



SSL を使用した Relay Server とマイクロソフト IIS の構成

ホワイトペーパー

著者： Joshua Savill、Product Manager

日付： 2008 年 9 月 26 日

このホワイトペーパーは、SQL Anywhere 11 に基づいて記載されています。

もくじ

| | |
|---|----|
| はじめに | 3 |
| 必要なソフトウェア | 3 |
| Relay Server | 3 |
| Relay Server のアーキテクチャ | 3 |
| 送信イネーブラ | 4 |
| Relay Serverの起動 | 4 |
| Microsoft Internet Information Services での Relay Server の設定 | 7 |
| Relay Server Web 拡張 | 7 |
| Relay Server 構成ファイル | 7 |
| Relay Server Web 拡張の配備 | 8 |
| アプリケーション・プールの作成 | 8 |
| Relay Server Web 拡張の有効化 | 8 |
| Microsoft IIS 用のRelay Serverに関する SQL Anywhere 11 のマニュアル | 9 |
| Relay Server構成ファイルの説明とRelay Serverを Windows サービスとして 起動する方法 | 9 |
| オプション・セクション | 9 |
| Relay Server セクション | 11 |
| バックエンド・ファーム・セクション | 12 |
| バックエンド・サーバ・セクション | 12 |
| 送信イネーブラの使用 | 13 |
| SSL を使用してテストするための Microsoft IIS の構成 | 14 |
| まとめ | 20 |
| | |
| 図 | |
| 図 1 - Mobile Link 同期を使用する Relay Server インフラストラクチャ | 4 |
| 図 2 - Relay Server の起動フェーズ | 5 |
| 図 3 - Relay Server の準備フェーズ | 6 |
| 図 4 - Relay Server の作業フェーズ | 7 |
| 図 5 - Microsoft IIS で SSL 通信用に作成した証明書 | 16 |
| 図 6 - 認証局によって作成された証明書の処理およびインストール | 18 |
| 図 7 - Microsoft IIS に表示された証明書の概要 | 19 |

はじめに

今日の無線および随時接続環境で使用される企業情報システムにとって、安全なデータ転送とデータ可用性は不可欠な要素です。また、データ侵害や機密情報の盗用が頻発する中、データ・セキュリティの必要性は高まる一方です。さらに、データの常時利用可能性への要求も加わり、企業情報システムは新たな限界点に達しつつあります。

Mobile Link は、スケーラビリティの高いセッションベースの同期システムをすでに提供しています。このシステムを利用すれば、統合データベースと呼ばれるメイン・データベースと多数のリモート・データベース間で双方向のデータ転送が可能になります。統合データベースとしては、SQL Anywhere、Sybase Adaptive Server Enterprise、Oracle、Microsoft SQL Server、MySQL、および IBM DB2 (メインフレーム) などの ODBC 準拠データベースのうちのいずれかを使用できます。

IT および Web インフラストラクチャへの新たなニーズが生まれる中、SQL Anywhere の Mobile Link 同期テクノロジーを利用すれば、エンタープライズ・アプリケーションを現場の従業員に流通させるための非常に安全で常時利用可能なソリューションをこれまでよりも柔軟に開発できます。Sybase iAnywhere は、SQL Anywhere 11 で既存の IT および Web インフラストラクチャへの統合を容易にし、データ同期に安全なゲートウェイを提供する新たな機能として Relay Server を導入しました。マルチテナント環境で Relay Server を使用すれば、エンタープライズ・ビジネスに必要な広範囲なサービスをコスト効率良く安全に提供できます。

必要なソフトウェア

- ・ Microsoft Windows 2003 Server
- ・ Microsoft Internet Information Service 6.0
- ・ SQL Anywhere (Mobile Link 11.0.0 および RSA 暗号化オプションを含む)

Relay Server

Relay Server のアーキテクチャ

Relay Server は、Microsoft Internet Information Services (IIS) および Apache Web サーバ用の Web 拡張であり、Web トラフィックの安全な通信を可能にします。これは、マルチテナント環境において負荷分散およびフェールオーバーを実現するうえ、Sybase iAnywhere 製品への統合が容易です。Relay Server は、既存の企業ファイアウォールや IT ポリシーに変更を加える必要なく、既存の IT および Web インフラストラクチャに簡単に統合できます。Relay Server は、Mobile Link、Ultra Light、Qanywhere、およびその他の iAnywhere HTTP/S クライアントから、送信インネーブラと呼ばれる複数のコネクタ・ピースを介して受信した HTTP および HTTPS 要求を処理するように設計されています。

Relay Server を使用すると、Mobile Link、Afari などの複数のバックエンド HTTP サービスが提供されます。Relay Server が企業 DMZ に配置されていれば、構成において内部や外部のファイアウォールで新たなポートを有効化する必要はありません。図 1 は、単一の Relay Server と Mobile Link サーバを使用する一般的な設定を示しています。Relay Server は、企業 DMZ に配置されています。

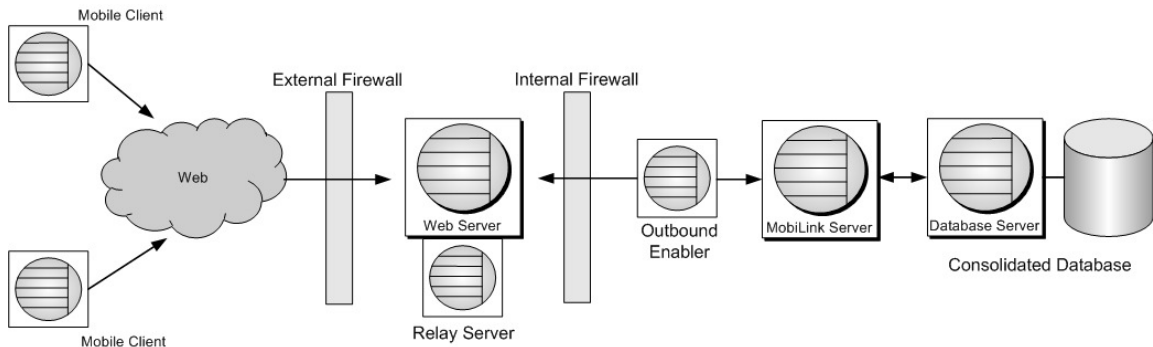


図 1 - Mobile Link 同期を使用する Relay Server インフラストラクチャ

送信イネーブラ

送信イネーブラは、特にバックエンド・サーバと Relay Server 間のコネクタとして使用される SQL Anywhere 11 の新機能です。上の図 1 では、バックエンド・サーバとして送信イネーブラと通信している Mobile Link サーバが示されています。送信イネーブラはダブル・コネクション・ピースの役割を果たします。Mobile Link サーバとのオンデマンド接続と、DMZ の Relay Server との上り／下りチャネル接続ペアを確立します。

Relay Server は、確立された上りチャネルを使用してクライアント要求を送信イネーブラに転送します。送信イネーブラは、クライアント要求をバックエンド・サーバ（この場合は Mobile Link サーバ）にリレーします。送信イネーブラは、Mobile Link サーバから応答を受信すると、確立された下りチャネルを使用して Relay Server に応答を返します。Relay Server は、その応答をクライアントにリレーします。送信イネーブラとクライアントは、2 種類の Web サーバ拡張を使用する Relay Server からサービスを提供されます。クライアント接続には Relay Server クライアント拡張、送信イネーブラにはサーバ拡張が使用されます。

Relay Server ファームが存在する場合、送信イネーブラは、Relay Server との HTTP または HTTPS 接続を確立し、使用可能なすべての Relay Server のリストを取り出すことができます。これを行うには、Relay Server サーバ拡張にマップする URL をサーバに割り当てます。Relay Server ファームを処理するロード・バランサがある場合、サーバ URL がロード・バランサを介して Relay Server サーバ拡張にマップします。

送信イネーブラは、使用可能な Relay Server に関する情報を取得した後、各 Relay Server を使用して上り／下りチャネルのペアを作成します。バックエンド Mobile Link サーバとの通信は、HTTP のみに限られます。送信イネーブラは Mobile Link サーバと同一マシン上で稼働するように設計されているため、HTTPS 通信は存在しません。したがって、この通信の暗号化は必要ありません。送信イネーブラの接続、転送、および切断の各アクティビティは、クライアントおよびバックエンド・サーバにより必

要に応じて実行されます。

Relay Server の起動

Relay Server のアーキテクチャは、以下の 3 つのフェーズに分けられます。

- ・ 起動フェーズ
- ・ 準備フェーズ
- ・ 作業フェーズ

図 2 に示されている起動フェーズは、送信イネーブラが Relay Server (Web サーバが複数ある場合はロード・バランサ) を実行している Web サーバとの接続を確立したときに開始されます。その後、送信イネーブラは、Relay Server ファーム内の使用可能なすべての Relay Server のリストを取得します。

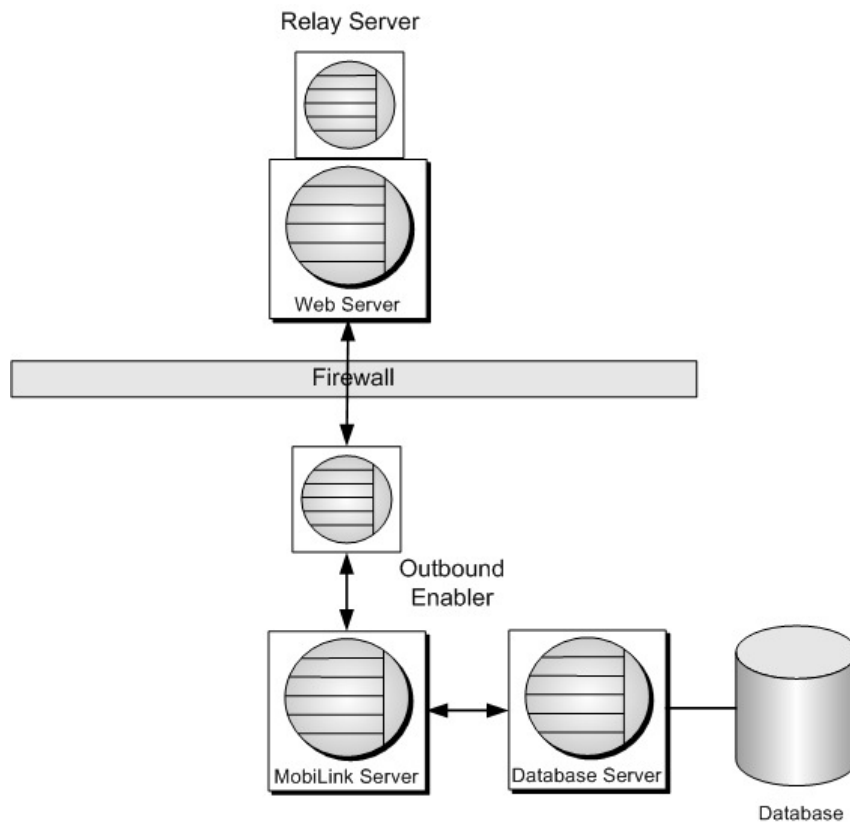


図 2 - Relay Server の起動フェーズ

図 3 に示されている準備フェーズは、送信イネーブラが使用可能なすべての Relay Server のリストを取得したときに開始されます。この時点で、送信イネーブラはバックエンド・サーバが使用可能であるかどうかを検出し、ロード・バランサが存在する場合はそれを迂回しながら各 Relay Server と直接接続を確立します。

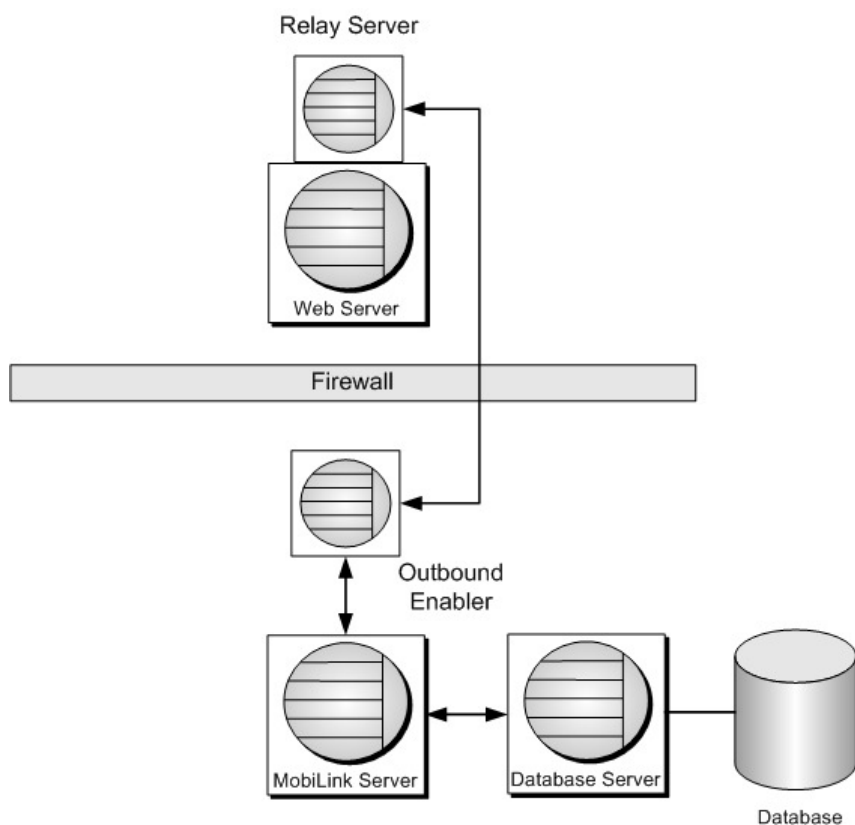


図 3 - Relay Server の準備フェーズ

図 4 に示されている作業フェーズは、Mobile Link、Ultra Light、または QAnywhere クライアントが Web サーバとの接続を確立したときに開始されます。図 4 では、ステートレスな HTTPS 接続が点線で描かれています。Relay Server とクライアント間のすべての接続が Web サーバ（または、存在する場合はロード・バランサ）を経由します。

パフォーマンスのヒント：

ロード・バランサは、クライアントと Relay Server 間の HTTP セッション・アフィニティを維持する必要がありません。同一 HTTP セッション内の各 HTTP 要求は、Relay Server ファームが存在する場合はファーム内の異なる Relay Server を経由できます。HTTP アフィニティ機能をオフにすることで、ロード・バランサのパフォーマンスが著しく向上します。

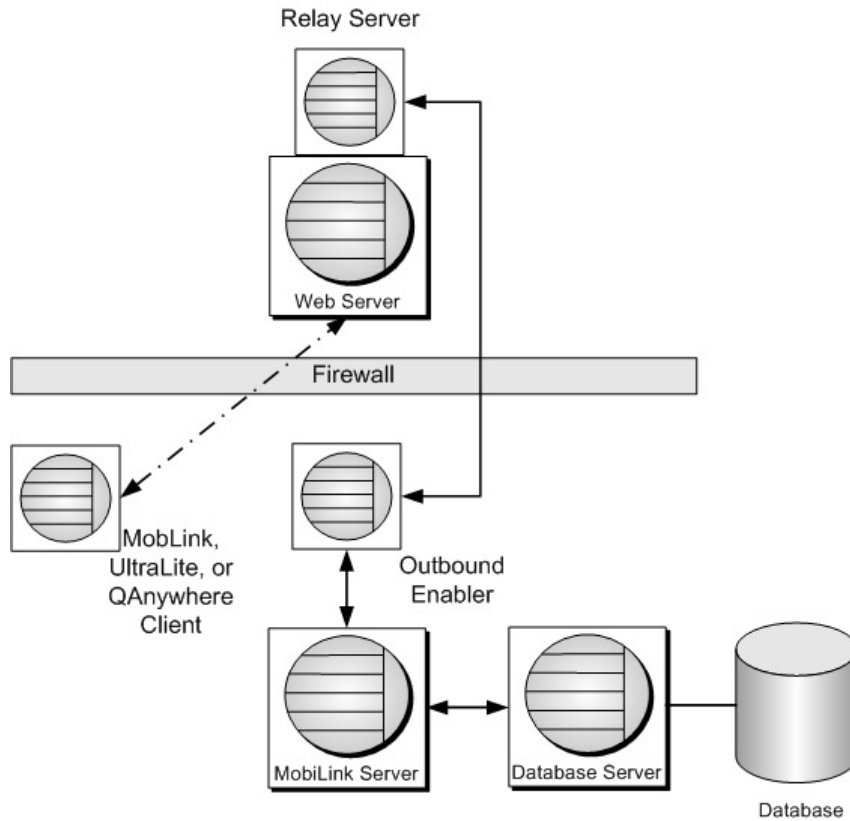


図 4 - Relay Server の作業フェーズ

Mobile Link サーバ・ファームを使用している場合、3 つのすべてのフェーズ（開始、準備、作業）が Mobile Link サーバの数に関係なく発生します。

Microsoft Internet Information Services での Relay Server の設定

Relay Server Web 拡張

Microsoft IIS の Relay Server Web 拡張は、以下の実行可能ファイルで構成されます。

- rs_client.dll
- rs_server.dll
- rshost.exe
- dbngenll.dll
- dbsvc.exe
- dbfhide.exe
- dblank.exe
- dbicull.dll
- dbicutll.dll
- dbsupport.exe
- dbghelp.dll

Relay Server 構成ファイル

Relay Server 構成設定は、以下のファイルに格納されています。

- . rs.config

Relay Server Web 拡張の配備

Windows エクスプローラで、以下の手順を実行します。

1. Relay Server のホーム・ディレクトリ [Default Web Site] (通常は C:\¥Inetpub) の下に、以下のディレクトリを作成します。
 - . ias_relay_server
 - . ias_relay_server¥client
 - . ias_relay_server¥server
2. rs_client.dll を ias_relay_server¥client ディレクトリにコピーします。
3. rs_server.dll、rshost.exe、および rs.config を ias_relay_server¥server ディレクトリにコピーします。
4. 残りの DLL および EXE を ias_relay_server¥server ディレクトリにコピーします。

注：

受信クライアントおよび送信イーネブラ接続のために、¥ias_relay_server¥server ディレクトリ内の DLL は、ネットワーク・サービスからアクセスできなければなりません。したがって、Windows のパスで ¥ias_relay_server¥server ディレクトリにアクセスする必要があります。Windows のパスで ¥ias_relay_server¥server ディレクトリを定義できない場合、手順 4 の DLL を [system32] フォルダまたは Windows のパスで定義されるディレクトリに配置してください。

アプリケーション・プールの作成

Internet Information Services (IIS) マネージャで、以下の手順を実行します。

1. [Application Pools] を右クリックし、[New] - [Application Pool...] を選択します。
2. 新規アプリケーション・プール RSOE_AP を呼び出します。
3. 新規アプリケーション・プール RSOE_AP を右クリックし、[Properties] を選択します。[Performance] タブで、[Shutdown worker processes after being idle for (time in minutes)] の選択を解除します。
4. [Recycling] テーブルで、[Recycle worker processes (in minutes)] の選択を解除します。

Relay Server Web 拡張の有効化

Internet Information Services (IIS) マネージャで、以下の手順を実行します。

1. [Web Sites] の下の ias_relay_server ディレクトリを右クリックし、[Properties] を選択します。[Virtual Directory] タブの [Execute permissions] で、[Scripts and Executables] を設定します。

2. [Application pool] で、関連付けられたアプリケーション・プールとして [RSOE_AP] を設定します。
3. [Web Server Extensions] で、rs_server.dll と rs_client.dll の両方を ISAPI として実行することを許可します。

注：

上記の変更を有効にするには、[Default Web Site] と Relay Server (rshost.exe) を停止して再起動する必要があります。

Microsoft IIS 用の Relay Server に関する SQL Anywhere 11 のマニュアル

Microsoft IIS への Relay Server の配備については、以下の SQL Anywhere 11 のマニュアルを参照してください。

Mobile Link ・ サーバ管理 >>

Mobile Link サーバ ・ テクノロジーの使用 >>

Relay Server >>

Relay Server の配備

Relay Server 構成ファイルの説明と Relay Server を Windows サービスとして起動する方法

Relay Server 構成ファイルを使用して、環境内のすべての Relay Server、Mobile Link サーバ、および Mobile Link サーバ ・ ファームを定義します。構成ファイル rs.config は、以下の 4 つのセクションに分かれています。

- Options
- Relay server
- Backend farm
- Backend server

注：

rs.config ファイルの変更後、Relay Server (rshost.exe) に変更をアップデートする必要があります。アップデートするには、コマンド ・ ラインで rshost -u -f rs.config を実行します。

オプション ・ セクション

ヒント：

Relay Server を Windows サービスとして起動するのが最善の方法であると考えられるため、この項では、Relay Server を Windows サービスとして起動する方法を説明します。

オプション・セクションを使用して、各 Relay Server に適用するプロパティを指定し、Relay Server の起動方法を指定します。このセクションのサンプルを以下に示します。

```
#-----  
# Relay server options  
#-----  
[options]  
start = no  
shared_mem = 10M  
verbosity = 2
```

以下のコマンドは、Relay Server を自動起動の Windows サービスとして設定します。

```
dbsvc -y -as -s Automatic -w rs  
"c:\Inetpub\wwwroot\ias_relay_server\server\rshost.exe" -q -qc  
-f "c:\Inetpub\wwwroot\ias_relay_server\server\rs.config" -o  
"c:\temp\myrshost.log"
```

上記のオプションは、10MB (デフォルト) の共有メモリ・キャッシュを使用して rshost.exe を自動的に起動します。冗長性には、要求レベル・ログ 2 が設定されます。ログ・ファイルは、デフォルトでは %TEMP%\ias_relay_server_host.log ファイルに配置されます。

以下のコマンドは、指定されたとおりに c:\Inetpub\wwwroot\ias_relay_server\server\rs.config ファイルを使用して Windows サービスを起動します。

```
dbsvc -u rs
```

以下のコマンドは、Windows サービスを停止します。

```
dbsvc -x rs
```

rshost.exe のログは、c:\temp ディレクトリに配置されている myrshost.log ファイルに記録されません。

注：

WWW サービスは、Relay Server サービスとは個別に起動および停止する必要があります。

オプション・セクションの詳細については、以下の SQL Anywhere 11 のマニュアルを参照してください。

Mobile Link - サーバ管理 >>

Mobile Link サーバ・テクノロジーの使用 >>

Relay Server >>

Relay Server 設定ファイル >>

オプション・セクション

Relay Server ・ セクション

Relay Server ・ セクションを使用して、環境内に存在する各 Relay Server を定義します。Relay Server セクションの各エントリは、ユニークな Relay Server です。

```
#-----  
# Relay server peers  
#-----  
[relay_server]  
enable          = yes  
host            = RelayHost1.com  
http_port      = 80  
https_port     = 443  
description    = Relay Server Definition 1  
  
[relay_server]  
enable          = yes  
host            = RelayHost2.com  
http_port      = 80  
https_port     = 443  
description    = Relay Server Definition 2
```

上記のサンプルは、ファーム内に RelayHost1.com と RelayHost2.com の 2 つの Relay Server があることを示しています。それぞれ、ポート 80 で HTTP 要求、ポート 443 で HTTPS 要求を受信するように定義されています。

Relay Server セクションの詳細については、以下の SQL Anywhere 11 のマニュアルを参照してください。

MobiLink - Server Administration »

Using MobiLink Server Technology »

Synchronizing through a web server with the relay server »

Relay server configuration file »

Relay server section

バックエンド・ファーム・セクション

バックエンド・ファーム・セクションは、Mobile Link サーバ・ファームのプロパティを指定します。環境内に複数の Mobile Link サーバ・ファームが存在する場合、このセクション内のエントリが複数になります。このセクションのサンプルを以下に示します。

```
#-----  
# Backend farms  
#-----  
[backend_farm]  
enable          = yes  
id              = MobiLink.Server  
client_security = on  
backend_security = on  
description     = The is the MobiLink server farm entry
```

上記のサンプルは、MobiLink.Server という ID を持つ Mobile Link サーバ・ファームが 1 つだけ存在することを示しています。

バックエンド・ファーム・セクションの詳細については、以下の SQL Anywhere 11 のマニュアルを参照してください。

Mobile Link - サーバ管理 >>

Mobile Link サーバ・テクノロジーの使用 >>

Relay Server >>

Relay Server 設定ファイル >>

バックエンド・ファーム・セクション

バックエンド・サーバ・セクション

バックエンド・サーバ・セクションは、Mobile Link サーバが稼働しているマシンへのバックエンド・サーバ接続を定義します。バックエンド・サーバ・セクションの各エントリは、1 つの Mobile Link サーバを定義します。送信イネーブラが Relay Server に接続するときにこの定義情報を使用します。このセクションのサンプルを以下に示します。

```
#-----
```

```

# Backend servers
#-----
[backend_server]
enable    = yes
farm      = MobiLink.Server
id        = MLServer1
mac       = 00-0C-29-7A-C2-AB
token     = 7b2493b0-d0d4-464f-b0de-24643e1e0feb

[backend_server]
enable    = yes
farm      = MobiLink.Server
id        = MLServer2
mac       = 00-0C-29-7A-C2-AB
token     = 9a2633e0-a1b5-321b-d0ac-2667f1a2abc

```

上記のサンプルは、MobiLink.Server サーバ・ファーム内に 2 つの Mobile Link サーバが存在することを示しています。それぞれの Mobile Link サーバが同一マシン上で稼働しており、ユニークな ID とマシンのネットワーク・アダプタの MAC アドレスで識別されています。Relay Server とのバックエンド・サーバ接続を認証するために、ユニークなセキュリティ・トークンも定義されています。バックエンド・サーバ・セクションの詳細については、以下の SQL Anywhere 11 のマニュアルを参照してください。

```

Mobile Link - サーバ管理 >>
  Mobile Link サーバ・テクノロジーの使用 >>
    Relay Server >>
      Relay Server 設定ファイル >>
        バックエンド・サーバ・セクション

```

送信イネーブラの使用

送信イネーブラは、Relay Server と Mobile Link サーバ間のダブル・クライアント・コネクタのようになっています。送信イネーブラは、HTTP または HTTPS を使用する Relay Server と、HTTP のみ使用する Mobile Link サーバとの接続を確立し、Relay Server と Mobile Link サーバ間の通信および要求を円滑にします。

さらに、送信イネーブラは、Mobile Link サーバとの接続を確立できない場合、Relay Server にレポートを返します。その時点で、送信イネーブラは Relay Server との接続を終了し、Mobile Link サーバが

オンライン状態に戻るまでは、Relay Server から新たな要求を受け付けません
送信イネーブラのサンプル・コマンド・ラインを以下に示します。

```
"%SQLANY11%\bin32\rsoe.exe" -cr "host=relayserver.sybase.com;port=80" -cs  
"host=localhost;port=80" -f MobiLink.Server -id MLServer1 -t  
7b2493b0-d0d4-464f-b0de-24643e1e0feb
```

- ・ rsoe.exe は、送信イネーブラ・ユーティリティです。
- ・ -cr <接続文字列> は、Relay Server (HTTP または HTTPS) への接続です。
- ・ -cs <接続文字列> は、Mobile Link サーバ (HTTP) への接続です。
- ・ -f MobiLink.Server は、バックエンド・サーバのファーム名です。
- ・ -id MLServer1 は、Mobile Link サーバに割り当てられる名前です。
- ・ -t 7b2493b0-d0d4-464f-b0de-24643e1e0feb は、Relay Server に渡されるセキュリティ・トークンです。

注：

-cs スイッチが送信イネーブラのコマンド・ラインで指定されていない場合、デフォルトで host=localhost;port=80 になります。

送信イネーブラ用に使用できる追加スイッチがあります。送信イネーブラの詳細については、以下の SQL Anywhere 11 のマニュアルを参照してください。

Mobile Link ・ サーバ管理 >>

Mobile Link サーバ・テクノロジーの使用 >>

Relay Server >>

Outbound Enabler

SSL を使用してテストするための Microsoft IIS の構成

SSL 暗号化を使用する Microsoft IIS を構成する際にまず必要なのは、認証局の証明書（ルート証明書）を作成することです。ルート証明書を作成するには、RSA 暗号化オプションに装備されている createcert ユーティリティを使用します。

注：createcert ユーティリティの詳細については、以下のサイトを参照してください。

<http://www.sybase.com/detail?id=1055179>

1. 以下のコマンドを実行します。

```
C:\>"%SQLANY11%\win32\createcert"  
SQL Anywhere X.509 Certificate Generator Version  
10.0.1.3662  
Choose encryption type ((R)SA or (E)CC): RSA  
Enter RSA key length (512-16384): 1024  
Generating key pair...
```

```
Country Code: CA  
State/Province: ON  
Locality: Waterloo  
Organization: Sybase  
Organizational Unit: Sybase  
Common Name: Sybase  
Enter file path of signer's certificate:  
Certificate will be a self-signed root  
Serial number [generate GUID]:  
Generated serial number:  
de9cd2c1270f4af980f525ca4a779b4a  
Certificate valid for how many years (1-100): 10  
Certificate Authority (Y/N) [N]: Y  
1. Digital Signature  
2. Nonrepudiation  
3. Key Encipherment  
4. Data Encipherment  
5. Key Agreement  
6. Certificate Signing  
7. CRL Signing  
8. Encipher Only  
9. Decipher Only  
Key Usage [6,7]:  
Enter file path to save certificate: rsa_root.crt  
Enter file path to save private key: rsa_key.key  
Enter password to protect private key: pwd  
Enter file path to save identity: id.pem
```

2. 通信の安全性を確保するために、Microsoft IIS Web サーバを構成する必要があります。それには、認証局の署名を受ける必要がある Web サーバ証明書を作成する必要があります。
 - a. Internet Information Services (IIS) マネージャで、[Default Web Site] - [Properties] を

選択します。

- b. [Web Site] タブで、[SSL port] に 443 を設定します。
- c. [Directory Security] タブで [Server Certificates] を選択し、[Create New Certificate] - [Prepare the request now, but send it later] を選択します。
- d. [Name] に Default Web Site、[Bit length] に 1024 を指定します。
- e. [Organization] および [Organizational unit] はどちらも Sybase にします。
- f. 新しい証明書の [Common name] は jsavill-iis にします。
- g. [Country] は CA、[Province] は ON、[City] は Waterloo にします。
- h. certreq.txt ファイルを保存します。

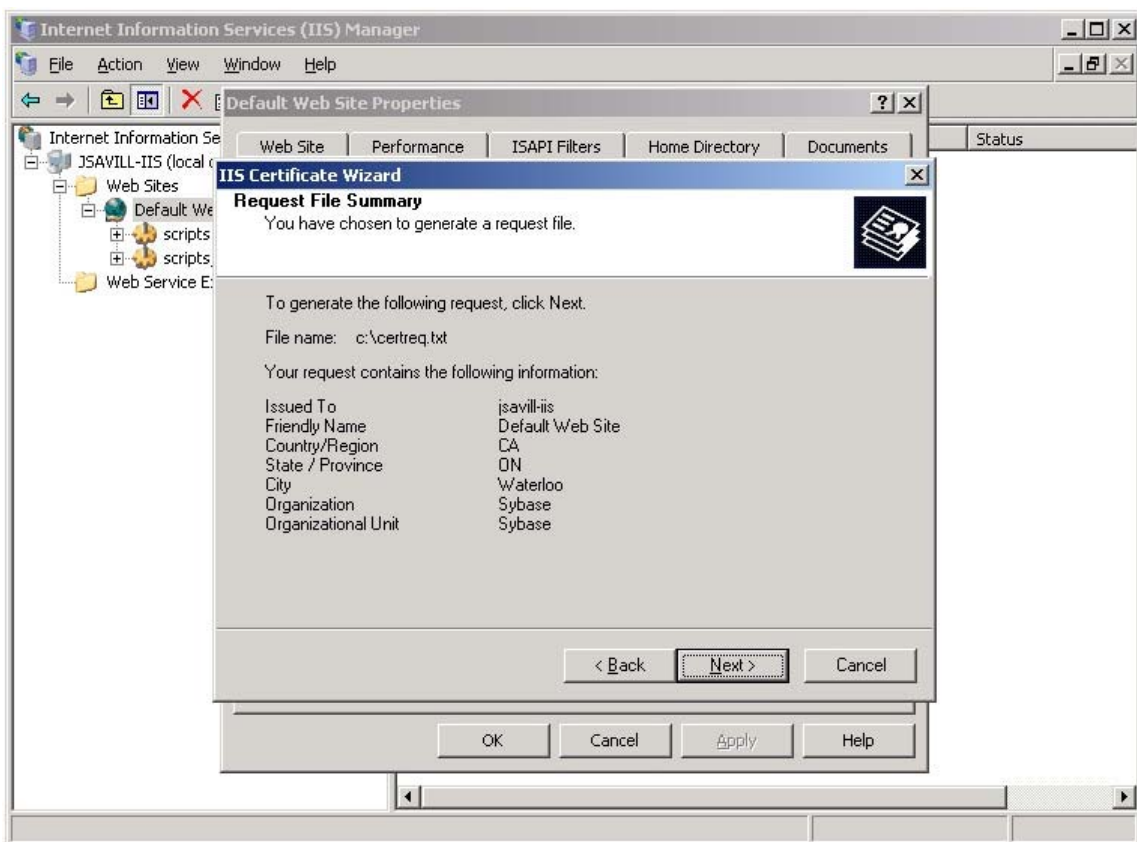


図 5 - Microsoft IIS で SSL 通信用に作成した証明書

- 3. Microsoft IIS で作成した certreq.txt ファイルを認証局に署名してもらう必要があります。以下のコマンドを実行します。

```
C:\>"%SQLANY11%\win32\createcert" -s certreq.txt
SQL Anywhere X.509 Certificate Generator Version
10.0.1.3662
Enter file path of signer's certificate: rsa_root.crt
Enter file path of signer's private key: rsa_key.key
```


Enter password for signer's private key: pwd
Serial number [generate GUID]:
Generated serial number:
c79a26d921ed411b91bf565ae0c30f28
Certificate valid for how many years (1-100): 10
Certificate Authority (Y/N) [N]:
1. Digital Signature
2. Nonrepudiation
3. Key Encipherment
4. Data Encipherment
5. Key Agreement
6. Certificate Signing
7. CRL Signing
8. Encipher Only
9. Decipher Only
Key Usage [3,4,5]:
Enter file path to save certificate: rsa_iis.crt

4. 証明書を確認するために、以下のコマンドを実行します。

```
C:\>"%SQLANY11%\win32\viewcert" rsa_iis.crt  
SQL Anywhere X.509 Certificate Viewer Version  
10.0.1.3662
```

X.509 Certificate

```
Common Name:          jsavill-iis  
Organizational Unit:   Sybase  
Organization:         Sybase  
Locality:             Waterloo  
State/Province:       ON  
Country Code:         CA  
Issuer:               Sybase  
Serial Number:  
c79a26d921ed411b91bf565ae0c30f28  
Issued:               Apr 9, 2008  14:08:00  
Expires:              Apr 10, 2018 14:08:00  
Signature Algorithm:  RSA, SHA1
```

Key Type: RSA
Key Size: 1024 bits
Basic Constraints: Is not a certificate authority
Key Usage: Key Encipherment, Data
Encipherment, Key Agreement

- Microsoft IIS で作成された certreq.txt ファイルを署名した後、createcert ユーティリティは SSL の証明書を作成しました。この証明書は、rsa_iis.crt として保存されています。この証明書を Microsoft IIS で処理してインストールする必要があります。Microsoft IIS で、[Default Web Site] - [Properties] を選択します。
- [Directory Security] タブで [Server Certificate] を選択し、[Process the pending request and install the certificate] を選択します。
- rsa_iis.crt の場所を指定します。

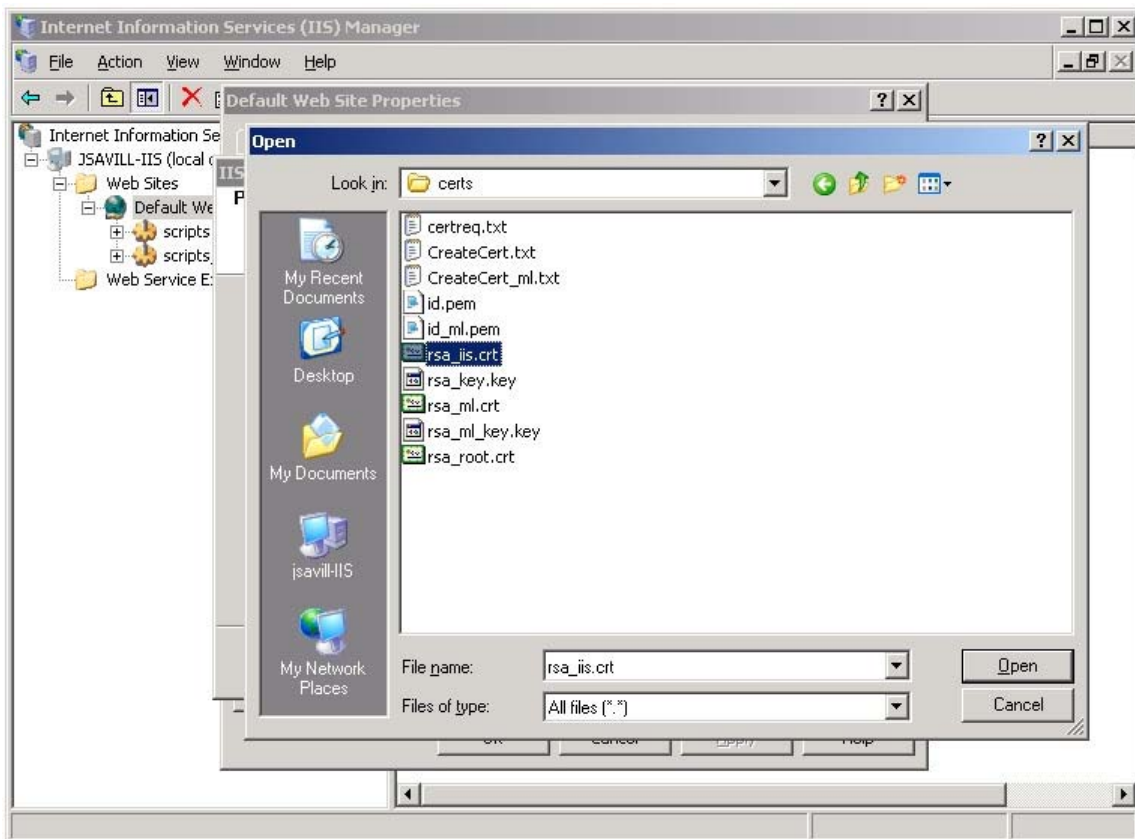


図 6 - 認証局によって作成された証明書の処理およびインストール

- [SSL port] に 443 を設定し、ウィザードを終了します。

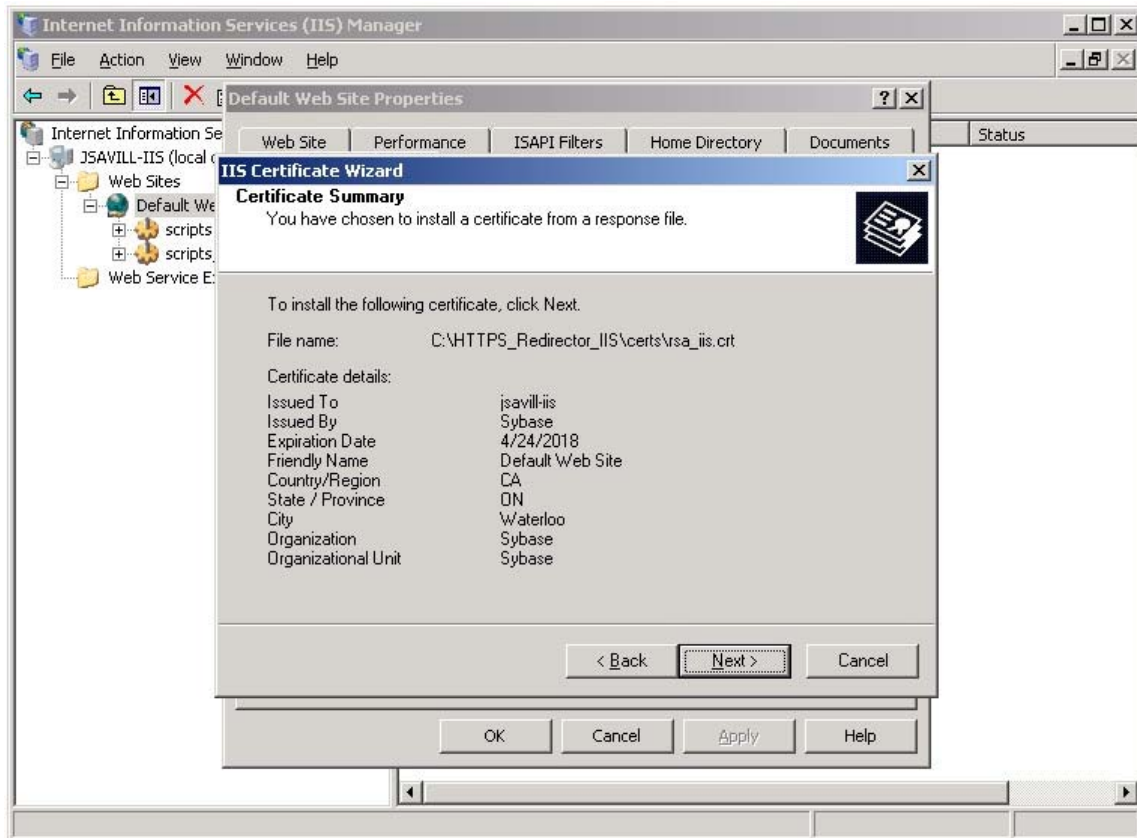


図 7 - Microsoft IIS に表示された証明書の概要

9. IIS への HTTPS 接続を確認します。
 - a. インターネット・ブラウザを実行します。
 - b. [アドレス] フィールドに `https://servername` を入力し、[Enter] を押します。
 - c. [Continue to this website] をクリックします。証明書が正しくインストールされていれば、Under Construction (作成中) が表示されます。

注：

運用システムの場合、評判の高い認証局からサーバ証明書を購入してください。Relay Server・ファームの証明書に関する考慮事項を以下に示します。

1. 標準的な証明書を持つロード・バランサ。Relay Server は、個々に標準的なサーバ証明書が必要です。
2. SSL を持たないロード・バランサ。Relay Server は、標準的なワイルドカード証明書が必要です。この設定は、ドメイン名と証明書の共通名を検証しないクライアントに有効です。たとえば Ultra Light には有効ですが、UltraLiteJ には無効です。
3. 標準的な証明書を持つが、Relay Server 用の証明書を持たないロード・バランサ。この設定は、送信インーブラと Relay Server 間の上り／下りチャネルで HTTPS をサポートしません。クライアントは、依然として通信に HTTPS を使用できます。

セキュリティのために必要な証明書の種類は、ビジネス・ニーズおよび暗号化の要件によってまったく異なります。

まとめ

iAnywhere は、SQL Anywhere 11 の新機能として Relay Server を導入しました。Relay Server により、既存の IT および Web インフラストラクチャとの統合が容易になると同時に、データ同期用にセキュアなゲートウェイを提供することが可能になります。マルチテナント環境での Relay Server の採用は、大企業に求められる広範なサービスをセキュリティ保護する方法として費用効果に優れていると言えます。

このマニュアルでは、Relay Server と マイクロソフト IIS の連携構成により、セキュアな Mobile Link 同期を実現する方法について説明しました。このマニュアルを通読することで、新しい Relay Server の機能を使用して Mobile Link、Ultra Light、QAnywhere、およびその他の iAnywhere クライアントとマイクロソフト IIS の間に SSL 通信に基づく包括的な同期システムをセットアップする方法を理解したことになります。

Copyright (C) 2008 iAnywhere Solutions, Inc. All rights reserved.

iAnywhere Solutions、iAnywhere Solutions（ロゴ）は、iAnywhere Solutions, Inc.とその系列会社の商標です。その他の商標はすべて各社に帰属します。

本書に記載された情報、助言、推奨、ソフトウェア、文書、データ、サービス、ロゴ、商標、図版、テキスト、写真、およびその他の資料（これらすべてを"資料"と総称する）は、iAnywhere Solutions, Inc.とその提供元に帰属し、著作権や商標の法律および国際条約によって保護されています。また、これらの資料はいずれも、iAnywhere Solutionsとその提供元の知的所有権の対象となるものであり、iAnywhere Solutionsとその提供元がこれらの権利のすべてを保有するものとしします。

資料のいかなる部分も、iAnywhere Solutionの知的所有権のライセンスを付与したり、既存のライセンス契約に修正を加えることを認めるものではないものとしします。

資料は無保証で提供されるものであり、いかなる保証も行われません。iAnywhere Solutionsは、資料に関するすべての陳述と保証を明示的に拒否します。これには、商業性、特定の目的への整合性、非侵害性の黙示的な保証を無制限に含みます。

iAnywhere Solutionsは、資料自体の、または資料が依拠していると思われる内容、結果、正確性、適時性、完全性に関して、いかなる理由であろうと保証や陳述を行いません。iAnywhere Solutionsは、資料が途切れていないこと、誤りがないこと、いかなる欠陥も修正されていることに関して保証や陳述を行いません。ここでは、「iAnywhere Solutions」とは、iAnywhere Solutions, Inc.またはSybase, Inc.とその部門、子会社、継承者、および親会社と、その従業員、パートナー、社長、代理人、および代表者と、さらに資料を提供した第三者の情報元や提供者を表します。