デジタル証明書がモバイルデバイス管理にとって不可欠である理由

本書の概要

このホワイトペーパーは、急速に進化しているモバイルワーカーの管理の課題である認証セキュリティ関連のニーズを調査したものです。詳細な議論とユースケースの検証を通じて、デジタル証明書が企業にとって多様な種類のモバイルデバイス向けの最も優れたセキュリティクレデンシャルであることを明らかにします。また、モバイルデバイス管理ソリューションが導入されているケースを示すほか、デジタル証明書を管理するためのクラス最高のソリューションとしてDigiCert PKI Platformを紹介します。

digicert®

目次

はじめに

企業のITにとってモバイルデバイスが欠かせないことに疑いの余地はありません。スマートフォン、タブレットやその他のモバイルデバイスが使いやすいサイズになり機能が進化を続けているため、多くの企業ではこれらの使いやすいデバイスでデスクトップPCやラップトップPCを置き換えようとしています。しかし、進化のペースがあまりにも速いため、IT部門にとって管理しにくいものとなっているほか、セキュリティの脆弱性を悪用し、個人情報を盗み出し、被害者になりすまそうとする攻撃者にとって格好の標的となっています。

今や企業は、社内のファイアウォールの内側に閉じ込められたデスクトップPCに限定されなくなっているため、モバイルデバイス上にあるデータやアプリケーションとデバイスの持ち主であるエンドユーザーを信頼できるようにすることが企業にとって不可欠となっています。

モバイル環境を管理し信頼性を高める

デスクトップの全盛時代には、IT部門は標準的なハードウェアとソフトウェアの構成の定義をはじめ、サポートの簡素化、メンテナンスコストの削減、セキュリティ脅威に対抗するための共通プラットフォームの維持を行ってきました。次第に各種のエンタープライズソフトウェア管理ツールが広く使われるようになると、これらのシステム上のすべてのソフトウェア、設定、セキュリティポリシーがリモートから一元管理されるようになりました。

当然ながら、IT部門はモバイルデバイスに関しても同様の機能を追求することで、デバイス設定の制御、クライアントサイドソフトウェアの配布と監視、脆弱性の軽減、データリスクの制御を行おうとしています。実際、モバイルデバイスは紛失や盗難に遭いやすく、企業の物理境界によって保護されていないため、IT部門は、これまでデスクトップ向けに用意してきた機能以上のものを必要としています。これに対処するために、各種のソフトウェア、サービス、および特化されたモバイルデバイス管理（MDM）プラットフォームが登場しており、リモートでのデバイスのプロビジョニング、インベントリの追跡、アプリケーションの管理、モバイルデバイスに対するポリシーの実施（企業によるリモート消去方法や現場におけるデバイスの無効化方法を含む）を可能にしています。モバイルデバイスをデスクトップと同じように緊密に管理することによってのみ、企業はデバイスをネットワークの延長として信頼することができます。

信頼できるモバイルアクセス

管理能力だけでは、必ずしも優れたセキュリティが得られるとは限りません。優れた認証がなければ、安全なモバイルデバイスのエコシステムは不完全なものになります。ほとんどのセキュリティ専門家は、ユーザー名とパスワードによるアクセスは、たとえMDMを使用していたとしても、企業のIT資産にとって十分に強力な認証方式ではないことに同意しています。パスワードの頻繁な変更の要求のような、パスワードの弱点を補うためのセキュリティ上の次善策は、しばしば裏目に出ることがあります。なぜなら、ユーザーはパスワードを憶えておくために、それらをメモに書き留めるという手段に訴えるからです。

ベストプラクティスとしてのセキュリティを実現するには、IT管理部門はデバイスのユーザーを企業のネットワーク上で企業アプリケーションと共に信頼できるものにするために、強力なセキュリティクレデンシャルを提供する必要があります。より強力なセキュリティクレデンシャルを使うと、個人の身元を確認するだけでなくデバイスの検証や当該情報の転送の保護も行えるようになります。このようなクレデンシャルは多くの形式を取りますが、これらの要件を満たす最も広く受け入れられているクレデンシャルが、デジタル証明書です。

デジタル証明書が使われる理由

デジタル証明書は、約20年近くにわたってネットワークやデータの安全性の確保に成功してきたという実績があります。公開鍵暗号化技術をベースにしたデジタル証明書は、強力な認証を実現するための優れた選択肢であり、単なるパスワードに比べてはるかに安全です。さらに、認証や暗号化だけでなく幅広いセキュリティ要件をサポートしていることが、デジタル証明書の価値を高めています。デジタル証明書は、Webサイト、VPN、ワイヤレスネットワーク、およびその他のアプリケーションを保護するために利用できます。デジタル証明書がこれほど広く受け入れられるようになったのは、各種の企業認証セキュリティタスクをサポートする単一のクレデンシャルを持つことによりもたらされる柔軟性のおかげです。

デジタル証明書は、Apple iOS®やAndroidのような、ラップトップ、タブレット、およびスマートフォン向けのオペレーティングシステムでもサポートされています。すべてではないにしても多くの企業ネットワークおよびソフトウェアアプリケーションは、デジタル証明書をサポートしています。モバイルデバイスで証明書を使用する主なアプリケーションの一部を図1に示します。

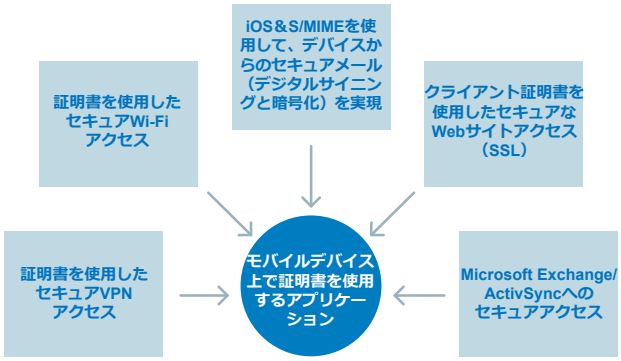

図1：デジタル証明書インフラストラクチャは、多くの企業アプリケーションに対応

デジタル証明書は、キーボードスペースが限られているモバイルデバイス上では、ユーザー名/パスワードを入力するよりもはるかに優れたユーザーエクスペリエンスを提供します。最終的に、デジタル証明書は、透過的な認証の理想的な形式となります。デジタル証明書は、利用に際して人の介入を必要としません（特別なアプリケーションでそうするように特別に設定されていない限り）。また、デジタル証明書は、30日、60日、90日ごとにユーザー名とパスワードを変更しなければならないという煩雑さからユーザーを解放します。

さらに、デジタル証明書は、事実上すべてのエンタープライズMDMソリューションによりサポートされています。MDMでのデジタル証明書の使用が必須ではないことは事実ですが、デジタル証明書を使用しないならば、ユーザー認証やデバイス検証を行うための通信（プロファイルの転送など）が安全でなくなることに注意する必要があります。具体的には、デバイスがプロファイルを持つと、たとえそれが単一のデバイスには送信されないユーザー名／パスワードやワンタイムパスワード（OTP）であったとしても、そのプロファイルを他のデバイスで復元することが可能になります。これらのプロファイルには、企業リソースへのアクセスに使用される平文のクレデンシャルが含まれている可能性があります。このため、すべてのMDMでデジタル証明書を使用してセキュアに転送し、プロファイルを保護することがベストプラクティスの要件となります。

デジタル証明書の重要性に関する表明として、Apple独自のドキュメントで規定されているプロファイルをセキュアに配信するためのプロトコルでは、PKI（デジタル証明書を利用するもの）の利用が要求されることが挙げられます。

多くのセキュリティニーズを満たすためのデジタル証明書の柔軟性は、十分に文書化されています。経験豊富な企業はバックエンドのMDMインフラストラクチャで必要とされる利用に加えて、デジタル証明書の認証クレデンシャルを自社の認証セキュリティ（電子メール、VPN、WiFiなど）に活用することで、投資を最適化し効率性を高めています。

エンタープライズ証明書管理

証明書のサポートはモバイルデバイス上のアプリケーションに組み込まれている場合もありますが、IT部門は、企業側から証明書のライフサイクルを管理する効果的な方法を必要としています。これには、証明書をセキュアにデバイス上に取得すること、証明書の更新、および必要に応じて証明書を失効することが含まれます。証明書管理ライフサイクル内における各種のプロセスを図2に示します。

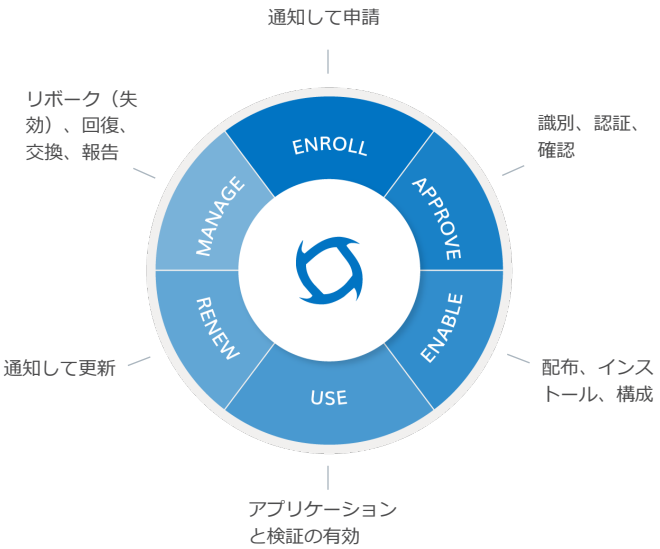

図2：証明書ライフサイクルプロセスの管理が重要

公開鍵暗号方式に基づくデジタル証明書を管理するには、公開鍵基盤（PKI）が必要となります。PKIの主な機能は、証明書（および関連する公開鍵）を正確かつ高い信頼性でユーザーやデバイスに配布すること、および証明書のライフサイクルを管理することです。このような重要な機能を提供するPKIの選択において、企業はPKIソフトウェアを社内に配備するか、それとも信頼性の高いプロバイダーにPKIサービスをアウトソーシングするかを選ぶ必要がありません。MDMを使用するかどうかにかかわらず、すべての社内プロジェクトでは、モバイルデバイスの管理を目的としたPKI配備環境をサポートするためのカスタム拡張が必要となることにご注意ください。

下記に示すオプションは、最も一般的な選択肢の一部です。

- OpenCATMやEnterprise Java Bean Certificate Authority（EJBCA）などのオープンソースソフトウェアツール。これらは、IT部門により自己管理とサポートが行われます。
- Microsoft Active Directory®証明書サービスなどの商用ソフトウェア。これには、初歩的なPKIツールが含まれています。
- DigiCert PKI Platformのような、マネージドサービスとして提供されるターンキー型のクラウドベースのPKIソリューション

企業におけるPKI配備の成功は、利用や管理がいかに容易であるか、そしてユーザーエクスペリエンスがいかにシームレスであるかにかかっているため、企業はどのアプローチを使用するかを慎重に決定する必要があります。さらにこの方法は、広範な種類のアプリケーションやデバイスを通じてこれらのクレデンシャルの利用をグローバルに拡大するため、企業のニーズに合わせて拡張が可能でなければなりません。

企業のニーズと利用可能なリソースを満たすPKIソリューションを選択する際に考慮すべき要因を、下記の表に示します。

成功要因	ホステッド型のPKIプラットフォーム（マネージドPKIサービス）	既製品または市販のPKIソフトウェア
PKI機能	信頼のグローバルルートと認証サービスを伴う完全な機能を備えたPKI。数百社もの企業にサービスを提供してきた、長年にわたる運用経験を持つ実績あるソリューションです。	企業は、サポートするインフラストラクチャの設計、構築、配備を行い、実装と運用の負担を100%引き受けます。
容易な実装	一般的な企業向けWebブラウザ、メールクライアント、企業向けVPN、ワイヤレスネットワークをサポートしています。環境は一般的なアプリケーション用に広く事前にプロビジョニングされており、ポータルは高度にテンプレート化されているため、簡単に利用を開始できます。	多くの場合、重要なカスタマイズや専門的なサービスの支援が必要となります。クロスプラットフォームのサポートが制限される場合や独自のクライアントソフトウェアが必要となる場合があります。
自動化	iOS OTAやMicrosoft AutoEnrollmentなどのクライアント自動化プロトコルをサポートしているため、ユーザーやデバイスの登録が簡単かつ透過的に行えます。証明書は、手動設定の必要なしにユーザーデバイスへと配信できます。	ほとんどのオンプレミスPKIソリューションは、このような機能をほとんど、あるいはまったく提供していません。たとえば、Microsoft Certificate Servicesは、Windows Mobileデバイスを使用した直接発行しかサポートしていません。
可用性とスケーラビリティ	契約で保証されたPKIバックボーンサービスと災害復旧（DR）。高い拡張性。大容量で耐障害性に優れたインフラストラクチャを活用。	企業はインフラストラクチャ、冗長性、および災害復旧（DR）サービスを100%自ら準備します。独自の可用性とスケーラビリティに関する要件を管理する必要があります。
セキュリティとリスク管理	業界をリードする成熟した鍵管理と証明書の実践。米国国防総省やAdobe CDSなどに向けた外部監査される運用およびポリシー認証。	企業はセキュリティインフラストラクチャを100%準備しないといけないほか、独自の運用ポリシーとプラクティスを設計し、リスクを100%引き受ける必要があります。

成功要因	ホステッド型の PKIプラットフォーム（マネージドPKIサービス）	既製品または市販のPKIソフトウェア
人員	DigiCertは、高度なトレーニングを受けたセキュリティのプロフェッショナルであり、厳しい審査プロセスを経ています。セキュリティとPKIに重点を置いており、高度なトレーニングを受け、最新の知識とスキルを有しています。	進化するテクノロジー、標準、リスクに後れずについて行くために人員をトレーニングし、スキルを更新する必要がある。経験不足や人員削減により、導入の遅れやダウンタイムが引き起こされるほか、セキュリティ上の格差が生じる可能性があります。
業務範囲	オンラインでの申請、認証、管理サービスを提供するパブリック認証局（CA）の包括的なポートフォリオ。企業は、プライベートおよび／またはパブリックなトラストネットワーク（世界最大）を選択できます。	企業は完全なカスタムソリューションを構築します。自己署名された証明書を使用したセルフマネージド型のプライベートシステムは、内部アプリケーションへの信頼を制限します。相互認証および検証はプライベートのみです。

DigiCert PKI Platformにより管理の簡素化とコスト削減を実現

DigiCert PKI Platformは、あらゆる規模の企業や組織がモバイルデバイスおよびモバイルデバイス管理環境のための証明書ライフサイクル手順をコスト効率よく配備し管理できるようにする、アウトソーシング型のマネージドサービスです。このプラットフォームは、企業のニーズの拡大に合わせてスケーリングを行うと同時に、証明書管理インフラストラクチャの計画、構築、維持にかかる負担を軽減できます。また、シームレスなユーザーエクスペリエンスを提供すると同時に、適切なポリシーの監視、実践、プロセスを維持するために必要となるすべてのものを管理者に提供します。DigiCert PKI Platformを使用すると、企業は、ユーザーとデバイスの認証セキュリティに関するベストプラクティスの制御を他の方法に比べてより低コストで、より少ない時間とリソースで、最善の結果で維持できるようになります。

DigiCert PKI Platformはクラウドベースのサービスであるため、ソフトウェアとハードウェアのインフラストラクチャはDigiCertによってホスティングされ、サービス契約に含まれています。同時に、クラウドベースのマネージドサービスモデルは、システムとソフトウェアの保守を排除することで運用コストを削減するため、企業はユーザー（特に遠隔地にいることが多いモバイルユーザー）への配備やサポートをより簡単に行えるようになります。DigiCert PKI Platformが持つグローバルリーチ、高可用性（HA）、災害復旧（DR）を企業が独自に実装するには莫大な費用がかかります。また、マネージドサービスアカウントには、99.5%のアップタイムを保証する法的拘束力のあるSLAが付属しているため、サービスを安心して利用できます。

安心してご利用いただけるように、マネージドサービスには99.5%のアップタイムを保証する法的拘束力のあるSLAが付属しています。

DigiCertのお客様である企業は、セキュリティとデータセンターの専門家が世界をリードするエンタープライズクラスのサービスに関して15年以上成功を続けてきた中で培ってきた知識、経験、ベストプラクティスのすべてを活用できます。DigiCertは、企業や個人が今日の複雑なグローバルネットワークを通じて検索、接続、保護、ビジネス取引を可能にするインフラストラクチャを運営しています。インターネットセキュリティとルートキー管理の業界リーダーとして、あらゆる規模の企業向けに最先端の統合PKIサービスプラットフォームを構築しています。実際の経験がDigiCert PKI Platformの設計およびサポートレディネスの基盤となっています。DigiCertの持つ専門知識とインフラストラクチャを活用することで、企業は社内インフラストラクチャの構築、配備、保守にかかる負担を軽減すると同時に、証明書のライフサイクル管理（発行、更新、失効を含む）に関する完全な制御権を確保できます。

DigiCert PKI Platformを使用して証明書管理を簡素化

クラウドベースのDigiCert PKI Platformを使用することで得られるコスト削減に加えて、DigiCert PKI Platformを使用してモバイルデバイスに対して証明書を発行することには、主に3つの運用上のメリットがあります。

1. **MDMソリューションとの統合により、各種の展開モデルを提供：**DigiCert PKI Platformは、Webサービスインターフェイスを介して、MobileIron®、AirWatch®、Fiberlink®、Zenprise®などの多数のMDMソリューションと緊密に統合されているため、さまざまなユーザー層をサポートし、多様な配備モデルを選択できます。
2. **モバイル対応の証明書サービスで証明書の管理が簡単：**DigiCert PKI Platformは、企業の証明書に関する信頼の階層、モバイルデバイスに必要な証明書フォーマット、継続的なユーザー登録、証明書の承認、証明書の検証、その他の運用上の問題に必要となる運用サービスを作成できるように、広く事前にプロビジョニングされたWebベースの環境を提供します。
3. **多様なモバイルプラットフォームやアプリケーションとのダイレクトな統合：**DigiCert PKI Platformは、iOSやAndroidなどの主要なモバイルクライアントプラットフォーム上で高度に統合された機能を提供します。これには、MDMが導入されていない状況であっても、クライアントデバイスとアプリケーションの設定を自動化できるという利点があります。

これ以降に示す例では、DigiCert PKI Platformを使用することでユーザー証明書の登録、配布、インストールがいかに簡素化されるかを示すことで、各種のモバイルデバイスのユースケースにおいて、最も一般的なメリットがどのようにもたらされるかを示します。

DigiCertの持つ専門知識とインフラストラクチャを活用することで、企業は社内インフラストラクチャの構築、配備、保守にかかる負担を軽減すると同時に、証明書のライフサイクル管理（発行、更新、失効を含む）に関する完全な制御権を確保できます。

モバイルデバイス管理システム（MDM）を使った運用

このモデルでは、MDM はモバイルデバイスと証明書サービス間におけるブローカーとして機能します。証明書は、アプリケーションやその他のセキュアなデータの一部であるかのように扱われるため、MDMを使用してデバイス上で管理する必要があります。下図に示すように、MDMサーバーは証明書サービスを通じて証明書を登録した後、独自の構成に基づいて、それらの証明書と関連する構成をモバイルデバイスへとインストールします。

DigiCert PKI Platformは、MDMソリューションによるDigiCertサービスとの統合を容易にするWebサービスインターフェイスを提供します。市場をリードするDigiCert Mobile Managementソリューションを含め、多くのサードパーティがこの方法で統合を行っています。また、DigiCert PKI PlatformはSimple Certificate Enrollment Protocol （SCEP）を提供します。SCEPは、MDMソリューションを通じたセキュアなプロファイルのダウンロードのための基礎を築く、デバイスID証明書の発行に使用されるプロトコルです。

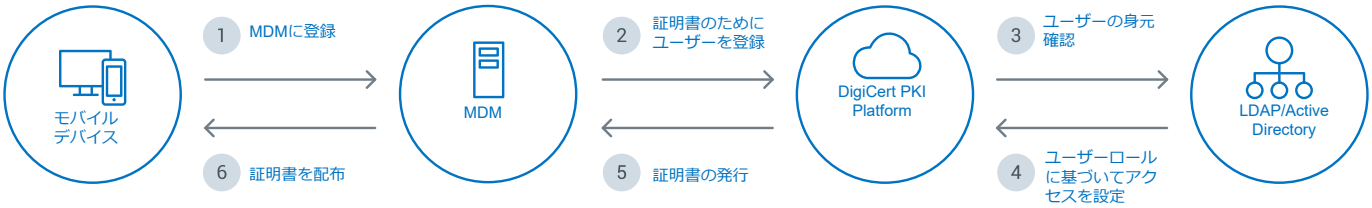

図3：モバイルデバイス管理システム（MDM）を使った運用

モバイル対応の証明書サービスを通じたダイレクトデバイスサポート

このモデルは、モバイルデバイス管理証明書をモバイルデバイス上に配備し、それらを他のアプリケーションでも使用するためのシンプルな軽量ソリューションを求めている企業に適しています。また、このモデルは、非モバイルユーザーを同時にサポートするためにも重要です。

このダイレクトデバイスサポートを利用すると、エンドユーザーは、デスクトップコンピュータで登録する場合と同じように、モバイルデバイス上でも直接証明書を登録できるようになります。登録ページはモバイルデバイス用にフォーマットされており、証明書サービスは証明書のインストールとそれを使用するアプリケーションの両方を自動的に設定します。

これは、エンドユーザーの設定を完全に自動化し透過的にできるという点で、モバイルデバイスのエンドユーザーとそれをサポートするIT部門にとって大きなメリットとなります。たとえば、Apple iOSにおいて、DigiCert PKI Platformは、組み込み型のiOS OTA（Over-the-Air）プロトコル機能を利用することで、iOSデバイスやアプリケーションがSCEP経由で証明書の登録要求を行うことを可能にしています。その後、プラットフォームは、証明書ペイロードと共にiOS OTA設定プロファイルを配信することで、証明書を使用するすべてのアプリケーションにおいて、証明書を使用するようデバイスが自己設定を行えるようにします。iOSデバイスにおけるこのプロセスを下記の図に示します。

iOSでDigiCert PKI Platformを使用する場合に得られるもう1つの大きなメリットは、サービス管理ワークフローによって、管理者がターゲットデバイスのOTA構成管理プロファイルを定義できることです。これにより、管理者のタスクを大幅に簡素化できます。

Androidデバイス、Microsoft Windows®、Apple Mac®タブレットのような、iOS OTAに相当する機能を持たないデバイス向けにDigiCertは、証明書を使用するようにデバイスやアプリケーションを設定する際の複雑さを軽減するWindows PKIクライアントを提供しています。

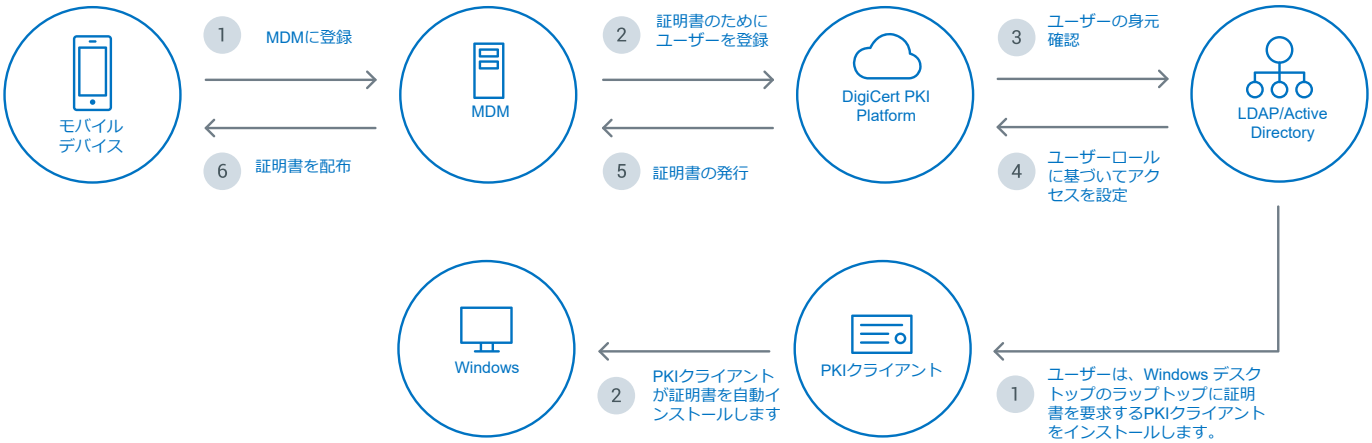

図4：モバイル対応の証明書サービスを通じたダイレクトデバイスサポート

まとめ

デジタル証明書は、パスワードなどの他のクレデンシャル技術に比べてユニークなメリットを提供します。単一のデジタル証明書を使うだけで、さまざまな要件に関する複数のパスワードが必要とされる多くのアプリケーションに対して、より優れた機能とアクセスを提供できるようになります。証明書は、業界で最高のセキュリティクレデンシャルとして認知されているだけでなく、何十年にもわたり使用され進化してきたという実績があります。証明書は、モバイルデバイス管理ソリューションを適切に保護するために必要となるだけでなく、モバイルデバイス上の多くのアプリケーションの内部サポートにも利用できます。DigiCert PKI Platformは、デジタル証明書を使用してモバイルデバイスを保護するためのクラス最高のソリューションを提供します。モバイルデバイスの内部サポートとMobileIron、AirWatch、Fiberlink、Zenpriseなどの主要なモバイルデバイス管理（MDM）パートナーとの幅広いパートナーシップにより、DigiCert PKI Platformは、モバイルデバイス上のコンテンツセキュリティを管理するための卓越したソリューションを提供します。DigiCert PKI Platformは、モバイルデバイス上のコンテンツセキュリティを管理する優れたソリューションを提供しています。これらのデバイスが進化を続けた結果、デスクトップコンピューターの機能を模倣するか、またはそれらを置き換えるようになると、企業はDigiCert PKI Platformを利用して必要なセキュリティクレデンシャルを提供することで、それらのデバイスが信頼され、データが保護され、デバイスが正当なユーザーによってのみ利用可能となることを保証できるようになるでしょう。DigiCert PKI PlatformおよびモバイルデバイスMDMソリューションの詳細については、営業担当者に問い合わせるかhttps://www.digicert.com/jp/をご覧ください。

用語集

認証局：公開鍵基盤（PKI）の一部としてデジタル証明書の発行、失効、または一時停止を行う権限を持つ信頼できる機関です。

デジタル証明書：電子署名の信頼できるセキュアな形式であり、ユーザーの身元確認、文書の完全性、タイムスタンプ、署名された電子文書の否認防止を提供します。

災害復旧（DR）：自然災害または人為的災害後の重要なテクノロジーインフラストラクチャの復旧または継続に向けた準備に関連するプロセス、ポリシー、手順です。

EJBCA（Enterprise Java Bean Certificate Authority）：スウェーデンの非営利企業によりメンテナンスと資金提供を受けているフリーソフトウェア版のPKI認証局用ソフトウェアパッケージです。

モバイルデバイス管理（MDM）：携帯電話事業者、サービスプロバイダー、および企業を通じて配備されたモバイルデバイスの保護、監視、管理、サポートを行うソフトウェアです。MDMの機能には、一般的に携帯電話、スマートフォン、タブレット、モバイルコンピューター、モバイルプリンタ、モバイルPOSデバイスなど、あらゆるタイプのモバイルデバイスに対するアプリケーション、データ、構成設定のOTA（Over-the-Air）配布が含まれています。

OTA（Over-the-Air）：携帯電話のようなデバイスに対して新しいソフトウェアアップデートや構成設定を配布するためのさまざまな方法を意味します。OTA設定は、新しいアップデートやサービスが登場するにつれ、ますます重要になってきています。

公開鍵基盤（PKI）：デジタル証明書の作成、管理、配布、使用、保存、失効に必要なハードウェア、ソフトウェア、人、ポリ シー、および手順からなるセットです。

Simple Certificate Enrollment Protocol（SCEP）：最も普及している証明書登録プロトコルであり、広く利用されている最も実績のあるプロトコルです。SCEPは、デジタル証明書の発行および失効を可能な限りスケーラブルにすることを目的として設計されています。

DigiCertについて

DigiCertは、シマンテックのWebサイトセキュリティ事業に加えて、デジタル証明書を提供するグローバルなリーディングプロバイダーです。世界トップクラスの銀行をはじめ、電子商取引、テクノロジー、医療、製造業などのさまざまな分野の企業が、最も価値のあるオンライン資産向けのスケーラブルな暗号化と認証を提供するために、DigiCertを利用しています。DigiCertは、Webの枠を超えて、モノのインターネット（IoT）やその他の新興コネクテッド市場向けに、アイデンティティ、認証、暗号化を実現する、市場をリードするスケーラブルで自動化されたPKIベースのソリューションを通じて、イノベーションを起こしています。

詳細については、https://www.digicert.com/jp/ のお問い合わせフォームよりお問い合わせください。

digicert®