インターシステムズ公開鍵インフラストラクチャ

Version 2023.1
2024-01-02

InterSystems Corporation　1 Memorial Drive　Cambridge MA 02142　www.intersystems.com

インターシステムズ公開鍵インフラストラクチャ
InterSystems IRIS Data Platform　Version 2023.1　2024-01-02

インターシステムズ社の製品に関するサポートやご質問は、以下にお問い合わせください：

InterSystems Worldwide Response Center (WRC)
Tel:　+1-617-621-0700
Tel:　+44 (0) 844 854 2917
Email:　support@InterSystems.com

目次

インターシステムズ公開鍵インフラストラクチャ

重要　　インターシステムズの PKI はテストのみを目的としています。運用設定では使用しないでください。

このドキュメントでは、以下の項目について説明します。

1 インターシステムズ公開鍵インフラストラクチャ (PKI) について

公開鍵インフラストラクチャ(PKI) は、秘密鍵、公開鍵、および証明書を作成、管理する手段を提供します。これらは、暗号化、解読、デジタル署名、シグニチャの検証などの暗号処理に使用されます。証明書は、公開鍵を識別情報と関連付ける手段を提供します。このために、PKI には認証局 (CA) と呼ばれる信頼されるサード・パーティが含まれます。

インターシステムズの PKI 実装では、InterSystems IRIS が認証機関 (CA) として機能できます。CA として機能する InterSystems IRIS のインスタンスは CA サーバと呼ばれ、CA のサービスを利用する InterSystems IRIS のインスタンスは CA クライアントと呼ばれます。InterSystems IRIS の 1 つのインスタンスは、CA サーバにも CA クライアントにもなることができます。CA サーバとしてのインスタンスは、自己署名 CA 証明書を生成して使用するか、商用のサード・パーティまたは製品により発行された CA 証明書を使用できます。 CA クライアントとしてのインスタンスは、CA サーバと関連付けられます。CA クライアントの証明書は、TLS、XML 暗号化、およびシグニチャの検証で使用できます。中間 CA として機能するように CA クライアントを構成することもできます。PKI が関与する通信は、Web サービスで発生します。

自身を CA サーバとして確立すると、InterSystems IRIS のインスタンスは、公開鍵と秘密鍵のペアを作成してその公開鍵を自己署名 X.509 証明書に埋め込むか、外部 CA により署名された X.509 証明書と秘密鍵を使用します。X.509 は業界標準の証明書構造で、公開鍵をエンティティとその他関連データの両方の識別情報に関連付けます。この識別情報は所有者識別名 (DN) と呼ばれ、エンティティの組織、場所、またはその両方に関するさまざまな固有情報で構成されます。X.509 証明書を使用して公開鍵ベースの高レベルのセキュリティを提供できるのは、秘密鍵の保護および証明書の発行に関する適切なセキュリティ・ポリシーが適用されている場合のみです。これには、CA サーバの秘密鍵ファイルの厳密な制御も含まれ、使用していないときには物理的に保護されるリムーバブル・メディアに保存することが推奨されます。

管理ポータルから InterSystems IRIS PKI インフラストラクチャを使用する場合、すべてのアクションは **[公開鍵インフラストラクチャ]** ページ (**[システム管理]** > **[セキュリティ]** > **[公開鍵インフラストラクチャ]**) から開始します。

PKI および CA の詳細は、付録 “公開鍵インフラストラクチャ (PKI) について” を参照してください。インターシステムズの PKI の基礎となる TLS 呼び出しの技術的な詳細は、″OpenSSL″ ライブラリを参照してください。X.509 証明書の技術的な詳細は、″RFC 5280″ の “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” を参照してください。

1.1 管理ポータルの PKI タスクのヘルプ

PKI タスクのヘルプへのリンクを以下に示します。

- 認証機関クライアント
  - 認証機関サーバへの証明書署名要求の送信
  - 認証機関サーバからの証明書の取得
  - ローカル認証機関クライアントの構成
- 認証機関サーバ
  - 保留中の証明書署名要求の処理
  - ローカル認証機関サーバの構成

2 認証機関サーバ・タスク

InterSystems IRIS インスタンスは、認証機関 (CA) サーバとして機能することができます。これには以下が含まれます。

1. CA サーバとしての InterSystems IRIS インスタンスの構成。これには、証明書に関する情報または、CA サーバが証明書署名要求の処理に使用する情報の提供が必要となります。
2. 保留中の証明書署名要求 (CSR) の管理。これは CA サーバの継続的な作業です。

注釈　これらは CA サーバ管理者のタスクであるため、このセクションはこれらの管理者を対象とします。CA クライアント・タスクはこれとは異なり、CA クライアントの管理者および技術担当者が担当します。

2.1 認証局サーバとしての InterSystems IRIS インスタンスの構成

PKI 処理を行うには、まず認証局 (CA) サーバとして InterSystems IRIS インスタンスを構成する必要があります。これには以下のいずれかが必要です。

- 新しい秘密鍵と証明書での CA サーバの構成
- 既存の秘密鍵と証明書での CA サーバの構成

CA サーバの再初期化が必要な場合もあります。

2.1.1 新しい秘密鍵と証明書での CA サーバの構成

新しい秘密鍵と証明書を作成している場合、手順は次のとおりです。

1. 選択した InterSystems IRIS インスタンスで、管理ポータルの **[公開鍵インフラストラクチャ]** ページ (**[システム管理]** > **[セキュリティ]** > **[公開鍵インフラストラクチャ]**) に移動します。
2. **[公開鍵インフラストラクチャ]** ページの **[認証機関サーバ]** で、**[ローカル認証機関サーバの構成]** を選択します。これにより、(1) CA サーバの証明書および秘密鍵のファイル名ルート、(2) これらのファイルがあるディレクトリの各フィールドが表示されます。

重要　既存の証明書と秘密鍵を指すパスおよびファイル名ルートを指定する場合、InterSystems IRIS はその CA サーバの証明書と秘密鍵を使用します。それ以外の場合、InterSystems IRIS は新しい証明書と秘密鍵を作成します（また、いずれか 1 つのファイルのみが存在する場合、InterSystems IRIS はこれに `.old` 接尾辞を付加して名前を変更し、新しいファイルを作成します）。

フィールドは以下のとおりです。

- **[認証機関の証明書と秘密鍵ファイルのファイル名ルート（拡張子なし）]** ― 必須。秘密鍵と証明書のファイル名の共通部分を指定します。これは、既存のファイルのペアのものでも新しいファイルのペアのものでもかまいません。したがって、ファイル名ルートとして **MyCA** を選択すると、秘密鍵は **MyCA.key** ファイルに保存され、証明書は **MyCA.cer** ファイルに保存されます。このフィールドで有効な文字は、英数字、ハイフン、およびアンダースコアです。ルートを文字列“cache”にすることはできません。
- **[認証機関の証明書と秘密鍵ファイルのディレクトリ]** ― 必須。CA の証明書と秘密鍵のファイルを格納するディレクトリへのパスです。ディレクトリが存在しない場合は、InterSystems IRIS がその作成を試みます。このディレクトリは、（ローカル・ハード・ドライブやネットワーク・サーバではなく）外部デバイス（暗号化された外部デバイスを推奨）に存在する必要があります。これは CA の秘密鍵を保持するディレクトリであるため、完全に安全な場所であることが極めて重要です。ここで相対パスを指定すると、InterSystems IRIS インスタンスの **<install-dir>/mgr/** を基準とした相対パスになります。

3. **[次]** をクリックして次に進みます。
4. 次に表示されるフィールドは、新しい秘密鍵と証明書ペアを作成しているのか、既存の秘密鍵と証明書を使用しているのかによって異なります。新しい秘密鍵と証明書を作成している場合、InterSystems IRIS には次のフィールドが表示されます。
   - **[認証機関の秘密鍵ファイルのパスワード]** および **[パスワード確認]** ― 必須。CA の秘密鍵ファイルを暗号化および解読するためのパスワードです。
   - **[認証機関所有者識別名]** ― CA 証明書のベアラを示す識別名（DN）を定義する 1 つ以上の名前と値のペアのセットです。1 つ以上の属性の値を指定する必要があります。属性は以下のとおりです。
     - **[国]** ― ISO 国コードを使用して国を識別する 2 文字のコードです。
     - **[州または県]** ― CA のある州または県の名前です。通常、CA 証明書ではこのフィールドは使用しません。
     - **[地域]** ― CA のある市町村の名前です。通常、CA 証明書ではこのフィールドは使用しません。
     - **[組織]** ― CA を管理している組織の名前です。規則により、この値は単に“InterSystems”や“InterSystems Corp”ではなく、“InterSystems Corporation”のように略さずに入力します。
     - **[組織単位]** ― その他の組織情報または CA に関する特記事項です。ここには、CA の部署、CA は社内のみで使用するという記述などを入力できます。
     - **[共通名]** ― “ドキュメント・テスト CA”など、CA のわかりやすい名前です。
   - **[認証機関の証明書の有効期間（日数）]** ― 必須。CA 証明書自体の有効期間（存続期間）です。
   - **[認証機関により発行された証明書の有効期間（日数）]** ― 必須。CA がそのクライアントに対して発行する証明書の有効期間（存続期間）です。
   - **[電子メールの構成]** ― CA およびそのタスクを管理するための電子メール・アカウントで必要な情報です。
     - **[SMTP サーバ]** ― 完全修飾ホスト名の形式の、CA メールを処理するSimple Mail Transfer Protocol（SMTP）サーバです（“MyMachine.MyDomain.com”など）。
     - **[SMTPユーザ名]** ― 指定した SMTP サーバが認証できるユーザ名です。このフィールドでは完全修飾ユーザ名とする必要はありません。
     - **[SMTP パスワード]** ― SMTP ユーザ名に関連付けられているパスワードです。

- **[パスワード確認]** – SMTP ユーザ名に関連付けられているパスワードの確認です。
- **[認証機関サーバ管理者の電子メール・アドレス]** – CA の証明書署名要求を受け取るユーザです。このフィールドは、“CAMgr@MyDomain.com”のように完全修飾ユーザ名とする必要があります。

5. 必要に応じてこれらのフィールドに入力し、**[保存]** をクリックします。InterSystems IRIS には、成功したことを示す次のようなメッセージが表示されます。

```
Certificate Authority server successfully configured.
Created new files: C:\pki\FileNameRoot.cer .key, and .srl.
Certificate Authority Certificate SHA-1 fingerprint:
E3:FB:30:09:53:90:9A:31:30:D3:F0:07:8F:64:65:CD:11:0A:1A:A2
Confirmation email sent to: CAserver-admin@intersystems.com
```

これは、秘密鍵、証明書、およびそれらに関連付けられた SRL (シリアル) ファイルが作成されたことを示しています (それ以外の場合はエラー・メッセージを表示します)。

ファイルが作成されたら、物理的に保護されるリムーバブル・メディアに秘密鍵を保存することを強くお勧めします。

警告　すべての秘密鍵を適切に保護することが重要です。特に CA の秘密鍵の保護は最も重要です。秘密鍵が漏洩されると、セキュリティの侵害、データの漏洩、財務損失、および法的な脆弱性が生じる可能性があります。

成功した場合、InterSystems IRIS では以下のようなアクションが実行されたことになります。

- 鍵のペアの作成。
- 指定のファイル名ルートで、指定の場所のファイルに秘密鍵を保存 (下記参照)。
- 公開鍵を含む自己署名 CA 証明書の作成。
- 指定のファイル名ルートで、指定の場所のファイルに証明書を保存 (下記参照)。
- 発行された証明書数のカウンタを作成し、証明書や秘密鍵と同じディレクトリにある SRL (シリアル) ファイルに保存(CA が新しい証明書を発行するたびに、InterSystems IRIS はこのカウンタに基づいて証明書に一意のシリアル番号を付与し、SRL ファイル内の値をインクリメントします)。

CA 秘密鍵と証明書を作成したら、証明書署名要求 (CSR) を処理できます。CA クライアントが CSR を作成すると、CA 管理者はこれについての電子メール通知を受け取ります。

2.1.2 既存の秘密鍵と証明書での CA サーバの構成

(別の InterSystems IRIS CA や、商用 CA などの外部 CA などからの) 既存の秘密鍵と証明書を使用している場合、手順は以下のとおりです。

1. 秘密鍵と証明書を作成または取得します。証明書は PEM 形式であるか、PEM 形式に変換できることが必要です。
2. 証明書と秘密鍵にまだ同一のファイル名ルートがない場合、証明書は filenameroot`.cer`、秘密鍵は filenameroot`.key` という名前に変更します。この filenameroot が使用するファイル名ルートです。
3. 両方のファイルを同じディレクトリに保存します。このディレクトリには、CA サーバとして構成している InterSystems IRIS インスタンスからアクセスできることを確認してください。このディレクトリは、(ローカル・ハード・ドライブやネットワーク・サーバではなく) 外部デバイス (暗号化された外部デバイスを推奨) に存在する必要があります。これは CA の秘密鍵を保持するディレクトリであるため、完全に安全な場所であることが極めて重要です。

警告　すべての秘密鍵を適切に保護することが重要です。特に CA の秘密鍵の保護は最も重要です。秘密鍵が漏洩されると、セキュリティの侵害、データの漏洩、財務損失、および法的な脆弱性が生じる可能性があります。

4. 選択した InterSystems IRIS インスタンスで、管理ポータルの [**公開鍵インフラストラクチャ**] ページ ([**システム管理**] > [**セキュリティ**] > [**公開鍵インフラストラクチャ**]) に移動します。
5. [**公開鍵インフラストラクチャ**] ページの [**認証機関サーバ**] で、[**ローカル認証機関サーバの構成**] を選択します。このページのフィールドに、以下のとおり入力します。
   - [**認証機関の証明書と秘密鍵ファイルのファイル名ルート (拡張子なし)**] – 必須。秘密鍵と証明書のファイル名の共通部分です。この値には、ファイルが持つファイル名ルート、または手順 2 で選択したファイル名ルートを使用します。
   - [**認証機関の証明書と秘密鍵ファイルのディレクトリ**] – 必須。CA の証明書と秘密鍵のファイルを保持するディレクトリへのパスです。この値には、手順 3 で選択したディレクトリを使用します。ここで相対パスを指定すると、InterSystems IRIS インスタンスの <**install-dir**>/**mgr**/ を基準とした相対パスになります。
6. [**次**] をクリックして次に進みます。
7. 次に表示されるフィールドは、新しい秘密鍵と証明書ペアを作成しているのか、既存の秘密鍵と証明書を使用しているのかによって異なります。既存の秘密鍵と証明書を使用している場合、InterSystems IRIS には次のフィールドが表示されます。
   - [**認証機関により発行された証明書の有効期間 (日数)**] – 必須。CA がそのクライアントに対して発行する証明書の有効期間 (存続期間) です。
   - [**電子メールの構成**] – CA およびそのタスクを管理するための電子メール・アカウントで必要な情報です。
     - [**SMTP サーバ**] – 完全修飾ホスト名の形式の、CA メールを処理するSimple Mail Transfer Protocol (SMTP) サーバです (“MyMachine.MyDomain.com” など)。
     - [**SMTPユーザ名**] – 指定した SMTP サーバが認証できるユーザ名です。このフィールドでは完全修飾ユーザ名とする必要はありません。
     - [**SMTP パスワード**] – SMTP ユーザ名に関連付けられているパスワードです。
     - [**パスワード確認**] – SMTP ユーザ名に関連付けられているパスワードの確認です。
     - [**認証機関サーバ管理者の電子メール・アドレス**] – CA の証明書署名要求を受け取るユーザです。このフィールドは、“CAMgr@MyDomain.com” のように完全修飾ユーザ名とする必要があります。

   重要　管理ポータルにこれら以外のフィールドが表示される場合は、使用しようとしている秘密鍵と証明書に向けて適切に指定していないことになります。表示されたすべてのフィールドに記入し、[**保存**] をクリックして成功すると、CA サーバの新しい秘密鍵と証明書の作成は完了です。
8. [**保存**] をクリックします。ローカル CA サーバの構成情報を保存する際、InterSystems IRIS は既存の証明書と秘密鍵を使用します(存在しない場合は SRL ファイルも作成します)。これで、次のような成功メッセージが表示されます。

```
Certificate Authority server successfully configured.
Using existing files: C:\pki\FileNameRoot.cer and .key
Certificate Authority Certificate SHA-1 fingerprint:
E3:FB:30:09:53:90:9A:31:30:D3:F0:07:8F:64:65:CD:11:0A:1A:A2
Confirmation email sent to: CAserver-admin@intersystems.com
```

新しい秘密鍵と証明書の作成の場合と同様に、この時点で、CA サーバは構成され、証明書署名要求 (CSR) を処理できる状態になります。CA クライアントが CSR を作成すると、CA 管理者はこれについての電子メール通知を受け取ります。

2.1.3 CA サーバの再初期化

CA サーバとしてすでにインスタンスを構成している場合、CA の構成用のページには [**再初期化**] ボタンが表示されます。これを選択すると、以下のような影響があります。

- CA サーバのすべての構成情報が削除されます。
- 発行された証明書のすべての情報が破棄されます。
- CA で保留中のすべての証明書署名要求が破棄されます。

注釈　再初期化では、CA の秘密鍵や既存の証明書を含むファイルは削除されません。CA の既存の SRL ファイルも削除されません。実際、これらは依然として有効で、使用可能です。また、すでに署名済みの無効な証明書はレンダリングされません。

このボタンをクリックすると、CA を再初期することを確認するプロンプトが表示されます。再初期化すると、新しい CA サーバを構成することができます。

2.2 保留中の証明書署名要求の管理

認証局 (CA) サーバが構成されると、CA サーバに関連する主なタスクは、潜在的な CA クライアントからの証明書署名要求 (CSR) の管理となります。これには以下のようなタスクが含まれます。

- 証明書署名要求 (CSR) の処理
- 証明書署名要求 (CSR) の削除

要求を承認するように処理する場合、CA サーバは CA の秘密鍵を使用して署名された X.509 証明書を発行し、発行された証明書のシリアル番号を通知する電子メールを CA クライアントの技術担当者に送信します。ここでは、要求を削除 (すなわち拒否) することもできます。

このプロセスでの重要なステップは検証です。ここで CA 管理者は、偽装ができない通信を使用して、要求元の識別情報、技術担当者が要求された DN の証明書を保持する権限、および証明書が発行される目的を検証します(このために、CA サーバの管理者は、CSR と共に、潜在的な CA クライアントから受け取った連絡先情報を使用します)。

2.2.1 証明書署名要求 (CSR) の処理

要求の処理とは、CSR を証明書に変換することです。以下はその方法です。

1. 管理ポータルで、**[公開鍵インフラストラクチャ]** ページ (**[システム管理]** > **[セキュリティ]** > **[公開鍵インフラストラクチャ]**) に移動します。
2. **[公開鍵インフラストラクチャ]** ページの **[認証機関サーバ]** で、**[保留中の証明書署名要求の処理]** を選択します。これにより、CA が受け取った後、処理または削除が行われていない CSR のテーブルが表示されます。各 CSR の右には、**[プロセス]** および **[削除]** リンクが表示されます。
3. CA サーバの証明書と秘密鍵のファイルが含まれるメディアをマウントします(これは、CA サーバとして InterSystems IRIS インスタンスを構成する際にこれらのファイルを格納したメディアです)。
4. CSR を処理するには、**[プロセス]** をクリックします。これにより CSR の内容が表示されます。
5. 証明書を発行する前に、証明書の使用法を指定する必要があります。**[証明書の使用法]** ラジオ・ボタンの選択により、証明書が実行できる処理が指定されます。
   - **[TLS/SSL および XML セキュリティ]** – InterSystems IRIS 内のさまざまなセキュリティ機能を直接使用している CA クライアント用。
   - **[中間認証機関]** – InterSystems IRIS の他のインスタンスの CA として機能している CA クライアント用。
   - **[コード署名]** – コード署名を実行する CA クライアント用。
6. 重要　この手順では、偽装を防止する手段を使用して、潜在的な CA クライアントの技術担当者の識別情報を検証する必要があります。

このページの手順で示したように、CSR を送信したインスタンスの指定された技術担当者に問い合わせる必要があります。組織のポリシーに従って、この担当者に電話で、または直接会って、確認します。

- この担当者の識別情報
- この担当者が、CA サーバ管理者が管理する CA によって署名された、上記所有者識別名を含む証明書を保持する権限
- 上記の SHA-1 指紋が、証明書署名要求の送信時にレポートされた指紋と一致すること

7. 証明書の目的を指定し、技術担当者に関連する情報を検証したら、証明書を発行できます。これを実行するには、**[証明書の発行]** をクリックします。これにより、ページに **[認証機関の秘密鍵ファイルのパスワード]** フィールドが表示されます。
8. **[認証機関の秘密鍵ファイルのパスワード]** フィールドに、CA サーバの秘密鍵ファイルを解読するためのパスワードを入力します。InterSystems IRIS を使用して秘密鍵と証明書を作成した場合、これは **[認証機関の秘密鍵ファイルのパスワード]** に入力した値となります。他のツールを使用して秘密鍵と証明書を作成した場合、これはこの目的でそれらのツールに指定したパスワード (存在する場合) です。
9. **[完了]** をクリックすると、証明書が作成されます。成功すると、InterSystems IRIS には次のようなメッセージが表示されます。

```
Certificate number 31 issued for Certificate Signing Request
"Santiago Development Group"
```

10. CA サーバの証明書と秘密鍵を保持するメディアを取り外し、安全な場所に保存します。

これで、InterSystems IRIS により証明書が作成され、CA クライアントの技術担当者には電子メールで証明書がダウンロード可能であることが通知されました。CA クライアントの技術担当者は、証明書をクライアント・ホストにダウンロードできるようになりました。

2.2.2 証明書署名要求 (CSR) の削除

要求を削除する手順は以下のとおりです。

1. 管理ポータルで、**[公開鍵インフラストラクチャ]** ページ (**[システム管理]** > **[セキュリティ]** > **[公開鍵インフラストラクチャ]**) に移動します。
2. **[公開鍵インフラストラクチャ]** ページの **[認証機関サーバ]** で、**[保留中の証明書署名要求の処理]** を選択します。これにより、CA が受け取った後、処理または削除が行われていない CSR のテーブルが表示されます。各 CSR の右には、**[プロセス]** および **[削除]** リンクが表示されます。
3. CSR を削除するには、**[削除]** をクリックします。操作を確認するダイアログが表示されます。
4. 確認ダイアログで **[OK]** をクリックします。
5. 必要に応じてこれらのフィールドに入力し、**[保存]** をクリックします。

これで CSR が削除されます。

3 認証機関クライアント・タスク

認証機関 (CA) クライアントには、1 回限りの設定タスクがあります。これは以下のとおりです。

1. CA クライアントとしての InterSystems IRIS インスタンスの構成。ここでは、潜在的な CA クライアントへの CA サーバの場所を指定や、CA クライアントの技術担当者の連絡先情報の指定も行います。
2. CA 証明書のコピーの取得。これにより他の証明書の検証が可能となります。

設定タスクの後の CA クライアント・タスクは以下のとおりです。

1. CA サーバへの証明書署名要求 (CSR) の送信。ユーザの観点では、この際、識別名 (DN) およびその他の情報の指定が必要となります(インスタンスに複数の個別の証明書を持つ理由がある場合、これは繰り返し行われることもあります)。
2. さまざまな証明書のコピーの取得。これには、CA クライアントの独自の証明書に加え、CA サーバが発行した他の証明書も含まれます。

これらのタスクを実行すると、CA クライアントは、PKI を使用する必要のある処理を実行できるようになります。これらのタスクは、安全な接続の最後に行われるため、エンド・エンティティと呼ばれています。

注釈　これらは CA クライアントの管理者または技術担当者のタスクであるため、このセクションはこれらの担当者を対象とします。認証機関サーバ・タスクはこれとは異なり、CA サーバ管理者が担当します。

3.1 認証局クライアントとしての InterSystems IRIS インスタンスの構成

認証局 (CA) クライアントとして InterSystems IRIS インスタンスを構成する手順では、潜在的な CA クライアントに対する CA サーバの場所の指定や、CA クライアントの技術担当者の連絡先情報の指定も行います。その手順は以下のようになります。

1. 管理ポータルで、**[公開鍵インフラストラクチャ]** ページ (**[システム管理]** > **[セキュリティ]** > **[公開鍵インフラストラクチャ]**) に移動します。
2. **[公開鍵インフラストラクチャ]** ページの **[認証機関クライアント]** で、**[ローカル認証機関クライアントの構成]** を選択します。このページのフィールドは以下のとおりです。
   - **[認証機関サーバ・ホスト名]** – 必須。CA サーバのマシンの完全修飾名です(具体的には、これは InterSystems IRIS のインスタンスが実行されているマシンで、このインスタンスが CA サーバとして機能しています。CA クライアントとしてインスタンスを構成する前に、CA サーバとしてこれを構成する必要があります)。
   - **[認証機関 Web サーバ・ポート番号]** – 必須。CA サーバとして機能する InterSystems IRIS のインスタンスの Web サーバ・ポート番号です。
   - **[認証機関サーバ・パス]** – 必須。CA サーバの Web サービスのパスです。既定では、これは **/isc/pki/PKI.CAServer.cls** です (この値は、CA の Web サービスへのアクセスの際に、サーバのホスト名とポート番号と共に使用されます)。
   - **[ローカル技術担当者]** – CA クライアントの代わりに CA サーバに検証情報を提供する担当者です。この担当者について、以下の情報が必要です。
     - Name – 必須。CA クライアントの技術担当者の名前です。
     - **[電話番号]** – 担当者の電話番号です。CA 管理者が CA クライアントの証明書を発行する前に検証を行う際に、CA クライアントの技術担当者と連絡を取るための番号です。InterSystems IRIS では特定の検証方法を必要とせず、例えば直接会って確認することもできるため、電話番号は必須ではありません。
     - **[電子メール・アドレス]** – 担当者の電子メール・アドレスです。CA サーバがクライアントの CSR を処理し、証明書が発行されたことを通知する電子メールを、CA クライアントの技術担当者が受信するためのアドレスです。サーバ管理者が新たに発行された証明書についてクライアントの技術担当者に連絡する手段はほかにもあるため、電子メール・アドレスは必須ではありません。
3. 必要に応じてこれらのフィールドに入力し、**[保存]** をクリックします。

InterSystems IRIS は、“認証機関クライアントは正常に構成されました” などのメッセージにより成功したことを認識します。ここで、次のタスクは、CA サーバの証明書のダウンロードです。

3.2 認証局サーバへの証明書署名要求の送信

InterSystems IRIS のインスタンスが認証局 (CA) クライアントとして構成されると、CA サーバに証明書署名要求 (CSR) を送信できるようになります。表面的には、この際、識別名 (DN) およびその他の情報の指定が行われます。内部では、CA クライアントで以下のようないくつかのアクションが実行されます。

1. 公開鍵と秘密鍵のペアの生成。
2. 公開鍵と指定された DN を含む証明書署名要求 (CSR) の作成。
3. Web サービスを使用した CSR の CA サーバへの送信。

PKI インフラストラクチャでは、自動的に CSR を CA サーバに提供し、その送信を認識して、CA サーバの管理者に電子メール通知を送信します。この送信には、CA クライアントのローカル技術担当者の連絡先情報が含まれています。その後、CA 管理者は、偽装ができない通信を使用して、要求元の識別情報、技術担当者が要求された DN の証明書を保持する権限、および証明書が発行される目的を検証します。要求が承認されると、CA サーバによる証明書の作成などの処理が行われます。

CSR を CA サーバに送信する手順は以下のとおりです。

1. 管理ポータルで、**[公開鍵インフラストラクチャ]** ページ (**[システム管理]** > **[セキュリティ]** > **[公開鍵インフラストラクチャ]**) に移動します。
2. **[公開鍵インフラストラクチャ]** ページの **[認証機関クライアント]** で、**[証明書署名要求の認証機関サーバへの送信]** を選択します。このページのフィールドは以下のとおりです。
   - **[ローカル証明書と秘密鍵ファイルのファイル名ルート(拡張子なし)]** ― 必須。秘密鍵と証明書のファイル名の共通部分を指定します。したがって、ファイル名ルートとして `CAClient` を選択すると、秘密鍵は CAClient.key ファイルに保存され、証明書は CAClient.cer ファイルに保存されます。このフィールドで有効な文字は、英数字、ハイフン、およびアンダースコアです。ルートを文字列“cache”にすることはできません。
   - **[認証機関の秘密鍵ファイルのパスワード]** および **[パスワード確認]** ― オプション。CA クライアントの秘密鍵を暗号化および解読するためのパスワードです。
   - **[所有者識別子]** ― クライアント証明書のベアラを示す識別名 (DN) を定義する 1 つ以上の名前と値のペアのセットです。1 つ以上の属性の値を指定する必要があります。属性は以下のとおりです。
     - **[国]** ― ISO 国コードを使用した、その国の 2 文字の国コードです。
     - **[州または県]** ― 完全な州または県の名前です。
     - **[地域]** ― 完全な市町村の名前です。
     - **[組織]** ― 証明書が関連付けられている組織の名前です。規則により、この値は単に“InterSystems”や“InterSystems Corp”ではなく、“InterSystems Corporation”のように略さずに入力します。
     - **[組織単位]** ― 部署など、その他の組織情報です。
     - **[共通名]** ― “ドキュメント・テスト・クライアント”など、クライアントのわかりやすい名前です。
3. 必要に応じてこれらのフィールドに入力し、**[保存]** をクリックします。成功すると、InterSystems IRIS には次のようなメッセージが表示されます。

```
SHA-1 Fingerprint:
0C:DA:5F:06:04:C7:AE:64:61:9C:5C:29:35:49:88:0D:B6:E5:7D:98,
Certificate Signing Request "CAClient060412"
successfully submitted to the Certificate Authority at instance MyCA
on node CATESTCLIENT.CATESTDOMAIN.COM
```

CSR の作成に成功した場合、InterSystems IRIS では以下のようなアクションが実行されたことになります。

- 鍵のペアの作成。

- 指定したファイル名ルートで管理者のディレクトリに秘密鍵を保存。
- 公開鍵を含む CSR を作成し、指定したファイル名ルートで管理者のディレクトリ内のファイルに保存。
- CA クライアントの構成プロセスの一部として指定されたホスト名、ポート、およびパスを使用して、その CSR を CA に送信。

(プロセスが成功しなかった場合、InterSystems IRIS にはエラー・メッセージが表示されます。)

ファイルが作成されたら、物理的に保護される暗号化されたリムーバブル・メディアに、この機密情報を保存することを強くお勧めします。

4. InterSystems IRIS に表示される SHA-1 指紋をコピーします。

   重要　　この情報は、後で、検証プロセスの一部として提供する必要があるため、なくさないでください。

5. この時点で、InterSystems IRIS を使用して CSR が作成され、送信されました。CA の管理者から問い合わせがあったら、最後の手順でコピーした SHA-1 指紋を提供してください。これにより管理者は証明書を作成します。この証明書は、"認証局サーバからの証明書の取得" の説明に従って、取得することができます。

3.3 認証局サーバからの証明書の取得

認証局 (CA) クライアントは、構成されると、CA サーバに関連付けられた任意の証明書をダウンロードできます。これには以下が含まれます。

- CA サーバの証明書。
- それ自体の証明書。これは、CA クライアントが証明書署名要求 (CSR) を CA サーバに送信し、CA サーバがこの要求を承認すると使用可能となります。
- 任意の他の CA クライアントに対して CA サーバが作成した任意の証明書。

証明書を取得する手順は以下のとおりです。

1. 管理ポータルで、**[公開鍵インフラストラクチャ]** ページ (**[システム管理]** > **[セキュリティ]** > **[公開鍵インフラストラクチャ]**) に移動します。
2. **[公開鍵インフラストラクチャ]** ページの **[認証機関クライアント]** で、**[認証機関サーバからの証明書の取得]** を選択します。これにより、ダウンロードできる証明書のリストおよび、(ダウンロード済みかどうかに関係なく) 現在のインスタンスに対して発行されている証明書を表示するボタンが表示されます。通常は、CA サーバ証明書と自身の証明書の両方が必要です。このページから、いくつかのタスクを実行できます。

   - CA 証明書をダウンロードするには、**[認証機関の証明書の取得]** をクリックします。以下のような確認メッセージが表示されます。

     ```
     Certificate Authority Certificate (SHA-1 Fingerprint:
     E2:FB:30:09:53:90:9A:31:30:C3:F0:07:8F:64:65:CD:11:0A:1A:A2)
     saved in file "c:\intersystems\myinstnace\mgr\MyCA.cer"
     ```

   - CA が発行した任意の証明書 (CA クライアント自体の証明書を含む) をダウンロードするには、そのシリアル番号、CA クライアントのホストの名前 (**[ホスト名]** 列)、CA クライアントのインスタンスの名前 (**[インスタンス]** 列)、または証明書のルート・ファイル名 (**[ファイル名]** 列) で証明書を探すことができます。
   - 現在のインスタンスに対して発行された任意の証明書を表示するには、**[このインスタンスの証明書を表示]** をクリックします。これにより、証明書のテーブルが表示され、ここから証明書をダウンロードできます。ここには、**[シリアル番号]** 列と **[ファイル名]** 列のみがリストされます。

3. **[取得]** をクリックして証明書をダウンロードすると、InterSystems IRIS には以下のような確認メッセージが表示されます。

```
Certificate number 74 (SHA-1 Fingerprint:
45:E8:DE:0C:15:BF:A7:89:58:04:5E:68:2E:4D:BB:01:F5:90:94:97)
saved in file "c:\intersystems\myinstance\mgr\IstanbulAcctsPayable.cer"
```

InterSystems IRIS が最初に管理者のディレクトリに証明書をダウンロードする際、一度それらの証明書がクライアント・ホストに置かれると、それらはどこにでも移動することができます。