記事
Hiroshi Sato · 2021年7月27日 4m read

スーパーサーバやTelnetポートでSSLを有効にする際のクライアントの設定

これは InterSystems FAQ サイト**の記事です。**

スーパーサーバでSSL/TLS接続を有効にする場合、クライアントアプリケーションは、使用するプロトコル、アクセスする証明書などを知るためにSSL設定が必要となります。

これらは下記のようにiniファイルを作成・編集することで設定可能です。

==========
設定ファイルの場所
==========

デフォルトでは、SSL設定ファイルはSSLdefs.iniと呼ばれ、32ビットの共通プログラムファイルのディレクトリ下の InterSystems\IRIS(またはInterSystems\Cache)ディレクトリに置く必要があります。

Windows 64bitの場合：C:\Program Files (x86)\Common Files\InterSystems\IRIS\SSLdefs.ini
C:\Program Files (x86)\Common Files\InterSystems\Cache\SSLdefs.ini
Windows 32bitの場合：C:\Program Files\Common Files\InterSystems\Cache\SSLdefs.ini

クライアントインストーラはこのファイルを自動生成しないため、ユーザ自身で作成する必要があります。

※ファイルはBOMなしUTF-8で保存してください。BOMありだと正常に動作しません。

ファイルパスとファイル名を変更したい場合は、環境変数ISCSSLconfigurationsを定義しファイルのフルパスを設定します。

==========
SSLdefs.iniファイルサンプル
==========

以下の2つのセクションからなるファイルを作成します。
最初のセクションは、各接続でどのSSL/TLS構成を使用するかを示します。
※2016.1以降のクライアントは、Addressに接続先サーバのIPアドレスとDNSの両方を指定することが可能です。
2つめのセクションでは、接続に使用するのSSL/TLS構成の設定情報を定義します。

```
[Development Server]
Address=10.100.0.17
Port=51773
TelnetPort=23
SSLConfig=DefaultSettings [DefaultSettings]
VerifyPeer=2
```

CAfile=c:\InterSystems\certificates\CAcert.pem
CertFile=
KeyFile=
Password=
KeyType=
Protocols=28
CipherList=ALL:!aNULL:!eNULL:!EXP:!SSLv2

==========
各パラメータの説明
==========

VerifyPeer

オプションは、0=なし、1=リクエスト、2=必須。 「必須」は推奨値。
「なし」を選択すると、悪意のあるサーバーが接続しようとしているサーバーのようなふりをする可能性がある。

「必須」を選択した場合は、CAfile を指定する必要がある(「リクエスト」の場合は任意)。
これは、管理ポータルの「サーバー証明書の検証」に相当する。

CAfile

信頼できる認証局(CA)ファイルのパス。VerifyPeer値が2である場合に入力する。
これは、管理ポータルの「信頼済み認証局の証明書を含むファイル」に相当する。
証明書はPEM形式でなければいけない。

CertFile
クライアントの証明書のパス。 クライアント認証情報が必要ない場合は空白にする。
これは、管理ポータルの「このクライアントの証明書を含むファイル」に相当する。
証明書はPEM形式でなければいけない。

KeyFile

CertFileの秘密鍵のパス。CertFileがある場合に設定する。
これは、管理ポータルの「関連づけられた秘密鍵を含むファイル」に相当する。

Password

秘密鍵の復号に必要なパスワード。 クライアントで証明書を使用していない場合、または証明書の秘密鍵がディスク上で暗号化されていない場合は空白にする。~

KeyType

秘密鍵タイプ。
CertFileおよびKeyFileが設定されている構成にのみ使用する(おそらくRSA)。

Protocols

クライアントが実行できるSSL/TLSのバージョンを指定する。
複数のバージョンを指定する場合は、数字を追加する(例：TLSv1+TLSv1.1+TLSv1.2=28)。
1 = SSLv2
2 = SSLv3
4 = TLSv1.0
8 = TLSv1.1
16 = TLSv1.2
これは、管理ポータルの「暗号方式設定/プロトコル」に相当する。
SSLv2とSSLv3には既知の問題があり、推奨されていない

CipherList

これは、ポータルの「有効な暗号化スイート」に相当する。

「ALL:!aNULL:!eNULL:!EXP:!SSLv2」は管理ポータルのデフォルト値(バージョンにより異なる)
設定ファイルについては下記ドキュメントもご参照ください。(英語)

Connecting from a Windows Client Using a Settings File

#システム管理 #Caché #Ensemble #InterSystems IRIS #InterSystems IRIS for Health

---

ソースURL:
https://jp.community.intersystems.com/post/%E3%82%B9%E3%83%BC%E3%83%91%E3%83%BC%E3%82%B5%E3%83%BC%E3%83%90%E3%82%84telnet%E3%83%9D%E3%83%BC%E3%83%88%E3%81%A7ssl%E3%82%92%E6%9C%89%E5%8A%B9%E3%81%AB%E3%81%99%E3%82%8B%E9%9A%9B%E3%81%AE%E3%82%AF%E3%83%A9%E3%82%A4%E3%82%A2%E3%83%B3%E3%83%88%E3%81%AE%E8%A8%AD%E5%AE%9A