
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～

第一回 検証構成と SSL 証明書の取得・配備計画



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

はじめに	5
検証の目的	5
テスト構成	5
SSL 証明書の取得・配備計画	7
SSL サーバー証明書はサーバーのため？それともサービスのため？	7
ホスト名を何枚の証明書にどのように割り振るか	8
1 枚の証明書は複数のサーバーに設置できるのか？	9
EV 証明書やドメイン証明書とは？	9
今回取得する証明書	10

はじめに

ウェブサイトの SSL 証明書というと実際にサイトを構築・運用している方はどのようなイメージをお持ちでしょうか。購入手続きや更新作業が面倒、どのサーバーに必要なのかといった疑問もお持ちかもしれません。また多数のクライアントをお持ちの Web 制作会社や Sier では数多くの SSL 証明書の更新作業が負担になりまたミスが発生しやすくなっている状況になっているかもしれません。

その一方で、増え続けるフィッシング詐欺や個人情報保護の意識の高まりから SSL 証明書の重要性と適用範囲は広まり続けています。増え続ける SSL 証明書の運用の効率化とセキュリティ（秘密鍵の管理等）の強化という二つの課題をバランスを取りながら実現していく必要があるのではないのでしょうか。

今回から 5 回にわたり紹介するソフトウェア、Kousec Server Certificate Manager、はそのようなニーズに答える SSL サーバー証明書の管理製品です。今回から Linux 環境に適用して行きその使用感・テスト結果などをレポートしていきます。

検証の目的

Kousec Server Certificate Manager を Linux ベースのインターネットサーバー環境で使用して SSL 証明書の各種管理を行い、その機能・使用感などをレポートします。

また今回の検証では最近利用が広まってきている Ubuntu Server 9.04 を Linux OS として使用します。Ubuntu は Debian 系ディストリビューションであり、サーバー用途でメジャーとなっている RHEL/CentOS とは異なる部分もすくなくありません。本レポートでは各サーバーソフトウェアの SSL 証明書の設定方法についても簡単に説明を入れています。今後 Ubuntu を使ってサーバーアプリケーションを使用する際、本レポートが少しでも参考になればと思っております。

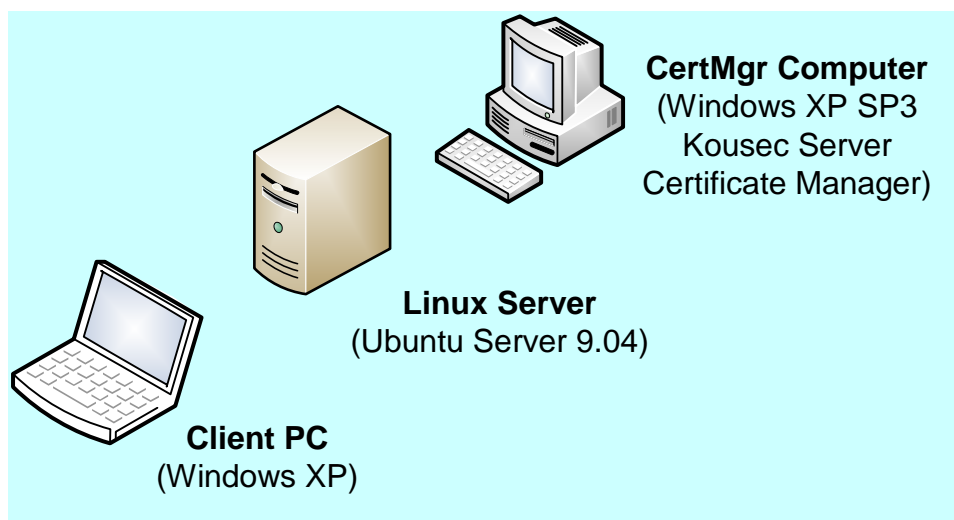
テスト構成

1 台の x86 サーバーを使用し、OS として Ubuntu Server 9.04 をインストールして外部との接続を持つウェブ・メールサーバーを構築します。将来的には負荷に応じてサービス単位で複数のサーバーに分散することを考慮した設計をします。

表 1 提供サービス

サービス	サーバーソフトウェア	用途
LDAP	OpenLDAP	各サービスが使用するユーザー認証
メイン web	Apache2	メインの公開ウェブ用
サブ web	Tomcat6	パートナー向けウェブ用
FTP サービス	Vsftpd	パートナー向け FTP サービス用
SMTP サービス	Postfix	メール送信および社外からの受信
POP3 サービス	Dovecot	社内 PC からのメールの受信
IMP4 サービス	Dovecot	社内 PC からのメールの受信

Kousec Server Certificate Manager は Windows XP の PC にインストールします。
以下に今回の検証でのハードウェア構成を示します。



SSL 証明書の取得・配備計画

この章では、どのサービスに SSL サーバー証明書を設置する必要があるかを挙げ、その場合どのような種類の証明書が適切かを検討していきます。

SSL サーバー証明書はサーバーのため？それともサービスのため？

SSL サーバー証明書を「サーバー証明書」とは呼んでいますが、筆者はサーバー毎ではなくサービス毎にサーバー証明書を取得するケースが多いと感じています。今回の検証では多くのサービスを 1 台のサーバー上で稼働させますが、通常は、負荷に応じて複数のサーバーマシンにサービス単位で分割・分散させていきます。特に LDAP サービスは実運用ではファイアウォール内のサーバーに設置することが必須になります。そして例えば Web/FTP サービスとメール関連サービスはそれぞれ専用のサーバーマシンに移動させることなどが考えられます。したがって SSL 証明書もサーバー毎ではなくサービス毎に取得するという考え方です。

逆に、サーバー毎に証明書を取得するケースも考えられます。SSH ではそのサービスを利用するのではなくそのサーバーを管理するために使います。この場合は SSH というサービスではなく管理対象のサーバーを特定するためのサーバー証明書を取得・設置するべきだと考えます。ただし今回使用する Ubuntu の OpenSSH では PKI 証明書はサポートしていないので今回の検証では SSH には証明書は使用しません¹。

すなわちサービスを提供するサーバーソフトウェアではサービス毎の証明書、管理対象としての口を提供するサーバーソフトウェアではサーバー毎の証明書が適切だといえます。

これをもとに今回の環境で必要となる SSL 証明書をリストアップしてみます。

表 2 証明書が必要なホスト名

証明書が証明するホスト名	用途	設置するサーバー	サーバー単位かサービス単位か
ldap.example.com	LDAP	server1	サービス
www.example.com	メイン web	server1	サービス
www2.example.com	サブ web	server1	サービス
ftp.example.com	FTP サービス	server1	サービス
smtp.example.com	SMTP サービス	server1	サービス

¹ SSH Communications Security Corp が提供する商用の SSH 製品ではサーバー認証およびユーザー認証に PKI 証明書が使用できる

pop.example.com	POP3 サービス	server1	サービス
imap.example.com	IMAP サービス	server1	サービス

ホスト名を何枚の証明書にどのように割り振るか

上記で、証明書が必要なサービスとそのサービス用ホスト名を列挙しました。次に、これらホスト名をカバーするためにどのような証明書を何枚取得するか検討していきます。

SSL 証明書は、1枚の証明書がカバーできるドメイン名（ホスト名）の数・種類によって3種類に分けられます。

- シングルドメイン証明書：1枚の証明書にはひとつのホスト名だけを登録できる。
- ワイルドカード証明書：1枚の証明書で、全てのサブドメインのホスト名をカバーできる。
例：証明書には、“*.example.com”という*を含んだホスト名を登録しておくことで、上記のような同じドメイン名で終わる全てのホスト名をカバーできる。
- マルチドメイン証明書：1枚の証明書に、複数の無関係なホスト名を登録することができる。
例：www.example.com, example.com, another.net, another.org

最も単純なのは、1枚のワイルドカード証明書で今回使用するホスト名を全部カバーすることです。ただし現実にはそう簡単ではありません。理由は以下のとおりです。

- ワイルドカード証明書を販売していないCAが多い。
- EV 証明書（後述）では、その仕様としてワイルドカード証明書は発行できない。
- ワイルドカード証明書の価格はシングルドメイン証明書の価格の数倍する。

誤解を恐れず言えば、高いアシュアランスレベルのサービスでは一般的にはワイルドカード証明書は使用しない、ということです。

マルチドメイン証明書は、複数のSSL対応していない仮想ホストをSSL化する場合や、複数のサーバーを統廃合する場合、または今までイントラネット内からサーバー名でアクセスしていたサーバーをインターネット経由でもアクセス可能にする場合などで頻繁に使用されます。

1枚の証明書は複数のサーバーに設置できるのか？

シングルドメイン証明書、ワイルドカード証明書にしろ、マルチドメイン証明書にしろ、1枚の証明書を複数のサーバーに設置する場合、一般的にCAでは「サーバーライセンス」という考え方を導入しています。これは1枚の証明書を何台のサーバーに設置できるかという購入者の使用权です。

CAによってこのサーバーライセンスの価格が異なります。証明書の取得コストを抑える目的で、一枚の証明書にホスト名を詰め込んでも、実際にサーバーを拡張する際にサーバーライセンスの追加費用が大きくなるというケースも考えられます。検討する際には必ずCAのサーバーライセンスに関する情報も入手しておきましょう。

EV証明書やドメイン証明書とは？

ドメインのカバレッジの種別とは別に、もうひとつSSL証明書製品の種別があります。証明書発行時の申請者の認証の方法（厳密さ）です。

SSLサーバー証明書は通信の暗号化とそれに必要な通信相手の認証のために使われています。ウェブ上ではさらに証明書が証明しているドメイン名上のサービスの信頼性（サービスの運営会社の信頼性など）が求められるゆえ、申請者組織の妥当性の確認が証明書発行時に行われます。特に増え続けるフィッシング詐欺を防止するためにこの確認をさらに厳密に行うEV証明書が数年前に導入されました。またそれとは逆に、個人サイトや非商用のサービスなどでもSSL導入のニーズが増え、低コストで取得できるドメイン証明書が導入されてきています。

- 組織認証 (Organization Validation)： CAによっては企業認証などとも呼ばれます。証明書に登録されるドメイン名の使用权の証明だけでなく、証明書申請者（団体や個人）の实在証明なども行います。
- 拡張認証 (Extended Validation)： 一般的にEV証明書と呼ばれます。組織認証よりさらに厳密な申請者の实在認証や企業・団体としての信頼性が審査の対象となります。申請可能な団体の条件も引き上げられています。
- ドメイン認証 (Domain Validation)： ドメイン名の使用权だけを確認し証明書が発行されます。なおドメイン認証による証明書の場合、申請者情報のうち、ドメイン名のみが証明書内のディスティンクティブネーム (DN) に設定されます。

EV 証明書は、金融機関や今後増えるであろう医療機関、そしてフィッシング詐欺に使われやすい著名企業や著名サービスで今後ますます必要になってくると考えています。

逆に内部アクセス、特にフィッシング詐欺が狙うようなウェブブラウザ上の人間によるアクセスではなく、ソフトウェアがアクセスするだけのものには、コストの面からドメイン証明書でもよいと筆者は考えています。

今回は検証であるから商用 CA からの証明書は購入せず、自分で運用するプライベート CA から発行する証明書を使用します。しかし検証システムから本番システムを設計する場合に証明書の情報が再利用できるよう、商用 CA の証明書の使用も見越した設計を行います。

今回取得する証明書

上記を考慮し今回のサーバーには下記のような証明書を取得することにしました。

表 3 今回取得する証明書

証明書内のホスト名	配備先	証明書名	用途・利用者	認証要件
ldap.example.com	LDAP	ldap.example.com	内部認証用	ドメイン
www.example.com	メイン web	www.example.com	公開サーバー	組織 (or EV)
www2.example.com	サブ web	www2.example.com	社内・パートナー向け	組織
ftp.example.com	FTP サービス			
smtp.example.com	SMTP サービス	smtp.example.com	社員の PC からのみメール転送を受付ける	ドメイン
pop.example.com	POP3 サービス	pop.example.com	社員の PC からのみ	ドメイン
imap.example.com	IMAP サービス			

前表の列の意味は以下のとおりです。

証明書内のホスト名： 証明書に含めるホスト名。複数名ある場合はマルチドメイン証明書を取得する必要がある。証明書の SubjectAltName に複数のホスト名が設定される。

配備先： 証明書を設置するサービス。

証明書名： 証明書を簡単に識別する名前。複数のホスト名を持つ場合は代表のホスト名を決めそれと同じにする。この名前を DN の CommonName にも設定する。また証明書ファイルのファイル名にも使用する。

用途・利用者： 実際にサービス接続時に証明書を確認する人・プログラムなど。

認証要件： 証明書が必要とする認証のレベル。EV、組織認証、ドメイン認証のいずれかから選択する。

今回、以下の方針に基づき認証要件を決めました。

www.example.com, www2.example.com, ftp.example.com:

公開サーバーやパートナー向けサービスといった、不特定多数からのウェブアクセスがメインとなるサービスについては**組織認証**の証明書としました。また公開サーバーが著名になり不特定多数（特に一般消費者）向けのショッピングサイトになる場合は **EV 証明書**が必要になると考えます。

ldap.example.com, smtp.example.com, pop.example.com, imap.example.com:

接続先の素性を事前に知り接続先として設定しているソフトウェアが証明書を受け取り接続先の確認を行う場合（メールクライアントソフトウェアやサーバーソフトウェア）であれば、ドメイン認証の証明書で確実な接続先認証が行えます。

それゆえ、各サービスからの内部認証用アクセスや社内 PC からの非ウェブブラウザによるアクセスとなるサービスは**ドメイン認証**としました。

ドメイン認証について。

ドメイン認証の証明書での一つの懸念は、CA が偽った申請者へ証明書を発行する可能性が組織認証証明書よりも高くなるのではという点です。ただし各 CA ともドメイン認証証明書を発行する際の確認方法に各社の独自技術を導入し、確認・発行のスピードと正確さの両方を向上させているようです。

なお今回は検証目的ですので、実際に商用 CA からの証明書は購入せずに、Kousec Server Certificate Manager に内蔵されているプライベート CA (Built-in Private CA)から証明書を発行します。

ドメイン名のカバレッジについて。

ホスト名 www2.example.com と ftp.example.com、そして pop.example.com と imap.example.com はそれぞれ2つのホスト名を1つの証明書に格納するマルチドメイン

証明書を取得することにします。pop と imap は単一のサーバーソフトウェア(Dovecot)が提供するので一つの証明書にしたほうが管理が楽になります。www2 と ftp は異なるサーバーソフトウェアが提供しますが、今回はもともと別マシンで運用されていた FTP サーバーを統合すると想定し、あえてマルチドメイン証明書にしました。

以上で、SSL 証明書の取得・配備計画は終了です。
次回からは、実際に Ubuntu Server 上に各サーバーソフトウェアをインストールし SSL 証明書の設定を行っていきます
