7. *install_dir*/install/bin にナビゲートします。
8. **setupfiles.sh** と入力します。
9. Sterling B2B Integrator を再始動します。 ui.properties.in ファイルで加えた変更内容が ui.properties ファイルに適用されて、すべてのユーザー・アカウントに反映されます。

## ロックアウト後のパスワードのリセット

ロックアウトされた場合、別のコンピューターを使用してログインするか、ロックが期限切れになるまで 30 分待つか、システム管理者に連絡してロックを解除してもらうことができます。

### このタスクについて

ロックアウトされた場合の対処法は次のとおりです。

- 対象システムへのアクセスが可能な他のコンピューターを使用してログインします。
- 30 分間経過すると、ロックが時間切れになり、ロックされたコンピューターを使用して再びログインできるようになります。
- システム管理者に連絡して、「ロック・マネージャー」ページを通じてロックを解除するように依頼します。これにより、ロックされたコンピューターを使用して再びログインできるようになります。

## カスタム・パスワード・ポリシーのエラー・メッセージの定義

カスタム・パスワード・ポリシー拡張のエラー・メッセージを定義できます。

### このタスクについて

エラー・メッセージでは、ユーザーにパスワード・ルールの内容が通知されて、パスワードの変更が拒否された理由が表示されます。カスタム・パスワード・エラー・メッセージは、Login_*language_dir*.properties_*uniqueID*_ext ファイルに定義されます。ユーザー固有のメッセージ・テキストが指定されていない場合は、デフォルトのエラー・メッセージがユーザーに表示されます。

Login_*language_dir*.properties_*uniqueID*_ext ファイルは、デフォルト・システム・

コードの一部ではありません。このファイルは、システムの初期インストールの後に作成される必要があるとともに、ご使用の環境に合わせて設定される必要があります。

カスタム・パスワード・ポリシー拡張のエラー・メッセージを定義するには、以下を実行します。

### 手順

1. */install_dir*/install/properties/lang/*language_dir* ディレクトリーに移動します。ここで、*language_dir* はユーザーのロケールに対して設定された言語です (en、ja、fr など)。
2. Login_*language_dir*.properties_*uniqueID*_ext ファイルを編集します。 ここで、language_dir はユーザーのロケールに対して設定された言語であり、<filename> は新しいカスタム・パスワード拡張の固有 ID です。例えば、Login_en.properties_custompasswd_ext です。
3. カスタム拡張ファイルで設定されたエラー条件についてこのファイルにエントリーを追加して、ユーザーに表示する説明テキストを定義します。 例えば、nogood の値として、「パスワードには、少なくとも 1 つの小文字、1 つの大文字、および 1 つの数字または特殊文字が含まれている必要があります。」と指定します。
4. 保存してファイルを閉じます。

## customer_overrides.properties ファイルでのカスタム・パスワード・ポリシー拡張の指定

パスワード・ポリシー拡張を実装する Java クラスを指定できます。

### このタスクについて

カスタム実装をプラグインするには、customer_overrides.properties ファイル内の passwordPolicyExtensionImpl プロパティーで Java クラス名を指定する必要があります。

パスワード・ポリシー拡張を実装する Java クラスを指定するには、以下を実行します。

### 手順

1. インストール・ディレクトリーに移動します。
2. properties ディレクトリーに移動します。
3. customer_overrides.properties ファイルを編集します。
4. このファイルの末尾に passwordPolicyExtensionImpl プロパティーを追加して、拡張されたパスワード検証を実装する Java クラスの名前を入力します。例えば、security.passwordPolicyExtensionImpl=test.policy.extension.PwdPolExtnImpl と入力します。
5. 保存してファイルを閉じます。

## カスタム・パスワード・ポリシーのクラスパスへの実装クラス JAR の追加

カスタム・パスワード・ポリシーでは、実装クラス JAR をクラスパスに追加する必要があります。

### このタスクについて

拡張実装クラスは、次のようにしてコンパイルおよび JAR 化される必要があります。

### 手順

1. *SI_Install_Dir* にナビゲートします。
2. 次のコマンドを入力して、カスタム・クラス・ファイルをコンパイルします。

   ```
   javac -cp /SI_Install_Dir/jar/platform_ifcbase/1_3/platform_ifcbase.jar
   test/policy/extension/*.java
   ```

3. *SI_Install_Dir* 内から次のコマンドを実行して、JAR ファイルを作成します。

   `jar cf` *`any_filename`*`.jar` *`absolute_path_to_custom_class_file`*`.class` ここで、*`any_filename`*`.jar` は、新規作成される JAR ファイルの名前で、*`absolute_path_to_custom_class_file`*`.class` は、カスタム実装 Java クラス・ファイルの名前です。例: `jar cf userExit.jar test/policy/extension/PwdPolExtnImpl.class`

4. *SI_Install_Dir*/bin ディレクトリーにナビゲートします。
5. 次のコマンドを入力して、クラスパスに新規作成された JAR を追加します。

   ```
   ./install3rdParty.sh userExit 1_0 -j
   path_to_jar_that_was_created_in_step3
   ```

   例: `./install3rdParty.sh userExit 1_0 -j` *`SI_Install_Dir`*`/userExit.jar`

# LDAP 認証

## Sterling B2B Integrator 用の認証ツールとしての Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) は、情報ディレクトリーに保管された情報にアクセスするために使用される一連のプロトコルです。この情報ディレクトリーは、LDAP ディレクトリーと呼ばれます。

LDAP ディレクトリーはデータベースですが、リレーショナル・データベースではありません。このデータベースは、ネットワーク上の複数のサーバーに分散された情報を管理するために使用され、読み取りパフォーマンスを高めるために最適化されています。

LDAP を使用すると、外部ユーザー・アカウントの認証を LDAP ディレクトリーに委任して、自社内の他のアプリケーション用に使用されているのと同じセキュリ

ティー情報を使用して認証を実行できます。自社で LDAP を既に導入済みの場合は、既存の LDAP ディレクトリーを使用できます。

ユーザー・アカウント認証には LDAP アダプターは必要ありません。LDAP アダプターは、JNDI (Java Naming and Directory Interface) を使用してローカルまたはリモートの LDAP サーバーと通信するために、ビジネス・プロセスとともに使用されます。

ご使用の LDAP サーバーが動作していない場合は、内部アカウントを持つユーザーはアクセスできますが、外部アカウントを持つユーザーは LDAP サーバーが復帰するまでアクセスできません。

Sterling B2B Integrator で LDAP を構成するには、以下が必要です。

- LDAP に関する知識
- ユーザー情報が格納されたインストール済みおよび構成済みの LDAP サーバーへのアクセス
- LDAP サーバーの場所情報
- (SSL 用) 鍵ストアとトラストストアにインストールされたセキュリティー証明書
- LDAP サーバーを通じて認証される各ユーザーの外部ユーザー・アカウント
- (SSL 用) 鍵ストアとトラストストアの場所情報

## 例: LDAP 認証の構成パラメーター

次の例では、LDAP 認証の構成パラメーターを示しています。

次の例では、LDAP 認証の構成パラメーターを示しています。

```
## GIS/LDAP Authentication configuration
## optional ssl (jsse) java system properties for locating and using
## the trustStore and the keyStore
## one set of keystore and truststore properties for all LDAP configuration.
# LDAP_SECURITY_TRUSTSTORE=/home/applications/properties/cacerts
# LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
# LDAP_SECURITY_KEYSTORE=/home/applications/properties/keystore
# LDAP_SECURITY_KEYSTORE_PASSWORD=password
#########################################################################
#
# GIS Authentication Configuration
#
#########################################################################
authentication_0.className=com.sterlingcommerce.woodstock.security
.GISAuthentication
authentication_0.display_name=GIS Authentication
#########################################################################
#
# For additional LDAP Server Authentication Configuration,
# copy-paste the following set of properties and uncomment all properties
# that start with "authentication_<number>". Replace the <number>
# tag with the additional number for the authenticationmethod. For example,
# if the last authentication method is "authentication_0", then you should
# replace the <number> tag with "1" for your next new LDAP authentication
# method.
# Then you have to change each property with the properLDAP server information.
#
# You can comment out or leave blank the "authentication_<number>
# .security_protocol"
# property if you are not going to use SSL for the security protocol.
#
```

```
# The authentication_1 LDAP authentication propertieswould be replaced if
# the customer already used LDAP authentication as configuredin security
# .properties.
#
#########################################################################
#########################################################################
#
# LDAP Server <number> Authentication Configuration
#
#########################################################################
# authentication_<number>.className=com.sterlingcommerce.woodstock.security
# .LDAPAuthentication
# authentication_<number>.display_name=LDAP Serveragrona <number>
## enable ldap authentication  (true, false) default=false
# authentication_<number>.enabled=true
## jndi parameters for ldap connections
# authentication_<number>.jndi_factory=com.sun.jndi.ldap.LdapCtxFactory
# authentication_<number>.server=acme.inc.com
# authentication_<number>.port=636
# authentication_<number>.security_type=simple
# authentication_<number>.principle=cn=Manager,dc=acme,dc=inc,dc=com
# authentication_<number>.credentials=SecretPassword
## comment out or leave as blank on this property if the server is not
## going to use SSL for the security protocol.
# authentication_<number>.security_protocol=ssl
## search parameters for user password
# authentication_<number>.password_attribute=userPassword
# authentication_<number>.search_root=dc=acme,dc=inc,dc=com
# authentication_<number>.search_filter=(uid=<userid>)
# authentication_<number>.with_user_bind=falseBelow the ##LDAP Authentication
```

## LDAP 認証構成のチェックリスト

Sterling B2B Integrator で LDAP を構成できます。

次のチェックリストに従って、Sterling B2B Integrator で LDAP を構成してください。

| タスク | **LDAP** 構成のチェックリスト |
|---|---|
| 1 | 次のいずれかのモードで LDAP を構成します。<br>• パスワード比較モード<br>• パスワード・バインディング・モード |
| 2 | Sterling B2B Integrator で LDAP を構成します。 |
| 3 | LDAP 構成を確認します。 |
| 4 | オプション。 LDAP パスワードを暗号化します。 |

## パスワード・バインディング・モードでの LDAP の構成

外部アカウントから「ユーザー **ID**」と「パスワード」を入力することで、LDAP をパスワード・バインディング・モードで構成できます。

### このタスクについて

LDAP をパスワード・バインディング・モードで構成するには、以下を実行します。

### 手順

外部ユーザー・アカウントの「ユーザー **ID**」と「パスワード」を入力します。 システムは次の操作を実行します。

- 必要なクエリーの実行を可能にする資格情報を使用して LDAP リポジトリーへのバインドを試行します。
- 適切なユーザー ID を使用して LDAP ディレクトリー内でそのユーザーを検索します。
- そのユーザーの識別名 (DN) を LDAP ディレクトリーから取得します。
- そのユーザーの DN とパスワードを使用して LDAP リポジトリーへのバインドを試行します。
- 成功 - システムはユーザーとして LDAP リポジトリーにバインドします。
- 失敗 - システムはユーザーとして LDAP リポジトリーにバインドできません。

## パスワード比較モードでの LDAP の構成

LDAP をパスワード比較モードで構成できます。

### このタスクについて

LDAP をパスワード比較モードで構成するには、以下を実行します。

### 手順

1. 外部ユーザー・アカウントの「ユーザー **ID**」と「パスワード」を入力します。
2. システムは、必要なクエリーの実行を可能にする資格情報を使用して LDAP リポジトリーへのバインドを試行します。
3. システムは、適切なユーザー ID を使用してそのユーザーを LDAP ディレクトリー内で検索します。
4. システムは、そのユーザーのパスワードを LDAP ディレクトリーから取得します。
5. システムは、ユーザーによって入力されたパスワードを LDAP ディレクトリーから取得したパスワードと比較します。これらのパスワードが一致した場合は、ユーザーは認証されて、システムへのアクセスを許可されます。これらのパスワードが一致しない場合は、ユーザーは認証されずに、アクセスを許可されません。

## Sterling B2B Integrator での LDAP の構成

Sterling B2B Integrator が LDAP を使用するように構成するには、authentication_policy.properties.in ファイルを編集する必要があります。customer_overrides.properties ファイルを使用して、パッチのインストールによって上書きできないプロパティー値を設定することもできます。

### このタスクについて

LDAP 認証を構成するには、以下を実行します。

## 手順

1. Sterling B2B Integrator を停止します。
2. インストール・ディレクトリーに移動します。
3. properties ディレクトリーに移動します。
4. authentication_policy.properties.in ファイルを開きます。
5. authentication_policy.properties.in ファイルで、## GIS/LDAP Authentication configuration というエントリーを探します。
6. ##GIS/LDAP Authentication 構成エントリーの下で、LDAP パラメーターに次の変更を加えます。

| パラメーター | 説明 | 初期値 | 変更後の値 |
|---|---|---|---|
| #LDAP_SECURITY_TRUSTSTORE | ローカル・トラストストアへのパス。LDAP で必須となる証明書を、トラストストアに格納しておく必要があります。取引パートナーから取得した証明書を使用することはできません。オプション。このパラメーターは、SSL を使用している場合にのみ使用します。 | Inactive path | ローカル・トラストストアへの絶対パス。 |
| #LDAP_SECURITY_TRUSTSTORE_PASSWORD | トラストストアにアクセスするためのパスワード。オプション。このパラメーターは、SSL を使用している場合にのみ使用します。 | changeit | ローカル・トラストストアにアクセスするためのパスワード。 |
| #LDAP_SECURITY_KEYSTORE | ローカル鍵ストアへのパス。LDAP で必須となる証明書を、鍵ストアに格納しておく必要があります。取引パートナーから取得した証明書を使用することはできません。オプション。このパラメーターは、SSL を使用している場合にのみ使用します。 | Inactive path | ローカル鍵ストアへの絶対パス。 |
| #LDAP_SECURITY_KEYSTORE_PASSWORD | 鍵ストアにアクセスするためのパスワード。オプション。このパラメーターは、SSL を使用している場合にのみ使用します。 | password | ローカル鍵ストアにアクセスするためのパスワード。 |

| パラメーター | 説明 | 初期値 | 変更後の値 |
| --- | --- | --- | --- |
| #authentication_<number>.enabled | LDAP を使用可能または使用不能にします。<br><br>False – この認証ホストから作成されたすべてのユーザーは無効になります (ログインできなくなります)。<br><br>True – 各ユーザーは内部アクセスまたは外部アクセスが可能ですが、各ユーザー ID は一意であるため、両方のアクセスはできません。この値は、内部認証用の場合はチェックされません。 | False | True |
| #authentication_<number>.jndi_factory | LDAP サービス・プロバイダーの初期コンテキストを作成するファクトリー・クラスのクラス名。これは、JDK に付属している標準のコンテキスト・ファクトリーです。 | com.sun.jndi.ldap.LdapCtxFactory | 変更なし |
| #authentication_<number>.server | LDAP サーバーのホスト名を指定する URL。 | Inactive path | ローカル LDAP ホスト URL。 |
| #authentication_<number>.port | LDAP サーバーのポート番号。 | | |
| #authentication_<number>.security_type | プロバイダーで使用する認証方式。システムでは、簡易認証のみがサポートされています。 | simple | 変更なし |
| #authentication_<number>.principle | システムでのクエリー実行を可能にする、認証するプリンシパルの ID。このパラメーターは、LDAP ASN.1 バインド要求内の名前コンポーネントです。 | cn=Manager, dc=amr, dc=stercomm, dc=com | ローカル命名情報。 |
| #authentication_<number>.credentials | システムでのクエリー実行を可能にする、LDAP プリンシパル用に LDAP リポジトリー内で設定されたパスワード。 | SecretPassword | ローカル・プリンシパルに割り当てられているローカル・パスワード。 |
| #authentication_<number>.security_protocol | 使用するプロバイダーのセキュリティー・プロトコルを指定するオブジェクト。 | SSL | 変更なし。このパラメーターは、SSL を使用しないことを選択した場合は表示されません。 |

| パラメーター | 説明 | 初期値 | 変更後の値 |
| --- | --- | --- | --- |
| #authentication_<br><number>.<br>password_attribute | ユーザー・パスワードが含まれた LDAP 属性の名前。<br><br>このパラメーターが使用されるのは、<br><br>#LDAP_<br>AUTHENTICATE_<br>WITH_USER_BIND<br>が false に設定されている場合のみです。 | userPassword | パスワードが含まれたローカル属性。 |
| #authentication_<br><number>.<br>search_root | ユーザー・クエリーのベースとなるルートを指定するオブジェクト。 | dc=amr, dc=stercomm,<br>dc=com | ローカル検索パス。 |
| #authentication_<br><number>.search_filter | 検索で使用するテンプレートを指定するオブジェクト。<userid> の値は、ユーザーから認証を要求された時に、そのユーザーのユーザー ID で動的に置換されます。 | (uid=<userid>) | Windows Active Directory サーバーでは<br>(sAMAccount<br>Name=<userid>) |
| #authentication_<br><number>.<br>with_user_bind | 成功したバインドに従ってユーザーを認証するのかどうかを指定します。<br><br>False – システムは、ユーザー・パスワードの値を LDAP サーバーから取得して、入力されたユーザー資格情報と比較します。<br><br>True – システムは、ユーザーの識別名および入力された資格情報を使用して LDAP サーバーにバインドします。正常にバインドできた場合は、認証に合格したことになります。 | false | ユーザー・バインドを使用して認証する場合は、true に変更します。 |

7. authentication_policy.properties.in ファイルを保存します。
8. /*install_dir*/install/bin/setupfiles.sh (UNIX) または ¥*install_dir*¥install¥bin¥setupfiles.cmd (Windows) と入力して、authentication_policy.properties.in ファイルから authentication_policy.properties ファイルに対して LDAP エントリーを更新します。
9. Sterling B2B Integrator を開始します。

   authentication_policy.properties ファイルに加えた変更が適用されて、LDAP サーバーを使用したユーザー認証を開始できるようになります。

始動後に、システムは authentication_policy.properties ファイルから LDAP サーバーを識別します。システムは、外部ユーザーをユーザーのログイン時に認証します。

## LDAP 構成の確認

Sterling B2B Integrator で LDAP を正しく構成されていることを確認するには、「ユーザー認証」で Authentication.log ファイルを参照して、システムで現在の LDAP 構成が受け入れられていることを確認してください。

### このタスクについて

LDAP ディレクトリーへの接続に問題がある場合や、LDAP 認証を正常に実行できない場合は、Authentication.log ファイル内の DEBUG ログ・ステートメントを確認して問題をトラブルシューティングしてください。Authentication.log ファイルには、成功したか失敗したかにかかわらず、すべてのログイン試行が記録されます。

## LDAP パスワードの暗号化

プロパティー・ファイル内の LDAP 関連パスワードが見えないようにするには、それらのパスワードを customer_overrides.properties ファイル内で暗号化します。

### このタスクについて

次のパラメーター (プロパティー) を使用して、customer_overrides.properties ファイル内で LDAP パスワードを暗号化できます。

| パラメーター/プロパティー | 説明 |
|---|---|
| authentication_policy.authentication_1.credentials | このパラメーターまたはプロパティーは、LDAP インスタンスにアクセスするために必要なプリンシパル・パスワードを制御します。セキュリティーとアクセスを制御するパスワードを非暗号化テキストで公開してはならないため、このパスワードを保護する必要があります。 |
| authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD | このパラメーターまたはプロパティーは、LDAP 接続を保護するために使用されるトラストストア (JKS フォーマット) のパスワードを制御します。このトラストストアは暗号化されたファイルであるため、この JKS のパスフレーズを指定して、このトラストストアへのアクセスを可能にする必要があります。 |
| authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD | クライアント・ベースの SSL 認証を使用して特定の LDAP インスタンスへの接続を保護している場合は、このパラメーターまたはプロパティーはそのパスワードを制御します。 |

LDAP パスワードを暗号化するには、以下を実行します。

### 手順

1. bin ディレクトリーに移動します。
2. encrypt_string.[sh/cmd] を使用して、暗号化するプロパティー/パラメーターの実際の値を指定します。
3. customer_overrides.properties ファイル内のパラメーター/プロパティーを更新して、次のエントリーを割り当てます。bin/encrypt_string.sh (または .cmd) を使用して、すべての <ENCVAL> を、そのプロパティーのコメント化された非暗号化ストリングを暗号化した値に置換します。次に例を示します。

```
authentication_policy.LDAP_SECURITY_TRUSTSTORE=&INSTALL_DIR;/../
woodstock2/com/sterlingcommerce/woodstock/security/units/cacerts
# non-encrypted
#authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
# encrypted
authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD=<ENCVAL>
authentication_policy.LDAP_SECURITY_KEYSTORE=&INSTALL_DIR;/../woodstock2/
com/sterlingcommerce/woodstock/security/units/keystore
# non-encrypted
#authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD=password
# encrypted
authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD=<ENCVAL>
authentication_policy.authentication_2.display_name=LDAP Server agrona 2
authentication_policy.authentication_2.enabled=true
authentication_policy.authentication_2.jndi_factory=com.sun.jndi.ldap.LdapCtxFactory
authentication_policy.authentication_2.server=agrona.sci.local
authentication_policy.authentication_2.port=18100
authentication_policy.authentication_2.security_type=simple
authentication_policy.authentication_2.principle=cn=Manager,dc=amr,dc=stercomm,dc=com
# non-encrypted
#authentication_policy.authentication_2.credentials=Sterling
# encrypted
authentication_policy.authentication_2.credentials=<ENCVAL>
authentication_policy.authentication_2.security_protocol=ssl
authentication_policy.authentication_2.password_attribute=userPassword
authentication_policy.authentication_2.search_root=dc=amr,dc=stercomm,dc=com
authentication_policy.authentication_2.search_filter=(uid=<userid>)
authentication_policy.authentication_2.with_user_bind=false
authentication_policy.authentication_2.className=com.sterlingcommerce.woodstock.security
.LDAPAuthentication
```

## ユーザー・ニュース

### ユーザー・ニュース

ユーザー・ニュース機能を使用すると、「管理コンソール・ホーム」ページにメッセージを投稿できます。ユーザー・ニュースを通じて、ユーザーに変更事項を通知したり、重要なイベントやタスクについて事前にユーザーに知らせたりできます。

メッセージを投稿できる対象は次のとおりです。

- すべてのユーザー
- 特定のユーザー
- 複数のユーザー

ニュース項目は、発効日と満了日に基づいて表示されます。メッセージを次のタイプとして設定することもできます。

| メッセージ・タイプ | シンボル | 説明 |
|---|---|---|
| 通知 |  | 一般的な優先度または低い優先度の告知情報を提供します。 |
| 警告 |  | 高い優先度の告知情報を提供します。 |

ユーザー・ニュース・メッセージを作成するには、アカウントに対する書き込みの許可を持っている必要があります。古いメッセージを削除すると、ストレージ要件が低減されるとともに、特定のメッセージを取得するために要する労力が軽減されます。

ユーザー・ニュースを対象にした作業は次のとおりです。

- 特定ユーザー向けのユーザー・ニュース・メッセージの作成
- すべてのユーザー向けのユーザー・ニュース・メッセージの作成
- ユーザー・ニュース・メッセージの検索
- ユーザー・ニュース・メッセージの編集
- ユーザー・ニュース・メッセージの削除

## すべてのユーザー向けのユーザー・ニュース・メッセージの作成

「管理」メニューから、すべてのユーザー向けのユーザー・ニュース・メッセージを作成できます。

### このタスクについて

開始前に、次の情報を把握する必要があります。

| フィールド | 説明 |
|---|---|
| タイプ (Type) | 作成するメッセージのタイプ。有効な値は「通知」と「警告」です。 |
| 件名 | 作成するメッセージの件名。 |
| メッセージ | 作成するメッセージの本文。 |

### 手順

1. 「管理メニュー」から、「アカウント」 > 「ユーザー・ニュース」を選択します。
2. 「新規メッセージ」の横にある「実行」をクリックします。
3. 「タイプ」を入力します。
4. 「件名」を入力します。
5. 「メッセージ」を入力します。
6. 「次へ **(Next)**」をクリックします。
7. 「すべてのユーザー」を選択して、「次へ **(Next)**」をクリックします。
8. メッセージの「有効開始日付」 (yyyy-mm-dd) を入力します。
9. メッセージの「有効期限」 (yyyy-mm-dd) を入力します。
10. 「次へ **(Next)**」をクリックします。

11. このニュース・メッセージの設定内容を確認します。
12. 「終了」をクリックします。

## 特定ユーザー向けのユーザー・ニュース・メッセージの作成

「管理」メニューから、特定ユーザー向けのユーザー・ニュース・メッセージを作成できます。

### このタスクについて

開始前に、次の情報を把握する必要があります。

| フィールド | 説明 |
|---|---|
| タイプ (Type) | 作成するメッセージのタイプ。有効な値は「通知」と「警告」です。 |
| 件名 | 作成するメッセージの件名。 |
| メッセージ | 作成するメッセージの本文。 |

### 手順

1. 「管理メニュー」から、「アカウント」 > 「ユーザー・ニュース」を選択します。
2. 「新規メッセージ」の横にある「実行」をクリックします。
3. 「タイプ」を入力します。
4. 「件名」を入力します。
5. 「メッセージ」を入力します。
6. 「次へ **(Next)**」をクリックします。
7. 「選択済みユーザー」を選択します。
8. このメッセージを受信する各ユーザーの名前を選択します。
9. 「次へ **(Next)**」をクリックします。
10. メッセージの「有効開始日付」 (yyyy-mm-dd) を入力します。
11. メッセージの「有効期限」 (yyyy-mm-dd) を入力します。
12. 「次へ **(Next)**」をクリックします。
13. このニュース・メッセージの設定内容を確認します。
14. 「終了」をクリックします。

## ユーザー・ニュース・メッセージの検索

「管理」メニューから、ユーザー・ニュース・メッセージを検索できます。

### このタスクについて

ユーザー・ニュース・メッセージを検索するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「ユーザー・ニュース」を選択します。
2. 次のいずれかの検索オプションを選択します。

| ユーザー・ニュースの検索オプション | アクション |
| --- | --- |
| ユーザー ID 別 | 「すべて」を選択するか、リストから特定のユーザーを選択します。 |
| 件名別 (by Subject) | メッセージ・テキストの一部を入力します。 |
| 有効開始日付別 (by Effective Date Range) | 日付範囲 (mm/dd/yyyy) を入力します。 |

3. 「実行 **(Go!)**」をクリックします。 「ユーザー・ニュース」ページに、検索条件に一致するすべてのメッセージが一覧表示されます。

## ユーザー・ニュース・メッセージの編集

「管理」メニューから、ユーザー・ニュース・メッセージを編集できます。

### このタスクについて

ユーザー・ニュース・メッセージを編集するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「ユーザー・ニュース」を選択します。
2. 編集するユーザー・ニュース・メッセージを検索します。
3. 編集するユーザー・ニュース・メッセージの「編集」をクリックします。
4. 必要に応じて、メッセージのタイプ、件名、およびメッセージを変更します。
5. 「次へ **(Next)**」をクリックします。
6. 必要に応じて、このメッセージを受信させるユーザーを変更して、「次へ **(Next)**」をクリックします。
7. 必要に応じて、メッセージの「有効開始日付」 (yyyy-mm-dd) を変更します。
8. 必要に応じて、メッセージの「有効期限」 (yyyy-mm-dd) を変更します。
9. 「次へ **(Next)**」をクリックします。
10. このニュース・メッセージの設定内容を確認します。
11. 「終了」をクリックします。

## ユーザー・ニュース・メッセージの削除

「管理」メニューから、ユーザー・ニュース・メッセージを削除できます。

### このタスクについて

ユーザー・ニュース・メッセージを削除するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「アカウント」 > 「ユーザー・ニュース」を選択します。
2. 削除するユーザー・ニュース・メッセージを検索します。
3. 削除するニュース・メッセージの「削除」をクリックします。

4. このニュース・メッセージの設定内容を確認します。
5. 「削除」をクリックします。 次のメッセージが表示されます。

```
The system update completed successfully.
```

# ドキュメント暗号化

## ドキュメント暗号化機能の概要

ドキュメント暗号化は、従来のファイル許可とデータベース許可に加えて追加のセキュリティー層を構成する、Sterling B2B Integrator に付属の機能です。Sterling B2B Integrator と統合した Sterling File Gateway では、保存データを保護するために同じドキュメント暗号化機能が使用されます。

Sterling File Gateway は、異なるプロトコル、ファイル命名規則、およびファイル形式を使用しているパートナー間でファイルを安全に転送するためのアプリケーションです。

ドキュメント暗号化機能の目的は、保存データをスヌープ (盗み見) から保護することです。この機能を使用すると、データベースおよびファイル・システム、またはそのいずれかに保管されたペイロード・データを暗号化できます。この機能のもう 1 つの目的は、システム外部の何者かがデータベースやファイル・システムに直接アクセスすることでペイロード・データを参照することを防止することです。

ドキュメント暗号化の重要な特徴は次のとおりです。

- インストール時のデフォルト構成では、暗号化は行われません。ドキュメントを暗号化するには、この機能を有効にする必要があります。
- この機能はいつでも有効にできますが、暗号化を有効にした後に受信されるドキュメントのみが暗号化されます。
- この機能を有効にすると、システム全体にわたるすべてのペイロード・データが暗号化の対象になります。
- ドキュメントのペイロード・データのみが暗号化されて、メタデータは暗号化されません。
- 暗号化と暗号化解除には同じ暗号化鍵が使用されます。
- システムでは、事前定義済みの証明書 (doccrypto) を使用してドキュメントが暗号化されます。この証明書とは異なるシステム証明書を作成できます。その場合は、customer_overrides.properties ファイル内の CERT_NAME の値を更新する必要があります。

暗号化を有効にするとパフォーマンスが影響を受けますが、パフォーマンスへの影響度はユーザーごとに異なり、影響度を左右する要因としては、使用しているハードウェア、処理対象のドキュメントの数とサイズ、および処理時間の相対的な量 (使用しているサーバーでドキュメントの保存と取得を実行するために費やされる処理時間とそれ以外のアクティビティーに費やされる処理時間との対比) が挙げられます。

## ドキュメント暗号化用の暗号鍵

データベース内やファイル・システム内のドキュメントの暗号化と暗号化解除には、同じ暗号鍵が使用されます。デジタル証明書を使用してこれらの鍵が生成および暗号化されて、システム・パスフレーズを使用してデジタル証明書が暗号化されます。

ドキュメント暗号化によってドキュメントあたり 1 つの鍵が作成されて、この鍵はそのドキュメントとともにメタデータの一部として保管されます。デジタル証明書は、他のシステム証明書と同じように保管されます。

システムでは、事前定義済みの証明書 (doccrypto) を使用して、ドキュメントを暗号化するために使用される鍵を生成および暗号化します。この証明書とは異なるシステム証明書を作成できます。その場合は、customer_overrides.properties ファイル内の CERT_NAME の値を更新する必要があります。

## ドキュメント暗号化用の異なる証明書の割り当て

システムでは、事前定義済みの証明書 (doccrypto) を使用してドキュメントが暗号化されます。以前の証明書の期限が切れた場合などに、別のシステム証明書を作成して文書の暗号化に使用することができます。その場合は、customer_overrides.properties ファイル内の CERT_NAME の値を更新する必要があります。

### このタスクについて

注意**:** 以前のシステム証明書を削除したり名前変更したりしないでください。以前の証明書は、その証明書で暗号化した文書を暗号化解除する場合に必要になります。このような文書は新しいシステム証明書を使用して暗号化されてはいないため、新しいシステム証明書では暗号化解除できません。

この手順を開始する前に、次のことを実行する必要があります。

- 新しい証明書を生成します。
- この証明書の名前を確認します。

CERT_NAME の値を更新するには、以下を実行します。

### 手順

1. install ディレクトリーに移動します。
2. properties ディレクトリーに移動します。
3. customer_overrides.properties ファイルを開きます。
4. ファイルに以下の行を追加します。

   ```
   security.CERT_NAME=name_of_new_system_certificate
   ```

5. customer_overrides.properties ファイルを保存して閉じます。
6. Sterling B2B Integrator を停止して再始動します。

## ファイル・システム内およびデータベース内のファイルに対するドキュメント暗号化の有効化

properties ディレクトリーからファイル・システム内やデータベース内のドキュメントを暗号化できます。

### このタスクについて

ファイル・システム内やデータベース内のドキュメントを暗号化するには、以下を実行します。

### 手順

1. install ディレクトリーに移動します。
2. properties ディレクトリーに移動します。
3. customer_overrides.properties ファイルを開きます。
4. ファイルに以下の行を追加します。

   ```
   security.ENC_DECR_DOCS=ENC_ALL
   ```
5. customer_overrides.properties ファイルを保存して閉じます。
6. Sterling B2B Integrator を停止して再始動します。

## データベース内のドキュメントに対するドキュメント暗号化の有効化

install ディレクトリーからデータベース内のドキュメントを暗号化できます。

### このタスクについて

データベース内のドキュメントを暗号化するには、以下を実行します。

### 手順

1. install ディレクトリーに移動します。
2. properties ディレクトリーに移動します。
3. customer_overrides.properties ファイルを開きます。
4. ファイルに以下の行を追加します。

   ```
   security.ENC_DECR_DOCS=ENC_DB
   ```
5. customer_overrides.properties ファイルを保存して閉じます。
6. Sterling B2B Integrator を停止して再始動します。

## ファイル・システム内のドキュメントに対するドキュメント暗号化の有効化

install ディレクトリーからファイル・システム内のドキュメントを暗号化できます。

### このタスクについて

ファイル・システム内のドキュメントを暗号化するには、以下を実行します。

### 手順

1. install ディレクトリーに移動します。
2. properties ディレクトリーに移動します。
3. customer_overrides.properties ファイルを開きます。
4. ファイルに以下の行を追加します。

   ```
   security.ENC_DECR_DOCS=ENC_FS
   ```
5. customer_overrides.properties ファイルを保存して閉じます。
6. Sterling B2B Integrator を停止して再始動します。

## ドキュメントに対するドキュメント暗号化の無効化

properties ディレクトリーからドキュメント暗号化を無効にできます。

### このタスクについて

インストール時のデフォルト構成では、暗号化は行われません。

ドキュメント暗号化を無効にするには、以下を実行します。

### 手順

1. install ディレクトリーに移動します。
2. properties ディレクトリーに移動します。
3. customer_overrides.properties ファイルを開きます。
4. ENC_DECR_DOCS の値を NONE に変更します。 次に例を示します。

   ```
   security.ENC_DECR_DOCS=NONE
   ```
5. customer_overrides.properties ファイルを保存して閉じます。
6. Sterling B2B Integrator を停止して再始動します。

# 証明書

## デジタル証明書

IBM 鍵管理ユーティリティー (iKeyman) を使用して、デジタル証明書を管理します。

システムでは、次のタイプのデジタル証明書が使用されます。

- CA 証明書とトラステッド証明書 - システム側に秘密鍵が保有されていないデジタル証明書。これらの証明書は、標準の DER フォーマットで保管されています。
- システム証明書 - システム側に秘密鍵が保有されているデジタル証明書。これらの証明書は、秘密鍵とともにセキュア・フォーマットで保管されています。

以下では、デジタル証明書の使用法に関する基本的な情報を示しています。

- セキュア・ドキュメントの受け渡しを行うすべての組織は、証明書を保有している必要があります。証明書は、iKeyman を使用して生成することも、外部で生成することもできます。 iKeyman について詳しくは、 70 ページの『IBM 鍵管理ユーティリティー (iKeyman)』を参照してください。

- 署名および暗号化されたドキュメントを受け渡しする相手である取引パートナーのすべての取引プロファイルは、証明書を保有している必要があります。
- 組織や取引プロファイルは、同時に複数のアクティブな証明書を保有することはできません。二重証明書の場合は、組織は、署名用の証明書と暗号化用の証明書で構成される 1 つのアクティブな証明書ペアを保有できます。
- 組織や取引プロファイルは、署名および暗号化されたドキュメントを正常に受け渡しするために、アクティブな証明書を保有している必要があります。
- 組織や取引プロファイルは、複数の有効な証明書を保有できます。
- 証明書を使用して、あらゆる伝送手段で送信するドキュメントに署名できます。
- 証明書の鍵の長さは、取引パートナーの証明書の鍵の長さと同じである必要はありません。
- 証明書の有効期間を設定する前に、「Microsoft PKI Quick Guide」に記載されているベスト・プラクティスの推奨事項を参照して適用することをお勧めします。証明書を使用する際のベスト・プラクティスの推奨事項については、http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html.

### サポートされているデジタル証明書

Sterling B2B Integrator は、バージョン 3 X.509 のデジタル証明書をサポートしています。デジタル証明書は、自己署名のものでも CA 署名のものでもかまいません。

- 自己署名証明書は、その証明書内の公開鍵に対応する秘密鍵で署名されたデジタル証明書であり、発行者がその証明書内の公開鍵に対応する秘密鍵を持っていることを証明します。
- CA 署名証明書は、認証局で保持されている鍵を使用して署名されたデジタル証明書です。CA は通常、証明書を発行する前に証明書の要求者を検証して、要求者が本当にその証明書で示されている証明書保有者であるかどうかを確認します。

## CA 証明書

CA 証明書とは、認証局 (CA) によって発行されたデジタル証明書のことです。CA は、トラステッド・ルートのトラステッド証明書を証明します。トラステッド・ルートは、証明書内の信頼チェーンが構成される基盤です。

CA ルートを信頼するということは、その CA によって発行されたすべての証明書を信頼するということです。CA ルートを信頼しないことを選択した場合は、Sterling B2B Integrator は、その CA によって発行されたどの証明書も信頼しません。

CA 証明書には、秘密鍵に対応する公開鍵が含まれています。CA は秘密鍵を所有しており、その CA で発行する証明書に秘密鍵を使用して署名します。トラステッド証明書を検証するには、まず CA 証明書をチェックインする必要があります。

一般的な CA のルート証明書は、Sterling B2B Integrator に付属している JVM 内の Java 鍵ストア (JKS) に格納されています。これによりユーザーは、これらの証明書を CA の Web サイトから検索して取得するよりも簡単に、認証局に基づいた信頼関係を構築できます。

CA 証明書は、トラステッド証明書とは分けて当製品内で保管されています。

ユーザー・インターフェースから、以下のいずれかのソースから得られた CA ルート証明書をチェックインできます。

- JKS 鍵ストア内にある、Sterling B2B Integrator に付属する一般的な CAルート証明書。
- 証明書とトラステッド証明書のみが認識されます。証明書と秘密鍵は UI には表示されません。
- 取引パートナーからインポートされた SSL 証明書。
- 外部から取得された他の証明書。

ご使用のサイトのセキュリティー・ポリシーに基づいて、JKS 鍵ストア内の CA 証明書をコンソールからチェックインすることもできます。CA 証明書は公開ドキュメントですが、誰が CA 証明書を追加する権限を持っているのかについて注意する必要があります。何者かが不正な目的のために、偽のエンド・ユーザー証明書を証明するために偽の CA 証明書を追加する可能性があるからです。

### CA 証明書名

CA 証明書名は、その証明書のコンテンツの一部ではありません。 CA 証明書名は、発行者の相対識別名 (RDN) とその証明書のシリアル番号に基づいて作成されます。ただし JKS 鍵ストア内の証明書には、任意の文字列を使用した名前が付けられています。

証明書名はシステム・データベースに格納されて、GUI でその証明書を表す別名として使用されるため、ユーザーのファイル命名規則に基づいて、CA 証明書名を短めの名前やわかりやすい名前に変更することをお勧めします。証明書の名前変更は、その証明書のチェックイン時や編集時に行うことができます。

## 自己署名デジタル証明書および CA 署名デジタル証明書の利点

ニーズによって、自己署名証明書と CA 署名デジタル証明書には長所と短所があります。

お客様の組織や取引パートナーが、自己署名証明書を生成するのか CA から署名済み証明書を購入するのかを決定する際は、次のことを考慮してください。

- Sterling B2B Integrator を使用して、自己署名証明書を簡単に作成できます。ただし、これらの自己署名証明書は信頼のおける第三者機関によっては証明されません。
- CA の証明書を使用することの主な利点は、証明書保有者の身元が信頼のおける第三者機関によって証明されることです。そのデメリットとしては、余分なコストと管理負担が生じることが挙げられます。第三者機関の証明書を使用する場合は、その証明書を CA から取得してください。
- CA は、証明書に関する情報 (期限切れの証明書に関する情報を含む) を公開および取得するための一元化された情報源を提供します。

デフォルトでは、システムは、当アプリケーションによって生成されたすべての自己署名証明書とすべての CA 証明書を信頼します。ただし、特定の CA によって

発行されたすべてまたは一部の証明書を信頼するかどうかをユーザーが指定できます。任意の取引パートナーの自己署名証明書を信頼しないように明示的に指定することもできます。

## 証明書の有効期限

アダプターとサーブレットをインバウンド通信用に使用している場合は、システム証明書の有効期限を監視して、それらの証明書が有効であることを確認する必要があります。これらの証明書は、期限切れになる前に有効な証明書と置換される必要があります。

## システム証明書パラメーターの定義

アダプターとサーブレットをインバウンド通信用に使用している場合は、システム証明書の有効期限を監視して、それらの証明書が有効であることを確認する必要があります。これらの証明書は、期限切れになる前に有効な証明書と置換される必要があります。

| パラメーター | 説明 |
|---|---|
| alias | HSM に保管されている鍵名。使用する別名は、A から Z の大文字/小文字、0 から 9 の数字、またはハイフン (-) で構成されており、その全体の長さはシステム GUID の長さ以下である必要があります。 |
| certname | データベース内のシステム証明書に割り当てる名前。 |
| Certtype | インポートする証明書タイプ。サポートされている証明書ファイルのタイプは、pkcs12、pkcs8、pem、および keystore の 4 タイプです。Sterling B2B Integrator でサポートされているのは、DES または 3DES で暗号化された pem 鍵のみです。<br><br>鍵ストアを一覧表示またはインポートするには、keystore を使用します。 |
| file | インポートするファイルの名前。 |
| keypass | Eracom 装置上のスロットの PIN。 |
| keystoretype | インポートする鍵ストア・タイプ。有効な値は CRYPTOKI です。 |
| keystoreprovider | プロバイダー・タイプ。Eracom は、HSM でサポートされている唯一のプロバイダー・タイプです。<br><br>有効な値は次のとおりです。<br>• ERACOM<br>• ERACOM.n (最初の位置以外のスロットに証明書をインポートする場合) |
| password | 証明書ファイルのストア・パスフレーズ。 |
| pkcs12file | インポートする PKCS12 ファイルの名前。 |
| pkcs12storepass | PKCS12 ファイルの生成に使用されるストア・パスフレーズ。 |
| pkcs12keypass | PKCS12 ファイルの有効なパスフレーズ。 |
| storepass | 鍵ストアが存在する Eracom 装置上のスロットの PIN。 |
| systempass | システム・パスフレーズ。 |

## IBM 鍵管理ユーティリティー (iKeyman)

IBM 鍵管理ユーティリティー (iKeyman) は、IBM SDK の 1 コンポーネントで、鍵、認証要求、および自己署名証明書を生成します。

iKeyman は、証明書を作成して通信を保護したり、データの暗号化や暗号化解除をするために使用できます。 SSL を使用したセキュアな転送では、証明書によりセキュリティー・レベルが追加されます。

Sterling B2B Integrator では、iKeyman を使用して以下を作成できます。

- 証明書署名要求 (CSR) - X.509 証明書を要求するために認証局に電子メールで送信されるファイル。
- 鍵証明書 – ASCII でエンコードされた証明書と ASCII でエンコードされた PKCS12 暗号化秘密鍵の組み合わせ。特定の暗号化方式に基づいた標準フォーマット (デフォルト) を使用して鍵証明書を生成した場合、出力される証明書は、Sterling B2B Integrator へのインポート時にエラーになります。 PKCS12 が鍵証明書の推奨フォーマットです。

iKeyman の構成と使用について詳しくは、 「IBM SDK、Java Technology Edition 7.0.0 の場合の iKeyman の概要 (iKeyman Overview for IBM SDK, Java Technology Edition 7.0.0)」 を参照してください

## 証明書のタスク

### 自己署名証明書の作成

「管理」メニューから、自己署名証明書を作成できます。

#### このタスクについて

自己署名証明書を作成するには、以下のようにします。

#### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「システム **(System)**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 自己署名証明書の作成 **(Create Self-signed Certificate)**」の横にある「実行 **(Go!)**」をクリックします。
3. 自己署名証明書の「名前」を入力します。
4. 発行元の「組織」の名前を入力します。
5. 自己署名証明書の「国」、または作成元を選択します。
6. 組織における証明書の責任者の連絡先「**E** メール」アドレスを入力して、「次へ **(Next)**」をクリックします。
7. 証明書の「シリアル番号」を入力します。 シリアル番号は、自己署名証明書に割り当てる番号です。
8. この自己署名証明書の有効日数を「期間 **(Duration)**」に入力します。

注**:** V5.2.6.2 以降では、最大の有効期限は *Jan 1, 2080* です。有効期限が 2080 年 1 月 1 日を超える期間を入力すると、デフォルトで *Jan 1, 2080* に設定されます。それより前のリリースでは、上限はありません。

9. SubjectAltName フィールドとして、証明書と関連付けるネットワーク・インターフェースの「**IP** アドレス **(IP addresses)**」を入力します。
10. SubjectAltName フィールドとして、証明書と関連付けるネットワーク・インターフェースの「**DNS** 名 **(DNS Names)**」を入力します。
11. 「鍵の長さ」を選択します。鍵の長さは次のいずれかから選択します。
    - 512
    - 1024
    - 2048

    注**:** セキュリティー、相互運用性、および効率のバランスの面から見ると、鍵の長さは 1024 が適しています。鍵の長さが 2048 の場合は、セキュリティーの面では最も優れていますが、低速になり、一部のアプリケーションで機能しない場合があります。

    注**:** 鍵の長さに 512 を選択した場合、JDK 7 SR5 を使用することも必要です。JDK 7 SR7 FP1 は、1024 未満の鍵の長さをサポートしていません。
12. 「署名アルゴリズム」を選択します。
13. オプション「使用時に検証 **(Validate When Used)**」を選択します。検証オプションは以下のとおりです。
    - 有効期間 (Validity) – 証明書の有効期間の日付がまだ有効であるかを検証します。日付が有効でない場合、証明書は使用されません。
    - 認証チェーン (Auth Chain) – 自己署名されていない証明書の信頼チェーンを構成します。有効な証明書を使用して信頼チェーンを構成できない場合、証明書は使用されません。証明書が自己署名されている場合、このオプションでは、証明書の署名のみが検証されます。
14. 「証明書署名ビットを設定 **(Set the Certificate Signing Bit)**」チェック・ボックスを選択して、これを有効にします。
15. 「次へ **(Next)**」をクリックします。
16. 自己署名証明書の情報を確認します。
17. 「終了」をクリックします。

## 取引パートナーからのトラステッド証明書の自動取得

証明書キャプチャー・ユーティリティーは、取引パートナーから SSL 証明書を取得するプロセスを自動化します。この方法で証明書情報を取得することで、パートナーは簡単に接続して証明書を保存できます。

### このタスクについて

その証明書を CA 証明書またはトラステッド証明書としてシステムにチェックインする前に、希望に応じて、アウト・オブ・バンド・セキュリティー・チェックを実行できます。

始める前に:

- パートナーのホスト・システムが SSL に対応していることを確認します。
- 取引パートナーのサーバーのホスト情報とポート情報を取得します。
- FTPS モードが使用される場合は、モードが明示または暗黙のどちらになるのかを特定します。
- デフォルトの SSLCertGrabberAdapter サービス・インスタンスで適切な周辺サーバーとプロキシー・サーバー (HTTPS のみ) が使用されるように構成します。詳しくは、アダプターの資料を参照してください。

取引パートナーから SSL 証明書を自動的に取得するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「取引パートナー」>「デジタル証明書」>「証明書キャプチャー・ユーティリティー」を選択します。
2. 「パートナー証明書のキャプチャー」の横にある「実行」をクリックします。
3. サーバーの接続タイプを選択して、「次へ **(Next)**」をクリックします。
   - FTPS
   - HTTPS
4. 「ホスト名」または「**IP** アドレス」を入力します。
5. 「ポート」番号を入力します。
6. FTPS の接続モードを選択します (HTTPS を使用している場合はこの手順をスキップします)。
   - 明示 - SSL ネゴシエーションは FTP 接続の確立後に実行されます。これがデフォルトです。
   - 暗黙 - SSL ネゴシエーションは FTP 接続の確立前に実行されます。
7. 「次へ **(Next)**」をクリックします。 システムによって接続および証明書の取得が試行されます。
8. キャプチャーが完了したら、サマリー情報を確認して、保存する証明書を決定します。
9. 各証明書のエンコード方式を選択して、「保存」をクリックします。エンコード方式は次のとおりです。
   - BASE64 – 標準の DER 証明書に対して Base64 エンコード方式を使用します。これがデフォルトです。
   - DER – これはデジタル証明書の標準フォーマットであり、ほとんどのアプリケーションが対応しています。
10. 「保存」をクリックして、ファイルを保存する場所に移動します。
11. デフォルトのファイル名をそのまま使用するか、各自のファイル命名規則に従って名前を編集して、「保存」をクリックします。
12. 保存後に、それらの証明書をシステムにチェックインできます。証明書をシステムにチェックインする場合は、以下を実行します。
    a. 各証明書が有効かつ信頼されていることを確認します。
    b. 証明書を、機能に応じて CA 証明書またはトラステッド証明書としてチェックインします。認証局に基づいた信頼の場合は、必要に応じて、エンド・ユーザー証明書を除いた証明書チェーンをチェックインします。直接信頼の場合は、エンド・ユーザー証明書をチェックインします。

## 証明書サマリーのステータス情報の構成

デフォルトでは、ハイパーリンク化された証明書名を選択すると、証明書のステータス情報がサマリー・ポップアップ・ウィンドウの末尾に表示されます。ステータス情報は含めることも除外することもできます。ステータス情報はリアルタイムで収集されるため、ステータス情報を含めない方がいい場合もあります。

### このタスクについて

VerificationOnPopupInfo プロパティーは、ステータス情報が証明書サマリーに表示されるかどうかを制御します。このプロパティーは、ui.properties ファイル内にあります。VerificationOnPopupInfo プロパティーの値は次のとおりです。

- true - 検証情報を含めます (デフォルト)。
- false - 検証情報を収集せず、ポップアップ・ウィンドウで表示しません。
- (他の任意の値) - 検証情報を含めます。

ステータス情報が収集および表示されないようにするには、以下を実行します。

### 手順

1. ui.properties ファイルを開きます。
2. VerificationOnPopupInfo の値を false に変更します。次に例を示します。

   ```
   VerificationOnPopupInfo=false
   ```
3. 保存してファイルを閉じます。
4. Sterling B2B Integrator を再始動します。

## サムプリント・ディスプレイの構成

事前計算された SHA1 ハッシュに加えて、追加の証明書サムプリントを証明書表示画面、確認画面、およびサマリー画面に表示できます。ハッシュ計算は、表示内容の生成時にオンデマンドで実行されます。

### このタスクについて

追加のサムプリントが GUI 画面に表示されますが、メッセージ処理やシステム通信は影響を受けません。

追加の証明書サムプリントを計算して表示するようにシステムを構成するには、以下を実行します。

### 手順

1. ui.properties ファイルで、次の行を変更します。

   ```
   AddtlCertThumbprintAlgs=hash_algorithm
   ```

   複数の追加ハッシュを表示するには、それぞれの値をコンマで区切ります。次に例を示します。

   ```
   AddtlCertThumbprintAlgs=SHA384,SHA512
   ```

| パラメーター | 説明 |
| --- | --- |
| hash_algorithm | 証明書サムプリントに適用するハッシュ・アルゴリズムの名前。有効な値は次のとおりです。<br>• SHA-256<br>• SHA-384<br>• SHA-512 |

2. ui.properties ファイルを保存して閉じます。
3. Sterling B2B Integrator を再始動します。

## CA 証明書の検索

「管理」メニューから、CA 証明書を検索できます。

### このタスクについて

CA 証明書を検索するには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理メニュー」から、「取引パートナー」>「デジタル証明書」>「**CA**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 次のいずれかを実行して、「実行」をクリックします。
   - 「検索」の「証明書名別」フィールドに、検索する CA 証明書名の一部または全体を入力します。「CA デジタル証明書」ページに、検索条件に一致するすべての CA 証明書が一覧表示されます。
   - 「リスト」の「英数字別」フィールドで、「すべて」を選択するか、検索する CA 証明書名の先頭文字を選択します。「すべて」を選択すると、すべての CA 証明書が一覧表示されます。「CA デジタル証明書」ページに、検索条件に一致するすべての CA 証明書が一覧表示されます。

## CA 証明書のサマリー情報の表示

証明書のリストが表示されたら、証明書名をクリックすることでその証明書のサマリー情報を表示できます。システム名、サムプリント、およびステータスを構成できます。

### このタスクについて

システムでは次のフィールドを構成できます。

| 証明書サマリー・フィールド | 説明 |
|---|---|
| システム名 | 証明書名はデータベース・ラベルです。証明書名は、GUI 上でこの証明書の呼称として使用され、この名前をそのデータベース内に格納するために使用されます。<br><br>JKS 鍵ストア内の証明書のデフォルト名は、任意のストリングです。他の証明書の名前は、発行者の相対識別名 (RDN) とその証明書のシリアル番号に基づいて作成されます。<br><br>証明書をチェックインまたは編集する際に、その証明書名を短い名前やわかりやすい名前に変更できます。 |
| サムプリント | SHA1 ハッシュの情報はデフォルトで含まれています。他のハッシュのサムプリント情報の計算と表示を構成するには、ui.properties ファイルを編集します。 |
| ステータス | 現在のステータスのリアルタイム・チェックであり、証明書の日付が有効であるかどうか、および証明書が検証済みかどうかを示します。この情報が表示時に計算されるかどうかを構成するには、ui.properties ファイルを編集します。 |

上記の説明は CA 証明書のサマリー情報に関するものですが、他のタイプの証明書についても類似するフィールドが「サマリー」画面と「確認」画面に表示されます。

## ユーザー・インターフェースからの CA 証明書のチェックイン

ユーザー・インターフェースの「管理メニュー」メニューから CA 証明書をチェックインできます。

### このタスクについて

ご使用のサイトのセキュリティー・ポリシーに基づいて、JKS 鍵ストア内の CA 証明書をコンソールからチェックインすることもできます。

開始前に、外部から取得したすべての CA 証明書をローカル・ファイルに保存します。

CA 証明書をチェックインするには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理メニュー」から、「取引パートナー」>「デジタル証明書」>「**CA**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2 管理 (AS2 Administration)**」メニューから、「証明書」を選択します。
2. 「新規証明書のチェックイン **(Check in New Certificate)**」の横にある「実行」をクリックします。

3. 証明書をインポートする方法を以下から選択します。

| インポート方法 | 次のステップ |
| --- | --- |
| JVM からのインポート – JKS 鍵ストアからのインポート | 1. 「**JVM (JVM)**」から「インポート」をクリックします。<br>2. パスワード・フィールドに表示されるデフォルトのパスワードを受け入れ、「次へ **(Next)**」をクリックします。<br><br>デフォルトの鍵ストア・パスワードは、Sun Microsystems 社から提供されています。パスワード・フィールドが空の場合も、システムではデフォルトのパスワードが使用されます。 |
| ファイルからのインポート – ローカル・ドライブにファイルとして保存された証明書のインポート | 1. 「ファイル」から「インポート」をクリックします。<br>2. ファイル名を入力するか、「参照」をクリックして CA 証明書ファイルを選択します。「次へ (Next)」をクリックします。<br><br>パスワード・フィールドに表示されるパスワードは無視してかまいません。エントリーを削除する必要はありません。 |

選択可能な証明書が識別情報の要約とともにリスト表示されます。デフォルトではすべての証明書が選択されています。

4. 各エントリーの左側にあるチェック・ボックスをクリックして、インポートする証明書を選択または選択解除します。
5. 選択した証明書のそれぞれについて、提案された証明書名を受け入れるか、使用するファイル命名規則に基づいて編集します。
6. 「使用時に検証」オプションを選択して、「次へ **(Next)**」をクリックします。検証オプションは以下のとおりです。
   - 有効期間 (Validity) – 証明書の有効期間の日付がまだ有効であるかを検証します。日付が有効でない場合、証明書は使用されません。
   - 認証チェーン – 自己署名のない証明書のルートまでの信頼チェーンの構成を試行します。有効な証明書を使用して信頼チェーンを構成できない場合、証明書は使用されません。証明書が自己署名されている場合、このオプションでは、証明書の署名のみが検証されます。
7. その証明書が、既にデータベースに存在する証明書と重複するというメッセージが表示された場合は、Y または N を入力して、重複する証明書をインポートするかどうかを指定します。

   このチェックは、単一の証明書でのみ実行されます。 1 つのファイルから 1 つ以上の証明書をチェックインする場合はこのチェックが実行されません。

   証明書は、重複の判別のために SHA1 ハッシュで識別されます。 データベース内に同じ証明書の複数のコピーが存在していてもかまいません。それぞれの証明書コピーは異なる行に格納され、個別のオブジェクト ID が割り当てられるからです。既存の証明書が上書きされることはありません。

8. CA 証明書情報を確認します。
9. 「終了」をクリックします。

## コンソールからの CA 証明書のチェックイン

すべての CA 証明書をローカル・ファイルに保存した後で、コンソールでインストール・ディレクトリーから CA 証明書をチェックインできます。

### このタスクについて

Sterling B2B Integrator に付属している JVM の一部である JKS 鍵ストアには、一般的な CA 証明書が含まれています。この JKS 鍵ストアの場所は、/install_dir/jdk/jre/lib/security/cacerts です。証明書を外部から取得することもできます。

Sterling B2B Integrator のトラステッド・リポジトリーに証明書をインポートするには、/install_dir/install/bin/ImportCACerts.sh (UNIX) または ¥install_dir¥install¥bin¥ImportCACerts.cmd (Windows) でコマンドを変更します。

開始前に、外部から取得したすべての CA 証明書をローカル・ファイルに保存します。

コンソールで CA 証明書をチェックインするには、以下を実行します。

### 手順

1. インストール・ディレクトリーに移動します。
2. bin ディレクトリーに移動します。
3. 次のコマンドを入力します。

   (UNIX) `./ImportCACerts.sh`

   (Windows) `ImportCACerts.cmd`

   ファイル内のすべての証明書が 1 つずつ一覧表示されますが、次の例外があります。
   - 対称鍵または秘密鍵が含まれたエントリーは処理も一覧表示もされません。
   - DER 形式ファイル内の最初の証明書のみが処理および一覧表示されます。
4. プロンプトに従って、インポートする証明書については Y (小文字でも可) を入力します。
5. インポート対象として選択した各証明書について、提示された証明書名をそのまま使用するか、ご使用のファイル命名規則に基づいてこの名前を変更します。
6. 証明書ラベルがデータベース内の既存のラベルと重複する場合は、`Y` または `N` (小文字でも可) を入力して、証明書ラベルを変更するかどうかを指定します。証明書は通常はラベルによって識別されず、データベースではラベルの重複が許可されていますが、一部のサービスではラベルに基づいて証明書が検索されます。予期せぬ問題を回避するためには、重複ラベルを避けてください。
7. 証明書がデータベース内の既存の証明書と重複する場合は (証明書の SHA1 ハッシュで判別可能)、Y または N を入力して、重複する証明書をインポートするかどうかを指定します。

証明書は、重複の判別のために SHA1 ハッシュで識別されます。 データベース内に同じ証明書の複数のコピーが存在していてもかまいません。それぞれの証明書コピーは異なる行に格納され、個別のオブジェクト ID が割り当てられるからです。既存の証明書が上書きされることはありません。

## CA 証明書の編集

「管理」メニューから、CA 証明書を編集できます。

### このタスクについて

CA 証明書を編集するには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理メニュー」から、「取引パートナー」>「デジタル証明書」>「**CA**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 「検索」または「リスト」を使用して編集する CA 証明書を探して、「実行」をクリックします。
3. 編集する **CA** 証明書の横にある「編集」をクリックします。
4. 「証明書名 (Certificate Name)」に入力します。
5. 「使用時に検証」オプションを選択して、「次へ **(Next)**」をクリックします。検証オプションは以下のとおりです。
   - 有効期間 (Validity) – 証明書の有効期間の日付がまだ有効であるかを検証します。日付が有効でない場合、証明書は使用されません。
   - 認証チェーン (Auth Chain) – 自己署名されていない証明書の信頼チェーンを構成します。有効な証明書を使用して信頼チェーンを構成できない場合、証明書は使用されません。証明書が自己署名されている場合、このオプションでは、証明書の署名のみが検証されます。
6. CA 証明書情報を確認します。
7. 「終了」をクリックします。

## CA 証明書の削除

「管理」メニューから、CA 証明書を削除できます。

### このタスクについて

CA 証明書を削除するには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理メニュー」から、「取引パートナー」>「デジタル証明書」>「**CA**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 「英数字別」の横にある「実行」をクリックします。

3. 削除する CA 証明書の横にある「削除」をクリックします。

## システム証明書の検索

「管理」メニューから、システム証明書を検索できます。

### このタスクについて

システム証明書を検索するには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「システム **(System)**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 「システム証明書」で、次のいずれかの操作を実行して、「実行」をクリックします。
   - 「検索」の「証明書名別」フィールドに、検索するシステム証明書名の一部または全体を入力します。「システム証明書」ページに、検索条件に一致するすべてのシステム証明書が一覧表示されます。
   - 「リスト」の「英数字別」フィールドで、「すべて」を選択するか、検索するシステム証明書名の先頭文字を選択します。「すべて」を選択すると、すべてのシステム証明書が一覧表示されます。「システム証明書」ページに、検索条件に一致するすべてのシステム証明書が一覧表示されます。

## システム証明書の編集

「管理」メニューから、システム証明書を編集できます。

### このタスクについて

システム証明書を編集するには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「システム **(System)**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 「検索」または「リスト」を使用して編集するシステム証明書を探して、「実行」をクリックします。
3. 編集するシステム証明書の横にある「編集」をクリックします。
4. 「証明書名 **(Certificate Name)**」に入力します。
5. 「使用時に検証」オプションを選択して、「次へ **(Next)**」をクリックします。検証オプションは以下のとおりです。

- 有効期間 (Validity) – 証明書の有効期間の日付がまだ有効であるかを検証します。日付が有効でない場合、証明書は使用されません。
- 認証チェーン (Auth Chain) – 自己署名されていない証明書の信頼チェーンを構成します。有効な証明書を使用して信頼チェーンを構成できない場合、証明書は使用されません。証明書が自己署名されている場合、このオプションでは、証明書の署名のみが検証されます。

6. このシステム証明書の情報を確認します。
7. 「終了」をクリックします。

## Sterling B2B Integrator 内のシステム証明書の識別

「管理」メニューから、システム証明書を識別できます。

### このタスクについて

システム証明書を識別するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「展開」>「サービス」>「構成」を選択します。
2. 「リスト」セクションで、該当するサービス・タイプまたはアダプター・タイプを「サービス・タイプ別 **(by Service Type)**」リストから選択して、「実行」をクリックします。
3. 構成のリストから、構成を選択します。
4. 「サービス名」をクリックして、構成情報を表示します。
5. 証明書のサマリー情報を確認します。

## システム証明書の有効期限の確認

アダプターとサーブレットをインバウンド通信用に使用している場合は、システム証明書の有効期限を監視して、それらの証明書が有効であることを確認する必要があります。

### このタスクについて

システム証明書の有効期限を確認するには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「システム **(System)**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. すべてのシステム証明書を表示するには、「アルファベット順 (Alphabetical)」ドロップダウン・リストから「すべて」を選択して、「実行」をクリックします。
3. 表示するシステム証明書の名前を選択します。 「証明書のサマリー」が表示されます。

4. 「証明書のサマリー」の「説明」セクションで、「有効な日付」フィールドに表示されている情報を参照します。
5. 「ステータス」セクションに表示されている情報を参照して、これらの日付が有効かどうか、およびこの証明書が証明済みであるかどうかを確認します。

## Sterling B2B Integrator でのシステム証明書のエクスポート

このエクスポート・コマンドは、Sterling B2B Integrator のシステム証明書のみに適用できます。このコマンドを使用して、HSM 上のシステム証明書をエクスポートすることはできません。

### このタスクについて

システム証明書をエクスポートするには、適切なパラメーターを指定して、次のコマンドを入力します。

```
./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass
```

| パラメーター | 説明 |
|---|---|
| keyname | エクスポートするシステム鍵の鍵名。 |
| pkcs12filename | エクスポートされる情報が含まれたファイルの名前。 |
| pkcs12storepass | ストアを保護するストア・パスワード。 |
| pkcs12keypass | 鍵を保護する鍵パスワード。 |

## Sterling B2B Integrator でのシステム証明書の削除

システム証明書を削除する前に、そのシステム証明書のコピーをローカル・ディスクにエクスポートすることができます。OpsDrv、OpsKey、および UIKeys は、削除できないシステム証明書です。

### このタスクについて

システム証明書を削除するには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「システム **(System)**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 「英数字別」の横にある「実行」をクリックします。
3. 削除するシステム証明書の横にある「削除」をクリックします。
4. 「確認」ページで「削除」をクリックします。

## システム証明書のチェックアウト

システム証明書をエクスポートするには、その証明書をチェックアウトする必要があります。以下の手順では、秘密鍵をエクスポートせずにパブリック証明書のみをエクスポートして、取引パートナーに送信するパブリック証明書が得られます。

### このタスクについて

システム証明書をチェックアウトするには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「システム **(System)**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 「検索」または「リスト」を使用して、チェックアウトするシステム証明書を探します。
3. チェックアウトするシステム証明書の横の「チェックアウト」をクリックします。
4. 「システム証明書のチェックアウト」ダイアログ・ボックスで、次のいずれかの証明書フォーマットを選択して、「実行」をクリックします。
   - PKCS12 – このオプションを選択すると、デジタル証明書が PKCS12 ファイルの形式に設定されます。秘密鍵パスワードと鍵ストア・パスワードを入力することもできます。
   - BASE64 – このオプションを選択すると、標準の DER 証明書に対して Base64 エンコード方式が使用されます。
   - DER – これはデジタル証明書の標準フォーマットであり、ほとんどのアプリケーションが対応しています。
5. 「ファイルのダウンロード **(File Download)**」ダイアログ・ボックスで、「保存」をクリックします。
6. 「別名保存」ダイアログ・ボックスで、証明書を保存する場所を選択して、「保存」をクリックします。 この証明書を開くためのオプションはサポートされていません。この証明書は、オペレーティング・システム内で開く必要があります。「これは無効なセキュリティー証明書ファイルです (This is an invalid Security Certificate file)」というエラー・メッセージが表示された場合は、そのファイルをテキスト・エディターで開いて、「-----BEGIN CERTIFICATE-----」より前にある空白行をすべて削除します。編集したファイルを保存してから、そのファイルを開いてみます。
7. 「システム証明書のチェックアウト」ダイアログ・ボックスで、「クローズ」をクリックします。 「システム証明書」ページが表示されます。

## トラステッド証明書の検索

「管理」メニューから、トラステッド証明書を検索できます。

### このタスクについて

トラステッド証明書を検索するには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。

- Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「トラステッド **(Trusted)**」を選択します。
- AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。

2. 「トラステッド・デジタル証明書」ページで、次のいずれかの操作を実行して、「実行」をクリックします。
   - 「検索」の「証明書名別」フィールドに、検索するトラステッド証明書名の一部または全体を入力します。「トラステッド・デジタル証明書」ページに、検索条件に一致するすべてのトラステッド証明書が一覧表示されます。
   - 「リスト」の「英数字別」フィールドで、「すべて」を選択するか、検索するトラステッド証明書名の先頭文字を選択します。「トラステッド・デジタル証明書」ページに、検索条件に一致するすべてのトラステッド証明書が一覧表示されます。

## トラステッド・システム証明書のチェックイン

取引パートナーからインポートされた SSL 証明書や外部のその他の証明書などのトラステッド証明書をチェックインできます。

### このタスクについて

トラステッド証明書は、次のソースから取得できます。

- 取引パートナーからインポートされた SSL 証明書
- 外部から取得された他の証明書

開始前に信頼されたシステム証明書を、ローカル・コンピューターのファイルに保存します。

信頼されたシステム証明書をチェックインするには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「トラステッド **(Trusted)**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 「新規証明書のチェックイン **(Check in New Certificate)**」の横にある「実行」をクリックします。
3. 「ファイル名」に入力するか、「参照」をクリックして、信頼される証明書のファイル名を選択し、「次へ **(Next)**」をクリックします。
4. 「証明書名 **(Certificate Name)**」に入力します。
5. チェックインする信頼された証明書の名前を検証します。 選択した証明書のそれぞれに対して「証明書名 (Certificate Name)」フィールドに提案名が表示され、その後ろに証明書の識別情報の要約が続きます。名前は、使用するファイル命名規則に基づいて変更できます。

6. 選択したファイルに複数のトラステッド証明書が含まれている場合は、各証明書の左側にあるチェック・ボックスを選択して各証明書をチェックインします。
7. 「使用時に検証」オプションを選択して、「次へ **(Next)**」をクリックします。検証オプションは以下のとおりです。
   - 有効期間 (Validity) – 証明書の有効期間の日付がまだ有効であるかを検証します。日付が有効でない場合、証明書は使用されません。
   - 認証チェーン – 自己署名のない証明書のルートまでの信頼チェーンの構成を試行します。有効な証明書を使用して信頼チェーンを構成できない場合、証明書は使用されません。証明書が自己署名されている場合、このオプションでは、証明書の署名のみが検証されます。
   - CRL キャッシュ – システム証明書を使用するたびに、CRL キャッシュを調べるかどうかを制御します。
8. 信頼された証明書情報を確認します。
9. 「終了」をクリックします。

## トラステッド証明書の編集

「管理」メニューから、トラステッド証明書を編集できます。

### このタスクについて

トラステッド証明書を編集するには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「トラステッド **(Trusted)**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 「検索」または「リスト」を使用して編集するトラステッド証明書を探して、「実行」をクリックします。
3. 編集するトラステッド証明書の横にある「編集」をクリックします。
4. 「証明書名 **(Certificate Name)**」に入力します。
5. 「使用時に検証」オプションを選択して、「次へ **(Next)**」をクリックします。検証オプションは以下のとおりです。
   - 有効期間 (Validity) – 証明書の有効期間の日付がまだ有効であるかを検証します。日付が有効でない場合、証明書は使用されません。
   - 認証チェーン – 自己署名のない証明書のルートまでの信頼チェーンの構成を試行します。有効な証明書を使用して信頼チェーンを構成できない場合、証明書は使用されません。証明書が自己署名されている場合、このオプションでは、証明書の署名のみが検証されます。
   - CRL キャッシュ – システム証明書を使用するたびに、CRL キャッシュを調べるかどうかを制御します。
6. この証明書の情報を確認します。
7. 「終了」をクリックします。

## トラステッド・システム証明書の削除

「管理」メニューから、トラステッド・システム証明書を削除できます。

### このタスクについて

トラステッド・システム証明書を削除するには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「トラステッド **(Trusted)**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 「英数字別」の横にある「実行」をクリックします。
3. 削除するトラステッド証明書の横にある「削除」をクリックします。

## PKCS12 システム証明書のインポート

PKCS12 システム証明書をインポートできます。

### このタスクについて

PKCS12 システム証明書をインポートするには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。

```
./ImportSystemCert.sh -pkcs12 systempass certname pkcs12file
pkcs12storepass pkcs12keypass keystoretype keystoreprovider storepass
keypass
```

## PKCS12 システム証明書のチェックイン

PKCS12 システム証明書をローカル・コンピューターのファイルに保存した後で、「管理」メニューからその PKCS12 システム証明書をチェックインできます。

### このタスクについて

開始前に、PKCS12 システム証明書をローカル・コンピューター上のファイルに保存する必要があります。

PKCS12 システム証明書をチェックインするには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「システム **(System)**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。

2. 「システム証明書」ページの「チェックイン」で、「**PKCS12** 証明書」の横にある「実行」をクリックします。
3. この PKCS12 証明書の「証明書名」を入力します。
4. 「秘密鍵パスワード **(Private Key Password)**」を入力します。 これは、PKCS12 証明書を暗号化するために使用されるパスワードです。
5. 「鍵ストア・パスワード」を入力します。 これは、PKCS12 オブジェクトのパスワードです。これは、秘密鍵のパスワードと同じでもかまいません。
6. 「ファイル名」に入力するか、「参照」をクリックして、 PKCS12 証明書のファイル名を選択してから、「次へ **(Next)**」をクリックします。
7. 「使用時に検証」オプションを選択して、「次へ **(Next)**」をクリックします。検証オプションは以下のとおりです。
   - 有効期間 (Validity) – 証明書の有効期間の日付がまだ有効であるかを検証します。日付が有効でない場合、証明書は使用されません。
   - 認証チェーン (Auth Chain) – 自己署名されていない証明書の信頼チェーンを構成します。有効な証明書を使用して信頼チェーンを構成できない場合、証明書は使用されません。証明書が自己署名されている場合、このオプションでは、証明書の署名のみが検証されます。
8. この PKCS12 システム証明書の情報を確認します。
9. 「終了」をクリックします。

## pem システム証明書のインポート

DES または 3DES で暗号化された pem システム証明書をインポートできます。

### このタスクについて

DES または 3DES で暗号化された pem 鍵のみがサポートされています。

pem システム証明書をインポートするには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。

```
./ImportSystemCert.sh -pem systempass certname file password
keystoretype keystoreprovider storepass keypass
```

## 鍵システム証明書のインポート

鍵システム証明書をインポートできます。

### このタスクについて

鍵システム証明書をインポートするには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。

```
./ImportSystemCert.sh -keycert systempass certname file
password keystoretype keystoreprovider storepass keypass
```

## 鍵ストア・システム証明書のインポート

鍵ストア・システム証明書を HSM 上で生成できます。

### このタスクについて

HSM 上で鍵ストア・システム証明書を生成するには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。

```
./ImportSystemCert.sh -keystore systempass certname
alias keystoretype keystoreprovider storepass keypass
```

## 鍵システム証明書のチェックイン

鍵システム証明書をローカル・コンピューターのファイルに保存した後で、「管理」メニューからその鍵システム証明書をチェックインできます。

### このタスクについて

開始前に、鍵システム証明書をローカル・コンピューターのファイルに保存します。

鍵システム証明書をチェックインするには、以下を実行します。

### 手順

1. 以下のいずれかを選択します。
   - Sterling B2B Integrator を使用している場合は、「管理」メニューから、「取引パートナー **(Trading Partner)**」>「デジタル証明書 **(Digital Certificates)**」>「システム **(System)**」を選択します。
   - AS2 Edition を使用している場合は、「**AS2** 管理 **(AS2 Administration)**」メニューから、「証明書」を選択します。
2. 「鍵証明書 **(Key Certificate)**」の横にある「実行 **(Go!)**」をクリックします。
3. 「証明書名 **(Certificate Name)**」に入力します。
4. 「秘密鍵パスワード **(Private Key Password)**」を入力します。 これは、秘密鍵を暗号化するために使用されるパスワードです。
5. 「ファイル名」に入力するか、「参照」をクリックして鍵証明書のファイル名を選択して、「次へ **(Next)**」をクリックします。
6. 「使用時に検証」オプションを選択して、「次へ **(Next)**」をクリックします。検証オプションは以下のとおりです。
   - 有効期間 (Validity) – 証明書の有効期間の日付がまだ有効であるかを検証します。日付が有効でない場合、証明書は使用されません。
   - 認証チェーン (Auth Chain) – 自己署名されていない証明書の信頼チェーンを構成します。有効な証明書を使用して信頼チェーンを構成できない場合、証明書は使用されません。証明書が自己署名されている場合、このオプションでは、証明書の署名のみが検証されます。
7. 鍵証明書情報を確認します。
8. 「終了」をクリックします。

# オンライン証明書状況プロトコル (OCSP)

## Sterling B2B Integrator でのオンライン証明書状況プロトコル (OCSP) のサポート

OCSP (Online Certificate Status Protocol) は、証明書失効状況に関する情報を要求および受信するための一連の ASN.1 定義のデータ構造体です。これらのデータ構造体は、原理的には多くのトランスポート・プロトコルによって送受信可能です。ただし実際には、HTTP が使用されます。

OCSP クライアントは、問い合わせを送信して、応答を処理します。OCSP 応答者は、問い合わせに回答して、応答を生成します。

## OCSP クライアントの機能

OCSP クライアントの実装は、OCSP 応答者に関する情報を管理するためのデータ構造、OCSP 要求を生成するための機能、OCSP 応答を処理するための機能、および OCSP 要求を送信および OCSP 応答を受信するための機能で構成されます。

OCSP クライアントの実装は以下で構成されています。

- OCSP 応答者に関する情報を管理するためのデータ構造体
- OCSP 要求を生成するための機能
- OCSP 応答を処理するための機能
- OCSP 要求を送信および OCSP 応答を受信するための機能

## Sterling B2B Integrator による OCSP チェックの実行方法

Sterling B2B Integrator 内の証明書に対する OCSP チェックが決定されるのは、Sterling B2B Integrator 内でその OCSP チェックが、データベースから証明書と鍵を取得するためにサービスによって使用される内部システム API の一部として実装されたときです。

### このタスクについて

OCSP チェックが Sterling B2B Integrator によって実行されるのは、証明書と鍵をデータベース内でカプセル化しているオブジェクトから証明書と鍵を取得するためにメソッドが呼び出されたときです。

次の手順では、OSCSP チェックが Sterling B2B Integrator で実装される方法を説明しています。

### 手順

1. システムは、証明書をカプセル化しているオブジェクトを調べて、OCSP チェックが有効になっているかどうかを確認します。これによりシステムは、追加のデータベース呼び出しを行うことなく、OCSP チェックを試行するかどうかを決定できます。
2. OCSP チェックが有効になっている場合は、システムはエンコードされた発行者名を証明書から取得します。
3. システムは、エンコードされた発行者名を SHA1 でハッシュ化します。
4. システムは、この証明書のハッシュと一致するハッシュに変換される名前を持つ構成済み認証局をシステム内で探します。

5. 該当する認証局が見つからない場合は、チェックは実行されません。
6. 該当する認証局が見つかった場合は、システムはその認証局の OCSP ポリシーをチェックします。このポリシーで OCSP チェックが許可または要求されている場合は、CERT_AUTHORITY 表を参照して詳細情報を確認してください。システムは、この認証局の OCSP 応答者を探します。
7. この認証局の OCSP 応答者が見つからない場合は、次のいずれかの状況になります。
   - この認証局のポリシーが、常にチェックを実行するように設定されている場合は、例外がスローされて、チェックは不合格になります。
   - この認証局のポリシーが、応答者が構成されている場合にのみチェックを実行するように設定されている場合は、チェックは実行されません。
   - この認証局の OCSP 応答者が見つかった場合は、OCSP チェックが試行されます。

## データベース表

OCSP 関連情報を管理するために、CERT_AUTHORITY および OCSP_RESPONDER が追加されます。

OCSP 関連情報を管理するために、次の 2 つの新しいデータベース表が追加されました。

- CERT_AUTHORITY
- OCSP_RESPONDER

### CERT_AUTHORITY

CERT_AUTHORITY 表には、認証局に関する情報が保持されます。

| 列 | タイプ **(Type)** | 説明 |
|---|---|---|
| OBJECT_ID | VARCHAR(255) | これは、レコードの固有 ID に相当する GUID です。これは 1 次キーです。NULL にすることはできません。 |
| NAME | VARCHAR(255) | レコードの名前。NULL が許可されています。 |
| CREATE_DATE | DATETIME | レコードの作成日。 |
| MODIFIED_DATE | DATETIME | レコードが最後に変更された日付。 |
| MODIFIED_BY | VARCHAR(255) | レコードを変更したユーザーに関する情報。 |
| ISSUER_NAME | BLOB | 認証局の RDN (その認証局の証明書から取得されたもの)。 |
| HASH_ALG | VARCHAR(128) | 名前と鍵のハッシュを計算するために使用されるハッシュ・アルゴリズム。SHA1 のみがサポートされています。 |
| RDN_HASH | VARCHAR(255) | 認証局の証明書から取得された DER エンコード済み発行者 RDN の Base64 エンコード済み SHA1 ハッシュ。この列は索引付けされています。 |
| KEY_HASH | VARCHAR(255) | 発行者の証明書内のエンコード済み公開鍵の Base64 エンコード済み SHA1 ハッシュ |

| 列 | タイプ **(Type)** | 説明 |
|---|---|---|
| CERT_OID | VARCHAR(255) | CA_CERT_INFO 表内の認証局の証明書の OBJECT_ID。各認証局は、データベース内に 1 つの CA 証明書を保有している必要があります。 NULL は許可されていません。 |
| OCSP_POLICY | VARCHAR(128) | 認証局の OCSP ポリシー。これは 2 つのコンマ区切り値で構成されています。これらの値によって、OCSP を使用する場合とチェック対象が指定されます。<br><br>指定できる値は次のとおりです。<br><br>**OCSP_When**<br>• never – OCSP を一切使用しません。<br>• resp – 要求の発行時に応答者が構成されている場合にのみ OCSP を使用します。<br>• always – 要求の発行時に常に OCSP を使用します。この値を指定した場合は、応答者が構成されていることが必要であり、応答者が構成されていない場合は証明書チェックは不合格になります。<br><br>**OCSP_What**<br>• none – どの証明書も一切チェックしません。<br>• end-user - エンド・ユーザー証明書のみをチェックします。<br>• both – エンド・ユーザー証明書と中間証明書の両方をチェックします。現在はサポートされていません。<br>• この列では NULL は許可されていません。 |
| CRL_POLICY | VARCHAR(128) | 現在は使用されていません。 |

## OCSP_RESPONDER

OCSP_RESPONDER 表には、OCSP 応答者に関する情報が保持されています。

| 列 | タイプ **(Type)** | 説明 |
|---|---|---|
| OBJECT_ID | VARCHAR(255) | これは、レコードの固有 ID に相当する GUID です。これは 1 次キーです。NULL にすることはできません。 |
| NAME | VARCHAR(255) | レコードの名前。NULL が許可されています。 |
| CREATE_DATE | DATETIME | レコードの作成日。 |
| MODIFIED_DATE | DATETIME | レコードが最後に変更された日付。 |
| MODIFIED_BY | VARCHAR(255) | レコードを変更したユーザーに関する情報。 |

| 列 | タイプ **(Type)** | 説明 |
|---|---|---|
| ISSUER_NAME | BLOB | 認証局の RDN (その認証局の証明書から取得されたもの)。 |
| HASH_ALG | VARCHAR(128) | 名前と鍵のハッシュを計算するために使用されるハッシュ・アルゴリズム。SHA1 のみがサポートされています。 |
| RDN_HASH | VARCHAR(255) | 認証局の証明書から取得された DER エンコード済み発行者 RDN の Base64 エンコード済み SHA1 ハッシュ。この列は索引付けされています。 |
| KEY_HASH | VARCHAR(255) | 発行者の証明書内のエンコード済み公開鍵の Base64 エンコード済み SHA1 ハッシュ |
| CERT_OID | VARCHAR(255) | CA_CERT_INFO 表内の認証局の証明書の OBJECT_ID。各認証局は、データベース内に 1 つの CA 証明書を保有している必要があります。 NULL は許可されていません。 |
| CACHE_TTL | VARCHAR(64) | OCSP 応答を内部応答キャッシュ内に存続させる秒数。<br><br>この列が NULL の場合は、OCSP 応答はキャッシュ内に 1 秒間しか保持されず、これは実質的にまったく保持されないのと同じことです。 |
| TRANS_PROF_OID | VARCHAR(255) | GIS データベース内のプロファイルの OBJECT_ID。応答者の正しい URL が含まれた、OCSP 応答者のプロファイルを作成する必要があります。 |
| COMM_BP | VARCHAR(255) | OCSP 応答者と通信するために使用するビジネス・プロセスの名前。これは、HTTP 通信を実行するビジネス・プロセスである必要があります。このビジネス・プロセス内のサービスは、送信時および受信時のそれぞれで、HTTP ヘッダーの要求もしなければ HTTP ヘッダーの提示もしないように構成されている必要があります。システムに付属している HTTPClientSend プロセスを使用することが可能であり推奨されます。 |
| COMM_WAIT | VARCHAR(24) | OCSP 応答者との通信を待つ秒数。この秒数を経過すると何らかの問題が発生していると見なされます。 |

## OCSP の構成

OCSP を使用するようにシステムを構成する場合に、認証局と応答者を無制限に作成できます。

## このタスクについて

システムの構成時に、希望の数の認証局と応答者を作成できます。

システムが OCSP を使用するように構成するには、以下を実行します。

## 手順

1. OCSP を使用してチェックインする証明書の発行者である認証局の証明書を Sterling B2B Integrator にチェックインして、その証明書が CA 証明書であることを確認します。
2. システム内の CA 証明書を一覧表示して、インストールしたばかりの証明書のオブジェクト ID を取得します。
3. 認証局の OCSP 応答署名証明書が認証局の証明書発行証明書と異なる場合は、認証局の OCSP 応答署名証明書をトラステッド証明書として Sterling B2B Integrator にチェックインします。

   注**:** 5.2.4.2 およびそれ以降では、トラステッド証明書としてレスポンダー証明書をチェックインする代わりに、CA としてレスポンダー証明書を発行したルート証明書をチェックインすることができます。レスポンダー証明書は頻繁に変更されるため、CA によっては、証明書が有効なものと置換されるまでに OCSP が失敗する原因となることがあります。ルート証明書はめったに変更されないため、今後はベスト・プラクティスとしてルート証明書を常にチェックインするべきです。しかし、両方のタイプが許可され続けます。
4. 追加の OCSP 署名証明書をチェックインした場合は、システム内の CA 証明書を一覧表示して、インストールしたばかりの証明書のオブジェクト ID を取得します。
5. Sterling B2B Integrator のインストール場所の bin ディレクトリーに移動します。
6. 必要に応じてデータベースを始動します。
7. bash シェルまたは sh シェルを開始します。
8. tmp.sh ファイルに対して source コマンドを実行します (「source tmp.sh」と入力)。
9. com.sterlingcommerce.security.ocsp.SCICertAuthority クラス内のユーティリティーを使用して、認証局を作成します。
10. com.sterlingcommerce.security.ocsp.SCIOCSPResponder クラス内のユーティリティーを使用して、OCSP 応答者を作成します。
11. この認証局の証明書または個別の証明書を更新して OCSP を有効にします。
    com.sterlingcommerce.security.ocsp.SetAuthorityCertificatesOCSPInfo ユーティリティーは、任意の認証局のすべてのトラステッド証明書とシステム証明書を構成します。
    com.sterlingcommerce.security.ocsp.SetSystemCertificateOCSPInfo ユーティリティーは、1 つのシステム証明書を構成します。
    com.sterlingcommerce.security.ocsp.SetTrustedCertificateOCSPInfo ユーティリティーは、1 つのトラステッド証明書を構成します。

## OCSP 構成のスクリプト

以下のスクリプトは、OCSP 構成ユーティリティーを実行するために OCSP ホット・フィックスに組み込まれています。各スクリプトには、UNIX/Linux バージョンと Windows バージョンがあります。これらのスクリプトは、これらのスクリプトによって呼び出されるユーティリティー・プログラムと同じコマンド・ライン引数を受け取ります。これらのスクリプトは、製品のインストール・ディレクトリーの bin ディレクトリーに配置されています。これらのスクリプトについて説明しているこのセクションでは、コマンド・ライン引数に関する情報は基本的に繰り返されているだけです。

### ManageCertAuthority.sh と ManageCertAuthority.cmd

| 引数 | 説明 |
|---|---|
| -a、-r、-d | 実行する操作:<br><br>-a 追加<br><br>-l 一覧表示<br><br>-d 削除<br><br>–l オプションには、追加の引数はありません。 –d オプションでは、単一の引数として、削除するレコードのオブジェクト ID を指定します。 |
| Name | 認証局の名前。-a では必須。 |
| Modified_by | ID を変更または作成したユーザー。 -a では必須。 |
| Hash_alg | 認証局のハッシュ・アルゴリズム。サポートされている値は SHA1 のみです。-a では必須。 |
| Certificate_id | 認証局と関連付けられた CA 証明書のオブジェクト ID。-a では必須。 |

| | |
|---|---|
| OCSP_policy | 認証局の OCSP ポリシー・ストリング。これは、CERT_AUTHORITY 表のセクションで説明しているのと同じコンマ区切りストリングです。-a では必須。<br><br>このストリングの 1 つ目の要素としては、以下を指定できます。<br>• never – OCSP を一切使用しません。<br>• resp – 要求の発行時に応答者が構成されている場合にのみ OCSP を使用します。<br>• always – 要求の発行時に常に OCSP を使用します。この値を指定した場合は、応答者が構成されていることが必要であり、応答者が構成されていない場合は証明書チェックは不合格になります。<br><br>このストリングの 2 つ目の要素としては、以下を指定できます。<br><br>**OCSP What**<br>• none – どの証明書も一切チェックしません。<br>• end-user - エンド・ユーザー証明書のみをチェックします。<br>• both – エンド・ユーザー証明書と中間証明書の両方をチェックします。現在はサポートされていません。<br><br>例:<br>• never,none<br>• always,end-user |
| Crl_policy | 認証局の CRL ポリシー・ストリング。 -a では必須。この引数には 1 つの値が必要ですが、この引数は現在は使用されていません。"None" という値を指定できます。 |
| Object_ID | このレコードの作成時に使用するオブジェクト ID。-a では任意指定。 |

## ManageOCSPResponder.sh と ManageOCSPResponder.cmd

| 引数 | 説明 |
|---|---|
| -l | 現在構成されている OCSP 応答者のリストを取得します。<br><br>このオプションには、追加の引数はありません。 |

| | |
|---|---|
| -d | 応答者構成データの指定されたオブジェクト ID を持つ構成済み OCSP 応答者を削除します。<br><br>このオプションは、追加の引数として object_id を受け取ります。 |
| -u2 | データベース内の既存のレコードを、認証局証明書の公開鍵と認証局証明書のサブジェクト DN に関する正しい情報によって更新します。<br><br>これは、認証局と OCSP 応答者の両方のすべての既存レコードに対して実行される必要があります。そうしない場合は、これらのレコードを削除および再作成して、適切な情報をデータベース内に取り込む必要があります。<br><br>このオプションは、追加の引数として object_id を受け取ります。 |
| -a | 指定された認証局によって発行された証明書の状況を確認するために使用される、新しい OCSP 応答者の構成データを追加します。<br><br>追加の引数は、name、 modified_by、 hash_alg、 authority_cert_oid、 response_signing_cert_oid、 resp_signing_cert_in_ca_store、 cache_ttl、 trans_prof_oid、 comm_bp、 comm_wait、 send_nonce、 require_nonce、および object_id です。 |
| name | (-a では必須) 認証局の名前。 |
| modified_by | (-a では必須) ID を変更または作成したユーザー。 |
| hash_alg | (-a では必須) 認証局のハッシュ・アルゴリズム。サポートされている値は SHA1 のみです。 |
| authority_cert_oid | (-a では必須) 認証局と関連付けられた CA 証明書のオブジェクト ID。 |
| response_signing_cert_oid | (-a では必須) OCSP サービスのプロバイダーが証明書の状況を通知する応答に署名するために使用した証明書のオブジェクト ID。この証明書は、CA デジタル証明書ストアまたはトラステッド・デジタル証明書ストアに追加される必要があります。これは、ストアに表示されるのと同じ証明書のシステム証明書 ID です。 |

| | |
|---|---|
| resp_signing_cert_in_ca_store | (-a では必須) response_signing_cert_oid 引数の 1 つ前の値が Sterling B2B Integrator 内の CA デジタル証明書ストア内で見つかったかどうかを示すフラグ。 |
| cache_ttl | (-a では必須) 内部キャッシュ内の OCSP 応答の存続時間 (秒単位)。 |
| trans_prof_oid | (-a では必須) OCSP 応答者との通信用に構成されたトランスポートのオブジェクト ID。 |
| comm_bp | (-a では必須) OCSP 応答者と通信するために使用するビジネス・プロセスの名前。これは、HTTP 通信を実行するビジネス・プロセスである必要があります。このビジネス・プロセス内のサービスは、送信時および受信時のそれぞれで、HTTP ヘッダーの要求もしなければ HTTP ヘッダーの提示もしないように構成されている必要があります。システムに付属している HTTPClientSend プロセスを使用することが可能であり推奨されます。 |
| comm_wait | (-a では必須) 応答者との通信を待つ秒数。この秒数を経過するとエラーが発生していると見なされます。 |
| send_nonce | (-a では必須) nonce 値が OCSP サービスに送信されるかどうかを指定します。nonce 値は、一部の OCSP プロバイダーによるリプレイ・アタックを防止するために使用されます。 |
| require_nonce | (-a では必須) サーバーから OCSP サービスに対して、応答内に nonce 値を含めることを要求するかどうかを指定します。 |
| object_id | (-a では必須) このレコードの作成時に使用するオブジェクト ID。 |

## SetSystemCertOCSPInfo.sh と SetSystemCerOCSPInfo.cmd

このユーティリティーは、単一のシステム証明書についてデータベース内の OCSP 情報を設定します。

| 引数 | 説明 |
|---|---|
| -o、-n | 2 つ目の引数をどのように解釈するかを指定します。<br><br>-o: オブジェクト ID として解釈<br><br>-n: 名前として解釈 |
| Object_ID/Name | 1 つ目の引数で指定した値に応じて、認証局のオブジェクト ID または名前を指定します。 |

### SetSystemCertOCSPInfo.sh と SetTrustedCertOCSPInfo.cmd

このユーティリティーは、単一のシステム証明書についてデータベース内の OCSP 情報を設定します。

| 引数 | 説明 |
|---|---|
| -o、-n | 2 つ目の引数をどのように解釈するかを指定します。<br><br>-o: オブジェクト ID として解釈<br><br>-n: 名前として解釈 |
| Object_ID/Name | 1 つ目の引数で指定した値に応じて、認証局のオブジェクト ID または名前を指定します。 |

## OCSP スクリプトの実行

以下の例は、OCSP 構成スクリプトの実行方法を示しています。これらのスクリプトの前提条件として、認証局の CA 証明書をチェックイン済みであること、データベースが始動されていること、Sterling B2B Integrator のインストール先の bin ディレクトリーが現行ディレクトリーであること、および bin ディレクトリー内の tmp.sh ファイルに対して source コマンドを実行済みであることが必要です。

### このタスクについて

認証局の CA 証明書のオブジェクト ID を取得したら、Sterling B2B Integrator の「管理メニュー」から、「取引パートナー」>「デジタル証明書 - **CA**」を選択します。証明書を選択します。「証明書のサマリー」ダイアログ・ボックスが開いて、証明書のオブジェクト ID を含む証明書情報が表示されます。

OCSP スクリプトを実行するには、以下のステップを実行します。OCSP スクリプト・コマンドの完全なリストについては、 93 ページの『OCSP 構成のスクリプト』を参照してください。

### 手順

1. 次のようなコマンドを実行して、システム内で認証局を作成します。

   ```
   ./ManageCertAuthority.sh -a VPCA admin SHA1 "sedna:a1807c:11dc6d53ba4:-7b4b"
    "always,end-user" "none"
   ```

2. 認証局を作成して、OCSP 応答者との通信用のプロファイルを作成したら、次のようなコマンドを実行して、システム内で OCSP 応答者を作成します。

   ```
   ./ManageOCSPResponder.sh -a CertAuth_TestOCSP admin SHA1
   "kenny:node1:13727b3f8e4:29762" "kenny:node1:13727275fd9:40698" false (use
   true if the checked in signing certificate
   is the same from the responding certificate, that is, checked in to the
   certificate authority in step 3) "2400" "14ffd4a0:1371823040d:-77c8"
   HTTPClientSend 3600 false false
   ```

3. 次のようなコマンドを実行して、システム内のすべての認証局を一覧表示します。

   ```
   ./ManageCertAuthority.sh -l
   ```

   各認証局の戻り出力が次のように表示されます。

```
CERT_AUTHORITY:
OBJECT_ID: sedna:1ded0fd:11dc9d22929:-7fbd
NAME: VPCA
CREATE_DATE: 2008-11-23
MODIFIED_DATE: 2008-11-23
MODIFIED_BY: null
ISSUER_NAME: Country=US, StateOrProvince=Dublin, OrganizationUnit=GIS
 Development, Organization=Sterling,
CommonName=Test CA
HASH_ALG: SHA1
RDN_HASH: 24E63F8AE9F51497529EA0CC34467A4680737A9F
ENCODED_RDN_HASH: JOY/iun1FJdSnqDMNEZ6RoBzep8=
KEY_HASH: C96F2FF442EBFA07672DCEC49B729D4D24898313
ENCODED_KEY_HASH: yW8v9ELr+gdnLc7Em3KdTSSJgxM=
CERT_OID: sedna:a1807c:11dc6d53ba4:-7b4b
OCSP_WHEN_POLICY: always
OCSP_WHAT_POLICY: end-user
CRL_POLICY: null
```

4. 次のようなコマンドを実行して、この認証局によって発行されたすべてのシステム証明書とすべてのトラステッド証明書に対して OCSP を有効にします。

```
./SetAuthorityCertsOCSPInfo.sh -o sedna:1ded0fd:11dc9d22929:-7fbd yes
```

## OCSP チェックのロジック

次の手順では、Sterling B2B Integrator での OCSP チェックのロジックを説明しています。証明書状況が OK の場合は、OCSP チェックは合格です。そうでない場合は、OCSP チェックは不合格です。

### 手順

1. 存続時間が満了していない既存の応答が見つかった場合は、その応答は OCSP 応答として使用されます。
2. キャッシュ内で既存の応答が見つからない場合や、キャッシュ内の応答の存続時間が満了している場合は、OCSP 要求が作成されます。
3. システムが OCSP 要求を作成した場合は、システムは OCSP 応答者向けに構成されたビジネス・プロセスを実行して、その要求を送信して応答を取得します。応答者が nonce 値を送信してもらうように構成されていた場合は、要求には nonce 値が格納されます。
4. ビジネス・プロセスが正常に完了した場合は、システムはそれ自体の 1 次ドキュメントを OCSP 応答として解析しようとします。OCSP 要求の送信と OCSP 応答の受信のために使用されるビジネス・プロセスは、応答から HTTP ヘッダーを削除します。
5. 1 次ドキュメントを OCSP 応答として解析できる場合は、システムは応答の状況を確認します。
6. 要求によって有効な応答が生成されたことが応答状況によって示されている場合は、システムは、OCSP 応答者用に構成された証明書を使用して OCSP 応答の署名を検証しようとします。
7. この署名が検証されて、応答者が nonce を要求するように構成されていた場合は、システムは応答から nonce を取得して確認しようとします。
8. 他のすべての検証に合格した場合は、システムは、要求が生成されて送信された対象である証明書の証明書状況情報を探します。
9. 状況情報が見つかった場合は、システムは、証明書の既存の OCSP 応答のために内部キャッシュを更新します。

# 連邦情報処理標準 (FIPS)

## 連邦情報処理標準 (FIPS) 140-2

FIPS 200 のセキュリティー要件に準拠するには、アプリケーションで使用する暗号モジュールは、暗号モジュール評価プログラム (Cryptographic Module Validation Program) によって認定されていること、および FIPS 140-1 または FIPS 140-2 に準拠していることが必要です。

認定された暗号方式をアプリケーションで使用するための最小要件は次のとおりです。

- すべての暗号処理 (鍵の生成を含む) は、認定された暗号モジュールによって実行されること。
- 承認済みのセキュリティー機能のみが許可されていること。
- 承認済みの鍵確立技法のみが許可されていること。

## Sterling B2B Integrator での FIPS 140-2

Certicom Government Service Edition (GSE) は、Sterling B2B Integrator に付属している FIPS 140-2 レベル 1 の認定済み暗号モジュールです。GSE は、Java で低レベル暗号ツールキットであり、未承認のセキュリティー機能を含むさまざまなセキュリティー機能を実装しています。

FIPS モードの場合は、次の処理を実行します。

- GSE FIPS 状態マシンを有効化して、電源オン自己診断テストを実行します。
- 暗号関連の関数呼び出しをコア・システムから GSE に転送します。

## インストール時の FIPS の有効化

新規インストール時に、FIPS モードで実行するかどうかを尋ねられたら、「TRUE」を選択します。

## FIPS モードの手動での有効化

Sterling B2B Integrator のインストール後に、FIPS モードを手動で有効にできます。開始する前に、FIPS モードで動作するためのライセンスを取得していることを確認してから、このモードを有効にしてください。ライセンスは始動時に検査され、FIPS モードが有効になっていてもライセンス交付されていない場合は始動しません。

### このタスクについて

FIPS モードを手動で有効にするには、以下を実行します。

### 手順

1. /*install_dir*/properties/. に移動します。
2. security.properties ファイルを探します。
3. テキスト・エディターで security.properties ファイルを開きます。security.properties ファイルに変更を加えた場合は、必ず security.properties.in ファイルにも同じ内容の変更を加えてください。これにより、カスタマイズした

設定が上書きされることが防止されます。プロパティー・ファイルを直接編集する代わりに、このセキュリティー・プロパティー・ファイルを使用して FIPS をカスタマイズしてください。

4. 「FIPSMode=true」という構成を指定します。
5. security.properties ファイルを保存して閉じます。
6. Sterling B2B Integrator を再始動します。これは、変更内容がシステムで認識されるために必要です。

## FIPS モードの無効化

FIPS モードは手動で無効にできます。

### このタスクについて

FIPS モードを手動で無効にするには、以下を実行します。

### 手順

1. */install_dir*/properties/. に移動します。
2. security.properties ファイルを探します。
3. テキスト・エディターで security.properties ファイルを開きます。
4. 「FIPSMode=false」という構成を指定します。
5. security.properties ファイルを保存して閉じます。
6. Sterling B2B Integrator を再始動します。 これは、変更内容がシステムで認識されるために必要です。

---

# 「プロキシー・サーバー」

## プロキシー・サーバー

プロキシー・サーバーは、システムのセキュリティーを高めます。

## HTTP プロキシー・サーバーの構成

「管理」メニューから、HTTP プロキシー・サーバーを構成できます。

### このタスクについて

HTTP プロキシー・サーバーを構成するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「操作」 > 「プロキシー・サーバー」を選択します。
2. 「追加 **(Add)**」をクリックします。
3. プロキシー・サーバーの「名前」を入力します。
4. 「タイプ」として「**HTTP**」を選択します。
5. 「ホスト」名を入力します。 IPv6 アドレスは、大括弧で囲む必要があります。
6. 「ポート」番号を入力します。

7. 「再試行回数」を入力します。
8. 「次へ **(Next)**」をクリックします。
9. ユーザーに基本認証を要求するには、以下を実行します。
   - 「はい」を選択し、「次へ **(Next)**」をクリックします。
   - 「いいえ」(デフォルト) を選択した場合は、「次へ **(Next)**」をクリックしてステップ 13 に進みます。
10. 「認証ユーザー **ID**」を入力します。
11. 「認証パスワード」を入力します。
12. 「次へ **(Next)**」をクリックします。
13. このプロキシー・サーバーの設定内容を確認します。
14. 「終了」をクリックします。

## SSP プロキシー・サーバーの構成

「管理」メニューから、SSP プロキシー・サーバーを構成できます。

### このタスクについて

SSP プロキシー・サーバーを構成するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「操作」 > 「プロキシー・サーバー」を選択します。
2. 「追加 **(Add)**」をクリックします。
3. プロキシー・サーバーの「名前」を入力します。
4. 「タイプ」として「**SSP**」を選択します。
5. 「ホスト」名を入力します。 IPv6 アドレスは、大括弧で囲む必要があります。
6. 「ポート」番号を入力します。
7. 「再試行回数」を入力します。
8. 「次へ **(Next)**」をクリックします。
9. 「ユーザーに基本認証を要求する (Is basic authentication required for the user)」で、「はい」または「いいえ」を選択します。
10. 「SSL が必要」で、「はい」または「いいえ」を選択します。
11. 「次へ **(Next)**」をクリックします。
12. このユーザーに対して基本認証を要求することを選択した場合は、「認証ユーザー **ID**」と「認証パスワード」を入力して、「次へ **(Next)**」をクリックする必要があります。 基本認証を要求しなかった場合は、このページは表示されません。
13. 「SSL が必要」で「はい」を選択した場合は、「暗号強度」、「**CA** 証明書」、および「鍵証明書」を選択して、「次へ **(Next)**」をクリックします。「SSL が必要」で「いいえ」を選択した場合は、このページは表示されません。
14. 「次へ **(Next)**」をクリックします。

15. このプロキシー・サーバーの設定内容を確認します。
16. 「終了」をクリックします。

## SSL 用プロキシー・サーバーの構成

SSL 証明書を作成するかインポートして、適切なアダプター構成内の「**SSL** の使用」フィールドを「必須」に設定することで、SSP プロキシー・サーバー構成で SSL を使用できます。

### このタスクについて

SSP プロキシー・サーバーの構成で SSL を使用する場合は、次の操作を実行する必要があります。

### 手順

1. SSL 証明書を作成するか、Sterling B2B Integrator 内の認証局から証明書をインポートします。
2. 適切なアダプター構成内の「**SSL** の使用」フィールドを「必須 **(Must)**」に設定します。

## プロキシー・サーバーの編集

「管理」メニューから、プロキシー・サーバー構成を編集できます。

### このタスクについて

プロキシー・サーバー構成を編集するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「操作」 > 「プロキシー・サーバー」を選択します。
2. 編集するプロキシー・サーバーの「編集」をクリックします。
3. 必要に応じて各フィールドを更新します。
4. 「次へ **(Next)**」をクリックします。
5. このプロキシー・サーバーの設定内容を確認します。
6. 「終了」をクリックします。

## プロキシー・サーバーの削除

### このタスクについて

プロキシー・サーバーの構成を削除すると、Sterling B2B Integrator の一部の機能でエラーが発生する可能性があります。必要に応じて特定のアダプターやサービスを再構成して、これらが特定のプロキシー・サーバー構成がなくても正常に機能するようにしてください。

プロキシー・サーバー構成を編集するには、以下を実行します。

### 手順

1. 「管理メニュー」から、「操作」 > 「プロキシー・サーバー」を選択します。
2. 編集するプロキシー・サーバーの「編集」をクリックします。

3. このプロキシー・サーバーの設定内容を確認します。
4. 「削除」をクリックします。

# SSL

## Sterling B2B Integrator への SSL の実装について

Secure Sockets Layer (SSL) は、インターネットを介したセキュア通信を提供します。SSL では、対称暗号方式と非対称暗号方式の両方が使用されます。

SSL セキュリティー・プロトコルは、Sterling B2B Integrator におけるサーバー認証とクライアント認証を実現します。

- サーバー認証は、クライアントがサーバーに接続したときに実行されます。初期ハンドシェークの後に、サーバーは自身のデジタル証明書をクライアントに送信します。クライアントは、サーバーの証明書または証明書チェーンを検証します。
- クライアント認証は、ハンドシェーク時にサーバーが証明書要求をクライアントに送信したときに実行されます。クライアントの証明書またはチェーンが有効であることが確認されて、証明書検証メッセージが有効であることが確認された場合は、ハンドシェークはさらに続行されます。
- オプションの追加認証は、リバース DNS ルックアップによって得られるサーバーの完全修飾ドメイン名と証明書内の共通名を照合することで実行されます。

### 信頼のタイプ

Sterling B2B Integrator では、SSL 証明書に次の 2 つのタイプの信頼がサポートされています。

- CA 信頼 - 他の証明書を発行するために使用されるルート証明書に基づいた階層的信頼。これは標準の SSL 証明書信頼モデルです。
- 直接信頼 - セキュア・アウト・オブ・バンド・メカニズムを通じて配布されると想定される自己署名証明書の直接信頼。直接信頼と自己署名証明書は SSL 標準の一部ではありませんが、特定の取引コミュニティーでは頻繁に使用されます。

### SSL 証明書

SSL を使用して通信するには、サーバー認証またはクライアント/サーバー認証をサポートするように関連システムを構成します。サーバーに対する認証を実行するには、チェーン内の一連の中間証明書とルート CA 証明書が必要であり、またはサーバーで自己署名証明書が使用される場合は、その自己署名証明書のコピーが必要です。

クライアント/サーバー認証をサポートするには、CA 証明書または自己署名証明書と、システム証明書が必要です。

SSL 証明書をトラステッド CA から取得するには、その CA に証明書署名要求 (CSR) を送信します。SSL 証明書は、公開鍵と SSL サーバーまたは SSL クライアントをバインドします。

クライアント/サーバー認証を使用する予定の場合は、システム証明書を構成します。システム証明書は次の方法で作成できます。

- 既存の鍵証明書ファイルまたは PKCS12 ファイルをチェックインします。
- 自己署名システム証明書を生成します。
- 鍵管理ユーティリティー (iKeyman) を使用して、CSR を生成して、CA から証明書を取得します。iKeyman について詳しくは、 70 ページの『IBM 鍵管理ユーティリティー (iKeyman)』を参照してください。

### 暗号スイート

Sterling B2B Integrator を使用する前に、使用可能な定義済みの暗号リストを確認し、それらを会社のセキュリティー要件に応じてカスタマイズする必要があります。

IBM SDK、Java Technology Edition、バージョン 7 暗号スイートは、次のサイトにあります。http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/ciphersuites.html Sterling B2B Integrator でサポートされるその他の JDK については、JDK サプライヤーのドキュメンテーションで、サポートされる暗号スイートのリストを参照してください。

暗号強度は、`security.properties` または `customer_overrides.properties` 内に構成されます。使用できる暗号スイートのレベルは次のとおりです。

- AllCipherSuite (UI の選択は **ALL**) - WEAK と STRONG にリストされるすべてを含みます。
- WeakCipherSuite (UI の選択は **WEAK**) - Sterling B2B Integrator と共に使用したい、サポートされる WEAK の暗号スイートを追加します。
- StrongCipherSuite (UI の選択は **STRONG**) - Sterling B2B Integrator と共に使用したい、サポートされる STRONG の暗号スイートを追加します。
- CipherSuiteDefault (V5.2.6 以上で使用可能) - デフォルトで、IBM JDK7 でサポートされる暗号のサブセットを含みます。 WeakCipherSuite と StrongCipherSuite が空の場合に使用されます。

## SSL のクライアント・アダプター

FTP クライアント・アダプター、HTTP クライアント・アダプター、および Sterling Connect:Direct® FTP+ リクエスター・アダプター (Secure+ オプション付き) では SSL がサポートされます。

次のクライアント・アダプターは SSL をサポートしています。

- FTP クライアント・アダプター
- HTTP クライアント・アダプター
- Sterling Connect:Direct FTP+ リクエスター・アダプター (Secure+ オプション付き)

SSL のパラメーターは、取引パートナー・プロファイルで設定することも、アダプターに対して設定することもできます。FTP クライアント・アダプターの場合は、これらのパラメーターは FTP クライアント・セッション開始サービスで設定されま

す。HTTP クライアント・アダプターの場合は、これらのパラメーターは HTTP クライアント・セッション開始サービスで設定されます。セッション開始サービスで設定されたパラメーターは、取引パートナー・プロファイル内の設定よりも優先されます。

次の表のパラメーターは、クライアントの観点から SSL を制御します。構成対象のアダプターやサービスの資料を参照してください。

| パラメーター | 説明 |
|---|---|
| SSL | SSL ソケット・ネゴシエーションを決定します。 |
| CACertificateId<br><br>(trusted_root) | トラステッド CA パブリック証明書のリスト。プロセス・データ内では、このパラメーターはオブジェクト ID として表示されます。 |
| CipherStrength | ソケット接続を介して伝送されるデータに適用する暗号化レベル。 |
| SystemCertificateId | 使用可能なシステム証明書のリストから選択します。この証明書は、クライアントの ID をサーバーに対して証明します。 |

## SSL のサーバー・アダプター

FTP サーバー・アダプター、HTTP サーバー・アダプター、Sterling Connect:Direct サーバー・アダプター (Secure+ オプション付き)、および SMTP 送信アダプターでは SSL がサポートされます。

次のサーバー・アダプターは SSL をサポートしています。

- FTP サーバー・アダプター
- HTTP サーバー・アダプター
- Sterling Connect:Direct サーバー・アダプター (Secure+ オプション付き)
- SMTP 送信アダプター

次の表のパラメーターは、サーバーの観点から SSL を制御します。構成対象のアダプターやサービスの資料を参照してください。

| パラメーター | 説明 |
|---|---|
| SSL | SSL が有効かどうかを制御します。 |
| Key Certificate Passphrase | サーバーの鍵証明書を保護するパスワード。このパスフレーズは、SSL ライブラリーを初期化するためにシステム内部で使用されます。 |
| CipherStrength | データの暗号化に使用されるアルゴリズムの強度。 |
| Key Certificate (System Store) | サーバー認証用の秘密鍵と証明書。 |
| CA Certificate | クライアントの証明書を検証するために使用される証明書 (存在する場合)。 |

## 証明書のチェックイン

クライアント/サーバー認証をサポートするには、CA 証明書または自己署名証明書と、システム証明書が必要です。

### このタスクについて

CA 証明書ストア内の CA 証明書または自己署名証明書をチェックインするには、「管理メニュー」から、「取引パートナー」 > 「デジタル証明書」 > 「**CA**」 > 「新規証明書のチェックイン **(Check in New Certificate)**」を選択します。

## テスト用の自己署名証明書の作成

テスト用に、自己署名証明書を使用できます。自己署名証明書は、Sterling B2B Integrator で生成して管理できます。

### このタスクについて

自己署名証明書を作成するには、以下のようにします。

### 手順

1. 「取引パートナー」 > 「デジタル証明書」 > 「システム証明書」 > 「自己署名証明書の作成 **(Create Self-Signed Certificate)**」を選択します。
2. 自己署名証明書を作成したら、その証明書を探して、ファイルにチェックアウトします。
3. この証明書を CA 証明書として Sterling B2B Integrator にチェックインして戻します。そのためには、「取引パートナー」 > 「デジタル証明書」 > 「**CA**」 > 「新規証明書のチェックイン **(Check In New Certificate)**」を選択します。

## SSL/TLS 再ネゴシエーション (V5.2.6 以降)

Sterling B2B Integrator は IBM JSSE パラメーターを使用して、SSL/TLS 再ネゴシエーションがどのように制限されるかを制御します。`security.properties` ファイルの以下のパラメーターを更新することができます。

| パラメーター名 | 定義 | 有効な値 |
| --- | --- | --- |
| **com.ibm.jsse2.<br>extended.<br>renegotiation.indicator** | このプロパティーを使用して、再ネゴシエーションだけでなく、すべてのネゴシエーションで RFC 5746 を必要とするように強制します。このネゴシエーションは、すべての必要な通信のパートナーが RFC 5746 を実装した後にのみ現実的となります。デフォルトの設定値は OPTIONAL です。 | 有効な値は次のとおりです。<br>• BOTH - IBM JSSE2 Server または IBM JSSE2 Client は、ピアで RFC 5746 再ネゴシエーションがサポートされていることが判明した場合にのみ接続します。注: プロパティーを BOTH に設定した場合、RFC 5746 をサポートするように更新されていないクライアントおよびサーバーでインターオペラビリティーの問題が発生します。<br>• CLIENT - IBM JSSE2 Client は、サーバーで RFC 5746 再ネゴシエーションがサポートされていることが判明した場合にのみ接続します。注: プロパティーを CLIENT に設定した場合、RFC 5746 をサポートするように更新されていないサーバーでインターオペラビリティーの問題が発生します。<br>• OPTIONAL - この設定値がデフォルトです。このオプションを使用することは、IBM JSSE2 Server および IBM JSSE2 Client は、初期ハンドシェーク中に再ネゴシエーション標識を必要としないことを意味します。<br>• SERVER - IBM JSSE2 Server は、クライアントで RFC 5746 再ネゴシエーションがサポートされていることが判明した場合にのみ接続します。注: プロパティーを SERVER に設定した場合、RFC 5746 をサポートするように更新されていないクライアントでインターオペラビリティーの問題が発生します。 |

| パラメーター名 | 定義 | 有効な値 |
| --- | --- | --- |
| **com.ibm.jsse2.renegotiate** | このプロパティーを使用して、IBM JSSE2 の再ネゴシエーションの能力を変更します。デフォルト値は NONE です。 | 有効な値は次のとおりです。<br>• ABBREVIATED - この設定値は優先され、セッションの継続性が証明されたときに、再ネゴシエーション中に無保護の簡略化されたハンドシェークができます。RFC 5746 再ネゴシエーションが許可されます。<br>• ALL - この設定値は優先され、再ネゴシエーション中に無保護の完全なハンドシェーク、および無保護の簡略化されたハンドシェークができます。RFC 5746 再ネゴシエーションが許可されます。<br>• DISABLED - この設定値は優先され、すべての無保護の RFC 5746 再ネゴシエーションを無効にします。<br>• NONE - この設定値がデフォルトです。無保護のハンドシェークの再ネゴシエーションは許可されません。RFC 5746 再ネゴシエーションのみ許可されます。 |

| パラメーター名 | 定義 | 有効な値 |
| --- | --- | --- |
| **com.ibm.jsse2.renegotiation.peer.cert.check** | このプロパティーを使用して、RFC 5746 で指定されているピア・サポートを必要とする IBM JSSE2 の再ネゴシエーションの能力を変更します。この要件は、すべての必要な通信のパートナーが RFC 5746 を実装した後にのみ現実的です。デフォルト値は OFF です。 | 有効な値は次のとおりです。<br>• OFF - この設定値がデフォルトです。これは、IBM JSSE2 Client および IBM JSSE2 Server が、ピアからの証明書に対して実行する識別検査を停止します。その結果、再ネゴシエーション中のピア証明書の変更が可能です。<br>• ON - この設定値では、IBM JSSE2 Client または IBM JSSE2 Server はピアからの証明書に対する比較を実行します。理由は、再ネゴシエーション中に証明書が変更されないようにするためです。比較は、保護と無保護の両方の再ネゴシエーションに適用できます。 |

## SSL のトラブルシューティング

エラー・メッセージが表示された場合は、SSL をトラブルシューティングできます。

### 壊れているか使用できない証明書のエラー・メッセージ

次のエラー・メッセージが表示される場合があります。

```
FATAL Alert:BAD_CERTIFICATE - A corrupt or unusable certificate was
received.
```

この場合の Perimeter ログ内の情報は次のとおりです。

```
ERROR <HTTPClientAdapter_HTTPClientAdapter_node1-Thread-19>
HTTPClientAdapter_HTTPClientAdapter_node1-Thread-172105824724com.
sterlingcommerce.perimeter.api.conduit.SSLByteDataConduit@4c2b95c6:
Doing reset3 c
om.certicom.net.ssl.SSLKeyException: FATAL Alert:BAD_CERTIFICATE -
A corrupt or unusable certificate was received.
 at com.certicom.tls.d.b.a(Unknown Source)
 at com.certicom.tls.d.b.do(Unknown Source)
```

この証明書をチェックインする際は、Sterling B2B Integrator の「ネーミング」画面に「無効な署名 (Invalid Signature)」というステータス値が表示されます。SSL を使用したアウトバウンド HTTP POST を実行するビジネス・プロセスが、HTTP メソッド・サービスで正常に実行されずにエラーが発生した場合は、次のメッセージが表示されます。

```
HTTP Status Code: -1
HTTP Reason Phrase: Internal Error: Connection was closed from the
perimeter side with error: CloseCode.CONNECTION_RESET
```

取引パートナーの適切な CA 証明書を取得します。取引パートナーが自己署名証明書を使用している場合は、その証明書自体を CA 証明書として使用できます。

## CA 信頼と直接信頼

Sterling B2B Integrator がクライアントである場合に、サーバー側で CA 発行の証明書が保有されており、その証明書の相対識別名 (RDN) というサブジェクト内にサーバーの DNS 名が含まれている場合は、ルート CA 証明書を CA ストアに配置して、その証明書を信頼できます。それでも SSL が機能しない場合は、直接信頼を試してください。サーバー証明書を CA ストアに配置して、その証明書を信頼します。

サーバーが自己署名証明書を使用している場合は、その証明書を CA ストアに配置して、その証明書を信頼します。この場合も、直接信頼を行っていることになります。

## 証明書なしの SSL の使用

必要な証明書やシステム証明書を持っていない場合は、SSL 対応のアダプターを使用できません。

## CBC ベースの暗号スイートを使用し SSL が機能しない場合

CBC モード暗号スイートを選択して SSL が機能しない場合は、CBC 保護をオフにする必要があります。

V5.2.5 以下の場合は、次の手順を実行します。

1. 編集するために tmp.sh ファイルを開きます。
2. 構成対象のオペレーティング・システムのサーバー・フラグを探して、次の値を追加します。

   ```
   -DDisableSSLEmptyRecords=true
   ```

3. 保存してファイルを閉じます。

V5.2.6 以上の場合は、次の手順を実行します。

1. *<B2Bi Install>*/bin ディレクトリーにおいて、Windows の場合は、InstallNoappsWindowsService.cmd.in と InstallContainerWindowsService.cmd.in を、その他のすべてのオペレーティング・システムの場合は、 tmp.sh_platform_ifcresources_ext.in を見つけます。
2. そのファイルを編集して、次のプロパティーのすべてのインスタンスを false に変更します。

   ```
   jsse.enableCBCProtection=true
   ```

3. setupfiles スクリプトを実行します。

## GPM の HTTPS 構成

SSL を介したセキュア HTTP アクセスは、Sterling B2B Integrator 内のほとんどの Web アプリケーションで、ベース HTTP ポート + 1 上でサポートされています。

この SSL 拡張機能によって、次のことが可能になります。

- グラフィカル・プロセス・モデラー (GPM) で HTTPS (SSL 暗号化機能付きの HTTP) を使用可能にします。
- ベース HTTP ポート上で Web アプリケーションを無効化したり別ポート (HTTPS を使用) にリダイレクトしたりできます。
- Web アプリケーションをセキュア HTTP サーバー・アダプター・インスタンス上にデプロイすることで、その Web アプリケーションへのセキュア・アクセスをサポートします。
- セキュリティー・リスクを低減します。

この機能を使用する場合は、グラフィカル・プロセス・モデラー (GPM) が HTTP の代わりに HTTPS を使用してダッシュボード Web アプリケーションと通信するように構成する必要があります。セキュア HTTP サーバー・アダプターを介してデプロイされた Web アプリケーションへのアクセスは、ベース・ポートを通じたアクセスよりも低速になる可能性があります。

注: V5.2.6 以上のデフォルト・セキュリティー・プロトコルは TLS 1.2 (ベース HTTP ポートの場合 + 1) です。. 必要に応じて、`properties_platform_ifcresources_ext` 内の **`jsseProtocol`** パラメーターを更新して、これを TLS 1.1 または TLS 1.0 に変更することができます。有効な値には、次のパラメーターが含まれます。

- **`TLS1-TLS1.1`** - TLS1.0 と TLS1.1 の場合
- **`TLS1.1-TLS1.2`** - TLS1.1 と TLS1.2 の場合
- **`TLS1`** - TLS1.0 のみの場合
- **`TLS1.1`** - TLS1.1 のみの場合
- **`TLS1.2`** - TLS1.2 のみの場合

## 新しい SSL パラメーター

拡張された SSL 機能をサポートするためにいくつかの新しいパラメーターが追加されました。これらのパラメーターを構成して、グラフィカル・プロセス・モデラー (GPM) とサーバーの間の SSL 通信を促進する必要があります。これらの新しいパラメーターは、両者それぞれのプロパティー・ファイルで設定する必要があります。

各自の環境用のすべてのカスタム・プロパティーは、customer_overrides.properties ファイルで設定する必要があります。そうすることで、アップグレード時やパッチのインストール時にそれらのプロパティーが上書きされることが防止されます。sandbox.cfg ファイルで設定されているプロパティーは、customer_overrides.properties ファイルで設定しないでください。これらのプロパ

ティーは customer_overrides.properties ファイル内では無視されるからです。customer_overrides.properties ファイルで設定されないプロパティーは、これらのプロパティーだけです。

次の表では、新しい SSL パラメーターを説明しており、各パラメーターが含まれているプロパティー・ファイルの名前を示しています。

| パラメーター名 | 定義 | プロパティー・ファイル |
| --- | --- | --- |
| WEBAPP_LIST_PORT | GPM クライアントがサーバーとの通信のために使用するポートを指定します。インストール時にはデフォルトであるベース・ポートに設定されます。<br><br>ダッシュボードと GPM の Web アプリケーションがセキュア HTTP サーバー・アダプター・インスタンスにデプロイされている場合は、このパラメーターを変更して、そのセキュア HTTP サーバー・アダプター・インスタンスのポートを指定する必要があります。<br><br>ベース SSL ポート (ベース HTTP ポート + 1) が GPM とダッシュボードのセキュア・デプロイのために使用されている場合は、このパラメーターを変更して、ベース SSL ポート (sandbox.cfg 内の SSL_PORT) を指定する必要があります。 | sandbox.cfg ファイル |
| WEBAPP_PROTOCOL | ダッシュボード Web アプリケーションとの通信のために使用するプロトコルを指定します (http/https)。 | sandbox.cfg ファイル |

| パラメーター名 | 定義 | プロパティー・ファイル |
| --- | --- | --- |
| SKIP_BASEPORT_<br>DEPLOYMENT_WARS | ベース・ポート上に war をデプロイする際にスキップする Web アプリケーションを指定します。このパラメーターでは、一連の war を .war 拡張子なしでコンマで区切って指定し、大文字と小文字が区別されます。<br><br>デフォルトでは、どの war もスキップされません。ダッシュボードと GPM の Web アプリケーションがセキュア HTTP サーバー・アダプターに正常にデプロイされたら、このパラメーターを =admin,dashboard,gbm という値に設定して、ベース・ポート上のこれらの Web アプリケーションへのアクセスを無効にしてもかまいません。Web アプリケーションの完全リストには以下が含まれます。<br>• myaft<br>• portlets<br><br>ALL という値をワイルドカードとして使用して、ベース HTTP ポート上にデプロイされたすべての war をスキップするように指定できます。ベース・ポートが外部アクセスに対してブロックされている場合は、この設定は不要である可能性があります。ALL という値は、他のどの値とも組み合わせて使用しないでください。 | customer_overrides.properties |
| HTTPS_REDIRECT_WARS | ベース HTTP ポートからセキュア HTTP サーバー・アダプターまたはベース SSL ポートに自動的にリダイレクトされる war を指定します。<br><br>ALL という値を使用して、ベース HTTP ポート上のすべてのスキップされる war を HTTPS_LIST_PORT (セキュア HTTP サーバー・アダプターまたはベース SSL ポート) にリダイレクトするように指定できます。<br><br>ALL という値は、他のどの値とも組み合わせて使用しないでください。 | customer_overrides.properties |
| HTTPS_LIST_PORT | ベース HTTP ポートに対して発行された要求のリダイレクト先ポートを指定します。セキュア HTTP サーバー・アダプターまたはベース SSL ポートの値に設定する必要があります。 | customer_overrides.properties |

| パラメーター名 | 定義 | プロパティー・ファイル |
| --- | --- | --- |
| HTTPS_CLIENT_CERTS | デフォルト・トラストストアに追加される必要のある公開鍵を持つ一連のシステム証明書をコンマで区切って指定します。これらの証明書は、ASI (application server-independent) サーバーからこのサーバー自体に対して HTTPS 呼び出しが発行された場合に、SSL ハンドシェーク時のクライアント・サイド検証のために使用されます。<br><br>このパラメーターを使用するには、**SubjectAltName** を持つサーバー証明書鍵が必要です。このパラメーターなしで既存の鍵を使用する場合は、この機能は正常に実行されずに、内容が不明なメッセージが出力されます。<br>**注:** ベース・ポート + 1 (sslCert) 上の HTTPS 用に構成された証明書は、トラストストアに自動的に追加されるため、このリストに追加する必要はありません。 | customer_overrides.properties |

この機能を構成する際に、SKIP_BASEPORT_DEPLOYMENT_WARS のみを設定して、HTTPS_REDIRECT_WARS と HTTPS_LIST_PORT を設定しなかった場合は、ベース・ポート上で Web アプリケーションにアクセスできなくなり、ユーザーは HTTPS ポートに自動的にリダイレクトされなくなります。セキュリティー上の理由からユーザーが自動リダイレクトされないことを希望する場合は、これは問題のない状況です。この場合でも、セキュア HTTP サーバー・アダプターまたはベース SSL ポート上でアクセスした場合は、Web アプリケーションを使用できます。

## HTTPS への自動リダイレクトの有効化

HTTPS への自動リダイレクトを有効にできます。

### このタスクについて

セキュア・ポート (HTTP サーバー・アダプターまたはベース SSL ポート) 上にデプロイされてベース・ポート上でスキップされる Web アプリケーションに対して、HTTPS への自動リダイレクトを構成することが可能になりました。これは必須の構成ではありませんが、強く推奨される構成です。

注: 各自の環境用のすべてのカスタム・プロパティーは、customer_overrides.properties ファイルで設定する必要があります。そうすることで、アップグレード時やパッチのインストール時にそれらのプロパティーが上書きされることが防止されます。

HTTPS への自動リダイレクトを有効にするには、以下を実行します。

### 手順

1. /<install_dir>/install/properties にナビゲートします。
2. customer_overrides.properties ファイルを開いて、次のパラメーター値を示されているとおりに設定します。

   ```
   HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
   HTTPS_LIST_PORT=<http_server_adapter_port or base_ssl_port>
   ```

   これらのパラメーターを構成することで、ユーザーは Web アプリケーションの HTTPS インスタンスに自動的にリダイレクトされるようになります。

   注: customer_overrides.properties ファイルは、デフォルト・システム・コードの一部ではありません。このファイルは、システムの初期インストールの後に作成される必要があるとともに、ご使用の環境に合わせて設定される必要があります。
3. 保存してファイルを閉じます。

### 実装例

以下に customer_overrides.properties ファイルの実装例を示します。

```
 ## Identifies wars for auto-redirect to the https port. Use comma-separated
## list to specify multiple wars
HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies the https port for the redirected wars. If specified, this
## should match the WEBAPP_LIST_PORT in sandbox.cfg
HTTPS_LIST_PORT=<http_server_adapter_port or base_ssl_port>
```

注: セキュア HTTP サーバー・アダプター・インスタンスを使用している場合は、この構成を使用すると、HTTPS_REDIRECT_WARS として指定されたすべての war が同じ HTTP サーバー・アダプター・インスタンス上にデプロイされることが必要になります。

## HTTPS_CLIENT_CERTS

セキュア HTTP サーバー・アダプター・インスタンスを使用している場合は、そのセキュア HTTP サーバー・アダプター・インスタンスを構成するために使用された SSL 証明書をトラステッド証明書リストに追加する必要があります。

この追加が必要な理由は、一部のダッシュボード画面では ASI サーバーへの逆方向 HTTPS 呼び出しが実行されるからです。これらの呼び出しによって SSL ハンドシェークを正常に完了するためには、当該証明書が ASI サーバー上のトラストストア内で構成されている必要があります。このためには、当該証明書の名前を HTTPS_CLIENT_CERTS リストで指定します。

これらのシステム証明書は、そのシステム証明書が作成されたときに代替名として指定された DNS 名と IP アドレスを持っている必要があります。JDK によって実行されるデフォルト SSL ホスト名検証では、SSL サーバーによって提供された証明書の名前が、http url で使用されているホスト名と一致すること、またはその証明書の SubjectAltName 属性で指定されたストリングのいずれかと一致することが要求されます。ダッシュボードの一部の画面は、SubjectAltName が構成されていない場合は正常に機能しません。

代替名は、システム証明書作成ウィザード (「取引パートナー」 > 「デジタル証明書」 > 「システム」) の「コンマ区切りの IP アドレス・リスト」フィールドと「コンマ区切りの DNS 名リスト」フィールドで構成します。

## GPM の HTTPS サポート

Java Web Start (JavaWS) は、HTTP を使用してグラフィカル・プロセス・モデラー (GPM) を起動するために使用されます。JavaWS は、HTTPS をサポートしているとともに、Web ブラウザーを使用した証明書の動的インポートをサポートしています。

SSL ハンドシェーク時に、サーバーは自身の証明書を提供して、JavaWS は信頼検証を処理します。この証明書を JavaWS によって検証できなかった場合は、その証明書を受け入れるか拒否するかを選択するためのプロンプトがユーザーに表示されます。SSL 証明書は、JavaWS によって自動的に検証できないため、ユーザーによって検証される必要があります。

### Java Web Start の証明書のインポート

Java Web Start (JavaWS) の動作時に、信頼されない証明書に関するプロンプトが表示されないようにするには、グラフィカル・プロセス・モデラー (GPM) を起動する前にそれらの証明書をローカル・マシン・ストアにインポートします。

#### このタスクについて

これにより、セキュア HTTP サーバー・アダプターまたはベース SSL ポートに関連付けられた SSL 証明書がユーザーのローカル・マシンによって信頼されない場合に、ユーザー側の混乱を低減できます。

トラステッド・ルート証明書を JavaWS にインポートするには、以下を実行します。

#### 手順

1. そのトラステッド・ルート証明書をローカル・コンピューター上のファイルに保存します。
2. ローカル・コンピューター上で「**Java** コントロールパネル」を開きます (`jre¥bin` 内の javaws.exe)。
3. 「セキュリティー」タブを開いて、「証明書」をクリックします。
4. 「インポート」をクリックして、トラステッド・ルート証明書を探して選択します。
5. 「開く」をクリックして、新しいトラステッド・ルート証明書をインポートします。 トラステッド・ルート証明書がチェックインされたら、JavaWS は SSL ハンドシェーク時にこのトラステッド・ルート証明書を使用して信頼検証を行います。

## ベース SSL ポートを使用した HTTP から HTTPS への切り替え

ベース SSL ポートを使用して HTTP から HTTPS に切り替えることができます。

## このタスクについて

ベース SSL ポートを使用して HTTP から HTTPS に切り替えるには、以下を実行します。

## 手順

1. /install_dir/install/properties に移動します。
2. sandbox.cfg ファイルを開きます。
3. 次のパラメーターを変更します。

   ```
   WEBAPP_PROTOCOL=https
   WEBAPP_LIST_PORT=<base_port + 1>
   ```

   これらのパラメーターは、グラフィカル・プロセス・モデラー (GPM) によってサーバーとの通信のために使用されます。
4. (オプション、推奨) ベース・ポート上のダッシュボードと GPM の Web アプリケーションへのアクセスを無効にして、HTTPS ポートへの自動リダイレクトを構成するには、customer_overrides.properties ファイルで次のパラメーターを指定します。

```
SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
HTTPS_LIST_PORT=<base_port + 1>
```

次に例を示します。

```
## Identifies the war files to be skipped during deployment on the base port.
## Use comma-separated list to specify multiple wars
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies wars for auto-redirect to the https port. Use comma-separated
## list to specify multiple wars
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies the https port for the redirected wars. If specified, this
## should match the WEBAPP_LIST_PORT in sandbox.cfg
noapp.HTTPS_LIST_PORT=<base_port + 1>
```

5. 保存してファイルを閉じます。
6. /install_dir/install/bin に移動します。
7. Sterling B2B Integrator を停止します。
8. 構成の変更内容を適用します。./setupfiles.sh と入力します。
9. 新しい構成をデプロイします。./deployer.sh と入力します。
10. Sterling B2B Integrator を開始します。
11. (オプション) ベース・ポート上のダッシュボードと GPM の Web アプリケーションへのアクセスを無効にした場合は (ステップ 4)、加えた変更内容を確認します。例えば、次のことを確認できます。
    - http://host:baseport/dashboard を通じたダッシュボード Web アプリケーションへのアクセスが不可能であるか、https://host:<base_port + 1>/dashboard に自動的にリダイレクトされる。

- http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp を通じた GPM Web アプリケーションへのアクセスが不可能であるか、https://host:<base_port + 1>/gbm/pmodeler/ProcessModeler.jnlp に自動的にリダイレクトされる。

## セキュア HTTP サーバー・アダプターを使用した HTTP モードから HTTPS モードへの切り替え

セキュア HTTP サーバー・アダプターを使用して HTTP モードから HTTPS モードに切り替えることができます。

### このタスクについて

HTTP モードから HTTPS モードに切り替えるには、以下を実行します。

### 手順

1. SSL が有効化された新しい HTTP サーバー・アダプター・インスタンスを作成します。次のパラメーターを示されているとおりに設定する必要があります。
   - 「ユーザー認証が必要」を「いいえ」に設定
   - 「**SSL** の使用」を「必要 **(Must)**」に設定
2. SSL が有効化された HTTP サーバー・アダプター・インスタンスへ必要な WAR ファイルをデプロイします。

   注**:** HTTP サーバー・アダプター・インスタンスを構成する際は、すべての WAR ファイルを `/install_dir/install/noapp/deploy` ディレクトリーから選択する必要があります。また、Admin Web アプリケーションのコンテキスト名は、`/install_dir/install/properties/sandbox.cfg` ファイル内の ADMIN_CONTEXT_PATH パラメーターの値と一致する必要があります。他のすべての Web アプリケーションについては、コンテキスト名は、.war 拡張子を省略した WAR ファイル名である必要があります。

   この操作が必要な理由は、パッチやホット・フィックスを通じて加えられた変更が、デプロイ済みの HTTP サーバー・アダプターに自動的に反映されるようにするためです。

   必要な WAR ファイルは次のとおりです。
   - admin.war
   - dashboard.war
   - gbm.war
   - myaft.war
   - portlets.war

   ユーザーによってダッシュボードに追加された新しい機能をサポートするために、追加の WAR ファイルが必要になることがあります。
3. sandbox.cfg ファイルを開き、以下のパラメーターを変更します。

```
WEBAPP_PROTOCOL=https
WEBAPP_LIST_PORT=<secure_http_server_adapter_port>
```

これらのパラメーターは、GPM によってサーバーとの通信のために使用されます。

4. (オプション、推奨) ベース・ポート上のダッシュボードと GPM の Web アプリケーションのデプロイを無効にするには、次のパラメーターを customer_overrides.properties ファイルで指定します。

```
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
noapp.HTTPS_LIST_PORT=<secure_http_server_adapter_port>
```

次に例を示します。

```
## Identifies the war files to be skipped during deployment on the base port.
## Use comma-separated list to specify multiple wars
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies wars for auto-redirect to the https port.
## Use comma-separated list to specify multiple wars
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies the https port for the redirected wars.
## If specified, this should match the WEBAPP_LIST_PORT in sandbox.cfg
noapp.HTTPS_LIST_PORT=<secure_http_server_adapter_port>
```

5. この機能に別の証明書を使用したい場合は、/install_dir/install/properties/customer_overrides.properties を変更して、*noapp.sslCert={mention_name_of_your_own_cert}* の行を追加します。別の証明書を指定しないと、この機能は ASISslCert を使用します。
6. (オプション) HTTPS のようなセキュア・プロトコルを使用してブラウザーから Cookie を送信するには、/install_dir/install/properties にナビゲートして、次のパラメーターを customer_overrides.properties ファイルで指定します。

   ```
   ## sending cookies as secure over https
   http.useSecureCookie=true
   ```

7. /install_dir/install/bin に移動します。
8. Sterling B2B Integrator を停止します。
9. 構成の変更内容を適用します。./setupfiles.sh と入力します。
10. 新しい構成をデプロイします。./deployer.sh と入力します。
11. Sterling B2B Integrator を開始します。
12. 11. https://host:<*secure_http_server_adapter_port*>/dashboard にアクセスして、HTTP サーバー・アダプターを通じてダッシュボード Web アプリケーションにアクセスできることを確認します。
13. https://host:<*secure_http_server_adapter_port*>/gbm/pmodeler/ProcessModeler.jnlp にアクセスして、セキュア HTTP サーバー・アダプターを通じて GPM Web アプリケーションにアクセスできることを確認します。
14. 保存してファイルを閉じます。
15. ベース・ポート上のダッシュボードと GPM の Web アプリケーションのデプロイを無効にした場合は (ステップ 4)、次のことを確認します。
    - http://host:baseport/dashboard を通じたダッシュボード Web アプリケーションへのアクセスが、 https://host:<*secure_http_server_adapter_port*>/dashboard に自動的にリダイレクトされる。

- http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp を通じた GPM Web アプリケーションへのアクセスが、https://host:<*secure_http_server_adapter_port*>/gbm/pmodeler/ProcessModeler.jnlp に自動的にリダイレクトされる。

## HTTPS モードから HTTP モードへの切り替え

HTTPS モードから HTTP モードに切り替えることができます。

### このタスクについて

HTTPS モードから HTTP モードに切り替えるには、以下を実行します。

### 手順

1. /install_dir/install/properties に移動します。
2. **sandbox.cfg** ファイルを開きます。
3. 次のパラメーターを変更します。

```
WEBAPP_PROTOCOL=http
WEBAPP_LIST_PORT=<base_port>
```

4. 保存してファイルを閉じます。
5. (オプション) HTTPS モードへの切り替え時に、ベース・ポート上のダッシュボードと GPM の Web アプリケーションのデプロイが無効化された場合は、customer_overrides.properties ファイルを開いて、次のパラメーターをコメント化して、これらのパラメーターが適用されないようにする必要があります。

```
## SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## HTTPS_LIST_PORT=<http_server_adapter_port>
```

6. (オプション) ファイルを保存して閉じます。
7. /install_dir/install/bin に移動します。
8. Sterling B2B Integrator を停止します。
9. 構成の変更内容を適用します。./setupfiles.sh と入力します。
10. 新しい構成をデプロイします。./deployer.sh と入力します。
11. Sterling B2B Integrator を開始します。
12. 以下を検証します。
    - ダッシュボード Web アプリケーションには、http://host:baseport/dashboard を通じてアクセスできます。
    - GPM Web アプリケーションには、http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp を通じてアクセスできます。
13. (オプション) SSL に対応した HTTP サーバー・アダプター・インスタンスから Web アプリケーションをアンデプロイします。

# ハードウェア・セキュリティー・モジュール (HSM) V5.2.3 - 5.2.5

## ハードウェア・セキュリティー・モジュール (HSM)

HSM は、暗号鍵を生成、保管、および保護するためのハードウェア・ベースのセキュリティー装置です。システム証明書は、Sterling B2B Integrator を使用してデータベースに保管することも、HSM に保管することもできます。

Sterling B2B Integrator は、次の HSM 装置をサポートしています。

- SafeNet Eracom ProtectServer Orange External
- ProtectServer Gold PCI 装置

HSM を使用して次のことを実行できます。

- HSM 上のシステム証明書の作成
- Sterling B2B Integrator からのシステム証明書のインポート
- Sterling B2B Integrator からのシステム証明書のエクスポート
- HSM からのシステム証明書の削除
- HSM 上の証明書のシステム証明書詳細の表示

## HSM をサポートするための Sterling B2B Integrator の機能

それぞれの鍵ペアと証明書について 1 つのエントリーが、Sterling B2B Integrator によって CERTS_AND_PRI_KEY 表内に保管されます。

このエントリーには、次の情報が含まれています。

- 鍵と証明書。これには、有効期間、シリアル番号、使用上の制約事項、およびその鍵や証明書に実際にアクセスすることなくユーザーに表示するために UI で使用される発行者と件名が含まれます。
- システムで検索時に使用される識別名の正規化
- レコードに対する変更内容
- 証明書の失効ステータス情報
- 鍵ストアのタイプ
- DATA_TABLE に保管されているバイナリー鍵ストア・オブジェクトへの参照。ソフトウェア鍵ストアが使用されている場合は、参照先のオブジェクトには鍵データが含まれていることがあります。HSM の場合は、参照先のオブジェクトには参照情報 (nCipher) またはプレースホルダー (Eracom) が含まれています。

## HSM 上のシステム証明書のパラメーター

次の表では、CreateSystemCert コマンド、ImportSystemCert コマンド、および ExportSystemCert コマンドのパラメーターを説明しています。

| パラメーター | 説明 |
|---|---|
| autogen | システム側で生成された情報を使用して鍵と鍵ストアへのアクセスを制御するのかどうかを指定します。HSM 上の鍵については false に設定する必要があります。 |

| パラメーター | 説明 |
| --- | --- |
| alias | HSM に保管されている鍵名。別名は、大文字/小文字の英字、数字、またはハイフン (-) で構成されており、その全体の長さはシステム GUID の長さ以下である必要があります。 |
| Certtype | インポートする証明書タイプ。サポートされている証明書ファイルのタイプは、pkcs12、pkcs8、pem、および keystore の 4 タイプです。Sterling B2B Integrator でサポートされているのは、DES または 3DES で暗号化された pem 鍵のみです。鍵ストアを一覧表示またはインポートするには、keystore を使用します。 |
| certname | Sterling B2B Integrator のデータベース内の証明書に割り当てる名前。 |
| file | インポートする Keycert ファイルまたは PEM ファイル。 |
| keyname | 作成する Sterling B2B Integrator システム鍵の名前。 |
| keypass | 鍵ストアが配置されている SafeNet Eracom HSM を保護しているトークンの PIN。 |
| key passphrase | 秘密鍵のパスフレーズ。この値は、コマンド・ライン上で省略可能です。この値を指定しなかった場合は、この値を求めるプロンプトが表示されます。鍵ストアが配置されている SafeNet Eracom HSM 上のトークンの PIN。 |
| keysize | RSA モジュラスの長さ (ビット単位)。有効な値は 768、1024、2048、3072、および 4096 です。 |
| keystoretype | インポートする鍵ストア・タイプ。有効な値は CRYPTOKI です。 |
| keystoreprovider | プロバイダー・タイプ。SafeNet Eracom は、HSM でサポートされている唯一のプロバイダー・タイプです。デフォルトのスロット 0 以外のスロットに証明書をインポートする場合は、ERACOM または ERACOM.n です。 |
| keytype | 公開鍵のアルゴリズム。RSA が唯一のサポートされているアルゴリズムです。 |
| ObjectID | システム証明書の ID。 |
| pkcs12file | インポートする pkcs12 ファイル。 |
| password | keycert ファイルまたは PEM ファイルのストア・パスフレーズ。 |
| pkcs12storepass | PKCS12 ファイルのストア・パスフレーズ。 |
| pkcs12keypass | PKCS12 ファイル内の秘密鍵を暗号化するために使用される鍵パスフレーズ。 |
| provider | 鍵ストア・タイプのプロバイダー。デフォルトのスロット 0 以外のスロットに証明書をインポートする場合は、ERACOM または ERACOM.n です。 |

| パラメーター | 説明 |
| --- | --- |
| rfc1779rdnsequence | 「識別名」ストリング・フィールドには、「有効な値」列で指定されたフィールドのいずれかが含まれています。「CN」フィールドのみが必須です。各フィールドをコンマで区切ってください。有効な情報:<br>• CN = 共通名<br>• O = 組織<br>• OU = 組織単位<br>• L = 場所<br>• ST = 都道府県<br>• C = 国 (2 文字の ISO3166-1 アルファ 2 コードを指定します) |
| storetype | 鍵ストア・タイプ。CRYPTOKI が唯一のサポートされている鍵ストア・タイプです。 |
| signingbit | 自己署名証明書の署名鍵使用ビットを設定します。有効な値は true または false です。 |
| serial | 証明書のシリアル番号。 |
| system passphrase | Sterling B2B Integrator のシステム・パスフレーズ。この値は、コマンド・ライン上で省略可能です。 |
| store passphrase | 鍵ストアにアクセスするためのパスフレーズ。鍵ストアが配置されている SafeNet Eracom HSM 上のトークンの PIN。この値は、コマンド・ライン上で省略可能です。 |
| systempass | Sterling B2B Integrator のシステム・パスフレーズ。 |
| storepass | 鍵ストアが配置されている SafeNet Eracom HSM を保護しているトークンの PIN。 |
| totrusttable | 証明書がトラステッド証明書表に追加されるかどうかを指定します。有効な値は true または false です。 |
| validityindays | 証明書の有効日数。 |

## SafeNet Eracom HSM

Sterling B2B Integrator で HSM を使用するには、Sterling B2B Integrator によって SafeNet Eracom HSM が使用および認識されるように構成する必要があります。

SafeNet Eracom HSM をインストールして設定するには、ベンダーの指示に従ってください。その場合は、Java ランタイムをインストールする必要があります。ユーティリティーを設定および使用する際は、Sterling B2B Integrator の鍵が格納されるスロットのプロバイダーを使用します。SafeNet Eracom スロットの PIN を作成した後に、その PIN を変更しないでください。その PIN を変更すると、Sterling B2B Integrator は HSM 上の鍵にアクセスできなくなります。

SafeNet Eracom のアーキテクチャーでは、HSM が複数のスロットに分割されています。ベンダーの指示に従って、カードまたは HSM をインストールおよび構成してください。各スロットには、1 つのセキュリティー・プロバイダーが関連付けられており、個別の個人識別番号 (PIN) によって保護できます。HSM 上に Sterling B2B Integrator 用の別個スロットを作成して、そのスロットを固有の PIN によっ

て保護できます。デフォルト・スロット 0 のプロバイダーは ERACOM です。追加スロットのプロバイダーには、ERACOM.*n* という形式の名前が付けられます (*n* はそのスロットの番号)。対象装置を操作するために Java ランタイム・コンポーネントを使用できることを確認してください。

## Sterling B2B Integrator で SafeNet Eracom HSM を使用するための構成

Sterling B2B Integrator が SafeNet Eracom HSM を使用するように構成できます。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次の行を tmp.sh ファイルと tmp.sh.in ファイルに追加します。

   ```
   LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/Eracom/lib

   export LD_LIBRARY_PATH
   ```

3. ネットワーク・ベース・サーバーを構成する場合は、次の行を tmp.sh ファイルと tmp.sh.in ファイルに追加します。ここで、*network_device_IP_OR_hostname* は SafeNet Eracom ネットワーク・ベース・サーバーの IP アドレスまたは完全修飾ドメイン名です。

   ```
   ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname

   export ET_HSM_NETCLIENT_SERVERLIST
   ```

4. jprov.jar を /opt/Eracom/lib ディレクトリーから */install_dir*/install/jdk/jre/lib/ext ディレクトリーにコピーします。
5. 各セキュリティー・プロバイダーの定義を */install_dir*/install/bin/jdk/jre/lib/security/java.security ファイルに追加します。定義を追加するには、Certicom プロバイダーに割り当てられた番号を確認して、その番号に 1 を足した番号を SafeNet Eracom プロバイダーに割り当てます。SafeNet Eracom プロバイダーの後に識別された他のすべてのプロバイダーについては、security.provider の番号を 1 ずつ増やしていきます。

   ```
   security.provider.n=com.certicom.ecc.jcae.Certicom

   security.provider.n+1=au.com.eracom.crypto.provider.ERACOMProvider
   ```

   SafeNet Eracom HSM 上の 0 以外のスロットを使用している場合は、そのスロットを次のように指定します (*x* はそのスロットの番号です)。

   ```
   security.provider.n+1=au.com.eracom.crypto.provider.slotx.ERACOMProvider
   ```

6. TLSProviderPolicy を */install_dir*/install/properties/security.properties ファイルで定義します。
   - 対象のプロバイダーがスロット 0 で定義されている場合は、TLSProviderPolicy パラメーターの唯一のコメント化されていない行は以下であることを確認します。

```
TLSProviderPolicy= TLS:*:ECMQV:P:.CT;TLS:SIG:MD2withRSA:P:ERACOM;TLS:Cipher:RawRSA:P:ERACOM;TLS:*
:RSA:P:ERACOM;TLS:*:*:P:Certicom
```

- 対象のプロバイダーが 0 以外のスロットで定義されている場合は、TLSProviderPolicy パラメーターを次のように変更します (*x* は構成対象のスロットです)。

```
TLSProviderPolicy=TLS:*:ECMQV:P:.CT;TLS:SIG:MD2withRSA:P:ERACOM.x;TLS:Cipher:RawRSA:P:ERACOM.
x;TLS:*:RSA:P:ERACOM.x;TLS:*:*:P:Certicom
```

7. KeyStoreProviderKey コマンドを */install_dir*/install/properties/security.properties ファイルで定義します。
   - 対象のプロバイダーがスロット 0 で定義されている場合は、KeyStoreProviderMap が次のように定義されていることを確認します。

```
KeyStoreProviderMap=SCIKS,SCIKS,false,Certicom,Certicom,false;
nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true;CRYPTOKI,ERACOM, true,ERACOM,ERACOM,true
```

   - 対象のプロバイダーが 0 以外のスロットで定義されている場合は、KeyStoreProviderMap パラメーターを次のように変更します (*x* はそのスロット番号です)。

```
KeyStoreProviderMap=SCIKS,SCIKS,false,Certicom,Certicom,false;
nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true; CRYPTOKI,ERACOM.x,true,ERACOM.x,ERACOM.x,true
```

### サポートされている nCipher と SafeNet/Eracom のネットワーク装置と PCI 装置

Sterling B2B Integrator は現在、nCipher のサポートに加えて、Safenet/Eracom ProtectServer Orange PCI カードおよび Orange External ネットワーク装置をサポートしています。

以下がサポートされています。

| 製造元 | サポートされている装置タイプ |
|---|---|
| nCipher | • nShield シリーズの PCI カード<br>• NetHSM ネットワーク装置 |
| Safenet/Eracom | • ProtectServer Gold PCI カード<br>• ProtectServer Orange PCI カード<br>• ProtectServer Orange External ネットワーク装置 |

## ハードウェア・セキュリティー・モジュールの使用

### HSM に保管するシステム証明書の作成

保管する自己署名システム証明書を HSM に作成できます。

### 始める前に

始める前に:

- Sterling B2B Integrator を停止します。
- Sterling B2B Integrator のデータベースが稼働していることを確認します。

### このタスクについて

HSM に保管する自己署名システム証明書を作成するには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。 `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase] [store passphrase] [key passphrase]`
3. コマンド・ラインでシステム・パスフレーズ、ストア・パスフレーズ、および鍵パスフレーズを入力しなかった場合は、これらの入力を求めるプロンプトが表示されます。

## HSM に保管されたシステム証明書の一覧表示

保管されたシステム証明書に関する情報を HSM に一覧表示できます。

### このタスクについて

HSM に保管されたシステム証明書に関する情報を一覧表示するには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。 `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

### 例

以下では、このコマンドの出力例を示しています。

```
Key exists with alias rayado-e5305c3-10d8f4bde7f--7fc1
Certificate Subject Info CN=test, OU=test, O=test, L=test, ST=Alabama, C=US
Certificate Issuer Info CN=Pythagoras, OU=System Verification, O=Sterling, L=Dublin,
ST=OH, C=US, EMAILADDRESS=caussuer@company.com
```

## HSM 上のシステム証明書の Sterling B2B Integrator データベースへのインポート

鍵と証明書が HSM 上に存在しており、Sterling B2B Integrator とは無関係にこれらの鍵と証明書が HSM に追加された場合は、この手順を使用します。HSM に保管されているシステム証明書を Sterling B2B Integrator で使用可能にするためには、そのシステム証明書の情報をデータベースにインポートする必要があります。

### このタスクについて

秘密鍵と証明書を HSM に追加するために使用される方法によっては、list 関数で、単一の鍵/証明書ペアについて重複するエントリーを表示することがあります。

システム証明書に関する情報をデータベースにインポートするには、そのシステム証明書の別名を知っている必要があります。

システム証明書をインポートするには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。 `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

## HSM に保管されたシステム証明書の削除

システム証明書を HSM から完全に削除できます。そのシステム証明書に含まれている秘密鍵データは復元できなくなります。

### このタスクについて

HSM に保管されたシステム証明書を削除するには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。 `./RemoveSystemCert.sh -r` *xxxx*

   ここで、*xxxx* は削除する証明書のオブジェクト ID です。

## システム証明書のエクスポート

Sterling B2B Integrator からシステム証明書をエクスポートして、それらを HSM にインポートできます。

### このタスクについて

HSM 上のシステム証明書は、ExportSystemCert.sh を使用してエクスポートすることはできません。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。 `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. パスフレーズを入力します。

## 例: HSM システム証明書

keycert、pkcs12、または pem のフォーマットで、システム証明書を HSM にインポートできます。システム証明書をインポートすると、鍵と証明書が HSM に追加されて、対応するエントリーが Sterling B2B Integrator のデータベース内に作成されます。

pem タイプの証明書と鍵をインポートする場合は、秘密鍵が DES 暗号化フォーマットまたは Triple-DES 暗号化フォーマットで作成されるようにしてください。

以下では、Triple-DES フォーマットで作成された pem 秘密鍵のサンプルを示しています。

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE0243B4833BD321
RtN+AFGTmx6EROcbo8fMXnMaRM/JcKIc3jbKYB5t6H6H5uvUrAmv+Si62QEtqg9V
x5r+GhiLcA9sdllKpnIXYg63Y+egn8DsxdGUCqnC+HDUlRVHX0NWKJ3FwXukr9iN
WP4MBr+NXMSETaBA0O0B4oSRCWvxelc2U2GItvUqJsOjLSILbahAgZk/j6LUDMy4
2FWoRtWZyGVz/gc+pN+bOwFHpbrZxd1YqZGRNKeZKTpXWslqxp5NDraBl1cmJ3vL
0RTnkwZnnyJ1Brc/WynlVfRK1gEEg8MPa3B9veat70ET/mLERuA4Ke8r0WAy5Y/w
7Yowicmwbo4q7RLVLm1ZmvPF4OXL8xIvaIUMOCW8/MNpanxZ4BB1CfTwQKQ9koJ7
9MT8K8ofu6V9TSK4Rw1cCpTKvattg/H72Ut39Yz185Ec+E8sV0BtilpqVsYSt1g6
lO805MqPym6gPo2NLpvk1iPLUZ1vIfthz+qb5cyXj1ng9aZSeRF/lytPLxSSy3LN
J9SZrnfHwbuhnyuQmco3SsCtYXnZ81cDHX+4O8sGqHA1zMwuqErorUvwxD6ZNnlc
DTmKIt826oows4Gtw48aEwjV4lk8FXQsWQjDWJHjFNNvGiyszPJjvPvM8zL1EwxO
mJFeNxBb0U3zgLs5aK/HHRn1/gzOBHwtr8bdFFBkpLoVGnbW+mRVxmJOvvPe7Zo+
sJXLEWC8Bm4klV8H6ynx6aQJ8a62HqbjPvShq1VH2I+1iwbyE3DzxY5sHrzZA2rb
dHabk3f0nBUvMegKI9Ye4ktLJf8yIQfsSBSJTEYXHqyx5ptoAEIlIQ==
-----END RSA PRIVATE KEY-----
```

# システム証明書ユーティリティーの管理

## HSM 上の鍵ペアと証明書署名要求

GenCSR ユーティリティーは、HSM 上に鍵ペアを生成して、その鍵ペア内の公開鍵を使用して PKCS10 証明書署名要求 (CSR) を作成します。その後、この CSR を認証局 (CA) に送信できます。

CA 発行の証明書を受け取ったら、GenCSR を使用してこの証明書を更新します。システム証明書は、CA 発行の証明書によって更新されるまで Sterling B2B Integrator で使用できません。

このユーティリティーを使用すると、CSR のリストを表示したり、CSR に関する情報をファイルに書き込んだり、CSR を削除したり、HSM に保管されている CA 発行の証明書に関する情報をファイルに書き込んだりすることもできます。CSR に関する情報は Sterling B2B Integrator のデータベースに保持されていますが、実際の鍵は HSM に保管されています。

このユーティリティーを使用するには、まず実行するアクションを決定します。次に、GenCSR ユーティリティーを使用して、コマンド・ラインでそのアクションを指定します。各アクションについて、そのアクションに必要な引数をプロパティー・ファイルで指定します。csr.properties.sample という名前のサンプル・プロパティー・ファイルが /*install_dir*/install/properties ディレクトリーに用意されています。

GenCSR ユーティリティーは、/*install_dir*/install/bin ディレクトリーにあります。

コマンド構文は、`GenCSR.sh -a ACTION -p PROPERTIES` です。

## GenCSR のパラメーター

次の表では、GenCSR スクリプトの実行時に使用されるパラメーターを示しています。

| パラメーター | 説明 | 有効な値 |
|---|---|---|
| -a ACTION | 実行するアクション。 | 有効なアクションは次のとおりです。<br>• CREATE<br>• UPDATE<br>• LIST<br>• DELETE<br>• GETPCKS10<br>• GETCACERT |
| -p PROPERTIES | 対象のアクションに必要な追加パラメーターが含まれたプロパティー・ファイル。そのプロパティー・ファイルへのパスを指定する必要があります。 | プロパティー・ファイルの名前。<br>例: `csr_create.properties` などです。 |

## CA 発行の証明書による HSM 鍵ストアの更新

CA 発行の証明書の情報を HSM 鍵ストアに追加するには、GenCSR ユーティリティーを update 引数付きで使用します。

### 手順

1. csr_update.properties ファイルが正しく構成されていることを確認します。

   次の表では、update 引数のために csr_update.properties ファイルで指定する必要のあるパラメーターを説明しています。

| パラメーター | 説明 | 有効な値 |
|---|---|---|
| provider | 鍵ストア・プロバイダーの名前。 | ERACOM または ERACOM.n |
| keystoretype | 使用される鍵ストアの名前。 | CRYPTOKI |
| certificate.request.Name | 更新する CSR の名前。 | CSR に割り当てられた名前 |
| add.trusted | 証明書情報がトラステッド証明書表に追加されるかどうかを指定します。 | true または false |
| ca.cert.file | CA 発行の証明書に関する情報を書き込むファイルのパスとファイル名。 | CA 発行証明書ファイルの有効なパスとファイル名 |

2. HSM 鍵ストアを更新します。

   コマンド構文は、`./GenCSR.sh -a update -p ../properties/csr_update.properties` です。

## 証明書署名要求の一覧表示

HSM データベース内の証明書署名要求 (CSR) を表示するには、GenCSR ユーティリティーを list 引数付きで使用します。list 引数のために必要なプロパティー・ファイル内の構成はありません。

### このタスクについて

コマンド構文は、`./GenCSR.sh -a list` です。

## 証明書署名要求の削除

証明書署名要求 (CSR) を削除するには、GenCSR ユーティリティーを delete 引数付きで使用します。このユーティリティーは、CSR のみを削除します。このユーティリティーは、CA 発行の証明書によって更新されるシステム証明書は削除しません。

### 手順

1. cacert.properties ファイルが適切に構成されていることを確認します。 delete 引数を使用する前に、このプロパティー・ファイルを構成する必要があります。次の表では、delete 引数のために cacert.properties ファイルで指定する必要のあるパラメーターを説明しています。

| パラメーター | 説明 | 有効な値 |
|---|---|---|
| certificate.request.Name | 削除する CSR の名前。 | CSR の名前 |
| keystoretype | 使用される鍵ストアの名前。 | CRYPTOKI |
| provider | 鍵ストア・プロバイダーの名前。 | ERACOM[.N] |

2. CSR を削除します。 コマンド構文は、`./GenCSR.sh -a delete -p ../properties/cacert.properties` です。

## pkcs10 フォーマットでの CSR 情報の書き込み

CSR を pkcs10 フォーマットで指定のファイルに書き込むには、GenCSR ユーティリティーを getpkcs10 引数付きで使用します。

### 手順

1. csr_getpkcs10.properties ファイルが正しく構成されていることを確認します。

   次の表では、getpkcs10 引数のために csr_getpkcs10.properties ファイルで指定する必要のあるパラメーターを説明しています。 getpkcs10 引数を使用する前に、このプロパティー・ファイルを構成する必要があります。

| パラメーター | 説明 | 有効な値 |
|---|---|---|
| certificate.request.Name | CSR の名前。 | CSR に割り当てられた名前 |
| keystoretype | 使用される鍵ストアの名前。 | CRYPTOKI |
| csr.file | CSR に関する情報を書き込むファイルの完全修飾パス。 | CSR 情報を書き込むファイルのパスとファイル名 |

2. CSR をファイルに書き込みます。

コマンド構文は、`./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties` です。

## HSM へのシステム証明書の移動

自己署名証明書または CA 発行の証明書をデータベースから HSM に移動できます。

### このタスクについて

よりセキュリティーの高い方法は、CreateSystemCert.sh または GenCSR.sh を使用して鍵と証明書を再生成することです。

自己署名証明書または CA 発行の証明書をデータベースから HSM に移動するには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. Sterling B2B Integrator を停止します。
3. データベースを始動します。
4. 次のコマンドを実行して、システム証明書を PKCS12 ファイルにエクスポートします。

   ```
   ./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass
   pkcs12keypass
   ```
5. 削除するシステム証明書のオブジェクト ID を確認します。次のように入力します。

   ```
   ./RemoveSystemCert.sh -l.
   ```
6. システム証明書をデータベースから削除します。次のように入力します。

   `RemoveSystemCert.sh -r xxxx` (*xxxx* は削除する証明書のオブジェクト ID)
7. エクスポートしたシステム証明書を HSM にインポートして、対応するデータベース・エントリーを作成するには、次のコマンドを実行します。

   ```
   ./ImportSystemCert.sh -pkcs12 systempass certname pkcs12file
   pkcs12storepass pkcs12keypass keystoretype keystoreprovider storepass
   keypass
   ```

   注**:** OpsDrv、OpsKey、および UIKey を HSM に移動する場合は、これらとまったく同じ名前を使用してください。そうしないと、Sterling B2B Integrator は正常に機能しなくなります。これら以外のシステム証明書については、名前は重要ではありません。OpsDrv、OpsKey、および UIKey 以外のシステム証明書を移動する際は、サービスとアダプターによって使用されているオブジェクト ID は変化します。移動したシステム証明書を使用するすべてのサービスを再構成してください。

## ファイルへの CA 発行証明書の書き込み

CA によって発行された証明書をファイルに書き込むには、GenCSR ユーティリティーを getcacert 引数付きで使用します。

### 手順

1. getcacert.properties ファイルが正しく構成されていることを確認します。

   次の表では、getcacert 操作のために getcacert.properties ファイルで指定する必要のあるパラメーターを説明しています。 getcacert 引数を使用する前に、getcacert.properties ファイルを構成する必要があります。

| パラメーター | 説明 | 有効な値 |
|---|---|---|
| certificate.request.Name | CSR の名前。 | 証明書名 |
| keystoretype | 使用される鍵ストアの名前。 | CRYPTOKI |
| ca.cert.file | CA 証明書に関する情報を書き込むファイルの完全修飾パス。 | CA 証明書ファイルのパスと名前 |

2. 証明書をファイルに書き込みます。

   コマンド構文は、`./GenCSR.sh -a getcacert -p ../properties/getcacert.properties` です。

## HSM 上の内部システム証明書 (OpsDrv、OpsKey、UIKey) の生成

内部処理を保護するための 3 つのシステム証明書が、Sterling B2B Integrator とともにインストールされます。これらのシステム証明書を HSM に移動しても、セキュリティー上の利点はほとんど得られません。セキュリティー・ポリシーでは、秘密鍵を含むすべての証明書が HSM に保管されている必要がある場合もあります。

### このタスクについて

HSM で OpsDrv、OpsKey、および UIKey という名前の Sterling B2B Integrator 内部システム証明書を生成する際には、これらとまったく同じ名前を使用してください。そうしないと、Sterling B2B Integrator は正常に機能しなくなります。

内部システム証明書を生成するには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. `./RemoveSystemCert.sh -l` と入力して、データベース内の証明書を表示します。各システム証明書のオブジェクト ID をメモしてください。
3. システム証明書をデータベースから削除するには、各証明書について次のコマンドを実行します: `./RemoveSystemCert.sh -r` *xxxx* ( *xxxx* は削除する証明書のオブジェクト ID)
4. 各証明書について次のコマンドを入力して、システム証明書を HSM 上で生成します。

   ```
   ./CreateSystemCert.sh storetype provider autogen totrusttable signingbit
   keytype keysize keyname rfc1779rdnsequence serial validityindays [system
   passphrase] [store passphrase] [key passphrase]
   ```

# nCipher と SafeNet Eracom の使用

## 鍵ストア・プロバイダーのマップ

Sterling B2B Integrator は、複数の暗号サービス・プロバイダーの間で固有の鍵ストア・タイプを保有しており、鍵ストア・オブジェクト自体、署名アルゴリズム、および鍵伝送アルゴリズムを実装するために必要なプロバイダーと鍵ストア・タイプの間のマッピングを定義できます。

鍵と鍵情報の抽象化オブジェクトには、com.sterlingcommerce.security.PrivateKeyInfo への参照とともにこの情報が含まれています。

これにより、Sterling B2B Integrator は、鍵または鍵情報をデータベースに初期ロードすること以外の追加の構成なしで、データベース内のソフトウェア・ストア内の鍵と HSM 上の鍵の組み合わせを同時に使用できます。Sterling B2B Integrator にとっては、これらの鍵はどこに保管されているかにかかわらずすべて同じように見えます。

マッピングは、security.properties ファイル内の KeyStoreProviderMap というプロパティーとして実装されます。このプロパティーは、セミコロン (;) で区切られた一連のエントリーで構成されています。各エントリーには、次のようにコンマで区切られた 6 つの要素が含まれています。

```
KeyStoreType, KeyStoreProvider, DoesAliasMatter, SignatureProvider,
EncryptionProvider, KeyOnHSM
```

次の表では、これらの要素について説明しています。

| エレメント | 説明 | 追加情報 |
|---|---|---|
| KeyStoreType | 鍵ストアのストリング・タイプ | |
| KeyStoreProvider | 鍵ストアを実装する暗号サービス・プロバイダーの名前 | |
| DoesAliasMatter | この鍵ストア・タイプについて鍵の別名が固有である必要があるかどうか | 指定可能な値は true または false です。装置あたり 1 つの鍵ストアしかない場合は、鍵は固有の別名を持っている必要があります。 |
| SignatureProvider | 鍵ストア内の鍵を使用して署名を作成するために使用する暗号サービス・プロバイダーの名前 | |
| EncryptionProvider | 鍵ストア内の鍵を使用して情報を暗号化解除する際に使用する暗号サービス・プロバイダーの名前 | これは主に RSA 鍵伝送処理用です。 |
| KeyOnHSM | 鍵ストアが HSM 上に配置されているかどうか | |

NULL というストリングを指定可能であり、この値を指定した場合は、どのプロバイダーも指定されていないのと同じ扱いになります。1 つのエントリーには 2 つ以上の値が含まれている必要があります。 1 つのエントリーに含まれている値が 5 つ以下の場合は、これらの値は左から右の順に、「鍵ストア・プロバイダー」、「鍵の保管時に別名が問題になるかどうか」、「署名プロバイダー」、「暗号プロバイダー」、および「鍵ストア・タイプについて鍵が HSM 上にあるかどうか」に割り当てられます。他の値は NULL として扱われ、どの特定プロバイダーもそのタイプの鍵を使用した処理を要求されません。

デフォルトの KeyStoreProviderMap は現在は次のとおりです。

```
KeyStoreProviderMap=SCIKS,SCIKS,false,Certicom,Certicom,false;nCipher.sworld,
nCipherKM,false,nCipherKM,nCipherKM,true;CRYPTOKI,ERACOM,true,ERACOM,ERACOM,true
```

## HSM 上の鍵と鍵情報の管理

Sterling B2B Integrator には、HSM 上の鍵を管理するためのいくつかの Java スクリプトが用意されています。

これらの Java プログラムは次のとおりです。

| プログラム | 目的 |
|---|---|
| com.sterlingcommerce.db.RemoveSystemCert | Sterling B2B Integrator のシステム証明書を一覧表示および削除します。削除時に、当プログラムは可能なかぎり、鍵を鍵ストアから消去して、データベース内の鍵ストア・オブジェクトを上書きしようとします。 |
| com.sterlingcommerce.db.CreateCertEx | HSM 上で鍵ペアを生成して、その鍵ペアの公開鍵が含まれた自己署名証明書を生成します。 |
| com.sterlingcommerce.security.util.<br>CertificateSigningRequest | HSM 上で鍵ペアを生成して、関連する PKCS10 証明書署名要求を作成および管理します。この PKCS10 を認証局に提供することで、その認証局によって署名された証明書を取得できます。その後にこのプログラムを使用して、その証明書を鍵ストアにロードして、正しい鍵ペアと関連付けることができます。 |
| com.sterlingcommerce.db.ImportSystemCert | 秘密鍵と証明書をサポートされているフォーマット (PKCS12 または PEM) で HSM 上の鍵ストアにインポートします。HSM 上の秘密鍵と証明書に関する情報を Sterling B2B Integrator のデータベースにインポートします。 |

## nCipher HSM をサポートするための JDK の変更

Sterling B2B Integrator で nCipher HSM を使用するためには、nCipher Java 暗号サービス・プロバイダーをインストールする必要があります。インストールするには、次の jar ファイルを JDK の jre/lib/ext サブディレクトリーにコピーします。nCipher プロバイダーをロードするために java.security ファイルを変更します。

次のファイルは、nCipher のインストール・プログラムによって /opt/nfast/java/classes に配置されます。

- rsaprivenc.jar
- nfjava.jar

- kmjava.jar
- jutils.jar
- kmcsp.jar

nCipher プロバイダーは、IBM JCE プロバイダーの後ろ、かつ Certicom プロバイダーの前に追加する必要があります。次に例を示します。

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ncipher.fixup.provider.nCipherRSAPrivateEncrypt
security.provider.3=com.ncipher.provider.km.nCipherKM
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.ibm.jsse2.IBMJSSEProvider2
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
```

SUN JDK を使用している Solaris システムでは、nCipher プロバイダーは、Sun JCA プロバイダーと JCE プロバイダーの後ろ、かつ Certicom プロバイダーの前に追加する必要があります。次に例を示します。

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.certicom.ecc.jcae.Certicom
security.provider.3=com.ncipher.fixup.provider.nCipherRSAPrivateEncrypt
security.provider.4=com.ncipher.provider.km.nCipherKM
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=com.sun.net.ssl.internal.ssl.Provider
security.provider.7=com.sun.rsajca.Provider
security.provider.8=sun.security.jgss.SunProvider
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
```

security.properties ファイル内のサンプルを使用して TLSProvider ポリシーを設定します。次に例を示します。

```
TLSProviderPolicy=TLS:MD:MD5:P:Certicom;TLS:MD:SHA1:P:Certicom;TLS:MAC:HmacMD5:P:Certicom;
TLS:MAC:HmacSHA1:P:Certicom;TLS:SIG:MD2withRSA:P:Certicom;TLS:Cipher:RawRSA:P:Certicom;
TLS:*:ECDH:P:Certicom;TLS:*:ECDSA:P:Certicom;TLS:*:*:P:nCipherKM
```

## Eracom HSM をサポートするための JDK の変更

Sterling B2B Integrator で Eracom HSM を使用するためには、Eracom Java 暗号サービス・プロバイダーをインストールする必要があります。インストールするには、JDK の jre/lib/ext サブディレクトリーに適切な .jar ファイルを配置してから、nCipher プロバイダーをロードするために java.security ファイルを変更します。

次のファイルは、nCipher のインストール・プログラムによって /opt/nfast/java/classes に配置されます。

- jcprov.jar
- jprov.jar

Eracom プロバイダーは、Certicom プロバイダーの後ろに追加する必要があります。次に例を示します。

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.certicom.ecc.jcae.Certicom
security.provider.3=au.com.eracom.crypto.provider.ERACOMProvider
security.provider.4=com.ibm.jsse2.IBMJSSEProvider2
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.8=com.sterlingcommerce.security.provider.SCI
```

注: Eracom では、カード上の各スロットについて指定できるプロバイダーが用意されています。スロット 8 のプロバイダーについては、次の設定を使用します。

```
security.provider.3=au.com.eracom.crypto.provider.slot8.ERACOMProvider
```

### nCipher HSM をサポートするための Linux 環境の変更

nCipher では、nCipher hardserver を実行するための特別なユーザー・アカウントを作成することをお勧めします。

Sterling B2B Integrator の実行元となるアカウントには同じ許可が割り当てられている必要があります。そうでない場合は、nCipher の特別アカウントからまたはルートとして Sterling B2B Integrator を実行する必要があります。これらの 2 つのどちらかを実行する場合、かつ MySQL を使用している場合は、MySQL の許可を変更するか、通常のアカウントから MySQL を開始してから run.sh を実行する必要があります。

### Eracom HSM をサポートするための Linux 環境の変更

Eracom 装置を使用するには、その装置にアクセスするセッションに対して、環境変数を通じて追加情報を提供する必要があります。

PATH、LD_LIBRARY_PATH、および MANPATH に対する推奨される変更は次のとおりです。

```
PATH=$PATH:/opt/Eracom/bin LD_LIBRARY_PATH=$LD_LIBRARY_PATH:
/opt/Eracom/lib MANPATH=$MANPATH:/opt/Eracom/man
```

また、ローカル PCI カードではなくネットワーク装置を使用している場合は、次のように ET_HSM_NETCLIENT_SERVERLIST を指定する必要があります。

```
ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname
```

これらの変数を tmp.sh にエクスポートする必要があります。

## ハードウェア・セキュリティー・モジュール (HSM) V5.2.6 以降

### ハードウェア・セキュリティー・モジュール (HSM)

HSM は、暗号鍵を生成、保管、および保護するためのハードウェア・ベースのセキュリティー装置です。システム証明書は、Sterling B2B Integrator を使用してデータベースに保管することも、HSM に保管することもできます。

Sterling B2B Integrator は、次の HSM 装置をサポートしています。

- SafeNet Luna SA
- nCipher nShield Connect

HSM を使用して次のことを実行できます。

- HSM 上のシステム証明書の作成
- Sterling B2B Integrator からのシステム証明書のインポート
- Sterling B2B Integrator からのシステム証明書のエクスポート
- HSM からのシステム証明書の削除
- HSM 上の証明書のシステム証明書詳細の表示

## HSM をサポートするための Sterling B2B Integrator の機能

それぞれの鍵ペアと証明書について 1 つのエントリーが、Sterling B2B Integrator によって CERTS_AND_PRI_KEY 表内に保管されます。

このエントリーには、次の情報が含まれています。

- 鍵と証明書。これには、有効期間、シリアル番号、使用上の制約事項、およびその鍵や証明書に実際にアクセスすることなくユーザーに表示するために UI で使用される発行者と件名が含まれます。
- システムで検索時に使用される識別名の正規化
- レコードに対する変更内容
- 証明書の失効ステータス情報
- 鍵ストアのタイプ
- DATA_TABLE に保管されているバイナリー鍵ストア・オブジェクトへの参照。ソフトウェア鍵ストアが使用されている場合は、参照先のオブジェクトには鍵データが含まれていることがあります。HSM の場合は、参照先のオブジェクトには参照情報 (nCipher) またはプレースホルダー (Luna) が含まれています。

## HSM 上のシステム証明書のパラメーター

次の表では、CreateSystemCert コマンド、ImportSystemCert コマンド、および ExportSystemCert コマンドのパラメーターを説明しています。

| パラメーター | 説明 |
|---|---|
| autogen | システム側で生成された情報を使用して鍵と鍵ストアへのアクセスを制御するのかどうかを指定します。HSM 上の鍵については false に設定する必要があります。 |
| alias | HSM に保管されている鍵名。別名は、大文字/小文字の英字、数字、またはハイフン (-) で構成されており、その全体の長さはシステム GUID の長さ以下である必要があります。 |
| Certtype | インポートする証明書タイプ。サポートされている証明書ファイルのタイプは、pkcs12、pkcs8、pem、および keystore の 4 タイプです。Sterling B2B Integrator でサポートされているのは、DES または 3DES で暗号化された pem 鍵のみです。鍵ストアを一覧表示またはインポートするには、keystore を使用します。 |
| certname | Sterling B2B Integrator のデータベース内の証明書に割り当てる名前。 |
| file | インポートする Keycert ファイルまたは PEM ファイル。 |
| keyname | 作成する Sterling B2B Integrator システム鍵の名前。 |

| パラメーター | 説明 |
| --- | --- |
| keypass | 鍵ストアが配置されている SafeNet または nCipher HSM を保護しているトークンの PIN。 |
| key passphrase | 秘密鍵のパスフレーズ。この値は、コマンド・ライン上で省略可能です。この値を指定しなかった場合は、この値を求めるプロンプトが表示されます。 |
| keysize | RSA モジュラスの長さ (ビット単位)。有効な値は 1024、2048、3072、および 4096 です。 |
| keystoretype | インポートする鍵ストア・タイプ。有効な値は、nCipher.sworld、Luna、および PKCS11IMPLKS (5.2.6.2 以降) です。 |
| keystoreprovider | プロバイダー・タイプ。有効な値は、nCipherKM、LunaProvider、および IBMPKCS11Impl (5.2.6.2 以降) です。 |
| keytype | 公開鍵のアルゴリズム。RSA が唯一のサポートされているアルゴリズムです。 |
| ObjectID | システム証明書の ID。 |
| pkcs12file | インポートする pkcs12 ファイル。 |
| password | keycert ファイルまたは PEM ファイルのストア・パスフレーズ。 |
| pkcs12storepass | PKCS12 ファイルのストア・パスフレーズ。 |
| pkcs12keypass | PKCS12 ファイル内の秘密鍵を暗号化するために使用される鍵パスフレーズ。 |
| provider | 鍵ストア・タイプのプロバイダー。有効な値は、nCipherKM、LunaProvider、および IBMPKCS11Impl (5.2.6.2 以降) です。 |
| rfc1779rdnsequence | 「識別名」ストリング・フィールドには、「有効な値」列で指定されたフィールドのいずれかが含まれています。「CN」フィールドのみが必須です。各フィールドをコンマで区切ってください。有効な情報:<br>• CN = 共通名<br>• O = 組織<br>• OU = 組織単位<br>• L = 場所<br>• ST = 都道府県<br>• C = 国 (2 文字の ISO3166-1 アルファ 2 コードを指定します) |
| storetype | 鍵ストア・タイプ。有効な値は、nCipher.sworld、Luna、および PKCS11IMPLKS (5.2.6.2 以降) です。 |
| signingbit | 自己署名証明書の署名鍵使用ビットを設定します。有効な値は true または false です。 |
| serial | 証明書のシリアル番号。 |
| system passphrase | Sterling B2B Integrator のシステム・パスフレーズ。この値は、コマンド・ライン上で省略可能です。 |

| パラメーター | 説明 |
|---|---|
| store passphrase | 鍵ストアにアクセスするためのパスフレーズ。この値は、コマンド・ライン上で省略可能です。この値を指定しなかった場合は、この値を求めるプロンプトが表示されます。 |
| systempass | Sterling B2B Integrator のシステム・パスフレーズ。 |
| storepass | 鍵ストアが配置されている SafeNet または nCipher HSM を保護しているトークンの PIN。 |
| totrusttable | 証明書がトラステッド証明書表に追加されるかどうかを指定します。有効な値は true または false です。 |
| validityindays | 証明書の有効日数。 |

# ハードウェア・セキュリティー・モジュールの使用

## HSM に保管するシステム証明書の作成

保管する自己署名システム証明書を HSM に作成できます。

### 始める前に

始める前に:

- Sterling B2B Integrator を停止します。
- Sterling B2B Integrator のデータベースが稼働していることを確認します。

### このタスクについて

HSM に保管する自己署名システム証明書を作成するには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。 `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase] [store passphrase] [key passphrase]`
3. コマンド・ラインでシステム・パスフレーズ、ストア・パスフレーズ、および鍵パスフレーズを入力しなかった場合は、これらの入力を求めるプロンプトが表示されます。

## HSM に保管されたシステム証明書の一覧表示

保管されたシステム証明書に関する情報を HSM に一覧表示できます。

### このタスクについて

HSM に保管されたシステム証明書に関する情報を一覧表示するには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。

2. 次のように入力します。 `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

### 例

以下では、このコマンドの出力例を示しています。

```
Key exists with alias rayado-e5305c3-10d8f4bde7f--7fc1
Certificate Subject Info CN=test, OU=test, O=test, L=test, ST=Alabama, C=US
Certificate Issuer Info CN=Pythagoras, OU=System Verification, O=Sterling, L=Dublin,
ST=OH, C=US, EMAILADDRESS=caussuer@company.com
```

注: V5.2.6.2 以降、Keystoretype に有効な値は PKCS11IMPLKS です。

## HSM 上のシステム証明書の Sterling B2B Integrator データベースへのインポート

鍵と証明書が HSM 上に存在しており、Sterling B2B Integrator とは無関係にこれらの鍵と証明書が HSM に追加された場合は、この手順を使用します。HSM に保管されているシステム証明書を Sterling B2B Integrator で使用可能にするためには、そのシステム証明書の情報をデータベースにインポートする必要があります。

### このタスクについて

秘密鍵と証明書を HSM に追加するために使用される方法によっては、list 関数で、単一の鍵/証明書ペアについて重複するエントリーを表示することがあります。

システム証明書に関する情報をデータベースにインポートするには、そのシステム証明書の別名を知っている必要があります。

システム証明書をインポートするには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。 `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

## HSM に保管されたシステム証明書の削除

### このタスクについて

この手順では、システム証明書を HSM から完全に削除します。そのシステム証明書に含まれている秘密鍵データは復元できなくなります。

HSM に保管されたシステム証明書を削除するには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。 `./RemoveSystemCert.sh -r xxxx`

   ここで、*xxxx* は削除する証明書のオブジェクト ID です。

### システム証明書のエクスポート

Sterling B2B Integrator からシステム証明書をエクスポートして、それらを HSM にインポートできます。

#### このタスクについて

HSM 上のシステム証明書は、ExportSystemCert.sh を使用してエクスポートすることはできません。

#### 手順

1. *install_dir*/install/bin にナビゲートします。
2. 次のように入力します。 `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. パスフレーズを入力します。

### 例: HSM システム証明書

keycert、pkcs12、または pem のフォーマットで、システム証明書を HSM にインポートできます。システム証明書をインポートすると、鍵と証明書が HSM に追加されて、対応するエントリーが Sterling B2B Integrator のデータベース内に作成されます。

pem タイプの証明書と鍵をインポートする場合は、秘密鍵が DES 暗号化フォーマットまたは Triple-DES 暗号化フォーマットで作成されるようにしてください。

以下では、Triple-DES フォーマットで作成された pem 秘密鍵のサンプルを示しています。

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE0243B4833BD321
RtN+AFGTmx6EROcbo8fMXnMaRM/JcKIc3jbKYB5t6H6H5uvUrAmv+Si62QEtqg9V
x5r+GhiLcA9sdllKpnIXYg63Y+egn8DsxdGUCqnC+HDUlRVHX0NWKJ3FwXukr9iN
WP4MBr+NXMSETaBA0O0B4oSRCWvxelc2U2GItvUqJsOjLSILbahAgZk/j6LUDMy4
2FWoRtWZyGVz/gc+pN+bOwFHpbrZxd1YqZGRNKeZKTpXWslqxp5NDraBl1cmJ3vL
0RTnkwZnnyJ1Brc/WynlVfRK1gEEg8MPa3B9veat70ET/mLERuA4Ke8r0WAy5Y/w
7Yowicmwbo4q7RLVLm1ZmvPF4OXL8xIvaIUMOCW8/MNpanxZ4BB1CfTwQKQ9koJ7
9MT8K8ofu6V9TSK4Rw1cCpTKvattg/H72Ut39Yz185Ec+E8sV0BtilpqVsYSt1g6
lO805MqPym6gPo2NLpvk1iPLUZ1vIfthz+qb5cyXj1ng9aZSeRF/lytPLxSSy3LN
J9SZrnfHwbuhnyuQmco3SsCtYXnZ81cDHX+4O8sGqHA1zMwuqErorUvwxD6ZNnlc
DTmKIt826oows4Gtw48aEwjV4lk8FXQsWQjDWJHjFNNvGiyszPJjvPvM8zL1EwxO
mJFeNxBb0U3zgLs5aK/HHRn1/gzOBHwtr8bdFFBkpLoVGnbW+mRVxmJOvvPe7Zo+
sJXLEWC8Bm4klV8H6ynx6aQJ8a62HqbjPvShq1VH2I+1iwbyE3DzxY5sHrzZA2rb
dHabk3f0nBUvMegKI9Ye4ktLJf8yIQfsSBSJTEYXHqyx5ptoAEIlIQ==
-----END RSA PRIVATE KEY-----
```

## システム証明書ユーティリティーの管理

### HSM 上の鍵ペアと証明書署名要求

GenCSR ユーティリティーは、HSM 上に鍵ペアを生成して、その鍵ペア内の公開鍵を使用して PKCS10 証明書署名要求 (CSR) を作成します。その後、この CSR を認証局 (CA) に送信できます。

CA 発行の証明書を受け取ったら、GenCSR を使用してこの証明書を更新します。システム証明書は、CA 発行の証明書によって更新されるまで Sterling B2B Integrator で使用できません。

このユーティリティーを使用すると、CSR のリストを表示したり、CSR に関する情報をファイルに書き込んだり、CSR を削除したり、HSM に保管されている CA 発行の証明書に関する情報をファイルに書き込んだりすることもできます。CSR に関する情報は Sterling B2B Integrator のデータベースに保持されていますが、実際の鍵は HSM に保管されています。

このユーティリティーを使用するには、まず実行するアクションを決定します。次に、GenCSR ユーティリティーを使用して、コマンド・ラインでそのアクションを指定します。各アクションについて、そのアクションに必要な引数をプロパティー・ファイルで指定します。csr.properties.sample という名前のサンプル・プロパティー・ファイルが /*install_dir*/install/properties ディレクトリーに用意されています。

GenCSR ユーティリティーは、/*install_dir*/install/bin ディレクトリーにあります。

コマンド構文は、`GenCSR.sh -a ACTION -p PROPERTIES` です。

## GenCSR のパラメーター

次の表では、GenCSR スクリプトの実行時に使用されるパラメーターを示しています。

| パラメーター | 説明 | 有効な値 |
|---|---|---|
| -a ACTION | 実行するアクション。 | 有効なアクションは次のとおりです。<br>• CREATE<br>• UPDATE<br>• LIST<br>• DELETE<br>• GETPCKS10<br>• GETCACERT |
| -p PROPERTIES | 対象のアクションに必要な追加パラメーターが含まれたプロパティー・ファイル。そのプロパティー・ファイルへのパスを指定する必要があります。 | プロパティー・ファイルの名前。<br><br>例: `csr_create.properties` などです。 |

## CA 発行の証明書による HSM 鍵ストアの更新

### このタスクについて

CA 発行の証明書の情報を HSM 鍵ストアに追加するには、GenCSR ユーティリティーを update 引数付きで使用します。

### 手順

1. csr_update.properties ファイルが正しく構成されていることを確認します。

   次の表では、update 引数のために csr_update.properties ファイルで指定する必要のあるパラメーターを説明しています。

| パラメーター | 説明 | 有効な値 |
|---|---|---|
| provider | 鍵ストア・プロバイダーの名前。 | IBMPKCS11IMPL (V5.2.6.2 以降)、nCipherKM、または LunaProvider |
| keystoretype | 使用される鍵ストアの名前。 | PKCS11IMPLKS (V5.2.6.2 以降)、nCipher.sworld、または Luna<br>**注:** 「keystoretype」値は「provider」値と同期している必要があります。 |
| certificate.request.Name | 更新する CSR の名前。 | CSR に割り当てられた名前 |
| add.trusted | 証明書情報がトラステッド証明書表に追加されるかどうかを指定します。 | true または false |
| ca.cert.file | CA 発行の証明書に関する情報を書き込むファイルのパスとファイル名。 | CA 発行証明書ファイルの有効なパスとファイル名 |

2. HSM 鍵ストアを更新します。

   コマンド構文は、`./GenCSR.sh -a update -p ../properties/csr_update.properties` です。

## 証明書署名要求の一覧表示

HSM データベース内の証明書署名要求 (CSR) を表示するには、GenCSR ユーティリティーを list 引数付きで使用します。list 引数のために必要なプロパティー・ファイル内の構成はありません。

### このタスクについて

コマンド構文は、`./GenCSR.sh -a list` です。

## 証明書署名要求の削除

証明書署名要求 (CSR) を削除するには、GenCSR ユーティリティーを delete 引数付きで使用します。このユーティリティーは、CSR のみを削除します。このユーティリティーは、CA 発行の証明書によって更新されるシステム証明書は削除しません。

### 手順

1. cacert.properties ファイルが適切に構成されていることを確認します。 delete 引数を使用する前に、このプロパティー・ファイルを構成する必要があります。次の表では、delete 引数のために cacert.properties ファイルで指定する必要のあるパラメーターを説明しています。

| パラメーター | 説明 | 有効な値 |
|---|---|---|
| certificate.request.Name | 削除する CSR の名前。 | CSR の名前 |
| keystoretype | 使用される鍵ストアの名前。 | PKCS11IMPLKS (V5.2.6.2 以降)、nCipher.sworld、または Luna |
| provider | 鍵ストア・プロバイダーの名前。 | IBMPKCS11IMPL (V5.2.6.2 以降)、nCipherKM、または LunaProvider<br>**注:** 「keystoretype」値は「provider」値と同期している必要があります。 |

2. CSR を削除します。 コマンド構文は、`./GenCSR.sh -a delete -p ../properties/cacert.properties` です。

## pkcs10 フォーマットでの CSR 情報の書き込み

### このタスクについて

CSR を pkcs10 フォーマットで指定のファイルに書き込むには、GenCSR ユーティリティーを getpkcs10 引数付きで使用します。

### 手順

1. csr_getpkcs10.properties ファイルが正しく構成されていることを確認します。

   次の表では、getpkcs10 引数のために csr_getpkcs10.properties ファイルで指定する必要のあるパラメーターを説明しています。 getpkcs10 引数を使用する前に、このプロパティー・ファイルを構成する必要があります。

| パラメーター | 説明 | 有効な値 |
|---|---|---|
| certificate.request.Name | CSR の名前。 | CSR に割り当てられた名前 |
| keystoretype | 使用される鍵ストアの名前。 | PKCS11IMPLKS (V5.2.6.2 以降)、nCipher.sworld、または Luna |
| csr.file | CSR に関する情報を書き込むファイルの完全修飾パス。 | CSR 情報を書き込むファイルのパスとファイル名 |

2. CSR をファイルに書き込みます。

   コマンド構文は、`./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties` です。

## HSM へのシステム証明書の移動

自己署名証明書または CA 発行の証明書をデータベースから HSM に移動できます。

### このタスクについて

よりセキュリティーの高い方法は、CreateSystemCert.sh または GenCSR.sh を使用して鍵と証明書を再生成することです。

自己署名証明書または CA 発行の証明書をデータベースから HSM に移動するには、以下を実行します。

### 手順

1. *install_dir*/install/bin にナビゲートします。
2. Sterling B2B Integrator を停止します。
3. データベースを始動します。
4. 次のコマンドを実行して、システム証明書を PKCS12 ファイルにエクスポートします。

   ```
   ./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass
   pkcs12keypass
   ```
5. 削除するシステム証明書のオブジェクト ID を確認します。次のように入力します。

   ```
   ./RemoveSystemCert.sh -l.
   ```
6. システム証明書をデータベースから削除します。次のように入力します。

   ```
   RemoveSystemCert.sh -r xxxx (xxxx は削除する証明書のオブジェクト ID)
   ```
7. エクスポートしたシステム証明書を HSM にインポートして、対応するデータベース・エントリーを作成するには、次のコマンドを実行します。

   ```
   ./ImportSystemCert.sh -pkcs12 systempass certname pkcs12file
   pkcs12storepass pkcs12keypass keystoretype keystoreprovider storepass
   keypass
   ```

   注**:** OpsDrv、OpsKey、および UIKey を HSM に移動する場合は、これらとまったく同じ名前を使用してください。そうしないと、Sterling B2B Integrator は正常に機能しなくなります。これら以外のシステム証明書については、名前は重要ではありません。OpsDrv、OpsKey、および UIKey 以外のシステム証明書を移動する際は、サービスとアダプターによって使用されているオブジェクト ID は変化します。移動したシステム証明書を使用するすべてのサービスを再構成してください。

## ファイルへの CA 発行証明書の書き込み

### このタスクについて

CA によって発行された証明書をファイルに書き込むには、GenCSR ユーティリティーを getcacert 引数付きで使用します。

### 手順

1. getcacert.properties ファイルが正しく構成されていることを確認します。

   次の表では、getcacert 操作のために getcacert.properties ファイルで指定する必要のあるパラメーターを説明しています。 getcacert 引数を使用する前に、getcacert.properties ファイルを構成する必要があります。

| パラメーター | 説明 | 有効な値 |
|---|---|---|
| certificate.request.Name | CSR の名前。 | 証明書名 |

| パラメーター | 説明 | 有効な値 |
| --- | --- | --- |
| keystoretype | 使用される鍵ストアの名前。 | PKCS11IMPLKS (V5.2.6.2 以降)、nCipher.sworld、または Luna |
| ca.cert.file | CA 証明書に関する情報を書き込むファイルの完全修飾パス。 | CA 証明書ファイルのパスと名前 |

2. 証明書をファイルに書き込みます。

   コマンド構文は、`./GenCSR.sh -a getcacert -p ../properties/getcacert.properties` です。

### HSM 上の内部システム証明書 (OpsDrv、OpsKey、UIKey) の生成

内部処理を保護するための 3 つのシステム証明書が、Sterling B2B Integrator とともにインストールされます。これらのシステム証明書を HSM に移動しても、セキュリティー上の利点はほとんど得られません。セキュリティー・ポリシーでは、秘密鍵を含むすべての証明書が HSM に保管されている必要がある場合もあります。

#### このタスクについて

HSM で OpsDrv、OpsKey、および UIKey という名前の Sterling B2B Integrator 内部システム証明書を生成する際には、これらとまったく同じ名前を使用してください。そうしないと、Sterling B2B Integrator は正常に機能しなくなります。

内部システム証明書を生成するには、以下を実行します。

#### 手順

1. *install_dir*/install/bin にナビゲートします。
2. `./RemoveSystemCert.sh -l` と入力して、データベース内の証明書を表示します。各システム証明書のオブジェクト ID をメモしてください。
3. システム証明書をデータベースから削除するには、各証明書について次のコマンドを実行します: `./RemoveSystemCert.sh -r` *xxxx* ( *xxxx* は削除する証明書のオブジェクト ID)
4. 各証明書について次のコマンドを入力して、システム証明書を HSM 上で生成します。

   ```
   ./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase] [store passphrase] [key passphrase]
   ```

## nCipher デバイスおよび SafeNet Luna デバイスの構成

### 鍵ストア・プロバイダーのマップ

Sterling B2B Integrator は、複数の暗号サービス・プロバイダーの間で固有の鍵ストア・タイプを保有しており、鍵ストア・オブジェクト自体、署名アルゴリズム、および鍵伝送アルゴリズムを実装するために必要なプロバイダーと鍵ストア・タイプの間のマッピングを定義できます。

鍵と鍵情報の抽象化オブジェクトには、com.sterlingcommerce.security.PrivateKeyInfo への参照とともにこの情報が含まれています。

これにより、Sterling B2B Integrator は、鍵または鍵情報をデータベースに初期ロードすること以外の追加の構成なしで、データベース内のソフトウェア・ストア内の鍵と HSM 上の鍵の組み合わせを同時に使用できます。Sterling B2B Integrator にとっては、これらの鍵はどこに保管されているかにかかわらずすべて同じように見えます。

マッピングは、security.properties ファイル内の KeyStoreProviderMap というプロパティーとして実装されます。このプロパティーは、セミコロン (;) で区切られた一連のエントリーで構成されています。各エントリーには、次のようにコンマで区切られた 6 つの要素が含まれています。

```
KeyStoreType, KeyStoreProvider, DoesAliasMatter, SignatureProvider,
EncryptionProvider, KeyOnHSM
```

次の表では、これらの要素について説明しています。

| エレメント | 説明 | 追加情報 |
|---|---|---|
| KeyStoreType | 鍵ストアのストリング・タイプ | |
| KeyStoreProvider | 鍵ストアを実装する暗号サービス・プロバイダーの名前 | |
| DoesAliasMatter | この鍵ストア・タイプについて鍵の別名が固有である必要があるかどうか | 指定可能な値は true または false です。装置あたり 1 つの鍵ストアしかない場合は、鍵は固有の別名を持っている必要があります。 |
| SignatureProvider | 鍵ストア内の鍵を使用して署名を作成するために使用する暗号サービス・プロバイダーの名前 | |
| EncryptionProvider | 鍵ストア内の鍵を使用して情報を暗号化解除する際に使用する暗号サービス・プロバイダーの名前 | これは主に RSA 鍵伝送処理用です。 |
| KeyOnHSM | 鍵ストアが HSM 上に配置されているかどうか | |

NULL というストリングを指定可能であり、この値を指定した場合は、どのプロバイダーも指定されていないのと同じ扱いになります。1 つのエントリーには 2 つ以上の値が含まれている必要があります。 1 つのエントリーに含まれている値が 5 つ以下の場合は、これらの値は左から右の順に、「鍵ストア・プロバイダー」、「鍵の保管時に別名が問題になるかどうか」、「署名プロバイダー」、「暗号プロバイダー」、および「鍵ストア・タイプについて鍵が HSM 上にあるかどうか」に割り当てられます。他の値は NULL として扱われ、どの特定プロバイダーもそのタイプの鍵を使用した処理を要求されません。

デフォルトの KeyStoreProviderMap は現在は次のとおりです。

```
nCipher = nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true
SafeNet Luna = Luna,LunaProvider,true,LunaProvider,LunaProvider,true
Use "PKCS11IMPLKS,IBMPKCS11Impl,true,IBMPKCS11Impl,IBMPKCS11Impl,true" for
both nCipher and SafeNet Luna from V5.2.6.2 onwards.
```

## nCipher HSM をサポートするための JDK の変更

Sterling B2B Integrator で nCipher HSM を使用するためには、nCipher Java 暗号サービス・プロバイダーをインストールする必要があります。インストールするには、次の jar ファイルを JDK の jre/lib/ext サブディレクトリーにコピーします。nCipher プロバイダーをロードするために java.security ファイルを変更します。

注:

1. V5.2.6.2 以降、「PKCS11IMPLKS」実装を使用して新規の鍵または証明書を作成する場合、以下のセットアップは必要ありません。
2. V5.2.6.2 へのアップグレード後に既存の鍵または証明書を引き続き使用するには、以下の手順に従います。

次のファイルは、nCipher のインストール・プログラムによって /opt/nfast/java/classes に配置されます。

- jcetools.jar
- jutils.jar
- keysafe.jar
- kmjava.jar
- nCipherKM.jar
- nfjava.jar
- rsaprivenc.jar

nCipher プロバイダーは、IBM JCE プロバイダーの後ろ、かつ Certicom プロバイダーの前に追加する必要があります。

リストから IBMJCEFIPS も削除する必要があります。

次に例を示します。

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ncipher.provider.km.nCipherKM
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
security.provider.10=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.11=com.certicom.jsse.provider.CerticomJSSE
```

既存の鍵または証明書をサポートするには、V5.2.6.2 以降では以下の例を使用してください。

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ncipher.provider.km.nCipherKM
security.provider.3=org.bouncycastle.jce.provider.BouncyCastleProvider
```

```
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.jsse2.IBMJSSEProvider2
security.provider.7=com.ibm.security.jgss.IBMJGSSProvider
security.provider.8=com.ibm.security.cert.IBMCertPath
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
security.provider.11=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.12=com.certicom.jsse.provider.CerticomJSSE
```

## SafeNet Luna HSM をサポートするための JDK の変更

Sterling B2B Integrator で SafeNet Luna HSM を使用するためには、SafeNet Luna Java 暗号サービス・プロバイダーをインストールする必要があります。インストールするには、JDK の jre/lib/ext サブディレクトリーに適切な .jar ファイルを配置してから、Luna プロバイダーをロードするために java.security ファイルを変更します。

注:

1. V5.2.6.2 以降、「PKCS11IMPLKS」実装を使用して新規の鍵または証明書を作成する場合、以下のセットアップは必要ありません。
2. V5.2.6.2 へのアップグレード後に既存の鍵または証明書を引き続き使用するには、以下の手順に従います。

次のファイルは、nCipher のインストール・プログラムによって /opt/nfast/java/classes に配置されます。

- libLunaAPI.so
- LunaProvider.jar

LunaProvider は、IBM JCE プロバイダーの後ろ、かつ Certicom プロバイダーの前に追加する必要があります。

リストから IBMJCEFIPS も削除する必要があります。

次に例を示します。

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.safenetinc.luna.provider.LunaProvider
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
security.provider.10=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.11=com.certicom.jsse.provider.CerticomJSSE
```

既存の鍵または証明書をサポートするには、V5.2.6.2 以降では以下の例を使用してください。

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.safenetinc.luna.provider.LunaProvider
security.provider.3=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.jsse2.IBMJSSEProvider2
security.provider.7=com.ibm.security.jgss.IBMJGSSProvider
security.provider.8=com.ibm.security.cert.IBMCertPath
```

```
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
security.provider.11=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.12=com.certicom.jsse.provider.CerticomJSSE
```

# IBM PKCS11IMPLKS を使用した HSM の構成 (V5.2.6.2 以降)

## IBM PKCS11 IMPLKS 実装を使用した HSM の構成 (V5.2.6.2 以降)

### このタスクについて

バージョン 5.2.6.2 以降から、システムでは HSM デバイスで IBM PKCS11 実装がサポートされます。HSM は Java JCE API を実装しています。このインターフェースは、デバイス内の鍵にアクセスします。

### 手順

1. PKCS11IMPLKS/IBMPKCS11Impl をサポートするために、新規のプロパティー・ファイル **hsm.properties.in** が追加されます。

   以下の表に、HSM の構成に固有のプロパティーをリストします。

| 属性 | 説明 |
|---|---|
| HSM_KEYSTORE_TYPE | HSM_ENABLED が *true* に設定されている場合、この属性値は *IBMPKCS11IMPLKS* でなければなりません。 |
| HSM_KEYSTORE_PROVIDER | HSM_ENABLED が *true* に設定されている場合、この属性値は *IBMPKCS11Impl* でなければなりません。 |
| HSM_KEYSTORE_FILE | <ブランクのままにする必要があります> |
| HSM_ADAPTER_TYPE | ncipher または safeNetFor ncipher。鍵または証明書の作成または更新中に以下のコマンドを実行します。<br><br>UNIX の場合: export CKNFAST_OVERRIDE_SECURITY_ASSURANCES=<br><br>"longterm;tokenkeys"<br><br>Windows の場合: set CKNFAST_OVERRIDE_SECURITY_ASSURANCES<br><br>="longterm;tokenkeys" |
| HSM_ENABLED | HSM のサポートのためには、この属性を *true* に設定する必要があります。 |
| HSM_PRNG_ALGORITHM | HSM_ENABLED が *true* に設定されている場合、この属性値は *PKCS11DeviceRNG* でなければなりません。 |
| HSM_CONFIG_FILE_LOCATION | HSM_ENABLED が *true* に設定されている場合、この属性値には IBMPKCS11 構成ファイルの場所が設定されている必要があります。 |

2. HSM タイプに基づいて、HSM のセットアップに必要な構成ファイルを更新または作成します。

HSM タイプの場合、以下の例に示すようにデバイス用の構成ファイルを見つけることも、IBM サポートに依頼して構成ファイルを入手することもできます。必要に応じて、任意のデフォルト設定を更新できます。ご使用の場所がデフォルトと異なる場合は、*library* 値を編集する必要があります。

```
For SafeNet Luna Device:

lunasa_5_0_jsse.cfgname = B2Bi
library=/usr/safenet/lunaclient/lib/libCryptoki2_64.so
description=Luna SA 5.0 IBM SSP config - JSSE

publickeyimportonly=false
slotListIndex = 0
disabledMechanisms = {
   CKM_MD5
   CKM_SHA_1
   CKM_MD5_HMAC
   CKM_SHA_1_HMAC
   CKM_DES_CBC
   CKM_DES_CBC_PAD
   CKM_DES_ECB
   CKM_DES3_CBC
   CKM_DES3_ECB
   CKM_DES3_CBC_PAD
   CKM_AES_CBC
   CKM_AES_ECB
   CKM_AES_CBC_PAD
   CKM_RC4
   CKM_SSL3_MASTER_KEY_DERIVE
   CKM_SSL3_KEY_AND_MAC_DERIVE
   CKM_SSL3_PRE_MASTER_KEY_GEN
   CKM_TLS_PRE_MASTER_KEY_GEN
   CKM_TLS_MASTER_KEY_DERIVE
   CKM_TLS_KEY_AND_MAC_DERIVE
   CKM_TLS_MASTER_KEY_DERIVE_DH
   CKM_TLS_PRF
   CKM_SHA256_HMAC
   CKM_SHA384_HMAC
   CKM_SHA512_HMAC
   CKM_EC_KEY_PAIR_GEN
   CKM_ECDSA_KEY_PAIR_GEN
   CKM_ECDH1_DERIVE
   CKM_ECDH1_COFACTOR_DERIVE
   CKM_ECMQV_DERIVE
   CKM_DH_PKCS_KEY_PAIR_GEN
   CKM_DH_PKCS_PARAMETER_GEN
   CKM_DH_PKCS_DERIVE
}
attributes (*, CKO_PRIVATE_KEY, *) = {
CKA_SENSITIVE = true
CKA_SIGN = true
CKA_DECRYPT = true
CKA_DERIVE=true}
attributes (*, CKO_PUBLIC_KEY, *) = {
CKA_VERIFY = true
CKA_ENCRYPT = true
CKA_DERIVE = true}
attributes (*, CKO_SECRET_KEY, *) = {
CKA_SENSITIVE = true
CKA_ENCRYPT = true
CKA_DECRYPT = true
CKA_SIGN = true
CKA_VERIFY = true}

For nCipher Device:

======= ncipher_gen2.cfg.jsse
```

```
#nCipher nShield, nForce - Generation 2 cards
name =B2Bi
library=/opt/nfast/toolkits/pkcs11/libcknfast.so
description= IBM SSP NCIPHER HSM ADAPTER config for JSSE

slotListIndex =  1
disabledMechanisms = {
   CKM_MD5
   CKM_SHA_1
   CKM_MD5_HMAC
   CKM_SHA_1_HMAC
   CKM_SHA256_HMAC
   CKM_SHA384_HMAC
   CKM_SHA512_HMAC
   CKM_EC_KEY_PAIR_GEN
   CKM_ECDSA_KEY_PAIR_GEN
   CKM_ECDSA
   CKM_ECDSA_SHA1
   CKM_ECDH1_DERIVE
   CKM_ECDH1_COFACTOR_DERIVE
   CKM_ECMQV_DERIVE
}
attributes(*, CKO_SECRET_KEY, *) = {
   CKA_ENCRYPT=true
   CKA_DECRYPT=true}
attributes (*, CKO_PRIVATE_KEY, *) = {
   CKA_TOKEN=false
   CKA_SIGN=true
   CKA_SENSITIVE=false}
attributes(GENERATE, CKO_PRIVATE_KEY, CKK_RSA) = {
   CKA_DECRYPT=true
   CKA_UNWRAP=true
   CKA_EXTRACTABLE=true}
attributes(GENERATE, CKO_PUBLIC_KEY, *) = {
   CKA_TOKEN=false
   CKA_VERIFY=true}
attributes(*, CKO_PUBLIC_KEY, CKK_RSA) = {
   CKA_ENCRYPT=true
   CKA_WRAP=true
   CKA_VERIFY=true}
attributes(IMPORT, CKO_PRIVATE_KEY, CKK_RSA) = {
   CKA_EXTRACTABLE=true
   CKA_DECRYPT=true
   CKA_UNWRAP=true
   CKA_DERIVE=true}
```

注: SafeNet Luna では、外部で作成された秘密鍵はインポートできません。 秘密鍵は HSM デバイスで作成して保管する必要があります。

# 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。この資料は、IBM から他の言語でも提供されている可能性があります。ただし、これを入手するには、本製品または当該言語版製品を所有している必要がある場合があります。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒*103-8510*
東京都中央区日本橋箱崎町*19*番*21*号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

*IBM Director of Licensing*
*IBM Corporation*
*North Castle Drive, MD-NC119*
*Armonk, NY 10504-1785*
*US*

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向性および指針に関する記述は、予告なく変更または撤回される場合があります。これらは目標および目的を提示するものにすぎません。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。 記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名前はすべて架空のものであり、名前や住所が類似する個人や企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラット

フォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。これらのサンプル・プログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。 IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次に示すように、著作権表示を入れていただく必要があります。



## 商標

IBM、 IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corp. の商標です。 他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

IT Infrastructure Library は英国 Office of Government Commerce の一部である the Central Computer and Telecommunications Agency の登録商標です。

Intel、 Intel ロゴ、Intel Inside、Intel Inside ロゴ、Intel Centrino、Intel Centrino ロゴ、Celeron、 Intel Xeon、Intel SpeedStep、Itanium、および Pentium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

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

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

ITIL は英国 Office of Government Commerce の登録商標および共同体登録商標であって、米国特許商標庁にて登録されています。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Java™ およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Cell Broadband Engine は、Sony Computer Entertainment, Inc. の米国およびその他の国における商標であり、同社の許諾を受けて使用しています。

Linear Tape-Open、LTO、LTO (ロゴ)、Ultrium および Ultrium (ロゴ) は、米国およびその他の国における HP、IBM、および Quantum の商標です。

Connect Control Center®、Connect:Direct®、Connect:Enterprise®、Gentran®, Gentran®:Basic®、Gentran:Control®、Gentran:Director®、Gentran:Plus®、Gentran:Realtime®、Gentran:Server®、Gentran:Viewpoint®、 Sterling Commerce™、Sterling Information Broker®、および Sterling Integrator® は、Sterling Commerce®, Inc.、IBM Company の商標です。

## 製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

### 適用範囲

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

### 個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

### 商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

### 権利

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

プログラム番号:

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21