DigiCert PKI Platform（公開鍵基盤）とは

ビジネスアプリケーションの安全性を確保する

本書の対象読者

企業がビジネスに不可欠なアプリケーションをインターネット上で運用するには、公開鍵基盤(PKI) によって証明書ベースの高度なセキュリティが必要です。このホワイトペーパーでは、あらゆる規模の企業が迅速、確実にPKIサービスを導入できるように支援するDigiCertが提供するDigiCert PKI Platformをご紹介します。

digicert®

目次

エグゼクティブサマリー

企業がビジネスに不可欠なアプリケーションをインターネット上で運用するには、公開鍵基盤 (PKI) によって証明書ベースの高度なセキュリティが必要です。PKIは、最高レベルのセキュリティが必要なアプリケーションを保護し、オンラインバンキング/トレーディング、ウェブサービスベースのビジネスプロセスの自動化、電子署名、および電子商取引を可能にします。さらに、ファイアウォール、仮想プライベートネットワーク（VPN）、ディレクトリ、エンタープライズアプリケーションも保護します。PKIに求められるものは、包括的な機能、社内外のアプリケーションへの容易な統合、数百万のユーザにも対応できる拡張性、24時間365日の完全な運用、軍事レベルの物理的セキュリティの確保です。さらに、企業がパートナ、顧客、サプライヤとの間で信頼のコミュニティを容易に構築できるよう支援することも求められます。

こうした重要な機能をPKIで実現しようとする場合、企業は社内にPKIソフトウェアを導入するか、信頼できるプロバイダにPKIサービスをアウトソースするかを選択する必要があります。社内での導入には、独自開発のソフトウェア、物理的セキュリティの制限、冗長性の不足などのさまざまな欠点が存在し、PKIの実装が失敗に終わってしまうことも少なくありません。これに対し、アウトソース型（クラウド型）のPKIサービスは、TCO（総所有コスト）の削減、迅速な導入、リスクの緩和といった多くの利点があります。

DigiCert PKI Platformは、あらゆる規模の企業が迅速かつ確実にPKIサービスを導入できるように支援する、DigiCertが提供するクラウド型ソリューションです。このソリューションを採用することで、企業は電子証明書の発行、一時停止、失効を社内で制御しながら、PKIの計画、構築、保守の負担を軽減できます。また、DigiCert PKI Platformを利用すると、企業は貴重なデータを安全にオンラインで通信が可能になるため、コストを削減し、プロセスを効率化し、パートナ、顧客、サプライヤとの関係を強化できます。

情報資産の保護

金融機関、メーカー、政府機関、医療機関およびその他の企業が、インターネットを活用してビジネスプロセスをつなぎ、通信を効率化して取引を行うなかで、オンラインでのデータ交換時における情報資産の保護は欠かせない要素となっていますが、複雑さも増しています。企業は機密情報を保護し、オンライン取引を行うパートナからの信頼を維持しつつ、オンラインデータに関する政府や業界の法規制を遵守する必要があります。

その一方で、ウイルスの配布方法が進化し、ハッカーの攻撃が高度化しているほか、無線通信などの技術的進歩によって並列的な環境を同時に保護しなければなくなりました。企業の情報資産の保護に関するセキュリティに期待されているものは、データ保護やネットワーク分離といったゲートキーパ的な機能だけではなく、外部アプリケーションへの企業データの連携、ユーザ同士を結び付けることによるコラボレーションの拡大、オンライン取引やオンライン通信の実現といったビジネスを促進する上で必要なセキュリティ機能にも及んでいます。

エンタープライズPKIの導入

このような多面的な環境でアプリケーションとネットワークのセキュリティを実現する基盤がPKIです。PKIは証明書ベースの公開鍵暗号システムの実装と運用をサポートする技術、基盤、業務運用を指します。このシステムは、数学的な関連性を持つ鍵のペア（秘密鍵と公開鍵）を使用して、機密情報の暗号化や復号、電子署名の生成や検証を行います。（電子署名は、トランザクションへの署名やリソースへのアクセス権を付与するユーザ/マシンの認証に使用されます。）PKIの主な機能は、必要としているユーザやアプリケーションに公開鍵を正確かつ確実に配布することです。このプロセスには、エンタープライズ認証局（CA）によってユーザまたはアプリケーションに発行される電子証明書が使用されます。証明書の発行にはユーザの本人確認が必要であり、これは通常、登録局（RA）によって行われます。

digicert®

エンタープライズPKIは次のような仕組みを用いて、電子証明書で情報資産を保護します。

- **認証** - コンピュータとユーザの識別情報を確認します。
- **暗号化** - データを暗号化して不正なユーザやコンピュータが情報を表示できないようにします。
- **電子署名** - 手書きの署名に代わる電子署名を提供します。企業は電子署名を利用してデータの整合性を検証し、送信中にデータの改ざんがあったかどうか判断します。
- **アクセスコントロール** - ユーザまたはアプリケーションがどの情報にアクセスできるか、およびユーザまたはアプリケーションが別のアプリケーションにアクセスした後にどの操作を実行できるかを決定します。これは承認とも呼ばれます。
- **否認防止** - 通信、データ交換、および取引が法的に有効であり、取消不能であることを保証します。

エンタープライズPKIの運用における重要な要素

企業がPKIソリューションを選択する際には、PKIの技術、基盤、業務運用に関する次の要素を検討する必要があります。

- **PKIの機能**。強力なセキュリティ、容易な管理運用、証明書管理の実践的な制御を実現するには、エンタープライズPKIがモジュラー設計に基づいている必要があります。このモジュラー設計に含まれる要素には、証明書の発行/ライフサイクル管理に対し確実かつ高度なサポート、多様な証明書タイプに対応できるプロトコル/処理能力、包括的な管理機能、記録の保存、ディレクトリの統合、および鍵管理があります。
- **統合の容易さ**。コストを最小限に抑えて、既存の投資を活用し、多様な環境で互換性を保証するために、企業は新旧を問わずすべてのサポート対象アプリケーションと容易に統合できるPKIを選択する必要があります。独自開発のPKIデスクトップソフトウェアしか使用できないようなPKIは、望ましくありません。また、社内のIT部門だけでなく、パートナー、サプライヤー、顧客のさまざまなデスクトップポリシーにも対応できる必要があります。
- **可用性と拡張性**。ユーザコミュニティが24時間いつでも、PKIを使用できる必要があります。また、企業の成長に合わせ、必要に応じて数百万のユーザにも対応できる拡張性が必要です。
- **セキュリティとリスク管理**。インターネットベースのPKIを運用している企業が、信頼を維持し、金銭的/法的責任を最小化するためには、PKI基盤や秘密鍵といった重要な資産を、ネットワーク経由の攻撃から守るだけではなく、これら資産を保管している物理的施設への脅威からも守る必要もあります。
- **専門知識**。企業がPKIを適切かつ確実に導入、保守、保護するためには、PKIに関して広範囲に渡って訓練されたセキュリティ専門家を雇用する必要があります。
- **対応範囲**。PKIに投資する企業が、ROI（投資収益率）を最大化し、コラボレーションを促し、ビジネスに柔軟に対応するためには、イントラネット、エクストラネット、インスタントメッセージング、ウェブサービスネットワーク、インターネット、VPNなど、関連するコミュニティ全体にわたってソリューションを容易に運用できる必要があります。

選択したPKIの導入モデルによって大きな影響を受けるこれらの要因は、エンタープライズPKI導入の成否を左右します。また、企業の重要なデータの交換に関する短期的な計画および長期的な計画にも影響を及ぼします。

PKI導入の2つのモデル

PKIを導入する際には、企業はインハウス型でPKIソフトウェアを購入して社内に導入するか、クラウド型でPKIプラットフォームを外部にアウトソースするかを選択する必要があります。2つのアプローチは、前述のような課題への対応力が異なることに加えて、TCO、実装時間、成功の可能性、運用スタッフ、リスクの程度、ブランド力といった点でも異なります。

インハウス型PKIソフトウェアの導入

インハウス型で社内にPKIを導入する場合、企業はPKIソフトウェアを購入して、PKIサービスを自社で構築します。このシナリオでは、企業はPKI自体に加えて、関連するすべての技術（システム、通信、データベースなど）のプロビジョニング、導入、保守にも100%責任を負います。また、安全な施設を準備する責任もあります。安全な施設に求められるものは、施設内の物理的セキュリティ、安全にインターネットを利用できるネットワーク構成、冗長化システム、災害復旧機能、PKIに関する実効性のある法的対応、財務的な責任への対策、高度に訓練された運用スタッフなどです。これらの要素が1つでも欠けると、企業の信頼が損なわれる可能性があります。

社内で導入したPKIが重要な成功要因に対応できるか否かに関わらず、実証されていないPKIに対する不安や、その企業自体の知名度の低さによって、パートナー、顧客、サプライヤーがPKI対応サービスの採用をためらう可能性もあります。さらに、否認防止機能（第三者によるトランザクションの監査/実証機能）が存在しない場合には、PKIの価値がさらに損なわれます。また、社内でのPKIの計画、購入、実装、導入、テストといったプロセスに何か月もかかる場合があるため、戦略的なビジネスイニシアティブの展開や既存投資の回収に時間がかかります。

クラウド型PKIプラットフォームのアウトソース

クラウド型でPKIを導入する場合、企業はPKIの構築、導入、保守といった作業を、信頼できるサードパーティにアウトソースし、証明書の処理、ルート鍵の保護、セキュリティおよびリスクの管理といったサービスを受けます。

PKIプラットフォームを提供するプロバイダにとっては、PKIこそがビジネスの中核であるため、大半の企業よりもはるかに多くの割合のリソースを、最先端のPKI技術やセキュリティ、トレーニングに注ぎ込むことができます。さらに、セキュリティプラクティス、手順、基盤も、長い時間をかけて検証されています。このため、迅速な導入が可能になるとともに、最高レベルの可用性とセキュリティを保ちつつPKIを確実に運用できます。

また、クラウド型サービスの課金は、電子証明書を発行するシート数、発行レート、またはその両方によるので、企業はコストをより正確に予測し、ビジネスの拡大に合わせてPKI機能をシンプルに追加できます。クラウド型PKIは、ユーザ認証や証明書ライフサイクル管理に関するセキュリティポリシーを、企業が制御および実行できるという点が重要なポイントです。

DigiCertからのご提案

DigiCertは、企業と個人が複雑化したグローバルネットワーク上で情報を発見、接続、セキュリティの確保、取引することを可能にするインフラストラクチャを運用しています。DigiCertはインターネットセキュリティとPKIの業界リーダーとして、あらゆる規模の企業に対応できる、最先端の統合PKIサービスプラットフォームをご提供しています。DigiCert PKI Platformの設計とサポート対応の基になっているのは、これまでの世界における実績です。企業はDigiCertの専門知識とインフラストラクチャを活用することで、証明書の発行、更新、失効などの証明書ライフサイクル管理全体を制御しながら、自社のインフラの構築、導入、保守などの負担を軽減できます。また、ウェブサービス、オンラインでのデータのやり取り、既存のアプリケーションなどの安全性を素早く確保し、投資を早期に回収し、進化するビジネス戦略に迅速に対応できます。

digicert®

DigiCert PKI Platformは、PKI導入の成功に求められる要素を網羅したうえで、次のようなメリットを提供します。

- **TCO（総所有コスト）の削減**。DigiCertは、PKIプラットフォームの構築、保守、更新、安全性確保、外部監査、および運用スタッフ配置に数百万ドルを投じています。DigiCert PKI Platformを活用することで、企業は、安全な施設、インフラストラクチャの整備、スタッフ配置にかかるコストを大幅に削減できます。実際に、社内PKIシステムTCOは、社内で準備するソフトウェアコストがゼロだったとしても、DigiCertにアウトソースした場合よりも高くなります。[1]
- **迅速な導入**。プラットフォーム、ポリシー、および手順が既に揃っているため、DigiCert PKI Platformは、従来のソフトウェアベースのインハウス型PKIに比べると3分の1以下の時間で実装できます。
- **確立された基盤**。DigiCert PKI Platformは、確立されたバックエンドインフラストラクチャに基づいているため、導入を確実に成功させることができます。
- **運用スタッフへの影響が最小限**。PKIの運用とメンテナンスは、DigiCertのセキュリティ専門家が担当するため、社内のITリソースは中核的なビジネスに集中できます。
- **強力なセキュリティ**。DigiCertはミリタリーグレードのセキュリティを誇る施設と業界をリードする認証業務により、最高レベルのセキュリティを保証します。
- **ブランド力**。DigiCertという広く知られた信頼のブランドを活用することで、企業はサプライヤー、パートナー、顧客の信頼をより簡単に得られます。

次の表は、インハウス型PKIとクラウド型PKI（DigiCert PKI Platform）の基本的な違いをまとめています。

エンタープライズPKIの要素

エンタープライズPKIへのDigiCertのアプローチが、インハウス型（自社構築型）のアプローチと異なる点は、ポリシーの制御や日常的な意思決定は企業が行いつつ、DigiCertがバックエンドの処理作業を行う点です。DigiCertのアプローチの優位性を説明するために、次のセクションではこれまでに取り上げた重要な成功要因（機能、統合の容易さ、可用性と拡張性、セキュリティとリスク管理、運用スタッフ、対応範囲）の観点から、PKIソリューション全体を検討します。

成功の要因	PKIの機能	インハウス型PKIソフトウェア
PKIの機能	世界最大規模の、24 時間365 日稼働のPKI サービスセンタで提供される、十分な機能を備えたPKI。数百の企業にサービスを提供してきた長年の運用実績。	企業がサポート基盤を設計、構築、導入し、実装や運用の負担をすべて担う。ソフトウェアベンダーにはPKIの運用経験がない。
統合の容易さ	広く普及しているウェブブラウザ、電子メールクライアント、企業向けアプリケーションなど、標準アプリケーションをすべてサポート。	すべてのユーザやアプリケーションに対応させるためには独自のクライアントソフトが必要。

1 -「Symantec Managed PKIサービスによる複雑さの解消と総所有コストを削減」、DigiCert、2018年

成功の要因	PKIの機能	インハウス型PKIソフトウェア
可用性と拡張性	PKIバックボーンサービスと災害復旧機能は、契約を通じて保証されます。オンデマンドの拡張性。耐障害性に優れた高キャパシティの基盤を活用。	基盤、災害復旧といったサービスすべてを企業側が準備。運用リスクを企業が全面的に引き受ける。冗長性の確保が難しく 拡張性には制限がある。
セキュリティとリスク管理	PKI バックボーンサービスと災害復旧機能は、契約を通じて保証。業界をリードする、熟練した鍵管理/証明書プラクティス。外部監査を実施。	企業側がセキュリティ基盤をすべて準備し、自社の運用ポリシーやプラクティスを設計し、リスクを全面的に引き受ける。
運用スタッフ	厳しい審査と高度な訓練を受けたセキュリティ専門家。セキュリティとPKIに関する最新の知識とスキルを維持している。	スタッフはトレーニングを受けるとともに、進化する技術、標準、およびリスクに対応するべくスキルを磨き続けることが必要。経験不足は導入を遅らせ、ダウンタイムを引き起こし、セキュリティギャップをもたらす。
対応範囲	認証局のグローバルネットワーク。企業はプライベートまたはパブリックの信頼ネットワーク（世界最大）を選択可能。	プライベートの相互認証のみ。企業はその都度カスタムソリューションを100%構築。パートナーがリスクを全面的に引き受ける。

DigiCert PKI Platformの機能

PKIの中核となるのは、CA（認証局）およびRA（登録局）機能、発行申請プロセス、証明書の更新とステータス確認サービス、ディレクトリとアプリケーションインターフェイス、秘密鍵の管理などを実装するソフトウェアとハードウェアです。この技術では、堅牢なセキュリティ、高い可用性、および複数のアプリケーションインターフェイスをサポートする必要があります。最も重要な要件は、PKIがモジュール型の設計であることです。これにより、企業の施設と、サポートを行うセキュアなデータセンタとの間で、PKI機能を分けることができます。

DigiCert PKI Platformのベースとなっているが管理する信頼ネットワークアーキテクチャは、堅牢で包括的です。世界の企業、商用認証局、ウェブサイトが求めるPKIサービスセンタのニーズをサポートし、セキュリティ、商取引、法律、およびベストプラクティスに関する最も厳しい要件を満たしています。

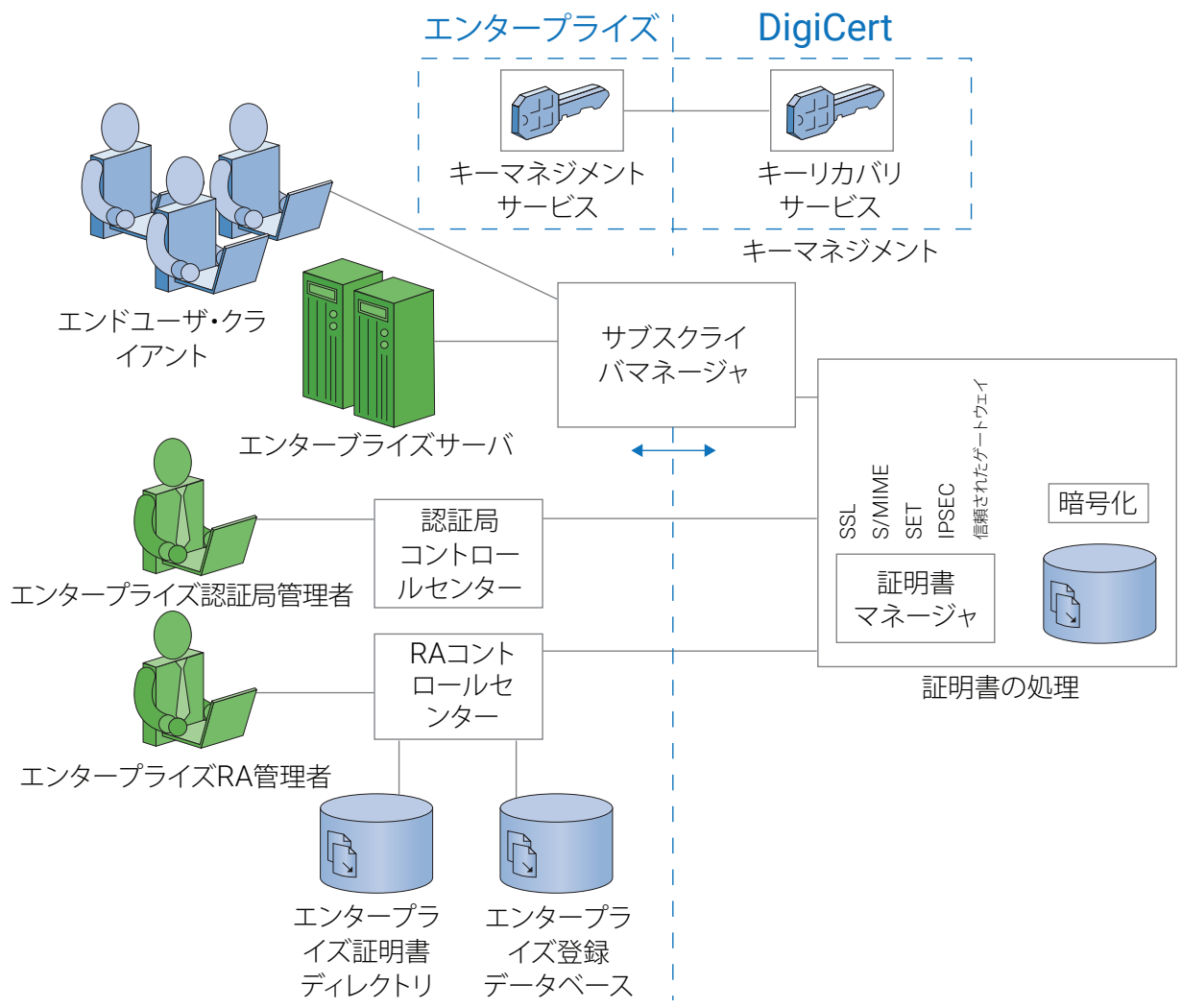

図1: DigiCertのPKIアーキテクチャ

信頼ネットワークのアーキテクチャは、次のモジュールファミリーで構成されています。

- **エンドユーザ登録ページ** - エンドユーザ登録と証明書の更新などのエンドユーザサービスを提供するローカライズ可能でブランド登録可能な登録ページです。
- **DigiCert PKI Platform Control Center** - 証明書の発行承認、失効の承認、一般管理機能などの社内の証明書管理機能を提供します。完全に自動化することができます。
- **認証局コントロールセンター** - 企業が証明書のコンテンツルールや管理権限などのローカル認証局ポリシーを確立できるようにします。
- **証明書処理** - 証明書の発行、証明書ライフサイクルの遵守およびプロトコルのサポート、オンライン証明書ステータスプロトコル（OCSP）、暗号鍵管理、記録の保管、その他の中核的機能などのプレミアム検証サービスが含まれます。
- **証明書マネージャ** - 企業がSSL、S/MIME、IPSec、または他の標準X.509証明書などの発行する証明書のタイプを選択できるようにします。
- **鍵管理サービス** - ユーザ鍵ペアに対して最高レベルのセキュリティで生成、バックアップ、および回復を提供し、デュアルキー（単一のアプリケーション内に別個の鍵ペア）をサポートしています。
- **エンタープライズ統合** - 証明書の自動発行やその他の管理機能、企業ディレクトリやデータベースへの証明書の自動送信、エンタープライズウェブサーバーによる証明書の失効情報へのアクセスをサポートするエンタープライズデータベースへのインターフェイスを提供します。
- **アプリケーション統合ツールキット** - 商用アプリケーションベンダーおよび企業がPKI対応アプリケーションを使用できるようにします。

統合の容易さ

PKI導入における最大の課題の1つが、社内外のアプリケーションをPKIに対応させることです。PKIベンダーが採用しているアーキテクチャが、独自開発か標準ベースかどうかが統合の容易さとコストに影響を与えます。

- **独自開発**。独自開発のPKIソフトウェアはすべてのデスクトップにインストールされます。PKIを使用するアプリケーションは、PKIベンダーの独自開発のソフトウェアインターフェイスを必要とするため、イントラネットの他の領域やパートナー、顧客、サプライヤーに対するアプリケーション拡張は多大なコストがかかる複雑なタスクになり、通常は実行できません。また、アプリケーションをアップグレードすると、既存のPKIと互換性がなくなることがあります。
- **標準ベース**。標準ベースのPKIでは、アプリケーションとPKIのインターフェイスには、業界標準のインターフェイスプロトコルが使用されるか、またはPKIアプリケーションベンダーとのパートナーシップによって実現された標準ベースのカスタムインターフェイスが使用されます。独自開発のPKIソフトウェアをデスクトップにインストールする必要はありません。DigiCertでは標準ベースのPKIアプローチを採用し、100社を超える独立系ソフトウェアベンダーと協力して、DigiCert PKI Platform向けの組み込みサポートを提供しています。アプリケーションは、ベンダーから出荷される時点でPKIに対応しています。ほぼすべてのアプリケーションとシームレスに動作できるように、DigiCert PKI Platformには使いやすいアプリケーションプログラミングインターフェイス（API）も含まれており、お客様が作成したアプリケーションをPKI対応にすることができます。

可用性と拡張性

ミッションクリティカルなアプリケーションをサポートするPKIは、24時間体制の可用性が必要であり、多数のユーザやアプリケーションをサポートできるよう、スムーズな拡張性も求められます。

可用性

継続的な可用性を確保するために、DigiCert PKI Platformの基盤は完全に冗長化されており、すべての重要コンポーネントに24時間365日のサービスレベルを保証します。離れた場所にあるバックアップ用の災害復旧サイトは、24時間365日、稼働しています。これに対してインハウス型のPKI製品は、冗長性を実現できる設計ではないことが多いため、予期しないダウンタイムが生じやすくなります。さらに、離れた安全な場所でのバックアップを手配しない限り、災害復旧機能が限定的になる場合があります。

拡張性

DigiCertによる電子証明書の発行は実世界で実証されており、数百から数百万のユーザに対応できるスムーズな拡張性を備えています。インハウス型のPKIソフトウェアは、トランザクションに最適化されたアーキテクチャではなく、データベースやディレクトリシステムの拡張性と回復性も限られているため、ユーザが数万人に達すると拡張性の限界が来ることがわかっています。

セキュリティとリスク管理

PKIを導入する企業が主に目指しているものは、ルート秘密鍵の保護、および継続的サービスの提供です。強力なセキュリティと24時間365日の可用性を確保するには、隙のない物理的セキュリティと、確実な認証業務が必要です。しかし、物理的セキュリティがPKI導入費用に占める割合は非常に大きく、また認証業務を十分に計画するには、セキュリティおよびリスク管理のアプローチを入念に考慮する必要があります。

DigiCertはセキュリティ技術に多大な投資を行い、業界をリードする認証業務運用規程（CPS）を策定することで、インハウス型でPKIを運用している企業よりも高いセキュリティレベルを保証します。DigiCert PKI Platformを活用することで、企業はコストを削減できるだけでなく、高いセキュリティと可能性を備えた施設の構築/運営というリスクを緩和できます。

物理的セキュリティ

ソフトウェアベースの暗号の実装は改ざんまたは誤用を招きやすいため、ビジネスに不可欠なアプリケーションをサポートするCAには、証明書の署名にハードウェアの暗号化モジュールを使用することが求められています。さらに、複数のCAをリンクさせるための基盤となるルート鍵には、特別な保管が必要です。その秘密鍵はオフラインの安全なハードウェアに保管し、署名時の鍵の有効化には複数の運用スタッフを関与させ、すべてのプロセスを厳密に制御および監査する必要があります。鍵の保護に特別な手法を用いるほかにも、重要なPKI機能を持った施設には、外部から侵入できないようにすることも必須です。さらに、電源や冷暖房空調設備（HVAC）を冗長化したり、熱や水による損傷を防ぐために特別な消防システムを導入したりする必要もあります。

DigiCertでは重要なPKI機能を、DigiCertや関連会社が24時間365日体制で運用するセキュアデータセンターに配置しています。最高水準のセキュリティと可用性を確保するために、DigiCert PKI Platformを通じて実装されるすべてのPKIでは、ハードウェアベースの暗号化、身元確認を行い高度なトレーニングを受けたスタッフ、ミリタリーグレードのセキュリティを誇る施設、厳格に監査された手続き管理システムを採用しており、24時間のサービスレベルがサポートされます。

digicert®

業務運用のサポート

企業が否認防止を保証してパートナー、カスタマー、サプライヤーの信頼を獲得するためには、PKIの管理、日常的な運用、記録の保存に関するプロセスを、十分に定義および監査する必要があります。これは特に、企業がPKIベースの電子署名を用いて、電子商取引や文書などの情報に電子署名している場合に重要です。この場合、トランザクションに確実に法的拘束力を持たせるためには、健全な業務運用と第三者により監査されたプロセスが不可欠です。

DigiCertは、最も厳しい業界標準に対応し監査を受けたビジネスプロセスを備えているPKI業務運用の開発における世界的リーダーです。DigiCertの認証業務運用規程（CPS）には、パブリックCAサービスの基盤となる業務運用について記載してあります。この規程は、同種の文書の中で最も包括的であると認められており、PKI業務運用の基盤として世界で活用されています。

DigiCertの業務運用には、証明や監査の対象となるCA鍵確立/管理プロセスと、複数の関係者によるすべての鍵マテリアルの厳格な制御が含まれています DigiCertは、WebTrust™ for CAおよびISAE3402/SSAE16という既存のセキュリティガイドラインに関して第三者によるセキュリティ監査を毎年受けています。また、米国国防総省の定義するポリシーおよび手順に即して証明書を発行していることが承認されています。DigiCertのプロセスが米国公認会計士協会（AICPA）のISAE3402/SSAE16に準拠していることは、KPMG®により認定されています。

専門の運用スタッフ

PKI導入の適切な計画、実装、保守には、高度なトレーニングを受け、実務経験を有するスタッフが必要です。企業が社内でPKIを導入するためにセキュリティチームを編成する場合、開発スタッフやITスタッフに専門外の業務をさせるか、当該業務に関するトレーニングを既存スタッフに受けさせるか、新たな人材を雇用する必要があります。PKIの導入後には、急速に変化するセキュリティトレンドや技術に対応するべく、継続的なスタッフへのトレーニングが欠かせません。全体的な経験不足や、個別の技術に対する知識不足、実証されていないセキュリティポリシーなどがあると、社内での導入が遅れたり、予期しないダウンタイムが生じたり、セキュリティが損なわれる恐れがあります。

豊富な経験を有するDigiCertのセキュリティ専門家にPKI導入をアウトソースすることで、企業は人件費を最小限に抑え、リスクを緩和し、導入を迅速化できます。インターネットの信頼サービスを提供する大手プロバイダとして、DigiCertは、PKIの開発、実装、保守に関する広範な経験を有しています。DigiCert PKI Platformチームは、セキュリティとPKI分野に専念しており、最先端の技術やセキュリティプラクティスに対応できるよう常にスキルの更新を図っています。

対応範囲

PKIは、特定のパートナーを含む企業のエクストラネットから、複数の企業にわたる業界固有のウェブサービスネットワーク、あらゆるユーザを受け入れるグローバルコミュニティ（インスタントメッセージングなど）に至るまで、いかなる規模のコミュニティにも対応できます。DigiCertの広範なコミュニティの実現と相互認証により、イントラネットを越えてコミュニティを容易に開発できるようになります。

幅広いコミュニティの実現

非公開のプライベートPKIを希望する企業もありますが、市販のウェブブラウザや他のデスクトップアプリケーションが、購入時の設定のままで自社の証明書を認識および信頼できるようにしたいと考える企業もあります。これが実現すれば、PKI運用企業の管理下にない組織のデスクトップシステムに、特別なソフトウェアをインストールまたは構成する必要がなくなるため、幅広いPKIコミュニティの確立が非常に容易になります。DigiCert PKI Platformによって企業は、分離されたプライベートPKIか、コミュニティまたは業界全体にわたるPKI、あるいは信頼されたネットワークにリンクされたPKIを構築できます。DigiCertと各国の関連会社が運用する信頼ネットワークは、グローバルな相互認証PKIです。信頼ネットワークのルート鍵は、Microsoft®およびMozillaクライアントを含む主要な市販デスクトップ製品すべてに事前にインストールされているため、製品のユーザはPKIで発行された証明書をすぐに認識できます。インハウス型PKIを導入した場合、クロスルート証明書やルート鍵を手作業で交換およびインストールする必要があるため、コミュニティの構築に大変な手間がかかります。

digicert®

相互認証

相互認証は、ある認証局が別の認証局のために証明書を発行するプロセスであり、複数の企業にわたるPKIコミュニティを証明書チェーンによってリンクできるようにします。相互認証に必要となる手順は、証明書の発行だけではありません。相互認証は特別なビジネスの取り決めであり、セキュリティプラクティスや法的責任の分担といった課題についての合意も含まれます。DigiCertは、複数の企業にわたる相互認証を行う認証局構造を多数構築しており、世界中の金融機関や商用認証局などの組織グループをリンクさせています。DigiCert PKI Platformは米国連邦ブリッジ認証局（FBCA）によって認可され、政府機関が安全に情報をやり取りできるようにしています。企業はDigiCertのソリューションを採用することで、あらゆる関係者のセキュリティ要件に対応する、相互認証プラクティスや合意を確立し、統合できるようになります。インハウス型PKIソフトウェアの場合、企業は自社で相互認証プロセスを開発し、実行する必要があります。

特徴のまとめ

DigiCertは、PKIサービスプラットフォームのコンセプトに基づいた完全なエンタープライズPKIソリューションを提供する数少ないベンダーです。

DigiCertソリューションの主な特徴は以下のとおりです。

PKIコンポーネント	DigiCertのアプローチ
PKIの機能	
証明書の署名用の暗号化ハードウェア	すべての認証局はハードウェア暗号化を使用し、FIPS 140-1レベル3を取得（ソフトウェア暗号化に固有の認証局秘密鍵の改ざんと漏洩のリスクを回避）
ルート鍵の保護	ルート鍵を常にネットワークから隔離された安全な施設内に保存。厳しく統制され、監査されたシークレットシェアリングによるアクティブ化（オンラインの運用環境にルート秘密鍵を保存している場合に生じる、侵入者/管理者による機密情報の漏洩および侵入のリスクを回避）
ユーザ鍵の管理	ユーザ暗号鍵を企業でバックアップ。過去の鍵をすべて保存。分散キーリカバリー技術による強力な保護
デュアル鍵サポート	あらゆるアプリケーションでシングルキーまたはデュアル鍵ペアをサポート（アプリケーションの要件と機能に依存）
失効	証明書失効リストを定期的に発行。ウェブサーバや標準ブラウザで失効を有効化。OCSPをサポート

PKIコンポーネント	DigiCertのアプローチ
統合の容易さ	
標準ベースのPKIと独自開発のPKI	標準ベースのPKI。デスクトップ上に独自開発ソフトウェアは不要。100社以上の独立系ソフトウェアベンダーパートナー。120件以上のアプリケーションに対応
ディレクトリ/データベース技術	企業がLDAP、X.500、SQLまたはレガシーDBMSから選択可能。ディレクトリスキーマの制限なし
可用性と拡張性	
冗長性	24時間365日のサービスレベル、冗長サーバ、データベース、ISP、通信を保証
災害復旧	リモートのセキュアサイトで24時間365日体制の災害復旧バックアップを保証
セキュリティとリスク管理	
施設のセキュリティ	防備を強化した建物、5層のセキュリティ。二重の生体認証によるアクセスコントロール、24時間体制の監視、動作探知、ネットワークセキュリティ監査
スタッフのセキュリティ	調査目的の審査、スペシャリストトレーニング、再トレーニングを実施
第三者による監査	KPMG®による独立SOC2/SOC3監査
業務運用のサポート	企業認証局、確かな業務運用が実証されている信頼のネットワークに参加するか、自社の業務運用を確立することが可能。DigiCertでは、業務運用のコンサルティングやCPSを提供
否認防止	評価/監査を受けた暗号化マテリアル管理および保安全な記録の保存により、紛争解決時に第三者による検証が可能な証拠を提供
専門知識	
専任スタッフ	厳しい身元確認と高度な訓練を受けたセキュリティ専門家がセキュリティとPKIに専念
最先端のスキル	教育や継続的なスキル更新によって、最新の技術知識を維持
対応範囲	
グローバルコミュニティの実現	市販のウェブ/メールクライアントすべてにルートが事前にインストールされているため、PKI 構造に参加可能
相互認証	企業のPKI Platform認証局と確立済みの信頼ネットワークやプライベートネットワークで相互認証が可能。プライベートなMozilla®またはMicrosoft®認証サーバの相互認証も可能。相互認証には業務運用の確立のサポートなどあらゆる段階が含まれる

digicert®

結論

インターネットセキュリティの役割が進化し、ゲートキーパ機能とネットワーク促進のための機能が求められているなかで、情報資産の保護は複雑化し、コストも増加しています。このような動的な環境でアプリケーションとネットワークのセキュリティを実現する基盤が、PKIです。PKIの導入を成功させるには、最先端の技術、細やかな認証業務、高度なトレーニングを受けた運用スタッフが必須であるため、自社でPKIを構築および導入する場合は膨大な時間と費用を投じる必要があります。また、企業がインハウス型PKIで、PKIとセキュリティに専念するサービスプロバイダと同レベルのセキュリティを実現するのは容易ではありません。

DigiCert PKI Platformは、企業のPKIの構築、導入、保守にかかる負担とリスクを軽減し、企業がセキュリティ上重要な電子証明書の発行、一時停止、失効を制御できるクラウド型のソリューションです。業界をリードするDigiCertの技術と専門知識、包括的な認証業務運用規程を活用することで、企業はコストを削減し、導入時間を短縮し、セキュリティを強化するのみならず、DigiCertのブランド力でパートナー、顧客、サプライヤーとの関係を強化することが可能です。

詳細情報

製品に関するお問い合わせ:

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

UID: 002/05/2018