DigiCert PKI Platform とオンプレミスソフトウェアの所有コストの比較

概要

PKI ソリューションの導入と管理に取り組むのは容易なことではありません。
特に、組織が自ら構築し、管理するオンプレミスの PKI ソフトウェアの場合はなおさらです。
本ホワイトペーパーでは、自前の PKI ソフトウェアにかかる隠れたコストを明らかにします。
一方、DigiCert PKI Platform は非常にコスト効率がよく、導入の手間が少ない上、
信頼できる認証、検証、完全性、暗号化を企業の最重要アプリケーションに提供できることを実証します。

digicert®

目次

はじめに

企業は、 機密データ保護の要請に応え、 信頼できるビジネスエコシステムを構築し、 社内のデジタル資産を不正アクセスから守るため、 PKI (公開鍵基盤) ソリューションをよりどころとして最高レベルの保護を実現しています。PKI は、 企業や官公庁、 あるいはネットワークでつながっているコミュニティなどで、安全で信頼できる認証や、デジタル署名、暗号化を実現するための、スタンダード的存在として認められています。

むろん暗号化は PKI 内部の中核的なメカニズムです。しかし、証明書の発行、管理、失効などが適切に行われなければ、PKI のメリットを十分に生かすことはできません。つまり、 一口に PKI の導入と言っても、どれでも同じというわけではないのです。たとえば、PKI の中には、組織内で送受信される電子メールの暗号化など、簡単なアプリケーションだけにしか対応していない、機能の限られたものもあります。一方、国の安全保障に関わる情報を保護する安全なサイトやネットワークへの物理的アクセスと論理的アクセスを統合的に管理する、複雑な機能を実現しているものもあります。

アプリケーションがどのようなものであれ、PKI ソリューションの導入と管理に取り組むのは容易なことではありません。PKI の場合、 他のテクノロジーソリューションと異なり、 ソフトウェアの範疇を大きく超える不確定要素が数多くあります。たとえば、ポリシーを作成するためのトレーニング、データセンターのセキュリティ、証明書の管理などです。PKI を実装するためのコストに加え、 堅牢で安全な PKI 環境を構築するためのあらゆる要素に、 さらにコストがかかるのです。こうした隠れたコスト、忘れられたコストが、ソフトウェア自体の購入コストよりもずっと高くつくこともあります。

特に、 組織が自らのデータセンター内に構築し、 管理するオンプレミス PKI の場合はなおさらです。本ホワイトペーパーでは、 自前の PKI ソフトウェアにかかる隠れたコストを明らかにします。同時に、DigiCert PKI Platform は非常にコスト効率がよく、 導入の手間が少ない上、信頼性も折り紙付きであり、認証、検証、完全性、暗号化を企業の最重要アプリケーションに提供するという目標を簡単に実現できるということを実証します。

オンプレミス PKI の複雑さ

PKI の場合、 他のテクノロジーソリューションと異なり、 認証ソフトウェアとそれを支えるインフラストラクチャだけがあればいいというわけにはいきません。オンプレミスの PKI を構築するためには、インフラを構築し、 管理し、 サポートするための教育訓練を受けた専従のスタッフが必要です。証明書用の鍵を保護するためには、高度なセキュリティを備えた設備が不可欠ですし、 しっかりとしたポリシーと手順もなくてはなりません。また、 確実に運用を継続するため、フェールオーバー技術や拡張可能なインフラも必要になります。PKI は常に利用可能であることが重要だからです。PKI が使用できないばかりに社員やパートナーが身元確認を行えなくなったとしたら、ビジネスのタイミングを逃してしまうかもしれません。

ルート証明書のセキュリティや、 証明書の発行プロセスも重要であり、オンプレミス PKI を構築する場合は、これらに適切に対処できるよう準備しておく必要があります。セキュリティレベルの設定、 身元確認、 手順など、あらゆることが適切に行われなければ、ルート証明書の信頼性が揺らぎかねません。企業を大きな危険にさらすことになります。ルート証明書の信頼性が揺らげば、 それを管理している認証局 (CA) から発行されたすべての証明書の信頼性も揺らぎ、その正当性に疑問符が付き、ひいては PKI の信頼の階層構造全体が危うくなってしまいます。

信頼は PKI の主要な構成要素です。自社の PKI を使用して、社外の組織との間で安全な通信や取引を行おうとする場合、信頼できる第三者機関である CA をルート認証局とする必要があります。企業自体が運営している CA から発行された証明書が、 社外の取引相手から完全な信頼を得られるとは考えにくいので、 BtoB 通信に対しては信頼できる CA を使用した PKI インフラストラクチャを別個に追加する必要があるのです。

また、 2 つ以上の独立した組織が相互に認証を行う信頼インフラストラクチャを構築するという方法も考えられます。この場合、 1 つの組織のルート CA 階層が、 他の組織の CA 階層の中の CA に、 下位 CA 証明書を発行することになります。つまり、 この相互認証の信頼ネットワークに参加する組織は、 相互運用的な形で稼働することになるのです。ただし、 相互認証のシステムを構築するためには、 法外なコストと膨大な時間がかかることを覚悟しなければなりません。

オンプレミス PKI の実コスト

組織が PKI を構築しようとする際、 ソフトウェアライセンスやハードウェア、 設置サービスなど、 従来のソリューションコストにのみ注目が集まりがちです。しかし、こと PKI に関しては、自前で構築するかどうかを検討するにあたって、他にも多くの要素やコストについて考慮しなければなりません。実際、 オンプレミス PKI の場合、 PKI ソリューションのソフトウェアやハードウェアにかかるコストは総所有コストのほんの一部にすぎないケースも多いのです。

拡張性、 信頼性、 安全性を備えたオンプレミス PKI を構築するには、購入費用だけでなく、以下に挙げるランニングコストについても十分考えておかなければなりません。

- ソフトウェアの購入および保守
- ハードウェアおよびネットワークインフラストラクチャ
- 安全な設備
- ポリシー及び手順の作成と監査
- 証明書ライフサイクルの管理
- 常に利用可能な検証インフラストラクチャ (証明書失効リスト (CRL)/Online Certificate Status Protocol (OCSP))
- エンドユーザーサポート
- IT トレーニング
- バックアップおよび障害復旧
- ユーザー数、アプリケーション数の増加に対応する拡張性

無料ソフトウェア使用の是非

一部のサーバー OS が提供する無料の PKI 機能を利用すれば、 低コストな PKI ソリューションが実現できそうに思われるかもしれません。しかし実際は、見逃されがちな作業やインフラのためのコストが必要であり、無料ソフトウェアを利用したソリューションではあってもやはり費用がかさみます。

しかも、このような「自家製」タイプの PKI の場合、PKI のインフラを構築し、 それを組織のニーズに合わせてカスタマイズし、 それを維持していくために、組織に大きな負担がのしかかります。組織は、従来の IT 部門に任せればコストをかけずにこうしたことを行えると考えますが、オンプレミス PKI ソリューションを効果的に実現できるだけの専門技術を持った人材は、 社内にはなかなかいないものです。しかも、 継続的な PKI のサポートのために莫大な IT リソース

を投入できるよう準備しておく必要があります。監査ログの管理や CRL の作成などは、 片手間でできる作業ではありません。しっかりトレーニングを受けた専従の PKI 要員を配置するか、 もしくは費用をかけて外部のコンサルタントを雇う必要があります。こうした点をしっかり検討しなければ、 組織の「信頼の起点 (トラストアンカー)」が弱体化し、PKI の価値も失われることになりかねません。

マネージド型 PKI サービスとオンプレミス PKI の比較

一方、 必要に応じて PKI の機能が提供されるマネージド型の PKI サービスを利用することもできます。マネージド型のサービスを利用すれば、組織の負担は劇的に軽減されますし、拡張性や可用性も保証されます。ポリシーや運用プロセス、証明書管理なども、サービスプロバイダ側で処理してもらえます。

ビジネスの成長ニーズに合わせて拡張することも、 マネージド型サービスならば簡単です。オンプレミスのソリューションを拡張する場合、ソフトウェアを追加でインストールしたり、ハードウェアや、バックアップ、 障害復旧などのインフラを増やしたりしなければならなくなることがあります。コストも、 マネージド型 PKI サービスを使用して PKI を導入する方が、 オンプレミスソリューションを構築するよりもはるかに低く抑えられます。例として、 DigiCert PKI Platform とオンプレミス PKI サービスを比較してみましょう。PKI ソリューションの導入および使用に際して組織が負担しなければならないコストのうち、主な 3 つの項目、すなわちソフトウェア、インフラストラクチャ、および人件費について、見ていきたいと思います。

前提条件

以下のコスト分析は、対象期間を 3 年とし、初期費用は初年度に発生するものとします。金額はすべて米ドルであり、GSA Advantage (米国一般調達局 (GSA) が提供するオンライン取引サービス) が公開する価格に基づいています。専門的サービスの価格は、業界の同等サービスの平均価格に基づいています。証明書の枚数 (シート数) は 1,000 枚とします (企業の平均的な発行枚数です)[1]。

ソフトウェア

DigiCert PKI Platform の場合、PKI を本番環境に展開するためのセットアップ料金はかかりません。ただし、年に 1 度サービス料金が発生します。サービス料金には基本サポートが含まれます [2]。ライセンス料やメンテナンス費用はかかりません。オンプレミスの場合、組織はソフトウェアライセンス、メンテナンス、サポートの費用を負担することになります。

ソリューションを組織全体に展開する前に行われる試験的導入のコストや、障害復旧のコストも、計算に含まれています。DigiCert PKI Platform の場合、 障害復旧は認証局運用規定 (CPS) の中に含まれています。

以下の表からわかるように、 オンプレミスの場合、 ソフトウェアの購入や導入の費用が著しく高額となります。

1 このサンプル比較は、マネージド型 PKI サービスの導入の利点や、マネージド型 PKI サービス導入に伴う直接費 (顧客対応やソリューション関連費など) を、第三者的に評価するために作成したものです。財務や投資に関するアドバイスを行うことは意図していません。考慮すべき点を明らかにするための情報のみを提示しています。すべてのシナリオは説明を目的とした仮想的なものです。導入や投資に関する意思決定を、 このサンプル比較にのみ基づいて行うことはしないでください。明示または黙示を問わず、 いかなる表明も保証もいたしません。DigiCert 社は結果について保証できませんし、保証いたしません。

2 追加料金のお支払いでプレミアムサポートをご利用になれます。

digicert®

DigiCert PKI Platform	合計金額		オンプレミス PKI	合計金額	
	初期費用	経常費用		初期費用	経常費用
試験的導入/テスト			**試験的導入/テスト**		
年間マネージドサービス料金	$0	$0	登録機関	$15,065	該当なし
年間シート料金	$0	$0	デジタル ID	$1,188	該当なし
サポート	$0	$0	サポート	$0	該当なし
小計	**$0**	**$0**	**小計**	**$16,253**	**$0**
本稼働			**本稼働**		
年間マネージドサービス料金	該当なし	$17,000	登録機関	$30,130	該当なし
年間シート料金	該当なし	$26,250	デジタル ID	$95,000	該当なし
サポート	該当なし	$0	サポート	該当なし	$25,026
小計	**$0**	**$43,250**	**小計**	**$125,130**	**$25,026**
障害復旧			**障害復旧**		
年間マネージドサービス料金	$0	$0	登録機関	$0	$0
年間シート料金	$0	$0	デジタル ID	$0	$0
サポート	$0	$0	サポート	$0	$0
小計	**$0**	**$0**	**小計**	**$0**	**$0**
ソフトウェア合計	**$0**	**$43,250**	**ソフトウェア合計**	**$141,383**	**$25,026**

インフラストラクチャ

インフラストラクチャのコストは、オンプレミス側でしか発生しません。DigiCert PKI Platform を利用する場合、オンプレミスのインフラを追加する必要がないため、インフラの購入や保守のための費用がかからないだけでなく、IT 部門がそれらを設置し、管理するための手間も省けます。

以下の表に示したインフラコストはかなり控えめな数字です。また、非常に安全性の高い設備がすでに存在するという前提で計算されています。安全性が確保された建物やデータセンター、装置などがない場合、さらに資金を投入して設備のセキュリティレベルを高め、PKI システムを保護する必要があります。

DigiCert PKI Platform	合計金額		オンプレミス PKI	合計金額	
	初期費用	経常費用		初期費用	経常費用
ハードウェア			**ハードウェア**		
サーバー	該当なし	該当なし	サーバー (Dell)	$8,800	$1,760
ロードバランサー	該当なし	該当なし	ロードバランサー (Foundry)	$19,500	$3,900
暗号ハードウェア	該当なし	該当なし	暗号ハードウェア (SafeNet)	$26,200	$3,930
小計	**$0**	**$0**	**小計**	**$54,500**	**$9,590**
ソフトウェア			**ソフトウェア**		
オペレーティングシステムライセンス	該当なし	該当なし	オペレーティングシステムライセンス (Microsoft®)	$4,116	$823
認証、自動化、バックアップのライセンス	該当なし	該当なし	認証、自動化、バックアップのライセンス (複数ベンダー)	$4,600	$920
データベースサーバーライセンス	該当なし	該当なし	データベースサーバーライセンス (LDAP)	$2,000	$400
小計	**$0**	**$0**	**小計**	**$10,716**	**$2,143**
インフラストラクチャ合計	**$0**	**$0**	**インフラストラクチャ合計**	**$65,216**	**$11,733**

人件費

PKI は複雑なテクノロジであるため、 オンプレミスのソリューションを構築するには知識豊富な人材が必要になります。IT 部門のスタッフまたはコンサルタントが、 ソフトウェアとハードウェアのコンポーネントの導入、ポリシーと手順の作成と実施、証明書ライフサイクルの管理、障害復旧計画の作成などを行わなければなりません。

以下のコスト比較表では、 PKI ソリューションの導入と管理にかかる人件費を計算しています。DigiCert PKI Platform の場合、 サービスの利用管理を担当する非常勤の管理者が 1 名いればよく、 特にトレーニングも必要ありません。勤務時間はフルタイム従業員の 4 分の 1、 フルタイム従業員 1 人当たりの費用は年間 8 万ドルとして、 コストを計算しています。DigiCert PKI Platform の場合、 導入、インテグレーション、コンサルティングの費用はかかりません。

以下の表からわかるように、オンプレミスの場合は常に IT 部門に高い負荷がかかるため、経常費用が高くなり、それが人件費の大きな差となって表れています。

DigiCert PKI Platform	合計金額		オンプレミス PKI	合計金額	
	初期費用	経常費用		初期費用	経常費用
専門サービス			**専門サービス**		
導入 (初期設定)	該当なし	該当なし	導入 (初期設定)	$17,600	該当なし
インターネットセキュリティ コンサルティング (PKI ポリシー)	該当なし	該当なし	インターネットセキュリティ コンサルティング (PKI ポリシー)	$35,200	該当なし
システム管理 (PKI 管理者)	該当なし	$20,000	システム管理 (PKI 管理者)	該当なし	$52,000
小計	**$0**	**$20,000**	**小計**	**$52,800**	**$52,000**
トレーニング			**トレーニング**		
管理者コース	該当なし	該当なし	管理者コース	$5,000	該当なし
PKI 総合コース	該当なし	該当なし	セキュリティ管理者総合コース	$7,500	該当なし
ツールキットコース	該当なし	該当なし	Java™ 開発者向け セキュリティツールキット コース	$7,500	該当なし
小計	**$0**	**$0**	**小計**	**$20,000**	**$0**
人件費合計	**$0**	**$20,000**	**人件費合計**	**$72,800**	**$52,000**

結論

上記の 3 つの主要な項目をすべて合わせると、購入および導入の費用合計は、オンプレミスの場合 368,000 ドル以上、DigiCert PKI Platform の場合 63,000 ドルとなります。オンプレミスでは、DigiCert PKI Platform に比べて経常費用が 40 パーセント以上も高くなっています。両者のコストの大きな違いを生んだ主な要因は、ソフトウェアと人件費です。オンプレミスでは、3 年間の総額が 545,000 ドル以上に達し、年平均は約 182,000 ドルとなります。DigiCert PKI Platform では、3 年間の総額が 189,750 ドルですから、オンプレミスのほぼ 1 年分です。

DigiCert PKI Platform	合計金額		オンプレミス PKI	合計金額	
	初期費用	経常費用		初期費用	経常費用
ソフトウェア合計	$0	$43,250	ソフトウェア合計	$141,383	$25,026
インフラストラクチャ合計	$0	$0	インフラストラクチャ合計	$65,216	$11,733
人件費合計	$0	$20,000	人件費合計	$72,800	$52,000
総額	**$0**	**$63,250**	**総額**	**$279,399**	**$88,759**

DigiCert PKI Platform の利点

DigiCert PKI Platform は、認証、暗号化、デジタル署名のために使われる電子証明書の管理 (発行、失効、再発行、キーエスクロー、ステータス表示、 レポート実行) をすべて可能にするホステッド型のソリューションです。DigiCert PKI Platform を導入すれば、オンプレミス PKI の場合のようにコストをかけたり開発期間に縛られたりすることなく、 堅牢な PKI と CA システムを構築することができます。

主要な企業や官公庁、あるいはネットワークでつながっているコミュニティなどで、 DigiCert PKI Platform が選ばれていますが、 それは以下のような点が評価されているからです。

- **総所有コストの削減** PKI のための先行投資や、 IT 人件費の経常費用を、劇的に削減できます。
- **迅速な導入** 社員、顧客、ビジネスパートナー、Web サービスアプリケーション、ネットワークデバイスなどに対し、PKI を迅速に導入することができます。
- **シームレスな統合** カスタマイズの費用をかけることなく、多くの組織の既存のアーキテクチャに PKI サービスを統合することができます。
- **使いやすさ** DigiCert PKI Platform は導入が容易です。また、 大量の証明書を迅速かつ容易に管理することができます。エンドユーザーがそれを意識することはありません。
- **拡張性と信頼性** DigiCert 社が提供する信頼性の高いインフラストラクチャは、 数百万ユーザーにまで拡張可能であり、ビジネスニーズの増大に柔軟に対応します。
- **市場優位性** DigiCert 社の長年にわたる方針や慣行は、多くの業界で、 組織の規模にかかわらず、 その有効性が証明されています。DigiCert PKI Platform は、 Avaya® Inc.、CertiPath® LLC、米国教育省など、数千に及ぶ組織のオンラインデータやシステムやプロセスを、不正侵入や業務の混乱から保護しています。
- **信頼できるソリューション** DigiCert 社は商用 PKI プラットフォームの運用期間で世界一を誇り、これまでに発行された証明書は 2 億枚を超えます。

まとめ

マネージド型 PKI サービスを利用すると、 インフラや IT エンジニアなどに高いコストをかけずにすみます。そのため、 規制の遵守、 企業の機密データの保護、信頼できる方法による外部との通信を、コスト効率の良い方法で実現することができます。

DigiCert 社は、 あらゆる企業や官公庁、 信頼できるコミュニティなどに、 10 年以上にわたって信頼できる PKI サービスを提供しています。DigiCert PKI Platform は、オンプレミスのソリューションのような複雑さもなければ、負担やコストをかけることもなく、組織が必要とする高度な保護を実現します。セキュリティの構築に高いお金をかけるか、それともセキュリティを侵害されて高い代償を払うか、企業はもう迷う必要はありません。重要な商取引を行うすべての組織にとって、PKI の導入こそ、コスト効率の良いソリューションなのです。

digicert®

用語集

認証局 (CA)	公開鍵基盤 (PKI) の一部として、デジタル証明書の発行、失効、停止を行う権限を持つ、信頼できる機関。
証明書失効リスト (CRL)	有効期限より前に失効した証明書の一覧。CA により電子署名され、定期的に発行される。CRL には一般に、発行者名、発行日、次回発行日、失効証明書のシリアル番号、失効日時および理由が記載される。
認証局運用規定 (CPS)	CA または登録局 (RA) が証明書を発行する際の慣行について示した文書。CA によって必要に応じて改訂が行われる。
クレデンシャル	個人または実体の身元をデジタル的に表すフォームファクタ。その個人または実体に対して要求または実行される認証のレベルに基づき、信頼できる機関 (CA など) が発行する。デジタル証明書はフォームファクタの一種であり、他のフォームファクタ (トークンやハードウェアセキュリティモジュールなど) と組み合わせて使用される場合もある。
デジタル証明書	公開鍵と秘密鍵のペアに基づく、X.509 ファイル。このファイルによって、公開鍵が個人または実体の身元に結び付けられる。デジタル証明書は、認証、暗号化、デジタル署名を目的として使用される。
デジタル署名	信頼できる安全な形式の電子的署名。ユーザーの身元の検証、文書の完全性、タイムスタンプ、署名された電子的文書の否認防止などを可能にする。
鍵生成	公開鍵と秘密鍵の生成、文書化、保存の、信頼できるプロセス。
秘密鍵	所有者が秘密で保持する、数学的な鍵。デジタル署名の生成や、対応する公開鍵で暗号化されたメッセージやファイルの復号に使用される。

詳細情報

デジサート・ジャパン合同会社

〒 104-0061
東京都中央区銀座 6 丁目 10 番地 1 号
GINZA SIX 8 階
https://www.digicert.co.jp
03-4560-3900
JPN-DIV-MPKI@digicert.com