
Linux インターネットサーバーの SSL 証明書管理

～Kousec Server Certificate Manager の導入効果の検証～

第四回： 証明書の配備と監視

Copyright 2009 Kousec Software, Inc. All rights reserved.
All company names and product names are trademarks of their respective holders.

シリーズインデックス

http://www.kousec.com/prod_cm_ja.html

第一回： 検証構成と SSL 証明書の取得・配備計画

PDF: http://www.kousec.com/tj/tj_review_S1.pdf

第二回： サーバー上での SSL 設定作業

PDF: http://www.kousec.com/tj/tj_review_S2.pdf

第三回： 証明書仕様の定義と証明書の取得

PDF: http://www.kousec.com/tj/tj_review_S3.pdf

第四回： 証明書の配備と監視

PDF: http://www.kousec.com/tj/tj_review_S4.pdf

第五回： セキュリティと運用のベストプラクティス

PDF: http://www.kousec.com/tj/tj_review_S5.pdf

Table of Contents

証明書 の 配 備 と 監 視	5
CertMgr を使った証明書 の 配 備 方 法 に つ い て	5
証明書 www.example.com の 配 備 (Apache)	7
証明書 - 配 備 情 報 の 入 力	7
証明書 - 証 明 書 の イ ン ス ト ー ル を 依 頼	10
証明書 - 配 備 チェック	13
監 視 コ ン ト ロ ー ル に 移 動	16
証明書 smtp.example.com の 配 備 (Postfix)	17
証明書 pop.example.com の 配 備 (Dovecot)	23
証明書 ldap.example.com の 配 備 (slapd)	25
証明書 www2.example.com の 配 備 (Tomcat6, vsftpd)	27
今 回 の ま と め	31

証明書の配備と監視

今回は、CertMgr 上で証明書定義を作成し、そこから証明書取得プロセスを開始してプライベート CA から証明書を取得しました。そして証明書が有効期限内に入っていたので証明書配備プロセスを開始するところまで行いました。

今回は証明書リポジトリに格納された証明書を、配備プロセスを通じてインストールしていきます。

CertMgr を使った証明書の配備方法について

CertMgr における証明書の配備とは、以下の作業を指します。

- 証明書リポジトリに格納された証明書および対応する秘密鍵を、証明書定義で指定しているサーバーマシン上のサーバーソフトウェアにインストールする。
- インストール先サーバーに対して「配備チェック」を行って、正しくインストールされていることを確認する。
- サーバー証明書定期監視に組み込む。

サーバーソフトウェアへの証明書のインストール方法には3つあります。

1. 自動インストール

CertMgr マシンから直接対象のサーバーに証明書を転送し、そこで証明書インストーラーをリモート実行します。CertMgr 管理者は必要な情報を設定しておけば、あとはボタンを一回押せば証明書のインストールが完了します。

2. ワンクリックインストーラー

証明書と秘密鍵、そして証明書インストーラーをパッケージしたファイル（証明書インストールパッケージ）を生成し、サーバー管理者に送付します。サーバー管理者は、転送用パスワードを入力してパッケージを展開し、インストーラーを開始すると自動的に証明書がインストールされます。

3. 手動でインストール

証明書ファイルをサーバーソフトウェアにあったファイルフォーマットに変換したものをサーバー管理者に送付します。サーバー管理者は従来どおりの方法でインストールを行います。

どの方法にしる、CertMgr からサーバー管理者へ、証明書インストール依頼もしくは証明書インストール通知のEメールが送付されます。

詳細は配備プロセスにしたがって説明していきます。

なお、今回使用する example.com は実在するドメインではないので、Ubuntu Server マシンや CertMgr マシンの/etc/hosts に、各ホスト名(*.example.com)を登録してから証明書の配備を行いました。

証明書 www.example.com の配備 (Apache)

該当の証明書オブジェクトを開くと、配備プロセス実行中の画面になります。証明書オブジェクトをアクセスするには、配備プロセス一覧から行くのが早道でしょう。

配備プロセス

Cert ID	証明書定義	配備ステータス	プロセス開始	Time Limit	Project ID	Monitor Result	Vendor
1	www.example.com	配備可能	2009/09/30		Ubuntu Test	N/A	
2	ldap.example.com	配備可能	2009/10/01		Ubuntu Test	N/A	
3	smtp.example.com	配備可能	2009/10/01		Ubuntu Test	N/A	
4	pop.example.com	配備可能	2009/10/01		Ubuntu Test	N/A	
5	www2.example.com	配備可能	2009/10/01		Ubuntu Test	N/A	

では配備プロセスの各ステップを簡単に説明していきます。

証明書 - 配備情報の入力

基本情報

証明書の基本的な情報が表示されています。ニックネームはこの証明書のニックネームで、デフォルトでは証明書定義のニックネーム+証明書オブジェクトの内部番号が付与されています。変更可能です。

[証明書を表示]をクリックすると証明書ファイルの内部データを表示します。

基本情報	
ニックネーム	<input type="text" value="www.example.com_c1"/>
配備ステータス	配備可能
証明書定義	1
秘密鍵	1
証明書要求	1
コモンネーム	www.example.com
Valid Begin	2009/10/03 1:56:58
Valid End	2010/10/03 1:56:58
発行元	Kousec CertMgr Built-in Private CA
Certificate Serial #	21
詳細	証明書を表示

ニックネーム この証明書のニックネーム。いつでも変更することができます。
デフォルト値: 証明書定義のニックネーム+証明書のID番号。証明書をインポートした場合は、接尾語 'imp' が含まれます。
例: www.example.com_8,
www.example.com-prod-2009,
www.example.com_imp_7

証明書配備

ここでは証明書をインストールする先であるターゲットサーバーに関する情報と証明書インストールパッケージの送付方法を入力します。

本証明書は Apache サーバーにインストールします。証明書定義を作成する時点でサーバーソフトウェアタイプを Apache/Linux に設定していたのでその設定が引き継がれています。サーバーネームは、証明書インストール時に使用するターゲットサーバーの名前です。

Server Instance と Server Software Options はサーバーソフトウェアのタイプに合わせて設定します。Apache/Linux の場合は下記のように設定します。

- Server Software Type には **Apache/Linux** を設定 (設定済み)
- Server Instance には任意の文字列を入力。CertMgr 管理者やサーバー管理者がサーバーソフトウェアを認識しやすいような文字列がよいでしょう。
- Server Software Options: 以下を設定し、最後に**[Set]ボタンをクリック**。
 - SSL Conf Path: **/etc/apache2/sites-available/default-ssl**
SSL 証明書の設定パラメーターが格納されている Apache の設定ファイルの場所 (設定ファイルのパス名) を入力する

CertMgr のマニュアルによると Ubuntu9 の場合、設定ファイルのパス名として `/etc/apache2/sites-available/default-ssl` がデフォルト値になっています。今回のサーバーもそのデフォルトの設定ファイルを使っているため、ここで設定する必要はありませんが、ここでは明示的に設定しておきます。

証明書配備

ガイド

証明書インストールパッケージを作成するのに必要な下記の情報を入力します。

1. 証明書をインストールするターゲット サーバに関する情報
2. 証明書パッケージの配布方法

Server Software Type: Apache/Linux

Server Name for Certificate: server1

Server Instance (Optional): Apache2 server

Server Software Options: Openssl | JKS | **Apache** | Other

Apache(Linux)
SSL Conf Path: /etc/apache2/sites-available/default-ssl

Set Cancel See Help

Server Admin's Email

サーバー名
この証明書を配備するサーバー名。このサーバー名は主に証明書インストール時に使用します。この項目は必須です。

次に、証明書インストールパッケージのサーバー管理者への配布方法を指定します。ただし、この配布方法は証明書の自動インストールでは使用されません。自動インストールでは選択したサーバーソフトウェアタイプ毎に決められた方法でターゲットサーバーに証明書ファイルを送信します。Apache/Linux では SSH を使います。

本証明書ではサーバー管理者への送付方法は指定せず、その下にある Auto Install Options をチェックします。そこでターゲットサーバー上のユーザー名とパスワードを指定します。このユーザー名で証明書ファイルが転送されかつ証明書のインストールが行われます。通常はここに root ユーザーを指定しますが、root ユーザーが使えず sudo コマンドを使う Ubuntu Server では、sudo 権限を持つユーザー名を指定してください。

Auto Install Options Show Automatic Certificate Install Options

Username for Auto-install: myadmin

Password for Auto-install

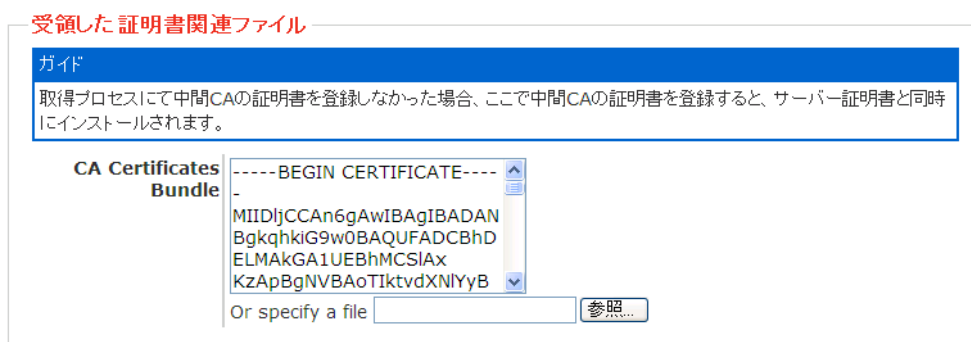
ターゲットサーバー上のユーザー名
ターゲットサーバーにアクセスするための OS ユーザー名。

受領した証明書関連ファイル

ここでは、受け取ったサーバー証明書と共にしよする中間 CA 証明書のファイルを追加・

変更できます。証明書の取得プロセスでサーバー証明書を登録する際に、必要な中間証明書を登録するのを忘れていたり間違っものを登録した場合に、ここで修正することができます。

今回は既にプライベート CA の証明書が登録されていますので変更しません。



入力し終わったらページ下部の[証明書パッケージを準備]ボタンをクリックします。証明書パッケージが作成されましたというメッセージと共に、次のステップに進みます。

証明書 - 証明書のインストールを依頼

このステップでは、証明書のインストールをサーバー管理者に依頼するメールを作成・送信します。

自動インストールのオプションが入力されていた場合は、自動インストールボタンが表示され自動インストールが可能になります。その場合、自動インストールの実行、次にインストール完了通知の送信という順になります。

ここで[Install Certificate now]ボタンをクリックすると自動インストールが始まります。自動インストールが成功すると自動インストールボタンがなくなり、メール本文の作成に移ります。失敗する場合は、ボタンの横にある [See Log]リンクをクリックし自動インストールの実行ログを確認します。

なお、Ubuntu Server 上の Apache へのインストールについては次の要件があり、満たされていないと失敗します。SSH で接続可能である、PHP の CLI 版と unzip がインストールされている。失敗した場合は要件を満たして再実行します。

インストール依頼メール

ガイド

Auto-Install(自動インストール)を行う場合は、Install Certificate Nowボタンを押しインストールを実行してください。自動インストールが失敗する場合は、サーバー管理者へインストールを依頼するEメール本文を作成します。

Install Request Text

下記サーバー用のSSLサーバー証明書を準備しました:

サーバー名: server1
コモンネーム: www.example.com
サーバーソフトウェア: Apache/Linux
サーバーインスタンス: /etc/apache2/sites-available/default-ssl

Mail To

Mail CC

Mail Title

Send as Attachment

Allow Web Access

Upload to FTP Server

Auto Install

自動インストール成功後、証明書関連ファイルと Apache の設定ファイルを確認しました。

```
root@ubuntu9-server2:/etc/apache2/ssl/certs# ls -l
-rw-r--r-- 1 root root 1328 2009-10-05 13:15 server-chain.crt
-rw-r--r-- 1 root root 1782 2009-10-05 13:15 www.example.com.crt
-rw-r--r-- 1 root root 1782 2009-10-05 11:57 www.example.com.crt.20091005-131521

root@ubuntu9-server2:/etc/apache2/ssl/private# ls -l
-rw----- 1 root root 1679 2009-10-05 13:15 www.example.com.key
-rw----- 1 root root 1679 2009-10-05 11:57 www.example.com.key.20091005-131521

root@ubuntu9-server2:/etc/apache2/sites-available# ls -l
-rw-r--r-- 1 root root 948 2009-04-02 01:01 default
-rw-r--r-- 1 root root 7440 2009-10-05 13:15 default-ssl
-rw-r--r-- 1 root root 7376 2009-10-05 13:15 default-ssl.20091005-131527
```

各ファイルがバックアップを取られて変更されています。今回 Apache の設定ファイル (default-ssl)も更新されたのは、SSLCertificateChainFile パラメータが追加されたからです。最初は自己署名証明書を使用していたのでこのパラメータは使用していませんでした。

また”See Log”ボタンをクリックし実行ログを確認すると、SUCCESS と表示されており、今回のインストールを取り消す UNDO スクリプトファイルが生成されています。このファ

イルは/tmp 以外のどこかに保存しておいたほうがよいでしょう。

```
SUCCESS: Done installing the certificate.
```

Run the following script to undo the changes done:

```
sh -x /tmp/undo-20091005-131521.sh
```

```
* Starting web server apache2
```

```
...done.
```

サーバー管理者へのメールの作成

自動インストールが成功すると、画面に表示されているメールのドラフト文が、インストール依頼からインストール通知に変わっています。

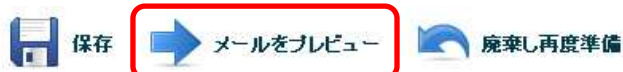
インストール依頼メール

ガイド
証明書のサーバーへのインストールについて通知するEメール本文を作成します。

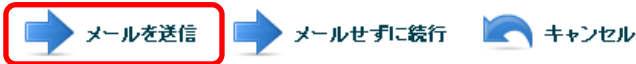
Install Request Text	新しいSSLサーバー証明書を下記サーバーにインストールしました: サーバー名: server1 コモンネーム: www.example.com サーバーソフトウェア: Apache/Linux サーバーインスタンス: /etc/apache2/sites-available/default-ssl
Mail To	<input type="text"/>
Mail CC	<input type="text"/>
Mail Title	[www.example.com] SSLサーバー証明書のインストール通知

Mail To にはサーバー管理者のメールアドレスが入っています。Mail CC には CertMgr 管理者のメールアドレスが入っています。必要に応じて CC に他のメールアドレスを追加します。

そして[メールをプレビュー]ボタンをクリックしメール送信の確認画面に移ります。



確認画面を終えたら[メールを送信]をクリックします。また、メールを送信したくない場合、たとえばメール本文と証明書インストールパッケージを USB メモリーなどで手渡す場合は [メールせずに続行]をクリックします。



証明書 - 配備チェック

最後のステップは、証明書が正しくインストールされているかの配備チェックを行います。

ここではチェックのためにアクセスするサーバー名とサーバープロトコル、ポート番号を入力します。チェック用のサーバー名(**Server Name to Check**)は、インストール用のサーバー名と別に設定できます。デフォルトで証明書のCOMMONNAMEが入っています。チェックするポート番号(**Server Port to Check**)は省略すると 443(HTTPS)が仮定されますがここでは明示的に指定します。

- Server Name to Check: **www.example.com**
- Server Protocol : **HTTPS/SSL-Wrapped** を選択
- Server Port to Check : **443** を入力



証明書 - 配備チェック

配備チェック

ガイド
下記を入力し、証明書がサーバーに正しく配備されたかどうかを確認します。もしCertMgrがターゲットサーバーに直接アクセスできない場合は、手動で配備チェックを行った後、[手動で配備を確認しました]をクリックして進みます。定期的な直接アクセスできない場合は、さらに定期監視を無効化してください。

Server Software Type	Apache/Linux
Server Name for Certificate	server1
Server Admin's Email	[Redacted]
Disable Periodic Monitoring	<input type="checkbox"/>
Server Name to Check	www.example.com
Server Protocol	HTTPS/SSL-Wrapped
Server Port to Check	443

チェック・監視するサーバーの本スト名
証明書の有効性と正しく配備されているかをチェックする際使用します。デフォルト値: 指定しない場合、証明書のCOMMONNAMEが使用されます。

入力を終えたら、[配備チェック]ボタンをクリックし、配備チェックを実行します。



証明書・配備チェックの結果

CertMgr マシンからサーバーにアクセスし配備チェックの結果が表示されます。以下はチェックの最終ステップで失敗したときの画面です。

証明書 - 配備チェックの結果

Check Result

ニックネーム	www.example.com_c1
配備ステータス	インストール要求中
サーバー名	www.example.com
サーバーのポート番号	443
証明書	証明書を表示

エラー

証明書は正しく配備されていません。

ステップ	結果	備考
ホスト名解決	✓	Hostname resolved to 1 192.168.239.91 443
ホストへ接続	✓	Connected to host
証明書一致	✓	Certificate is same as the one in CertMgr
証明書検証	✗	self signed certificate in certificate chain

再度、配備チェック実行 1ステップ戻る チェックの設定変更 チェックせずに続行

配備チェックでは以下の5つのチェックを順に行っていきます。

ステップ	チェックの内容
ホスト名解決	Server Name to Check で指定したホスト名を IP アドレスに変換できるか。
ホストへ接続	指定したポートでサーバーにネットワーク接続できるか。
SSL で接続	SSL 接続が確立できるか。
証明書一致	サーバー上で見つかった証明書が CertMgr の証明書リポジトリ内の現行証明書と一致するか。
証明書検証	サーバー証明書チェーンの検証を行う。

最後の証明書検証で、さまざまな証明書チェーン全体に関するチェックを行います。全てのチェックが通ったら証明書の配備が確認できたことになります。

今回のテストで発生したエラーと対処について簡単に列挙しておきます。エラーメッセージは OpenSSL の証明書検証からの出力ですので、その他のエラーの場合、Ubuntu Server 上で “man verify” を打てば各エラーの説明が表示されます。

	エラーメッセージ	説明	考えられる原因と対処
1	self signed certificate in certificate chain	証明書チェーンはルートまで到達したが、そのルート CA は信頼されていない。	配備チェックツールが使う信頼する CA ストアに、ルート CA が登録されていません。
2	unable to get local issuer certificate	証明書チェーンがルートまで到達できなかった。	中間 CA の証明書をサーバーが送って来てない。SSLCertificateChainFile が正しく設定されていることを確認する。
3	certificate has expired	有効期限が切れている	文字通りだが、CertMgr で管理していれば通常はここまで行かない。

1 の「配備チェックツールが使う信頼 CA ストア」の更新方法については CertMgr のマニュアルを参照してください。

問題を修正した後、[再度配備チェック実行]ボタンをクリックします。配備が確認できたならば、下記のような画面が表示されます。[完了]ボタンをクリックし配備プロセスを完了します。

情報

証明書は正しく配備されています。

ステップ	結果	備考
ホスト名解決	✓	Hostname www.example.com resolved to 1 192.168.239.91 443
ホストへ接続	✓	Connected to host
SSLで接続	✓	Established SSL connection (Over-SSL)
証明書一致	✓	Certificate is same as the one in CertMgr
証明書検証	✓	Certificate verified



CertMgr マシンとターゲットサーバーが直接ネットワークで接続されていない場合などでは、CertMgr から配備チェックが行えません。その場合はターゲットサーバーにアクセスできる環境から手動で配備チェックを実施します。そして前画面の[チェックせずに続行]

ボタンをクリックして、配備プロセスを完了します。

監視コントロールに移動

配備プロセスが完了した証明書は、デフォルトで証明書監視対象になっています。配備プロセス完了画面から [監視コントロール] をクリックして監視画面に移動します。

監視コントロール

最新の証明書監視結果

Notice

There is no result for deploy check

Cert	配備ステータス	Time Limit	証明書定義	Check Result
------	---------	------------	-------	--------------

監視実行履歴

Exec At	OK count	NG count	Actions
2009/10/05 1:30:10	0	0	
2009/10/04 1:30:38	0	0	
2009/10/03 2:00:17	0	0	

Run Deploy Checks Immediately

監視スケジュール

Run Checks At 1 : 23

Next scheduled 2009/10/06 1:23:20

Mode Daily

Change Monitor Schedule

証明書監視とは 1 日 1 回、配備済みもしくは証明書インストール作業中の全証明書に対して、配備チェックを行い異常があれば CertMgr 管理者と該当サーバーの管理者に E メールを送る機能です。

画面の「最新の証明書監視結果」には最後に行われた配備チェックの結果一覧が表示されています。次の「監視実行履歴」には、この数日間で行われた監視実行結果のサマリーが表示されています。OK count は配備チェックが成功したサーバーの数、NG count は失敗したサーバーの数です。その下に [Run Deploy Checks Immediately] ボタンを押すと、監視実行のスケジュールされた時間と関わらず、配備チェックが即時に実行されます。

「監視スケジュール」では、監視実行の時間を変更できます。また、監視の頻度を一日単位から 1 時間単位に変更することができます。

[Run Deploy Checks Immediately]ボタンをクリックし、監視の即時実行を行うと下記のように配備チェックの結果が表示されます。

最新の証明書監視結果

情報				
Last deployment check was 2009/10/06 14:15:31				
Cert	配備ステータス	Time Limit	証明書定義	Check Result
1	確認済		www.example.com	OK

Check Result 列の[OK]や[NG]をクリックすると、配備チェック内での各ステップでの結果が表示されます。

ここまでが、1枚の証明書を配備する流れです。同様に、他の証明書も配備していきます。

証明書 smtp.example.com の配備 (Postfix)

配備プロセス一覧から証明書 smtp.example.com を選び開きます。

ステップ 証明書 - 配備情報の入力

Server Instance と Server Software Options はサーバーソフトウェアのタイプに合わせて設定します。Postfix の場合は下記のように設定します

- Server Software Type には **Openssl(generic)**を設定
- Server Instance には任意の文字列を入力。CertMgr 管理者やサーバー管理者がサーバーソフトウェアを認識しやすいような文字列がよいでしょう。
- Server Software Options: 以下を設定し、最後に[Set]ボタンをクリック。
 - Software Type: **Postfix**
 - Conf File Path: **/etc/postfix/main.cf**
 - Unencrypted private key: **チェックしない**
 - Do not automatically stop and start service: **チェックしない**

Server Software Type	Openssl (generic) ▾
Server Name for Certificate	server1
Server Instance (Optional)	Postfix
Server Software Options	<div><p>Openssl(generic) JKS(generic) Other</p><p>Openssl</p><p>Software Type ▾ Postfix</p><p>Conf File Path /etc/postfix/main.cf</p><p>Unencrypted private key <input type="checkbox"/></p><p>Do not automatically stop and start service <input type="checkbox"/></p><p>Set Cancel See Help</p></div>

Postfix も Apache と同様に自動インストールがサポートされていますので、自動インストール用にユーザー名とパスワードを設定しておけばボタンを押すだけで証明書がインストールされます。ただ今回は評価のために、ワンクリックインストーラーを使用してみます。ワンクリックインストーラー場合、サーバー管理者に証明書インストールパッケージを送付する必要があります。証明書インストールパッケージの送信方法としては、Eメールに添付を選択します。

<input checked="" type="checkbox"/>	Send as Attachment
<input type="checkbox"/>	Allow Web Access
<input type="checkbox"/>	Upload to FTP Server
<input type="checkbox"/>	Auto Install Options Show Automatic Certificate Install Options

[証明書パッケージを準備]ボタンをクリックして進みます。

ステップ 証明書 - 証明書のインストールを依頼

インストール依頼メールにおいて、必要に応じてメール本文を修正・追記し、メール送付先も確認します。また全ステップで設定した「Send as Attachement」がチェックされていることを確認します。

[メールをプレビュー]ボタンをクリックし、確認画面に進みます。



Attachments の欄に、cert.zip とあるのが証明書インストールパッケージであり、zip でパスワードがかけられています。[メールを送信]ボタンをクリックして送信します。

送信が終わるとサーバー管理者のメールボックスに、添付ファイルの付いたメールが到着します。注意しなければいけない点があります。

- 暗号化 zip ファイルなので、ウイルスフィルタリングが入ったメール環境によっては警告付メールになったり破棄される可能性もある。
- zip のパスワードも同一メール内に記載されているので暗号化する意味が薄い。

証明書インストールパッケージの配布方法の安全性については次回で検討します。

では、サーバー管理者に届いた cert.zip ファイルを Ubuntu Server にアップロードし、証明書インストーラーを実行します。メールを受け取った PC から server1 の/tmp に SCP などからコピーしてから、SSH で server1 にログインします。/tmp 配下で cert.zip を unzip し、その中にあるインストールスクリプト(inst_opssl.sh)を実行します。

```
>sudo bash
#cd /tmp
#unzip cert.zip
[ zip パスワードを入力 ]
#bash /tmp/cert/inst_opssl.sh
--- One-click installer 0.1.7-pre5 ---
Linux Distribution Version: UB9
Server Name: server1
Server Type: 46
SSL Config File specified: /etc/postfix/main.cf
SSL Config File found: /etc/postfix/main.cf
Service Name Found: postfix
SSLCertificateFile: /etc/postfix/ssl/certs/smtp.example.com.crt
SSLCertificateKeyFile: /etc/postfix/ssl/private/smtp.example.com.key
SSLCertificateChainFile:
--- Existing Certificate ---
subject= /CN=ubuntu9-server2.localdomain
issuer= /CN=ubuntu9-server2.localdomain
notBefore=Sep 24 08:53:53 2009 GMT
notAfter=Sep 22 08:53:53 2019 GMT
-----
--- New Certificate ---
subject= /C=JP/O=Example, Inc./CN=smtp.example.com
issuer= /C=JP/O=Kousec CertMgr Built-in Private CA/CN=Kousec CertMgr
Auto-Generated CA 20090731201227/ST=Tokyo
notBefore=Oct 2 17:23:35 2009 GMT
notAfter=Oct 2 17:23:35 2010 GMT
-----
* Stopping Postfix Mail Transport Agent postfix [ OK ]
Decrypting private key to /tmp/cert/secret.key-dec
writing RSA key
SUCCESS: Done installing the certificate.

Run the following script to undo the changes done:
sh -x /tmp/undo-20091007-191646.sh
* Starting Postfix Mail Transport Agent postfix [ OK ]
```

#

最後に「SUCCESS: Done installing the certificate」というメッセージが表示され、証明書のインストールが成功しました。またこのインストールの UNDO スクリプトも生成されています。

また Apache へのインストール時と同様に/etc/postfix/ssl に新しい証明書がインストールされていることも確認できます。

ステップ 証明書 - 配備チェック

CertMgr の画面は配備チェックに移っています。

ここでは、下記項目を設定します。

- Server Protocol : **SMTP TLS** を選択
- Server Port to Check : **587** を入力

配備チェック

ガイド	
下記を入力し、証明書がサーバーに正しく配備されたかどうかを確認します。もしCertMgrがターゲットサーバーに直接アクセスできない場合は、手動で配備チェックを行った後、[手動で配備を確認しました]をクリックして進みます。定期的に直接アクセスできない場合は、さらに定期監視を無効化してください。	
Server Software Type	Openssl (generic)
Server Name for Certificate	server1
Server Admin's Email	████████████████████
Disable Periodic Monitoring	<input type="checkbox"/>
Server Name to Check	smtp.example.com
Server Protocol	SMTP TLS
Server Port to Check	587

そして[配備チェック]ボタンをクリックすると、チェックの結果が表示されます。

Check Result

ニックネーム	smtp.example.com_c1
配備ステータス	確認済
サーバー名	smtp.example.com
サーバーのポート番号	587
証明書	証明書を表示

情報

証明書は正しく配備されています。

ステップ	結果	備考
ホスト名解決	✓	Hostname smtp.example.com resolved to 1 192.168.239.91 587
ホストへ接続	✓	Connected to host
SSLで接続	✓	Established SSL connection (STARTTLS)
証明書一致	✓	Certificate is same as the one in CertMgr
証明書検証	✓	Certificate verified

最後に[完了]を押して配備プロセスを完了します。本証明書も定期監視に組み込まれています。

証明書 pop.example.com の配備 (Dovecot)

Dovecot にインストールする証明書も Postfix とほぼ同様です。Postfix との差分のみ記載します。ただし自動インストールを行います。

ステップ 証明書 - 配備情報の入力

Dovecot の場合は下記のように設定します

- Server Software Type には **Openssl(generic)**を設定
- Server Instance には任意の文字列を入力。CertMgr 管理者やサーバー管理者がサーバーソフトウェアを認識しやすいような文字列がよいでしょう。
- Server Software Options: 以下を設定し、最後に[Set]ボタンをクリック。
 - Software Type: **Dovecot**
 - Conf File Path: **/etc/dovecot/dovecot-postfix.conf**
 - Unencrypted private key: **チェックしない**
 - Do not automatically stop and start service: **チェックしない**

また自動インストールを行うため、Auto Install Options をチェックしターゲットサーバー上のユーザー名とパスワードを指定します。Apache のケースと同じく、Unbuntu Server では、sudo 権限を持つユーザー名を指定してください。

Auto Install Options	<input checked="" type="checkbox"/> Show Automatic Certificate Install Options
Username for Auto-install	<input type="text" value="myadmin"/>
Password for Auto-install	<input type="password"/>

ターゲットサーバー上のユーザー名
ターゲットサーバーにアクセスするためのOSユーザー名。

ステップ 証明書 - 証明書のインストールを依頼

[Install Certificate now]ボタンをクリックし自動インストールを行います。失敗する場合は、ボタンの横にある [See Log]リンクをクリックし自動インストールの実行ログを確認します。

ステップ 証明書 - 配備チェック

ここで 1 点注意することがあります。Dovecot では POP3 と IMAP の 2 つのサービスを提

供しています。かつそれぞれのサービスに Over-SSL と STARTTLS という 2 つの異なるポートを割り当てており、合計 4 つのポートを使用しています。

少なくとも POP3 のポート 1 つと IMAP のポート 1 つはチェックしたいのですが、CertMgr の配備チェックでは一つのポートしかチェックできません（対応予定とのこと）。

今回は、代表して POP3 over SSL であるポート 995 をチェックします。

- Server Protocol : **HTTPS/SSL-Wrapped** を選択
- Server Port to Check : **995** を入力

あとは、Postfix と同様に配備チェックを行い、配備プロセスを完了します。

証明書 ldap.example.com の配備 (slapd)

OpenLDAP(slapd)も Postfix や Dovecot と同様に、OpenSSL ベースのサーバーソフトウェアですが¹、現バージョンの CertMgr では専用のインストール機能はありません。今回は、サーバーソフトウェアタイプとして OpenSSL(generic)を選択し、さらにサブタイプとしては Not Listed を指定し手動インストールを行います。

ステップ 証明書・配備情報の入力

OpenSSL ベースのソフトウェアへの手動インストールの場合は下記のように設定します

- Server Software Type には **Openssl(generic)**を設定
- Server Instance には任意の文字列を入力。CertMgr 管理者やサーバー管理者がサーバーソフトウェアを認識しやすいような文字列がよいでしょう。
- Server Software Options: 以下を設定し、最後に**[Set]ボタンをクリック**。
 - Software Type: **Not Listed**
 - Unencrypted private key: **チェックする**

Unencrypted private key(秘密鍵を暗号化しない)にチェックを入れると、証明書インストールパッケージ(cert.zip)には暗号化されていない秘密鍵が格納されます。そうするとサーバー管理者は cert.zip を展開後、cp コマンドでファイルをコピーするだけで済みます。

ステップ 証明書・証明書のインストールを依頼

CertMgr からサーバー管理者が証明書インストールパッケージを受け取り、Ubuntu Server の/tmp にアップロードし、unzip します。そして OpenLDAP サービスを停止し、証明書・秘密鍵ファイルをコピーします。

cert.zip を展開。インストーラーも起動してみる。

```
#unzip cert.zip
#cd cert
#bash ./inst_opssl.sh [ インストーラーがあるので起動してみる ]
--- One-click installer 0.1.7-pre5 ---
NOTICE: you cannot use this certificate installer to install the certificate
```

¹ Ubuntu Server の OpenLDAP は正確には GnuTLS を使ってビルドされています。ただし証明書のファイル形式など多くの点で OpenSSL に合わせています。

Follow the manual instructions included in the install request email.

[手動でインストールせよとのメッセージ]

手動でインストールする。

```
#cd /tmp/cert
#ldapsearch -xLLL -b cn=config -D cn=admin,cn=config -W 'objectClass=olcGlobal'
[ olcTLSCertificateFile など 証明書関連ファイルのパスを確認 ]
#/etc/init.d/slaped stop [ slaped を停止 ]
Stopping OpenLDAP: slaped.
# cp cert_chain.crt /etc/ldap/ssl/certs/ldap.example.com.crt
# cp cacerts.pem /etc/ldap/ssl/certs/trusted-ca.crt
# cp secret.key /etc/ldap/ssl/private/ldap.example.com.key
#/etc/init.d/slaped start [ slaped を開始 ]
Starting OpenLDAP: slaped.
```

ステップ 証明書 - 配備チェック

配備チェックも LDAP/STARTTLS はサポートしていませんが、LDAP over SSL のポートも有効なので、そちらを使ってチェックします。

- Server Protocol : **HTTPS/SSL-Wrapped** を選択
- Server Port to Check : 636 を入力

あとは、他の証明書と同様に配備チェックを行い、配備プロセスを完了します。

証明書 www2.example.com の配備 (Tomcat6, vsftpd)

前回「証明書仕様の定義と証明書の取得」で書いたように、現バージョンの CertMgr では一つの証明書を複数のサーバーソフトウェアに配備することはできません。したがって、ここでは配備プロセスを途中まで Tomcat6 で進めていき、配備チェックが終わったら配備プロセスを巻き戻し vsftpd 用に変更して、配備プロセスを完了するようにします。

ステップ 証明書 - 配備情報の入力

Java ベースのソフトウェアへの手動インストールの場合は下記のように設定します

- Server Software Type には **JKS(generic)**を設定
- Server Instance には任意の文字列を入力。CertMgr 管理者やサーバー管理者がサーバーソフトウェアを認識しやすいような文字列がよいでしょう。
- Server Software Options: 以下を設定し、最後に[Set]ボタンをクリック。
 - JKS File Path: **/etc/tomcat6/ssl/private/www2.example.com.jks**
 - Alias in Keystore: **tomcat**
 - Keystore Password: **changeit**

なお、JKS(generic)の場合、サーバーソフトウェアの停止・開始は手動で行う必要があります。

ステップ 証明書 - 証明書のインストールを依頼

CertMgr からサーバー管理者が証明書インストールパッケージを受け取り、Ubuntu Server の/tmp にアップロードし、unzip します。以下のコマンドでインストーラーを起動します。なお、当サーバーに Java (JRE 1.4 以上)がインストールされている必要があります。

```
#/etc/init.d/tomcat6 stop [ Tomcat6 を停止 ]
#unzip cert.zip
#bash ./cert/jks_inst.sh
Kousec Certmgr Cert Installer for JKS 0.1.5
successfully read parameter file
Keystore file [/etc/tomcat6/ssl/private/www2.example.com.jks] has been backed up to
[/etc/tomcat6/ssl/private/www2.example.com.jks.20091008184754].
WARNING: hostname of this computer (ubuntu9-server2) does not match the server name
```

```
specified by CertMgr administrator (server1)
Continue to install this certificate?(y/n)y
Certificate chain length: 2
Subject: CN=www2.example.com
Validity Period: 2009/10/08 18:44:38 to 2010/10/08 18:44:38
Intermediate CA Certificates
Subject: CN=Kousec CertMgr Auto-Generated CA 20091008125945
The alias [tomcat] exists. It will be overwritten.
SUCCESS: The new key and certificate chain have been inserted to the keystore.
Alias and key password are set as follows:
    Alias:tomcat Password:changeit
You can change them using one of the commands below:
keytool -keypasswd -alias tomcat -keystore "/etc/tomcat6/ssl/private/www2.example.com.jks"
keytool -changealias -alias tomcat -keystore "/etc/tomcat6/ssl/private/www2.example.com.jks"
Enter 'y' or 'n' to end this program(y/n)y
# /etc/init.d/tomcat6 start [ Tomcat6 を開始 ]
```

SUCCESS: The new key and ... と表示され証明書がインストールされたことが分かります。また keystore パスワードや alias を変更する方法も表示されています。

ステップ 証明書 - 配備チェック

Tomcat6 のプロトコルは HTTPS ですので下記を入力し配備チェックを行います。

- Server Protocol : **HTTPS/SSL-Wrapped** を選択
- Server Port to Check : **8443** を入力

[配備チェック]をクリックし、配備チェックが成功することを確認します。

配備プロセスを巻き戻す

Tomcat6 の確認が取れたら、そこで配備プロセスを完了せずに、サーバーソフトウェアタイプの選択ステップまで戻ります。

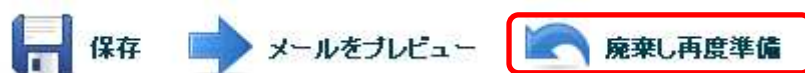
「証明書 - 配備チェックの結果」画面で、[チェックの設定変更]をクリック



「証明書 - 配備チェック」画面で、[1 ステップ戻る]をクリック



「証明書 - 証明書のインストールを依頼」画面で、「廃棄し再度準備」をクリック



すると「証明書 - 配備情報の入力」画面まで戻りました。

準備した証明書インストールパッケージを廃棄しました。



証明書 - 配備情報の入力

ここから、再度配備プロセスを進めていきます。

ステップ 証明書 - 配備情報の入力 (2)

vsftpd ヘインストールするため以下の設定します

- Server Software Type には **OpenSSL(generic)**を設定
- Server Instance には任意の文字列を入力。CertMgr 管理者やサーバー管理者がサーバーソフトウェアを認識しやすいような文字列がよいでしょう。
- Server Software Options: 以下を設定し、最後に[Set]ボタンをクリック。
 - Software Type: **vsftpd**
 - Conf File Path: **/etc/vsftpd.conf**
 - Unencrypted private key: **チェックしない**
 - Do not automatically stop and start service: **チェックしない**
- Auto-Install Options: sudo 権限を持つユーザー名とそのパスワードを入力

ステップ 証明書 - 証明書のインストールを依頼 (2)

Apache や Dovecot と同様に、Install Certificate now ボタンを押して自動インストールをおこないます。

ステップ 証明書 - 配備チェック

下記を入力し配備チェックを行います。

- Server Protocol : **FTP TLS** を選択
- Server Port to Check : **21** を入力

[配備チェック]をクリックし、配備チェックを実行します。

配備チェックが成功したら、チェック結果画面にて[完了]ボタンをクリックし配備プロセスを完了します。

これで証明書 `www2.example.com` の配備は完了しました。注意点があります。

- Tomcat6 は証明書監視の対象になっていない。
- 証明書 `www2.example.com` を更新する際、今回と同様の手順を踏む必要がある。

今回のまとめ

前回取得した証明書 5 枚を、今回 Ubuntu Server の各サーバーにインストールしました。

証明書	インストール方法	対象サーバーソフトウェア
www.example.com	自動インストール	Apache
smtp.example.com	ワンクリックインストール	Postfix
pop.example.com	自動インストール	Dovecot
ldap.example.com	手動インストール	OpenLDAP
www2.example.com	ワンクリックインストール	Tomcat6 =>
	自動インストール	vsftpd

証明書の自動インストール(Apache, Dovecot, vsftpd)が最も容易で運用者に負担がかからない方法でした。Postfix も自動インストールが可能です。その他のサーバーソフトウェアでも自動インストールがサポートされた時点でそちらに切り替えるのがよいと考えます。

www2 証明書については、一旦 Tomcat6 にインストールしてから配備プロセスを巻き戻し vsftpd にインストールしなおすという手順が必要でした。

証明書監視については、デフォルトでは 1 日一回、各サーバーに配備チェックを行っています。その結果については「監視コントロール画面」で確認できます。

証明書インストールパッケージをサーバー管理者に送付するのに、今回は E メールに添付する方法を取りました。他の方法として、FTP サーバーにアップロードすることや Kousec Server Certificate Manager のウェブサーバーから直接ダウンロードしてもらうことも可能です。次回にこれらの方法も実際にテストも行い、どの方法が今回の環境に適しているか検討します。

次回（最終回）は、証明書パッケージの他の送付方法（FTP 等）の検証などを行います。またセキュリティを考慮した運用のベストプラクティスについて考えていきます。