

---

# 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～

第五回：セキュリティと運用のベストプラクティス

---

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](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](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](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](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](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](http://www.kousec.com/tj/tj_review_S5.pdf)

---

## Table of Contents

CertMgr からのアラートメール .....	5
配備に関するアラート .....	5
テスト：インストールした証明書を古い証明書で上書きする .....	5
FTP サーバーを経由した証明書パッケージの送信 .....	9
CertMgr 運用のベストプラクティス .....	10
CertMgr マシンへのアクセス .....	10
CertMgr の運用で検討すべきこと .....	10
SSL 証明書の運用におけるセキュリティの考察 .....	13

---

今回は SSL 証明書の配備と監視の設定を行いました。今回は監視結果によって送出されるアラートメールを確認、また前回行わなかった FTP を使った証明書の送付方法を検証します。最後に、CertMgr の運用上のセキュリティについて考えます。

## CertMgr からのアラートメール

CertMgr は Web コンソール以外に、E メールを使ってアラート（警報）をあげることができます。

証明書の配備に関するアラートと証明書の取得に関するアラートに大別できます。前者は、サーバー上に正しく証明書がインストールされていない場合などに上げられます。後者は例えば、証明書の有効期限が 2 ヶ月を切ったのにまだ更新取得の手続きを始めていない場合などに上げられます。

### 配備に関するアラート

証明書の配備に関して、CertMgr は下記の 2 つのケースで証明書アラートをメールで通知してきます。

1. 証明書のステータスは「配備確認済み」（すなわち配備プロセスは完了している）であるのに、1 日 1 回の配備チェックが失敗した。
2. 証明書のステータスは「配備要求中」（すなわち配備プロセスは進行中）で、1 日 1 回の配備チェックが成功した。

1 の状況は、一度正しく証明書がインストールされたのに、何らかの原因で証明書がおかしくなったというものです。

2 の状況は、配備プロセスにおいてサーバー管理者に証明書のインストール依頼を行い、その結果サーバー管理者が証明書のインストールを正しく完了したということです。

管理下の SSL 証明書のうちどれか一つが 1 か 2 の状況になったと検知されると、CertMgr 管理者宛にアラートメールが送信されます。また 1 の場合は、該当サーバーのサーバー管理者にもアラートメールが送信します。

**テスト：インストールした証明書を古い証明書で上書きする**

---

では、実際にどのようなアラートメールが送信されるのか、テストをしてみます。

Apache の証明書 `www.example.com` を最初に自動生成された自己署名証明書で上書きします。誤って古い証明書に戻したことを想定しています。

```
# cp /etc/ssl/certs/ssl-cert-snakeoil.pem /etc/apache2/ssl/certs/www.example.com.crt
# cp /etc/ssl/private/ssl-cert-snakeoil.key /etc/apache2/ssl/private/www.example.com.key
# /etc/init.d/apache2 restart
```

またもう一つ、`vsftpd` は単にサービスを落としておきます。

これで、証明書の定期監視が動くのを待ちます。定期監視の間隔はデフォルト 24 時間ですが、ここではテストのため 1 時間に変更します。しばらくすると下記メールを受信しました。

#### CertMgr 管理者が受信するアラートメール

まだ日本語化はされていませんが以下のような、誤った証明書を使っているサーバーや稼動していないサーバーの一覧と、CertMgr 管理者として取るべきアクションが記載されたメールが送信されてきます。

```
SSL Server Certificates Status Monitor
```

```
(This is sent from Kousec Server Certificate Manager)
```

```
As of 2009/10/16 12:00:41 (UTC: 2009-10-16 03:00:41+00:00)
```

```
Certificates and servers that need your immediate attention
```

```
-----
These servers previously had correct certificates installed, but at the time
of our daily certificate checking, they are not correctly installed.
```

```
[下記に、配備確認済みであるが、配備チェックが失敗した証明書が列挙されている]
```

```
Cert-CommonName  Server Name  Status      Check  Server-Admin
www2.example.com  server1  Deploy-Confirmed  NG  svr-admin@xxxx.com
www.example.com   server1  Deploy-Confirmed  NG  svr-admin@xxxx.com
```

```
What you need to do: Open the certificate screen for each certificate on Kousec Server
```

Certificate Manager and do a deploy check again to determine if the failure is persistent.  
If the deploy check still fails, follow the “Re-install Certificate” section on the same page.

[CertMgr 上の各証明書へのリンクが列挙されている]

Cert-CommonName    Link to Kousec CertMgr

**www2.example.com**    <http://PC2:23456/cake/cm/certificates/edit/1>

**www.example.com**    <http://PC2:23456/cake/cm/certificates/edit/2>

Certificates and servers that need your attention

-----

You are requesting server administrators of these servers to  
install the certificates, and at the time of our daily certificate checking,  
they have been found to have the certificate installed.

[下記に、インストール依頼中の証明書のうち、配備チェックが成功した証明書が列挙されている]

[今回は対象の証明書はない]

[以下省略]

メール内にある URL をクリックし Kousec CertMgr にログインした後、証明書オブジェクトの画面が開きます。「証明書の再インストール」セクション上で、自動インストールの再実行やインストール依頼メールの再送信が行なえます。

**証明書の再インストール**

**Guide**  
証明書の再インストールが必要な場合、ここで自動インストールを再実行するかインストール依頼メールを再送してください。

<b>Auto Install</b>	<input type="button" value="Install certificate now"/>	<a href="#">See log</a>
<b>Last Successful Auto-Install</b>	2009/10/16 11:30:12	
<b>Install Request Email</b>	<input type="button" value="Re-send install request email"/>	

ただし、サーバーが一時的に落ちていたり、何らかの理由でバックアップからリストア途中であったりする可能性があるため、まずはサーバー管理者に確認してみることがベストでしょう。上記アラートメールと同時に、サーバー管理者にも CertMgr からアラートメールが送られています。

---

## 各サーバー管理者へ送信されるアラートメール

まだ日本語化はされていませんが以下のような、証明書の配備チェックが失敗しサーバーそれぞれに対して、そのサーバー管理者に以下のようなメールが送信されてきます。

SSL Server Certificate Alert

As of 2009/10/16 15:00:52 (UTC: 2009-10-16 06:00:52+00:00)

We have detected that the SSL server certificate on the the server below is not installed correctly.

SSL certificate common name : **www.example.com**

Server Name : **server1**

Host checked : **www.example.com**

Port checked : **443**

You are receiving this email because your email address is registered as the server administrator for this server.

The following is the result of certificate checking on the server.

[配備チェックの各ステップの結果が掲載されている]

**check\_result | NG |**

**Resolved Hostname | OK | Hostname www.example.com resolved to 1|192.168.239.91|443**

**Connected to Host | OK | Connected to host**

**Connected via SSL | OK | Established SSL connection (Over-SSL)**

**Certs Matched | NG | Received certificate is not the one in CertMgr**

Note: "1|xx.xx.xx.xx|nnn" indicates that it is an IPv4 TCP endpoint with IP address of xx.xx.xx.xx and port number of nnn.

Please correct this problem and let our certificate administrator (cmadmin@xxxx.com) know when it's corrected or the problem needs attention from him/her

The certificate administrator has also been notified of this issue.

サーバー管理者はこのメールを受け取り、必要あれば証明書の問題を修正します。

---

---

## FTP サーバーを経由した証明書パッケージの送信

前回の配備プロセスの回にでは取り上げなかった FTP サーバーを使って証明書パッケージをサーバー管理者に送信する方法を紹介します。次章の運用ベストプラクティスで本方法を推奨しています。

FTP サーバーの設定は、Applications > Settings 画面から行います。

FTP Upload Directory に証明書インストールパッケージをアップロードするディレクトリのパスを入力します。例えば /home/myadmin/certs/ を入力した場合、/home/myadmin/certs/c<証明書内部番号>/cert.zip にアップロードされます。

各サーバー管理者が本 FTP サーバーにログインできるようにアカウントを用意する必要があります。

CertMgr が FTP サーバーに証明書パッケージをアップロードするタイミングは、証明書インストール依頼メールを送信する直前です。

---

## CertMgr 運用のベストプラクティス

ここでは Kousec CertMgr の運用法について考えてみます。

### CertMgr マシンへのアクセス

CertMgr の証明書リポジトリには、管理対象のサーバー証明書の秘密鍵が格納されています。さらに自動インストールで使用する対象サーバーの管理権限ユーザーのパスワードや、証明書を購入する CA のシステム上のアカウントなども格納できます。

万が一悪意を持った者に侵入されるとこれら全てが漏洩しかねません。

まず、CertMgr のインストール環境の基本的なセキュリティを固める必要があります。一般的ですが以下のようなことを実施します。

- CertMgr のウェブインターフェースは非 SSL を禁止する。  
今回評価を行ったのはベータ版で CertMgr 自体は SSL が有効にはなっていませんでしたがリリースされるものは SSL も有効になります。
- ユーザー admin のパスワードを変更する。複数の人間で CertMgr を使用する場合は、かならず新しいユーザーを作成する。
- CertMgr のウェブインターフェースを IP アドレスで制限し、さらに OS のファイアウォールを有効にする。
- 他のサーバーアプリケーションと同居させない。
- CertMgr のバックアップはかならず暗号化を実施する。

### CertMgr の運用で検討すべきこと

次に、CertMgr の運用に関していくつか決めなければならないことがあります。

- A) 証明書の自動インストールを使うか否か。  
自動インストールを使う場合、対象サーバー上で管理権限を持つユーザーのユーザー名・パスワードを CertMgr 内に記録することになります。
  - B) 自動インストールを使わない場合の、証明書パッケージのサーバー管理者への送信方法のうち、どれを選ぶか。
  - C) 証明書監視（配備チェック）を行うために、インターネットへのアクセスを許すか。
  - D) CertMgr のメール送信などのネットワークアクセス自体を許すべきか。
-

---

それぞれについて検討した結果をベストプラクティスとして記します。

### **証明書自動インストールを使うか**

自動インストールを使うには CertMgr に対象サーバーの管理権限ユーザーのパスワードを記録しておく必要が出てきます。

必要以上の機密情報を保持するのを避けながら運用の効率化とバランスを取るために以下のような運用方法にします。

Web サーバーのような台数が多いサーバーについては自動インストールを使用します。LDAPサーバーのようにユーザー認証の根幹に関わるようなサーバーの証明書については、自動インストールではなくワンクリックインストーラーでインストールを行います。

### **証明書パッケージのサーバー管理者への送信方法**

CertMgr が提供する方法は、メールに添付、FTP サーバーにアップロード、そして CertMgr のウェブサーバーから直接ダウンロードする方法です。そのほかには、ネットワークを使用せず USB メモリなどで運ぶということも考えられます。

まず除外できるのは CertMgr のウェブサーバーから直接ダウンロードする方法です。これは複数のサーバー管理者がさまざまな場所から CertMgr のウェブサーバーにアクセスすると侵入されるリスクが高まるからです。メールに添付する方法も zip パスワードと一緒に送信されるという問題だけでなく、いつ誰によって開封されるか分からないという点からも懸念があります。

FTP サーバーなどの別のサーバー証明書パッケージを置き、zip パスワードだけをメールで送付するのがより安全でしょう。

また、証明書パッケージの作成は zip ではなくより強固な暗号化を持つ 7zip を使うように設定したほうが安全です。インストール依頼メールにも 7zip アーカイブの展開方法も記載します。

証明書パッケージの送付用に 1 台 FTP サーバーを用意します。この送付用サーバーにはサーバー管理者がそれぞれ自分のアカウントでログインできるようにします。CertMgr はこの FTP サーバーに証明書パッケージをアップロードするようにします。またアップロードしたファイルは 1 週間で消すなどの運用を行うほうがよいでしょう。

証明書パッケージは標準の zip ではなく 7zip を使うように CertMgr を設定します。

---

### **証明書監視（配備チェック）のためにインターネットへのアクセスを許すか**

配備チェックは CertMgr から監視対象サーバーへの外向きの通信であり、さらにウェブブラウザを使うのではなく専用のツールが必要最低限のアクセスだけを行います。従ってインターネット経由での配備チェックはセキュリティの低下をもたらすものではありません。しかし CertMgr マシンをよりインターネット接続ができないよりセキュアなネットワーク内に配置したいユーザーもいるでしょう。

ネットワークセキュリティ上の理由から CertMgr マシンを、インターネットに接続できないネットワーク内に配置する場合は、配備チェック用のサーバー名を証明書のコモンネームではなく内部サーバー名に設定し、内部ネットワークからの監視を行います。それでも配備チェックが出来ないサーバーについては CertMgr 上では定期監視を無効にします。

### **CertMgr のメール送信などのネットワークアクセス自体を許すべきか**

仮に CertMgr マシンをネットワークから切り離しオフラインで運用すると、CertMgr を使用して得られる効用自体が大きく制限されてしまいます。

メールの送受信が行えるネットワークに CertMgr マシンを配置します。

---

## SSL 証明書の運用におけるセキュリティの考察

さて、みなさんは SSL サーバー証明書の秘密鍵をどのくらい厳重に保管すべきだと考えていますでしょうか。

### SSL 証明書の秘密鍵管理の実情

暗号化を行う如何なるアプリケーションで暗号鍵の管理はそのセキュリティの根幹となります。SSL 証明書の秘密鍵も、鍵の保護を他のいかなることよりも重要視するのであれば、HSM（ハードウェア・セキュリティ・モジュール）をサーバーに搭載しその中に秘密鍵を閉じ込めて運用することになります。

しかし、SSL の適用範囲の拡大と汎用 CPU の高性能化から、SSL サーバースマシンの数が大きく増加しました。その結果、多数のサーバースマシンのひとつずつに SSL 用秘密鍵を紐づけることが不可能になり、秘密鍵を 1 か所で生成・維持し、サーバーに配布するという管理手法が出てきています。また各サーバーでは無人リブートを可能にするため秘密鍵は暗号化しない、暗号化してもそのパスワードもファイルに書き込んでおくといった使用方法がとられています。

### 通信暗号化とディスク暗号化における鍵管理の重要性の違い

また誤解を恐れずに言えば、SSL は通信の暗号化であり、ディスク暗号化における鍵管理の要求レベルより一段、要求レベルが低いことも、秘密鍵を配布するという管理手法が出てきた一つの原因かと考えます。通信暗号化とディスクの暗号化を比較します。

- 通信暗号化：鍵が漏えいした場合、その鍵を使った全通信セッションを終了し、CA が証明書を失効させる。また使用しなくなった鍵は保存しなくてもよい。
- ディスク暗号化：鍵が漏えいした場合、その鍵でそれまで暗号化したすべてのデータを再暗号化しなければならない。また使用しなくなった鍵はその鍵で暗号化したデータを保持する限り安全に保持し続けなければならない。

すなわち、SSL 証明書の秘密鍵が漏えいした場合、CA が即座に該当証明書を失効させ、新しい鍵で証明書を再発行すればいいと認識されがちです。

### SSL 証明書の秘密鍵漏えい時のコストは？

しかし、この認識に問題はないのでしょうか。

ディスク暗号用の秘密鍵がデータセンターの奥深くで使用されているのに対し、SSL 用秘

---

---

秘密鍵は、インターネットと企業内部ネットワークとの境界で使用されています。すなわち鍵が漏えいすれば誰にでも簡単に侵入するチャンスがあります。さらに侵入といっても SSL が保護しているサーバー内部に侵入するのではなく、クライアント PC との SSL サーバーの間に入り込み、自社のシステムを使用するエンドユーザーの重要な個人情報を盗みます。

### 実際の漏えい時点から漏えいしたと認識するまでの期間が長ければリスクが高くなる

SSL の秘密鍵さえ入手できれば、ホテルやその他公共の場所での無線 LAN 環境で簡単にこのようなことが可能になります。そして自社のシステムには何の痕跡も残しません。

したがって秘密鍵が漏えいしたかなどは実際に被害などが報告されてからでないと分かりません。実際に鍵が漏えいしてから自社システムの管理者が漏えいに気づくまでにかなりの時間が掛かりえます。

### 秘密鍵を頻繁に替えることが現実的な対処

SSL 証明書の秘密鍵もディスク暗号化の秘密鍵と同等レベルの保護をすることで、漏えいのリスクが小さくなりますが、現実的にはサーバー数が多い・無人リブートが必須・サーバーソフトウェアが対応していないといった理由から、ほとんどの場合現実的ではありません。

現実的な対処は、秘密鍵を頻繁に替えることでしょう。定期的な鍵の変更に加えて漏えいする可能性が高いイベント発生後に替えたほうがよいでしょう。

たとえば以下のようなイベントが考えられます。」

- A) SSL サーバーへ侵入された可能性が発見された場合即座に新しい鍵に切り替える。(これは当然です)
- B) システム構築においてテスト後、秘密鍵・証明書を切り替える。
- C) サーバーの移動・入れ替えなどの後に、秘密鍵・証明書を切り替える。

このように鍵の漏えいリスクが高まるイベント後に鍵を変更することが重要だと考えます。最近は何年かの有効期間を持つ SSL 証明書も販売されていますが、そのような証明書でも一度設置してしまえば契約年数は大丈夫というわけではなく、rekeying (秘密鍵を変更して証明書を再発行すること) をすることで漏えいリスクを軽減すべきでしょう。

### まとめ

SSL サーバー証明書の現状の設置方法を考慮すると、rekeying (秘密鍵を変更して証明書を再発行すること) を運用に取り入れることが鍵の漏えいリスクを軽減する最も有効な手段である。長期の有効期間を持つ SSL 証明書を利用している場合でも鍵の漏えいの恐れが
---

あるイベントの後にはかならず rekeying を行い、証明書を切り替えるようにする。

今回がこのシリーズの最終回となります。SSL サーバー証明書を使用するサーバーアプリケーションは多数存在し、その設定・運用方法はさまざまです。今回の検証では Linux 上のメール・ウェブ・FTP サーバーといったメジャーなソフトウェアへの証明書設置を通じて Kousec Server Certificate Manager の使い勝手と運用上の注意点をレポートいたしました。