INFORMATION ANYWHERE

iAnywhere
A SYBASE COMPANY

Technical Guide

暗号化とTransport Layer Security

SQL Anywhere Studio 9.0.2

目次

はじめに

ソフトウェアバージョン
本書の内容は、SQL Anywhere Studioのバージョン9.0.2を対象にしています。

SQL Anywhere Studioは、クライアント／サーバとMobile Link間の通信ストリームの暗号化、またデジタル証明書とTransport Layer Security（以下TLS）によるデータベースの暗号化をサポートします。

本書はSQL Anywhere Studioのバージョン9.0.2が提供する各種の暗号化機能、暗号化及びTLSの要件、追加ライセンスとして別途ご購入いただける暗号化通信オプションについて簡単に説明するものです。

ご購入いただける暗号化通信オプションライセンス

Advanced Encryption Standard（AES）とシンプルなデータベース暗号化はSQL Anywhere Studioの基本パッケージに含まれますが、これら以外の暗号化機能をご使用になる場合は、以下のいずれかの暗号化通信オプションを別途追加ライセンスとしてご購入いただく必要があります。各オプションは¥9,000（2005年9月現在、税別）でアイエニウェア・ソリューションズから入手可能です。

- **ECC（楕円曲線暗号化システム）暗号化通信オプション**

  このオプションでは、クライアント／サーバ間のTLSやMobile Linkの通信にECCデジタル証明書を使うことができます。SQL Anywhere StudioではCerticom社のECCを採用しています。ECCはRSAによる暗号化よりも高速でリソース効率が高く、小さいキーサイズで同等のセキュリティが提供できることを特長としており、処理能力と通信リソースに乏しいPDAやスマートフォンなどのデバイスに適しています。ただしECCデジタル証明書が使えるのはTCP/IP上に限られます。

- **RSA暗号化通信オプション**

  このオプションでは、クライアント／サーバ間のTLSやMobile Linkの通信にRSAデジタル証明書を使うことができます。SQL Anywhere StudioではCerticom社のRSA暗号化技術を採用しています。RSAは最も広く使われている強力な暗号化技術の一つですが、ECCと同等のセキュリティを得るにはより大きなキーサイズが必要となります。RSAデジタル証明書はTCP/IPとHTTPS上で使えます。

- **RSA FIPS暗号化通信オプション**

  このオプションはRSA暗号化通信オプションと同等の機能を提供しますが、アメリカ合衆国政府機関の標準であるFIPS（米連邦情報処理基準）に準拠している点が特長です。現時点ではWindows CEを除くWindows 32bitプラットホームのみでのサポートとなります。このオプションでは、クライアント／サーバ間やMobile Linkの通信にRSA-FIPS暗号化を使えます。またデータベースをAES FIPSで暗号化できます。

暗号化オプションに含まれるファイル

暗号化オプションに含まれるファイルは以下のとおりです。また暗号化オプションの購入に関する情報はアイエニウェア・ソリューションズの以下のサイトでご覧いただけます。

http://www.ianywhere.jp/sas/price.html

表1　各暗号化オプションとファイル

		ECC暗号化通信オプション	RSA暗号化通信オプション	RSA FIPS暗号化通信オプション
ユーティリティファイル		gencert.exe readcert.exe reqtool.exe	gencert.exe readcert.exe reqtool.exe	gencert.exe readcert.exe reqtool.exe
証明書サンプル		eccroot.crt sample.crt	rsaroot.crt rsaserver.crt	rsaroot.crt rsaserver.crt
サーバDLL	クライアントインストール時に含まれるファイル	dbecc9.dll	dbrsa9.dll	dbrsa9f.dll （AES FIPSデータベース暗号化とRSA通信暗号化含む）
ｸﾗｲｱﾝﾄDLL	Windowsアプリケーション	dbmltls9.dll	dbmlrsa9.dll dbmlhttps9.dll	dbmlrsafips9.dll dbmlhttpsfips9.dll
	Ultra Lightアプリケーション	ulecc9.dll	ulrsa9.dll	
	Ultra Light Unicodeアプリケーション	uleccw9.dll	ulrsaw9.dll	

NOTE

- RSA FIPSオプションには、Certicom Security Builder用のセルフテスト・ユーティリティ「sbgtest.exe」が含まれます。
- .dllはWindows OS用のファイルです。UNIX用ファイルの場合は拡張子が.soとなります。

データベースの暗号化

SQL Anywhere Studioは、Adaptive Server AnywhereとUltra Lightのデータベースの暗号化をサポートします。シンプルな暗号化と強力な暗号化が提供されます。

- **シンプルな暗号化**

  ディスクユーティリティを使ってファイルを見た者がデータベース中のデータを解読することを困難にするもので、いわゆる難読化に相当します。シンプルな暗号化ではデータベースを暗号化するためのキー（特別なパスワード）は必要ありません。シンプルな暗号化には、強い暗号化に比べてパフォーマンスに及ぼす影響が小さいという利点があります。

- **強力な暗号化**

  キーがない限りデータベースへのアクセスまたはその操作を拒否するもので、特殊なアルゴリズムでデータベースとトランザクション・ログファイルに含まれる情報を暗号化します。一般にキーが長いほど暗号は強力になりますが、それに伴って処理時間も増えます。Adaptive Server Anywhereの強い暗号化では、AES（Advanced Encryption Standard：次世代標準暗号）とAES FIPSがサポートされています。

  - AES

    米国の国立標準技術研究所（NIST）が採用したブロック暗号化アルゴリズムです。AESでデータベースファイルを暗号化する機能は、Adaptive Server Anywhereのデータベースエンジンに組み込まれています。これはSQL Anywhere Studioの基本パッケージに含まれますので、暗号化パッケージを改めてご購入いただく必要はありません。AESによるデータベース暗号化は、Windows CEを含むすべてのプラットホームでサポートされます。

  - AES FIPS

    AES FIPSは、FIPS準拠のAESでデータベースを暗号化する点でAESと異なります。AES FIPSは現時点ではWindows 32bitプラットホーム（Windows CEを除く）のみでのサポートとなり、また別途RSA FIPS通信暗号化オプションをご購入いただく必要があります。

データベース暗号化がパフォーマンスに及ぼす影響

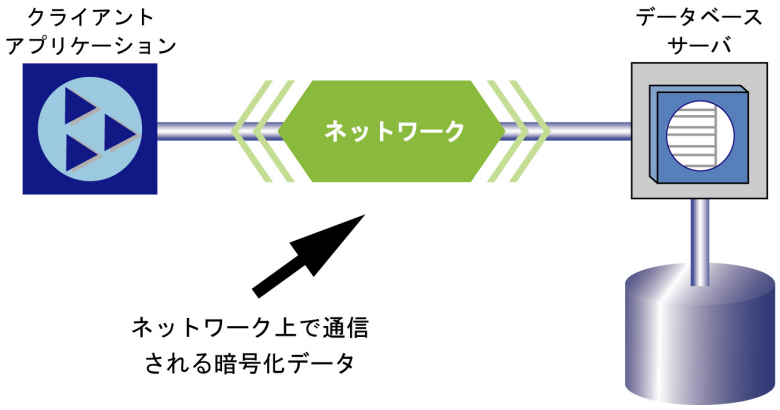
Adaptive Server Anywhereのパフォーマンスはデータベースの暗号化により若干低下します。パフォーマンスへの影響はディスクからのページ読み込み／書き込みの頻度によって変わりますが、サーバに十分なキャッシュサイズを与えることで最小限にとどめることができます。キャッシュの起動サイズを増やすには「-c」サーバオプションを使います。動的なキャッシュのリサイジングをサポートするOSの場合は、利用可能なメモリ量によってキャッシュサイズが制約される可能性があります。この場合はマシンが使用可能なメモリの量を増やしてください。

クライアント／サーバの暗号化とTLS

クライアント／サーバの暗号化は、ネットワークを通過するデータの安全性を高めます。Adaptive Server Anywhereは、シンプルな暗号化とTLSの二つのタイプの通信暗号化をクライアント／サーバに提供します。

- **シンプルな暗号化**

  シンプルな暗号化で処理された通信パケットに対応する機能です。Windows CEを含むすべてのプラットホームでサポートされます。



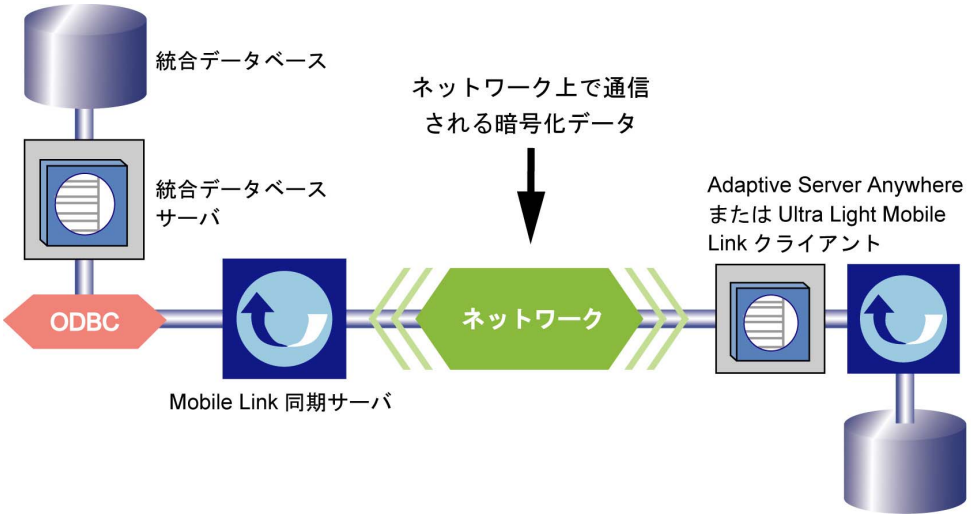
- **TLS**

  デジタル証明書と公開鍵暗号によりクライアント／サーバ・アプリケーションの安全性を確保するもので、IETF標準のプロトコルとなっています。TLSでは暗号化、干渉検出、証明書の認証を行うことができます。強力な通信暗号化によるTLSは、Solaris、Linux、Mac OS X、NetWare、32bit Windows OS（Windows CEを除く）のTCP/IPポートでのサポートとなります。以下の三つのオプションがご利用いただけます。

  - ECC暗号化通信オプション
  - RSA暗号化通信オプション
  - RSA FIPS暗号化通信オプション

Mobile LinkのTLS暗号化

Mobile Link同期サーバとMobile Linkクライアント間の通信は、Mobile LinkのTLSにより暗号化できます。Mobile LinkのTLSでは、クライアント／サーバの暗号化と同様、暗号化通信オプションのいずれか一つを別途ご購入いただく必要があります。



デジタル証明書

Mobile LinkあるいはAdaptive Server AnywhereのTLSを設定するには、デジタル証明書を生成する必要があります。デジタル証明書には以下の種類があります。

- **自己署名証明書**

  単独のサーバによる単純な設定であれば自己署名証明書を使うことができます。この場合は信頼できる公開証明書の生成に使う秘密鍵を、民間の証明機関や専用設備ではなくサーバ自体に保存します。

- **企業内root証明書**

  企業内root証明書はサーバを複数配置する場合にデータの安全性と拡張性を高めるもので、社外の証明機関に頼る必要はありません。企業内root証明書により、クライアントを再設定せずにMobile Link同期サーバを追加できます。

- **グローバル証明書**

  グローバル証明書は企業内root証明書に代わるもので、民間の認証機関が、サーバの身元証明書に署名します。民間の証明機関は秘密鍵を保存する専用設備を持ち、高品質のサーバ証明書を生成します。グローバル証明書には次のような利点があります。

  - 認証機関はそれが署名するあらゆる証明書について身元情報の正しさを保証する義務があるので、定評ある外部の認証機関への委託は企業間通信におけるシステムの信頼性を高める可能性があります。
  - 認証機関は、制御された環境と先進的な手段で証明書を生成します。
  - 証明書の秘密鍵は厳重に秘匿されなくてはなりません。企業にはこのきわめて重要な情報を保存する適当な場所がない可能性がありますが、認証機関は専用の設備を保持しています。

法的注意

アイエニウェア・ソリューションズ株式会社
http://www.ianywhere.jp/