TLS について

Version 2024.1
2024-06-03

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

TLS について
InterSystems IRIS Data Platform　Version 2024.1　2024-06-03

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

目次

TLS について

Transport Layer Security (TLS) では、エンティティ・ペア間における通信が強力に保護されます。これによって、認証、データ整合性保護、およびデータ暗号化が可能です。TLS は Secure Sockets Layer (SSL) の後継機能です。

SSL は Netscape で 1990 年代半ばに開発されました。TLS は SSL 3.0 の標準化として作成され、TLS version 1.0 は 1999 年にリリースされました。InterSystems IRIS で利用可能な TLS の最新バージョンは 1.3 で、多くの場合 TLS v1.3 と呼ばれます。InterSystems IRIS® データ・プラットフォームでサポートされているバージョンの TLS の中で、使用可能な最新バージョンを使用することをお勧めします。

注釈　　インターシステムズのドキュメントでは、用語としての SSL/TLS と SSL が TLS と同じ意味を持っています。

TLS 接続ではクライアント・サーバ・モデルが使用され、2 つのエンティティが TLS ハンドシェイクによって接続を確立します。2 つのエンティティでハンドシェイクが完了した場合、それは以下が行われたことを意味します。

- クライアントがサーバを認証した。
- サーバにクライアント認証が必要な場合にこれが行われます(クライアントとサーバの両方が互いを認証する方式は相互認証として知られています)。
- クライアントとサーバはセッション・キーについて合意した(セッション・キーは、対称鍵アルゴリズムで使用するためのキーで、これによってエンティティではそれ以降の通信でデータを保護できます)。
- それ以降の通信は暗号化できる。
- それ以降の通信の整合性は検証できる。

クライアントとサーバの暗号スイートでは、これらの処理がハンドシェイクの一部としてどのように行われるか、またこれらの処理が保護された接続に対してどのようにサポートされるかが指定されます。特に、通信相手の暗号スイートでは、サポートしている機能とアルゴリズムが指定されます。クライアントが使用可能な暗号化セットを提案し、提案された中からサーバが 1 つを選択します(クライアントとサーバとの間で共通の暗号化がないと、ハンドシェイクは失敗します)。

ハンドシェイクを行うには、通常、TLS は公開鍵暗号化を使用します (ただし、Diffie-Hellman プロトコルなどの他の方法も使用できます)。公開鍵暗号化では、それぞれの通信相手 (クライアントまたはサーバ) には公開鍵と秘密鍵があります。秘密鍵は機密の値で、公開鍵は幅広く公開される値です。一般的に、公開鍵は証明書にカプセル化されます。この証明書には、名前、組織、場所、発行者の妥当性などの所有者の識別情報も格納されます。InterSystems IRIS では、TLS 構成 (詳細は、"構成について" を参照) により、証明書ファイル、秘密鍵ファイル、暗号スイートのオプション・セットなど、TLS 関連値の名前付きセットが指定されます。

成功すると、ハンドシェイクではセッション・キーが作成され、以降の通信を保護するために使用されます。

InterSystems IRIS とアプリケーションは TLS とのさまざまな相互作用を必要としますが、一般的にエンドユーザにはそのような直接の相互作用がありません。例えば、ブラウザでは TLS を使用して、指定された Web サイトと安全な接続を確立します。その際、サイト (この場合、サーバ) が自らをブラウザに認証する (ブラウザのユーザにはこれはわかりません) 必要があります。ブラウザに表示される鍵アイコンは、TLS により接続が保護されていることを示すためのものです。

1 InterSystems IRIS での TLS のサポート

InterSystems IRIS では、TLS がサポートされており、以下のようないくつかの接続タイプが保護されます。

- InterSystems IRIS スーパーサーバと対話するさまざまなクライアント・アプリケーション (ODBC、JDBC、スタジオなど) からの接続。

- Telnet サーバと対話する Telnet クライアントからの接続。
- InterSystems IRIS インスタンスがクライアントまたはサーバである (または、InterSystems IRIS インスタンスが両端にある) TCP 接続と共に使用するための接続。
- ECP (エンタープライズ・キャッシュ・プロトコル) を使用する接続。TLS を ECP と併用する方法の詳細は、"アプリケーション・サーバのデータ・サーバへの接続の TLS によるセキュリティ保護" を参照してください。

InterSystems IRIS がサーバとして機能する場合、接続を受け入れて TLS の使用を確立します。InterSystems IRIS がクライアントとして機能する場合は、TLS を使用する必要のあるサーバに接続できます。どのような場合でも、いわゆる TLS 構成が使用されます。この構成によって、TLS 接続の一部としての InterSystems IRIS インスタンスの各種特性が指定されます。TLS を構成する方法の詳細は、"TLS の構成" を参照してください。

2 自身の InterSystems IRIS のインスタンスでサポートされている TLS のバージョン

InterSystems IRIS のインスタンスで利用可能な TLS のバージョンは、以下の複数の要因によって異なります。

1. オペレーティング・システム (OS) バージョンで利用可能な OpenSSL ライブラリのメジャー・バージョン。このライブラリにより、オペレーティング・システムでサポートされる、使用可能な TLS プロトコルのバージョンが決まります。
2. オペレーティング・システムのベンダがサポート対象バージョンのプロトコルに対して設定している他の制約 (Ubuntu 20.04 の制約など)。
3. このバージョンの InterSystems IRIS に対応する TLS の最小サポート対象バージョン。このリリースでは、TLS v1.0 です。

コンテナの場合、TLS のサポート対象バージョンは、コンテナ・ホストのオペレーティング・システムとバージョンによって異なります。

重要　オペレーティング・システムのバージョンによってプロトコルが変わるため、同じバージョンの InterSystems IRIS の 2 つのインスタンスであっても同じバージョンの TLS プロトコルがサポートされない場合があります。すべてのプラットフォームでサポートされているバージョンは TLSv1.2 だけです。

OS	バージョン	OpenSSL のバージョン	TLS のバージョン	注
AIX	7.2	1.0.2	1.0、1.1、1.2	以下の "AIX 7.2 の TLS に関する注" を参照。
AIX	7.3	3.0	1.2、1.3	
Red Hat Linux	8	1.1.1	1.0、1.1、1.2、1.3	以下の "Red Hat Linux 8 の TLS に関する注" を参照。
Red Hat Linux	9	3.0	1.2、1.3	
SUSE Linux	すべて	1.1.1	1.0、1.1、1.2、1.3	
Ubuntu Linux	18.04	1.1.1	1.0、1.1、1.2、1.3	
Ubuntu Linux	20.04	1.1.1	1.2、1.3	以下の "Ubuntu Linux 20.04 と 22.04 の TLS に関する注" を参照。
Ubuntu Linux	22.04	3.0	1.2、1.3	以下の "Ubuntu Linux 20.04 と 22.04 の TLS に関する注" を参照。
Windows	すべて	3.1.1	1.2、1.3	以下の "Windows の TLS に関する注" を参照。

注釈　　Oracle Linux のバージョンについての情報は、Red Hat Linux の類似バージョンを参照してください。

2.1 AIX 7.2 の TLS に関する注

AIX 7.2 では OpenSSL 1.0.2 ライブラリを使用するので以下に注意してください。

- OpenSSL 1.0.2 ライブラリでサポートされるのは SSLv3 ～ TLSv1.2 です。InterSystems IRIS は SSLv3 をサポートしないため、TLSv1.0 ～ TLSv1.2 のみのサポートになります。
- OpenSSL 1.0.2 ライブラリには SHA-3 が含まれないため、インターシステムズは SHA-3 の独自実装を提供しています。この実装は RSASHA3Sign 関数および RSASHA3Verify 関数と互換性がありません。これらの関数の呼び出しは <UNIMPLEMENTED> エラーを返します。

2.2 Red Hat Linux 8 の TLS に関する注

FIPS モードの場合、Red Hat Linux 8 では TLSv1.2 と TLSv1.3 のみがサポートされます。

2.3 Ubuntu Linux 20.04 と 22.04 の TLS に関する注

Ubuntu 20.04 と 22.04 では TLSv1.2 と TLSv1.3 のみがサポートされます。これらのバージョンの Ubuntu では TLSv1.0 と TLSv1.1 の使用が禁じられているからです。

2.4 Windows の TLS に関する注

Windows では OpenSSL は使用されないため、インターシステムズは OpenSSL 3.1.1 ライブラリを InterSystems IRIS ディストリビューションの一部として出荷しています。したがって、TLSv1.2 ～ TLSv1.3 がサポートされます。