

---

テクニカル・ホワイトペーパー

## Kousec Server Certificate Manager

### 製品概要



Copyright 2009-2011 Kousec Software, Inc. All rights reserved.  
All company names and product names are trademarks of their respective holders.

R7



---

## 目次

はじめに .....	4
IT システムの全レイヤーで導入される SSL/TLS .....	4
SSL/TLS 導入の効果 .....	5
コストを削減しつつ安全に SSL/TLS を導入する実行手段 .....	6
証明書管理システムを導入する際の成功要因 .....	7
<b>KOUSEC SERVER CERTIFICATE MANAGER.....</b>	<b>7</b>
製品の導入 .....	7
SERVER CERTIFICATE MANAGEMENT の主要コンポーネント .....	9
証明書検出 .....	9
証明書ライフサイクル管理 .....	10
監視 .....	11
アラートと通知 .....	11
鍵管理 .....	11
ビルトイン・プライベート CA .....	11
管理 WEB コンソール .....	12
管理対象サーバー・アプリケーションとプラットフォームのサポート .....	12
WINDOWS 証明書サービスとの統合 .....	12
<b>結論 .....</b>	<b>14</b>

## はじめに

SSL/TLSプロトコルを使用した安全なネットワーク通信はあらゆる規模のITシステムで必要になってきており、安全でない通信や独自の暗号化通信技術はSSL/TLSに取って代わられてきています。また、企業や政府がITシステムをクラウドへ展開するにつれこの傾向はますます強まっています。

### IT システムの全レイヤーで導入される SSL/TLS

今日、SSL/TLS の技術は IT システムの全レイヤーに導入されています。ハードウェアデバイスは 管理/制御通信を保護するために SSL を使用します。OS のようなプラットフォーム・レイヤーやアプリケーション・プラットフォーム、仮想化プラットフォーム、ミドルウェアのほとんどの主要コンポーネントはみな、情報の信頼性と機密性を確保するために通信手段として SSL を使用します。

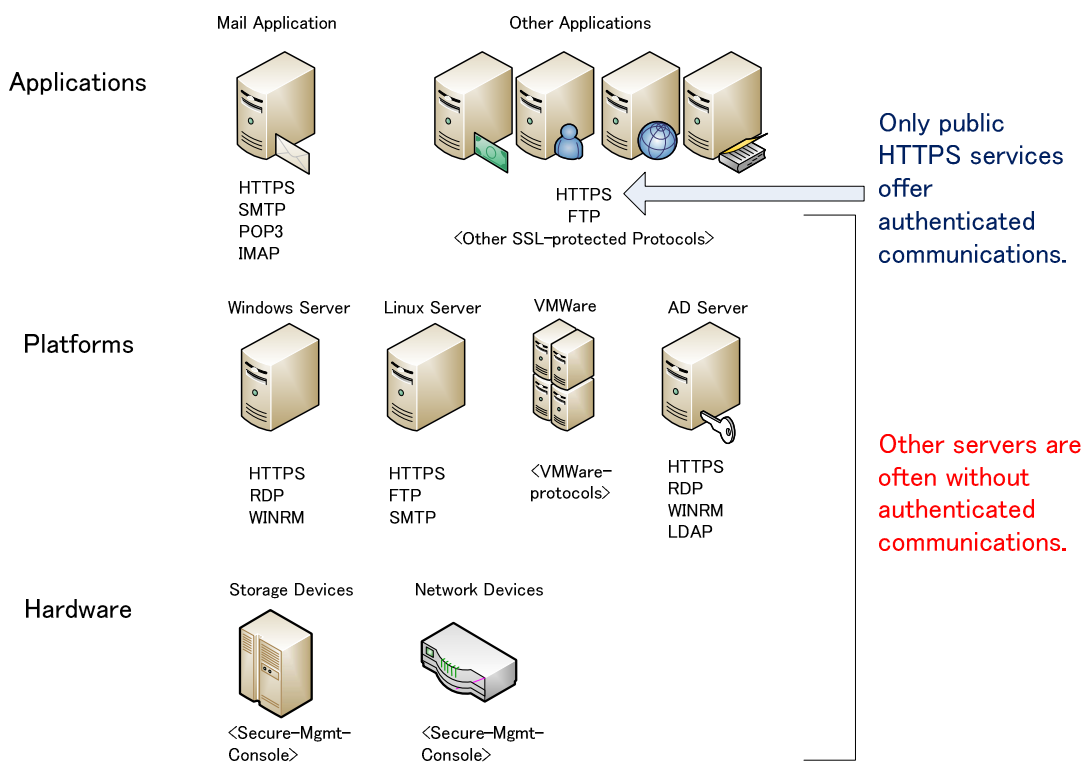


Figure 1. 全レイヤーでの SSL

---

## SSL/TLS 導入の効果

SSL/TLS には 2 つの主要なセキュリティ機能があります。

- 業界標準の暗号化強度
- 通信相手の認証

しかしながら、SSL を有効にしたサーバーの数が大幅に増えるにつれ、多くの SSL 導入環境ではこれらの利点の半分あるいはそれ以下しか享受できなくなっています。そこにはいくつかの障壁があります。

### 信頼された SSL 証明書の欠如による認証されない通信

SSL を有効にしたサーバーは増加していますが、公開用 HTTPS サーバーのみに信頼された SSL 証明書を入手する組織がしばしばあります。自己署名やその他信頼に値しない証明書をクライアント・ソフトウェア（エンド・ユーザーや他のシステム）に提示した場合、クライアントは意図通りの相手と通信しているという確信を持つことができません。典型的な IT システムでは、エンド・ユーザーや他のクライアント・コンピューターシステムはユーザー名とパスワードをサーバーへ送信します。適切な SSL 証明書がない場合、これは”ランダムな番号に電話をかけ電話に出た人に秘密を教えるようなもの”になってしまいます。

#### 例

- ホテルや空港から無線経由で会社のメール・システムにアクセスするユーザー。会社のメール・サーバーが自己署名証明書を使用しており、ユーザーが接続のためのメール・サーバー認証を無効にしている。

### SSL サーバーの広範な使用により起こりえる秘密鍵の漏えい

ディスク暗号化システムの暗号化鍵に比べ、SSL の秘密鍵の保護は”軽視”されてきました。これは、SSL は HSM (hardware security modules)のない多くの標準サーバーに導入され、また、動的なビジネスの変化に適合するようしばしば移動または再設定しなければならないためです。秘密鍵はこのレベルの保護では外部に漏えいする重大な危険性にさらされています。

#### 例

- Web サーバーのハードウェア・アップグレードが安全なディスク消去手順に従わず実施された。

### SSL 証明書の数が増えるにつれ有効期間中の更新がなされない

SSL 証明書にはさまざまな理由から有効期限があります。有効期限の切れた証明書を持つバックエンドのサーバーに接続しようとすると接続は繰り返し失敗します。それがシステム障害にもつながります。

#### 例

- 
- ”ネットワーク接続失敗”というエラー診断メッセージのみを出力し不意に障害の発生する大規模チケット販売システム。一つのバックエンドサーバーの証明書が有効期限切れになったことが原因だった。

## コストを削減しつつ安全に SSL/TLS を導入する実行手段

先に述べた障壁を克服するためには、適切な証明書管理システムを整えなければなりません。システムは下記の機能を備えている必要があります。

**証明書管理者が複数のソースから証明書入手・管理し、アプリケーションやビジネスの要件の変化に伴い証明書ベンダーを変更することができるようにすること。** システムを使用し、証明書管理者はまずプライベート CA 発行の証明書を使って、多くのアプリケーションでインストール時に生成される自己署名証明書を置き換えます。それから、ビジネス・ニーズの変化に伴い、商用 CA の”外向け”証明書や会社内の CA のその他証明書に移行することができます。このようにして、証明書管理者は単一のシステムを使用して全サーバー証明書を管理下におくことができます。

**必要なときに秘密鍵を変更することができるように証明書の秘密鍵再発行を容易にし、秘密鍵漏えいの危険性を低減すること。**

秘密鍵は、証明書の有効期間にかかわらず、定期的に、また、漏えいの危険性が生じたときに変更すべきです。そのためには、証明書更新時の CSR 生成と証明書インストールを自動化すべきです。

**管理されていない、または、有効期限の切れた証明書を見つけるために会社のネットワークを継続的に監視するシステムを使用することで、安全で信頼済みアプリケーションを十分に利用し、有効期限切れ証明書によるシステム障害を防止すること。**

体系的な手段をとらずに証明書管理者やサーバー管理者が組織内の全証明書の状況を追跡するのは非現実的、あるいは、不可能です。管理されたサーバー証明書の継続的な監視と管理されていないサーバー証明書の検出の自動化は、管理者が仕事を達成するための手助けとなります。

IT システムは、今日の常に変化し続けるビジネス状況に順応するために再設定、再配置、アップグレード、統合等が数年の間になされます。したがって、複数年の有効期間をもつ証明書をインストールするだけでは根本的な問題の解決にはなりません。

---

## 証明書管理システムを導入する際の成功要因

証明書管理システム・ソリューション（あるいは他のいかなる IT ソリューションも）を導入する際の成功要因は、大規模な組織と中小規模の組織とでは大きく異なります。数千台のサーバーをもつ大規模組織は、エンタープライズ PKI システムを導入できる IT セキュリティ専門家を雇います。一方、小規模な組織は、十分な PKI の知識をもつ専任の IT セキュリティ管理者を雇う余裕のないことがよくあります。

そのような会社こそ、SSL 導入環境は、PKI の見た目や専門用語の複雑さがネックとなり管理されずに放置されていることが多く、適切な証明書管理ソリューションが必要です。

使用方法が簡単で、PKI の専門用語が一般向けに書かれている製品を選択することは、証明書管理ソリューションの導入を成功に導く重要な要因となります。

## Kousec Server Certificate Manager

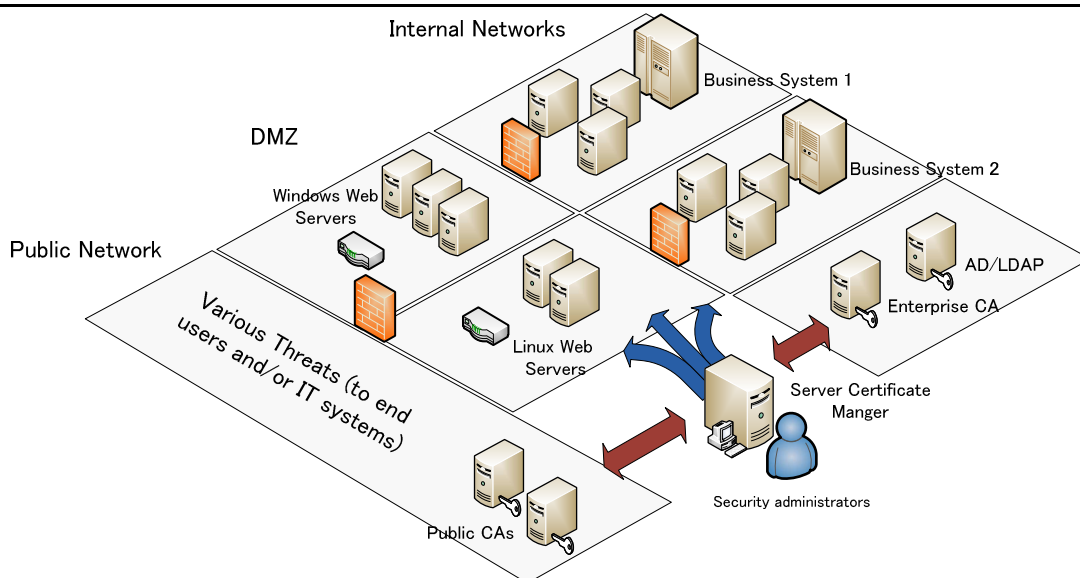
### “サーバー証明書管理をより簡単に”

Kousec Server Certificate Manager は SSL/TLS の管理を実現する現実的な方法を提供する製品です。その証明書検出機能やライフサイクル管理機能を使用することで、組織内で安全で費用対効果の高い SSL/TLS インフラを実現することができます。

本製品の理念は、使い勝手の良さとシンプルさに重きを置いています。PKI の知識があまりない証明書管理者でも簡単に導入でき、すぐに使用を開始することができます。本製品は組織内で既存システム管理ソフトウェアが既に実施していたことを重複してしようとしているわけではありません。

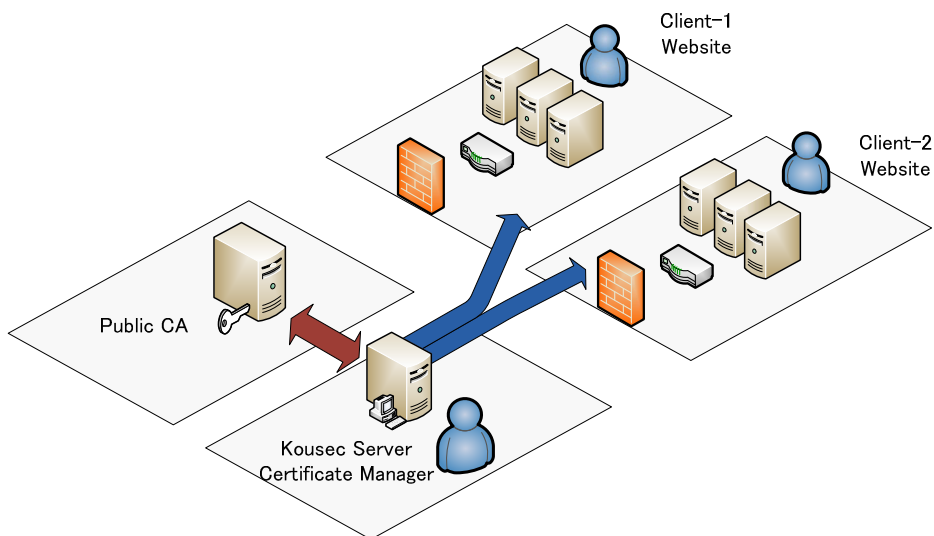
### 製品の導入

Kousec Server Certificate Manager は、組織内ネットワークのコンピューターにインストールされ、そこがサーバー証明書の管理者が管理する中枢となります。証明書管理者は一般の CA や内部の CA（ある場合）、または、ビルトイン・プライベート CA からの証明書を手し、サーバーへインストール、コンソールから監視することができます。



**Figure 2.** 導入例

他にも、管理対象サーバーの存在するネットワークから分断されたネットワークに Server Certificate Manager をインストールする導入シナリオがあります。この場合、ウェブサイト管理者が SSL 証明書とサーバーの詳細を Server Certificate Manager の管理者に伝え、Server Certificate Manager の管理者はワン・クリック・インストーラー・パッケージに入った証明書を提供します。このようにして、ウェブサイト管理者がしなければならないのはインストーラー・パッケージを実行することだけになります。二者は、例えば証明書リセラーとウェブサイト・オーナーのように、ビジネス上の境界で区切ることもできます。下図はこのシナリオの一例を示しています。



**Figure 3.** ネットワークが分断された環境への導入

## Server Certificate Management の主要コンポーネント

Server Certificate Management の主要コンポーネントは、下記に述べるとおり、証明書リポジトリや自動化された管理機能を提供します。

### 証明書検出

証明書検出コンポーネントは会社のネットワークをスキャンし証明書管理者が認識していない SSL サーバー証明書を明らかにします。全ての証明書を見つけた後、Server Certificate Manager で設定した信頼された証明書ポリシーに従い検証され、レポートが生成されます。

その後、管理者はその証明書を Server Certificate Manager の管理下に置くべきかどうかを決定し、置く場合、インポート・プロセスを開始することができます。証明書検出は、Server Certificate Manager を組織の IT システムに導入する際の最初のステップとして使用されます。また定期的にサーバー・アプリケーションによりインストール時に作成され管理されていない証明書を検出するために使用するべきです。下図は 検出レポート の例です。

#### Discover Certificates - Report

Summary of Server Certificates Found								
Out of 14 discovered certificates, 0 are valid certificates, 2 are self-signed certificates, 12 are untrusted certificates, 0 are expired certificates, 0 are revoked certificates. Analysis Date: 2009/11/18 17:50:09 Trusted Cert Store: CertMgr-Trust-Store Kousec CertMgr Version: RC-1c								
IP Address	Port	Hostname	Port Use	Common Name	Issuer	Validity	Expires	Others
192.168.239.91	21	server1	ftp	www2.example.com	Kousec CertMgr Built-in Private CA	untrusted	2010/10/08	
192.168.239.91	993	server1	imaps	pop.example.com	Kousec CertMgr Built-in Private CA	untrusted	2010/10/08	unsafe-renego
192.168.239.91	587	server1	smtp-submission	smtp.example.com	Kousec CertMgr Built-in Private CA	untrusted	2010/10/08	unsafe-renego
192.168.239.91	995	server1	pop3s	pop.example.com	Kousec CertMgr Built-in Private CA	untrusted	2010/10/08	unsafe-renego
192.168.239.91	636	server1	ldaps	ldap.example.com	Kousec CertMgr Built-in Private CA	untrusted	2010/10/08	
192.168.1.153	3269	WIN2003EN32	msft-gc-ssl	win2003en32.orenosv.com		untrusted untrusted	2010/11/15	
192.168.1.153	636	WIN2003EN32	ldaps	win2003en32.orenosv.com		untrusted untrusted	2010/11/15	
192.168.1.107	902	PC1	vmware-authd	PC1	VMware, Inc.	self-signed	2029/01/11	unsafe-renego
192.168.1.107	8333	PC1	https-vmware	PC1	VMware, Inc.	self-signed	2029/01/11	unsafe-renego
192.168.1.21	3389		ms-wbt-server	win2008jp32base		untrusted untrusted	2010/05/07	

Figure 4. 検出レポート

---

## 証明書ライフサイクル管理

ひとたび証明書を Server Certificate Manager にインポートすると、証明書管理者は 証明書ライフサイクル コンポーネントのもとで管理することができるようになります。

**証明書の登録と更新:** Server Certificate Manager は証明書管理者が証明書製品を選択するプロセスを進め、CSR を生成し、注文、証明書の受け取りを行うことを支援します。新規登録(enrollment)であれ更新(renewal)であれ、このプロセスは、Server Certificate Manager では証明書取得プロセスと呼ばれます。また、証明書ライフサイクルマネージャーはこれら操作のための基礎を形成します。

このコンポーネントを使用すればサーバー管理者は証明書要求プロセス (CSR 生成) で作業を実施しなくてよくなります。また、組織にとって重要となるネットワークとウェブ・サーバーの一貫性を維持するため、サーバー証明書の情報と目録を一か所で集中管理・保護するほか、会社内で決められた証明書ポリシーを施行することができるようになります。

**証明書インストール:** いったんサーバー証明書の受け取り Server Certificate Manager に格納したら、証明書管理者は証明書配備プロセスを開始することができます。証明書配備プロセスでは証明書をサーバーにインストールし、動作確認を行い、証明書監視対象として登録します。

サーバー証明書インストーラーは、証明書と秘密鍵そして中間 CA 証明書を特定のサーバーにインストールする最善の方法を選択します。このコンポーネントを使用すると証明書インストールと操作テストは自動化され、サーバー管理者は間違いの起こりやすい操作から解放されます。

証明書管理者は各サーバー証明書に対する自動化レベルを選択することができます。

- **全自動化されたリモート・インストレーション:** サーバー OS やサーバー・アプリケーションのユーザー名・パスワードは Server Certificate Manager に登録されている必要があります。
- **ワン・クリック・インストーラー:** サーバー管理者は、証明書インストーラー・パッケージを受け取り、証明書をインストールするサーバー上で実行します。サーバー・アプリケーションにアクセスするのにユーザーパスワードが必要な際、サーバー管理者はパスワードを入力するよう促されます。サーバー管理者はいつ証明書をインストールするかをコントロールすることもで

---

きます。

- **手動インストール:** サーバー管理者は、証明書パッケージを受け取り、手動インストールを実施します。この方式は、対象サーバー・アプリケーションやその設定でサーバー管理者の特別な処理が必要なときに使用されます。

**証明書の引退(retire):** 証明書は、新しい証明書に取って代わられたとき、または、発行した CA に無効にされたとき、または、不要になり無効であると宣言されたときに引退(retire)されます。これらの証明書と対応鍵は、アーカイブが取られ保持されます。

## 監視

サーバー証明書は、ひとたびサーバーにインストールされると、Server Certificate Manager により一定間隔ごとに監視、検証されます。不注意、または、計画外のネットワーク設定変更により上書きされた証明書のような例外を検出するためにを行っています。

## アラートと通知

Server Certificate Manager は重要なイベント時にはアラートを上げ、eメールのメッセージの形式や SNMP トラップで関係者に通知します。アラートは監視下の証明書に対してだけでなく、プロセス、たとえば、証明書の登録や導入プロセスの期限が迫っているときや、開始されているべき時期に開始されていない更新プロセスに対して上がります。

## 鍵管理

このコンポーネントは、証明書に使用される鍵ペアを生成、保管、保護します。秘密鍵をディスク上で保管する際は必ず暗号化し、証明書インストール・パッケージの一部として秘密鍵を送信する際は暗号化パスワードを変更します。

## ビルトイン・プライベート CA

商用のサード・パーティ証明書機関や会社内のエンタープライズ CA のほか、Server Certificate Manager にはビルトイン・プライベート CA 機能があります。このプライベート CA は開発期間中、手軽に使用することができます。そして開発が終盤になると証明書は本番環境に向け商用 CA のものに移行できます。すでに Windows サーバー PKI を導入している会社では、このプライベート CA を PKI CA 階層の一部として使用することができ、他の信頼済みルート CA の証明書を導入する必要がなくなります。

---

## 管理 Web コンソール

管理 Web コンソールは、証明書管理者が Server Certificate Manager の主要コンポーネントにアクセスするためのインターフェースです。複数のユーザー・アカウントの作成と、ユーザー・アカウントに2つのレベルの権限を与えることができるようになっています。

証明書管理画面によってユーザーは分かりやすい手順の流れに従うことができます。

## 管理対象サーバー・アプリケーションとプラットフォームのサポート

Server Certificate Manager は、下記のような製品に自動証明書インストーラーやワン・クリック・インストーラーを提供しサポートしています。Kousec Software は顧客からの要望に基づきサポート製品を拡大しています。

### Windows プラットフォーム

- IIS 6.0, 7.0, 7.5
- Exchange Server 2003

### Linux、Unix プラットフォーム

- Apache HTTPD Server
- Mail servers (Postfix, Dovecot)
- FTP servers (vsftpd)

Oracle WebLogic Server 8, 9, 10

Apache Tomcat 4, 5, 6

Sun Java Web Server

VMware ESXi 3.5, 4.0, ESX 4.0, vCenter Server 4.0

最新情報はお問い合わせください。

## Windows 証明書サービスとの統合

Server Certificate Manager は Windows 証明書サービスへの証明書発行要求を自動化できます(auto-enrollment)。これにより、既に Windows 証明書サービスを使用している環境においても Linux サーバーも含めて一元管理可能になります。

また Windows CA に加えて、Windows Server 2008 R2 で導入された Certificate Enrollment Web Service にも対応しています。



---

## 結論

Kousec Server Certificate Manager により、企業・官公庁は運用・取得コストを削減しつつ様々なプライバシー規制やセキュリティ標準の要件を満たす高度に安全なシステムを実現することができ、また IT システムへの来るべき変化に十分に備えることができます。これは、変化するニーズに合致する最適な SSL 証明書ベンダーを選択することと同様に、自動化された証明書の検出や配備、監視によって可能になります。

専任のセキュリティ管理者がいなくさんのビジネス環境でもソリューションを容易に導入することができるようになります。また、コウセック・ソフトウェアではお客様が SSL 証明書を費用対効果の高い方法で管理するためのご支援もいたします。

### お問い合わせ

株式会社コウセック・ソフトウェア

Tel/Fax: 044-833-4666

Email: [info@kousec.com](mailto:info@kousec.com)

Web: <http://www.kousec.com/>