JDMail V3.10 SSL/TLS 数字签名及加密邮件

邮件数字安全传输及数字签名是安全邮件的灵魂。但是由于 CA 认证的复杂及难于管理导致很多企业没有用起来。JDMail 在长期客户服务过程中，感同身受，切肤之痛。

为此，JDMail V3.10 采用内嵌 CA 中心的做法，支持公共 CA 和私用 CA 两种方式，化繁为简，让企业不需要借助公共 CA，不需要购买 CA 证书，就可以使用安全电子邮件传输服务。

要使用 JDMail 的 SSL/TLS 服务您需要必要的证书(服务器证书、客户端证书、CA 证书)、生成・管理私钥。同时，创建私用认证中心(CA)认证 SSL/TLS 服务。

此外，用 JDMail 制作的证书还可以用作其它网络服务。

TOP(关于 SSL/TLS)
关于 SSL/TLS 的概要和在 JDMail 的 SSL/TLS 实现的说明。

现在的环境
为了让 JDMail 具备运行 SSL/TLS 的环境，检查现在的安装状况。

公共运行环境的安装
在使用公共认证机构（CA）证书的场合，需要从本菜单创建私钥和 CSR（证书签名请求）。CSR 经过 CA 认证签名后方可使用。

私用运行环境的安装
服务器证书由自己签署并且私用的场合可以使用本菜单。

私人证书颁发机构（CA）的使用
如果安装私人证书颁发机构（CA），可以利用本菜单生成里签名了的服务器证书。这个情况下，需要客户端(Outlook 等)安装 CA 证书。否则连接时会有警告。

CA 证书的生成
为使客户端通过认证，客户端需要安装设置 CA 证书。

客户端证书的生成

创建一个由私人证书颁发机构签署的客户端证书。客户端证书的安装运行可以使客户端软件（如 Outlook）运行更加安全。

已制作证书的管理

使用本菜单查看已生成的证书、内容的确认、失效处理、删除等操作。

SSL/TLS 简介

关于 SSL/TLS

jdmail 的 SSL/TLS 有很多选项，创建一个证书过程对初次接触者似乎有些挑战。本页明确描述了建立 SSL/TLS 生产环境的步骤，您可以据此创建您环境。

SSL 和 TLS
jdmail 的 SSL/TLS 功能
SSL/TLS 使用环境设置
SSL/TLS 功能的禁用
只使用 SSL 功能

SSL 和 TLS

SSL(Secure Socket Layer)是 Netscape 公司开发的安全性协议，是一种用来加密网络数据通信的机制。该版本 3(SSL v3)被 IETF(The Internet Engineering Task Force)作为互联网标准的规范(RFC 3207)，称为 TLS(Transport Layer Security) 。

SSL 是一种加密通讯链路结构。添加了证书等基本认证的东西是 TLS。今天，实际被运用的技术是 TLS。 因为习惯问题，一般写作 SSL/TLS 。

JDMail 的 SSL/TLS 功能

jdmail 的 SSL/TLS 可以承受在大企业集团等组织的正式使用，中小企业也简单易用。

服务器端和客户端 SSL/TLS 的特点：

支持 STARTTLS SMTP、STLS POP3 。
不仅仅是客户/服务器间,转发服务器间也能使用 SSL/TLS 。
网关连接和转发连接，不同情况下 SSL/TLS 的使用由开/关决定。

可以映射到任意 IP 地址和端口号来使用 SSL/TLS 功能。
创建服务器证书和私钥（公共密钥，数字 ID）的 OpenSSL 库也包括在内。
可以自行创建证书颁发机构（CA 中心），不依赖于公众 CA 中心（证书颁发机构），所以您可以立即启动该服务。

SSL/TLS 使用环境安装

典型的 SSL/TLS 运行环境的安装。

现在的环境
[jdmail 环境设定]、[jdwa 环境设定] 查看当前的 SSL/TLS 环境设置。如果安装不顺利，请检查这个设置。

制作服务器证书请求文件
如果从正式的认证机关(CA)取得服务器证书(公钥)安装公共服务的手续，提交 CSR 文件生成服务器证书。大部分的正式认证机关需要收费才能取得证书。

制作、安装自签名服务器证书
自己制作服务器证书。

创建私用证书颁发机构（CA 中心），制作、安装私用 CA 签名的服务器证书
创建私用的 CA 发证机构，为服务器和客户端生成 CA 证书。

安装 CA 证书
如果 jdmail 进行客户端证书的验证，客户端 CA 证书也有必要安装。jdmail 不使用 Windows 的证书存储区。jdmail 默认不进行客户证书的验证。

制作客户端私钥・证书
使能实行客户端认证。客户端认证，在服务器方面以 SSL/TLS session 验证 Mailer 等出示的客户端证书。推荐用于特别重视安全性服务的情况。

已生成证书的管理
管理已经制作的证书和已发行证书的失效处理。

要完全停止 SSL/TLS 功能

jdmail 默认 SSL/TLS 为开。如果 OpenSSL 相关文件缺失或者服务器证书、密钥不存在，可能会导致使用异常。如果您禁用 SSL/TLS 可以照以下步骤做。

停用 SSL ，[基本设置]-[注册表登记] jdmail 的启动选项追加 -B- -W- -X- 。

停用 TLS ，[环境设置]-[jdmail 环境设置]-[SSL/TLS 相关设置] 以下的 3 项目设为 "无效" 。

1) CTRL TLS 支持 (EnableCTRL-TLS)
2) POP3 TLS 支持 (EnablePOP3-TLS)
3) SMTP TLS 支持 (EnableSMTP-TLS)

只使用 SSL 功能

只使用 SSL 做加密通信，不使用 TLS ，做如下配置： [环境配置]-[jdmail 环境配置]-[SSL/TLS 相关设置] 以下的 3 项设为"无效"。

1) CTRL TLS 支持 (EnableCTRL-TLS)
2) POP3 TLS 支持 (EnablePOP3-TLS)
3) SMTP TLS 支持 (EnableSMTP-TLS)

诊断当前的运行环境

现在的运行环境

JDMail 可以自动诊断当前系统的 SSL/TLS 环境。请根据诊断结果做相应配置。

JDMail 使用 SSL/TLS 服务，必须至少满足以下的条件。

OpenSSL 库文件(libeay32.dll, ssleay32.dll)合适的版本放在正确的路径下。
服务器证书（server.cert）和私钥（server.key）在 JDMail 的 MailRoot 下。
使用客户端证书需要在 MailRoot 内有 CA 的根证书(certs.pem)。或在 MailRoot\certs 内有转换为哈希保存的 CA 证书。

JDMail 的环境配置 SSL/TLS 为开。这是 JDMail 的默认设置。
本页具体检查以下各项目。以下任何一项有问题， SSL/TLS 服务将不能运行。

«诊断» OpenSSL 的环境
«诊断» 私钥、服务器证书(公钥)、CA 证书(可选)
«诊断» JDMail 的 SSL/TLS 环境

诊断» OpenSSL 的环境

本地主机 SSL/TLS 的 OpenSSL 的通信所需的库当前状态为如下。

OpenSSL 命令(c:\MailRoot\bin\openssl.exe) 的版本是 0.9.8i 。
libeay32.dll 在 C:\WINDOWS\system32 已安装。

ssleay32.dll が C:\WINDOWS\system32 已安装。

OpenSSL 的环境是没有问题的。 如果关联文件的配置没有问题，服务器证书和 JDMail 环境也没有问题，但是不能使用 SSL/TLS 服务的情况，可能因为版本没检查，openssl.exe 与 libeay32.dll、ssleay32.dll 有版本不一致的可能性。请用 JDMail 安装包中包含的这些文件二进制试试。

如果在同样主机上安装 Apache 等其它使用 SSL 的 WWW 服务器，由于 C:\WINDOWS\system32 目录相关文件被覆盖，与 JDMail 自带的 openssl.exe 版本不一致。这个情况下，请从 OpenSSL 网站(http://www.openssl.org) 重新下载安装最新版本，使之相互兼容。

诊断» 私钥、服务器证书(公钥)、CA 证书

本地主机的 SSL/TLS 的通讯所需的文件的当前状态如下。

服务器证书文件(c:\MailRoot\server.cert)存在。这个证书和密钥不是一对(验证完成)。
私钥文件(c:\MailRoot\server.key)存在。
CA 证书文件(c:\MailRoot\certs.pem)存在。
当前的环境 SSL/TLS 不能使用。
为了 JDMail 使用 SSL/TLS ，至少需要密钥和服务器证书。

诊断» JDMail 的环境

本地主机当前 JDMail 的环境如下。

POP3S(POP3 over SSL) 有效。
SMTPS(SMTP over SSL) 有效。
CTRLS(CTRL over SSL) 有效。
POP3S-TLS 已停止。
SMTP-TLS 已停止。
CTRL-TLS 已停止。
没实行客户端证书认证。
POP3S，SMTPS，CTRLS 启用，SSL 协议可以互相沟通。换言之，可以进行简单的加密传输。

POP3S-TLS、SMTPS-TLS、CTRLS-TLS 设为有效的场合，TLS 协议可以互相沟通。TLS 通信时，客户端首先使用非 SSL 协议连接到服务器，服务器端启动 TLS 回应等待确认，如果回应，重新开始 SSL 连接。

如果 POP3S、SMTPS、CTRLS 设为无效， POP3S-TLS、SMTPS-TLS、CTRLS-TLS 设为有效的情况下，也可以使用 SSL 通信。

配置为公共运行环境下

公用运行环境的安装

为了从正式的证书颁发机构(CA)取得您的 JDMail 服务器的证书，正式运营 SSL/TLS 服务需要进行以下的工作。

生成您的 JDMail 的私钥和证书签名请求(CSR)文件(表单提交自动生成)。
证书签名请求文件发送到证书颁发机构（手动）。
从证书颁发机构（CA）得到服务器证书、CA 证书。CA 证书也有没有的情况(手工操作)。

服务器证书和私钥、CA 证书（本地主机如有的话）安装在 c:\MailRoot 或 JDMail 其它的 MailRoot 文件夹（手动）。

JDMail 的环境配置把 SSL/TLS 设为开。这是 JDMail 的默认设置。
正式的 SSL/TLS 服务，在互联网邮件服务中使加密通讯成为可能的同时，证书颁发机构（CA）保证你的使用的合法性。由于可以进行客户端认证，有效地防止了「冒充」、「欺骗」，因而能提供更高安全水平的邮件服务。

«诊断» 本地主机当前的运行环境如下。私钥、服务器证书是运行 SSL/TLS 必不可少的。如果进行客户证书的验证还需要 CA 证书。

私钥和服务器证书对不存在。
私钥已安装。
CA 证书已安装。

新建私钥、证书签名请求(CSR)

本地主机（localhost）的私钥文件(server.key)在文件夹 c:\MailRoot\sslconf 中。和证书签发请求文件（server.csr）自动成对创建的。这两个文件可以从处理完成页，或 [已生成证书的管理]页下载。

▽如果使用过去的生成信息请选择 2009/08/17 18:15 生成 - mail.mailer.cn 2009/08/17 17:47 生成 - mail.mailer.cn

国家代码 (2 个字符。中国是 CN)
省市县名 (ex: Beijng)
市区镇村名 (ex:haidian)

组织名　(ex: Chundi　Co., Ltd.)
部门名称　(ex: Development、空白可)
通用名称　(ex: mail.mailer.cn)
电子邮件　(空白可)
密钥长度　(ex: 1024)
备注

你必须填写正确的信息。
根据证书颁发机关的不同,「市区镇村名」被要求详细输入，工作岗位名有被认为是必需的。
「通用名称」是指定您的邮件服务器（FQDN）的完全合格的域名。域名的 MX 请在资源记录定义。同时，在这里指定的域名必须以「组织名」指定的组织所有。

当有多台 JDMail 服务器需要安装证书，您可以(1) 根据每个通用名称不同获取不同的证书(2) 获取通配符证书（*. domain.com 指定为共同的名字）。
「密钥的长度」请遵从发证机关申请的内容。
「备注」作为参考可以用任意的内容(可中文)。

请设定 Mailer 的「证书验证」

如果您将 JDMail 配置为公共的 SSL/TLS，请把对本地用户 Mailer 验证证书的设定设为开，这样将提高安全性。

如果使用 Mailer 验证证书，需要在那个环境中配置邮件服务器名与用上列「通用名字」相同。

这个运行环境的问题点

除了费用、时间外，这个运行环境基本没有问题点。如果是大型集团企业、政府公众服务机构等伴随社会责任的组织，建议使用公共 SSL/TLS 服务运行环境。

您在正式购买 CA 证书前，最好先试用免费证书（一般 30 天）服务。

配置为私用运行环境下

私用运行环境的安装

如果不是从正式的发证机关(CA)获取服务器证书，而是使用自我签名的私用证书运营 SSL/TLS 服务，需要准备以下的工作。

由 JDMail 服务器创建一对自签名的服务器证书和私钥（表单自动处理）。
用同样的一对密钥可以安装多个 JDMail 服务器。

在本地主机服务器证书和私钥对安装在 c:\MailRoot 或其它的 JDMail 的 MailRoot 文件夹内(表单自动处理或手动)。

JDMail 的环境配置把 SSL/TLS 设为开。是 JDMail 的默认设置。
利用私用的服务器证书的 SSL/TLS 服务，验证证书的合法有效性的话会出错。
Mailer 默认不检查合法性是不可能的。如果 Mailer 验证服务器证书内容有问题，可以在 Mailer 证书类型选择 [私用证书颁发机构]。

«诊断» 本地主机当前的运行环境如下。 不创建私钥・服务器证书密钥对不能使用 SSL/TLS 服务。如果进行客户端证书的验证 CA 证书也必须要。

私钥和服务器证书对不存在。
私钥已安装。
CA 证书已安装。

新建私钥・服务器证书

本地主机的私钥(server.key)和自签名的证书(server.cert)自动生成在 c:\MailRoot\sslconf 文件夹内。两个文件可以从处理完成页或 [已创建证书的管理]页下载。如果您安装在本地主机上，直接[立即安装]，并检查。

▽如果您使用在过去创建的信息，请选择 2009/09/17 10:18 作成 - mail2.mailer.cn 2009/08/17 18:17 作成 - mail.mailer.cn

国家代码 (2 个字母。中国是 CN)
省市名 (ex: Beijing)
区县名 (ex: haidian)
组织名 (ex: Chundi Co., Ltd.)
部门名 (ex: Development、空白可)
通用名称 (ex: mail.mailer.cn)
电子邮件 (空白可)
密钥长度 (ex: 1024)
有效天数 (ex: 3650)
安装 立即安装
备注

包括「通用名」可以登记虚构的内容，不过，内容有可能被客户端用户看到。
立刻安装的话，现有的内容会被覆盖，如果既存的东西是自我签名的没有问题，
如果是正式的东西请务必先做好备份。
如果继续私用，用本菜单重新生成私钥和证书覆盖旧的，也没有影响。
「备注」作为参考项可以用任意的内容(中文也可)。

客户端 Mailer 设定为「不验证证书」

如果设置 JDMail SSL/TLS 服务为私用，对 JDMail 的本地用户 Mailer，请设定证书的验证功能为关。如果把验证功能打开，有可能会报错误而不能使用服务的情况。按 Mailer 的具体设置请查阅下列「Mailer 的设置」。

如果使用 Outlook(Express) 没有把证书的验证功能关闭的情况下，在最初的连接的时候会发出警告，不过，如果不中止继续执行，此后就可以使用服务，直到关闭都不会报错。

这个使用环境的问题点

JDMail 服务器证书的取得不需要任何费用，简单地就可以安装运行 SSL/TLS 环境。不过，有不能验证证书这样的问题点。即，在维持高度安全性环境下，少数的 Mailer 等实际连接会有警告问题。

Mailer 的设置注意事项

以下总结了从本页制作的私钥和证书进行私用的 SSL/TLS 服务的主要的 Mailer 的使用状况。

Windows XP 环境	发信(SMTP)	收信(POP3)
Becky!(试用版)	△(验证证书×)	△(验证证书×)
EdMax(免费版)	△(验证证书×)	△(验证证书×)
Mozilla Thunderbird	△(最初连接有安全警告，可以继续执行)	△(最初连接有安全警告，可以继续执行)
nPOP	△(验证证书×)	△(验证证书×)
Outlook(Office 2003)	△(最初连接有安全警告，可以继续执行)	△(最初连接有安全警告，可以继续执行)、TCP/110×
Outlook Express 6	△(最初连接有安全警告，可以继续执行)	△(最初连接有安全警告，可以继续执行)、TCP/110×
Windows Vista 环境	发信(SMTP)	收信(POP3)
Becky!(試用版)	△(验证证书×)	△(验证证书×)
EdMax(免费版)	×(只可使用非 SSL)	×(只可使用非 SSL)
Mozilla Thunderbird	△(最初连接有安全警告，可以继续执行)	△(最初连接有安全警告，可以继续执行)

nPOP	△(验证证书×)	△(验证证书×)
Outlook(Office 2007)	△(最初连接有安全警告，可以继续执行)	△(最初连接有安全警告，可以继续执行)

私用 CA 的使用

私用证书颁发机构（私用 CA）的使用

安装私用证书颁发机关(自我认证，私用认证)，作为「被信赖了的证明机关」登记在客户端 PC。由这个发证机关发行的服务器证书和客户证书的验证就不会出现错误。想用客户端证书认证 SSL/TLS 服务的情况可以用本菜单。

步骤如下。用本菜单安装私用 CA 是为了能制作 •安装 JDMail 的的服务器证书。如果制作 Mailer 的客户证书请用 [私人客户证书的制作]菜单。

安装私用 CA(自我认证)，制作 CA 自身的密钥 • 证书(表单提交自动生成)。
生成客户端 PC 安装的私用 CA 证书(DER 文件)(手工)。
生成 JDMail 的私钥和证书签名要求(CSR)，用私用 CA 证书签名证书签名要求，制作 JDMail 服务器的证书(从表单自动处理)。
本地主机私钥 •证书安装在 c:\MailRoot 或其它的 JDMaill 的 MailRoot 文件夹内。(表单自动处理或手动)。
JDMail 的环境配置把 SSL/TLS 设为开，这是 JDMail 的默认设置。
如果有多个 JDMail 服务器，重复 3-5 步。
如果使用私用 CA 的 SSL/TLS，JDMail 服务器证书 •私钥不是用 [私人使用]菜单，而是使用本菜单制作。

«诊断» 本地主机的现在的运行环境如下。私钥 •服务器证书是一对，缺一不可运行 SSL/TLS 服务。如果进行客户证书的验证 CA 证书也必须。

私用 CA 已安装。
服务器证书存在,不过，未被现在的私用 CA 签名。
私钥存在，但是和服务器证书不配对。
CA 证书已安装。

私用证书颁发机构（私用 CA）成立

有效期限内不需要重新做 CA。
CA 有效期限从 2009/09/17 到 10000 日(約 27 年) 。

如果需要重新做 CA，CA 证书(DER 文件)需要重新安装，之前制作的服务器证书也需要重新制作。

下载客户 PC 安装用 CA 证书(DER 文件)。
安装方法请看这里。

国家代码 (2 个字符。中国是 CN)
省市 (ex: Osaka)
县乡村 (ex: Kita-ku)
组织名 (ex: MyCorp)
部门 (ex: Sales、空白可)
通用名称 (ex: Private CA)
电子邮件 (空白可)
备注

包含「通用名」可以输入虚构的信息，但是，内容有可能被客户看到。
使用用这个表单，有效期限 10000 日的 CA 证书被制作。

制作私用 CA 签名的服务器证书

本地主机的 c:\MailRoot\sslconf 文件夹内私钥文件(server.key)和私用 CA 签名了的服务器证书文件(server.cert)自动生成。两个文件可以从处理完成页或[已制作完毕证书的管理]页下载。如果是本地主机请选择 [立刻安装] 并检查安装结果。

▽如果利用过去的制作信息请选择 2009/09/17 10:33 制作 - mx.mailer.cn 2009/08/17 17:46 制作 - mail.mailer.cn

国家代码 (2 个字母。中国是 CN)
省市 (ex: Tokyo)
县乡村 (ex: Shibuya-ku)
组织名 (ex: JDMail.)
部门 (ex: Development、空白可)
通用名 (ex: mx.mailer.cn)
Email (空白可)
密钥长度 (ex: 1024)
有效天数 (ex: 3650)
安装 立即安装
备注

「通用名」以外能记入虚构的信息，不过，有被客户看到内容的可能性。
全名「通用名」是您的 JDMMail 的域名(FQDN)，也可以用通配符(ex:*.domain.com)

指定。在这里指定的名字，为使使用 SSL/TLS 服务的全部用户通过 DNS 访问服务器，必须指定。如果运营多个 JDMail，所有的通用名必须不同。
如果一直私用，用本菜单制作了私钥和证书覆盖旧的也没有影响。
「备注」是说明文字，可以输入任意内容。(中文也可)。

本地用户的 Mailer 的设定注意

使用私用 CA 的 SSL/TLS 服务，请对各个的 JDMail 的本地用户进行以下设置。

需要用户的 PC 安装私用 CA 的证书(DER 文件)(安装方法见下面) 。
Mailer 的环境配置指定 POP3/SMTP 服务器的时候，与用证书的全名 FQDN 指定的必须相同。用 IP 地址指定的话会有错误。
能把 Mailer 的环境配置验证证书的选择设为开，就会更加提高安全性。

用户的 PC 安装私人 CA 的证书(DER 文件)

用户的 PC 安装私人 CA 的证书的话，如果 Mailer 进行了服务器证书的验证，就不会报错。安装请做到以下那样(Windows XP/Vista 的情况)。

私人 CA 证书(DER 文件)从这里下载。

根据浏览器的不同,下载 DER 文件会立刻打开证书的安装界面。按界面提示安装即可。但是，因为证明存储区的问题，使用 Mozilla Thunderbird（是 Firefox 的)就不能使用这个方法。

■ Mozilla Thunderbird

下载证书，放置在任意的地方。
启动 Mozilla Thunderbird ，[工具]-[选择]-打开[详细]菜单。
通过点击 [证书]按钮，打开[证书选项卡]，打开「证书管理器」。
[CA 证书] 打开标签 [导入] 选择下载的证书文件。
「被要求信赖新的认证(CA)。真的信赖这个 CA 吗？」全部选中 3 个复选框，按[OK]按钮。
至此安装完成。Thunderbird 和 Netscape(Firefox)的证书存储不同，请务必使用 Thunderbird 的菜单安装证书。

■ Outlook(2003/2007)、Outlook Express(XP)、Windows Mail(Vista)

下载证书，并把它存在任何地方。
打开菜单，点击证书按钮，单击安装证书，“启动证书导入向导”将出现。
[证书存储] [所有证书放入下列存储区] 选中[信任根证书] 。
安装过程中会有安全性警告提示，不要理会，继续执行安装直到完成。

■ 其它 Mailer

可能还有很多其他的邮件程序，请参考 Windows 证书存储。

这个运行环境的问题点

JDMail 不需要花费就可以创建 CA 中心，获取 CA 证书及服务器证书・私钥，在主机和客户端之间，很容易地配置使用 SSL/TLS 环境。另外还可以进行本地用户证书的验证。在本地用户和服务器之间维持高度的安全性和稳定性。但是，用户的本地 PC 必须单独安装 CA 证书，没有安装证书的用户从外部访问 SMTP 服务器，将会证书验证失败而无法连接。

私人 CA 使用很方便，不过，长时间一直没进行证书的失效处理等会降低安全性。请使用证书的失效处理 [已制作证书的管理]菜单。

Mailer 的设置注意事项

以下总结了安装私人 CA 并使用 SSL/TLS 服务主要的 Mailer 的设置。

(◎没问题、△根据选项设定、×不支持)

	(◎没问题、△根据选项设定、×不支持)	
Windows XP 环境	发信(SMTP)	收信(POP3)
Becky!(试用版)	◎	◎
EdMax(免费版)	◎	◎
Mozilla Thunderbird	◎	◎
nPOP	◎	TCP/995◎、TCP/110×
Outlook(Office2003)	◎	TCP/995◎、TCP/110×
Outlook Express 6	◎	TCP/995◎、TCP/110×
秀丸邮件	△(验证证书×)	△(验证证书×)
Windows Vista 环境	发信(SMTP)	收信(POP3)
Becky!(试用版)	◎	◎
EdMax(免费版)	×(非 SSL 可用)	×(非 SSL 可用)
Mozilla Thunderbird	◎	◎
nPOP	◎	◎
Outlook(Office2007)	◎	◎
Windows Mail	◎	TCP/995◎、TCP/110×
秀丸邮件	△(验证证书×)	△(验证证书×)

CA 证书的生成

CA 证书的生成

特别重视安全性的 SSL/TLS 服务不仅仅是服务器的认证(服务器证书的验证)，客户端的认证(客户证书的验证)也需要，不过，为了进行客户端认证需要 CA 证书。 JDMail 因为不使用 Windows 的证书，你必须自己制作。

«诊断» 现在的环境设置如下。

JDMail 设置为不进行客户端认证(默认动作)。
JDMail CA 证书已安装。
c:\MailRoot\bin\certs 文件夹内 CA 证书文件(.pem)未找到。
CA 证书未成批安装。

二种安装方法

JDMail 的 CA 证书可以用下面两种方法安装。

在 JDMail 的 MailRoot 文件夹内安装 certs.pem 文件。

如果将所有 CA 证书保存在 1 个文件里就是这个方法。如果使用私人 CA，证书的数量少，使用这个方法比较简单。使用这个方法， 需要将[环境配置]-[JDMail 环境配置] "CA 证书需要从 certs.pem 文件取得(SSLUseCertsFile)"设为"有效"。

如果从[私用证书颁发机构]菜单制作了私人 CA，CA 证书会自动生成并存放在 c:\MailRoot 。这个证书除了用来制作客户端证书以外，还可以复制到其它使用同样私人 CA 的 JDMail 使用。同时，certs.pem 可以保存多个证书，您可以记事本等工具添加到 certs.pem 文件。

JDMail 的 MailRoot\certs 文件夹内安装证书文件。

如果使用互联网真正的 SSL/TLS 服务，JDMail 需要很多的 CA 证书。展开 JDMail 的二进制安装包的话，那个 certs 文件夹内有许多以 pem 为扩展名的文件。这些全部是正式的认证机关的 CA 证明书。

包括私人 CA 的证书，JDMail 都将这些证书放在 MailRoot\certs 文件夹内安装使用。证书比较多的情况下，这样更容易维护。使用这种模式，需要将[环境配置]-[JDMail 环境配置] "CA 证书从 certs 文件夹取得(SSLUseCertsDir)"设为"有效"。

但是，在这种情况下，JDMail 为了实现高速证书检索，需要变更 CA 证书的文件名(对文件名作哈希 hash 运算)。

请检查 JDMail 的环境。

为了用 SSL/TLS 服务进行客户认证，CA 证书的安装之外还需要[环境配置]-[JDMail 环境配置]做以下的工作。

"远程主机要求 SSL 证书 (SSLWantCert)" 设为"有效"。根据这个不能出示客户端

证书的客户将不能使用 SSL/TLS 连接 JDMail。(非 SSL 连接没有影响)

如果验证客户证书的内容 "远程主机的 SSL 证书验证 (SSLWantVerify)" 设为 "有效"。不能出示正确的证书的客户将不能使用 SSL/TLS 连接 JDMail 。

如果证书保存在 MailRoot\certs 文件夹，"CA 证书在 certs 文件夹内取得 (SSLUseCertsDir)" 设为 "有效"。

如果您接受客户端证书由私人证书颁发机构颁发 "允许自签名的证书 (SSLAllowSelfSigned)" 设为 "有效" 。

制作客户端证书

制作客户端证书

为验证客户端，通过私用 CA 制作客户端证书。客户端验证，是在与服务器以 SSL/TLS 会话时，Mailer 等客户端软件出示客户端证书。服务器证书可以有效防止服务器被冒充，客户端证书防止客户被冒充。特别重视安全性服务的情况下推荐使用。

客户端认证的安装步骤如下。

[环境设置]-[JDMail 环境设置] SSL/TLS 设为开。这是 JDMail 的默认设置。
[环境设置]-[JDMail 环境设置] 相关的客户认证功能设为开。(后面详述)。

已经安装了正式客户端证书的用户，就可以使用服务了。
以下是使用私用 CA 安装客户端认证的追加设置。

用[建立私用 CA]菜单创建私用 CA(制作完毕)。
用本页给每个用户制作客户端证书(表单提交自动处理)。
向用户分发制作好的客户端证书。如果用户自己的 PC 没安装 CA 证书(DER 文件)，那个文件同时也分发(手工操作)。
JDMail 的用户自己的 PC 安装客户端证书(和私用 CA 证书)(手工操作)。

制作客户端证书

c:\MailRoot\sslconf 文件夹内自动创建客户端证书。
制作完成的证书可以从本页或 [制作完毕证书的管理]页下载。
证书采用 PKCS(Public Key Cryptography Standard)格式(是 P12 扩展名)。

▽如果使用过去的制作信息请选择 2009/09/17 17:31 制作 - shenzy2 2009/09/17 17:04 制作 - shenzy 2009/08/17 17:51 制作 - shenzy

通用名 (ex: Sindbad the Sailor)
Email

密钥长度　(ex: 1024)
有效天数　(ex: 1095)
备注

「通用名」「邮件地址」能登记虚构的内容，不过，「通用名」要和用户相关联。「备注」可以输入任意内容(可用中文)。

JDMail 的准备工作

JDMail 默认不进行客户认证。为了实现客户认证 [环境配置]-[JDMail 环境配置]需要进行以下的工作。

把[远程主机要求 SSL 证明书(SSLWantCert)]设为"有效"。这个必须。
如果[远程主机的 SSL 证明书(SSLWantVerify)]设为"有效"，这个更加安全。不过，远程主机不能出示正确的 CA 颁发的客户证书的情况下，连接被切断。
客户端验证 CA 证书文件 Mailroot\certs.pem 的情况下， [CA 证书 certs.pem 文件取得(SSLUseCertsFile)] 设为 "有效" 。
客户端验证 CA 证书文件在 Mailroot\certs 内的情况下， [CA 证书 certs 文件夹内取得(SSLUseCertsDir)] 设为 "有效"。但这种情况，需要使用[CA 证书生成]菜单将 CA 证书名预先转换为 hash 名。
如果接受自我签名的客户证书，需要 [自我签名的证书(SSLAllowSelfSigned)] 设为"有效"。
设定结束，需要重新启动 JDMail。

客户 PC 的准备工作

在 SSL/TLS 服务中如果进行客户认证，需要客户 PC 进行以下的工作。

管理者需要送交客户 PC 的所有者用本菜单生成了的客户证书。这个时候，安装客户证书的口令也必须同时提供。

客户证书保存在 MailRoot\sslconf 文件夹内的 xxxxxxxx-yyyyyy 这个名字的子文件夹。扩展名为.p12。那里有证书摘要文件 profile.tab ，可以确认证书的详细信息。
安装客户证书的口令保存在 profile.tab 里面的 mypass2 变量。从[制作完毕证书的管理]页也能确认。
PC 的所有者在自己的 PC 上安装客户证书。根据使用的邮件客户端软件不同，安装步骤也有不同(参照下面)。
没安装 CA 证书(DER 文件)的情况，也需要安装 CA 证书。请参考[私用 CA]内的说明。 CA 的 DER 文件如果没有变更，只需要安装一次。CA 证书(DER 文件)您可以从这里下载。

客户证书(P12 文件)的安装

客户端证书（p12 文件）在客户端 PC 上安装参考以下步骤（Windows XP / Vista）。

■ Mozilla Thunderbird

从管理者得到证书文件，放置在任意的地方。
启动 Mozilla Thunderbird ，[工具]-[选择]-打开[详细]菜单。
打开 [证书] 标签，点击 [查看证书] 按钮，打开「证书管理」。
[您的证书]，打开标签[导入]，导入已下载的证书文件。
证书第一次安装，"Software Security Device"的要求登记口令。这个口令可以任意。注意一定不能忘记。如果忘记了，会面临重新安装 Thunderbird 的困境。
其次要求证书的口令，这里用管理者告知的口令完成登记。

■ Outlook(2003/2007)、Outlook Express(XP)、Windows Mail(Vista)

从管理者得到证明书文件，放置在任意的地方。
选择证书，打开右键菜单,出现[PFX 的安装]菜单。选择"证书导入向导的开始"。
根据提示一步步操作。
如果提示输入"证书口令"，就输入管理员告知的口令。如果以后要导出备份，[可以导出这个密钥]选中。
[根据证书类型自动选择存储区]，然后证书导入完成。

■ 其它邮件客户端

很多其他的邮件程序使用 Windows 证书存储区（Outlook 中的位置）。因此，请参考 Outlook 的设置。

Mailer 设置注意事项

以下总结了客户 PC 安装在本页中生成的客户证书，JDMail 进行了客户认证的结果。

	（ ◎没有问题、△选项设定、×不支持 ）	
Windows XP 环境	发信(SMTP)	收信(POP3)
Becky!(试用版)	◎	◎
EdMax(免费版)	◎	◎
Mozilla Thunderbird	◎	◎
nPOP	×(非 SSL 可用)	×(非 SSL 可用)
Outlook(Office2003)	◎	×(连接被中断、非 SSL 可用)
Outlook Express 6	◎	×(连接被中断、非 SSL 可用)
秀丸邮件	△(证书验证×)	△(证书验证×)
Windows Vista 环境	发信(SMTP)	收信(POP3)
Becky!(试用版)	◎	◎

EdMax(免费版)	×(非 SSL 可用)	×(非 SSL 可用)
Mozilla Thunderbird	◎	◎
nPOP	×(非 SSL 可用)	×(非 SSL 可用)
Outlook(Office2007)	◎	◎
Windows 邮件	◎	◎

证书管理

管理在本站制作的证书。也可以做证书吊销处理。但是，这个版本不能管理吊销证书名单，吊销证书的客户如果想继续使用 SSL/TLS， 只能利用删除功能。

吊销" 如果选中，相应的证书立刻使之失效，那个证书存储也删除。
"删除" 如果选中，相应的证书存储删除，不过，预装的服务器证书不删除。要作废预装服务器证书，请手工删除 其它的 JDMail 的 MailRoot 目录下的 server.cert、server.key 。

为了避免由于疏忽大意造成事故，以公共目的被制作了的证书存储从本菜单不能删除。请到 sslconf 手工删除。